NIST Special Publication 800-53

Revision 4

連邦政府情報システム
および連邦組織のための
セキュリティ管理策とプライバシー管理策

ジョイントタスクフォースによる
変革への取り組み

http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-53
Revision 4

連邦政府情報システム
および連邦組織のための
セキュリティ管理策とプライバシー管理策

ジョイントタスクフォースによる
変革への取り組み

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

http://dx.doi.org/10.6028/NIST.SP.800-53r4

2013年4月
2014年1月15日時点の更新内容を含む（ページXVII）

米国商務省　長官代理
Rebecca M. Blank

米国国立標準技術研究所　標準技術担当次官兼所長
Patrick D. Gallagher

準拠法令について

この文書は、情報セキュリティに関連して連邦政府の情報システムに対する最低限の要求事項を規定した標準を同様の要求事項を規定した指針とともに策定するよう FISMA と呼ばれる連邦情報セキュリティ管理法（法律第 107-347 号）によって NIST に対して定められた法的義務を果たすために NIST が制定したものである。ただし、国家安全システムに関する政策を決定する権限を有する連邦政府職員による明示的な承認が無い限り、この文書を国家安全システムに対して適用してはならない。

なお、連邦行政管理予算局（OMB）通達 A-130 号の付録 IV（付録名：「重要部門に対する分析」）において分析されている通り、この文書によって NIST によって策定された情報セキュリティに関連して連邦政府の情報システムに対する最低限の要求事項を規定した指針は、連邦行政管理予算局（OMB）通達 A-130 号の第8条 b 項 3 号（見出し：「政府機関の情報システムのセキュリティ」）に規定された要求事項に準拠して策定されている。また、補足情報は、連邦行政管理予算局（OMB）通達 A-130 号の付録 III（付録名：連邦政府の情報リソースとして自動化されたリソースのセキュリティ）に記載されている。ただし、この NIST Special Publication 800-53 の文書のいかなる部分についても標準および指針として連邦政府の商務長官が法的権限に基づいて連邦政府機関に対して順守するよう義務づけたものと相反する解釈がなされてはならない（特に、連邦政府の商務長官が法的権限に基づいて連邦政府機関に対して順守するよう義務づけた指針については、連邦政府の商務長官および連邦行政管理予算局長等のすべての連邦政府高官が現在有している権限を停止・剥奪するものであると解釈してはならない）。

この NIST Special Publication 800-53 の文書は米国著作権法の適用対象ではないため、政府以外の組織はこの文書を自由に利用する事ができる。ただし、出典が明記される事が望ましい。

NIST Special Publication 800-53, Revision 4（2013 年 4 月：460 ページ）
http://dx.doi.org/10.6028/NIST.SP.800-53r4
CODEN: NSPUE2

セキュリティ実験の目的またはセキュリティ実験の手順を過不足無く説明するために、特定の商行為の主体または特定の装置（もしくは特定の資料）がこの文書に記載される可能性がある。ただし、特定の商行為の主体または特定の資料（もしくは特定の装置）がこの文書に記載された場合であっても、NIST が特定の商行為の主体または特定の資料（もしくは特定の装置）を間接的に推奨するものではない。また、特定の商行為の主体または特定の資料（もしくは特定の装置）がセキュリティ実験の目的を達成する上で常に最適なものであるという事を意味するものではない。

なお、この文書においては、自身に対する法的義務を果たすために NIST によって現在策定中の他の文書を参照する場合がある。この場合、連邦政府機関は、この NIST Special Publication 800-53 の文書に記載された情報（すなわち、セキュリティ実験の目的およびセキュリティ実験の手順等）を利用してもよい。ただし、当該参照文書が全て完成するまでは、要求事項・指針・手順として既に策定された文書に記載された事項は引き続き有効である。連邦政府機関は、計画作成および移行を目的として、NIST によるこれらの新文書の作成状況を知りたいと考えるかも。

パブリックコメントの募集期間中に、組織が草案をすべて閲覧のうえ NIST に対して草案のフィードバックを行う事が望ましい。NIST Computer Security Division が発行するすべての文書は、現在策定中の他の文書を除き、http://csrc.nist.gov/publications から入手できる。

この文書に対するご意見は、下記まで:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
電子メール: sec-cert@nist.gov

コンピュータシステムの技術に関する報告書

米国国立標準技術研究所（NIST）の情報技術ラボラトリ（Information Technology Laboratory：ITL）は、米国の経済を発展させるとともに、国内において公共の福祉を増進させる事ができるよう、度量衡および標準規格という国家の骨格をなす制度について技術的な指針を提供している。また、ITL は、テスト（またはテスト技法）を開発するだけではなく、参照データを作成するとともに実証実験を実施しながら技術的な分析を行うことによって、さらなる情報技術の開発に加えて情報技術の生産的利用を促進する。

なお、ITL の責務には、連邦政府の情報システムについて、国家の安全保障情報以外の情報に対する費用対効果の高いセキュリティ関連のシステムプライバシーを実現するための管理面・運用面・技術面・物理面で標準規格を指針とともに策定する事がある。

この NIST Special Publication 800 のシリーズでは、情報システムのセキュリティに関する ITL による調査について情報システムのセキュリティに関する ITL の指針とともに言及される。また、ITL による業界団体・政府機関・学術機関との共同活動についても言及される。

要約

この文書は、連邦政府組織（および連邦政府の情報システム）に対するセキュリティ管理策のカタログを連邦政府組織（および連邦政府の情報システム）に対するプライバシー管理策のカタログと合わせて提示する文書であるとともに、さまざまな脅威（自然災害・人的ミス・悪質なサイバー攻撃・構造上の欠陥等）から（組織の）ミッション・（組織が有する）機能・（組織の）イメージ・（組織に対する）評判・（組織の）業務・（組織の）資産・個人・他組織・国家を保護するために管理策を選択するプロセスを提示する文書である。当該管理策は、カスタマイズが可能な管理策であるだけではなく、組織全体にわたって情報セキュリティをプライバシーリスクとともに管理するプロセスの一部として実装される管理策であるとともに、連邦政府（または重要インフラ）の全体に対して法律・大統領命令・政策・指令・規制・標準のいずれか（または全て）が要求する（またはミッションニーズ・業務ニーズから要求される）セキュリティ（またはプライバシー）要求事項に対応するための管理策である。

なお、この文書には、（特定の）ミッション・（特定の）業務機能・（特定の）技術・（特定の）システム・（特定の）稼動環境のいずれかに合わせて調整された特殊なセキュリティ管理策一式をどのように策定するかとともに、（特定の）ミッション・（特定の）業務機能・（特定の）技術・（特定の）システム・（特定の）稼動環境のいずれかに合わせて調整された特殊なオーバーレイをどのように形成するかについても記載されている。

セキュリティ管理策カタログは、セキュリティ機能性（セキュリティ管理策によってもたらされるセキュリティ機能の強度およびセキュリティ管理策によってもたらされるセキュリティメカニズムの強度）ならびにセキュリティ保証（実装されたセキュリティ機能の信頼性）の 2 つの観点からセキュリティを確保する管理策のカタログである。機能性およびセキュリティ保証の 2 つの観点からセキュリティが確保される事で、IT 製品および当該 IT 製品をもとにシステムエンジニアリング・セキュリティエンジニアリングのそれぞれの原理を適切に応用して構築された情報システムは、十分に信頼に値するものになる。

キーワード

セキュリティ保証・コンピュータセキュリティ・FIPS Publication 199・FIPS Publication 200・FISMA・プライバシー保護法・リスク管理フレームワーク・セキュリティ管理策・セキュリティ要求事項

謝辞

この文書は、連邦政府のために情報セキュリティに関する統一的な枠組みを構築するための継続的な取り組みの一環として、民間・軍隊・情報機関のそれぞれの代表からなる省庁間作業グループである *Joint Task Force Transformation Initiative* によって作成された文書である。NIST は、上記省庁間作業グループの構成員または商務省・国防総省・国家情報長官室・国家安全保障システム委員会のそれぞれのシニアリーダーとしてこの文書の発行に尽力し大きく貢献した以下の方に対して、ここに感謝の意を表明する:

米国国防総省

Teresa M. Takai
DoD Chief Information Officer

Robert J. Carey
Principal Deputy DoD Chief Information Officer

Richard Hale
Deputy Chief Information Officer for Cybersecurity

Dominic Cussatt
Deputy Director, Cybersecurity Policy

国家情報局

Adolpho Tarasiuk Jr.
Assistant DNI and Intelligence Community Chief Information Officer

Charlene Leubecker
Deputy Intelligence Community Chief Information Officer

Catherine A. Henson
Director, Data Management

Greg Hall
Chief, Risk Management and Information Security Programs Division

NIST

Charles H. Romine
Director, Information Technology Laboratory

Donna Dodson
Cybersecurity Advisor, Information Technology Laboratory

Donna Dodson
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

国家安全保障システム委員会

Teresa M. Takai
Chair, CNSS

Richard Spires
Co-Chair, CNSS

Dominic Cussatt
CNSS Subcommittee Tri-Chair

Jeffrey Wilk
CNSS Subcommittee Tri-Chair

Richard Tannich
CNSS Subcommittee Tri-Chair

Joint Task Force Transformation Initiative

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Richard Graubart *The MITRE Corporation*	Kelley Dempsey *NIST*
Esten Porter *The MITRE Corporation*	Bennett Hodge *Booz Allen Hamilton*	Karen Quigg *The MITRE Corporation*	Christian Enloe *NIST*
Kevin Stine *NIST*	Jennifer Fabius *The MITRE Corporation*	Daniel Faigin *The Aerospace Corporation*	Arnold Johnson *NIST*
Lisa Kaiser *DHS*	Pam Miller *The MITRE Corporation*	Sandra Miravalle *The MITRE Corporation*	Victoria Pillitteri *NIST*

上記の謝辞にて列挙した方に加えて、事務的なサポートに加えて技術的文章の編集に手腕を発揮頂いた Peggy Himes および Elizabeth Lennon の各氏（両氏とも NIST に所属）に対して、特に感謝の意を表明する。また、Marshall Abrams・Nadya Bartol・Frank Belz・Deb Bodeau・Dawn Cappelli・Corinne Castanza・Matt Coose・George Dinolt・Kurt Eleam・Jennifer Guild・Cynthia Irvine・Cass Kelly・Steve LaFountain・Steve Lipner・Tom Macklin・Tim McChesney・

Michael McEvilley・John Mildner・Joji Montelibano・George Moore・LouAnna Notargiacomo・Dorian Pappas・Roger Schell・Carol Woody の各氏および NIST Computer Security Division の調査スタッフには、この文書の内容がより良いものになるよう並々ならぬ貢献を頂いた事に対しても、感謝の意を表明する。

なお、国内外・官民を問わず様々な個人・作業部会・団体がこの文書の発行に貢献したという事についても理解しており、ここに大いなる感謝の意を表明するものである。様々な個人・作業部会・団体による建設的かつ思慮深い意見によって、この文書の品質が全般的に向上するとともに、内容がより一貫した文書（かつより実用的なもの）になった。

FIPS 200とSP 800-53との関係

情報セキュリティ標準および指針を実装する

FIPS Publication 200（題名：「連邦政府の情報および連邦政府の情報システムに対する最低限のセキュリティ要求事項」）は、FISMAに対応してNISTが策定した連邦標準規格として強制力のある規格である。FIPS Publication 200に準拠できるよう、組織は、組織の情報システムのセキュリティをFIPS Publication 199（題名：「連邦政府の情報のセキュリティおよび連邦政府の情報システムのセキュリティの分類に関する規格」）に基づいて分類した上で、セキュリティの分類が組織の情報システムに与える影響をFIPS 200に基づいて判断する。その上で、調整されたベースライン管理策セットとしてNIST Special Publication 800-53（題名：「連邦政府の情報システムおよび連邦政府組織に対して策定されるセキュリティ管理策および連邦政府の情報システムおよび連邦政府組織に対して策定されるプライバシー管理策」）に記載されたセキュリティ管理策を適用する。

なお、NIST Special Publication 800-53に記載された手引きの通りセキュリティ管理策のベースライン管理策を柔軟に適用する事が可能な組織は、組織のミッションおよび組織に対する業務上の要求事項ならびにシステムの稼働環境により適合したセキュリティ管理策のベースライン管理策を適用する事ができるよう、適用するベースライン管理策を調整する事ができる。

FIPS 200およびNIST Special Publication 800-53は、連邦政府のあらゆる情報および連邦政府のあらゆる情報システムに対して適切なセキュリティ要求事項および適切なセキュリティ管理策が確実に適用されるようにするための文書である。

なお、組織がリスクを管理する事によって、当初選択したセキュリティ管理策が妥当であったかを判断できるようになるとともに、（組織の）業務・（組織の）ミッション・（組織の）機能・（組織の）イメージ・（組織の）評判・（組織の）資産・個人・他組織・国家を保護するために追加でセキュリティ管理策を策定する事が必要であるか否かを判断できるようになる。当初選択されたセキュリティ管理策として妥当な管理策（または追加で策定されたセキュリティ管理策）は、組織がどの程度セキュリティを評価したのかを示す管理策である。

情報セキュリティの共通基盤の構築

官民提携

FISMA によって策定する事が義務化された標準を同様に策定が義務化された指針とともに策定するにあたり、作業の重複という不要かつ無駄な費用を生じさせる行為を避けながら情報セキュリティの向上を図る事ができるよう（なおかつ標準・指針として策定しようとする文書が国家の国家安全システムを保護するために策定された標準・規格に完全に準拠したものであるよう）、NIST は他の連邦政府機関のみならず民間部門にも助言を求める。また、FISMA によって策定する事が義務化された標準を同様に策定が義務化された指針とともに策定するに当たり、NIST は、公開の場で行われる包括的な策定プロセスの構築に加えて、国家情報長官室(ODNI)・国防総省(DoD)・国家安全保障システム委員会(CNSS)と連携して、連邦政府に対して適用されるべき統一的な情報セキュリティフレームワークの構築に努める。

なお、国防部門・情報部門とその取引先に同じく、連邦政府の非軍事部門とその取引先は、情報セキュリティの共通基盤が構築される事によって、情報セキュリティに関連して（組織の）業務・（組織の）資産・個人・他組織・国家が負うリスクをより効率的かつ合理的に管理できるようになる。また、情報セキュリティの共通基盤が構築される事によって、連邦政府とその取引先との間でセキュリティ認可が確実に実行されるようになるとともにより一層の情報共有が図られるようになる。

NIST は、官民の多くの機関と連携して、NIST ならびに ISO および IEC によって策定されたセキュリティ標準が NIST ならびに ISO および IEC によって策定されたガイドラインと関連性を有する事ができるように努める。

セキュリティ要求事項

さまざまな利害関係者から見た場合

「セキュリティ要求事項」という用語は、さまざまなコミュニティやグループによってさまざまな意味合いで用いられている。ただし、様々な意味合いで用いられている「セキュリティ要求事項」という用語が具体的にどのような場面で用いられているかについて、より詳しく明らかにする必要が生じる可能性がある。

なお、FISMA および FIPS Publication 200 において定義されたセキュリティ要求事項のように、セキュリティ要求事項は、法律・大統領命令・指令・政策・標準に加えて、ミッションニーズ（および／または業務ニーズ）を記した文書等において高度に抽象的な形で定義する事ができる。

購買担当者は、ミッションニーズ（および／または業務ニーズ）を満たす上で必要なセキュリティを確保できるようにする購買契約を締結できるよう、セキュリティ要求事項を定義する。また、システムエンジニア・セキュリティエンジニア・システム開発者・システムインテグレータは、情報システムのセキュリティ設計要件を定義するのに加えて、システムセキュリティアーキテクチャおよび当該アーキテクチャに固有のセキュリティ要求事項を定義するとともに、ハードウェアコンポーネント・ソフトウェアコンポーネント・ファームウェアコンポーネントのそれぞれに固有のセキュリティ機能を実装する。

セキュリティ要求事項は、ハードウェアコンポーネント・ソフトウェアコンポーネント・ファームウェアコンポーネントのそれぞれに対するセキュリティ管理策のうち、組織の内部で情報を管理・運用する際のポリシー（または組織の内部で情報を管理・運用する際の手順）といった非技術的なセキュリティ管理策の内容に反映される。ただし、ポリシー・アーキテクチャ・調達・エンジニアリングのそれぞれの責任者に加えて、ミッションおよび／または業務を保護する責任を有する個人等の集団が互いの意図を明確に伝える事ができるよう、「セキュリティ要求事項」という用語をどのような場合に用いるのか定義する事が重要である。

組織は、セキュリティ要求事項を満たす事によってミッション・業務を適切に保護する上で必要な特定の能力をセキュリティ能力として定義してもよい。ただし、通常、セキュリティ能力は必要に応じて適切に調整されたベースライン管理策の中から特定のセキュリティ管理策（すなわち保護手段および／または保護対策）一式を抽出する事によって定義される。

技術的・政策的な中立性について

セキュリティ管理策の特徴

セキュリティ管理策カタログを構成するセキュリティ管理策は、その拡張管理策と同様、わずかな例外を除き技術的・政策的に中立な管理策である事から、処理中・保存中・伝送中の情報を保護する上で必要となる基本的な機能のうちもっぱら安全機能・防護機能について策定された管理策であるため、この文書は（特定の）技術・（特定の）稼働環境・（特定の）利害関係者・（特定の）ミッション・（特定の）業務機能のいずれかを保護するためにセキュリティ管理策を適用するに当たっての手引きを提供する文書となり得ない。

なお、アプリケーションに固有の領域については、セキュリティ管理策を調整するプロセスとしてこの文書の第3章に記載されているプロセスとともに、オーバーレイの利用についてこの文書の付録Ｉに記載されている事項を参照の事。ただし、セキュリティ管理策カタログを構成するセキュリティ管理策が一部の例外を除き技術的・政策的に中立な管理策である事は、セキュリティ管理策が政策・技術と無縁である事を意味するものではなく、セキュリティ管理策が確実かつ適切に実装されるようにするためにも、政策を技術とともに理解する事が必要である。

まれにセキュリティ管理策が特定の技術（例：携帯機器・公開鍵基盤・無線通信・VOIP）を保護するために策定される場合があるため、十分なセキュリティを確保するためには、組織は特定の技術を保護するための1つのセキュリティ管理策でセキュリティ要求事項のすべてを満たす事ができないという事に留意しなければならない。また、安全機能・防護機能として必要な機能の多くは、セキュリティ管理策カタログを構成する他のセキュリティ管理策のうち、セキュリティ計画を策定するとともにオーバレイを合わせるに当たって当初ベースライン管理策として割り当てられたセキュリティ管理策によって実現する機能である。ただし、異なるセキュリティ管理策ファミリに属するセキュリティ管理策が特定の技術を保護する場合、内容が重複する場合がある。

特定のオーバーレイとともに顧客によって策定される特定のセキュリティ計画に加えて、NISTが発行するSpecial Publicationsは、同じくNISTが発行するInteragency Reportsとともに、スマートグリッド・産業用制御システム・携帯機器といった特定の技術向けに推奨されるセキュリティ管理策に加えて、特定のセクター（例：保険医療部門）向けのアプリケーション向けに推奨されるセキュリティ管理策に関する手引きを提供する事ができる。

技術的・政策的に中立なセキュリティ管理策カタログの利用は、組織に

- 組織の情報システムにおいて利用されている情報技術に関係なく、ミッションおよび／または業務を成功させるうえで必要かつ情報を保護するうえで必要なセキュリティを確保できるようになる
- （特定の）技術・（特定の）運用環境・（特定の）ミッション・（特定の）業務機能・（特定の）COI のぞれぞれに対して個別のセキュリティ管理策が適用可能かどうか分析できるようになる
- 流動的な内容が含まれたセキュリティ管理策を調整するプロセスのなかで、セキュリティポリシーを特定する事ができるようになる

といった利点をもたらす。

調整に関するガイダンスがオーバーレイとともに含まれた専門的なセキュリティ計画を技術的かつ政策的に中立なセキュリティ管理策一式と共に策定する事によって、いかなる部門・技術・運用環境においても、組織はリスクベースの情報セキュリティを最小限の費用で最大限確保できるようになる。

情報セキュリティ評価

組織のミッション（および／または組織の業務）に対するリスク管理

このNIST Special Publication 800-53の文書に記載されたセキュリティ管理策は、関連する連邦法・大統領命令・指令・政策・規制・標準・指針に準拠したセキュリティを確保できるようにするための管理策である。ただし、関連する連邦法・大統領命令・指令・政策・規制・標準・指針に準拠したセキュリティの確保とは、静的なチェックリストに準拠する事を意味するものではないとともに、FISMAによって要求された報告に関連して不要な書類を作成させる事を意味するものでもない。関連する連邦法・大統領命令・指令・政策・規制・標準・指針に準拠したセキュリティを確保するためには、組織が情報セキュリティリスクの管理について評価しなければならない。

なお、情報セキュリティは、組織全体にわたるリスク管理プログラムの一環として調整に関するガイダンスを効果的に活用できるよう（なおかつNIST Publications本来の柔軟性を効果的に活用できるよう）、あらゆる情報を適正に利用する事によっても評価される。情報セキュリティがあらゆる情報を適正に利用する事によって評価される事で、この文書に記載されたセキュリティ管理策から組織のセキュリティ計画に記載するために選ばれた管理策は、ミッション上組織に要求される事項（および／または業務上組織に要求される事項）を満たすセキュリティ管理策となる。

（組織の）業務・（組織の）資産・個人・他組織・国家が現在直面している脅威に対処するためのメカニズムとして必要十分な安全対策等を策定・実装・維持するうえで、組織が手持ちのリスク管理ツールを手持ちのリスク管理技術とともに活用する事が不可欠である。また、連邦政府のすべてのシステムは、リスクベースのプロセスをそれぞれリスクベースの手順・技術とともに効果的に利用する事によって、連邦政府が現時点で負っている責任をまっとうする上で必要な障害許容力を確保できるようになるだけではなく、重要インフラ用のアプリケーションを最適化する上で必要な障害許容力を確保できるようになるとともに、連邦政府の業務の継続性を担保する上で必要な障害許容力を確保できるようになる。

プライバシー管理策

連邦政府が有する情報のプライバシー保護

この文書の付録J（題名：「プライバシー管理策カタログ」）は、このRevision 4の文書において新規に追加された内容である。当該付録は、連邦政府機関に求められるプライバシー管理とは何かを明らかにするために追加された部分である。

なお、当該付録は、

- 組織がそれぞれ関連する連邦法・大統領命令・指令・指示・規制・政策・標準・指針・（特定の組織を対して発令された）文書等に従う事ができるようベストプラクティスに基づいて策定された体系的なプライバシー管理策一式を記載した文書でありながら、
- 連邦政府機関・（連邦政府の）情報システム・（連邦政府の）プログラムのそれぞれに対するセキュリティ（またはプライバシー）要求事項のうち概念的に重複する可能性のある要求事項を必ず満たす事ができるようプライバシー管理策をセキュリティ管理策と関連付けるのに加えて、連邦政府機関・（連邦政府の）情報システム・（連邦政府の）情報プログラムのそれぞれに対するセキュリティ（またはプライバシー）要求事項のうち重複して実装される可能性のある要求事項を必ず満たす事ができるようプライバシー管理策をセキュリティ管理策と関連付ける文書であるとともに、
- 連邦政府・（連邦政府の）情報システム・（連邦政府の）プログラムのそれぞれに対して策定されたプライバシー管理策を選択・実装・評価しながらモニタリングする際に、NISTが発行するリスク管理フレームワークが適用可能な事を示す文書であるのに加えて、
- プライバシー関連の連邦法・（プライバシーに関連した連邦政府の）政策・（連邦政府によるプライバシー関連の）規制・（プライバシーに関連した連邦政府の）指令・（プライバシーに関連して連邦政府が制定した）規格・（プライバシーに関連して連邦政府が制定した）手引のそれぞれが要求する事項を確実に満たす事ができるようにするという経営幹部の目論見が成功するよう、連邦政府の個人情報管理担当職員とセキュリティ担当職員のそれぞれがより一層緊密に連携できるようにする文書である。

当該付録Jに記載されたプライバシー管理策は、この文書のそれぞれ付録Fおよび付録Gに記載されたセキュリティ管理策の構造と非常に類似している。例えば、当該付録Jに記載されたプライバシー管理策は、この文書のそれぞれ付録Fおよび付録Gに記載されたセキュリティ管理策とともに、AR-1（ガバナンスおよびプライバシープログラム）のプライバシー管理策が組織に対して組織レベルまたはプログラムレベルで実装可能なプライバシー計画を策定するよう要求している。当該プライバシー計画は、組織がセキュリティ管理策一式と合わせて適切なプライバシー管理策一式を（組織の）ミッション・（組織における業務上の）要求事項・（組織が業務を行う）環境のそれぞれに応じて適切に選択できるようにするプライバシー計画として、セキュリティ計画とともに利用可能な計画である。

なお、情報セキュリティのリスクを管理する際に用いられる概念と同一の概念を導入する事で、組織は費用対効果に優れたリスクベースのプライバシー管理策を個人のプライバシーを保護しつつ法令上従わなくてはならない要件を満たしながら実装できるようになる。当該プライバシー管理策は、組織がプライバシーに関連して連邦政府によって要求された事項を満たす（なおかつ組織が当該要求事項に準拠している事を示す）ための管理策として、より統一的かつ厳格なアプローチである。

注意

NIST SPECIAL PUBLICATION 800-53の改定よって変更された内容の実装について

NIST が Special Publication 800-53 を改訂する場合、主に①付録 F・付録 G・（上位・中位・下位の）ベースライン管理策のいずれか（もしくはそれらのすべて）に追加されたセキュリティ管理策（※拡張管理策が含まれる場合あり）または付録 F・付録 G・（上位・中位・下位の）ベースライン管理策のいずれか（もしくはそれらのすべて）から削除されたセキュリティ管理策（※拡張管理策が含まれる場合あり）②補足的ガイダンス③主な章（または主な付録）の内容④用語（※文書全体を通しての明確化および／または更新）の 4 点について変更する。

なお、既存のセキュリティ管理策のベースライン管理策として調整済みの下位の管理策を（NIST Special Publication 800-39 に記載の通り）修正するとともに任意のセキュリティ管理策を NIST Special Publication 800-53 の改訂として更新する場合、組織は許容可能なリスクを直近で評価した結果に基づいてセキュリティ管理策を慎重に変更・更新するのが望ましい。

また、OMB によるポリシーによって規定されている場合を除き、この Special Publication 800-53 の文書の改訂内容を実装するに当たっては、

- まず、追加されたセキュリティ管理策（および／または拡張管理策として追加された管理策）が組織の情報システム（またはシステムの運用環境）に適用可能な管理策であるかどうか、組織がこの文書に記載された調整ガイドラインに従って判断する
- 次に、Revision 3 からの変更部分が組織の何らかの情報システムに対して適用されるかどうかとともに組織による何らかのアクションが直ちに必要かどうかについて組織が判断できるよう、この Revision 4 の文書全体を通して、補足的ガイダンスに対する変更とともに主な章および主な付録に記載された指針に対する変更について組織がレビューするのに加えて、この文書において新たに更新および／または明確化された用語について組織がレビューする
- 最後に、補足的ガイダンスに対する変更とともに主な章および主な付録に記載された指針に対する変更として必要に応じて行われる Special Publication 800-53 の文書の全面的な改訂を組織が決定した場合、可能な限り既存のセキュリティモニタリングのプロセスのなかで行う。ただし、補足的ガイダンスに対する変更とともに主な章および主な付録に記載された指針に対する変更として必要に応じて行われる Special Publication 800-53 の文書の全面的な改訂を順次実装するに当たっては、特定のアクティブな脅威に対処するために修正または新たに策定されたセキュリティ管理策を実装する事を常に最優先させる一方、既存のレビューサイクルのなかで原則としてテンプレート変更または若干のポリシー変更もしくは若干の手順変更等を最後に行う

の 3 つの活動を実施するのが望ましい。

目次

序文

「・・・リスク管理プロセスのなかで、（米国の）リーダーは、サイバー空間を悪用する敵が米国の権益を侵害するリスクを勘案する一方で、自国が軍事作戦上・諜報活動上・ビジネス上の目的を達成しようとするなかでグローバルなサイバー空間を利用する事から生じるリスクについても勘案しなければならない・・・」

「・・・業務計画を策定するうえで①（サイバー攻撃の）主な動向を把握する②（サイバー攻撃の）脅威からの影響を無くす（または小さくする）ために何をしなければならないかについて決定する③（サイバー攻撃に対する）脆弱性を解消する（または弱める）ために何をしなければならないかについて決定する④サイバー空間上で行われる全ての活動を評価・調整するとともにサイバー空間上で行われる活動が重複しないようにするために何をしなければならないかについて決定するためには、（サイバー攻撃の）脅威・（サイバー攻撃に対する）脆弱性・（サイバー攻撃から受ける）影響を同時に評価しなければならない・・・」

「・・・あらゆる立場のリーダーは、他のあらゆる部署と同等の体制を整備のうえセキュリティを確保する責任がある・・・」

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

前文

この NIST Special Publication 800-53, Revision 4 は、2009 年に結成された合同タスクフォースとしての省庁間パートナーシップの一環として NIST・国防総省・諜報当局・国家安全保障システム委員会の四者によって策定された文書にして、NIST Special Publication 800-53 が発行された 2005 年以降に行われたセキュリティ管理策カタログに対する最も包括的な改正である。この改正が行われた背景には、敵の動きがより速くなりサイバー攻撃がより巧妙になっている（すなわち、攻撃がより頻繁になっているとともに、攻撃の持続性および攻撃者の専門性がより高くなっている）ために脅威が増大している事が大きい。

なお、現時点で実用化されているセキュリティ管理策（およびその拡張管理策）としてこの文書に記載されているものは、モバイルコンピューティング・クラウドコンピューティング・アプリケーションセキュリティ・信頼性・セキュリティ保証・（情報システムの）回復性・インサイダー脅威・サプライチェーンセキュリティ・APT 攻撃などに関するセキュリティ管理策カタログとして一体的に策定されたものである。この文書では、国際的に認められた「公正な情報取扱原則」（Fair Information Practice Principles）に基づいて新たに定められた8つのプライバシー管理策ファミリが記載されているとともに、サイバー攻撃等の脅威が顕在化した場合により弾力的に対処する事が可能なシステムを構築できるよう、情報セキュリティおよびリスク管理に対するより**包括的**なアプローチとして、「Build It Right（正しいモノづくり）」戦略の名目で、組織の情報システムにとどまらず組織の情報システムの運用環境を抜本的に強化するうえで欠かせない詳細なセキュリティ管理策が幅広く組織に提供されている。また、当該戦略によって策定されたセキュリティ管理策とセキュリティモニタリングを継続的に行うために策定された数多くのセキュリティ管理策とがグループ化される事により、ミッションクリティカルな業務に対するリスクベースの経営判断を継続的に行なう上級幹部職員にとって必要不可欠な情報がリアルタイムに近い状態で組織に提供される。

セキュリティ管理策およびプライバシー管理策のそれぞれの拡張管理策セットを有効に活用できるよう（なおかつ組織が自らの情報システムをより柔軟かつ迅速に保護できるよう）この文書において取り入れられているのは、「オーバーレイ」の概念である。カタログとしてまとめられた脅威ベースのセキュリティ管理策およびその拡張管理策の数が増えているため（また、セキュリティを確保するためにリスクをあらかじめ定められた許容可能な範囲内に留めるというリスク管理戦略が組織によって個別に策定されるため）、組織がセキュリティ管理策のベースライン管理策を調整しながら特定のミッションおよび特定の業務（ならびに特定のシステム運用環境および特定の技術）のすべて（またはそれらのいずれか）に対して個別に適用可能なセキュリティ計画を策定できるようにする体系的な概念として、オーバーレイの概念は重要な役割を果たす。

なお、セキュリティ管理策およびプライバシー管理策のそれぞれの拡張管理策セットが組織にとってより使いやすいものになるよう、この文書では、下記の通り列挙した内容が新たに追加されている:

- セキュリティ管理策のベースライン管理策を策定するにあたり前提となる事項

  管理策の調整に関連して拡張・更新・統合されたガイダンス
- セキュリティ管理策またはプライバシー管理策を追加で割り当てるステートメントまたはセキュリティ管理策またはプライバシー管理策を追加で選択するステートメントのオプション

- セキュリティ管理策の拡張管理策（およびプライバシー管理策の拡張管理策）の説明的な名前
- ベースライン管理策ごとにセキュリティ管理策およびその拡張管理策を管理策ファミリとしてまとめた管理策一覧
- セキュリティ管理策が確実に策定・評価・運用されるようにする目的で作成されたセキュリティ管理策一覧
- 国際的な情報セキュリティ評価基準である ISO/IEC 15408（コモンクライテリア）に基づいて評価されるマッピングテーブル

より柔軟に管理策が実装できるようにするために、この文書に記載されたセキュリティ（またはプライバシー）管理策は、ポリシー（または技術）に大きく左右される事がないよう、おおむね中立的に設計されている。また、この文書に記載されたセキュリティ（またはプライバシー）管理策は、情報セキュリティおよびプライバシーの２つの考え方を組織のプロセス（エンタープライズアーキテクチャプロセス・システムエンジニアリングプロセス・システム開発ライフサイクルおよび購買プロセス等）に組み込むのに最適な管理策である。

なお、この文書に記載されたセキュリティ（またはプライバシー）管理策が組織のプロセスに完全に組み込まれた場合、セキュリティ（またはプライバシー）プログラムの成熟度が高まった事を意味するとともに、セキュリティ（またはプライバシー）関連の投資が組織の中核的業務および組織の中核的ミッションとより密接に関係したものになる。

ジョイントタスクフォース

正誤表

この文書（Revision 4）において旧版から変更された内容は、以下の通りである。

日付	タイプ	変更内容	頁
05-07-2013	編集	表 D-2 内の CA-9 の優先順位コードを P1 から P2 に変更。	D-3
05-07-2013	編集	表 D-2 内の CM-10 の優先順位コードを P1 から P2 に変更。	D-4
05-07-2013	編集	表 D-2 内の MA-6 の優先順位コードを P1 から P2 に変更。	D-5
05-07-2013	編集	表 D-2 内の MP-3 の優先順位コードを P1 から P2 に変更。	D-5
05-07-2013	編集	表 D-2 内の PE-5 の優先順位コードを P1 から P2 に変更。	D-5
05-07-2013	編集	表 D-2 内の PE-16 の優先順位コードを P1 から P2 に変更。	D-5
05-07-2013	編集	表 D-2 内の PE-17 の優先順位コードを P1 から P2 に変更。	D-5
05-07-2013	編集	表 D-2 内の PE-18 の優先順位コードを P2 から P3 に変更。	D-5
05-07-2013	編集	表 D-2 内の PL-4 の優先順位コードを P1 から P2 に変更。	D-6
05-07-2013	編集	表 D-2 内の PS-4 の優先順位コードを P2 から P1 に変更。	D-6
05-07-2013	編集	表 D-2 内の SA-11 の優先順位コードを P2 から P1 に変更。	D-6
05-07-2013	編集	表 D-2 内の SC-18 の優先順位コードを P1 から P2 に変更。	D-7
05-07-2013	編集	表 D-2 内の SI-8 の優先順位コードを P1 から P2 に変更。	D-8
05-07-2013	編集	表 D-17 内の SA-5 (6) への言及を削除。	D-32
05-07-2013	編集	表 E-2 から CM-4 (3)を削除。	E-4
05-07-2013	編集	表 E-3 から CM-4 (3) を削除。	E-5
05-07-2013	編集	SA-5 (6)への言及を削除。	F-161
05-07-2013	編集	SI-16 の優先順位コードを P0 から P1 に変更。	F-233
01-15-2014	編集	Abstract の 5 行目の"(both intentional and unintentional)"を削除。	iii
01-15-2014	編集	Abstract の 5 行目の"security and privacy" を削除。	iii
01-15-2014	編集	セクション 2.1 の RMF Step 2 内の"an initial set of baseline security controls"を"the applicable security control baseline"に変更。	9
01-15-2014	編集	以下の段落を削除："The security control enhancements section provides…in Appendix F."	11
01-15-2014	編集	セクション 2.3、第 2 段落、6 行目の"baseline security controls"を"the security control baselines"に変更。	13
01-15-2014	編集	セクション 3.1、第 2 段落、4 行目の"an initial set of security controls"を"the applicable security control baseline"に変更。	28
01-15-2014	編集	セクション 3.1、第 2 段落、5 行目の"security control baselines"を"baselines identified in Appendix D"に変更。	28
01-15-2014	編集	セクション 3.1、第 3 段落、3 行目の"an appropriate set of baseline controls"を"the appropriate security control baseline"に変更。	29
01-15-2014	編集	セクション 3.1、第 3 段落、4 行目の"security control baseline"の前の"initial"を削除し、"impact level"の前に"FIPS 200"を追加。	29
01-15-2014	編集	セクション 3.1、第 3 段落、6 行目の"sets of baseline security controls"を"security control baselines"に変更。	29
01-15-2014	編集	セクション 3.2、第 1 段落、1 行目の"initial set of baseline security controls"を"applicable security control baseline"に変更。	30

日付	タイプ	変更内容	頁
01-15-2014	編集	セクション 3.2、第 3 段落、5 行目の"initial set of baseline security controls"を"applicable security control baseline"に変更。	31
01-15-2014	編集	セクション 3.2、Applying Scoping Considerations、Mobility の段落、1 行目の"security controls"の前の"set of"を削除。	33
01-15-2014	編集	セクション 3.2、Applying Scoping Considerations、Mobility の段落、2 行目の"set of"の前の"initial"を削除。	33
01-15-2014	編集	セクション 3.2、Applying Scoping Considerations、Mobility の段落、3 行目の"the baselines"を"each baseline"に変更。	33
01-15-2014	編集	セクション 3.2、Applying Scoping Considerations、Mobility の段落、5 行目の"initial set of security controls"を"security control baseline"に変更。	33
01-15-2014	編集	セクション 3.2、Applying Scoping Considerations、Mobility の段落、6 行目の"locations"の前に"specific"を追加。	33
01-15-2014	編集	セクション 3.2、Applying Scoping Considerations、Mobility の段落、8 行目の"initial"を"three"に変更。	33
01-15-2014	編集	セクション 3.2、Selecting Compensating Security Controls、10 行目の "initial set of baseline security controls"を"applicable security control baseline"に変更。	36
01-15-2014	編集	セクション 3.3、1 行目の"a set of initial baseline security controls"を "security control baselines"に変更。	40
01-15-2014	編集	Policies, Directives, Instructions, Regulations, and Memoranda の 3.内の "C.F.R"の後に"."を追加。	A-1
01-15-2014	編集	References の NIST Special Publication 800-52 の後に"Revision 1 (Draft)"を追加。	A-7
01-15-2014	編集	NIST Special Publication 800-52, Revision 1 のタイトルに "Configuration,"を追加。	A-7
01-15-2014	編集	NIST Special Publication 800-52, Revision 1 の日付を 2013 年 9 月に変更。	A-7
01-15-2014	編集	Glossary 内の Information Security Program Plan の後に Information Security Risk の定義を移動。	B-11
01-15-2014	編集	表 D-2 内の AC-2 の「高位影響のベースライン」に (11)を追加。	D-2
01-15-2014	編集	表 D-2 内の AC-10 の優先順位コードを P2 から P3 に変更。	D-2
01-15-2014	編集	表 D-2 内の AC-14 の優先順位コードを P1 から P3 に変更。	D-2
01-15-2014	編集	表 D-2 内の AC-22 の優先順位コードを P2 から P3 に変更。	D-2
01-15-2014	編集	表 D-2 内の AU-10 の優先順位コードを P1 から P2 に変更。	D-3
01-15-2014	編集	表 D-2 内の CA-6 の優先順位コードを P3 から P2 に変更。	D-3
01-15-2014	編集	表 D-2 内の CA-7 の優先順位コードを P3 から P2 に変更。	D-3
01-15-2014	編集	表 D-2 内の CA-8 の優先順位コードを P1 から P2 に変更。	D-3
01-15-2014	編集	表 D-2 内の IA-6 の優先順位コードを P1 から P2 に変更。	D-4
01-15-2014	編集	表 D-2 内の IR-7 の優先順位コードを P3 から P2 に変更。	D-5
01-15-2014	編集	表 D-2 内の MA-3 の優先順位コードを P2 から P3 に変更。	D-5
01-15-2014	編集	表 D-2 内の MA-4 の優先順位コードを P1 から P2 に変更。	D-5
01-15-2014	編集	表 D-2 内の MA-5 の優先順位コードを P1 から P2 に変更。	D-5

日付	タイプ	変更内容	頁
01-15-2014	編集	表 D-2 から Program Management Controls を削除。	D-8/9
01-15-2014	編集	段落の最後の以下の文章を削除: "There is no summary table provided for the Program Management (PM) family since PM controls are not associated with any particular security control baseline."	D-9
01-15-2014	編集	表 D-3 内の AC-2 (12) と AC-2 (13)を高位影響のベースラインに追加。	D-10
01-15-2014	編集	表 D-3 内の AC-17 (5) の"incorporated into AC-17"を"incorporated into SI-4"に変更。	D-12
01-15-2014	編集	表 D-3 内の AC-17 (7) の"incorporated into AC-3"を"incorporated into AC-3 (10)"に変更。	D-12
01-15-2014	編集	表 D-5 内の AU-2 (4)の"incorporated into AC-6"を"incorporated into AC-6 (9)"に変更。	D-15
01-15-2014	編集	表 D-17 内の SA-19 (4)の"Training"を"Scanning"に変更。	D-34
01-15-2014	編集	表 D-18 から SC-9 (1)、SC-9 (2)、SC-9 (3)、および SC-9 (4)を削除。	D-37
01-15-2014	編集	表 D-18 内の SC-14 に AC-2 と AC-5 を追加し、SC-14 から SI-9 を削除。	D-37
01-15-2014	編集	表 E-2 から CA-3 (5)を削除。	E-4
01-15-2014	編集	表 E-2 に CM-3 (2)を追加。	E-4
01-15-2014	編集	表 E-2 に RA-5 (2)と RA-5 (5)を追加。	E-4
01-15-2014	編集	表 E-3.から CA-3 (5)を削除。	E-5
01-15-2014	編集	表 E-3 に CM-3 (2)を追加。	E-5
01-15-2014	編集	表 E-3 内の RA-5 (2)と RA-5 (5)から太字の書式を削除。	E-5
01-15-2014	編集	表 E-4 に CM-8 (9)を追加。	E-7
01-15-2014	編集	表 E-4 に CP-4 (4)を追加。	E-7
01-15-2014	編集	表 E-4 に IR-3 (1)を追加。	E-7
01-15-2014	編集	表 E-4 に RA-5 (3)を追加。	E-7
01-15-2014	編集	表 E-4 から SA-4 (4)を削除。	E-7
01-15-2014	編集	表 E-4 内の"SA-21 (plus "の後の"enhancements"を"enhancement"に変更。	E-7
01-15-2014	編集	表 E-4 から SI-4 (8)を削除。	E-7
01-15-2014	編集	Using the Catalog の 4 行目の"risk management process"を"RMF"に変更。	F-6
01-15-2014	編集	Using the Catalog の 5 行目の"an appropriate set of security controls"を"the appropriate security control baselines"に変更。	F-6
01-15-2014	編集	AC-2 の g.の"Monitors the use of"の後ろの","を削除。	F-7
01-15-2014	編集	AC-2 (11) を高位影響のベースラインに追加。	F-10
01-15-2014	編集	AC-3 (2) の Supplemental Guidance に以下のテキストを追加: "Dual authorization may also be known as two-person control."	F-11
01-15-2014	編集	AC-4 の References セクションの"ucdmo.gov"を"None"に変更。	F-18
01-15-2014	編集	AT-2 の References セクションの"C.F.R"の後に"."を追加。	F-38

日付	タイプ	変更内容	頁
01-15-2014	編集	AU-2 (4)の"incorporated into AC-6"を"incorporated into AC-6 (9)"に変更。	F-42
01-15-2014	編集	AU-2 の References セクションから"csrc.nist.gov/pcig/cig.html"を削除し、URL に"http://"を追加。	F-42
01-15-2014	編集	AU-6 (6)の Supplemental Guidance セクションの"identify"を"identity"に変更。	F-46
01-15-2014	編集	AU-9 (5) の Supplemental Guidance セクションに以下のテキストを追加: "Dual authorization may also be known as two-person control."	F-49
01-15-2014	編集	AU-15 に"Control Enhancements: None."を追加。	F-53
01-15-2014	編集	CM-2 (7) の Supplemental Guidance セクションから最後尾の余分な"."を削除。	F-66
01-15-2014	編集	CM-3 の g.の"board"の後に")"を追加。	F-66
01-15-2014	編集	CM-3 の related controls セクションに CA-7 を追加。	F-66
01-15-2014	編集	CM-5 (4) の Supplemental Guidance セクションに以下のテキストを追加: "Dual authorization may also be known as two-person control."	F-69
01-15-2014	編集	CM-6 の References セクションの各 URL に"http://"を追加。	F-71
01-15-2014	編集	CM-8 (5)の"inventories"の前に"component"を追加。	F-74
01-15-2014	編集	CP-8 の References セクションの"tsp.ncs.gov"を"http://www.dhs.gov/telecommunications-service-priority-tsp"に変更。	F-86
01-15-2014	編集	CP-9 (7)の Supplemental Guidance セクションに以下のテキストを追加: "Dual authorization may also be known as two-person control."	F-87
01-15-2014	編集	IA-2 の References セクションの"HSPD 12"を"HSPD-12"に変更し、URL に"http://"を追加。	F-93
01-15-2014	編集	IA-5 (1)の(c)の"encrypted representations of""を"cryptographically-protected"に変更。	F-96
01-15-2014	編集	IA-5 (1)の Supplemental Guidance セクションの"Encrypted representations of""を"Cryptographically-protected"に変更。	F-97
01-15-2014	編集	IA-5 (1)の Supplemental Guidance セクションに以下のテキストを追加: "To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords."	F-97
01-15-2014	編集	IA-5 の References セクションの URL に"http://"を追加。	F-99
01-15-2014	編集	IA-7 の References セクションの URL に"http://"を追加。	F-99
01-15-2014	編集	IA-8 の References セクションの URL に"http://"を追加。	F-101
01-15-2014	編集	IR-6 の References セクションの"800-61"の後の":"を";"に変更し、URL に"http://"を追加。	F-108
01-15-2014	編集	MP-6 (7)の Supplemental Guidance セクションに以下のテキストを追加: "Dual authorization may also be known as two-person control."	F-124
01-15-2014	編集	MP-6 の References セクションの URL に"http://"を追加。	F-124
01-15-2014	編集	PE-3 の References セクションの"DoDI"を"DoD Instruction" に変更し、URL に "http://"を追加。	F-130
01-15-2014	編集	PL-2 の a. 内の 8.の"tailoring"の後の"and supplementation"を削除。	F-140

日付	タイプ	変更内容	頁
01-15-2014	編集	PL-4 の References セクションの"Publication"の前に"Special"を追加。	F-141
01-15-2014	編集	PL-7 に"Control Enhancements: None."を追加。	F-142
01-15-2014	編集	PL-9 の Supplemental Guidance セクションから AT-5 、AC-19 (6) (8) (9)を削除。	F-144
01-15-2014	編集	PL-9 に"Control Enhancements: None."を追加。	F-144
01-15-2014	編集	PL-9 の References セクションの"Publication"の前に"Special"を追加。	F-144
01-15-2014	編集	PS-2 の References セクションの"731.106(a)"を"731.106"に変更。	F-145
01-15-2014	編集	RA-3 の References セクションの"Publication"を"Publications"に変更し、URL に"http://"を追加。	F-153
01-15-2014	編集	RA-5 の References セクションの URL に"http://"を追加。	F-155
01-15-2014	編集	SA-4 の References セクションの URL に"http://"を追加。	F-160
01-15-2014	編集	SA-11 (8)の Supplemental Guidance セクションに以下のテキストを追加: "To understand the scope of dynamic code analysis and hence the assurance provided, organizations may also consider conducting code coverage analysis (checking the degree to which the code has been tested using metrics such as percent of subroutines tested or percent of program statements called during execution of the test suite) and/or concordance analysis (checking for words that are out of place in software code such as non-English language words or derogatory terms)."	F-169
01-15-2014	編集	SA-11 の References セクションの URL に"http://"を追加。	F-169
01-15-2014	編集	SA-16 に"Control Enhancements: None."を追加。	F-177
01-15-2014	編集	SA-19 (4)のタイトル内の"Training"を"Scanning"に変更。	F-181
01-15-2014	編集	SC-8 の Supplemental Guidance セクションの"physical"を"protected"に変更。	F-193
01-15-2014	編集	SC-13 の References セクションの"140-2"を"140"に変更し、. URL に"http://"を追加。	F-196
01-15-2014	編集	SC-20 の a. の"data origin"の後に"authentication"を追加。	F-199
01-15-2014	編集	SC-20 の a. の"integrity"の後に"verification"を追加。	F-199
01-15-2014	編集	SC-35 に"Control Enhancements: None."を追加。	F-209
01-15-2014	編集	SI-7 から余分な"References: None"を削除。	F-228
01-15-2014	編集	Appendix G に、以下のテキストを新しい第 3 段落として追加: "Table G-1 provides a summary of the security controls in the program management family from Appendix G. Organizations can use the recommended priority code designation associated with each program management control to assist in making sequencing decisions for implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; and a Priority Code 2 [P2] control has a higher priority for implementation than a Priority Code 3 [P3] control."	G-1/2
01-15-2014	編集	Appendix G に表 G-1 を追加。	G-2
01-15-2014	編集	PM-5 の References セクションの URL に"http://"を追加。	G-5
01-15-2014	編集	PM-7 の References セクションから"Web: www.fsam.gov"を削除。	G-5
01-15-2014	編集	脚注 124 の URL に"http://"を追加。	J-22

第 1 章

はじめに

情報・情報システムを保護する必要性

情報システム[1]のセキュリティ管理策を選択・実装するタスクは、組織のセキュリティ管理策を選択・実装するタスクとともに、（組織の）業務[2]・（組織[3]の）資産に大きな影響を与える可能性がある重要なタスクであるだけではなく、（個人・国家の）安寧に非常に大きな影響を与える可能性のある重要なタスクである。

なお、セキュリティ管理策は、

① 情報システム（および／または組織）によって処理・保存・伝送される情報について、機密性・完全性・可用性を保護する事

② 定められたセキュリティ要求事項をすべて満たす事[4]

の2つを実現するために情報システムまたは組織に対して定められた保護対策である。

ただし、組織による情報システムの情報セキュリティについての取り組みが成功するかどうかは、以下の疑問点が解消されているかどうか次第である：

- セキュリティ要求事項を満たしながら業務を遂行する事で組織が情報・情報システムの利用から生じるリスクを最小化する事が可能なセキュリティ管理策として、どのようなセキュリティ管理策が必要なのか？
- セキュリティ要求事項を満たしながら業務を遂行する事で組織が情報・情報システムの利用から生じるリスクを最小化する事が可能なセキュリティ管理策が実装されているか？（または、当該セキュリティ管理策の実装が計画されているか？）
- セキュリティ要求事項を満たしながら業務を遂行する事で組織が情報・情報システムの利用から生じるリスクを最小化する事が可能なセキュリティ管理策が実装された場合、どの程度まで当該管理策の効果的な適用を保証する事が望ましいのか？（あるいは、当該セキュリティ管理策が実装された場合、どの程度まで当該管理策の効果的な適用を保証する事が必要なのか？）[5]

---

[1] 情報システムとは、完全に独立した情報リソースのセットとして、情報を収集・処理・メンテナンス・利用・共有・配布・配置するにあたり特別に編成されたものである。なお、情報システムには、産業用制御システム・プロセス制御システム・電話交換システム・構内電話交換機（PBX）システム・環境管理システム等の特殊なシステムも含まれる。

[2] ここで言う「組織の業務」には、組織のミッションが含まれるとともに、組織のイメージに加えて組織の評判として言い換える事ができる。

[3] ここで言う「組織」とは、組織の規模または組織構造の複雑性（もしくは組織内における位置付け）を問わず、連邦政府機関（または連邦政府機関の業務担当部署）といった主体を指す。

[4] セキュリティ要求事項とは、組織における情報システムによって処理または保存（もしくは伝送）される情報について機密性・完全性・可用性を確保するために、ミッションのニーズおよび／または業務上のニーズに加えて、法律・大統領命令・指令・規制・政策・指示・標準・ガイドライン・手順のいずれか（またはそれらすべて）に基づいて要求される事項である。

[5] 「管理策の効果的な適用」とは、セキュリティ管理策の正確な実装（または意図した通りにセキュリティ管理策が運用される事）を意味するとともに、組織が情報・情報システムの利用から生じるリスクを最小化できるよう情報システムが固有の操作環境下でセキュリティ要求事項を満たしながら業務を遂行する事（または既定のセキュリティポリシーを場合によっては強制適用する事）を指す。

なお、これらの疑問に対する回答は個別になされるのではなく、情報が抱えるリスク[6]（および情報システムが抱えるリスク）を具体的に明らかにした組織が必要に応じてリスクを最小化する事を可能にする効果的なリスク管理プロセスの観点から包括的になされるとともに、情報が抱えるリスク（および情報システムが抱えるリスク）を具体的に明らかにした組織がリスクを継続的に監視する事を可能にする効果的なリスク管理プロセスの観点から包括的になされる。

NIST Special Publication 800-39 は、3 つのまったく異なる物理階層（すなわち、組織レベル・業務プロセスレベル・情報システムレベルの各階層）において情報セキュリティリスクを管理するためのガイダンスについて記載している一方、この NIST Special Publication 800-53 の文書にて定義されているセキュリティ管理策のうち組織の情報セキュリティ要求事項を満たすために各組織が策定するよう推奨されている管理策は、組織の情報セキュリティプログラムをサポートするプロセスとして明確に定義されたリスク管理プロセスの一部として導入されるべきものである[7]。

なお、担当職員は、（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれに悪影響をもたらす可能性のあるリスク等の因子について把握しなければならない[8]。また、情報（または情報システム）へのリスクを許容可能な水準にまで軽減する投資判断を行うことができるよう、担当職員は、情報（または情報システム）の保護を目的に導入された（または導入が計画されている）組織のセキュリティプログラムの現在のステータスについて把握しなければならないとともに、同様に情報（または情報システム）の保護を目的に導入された（または導入が計画されている）管理策の現状についても把握しなければならない。

最終的には、情報への不正アクセスのリスクに加えて（情報の）不正利用・（情報の）不正開示・（情報の）改ざん・（情報の）破壊といったリスクに対応するセキュリティとして連邦行政管理予算局（OMB）通達 A-130 号が規定するところの「必要十分なセキュリティ」に準拠して組織の日常業務を遂行できるようになる事で、組織が定められたミッションを達成するとともに定められた業務を遂行できるようにならなければならない。

1.1 この文書の目的および適用範囲

この文書の目的は、『Minimum Security Requirements for Federal Information and Information Systems（連邦政府の情報および連邦政府の情報システムのそれぞれに対する最低限のセキュリティ要求事項）』と題する FIPS Publication 200 に記載されたセキュリティ要求事項を満たす事ができるよう、連邦政府の行政機関（および当該機関をサポートする情報システム）に対するセキュリティ管理策を選択・特定するにあたっての指針を示す事である。また、こ

[6] 情報セキュリティ関連のリスクとは、情報または情報システムが機密性・完全性・可用性のいずれかを喪失する事によって組織の業務および組織の資産（ひいては個人・他組織・国家）に負の影響をもたらす可能性のあるリスクを指す。

[7] この文書の付録 G に記載されたプログラム管理策は、情報システムに対するセキュリティ管理策（同じくこの文書の付録 F）を補足する管理策として、組織レベルの情報セキュリティ要求事項のうち特定の情報システムに依存しない要求事項として情報セキュリティプログラムを管理する上で必要不可欠な事項に対する管理策である。

[8] （組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれに悪影響をもたらす可能性のあるリスクには、重要インフラに対するリスク（および／または重要リソースに対するリスク）として国土安全保障に関する大統領令第 7 号に記載されているリスクが含まれる。

れらの指針は、連邦政府の情報について処理・保存・伝送のいずれかを行う情報システムのすべてのコンポーネント[9]に適用される。

なお、連邦政府の内部において、

- 情報システムに対するセキュリティ管理策を組織に対するセキュリティ管理策とともに選択・指定するための手法として、より一貫性がありながら、より容易に比較可能かつより簡単に繰り返し利用する事が可能な手法を推進
- セキュリティ上の脅威に加えてセキュリティ要求事項・セキュリティ技術のそれぞれの変化に基づいて将来発生する事が見込まれる情報保護のニーズを現時点における情報保護のニーズとともに満たすためのセキュリティ管理策のカタログとして、安定的でありながら柔軟さを兼ね備えた管理策を列挙
- 『Standards for Security Categorization of Federal Information and Information Systems（連邦政府の情報および連邦政府の情報システムのそれぞれのセキュリティのカテゴリ化に関する規格）』と題する FIPS Publication 199 にしたがって分類された情報システムに対して推奨されるセキュリティ管理策を策定
- セキュリティ管理策の有効性について判断するための評価手法を策定する基盤の提供とともに、セキュリティ管理策の有効性について判断するための評価手順を策定する基盤の提供
- リスク管理のとは何かについての議論に資する共通用語集を提供する事によって、組織間でより円滑に意思疎通が行なわれるようにする

の５つの手段によって情報システムをよりセキュアなものにしながらより効果的にリスクを管理するための指針が策定されている。

なお、上記の５つの手段のなかで登場したセキュリティ管理策に加えて、このSpecial Publication 800-53は、

① 情報セキュリティプログラムマネジメントに関連して通常は組織レベルで実装されるにも関わらず組織内の個々の情報システムを直接の管理対象としないセキュリティ管理策一式

② 連邦法・（連邦政府の）指令・（連邦政府の）政策・（連邦政府による）規制・（連邦政府が制定した）標準のそれぞれに基づいたプライバシー要求事項を組織が容易に充足できるようにするための国際標準に準拠するとともに、同様に組織が容易に充足できるようにするためのベストプラクティスに準拠したプライバシー管理策一式

の２つを提供する文書である。

また、この Special Publication 800-53 の文書は、プライバシー要求事項およびセキュリティ要求事項のそれぞれの要求事項を強制的に適用する事で、プライバシー管理策およびセキュリティ管理策のそれぞれの内容が重複するだけではなく、連邦政府組織の内部または連邦政府の情報システムの内部もしくは連邦政府のプログラムの内部でプライバシー管理策とセキュリ

[9] 情報システムのコンポーネントには、大型汎用コンピュータ・ワークステーション・（データベースサーバ・メールサーバ・認証サーバ・ウェブサーバ・プロキシサーバ・ファイルサーバ・ドメインネームサーバ等の）サーバ・（スキャナ・コピー機・プリンター等の）入力（出力）装置・（ファイアウォール・ルータ・ゲートウェイ・音声スイッチ・データスイッチ・プロセスコントローラ・ワイヤレスアクセスポイント・ネットワークアプライアンス・センサ等の）ネットワークコンポーネント・オペレーティングシステム・仮想マシン・ミドルウェア・アプリケーション等が含まれる。

ティ管理策とが重複して実装されるよう、プライバシー管理策とセキュリティ管理策との関係性を確立する文書である。

なお、連邦法・(連邦政府の)指令・(連邦政府の)政策・(連邦政府による)規制・(連邦政府が制定した)標準のそれぞれに基づいたプライバシー要求事項を組織が容易に充足できるようにするための国際標準に準拠したプライバシー管理策は、組織が連邦政府によるプライバシー要求事項をより統制のとれた構造化された形で満たすための手段である。また、プライバシー管理策およびセキュリティ管理策のそれぞれの内容が重複する事で、組織は、費用対効果の高いリスクベースのプライバシー管理策を実装できるようになる。

FIPS Publication 200に記載されたセキュリティ要求事項を満たす事ができるよう連邦政府の行政機関(および当該機関をサポートする情報システム)に対するセキュリティ管理策を選択・特定するにあたっての指針としてこのSpecial Publication 800-53の文書にて示された指針は、合衆国法律集第44編3542条において国家安全システム[10]として規定されているもの以外で連邦政府が保有するすべての情報システム[11]に適用できるものであるとともに、国家のセキュリティ関係のシステムに対する類似の指針を技術的な観点から幅広く補足する目的で作成されたものである。

なお、当該指針は、国家のセキュリティ関係のシステムに対するポリシーを策定する権限を行使する連邦政府当局者が承認する事を前提に、国家安全システムに対して適用してもよい[12]。また、州政府・市町村・居留区政府のみならず民間組織においても必要に応じて当該指針の利用を検討する事が推奨される。

1.2 対象と想定する読者

この Special Publication 800-53 の文書は、

- 運用認可責任者・最高情報責任者・最高情報セキュリティ責任者[13]・情報システム管理者・情報セキュリティ管理者等、情報システム・情報セキュリティ・リスク管理のいずれか(または情報システム・情報セキュリティ・リスク管理のすべて)およびリスクモニタリングについて責任を負う者

[10] 連邦政府の情報システムとは、行政機関または行政機関と役務・物品を提供する契約を結んだ者もしくは行政機関の代理人の他の組織のいずれかによって利用または運用される情報システムである。

[11] 国家安全システムとは、政府機関または政府機関と役務・物品を提供する契約を結んだ者もしくは政府機関の代理人の他の組織によって何らかの形で利用または運用される情報システム(政府機関または政府機関と役務・物品を提供する契約を結んだ者もしくは政府機関の代理人の他の組織によって何らかの形で利用または運用される通信システムを含む)である。また、国家安全システムは、①諜報活動のなかで機能する(または諜報活動のなかで運用もしくは利用される)システム②安全保障に関する暗号に関係するシステム③軍隊の指揮命令に関わるシステム④武器(システム)と一体化した機器に関係するシステム⑤軍事作戦または諜報作戦の成功に直結する必要不可欠なシステム(給与管理・財務管理・物流管理・人事管理といった定型的な管理業務に関するアプリケーション用のシステムを除く)のいずれかでありながら、大統領令または議会制定法が定める要件のもとで国防上または外交政策上の利益の観点から機密として扱われる事が特別に許可された情報の取り扱いに関する手順によって常に保護されるシステムである。

[12] 米国国家安全システム委員会(CNSS)通達第 1253 号は、国家安全システムの実装指針を定めた通達である。

[13] 政府機関レベルでは、この役職は「政府機関上級情報セキュリティ責任者」として呼ばれている。ただし、組織によっては、この役職を「上級情報セキュリティ責任者」または「最高情報セキュリティ責任者」と呼ぶ事もある。

- プログラムマネージャー・システム設計者・システム開発者・情報セキュリティエンジニア・システムインテグレータ等、情報システムの開発について責任を負う者
- 業務オーナー・企業オーナー・情報システムオーナー・共通管理策提供者・情報オーナー・情報管理者・システムアドミニストレータ・情報システムセキュリティ責任者等、情報セキュリティの実装（および情報セキュリティの運用）について責任を負う者
- 監査人・首席監察官・システム評価者・独立検査人・アナリスト・情報システムオーナー等、情報セキュリティ評価・情報セキュリティモニタリングについて責任を負う者
- IT 製品・IT システムを生産している営利企業または情報セキュリティ関連の技術を創出している営利企業（もしくは情報セキュリティサービスを提供している営利企業）

といった情報システム・情報セキュリティ関係の専門的なユーザにとって役に立つ事を目指す文書である。

1.3 セキュリティ管理策に関する他の発行文書との関係

この NIST Special Publication 800-53 の文書の目的は、情報セキュリティに関する既存の標準との整合性を保ちながらそれらを補足するセキュリティ管理策一式として、組織・ミッション・業務・情報システムに対して幅広く要求されるセキュリティ要求事項[14]の充足が可能なセキュリティ管理策一式を提供する事である。

組織は、運用上・環境上・技術上さまざまな形で起こりうる従来型の APT 攻撃から情報および情報システムを保護するうえで、この Special Publication 800-53 の文書に記載されているセキュリティ管理策カタログを効果的に活用する事ができる。また、この Special Publication 800-53 の文書に記載されているセキュリティ管理策カタログは、運用上・環境上・技術上さまざまな形で起こりうる従来型の APT 攻撃から情報および情報システムを保護するうえでも効果的に活用する事ができるとともに、政府・組織のいずれかによるセキュリティ要求事項または制度上のセキュリティ要求事項に準拠している事を示すうえで効果的に活用する事もできる。ただし、組織は、適切なセキュリティ管理策を選択する責任とともに適切なセキュリティ管理策を正しく実装する責任を負うのに加えて、適切とされたセキュリティ管理策が確立されたセキュリティ要求事項を満たす管理策であるかどうか証明する責任を負う[15]。

セキュリティ要求事項が正確に満たされるという確信を組織が常に得られるよう、セキュリティ管理策には、その効果の評価を可能にする評価手法・評価手順が策定される。また、組織は、特殊なオーバーレイシステムもしくはオーバーレイ技術または重ね合わせ操作の環境もしくは重層的な協力関係のいずれかを構築するためにセキュリティ管理策を利用する事ができる(※この文書の付録 I を参照)。

なお、この文書を作成するにあたっては、技術的観点から合理的なセキュリティ管理策一式として広く組織および情報システムに対して適用可能なセキュリティ管理策一式が策定できるよう、国防・監査・財務・健康保険・インテリジェンスコミュニティ・産業制御・プロセス制御関連で

[14] セキュリティ要求事項とは、処理または保存（もしくは伝送）された情報について機密性・完全性・可用性を確保できるよう法律・大統領令・指令・政策・手引・規制・標準・指針・（組織の）ミッションニーズのいずれかの観点から情報システムに対して求められる要求事項である。

[15] NIST Special Publication 800-53A の文書は、セキュリティ管理策の有効性の評価に関する手引きである。

採用されているセキュリティ管理策の内容に加えて、国内外の標準化団体によって定められたセキュリティ管理策といった様々な資料の内容を確認している。

1.4 組織の責任

組織は、組織の情報（および組織の情報システム）のセキュリティを区分するにあたって、連邦情報処理規格（FIPS） Publication 199 を利用する。また、セキュリティを区分する行為は、運用認可責任者・最高情報責任者・上級情報セキュリティ責任者・情報の所有者（および／または情報の管理者）・情報システムの所有者・リスク担当役員（またはリスク担当役員の機能を担う者）といった組織の上級職員の関与のもと、組織全体にわたる活動[16]として行われる。[17]

なお、情報は、物理層（組織階層）の情報およびデータリンク層（ミッション階層および／または業務プロセス階層）の情報に区分される事から、ネットワーク層（情報システム階層）に存在する（組織の）情報システムを①低位影響レベルのシステム②中位影響レベルのシステム③高位影響レベルのシステムのいずれかに指定するうえで、組織は FIPS Publication 200 に基づいて物理層（組織レベル）における情報のセキュリティとデータリンク層（ミッションレベルおよび／または業務プロセスレベル）における情報のセキュリティを区分する。また、セキュリティ管理策として策定されるべき管理策としてこの文書の付録 D において定義されているベースライン管理策は、通常、ネットワーク層に存在する（組織の）情報システムに対して策定されたセキュリティ管理策を調整する基準でありながら、物理層・データリンク層のいずれかに存在する（組織の）情報システムに対して策定されたセキュリティ管理策を幅広く調整する事が可能な基準である。

FIPS Publication 199 においては、情報セキュリティまたはネットワーク層（運用・利用される情報システムの階層）のセキュリティが（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれに対してもたらされる可能性のある最も深刻な影響に即して区分されている[18]。また、脆弱性が悪用される脅威に関連して具体的かつ信頼できる情報等をもとに組織が行うリスク評価の結果（すなわち、脆弱性が悪用される脅威が実際に発生する可能性）は、どのように管理策を調整するべきかについての目安を提供するとともに、最終的にどのセキュリティ管理策を選択するべきかについての目安を提供する[19]。

なお、情報システムのセキュリティ計画書には、組織の具体的なミッションニーズならびに組織の具体的な業務ニーズ（および組織にとって許容可能なリスクの具体的範囲）に見合った管理策として最終的に策定されたセキュリティ管理策一式が相応の策定理由とともに記載される[20]。また、（最低限のセキュリティ管理策としてのベースライン管理策を含めて）Special

[16] FIPS Publication 200 の脚注 7 を参照。

[17] 通常、組織は、組織の情報システムおよび組織の情報システムのセキュリティについて資金面を含めて管理するとともに、組織の情報システムおよび組織の情報システムのセキュリティの運用管理を行う。具体的には、（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれを保護する上で必要と考えられるセキュリティ管理策を義務付ける権限（または義務付ける機能）とともに、（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれを保護する上で必要と考えられるセキュリティ管理策を実装する権限（または実装する機能）等によって行われる。

[18] 米国愛国者法および国土安全保障に関する大統領令（HSPDs）により、組織の情報システムは国家（または他の組織）が被る可能性のある影響を考慮して区分される。

[19] リスク評価は組織の具体的なニーズに応じて様々な方法で行う事ができる。なお、NIST Special Publication 800-30 は、包括的なリスク管理のプロセスの一環としてリスクを評価するにあたっての手順を示した文書である。

[20] セキュリティ計画を承認する事によって、運用認可責任者または運用認可責任者が指定した代表者は、組織に対するセキュリティ要求事項（組織のミッションに対するセキュリティ要求事項および組織の業務プロセスに対するセキ

Publication 800-53 に記載されたセキュリティ管理策を利用する事で、連邦政府の各機関および連邦政府の情報システムがより巧妙化かつ悪質化する脅威かつ急速に変化する技術（または場合によっては固有のシステム運用環境）に対応するうえで連邦政府の各機関に必要な柔軟性を同様に必要な俊敏性とともに維持しながらより適切なセキュリティ水準を確保できるようになる。同じく、（最低限のセキュリティ管理策としてのベースライン管理策を含めて）Special Publication 800-53 に記載されたセキュリティ管理策を利用する事で、連邦政府の各機関および連邦政府の情報システムが組織における特定のミッションおよび／または組織における特定の業務機能に対応するうえで連邦政府の各機関に必要な柔軟性を同様に必要な俊敏性とともに維持しながらより適切なセキュリティ水準を確保できるようになる。

なお、組織・ミッションプロセス・業務プロセス・情報システムのそれぞれについてセキュリティを十分に確保する事は:

- 明確なセキュリティ要求事項および明確なセキュリティ仕様
- 実際のハードウェア（またはファームウェアもしくはソフトウェア）開発プロセスに基づき設計・製造された良質な IT 製品
- システムエンジニアリングおよびセキュリティエンジニアリングに関連して組織の情報システムに IT 製品を効果的に組み込むための合理的な原理原則および同様の目的で行われる活動
- 組織の職員が研修を受けなければならない事項のうち、組織内のセキュリティについて責任を負う職員の日常業務の一環として行われる合理的な情報セキュリティ活動として詳細に規定された活動
- ①実装されたセキュリティ管理策の現時点における有効性②情報システムおよびシステム運用環境のそれぞれの変化③法律・指令・政策・標準に準拠しているかどうかの 3 つを判断するために組織および情報システムに対して行われる継続的なモニタリング[21]
- 情報セキュリティ計画の立案とともに、システム開発ライフサイクルの管理[22]

のすべてが要求される多面的な取り組みである。

技術的観点からは、情報セキュリティとは、組織のミッションおよび／または組織の業務プロセスをサポートする情報システムの運用にあたり要求される多くの機能のうちの 1 つであるに過ぎない一方で、ミッション・業務において成功を収めるうえで組織がシステム開発ライフサイクルの全般にわたり投資を行わなければならない機能である。

なお、情報セキュリティについては、組織が（組織の）業務・（組織の）資産・個人・他組織・国家に対するリスクのうちミッションに由来するリスクおよび／または業務プロセスに由来するリスクについて情報システムの運用を開始または継続する事によって**現実に即して**評価する事が重要となる。ただし、リスクを現実に即して評価するにあたっては、組織に内在する脆弱性が

ュリティ要求事項を含む）および／または指定された情報システムに対するセキュリティ要求事項を満たす事ができるよう策定されたセキュリティ管理策一式に同意した事になる。

[21] NIST Special Publication 800-137 は、組織の情報システムを継続的にモニタリングするにあたっての目安を提供するとともに、（組織の情報システムの）運用環境を継続的にモニタリングするにあたっての目安を提供している。

[22] NIST Special Publication 800-64 は、システム開発ライフサイクルにおいて考慮する情報セキュリティについての目安を提供している。

実際に悪用されるという組織に対する脅威についての理解に加えて、それによって生じる可能性のある負の影響についても理解しなければならない[23]。

組織の情報システムを取得・実装・運用する事によって支出される可能性のある費用②組織の情報システムを取得・実装・運用するスケジュール③組織の情報システムを取得・実装・運用するにあたってのパフォーマンスの3つに鑑みて、組織のリスク管理戦略の一環としてセキュリティ要求事項を満たすにあたっては、組織のリスク管理戦略について十分な知識を持たなければならない[24]。

1.5 この文書の構成

第 2 章以降の構成は、次の通りである:

- **第 2 章**では、①重層的なリスク管理②セキュリティ管理策の構造およびセキュリティ管理策ファミリがどのような管理策から構成されているか③管理目標としてのセキュリティ管理策のベースライン管理策④共通管理策の利用およびセキュリティ機能の継承⑤外部環境とサービスプロバイダ⑥保証と信頼性⑦セキュリティ管理策のベースライン管理策の改訂（および拡張）等、セキュリティ管理策の選択（および指定）に関連する基本的な概念について記述する。
- **第 3 章**では、①セキュリティ管理策のベースライン管理策として適切な管理策の選択②特殊なオーバーレイの作成を含むベースライン管理策の調整③セキュリティ管理策を選択するプロセスの文書化④セキュリティ管理策のベースライン管理策を選択するプロセスの適用（新システムおよびレガシーシステムの双方に対して）等、組織の情報システムのセキュリティ管理策を選択・指定するプロセスについて記述する。
- **本論を補足する付録**では、①一般的な参考文献[25]②定義と用語③略語④低位影響レベルの情報システムおよび中位影響レベルの情報システムならびに高位影響レベルの情報システムのそれぞれのセキュリティ管理策のベースライン管理策⑤情報システムの保証（および情報システムの信頼性）に関する手引き⑥セキュリティ管理策カタログ[26]⑦情報セキュリティプログラム管理に関する管理策のカタログ⑧情報セキュリティに関する国際標準との対応関係⑨組織または利害関係者がオーバーレイを作成するに当たっての手引き⑩プライバシー管理策のカタログ等、セキュリティ管理策を選択・指定するうえで必要不可欠な情報を提供する。

[23] NIST Special Publication 800-30 は、リスク評価のプロセスに関する手引きである。

[24] 組織は、情報セキュリティ要求事項に加えて、連邦法（および連邦政府の政策）に基づくプライバシー要求事項を満たさなければならない。また、セキュリティを包括的に確保するとともにプライバシーを包括的に保護できるよう、組織はこの文書の付録 J に記載されたプライバシー管理策を同じくこの文書の付録 F に記載されたセキュリティ管理策と合わせて採用する事ができる。

[25] 特に明記しない限り、この文書が参照する NIST 発行文書(すなわち、FIPS および Special Publication)はすべて最新版の文書である。

[26] この文書に記載されているセキュリティ管理策は、NIST のウェブサイト(http://web.nvd.nist.gov/view/800-53/home)にて内容を確認する事ができる。また、当該サイトから様々なファイル形式でダウンロードする事も可能。

第 2 章

基本事項

セキュリティ管理策の構造・構成および（セキュリティ管理策の）ベースライン管理策・（セキュリティ管理策による）セキュリティ保証

セキュリティ管理策の選択およびセキュリティ管理策の指定に関連して、本章では、①上位・中位・下位ごとの重層的なリスク管理②セキュリティ管理策の構造およびセキュリティ管理策カタログの構成③セキュリティ管理策のベースライン管理策④共通セキュリティ管理策の利用・識別について⑤外部環境におけるセキュリティ管理策⑥セキュリティ管理策によるセキュリティの保証⑦セキュリティ管理策・セキュリティ管理策カタログ・（セキュリティ管理策の）ベースライン管理策のそれぞれについて将来行われる見直しの 7 つの基本的な内容を記述している。

2.1 重層的なリスク管理

情報システムのセキュリティ管理策は、情報システムを運用する事による（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれへのリスクを組織全般にわたって管理する事を目指して情報セキュリティプログラムを実行するなかで選択・指定する。情報システムのセキュリティ管理策をリスクベースで選択・指定するに当たっては、連邦法・大統領命令・指令・政策・規制・標準・指針に照らして効果的なものであるかどうかと合わせて連邦法・大統領命令・指令・政策・規制・標準・指針に照らして効率的なものであるかどうかについて考慮するとともに、連邦法・大統領命令・指令・政策・規制・標準・指針に起因する制約事項についても考慮する。

なお、ミッション・業務を遂行する上で重要な事項により効果的に対応するために組織全体のリスクを一体的なプロセスによって管理できるよう、①**組織**レベル②**ミッション・業務プロセス**レベル③**情報システム**レベルでリスクに対応する 3 段階のアプローチを採用する。リスク管理のプロセスは、組織のリスク対応を継続的に改善する事で組織によるミッション（および／または業務）の成功という利益を共有するすべての関係者が①**組織**レベル②**ミッション・業務プロセス**レベル③**情報システム**レベルのいずれか（もしくはそのすべて）で効果的なコミュニケーションを図る事ができるようにするという全体的な目的のもと、①**組織**レベル②**ミッション・業務プロセス**レベル③**情報システム**レベルの 3 段階で実施される。

下の図1は、①**組織**レベル②**ミッション**レベルおよび**業務プロセス**レベル③**情報システム**レベルでリスクに対応する 3 段階のアプローチを図式化したものである。

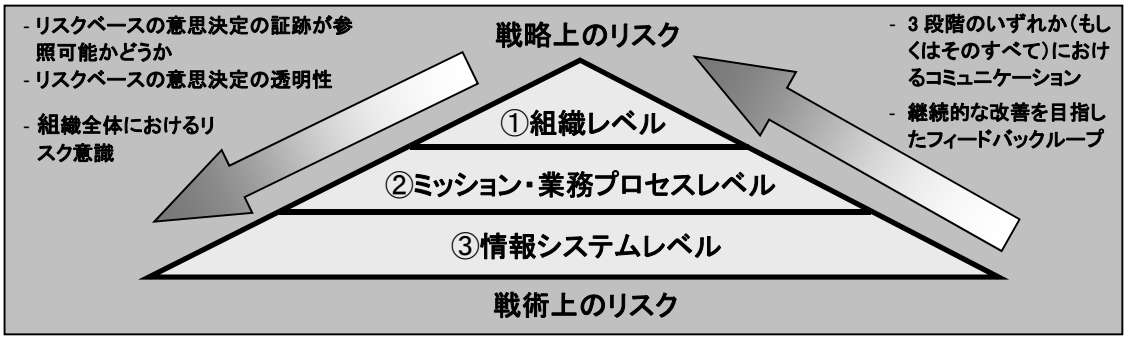
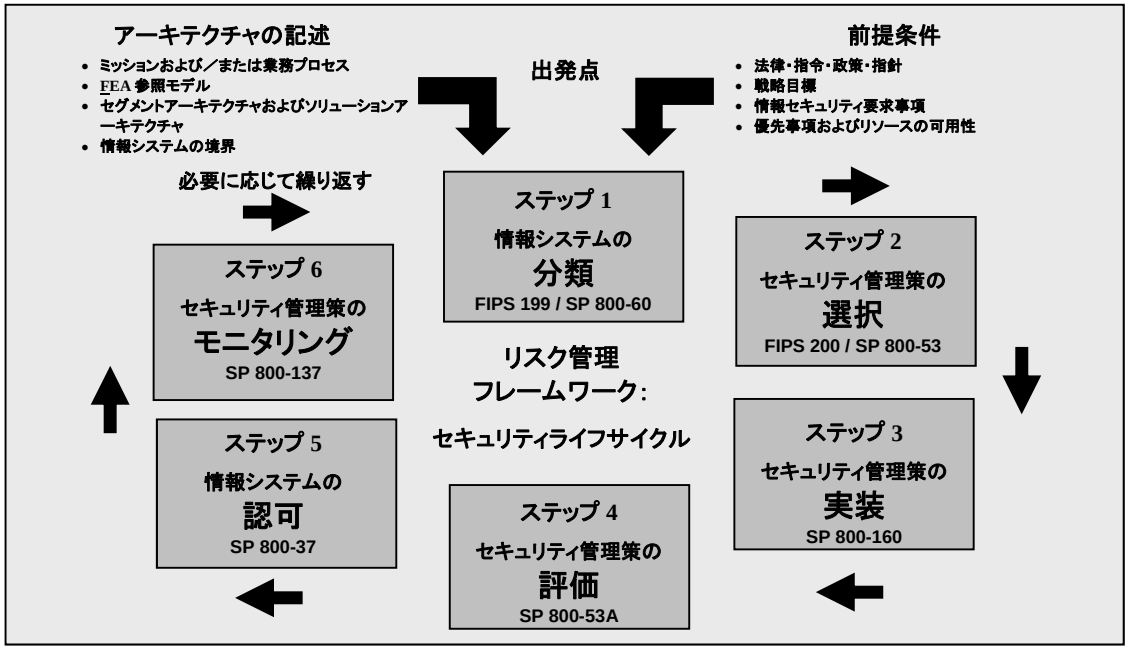


図 1：3 段階でリスクを管理するアプローチ

投資戦略・投資判断の基となる優先順位が組織レベルでリスクを管理する事によってミッション・業務機能の両面で明確になるため、組織の戦略目標に加えて目安となる性能に適合した費用対効果が高く効率的な IT ソリューションが実現する。また、ミッション・業務プロセスレベルにおいて行われるリスク管理とは、具体的に①組織におけるミッション（および／または組織における業務機能）の支援に必要なミッションを定義する事および／または組織におけるミッション（および／または組織における業務機能）の支援に必要な業務プロセスを定義する事②組織におけるミッション（および／または組織における業務機能）の支援に必要なミッションおよび／または組織におけるミッション（および／または組織における業務機能）の支援に必要な業務プロセスを実行するのに当たって必要な情報システムのセキュリティカテゴリを決定する事③組織におけるミッション（および／または組織における業務機能）の支援に必要なミッションおよび／または組織におけるミッション（および／または組織における業務機能）の支援に必要な業務プロセスに対して情報セキュリティ要求事項を反映させる事④組織の情報システムおよびシステム運用環境に対してセキュリティ管理策を円滑に割り当てる事ができるよう、組み込み型情報セキュリティアーキテクチャ等のエンタープライズアーキテクチャを確立する事の 4 つを指す。

なお、情報システムレベルでリスクを管理する一般的な手法として、図 2 において図式化されているリスク管理フレームワーク（RMF）がある[27]。この Special Publication 800-53 の文書においては、組織が直面するリスクを①組織レベル②ミッション・業務プロセスレベル③情報システムレベルの 3 段階で管理するという観点から、RMF のステップ 2 を構成する「セキュリティ管理策の選択」のプロセスについてもっぱら記載している。



注記：CNSS Instruction 1253 は、国家安全保障システム（NSS）における RMF のステップ 1 および 2 に関する手引きである。

図 2：リスク管理フレームワーク

[27] NIST Special Publication 800-37 は、リスク管理フレームワーク（RMF）の実装に関する手引きである。RMF をサポートしている文書として図 2 に記載されたすべての文書の一覧は、この文書の付録 A に記載されている。

RMF は、組織が情報システムを設計・開発・実装・運用・廃棄するに当たってセキュリティ上重要となる事項に加えて、組織がシステムを運用する環境に関連してセキュリティ上重要となる事項についてのフレームワークであり、

ステップ 1：FIPS Publication 199 に記載された影響評価に基づいて、情報システムを分類する[28]

ステップ 2：前記のステップ 1 においてセキュリティを分類した結果に基づいてセキュリティ管理策のベースライン管理策として適切な管理策を選択のうえ、オーバーレイを利用するなど管理策の調整に関するガイダンスを適用する

ステップ 3：セキュリティ管理策を実装のうえ、当該管理策を設計・開発・実装する際の詳細を文書化する

ステップ 4：セキュリティ管理策を評価する事によって、当該管理策がどの程度正しく実装されているかとともにどの程度意図した通りに運用されているかに加えて、どの程度当該管理策は情報システムのセキュリティ要求事項を満たしているかについて判断する[29]

ステップ 5：（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれに対するリスクのうち情報システムを運用・利用する事によって生じるリスクとして顕在化したものを許容する事が可能であるという判断に基づいて、情報システムの運用を認可する

ステップ 6：情報システムのセキュリティ管理策に加えてシステム稼動環境におけるセキュリティ管理策を継続的にモニタリングする事によって、システムおよび／または環境が変更されているかどうかおよびセキュリティ管理策が有効であるかどうかに加えて、セキュリティ管理策が法律・大統領命令・指令・政策・規制・標準に準拠しているかどうかについて判断する

の 6 つのステップからなるフレームワークである。

2.2 セキュリティ管理策の構造

この Special Publication 800-53 の文書に記載されているセキュリティ管理策は、その構成や構造が明確に定義されているのに加えて、セキュリティ管理策を簡単に選択・指定できるよう、18 の管理策ファミリにまとめられている[30]。それぞれの管理策ファミリには、管理策ファミリ全般に関係するセキュリティトピックに関連したセキュリティ管理策があり、例えば人的セキュリティ（PS）に関連したセキュリティ管理策のファミリは PS というように、2 文字からなる頭文字によって、一意に識別される。また、18 のセキュリティ管理策ファミリにまとめられたセキュリティ管理策は、ポリシーもしくは監視または手動プロセス・（個人の）アクション・（情報システムおよび／または情報機器によって実装される）自動メカニズムのいずれかに関係するセキュリティ管理

[28] CNSS Instruction 1253 には、国家安全保障システムのセキュリティ分類についての手引きが記載されている。

[29] NIST Special Publication 800-53A は、セキュリティ管理策の有効性を評価するに当たっての手引きが記載されている。

[30] この NIST Special Publication 800-53 の文書に記載されている 18 のセキュリティ管理策ファミリのうち、この文書の付録 F に記載されている 17 の管理策ファミリは、FIPS Publication 200 に記載されている 17 の最低限のセキュリティ要求事項と密接に関係する。なお、残る一つのプログラム管理（PM）のセキュリティ管理策ファミリは、FISMA が要求する情報セキュリティプログラムに対するセキュリティ管理策となる。当該セキュリティ管理策ファミリは、FIPS200 において明示的に参照されていないにも関わらず、情報システムレベルではなく組織レベルのセキュリティ管理策となる。当該セキュリティ管理策ファミリの詳細および当該セキュリティ管理策ファミリの実装ガイダンスについては、この文書の付録 G を参照のこと。

策である。表 1 は、セキュリティ管理策ファミリの名称とセキュリティ管理カタログにおいてセキュリティ管理策ファミリを一意に識別するための頭文字との対照表である[31]。

表 1:セキュリティ管理策ファミリの名称と頭文字との対照表

ID	ファミリ	ID	ファミリ
AC	アクセス制御	MP	メディアの保護
AT	意識向上およびトレーニング	PE	物理的および環境的な保護
AU	監査および責任追跡性	PL	計画作成
CA	セキュリティ評価および運用認可	PS	人的セキュリティ
CM	構成管理	RA	リスク評価
CP	緊急時対応計画	SA	システム調達およびサービスの調達
IA	識別および認証	SC	システム保護および通信の保護
IR	インシデント対応	SI	システムおよび情報の完全性
MA	保守	PM	プログラム管理

この Special Publication 800-53 の文書に記載されているセキュリティ管理策は、①管理策セクション②補足的ガイダンスセクション③拡張管理策セクション④リファレンスセクションおよび⑤優先順位をベースライン管理策とともに割り当てるセクションの 4 つのコンポーネントからなる構造を有する管理策である。

なお、監査および責任追跡性（AU）のセキュリティ管理策ファミリについての以下の内容は、典型的なセキュリティ管理策についてその構造を具体的に記述したものである。

AU-3　監査記録の内容

管理策：情報システムは、発生したイベントについて種類・発生日時・発生場所・発生原因・結果と合わせて当該イベントに関係する個人（または当該イベントに関係するサブジェクト）の属性を明らかにする情報が含まれた監査記録を生成する。

補足的ガイダンス：AU のセキュリティ管理策ファミリの要求事項を満たす上で監査記録に記載されなければならない場合がある事項には、タイムスタンプ・送信元アドレス・送信先アドレス・（ユーザまたはプロセスの）頭文字・（イベントに関する）説明・（成功および／または失敗を示す）通知・（関連する）ファイル名・（呼び出された）アクセス制御ルール等がある（※ただし、アクセス制御ルールに代わり、フロー制御ルールの場合あり）。また、監査記録に記載されたイベントの結果には、（成功および／または失敗を示す）通知に加えて、イベント発生後における情報システムのセキュリティ状態など、個々のイベントによって異なる結果が含まれる場合がある。なお、関連する管理策は次の通り：AU-2・AU-8・AU-12・SI-11。

拡張管理策：

(1) 監査記録の内容：追加の監査情報

[詳細な追加情報として組織が定義した情報の割り当て]によって割り当てられた情報が記載された監査記録を情報システムが生成する

補足的ガイダンス：組織が監査記録に記載された情報のなかで内容を詳細に検討する可能性のある情報には、記録された特権コマンドの全文に加えて、グループアカウントの各ユーザーに関する情報等がある。なお、誤解を招く可能性のある情報や欲しい情報を見つけ

[31] この文書の付録 J に記載されているプライバシー管理策は、8 つのプライバシー管理策ファミリを 2 文字からなる頭文字によって識別している事を含めて、構成・構造がセキュリティ管理策に近似している。

るのをより困難にしかねない情報が監査記録に含まれるのを防ぐ事で監査証跡と監査ログが容易に利用できるよう、組織は、特定の監査要件を満たす上で明らかに必要な監査情報のみを追加する方向で検討する。

(2) 監査記録の内容:監査記録に取り込まれる予定の内容の集中的管理

監査記録に取り込む内容として[情報システムコンポーネントとして組織が定義したコンポーネントの割り当て]によって生成され事項を情報システムが集中的に管理・構成する。

補足的ガイダンス:この拡張管理策を適用するに当たっては、監査記録に取り込む予定の内容を、一つの場所から必ず自動的かつ集中的に構成する事が要求される。

なお、組織は、情報システムが監査記録に取り込む内容を集中的に管理・設定できるよう、監査記録に取り込まれなければならない内容を選択する。

なお、関連する管理策は次の通り:AU-6・AU-7

参考文献:なし

優先順位の割り当てとベースライン管理策の割り当て:

P1	**低**:AU-3	**中**:AU-3 (1)	**高**:AU-3 (1) (2)

この文書において管理策について規定した部分は、組織または情報システムによって行われるセキュリティ関連の活動について具体的に規定した部分である。情報システムとは、通常はハードウェア・ソフトウェア・ファームウェアといった情報技術の実装を伴う構造体を指す一方、組織とは、通常、プロセス駆動型またはエンティティ駆動型の活動(すなわち、通常、セキュリティ管理策が人間というエンティティによってまたはプロセスによって実装される事)を行う主体を指す。ただし、組織という用語が登場するセキュリティ管理策であっても、セキュリティを確保する上で情報システムが一定の役割を果たす場合がある一方、情報システムという用語が登場するセキュリティ管理策も、セキュリティを確保する上で組織が一定の役割を果たす場合がある。また、セキュリティ管理策において登場する組織および/または情報システムといった用語は、組織レベル・ミッションレベル・業務プロセスレベル・情報システムレベルのいずれかのリスク管理階層におけるセキュリティ管理策の適用を妨げるものではない。

なお、組織は、セキュリティ管理策に関する特定の変数の値を定義する事でセキュリティ管理策カタログを構成する管理策の一部を若干柔軟に適用する事ができる。セキュリティ管理策に関する特定の変数の値は、セキュリティ管理策およびその拡張管理策に組み込まれている割り当てステートメントと選択ステートメントを利用する事によって定義される。詳細な追加情報として組織が定義した情報に関連して上記の AU-3(1)において具体的に記載した通り、割り当てステートメントと選択ステートメントは、監査イベント処理をサポートできるよう監査記録に追加されなければならない情報の指定など、組織が①(組織の)ミッションの達成および(組織の)業務機能の確保ならびに(組織の)ニーズの充足のためのセキュリティ要求事項②リスク評価結果と組織のリスク許容度③連邦法・大統領命令・指令・政策・規制・標準・指針のいずれかに由来するセキュリティ要求事項[32]の 3 つに基づいてセキュリティ管理策およびその拡張管理策を調整できるようにする。上記の AU-3(1)における[詳細な追加情報として組織が定義した情報の割り当て]によって割り当てられる情報は、監査が失敗した場合に情報システムが行う特定

[32] 通常、基本的なセキュリティ管理策に指定・選択の両ステートメントとして組み込まれているステートメントにおいて組織が定義した変数として使用されている数値は、基本的なセキュリティ管理策に関連するすべての拡張管理策にも適用される。

のアクションに関する情報である可能性があるとともに、システムバックアップが行われる頻度に関する情報である可能性がある。また、上記の AU-3(1)における[詳細な追加情報として組織が定義した情報の割り当て]によって割り当てられる情報は、パスワード利用制限に関する情報である可能性があるとともに、組織のポリシー（および組織が踏む手順）に関する配布リストに関する情報である可能性がある[33]。ただし、監査イベント処理をサポートできるよう監査記録に追加されなければならない情報が指定された場合[34]、割り当て・選択の両ステートメントで組織が定義した値はセキュリティ管理策に関する数値となるに加えて、管理策はセキュリティ管理策に組み込まれている完全なステートメントに照らし合わせて実装が評価される。

なお、割り当てステートメントによって組織はあらかじめ定義された特定の複数の値の一つに固定させる事なく変数を自由に指定する事ができる一方、選択ステートメントは組織が指定すべき入力値の一覧を具体的に提示する事によって、入力値を間接的に制限する[35]。

この文書における補足的ガイダンスのセクションとは、特定のセキュリティ管理策を補足する情報を追加で提供する部分であり、セキュリティ管理策について定義・策定・実装のすべて（もしくは定義・策定・実装のいずれか）を行う場合、組織は必要に応じて補足的ガイダンスを適用する事ができる。また、補足的ガイダンスは、操作環境の観点もしくはリスク評価の観点からセキュリティ管理策を実装する場合またはミッション上（および／または業務上）の要求事項の観点からセキュリティ管理策を実装する場合に考慮すべき重要な事項を示しうる部分であるとともに、特定の管理策についてその目的または意義を説明しうる部分である。

なお、セキュリティ管理策全体に対して適用できない補足的ガイダンスが特定の拡張管理策に限定して適用される場合、当該拡張管理策は補足的ガイダンスを含む管理策である可能性がある。また、セキュリティ管理策に対する補足的ガイダンスのセクションと同様、拡張管理策に対する補足的ガイダンスのセクションには、関連する管理策の一覧が表示されている可能性がある。関連する管理策の一覧に表示される管理策には、①特定のセキュリティ管理策（もしくは特定の拡張管理策）の実装を直接支援するまたは特定のセキュリティ管理策（もしくは特定の拡張管理策）の実装に直接的な影響を与えるという特徴に加えて、②セキュリティ機能と密接に関連するという特徴とともに、③補足的ガイダンスにおいて参照されるという 3 つの特徴がある。

セキュリティ管理策の拡張管理策は、定義上、ベースライン管理策関連の管理策である。ベースライン管理策の補足的ガイダンスに記載されているところの「関連する管理策」の一覧は、セキュリティ管理策の拡張管理策における補足的ガイダンスに重複して記載される事はない。ただし、セキュリティ管理策の拡張管理策における補足的ガイダンスには、ベースライン管理策の補足的ガイダンスに記載されているところの「関連する管理策」の一覧に記載されていない管理策が含まれている場合がある。

---

[33] 組織は、特定の割り当てステートメントまたは選択ステートメントが①組織レベル②ミッション・業務プロセスレベル③情報システムレベルのどのレベルにおいて（あるいは①組織レベル②ミッション・業務プロセスレベル③情報システムレベルのどのレベルにまたがって）完了するのかについて、判断する。

[34] 組織は、セキュリティ管理策に記載された割り当て・選択の両ステートメントをセキュリティ計画の一環として完了させる代わりに、セキュリティ計画書に記載されているソースドキュメントを参照しながら、2 つ以上の情報システムに対して適用できる可能性がある値として、セキュリティ管理策における具体的な変数値をポリシー・手順・指針のいずれかのなかで定義するという選択をしてもよい。

[35] セキュリティ管理策は、通常、特定の実装に依存しない技術的に中立な管理策として策定されている事から、技術・実装に関連して特定の要求事項を含む管理策ではない。当該要求事項は、組織によって適宜情報システムのセキュリティ計画書に記載される。

セキュリティ管理策の拡張管理策のセクションとは、セキュリティ管理策の機能を具体的に策定する（および／または管理策を強化する）ために、セキュリティ機能に関するステートメントを提供する部分である。セキュリティ管理策の拡張管理策は、セキュリティ機能に関するステートメントが提供される目的のいかんに関わらず、リスクの自己評価に基づいて組織がベースライン管理策の機能を具体的に策定する際に情報システム（および操作環境）のセキュリティがベースライン管理策によって担保されるセキュリティ以上に確保されなければならない場合に策定される。また、セキュリティ管理策の拡張管理策は、セキュリティ機能に関するステートメントが提供される目的のいかんに関わらず、組織が情報システム（および操作環境）に悪影響を与えないよう情報システム（および操作環境）のセキュリティがベースライン管理策によって担保されるセキュリティ以上に確保されなければならない場合に策定される。

なお、ベースライン管理策を補足する拡張管理策を選択する際、選択された拡張管理策に対してセキュリティ管理策ごとに順番に番号を振る事によって、それぞれの拡張管理策を容易に識別できるようになる。具体的には、この文書の AU-3 においてベースライン管理策を補足する拡張管理策として最初に選択された管理策の番号は「AU-3(1)」となる。また、ベースライン管理策を補足するそれぞれの拡張管理策には、当該拡張管理策が提供しようとしているセキュリティ機能について説明した短い副題が付いている。ただし、ベースライン管理策を補足する拡張管理策の番号は、特定のベースライン管理策を補足する拡張管理策の 1 つを識別する目的にのみ利用される番号であり、拡張管理策の強度を表す番号ではないと同時に、特定のベースライン管理策における複数の拡張管理策の間の階層的な関係を表す番号ではない。また、（この文書の）付録 D に記載されたベースライン管理策の仕様の通り、ベースライン管理策を補足する拡張管理策が個別の管理策として割り当てられる事はない（すなわち、この文書の付録 F に記載された通りセキュリティ管理策のベースライン管理策が割り当てられる場合と同様、ベースライン管理策を補足する拡張管理策が個別の管理策として割り当てられる事はない）。

参考文献のセクションには、連邦行政管理予算局通達・Homeland Security Presidential Directive（国土安全保障に関する大統領指令：以後、HSPD）・FIPS 文書・NIST Special Publications 等、この文書に記載された特定のセキュリティ管理策[36]が準拠する連邦法・大統領命令・指令・政策・規制・標準・指針が列挙されているとともに、拡張管理策を含めセキュリティ管理策を実装する根拠となる連邦法に加えて、拡張管理策を含めたセキュリティ管理策を実装する根拠となる連邦政府の政策が補足情報と合わせて記載されている。また、参考文献のセクションには、セキュリティ管理策を実装・評価するために情報を追加取得しようとする組織が利用する関連サイトの URL が記載されている。

ベースライン管理策の割り当て順序に関するセクションには、セキュリティ管理策の実装順序を決定する際に利用する事が推奨される優先度コードが記載されているとともに、拡張管理策を含めセキュリティ管理策を当初ベースライン管理策として割り当てた順序が記載されている。組織は、個別のセキュリティ管理策の優先度コードを指定することによってセキュリティ管理策の実装順序を決定することができる（すなわち、優先度コードが 1（[P1]）のセキュリティ管理策は優先度コードが 2（[P2]）のセキュリティ管理策よりも優先的に実装され、優先度コードが 2（[P2]）のセキュリティ管理策は優先度コードが 3（[P3]）のセキュリティ管理策よりも優先的に実装されるということを意味すると同時に、優先度コードが 0（[P0]）はいかなるセキュリテ

[36] 参考文献セクションに記載されている文書は、全て最新版である。また、参考文献セクションは、組織がセキュリティ管理策を適用できるようサポートする目的で提供されている一方、参考文献を包括的かつ完全に網羅するセクションではない。

ィ管理策もベースライン管理策とし割り当てられていないことを意味する)。また、他のセキュリティ管理策の基礎となる基本的なセキュリティ管理策が先行して確実に実装されるよう個別のセキュリティ管理策の優先度コードを指定することによって、組織はセキュリティ管理策を利用可能なリソースに応じて適宜より体系的に展開することができる。ただし、リスクを確実に軽減するためには、セキュリティ計画におけるすべてのセキュリティ管理策を優先度コード通りに実装しなければならない。

なお、優先度コードは、実装順序の決定のみを目的として指定されたものであって、セキュリティ管理策を割り当てる目的で指定されたものではない。

2.3 セキュリティ管理策のベースライン管理策

組織は、業務およびミッションの遂行を目的とした情報・情報システムの利用から生じるリスクを最小化しなければならない。この場合、費用対効果が最も高い最適な管理策一式として組織が特に策定するのは、実際に実装された場合に連邦法・大統領命令・規制・政策・指令・標準のいずれか(すなわち、FISMA・連邦行政管理予算局通達 A-130・HSPD-12・FIPS Publication 200 等のいずれか)が規定したセキュリティ要求事項に適合できるようリスクを抑制することが可能なセキュリティ管理策一式である。ただし、組織がセキュリティに関連して関心を抱くすべての事項にあらゆる局面において対応可能な正規のセキュリティ管理策一式は決して存在しない。

なお、リスクを最小化することができるよう組織が特定の場面(または特定の情報システム)に最適なセキュリティ管理策一式を策定することは、組織のミッションにおける優先順位(および/または組織の業務における優先順位)に対する根本的な理解とともに、情報システムがサポートするミッション(および情報システムがサポートする業務)に対する根本的な理解に加えて情報システムが設置される場所におけるシステム運用環境に対する根本的な理解が必要な重要タスクである。組織のミッションにおける優先順位(および/または組織の業務における優先順位)を情報システムがサポートするミッション(および情報システムがサポートする業務)に加えて情報システムが設置される場所におけるシステム運用環境とともに根本的に理解することによって、組織はミッションニーズ(および/または業務ニーズ)をサポートする管理策として組織の情報(および組織の情報システム)の機密性を完全性・可用性とともに最も効果的に確保するためのセキュリティ管理策を IT デューディリジェンスを踏まえて策定することが可能になる。また、組織が利用する情報システムを完全に保護できるよう適切なセキュリティ管理策一式を策定・実装・維持するためには、ミッション(および/または業務)・運用環境・システム利用状況のそれぞれに対して加えられる変更を把握できるようシステム所有者と緊密に連携する必要がある。

この Special Publication 800-53 の文書においては、組織が情報システムのセキュリティ管理策を適切に選択する事ができるよう、ベースライン管理策の概念が取り入れられている。ベースライン管理策は、セキュリティ管理策を割り当てるプロセスとしてこの文書に記載されたプロセスの土台となるものであり、FIPS Publication 199 に準拠して定められたセキュリティカテゴリおよび FIPS Publication 200 に準拠して定められた影響度の組み合わせに基づいて割り当てられる[37]。

なお、この文書の付録 D においては、影響度が高い情報システムおよび影響度が低い情報システムならびに影響度が中程度の情報システムのそれぞれに対するセキュリティ管理策を

[37] CNSS Instruction 1253 は、国家安全システムに対するセキュリティ管理策ベースライン管理策の指針となる。

策定するために（この文書の）3.1 において引用されている（FIPS Publication 200 によって定義された）ハイウォーターマークの概念をもとに策定されたベースライン管理策として、影響度が高い情報システムおよび影響度が低い情報システムならびに影響度が中程度の情報システムのそれぞれに対する 3 つのベースライン管理策がリストアップされている[38]。また、この文書の付録 F においては、組織的なセキュリティ管理策および情報システムのセキュリティ管理策がセキュリティ管理策ファミリごとに並べられた包括的なセキュリティ管理策カタログが記載されている一方、この文書の第 3 章においては、リスクを最小化するためにセキュリティ管理策のベースライン管理策の調整ガイダンスを適用する際に、FIPS Publication 199 によって定義されているセキュリティカテゴリとともに FIPS Publication 200 によってシステムへの影響度として定義されている影響度をどのように活用するかについての追加情報が記載されている。この文書の 3.2 のセクションに記載された調整ガイダンスにより、組織はセキュリティ管理策のベースライン管理策としてリスクの自己評価の結果に基づき選択した管理策を容易にカスタマイズすることができる。

なお、ベースランイ管理策の調整とは、①共通管理策の策定・指定②選定された管理策の実施③代替管理策の選択④セキュリティ管理策におけるパラメータに対する具体的な数値の割り当て⑤セキュリティ管理策またはその拡張管理策の追加を通じたベースライン管理策の補充⑥管理策を実装するための情報の追加提供等を指す。

実装に関するヒント

セキュリティ管理策カタログ（この文書の付録 F）に記載されたセキュリティ管理策およびその拡張管理策の中には、影響度の高いベースライン管理策としてのみ採用される（あるいは全くベースライン管理策とならない）ものがある。セキュリティ管理策カタログ（この文書の付録 F）に記載されたセキュリティ管理策およびその拡張管理策は、組織的なセキュリティ管理策として適用することができる。また、セキュリティ管理策カタログ（この文書の付録 F）に記載されたセキュリティ管理策およびその拡張管理策をベースライン管理策として調整することによって、リスクを自己評価した結果に基づいて必要なセキュリティを確保することができる。

なお、セキュリティ計画におけるセキュリティ管理策一式は、組織のリスク許容度に基づいて（組織の）業務・（組織の）資産・個人・他組織・国家のぞれぞれに対するリスクを最小化する管理策でなければならない。

2.4 セキュリティ管理策の指定方法

この文書の付録 F に記載されているセキュリティ管理策は、①管理策の適用範囲②管理策に共通した性質③管理策を策定・実装・評価・認可する責任のそれぞれについて定める管理策である。なお、これらを指定する管理策には、共通管理策およびハイブリッド管理策だけではなく、特定のシステムに固有の管理策も含まれる。

共通管理策は、セキュリティ機能についての最終的な実装となるセキュリティ管理策として、組織が保有する一つあるいは複数の情報システムによって継承が可能なものである。なお、実装された管理策によって情報システムまたは情報システムコンポーネントが保護されているものの、情報システムまたは情報システムコンポーネントを扱うもの以外のエンティティ（すなわち、情報システムまたは情報システムコンポーネントが存在する組織の内部もしくは外部にあるエンティティ）によって管理策が策定・実装・評価・認可・モニタリングされる場合、情報システ

[38] この文書の付録 D にリストアップされているベースライン管理策は、組織がセキュリティ計画の内容の通り運用認可責任者が設定した諸条件にしたがってセキュリティ管理策を調整できるよう（この文書の）3.2 のセクションに記載された調整ガイダンスによって調整される管理策である。

ムまたは情報システムコンポーネントによるセキュリティ管理策の継承が可能である。ちなみに、共通管理策が提供するセキュリティ機能は、たとえば、組織・組織のミッション・組織の業務分野・サイト・孤立領域・システム運用環境・他の情報システムなどの多くのソースから継承することができる。また、組織の情報システムを保護するのに必要な管理策の多く(例:セキュリティ意識向上トレーニング、インシデント対応計画、設備に対する物理アクセス、行動原則)は、共通管理策の有力な候補である。さらに、公開鍵基盤[PKI]、クライアント(もしくはサーバー)のセキュアな標準構成として認可されたもの、アクセス制御システム、境界保護、クロスドメイン・ソリューションといった様々な技術的な共通管理策がありうる。ちなみに、共通管理策についてその策定・実装・評価・認可・モニタリングを集中的に管理・文書化することによって、セキュリティコストを複数の情報システムにまたがって償却できる。

組織は、組織内の適当な職員(すなわち、共通管理策の提供者)に共通管理策に対する責任を割り振り、共通管理策の策定・実装・評価・認可・モニタリングを調整する[39]。なお、共通管理策の定義に当っては、最高情報責任者・上級情報セキュリティ責任者・リスク担当役員(またはリスク担当役員の機能)・運用認可責任者・情報所有者および/または情報スチュワード・情報システムセキュリティ責任者に加えて、情報システムの所有者の積極的な関与のもとで行われる組織全体にわたる活動として取り組む事が最も有効である。こうした組織全体にわたる活動としての取り組みでは、組織内部の各情報システムのセキュリティカテゴリについて考慮されるとともに、それらのシステムを使用する事により生じるリスクの適切な軽減に必要なセキュリティ管理策について考慮される(2.3 の「セキュリティ管理策ベースライン」の項目を参照)[40]。また、組織内部の情報システムについて全てではないものの複数の情報システムに影響を与える共通管理策を定義する際に同様のアプローチを取ることが有効な場合がある。なお、主な利害関係者は、ミッション(および/または業務分野)・サイト・孤立領域において、いつ共通管理策を有効に使用するかを判断するために互いに協力する。

共通管理策が組織の情報システムをそれぞれ異なった影響度のもとで複数保護する場合、共通管理策は最も高い影響度のもとで実装される。仮に、共通管理策が最も高い影響度のもとで実装されない場合、システムの所有者は、こうした状況を自身のリスク評価に織り込みながら、セキュリティ管理策(または拡張管理策)の追加またはセキュリティ管理策のパラメータに当てはめた数値の変更あるいは代替管理策の実装もしくはミッションおよび/または業務プロセス部分的な変更といった適切なリスク軽減措置を講じる必要に迫られる。なお、有効性に乏しい共通管理策を実装する(またはより高位影響レベルの情報システムに不十分なセキュリティ機能しかもたらさない共通管理策を実装する)ことで、組織のミッション・業務機能のいずれかに重大な負の影響がもたらされる可能性がある。

共通管理策は、通常、特定の情報システムの一部として実装される場合を除き、組織の全体に関係する情報セキュリティプログラム計画書のなかに文書化される。なお、特定の情報システムの一部として実装される場合には、それらの管理策は、その特定の情報システムのセキュリティ計画書のなかに文書化される[41]。組織は、共通管理策を単一のドキュメントに記載す

[39] 最高情報責任者および上級情報セキュリティ責任者ならびにその他組織から任命された上級管理職相当の職員は、共通管理策の策定・実装・評価・認可・モニタリングに関する責任を(組織の内外のいずれかにおける)適切なエンティティに割り当てる。

[40] 組織が選択した各共通管理策については、組織の各情報システムに対して適用可能かどうかの検討が行われる。通常、このレビューは、情報システム所有者および運用認可責任者によって行われる。

[41] この文書の付録 G では、情報セキュリティプログラム計画書について言及している。なお、組織は、共通管理策が提供するあらゆるセキュリティ機能(すなわち、組織の他のエンティティ継承可能なセキュリティ機能)の詳細を確

るかどうか（または複数のドキュメントにリファレンスまたはポインタを含めて記載するかどうか）、柔軟に選択する事ができる。複数ドキュメントの場合、共通管理策について記載しているドキュメントは、情報セキュリティプログラム計画書の添付資料になる。なお、情報セキュリティプログラム計画書に複数のドキュメントが含まれている場合、組織は、各ドキュメントのごとの共通管理策の策定・実装・評価・認可・モニタリングに責任を持つ職員をそれぞれのドキュメントに明記する。たとえば、「PE」（物理的保護・環境保護）のセキュリティ管理策ファミリが特定の情報システムにのみ対応する代わりに複数の情報システムをサポートする場合、組織は、「PE」（物理的および環境的な保護）のセキュリティ管理策ファミリに属する管理策を策定・実装・評価・認可したうえで継続的にモニタリングするよう Facilities Management Office に対して義務付けることができる。共通管理策が情報システムのセキュリティ計画書ごとに別々に記載されている場合（例：セキュリティ管理策が、組織の情報システムの 1 つ以上によって継承される境界保護を提供する侵入検知システムの一部として使用されている場合）、情報セキュリティプログラム計画書は、どのセキュリティ計画書が共通管理策についての記載しているかを示す。

実装に関するヒント

共通管理策を選択するに当っては、組織全体にわたる活動として組織の上層部（すなわち、ミッションの責任者・オーナー経営者・運用認可責任者、最高情報責任者・上級情報セキュリティ責任者・情報システムの所有者・情報の所有者・情報スチュワード・リスク担当役員）による関与することが最も効果的である。これらの者は、組織が優先させる事項組織において業務・資産が果たす重要性に加えて、組織において業務・資産をサポートするうえで情報システムが果たす重要性について、知見を蓄積している。なお、組織の上層部は、共通のセキュリティ管理策ベースラインを選択するのに加えて、これらの管理策を策定・実装・評価・認可・継続的にモニタリングに関して具体的な責任を割り当てるのに最もふさわしい立場にある。

共通管理策は、組織の情報システムにおいて使用する（またはシステムの運用環境の下で使用する）場合のいかんにかかわらず、共通管理策を継承する情報システムに関する運用認可責任者と少なくとも同等のリスク管理権限・リスク管理責任を負う上級職員が認可する。そして、認可した共通管理策の内容は、情報システムの所有者および情報システムの運用認可責任者の両者のうち、しかるべき者との間で共有される。なお、独立的な評価から効果に乏しいと判断された共通管理策については、行動計画およびマイルストーンが確固たるものとして策定される。情報システムの所有者で効果に乏しい共通管理策に依存する者は、関連するリスクを受け入れるのか（または効果に乏しい管理策の弱点や欠陥に対処するために管理策の調整が追加で必要な場合はどうするのか）について検討する。そうしたリスクベースの意思決定は、利用可能なリソースに加えて、運用認可責任者および組織が許容できるリスクの水準や組織が採用するトラストモデルによって左右される[42]。なお、共通管理策に対しては、組織における個々の情報システムに対して使用されている管理策のうち特定のシステムに固有のものと同じ評価要件が、同様のモニタリング要件とともに課せられる。共通管理策は 2 つ以上のシステムに影響を与えるため、それらの管理策の有効性に関して、より高い信頼性が求められる可能性がある。

共通管理策として指定されていないセキュリティ管理策は、特定のシステムに固有の管理策またはハイブリッド管理策であるとみなされる。特定の情報システムに固有の管理策に関して

実な形で十分に記載する。これは、セキュリティ機能を継承するエンティティが共通管理策の実装についてより適切な形で理解できるようにするためのものである。

[42] NIST Special Publication 800-39 の文書は、トラストモデルのうち検証済み（もしくは直接的な履歴となる）ものまたはトラストモデルのうち仲介の（もしくは要求された）ものに関する手引きである

は、情報システムを所有する者および情報システムの運用認可責任者のそれぞれが、第一義的な責任を負う。組織は、セキュリティ管理策の一部が共通で他の部分は特定の情報システムに固有である場合に、セキュリティ管理策にハイブリッドというステータスを割り当てる。たとえば、組織は、インシデント対応策およびインシデント対応手順（IR-1）について、管理策のうちポリシーに該当する部分を共通管理策と指定し手順に該当する部分を特定のシステムに固有の管理策と指定することで、ハイブリッド管理策として実装するかどうか選択する事ができる。なお、ハイブリッド管理策は、管理策をさらに改良するためにあらかじめ定められたテンプレートとしての役割も果たすことができる。たとえば、組織は、緊急時対応計画のセキュリティ管理策（CP-2）に関連して、組織のすべての情報システムに対する一般的な緊急時対応計画（特定の情報システムに固有の用途のために情報システムの所有者によって適宜調整される計画）をあらかじめ定義したテンプレートとして実装するかどうか選択することができる。

共通管理策・ハイブリッド管理策・特定のシステムに固有の管理策という 3 つのセキュリティ管理策に区分することは、組織にとって、実装・評価の双方にかかるコストの大幅な節約に加えて、より整合性のある形でセキュリティ管理策を組織全体にわたって適用する事につながる。なお、セキュリティ管理策が共通管理策・ハイブリッド管理策・特定のシステムに固有の管理策の 3 つに区分されていることは概念的には分かり易く直感的なものである一方で、実際に適用しようとする際には、相当量の計画作りと調整が必要となる。また、システムのレベルでは、共通セキュリティ管理策・ハイブリッドセキュリティ管理策・特定のシステムに固有のセキュリティ管理策のどれであるかの判断は、調整されたベースライン管理策の策定後に行われる。組織は、セキュリティ管理策をどのように実装・運用・維持管理するかについての責任を割り当てる前に、まずは、どのようなセキュリティ機能が必要であるかを判断する必要がある。

個別情報システムのセキュリティ計画書は、それら個別の情報システムにとって欠かす事のできないセキュリティ管理策のどれが組織によって共通管理策として指定されているのかに加えて、同様にどれがそれぞれ特定のシステムに固有の管理策またはハイブリッド管理策として指定されているかについて明らかにするものである。なお、情報システムの所有者は、共通管理策に関連して、特定のシステムに固有の実装の詳細について、どんな形であれ責任がある。特定のシステムに固有の実装の詳細については、個別情報システムのセキュリティ計画書において明示・記載される。また、組織の上級情報セキュリティ責任者は、共通管理策の提供者（例：施設管理者・サイト管理者・人事マネージャー・侵入検知システムの所有者）と連携して、管理策の策定・実装、および有効性の評価を確実に行う。個別情報システムのセキュリティ計画書に加えて、組織全体にまたがる情報セキュリティプログラム計画書は、組織の内部において使用されるすべてのセキュリティ管理策を網羅している。

あるセキュリティ管理策が共通管理策・ハイブリッド管理策・特定のシステムに固有の管理策のいずれであるかの判断は、状況次第である。なお、単に管理策の字面を確認しただけでは、セキュリティ管理策が共通管理策・ハイブリッド管理策・特定のシステムに固有の管理策のいずれかに分類どれに該当するか判断することはできない。これは、具体的には、ある管理策は、ある特定の情報システムにとっては固有なものでありながら、別の情報システムにとってはある特定のシステムから継承を受けた別の共通管理策となりうるという事を指す。なお、ある特定の情報システムに固有の管理策が別の情報システムにとっては共通の管理策となるか否かを知る方法の1つに、誰がまたは何が検討対象の管理策の機能に依存しているかを考えることがある。ある情報システムの特定の部分もしくは外部にあるソリューションの一部がその管理策の機能に依存している場合には、その管理策は共通管理策として明示してもよい。

2.5 外部のサービスプロバイダ

重要なミッションや重要な業務機能を実施する際、組織は外部のシステムプロバイダによって提供される情報システムサービスにより一層依存するようになっている。なお、（外部の情報システムを対象とした）情報システムサービスとは、情報システムに関連して組織が定めた従来のセキュリティ境界の外側で実装されるコンピューティングサービス・ITサービスである。情報システムの物理空間および情報システム資産の管理策の双方に関連して組織が定めた従来のセキュリティ境界では、外部サービスの使用が増加するのに伴い（論理面と物理面の両方で）拡張される。こうした背景のもと、以下の3つが外部サービスを提供する：①組織内のエンティティでありながら、組織の情報システムに関連して定められたセキュリティ境界の外側に存在するエンティティ②組織外のエンティティでありながら公共部門に（例：連邦政府機関）または民間部門のいずれかに属するもの（例：商業サービスプロバイダ）③公共部門のオプションと民間部門のオプションとのなんらかの組み合わせ。また、外部の情報システムに関するサービスとは、たとえば、サービス指向アーキテクチャ(SOA)もしくはクラウドベースのサービス（クラウドベースのインフラストラクチャ、クラウドベースのプラットフォーム、クラウドベースのソフトウェア）またはデータセンターの運用といったものである。ただし、外部の情報システムに関するサービスは組織の情報システム対して使用される可能性があるものの、通常は組織の情報システムの一部でない。場合によっては、（外部の情報システムを対象とした）情報システムサービスは、組織の内部情報システムのルーチン機能を完全に置き換えたり、その機能を大幅に増強する可能性がある。

連邦政府の情報について連邦政府に代わって処理または保存あるいは伝送する（もしくは、情報システムを運用する）外部のサービスプロバイダを利用するよう連邦政府機関に義務付けている FISMA は、OMB の政策とあわせて、外部のサービスプロバイダを利用する事が連邦政府機関が満たさなければならないものと同一のセキュリティ要求事項を満たすものである事を保証する。なお、外部の情報システムに対するセキュリティ管理策など外部のサービスプロバイダに対するセキュリティ要求事項は、契約書または他の正式な合意文書に記載される[43]。また、外部のサービスプロバイダが提供する情報システムサービスを使用する事によって生じる情報セキュリティリスクに対しての責任と説明義務を負う事から、組織は、リスクマネジメントフレームワーク（RMF）を外部プロバイダとの間の契約書における契約条件の一部として組み入れることで、当該情報セキュリティリスクに対処する。さらに、外部の情報システムサービスを利用する際における情報セキュリティリスクの管理について連邦政府が固有の責任を直接負うのと同様に、組織は、外部の情報システムサービスプロバイダに対して、ステップ 5（セキュリティ認可のステップ）以外の RMF のすべてのステップを実装するよう義務付ける事ができる[44]。組織は、外部プロバイダに対して、連邦政府の情報を保護するにあたり RMF に準拠していることを示す適切なエビデンスを提供するよう、義務付けることもできる。ただし、連邦政府機関は、（外部の情報システムを対象とした）情報システムサービスの提供を認可することで、当該情報システムサービス全般のセキュリティについて、直接責任を負う。

---

[43] 組織は、クラウドサービスを外部のサービスプロバイダから取得する場合には、Federal Risk and Authorization Management Program (FedRAMP)に留意する。また、FedRAMP は、さまざまなクラウドサービスに不可欠なセキュリティ管理策を取り扱うのに加えて、さまざまなクラウドサービスについて独立的な評価に取り組む。なお、追加の情報は以下のサイトから入手できる：http://www.fedramp.gov

[44] 組織は、外部のサービスプロバイダの情報システムのうち情報技術またはサービスとして連邦政府に対して提供された部分に該当するもの（インフラストラクチャ・プラットフォーム・ソフトウェア等）に対してセキュリティ認可を行う事によって、情報セキュリティリスクを実効的に管理する。なお、セキュリティ認可の要件は、上記のインフラストラクチャ・プラットフォーム・ソフトウェア等を提供する外部のサービスプロバイダとの間の契約条件として表される。

外部のサービスプロバイダとの間で構築する関係には、たとえば、ジョイントベンチャー・業務提携・外注（具体的には、契約・省庁間合意・業務計画全体・サービス品質保証契約を通じた取り決め）・ライセンス契約および／またはサプライチェーン取引など様々な形がある。外部のサービスプロバイダの利用が増加している事は、それによって外部のサービスプロバイダとの間で構築される新たな関係と同じく、とりわけ情報システムセキュリティの分野において組織が直面する以下の新たな難しい課題を提示している：

- 外部の情報システムサービスのうち、組織に提供されるサービスのタイプを定義する事
- 組織の情報セキュリティ要求事項に準拠して、外部の情報システムサービスがどのように保護されているかを説明する事
- 必要に応じて、外部の情報システムサービスを使用する事により（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれに対して生じるリスクが許容範囲に収まるという保証を得る事

外部の情報システムサービスの利用により生じるリスクが許容範囲内であることがどの程度まで確信できるかは、組織が外部のサービスプロバイダに寄せる信頼次第である。なお、ある状況のもとでは、組織が外部のサービスプロバイダをどの程度まで信頼するかは、サービスおよび／または情報を保護するうえで必要なセキュリティ管理策を使用するにあたって、なおかつ当該セキュリティ管理策の有効性に関して持ち出されるエビデンスを使用するにあたって組織が外部のサービスプロバイダをどの程度まで直接管理できるかに基づくこともある[45]。また、組織が外部のサービスプロバイダをどの程度まで管理するかは、通常、外部のサービスプロバイダと交わすサービス品質保証契約等の契約における契約条件によって、詳細管理策（例：外部のサービスプロバイダに対する詳細なセキュリティ要求事項について規定する契約または取り決めについて交渉する事）に始まり非常に限定的な管理策（例：商用通信サービスなどの汎用サービスを入手するためにサービス品質保証契約またはその他の契約を利用する事）に至るまで、多岐にわたって定めることができる[46]。それ以外にも、外部のサービスプロバイダをどの程度まで信頼するかは、必要なセキュリティ管理策が使用されたと組織に納得させる形跡に加えて、管理策の有効性が実際に判断されたとと組織に納得させる形跡による。たとえば、それぞれ別々に認可された外部の情報システムサービスのうち、一連の良好な取引関係を通じて組織に提供されるものは、それぞれ別々に認可された外部の情報システムサービスの全てについて、リスクがサービスを使用する者（組織・運用認可責任者）の許容する範囲内に収まる事への相当な信頼感を与える可能性がある。

外部のサービスプロバイダによるサービスの提供によって特定のサービスについて組織と外部のサービスプロバイダとの間で明示的な契約がないという事態が起きる可能性があるため、（サービス品質保証契約等の契約を介して）明示的な契約が現実的に可能な場合、組織

[45] 組織が外部のサービスプロバイダをどの程度まで信頼するかは、高い信頼を得ているプロバイダ（例：組織との間でジョイントベンチャー上のビジネスモデル・目標を共有するビジネスパートナー）がある一方で、より信頼されないも関わらずより大きなリスク源となるプロバイダ（例：ある未開拓分野に関してはビジネスパートナーであるが、他の市場分野では競争相手でもある）もあり、プロバイダによって大きく異なりうる。なお、NIST Special Publication 800-39 の文書は、外部のサービスプロバイダとの関係を確立する際に組織が使用できる様々なトラストモデルについて記載している。

[46] 通常、コモディティサービスを提供する商業サービスプロバイダは、多様な顧客層との間でリソース・機器を幅広く共有するという概念を中心に、ビジネスモデルとサービスを体系化する。したがって、組織が商業サービスプロバイダから専用のサービスを入手しない限り、外部のサービスに依存する情報システム対して必要な保護をもたらすうえで補完的なセキュリティ管理策により大きく依存することになる可能性がある。リスクおよびその軽減について組織が行う評価は、このような状況のもとで行われる。

は常に明示的な契約を締結して、この Special Publication 800-53 の文書の付録 F に記載されているセキュリティ管理策の使用を義務付ける。反対に、組織が外部のサービスプロバイダに対して明示的な契約を義務付ける立場にない場合（例：組織がサービスの対象となる事を強制されている場合、もしくはサービスがコモディティサービスである場合）、組織はセキュリティサービスを提供する上での前提条件を明示した文書を作成する。なお、連邦政府一般調達局（もしくはその他、情報システムサービスを調達することが望ましい組織および／または情報システムサービスを調達しなければならない組織）による政府調達契約といった調達ビークルを通じて組織が情報システムサービスを集中的に調達する場合、契約元の組織にとっては、（義務付けられたセキュリティ管理策を提供するにあたり、当該管理策を定義する事に加えて、どの程度まで当該管理策を保証するか明らかにする事を含めて）外部のサービスプロバイダとの間で一定の信頼を確立・維持することが効率的かつ費用照らし合わせて効果的である可能性がある。さらに、外部のサービスプロバイダとの間で一定の信頼を確立・維持した後になって集中契約によって情報システムサービスを調達する組織は、調達元が定めた交渉対象となっている信頼レベルについて活用することができることから、そうした信頼を確立するのに必要な活動について無駄な繰り返しを回避する事ができる[47]。集中的に管理された調達のビークル（例：契約）については、組織の積極的な関与が必要となる場合もある。たとえば、組織は、契約の条項によって、外部サービスプロバイダが推奨するクライアントソフトウェアで公開鍵暗号が可能なものをインストールするよう、義務付けられることがある。

外部の情報システムサービスを使用する事から生じる許容不可能なリスクについて適切な形で軽減する最終的な責任は、運用認可責任者が負っている。また、情報システムセキュリティに関連する多くの問題を扱う場合、組織は外部のサービスプロバイダとの間に適切なトラストチェーンが確立されることを義務付ける。なお、組織は、コンシューマとプロバイダとの間における多分に複雑な関係のなかで組織に向けてサービスを提供するサービスプロバイダが適切な保護を提供する事について一定の信頼を獲得し続ける。コンシューマ・プロバイダに関係するエンティティ数や、当事者間の関係性によっては、コンシューマ・プロバイダにトラストチェーンをより複雑にしうる。外部のサービスプロバイダは、選択したサービスを他の外部組織に委託する可能性があり、この事はトラストチェーンの管理をより困難かつ複雑なものにする。サービスの性質によっては、組織が外部のサービスプロバイダに大きな信頼を寄せることが不可能である場合がある。ただし、このような状況は、外部のサービスプロバイダの側に固有の信頼性が欠けている事に起因するのでは全くなく、外部のサービスプロバイダが選択したサービスに内在するリスクに起因する[48]。

外部サービスおよび／またはサービスプロバイダが信頼を十分に獲得することが不可能な場合、組織は、①代替の管理策を導入することによってリスクを軽減できる②許容できるリスクの範囲内でリスクを受け入れる事ができる③発生しうる損失を補てんできる保険を確保することによってリスクを移転できる④特定のサービスプロバイダから外部サービスを取得しないという選択することによってリスクを回避できる（結果として、機能性が抑制あるいは全くない状態で

[47] たとえば、調達元は、連邦政府に対して外部のサービスを提供する情報システムについて、具体的な契約条件のもとでこれをセキュリティ認可することが出来る。なお、具体的な契約条件のもとで外部のサービスの提供を要求する連邦政府機関は、外部のサービスを取得するにあたって、その情報システムを再認可しなければならない事はない可能性がある（ただし、サービス提供要求が原契約の範囲外のサービスを含む限りにおいて当てはまる）。

[48] セキュリティ上の観点から特定の機能を許可しないことによるリスクが浮上する可能性もある。ただし、セキュリティとは、リスク全般について判断する上で勘案しなければならない要素の一つに過ぎない。

ミッション・業務を遂行することになる）[49]。たとえば、クラウドベースの情報システムおよびクラウドベースのサービスでは、代替管理策として情報セキュリティを強化する目的で、組織がクラウドに保存されているすべての情報の暗号化を義務付ける可能性がある。組織は、（情報の重大性もしくは機微性次第で）クラウドに保存されている情報の一部の暗号化を義務付ける可能性がある。この場合、追加のリスクを受け入れることになるが、それでもすべての情報を暗号化しないまま保存するリスクを抑制する。

2.6 保証と信頼性

組織が構想するリスク管理戦略においては、情報システム・システムコンポーネント・情報システムサービスのそれぞれについて、それらに対する保証ならびに信頼性がより鍵を握るようになってきている。情報システムは、たとえば、国の航空管制システムに対する運用支援に加えて、主要な金融機関の運営支援や大都市に電気を供給する原子力発電所に対する運転支援、さらには軍隊やその戦闘機に対する運用支援などといった導入目的の如何に関わらず、情報システムは、ますます広範囲にわたって巧妙になる広範囲にわたる脅威に対して安定性・信頼性・耐性を兼ね備えたものでなければならない。なお、信頼できるシステムを組織がどのようにして実現するのか、そして信頼性という側面に関連して「保証」が担う役割について理解するためには、まず初めに、「信頼」という用語を定義することが重要である。信頼とは、通常、特定の環境・条件・状況のもとで、エンティティが予測可能な形でふるまうという確信を意味する。また、エンティティは、人・プロセス・情報システム・システムコンポーネント・複数のシステムから成るシステムの単体もしくはそれらのいずれかを組み合わせたものである。

情報セキュリティの面で、信頼とは、中断・人的ミス・コンポーネント障害・コンポーネントエラー・運用環境下における悪意のある攻撃の渦中にあっても、特定の条件（および／または特定の状況）のもとで定められた一連のセキュリティ要求事項を満たしているならば、セキュリティ関連のエンティティは必ず予測可能な形でふるまうという確信を意味する。なお、信頼の度合いは、通常、特定のセキュリティ能力[50]によって決まり、なおかつ個々のシステムコンポーネントあるいは情報システム全体に対して決めるころが可能である。ただし、情報システムとしての信頼の度合いは、一連の信頼できるシステムコンポーネントによってセキュリティ能力を定義することによって得られるのではなく、そのシステムの管理・開発・運用・維持を担うライフサイクル活動を踏まえ、エンティティ（すなわち、技術的コンポーネント・物理的コンポーネント・個人）の複雑な相互作用から自動的に決まるのが基本となる。すなわち、セキュリティ能力が信頼を得るには、セキュリティ能力を定義する一連のセキュリティ関連のエンティティが基本的に十分信頼（信頼性）されていることが求められる。

情報システムにおける信頼性とは、情報システムが様々な脅威に共通して処理・保存・伝送する情報に関連して、情報システムの機密性・完全性・可用性がどこまで確実に担保されているのかについて示すものである。

信頼できる情報システムとは、システムの運用環境において発生することが予想される環境破壊・人的ミス・構造エラー・（意図的な）攻撃に左右されることなく、所定のリスク許容度の

[49] 通常コストはより高くなるものの、より高い信頼基盤を提供する別のプロバイダを利用できる可能性がある。

[50] セキュリティ能力は、技術的手段（すなわち、ハードウェア・ソフトウェア・ファームウェアのそれぞれの機能性）、物理的手段（すなわち、物理デバイス・保護対策）、および／または手続的手段（すなわち、個人によって実施される手続）によって実施される相互補完的なセキュリティ管理策（すなわち、セーフガードおよび／または防護対策）の組み合わせである。

範囲内で運用ができると考えられているシステム（すなわち、負荷を与えた不安定な状態においても割り当てられたミッション・業務機能を遂行するという信頼性を得ているシステム）である[51]。

セキュリティ能力

組織は、セキュリティ管理策の選択プロセスよりも前に、一連のセキュリティ能力の定義を検討するプロセスを置く事ができる。なお、セキュリティ能力（※原文イタリック）は、「情報システムによって処理・保存・伝送される情報が、ひとつの安全機能・防護対策（すなわち、セキュリティ管理策）ひとつによってのみ保護されることはまずない」という構造的な考え方である。ほとんどの場合、情報システムによって処理・保存・伝送される情報は、相互に補強し合うセキュリティ管理策一式を選択・実装することによって保護される。また、組織は、リモート認証を安全に行うためのセキュリティ能力の定義を希望するといった事も出来る。さらに、セキュリティ能力は、この文書の付録 F から一連のセキュリティ管理策を選択・実装する（例：IA-2 [1]、IA-2 [2]、IA-2 [8]、IA-2 [9]、および SC-8 [1]）、導入することによって得ることが可能である。なおかつ、セキュリティ能力は、たとえば技術的・物理的・手続的のいずれか1つ以上の手段等のさまざまな側面に対応する事が可能である。したがって、安全なリモートアクセスのための上記の機能的能力に加えて、組織には安全なリモートアクセスのための上記の機能的能力に加えて、暗号モジュールに対する改ざんを検知する事や軌道上の宇宙飛行体について異常を検知・分析するなどの物理的手段に対応するセキュリティ能力も必要になる可能性がある。

この文書の付録 F に記載されたセキュリティ管理策の数がますます巧妙になる脅威に対応する形で時間の経過と共に増加する事から、組織にとって、主要なミッションおよび／または主要な業務機能の保護に必要な主要なセキュリティ能力に加えて、正しく設計・策定・実装された場合に当該セキュリティ能力を作り出す一連のセキュリティ管理策をそれぞれ記述・定義できることが重要になる。なお、一連のセキュリティ管理策をそれぞれ記述・定義できることで、「情報システムによって処理・保存・伝送される情報が、ひとつの安全機能・防護対策（すなわち、セキュリティ管理策ひとつによってのみ保護されることはまずない」という問題が、より簡潔に示される。セキュリティ能力という構造的な考え方を活用することで、共通の用途のために、あるいは共通の目的を達成するために導入されるセキュリティ管理策を簡単にグループ化することができるようになるという事であり、セキュリティ管理策の有効性を評価するといった際における重要な考慮事項となる。

従来の評価は、セキュリティ管理策の有効性は、個別の管理策ごとに実施され、その結果は合格（すなわち、管理策が有効であることを意味する）または不合格（すなわち、管理策が無効であることを意味する）で行われていた。ただし、1つの管理策（場合によっては複数の管理策）の不具合が、組織が必要とするセキュリティ能力の全体に影響を与えるとは限らない。ちなみに、セキュリティ能力についてより構造的な考え方を使用することにより、組織は、情報システムにおいて発見された脆弱性の重大さについて評価する事が可能になる同時に、（脆弱性に関連して）特定のセキュリティ管理策に生じている不具合または特定の管理策を導入しないとする意思決定がミッション・業務を保護するにあたって必要となる能力全体に影響を与えるとしたらどうなるかについて、判断する事が可能になる。また同様に、管理策どうしで確立された関係に基づいて、1つのセキュリティ管理策の不具合から他の管理策の不具合を見つける事が可能であるかを判断するために、根本原因の分析も容易になる。なお、セキュリティ認可の判断（すなわち、リスクを受容する判断）は、最終的には望ましいセキュリティ能力がどの程度効果的に確保されているかに加えて、組織が定めたセキュリティ要求事項を満たしているかに基づいて行われる。これらのリスクベースの意思決定は、組織が自身のリスクマネジメント戦略の一環として定義したリスク許容度に直接関係する。

情報システムの信頼性に影響を与える２つの基本要素は、「セキュリティ機能性」と「セキュリティ保証」である。通常、セキュリティ機能性は、セキュリティ特性・セキュリティ機能・セキュリティメカニズム・セキュリティサービス・セキュリティ手続・セキュリティアーキテクチャとして組織の情報システムまたはそれらのシステムの運用環境において実装されるもののそれぞれに対し

[51] （組織にとって）情報が一番の関心事である一方で、信用は組織が極めて重要なものであると考えるすべての資産を技術（すなわち、ハードウェア・ソフトウェア・ファームウェア）・物理的要素（すなわち、ドア・ロック・モニタリング）・人的要素（すなわち、人間・プロセス・手続）のそれぞれによって保護する事に関係する。

て定義される。また、セキュリティ保証とは、セキュリティ機能性に関連して①正しく実装されている事②それが意図したとおりに運用されている事③それが情報システムにおけるセキュリティ要求事項を満たしている事（すなわち、確立したセキュリティポリシーを正確に関連付けたうえで正しく適用する能力を有する事）のすべてに対する一定の信頼を指す。なお、セキュリティ管理策は、セキュリティ機能性とセキュリティ保証の両方について考慮する。PE-3 (Physical Access Control)や IA-2 (Identification and Authentication)に加えて SC-13 (Cryptographic Protection)や AC-2 (Account Management)といった主にセキュリティ機能性に焦点を当てたセキュリティ管理策もあれば、他方で CA-2 (Security Assessment)や SA-17 (Developer Security Architecture and Design)に加えて CM-3 (Configuration Change Control)といった主にセキュリティ保証に焦点を当てたセキュリティ管理策もある。また、RA-5 (Vulnerability Scanning)や SC-3 (Security Function Isolation)に加えて AC-25 (Reference Monitor)といった一部の管理策は、セキュリティ機能性とセキュリティ保証の両方をサポートする事が可能である。なお、機能性に関連するセキュリティ管理策は、セキュリティ保証に関連してセキュリティ能力が組織のリスク許容度の範囲内に収まっている事への信頼度を規定する目的で実装される管理策と一体となる。

セキュリティ保証のエビデンスー開発活動および運用活動から

組織は、情報システムに関連して、その開発者・実装者・運用者・メンテナンス要員・評価者のそれぞれが取る行動によって、セキュリティ保証を実現する。また、セキュリティ能力を提供するにあたって必要なセキュリティ機能性に関連して、情報システムを開発および／または運用する過程で個人および／またはグループが取る行動を通じて、セキュリティ保証または信頼性のいずれかの向上に寄与するセキュリティエビデンスが作り出される。なお、情報システムを開発および／または運用する過程で個人および／またはグループが取る行動の範囲としてこの文書の付録Eに記載されているものは、エビデンスの有効性に加えて信頼性にも影響を与える。システム開発ライフサイクルにおいて開発者・実装者・オペレータ・評価者・メンテナンス要員を通じて作り出されたエビデンス（例：設計成果物・開発成果物・評価結果・保証書・評価証明書・検証証明書）は、組織が実装したセキュリティ管理策について理解するのに役立つ。

セキュリティ機能性の強度[52]は、必要なセキュリティ能力を確保した後に組織のセキュリティ要求事項を満たす事を可能にする上で、重要な役割を果たす。なお、情報システムの開発者は、ハードウェア開発プロセス・ソフトウェア開発プロセス・ファームウェア開発プロセスの一部として以下を採用することによって、セキュリティ機能性の強度を高めることができる：①明確なセキュリティポリシーに加えて、セキュリティポリシーについて明快なモデル②それぞれ綿密に構造化された設計技法・開発技法③合理的なシステムエンジニアリング（もしくは合理的なセキュリティエンジニアリング）の原理原則。また、静的テストや動的テストのそれぞれの結果を含めて、ハードウェア開発プロセス・ソフトウェア開発プロセス・ファームウェア開発プロセスという開発活動を通じて生成された機能仕様書・上位レベル設計・下位レベル設計・実装表現（ソースコード一覧・ハードウェア一覧）・コード解析結果は、情報システムならびに当該情報システムを構成するコンポーネントがより信頼性の高いシステムとなるよう、重要なエビデンスを提供することができる。セキュリティエビデンスは、独立性を有する公認の第三者評価機関によって実施されるセキュリティテスト（例：Common Criteria Testing Laboratoriesおよび

[52] 情報システムのコンポーネント（すなわち、ハードウェア・ソフトウェア・ファームウェア）のセキュリティ強度は、そのコンポーネントに実装されているセキュリティ機能がどの程度まで正確・完全であるかとともに、当該セキュリティ機能がどの程度まで直接的な攻撃に耐えているのか（メカニズムの強度）に加えて、どの程度までバイパス・改ざんに耐えているのかによって決まる。

Cryptographic/Security Testing Laboratoriesの両者による評価活動や、その他の政府機関および民間組織による評価活動）からも生成する事ができる[53]。

組織は、開発環境で提示されるエビデンスに加えて、システムの運用環境からもエビデンスを提示する事ができる。なお、システムの運用環境から提示されたエビデンスは、セキュリティ機能性の担保（ひいてはセキュリティ能力の担保）に貢献する。運用のエビデンスとしては、たとえば、バグレポート・レコード・セキュリティインシデントレポートに加えて、組織による継続的モニタリング結果などがあり、実装されたセキュリティ管理策の有効性についての判断材料となるだけではなく、情報システム（およびその運用環境）に加えられた変更についての判断材料となるとともに、連邦政府が制定した法律・政策・指令・規制・標準の対応についての判断材料となる。また、取得元が開発活動・運用活動のどちらであるかに関わらず、実装・使用するセキュリティ管理策について組織がセキュリティエビデンスを通じてより深く理解することができるようになるだけではなく、システム開発ライフサイクルにおいて開発者・実装者・オペレータ・メンテナンス要員・評価者が取った行動を裏付けるエビデンスから、組織の情報システムの内部でどこまでセキュリティ機能性が正しく実装されているかとともに、組織の情報システムの内部でどこまでセキュリティ機能性が意図したとおりに運用されているかに加えて、所定のセキュリティ要求事項を満たす観点から（および確立したセキュリティポリシーの適用または関連付けの観点から）要求した成果がどこまで挙がっているのかについて組織が判断できるようになることから、セキュリティ能力の信頼性は向上する。

「保証」について納得のいく論拠

組織の情報システムがどのように振る舞うかに加えて当該組織の情報システムの機能性に関連して、信頼できるエビデンスを生成する活動を定義する目的のもと、組織はセキュリティ保証関連の管理策を指定する。なお、組織の情報システムがどのように振る舞うかや当該情報システムの機能性を定義する要素にたどりつくまで証跡をたどる目的のもとでも、それは指定される。

このエビデンスは、意図したシステム運用環境において、組織の情報システムを脅威にさらしがらも、組織のミッション・業務を効果的に支援しつつ、所定のセキュリティ要求事項を満たしているという信頼度を得るために使用される。

作成されるセキュリティエビデンスに関しては、そうしたエビデンスの範囲が実装されるセキュリティ機能性の保証レベルに影響を与える。なお、範囲とは、評価手法とセキュリティエビデンスの生成に関連する属性である。評価手法は、開発上の保証と運用上の保証に適用することができる。開発上の保証の場合、depth 属性は、情報システムのハードウェア・ソフトウェア／ファームウェアコンポーネントの設計に加えて、機能仕様書・上位レベル設計・下位レベル設計・ソースコードなどのうち開発時に生成されるものの精密性・形式と関連している。開発関連のアーチファクトの詳細レベルは、システム開発ライフサイクルにおいて実施されるテスト、評価、および解析・グレーボックステスト・ホワイトボックステスト・静的解析・動的解析）に影響を与える。運用上の保証の場合、属性は選択され導入された保証関連のセキュリティ管理策の数とタイプを取り扱う。一方、coverage 属性は、開発および実装時に導入される評価手法に関連し、評価に含まれる対象の範囲と幅を取り扱う（例：ソースコードに対して実施されたテストの数／タイプ、レビューされたソフトウェアモジュールの数、脆弱性スキャンが実施されたネットワ

[53] 具体的には、第三者評価機関は、クラウドサービスとサービスプロバイダを評価する事で、Federal Risk and Authorization Management Program (FedRAMP)を支援する。Common Criteria Testing Laboratories は、ISO/IEC standard 15408 を使用して IT 製品をテストし、評価する。Cryptographic/Security Testing Laboratories は、FIPS 140-2 standard を使用して暗号モジュールをテストする。

ークノード・携帯機器・緊急時対応についての責任を基本的に理解しているかどうかを確認するためのインタビューを受けた個人の数）[54]。

情報システムを調達・開発する際にセキュリティ保証関連の管理策に対応することによって、十分に信頼性の高い情報システムをより信頼性が高く障害発生の可能性が低いコンポーネントとともに組織が取得することが容易となる可能性がある。なお、セキュリティ保証関連の管理策には、包括的なセキュリティアーキテクチャを提供する事や厳格な構成管理を実施する事にを保証する内容とともに、情報システムおよびソフトウェアの変更に対する厳格な制御の実施等、システムセキュリティエンジニアリングの合理的な原則およびそれに基づいた手順を開発者が導入することを保証する内容が含まれている。また、情報システムの展開後におけるセキュリティ保証関連の管理策は、組織がシステムを信頼し続ける事を可能にしうる管理策である。セキュリティ保証関連の管理策には、ソフトウェアコンポーネント・ファームウェアコンポーネントに対する整合性チェックの実施とあわせて、組織の情報システムの脆弱性を見付けるための侵入テストの実施の他に、確立したセキュアな構成の設定のモニタリングに加えて、システム利用・システム運用の支援に関連してポリシーおよび／または手順の策定等がある。

セキュリティ要求事項・セキュリティ能力・セキュリティ管理策・セキュリティ機能性・セキュリティ保証といった概念は、情報システムおよびシステムコンポーネントに対する信頼を示すモデルとして関連付けられている。なお、下記の図 3 は、当該モデルの主要な構成要素と、それらの要素間の関係を示している。

[54] NIST Special Publication 800-53A は、システム開発ライフサイクルにおいて実施されるセキュリティアセスメントに関連するセキュリティエビデンスの生成に関する手引きである。

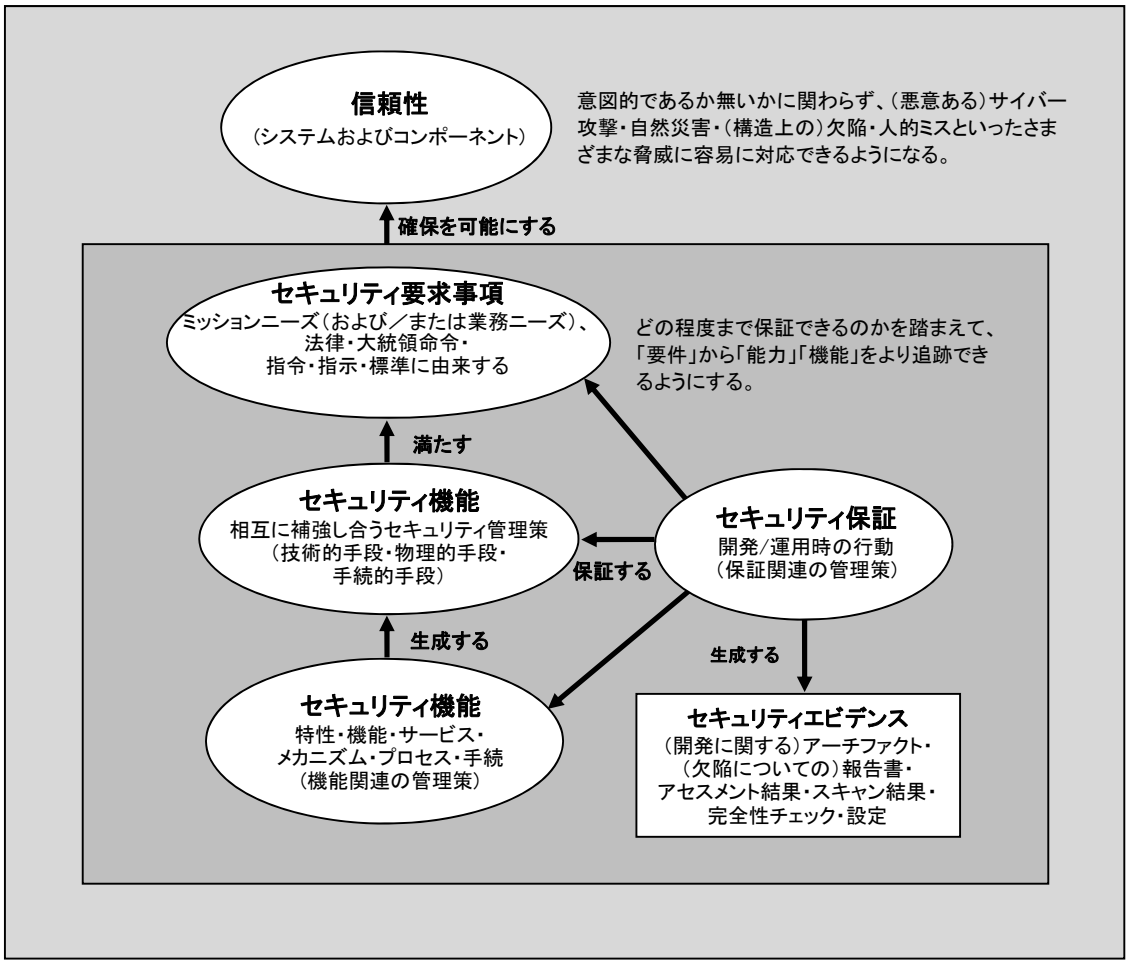


図 3: 信頼性モデル

高い保証を実現するための開発および運用活動

組織にとって高コストかつ困難なものである可能性があるものの、クリティカルなアプリケーション・ミッション・業務に対する保証の水準を引き上げることが不可欠な場合がある。また、実装されたセキュリティ機能性に関連して、組織の IT インフラのどの部分に対してより高い保証が必要なのかを判断することは、直接的もしくは間接的なリスク管理活動である（第 2 章の図 1 を参照）。なお、この種の活動は、組織が（組織の）業務（すなわち、ミッション・機能・イメージ・評判の一部）・（組織の）資産・個人・他組織・国家を保護するのに必要なセキュリティ要求事項を判断する際に発生する。セキュリティ要求事項と適切な保護の提供に必要なセキュリティ能力の組み合わせについて判断することは、NIST Special Publication 800-39 に記載されている「組織のリスク管理プロセス」と一体不可分な行為である。NIST Special Publication 800-39 に記載されている「組織のリスク管理プロセス」とは、具体的に、「リスクのフレーム化」および「リスク評価」の両ステップ（リスクについて優先順位・前提・制限・リスク許容度を確立したうえで、リスクが与える脅威・リスクが突く脆弱性・ミッションに対する影響・業務に対する影響・脅威が発生する可能性を組織が評価するステップ）に続く、「リスク対応戦略」の策定を指す。また、第 1 層と第 2 層における（要求されているセキュリティ能力の信頼性を高めるためのセキュリティ保証要件を含めて）セキュリティ要求事項・セキュリティ能力の判断を踏まえて、セキュリティ要

求事項・セキュリティ能力は、エンタープライズアーキテクチャの設計の他に、関連するミッションや関連する業務プロセスに加えて、関連する業務プロセスをサポートするにあたって必要な（組織の）情報システムに反映される。さらに、ミッション・業務機能の双方のうち主要なものを実施するために導入されている情報システムおよびシステムコンポーネントに対して適切な保証レベルを確保するために、組織は NIST Special Publication 800-37 に記載されているリスクマネジメントフレームワーク(RMF)を使用することができる（なお、ミッション・業務機能の双方のうち主要なものを実施するために導入されているシステムコンポーネントに対しても同様）。これは主に第 3 層における活動であるものの、たとえば共通管理策を選択する場面において、第 1 層および第 2 層における活動と重複する可能性がある。

ソフトウェアおよびシステム開発の観点からすれば、信頼性の高い情報システムを構築するのは難しいものの、適用された場合により信頼性の高いシステムを構築できる設計上・アーキテクチャ上・実装上の諸原則が不特定数存在する。これら主要なセキュリティ原則たる設計上・アーキテクチャ上・実装上の諸原則は、具体的には、分かりやすさ・モジュール・階層化・ドメインの分離・最小権限・最小機能性・リソースのそれぞれの分離および／またはカプセル化などを指す。なお、IT 製品・システムとしてより信頼性の高いもの（すなわち、製品および／またはシステムとして、必要なセキュリティ機能性とセキュリティ保証を有するもの）は、設計・実装上の潜在的な欠陥を有する可能性が低いと見込まれる。同様に、IT 製品・システムとしてより信頼性の高いもの（すなわち、製品および／またはシステムとして、必要なセキュリティ機能性とセキュリティ保証を有するもの）は、高度サイバー攻撃・自然災害・事故・ミス（ただし、ミスの意図を問わず）といった様々なシステム侵入の脅威に対する耐性が高いと見込まれている[55]。IT 製品・システムに必要とされる信頼性の水準は、（組織の）ミッションおよび／または（組織の）業務ならびにそれをサポートする情報システムに対する既知の脅威に対する脆弱性・感受性から決まるだけではなく、組織のミッションおよび／または組織の業務機能をサポートするシステムが導入されているシステム運用環境に加えて、許容可能な情報セキュリティリスクの水準から決まる。

[55] 組織は、この文書の表 E-1 から E-3 に記載されているセキュリティ保証関連の管理策によって示されている運用の観点からのセキュリティ保証にも大きく依存する。なお、運用面でのセキュリティ保証は、開発活動以外の活動（IT 製品に対するセキュリティ構成の設定を定義・適用する事と合わせて、ポリシーおよび手順を定める事とともに、セキュリティ管理策を評価する事に加えて、厳格な継続的モニタリングプログラムを実施する事などを含む）によって得られる。ただし、場合によっては、貧弱または不完全な情報技術をもって必要なセキュリティ能力を実現するために、組織が運用面での保証を強化することによって足らざるものを補う事がある。

セキュリティ保証が重要である理由

セキュリティ保証の重要性は、各人の家の居間の壁にある照明スイッチを例に使用して説明することができる。各人は、単なる照明スイッチの切り替えを通じて、スイッチが機能仕様に従って機能しているというセキュリティ保証の重要性を確認することができる。なお、スイッチが機能仕様に従って機能しているというセキュリティ保証の重要性を確認する事は、情報システム（またはシステムコンポーネント）のセキュリティ機能性についてブラックボックステストを実施する事と近い関係にある。ただし、より重要と思われる問題は下記の通り:

- 照明スイッチは、本来行うべきこと以外に何か別のことを行うか？
- 照明スイッチは壁の裏側からはどのように見えるか？
- 照明スイッチを構築するに当たりどのようなタイプのコンポーネントが使用されたか、また、照明スイッチはどのように組み立てられたか？
- スイッチの製造業者は開発プロセスにおいて業界のベストプラクティスに従ったか？

各人の家の居間の壁にある照明スイッチを例に使用してセキュリティ保証の重要性を説明する事は、情報システム（またはシステムコンポーネント）のセキュリティ機能性の品質に関連する課題を解決するために行われる多くの開発活動（設計原理・コーディング技法・コード解析・テスト・評価等が含まれる）と近い関係にある。

セキュリティ保証上の要求事項およびそれに関連するセキュリティ保証関連のセキュリティ管理策としてそれぞれこの規格の付録 E に記載されているものは、上記のより重要と思われる問題を壁の表側から解決するためのものである。ただし、これらのセキュリティ保障上の要求事項およびセキュリティ管理策は、照明スイッチを構築するために使われるコンポーネントがどれだけ信頼されている必要があるのか次第では、上記のより重要と思われる問題を壁の裏側から解決するためのものとなる。なお、業務機能および／または組織のミッションのうち重要度が低い（すなわち、影響度が低い）ものに対しては、セキュリティ保証はより低い水準でよい可能性がある。逆に、ミッションおよび／または業務機能がより重要になり（すなわち、中程度のまたは強い影響が生じ）、なおかつ情報システム・組織がハイレベルな敵対者によって APT(advanced persistent threats)攻撃を受ける可能性が高くなるにつれて、より高レベルのセキュリティ保証が必要となる可能性がある。また、組織が外部の情報システムサービスおよび外部のプロバイダにますます依存するようになってきた事から、セキュリティ保証の重要性も増している。セキュリティ保証は、外部プロバイダのセキュリティ能力について織が理解・検証するうえで（および連邦政府に対して提供されたサービスについて組織が理解・検証するうえで）、より深い理解と安心感を提供する。したがって、（組織の）業務・（組織の）資産・個人・他組織・国家にもたらされる可能性のある影響が非常に大きい場合、上記のより重要と思われる問題を壁の裏側から解決できるよう、より一層努力する必要がある。

この文書の付録 E は、連邦政府組織および連邦政府の情報システムに対するセキュリティ保証上の最低限の要求事項について記述している。また、当該要求事項が確実に満たされるよう、同じくこの文書の付録 D に記載されているベースライン管理策を構成するセキュリティ保証関連のセキュリティ管理策に焦点を当てている[56]。

2.7 改訂と拡張

この Special Publication 800-53 の文書に記載されているセキュリティ管理策は、連邦政府組織および（連邦政府の）情報システム向けに実用化されている保護手段および対策である。こ

[56] CNSS Instruction 1253 は、安全保障に関わるシステム用のセキュリティ管理策のベースライン管理策を規定している。したがって、安全保障の関係者に向けて策定されたベースライン管理策のなかのセキュリティ保証関連のセキュリティ管理策は、指定された内容次第では、国家以外のセキュリティシステム対して指定されたセキュリティ保証関連のセキュリティ管理策とは異なる可能性がある。

れらのセキュリティ管理策[57]は、以下を反映させるために慎重ながらも定期的に見直され、改定される:

- 管理策を利用することによって得られた経験
- 連邦法・大統領命令・指令・規制・政策のいずれか新しいもの
- 変化するセキュリティ要求事項
- 脅威・脆弱性・攻撃手法の顕在化
- 利用可能となった新しい技術

なお、セキュリティ管理策カタログ内のセキュリティ管理策は、管理策の撤廃・修正・追加に伴い時間と共に変化することが予想される。また、高レベル・中レベル・低レベルのそれぞれのベースライン管理策として定義されているセキュリティ管理策も、組織の内部におけるリスクの削減に関連してセキュリティと注意義務の水準が変化するのに伴い、時間と共に変化することも予想される。さらに、こうした予想される変化の要請に加えて、セキュリティ管理策に対して提案されている変更について、公共と民間の両部門からのフィードバックを経た上で、厳格な公開レビューのプロセスを通じてを得た後に、そうした変更に対する合意の形成がなされることを要求することによって対応する安定性の要請にも対応する。これによって、ゆくゆくは、セキュリティ管理策カタログを使用する連邦政府・受託業者・他のいかなる組織にとって安定性と柔軟性を兼ね備え、技術的に理にかなったセキュリティ管理策の一式が与えられる。

[57] この文書の付録 J に記載されているプライバシー管理策も、将来、同様の基準を用いて日常的に更新される。

第三章

セキュリティ管理策を選択・指定するプロセス

この章は、①セキュリティ管理策のベースライン管理策の適切な選択②セキュリティ管理策のベースライン管理策の調整③セキュリティ管理策を選択するプロセスの明文化④レガシーシステムおよび新たに開発する情報システムの双方の管理策の選択の4つを行うために組織の情報システムのセキュリティ管理策をその拡張管理策とともに選択・特定するプロセスについて論じる章である。

3.1 セキュリティ管理策のベースライン管理策の選択

組織の情報システムおよびその運用環境の双方に適合したセキュリティ管理策を選択・特定するにあたり、組織は当該情報システムによって処理・格納・伝送される情報の重要性についての判断を FIPS Publication 199 において記載されている「セキュリティカテゴリの定義」のプロセスとして当該情報の機密性についての判断とともに先行して行う[58]。

なお、セキュリティカテゴリの定義に関する FIPS Publication 199 の規格は、組織の情報システムに対してもたらされる可能性のある負の影響に即してセキュリティカテゴリを定義するという単純明快な考え方に立脚した規格であり、情報システムを情報セキュリティの 3 要素（機密性・完全性・可用性）ごとにそれぞれ低レベル・中レベル・高レベルのいずれかに分類する（リスク管理フレームワークにおけるステップ 1）よう、組織に対して義務付けている規格である。FIPS Publication 199 に基づいてセキュリティカテゴリが定義されることによって、組織の情報システムを十分に保護できるよう適切なセキュリティ管理策（すなわち、セーフガード・防護対策）を容易に選択できるようになるとともに、組織の情報システムを十分に保護できるよう管理策（すなわち、セーフガード・防護対策）が適切に選択されたことを証明することができるようになる。また、組織の情報システムのセキュリティ管理策として選択された管理策は、情報セキュリティの 3 要素のうち機密性・完全性・可用性のいずれかが損なわれている場合に（組織の）業務・（組織の）資産・個人・他組織・国家に対してもたらされる可能性のある負の影響に対応するための管理策である。

情報セキュリティに対する潜在的な脅威は、組織の情報システムによって処理・格納・伝送のいずれかが行われた情報ごとに分類されたセキュリティカテゴリを表す数値のうち最も高い値（すなわち、ハイウォーターマーク）によって表される[59]。

情報システムのセキュリティカテゴリの一般的な表記は次の通り：

> **SC** 情報システムのセキュリティカテゴリ = {(**機密性**: 影響を表した値), (**完全性**: 影響を表した値), (**可用性**: 影響を表した値)}

[58] CNSS Instruction 1253 は、国家のセキュリティシステムに関連して、セキュリティ分類のガイダンスについて規定している。

[59] *NIST Special Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories"*（情報タイプ・情報システムタイプのセキュリティ分類へのマッピングに関するガイド）は、情報システムのセキュリティを分類するに当たってのガイダンスについて規定している。

なお、特定の情報システムにおいては、機密性・完全性・可用性という情報セキュリティの 3 要素のそれぞれに対する潜在的な脅威を表す数値が常に同じであるとは限らないため、セキュリティ管理策のベースライン管理策として特別に適用可能な管理策をこの文書の付録 D において規定された 3 つのベースライン管理策の中から 1 つ選択する場合、FIPS Publication 200 では FIPS Publication 199 で導入されている「ハイウォーターマーク」の概念を用いる事によって脅威レベルを判断する[60]。強固な情報システムとは、機密性・完全性・可用性のいずれについても高い情報システムを指す。また、脅威にさらされている情報システムとは、機密性・完全性・可用性の 3 要素の少なくとも一つが脅威にさらされている情報システムを指すとともに、脆弱な情報システムとは、機密性・完全性・可用性の少なくとも一つに対する重大な脅威が存在する情報システムを指す。

実装に関するヒント

情報システムに対する脅威レベルを判断するためには、

- まずは、情報システムによって処理または格納もしくは伝送される情報の種類の違いが明確にされなければならない。（なお、一般的な情報の種類については NIST Special Publication 800-60 を参照のこと。）
- なおかつ、セキュリティカテゴリは、FIPS Publication 199 において規定された脅威レベルおよび NIST Special Publication 800-60 において規定された推奨事項に準拠して機密性・完全性・可用性という情報セキュリティの 3 要素ごとに定義されなければならない。
- さらに、情報システムのセキュリティカテゴリは、機密性・完全性・可用性という情報セキュリティの 3 要素のそれぞれに対する脅威を表す数値のうち最も高い値としてのハイウォーターマークとして定義されなければならない。
- 加えて、全般的な脅威レベルは、機密性・完全性・可用性という情報セキュリティの 3 要素のそれぞれに対する脅威を表す数値のうち最も高い値から判断されなければならない。

注記：組織は、CNSSI 1253 に準拠して国家安全保障システムのセキュリテカテゴリを作成する。

機密性・完全性・可用性という（情報セキュリティの）3 要素のそれぞれに対する脅威を表す数値のうち最も高い値から判断された脅威レベルとして FIPS 200 において規定された（情報システムの）脅威レベルに基づいて選択・指定されたセキュリティ管理策を情報システムに対する適切なベースライン管理策として選択・指定するプロセス（RMF におけるステップ 2）に先立って、組織は情報システムに対する脅威について判断する[61]。また、組織はセキュリティ管理策のベースライン管理策としてこの文書の付録 D に記載されている 3 つの管理策のなかから 1 つの管理策を情報システムに対する脅威レベル（高・中・低のいずれか）に応じて選択する[62]。た

[60] 最高水準の概念が採用されている理由は、機密性に関連する情報セキュリティ目的および完全性に関連する情報セキュリティ目的ならびに可用性に関連する情報セキュリティ目的のそれぞれと大きな相互依存関係があるからに他ならない。大抵の場合、上記の 3 つの情報セキュリティ目的のうちいずれか 1 つが侵害された場合、最終的には残りの 2 つのセキュリティ目的にも影響が及ぶ。したがって、セキュリティ管理策はセキュリティ目的別に分類されていない。ただし、セキュリティ管理策が各ベースライン管理策ごとにグループ分けされ事によって、情報システムに対する影響度を基準にした全般的な保護機能が情報システムのクラスに提供される。

[61] セキュリティ管理策を選択する一般的なプロセスは、セクション 3.3（「オーバーレイを作成する」）および付録 I（「オーバーレイを開発するためのテンプレート」）に記載されたような特定の分野に特化した追加の手引きにて、より詳細に展開・記述される可能性がある。

[62] CNSS Instruction 1253 は、国家安全システムに対するセキュリティ管理策のベースライン管理策について規定している。

だし、ベースライン管理策となるセキュリティ管理策はこの文書の付録 D の表 D-2 において「not selected（選択されていない)」と記載されている管理策の数の通り一部にすぎないとともに、この文書の付録 D の表 D-3 から D-19 にわたって示されているように、セキュリティ管理策のうち一部の拡張管理策がベースライン管理策となるにすぎない。

なお、この文書の付録 D の表 D-3 から D-19 では、ベースライン管理策となる拡張管理策に対して「高」のベースライン管理策の列または「中」のベースライン管理策の列もしくは「低」のベースライン管理策の列のいずれかにおいて「x」印が付けられている。また、セキュリティ管理策（および／またはその拡張管理策）が（この文書の 3.2 のセクションに記載されている）調整ガイダンスに基づいて削除もしくは追加される（または特殊な管理策として扱われる）場合、意図的にベースライン管理策と呼ばれるセキュリティ管理策およびその拡張管理策のそれぞれは最初に削除もしくは追加される（または特殊な管理策として扱われる）管理策となる。

この文書の付録 D に記載されているセキュリティ管理策のベースライン管理策は、個人ユーザ・組織といった広範かつ多様な利用者層のセキュリティニーズに対応する管理策である。ただし、当該ベースライン管理策は、一般的に①組織の情報システムの運用環境②組織によるシステム運用の特徴③情報システムが有する機能④組織・情報システム・ミッション（および／または業務プロセス）が直面している脅威のタイプ⑤情報システムによって処理または保存もしくは伝送される情報のタイプ等を自明の前提として策定される管理策である。管理策が自明の前提とする組織の情報システムの運用環境等は、NIST Special Publication 800-39 に記載されているリスク管理プロセスを構成するステップのうち冒頭のリスクのフレーミングのステップのなかで明らかにしなければならない。

なお、この文書の付録 D に記載されたベースライン管理策は、

- 組織の情報システムが物理的に施設内に設置されていること
- 組織の情報システムにユーザデータ（ユーザ情報）が半永久的に存在すること[63]
- 情報システムが複数のユーザによって連続して（あるいは同時に）運用されること
- 組織の情報システムへのアクセスが許可された他のユーザとの間でユーザデータ（ユーザ情報）の一部が共有不可であること
- ネットワーク化された環境下に情報システムが存在していること
- 情報システムが当初より一般的な用途に使用されていること
- 管理策を実装するうえで必要な体制を組織が整えていることおよび管理策を実装するうえで必要なリソースを必要なインフラとともに組織が有していること[64]

等を自明の前提として策定されている。ただし、上記の通り組織の情報システムが物理的に施設内に設置されていること等の前提のうちの1つあるいは 2 つ以上が成立しない場合、ベース

[63] 永続的なデータおよび／または永続的な情報とは、データおよび／または情報のうち比較的長い期間（例：数日間・数週間）にわたって使用可能なものを意味する。

[64] 通常、連邦政府の各省庁は、この前提を満たす。反面、この前提は、市町村・ファースト・レスポンダー・小規模請負事業者などの連邦政府以外のエンティティにとってより大きな問題となる。連邦政府以外のエンティティは、ベースライン管理策よって担保される幅広いセキュリティ能力を提供する要素を有するに当たって、十分な規模または十分なリソースを有していない可能性があるため、リスクに基づいた意思決定を行うにあたり、組織はそうした要素を考慮する。

ライン管理策として（この文書の）付録 D の冒頭に記載されているセキュリティ管理策の一部が適用できない可能性がある（なお、該当する管理策はこの文書の 3.2 のセクションに記載されている調整ガイダンスに従って容易に適用することができる。また、該当する管理策は組織がリスクを評価することによって容易に適用することができるようになる）。また、

- 組織の内部で内部不正が行われている
- 情報システムが機密データを処理・保存・送信している
- 組織が APT(Advanced persistent threat)攻撃を受けている
- 連邦法・（連邦政府の）指令・（連邦政府による）規制・（連邦政府の）政策に基づいて選択されたデータおよび／または選択された情報を特別に保護しなければならない
- 異なるセキュリティドメイン間で情報システムが他の情報システムとの間で通信を行わなければならない

のそれぞれに該当する場合、組織は当該ベースライン管理策を当然に適用することができない。

ベースライン管理策として（この文書の）付録 D に記載されたセキュリティ管理策が適用できない場合、この文書の付録 F にて追加されているセキュリティ管理策によってセキュリティを十分に確保する必要が生じうる。（なお、この文書の付録 D においてベースライン管理策として記載されたセキュリティ管理策は、セキュリティ管理策の補足的ガイダンス等、この文書の 3.2 のセクションに記載されている調整ガイダンスに従って効果的に適用することができる。また、当該セキュリティ管理策は、組織がリスクを評価することによって効果的に適用することができるようになる）。

3.2 セキュリティ管理策のベースライン管理策の調整

この文書の付録 D からベースライン管理策として適用可能なセキュリティ管理策を選択した組織は、選択された管理策が組織のミッションもしくは組織の業務機能（または組織の情報システムもしくは組織のシステム運用環境）といった特定の内的条件とできるだけ矛盾しないよう、

- セキュリティ管理策のベースライン管理策に関連して、当初のベースライン管理策の中から共通管理策を策定・指定すること
- 当初のベースライン管理策のうち共通管理策として策定・指定されなかったセキュリティ管理策に対して「スコーピングにあたっての考慮事項」を適用すること
- 必要に応じて代替管理策を選択すること
- 明示的ステートメントとしての指定ステートメントおよび明示的ステートメントとしての選択ステートメントを通じて、セキュリティ管理策に関する変数として組織が定義した変数に具体的な数値を割り当てるること
- セキュリティ管理策（およびその拡張管理策）を追加することによって必要に応じてベースライン管理策を補足すること
- 必要に応じて管理策の実装仕様に関する情報を追加提供するプロセス

など、当該管理策を調整しながら適切に修正するプロセスに着手する。

（セキュリティ管理策を選択・特定するプロセスと不即不離の関係にある包括的なリスク管理プロセスの一部として）組織がセキュリティ管理策を調整するプロセスとは、可視化された情報

セキュリティリスクを評価したうえで情報セキュリティリスクへの対応状況をモニタリングするプロセスであるとともに、組織がミッションおよび／または業務を効率的かつ安全に遂行できるようにするプロセスである。また、リスク管理ガイダンスとは、セキュリティ管理策がベースライン管理策として適用可能かどうかの意思決定を組織がリスクベースで容易に行うことができるようにするガイダンスである。

なお、リスク管理担当役員・最高情報責任者・上級情報セキュリティ責任者・情報システムオーナーに加えて共通管理策の提供者等の運用認可責任者は、調整されたセキュリティ管理策を実装するかどうか、その他の重役の一部とともに判断する。また、特定のミッションプロセス（および／または特定の業務プロセス）もしくは特定の事業部門をサポートする目的で、組織は、不可欠なベースライン管理策として（および／または特定の情報システムに対するセキュリティ管理策を調整できるよう）情報システムのセキュリティ管理策を全面的（および／または個別）に調整するかどうか柔軟に決定することができる[65]。ただし、組織は運用上の都合からセキュリティ管理策を廃止する事はない。また、セキュリティ管理策の調整は、ミッションニーズおよび／または業務ニーズに基づいて正当化できる内容でなければならないとともに、リスクベースの明確な意思決定に基づいて行われなければならない[66]。

なお、セキュリティ管理策を調整するプロセスについては、セキュリティ管理策を調整しなければならない具体的な理由を含めて組織の情報システムに関するセキュリティ計画書に記載される。組織（共通管理策提供者等）または組織の情報システムのオーナーはベースライン管理策として適用可能な全てのセキュリティ管理策について説明する責任を負っているため、特定のセキュリティ管理策が調整された場合、情報システムのセキュリティ計画書には、セキュリティ計画を承認するプロセスのなかで組織の責任者によって承認された内容として、セキュリティ管理策が調整された理由（またはセキュリティ管理策が調整された理由について記された関連文書名が記載される[67]。

情報システムを運用認可するか否かについてリスクベースで正確に判断するために必要な情報を運用認可責任者が得られるようになるためには、セキュリティ管理策を選択するプロセスのなかで、リスクを管理するにあたって行われた重要な意思決定を文書化することが不可欠である。ただし、情報システムを運用認可するか否かについて運用認可者が行った当初の判断を見直す際、情報システム・システム運用環境・（システム開発ライフサイクルに関係する）職員を変更する可能性があることから、情報システムを運用認可するか否かについて運用認可者が行った当初の判断の際に前提となった条件（ならびに当該判断の根拠となった事柄および当該判断の際に制約となった事項）が文書化されることにより、将来情報システムのセキ

[65] 3.3『オーバーレイを作成する』と付録 I『オーバーレイを作成するためのテンプレート』も参照のこと。

[66] セキュリティ管理策を調整できるかどうかは、特定の定められた条件下で選択されたセキュリティ管理策が打ち出されるタイミングに加えて、当該管理策が適用出来るかどうか次第となる場合もある。そのことは、セキュリティ管理策があらゆる状況に適用されるわけではないということか、もしくは指定ステートメントに関する変数値が特定の状況において変化する可能性がある事に他ならない。なお、オーバーレイによって、セキュリティ管理策が適用されない特別な状況とは何かに加えてセキュリティ管理策を調整する場合における特定の条件とは何かについて、なおかつセキュリティ管理策が打ち出されるタイミングに関連して考慮すべき事項とは何かについて、定義することができる。

[67] セキュリティ管理策を選択するプロセスにおいてセキュリティ管理策の調整に関する判断をどの程度まで詳細に文書化しなければならないかは、組織の自由裁量に任されていると同時に、セキュリティ管理策を実装または継承する情報システムがどの程度影響を受けるのかによって変わる。

ュリティがどこまで担保されるか（または当該判断の際のシステム運用環境）について、より正確に認識することが可能になる。

共通管理策の指定

共通管理策は、組織の情報システムの 1 つ以上に適用される管理策である。情報システムに共通管理策が適用された場合、別のエンティティによってセキュリティが確保されているため、当該情報システムに当該管理策が明示的に実装される必要はない。また、この文書の付録 F に記載されているセキュリティ管理策が情報システムに特定のセキュリティ機能が実装または実行されるよう要求する場合であっても、より大規模かつ複雑な情報システムの一部を構成するシステムもしくは特定の情報システムのすべてのコンポーネントにセキュリティ管理策またはセキュリティ機能が実装される必要があると解釈してはならない。

なお、どのセキュリティ管理策を共通管理策として指定するかについての組織の判断は、特定のベースライン管理策を実装するにあたってシステムオーナーの各自が負う責任の内容に大きな影響を与える。また、実装される共通管理策の数が多いほど費用を節減できる可能性が高いことから、当該判断は組織によるリソース消費全般にも影響を与えうる。

「スコーピングについての考慮事項」の適用

リスク管理ガイダンスと共に適用される「スコーピングについての考慮事項」はリスクベースの意思決定を行う際に必要となるより詳細な情報を組織に対して提供する[68]。なお、「スコーピングについての考慮事項」を適用する事により、セキュリティ管理策のベースライン管理策として当初策定されたものから不必要なセキュリティ管理策を削除することができる。ちなみに、「スコーピングについての考慮事項」の適用は、適切なレベルの保護（すなわち、ミッションおよび／または業務機能として組織の情報システムがサポートするものに基づくのに加えて、システム運用環境に基づく保護）を組織の情報システムに対して提供するのに必要なセキュリティ管理策のみが組織によって選択されるよう、組織を支援するものである。また、組織は、セキュリティ管理策を選択・指定するに当たって行われるリスクベースの意思決定（すなわち、組織によってセキュリティ管理策のベースライン管理策がどのように適用・実装されるかに影響を与える可能性がある意思決定）を行うのを容易に行えるようにするために、以下に記載されている「スコーピングについての考慮事項」を適用できる：

- セキュリティ管理策について、その割り当て・配置に当たり考慮する事項

  「情報システム」という用語は、システムオブシステムズから個々のシングルユーザシステムに至るまで、抽象度の異なる様々なシステムを指す言葉として用いる事が可能である。また、多くの情報システムが、より複雑になる事で、特定のいかなるアーキテクチャー上の視点またはアーキテクチャーソリューションを設定することなく 3 つのリスク管理階層（組織階層・情報システム階層に加えて、ミッションおよび／または業務プロセス階層）のうちどの階層にセキュリティ管理策を割り当てるか（および／または導入するか）について、慎重な分析しなければならない[69]。セキュリティ管理策のベースライン管理策として当初策定され

[68] このセクションにおいて列挙されている「スコーピングについての考慮事項」は、代表的なものであり、その他考慮する事項として正当な理由に基づいて組織が定義したものに依拠したリスクベースの意思決定を各組織が下すのを制限する事を意図するものではない。

[69] これは、サービス指向型アーキテクチャの出現に関連して、ある 1 つの機能を実装する目的で特定のサービスが提供される場合において、顕著な事実となっている。

た管理策は、情報システム全体に関係するセキュリティ管理策の一式でありながら、すべての個別の情報システムコンポーネントに適用できない可能性がある管理策を指す。なお、セキュリティ管理策は、管理策に規定されている情報セキュリティ能力を提供またはサポートする情報システムコンポーネントにのみ適用できる[70]。また、必要なセキュリティ能力を実現するため、なおかつセキュリティ要求事項を充足するために、組織は自己の情報システムのどの部分に特定のセキュリティ管理策を適用する（または割り当てる）かについてのリスクベースの意思決定を着実に実行する[71]。前記の通り、組織が自己の情報システムのどの部分に特定のセキュリティ管理策を割り当てるかについて、リスクベースの意思決定を確実に行う場合における特定のセキュリティ管理策の割り当ての例として、ゲスト用のサブネットワークで他のシステムコンポーネントに接続されていないものに対するワイヤレスアクセスを除く全てのワイヤレスアクセスに対して、この文書の AC-18(1)におけるセキュリティ要求事項を適用すること（すなわち、認証および／または暗号化を使用して情報システムに対するワイヤレスアクセスを保護すること）がある。

- 運用および／または環境に関連して考慮する事項

  セキュリティ管理策のベースライン管理策の内いくつかのセキュリティ管理策は、運用要素および／または環境要素が特定の形で存在するという前提に基づいている。なお、運用要素および／または環境要素について、特定の形で存在していない（もしくはベースライン管理策が前提とする）諸事項と大きく異なるものとなる場合に、ベースライン管理策の調整を正当化できる。運用要素および／または環境要素のうちより一般的な要素の一部は、以下の通り:

  - **モビリティ**

    物理的ホスティング環境の移動性モビリティは、組織の情報システム用に選択されたセキュリティ管理策に影響を与える。上の通り、この文書の付録 D のそれぞれのベースラインに割り当てられているセキュリティ管理策の一式は、情報システムが固定の設備かつ固定の場所で稼働していることを前提としている。仮に組織の情報システムが主にモバイル環境下で稼働する場合、組織の情報システムが存在する特定の場所のモビリティとアクセシビリティの違いに対応できるよう、セキュリティ管理策のベースライン管理策を適切に調整しなければならない。たとえば、PE（物理的保護・環境保護）ファミリセキュリティ管理策は、適切な物理的保護を必要とする物理的な設備および／または物理的な複合設備に情報システムが存在するという前提を反映したものである。なお、これら 3 つのベースライン管理策の全ては、船舶・航空機・自動車・バンまたは宇宙を基盤に展開されている情報システムなどのモバイル環境下においては、付加価値をもたらさない可能性が高い[72]。

---

[70] たとえば、システム監査管理策は、通常は監査機能を提供する情報システムコンポーネント（例：サーバーなど）に適用され、必ずしも組織内のすべてのユーザレベルにあるワークステーションに適用されるという事ではない。なお、組織はコンポーネントのインベントリとして組織の情報システムを構成するものを慎重に評価のうえ、様々なコンポーネントにどのセキュリティ管理策が適用可能であるかを判断しなければならない。

[71] 情報技術が進歩するにつれ、より強力かつより多様な機能性をスマートフォン・タブレット等その他のタイプの携帯機器に見出す事が出来る。なお、調整に関するガイダンスが特定のセキュリティ管理策を特定の技術（または特定の機器）に割り当てないことをサポートする可能性がある反面、（組織の）業務・（組織の）資産・個人・国家・その他組織を十分に保護するためにも、リスクを評価するにあたっては、セキュリティ管理策が特定の形で存在しない事に伴うその他のいかなるリスクを考慮しなければならない。

[72] （情報システム等の）機器が有する「モバイル」という特性は、（情報システム等の）機器が、ある一定の期間にわ

- **シングルユーザシステムおよび単独ユーザによる運用**

  シングルユーザシステムとして運用するように設計された情報システム（例：スマートフォン）にとって、ユーザ間の共有に対応するためのセキュリティ管理策のいくつかは不要なものである可能性がある。なお、単独ユーザが使用している情報システム（および／または単独ユーザが使用している機器）は、情報システムおよび／または機器として長期にわたって単独の人間によって使用される（すなわち、排他的に使用する）ことが意図されたものを指す。ただし、長期にわたって複数のユーザによって共有されるシステム（または長期にわたって複数のユーザによって共有される機器）は、シングルユーザとはみなされない。シングルユーザシステム（および／または単独ユーザによる運用）では、AC-10（同時セッションの管理）・SC-4（共有リソース内の情報）・AC-3（アクセス強制）[73]などのセキュリティ管理策が不要となる可能性に加えて、組織の自由裁量によりベースライン管理策から除外される可能性がある。

- **データ接続とデータの帯域幅**

  多くの情報システムは、相互に接続されている。他方で、セキュリティ上または運用上の理由によりネットワーク機能を持たない情報システム、（すなわちネットワークからは隔離されている情報システム）もある。ネットワーク化されていない情報システムでは、AC-17（リモートアクセス）・SC-8（データ送信の機密性およびその整合性）・SC-7（境界保護）などのセキュリティ管理策は適用できないだけではなく、組織の自由裁量による調整の結果、ベースライン管理策から除外される可能性がある。なお、ネットワーク化されていない情報システムに加えて、はなはだ限定的な若しくは不規則な帯域幅を持つ情報システムもある（例：軍隊や警察による作戦を支援する戦術的なシステム）。はなはだ限定的な（または不規則な）帯域幅を持つ情報システムでは、不規則および／またははなはだ限定的な帯域幅に対してセキュリティ管理策を実際に実装できるかどうかに加えて、敵対者が限られた帯域幅上でサイバー攻撃を行うことが現実のものとなる可能性の双方に影響を与えうるため、セキュリティ管理策を適用する当っては、慎重な検証が必要になる事が見込まれる。

- **機能性が限定された情報システム（または機能性が限定されたシステムコンポーネント）**

  2002 年の電子政府法の適用対象となる情報システムは相当広範囲に及び、ファックス・プリンター・スキャナー・ポケットベル・スマートフォン・タブレット・電子書籍端末・デジタルカメラは、すべて情報システム（または情報システムコンポーネント）に分類される可能性がある。なお、2002 年の電子政府法の適用対象となるタイプの情報システムおよびそのコンポーネントには、セキュリティ管理策のベースライン管理策が前提とする一般的な処理能力を備えていないという制約が存在する可能性もある。ただし、こうした制約の性質上 2002 年の電子政府法の適用対象となる情報システムが直面する脅威が限定的なタイプのものにとどまるがゆえに、一部のセキュリティ管理策の妥当性も限定的なものとなる可能性がある。したがって、（すべての場合において必ずベースライン管理策となる）SI-3（悪質なコードからの保護）などのセキュリティ管理

たって固定の施設または固定の場所におけ施設に存在する可能性があることを意味する。その際、PE ファミリに属するセキュリティ管理策が適用される可能性が多分にある。

[73] AC-3 の管理策をセキュリティ管理策のベースライン管理策から除外する前に、組織は個々のユーザが管理者権限を持っているか否について検討する。

策は、テキストのみを扱うポケットベル等、コードを実行することができない情報システム（またはそのコンポーネント）にとって役立ずなものとなる可能性がある。他方で、例えばスマートフォンはデジタル電話・デジタルカメラ・デジタルコンピュータの機能を併せ持つといったように、コードを実行することができないタイプの情報システムの間、（またはそのコンポーネント間）に明確な区分けがないことが多いため、機能性が限られた情報システム（またはそのコンポーネント）に対するセキュリティ管理策の適用は慎重に行うことが重要である。さらに、同様の理由から、システムについて意図した用途についてに加えて、システム能力についてや侵害のリスクについて常に考慮する事も重要である。

- **システムの非永続性と情報との関係**

  組織の情報システムの内部にあるユーザ情報は、相当の期間にわたって存在し続けるという想定がなされることが多い。ところが、戦術的なシステムや産業用制御システム等における一部のアプリケーションにおいては（もしくは戦術的なシステムや産業用制御システム等を運用する環境によっては）、ユーザ情報を保持する期間が非常に短い場合が多い。さらに、CP-6（代替ストレージサイト）・CP-7（代替処理サイト）・CP-9（情報システムのバックアップ）などの CP（緊急時対応計画）ファミリに属するいくつかのセキュリティ管理策は、そうした非永続の情報について処理もしくは保存または伝送する情報システムに適用できない可能性があるのに加えて、組織の自由裁量による調整の結果ベースライン管理策から除外される可能性がある。同様の理由から、MP-6（メディアサニタイズ）・SC-28（非アクティブ情報の保護）などのセキュリティ管理策も、調整の結果ベースライン管理策から除外される可能性が高い[74]。なお、情報が非永続性なものとなるだけではなく、情報システムおよび／または情報サービスも非永続的なものとなる可能性がある。また、非永続的情報サービスおよび／または非永続的な情報システムは、仮想化技術を使用してオペレーティングシステムやアプリケーションの非永続的インスタンスを導入することによって実現できる。ただし、インスタンスの有効期間によっては、一部のベースライン管理策が適用できない可能性がある。

- **パブリックアクセス**

  セキュリティ管理策のベースライン管理策のうち特定の管理策（例：識別および認証に関する管理策ならびに職員に関する管理策）がパブリックアクセスに対して適用できない可能性があるため、組織の情報システムへのパブリックアクセスが許可されている場合、セキュリティ管理策を適用するかどうかは自由裁量となる可能性がある。一般の人々が連邦政府の各機関のウェブサイトにアクセスする場合（例：書式をはじめ、緊急事態に備えるための情報など一般の人々がアクセス可能な情報のダウンロード）、AC-7（ログイン試行失敗）・AC-17（リモートアクセス）・IA-2（識別および認証）・IA-4（識別子管理）・IA-5（認証子管理）などのセキュリティ管理策は、アクセス認可またはアクセス権限の有効化には通常は対応しない可能性がある。ただし、個人情報にアクセス若しくは個人情報を変更しようとする際に、パブリックアクセスのインターフェイスを通じてユーザーがプライベートな情報システムへアクセスするうえで前記 AC-7 等のセキュリティ管理策の多くは依然必要となる可能性がある。

[74] 組織は、情報の永続性と情報の機微度とを整合させる。なお、非永続の情報であっても、消去後にサニタイゼーションが必要になる場合がある。さらに、永続的な情報である可能性がありながら非永続的な機微情報も一部存在することから、組織はある情報がいつまで機微情報であり続けるのかについても検討する

- 情報セキュリティ目的に関連して考慮すべき事項

  以下の場合においては、情報セキュリティによって維持されるべき機密性・完全性・可用性の 3 要素の全てをサポートしないセキュリティ管理策は、より下位のベースライン管理策に格下げ（あるいは、より下位のベースライン管理策としてではない場合は、当該管理策は修正または削除）される可能性がある：①情報セキュリティによって維持されるべき機密性・完全性・可用性の 3 要素に関連したセキュリティのカテゴリとして影響度（すなわち FIPS Publication 200 に記載された最高水準）に先行して FIPS Publication 199 に記載されたカテゴリを反映している場合[75]②組織によるリスク評価によって裏打ちされたものである場合③情報システム内のセキュリティ関連情報の保護水準に負の影響を与えない場合[76]。具体的には、仮に最高水準の概念を当てはめたところ、情報セキュリティの三要素のうち機密性および／または完全性は中程度の水準に分類されるにも関わらず可用性の要素が低水準に分類されるために情報システムが中程度の影響を有するものとして分類された場合、可用性の要素のみをサポートするセキュリティ管理策として下位のベースライン管理策（要件）に格下げされる可能性がある管理策がいくつか存在する事になる。CP-2(1)の拡張管理策は、情報セキュリティの三要素のうち可用性の要素のみをサポートするものであって、中位のベースライン管理策として格付けされているものの低位のベースライン管理策としては格付けされていないため、実装されるべき管理策に該当しない可能性がある。なお、格下げられる可能性があるセキュリティ管理策およびその拡張管理策は以下の通り：[77]

  - 機密性：AC-21・MA-3(3)・MP-3・MP-4・MP-5・MP-5(4)・MP-6(1)・MP-6(2)・PE-4・PE-5・SC-4・SC-8・SC-8(1)
  - 完全性：CM-5・CM-5(1)・CM-5(3)・SC-8・SC-8(1)・SI-7・SI-7(1)・SI-7(5)・SI-10;and

[75] セクション 3.1 に記載されている「最高水準」を適用する場合、情報セキュリティによって維持されるべき機密性・完全性・可用性の 3 要素として当初 FIPS Publication 199 に記載されたもののなかには、より上位のベースライン管理策によってサポートされるようになる可能性がある。反面、上位のベースライン管理策によってサポートされるようになる過程で、不必要であるにも関わらず、機密性・完全性・可用性といった情報セキュリティによって維持されるべきものを単独でサポートするセキュリティ管理策が更新されてしまうことがある。したがって、費用対効果に優れたリスクベースのセキュリティ管理策を確実に適用するうえで、適切かつ許容可能な格下げ作業を行えるよう組織が検討することを推奨する。

[76] 情報システムのレベルにおけるセキュリティ関連情報（例：パスワードファイル・ネットワークルーティングテーブル・暗号鍵管理情報）は、同一の情報システム内のユーザレベル情報とは区別される。なお、情報セキュリティによって維持されるべき要素である機密性と完全性の2つをサポートする目的で、ユーザレベル情報とシステムレベルの情報の双方に対して特定のセキュリティ管理策を使用する。機密性または完全性に関連したセキュリティ管理策を格下げする場合には、格下げによって情報システム内のセキュリティ関連情報に対する保護が不十分なものとなる結果を招かないように注意を払わなければならない。ユーザレベル情報に関連して機密性・完全性・可用性という情報セキュリティによって維持されるべき要素のいずれかについて同様の水準の保護を達成するためにも、セキュリティ関連の情報については、最高水準の保護がなされなければならない。

[77] 格下げの対象となるのは、中位および上位のベースライン管理策のみである。通常は格下げの有力な候補とみなされるセキュリティ管理策のうち、機密性・完全性・可用性の三要素のいずれかのみの確保を目的とする AC-16・AU-10・IA-7・PE-12・PE-14・SC-5・SC-13・SC-16 などの管理策は、いかなる場合においてもベースライン管理策となることから格下げが可能な拡張管理策がないため、あるいは管理策は任意なものである事からいかなる場合においてもベースライン管理策とならないため、格下げの検討対象から外される。この文書のセクション 3.2 における一覧表に記載されていないセキュリティ管理策を格下げする場合には、格下げによって情報セキュリティによって維持されるべき機密性・完全性・可用性の三要素のうち当該管理策によって確保されるもの以外の要素が影響を受けないように、組織は注意を払わなければならない。

- 可用性：CP-2(1)・CP-2(2)・CP-2(3)・CP-2(4)・CP-2(5)・CP-2(8)・CP-3(1)・CP-4(1)・CP-4(2)・CP-6・CP-6(1)・CP-6(2)・CP-6(3)・CP-7・CP-7(1)・CP-7(2)・CP-7(3)・CP-7(4)・CP-8・CP-8(1)・CP-8(2)・CP-8(3)・CP-8(4)・CP-9(1)・CP-9(2)・CP-9(3)・CP-9(5)・CP-10(2)・CP-10(4)・MA-6・PE-9・PE-10・PE-11・PE-11(1)・PE-13(1)・PE-13(2)・PE-13(3)・PE-15(1)

- 技術に関連して考慮すべき事項

  特定の技術（例：ワイヤレス技術・暗号技術・公開鍵基盤技術）に関するセキュリティ管理策は、当該技術が組織の情報システムに導入されている（あるいは導入が必要である）場合にのみ適用できる。なお、自動化されたメカニズムが既存のものでない場合または市販用（または政府向けの）既製品において容易に見出す事ができない場合、自動化されたメカニズムによるサポートを明示的に（もしくは暗黙裡に）受ける可能性のあるセキュリティ管理策は自動化されたメカニズムを新たに開発するよう要求する事はない。自動化されたメカニズムを容易に見出す事ができない場合または自動化されたメカニズムが費用対効果に優れた場合（もしくは自動化されたメカニズムが技術的に実現可能な場合）、自動化されていないメカニズムまたは手続によって実装される補完的管理策を使用することによって指定されたセキュリティ管理策またはその拡張管理策を満たすといった選択肢もある（補完的管理策の適用に関する後記の諸条件を参照）。

- ミッション上の要求事項に関連して考慮すべき事項

  実装によって組織のいずれもクリティカルなミッションおよび／または業務が弱体化または妨害される可能性がある場合、一部のセキュリティ管理策は適用できない（または管理策として適切でない）可能性がある。具体的には、クリティカルなオペレータコンソール（例：航空管制官用のコンソール）上にミッションクリティカルな情報が途切れることなく表示されることを組織のクリティカルなミッションが要求する場合、AC-11(Session Lock)またはSC-10 (Network Disconnect)を実装しないことが望ましい。

補完的管理策を選択する

組織においては、補完的なセキュリティ管理策を導入しなければならない場合がある。補完的管理策とは、それぞれ低位・中位・上位のベースライン管理策としてこの文書の付録 D に記載されている管理策のうち、特定のセキュリティ管理策の代わりに組織によって採用された代替管理策（すなわち、組織の情報システムによって処理または保存もしくは伝送される情報に対して、組織の情報システムと同等または匹敵する保護を提供する管理策）を指す[78]。補完的管理策は、たとえば、組織がセキュリティ管理策のうち特定のベースライン管理策を有効に実装できない場合（または情報システムに固有の理由もしくはシステムの運用環境上の理由からベースライン管理策がリスクを必要に応じて軽減するうえで費用対効果に優れた手段とならない場合）に採用される。また、補完的管理策は、通常、調整に関するガイダンスにおいて記載されている「スコーピングについての考慮事項」をセキュリティ管理策のベースライン管理策として適用可能な管理策に対して適用した後に採用される。組織は、

[78] この文書の付録 F 記載されているセキュリティ管理策のうち、特定のセキュリティ管理策に関しては、同等の保護を提供するのに 2 つ以上の代替管理策が必要になる可能性がある。たとえば、職員の数が非常に限られている組織は、「監査」、「説明責任」、および「職員によるセキュリティ」管理策を強化することによって、「職務の分離」セキュリティ管理策を埋め合わせることも考えられる。

- 組織がこの文書の付録 F から補完的管理策を選択する場合。ただし、適切な補完的管理策がない場合は、他のソースから適切な補完的管理策が採用される[79]。
- どのように補完的管理策が組織の情報システムに対して同等のセキュリティ能力を提供するのかとともに、なぜセキュリティ管理策のベースライン管理策を採用できないのかについて、組織によって裏付けとなる根拠が示された場合。
- 組織の情報システムに代替管理策を実装することによって生じるリスクを評価した組織が当該リスクを受け入れる場合。

のすべてに該当する場合にのみ、補完的管理策を採用してもよい。

セキュリティ管理策に関する変数値の割り当て

特定の組織的な要求事項をサポートする管理策としてセキュリティ管理策および拡張管理策のうち埋め込み変数（すなわち、「指定」ステートメントと「選択」ステートメント）が盛り込まれた管理策は、セキュリティ管理策および拡張管理策の特定の部分を組織が柔軟に定義できるようにする管理策である。「スコーピングについての考慮事項」を最初に適用し代替管理策を選択した組織は、組織が定めた適当な値を「指定」ステートメント（および／または「選択」ステートメント）用のセキュリティ管理策について当該管理策の拡張管理策とともに見直しを行うことによって変数として定義する。ただし、定義された変数の値は、関連する連邦法・大統領命令・指令・規制・政策・標準によって規定される場合がある。また、「指定」ステートメントや「選択」ステートメントは、セキュリティ管理策に関する変数の値および拡張管理策に関する変数の値のそれぞれが定義される事によって、セキュリティ管理策および拡張管理策のそれぞれの一部となる[80]。変数が指定されることによって管理策の定義が完全なものとなる事から（また、変数の指定が指定補完的管理策の要求事項に影響を及ぼす可能性がある事から）、組織は補完的管理策を選択する前にセキュリティ管理策に関する変数の値を指定することができる。

なお、変数の値を開発するために協力することによって、大きなメリットがもたらされる可能性がある。具体的には、頻繁に共同作業を行う組織にとって、セキュリティ管理策に関する変数として両者で合意可能な統一値の一式を開発することが有益である可能性があるため、相手の組織が提供する情報システム（および／または相手の組織が提供するサービス）に依存している場合に、一方の組織には大きな利益がもたらされる可能性がある。

セキュリティ管理策ベースラインの補足

組織の情報システムおよび当該システムの運用環境において十分なセキュリティを提供するのに必要なセキュリティ管理策の一式が適切な管理策の一式であるかどうかは、（組織の）業務・（組織の）資産・個人・他組織・国家に対するリスクを十分に軽減するために何が必要かについて検討された結果をリスク評価の結果と突き合わせることによって最終的に決定される[81]。ただし、今後は、組織・ミッション・業務プロセス・情報システムのすべて（またはいずれか）に

[79] 組織は、この文書の付録 F に記載されているセキュリティ管理策カタログから代替管理策を選択できるよう、最大限に努力しなくてはならない。組織が定めた代替管理策は、セキュリティ管理策カタログ内に代替となる適切な管理策がないと組織が判断した場合にのみ採用される。

[80] CNSS Instruction 1253 は、国家のセキュリティシステムに適用可能なものとして組織が定めた変数に最小値を設定する事について規定している。なお、変数値は、この文書における 3.4 のセクションに記載されているオーバーレイの一部として設定することも可能である。

[81] 組織の情報システムを分類する事が国家および他の組織に及ぼしうる影響について考慮する根拠として、アメリ

対する特定の脅威に加えて組織等に内在する脆弱性に対処するとともに、関連する連邦法・大統領命令・指令・政策・標準・規制が要求する事項を満たすために、この文書の付録 D に記載されたセキュリティ管理策のベースライン管理策および当該セキュリティ管理策の拡張管理策以外にセキュリティ管理策を追加することが多くの場合必要になる[82]。また、セキュリティ管理策を選択するなかでリスク評価を行う事により、ベースライン管理策として当初策定されたセキュリティ管理策およびその拡張管理策の必要性を判断するに当たって重要かつ不可欠な情報が得られるとともに、ベースライン管理策として当初策定されたセキュリティ管理策およびその拡張管理策が十分なものであるかどうかについて判断するに当たって重要かつ不可欠な情報が得られる。組織は、当初のベースライン管理策を補足するプロセスがセキュリティ管理策および／または拡張管理策を追加することによって容易になるよう、この文書の付録 F を最大限に活用することが望ましい[83]。

ベースライン管理策を補足することが必要となる可能性のある状況

運用または環境もしくは脅威の見地から、組織のミッションおよび組織の業務を（組織の）業務・（組織の）ミッションをサポートする情報システムとともに完全に保護することができるよう、補足管理策を追加で選択・実装する事が組織に義務付けられる可能性がある。

なお、組織に義務付けられる可能性がある条件（および追加で選択・実装するよう組織に対して義務付けられる可能性がある補足管理策に関する具体的内容）は、以下を参照のこと:

- APT 攻撃に関連して

セキュリティ管理策のベースライン管理策は敵対者が組織および組織の情報システムのそれぞれの内部において大きな地位を占めるようになった（すなわち、組織が APT と呼ばれる持続的標的型攻撃に対処している）現在の脅威環境を前提に策定されたものではないため、敵対者は組織の情報システムおよび IT 基盤を執拗に攻撃のうえ破壊することに成功している。なお、APT に全面的に対処する管理策としては、「インサイダー脅威からの保護」(CM-5(4))・「不均質性」(SC-29)・「詐欺」(SC-26・SC-30)・「非永続性」(SC-25 および SC-34)・「セグメンテーション」(SC-7(13))などの管理策が該当する可能性がある。

- クロスドメインサービスに関連して

  セキュリティ管理策のベースライン管理策は、情報システムを複数のセキュリティドメインにわたって運用しなければならないということを前提として策定されている管理策ではない。なお、セキュリティ管理策のベースライン管理策は、平面的な情報の流れ（すなわち、情報が承認された範囲を越えて異なるドメインに移動してもセキュリティポリシーが同じであること）を前提としている。異なる情報セキュリティポリシーを持つ複数の情報システム間で伝送される情報を十分に保護するよう万全を期すべくセキュリティ管理策のベースライン管理

カ合衆国の愛国者法および国土安全保障に関する大統領指令（HSPDs がある。

[82] この Special Publication 800-53 の文書の旧版では、「調整」とはセキュリティ管理策のベースライン管理策を削除することを意味し、「補足」とはセキュリティ管理策のベースライン管理策を追加することを指していた。なお、この版の文書においては、「調整」という用語はセキュリティ管理策のベースライン管理策について追加（すなわち、調整による追加）と撤廃（すなわち、調整による撤廃）の両方を意味するように再定義されている。

[83] ベースライン管理策を補足する目的で選択されたセキュリティ管理策およびその拡張管理策は、適切な情報システムコンポーネントに対して、当初のベースライン管理策によって組織が実施する管理策の割り当てと同じ方法で割り当てられる。

策がクロスドメインサービスおよびドメイン間トランザクションに対応するうえで、AC-4 の拡張管理策のサブセットのいくつかについて、運用を検討する余地がある。

- 移動性に関連して

  携帯機器を使用する事によって、セキュリティ管理策（およびその拡張管理策）のうち当初はベースライン管理策として選択しなかった管理策をベースライン管理策として追加する必要が生じる可能性がある。具体的には、携帯機器の盗難や紛失の脅威に対処するために、（組織が所定の回数にわたってログオン試行が失敗した場合に情報を消去もしくはワイプすることを課す）AC-7(2)または（リモートで情報を消去もしくはワイプできることを課す）MP-6(8)のいずれかが追加で選択される可能性がある。

- 機密情報に関連して

  一部の環境においては、機密情報および機微情報[84]がすべてのユーザには機密情報および機微情報のすべてにアクセスするうえで必要な権限が与えられていない状態で国家安全システムのなかに収容されている可能性がある。ただし、そうした環境においては、許可のないユーザによる厳重に隔離されなければならない情報へのアクセスが決して起こらないよう、追加的なセキュリティ管理策（より厳格なアクセス制御について規定した管理策としては、AC-3(3)・AC-16 などの管理策がある）が必要になる。また、複数のエンティティ（例：軍事同盟の相手方）との間で共同所有する情報システムにおいて機密情報が処理または保存もしくは伝送される場合には、MA-5(4)といったメンテナンス要員向けのより限定的なセキュリティ管理策が必要となる可能性がある。

追加のセキュリティ管理策を必要に応じて特定するためのプロセス

組織は、当初のベースライン管理策を補足する目的でセキュリティ管理策および拡張管理策を選択する場合、要件定義アプローチまたはギャップ分析アプローチを用いることができる。要件定義のアプローチが選択されて場合、組織は特定の能力を有する可能性のある敵対者または特定の攻撃を行う可能性がある敵対者の活動に関連してスキル水準・専門知識・利用可能リソースといった具体的かつ信頼のおける脅威情報[85]を入手できるようになる（または、特定の能力を有する可能性のある敵対者または特定の攻撃を行う可能性がある敵対者の活動について、合理的な仮説を立てることができるようになる）。また、特定の能力がある（または特定の攻撃を行う可能性がある）敵対者からのサイバー攻撃に対して効果的に立ち向かうために、組織は一定の防御能力を確保できるようになることによって、サイバー攻撃に対して一定程度備えることができるようになる。一定の防御能力を確保することによってサイバー攻撃に対して一定程度備えることができるよう、組織はこの文書の付録 F に記載された管理策の中からセキュリティ管理策およびその拡張管理策を追加で選択することができる。

なお、要件定義アプローチとは対照的に、ギャップ分析アプローチは組織が現在有する防御能力（すなわち、サイバー攻撃に対して組織がどの程度備えているか）を評価することから始まるアプローチである。組織は、防御能力について当初評価した内容をもとに、どのような種類の脅威ならば対抗できるという合理的な見通しを立てることができるのかについて判断を下す。ギャップ分析アプローチでは、組織が現在十分な防御能力を有していない場合（すなわち、サ

[84] ここでの例は、明示的な例にすぎない。CNSS Instruction 1253 においては、国家のセキュリティシステムに必要なセキュリティ管理策に関する具体的なガイダンスが規定されている。

[85] この例は、意図的な攻撃が情報システムにもたらす脅威に焦点を当てている。しかしながら、組織に対して懸念される可能性がある脅威には、環境破壊や人的ミスも含まれる。

イバー攻撃に対する組織の備えが十分ではない場合）に、組織がどの程度防御能力を増強しなければならないのか（すなわち、サイバー攻撃に対して組織がどこまで備えなければならないのか）について、判断することができる。

なお、組織は、防御能力（すなわち、サイバー攻撃に対する備え）を強化するために必要なセキュリティ管理策を拡張管理策とともにこの文書の付録 F をもとに策定することができる。ただし、要件定義アプローチまたはギャップ分析アプローチのいずれのアプローチも、組織がタイムリーかつ正確な脅威情報を保有していることが必要なアプローチである。また、タイムリーかつ正確な脅威情報を得る上で、脅威を識別する適切なコンポーネントを用いる事が不可欠である。

管理策を調整するプロセスのなかで優先順位コードの変更が適切であるかを適宜判断するために、組織はセキュリティ管理策のベースライン管理策をもとに優先順位コードを再評価する。ベースライン管理策として追加される全く新たなセキュリティ管理策が P0 の優先順位コードを有している事から、ベースライン管理策として全く新たなセキュリティ管理策を追加する際にセキュリティ管理策のベースライン管理策をもとに優先順位コードを再評価することが非常に大切である。

なお、優先順位コードは、①組織によるリスク評価②セキュリティアーキテクチャの設計および／またはセキュリティアーキテクチャの開発に関連する決定事項③システムエンジニアリングプロセスおよびセキュリティエンジニアリングプロセスのうちセキュリティ管理策を実装する際に一定の順序のもとに行われなければならないプロセスのいずれかを通じて再評価することができる。

選択された管理策を変更せずに強化される情報セキュリティ

組織が特定の情報技術を利用する場合（または組織が特定のコンピューティングパラダイムを活用する場合）リスクを十分に軽減または緩和するうえで適切なセキュリティ管理策を自らの情報システムに対して適用できないという状況が発生する可能性があるため、組織のミッション（および／または組織の業務）が負の影響を受けないよう、代替管理策（すなわち、ミッションおよび業務に対するリスクとして情報技術の積極的な使用により生じるリスクについて考慮した管理策）が必要になる。付随的管理策と同時に（または付随的管理策に代わって）リスクを低減させる代替管理策は、利用される技術の種類を制限することに加えて組織の情報システムがどのように利用されるかを制限することによって策定される。ただし、情報システムの利用に対する制限は、特定の情報技術の利用に対する制限とともに、場合によっては、割り当てられたミッション（および／または割り当てられた業務）を遂行する能力を確保できるよう敵対者と判断された者を前にして組織が取る事が可能な行動として現実的または合理的な唯一の行動となる可能性がある。

なお、情報システムの利用に対する制限および特定の情報技術の利用に対する制限とは、具体的に、

- 情報システムが処理または保存もしくは伝送することが可能な情報の量を制限すること（または組織のミッションおよび／または組織の業務の自動化を制限すること）
- 選択した情報システムコンポーネントをネットワークから削除することによって、外部から組織の情報にアクセスできないようにすること（すなわち、エアギャップ）

- 公衆のアクセスを明示的に許可するリスク判断がなされない限り、影響度が中程度の情報または影響度が高い情報を組織の情報システムコンポーネントとして公衆にアクセスさせないようにすること。

の 3 つを指す。

管理策の実装に関して追加の仕様情報の提供

セキュリティ管理策とはセキュリティ能力をきわめて抽象的に記載した文章であることから実際に管理策を実装するための情報が十分に記載されていない可能性があるため、実際に管理策を実装するための情報が十分に記載されていないセキュリティ管理策がどのような目的で実装されるのかが完全に定義できるよう（なおかつ当該セキュリティ管理策が要求する事項をすべて満たすことができるよう）、管理策の内容を補足しなければならない可能性がある。具体的には、セキュリティ管理策が要求する事項を満たすことができるよう管理策の内容が補足される可能性があるのと同時に、実装の詳細（または実装範囲）を再定義できるよう（または、同一の管理策を異なる実装範囲ごとに異なる形式で適用できるよう）、管理策の内容が補足される可能性がある。ただし、「選択」ステートメントおよび「指定」ステートメント等の既存のセキュリティ管理策がその目的を十分に果たすことができるよう定義された管理策ではない場合、組織は管理策の内容を補足しなければならない。

なお、組織は、管理策に新たな文章を追加すること（または補足的ガイダンスもしくは管理策の付録）によって補足するのかどうか、柔軟に判断する事ができる。ただし、組織が管理策の内容を補足するに当たっては、当初のセキュリティ管理策の趣旨を逸脱してしまう（または、当初の管理策の文章を修正してしまう）ことがないよう、注意しなければならない。また、実装に関する追加情報は、セキュリティ計画（またはシステムエンジニアリング計画およびセキュリティエンジニアリング計画）として文書化することができる。セキュリティ管理策を完全に実装する場合に必要となる可能性がある詳細な追加情報については、下記の SI-7(6)の通り:

SI-7　ソフトウェア・ファームウェアと情報の完全性との関係

(6) ソフトウェア・ファームウェアと情報の完全性との関係 | 暗号による保護

情報システムは、暗号メカニズムをソフトウェア・ファームウェア・情報のそれぞれに対する不正な変更を検出する目的で実装する。

補足的ガイダンス: 情報の完全性を保護する目的で使用される暗号メカニズムには、具体的には、①デジタル署名②非対称鍵暗号を利用して署名されたハッシュ値の計算および同様に署名されたハッシュ関数の適用③ハッシュ値を生成する目的で利用した鍵の機密性の保護④公開鍵を使用したハッシュ情報の確認等がある。

なお、この文書に記載されたセキュリティ管理策のうち当該部分に関連する管理策は、SC-13 の管理策である。

SI-7 (6)の実装に関する詳細な追加情報:

デジタル署名は、SHA-256 または少なくとも同一の強度のメカニズムを有する事が別途実証されている承認された NIST アルゴリズムを利用したトラフィックのうち、否認防止が必要な全てのトラフィックに対して適用される。

3.3 オーバーレイの作成

先のセクションは、組織がより的確かつより適切なセキュリティ能力を実現するためにセキュリティ管理策のベースライン管理策を調整する過程についての説明であった。なお、関係者全体が使用するためのセキュリティ管理策の一式を策定する上であるいはな要求事項または特殊な技術もしくは特有のミッションあるいは特有の稼働環境に対応する上で、特定の状況においては組織が調整に関するガイダンスをベースライン管理策に適用することが有用でありうる

[86]。ちなみに、連邦政府はセキュリティ管理策の一式および実装に関するガイダンスとして以下のような政府全体にわたるものを策定に向けて取り組む事が可能である：①連邦政府の諸機関において実装されている全ての公開鍵基盤（PKI）システムに対して一律に適用可能な PKI システム②様々なクラウドサービスを調達または実装している全ての連邦政府機関に対して一律に適用できるクラウドベースの情報システム③連邦政府の諸施設において電力を生産している若しくは連邦政府の諸施設において当該施設における環境システムを制御している産業用制御システム（ICS）。他方で、特殊なセキュリティ要求事項を共有する特定の利害関係者に対応するために、例えば、国防総省等による戦術作戦および戦術環境用のセキュリティ管理策の一式と併せて実装ガイダンスの一式を策定する決定を行う可能性がある。ただし、こうした決定は、国家のセキュリティシステム用のセキュリティ管理策の標準的なベースライン管理策に対して調整に関するガイダンスを適用する事によって、より専門的なソリューションを実現するべく行われる。また、上こうした決定が行われた場合、調整されたベースライン管理策を各 IT 分野に即してまたは個別の状況や個別の環境に即して策定する事が可能になる事で、利関係者に対して幅広く普及させることが可能となる。これにより、標準化されたセキュリティ能力に加えて、一貫した実装、なおかつ費用対効果に優れたセキュリティソリューションを実現する。

情報システムおよび組織にコミュニティ全体に関係する特殊なセキュリティ管理策の一式を策定するニーズに対応するために、オーバーレイという概念が導入されている。なお、オーバーレイとは、セキュリティ管理策・（その）拡張管理策・補足的ガイダンスのうち、この文書の付録 D に記載されたセキュリティ管理策のベースライン管理策に対して 3.2 のセクションに記載された調整に関するガイダンスを適用する事によって策定される管理策等について、例外なく指定したものである[87]。また、オーバーレイは、以下の手法を通じてセキュリティ管理策のベースライン管理策を補足する：①管理策を追加あるいは削除する機会の②コンピューティングパラダイム・運用環境・オペレーティングモード・産業セクターの外に、特定の情報技術に加えて、法律や規制が要求する事項と併せて、情報システム・ミッション・業務のそれぞれのタイプについて、セキュリティ管理策を適用する上での条件に加えて、セキュリティ管理策の解釈の提示③セキュリティ管理策および拡張管理策において、「指定」ステートメントおよび／または「選択」ステートメントに設定する関係者全体向けのパラメータ値の設定④必要に応じたセキュリティ管理策の補足的ガイダンスの拡張。通常、セキュリティ管理策のベースライン管理策（セクション 3.1 を参照）を当初策定した際に用いた基本的な前提から乖離している場合に、組織は「オーバーレイ」の概念を用いる。反対に、当初策定したベースライン管理策における基本的な前提から乖離していない場合には、オーバーレイを作成する必要性は組織にない可能性がある。ただし、ベースライン管理策は主要な前提を欠いている事もありうる。従って、追加の前提をもってオーバーレイを作成することが正当化される場合もある。

組織は、ベースライン管理策の調整に関する一連の活動を全て各 IT 分野をサポートするベースライン管理策のうち調整されたものを策定するために提供される統制のとれた構造的アプローチのために活用できる。なお、利益関係者間で合意を形成を図る機会を提供するのに加えて、オーバーレイは特定の具体的な状況等や条件を幅広くサポートする情報システムとして

[86] この種の調整は、連邦政府レベルにおいて実施することができる一方、個々の組織による実施も可能である。

[87] 国家安全システムに関連して、CNSS Instruction 1253 は、調整に関するガイダンスについて規定すると同時に、セキュリティ管理策のベースライン管理策について規定している。

組織が有するもののセキュリティ計画を策定する機会を提供する。ちなみに、オーバーレイのカテゴリーのとして有用であると考えられるものには、例えば以下のものがある:

- 保健医療・警察・諜報・財務・運輸・エネルギー等のいずれか若しくはそれらのそれぞれの関連の若しくはそれらのいずれか2つ以上の関連の利害関係者または業界関係者もしくは提携者あるいはパートナー
- クラウドコンピューティング・モバイルシステム・PKI・スマートグリッド・クロスドメインサービス等の情報技術やコンピューティングについて、そのパラダイム
- 空間的な運用環境や戦術上の運用環境
- 産業制御システム・プロセス制御システム・武器システム・シングルユーザシステム・スタンドアロンシステム等の情報システム(オペレーティングモード)のタイプ
- 攻撃対策・初期対応・研究・開発・テスト・評価等、ミッション(および/または業務)のタイプ
- Foreign Intelligence Surveillance Act・Health Insurance Portability and Accountability Act・Privacy Act 等の法律(および/または規制)が要求する事項

オーバーレイの作成に当たって、組織は NIST Special Publication 800-39 において定義されているリスク管理の概念を有効に活用する事ができる。なお、オーバーレイの作成に成功するために関与が必要な者は以下の通り:①オーバーレイを作成するに当たって焦点となる特定の主題領域について理解している情報セキュリティの専門家②オーバーレイの分野における特定の主題に関する専門家で、この文書の付録 F に記載されているセキュリティ管理策に加えて同じくこの文書の付録 D に記載されている当初のベースライン管理策について理解している者。オーバーレイを作成するに当たってのフォーマットと構造は、同じくこの文書の付録 I にて記載されている。

セキュリティ管理策のベースライン管理策の1つに対して、複数のオーバーレイを適用することができる。また、オーバーレイを策定するプロセスの結果調整されたベースライン管理策は、当初ベースライン管理策であったセキュリティ管理策に比べて幾らかは厳格である。なお、リスク評価は、調整されたベースライン管理策を実装する事によって生じるリスクがオーバーレイを作成する組織(または利害関係者)にとって許容可能なリスクの範囲に収まるか否か判断するのに必要な情報を提供するものである。ただし、仮に複数のオーバーレイが利用された場合、オーバーレイの競合が起きる可能性がある。また、仮に複数のオーバーレイを使用する事によりアプリケーションの競合が起きるもしくはセキュリティ管理策が削除されてしまう場合、運用認可責任者(または指定された者)は(ミッション)の責任者および/または(情報の)所有者とともに企業オーナーおよび/または情報スチュワードと協力して競合を解消する事ができる。ちなみに、通常、オーバーレイは、共通の状況等により密接に対応する拡張管理策を含めた管理策の一式および/または共通の条件により密接に対応する拡張管理策を含めた管理策の一式を選択する事によって、組織がベースライン管理策をアドホックに調整する必要を無くしていく事を意図している。ただし、オーバーレイの使用は、組織特有のニーズまたは組織特有の前提条件もしくは組織特有の制約事項を反映する目的で、組織がさらなる調整を行う可能性を排除するものではない。他方で、オーバーレイは、当該オーバーレイに埋め込まれた制約として定義されたものに従って調整され、その際運用認可責任者(または組織が指定した別の個人)による同意や承認が必要となりうる。たとえば、産業用制御システム(ICS)用に作成されたオーバーレイは、特定のタイプの ICS に適用できるよう、なおかつ当該 ICS の運用環境に

適用できるよう、調整が必要になる可能性がある。ただし、オーバーレイを使用することで、特定の組織を適宜調整しなければならない回数が大きく減るのと同時に、調整する範囲が大幅に縮小する事が期待される。

3.4 管理策を選択するプロセスの文書化

組織は、セキュリティ管理策を選択するプロセスのなかで決定された事項をに関連して、合理的な根拠と併せてそれらを文書化する。なお、こうして文書化されたものは、組織の情報システムにおけるセキュリティに関連してミッション（および／または業務）に与えうる影響の観点から考慮する事項について検討する上で不可欠なものである。ちなみに、セキュリティ計画書においては、上記の通り文書化された結果得られたセキュリティ管理策の一式に加えて、セキュリティ管理策を選択するプロセスのなかで行われた決定を裏付ける（情報システムを利用するに当たって組織が課す何らかの制限を含めた）合理的な根拠についても文書化されている。また、組織の情報システムを認可するかどうか情報に基づいて判断する上で必要な情報に運用認可責任者がアクセスできるようにするためには、セキュリティ管理策を選択するプロセスにいてリスク管理に関する重要な決定事項を文書化する事が非常に重要となる[88]。組織の情報システムを認可するかどうか情報に基づいて判断するために必要な情報がなければ、セキュリティ管理策を選択するプロセスにおいて行われるリスク管理に関する重要な決定に関連して情報システムの状態またはシステムの運用環境のいずれかが変化した場合に加えて当初のリスク判断の見直しが行われた場合に当該決定の背景にある認識に加えて当該決定を行う前提となる事項と併せて当該決定を行うに当たって制約となる事項なおかつ当該決定を行う根拠にたどり着く事は、おおよそ望めない。※当初セキュリティ管理策のベースライン管理策を選択したプロセスについては、この文書の 3.2 のセクションに記載されたガイダンスの適用を通じたベースライン管理策の調整と合わせて、図4が要約した通り:

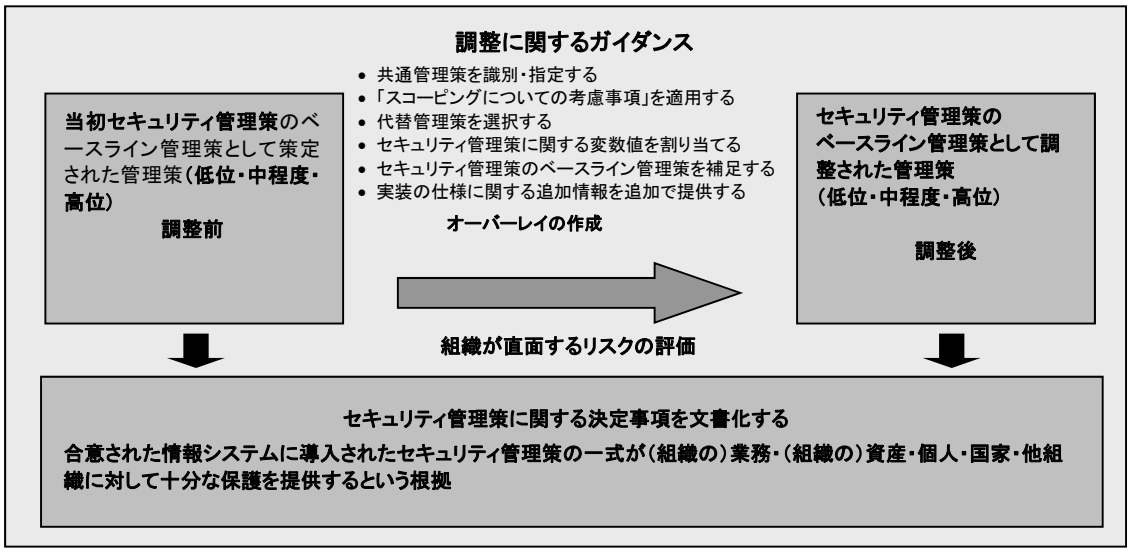


図 4: セキュリティ管理策を選択するプロセス

[88] セキュリティ管理策を選択するプロセスは、共通管理策の提供者に対しても適用されるとともに、組織の内部で展開された共通管理策について認可する判断を行う運用認可責任者に対しても適用される。

セキュリティ管理策の調整が動的にかつ反復して行われる性質について

前記の通りセキュリティ管理策を調整するプロセスは本質的にシーケンシャルであるように見えるものでありながら、反復するという側面も併せ持つ。調整プロセスの各ステップについて、組織は組織のニーズおよびリスク評価から生成された情報の双方を基にいかなる順番で実行してもよい。具体的には、一部の組織は、代替管理策の選択に先立って当初策定されたベースライン管理策におけるセキュリティ管理策に対するパラメータ値を定めてもよい。また、他の組織は、セキュリティ管理策を補足するアクティビィティが完了するまで「指定」・「選択」の両ステートメントを完成させなくてもよい。なお、意図した運用環境に即してセキュリティ管理策を完全に指定する際に、組織が（代替）管理策を追加するしなければならなくなるという問題が浮上する可能性がある。ちなみに、セキュリティ管理策を調整するプロセスは静的ではない。それはすなわち、組織がセキュリティ管理策を現在進めているリスク評価に基づいて適宜繰り返し調整する手順を踏む必要があるを意味する。

セキュリティ管理策を調整するプロセスが動的に反復する性質とは別に、セキュリティ管理策のベースライン管理を追加・削除する際に、副作用が生じる可能性がある。具体的には、この文書の付録 F に記載されたセキュリティ管理策は、他の管理策との間に一定程度依存関係や機能的重複があり、多くの場合、1つのセキュリティ能力を実現するために、複数のセキュリティ管理策が連携するため、セキュリティ管理策を調整するプロセスにおいて特定のセキュリティ管理策をベースライン管理策から削除することで、それ以外の管理策に対して意図せざる副作用（将来的には、負の影響）がもたらされる可能性がある。他方で、新規のセキュリティ管理策によって提供されるセキュリティ能力が他のセキュリティ管理策によって提供されるそれよりも優れている事から、セキュリティ管理策を調整するプロセスにおいて新規のセキュリティ管理策がベースライン管理策として追加される事で、特定のセキュリティ管理策が必要なくなるまたは特定のセキュリティ管理策の必要性が低下する場合がある。たとえば、変化する多様なものとして組織がオペレーティングシステムやアプリケーションをランダムにおよび／または頻繁に展開するために仮想化技術を利用して SC-30(2)を実装アプローチを取った場合、CM-2(2)におけるセキュリティ構成を更新する必要性が少なくなる事が見込まれる。したがって、セキュリティ管理策は組織（または組織の情報システム）における全体的な情報セキュリティニーズの観点から追加または削除されるもので、単なる管理策の追加または管理策の削除とみなす事はできない。

実装に関するヒント

セキュリティ管理策を調整するプロセスの過程でセキュリティ管理策のベースライン管理策から乖離する場合には、組織はセキュリティ管理策とそれらの拡張管理策との多種多様な関連性のうちいくつかの非常に重要なものについて検討する。なお、当該関連性は、ベースライン管理策およびそれらの拡張管理策を選択する過程で捉えられる。ちなみに、これらの関連性は、（この文書においては 3.3 のセクションに加えて付録 I のそれぞれに記載されている）オーバーレイを作成する際に特に重要である。ただし、オーバーレイの作成に当たり、場合によっては、他のセキュリティ管理策やそれらの拡張管理策を欠いたままセキュリティ管理策やその拡張管理策を関連付ける意味のない事がある。必要なセキュリティ能力は、セキュリティ管理策」およびそれらの拡張管理策の全てを通じてもたらされる。なお、セキュリティ管理策とそれらの拡張管理策との多種多様な関連性の中には、AC-3 (3)（必須アクセス管理に関係するセキュリティ管理策の拡張管理策）と AC-16（セキュリティ属性）との間の関連性のように明白なものもある。ただし、それら以外については、セキュリティ機能関係のセキュリティ管理策とセキュリティ保証関係のセキュリティ管理策との関連性についてこの文書の付録 E に記載されているところにおいて顕著なように、より微妙なものとなる可能性がある。たとえば、AC-3 (3)のセキュリティ管理策は、AC-25（参照モニターに関係するセキュリティ管理策）の実装を伴わなければ、特段実装する意味がない。ゆえに、組織は、セキュリティ管理策とそれらの拡張管理策との関連性を容易に特定するするために、セキュリティ管理策の補足的ガイダンスに記載されている「関連する管理策」のセクションに細心の注意を払う事が推奨される。

その他考慮すべき事項

組織によるセキュリティ管理策の調整は、独立したプロセスではない。したがって、セキュリティ管理策の調整については、情報セキュリティに関連して考慮すべき事項に的確に対応するものでありながら、日常的に組織が対処するその他のリスク要因に即したものにする事が重要である。なお、システム運用環境に加えて組織の情報システムの双方に関連してどのセキュリティ管理策を利用するかについて全般的に判断する際には、費用・日程・パフォーマンスなどのリスク要因を考慮する。たとえば、軍の指揮命令システムという人命に関わるシステムに対するセキュリティ管理策は、運用上の必要性とのバランスを取りながら策定される。ちなみに、航空管制システムやコンソールといった航空管制官によって使用されるものに関しては、空域を管理するためにリアルタイムでコンソールにアクセスするニーズがAC-11（セッションロック）に対するセキュリティニーズを上回る。よって、（この文書の3.2のセクションに記載されているものも含めて）セキュリティ管理策を選択するプロセスは、NIST Special Publication 800-39に記載されているように、リスクを全般的に評価するプロセスに組み入れられなければならない。

なお、組織は、スケーラビリティについて勘案しながらセキュリティ管理策を選択する。すなわち、セキュリティ管理策を実装する範囲という意味においても、あるいはセキュリティ管理策の厳密な実装という意味においても、セキュリティ管理策はスケーラブルに実装する事が可能である。なお、スケーラビリティは、それらのセキュリティ管理策が適用される予定の情報システムにおけるセキュリティカテゴリとして FIPS Publication 199 上のものに加えて、当該情報システムにおける影響レベルとして FIPS Publication 200 上のものによって規定される。例えば、実装に関する詳細な情報が著しく多く含まれる事から、影響度が高い情報システムに対する緊急時対応計画は、多分に長くなる可能性がある。反対に、影響度が低いシステムに対する緊急時対応計画においては実装に関する詳細な情報が相対的に少なく、ゆえに当該計画は多分に簡潔になる可能性がある。ちなみに、特定の運用環境におけるスケーラビリティの要素を考慮に入れた上で組織の情報システムにセキュリティ管理策を適用するかどうかは、組織の裁量に属する。また、セキュリティ管理策をシステムに対する影響度に相応しい水準拡張する事によって、リスクベースのセキュリティ管理策をより費用対効果に優れた形で実装できるよう

になる（すなわち、リスクを十分に軽減する事によって十分なセキュリティを確保する上で必要な範囲内に限りリソースを消費するようになる）。

3.5 新規開発システムとレガシーシステム

組織の情報システムに対しては、セキュリティ管理策を選択するプロセスとしてこのセクションに記載されているものを新規開発およびレガシーという異なる 2 つの観点から適用することができる。ただし、未だに存在していない新規開発システムにおいては組織がセキュリティカテゴリを初めて分類するため、セキュリティ管理策を選択するプロセスは、要件定義の観点から適用される。なお、情報システムのセキュリティ計画書に含まれているセキュリティ管理策は、セキュリティ仕様としての役割を果たしながら、システム開発ライフサイクルにおいては開発フェーズおよび実装フェーズのなかでシステムに組み込まれる見込みとなっている。反対に、レガシー情報システムにおいては、システムに対する大きな変更が組織に織り込み済みの場合（例：修正またはアウトソーシング若しくは主要なアップグレード）、セキュリティ管理策を選択するプロセスについてはギャップ分析の観点から適用される。ちなみに、既存の情報システムである事から、いかなる状況下にあであっても、組織はセキュリティ管理策を選択するプロセスに加えてセキュリティ分類プロセスを完了させている。その結果、対応するセキュリティ計画書上にセキュリティ管理策として事前に合意済のものが策定され、なおかつ情報システムに当該セキュリティ管理策が実装される。このため、ギャップ分析を以下の通り応用する事が可能である：

① 現在情報システムによって処理・保存・伝送のいずれかがなされている情報のタイプに基づいて、情報システムにおけるセキュリティカテゴリ（および情報システムに与える影響度）を必要に応じて再確認または更新する。

② セキュリティカテゴリおよび情報システムに与える影響度に対する何らかの更新についてのみならず、組織またはミッションプロセスあるいは業務プロセスもしくは情報システムないしシステム運用環境に対する何らかの変更について考慮しながら、現在導入されているセキュリティ管理策について記載している既存のセキュリティ計画書について見直しを行う。さらに、情報システム上必要となる事が見込まれる何らかのセキュリティ管理策として（組織の）業務または（組織の）資産もしくは個人あるいは（他の）組織ないし国家に対するリスクが決して許容範囲を越える事が無いよう追加で策定されたものを文書化することを含めて、リスクを再評価のうえ、必要に応じてセキュリティ計画書を修正する。

③ 更新されたセキュリティ計画書上記載されているセキュリティ管理策をする。また、行動計画およびマイルストーンに実装されていないの管理策がある場合、それらを記載~~し~~する。さらに、リスクマネジメントフレームワークにおけるステップのうち残りのものについて、新規開発システムの場合と同じように継続する。

外部サービスプロバイダにギャップ分析を応用する

ギャップ分析は、外部のサービスプロバイダと情報をやりとりする際にも適用される。この文書のセクション 2.5 に記載されている通り、組織は情報システムサービスに関して外部のサービスプロバイダにより一層依存するようになっている。ゆえに、いずれもリスクマネジメントフレームワークに記載されたセキュリティを分類するステップおよびセキュリティ管理策を選択するステップの実施を外部プロバイダに対して義務付けるに当たり、組織は調達プロセスと併せて適切なビークルとしての契約を上記の通り応用されたギャップ分析を用いる事によって効果的

に使用する事ができる。また、組織が調達プロセスと併せて適切なビークルとしての契約を効果的に使用する事ができた結果として得られる情報は、今後提供される情報システムサービスにおいて外部プロバイダが実装しているセキュリティ管理策とは何か（または外部プロバイダが実装しようとするセキュリティ管理策とは何か）についての判断に役立てる事ができる。なお、セキュリティ管理策が不十分である場合、外部の情報システムサービスを使用する事により生じる許容不可能なリスクを十分に軽減する責任は運用認可責任者に残る。ただし、以下を通じて、組織は自身が直面するリスクを許容可能な水準まで軽減する事ができる：

- 既存のビークルとしての契約を利用する事によって、組織が策定した（セキュリティ管理策の）追加要求事項を充足するよう外部プロバイダに対して義務付けること
- 既存のビークルとしての契約が組織によって策定された（セキュリティ管理策の）追加要求事項について規定してない場合に、セキュリティ管理策が追加されるよう外部プロバイダと交渉すること
- 外部プロバイダが補完的管理策の利用について許可すること
- 契約が存在しないまたは契約が必要なセキュリティ管理策を策定する上で不可欠な力を組織に与えない場合に、組織の情報システムにおいて契約に代わってリスク軽減措置[89]を講じること

導入に関するヒント

多くの組織は、通常「システムオブシステムズ」と呼ばれる複雑な情報システムを維持・運用している。なお、これらのシステムオブシステムズと呼ばれるタイプの情報システムに関連してセキュリティ管理策を選択するプロセスにおいてエンタープライズアーキテクチャは重要不可欠な役割を担っている。また、組織は、システムオブシステムズを 2 つ以上のサブシステムに分割のうえ各サブシステムに対して FIPS 199 において規定されたセキュリティカテゴリと併せて FIPS 200 において規定された影響度を適用する事によってシステムオブシステムズにおける複雑な問題に対応する事が可能である。ただし、個別のサブシステムにそれぞれ異なる影響度を適用する事によって、システムオブシステムズと呼ばれるタイプの情報システムが与える全般的な影響度を変える事なく影響度のより高いセキュリティ管理策を横断的に展開する事なく当該システムを構成する全てのサブシステムに対してにセキュリティ管理策を個別に割り当てることが可能になる。なお、システムオブシステムズを構成する各サブシステムは独立して相互に接続されているため、サブシステムを完全に独立したエンティティとして扱うのは適切ではない。

組織は、そのシステム内にある重要な境界で通信を監視・制御する事も含めて、システムオブシステムズを構成する各サブシステムにセキュリティ管理策を適用するためにセキュリティアーキテクチャを策定する。加えて、システムオブシステムズの全体にわたるセキュリティ管理策として当該システムを構成する各サブシステム（このセキュリティ管理策が規定する情報セキュリティ能力を継承したもの）が与える最も大きな影響に見合うもしくは以上のものを提供するためにも、組織はセキュリティアーキテクチャを策定する。複雑なシステム内において複製されたサブシステムが共通の脅威によって悪用されるという共通の脆弱性が明らかとなりうる事から、組織はリスク軽減措置として信じられてきたであろう冗長性が無効になる可能性について考慮する。なお、システムオブシステムズを構成するサブシステムの１つについて起きたセキュリティインシデントがもたらした影響は、一度に多くのサブシステムに大きな影響を与える可能性がある。

[89] たとえば、ギャップ分析によって特定されたリスクを軽減する代替措置として、組織は（局所的な）政策・手順・代替管理策のすべて（またはそれらのいずれか）を策定することができる。

付録 A

参考文献

法律・政策・指令・規制・覚書・標準・指針

法律・大統領命令
1. 「連邦電子政府法」(E-Government Act) [includes FISMA] (P.L. 107-347), 2002 年 12 月.
2. 「連邦政府情報セキュリティ法」(Federal Information Security Management Act) I (P.L. 107-347, Title III), 2002 年 12 月.
3. Paperwork Reduction Act (P.L. 104-13), 1995 年 5 月.
4. 米国愛国者法(USA PATRIOT Act) (P.L. 107-56), 2001 年 10 月.
5. Privacy Act of 1974 連邦プライバシー法 (P.L. 93-579), 1974 年 12 月.
6. Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996.
7. Health Insurance Portability and Accountability Act (P.L. 104-191), 1996 年 8 月.
8. The Atomic Energy Act of 1954 連邦エネルギー法 (P.L. 83-703), 1954 年 8 月.
9. Executive Order 13556, Controlled Unclassified Information, 2010 年 11 月.
10. Executive Order 13587, Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 2011 年 10 月.

政策・指令・指示・規制・覚書
1. Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, 2012 年 11 月.
2. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106, *Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106).
3. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R. 930.301-305).
4. Committee on National Security Systems Policy (CNSSP) No. 11, *National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products*, 2003 年 7 月.
5. Committee on National Security Systems Policy (CNSSP) No. 12, *National Information Assurance Policy for Space Systems Used to Support National Security Missions*, 2007 年 3 月.
6. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, 2010 年 4 月.

7. Committee on National Security Systems (CNSS) Instruction 1253, Version 2, *Security Categorization and Control Selection for National Security Systems,* 2012 年 3 月.

8. Committee on National Security Systems Directive (CNSSD) No. 504, *Directive on Protecting National Security Systems from Insider Threat*, 2012 年 1 月.

9. Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)*, 2009 年.

10. Intelligence Community Directive (ICD) 705, *Sensitive Compartmented Information Facilities*, 2010 年 5 月.

11. Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, 2008 年 2 月.

12. Executive Office of the President of the United States and Federal CIO Council, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, 2011 年 12 月.

13. Homeland Security Presidential Directive 7,大統領命令 *Critical Infrastructure Identification, Prioritization, and Protection*, 2003 年 12 月.

14. Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, 大統領命令 2004 年 8 月.

15. Homeland Security Presidential Directive 20 (National Security Presidential Directive 51), *National Continuity Policy*, 大統領命令 2007 年 5 月.

16. Intelligence Community Directive Number 704, *Personnel Security Standards and Procedures Governing Eligibility For Access To Sensitive Compartmented Information And Other Controlled Access Program Information,* 大統領命令 2008 年 10 月.

17. National Communications System (NCS) Directive 3-10, *Minimum Requirements for Continuity Communications Capabilities*, 2007 年 7 月.

18. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, 1996 年 12 月.

19. Office of Management and Budget Circular 覚書 A-130, 付録 III, Transmittal Memorandum #4, *Management of Federal Information Resources*, 2000 年 11 月.

20. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *FEA Consolidated Reference Model Document*, Version 2.3, 2007 年 10 月.

21. Office of Management and Budget, *Federal Segment Architecture Methodology (FSAM)*, 2009 年 1 月.

22. Office of Management and Budget Memorandum 01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, 2000 年 12 月.

23. Office of Management and Budget Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, 2001 年 10 月.

24. Office of Management and Budget Memorandum 03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, 2003 年 8 月.

25. Office of Management and Budget Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, 2003 年 9 月.

26. Office of Management and Budget Memorandum 04-04, *E-Authentication Guidance for Federal Agencies*, 2003 年 12 月.

27. Office of Management and Budget Memorandum 04-26, *Personal Use Policies and File Sharing Technology*, 2004 年 9 月.

28. Office of Management and Budget Memorandum 05-08, *Designation of Senior Agency Officials for Privacy*, 2005 年 2 月.

29. Office of Management and Budget Memorandum 05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, 2005 年 8 月.

30. Office of Management and Budget Memorandum 06-15, *Safeguarding Personally Identifiable Information*, 2006 年 5 月.

31. Office of Management and Budget Memorandum 06-16, *Protection of Sensitive Information*, 2006 年 6 月.

32. Office of Management and Budget Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, 2006 年 7 月.

33. Office of Management and Budget Memorandum, *Recommendations for Identity Theft Related Data Breach Notification Guidance*, 2006 年 9 月.

34. Office of Management and Budget Memorandum 07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, 2007 年 3 月.

35. Office of Management and Budget Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, 2007 年 5 月.

36. Office of Management and Budget Memorandum 07-18, *Ensuring New Acquisitions Include Common Security Configurations*, 2007 年 6 月.

37. Office of Management and Budget Memorandum 08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, 2008 年 8 月.

38. Office of Management and Budget Memorandum 08-23, *Securing the Federal Government's Domain Name System Infrastructure*, 2008 年 8 月.

39. The White House, Office of the Press Secretary, *Designation and Sharing of Controlled Unclassified Information (CUI)*, 2008 年 5 月.

40. The White House, Office of the Press Secretary, *Classified Information and Controlled Unclassified Information*, 2009 年 5 月.

41. Office of Management and Budget Memorandum 11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors*, 2011 年 2 月.

42. Office of Management and Budget Memorandum, *Requirements for Accepting Externally-Issued Identity Credentials*, 2011 年 10 月.

43. Office of Management and Budget Memorandum 11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, 2011 年 9 月.

標準

1. International Organization for Standardization/International Electrotechnical Commission 27001:2005, *Security techniques -- Information security management systems -- Requirements*.

2. International Organization for Standardization/International Electrotechnical Commission 15408-1:2009, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model.*

3. International Organization for Standardization (ISO)/International Electrotechnical Commission ()15408-2:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements*.

4. International Organization for Standardization/International Electrotechnical Commission 15408-3:2008, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*.

5. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, 2001 年 5 月.
National Institute of Standards and Technology Federal Information Processing Standards Publication 140-3 (Draft), *Security Requirements for Cryptographic Modules*, 2009 年 12 月.

6. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-4, *Secure Hash Standard (SHS)*, 2012 年 3 月.

7. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3, *Digital Signature Standard (DSS)*, 2009 年 6 月.

8. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Label for Information Transfer*, 1994 年 9 月.

9. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, 1994 年 9 月.

10. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, 2001 年 11 月.

11. National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, 2008 年 7 月.

12. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, 2004 年 2 月.

13. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, 2006 年 3 月.

14. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, 2006 年 3 月.

指針・省庁間共同報告

1. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, 1995 年 10 月.

2. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, 1995 年 10 月.

3. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 1996 年 9 月.

4. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC)*, Version 1, 1998 年 1 月.

5. National Institute of Standards and Technology Special Publication 800-16, *Information Security Training Requirements: A Role- and Performance-Based Model*, 1998 年 4 月.

6. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, 1998 年 2 月.

7. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, 2006 年 2 月.

8. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, 1999 年 10 月.

9. National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)*: *Requirements and Procedures*, 1999 年 10 月.

10. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, 2005 年 12 月.

11. National Institute of Standards and Technology Special Publication 800-22, Revision 1a, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, 2010 年 4 月.

12. National Institute of Standards and Technology Special Publication 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, 2000 年 8 月.

13. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, 2000 年 8 月.

14. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, 2000 年 10 月.

15. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, 2004 年 6 月.

16. National Institute of Standards and Technology Special Publication 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, 2008 年 3 月.

17. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, 2001 年 6 月.

18. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, 2012 年 9 月.

19. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, 2001 年 2 月.

20. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, 2001 年 12 月.

21. National Institute of Standards and Technology Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, 2010 年 5 月.

22. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, 2003 年 10 月.

23. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, 2003 年 10 月.

24. National Institute of Standards and Technology (NIST) Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, 2010 年 2 月.

25. National Institute of Standards and Technology (NIST) Special Publication 800-38A—Addendum, *Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode*, 2010 年 10 月.

26. National Institute of Standards and Technology (NIST) Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, 2005 年 5 月.

27. National Institute of Standards and Technology (NIST) Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, 2004 年 5 月.

28. National Institute of Standards and Technology (NIST) Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*, 2007 年 11 月.

29. National Institute of Standards and Technology(NIST) Special Publication 800-38E, *Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices*, 2010 年 1 月.

30. National Institute of Standards and Technology (NIST) Special Publication 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, 2012 年 12 月.

31. National Institute of Standards and Technology (NIST) Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, 2011 年 3 月.

32. National Institute of Standards and Technology (NIST) Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, 2005 年 11 月.

33. National Institute of Standards and Technology (NIST) Special Publication 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, 2009 年 9 月.

34. National Institute of Standards and Technology (NIST) Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional System*, 2002 年 11 月.

35. National Institute of Standards and Technology Special (NIST) Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, 2007 年 9 月.

36. National Institute of Standards and Technology (NIST) Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, 2007 年 2 月.

37. National Institute of Standards and Technology (NIST) Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, 2009 年 6 月.

38. National Institute of Standards and Technology (NIST) Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, 2002 年 8 月.

39. National Institute of Standards and Technology (NIST) Special Publication 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, 2008 年 7 月.

40. National Institute of Standards and Technology (NIST) Special Publication 800-49, *Federal S/MIME V3 Client Profile*, 2002 年 11 月.

41. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, 2003 年 10 月.

42. National Institute of Standards and Technology (NIST) Special Publication 800-51, Revision 1, *Guide to Using Vulnerability Naming Schemes*, 2011 年 2 月.

43. National Institute of Standards and Technology (NIST) Special Publication 800-52, Revision 1 (Draft), Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, 2013 年 9 月.

44. National Institute of Standards and Technology (NIST) Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, 2010 年 6 月.

45. National Institute of Standards and Technology (NIST) Special Publication 800-54, *Border Gateway Protocol Security*, 2007 年 7 月.

46. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, 2008 年 7 月.

47. National Institute of Standards and Technology (NIST) Special Publication 800-56A (Revised), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, 2007 年 3 月.

48. National Institute of Standards and Technology (NIST) Special Publication 800-57 Revision 3, *Recommendation for Key Management*, 2012 年 7 月.

49. National Institute of Standards and Technology (NIST) Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, 2005 年 1 月.

50. National Institute of Standards and Technology (NIST) Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, 2003 年 8 月.

51. National Institute of Standards and Technology (NIST) Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, 2008 年 8 月.

52. National Institute of Standards and Technology (NIST) Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, 2012 年 8 月.

53. National Institute of Standards and Technology (NIST) Special Publication 800-63-1, *Electronic Authentication Guideline*, 2011 年 12 月.

54. National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, 2008 年 10 月.

55. National Institute of Standards and Technology Special Publication 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, 2005 年 1 月.

56. National Institute of Standards and Technology Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, 2008 年 10 月.

57. National Institute of Standards and Technology (NIST) Special Publication 800-67, Revision 1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, 2012 年 1 月.

58. National Institute of Standards and Technology (NIST) Special Publication 800-68, Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, 2008 年 10 月.

59. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, 2006 年 9 月.

60. National Institute of Standards and Technology Special Publication 800-70, Revision 2, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, 2011 年 2 月.

61. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, 2004 年 11 月.

62. National Institute of Standards and Technology Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, 2010 年 2 月.

63. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, 2007 年 1 月.

64. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, 2005 年 12 月.

65. National Institute of Standards and Technology Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification (PIV)*, 2010 年 12 月.

66. National Institute of Standards and Technology Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, 2008 年 6 月.

67. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, Revision 1, 2010 年 4 月.

68. National Institute of Standards and Technology Special Publication 800-82, Revision 1, *Guide to Industrial Control Systems (ICS) Security*, 2013 年 4 月.

69. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, 2005 年 11 月.

70. National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, 2006 年 9 月.

71. National Institute of Standards and Technology Special Publication 800-85A-2, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-3 Compliance)*, 2010 年 7 月.

72. National Institute of Standards and Technology Special Publication 800-85B-1, (Draft) *PIV Data Model Test Guidelines*, 2009 年 9 月.

73. National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, 2006 年 8 月.

74. National Institute of Standards and Technology Special Publication 800-87, Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, 2008 年 4 月.

75. National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, 2006 年 9 月.

76. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, 2006 年 11 月.

77. National Institute of Standards and Technology Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, 2012 年 1 月.

78. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, 2006 年 9 月.

79. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, 2007 年 2 月.

80. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, 2007 年 8 月.

81. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines*, 2006 年 9 月.

82. National Institute of Standards and Technology Special Publication 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i*, 2007 年 2 月.

83. National Institute of Standards and Technology Special Publication 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, 2007 年 4 月.

84. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, 2006 年 10 月.

85. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics*, 2007 年 5 月.

86. National Institute of Standards and Technology Special Publication 800-103 (Draft), *An Ontology of Identity Credentials, Part I: Background and Formulation*, 2006 年 10 月.

87. National Institute of Standards and Technology Special Publication 800-104, *A Scheme for PIV Visual Card Topography*, 2007 年 6 月.

88. National Institute of Standards and Technology Special Publication 800-106, *Randomized Hashing Digital Signatures*, 2009 年 2 月.

89. National Institute of Standards and Technology Special Publication 800-107, *Recommendation for Applications Using Approved Hash Algorithms*, 2012 年 8 月.

90. National Institute of Standards and Technology Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, 2009 年 10 月.

91. National Institute of Standards and Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, 2007 年 11 月.

92. National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, 2008 年 7 月.

93. National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, 2007 年 11 月.

94. National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, 2008 年 9 月.

95. National Institute of Standards and Technology Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, 2008 年 11 月.

96. National Institute of Standards and Technology Special Publication 800-117, Version 1.0, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, 2010 年 7 月.

97. National Institute of Standards and Technology Special Publication 800-118 (Draft), *Guide to Enterprise Password Management*, 2009 年 4 月.

98. National Institute of Standards and Technology Special Publication 800-121, Revision 1, *Guide to Bluetooth Security*, 2012 年 6 月.

99. National Institute of Standards and Technology Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010 年 4 月.

100. National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, 2008 年 7 月.

101. National Institute of Standards and Technology Special Publication 800-124, *Guidelines on Cell Phone and PDA Security*, 2008 年 10 月.

102. National Institute of Standards and Technology Special Publication 800-125, *Guide to Security for Full Virtualization Technologies*, 2011 年 1 月.

103. National Institute of Standards and Technology Special Publication 800-126, Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, 2011 年 9 月.

104. National Institute of Standards and Technology Special Publication 800-127, *Guide to Securing WiMAX Wireless Communications*, 2010 年 9 月.

105. National Institute of Standards and Technology Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, 2011 年 8 月.

106. National Institute of Standards and Technology Special Publication 800-133, *Recommendation for Cryptographic Key Generation*, 2012 年 12 月.

107. National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, 2011 年 9 月.

108. National Institute of Standards and Technology Special Publication 800-142, *Practical Combinatorial Testing*, 2010 年 10 月.

109. National Institute of Standards and Technology Special Publication 800-144, *Guidelines for Security and Privacy in Public Cloud Computing*, 2011 年 12 月.

110. National Institute of Standards and Technology Special Publication 800-145, *The NIST Definition of Cloud Computing*, 2011 年 9 月.

111. National Institute of Standards and Technology Special Publication 800-146, *Cloud Computing Synopsis and Recommendations*, 2012 年 5 月.

112. National Institute of Standards and Technology Special Publication 800-147, *Basic Input/Output System (BIOS) Protection Guidelines*, 2011 年 4 月.

113. National Institute of Standards and Technology Special Publication 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, 2011 年 9 月.

114. National Institute of Standards and Technology Interagency Report 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, 2012 年 10 月.

付録 B

用語集

一般的な用語と定義

この付録 B は、Special Publication 800-53 内で使用されているセキュリティ用語の定義を示す付録である。この文書で使用されているすべての用語は、この用語集で定義されているものを除き、CNSS Instruction 4009（国家安全保障システム委員会の指示 4009）『*National Information Assurance Glossary*（国家情報保証に関する用語集）』に含まれる定義と一致する。

十分なセキュリティ (Adequate Security) [OMB Circular A-130, Appendix III, Adapted]	情報の消失・誤用・悪用・情報への不正なアクセスもしくは情報の改ざんがもたらすリスクに見合うセキュリティ。
APT (Advanced Persistent Threat)	複数の攻撃ベクトル（例：サイバー、物理的、および詐欺）を使用して自身の目的を達成する機会を創出するための、高度な専門知識と十分なリソースを有する敵対者。それらの目的は、通常、標的となる組織の IT インフラ内に足場を確立・拡張し、情報を盗む、またはミッション、計画、もしくは組織の極めて重要な側面を損なわせる（または妨げる）あるいは将来にわたってそれらの目的を果たせる立場に自身を置くことを含む。なお、APT は：①長期にわたって執拗に自身の目的を追求する②抵抗しようとする防衛者側の取り組みに順応するならびに③自身の目的を果たすのに必要なレベルの情報のやりとりを維持しようとする。
政府機関 (Agency)	＜執行機関 (*Executive Agency*)＞を参照。
オール・ソース・インテリジェンス (All Source Intelligence) [Department of Defense, Joint Publication 1-02]	多分に人による諜報、画像分析、科学分析、無線諜報、ならびに情報検証していくなかで収集したオープンソースデータといったあらゆる情報源を統合するためのすべての製品および／または組織と活動を指す。
アセスメント (Assessment)	＜セキュリティ管理策アセスメント (*Security Control Assessment*)＞を参照。
アセサー (Assessor)	＜セキュリティ管理策評価者 (*Security Control Assessor*)＞を参照。
保証 (Assurance) [CNSSI 4009]	情報システムのセキュリティ機能・セキュリティ慣行・セキュリティ手順・セキュリティアーキテクチャのそれぞれについて、セキュリティポリシーセキュリティポリシーと関連付けて正確に適用していることへの一定の信頼。

保証ケース (Assurance Case) [Software Engineering Institute, Carnegie Mellon University]	情報システムにおいてある特定の品質特性に関する具体的な主張が裏付けられていることを示す、体系的な議論を伴ったエビデンス。
監査ログ (Audit Log) [CNSSI 4009]	情報システム活動の発生順の記録で、所定の期間内におけるシステムに対するアクセスと操作を含むもの。
監査記録 (Audit Record)	監査ログ内における一つ一つの項目で、監査されたイベントに関連するもの。
監査軽減ツール (Audit Reduction Tools) [CNSSI 4009]	担当者によるレビューを容易にする目的のもと、監査記録の量を減らすように設計された前処理プログラム。このツールを使用すれば、セキュリティレビューの前に、セキュリティ上重要でないことが確認されている多くの監査記録を取り除くことができる。これらのツールは、通常、夜間のバックアップによって生成されたものなどの、特定の種類のイベントによって生成された監査記録を取り除く。
監査証跡 (Audit Trail) [CNSSI 4009]	開始から最終結果を得るまでのセキュリティ関連のトランザクションにおける特定のオペレーション、手続き、またはイベントに関連する、あるいはそれらにつながる一連の活動を再現し検証するための発生順の記録。
認証 (Authentication) [FIPS 200]	通常は情報システム内のリソースに対するアクセスを許可するための必要条件として、ユーザ、プロセス、または機器を識別すること。
オーセンティケータ (Authenticator)	ユーザ・プロセッサ・機器のいずれかを識別するために用いられる手段（例：利用者パスワードまたはトークン）
真正性 (Authenticity)	本物であると同時にそのことが信頼のもとで確認可能なことを示す特性や、トランスミッション、メッセージ、またはメッセージ発信者の正しさに対する信頼。＜認証 (*Authentication*)＞を参照。
運用認可 (Authorization (to operate))	組織の高官による正式な経営判断で、情報システムの運用を認可し、合意されたセキュリティ管理策を導入したうえで（組織の）業務・（組織の）ミッション・機能・イメージ（または評判）・（組織の）資産・個人・他組織・国家に対するリスクを明示的に許容するもの。
認可を出す範囲 (Authorization Boundary)	運用認可責任者によってその運用が認可されるべき情報システム（ただし、その情報システムが接続しているシステムであっても、個別に運用認可を受けたものは含まない）の、すべてのコンポーネント。

認可処理 (Authorize Processing)	＜運用認可(*Authorization*)＞を参照。
運用認可責任者 (Authorizing Official)	（組織の）業務・ミッション・機能・イメージ・評判・資産・個人・他組織・国家のそれぞれに対するリスクを許容範囲内に収める形で、情報システムの運用する責任を公式に負う（連邦）政府機関の高官。
可用性 (Availability) [44 U.S.C., Sec. 3542]	情報へのタイムリーで確かなアクセスと利用の確保。
ベースライン構成 (Baseline Configuration)	情報システムの仕様を文書化したもの、またはシステム内の設定構成項目の1つ。所定の時点で正式にレビューされ合意がなされたものであり、変更制御手順を介してのみ変更が可能である。
ブラックリストの作成 (Blacklisting)	以下を識別するのに用いられるプロセス：①ある情報システム上で実行することが許可されていないソフトウェアプログラム;あるいは②（アクセスが）許可されていない URL／ウェブサイト。
境界保護 (Boundary Protection)	境界保護装置（例：ゲートウェイ、ルーター、ファイアウォール、ガード、暗号化トンネル）の利用により、情報システムの外部境界において通信をモニタリング・制御し、悪意のある通信またはその他の不正な通信を検出し、阻止すること。
境界保護装置 (Boundary Protection Device)	以下を実現するための適切なメカニズムを備えた装置:①相互接続された異なるシステムのそれぞれに対するセキュリティポリシーの策定を容易にすること（例：相互接続されたシステムへの入力情報と、そのシステムからの出力情報の流れを制御する）および／または②情報システム境界保護を提供すること。
一元的管理 (Central Management)	選択されたセキュリティ管理策とそれに関連するプロセスを、組織全体にわたり管理・実装すること。一元的管理には、組織が定めた中央集権型のセキュリティ管理策とプロセスを策定・導入・評価・認可・モニタリングすることが含まれる。

最高情報責任者 (Chief Information Officer) [PL 104-106, Sec. 5125(b)]	以下の項目に責任のある、政府機関の職員: (i) 法律・大統領命令・指令・施策・規制(または政府機関の長)によって定められた優先順位に基づいた方法で情報技術が調達され、情報資源が管理されていることを確実にするために、政府機関の長や他の上級管理職に対して助言や様々な支援を提供すること。 (ii) 政府機関用の合理的な統合情報技術アーキテクチャを開発(または保守もしくは導入促進)すること。 (iii) 政府機関のすべての主要な情報資源管理プロセスに関して、効果的かつ効率的な設計および運用を促進する。この活動には、政府機関の作業プロセスの向上も含まれる。 注:連邦政府機関の下部組織では、政府機関レベルの最高情報責任者が担うセキュリティ上の責任と類似の責務を担う個人を示す用語として、「最高情報責任者」を用いる場合がある。
最高情報セキュリティ責任者 (Chief Information Security Officer)	<政府機関における上位の情報セキュリティ責任者 (*Senior Agency Information Security Officer*)>を参照。
最高プライバシー責任者 (Chief Privacy Officer)	<政府機関における上位のプライバシー責任者 (*Senior Agency Official for Privacy*)>を参照。
機密情報 (Classified Information)	機密情報とは、①大統領命令第13526号によって改定された大統領命令第12958 号等の旧命令に準拠して、国家安全保障に関わる機密の情報であると判断された情報あるいは②1954年に施行されたAtomic Energy Act(原子力法)(改正法を含む)に準拠して、Restricted Data(秘密のデータ)であると判断された情報。
汎用サービス (Commodity Service)	通常は、多様な大勢の消費者を対象にサービス提供事業者によって提供される情報システムサービス(例: 通信サービス)を指す。なお、汎用サービスを購入する、および/または受ける組織にとって、情報システムサービスの提供事業者の運営システムや運用は不透明なものである。組織が、プロバイダとの間でサービス品質の保証内容について交渉できる場合もあるが、通常はサービス提供事業者に対して、特定のセキュリティ管理策の導入を課す立場にない。
一般通信事業者 (Common Carrier)	電気通信の分野で、一般の人々に対して、有料で通信(伝送)サービスを提供する業者。 注:アメリカでは、このような事業者は、通常、連邦政府または州の規制委員会が定める規制の対象となる。

共通管理策 (Common Control) [NIST SP 800-37・CNSSI 4009]	組織のセキュリティ管理策のうち、単一または複数の情報システム継承が可能な管理策。＜セキュリティ管理策の継承 *(Security* Control *Inheritance)*＞を参照。
共通管理策の提供者 (Common Control Provider) [NIST SP 800-37]	共通管理策（すなわち、複数の情報システムによる継承が可能なセキュリティ管理策）を策定・導入・評価・モニタリングすることに責任を持つ組織の職員。
コモンクライテリア (Common Criteria) [CNSSI 4009]	製品やシステムについて、そのセキュリティ機能や保証要求事項を包括的かつ厳密に規定する主要な文書。
一般的なセキュアな設定構成 (Common Secure Configuration)	所定のITプラットフォームに対する具体的なセキュアな設定について規定する、標準化されなおかつ確立された、広く認められているベンチマーク。
補完的セキュリティ管理策 (Compensating Security Controls) [CNSSI 4009, Adapted]	NIST Special Publication 800-53 および CNSS Instruction 1253 に記載されているセキュリティ管理策ベースラインにおいて推奨されるセキュリティ管理策の代わりに採用されたセキュリティ管理策であり、情報システムまたは組織に対して推奨管理策と同等の（または匹敵する）保護を提供する。
コンピュータマッチング契約 (Computer Matching Agreement)	コンピュータマッチングプログラムに関する契約であり、1988 年に制定された Computer Matching and Privacy Protection Act の規定に従って、プログラムに関与する組織によって締結される。一部の例外はあるものの、コンピュータマッチングプログラムとは、任意の 2 つ以上の自動化された記録システム同士をコンピュータによって比較したもの、あるいは連邦政府の補助金制度のもとで行われる現金（または現物支給もしくは払込）に関連して、サービスの申請者またはサービスの受給者もしくはサービスの受益者（または参加者もしくはサービスの提供者）が法規制上の要件を適宜継続的に満たす目的のもとで（または法規制上の要件を適宜継続的に満たしているかどうかを確認する目的のもとで）連邦政府所有のものではない記録を扱うシステムである。なお、コンピュータマッチングプログラムとは、連邦政府の職員または給与に関する記録を扱う 2 つ以上の自動化された記録システム同士をコンピュータによって比較したもの、あるいは連邦政府の職員または給与に関する連邦政府の職員または給与に関する連邦政府所有のものではない記録を扱うシステムでもありうる。
機密性 (Confidentiality) [44 U.S.C., Sec. 3542]	個人のプライバシー情報や専有情報の保護手段等、情報へのアクセスや開示を公式に規制する状態。

構成変更の管理 (Configuration Control) [CNSSI 4009]	情報システムの導入前、導入時、および導入後にその情報システムを不適切な変更から保護することを目的として、ハードウェア、ファームウェア、ソフトウェア、およびドキュメントに対する変更を管理する過程。
構成項目 (Configuration Item)	構成管理の対象として指定された、情報システムコンポーネントの集合。構成管理プロセスにおいて単一のエンティティとして扱われる。
構成管理 (Configuration Management)	IT 製品と情報システムの一体性を確立・維持することに重きを置いた一連の活動であり、システム開発ライフサイクル全体を通じてIT製品と情報システムの双方の構成について初期化、変更、モニタリングの一連のプロセスを管理する。
設定された構成 (Configuration Settings)	ハードウェア・ソフトウェア・ファームウェアのいずれかのパラメータの集合。変更が可能であるが、その場合、情報システムのセキュリティについて、その状態および／または機能性に影響を与える。
管理された領域 (Controlled Area)	規定された要求事項が十分に満たされるよう物理的・手続的の両面において情報や情報システムの保護が提供される、組織胸を張っている領域または空間。
制御されたインターフェース (Controlled Interface) [CNSSI 4009]	セキュリティポリシーを強制のうえ相互接続されている情報システム間の情報の流れを制御する一連のメカニズムの境界線。
管理されている非機密扱いの情報 (Controlled Unclassified Information) [E.O. 13556]	大統領命令第 12958 号（改正令を含む）が規定する National Security Classification の基準を満たさない非機密情報として分類されたもので、①アメリカ合衆国の国益または米連邦政府以外の関係者の重要な利益に関連し、かつ②法律または政策に則って、不正な開示からの保護、特殊な取扱いによる保護、情報の交換または発信に対する所定の制限が必要となる情報である。
対策 (Countermeasures) [CNSSI 4009]	情報システムの脆弱性を軽減するために行われる対策として、活動、手段、手順、技術、対策。セキュリティ管理策(security controls)および保護手段(safeguards)と同義。
隠れチャネル解析 (Covert Channel Analysis) [CNSSI 4009]	セキュリティポリシーモデルと、それに関連して記述された低レベルプログラムが、情報への不正アクセスをどの程度まで許してしまうかを特定すること。
隠れストレージチャネル (Covert Storage Channel) [CNSSI 4009]	ある特定のプロセスによって記憶場所へ直接的／間接的なに書き込まれ、別のプロセスによって記憶場所から直接的／間接的に読み出される隠れチャネル。隠れストレージチャネルは、通常、異なるセキュリティレベルを有する 2 つのサブジェクトによって共有される、限られたリソース（例：ディスク上のセクター）を含む。

隠れタイミングチャネル (Covert Timing Channel) [CNSSI 4009]	あるプロセスから別のプロセスに情報をが伝わる隠れチャネル。その際、前者のプロセスはシステムリソースの利用（例：CPU 時間）を調整するが、これにより後者のプロセスによって観測される実際の応答時間が変わってくる。
クロスドメイン・ソリューション (Cross Domain Solution) [CNSSI 4009]	管理されたインターフェースの一形態。手動および／または自動による、異なるセキュリティドメイン間での情報のアクセスおよび／または転送を可能にする。
サイバー攻撃 (Cyber Attack) [CNSSI 4009]	サイバー空間を介した攻撃。コンピュータ環境／インフラの途絶、機能停止、破壊を引き起こしたり、それらを不当に制御するために、あるいはそのデータの完全性を損なわせたり、管理されている情報を盗む目的で、企業がサイバー空間を活用する企業を狙う。
サイバーセキュリティ (Cyber Security) [CNSSI 4009]	サイバー攻撃からサイバー空間を保護または防御すること。
サイバー空間 (Cyberspace) [CNSSI 4009]	インターネット、電気通信網、コンピュータシステム、組み込み式プロセッサおよびコントローラを含む、ネットワークでつながっていて相互に関係しあうする情報システムインフラによって構成される、情報環境内の世界的規模のドメイン。
データマイニング／データ取得 (Data Mining/Harvesting)	データまたはナレッジの発見を目的として、大規模なデータセット内の相互関係またはパターンの特定を試みる分析プロセス。
広域防御 (Defense-in-Breadth) [CNSSI 4009]	システム／ネットワーク／サブコンポーネントのライフサイクルのすべての段階（システムまたはネットワークもしくは製品の設計および開発・製造・梱包・組み立て・システム統合・販売・運用・メンテナンス・削除）において脆弱性が利用されることによるリスクを特定・管理・低減するための計画的かつ系統だった一連の総合的な活動。
多重防護御 (Defense-in-Depth)	人、技術、および業務遂行能力を統合して、組織内の階層およびミッションごとに複数の調節可能な防壁を築く情報セキュリティ戦略。
開発者 (Developer)	以下を含む一般用語：①情報システム・システムコンポーネント・情報システムサービスの開発者または製造者②システムインテグレータ③ベンダー④ならびに製品の再販売業者。システム／コンポーネント／サービスの開発は、組織内で内部的に行われる場合もあれば（すなわち、社内開発）、外部の関係者によって行われる場合もある。
デジタルメディア (Digital Media)	電子媒体の一形態であり、データは（アナログメディアとは対照的に）デジタル形式で保存される。

任意のアクセス制御 (Discretionary Access Control)	情報システムのすべてのサブジェクトとオブジェクトにわたって実施されるアクセス制御ポリシーであり、情報のアクセスを許可されたサブジェクトに対して、以下の1つ以上の実施を許可するもの：①他のサブジェクトまたはオブジェクトに情報を渡す②自身の権限を他のサブジェクトに与える③サブジェクト、オブジェクト、情報システム、またはシステムコンポーネント上のセキュリティ属性を変更する④新たに作成されたオブジェクトまたは変更されたオブジェクトに関連するセキュリティ属性を選択する; あるいは⑤アクセス制御を規定するルールを変更する。「必須のアクセス制御」は、このような行為を制限する。
[CNSSI 4009]	サブジェクト（例：ユーザ、プロセス）の身元ならびにサブジェクトについて知らなければならない事柄（need-to-know）および／またはそのオブジェクトが所属するグループに基づきオブジェクト（例：ファイル、データエンティティ）に対するアクセスを制限する手段。この制御は任意であり、特定のアクセス許可を有するサブジェクトが、その許可を（間接的かも知れないが）他のサブジェクトに渡すことができる（ただし、「必須のアクセス制御」によって抑制されるた場合に限る）。
ドメイン (Domain) [CNSSI 4009]	一連のシステムリソースとそれらのリソースに対するアクセス権を有する一連のシステムエンティティの双方を含む環境またはコンテキスト。アクセス権の定義は、共通のセキュリティポリシー、セキュリティモデル、またはセキュリティアーキテクチャによってなされる。＜セキュリティドメイン(*Security Domain.*)＞を参照。
エンタープライズ（企業） (Enterprise) [CNSSI 4009]	定められたミッション・目標と、定められた境界を有する組織であり、情報システムを使用してそのミッションを遂行し、組織のリスクとパフォーマンスの管理に責任を負う。エンタープライズにおいては、以下の業務が全面的もしくは部分的に行われている：調達・プログラム管理・財務管理（例：予算）・人材・セキュリティ・情報システム・情報・ミッションそれぞれの管理。＜組織(*Organization*)＞を参照。
エンタープライズアーキテクチャ (Enterprise Architecture) [44 U.S.C. Sec. 3601]	戦略的な情報資産基盤で、ミッションを定義するもの。または、そのミッションを果たすのに必要な情報。あるいは、そのミッションを果たすのに必要なテクノロジー。もしくは、ミッションに求められるニーズの変化に対応して新たなテクノロジーを導入する切り替えプロセス。エンタープライズアーキテクチャには、ベースラインアーキテクチャおよびターゲットアーキテクチャならびに順序付け計画が含まれる。
情報システムが稼働する環境 (Environment of Operation) [NIST SP 800-37]	情報システムによる情報について処理・蓄積・伝送が行われる物理的な環境。

イベント（事象） (Event) [CNSSI 4009, Adapted]	情報システムにおいて発生する、監視可能なあらゆる事象。
執行機関 (Executive Agency) [41 U.S.C., Sec. 403]	合衆国法律集第 5 編 101 条で規定された執行部署、同 102 条で規定された軍の部局、5 U.S.C., Sec. 104（1）同 104 条 1 項で規定された独立機関および同法律集第 31 編 91 条の規定に全面的に基づいた純然たる国有企業。
ハッキングによる情報の窃盗 (Exfiltration)	情報システムから情報を不正に転送すること。
外部情報システム（または外部情報システムのコンポーネント） (External Information System (or Component))	組織のセキュリティ境界の外にある情報システムまたは情報システムのコンポーネント。通常、組織は、これらのシステムやコンポーネントに対する必要なセキュリティ管理策を直接適用やできず、セキュリティ管理策の有効性を直接評価できない。
（外部の情報システムを対象とした）情報システムサービス (External Information System Service)	組織が認可するセキュリティ境界の外側で実装される情報システムサービス（すなわち、組織の情報システムによって利用されるサービスではありながら、そのシステムの一部ではないもの）。通常、組織は、これらのシステムに対する必要なセキュリティ管理策を直接適用できず、セキュリティ管理策の有効性を直接評価できない。
（外部の情報システムを対象とした）情報システムサービスのプロバイダ (External Information System Service Provider)	組織に対して、さまざまな形態の需給関係を介して外部情報システムのサービスを提供する者。需給関係には、ジョイントベンチャー・ビジネスパートナーシップ・（契約および省庁間の取り決めならびに業務に関する一連の取り決めを介した）外注・ライセンス契約・サプライチェーン取引があるが、これらに限定されない。
外部ネットワーク (External Network)	組織によって管理されないネットワーク。
障害迂回 (Failover)	稼働していたシステムが障害ををを起こしたもしくは異常終了した場合に、代わりとなるもしくは余っている情報システムに（通常、人手を介さずにまたは警告なしで）自動的に切り替わる機能。
公正情報行動原則 (Fair Information Practice Principles)	プライバシーに関する一般的な枠組みとして、アメリカ合衆国でも国際的にも広く受け入れられている原則。連邦法および（連邦政府の）政策にとどまらず、国際的な公共政策や多くの国際条約に内容が反映されている。この原則は、多くの組織において、プライバシー関連のリスクを分析のうえ適切な形で軽減する戦略を決定するための基盤となる。
連邦政府機関 (Federal Agency)	＜執行機関 (*Executive Agency*＞を参照。

連邦エンタープライズアーキテクチャ (Federal Enterprise Architecture) [FEA Program Management Office]	行政管理予算局よって策定された、政府全体にわたる業務改善のためのビジネスベースのフレームワーク。その目的は、連邦政府を国民主体で市場本位かつ結果重視の組織に変えるための取組みを容易にすることにある。
連邦政府の情報システム (Federal Information System) [40 U.S.C., Sec. 11331]	行政機関、行政機関と役務・物品を提供する契約を締結した者、または行政機関を代理する他の組織によって使用または運用される情報システム。
FIPS 確認が行われた暗号技術 (FIPS-Validated Cryptography)	FIPS Publication 140-2（改正版を含む）が規定する要求事項を満たすべく Cryptographic Module Validation Program (CMVP) の試験が行われた暗号モジュール。CMVP の試験を行う前提条件として、その暗号モジュールが、Cryptographic Algorithm Validation Program (CAVP)の試験に合格した暗号アルゴリズムを実装していることが必須となる。＜NSA 認定の暗号技術 NSA-Approved Cryptography)＞を参照。
ファームウェア (Firmware) [CNSSI 4009]	ハードウェアに格納されているコンピュータープログラムおよびデータ。通常、ROM またはプログラマブル ROM に格納される。したがって、それらの プログラムとデータは、プログラムの実行中は動的に書き込んだり変更することができない。
ガード（システム） (Guard (System)) [CNSSI 4009, Adapted]	情報システム間またはサブシステム間における情報のやり取りを制限するメカニズム。
ハードウェア (Hardware) [CNSSI 4009]	情報システムの物理的な構成要素。＜ソフトウェア(Software)とファームウェア(Firmware)＞を参照。
影響度が高いシステム (High-Impact System) [FIPS 200]	FIPS Publication 199 に従って分類を行った結果、セキュリティの三要素（すなわち、機密性・完全性・可用性）のうち少なくとも１つについて、潜在的な影響度の分類が「高」と判断された情報システム。
ハイブリッドセキュリティ管理策 (Hybrid Security Control) [CNSSI 4009]	情報システムに実装されているセキュリティ管理策の一種。共通管理策としての役割と、特定の情報システム固有の管理策としての役割を併せ持つ。＜共通管理策(Common Control) ＞と＜システム固有のセキュリティ管理策(System-Specific Security Control)＞を参照。
影響度 (Impact)	情報または情報システムの機密性、完全性、または可用性の喪失によりもたらされる、組織の業務・組織の資産・個人・他の組織、または米国（国家安全保障上の利益を含む）に対する影響。

影響度の評価結果 (Impact Value)	情報の機密性、完全性、または可用性の侵害によってもたらされる潜在的な影響の度合を評価した結果であり、「低」・「中」・「高」のいずれかによって表される。
インシデント (Incident) [FIPS 200]	情報システムまたはそのシステムが処理または保存もしくは伝送する情報の機密性、完全性または可用性を実際に損なわせる（もしくは、その可能性のある）事象、あるいはセキュリティポリシー、セキュリティ手順、または利用規定に対する違反に当たる（もしくは、差し迫った脅威となる）事象。
産業用制御システム (Industrial Control System)	製造、製品の出荷、生産、および販売などの産業プロセスを制御するのに使用される情報システム。産業用制御システムには、地理的に分散している資産を管理するのに使用される監視制御データ収集システム（SCADA）、分散制御システム（DCS）、および前二者より小規模ながらローカルなプロセスをプログラマブル論理制御装置の利用を通じて制御するシステムなどがある。
情報 (Information) [CNSSI 4009] [FIPS 199]	事実・データ・意見などの知識を媒体によって、あるいはテキスト・数値・図・地図・物語などの形式で、もしくは視聴覚的に伝達する、あるいは表現すること。 情報タイプの一つの例。
情報漏えい (Information Leakage)	故意にあるいは不注意によって、情報を信頼性に欠ける環境にさらすこと。
情報所有者 (Information Owner) [CNSSI 4009]	特定の情報に対する法的権限または運用権限を持ち、その情報の生成、収集、処理、配布、および廃棄に関する管理策の制定に責任のある職員。
情報資源 (Information Resources) [44 U.S.C., Sec. 3502]	情報および関連資源（人的資源・設備・資金・情報技術など）。
情報セキュリティ (Information Security) [44 U.S.C., Sec. 3542]	機密性、完全性、および可用性を確保するために、情報と情報システムを不正なアクセス、利用、開示、中断、変更、破壊から保護すること。
情報セキュリティアーキテクチャ (Information Security Architecture)	エンタープライズアーキテクチャに欠くべからざるものとして組み込まれている部分であり、エンタープライズのセキュリティプロセス、情報セキュリティシステム、職員および組織のサブユニットのそれぞれについて構造と振る舞いを記述したもの。エンタープライズのミッションおよび戦略計画に準拠していることを示すためのアーキテクチャである。
情報セキュリティポリシー (Information Security Policy) [CNSSI 4009]	組織がどのように情報を管理・保護・配布すべきかを定めている指示や規制といったルールおよび慣行を一つにまとめたもの。

情報セキュリティプログラム (Information Security Program Plan)	組織全体にわたる情報セキュリティプログラムにおけるセキュリティ要求事項の概要を示し、それらの要求事項を満たすために導入済または導入が計画されている計画管理策および共通管理策について記述する正式な文書。
情報セキュリティリスク (Information Security Risk)	情報や情報システムへの不正なアクセス(または情報や情報システムの不正な利用・開示・中断・途絶・変更・破壊)に起因する(組織のミッション・機能・イメージ・評判のそれぞれとともに)組織の業務ならびに組織の資産および個人・他組織・国家のぞれぞれに対するリスク。
情報スチュワード (Information Steward) [CNSSI 4009]	特定の情報に対する法的権限または運用権限を持ち、その情報の生成、収集、処理、配布、および廃棄に関する管理策の制定に責任のある連邦政府の当局者。
情報システム (Information System) [44 U.S.C., Sec. 3502]	情報収集・情報処理・保守・情報活用・情報共有・情報配布・情報廃棄のいずれかを目的として編成された、離散的情報源の集まり 注記:情報システムには、産業用制御システム・プロセス制御システム・電話交換機・構内電話交換機(PBX)・環境制御システムなど、専門分野に特化したシステムも含まれる。
情報システムの境界 (Information System Boundary)	＜認可を出す範囲 (*Authorization Boundary*)＞を参照。
情報システムコンポーネント (Information System Component) [NIST SP 800-128, Adapted]	情報システムを構成する、独立し識別可能な IT 資産(例:ハードウェア、ソフトウェア、ファームウェア)。情報システムコンポーネントには、市販の IT 製品も含まれる。
情報システム所有者(または、プログラム管理者) (Information System Owner (or Program Manager))	情報システムのそれぞれ調達、開発、統合、変更、または運用と保守の全体に責任のある職員。
情報システムの耐障害性 (Information System Resilience)	情報システムが以下の状態を維持できること:①悪条件下にあっても、あるいは負荷が掛かった状態であっても、(顕著に低下した状態または無力化したような状態に陥ったとしても)稼働して、基礎的な運用能力を維持すること②ミッションニーズと平仄が合う時間内に、有効的に運用されている状態に復旧すること。

情報システムセキュリティ責任者 (Information System Security Officer) [CNSSI 4009]	情報システムまたは情報プログラムの運用面での適切なセキュリティ体制を維持する責任が割り当てられている個人。
情報システムサービス (Information System Service)	情報システムによって提供される機能のであり、情報の処理、保存、または伝送を容易にする。
情報システム関連のセキュリティリスク (Information System-Related Security Risks)	情報または情報システムの機密性、完全性、または可用性の喪失により生じるリスクであり、組織（資産、ミッション、機能、イメージ、または評判を含む）、個人、他の組織、および国家に対する影響（組織のそれぞれ資産、ミッション、機能、イメージ、または評判に対するものを含む）をが考慮されなければならないもの。＜リスク(Risk)＞を参照。
情報技術 (Information Technology) [40 U.S.C., Sec. 1401]	データまたは情報の自動的な入手、保存、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信の目的で政府行政機関によって利用される機器、または相互接続された機器システム・サブシステム。上記の目的のために、行政機関が該当機器を直接用いる場合または行政機関との間で下記を条件とする契約関係にある者が使用する場合には、該当機器は行政機関によって使用されたものとする：①そうした機器の使用を義務付けている場合②サービスの実施や製品の供給にあたって、該当機器の使用を相当程度義務付けている場合。 「情報技術」には、コンピュータ・補助機器・ソフトウェア・ファームウェア・関連手続・関連サービス（サポートサービスを含む）・関連リソースも含まれる。
IT 製品 (Information Technology Product)	＜情報システムコンポーネント (*Information System Component*)＞を参照。
情報のタイプ (Information Type) [FIPS 199]	組織によって（または特定の法律・大統領命令・指令・政策・規制によって定められている）プライバシー・医療・財産権・財務状況・捜査・契約者機密・セキュリティ管理等に関する情報の種類。
内部関係者 (Insider) [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	米国政府の何らかのリソース（職員、施設、情報、設備、ネットワーク、またはシステムを含む）に対するアクセスが許可されている者。

インサイダー脅威 (Insider Threat) [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	故意の有無にかかわらず、内部関係者が自身のアクセス権限を利用して、アメリカ合衆国のセキュリティに害を及ぼす脅威。ここでいう脅威には、スパイ行為、テロ行為、国家の安全保障に関わる情報の不正開示、または部門のリソースまたは機能の喪失や低下によってもたらされる、アメリカ合衆国に対する被害が含まれる場合がある。
[CNSSI 4009]	(セキュリティドメイン内で)アクセス権限を有する者で、データの破壊・不正開示・改ざん・サービス妨害のいずれか(またはそれらのすべて)を引き起こして、情報システムまたはエンタープライズに害を与える可能性のある者。
インサイダー脅威対策プログラム (Insider Threat Program) [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	機微な情報が不正に開示されることを検知・防止するために編成されたグループであり、一元的管理下に置かれる。機密情報を取り扱う部門および政府機関において「インサイダー脅威対策プログラム」は、情報へのアクセスの許可、一元的な情報統合・情報分析・情報対応、インサイダー脅威に関する意識を向上させるための従業員に対するトレーニングならびに政府保有のコンピュータ上でのユーザ操作のモニタリングが最低限可能なものでなけてはならない。機密情報を取り扱わない部門や機関では、機密でないものの機微な情報を保護するために、本プログラムを効果的に使用できる。
完全性 (Integrity) [44 U.S.C., Sec. 3542]	不正な改ざんまたは破壊から情報を保護されていること(否認防止および真正性が確担保されていることを含めて)。
内部ネットワーク (Internal Network)	①セキュリティ管理策の策定・維持・提供が、組織の職員または組織と役務・物品を提供する契約を結んだ者によって直接行われる②組織が管理するエンドポイント間で実装される暗号化・カプセル化もしくは類似のセキュリティ技術が(少なくとも機密性と完全性に関して)同等の効果をもたらすという 2 つの特徴をもったネットワーク。 内部ネットワークは、通常、組織が所有するが、組織が所有しない場合であっても、組織によって管理される場合がある。
ラベル (Label)	＜セキュリティ ラベル(*Security Label*)＞を参照。
基幹業務 (Line of Business)	OMB によって定められた、以下のプロセス区域: ケース管理、財務管理、助成金管理、人材管理、ならびにそれぞれ連邦政府の保健医療とITに関するエンタープライズアーキテクチャ、情報システムセキュリティ、予算の編成と執行、地理空間、および IT インフラの関連のもの。 なお、これらはほぼすべての連邦政府関係機関に共通なものである。

ローカルアクセス (Local Access)	ユーザ（またはユーザの名のもとで稼働しているプロセス）がネットワークを介さずに直接接続して情報をやりとりすることによって組織の情報システムへアクセスすること。
論理アクセス制御システム (Logical Access Control System) [FICAM Roadmap and Implementation Guidance]	ワークステーション、ネットワーク、アプリケーション、データベースなどのうち少なくとも1つのコンピュータのシステムリソースに対する個人のアクセスを制御するための自動システム。論理アクセス制御システムでは、暗証番号、カード、生体情報、またはその他のトークンなどのなんらかの仕組みを介して、個人の身元を確認することが求められる。このようなシステムでは、組織の各人に対して、組織内における彼（彼女）らの役割と責任に応じて異なるアクセス権限を割り当てることが可能である。
影響度が低位いのシステム (Low-Impact System) [FIPS 200]	FIPS Publication 199 に従って分類を行った結果、3 つのすべてのセキュリティの三要素（すなわち、機密性・完全性・可用性）のすべてについて、潜在的な影響度の分類が「低」と判断された情報システム。
悪質コード (Malicious Code)	許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェアまたはファームウェア。すなわち、ウイルス・ワーム・トロイの木馬など、ホストに感染するコードエンティティを指す。アドウェアようなものやスパイウェアも、悪質コードの一例である。
マルウェア (Malware)	＜悪質コード *Malicious Code*＞を参照。
管理されたインターフェース (Managed Interface)	情報システム内のインターフェースの1つであり、自動化されたメカニズムまたは自動機器を使用して境界保護機能を提供する。

必須のアクセス制御 (Mandatory Access Control) [CNSSI 4009]	情報システムの境界内におけるサブジェクト・オブジェクト双方の全てに対して一様に実施されるアクセス制御ポリシーである。なお、情報へのアクセスが許可されたサブジェクトは、以下のいずれかを実施する事が制される：①無許可のサブジェクト（または無許可のオブジェクト）に情報を渡す②自身の権限を他のサブジェクトに与える③サブジェクト、オブジェクト、情報システム、またはシステムコンポーネントのうち少なくとも1つについてのセキュリティ属性を変更する④新たに作成されたオブジェクト、または変更されたオブジェクトに関連するセキュリティ属性を選択するあるいは ⑤アクセス制御について規定するルールを変更する。 なお、組織が定めたサブジェクトには、組織が定めた権限が明示的に与えられる場合がある（すなわち、それらのサブジェクトは信頼できるものであることを意味している）。その場合、上述の制約の一部、あるいはすべてから解放される。 また、「必須のアクセス制御」は、オブジェクトに含まれる情報の機微度（セキュリティラベルによって示される）と、サブジェクトがそうした機微度を有する情報にアクセスするための大義名分（すなわち、セキュリティ許容度、正式なアクセス許可、および知る必要性）をに基づいて、オブジェクトに対するアクセスを制限する手段であり、任意でないアクセス制御の一種である。
マーキング (Marking)	＜セキュリティマーキング (*Security Marking*)＞を参照。
媒体 (Media) [FIPS 200]	物理的な装置または情報を書き込む面。これらの媒体として、情報システム内に情報を記録または保存あるいは複製したりするための磁気テープ・光ディスク・磁気ディスク・大規模集積回路（LSI）・ハードコピー（ディスプレー媒体は含まれない）が含まれるが、これらに限定されない。
メタデータ (Metadata)	データの特性について説明するための情報。メタデータには、たとえば、データ構造（例：データのフォーマット・シンタクス、およびデータに対するコマンド）について説明する構造的なメタデータや、データ内容（例：セキュリティラベル）について説明する記述的なメタデータなどがある。
モバイルコード (Mobile Code)	遠隔の情報システムから取り込まれ、ネットワークを介して伝送のうえローカルの情報システム上で実行されるソフトウェアプログラム（またはプログラムの一部）で、受信者による明示的なインストールや実行を必要としないもの。
モバイルコード技術 (Mobile Code Technologies)	モバイルコードを作成し使用するためのメカニズムを提供する、ソフトウェア技術（例：Java、JavaScript、ActiveX、VBScript)。

携帯機器 (Mobile Device)	以下の特徴を持つ、持ち運び可能なコンピュータデバイス：①個人が一人で容易に持ち運べるようなスモールフォームファクタ型である②物理的な接続なしで稼働するように設計されている（例：ワイヤレスで情報を送受信する）③取り外し（不）可能なデータ記憶装置をローカルに有するならびに④自給電源を有する。 なお、スマートフォン、タブレット、および電子書籍端末といった携帯機器は、音声通信機能・情報の取得を可能にする搭載センサー・遠隔地にあるローカルデータ同士の同期のいずれか（またはそれらすべて）を行うための内蔵機能もを有している場合もある。
影響度が中程度のシステム (Moderate-Impact System) [FIPS 200]	FIPS Publication 199 に従って分類を行った結果、セキュリティの三要素（すなわち、機密性、完全性、または可用性）のうち少なくとも1つについて潜在的な影響度の分類が「中」でありながら、「高」であるものはひとつもないと分類された情報システム。
多要素認証 (Multifactor Authentication)	2 つ以上の異なる要素を使用する認証。要素には、以下をのものが含まれる：①被認証者が知っていること（例：パスワード・暗証番号）②被認証者が持っているもの（例：暗号認証デバイス・トークン）③被認証者であること（例：生体認証情報）。 ＜オーセンティケータ(*Authenticator*)＞を参照。
多層セキュリティ (Multilevel Security) [CNSSI 4009]	分類とカテゴリーが異なる情報を処理するという考え方。セキュリティクリアランスがそれぞれに異なる複数のユーザに対してアクセスを一斉に許可したり、権限がない複数のユーザに対してアクセスを同時に拒否することを可能にする。
多層セキュリティレベル (Multiple Security Levels) [CNSSI 4009]	情報システムの機能で、複数の（セキュリティドメインが異なる）リソース（とりわけ保存されているデータ）を確実に区切ったもの。
連邦政府緊急時予備電気通信サービス (National Security Emergency Preparedness Telecommunications Services) [47 C.F.R., Part 64, App A]	アメリカ合衆国の住民にけがを負わせたり、害を及ぼしたり、財産の毀損または喪失を引き起こす、あるいはアメリカ合衆国の安全保障を脅かしたり、緊急時に対応する体制を弱体化させたりする若しくはそういった可能性があるあらゆるでき事や危機的状況（いずれも地方的、国家的、国際的なものかどうかは問わず）に対する心構えを常に持ち、かつそれらに対する即応する体制を整えるために使用される電気通信サービス。

国家安全システム (National Security System) [44 U.S.C., Sec. 3542]	政府機関、政府機関の委託業者または政府機関のるために活動する他の組織によって使用・運用されるなんらかの情報システム（通信システムを含む）であり、下記のいずれかの特徴を備える： (i) 情報システム（ただし、それぞれ給与・財務・物流・人材管理関係のアプリケーション等、管理用もしくは業務用のルーチンアプリケーションとして用いられる情報システムを除く）の機能および運用または当該システムを使用することが、下記の５つを意味する： ①インテリジェンス活動に関係する ②国家安全保障に関わる暗号活動の一翼を担う ③軍隊の指揮統制の一翼を担う ④武器または武器システムと一体化した機器に関係するシステムである ⑤軍隊または情報当局による作戦の遂行に欠かせない (ii)大統領命令または連邦法が定める基準のもとで国防や外交政策上の利益の観点から機密にすることが特別に認められた情報を保護するために制定された手順によって、常に保護される。
ネットワーク (Network) [CNSSI 4009]	相互接続されたコンポーネントの集合が実装された情報システム。コンポーネントには、ルーター・ハブ・ケーブル・通信制御装置・KDC（Key Distribution Center）・制御デバイスなどが該当する可能性がある。
ネットワークアクセス (Network Access)	情報システムに対して、ユーザ（またはユーザのために稼働するプロセス）がネットワーク (例：LAN・WAN・インターネット）を介してアクセスすること。
強制アクセス制御 (Nondiscretionary Access Control)	＜必須のアクセス制御 (*Mandatory Access Control*)＞を参照。
リモートメンテナンス (Nonlocal Maintenance)	外部ネットワーク（例：インターネット）あるいは内部ネットワークのいずれかを介して情報をやりとりする個人によって実施されるメンテナンス活動。
法人ユーザ以外のユーザ (Non-Organizational User)	法人ユーザ以外のユーザ（パブリックユーザを含む）。
否認防止 (Non-repudiation)	特定のアクションを実施したことを偽って否定する個人から保護すること。当該個人が特定の行動（情報の作成、メッセージの送信、情報の承認、およびメッセージの受信など）を実施したかどうかをについて特定することを可能にする。

NSA 認定の暗号技術 (NSA-Approved Cryptography)	以下によって構成される暗号技術：①承認されたアルゴリズム②特定の環境におけるそれぞれ機密情報及び／または CUI（Controlled Unclassified Information：管理下にある非機密情報）の保護に関して認定された実装ならびに③それらを支援する鍵管理基盤。
オブジェクト (Object)	情報システム関連の受動的なエンティティのうち、情報を含む（または情報を受け取る）エンティティ（例：デバイス・ファイル・レコード・テーブル・プロセス・プログラム・ドメイン）。サブジェクトがオブジェクトにアクセスするということは、そのオブジェクトが含む情報にもアクセスすることを意味する。＜サブジェクト (*Subject*)＞を参照。
運用面でのセキュリティ (Operations Security) [CNSSI 4009]	系統だった実績のあるプロセスで、デリケートな活動の計画および実施に関する通常は非機密扱いの証拠を特定・管理・保護することによって、能力と意図に関する情報が敵対者となりうる者に渡らないようにするもの。このプロセスは、以下の5つの段階に分かれる：①クリティカルな情報の特定②脅威の分析③脆弱性の分析④リスクのアセスメント⑤適切な対策の適用。
組織 (Organization) [FIPS 200, Adapted]	組織体（たとえば、連邦政府機関または適宜連邦政府機関の業務部門）を構成する組織（組織体全体に占める当該組織の規模または組織体におけるその複雑または位置づけは問わない）。
組織のユーザ (Organizational User)	組織の職員またはその組織が職員と同等の地位を有するとみなされた個人（例えば、客員研究員および組織および役務・物品の提供契約を結んだ者ならびに別の組織から業務命令により派遣された個人など）。それら個人に対して職員と同等の地位を与える政策と手続には、知る必要性、組織とのリレーションシップ、および市民権等がありうる。
オーバーレイ (Overlay)	セキュリティ管理策ベースラインの補足（およびさらなる改良）を目的として調整プロセスにて用いられる内容をセキュリティ管理策・拡張管理策・補足的ガイダンス・その他の補足情報として示したもの。オーバーレイの仕様は、元のセキュリティ管理策ベースラインの仕様に比べてより厳格である場合もあればより緩やかである場合もあり、複数の情報システムに適用可能である。
侵入テスト (Penetration Testing)	評価者が、通常は特定の制約のもとで、情報システムのセキュリティ機能の回避または突破を試みるテスト方法の一種。
個人情報 (Personally Identifiable Information) [OMB Memorandum 07-16]	個人の身元の識別や追跡に使用できる情報。そうした情報には、氏名・社会保障番号・生体認証記録等のように、単独で特定の個人に結びつくものもあれば、生年月日と出生地・母親の旧姓など、他の個人情報または識別情報との組み合わせによって特定の個人に結びつくものもある。

物理アクセス制御システム (Physical Access Control System) [FICAM Roadmap and Implementation Guidance]	人々または資産の移動を、承認規則にてセキュアな境界で管理する自動化システム。
行動計画とマイルストーン (Plan of Action and Milestones) [OMB Memorandum 02-01]	達成する必要があるタスクを示す文書。行動計画とマイルストーンは、計画の中の各項目の達成に必要なリソースとともに、マイルストーンとなる何らかのタスクの達成およびそのマイルストーンの完了予定日を詳述したものである。
持ち運び可能な記憶装置 (Portable Storage Device)	情報システムへの挿入と情報システムからの取り外しが可能な情報システムコンポーネントであり、テキスト・映像・音声・画像データといった情報を保存するのに使用される。そうしたコンポーネントは、通常、磁気装置・光学装置・ソリッドステートデバイスフロッピーディスク・CD・DVD・フラッシュ・サムドライブ・外付け HDD・不揮発性フラッシュメモリーカード・不揮発性フラッシュメモリードライブといった磁気装置・光学装置・ソリッドステートデバイスに実装される。
潜在的影響 (Potential Impact) [FIPS 199]	機密性、完全性、または可用性の喪失が組織の業務、組織の資産、または個人にもたらすであろう影響であり、以下のように分類される:①(FIPS Publication 199 に従って「低」と判断された場合)限られた負の影響②(FIPS Publication 199 に従って「中」と判断された場合)重大な負の影響あるいは③FIPS Publication 199 に従って「高」と判断された場合)深刻な、または壊滅的な負の影響。
プライバシー保護ポリシー (Privacy Act Statement)	1974 年に制定された Privacy Act(以降の改正を含む)の Section (e)(3)により、組織が個人から個人情報を収集する目的で用いる文書の一部を構成しなければならないもので、Privacy Act System of Records(SORN)に保存することが義務付けられた開示に関するステートメント。
プライバシー影響評価 (Privacy Impact Assessment) [OMB Memorandum 03-22]	以下を目的とする、情報がどのように扱われるかについての分析:①プライバシーに関して法律・規制・政策が定める要求事項が満たされるよう、情報が取り扱われるようにすること②電子情報システムによって情報を識別可能な形で収集・維持するする及び流布させる際のリスクと影響を特定すること③プライバシーが抱える潜在的リスクを軽減するために、情報処理の過程において情報を保護するプロセスとそれらを代替するプロセスとを検証・評価すること。
特権アカウント (Privileged Account)	特権ユーザの権限を与えられた情報システムアカウント。

特権コマンド (Privileged Command)	情報システムにおいて手動で実行するコマンドとして、(セキュリティ機能およびセキュリティに直接関連する情報を具備した)当該情報システムの制御・モニタリング・管理のいずれかに関係するコマンド。
特権ユーザ (Privileged User) [CNSSI 4009]	一般ユーザには許可されていないセキュリティ関連機能の実施を許可されている(したがって、信頼されている)ユーザ。
伝送を保護するシステム (Protective Distribution System)	ワイヤーラインまたは光ファイバーシステムで、音響および物質面ならびに電気的および電磁気的な側面等において十分な保護手段および/または対策が施されたことにより、暗号化されていない情報の伝送に使用できるもの。
来歴 (Provenance)	コンポーネント、コンポーネントのプロセス、情報、システム、組織、および組織のプロセスに関して、その所有と変更について記録したもの。この記録は、コンポーネント・コンポーネントのプロセス・情報・システム・組織・組織のプロセスのそれぞれのベースラインに対するあらゆる変更を特定のそれぞれアクター・機能・ロケール・アクティビティに適用されることを可能にする。
公開鍵基盤 (Public Key Infrastructure) [CNSSI 4009]	公開鍵証明書を生成・作成・配布・管理・アカウンティング・破壊するためのサービスの枠組み。人員・ポリシー・プロセス・サーバープラットフォーム・ソフトウェア・ワークステーションで構成され、公開鍵と秘密鍵のペアの管理や公開鍵証明書を管理する目的で利用される。なお、公開鍵基盤は、公開鍵証明書を発行・復元・失効させる機能または公開鍵証明書を失効させないようにする機能を管理する目的でも利用される。
除去 (Purge)	無害化されたデータがラボラトリアタックによって復旧されないようにすること。
セキュリティの互換性設定 (Reciprocity) [CNSSI 4009]	情報システムリソースを再利用するために互いのセキュリティアセスメントを受け入れること、および/または情報共有を目的として互いのセキュリティ状態の評価結果を受け入れることに、関係組織間で合意すること。
記録 (Records)	実施された活動または得られた結果についてのエビデンス・報告書・テスト結果などの形式で(自動/手動で)記録したもの。組織および情報システムが意図したとおりに機能していることを検証する際の基盤となる。また、複数の関連するデータフィールド群(すなわち、プログラムによるアクセスが可能であり、特定の項目に関するフルセットの情報を含むデータフィールドの集合)を示す場合もある。
レッドチームの訓練 (Red Team Exercise)	現実世界の状況を反映して、敵対者による組織のミッションおよび/または組織の業務プロセスへの侵害をシミュレーションしながら行われる訓練のこと。この訓練は、情報システムおよび組織におけるセキュリティ機能の包括的な評価を目的とする。

リファレンスモニタ (Reference Monitor)	参照を検証するメカニズムについて、設計上の要求事項の一式で、オペレーティングシステムの主要な構成要素として、すべてのサブジェクトとオブジェクトに対してアクセス制御ポリシーを実施するもの。なお、参照を検証するメカニズムでは、以下の要件が満たされていなければならない: ①常に機能している(すなわち、完全に自動調停する)こと ②改ざんを防止できること ③分析とテストが可能な大きさであり、その完全性が保証される(すなわち、検証できる)こと。
リモートアクセス (Remote Access)	組織の情報システムに対して、ユーザ(またはユーザを手助けするために稼働しているプロセス)が外部ネットワーク(例:インターネット)を介してアクセスすること。
リモートメンテナンス (Remote Maintenance)	外部ネットワーク(例:インターネット)を介して情報をやりとりする個人によって実施される、メンテナンス活動。
耐障害性 (Resilience)	<情報システムの耐障害性(*Information System Resilience*)>を参照。
秘密データ (Restricted Data) [Atomic Energy Act of 1954]	以下に関するあらゆるデータ: ①核兵器の設計、製造、または利用 ②特殊な核物質の製造 ③エネルギーを生成する際における特殊な核物質の使用。ただし、この場合、1954 年における改正 Atomic Energy Act (原子力法)の第 142 条の規定により削除されたもしくは Restricted Data(秘密データ)扱いを解かれたデータ以外を対象とする。
リスク (Risk) [FIPS 200, Adapted]	発生しうる事情または事象によってどの程度エンティティが脅かされるのかに関連して、通常は、以下について表した数式である: ①当該事情または事象が発生した場合にもたらされる負の影響 ②当該事情または事象が発生する可能性 情報システム関連のセキュリティリスクとは、情報または情報システムの機密性、完全性、または可用性の喪失により生じるリスクであり、(組織の)業務(あるいは、組織のそれぞれミッション・機能・イメージ・評判を含む)・(組織の)資産・個人・他組織・国家のそれぞれに対してもたらされる可能性のある負の影響をを反映したものである。

リスク評価 (Risk Assessment)	情報システムの運用により生じる組織の業務（あるいは、組織のそれぞれミッション、機能、イメージ、評判）、組織の資産、個人、他の組織、および国家に対するリスクを特定するプロセス。 リスクマネジメントの一部として、それぞれ脅威と脆弱性の分析を合体させたうえで、導入が計画されている（あるいは既に導入されている）セキュリティ管理策によって提供されるリスク軽減策について検討する。「リスク分析」と同義である。
リスク担当重役（の機能） (Risk Executive (Function)) [CNSSI 4009]	以下の項目が確実に行われるよう支援する、組織内の個人またはグループ: ①使命に基づいて業務を遂行する組織の全体的な戦略目標に関連して、個々の情報システムについてセキュリティリスクの関連で検討すべき事項（それらのシステムに関する承認判断を追加で行うためのそれを、観組織横断的な視点から捉えること ②個々の情報システムを発生源とするリスクの管理について、組織全体で整合性を確保したうえで組織のリスク許容度を反映したものにすると同時に、使命に基づいた業務の成功を妨げる他のリスクについても考慮しながら行うこと。
リスク管理 (Risk Management) [CNSSI 4009, adapted]	（組織の）業務・（組織の）ミッション・（組織の）機能・（組織の）イメージ・（組織に対する）評判・（組織の）資産・個人・他組織・国家のいずれかに対する情報セキュリティリスクを管理するための計画的な支援プロセスであり、以下などが該当する: ①リスク関連活動のコンテクストの確立 ②リスクの評価 ③特定されたリスクへの対応 ④長期間にわたるリスクのモニタリング。
リスクの軽減 (Risk Mitigation) [CNSSI 4009]	リスク軽減を目的としてリスクマネジメントプロセスのなかで推奨されるしかるべき対策やセキュリティ管理策を優先順位付けし、評価し、実施すること。
リスクのモニタリング (Risk Monitoring)	組織のリスク環境、リスクマネジメント計画、およびその他リスクを判断する前提となる活動について常に意識し続けること。
リスクへの対応 (Risk Response)	組織の業務に対するリスク（すなわち、組織が掲げるミッション、組織が果たす機能、組織が持たれるイメージ、または組織が得ている評判に対するそれ）や、組織の資産、個人、他の組織、または国家に対するリスクへの対応であり、リスクを許容する、回避する、軽減する、共有する、または移転する、などがある。

ロール･ベースのアクセス制御 (Role-Based Access Control)	アクセス制御のうち、ユーザの役割に依拠したもの（すなわち、所定の役割を果たすという明示的な若しくは暗黙裡の前提のもと、ユーザが受け取る一連のアクセス権限）。ロール許可は、役割階層を通じて継承される場合があり、通常は、定義された機能を組織内で実行するのに必要な許可を反映したものになる。役割は、一人に割り当てられる場合と、複数の人に割り当てられる場合がある。
保護手段 (Safeguards) [CNSSI 4009]	情報システムにおけるセキュリティ要求事項（すなわち、機密性、完全性および可用性）を満たすために規定された保護対策。保護手段には、セキュリティ機能、管理上の制約、職員のセキュリティ、ならびにそれぞれが物理的な構築物・領域・機器のセキュリティをが組み込まれうる。セキュリティ管理策(security control)や対策(countermeasures) と同義。
データの無害化 (Sanitization)	一般的な方法や（場合によっては）特別な方法を用いて、媒体上に書き込まれたデータを復旧できなくするアクションを指す。なお、データを復旧できないように媒体から情報を取り除くプロセスとして、分類ラベル・マーキング・活動ログの全面的な削除といったプロセスも指す。
スコーピングにおいて考慮すべき事項 (Scoping Considerations)	調整に関するガイダンスの一部として、セキュリティ管理策ベースライン内のセキュリティ管理策が適用可能かどうかについて及び当該管理策の実装の双方について組織が具体的に考慮すべき事項を示す。なお、具体的に考慮すべき事項には、政策・規制・技術・物理インフラ・（システムコンポーネントの）割り当て・（システムコンポーネントの）運用・（システムコンポーネントの）環境・公衆アクセス・拡張性・共通管理策・セキュリティ目的などがある。
セキュリティ (Security) [CNSSI 4009]	保護対策を確立・維持することによってもたらされる状況であり、情報システムを使用することによって企業が直面する脅威から派生するリスクがあったとしても、企業がミッションまたは重要な機能を実行できるようにするもの。保護対策は、企業の様々なリスク管理手法のうち、リスクをそれぞれ抑制・回避・予防・検知する手法ならびに情報システムを復旧させる手法および（情報システムを）修正する手法を組み合わせたものとなる可能性がある。
セキュリティ評価(Security Assessment)	＜セキュリティ管理策の評価(Security Control Assessment)＞を参照のこと。
セキュリティ評価計画 (Security Assessment Plan)	セキュリティ管理策のアセスメントを行う目的と、実施方法について、詳細な工程表を示したもの。
セキュリティ保証 (Security Assurance)	＜保証(Assurance)＞を参照のこと。

セキュリティ属性 (Security Attribute)	情報保護の観点から、エンティティの基本的なプロパティまたは特性を示した抽象概念。通常は、情報システムの内部データ構造（例：レコード・バッファー構造・ファイル構造）と関連し、アクセス制御ポリシーとフロー制御ポリシーの実装を可能にしたり、それぞれ特別な配布命令・処理命令・または割り当て命令を反映させたり、その他情報セキュリティポリシーの内容をサポートする目的で使用される。
セキュリティ認可 (Security Authorization)	＜運用認可(*Authorization*)＞を参照のこと。
セキュリティ認可を出す範囲 (Security Authorization Boundary)	＜認可を出す範囲(*Authorization Boundary*)＞を参照のこと。
セキュリティ機能 (Security Capability)	相互に補強し合うセキュリティ管理策（すなわち、保護手段および保護対策）の組み合わせで、技術的方法（すなわち、それぞれハードウェア、ソフトウェア、およびファームウェアの機能を実装すること）、物理的方法（すなわち、物理デバイスと保護対策を実装すること）、および手続的方法（すなわち、個人によって行われるプロシージャ）によって実施されるもの。
セキュリティカテゴリの作成 (Security Categorization)	情報または情報システムのセキュリティカテゴリを判断すること。セキュリティカテゴリを作成する方法は、国家安全保障に関わる情報システムについては CNSS Instruction 1253 に、国家安全保障に関わらない情報システムについては FIPS Publication 199 に記載されている。 ＜セキュリティカテゴリ（Security Category）＞を参照のこと。
セキュリティカテゴリ (Security Category) [FIPS 199, Adapted; CNSSI 4009]	情報または情報システムが機密性・完全性・可用性を喪失することが（組織の）業務・（組織の）資産・個人・他組織・国家にもたらす可能性のある影響についての評価に基づいて、情報または情報システムを特徴付けること。
セキュリティ管理策 (Security Control) [FIPS 199, Adapted]	情報システムまたは組織を保護する手段（もしくは対策）で、情報システムまたは組織に帰属する情報の機密性・完全性・可用性を保護しつつ定められた一連のセキュリティ要求事項を満たすために規定されたもの。
セキュリティ管理策のアセスメント (Security Control Assessment) [CNSSI 4009, Adapted]	セキュリティ管理策のテスト（または評価）で、セキュリティ管理策がどの程度正しく実装されているか、またどの程度意図した通りに運用されているかや情報システムまたは組織がセキュリティ要求事項を満たす成果をどの程度上げているかを判断するためのもの。

セキュリティ管理策の評価者 (Security Control Assessor)	セキュリティ管理策アセスメントを実施する責任を負う個人、グループ、または組織。
セキュリティ管理策ベースライン (Security Control Baseline) [FIPS 200, Adapted]	低位影響・中位影響・高位影響の区別に関わらず情報システムが最低限満たさなければならないセキュリティ管理策の一式であり、調整プロセスの土台となるもの。
セキュリティ管理策の拡張 (Security Control Enhancement)	以下のとおり、セキュリティ管理策を増強拡張すること: ①管理策に、関連する追加の機能を組み入れる ②管理策の強度を高める ③管理策の保証をより堅固なものにする。
セキュリティ管理策の継承 (Security Control Inheritance) [CNSSI 4009]	情報システムまたはアプリケーションが、策定・実装・監視され評価・承認を受けるセキュリティ管理策の全体もしくは一部分による保護を、①当該システムまたはアプリケーションについて責任を負っているエンティティ以外のエンティティおよび②組織の外部（もしくは内部）にあるエンティティで情報システムまたはアプリケーションが存在するものを通じてけているという状況。＜共通管理策 (Common Control)＞を参照のこと。
セキュリティ管理策オーバーレイ (Security Control Overlay)	＜オーバーレイ(Overlay)＞を参照のこと。
セキュリティドメイン (Security Domain) [CNSSI 4009]	セキュリティポリシーの実装を行うドメイン。単一の所轄機関によって管理される。
セキュリティ機能性 (Security Functionality)	セキュリティに関連して組織の情報システムまたはそれらのシステムが稼働する環境下において実施される特性・機能・メカニズム・サービス・手続・アーキテクチャのいずれか（またはそれらのすべて）。
セキュリティ機能 (Security Functions)	ハードウェア・ソフトウェアおよび／またはファームウェアで、情報システムのセキュリティポリシーを強制のうえ保護を行う前提としてコードとデータを分離する手助けをするという任務を帯びた情報システムのもの。
セキュリティに与える影響の分析(Security Impact Analysis) [CNSSI 4009]	情報システムに対する変更がシステムのセキュリティ状態にどの程度の影響をもたらしたかを判断するために、組織の担当者によって実施される分析。
セキュリティインシデント (Security Incident)	＜インシデント(Incident)＞を参照。

セキュリティカーネル (Security Kernel) [CNSSI 4009]	「リファレンスモニタ」の概念の実装に関連して信頼できるコンピュータ基盤のハードウェア・ファームウェア・ソフトウェア要素として、「リファレンスモニタ」の概念を実装するもの。セキュリティカーネルは、すべてのアクセスを仲介するだけではなく、改変から保護されることとともに、その正しさを検証できることが求められる。
セキュリティラベル (Security Label)	セキュリティ属性の集合体を特定の情報オブジェクトに結び付け、当該情報オブジェクトのデータ構造の一部にするために用いられる手段。
セキュリティマーキング (Security Marking)	セキュリティ属性の集合体を、人間による解読が可能な形式で、オブジェクトに結び付けるために用いられる手段。セキュリティマーキングは、情報セキュリティポリシーを組織のプロセスのベースで強制可能にする。
セキュリティ目的 (Security Objective) [FIPS 199]	機密性、完全性、または可用性。
セキュリティ計画 (Security Plan)	情報システム（または情報セキュリティプログラム計画書）に対するセキュリティ要求事項の概要を示したうえで、それらの要求事項を満たすために現在導入されている（またはこれまで導入が計画された）セキュリティ管理策について記述する正式な文書。 ＜システムセキュリティ計画(System Security Plan)または情報セキュリティプログラムの計画 (Information Security Program Plan)＞を参照のこと。
セキュリティポリシー (Security Policy) [CNSSI 4009]	セキュリティサービスの提供に関する基準の集合体。

セキュリティポリシーのフィルター (Security Policy Filter)	以下の機能を1つ以上行するハードウェアコンポーネントおよび／またはソフトウェアコンポーネント: ①コンテンツの検証で、提供されたコンテンツのデータタイプをの正確性を担保するために行うもの ②コンテンツの検査とともに、あらかじめ定義されたセキュリティポリシーに適合しているかどうかを検証するために行なわれる提供されたコンテンツの分析（例:ファイルコンストラクタおよびコンテンツ部分について、許可されたものと許可されていないものとの比較） ③悪意のあるコンテンツのチェックで、悪質コードが含まれていないかコンテンツを評価するもの ④不審な動作のチェックで、例えば、サンドボックスやチャンバーにおいて不審な動作を監視するもののように、安全な方法によってコンテンツを評価または実行するもの ⑤コンテンツのそれぞれ無害化・クレンジング・変換で、提供されたコンテンツをあらかじめ定義されたセキュリティポリシーに適合するよう修正するもの。
セキュリティ要求事項 (Security Requirement) [FIPS 200, Adapted]	処理・格納または伝送された情報の機密性・完全性・可用性を確保するために情報処理システムまたは組織に課される要求事項で、準拠法・大統領命令・指令・政策・標準・指示・規定・手順・ミッションニーズ・業務ニーズのいずれか（またはそれらすべて）に由来するもの。 注記:セキュリティ要求事項は、システム開発とエンジニアリング規約の分野において、高レベルのポリシー政策に関連した上流での活動から、低レベルの実装に関連のした下流での活動に至るまで、さまざまな状況下で用いることが可能である。
セキュリティサービス (Security Service) [CNSSI 4009]	機密性・完全性・可用性のいずれか1つあるいは複数のセキュリティ要求事項を支援する機能。セキュリティサービスの例として、鍵管理・アクセス制御・認証が挙げられる。
セキュリティ関連の情報 (Security-Relevant Information)	情報システム内の情報で、情報システムのセキュリティポリシーが強制できなくなる又はコードとデータの分離を維持できなくなる事態をもたらすほど、セキュリティ機能のオペレーションまたはセキュリティサービスの提供に潜在的な影響を与える可能性のあるもの。

政府機関の上級情報セキュリティ責任者 (Senior Agency Information Security Officer) [44 U.S.C., Sec. 3544]	最高情報責任者の職責として FISMA が規定する内容を執行する責任を有する職員で、最高情報責任者にとって、政府機関における承認責任者・情報システムの所有者および情報システムセキュリティ責任者との主要な連絡窓口としての役割を果たす職員。 注記：連邦政府機関の下部組織では、政府機関の上級情報セキュリティ責任者が担う責務とに類似のした責務を担う個人を示す用語として、「上級情報セキュリティ責任者(Senior Information Security Officer)」または「最高情報セキュリティ責任者(Chief Information Security Officer)」を用いる場合がある。
政府機関の上級プライバシー保護責任者 (Senior Agency Official for Privacy)	組織におけるプライバシー保護の問題に関して全体的な責任を負う上級職員。
上級情報セキュリティ責任者 (Senior Information Security Officer)	＜政府機関の上級情報セキュリティ責任者(*Senior Agency Information Security Officer*)＞を参照のこと。
機微な情報 (Sensitive Information) [CNSSI 4009, Adapted]	その情報の消失・誤用・悪用・ハッキングまたはその情報に対する不正アクセスが、国益または連邦政府による各種プログラムの遂行もしくは合衆国法律集第 5 編 552 条 a（連邦プライバシー法）の規定に基づいて各人に保障されたプライバシー権に悪影響を与える可能性のある情報で、大統領命令または議会制定法が定めた基準のもとでは、国防上や外交政策上の利益の観点から機密にすることが明示されなかったもの。
機密コンパートメント情報 (Sensitive Compartmented Information) [CNSSI 4009]	情報源・情報入手方法・分析プロセスに関連した機密情報またはそれらを通じて引き出した機密情報であり、国家情報局長官によって築かれた正式なアクセス制御システムの範疇で処理されることが要求されるもの。
サービス指向型アーキテクチャ (Service-Oriented Architecture)	相互運用可能なサービスの形式でソフトウェアを設計・開発するための原則および方法論の一式。これらのサービスは、周到に定義されたビジネス機能であり、さまざまな意図のもとで再利用できるソフトウェアコンポーネント（すなわち、別々のコードおよび／またはデータ構造）として構築されている。
ソフトウェア (Software) [CNSSI 4009]	関連データを含めて、実行時における書き込みや変更が動的に可能なコンピュータプログラム。
スパム (Spam)	電子メール送信システムを悪用して、無差別に大量の未承諾メールを送信すること。

特殊なアクセスプログラム (Special Access Program) [CNSSI 4009]	特定の種類の機密情報に対して制定されたプログラムで、同じ分類レベルの情報に通常求められるもの以上の保護対策およびアクセス要件を課す。
スパイウェア (Spyware)	情報システムにひそかにインストールされ個人や組織に関する情報を気づかれないように収集するソフトウェアであり、悪質コードの一種。
サブジェクト (Subject)	通常は、オブジェクト間で情報が流れるようにしたり、システム状態に変化をもたらす個人、プロセス、または機器。＜オブジェクト(Object)＞を参照。
サブシステム (Subsystem)	単一の情報システムを大きく分けた個々のパーツまたはコンポーネント。情報や情報技術、および 1 つ以上の特定の機能を実施する人員で構成される。
補足的ガイダンス (Supplemental Guidance)	セキュリティ管理策またはその拡張管理策について、追加の説明情報を提供するために用いられる文書。
補足 (Supplementation)	組織のリスクマネジメントニーズを十分に満たすために、（セキュリティ管理策を選択する際における）調整プロセスの一環として、セキュリティ管理策ベースラインにセキュリティ管理策または追加のセキュリティ管理策を追加する過程。
サプライチェーン (Supply Chain) [ISO 28001, Adapted]	複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達に始まり設計・開発・製造・加工・販売および購入者への配送に至る一連の流れ。
サプライチェーンエレメント (Supply Chain Element)	プログラム可能なロジック（論理）を含む IT 製品またはそうした製品の構成要素であり、情報システムを機能させる上で極めて重要であるもの。
システム (System)	＜情報システム(Information System)＞を参照のこと。
SORN (System of Records Notice)	組織が管理している（単数もしくは複数の）体系的な個人情報についての正式な公示で、1974 年に制定された Privacy Act（連邦プライバシー法）によって作成が義務付けられ、なおかつ次の事柄について規定するもの。①個人情報が体系化された目的②体系的な個人情報における「個人情報」の主体である個人③体系的な個人情報において、保持する「個人情報」の種類④当該個人情報がどのように共有されるか。
システムセキュリティ計画 (System Security Plan) [NIST SP 800-18]	情報システムに対するセキュリティ要求事項の概要を示し、それらの要求事項を満たすために既に導入されている（または導入が計画されている）セキュリティ管理策について記述する正式な文書。

システム固有のセキュリティ管理策 (System-Specific Security Control)	情報システムにおけるセキュリティ管理策でありながら、共通セキュリティ管理策ではないもの又は情報システムに実装される予定のハイブリッド管理策の一部。
調整されたセキュリティ管理策ベースライン (Tailored Security Control Baseline)	セキュリティ管理策ベースラインに調整に関するガイダンスを適用することによって得られる一連のセキュリティ管理策。＜調整(Tailoring)＞を参照のこと。
調整 (Tailoring)	以下のプロセスを通じてセキュリティ管理策ベースラインをが修正されること: ①共通管理策とは何かを明らかにした上で指定する ② ベースライン管理策の適用性と実装について考慮すべき事項であるところの「スコーピングについての考慮事項」を適用する ③代替のセキュリティ管理策を選択する ④組織が定義したセキュリティ管理策に関する変数に具体的な数値を割り当てる ⑤追加のセキュリティ管理策やその拡張セキュリティ管理策をもってセキュリティ管理策のベースライン管理策を補足する ⑥管理策の実装に関する追加の仕様情報を提供する。
脅威 (Threat) [CNSSI 4009, Adapted]	情報システムへの不正アクセス、情報システムの破壊・改変、システム内情報の不正開示および／または情報システムに対するサービス妨害攻撃(DoS)によって、情報システムが組織の業務（および組織のミッション・機能・イメージ・評判のいずれか）または（組織の）資産・個人・他組織・国家のいずれかに対して負の影響をもたらしうるあらゆる状況または事象。
脅威のアセスメント (Threat Assessment) [CNSSI 4009]	情報システムに対する脅威について、記述および評価を公式に行ったもの。
脅威源 (Threat Source) [FIPS 200]	脆弱性そのもの若しくは結果的に脆弱性を生じさせてしまうような方法（あるいは状況）を意図的に悪用する意思（あるいは手口）。なお、「脅威エージェント」と同義。
高信頼パス (Trusted Path)	情報システムにおけるセキュリティポリシーをサポートするために、ユーザが（入力装置を介して）情報システムのセキュリティ機能に必然的に安定した形で直接接続することを可能にするメカニズム。このメカニズムは、ユーザまたは情報システムのセキュリティ機能によってのみアクティブ化が可能であり、信頼されていないソフトウェアによって模倣することは不可能なものである。

信頼性 (Trustworthiness) [CNSSI 4009]	人または企業の属性であり、人または企業が特定のタスクを実施のうえ、割り当てられた責務を果たす資格・能力や割り当てられた責務を果たすことへの信頼性を有しているという安心感を他者に対して与えるもの。
(情報システムの)信頼性 (Trustworthiness (Information System))	情報システム(そのシステムを構築するのに使用されたITコンポーネントを含む)が、あらゆる種類の脅威に対して、システムを通じて処理・保存・伝送のいずれかを行う情報の機密性・完全性・可用性をどの程度維持することが期待できるかを示す度合。信用できる情報システムとは、そのシステムが稼働する環境において予想される環境破壊・人的ミス・構造破損・意図的な攻撃が発生しても、リスクを所定の範囲内に抑えて稼働できるとされているシステムである。
ユーザ (User) [CNSSI 4009, adapted]	情報システムにアクセスすることが許可された個人(または情報システムにアクセスすることが許可された個人のシステムプロセス)。 ＜組織におけるユーザ(Organizational User)＞および＜組織以外におけるユーザ(Non-Organizational User)＞を参照のこと。
仮想プライベートネットワーク (Virtual Private Network) [CNSSI 4009]	トンネリング・セキュリティ管理策・エンドポイントアドレスの変換の三者によって保護されされた情報システムのリンクで、専用回線を思わせるもの。
脆弱性 (Vulnerability) [CNSSI 4009]	情報システム・システムセキュリティ手順・内部統制・実装のいずれかに存在する弱点で、脅威源によって悪用される(またはその存在が表面化する)可能性があるもの。
脆弱性分析 (Vulnerability Analysis)	＜脆弱性のアセスメント(Vulnerability Assessment)＞を参照のこと。
脆弱性のアセスメント (Vulnerability Assessment) [CNSSI 4009]	以下を目的をした情報システムまたは製品の体系的な検査: ①セキュリティ対策が適切であるかの判断 ②セキュリティ上の欠陥の特定 ③計画されているセキュリティ対策の有効性を予測するためのデータの提供 ④した対策が適切であるかの事後確認。
ホワイトリストの作成 (Whitelisting)	以下のいずれかを識別するのに用いられるプロセス: ①情報システム上で実行することが承認されたソフトウェアプログラム ②承認された URL・ウェブサイト。

1

付録 C

略語

一般的略語

APT	APT (Advanced Persistent Threat)
CFR	連邦規則集(Code of Federal Regulations)
CIO	最高情報責任者(Chief Information Officer)
CISO	最高情報セキュリティ責任者(Chief Information Security Officer)
CAVP	暗号アルゴリズムの評価(Cryptographic Algorithm Validation Program)
CMVP	暗号モジュールの評価(Cryptographic Module Validation Program)
CNSS	国家安全保障システム委員会(Committee on National Security Systems)
CPO	最高プライバシー責任者(Chief Privacy Officer)
CUI	管理されている、非機密扱いの情報(Controlled Unclassified Information)
DCS	分散制御システム(Distributed Control System)
DNS	ドメインネームシステム(Domain Name System)
DoD	国防総省(Department of Defense)
FAR	連邦調達規則(Federal Acquisition Regulation)
FEA	連邦エンタープライズアーキテクチャ(Federal Enterprise Architecture)
FICAM	FICAM (Federal Identity, Credential, and Access Management)
FIPP	公正情報行動原則(Fair Information Practice Principles)
FIPS	連邦情報処理規格(Federal Information Processing Standards)
FISMA	連邦情報セキュリティマネジメント法(Federal Information Security Management Act)
HSPD	国土安全保障に関する大統領指令(Homeland Security Presidential Directive)
ICS	産業用制御システム(Industrial Control System)
IEEE	電気電子技術者協会(Institute of Electrical and Electronics Engineers)
IPsec	インターネットプロトコルセキュリティ(Internet Protocol Security)
ISO/IEC	国際標準化機構／国際電気標準会議(International Organization for Standardization/International Electrotechnical Commission)
ITL	情報技術ラボラトリ(Information Technology Laboratory)
LACS	論理アクセス制御システム(Logical Access Control System)
LSI	大規模集積化(Large-Scale Integration)
NIST	米国国立標準技術研究所(National Institute of Standards and Technology)

NISTIR	NIST が発行する省庁間共同報告書または内部報告書(National Institute of Standards and Technology Interagency or Internal Report)
NSA	国家安全保障局(National Security Agency)
NSTISSI	NSTISSI (National Security Telecommunications and Information System Security Instruction)
ODNI	国家情報長官室(Office of the Director of National Intelligence)
OMB	行政管理予算局(Office of Management and Budget)
OPSEC	運用セキュリティ(Operations Security)
PBX	構内電話交換機(Private Branch Exchange)
PACS	物理的アクセス制御システム(Physical Access Control System)
PIA	プライバシー影響評価(Privacy Impact Assessment)
PII	個人情報(Personally Identifiable Information)
PIV	本人確認(Personal Identity Verification)
PKI	公開鍵基盤(Public Key Infrastructure)
RBAC	役割ベースのアクセス制御(Role-Based Access Control)
RD	秘密データ(Restricted Data)
RMF	リスクマネジメントフレームワーク(Risk Management Framework)
SAISO	政府機関の上級情報セキュリティ責任者(Senior Agency Information Security Officer)
SAMI	ソースおよびメソッド情報(Sources And Methods Information)
SAOP	政府機関の上級プライバシー責任者(Senior Agency Official for Privacy)
SAP	特殊なアクセスプログラム(Special Access Program)
SC	セキュリティカテゴリ(Security Category)
SCADA	SCADA(Supervisory Control and Data Acquisition)
SCI	機密コンパートメント情報(Sensitive Compartmented Information)
SOA	サービス指向アーキテクチャ(Service-Oriented Architecture)
SORN	System of Records Notice)
SP	特定発行文書(Special Publication)
TCP/IP	伝送制御プロトコル/インターネットプロトコル(Transmission Control Protocol/Internet Protocol)
USB	ユニバーサルシリアルバス(Universal Serial Bus)
VoIP	ボイスオーバーアイピー(Voice over Internet Protocol)
VPN	仮想プライベートネットワーク(Virtual Private Network)

付録 D

セキュリティ管理策のベースライン管理策の概要

影響度が低い情報システムに対するベースライン管理策、影響度が中程度の情報システムに対するベースライン管理策および影響度が高い情報システムに対するベースライン管理策

この付録は、影響度が低い情報システム対するセキュリティ管理策、影響度が中程度の情報システム対するセキュリティ管理策および影響度が高い情報システムに対するセキュリティ管理策を決定するきっかけとなるベースライン管理策としてのセキュリティ管理策について記載するものである[90]。なお、3 つのベースライン管理策としてのセキュリティ管理策は、セキュリティ管理策のベースライン管理策である関係上、本質的に階層関係にある[91]。ちなみに、ある1つのセキュリティ管理策がベースライン管理策として選択されている場合においては、該当欄にファミリ識別子に加えてセキュリティ管理策番号が記載されている。ただし、特定のベースライン管理策としてセキュリティ管理策が使用されない場合、該当欄においては *"not selected"*（選択されていない）と記載されている。また、セキュリティ管理策の拡張管理策がセキュリティ管理策を補足するものである場合、該当する拡張管理策は番号によって表されている。たとえば、IR-2 のセキュリティ管理策のなかで影響度が高いベースライン管理策が記載されている欄であるところの IR-2(1)は、「インシデント対応」のファミリにおける 2 番目のセキュリティ管理策が（1）の拡張管理策としてのセキュリティ管理策と共に表記されていることを示すものである。なお、組織は、この付録に記載されているベースライン管理策に採録されていないものでありながら、セキュリティ管理策カタログの一部のセキュリティ管理策を同カタログの一部の拡張管理策を含めて必要に応じて利用することができる。ちなみに、セキュリティ管理策カタログの一部のセキュリティ管理策は、たとえば、リスクを評価したところ（組織の）業務・組織の）資産・個人・（他）組織・国家に対するリスクを満足に緩和するためにはセキュリティ管理策（またはその拡張管理策）を追加しなければならないことが明らかになった場合に、同カタログの一部の拡張管理策を含めて利用することができるようになる。

組織は、セキュリティ管理策の実装順序を決める足がかりとして、セキュリティ管理策のベースライン管理策のそれぞれに関連して、推奨された「優先順位コード」を明示する（すなわち、優先順位コードが 1[P1]のセキュリティ管理策は優先順位コードが 2[P2]のセキュリティ管理策よりも実装の優先順位が高く、なおかつ優先順位コードが 2[P2]のセキュリティ管理策は優先順位コードが 3[P3]のセキュリティ管理策よりも実装の優先順位が高いということを示すと同時に、優先順位コードが 0[P0]の場合は、セキュリティ管理策が何らベースライン管理策として選択されていないことを示す）ことができる。なお、推奨された優先順位コードを明示する事によっ

[90] 全てのセキュリティ管理策は、この文書の付録 F に加えてこの文書の付録 G に網羅されている。なお、セキュリティ管理策のベースライン管理策の文書については、Annex 1・同 2・同 3 としてリスト化されたものを http://csrc.nist.gov/publications から個別に入手する事が可能である。また、セキュリティ管理策カタログのオンライン版についても、http://web.nvd.nist.gov/view/800-53/home から入手する事が可能である。

[91] 影響度の低いセキュリティ管理策に加えて、影響度が中程度のセキュリティ管理策ならびに影響度の高いセキュリティ管理策のそれぞれの管理策のセキュリティ要求事項（すなわち、基準となる管理策およびその拡張管理策の全て）は、階層的性質を持つ。すなわち、一定の影響度を持つセキュリティ管理策の要求事項(例：CP-4コンティンジェンシープランのテスト—（影響度が）中程度: CP-4 (1))は、当該セキュリティ管理策のなかで影響度が1段低い管理策(例：CP-4 コンティンジェンシープランのテスト—低い:CP-4)に対する要求事項と比較して、より強力なセキュリティ要求事項を満たしている。

て実装順序を決定することは、他のセキュリティ管理策の基本となるセキュリティ管理策を確実に先行して実装するのに役立つ。したがって、組織が利用可能なリソースに応じてセキュリティ管理策をより構造化されたタイムリーな形で展開することが可能となる。ただし、セキュリティ計画の中にある全てのセキュリティ管理策が実装されるまでは、優先順位コードの順序通りにセキュリティ管理策を実装することによってリスクが一定程度軽減されたことにはならない。優先順位コードは、実装の順序を決める目的にのみ利用され、どのセキュリティ管理策を選択するか決定する目的で利用されることはない。ちなみに、表 D-1 は、表 D-2 上に記載されたベースライン管理策としてのセキュリティ管理策に関連した優先順位コードは、表 D-1 の通りである:

表 D-1: セキュリティ管理策の優先順位コード

優先順位コード	順序	アクション
優先順位コード 1 **(P1)**	最初	最初の実装として P1 セキュリティ管理策を実装する。
優先順位コード 2 **(P2)**	次	P1 管理策の後に P2 セキュリティ管理策を実装する。
優先順位コード 3 **(P3)**	最後	P1 管理策の実装後および P2 管理策の実装後に P3 セキュリティ管理策を実装する。
優先順位指定なし **(P0)**	指定なし	何らベースライン管理策としてセキュリティ管理策を選択しない。

なお、表 D-2 は、それぞれ上位・中程度・下位のベースライン管理策として当初割り当てられていたセキュリティ管理策およびその拡張管理策を要約した表として、この文書の付録 F に記載されたものの概要を示している。また、表 D-2 においては、セキュリティ管理策を実装するための優先順位コードに加えて、この文書の付録 F から削除されたセキュリティ管理策についても記載されている。さらに、表 D-2 以外にも、優先順位コードがセキュリティ管理策のベースライン管理策と共にこの文書の付録 F 上の各セキュリティ管理策の下に記載されたベースライン管理策の割り当てについておよび優先順位についてのセクションに追記されている。

表 D-2: セキュリティ管理策のベースライン管理策[92]

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
アクセス制御					
AC-1	アクセス制御ポリシーおよびアクセス制御手順	P1	AC-1	AC-1	AC-1
AC-2	アカウント管理	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	アクセス強制	P1	AC-3	AC-3	AC-3
AC-4	情報フローの強制	P1	選択されていない	AC-4	AC-4
AC-5	職務の分離	P1	選択されていない	AC-5	AC-5
AC-6	最小権限の原則	P1	選択されていない	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	不正ログイン試行	P2	AC-7	AC-7	AC-7

[92] 上記の表 D-2 において列挙されたベースライン管理策としてのセキュリティ管理策は、当初この文書の 3.2 のセクションに記載されている調整活動の実施に先立って組織によって選択されたベースライン管理策である。なお、これらのベースライン管理策としてのセキュリティ管理策は、優先順位コードとともに国家のシステムではないセキュリティシステムにのみ適用できる。また、国家安全システムに対するセキュリティ管理策のベースライン管理策は、CNSS Instruction 1253 に盛り込まれている。

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
AC-8	システム利用通知	P1	AC-8	AC-8	AC-8
AC-9	ログイン（アクセス）通知	P0	選択されていない	選択されていない	選択されていない
AC-10	コンカレントセッションに関する管理策	P3	選択されていない	選択されていない	AC-10
AC-11	セッションロック	P3	選択されていない	AC-11 (1)	AC-11 (1)
AC-12	セッションの正常終了	P2	選択されていない	AC-12	AC-12
AC-13	**（削除された）**	---	---	---	---
AC-14	識別・認証のいずれも必要としない許可されたアクション	P3	AC-14	AC-14	AC-14
AC-15	**（削除された）**	---	---	---	---
AC-16	セキュリティ属性	P0	選択されていない	選択されていない	選択されていない
AC-17	リモートアクセス	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	ワイヤレスアクセス	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	携帯機器に対するアクセス制御	P1	AC-19	AC-19 (5)	AC-19 (5)
AC-20	外部情報システムの使利用	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	情報共有	P2	選択されていない	AC-21	AC-21
AC-22	一般の人がアクセスできるコンテンツ	P3	AC-22	AC-22	AC-22
AC-23	マイニングされたデータの保護	P0	選択されていない	選択されていない	選択されていない
AC-24	アクセス制御の決定	P0	選択されていない	選択されていない	選択されていない
AC-25	参照モニタ	P0	選択されていない	選択されていない	選択されていない
セキュリティ意識向上トレーニング					
AT-1	セキュリティ意識向上トレーニングについて、そのポリシーおよび手順	P1	AT-1	AT-1	AT-1
AT-2	セキュリティ意識向上トレーニング	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	ロールベースのセキュリティトレーニング	P1	AT-3	AT-3	AT-3
AT-4	セキュリティトレーニングの記録	P3	AT-4	AT-4	AT-4
AT-5	**（削除された）**	---	---	---	---
監査およびその説明					
AU-1	監査およびの監査結果の説明のそれぞれについてのポリシーおよび手順	P1	AU-1	AU-1	AU-1
AU-2	監査イベント	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	監査記録の内容	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	監査記憶容量	P1	AU-4	AU-4	AU-4
AU-5	監査処理エラーへの対応	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	監査レビュー・監査分析・監査報告	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	監査削減および監査報告書生成	P2	選択されていない	AU-7 (1)	AU-7 (1)
AU-8	タイムスタンプ	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	監査情報の保護	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	否認防止	P2	選択されていない	選択されていない	AU-10
AU-11	監査記録の保存	P3	AU-11	AU-11	AU-11
AU-12	監査の生成	P1	AU-12	AU-12	AU-12 (1) (3)

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
AU-13	情報開示のためのモニタリング	P0	選択されていない	選択されていない	選択されていない
AU-14	セッション監査	P0	選択されていない	選択されていない	選択されていない
AU-15	補完された監査能力	P0	選択されていない	選択されていない	選択されていない
AU-16	組織横断型監査	P0	選択されていない	選択されていない	選択されていない
セキュリティアセスメントおよび認可					
CA-1	セキュリティ評価およびセキュリティ認可のそれぞれについてのポリシーおよび手順	P1	CA-1	CA-1	CA-1
CA-2	セキュリティ評価	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	システムの相互接続	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	**（削除された）**	---	---	---	---
CA-5	行動計画とマイルストーン	P3	CA-5	CA-5	CA-5
CA-6	セキュリティ認可	P2	CA-6	CA-6	CA-6
CA-7	継続的なモニタリング	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	侵入テスト	P2	選択されていない	選択されていない	CA-8
CA-9	内部システム接続	P2	CA-9	CA-9	CA-9
構成管理					
CM-1	構成管理ポリシーおよび構成管理手順	P1	CM-1	CM-1	CM-1
CM-2	ベースライン構成	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	構成変更管理	P1	選択されていない	CM-3 (2)	CM-3 (1) (2)
CM-4	セキュリティ影響分析	P2	CM-4	CM-4	CM-4 (1)
CM-5	変更に対するアクセス制限	P1	選択されていない	CM-5	CM-5 (1) (2) (3)
CM-6	構成設定	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	最小機能	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	情報システムコンポーネントのインベントリ	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	構成管理計画	P1	選択されていない	CM-9	CM-9
CM-10	ソフトウェアの使用制限	P2	CM-10	CM-10	CM-10
CM-11	ユーザがインストールしたソフトウェア	P1	CM-11	CM-11	CM-11
緊急時対応計画					
CP-1	緊急時対応計画のポリシーと手順	P1	CP-1	CP-1	CP-1
CP-2	緊急時対応計画	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	緊急時対応トレーニング	P2	CP-3	CP-3	CP-3 (1)
CP-4	コンティンジェンシープランのテスト	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	**（削除された）**	---	---	---	---
CP-6	代替格納拠点	P1	選択されていない	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	代替処理拠点	P1	選択されていない	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	通信サービス	P1	選択されていない	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
CP-9	情報システムのバックアップ	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	情報システムの復旧と情報システムの再構成	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	代替通信プロトコル	P0	選択されていない	選択されていない	選択されていない
CP-12	セーフモード	P0	選択されていない	選択されていない	選択されていない
CP-13	代わりのセキュリティメカニズム	P0	選択されていない	選択されていない	選択されていない
識別および認証					
IA-1	識別および認証のそれぞれについてのポリシーおよび手順	P1	IA-1	IA-1	IA-1
IA-2	(組織ユーザの)識別および認証	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	デバイスの識別およびデバイスの認証	P1	選択されていない	IA-3	IA-3
IA-4	識別子の管理	P1	IA-4	IA-4	IA-4
IA-5	認証子の管理	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	認証によるフィードバック	P2	IA-6	IA-6	IA-6
IA-7	暗号モジュールの認証	P1	IA-7	IA-7	IA-7
IA-8	(組織ユーザ以外のユーザの)識別および認証	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	サービスの識別およびサービスの認証	P0	選択されていない	選択されていない	選択されていない
IA-10	状況に応じた識別および状況に応じた認証	P0	選択されていない	選択されていない	選択されていない
IA-11	再認証	P0	選択されていない	選択されていない	選択されていない
インシデント対応					
IR-1	インシデント対応のポリシーおよびインシデント対応の手順	P1	IR-1	IR-1	IR-1
IR-2	インシデント対応トレーニング	P2	IR-2	IR-2	IR-2 (1) (2)
IR-3	インシデント対応テスト	P2	選択されていない	IR-3 (2)	IR-3 (2)
IR-4	インシデント管理	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	インシデント監視	P1	IR-5	IR-5	IR-5 (1)
IR-6	インシデントの報告	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	インシデント対応支援	P2	IR-7	IR-7 (1)	IR-7 (1)
IR-8	インシデント対応計画	P1	IR-8	IR-8	IR-8
IR-9	情報流出への対応	P0	選択されていない	選択されていない	選択されていない
IR-10	統合情報セキュリティ分析チーム	P0	選択されていない	選択されていない	選択されていない
メンテナンス					
MA-1	システムメンテナンスの手順およびシステムメンテナンスポリシー	P1	MA-1	MA-1	MA-1
MA-2	メンテナンス管理	P2	MA-2	MA-2	MA-2 (2)
MA-3	メンテナンスツール	P3	選択されていない	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	広域メンテナンス	P2	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	メンテナンス要員	P2	MA-5	MA-5	MA-5 (1)

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
MA-6	タイムリーなメンテナンス	P2	選択されていない	MA-6	MA-6
メディアの保護					
MP-1	メディア保護ポリシーおよびメディア保護のための手順	P1	MP-1	MP-1	MP-1
MP-2	メディアへのアクセス	P1	MP-2	MP-2	MP-2
MP-3	メディアのマーキング	P2	選択されていない	MP-3	MP-3
MP-4	メディアの格納	P1	選択されていない	MP-4	MP-4
MP-5	メディアの伝送	P1	選択されていない	MP-5 (4)	MP-5 (4)
MP-6	メディアの無害化	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	メディアの利用	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	メディアのダウングレード	P0	選択されていない	選択されていない	選択されていない
物理的保護および環境保護					
PE-1	物理的保護ポリシーおよび環境保護ポリシーに加えて、物理的保護および環境保護のそれぞれの手順	P1	PE-1	PE-1	PE-1
PE-2	物理的アクセスの認可	P1	PE-2	PE-2	PE-2
PE-3	物理的アクセス制御	P1	PE-3	PE-3	PE-3 (1)
PE-4	伝送メディア関係のアクセス制御	P1	選択されていない	PE-4	PE-4
PE-5	出力装置関係のアクセス制御	P2	選択されていない	PE-5	PE-5
PE-6	物理アクセスの監視	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	**（削除された）**	---	---	---	---
PE-8	ビジターアクセスのレコード	P3	PE-8	PE-8	PE-8 (1)
PE-9	電力設備および電力ケーブル配線	P1	選択されていない	PE-9	PE-9
PE-10	緊急停止	P1	選択されていない	PE-10	PE-10
PE-11	非常用電源	P1	選択されていない	PE-11	PE-11 (1)
PE-12	非常用照明	P1	PE-12	PE-12	PE-12
PE-13	防火	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	温度管理および湿度管理	P1	PE-14	PE-14	PE-14
PE-15	水濡れ被害からの保護	P1	PE-15	PE-15	PE-15 (1)
PE-16	配信および削除	P2	PE-16	PE-16	PE-16
PE-17	代わりの仕事場	P2	選択されていない	PE-17	PE-17
PE-18	情報システムコンポーネントの場所	P3	選択されていない	選択されていない	PE-18
PE-19	情報漏えい	P0	選択されていない	選択されていない	選択されていない
PE-20	資産のモニタリングおよび資産の追跡	P0	選択されていない	選択されていない	選択されていない
計画作成					
PL-1	セキュリティ計画策定する上でのポリシーおよびセキュリティ計画を策定する手順	P1	PL-1	PL-1	PL-1
PL-2	システムセキュリティ計画	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	**（削除された）**	---	---	---	---
PL-4	行動規範	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	**（削除された）**	---	---	---	---

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
PL-6	**（削除された）**	---	---	---	---
PL-7	上のセキュリティの概念	P0	選択されていない	選択されていない	選択されていない
PL-8	情報セキュリティアーキテクチャ	P1	選択されていない	PL-8	PL-8
PL-9	集中管理	P0	選択されていない	選択されていない	選択されていない
職員によるセキュリティ					
PS-1	職員のセキュリティポリシーおよび職員がセキュリティを確保する手順	P1	PS-1	PS-1	PS-1
PS-2	ポジションリスクの指定	P1	PS-2	PS-2	PS-2
PS-3	職員のスクリーニング	P1	PS-3	PS-3	PS-3
PS-4	職員の雇用の終了	P1	PS-4	PS-4	PS-4 (2)
PS-5	職員の異動	P2	PS-5	PS-5	PS-5
PS-6	アクセス契約	P3	PS-6	PS-6	PS-6
PS-7	職員によるセキュリティ	P1	PS-7	PS-7	PS-7
PS-8	職員に対する制裁	P3	PS-8	PS-8	PS-8
リスク評価					
RA-1	リスク評価ポリシーおよびリスク評価手順	P1	RA-1	RA-1	RA-1
RA-2	セキュリティカテゴリ	P1	RA-2	RA-2	RA-2
RA-3	リスク評価	P1	RA-3	RA-3	RA-3
RA-4	**（削除された）**	---	---	---	---
RA-5	脆弱性スキャン	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Technical Surveillance Countermeasures に関する調査	P0	選択されていない	選択されていない	選択されていない
システムおよびサービスの調達					
SA-1	システム調達およびサービスの調達のポリシーと手順	P1	SA-1	SA-1	SA-1
SA-2	リソースの割り当て	P1	SA-2	SA-2	SA-2
SA-3	システム開発ライフサイクル	P1	SA-3	SA-3	SA-3
SA-4	調達プロセス	P1	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	情報システムの文書化	P2	SA-5	SA-5	SA-5
SA-6	**（削除された）**	---	---	---	---
SA-7	**（削除された）**	---	---	---	---
SA-8	セキュリティエンジニアリングの諸原則	P1	選択されていない	SA-8	SA-8
SA-9	外部情報システムサービス	P1	SA-9	SA-9 (2)	SA-9 (2)
SA-10	開発者構成管理	P1	選択されていない	SA-10	SA-10
SA-11	開発者によるセキュリティテストを経た開発者によるセキュリティ評価	P1	選択されていない	SA-11	SA-11
SA-12	サプライチェーンの保護	P1	選択されていない	選択されていない	SA-12
SA-13	信頼性	P0	選択されていない	選択されていない	選択されていない
SA-14	深刻度分析	P0	選択されていない	選択されていない	選択されていない

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
SA-15	開発プロセス・規格・ツール	P2	選択されていない	選択されていない	SA-15
SA-16	開発者が提供する訓練	P2	選択されていない	選択されていない	SA-16
SA-17	開発者が描くセキュリティアーキテクチャ(および設計)	P1	選択されていない	選択されていない	SA-17
SA-18	改ざんに対する耐性と改ざんの検知	P0	選択されていない	選択されていない	選択されていない
SA-19	コンポーネントの真正性	P0	選択されていない	選択されていない	選択されていない
SA-20	重要なコンポーネントの受託カスタマイズ開発	P0	選択されていない	選択されていない	選択されていない
SA-21	開発者に対するスクリーニング	P0	選択されていない	選択されていない	選択されていない
SA-22	サポートされていないシステムコンポーネント	P0	選択されていない	選択されていない	選択されていない
システムおよび通信の保護					
SC-1	システム保護ポリシー・通信保護ポリシー・システム保護手順・通信保護手順	P1	SC-1	SC-1	SC-1
SC-2	アプリケーションの分割	P1	選択されていない	SC-2	SC-2
SC-3	セキュリティ機能の分離	P1	選択されていない	選択されていない	SC-3
SC-4	共有リソース内の情報	P1	選択されていない	SC-4	SC-4
SC-5	サービス妨害からの保護	P1	SC-5	SC-5	SC-5
SC-6	リソースの可用性	P0	選択されていない	選択されていない	選択されていない
SC-7	境界保護	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	伝送の機密性と完全性	P1	選択されていない	SC-8 (1)	SC-8 (1)
SC-9	**(削除された)**	---	---	---	---
SC-10	ネットワーク切断	P2	選択されていない	SC-10	SC-10
SC-11	高信頼パス	P0	選択されていない	選択されていない	選択されていない
SC-12	暗号鍵の作成と管理	P1	SC-12	SC-12	SC-12 (1)
SC-13	暗号化保護	P1	SC-13	SC-13	SC-13
SC-14	**(削除された)**	---	---	---	---
SC-15	共用コンピュータデバイス	P1	SC-15	SC-15	SC-15
SC-16	セキュリティ属性の送信	P0	選択されていない	選択されていない	選択されていない
SC-17	PKI 証明書	P1	選択されていない	SC-17	SC-17
SC-18	モバイルコード	P2	選択されていない	SC-18	SC-18
SC-19	ボイスオーバーインターネットプロトコル	P1	選択されていない	SC-19	SC-19
SC-20	セキュアな名前／アドレス解決サービス(信頼できるソース)	P1	SC-20	SC-20	SC-20
SC-21	セキュアな名前解決サービスおよびセキュアなアドレス解決サービス(再帰的リゾルバもしくはキャッシングリゾルバ)	P1	SC-21	SC-21	SC-21
SC-22	名前解決サービス・アドレス解決サービスのそれぞれのアーキテクチャおよび両サービスのプロビジョニング	P1	SC-22	SC-22	SC-22
SC-23	セッションの信頼性	P1	選択されていない	SC-23	SC-23
SC-24	既知の失敗	P1	選択されていない	選択されていない	SC-24
SC-25	シンノード	P0	選択されていない	選択されていない	選択されていない
SC-26	ハニーポット	P0	選択されていない	選択されていない	選択されていない

9

管理策番号	管理策名	優先順位	当初のベースライン管理策		
			低	中	高
SC-27	プラットフォームに依存しないアプリケーション	P0	選択されていない	選択されていない	選択されていない
SC-28	滞留している情報の保護	P1	選択されていない	SC-28	SC-28
SC-29	異種性	P0	選択されていない	選択されていない	選択されていない
SC-30	隠匿および誤命令	P0	選択されていない	選択されていない	選択されていない
SC-31	隠れチャネル分析	P0	選択されていない	選択されていない	選択されていない
SC-32	情報システムの分割	P0	選択されていない	選択されていない	選択されていない
SC-33	**（削除された）**	---	---	---	---
SC-34	変更できない実行可能プログラム	P0	選択されていない	選択されていない	選択されていない
SC-35	ハニークライアント	P0	選択されていない	選択されていない	選択されていない
SC-36	分散処理および分散ストレージ	P0	選択されていない	選択されていない	選択されていない
SC-37	帯域外チャネル	P0	選択されていない	選択されていない	選択されていない
SC-38	オペレーションセキュリティ	P0	選択されていない	選択されていない	選択されていない
SC-39	プロセス分離	P1	SC-39	SC-39	SC-39
SC-40	ワイヤレス接続の保護	P0	選択されていない	選択されていない	選択されていない
SC-41	ポートと入出力装置とのアクセス	P0	選択されていない	選択されていない	選択されていない
SC-42	センサー機能およびセンサーデータ	P0	選択されていない	選択されていない	選択されていない
SC-43	使用制限	P0	選択されていない	選択されていない	選択されていない
SC-44	デトネーションチャンバ	P0	選択されていない	選択されていない	選択されていない
システムの完全性および情報の整合性					
SI-1	システムの完全性および情報の完全性の双方に関するポリシーならびに手順	P1	SI-1	SI-1	SI-1
SI-2	欠陥の修復	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	悪質なコードからの保護	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	情報システムのモニタリング	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	セキュリティの警告に加えて、勧告・命令	P1	SI-5	SI-5	SI-5 (1)
SI-6	セキュリティ機能の検証	P1	選択されていない	選択されていない	SI-6
SI-7	ソフトウェア・ファームウェア、・情報のそれぞれの完全性	P1	選択されていない	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	スパムからの保護	P2	選択されていない	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	**（削除された）**	---	---	---	---
SI-10	入力の妥当性確認	P1	選択されていない	SI-10	SI-10
SI-11	エラー処理	P2	選択されていない	SI-11	SI-11
SI-12	情報の取り扱いおよび情報の保持	P2	SI-12	SI-12	SI-12
SI-13	予測可能な障害の防止	P0	選択されていない	選択されていない	選択されていない
SI-14	非永続性	P0	選択されていない	選択されていない	選択されていない
SI-15	出力のフィルタリング	P0	選択されていない	選択されていない	選択されていない
SI-16	メモリーの保護	P1	選択されていない	SI-16	SI-16
SI-17	緊急時の順	P0	選択されていない	選択されていない	選択されていない

表 D-3 から表 D-19 までのそれぞれの表は、この文書の付録 F に記載されたセキュリティ管理策およびその拡張管理策についてより詳細に概要を明示するものとして、それぞれが異なったセキュリティ管理策ファミリを対象にとりまとめられている。

なお、表 D-2 は、セキュリティ管理策およびその拡張管理策ののうちベースライン管理策として選択された 3 つの管理策が記載されているに過ぎない一方、表 D-3 から表 D-19 までのそれぞれの表には、該当するセキュリティ管理策ファミリに属する管理策およびその拡張管理策についての情報として、①セキュリティ管理策のベースライン管理策として選択されたセキュリティ管理策およびその拡張管理策（※各表中、選択されたベースライン管理策に関する欄において「x」印で示されているセキュリティ管理策およびその拡張管理策）[93]②何らセキュリティ管理策のベースライン管理策として選択されていない（すなわち、ベースライン管理策として選択することによってより高度な保護を実現することが可能な）セキュリティ管理策およびその拡張管理策（※各表中、選択されたベースライン管理策に関する項目が空白となっているセキュリティ管理策およびその拡張管理策）③この文書の付録 F から削除されたセキュリティ管理策とその拡張管理策（※各表中、削除された管理策に対応する欄において「x」印で示されているセキュリティ管理策およびその拡張管理策）④セキュリティを保証する特性またはセキュリティを保証する属性を有する（すなわち、セキュリティ保証に関する）セキュリティ管理策およびその拡張管理策（※各表中、セキュリティ保証に関する管理策に対応する欄において「x」印で示されているセキュリティ管理策およびその拡張管理策）についての情報が全て盛り込まれている。ちなみに、セキュリティ管理策のベースライン管理策としてセキュリティ保証に関する管理策は、この文書の付録 E においてより詳しく論じられる。従って、セキュリティ管理策のベースライン管理策としてセキュリティ保証に関する管理策を選択することができる（表 E-1 から同 E-3 までを参照）。

[93] この文書の D-3 から D-19 までの表に記載されたセキュリティ管理策のベースライン管理策は、国家安全システム以外のシステムにのみ適用できる。なお、国家安全システムに対するセキュリティ管理策ベースライン管理策は、CNSS Instruction 1253 に記載されている。

表 D-3: 一覧 — アクセス制御

管理策番号	管理策の名称 ※拡張管理策の名称を含む	削除技術	セキュリティ保証	管理策ベースライン管理策		
				低	中	高
AC-1	**アクセス制御のポリシーおよびアクセス制御の手順**		x	x	x	x
AC-2	**アカウント管理**			x	x	x
AC-2 (1)	アカウント管理 | 自動化されたシステムアカウント管理				x	x
AC-2 (2)	アカウント管理 | 一時的アカウントの削除および非常用アカウントの削除				x	x
AC-2 (3)	アカウント管理 |非アクティブアカウントの無効化				x	x
AC-2 (4)	アカウント管理 | 自動化された監査アクション				x	x
AC-2 (5)	アカウント管理 | 非アクティブログアウト					x
AC-2 (6)	アカウント管理 | 動的権限管理					
AC-2 (7)	アカウント管理 |ロースベースのスキーム					
AC-2 (8)	アカウント管理 | 動的アカウント作成					
AC-2 (9)	アカウント管理 | 共有アカウント・グループアカウントに対する使用制限					
AC-2 (10)	アカウント管理 | 共有アカウント資格情報・グループアカウント資格情報を無効にする					
AC-2 (11)	アカウント管理 |利用条件					x
AC-2 (12)	アカウント管理 |通常とは異なる用い方をされたアカウントの監視					x
AC-2 (13)	アカウント管理 | リスクの高い個人が有するアカウントの無効化					x
AC-3	**アクセス強制**			x	x	x
AC-3 (1)	アクセス強制 | 特権的機能への限定的なアクセス	x	AC-6 に統合された。			
AC-3 (2)	アクセス強制 | 二重認証					
AC-3 (3)	アクセス強制| 必須のアクセス制御					
AC-3 (4)	アクセス強制| 任意のアクセス制御					
AC-3 (5)	アクセス強制| セキュリティ関連の情報					
AC-3 (6)	アクセス強制| ユーザ情報とシステム情報の保護	x	MP-4 と SC-28 に統合された。			
AC-3 (7)	アクセス強制| 役割ベースのアクセス制御					
AC-3 (8)	アクセス強制| アクセス権限の失効					
AC-3 (9)	アクセス強制| 管理されたリリース					
AC-3 (10)	アクセス強制|アクセス制御メカニズムを上書きした上で監査する					
AC-4	**情報フローの強制**				x	x
AC-4 (1)	情報フロー制御の強制 | オブジェクトのセキュリティ属性					
AC-4 (2)	情報フロー制御の強制| 処理ドメイン					
AC-4 (3)	情報フロー制御の強制| 動的情報フロー制御					
AC-4 (4)	情報フロー制御の強制| 暗号化された情報の内容をチェックするコンテンツの確認が暗号化された情報					
AC-4 (5)	情報フロー制御の強制| 埋め込みデータのタイプ					
AC-4 (6)	情報フロー制御の強制| メタデータ					
AC-4 (7)	情報フロー制御の強制| 一方向フローメカニズム					
AC-4 (8)	情報フロー制御の強制| セキュリティポリシーフィルタ					
AC-4 (9)	情報フロー制御の強制| 人によるレビュー					

管理策番号	管理策の名称 ※拡張管理策の名称を含む	削除/採択	セキュリティ保証	管理策ベースライン管理策		
				低	中	高
AC-4 (10)	情報フロー制御の強制| セキュリティポリシーフィルタを有効 / 無効にする					
AC-4 (11)	情報フロー制御の強制| セキュリティポリシーフィルタの構成					
AC-4 (12)	情報フロー制御の強制| データタイプ識別子					
AC-4 (13)	情報フロー制御の強制| セキュリティポリシー関連のサブコンポーネントに分解する					
AC-4 (14)	情報フロー制御の強制| セキュリティポリシーフィルタの制約					
AC-4 (15)	情報フロー制御の強制| 認許可されていない情報の検知					
AC-4 (16)	情報フロー制御の強制| 相互接続システム内での情報の転送	x	AC-4 に統合された。			
AC-4 (17)	情報フロー制御の強制|ドメイン認証					
AC-4 (18)	情報フロー制御の強制| セキュリティ属性をバインドする					
AC-4 (19)	情報フロー制御の強制| メタデータの検証					
AC-4 (20)	情報フロー制御の強制| 承認されたソリューション					
AC-4 (21)	情報フロー制御の強制| 情報フローの物理的/・論理的な分離					
AC-4 (22)	情報フロー制御の強制| アクセス専用					
AC-5	**職務の分離**				x	x
AC-6	**最小権限**				x	x
AC-6 (1)	最小権限 | セキュリティ機能へのアクセスを許可する				x	x
AC-6 (2)	最小権限 | 非セキュリティ機能への非特アクセス				x	x
AC-6 (3)	最小権限 | 特権コマンドへのネットワークアクセス					x
AC-6 (4)	最小権限 |別々の処理ドメイン					
AC-6 (5)	最小権限 | 特権アカウント				x	x
AC-6 (6)	最小権限 | 組織ユーザ以外のユーザによる特権アクセス					
AC-6 (7)	最小権限 | ユーザ特権の見直し					
AC-6 (8)	最小権限 | コードの実行するに当たっての特権レベル					
AC-6 (9)	最小権限 | 特権的機能の使用を監査する				x	x
AC-6 (10)	最小権限 | 特権ユーザ以外のユーザによる特権的機能の実行を禁止する				x	x
AC-7	**ログオン試行の失敗**			x	x	x
AC-7 (1)	ログオン試行の失敗 | アカウントの自動ロック	x	AC-7 に統合された。			
AC-7 (2)	ログオン試行の失敗 | 携帯機器のデータを消去または完全消去する					
AC-8	**システム利用通知**			x	x	x
AC-9	**ログオン(アクセス)に関する前回の通知**					
AC-9 (1)	ログオンに関する前回の通知 | ログオンの失敗					
AC-9 (2)	ログオンに関する前回の通知 | ログオンの成功/(あるいは失敗)					
AC-9 (3)	ログオンに関する前回の通知 | アカウント変更通知					
AC-9 (4)	ログオンに関する前回の通知 | 追加のログオン情報					
AC-10	**セッション同時制御**					x
AC-11	**セッションのロック**				x	x
AC-11 (1)	セッションのロック | パターンパターンが表示されていないディスプレイ				x	x

管理策番号	管理策の名称 ※拡張管理策の名称を含む	削除技術	セキュリティ保証	管理策ベースライン管理策		
				低	中	高
AC-12	**セッションの終了**				x	x
AC-12 (1)	セッションの終了 | ユーザによるログアウトおよびそれに伴うメッセージ表示					
AC-13	**アクセス制御の監視および監視結果のレビュー**	x	AC-2 と AU-6 に統合された。			
AC-14	**識別または認証せずに許可されたアクション**			x	x	x
AC-14 (1)	識別または認証せずに許可されたアクション | 必然的な利用	x	AC-14.に統合された。			
AC-15	**自動マーク付け**	x	MP-3 に統合された。			
AC-16	**セキュリティ属性**					
AC-16 (1)	セキュリティ属性 |属性の動的な関連付け					
AC-16 (2)	セキュリティ属性 |正規ユーザによる属性値の変更					
AC-16 (3)	セキュリティ属性 | 情報システムを通じて属性の関連付け~~の~~を維持すること					
AC-16 (4)	セキュリティ属性 |正規ユーザによる属性の関連付け					
AC-16 (5)	セキュリティ属性 | 出力装置のための属性の表示					
AC-16 (6)	セキュリティ属性 | 組織による属性の関連付けの維持					
AC-16 (7)	セキュリティ属性 | 矛盾のない属性の解釈					
AC-16 (8)	セキュリティ属性 |属性を関連付ける特別な方法（技術）					
AC-16 (9)	セキュリティ属性 | 属性を再度関連付ける					
AC-16 (10)	セキュリティ属性 | 許可されている個人による属性の構成					
AC-17	**リモートアクセス**			x	x	x
AC-17 (1)	リモートアクセス | 自動モニタリング・自動制御				x	x
AC-17 (2)	リモートアクセス | 暗号化による情報の機密性および完全性の保護				x	x
AC-17 (3)	リモートアクセス |アクセス制御管理ポイント				x	x
AC-17 (4)	リモートアクセス | 特権コマンド・特権アクセス				x	x
AC-17 (5)	リモートアクセス | 無許可接続を監視する	x	SI-4 に統合された。			
AC-17 (6)	リモートアクセス | 情報の保護					
AC-17 (7)	リモートアクセス | セキュリティ機能へのアクセスに対する追加保護	x	AC-3 (10)に統合された。			
AC-17 (8)	リモートアクセス | セキュアではないネットワークプロトコルの無効化	x	CM-7 に統合された。			
AC-17 (9)	リモートアクセス | リモートアクセスの切断・-無効化					
AC-18	**ワイアレスアクセス**			x	x	X
AC-18 (1)	ワイヤレスアクセス | 認証と暗号化				x	X
AC-18 (2)	ワイヤレスアクセス | 無許可接続を監視する	x	SI-4 に統合された。			
AC-18 (3)	ワイヤレスアクセス：ワイヤレスネットワークの無効化					
AC-18 (4)	ワイヤレスアクセス：ユーザが構成することをできなくする					x
AC-18 (5)	ワイヤレスアクセス：アンテナ・伝送強度					x
AC-19	**携帯機器に対するアクセス制御**			x	x	x
AC-19 (1)	携帯機器に対するアクセス制御 | 書き込み可能な / 持ち運び可能な記憶装置の使用	x	MP-7 に統合された。			
AC-19 (2)	携帯機器に対するアクセス制御 | 私有の持ち運び可能な記憶装置の使用	x	MP-7 に統合された。			
AC-19 (3)	携帯機器に対するアクセス制御 | 所有者が特定できない持ち運び可能な記憶装置の使用	x	MP-7 に統合された。			

管理策番号	管理策の名称 ※拡張管理策の名称を含む	削除採択	セキュリティ保証	管理策ベースライン管理策		
				低	中	高
AC-19 (4)	携帯機器に対するアクセス制御 | 機密情報に対する制限					
AC-19 (5)	携帯機器に対するアクセス制御 | 機器全体の暗号化 / コンテナの暗号化				x	x
AC-20	**外部情報システムの利用**			x	x	x
AC-20 (1)	外部情報システムの使用 | 許可された利用の制限				x	x
AC-20 (2)	外部情報システムの使用 | 持ち運び可能な記憶装置				x	x
AC-20 (3)	外部情報システムの使用 | 組織が所有していないシステム / コンポーネント / デバイス					
AC-20 (4)	外部情報システムの使用 | ネットワーク経由でアクセス可能な記憶装置					
AC-21	**情報共有**				x	x
AC-21 (1)	情報共有 | 自動で意思決定を支援する					
AC-21 (2)	情報共有 | 情報の検索と取得					
AC-22	**一般の人がアクセスできるコンテンツ**			x	x	x
AC-23	**データマイニングからの保護**					
AC-24	**アクセス制御に関する決定**					
AC-24 (1)	アクセス制御に関する決定 | アクセス権限に関する情報を伝送する					
AC-24 (2)	アクセス制御に関する決定 | ユーザまたはプロセスの識別情報を含まない					
AC-25	**リファレンスモニタ**		x			

15

表 D-4: 一覧—「意識向上およびトレーニング」管理策

管理策番号	管理策の名称 ※拡張管理策の名称を含む	選択	説明	管理策ベースライン		
				低	中	高
AT-1	**セキュリティ意識向上およびトレーニングのポリシーと手順**		x	x	x	x
AT-2	**セキュリティ意識向上トレーニング**		x	x	x	x
AT-2 (1)	セキュリティ意識向上トレーニング |実践的な訓練		x			
AT-2 (2)	セキュリティ意識向上トレーニング | インサイダー脅威		x		x	x
AT-3	**役割ベースのセキュリティトレーニング**		x	x	x	x
AT-3 (1)	セキュリティトレーニング | 環境に関する管理策		x			
AT-3 (2)	セキュリティトレーニング | 物理的なセキュリティ管理策		x			
AT-3 (3)	セキュリティトレーニング |実践的な訓練		x			
AT-3 (4)	セキュリティトレーニング | 疑わしい通信と、システムの挙動不審		x			
AT-4	**セキュリティトレーニングレコード**		x	x	x	x
AT-5	**セキュリティ関連のグループやセキュリティ団体と連絡を取り合う**	x	PM-15 に統合された。			

表 D-5: 一覧—「監査および説明責任」管理策

管理策番号	管理策の名称 ※┗拡張管理策の名称を含む	選択	補足	管理策ベースライン管理策		
				低	中	高
AU-1	**監査ポリシーおよび監査手順およびのポリシーと手順**		x	x	x	x
AU-2	**監査イベント**			x	x	x
AU-2 (1)	監査イベント	複数のソースからの監査記録のとりまとめ	x	AU-12 に統合された。		
AU-2 (2)	監査イベント	コンポーネントごとに監査イベントの選択	x	AU-12 に統合された。		
AU-2 (3)	監査イベント	レビューと更新			x	x
AU-2 (4)	監査イベント	特権的機能	x	AC-6 (9)に統合された。		
AU-3	**監査記録の内容**			x	x	x
AU-3 (1)	監査記録の内容	追加の監査情報			x	x
AU-3 (2)	監査記録の内容	予定している監査記録内容の一元的管理				x
AU-4	**監査記録の記憶容量**			x	x	x
AU-4 (1)	監査記録の記憶容量	代替ストレージへの移動				
AU-5	**監査処理異常時の対応**			x	x	x
AU-5 (1)	監査処理が失敗した時の対応	監査記録の記憶容量				x
AU-5 (2)	監査処理が失敗した時の対応	リアルタイムの警告				x
AU-5 (3)	監査処理が失敗した時の対応	トラフィック量の閾値を設定できるようにする				
AU-5 (4)	監査処理が失敗した時の対応	失敗した時のシャットダウン				
AU-6	**監査レビュー・監査分析・監査報告**		x	x	x	x
AU-6 (1)	監査記録のレビュー、分析、報告	プロセスの統合	x		x	x
AU-6 (2)	監査記録のレビュー、分析、報告	自動でセキュリティアラートを発する	x	SI-4 に統合された。		
AU-6 (3)	監査記録のレビュー、分析、報告	監査リポジトリを相互に関連付ける		x	x	x
AU-6 (4)	監査記録のレビュー、分析、報告	一つの場所でのレビューと分析		x		
AU-6 (5)	監査記録のレビュー、分析、報告	統合 / スキャンおよびモニタリング機能		x		x
AU-6 (6)	監査記録のレビュー、分析、報告	物理的モニタリングの結果と相関に関連付ける		x		x
AU-6 (7)	監査記録のレビュー、分析、報告	許可されているアクション		x		
AU-6 (8)	監査記録のレビュー、分析、報告	特権的コマンドとして入力されたテキストのすべての分析		x		
AU-6 (9)	監査記録のレビュー、分析、報告	非技術系の情報源からの情報と相関に関連付ける		x		
AU-6 (10)	監査記録のレビュー、分析、報告	監査レベルの調整		x		
AU-7	**監査削減と監査報告書生成**			x	x	x
AU-7 (1)	監査削減と報告書自動作成	自動処理		x	x	x
AU-7 (2)	監査削減と報告書自動作成	自動での並べ替えと検索				
AU-8	**タイムスタンプ**			x	x	x
AU-8 (1)	タイムスタンプ	信頼できる時間情報源との同期			x	x
AU-8 (2)	タイムスタンプ	二番目に信頼できる時間情報源				
AU-9	**監査情報の保護**			x	x	x

管理策番号	管理策の名称 ※「拡張管理策の名称を含む	変更	削除	管理策ベースライン管理策		
				低	中	高
AU-9 (1)	監査情報の保護 | ハードウェア上、一度だけ書き込み可能な媒体					
AU-9 (2)	監査情報の保護 | 物理的に異なるシステム / コンポーネントに監査記録をバックアップする					x
AU-9 (3)	監査情報の保護 | 暗号化による保護					x
AU-9 (4)	監査情報の保護 | 一部の特権ユーザのによるアクセス				x	x
AU-9 (5)	監査情報の保護 | 二重認証					
AU-9 (6)	監査情報の保護 | 読み出し専用アクセス					
AU-10	**否認防止**		x			x
AU-10 (1)	否認防止 | 身元との関連付け		x			
AU-10 (2)	否認防止 | 情報作成者の身元との結び付けを確認する		x			
AU-10 (3)	否認防止 | チェイン・オブ・カストデイ		x			
AU-10 (4)	否認防止 | 情報レビュー者の身元との結び付けを確認する		x			
AU-10 (5)	否認防止| 電子署名	x	SI-7 に統合された。			
AU-11	**監査記録の保管**			x	x	x
AU-11 (1)	監査記録の保管 | 長期にわたって取り出すことが可能である		x			
AU-12	**監査記録の生成**			x	x	x
AU-12 (1)	監査記録の生成 | システム全体にわたる / 時間相関のある監査証跡					x
AU-12 (2)	監査記録の生成 | 標準化されたフォーマット					
AU-12 (3)	監査記録の生成 | 許可された個人による変更					x
AU-13	**情報開示のモニタリング**		x			
AU-13 (1)	情報開示のモニタリング | 自動化されたツールの使用		x			
AU-13 (2)	情報開示のモニタリング | モニタリング対象サイトの見直し		x			
AU-14	**セッションの監査**		x			
AU-14 (1)	セッションの監査 | システムの起動時		x			
AU-14 (2)	セッションの監査 | 内容を取得 / 記録し、ログファイルに書き込む		x			
AU-14 (3)	セッションの監査 | 遠隔地から見る / 聞く		x			
AU-15	**代替監査機能**					
AU-16	**組織をまたがるる監査**					
AU-16 (1)	組織をまたがる監査 | 識別情報の保持					
AU-16 (2)	組織をまたがる監査 | 監査情報の共有					

表 D-6: 一覧— 「セキュリティアセスメントおよび認可」管理策

管理策番号	管理策の名称 ※拡張管理策の名称を含む	廃棄	説明	管理策ベースライン管理策		
				低	中	高
CA-1	**セキュリティ評価ポリシーおよびセキュリティ評価手順ならびにセキュリティ承認ポリシーおよびセキュリティ承認手順**		x	x	x	x
CA-2	**セキュリティト評価**		x	x	x	x
CA-2 (1)	セキュリティ評価 | 独立性を有する		x		x	x
CA-2 (2)	セキュリティ評価| 特殊な評価		x			x
CA-2 (3)	セキュリティ評価| 外部の組織		x			
CA-3	**システムの相互接続**		x	x	x	x
CA-3 (1)	システムの相互接続 | 非機密扱いの国家安全システムへの接続					
CA-3 (2)	システムの相互接続 | 機密扱いの国家安全システムへの接続					
CA-3 (3)	システムの相互接続 | 非機密扱いの国家安全保障にかかわらないシステムへの接続					
CA-3 (4)	システムの相互接続 | パブリックネットワークへの接続					
CA-3 (5)	システムの相互接続 | 外部のシステムとの接続制限				x	x
CA-4	**セキュリティ証明**	x	CA-2 に統合された。			
CA-5	**行動計画とマイルストーン**		x	x	x	x
CA-5 (1)	行動計画とマイルストーン | 正確かつ最新になることを自動で支援する		x			
CA-6	**セキュリティ承認**		x	x	x	x
CA-7	**継続的なモニタリング**		x	x	x	x
CA-7 (1)	継続的なモニタリング | 独立性が確保されたアセスメント		x		x	x
CA-7 (2)	継続的なモニタリング | アセスメントタイプ	x	CA-2 に統合された。			
CA-7 (3)	継続的なモニタリング | 動向分析		x			
CA-8	**侵入テスト**		x			x
CA-8 (1)	侵入テスト | 独立性を有する侵入エージェントまたは侵入チーム		x			
CA-8 (2)	侵入テスト | レッドチーム訓練		x			
CA-9	**システム内部接続**		x	x	x	x
CA-9 (1)	システムに対する内部接続 | セキュリティコンプライアンスチェック		x			

表 D-7: 一覧 —「構成管理」管理策

管理策番号	管理策の名称 ※拡張管理策の名称を含む	選択	組織	管理策ベースライン管理策		
				低	中	高
CM-1	**構成管理ポリシーおよび構成管理手順**		x	x	x	x
CM-2	**ベースライン管理策の構成**		x	x	x	x
CM-2 (1)	ベースライン管理策の構成 | レビューと更新		x		x	x
CM-2 (2)	ベースライン管理策の構成 | 正確かつ最新になることを自動で支援する		x			x
CM-2 (3)	ベースライン管理策の構成 | 以前の構成を記録しておく		x		x	x
CM-2 (4)	ベースライン管理策の構成 | 許可されていないソフトウェア	x	CM-7 に統合された。			
CM-2 (5)	ベースライン管理策の構成 | 許可されているソフトウェア	x	CM-7 に統合された。			
CM-2 (6)	ベースライン管理策の構成 | 開発環境およびテスト環境		x			
CM-2 (7)	ベースライン管理策の構成 | リスクの高い場所に持ち込まれるシステム、コンポーネント、または機器の設定		x		x	x
CM-3	**構成変更管理**		x		x	x
CM-3 (1)	構成変更管理 | 変更を自動で文書化/ 報告 /禁止する		x			x
CM-3 (2)	構成変更管理 | 変更をテスト / 承認 / 文書化する		x		x	x
CM-3 (3)	構成変更管理 | 変更を自動で実施する					
CM-3 (4)	構成変更管理 | セキュリティ担当者					
CM-3 (5)	構成変更管理 | 自動化されたセキュリティレスポンス					
CM-3 (6)	構成変更管理 | 暗号管理					
CM-4	**セキュリティ影響分析**		x	x	x	x
CM-4 (1)	セキュリティ影響分析 | 切り離されたテスト環境下における分析		x			x
CM-4 (2)	セキュリティ影響分析| セキュリティ機能の確認		x			
CM-5	**変更に対するアクセス制限**				x	x
CM-5 (1)	変更に対するアクセス制限 | アクセス制御を自動で実施 / 確認する					x
CM-5 (2)	変更に対するアクセス制限 | システムに対する変更をレビューする					x
CM-5 (3)	変更に対するアクセス制限 | デジタル署名されたコンポーネント					x
CM-5 (4)	変更に対するアクセス制限 | 二重認証					
CM-5 (5)	変更に対するアクセス制限 | 本番環境における権限を制限する					
CM-5 (6)	変更に対するアクセス制限 | ライブラリに対する権限を制限する					
CM-5 (7)	変更に対するアクセス制限 | セキュリティ対策を自動で実施する	x	SI-7 に統合された。			
CM-6	**設定項目**			x	x	x
CM-6 (1)	設定項目 | 一つの場所から自動で管理 / 適用 / 検証する					x
CM-6 (2)	設定項目 | 不正な変更に対処する					x
CM-6 (3)	設定項目 | 不正な変更を検知する	x	SI-7 に統合された。			
CM-6 (4)	設定項目 | 準拠していることを示す	x	CM-4 に統合された。			
CM-7	**最小機能**			x	x	x
CM-7 (1)	最小機能 | 定期的なレビュー				x	x
CM-7 (2)	最小機能 | プログラムの実行を阻止する				x	x
CM-7 (3)	最小機能 | 登録要件への準拠					
CM-7 (4)	最小機能 | 許可されていないソフトウェア / ブラックリスト化				x	
CM-7 (5)	最小機能 | 許可されているソフトウェア / ホワイトリスト化					x

管理策番号	管理策の名称 ※拡張管理策の名称を含む	選択	説明	管理策ベースライン管理策		
				低	中	高
CM-8	**情報システムコンポーネント一覧**		x	x	x	x
CM-8 (1)	情報システムコンポーネント一覧 | インストール / 削除の際に更新する		x		x	x
CM-8 (2)	情報システムコンポーネント一覧 | 自動で維持管理する		x			x
CM-8 (3)	情報システムコンポーネント一覧 | 許可されていないコンポーネントを自動で検知する		x		x	x
CM-8 (4)	情報システムコンポーネント一覧 | 責任に関する情報		x			x
CM-8 (5)	情報システムコンポーネント一覧 | コンポーネントの記載が重複しないようにする		x		x	x
CM-8 (6)	情報システムコンポーネント一覧 | アセスメントされた設定 / 許可された逸脱		x			
CM-8 (7)	情報システムコンポーネント一覧 | 集中型リポジトリ		x			
CM-8 (8)	情報システムコンポーネント一覧 | 位置を自動で追跡する		x			
CM-8 (9)	情報システムコンポーネント一覧 | システムにコンポーネントを割り当てる		x			
CM-9	**構成管理計画**				x	x
CM-9 (1)	構成管理計画 | 責任の割り当て					
CM-10	**ソフトウェアの使用制限**			x	x	x
CM-10 (1)	ソフトウェアの使用制限 | オープンソースソフトウェア					
CM-11	**ユーザによるソフトウェアのインストール**			x	x	x
CM-11 (1)	ユーザによるソフトウェアのインストール | 不正なインストールが行われた場合の警告					
CM-11 (2)	ユーザによるソフトウェアのインストール | 特権ステータスを持たないユーザによるインストールを禁止する					

表 D-8: 一覧—「緊急時対応計画」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	説明	管理策ベースライン		
				低	中	高
CP-1	**緊急時対応計画のポリシーと手順**		x	x	x	x
CP-2	**緊急時対応計画**			x	x	x
CP-2 (1)	緊急時対応計画 | 関連する計画との調整				x	x
CP-2 (2)	緊急時対応計画 | 能力の計画					x
CP-2 (3)	緊急時対応計画 | 極めて重要なミッション・業務機能を再開する				x	x
CP-2 (4)	緊急時対応計画 | すべてのミッション / 業務機能を再開する					x
CP-2 (5)	緊急時対応計画 | 極めて重要なミッション / 業務機能を継続する					x
CP-2 (6)	緊急時対応計画 | 代替処理 / 保管拠点					
CP-2 (7)	緊急時対応計画 | 外部のサービスプロバイダとの調整					
CP-2 (8)	緊急時対応計画 | 極めて重要な資産を特定する				x	x
CP-3	**緊急時対応トレーニング**		x	x	x	x
CP-3 (1)	緊急時対応トレーニング | イベントのシミュレーション		x			x
CP-3 (2)	緊急時対応トレーニング |自動化されたトレーニング環境		x			
CP-4	**緊急時対応計画のテスト**		x	x	x	x
CP-4 (1)	緊急時対応計画のテスト | 関連する計画との調整		x		x	x
CP-4 (2)	緊急時対応計画のテスト | 代替処理拠点		x			x
CP-4 (3)	緊急時対応計画のテスト | 自動でテストする		x			
CP-4 (4)	緊急時対応計画のテスト | 完全な復旧 / 再構築		x			
CP-5	**緊急時対応計画の更新**	x	CP-2 に統合された。			
CP-6	**代替保管拠点**				x	x
CP-6 (1)	代替保管拠点 | 一次拠点からの切り離し				x	x
CP-6 (2)	代替保管拠点 | 目標復旧時間 / ポイント					x
CP-6 (3)	代替保管拠点 | アクセスできなくなった場合				x	x
CP-7	**代替処理拠点**				x	x
CP-7 (1)	代替処理拠点| 一次拠点からの切り離し				x	x
CP-7 (2)	代替処理拠点 | アクセスできなくなった場合				x	x
CP-7 (3)	代替処理拠点 | サービス優先				x	x
CP-7 (4)	代替処理拠点 | 使用のための準備					x
CP-7 (5)	代替処理拠点 | 同等の情報セキュリティ対策	x	CP-7 に統合された。			
CP-7 (6)	代替処理拠点 | 一次拠点に戻れない					
CP-8	**通信サービス**				x	x
CP-8 (1)	通信サービス | サービス提供の優先順位				x	x
CP-8 (2)	通信サービス | 単一障害点				x	x
CP-8 (3)	通信サービス | 一次 / 代替プロバイダの分離					x
CP-8 (4)	通信サービス | プロバイダの緊急時対応計画					x
CP-8 (5)	通信サービス | 代替通信サービスのテスト					
CP-9	**情報システムのバックアップ**			x	x	x
CP-9 (1)	情報システムのバックアップ | 信頼性・完全性の確認				x	x
CP-9 (2)	情報システムのバックアップ | サンプルを使用して復旧されるかどうかをテストする					x

管理策番号	管理策の名称 拡張管理策の名称	整理	追加	管理策ベースライン		
				低	中	高
CP-9 (3)	情報システムのバックアップ | 極めて重要な情報は、別の記憶装置に保管する					x
CP-9 (4)	情報システムのバックアップ | 不正な変更からの保護	x	CP-9 に統合された。			
CP-9 (5)	情報システムのバックアップ | 代替保管拠点に転送する					x
CP-9 (6)	情報システムのバックアップ | 予備の二次システム					
CP-9 (7)	情報システムのバックアップ | 二重認証					
CP-10	**情報システムの復旧と再構成**			x	x	x
CP-10 (1)	情報システムの復旧と再構成 | 緊急時対応計画のテスト	x	CP-4 に統合された。			
CP-10 (2)	情報システムの復旧と再構成 | トランザクションの回復				x	x
CP-10 (3)	情報システムの復旧と再構成 | 補完的セキュリティ管理策	x	調整を通じて対処される。			
CP-10 (4)	情報システムの復旧と再構成 | 期間内に復旧する					x
CP-10 (5)	情報システムの復旧と再構成 | 障害迂回機能	x	SI-13 に統合された。			
CP-10 (6)	情報システムの復旧と再構成 | コンポーネントの保護					
CP-11	**代替通信プロトコル**					
CP-12	**セーフモード**		x			
CP-13	**代替のセキュリティメカニズム**					

表 D-9: 一覧 —「識別および認証」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	識別	管理策ベースライン		
				低	中	高
IA-1	**識別および認証のポリシーと手順**		x	x	x	x
IA-2	**識別および認証（組織的ユーザ）**			x	x	x
IA-2 (1)	識別および認証（組織的ユーザ）| 特権アカウントに対するネットワークアクセス			x	x	x
IA-2 (2)	識別および認証（組織的ユーザ）| 特権アカウントでないアカウントに対するネットワークアクセス				x	x
IA-2 (3)	識別および認証（組織的ユーザ）| 特権アカウントに対するローカルアクセス				x	x
IA-2 (4)	識別および認証（組織的ユーザ）| 特権アカウントでないアカウントに対するローカルアクセス					x
IA-2 (5)	識別および認証（組織的ユーザ）| グループ認証					
IA-2 (6)	識別および認証（組織的ユーザ）| 特権アカウントに対するネットワークアクセス - 切り離されたデバイス					
IA-2 (7)	識別および認証（組織的ユーザ）| 特権アカウントでないアカウントに対するネットワークアクセス - 切り離されたデバイス					
IA-2 (8)	識別および認証（組織的ユーザ）| 特権アカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性				x	x
IA-2 (9)	識別および認証（組織的ユーザ）| 特権アカウントでないアカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性					x
IA-2 (10)	識別および認証（組織的ユーザ）| シングルサインオン					
IA-2 (11)	識別および認証（組織的ユーザ）| リモートアクセス - 切り離されたデバイス				x	x
IA-2 (12)	識別および認証（組織的ユーザ）| PIV クレデンシャルを受け入れる			x	x	x
IA-2 (13)	識別および認証 | 帯域外認証					
IA-3	**デバイスの識別および認証**				x	x
IA-3 (1)	デバイスの識別および認証 | 暗号を用いた双方向認証					
IA-3 (2)	デバイスの識別および認証 | 暗号を用いた双方向ネットワーク認証	x	IA-3 (1) に統合された。			
IA-3 (3)	デバイスの識別および認証 | アドレスを動的に割り当てる					
IA-3 (4)	デバイスの識別および認証 | デバイス認証					
IA-4	**識別子の管理**			x	x	x
IA-4 (1)	識別子の管理 | パブリック識別子をアカウント識別子として使用するのを禁止する					
IA-4 (2)	識別子の管理 | 管理者による承認					
IA-4 (3)	識別子の管理 | 複数の形態の証明書					
IA-4 (4)	識別子の管理 | ユーザステータスを識別する					
IA-4 (5)	識別子の管理 | 動的な管理					
IA-4 (6)	識別子の管理 | 組織を跨る管理					
IA-4 (7)	識別子の管理 | 本人による登録					
IA-5	**オーセンティケータの管理**			x	x	x
IA-5 (1)	オーセンティケータの管理 | パスワードによる認証			x	x	x
IA-5 (2)	オーセンティケータの管理 | 公開鍵基盤による認証				x	x
IA-5 (3)	オーセンティケータの管理 | 本人、または信任を得ている第三者による登録				x	x

管理策番号	管理策の名称 拡張管理策の名称	選択	追加	管理策ベースライン		
				低	中	高
IA-5 (4)	オーセンティケータの管理 | パスワードの強度についての判断を自動で支援する					
IA-5 (5)	オーセンティケータの管理 | 出荷前にオーセンティケータを変更する					
IA-5 (6)	オーセンティケータの管理| オーセンティケータの保護					
IA-5 (7)	オーセンティケータの管理 | 暗号化されていない静的なオーセンティケータの埋め込みを禁止する					
IA-5 (8)	オーセンティケータの管理 | 複数の情報システム上のアカウント					
IA-5 (9)	オーセンティケータの管理 | 組織を跨いで認証情報を管理する					
IA-5 (10)	オーセンティケータの管理 | 認証情報を動的に関連付ける					
IA-5 (11)	オーセンティケータの管理 | ハードウェアトークンによる認証			x	x	x
IA-5 (12)	オーセンティケータの管理 | 生体認証					
IA-5 (13)	オーセンティケータの管理 | キャッシュされたオーセンティケータの期限切れ					
IA-5 (14)	オーセンティケータの管理 | PKIトラストストアの内容の管理					
IA-5 (15)	オーセンティケータの管理| FICAM 認定の製品およびサービス					
IA-6	**オーセンティケータのフィードバック**			x	x	x
IA-7	**暗号モジュールの認証**			x	x	x
IA-8	**識別および認証（組織的ユーザ以外のユーザ）**			x	x	x
IA-8 (1)	識別および認証（組織的ユーザ以外のユーザ）| 他の政府機関からの PIV クレデンシャルを受け入れる			x	x	x
IA-8 (2)	識別および認証（組織的ユーザ以外のユーザ）| 第三者クレデンシャルを受け入れる			x	x	x
IA-8 (3)	識別および認証（組織的ユーザ以外のユーザ）| FICAM 認定の製品を使用する			x	x	x
IA-8 (4)	識別および認証（組織的ユーザ以外のユーザ）| FICAM 発行のプロファイルを使用する			x	x	x
IA-8 (5)	識別および認証（組織的ユーザ以外のユーザ）| PIV-I クレデンシャルを受け入れる					
IA-9	**サービスの識別および認証**					
IA-9 (1)	サービスの識別および認証 | 情報交換					
IA-9 (2)	サービスの識別および認証 | 判定の伝達					
IA-10	**適応性のある識別および認証**					
IA-11	**再認証**					

表 D-10: 一覧 — 「インシデント対応」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	説明	管理策ベースライン		
				低	中	高
IR-1	**インシデント対応のポリシーと手順**		x	x	x	x
IR-2	**インシデント対応トレーニング**		x	x	x	x
IR-2 (1)	インシデント対応トレーニング | イベントのシミュレーション		x			x
IR-2 (2)	インシデント対応トレーニング | 自動化されたトレーニング環境		x			x
IR-3	**インシデント対応テスト**		x		x	x
IR-3 (1)	インシデント対応のテスト | 自動でテストする		x			
IR-3 (2)	インシデント対応のテスト | 関連する計画との調整		x		x	x
IR-4	**インシデント対応**			x	x	x
IR-4 (1)	インシデント対応 | 自動化されたインシデント対応プロセス				x	x
IR-4 (2)	インシデント対応| 動的な再構成					
IR-4 (3)	インシデント対応 | 業務の継続					
IR-4 (4)	インシデント対応 | 情報を相互に関連付ける					x
IR-4 (5)	インシデント対応 | 情報システムを自動で無効にする					
IR-4 (6)	インシデント対応 | インサイダー脅威 - 特定の能力					
IR-4 (7)	インシデント対応| インサイダー脅威 - 組織内の連携					
IR-4 (8)	インシデント対応 | 外部組織と連携して相互に関連付ける					
IR-4 (9)	インシデント対応 | 動的に対応できる					
IR-4 (10)	インシデント対応 | サプライチェーンとの連携					
IR-5	**インシデントモニタリング監視**		x	x	x	x
IR-5 (1)	インシデントモニタリング監視 | 追跡 / データ収集/分析を自動で行う		x			x
IR-6	**インシデント報告**			x	x	x
IR-6 (1)	インシデント報告|自動で報告する				x	x
IR-6 (2)	インシデント報告 | インシデントに関連する脆弱性					
IR-6 (3)	インシデント報告 | サプライチェーンとの連携					
IR-7	**インシデント対応の支援**			x	x	x
IR-7 (1)	インシデント対応の支援 | 情報の可用性/および支援の可用性を自動で支援する				x	x
IR-7 (2)	インシデント対応の支援 | 外部プロバイダとの調整					
IR-8	**インシデント対応計画**			x	x	x
IR-9	**情報流出対応**					
IR-9 (1)	情報流出対応 | 責任を有する職員					
IR-9 (2)	情報流出対応 |トレーニング					
IR-9 (3)	情報流出対応 | 流出後の活動					
IR-9 (4)	情報流出対応 | 権限のない職員に晒される					
IR-10	**統合情報セキュリティ分析チーム**					

表 D-11: 一覧 — 「メンテナンス」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	説明	管理策ベースライン		
				低	中	高
MA-1	**システムメンテナンスのポリシーと手順**		x	x	x	x
MA-2	**管理されたメンテナンス**			x	x	x
MA-2 (1)	管理されたメンテナンス | 記録内容	x	MA-2 に統合された。			
MA-2 (2)	管理されたメンテナンス | メンテナンス活動を自動で実施する					x
MA-3	**メンテナンスツール**				x	x
MA-3 (1)	メンテナンスツール | ツールを検査する				x	x
MA-3 (2)	メンテナンスツール | 媒体を検査する				x	x
MA-3 (3)	メンテナンスツール | 許可なく撤去されるのを防止する					x
MA-3 (4)	メンテナンスツール | ツールの使用制限					
MA-4	**非局所的なメンテナンス**			x	x	x
MA-4 (1)	非局所的なメンテナンス | 監査とレビュー					
MA-4 (2)	非局所的なメンテナンス | 非局所的なメンテナンスについて記載する				x	x
MA-4 (3)	非局所的なメンテナンス | 同等のセキュリティ / 無害化					x
MA-4 (4)	非局所的なメンテナンス | メンテナンス用セッションの認証 / 切り離し					
MA-4 (5)	非局所的なメンテナンス | 承認と通知					
MA-4 (6)	非局所的なメンテナンス | 暗号化による保護					
MA-4 (7)	非局所的なメンテナンス | リモート接続の確認					
MA-5	**メンテナンス要員**			x	x	x
MA-5 (1)	メンテナンス要員 | 適切なアクセス権限を持たない個人					x
MA-5 (2)	メンテナンス要員 | 機密情報を扱うシステムに対するセキュリティクリアランス					
MA-5 (3)	メンテナンス要員 | 機密情報を扱うシステムに対するアメリカ合衆国国民である必要性					
MA-5 (4)	メンテナンス要員 | 外国籍の人					
MA-5 (5)	メンテナンス要員 | システムとは関連しないメンテナンス					
MA-6	**タイムリーなメンテナンス**				x	x
MA-6 (1)	タイムリーなメンテナンス | 予防的メンテナンス					
MA-6 (2)	タイムリーなメンテナンス |予測的なメンテナンス					
MA-6 (3)	タイムリーなメンテナンス | 予測的なメンテナンスを支援する自動化されたメカニズム					

表 D-12: 一覧 —「媒体の保護」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	組織	管理策ベースライン		
				低	中	高
MP-1	**媒体保護のポリシーおよび手順**		x	x	x	x
MP-2	**媒体に対するアクセス**			x	x	x
MP-2 (1)	媒体に対するアクセス | 自動化されたアクセス制限	x	MP-4 (2) に統合された。			
MP-2 (2)	媒体に対するアクセス | 暗号化による保護	x	SC-28 (1) に統合された。			
MP-3	**媒体のマーキング**				x	x
MP-4	**媒体の保管**				x	x
MP-4 (1)	媒体の保管 | 暗号化による保護	x	SC-28 (1) に統合された。			
MP-4 (2)	媒体の保管 | 自動化されたアクセス制限					
MP-5	**媒体の移動**				x	x
MP-5 (1)	媒体の移動 | 管理された領域外での保護	x	MP-5 に統合された。			
MP-5 (2)	媒体の移動 | 活動の文書化	x	MP-5 に統合された。			
MP-5 (3)	媒体の移動 | 守衛					
MP-5 (4)	媒体の移動 | 暗号化による保護				x	x
MP-6	**媒体の無害化**			x	x	x
MP-6 (1)	媒体の無害化 | レビュー / 承認 / 追跡 / 文書化 / 確認					x
MP-6 (2)	媒体の無害化| 機器のテスト					x
MP-6 (3)	媒体の無害化| 非破壊的な技法					x
MP-6 (4)	媒体の無害化| CUI（管理されている、非機密扱いの情報）	x	P-6 に統合された。			
MP-6 (5)	媒体の無害化| 機密情報	x	MP-6 に統合された。			
MP-6 (6)	媒体の無害化| 媒体の破壊	x	MP-6 に統合された。			
MP-6 (7)	媒体の無害化| 二重認証					
MP-6 (8)	媒体の無害化|リモートで情報を消去する					
MP-7	**媒体の使用**			x	x	x
MP-7 (1)	媒体の使用 | 所有者がいない場合には、使用を禁止する				x	x
MP-7 (2)	媒体の使用 |無害化に対する耐性を有する媒体の使用を禁止する					
MP-8	**媒体のダウングレード**					
MP-8 (1)	媒体のダウングレード | プロセスの文書化					
MP-8 (2)	媒体のダウングレード | 機器のテスト					
MP-8 (3)	媒体のダウングレード | CUI（管理されている、非機密扱いの情報）					
MP-8 (4)	媒体のダウングレード | 機密情報					

表 D-13: 一覧 —「物理面と環境面での保護」管理策

管理策番号	管理策の名称 拡張管理策の名称	廃棄	追加	管理策ベースライン		
				低	中	高
PE-1	**物理面と環境面での保護のポリシーと手順**		x	x	x	x
PE-2	**物理アクセス権限**			x	x	x
PE-2 (1)	物理アクセス権限 | 地位 / 役割に基づいたアクセス					
PE-2 (2)	物理アクセス権限 | 2 つの識別形式					
PE-2 (3)	物理アクセス権限 | 付き添われていないアクセスを制限する					
PE-3	**物理アクセス制御**			x	x	x
PE-3 (1)	物理アクセス制御 | 情報システムに対するアクセス					x
PE-3 (2)	物理アクセス制御 | 施設 / 情報システムの境界					
PE-3 (3)	物理アクセス制御 | 警備員 / アラームによる、継続的なモニタリング					
PE-3 (4)	物理アクセス制御 | 鍵のついている箱					
PE-3 (5)	物理アクセス制御 | 改ざん防止					
PE-3 (6)	物理アクセス制御 | 施設に対する侵入テスト					
PE-4	**伝送媒体に対するアクセス制御**				x	x
PE-5	**出力装置に対するアクセス制御**				x	x
PE-5 (1)	出力装置に対するアクセス制御 | 許可された個人による、出力情報のアクセス					
PE-5 (2)	出力装置に対するアクセス制御 | 個別の ID による出力情報のアクセス					
PE-5 (3)	出力装置に対するアクセス制御 | 出力装置のマーキング					
PE-6	**物理アクセスのモニタリング**		x	x	x	x
PE-6 (1)	物理アクセスのモニタリング | 侵入に対する警報 ／ 監視装置		x		x	x
PE-6 (2)	物理アクセスのモニタリング | 自動化された、侵入検知 / 対応		x			
PE-6 (3)	物理アクセスのモニタリング | ビデオ監視		x			
PE-6 (4)	物理アクセスのモニタリング | 情報システムに対する物理アクセスをモニタリングする		x			x
PE-7	**来客の管理**	x	PE-2 と PE-3 に統合された。			
PE-8	**来客のアクセス記録**		x	x	x	x
PE-8 (1)	来客のアクセス記録 | 記録を自動で保管 / レビューする					x
PE-8 (2)	来客のアクセス記録 | 物理アクセス記録	x	PE-2 に統合された。			
PE-9	**電力設備と電力ケーブル**				x	x
PE-9 (1)	電力設備と電力ケーブル | 予備ケーブル					
PE-9 (2)	電力設備と電力ケーブル | 自動電圧制御					
PE-10	**緊急遮断**				x	x
PE-10 (1)	緊急遮断 | 偶発的な / 不正なアクティブ化	x	PE-10 に統合された。			
PE-11	**非常用電源**				x	x
PE-11 (1)	非常用電源 | 長期間使用可能な代替電源 - 最低限必要な業務能力					x
PE-11 (2)	非常用電源 | 長期間使用可能な代替電源 - 自己完結					
PE-12	**非常用照明**			x	x	x
PE-12 (1)	非常用照明 | 極めて重要なミッション / 業務機能					
PE-13	**防火**			x	x	x
PE-13 (1)	防火 | 火災検知器 / システム					x

管理策番号	管理策の名称 拡張管理策の名称	選択	追加	管理策ベースライン		
				低	中	高
PE-13 (2)	防火 | 消火器 / システム					x
PE-13 (3)	防火 | 自動消火				x	x
PE-13 (4)	防火 | 点検					
PE-14	**温度および湿度の管理**			x	x	x
PE-14 (1)	温度および湿度の管理 | 自動化された制御					
PE-14 (2)	温度および湿度の管理 | 警告/ 通知を伴うモニタリング					
PE-15	**浸水による被害からの保護**			x	x	x
PE-15 (1)	浸水による被害からの保護 | 自動化を支援する					x
PE-16	**搬入と搬出**			x	x	x
PE-17	**代替の仕事場**				x	x
PE-18	**情報システムコンポーネントの設置場所**					x
PE-18 (1)	情報システムコンポーネントの設置場所 | 施設内の設置場所					
PE-19	**情報が漏れること**					
PE-19 (1)	情報が漏れること | 排気と暴風雨に関する国家のポリシーと手順					
PE-20	**資産のモニタリングと追跡**					

表 D-14: 一覧 —「計画作成」管理策

管理策番号	管理策の名称 拡張管理策の名称	吸収	追加	管理策ベースライン		
				低	中	高
PL-1	**セキュリティ計画のポリシーおよび手順**		x	x	x	x
PL-2	**システムセキュリティ計画**		x	x	x	x
PL-2 (1)	システムセキュリティ計画 | 運用概念	x	PL-7 に統合された。			
PL-2 (2)	システムセキュリティ計画 | 機能アーキテクチャ	x	PL-8 に統合された。			
PL-2 (3)	システムセキュリティ計画 | 組織内の他のエンティティ（部署、グループ、人、）と共に計画し、調整を行う		x		x	x
PL-3	**システムセキュリティ計画の更新**	X	PL-2 に統合された。			
PL-4	**行動規範**		x	x	x	x
PL-4 (1)	行動規範 | ソーシャルメディア／ネットワーキングの制限		x		x	x
PL-5	**プライバシー影響のアセスメント**	x	付録 J, AR-2 に統合された。			
PL-6	**セキュリティ関連活動の計画作成**	x	PL-2 に統合された。			
PL-7	**セキュリティの観点からの運用概念**					
PL-8	**情報セキュリティアーキテクチャ**		x		x	x
PL-8 (1)	情報セキュリティアーキテクチャ | 深層防護		x			
PL-8 (2)	情報セキュリティアーキテクチャ |供給業者の多様性		x			
PL-9	**一元的管理**		x			

表 D-15: 一覧 — 「職員によるセキュリティ」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	説明	管理策ベースライン		
				低	中	高
PS-1	**職員によるセキュリティのポリシーと手順**		x	x	x	x
PS-2	**役職ごとのリスク記号**			x	x	x
PS-3	**職員の審査**			x	x	x
PS-3 (1)	職員の審査 | 機密情報					
PS-3 (2)	職員の審査 | 形式的な啓発					
PS-3 (3)	職員の審査 | 特別な保護対策を必要とする情報					
PS-4	**職員の雇用の終了**			x	x	x
PS-4 (1)	職員の雇用の終了 | 雇用終了後の要求事項					
PS-4 (2)	職員の雇用の終了 | 自動化された通知					x
PS-5	**職員の異動**			x	x	x
PS-6	**アクセス契約**		x	x	x	x
PS-6 (1)	アクセス契約 | 特別な保護を必要とする情報	x	S-3 に統合された。			
PS-6 (2)	アクセス契約 | 特別な保護を必要とする機密情報		x			
PS-6 (3)	アクセス契約 | 雇用終了後の要求事項		x			
PS-7	**第三者職員によるセキュリティ**		x	x	x	x
PS-8	**職員に対する制裁**			x	x	x

表 D-16: 一覧 — 「リスクアセスメント」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	組織	管理策ベースライン		
				低	中	高
RA-1	**リスクアセスメントのポリシーと手順**		x	x	x	x
RA-2	**セキュリティカテゴリ**			x	x	x
RA-3	**リスクアセスメント**		x	x	x	x
RA-4	**リスクアセスメントの更新**	x	RA-3 に統合された。			
RA-5	**脆弱性スキャン**		x	x	x	x
RA-5 (1)	脆弱性スキャン | ツールの更新機能		x		x	x
RA-5 (2)	脆弱性スキャン | 定められた頻度で / 新たなスキャンの前に / 特定された場合に更新する		x		x	x
RA-5 (3)	脆弱性スキャン | 適用の広さ / 深さ		x			
RA-5 (4)	脆弱性スキャン | 発見可能な情報		x			x
RA-5 (5)	脆弱性スキャン | 特権的アクセス		x		x	x
RA-5 (6)	脆弱性スキャン | 自動化された傾向分析		x			
RA-5 (7)	脆弱性スキャン | 許可されていないコンポーネントを自動で検出し、通知する	x	CM-8 に統合された。			
RA-5 (8)	脆弱性スキャン | 過去の監査ログをレビューする		x			
RA-5 (9)	脆弱性スキャン | 侵入テストおよび分析	x	CA-8 に統合された。			
RA-5 (10)	脆弱性スキャン | スキャン情報を相互に関連付ける		x			
RA-6	**科学的情報収集対策に関する調査**		x			

表 D-17: 一覧 —「システムおよびサービスの調達」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	組込	管理策ベースライン		
				低	中	高
SA-1	**システムおよびサービスの調達のポリシーと手順**		x	x	x	x
SA-2	**リソースの割り当て**		x	x	x	x
SA-3	**システム開発ライフサイクル**		x	x	x	x
SA-4	**調達プロセス**		x	x	x	x
SA-4 (1)	調達プロセス	セキュリティ管理策の機能特性		x		x	x
SA-4 (2)	調達プロセス	セキュリティ管理策の設計 / 導入に関する情報		x		x	x
SA-4 (3)	調達プロセス	開発手法 / 技法 / プラクティス		x			
SA-4 (4)	調達プロセス	システムにコンポーネントを割り当てる	x	CM-8 (9) に統合された。		
SA-4 (5)	調達プロセス	システム / コンポーネント / サービスの設定		x			
SA-4 (6)	調達プロセス	情報保証製品の使用		x			
SA-4 (7)	調達プロセス	NIAP 認定の保護プロファイル		x			
SA-4 (8)	調達プロセス	継続的にモニタリングするための計画		x			
SA-4 (9)	調達プロセス	使用されている機能 / ポート / プロトコル / サービス		x		x	x
SA-4 (10)	調達プロセス	承認された PIV 製品の利用		x	x	x	x
SA-5	**情報システム文書**			x	x	x	x
SA-5 (1)	情報システム文書	セキュリティ管理策の機能特性	x	SA-4 (1) に統合された。		
SA-5 (2)	情報システム文書	セキュリティ関連の外部システムインターフェース	x	SA-4 (2) に統合された。		
SA-5 (3)	情報システム文書	上位レベル設計	x	SA-4 (2) に統合された。		
SA-5 (4)	情報システム文書	下位レベル設計	x	SA-4 (2) に統合された。		
SA-5 (5)	情報システム文書	ソースコード	x	SA-4 (2) に統合された。		
SA-6	**ソフトウェアの利用の制限**		x	CM-10 と SI-7 に統合された。		
SA-7	**ユーザによるソフトウェアのインストール**		x	CM-11 と SI-7 に統合された。		
SA-8	**セキュリティエンジニアリング原則**			x		x	x
SA-9	**外部情報システムサービス**			x	x	x	x
SA-9 (1)	外部情報システム	リスクアセスメント / 組織による承認		x			
SA-9 (2)	外部情報システム	機能 / ポート / プロトコル / サービスを明確にする		x		x	x
SA-9 (3)	外部情報システム	プロバイダとの間に信頼関係を構築し、維持する		x			
SA-9 (4)	外部情報システム	プロバイダ側と利用者側の利害の一致		x			
SA-9 (5)	外部情報システム	処理拠点、処理拠点、保管拠点、およびサービス拠点		x			
SA-10	**開発者による構成管理**			X		x	x
SA-10 (1)	開発者による構成管理	ソフトウェア / ファームウェアの完全性検証		x			
SA-10 (2)	開発者による構成管理	代替の構成管理プロセス		x			
SA-10 (3)	開発者による構成管理	ハードウェアの完全性検証		x			
SA-10 (4)	開発者による構成管理	信頼できる生成		x			
SA-10 (5)	開発者による構成管理	バージョン管理のための、マッピングの整合性		x			
SA-10 (6)	開発者による構成管理	信頼できる配布		x			
SA-11	**開発者によるセキュリティテストおよび評価**			x		x	x

管理策番号	管理策の名称 拡張管理策の名称	選定	組込	管理策ベースライン		
				低	中	高
SA-11 (1)	開発者によるセキュリティテストおよび評価 | 静的なコード解析		x			
SA-11 (2)	開発者によるセキュリティテストおよび評価 | 脅威分析と脆弱性分析		x			
SA-11 (3)	開発者によるセキュリティテストおよび評価 | アセスメント計画 / エビデンスの独立検証		x			
SA-11 (4)	開発者によるセキュリティテストおよび評価 | 手動でのコードレビュー		x			
SA-11 (5)	開発者によるセキュリティテストおよび評価 | 侵入テスト / 解析		x			
SA-11 (6)	開発者によるセキュリティテストおよび評価 | 攻撃の矢面についてレビューする		x			
SA-11 (7)	開発者によるセキュリティテストおよび評価 | テスト / 評価の範囲を確認する		x			
SA-11 (8)	開発者によるセキュリティテストおよび評価 | 動的なコード解析		x			
SA-12	**サプライチェーンの保護**		x			x
SA-12 (1)	サプライチェーンの保護 | 調達戦略 / ツール / 方法		x			
SA-12 (2)	サプライチェーンの保護 | 供給業者に対するレビュー		x			
SA-12 (3)	サプライチェーンの保護 | 信頼されている配送および倉庫保管	x	SA-12 (1) に統合された。			
SA-12 (4)	サプライチェーンの保護 | 供給業者の多様性	x	SA-12 (13) に統合された。			
SA-12 (5)	サプライチェーンの保護 | 被害を抑える		x			
SA-12 (6)	サプライチェーンの保護 | 調達にかかる時間を最小にする	x	SA-12 (1) に統合された。			
SA-12 (7)	サプライチェーンの保護 | 選択 / 受け入れ / アップデートに先立つアセスメント		x			
SA-12 (8)	サプライチェーンの保護 | あらゆる情報源からの情報の利用		x			
SA-12 (9)	サプライチェーンの保護 | 運用上のセキュリティ		x			
SA-12 (10)	サプライチェーンの保護 | 本物であることと、改変されてないことを確認する		x			
SA-12 (11)	サプライチェーンの保護 | エレメント、プロセス、および関係者の侵入テスト／分析		x			
SA-12 (12)	サプライチェーンの保護 | 組織間の合意		x			
SA-12 (13)	サプライチェーンの保護 | 極めて重要な情報システムコンポーネント		x			
SA-12 (14)	サプライチェーンの保護 | 識別情報と追跡可能性		x			
SA-12 (15)	サプライチェーンの保護 | 弱点または欠陥に対処するためのプロセス		x			
SA-13	**信用性**		x			
SA-14	**クリティカリティ分析**		x			
SA-14 (1)	クリティカリティ分析 | 適切な代替の調達元が存在しない、クリティカルコンポーネント	x	SA-20 に統合された。			
SA-15	**開発プロセス、標準、およびツール**		x			x
SA-15 (1)	開発プロセス、標準、およびツール | 品質の評価指標		x			
SA-15 (2)	開発プロセス、標準、およびツール | セキュリティ追跡ツール		x			
SA-15 (3)	開発プロセス、標準、およびツール | クリティカリティ分析		x			
SA-15 (4)	開発プロセス、標準、およびツール | 脅威のモデル化 / 脆弱性分析		x			
SA-15 (5)	開発プロセス、標準、およびツール | 攻撃の矢面を減らす		x			
SA-15 (6)	開発プロセス、標準、およびツール | 継続的な改善		x			
SA-15 (7)	開発プロセス、標準、およびツール | 自動化された脆弱性分析		x			
SA-15 (8)	開発プロセス、標準、およびツール | 脅威 / 脆弱性情報の再利用		x			

管理策番号	管理策の名称 拡張管理策の名称	選択	組織	管理策ベースライン		
				低	中	高
SA-15 (9)	開発プロセス、標準、およびツール | 実データの使用		x			
SA-15 (10)	開発プロセス、標準、およびツール | インシデント対応計画		x			
SA-15 (11)	開発プロセス、標準、およびツール | 情報システム / コンポーネントをアーカイブする		x			
SA-16	**開発者が提供する訓練**		x			x
SA-17	**開発者によるセキュリティアーキテクチャおよび設計**		x			x
SA-17 (1)	開発者によるセキュリティアーキテクチャおよび設計 | 形式的なポリシーモデル		x			
SA-17 (2)	開発者によるセキュリティアーキテクチャおよび設計 | セキュリティ関連のコンポーネント		x			
SA-17 (3)	開発者によるセキュリティアーキテクチャおよび設計 | 形式的なコレスポンデンス		x			
SA-17 (4)	開発者によるセキュリティアーキテクチャおよび設計 | 非形式的なコレスポンデンス		x			
SA-17 (5)	開発者によるセキュリティアーキテクチャおよび設計 | 概念的にシンプルな設計		x			
SA-17 (6)	開発者によるセキュリティアーキテクチャおよび設計 | テスト構造		x			
SA-17 (7)	開発者によるセキュリティアーキテクチャおよび設計 | 最小権限のための構造		x			
SA-18	**改ざんの防止と検知**		x			
SA-18 (1)	改ざんの防止と検知 | システム開発ライフサイクルの各フェーズ		x			
SA-18 (2)	改ざんの防止と検知 | 情報システム、コンポーネント、または機器の検査		x			
SA-19	**コンポーネントの真正性**		x			
SA-19 (1)	コンポーネントの真正性 | 偽造防止のための訓練		x			
SA-19 (2)	コンポーネントの真正性 | 修復の対象のコンポーネントに対する構成管理		x			
SA-19 (3)	コンポーネントの真正性 | コンポーネントの廃棄		x			
SA-19 (4)	コンポーネントの真正性 | 偽造防止のためのスキャニング		x			
SA-20	**重要なコンポーネントの受託開発**		x			
SA-21	**開発者に対する審査**		x			
SA-21 (1)	開発者に対する審査 | 審査の有効性を確認する		x			
SA-22	**サポートが得られないシステムコンポーネント**		x			
SA-22 (1)	サポートが得られないシステムコンポーネント | 継続的なサポートのための、代替の情報源		x			

表 D-18: 一覧 —「システムおよび通信の保護」管理策

管理策番号	管理策の名称 拡張管理策の名称	廃棄	追加	管理策ベースライン		
				低	中	高
SC-1	**システムおよび通信の保護のポリシーと手順**		x	x	x	x
SC-2	**アプリケーションの分割**		x		x	x
SC-2 (1)	アプリケーションの分割 | 特権ユーザ以外のユーザ向けのインターフェース		x			
SC-3	**セキュリティ機能の分離**		x			x
SC-3 (1)	セキュリティ機能の分離 | ハードウェアの分離		x			
SC-3 (2)	セキュリティ機能の分離 | アクセス / フロー制御機能		x			
SC-3 (3)	セキュリティ機能の分離 | 非セキュリティ機能の数を最小限に抑える		x			
SC-3 (4)	セキュリティ機能の分離 | モジュールの結合度と凝集度		x			
SC-3 (5)	セキュリティ機能の分離 | 重層構造		x			
SC-4	**共有リソース内の情報**				x	x
SC-4 (1)	共有リソース内の情報 | セキュリティレベル	x	SC-4 に統合された。			
SC-4 (2)	共有リソース内の情報 | 処理している期間					
SC-5	**サービス妨害からの保護**			x	x	x
SC-5 (1)	サービス妨害からの保護 | 社内ユーザを限定する					
SC-5 (2)	サービス妨害からの保護 | 予備の容量 / 帯域幅 / その他の予備					
SC-5 (3)	サービス妨害からの保護 | 検知 / モニタリング					
SC-6	**リソースの可用性**		x			
SC-7	**境界保護**			x	x	x
SC-7 (1)	境界保護 | 物理的に切り離されたサブネットワーク	x	SC-7 に統合された。			
SC-7 (2)	境界保護 | 一般からのアクセス	x	SC-7 に統合された。			
SC-7 (3)	境界保護 | アクセスポイント				x	x
SC-7 (4)	境界保護 | 外部通信サービス				x	x
SC-7 (5)	境界保護 | デフォルトで拒否/ 例外的に許可				x	x
SC-7 (6)	境界保護 | 確認された不具合への対応	x	SC-7 (18) に統合された。			
SC-7 (7)	境界保護 | 遠隔装置上での分割トンネルを防止する				x	x
SC-7 (8)	境界保護 | 認証されたプロキシサーバーにトラフィックをルーティングする					x
SC-7 (9)	境界保護 | 脅威となる外向け通信トラフィックを禁止する					
SC-7 (10)	境界保護 | 情報の不正な引き出しを阻止する					
SC-7 (11)	境界保護 | 内向け通信トラフィックを制限する					
SC-7 (12)	境界保護 | ホストベースの保護					
SC-7 (13)	境界保護 | セキュリティツール / メカニズム / 支援コンポーネントの分離					
SC-7 (14)	境界保護 | 不正な物理接続から保護する					
SC-7 (15)	境界保護 | ルート権限でのネットワークアクセス					
SC-7 (16)	境界保護 | コンポーネント / 機器が発見されないようにする					
SC-7 (17)	境界保護 | プロトコルフォーマットの自動遵守					
SC-7 (18)	境界保護 | フェールセキュア		x			x
SC-7 (19)	境界保護 | 組織によって設定されたホストではないホストからの通信を遮断する					
SC-7 (20)	境界保護 | 動的な分離／隔離					

管理策番号	管理策の名称 拡張管理策の名称	選択	追加	管理策ベースライン		
				低	中	高
SC-7 (21)	境界保護 | 情報システムコンポーネントの分離		x			x
SC-7 (22)	境界保護 | 異なるセキュリティドメインに接続できるよう、分離されたサブネットを使用する		x			
SC-7 (23)	境界保護 | プロトコル検証における不具合発生時の、送信者へのフィードバックを無効にする					
SC-8	**伝送される情報の機密性と完全性**				x	x
SC-8 (1)	伝送される情報の機密性と完全性 | 暗号化による、あるいは代替の物理面での保護				x	x
SC-8 (2)	伝送される情報の機密性と完全性 | 伝送前 / 伝送後のハンドリング					
SC-8 (3)	伝送される情報の機密性と完全性 | メッセージの外側を暗号化によって保護する					
SC-8 (4)	伝送される情報の機密性と完全性 | 通信パターンを見えないようにする／無作為化する					
SC-9	**伝送中の機密性**	x	SC-8 に統合された。			
SC-10	**ネットワークの切断**				x	x
SC-11	**高信頼パス**		x			
SC-11 (1)	高信頼パス | 論理的な切り離し		x			
SC-12	**暗号鍵の作成と管理**			x	x	x
SC-12 (1)	暗号鍵の作成と管理 | 可用性					x
SC-12 (2)	暗号鍵の作成と管理 | 対称鍵					
SC-12 (3)	暗号鍵の作成と管理 | 非対称鍵					
SC-12 (4)	暗号鍵の作成と管理 | PKI 証明書	x	SC-12 に統合された。			
SC-12 (5)	暗号鍵の作成と管理 | PKI 証明書/ ハードウェアトークン	x	SC-12 に統合された。			
SC-13	**暗号化による保護**			x	x	x
SC-13 (1)	暗号化による保護 | FIPS によって有効性が確認された暗号技術	x	SC-13 に統合された。			
SC-13 (2)	暗号化による保護 | NSA 認定の暗号技術	x	SC-13 に統合された。			
SC-13 (3)	暗号化による保護 | アクセスが正式に許可されていない個人	x	SC-13 に統合された。			
SC-13 (4)	暗号化による保護 | 電子署名	**x**	SC-13 に統合された。			
SC-14	**一般からのアクセスからの保護**	**x**	AC-2, AC-3, AC-5, SI-3, SI-4, SI-5, SI-7, SI-10 によって提供される機能。			
SC-15	**連携するコンピュータデバイス**			x	x	x
SC-15 (1)	連携するコンピュータデバイス | 物理的な切り離し					
SC-15 (2)	連携するコンピュータデバイス | 内向け / 外向け通信トラフィックを遮断する	x	SC-7 に統合された。			
SC-15 (3)	連携するコンピュータデバイス | 安全な作業領域内での無効化 / 撤去					
SC-15 (4)	連携するコンピュータデバイス | 現在の参加者を明示する					
SC-16	**セキュリティ属性の伝送**					
SC-16 (1)	セキュリティ属性の伝送 | 完全性検証					
SC-17	**PKI 証明書**				x	x
SC-18	**モバイルコード**				x	x
SC-18 (1)	モバイルコード | 許容できないコードを検知し、是正措置を取る					
SC-18 (2)	モバイルコード | 調達 / 開発 / 使用					
SC-18 (3)	モバイルコード | ダウンロード / 実行を防止する					

管理策番号	管理策の名称 拡張管理策の名称	選択	追加	管理策ベースライン		
				低	中	高
SC-18 (4)	モバイルコード | 自動実行を防止する					
SC-18 (5)	モバイルコード | 閉ざされた環境でのみ実行を許可する					
SC-19	**ボイスオーバーインターネットプロトコル**				x	x
SC-20	**セキュアな名前／アドレス解決サービス（信頼できるソース）**			x	x	x
SC-20 (1)	セキュアな名前／アドレス解決サービス（信頼できるソース） | 子サブスペース	x	SC-20 に統合された。			
SC-20 (2)	セキュアな名前／アドレス解決サービス（信頼できるソース) | データ元 / 完全性					
SC-21	**セキュアな名前／アドレス解決サービス (再帰的な問合わせを行うリゾルバ／キャッシングリゾルバ)**			x	x	x
SC-21 (1)	セキュアな名前／アドレス解決サービス(再帰的な問合わせを行うリゾルバ／キャッシングリゾルバ) | データ元 / 完全性	x	SC-21 に統合された。			
SC-22	**名前／アドレス解決サービスの構成およびサービスの提供**			x	x	x
SC-23	**セッションの真正性**				x	x
SC-23 (1)	セッションの真正性 | ログアウト時に、セッション識別子を無効にする					
SC-23 (2)	セッションの真正性 | ユーザが開始したログアウト / メッセージ表示	x	AC-12 (1) に統合された。			
SC-23 (3)	セッションの真正性 | ランダム化を経た一意のセッション識別子					
SC-23 (4)	セッションの真正性 | ランダム化を経た一意のセッション識別子	x	SC-23 (3) に統合された。			
SC-23 (5)	セッションの真正性 | 認可された認証局					
SC-24	**既知の状態に陥ること**		x			x
SC-25	**薄いノード**					
SC-26	**ハニーポット**					
SC-26 (1)	ハニーポット | 悪質コードの検出	x	SC-35 に統合された。			
SC-27	**プラットフォームに依存しないアプリケーション**					
SC-28	**保存されている情報の保護**				x	x
SC-28 (1)	保存されている情報の保護 | 暗号化による保護					
SC-28 (2)	保存されている情報の保護 | オフライン記憶装置					
SC-29	**異種性**		x			
SC-29 (1)	異種性 | 仮想化技術		x			
SC-30	**隠匿、および誤った方向に向けること**		x			
SC-30 (1)	隠匿、および誤った方向に向けること | 仮想化技術	x	SC-29 (1) に統合された。			
SC-30 (2)	隠匿、および誤った方向に向けること | ランダム化		x			
SC-30 (3)	隠匿、および誤った方向に向けること | 処理/ 保管拠点の変更		x			
SC-30 (4)	隠匿、および誤った方向に向けること | 誤った情報を与える		x			
SC-30 (5)	隠匿、および誤った方向に向けること | システムコンポーネントの隠匿		x			
SC-31	**隠れチャネル分析**		x			
SC-31 (1)	隠れチャネル分析 | 隠れチャネルをテストして、利用される可能性を特定する		x			
SC-31 (2)	隠れチャネル分析 | 最大帯域幅		x			
SC-31 (3)	隠れチャネル分析 | システムの運用環境における帯域幅を測定する		x			
SC-32	**情報システムの分割**		x			

管理策番号	管理策の名称 拡張管理策の名称	選定	組込	管理策ベースライン		
				低	中	高
SC-33	**伝送準備段階での完全性**	x	SC-8 に統合された。			
SC-34	**変更できない実行可能プログラム**		x			
SC-34 (1)	変更できない実行可能プログラム | 書き込み可能な記憶装置が使われないようにする		x			
SC-34 (2)	変更できない実行可能プログラム | 完全性の保護 / 読み出し専用媒体		x			
SC-34 (3)	変更できない実行可能プログラム | ハードウェアベースの保護		x			
SC-35	**ハニークライアント**					
SC-36	**分散された処理／保管**		x			
SC-36 (1)	分散された処理／保管 | ポーリング技術		x			
SC-37	**帯域外チャネル**		x			
SC-37 (1)	帯域外チャネル | 確実に届ける / 電子的に送る		x			
SC-38	**運用上のセキュリティ**		x			
SC-39	**プロセスの分離**		x	x	x	x
SC-39 (1)	プロセスの分離 | ハードウェアの分離		x			
SC-39 (2)	プロセスの分離 | スレッドの分離		x			
SC-40	**ワイヤレスリンクの保護**					
SC-40 (1)	ワイヤレスリンクの保護 | 電磁妨害					
SC-40 (2)	ワイヤレスリンクの保護 | 発見される可能性を減らす					
SC-40 (3)	ワイヤレスリンクの保護 | 模倣による、あるいは操作による通信欺騙					
SC-40 (4)	ワイヤレスリンクの保護 | 信号パラメータの特定					
SC-41	**ポートおよび入出力装置に対するアクセス**					
SC-42	**センサー機能およびデータ**					
SC-42 (1)	センサー機能およびデータ | 権限を与えられた個人または役職に報告する					
SC-42 (2)	センサー機能およびデータ | 許可されている用途					
SC-42 (3)	センサー機能およびデータ | 機器の使用を禁止する					
SC-43	**使用制限**					
SC-44	**デトネーションチャンバー**					

表 D-19: 一覧—「システムおよび情報の完全性」管理策

管理策番号	管理策の名称 拡張管理策の名称	選択	組織	管理策ベースライン		
				低	中	高
SI-1	**システムおよび情報の完全性のポリシーと手順**		x	x	x	x
SI-2	**欠陥の修正**			x	x	x
SI-2 (1)	欠陥の修正 | 一元的管理					x
SI-2 (2)	欠陥の修正 | 欠陥修正状況を判断するための自動化されたメカニズム				x	x
SI-2 (3)	欠陥の修正 | 欠陥修正期限 / 是正措置のためのベンチマーク					
SI-2 (4)	欠陥の修正 | 自動化されたパッチ管理ツール	x	SI-2 に統合された。			
SI-2 (5)	欠陥の修正 | 自動化されたソフトウェア / ファームウェアアップデート					
SI-2 (6)	欠陥の修正 | 旧バージョンのソフトウェア / ファームウェアの削除					
SI-3	**悪質コードからの保護**			x	x	x
SI-3 (1)	悪質コードからの保護 | 一元的管理				x	x
SI-3 (2)	悪質コードからの保護 | 自動更新				x	x
SI-3 (3)	悪質コードからの保護 | 特権ユーザ以外のユーザ	x	AC-6 (10) に統合された。			
SI-3 (4)	悪質コードからの保護 | 特権ユーザが指示した場合のみ、更新する					
SI-3 (5)	悪質コードからの保護 | 持ち運び可能な記憶装置	x	MP-7 に統合された。			
SI-3 (6)	悪質コードからの保護 | テスト / 検証					
SI-3 (7)	悪質コードからの保護 | 署名ベースでない検知					
SI-3 (8)	悪質コードからの保護 | 許可されていないコマンドを検知する					
SI-3 (9)	悪質コードからの保護 | リモートコマンドの認証を行う					
SI-3 (10)	悪質コードからの保護 | 悪質コード分析					
SI-4	**情報システムのモニタリング**		x	x	x	x
SI-4 (1)	情報システムのモニタリング | システム全体にわたる侵入検知システム		x			
SI-4 (2)	情報システムのモニタリング | リアルタイム分析のための自動化されたツール		x		x	x
SI-4 (3)	情報システムのモニタリング | 自動化されたツールの統合		x			
SI-4 (4)	情報システムのモニタリング | 内向け／外向けの通信トラフィック		x		x	x
SI-4 (5)	情報システムのモニタリング | システムが生成する警告		x		x	x
SI-4 (6)	情報システムのモニタリング | 特権ユーザ以外のユーザを限定する	x	AC-6 (10) に統合された。			
SI-4 (7)	情報システムのモニタリング | 自動化された、疑わしいイベントに対する対応		x			
SI-4 (8)	情報システムのモニタリング | モニタリング情報の保護	x	SI-4 に統合された。			
SI-4 (9)	情報システムのモニタリング | モニタリングツールのテスト		x			
SI-4 (10)	情報システムのモニタリング | 暗号化された通信の可視性		x			
SI-4 (11)	情報システムのモニタリング | 通信トラフィックを分析し、異常の有無を確認する		x			
SI-4 (12)	情報システムのモニタリング | 自動で警告と勧告を発する		x			
SI-4 (13)	情報システムのモニタリング | トラフィック / イベントパターンを分析する		x			
SI-4 (14)	情報システムのモニタリング | ワイヤレスでの侵入検知		x			
SI-4 (15)	情報システムのモニタリング | 無線－有線通信		x			
SI-4 (16)	情報システムのモニタリング | モニタリング情報を相互に関連付ける		x			

管理策番号	管理策の名称 拡張管理策の名称	選定	組織	管理策ベースライン		
				低	中	高
SI-4 (17)	情報システムのモニタリング | 総合的な状況認識		X			
SI-4 (18)	情報システムのモニタリング | トラフィックを分析し、情報の密かな取り出しの検知		X			
SI-4 (19)	情報システムのモニタリング | 高いリスクをもたらす個人		X			
SI-4 (20)	情報システムのモニタリング | 特権ユーザ		X			
SI-4 (21)	情報システムのモニタリング | 試験採用期間		X			
SI-4 (22)	情報システムのモニタリング | 許可されていないネットワークサービス		X			
SI-4 (23)	情報システムのモニタリング | ホストにベースの機器		X			
SI-4 (24)	情報システムのモニタリング | 侵害の兆候		X			
SI-5	**セキュリティアラート、勧告、およびディレクティブ**		X	X	X	X
SI-5 (1)	セキュリティアラート、勧告、およびディレクティブ | 自動で警告と勧告を発する		X			X
SI-6	**セキュリティ機能の検証**		X			X
SI-6 (1)	セキュリティ機能の検証 | セキュリティテストの失敗についての通知	X	SI-6 に統合された。			
SI-6 (2)	セキュリティ機能の検証 | 分散テストを支援する自動化されたメカニズム					
SI-6 (3)	セキュリティ機能の検証 | 検証結果を報告する					
SI-7	**ソフトウェア、ファームウェア、および情報の完全性**		X		X	X
SI-7 (1)	ソフトウェア、ファームウェア、および情報の完全性 | 完全性チェック		X		X	X
SI-7 (2)	ソフトウェア、ファームウェア、および情報の完全性 | 完全性違反の自動通知		X			X
SI-7 (3)	ソフトウェア、ファームウェア、および情報の完全性 | 一元的に管理される完全性検証ツール		X			
SI-7 (4)	ソフトウェア、ファームウェア、および情報の完全性 | 不正開封の跡がすぐ分かる梱包	X	SA-12 に統合された。			
SI-7 (5)	ソフトウェア、ファームウェア、および情報の完全性 | 自動化された、完全性違反に対する対応		X			X
SI-7 (6)	ソフトウェア、ファームウェア、および情報の完全性 | 暗号化による保護		X			
SI-7 (7)	ソフトウェア、ファームウェア、および情報の完全性 | 検知と対応の一体化		X		X	X
SI-7 (8)	ソフトウェア、ファームウェア、および情報の完全性 | 重要なイベントのチェック機能		X			
SI-7 (9)	ソフトウェア、ファームウェア、および情報の完全性 | ブート処理を検証する		X			
SI-7 (10)	ソフトウェア、ファームウェア、および情報の完全性 | ブートファームウェアの保護		X			
SI-7 (11)	ソフトウェア、ファームウェア、および情報の完全性 | 権限が制限された、閉ざされた環境		X			
SI-7 (12)	ソフトウェア、ファームウェア、および情報の完全性 | 完全性検証		X			
SI-7 (13)	ソフトウェア、ファームウェア、および情報の完全性 | 保護された環境内でのコードの実行		X			
SI-7 (14)	ソフトウェア、ファームウェア、および情報の完全性 | バイナリーコードまたはマシンコード		X			X
SI-7 (15)	ソフトウェア、ファームウェア、および情報の完全性 | コード認証		X			

管理策番号	管理策の名称 拡張管理策の名称	選定	追加	管理策ベースライン		
				低	中	高
SI-7 (16)	ソフトウェア、ファームウェア、および情報の完全性 | モニタリングなしのプロセスの実行に、タイムリミットを課す		x			
SI-8	**スパムからの保護**				x	x
SI-8 (1)	スパムからの保護 | 一元的管理				x	x
SI-8 (2)	スパムからの保護 | 自動更新				x	x
SI-8 (3)	スパムからの保護 | 継続的に学ぶ能力					
SI-9	**情報入力制限**	x	AC-2, AC-3, AC-5, AC-6 に統合された。			
SI-10	**入力情報の妥当性確認**		x		x	x
SI-10 (1)	入力情報の妥当性確認 | 手動によるオーバーライド機能		x			
SI-10 (2)	入力情報の妥当性確認 | エラーのレビュー / 解消		x			
SI-10 (3)	入力情報の妥当性確認 | 予測可能な振る舞い		x			
SI-10 (4)	入力情報の妥当性確認 | やりとりをレビューし、タイミングを調整する		x			
SI-10 (5)	入力情報の妥当性確認 | 入力情報を信頼できる情報源と、認可されたフォーマットに限定する		x			
SI-11	**エラー処理**				x	x
SI-12	**情報の処理および保有**			x	x	x
SI-13	**予測可能な障害の防止**		x			
SI-13 (1)	予測可能な障害の防止 | コンポーネントの権限を委譲する		x			
SI-13 (2)	予測可能な障害の防止 | モニタリングなしのプロセスの実行に、タイムリミットを課す	x	SI-7 (16) に統合された。			
SI-13 (3)	予測可能な障害の防止 | コンポーネント間の手動での委譲		x			
SI-13 (4)	予測可能な障害の防止 | 予備コンポーネントのインストール / 通知		x			
SI-13 (5)	予測可能な障害の防止 | 障害迂回機能		x			
SI-14	**非永続性**		x			
SI-14 (1)	非永続性 | 信頼できる情報源を利用したリフレッシュ		x			
SI-15	**出力情報のフィルタリング**		x			
SI-16	**メモリーの保護**		x		x	x
SI-17	**安全を保証するための手続き**		x			

セキュリティ管理策のベースライン管理策の調整

ベースライン管理策の選択および優先順位コード定義

セキュリティ管理策のベースライン管理策については、SP 800-53 が改定される都度、セキュリティ管理策および／またはその拡張管理策の選択、もしくは選択されたセキュリティ管理策」および／またはその拡張管理策の廃止、あるいは優先順位コード（P コード）の変更といった微調整がなされる可能性がある。なお、当該微調整は、①脅威情報を継続的に収集・分析した内容に加えて、②セキュリティ管理策のベースライン管理策を策定するに当たって前提となった事項を定期的に見直した内容③(特定のオーバーレイをもとに初めて策定した共通の管理策を何らかの形で事後調整しながら、)関係者をひとくくりにできるよう、安全保障関係の情報システムと、安全保障関係以外に関係する情報システム用に共通のセキュリティ管理策のベースライン管理策が初めて策定される事に対する期待④セキュリティ管理策の実装に必要な作業量を妥当な水準となるまで平準化するために行う優先順位コードの定期的な見直しを反映したものとなる。ただし、時間と共に、ダイナミックにより洗練されて大きくなる脅威いう果てしない試練に立ち向かうためにセキュリティ管理策カタログが拡張されるにつれて、組織のセキュリティ計画に関連して必要な特殊化を行うにあたって、組織はオーバーレイにより大きく依存する事になる。

付録 E

保証と信頼性

情報システムの信頼性の水準

セキュリティ保証は、情報システムの信頼性を判断する上で不可欠な要素であり、組織の情報システムにおいてセキュリティを確保する手順と合わせて、また組織の情報システムにおける新たな情報セキュリティポリシーと合わせて、組織の情報システムにおけるセキュリティ機能・セキュリティ上の特徴・セキュリティ慣行・情報セキュリティポリシー・セキュリティメカニズム・セキュリティアーキテクチャのそれぞれが既定のセキュリティポリシーをどれだけ忠実に反映・適用したものであると判断できるかを示す指標である[94]。なお、この付録部分の制定趣旨は下記の通り:

- 組織に対して、情報システム・システムコンポーネント・サービスを調達するに当たってセキュリティ保証要求事項を取り入れるよう促すこと
- ハードウェア・ソフトウェア・ファームウェアのそれぞれの開発者に対して、IT 製品およびシステムとしてより信頼性が高いものの開発につながる開発プラクティスの採用を促すこと
- セキュリティが適正な水準にあるという保証のもとで構築された IT 製品を特定・選択・利用するよう組織に促すことに加えて、システム開発ライフサイクルプロセスのなかでシステムエンジニアリング・セキュリティエンジニアリングのそれぞれの技法として合理的なものを採用するよう組織に促すこと
- ミッションクリティカルな情報システムまたはミッションクリティカルなシステムコンポーネントの内部に信頼性がより高い IT 製品を導入する事によって、情報セキュリティリスクを縮減させる事
- 情報システムの信頼性を維持するために、セキュリティが保証されている事を示すエビデンスを継続的に確保するよう開発者と組織に促す事

連邦政府が保有する情報および連邦政府が保有する情報システムのそれぞれに対する最低限のセキュリティ要求事項については、FIPS Publication 200 において定義されている。組織は、この文書の付録 D に記載されているセキュリティ管理策のうち上位・中位・下位のいずれかのベースライン管理策に関連してセキュリティが保証されている事を示すエビデンスを選択・調整・実装・確保する事で当該要求事項を満たす事ができる[95]。なお、この文書の付録 D に記載されているセキュリティ管理策のうち上位・中位・下位のいずれかのベースライン管理策の中には、連邦政府が保有する情報および連邦政府が保有する情報システムのそれぞれに対して一般的に適用する事が可能な最低限のセキュリティ保証要求事項に対応したセキュリティ保証関連のセキュリティ管理策も含まれる[96]。ただし、APT が（組織の）業

[94] この文書の 2.6 のセクションでは、セキュリティ保証および信頼性という 2 つの概念が紹介されている。また、当該セクションでは、セキュリティ保証および信頼性という 2 つの概念がどのように関連しているかについて示している。なお、信頼性モデルについては当該セクションの図 3 に示されている。

[95] CNSS Instruction 1253 の文書は、安全保障関係のシステム用のセキュリティ管理策のベースライン管理策について記載している。したがって、当該文書の表 E-1 から表 E-3 にわたって指定されている管理策は、それゆえに安全保障の関係者向けに策定されたセキュリティ管理策のベースライン管理策のうちセキュリティ保証関連の管理策とは異なる可能性がある。

[96] ベースライン管理策としてこの文書の付録 D に記載されたセキュリティ管理策のうち一定の管理策が全情報技術・全ユーザ・全プラットフォーム・全組織に共通して必要なセキュリティについて保証しているかどうかを判断するのは、困難である。具体的には、クロスドメイン対応の製品のセキュリティを保証するためには正式な手法を用いることが適切であるのに対して、複雑な航空管制システムや、国土安全保障省からの緊急時への備えに関する情報を提供するウェブサーバーに対しては、異なる保証技術を用いることが適切であると考えられる。ただし、既存のベースライン管理策は、すべてのテクノロジー・ユーザ・プラットフォーム・組織に共通と考えられる最低限のセキュリティを保証する側面を有する。

務・（組織の）資産・個人・他組織・国家にもたらすリスクが増大傾向にある事に加えて現在 APT がもたらしている脅威に鑑みて、組織はこの文書の付録 F に記載されたセキュリティ保証関連のセキュリティ管理策を追加で選択のうえ実装してもよい。また、組織は、当該セキュリティ管理策をこの文書の 3.2 のセクションに記載されている調整に関するガイダンスに基づいて選択することができる。さらに、組織は高水準のセキュリティを保証するオーバーレイを次のいずれかのために作成させるよう、検討することができる（なお、この文書の 3.3 のセクションおよび付録 I を参照のこと）。①クリティカルなミッションおよびミッションクリティカルな機能ならびに特殊な運用環境および特殊な情報技術②クリティカルなミッション③ミッションクリティカルな機能④特定の運用環境⑤情報技術。他方で、組織がセキュリティ保証関連の管理策を充足できない場合には、補完的管理策を提案（例：不完全な技術に基づいたソリューションを補完する管理策として、手順に関するソリューションおよび／または運用に関するソリューションを提案する）しなければ、組織はこれまで実際に培ってきた情報セキュリティの能力に関連してより大きなリスクを負うことになる。

セキュリティ保証の新たな形

この文書の旧版ではセキュリティ保証要件としてもっぱら上位・中位・および下位のそれぞれのベースライン管理策に適用されるより高度な要件として比較的抽象度が高いものについて最低限言及するにとどまっていたものの、この版では、組織内部の情報システムにおけるセキュリティの保証に関連してセキュリティのカテゴリごとに組織が実装できる特定のセキュリティ管理策を付録 F のなかで策定するという根本的に異なるアプローチを採用している。こうしたアプローチを採用する事で、セキュリティ保証要件は満たしやすくなるのみならず、ミッションニーズ・業務ニーズとともに、現在の脅威もしくは今後予測される脅威または独自の運用環境もしくは新技術の利用のいずれかを理由にセキュリティの保証水準を高める事ができるようになる。また、上位・中位・下位のそれぞれのベースライン管理策としてセキュリティの保証に関連する特定のセキュリティ管理策が読みやすい表（E-1・E-2・E-3 の各表）に記載されている事で、組織は、最低限のセキュリティ保証要件を満たすのに必要なセキュリティ管理策をより迅速に定義することができるようになる。

なお、セキュリティの保証に関連して表 E-4 に記載されているセキュリティ管理策のうち任意に適用することが可能な管理策は、情報システム・情報システムコンポーネント・情報システムサービスのそれぞれの開発者がセキュリティを確保する際に利用する専用の仕様言語を組織にもたらす。また、当該管理策は、組織の情報システム（または組織の重要インフラ）に組み入れられるハードウェアコンポーネントの品質を抜本的に向上させるためのものであるのに加えて、組織の情報システム（または組織の重要インフラ）に組み入れられるソフトウェアコンポーネントの品質を抜本的に向上させるためのものであると同時に、組織の情報システム（または組織の重要インフラ）に組み入れられるファームウェアコンポーネントの品質を抜本的に向上させるためのものであって、方法・技法・設計について具体的な形で策定された管理策として設計上考慮すべき事項について策定されたものであり、合理的なシステムエンジニアリング原則および合理的なセキュリティエンジニアリング原則に基づいて策定された管理策である。また、セキュリティの保証に関連した管理策は、それ自体の重要性がより高まっている事を黙示的に示すために策定されたのではない。セキュリティの保証という概念の重要を踏まえて、機能性をさらに保証する管理策ではなくセキュリティをさらに保証するセキュリティ管理策はどれなのかについて理解した場合にのみ、組織は（組織の）業務・（組織の）資産・個人・他組織・国家のそれぞれを保護するセキュリティ管理策の組み合わせを最適な形で選択できるようになる。

セキュリティの保証に関連するベースライン管理策としてこの文書の付録Dに位置付けられたセキュリティ管理策について個別に記載した内容は、下記の通りである。なお、あるセキュリティ管理策がセキュリティ保証に関連する管理策であるか又は機能性に関連する管理策であるかは、当該管理策の全般的な特性をもとに判断される。なお、セキュリティの保証に関連した管理策とは、通常、①プロセス・手順・技法・方法として情報システムをシステムコンポーネント（すなわち、ハードウェア・ソフトウェア・ファームウェア）とともに設計・開発するものについて定義するセキュリティ管理策②システム・コンポーネント・プロセスのそれぞれの品質向上について支援する運用プロセスを提供するセキュリティ管理策③開発活動または運用活動のなかで生成されるセキュリティエビデンスについて規定するセキュリティ管理策④監査・テスト・評価・分析・現状把握・検査・検証・監視等を経て策定されたセキュリティ管理策の有効性（または監査・テスト・評価・分析・現状把握・検査・検証・監視等を経て策定されたセキュリティ管理策が

抱えるリスク）について規定するセキュリティ管理策⑤セキュリティ意識向上・セキュリティトレーニング・セキュリティインシデント対応トレーニング・セキュリティ緊急時対応トレーニングについて規定したセキュリティ管理策として、専門知識・理解とあわせて職員のスキルを向上させる管理策の5つを指す。

一部のセキュリティ管理策については、機能的な特性または機能的な属性を何らかの形で示す場合であっても、セキュリティの保証に関連した管理策として指定される場合がある（SI-4「情報システムの監視」に実例あり）。なお、調整プロセスによってベースライン管理策となる3つのセキュリティ管理策は、情報システム・組織のそれぞれを保護するセキュリティ計画の一部を構成するため、ベースライン管理策としてセキュリティの保証に関係するセキュリティ管理策を策定する際に、セキュリティ機能性とセキュリティの保証とを区別する意義は乏しい[97]。ただし、組織がセキュリティ機能性をより保証する（またはセキュリティ機能性に対する信頼をより高める）ためにおよびセキュリティ能力の保証水準（またはセキュリティ能力の信頼性）をより高めるためにセキュリティ管理策を追加で選択するオプションを行使する場合、セキュリティ機能性とセキュリティの保証とを区別する重要性は高まる。

最低限の保証要件―影響度が低いシステム

保証要件：セキュリティ要求事項の内容からに加えてセキュリティポリシーの内容および要求されるセキュリティ能力の内容から、セキュリティ機能には限界があるという見込みが組織にあることに加えて、広範囲にわたるセキュリティ機能を裏付けるエビデンスの詳細を踏まえて、セキュリティ機能は首尾一貫して完全に正しいという確証を限定的ながらも得られる見込みが組織にあること。

補足的ガイダンス：影響度が低いシステムにおけるセキュリティは、この文書の付録 D に記載されたセキュリティ管理策のうち調整済みの下位のベースライン管理策の実装を通じてセキュリティ機能が確保されることによって保証される。ただし、影響度が低いシステムに対する保証要件（当該システムの一部を構成する IT コンポーネントの保証要件を含む）は、COTS（商用オフザシェルフ）製品の原型および COTS サービスの原型から容易に推認することが可能な保証要件と同一である。影響度が低いシステムにおいてはセキュリティ機能の強度は限定的であることが見込まれるため、詳細なエビデンスに裏打ちされたセキュリティの範囲[98]は最小限度にとどまると同時に、COTS 製品（または COTS サービス）を製造する者・販売する者・再販売する者によって日常的に提供される詳細なエビデンスに裏打ちされたセキュリティの範囲を越える見込みはない。ただし、セキュリティの範囲を裏付ける詳細なエビデンスは、セキュリティ管理策を評価した結果によってさらに補強されるのに加えて、組織の情報システムを運用環境とともに継続的に監視することによって一層の補強がなされる。

なお、技術的な機能以外で重要視されるのは、セキュリティ手順の機能もしくはセキュリティオペレーションの機能またはその両方（具体的には、情報セキュリティポリシーの機能などに加えて、物理的なセキュリティの機能とともに職員によるセキュリティの機能）が完全・正確であるとともに整合性が取れていることに対する一定の信頼である。
なお、下記の表 E-1 には、影響度が低いシステム用のセキュリティ管理策のうちセキュアな開発を保証する管理策がセキュアな運用を保証する管理策とともに保証要件として記載されている。また、組織は下記の E-1 の表に記載されているセキュリティ管理策の一式を（組織的なリスク評価等の）調整プロセスの対象とすることによって、
①セキュリティ保証関連の他のセキュリティ管理策
②上記管理策の拡張管理策
③拡張管理策を含むセキュリティ保証関連の他の管理策

[97] ミッション・業務を保護するうえで不可欠なセキュリティ機能性が信頼できるものである事を示すセキュリティ管理策は誤って撤廃されていない事を確実に示す事ができるよう、組織は、オーバーレイを作成するプロセス等の調整プロセスのなかで、ベースライン管理策としてセキュリティ保証に関連したセキュリティ管理策を入念に策定しなければならない。

[98] NIST Special Publication 800-53A の文書は、セキュリティ管理策をどの程度まで広範囲かつ詳細に評価するかについての情報を提供する。

いずれかのセキュリティ管理策を追加で策定してもよい。

表 E-1:影響度が低いシステム用のセキュリティ管理策のうちセキュリティの保証に関連した管理策[99]

ID	セキュリティ管理策	ID	セキュリティ管理策
AC	AC-1	MP	MP-1
AT	AT-1, AT-2, AT-3, AT-4	PE	PE-1, PE-6, PE-8
AU	AU-1, AU-6	PL	PL-1, PL-2, PL-4
CA	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, CA-9	PS	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-4, CM-8	RA	RA-1, RA-3, RA-5
CP	CP-1, CP-3, CP-4	SA	SA-1, SA-2, SA-3, SA-4, SA-4 (10), SA-5, SA-9
IA	IA-1	SC	SC-1, SC-39
IR	IR-1, IR-2, IR-5	SI	SI-1, SI-4, SI-5
MA	MA-1		

最低限の保証要件—影響度が中程度のシステム

保証要件:セキュリティ要求事項の内容からに加えてセキュリティポリシーの内容および要求されるセキュリティ能力の内容から、セキュリティ機能の強度は中程度であるという見込みが組織にあることに加えて、②広範囲にわたるセキュリティ機能を裏付けるエビデンスの詳細を踏まえて、セキュリティ機能が首尾一貫して完全に正しいという確証を適度に得られる見込みが組織にあること。

補足的ガイダンス:影響度が中程度のシステムにおけるセキュリティ関連の機能性と保証は、この文書の付録 D に記載されたセキュリティ管理策のうち調整済みの中位のベースライン管理策の実装を通じてセキュリティ機能が確保されることによって保証される。影響度が中程度のシステムの保証要件(当該システムの一部を構成する IT コンポーネントの保証要件を含む)は、影響度が低いシステムの保証要件とは別に、メカニズム・能力ともに影響度が低いシステムのそれよりも強力な COTS のセキュリティ機能を組み込むという保証要件が追加されたものであるとともに、なんらかの特別な開発等の要求が場合によっては保証要件として追加される。また、影響度が中程度のシステムの保証要件(当該システムの一部を構成する IT コンポーネントにおける保証要件を含む)は、影響度が低いシステムの保証要件とは別に、よりセキュアな構成を設定するという保証要件が追加されたものであるとともに、実装されたセキュリティ能力に対して何らかの追加評価を要求するという保証要件が追加されたものである。ただし、影響度が中程度のシステムは中程度の機能を発揮することが見込まれることから、セキュリティの詳細な内容をその影響範囲とともに裏付けるエビデンス[100]として生成されたものは影響度が低いシステムについて生成される最小限のエビデンスよりも強固なものである一方、COTS の製造者または COTS の再販業者もしくは COTS ベンダーが提供可能なエビデンスの域を超えない。また、セキュリティの詳細な内容をその範囲とともに裏付けるエビデンスは、セキュリティ管理策を追加評価した結果によってさらに補強されるのだけではなく、組織の情報システムを運用環境とともに継続的にモニタリングすることによってさらに補強される。なお、技術を基盤とした機能以外で重要視されるのは、セキュリティ手順の機能、セキュリティオペレーションの機能またはその両方(具体的には、情報セキュリティポリシーの機能、物理的なセキュリティの機能、職員によるセキュリティの機能等)が完全・正確であって整合性が取れていることに対する一定の信頼である。
下記の表 E-2 には、影響度が中程度のシステムにおける保証要件として、開発におけるセキュリティを保証する管理策および運用におけるセキュリティを保証する管理策が記載されている。組織は、(組織

[99] セキュリティの保証に関連してこの文書の表 E-1 に記載されたセキュリティ管理策は、ベースライン管理策としてこの文書の付録 D に記載された影響度が低いシステム用のセキュリティ管理策のサブセットである。また、影響度が低いシステムに対する最低限の保証要件として FIPS Publication 200 の規格によって義務付けられている要件は、(NIST Special Publication 800-53A の規格におけるエビデンスとしてセキュリティの詳細な内容をその範囲とともに裏付けるものを伴った)当該セキュリティ管理策を実装する事によって満たされる。

[100] NIST Special Publication 800-53A の規格は、セキュリティ管理策をどこまで詳細かつ広範囲に評価するかについての情報を追加で提供している。

的なリスク評価を含む）調整プロセスを通じて、表 E-2 に記載されたセキュリティ管理策の一式にセキュリティ保証関連の他の管理策をその拡張管理策とともに（または抜きで）追加してもよい。

表 E-2：影響度が中程度のシステム用のセキュリティ管理策[101]

ID	セキュリティ管理策	ID	セキュリティ管理策
AC	AC-1	**MP**	MP-1
AT	AT-1, AT-2, **AT-2 (2)**, AT-3, AT-4	**PE**	PE-1, PE-6, **PE-6 (1)**, PE-8
AU	AU-1, AU-6, **AU-6 (1)**, **AU-6 (3)**, **AU-7**, **AU-7 (1)**	**PL**	PL-1, PL-2, **PL-2 (3)**, PL-4, **PL-4 (1)**, **PL-8**
CA	CA-1, CA-2, **CA-2 (1)**, CA-3, CA-5, CA-6, CA-7, **CA-7 (1)**, CA-9	**PS**	PS-1, PS-6, PS-7
CM	CM-1, CM-2, **CM-2 (1)**, **CM-2 (3)**, **CM-2 (7)**, **CM-3**, **CM-3 (2)**, CM-4, CM-8, **CM-8 (1)**, **CM-8 (3), CM-8 (5)**	**RA**	*RA-1, RA-3, RA-5, RA-5 (1), RA-5 (2), RA-5 (5)*
CP	CP-1, CP-3, CP-4, **CP-4 (1)**	**SA**	SA-1, SA-2, SA-3, SA-4, **SA-4 (1)**, **SA-4 (2)**, **SA-4 (9)**, SA-4 (10), SA-5, **SA-8**, SA-9, **SA-9 (2)**, **SA-10**, **SA-11**
IA	IA-1	**SC**	SC-1, **SC-2**, SC-39
IR	IR-1, IR-2, **IR-3**, **IR-3 (2)**, IR-5	**SI**	SI-1, SI-4, **SI-4 (2)**, **SI-4 (4)**, **SI-4 (5)**, SI-5, **SI-7**, **SI-7 (1)**, **SI-7 (7)**, **SI-10**, **SI-16**
MA	MA-1		

[101] この文書の表 E-2 に記載されたセキュリティ保証関連の管理策は、中程度の影響度を有するシステム用のベースライン管理策としてこの文書の付録 D に記載されたセキュリティ管理策のサブセットである。また、FIPS Publication 200 の規格によって義務付けられている影響度が中程度のシステム向けの最低限の保証要件は、（NIST Special Publication 800-53A の規格におけるエビデンスとしてセキュリティの詳細な内容をその範囲とともに裏付けるものを伴った）セキュリティ保証関連の管理策として表 E-2 に記載されたセキュリティ管理策を実装する事によって満たされる。なお、太字のテキストは、影響度の低いベースライン管理策から派生した管理策（すなわち、セキュリティ保証を影響度が中程度のベースライン管理策においてより強固に実現されるよう、影響度が低いセキュリティ管理策に追加されたセキュリティ保証関連の管理策）を表している。

最低限の保証要件—影響度が高いシステム

保証要件：セキュリティ要件の内容に加えてセキュリティポリシーの内容および要求されるセキュリティ能力の内容からセキュリティ機能の強度は高いという見込みが組織にあることに加えて、広範囲にわたるセキュリティ機能を裏付けるエビデンスの詳細を踏まえてセキュリティ機能が首尾一貫して完全に正しいものであるという確証を組織が多分に得られる見込が組織にあること。

補足的ガイダンス：影響度が高いシステムにおけるセキュリティは、この文書の付録 D に記載されたセキュリティ管理策のうち調整済みの高位のベースライン管理策の実装を通じてセキュリティ機能が確保されることによって保証される。影響度が高いシステムの保証要件（当該システムの一部を構成する IT コンポーネントの保証要件を含む）は、影響度が中程度のシステムの保証要件とは別に、隠れた脆弱性が発生する割合を減らすために商用開発のベストプラクティスとして広く認められたものを適用することによって得られた COTS のセキュリティ能力のうちより高度なものを組み込むという保証要件であるとともに、何らかの開発を特別に行うのに加えて実装されたセキュリティ能力を追加評価するという保証要件である。また、影響度が高いシステムにおけるセキュリティ機能の強度は高いことが見込まれるため、セキュリティの詳細な内容をその範囲とともに裏付けるもの[102]として生成されたエビデンスは、影響度が中程度のシステムについて生成されるエビデンスよりも包括的なものである。また、セキュリティの詳細な内容をその範囲とともに裏付けるエビデンスとして生成されたものは、影響度が高いシステムが高い機能を発揮すると見込まれることから、影響度が中程度のシステムについて生成されたそれよりもさらに包括的なものとなる。ただし、エビデンスが COTS の製造者または COTS の再販業者もしくは COTS ベンダーによって提供可能な範囲を依然として超えるものではない可能性があるため、独立したプロバイダによるエビデンス評価を通じてセキュリティをより確実に保証しなければならない可能性がある。セキュリティの詳細な内容をその範囲とともに裏付けるエビデンスは、セキュリティ管理策を追加で評価した結果次第でさらに補強されるのに加えて、組織の情報システムを運用環境とともに継続的に監視することによってさらに補強される。

なお、技術を基盤とした機能以外の機能では、
①情報セキュリティポリシーの機能
②物理的なセキュリティの機能
③職員によるセキュリティの機能
といったセキュリティ手順の機能（および／またはセキュリティオペレーションの機能）に対して高い信頼が寄せられている。

下記の表 E-3 には、影響度が高い情報システムにおける保証要件として、開発におけるセキュリティを保証する管理策が運用におけるセキュリティを保証する管理策とともに記載されている。組織は、（組織的なリスク評価を含む）調整プロセスを通じて、表 E-3 に記載されたセキュリティ管理策の一式にセキュリティを保証する他の管理策をその拡張管理策とともに（または抜きで）追加してもよい。

[102] NIST Special Publication 800-53A の規格は、セキュリティ管理策をどこまで詳細かつ広範囲に評価するかについての情報を追加で提供している。

表 E-3:影響度が高いシステム用のセキュリティ管理策[103]

ID	セキュリティ管理策	ID	セキュリティ管理策
AC	AC-1	**MP**	MP-1
AT	AT-1, AT-2, AT-2 (2), AT-3, AT-4	**PE**	PE-1, PE-6, PE-6 (1), **PE-6 (4)**, PE-8
AU	AU-1, AU-6, AU-6 (1), AU-6 (3), **AU-6 (5)**, **AU-6 (6)**, AU-7, AU-7 (1), **AU-10**	**PL**	PL-1, PL-2, PL-2 (3), PL-4, PL-4 (1), PL-8
CA	CA-1, CA-2, CA-2 (1), **CA-2 (2)**, CA-3, CA-5, CA-6, CA-7, CA-7 (1), **CA-8**, CA-9	**PS**	PS-1, PS-6, PS-7
CM	CM-1, CM-2, CM-2 (1), **CM-2 (2)**, CM-2 (3), CM-2 (7), CM-3, **CM-3 (1)**, CM-3 (2), CM-4, **CM-4 (1)**, CM-8, CM-8 (1), **CM-8 (2)**, CM-8 (3), **CM-8 (4)**, CM-8 (5)	**RA**	RA-1, RA-3, RA-5, RA-5 (1), RA-5 (2), **RA-5 (4)**, RA-5 (5)
CP	CP-1, CP-3, **CP-3 (1)**, CM-3 (2), CP-4, CP-4 (1), **CP-4 (2)**	**SA**	SA-1, SA-2, SA-3, SA-4, SA-4 (1), SA-4 (2), SA-4 (9), SA-4 (10), SA-5, SA-8, SA-9, SA-9 (2), SA-10, SA-11, **SA-12**, **SA-15**, **SA-16**, **SA-17**
IA	IA-1	**SC**	SC-1, SC-2, **SC-3**, **SC-7 (18)**, **SC-7 (21)**, **SC-24**, SC-39
IR	IR-1, IR-2, **IR-2 (1)**, **IR-2 (2)**, IR-3, IR-3 (2), IR-5, **IR-5 (1)**	**SI**	SI-1, SI-4, SI-4 (2), SI-4 (4), SI-4 (5), SI-5, **SI-5 (1)**, **SI-6**, SI-7, SI-7 (1), **SI-7 (2)**, **SI-7 (5)**, SI-7 (7), **SI-7 (14)**, SI-10, SI-16
MA	MA-1		

セキュリティを保証する拡張管理策

この文書におけるこれまでの項目のなかで"Low"・"Moderate"・"High"のそれぞれのレベルのベースライン管理策として分類されたセキュリティ管理策は最低限のセキュリティを保証する管理策であることから、新たなセキュリティ管理策をベースライン管理策として追加することでセキュリティ機能を高めると同時に、セキュリティ機能が首尾一貫して正確なものであるという信頼性を高めて不正侵入・改ざん・すり抜けに対するセキュリティ機能の能力を高めることによって、組織は自己の情報システムにおいて保証されるセキュリティの水準をさらに高めることが可能となるとともに、当該情報システムの信頼性を高めることが出来るようになる。なお、不正侵入・改ざん・すり抜けに対応する能力の高いセキュリティ機能は、当該機能が使用された情報システム(またはシステムコンポーネント)の機密性・完全性・可用性を侵害しようとする敵対者の側に相当量の作業を強いるものとなる。

高度なセキュリティが保証された IT 製品は高価かつ入手が困難な可能性があることから、組織は自らの情報システムをそれぞれ別々のサブシステムに分割することで重要なコンポーネントを切り離してもよい。また、同様の可能性から、組織は情報資源のサブセットとしてより狭義に定義されたものに対してのみ高度なセキュリティを保証する作業を行ってもよい。ただし、高水準のセキュリティを保証する IT ソリューションを確保することが困難な組織は、ミッション・業務を確実に成功させるうえで、高度な脅威から影響を受けにくくなるようクリティカルなミッションおよび/またはクリティカルな業務プロセスを再設計するなど、セキュリティを確保する手順またはセキュリティを確保する運用により大きく依存しなければならない可能性がある。

[103] この文書の表 E-3 に記載されたセキュリティ保証関連の管理策は、影響度の高いシステム用のベースライン管理策としてこの文書の付録 D に記載されたセキュリティ管理策のサブセットである。また、影響度が高いシステム向けの最低限の保証要件として FIPS Publication 200 の規格によって義務付けられている要件は、表 E-3(NIST Special Publication 800-53A の規格におけるエビデンスとしてセキュリティの詳細な内容をその範囲とともに裏付けるものを伴った)セキュリティ保証関連の管理策として表 E-3 に記載されたセキュリティ管理策を実装する事によって満たされる。なお、太字のテキストは、影響力が中程度のベースライン管理策から派生した管理策(すなわち、セキュリティ保証を影響度が高いベースライン管理策においてより強固に実現できるよう、影響度が中程度のセキュリティ管理策に追加されたセキュリティ保証関連の管理策)を表している。

なお、下記の表 E-4 においては、組織がより高水準のセキュリティを確保する上で追加で選択可能な開発活動が追加で選択可能な運用活動とともに SA・SI・CM 等のセキュリティ管理策ファミリとして記載されている。ただし、セキュリティ管理策ファミリは、全ての管理策を網羅することを意図するものではない。調整プロセスのなかで、組織は他のセキュリティ管理策を下記の表 E-4 にモデルとして記載されたセキュリティ管理策のセットとともにセキュリティ保証関連の管理策として指定する選択をしてもよい。

9

表 E-4:セキュリティ管理策の拡張管理策[104]

ID	管理策	ID	管理策
AC	**AC-25**	**MP**	追加で策定されたセキュリティ管理策はなし
AT	**AT-2(1)**, **AT-3**(すべて拡張管理策)	**PE**	**PE-6(2)**, **PE-6(3)**
AU	**AU-6(4)**, **AU-6(7)**, **AU-6(8)**, **AU-6(9)**, **AU-6(10)**, **AU-10**(すべて拡張管理策), **AU-11(1)**, **AU-13**(および拡張管理策), **AU-14**(および拡張管理策)	**PL**	**PL-8**(すべて拡張管理策), **PL-9**
CA	**CA-2(3)**, **CA-5(1)**, **CA-7(3)**, **CA-8**(すべて拡張管理策), **CA-9(1)**	**PS**	**PS-6(2)**, **PS-6(3)**
CM	**CM-2(6)**, **CM-4(2)**, **CM-8(6)**, **CM-8(7)**, **CM-8(8)**, **CM-8(9)**	**RA**	**RA-5(3)**, **RA-5(6)**, **RA-5 (8)**, **RA-5 (10)**, **RA-6**
CP	**CP-3(2)**, **CP-4(3)**, **CP-4(4)**, **CP-12**	**SA**	**SA-4 (3)**, **SA-4 (5)**, **SA-4 (6)**, **SA-4(7)**, **SA-4(8)**, **SA-9(1)**, **SA-9(3)**, **SA-9(4)**, **SA-9(5)**, **SA-10**(すべて拡張管理策), **SA-11**(すべて拡張管理策), **SA-12**(すべて拡張管理策), **SA-13**, **SA-14**, **SA-15**(すべて拡張管理策, **SA-17**(すべて拡張管理策), **SA-18**(および拡張管理策), **SA-19**(および拡張管理策), **SA-20**, **SA-21**(および拡張管理策), **SA-22**(および拡張管理策)
IA	追加で策定されたセキュリティ管理策はなし	**SC**	**SC-2 (1)**, **SC-3**(すべて拡張管理策), **SC-6**, **SC-7(22)**, **SC-11**(および拡張管理策), SC-**29** (および拡張管理策), **SC-30** (および拡張管理策), **SC-31** (および拡張管理策), **SC-32**, **SC-34** (および拡張管理策), **SC-36** (加えて拡張管理策), **SC-37** (および拡張管理策), **SC-38**, **SC-39** (すべて拡張管理策)
IR	**IR-3(1)**	**SI**	**SI-4** (1), **SI-4 (3)**, **SI-4 (7)**, **SI-4 (9)**, **SI-4 (10)**, **SI-4 (11)**, **SI-4 (12)**, **SI-4 (13)**, **SI-4 (14)**, **SI-4 (15)**, **SI-4 (16)**, **SI-4 (17)**, **SI-4 (18)**, **SI-4 (19)**, **SI-4 (20)**, **SI-4 (21)**, **SI-4 (22)**, **SI-4 (23)**, **SI-4 (24)**, **SI-7 (3)**, **SI-7 (6)**, **SI-7 (8)**, **SI-7 (9)**, **SI-7 (10)**, **SI-7 (11)**, **SI-7 (12)**, **SI-7 (13)**, **SI-7 (15)**, **SI-7 (16)**, **SI-10**(すべて拡張管理策), **SI-13**(および拡張管理策), **SI-14**(および拡張管理策), **SI-15**, **SI-17**
MA	追加で策定されたセキュリティ管理策はなし		

[104] この文書の表 E-4 に記載されたセキュリティ保証関連のセキュリティ管理策は、セキュリティ保証をより強固に実現するのに必要な追加管理策（すなわち、セキュリティ保証関連のセキュリティ管理策という体裁のもと、この文書の E-1・E-2・E-3 の各表に示されている最低限の保証水準以上のセキュリティ保証を実現するのに必要なセキュリティ管理策）である。ただし、セキュリティ保証関連のセキュリティ管理策がベースライン管理策として策定されている（すなわち、E-1・E-2・E-3 のいずれかの表に記載されている）にもかかわらず当該管理策の拡張管理策の全てが表 E-4 に記載されている場合、該当する拡張管理策は表 E-4 においては“管理策（ただし、全て拡張管理策）”と表示されている。また、セキュリティ保証関連の管理策がその拡張管理策を含めてベースライン管理策として策定されていない場合、セキュリティ保証関連の管理策は、その拡張管理策を含めて表 E-4 においては全て“管理策（「管理策の拡張管理策を含む）”と表示されている。また、セキュリティ保証関連の管理策のうち特定の管理策の拡張管理策がベースライン管理策の 1 つとして策定されている場合、それ以外選択されなかった残りの関連管理策の拡張管理策が表 E-4 において個別に記載されている。

付録 F

セキュリティ管理策カタログ

セキュリティ管理策・拡張管理策・補足的ガイダンス

この付録 F に記載されたセキュリティ管理策カタログは、組織・情報システムににとって、セーフガードとともに様々な防護対策を提供するものとなる[105]。なお、当該セキュリティ管理策カタログにおける管理策は、連邦法・大統領命令・指令・政策・規制・標準・指針のうち関連したものの遵守するよう促す目的で策定されている[106]。この文書の第 2 章においては、セキュリティ管理策カタログについて、その構成・構造に加えて同じくこの文書の付録 D にセキュリティ管理策およびその拡張管理策をベースライン管理策として当初策定したことの意味について説明されている。また、セキュリティ管理策カタログを構成するセキュリティ管理策は、わずかな例外を除き、政策的・技術的に中立な形で設計されている。このことは、セキュリティ管理策およびその拡張管理策が処理ストレージ・伝送の際における情報の保護に必要な事項としてセーフガード・防護対策についてもっぱら策定したものであるということを意味する。したがって、セキュリティ管理策が適用されるにあたっての技術・利害関係者・運用環境・ミッション・業務機能のうち特定のものに対してガイダンスを提供することはこの文書が扱う範囲を超えることから、この文書の第 3 章に記載されている調整プロセスを利用することに加えて同じくこの文書の付録 I に記載されているオーバーレイを作成することによって対応する。

稀にセキュリティ管理策がモバイル技術・公開鍵基盤・ワイヤレス技術・VOIP 等の特定の技術に対するものである場合、当該技術に関連ある1つのセキュリティ管理策が要求する事項を満たす以前に組織が十分なセキュリティを確実に施すことが大前提となる。また、必要とされるセーフガード（および／または必要とされる防護対策）は、多くの場合、セキュリティ管理策カタログを構成するセキュリティ管理策のうち調整プロセスを利用してセキュリティ計画およびオーバーレイを策定するうえで基本となるベースライン管理策として当初策定された他のセキュリティ管理策のなかから得られる。
なお、NIST Special Publications および NIST Interagency Reports は、組織が特定のセキュリティ計画を作成するにあたっての手引きとなるのと同時に、特定のオーバーレイを作成するにあたっての手引きとなる。また、NIST Special Publications および NIST Interagency Reports は、特定の技術に対して推奨されるセキュリティ管理策を策定する手引きとなると同時に、特定の分野（例：スマートグリッド・ヘルスケア・産業用制御システム・モバイル）向けのアプリケーションに対して推奨されるセキュリティ管理策を策定する手引きとなる。

政策的・技術的に中立なセキュリティ管理策カタログを採用することには、以下のようなメリットがある。

---

[105] セキュリティ管理策カタログのオンライン版は、http://web.nvd.nist.gov/view/800-53/home からも入手できる。

[106] 連邦法・大統領命令・指令・政策・規制・標準・ガイドラインを遵守する組織は、情報セキュリティに関連した注意義務に加えてリスク管理に関連した注意義務を果たさなければならない。なお、情報セキュリティに関連した注意義務には、調整に関するガイダンスを NIST Publications に沿って弾力的に利用できるよう、あらゆる適切な情報をリスク管理プログラムの一環として適切に利用しなければならない事が含まれる。これは、組織のセキュリティ計画に記載されている選択されたセキュリティ管理策が組織のミッション・業務上の要求事項を満たすことを確実にするために必要である。ただし、（組織の）業務・（組織の）資産・個人・他組織・国家に対して現存する脅威に対処するうえで必要十分なメカニズムを備えた安全機能について（同様のメカニズムとして機能する保護対策とともに）開発（策定）・実装・維持するためには、組織による利用可能なリスク管理ツールの利用に加えて、組織による利用可能なリスク管理技術の利用が不可欠である。連邦政府組織全体に加えて連邦政府における全ての情報システムは、プロセス・手順・技術として効果的かつリスクベースのものを採用する事で、現在連邦政府が負っている義務に見合った回復力が確実に確保できるようになると同時に、重要なインフラストラクチャーアプリケーションをサポートするのに必要な回復力が行政の継続性を担保するのに必要な回復力とともに確実に確保できるようになる。

- 組織に対して、組織が自己の情報システムに導入使用されている情報技術に左右されること無く情報を保護しつつミッション／業務を成功に導く上で必要なセキュリティ能力に重きを置くように促す注目するようになる
- 組織が特定の技術、特定の運用環境、特定のミッション、特定の業務機能および特定の利害関係者に対するセキュリティ管理策のそれぞれが適用可能かどうかについて分析出来るようになる
- 組織にが変数パラメータが含まれているセキュリティ管理策の調整プロセスの一環としてセキュリティポリシーを明示するようになる

といった利点がある。

具体的には、スマートフォン・タブレットまたはその他の種類のモバイル機器を利用している組織は、政策的・技術的に中立なセキュリティ管理策カタログを採用することによって上位・中位・下位のいずれかのベースライン管理策として適切なセキュリティ管理策の全てが拡張管理策の全てとともに必要であることを前提に調整プロセスを開始することが見込まれる。なお、調整プロセスの結果、例えばセキュリティ管理策の実装をサポートできる技術ではないといったような様々な理由から特定のセキュリティ管理策が削除される場合がある。ただし、組織のミッションおよび組織の業務機能に与えうる負の影響を理解すること無く管理策を削除することで情報セキュリティリスクが著しく増大する可能性があるため、セキュリティ管理策を削除するに当たっては慎重な分析をすることが望ましい。なお、当該分析は、スマートフォン・タブレットなど新しいモバイル機器（新しいモバイルテクノロジー）の利用を考えている組織が適切な代替管理策を選択するなどの際に効果的なリスクベースの判断を行う上で不可欠なものである。オーバーレイに加えて技術的・政策的に中立なセキュリティ管理策を調整に関するガイダンスとともに用いながらセキュリティ計画を適合させることで、組織の情報セキュリティは部門・技術・運用環境の如何を問わずより費用対効果が高くリスクベースなものとなる。

セキュリティ管理策カタログの内のセキュリティ管理策は、管理策が撤廃・改定または追加されるのに伴い時間と共に変化することが期待されている。なお、セキュリティ計画の安定性を Special Publication 800-53 の実装をサポートする自動化ツールの安定性とともに維持する都合上、セキュリティ管理策の番号は管理策が削除される都度振り直されることはない。ただし、撤廃されたセキュリティ管理策の表記は、履歴を残すためにセキュリティ管理策カタログの内に残る。なお、セキュリティ管理策は、例えば撤廃されたセキュリティ管理策によって提供されていたセキュリティ能力が別のセキュリティ管理策によって提供されるようになったためといったような様々な理由で削除される。また、セキュリティ管理策は撤廃されたセキュリティ管理策によって提供されていたセキュリティ能力が既存の管理策によって不必要であるあるいは提供されるセキュリティと重複するためといった理由またはセキュリティ管理策がもはや必要ないとみなされたためといった理由でも削除される。

セキュリティ管理策カタログの一部を構成するセキュリティ管理策の要求事項が当該管理策の拡張管理策の要求事項において繰り返される場合がありうる。なお、こうした要求事項の繰り返しは、複数のセキュリティ管理策および／または複数の拡張管理策によるセキュリティ要求事項の補強を意図して行われる。具体的には、メンテナンスアクティビィティをリモートで実施する際に要求される強力な識別および強力な認証といった事項は、組織によって実施されるシステムメンテナンスアクティビィティという特定の文脈における要求事項として、この文書における「MA」の管理策ファミリの要求事項となる。また、当該要求事項は、この文書における「IA」の管理策ファミリにもより一般的な形で含まれている。なお、当該要求事項は冗長である（すなわち、重複している）ように見えるものの実際は、相互補完的な内容に構成されている。また、セキュリティプログラムを策定・実装する場合に組織の側からさらなる取り組みが必要となることは想定されていない。

3

実装に関するヒント

新しいセキュリティ管理策およびその拡張管理策は、敵対者がサイバー攻撃を仕掛けるに当たって採用する戦術・技術・手順に関する情報に加えて、脅威に関する全国レベルのデータベースから得られた生の情報とともに脆弱性に関する全国レベルのデータベースから得られた生の情報を利用して策定される。また、ベースライン管理策を含むセキュリティ管理策の改定サイクルのなかで、ベースライン管理策を含むセキュリティ管理策に対して提案されている変更は、セキュリティ管理策カタログに記載された管理策の安定性を望む声とに対する要求に加えて、脅威・脆弱性・攻撃手法・情報技術のそれぞれの変化に対応する必要性に配慮しながら慎重に検討される。なお、全般的な目的は、情報セキュリティの基本的水準を時間の経過とともに向上させることにある。組織は、特定のセキュリティ能力が必要かつこの文書の付録 F（または付録 G）に適切なセキュリティ管理策の記載が見当たらない場合には、新しいセキュリティ管理策を策定してもよい。

セキュリティ管理策クラスの指定について

マネジメントに関するリファレンス・運用に関するリファレンス・テクニカルリファレンス

この文書の付録 F におけるセキュリティ管理策ファミリに属するセキュリティ管理策の多くは管理策の特性を運用の特性に加えて技術の特性とともに多様な特性として持っている事から、クラスを指定する特定の管理策はこの文書の付録 F におけるセキュリティ管理策ファミリから削除されている。ただし、クラスを指定する特定の管理策を個別のセキュリティ管理策および拡張管理策として利用する事または特定の管理策および／またはその拡張管理策のなかの一部分として利用する事が依然として組織にとって有益である可能性がある。なお、セキュリティ管理策のグループ化またはセキュリティ管理策の参照の手段としてクラスを指定する管理策の利用が組織にとって有益である可能性がある。また、クラスを指定するセキュリティ管理策は、①（例えば共通管理策またはハイブリッド管理策として）責任を負う当事者または責任を負う情報システム②（例えば共通管理策またはハイブリッド管理策として）責任を負う当事者または責任を負う情報システム③特定の役割④システムにおける特定のコンポーネントのいずれかに対する組織によるセキュリティ管理策およびその拡張管理策の適用を円滑にする役割を果たす。具体的には、組織は、情報システムに固有のものとして管理クラスに割り当てられたセキュリティ管理策に対する責任を当該情報システムの所有者に帰属すると判断してもよい。また、運用クラスに割り当てられたセキュリティ管理策に対する責任は情報システムセキュリティ責任者(ISSO)に帰属するとし、技術クラスに割り当てられたセキュリティ管理策に対する責任は単独のあるいは複数のシステムアドミニストレータに帰属するとする場合がある。なお、この例はセキュリティ管理策および／またはその拡張管理策に対してクラスを指定がもたらすする潜在的な有用性を示すためのものであり、組織に対して追加のタスクを提案するまたは義務付けるものではない。

注意

システム開発・コンポーネント開発・サービス開発

情報システムの信頼性に加えてサプライチェーンのセキュリティが改めて注目されるなか、システム・コンポーネント・サービスのそれぞれについて業務およびミッションを成功させる上で必要なものを維持しIT業界を活性化させるためには、情報セキュリティ要求事項について明確かつ具体的に表す能力を組織が確実に身に付けていなければならない。Special Publication 800-53においては、情報セキュリティ要求事項について明確かつ具体的に表す能力を組織が確実に身に付けているよう、システムおよびサービスを確保するためのセキュリティ管理策の管理策ファミリ（すなわち、SAファミリ）に属するセキュリティ管理策の一式が情報システム・IT製品・情報システムサービスを開発するための要求事項に対応したセキュリティ管理策として規定されている。その結果、SAファミリに属するセキュリティ管理策の多くは、システム・コンポーネント・およびサービスとしてミッション／業務の成功に必要なものの開発者を対象に策定されている。なお、SAファミリに属するセキュリティ管理策の多くは、システム・コンポーネント・サービスのについて業務およびミッションを成功させる上で必要なものの開発者に対して策定されている。また、組織について再構成する事が重要である。なお、影響を受けるセキュリティ管理策には、SA-8・SA-10・SA-11・SA-15・SA-16・SA-17・SA-20・SA-21などがある。

セキュリティ管理策カタログに関する基本事項

通常、この文書の付録 F（および付録 G）に記載されたセキュリティ管理策は、その拡張管理策とともにポリシーに依存しない管理策かつ実装された技術に依存しない管理策として策定されている。なお、組織が当該セキュリティ管理策に関する情報をその拡張管理策に関する情報とあわせて提供する方法は、以下の 2 つの通り。

- 情報システムのセキュリティ計画（または組織のセキュリティプログラム計画）にセキュリティ管理策の実装に関する詳細な情報（例：プラットフォームへの依存）を明示する方法
- 指定ステートメントおよび選択ステートメントを用いて、選択されたセキュリティ管理策の変数部分に特定の値を設定する方法

組織は、指定ステートメントおよび選択ステートメントによって、組織のセキュリティ要求事項にセキュリティ管理策およびその拡張管理策を適合させることまたは連邦法・大統領命令・指令・政策・規制・標準・指針に由来するセキュリティ要求事項にセキュリティ管理策およびその拡張管理策を適合させる事が可能になる。なお、基本となるセキュリティ管理策のなかの指定ステートメントおよび選択ステートメントにおいて組織が定義した変数として使用されているものは、基本となるセキュリティ管理策の拡張管理策の全てにおいても用いられる。ただし、セキュリティ管理策の拡張管理策は、基本となるセキュリティ管理策の基本的なセキュリティ機能が強化されるものの、セキュリティ管理策により適合させるために指定ステートメントおよび選択ステートメントを用いることの代わりとはならない。また、セキュリティ管理策（およびその拡張管理策）のなかの指定ステートメントにおいては、最小値または最大値が含まれない（例：少なくとも年に 1 度は緊急時対応計画をテストした場合において）。なお、最小値または最大値について、組織は最も信頼のおける参照元として連邦法・大統領命令・指令・規制・政策・標準・指針のいずれかを参照するのが望ましい。ただし、セキュリティ管理策「およびその拡張管理策に最小値および最大値が含まれないことによって、それらの最も信頼のおける参照元に記載された要求事項を遵守する必要性が組織からなくなる事はない。

個別のセキュリティ管理策ファミリのなかの他のセキュリティ管理策を効果的に実装するうえで必要なポリシーについての要求事項はセキュリティ管理策の効果的な実装に必要な手順についての要求事項とともに個別のセキュリティ管理策ファミリの 1 番目のセキュリティ管理策（すなわち、末尾が「1 のセキュリティ管理策）によって策定されるため、個別のセキュリティ管理策ファミリを構成する別のセキュリティ管理策およびその拡張管理策はいずれの要求事項も策定しない。なお、セキュリティ管理策（およびその拡張管理策）のなかの補足的ガイダンスの部分には、FIPS または NIST Special Publications は一切参照されていないのと同時に、要求事項も一切含まれていない。ただし、NIST publications は、個別のセキュリティ管理策の参考文献の部分に含まれている。

連邦政府用の統合情報セキュリティフレームワークを構築するための合同作業グループの取り組みを支援するものとして、この付録 F には、国家のセキュリティ関係の情報システムに対するセキュリティ管理策およびその拡張管理策が含まれている。ただし、セキュリティ関係の情報システムに対するセキュリティ管理策およびその拡張管理策が含まれていることは、国家のセキュリティ関係の情報システムを運用する組織に対してセキュリティ要求事項を課すことを意図するものではなく、国家ののセキュリティ関係の情報システムに対するポリシーを策定する権限を有する連邦政府職員による承認のもとで、組織はセキュリティ管理策をその拡張管理策とともに任意で使用できる。また、この文書の付録 D に記載されているセキュリティ管理策の優先順位（および同じくこの文書の付録 D に記載されているセキュリティ管理策のベースライン管理策）としてこの文書の付録 F におけるセキュリティ管理策の下にある概要ボックスに記載されたものは、国家の情報セキュリティ政策を策定する権限を有する連邦政府職員によって別途指示された場合にのみ、国家のセキュリティ関係の情報システム以外の情報システムにも適用される。

カタログを使用する

組織は、連邦政府の下にある情報システムおよび当該システムの運用環境に対してセキュリティ管理策[107]を FIPS Publication 199・FIPS Publication 200・NIST Special Publications 800-37・NIST Special Publications 800-39 の各文書に従って策定する。なお、FIPS Publication 199 によって義務付けられた通り、連邦政府の下にある情報についてセキュリティを分類することは、連邦政府の情報システムについてセキュリティを分類することとともに RMF の 1 番目のステップである[108]。また、RMF の 2 番目のステップとして、組織は FIPS Publication 200 に規定されている最低限のセキュリティ要求事項を満たすことによって自らの情報システムに対するセキュリティ管理策のベースライン管理策として適切なものを選択する。ただし、この文書の付録 D には、情報システムが与える所定の影響のレベルとしてセキュリティカテゴリを作成するプロセスのなかで決定されたものに対応する 3 つのセキュリティ管理策のベースライン管理策が含まれている[109]。なお、組織はベースライン管理策を選択した後に①共通管理策を定義・指定すること②「スコーピングについての考慮事項」を適用する事③必要に応じて、補完的管理策を選択する事④「選択」ステートメント・「指定」ステートメントにセキュリティ管理策に関する変数の値を設定する事⑤セキュリティ管理策およびその拡張管理策としてセキュリティ管理策カタログのなかから追加されたものによってベースライン管理策を補足する事⑥管理策を実装するにあたり追加の情報を提供することの 6 つによって、ベースライン管理策を調整する。また、組織は、この文書の 3.2 のセクションに記載されていると同時に同じくこの文書の付録 I に記載されているオーバーレイの概念と共に、ベースライン管理策の調整プロセスを利用することができる。なお、NIST Special Publication 800-30 に記載されているように、セキュリティ管理策を選択するプロセスは、リスクを評価することによって行われる[110]。

注意書

暗号技術の利用

この文書の付録 F から選択されたセキュリティ管理策に基づいて情報を保護するのに当たり暗号技術が必要となる場合に組織の情報システムによって事後に暗号技術が実装された場合、暗号技術は該当する連邦法・大統領命令・指令・政策・規制・標準・手引に準拠したものとなる。具体的には、機密情報を保護するため NSA によって認定された暗号技術に加えて、非機密扱いの情報を保護するため FIPS によって有効性が確認された暗号技術とともに、それぞれ FIPS に準拠した NSA 認定の鍵管理技術および NSA 認定の鍵管理プロセスが含まれる。なお、セキュリティ管理策 SC-12 および SC-13 の両セキュリティ管理策は、暗号メカニズムの強度等、適切な暗号メカニズムを選択するに当たっての具体的な情報を提供する。

[107] NIST Special Publication 800-53 に記載されているセキュリティ管理策はオンラインで入手可能であり、NIST のウェブサイト（http://web.nvd.nist.gov/view/800-53/home）からさまざまな形式でダウンロード可能である。

[108] CNSS Instruction 1253 は、国家安全システムににについてセキュリティを分類する上での手引きである。

[109] CNSS Instruction 1253 は、国家安全システムに対するセキュリティ管理策のベースライン管理策についてのガイダンスとなっているのみならず、当該システムに関連してセキュリティ管理策を調整する際の具体的な要求事項についてのガイダンスとなっている。

[110] セキュリティ管理策およびその拡張管理策のうち追加された管理策としてセキュリティ管理策カタログに登場する管理策の中には、いかなる形であれ当初はベースライン管理策として利用されていないものがある。なお、セキュリティ管理策およびその拡張管理策のうち追加された管理策としてセキュリティ管理策カタログに登場する管理策は、組織が利用可能な管理策であると同時に、組織的なリスク評価に応じて必要な保護を提供するためにセキュリティ管理策を調整するプロセスのなかで利用できる管理策である。

ファミリ:アクセス制御

AC-1　アクセス制御ポリシーおよびアクセス制御手順

セキュリティ管理策:組織が

a. [組織が規定する職員を割り当てるまたは組織によって定義された役割を割り当てる]の形で策定・文書化・推進するセキュリティ管理策は以下の通り。
   1. 目的・適用範囲・役割・責任・経営方針に応じてコンプライアンスに対応するアクセス制御ポリシーとして、組織エンティティ間の協調に対応したもの
   2. アクセス制御ポリシーの実装およびアクセス制御管理策の実装を容易にするための手順
b. 最新版をレビューかつ更新するセキュリティ管理策は以下の通り
   1. [組織が規定した周波数を割り当てる]のアクセス制御ポリシー
   2. [組織が規定した周波数を割り当てる]のアクセス制御手順

補足的ガイダンス:当該管理策は、AC ファミリ内で選択されたセキュリティ管理策をその拡張管理策とともに効果的に実装するためのポリシーについての管理策となると同時に、AC ファミリ内で選択されたセキュリティ管理策をその拡張管理策とともに効果的に実装するための手順についての管理策となる。また、当該ポリシーは、前記手順とともに連邦法・大統領命令・指令・規制・政策・標準・手引のうち適用可能なものを反映したポリシーになる。なお、セキュリティプログラムに関連して、組織におけるポリシーは、組織における手順と同様、システム固有のポリシーをシステム固有の順とともに不要なものにする可能性がある。また、AC ファミリ内で選択されたセキュリティ管理策をその拡張管理策とともに効果的に実装するためのポリシーは、組織の全般的な情報セキュリティポリシーの一部に含まれ得ると同時に、特定の組織の複雑な性質を反映して複数となりうる。なお、AC ファミリ内で選択されたセキュリティ管理策をその拡張管理策とともに効果的に実装するための手順は、一般的なセキュリティプログラムとして設定しうると同時に、必要に応じて特定の情報システムのために設定することもできる。なお、組織のリスク管理戦略は、AC ファミリ内で選択されたセキュリティ管理策をその拡張管理策とともに効果的に実装するためのポリシーが C ファミリ内で選択されたセキュリティ管理策をその拡張管理策とともに効果的に実装するための手順とともに策定される上で鍵を握る要素である。また、関連するセキュリティ管理策は、PM-9 である。

拡張管理策:なし

参考文献:

NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位の割り当ておよびベースライン管理策の割り当て:

P1	**低**:AC-1	**中**:AC-1	**高**:AC-1

AC-2　アカウント管理

セキュリティ管理策:組織によるセキュリティ管理策は、下記の通り。

a. 組織のミッションおよび／または組織の業務機能をサポートするために、[組織が定義した情報システムアカウントタイプの割り当て]のタイプの情報システムアカウントを識別・選択する
b. 情報システムアカウントを管理するアカウントマネージャを任命する

c. グループメンバーシップ条件およびロールメンバーシップ条件を設定する

d. 情報システムの利用が許可されたユーザをアカウントごとに（必須のものとして）指定するのに加えて、グループメンバーシップ・ロールメンバープを属性とともにアカウントごとに（必須のものとして）指定するとともに、アクセス許可（すなわちアクセス権限）をアカウントごとに（必須のものとして）定義する

e. 情報システムアカウント作成要求に対して、[指定：組織が定めた職員または役職] [組織が規定した職員の割り当て（または組織によって定義された役割の割り当て）]による承認を必須とする

f. [組織によって規定された手順を割り当てるまたは組織によって定義された条件を割り当てる]に応じて、情報システムアカウントを作成・有効化・変更・無効化・削除する

g. 情報システムアカウントの利用状況を監視する

h. 以下の場合に、アカウントマネージャに通知する

   1. アカウントがもはや必要ではない場合
   2. ユーザアカウントが終了したまたは移行した場合
   3. 個々の情報システムの使い方が変化した場合または知らなければならないことが変化した場合

i. 以下に基づいて、情報システムに対するアクセスを許可する：

   1. 有効なアクセス許可
   2. システムの利用目的
   3. その他、組織、組織のミッションまたは組織の業務機能に必要な属性

j. [指定：組織が規定した周波数の割り当て]のアカウント管理要件に準拠しているかどうか、アカウントを確認する

k. 個人がグループから削除された場合に、共有アカウントの認証情報（展開されている場合）に加えてグループアカウントの資格証明書（展開されている場合）を再発行するためのプロセスを設定する。

補足的ガイダンス：情報システムアカウントには、たとえば、個人アカウント・共有アカウント・グループアカウント・システムアカウント・ゲスト（および／または匿名）アカウント・非常時アカウント・開発者（および／または製造者）アカウント・開発者（および／またはベンダー）アカウント・製造者（および／またはベンダー）アカウント・一時利用アカウント・サービスアカウントといったタイプがある。なお、組織の情報システムが上記に列挙されたセキュリティ管理策のうち「j」の管理策における[組織が規定した周波数の割り当て]のアカウント管理要件の一部を実装する場合がある。また、情報システムの利用を許可されたユーザが誰であるのかは、情報システムのアクセス特権の仕様とともに、セキュリティ計画を構成する他のセキュリティ管理策の要件を反映したものとなる。ただし、情報システムアカウントの管理者権限が必要なユーザは、情報システムアカウントおよび特権的アクセスの承認について責任のある適切なを負う職員（例：システムオーナー・ビジネスオーナー・最高情報セキュリティ責任者。その他、ミッションの責任者も含まれる）から、さらに詳しい審査を受ける。また、組織は、アクセス特権またはその他属性をアカウントごとにおよび／またはアカウントタイプごとに定義してもよい。なお、アクセスを許可するのに必要なその他属性には、例えば、日時によるアクセス制限に加えて、曜日によるアクセス制限および発生場所によるアクセス制限等がある。ただし、①時差②顧客からの要求事項および③旅行の際に要求される事項をサポートするリモートアクセスといった他のアカウント属性を定義するに当っては、組織は情報システムに関する要求事項（例：システムアップグレードおよび定期的なメンテナンス）について考慮するとともに、ミッションの要求事項（および／または業務上の要求事項）について考慮する。これらの因子を考慮しない場合、情報システムの可用性が損なわれる可能性がある。なお、一時利用アカウントおよび非常時アカウントは、短期間の利用を

意図したアカウントであり、直ちにアカウントをアクティベートする必要が無いにもかかわらず短期間の利用を意図したアカウントが必要な場合に、組織は通常通りアカウントをアクティブ化する手順の一環として一時利用アカウントを設定する。また、組織は危機が発生した際ただちにアカウントをアクティブ化する必要性が生じた場合に備えて非常時アカウントを設定する。これにより、非常時アカウントが通常のアカウント認証プロセスを経ずにアクティブ化される場合がある。ただし、非常時アカウントおよび一時利用アカウントは、利用頻度の低いアカウント（例：組織が定義したタスクのうちに使用されるローカルログオンアカウントに加えて、ネットワークリソースが利用できない場合に使用されるローカルログオンアカウント）とは明確に区別される。なお、利用頻度の低いアカウントは依然として利用可能であると同時に、自動的に無効となるまたは特定の日に削除されることはない。ただし、利用頻度の低いアカウントを無効にするまたは非アクティブ化する条件のなかには、①共有するグループアカウント、非常時アカウントまたは一時利用アカウントがもはや必要ではない場合または②個人が引越または死亡した場合等も含まれる。なお、情報システムアカウントの中には、特定のトレーニングが必要なタイプが存在する可能性がある。また、関連するセキュリティ管理策は AC-3・AC-4・AC-5・AC-6・AC-10・AC-17・AC-19・AC-20・AU-9・IA-2・IA-4・IA-5・IA-8・CM-5・CM-6・CM-11・MA-3・MA-4・MA-5・PL-4・SC-13 である。

拡張管理策：

(1) アカウント管理 | 自動化されたシステムアカウント管理

組織は、情報システムアカウントの管理をサポートする目的で自動化されたメカニズムを使用する。

補足的ガイダンス：自動化されたメカニズムを利用するということには、たとえば、ユーザが死亡したまたは引っ越した場合にアカウントマネージャに対して自動的に通知する目的で電子メールまたはテキストメッセージを利用するということに加えて、アカウント利用状況について監視するすることとともに異常なシステムアカウント利用についてレポートするために電話通知を利用することなども含まれる可能性がある。

(2) アカウント管理 | 一時利用（または緊急）アカウントの削除

情報システムは、一時利用アカウントおよび緊急アカウントを［指定：それぞれのタイプのアカウントに対して組織が定めた期間］の経過後に、自動的に［選択：削除する無効にする］。

補足的ガイダンス：この拡張管理策は、一時利用アカウントおよび緊急アカウントの両方について、所定期間の経過後にシステムアドミニストレータの都合よりも優先して自動的に削除することを要求する。

(3) アカウント管理 | 使用されていないアカウントを無効にする

情報システムは、使用されていないアカウントを［組織が定めた期間の指定］が経過した時点で、自動的に無効にする。

(4) アカウント管理 | 自動監査

情報システムは、アカウント作成・アカウント変更・アカウント削除について、アカウントの無効化および無効化とともに自動的に監査すると同時に、[組織が定めた職員または役職の指定]に通知する。

補足的ガイダンス：関連するセキュリティ管理策は AU-2 および AU-12 の管理策である。

(5) アカウント管理 |アイドルログアウト

組織は、［指定：組織が定めたアクティブでない期間が経過した場合や、組織が定めたログアウトすべき時が来た場合に］ユーザがログアウトすることを要求する。

補足的ガイダンス：関連するセキュリティ管理策は SC-23 である。

(6) アカウント管理| 動的な権限管理

[指定:組織が定めた動的な権限管理機能の一覧]の動的な権限管理機能が情報システムによって実装される

補足的ガイダンス:情報システムの静的アカウントを一連の定義済みのユーザ権限とともに用いる通常のアクセス制御のアプローチとは対照的に、動的なアクセス制御のアプローチ(例:サービス指向型アーキテクチャ)とは、アクセス権を動的に管理することによるランタイムのアクセス管理に他ならない。ユーザ情報は長期にわたってどちらかといえば不変であるにも関わらず、ユーザ権限は組織が現在進めているミッションおよび/または組織が現在遂行している業務上の要求事項と併せて運用ニーズに基づいてより一層頻繁に変わる。なお、アクセス権限の動的管理には、例えば、ユーザが持つ権限を即座に取り消すことがある。これは、権限になんらかの変更が合った場合に、その変更を反映するために、ユーザ側にセッションの終了と再開を要求することとは対照的である。動的な権限管理は、また、ユーザのプロファイルを編集することとは対照的に、動的なルールに基づいてユーザの権限を変更するメカニズムを指す場合がある。この種の権限管理には、たとえば、ユーザが通常の勤務時間外に作業を行う場合や、情報システムが圧迫されている、あるいは緊急のメンテナンスを要する場合に、権限を自動的に調整することがある。この拡張管理策は、また、権限の変更(たとえば、通信に使用されている暗号鍵の変更)がもたらす付属的な影響も取り扱う。動的な権限管理は、情報システムの耐性に関する要求事項を支援する。なお、関連するセキュリティ管理策は AC-16 である。

(7) アカウント管理| 役割に基づいたスキーム

組織は、以下の行為を行う:

(a) **情報システムへのアクセスがその役割となる役割ベースのアクセススキームに従って、特権ユーザアカウントを作成・管理する**

(b) **特権ロールの割り当てを監視する**

(c) **特権ロールの割り当てがもはや適切でない場合に、[組織が定義したアクションの割り当て]を講ずる。**

補足的ガイダンス:特権ロールは、組織が定義した役割として、許可されていない通常のユーザが特定のセキュリティ関連機能を実施できるよう個人に割り当てられたものである。ここでいう特権ロールには、例えば、鍵管理・アカウント管理・ネットワーク(およびシステム)管理・データベース管理・ウェブ管理がある。

(8) アカウント管理 | 動的なアカウント作成

情報システムは、[組織が定めた情報システムアカウントを割り当てる]を動的に作成する。

補足的ガイダンス:サービス指向型アーキテクチャの内部で実装されたように、情報システムアカウントを動的に作成するアプローチは、かつては未知のエンティティを実行するなかでアカウント(ID)を作成出来るかどうかに掛かっている。組織は情報システムアカウントへのアクセス許可および当該アカウントへのアクセス権限を適切な関係機関との間で信頼関係(信頼メカニズム)を築くことによってアカウントを動的に作成することを通じて検証する。なお、関連するセキュリティ管理策は AC-16 である。

(9) アカウント管理 | 共有グループおよび/または共有アカウントを利用するにあたっての制約

組織は共有アカウントおよび/またはグループアカウントのうち[共有アカウントおよび/またはグループアカウントを作成するために組織が定めた条件を割り当てる]を満たすアカウントの利用のみを許可する。

(10) アカウント管理 | 共有アカウントの資格情報および／またはグループアカウントの資格情報を無効にする

メンバーがグループを離れた場合、情報システムは共有アカウントの資格情報および／またはグループアカウントの資格情報を無効にする。

(11) アカウント管理| 使用条件

情報システムは、[組織で定義した情報システムアカウントを割り当てる]ために、[組織が定義した circumstance および／または組織所定の使利用条件を割り当てる]を強制する。

補足的ガイダンス：組織は、情報システムアカウントが利用可能な特定の条件または特定の circumstance を特定の曜日または特定の時間帯または特定の期間に限って利用することなどによって示すことができる。

(12) アカウント管理| アカウントの監視についておよび特殊な使い方について

組織は、以下を行う:

(a) [組織が特殊な使い方を指定(定義)する]ために情報システムアカウントを監視する

(b) [組織が職員または役割を指定（定義）する]ために、情報システムアカウントの特殊な使い方を報告する。

補足的ガイダンス：例えば、ある特定の時間に組織内で働いている個人が通常の利用パターンの際とは異なる場所から情報システムへアクセスするといったことも、特殊な使い方に含まれる。なお、関連するセキュリティ管理策は、CA-7 である。

(13) アカウント管理| リスクの高い個人のアカウントを無効にする

リスクを発見するために[組織が期間を指定（定義）する]期間のうちに、組織は、重大なリスクをもたらすユーザのアカウントを無効にする。

補足的ガイダンス：組織に対して重大なリスクをもたらすユーザには、確固たる証拠（または確かな情報）によって情報システムへのアクセス許可を悪用して害を及ぼそうとしていることまたは害を及ぼす敵対者であることが明白となった個人等が含まれる。ただし、ここでいう害には、組織の業務（および組織の資産）が被る可能性のある負の影響に加えて、個人・他組織・国家のいずれかが被る可能性のある負の影響が含まれる。なお、当該拡張管理を適宜実施するためには、運用認可責任者・情報システム管理者・人事部長との緊密な連携が不可欠である。また、関連するセキュリティ管理策は PS-4 である。

参考文献：なし

優先順位の割り当ておよびベースライン管理策の割り当て:

P1	**低** AC-2	**中** AC-2 (1) (2) (3) (4)	**高** AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

AC-3 アクセス制御の実施

セキュリティ管理策：情報への論理アクセスおよびシステムリソースへの論理アクセスに関連して、情報システムが関係するアクセス制御ポリシーに従ってアクセス許可を強制する。

補足的ガイダンス：アクセス制御ポリシー（例：識別情報ベースのポリシー・役割ベースのポリシー・属性ベースのポリシー）は、ユーザに代わるユーザまたはユーザに代わるプロセスといった情報システムのサブジェクトまたは能動的なエンティティと機器・ファイル・レコード・ドメインといったオブジェクトまたは受動的なエンティティとの間のアクセスを制御する。また、アクセス制御メカニズムは、強制的にシステムアクセスするためのほかに、組織のミッション組織の業務をサポートする多くのサービスについて、組織のミッションおよび組織の業務をサポートする多くのアプリケーションの場合と同様に、情報システムが提供できるということを確認するためだけではなく情報セキュリティを強化するためにも利用することができる。なお、関連するセキュリティ管理策

は AC-2・AC-4・AC-5・AC-6・AC-16・AC-17・AC-18・AC-19・AC-20・AC-21・AC-22・AU-9・CM-5・CM-6・CM-11・MA-3・MA-4・MA-5・PE-3 である。

拡張管理策:

(1) アクセス制御の実施 | 特権機能へのアクセスの制限

[削除された:AC-6 に統合された]

(2) アクセス制御の実施|2段階認証

情報システムは、[組織が定義した特権コマンドおよび／または組織が定義したその他のアクションを割り当てる]ために2段階認証を強制する。

補足的ガイダンス:2 段階認証メカニズムを実施するためには、権限のある二人の個人による許可が必要になる。ただし、公共の安全を確保するため及び環境を確実に保護するための対応が速やかに必要な場合、2段階認証メカニズムは組織において必要とされない。なお、2 段階認証は、「ツーパーソンルール」としても知られている。また、関連するセキュリティ管理策は CP-9 および MP-6 である。

(3) アクセス制御の実施 | 必須アクセス制御

情報システムは、すべてのサブジェクトとオブジェクトに対して[組織が定義した必須アクセス制御ポリシーを割り当てる]を強制する。なお、組織によって定義された必須アクセス制御ポリシーが明示している事項は、下記の通り:

(a) **情報システム内の全てのサブジェクトとオブジェクトに対して一律に強制すること**

(b) **情報へのアクセスが許可されたサブジェクトは、以下のいずれについても行うことができないということ:**

(1) **権限のないサブジェクトまたは権限のないオブジェクトに情報を渡すこと**

(2) **自己の権限を他のサブジェクトに提供すること**

(3) **サブジェクト・オブジェクト・情報システム・情報システムコンポーネントのうち、1 つ以上のセキュリティ属性を変更すること**

(4) **新たに作成されたオブジェクトのセキュリティ属性または変更されたオブジェクトのセキュリティ属性を属性値とともに選択すること**

(5) **アクセス制御について規定律するルールを変更すること**

(c) **[組織が定義したサブジェクトを割り当てる]ことによって、上記(b)の一部または全部による制約を受けることなく[組織が定義した特権を(信頼されているサブジェクトに対して)割り当てる]ことが明示的に認められる可能性があること。**

補足的ガイダンス:上記拡張管理策に定義されている必須アクセス制御は非任意アクセス制御と同義であり、特定の従来からの使用途(例:Bell-LaPadula モデルを使った実装)に留まらない使われ方がなされる。なお、必須アクセス制御ポリシーが明示している上記の事項においては、すでにアクセスが可能なデータオブジェクトからの情報によってサブジェクトの行為が制限されるため、あるサブジェクトが権限を持たないサブジェクトおよび権限を持たないオブジェクトに情報を提供することはできない。また、当該事項においては、アクセス制御特権を伝達する事に関連してサブジェクトの行為が制限されるため、特権サブジェクトは、その特権を他のサブジェクトに渡す事はできない。ただし、必須アクセス制御ポリシーは、サブジェクトおよびオブジェクトとして情報システムの管理下にあるものの全てに対して一律に強制されなければ、回避される可能性がある。なお、必須アクセス制御ポリシーは、通常、リファレンスモニタの概念(AC-25 を参照)をに基づいて実装することによって強制される。ただし、必須アクセス制御ポリシーは、情報システム境界の内側にあるポリシーであるため、一旦情報が情報システムの必須アクセス制御の対象外となった場合、情報についての制約が今後も有効であり続けるよう追加で手段を講じる必要が生じる可能性がある。なお、信頼されているサブジェクトには、最小特権の概念(AC-6 を参照)に沿って権限が与

えられ、信頼されているサブジェクトには、必須アクセス制御ポリシーに関連して、組織のミッションに合致させるためおよび／または組織の業務ニーズを満たすために必要な最小特権のみが与えられている。また、必須アクセス制御は、機微情報および／または機密情報へのアクセスに関する政策を遂行する上での何らかの公的な裏付け（例：法律・大統領命令・指令・規制）があるとともに情報システムのユーザの一部には機微情報および／または機密情報として情報システムの中にある全ての情報にアクセスすることが認められていない場合に、最大限適用可能な機能である。なお、当該拡張管理策によって管理される必須アクセス制御は、下記 AC-3(4)の拡張管理策と共に実施する事が可能である。ただし、当該拡張管理策によって管理される必須アクセス制御ポリシーによって運用面での制約を受けるサブジェクトは、下記 AC-3(4)の拡張管理策による制約のうちより緩やかな制約のもとで運用する事が可能である一方、必須アクセス制御ポリシーは、下記 AC-3(4)の拡張管理策による制約のうちより緩やかなものに優先する。具体的には、必須アクセス制御ポリシーによって、機密度ラベルの異なる別のサブジェクトへのサブジェクトによる情報伝達は禁止される一方、下記 AC-3(4)の拡張管理策によって、同じ機密度ラベルの別のサブジェクトへのサブジェクトによる情報伝達は許可される。なお、関連するセキュリティ管理策は AC-25 および SC-11 である。

(4) アクセス制御の実施 | 任意アクセス制御

情報システムは、定義されたサブジェクトとともに定義されたオブジェクトに対して［組織が定義した任意アクセス制御ポリシーの割り当て］を強制する。なお、任意アクセス制御ポリシーは、情報に対するアクセスを許可されたサブジェクトが以下のうち１つ以上を実施できることを規定する：

- **(a) 他のサブジェクトまたは他のオブジェクトに情報を伝達すること**
- **(b) 自己の特権を他のサブジェクトに提供すること**
- **(c) サブジェクト・オブジェクト・情報システム・情報システムコンポーネントのいずれかのセキュリティ属性を変更すること**
- **(d) 新たに作成されたオブジェクトのセキュリティ属性または変更されたオブジェクトのセキュリティ属性を選択すること**
- **(e) アクセス制御について規律するルールを変更すること**

補足的ガイダンス：任意アクセス制御ポリシーが実装されている場合、既にアクセス権を持つ情報の扱いについてサブジェクトは自由に決めることができるため、既にアクセス権を持つ情報へのアクセス権を与えられたサブジェクトは、当該情報を他のサブジェクトまたは他のオブジェクトに伝達することが出来なくなるということはない（すなわち、伝達に関してサブジェクトに裁量の余地がある）。なお、当該拡張管理策は、AC-3(3)の拡張管理策と一体的に運用することができる。また、AC-3(3)の拡張管理策によって管理されるポリシーによって運用上の制約を受けるサブジェクトは、当該拡張管理策による制約のうちより緩やかな制約のもとで運用することが可能であるため、AC-3(3)の拡張管理策による機微密度ラベルの異なる別のサブジェクトへのサブジェクトによる情報伝達は禁止される一方で、下記 AC-3(4)の拡張管理策によって、同じ機密度ラベルの別のサブジェクトへのサブジェクトによる情報伝達は許可される。ただし、任意アクセス制御ポリシーは、情報システム境界の内側にあるポリシーである。一旦情報が情報システムの必須アクセス制御の対象外となった場合、情報についての制約が今後も有効であり続けるよう追加で手段を講じる必要が生じる可能性がある。なお、従来からの定義によれば、任意アクセス制御は ID ベースのアクセス制御であることが要求されるにもかかわらず、当該拡張管理策においてはそうした制限は要求されない。

(5) アクセス制御の実施| セキュリティ関連情報

セキュアなシステムを使用できないという状態にある場合を除き、情報システムが［組織によって明示されたセキュリティ情報を割り当てる］アクセスできないようにする。

補足的ガイダンス：セキュリティ関連情報とは、情報システムの内にある情報のうち、侵害されるとセキュリティ機能の実運用またはセキュリティサービスの提供に潜在的な影響をもたらす可能性があり、ひいてはシステムセキュリティポリシーを強制することが不可能になる可能性がある（若しくはコードとデータ分離し続ける事が不可能になる可能性がある）情報である。なお、セキュリティ関連情報には、例えば、ルーター（および／またはファイアウォール）のフィルタリングルールに加えて、セキュリティサービスの設定パラメータとともに、暗号管理情報およびアクセス制御リスト等がある。また、セキュアなシステムを使用できない状態にある場合の例として、情報システムがミッション関連および／または業務関連の処理を行っていない時間（例：メンテナンス・トラブルシューティング・起動中・シャットダウン済等の理由でシステムがオフラインになっている）等が挙げられる。なお、関連するセキュリティ管理策は CM-3 である。

(6) アクセス制御の実施| ユーザ情報とシステム情報の保護

[削除：MP-4 および SC-28 に統合された]

(7) アクセス制御の実施| 役割ベースのアクセス制御

[組織が定義した役割とともに当該役割を承認したユーザを割り当てる]に基づいて、情報システムが定義されたサブジェクトおよび定義されたオブジェクトに対して役割ベースのアクセス制御ポリシーを強制する。

補足的ガイダンス：「役割ベースのアクセス制御（以下、RBAC）」は、承認されたユーザにのみ情報システムへのアクセスを許可されたユーザに限定するためのアクセス制御ポリシーである。組織は、組織が定義した役割に対応する操作を必要なに応じて実行するために特定の役割をアクセス権限（すなわちアクセス特権）および職務権限に基づいて作成することができる。ただし、組織が定義した役割に対してユーザが割り当てられた場合、それらの役割として定義したアクセス権限（アクセス特権）を継承する。なお、アクセス権限（アクセス特権）は、全てのユーザ（中規模から大規模の組織においては、大きな人数となる可能性がある）に直接割り当てられのではなく役割が割り当てられることによって取得できるものであるため、RBAC によって組織のためのアクセス権限（アクセス特権）の管理は容易なものになる。また、RBAC によって、必須アクセス制御としてまたは任意アクセス制御┼として実装することができる。なお、必須アクセス制御として RBAC を実装する組織に対しては、AC-3(3)の拡張管理策の要求事項として、アクセス制御ポリシーが適用されるサブジェクトの範囲について、アクセス制御ポリシーが適用されるオブジェクトの範囲とともに定義されている。

(8) アクセス制御の実施| アクセス権限の取り消し

情報システムは、サブジェクトのセキュリティ属性が変更されるのに加えてオブジェクトのセキュリティ属性が変更されるのにい、アクセス権限（アクセス特権）を取り消すタイミングについて管理するルールとして組織が定めたものを割り当てる]に基づいてアクセス権限（アクセス特権）を強制的に取り消す。

補足的ガイダンス：アクセス権限の取り消しに関するルールは、どのようなアクセス権限を取りすかによって変わる可能性がある。具体的には、あるサブジェクト（すなわちあるユーザまたはあるプロセス）がグループから除外された場合、次回オブジェクト（例：ファイル）が開かれるまで（または次回サブジェクトがオブジェクトへアクセスしようと試みるまで）アクセス権限は取り消されない可能性がある。ただし、セキュリティラベルの変更により、アクセス権限は直ちに取り消される場合がある。なお、必要に応じてアクセス権限を即時に取り消す能力が情報システムにない場合、組織は代替策を講じることで直ちにアクセス権限を取り消すことができる。

(9) アクセス制御の実施|送信管理

形成されたセキュリティ境界の外側に情報システムが情報を送信するのは、以下の場合に限る:

(a) 受け取る[組織が定義した情報システムまたは組織が定義した情報システムコンポーネントを割り当てる]が、[組織が規定したセキュリティ対策を割り当てる]

(b) [組織が規定したセキュリティ対策を割り当てる]によって、割り当てを解除する対象の情報の妥当性が検証される場合

補足的ガイダンス:情報システムは、組織における情報のうち、形成されたシステム境界の内側にある情報のみを保護できる。ただし、形成されたセキュリティ境界をそうした情報が越えてもなお情報が確実に保護されるようにするためには、追加的なセキュリティ対策が必要になる可能性がある。なお、形成されたセキュリティ境界を情報が越える場合の具体例には、情報を外部の情報システムに伝送する場合とともに、情報システムのプリンターの1つを用いて情報を印刷する場合がある。また、セキュリティ境界の外にあるエンティティによる保護が適切であるか情報システムが判断できない場合、組織はリスク軽減策として外部の情報システムが適切なセキュリティを提供しているかどうかについて手続的に判断する。なお、外部の情報システムによって提供されるセキュリティが十分であるかどうかを判断するための手段には、例えば、検査または定期的なテストを実施すること、その組織と相手組織との間で合意を確立すること、あるいは他のプロセスを実施することがある。また、情報を保護するためにセキュリティ境界外のエンティティが用いる手段は、委託側の組織のものと同じである必要はないが、受け取った情報を保護するためにも、セキュリティポリシーに対する一貫した判断を行うのに十分なレベルである必要がある。なお、上記 AC-3 (9)の拡張管理策は、情報システムに対して、外部の情報システムに情報を送信する前に、当該情報の妥当性を確認するための技術的または手続的を講じることを要求する。例えば、当該情報システムが別の組織によって管理されている別のシステムに情報を場合、渡される情報に関連するセキュリティ属性が、情報を受け取る側のシステムにとって適切であるかを判断するための技術的手段が講じられる。また、その情報システムが、組織が管理する領域内のプリンターに情報を渡す場合、許可されている個人のみがプリンターにアクセスできるよう、手続的手段が講じられる。また、上記 AC-3 (9)の拡張管理策は、政策を遂行する上での何らかの公的な裏付け(例:法律・大統領命令・指令・規制のいずれか)がある場合、かつ、そのポリシーが特定の情報システムまたは組織の枠を超えて適用される場合に最大限適用可能となる。

(10) アクセス制御の実施| アクセス制御メカニズムの必要に応じたオーバーライド

組織は、[組織が定義した条件の割り当て]が満たされる場合に、自動アクセス制御メカニズムのオーバーライドを実施する。

補足的ガイダンス:関連するセキュリティ管理策は、AU-2 および AU-6 である。

参考文献:なし

優先順位の割り当てベースライン管理策の割り当て:

P1	**低** AC-3	**中** AC-3	**高** AC-3

AC-4 情報フロー制御の実施

(情報システムの)セキュリティ管理策:[組織が定義した情報フロー制御ポリシーを割り当てる]に基づいてシステム内(および相互接続システム間)の情報フローを制御するために、(管理者によって)承認されたアクセス権限を強制的に適用する。

補足的ガイダンス：情報フロー制御は、（情報へのアクセスが許可された者は誰であるのかについて規定するのではなく）情報システム内における情報伝達が許可される範囲について規定する約であると同時に情報システム間における情報伝達が許可される範囲について規定する制約であり、具体的には、エクスポート規制された情報を平文でインターネットに送信できないようにすること、組織内からの送信とされる外部からのトラフィックを遮断すること、組織の Web プロキシサーバー以外からの HTTP リクエストを禁止する事、またはデータ構造・データコンテンツに応じ組織間の情報のやり取りを制限する事等を指す。なお、セキュリティポリシーが異なるためにセキュリティドメインが異なる情報システム間で情報が伝達される事により、ドメインのセキュリティポリシーの1つまたは複数に違反するリスクが誘発される。そこでは、情報所有者／情報スチュワードが相互接続されたシステム間でセキュリティポリシーを実施するように指定されたポイントにおける手引を提供する。また、組織は、特定のセキュリティポリシーを実装が要求される場合には、具体的な構造的解決法を義務付けることを検討する。なお、アクセス強制には、例えば、相互接続されたシステム間の情報伝達を禁止する（すなわち、アクセスのみ許可する）、ハードウェアメカニズムを採用して、一方向の情報フローを強制する、またはセキュリティ属性をセキュリティラベルとともに再度割り当てるために信頼できる再配分メカニズムを実装する等がある。

指定された送信元（のネットワーク・個人・デバイス等）から指定された送信先（のネットワーク・個人・デバイス等）までのシステム内の情報フローに加えて相互接続されたシステム間の情報フローを制御するための情報フロー制御ポリシーは、指定された送信元（のネットワーク・個人・デバイス等）から指定された送信先（のネットワーク・個人・デバイス等）までのシステム内の情報フローに加えて相互接続されたシステム間の情報フローを制御するための実施メカニズムとともに、組織によって一般的に導入されている。なお、情報フローは、情報の特性および／または情報経路の特性に基づいて制御される。また、指定された送信元（のネットワーク・個人・デバイス等）から指定された送信先（のネットワーク・個人・デバイス等）までのシステム内の情報フローは、相互接続されたシステム間の情報フローとともに、例えば、情報システムサービスを制限するルールセットを使用する（または情報システムサービスを制限する構成設定を確立する）境界保護装置（例：ゲートウェイ・ルーター・ガード・暗号化トンネル・ファイアウォール等）において制御される。ただし、指定された送信元（のネットワーク・個人・デバイス等）から指定された送信先（のネットワーク・個人・デバイス等）までのシステム内の情報フローは、ヘッダー情報に基づいた境界保護装置または、メッセージ内容に沿ったメッセージフィルタリング能力を持つ例えば、キーワード検索を実装するもしくはドキュメント特性を利用する境界保護装置においても制御される。また、情報フロー制御を左右するフィルタリング（および／または検査）メカニズムの信頼性（すなわち、ハードウェアコンポーネント・ファームウェアコンポーネント・ソフトウェアコンポーネントのそれぞれの信頼性）については、組織による検討が行われる。なお、下記の(3)から(22)までの拡張管理策は、高いセキュリティを保証するセキュリティガード等、（高度なフィルタリング技術に加えて）綿密な分析が中心となるとともに複数のドメインにまたがる製品に実装されているより強力なフロー制御メカニズムを中心にしたクロスドメインソリューションに対するニーズに主に対応するものである。ただし、機能は、通常、市販の IT 製品には備わっていない。なお、関連するセキュリティ管理策は AC-3・AC-17・AC-19・AC-21・CM-6・CM-7・SA-8・SC-2・SC-5・SC-7・SC-18 である。

拡張管理策：

(1) 情報フロー制御の実施 | オブジェクトのセキュリティ属性に対する情報フロー制御の実施

情報システムは、情報フロー制御の前提として［組織が定義した情報フロー制御ポリシーの割り当て］を実施するために、［組織が定義した情報オブジェクト、組織が定義した送信元オブジェクト、および組織が定義した送信先オブジェクトの割り当て］に関連して［組織が定義したセキュリティ属性の割り当て］を行う。

補足的ガイダンス：情報フロー制御のメカニズムにおいては、情報に関連するセキュリティ属性（具体的には、データ内容およびデータ構造）が送信元オブジェクトおよび／または送

信先オブジェクトに関連するセキュリティ属性と比較されるとともに、情報フローポリシーによって明示的に許可されていない情報フローに対しては適切な対応（例：遮断・検査・アドミニストレータのいずれかへの通知）がなされる。具体的に、「機密」とラベル付けされた情報オブジェクトは「機密」とラベル付けされている送信先オブジェクトに移行する可能性がある一方、「極秘」とラベル付けされた情報オブジェクトは「機密」とラベル付けされた送信先オブジェクトに移行しない可能性がある。また、トラフィックフィルタファイアウォールのアドレスとなっている送信元（送信先）アドレス等もセキュリティ属性となる可能性がある。なお、特定の種類の情報については、明示的なセキュリティ属性に基づいて情報フロー制御を実施することによって情報の公開を管理することができる。なお、関連するセキュリティ管理策は AC-16 である。

(2) 情報フロー制御の実施| 処理ドメインに対する情報フロー制御の実施

フロー制御の前提として[組織が定義した情報フロー制御ポリシーを割り当てる]を実施するにあたって、情報システムが保護された処理ドメインを使用する。

補足的ガイダンス：保護された処理ドメインとして情報システムの内部で他の処理ドメイン間のインタラクションが制限される処理ドメインは、ドメインおよび Type Enforcement を実装することでドメイン間の情報フローを制御することが可能であるのに加えて、ドメインおよび Type Enforcement を実装する事でデータオブジェクトおよび／または情報オブジェクトへの情報フローをデータオブジェクトおよび／または情報オブジェクトから情報フロー）とあわせて制御する事が可能である。なお、ドメインおよび Type Enforcement に関連して、情報システムによる処理はドメインごとに行われると同時に、情報のタイプが識別される。また、情報フローは、（ドメイン・情報タイプに基づいて）アクセスが許可された情報へのアクセスに基づいて制御されるとともに、ドメイン間で許可された信号通信に基づいて制御されると同時に、別ドメインへの移行が許可されたプロセスに基づいて制御される。

(3) 情報フロー制御の実施 | 動的情報フロー制御の実施

[組織が定義したポリシーの割り当て]に従って情報システムが動的情報フロー制御を実施する。

補足的ガイダンス：動的情報フロー制御に関する組織のポリシーには、組織のミッション（および／または組織の業務）に対するニーズを反映して組織のミッション（および／または組織の業務）の優先順位が変化したことによって組織のリスク許容度が変化するという状況変化に応じて情報フローを許可または未許可にすることに加えて、脅威環境の変化（または有害なイベントの検出）といった状況の変化に応じて情報フローを許可または未許可にすることなどがある。また、その他、変化する組織のミッション（および／または変化する組織の業務）に関する考慮事項に基づいて情報フローを許可または未許可にすることがある。なお、関連するセキュリティ管理策は、SI-4 である。

(4) 情報フロー制御の実施 | 暗号化された情報内容チェック

情報システムが[①情報の復号化②暗号化された情報のフローの遮断③暗号化された情報を渡すセッションの切断④[組織が定義した手順（または組織が定義した手法）の割り当て]のいずれかを（1 つまたは複数）選択]することによって、暗号化された情報を照合する仕組みが機能しない事態を防ぐ。

補足的ガイダンス：関連するセキュリティ管理策は SI-4 である。

(5) 情報フロー制御の実施 | 埋込みデータ型の制御

あるデータ型を他のデータ型に埋め込む事に関して、情報システムが[組織が定義した制限の割り当て]を実施する。

補足的ガイダンス：データタイプを他のデータタイプに埋め込むことにより、情報フロー制御の有効性が低下する場合がある。データタイプの埋め込みには、例えば、文書作成ソフトで作成されたファイルに、実行ファイルをオブジェクトとして挿入すること、メディアファイルに

参照情報または記述的情報を挿入すること、複数の埋め込みデータタイプを含んでいる圧縮データまたはアーカイブデータタイプがある。データタイプの埋め込みに関する制限では、許容できる埋め込みレベルと、検査ツールの能力が及ばない許容できないデータタイプの埋め込みについて考慮する。

(6) 情報フロー制御の実施 | メタデータによる制御

[組織が定義したメタデータの割り当て]によって、情報システムが情報フロー制御を実施する。

補足的ガイダンス：メタデータとは、データの特性を説明するために用いられる情報である。ただし、組織が定義したメタデータは、データ構造（例：データフォーマット・データシンタックス・データシマンティクス）を説明する構造的メタデータである可能性があると同時に、データ内容（例：年齢・場所・電話番号）について説明する記述的メタデータである可能性がある。なお、制御可能な情報フローをメタデータによって制御することによって、より簡素かつより効果的な情報フロー制御を可能となる。組織は、メタデータの正確さ（すなわち、メタデータの値がデータの値として正しい事への認識）という観点からメタデータの信頼性について検討すると共に、メタデータの整合性（すなわち、メタデータのタグが不正な変更から保護されているさま）という観点からメタデータの信頼性について検討する。また、組織は、メタデータとデータ本体とのバインディング（すなわち、強力なデータバインディング技法としてセキュリティを適切な水準まで保証する上で十分なもの）の観点からメタデータの信頼性について検討する。なお、関連するセキュリティ管理策は、AC-16 および SI-7 である。

(7) 情報フロー制御の実施 | メカニズムとしての一方向の情報フロー制御

ハードウェアフロー制御のメカニズムを使用して情報システムが[組織が定義した一方向の情報フローの割り当て]を実施する。

(8) 情報フロー制御の実施 | ポリシーで定義されたセキュリティフィルターによる情報フローの制御

[組織が定義した情報フローの割り当て]におけるフロー制御の前提として、情報システムが[組織によってポリシーで定義されたセキュリティフィルターの割り当て]を使用して情報フロー制御を実施する。

補足的ガイダンス：組織によってポリシーで定義されたセキュリティフィルターを通じて、データ構造のフィルタリングおよびデータコンテンツのフィルタリングとして、ファイルの長さの最大値をチェックするといったことが可能になるとともに、構造化された（または構造化されていない）データのデータ型（および／またはファイルタイプ）を最大フィールドサイズとともにチェックするといったことが可能になる。また、データコンテンツをフィルタリングするためにポリシーで定義されたセキュリティフィルターは、特定の単語についてチェック（例：侮蔑語かそうでないかをフィルタリング）することが可能であるとともに、データ値の範囲または列挙値・非表示コンテンツであるかどうかをチェックすることが可能であるとともに、データ構造のコンテンツは、アプリケーションによって解釈することができる。なお、構造化されていないデータとは、通常、特定のデータ構造を持たないまたはデータ構造を持ちながらも情報フロー制御に影響を及ぼさないデジタル情報を指す。ただし、構造化されていないデータとは、デジタル情報としてデータ構造を持つちながらも、構造化されていないデータによって伝達されたデジタル情報について特定の機微度に応じたルールセットの作成に影響を及ぼさないデジタル情報を指す場合がある。なお、構造化されていないデータの構成は以下の通り：①本質的に言語ベースではないビットマップオブジェクト（すなわち、画像・動画・オーディオファイル）②（文字または活字という）言語ベースのテキストオブジェクト（例：市販のワープロソフトによる文書に加えて、スプレッドシート・電子メール等）。組織は、情報フローを制御する目的を達成するために、ポリシーによって定義された 2 つ以上のセキュリティフィルターを実装することができる（例：誤判定を減らすために、侮蔑語でない用語のリストを侮蔑語のリストと併用することができる）。

(9) 情報フロー制御の実施 |目視レビューによる情報フローの制御

[組織が定義した情報フローの割り当て]において情報システムが目視レビューを実施できるのは、[組織が定義した条件の割り当て]の場合に限る

補足的ガイダンス：組織によって、ポリシーによって定義されたセキュリティフィルターとして、自動フロー制御が可能なあらゆる状況下で使用可能なセキュリティフィルターが定義される。ただし、フロー制御を完全に自動化することが不可能な場合には、ポリシーによって定義された自動的なセキュリティフィルターの代わりまたは補完するものとして、目視レビューが実施される可能性がある。なお、目視レビューは、適宜組織によって実施される。

(10) 情報フロー制御の実施 | ポリシーで定義されたセキュリティフィルタを有効化および/または無効化する

[組織が定義した条件の割り当て]の場合に、情報システムが特権管理者に対して[組織がポリシーで定義したセキュリティフィルターの割り当て]を有効化および／または無効化する機能を提供する

補足的ガイダンス：具体的には、セキュリティポリシーによってチェックされる侮蔑語の一覧の内容を組織が定義した侮蔑語の意味に即して変更することで、管理者はセキュリティポリシーに対する変更を反映させる事ができる。

(11) 情報フロー制御の実施 | 情報フロー制御によるポリシーで定義されたセキュリティフィルタの構成

さまざまなセキュリティポリシーをサポートできるよう、情報システムが特権を管理者が[組織が定めたポリシーで定義されたセキュリティフィルタの割り当て]を設定できるようにする

補足的ガイダンス：具体的には、管理者は、組織によって定義されるセキュリティポリシーによってチェックされる侮蔑語のリストの内容を管理者がセキュリティポリシーの変更を反映する形で変更することができる。

(12) 情報フロー制御の実施 | データタイプ識別子

異なるセキュリティドメイン間で情報を流す際に、情報システムが[組織が定義したデータタイプ識別子の割り当て]によって情報フロー制御に不可欠なデータの確認を行う

補足的ガイダンス：データタイプ識別子には、例えば、ファイル名・ファイルタイプ・ファイルシグネチャ・ファイルトークン・（複数の内部ファイル）シグネチャ／トークン等がある。なお、情報システムは、データタイプフォーマットの仕様に適合する場合にのみデータの伝送を許可しうる。

(13) 情報フロー制御の実施 | ポリシー関連のサブコンポーネントに分割する

情報システムは、異なるセキュリティドメイン間で情報を伝送する際には、情報を[指定：組織が定義したサブコンポーネント（ポリシー関連）の割り当て]によってポリシーを実施するために、異なるセキュリティドメイン間で情報を流す際に情報システムが情報を分割する

補足的ガイダンス：ポリシーが実施されることによって、ポリシー関連のサブコンポーネントに対してフィルタリングルール・検査ルールおよび／または削除ルールが適用されるとともに、異なるセキュリティドメイン間で情報をやりとりするに当たっての情報フロー制御が円滑に行われるようになる。また、流すファイルが解析されることによって、送信元・送信先・証明書・分類・添付ファイルといったセキュリティに関係する個別のコンポーネントに対するポリシー策定が円滑に行われるようになる。

(14) 情報フロー制御の実施 | ポリシーで定義されたセキュリティフィルターによる制限

情報システムが異なるセキュリティドメイン間で情報を流す際、データ構造（およびデータコンテンツ）を規定するデータフォーマットとして完全に列挙されたものが必要な[組織がポリシーで定義したセキュリティフィルターの割り当て]を実装する

補足的ガイダンス：データ構造（およびデータコンテンツ）が制限されることによって、ドメイン間のトランザクションにおいて悪意のある可能性があるコンテンツ（および／または許可されていない可能性があるコンテンツ）がされる。ただし、データ構造を制限するセキュリティフィルターとしてポリシーで定義されたものの中には、例えば、ファイルサイズとフィールド長を制限がある。なお、データコンテンツのフィルター処理としてポリシーで定義されたものの一部は、以下の通り：①文字セットのフォーマットをエンコードする（例：Universal Character Set Transformation Formats および American Standard Code for Information Interchange）②文字データフィールドを英数字のみ含まれるようにする③特殊文字を禁止する④スキーマ構造を確認する。

(15) 情報フロー制御の実施 |許可されていない情報の検出

情報システムが異なるセキュリティドメイン間で情報を流す、[許可されていない情報として組織的に定義された情報の割り当て]の有無を調べたうえで、[組織が定義したセキュリティポリシーの割り当て]に従って情報を流す事を禁止する。

補足的ガイダンス：許可されていない情報を検出することの中には、例えば、侮辱語または悪質なコードを求めて、流される全ての情報をチェックすることも含まれる。なお、関連するセキュリティ管理策は SI-3 である。

(16) 情報フロー制御の実施 | 相互接続された情報システム内で情報のやり取りを行う

[削除:AC-4 に統合]

(17) 情報フロー制御の実施 |ドメイン認証

情報をやり取りするにあたって、[組織・システム・アプリケーション・個人を1つ（または複数）選択]を通じて情報システムがソース・ターゲットを一意に識別（および一意に認証）する。

補足的ガイダンス：属性は、オペレーションセキュリティを考える上で重要なコンポーネントである。なお、情報システム内の情報フローのソース・ターゲットを特定できることによって、必要に応じてイベントを復元することが可能になるとともに、ポリシーに違反した特定の組織（および／または特定の個人）を明らかにすることによってポリシーをより一層順守するよう促す事が可能になる。ただし、ドメイン認証に成功するためには、情報を配布準備・送信・受信・配布するシステム・組織・個人をシステムラベルが区別する事が求められる。なお、関連するセキュリティ管理策は、IA-2・IA-3・IA-4・IA-5 である。

(18) 情報フロー制御の実施 | セキュリティ属性のバインド

情報フローポリシーの実施を容易にするために、情報システムが[組織が定義したバインディング技法の割り当て]を用いてセキュリティ属性情報にバインドする。

補足的ガイダンス：情報システムが実装するバインディング技法は、どの程度情報がセキュリティ属性にバインドされているかに影響を与える。また、セキュリティを保証するバインディング技法は、どの程度情報がセキュリティ属性にバインドされているかとともに、組織が情報フロー制御のプロセスを信頼するうえで重要な要素となる。ただし、この技法は、レビュー回数を含めて組織が追加要求するレビューの規模に影響を与える。なお、関連するセキュリティ管理策は、AC-16 および SC-16 である。

(19) 情報フロー制御の実施 | メタデータの検証

異なるセキュリティドメイン間で情報を流す際、データそのものに対して適用されるものと同じセキュリティフィルターとしてポリシーで定義されたものを情報システムがメタデータにも適用する。

補足的ガイダンス：この拡張管理策は、メタデータが適用されるデータをメタデータとともに検証することを義務付けている。ただし、一部の組織はメタデータをデータそのもの（すなわち、メタデータをバインドするデータの部分のみ）と区別する一方で、その他の組織はメタデータが適用されるデータをメタデータとともにデータ本体の一部とみなし、区別をしない。な

お、(メタデータが適用されるデータを含めて)メタデータ等の全ての情報はフィルタリングおよび検査の対象である。

(20) 情報フロー制御の実施 | 承認されたソリューションの定義付け

複数のセキュリティドメインにまたがって[組織が定義した情報の割り当て]による情報フローを制御するために、組織が[組織が定義したソリューションとしての承認された構成の割り当て]を使用する。

補足的ガイダンス:組織は、分類境界を越える情報フローのタイプに応じて、ソリューションとして承認された構成をクロスドメインポリシーおよびガイダンスとして定義する。なお、UCDMO(The Unified Cross Domain Management Office)は、承認されたクロスドメインリューションに関するベースライン管理策の一覧を提供している。

(21) 情報フロー制御の実施 | 情報フローの物理的 / 論理的な分離

[組織が定義したメカニズム(および/または組織が定義した技法)の割り当て]を用いて情報フローを論理的または物理的に分離することによって、情報システムが[組織情報の種類で必要に応じて情報フローが分離されるよう組織により定義された割り当て]を行う。

補足的ガイダンス:情報の種類で情報フローを分離する事は、送信中に情報が混ざらない事を保証するとともに、他の手段を以ってしてはおおよそ不可能なフロー制御として、データ転送経路による情報フロー制御を可能にするため、(情報を)より強力に保護する事が可能になる。なお、分離可能な情報には、例えば、インバウンドトラフィック・アウトバウンドトラフィック・サービス要求とともに、サービス要求に対する応答に加えて、セキュリティカテゴリが異なる情報等がある。

(22) 情報フロー制御の実施 | アクセス専用回線

複数の異なるセキュリティドメインに属するコンピュータプラットホーム、(または複数の異なるセキュリティドメインに属するアプリケーション、もしくは複数の異なるセキュリティドメインに属するデータ)へのアクセスを(異なるセキュリティドメイン間の情報フローを遮断する情報システムが)デバイス単位で提供する。

補足的ガイダンス:情報システムは、異なるセキュリティドメイン間で情報をやり取りできるようにする仕組みは提供しない一方で、接続されている各セキュリティドメインにユーザがデスクトップコンピュータ等からアクセスできるようにする。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** AC-4	**高** AC-4

AC-5 職務の分離

セキュリティ管理策:

a. 組織は、[組織が担当者の職務として定めた職務の割り当て]によって割り当てられた職務を分離する

b. 組織は、担当者の職務について職務分離を明文化する

c. 組織は、職務分離をサポートするアクセス権限を情報システムに対して定義する

補足的ガイダンス:職務分離は、アクセス権限が悪用される可能性に対処するものとして、ある一人によって悪事が行われるリスクを減らす一端を担う。なお、以下の事項も職務分離の一例である:

① 職務を個人および/または役割ごとにミッション関連と情報システムサポート関連とに割り振ること

② 情報システム支援機能を別の担当者(例:システム管理担当者･プログラミング担当者･構成管理担当者･品質保証担当者･テスト担当者･ネットワークセキュリティ担当者)が実施すること
③ アクセス制御を管理するセキュリティ責任者に監査機能を管理させないようにすること

また、関連するセキュリティ管理策は AC-3･AC-6･PE-3･PE-4･PS-2 である。

拡張管理策:なし

参考文献:なし

優先順位の割り当てベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** AC-5	**高** AC-5

AC-6 最小権限の原則の採用

セキュリティ管理策:最小権限の原則の採用を通じて、組織のミッション(および組織の業務機能)に応じて割り当てられたタスクの実行に必要な正規のアクセス(または組織のミッションに応じて割り当てられたタスクを実行するうえで必要なプロセス)のみ(または組織の業務機能に応じて割り当てられたタスクをユーザが実行するのに必要なプロセスのみ)、組織がユーザに許可する。

補足的ガイダンス:組織は、特定の職務権限(および特定の情報システム)に対して最小権限の原則を採用する。また、情報システムプロセスに対して最小権限の原則が適用されることによって、情報システムプロセスは組織に必要なミッションを達成する(および／または組織に必要な業務機能を確保する)のにふさわしい水準にて確実に運用される。なお、最小権限の原則を採用するにを検討する。また、組織は自己の情報システムを開発･導入･運用する際に最小権限の原則を採用する。なお、関連するセキュリティ管理策は AC-2･AC-3･AC-5･CM-6･CM-7･PL-2 である。

セキュリティ管理策の拡張管理策:

(1) 最小権限の原則の採用 | セキュリティ機能へのアクセス承認

[組織が定義した(ハードウェア･ソフトウェア･ファームウェアに導入されている)セキュリティ機能の割り当てとともに、組織が定義したセキュリティ関連情報の割り当て]へのアクセスを組織が明示的に許可する。

補足的ガイダンス:セキュリティ機能には、例えば、システムアカウントを作成することと合わせて、アクセス権限(すなわち、アクセス許可またはアクセス特権)を構成することとともに、監査対象のイベントを設定することに加えて、不正侵入検知パラメータを設定する事等が含まれる。また、セキュリティ関連情報には、例えば、ルーターのフィルタリングルール(および／またはファイアウォールのフィルタリングルール)と合わせて、暗号鍵の管理情報とともに、セキュリティサービスの構成パラメータに加えて、アクセス制御リストが含まれるなお、明示的アクセス権限を持つ職員には、例えば、セキュリティ管理者･システムアドミニストレータ･ネットワークアドミニストレータ･システムセキュリティ責任者･システムメンテナンス要員･システムプログラマ等の特権ユーザが含まれる。また、関連するセキュリティ管理策は、AC-17･AC-18･AC-19 である。

(2) 最小権限の原則の採用 | 非セキュリティ機能への非特権アクセス

非セキュリティ機能にアクセスする際に、情報システムアカウントのユーザのうち[組織が定義したセキュリティ機能(または組織が定義したセキュリティ関連情報)の割り当て]にアクセスしているユーザに対して、組織が非特権アカウントまたは非特権的なロールの利用を要求する。また、同じく非セキュリティ機能にアクセスする際に、情報システムアカウント

の役割のうち[組織が定義したセキュリティ機能(または組織が定義したセキュリティ関連情報)の割り当て]にアクセスする役割に関連して、組織が非特権アカウントまたは非特権ロールの利用を要求する。

補足的ガイダンス:この拡張管理策によって、特権アカウントを運用する際または特権ロールを運用する際にデータが不正利用される可能性が減る。なお、特権ロールが拡張管理策の対象に含まれることによって、組織による(役割ベースのアクセス制御などの)アクセス制御ポリシーの実装に対して拡張管理策が適用できるようになるとともに、アカウントから非特権アカウント(またはその逆)への変更によって保証されるセキュリティと同等のセキュリティを保証する拡張管理策が特権ロールを変更することで適用できるようになる。また、特権ロールが拡張管理策の対象に含まれることによって、(2)ユーザに対して同等のセキュリティを保証するとともにユーザ向けの全てのプロセスに対して同等のセキュリティを保証する拡張管理策が特権ロールを変更することで適用できるようになる。なお、関連するセキュリティ管理策は、PL-4 である。

(3) 最小権限の原則の採用 | 特権コマンドへのネットワークアクセス

[組織が定義した運用上クリティカルなニーズの割り当て]のみを目的に組織が[組織が定義した特権コマンドの割り当て]へのネットワークアクセスを承認するとともに、組織が情報システムのセキュリティ計画に承認したネットワークアクセスの根拠を記載する。

補足的ガイダンス:ネットワークアクセスとは、ローカルアクセスとは異なり、何らかの形でネットワークへ接続すること(すなわち、ユーザが機器上にに表示される事)を指す。なお、関連するセキュリティ管理策は、AC-17 である。

(4) 最小権限の原則の採用| 個別の処理ドメインの提供

ユーザ権限をきめ細かく割り当てることが出来るよう、情報システムが処理ドメインを別途用意する。

補足的ガイダンス:ユーザ権限をきめ細かく割り当てる事ができるよう、:

① ある仮想マシン(または仮想化マシンが構築された実機)ではユーザ権限を制限する一方、仮想化技術を用いて別の仮想マシン内でユーザ権限の追加を許可する
② ハードウェアドメインを分離するメカニズムおよび/またはソフトウェアドメインを分離メカニズムを用いる
③ 個別の物理ドメインを実装する

といった措置を通じて処理ドメインが別途提供される。なお、関連するセキュリティ管理策は AC-4・SC-3・SC-30・SC-32 である。

(5) 最小権限の原則の採用 |特権アカウントの制限

[組織が定めた職員(または組織が定義した役割)の割り当て]のために組織が情報システムの特権アカウントを制限する。

補足的ガイダンス:スーパーユーザアカウントを含めて、特権アカウントは、通常さまざまな種類の市販のオペレーティングシステムにおいてシステムアドミニストレータアカウントであるとされるため、特権アカウントの利用者が特定の職員または特定の役割に制限されることで、日常業務を行うユーザは特権的情報および/または特権的機能へアクセスすることができなくなる。なお、この拡張管理策を適用するに当たり、組織はローカルアカウントの権限とドメインアカウントの権限を区別してもよい。ただし、組織がシステムの主要なセキュリティパラメータの構成を管理する能力をその他必要なものとともに維持することでリスクが十分に軽減される場合に限る。なお、関連するセキュリティ管理策は、CM-6 である。

(6) 最小権限の原則の採用 | 組織的ユーザ以外のユーザによる特権的アクセスの禁止

組織ユーザ以外のユーザによる情報システムへの特権的アクセスを組織が禁止する。

補足的ガイダンス:関連するセキュリティ管理策は、IA-8 である。

(7) 最小権限の原則の採用 | ユーザ権限の見直し

ユーザ権限が必要かどうか検証するために、(a)[組織が定義した役割（または組織が定義したユーザのクラス）の割り当て]に当たり、[組織が定義した頻度の割り当て]というユーザ権限を組織が見直すと同時に、b)組織のミッション（および／または組織の業務ニーズ）を正しく反映するために、組織が必要に応じてユーザ権限を再度割り当てする（または、組織が必要に応じてユーザ権限を取り消す）。

補足的ガイダンス：割り当てられた特定のユーザ権限の必要性は、（運用環境・技術・脅威の変化を反映するのに加えて）組織のミッションおよび／または組織の業務環境の変化を反映して、時間の経過と共に変わりうる。また、割り当てられた特定のユーザ権限が正当なままなのかどうかについて判断するためには、割り当てられた特定のユーザ権限を定期的に見直す必要がある。なお、定期的な見直しのなかで、割り当てられた特定のユーザ権限の必要性が再確認できない場合には、組織は適切な是正措置を取る。また、関連するセキュリティ管理策は、CA-7 である。

(8) 最小権限の原則の採用 | コードを実行するための権限のレベル設定

ユーザがソフトウェアを実行する際よりも高い権限からの[組織が定義したソフトウェアの割り当て]の実行を情報システムが阻止する。

補足的ガイダンス：特定の状況下でソフトウェアアプリケーションおよび／またはソフトウェアプログラムが必要な機能を実行するためには、当該アプリケーションおよび／またはプログラムが通常より高い権限で実行される必要がある。ただし、その際必要な権限が当該アプリケーションおよび／またはプログラムを呼び出す組織ユーザに割り当てられた権限よりも高い場合、当初組織によって割り当てられたものよりも高い権限が当該組織ユーザに対して間接的に与えられる。

(9) 最小権限の原則の採用 | 特権的機能の使用のチェック

特権的機能の実行をシステムが監査する。

補足的ガイダンス：許可されているユーザが特権的機能を悪用することまたは許可なく情報システムアカウントに侵入する部外者が特権的機能を悪用する事は、今なお深刻な問題であり、意図するせざるに関わらず、組織に著しい悪影響を及ぼす可能性がある。なお、特権的機能の悪用を検知する1つの手段として特権的機能の利用状況の監査があり、インサイダー脅威によってもたらされるリスクの軽減に役立つと同時に、APT(advanced persistent threat)によってもたらされるリスクの軽減に役立つ。なお、関連するセキュリティ管理策は AU-2 である。

(10) 最小権限の原則の採用 | 非特権ユーザによる特権的機能の実行の禁止

非特権ユーザによって変更されて実装されたセキュリティ対策を無効にするとともに回避・変更するなど、情報システムが非特権ユーザによる特権的機能の実行を禁止する。

補足的ガイダンス：特権的機能には、情報システムアカウントの作成、システムの完全性チェックの実行、暗号鍵管理活動の管理等がある。なお、非特権ユーザとは、適切な権限を持たない個人であり、非特権ユーザから保護されるべき特権的機能の例として、侵入検出メカニズムを兼ねた侵入防止メカニズムを迂回することとともに、悪質なコードからシステムを保護するメカニズムを迂回することがある。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** AC-6 (1) (2) (5) (9) (10)	**高** AC-6 (1) (2) (3) (5) (9) (10)

AC-7　ログオン試行の失敗

セキュリティ管理策:

a. [組織が定義した期間の割り当て]のなかでユーザが連続して[組織が定義した数字の割り当て]への（による？）ログオンに失敗できる上限を情報システムが強制的に設定する

b. 規定回数以上ログオンに失敗した場合、[次のいずれかを選択:①[組織が定義した期間の割り当て]のためにアカウントおよび／またはノードをロックする②管理者によって解除されるまでアカウントおよび／またはノードをロックする③[組織が定義した遅延アルゴリズム]に沿って次回のログオンプロンプトを遅らせる]]を自動的に行う。

補足的ガイダンス:このセキュリティ管理策は、ローカル接続でログオンまたはネットワーク接続でログオンの如何を問わず適用される。また、サービス拒否につながる可能性があるため、情報システムが原因の自動ロックアウトは通常一時的なものであり、組織があらかじめ設定した期間が過ぎると自動的に解除される。なお、遅延アルゴリズムが選択された場合、組織は情報システムのそれぞれのコンポーネントに対してコンポーネントの機能に応じて異なるアルゴリズムを使採用してもよい。ただし、オペレーティングシステムレベルおよびアプリケーションレベルの両方でログオン試行に失敗した場合の応答が実装される可能性がある。なお、関連するセキュリティ管理策は、AC-2・AC-9・AC-14・IA-5 である。

拡張管理策:

(1) ログオン試行の失敗 | アカウントを自動でロックする

[削除された:AC-7 に統合された]

(2) ログオン試行の失敗 | 携帯機器のデータを消去 /またはワイプする

[組織が定義した携帯機器を割り当てる]へのログオンが[組織が定めた回数の割り当て]にわたって連続して失敗した場合に、[組織が定義した、除去／消去に関する要求事項／技術を割り当て]に基づいて、情報システムが携帯機器上の情報を消去またはワイプする。

補足的ガイダンス:この拡張管理策は、ログオンが必要な携帯機器（例: PDA・スマートフォン・タブレット）にのみ適用される。ただし、ここでいうログオンとは携帯機器へのそれであり、携帯機器上の特定のアカウントに対するものへのそれではないため、携帯機器上の特定のアカウントへのログオンに成功した場合、それまでのログオンに失敗した回数はゼロにリセットされる。なお、消去またはワイプを過剰な頻度で行うことによって機器が使用不能となる事態を回避できるよう、組織は消去する情報またはワイプする情報を慎重に定義しなければならない。ただし、携帯機器上の情報が強力な暗号メカニズムによって十分に保護されている場合には、消去またはワイプが不要な場合もありうる。なお、関連するセキュリティ管理策は、AC-19・MP-5・MP-6・SC-13 である。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** AC-7	**中** AC-7	**高** AC-7

AC-8　システムの利用に関する通知

セキュリティ管理策:

a. ①ユーザが連邦政府の情報システムにアクセスしていること②情報システムの利用状況が監視・記録されうるとともに、それが監査の対象となりうること③情報システムの無許可利用が禁止されるとともに、それらが民事・刑事の両面による責任追及の対象となる事④情

報システムを利用する事がすなわちそれらを監視・記録する事に同意したものとみなされる事の4つを規定したプライバシーおよびセキュリティに関する通知を提供する情報システムとして、プライバシーおよびセキュリティに関する通知として連邦法・大統領命令・指令・政策・規制・標準・手引に準拠したものを提供する情報システムへのアクセスを許可する前に、[組織が定義したバナー(またはシステムの利用に関連して組織が定義した通知メッセージ)の割り当て]を情報システムのユーザに対して表示する。

b. ユーザが使用条件に同意するとともに情報システムにログオンする明示的なアクションまたは情報システムへさらにアクセスする明示的なアクションを取るまで、通知メッセージまたはバナーを情報システムの画面に表示したままにする。

c. 一般ユーザがアクセス可能なシステムの場合:①アクセスを将来許可する前に、システムの使用に関する[組織が定義した条件の割り当て]を情報システム上に表示するのに加えて、②通常はシステム監視・システムレコーディング・システム監査を禁止しているプライバシーに関する特約に反しない形で監視・レコーディング・監査する目的でリファレンスを適宜表示するとともに、③システムの正規な利用について記述する。

補足的ガイダンス:システム利用通知は、個人が情報システムにログインする前に表示されるメッセージまたは警告バナーを用いることによって実装することが可能である。ただし、システム利用通知は生身の人間であるユーザがログオンインターフェースにアクセスする場合にのみ使用されるため、生身の人間であるユーザがログオンインターフェースにアクセスしない場合、システム利用通知は必要でない。なお、組織は、警告バナーの内容に対するリーガルチェックを法務部門に依頼するとともに、情報システムのユーザ数次第で、組織はシステム利用通知(システム利用メッセージおよび/またはバナー通知)の多言語表示について具体的なニーズを基に検討する。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** AC-8	**中** AC-8	**高** AC-8

AC-9 前回のログオン(アクセス)に関する通知

セキュリティ管理策:システムへのログオン(アクセス)に成功した場合、情報システムが前回のログオン(アクセス)日時をユーザに通知する。

補足的ガイダンス:このセキュリティ管理策は、生身の人間であるユーザがログオンインターフェースにアクセスすることによって情報システムにログオンする場合にとどまらず、その他のアーキテクチャ(例:サービス指向型アーキテクチャ)によって情報システムにログオンする場合に適用できる。なお、関連するセキュリティ管理策は AC-7 および PL-4 である。

拡張管理策:

(1) 前回ログオンに関する通知 | ログオン試行の失敗の通知

ログオン(アクセス)に成功した際に、前回ログオン(アクセス)に成功した時点以降ログオン(アクセス)の試行に失敗した回数を情報システムがユーザに対して通知する。

(2) 前回ログオンに関する通知 | ログオン試行の成功の通知および／またはログオン試行の失敗の通知

[組織が定義した期間の割り当て]の間おける[成功したログオン試行もしくは成功したアクセス試行（および／または失敗したログオン試行もしくは失敗したアクセス試行）の選択]の回数を情報システムがユーザに通知する。

(3) 前回ログオンに関する通知 | アカウントに対する変更の通知

[組織が定義した期間の割り当て]の間における[ユーザアカウントのセキュリティ特性（および／またはユーザアカウントのセキュリティパラメータ）として組織が定義したものの割り当て]に対する変更を情報システムがユーザに通知する。

(4) 前回ログオンに関する通知 |ログオンに関する追加情報の通知

ログオン（アクセス）に成功した際に、情報システムが[前回のログオン（アクセス）日時以外に含まれる情報として組織が定めたものの割り当て]についての追加情報をユーザに通知する。

補足的ガイダンス：この拡張管理策によって、ログオンする際にユーザに提供される予定の情報（例えば、前回ログオンした場所など）を組織が追加で指定できるようになる。なお、ユーザロケーションは、ネットワークにログオンした情報システムのユーザの IP アドレスによって特定することが可能な情報として定義されるとともに、情報システムのデバイス ID（または情報システムへのローカルログオンに関する通知など）によって特定することが可能な情報であとして定義される。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AC-10 同時セッションの制御

セキュリティ管理策：同時処理される[組織が定義したアカウントの割り当て（および／または組織が定義したアカウントタイプの割り当て）]の各セッションの数を情報システムが[組織が定めた数の割り当て]まで制限する。

補足的ガイダンス：組織は、情報システムアカウントのセッションのうち同時処理されるセッションの数の最大値をアカウントタイプ別（例：特権ユーザもしくは特権ユーザ以外のユーザ別またはドメインもしくは特定のアプリケーション別）および／またはアカウント別にグローバルに定義してもよい。具体的には、組織は、システム管理者（または特に重要なドメインにおける作業を行っている個人）が同時処理するセッションの数を制限（またはミッションクリティカルなアプリケーションの数を制限）してもよい。なお、このセキュリティ管理策は、情報システムアカウントのセッションのうち同時処理されるセッションに対する管理策である。ただし、このセキュリティ管理策は、情報システムアカウントのセッションのうちシングルユーザによって同時処理される複数のセッションに対する管理策ではない。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

3	**低** 選択されていない	**中** 選択されていない	**高** AC-10

AC-11 セッションのロック

セキュリティ管理策:

a. [組織が定めた期間の割り当て]によってアイドル時間が割り当てられた場合(またはユーザから要求された場合)、情報システムがセッションをロックすることによって以降のアクセスを遮断する。

b. 識別手順として確立された手順とともに認証手順として確立された手順を用いたユーザによってアクセスが再確立されるまで、情報システムがセッションをロックする。

補足的ガイダンス:セッションロックは、ユーザが作業を中断して情報システムのから離れる時間が一時的であることからログアウトしたくない場合に行われる一時的なアクションである。なお、セッションロックは、セッションがアクティブである場合に実行され、通常はオペレーティングシステムレベルで行われる一方、アプリケーションレベルで行われる場合もある。ただし、組織がユーザに対して 1 日の作業が終わった際に情報システムからログアウトすることを義務付けている等の場合、ログアウトする代わりにセッションをロックする事はできない。なお、関連するセキュリティ管理策は、AC-7 である。

拡張管理策:

(1) セッションのロック | セッションのパターンを隠して表示する

従来は画面上で誰でも見る事ができた画像を情報システムがセッションロックによって隠す。

補足的ガイダンス:従来は誰でも見る事ができた画像には、スクリーンセーバのパターンといった動的(または静的)な画像に加えて、バッテリーのインジケーター等の動的(または静的)な画像が含まれている事があるとともに、写真画像・単色画像・時計・ブランクスクリーン等の動的(または静的)な画像が含まれている事がある。ただし、これらの動的(または静的)な画像は、いずれも機微な情報ではない。

参考文献:OMB Memorandum 06-16

優先順位とベースライン管理策の割り当て:

P3	**低** 選択されていない	**中** AC-11 (1)	**高** AC-11 (1)

AC-12 セッションの終了

セキュリティ管理策:[セッションの切断が必要な条件(または組織が定義したトリガーイベント)として組織が定義したものの割り当て]後に、情報システムがユーザセッションを自動的に終了させる。

補足的ガイダンス:このセキュリティ管理策は、この文書のSC-10のセキュリティ管理策とは異なり、ネットワーク接続のセッションが終了する場合(すなわち、ネットワークが切断される場合)のセキュリティ管理策ではなく、ユーザによって確立された論理セッションが終了する場合のセキュリティ管理策である。なお、ローカルセッション・ネットワークセッション・リモートアクセスセッションとしてユーザによって確立された論理セッションは、ユーザ(またはユーザプロセス)が組織の情報システムにアクセスすることによって確立される。また、当該セッションに関連して、ネットワークセッション以外のセッションについてユーザがネットワークセッションを終了させるなく終了させる事によって、ユーザは組織の情報システムへのアクセスを終了する事ができる。ただし、ローカルセッション・ネットワークセッション・リモートアクセスセッションとしてユーザによって確立された論理セッションが終了する事によって、当該論理セッションに関係した全てのプロセス(ただし、当該論理セッションが終了した後も継続するプロセスとしてセッションのオーナーであるユ

ーザによって作成された特定のものを除く）が終了する。なお、当該論理セッションが自動的に終了する際の前提条件として（または当該論理セッションが必ず自動的に終了する際のトリガーイベント）として、組織が定めた期間にわたってユーザがアクティブでない事に加えて、特定のタイプのインシデントのみに対応している事とともに、時間帯によって情報システムの利用が制限される事などが挙げられる。また、関連するセキュリティ管理策は、SC-10およびSC-23である。

拡張管理策:

(1) セッションの終了 | ユーザによるログアウト /ユーザが操作したことによるメッセージ表示

(a) [組織が定めた情報資源の割り当て]のためにユーザ認証を利用しなければならない場合、ユーザによって開始された通信セッションをユーザがログアウトできる機能を情報システムが提供する

(b) 認証された通信セッションが確実に終了した旨を示す明示的なログアウトメッセージを情報システムがユーザに対して表示する。

補足的ガイダンス:認証されたユーザがアクセスできる情報資源には、ローカルワークステーション・データベース等に加えて、（それぞれパスワードで保護されている）ウェブサイト・ウェブサービスがある。なお、アクセスしたウェブページからログアウトした際に表示されるメッセージは、認証されたセッションが終了した後などに表示することができる。ただし、FTP（ファイル転送プロトコル）セッションなどの一部の対話型セッションの場合、情報システムはセッションが終了する前の最終メッセージとして通常はログアウトメッセージを表示する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** AC-12	**高** AC-12

AC-13 監視およびレビュー:アクセス制御

[削除された:AC-2 および AU-6 に統合された]

AC-14 ユーザによる識別（またはユーザによる認証）が不要なアクションとして許可されたもの

セキュリティ管理策:

a. 組織のミッションおよび／または組織の業務機能に応じて、情報システム上で識別または認証なしで実施できる[組織が定義したユーザアクションの割り当て]情報システムがを識別する

b. 裏付けとなる根拠をユーザによる識別（またはユーザによる認証）が不要なアクションとは何かとともに組織が情報システムのセキュリティ計画に記載する。

補足的ガイダンス:このセキュリティ管理策は、組織の情報システムユーザによる識別（またはユーザによる認証）が不要であると組織が判断した場合に対処するためのセキュリティ管理策である。公式サイトなど連邦政府の情報システムのうち個人がアクセス可能な情報システムにアクセスする場合とともに、個人が携帯電話を利用して電話を受信する（またはファクシミリを受信する）場合、組織はユーザによって識別・認証されないユーザアクションを限定的に許可してもよい。また、組織は、ユーザによる識別（またはユーザによる認証）が通常は必要なアクションでありながら特定の状況下（例:緊急時）ではユーザによる識別（またはユーザによる認証）というメカニズムをバイパスするアクションについて定義する。なお、ユーザによる識別（またはユーザによる認証）という通常必要なメカニズムをバイパスするアクションは、ログオン機能をバイパスする物理スイッチとしてソフトウェアで読み取り可能なもののうち、監視される（または誤って

使用されない）スイッチ等を介して行われる可能性がある。また、このセキュリティ管理策は、再識別および再認証がまだの場合には適用される一方、ユーザが再識別と（および再認証）することがない場合には適用されない。ただし、組織は、組織の情報システムにおいてユーザによって識別・認証されないユーザアクションとがない（すなわち、「指定」ステートメントの値は「0」となる）事を定めてもよい。なお、関連するセキュリティ管理策は CP-2 および IA-2 である。

拡張管理策：なし

(1) 識別または認証を必要としないアクション | 必要な利用

[削除された：AC-14 に統合された]

参考文献：なし

優先順位とベースライン管理策の割り当て：

P3	**低** AC-14	**中** AC-14	**高** AC-14

AC-15 自動マーキング

[削除された：MP-3 に統合された]

AC-16 セキュリティ属性

セキュリティ管理策：

a. ［組織が定義したセキュリティ属性値の割り当て］を伴う［組織が定義したタイプのセキュリティ属性の割り当て］を保存中・処理中・伝送中の情報（もしくは保存中・処理中・伝送中のいずれかの情報）と関連付けて行う手段を組織が提供する

b. セキュリティ属性と保存中・処理中・伝送中の情報（もしくは保存中・処理中・伝送中のいずれかの情報）との関連付けが組織によって確実に維持されるようにする

c. 組織が［組織が定義した情報システムの割り当て］のために許可された［組織が定義したセキュリティ属性の割り当て］を設定する

d. 設定されたセキュリティ属性の各々に対して許容される［組織が定義した値（または組織が定義した範囲）の割り当て］について組織が決定する

補足的ガイダンス：情報システム内の情報は、データ構造という抽象概念を用いて内部的に表現される。なお、内部データ構造は、能動的エンティティ・受動的エンティティという2つのエンティティのどちらでもありうる。ただし、サブジェクトの名称でも知られている能動的エンティティは、個人・デバイス・ユーザプロセスのいずれかに通常は関連付けられる。また、オブジェクトの名称でも知られている受動的エンティティは、レコード・バッファ・テーブル・ファイル・プロセス間パイプ・COM ポートなどのデータ構造体に通常は関連付けられる。

メタデータの形式をとるセキュリティ属性とは、情報保護関連の能動的エンティティ（および情報保護関連の受動的エンティティ）の基本的なプロパティ（または基本的な特性）を表す抽象概念である。なお、メタデータの形式をとるセキュリティ属性は、情報を受信（または送信）する可能性のあるアクティブなエンティティ（すなわち、情報を送受信する可能性のあるサブジェクト）と関連付けられる可能性があるとともに、オブジェクト間で情報をやりとりできるようにする能動的エンティティ（すなわち、オブジェクト間で情報をやりとりできるようにするサブジェクト）と関連付けられる可能性が有る。また、メタデータの形式をとるセキュリティ属性は、情報システムの状態を変化させる能動的エンティティ（すなわち、情報システムの状態を変化させるサブジェクト）と関連付けられる可能性もある一方、情報を格納する受動的なエンティティ（すなわち、情報を格納するオブジェクト）に関連付けられる可能性もあるとともに、情報を受け取る受動的なエンティティ（すなわち、情報を受け取るオブジェクト）と関連付けられる可能性もある。

セキュリティ属性がサブジェクトおよびオブジェクトと関連付けられることをデータバインディングという。なお、データバインディング時に、通常は属性タイプが属性値とともに設定される。

アクセス制御に関する情報セキュリティポリシー（および情報フロー制御ポリシー）は、情報システムの機能（または情報システムのメカニズム）を通じて（もしくは組織的プロセスを通じて）セキュリティ属性が別のデータと関連付けられる事によって適用可能となる。なお、セキュリティ属性の内容（またはセキュリティ属性として割り当てられた値）は、個人が組織の情報にアクセスできるかどうかを直接左右する。

組織は、選択された情報システムによるミッションおよび／または業務機能のサポートに必要な属性のタイプを定義する事ができる。なお、セキュリティ属性として割り当て可能な値の範囲が広い可能性があるとともに、情報の公開に当っては、「アメリカ合衆国のみ」・「北大西洋条約機構向け」・「外国人には公開不可」などと記される可能性もある。また、許容される属性値をその範囲とともに指定することによって、組織はセキュリティ属性値を有意かつ適切な値に保つ事ができる。

セキュリティラベリングという用語は、情報システムベースの情報セキュリティポリシーを適用することができるようセキュリティ属性を組織の情報システムのデータ構造として内部的に表現されたサブジェクト（および組織の情報システムのデータ構造として内部的に表現されたオブジェクト）と関連付けることを指す。なお、セキュリティラベリングされたラベルには、データライフサイクルを管理することによってラベル付けされたラベル（すなわち、暗号に加えて、データの期限）とともに、アクセス権限・国籍・請負関係に加えて、法令上遵守すべき要件に従って分類された情報などがある。

「セキュリティマーキング」という用語は、組織が情報セキュリティポリシーをプロセスごとに適用することができるよう、セキュリティ属性を人間が判読できるフォームでオブジェクトと関連付けることであるため、組織はプロセスをベースに情報セキュリティポリシーを適用することが可能になる。

この文書の AC-16 のベースライン管理策は、ユーザのセキュリティ属性を関連付ける（すなわち、マーキング）に当たっての要求事項である。また、AC-16 の拡張管理策は、情報システムのセキュリティ属性を関連付ける（すなわち、ラベリング）るに当たっての追加要求事項でもある。なお、セキュリティ属性のタイプには、オブジェクトの分類レベルに加えてサブジェクトのセキュリティ許容度（すなわち、サブジェクトへのアクセス権限のレベル）等があり、極秘のセキュリティラベルは、（オブジェクトの分類レベルおよびサブジェクトのセキュリティ許容度の）双方のタイプのセキュリティ属性のラベルの一例である。また、関連するセキュリティ管理策は、AC-3・AC-4・AC-6・AC-21・AU-2・AU-10・SC-16・MP-3 である。

拡張管理策:

(1) セキュリティ属性 |セキュリティ属性の動的な関連付け

情報システムは、情報が作成・結合された際、［組織が定義したセキュリティポリシーの割り当て］に沿った［組織が定義したサブジェクト（組織が定義したオブジェクト）の割り当て］によって情報システムがセキュリティ属性を動的に関連付ける。

補足的ガイダンス:情報のセキュリティ特性が時間の経過と共に変化しようとも、セキュリティ属性の動的な関連付けは常に適切である。なお、セキュリティ属性は、例えば、情報要素を組み合わせるに当たっての問題（すなわち、個々の情報要素のセキュリティ特性は個々の情報要素の組み合わせのセキュリティ特性とは異なるということ）に起因するとともに、個々のアクセス権限（すなわち、個々のアクセス特権）の変化に加えて、情報のセキュリティカテゴリの変化等に起因して変化する可能性がある。なお、関連するセキュリティ管理策は、AC-4 である。

(2) セキュリティ属性 |アクセスが承認された個人によるセキュリティ属性値の変更

アクセスが承認された個人（またはアクセスが承認されたユーザプロセス）に情報システムがセキュリティ属性の値を定義・変更できる機能を提供する。

補足的ガイダンス：セキュリティ属性の内容（または割り当てられたセキュリティ属性値）は個人が組織の情報にアクセスできるか否かを直接左右するため、セキュリティ属性の作成・変更能力を情報システムがアクセス承認済みユーザに限定できるかどうかが重要となる。なお、関連するセキュリティ管理策は、AC-6 および AU-2 である。

(3) セキュリティ属性 | 情報システムによって関連付けられたセキュリティ属性のメンテナンス

整合性を確保しながら情報システムが［組織が定義したセキュリティ属性の割り当て］と［組織が定義したサブジェクト（および組織が定義したオブジェクト）の割り当て］との関連付けを維持する。

補足的ガイダンス：セキュリティが十分に確保された状態で整合性を確保しながらセキュリティ属性をサブジェクトおよびオブジェクトに関連付けることによって、自動的に適用されるポリシーの基盤として、関連付けられたセキュリティ属性を活用することができる。なお、自動的に適用されるポリシーには、アクセス制御または情報フロー制御等がある。

(4) セキュリティ属性 |アクセスが承認されたユーザによるセキュリティ属性の関連付け

情報システムがユーザプロセス（または許可された個人）による［組織が定義したセキュリティ属性の割り当て］と［組織が定義したサブジェクト（および組織が定義したオブジェクト）の割り当て］との関連付けについてサポートする。

補足的ガイダンス：情報システムによるサポートは、①特定の情報オブジェクトに関連付けられるセキュリティ属性を選択するようユーザに対して要求する②定義されたポリシーに基づいて適切なセキュリティ属性によって情報を分類するための自動化されたメカニズムの使用③選択されたセキュリティ属性の組み合わせが有効であることを確認する等、多岐にわたる可能性がある。なお、監査可能なイベントを定義する際、組織はセキュリティ属性を作成または削除（もしくは変更）することについて検討する。

(5) セキュリティ属性 | 出力装置用にセキュリティ属性を表示

［人間が判読可能な形式を持っている標準的な命名規則として組織が定義したものの割り当て］を用いて［特殊な配布命令または特殊な処理命令（もしくは特殊な配信命令）として組織が定義したものの割り当て］を識別するために情報システムが出力デバイスへ送信するセキュリティ属性について、情報システムとしてオブジェクトとして（人間が判読可能なフォームで表示する。

補足的ガイダンス：情報システムの出力先には、例えば、ページ・スクリーン等が（またはそれらと同等の形式がなものとともに）ある。なお、情報システムの出力デバイスには、それぞれワークステーションと接続されているプリンターおよびビデオディスプレイに加えて、ノートパソコン・携帯情報端末等がある。

(6) セキュリティ属性 | 組織によるセキュリティ属性の関連付けの維持

［組織が定義したセキュリティポリシーの割り当て］に応じて関連付けることを組織が職員に対して許可することによって相互に関連付けられた［組織が定義したセキュリティ属性の割り当て］および［組織が定義したサブジェクト（および組織が定義したオブジェクト）の割り当て］のそれぞれを維持する事について、組織が職員に対して許可する。

補足的ガイダンス：この拡張管理策は、個々のユーザに対して（情報システムの場合とは逆に）セキュリティ属性とサブジェクト（またはオブジェクト）との関連付けを維持する事を要求する。

(7) セキュリティ属性 |整合性の取れた属性解釈

配置された情報システムコンポーネント間で送信されるセキュリティ属性にの解釈について、組織が提供する。

補足的ガイダンス：分散情報システム（例：分散型データベース管理システム・サービス指向アーキテクチャ等に加えて、クラウドベースのシステム）の複数のコンポーネントにセキュリティポリシーを適用するために、組織はセキュリティ属性を適切に変換することによってアクセス・情報フローを強制する。なお、組織は、分散情報システムの全てのコンポーネントがセキュリティ属性を適切かつ自動的に変換する事によってアクセス（および／または情報フロー）を強制するセキュリティ属性の実装契約を締結する。また、組織は、分散情報システムの全てのコンポーネントがセキュリティ属性を適切かつ自動的に変換することによってアクセス（および／または情報フロー）を強制するセキュリティ属性の実装プロセスを確立する。

(8) セキュリティ属性 |情報をセキュリティ属性に関連付ける手法 /情報をセキュリティ属性に関連付けるテクノロジー

情報をセキュリティ属性に関連付けるなかで、情報システムが［組織が定めた水準のセキュリティの保証］によって［組織が定義した手法または（組織が定義したテクノロジー）の割り当て］を実装する。

補足的ガイダンス：アクセスを自動的に強制（および情報フローを自動的に強制）する上で、セキュリティ属性がシステム内の情報と関連付いていること（すなわち、データバインディング）が非常に重要である。なお、セキュリティ属性は、様々なレベルでセキュリティを保証する手法（および／または様々なレベルでセキュリティを保証するテクノロジー）を用いることによってシステム内の情報と関連付く。例えば、情報システムは、ハードウェアの信頼ルートとしてハードウェア機器によって保護される支援暗号鍵付きの電子署名を使って、セキュリティ属性と情報とを暗号でバインドすることができる。

(9) セキュリティ属性 | セキュリティ属性の再割り当て

情報に関連付けられたセキュリティ属性が［組織が定義した技法（または組織が定義した手順）の割り当て］によるセキュリティ属性の再構成のメカニズムのなかでのみ再度割り当てられることを組織が保証する。

補足的ガイダンス：セキュリティ属性を構成するメカニズムとして正当なものは、セキュリティ属性を再度割り当てるのに必要なレベルのセキュリティについて組織が保証するために使利用される。なお、セキュリティ属性を再構成するメカニズムの正当性は、セキュリティ属性を再構成する目的は一つであるという保証によって高まるとともに、当該メカニズムは限定的な機能のみを有するということが保証されることによって高まる。また、再度割り当てられたセキュリティ属性がアクセス（および／または情報フロー）の強制等によって適用されるセキュリティポリシーに影響を与える可能性があるため、セキュリティ属性を再構成するメカニズムが適切な（および／または正しい）操作モードで実行できるよう、セキュリティ属性を構成するメカニズムとして信頼に値するものを使用することが必要である。

(10) セキュリティ属性 |認可された個人による属性の構成

サブジェクトおよびオブジェクトの両方に関連付けることが可能なセキュリティ属性のタイプについて、当該属性の値とともに定義・変更できる能力を情報システムが認可された個人に対して提供する。

補足的ガイダンス：セキュリティ属性の内容（またはセキュリティ属性に割り当てられた値）は個人が組織の情報にアクセスする能力に直接的な影響を及ぼすことができるため、情報システムがセキュリティ属性の作成能力をセキュリティ属性の変更能力とともに認可された個人のみに制限できるようになることが重要である。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AC-17 リモートアクセス

セキュリティ管理策:

a. 許可されているリモートアクセスのタイプごとに組織が使用制限・構成要件(および/または接続要件)・実装ガイダンスを定めて文書化する

b. 情報システムに対してリモートアクセスを許可する前に組織が情報システムに対するリモートアクセスを承認する。

補足的ガイダンス:リモートアクセスとは、ユーザ(またはユーザのために機能するプロセス)が外部ネットワーク(例:インターネット)を通じて組織の情報システムにアクセスすることである。なお、リモートアクセスには、例えば、ダイアルアップ・ブロードバンド・ワイヤレス等の方式がある。また、組織は、通常、リモート接続における機密性を暗号化された仮想プライベートネットワークを利用して完全性とともに向上させることが多い。ただし、暗号化された仮想プライベートネットワークの利用がすなわちリモートアクセスの実現につながらない一方、適切なセキュリティ管理策が十分に提供された場合(すなわち、情報の機密性とともに情報の完全性を適切に保護するための暗号技術が用いられた場合)、組織による内部ネットワークへのリモート接続が事実上常に可能となる可能性は十分にある。なお、仮想プライベートネットワーク接続は外部ネットワークに対して行われるため、暗号化された仮想プライベートネットワークによってリモート接続の可用性が向上することはない。また、悪質コードを探すために組織がネットワーク通信トラフィックを適切に監視する能力は、暗号化トンネルを利用する仮想プライベートネットワークの影響を受ける可能性がある。ただし、リモートアクセスに関するセキュリティ管理策は、パブリック Web サーバー(またはパブリックアクセス用に設計された情報システム)以外の情報システムに適用される。なお、このセキュリティ管理策は、リモートアクセスが設定されていないにもかかわらずリモートアクセスを許可する前提としてリモートアクセス権限を付与する場合に関連して策定されたものである。また、このセキュリティ管理策では、組織は相互接続のセキュリティに関する合意に基づいてリモートアクセスを許可する必要がないのに対して、この文書の AC-3 のセキュリティ管理策はリモートアクセスを強制的に制限する。なお、この AC-17 の管理策に関連するセキュリティ管理策は AC-2・AC-3・AC-18・AC-19・AC-20・CA-3・CA-7・CM-8・IA-2・IA-3・IA-8・MA-4・PE-17・PL-4・SC-10・SI-4 である。

拡張管理策:

(1) リモートアクセス | 自動監視 / 自動制御

情報システムがリモートアクセス方式を監視・制御する。

補足的ガイダンス:リモートアクセスセッションが自動で監視・制御されることによって、組織はサイバー攻撃を検知することが可能になるとともに、組織は情報システムのさまざまなコンポーネントへのリモートアクセスを監査することによって従来のリモートアクセスポリシーに準拠出来るようになる。なお、関連するセキュリティ管理策は、AU-2 および AU-12 である。

(2) リモートアクセス | 暗号化を用いた機密性の保護 / 暗号化を用いた完全性の保護

リモートアクセスセッションの機密性を完全性とともに保護するため、情報システムに暗号メカニズムを実装する。

補足的ガイダンス：暗号メカニズムに求められる暗号化の強度は、情報のセキュリティカテゴリに基づいて決まる。なお、関連するセキュリティ管理策は、SC-8・SC-12・SC-13 である。

(3) リモートアクセス | 管理されたアクセス制御ポイント

[組織が定めた数の割り当て]によってネットワークへのアクセスが管理される場合、情報システムはすべてのリモートアクセスが制御ポイントに対して行われるようにする。

補足的ガイダンス：組織は、リモートアクセス先の制御ポイントの数を制限することによって攻撃対象領域を減らすことができる。なお、組織は Trusted Internet Connections（TIC）のイニシアチブが要求する事項を考慮して外部のネットワークと接続する。また、関連するセキュリティ管理策は、SC-7 の管理策である。

(4) リモートアクセス | 特権的コマンド / 特権的アクセス

(a) 組織が[組織が定めたニーズの割り当て]のみを目的としたリモートアクセスによる特権コマンドの実行を（リモートアクセスによるセキュリティ関連情報へのアクセスとともに）認可する。

(b) 情報システムのセキュリティ計画に、組織がリモートアクセスによって特権コマンドを実行した理由とともにリモートアクセスによってセキュリティ関連情報にアクセスした理由を記載する。

補足的ガイダンス：この拡張管理策に関連するセキュリティ管理策は AC-6 である。

(5) リモートアクセス |認可されていない接続の有無の監視

[削除：SI-4 に統合]

(6) リモートアクセス | 情報の保護

組織はユーザがリモートアクセスメカニズムに関する情報を不正使用・不正開示から確実に保護できるようにする。

補足的ガイダンス：この拡張管理策に関連するセキュリティ管理策は、AT-2・AT-3・PS-6 である。

(7) リモートアクセス | セキュリティ機能へのアクセスを保護するための追加措置

[削除：AC-3 (10)に統合]

(8) リモートアクセス | セキュアでないネットワークプロトコルの無効化

[削除:CM-7 に統合]

(9) リモートアクセス | アクセスの切断および/または無効化

情報システムへのリモートアクセスについて[組織が定めた期間の割り当て]の範囲内で迅速に切断・無効化する機能を組織が提供する。

補足的ガイダンス：この拡張管理策は、組織がユーザによる情報システムへのリモートアクセスを迅速に切断する能力および／またはリモートアクセスを無効化する機能を有するよう要求する管理策である。なお、リモートアクセスをどれだけ早く切断（または無効化）出来るかは、ミッション（および／または業務機能）の重要性によって異なるとともに、組織の情報システムへのリモートアクセスを直ちに削除しなければならないのかによっても異なる。

参考文献：NIST Special Publications 800-46・NIST Special Publications 800-77・NIST Special Publications 800-113・NIST Special Publications 800-114・NIST Special Publications 800-121

優先順位とベースライン管理策の割り当て：

P1	**低** AC-17	**中** AC-17 (1) (2) (3) (4)	**高** AC-17 (1) (2) (3) (4)

AC-18 ワイヤレスアクセス

セキュリティ管理策:

a. ワイヤレスアクセスの使用を制限するとともに、ワイヤレスアクセスの実装ガイダンスを設定要件および／または接続要件とともに定める。

b. 情報システムへの無線によるアクセスを許可するのに先立って、無線で情報システムにアクセスする権限を与える。

補足的ガイダンス:ワイヤレス技術には、例えば、マイクロ波・パケット無線(UHF/VHF)・802.11x・Bluetooth 等がある。また、ワイヤレスネットワークでは、資格情報の保護を可能にするとともに相互認証を可能にする認証プロトコル（例: EAP/TLS・PEAP 等）が用いられる。なお、関連するセキュリティ管理策は AC-2・AC-3・AC-17・AC-19・CA-3・CA-7・CM-8・IA-2・IA-3・IA-8・PL-4・SI-4 の管理策である。

拡張管理策:

(1) ワイヤレスアクセス | 認証および暗号化

情報システムへの無線アクセスは、[ユーザおよび機器を（複数）選択]による認証を暗号化とともに用いることによって保護する。

補足的ガイダンス:関連するセキュリティ管理策は SC-8 および SC-13 の管理策である。

(2) ワイヤレスアクセス | 許可されていない接続の監視

[削除:SI-4 に統合]

(3) ワイヤレスアクセス | ワイヤレスネットワークの無効化

導入・展開する情報システムコンポーネントに組み込まれているワイヤレスネットワーク機能が使用されない場合、組織が当該機能を無効にする。

補足的ガイダンス:関連するセキュリティ管理策は AC-19 の管理策である。

(4) ワイヤレスアクセス | ユーザによるを制限する

組織によってワイヤレスネットワーク機能を個別に設定することが認められたユーザに対して、組織が明示的な許可を与える。

補足的ガイダンス:選ばれたユーザによるワイヤレスネットワーク機能の構成を組織に許可するアクセス権限の一部は、組織の情報システムにおけるアクセス強制のメカニズムを通じて適用される。なお、関連するセキュリティ管理策は、AC-3 および SC-15 の管理策である。

(5) ワイヤレスアクセス | アンテナの水準/送信される電力の水準

セキュリティの外側で使用可能な信号を受信してしまう確率が低くなるよう、組織がラジオアンテナを選択するとともに、送信される信号の出力レベルを調整する。

補足的ガイダンス:セキュリティ境界の外側で不正な無線通信を抑制するために組織が取る措置の一例として、①組織の物理的境界の外側に存在する敵対者によって使用可能な信号が発せられる可能性を減らすために、無線通信の出力を下げる②TEMPEST などの対策を用いて、無線伝送を制御する③受信者が期せずして信号を傍受する可能性を減少させる指向性アンテナおよび／またはビーム形成アンテナを使用する等がある。なお、組織は、組織の情報システムのみならずセキュリティ境界の内側で稼動している可能性のある他の情報システムの周波数プロファイルを知るための上記の措置を取る前に定期的な無線調査を上記の措置を取る前に行うことができる。なお、関連するセキュリティ管理策は PE-19 の管理策である。

参考文献:NIST Special Publications 800-48・NIST Special Publications 800-94・NIST Special Publications 800-97

優先順位とベースライン管理策の割り当て:

P1	**低** AC-18	**中** AC-18 (1)	**高** AC-18 (1) (4) (5)

AC-19 携帯機器に対するアクセス制御

セキュリティ管理策:

a. 管理する携帯機器の使用を組織が制限するとともに、管理する携帯機器について組織が設定要件を接続要件および実装ガイダンスとともに定める

b. 携帯機器から組織の情報システムへ接続することを組織が承認する。

補足的ガイダンス:携帯機器とは、スマートフォン・電子書籍端末・タブレット等、①小型のフォームファクターとして一人の人間が簡単に持ち運べるコンピュータデバイスであるとともに、②物理接続なしで稼働する設計になっている(例:無線で情報を送受信する)コンピュータデバイスである。なお、携帯機器は、③ローカルの取り外し可能な(および/またはローカルの取り外し不可能な)データ記憶装置を有するコンピュータデバイスであるとともに、④内蔵型の電源を備えているコンピュータデバイスでもある。ただし、携帯機器には、音声通信機能(および/または情報を携帯機器に取り込むためのセンサー)が搭載されている場合がある。また、ローカルデータをリモートデータと同期させるために内蔵されている機能が音声通信機能とともに搭載されている場合があるとともに、情報を携帯機器に取り込むためのセンサーがローカルデータをリモートデータと同期させるために内蔵されている機能とともに搭載されている場合がある。なお、情報を携帯機器に取り込むためのセンサー(またはローカルデータをリモートデータと同期させるために内蔵されている機能のいずれか)が単独で搭載されている場合もある。

携帯機器は、通常、紐付けられた個々人の近くに存在する。ただし、どの程度まで近くに置かれるかは、携帯機器の形状と大きさによって異なりうる。また、携帯機器の使用目的に加えてその性質によっては、携帯機器がデータを処理する能力は、データ容量・通信能力とともにデスクトップ端末に匹敵する場合もある一方、データ容量・通信能力とともに単にデスクトップ端末の能力の一部を構成するに過ぎない場合もある。なお、携帯機器は技術特性・機能ともにそれぞれに異なる多種多様なものであるため、組織が携帯機器を利用する際の制約は、携帯機器の種類ごとに異なりうる。

携帯機器の利用を制約する場合と同様、携帯機器の実装に関するガイダンスのうち特定のものには、例えば、構成管理ならびに機器の識別および機器の認証に加えて、悪質コードの検出(またはファイアウォールの設定)といった必須のソフトウェアとしての防護ソフトの実装と合わせて、悪質コードを検出するための携帯端末のスキャン等の内容が盛り込まれているとともに、ウイルス防御ソフトのアップデートに加えて、クリティカルなソフトウェアアップデートの有無のスキャンおよびパッチの有無のスキャンと合わせて、プライマリオペレーティングシステム(場合によっては他の常駐ソフトウェア)のインテグリティチェックの実施が含まれている。また、携帯機器の実装に関するガイダンスのうち特定のものには、携帯機器の利用を制約する場合と同様に、不必要なハードウェア(例:無線ハードウェア・赤外線ハードウェア)の無効化も含まれている。なお、組織は、携帯機器のセキュリティが十分確保されるようにする必要性については、このセキュリティ管理策で要求される範囲を超えた事項であることに留意しなければならない。

携帯機器を保護するための機能は、携帯機器を防護するための対策と同様、策定されるセキュリティ計画の根幹をなすセキュリティ管理策のベースライン管理策として当初策定されたセキュリティ管理策のカタログを構成する他のセキュリティ管理策に反映されている。また、携帯機器を防護するための対策と同様、携帯機器を保護するための機能は、オーバーレイを開始するためのセキュリティ管理策のベースライン管理策として当初策定されたセキュリティ管理策のカタログを構成する他のセキュリティ管理策に反映されている。ただし、異なるセキュリティ管理策ファミリに属するセキュリティ管理策に規定されている要求事項が部分的に重複している場合が

ある。なお、関連するセキュリティ管理策は AC-3・AC-7・AC-18・AC-20・CA-9・CM-2・IA-2・IA-3・MP-2・MP-4・MP-5・PL-4・SC-7・SC-43・SI-3・SI-4 であり、そのうち AC-20 のセキュリティ管理策は、組織の管理下にない携帯機器に対応した管理策である。

拡張管理策:

(1) 携帯機器に対するアクセス制御 | 書き込み可能および/または持ち運び可能な記憶装置の使用

[削除:MP-7 のセキュリティ管理策に統合済]。

(2) 携帯機器に対するアクセス制御 |個人のポータブル記憶装置の使用

[削除:MP-7 の管理策に統合済]。

(3) 携帯機器に対するアクセス制御 | 所有者が特定できないポータブル記憶装置の使用[削除:MP-7 に統合済]。

(4) 携帯機器に対するアクセス制御 | 機密情報に関する制限

(a) 運用認可責任者によって許可されている場合を除き、機密情報を処理または保存もしくは伝送する情報システムが設置されている施設による未確認の携帯機器の使用を組織が禁止する

(b) 機密情報を処理・保存・伝送する情報システムが設置されている施設において、非未確認の携帯を使用することが運用認可責任者によって許可されている個人に対して、組織が以下の制限を実施する:

(1) 機密情報システムに未確認の携帯機器が接続を禁止する

(2) 未確認の携帯機器が未確認の情報システムに接続する場合に、運用認可責任者による承認を必要条件とする

(3) 未確認の携帯機器に組み込まれている内蔵モデムもしくは外付けモデムまたは無線インターフェースの使用を禁止する

(4) 非未確認の携帯機器は、機器それらに保存されている情報とともに、[組織が定めたセキュリティ担当者の割り当て]による無作為検査の対象となる。なお、機密情報が見つかった場合には、インシデント対応ポリシーに従う

(c) [組織が定めたセキュリティポリシーの割り当て]に従って、機密扱いの携帯機器による機密扱いの情報システムへの接続を制限する。

補足的ガイダンス:関連するセキュリティ管理策は、CA-6 および IR-4 の管理策である。

(5) 携帯機器に対するアクセス制御 | 機器全体の暗号化 / コンテナの暗号化

[組織が定めた携帯機器の割り当て]の際に情報の機密性を情報の完全性とともに保護するために、組織が[機器全体の暗号化またはコンテナの暗号化のいずれかを選択]する。

補足的ガイダンス:コンテナベースの暗号化によって、携帯機器に保存されているデータ(携帯機器に保存されている情報)をより細かく分けて暗号化できるようになることで、ファイル・レコード・フィールドなどのデータ構造を選択して暗号化できるようになる。なお、関連するセキュリティ管理策は、MP-5・SC-13・SC-28 の管理策である。

参考文献:OMB Memorandum 06-16・NIST Special Publications 800-114・NIST Special Publications 800-124・NIST Special Publications 800-164

優先順位とベースライン管理策の割り当て:

P1	**低** AC-19	**中** AC-19 (5)	**高** AC-19 (5)

AC-20 外部の情報システムの使用

セキュリティ管理策：外部の情報システムを所有および／または運用（および／または保守管理）する他の組織との間で確立された信頼関係に基づいて、組織が関係者に対して

a. 外部の情報システムから組織の情報システムにアクセスすること

b. 外部の情報システムを使用いて組織の管理下にある情報を処理または保存もしくは伝送すること

の二つを許可するうえでの条件を設定する。

補足的ガイダンス：外部の情報システムとは、組織による認許可の対象ではない情報システムまたは（情報システムの）コンポーネントとして、通常、必要なセキュリティ管理策の適用、セキュリティ管理策の有効性のアセスメントについて組織が直接管理監督できないものを指す。なお、外部の情報システムとは、具体的には、①ノートパソコン・スマートフォン・タブレット・携帯情報端末のうち、個人が所有する情報システム（および／または個人が所有するデバイス）②個人が所有するコンピュータデバイス（および個人が所有する通信機器）のうち、ホテル・鉄道駅・コンベンションセンター・ショッピングモール・空港といった商業（または公共）施設で使用されるもの③連邦政府以外の政府機関によって所有（または連邦政府以外の政府機関によって管理）されている情報システム④連邦政府の情報システムのうち、連邦政府の機関によって所有または運用もしくは直接管理監督されていないシステムを指す。なお、この A-20 のセキュリティ管理策は、クラウドサービス（IaaS・PaaS・SaaS 等）にアクセスする際など、組織の情報を処理または保存もしくは伝送する際に外部の情報システムを利用する際の管理策である。

連邦政府機関と当該政府機関の下部組織との間で成立している信頼関係次第では、連邦政府（または連邦政府の下部組織）が運用している外部の情報システムの一部に関連して、①外部の情報システムから組織の情報システムにアクセスすることおよび②外部の情報システムを用いて組織の管理下にある情報を処理または保存もしくは伝送することの二つを許可する上での条件を明示する必要がないもありうる。その場合、連邦政府（または連邦政府の下部組織）が運用している外部の情報システムは、外部の情報システムとはみなされない。例えば、ある連邦政府機関（または当該政府機関の下部組織）と他の連邦政府機関（または当該政府機関の下部組織）との間で情報システムの共有が前もって明示的に（または既に暗黙裡に）合意されている場合、前者の連邦政府機関（または当該政府機関の下部組織）の内部の情報システムが外部の情報システムとして認識されることはない。また、ある連邦政府機関（または当該政府機関の下部組織）と他の連邦政府機関（または当該政府機関の下部組織）との間で信頼関係が既に暗黙裡に成立している場合（もしくは信頼関係の成立が明示的に確認されている場合）または信頼関係の成立が法律・大統領命令・指令・政策によって規定されている場合、前者の連邦政府機関（または当該政府機関の下部組織）の内部の情報システムが外部の情報システムとして認識されることはない。なお、連邦政府機関において①外部の情報システムから組織の情報システムにアクセスすることおよび②外部の情報システムを用いて組織の管理下にある情報を処理または保存もしくは伝送することの二つが許可された個人とは、具体的には、システムにアクセスするに当たって行動規範を順守するよう組織が義務付けることができる者として、組織の職員・業務請負人をはじめ組織の情報システムへのアクセスが許可された者のことを指す。ただし、ある連邦政府機関（または当該政府機関の下部組織）と他の連邦政府機関（または当該政府機関の下部組織）との間で成立している信頼関係次第で上記行動規範の内容は変わりうるため上記行動規範それ自体は画一的である必要はないことから、連邦政府機関（または当該政府機関の下部組織）はセキュリティについてに対して州政府・地方政府・居留区政府のいずれとも異なる行動規範を順守するよう義務付けもよい。

このセキュリティ管理策は、外部の情報システムを利用して組織の情報システムのパブリックインターフェースにアクセスする（例：個人が www.usa.gov のサイトにアクセスすることによって連邦政府の情報にアクセスする）場合には適用されない。なお、組織は、外部の情報システムを使用するに当たっての諸条件を組織のセキュリティポリシー（およびセキュリティプロシジャー）

に従って定める。ただし、当該諸条件は、外部の情報システムから組織の情報システムにアクセス可能なアプリケーションの種類に加えて、外部情報システム上で処理・保存・伝送のいずれかがなされる情報のセキュリティを分類す最上位に位置付けられるもの等、最低限の条件として定められたものである。なお、外部情報システムの所有者との間で外部の情報システムを使用するに当たっての諸条件を定めることができない場合には、組織は外部システムを使用する組織の職員に対して行動規範を順守するよう義務付けてもよい。なお、関連するセキュリティ管理策は、AC-3・AC-17・AC-19・CA-3・PL-4・SA-9 の管理策である。

拡張管理策:

(1) 外部の情報システムの利用 |アクセス権限の制限

組織の情報システムに関連して外部の情報システムの利用について許可された個人によるアクセス(もしくは組織が管理する情報について外部の情報システムの利用を許可された個人による処理)または組織が管理する情報について外部の情報システムを利用許可された個人による保存(もしくは組織が管理する情報について外部の情報システムの利用を許可された個人による伝送)が組織によって許可されるのは、

(a) 外部の情報システム上で必要なセキュリティ管理策が組織の情報セキュリティポリシーおよび組織のセキュリティ計画に規定されている通りに実装されている事を確認した場合

(b) 情報システムへの接続として許可された接続を外部の情報システムを運用する組織との間で維持する場合または外部の情報システムを運用する組織との間で結んだ情報システムの処理に関する契約を維持する場合

に限られる。

補足的ガイダンス:この拡張管理策は、外部の情報システムを使用している個人(例:業務委託業者・業務提携者)が場合によっては組織の情報システムにアクセスする必要がある事を想定している。ただし、そのような状況下では、組織の情報システムのセキュリティが破られる事のないよう、また組織の情報システムが損害を受ける等の害が及ばないよう、組織は外部の情報システムに必要なセキュリティ対策(すなわち、セキュリティ管理策)が確実に実装されるようにする必要がある。なお、必要なセキュリティ管理策が実装されているかどうかは、組織が要求するセキュリティの水準次第では認証等によって確認することができると同時に、組織が要求するセキュリティの水準次第では第三者による独立した評価等によっても確認する事ができる。なお、この文書の中で関連するセキュリティ管理策は、CA-2 の管理策である。

(2) 外部情報システムの利用 | 持ち運び可能な記憶装置

許可された個人が外部の情報システムの一部として組織が管理する持ち運び可能な記憶装置を利用することについて組織が[制限するか禁止するかを選択]する。

補足的ガイダンス:外部の情報システムで組織が管理する持ち運び可能な記憶装置の利用が制限される例としては、当該装置の利用が完全に禁止されることを挙げることが出来るのに加えて、当該装置に対して想定される利用方法の制限とともに、当該装置装置をどのような状態で利用する可能性があるのかについての制約を挙げることができる。

(3) 外部の情報システムの利用 | 組織が所有していないシステム /組織が所有していないコンポーネント /組織が所有していないデバイス

組織が所有していない情報システムまたは組織が所有していないシステムコンポーネント(もしくは組織が所有していないデバイス)をして組織の情報の処理または保存(もしくは送信)のために利用することについて組織が[制限するか禁止するかを選択]する。

補足的ガイダンス:組織内部で所有していないデバイスには、他の組織(例:連邦政府機関・州政府機関・業務委託業者)が所有するデバイス等に加えて、私有のデバイス等も含ま

れる。ただし、組織内で所有していないデバイスの利用は、リスクを伴う。なお、場合によっては、組織内で所有していないデバイスの利用を禁止しなければならない水準までリスクが高い場合もある。また、場合によっては、組織内で所有していないデバイスの利用が許可されるものの、例えば、組織内で所有していないデバイスの利用が許可される前に、組織によって承認されたセキュリティ管理策の実装が要求される②情報・サービス・アプリケーションのうち特定のタイプのものに対するアクセスが制限される③組織が導入したサーバー等のシステムコンポーネントに対する処理（および組織が導入したサーバー等のシステムコンポーネントに保存すること）を制限するために、仮想化技術を利用させられる④利用に関する諸条件に同意させられるといった何らかの制約が課されることもある。なお、組織は私有のデバイスを業務環境で利用する事に伴う法律上の問題について（具体的には、インシデント発生後の調査時にデジタルフォレンジックを実施するための要件等を含めて）、法務担当部署に助言を求めなければならない。

(4) 外部情報システムの利用 | NAS デバイス

外部の情報システムでの［組織が定義した NAS デバイスの割り当て］を組織が禁止する。

補足的ガイダンス：外部の情報システム、を構成する NAS デバイスとは、具体的にはパブリッククラウドシステム・ハイブリッドクラウドシステム・コミュニティクラウドシステムを構成するオンラインストレージ装置等を指す。

参考文献：FIPS Publication 199

優先順位とベースライ管理策の割り当て：

P1	**低** AC-20	**中** AC-20 (1) (2)	**高** AC-20 (1) (2)

AC-21 情報共有

セキュリティ管理策：

a. ［ユーザが自由意志に基づいて情報を共有することが欠かせない場面として組織が定めた場面の指定］の際、情報を共有する相手に割り当てられたアクセス権限が当該情報に対するアクセス制限に適合するかどうかアクセス権限を有するユーザが判断できるようにするによって、組織が情報共有を促進する。

b. 情報共有および／またはコラボレーションに関してユーザが意思決定を行う際、組織が［自動化されたメカニズムとして組織が定義したもの（または組織が定義した手動プロセス）の割り当て］を通じて支援する。

補足的ガイダンス：このセキュリティ管理策は、何らかの形式的または管理運営上の決定に基づいて何らかの形で制限される情報（例：診察に関する情報および契約上の秘密情報に加えて、機密情報・個人情報とともに、特定のアクセスプログラムに関する機密情報または機密コンパートメント情報）に対して適用される。なお、情報を共有する相手については情報共有が行われる個別の場面に応じて個人レベルまたはグループレベル（もしくは組織レベル）で定義してもよい。また、共有する情報については、内容・タイプ・セキュリティカテゴリ・または特定のアクセスプログラムおよび／またはコンパートメントごとに定義してもよい。なお、関連するセキュリティ管理策は AC-3 の管理策である。

拡張管理策：

(1) 情報共有 | 自動的な情報共有のサポート

情報を共有する相手が有するアクセス権限に加えて、共有される情報に対するアクセス制限に即して、許可されたユーザに対してシステムが自動的に情報を共有させる

(2) 情報共有 | 情報の検索と取り出し

情報を検索・取得するサービスのうち、[情報共有に関連して組織が定めた制限の割り当て]を自動的に行うサービスを情報システムが実施する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** AC-21	**高** AC-21

AC-22 公開情報

セキュリティ管理策:

a. 公開情報のシステムに情報を掲載する権限のある個人を組織が指定する

b. 公開情報に非公開情報が決して含まれないよう、情報を掲載する権限のある個人に対して教育を行う

c. 公開情報のシステムに情報をアップロードする前に組織がアップロードされる予定の情報の内容を確認して、非公開情報が決して含まれないようにする

d. 公開情報のシステムに掲載されている情報の内容を確認するためのを[組織が定めた頻度での割り当て]実施して、非公開情報が含まれていることが判明した場合には、組織がそうした情報を削除する

補足的ガイダンス:連邦法・大統領命令・指令・政策・規制・標準・手引の全てまたは(それらのいずれかを理由に、プライバシー保護法によって保護されている情報(または機密情報)といった非公開情報に一般市民がアクセスすることは認められていない。なお、このセキュリティ管理策は、組織による管理のもと一般市民が通常は識別なしまたは認証なしで利用できる情報システムに対して策定された管理策である。なお、関連するセキュリティ管理策は、AC-3・AC-4・AT-2・AT-3・AU-13の管理策である。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P3	**低** AC-22	**中** AC-22	**高** AC-22

AC-23 データマイニングによる保護

セキュリティ管理策:組織情報に対するデータマイニングを認識することで組織の情報をデータマイニングから保護できるよう、[組織が定義したデータストレージオブジェクトの割り当て]に関連して、そうした行為から保護するために、組織が[指定:組織が定めた、データマイニングを認識・防止する手法として組織が定めた手法の割り当て]を行う。

補足的ガイダンス:データストレージオブジェクトには、データベース・データベースレコード・データベースフィールド等がある。また、データマイニングを認識・防止する手法には、①データベースクエリーに対する応答のタイプを指定する②(データマイニングを行おうとする者が)データストレージオブジェクトとしてのデータベースの内容を分析しようとする際、必要となる作業負荷を増やすことができるよう、データベースクエリーの数(および/またはデータベースクエリーの間隔)を指定する③データベースへの通常とは異なるアクセスまたは異常なデータベースクエリーが発生した場合に組織の職員へ知らせるといった手法がある。なお、このAC-23のセキュリテ

ィ管理策は、組織の情報として組織のデータストレージに存在している情報をデータマイニングから保護するための管理策である一方、AU-13のセキュリティ管理策は、データマイニングされた可能性のある（またはデータストアレージから取得された可能性のある）組織の情報のうち外部サイトに現存する公開情報としてソーシャルメディアサイト等を通じて入手可能な情報について管理するためのセキュリティ管理策である。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AC-24 アクセス制御に関する決定

セキュリティ管理策：アクセス要求のたびに［組織が下したアクセス制御の決定の割り当て］が強制アクセス制御を行う前に確実に適用されるようにするための手順を組織が定める。

補足的ガイダンス：アクセス制御の決定（「アクセス認可の決定と同義）は、アクセスが具体的に認可された場合に下される。のに対して、強制アクセス制御は、情報システムが具体的なアクセス制御強制的に行う場合を指す。ただし、アクセス制御の決定が強制アクセス制御の場合と同一のエンティティによって実装されるのが一般的である一方、アクセス制御の決定が強制アクセス制御の場合と同一のエンティティによって実装されなければならないということではなく、アクセス制御の決定が強制アクセス制御の場合と同一のエンティティによって実装される事が必ずしも常に最適な選択とは限らないため、一部のアーキテクチャ（および一部の分散情報システム）では、アクセス制御の決定が強制アクセス制御の場合とは異なるエンティティによって実装される可能性がある。　拡張管理策：

(1) アクセス制御の決定 | アクセス認可に関する情報の伝達

［組織が定義した情報システムの割り当て］のために、情報システムが［組織が定めたセキュリティ対策の割り当て］を利用して［組織が定義したアクセス認可情報の割り当て］を行う。

補足的ガイダンス：分散情報システムでは、アクセス認可プロセスがアクセス制御のプロセスとは異なる場所で実行される場合がある。ただし、この場合、アクセス制御のプロセスが適切な場所で適宜行われるよう、アクセス認可情報をがプロセス間で安全に受け渡される必要がある。また、分散情報システムでは複数の異なるアクセス制御が行われる必要があるとともに、何らかのセキュリティ属性を必要とする異なるエンティティ（例：サービス）による複数の異なるアクセス制御が連続的に行われることによって、アクセス制御のプロセスをサポートするセキュリティ属性を受け渡す必要が可能性もある。なお、アクセス認可（すなわち、アクセス制御）の情報を受け渡し中に改ざん・スプーフィング・侵害する事は、当該情報が保護されるため不可能である。

(2) アクセス制御の決定 | ユーザの識別情報（またはプロセスの識別情報）を含まない場合

ユーザ ID（またはユーザプロセス情報）を割り当てない［組織が定義したセキュリティ属性の割り当て］に基づいて、情報システムが強制アクセス制御を行なう。

補足的ガイダンス：重要なのは、特定の状況においては、アクセス制御のプロセスがアクセス要求を行ったユーザの ID を欠いたまま行なわれることがありうるということであって、それは、個人のプライバシーの保護が最重要視されているということを示す一般的な例となる。ただし、特定の状況以外の状況下では、ユーザ ID はアクセス制御を行う上で全く必要

ない。なお、分散情報システムの場合、ユーザ ID をセキュリティが十分に確保された状態で受け渡すことは不可能であるか、可能であったとしても莫大な費用がかかる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AC-25 リファレンスモニタ

セキュリティ管理策:[組織が定めたアクセス制御ポリシーの割り当て]のために常時機能しているリファレンスモニタとして改ざん防止機能を備えたもののうち、(リファレンスモニタの脆弱性またはリファレンスモニタの欠陥の有無を)分析・テストすることが可能なほど小規模なものであってセキュリティが完全に確保されているものを情報システムが実装する。

補足的ガイダンス:情報は、データ構造といわれる抽象概念を用いて内部的に表現される。なお、内部データ構造は、能動的・受動的の両方の異なるタイプのエンティティを表現することができる。また、サブジェクトとしても知られている能動的なエンティティは、通常、個人・機器・ユーザプロセスのいずれかに関係するエンティティであり、オブジェクトとしても知られている受動的なエンティティは、通常、レコード・バッファ・テーブル・ファイル・プロセス間パイプ・通信ポートなどのデータ構造に関係するエンティティである。

リファレンスモニタは、通常、サブジェクトのID(またはサブジェクトが所属するグループ)に基づいてオブジェクトへのアクセスを制限するアクセス制御として、必須アクセス制御ポリシーを強制的に適用する。また、特定の特権(すなわちアクセス権)が与えられているサブジェクトは、アクセス権を直接的・間接的に他のサブジェクトへ渡すことができない(換言すれば、必須アクセス制御ポリシーによって設定されたルールセットに基づいて情報システムが当該ポリシーを実厳格に適用する)ため、リファレンスモニタは必須アクセス制御である。なお、リファレンスモニタの属性のうち改ざん防止機能という属性とは、敵対者によるアクセス制御の侵害を防ぐ特性を指す。また、常時機能しているという属性とは、敵対者によるアクセス制御のすり抜けというセキュリティポリシー違反を防ぐ属性である。ただし、(リファレンスモニタの脆弱性またはリファレンスモニタの欠陥の有無を)分析・テストすることが可能なほど小規模という属性とは、リファレンスモニタの脆弱性(またはリファレンスモニタの欠陥)をセキュリティポリシーの強制適用を妨げる潜在的なセキュリティ上の不備として検知するために行われるアクセス制御の解析についてその完全性を担保するための属性であるとともに、同様の目的で行われるアクセス制御のテストについてその完全性を担保するための属性である。なお、関連するセキュリティ管理策は、AC-3・AC-16・SC-3・SC-39の管理策である。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

セキュリティ管理策ファミリ:セキュリティアウェアネストレーニング

AT-1　セキュリティアウェアネストレーニングのポリシーとその手順

セキュリティ管理策:

a. [組織が定めた職員(または組織が定めた役割)の割り当て]のために、
   1. セキュリティアウェアネストレーニングに関連して、その目的・適用範囲・役割とともに、セキュリティトレーニングが達成すべき目標に加えて、セキュリティトレーニングのなかで経営陣が果すべき役割について規定されたトレーニングポリシーとして、組織の構成員同士で行われる協調について準拠法についてとともに規定されたポリシー
   2. セキュリティアウェアネスを向上させるとともにセキュリティトレーニングに関連するセキュリティ管理策を実装しやすくするセキュリティアウェアネストレーニングのトレーニングポリシーを実装しやすくするための手順

   の2つを組織が策定・文書化・公表する。

b. 更新することを前提に、組織が
   1. 現在のセキュリティアウェアネストレーニングのトレーニングポリシーの[組織が定めた頻度での割り当て]
   2. 現在のセキュリティアウェアネストレーニングの手順の[組織が定めた頻度での割り当て]

   の2つを見直す。

補足的ガイダンス:このセキュリティ管理策は、この文書のなかで"AT"から始まる項目に記載されたセキュリティ管理策ファミリのなかから特に選ばれたセキュリティ管理策(およびその拡張管理策)の効果的な実装を可能にするための手順が規定されたトレーニングポリシー策定するための管理策である。なお、当該トレーニングポリシーは、連邦法・大統領命令・指令・規制・政策・標準・手引のうち、関係するものを反映したものとなる。

セキュリティプログラム用のポリシーとしての組織レベルのポリシーによって、特定のシステムに固有のポリシーが不要になる可能性がある(すなわち、セキュリティプログラム用のポリシーとしての組織レベルのポリシーに規定された手順によって、特定のシステムに固有のポリシーに規定された手順が不要になる可能性がある)。なお、セキュリティプログラム用のポリシーとしての組織レベルのポリシーは、組織の全般的な情報セキュリティポリシーの一部を構成する(または、特定の組織の複雑な性質を反映して複数の情報セキュリティポリシーから構成される)可能性がある。

一般的なセキュリティプログラムにおいては、特定の情報システムにおける場合と同様、ポリシーに手順が必要に応じて規定される。

手順を規定するポリシーを策定する上で鍵となるのは、組織のリスク管理戦略である。なお、関連するセキュリティ管理策は、PM-9 の管理策である。

拡張管理策:なし

参考文献 NIST Special Publications 800-12・NIST Special Publications 800-16・NIST Special Publications 800-50・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** AT-1	**中** AT-1	**高** AT-1

AT-2　セキュリティ意識アウェアネストレーニング

セキュリティ管理策：情報システムに対する変更により必要になった場合、新規ユーザに対する初回のトレーニングの一部として組織が情報システムのユーザ（管理職・首脳陣・請負業者を含む）に対して基本的なセキュリティ意識向上トレーニングを実施する（なお、その後は[組織が定めた頻度での割り当て]）。

補足的ガイダンス：組織は、具体的な要求をもとに、何をセキュリティアウェアネストレーニングとしてどのように行うかについて、職員がアクセス権限を有している情報システムに即して沿う形でに定める。なお、セキュリティアウェアネストレーニングのは、情報セキュリティの必要性と合わせて、セキュリティインシデントが疑われる場合に対応しながらセキュリティを維持するユーザアクションについて基本的な理解を与えるものである。また、セキュリティアウェアネストレーニングの内容は、運用上のセキュリティを確保する必要性について留意させるものになる。なお、具体的にセキュリティアウェアネスを向上させる手法としては、ポスター展示およびセキュリティに関する注意喚起が記された贈呈品の提供とともに、組織の上級職員からの電子メールによる注意喚起と合わせて、ログオン画面におけるメッセージ表示に加えて、セキュリティアウェアネス向上のためのイベントの実施などがある。なお、関連するセキュリティ管理策は AT-3・AT-4・PL-4 の管理策である。

拡張管理策：

(1) セキュリティアウェアネストレーニング |実践的な訓練

セキュリティアウェアネストレーニングのなかで組織が実際のサイバー攻撃を想定した実践的な訓練を実施する。

補足的ガイダンス：実際のサイバー攻撃を想定した実践的な訓練として、情報の不正入手または情報への不正アクセスを目的とした抜き打ちでのソーシャルエンジニアリング攻撃に加えて、電子メールに添付された悪意のある添付ファイルを開いた場合に生じる悪影響（もしくは標的型フィッシング攻撃を通じて不正なハイパーリンクを開いた場合の悪影響）のシミュレーションを目的とした抜き打ちでのソーシャルエンジニアリング攻撃等がありうる。なお、関連するセキュリティ管理策は CA-2・CA-7・CP-4・IR-3 の管理策である。

(2) セキュリティアウェアネストレーニング | 内部不正

組織が内部不正の兆候を認識・報告するためのセキュリティアウェアネストレーニングを実施する。

補足的ガイダンス：内部不正の原因となりうる（誘発しうる）行為としては、仕事に対して長い間抱いてきた大きな不満とともに、業務の遂行に不必要情報へのアクセス加えて、使途が明らかにされていない資金の利用と合わせて、職場内暴力および同僚に対するいじめ（セクハラを含む）といった、組織におけるポリシー（もしくは組織おける手順）または組織におけるルール（もしくは組織における慣行）に対する重大な違反および組織による命令に対する重大な違反等がある。なお、セキュリティアウェアネストレーニングには、内部不正の原因となりうる行為についての認識について、組織において確立されたポリシー（および組織において確立された手順）に沿った適切なチャネルを通じて従業員と経営者とでどのように共有できるか関するトレーニングが含まれる。なお、関連するセキュリティ管理策は、PL-4・PM-12・PS-3・PS-6 の管理策である。

参考文献：C.F.R. Part 5 Subpart C (5 C.F.R. 930.301)・Executive Order 13587・NIST Special Publication 800-50

優先順位とベースライン管理策の割り当て：

P1	**低** AT-2	**中** AT-2 (2)	**高** AT-2 (2)

AT-3　役割ベースのセキュリティトレーニング

セキュリティ管理策：セキュリティに関する役割責任を負う職員に対して

a. 情報システムに対するアクセスを許可する前または彼らがられた職務を行う前

b. 情報システムを変更したことによりセキュリティトレーニングが必要となった場合

c. [組織が定めた頻度での割り当て]後

のいずれかの場合に、組織が役割ベースのセキュリティトレーニングを実施する

補足的ガイダンス：組織は、個人に割り当てられた役割をもとに、個人に割り当てられた責任とともに、組織における特定のセキュリティ要求事項に加えて、職員がアクセス権限を有する情報システムに基づいて、セキュリティトレーニングの内容を適切に決定する。また、組織は、エンタープライズアーキテクト・情報システム開発者・ソフトウェア開発者・購買担当者・情報システム管理者・システムアドミニストレータ・ネットワークアドミニストレータ・セキュリティ管理策評価者に加えて、構成管理を監査とともに担当する職員および独立した検査検証を行う職員ならびにシステムレベルのソフトウェアにアクセス可能なその他の職員に対して、それぞれの任務に応じたセキュリティ関連技術の研修として、役割ベースのセキュリティトレーニングを十分に実施する。なお、一般的な役割ベースのセキュリティトレーニングは、管理面・運用面・技術面で上記のそれぞれの者が果たすべき役割に対応した研修であるとともに、管理面・運用面・技術面で上記のそれぞれの者が果たすべき責任に対応した研修として、物理的技術的な安全対策と合わせて職員による安全対策を網羅したものとなる。また、一般的な役割ベースのセキュリティトレーニングには、例えば、セキュリティに関連して組織が果たす役割として定義されたものについてのポリシー・手順・ツール・成果物が含まれる。なお、組織は、組織の情報セキュリティプログラムによって確保される運用上の（またはサプライチェーンの）セキュリティに関連して、個人が管理面・運用面・技術面で自らの責任を果たせるように、セキュリティトレーニングの機会を提供する。なお、役割ベースのセキュリティトレーニングの機会は、連邦政府機関との間でサービス契約を締結している者に対しても適用される。なお、関連するセキュリティ管理策は AT-2・AT-4・PL-4・PS-7・SA-3・SA-12・SA-16 の管理策である。

拡張管理策：

(1) セキュリティトレーニング | 環境に関するセキュリティ管理策

環境に関するセキュリティ管理策を導入・運用した当初に[組織が定めた頻度での割り当て]のもとで行われるセキュリティトレーニングに関連して、組織が[組織が定めた職員（または組織が定めた役職）の割り当て]を行う。

補足的ガイダンス：環境に関する管理策には、火災検知装置（または消火機能付きの火災検知システム）および固定された消防ホースとともに、スプリンクラーシステム・動式消火器・煙探知器・温度・湿度・冷暖房空調・内部電源等がある。なお、組織は、環境に関する管理策に関連して責任と持って特定の役割を担う者として専門的なセキュリティトレーニングが必要な職員について定める。また、関連するセキュリティ管理策は PE-1・PE-13・PE-14・PE-15 の管理策である。

(2) セキュリティトレーニング | 物理的なセキュリティ管理策

物理的なセキュリティ管理策を導入・運用した当初に[組織が定めた頻度での割り当て]のもとで行われるセキュリティトレーニングに関連して、組織が[組織が定めた職員（または組織が定めた役職）の割り当て]行う。

補足的ガイダンス：物理的なセキュリティ管理策には、物理的アクセス制御装置・不審者侵入警報装置・監視機器・警備員等とともに、警備員の導入手順に加えて、警備員の運用手順がある。なお、組織は、物理的なセキュリティ管理策に関連して責任と持って特定の役割と責任を担う者として専門的なセキュリティトレーニングが必要な職員について定める。また、関連するセキュリティ管理策は PE-2・PE-3・PE-4・PE-5 の管理策である。

(3) セキュリティトレーニング |実践的な訓練

セキュリティトレーニングの目的が確実に達成されるよう、組織が実践的な訓練を行う。

補足的ガイダンス：実践的な訓練には、ソフトウェアの一般的な脆弱性（例：バッファーオーバーフロー）を悪用したサイバー攻撃のシミュレーション等のソフトウェア開発者向けのセキュリティトレーニングとともに、スピアフィッシング・ホエーリングのそれぞれによる上層幹部・経営陣を狙った攻撃のシミュレーションを挙げることができる。なお、上記に列挙された実践的な訓練によって、開発者が脆弱性の影響をより良く理解し、セキュアコーディングスタンダードを確立のうえセキュアコーディングのプロセスを確立する必要性についてより理解することが可能になる。

(4) セキュリティトレーニング | 疑わしい通信（およびシステムの異常な動作）

組織の情報システムにおける異常な動作を疑わしい通信とともに検知できるようするために、が［悪意のあるコードであることを表すインジケータとして組織が定義したものの割り当て］にトレーニングを職員に対して行う。

補足的ガイダンス：組織の職員が十分な訓練を積むことで、電子メールまたはウェブアプリケーションを通じて入り込んでくる悪意のあるコードから組織を守るるための綿密なセキュリティ戦略の一環として導入することが可能な別のセキュリティ対策を組織全体で講じることが可能になる。なお、職員は、見知らぬ送信者からの電子メールをはじめ、文法的に不自然な（または文法的に稚拙な）文面の電子メールに加えて、実在する関係者（または実在する取引先）らしき見知らぬ送信者からの電子メールといった悪意のある可能性がある電子メールを受信した痕跡を見逃さない訓練を受ける。また、職員は、添付ファイルを開かない（もしくは埋め込みリンクをクリックしない）または電子メールの送信者のアドレスを確かめるなど、悪意のある可能性がある電子メール（または悪意のある可能性があるウェブ通信）にどのように対応するかについても、訓練を受ける。ただし、訓練が効果的に機能するためには、組織の全職員が何を以って「疑わしい通信」となるのかについて知った上で訓練を受ける必要がある。なお、組織の職員に対して組織の情報システムにおける異常な動作を検知する方法についての訓練を課すことによって、悪意のあるコードが発見された場合に早期に警告が発せられるようになる。悪意のあるコードを自動的に検知することで組織を保護するために組織によって導入されたツール（または、悪意のあるコードを自動的に検知する事で組織を保護するために組織によって導入されたシステム）を補うのは、組織の情報システムにおける異常な動作を組織の職員が発見することである。

参考文献：C.F.R. Part 5 Subpart C (5 C.F.R. 930.301)・NIST Special Publications 800-16・NIST Special Publications 800-50

優先順位とベースライン管理策の割り当て：

P1	**低** AT-3	**中** AT-3	**高** AT-3

AT-4 セキュリティトレーニング記録

セキュリティ管理策：

a. 基本的なセキュリティアウェアネストレーニング、特定の情報システムに関するセキュリティトレーニングといった、情報システムに関するセキュリティトレーニングを組織が個別に文書化・監視する

b. 個々のトレーニングレコードを組織が［組織が定めた期間の割り当て］によって割り当てられた期間保持する。

補足的ガイダンス：専門的なセキュリティトレーニングは、組織の自由意思で、個々の管理者によって文書化される場合がある。なお、関連するセキュリティ管理策は AT-2・AT-3・PM-14 である。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P3	**低** AT-4	**中** AT-4	**高** AT-4

AT-5　セキュリティグループ（およびセキュリティ団体等）との連携

[削除された：PM-15 に統合された]

ファミリ:監査および責任追跡性

AU-1 （監査関連および責任追跡性関連の）ポリシーおよび手順

セキュリティ管理策:

a. [組織が定めた職員（または組織が定めた役割）の割り当て]のために、
   1. 監査および責任追跡性に関連して、その目的・適用範囲・役割・責任・適合性とともに組織間の整合性について規定したポリシー
   2. 監査および責任追跡性関連のポリシーを関連するセキュリティ管理策とともに容易に適用できるようにするための手順

   の 2 つを組織が配布される文書として策定する

b. 見直された結果を踏まえて、
   1. 現時点における監査関連のポリシーおよび責任追跡性関連のポリシーの[組織が定めた頻度での割り当て]
   2. 現時点における監査関連の手順および責任追跡性関連の手順の[組織が定めた頻度での割り当て]

   の2つを組織が更新する。

補足的ガイダンス:このセキュリティ管理策は、この文書における AU ファミリ内の選択されたセキュリティ管理策について拡張管理策とともに効果的に実装するための手順が規定されたポリシーを策定するための管理策である。なお、当該ポリシーは、連邦法・大統領命令・指令・規制・政策・標準・手引のうち、関連する内容を反映したものになる。

組織レベルでセキュリティプログラムに関する手順を規定したポリシーによって、特定のシステムに固有の手順を規定したポリシーが不要になる可能性がある。なお、当該ポリシーは、組織の一般的な情報セキュリティポリシーの一部を構成する（または、特定の組織の複雑な性質を反映して複数の情報セキュリティポリシーから構成される）可能性がある。

一般的なセキュリティプログラム（特定の情報システム）については、ポリシーに手順が必要に応じて規定される。

手順を規定するポリシーを策定する上で鍵となるのは、組織のリスク管理戦略である。なお、関連するセキュリティ管理策は PM-9 の管理策である。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** AU-1	**中** AU-1	**高** AU-1

AU-2 監査イベント

セキュリティ管理策:

a. ［組織が定めた監査イベントの割り当て］に関連して、システムイベントの監査が可能かどうか、組織が確認する。

b. 相互支援が強化されるとともに監査可能なイベントが容易に選択できるよう、監査に関連する情報が必要な他の組織との間で組織がセキュリティ監査の整合性を保つことができるようにする

c. 監査可能なイベントがセキュリティインシデント発生後の調査において決定的な役割を果たすと考えられているのはなぜかについての根拠を組織が示す

d. [組織が定めた監査済みイベント(この文書の AU-2 a.に定義されている監査可能なイベントのサブセットである)および定義されたイベントのそれぞれを監査する頻度(あるいは監査が必要な状況)の割り当て]に関連して、今後システム監査の対象となるイベントは何か、組織が確認する。

補足的ガイダンス:イベントとは、組織の情報システムにおいて発生しうるあらゆる事象である。組織は、特定の監査に対する現在の需要を満たすために、情報システムのセキュリティ(および情報システムが稼働する環境)に関係する重要なイベントを監査イベントとみなす。なお、監査イベントには、パスワード変更・ログオン失敗に加えて、情報システムへのアクセスの失敗と合わせて、管理者権限・PIV 資格情報のそれぞれの使用とともに、第三者のクレデンシャル情報の使用等がある。また、監査可能なイベントの一式を決定するに当たって、組織は実装する各セキュリティ管理策を適切に監査できないか検討する。なお、監査要件と情報システムが満たすべき他の要件との整合性を取るために、この AU-2 のセキュリティ管理策では、特定の時点で監査される監査可能なイベントのサブセットを特定されることを要求される。また、組織が決定するそうした機能はシステム性能に負荷をかけるため、アクセスに成功したか失敗したかを問わず、特定の状況以外には情報システムがファイルへのアクセスをすべてログに記録しないと決定する場合がある。なお、監査対象イベントの必要性を含む監査要件は、他のセキュリティ管理策や拡張管理策から参照される場合がある。なお、組織は、また、連邦法・大統領命令・指令・政策・規制・標準のうち関連する内容によって要求される監査対象イベントも含める。なお、監査記録は、情報がネットワークを流れる際のパケットレベルなど、さまざまな抽象レベルの生成が可能である。なお、適切な抽象レベルを選択することは、監査能力の重要な側面であり、問題の根本的原因の特定を容易にする。なお、組織は、監査対象イベントを定義する際に、関連するイベントも取り扱う監査を検討する。なお、関連するイベントには、例えば、分散しているトランザクションベースのプロセス(例:複数の組織にわたって分散しているプロセス)の各ステップや、サービス指向型アーキテクチャにおいて発生するアクションがある。なお、関連するセキュリティ管理策は、AC-6・AC-17・AU-3・AU-12・MA-4・MP-2・MP-4・SI-4 の管理策である。

拡張管理策:

(1) 監査イベント | 複数のソースからの監査記録の編集

[削除された:AU-12 に統合された]

(2) 監査イベント | コンポーネントごとの監査イベントの選択

[削除された:U-12 に統合された]

(3) 監査イベント |見直された結果を踏まえて更新

見直された結果を踏まえて、監査済のイベントの[組織が定めた頻度で割り当て]を組織が更新する。

補足的ガイダンス:監査が必要であると組織が考えるイベントは、時間の経過と共に変化する可能性がある。なお、今なお監査可能なイベントの一式が依然として必要十分であることを証明するためには、見直された結果を踏まえて監査可能なイベントの一式を定期的に更新する事が必要である。

(4) 監査イベント | 特権的機能

[削除された:AC-6 (9)に統合された]

参考文献:NIST Special Publication 800-92・ウェブサイト http://idmanagement.gov

優先順位とベースライン管理策の割り当て:

P1	**低** AU-2	**中** AU-2 (3)	**高** AU-2 (3)

AU-3 監査記録の内容

セキュリティ管理策:どのようなタイプのイベントがいつどこで何によって誰が(あるいは何が)関係して発生し、どのような結果をもたらしたかについての情報が記録された監査記録を情報システムが生成する。

補足的ガイダンス:このセキュリティ管理策の要求事項を満たすために必要な監査記録の内容として、タイムスタンプ・送信元アドレス・送信先アドレス・ユーザ識別子・プロセス識別子・成功通知・失敗・通知・関連ファイル名とともに、監査イベントの概要に加えて、アクセス制御(またはフロー制御)を適用するためのルール等が必要になる可能性がある。なお、イベントの監査結果は、イベントの成功(もしくは失敗)を示す通知(または、イベント発生後における情報システムのセキュリティ状態等を示す通知など、具体的なイベントの結果を示す通知)によって示す事ができる。なお、関連するセキュリティ管理策は AU-2・AU-8・AU-12・SI-11 の管理策である。

拡張管理策:

(1) 監査記録の内容 | 追加の監査情報

[組織が定義したより詳細な追加情報の割り当て]における追加情報が含まれた監査記録を情報システムが生成する。

補足的ガイダンス:[組織が定義したより詳細な追加情報の割り当て]における追加情報が記録された監査記録に関連して組織が定義する可能性のある詳細な追加情報としては、特権コマンドのコマンドテキスト全文とともに、個別のグループアカウントユーザの ID 等がある。なお、当該追加情報について、特定の監査要件を満たすために明示的に必要なもののみに制限できないか組織が検討することによって、誤解を招く恐れのある情報に加えて、重要な情報を見つける事より困難にする情報が含まれなくなるため、監査証跡および監査ログがより普及するようになる。

(2) 監査記録の内容 |監査記録に記録される予定の内容の一元的管理

[組織が定義した情報システムコンポーネントの割り当て]によって生成される監査記録に記録される内容について集中的に管理する機能を情報システムが提供するとともに、[組織が定義した情報システムコンポーネントの割り当て]によって生成される監査記録に記録される内容を情報システムが一元的に設定する。

補足的ガイダンス:この拡張管理策は、監査記録に記録される内容が一元的(かつ必ず自動的)に設定されることを要求する管理策である。なお、組織は、監査記録に記録される内容を集中的に管理するために(かつ監査記録に記録される内容を情報システムによって設定できるよう)、監査が必要なイベントを適宜選択する。なお、関連するセキュリティ管理策は AU-6 および AU-7 の管理策である。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** AU-3	**中** AU-3 (1)	**高** AU-3 (1) (2)

AU-4 監査記録のデータ容量

セキュリティ管理策:[組織が定めた監査記録の保管に関する要件の割り当て]に従って、組織が監査記録データ容量と同等のデータ容量を記憶装置に対して割り当てる。

補足的ガイダンス：監査記録のデータ容量と同等のデータ容量を記憶装置に対して割り当てる際、組織は（実施される監査の種類に加えて）監査要求事項について考慮する。なお、記憶装置に対して十分なデータ容量を割り当てることで、データ容量が超過することによって監査能力が失われる（または低下する）可能性はる。なお、関連するセキュリティ管理策は AU-2・AU-5・AU-6・AU-7・AU-11・SI-4 の管理策である。

拡張管理策：

(1) 監査記録のデータ容量| 代替ストレージへの移動

情報システムが監査記録を[組織が定めた頻度で割り当て]によって監査対象システム以外のシステムまたは媒体にオフロード（移動）させる。

補足的ガイダンス：オフロードとは、監査記録のデータ容量が限られている情報システムにおいて、監査記録をプライマリシステムからセカンダリ（またはそれ以外の）システムに移動させることによって監査記録の機密性を完全性とともに保全するための一般的なプロセスである。なお、監査用ストレージは、データ容量の限られた情報システムが監査記録を格納できるよう設計されているセカンダリ（またはそれ以外の）システムに接続することで情報を移動できるようになるまでの間にのみ、一時的に使用される。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** AU-4	**中** AU-4	**高** AU-4

AU-5 監査処理が失敗した時の対応

セキュリティ管理策：

a. 監査処理が失敗した場合、情報システムが[組織が定めた職員（または組織が定めた役割）の割り当て]を警告する

b. 情報システムが[情報システムのシャットダウンまたは最も古い監査記録をの上書き（もしくは監査記録の生成の中止）といった、組織が定めた行動の割り当て]を行う

補足的ガイダンス：監査処理の失敗としては、ソフトウェアエラーおよびハードウェアエラーならびに監査記録を採取するメカニズムの不具合と合わせて、監査記録のデータ容量が上限に達する（または上限を超過する）ことなどがある。なお、前記に列挙した以外の監査処理の失敗に対しては、組織は、タイプ別または発生場所別もしくは重大さ別に（またはタイプ別・発生場所別・重大さ別の組み合わせで）追加で対応してもよい。また、このセキュリティ管理策は、監査データを格納するための各リポジトリ（すなわち、情報システムコンポーネントのうち、監査記録が格納される一意の各コンポーネント）および／または組織の監査記録の全データに対して適用する事が可能である。なお、関連するセキュリティ管理策は、AU-4 および SI-12 の管理策である。

拡張管理策：

(1) 監査失敗時の対応 | 監査記録データ容量

割り当てられた監査記録の最大データ容量が[組織が定めた比率の指定]において組織が定めたリポジトリ内の監査記録のデータ容量の比率と同じ値に達した場合に、情報システムが[組織が定めた期間の指定]のうち[組織が定めた職員・役職・場所のすべてもしくはいずれかの指定]に対して警告する。

補足的ガイダンス：組織は、監査記録が格納されたリポジトリのうち、記録容量がそれぞれ異なるものを複数の情報システムコンポーネントに割り当てもよい。

(2) 監査失敗時の対応 | リアルタイムの警告

[リアルタイムの警告が必要な監査失敗イベントとして組織が定めたものの割り当て]において組織が定めた監査失敗イベントが発生した場合に、情報システムが[組織が定めたリアルタイム期間に指定]によって[組織が定めた職員・役職・場所のすべてまたはいずれかの割り当て]に対して警告する。

補足的ガイダンス：警告は、組織に対して緊急のメッセージを伝える。なお、リアルタイムの警告は、組織に対する緊急のメッセージを瞬時に提供する具体的に、イベントが検知されてから警告が発せられるまでの間は、数秒以内である）。

(3) 監査失敗した時の対応 | トラフィック量の閾値を設定できるようにするとして構成可能な値

システム監査能力が限界に達した場合、情報システムがネットワーク通信トラフィック量の閾値として構成可能な値を上回るネットワークトラフィックに対して情報システムが[（ネットワークトラフィックを）拒否するまたは遅延させる]を行う。

補足的ガイダンス：ネットワーク通信トラフィックの監査した結果、システム監査が可能なデータの範囲を超えることが明らかな場合、組織はネットワーク通信トラフィックの処理を拒否する（または遅らせる）能力を有する。なお、ネットワーク通信トラフィックの処理の拒否（または遅延）は、組織のネットワーク通信トラフィックの量の閾値（システム監査が可能なデータの範囲の変化に合わせて変動）として知られる値によって誘発される。

(4) 監査失敗時の対応 | 失敗時のシャットダウン

別の手段で監査が行われない限り、[組織が定めた監査の失敗とは何かを定義]する際、システムが[システムの完全なシャットダウンまたはシステムの部分的なシャットダウン（もしくはデグレードモードによるミッションおよび／または業務機能の制限）のいずれかを選択]を呼び出す。

補足的ガイダンス：組織は、情報システムの自動シャットダウン（またはデグレード）を誘発するような監査の失敗について具体的に判断する。なお、ミッションおよび／または業務の継続性を確保する重要性にかんがみ、組織は、監査の失敗が非常に重大な性質を帯びたものではないと判断したにもかかわらず、組織の主要なミッション（および／または組織における主要な業務）をサポートする情報システムについて、完全なシャットダウンを実施してもよい。ただし、その場合であっても、情報システムの完全なシャットダウンではなく、部分的なシャットダウン（または冗長性機能が低下したデグレードモード運転）でもよい。なお、関連するセキュリティ管理策はAU−15 の管理策である。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** AU-5	**中** AU-5	**高** AU-5 (1) (2)

AU-6 監査記録レビュー・監査分析・監査レポート

セキュリティ管理策：

a. 情報システムの監査記録を[組織が定めた頻度での割り当て]でレビュー・分析して、[組織が定めた不適切な活動または普段と違う活動の割り当て]の兆候の有無を組織が確認する

b. [組織が定めた職員または役割の割り当て]のために組織が結果を報告する。

補足的ガイダンス：監査レビュー・監査分析・監査レポートの対象となるのは、アカウント利用・リモートアクセス・ワイヤレス接続・設定項目・システムコンポーネントの一覧・物理アクセス・温湿

度・モバイルコード利用・VoIP 利用と合わせて、携帯機器による接続に加えて、非ローカルメンテナンスの実施を含めたメンテナンスツールの利用とともに、機器の搬入と搬出ならびにシステム境界における通信などに関連して組織が行う情報セキュリティ関係の監査である。なお、監査レビュー・監査分析・監査レポートのそれぞれの内容は、インシデント対応チーム・ヘルプデスクに加えて、情報セキュリティに関連するグループ(および／または情報セキュリティに関連する部署)など、組織内のエンティティに対して報告される可能性がある。また、組織が監査情報をレビュー・分析することが禁止されている場合または連邦政府のセキュリティ関係のアプリケーションのうち特定のもの(または連邦政府のセキュリティ関係のシステムのうち特定のもの)について監査情報をレビュー・分析する活動を実施できない場合、監査情報をレビューおよび／または分析する権限を与えられた他の組織が監査情報をレビューおよび／または分析する可能性もある。なお、関連するセキュリティ管理策は AC-2・AC-3・AC-6・AC-17・AT-3・AU-7・AU-16・CA-7・CM-5・CM-10・CM-11・IA-3・IA-5・IR-5・IR-6・MA-4・MP-4・PE-3・PE-6・PE-14・PE-16・RA-5・SC-7・SC-18・SC-19・SI-3・SI-4・SI-7 のそれぞれの管理策である。

拡張管理策:

(1) 監査レビュー・監査分析・監査レポート | プロセス統合

不審なアクティビティに対する組織的な調査・対応のためのプロセスをサポートする監査レビュー・監査分析・監査レポートのそれぞれについて、一体的に扱う自動的なメカニズムを組織が採用する。

補足的ガイダンス:組織のプロセスのうち監査レビュー・監査分析・監査報告の一体化による恩恵を受けるプロセスには、インシデント対応と合わせて、継続的なモニタリングとともに、緊急時対応計画の作成に加えて、監察官による監査等がある。なお、関連するセキュリティ管理策は、AU-12 および PM-7 のそれぞれの管理策である

(2) 監査レビュー・監査分析・監査レポート | 自動セキュリティアラート

[削除された:SI-4 に統合された]

(3) 監査レビュー・監査分析・監査レポート | 監査リポジトリの関連付け

組織全体の状況が把握できるよう、組織がリポジトリの異なる複数の監査記録を分析のうえ関連付ける。

補足的ガイダンス:複数の組織全体で把握される状況には、それぞれリスク管理の対象となる組織・ミッション(業務)プロセス・情報システムの 3 つに関する状況がある。なお、関連するセキュリティ管理策は、AU-12 および IR-4。

(4) 監査レビュー・監査分析・監査レポート|集中的なレビューおよび集中的な分析

システムの複数のコンポーネントに記録された監査記録を集中的にレビューのうえ分析する機能を情報システムが提供する。

補足的ガイダンス:集中的なレビューおよび(集中的な分析)のために自動化されたメカニズムには、Security Information Management 等の製品がある。なお、関連するセキュリティ管理策は、AU-2 および AU-12 のそれぞれの管理策である。

(5) 監査レビュー・監査分析・監査レポート | 統合 / スキャン機能およびモニタリング機能

正常(または異常)なアクテビィティを検知する機能をより高めるために、監査記録の分析と[①脆弱性スキャンに関する情報②パフォーマンスデータ③情報システムのモニタリングに関する情報④[他のソースから収集したデータおよび／または他のソースから収集した情報)として組織が定めたもの]の割り当て]のいずれかを 1 つ以上選択]の分析とを組織が統合して行う。

補足的ガイダンス:上記の拡張管理策においては、脆弱性スキャンまたはパフォーマンスデータの生成(もしくは情報システムのモニタリング)は要求事項ではない。ただし、この拡張管理策においては、脆弱性スキャンまたはパフォーマンスデータの生成(もしくは情報シ

ステムのモニタリング）の結果生成される情報の分析と監査記録の分析とを統一的に行うことが要求される。なお、Security Event and Information Management System のツールによって、複数の情報システムコンポーネントに記録されている監査記録を関連付けたうえで集約・統合する作業について、複数の情報システムコンポーネントに記録されている監査記録の分析と平行して行うことが可能になる。また、組織が必要に応じて部分的な修正を行いながら開発した標準的な監査記録を分析する分析スクリプトによって、他のソースから収集された監査記録情報は安価かつ効率的に良く分析できるようになる。

なお、監査記録情報と脆弱性スキャン情報との相関関係は、脆弱性スキャンの正確性について判断する上で重要であるとともに、攻撃の検知というイベントとスキャン結果との相関関係について判断する上で重要である。パフォーマンスデータと監査記録との相関関係を通じて、DoS 攻撃またはリソースの不正使用につながるとサイバー攻撃）を検知できる可能性がある。また、システムモニタリング情報と監査記録との相関関係を通じてサイバー攻撃を検知できる可能性があるとともに、システムモニタリング情報との相関関係を通じて監査記録が実際のシステム運用に即したものになる可能性がある。

なお、関連するセキュリティ管理策は、AU-12・IR-4・RA-5 のそれぞれの管理策である。

(6) 監査レビュー・監査分析・監査レポート| 物理的監視との相関関係

組織は、監査記録から得た情報と、物理的アクセスのモニタリングから得た情報を相互に関連付けることにより、不審な活動、もしくは不適切な（または例外的もしくは悪質な）アクティビティを検知する能力を高めるために、組織が監査記録情報と物理アクセスの監視から得た情報と照らし合わせる。

補足的ガイダンス：不審な動作について組織が裏づけとなる証拠とともに具体的に明らかにする手がかりとして、物理的セキュリティの監査の監査記録と情報システムが生成する監査ログとの照合が役に立つ可能性がある。具体的には、物理的なセキュリティに関する付随的な情報のうち個人が施設に実在した状態で論理アクセスが行われたことを示す情報と特定の情報システムに論理アクセスした個人のユーザ情報との照合は、調査のに役に立つ可能性がある。

(7) レビュー・監査分析・監査レポート | 許可されたアクション

監査レビュー・監査分析・監査報告に関連して許可される[（情報システムの）プロセス・（情報システムの）役割・（情報システムの）ユーザをそれぞれ 1 つ以上選択]を組織が定義する。

補足的ガイダンス：組織は、（情報システムの）プロセス・（情報システムの）役割・（情報システムの）ユーザに対するアクションとして、監査レビュー・監査分析・報告・監査レポートに関連して許可されるものをアカウントの管理を通じて定義する。

なお、最小権限の原則は、監査情報に関連して許可されるアクションを定義することによって適用される。また、情報システムによって強制されるアクションとして許可されているものには、読み取り・書き込み・実行・追加・削除等がある。

(8) 監査レビュー・監査分析・監査レポート | 特権的コマンドのフルテキスト分析

物理的に区分されたコンポーネント（もしくは情報システムのサブシステムのコマンド）またはフルテキスト分析を実行するためのその他の情報システムの特権コマンドのうち監査対象の特権コマンドについて、組織がフルテキスト分析を行う。

補足的ガイダンス：この拡張管理策は、昇格された特権によりユーザが特権コマンドを実行することができるなかで、情報システムにおける情報のうち特権ユーザに関する監査情報を毀損することなく全く別の環境のもとで専門的に分析できるよう要求する管理策である。

なお、フルテキスト分析とは、コマンド名についてのみ検討する分析ではなく、特権コマンドのテキストの全文について（全てのパラメータとともに）検討する分析である。また、フルテキスト分析は、パターンマッチング・経験則等を用いて行われる。

なお、関連するセキュリティ管理策は、AU-3・AU-9・AU-11・AU-12。

(9) 監査レビュー・監査分析・監査レポート |非技術的な情報との照合

組織全体で状況をより的確に把握できるよう、組織が監査情報を非技術系の情報源から得た的な情報と、監査情報を相互に関連付けることにより、組織全体にわたる状況認識を高める照合する。

補足的ガイダンス：非技術的な情報源には、例えば、組織のポリシーに対する違反（例：セクハラ事件、組織の情報資産の不正な使用またはセクシャルハラスメント事案）について記されている人事関係の記録等がある。

なお、非技術的な情報によって、内部不正となりうる活動を組織がよりかつ正確（的確）に検知するすることが可能になる。また、非技術的な情報から得られる情報は機微情報であることから、知る権利がない個人に対して第三者のプライバシーに関わる情報を誤って開示してしまうリスクを最小化できるよう、組織は非技術的な情報へのアクセスを制限するため、通常、監査情報はセキュリティインシデントに関与していることが疑われる者が存在する場合にのみ非技術的な情報と照合される。ただし、組織による監査情報の非技術的な情報との照合は、法的な根拠に基づいて行われなければならない。

なお、関連するセキュリティ管理策は AT-2 の管理策である。

(10) 監査レビュー・監査分析・監査レポート| 監査内容の調整

法執行機関からの情報（もしくは情報機関からの情報）またはその他信頼できる情報源からの情報からリスクが変化したことが明らかな場合、組織が情報システムの監査レビュー・監査分析・監査レポートの内容を調整する。

補足的ガイダンス：（法執行機関・情報機関等の情報源から）新たに受け取った情報をもとに、組織は監査レビュー・監査分析・監査レポートのいずれか（またはそれらすべて）の頻度・範囲・詳しさについて、組織のニーズを満たす事ができるように調整する。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** AU-6	**中** AU-6 (1) (3)	**高** AU-6 (1) (3) (5) (6)

AU-7 監査量縮小と報告書作成

セキュリティ管理策：

(a)①オンデマンドの監査レビュー②オンデマンドの監査分析③オンデマンドの監査要件に沿った（セキュリティインシデントの）事後調査のそれぞれをサポートするプロセスとして、かつ(b)監査記録の当初の内容または監査記録が記録される順序に対して変更を加えないプロセスとして、情報システムが監査縮小プロセスを監査レポート生成のプロセスとともに実行する。

補足的ガイダンス：監査縮小プロセスとは、収集された監査情報を操作して当該情報が分析者にとってより意味のある情報となるよう圧縮するプロセスである。

監査レポート生成のプロセスと同じく、監査縮小プロセスは、必ずしも監査を実施する情報システム（または監査を実施する組織）によって行われるとは限らない。例えば、最新のデータフィル

タを用いて監査記録に記録された異常な振る舞いを検知する最新のデータマイニング技法が、監査縮小プロセスを構成する要素となりうる。

なお、情報システムによって実行される監査レポート生成プロセスによって、カスタマイズされた監査レポートを作成することができる。また、監査記録として記録されたタイムスタンプの正確性が十分でない場合、監査記録が記録された時間的順序が重要になる場合がある。なお、関連するセキュリティ管理策は、AU-6 の管理策である。

拡張管理策:

(1) 監査量縮小と監査レポート生成 | 自動処理

[組織が定義した監査記録内の監査フィールドの指定]に基づいて、重要なイベントに関する監査記録について処理するプロセスを情報システムが提供する。

補足的ガイダンス:重要なイベントは、個人の識別情報をはじめ、(イベントの)タイプ・(イベントの)発生場所・(イベントの)発生時刻・(イベントの)発生日・(イベントの)IP アドレスといった情報とともに、関連するシステムリソースに加えて、アクセスされた情報オブジェクトといった監査記録のフィールドのうち特定のフィールドの内容によって識別することができる。また、組織は、監査イベント条件を一般的なネットワークもしくは一般的なサブネットワークのある場所(または特定の情報システムコンポーネントが選択可能な場所)に関連してどの程度詳細に定義するか、自由に決定することができる。
なお、関連するセキュリティ管理策は、AU-2 および AU-12 の管理策である。

(2) 監査量縮小と監査レポート自動生成 | 自動ソートおよび自動検索

[組織が定義した監査記録内の監査フィールドを指定]の内容に基づいて、重要なイベントに関する監査記録について並べ替える(または重要なイベントに関する監査記録について検索する)機能を情報システムが提供する。

補足的ガイダンス:フィールドの内容のうち①イベントの発生日(および/またはイベントの発生時刻)②ユーザ識別子③イベントの IP アドレス④イベントのタイプ⑤イベントの成否などに基づいて、監査記録が並び替えられる(または検索される)可能性がある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** AU-7 (1)	**高** AU-7 (1)

AU-8 タイムスタンプ

セキュリティ管理策:

a. システム内のクロックを使用して情報システムが監査記録のタイムスタンプを生成する

b. 監査記録のタイムスタンプのうち、協定世界時(UTC)またはグリニッジ標準時(GMT)に対応可能かつ[組織がどの程度詳細に時間を測定できるかについて定める]に対応するものについて情報システムが記録する。

補足的ガイダンス:情報システムによって付与されるタイムスタンプには、日付と時刻をが含むまれる。ただし、タイムスタンプに刻印される時刻は、一般的に協定世界時(UTC)もしくは現地時間(すなわち UTC との時差)または今日まで続くグリニッジ標準時(GMT)である。なお、時間測定の正確さは、情報システムのクロックと基準クロックが数百ミリ秒内または数十ミリ秒内といった単位でどの程度同期しているかによって表される。ただし、組織は、システムコンポーネントごとに異なる単位で時間の正確さを表すことができる。なお、アクセス制御・識別・認証等を可能にするメカニズムの内容次第では、タイムスタンプのサービスがアクセス制御・識別・認証

等によってセキュリティが確保されているかどうかの指標となる場合がある。また、関連するセキュリティ管理策は、AU-3 および AU-12 の管理策である。

拡張管理策:

(1) タイムスタンプ | 信頼できるタイムソースとの同期

(a) [組織が定義した周期で割り当て]によって割り当てられた情報システム内部のクロックについて、情報システムが[によって定義された信頼できるタイムソースの指定]によって指定されたタイムソースと比較する

(b) 信頼できるタイムソースとシステム内のクロックとの時間差が[組織によって定義された時間差の指定]によって指定された時間差よりも大きい場合、情報システムがシステム内のクロックを(信頼できるタイムソースに)合わせる。

補足的ガイダンス:この拡張管理策は、複数のシステムクロックを有する情報システムのタイムスタンプの一貫性を確保するための管理策であるとともに、ネットワークを通して接続されている複数のシステムにおけるタイムスタンプの一貫性を確保するための管理策である。

(2) タイムスタンプ |信頼できるセカンダリタイムソース

信頼できるプライマリタイムソースとは別の場所にあるセカンダリタイムソースを情報システムが認識する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** AU-8	**中** AU-8 (1)	**高** AU-8 (1)

AU-9 監査情報の保護

セキュリティ管理策:情報システムが監査情報および監査ツールを不正アクセス・不正変更・不正削除から保護する。

補足的ガイダンス:監査情報には、情報システムのアクティビティを適切に監査するうえで必要な全ての情報(例:監査記録・監査設定・監査報告書)が含れる。なお、この管理策は、もっぱら監査情報を保護する技術に関する管理策であって、監査情報の物理的な保護に関するセキュリティ管理策は媒体の保護に関する管理策および監査情報を保護する環境に関する管理策である。なお、関連するセキュリティ管理策は、AC-3・AC-6・MP-2・MP-4・PE-2・PE-3・PE-6 のそれぞれの管理策である。

拡張管理策:

(1) 監査情報の保護 | ハードウェア内の ROM

ハードウェア内の ROM に情報システムが監査証跡を書き込む。

補足的ガイダンス:この拡張管理策は、初めて監査証跡を生成する(すなわち、検知・分析・報告のために使用される監査情報が記録された監査記録を収集する)際に適用されるだけではなく、初めて監査証跡のバックアップを行う際にも適用される。ただし、この拡張管理策は、監査証跡として書き込まれる監査記録を生成する段階では適用されない。なお、追記型の媒体(WORM)には、CD-R・DVD-R 等がある。ただし、テープカートリッジや USB ドライブなどは、追記型の媒体ではないにもかかわらず書き込み禁止の媒体である。なお、関連するセキュリティ管理策は、AU-4 および AU-5 の管理策である。

(2) 監査情報の保護 | 物理的に異なるシステム / システムコンポーネント監査記録へのバックアップ

監査対象のシステムもしくは監査対象のシステムコンポーネントとは物理的に異なるシステム（または監査対象のシステムもしくは監査対象のシステムコンポーネントとは物理的に異なるシステムコンポーネント）を保存先として情報システムが［組織が定めた頻度で割り当て］で定められた頻度で監査記録のバックアップを行う。

補足的ガイダンス：この拡張管理策は、監査対象の情報システムの侵害が、監査記録が改ざんされないようにするための管理策である。なお、関連するセキュリティ管理策は、AU-4・AU-5・AU-11 のそれぞれの管理策である

(3) 監査情報の保護 | 暗号化による保護

監査情報および監査ツールのそれぞれの完全性を保護するために、情報システムが暗号メカニズムを実装する。

補足的ガイダンス：監査情報の完全性を保護するための暗号メカニズムには、ハッシュの生成に使用される秘密鍵の機密性を維持しながらハッシュ値を検証するための公開鍵の配布を可能にする非対称鍵暗号を用いた署名ハッシュ関数等がある。

なお、関連するセキュリティ管理策は、AU-10・SC-12・SC-13 のそれぞれの管理策である。

(4) 監査情報の保護 | 一部の特権ユーザによるアクセス

［組織が定めた一部の特権ユーザの割り当て］によって割り当てられたユーザに対してのみ、組織が監査機能の管理権限を付与する。

補足的ガイダンス：情報システムによる監査の対象でありながら当該システムに対するアクセス特権を有する個人が、監査活動の妨害または監査記録の改ざんにより、監査情報の信頼性に影響を与える可能性がある。ただし、この拡張管理策は、システムによる監査の対象である個人が有するアクセス特権と他のアクセス特権とをより詳細に区別するよう要求することによって、システムによる監査の対象でありながらシステムに対するアクセス特権を有するユーザの数を制限する管理策である。なお、関連するセキュリティ管理策÷は、AC-5 の管理策である。

(5) 監査情報の保護 | 二重認証

［組織が定めた監査情報の割り当て］に関連して［移動・削除のいずれか（または両方）を選択］する際、組織が二段階認証を強制する。

補足的ガイダンス：二段階認証を強制するにあたり、組織は監査情報のタイプごとに異なる選択肢を用意することができる。ただし、二段階認証を実施するうえで権限のある二人の個人による承認が必要になるため、二段階認証は、「二人の認証("two-person control")」と呼称される場合がある。

なお、関連するセキュリティ管理策は、AC-3 および MP-2 の管理策である。

(6) 監査情報の保護 | 読み取り専用アクセス

［組織が定めた一部の特権ユーザの割り当て］のために、組織が監査情報への読み取り専用アクセスを許可する。

補足的ガイダンス：ユーザ特権を読み取りのみに制限することにより、特権ユーザが組織にもたらす可能性のある被害（例：悪意に満ちた行為を隠蔽するために監査記録が削除される）を限定的なものにすることができる。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** AU-9	**中** AU-9 (4)	**高** AU-9 (2) (3) (4)

AU-10 否認防止

セキュリティ管理策:[否認防止がなされるよう組織が定めた行為の指定]を実施したにもかかわらず誤ってその事実を否定してしまう個人(または[否認防止の対象として組織が定めた行為の指定]を実施したにもかかわらず誤ってその事実を否定してしまう個人プロセス)から情報システムが保護する。

補足的ガイダンス:

①文書を執筆した者が後になって文書を執筆していないことを主張する

②メッセージを送信した者が後になってメッセージを送信していないことを主張する

③メッセージを受信した者が後になってメッセージを受信していないことを主張する

④文書に署名した者が後になって文書に署名していないことを主張する

といった行為から個人を保護するための否認防止策が実施される行為として、例えば、情報作成・メッセージ送受信に加えて、同意の意思表示(または契約書への署名)などといった承認行為が挙げられる。なお、特定の個人が情報源なのか否か(または契約書への署名行為に加えて電子メール送信および調達依頼といった特定の行為が個人によって実施されたのか否かもしくは個人が特定の情報を受信したのか否か)を確認するために否認防止策を利用することができる。また、組織は、電子メッセージを受信するといった手段に加えて電子署名などのさまざまな手段を通じて否認防止策を行うことができる。なお、関連するセキュリティ管理策は、SC-12・SC-8・SC-13・SC-16・SC-17・SC-23のそれぞれの管理策である。

拡張管理策:

(1) 否認防止 |情報と情報作成者のとの関係

(a) [情報作成者の身元を組織が指定]に情報と情報作成者のとの関係性に関する情報を情報システムが関連付ける

(b) 情報作成者の身元について許可された個人が判別する手段を情報システムが提供する

補足的ガイダンス:この拡張管理策は、情報が転送された場合に誰によって情報が作成されたのかについて監査の際に判別する手段を組織の職員に対して提供する上で要求される事項に対応した管理策である。なお、組織は、情報のセキュリティカテゴリおよびとその背景にあるリスク要因に基づいて情報作成者の身元を判別する。なお、関連するセキュリティ管理策は、AC-4 および AC-16 のそれぞれの管理策である。

(2) 否認防止 | 情報と情報作成者の身元との関係性の確認

(a) [(組織が定義した操作の)割り当て]に基づいて情報システムが情報と情報作成者との関係性を確認する

(b) 情報作成者の身元の確認ができない場合、情報システムが[(組織が定義した操作の)割り当て]を実行する

補足的ガイダンス:この拡張管理策は、作成された情報がレビュー前に改ざんされないようにする管理策である。

なお、情報と情報作成者との関係性は、暗号チェックサム使の利用等によって確認できる。また、組織は、情報と情報作成者との関係性の確認がユーザのリクエストに応じて行われたのか(またはユーザのリクエストに関係なく自動的に行われたのかどうか)を判別する。

なお、関連するセキュリティ管理策は、AC-3・AC-4・AC-16 のそれぞれの管理策である。

(3) 否認防止 |チェーン・オブ・カストディ

レビュー(または開示)されるすべての情報に関連して、情報システムがレビュー担当者(または開示者)の身元情報のチェーン・オブ・カストデイを資格証明のチェーン・オブ・カストデイとともに担保する。

補足的ガイダンス:チェーン・オブ・カストディとは、証拠を取り扱った全ての者および証拠が収集された日時ならびに証拠が移動した日時および証拠が移動した理由を記録する(すなわち、証拠収集・証拠保全・証拠検討などの段階における証拠の状態を記録する)プロセスである。

なお、人間が行う情報レビューの場合(または情報のレビューが情報の開示または情報の転送とは別に行われる)場合、情報システムは開示される情報のレビュー担当者の身元を判別したうえでレビュー担当者の身元から情報のラベルを作成する一方で、組織の職員はこの拡張管理策によってレビュー担当者(または開示者)が誰か特定する手段を得る。また、自動的な情報レビューの場合、この拡張管理策が確実に適用されるのは承認されたレビューのみである。

なお、関連するセキュリティ管理策は、AC-4・AC-16 のそれぞれの管理策である。

(4) 否認防止 |情報と情報レビュー担当者の身元との関係性の確認

(a) [組織が定め義したセキュリティドメインの割り当て]との関係で情報を転送・開示する前に、情報システムが(情報を転送・開示する時点における)情報と情報のレビュー担当者との関係性を確認する

(b) 情報と情報のレビュー担当者との関係性が確認できない場合、情報システムが[(組織が定め義した操作の)割り当て]を実施する。

補足的ガイダンス:この拡張管理策は、レビューされた情報が転送および/または開示される前に改ざんされないようにする管理策である。

なお、情報と情報作成者との関係性は、暗号チェックサムの利用等によって確認できる。また、組織は、情報と情報作成者との関係性の確認がユーザのリクエストに応じて行われたのか(またはユーザのリクエストに関係なく自動的に行われたのかどうか)を判別する。

なお、関連するセキュリティ管理策は、AC-4 および AC-16 の管理策である。

(5) 否認防止 | 電子署名

[削除された:SI-7 に統合された]

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** 選択されていない	**高** AU-10

AU-11 監査記録の保持

セキュリティ管理策:法令上要求される事項を満たす事ができるよう(かつ組織に対して課される情報保持の義務を果たす事ができるよう)、組織が[記録保持ポリシーに準拠した期間として組織が定義した期間の割り当て]についての監査記録を保持する事によって、セキュリティインシデントの事後調査を支援する。

補足的ガイダンス:組織は、経営上・法律上・監査上の目的等の実務上の目的を果たすうえでもはや必要ないと判断された時点まで米国連邦情報公開法(FOIA)が要求する事項に関係する監査記録(または命令による監査記録もしくは捜査のための監査記録)等を利用可能な状態で保持する。また、組織は、捜査のための監査記録を標準的な方法で分類するとともに、標準的な捜査対応プロセスを確立する。

なお、アメリカ国立公文書記録管理局(NARA)の General Records Schedules は、記録の保管に関する連邦政府の方針を規定したものである。また、関連するセキュリティ管理策は、AU-4・AU-5・AU-9・MP-6 のそれぞれの管理策である。

拡張管理策:

(1) 監査記録の保持 | 長期にわたって取得する機能

情報システムによって生成された監査記録のうち組織が長期にわたって取得する監査記録を確実に取得できるよう、組織が[組織が定義した対策の割り当て]を実施する。

補足的ガイダンス:監査記録を容易に取得できるようにするために組織が活用する対策には、監査記録の新しいフォーマットへの変換とともに、記録の読み出しが可能な機器の保持に加えて、監査記録読み取り方について組織の職員が理解できるようにするうえで必要な文書の保持等がある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P3	**低** AU-11	**中** AU-11	**高** AU-11

AU-12 監査記録の生成

セキュリティ管理策:

a. この文書の AU-2 a.の項目にて[情報システムコンポーネントとして組織が定義したコンポーネントの割り当て]として定義されている監査可能なイベントのために監査記録を生成する機能を情報システムが提供する

b. [組織が定めた職員(または組織が定めた役割)の割り当て]が特定の情報システムコンポーネントによって監査される監査可能なイベントについて選択することを情報システムが許可する

c. この文書の AU-2 d.の項目にて定義されているイベントに関する監査記録を(この文書の)AU-3 に定義されている内容で情報システムが生成する。

補足的ガイダンス:情報システムは、さまざまな情報システムコンポーネントから監査記録を生成することができる。

なお、監査イベント一覧は、監査が行われる予定のイベントの一覧である。また、これらのイベントは、通常、情報システムが監査記録を生成できるようになるための全てのイベントの一部である。

なお、関連するセキュリティ管理策は、AC-3・AU-2・AU-3・AU-6・AU-7 のそれぞれの管理策である。

拡張管理策:

(1) 監査記録の生成 | システム全体にわたる監査証跡 /監査証跡としてのタイムスタンプ

[組織が定義した情報システムコンポーネントの割り当て]についての監査記録をシステム全体にわたる監査証跡として、[監査証跡としての監査記録のうち個々のタイムスタンプの位置づけについて組織が定義した許容範囲の割り当て]の範囲内で(論理的・物理的を問わず)管理する。

補足的ガイダンス:タイムスタンプが複数の監査記録で確実に一致する場合、タイムスタンプは組織が許容する時間に監査記録が記録されたことについての監査証跡となる。

なお、関連するセキュリティ管理策は、AU-8 および AU-12 の管理策である。

(2) 監査記録の生成 | 標準化されたフォーマット

システム全体にわたる監査証跡となる論理的・物理的な証跡として、(標準化されたフォーマットの)監査記録を情報システムが作成する。

補足的ガイダンス：共通の標準に適合するように標準化された監査情報が異なるデバイス間（および異なる情報システム間）で容易に共有・交換されることにより、イベント情報をより容易に分析・関連付けることが可能になる。また、標準化されたフォーマットの監査記録には、共通イベント表現（CEE）に正規化されたシステムログ等の監査記録がある。

なお、情報システムログが標準化されたフォーマットのログではない場合には、当該情報システムログがシステム全体にわたる監査証跡となるよう、当該ログは標準化されたフォーマットのログに変換される。

(3) 監査記録の生成 | 許可された個人による変更

[[組織が定義した時間しきい値の割り当て]における[組織が定義した選択可能なイベント条件の割り当て]に基づいて、情報システムが[組織が定義した情報システムコンポーネントの割り当て]について行われる監査を[組織が定めた個人（または組織が定めた役割）の割り当て]によって変更できるようにする。

補足的ガイダンス：この拡張管理策は、組織による要求事項を満たすことができるよう、組織が必要に応じて監査を拡張・制限できるようにする管理策である。

なお、情報システムのリソースを節約するために監査が制限されているにもかかわらず、特定の脅威に対処するために監査が拡張される場合がある。また、監査を削減すると同時に、監査について容易に分析・報告できるよう、監査が特定のイベントのセットに対してのみに制限される場合がある。

なお、監査の変更に関連して、組織は時間しきい値をほぼリアルタイムもしくは数分内または数時間内などに設定できる。また、関連するセキュリティ管理策は、AU-7 である。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** AU-12	**中** AU-12	**高** AU-12 (1) (3)

AU-13 情報漏洩の監視

セキュリティ管理策：組織の情報が漏えいした痕跡を見逃さないよう、[組織が定めた頻度で割り当て]によって割り当てられた頻度で組織が[組織が定義したオープンソースソフトウェア（および／またはオープンソースソフトウェアのサイトとして組織が定義したサイト）の割り当て]を監視する。

補足的ガイダンス：オープンソースソフトウェアには、SNS ソフトウェア等がある。

なお、関連するセキュリティ管理策：は、PE-3 および SC-7 のそれぞれの管理策

拡張管理策：

(1) 情報漏洩の監視 | 自動化されたツールの利用

組織の情報が漏洩していないかを組織が自動化されたメカニズムを利用して判断する。

補足的ガイダンス：自動化されたメカニズムには、選択されたウェブサイトに新たに投稿されたメッセージを監視するための自動化スクリプトに加えて、組織に対して通知・警告する商用サービス等がある。

(2) 情報漏洩の監視 |監視するサイトのレビュー

組織がオープンソースソフトウェアのサイトとして[組織が定めた頻度で割り当て]によって割り当てられた頻度で監視されているサイトのレビューを行う。

参考文献：なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AU-14 セッションの監査

セキュリティ管理策:記録または再生するユーザセッションについて許可されたユーザが選択できるようにする機能を情報システムが提供する。

補足的ガイダンス:セッションの監査では、キー入力のチェックに加えてアクセスしたウェブサイトをの追跡が行われるとともに、情報(および/またはファイル)転送の収集等が行われる。

なお、セッションの監査は、法律顧問の助言のもと、関連する法令(連邦法・大統領命令・指令・政策・規制・標準)にのっとって具体的に計画されたうえで行われる。また、関連するセキュリティ管理策は、AC-3・AU-4・AU-5・AU-9・AU-11 のそれぞれの管理策である。

拡張管理策:

(1) セッションの監査 |起動時の監査

情報システムを起動する際にセッションの監査を行う。

(2) セッションの監査 |記録とユーザセッションログの記録

許可されたユーザによるユーザセッションログの記録機能を情報システムが提供する。

(3) セッションの監査 |ユーザセッションのリモート再生

許可されたユーザによる確立されたユーザセッションのリモート再生機能を情報システムがリアルタイムで提供する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AU-15 代わりに割り当てられた監査

セキュリティ管理策:当初の監査が失敗した場合、組織が[組織が代わりに定義した監査の割り当て]によって代わりに割り当てられた監査を実施する。

補足的ガイダンス:代わりに割り当てられた監査は監査の失敗が解消されるまでの短期間の管理策にとどまる可能性があるため、組織は、当該監査を当初の監査を部分的に補うに過ぎないものとして位置付けても良い。

なお、関連するセキュリティ管理策は、AU-5 の管理策である。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

AU-16 組織横断的な監査

セキュリティ管理策:組織が外部の組織と[組織が定義した監査情報の割り当て]について調整するために監査情報を外部に送信する場合、[組織が定義したメソッドの割り当て]を利用する。

補足的ガイダンス:監査を行うに当たり組織が外部の組織の情報システム(および/または外部の組織のサービス)を使利用する場合は、組織間で調整することが必要となるため、組織間で特定のサービスをリクエストした個人の識別情報を保持することは非常に困難である場合が多い。

なお、組織間で特定のサービスを要求した個人の ID を保持した場合、パフォーマンスに著しい影響を与える可能性があるため、組織横断的な監査(例:サービス指向の監査)では、ある一方の情報システムにおいて特定のサービスを要求した個人の ID を取得する一方、もう一方の情報システムでは許可された個人によって特定のサービスが要求されたことを記録するという場合が多い。なお、関連するセキュリティ管理策は AU-6 の管理策である。

拡張管理策:

(1) 組織横断的な監査 | ID の保持

組織横断的な監査の証跡として個人の ID が保持されなければならないことを組織が要求する。

補足的ガイダンス:この拡張管理策は、特定の個人に対して組織を超えて実施されるアクションが必ず追跡可能な状態でなければならない場合に適用される。

(2) 組織横断的な監査 | 監査情報の共有

[組織間での監査情報の共有についての契約として組織が定義した契約の割り当て]に基づいて、組織が[監査情報を共有する他の組織として組織が定義した組織の割り当て]のために監査情報を他の組織に提供する。

補足的ガイダンス:組織の情報資産が他の組織の個人によって適切に使用されているか(あるいは不適切に使用されていないか)を判断する上で必要十分な情報が組織の監査記録に含まれていない場合があることから、これまでに実施された監査を十分に分析するためには、共有される前提の監査情報を組織間で共有する事が不可欠な場合がある。

なお、監査情報を組織間で共有するかどうかを判断するに当たって必要十分な情報を個人が所属する組織のみが有している場合は、組織間で監査情報を共有することが必要になる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

セキュリティ管理策ファミリ：セキュリティ評価およびセキュリティ認可

CA-1　セキュリティ評価ポリシーならびにセキュリティ評価手順（およびセキュリティ認可ポリシーならびにセキュリティ認可手順）

セキュリティ管理策：

a. [組織が定めた職員（または組織が定めた役割）の割り当て]のため、組織が
   1. セキュリティ評価ポリシーおよびセキュリティ認可ポリシーとして、その目的・適用範囲に加えて果たすべき役割について規定するとともに、セキュリティ評価およびセキュリティ認可によって生じる責任について規定したものでありながら、経営者の関与と合わせて、組織の関係者の間で行われる調整に加えて順守すべき法令について規定したポリシー
   2. セキュリティ評価ポリシーおよびセキュリティ認可ポリシーをセキュリティ評価関連およびセキュリティ認可関連の管理策とともに容易に実装できるようにするための手順

   の2つを策定・文書化のうえ普及させる。
b. 組織が
   1. セキュリティ評価ポリシーの[組織が定義した頻度で割り当て]およびセキュリティ認可ポリシーの[組織が定義した頻度で割り当て]について、現時点における状況
   2. セキュリティ評価手順およびセキュリティ認可手順の[組織が定義した頻度で割り当て]について、現時点における状況

   の2つをレビューのうえ更新する。

補足的ガイダンス：このセキュリティ管理策は、CA の管理策ファミリのセキュリティ管理策のうち選択された管理策を拡張管理策とともに効果的に実装するためのポリシーについて規定した管理策であると同時に、CA の管理策ファミリのセキュリティ管理策のうち選択された管理策を効果的に実装するための手順について規定した管理策である。

なお、CA の管理策ファミリのセキュリティ管理策のうち選択された管理策を効果的に実装するためのポリシーは、関連する連邦法・大統領命令・指令・規制・政策・標準・手引に準拠したものになると同時に、CA の管理策ファミリのセキュリティ管理策のうち選択された管理策を効果的に実装するための手順も、関連する連邦法・大統領命令・指令・規制・政策・標準・手引に準拠したものになる。ただし、組織レベルでセキュリティプログラムを実装するためのポリシーとともに組織におけるセキュリティプログラム実装手順によって、特定のシステムにおいてセキュリティプログラムを実装するためのポリシーが（特定のシステムにおけるセキュリティプログラム実装手順とともに）不要になる可能性がある。

なお、組織レベルでセキュリティプログラムを実装するためのポリシーは、組織の全般的な情報セキュリティポリシーの一部となりうるとともに、特定の組織における複雑な組織構造を反映して複数のポリシーから構成される可能性がある。また、組織におけるセキュリティプログラム実装手順は、必要に応じてセキュリティプログラム全般に関係する手順となりうるとともに、必要に応じて特定の情報システムにおけるセキュリティプログラム手順となりうる。

なお、組織レベルでセキュリティプログラムを実装するためのポリシーを組織におけるセキュリティプログラム手順とともに策定する上で鍵を握るのは、組織のリスク管理戦略である。また、関連するセキュリティ管理策は PM-9 の管理策である。

拡張管理策：なし

参考文献：NIST Special Publications 800-12・NIST Special Publications 800-37・NIST Special Publications 800-53A・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** CA-1	**中** CA-1	**高** CA-1

CA-2 セキュリティ評価

セキュリティ管理策:

a. セキュリティ評価に関連して
   1. セキュリティ評価を行うセキュリティ管理策およびその拡張管理策
   2. セキュリティ管理策の有効性を判断するために利用されるセキュリティ評価手順
   3. セキュリティ評価環境・セキュリティ評価チームに加えて、セキュリティ評価が果たすべき役割とともにセキュリティ評価が果たすべき責任

   といった詳細について記述されたセキュリティ評価計画を組織が策定する。

b. セキュリティ管理策が正しく実装されているかに加えて、意図した通りにセキュリティ管理策が運用されているかとともに、決められたセキュリティ要求事項を満たす管理策であるかという意味においてセキュリティ管理策が期待された成果を上げているかについて判断するために、情報システムに対するセキュリティ管理策および当該管理策が運用されている環境について、[組織が定義した頻度で割り当て]が行われているかどうか評価する。

c. セキュリティ評価の結果を記載したセキュリティ評価レポートを組織が作成する

d. [組織が定めた個人(または組織が定めた役割)の割り当て]のために、セキュリティ管理策の評価結果を組織が報告する。

補足的ガイダンス:組織は、①当初から継続的に行われているセキュリティ認可②FISMA のもとで行われる年次評価③継続的な情報セキュリティモニタリング④システム開発ライフサイクルのアクティビティのそれぞれの一環として、組織の情報システムに対するセキュリティ管理策を当該システムの運用環境と合わせて評価する。

なお、セキュリティ評価とは、①組織の情報システムのセキュリティが必ず確保されるよう行われる行為であるのみならず、②開発プロセスの早い段階でセキュリティ上の弱点やセキュリティ上の欠陥を特定できるようにする行為であるのに加えて、③セキュリティ認可のプロセスのなかでリスクベースの判断が行なわれる際に必要となる重要な情報を提供する行為であるとともに、④脆弱性を軽減するための手順をが必ず順守されるよう行われる行為である。また、セキュリティ評価は、情報システムセキュリティ計画および情報セキュリティプログラムの計画にある通り、この文書の付録 F(一般的なセキュリティ管理策のカタログ)に記載されたセキュリティ管理策とともに、同じくこの文書の付録 G(情報セキュリティプログラムを管理するためのセキュリティ管理策について)に記載されたセキュリティ管理策として実装された管理策に対して行われる。

なお、システム開発ライフサイクルを通じて情報システムのセキュリティを維持するために、組織は、脆弱性スキャンやシステム監視など上記の4つ以外のタイプのセキュリティ評価を行うことができる。また、セキュリティ評価レポートにおけるセキュリティ評価結果は、当該レポートが正確・完全であるかについてと合わせて、セキュリティ管理策が正しく実装されているかについてとともにセキュリティ管理策が意図した通りに運用されるているかについてに加えて、セキュリティ要求事項を満たすセキュリティ管理策であるかという意味においてセキュリティ管理策が期待された成果を上げているかについて組織が判断できるよう、組織が必要十分であると判断した内容が記載されたものである。ただし、少なくとも年に 1 回のセキュリティ管理策を評価することが FISMA によって義務付けられている一方、FISMA は組織のセキュリティ認可プロセスに既に組み込まれている行為の他にセキュリティ評価を追加で行う事を義務付ける法律ではない。

なお、セキュリティ評価の結果は、実施されるセキュリティ評価のタイプに応じて個人または特定の役割に対して提供される。例えば、セキュリティ認可をを行うにあたって実施されるセキュリティ評価の結果は、運用認可責任者または運用認可責任者が指名した代表者に対して提供される。また、セキュリティ評価を毎年行うわなければならないという要求事項を満たすことができるよう、組織は、①当初または現在認可された情報システムのセキュリティを評価することができるとともに、②継続的にセキュリティモニタリングを行うことができるのに加えて、③システム開発ライフサイクルの各アクティビティのセキュリティを評価することが出来る。ただし、セキュリティ管理策の有効性を判断するうえで、組織は、セキュリティ評価の結果が最新かつ適切なものでありながら一定の独立性を有する評価者によって求められたものであるようにする。ただし、過去に評価者によって求められたセキュリティ評価の結果は、当該評価結果が今なお有効な場合かつ必要に応じて追加的なセキュリティ評価を行うことが可能な場合に限り、繰り返し参照される。

なお、当初認可された情報システムについて継続的にセキュリティモニタリングが行われる中、組織は、OMB ポリシーに準拠したセキュリティ評価を行う。また、組織は、現時点におけるセキュリティ評価の頻度を組織が継続的にセキュリティモニタリングを行うに当たっての戦略に沿って決定する。

なお、Information Assurance Vulnerability Alerts では、脆弱性を軽減するうえで具体的に有用な手順を示している。ただし、外部監査（例：規制当局などの外部組織による監査）は、この管理策の守備範囲外である。

なお、関連するセキュリティ管理策は、CA-5・CA-6・CA-7・PM-9・RA-5・SA-11・SA-12・SI-4 のそれぞれの管理策である。

拡張管理策:

(1) セキュリティ評価 | 独立した評価者

セキュリティ管理策を評価するために、組織が[組織が定義したレベルの独立性の割り当て]によって評価者または評価チームを採用する。

補足的ガイダンス：独立した評価者（または独立した評価チーム）とは、組織の情報システムのに対するセキュリティ管理策を公平に評価する個人（または組織の情報システムのセキュリティ管理策を公平に評価するグループ）を指す。ただし、セキュリティ管理策の公平な評価とは、組織の情報システムを開発または運用もしくは管理するうえでのセキュリティ評価のうち（またはセキュリティ管理策の有効性に関するセキュリティ評価のうち）、評価者・評価チームが評価対象の情報システムを抱える組織といかなる利害関係を有しないと考えられる（または評価者・評価チームが評価対象の情報システムを抱える組織と実際にいかなる利害関係を有しない）状態で行われるセキュリティ評価を指す概念である。

なお、情報システムに対するセキュリティ管理策が公正に評価できるよう、評価者・評価チームは①評価対象の情報システムを抱える組織と癒着してはならないとともに評価対象の情報システムを抱える組織の利益に反する行為をしてはならないだけではなく、②評価対象に対するセキュリティ評価について自己評価をしてはならないのと同時に、③評価対象の情報システムを抱える組織の経営者（または評価対象の情報システムを抱える組織の職員）として活動してはならないのに加えて、④評価対象の情報システムを抱える組織の代理人となってはならない。ただし、組織内の部署は独立した評価者（または独立した評価チーム）としてセキュリティ評価を行うことができる一方、官民を問わず外部の組織も独立した評価者（または独立した評価チーム）としてセキュリティ評価を行うことができる。

運用認可責任者は、誰を独立した評価者（または独立した評価チーム）とするかについて、（情報システムの）セキュリティカテゴリに応じて決定するとともに、組織が業務面または資産面で直面する最大のリスク（または個人が直面する最大のリスク）に応じて決定する。ただし、誰を独立した評価者（または独立した評価チーム）とするかについて、運用認可責任者は上記のセキュリティカテゴリまたはリスクのどちらか一方に応じて決定する場

合もある。また、運用認可責任者は、セキュリティが保証されているかどうかについて、セキュリティが独立した評価者（または独立した評価チーム）によって十分に保証されているかどうかによって判断する。同様に、運用認可責任者は、リスクベースの意思決定を正確に行うことができるかどうかについても、セキュリティが独立した評価者（または独立した評価チーム）によって十分に保証されているかどうかによって判断する。ただし、上記の事項についての判断は、情報システムの所有者が評価者（または評価チーム）との評価契約の手続に直接関与していないといったような場合に、外注したセキュリティ評価サービスが情報システムの所有者から完全に独立した評価者によって行われたものであるのかどうかについての判断を伴うものであるとともに、情報システムの所有者がセキュリティ評価者（またはセキュリティ評価チーム）の独立性に悪影響を与えることができないといったような場合に、外注したセキュリティ評価サービスが情報システムの所有者から完全に独立した評価者によって行われたものであるのかどうかについての判断も伴うものである。なお、情報システムを所有する組織が小規模である（または、組織の指揮命令系統上、システムの所有者から開発または運用もしくは管理を任された個人がセキュリティ評価を実施しなければならない）といった特殊な状況下では、独立した評価者は、セキュリティの完全性・正確性・一体性・信頼性が確保されているという評価結果について検証する独立した専門家のチームによって評価結果が慎重に再検討・分析されることを保証することによって初めてセキュリティ評価を行う事ができるようになる。

なお、完全に独立した評価者（または完全に独立した評価チーム）が実施するセキュリティ評価は、当該評価が認可の判断材料の提供を直接の目的とするものであるか否かを問わず、認可の判断材料として活用可能であるため、組織として重複してセキュリティ評価を行う必要が少なくなる。

(2) セキュリティ評価 | 特殊なセキュリティ評価

セキュリティ管理策について評価する一環として、組織が[組織が定義した頻度で割り当て]・[予告のうえ（予告なしで）割り当て]・[①詳細なセキュリティモニタリング②脆弱性スキャン③ユーザに悪意があるかどうかを判定するテスト④内部不正に対するセキュリティの評価⑤パフォーマンステスト⑥負荷テスト⑦[その他組織が実施する旨定めたセキュリティ評価の割り当て]を1つ（または複数）選択]のそれぞれを実施する。

補足的ガイダンス：ユーザがその能力をより発揮するとともにセキュリティを向上することを目指したアクションを集約するために現在のパフォーマンスレベルを示すことができるよう、組織は、情報システムに対するセキュリティモニタリングを行うことができるのに加えて内部不正に対するセキュリティの評価を行うことができるとともに、ユーザに悪意があるかどうかを判定するテストと合わせて、その他の形式のパフォーマンステストおよび／または負荷テスト（例：パフォーマンスおよび／または負荷の検証およびパフォーマンスおよび／または負荷の有効性確認）を行うことができる。また、組織は、関連する連邦法・大統領命令・指令・政策・規制・標準に準拠して評価活動を実施する。一方、運用認可責任者は、組織のリスク機能とと合わせてセキュリティ評価手法の認可を行う。ただし、組織は、セキュリティ管理策を評価した際に発見された脆弱性について脆弱性修正プロセスの対象に含めることができる。

なお、関連するセキュリティ管理策は、PE-3 および SI-2 のそれぞれの管理策である。

(3) セキュリティ評価 | 外部の組織

セキュリティ評価によって[組織が定義した要求事項の割り当て]によって割り当てられた要求事項を満たすセキュリティ管理策であることが明らかになった場合、[組織が定義した外部の組織の割り当て]によって割り当てられた外部の組織による[組織が定義した情報システムの割り当て]のセキュリティを評価した結果を組織が受け入れる。

補足的ガイダンス：特定の情報システムのセキュリティ評価を外部の組織に委ねることが多くなる可能性がある組織は、すでに外部の組織に委ねたセキュリティ評価を活用する事（す

なわち、既存の監査証跡を再利用する事）により、組織が独自に行わなければならないセキュリティ評価の活動が少なくなるため、組織自体が実施しなければならないセキュリティ評価に要する時間を大幅に減らすことができるとともに、組織自体が実施しなければならないセキュリティ評価に要するリソースを大幅に減らすことができる。

なお、外部の組織によるセキュリティ評価の結果を受け入れるか否かを判断する際に組織が考慮しうる要素は、多岐に及ぶ可能性がある。ただし、当該判断は、ある組織が別の組織に対して過去に実施したセキュリティ評価に関する経験とともに、セキュリティ評価を実施する組織に対する評判に加えて、セキュリティ評価の根拠となる文書として提供されたものがどの程度まで詳細であるかに加えて、連邦法または連邦政府の政策（もしくは連邦政府による指令）によってセキュリティ評価を実施する組織に課せられている義務といったものに基づいて行われる可能性がある。

参考文献：Executive Order 13587・FIPS Publication 199・NIST Special Publications 800-37・NIST Special Publications 800-39・NIST Special Publications 800-53A・NIST Special Publications 800-115・NIST Special Publications 800-137

優先順位とベースライン管理策の割り当て：

P2	**低** CA-2	**中** CA-2 (1)	**高** CA-2 (1) (2)

CA-3 システムの相互接続

セキュリティ管理策：

a. 一方の情報システムから他方の情報システムへの接続に関して、Interconnection Security Agreements を使用した接続を組織が許可する

b. インターフェース特性に加えて、セキュリティ要求事項とともに、伝達された情報の性質を相互接続の都度、組織が文書化する

c. Interconnection Security Agreements における［組織が定めた頻度で割り当て］について、組織がレビュー・更新する。

補足的ガイダンス：このセキュリティ管理策は、情報システム間の専用接続（すなわち、システムの相互接続）に対して適用される管理策である一方、電子メールの送受信またはウェブサイトの閲覧など、ユーザによる一時的な接続に対しては適用されない。

なお、異なるセキュリティ要件のもとで異なるセキュリティ管理策を採用する情報システムが他の情報システムと相互接続した場合、組織はその内外を問わず発生するリスクを慎重に見極めるなか、運用認可責任者は、異なるセキュリティ要件のもとで異なるセキュリティ管理策を採用する情報システムと相互接続することによるリスクを見極めたうえで適切なセキュリティ管理策を採用する。ただし、相互接続されている情報システムの運用認可責任者が共通である場合、相互接続のセキュリティに関する契約を締結する必要がない組織は、相互接続されているシステムのインターフェースの特性をそれぞれのシステムのセキュリティ計画に記載することができる。

相互接続されているシステムの運用認可責任者が組織のなかで異なる場合、組織は相互接続のセキュリティに関する契約を締結する（またはシステムのインターフェースの特性を相互接続されている各システムのセキュリティ計画に記載する）ことができる。また、連邦政府の情報システムと連邦組織以外（すなわち、民間部門）の組織の情報システムが相互接続されている場合、組織は、正式な契約の内容として、組織のなかで情報システムの運用認可責任者が異なる場合における相互接続のセキュリティに関する）契約の内容を一部盛り込んでもよい。

なお、複数の情報システムが同一のネットワークを共有する場合においても、異なるセキュリティ要件のもとで異なるセキュリティ管理策を採用する情報システムが他の情報システムと相互接続した場合のリスクを見極めることが必要である。

宇宙科学・無人機・医療機器といった特定の分野の技術では、もっぱら実際に操作する前のテストの段階で情報システムが相互に接続される場合がある。ただし、実際に操作する前のテストの段階で情報システムが相互に接続される場合、相互接続のセキュリティに関する契約が必となりうることから、追加のセキュリティ管理策を追加で策定することを余儀なくされる可能性がある。

なお、関連するセキュリティ管理策は、AC-3・AC-4・AC-20・AU-2・AU-12・AU-16・CA-7・IA-3・SA-9・SC-7・SI-4 のそれぞれの管理策である。

拡張管理策:

(1) システムの相互接続 |国家安全保障に関わるシステムのうち非機密扱いのシステムへの接続

[組織が定義した境界保護デバイスの割り当て]を利用することなく[国家安全システムのうち非機密扱いのシステムとして組織が定義したシステムの割り当て]によって外部ネットワークに直接接続することを組織が禁止する。

補足的ガイダンス:通常、組織は、インターネット等の外部ネットワークを管理できない一方、ルータ・ファイアウォール等の承認された境界保護デバイスによって外部ネットワークは(国家安全保障に関わるシステムのうち)非機密扱いのシステムとが接続される(すなわち、非機密扱いのシステムと外部ネットワークとの間の情報をフローさせる)。

なお、この拡張管理策は、CUI(管理指定された非機密扱いの情報)を処理または保存もしくは伝送する組織にとって必須の管理策である。

(2) システムの相互接続 |国家安全保障に関わるシステムのうち機密扱いのシステムへの接続

[組織が定義した境界保護デバイスの割り当て]を利用することなく国家安全保障に関わるシステムのうち機密扱いのシステムが外部ネットワークに直接接続する事を組織が禁止する。

補足的ガイダンス:通常、組織は、インターネット等の外部ネットワークを管理できない一方、ルータ・ファイアウォール等の承認された境界保護デバイスによって外部ネットワークは(国家安全保障に関わるシステムのうち)機密扱いのシステムとが接続される(すなわち、機密扱いのシステムと外部ネットワークとの間の情報をフローさせる)。

なお、承認された境界保護デバイスは、管理された通常のインターフェース(および/または管理された通常のドメイン共通システム)として、情報システムから外部ネットワークへの情報フローを管理する。

(3) システムの相互接続 |国家安全保障に関わらない非機密扱いのシステムへの接続

[組織が定義した境界保護デバイスの割り当て]を利用することなく[組織が定義した国家安全保障に関わらない非機密扱いのシステムの割り当て]によって外部ネットワークに直接接続することを組織が禁止する。

補足的ガイダンス:通常、組織は、インターネット等の外部ネットワークを管理することができない一方、ルータ・ファイアウォール等の承認された境界保護デバイスによって、外部ネットワークは(国家安全保障に関わらないシステムのうち)非機密扱いのシステムと接続される(すなわち、機密扱いのシステムと外部ネットワークとの間の情報をフローさせる)。

なお、この拡張管理策は、CUI(管理指定された非機密扱いの情報)を処理または保存もしくは送信する組織に必要なセキュリティ管理策である。

(4) システムの相互接続 | パブリックネットワークへの接続

[組織が定義した情報システムの割り当て]によるパブリックネットワークへの直接接続を組織が禁止する。

補足的ガイダンス：パブリックネットワークは、パブリックアクセス可能な（組織の）エクストラネットをはじめ、インターネットなど、一般の人々がアクセス可能な任意のネットワークを指す。

(5) システムの相互接続 | 外部システムとの接続に対する制限

外部の情報システムに接続する目的で[組織が定義した情報システムの割り当て]を許可するにあたり、組織が[次のいずれかを選択：例外を除き全てを許可するまたは例外を除きすべてを許可しない]によって選択されたポリシーを採用する。

補足的ガイダンス：組織は、①例外を除き全てを許可するポリシー（すなわち、より緩やかなポリシーとしてのブラックリスト化）または②例外を除き全てを許可しないポリシー（すなわち、より厳格なポリシーとしてのホワイトリスト化）の 2 つのいずれかを採用することによって、情報システムによるウェブサイト等の外部ドメインへの接続を制限できる。ただし、組織は、いずれのポリシーについても例外が存在することを前提に、どのような例外ならば許容する事ができるのかについて定める。

なお、関連するセキュリティ管理策は、CM-7 の管理策である。

参考文献：FIPS Publication 199・NIST Special Publication 800-47

優先順位とベースライン管理策の割り当て：

P1	**低** CA-3	**中** CA-3 (5)	**高** CA-3 (5)

CA-4 セキュリティ認証

[削除された：CA-2 に統合された]

CA-5 マイルストーン計画

セキュリティ管理策：

a. 情報システムのセキュリティ管理策を評価した際に発見された脆弱性（または情報システムのセキュリティ管理策を評価した際に発見されたセキュリティ上の欠陥）を解消するために組織によって行われる予定の修復作業のについて記載されたマイルストーン計画を組織が作成する

b. セキュリティ管理策の評価によって得られた知見に加えてセキュリティへの影響の分析によって得られた知見に基づきながら、継続的なセキュリティモニタリングによって得られた知見に基づいて、[（マイルストーン計画に既に記載されたマイルストーンを）組織が定義した頻度で割り当て]を更新する。

補足的ガイダンス：マイルストーン計画は、一連のセキュリティ認可のプロセスにおける主要な文書であるとともに、OMB が当局に報告する義務を課している文書である。

なお、関連するセキュリティ管理策は、CA-2・CA-7・CM-4・PM-4 のそれぞれの管理策である。

拡張管理策:

(1) マイルストーン計画 |マイルストーン計画の正確性・最新性を担保するための自動化されたメカニズム

情報システムのマイルストーン計画が確実に正確・最新かつ具体的なものになるよう、組織が自動化されたメカニズムを採用する。

参考文献:OMB Memorandum 02-01・NIST Special Publication 800-37

優先順位とベースライン管理策の割り当て:

P3	**低** CA-5	**中** CA-5	**高** CA-5

CA-6 セキュリティ認可

セキュリティ管理策:

a. 組織が上級管理職(または上級幹部)を情報システムの運用認可責任者として任命する。

b. する情報システムが運用認可責任者によって実際に運用を開始する前に認可されるよう、組織が万全を期す。

c. 組織が[組織が定めた頻度で(セキュリティ認可を)割り当て]を更新する。

補足的ガイダンス:セキュリティ認可は、システム運用認可のために加えて、合意されたセキュリティ管理策を実装するにあたって(組織の)業務・(組織の)資産・他組織・国家に対するリスクを正式に対処するのために運用認可責任者(すなわち、組織の経営者)によって行われる文書を通じた正式な管理判断である。

組織の情報システムに関連した予算を管理しない場合、運用認可責任者は組織のシステムがサポートするミッション(および/または組織のシステムがサポートする業務)に対して責任を負う。また、セキュリティ認可のプロセスが基本的に連邦政府の責任のもとで行われなけらばならないプロセスであるために運用認可責任者は必ず連邦政府職員でなければならない。

なお、セキュリティ認可のプロセスのなかで組織の情報システムを運用・利用することによるセキュリティリスクについて責任を負う運用認可責任者は、当該リスクについて認識した内容に基づき受容するという判断を下すことができる権限を持つ。

OMB(連邦予算管理局)の政策は、実装されたセキュリティモニタリングプログラムを利用して情報システムのセキュリティ認可を実行するよう組織に対して要求する政策である。当該セキュリティモニタリングプログラムによって組織が情報システムのセキュリティ認可を 3 年ごとに実行しなければならないという要件を満たす事ができるため、組織が別途セキュリティ認可を実行する必要がない。包括的なセキュリティモニタリングプロセスである当該プロセスを用いる事により、認可パッケージ(すなわち、セキュリティ計画・セキュリティアセスメントレポート・行動計画・マイルストーン)に含まれる重要な情報が引き続き更新され、運用認可責任者と情報システムの所有者には、組織の情報システムと稼働環境の最新のセキュリティ状態が伝達されるようになる。セキュリティを認可するかどうかの決定をやり直すかどうかの判断の際、セキュリティ認可のやり直すに当たっての管理上のコストを減らすために、運用認可責任者は当該ポリシーが利用するモニタリングプロセスの結果を最大限に利用する。

なお、関連するセキュリティ管理策は、CA-2・CA-7・PM-9・PM-10 のそれぞれの管理策である。

拡張管理策:なし

参考文献:OMB Circular A-130・OMB Memorandum 11-33・NIST Special Publications 800-37・NIST Special Publications 800-137

優先順位とベースライン管理策の割り当て:

P2	**低** CA-6	**中** CA-6	**高** CA-6

CA-7 継続的なモニタリング

セキュリティ管理策:組織がセキュリティを継続的にモニタリングする戦略を策定のうえ、

a. セキュリティモニタリングの対象となる[組織が定めたメトリクスの割り当て]を確立しながら、
b. セキュリティモニタリングの頻度を[組織が定義した頻度の割り当て]に、また、そうしたモニタリングを支援するセキュリティ評価の頻度を[組織が定義した頻度の割り当て]に設定するとともに、
c. 組織が継続的にセキュリティモニタリングを行うための戦略に従って、セキュリティ管理策を継続的に評価しつつ、
d. 組織の継続的モニタリング戦略に従って、組織が定めたメトリクスのセキュリティ状態のモニタリングを継続的に実施するのに加えて、
e. セキュリティ評価とモニタリングにより生成された、セキュリティ情報の相関処理と分析を行うのに合わせて、
f. セキュリティ情報の分析結果に応じた対応措置を取りながら、
g. 組織および情報システムのセキュリティ状態を[組織が定めた職員(または組織が定めた役職)を割り当て]に、[組織が定めた頻度で割り当て]報告するという

継続的モニタリングプログラムを実施する。

補足的ガイダンス:継続的モニタリングプログラムは、組織がリスクを管理するなかで脅威・脆弱性・情報セキュリティのそれぞれについて意識することを怠らないようサポートするプログラムである。「継続的な(continuous)」や「最新の(ongoing)」という用語は、組織がセキュリティ管理策と情報セキュリティ関連のリスクの評価/分析を組織によるリスクに基づいた判断をサポートするのに十分な頻度で実施することを意味する。継続的モニタリングプログラムの結果は、組織が取るべき適切なリスク対応活動を生み出す。継続的モニタリングプログラムは、また、組織がミッションおよび/または業務ニーズ、脅威、脆弱性、およびテクノロジーが変化する極めて動的な稼働環境において、長期にわたって情報システムと共通管理策のセキュリティ認可を維持する事を可能にする。セキュリティ関連の情報にレポートおよび/またはダッシュボードを通じて継続的にアクセスできれば、組織の担当者は、最新のセキュリティ認可判断を含む、より効果的でタイムリーなリスク管理判断を下せるようになる。自動化が実現すれば、セキュリティ認可パッケージ、ハードウェア/ソフトウェア/ファームウェア一覧、およびその他のシステム情報のより高い頻度での更新が可能になる。継続的なモニタリングの結果のフォーマットが整えられ、具体的で、測定できて、すぐ使用できて、適切かつタイムリーな情報が提供されるようになれば、有効性はさらに向上する。継続的モニタリング活動は、情報システムのセキュリティカテゴリに応じて拡張されたり、縮小されたりする。関連するセキュリティ管理策は、CA-2・CA-5・CA-6・CM-3・CM-4・PM-6・PM-9・RA-5・SA-11・SA-12・SI-2・SI-4 のそれぞれの管理策である。

拡張管理策:

(1) 継続的なモニタリング | 独立した評価者(または独立した評価チーム)によるセキュリティ評価

[組織が定めたレベルの独立性の割り当て]を有する評価者または評価チームを採用して、情報システムに導入されているセキュリティ管理策を組織が継続的にモニタリングする。

補足的ガイダンス：組織は、継続的監視プロセス時に実施されるセキュリティ管理策評価の価値を最大限に引き出すために、そうしたセキュリティ評価が継続的モニタリング戦略に基づいた適切なレベルの独立性を有する評価者または評価チームによって実施されることを要求できる。評価者の独立性が確保されていれば、セキュリティモニタリングのプロセスに一定の公平さがもたらされる。そうした公平さを実現するには、アセサーが以下を行わない事が求められる：①セキュリティ評価が実施されている組織との間で、相互利益や利害の対立を引き起こす②自身の仕事を評価する③自身が使える組織の経営者または職員として活動するあるいは④自身が提供するサービスを受ける組織にとって、その組織をする立場に身を置く。

(2) 継続的なモニタリング | アセスメントタイプ

[削除：CA-2 に統合された]

(3) 継続的なセキュリティモニタリング | 動向分析

動向分析を実施して、セキュリティ管理策の導入、継続的モニタリング活動の頻度、および／または継続的モニタリングプロセスに用いられている活動の修正の必要性を経験上のデータに基づいて判断する。

補足的ガイダンス：動向分析は、例えば、組織内または連邦政府内で発生した脅威イベントに関する最新の脅威情報、特定のタイプのサイバー攻撃の成功率、情報技術の新たに発見された脆弱性、進化するソーシャルエンジニアリング技法、複数回にわたるセキュリティ管理策アセスメントの結果、設定項目の有効性および監察長官または監査人の所見を検証することを含む。

参考文献：OMB Memorandum 11-33・NIST Special Publications 800-37・NIST Special Publications 800-39・NIST Special Publications 800-53A・NIST Special Publications 800-115・NIST Special Publications 800-137・US-CERT Technical Cyber Security Alerts・DoD Information Assurance Vulnerability Alerts

優先順位とベースライン管理策の割り当て：

P2	**低** CA-7	**中** CA-7 (1)	**高** CA-7 (1)

CA-8 侵入テスト

セキュリティ管理策：[組織が定めた情報システムまたはシステムコンポーネントの割り当て]に対する侵入テストを組織が[組織が定めた頻度で割り当て]実施する。

補足的ガイダンス：侵入テストは、情報システムまたはシステムの個々のコンポーネント上で、敵対者によって利用される可能性のある脆弱性を特定するために実施される特殊なタイプの評価である。そうしたテストは、脆弱性を確認するために、あるいは指定された一連の制約のもとで（例：時間、リソース、および／またはスキル）敵対者に対して、組織の情報システムがどの程度耐性を有するかを特定するために用いられる。侵入テストでは、組織に対して敵意を持ったサイバー攻撃をしかける敵対者が取るアクションを模倣して、セキュリティ関連の弱点／欠陥を詳細に分析する。組織は、また、侵入テスト活動を支援するために、脆弱性分析の結果を使用できる。侵入テストは、情報システムのハードウェアコンポーネント、ソフトウェアコンポーネント、またはファームウェアコンポーネント上で実施することができ、物理面でのセキュリティ管理策と技術面でのセキュリティ管理策の両方をことになる。侵入テストの標準手法には、例えば、以下がある：①対象システムについて十分に理解した上で、事前分析を行うこと②事前分析の結果に基づいて、事前に脆弱性を特定する事③特定された脆弱性が利用される可能性を判断するための、テストを実施する事。すべての関係者は侵入テストシナリオを実行する前に、活動規則に同意する。組織は、敵対者が攻撃を行うのに使用する事が予想されるツール・技法・手順と、侵入テストの活動規則とを相互に関連付ける。組織によるリスク評価は、侵入テストを実施する

職員に求められる、独立性のレベルの決定に役立つ。関連するセキュリティ管理策は、SA-12の管理策である。

拡張管理策:

(1) 侵入テスト | 独立性した侵入エージェントまたは独立した侵入チーム

組織は、独立性を有する侵入エージェントまたは侵入チームを採用して、情報システムまたはシステムコンポーネントに対する侵入テストを実施する。

補足的ガイダンス:独立性を有する侵入エージェントまたは侵入チームとは、組織の情報システムに対して公平な侵入テストを実施できる、個人またはグループである。ここでいう公平さとは、侵入エージェントまたは侵入チームが侵入テストの対象である情報システムの開発または運用もしくは管理に関して認識された、または実際の利害の衝突とは無関係であることを意味する。CA-2(1)の補足的ガイダンスは、侵入テストに適用できる独立性が確保されたアセスメントに関する追加情報を提供する。関連するセキュリティ管理策は、CA-2 の管理策である。

(2) 侵入テスト | レッドチーム訓練

組織は、[組織が定めたレッドチーム訓練の割り当て]を用いて、[組織が定めた活動規則]に従って、組織の情報システムに対する敵対者による侵害の試みを試算する。

補足的ガイダンス:レッドチーム訓練では、侵入テストの目的を広げて組織のセキュリティ姿勢と、組織が効果的なサイバー防御を実施できるかどうかを検証する。したがって、レッドチーム訓練には、組織のミッション／業務機能に対する敵対者による侵害の試みをシミュレートし、情報システムと組織のセキュリティ状態を包括的に評価できるといった利点がある。組織のミッション(および／または組織の業務機能)と、それらのミッション／機能を支援する情報システムに対する敵対者による侵害の試みのシミュレーションでは、例えば、テクノロジーを重視した攻撃(例:ハードウェアコンポーネント、ソフトウェアコンポーネント、またはファームウェアコンポーネントおよび／またはミッション／業務プロセスに対する干渉)や、ソーシャルエンジニアリングを用いた攻撃(例:電子メール、電話、ショルダーサーフィン、または個人的な会話を介して情報を得ること)を試算する。侵入テストが概して実験室ベースのテストであるのに対し、レッドチーム訓練は現実世界の状況を反映したより包括的なアセスメントを目的として組織が採用する。レッドチーム訓練は、セキュリティ意識とトレーニングを向上させると同時に、セキュリティ管理策の有効性レベルを評価するために用いることができる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** 選択されていない	**高** CA-8

CA-9 システムに対する内部接続

セキュリティ管理策:組織は、

a. 情報システムに対する、[組織が定めた情報システムコンポーネントまたはコンポーネントの集合]からの内部接続を正式に許可するとともに、

b. 内部接続の各々について、インターフェース特性・セキュリティ要求事項・および伝達される情報の性質を文書化する。

補足的ガイダンス:このセキュリティ管理策は、組織の情報システムと、そのシステムを構成する(切り離されている)コンポーネントとの間の接続に適用される(例:イントラシステムのコンポーネント)。そうした接続には、例えば、携帯機器・ノートパソコン・デスクトップコンピュータ・プリ

ンター・コピー機・ファクシミリ装置・スキャナー・センサー・サーバーシステムとの接続がある。組織は、個々の内部接続を認可する代わりに、共通の特性や設定を有するコンポーネント群からの内部接続を認可することができる。例としては、処理・保存・伝送のそれぞれについて指定された機能を備えたすべてのデジタルプリンター・スキャナー・コピー機とともに、特定のベースライン設定がなされているすべてのスマートフォンが挙げられる。関連するセキュリティ管理策は、AC-3・AC-4・AC-18・AC-19・AU-2・AU-12・CA-7・CM-2・IA-3・SC-7・SI-4 のそれぞれの管理策である。

セキュリティ管理策の拡張管理策:

(1) システムに対する内部接続 | セキュリティコンプライアンスチェック

情報システムは、内部接続を確立する前にシステムを構成する各コンポーネントに対してセキュリティコンプライアンスチェックを実施する。

補足的ガイダンス:セキュリティコンプライアンスチェックには、例えば、関連するベースライン設定の検証が含まれる場合がある。関連するセキュリティ管理策は、CM-6 のそれぞれの管理策である。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** CA-9	**中** CA-9	**高** CA-9

ファミリ:構成管理

CM-1　構成管理のポリシーと手順

セキュリティ管理策:

a. 以下を策定・文書化し、[組織が定めた職員または役職]に配布する:

組織が

1. 目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー
2. 構成管理ポリシーと関連する「構成管理」管理策の実施を容易にするための手順

の2つを策定・文書化する。

b. 以下の最新版をレビューし、更新する:

1. 構成管理のポリシーを[指定:組織が定めた頻度で]
2. 構成管理の手順を[指定:組織が定めた頻度で]

補足的ガイダンス:この管理策は、CM ファミリ内の選択されたセキュリティ管理策と「拡張管理策」を効果的に導入するためのポリシーと手順の策定について取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーおよび手順を策定する上で鍵となる。関連するセキュリティ管理策は、PM-9 の管理策である。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** CM-1	**中** CM-1	**高** CM-1

CM-2　ベースライン構成

セキュリティ管理策:構成管理の一環として、組織が情報システムの最新のベースライン構成を把握・文書化・維持する。

補足的ガイダンス:この管理策は、情報システムとシステムコンポーネントのベースライン構成(システムの通信と接続性の側面を含む)を把握するためのものである。ベースライン構成は、文書化、正式なレビューおよび合意を経た、情報システムの仕様、またはそれらのシステムの設定項目である。ベースライン構成は、情報システムの将来にわたる構築、リリース、および/または変更の際にベースになる。ベースライン構成は、情報システムコンポーネント(例:ワークステーション、ノートパソコン、サーバー、ネットワークコンポーネント、または携帯機器にインストールされている標準ソフトウェアパッケージ・オペレーティングシステムとアプリケーションの現在のバージョン番号とパッチ情報・設定項目/パラメータ)、ネットワークの接続形態、およびシステム構成内のそれらのコンポーネントの論理的な配置に関する情報を含む。ベースライン構成を維持するには、組織の情報システムが時間の経過と共に変化することから、新しいベースラインを作成する必要がある。情報システムのベースライン構成は、現在のエンタープライズアー

キテクチャを反映する。関連するセキュリティ管理策：CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7。

拡張管理策：

(1) ベースライン構成 | レビューと更新

組織は、以下のタイミングで、情報システムのベースライン構成をレビューし、更新する:

(a) ［指定：組織が定めた頻度］

(b) ［指定：組織が定めた状況］に起因して必要な場合

(c) 情報システムコンポーネントのインストール時やアップグレード時

補足的ガイダンス：関連するセキュリティ管理策は、CM-5。

(2) ベースライン構成| 正確かつ最新になることを自動で支援する

組織は、最新、完全、正確であり、かつ、すぐに利用できる、情報システムのベースライン構成を維持するための自動化されたメカニズムを使用する。

補足的ガイダンス：組織による、情報システムの一貫性のあるベースライン管理策の構成の維持を支援する自動化されたメカニズムには、例えば、ハードウェア／ソフトウェア一覧作成ツール・構成管理ツール、ネットワーク管理ツール等がある。そうしたツールは、情報システムレベルで、あるいはオペレーティングシステムレベルまたはコンポーネントレベル（例：ワークステーション、サーバー、ノートパソコン、ネットワークコンポーネント、携帯機器）で共通管理策として使用したり、割り当てることが可能である。ツールは、例えば、オペレーティングシステムアプリケーションのバージョン番号、インストールされているソフトウェアのタイプ、現在のパッチレベルなどを把握するために使用できる。この拡張管理策は、組織が情報システムコンポーネント一覧とベースライン構成活動を結び付けたいと考える場合には、CM-8(2)の管理策を実施することで満たせるようになる。関連するセキュリティ管理策は、CM-7・RA-5 のそれぞれの管理策である。

(3) ベースライン構成 | 以前の構成を記録しておく

情報システムのベースライン構成のロールバックを可能にするために、組織が［指定：組織が定めた分だけ前のバージョンのベースライン構成］から記録する。

補足的ガイダンス：ロールバックを可能にするために旧バージョンのベースライン構成を記録する際の記録内容には、例えば、ハードウェア・ソフトウェア・ファームウェア・構成ファイル・構成記録がある。

(4) ベースライン管理策の構成 | 許可されていないソフトウェア

[削除された：CM-7 に統合された]

(5) ベースライン管理策の構成 | 許可されているソフトウェア

[削除された：CM-7 に統合された]

(6) ベースライン管理策の構成| 開発およびテスト環境

本番環境におけるベースライン構成とは別に管理される開発環境とテスト環境におけるベースライン構成を組織が維持する。

補足的ガイダンス：開発環境・テスト環境・本番環境において、それぞれに別のベースライン管理策の構成を確立することは、開発およびテスト活動に関連する予想外の／予期せぬイベントから情報システムを保護するのに役立つ。それぞれに別のベースライン管理策の構成を確立する事で、組織は、それぞれのタイプの構成に対して、最も適切な構成管理を適用できるようになる。例えば、本番環境における構成の管理は、通常は安定性を重視するが、開発／テスト環境における構成の管理は、より高い柔軟性を必要とする。テスト環境における構成は、テスト結果に稼働中のシステムに対して提案されている変更が反映されるよう、可能な範囲で本番環境における構成をまねる。この拡張管理策は、個別の構成を

必要とするが、必ずしも物理的に異なる環境である必要はない。関連するセキュリティ管理策は、CM-4・SC-3・SC-7。

(7) ベースライン構成|リスクの高い場所に持ち込まれるシステム、コンポーネント、または機器の設定

組織は、

(a) リスクが著しく高いと組織が考える場所に出向く個人に対しては、[指定:組織が定めた設定]がなされた、[指定:組織が定めた情報システム、システムコンポーネント、またはデバイス]を貸与する

(b) 上記の個人が戻ってきた時に、貸与されたデバイスに対して、[指定:組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス:情報システム・システムコンポーネント・デバイス(それぞれの例:ノートパソコン、携帯機器)がリスクの高い場所に置かれることが分かっている場合には、組織によって管理される領域とは対照的に物理的セキュリティが確保されないため、大きな脅威に対処するために追加のセキュリティ管理策が実施される可能性がある。例えば、出張する個人が使用するノートパソコンと出張から帰ってきた個人が出張中に使用したノートパソコンに対する組織のポリシーと手順には、例えば、懸念される場所を特定すること、デバイスに必要な設定を定めること、出張前にデバイスが意図した通りに設定されるているのを確認すること、出張後にデバイスに特定の対策を実施することなどが挙げられる。特殊な設定がなされたノートパソコンには、例えば、ハードディスクを無害化し、搭載するアプリケーションを限定して、追加の強化策(例:より厳格な設定)を施したノートパソコンがある。出張から帰ってきた時点で携帯機器に適用される対策には、例えば、機器を検証して物理的な改ざんがなされていないことを確認する事や、ハードディスクの情報を消去・再イメージングすることがある。携帯機器上の情報の保護に関しては、「媒体の保護」の管理策ファミリで取り扱われている。

参考文献:NIST Special Publication 800-128

優先順位とベースライン管理策の割り当て:

P1	**低** CM-2	**中** CM-2 (1) (3) (7)	**高** CM-2 (1) (2) (3) (7)

CM-3 構成変更管理

セキュリティ管理策:組織は、

a. 構成管理の対象となる情報システムに対する変更について定める
b. 構成管理の対象となる情報システムに対して提案されている変更をレビューし、セキュリティ影響分析結果を考慮した上で、そうした変更を許可する/許可しない
c. その情報システムの構成変更についての決定を文書化する
d. 許可された情報システムに対する変更を実施する
e. 構成管理の対象となる情報システムに対する変更について、記録を[指定:組織が定めた期間]にわたって保管する
f. 構成管理の対象となる情報システムに対する変更について、関連する活動を監査し、レビューする
g. [選択(1つ以上):[指定:組織が定めた頻度で]、[指定:組織が定めた、構成変更に関する条件が満たされる場合に]]招集される、[指定:組織が定めた構成変更管理グループ(例:委員会、役員会)]を通じて、構成変更管理活動を調整・監督する。

補足的ガイダンス：組織の情報システムの構成変更管理は、システムのアップグレードや変更などの、システムに対する変更の系統立った提案、是非の判断、実施、テスト、レビュー、破棄を含む。構成変更管理は、情報システムのコンポーネントや構成品目のベースライン構成の変更、IT 製品（例：オペレーティングシステム・アプリケーション・ファイアウォール・ルーター・携帯機器）の設定項目の値の変更、予定外の／許可されていない変更、そして脆弱性を修正するための変更を対象にする。情報システムの構成変更を管理するための典型的なプロセスには、たとえば、システムに対して提案されている変更を許可する権限を有する Configuration Control Boards がある。組織は、情報システムを新規に開発する場合や、システムの大幅なアップグレードを行う場合には、開発組織の代表を Configuration Control Boards に含めることを検討する。変更の監査は、組織の情報システムに対する変更が実施される前後の活動と、そうした変更を実施する際に必要な監査活動を含む。関連するセキュリティ管理策は、CA-7・CM-2・CM-4・CM-5・CM-6・CM-9・SA-10・SI-2・SI-12。

拡張管理策：

(1) 構成 変更管理 | 変更を自動で文書化/ 報告 /禁止する

以下を実施するための自動化されたメカニズムを組織が使用する:

(a) 情報システムに対して提案されている変更を文書化する

(b) 情報システムに対して提案されている変更について、[組織が定めた承認権限者の割り当て]に報告し、変更の承認を要請する

(c) 情報システムに対して提案されている変更のうち、[組織が定めた期限の割り当て]までに許可／未許可が決定されていないものをハイライトする

(d) 所定の承認を得られるまで、情報システムに対する変更を禁止する

(e) 情報システムに対するすべての変更を文書化する

(f) 情報システムに対する承認された変更が完了した時点で、[組織が定めた職員の割り当て]に報告する。

(2) 構成変更管理 | 変更をテスト / 承認 / 文書化する

組織は、稼働している情報システムに対して変更を実施する前に、それらの変更をテスト・承認・文書化する。

補足的ガイダンス：情報システムに対する変更は、ハードウェアコンポーネント、ソフトウェアコンポーネント、またはファームウェアコンポーネントに対する変更と、CM-6 のセキュリティ管理策に定義されている設定項目に対する変更を含む。組織は、テストが、情報システムの稼働を妨げることがないようにする。テストを実施する個人／グループは、組織のセキュリティポリシーと手順、情報システムセキュリティポリシーと手順、および特定の施設／プロセスにおける健康面・安全面・環境面での具体的なリスクを理解する事。稼働中のシステムは、テストが実施される前に、オフラインにされたり、可能な範囲で複製されたりする。テストのために情報システムをオフラインにする必要がある場合、テストは可能な場合は常にシステムの予定された停止期間内に行われるようスケジュールが組まれる。組織は、稼働中のシステム上でテストを実施できない場合には、補完的管理策を実施する（例：複製されたシステム上でテストを実施する）。

(3) 構成変更管理 | 変更を自動で実施する

組織は、現在の情報システムベースラインに対する変更を実施するための自動化されたメカニズムを使用し、更新されたベースライン管理策を設置基盤に展開する。

(4) 構成変更管理 | セキュリティ担当者

組織は、情報セキュリティ担当者の一人が、[組織が定めた.構成変更管理グループの割り当て]の一員となることを要求する。

補足的ガイダンス：情報セキュリティ担当者には、例えば、政府機関の上級情報セキュリティ責任者・情報システムセキュリティ責任者・情報システムセキュリティ管理者がいる。情報セキュリティの専門知識を有する職員によって構成される情報セキュリティ担当者の存在は重要である。なぜなら、情報システムの構成の変更が、セキュリティ関連の副作用を及ぼすことがあるからである。そうした変更をプロセスの初期段階で発見できれば、組織の情報システムのセキュリティ状態を最終的に変化させる予期せぬ負の影響を回避できる。この拡張管理策における構成変更管理グループは、CM-3 のセキュリティ管理策に記載されている各組織が定める構成変更管理グループと同一である。

(5) 構成変更管理 | 自動化されたセキュリティレスポンス

ベースライン構成が不正に変更された場合に、情報システムが[組織が定めたセキュリティレスポンス]を自動的に実施する。

補足的ガイダンス：セキュリティレスポンスの例としては、構成品目が一つでも不正に変更された場合に、情報システムの処理を停止する、選択されたシステム機能を停止する、あるいは組織の職員に警告を発する／報告するといったことが挙げられる。

(6) 構成変更管理 | 暗号管理

組織は、[指定：組織が定めたセキュリティ対策]を提供する暗号メカニズムが、構成管理の対象に含まれるようにする。

補足的ガイダンス：使用されている暗号手法（例：公開鍵秘密鍵共有秘密鍵）にかかわらず、組織は、手法を効果的に管理するためのプロセスと手順を用意する。例えば、デバイスが証明書を識別と認証のベースとして使用する場合、それらの証明書の失効に対処するためのプロセスが必要になる。関連するセキュリティ管理策は、SC-13 の管理策である。

参考文献：NIST Special Publication 800-128

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** CM-3 (2)	**高** CM-3 (1) (2)

CM-4 セキュリティ影響分析

セキュリティ管理策：組織は、情報システムに対する変更を実施する前に、変更を分析して、セキュリティ影響を特定する。

補足的ガイダンス：情報セキュリティに責任のある職員（例：情報システムアドミニストレーター・情報システムセキュリティ責任者・情報システムセキュリティ管理者・情報システムセキュリティエンジニア）は、セキュリティ影響分析を実施する。セキュリティ影響分析を実施する個人は、情報システムに対する変更と、関連するセキュリティ影響を分析するのに必要なスキル／技術的専門知識を有する。セキュリティ影響分析は、例えば、セキュリティ計画をレビューして、必要なセキュリティ管理策を把握することと、システム設計書をレビューして、管理策の導入方法と、特定の変更がそれらの管理策にどのように影響を及ぼすかを理解する事を含む。セキュリティ影響分析は、また、リスクを評価し、変更による影響をより良く理解して、追加のセキュリティ管理策が必要であるかを判断する事を含む。セキュリティ影響分析は、情報システムのセキュリティカテゴリに応じて拡張または縮小される。関連するセキュリティ管理策は、CA-2・CA-7・CM-3・CM-9・SA-4・SA-5・SA-10・SI-2 のそれぞれの管理策である。

拡張管理策：

(1) セキュリティ影響分析 | 切り離されたテスト環境

情報システムに対する変更を本番環境で実施する前に、そうした変更を本番環境とは切り離されたテスト環境で分析し、欠陥・弱点・互換性が無いこと、あるいは意図的な犯意に起因するセキュリティ影響を組織が特定する。

補足的ガイダンス：この文脈で「切り離されたテスト環境」とは、本番環境とは物理的に、または論理的に切り離されている環境を意味する。切り離しはテスト環境における活動が本番環境における活動に影響を及ぼすことが無いように、また本番環境で扱う情報が誤ってテスト環境に伝送され無いように十分なレベルであることを指す。環境の切り離しは、物理的または論理的に実現できる。物理的に切り離されたテスト環境が使用されない場合には、組織は論理的な切り離し（例：仮想マシンによる切り離し）を行うことになるが、その際、必要なメカニズムの強度を決定する。関連するセキュリティ管理策：SA-11・SC-3・SC-7。

(2) セキュリティ影響分析 | セキュリティ機能の確認

組織は、情報システムが変更された後にセキュリティ機能をチェックし、それらの機能が正しく導入されると同時に意図したとおりに運用されるとともに、システムのセキュリティ要求事項に対する適合性の観点から所望の結果を産出しているかどうかを確認する。

補足的ガイダンス：この文脈で「導入」とは、変更されたコードを稼働している情報システムに組み込むことを意味する。関連するセキュリティ管理策は、SA-11 の管理策である。

参考文献：NIST Special Publication 800-128

優先順位とベースライン管理策の割り当て：

P2	**低** CM-4	**中** CM-4	**高** CM-4 (1)

CM-5 変更に対するアクセス制限

セキュリティ管理策：組織は、情報システムに対する変更に関して、物理的／論理的なアクセス制限を定義・文書化・承認のうえ実施する。

補足的ガイダンス：情報システムのハードウェア、ソフトウェア、および／またはファームウェアコンポーネントに対する変更は、どのようなものであれ、システムの全般的なセキュリティに重大な影響を及ぼす可能性がある。したがって、組織は資格のある権限を与えられた個人にのみが、アップグレードや修正を含む変更のために情報システムにアクセスできるようにする。組織はアクセス記録を保管する事で、構成変更管理が確実に実施されるようにし、かつ、なんらかの不正な変更を発見した場合に事後措置を取れるようになる。変更に対するアクセス制限は、ソフトウェアライブラリも対象が含まれる。アクセス制限には、例えば、物理的／論理的なアクセス制御（AC-3 および PE-3 のそれぞれの管理策を参照）、ワークフローの自動化、メディアライブラリ、抽象レイヤー（例：変更が情報システムに対して直接ではなく、第三者インターフェースを介して実施される）、ウィンドウの切り替え（例：切り替えを指定された時間内に限定することで、不正な切り替えを発見しやすくする）。関連するセキュリティ管理策は、AC-3・AC-6・PE-3 のそれぞれの管理策である。

拡張管理策：

(1) 変更に対するアクセス制限 | アクセス制御を自動で実施 / 確認する

情報システムは、アクセス制限を実施し、実施状況の確認を支援する。

補足的ガイダンス：関連するセキュリティ管理策は、AU-2・AU-12・AU-6・CM-3・CM-6 のそれぞれの管理策である。

(2) 変更に対するアクセス制限 | システムに対する変更のレビュー

情報システムに対する変更を［組織が定めた頻度で割り当て］、また、［組織が定めた状況が発生した場合に割り当て］レビューし、不正な変更の有無を組織が確認する。

補足的ガイダンス：情報システムに対する変更のレビューを必要とする兆候と、そうしたレビューを必要とする状況は、構成変更プロセス時に組織が実施する活動から、具体的な例が得られるだろう。関連するセキュリティ管理策：AU-6, AU-7, CM-3, CM-5, PE-6, PE-8。

(3) 変更に対するアクセス制限 | デジタル署名されたコンポーネント

情報システムは、[指定：組織が定めたソフトウェアコンポーネントとファームウェアコンポーネント]が、組織が認めて承認した証明書を使用してデジタル署名されたことが確認できないのであれば、コンポーネントのインストールをさせない。

補足的ガイダンス：認められて承認された証明書を使用して署名されない限りインストールが許されないソフトウェアコンポーネントとファームウェアコンポーネントには、例えば、ソフトウェア／ファームウェアのバージョンアップ、パッチ、サービスパック、デバイスドライバ、および BIOS のアップデートがある。組織は、該当するソフトウェアコンポーネントとファームウェアコンポーネントをタイプ別、項目別、あるいは両方の組み合わせで指定することができる。デジタル署名を使用して、かつ、そうした署名を組織が確認する事は、コード認証の1つの方法となる。関連するセキュリティ管理策は、CM-7・SC-13・SI-7。

(4) 変更に対するアクセス制限 | 二重認証

組織は、[指定：組織が定めた、情報システムコンポーネントとシステムレベルの情報]に対する変更が行われる際には、二重認証を実施する。

補足的ガイダンス：組織は、選択された情報システムコンポーネントと情報に対するすべての変更が、資格のある二人の個人によって実施されない限り発生しないよう、二重認証を実施する。それらの二人の個人は、提案されている変更が、承認された変更を正しく実施するものであるかを判断できる十分なスキル／専門知識を有するものとする。二重認証は、「二人立会制御（two-person control）」としても知られている。関連するセキュリティ管理策は、AC-5・CM-3。

(5) 変更に対するアクセス制限 | 本番環境における権限を制限する

組織は、

(a) 本番環境内の情報システムコンポーネントとシステム関連情報を変更する権限をに制限する

(b) 権限のレビューと再評価を[指定：組織が定めた頻度で]行う。

補足的ガイダンス：多くの組織では、情報システムは複数の主要なミッション／業務機能を支援する。稼働中のシステムのシステムコンポーネントを変更する権限を制限することは、必要である。特定の情報システムコンポーネントに対する変更が、そのコンポーネントが設置されているシステムによってサポートされるミッション／業務プロセスに、広範囲な影響を及ぼすことがあるからである。システムとミッション／業務プロセス間に複雑な、多対多の関係があるにもかかわらず、その事実を開発者は知らないこともある。関連するセキュリティ管理策は、AC-2。

(6) 変更に対するアクセス制限 | ライブラリに対する権限を制限する

組織は、ソフトウェアライブラリ内のソフトウェアを変更する権限を制限する。

補足的ガイダンス：ソフトウェアライブラリは、特権的なプログラムも含む。関連するセキュリティ管理策は、AC-2。

(7) 変更に対するアクセス制限 | セキュリティ対策を自動で実施する

[削除された：SI-7 に統合された]

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** CM-5	**高** CM-5 (1) (2) (3)

CM-6　設定項目

セキュリティ管理策：組織は、

a. 運用上の要求事項に適合する最も制限されたモードを反映する［指定：組織が定めたセキュリティ設定チェックリスト］を使用して、情報システムに導入されている IT 製品の設定項目を把握のうえ文書化するのと合わせて、

b. 上記で把握されている/文書化されている設定項目を実施するとともに、

c. ［指定：組織が定めた運用上の要求事項］に基づいて、［指定：組織が定めた情報システムコンポーネント］の定められた設定からの逸脱を特定・文書化のうえ承認するのに加えて、

d. 設定に対する変更を組織のポリシーと手順に従ってモニタリングのうえ管理する。

補足的ガイダンス：設定項目とは、情報システムのハードウェアコンポーネント、ソフトウェアコンポーネント、またはファームウェアコンポーネントの値を変更できるパラメータであり、システムのセキュリティ状態および／または機能を左右する。セキュリティ設定項目を定義できる IT 製品には、たとえば、メインフレームコンピュータ・サーバー（例：データベース・電子メール・認証・ウェブ・プロキシ・ファイル。ドメイン名）、ワークステーション・入出力装置（例：スキャナー・コピー機・プリンター）、ネットワークコンポーネント（例：ファイアウォール・ルーター・ゲートウェイ・音声／データスイッチ・ワイヤレスアクセスポイント・ネットワーク装置・センサー）・オペレーティングシステム・ミドルウェア・アプリケーションがある。セキュリティパラメータは、情報システムのセキュリティ状態に影響を及ぼすパラメータであり、その一部は、その他のセキュリティ管理策要求事項を満たすのに必要である。セキュリティパラメータには、例えば、以下がある：①レジストリの設定②アカウント・ファイル・ディレクトリのパーミッション設定③機能・ポート・プロトコル・サービス・リモート接続などの設定。組織は、組織全体にわたる設定項目を定め、その後、情報システムに特化した設定を定める。定められた設定は、システムを構成するベースライン管理策の一部となる。

コモンセキュアコンフィギュレーション（セキュリティ設定チェックリス・封鎖および堅牢化の手引き・セキュリティリファレンスガイド・セキュリティ技術実装ガイドと称される場合もある）は、特定の IT プラットフォーム／製品向けのセキュアな設定を規定し、運用上の要求事項が満たされるようにそうした情報システムコンポーネントを設定する方法を示す、認められていて、標準化されていて、かつ定評のあるベンチマークを提供する。コモンセキュアコンフィギュレーションは、たとえば、IT 製品の開発業者をはじめ、製造業者・ベンダー・合弁企業・学会・産業・連邦政府機関に加えて、公共部門と民間部門の他の組織など、さまざまな組織によって策定される。コモンセキュアコンフィギュレーションには、CM-6・AC-19・CM-7 などの他のセキュリティ管理策の導入に影響を及ぼす USGCB（United States Government Configuration Baseline：米国政府構成ベースライン管理策）がある。SCAP(Security Content Automation Protocol)と、その中で定義されている標準（例：Common Configuration Enumeration）は、設定項目を一意に特定・追跡し・管理するための効果的な手段になる。OMB は、連邦政府情報システムの構成必要条件に関する連邦政府の政策を規定している。関連するセキュリティ管理策は、AC-19・CM-2・CM-3・CM-7・SI-4。

拡張管理策：

(1) 設定項目| 一つの場所から自動で管理 / 適用 / 検証する

組織は、［指定：組織が定めた情報システムコンポーネント］の設定を一つの場所から管理・適用のうえ検証するための自動化されたメカニズムを使用する。

補足的ガイダンス：関連するセキュリティ管理策は、CA-7・CM-4。

(2) 設定項目 | 不正な変更に対処する

組織は、［指定：組織が定めた設定］の不正な変更に対処するための、［指定：組織が定めたセキュリティ対策］を実施する。

補足的ガイダンス：設定の不正な変更への対処には、例えば、指定された組織の職員を交代させる、定められた設定に戻す、あるいは極端な場合には、影響を受ける情報システム処理を停止することが含まれる。関連するセキュリティ管理策は、IR-4・SI-7。

(3) 設定項目| 不正な変更の検知

[削除された：SI-7 に統合された]

(4) 設定項目| 準拠していることを示す

[削除された：CM-4 に統合された]

参考文献：OMB Memoranda 07-11・OMB Memoranda 07-18・OMB Memoranda 08-22・NIST Special Publications 800-70・NIST Special Publications 800-128・ウェブサイト http://nvd.nist.gov・ならびに http://checklists.nist.gov および http://www.nsa.gov

優先順位とベースライン管理策の割り当て：

P1	**低** CM-6	**中** CM-6	**高** CM-6 (1) (2)

CM-7 最小機能

セキュリティ管理策：組織は、

a. 不可欠な機能のみを提供するように、情報システムを設定する

b. 以下の機能、ポート、プロトコル、および／またはサービスの使用を禁止または制限する：［指定：機能・ポート・プロトコル・サービスのうち禁止または制限の対象として組織が定めたもののすべて（またはそれらのいずれか）］。

補足的ガイダンス：情報システムは、さまざまな機能とサービスを提供する。デフォルトで提供される機能やサービスの中には、組織の極めて重要な業務（例：主要なミッションおよび主要な機能）をサポートしないものもある。また、単一の情報システムコンポーネントによって複数のサービスを提供する方が便利な場合もある。しかしながら、そうすることによって、個々のコンポーネントによって提供されるサービスを制限することに伴うリスクが増加する。組織は、可能な場合にはコンポーネントの機能を、一台のデバイスに一つの機能といった形で制限する（例：電子メールサーバーまたはウェブサーバー、ただし両方であってはならない）。組織は、情報システムまたは情報システムの個々のコンポーネントによって提供される機能とサービスをレビューし、削除の候補となる機能とサービスを特定する（例：(VoIP)、インスタントメッセージ、自動実行、ファイル共有）。組織は、デバイスの不正な接続、情報の不正な転送、または許可されていないトンネリングを防止できるよう、情報システム上の使用されていない、または必要でない物理的な／論理的なポート／プロトコル（例：USB、FTP、HTTP）を無効にすることを検討する。組織は、禁止されている機能、ポート、プロトコル、サービスの使用を検知し防止するために、ネットワークスキャンツール、侵入検知防止システム、エンドポイントプロテクション（ファイアウォール、ホストベースの侵入検知システムなど）を活用することができる。なお、関連するセキュリティ管理策は、C-6・CM-2・RA-5・SA-5・SC-7。

拡張管理策：

(1) 最小機能 | 定期的なレビュー

組織は、

(a) 情報システムを［指定：組織が定めた頻度で］レビューし、必要でなかったり、セキュアでない機能に、ポートプロトコル・サービスを特定するとともに、

(b) ［指定：組織が定めた情報システム内の必要でなかったり、セキュアでないとみなされた機能として、組織が定めたポート・プロトコル・サービス］を無効にする。

補足的ガイダンス：組織は、機能・ポート・プロトコルおよび／またはサービスの相対的セキュリティを判断するか、あるいは他のエンティティのアセスメント結果に基づいてそうしたセキュリティ判断を下す。Bluetooth、FTP、ピアツーピアのネットワークは、セキュアであるとは言えないプロトコルの例である。なお、関連するセキュリティ管理策は、AC-18・CM-7・IA-2のセキュリティ管理策である

(2) 最小機能 | プログラムの実行を阻止する

情報システムは、[選択（1つ以上）：[指定：組織が定めた、ソフトウェアプログラムの使用と制限に関するポリシー]・ソフトウェアプログラムの使用の諸条件を規定するルール]に従って、プログラムの実行を阻止する。

補足的ガイダンス：関連するセキュリティ管理策は、CM-8 および PM-5 である。

(3) 最小機能 | 登録要件への準拠

組織は、[指定：組織が定めた、機能、ポート、プロトコル、サービスの登録要件]への適合を確実なものとする。

補足的ガイダンス：組織は、登録プロセスを使用して、情報システムと、導入されている機能、ポート・プロトコル・サービスを管理・追跡・監視する。

(4) 最小機能 | 許可されていないソフトウェア / ブラックリスト化

組織は、

(a) [組織が定めた、その情報システム上での実行が許可されないソフトウェアプログラムの割り当て]を識別するとともに、

(b) 「例外を除きすべてを許可する」ポリシーを用いて、その情報システム上で許可されていないソフトウェアプログラムを実行できないようにするのに加えて、

(c) 許可されていないソフトウェアプログラムの一覧を[指定：組織が定めた頻度で]レビューし、更新する。

補足的ガイダンス：組織の情報システム上で実行することが許可されていないソフトウェアプログラムを識別するのに使用されるプロセスは、一般的に、ブラックリスト化と称されている。組織は、ホワイトリスト化（ブラックリスト化よりも強い）がソフトウェアプログラムの実行を制限するのに望ましいアプローチである場合には、拡張管理策の代わりに CM-7(5)の拡張管理策を実施してもよい。関連するセキュリティ管理策は、CM-6・CM-8・PM-5。

(5) 最小機能 | 許可されているソフトウェア / ホワイトリスト化

組織は、

(a) [指定：組織が定めた、その情報システム上での実行が許可されているソフトウェアプログラム]を識別するとともに、

(b) 「例外を除きすべてを許可しない」ポリシーを用いて、その情報システム上で許可されているソフトウェアプログラムを実行できるようにするのに加えて、

(c) 許可されているソフトウェアプログラムの一覧を[指定：組織が定めた頻度で]レビューのうえ更新する。

補足的ガイダンス：組織の情報システム上で実行することが許可されているソフトウェアプログラムを識別するのに使用されるプロセスは、一般的に「ホワイトリスト化」と称されている。ホワイトリスト化に加えて、組織は、例えば、暗号チェックサム、デジタル署名、またはハッシュ関数を使用して、ホワイトリスト化されたソフトウェアプログラムの完全性を検証することを検討する。ホワイトリスト化されたソフトウェアの検証は、実行に先立って、あるいはシステムの起動時に行われる。関連するセキュリティ管理策は、CM-2・CM-6・CM-8・PM-5・SA-10・SC-34・SI-7。

参考文献：DoD Instruction 8551.01

優先順位とベースライン管理策の割り当て:

P1	**低** CM-7	**中** CM-7 (1) (2) (4)	**高** CM-7 (1) (2) (5)

CM-8 情報システムコンポーネント一覧

セキュリティ管理策:組織は、

a. 以下を満たす、情報システムコンポーネント一覧を作成し、文書化する:
   1. 現行の情報システムを正確に反映する
   2. その情報システムの認可が出される範囲内に含まれる、すべてのコンポーネントを対象とする
   3. 追跡と報告に必要と考えられる詳細レベルになっている
   4. [指定:組織が定めた、情報システムコンポーネントの効果的な説明責任を果たすのに必要と考えられる情報]を含んでいる

b. 情報システムコンポーネント一覧を[指定:組織が定めた頻度で]レビューし、更新する。

補足的ガイダンス:組織は、組織のすべての情報システムのコンポーネントを対象にした、情報システムコンポーネント一覧を作成することを選択できる。そうした状況では、組織は最終的な一覧に、コンポーネントの適切な説明に必要なシステムに特化した情報(例:情報システムの関連付け、情報システムの所有者)が確実に含まれるようにする。情報システムコンポーネントの効果的な説明に必要であると考えられる情報には、例えば、ハードウェア一覧の明細、ソフトウェアライセンス情報、ソフトウェアバージョン番号、コンポーネントの所有者、そしてネットワークコンポーネントまたはデバイスの場合には、マシン名とネットワークアドレスがある。一覧の明細は、例えば、製造業者・デバイスタイプ・モデル・シリアル番号とともに、物理的な位置を含む。関連するセキュリティ管理策は、CM-2・CM-6・PM-5。

拡張管理策:

(1) 情報システムコンポーネント一覧 | インストール / 削除の際に更新する

組織は、コンポーネントのインストールや削除の際に、また、情報システムのアップデートの際に、その一環として情報システムコンポーネント一覧を更新する。

(2) 情報システムコンポーネント一覧 | 自動で維持管理する

組織は、情報システムコンポーネント一覧が最新で、完全で、正確で、かつ、すぐに利用できるようにするための自動化されたメカニズムを実施する。

補足的ガイダンス:組織は、可能な範囲で情報システム一覧を維持管理する。仮想マシンは未使用時にはネットワークから見えないため、モニタリングが困難になる。そうした場合には、組織は妥当なレベルまで一覧を最新に、かつ完全で正確になるようにする。この拡張管理策は、組織が情報システムコンポーネント一覧とベースライン構成活動を結び付けたいと考える場合には、CM-2(2)の拡張管理策を実施することで満たせるようになる。関連するセキュリティ管理策は、SI-7。

(3) 情報システムコンポーネント一覧 | 許可されていないコンポーネントを自動で検知する

組織は、

(a) 情報システム内に許可されてないハードウェアコンポーネント・ソフトウェアコンポーネント・ファームウェアコンポーネントが存在する場合に検知できる、自動化されたメカニズムを[指定:組織が定めた頻度で]使用する

(b) 許可されてないコンポーネントが検知された場合に、以下の措置を講じる:[選択(1つ以上):そうしたコンポーネントによるネットワークアクセスを無効にする・それらのコンポーネントを切り離す・[指定:組織が定めた職員または役職]に報告する]。

補足的ガイダンス：この拡張管理策は、許可されていないリモート接続および携帯機器のモニタリングと併せて適用される。許可されていないシステムコンポーネントのモニタリングは継続的に行うか、あるいは、システムの定期的なスキャンによってを実現できる。自動化されたメカニズムは情報システム内で実施されたり、その他個別のデバイス内で実施されたりする。分離の手段としては、例えば、許可されていない情報システムコンポーネントを別のドメインまたはサブネットに置く、そうしたコンポーネントを切り離す、などがある。この種のコンポーネントの切り離しは、一般的に「サンドボックス化」と称されている。関連するセキュリティ管理策は、AC-17・AC-18・AC-19・CA-7・SI-3・SI-4・SI-7・RA-5。

(4) 情報システムコンポーネント一覧 | 責任に関する情報

組織は、情報システムコンポーネント一覧の情報に、コンポーネントの管理に責任のある個人を[選択（1つ以上）：氏名・地位・役職]によって特定できる手段を含める。

補足的ガイダンス：情報システムコンポーネントの管理に責任のある個人を特定できれば、割り当てられたコンポーネントが適切に管理され、なんらかのアクションが必要な場合に、組織がそうした個人に連絡を取れるようになる（例：コンポーネントが違反／侵害の元となっていることが判明した場合、コンポーネントをリコール／交換する必要がある場合、コンポーネントを移動する必要がある場合）。

(5) 情報システムコンポーネント一覧 | コンポーネントの記載が重複しないようにする

組織は、情報システムの認可が出される範囲内のすべてのコンポーネントに関して、別の情報システムコンポーネント一覧にも重複して記載されていないことを確認する。

補足的ガイダンス：この拡張管理策は、相互接続されている大規模または複雑な情報システムにおいて、情報システムコンポーネントの説明が重複する問題に対処するためのものである。

(6) 情報システムコンポーネント一覧 | アセスメントされた設定 / 許可された逸脱

組織は、情報システムコンポーネント一覧に、アセスメントされたコンポーネントの設定と、現在の設定からの許可された逸脱を含める。

補足的ガイダンス：この拡張管理策は、組織が情報システムコンポーネントに対して定めた設定・要求されている設定を遵守しているかどうかを判断するために評価されたコンポーネント、定められた設定からの許可された逸脱に焦点を当てている。関連するセキュリティ管理策は、CM-2・CM-6。

(7) 情報システムコンポーネント一覧 | 集中型リポジトリ

組織は、情報システムコンポーネント一覧を一つの場所で管理するためのリポジトリを用意する。

補足的ガイダンス：組織は、組織のすべての情報システムのコンポーネントを対象とする、一つの場所で管理される情報システムコンポーネント一覧を実施することを選択できる。情報システムコンポーネント一覧用の集中型リポジトリは、組織のハードウェア資産、ソフトウェア資産、ファームウェア資産についての説明を効率化する機会を提供する。そうしたリポジトリは、また、侵害／セキュリティ侵害された、あるいはリスク軽減活動が必要なシステムコンポーネントの位置と、そうしたコンポーネントに責任のある個人を組織が迅速に特定できるようにする。組織は最終的な一覧に、コンポーネントの適切な説明に必要なシステムに特化した情報（例：情報システムの関連付け、情報システムの所有者）が確実に含まれるようにする。

(8) 情報システムコンポーネント一覧 | 位置を自動で追跡する

組織は、地理的な位置による情報システムコンポーネントの追跡を支援する、自動化されたメカニズムを使用する。

補足的ガイダンス：情報システムコンポーネントの位置を追跡するための自動化されたメカニズムを使用することにより、コンポーネント一覧が、より正確なものになる。そうした機能

は、また、侵害／セキュリティ侵害された、あるいはリスク軽減活動が必要なシステムコンポーネントの位置と、そうしたコンポーネントに責任のある個人を組織が迅速に特定できるようにする。

(9) 情報システムコンポーネント一覧 | システムにコンポーネントを割り当てる

組織は、

(a) 情報システムに[指定：組織が定めた、取得した情報システムコンポーネント]を割り当てる

(b) 上記の割り当てに関して、情報システムの所有者から承認を得る。

補足的ガイダンス：組織は、拡張管理策の対象となる情報システムコンポーネントを選択するための基準またはそうしたコンポーネントのタイプを決定する（例：マイクロプロセッサ・マザーボード・ソフトウェア・プログラマブル論理制御装置・ネットワーク装置）。関連するセキュリティ管理策は、SA-4。

参考文献：NIST Special Publication 800-128

優先順位とベースライン管理策の割り当て：

P1	**低** CM-8	**中** CM-8 (1) (3) (5)	**高** CM-8 (1) (2) (3) (4) (5)

CM-9 構成管理計画

セキュリティ管理策：組織は、

a. 役割、責任、構成管理プロセスおよび手順を記載している
b. システム開発ライフサイクル全体を通して構成品目を特定し、それらの構成品目の構成を管理するためのプロセスを規定している
c. 情報システムの構成品目を定めて、それらの構成品目を構成管理下に置いている
d. 構成管理計画を不正な開示や変更から保護している

の 4 つを満たす情報システムの構成管理計画を作成・文書化のうえ実施する。

補足的ガイダンス：構成管理計画は、構成管理ポリシーの要求事項を満たすものであり、個々の情報システムに合わせて調整される。計画は、システム開発ライフサイクルにおける活動を情報システムレベルで支援するために構成管理がどのように使用されるかを示す、詳細なプロセスと手順を定義する。構成管理計画は、通常はシステム開発ライフサイクルの開発／調達フェーズにおいて作成される。構成管理計画は、変更を変更管理プロセス内でどのように進めるか、設定項目とベースラインをどのように更新するか、情報システムコンポーネント一覧をどのように維持管理するか、開発環境、テスト環境、本番環境をどのように制御するか、主要ドキュメントをどのように作成・リリース・更新するかについて記述する。組織は構成管理計画が一貫性を持ってタイムリーに作成・実施されるよう、テンプレートを使用してもよい。そうしたテンプレートは、組織全体にわたる基本構成管理計画にもなる。その場合、システムごとに、計画のサブセットが実施される。構成管理承認プロセスは、情報システムに対して提案されている変更をレビューし承認することに責任のある、主要なマネジメント関係者と、それらのシステムに対する変更を実施する前にセキュリティ影響分析を行う職員を指定することを含む。構成品目とは構成管理下に置かれる、情報システムを構成する品目（ハードウェア・ソフトウェア・ファームウェア・ドキュメント）である。情報システムはシステム開発ライフサイクル全体を通して存続するため、新しい構成品目が特定されたり、既存の構成品目が構成管理から外されたりする。関連するセキュリティ管理策は、CM-2・CM-3・CM-4・CM-5・CM-8・SA-10。

拡張管理策:

(1) 構成管理計画 | 責任の割り当て

組織は、構成管理プロセスを策定する責任を、情報システムの開発に直接関与しない職員に割り当てる。

補足的ガイダンス:組織内に専任の構成管理チームがいない場合には、システム開発または統合に直接関与していない職員を使って構成管理プロセスを策定する任務が、システム開発者に課せられる場合がある。このような職務の分離は、情報システムの開発・統合プロセスと、構成管理プロセス間に十分なレベルの独立性を確立し、維持するのに役立ち、その結果、品質管理が容易になり、より効果的なモニタリングが可能になる。

参考文献:NIST Special Publication 800-128

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** CM-9	**高** CM-9

CM-10 ソフトウェアの使用制限

セキュリティ管理策:組織は、

a. 契約上の取り決めと著作権法に従って、ソフトウェアと関連ドキュメントを使用する
b. 数量のライセンスによって保護されるソフトウェアと関連ドキュメントの使用を追跡することによって、それらが複製されて販売されないようにする
c. ピアツーピアのファイル共有技術の使用を管理、文書化して、本機能が著作物の不正な配布・表示・実行・複製に使用されないようにする。

補足的ガイダンス:ソフトウェアライセンスの追跡は、組織のニーズに合わせて手動で(例:シンプルなスプレッドシート)、あるいは自動で(例:特殊な追跡用アプリケーション)実施される。関連するセキュリティ管理策は、AC-17・CM-8・SC-7。

拡張管理策:

(1) ソフトウェアの使用制限 | オープンソースソフトウェア

組織は、オープンソースソフトウェアの使用に関して、以下の制限を実施する:[指定:組織が定めた制限]。

補足的ガイダンス:オープンソースソフトウェアとは、ソースコード形式で入手可能なソフトウェアである。ソフトウェア権限の内、通常は著作権保持者が保持するものは、通常はソフトウェアライセンス契約のもとで提供され、各人がソフトウェアを研究・変更・改良することが許される。セキュリティの観点から見た、オープンソースソフトウェアの大きな利点は、組織がソースコードを検証できることである。しかしながら、オープンソースソフトウェアには、たとえば、そうしたソフトウェアの派生的な使用に対する制約など、さまざまなライセンス問題がある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** CM-10	**中** CM-10	**高** CM-10

CM-11 ユーザによるソフトウェアのインストール

セキュリティ管理策:組織は、

a. ユーザによるソフトウェアのインストールを管理するための[指定:組織が定めたポリシー]を確立する
b. ソフトウェアのインストールに関するポリシーを[指定:組織が定めた方法]で実施する
c. ポリシーの遵守を[指定:組織が定めた頻度で]モニタリングする。

補足的ガイダンス:必要な権限が与えられている場合、ユーザは組織の情報システムにソフトウェアをインストールすることができる。ソフトウェアのインストールに対する管理を維持するために、組織はソフトウェアのインストールに関して許可されているアクションと、禁止されているアクションを指定する。許可されているソフトウェアのインストールの例としては、既存のソフトウェアに対するアップデート/セキュリティパッチや、組織が承認している「アプリケーションストア」からアプリケーションをダウンロードすることがある。禁止されているソフトウェアのインストールの例としては、出所が不明な/疑わしいソフトウェアや、組織が悪質であると考えるソフトウェアがある。組織が選択するユーザによるソフトウェアのインストールを管理するためのポリシーは、組織によって策定される場合もあれば、外部組織によって提供される場合もある。ポリシーを実施する方法には、手続きによるもの(例:ユーザアカウントの定期的な検査)、自動化によるもの(例:組織の情報システムに対する設定)、あるいは、その両方がある。関連するセキュリティ管理策は、AC-3・CM-2・CM-3・CM-5・CM-6・CM-7・PL-4。

拡張管理策:

(1) ユーザによるソフトウェアのインストール | 不正なインストールが行われた場合の警告

情報システムは、ソフトウェアの不正なインストールが検知された場合に、[指定:組織が定めた職員または役職]に警告を発する。

補足的ガイダンス:関連するセキュリティ管理策は、CA-7・SI-4。

(2) ユーザによるソフトウェアのインストール | 特権ステータスを持たないユーザによるインストールを禁止する

情報システムは、明確な特権ステータスを持たないユーザによるソフトウェアのインストールを禁止する。

補足的ガイダンス:特権ステータスは、例えば、システムアドミニストレータの役割を果たすことによって得られる。関連するセキュリティ管理策:AC-6。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** CM-11	**中** CM-11	**高** CM-11

ファミリ:緊急時対応計画

CP-1　緊急時対応計画のポリシーと手順

セキュリティ管理策:組織は、

a. 以下を策定・文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的・適用範囲・役割・責任・経営コミットメントとともに組織間の調整およびコンプライアンスを取り扱う、緊急時対応計画のポリシー
   2. 緊急時対応計画のポリシーと関連する「緊急時対応計画」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. 緊急時対応計画のポリシーを[指定:組織が定めた頻度で]
   2. 緊急時対応計画の手順を[指定:組織が定めた頻度で]

補足的ガイダンス:このセキュリティ管理策は、CP ファミリ内の選択されたセキュリティ管理策と拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引きを反映する。組織レベルでのセキュリティプログラムの政策と手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現する事もできる。また、この手順は、一般的なセキュリティプログラムの一部として策定する事もできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で、鍵となる。関連するセキュリティ管理策:PM-9。

拡張管理策:なし

参考文献:Federal Continuity Directive 1・NIST Special Publications 800-12・NIST Special Publications 800-34・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** CP-1	**中** CP-1	**高** CP-1

CP-2　緊急時対応計画

セキュリティ管理策:組織は、

a. 以下を満たす、情報システムの緊急時対応計画を作成する:
   1. 極めて重要なミッション／業務機能と、関連する緊急時対応要件を明らかにする
   2. 復旧目標、復旧の優先順位、およびメトリクスを示す
   3. 緊急時対応における役割、責任、そうした役割と責任を割り当てられた個人と連絡先情報を示す
   4. 情報システムの途絶または侵害もしくは不具合が発生しても、極めて重要なミッション／業務機能を維持できるようにする
   5. 最初に計画・導入されているセキュリティ対策を低下させることなく、最終的に情報システムを完全復旧できるようにする
   6. [指定: 組織が定めた職員または役職]によってレビューされ、承認される
b. 緊急時対応計画のコピーを[指定:組織が定めた、主な緊急時対応要員(氏名や役割によって特定される)と、担当部署]に配布する

c. 緊急時対応計画に伴う活動とインシデント対応活動を調整する

d. 情報システムの緊急時対応計画を[指定:組織が定めた頻度で]レビューする

e. 組織、情報システム、またはシステムが稼働する環境の変化と、緊急時対応計画の導入時(または実施時もしくはテスト時)に発覚した問題に対処するために、緊急時対応計画を更新する

f. 緊急時対応計画の変更について、[指定:組織が定めた、主な緊急時対応要員(氏名や役割によって特定される)と担当部署]に報告する

g. 緊急時対応計画を不正な開示や変更から保護する。

補足的ガイダンス:情報システムの緊急時対応計画は、ミッション/業務機能を遂行できるよう業務を継続させるための、組織全般的なプログラムの一部である。緊急時対応計画は、情報システムが侵害された場合の、システムの復旧と、代替のミッション/業務プロセスの実施を取り扱う。緊急時対応計画の有効性は、そうした計画をシステム開発ライフサイクルのすべてのフェーズを通して考えることによって、最大限に引き出せる。ハードウェア開発、ソフトウェア開発、ファームウェア開発において緊急時対応計画を立てる事は、情報システムの耐性を実現するための効果的な手段となる。緊急時対応計画は、望まれるレベルの業務継続を達成するのにすべてのシステムが完全復旧する必要はない事から、組織の情報システムに求められる復旧の度合を反映したものとなる。情報システムの復旧目標は、該当する連邦法・大統領命令・指令政策・標準・規制・指針を反映する。情報システムの可用性に加えて、緊急時対応計画は、例えば、情報システムの機密性または完全性を損なわせる悪意のある攻撃など、ミッション/業務の有効性を低下させる他のセキュリティイベントにも対処する。緊急時対応計画に含まれるアクションには、例えば、順序正しい/正常なデグラデーション、情報システムのシャットダウン、手動モードへのフォールバック、代替の情報フロー、システムが攻撃を受けている場合に適用される運用モードがある。緊急時対応計画とインシデント対応活動を綿密に調整することによって、組織は必要な緊急時対応活動の準備を行い、セキュリティインシデント発生時に発動できるようになる。関連するセキュリティ管理策は、C-14・CP-6・CP-7・CP-8・CP-9・CP-10・IR-4・IR-8・MP-2・MP-4・MP-5・PM-8・PM-11。

拡張管理策:

(1) 緊急時対応計画 | 関連する計画との調整

組織は、緊急時対応計画の作成を、関連する計画に責任のある部署との間で調整する。

補足的ガイダンス:組織の情報システムの緊急時対応計画に関連する計画には、例えば、事業継続計画・災害復旧計画・政府存続計画・緊急時コミュニケーション計画・重要インフラ計画・サイバーインシデント対応計画・居住者非常時計画のほか、インサイダー脅威に対する実行計画がある。

(2) 緊急時対応計画 | 能力についての計画

組織は、緊急時の運用において情報処理、通信、環境支援に必要な能力が備わっている事を確実にするために、能力についての計画を立てる。

補足的ガイダンス:能力についての計画が必要な理由は、さまざまなタイプの脅威(例:自然災害、標的型サイバー攻撃)が、組織のミッション/業務機能を支援することを目的とした処理、通信、支援サービスの低下を招く可能性があるからである。組織は、緊急時には機能を低下させた運用となる事も想定し、能力についての計画の立てる際に、そうした低下を考慮する。

(3) 緊急時対応計画 | 極めて重要なミッション / 業務機能を再開する

組織は、緊急時対応計画が始動してから[指定:組織が定めた期間]内に、極めて重要なミッション/業務機能を再開するための計画を立てる。

補足的ガイダンス:組織は、この拡張管理策に記載されている緊急時対応計画に伴う活動を、例えば、ビジネスインパクト分析の一環としてなど、組織の事業継続計画の一環として

実施することを選択できる。極めて重要なミッション／業務機能の再開の期限は、情報システムとシステムを支えるインフラの途絶が、どれだけ深刻であるか寄る場合がある。関連するセキュリティ管理策は、PE-12。

(4) 緊急時対応計画 | すべてのミッション / 業務機能を再開する

組織は、緊急時対応計画が始動してから[指定：組織が定めた期間]内に、すべてのミッション／業務機能を再開するための計画を立てる。

補足的ガイダンス：組織は、この拡張管理策に記載されている緊急時対応計画に伴う活動を、たとえば、ビジネスインパクト分析の一環としてなど、組織の事業継続計画の一環として実施することを選択できる。すべてのミッション／業務機能の再開の期限は、情報システムとシステムを支えるインフラの途絶が、どれだけ深刻であるか寄る場合がある。関連するセキュリティ管理策は、PE-12。

(5) 緊急時対応計画 | 極めて重要なミッション / 業務機能を継続する

組織は、極めて重要なミッション／業務機能を業務の継続性を失わせることなく継続するための計画を立てて、一次処理拠点および／または一次保管拠点で情報システムが完全復旧するまで、そうした継続性を維持する。

補足的ガイダンス：組織は、この拡張管理策いる緊急時対応計画に伴う活動を、たとえば、ビジネスインパクト分析の一環としてなど、組織の事業継続計画の一環として実施する事を選択できる。緊急時対応計画の一部として組織が定めた一次処理拠点および／または一次保管拠点は、緊急時対応を伴う状況によって変化する（例：バックアップ拠点が一次拠点になる場合がある）。関連するセキュリティ管理策は、PE-12。

(6) 緊急時対応計画 | 代替処理 / 保管拠点

組織は、極めて重要なミッション／業務機能を業務の継続性を失わせることなく代替処理拠点および／または代替保管拠点に転送するための計画を立てて、一次処理拠点および／または一次保管拠点で情報システムが復旧するまで、そうした継続性を維持する。

補足的ガイダンス：組織は、この拡張管理策にいる緊急時対応計画に伴う活動を例えば、ビジネスインパクト分析の一環としてなど、組織の事業継続計画の一環として実施することを選択できる。緊急時対応計画の一部として組織が定めた一次処理拠点および／または一次保管拠点は、緊急時対応を伴う状況によって変化する（例：バックアップ拠点が一次拠点になる場合がある）。関連するセキュリティ管理策は、PE-12。

(7) 緊急時対応計画 | 外部サービスプロバイダとの調整

組織は、緊急時対応要件が満たされるよう、自組織の緊急時対応計画と、外部サービスプロバイダの緊急時対応計画を調整する。

補足的ガイダンス：組織の主要なミッション／業務機能を成功裏に実施するための組織の能力が、外部サービスプロバイダに依存する場合は、タイムリーで包括的な緊急時対応計画を作成することが、より困難になる。この状況では、組織が外部組織との間で緊急時対応計画に伴う活動を調整して、個々の計画に組織の全般的な緊急時対応ニーズが反映されるようにする。関連する管理策は、SA-9。

(8) 緊急時対応計画 | 極めて重要な資産を特定する

組織は、極めて重要なミッション／業務機能を支援する重要な情報システム資産を明確にする。

補足的ガイダンス：組織は、この管理策に記載されている緊急時対応計画に伴う活動を、例えば、ビジネスインパクト分析の一環としてなど、組織の事業継続計画の一環として実施することを選択できる。組織は、極めて重要な情報システム資産を明確にして、緊急時の運用においても組織のミッション／業務機能が引き続き実施されるよう、そうした資産に対して（日常的に実施されているセキュリティ対策／対策を上回る）追加のセキュリティ対策／対策を実施できるようにする。また、極めて重要な情報資産を明確にできれば、組織のリソー

スの優先順位付けが容易になる。極めて重要な情報システム資産は、技術的な側面と、動作的な側面を有する。技術的な側面には、例えば、IT サービス・情報システムコンポーネント・IT 製品・メカニズムがある。動作的な側面には、例えば、手続き（手動で実行されるオペレーション）や人員（技術的な対策を実施する個人および／または手動での手続きを実施する個人）がある。組織のプログラム保護計画は、極めて重要な資産を明確にするのを支援する。関連するセキュリティ管理策は、SA-14・SA-15。

参考文献：Federal Continuity Directive 1・NIST Special Publication 800-34

優先順位とベースライン管理策の割り当て：

P1	**低** CP-2	**中** CP-2 (1) (3) (8)	**高** CP-2 (1) (2) (3) (4) (5) (8)

CP-3 緊急時対応トレーニング

セキュリティ管理策：組織は、

a. 緊急時の役割または責任を担うことになる[指定：組織が定めた期間]内に

b. 情報システムに対する変更に伴い、必要になった場合

c. その後は[指定：組織が定めた頻度で]

情報システムのユーザに対して、割り当てられた役割と責任に応じた緊急時対応トレーニングを実施する。

補足的ガイダンス：組織が実施する緊急時対応トレーニングは、そうしたトレーニングが適切な内容と詳細レベルになるよう、組織の職員に割り当てられた役割と責任に応じたものでなければならない。例えば、一般ユーザであれば、緊急時の運用において、あるいは通常の職務に影響がある場合に、いつ、どこに報告すべきかを知っているだけで済む。システムアドミニストレータであれば、代替処理拠点および代替保管拠点においてどのようにして情報システムをセットアップするかについての追加のトレーニングが必要になる。また、管理者／シニアリーダーであれば、指定された遠隔地においてどのようにしてミッション遂行に不可欠な機能を実施するかについて、また、緊急時対応に関連する活動の調整を目的として、どのようにして他の政府機関との間でコミュニケーションを確立するかについての、特殊なトレーニングを受けることになるだろう。緊急時の役割／責任に応じたトレーニングは、緊急時対応計画に記載されている具体的な緊急時対応要件を反映する。関連するセキュリティ管理策は、AT-2・AT-3・CP-2・IR-2。

拡張管理策：

(1) 緊急時対応トレーニング | イベントのシミュレーション

組織は、危機的状況において職員が効果的に対応できるよう、緊急時対応トレーニングにイベントのシミュレーションを取り入れる。

(2) 緊急時対応トレーニング | 自動化されたトレーニング環境

組織は、より徹底した、より現実に即した、緊急時対応トレーニングの環境を提供する、自動化されたメカニズムを使用する。

参考文献：Federal Continuity Directive 1・NIST Special Publications 800-16・NIST Special Publications 800-50

優先順位とベースライン管理策の割り当て：

P2	**低** CP-3	**中** CP-3	**高** CP-3 (1)

CP-4　緊急時対応計画のテスト

セキュリティ管理策：組織は、

a. 情報システムの緊急時対応計画を［指定：組織が定めたテスト］を用いて［指定：組織が定めた頻度で］テストし、計画の有効性と、組織が計画を実施する準備が整っているかどうかを判断する

b. 緊急時対応計画のテスト結果をレビューする

c. 必要な場合、是正活動を実施する。

補足的ガイダンス：緊急時対応計画の有効性を判断し、計画の欠陥を特定するための緊急時対応計画のテスト方法には、例えば、実地訓練と机上訓練、チェックリスト、シミュレーション（平行した、完全な割り込み型の）、包括的な訓練がある。組織は、緊急時対応計画の緊急時対応要件に基づいてテストを実施することになるが、このテストには緊急時の運用に伴う組織の業務、資産、個人に対する影響の判断が含まれる。組織は是正活動の広さ、深さ、スケジュールを柔軟に、かつ自由裁量で決定できる。関連するセキュリティ管理策は、CP-2・CP-3・IR-3。

拡張管理策：

(1) 緊急時対応計画のテスト | 関連する計画との調整

組織は、緊急時対応計画のテストを、関連する計画に責任のある部署との間で、調整する。

補足的ガイダンス：組織の情報システムの緊急時対応計画に関連する計画には、たとえば、事業継続計画、災害復旧計画、政府存続計画、緊急時コミュニケーション計画、重要インフラ計画、サイバーインシデント対応計画、居住者非常時計画がある。この拡張管理策は、組織に対して、関連する計画を扱う部署を編成したり、そうした部署に特定の計画を割り当てることを要求するわけではない。しかしながら、そうした部署が、関連する計画に責任のある場合には、組織はそうした部署と連携しなければならない。関連するセキュリティ管理策は、IR-8・PM-8。

(2) 緊急時対応計画のテスト | 代替処理拠点

組織は、以下を目的として、代替処理拠点において緊急時対応計画をテストする:

(a) 緊急時対応要員に、代替処理拠点と利用可能なリソースに慣れさせる

(b) 緊急時の運用を支援するために、代替処理拠点に備わっている機能を評価する。

補足的ガイダンス：関連するセキュリティ管理策は、CP-7

(3) 緊急時対応計画のテスト | 自動でテストする

組織は、緊急時対応計画をより徹底的に、かつ、より効果的にテストするための、自動化されたメカニズムを使用する。

補足的ガイダンス：自動化されたメカニズムは、たとえば、以下を実施することにより、緊急時対応計画をより徹底的に、かつ、より効果的にテストできるようにする：①緊急時対応問題を、より完全にカバーする②より現実に即したテストシナリオとテスト環境を選択する③情報システムと支援されるミッションを効果的に重要視する。

(4) 緊急時対応計画のテスト | 完全な復旧 / 再構築

組織は、緊急時対応計画のテストに、情報システムを既知の状態に完全復旧し、再構築できるかどうかを含める。

補足的ガイダンス：関連するセキュリティ管理策は、CP-10 および SC-24。

参考文献：Federal Continuity Directive 1・FIPS Publication 199・NIST Special Publications 800-34・NIST Special Publications 800-84

優先順位とベースライン管理策の割り当て:

P2	**低** CP-4	**中** CP-4 (1)	**高** CP-4 (1) (2)

CP-5 緊急時対応計画の更新

[削除された:CP-2 に統合された]

CP-6 代替保管拠点

セキュリティ管理策:組織は、

a. 代替保管拠点を定める。これには、情報システムのバックアップ情報の保管と取り出しを許可するのに必要な契約が含まれる

b. 代替保管拠点において、一次保管拠点と同等の情報セキュリティ対策が実施されるようにする。

補足的ガイダンス:代替保管拠点は、一次保管拠点から地理的に離れた拠点である。代替保管拠点は、一次保管拠点が利用できない場合に、情報とデータの複製を維持管理する。代替保管拠点契約が扱う項目には、例えば、代替拠点における環境条件、アクセスルール、物理面と環境面での保護要件、バックアップ媒体の配布/回収の調整がある。代替保管拠点は緊急時対応計画に記載されている要求事項を反映するため、組織は情報システムの途絶、侵害、または不具合が発生しても、極めて重要なミッション/業務機能を維持できるようになる。関連するセキュリティ管理策は、CP-2・CP-7・CP-9・CP-10・MP-4。

拡張管理策:

(1) 代替保管拠点 | 一次拠点からの切り離し

組織は、同じ脅威に晒されるリスクを減らすために、一次保管拠点から離れた代替保管拠点を指定する。

補足的ガイダンス:代替保管拠点に影響を与える脅威は、通常、組織のリスクアセスメント計画に定義されていて、その例としては自然災害、構造上の欠陥、敵意を持ったサイバー攻撃、作為/不作為の誤りがある。組織は、懸念されるタイプの脅威に基づいて、一次保管拠点と代替保管拠点が、どれだけ離れていれば十分であるかについて判断する。敵意を持ったサイバー攻撃など、脅威のタイプによっては、2 つの拠点がどれほど離れているかは重要でない。関連するセキュリティ管理策は、RA-3。

(2) 代替保管拠点 | 目標復旧時間 / ポイント

組織は、目標復旧時間と目標復旧ポイントに従った復旧作業が容易になるよう、代替保管拠点の設定を行う。

(3) 代替保管拠点 | アクセスできなくなった場合

組織は、区域全体に及ぶ途絶または災害時に、代替保管拠点にアクセスできなることを想定し、これに伴う問題を特定し、明確な軽減活動について説明する。

補足的ガイダンス:区域全体に及ぶ途絶は、地理的範囲が広いタイプの途絶(例:ハリケーン、地域全体の停電)であり、そのような途絶であるか否かの判断は、リスクアセスメントの結果に基づいて組織が行う。明確な軽減活動は、例えば、以下を含む:①始めに指定された代替保管拠点においてアクセス問題が発生した場合に、他の代替保管拠点においてバックアップ情報を複製するあるいは②代替保管拠点への電子アクセスが途絶えた場合に、バックアップ情報を取り出せるようにするための、物理アクセスについて計画を立てる。関連するセキュリティ管理策は、RA-3。

参考文献:NIST Special Publication 800-34

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** CP-6 (1) (3)	**高** CP-6 (1) (2) (3)

CP-7 代替処理拠点

セキュリティ管理策:組織は、

a. 代替処理拠点を定める。これには、一次処理機能が利用できない場合に、[指定:組織が定めた、目標復旧時間と目標復旧ポイントに適合する期間]内に、[指定:組織が定めた、情報システムオペレーション]を移転・再開して、極めて重要なミッション／業務機能を遂行できるようにするための契約が含まれる

b. オペレーションを移転し再開するのに必要な機器や備品を代替処理拠点に配備して利用できるようにするか、あるいは、外部に委託してそうした配備が、組織が定めた転送／再開期限内に行われるようする

c. 代替処理拠点において、一次拠点と同等の情報セキュリティ対策が実施されるようにする。

補足的ガイダンス:代替処理拠点は、一次処理拠点から地理的に離れた拠点である。代替処理拠点は、一次処理拠点が利用できない場合に、処理能力を提供する。代替処理拠点契約が扱う項目には、例えば、代替拠点における環境条件、アクセスルール、物理面と環境面での保護要件、および職員の異動／割り当ての調整がある。代替処理拠点には、緊急時対応計画に記載されている要件を反映する要件が割り当てられるため、組織は情報システムの途絶、侵害、または不具合が発生しても、極めて重要なミッション／業務機能を維持できるようになる。関連するセキュリティ管理策は、CP-2・CP-6・CP-8・CP-9・CP-10・MA-6。

拡張管理策:

(1) 代替処理拠点 | 一次拠点からの切り離し

組織は、同じ脅威に対する脆弱さを減らすために、一次処理拠点から離れた代替処理拠点を指定する。

補足的ガイダンス:代替処理拠点に影響を与える脅威は、通常、組織のリスクアセスメント計画に定義されていて、その例としては自然災害、構造上の欠陥、敵意を持ったサイバー攻撃、作為／不作為の誤りがある。組織は、懸念されるタイプの脅威に基づいて、一次処理拠点と代替処理拠点が、どれだけ離れていれば十分であるかについて判断する。敵意を持ったサイバー攻撃など、脅威のタイプによっては、2 つの拠点がどれほど離れているかは重要でない。関連するセキュリティ管理策は、RA-3。

(2) 代替処理拠点 | アクセスできなくなった場合

組織は、区域全体に及ぶ途絶または災害が発生した場合に、代替処理拠点にアクセスできなくなることに伴う諸問題を特定し、明確な軽減活動について説明する。

補足的ガイダンス:区域全体に及ぶ途絶は、地理的範囲が広いタイプの途絶(例:ハリケーン、地域全体の停電)であり、そのような途絶であるか否かの判断は、リスクアセスメントの結果に基づいて組織が行う。関連するセキュリティ管理策:RA-3。

(3) 代替処理拠点 | サービス優先

組織は、組織の可用性に関する要求事項(目標復旧時間を含む)に従って、サービス優先に関する条項を含む、代替処理拠点契約を作成する。

補足的ガイダンス:サービス優先に関する合意は、組織が組織の可用性に関する要求事項と、代替処理拠点における情報資源の可用性に基づいて、優先付けされたサービスを受けられるようにするための、サービスプロバイダとの交渉による合意である。

(4) 代替処理拠点 | 使用のための準備

組織は、極めて重要なミッション／業務機能を支援する運用拠点として使用できる代替処理拠点を用意する。

補足的ガイダンス：そうした拠点を用意するステップには、例えば、代替処理拠点における情報システムコンポーネントの設定の際に、一次拠点におけるそうした設定に対する要求事項に適合する設定にすることや、必要不可欠な備品を用意し、物流に関する考慮がなされるようにすることがある。関連するセキュリティ管理策は、CM-2・CM-6。

(5) 代替処理拠点 | 同等の情報セキュリティ対策

[削除された：CP-7 に統合された]

(6) 代替処理拠点 | 一次拠点に戻れない

組織は、一次処理拠点に戻れなくなる状況を想定して、計画を立てて、備える。

参考文献：NIST Special Publication 800-34

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** CP-7 (1) (2) (3)	**高** CP-7 (1) (2) (3) (4)

CP-8 通信サービス

セキュリティ管理策：組織は、代替通信サービスを確立する。これには、一次処理拠点／一次保管拠点や代替処理拠点／代替保管拠点のいずれかにおいて一次通信能力が利用できない場合に、[指定：組織が定めた期間]内に、極めて重要なミッション／業務機能を支援する[指定：組織が定めた、情報システムオペレーション]を再開できるようにするための契約が含まれる。

補足的ガイダンス：このセキュリティ管理策は、一次処理拠点／一次保管拠点と代替処理拠点／代替保管拠点における通信サービス（データと音声）に適用される。代替通信サービスは、一次通信サービスが失われても、極めて重要なミッション／業務機能を維持できるといった緊急時対応計画内の継続要件を反映する。組織は、一次／代替拠点に対してそれぞれに異なる期間を指定できる。代替通信サービスには、例えば、地上通信の代わりに追加される、組織が用意する、または市販の地上回路／回線や衛星がある。組織は、代替通信の契約を結ぶ際には、可用性、サービスの質、アクセスなどの要素について検討する。関連するセキュリティ管理策は、CP-2・CP-6・CP-7。

拡張管理策：

(1) 通信サービス | サービス提供の優先順位

組織は、

(a) 組織は、組織の可用性に関する要求事項（目標復旧時間を含む）に従って、サービス優先に関する条項を含む一次／代替通信サービス契約を作成する

(b) 一次および／または代替通信サービスが電気通信事業者によって提供される場合に、国家安全保障の緊急時対応に使用されるすべての通信サービスに対して、通信サービス優先 (Telecommunications Service Priority) を要求する。

補足的ガイダンス：組織は、通信サービスプロバイダが他の組織に対しても、同様のサービス優先に関する条項に基づいてサービスを提供している場合には、ミッション／業務に対する影響について考慮する。

(2) 通信サービス | 単一障害点

組織は、一次通信サービスとの間で単一障害点が共有される可能性を減らすために、代替通信サービスを取得する。

(3) 通信サービス | 一次 / 代替プロバイダの分離

組織は、同じ脅威に晒されるリスクを減らすために、一次サービスプロバイダではないプロバイダから、代替通信サービスを取得する。

補足的ガイダンス：通信サービスに影響を与える脅威は、通常、組織のリスクアセスメント計画に定義されていて、その例としては自然災害、構造上の欠陥、敵意を持ったサイバー／物理攻撃、作為／不作為の誤りがある。組織は、たとえば、通信サービスプロバイダ間で共有されるインフラを最小限に抑えて、サービス間の地理的な距離を十分に確保することによって、脆弱さが共有されるリスクを減すことに努める。組織は、サービスプロバイダが、リスクアセスメントにおいてアセスメントされる分離ニーズを満たす代替通信サービスを提供できるのであれば、そのサービスプロバイダのみを使用することを検討してもよい。

(4) 通信サービス | プロバイダの緊急時対応計画

組織は、

(a) 一次／代替通信サービスプロバイダに対して、緊急時対応計画を立てることを要求する

(b) プロバイダの緊急時対応計画をレビューして、組織の緊急時対応要件を満たしているかを確認する

(c) プロバイダが緊急時対応テスト／トレーニングを実施しているのを示す証拠を、[指定：組織が定めた頻度で]得る。

補足的ガイダンス：プロバイダの緊急時対応計画のレビューでは、そうした計画の所有権がプロバイダにあることを考慮する。場合によっては、プロバイダの緊急時対応計画の概要だけでも、組織がレビュー要件を満たすのに十分な証拠になる。通信サービスプロバイダは、また、国土安全保障省、州政府、および地方政府と連携して、現行の災害復旧訓練に参加する場合がある。組織は、これらのタイプの活動を通じて、サービスプロバイダの緊急時対応計画のレビュー・テスト・トレーニングに関する証拠取得要件を満たすことができる。

(5) 通信サービス | 代替通信サービスのテスト

組織は、代替通信サービスを[指定：組織が定めた頻度で]テストする。

参考文献：NIST Special Publication 800-34・National Communications Systems Directive 3-10・ウェブサイト http://www.dhs.gov/telecommunications-service-priority-tsp

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** CP-8 (1) (2)	**高** CP-8 (1) (2) (3) (4)

CP-9 情報システムのバックアップ

セキュリティ管理策：組織は、

a. 情報システムに含まれるユーザレベルの情報のバックアップを[指定：組織が定めた、目標復旧時間と目標復旧ポイントに応じた頻度で]実施する

b. 情報システムに含まれるシステムレベルの情報のバックアップを[指定：組織が定めた、目標復旧時間と目標復旧ポイントに応じた頻度で]実施する

c. セキュリティ関連のドキュメントを含む、情報システムドキュメントのバックアップを[指定：組織が定めた、目標復旧時間と目標復旧ポイントに応じた頻度で]実施する

d. 保管拠点におけるバックアップ情報の機密性を完全性・可用性とともに保護する。

補足的ガイダンス:システムレベルの情報には、例えば、システム状態に関する情報、オペレーティングシステムおよびアプリケーションソフトウェア、ライセンスがある。ユーザレベルの情報は、システムレベルの情報以外のすべての情報である。情報システムのバックアップの完全性を保護するために組織が導入するメカニズムには、たとえば、電子署名や暗号学的ハッシュがある。伝送中のシステムバックアップ情報の保護に関しては、本管理策が扱う範囲外である。情報システムバックアップは、緊急時対応計画に記載されている要求事項と、情報のバックアップに関する組織の他の要求事項を反映する。関連するセキュリティ管理策は、CP-2・CP-6・MP-4・MP-5・SC-13。

拡張管理策:

(1) 情報システムのバックアップ | 信頼性 / 完全性の確認

組織は、バックアップ情報を[指定:組織が定めた頻度で]テストして、媒体の信頼性と情報の完全性を確認する。

補足的ガイダンス:関連するセキュリティ管理策は、CP-4。

(2) 情報システムのバックアップ | サンプルを使用して復旧されるかどうかをテストする

組織は、緊急時対応計画のテストの一環として、サンプルバックアップ情報を利用して、選択された情報システム機能が復旧されるかどうかをテストする。

補足的ガイダンス:関連するセキュリティ管理策は、CP-4

(3) 情報システムのバックアップ | 極めて重要な情報は、別の記憶装置に保管する

組織は、[指定:組織が定めた、極めて重要な情報システムソフトウェアと、その他のセキュリティ関連情報]のバックアップコピーを、稼働しているシステムとは異なる施設、または防火コンテナに保管する。

補足的ガイダンス:極めて重要な情報システムソフトウェアには、例えば、オペレーティングシステム、暗号鍵管理システム、侵入検知防止システムがある。セキュリティ関連情報には、例えば、組織が作成する、ハードウェアコンポーネント一覧、ソフトウェアコンポーネント一覧、ファームウェアコンポーネント一覧がある。代替保存拠点は、通常、組織にとっては別の保管場所となる。関連するセキュリティ管理策は、CM-2・CM-8。

(4) 情報システムのバックアップ | 不正な変更からの保護

[削除された:CP-9 に統合された]

(5) 情報システムのバックアップ | 代替保管拠点に転送する

組織は、情報システムのバックアップ情報を代替保管拠点に[指定:組織が定めた、目標復旧時間と目標復旧ポイントに応じた期間と転送速度で]転送する。

補足的ガイダンス:情報システムのバックアップ情報を代替保管拠点に転送する方法には、電子的に転送する、または記憶媒体に保存して物理的に発送するなどがある。

(6) 情報システムのバックアップ | 予備の二次システム

組織による情報システムのバックアップは、一次システムと同じ場所に設置されず、かつ、情報の喪失または稼働中止を引き起こすことなくアクティブにできる、予備の二次システテを維持管理することによって実現する。

補足的ガイダンス:関連するセキュリティ管理策:CP-7・CP-10

(7) 情報システムのバックアップ | 二重認証

組織は、[指定:組織が定めたバックアップ情報]の削除または破棄に対して二重認証を実施する。

補足的ガイダンス:二重認証は、バックアップ情報の削除または破棄が資格のある二人の個人によって実施されない限り、発生しないようにするのに役立つ。バックアップ情報を削

除／破棄する個人は、提案されている削除／破棄が組織のポリシーと手順に沿っているかどうかを判断するのに十分な、スキル／専門知識を有するものとする。二重認証は、「二人立会制御 (two-person control)」としても知られている。関連するセキュリティ管理策：AC-3・MP-2。

参考文献：NIST Special Publication 800-34

優先順位とベースライン管理策の割り当て：

P1	**低** CP-9	**中** CP-9 (1)	**高** CP-9 (1) (2) (3) (5)

CP-10 情報システムの復旧と再構成

管理策：組織は、情報システムの途絶、侵害、または不具合が発生した場合に、情報システムを既知の状態に復旧し、再構成できるようにする。

補足的ガイダンス：復旧とは、組織のミッション／業務機能を復旧するための、情報システムの緊急時対応計画に記載されている活動を実施することである。再構成は、復旧の後に行われ、組織の情報システムを完全に機能する状態に戻すための活動を含む。復旧および再構成作業は、ミッション／業務の優先順位、目標復旧ポイント／時間および再構成、緊急時対応計画に記載されている要求事項に適合する確立されたメトリクスを考慮する。再構成は、復旧作業中に必要であった暫定的な情報システム機能を無効にすることを含む。再構成は、また、完全に復旧された情報システム機能のアセスメント、継続的モニタリング活動の復旧、場合によっては情報システムの再認可、今後起こりうるシステムの途絶、侵害、または不具合に備えるための活動を含む。組織が使用する復旧／再構成のための機能には、自動化されたメカニズムによるものと、手作業によるものがある。関連する管理策：CA-2・CA-6・CA-7・CP-2・CP-6・CP-7・CP-9・SC-24。

拡張管理策：

(1) システムの復旧と再構成 | 緊急時対応計画のテスト

[削除された：CP-4 に統合された]

(2) 情報システムの復旧と再構成 | トランザクションの回復

情報システムは、トランザクションベースのシステムを対象に、トランザクションの回復を実施する。

補足的ガイダンス：トランザクションベースの情報システムには、例えば、データベース管理システムとトランザクション処理システムがある。トランザクションの回復を支援するメカニズムには、例えば、トランザクションのロールバックとトランザクションのジャーナル処理がある。

(3) 情報システムの復旧と再構成 | 補完的セキュリティ管理策

[削除された：調整プロセスで扱っている]

(4) 情報システムの復旧と再構成 | 期間内に復旧する

組織は、情報システムコンポーネントの既知の稼働状態を示す、構成管理下にあり、その完全性が保護されている情報を使用して、情報システムコンポーネントを［指定：組織が定めた復旧期間］内に復旧できるようにする。

補足的ガイダンス：情報システムコンポーネントの復旧は、例えば、コンポーネントを既知の稼働状態に戻すための再イメージングを含む。関連するセキュリティ管理策は、CM-2。

(5) 情報システムの復旧と再構成 | 障害迂回機能

[削除された：SI-13 に統合された]

(6) 情報システムの復旧と再構成 | コンポーネントの保護

組織は、バックアップや復旧がなされたハードウェア、ファームウェア、ソフトウェアを保護する。

補足的ガイダンス：バックアッや復旧がなされたハードウェアコンポーネント、ファームウェアコンポーネント、ソフトウェアコンポーネントの保護には、物理面と技術面の対策がある。バックアッや復旧がなされるソフトウェアには、例えば、ルーターテーブル、コンパイラ、セキュリティ関連のシステムソフトウェアがある。関連するセキュリティ管理策は、AC-3・AC-6・PE-3。

参考文献：Federal Continuity Directive 1・NIST Special Publication 800-34

優先順位とベースライン管理策の割り当て：

P1	**低** CP-10	**中** CP-10 (2)	**高** CP-10 (2) (4)

CP-11 代替通信プロトコル

セキュリティ管理策：情報システムは、ユーザが、業務の継続性を維持するための［指定：組織が定めた代替通信プロトコル］を使用できるようにする。

補足的ガイダンス：緊急時対応計画と、それらの計画に伴うトレーニングおよびテストには、組織の情報システムの耐性を向上させるための代替通信プロトコル機能も含める。代替通信プロトコルの例としては、TCP/IP バージョン 4 から TCP/IP バージョン 6 への切り替えがある。通信プロトコルを切り替えると、ソフトウェアアプリケーションに影響が生じる場合があるため、代替通信プロトコルを導入する前に、導入に伴う副次的な悪影響の分析が必要になる。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

CP-12 セーフモード

セキュリティ管理策：情報システムは、［指定：組織が定めた条件］に合う場合には、［指定：組織が定めた、セーフモード時の制約］が課せられるセーフモードに切り替わる。

補足的ガイダンス：例えば、軍事行動や武器システム、民間のスペースオペレーション、原子力発電所の運転、航空管制システムの運用（特にリアルタイムの運用環境）などの、極めて重要なミッション／業務機能を支援する情報システムの場合、組織がそれらのシステムが所定のセーフモードに切り替わることになる、特定の条件を指定する場合がある。セーフモードは自動あるいは手動でアクティブ化され、定められた条件に合う場合には、情報システムが実施できる活動またはオペレーションが限定される。制約には、例えば、特定の機能のみを限られた電力で、または低減された通信帯域幅で実施できるようにすることがある。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

CP-13 代替のセキュリティメカニズム

セキュリティ管理策:組織は、[指定:組織が定めたセキュリティ機能]を実施するための主な手段が利用できない場合、または侵害された場合に、それらのセキュリティ機能を満たすための[指定:組織が定めた、代替の、または補足的なセキュリティメカニズム]を実施する。

補足的ガイダンス:このセキュリティ管理策は、情報システムの耐性と緊急時対応計画／業務の継続性を支援する。ミッション／業務の継続性を確保するために、組織は代替のまたは補足的なセキュリティメカニズムを実施してもよい。これらのメカニズムは、一次的なメカニズムに比べて有効性が劣るかも知れない(例:使いやすさが劣る、拡張性が劣る、セキュリティ面で劣る)。しかしながら、これらの代替の／補足的なメカニズムをすぐに使用できれば、全般的なミッション／業務の継続性が向上する。そうでなければ、それらの機能を実施するための一次的な手段が復旧するまで組織の業務が縮小され、ミッション／業務の継続性に負の影響が及ぶ。そうした代替の能力を用意するのに必要な費用と労力を考慮すると、このセキュリティ管理策は、通常は、情報システム、システムコンポーネント、または情報システムサービスが提供するセキュリティ機能のうち、極めて重要な機能にのみ適用されるのだろう。たとえば、組織がリモート認証を安全に行うための標準的な手段として多要素トークンを使用していて、そうしたトークンが侵害された場合には、上級管理者とシステムアドミニストレータにワンタイムパッドを発行することが考えられる。関連するセキュリティ管理策は、CP-2。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:識別および認証

IA-1　識別および認証のポリシーと手順

セキュリティ管理策:組織は、

a. 以下を策定・文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 識別および認証のポリシーのうち、目的・適用範囲・役割・責任・経営コミットメント・(組織間の)調整・コンプライアンスに関するもの
   2. 識別および認証のポリシーと、関連する「識別および認証」管理策の実施を容易にするための手順
b. 以下の最新版をレビュー・更新する:
   1. 識別および認証のポリシーを[指定:組織が定めた頻度で]
   2. 識別および認証の手順を[指定:組織が定めた頻度で]

補足的ガイダンス:このセキュリティ管理策は、IA ファミリ内の選択されたセキュリティ管理策とこの拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連するセキュリティ管理策:PM-9。

拡張管理策:なし

参考文献:FIPS Publication 201・NIST Special Publications 800-12・NIST Special Publications 800-63・NIST Special Publications 800-73・NIST Special Publications 800-76・NIST Special Publications 800-78・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** IA-1	**中** IA-1	**高** IA-1

IA-2　識別および認証(組織的ユーザ)

セキュリティ管理策:情報システムは、組織的ユーザ(または組織的ユーザの代わりに稼働するプロセス)を一意に識別し認証する。

補足的ガイダンス:組織的ユーザは、職員、または組織が職員と同等のステータスを有するとみなす個人(例:受託者、客員研究員)を含む。このセキュリティ管理策は、以下を除くすべてのアクセスに適用される:①AC-14のセキュリティ管理策に明確に示されていて、文書化されるアクセスならびに②個人の認証ではなく、グループ認証を経て発生するアクセス。組織は、グループアカウント(例:共有される特権アカウント)を有する個人の一意的な識別や、個人の活動についての詳細な説明を要求できる。組織は、ユーザの身元の認証にパスワード・トークン・生体情報のいずれかを使用したり、多要素認証の場合には、それらの組み合わせを使用する。組織の情報システムに対するアクセスには、「ローカルアクセス」と「ネットワークアクセス」がある。ローカルアクセスは、組織の情報システムに対して、ユーザ(またはユーザの代わりに稼働するプロセス)がネットワークを介さずに直接接続する形式のアクセスである。ネットワークアクセスは、組織の情報システムに対して、ユーザ(またはユーザの代わりに稼働するプロセス)がネットワーク接続を介して接続する形式のアクセスである(すなわち、ローカルアクセスではない)。リモ

ートアクセスは、外部ネットワーク（例：インターネット）を介した通信を伴うネットワークアクセスである。内部ネットワークには、ローカルエリアネットワークや広域ネットワークなどがある。また、組織が管理するエンドポイントと組織が管理しないエンドポイント間のネットワーク接続のために暗号化された仮想プライベートネットワーク(VPN)を使用する場合は、ネットワークを通過する情報の機密性と完全性を保護する観点から、内部ネットワークとして扱われることがある。

組織は、組織の具体的な導入計画に沿ってHomeland Security Presidential Directive 12の要求事項を満たす事によって、この管理策の「識別および認証」に関する要求事項を満たす事ができる。多要素認証は、認証を実現するために2つ以上の異なる要素を必要とする。それらの要素は、以下のように定義される：①貴殿が知っている事（例：パスワード／暗証番号）②貴殿が持っているもの（例：暗号識別装置、トークン）あるいは③貴殿である事（例：生体情報）。アクセスを得る情報システムとは切り離されたデバイスを必要とする多要素ソリューションには、例えば、時間ベースの、またはチャレンジ・レスポンス方式の認証情報を提供するハードウェアトークンや、U.S. Government Personal Identity Verification カードやDoD共通アクセスカードなどのスマートカードがある。組織は情報システムレベルで（すなわち、ログオン時に）ユーザを識別し、認証する事に加えて、情報セキュリティを向上させるために必要に応じて、アプリケーションレベルの識別および認証メカニズムを実施する。組織的ユーザ以外のユーザに対する識別および認証に関する要求事項は、IA-8のセキュリティ管理策に記載されている。関連するセキュリティ管理策は、AC-2・AC-3・AC-14・AC-17・AC-18・IA-4・IA-5・IA-8。

拡張管理策：

(1) 識別および認証（組織的ユーザ）| 特権アカウントに対するネットワークアクセス

情報システムは、特権アカウントに対するネットワークアクセスに対して多要素認証を実施する。

補足的ガイダンス：関連するセキュリティ管理策：AC-6

(2) 識別および認証（組織的ユーザ）| 特権アカウントでないアカウントに対するネットワークアクセス

情報システムは、特権アカウントでないアカウントに対するネットワークアクセスに対して多要素認証を実施する。

(3) 識別および認証（組織的ユーザ）| 特権アカウントに対するローカルアクセス

情報システムは、特権アカウントに対するローカルアクセスに対して多要素認証を実施する。

補足的ガイダンス：関連するセキュリティ管理策：AC-6

(4) 識別および認証（組織的ユーザ）| 特権アカウントでないアカウントに対するローカルアクセス

情報システムは、特権アカウントでないアカウントに対するローカルアクセスに対して多要素認証を実施する。

(5) 識別および認証（組織的ユーザ）| グループ認証

組織は、グループオーセンティケータが使用される場合には、個人に対して個人用オーセンティケータによる認証経ることを要求する。

補足的ガイダンス：個人に対して個人用オーセンティケータを第二レベルの認証として使用することを要求することは、組織にとって、グループオーセンティケータの使用に伴うリスクを軽減するのに役立つ。

(6) 識別および認証（組織的ユーザ）| 特権アカウントに対するネットワークアクセス - 切り離されたデバイス

情報システムは、特権アカウントに対するネットワークアクセスに対して多要素認証を実施するが、その際、アクセスを得るシステムとは切り離されたデバイスであり、かつ[指定：組

織が定めた、メカニズムの強度に関する要件]を満たすデバイスによって、それらの要素の内の1つが提供されるようにする。

補足的ガイダンス:関連するセキュリティ管理策:AC-6

(7) 識別および認証(組織的ユーザ) | 特権アカウントでないアカウントに対するネットワークアクセス - 切り離されたデバイス

情報システムは、特権アカウントでないアカウントに対するネットワークアクセスに対して多要素認証を実施するが、その際、アクセスを得るシステムとは切り離されたデバイスであり、かつ[指定:組織が定めた、メカニズムの強度に関する要件]を満たすデバイスによって、それらの要素の内の1つが提供されるようにする。

(8) 識別および認証(組織的ユーザ) | 特権アカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性

情報システムは、特権アカウントに対するネットワークアクセスに関して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。

補足的ガイダンス:前回の認証メッセージをリプレイすることによって認証を成功裏に実施できない場合には、認証プロセスはリプレイ攻撃に耐えられるようでなければならない。リプレイ攻撃に対する耐性を実現するための技術には、例えば、トランスポート層セキュリティや、時間同期形式またはチャレンジ・レスポンス方式のワンタイムオーセンティケータなどの、ノンスまたはチャレンジを使用するプロトコルがある。

(9) 識別および認証(組織的ユーザ) | 特権アカウントでないアカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性

情報システムは、特権アカウントでないアカウントに対するネットワークアクセスに関して、リプレイ攻撃に対する耐性のある認証メカニズムを実施する。

補足的ガイダンス:前回の認証メッセージを記録/リプレイすることによって認証を成功裏に実施できない場合には、認証プロセスはリプレイ攻撃に耐えられるようでなければならない。リプレイ攻撃に対する耐性を実現するための技術には、例えば、トランスポート層セキュリティや、時間同期形式またはチャレンジ・レスポンス方式のワンタイムオーセンティケータなどの、ノンスまたはチャレンジを使用するプロトコルがある。

(10) 識別および認証(組織的ユーザ) | シングルサインオン

情報システムは、[指定:組織が定めた、一覧に記載されている情報システムアカウントおよびサービス]に対して、シングルサインオン機能を提供する。

補足的ガイダンス:シングルサインオンでは、ユーザが一度ログインすれば、複数の情報システムリソースにアクセスできるようになる。組織は、シングルサインオン機能がもたらすオペレーション上の効率性と、単一のオーセンティケータの漏えいが複数のシステムリソースに対するアクセスを許してしまうといったリスクの増加について考慮する。

(11) 識別および認証(組織的ユーザ) | リモートアクセス - 切り離されたデバイス

情報システムは、特権アカウントへのリモートアクセスと、特権アカウントでないアカウントへのリモートアクセスに対して多要素認証を実施するが、その際、アクセスを得るシステムとは切り離されたデバイスであり、かつ、[指定:組織が定めた、メカニズムの強度に関する要件]を満たすデバイスによって、それらの要素の内の1つが提供されるようにする。

補足的ガイダンス:特権アカウント/特権アカウントでないアカウントに対するリモートアクセスに対して多要素認証が実施される際に、アクセスを得る情報システムとは切り離されたデバイスによって、それらの要素の内の1つが提供されるのを要求する目的は、システムに保存されている認証情報が漏洩する可能性を減らすことにある。例えば、組織の情報システムに悪質コードを実装する敵対者は、システムに保存されているそうした認証情報を読み取って、許可されたユーザになりすます可能性がある。関連するセキュリティ管理策は、AC-6。

(12) 識別および認証（組織的ユーザ）| PIV クレデンシャルを受け入れる

情報システムは、PIV（Personal Identity Verification:個人の身元の確認）クレデンシャルを受け入れて、電子的に確認する。

補足的ガイダンス：この拡張管理策は、論理アクセス制御システム(LACS)と物理アクセス制御システム(PACS)を実施する組織に適用される。PIV クレデンシャルは、連邦政府機関によって発行されるクレデンシャルであり、FIPS Publication 201 と、関連するガイダンス文書に準拠する。OMB Memorandum 11-11 は、PIV クレデンシャルが連邦政府機関全体にわたって使用されるよう、連邦政府機関に対して HSPD-12 に規定されている要求事項を継続して満たすことを要求する。関連するセキュリティ管理策は、AU-2・PE-3・SA-4。

(13) 識別および認証（組織的ユーザ）| 帯域外認証

情報システムは、[指定：組織が定めた条件]のもとで[指定：組織が定めた帯域外認証]を実施する。

補足的ガイダンス：帯域外認証(OOBA)とは、2 つの異なる通信経路を使用して、情報システムにアクセスしようとするユーザまたはデバイスを識別し、認証することである。1 番目の経路（すなわち、帯域内経路）は、ユーザまたはデバイスを識別し、認証するのに使用され、通常は、この経路を通じて情報が流れる。2 番目の経路（すなわち、帯域外経路）は、本物であること、および／またはリクエストされたアクションを個別に検証するのに使用される。たとえば、ユーザがノートパソコンを使用して遠隔サーバーにアクセスしようとして、サーバーによる認証を受けて通過し、その通信経路を通じてサーバー側のなんらかのアクションをリクエストしたとする。続いて、サーバーはユーザの携帯電話に連絡を取り、そのアクションをリクエストしたかどうかを確認する。ユーザは、電話の相手に意図したアクションであることを伝えるか、あるいは電話で認証コードを入力する。このタイプの認証は、介入者攻撃が疑われる、または実際に行われている場合に、軽減策として組織が使用できる。アクティブにする条件には、例えば、不審な活動、新たな脅威の兆候または脅威レベルの上昇、リクエストされたトランザクションの対象である情報の影響レベルや分類レベルが含まれる。関連するセキュリティ管理策：IA-10, IA-11, SC-37。

参考文献：HSPD-12・OMB Memoranda 04-04・OMB Memoranda 06-16・OMB Memoranda 11-11・FIPS Publication 201・NIST Special Publications 800-63・NIST Special Publications 800-73・NIST Special Publications 800-76・NIST Special Publications 800-78・FICAM Roadmap and Implementation Guidance・ ウェブサイト http://idmanagement.gov

優先順位とベースライン管理策の割り当て：

P1	**低** IA-2 (1) (12)	**中** IA-2 (1) (2) (3) (8) (11) (12)	**高** IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

IA-3 デバイスの識別および認証

セキュリティ管理策：情報システムは、[指定：組織が定めた特定の、および／またはタイプのデバイス]に関して、[選択（1つ以上）：ローカル・リモート・ネットワーク]接続を確立する前に、それらのデバイスを一意に識別し、認証する。

補足的ガイダンス：デバイスごとの一意的な識別と認証を必要とする組織のデバイスは、タイプ別に、またはデバイス別に、あるいは タイプ／デバイスの組み合わせによって定義することができる。情報システムは、通常、ローカルエリアネットワークおよび／または広域ネットワーク上のデバイスを識別／認証する際に、デバイスの識別に使用される共有される既知情報（例：MAC（媒体アクセス制御） アドレスまたはTCP/IPアドレス)、または組織の認証ソリューション（例：IEEE 802.1xと拡張可能認証プロトコル(EAP)、EAP-トランスポート層セキュリティ認証が可能なRadiusサーバー、ケルベロス）を使用する。組織は、情報システムのセキュリティカテゴリに

応じて、認証メカニズムに求められる強度を決定する。このセキュリティ管理策を大規模に適用するのは困難であるため、組織にはこの機能をサポートする必要がある数（およびタイプ）のデバイスのみに、この管理策を適用することが推奨される。関連するセキュリティ管理策は、AC-17・AC-18・AC-19・CA-3・IA-4・IA-5。

拡張管理策:

(1) デバイスの識別および認証 | 暗号を用いた双方向認証

情報システムは、[指定:組織が定めた特定のデバイスおよび／またはタイプのデバイス]に関して、[選択（1つ以上）:ローカル・リモート・ネットワーク]接続を確立する前に、暗号を用いた双方向認証を使用して、それらのデバイスを認証する。

補足的ガイダンス:ローカル接続とは、ネットワークを介さずに情報をやりとりするデバイスとの接続である。ネットワーク接続とは、ネットワークを介して情報をやりとりするデバイスとの接続である（例:ローカルエリアネットワークや広域ネットワーク・インターネット）。リモート接続とは、外部ネットワークを介して情報をやりとりするデバイスとの接続である（例:インターネット）。双方向認証は、リスクが高い接続（例:リモート接続）を試みる上記以外のデバイスの身元を確認するための、より強力な保護対策となる。関連するセキュリティ管理策は、SC-8・SC-12・SC-13。

(2) デバイスの識別および認証 | 暗号を用いた双方向ネットワーク認証

[削除された:IA-3(1)に統合された]

(3) デバイスの識別および認証 | アドレスを動的に割り当てる

組織は、

(a) [指定:組織が定めたリース情報とリース期間]に沿ってデバイスに割り当てられる、リース情報とリース期間に対するアドレスの動的な割り当てを標準化する

(b) リース情報がデバイスに割り当てられる際に、情報を確認する。

補足的ガイダンス:DHCP サーバーから IP アドレスを貸与される DHCP 対応クライアントは、デバイスに対するアドレスの動的な割り当ての、典型的な例である。関連するセキュリティ管理策は、AU-2・AU-3・AU-6・AU-12。

(4) デバイスの識別および認証 | デバイス認証

組織は、デバイス認証(attestation)に基づいたデバイスの識別と認証が、[指定:組織が定めた構成管理プロセス]によって扱われるようにする。

補足的ガイダンス:デバイス認証とは、デバイスの構成と既知の稼働状態に基づいて、デバイスを識別し、認証することである。これは、そのデバイスの暗号学的ハッシュによって決定される場合がある。デバイス認証が識別と認証の手段である場合、デバイスに対するパッチの適用や更新が構成管理プロセスを介して安全に行われるようにすると同時に、他のデバイスの識別と認証を妨げることがないようにする。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** IA-3	**高** IA-3

IA-4 識別子の管理

セキュリティ管理策:組織は、

a. 個人・グループ・役割・デバイスのいずれかの識別子を割り当てることに関して、[指定:組織が定めた職員または役職]から許可を得る

b. 個人・グループ・役割・デバイスのいずれかを識別するための識別子を選択する

c. 個人・グループ・役割・デバイスのいずれか意図したものに対してに識別子を割り当てる

d. ［指定：組織が定めた期間］内は、識別子が再利用されるのを防止する

e. ［指定：組織が定めた、アクティブでない期間］が経過した識別子を無効にする。

の 5 つを実施することによって、情報システムの識別子を管理する。

補足的ガイダンス：一般的なデバイス識別子には、たとえば、MAC アドレス・IP アドレス・デバイスに特化したトークン識別子がある。個別の識別子の管理は、共有される情報システムアカウント（例：ゲストアカウントや匿名アカウント）には適用されない。通常、個別の識別子は、それらの個人に割り当てられた情報システムアカウントのユーザ名である。そうした場合、AC-2 のアカウント管理活動では、IA-4 のセキュリティ管理策が提供するアカウント名を使用することになる。このセキュリティ管理策は、情報システムアカウントとは関連しない場合もある個別の識別子（例：情報システムにアクセスしようとする者がバッジをかざす、バッジ読み取りシステムによってアクセスされる「物理面でのセキュリティ管理策」データベースにおいて使用されている識別子）にも対応する。識別子の再利用の防止とは、以前に使用された個人、グループ、役割、またはデバイスの識別子が、別の個人、グループ、役割、またはデバイスに割り当てられるのを防止することを意味する。関連するセキュリティ管理策は、AC-2・IA-2・IA-3・IA-5・IA-8・SC-37。

拡張管理策：

(1) 識別子の管理 | パブリック識別子をアカウント識別子として使用するのを禁止する

組織は、個別の電子メールアカウントのパブリック識別子を情報システムアカウント識別子として使用するのを禁止する。

補足的ガイダンス：電子メールアドレスの個人の識別子セクションなどの、なんらかのパブリック識別子を情報システムアカウント識別子として使用するのを禁止することで、敵対者にとっては、組織の情報システム上のユーザ識別子を推測するのが困難になる。関連するセキュリティ管理策は、AT-2。

(2) 識別子の管理 | 管理者による承認

組織は、個人の識別子を得るための登録プロセスに、管理者による承認が含まれることを要求する。

(3) 識別子の管理 | 複数の形態の証明書

組織は、個人の身元を証明する複数の形態の証明書を要求する。例えば、登録機関に提出される書証や、ドキュメントと生体情報の組み合わせを要求できる。

補足的ガイダンス：身元を証明する複数の形態の証明書を要求することは、個人が偽の身分証明書を使って身元を証明する可能性を減らしたり、少なくとも敵対者の作業要因を増やすことにつながる。

(4) 識別子の管理 | ユーザステータスを識別する

組織は、各人を一意に識別できるよう、識別子に［指定：組織が定めた、個人のステータスを示す特性］を含める形で管理する。

補足的ガイダンス：個人のステータスを示す特性には、例えば、契約社員や外国籍がある。具体的な特性によって個人のステータスを識別できれば、組織の職員と情報をやりとりする人々について、追加の情報が得られる。例えば、政府機関の職員であれば、電子メールのメッセージの送信先の一人が契約社員であることを事前に分かっていれば、そうした情報が役に立つだろう。関連するセキュリティ管理策は、AT-2。

(5) 識別子の管理 | 動的な管理

情報システムは、識別子を動的に管理する。

補足的ガイダンス：事前に登録されたユーザにアカウントを静的に割り当てる従来のアプローチとは対照的に、分散情報システム（サービス指向型アーキテクチャを含む）の多くは、今まで知られていなかったエンティティにランタイムで識別子を割り当てる方式に依存する。こうした状況では、組織は識別子を動的に割り当てるための準備をして、割り当てを実施する。識別子と、対応する認証情報が正しいかどうかを確認するために、適切な機関との間で事前に確立された信頼関係と信頼メカニズムは、極めて重要である。関連するセキュリティ管理策は、AC-16。

(6) 識別子の管理 | 組織を跨る管理

組織は、[指定：組織が定めた外部組織]と連携して、組織を跨いで識別子を管理する。

補足的ガイダンス：組織を跨いで識別子を管理することで、組織は情報の処理または保存もしくは伝送を伴う組織を跨る活動を実施する際に、個人・グループ・役割・デバイスを適切に識別できるようになる。

(7) 識別子の管理 | 本人による登録

組織は、個人の識別子を得るための登録プロセスを本人が直接、指定された登録機関に出向いて実施することを要求する。

補足的ガイダンス：本人が物理的に居合わせると同時に、指定された登録機関と実際に対面して手続きを行うため、本人による登録は、偽の識別子が発行される可能性を低減する。

参考文献：FIPS Publication 201・NIST Special Publications 800-73・NIST Special Publications 800-76・NIST Special Publications 800-78

優先順位とベースライン管理策の割り当て：

P1	**低** IA-4	**中** IA-4	**高** IA-4

IA-5 オーセンティケータの管理

セキュリティ管理策：組織は、

a. オーセンティケータの初回の配布の一環として、オーセンティケータを受け取る個人、グループ、役割、またはデバイスの身元を確認する
b. 組織によって定められるオーセンティケータの、初期の内容を定める
c. オーセンティケータのメカニズムの強度が、目的の用途を果たすのに十分であることを確認する
d. オーセンティケータの初回の配布時、オーセンティケータの紛失時／侵害発生時または損傷時、オーセンティケータの無効化時の管理手順を定めて、実施する
e. 情報システムをインストールする前に、オーセンティケータの初期の内容を変更する
f. オーセンティケータの最短／最長有効期間と、再利用の条件を定める
g. [指定：組織が定めた、オーセンティケータのタイプ別の期間]が経過したら、オーセンティケータを変更／リフレッシュする
h. オーセンティケータの内容を、不正な開示や変更から保護する
i. 個人に対して、オーセンティケータを保護するための具体的なセキュリティ対策を実施することを要求し、デバイスにも、そうした対策を実施させる
j. グループ／役割アカウントの構成員が変わった場合に、それらのアカウントのオーセンティケータを変更する

を実施することによって、情報システムのオーセンティケータを管理する。

補足的ガイダンス：個人用オーセンティケータには、例えば、パスワード、トークン、生体情報、PKI 証明書、および鍵カードがある。オーセンティケータの初期の内容は、現在の内容（例：初期パスワード）であり、オーセンティケータの内容についての要求事項（例：最短のパスワード長よりも長くする）とは相反する。多くの場合、開発者が情報システムコンポーネントを出荷する際には、初期インストールおよび設定を可能にするために、工場出荷時の認証情報になっている。デフォルトの認証情報は、多くの場合なじみ深く、見破られやすいため、大きなセキュリティリスクになる。個人用オーセンティケータを保護する必要性は、個人が所有するオーセンティケータであれば、PL-4 のセキュリティ管理策または PS-6 のセキュリティ管理策を実施することによって、また、組織の情報システムに保存されているオーセンティケータ（例：ハッシュ化または暗号化された状態で保存されているパスワード、管理者権限でアクセス可能な、暗号化された／ハッシュ化されたパスワードを含むファイル）であれば、AC-3、AC-6、SC-28 のセキュリティ管理策のそれぞれを実施することによって満たされる。情報システムは、オーセンティケータのさまざまな特性に対して組織が定めた設定と制約（たとえば、最短のパスワード長、パスワード構成、時間同期形式のワンタイムトークンの検証のための時間窓、生体認証の検証段階における許容される拒否回数を含む）によって、個人用オーセンティケータの管理を支援する。オーセンティケータを保護するために取れる具体的な措置には、例えば、個人用オーセンティケータの所有の維持や、個人用オーセンティケータを他の人と共有したり、他の人に貸したりしないこと、オーセンティケータの紛失、盗難、または侵害時に即座に報告することがある。オーセンティケータ の管理は、リモートメンテナンスなどに必要な一時アクセスを確保するためにオーセンティケータを発行することと、そうしたオーセンティケータが必要でなくなった場合に失効させる事を含む。デバイスのオーセンティケータには、例えば、証明書やパスワードがある。関連するセキュリティ管理策は、AC-2・AC-3・AC-6・CM-6・IA-2・IA-4・IA-8・PL-4・PS-5・PS-6・SC-12・SC-13・SC-17・SC-28。

拡張管理策：

(1) オーセンティケータの管理 | パスワードによる認証

パスワードによる認証が行われる場合、情報システムは:

(a) パスワードに関して、[指定：組織が定めた、大文字と小文字の区別、文字数、大文字と小文字と数字と特殊文字を組み合わせることに関する要求事項と、各タイプの最低限の要求事項]を課すことで、パスワードに最低限必要な複雑さを確保する

(b) 新しいパスワードが作成される際には、少なくとも以下の数の文字を変更させる：[指定：組織が定めた数]

(c) 暗号によって保護されたパスワードのみを保存・伝送する

(d) パスワードの最短／最長有効期間を[指定：組織が定めた最短／最長有効期間]に設定する

(e) 同じパスワードを[指定：組織が定めた数の]世代にわたって再利用するのを禁止する

(f) 永続的なパスワードにすぐに変更するのを条件に、システムへのログオン時に、一時的なパスワードを使用することを許可する。

補足的ガイダンス：この拡張管理策は、パスワードを個人用オーセンティケータまたはグループオーセンティケータとして使用する、個人に対する単一要素認証時に適用され、また、パスワードが多要素オーセンティケータの一部である場合にも、同様に適用される。この拡張管理策は、ハードウェアオーセンティケータのロックを解除するためにパスワードが使用される場合（例：PIVカード）には適用されない。そうしたパスワードメカニズムを実施する場合、この拡張管理策の要求事項のすべてが満たされることは保証されない。暗号によって保護されたパスワードには、例えば、パスワードを暗号化したものや、パスワードに一方向の暗号学的ハッシュを適用したものがある。変更文字数は、現在のパスワードの文字数に対して、いくつの文字を変更するかを示す。パスワードの有効期間についての制約は、一時的なパスワードには適用されない。組織は、パスワードに対する特定のブルートフォース

攻撃に対処するために、パスワードのソルト化を検討する。関連するセキュリティ管理策は、IA-6。

(2) オーセンティケータの管理 | 公開鍵基盤による認証

公開鍵基盤による認証が行われる場合、情報システムは:

(a) 認められているトラストアンカーまでの認証経路を確立し、妥当性を確認して、証明書のステータス情報も含めて、証明書を検証する

(b) 対応する秘密鍵に対するアクセスは、許可制にする

(c) 認証された ID と、個人またはグループのアカウントを対応付ける

(d) 取り消しに関するデータをローカルのキャッシュメモリーに保存して、ネットワーク経由で取り消しに関する情報にアクセスできない場合に、経路を見つけ出して、妥当性を確認できるようにする。

補足的ガイダンス:認証経路のステータス情報には、例えば、証明書の取り消し一覧、または証明書のステータスプロトコルレスポンスがある。PIV カードの場合、証明書が本物であるかどうかの確認は、Common Policy Root トラストアンカーまでの認証経路の確立と妥当性の確認(証明書ポリシーの処理を含む)を伴う。関連するセキュリティ管理策は、IA-6。

(3) オーセンティケータの管理 | 本人、または信任を得ている第三者による登録

組織は、[指定:組織が定めたタイプの、および/または特定のオーセンティケータ]を得るための登録プロセスを[選択:本人(または信任を得ている第三者)]が直接、[指定:組織が定めた職員または役職]の認可を受けた[指定:組織が定めた登録機関]にを出向いて実施することを要求する。

(4) オーセンティケータの管理 | パスワードの強度についての判断を自動で支援する

組織は、パスワードに含まれるオーセンティケータが、[指定:組織が定めた要求事項]を満たすのに十分な強度を有するかどうかを判断するための、自動化されたツールを使用する。

補足的ガイダンス:この拡張管理策は、推測されにくいパスワードの作成と、使用の前のそうしたパスワードの特性(例:複雑さ)に焦点を当てている。この拡張管理策は、IA-5(1)に規定されているように、組織の情報システによって実施される。関連するセキュリティ管理策は、CA-2・CA-7・RA-5。

(5) オーセンティケータの管理 | 出荷前にオーセンティケータを変更する

組織は、情報システムコンポーネントの開発者/インストールを行う者に対して、出荷/インストール前に一意のオーセンティケータを提供するか、あるいはデフォルトのオーセンティケータを変更することを要求する。

補足的ガイダンス:この拡張管理策は、組織が情報システムのインストール時にデフォルトのオーセンティケータを変更する必要性を拡張するものであり、システムコンポーネントの開発者/インストールを行う者に対して、出荷/インストール前に一意のオーセンティケータを提供するか、あるいはデフォルトのオーセンティケータを変更することを要求する。しかしながら、この拡張管理策は、通常は、市販の IT 製品の開発者には適用されない。一意のオーセンティケータを要求する旨は、情報システムまたはシステムコンポーネントを調達する際に組織が用意する調達ドキュメントに記載される場合がある。

(6) オーセンティケータの管理 | オーセンティケータの保護

組織は、そのオーセンティケータを使用してアクセスできる情報のセキュリティカテゴリに応じたレベルで、オーセンティケータを保護する。

補足的ガイダンス:情報システムが複数のセキュリティカテゴリに分類される情報を含む場合で、かつ、それらの分類間に信頼できる物理的な、あるいは論理的な分離がなされていない場合には、システムに対するアクセスを得るために使用されるオーセンティケータを、

そのシステム上の情報のセキュリティカテゴリの内、最も高いものに相応するレベルで保護する。

(7) オーセンティケータの管理 | 暗号化されていない静的なオーセンティケータの埋め込みを禁止する

組織は、暗号化されていない静的なオーセンティケータが、アプリケーションまたはアクススクリプトに埋め込まれていないように、あるいはファンクションキーに記憶されていないようにする。

補足的ガイダンス：組織が、埋め込まれている／記憶されているオーセンティケータが暗号化されているか、それとも暗号化されていないかを判断する際には、注意が必要である。オーセンティケータが記憶された状態で使用される場合には、それらは暗号化されていないオーセンティケータとみなされる。このことは、何か他のもの（例：パスワード）が暗号化されている場合であっても同じである。

(8) オーセンティケータの管理 | 複数の情報システム上のアカウント

組織は、個人が複数の情報システム上のアカウントを有することに起因する、侵害のリスクを管理するために、[指定：組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス：個人が複数の情報システム上でアカウントを有する場合、個人が同じオーセンティケータを使用していると、1 つのアカウントの侵害がその他のアカウントの侵害につながるリスクがある。代替策として考えられるのは、たとえば、以下がある：①すべてのシステム上でそれぞれに異なるオーセンティケータを使用する②なんらかの形式のシングルサインオンメカニズムを使用する③すべてのシステム上でなんらかの形式の使い捨てパスワードを使用する。

(9) オーセンティケータの管理 | 組織を跨いで認証情報を管理する

組織は、[指定：組織が定めた外部組織]と連携して、組織を跨いで認証情報を管理するを行う。

補足的ガイダンス：組織を跨いで認証情報を管理することにより、組織は情報の処理または保存もしくは伝送を伴う、組織を跨る活動を実施する際に、個人・グループ・役割・デバイスを適切に認証できるようになる。

(10) オーセンティケータの管理 | 認証情報を動的に関連付ける

情報システムは、動的に識別情報を発行する。

補足的ガイダンス：認証では、識別情報と、識別情報を確認するのに使用されるオーセンティケータを、なんらかの形式で結び付けることが必要になる。従来のアプローチでは、情報システムに対して、識別情報とオーセンティケータの両方をあらかじめ用意することによって、この結び付けがなされていた。例えば、ユーザ名（すなわち、識別情報）とパスワード（すなわち、オーセンティケータ）の結び付けは、情報システムに対して識別情報とオーセンティケータをペアにして用意する事によって実現される。最近の認証技術では、識別情報とオーセンティケータの結び付けを情報システムの外側で実施することが可能である。たとえば、スマートカードの場合、識別情報とオーセンティケータが一体となってカード上に記憶されている。これらの認証情報を使用すれば、情報システムはあらかじめ用意されているわけではない識別情報を認証し、認証後に正式な識別情報を動的に用意することが可能になる。こうした状況では、識別情報を動的に用意するための準備が必要になる。識別情報と、対応する認証情報が正しいかどうかを確認するために、適切な機関との間で事前に確立された信頼関係と信頼メカニズムは極めて重要である。

(11) オーセンティケータの管理 | ハードウェアトークンによる認証

情報システムは、ハードウェアトークンによる認証が行われる場合には、[指定：組織が定めた、トークンの質に関する要求事項]を満たすメカニズムを使用する。

補足的ガイダンス：ハードウェアトークンによる認証は、通常、米国政府の PIV カードなどの、PKI ベースのトークンを使用することを意味する。組織は、特定の PKI と連携するなどの、トークンに関する具体的な要求事項を定める。

(12) オーセンティケータの管理 | 生体認証

情報システムは、生体認証が行われる場合には、[指定：組織が定めた、生体の質に関する要求事項]を満たすメカニズムを使用する。

補足的ガイダンス：パスワードによる認証では、ユーザが入力したパスワードと、記憶されているパスワードとが完全に一致するかを確認するのに対し、生体認証では、そうした完全な一致は保証されない。生体情報のタイプや収集メカニズムのタイプによっては、提示される生体情報と、比較のベースになる記憶されている生体情報との間になんらかの相違が生じる可能性が高い。そうした比較を行うと、認証が誤って通ってしまったり、誤って通らなかったりする。他人許容率と本人拒否率が等しくなる率は、「交叉率」として知られている。生体の質に関する要求事項には、例えば、生体情報の正確さを反映する許容交叉率が含まれる。

(13) オーセンティケータの管理 | キャッシュされたオーセンティケータの期限切れ

情報システムは、キャッシュされたオーセンティケータが[指定：組織が定めた期間]を過ぎたら、使用を禁止する。

(14) オーセンティケータの管理 | PKI トラストストアの内容の管理

組織は、PKI による認証を行う場合には、ネットワーク、オペレーティングシステム、ブラウザー、アプリケーションを含む、すべてのプラットフォームにインストールされている PKI トラストストアの内容を管理するために熟考された、組織全体にわたる方法を用いる。

(15) オーセンティケータの管理 | FICAM 認定の製品およびサービス

組織は、FICAM 認定の経路検出・検証用製品およびサービス以外は使用しない。

補足的ガイダンス：FICAM (Federal Identity, Credential, and Access Management) 認定の経路検出・検証用製品およびサービスは、適用できる場合に、FICAM 適合性評価を通じて認定された製品およびサービスである。

参考文献：OMB Memoranda 04-04・OMB Memoranda 11-11・FIPS Publication 201・NIST Special Publications 800-73・NIST Special Publications 800-63・NIST Special Publications 800-76・NIST Special Publications 800-78・FICAM Roadmap and Implementation Guidance・ウェブサイト http://idmanagement.gov

優先順位とベースライン管理策の割り当て：

P1	**低** IA-5 (1) (11)	**中** IA-5 (1) (2) (3) (11)	**高** IA-5 (1) (2) (3) (11)

IA-6 オーセンティケータのフィードバック

セキュリティ管理策：情報システムは、認証プロセス時に認証情報のフィードバックを見えないようにすることによって、認証情報が権限のない個人によって悪用／利用されないようにする。

補足的ガイダンス：情報システムからのフィードバックには、権限のない個人による、認証メカニズムの侵害を許してしまうような情報は含めないようにする。情報システムまたはシステムコンポーネントのタイプによっては、例えば、モニターが比較的大きいデスクトップ／ノートパソコンの場合には、（ショルダーサーフィンと称されることが多い）脅威が深刻である。一方で、その他のタイプのシステムまたはコンポーネント、例えば、画面の大きさが 2 ないし 4 インチの携帯機器では、そうした脅威はさほど深刻ではないが、キーボードが小さいが故に入力エラーの可能性が高まることとのバランスを考慮する必要がある。したがって、オーセンティケータのフィード

バックを見えなくする手段は、それぞれのタイプに応じて選択される。認証情報のフィードバックを見えなくする手段には、例えば、ユーザが入力装置に入力するパスワードをアスタリスクで表示することや、フィードバックは完全に見えなくする前の、極めて限られた時間しか表示しないことがある。関連するセキュリティ管理策:PE-18。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** IA-6	**中** IA-6	**高** IA-6

IA-7 暗号モジュールの認証

セキュリティ管理策:情報システムは、暗号モジュールに対する認証を扱う連邦法・大統領命令・指令・政策・規制・標準・手引が規定する要求事項を満たす認証メカニズムを実施する。

補足的ガイダンス:暗号モジュールに対しても、モジュールにアクセスするオペレータを認証し、そのオペレータが必要な役割を担い、その役割の範囲内でサービスを実施することを許可されている事を確認するためにも、認証メカニズムが必要になる。関連するセキュリティ管理策は、SC-12, SC-13。

拡張管理策:なし

参考文献:FIPS Publication 140・ウェブサイト http://csrc.nist.gov/groups/STM/cmvp/index.html

優先順位とベースライン管理策の割り当て:

P1	**低** IA-7	**中** IA-7	**高** IA-7

IA-8 識別および認証(組織的ユーザ以外のユーザ)

セキュリティ管理策:情報システムは、組織的ユーザ以外のユーザ(または組織的ユーザ以外のユーザの代わりに稼働するプロセス)を一意に識別のうえ認証する。

補足的ガイダンス:組織的ユーザ以外のユーザには、IA-2に記載されている組織的ユーザ以外の、情報システムユーザが含まれる。これらの個人は、AC-14に記載されているアクセス以外のアクセスのために、一意に識別・認証される。電子認証電子政府イニシアチブに従って連邦政府の情報システムにアクセスする、組織的ユーザ以外のユーザの認証では、(国家安全保障に関わるシステムが扱う情報を除く)連邦情報、機密情報、またはプライバシーに関わる情報を保護する必要がある。組織はリスクアセスメントを通じて認証ニーズを決定し、拡張性、実用性、セキュリティを考慮しながら、連邦情報と情報システムにアクセスする際の使いやすさを確保する必要性と、それらの情報とシステムを保護し、リスクを十分に軽減する必要性とのバランスをとる。IA-2は、情報システムにアクセスしようとする、組織的ユーザの識別および認証についての要求事項を規定している。関連するセキュリティ管理策は、AC-2・AC-14・AC-17・AC-18・IA-2・IA-4・IA-5・MA-4・RA-3・SA-12・SC-8。

拡張管理策:

(1) 識別および認証 | 他の政府機関からの PIV クレデンシャルを受け入れる

情報システムは、他の連邦政府機関からの PIV クレデンシャルを受け入れて、電子的に検証する。

補足的ガイダンス:この拡張管理策は、論理アクセス制御システム(LACS)と物理アクセス制御システム(PACS)に適用される。PIV クレデンシャルは、連邦政府機関によって発行さ

れるクレデンシャルであり、FIPS Publication 201 と、関連するガイダンス文書に準拠する。OMB Memorandum 11-11 は、PIV クレデンシャルが連邦政府機関全体にわたって使用されるよう、連邦政府機関に対して HSPD-12 に規定されている要求事項を継続して満たすことを要求する。関連するセキュリティ管理策は、AU-2・PE-3・SA-4。

(2) 識別および認証 | 第三者クレデンシャルを受け入れる

情報システムは、FICAM 認定の第三者クレデンシャルのみを受け入れる。

補足的ガイダンス：この拡張管理策は、通常、一般の人々がアクセスできる組織の情報システム（たとえば、一般向けに提供されているウェブサイト）に適用される。第三者クレデンシャルは、FICAM トラストフレームワークソリューションイニシアチブによって認可された、非連邦政府機関によって発行されるクレデンシャルである。認可された第三者クレデンシャルは、連邦政府全体にわたる技術面、セキュリティ面、プライバシー面での最低限の要求事項と、組織の成熟度に関する最低限の要求事項を満たす（あるいは上回る）。これは、連邦政府が信頼する関係者が、彼らが認める保証レベルが確保されるのであれば、そうしたクレデンシャルを信頼できるようにする。関連するセキュリティ管理策は、AU-2。

(3) 識別および認証 | FICAM 認定の製品を使用する

組織は、第三者クレデンシャルを受け入れるにあたって、[指定：組織が定めた情報システム]に、FICAM 認定の情報システムコンポーネントのみを使用する。

補足的ガイダンス：この拡張管理策は、通常は、一般向けに提供されているウェブサイトなどの、一般の人々がアクセスできる情報システムに適用される。FICAM 認定の情報システムコンポーネントには、たとえば、FICAM 適合性評価を通じて認可された IT 製品とソフトウェアライブラリがある。関連するセキュリティ管理策は、SA-4。

(4) 識別および認証 | FICAM 発行のプロファイルを使用する

情報システムは、FICAM 発行のプロファイルに準拠する。

補足的ガイダンス：この拡張管理策は、識別情報のオープンな管理規格を取り扱う。これらの規格が実行可能で、堅牢であり、信頼できて、枯渇することなく利用できる（例：市販の IT 製品から得られる）ものとなるように、また、記載どおりに相互運用可能なものとなるように、米国政府は識別情報管理規格および技術の実装を、該当する連邦法、指令、ポリシー、要求事項に照らし合わせて評価し、詳しく調べる。その結果として得られるのは、FICAM が発行する、認可されたプロトコル（例：SAML 2.0 や OpenID 2.0 などの FICAM 認証プロトコルや、FICAM Backend Attribute Exchange などの他のプロトコル）の実装プロファイルである。関連するセキュリティ管理策は、SA-4。

(5) 識別および認証 | PIV-I クレデンシャルを受け入れる

情報システムは、PIV-I クレデンシャルを受け入れて、電子的に確認する。

補足的ガイダンス：この拡張管理策は①論理アクセス制御システムと物理アクセス制御システムに適用される②米国政府の PIV 情報システムと相互運用されることを望んでいて、かつ、連邦政府が信頼する関係者から信頼されている、連邦政府以外の発行機関によって発行される ID カードを取り扱う。FBCA(Federal Bridge Certification Authority)に対する X.509 証明書ポリシーは、PIV-I の要求事項にも対応している。PIV-I カードは、OMB Memorandum 04-04 と NIST Special Publication 800-63 に定義されている「保証レベル 4」と、NIST Special Publication 800-116 に定義されている多要素認証に適している。PIV-I クレデンシャルは、自社の PIV-I 証明書ポリシーが Federal Bridge PIV-I Certificate Policy に適合する PIV-I プロバイダが発行する、クレデンシャルである。PIV-I プロバイダは FBCA との間で（直接、または別の PKI ブリッジを介して）相互認証されるが、その際に適用されるポリシーは、FBCA 証明書ポリシーに定められている PIV-I ポリシーの要求事項を満たすものとして対応付けられ、承認されたポリシーである。関連するセキュリティ管理策は、AU-2。

参考文献：OMB Memoranda 04-04・OMB Memoranda 11-11・OMB Memoranda 10-06-2011・FICAM Roadmap and Implementation Guidance; FIPS Publication 201; NIST Special Publications 800-63 NIST Special Publications 800-116・National Strategy for Trusted Identities in Cyberspace・ ウェブサイト http://idmanagement.gov

優先順位とベースライン管理策の割り当て：

P1	**低** IA-8 (1) (2) (3) (4)	**中** IA-8 (1) (2) (3) (4)	**高** IA-8 (1) (2) (3) (4)

IA-9 サービスの識別および認証

セキュリティ管理策：組織は、[指定：組織が定めたセキュリティ対策]を用いて、[指定：組織が定めた情報システムサービス]を識別・認証する。

補足的ガイダンス：このセキュリティ管理策は、情報システムサービスの識別と認証を必要とするサービス指向型アーキテクチャや、その他の分散型アーキテクチャのアプローチをサポートする。そうしたアーキテクチャでは、外部サービスが動的に出現することが多い。したがって、情報システムは、外部プロバイダおよび関連するサービスが本物であるかを動的に判断できなければならない。組織の情報システムがプロバイダとサービスが本物であるかどうかを確認するために実施する対策には、たとえば、情報またはコードの署名、来歴グラフ、および／またはサービスの供給元を示す、または含む電子署名がある。

拡張管理策：

(1) サービスの識別および認証 | 情報交換

組織は、サービスプロバイダが識別および認証情報を受け取り・確認のうえ、伝送できるようにする。

(2) サービスの識別および認証 | 判定の伝達

組織は、識別と認証に関する判定が、組織のポリシーに従って[指定：組織が定めたサービス]間で伝送されるようにする。

補足的ガイダンス：分散型アーキテクチャ（例：サービス指向型アーキテクチャ）の場合、掲示された識別・認証情報が正しいかどうかの判定は、本来それらの判定を行うサービスとは異なるサービスによって行われる場合がある。そうした状況では、識別と認証に関する判定が、本来それらの判定を行う必要があるサービスに伝達されなければならない（これは実際の識別と認証とは対照的である）。関連するセキュリティ管理策は、SC-8。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

IA-10 適応性のある識別および認証

管理策：組織は、情報システムにアクセスする個人に対して、[指定：組織が定めた状況]に当てはまる場合に、[指定：組織が定めた補足的な認証技術またはメカニズム]を使用することを要求する。

補足的ガイダンス：敵対者は、個別の認証メカニズムを侵害した後に、正規ユーザになりすます可能性がある。こうした状況は、組織が使用するあらゆる認証メカニズムで起こりうる。この脅威に対処するために、組織は特定の技術／メカニズムを使用して、不審な振る舞い（例：個人が通常の職務、役割、または責任の一環として通常はアクセスすることのない情報にアクセスする、個人が日常的にアクセスする情報よりも多くの情報にアクセスする、不審なネットワークアド

レスから情報にアクセスしようしている)をアセスメントするためのプロトコルを確立する。これらのように、あらかじめ定められた特定の条件またはトリガーが発生した場合には、組織が選択された個人に対して、追加の認証情報の提供を要求することができる。適応性のある識別および認証は、アクセスされるレコードの数および／またはタイプに応じて、メカニズムの強度を高めるために使用してもよい。関連するセキュリティ管理策は、AU-6・SI-4。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

IA-11 再認証

セキュリティ管理策:組織は、[指定:組織が定めた、再認証を必要とする状況]が発生した場合に、ユーザやデバイスに対して再認証を受けることを要求する。

補足的ガイダンス:セッションロックに伴う再認証に加えて、組織は、たとえば以下のようなその他の状況において、個人および／またはデバイスの再認証を必要とする:①オーセンティケータが変わった時②役割が変わった時③情報システムのセキュリティカテゴリが変わった時④特権的機能が実行された時⑤一定期間が過ぎた時⑤定期的に。関連するセキュリティ管理策は、AC-11。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:インシデント対応

IR-1　インシデント対応のポリシーと手順

セキュリティ管理策:組織は、

a. 以下を策定・文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメントを取り扱うとともに、組織間の調整およびコンプライアンスを取り扱うインシデント対応のポリシー
   2. インシデント対応のポリシーとともに、関連する「インシデント対応」管理策の実施を容易にするための手順

b. 以下の最新版をレビューし、更新する:
   1. インシデント対応のポリシーを[指定: 組織が定めた頻度で]
   2. インシデント対応の手順を[指定: 組織が定めた頻度で]

補足的ガイダンス:この管理策は、IR ファミリ内の選択されたセキュリティ管理策とこの拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で、鍵となる。関連するセキュリティ管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-61・NIST Special Publications 800-83・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** IR-1	**中** IR-1	**高** IR-1

IR-2　インシデント対応トレーニング

管理策:組織は、情報システムのユーザに対して、

a. インシデント対応に関わる役割または責任を担うことになる[指定:組織が定めた期間]内に

b. 情報システムに対する変更により、必要になった場合

c. その後は[指定:組織が定めた頻度で]

割り当てられた役割と責任に応じたインシデント対応トレーニングを実施する。

補足的ガイダンス:組織が実施するインシデント対応トレーニングは、そうしたトレーニングが適切な内容と詳細レベルになるよう、組織の職員に割り当てられた役割と責任に応じたものでなければならない。たとえば、一般ユーザであれば、情報システムにおけるインシデント発生時に誰に連絡するか、またはインシデントをどのように見分けるかを知るだけでよいのに対し、システムアドミニストレータであれば、インシデントにどのように対処する／インシデントをどのように解決するかについての追加のトレーニングが必要になる可能性がある。また、インシデントに対応する者であれば、科学捜査、報告、システムの復旧、再構築についての特殊なトレーニングを受けることになる可能性がある。インシデント対応トレーニングには、ユーザが内外からの不

審な活動を特定し、報告できるようにするための、ユーザトレーニングも含まれる。関連するセキュリティ管理策は、AT-3・CP-3・IR-8。

拡張管理策:

(1) インシデント対応トレーニング | イベントのシミュレーション

組織は、危機的状況において職員が効果的に対応できるよう、インシデント対応トレーニングにイベントのシミュレーションを取り入れる。

(2) インシデント対応トレーニング | 自動化されたトレーニング環境

組織は、より徹底した、より現実に即したインシデント対応トレーニング環境を提供する、自動化されたメカニズムを使用する。

参考文献:NIST Special Publications 800-16・NIST Special Publications 800-50

優先順位とベースライン管理策の割り当て:

P2	**低** IR-2	**中** IR-2	**高** IR-2 (1) (2)

IR-3 インシデント対応のテスト

セキュリティ管理策:組織は、[指定:組織が定めたテスト]を用いて、情報システムのインシデント対応能力を[指定:組織が定めた頻度で]テストし、インシデント対応の有効性を判断した後に、結果を文書化する。

補足的ガイダンス:組織は、インシデント対応能力をテストして、そうした能力の全般的な有効性を判断し、弱点または欠陥を特定する。インシデント対応テストには、たとえば、チェックリストの使用、実地訓練または机上訓練、シミュレーション(平行した、完全な割り込み型の)、包括的な訓練がある。インシデント対応のテストには、また、インシデント対応が組織の業務にもたらす影響(例:ミッション遂行能力の低下)と、組織の資産や個人にもたらす影響の判断も含まれる。関連するセキュリティ管理策は、CP-4・IR-8。

拡張管理策:

(1) インシデント対応のテスト | 自動でテストする

組織は、インシデント対応能力をより徹底的に、かつ、より効果的にテストするための、自動化されたメカニズムを使用する。

補足的ガイダンス:組織は、たとえば、以下を実施することにより、インシデント対応計画をより徹底的に、かつ、より効果的にテストすることを可能にする、自動化されたメカニズムを使用する:①インシデント対応問題を、より完全にカバーする②より現実に即したテストシナリオとテスト環境を選択するならびに③対応能力を重要視する。関連するセキュリティ管理策は、AT-2。

(2) インシデント対応のテスト | 関連する計画との調整

組織は、インシデント対応テストを、関連する計画に責任のある部署との間で調整する。

補足的ガイダンス:インシデント対応テストに関連する計画には、たとえば、事業継続計画、緊急時対応計画、災害復旧計画、政府存続計画、緊急時コミュニケーション計画、重要インフラ計画、居住者非常時計画がある。

参考文献:NIST Special Publications 800-84・NIST Special Publications 800-115

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** IR-3 (2)	**高** IR-3 (2)

IR-4　インシデント対応

管理策：組織は、

a. セキュリティインシデントに対応するための準備と、インシデントの検知および分析、封じ込め、根絶、復旧を含む、インシデント対応能力を備え

b. 緊急時対応計画に伴う活動とインシデント対応活動を調整する

c. インシデント対応活動から学んだ教訓をインシデント対応手順、トレーニング、テスト／訓練に取り入れて、結果として必要となる変更を実施する。

補足的ガイダンス：組織はインシデント対応能力は組織の情報システムの能力と、それらのシステムによって支援されるミッション／業務プロセスに左右されることを認識する。したがって、組織はインシデント対応をミッション／業務プロセスと情報システムの定義・設計・開発の一環としてとらえる。インシデント関連情報は、たとえば、監査モニタリング、ネットワークモニタリング、物理アクセスのモニタリング、ユーザ／アドミニストレータが作成したレポート、報告されたサプライチェーンイベントなど、さまざまな情報源から入手できる。効果的なインシデント対応能力は、組織内のさまざまな部署や人（たとえば、ミッション／業務遂行責任者・情報システム所有者・運用認可責任者・人事部法務部・業務職員・調達担当部署・リスクエグゼクティブ・リスクエグゼクティブ機能）とともに、職員による／物理的なセキュリティを担当する部署・）間の連携も含む。関連するセキュリティ管理策：AU-6・CM-6・CP-2・CP-4・IR-2・IR-3・IR-8・PE-6・SC-5・SC-7・SI-3・SI-4・SI-7。

セキュリティ管理策の拡張管理策：

(1) インシデント対応 | 自動化されたインシデント対応プロセス

組織は、インシデント対応プロセスを支援する自動化されたメカニズムを使用する。

補足的ガイダンス：インシデント対応プロセスを支援する自動化されたメカニズムには、たとえば、オンラインでのインシデント管理システムがある。

(2) インシデント対応 | 動的な再構成

組織は、インシデント対応能力に［指定：組織が定めた情報システムコンポーネント］の動的な再構成を含める。

補足的ガイダンス：動的な再構成には、たとえば、ルーターのルールの変更、アクセス制御リストの変更、侵入検知／防止システムのパラメータの変更、ファイアウォールやゲートウェイのフィルタールールの変更がある。組織は、たとえば攻撃を止めたり、攻撃者を誤った方向に向けたり、情報システムのコンポーネントを隔離して、違反または侵害による被害を抑えられるよう、情報システムの動的な再構成を実施する。組織は、高度なサイバー脅威に効果的に対処するための迅速な対応の必要性を考慮した上で、情報システムの再構成の達成期限を再構成の定義に含める。関連するセキュリティ管理策は、AC-2・AC-4・AC-16・CM-2・CM-3・CM-4。

(3) インシデント対応 | 業務の継続

組織は、組織のミッション／業務機能の継続を確保するために、［指定：組織が定めた類のインシデント］と［指定：組織が定めた類のインシデントに対して取るべきアクション］を明確にする。

補足的ガイダンス：上述の類のインシデントには、たとえば、設計／実装の誤りや漏れによる誤動作、標的型の悪意のある攻撃、非標的型の悪意のある攻撃がある。適切なインシデント対応活動には、たとえば、正常なデグラデーション、情報システムのシャットダウン、手動モード／代替技術へのフォールバックがある。フォールバックの場合、だましの対策、代替の情報フロー、またはシステムが攻撃を受けている場合にのみ適用される運用モードが実施されるため、システムの動作は、通常とは異なる。

(4) インシデント対応 | 情報を相互に関連付ける

組織は、インシデント情報と、個々のインシデント対応を相互に関連付けることによって、インシデント認識および対応に関する組織全体にわたる視点を持てるようにする。

補足的ガイダンス：脅威イベントの性質は、敵意を持ったサイバー攻撃など場合によっては、さまざまな情報源からの情報をまとめることによってのみ観測できる。そうした情報源は、さまざまな報告書と、組織が定めた報告手順を含む。

(5) インシデント対応 | 情報システムを自動で無効にする

組織は、[指定：組織が定めたセキュリティ違反]が発見された場合に情報システムを自動で無効にするための、設定可能な機能を実施する。

(6) インシデント対応 | インサイダー脅威 - 特定の能力

組織は、インサイダー脅威に対するインシデント対応能力を備える。

補足的ガイダンス：多くの組織がインサイダー脅威によるインシデントを組織のインシデント対応能力の一部ととらえて取り組んでいるが、この拡張管理策はこのタイプの脅威と具体的なインシデント対応能力の必要性（組織内で定義されているように）を改めて重要視し、適切かつタイムリーな対応を可能にする。

(7) インシデント対応 | インサイダー脅威 - 組織内の連携

組織は、インサイダー脅威に対するインシデント対応能力を[指定：組織が定めた、組織のコンポーネントまたはエレメント]間で連携させる。

補足的ガイダンス：インサイダー脅威によるインシデントに対するインシデント対応（準備、検知と分析、封じ込め、根絶、復旧を含む）は、組織のさまざまなコンポーネントまたはエレメント間の緊密な連携があって、初めて有効になる。これらのコンポーネントまたはエレメントには、たとえば、ミッション／業務遂行の責任者、情報システム所有者、人事部、調達担当部署、職員による／物理的なセキュリティを扱う部署、業務職員、リスクエグゼクティブ（機能）がある。また、組織は連邦・州・地方の法執行機関からの外部支援を必要とする場合がある。

(8) インシデント対応 | 外部組織と連携して相互に関連付ける

組織は、[指定：組織が定めた外部組織]と連携して、[指定：組織が定めたインシデント情報]を相互に関連付けて、共有することによって、インシデント認識に関して、組織を跨る視点を確立し、より効果的なインシデント対応を実現する。

補足的ガイダンス：例えば、ミッション／業務上のパートナー、軍事パートナー／連立相手、顧客、複層的な開発者などの外部組織との間でインシデント情報を共有することは、大きな利益をもたらす場合がある。インシデント対応のための組織を跨る連携は、重要なリスクマネジメント能力でもある。こうした能力が備われば、組織は、さまざまな情報源から得られる重要な情報を活用して、組織の業務、資産、個人に影響を与えうる情報セキュリティ関連インシデントに効果的に対処できるようになる。

(9) インシデント対応 | 動的に対応できる

組織は、セキュリティインシデントに効果的に対処するために[指定：組織が定めた動的な対応機能]を使用する。

補足的ガイダンス：この拡張管理策は、セキュリティインシデント（例：敵意を持ったサイバー攻撃時に敵対者が取るアクション）に対処するために、新しい機能または代替の機能をタイムリーに展開できるようにする。これには、ミッション／業務プロセスレベルで実施される機能（例：代替のミッション／業務プロセスをアクティブにする）と、情報システムレベルで実施される機能も含まれる。関連する管理策は、CP-10。

(10) インシデント対応 | サプライチェーンとの連携

組織は、サプライチェーンに関与する他の組織との間で、サプライチェーンイベントの対処を含む、インシデント対応活動を調整する。

補足的ガイダンス：サプライチェーン活動に関与する組織の例としては、システム／製品開発者・インテグレータ・製造業者・梱包業者・組み立て業者・販売業者・ベンダー・再販売業者が挙げられる。サプライチェーンインシデントには、たとえば、情報システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害がある。

参考文献：Executive Order 13587・NIST Special Publication 800-61

優先順位とベースライン管理策の割り当て：

P1	**低** IR-4	**中** IR-4 (1)	**高** IR-4 (1) (4)

IR-5 インシデントモニタリング

セキュリティ管理策：組織は、情報システムのセキュリティインシデントを追跡・文書化する。

補足的ガイダンス：情報システムのセキュリティインシデントを文書化することには、たとえば、それぞれのインシデントについての記録、インシデントのステータス、科学捜査に必要な関連情報を維持すること、インシデントの詳細、傾向、対処を評価することも含まれる。インシデント情報は、たとえばインシデントレポート、インシデント対応チーム、監査モニタリング、ネットワークモニタリング、物理アクセスのモニタリング、ユーザ／アドミニストレータが作成したレポートなど、さまざまな情報源から入手できる。関連する管理策は、AU-6・IR-8・PE-6・SC-5・SC-7・SI-3・SI-4・SI-7。

拡張管理策：

(1) インシデントモニタリング | 追跡 / データ収集 / 分析を自動で行う

組織は、セキュリティインシデントの追跡と、インシデント情報の収集および分析を支援する自動化されたメカニズムを使用する。

補足的ガイダンス：セキュリティインシデントの追跡と、インシデント情報の収集／分析のための自動化されたメカニズムには、たとえば、Einstein ネットワークモニタリング装置や、オンライン CIRCs (Computer Incident Response Centers)や、インシデント情報を提供する電子データベースを参照することがある。関連する管理策：AU-7・IR-4。

参考文献：NIST Special Publication 800-61

優先順位とベースライン管理策の割り当て：

P1	**低** IR-5	**中** IR-5	**高** IR-5 (1)

IR-6 インシデント報告

セキュリティ管理策：組織は、

a. 職員に対して、セキュリティインシデントの疑いがある場合に、[指定：組織が定めた期間]内に組織のインシデント対応チームに報告することを要求する

b. セキュリティインシデント情報を[指定：組織が定めた機関]に報告する。

補足的ガイダンス：この管理策の目的は、組織内のインシデント報告要件と、連邦政府機関と下部組織のフォーマルなインシデント報告要件の両方を満たすことにある。セキュリティインシデントの疑いがある場合とは、たとえば、悪質コードを含んでいる可能性のある疑わしい電子メ

ールを受け取った場合がある。報告されるセキュリティインシデントの種別、報告の内容と適時性、指定された報告先の機関は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。現行の連邦政府ポリシーは、すべての連邦政府機関（そうした要求事項から免除されることが明示されている場合を除く）に対して、セキュリティーインシデントに関する報告をUS-CERT Concept of Operations for Federal Cyber Security Incident Handling が規定する時間内に US-CERT に対して行うことを要求する。関連するセキュリティ管理策：IR-4・IR-5・IR-8。

拡張管理策：

(1) インシデント報告 | 自動で報告する

組織は、セキュリティインシデントの報告を支援する自動化されたメカニズムを使用する。

補足的ガイダンス：関連する管理策は、IR-7

(2) インシデント報告 | インシデントに関連する脆弱性

組織は、報告されたセキュリティインシデントに関連する情報システムの脆弱性を[指定：組織が定めた職員または役職]に報告する。

(3) インシデント報告 | サプライチェーンとの連携

組織は、セキュリティインシデント情報を、そのインシデントに巻き込まれた情報システムまたは情報システムコンポーネントの、サプライチェーンに関与する他の組織に提供する。

補足的ガイダンス：サプライチェーン活動に関与する組織の例としては、システム／製品開発者、インテグレータ、製造業者、梱包業者、組み立て業者、販売業者、ベンダー、再販売業者が挙げられる。サプライチェーンインシデントには、たとえば、情報システムコンポーネント、IT 製品、開発プロセスまたは開発者、流通過程または倉庫施設に対する侵害がある。組織が共有すべき適切な情報を決定する際には、外部組織によるサポートから得られる利点と、信頼性が疑わしい外部組織に機微な情報が開示されてしまうことによる被害を考慮する。

参考文献：NIST Special Publication 800-61・ウェブサイト http://www.us-cert.gov

優先順位とベースライン管理策の割り当て：

P1	**低** IR-6	**中** IR-6 (1)	**高** IR-6 (1)

IR-7 インシデント対応の支援

セキュリティ管理策：組織は、情報システムのユーザにセキュリティインシデントの対応と報告に関する助言と支援を提供する、組織のインシデント対応能力に不可欠な、インシデント対応支援リソースを用意する。

補足的ガイダンス：組織が用意するインシデント対応支援リソースには、たとえば、ヘルプデスク、支援グループ、科学捜査サービスの利用（必要な場合）がある。関連する管理策は、AT-2・IR-4・IR-6・IR-8・SA-9。

拡張管理策：

(1) インシデント対応の支援 | 情報 / 支援の可用性を自動で支援する

組織は、インシデント対応に関連する情報と支援の可用性を向上させるための、自動化されたメカニズムを使用する。

補足的ガイダンス：自動化されたメカニズムを通じて、ユーザが能動的に、および／または受動的にインシデント対応支援を得ることが可能になる。たとえば、個人がウェブサイトにアクセスして支援能力について問い合わせたり、反対に支援機能側から積極的にユーザに情報を配信して（通常の配信または的を絞った配信を通じて）、ユーザが現行の対応能力と支援について理解を深めるのを支援する、といったことが考えられる。

(2) インシデント対応の支援 | 外部プロバイダとの調整

組織は、

(a) 自組織のインシデント対応チームと、情報システムの保護機能を提供する外部プロバイダとの間で直接的な協力関係を築く

(b) 外部プロバイダに対して、自組織のインシデント対応チームのメンバーを明らかにする。

補足的ガイダンス：情報システムの保護機能を提供する外部プロバイダには、たとえば、米国防総省内の Computer Network Defense プログラムがある。外部プロバイダは、組織の情報システムとネットワーク内の許可されていない活動からの保護、そうした活動のモニタリング、分析、検知、そうした活動に対する対応を支援する。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P2	**低** IR-7	**中** IR-7 (1)	**高** IR-7 (1)

IR-8 インシデント対応計画

セキュリティ管理策：組織は、

a. 以下を満たすインシデント対応計画を作成する：
   1. 組織のインシデント対応機能を実施するためのロードマップを示す
   2. インシデント対応機能の構造と編成について記述する
   3. インシデント対応機能が組織全体にどのように適合するかについて、概要を示す
   4. 組織のミッション、規模、構造、機能に関する、組織の要求事項を満たす
   5. 報告義務のあるインシデントを定める
   6. 組織のインシデント対応機能を測定するためのメトリクスを示す
   7. インシデント対応機能を効果的に維持し、成熟させるのに必要なリソースと管理支援を定める
   8. [指定： 組織が定めた職員または役職]によってレビュー・承認される
b. インシデント対応計画のコピーを[指定：組織が定めた、インシデント対応要員（氏名および／または役割によって特定される）と部署]に配布する
c. インシデント対応計画を[指定：組織が定めた頻度で]レビューする
d. システム／組織の変化に対応するために、あるいは計画の導入、実施、またはテスト時に発見された問題に対処するために、インシデント対応計画を更新する
e. インシデント対応計画の変更について、[指定：組織が定めたインシデント対応要員（氏名および／または役割によって特定される）と部署]に報告する
f. インシデント対応計画を不正な開示や変更から保護する。

補足的ガイダンス：組織がインシデント対応の組織的なアプローチを策定して実施することは、重要である。インシデント対応機能の構造を決定する際には、組織のミッション、業務機能、戦略、目標、インシデント対応の目的を考慮することが一助となる。包括的なインシデント対応機能の一環として、組織は外部組織（たとえば、組織の情報システムのサプライチェーンに関与する外部サービスプロバイダや組織を含む）との連携と情報共有について検討する。関連する管理策は、MP-2・MP-4・MP-5。

拡張管理策：なし

参考文献：NIST Special Publication 800-61

優先順位とベースライン管理策の割り当て：

P1	**低** IR-8	**中** IR-8	**高** IR-8

IR-9 情報流出対応

セキュリティ管理策：組織は、

a. 情報システムの汚染に関わっている情報を特定する

b. 情報の流出が発生した場合に、流出とは無関係の伝達手段によって、[指定：組織が定めた職員または役職]に知らせる

c. 汚染された情報システムまたはシステムコンポーネントを隔離する

d. 汚染された情報システムまたはコンポーネントから情報を消し去る

e. その後に汚染された可能性のある他の情報システムまたはシステムコンポーネントを特定する

f. [指定：組織が定めた措置]を取る。

の 6 つを実施することによって情報の流出に対処する。

補足的ガイダンス：情報の流出とは、機密情報または機微な情報が、そうした情報を処理することが許可されていない情報システムに誤って置かれることである。そうした情報の流出は、機微度が初めは低いと思われたたが、後に高いことが判明することになる情報が、情報システムに伝送される場合に発生することが多い。そこで、是正処置が必要になる。組織の対応がどのようなものになるかは、通常は、流出した情報の機微度（例：セキュリティカテゴリまたは分類レベル）、その情報システムのセキュリティ能力、汚染された記憶媒体の性質、汚染されたシステムに対するアクセスが許可された個人のアクセス権限（例：セキュリティクリアランス）によって変わる。流出発生後に、流出に関する情報を伝達する手段は、そうした汚染が隔離され、根絶される前に汚染が広がるリスクを最小限にするためにも、実際の流出に直接関わる手段であってはならない。

拡張管理策：

(1) 情報流出対応 | 責任を割り当てられた職員

組織は、[指定：組織が定めた職員または役職]に対して、情報の流出に対処する責任を割り当てる。

(2) 情報流出対応 | トレーニング

組織は、情報の流出に対処するためのトレーニングを[指定：組織が定めた頻度で]実施する。

(3) 情報流出対応 | 流出後の活動

組織は、汚染されたシステムを修復する作業が行われている間に、情報流出の影響を受けた職員が割り当てられたタスクを引き続き実施できるようにするための、[指定：組織が定めた手順]を実施する。

補足的ガイダンス：情報の流出によって汚染された情報システムに対する修復作業は、非常に時間がかかる場合がある。職員は、そうした期間にわたって、汚染されたシステムにアクセスできず、彼らが業務を行う能力に影響が及ぶ可能性がある。

(4) 情報流出対応 | 権限のない職員に晒される

組織は、割り当てられたアクセス権限ではアクセスできない情報に、職員がアクセスできてしまう場合の対策として、[指定：組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス：セキュリティ対策には、たとえば、流出した情報にアクセスできてしまう職員に、その情報に関する連邦法・指令・政策（および／または規制）について、また、そうした情報にアクセスするのに課せられる制約について認識させることがある。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

IR-10 統合情報セキュリティ分析チーム

管理策：組織は、フォレンシックアナリスト／悪質コード解析者、ツール開発者、リアルタイムオペレーション要員から成る統合チームを設置する。

補足的ガイダンス：インシデント対応のための統合チームが備わっていれば、情報共有が容易になる。そうしたチームは、開発者、導入者、オペレータを含む組織の職員が、脅威に関するチームの知見を活用し、侵入をより効果的に防げる防御対策を実施できるようにする。また、侵入を迅速に検知し、適切な軽減措置を考案し、効果的な防御対策を実施できるようする。たとえば、侵入が検知された場合、統合セキュリティ分析チームは、オペレータが実施すべき適切な対応を迅速に考案し、新たに発生したインシデントを過去のインシデントに関する情報と関連付けて、現行の知能発達を補強することが可能である。これによりチームは、オペレーションのテンポまたは特定のミッション／業務機能に関連がある敵対者の戦術・技術・手順を特定し、ミッション／業務を中断させることのない対応措置を定義することが可能になる。理想としては、耐性を高めるために、組織内に複数の情報セキュリティ分析チームが配備されることが望ましい。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:メンテナンス

MA-1　システムメンテナンスのポリシーと手順

管理策:組織は、

a. 以下を策定・文書化のうえ、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、システムメンテナンスのポリシー
   2. システムメンテナンスのポリシーと、関連する「システムメンテナンス」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. システムメンテナンスのポリシーを[指定:組織が定めた頻度で]
   2. システムメンテナンスの手順を[指定:組織が定めた頻度で]

補足的ガイダンス:この管理策は、MA ファミリ内の選択されたセキュリティ管理策とその拡張管理策のを効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** MA-1	**中** MA-1	**高** MA-1

MA-2　管理されたメンテナンス

管理策:組織は、

a. 製造業者またはベンダーの仕様書および／または組織の要求事項に従って、情報システムコンポーネントのメンテナンスと修理を計画、実施、文書化し、記録をレビューする
b. メンテナンス活動が現地で行われるか、遠隔で行われるかにかかわらず、また、その機器が現地でメンテナンス／修理を受けるか、別の場所に移動されてメンテナンス／修理を受けるかにかかわらず、すべてのメンテナンス活動を承認し、モニタリングする
c. 情報システムまたはシステムコンポーネントが組織の施設から離れた場所でメンテナンスまたは修理される場合に、施設からの移動について、[指定:組織が定めた職員または役職]による明示的な承認を要求する
d. 機器が組織の施設から離れた場所でメンテナンスまたは修理される場合に、施設からの移動に先立って、関連する媒体からすべての情報を消去するための機器の無害化を実施する
e. メンテナンスまたは修理後に、影響を受けた可能性のあるすべてのセキュリティ管理策をチェックして、それらの管理策が正しく機能しているかどうかを確認する
f. [指定:組織が定めた、メンテナンス関連情報]を組織のメンテナンス記録に含める。

補足的ガイダンス:この管理策は、情報システムメンテナンス計画の情報セキュリティの側面を取り扱うものであり、あらゆるシステムコンポーネント(アプリケーションを含む)に対してローカルエンティティまたは非ローカルエンティティ(例:契約、保証、社内、ソフトウェア保全契約)によって実施される、あらゆるタイプのメンテナンスに適用される。システムメンテナンスは、また、スキャナー、コピー機、プリンターなどの、情報処理および/またはデータ/情報保持に直接関連しないコンポーネントも対象とする。効果的なメンテナンス記録を作成するのに必要な情報は、たとえば、以下を含む:①メンテナンスの日時②メンテナンスを実施した個人またはグループの名前③付添人の名前(必要であれば)④実施されたメンテナンスの内容⑤取り外された/交換された情報システムコンポーネント/機器(識別番号がある場合には、それも記載する)。メンテナンス記録の詳細レベルは、組織の情報システムのセキュリティカテゴリに基づく場合がある。組織は、情報システムにおいて交換されるコンポーネントの、サプライチェーンの問題について考慮する。関連するセキュリティ管理策は、CM-3・CM-4・MA-4・MP-6・PE-16・SA-12・SI-2。

拡張管理策:

(1) 管理されたメンテナンス | 記録内容

[削除された:MA-2 に統合された]

(2) 管理されたメンテナンス | メンテナンス活動を自動で実施する

組織は、

(a) メンテナンスと修理を計画、実施、文書化するための自動化されたメカニズムを使用する

(b) リクエストされた/計画された/進行中の/完了したすべてのメンテナンスおよび修理に関する最新かつ正確で完全な記録を作成する。

補足的ガイダンス:関連する管理策は、CA-7・MA-3。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** MA-2	**中** MA-2	**高** MA-2 (2)

MA-3 メンテナンスツール

管理策:組織は、情報システムのメンテナンスツールを承認・管理のうえモニタリングする。

補足的ガイダンス:この管理策は、組織の情報システムに対する診断や修理に使用されるメンテナンスツールの、セキュリティ問題に対処する。メンテナンスツールには、ハードウェア製品・ソフトウェア製品・ファームウェア製品がある。メンテナンスツールは、意図的であるなしにかかわらず、悪質コードを施設に持ち込んで、その後、組織の情報システムに挿入するのに利用される可能性がある。メンテナンスツールには、たとえば、ハードウェア/ソフトウェア診断用の検査機器や、ハードウェア/ソフトウェアパケットスニファーがある。本管理策は、情報システムのメンテナンスを支援するもののシステムの一部でもあるハードウェア/ソフトウェアコンポーネント(たとえば、「ping」・「ls」・「ipconfig」を実施するソフトウェア、または、Ethernet switch のモニタリングポートを実装しているハードウェア/ソフトウェア)は扱わない。関連する管理策は、MA-2・MA-5・MP-6。

拡張管理策:

(1) メンテナンスツール | ツールを検査する

組織は、メンテナンス要員が施設に持ち込むメンテナンスツールを検査し、不適切な変更または不正な変更の有無を確認する。

補足的ガイダンス：メンテナンスツールを検査して、ツールが不適切に／不正に変更された、またはツールに悪質コードが含まれていると組織が判断した場合には、組織のインシデント対応ポリシーおよび手順に従ってインシデントが処理される。関連する管理策は、SI-7。

(2) メンテナンスツール | 媒体を検査する

組織は、診断プログラムおよびテストプログラムが入っている媒体を検査して、悪質コードが含まれていないことを確認した上で、情報システムに使用する。

補足的ガイダンス：メンテナンス用の診断プログラムおよびテストプログラムが入っている媒体を検査して、媒体に悪質コードが含まれていると組織が判断した場合には、組織のインシデント対応ポリシーおよび手順に従ってインシデントが処理される。関連する管理策は、SI-3。

(3) メンテナンスツール | 許可なく撤去されるのを防止する

組織は、組織の情報を含んでいるメンテナンス機器が許可なく持ち去されるのを

(a) その機器に組織の情報が含まれていないことを確認する

(b) 機器を無害化または破壊する

(c) 機器を施設内で保持する

(d) 機器を施設から持ち去ることに関して、明示的に許可を与える権限のある[指定：組織が定めた職員または役職]から、許可を得る。

の 4 つを実施することによって防止する。

補足的ガイダンス：組織の情報は、組織が所有するすべての情報と、情報のスチュワードとして使える組織に提供される情報を含む。

(4) メンテナンスツール | ツールの使用制限

情報システムは、メンテナンスツールの使用を許可された職員に限定する。

補足的ガイダンス：この拡張管理策は、メンテナンス機能を実施するのに使用される情報システムに適用される。関連する管理策は、AC-2・AC-3・AC-5・AC-6。

参考文献：NIST Special Publication 800-88

優先順位とベースライン管理策の割り当て：

P3	**低** 選択されていない	**中** MA-3 (1) (2)	**高** MA-3 (1) (2) (3)

MA-4 非局所的なメンテナンス

管理策：組織は、

a. 非局所的なメンテナンスおよび診断を承認のうえモニタリングするのに合わせて、

b. 非局所的なメンテナンスおよび診断用ツールは、組織のポリシーに沿っている場合かつ情報システムのセキュリティ計画に記載されている通りである場合のみ、使用を許可するとともに、

c. 非局所的なメンテナンスおよび診断のためのセッションを確立する際には、厳密なオーセンティケータを使用するのに加えて、

d. 非局所的なメンテナンスおよび診断の記録を保管するだけではなく、

e. 非局所的なメンテナンスが完了したら、セッションとネットワーク接続を終了する。

補足的ガイダンス：非局所的なメンテナンスおよび診断活動は、外部ネットワーク（例：インターネット）あるいは内部ネットワークのいずれかを介して情報をやりとりする個人によって実施される。局所的なメンテナンスおよび診断活動は、情報システムまたは情報システムコンポーネント

の前に物理的に居る個人によって、ネットワーク接続を介さずに実施される。非局所的なメンテナンスおよび診断のためのセッションを確立するのに使用される認証技術は、IA-2 に記載されているネットワークアクセス要件を満たす。通常、厳密な認証では、リプレイ攻撃に対して耐性を有し、多要素認証を使用するオーセンティケータが必要である。厳密なオーセンティケータには、たとえば、パスワード、パスフレーズ、または生体認証によって保護されるトークンに証明書が保存される公開鍵基盤がある。MA-4 の要求事項は、他の管理策によってその一部が満たされる。関連する管理策は、AC-2・AC-3・AC-6・AC-17・AU-2・AU-3・IA-2・IA-4・IA-5・IA-8・MA-2・MA-5・MP-6・PL-2・SC-7・SC-10・SC-17。

拡張管理策:

(1) 非局所的なメンテナンス | 監査とレビュー

組織は、

(a) [指定:組織が定めた監査イベント]の、非局所的なメンテナンス および診断のために確立されたセッションを監査するとともに、

(b) メンテナンスおよび診断のために確立されたセッションの記録をレビューする。

補足的ガイダンス:関連する管理策は、AU-2・AU-6・AU-12。

(2) 非局所的なメンテナンス | 非局所的なメンテナンスについて記載する

組織は、非局所的なメンテナンス および診断のための接続の確立と使用に関するポリシーと手順を、情報システムのセキュリティ計画に記載する。

(3) 非局所的なメンテナンス | 同等のセキュリティ / 無害化

組織は、

(a) 非局所的なメンテナンス および診断サービスが、サービスを受ける情報システム上で実施されるセキュリティ機能と同等のセキュリティ機能を実施する情報システムから、実施されることを要求するとともに、

(b) 非局所的なメンテナンスまたは診断サービスを受けるコンポーネントを、サービスの実施に先立ち情報システムから切り離して、(組織の情報を消すために)無害化した後に、組織の施設から移動する。また、サービス実施後は、(悪質なソフトウェアに関して)コンポーネントを検査・無害化してから、情報システムに再接続する。

補足的ガイダンス:メンテナンスサービスを提供する情報システム、診断ツール、機器上で同等のセキュリティ機能を実施するということは、サービスを提供する側の情報システム、診断ツール、機器上で実施されるセキュリティ管理策と、サービスを受ける側の情報システム上で実施されるセキュリティ管理策の包括さが、少なくとも同等であること意味する。関連する管理策は、MA-3・SA-12・SI-3・SI-7。

(4) 非局所的なメンテナンス | メンテナンス用セッションの認証 / 切り離し

組織は、以下を実施することによって、非局所的なメンテナンス用のセッションを保護する:

(a) [指定:組織が定めた、リプレイ攻撃に対して耐性を有するオーセンティケータ]を使用する

(b) 以下のいずれかを実施することによって、情報システムのメンテナンス用セッションを、他のネットワークセッションから分離する:

(1) 物理的に分離された通信経路

(2) 暗号化をベースにした、論理的に分離されている通信経路。

補足的ガイダンス:関連する管理策は、SC-13

(5) 非局所的なメンテナンス | 承認と通知

組織は、

(a) 非局所的なメンテナンス用セッションの各々について、[指定: 組織が定めた職員または役職]による承認を要求するとともに、

(b) 予定されている非局所的なメンテナンスの日時を[指定: 組織が定めた職員または役職]に知らせる。

補足的ガイダンス: 通知は、メンテナンス要員によって行われる場合がある。非局所的なメンテナンス用セッションの承認は、提案されているメンテナンスが適切であるかどうかを判断するのに十分な、情報セキュリティと情報システムに関する知識を有する職員が行う。

(6) 非局所的なメンテナンス | 暗号化による保護

情報システムは、非局所的なメンテナンス および診断時のコミュニケーションの完全性と機密性を保護するために、暗号メカニズムを使用する。

補足的ガイダンス: 関連する管理策は、SC-8・SC-13。

(7) 非局所的なメンテナンス | リモート接続の確認

情報システムは、非局所的なメンテナンスおよび診断のために確立されたセッションの終了時に、リモート接続の切断を確認する。

補足的ガイダンス: リモート接続の切断を確認することによって、非局所的なメンテナンスのために確立されたセッションによるリモート接続が終了していて、かつ、使用できない状態になっているかを確認できる。関連する管理策は、SC-1。

参考文献: FIPS Publications 140-2・同 197・同 201。その他、NIST Special Publications 800-63 および同 800-88 ならびに CNSS Policy 15。

優先順位とベースライン管理策の割り当て:

P2	**低** MA-4	**中** MA-4 (2)	**高** MA-4 (2) (3)

MA-5 メンテナンス要員

管理策: 組織は、

a. メンテナンス要員の認可プロセスを確立し、認可されたメンテナンス組織または要員の一覧を維持する

b. メンテナンス要員が付添いなしで情報システムのメンテナンスを行う場合に、その職員が必要なアクセス権限を有することを確認する

c. 必要なアクセス権限を持たない要員によるメンテナンス活動を監督するのに必要な、アクセス権限と技術的能力を有する組織の職員を指定する。

補足的ガイダンス: PE-2 は、システムの物理的な保護領域内でメンテナンスを行う個人(例: 管理スタッフ、施設のメンテナンス要員)による物理アクセスを扱うが、この管理策は、組織の情報システム上でハードウェアまたはソフトウェアのメンテナンスを行う個人に適用される。監督する側の技術的能力は、情報システム上で実施されるメンテナンスに関連し、必要なアクセス権限を有することは、システム上またはシステムの傍で実施されるメンテナンスに関連する。IT 製造業者、ベンダー、システムインテグレータ、コンサルタントなどの権限を有するメンテナンス要員としては認められていない個人が、たとえば簡素な通知で(あるいは通知なしで)組織の情報システムのメンテナンス活動を行う必要がある場合には、そのシステムに対する特権的アクセスが必要になる。組織はリスクアセスメント結果に基づいて、そうした個人に一時的なクレデンシャルを発行してもよい。一時的なクレデンシャルは、1 回しか使用できなかったり、非常に限られた

期間しか使用できなかったりする。関連する管理策は、AC-2・IA-8・MP-2・PE-2・PE-3・PE-4・RA-3。

拡張管理策:

(1) メンテナンス要員 | 適切なアクセス権限のない個人

組織は、

(a) 適切なセキュリティクリアランスを持たないメンテナンス要員、またはアメリカ合衆国国民でないメンテナンス要員を使用する際の手順を実施する。なお、そうした手順は、以下の要求事項を含むものとする:

(1) 必要なアクセス権限、クリアランス、または正式なアクセス許可を持たないメンテナンス要員が情報システム上でメンテナンスや診断を行う場合には、許可されていて、適切なアクセス権限を有し、かつ、技術的にも資格のある職員が付き添って、監督する

(2) 必要ななアクセス権限、クリアランス、または正式なアクセス許可を持たないメンテナンス要員がメンテナンスまたは 診断を行う場合には、それに先立って情報システム内の揮発性の情報記憶コンポーネントをすべて無害化し、不揮発性の記憶媒体はすべてシステムから取り外す、または物理的に切り離して、保護する

(b) 情報システムコンポーネントの無害化や、システムからの取り外し／切り離しが不可能な場合には、代替のセキュリティ対策を考案・実施する。

補足的ガイダンス:この拡張管理策は、適切なセキュリティクリアランスを持たない個人(すなわち、セキュリティクリアランスを持たない個人、または必要なレベルよりも低いレベルのセキュリティクリアランスを持つ個人)またはアメリカ合衆国国民でない個人に対して、組織の情報システムに含まれる機密情報、CUI(管理されている、非機密扱いの情報)、または他の機微な情報に対する視覚的アクセスと電子アクセスを拒否する。メンテナンス要員の使用に関する手順は、情報システムのセキュリティ計画に記載してもよい。関連する管理策:MP-6・PL-2。

(2) メンテナンス要員 | 機密情報を扱うシステムに対するセキュリティクリアランス

組織は、機密情報を処理または保存もしくは伝送する情報システム上でメンテナンスや診断を行う職員が、少なくとも最も高い分類レベルに見合っていて、かつ、システム上のすべての情報を対象にした、セキュリティクリアランスおよび正式なアクセス許可を有することを確認する。

補足的ガイダンス:関連する管理策は、PS-3。

(3) メンテナンス要員 | 機密情報を扱うシステムに対する、アメリカ合衆国国民である必要性

組織は、機密情報を処理または保存もしくは伝送する情報システム上でメンテナンスや診断を行う職員がアメリカ合衆国国民であることを確認する。

補足的ガイダンス:関連する管理策は、PS-3。

(4) メンテナンス要員 | 外国籍の人

組織は、

(a) 機密扱いの情報システム上でのメンテナンスや診断を、認可を得た外国籍の人(すなわち、適切なセキュリティクリアランスを有する外国籍の人)に実施させるにあたっては、アメリカ合衆国と、同盟関係にある外国政府が、そのシステムを共同で所有し、運用している、あるいは同盟関係にある外国政府が、そのシステムを単独で所有・運用している場合にのみに実施するよう、万全を期す。

(b) 機密扱いの情報システム上で のメンテナンスや診断を外国籍の人に実施させる場合の承認、同意、詳細な運用条件に関しては、協定書にすべて確実に記載されるようにする。

補足的ガイダンス：関連する管理策は、PS-3。

(5) メンテナンス要員 | システムとは関連しないメンテナンス

組織は、情報システムとは直接関連しないメンテナンスではあるが、システムに物理的に近い場所で、付添いなしでそうしたメンテナンスを実施する要員が、必要なアクセス権限を有することを確認する。

補足的ガイダンス：情報システムとは直接関連しないメンテナンス活動を実施する職員には、たとえば、施設の人員や守衛がいる。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P2	**低** MA-5	**中** MA-5	**高** MA-5 (1)

MA-6 タイムリーなメンテナンス

管理策：組織は、[指定：組織が定めた情報システムコンポーネント]の障害が発生した場合に、[指定：組織が定めた期間]内にメンテナンスサポートを得る、および／または予備の部品を調達する。

補足的ガイダンス：組織は情報システムコンポーネントによって提供される機能が機能しない場合に、（組織の）業務・（組織の）資産・個人・他組織・国家のいずれかに対するリスクの増加につながる情報システムコンポーネントを明確にする。メンテナンスサポートを得るために組織が取るアクションには、通常、適切な契約を結ぶことも含まれる。関連する管理策は、CM-8・CP-2・CP-7・SA-14・SA-15。

拡張管理策：

(1) タイムリーなメンテナンス | 予防のためのメンテナンス

組織は、[指定：組織が定めた情報システムコンポーネント]に対して、[指定：組織が定めた時間間隔]で予防のためのメンテナンスを実施する。

補足的ガイダンス：予防のためのメンテナンスは、機器や施設を満足できる稼働状態に保つために、組織の情報システムコンポーネントを予防的にケアし、メンテナンスすることを含む。そうしたメンテナンスには、初期不良が発生する前に実施される、あるいは、そうした初期不良が重大な欠陥に発展する前に実施される、初期不良の系統立った検査、テスト、測定、調整、部品の交換、検出、修正も含まれる。予防のためのメンテナンスの第一の目的は、機器の不具合がもたらす影響を回避／軽減することにある。予防のためのメンテナンスは、使い古されたコンポーネントが実際に故障する前に、新しいのと交換することによって、機器の信頼性を維持し、取り戻すことを可能にする。適用すべき、予防のための（あるいは、その他の）障害管理ポリシーを決定する方法としては、たとえば、相手先商標製品の製造会社(OEM)による推奨、統計的な障害記録、法典が定める要求事項、法律、または管轄区域内の規定、専門家の意見、類似の機器に対して既に実施されたメンテナンス、または測定値や性能表示がある。

(2) タイムリーなメンテナンス | 予測的なメンテナンス

組織は、[指定：組織が定めた情報システムコンポーネント]に対して、[指定：組織が定めた時間間隔]で予測的なメンテナンスを行う。

補足的ガイダンス：予測的なメンテナンス（条件ベースのメンテナンスともいう）では、機器の状態を調べるために、定期的に、または継続的に（オンラインで）機器の状態をモニタリングする。予測的なメンテナンスの目的は、メンテナンス活動の費用効率が最も高くなるタイミングで、かつ、機器の性能が低下し閾値に達する前に、メンテナンスを実施することにある。

予測的なメンテナンスの予測コンポーネントは、機器の状態の今後の傾向を予測するといった目的に基づいて決定される。このアプローチでは、将来にわたってどの地点でメンテナンス活動を行うのが適切であるかを決定するために、「統計に基づくプロセス制御」の原理を用いる。予測的なメンテナンスのための検査の多くは、機器の稼働中に実施されるため、通常のシステムの稼動が中断する期間を最小限に抑えられる。予測的なメンテナンスは、費用を大幅に削減し、システムの信頼性を向上させる。予測的なメンテナンスは、対象物の測定を含む傾向にある。予測的なメンテナンスでは、機器の状態を調べるために赤外線、音響（部分放電や空中超音波）、コロナ検出、振動解析、音圧レベル測定、油分析、その他の特定のオンラインテストなどの、非破壊検査の技術を活用する。

(3) タイムリーなメンテナンス | 予測的なメンテナンスを支援する自動化されたメカニズム

組織は、予測的なメンテナンスのデータをコンピュータ化されたメンテナンス管理システムに伝送するための、自動化されたメカニズムを使用する。

補足的ガイダンス：コンピュータ化されたメンテナンス管理システムは、組織のメンテナンス活動についての情報を蓄積したコンピューターデータベースを維持し、機器の状態データの処理を自動化することによって、メンテナンス計画の作成、メンテナンスの実施および報告が行われるようにする。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P2	**低** 選択されていない	**中** MA-6	**高** MA-6

ファミリ:媒体の保護

MP-1　媒体保護のポリシーと手順

管理策:組織は、

a. 以下を策定、文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、媒体保護のポリシー
   2. 媒体保護のポリシーと、関連する「媒体の保護」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. 媒体保護のポリシーを[指定:組織が定めた頻度で]
   2. 媒体保護の手順を[指定:組織が定めた頻度で]

補足的ガイダンス:この管理策は、MP ファミリ内の選択されたセキュリティ管理策とその拡張管理策のを効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** MP-1	**中** MP-1	**高** MP-1

MP-2　媒体に対するアクセス

管理策:組織は、[指定:組織が定めたタイプのデジタル媒体および／または非デジタル媒体]に対するアクセスを[指定:組織が定めた職員または役職]に限定する。

補足的ガイダンス:情報システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、たとえば、ディスケット・磁気テープ・外部／リムーバブルハードディスク・フラッシュドライブ・コンパクトディスク・デジタルビデオディスクがある。非デジタル媒体には、たとえば、紙やマイクロフィルムがある。非デジタル媒体に対するアクセスの制限には、たとえば、地域病院の患者の医療記録に対するアクセスを、アクセス要求する者が認可された医療提供者である場合を除いて拒否することが含まれる。デジタル媒体に対するアクセスを制限することには、たとえば、メディアライブラリ内のコンパクトディスクに保存されている設計仕様書に対するアクセスを、プロジェクトリーダーと開発チームのメンバーに限定することが含まれる。関連する管理策は、AC-3・IA-2・MP-4・PE-2・PE-3・PL-2。

拡張管理策:

(1) 媒体に対するアクセス | 自動化されたアクセス制限

[削除された:MP-4(2)に統合された]

(2) 媒体に対するアクセス | 暗号化による保護

[削除された：SC-28(1)に統合された]

参考文献：FIPS Publication 199・NIST Special Publication 800-111

優先順位とベースライン管理策の割り当て：

P1	**低** MP-2	**中** MP-2	**高** MP-2

MP-3 媒体のマーキング

管理策：組織は、

a. 情報システム媒体に、配布制限とともに取扱い上の注意および情報のセキュリティマーク（用意されている場合）を記す（すなわち、マーキング）とともに、

b. ［指定：組織が定めたタイプの情報システム媒体］であり、かつ、［指定：組織が定めた、管理された領域］に保管されている場合には、上述のマーキングの対象から外す。

補足的ガイダンス：「セキュリティマーキング」という用語は、セキュリティ属性を人が読めるの形式で記すことを意味する。「セキュリティラベリング」という用語は、情報システム内の内部データ構造のセキュリティ属性を記すことを意味する（AC-16 を参照）。情報システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、たとえば、ディスケット、磁気テープ、外部／リムーバブルハードディスク、フラッシュドライブ、コンパクトディスク、デジタルビデオディスクがある。非デジタル媒体には、たとえば、紙やマイクロフィルムがある。「セキュリティマーキング」は、通常、媒体に含まれる情報が、組織の判断によりパブリックドメインに置かれる場合や、一般への公開が可能な情報である場合には、必要でない。しかしながら、組織によっては、パブリックな情報が一般への公開が可能であることを示すために、そうした情報に対してマーキングを必要とする場合がある。情報システム媒体のマーキングは、該当する連邦法・大統領命令・指令・政策・規制・標準・手引を反映する。関連する管理策は、AC-16・PL-2・RA-3。

拡張管理策：なし

参考文献：FIPS Publication 199

優先順位とベースライン管理策の割り当て：

P2	**低** 選択されていない	**中** MP-3	**高** MP-3

MP-4 媒体の保管

セキュリティ管理策：組織は、

a. ［指定：組織が定めたタイプのデジタル媒体および／または非デジタル媒体］を［指定：組織が定めた、管理された領域］内で物理的に管理し、安全に保管するとともに、

b. 情報システム媒体が、承認された機器、技法、手順を用いて破壊される、または無害化されるまで保護する。

補足的ガイダンス：情報システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、例えば、ディスケット、磁気テープ、外部／リムーバブルハードディスク、フラッシュドライブ、コンパクトディスク、デジタルビデオディスクがある。非デジタル媒体には、たとえば、紙やマイクロフィルムがある。情報システム媒体を物理的に管理することには、たとえば、在庫を調べること、個人がメディアライブラリから媒体を借り出して返却することを可能にする手順を用意すること、保存されているすべての媒体に対する説明責任を果たすことが含まれる。安全な保管場所には、例えば、鍵が掛かった引き出し、机、キャビネットや、アクセスが制御されるメディアライブラリがある。媒体の保管場所のタイプは、その媒体に格納される情報のセキュリティカ

テゴリおよび／または分類レベルに相応する。管理された領域とは、情報および／または情報システムを保護するために定められた要求事項を満す物理面と手続き面での保護が、組織によって提供される領域である。媒体に含まれる情報が、組織の判断によりパブリックドメインに置かれる場合や、一般への公開が可能な情報である場合、または権限を与えられた職員以外の者がアクセスしたとしても、組織や個人に及ぶ負の影響が限られている、あるいは全くない場合には、必要な対策の数は少なくなる。こうした状況では、物理アクセス制御が適切な保護をもたらす。関連するセキュリティ管理策は、CP-6・CP-9・MP-2・MP-7・PE-3。

拡張管理策:

(1) 媒体の保管 | 暗号化による保護

[削除された:SC-28(1)に統合された]

(2) 媒体の保管 | 自動化されたアクセス制限

組織は、媒体が保管されているエリアに対するアクセスを制限し、アクセスの試みや、許したアクセスを監査するための、自動化されたメカニズムを使用する。

補足的ガイダンス:自動化されたメカニズムには、たとえば、媒体が保管されているエリアへの外部からの入室に対して、キーパッドによる制御を行うことがある。関連する管理策は、AU-2・AU-9・AU-6・AU-12。

参考文献:FIPS Publication 199・NIST Special Publications 800-56・NIST Special Publications 800-57・NIST Special Publications 800-111

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** MP-4	**高** MP-4

MP-5 媒体の移動

セキュリティ管理策:組織は、

a. [指定:組織が定めたタイプの情報システム媒体]が、管理された領域外に持ち出されている間は、[指定:組織が定めたセキュリティ対策]を用いて保護し、管理するのと合わせて、
b. 情報システム媒体が、管理された領域外に持ち出される場合の説明責任を果たすとともに、
c. 情報システム媒体の持ち出しに関連する活動を文章化するのに加えて、
d. 情報システム媒体の持ち出しに関連する活動を、権限を与えられた職員に限定する。

補足的ガイダンス:情報システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、たとえば、ディスケット・磁気テープ・外部／リムーバブルハードディスク・フラッシュドライブ・コンパクトディスク・デジタルビデオディスクがある。非デジタル媒体には、たとえば、紙やマイクロフィルムがある。この管理策は、管理された領域外に持ち出させる、情報を保存できる携帯機器(例:スマートフォン・タブレット・電子書籍端末)にも適用される。管理された領域とは、情報および／または情報システムを保護するために定められた要求事項を満す物理面および／または手続き面での保護が、組織によって提供される領域、または空間である。

媒体を保護するための物理面と技術面での対策は、その媒体に格納される情報のセキュリティカテゴリまたは分類レベルに相応する。持ち出されている媒体を保護するための対策には、たとえば、鍵が掛かったコンテナや暗号技術がある。使用する暗号メカニズムによっては、機密性と完全性が保護される。持ち出しに関連する活動は、実際の持ち出しに加えて、持ち出しのために媒体をリリースすることや、媒体が適切な持ち出しのためのプロセスを経るようにすることなどの活動を含む。実際の持ち出しを許可される輸送要員や配送業者には、組織外の個人が含まれる場合がある(例:米国郵政公社、または商用の輸送／配送サービス)。持ち出されてい

る媒体の説明責任を果たすことは、たとえば、持ち出しを権限を与えられた職員に限定することや、媒体が輸送システム内を進む間に、持ち出しの明示的な記録を追跡および／または取得することによって、紛失または破壊もしくは改ざんを検知・防止することを含む。組織は、組織によるリスクアセスメントの結果に基づいて、情報システム媒体の持ち出しに伴う活動の、文書化要件を定める。そうした要件は、輸送関連の記録を取るための全般的な仕組みの一環として、媒体輸送手段のタイプ別に、記録を取る手法を定めるといった柔軟性も含むものとする。関連する管理策は、AC-19・CP-9・MP-3・MP-4・RA-3・SC-8・SC-13・SC-28。

拡張管理策:

(1) 媒体の移動 | 管理された領域外での保護

[削除された:MP-5 に統合された]

(2) 媒体の移動 | 活動の文書化

[削除された:MP-5 に統合された]

(3) 媒体の移動 | 守衛

組織は、情報システム媒体が管理された領域外に持ち出されている間、身元が確認できる守衛を採用する。

補足的ガイダンス:身元が確認できる守衛は、組織に対して、媒体が持ち出されている間の連絡窓口となり、そうした媒体の説明責任を果たすのを支援する。守衛の責務は、ある個人から別の個人へと委譲する場合があるが、誰が守衛であるかを常に確認できることが前提になる。

(4) 媒体の移動 | 暗号化による保護

情報システムは、情報が保存されているデジタル媒体が、管理された領域外に持ち出されている間、保存されている情報の機密性と完全性を保護するための暗号メカニズムを実施する。

補足的ガイダンス:この拡張管理策は、持ち運び可能な記憶装置(例:USB メモリースティック・コンパクトディスク・デジタルビデオディスク・外部／リムーバブルハードディスク)と、情報を保存できる携帯機器(例:スマートフォン・タブレット・電子書籍端末)の両方に適用される。関連する管理策は、MP-2。

参考文献:FIPS Publication 199・NIST Special Publication 800-60

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** MP-5 (4)	**高** MP-5 (4)

MP-6 媒体の無害化

管理策:組織は、

a. [指定:組織が定めた情報システム媒体]を廃棄する前に、または組織による管理から離れる前に、もしくは再利用のためにリリースする前に、該当する連邦法と組織の標準およびポリシーに従って[指定:組織が定めた無害化技法および手順]を用いて、媒体を無害化するとともに、

b. その情報のセキュリティカテゴリまたは分類レベルに相応する強度と完全性を備えた、無害化メカニズムを使用する。

補足的ガイダンス:この管理策は、廃棄または再利用される情報システム媒体のすべて(デジタル媒体と非デジタル媒体の両方)に対して、それらの媒体が取り外し可能であるか否かにかかわらず適用される。例としては、スキャナー・コピー機・プリンター・ノートパソコン・ワークステーション・ネットワークコンポーネント・携帯機器に使用される媒体がある。無害化プロセスでは、媒

体の情報を読み出したり、再構築できないように、情報を消し去る。消去、除去、暗号化消去、破壊を含む無害化技法は、そうした媒体の再利用時、または廃棄のためのリリース時に、情報が権限のない個人に開示されるのを防止する。組織が適切な無害化手段を決定する際には、破壊以外に適用できる手段がないこともあるので、注意が必要である。組織は、媒体に含まれる情報が、組織の判断によりパブリックドメインに置かれる場合や、一般への公開が可能な情報である場合、または再利用または廃棄のためにリリースされたとしても、組織または個人に及ぶ負の影響が全くない場合には、承認された無害化技法と手順を自由裁量で用いる。非デジタル媒体の無害化の例としては、機密扱いの付録以外は非機密扱いであるドキュメントから、そうした付録を取り除くことや、ドキュメント内の選択された節または単語を見えなくなるように編集することによって、実際にドキュメントから削除する場合と同等の効果を得ること、などが挙げられる。NSA 標準およびポリシーは、機密情報を含む媒体の無害化プロセスを規定する。関連する管理策は、MA-2・MA-4・RA-3・SC-4。

拡張管理策:

(1) 媒体の無害化 | レビュー / 承認 / 追跡 / 文書化 / 確認

組織は、媒体の無害化および廃棄作業をレビュー・承認・追跡・文書化することによって確認する。

補足的ガイダンス:組織は、記録の保管に関するポリシーを遵守するために、無害化を予定している媒体をレビューのうえ承認する。作業の追跡／文書化は、たとえば、無害化および廃棄作業をレビューし、承認した職員と、無害化された媒体のタイプ、媒体に保存されていたファイル、使用された無害化手法、無害化の実施日と時刻、無害化を実施した職員、実施された確認作業、確認を行った職員、実施された廃棄作業を記載することを含む。組織は、媒体を廃棄する前に、媒体の無害化が実施されたことを確認する。関連する管理策は、SI-12。

(2) 媒体の無害化 | 機器のテスト

組織は、無害化のための機器と手順を[指定:組織が定めた頻度で]テストし、意図した無害化がなされることを確認する。

補足的ガイダンス:無害化のための機器と手順のテストは、資格のある、認可された外部組織(例:他の連邦政府機関または外部サービスプロバイダ)によって実施される場合がある。

(3) 媒体の無害化 | 非破壊的な技法

組織は、以下の状況下で、持ち運び可能な記憶装置を情報システムに接続する前に、装置に対して非破壊的な無害化技法を適用する:[指定:組織が定めた、持ち運び可能な記憶装置の無害化を必要とする状況]。

補足的ガイダンス:この拡張管理策は、機密情報や CUI(管理されている、非機密扱いの情報)を含むデジタル媒体に適用される。持ち運び可能な記憶装置は、悪質コードを組織の情報システムに挿入するのに利用される可能性がある。これらの装置の多くは、出所が不明であったり、信頼できない場合もあり、USB ポートやその他の進入路を介して情報システムに容易に伝送される、悪質コードを含んでいる可能性がある。そうした記憶装置のスキャニングは常に推奨されるが、無害化は、ゼロ・デイ攻撃を開始するコードなどの悪質コードが装置に含まれないことを保証する。組織は、製造業者やベンダーから購入した持ち運び可能な記憶装置を無害化する場合や、組織が詳細な記録を失った持ち運び可能な記憶装置を無害化する場合には、非破壊な無害化について検討する。関連する管理策は、SI-3。

(4) 媒体の無害化 | CUI(管理されている、非機密扱いの情報)

[削除された:MP-6 に統合された]

(5) 媒体の無害化 | 機密情報

[削除された：P-6 に統合された]

(6) 媒体の無害化 | 媒体の破壊

[削除された：MP-6 に統合された]

(7) 媒体の無害化 | 二重認証

組織は、[指定：組織が定めた情報システム媒体]の無害化が行われる際には、二重認証を実施する。

補足的ガイダンス：組織は情報システム媒体の無害化が、技術的に資格のある二人の個人によって実施される場合を除き実施されないようにするために、二重認証を用いる。情報システム媒体の無害化を実施する個人は、提案されている無害化が該当する連邦政府／組織標準、ポリシー、手順を反映しているかどうかを判断するのに十分な、スキル／専門知識を有する。二重認証は、また、無害化が意図されたとおりに行われるようにし、エラーや、無害化作業を実施したと偽って主張されることから保護するのに役立つ。二重認証は、「二人立会制御 (two-person control)」としても知られている。関連する管理策は、AC-3・MP-2。

(8) 媒体の無害化| リモートで情報を消去する

組織は、[指定：組織が定めた情報システム、システムコンポーネント、またはデバイス]上の情報をリモートで、あるいは以下の条件が満たされる場合に消去する：[指定：組織が定めた条件]。

補足的ガイダンス：この拡張管理策は、組織の情報システム、システムコンポーネント、または機器（例：携帯機器）が権限のない個人の手に渡った場合に、それらに保存されているデータ／情報が保護されるようにする。リモートでの除去／消去のためのコマンドは、権限のない個人によってシステム / コンポーネント / デバイス上のデータ／情報が消去されるリスクを軽減するために、厳密な認証を必要とする。消去機能は、たとえば、データ／情報を複数回にわたって上書きしたり、暗号化されたデータを複合するのに必要な鍵を破壊するなどの、さまざまな方法で実現できる。

参考文献：FIPS Publication 199・NIST Special Publications 800-60・NIST Special Publications 800-88・ウェブサイト
http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

優先順位とベースライン管理策の割り当て：

P1	**低** MP-6	**中** MP-6	**高** MP-6 (1) (2) (3)

MP-7 媒体の使用

管理策：組織は、[指定：組織が定めたタイプの情報システム媒体]が[指定：組織が定めた情報システムまたはシステムコンポーネント]のため利用されないよう、[指定：組織が定めたセキュリティ対策]を用いて[選択：制限・禁止]する。

補足的ガイダンス：情報システム媒体には、デジタル媒体と非デジタル媒体がある。デジタル媒体には、たとえば、ディスケット、磁気テープ、外部／リムーバブルハードディスク、フラッシュドライブ、コンパクトディスク、デジタルビデオディスクがある。非デジタル媒体には、たとえば、紙やマイクロフィルムがある。この管理策は、情報を保存できる携帯機器（例：スマートフォン、タブレット、電子書籍端末）にも適用される。MP-2 が媒体に対するユーザアクセスを制限するのに対して、この管理策は、たとえば、フラッシュドライブまたは外部ハードディスクの使用を制限する／禁止するなど、特定のタイプの媒体を情報システムに使用するのを制限する。組織は、情報システム媒体の使用を制限するにあたって、技術面での対策と、非技術面での対策（例：ポリシ

一、手順、行動規則）を用いることができる。組織は持ち運び可能な記憶装置の使用を制限することができ、その手段としては、ワークステーション上に物理的なケージを設置して、特定の外部ポートにアクセスできないようにする、持ち運び可能な記憶装置に対する挿入、読み出し、または書き込機能を無効化する／削除するなどがある。組織は持ち運び可能な記憶装置の使用を、たとえば組織が用意した装置、認可された他の組織が用意した装置、私有でない装置などの、許可された装置に限定してもよい。最後に、組織は持ち運び可能な記憶装置の使用を、装置のタイプに応じて制限できる。その例としては、書き込み可能かつ持ち運び可能な記憶装置の使用を禁止することや、そうした装置に対する書き込み機能を無効化／削除することがある。関連する管理策は、AC-19・PL-4。

拡張管理策:

(1) 媒体の使用 | 所有者がいない場合には、使用を禁止する

組織は、持ち運び可能な記憶装置の所有者が特定できない場合には、組織の情報システムに使用することを禁止する。

補足的ガイダンス:持ち運び可能な記憶装置の使用に関して、所有者（例:個人・組織・プロジェクト）を特定できることを前提とすることで、装置の既知の脆弱性（例:悪質コードが挿入されてしまう）に対処する責任と説明責任を組織が割り当てることが可能になり、そうしたテクノロジーの使用に伴うリスクが減少する。関連する管理策は、PL-4。

(2) 媒体の使用 | 無害化に対する耐性を有する媒体の使用を禁止する

組織は、無害化に対する耐性を有する媒体を、組織の情報システムに使用することを禁止する。

補足的ガイダンス:無害化に対する耐性は、媒体から情報を除去する機能に対する耐性である。特定のタイプの媒体は、無害化コマンドをサポートしていなかったり、サポートしていても、インターフェースが、そうした媒体に対して標準化された形でサポートされていなかったりする。無害化に対する耐性を有する媒体には、たとえば、コンパクトフラッシュ、ボードやデバイスに内蔵されているフラッシュ、半導体ドライブ、USB リムーバブルメディアがある。関連する管理策は、MP-6。

参考文献:FIPS Publication 199・NIST Special Publication 800-111

優先順位とベースライン管理策の割り当て:

P1	**低** MP-7	**中** MP-7 (1)	**高** MP-7 (1)

MP-8 媒体のダウングレード

管理策:組織は、

a. 情報システム媒体に対する[指定:組織が定めた強度と完全性]を備えたダウングレードメカニズムの使用を含む[指定:組織が定めた、情報システム媒体のダウングレードプロセス]を確立するのと合わせて、

b. 情報システム媒体のダウングレードプロセスが、消去される情報のセキュリティカテゴリおよび／または分類レベルと、ダウングレードされた情報を受け取る者のアクセス権限に見合っていることを確認するとともに、

c. [指定:組織が定めたダウングレードを必要とする情報システム媒体]を識別するのに加えて、

d. 識別された情報システム媒体を、確立されたプロセスを用いてダウングレードする。

補足的ガイダンス:この管理策は、組織外にリリースされる情報システム媒体のすべて（デジタル媒体と非デジタル媒体の両方）に対して、それらの媒体が取り外し可能であるか否かにかか

わらず適用される。ダウングレードプロセスがシステム媒体に適用される場合で、それらの媒体から情報を消去する際には、情報の取り出しや再構築ができないようにするために、通常はセキュリティカテゴリまたは分類レベルに応じた消去が行われる。媒体のダウングレードは、より広範囲にわたるリリースと配布を可能にするために情報を編集することを含む。媒体のダウングレードは、また、媒体上の空きスペース（例：ファイル内の未使用領域）が情報を持たないようにするのに役立つ。

拡張管理策：

(1) 媒体のダウングレード | プロセスの文書化

組織は、情報システム媒体のダウングレード作業について文書化する。

補足的ガイダンス：組織は、媒体のダウングレードプロセスについて文書化する際に、使用されたダウングレード技法、ダウングレードされた媒体の識別番号、ダウングレード作業を許可および／または実施した個人の身元などの情報を記載できる。

(2) 媒体のダウングレード | 機器のテスト

組織は、[指定：組織が定めた頻度で]、ダウングレードする機器と手順を[指定：組織が定めたテスト]を用いてテストし、ダウングレードが正しく実施されることを確認する。

(3) 媒体のダウングレード | CUI（管理されている、非機密扱いの情報）

組織は、[指定：組織が定めた、CUI（管理されている、非機密扱いの情報）]を含む情報システム媒体を、該当する連邦政府／組織標準およびポリシーに従って、一般に公開する前にダウングレードする。

(4) 媒体のダウングレード | 機密情報

組織は、機密情報を含む情報システム媒体を、NSA 標準およびポリシーに従って、必要なアクセス権限を持たない個人に公開する前にダウングレードする。

補足的ガイダンス：機密情報のダウングレードでは、機密扱いの情報システムから非機密扱いの媒体に対して非機密扱いであることが確認済の情報が伝送できるよう、承認された無害化ツールを技法・手順とともに利用する。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:物理面と環境面での保護

PE-1　物理面と環境面での保護のポリシーと手順

管理策:組織は、

a. 以下を策定・文書化のうえ、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、物理面と環境面での保護のポリシー
   2. 物理面と環境面での保護のポリシーと、関連する「物理面と環境面での保護」管理策の実施を容易にするための手順
b. 以下の最新版をレビュ・更新する:
   1. 物理面と環境面での保護のポリシーを[指定:組織が定めた頻度で]
   2. 物理面と環境面での保護の手順を[指定:組織が定めた頻度で]。

補足的ガイダンス:この管理策は、PE ファミリ内の選択されたセキュリティ管理策とその拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** PE-1	**中** PE-1	**高** PE-1

PE-2　物理アクセス権限

管理策:組織は、

a. 情報システムが設置されている施設に対するアクセスが許可されている個人のリストを作成・承認のうえ維持管理するのと合わせて、
b. 施設にアクセスするのに必要な許可証明書を発行するとともに、
c. 施設に対するアクセスを許可された個人を列挙したアクセスリストを[指定:組織が定めた頻度]レビューするのに加えて、
d. 施設に対するアクセスがもはや必要でない個人を、施設のアクセスリストから除外する。

補足的ガイダンス:この管理策は、組織の職員と来客に適用される。恒久的な物理アクセスの許可証明書を有する個人(例:職員・契約社員等)は、来客とはみなされない。許可証明書には、たとえば、バッジ、身分証明書、スマートカードがある。組織は、連邦政府標準・ポリシー・手順に従って、許可証明書に必要な強度(バッジ・スマートカード・身分証明書として偽造防止対策を施したものの保護レベルを含む)を決定する。この管理策は、施設内の一般の人がアクセスできる指定エリア以外のエリアに適用される。関連する管理策は、PE-3・PE-4・PS-3。

拡張管理策:

(1) 物理アクセス権限 | 地位 / 役割に基づいたアクセス

組織は、情報システムが設置されている施設への物理アクセスを、地位または役割に基づいて許可する。

補足的ガイダンス:関連する管理策は、AC-2・AC-3・AC-6。

(2) 物理アクセス | 2 つの識別形式

組織は、情報システムが設置されている施設への来客によるアクセス対して、[指定:組織が定めた、許容される識別形式のリスト]から、2 つの識別形式を選択して適用する。

補足的ガイダンス:政府発行の写真付き身分証明書として受け入れられるものには、たとえば、パスポート、PIV カード、運転免許証がある。自動化されたメカニズムを使用して施設にアクセスできるようにするための仕組みとして、組織は PIV カード、鍵カード、暗証番号、生体情報を使用できる。関連する管理策は、IA-2・IA-4・IA-5。

(3) 物理アクセス権限 | 付き添われていないアクセスを制限する

組織は、情報システムが設置されている施設に対する付添いなしのアクセスを、[選択(1つ以上):システムに含まれるすべての情報に対するセキュリティクリアランス;システムに含まれるすべての情報に対する正式なアクセス権限; システムに含まれるすべての情報にアクセスする必要性; 指定:組織が定めたクレデンシャル]]を有する個人に限定する。

補足的ガイダンス:機微度が高い機密情報を保管している施設に、十分なセキュリティクリアランス、アクセス許可、または「知る必要性」を持たない個人が入る場合には、そうした情報が目に入ったり、侵害されないようにするためにも、適切なクレデンシャルを有する個人が付き添うことが重要である。関連する管理策は、PS-2・PS-6。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** PE-2	**中** PE-2	**高** PE-2

PE-3 物理アクセス制御

管理策:組織は、

a. 以下を実施することによって、[指定:組織が定めた、情報システムが設置されている施設の入口と出口]にて、物理アクセスの許可を実施する
   1. 施設に対するアクセスを許可する前に、個人のアクセス権限を確認する
   2. [選択(1つ以上):[指定:組織が定めた、物理アクセス制御システム/機器]; ガード]を使用して、施設の入口と出口を制御する
b. [指定:組織が定めた入口/出口]に対する物理アクセスの監査ログを保持する。
c. 施設内の、一般の人がアクセスできる指定エリアに対するアクセスを制御するための、[指定:組織が定めたセキュリティ対策]を実施する。
d. [指定:組織が定めた、来客に付き添うことと、来客をモニタリングすることを必要とする状況]において、来客に付き添って、来客の行動をモニタリングする。
e. 鍵・ダイヤル錠などの物理アクセスデバイスのセキュリティを確保する。
f. [指定:組織が定めた物理アクセスデバイス]の一覧を[指定:組織が定めた頻度で]作成し直す。
g. ダイヤル錠と鍵を[指定:組織が定めた頻度で]、および/または鍵の紛失時、ダイヤル錠の侵害時、または個人の異動または退職時に変更する。

補足的ガイダンス:この管理策は、組織の職員と来客に適用される。恒久的な物理アクセスの許可証明書を有する個人(例:職員、契約社員、その他)は、来客とはみなされない。組織は、必要な施設警備員のタイプ(たとえば、プロの物理セキュリティスタッフ、または管理スタッフや情報システムユーザなどの他の人員を含む)を決定する。物理アクセスデバイスには、たとえば、鍵、錠、ダイヤル錠、カードリーダーがある。組織の施設内の、一般の人がアクセスできるエリアに対する保護対策には、たとえば、カメラ、警備員によるモニタリング、選択された情報システムおよび/またはシステムコンポーネントをセキュリティが確保されたエリアに隔離することがある。物理アクセス制御システムは、該当する連邦法・大統領命令・指令・政策・規制・標準・手引に準拠する。FICAM (Federal Identity, Credential, and Access Management) Program は、物理アクセス制御システムの ID、クレデンシャル、アクセスの管理機能の、導入の手引きを示している。組織は、使用する監査ログのタイプに関して柔軟性を有する。監査ログは、手続きに関するものであったり(例:個人が施設にアクセスした際に書き込まれるログ)、自動化されたものであったり(例:PIV カードによって示される ID を記録する)、あるいは、それらの組み合わせであったりする。物理アクセスポイントには、施設に対するアクセスポイント、補足的なアクセス制御を必要とする情報システムおよび/またはコンポーネントへの内部アクセスポイント、あるいは、それらの両方がある。組織の情報システムのコンポーネント(例:ワークステーション、端末)は、一般の人がアクセスできる指定エリアに置かれる場合があるが、その場合、機器に対するアクセスを組織が保護する必要がある。関連する管理策は、AU-2・AU-6・MP-2・MP-4・PE-2・PE-4・PE-5・PS-3・RA-3。

拡張管理策:

(1) 物理アクセス制御 | 情報システムに対するアクセス

組織は、施設内の[指定:組織が定めた、情報システムの 1 つ以上のコンポーネントが設置されている物理的な空間]において、施設に対する物理アクセス制御と、情報システムに対する物理アクセス制御を実施する。

補足的ガイダンス:この拡張管理策は、施設内の、情報システムコンポーネントが集中しているエリア(例:サーバールーム、媒体が保管されているエリア、データおよび通信センター)に対する追加の物理セキュリティをもたらす。関連する管理策は、PS-2。

(2) 物理アクセス制御 | 施設 / 情報システムの境界

組織は、施設または情報システムの物理的境界におけるセキュリティチェックを[指定:組織が定めた頻度で]実施して、情報の不正な引き出しや、情報システムコンポーネントの不正な削除の有無を確認する。

補足的ガイダンス:組織は、引き出しに関するリスクを十分に軽減するためのセキュリティチェックの範囲、頻度、および/またはランダムさを決定する。関連する管理策は、AC-4・SC-7。

(3) 物理アクセス制御 | 警備員 / アラームによる、継続的なモニタリング

組織は、警備員および/またはアラームを使用して、情報システムが設置されている施設に対する物理アクセスポイントの各々を、1 日 24 時間、1 週 7 日間継続してモニタリングする。

補足的ガイダンス:関連する管理策は、CP-6・CP-7。

(4) 物理アクセス制御 | 鍵のついている箱

組織は、鍵のついている箱を使用して、[指定:組織が定めた情報システムコンポーネント]を不正な物理アクセスから保護する。

(5) 物理アクセス制御 | 改ざん防止

組織は、情報システム内の[指定:組織が定めたハードウェアコンポーネント]の物理的な改ざん、または改変を[選択(1つ以上):検出する; 防止する]ために、[指定:組織が定めたセキュリティ対策]を用いる。

補足的ガイダンス：組織には、選択されたハードウェアコンポーネントにおいて改ざんを検出／防止する、あるいは、改ざんを検出するためのコンポーネントと改ざんを防止するためのコンポーネントを分ける、といった選択肢がある。改ざんの検出／防止作業では、たとえば、改ざんの検知用のシール、改ざん防止のためのコーティングなど、多様な改ざん防止技術を使用できる。改ざん防止プログラムは、偽造や、サプライチェーン関連の他のリスクによるハードウェアの改変を検出するのに役立つ。関連する管理策：SA-12。

(6) 物理アクセス制御 | 施設に対する侵入テスト

組織は、施設の物理アクセスポイントにおいて実施されるセキュリティ管理策を擦り抜ける／回避するといった試みを、[指定：組織が定めた頻度で]、アナウンスすることなく実施することを含む、侵入テストプロセスを用いる。

補足的ガイダンス：関連する管理策は、CA-2・CA-7

参考文献：FIPS Publication 201・NIST Special Publications 800-73・NIST Special Publications 800-76・NIST Special Publications 800-78・NIST Special Publications 800-116・ICD 704・ICD 705・DoD Instruction 5200.39・Personal Identity Verification (PIV) in Enterprise Physical Access Control System (E-PACS)・ウェブサイト http://idmanagement.gov および http://fips201ep.cio.gov

優先順位とベースライン管理策の割り当て：

P1	**低** PE-3	**中** PE-3	**高** PE-3 (1)

PE-4 伝送媒体に対するアクセス制御

管理策：組織は、組織の施設内の[指定：組織が定めた、情報システムの配電線および伝送回線]に対する物理アクセスを、[指定：組織が定めたセキュリティ対策]を用いて制御する。

補足的ガイダンス：情報システムの配電線および伝送回線に適用される物理面でのセキュリティ対策は、事故による損傷、途絶、物理的な改ざんから保護するのに役立つ。また、物理面での対策は、情報が暗号化されていない状態で伝送される間に盗聴されたり、改変されることを防止するためにも必要である。システムの配電線および伝送回線に対する物理アクセスを制御するためのセキュリティ対策には、たとえば、以下がある：①鍵が掛かったワイヤークローゼット②切り離された、または鍵が掛かった予備ジャックおよび／または③電線管またはケーブルトレイによる配線の保護。関連する管理策は、MP-2・MP-4・PE-2・PE-3・PE-5・SC-7・SC-8。

拡張管理策：なし

参考文献：NSTISSI No. 7003

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** PE-4	**高** PE-4

PE-5 出力装置に対するアクセス制御

管理策：組織は、情報システムの出力装置に対する物理アクセスを制御して、権限のない個人が、装置からの出力情報を取得できないようにする。

補足的ガイダンス：出力装置に対する物理アクセスの制御には、たとえば、出力装置を鍵が掛かった部屋などの、セキュリティが確保されたエリアに置くこと、権限を与えられた個人にのみアクセスを許可すること、出力装置を組織の職員がモニタリングできる場所に置くことがある。情報システムの出力装置には、モニター、プリンター、コピー機、スキャナー、ファクシミリ装置、オーディオ装置などがある。関連する管理策は、PE-2・PE-3・PE-4・PE-18。

拡張管理策:

(1) 出力装置に対するアクセス制御 | 許可された個人による、出力情報のアクセス

組織は、

(a) [指定:組織が定めた出力装置]からの出力情報に対する物理アクセスを制御する

(b) 許可された個人のみが、装置からの出力情報を受け取れるようにする。

補足的ガイダンス:選択された出力装置に対する物理アクセスの制御には、たとえば、プリンター、コピー機、ファクシミリ装置をキーバッドによってアクセスが制御される、管理された領域に置くことや、特定のタイプのバッジを持つ個人にアクセスを限定することが含まれる。

(2) 出力装置に対するアクセス制御 | 個別の ID による出力情報のアクセス

情報システムは:

(a) [指定:組織が定めた出力装置]からの出力情報に対する物理アクセス を制御する

(b) 個人の識別情報と、装置からの出力情報を受け取る者を対応付ける。

補足的ガイダンス:選択された出力装置に対する物理アクセスの制御には、たとえば、プリンター、コピー機、ファクシミリ装置からの出力情報が個人に開示される前に、組織が暗証番号やハードウェアトークンなどを使用して、それらの出力装置上で認証を行うことを可能にするセキュリティ機能を装置にインストールすることを含む。

(3) 出力装置に対するアクセス制御 | 出力装置のマーキング

組織は、[指定:組織が定めた情報システムの出力装置]に対して、その情報が装置からの出力が許可されている旨を示す、適切なセキュリティマークを付ける。

補足的ガイダンス:出力装置には、たとえば、プリンター・モニター・ファクシミリ装置・スキャナー・コピー機・オーディオ装置がある。この拡張管理策は、通常、携帯機器以外の、情報システム出力装置に適用される。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** PE-5	**高** PE-5

PE-6 物理アクセスのモニタリング

管理策:組織は、

a. 情報システムが設置されている施設に対する物理アクセスをモニタリングすることによって、物理的なセキュリティインシデントを検出し、対応できるようにするとともに、

b. 物理アクセスログを[指定:組織が定めた頻度で]、また、[指定:組織が定めたイベントが発生した場合や、イベントの兆候がある場合]にレビューするのに加えて、

c. レビューと調査の結果について、組織のインシデント対応チームとの間で整理する。

補足的ガイダンス:組織のインシデント対応チームの役割は、確認された物理的なセキュリティインシデントに対する調査と対応を含む。セキュリティインシデントには、たとえば、明らかなセキュリティ違反、または疑わしい物理アクセス活動がある。疑わしい物理アクセス活動には、たとえば、以下がある:①通常の勤務時間外のアクセス②通常はアクセスされないエリアに対する度重なるアクセス③異常に長い時間にわたるアクセスならびに④順序が正しくないアクセス。関連する管理策は、CA-7・IR-4・IR-8。

拡張管理策:

(1) 物理アクセスのモニタリング | 侵入に対する警報 ／ 監視装置

組織は、物理的な侵入に対する警報と監視装置をモニタリングする。

(2) 物理アクセスのモニタリング | 自動化された、侵入検知 / 対応

組織は、[指定:組織が定めたクラス／タイプの侵入]を検知し、[指定:組織が定めた対応措置]を行うための、自動化されたメカニズムを使用する。

補足的ガイダンス:関連する管理策は、SI-4。

(3) 物理アクセスのモニタリング | ビデオ監視

組織は、[指定:組織が定めた作動エリア]に対するビデオ監視を実施し、ビデオ記録を[指定:組織が定めた期間]にわたって保管する。

補足的ガイダンス:この「管理策の強化」は、監視ビデオによる記録を保管し、状況により必要な場合(例:他の手段によって侵入が検知された場合)には、レビューを実施することに焦点を当てている。組織がビデオ監視を実施することを選択するケースもあるが、この「管理策の強化」は、そうすることを要求していない。ビデオ監視を実施し、記録を保管するにあたっては、とりわけそうした監視が公共の場で行われる場合には、法律上考慮すべき事項があることに留意すること。

(4) 物理アクセスのモニタリング | 情報システムに対する物理アクセスをモニタリングする

組織は、[指定:組織が定めた、情報システムの 1 つ以上のコンポーネントが設置されている物理的な空間]である施設に対する、物理アクセスのモニタリングに加えて、情報システムに対する物理アクセスのモニタリングを実施する。

補足的ガイダンス:この拡張管理策は、施設内の、情報システムコンポーネントが集中している施設(例:サーバールーム・通信センターとともに、媒体が保管されているエリア)に対する、追加のモニタリングをもたらす。関連する管理策は、PS-2・PS-3。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** PE-6	**中** PE-6 (1)	**高** PE-6 (1) (4)

PE-7 来客の管理

[削除された:PE-2 および PE-3 に統合された]

PE-8 来客のアクセス記録

管理策:組織は、

a. 情報システムが設置されている施設に対する来客のアクセス記録を、[指定:組織が定めた期間]にわたって保管するとともに、

b. 来客のアクセス記録を[指定:組織が定めた頻度で]レビューする。

補足的ガイダンス:来客のアクセス記録は、たとえば、来客の氏名と所属組織、来客による署名、身分証明書、訪れた日、入退出の時刻、訪れた目的、および来訪を受けた人の氏名と所属組織を含む。一般の人がアクセスできるエリアに対していは、来客のアクセス記録は必要でない。

拡張管理策:

(1) 来客のアクセス記録 | 記録を自動で保管 / レビューする

組織は、来客のアクセス記録の保管とレビューを容易にするための、自動化されたメカニズムを使用する。

(2) 来客のアクセス記録 | 物理アクセス記録

[削除された:PE-2 に統合された]

参考文献:なし

優先順位とベースライン管理策の割り当て:

P3	**低** PE-8	**中** PE-8	**高** PE-8 (1)

PE-9 電力設備と電力ケーブル

管理策:組織は、情報システムの電力設備と電力ケーブルを損傷および破壊から保護する。

補足的ガイダンス:組織は、組織の施設や、システムが稼働する環境の内部と外部の両方の異なるロケーションで使用されている、電力設備と電力ケーブルに必要なタイプの保護について決定する。これは、たとえば、建物の外側の発電機と電力ケーブル、オフィスまたはデータセンター内の内部ケーブルと無停電電源、および乗り物や人工衛星などの自己完結的なエンティティ向けの電源を含む。関連する管理策は、PE-4。

拡張管理策:

(1) 電力設備と電力ケーブル | 予備ケーブル

組織は、[指定:組織が定めた距離]にわたって物理的に離れている、予備の電力ケーブル経路を使用する。

補足的ガイダンス:物理的に離れている、予備の電力ケーブルは、ケーブルの1つが切れてしまったり、損傷した場合でも、電力が流れるようにするのに役立つ。

(2) 電力設備と電力ケーブル | 自動電圧制御

組織は、[指定:組織が定めた、極めて重要な情報システムコンポーネント]に対して自動電圧制御を導入する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** PE-9	**高** PE-9

PE-10 緊急遮断

管理策:組織は、

a. 緊急時に、情報システムまたは個々のシステムコンポーネントの電源を遮断できる機能を提供するとともに、

b. 緊急時 の遮断用スイッチまたは装置を[指定:組織が定めた、情報システムまたはシステムコンポーネントに近い場所]に置くことによって、職員が安全に、かつ簡単にアクセスできるようにするのに加えて、

c. 緊急時に電源を遮断する機能が、不正に起動されないようにする。

補足的ガイダンス:この管理策は、主に、情報システムリソースが集中している施設(たとえば、データセンター、サーバールーム、メインフレームコンピュータルームなど)に適用される。関連する管理策は、PE-15。

拡張管理策:

(1) 緊急遮断 | 偶発的な / 不正なアクティブ化

[削除された:PE-10 に統合された]

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** PE-10	**高** PE-10

PE-11 非常用電源

管理策:組織は、一次電源が失われた場合に、[選択(1つ以上):情報システムの所定のシャットダウン;情報システムの、長期間使用可能な代替電源への切り替え]を支援する、短期無停電電源装置を用意する。

補足的ガイダンス:関連する管理策は、AT-3・CP-2・CP-7。

拡張管理策:

(1) 非常用電源 | 長期間使用可能な代替電源 - 最低限必要な業務能力

組織は、情報システム用の一次電源が長期間失われた場合に、システムが最低限必要な運用能力を維持できるよう、長期間使用可能な代替電源を用意する。

補足的ガイダンス:この拡張管理策は、たとえば、二次的な商用の電源や、その他の外部電源を使用することで満たせるようになる。情報システム用の長期間使用可能な代替電源は、手動か自動のいずれかで、入れることが可能である。

(2) 非常用電源 | 長期間使用可能な代替電源 - 自己完結

組織は、以下の特徴を持つ、情報システム用の長期間使用可能な代替電源を用意する:

(a) 自己完結型である

(b) 外部発電に依存しない

(c) 一次電源が長期間失われる場合に、[選択:最低限必要な運用能力; 最大限の運用能力]を維持することが可能である。

補足的ガイダンス:この拡張管理策は、たとえば、組織のニーズを満たすのに十分な能力を備えた、1 つ以上の発電機を使用することによって満たされる。組織の情報システム用の長期間使用可能な代替電源は、手動か自動のいずれかで、入れることが可能である。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** PE-11	**高** PE-11 (1)

PE-12 非常用照明

管理策:組織は、停電が発生した場合や、電力が途絶えた場合に作動し、施設内の非常口と避難経路を照らす自動非常用照明を情報システムに導入し、維持する。

補足的ガイダンス:この拡張管理策は、主に、情報システムリソースが集中している施設(たとえば、データセンター・サーバールーム・メインフレームコンピュータルームなど)に適用される。関連する管理策は、CP-2・CP-7。

拡張管理策:

(1) 非常用照明 | 極めて重要なミッション / 業務機能

組織は、施設内の極めて重要なミッション／業務機能を支援するすべてのエリアに、非常用照明を設置する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** PE-12	**中** PE-12	**高** PE-12

PE-13 防火

管理策:組織は、独立したエネルギー源によってサポートされる、消火および火災検知のための装置／システムを情報システムに導入し、維持する。

補足的ガイダンス:この管理策は、主に、情報システムリソースが集中している施設(たとえば、データセンター、サーバールーム、メインフレームコンピュータルームなど)に適用される。消火および火災検知のための装置／システムには、たとえば、スプリンクラー装置、手持ち式の消火器、固定式消火ホース、煙探知器がある。

拡張管理策:

(1) 防火 | 火災検知器 / システム

組織は、火災発生時に自動的に作動し、[指定: 組織が定めた職員または役職]と、[指定:組織が定めた緊急対応者]に知らせる、火災検知器／システムを導入する。

補足的ガイダンス:組織は、通知リストに記載されている個人が、たとえば機密扱いの業務が行われている施設、あるいは機密扱いの情報を含む情報システムが設置されている施設に対するアクセスを得るための、適切なアクセス権限および／またはクリアランスを有するイベントが発生した場合に備えて、該当する職員、役割、および緊急時対応者を指定することができる。

(2) 防火 | 消火器 / システム

組織は、作動時に[指定: 組織が定めた職員または役職]と、[指定:組織が定めた緊急対応者]に自動通知する、消火器／システムを導入する。

補足的ガイダンス:組織は、通知リストに記載されている個人が、たとえば機密扱いの作業が行われている施設、あるいは機密扱いの情報を含む情報システムが設置されている施設に対するアクセスを得るための適切なアクセス権限および／またはクリアランスを有するイベントが発生した場合に備えて、該当する職員、役割、および緊急時対応者を指定することができる。

(3) 防火 | 自動消火

組織は、情報システムが設置されている施設に職員が常駐しない場合には、自動消火機能を導入する。

(4) 防火 | 点検

組織は、施設が、権限を与えられている、資格のある点検者による[指定:組織が定めた頻度]の点検を受けるようにし、特定された欠陥を[指定:組織が定めた期間]内に解消する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** PE-13	**中** PE-13 (3)	**高** PE-13 (1) (2) (3)

PE-14 温度および湿度の管理

管理策:組織は、

a. 情報システムが設置されている施設内の温度と湿度を[指定:組織が定めた許容レベル]に保つ

b. 温度と湿度を[指定:組織が定めた頻度で]モニタリングする。

補足的ガイダンス:この管理策は、主に、情報システムリソースが集中している施設(たとえば、データセンター、サーバールーム、メインフレームコンピュータルームなど)に適用される。関連する管理策は、AT-3。

拡張管理策:

(1) 温度および湿度の管理 | 自動化された制御

組織は、施設の温度と湿度を自動制御する仕組みを導入することによって、情報システムに害を及ぼす可能性のある変動を防止する。

(2) 温度および湿度の管理 | 警告/通知を伴うモニタリング

組織は、温度と湿度をモニタリングする仕組みを導入することによって、職員または機器に害を及ぼす可能性のある変動があった場合に、警告を発する、または通知が行われるようにする。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** PE-14	**中** PE-14	**高** PE-14

PE-15 浸水による被害からの保護

管理策:組織は、主要職員がその存在を知っていて利用できる、正しく機能しているマスター閉止弁/遮断弁を用意することによって、情報システムを水漏れに起因する被害から保護する。

補足的ガイダンス:この管理策は、主に、情報システムリソースが集中している施設(たとえば、データセンター、サーバールーム、メインフレームコンピュータルームなど)に適用される。遮断弁は、組織全体に影響を与えることなく懸念されるエリアでの給水を止めるために、マスター閉止弁と併用する、あるいはその代わりに使用することができる。関連する管理策は、AT-3。

拡張管理策:

(1) 浸水による被害からの保護 | 自動化を支援する

組織は、情報システムの周辺の水の存在を検知するための自動化されたメカニズムを使用し、検知された場合には[指定:組織が定めた職員または役職]に知らせる。

補足的ガイダンス:自動化されたメカニズムには、たとえば、水検出用センサー・アラーム・通知システムが含まれる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** PE-15	**中** PE-15	**高** PE-15 (1)

PE-16 搬入と搬出

管理策:組織は、施設に搬入・搬出される[指定:組織が定めたタイプの情報システムコンポーネント]に対して許可・未許可、モニタリング、および管理を行い、それらのアイテムについての記録を保管する。

補足的ガイダンス:情報システムコンポーネントの搬入と搬出に対する許可・未許可を効果的に実施するには、搬入・搬出エリアに対するアクセスを制御することや、場合によってはそうしたエリアを情報システムおよびメディアライブラリから切り離すことが必要になるだろう。関連する管理策は、CM-3・MA-2・MA-3・MP-5・SA-12。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** PE-16	**中** PE-16	**高** PE-16

PE-17 代替の仕事場

管理策:組織は、

a. 代替の仕事場に[指定:組織が定めたセキュリティ管理策]を導入する
b. 代替の仕事場におけるセキュリティ管理策の有効性を、実現可能な限りアセスメントする
c. セキュリティインシデント発生時または問題発生時に、職員が情報セキュリティ責任者と連絡を取り合う手段を用意する。

補足的ガイダンス:代替の仕事場は、たとえば、政府施設や職員の私邸を含む場合がある。代替の仕事場は、通常は代替処理拠点と区別されるが、緊急時対応の一環としてすぐに利用できる代替の場所となる。組織は、特定の代替の仕事場や、仕事場のタイプごとに、それらの場所で実施される仕事関連の作業に応じて異なるセキュリティ管理策セットを定義してもよい。本管理策は、組織の緊急時対応計画に伴う活動と、連邦政府の在宅勤務への取り組みを支援する。関連する管理策は、AC-17・CP-7。

拡張管理策:なし

参考文献:NIST Special Publication 800-46

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** PE-17	**高** PE-17

PE-18 情報システムコンポーネントの設置場所

管理策:組織は、[指定:組織が定めた物理面と環境面でのハザード]によってもたらされる被害を最小限に抑えて、かつ、不正アクセスの機会を最小限に抑えられるよう、施設内の適切な場所に情報システムコンポーネントを設置する。

補足的ガイダンス：物理面と環境面でのハザードには、たとえば、洪水、火災、竜巻、地震、ハリケーン、テロ行為、公共物破壊、電磁パルス、電気的干渉、およびその他の形態の入射する電磁放射線がある。さらに組織は、アクセスが許可されていない個人が情報システムに接近できてしまい、その結果として組織の通信が（例：ワイヤレススニファーやマイクを使用して）不正にアクセスされる可能性が高まる、物理的な入口についても考慮する。関連する管理策は、CP-2・PE-19・RA-3。

拡張管理策：

(1) 情報システムコンポーネントの設置場所 | 施設内の設置場所

組織は、施設内の、情報システムの設置場所を計画する際には、物理面と環境面でのハザードを考慮する。また、既存の施設については、組織のリスク緩和戦略において物理面と環境面でのハザードを考慮する。

補足的ガイダンス：関連する管理策は、PM-8。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P3	**低** 選択されていない	**中** 選択されていない	**高** PE-18

PE-19 情報漏えい

管理策：組織は、電磁信号の放射によって情報システムを情報漏えいから保護する。

補足的ガイダンス：情報が漏れるということは、電磁信号の放射によって、情報が信頼できない環境に意図的に、あるいは誤ってリリースされることである。情報システムのセキュリティカテゴリまたは分類レベル（機密性に関して）と、組織のセキュリティポリシーによって、電磁信号の放射によって情報が漏れることからシステムを保護するためのセキュリティ管理策が導出される。

拡張管理策：

(1) 情報が漏れること | 排気と暴風雨に関する国家のポリシーと手順

組織は、情報システムコンポーネントおよび関連するデータ通信ならびにネットワークが情報のセキュリティカテゴリまたは分類レベルに基づいて、排気と暴風雨に関する国家のポリシーと手順に従って保護されるようにする。

参考文献：FIPS Publication 199

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

PE-20 資産のモニタリングと追跡

管理策：組織は、

a. ［指定：組織が定めた、管理された領域］内での［指定：組織が定めた資産］の位置や移動を追跡し、モニタリングするための［指定：組織が定めた、資産の位置技術］を使用するとともに、

b. 資産の位置技術が、該当する連邦法・大統領命令・指令・規制・政策・標準・手引に従って使用されるようにする。

補足的ガイダンス：資産の位置技術は、乗り物または重要な情報システムコンポーネントなどの極めて重要な資産が、許可されている場所に保管されるのを支援する。組織は、資産の位置技

術の導入と使用に関して、プライバシー問題に対処するために、法律顧問室と、政府機関の上級プライバシー責任者／最高プライバシー責任者に助言を求める。関連する管理策は、CM-8。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:計画作成

PL-1　セキュリティ計画のポリシーと手順

管理策:組織は、

a. 以下を策定、文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、セキュリティ計画のポリシー
   2. セキュリティ計画のポリシーと、関連する「セキュリティ計画」管理策の実施を容易にするための手順

b. 以下の最新版をレビューし、更新する:
   1. セキュリティ計画保護のポリシーを[指定:組織が定めた頻度で]
   2. セキュリティ計画の手順を[指定:組織が定めた頻度で]

補足的ガイダンス:この管理策は、PL ファミリ内の選択されたセキュリティ管理策とその拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-18・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** PL-1	**中** PL-1	**高** PL-1

PL-2　システムセキュリティ計画

管理策:組織は、

a. 以下を満たす、情報システムのセキュリティ計画を作成する:
   1. 組織のエンタープライズアーキテクチャに適合する
   2. システムに対する認可を出す範囲を明示的に定義する
   3. ミッション／業務プロセスの観点から、情報システムをどのように使用できるかについて説明する
   4. 情報システムのセキュリティカテゴリを、裏付けとなる根拠と共に示す
   5. 情報システムが稼働する環境と、他の情報システムとの関係またはつながりを示す
   6. システムのセキュリティ要求事項の概要を示す
   7. 関連するすべてのオーバーレイを示す(該当する場合)
   8. それらの要求事項を満たすために導入されている、または導入が計画されているセキュリティ管理策について(調整に関する意思決定の根拠を含めて)記述する

9. 計画の実施に先立ち、運用認可責任者または運用認可責任者が指定した代表者によってレビューされ、承認される

b. セキュリティ計画のコピーを[指定: 組織が定めた職員または役職]に配布し、その後の変更について通知する

c. 情報システムのセキュリティ計画を[指定:組織が定めた頻度で]レビューする

d. 情報システムの変化／システムが稼働する環境の変化や、計画の実施またはセキュリティ管理策のアセスメント時に特定された問題に対処するために、計画を更新する

e. セキュリティ計画を、不正な開示や変更から保護する。

補足的ガイダンス:セキュリティ計画は、セキュリティ要求事項と、一連のセキュリティ管理策およびその拡張管理策を関連付ける。セキュリティ計画は、また、高レベルで、セキュリティ管理策とその拡張管理策がどのようにして、それらのセキュリティ要求事項を満たすかについて説明する。ただし、それらの管理策／拡張管理策の設計または導入についての詳細な技術的解説は行わない。セキュリティ計画は、計画の意図に、また、計画が意図された通りに実施された場合の組織の業務と資産、個人、他の組織、および国家に対するリスクの判断結果に明確に準拠する設計と導入を可能にするための、十分な情報(「指定ステートメント」と「選択ステートメント」のパラメータ値を明示的に、あるいは参照によって示すことを含む)を含む。組織は、また、コミュニティ全体にわたって使用できるオーバーレイを策定するために、あるいは特定の要求事項、技術、またはミッション／システムが稼働する環境(例:DoD-tactical、連邦公開鍵基盤、FICAM、宇宙活動)に対処するために、付録 D と CNSS Instruction 1253 のセキュリティ管理策ベースラインに調整に関するガイダンスを適用することができる。付録 I は、オーバーレイの策定に関する手引きである。

セキュリティ計画は、単一のドキュメントである必要はない。セキュリティ計画は、既存のドキュメントを含む、さまざまなドキュメントの集合であってもよい。効果的なセキュリティ計画は、ポリシー、手順、および、より詳細な情報が得られる追加のドキュメント(例:設計と導入についての仕様書)への参照を広く利用する。これにより、セキュリティプログラムに関連するドキュメント要件を減らすことができ、セキュリティ関連の情報をエンタープライズアーキテクチャ、システム開発ライフサイクル、システムエンジニアリング、および調達に関連する確立された管理／運用区域に保管できるようになる。たとえば、セキュリティ計画は、緊急時対応計画またはインシデント対応計画についての詳細情報を含まないが、代わりにそれらの計画によって成し遂げられるべきものを定義するための、十分な情報を明示的に、あるいは参照によって提供する。関連する管理策は、AC-2・AC-6・AC-14・AC-17・AC-20・CA-2・CA-3・CA-7・CM-9・CP-2・IR-8・MA-4・MA-5・MP-2・MP-4・MP-5・PL-7・PM-1・PM-7・PM-8・PM-9・PM-11・SA-5・SA-17。

拡張管理策:

(1) システムセキュリティ計画 | 運用概念

[削除された:PL-7 に統合された]

(2) システムセキュリティ計画 | 機能アーキテクチャ

[削除された:PL-8 に統合された]

(3) システムセキュリティ計画 | 組織内の他のエンティティ(部署、グループ、人、)と共に計画し、調整を行う

組織は、情報システムに影響を与えるセキュリティ関連の活動に関して、そうした活動を実施する前に[指定:組織が定めた個人またはグループ]との間で活動を計画・調整することによって、組織内の他の部署に対する影響を減らす。

補足的ガイダンス:セキュリティ関連の活動は、たとえば、セキュリティアセスメント、監査、ハードウェアとソフトウェアのメンテナンス、パッチ管理、および緊急時対応計画のテストを含む。事前の計画作成および調整は、緊急な場合と緊急でない場合がある (すなわち、計画されていた、あるいは急を要さない、計画されていたわけではない)。セキュリティ関連の

活動を計画し、調整するために組織が定義するプロセスは、情報システムのセキュリティ計画に、あるいは必要に応じて他のドキュメントに記載される。関連する管理策は、CP-4・IR-4.。

参考文献：NIST Special Publication 800-18

優先順位とベースライン管理策の割り当て：

P1	**低** PL-2	**中** PL-2 (3)	**高** PL-2 (3)

PL-3 システムセキュリティ計画の更新

[削除された：PL-2 に統合された]

PL-4 行動規範

管理策：組織は、

a. 情報システムに対するアクセスを要求する個人に対して、情報と情報システムの使用に関する彼らの責任と期待される振る舞いを記したルールを作成し、すぐに利用できるようにするのと合わせて、

b. そうした個人に情報と情報システムに対するアクセスを許可する前に、彼らが行動規範を読んで理解したことと、行動規範に従うことに同意したことを示す署名による同意を得るとともに、

c. 行動規範を［指定：組織が定めた頻度で］レビューし、更新するのに加えて、

d. 行動規範が修正／更新された場合に、以前のバージョンの行動規範に署名した個人に対して、新しい行動規範を読んで、再度署名することを要求する。

補足的ガイダンス：この拡張管理策は、組織的ユーザに適用される。組織は、個人ユーザの役割と責任に基づいて行動規範を検討する（たとえば、特権ユーザに適用される行動規範と、一般ユーザに適用される行動規範を分けるなど）。たとえば、連邦政府の情報システムからデータ／情報を受け取るだけの個人を含む、なんらかのタイプの「組織的ユーザ以外のユーザ」に対する行動規範を規定することは、そうしたユーザが大勢いることと、システムとのやりとりも限られていることから、実現可能でないことが多い。組織的ユーザと「組織的ユーザ以外のユーザ」の両方に対する行動規範は、AC-8 (System Use Notification)において規定することも可能である。PL-4 b.（この管理策の「署名による同意」の部分）は、組織が実施するセキュリティ意識向上トレーニングと、役割に基づいたセキュリティトレーニングが行動規範を含むのであれば、それらのトレーニングによって満たされるだろう。組織は、行動規範の同意に関して、電子署名を使用することができる。関連する管理策は、AC-2・AC-6・AC-8・AC-9・AC-17・AC-18・AC-19・AC-20・AT-2・AT-3・CM-11・IA-2・IA-4・IA-5・MP-7・PS-6・PS-8・SA-5。

拡張管理策：

(1) 行動規範 | ソーシャルメディア / ネットワーキングの制限

組織は、行動規範に、ソーシャルメディア／ネットワーキングサイトの利用と、組織の情報をパブリックなウェブサイトに載せることに対する明確な制限を含める。

補足的ガイダンス：この拡張管理策は、以下に該当する場合の、ソーシャルメディア／ネットワーキングサイトの使用に関連する行動規範を扱う：①組織の職員が職務のために、あるいは職務を遂行するために、そうしたサイトを使用している場合②組織の情報がソーシャルメディア／ネットワーキングのトランザクションに関与する場合③職員が組織の情報システムからソーシャルメディア／ネットワーキングサイトにアクセスしている場合。組織は、また、権限のないエンティティが組織のパブリックでない情報（例：システムアカウント情報・個

人情報）をソーシャルメディア／ネットワーキングサイトから取得する、および／または推測するのを防止するための、具体的なルールを作成する。

参考文献：NIST Special Publication 800-18

優先順位とベースライン管理策の割り当て：

P2	**低** PL-4	**中** PL-4 (1)	**高** PL-4 (1)

PL-5 プライバシー影響のアセスメント

[削除された：AR-2 の付録 J に統合された]

PL-6 セキュリティ関連活動の計画作成

[削除された：PL-2 に統合された]

PL-7 セキュリティの観点からの運用概念

管理策：組織は、

a. 情報システムの、セキュリティの観点からの運用概念をまとめる（なお、このコンセプトは、少なくとも組織が情報セキュリティの観点から、情報システムをどのように運用するかを含む）とともに、

b. 運用概念を［指定：組織が定めた頻度で］レビューし、更新する。

補足的ガイダンス：セキュリティの観点からの運用概念は、情報システムのセキュリティ計画に、または必要に応じてシステム開発ライフサイクル関連の他のドキュメントに含まれる。運用概念に対する変更は、セキュリティ計画、情報セキュリティアーキテクチャ、および組織の他の適切なドキュメント（例：資材調達／調達におけるセキュリティ仕様書、システム開発ライフサイクルに関するドキュメント、およびシステム／セキュリティエンジニアリングに関するドキュメント）に対する後続の更新に反映される。関連する管理策は、PL-2。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

PL-8 情報セキュリティアーキテクチャ

セキュリティ管理策：組織は、

a. 以下を満たす、情報システムの情報セキュリティアーキテクチャを策定する：

1. 組織の情報の機密性、完全性、および可用性を保護するのに使用できる全般的な方針、要求事項、およびアプローチについて記述する
2. 情報セキュリティアーキテクチャがどのようにしてエンタープライズアーキテクチャに組み入れられるか、また、どのようにしてエンタープライズアーキテクチャを支援するかについて記述する
3. 外部サービスの情報セキュリティに関する想定と、それらのサービスへの依存について記述する

b. エンタープライズアーキテクチャに対する更新を反映するために、情報セキュリティアーキテクチャを[組織が定めた頻度で]レビューし、更新する

c. 予定されている、情報セキュリティアーキテクチャに対する変更が、セキュリティ計画、セキュリティの観点からの運用概念、および組織の資材調達／調達に反映されるようにする。

補足的ガイダンス:このセキュリティ管理策は、組織が情報システムの設計と開発において取れるアクションを取り扱う。個々の情報システムレベルでの情報セキュリティアーキテクチャは、エンタープライズアーキテクチャにとって不可欠でありその一部として策定される、PM-7 のセキュリティ管理策に記載されている、よりグローバルな、組織全体にわたる情報セキュリティアーキテクチャに適合し、そのアーキテクチャを補足する。その情報セキュリティアーキテクチャは、アーキテクチャ記述、セキュリティ機能(セキュリティ管理策を含む)の設置／割り当て、外部インターフェースのセキュリティに関連する情報、インターフェース間で交換される情報、各インターフェースに関連する保護メカニズムを含む。また、そのセキュリティアーキテクチャは、たとえば、それぞれの役割に割り当てられたユーザーロールとアクセス権限、独自のセキュリティ要求事項、情報システムによって処理、保存、伝送される情報、情報と情報システムサービスの復旧の優先順位、および他の具体的な保護ニーズなどの、他の重要なセキュリティに関連する情報を含む場合がある。

今日の近代的なアーキテクチャでは、組織がすべての情報資源を管理することは少なくなってきている。外部の情報サービスとサービスプロバイダに大きく依存する部分も出てくるだろう。情報セキュリティアーキテクチャにおけるこうした依存について記述する事は、包括的なミッション／業務保護戦略を策定する上で重要になる。組織の情報システムのベースライン構成を規定、開発、文書化し、構成管理下に置く事は、効果的な情報セキュリティアーキテクチャを導入し、維持する上で不可欠である。情報セキュリティアーキテクチャの策定は、プライバシー要件をサポートするのに必要なセキュリティ管理策が特定され、効果的に導入されるようにするためにも、政府機関の上級プライバシー責任者／最高プライバシー責任者との間で調整がなされる。PL-8 のセキュリティ管理策は、主に、組織が情報システムに対する情報セキュリティアーキテクチャを策定するのを支援し、かつ、組織全体にわたる情報セキュリティアーキテクチャを介して、セキュリティアーキテクチャがエンタープライズアーキテクチャに組み入れられ、密につながるようにするために用意されている管理策である(すなわち、内部に焦点が置かれている)。これとは対照的に、SA-17 のセキュリティ管理策は、主に外部の IT 製品／システム開発者およびインテグレータ向けに用意された管理策である(SA-17 のセキュリティ管理策は、社内でのシステム開発時に、組織内で内部的に使用することができるが)。PL-8 の管理策への補足となる SA-17 の管理策は、組織が情報システムまたは情報システムコンポーネントの開発を外部組織に委託する場合に選択されるが、組織のエンタープライズアーキテクチャと情報セキュリティアーキテクチャに適合することを示す必要がある。関連するセキュリティ管理策:CM-2・CM-6・PL-2・PM-7・SA-5・ SA-17,付録 J。

拡張管理策:

(1) 情報セキュリティアーキテクチャ | 深層防護

以下を満たす「深層防護」のアプローチを使用して、セキュリティアーキテクチャを組織が設計する:

(a) [指定:組織が定めたセキュリティ対策]を[指定:組織が定めたロケーションとアーキテクチャ層]に割り当てる

(b) 割り当てられたセキュリティ対策が、協調的かつ相互に補強し合う形で機能するようにする。

補足的ガイダンス:組織は、セキュリティ対策(手続き面、技術面、あるいはその両方)をセキュリティアーキテクチャに戦略的に割り当てることによって、敵対者がいくつもの対策を打ち破らない限り、自身の目的を達成できないようにする。敵対者がいくつものメカニズムを打ち破らなければならないようにすれば、敵対者にとっては、極めて重要な情報資源を成

功裏に攻撃することがより困難になり（すなわち、敵対者の作業要因が増える）、攻撃が検出される可能性も増加する。割り当てられた対策の調整は、1つの対策が関与する攻撃が、他の対策に支障をきたし、意図しない悪影響（例：ロックアウト、アラームの連鎖反応）を引き起こさないようにするためにも重要である。セキュリティ対策の導入は、重要な活動である。資産の重要度が高い、あるいは情報の価値が高い場合には、層を追加するに値する。したがって、組織は、（組織の）境界層・電子メール／ウェブサーバー・ノートパソコン・ワークステーションにウイルス対策ソフトを導入することによって、敵対者が情報と情報システムを侵害するために打ち破らなければならない関連対策の数を最大にすることができる。関連する管理策は、SC-29・SC-36。

(2) 情報セキュリティアーキテクチャ |供給業者の多様性

組織は、[指定：組織が定めたロケーションとアーキテクチャ層]に割り当てられる[指定：組織が定めた．セキュリティ対策]が、複数の供給業者から供給されることを要求する。

補足的ガイダンス：IT 製品は、製品が異なれば、長所と短所も異なる。幅広い製品を用意すれば、個々の製品が提供する機能を補完することができる。たとえば、悪質コードからの保護を提供するベンダーは、既知のウイルス、トロイの木馬、またはワームに対する解決策を、自身の優先事項や開発スケジュールに沿って用意することが多いため、通常は製品のアップデートのタイミングもそれぞれに異なる。ロケーション（例：サーバー・境界・デスクトップ）ごとに異なる製品を持たせる事で、少なくとも1つの製品が悪質コードを検出する可能性が高まる。関連するセキュリティ管理策は、SA-12。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** PL-8	**高** PL-8

PL-9 一元的管理

管理策：組織は、[指定：組織が定めたセキュリティ管理策および関連プロセス]を集中的に管理する。

補足的ガイダンス：一元的管理は、選択されたセキュリティ管理策と、関連プロセスを組織全体にわたって管理・導入することをいう。一元的管理は、組織が定めた、集中的に管理されるセキュリティ管理策とプロセスを策定、導入、アセスメント、認可し、モニタリングすることを含む。セキュリティ管理策の一元的管理は、通常、共通管理策と関連するため、そうした管理により、セキュリティ管理策の導入と管理の標準化が促進され、容易になり、組織の資源が慎重に使われるようになる。集中的に管理されるセキュリティ管理策とプロセスは、また、組織の継続的なモニタリングの一環である初期の、およびその後の運用認可を支援するための、アセスメントの独立性に関する要件を満たす。セキュリティ管理策の選択プロセスの一環として、組織は、組織のリソースと能力に基づいて、一元的管理に適したセキュリティ管理策を決定する。組織は、セキュリティ管理策のすべての側面を集中的に管理することができないと判断する場合がある。そうした場合には、そのセキュリティ管理策はハイブリッド管理策として扱われ、集中的に、あるいは情報システムレベルで管理・導入される。完全な、あるいは部分的な一元的管理の候補となるセキュリティ管理策および拡張管理策は、：AC-2 (1) (2) (3) (4)・AC-17 (1) (2) (3) (9)・AC-18 (1) (3) (4) (5)・AC-19 (4)・AC-22・AC-23・AT-2 (1) (2)・AT-3 (1) (2) (3)・AT-4・AU-6 (1) (3) (5) (6) (9)・AU-7 (1) (2)・AU-11・AU-13・AU-16・CA-2 (1) (2) (3)・CA-3 (1) (2) (3)・CA-7 (1)・CA-9・CM-2 (1) (2)・CM-3 (1) (4)・CM-4・CM-6 (1)・CM-7 (4) (5)・CM-8 (すべて)・CM-9 (1)・CM-10・CM-11・CP-7 (すべて)・CP-8 (すべて)・SC-43・SI-2・SI-3・SI-7・SI-8 の各セキュリティ管理策を含むがこれらに限定されない

拡張管理策：なし

参考文献：NIST Special Publication 800-37

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:職員によるセキュリティ

PS-1　職員によるセキュリティのポリシーと手順

管理策:組織は、

a. 以下を策定・文書化のうえ、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、職員によるセキュリティのポリシー
   2. 職員によるセキュリティのポリシーと、関連する「職員によるセキュリティ」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. 職員によるセキュリティのポリシーを[指定: 組織が定めた頻度で]
   2. 職員によるセキュリティの手順を[指定: 組織が定めた頻度で]。

補足的ガイダンス:このセキュリティ管理策は、PS ファミリ内の選択されたセキュリティ管理策と拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引きのうち該当するものを反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。なお、関連するセキュリティ管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** PS-1	**中** PS-1	**高** PS-1

PS-2　役職ごとのリスク記号

管理策:組織は

a. 組織内のすべての役職にリスク記号を割り当てる
b. そられの職務を担う個人に対する審査基準を定める
c. 役職ごとのリスク記号を[指定:組織が定めた頻度で]レビューし、更新する。

補足的ガイダンス:役職ごとのリスク記号は、Office of Personnel Management のポリシーと手引きを反映する。リスク記号は、個人が組織の情報と情報システムにアクセスする際に受ける認可のタイプを導き、情報を与える。役職ごとの審査基準は、情報セキュリティ上の役割の割り当てに関する明示的な要求事項(例:トレーニング・セキュリティクリアランス)を含む。なお、関連する管理策は、AT-3・PL-2・PS-3。

拡張管理策:なし

参考文献:5 C.F.R. 731.106

優先順位とベースライン管理策の割り当て:

P1	**低** PS-2	**中** PS-2	**高** PS-2

PS-3 職員の審査

セキュリティ管理策:組織は、

a. 情報システムに対するアクセスを許可する前に、個人を審査するとともに、

b. [指定:組織が定めた、再審査が必要な条件に従って、かつ指定されている場合は、そうした再審査の頻度で]個人を再審査する。

補足的ガイダンス:職員の審査および再審査活動は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引きおよび割り当てられた役職に対するリスク記号ごとに定められた基準を反映する。組織は、情報システムにアクセスする職員に対する再審査の条件と頻度をそのシステムによって処理または保存(または伝送される情報のタイプに基づいて変えてもよい。関連する管理策は、AC-2・IA-4・PE-2・PS-2。

拡張管理策:

(1) 職員の審査 | 機密情報

組織は、機密情報を処理または保存(もしく)は伝送する情報システムにアクセスする個人が、そのシステム上で彼らがアクセスできる情報の中で、機密レベルが最も高いものに対して使用が許可されていて、教え込まれるようにする。

補足的ガイダンス:関連するセキュリティ管理策は、AC-3・AC-4。

(2) 職員の審査 | 形式的な啓発

組織は、形式的な啓発を必要とするタイプの 機密情報を処理、保存、または伝送する情報システムにアクセスする個人が、そのシステム上で彼らがアクセスできる情報の中で、関連するタイプの情報すべてに対して、形式的な啓発を受けるようにする。

補足的ガイダンス:形式的な啓発を必要とするタイプの機密情報には、たとえば、特殊アクセスプログラム(Special Access Program)・秘密データ(Restricted Data)・機密コンパートメント情報(Sensitive Compartment Information)がある。関連する管理策は、AC-3・AC-4。

(3) 職員の審査 | 特別な保護対策を必要とする情報

組織は、特別な保護を必要とする情報を処理、保存、または伝送する情報システムにアクセスする個人が、以下を満たすようにする:

(a) 有効なアクセス権限を有し、そのことが割り当てられた公務によって示されること

(b) [指定:組織が定めた、職員に対する追加の審査基準]を満たす事。

補足的ガイダンス:特別な保護を必要とする組織の情報には、たとえば、CUI(管理されている、非機密扱いの情報)や、ソースおよびメソッド情報(Sources and Methods Information)がある。職員のセキュリティ基準には、例えば、高い役職の適性検査(position sensitivity background screening requirements)がある。

参考文献:5 C.F.R. 731.106・FIPS Publications 199・FIPS Publications 201・NIST Special Publications 800-60・NIST Special Publications 800-73・NIST Special Publications 800-76・NIST Special Publications 800-78・ICD 70

優先順位とベースライン管理策の割り当て:

P1	**低** PS-3	**中** PS-3	**高** PS-3

PS-4　職員の雇用の終了

セキュリティ管理策：組織は、個人の雇用の終了時に、以下を実施する：

a. 情報システムに対するアクセスを［指定：組織が定めた期間］内に無効にする
b. その個人に関連するオーセンティケータ／クレデンシャルをすべて終了させる／無効にする
c. 退職者面接を実施する（［指定：組織が定めた、情報セキュリティトピック］についての話し合いを含む）
d. セキュリティに関連する、組織の情報システム関連の所有物をすべて回収する
e. 退職する個人が管理していた組織の情報と情報システムに対するアクセスを保持する
f. ［指定：組織が定めた期間］内に[指定：組織が定めた職員または役職]に知らせる。

補足的ガイダンス：情報システム関連の所有物には、例えば、ハードウェア認証トークン、システム管理技術マニュアル・鍵・身分証明書・入館証がある。退職者面接は、雇用が終了した個人が、元職員であるために課せられるセキュリティ制約について理解し、情報システム関連の所有物に対する適切な説明責任が果たされるようにする。退職者面接時の重要なセキュリティトピックには、例えば、雇用が終了した個人に機密保持契約について、また、今後の雇用に関する制約について想起させることがある。退職者面接は、たとえば、就業放棄、病気、上司が不在の場合には、雇用が終了した個人に対して実施できない場合がある。退職者面接は、セキュリティクリアランスを有する個人にとっては重要である。正当な理由により雇用が終了した個人に対して、雇用終了時のアクションをタイムリーに実施することは極めて重要である。組織は、場合によっては、雇用が終了した個人の情報システムアカウントを、それらの個人に通知する前に無効にすることを検討する。関連するセキュリティ管理策は、AC-2・IA-4・PE-2・PS-5・PS-6。

拡張管理策：

(1) 職員の雇用の終了 | 雇用終了後の要求事項

組織は、

(a) 雇用が終了した個人に、組織の情報を保護するために適用される、法的拘束力のある「雇用終了後の要求事項」について知らせる

(b) 雇用が終了した個人に対して、組織の契約終了プロセスの一環として、「雇用終了後の要求事項」の用紙に署名することを要求する。

補足的ガイダンス：組織は、雇用が終了した個人に対する、雇用終了後の要求事項に関して、法律顧問室に助言を求める。

(2) 職員の雇用の終了 | 自動化された通知

組織は、個人の雇用の終了時に[指定：組織が定めた職員または役職]に知らせるための自動化されたメカニズムを使用する。

補足的ガイダンス：多数の職員を抱える組織では、雇用終了時のアクションについてすべての職員が知る必要があったとしても、全員が適切な通知を受けるわけではなかったり、通知は行われてもタイムリーに実施されなかったりする。自動化されたメカニズムは、個人の雇用の終了時に、組織の特定の職員または役職（例：経営陣、上司、「職員によるセキュリティ」の担当者、情報セキュリティ責任者、システムアドミニストレータ、または IT アドミニストレータ）に自動警告／通知を送るために使用できる。そうした自動警告／通知は、たとえば、電話で、電子メールにて、テキストメッセージにて、あるいはウェブサイトを介してなど、さまざまな方法で伝えることができる。

参考文献：なし

優先順位とベースライン管理策の割り当て:

P1	**低** PS-4	**中** PS-4	**高** PS-4 (2)

PS-5 職員の異動

管理策:組織は、

a. 職員が組織内の他部署に配置転換／異動になった場合に、情報システム／施設に対する現行の論理アクセス権限と物理アクセス権限が引き続き必要であるかどうかをレビューし、確認するのと合わせて、

b. [指定:組織が定めた、異動時の形式的なアクションが終了してからの期間]内に[指定:組織が定めた、異動または配置転換時のアクション]を開始するとともに、

c. 配置転換／異動に起因する業務ニーズの変化に対応するように、適宜、アクセス権限を変更するのに加えて、

d. [指定:組織が定めた期間]内に[指定: 組織が定めた職員または役職]に知らせる。

補足的ガイダンス:このセキュリティ管理策は、個人の配置転換／異動が恒久的である場合や、それらのアクションが必要なほど長期にわたる場合に適用される。組織は、配置転換および／または異動が恒久的であれ、長期であれ、それらのタイプに適したアクションを定義する。職員の組織内の他部署への配置転換および／または異動時に必要なアクションは、例えば、以下を含む:①鍵、身分証明書、および入館証の古い方を返却させ、新しいのを発行する②情報システムアカウントを閉鎖し、新しいアカウントを開設する③情報システムに対するアクセス許可(すなわち、アクセス権限)を変更するならびに④個人が前の勤務地で、前の情報システムアカウントを利用してアクセスできた公式記録に関しては、アクセスできるようにする。なお、関連するセキュリティ管理策は、AC-2・IA-4・PE-2・PS-4。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** PS-5	**中** PS-5	**高** PS-5

PS-6 アクセス契約

セキュリティ管理策:組織は、

a. 組織の情報システムに対するアクセス契約を定めて文書化するとともに、

b. アクセス契約を[指定:組織が定めた頻度で]レビュー・更新するのに加えて、

c. 組織の情報と情報システムに対するアクセスを要求する個人に対して、以下を実施させる:

   1. アクセスを得る前に、適切なアクセス契約に署名する
   2. アクセス契約が更新された場合、あるいは[指定:組織が定めた頻度で]、組織の情報システムに対するアクセスを維持できるよう、アクセス契約に再度署名する。

補足的ガイダンス:アクセス契約には、例えば、機密保持契約・利用規定・行動規則に加えて、利害の衝突に関する契約を含むまれる。また、署名がなされるアクセス契約には、アクセスが許可される組織の情報システムに関連する制約について、個人が読んで、理解したこと、また、従うことに同意することを示す承諾書を含まれる。組織は、組織の方針により禁止されている場合を除き、アクセス契約に同意することを示す手段として、電子署名を使用することができる。関連するセキュリティ管理策は、PL-4・PS-2・PS-3・PS-4・PS-8。

拡張管理策:

(1) アクセス契約 | 特別な保護を必要とする情報

[削除された:PS-3 に統合された]

(2) アクセス契約 | 特別な保護を必要とする機密情報

組織は、特別な保護を必要とする機密情報に対するアクセスが、以下を満たす個人にのみ与えられるようにする:

(a) 有効なアクセス権限を有し、そのことが割り当てられた公務によって示されること

(b) 関連する、職員のセキュリティ基準を満たすこと

(c) 機密保持契約を読んで、理解し、契約に署名すること

補足的ガイダンス:特別な保護を必要とする機密情報には、例えば、担保に関する情報、特殊なアクセスプログラム(Special Access Program)に関する情報、機密コンパートメント情報(Sensitive Compartment Information)がある。職員のセキュリティ基準は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引のうち該当するものを反映する。

(3) アクセス契約 | 雇用終了後の要求事項

組織は、

(a) 個人に対して、組織の情報を保護するために適用される、法的拘束力のある雇用終了後の要求事項について知らせる

(b) 個人に対して、保護された情報に対する初期アクセスを許可する前に、該当する場合にはそれらの要求事項を盛り込んだ承諾書に署名することを要求する。

補足的ガイダンス:組織は、雇用が終了した個人に対する、雇用終了後の要求事項に関して、法律顧問室に助言を求める。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P3	**低** PS-6	**中** PS-6	**高** PS-6

PS-7 第三者職員によるセキュリティ

セキュリティ管理策:組織は、

a. 第三者プロバイダに対する「職員によるセキュリティ」の要求事項(セキュリティ上の役割と責任を含む)を定める

b. 第三者プロバイダに対して、組織が定めた「職員によるセキュリティ」のポリシーと手順に従うことを要求する

c. 「職員によるセキュリティ」の要求事項を文書化する

d. 第三者プロバイダに対して、組織が発行するクレデンシャルおよび/またはバッジを保有する第三者職員、または[指定:組織が定めた期間]にわたって情報システムに対する権限を有する第三者職員が異動になる、または雇用が終了する場合に、[指定:組織が定めた職員または役職]に知らせることを要求する

e. プロバイダによる遵守状況をモニタリングする

補足的ガイダンス:第三者プロバイダには、たとえば、サービス機関、請負業者、そして情報システム開発、IT サービス、外部委託によるアプリケーション、ネットワークとセキュリティの管理などのサービスを提供する他の組織がある。組織は、「職員によるセキュリティ」の要求事項を調達関連文書に明示的に含める。第三者プロバイダは、組織が発行するクレデンシャル、バッジ、または情報システムに対する権限を持って組織の施設で働く職員を抱える場合がある。第

三者職員の異動について通知を受けることで、権限とクレデンシャルを確実に無効にできるようになる。組織は、報告義務のある異動や雇用の終了を定める際には、セキュリティ関連の特性（例えば、異動になる、または雇用が終了する個人の職務、役割、および所有するクレデンシャル／権限の性質を含む）ごとに定める。なお、関連するセキュリティ管理策は、PS-2・PS-3・PS-4・PS-5・PS-6・SA-9・SA-21。

拡張管理策：なし

参考文献：NIST Special Publication 800-35

優先順位とベースライン管理策の割り当て：

P1	**低** PS-7	**中** PS-7	**高** PS-7

PS-8　職員に対する制裁

セキュリティ管理策：組織は、

a. 組織は、組織が定めた情報セキュリティポリシーおよび手順に従わない個人に対する形式的な制裁プロセスを導入するとともに、
b. 職員に対する形式的な制裁プロセスが開始された場合に、制裁を受ける個人と、制裁の理由を［指定：組織が定めた期間］内に[指定： 組織が定めた職員または役職]に知らせる。

補足的ガイダンス：組織の制裁プロセスは、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。制裁プロセスはアクセス契約に記載され、組織の全般的な「職員に関するポリシーおよび手順」の一部として含めることができる。組織は、職員に対する制裁に関して、法律顧問室に助言を求める。なお、関連するセキュリティ管理策は、PL-4・PS-6。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P3	**低** PS-8	**中** PS-8	**高** PS-8

ファミリ:リスクアセスメント

RA-1　リスクアセスメントのポリシーと手順

セキュリティ管理策:組織は、

a. 以下を策定・文書化のうえ、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、リスクアセスメントのポリシー
   2. リスクアセスメントのポリシーと、関連する「リスクアセスメント」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. リスクアセスメントのポリシーを[指定:組織が定めた頻度で
   2. リスクアセスメントの手順を[指定:組織が定めた頻度で]

補足的ガイダンス:このセキュリティ管理策は、RA のセキュリティ管理策ファミリ内の選択されたセキュリティ管理策と拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。なお、関連するセキュリティ管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-30・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** RA-1	**中** RA-1	**高** RA-1

RA-2　セキュリティカテゴリ

セキュリティ管理策:組織は、

a. 連邦法・大統領命令・指令・政策・規制・標準・指針のうち該当するものに従って、情報と情報システムを分類するとともに、
b. セキュリティ分類結果(裏付けとなる根拠を含む)を情報システムのセキュリティ計画に記載するのに加えて、
c. セキュリティカテゴリに関する決定が運用認可責任者または運用認可責任者が指定した代表者によってレビューされ、承認されるようにする。

補足的ガイダンス:明確に定義された「認可を出す範囲」は、セキュリティカテゴリに関する効果的な意思決定には、必要な条件となる。セキュリティカテゴリは、組織の情報と情報システムの機密性、完全性、または可用性が失われて侵害された場合に、組織の業務、組織の資産、および個人にもたらされる負の影響を示す。組織はセキュリティ分類プロセスを最高情報責任者・上級情報セキュリティ責任者・情報システム所有者・ミッション／業務遂行責任者・情報所有者／スチュワードが関与する組織全体にわたる活動として実施する。組織は、また、他組織にもたらされる負の影響についても考慮し、さらに 2001 年施行の米国愛国者法と、国土安全に関する

大統領指令に従って国家レベルの影響についても考慮する。組織が実施するセキュリティ分類プロセスは、情報資産の一覧の作成を容易にし、また管理策 CM-8 と共に、情報が処理または保存（もしくは伝送）される情報システムコンポーネントへのマッピングを容易にする。なお、関連する管理策は、CM-8・MP-4・RA-3・SC-7。

拡張管理策：なし

参考文献：FIPS Publication 199・NIST Special Publications 800-30・NIST Special Publications 800-39・NIST Special Publications 800-60

優先順位とベースライン管理策の割り当て：

P1	**低** RA-2	**中** RA-2	**高** RA-2

RA-3 リスクアセスメント

管理策：組織は、

a. 情報システムと、その情報システムが処理、保存、または伝送する情報の不正なアクセス、利用、開示、中断／途絶、変更、破壊が発生する可能性と被害の大きさを含めた、リスクアセスメントを実施するのと合わせて、

b. リスクアセスメント結果を［選択：セキュリティ計画; リスクアセスメントレポート; ［指定：組織が定めたドキュメント］］に記載するとともに、

c. リスクアセスメント結果を［指定：組織が定めた頻度で］レビューするのに加えて、

d. リスクアセスメント結果を [指定： 組織が定めた職員または役職]に配布するだけではなく、

e. リスクアセスメントを［指定：組織が定めた頻度で］、あるいは情報システム、またはシステムが稼働する環境に大きな変化があった場合（新たな脅威や脆弱性の特定を含む）、もしくはシステムのセキュリティ状態に影響を与える他の状況が発生した場合に更新する。

補足的ガイダンス：明確に定義された「認可を出す範囲」は、効果的なリスクアセスメントには、必要な条件となる。リスクアセスメントは、脅威、脆弱性、発生可能性、および情報システムの運用と使用が組織の業務と資産、個人、他の組織、および国家にもたらす影響を考慮する。リスクアセスメントは、また、外部関係者（例:サービスプロバイダ、組織に代わって情報システムを運用する請負業者、組織の情報システムにアクセスする個人、外部委託先のエンティティなど）によってもたらされるリスクも考慮する。連邦政府の情報システムにアクセスする一般ユーザに対しても、OMB ポリシーと、関連する電子認証イニシアチブに従って、非公開の情報またはプライバシー関連情報を保護するために認証が必要になる場合がある。このため、組織によるリスクアセスメントでは、連邦政府の情報システムへの一般の人からのアクセスも取り扱う。

リスクアセスメント（形式的あるいは非形式的）は、リスクマネジメント階層の 3 つのすべての層（すなわち、組織レベル、ミッション／業務プロセスレベル、または情報システムレベル）と、システム開発ライフサイクルのすべてのフェーズで実施することができる。リスクアセスメントは、また、リスクマネジメントフレームワークにおける分類、セキュリティ管理策の選択、セキュリティ管理策の導入、セキュリティ管理策のアセスメント、情報システムの運用認可、およびセキュリティ管理策のモニタリングといった、各ステップにて実施することができる。RA-3 は、リスクマネジメントフレームワークのステップ 1 とステップ 2 を成し遂げるために、他の管理策を実施する前に部分的に実施する必要があることから注目に値する。リスクアセスメントは、セキュリティ管理策の選択プロセスにおいて、とりわけ、セキュリティ管理策の補足を含む調整に関するガイダンスの適用時に重要な役割を果たす場合がある。関連する管理策：RA-2・PM-9。

拡張管理策:なし

参考文献:OMB Memorandum 04-04・NIST Special Publications 800-30・NIST Special Publications 800-39・ウェブサイト http://idmanagement.gov

優先順位とベースライン管理策の割り当て:

P1	**低** RA-3	**中** RA-3	**高** RA-3

RA-4 リスクアセスメントの更新

[削除された:RA-3 に統合された]

RA-5 脆弱性スキャン

管理策:組織は、

a. 情報システムと、ホストされるアプリケーションの脆弱性のスキャンを[指定:組織が定めた頻度で、および/または組織が定めたプロセスに従ってランダムに]、かつ、それらのシステム/アプリケーションに影響を及ぼす新たな脆弱性が確認され、報告された場合に実施する

b. 脆弱性スキャンツールと技法を用いる。それらはツール間の相互運用を容易にし、以下を満たす標準を使用することによって、脆弱性管理プロセスの一部を自動化できることが求められる:

   1. プラットフォーム、ソフトウェアの欠陥、および誤った設定を列挙する
   2. チェックリストとテスト手順をフォーマットする
   3. 脆弱性による影響を評価する

c. 脆弱性スキャンレポートと、セキュリティ管理策アセスメントの結果を分析する

d. 組織によるリスクアセスメントを通じて特定された脆弱性を[指定:組織が定めたレスポンスタイム]内に修正する

e. 脆弱性スキャンプロセスとセキュリティ管理策アセスメントから得た情報を[指定:組織が定めた職員または役職]と共有することによって、他の情報システム内の同様の脆弱性(すわわち、体系的な弱点または欠陥)を排除する。

補足的ガイダンス:情報システムのセキュリティカテゴリは、脆弱性スキャンの頻度と包括性を導き出す。組織は、すべての情報システムコンポーネントに対して、ネットワークで結ばれたプリンター、スキャナー、コピー機などの脆弱性の元が見過ごされないよう、必要な脆弱性スキャンを決定する。カスタムソフトウェアアプリケーションの脆弱性分析では、静的解析、動的解析、バイナリー解析、あるいはそれらの 3 つのアプローチの混合などの、追加のアプローチが必要になる場合がある。組織は、これらの解析アプローチをさまざまなツール(例:ウェブ上のアプリケーションスキャナー、静的解析ツール、バイナリーアナライザ)で実現することができ、また、これらの解析アプローチをソースコードレビューに使用してもよい。脆弱性スキャンは、たとえば、以下を含む:①パッチレベルを確認するするためのスキャン②ユーザまたは機器からのアクセスが許可されていない機能、ポート、プロトコル、およびサービスに対するスキャンならびに③情報フロー制御メカニズムの設定に誤りがないか、または不適切に作動していないかを確認するためのスキャン。組織は、CVE(Common Vulnerabilities and Exposures:共通脆弱性識別子)の命名規則に沿って脆弱性を表現するツールであり、かつ、OVAL(Open Vulnerability Assessment Language) を使用して脆弱性の有無を判断/テストするツールの使用を検討する。推脆弱性情報の情報源として奨されるのは、CWE (Common Weakness Enumeration:共通脆弱性タイプ一覧)や、NVD (National Vulnerability Database)がある。また、レッドチーム訓練などのセキュリティ管理策アセスメントは、他にもスキャンすべき脆弱性の元を示してくれる。組織は、

また、脆弱性による影響を CVSS (Common Vulnerability Scoring System：共通脆弱性評価システム)によって表現するツールの使用を検討する。関連する管理策は、CA-2・CA-7・CM-4・CM-6・RA-2・RA-3・SA-11・SI-2。

拡張管理策：

(1) 脆弱性スキャン | ツールの更新機能

組織は、スキャンすべき情報システムの脆弱性をすぐに更新できる脆弱性スキャンツールを使用する。

補足的ガイダンス：スキャンすべき脆弱性は、新たな脆弱性が発覚、公表されて、スキャンの方法が開発されたら、すぐに更新する必要がある。この更新プロセスにより、情報システムの脆弱性が一刻も早く特定され、対処されるようになる。関連する管理策は、SI-3・SI-7。

(2) 脆弱性スキャン | 定められた頻度で / 新たなスキャンの前に / 特定された場合に更新する

組織は、スキャンされた情報システムの脆弱性を[選択（1つ以上）：[指定：組織が定めた頻度で]; 新たなスキャンの前に; 新たな脆弱性が特定され、報告された場合に]更新する。

補足的ガイダンス：関連する管理策は、SI-3・SI-5。

(3) 脆弱性スキャン | 適用の広さ / 深さ

組織は、適用の広さと深さ（すなわち、スキャンされた情報システムコンポーネント、チェックされた脆弱性）を特定できる脆弱性スキャン手順を用いる。

(4) 脆弱性スキャン | 発見可能な情報

組織は、情報システムに関する情報の内、どの情報が敵対者によって発見可能であるかを判断し、次に[指定：組織が定めた是正措置]を講じる。

補足的ガイダンス：発見可能な情報は、敵対者がその情報システムを直接侵害したり、システムに侵入しなくても、たとえば、そのシステムによってさらされている情報を収集したり、あるいはウェブの広範囲にわたる検索を実施することによって取得できる情報である。是正措置は、たとえば、組織内の適切な職員に知らせる、指定された情報を削除する、あるいは情報システムに変更を加えて、指定された情報が敵対者にとって関係が薄くなるようにしたり、魅力的でなくなるようにする、といったことを含む。関連する管理策は、AU-13。

(5) 脆弱性スキャン | 特権的アクセス

情報システムは、選択された[指定：組織が定めた脆弱性スキャン活動]に関して、[指定：組織が定めた情報システムコンポーネント]に対する特権的アクセスの許可制度を実施する。

補足的ガイダンス：特定の状況では、脆弱性スキャンがより立ち入ったものとなったり、スキャンの対象である情報システムコンポーネントが、機微度が高い情報を含むことがある。選択されたシステムコンポーネントに対する特権的アクセスの許可制度を実施することで、より徹底した脆弱性スキャンが容易になり、そうしたスキャンの機密性が保護される。

(6) 脆弱性スキャン | 自動化された傾向分析

組織は、長期にわたる脆弱性スキャン結果を比較して、情報システムの脆弱性の傾向を特定できるようにするための、自動化されたメカニズムを使用する。

補足的ガイダンス：関連する管理策は、IR-4・IR-5・SI-4。

(7) 脆弱性スキャン | 許可されていないコンポーネントを自動で検出し、通知する

[削除された：CM-8 に統合された]

(8) 脆弱性スキャン | 過去の監査ログをレビューする

組織は、過去の監査ログをレビューし、その情報システムにおいて特定された脆弱性が以前にも利用されたかどうかを確認する。

補足的ガイダンス：関連する管理策は、AU-6。

(9) 脆弱性スキャン | 侵入テストおよび分析

[削除された：CA-8 に統合された]

(10) 脆弱性スキャン | スキャン情報を相互に関連付ける

組織は、脆弱性スキャンツールからの出力情報を相互に関連付けて、複数の脆弱性を利用する／マルチホップな攻撃ベクトルの有無を確認する。

参考文献：NIST Special Publications 800-40・NIST Special Publications 800-70・NIST Special Publications 800-115・ウェブサイト http://cwe.mitre.org および http://nvd.nist.gov

優先順位とベースライン管理策の割り当て：

P1	**低** RA-5	**中** RA-5 (1) (2) (5)	**高** RA-5 (1) (2) (4) (5)

RA-6 科学的情報収集対策に関する調査

管理策：組織は、[指定：組織が定めたロケーション]で、[選択（1つ以上）：[指定：組織が定めた頻度で];[指定：組織が定めたイベントが発生した場合、または兆候があった場合に]]科学的情報収集対策に関する調査を実施する。

補足的ガイダンス：科学的情報収集対策に関する調査は、資格のある担当者によって実施され、科学的情報収集用の機器／ハザードの存在の確認や、調査対象の施設への技術的な侵入を容易にする技術面でのセキュリティ上の弱点の特定がなされる。そうした調査を通じて、組織の技術面でのセキュリティ姿勢が評価され、調査対象の施設内での、および施設に関する徹底的な視覚的検証、電子的検証、および物理的検証が容易になる。この調査は、また、リスクアセスメントに有力な入力情報を提供し、組織が敵対者にどの程度さらされているかを示す。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

ファミリ:システムおよびサービスの調達

SA-1　システムおよびサービスの調達のポリシーと手順

管理策:組織は、

a. 以下を策定のうえ文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、システムおよびサービスの調達のポリシー
   2. システムおよびサービスの調達のポリシーと、関連する「システムおよびサービスの調達」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. システムおよびサービスの調達のポリシーを[指定:組織が定めた頻度で]
   2. システムおよびサービスの調達の手順を[指定:組織が定めた頻度で]。

補足的ガイダンス:この管理策は、SA ファミリ内の選択されたセキュリティ管理策とその拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準、手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12・NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** SA-1	**中** SA-1	**高** SA-1

SA-2　リソースの割り当て

管理策:組織は、

a. ミッション／業務プロセスの計画作成時に、情報システムまたは情報システムサービスの情報セキュリティ要求事項を決定するとともに、
b. 組織の資本計画および投資管理プロセスの一環として、情報システムまたは情報システムサービスを保護するのに必要なリソースを決定・文書化のうえ割り当てるのに加えて、
c. 情報セキュリティの個々の予算項目を、組織の計画および予算関連の資料に記載する。

補足的ガイダンス:情報セキュリティのリソースの割り当ては、情報システムまたは情報システムサービスの初期の調達に必要な資金と、それらのシステム／サービスの維持に必要な資金も対象とする。関連する管理策は、PM-3・PM-11。

拡張管理策:なし

参考文献:NIST Special Publication 800-65

優先順位とベースライン管理策の割り当て:

P1	**低** SA-2	**中** SA-2	**高** SA-2

SA-3　システム開発ライフサイクル

管理策:組織は、

a. 情報セキュリティ上の考慮事項を含む[指定:組織が定めたシステム開発ライフサイクル]を使用して、情報システムを管理するのと合わせて、

b. システム開発ライフサイクル全体を通しての情報セキュリティ上の役割と責任を定義し、文書化するとともに、

c. 情報セキュリティ上の役割と責任を有する個人を指定するのに加えて、

d. 組織の情報セキュリティリスクマネジメントプロセスをシステム開発ライフサイクル活動に組み入れる。

補足的ガイダンス:明確に定義されたシステム開発ライフサイクルは、組織の情報システムを成功裏に開発、導入し、運用するための基盤を提供する。必要なセキュリティ管理策をシステム開発ライフサイクルに適用するには、情報セキュリティ、脅威、脆弱性、負の影響、および極めて重要なミッション／業務機能に対するリスクについて基本的な理解が必要になる。SA-8「セキュリティエンジニアリング原則」は、情報システムおよびシステムコンポーネント(IT 製品を含む)を設計、コーディングし、テストする個人がセキュリティを理解していなければ、正しく使用できない。しがたって、組織は、たとえば、最高情報セキュリティ責任者、セキュリティアーキテクト、セキュリティエンジニア、および情報システムセキュリティ責任者などの、資格のある担当者をシステム開発ライフサイクル活動に関与させることによって、セキュリティ要求事項が組織の情報システムに組み入れられるようにする。同様に重要なのは、開発者が、必要なセキュリティ能力が情報システムに効果的に組み入れられるようにするためにも、セキュリティに関する必要な専門知識と技能を有する個人を開発チームに含めることである。セキュリティ意識向上およびトレーニングプログラムは、セキュリティ上重要な役割と責任を担う個人が、割り当てられたシステム開発ライフサイクル活動を実施するのに適切な経験・技能・専門知識を有することを支援する。セキュリティ要求事項をエンタープライズアーキテクチャに効果的に組み入れられれば、セキュリティ上重要な考慮事項がシステム開発ライフサイクルの早い段階で考慮され、それらの考慮事項が組織のミッション／業務プロセスに直接結び付くようになる。このプロセスは、また、組織のリスクマネジメント戦略と情報セキュリティ戦略に沿って、情報セキュリティアーキテクチャをエンタープライズアーキテクチャに組み入れることを容易にする。関連する管理策は、AT-3・PM-7・SA-8。

拡張管理策:なし

参考文献:NIST Special Publications 800-37・NIST Special Publications 800-64

優先順位とベースライン管理策の割り当て:

P1	**低** SA-3	**中** SA-3	**高** SA-3

SA-4　調達プロセス

管理策:組織は、該当する連邦法・大統領命令・指令・政策・規制・標準・指針とともに、組織のミッション／業務ニーズに応じて、情報システム、システムコンポーネント、または情報システムサービスの調達契約に明示的に、あるいは参照によって以下の要求事項、記述、および基準を含める:

a. セキュリティ機能に関する要求事項

b. セキュリティ強度に関する要求事項

c. セキュリティ保証に関する要求事項

d. セキュリティ関連のドキュメントに関する要求事項

e. セキュリティ関連のドキュメントの保護に関する要求事項

f. その情報システムの開発環境と、そのシステムを稼働させる予定の環境についての記述

g. 受け入れ基準。

補足的ガイダンス：情報システムコンポーネントは、情報システムの構成要素である個別の、識別可能な IT 資産（例：ハードウェア・ソフトウェア・ファームウェアのいずれか）である。情報システムコンポーネントは、市販の IT 製品を含む。セキュリティ機能に関する要求事項は、セキュリティ能力、セキュリティ機能、およびセキュリティメカニズムも取り扱う。そうした能力、機能、およびメカニズムに関連する、セキュリティ強度に関する要求事項は、正しさ、完全さ、直接的な攻撃に対する耐性、改ざんまたは擦り抜けに対する耐性の、それぞれの度合も取り扱う。セキュリティ保証に関する要求事項は、以下を含む：①開発プロセス、手順、プラクティス、および方法; ならびに②開発活動とアセスメント活動から得たエビデンスであり、必要なセキュリティ機能が導入されていて、必要なセキュリティ強度が確保されていることへの信頼の根拠を示すもの。セキュリティドキュメントに関する要求事項は、システム開発ライフサイクルのすべてのフェーズに当てはまる。

セキュリティ機能、保証、およびドキュメントに関する要求事項は、調整プロセスを経て選択されたセキュリティ管理策と拡張管理策によって表される。セキュリティ管理策の調整プロセスは、たとえば、「指定ステートメント」と「選択ステートメント」の使用によるパラメータ値の指定や、プラットフォームの依存関係と導入に関する情報の明示を含む。セキュリティドキュメントは、セキュリティ管理策の導入と運用に関するユーザとアドミニストレータ向けの手引きとなる。セキュリティドキュメントに必要な詳細レベルは、その情報システムのセキュリティカテゴリまたは分類レベルと、組織が（組織のリスクマネジメント戦略に定義されているように）全般的なリスク対応に関する期待に応えるためにそれらのセキュリティ能力、機能、またはメカニズムにどの程度依存するかに依る。セキュリティ要求事項は、許可されている機能、ポート、プロトコル、およびサービスを指定するための、組織の必須の設定を含む場合がある。情報システム、システムコンポーネント、および情報システムサービスの受け入れ基準は、組織のあらゆる調達／資材調達に関するそうした基準と同じ方法で定義される。Federal Acquisition Regulation (FAR) Section 7.103 には、FISMA が規定する情報セキュリティ要求事項が記載されている。関連する管理策は、CM-6・PL-2・PS-7・SA-3・SA-5・SA-8・SA-11・SA-12。

拡張管理策：

(1) 調達プロセス | セキュリティ管理策の機能特性

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、導入されるセキュリティ管理策の機能特性についての記述の提供を要求する。

補足的ガイダンス：セキュリティ管理策の機能特性は、それらの管理策のインターフェースにおいて目に見える機能（すなわち、セキュリティ能力、機能、またはメカニズム）を説明するものであり、それらの管理策の運用における機能とデータ構造は含まない。関連する管理策は、SA-5。

(2) 調達プロセス | セキュリティ管理策の設計 / 導入に関する情報

組織は、情報システム・システムコンポーネント・情報システムサービスのいずれかを開発する者に対して、導入されるセキュリティ管理策の設計と導入に関する情報の提供を要求する。この情報は、以下を含む：[指定：組織が定めた詳細レベル]での[選択（1つ以上）：セキュリティ関連の外部システムインターフェース;上位レベル設計;下位レベル設計; ソースコードまたはハードウェアの図解;[指定：組織が定めた、設計／導入に関する情報]]。

補足的ガイダンス：組織は、組織の情報システム、システムコンポーネント、または情報システムサービスに導入されているセキュリティ管理策の設計と導入に関するドキュメントに関して、ミッション／上位レベル設計業務上の要求事項、信用／耐性に関する要求事項、および分析とテストに関する要求事項に応じてさまざまな詳細レベルのドキュメントを要求することができる。情報システムは、複数のサブシステムに分割することができる。システ

ム内の各サブシステムは単一の、あるいは複数のモジュールを含む。システムの上位レベル設計は、複数のサブシステムと、セキュリティ関連機能を提供するサブシステム間のインターフェースによって表される。システムの下位レベル設計は、モジュールによって表されるが、ソフトウェアとファームウェア（ただし、ハードウェアを除外するわけではない）、およびセキュリティ関連機能を提供するモジュール間のインターフェースにに重点が置かれる。ソースコードと、ハードウェアの図解は、通常はその情報システムの「実装表現」と称される。関連する管理策は、SA-5。

(3) 調達プロセス | 開発手法 / 技法 / プラクティス

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、[指定：組織が定めた、最新のシステム／セキュリティエンジニアリング手法、ソフトウェア開発手法、テスト／評価／有効性判断のための技法、および品質管理プロセス]を含む、システム開発ライフサイクルを使用していることへの実証を要求する。

補足的ガイダンス：最新のソフトウェア開発手法、システム／セキュリティエンジニアリング手法、品質管理プロセス、およびテスト、評価、有効性判断のための技法を含む、明確に定義されたシステム開発ライフサイクルに従うことで、情報システム、システムコンポーネント、および情報システムサービス内の潜在的エラーの数を減らし、重大さを緩和することができる。そうしたエラーの数を減らし、重大さを緩和できれば、それらのシステム、コンポーネント、およびサービスの脆弱性の数を減らすことができる。関連する管理策は、SA-12。

(4) 調達プロセス | システムにコンポーネントを割り当てる

[削除された：CM-8(9)に統合された]

(5) 調達プロセス | システム / コンポーネント / サービスの設定

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する：

(a) システム、コンポーネント、またはサービスに[指定：組織が定めたセキュリティ設定]を施した上で、それらを出荷する

(b) 後にシステム、コンポーネント、またはサービスを再インストールまたはアップグレードする際にも、その設定をデフォルトして使用する。

補足的ガイダンス：セキュリティ設定は、たとえば、USGCB（米国政府共通設定）や、機能、ポート、プロトコル、およびサービスに対するあらゆる制限を含む。セキュリティ特性は、たとえば、すべてのデフォルトパスワードを変更するよう求めることを含む。関連する管理策は、CM-8。

(6) 調達プロセス | 情報保証製品の使用

組織は、

(a) NSA 認定のソリューションを構成する、政府調達向けの、または 市販の情報保証／情報保証が可能な IT 製品のみを使用する。これにより、機密情報を伝送するのに使用されるネットワークが、伝送される情報よりも分類レベルが低い場合にも、機密情報が保護される

(b) これらの製品が NSA によって、あるいは NSA 認定の手順に従って、評価および／または有効性確認がなされるようにする。

補足的ガイダンス：暗号手段によって機密情報を保護するのに使用される市販の情報保証／情報保証が可能な IT 製品の場合には、NSA 認定の鍵管理の使用が必要になる場合がある。関連する管理策は、SC-8・SC-12・SC-13。

(7) 調達プロセス | NIAP 認定の保護プロファイル

組織は、

(a) 市販の情報保証／情報保証が可能な IT 製品の使用に関して、特定のテクノロジー向けの NIAP(National Information Assurance partnership：全米情報保証パートナーシップ) 認定の保護プロファイルが存在する場合には、そのプロファイルによって評価され、合格とされた製品のみに限定する

(b) 上記のような、特定のテクノロジー向けの NIAP 認定の保護プロファイルが存在しないのに、市販の IT 製品がセキュリティポリシーを実施するために暗号機能に依存する場合には、その暗号モジュールが FIPS によって有効性が確認されているモジュールであることを要求する。

補足的ガイダンス：関連する管理策は、SC-12・SC-13。

(8) 調達プロセス | 継続的にモニタリングするための計画

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、セキュリティ管理策の有効性を継続的にモニタリングするための計画を［指定：組織が定めた詳細レベル］で作成することを要求する。

補足的ガイダンス：継続的にモニタリングするための計画の目的は、発生する避けることのできない変化に基づいて、情報システム、システムコンポーネント、または情報システムサービスに導入される予定の、必要な、かつ導入されるセキュリティ管理策が長期にわたって引き続き有効であるかどうかを判断することにある。開発者による継続的にモニタリングするための計画は、その情報が組織が実施する継続的モニタリング戦略およびプログラムに組み入れられるよう、十分な詳細さをもって作成される。関連する管理策は、CA-7。

(9) 調達プロセス | 使用されている機能 / ポート / プロトコル / サービス

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、組織が使用する機能・ポート・プロトコル・サービスをシステム開発ライフサイクルの早い段階で特定することを要求する。

補足的ガイダンス：機能、ポート、プロトコル、およびサービスをシステム開発ライフサイクルの早い段階で（例：初期の要件定義フェーズと設計フェーズにて）特定することは、組織による情報システム、情報システムコンポーネント、または情報システムサービスの設計に影響を与える。こうしたシステム開発ライフサイクルの早い段階での関与は、組織が不必要に高いリスクをもたらす機能、ポート、プロトコル、またはサービスの使用を回避する、または最小限に抑えるのを支援し、また、特定のポート、プロトコル、またはサービスを遮断する場合（または情報システムサービスプロバイダに遮断を依頼する場合）のトレードオフについて理解するのを支援する。機能、ポート、プロトコル、およびサービスを早い段階で特定できれば、情報システム・システムコンポーネント・情報システムサービスのいずれかが実施された後にセキュリティ管理策を導入することによるコスト高を避けられる。SA-9 は、外部情報システムサービスについて、組織が外部ソースから提供される機能、ポート、プロトコル、およびサービスを特定することを前提とした要求事項を記載している。関連する管理策は、CM-7・SA-9。

(10) 調達プロセス | 承認された PIV 製品の利用

組織は、組織の情報システム内で実施される PIV（Personal Identity Verification:個人の身元の確認）機能に関して、FIPS 201 認証製品リストに記載されている IT 製品のみを使用する。

補足的ガイダンス：関連する管理策は、IA-2・IA-8。

参考文献：HSPD-12・ISO/IEC 15408・FIPS Publications 140-2・FIPS Publications 201・NIST Special Publications 800-23・NIST Special Publications 800-35・NIST Special Publications 800-36・NIST Special Publications 800-37・NIST Special Publications 800-64・NIST Special

Publications 800-70・NIST Special Publications 800-137・Federal Acquisition Regulation・ウェブサイト http://www.niap-ccevs.org ならびに http://fips201ep.cio.gov および http://www.acquisition.gov/far

優先順位とベースライン管理策の割り当て:

P1	**低** SA-4 (10)	**中** SA-4 (1) (2) (9) (10)	**高** SA-4 (1) (2) (9) (10)

SA-5 情報システム文書

管理策:組織は、

a. 以下を説明する、情報システム、システムコンポーネント、または情報システムサービスのアドミニストレータ向けのドキュメントを取得する:
   1. システム、コンポーネント、またはサービスのセキュアな設定、インストール,、および運用
   2. セキュリティ機能／メカニズムの有効利用とメンテナンス
   3. 管理(すなわち、特権)機能の設定と使用に関する既知の脆弱性
b. 以下を説明する、情報システム、システムコンポーネント、または情報システムサービスのユーザ向けのドキュメントを取得する:
   1. ユーザが利用できるセキュリティ機能／メカニズム、そして、それらのセキュリティ機能／メカニズムをどのようにして有効利用するか
   2. 個人がそのシステム、コンポーネント、またはサービスをより安全に利用できるようにする、ユーザインタラクション手段
   3. システム、コンポーネント、またはサービスのセキュリティを維持するとった、ユーザ側の責任
c. 情報システム、システムコンポーネント、または情報システムサービスに関するドキュメントが入手できない、または存在しない場合に、そうしたドキュメントを入手するための試みと、対応するための[指定:組織が定めたアクション]を文書化する
d. リスクマネジメント戦略に沿って、必要に応じてドキュメントを保護する
e. ドキュメントを [指定: 組織が定めた職員または役職]に配布する。

補足的ガイダンス:この管理策は、情報システム、システムコンポーネント、および情報システムサービスに関連するセキュリティ管理策の導入と運用について、組織の職員が理解するのを支援する。組織は、提供される内容の質／完全さを判断するための具体的な対策を立てる。必要なドキュメントを入手できないことは、たとえば、情報システム／コンポーネントの年数がかなりたっている、または開発者や請負業者からのサポートが得られない場合に発生する。そうした状況では、選択されたドキュメントがセキュリティ管理策の効果的な導入または運用には不可欠な場合には、組織がドキュメントを作り直す必要がある。選択されたシステム、コンポーネント、またはサービスに関するドキュメントの保護レベルは、そのシステムのセキュリティカテゴリまたは分類レベルに相応する。たとえば、米国防総省の重要な武器システムまたは指揮管理システムに関連するドキュメントは、通常は、日常的な管理システムよりも高いレベルの保護を必要とするだろう。情報システムの脆弱性を扱うドキュメントも、より高いレベルの保護を必要とするだろう。情報システムのセキュアな稼働は、たとえば、初めにシステムを起動し、システムが稼働してある程度時間が経過したら、セキュアなシステム稼働を再開することを含む。関連する管理策:CM-6・CM-8・PL-2・PL-4・PS-2・SA-3・SA-4。

拡張管理策:

(1) 情報システム文書 | セキュリティ管理策の機能特性
[削除された:SA-4(1)に統合された]

(2) 情報システム文書 | セキュリティ関連の外部システムインターフェース
[削除された:SA-4(2)に統合された]

(3) 情報システム文書 | 上位レベル設計
[削除された:SA-4(2)に統合された]

(4) 情報システム文書 | 下位レベル設計
[削除された:SA-4(2)に統合された]

(5) 情報システム文書 | ソースコード
[削除された:SA-4(2)に統合された]

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** SA-5	**中** SA-5	**高** SA-5

SA-6 ソフトウェアの利用の制限

[削除された:CM-10 および SI-7 に統合された]

SA-7 ユーザによるソフトウェアのインストール

[削除された:CM-11 および SI-7 に統合された]

SA-8 セキュリティエンジニアリング原則

管理策:組織は、情報システムの仕様書、設計、開発、導入、および変更に、情報システムのセキュリティエンジニアリング原則を適用する。

補足的ガイダンス:組織が セキュリティエンジニアリング原則を適用するのは、主に、新規開発の情報システムや、大幅なアップグレードがなされるシステムである。レガシーシステムでは、組織はシステムのアップグレードや変更時に、それらのシステム内のハードウェア、ソフトウェア、およびファームウェアの現在の状態を考慮して、可能な範囲内でセキュリティエンジニアリング原則を適用する。セキュリティエンジニアリング原則は、たとえば、以下を含む:①階層化された保護機能を開発する②設計の基盤となる健全なセキュリティポリシー、セキュリティアーキテクチャ、およびセキュリティ管理策を確立する③セキュリティ要求事項をシステム開発ライフサイクルに組み入れる④物理的および論理的セキュリティ境界を明確にする⑤セキュアなソフトウェアを開発する方法について、システム開発者がトレーニングを受けるようにする⑥セキュリティ管理策が組織のニーズと運用ニーズを満たすよう、管理策を調整する⑦使用事例、脅威エージェント、攻撃ベクトル、攻撃パターン、そして、リスクを軽減するのに必要な補完的管理策と設計パターンを特定するための、脅威のモデル化を実施するならびに⑧リスクを許容レベルにまで軽減し、情報に基づいたリスクマネジメントに関する意思決定を可能にする。関連する管理策は、PM-7・SA-3・SA-4・SA-17・SC-2・SC-3。

拡張管理策:なし

参考文献:NIST Special Publication 800-27

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** SA-8	**高** SA-8

SA-9 外部情報システムサービス

管理策:組織は、

a. 外部情報システムサービスのプロバイダに対して、該当する連邦法・大統領命令・指令・政策・規制・標準・指針に従って、組織の情報セキュリティ要求事項を満たし、[指定:組織が定めたセキュリティ管理策]を導入することを要求する

b. 外部情報システムサービスに関して、政府によるモニタリングと、ユーザの役割と責任を定義し、文書化する

c. 外部サービスプロバイダによるセキュリティ管理策の遵守状況を継続的にモニタリングするための、[指定:組織が定めたプロセス、手法、および技法]を用いる。

補足的ガイダンス:外部情報システムサービスは、組織が認可を出す範囲外で実施される情報システムサービスである。これは、組織の情報システムによって利用されるものの、その一部ではないサービスを含む。FISMAおよびOMBポリシーは、連邦政府の情報を処理、保存、または伝送する外部サービスプロバイダを利用する組織、あるいは連邦政府に代わって情報システムを運用する外部サービスプロバイダを利用する組織に対して、そうしたプロバイダが、連邦政府が満たす必要があるセキュリティ要求事項と同じ要求事項を満たすことを確実にするよう求めている。組織が外部サービスプロバイダとの間で関係を築く方法としては、たとえば、ジョイントベンチャー、ビジネスパートナーシップ、契約、省庁間の取り決め、事業部門間の取り決め、ライセンス契約、およびサプライチェーンの交換がある。外部情報システムサービスの利用により生じるリスクを軽減する責任は、運用認可責任者にある。組織にとって外部のサービスである場合、トラストチェーンの構築には、複雑になりうる消費者—プロバイダ関係に関与する各プロバイダが、提供されるサービスに対して適切な保護を行っていることに関して、一定レベルの信頼が組織によって確立され、維持されることが求められる。このトラストチェーンの範囲と性質は、組織と外部プロバイダの関係によって異なる。組織は、信頼関係を長期にわたってモニタリングできるよう、信頼関係のベースを文書化する。外部情報システムサービスに関するドキュメントは、政府、サービスプロバイダ、およびユーザの各々のセキュリティ上の役割と責任、そしてサービス内容合意書を含む。サービス内容合意書では、セキュリティ管理策のパフォーマンスについて期待されることを定義し、測定可能な結果を記述し、特定された遵守されていないの項目に対する是正措置と対応のための要求事項を示す。関連する管理策は、CA-3・IR-7・PS-7。

拡張管理策:

(1) 外部情報システム | リスクアセスメント / 組織による承認

組織は、

(a) 専用の情報セキュリティ サービスを調達する、または外部委託する前に、リスクアセスメントを実施する

(b) 専用の情報セキュリティ サービスの調達または外部委託が、[指定:組織が定めた職員または役職]によって承認されるようにする。

補足的ガイダンス:専用の情報セキュリティ サービスには、たとえば、インシデントのモニタリング、分析、および対応、ファイアウォールなどの情報セキュリティ関連機器の操作、鍵管理サービスがある。関連する管理策は、CA-6・RA-3。

(2) 外部情報システム | 機能 / ポート / プロトコル / サービスを明確にする

組織は、[指定:組織が定めた外部情報システムサービス]のプロバイダに対して、そうしたサービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にする。

補足的ガイダンス：外部サービスプロバイダから提供される、そうしたサービスの提供に使用される特定の機能、ポート、プロトコル、およびサービスに関する情報は、特定の機能／サービスを制限する場合や、特定のポート／プロトコルを遮断する場合のトレードオフを理解する必要が生じた場合に、特に有用である。関連する管理策は、CM-7。

(3) 外部情報システム | プロバイダとの間に信頼関係を構築し、維持する

組織は、[指定：（組織が定めた）セキュリティ要求事項・（組織が定めた）属性・（組織が定めた）要員を（組織が定めた）受け入れられる信頼関係とともに定義する条件]に基づいて、外部サービスプロバイダとの間に信頼関係を構築・文書化のうえ維持する。

補足的ガイダンス：外部サービスの利用により生じるリスクが許容レベルであることについての信頼の度合は、組織が外部サービスプロバイダに寄せる信頼（個別に、あるいは総合で）による。信頼関係は、関与するサービスプロバイダが、提供されるサービスに対して適切な保護を行っていることに関して、組織がさらなる自信を得られるようにする。そうした関係は、利用者－プロバイダ間のやりとりに関与する組織の数や、従属関係と信頼レベル、それらの組織間のやりとりのタイプによっては複雑になる。場合によっては信頼の度合が、サービス／情報の保護に必要なセキュリティ管理策の導入と、それらの管理策の有効性に関して提出されるエビデンスに関して、組織が外部サービスプロバイダをどの程度、直接管理できるかに基づくこともある。管理レベルは、通常、外部サービスプロバイダと交わす契約またはサービス内容合意書の諸条件によって定められ、その範囲は幅広い管理（例：プロバイダに対するセキュリティ要求事項を規定する契約または取り決めについて交渉する）から、非常に限られた管理（例：商用通信サービスなどの汎用サービスを得るために契約またはサービス内容合意書を利用する）までさまざまである。この他にも信頼の度合は、必要なセキュリティ管理策が導入されていることと、管理策の有効性に対する決定因子が存在することを組織に納得させることができる要素の有無によって左右されることがある。たとえば、確立された事業部門間関係を通じて組織に提供される、個別に認可された外部情報システムサービスは、それらのサービスを使用する組織のリスク許容範囲に収まることに関して、相応の信頼感を与えるだろう。外部サービスプロバイダが選択されたサービスを他の外部組織に委託することも考えられるが、この場合トラストチェーンの管理がより困難に、かつ複雑になる。サービスの性質によっては、組織が、外部のプロバイダに大きな信頼を寄せることが非常に困難だと感じる場合がある。このような状況は、プロバイダ側がもともと信用できないからではなく、それらのサービスに内在するリスクに起因する。

(4) 外部情報システム | プロバイダ側と利用者側の利害の一致

組織は、[指定：組織が定めた外部サービスプロバイダ]の利害が組織の利害と一致し、反映することを確実にするための、[指定：組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス：組織による外部サービスプロバイダの使用が増えるにつれて、サービスプロバイダの利害と組織の利害が異なる可能性もある。そうした場合、単に技術面、手続き面、または運用面での正しい対策を実施したとしても、それらの対策を実施・管理するサービスプロバイダが利用者側である組織の利害に合う形で経営していないと、十分でないだろう。そうした問題に対処するために組織が取れるアクションには、たとえば、選択されたサービスプロバイダの職員に対する素性調査を要求すること、所有者記録を調べること、信頼できるサービスプロバイダ（すなわち、組織が過去によい経験をしたプロバイダ）のみを使用すること、サービスプロバイダの施設に定期的に訪問する／予告なしで訪問することがある。

(5) 外部情報システム | 処理拠点、保管拠点、およびサービス拠点

組織は、[指定：組織が定めた要求事項または条件]に基づいて、[選択（1つ以上）：情報処理;情報／データ;情報システムサービス]のロケーションを[指定：組織が定めたロケーション]に限定する。

補足的ガイダンス：組織にとって極めて重要な情報処理、情報／データ保管、または情報システムサービスの拠点は、組織がミッション／業務機能を成功裏に実施する能力に直接的な影響を及ぼす。このような状況は、外部プロバイダが処理、保管、またはサービスの拠点を管理する場合に発生する。外部プロバイダが処理、保管、またはサービスの拠点の選択に使用する基準は、組織の基準とは異なる場合がある。たとえば、組織は、データ／情報の保管場所を特定の拠点に限定することによって、情報セキュリティの違反／侵害が発生した場合のインシデント対応活動（例：法医学的分析、事後の調査）を容易にしたいと考えるだろう。そうしたインシデント対応活動は、処理または保管がなされる拠点や、情報システムサービスが提供される拠点の準拠法またはプロトコルによる負の影響を受ける場合がある。

参考文献：NIST Special Publication 800-35

優先順位とベースライン管理策の割り当て：

P1	**低** SA-9	**中** SA-9 (2)	**高** SA-9 (2)

SA-10 開発者による構成管理

管理策：組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する：

a. システム、コンポーネント、またはサービスの［選択（1つ以上）：設計・開発・導入・運用］時に、構成管理を実施する
b. ［指定：組織が定めた、構成管理下にある構成項目］に対する変更を文書化、管理し、その整合性を確保する
c. システム、コンポーネント、またはサービスに対する変更は、組織が承認した変更のみ実施する
d. 承認された、システム、コンポーネント、またはサービスに対する変更と、そうした変更がもたらすセキュリティ影響を文書化する
e. システム、コンポーネント、またはサービスのセキュリティ上の欠陥と、欠陥がどのように解消されたかを追跡し、分かったことを［指定：組織が定めた職員］に報告する

補足的ガイダンス：管理策は、社内で情報システムの開発とインテグレーションを行っている組織にも適用される。組織は、効果的なセキュリティ対策を実施していることへの証として、開発者が実施する構成管理活動の質と完全さを検証する。対策は、たとえば、不正な変更または破壊から保護すること、システムハードウェア、ソフトウェア、およびファームウェアのセキュリティに関連する部分を生成するのに使用される、すべての資料の原本を保護することを含む。情報システム、情報システムコンポーネント、または情報システムサービスに対する変更の整合性を維持するには、システム開発ライフサイクル全体を通して構成管理を行い、許可された変更を追跡し、不正な変更を防止することが求められる。構成管理下に置かれる構成項目（その存在／使用が他のセキュリティ管理策によって求められる）には、形式的なモデル仕様書、機能仕様書、上位レベル設計仕様書、および下位レベル設計仕様書、その他の設計データ、実行計画書、ソースコードと、ハードウェアの図解、実行されているオブジェクトコード、セキュリティ関連のハードウェア記述とソフトウェア／ファームウェアソースコードの新しいバージョンと旧バージョンを比較するためのツール試験装置およびドキュメントがある。組織のミッション／業務ニーズと、現時点の契約関係の性質によっては、システム開発ライフサイクルの運用フェーズとメンテナンスフェーズにおいて、開発者が構成管理に必要な支援を行うことがある。関連する管理策は、CM-3・CM-4・CM-9・SA-12・SI-2。

拡張管理策:

(1) 開発者による構成管理 | ソフトウェア / ファームウェアの完全性検証

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、ソフトウェアコンポーネントとファームウェアコンポーネントの完全性を確認できるようにすることを要求する。

補足的ガイダンス:この拡張管理策は、組織が、ソフトウェアコンポーネントとファームウェアコンポーネントに対する不正な変更を開発者が提供するツール、技法、および／またはメカニズムを使用して検出できるようにする。完全性チェックメカニズムは、ソフトウェアコンポーネントとファームウェアコンポーネントの偽造にも対処できる。組織は、たとえば、開発者が提供するセキュアな一方向性ハッシュを使用してソフトウェアコンポーネントとファームウェアコンポーネントの完全性を確認する。引き渡されるソフトウェアコンポーネントとファームウェアコンポーネントは、そうしたコンポーネントに対するあらゆるアップデートも含む。関連する管理策は、SI-7。

(2) 開発者による構成管理 | 代替の構成管理プロセス

組織は、構成管理に専念する開発者チームが存在しない場合は、組織の職員を使用した代替の構成管理プロセスを用意する。

補足的ガイダンス:代替の構成管理プロセスは、たとえば、組織が市販の IT 製品を使用する場合に必要になる。代替の構成管理プロセスは、以下を満たす組織の職員を含む:①情報システム、システムコンポーネント、および情報システムサービスに対して提案されている変更をレビュー／承認する責任がある②システム、コンポーネント、またはサービスに対する変更を実施する前に、セキュリティ影響分析を実施する(例:開発時に、変更がもたらすセキュリティ影響について考慮する構成管理委員会であり、該当する場合、組織と開発者の両方の代表者を含む)。

(3) 開発者による構成管理 | ハードウェアの完全性検証

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、ハードウェアコンポーネントの完全性を確認できるようにすることを要求する。

補足的ガイダンス:この拡張管理策は、組織が、ハードウェアコンポーネントに対する不正な変更を開発者が提供するツール、技法、および／またはメカニズムを使用して検出できるようにする。組織は、たとえば、開発者が提供する複製しにくいラベルや、検証可能なシリアル番号を使用して、また、改ざん防止技術の導入を要求することによって、ハードウェアコンポーネントの完全性を確認する。引き渡されるハードウェアコンポーネントは、そうしたコンポーネントに対するアップデートも含む。関連する管理策は、SI-7。

(4) 開発者による構成管理 | 信頼できる生成

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、セキュリティ関連のハードウェア記述とソフトウェア／ファームウェアソース／オブジェクトコードの新しいバージョンと旧バージョンを比較するためのツールの使用を要求する。

補足的ガイダンス:この拡張管理策は、開発時の、ハードウェアコンポーネント、ソフトウェアコンポーネント、ファームウェアコンポーネントのバージョン間の変更を取り扱う。対照的に SA-10(1)と SA-10(3)は、組織が、ハードウェアコンポーネント・ソフトウェアコンポーネント・ファームウェアコンポーネントに対する不正な変更を開発者が提供するツール、技法、および／またはメカニズムを使用して検出できるようにする。

(5) 開発者による構成管理 | バージョン管理のための、マッピングの整合性

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、現バージョンのセキュリティに関連するハードウェア、ソフトウェア、およびファームウェアについて記述するマスタービルドデータ(ハードウェア図面と、ソフトウェア／ファーム

ウェアコード)と、現バージョンのデータのマスターコピー間のマッピングの整合性を維持することを要求する。

補足的ガイダンス:この拡張管理策は、初期開発時と、システムライフサイクル更新時のハードウェアコンポーネント、ソフトウェアコンポーネント、ファームウェアコンポーネントに対する変更を取り扱う。セキュリティに関連するハードウェア、ソフトウェア、およびファームウェア(設計とソースコードを含む)のマスターコピーと、システムが稼働する環境で使用されているマスターコピー内の対応データ間の整合性を維持することは、極めて重要なミッションおよび/または業務機能を支援する組織の情報システムの可用性を確保するうえで不可欠である。

(6) 開発者による構成管理 | 信頼できる配布

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、組織に配布されるセキュリティに関連するハードウェア、ソフトウェア、およびファームウェアアップデートが、マスターコピーが示すものであることを確認するための手順の実施を要求する。

補足的ガイダンス:セキュリティに関連するハードウェア、ソフトウェア、およびファームウェアアップデートの信頼できる配布は、そうしたアップデートが、開発者が保持するマスターコピーを忠実に表現したものとなり、かつ、配布時に改ざんされないことを保証する。

参考文献:NIST Special Publication 800-128

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** SA-10	**高** SA-10

SA-11 開発者によるセキュリティテストおよび評価

管理策:組織は、情報システム・システムコンポーネント・情報システムサービスのいずれかを開発した者に対して、以下を実施することを要求する:

a. セキュリティアセスメント計画を作成・実施する

b. [選択(1つ以上): 単体; 統合; システム; 回帰] テスト/評価を[指定:組織が定めた深さと範囲]で実施する

c. セキュリティアセスメント計画を実施したというエビデンスを生成し、セキュリティテスト/評価の結果を示す

d. 検証可能な欠陥修正プロセスを実施する

e. セキュリティテスト/評価時に特定された欠陥を修正する。

補足的ガイダンス:段階的なセキュリティテスト/評価は、システム開発ライフサイクルの設計フェーズ後のすべてのフェーズで行われる。そうしたテスト/評価では、必要なセキュリティ管理策が正しく導入されているか、意図したとおりに運用されているか、適切なセキュリティポリシーが実施されているか、定められたセキュリティ要求事項が満たされているかを確認する。情報システムのセキュリティ特性は、システムコンポーネントの相互接続、またはそれらのコンポーネントに対する変更による影響を受ける場合がある。これらの相互接続または変更(例:アプリケーションやオペレーティングシステムのアップグレードまたは交換)は、すでに導入されているセキュリティ管理策に負の影響をもたらす可能性がある。本管理策は潜在的な欠陥を減らす、または、なくすために開発者が実施できる追加のセキュリティテスト/評価を示す。カスタムソフトウェアアプリケーションのテストでは、静的解析、動的解析、バイナリー解析、あるいはそれらの3つのアプローチの混合などのアプローチが必要になる場合がある。開発者は、これらの解析アプローチをさまざまなツール(例:ウェブ上のアプリケーションスキャナー、静的解析ツール、バイナリーアナライザ)で実現することができ、また、これらの解析アプローチをソースコードレビ

ューに使用してもよい。セキュリティアセスメント計画は、ソフトウェアコンポーネントとファームウェアコンポーネントの分析、テスト、評価、およびレビューのタイプ、適用される厳密さの度合、それらのプロセス時に生成されるアーチファクトのタイプを含む、開発者が実施を計画している具体的な活動を示す。セキュリティテスト／評価の「深さ」とは、アセスメントプロセス（例：ブラックボックステスト、グレーボックステスト、またはホワイトボックステスト）に関連する厳密さと詳細レベルである。セキュリティテスト／評価の「範囲」とは、アセスメントプロセスに含まれるアーチファクトのスコープ（すなわち、数とタイプ）である。契約書は、セキュリティアセスメント計画の受け入れ基準、欠陥修正プロセス、それらの計画／プロセスがきちんと適用されたことを示すエビデンスを規定する。アセスメント計画、エビデンス、およびドキュメントをレビューし保護するための手法は、情報システムのセキュリティカテゴリまたは分類レベルに相応する。契約書がドキュメントの保護に関する要求事項を規定する場合がある。関連する管理策は、CA-2・CM-4・SA-3・SA-4・SA-5・SI-2。

拡張管理策：

(1) 開発者によるセキュリティテストおよび評価 | 静的なコード解析

組織は、情報システム・システムコンポーネント・情報システムサービスのいずれかを開発している者に対して 、静的なコード解析用ツールを使用して、共通の欠陥を特定し、解析結果を文書化することを要求する。

補足的ガイダンス：静的なコード解析は、セキュリティレビューのための技術と方法を提供する。そうした解析は、セキュリティ上の脆弱性を特定し、セキュリティコーディングプラクティスを実施するために使用できる。静的なコード解析は、開発プロセスの早い段階で使用され、コードが変更されたら自動的にスキャンされ潜在的な欠陥が特定されるといった場合に、その効果が最大になる。静的解析は、修正に関する明確な手引きを、欠陥と共に示す。そのため、開発者は、そうした欠陥を修正できるようになる。静的解析が正しく実施されたというエビデンスは、たとえば、致命的な欠陥の総合欠陥密度、欠陥が開発者またはセキュリティの専門家によって検査されたというエビデンス、欠陥が修正されたというエビデンスを含む。所見の見逃し（一般的には「無視された」または「誤判定」と称される）の密度が過度に高い場合、解析プロセスまたは解析ツールに問題があると考えられる。そうした場合、組織は、提示されたエビデンスの有効性と、他から得たエビデンスを比較する。

(2) 開発者によるセキュリティテストおよび評価 | 脅威分析と脆弱性分析

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、脅威分析と脆弱性分析を実施して、その後、形成されたシステム、コンポーネント、またはサービスのテスト／評価を行うことを要求する。

補足的ガイダンス：アプリケーションは、システム開発ライフサイクルの要件定義フェーズと設計フェーズで作成された設計仕様から大きく逸脱する可能性がある。したがって、出荷前に行う情報システム、システムコンポーネント、および情報システムサービスの脅威分析と脆弱性分析は、それらのシステム、コンポーネント、およびサービスの効果的な運用には不可欠である。システム開発ライフサイクルの、このフェーズで実施される脅威分析と脆弱性分析は、設計変更または導入変更が説明されることと、それらの変更に起因して作り込まれた新たな脆弱性がレビューされ、軽減されることを支援する。関連する管理策は、PM-15・RA-5。

(3) 開発者によるセキュリティテストおよび評価 | アセスメント計画 / エビデンスの独立検証

組織は、

(a) ［指定：組織が定めた、独立性に関する基準］を満たしている独立エージェントに対して、開発者によるセキュリティアセスメント計画が正しく実施されているかどうかを確認し、セキュリティテスト／評価時に生成されたエビデンスを確認するよう求める

(b) その独立エージェントに対して、確認プロセスを完了させるのに十分な情報が提供されるようにする、または、そうした情報を得るための権限が与えられるようにする。

補足的ガイダンス：独立エージェントは、開発者によるセキュリティアセスメント計画が正しく実施されているかどうかを確認するのに必要な資格（すなわち、専門知識、技能、トレーニング、および経験）を有する。関連する管理策：AT-3・CA-7・RA-5・SA-12。

(4) 開発者によるセキュリティテストおよび評価 | 手動でのコードレビュー

組織は、情報システム・システムコンポーネント・情報システムサービスのいずれかを開発している者に対して、[指定：組織が定めた特定のコード]を[指定：プロセス・手順・技法として組織が定めたものの全て（またはそれらのいずれか）]を使用して手動でレビューすることを要求する。

補足的ガイダンス：手動でのコードレビューは、通常、情報システムの極めて重要なソフトウェアコンポーネントとファームウェアコンポーネントを対象に実施される。そうしたコードレビューは、アプリケーションの要件またはコンテクストを知る必要がある欠陥を特定するのに、とりわけ効果的である。そうした情報は、静的解析や動的解析などの、より自動的な解析ツールと技法では通常は利用できない。手動でのレビューから便益を得るのは、たとえば、アプリケーション制御とアクセス制御マトリクスの照合や、暗号の実装と制御のより詳細な側面のレビューがある。

(5) 開発者によるセキュリティテストおよび評価 | 侵入テスト / 解析

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、侵入テストを[指定：組織が定めた広さ／深さ]で、かつ、[指定：組織が定めた制約]のもとで実施することを要求する。

補足的ガイダンス：侵入テストはアセスメント方法の一つであり、アセサーは、利用可能なすべての IT 製品および／または情報システムドキュメント（例：製品／システム設計仕様書、ソースコード、アドミニストレータ／オペレータ向けマニュアル）を使用して、特定の制約のもとで、IT 製品や情報システムに導入されているセキュリティ機能の回避を試みる。侵入テストでは、たとえば、熟練したセキュリティの専門家が、敵対者による活動をシミュレートしてホワイトボックステスト、グレーボックステスト、またはブラックボックステストを実施する。侵入テストの目的は、導入ミス、設定の誤り、あるいは運用のための配備に関する弱点または欠陥に起因する、IT 製品や情報システムの脆弱性を明らかにすることにある。侵入テストは、自動／手動でのコードレビューと併せて実施することができる。そうすることで、普通の解析よりも詳細な解析が可能になる。

(6) 開発者によるセキュリティテストおよび評価 | 攻撃の矢面についてレビューする

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して 、攻撃の矢面についてレビューすることを要求する。

補足的ガイダンス：情報システムの攻撃の矢面とは、サイバー攻撃に対してシステムが脆弱になる露出部のことをいう。攻撃の矢面には、情報システム（ハードウェアコンポーネント、ソフトウェアコンポーネント、ファームウェアコンポーネント）の弱点または欠陥が、敵対者による脆弱性利用の機会を与えてしまうアクセス可能なすべての領域が含まれる。攻撃の矢面についてレビューすることで、開発者は以下を実施できるようになる：①情報システムに対する設計変更と導入変更の両方を解析するならびに②それらの変更により生じる攻撃ベクトルを緩和する。特定された欠陥の修正は、たとえば、安全でない機能の廃止を含む。

(7) 開発者によるセキュリティテストおよび評価 | テスト / 評価の範囲を確認する

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、[指定：組織が定めた深さのセキュリティテスト／評価]が、必要なセキュリティ管理策すべてを対象としていることの確認を要求する。

補足的ガイダンス：セキュリティテスト／評価が必要なセキュリティ管理策すべてを対象としているかの確認は、形式的でなものから形式的なものまで、さまざまな解析手法によって行うことができる。これらの手法は各々が、解析がどの程度形式的であるかに応じたレベル

の保証を提供する。最高レベルの保証をもって、対象となるセキュリティ管理策を厳密に示すには、形式的なモデリング手法と解析手法（管理策の導入と、対応するテストケース間の相互関係を含む）を使用することができる。

(8) 開発者によるセキュリティテストおよび評価 | 動的なコード解析

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、動的なコード解析用ツールを使用して、共通の欠陥を特定し、解析結果を文書化することを要求する。

補足的ガイダンス：動的なコード解析は、ソフトウェアプログラムの実行時の検証を行うための手段であり、ソフトウェアプログラムを実行してメモリーの破損、ユーザ権限に関わる問題、およびその他の潜在的なセキュリティ問題の有無を確認できるツールが使用される。また、動的なコード解析では、セキュリティ機能が設計された通りに機能するかどうかを確認するためにランタイムツールが使用される。ファズテストとして知られている特殊なタイプの動的解析は、不正な形式のデータまたはランダムデータを意図的にソフトウェアプログラムに投入することによって、プログラムの不具合を引き起こす。ファズテスト戦略は、アプリケーションの目的の用途と、アプリケーションの機能仕様書と設計仕様書から導出される。動的なコード解析のスコープを理解し、さらに、提供される保証について理解するために、組織はコードカバレージ解析（テストされたサブルーチンの割合、またはテストスイートの実行時に呼び出されたプログラムステートメントの割合などの、評価指標を使用してテストされたコードの割合を調べる）や、一致分析（英語以外の言語や軽蔑語などの、ソフトウェアコードにふさわしくない語が含まれていないかをチェックする）の実施も検討する。

参考文献：ISO/IEC 15408・NIST Special Publication 800-53A・ウェブサイト http://nvd.nist.gov および http://cwe.mitre.org ならびに http://cve.mitre.org および http://capec.mitre.org

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** SA-11	**高** SA-11

SA-12 サプライチェーンの保護

管理策：組織は、包括的な、深層防護を可能にする情報セキュリティ戦略の一環としての［指定：組織が定めたセキュリティ対策］を実施することで、情報システム、システムコンポーネント、または情報システムサービスに対するサプライチェーン関連の脅威から保護する。

補足的ガイダンス：情報システム（それらのシステムを構成するシステムコンポーネントを含む）は、システム開発ライフサイクル全体を通して（すなわち、設計、開発、製造、パッケージング、組み立て、配布、システムの統合、運用、メンテナンス、およびリタイアメント）保護される必要がある。組織の情報システムの保護は、脅威認識、システム開発ライフサイクルの各フェーズにおける脆弱性の特定、管理、および軽減、そして、リスクに対応するための補完的な、相互に補強し合う戦略の使用によって実現される。組織は、情報システムとシステムコンポーネントのサプライチェーン関連のリスクに対処し、脅威、リスク、および必要なセキュリティ管理策に関して調達要員を教育するための、標準化されたプロセスの実施を検討する。組織は、調達／資材調達プロセスを用いて、サプライチェーンを提供する組織に対して、以下を実現するために必要なセキュリティ対策の実施を要求する：①サプライチェーン内の各段階で不正な変更がなされる可能性を減らす②情報システムと情報システムコンポーネントの配達を受ける前に、そうしたシステム／コンポーネントを保護する。この拡張管理策は、情報システムサービスにも適用される。セキュリティ対策は、たとえば、以下を含む：①開発システム、開発設備、開発システムに対する外部からの接続に対するセキュリティ管理策②開発に携わる職員の信用度調査ならびに③配送／倉庫保管時に、不正開封の跡がすぐ分かるパッケージングを使用すること。開発計画、エビデンス、およびドキュメントをレビューし、保護するための手法は、その情報システムのセキュ

リティカテゴリまたは分類レベルに相応する。契約書がドキュメントの保護に関する要求事項を規定する場合がある。関連する管理策は、AT-3・CM-8・IR-4・PE-16・PL-8・SA-3・SA-4・SA-8・SA-10・SA-14・SA-15・SA-18・SA-19・SC-29・SC-30・SC-38・SI-7。

拡張管理策:

(1) サプライチェーンの保護 | 調達戦略 / ツール / 方法

組織は、情報システム、システムコンポーネント、または情報システムサービスを供給業者から購入する際に、[指定:組織が定めた、調整された調達戦略、契約ツール、および調達方法]を用いる。

補足的ガイダンス:システム開発ライフサイクルの早い段階で組織が調達／資材調達プロセス使用することは、サプライチェーンを保護するための重要な手段となる。組織は、あらゆる情報源からの情報を解析して、調達戦略、ツール、および方法の調整に情報を提供する。利用可能なツールと技法は、数多く存在する(例:情報システムまたはシステムコンポーネントの末端の利用を、身元を伏せた購入またはフィルターをかけた購入によって、見えないようにする)。組織は、また、以下を満たす供給業者に対するインセンティブの創出を検討する:①必要なセキュリティ対策を実施している②組織のプロセスおよびセキュリティ実践に対する透明性を推進している③下位の供給業者のプロセスおよびセキュリティ実践と、極めて重要な情報システムコンポーネント、およびサービスに対する追加の信用度調査を行っている④特定の供給業者または国からの購入を禁止しているならびに⑤傷ついた、または偽造されたコンポーネントを禁止することに関して契約文書を用意している。また、組織は、購入に関する決定から必要な配送までの時間を最小にするによって、敵対者が情報システムコンポーネントまたは製品にエラーを持ち込む機会を最小限に抑える。最後に、組織はサプライチェーン関連のリスクを減らすために、信頼されている／管理されている配布、配送、および倉庫保管オプションを使用することができる(例:配送／倉庫保管時に、情報システムコンポーネントに対して、不正開封の跡がすぐ分かるパッケージングを使用することを要求する)。関連する管理策は、SA-19。

(2) サプライチェーンの保護 | 供給業者に対するレビュー

組織は、情報システムまたはシステムコンポーネントもしくは情報システムサービスを調達するための契約を結ぶ前に前に、供給業者に対するレビューを実施する。

補足的ガイダンス:供給業者に対するレビューは、たとえば、以下を含む:①情報システム、システムコンポーネント、および情報システムサービスを設計、開発、テスト、導入、検証、配送し、サポートするのに使用される供給業者側のプロセスを分析する; ならびに②必要なセキュリティ能力を備えたシステム、コンポーネント、またはサービスの開発に必要な、供給業者側のトレーニングと経験をアセスメントする。これらのレビューは、システム開発ライフサイクルにおける供給業者側の活動に対する可視性を高めて、組織がサプライチェーン関連のリスクをより効果的に管理できるようにする。供給業者に対するレビューは、また、一次供給業者がセキュリティ対策を実施しているかどうか、また、下位の供給業者(たとえば、二次および三次供給業者や、下請業者)に対する信用度調査を実施しているかどうかを判断するのに役立つ。

(3) サプライチェーンの保護 | 信頼されている配送および倉庫保管

[削除された:SA-12(1)に統合された]

(4) サプライチェーンの保護 | 供給業者の多様性

[削除された:SA-12(13)に統合された]

(5) サプライチェーンの保護 | 被害を抑える

組織は、組織のサプライチェーンを特定し、標的にする敵対者がもたらす被害を抑えるための、[指定:組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス：サプライチェーン関連のリスクは、APT (advanced persistent threat)の一部である。敵対者がサプライチェーンを成功裏に特定し、標的にする可能性を減らすためのセキュリティ対策と対策は、たとえば、以下を含む：①特定の組織を標的にしたサプライチェーン攻撃を介して破損した情報システム、コンポーネント、または製品を調達するリスクを減らすためにも、カスタム設定の購入を避ける②多様な供給業者を使用することで、サプライチェーン内のいずれかの供給業者によってもたらされる被害を抑える③業界で評判が高い、承認されたベンダーが記載されているリストを使用するならびに④調達におけるカーブアウト（すなわち、コミットメントや義務からの除外）を使用する。

(6) サプライチェーンの保護 | 調達にかかる時間を最小にする

[削除された：SA-12(1)に統合された]

(7) サプライチェーンの保護 | 選択 / 受け入れ / アップデートに先立つアセスメント

組織は、情報システム、システムコンポーネント、または情報システムサービス の選択、受け入れ、またはアップデートに先立って、アセスメントを実施する。

補足的ガイダンス：アセスメントは、たとえば、テスト、評価、レビュー、および解析を含む。独立した、第三者組織または組織の職員は、システム、コンポーネント、製品、ツール、およびサービスのアセスメントを実施する。組織は、たとえば、悪質コード、悪質プロセス、欠陥のあるソフトウェアや、偽造などの、意図していない脆弱性と意図的に作り込まれた脆弱性を明らかにするためのアセスメントを実施する。アセスメントは、たとえば、静的解析、動的解析、シミュレーション、ホワイトボックステスト、グレーボックステスト、ブラックボックステスト、ファズテスト、侵入テスト、そして、コンポーネントまたはサービスが本物であることを確認すること（例：タグ、暗号学的ハッシュによる検証、または電子署名を使用して）を含む。セキュリティアセスメント時に生成されたエビデンスは、組織が実施する後続のアクションに役立つよう、文書化させる。関連する管理策は、CA-2・SA-11。

(8) サプライチェーンの保護 | あらゆる情報源からの情報の利用

組織は、情報システム、システムコンポーネント、または情報システムサービスの供給業者および供給業者の候補に対して、あらゆる情報源からの情報の解析を実施する。

補足的ガイダンス：あらゆる情報源からの情報の解析は、組織が、エンジニアリング、調達、およびリスクマネジメントに関する意思決定に情報を与えるために実施するものである。あらゆる情報源とは、人による諜報、画像諜報、測定およびシグネチャ諜報、無線諜報、ならびに完了済みの情報収集から得たオープンソースデータを含むことが多く、そうした情報収集のための製品および／または組織と活動から成る。利用可能な場合、そうした情報は開発、製造、および配布のプロセス、要員、および環境における、意図的に作り込まれた脆弱性と意図していない脆弱性の両方に起因するリスクを分析するために使用される。このレビューは、リスクを管理するのに十分な複数の層を有するサプライチェーン内の、それぞれの層の供給業者に対して実施される。関連する管理策は、SA-15。

(9) サプライチェーンの保護 | 運用上のセキュリティ

組織は、情報システム、システムコンポーネント、または情報システムサービスのサプライチェーン関連の情報を保護するための分類ガイドに沿って、[指定：組織が定めた運用上のセキュリティ(OPSEC)対策]を実施する。

補足的ガイダンス：サプライチェーン情報は、たとえば、ユーザ識別情報および情報システムならびに情報システムコンポーネントを含めて、情報システムサービスの使用状況および供給業者の識別情報および供給業者のプロセスおよびセキュリティ要求事項および設計仕様書およびテストおよび評価の結果およびシステム／コンポーネントの構成を含む。この拡張管理策は、運用上のセキュリティの範囲を、供給業者と供給業者の候補が含まれるよう拡張する。運用上のセキュリティは、極めて重要な情報を特定し、その後以下を目的として、業務とその他の活動に付随する友誼的なアクションを分析するプロセスである：①敵対者によって観測される可能性のあるアクションを特定する②敵対者が取得する可能性の

ある兆候であり、解釈やつなぎ合わせによって、組織に危害を加えるための情報を十分な時間をかけて引き出すことを可能にするものを特定する③利用できる脆弱性を排除する、あるいは許容レベルにまで軽減するための保護対策または対策を実施するならびに④1つにまとめられた情報が、サプライチェーンの利用者または利用の機密性をどのように侵害するかについて考察する。運用上のセキュリティは、組織に対して、極めて重要なミッション／業務情報を供給業者に知らせないことを要求する場合もあり、また情報システム、システムコンポーネント、または情報システムサービスの末端の利用、または利用者を隠すための仲介者の利用を含む場合がある。関連する管理策は、PE-21。

(10) サプライチェーンの保護 | 本物であることと、改変されてないことを確認する

組織は、[指定：組織が定めたセキュリティ対策]を用いて、受け取った情報システムまたはシステムコンポーネントが本物であり、改変されていないことを確認する。

補足的ガイダンス：情報システムコンポーネントによっては、とりわけハードウェアの場合には、それらのコンポーネントが本物であるか、あるいは改変されていないかを確認するための技術的手段が用意されている。情報システムまたは情報システムコンポーネントが本物であるかを確認するためのセキュリティ対策には、たとえば、光タグ／ナノテクノロジータグを使用したタグ付けや、サイドチャネル解析がある。ハードウェアの場合、詳細な部品表により、ロジックが組み込まれている部品と、それらの部品とコンポーネントのロケーションが明らかになるだろう。

(11) サプライチェーンの保護 | エレメント、プロセス、および関係者の侵入テスト / 分析

組織は、情報システムまたはシステムコンポーネントもしくはまたは情報システムサービスに関連する[指定：組織が定めた、サプライチェーンエレメント、プロセス、および関係者]に対して、[選択（1つ以上）：組織による分析、独立した第三者による分析, 組織による侵入テスト、独立した第三者による侵入テスト]を実施する

補足的ガイダンス：この拡張管理策は、配送されるアイテムだけでなく、サプライチェーンの分析および／またはテストも取り扱う。サプライチェーンエレメントは、プログラム可能なロジックを含み、情報システムの機能にとって極めて重要な IT 製品または製品コンポーネントである。サプライチェーンプロセスは、①ハードウェア、ソフトウェア、およびファームウェア開発プロセス②出荷／取り扱い方法③職員による／物理的なセキュリティプログラム④プロベナンスを維持するための構成管理ツール／対策あるいは⑤サプライチェーンエレメントの生産／配布に関連するその他のプログラム、プロセス、または手順等で構成されるプロセスである。サプライチェーン関係者は、サプライチェーンにおいて特定の役割と責任を有する個人である。サプライチェーンエレメント、プロセス、および関係者の分析およびテスト中に生成されたエビデンスは、文書化され、組織のリスクマネジメント活動と、リスクマネジメントに関する意思決定に情報を与えるために使用される。関連する管理策は、RA-5。

(12) サプライチェーンの保護 | 組織間の合意

組織は、情報システム、システムコンポーネント、または情報システムサービスのサプライチェーンに関与する組織との間で、組織間の合意と手順を確立する。

補足的ガイダンス：組織間の合意と手順を確立することによって、サプライチェーンが侵害された場合に通知がなされる。サプライチェーンが侵害され、組織の情報システム（極めて重要なシステムコンポーネントを含む）に負の影響が及ぶ可能性がある、あるいは既に影響が及んでいる場合に早期に通知することは、そうしたインシデントに組織が適切に対応するためにも不可欠である。

(13) サプライチェーンの保護 | 極めて重要な情報システムコンポーネント

組織は、[指定：組織が定めたセキュリティ対策]を実施して、[指定：組織が定めた極めて重要な情報システムコンポーネント]が正しく供給されるようにする。

補足的ガイダンス：敵対者は、極めて重要な情報システムコンポーネントの供給を中断させる、あるいは供給業者の業務を損なわせることによって、組織の業務を妨げようとする可能

性がある。極めて重要な情報システムコンポーネントが正しく供給されるようにするための対策は、たとえば、以下を含む:①特定された極めて重要なコンポーネントのサプライチェーンに関して、複数の供給業者を使用する②ミッションクリティカルな期間に業務を継続できるよう、予備コンポーネントを備蓄する。

(14) サプライチェーンの保護 | 識別情報と追跡可能性

組織は、情報システム、システムコンポーネント、または情報システムサービスの[指定:組織が定めた、サプライチェーンエレメント、プロセス、および関係者]の一意の識別情報を確立し、維持する。

補足的ガイダンス:組織のサプライチェーンに誰が、そして何が関与しているかを知ることは、そうしたサプライチェーン内で何が起こっているかについて可視性を得るために、また、リスクが高いイベントや活動をモニタリングし特定するためには不可欠である。サプライチェーン(すなわち、エレメント・プロセス・関係者)に対する十分な可視性と追跡可能性が得られない場合、組織がリスクを理解し、管理すること、また、有害なイベントが発生する可能性を減らすことが非常に困難になる。入手者とインテグレータの役割、組織、職員、ミッションプロセスとエレメントプロセス、テストおよび評価手順、配送メカニズム、サポートメカニズム、通信経路/配送経路、および廃棄/最終処分に関わる活動、ならびに使用されるコンポーネントとツールを一意に識別することは、サプライチェーン活動のアセスメントに必要な、基本的なアイデンティティ構造を規定するのに役立つ。たとえば、ソフトウェアパッケージ、モジュール、ハードウェアデバイス、およびそれらのエレメントに関連するプロセスなどの、個々のサプライチェーンエレメントに対するラベル付け(例:通し番号を使用)やタグ付け(例:ワイヤレス IC タグを使用)は、この目的に使用できる。同定法は、サプライチェーン関連の問題が発生した場合や、サプライチェーンに有害なイベントが発生した場合に、プロベナンスを支援する。

(15) サプライチェーンの保護 | 弱点または欠陥に対処するためのプロセス

組織は、第三者によるアセスメント、または組織のアセスメントにおいて特定されたサプライチェーンエレメントの弱点または欠陥に対処するためのプロセスを確立する。

補足的ガイダンス:サプライチェーンエレメントの第三者によるアセスメント、または組織のアセスメント(例:侵入テスト、監査、検証/有効性確認活動)において生成されたエビデンスは、特定された弱点や欠陥に関連するリスクに対処するための後続のプロセスで使用される。サプライチェーンエレメントには、たとえば、供給業者の開発プロセスと、供給業者の流通システムがある。

参考文献:NIST Special Publication 800-161・NIST Interagency Report 7622

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** 選択されていない	**高** SA-12

SA-13 信用性

管理策:組織は、

a. 極めて重要なミッション/業務機能を支援する[指定:組織が定めた情報システム、情報システムコンポーネント、または情報システムサービス]に必要な信用性について記述するとともに、

b. そうした信用性を実現するために[指定:組織が定めた保証オーバーレイ]を実施する。

補足的ガイダンス:この管理策は、組織の極めて重要なミッション/業務機能を実施するのに必要な情報システムを設計、開発し、導入する際に、組織が信用性に関する明確な意思決定を行うことを支援する。信用性とは、情報システムの特性/属性の 1 つであり、そのシステムが処

理、保存、または伝送する情報の機密性・完全性・可用性をシステムがどの程度まで維持できるかを示すものである。信用できる情報システムとは、指定された稼働環境において発生することが予想される環境破壊、人的ミス、および意図的な攻撃が発生しても、リスクを所定の範囲内に抑えて稼働できるシステムである。信用できるシステムは、ミッション／業務を成功させるうえで重要である。情報システムの信用性に影響を与える 2 つの要素は、以下を含む:①セキュリティ上の機能性(すなわち、そのシステム、または、そのシステムが稼働する環境において実施されるセキュリティ上の特性、機能、および／またはメカニズム)②セキュリティ保証(すなわち、セキュリティ上の機能性が適用された場合に有効であることへの信頼の根拠)。組織の情報システムの開発者・導入者・オペレータ・メンテナンス要員は、たとえば、明確に定義されたセキュリティポリシーモデル、ハードウェア、ソフトウェア、およびファームウェアの構造化された綿密な開発技法、健全なシステム／セキュリティエンジニアリング原則、ならびにセキュアな設定(付録 E に記載されている保証関連のセキュリティ管理策一式によって定義される)を用いることによって、保証レベルを高められる。

保証は、システム開発ライフサイクルにおいて生成されたエビデンスのアセスメントにも、基づく。極めて重要なミッション／業務機能は、高位影響システムと、そうしたシステムに対する保証要件によってサポートされる。付録 E の表 E-4 に記載されている追加の保証管理策(使用は任意である)は、特定の情報システムやシステムコンポーネントに、付録 I に記載されているオーバーレイの概念を用いて保証の高いソリューションを開発・実施するのに使用できる。組織は、コミュニティ向け(例:組織を跨ぐ、政府全体の)に開発、検証、および承認がなされた保証オーバーレイを選択することによって、そうしたオーバーレイを組織ごとに策定することを制限する。組織は、保証の高いソリューションを必要とする情報システム、システムコンポーネント、または情報システムサービスを特定する手段として、SA-14 に記載されているようにクリティカリティ分析を実施してもよい。信用性に関する要求事項と、保証オーバーレイは、組織の情報システムのセキュリティ計画に記載される場合がある。関連する管理策は、RA-2・SA-4・SA-8・SA-14・SC-3。

拡張管理策:なし

参考文献:FIPS Publications 199, 200・NIST Special Publications 800-53・NIST Special Publications 800-53A・NIST Special Publications 800-60・NIST Special Publications 800-64

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SA-14 クリティカリティ分析

管理策:組織は、[指定:組織が定めた、情報システム、情報システムコンポーネント、または情報システムサービス]のクリティカリティ分析を[指定:組織が定めた、システム開発ライフサイクルにおける決定点]で実施して、極めて重要な情報システムコンポーネントと機能を特定する。

補足的ガイダンス:クリティカリティ分析は、サプライチェーンのリスク管理の基本理念であり、サプライチェーンを保護するための活動(攻撃の矢面を減らす、あらゆる情報源からの情報の利用、調整された調達戦略など)に情報を与える。情報システムエンジニアには、情報システムを機能面で細かく分解することによって、ミッションクリティカルな機能とコンポーネントを特定するといった選択肢がある。機能面での分解は、たとえば、そのシステムによって支援される組織の主要なミッションを特定すること、それらのミッションを果たす特定の機能を割り出せるまで分解すること、そして、それらの機能を実施するハードウェアコンポーネント、ソフトウェアコンポーネント、ファームウェアコンポーネントに対する追跡可能性(それらの機能が、いつ、その情報システムの境界の内外で多くのコンポーネントによって共有されるかを含む)を確保することを含む。極めて重要なコンポーネントまたは機能に対する仲介のないアクセスを可能にする情報システ

ムコンポーネントは、そうしたコンポーネントが脆弱性をもたらすため、クリティカルであるとみなされる。クリティカリティは、その機能またはコンポーネントの不具合が、情報システムによって支援される組織のミッションを遂行するといった、コンポーネントの能力に与える影響の観点からアセスメントされる。クリティカリティ分析は、アーキテクチャまたは設計が開発される、またはアップグレードを含めて変更される場合には常に実施される。関連する管理策は、CP-2・PL-2・PL-8・PM-1・SA-8・SA-12・SA-13・SA-15・SA-20。

拡張管理策:なし

(1) クリティカリティ分析 | 適切な代替の調達元が存在しない、クリティカルコンポーネント
[削除された:SA-20 に統合された]

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SA-15 開発プロセス・標準・ツール

管理策:組織は、

a. 情報システム・システムコンポーネント・情報システムサービスのいずれかを開発する者に対して、以下を満たす、文書化された開発プロセスに従うことを要求する:
   1. セキュリティ要求事項を明確に示す
   2. 開発プロセスで使用される標準とツールを特定する
   3. 開発プロセスで使用される特定のツールオプションとツール設定について文書化する
   4. 開発に使用されるプロセスおよび／またはツールに対する変更を文書化、管理し、変更の整合性を維持する
b. 選択され導入された開発プロセス・標準・ツール・ツールオプション(または設定)として選択され導入されたものが[指定:組織が定めたセキュリティ要求事項]を満たすかどうかを判断するために、それらのプロセス・標準・ツール・ツールオプション(または設定)をレビューする。

補足的ガイダンス:開発ツールには、たとえば、プログラミング言語 や CAD システムがある。開発プロセスのレビューは、たとえば、成熟度モデルを使用して、そうしたプロセスの潜在的な有効性を判断することを含む。ツールやプロセスに対する変更の整合性を維持することで、サプライチェーンのリスクを正確にアセスメントし、軽減できるようになる。ただし、これには許可された変更を追跡し、不正な変更を阻止できるよう、(設計・開発・輸送・配達・統合・メンテナンスを含む)ライフサイクル全体を通した堅牢な構成管理が必要になる。関連する管理策は、SA-3・SA-8。

拡張管理策:

(1) 開発プロセス、標準、およびツール | 品質の評価指標

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する:

(a) 開発プロセスの始めに品質の評価指標を定義する

(b) 品質の評価指標を満たしていることを示すエビデンス を[選択(1つ以上):[指定:組織が定めた頻度で];[指定:組織が定めた、プログラムレビューのマイルストーン]に従って; 配送の際に]提出する。

補足的ガイダンス：組織は、品質の評価指標を使用して、情報システムの品質の許容レベルに関して、最低レベルを定める。評価指標は、クオリティゲートを含む場合がある。クオリティゲートとは、システム開発プロジェクトの特定のフェーズを順調に実施できるようにするための、十分性に関する基準（終了基準）の集合である。クオリティゲートは、たとえば、コンパイラが発する警告ををすべて消去すること、またはそれらの警告が必要なセキュリティ能力の有効性に影響を及ぼさないことを確認することを含む。開発プロジェクトの実施フェーズにおいて、クオリティゲートは進捗状況を明確に示す。開発プロジェクト全体に対しては、他の評価指標が適用される。これらの評価指標には、脆弱性の深刻さの閾値を定義することが含まれる場合がある。例としては、CVSS(Common Vulnerability Scoring System)による深刻さの判定結果が"Medium"あるいは"High"となるような既知の脆弱性が、納品される情報システムに存在しないことを要求することが挙げられる。

(2) 開発プロセス・標準・ツール | セキュリティ追跡ツール

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、開発プロセスにおいて使用できるセキュリティ追跡ツールを選択し、使用することを要求する。

補足的ガイダンス：情報システム開発チーム は、セキュリティ追跡ツールを選択し、使用する。そうしたツールには、たとえば、システム開発プロセスに関連する完成した作業項目またはタスクの割り当て、並べ替え、フィルタリング、および追跡を容易にする、脆弱性／作業項目追跡システムがある。

(3) 開発プロセス・標準・ツール | クリティカリティ分析

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、クリティカリティ分析を[指定：組織が定めた広さ／深さ]をもって、[指定：組織が定めた、システム開発ライフサイクルにおける決定点]で実施することを要求する。

補足的ガイダンス：この拡張管理策は、組織が SA-14 に記載されているクリティカリティ分析を行う際に利用できる、開発者からのインプットを取り扱う。開発者からのインプットは、そうした分析には不可欠である。なぜならば、情報システムコンポーネントが市販の IT 製品として開発されている場合、組織は詳細な設計文書（例：機能仕様書、上位レベル設計、下位レベル設計、およびソースコード／ハードウェアの図解）にアクセスできないからである。関連する管理策は、SA-4・SA-14。

(4) 開発プロセス・標準・ツール | 脅威のモデル化 / 脆弱性分析

組織は、開発者に対して、情報システムに対する脅威のモデル化と脆弱性分析を[指定：組織が定めた広さ／深さ]をもって実施することを要求する:

(a) [指定：組織が定めた、影響、システムが稼動する環境、既知の脅威または想定される脅威、およびリスクの許容レベルに関する情報]を使用する

(b) [指定：組織が定めたツールと手法]を用いる

(c) [指定：組織が定めた、受け入れ基準]を満たすエビデンスを生成する。

補足的ガイダンス：関連する管理策は、SA-4。

(5) 開発プロセス・標準・ツール | 攻撃の矢面を減らす

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、攻撃の矢面を[指定：組織が定めた閾値]に収まるまで減らすことを要求する。

補足的ガイダンス：攻撃の矢面を減らすことは、開発者による脅威分析と脆弱性分析、そして情報システムアーキテクチャおよび設計に密接に関連する。攻撃の矢面 を減らすことは、情報システム、情報システムコンポーネント、および情報システムサービスの弱点または欠陥（すなわち、潜在的な脆弱性）をアタッカーが利用する機会を減らし、組織に対するリスクを減らす手段となる。攻撃の矢面を減らすことは、たとえば、「最小権限」の原則を適用すること、階層化された防御機能を使用すること、「最小機能」の原則（すなわち、ポート、プ

ロトコル、機能、およびサービスを限定する）を適用すること、安全でない機能を廃止すること、サイバー攻撃の対象になりやすい API（アプリケーションプログラミングインターフェース）を除くことを含む。関連する管理策は、CM-7。

(6) 開発プロセス・標準・ツール | 継続的な改善

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、開発プロセスを継続的に改善するための明示的なプロセスを実施することを要求する。

補足的ガイダンス：情報システム、情報システムコンポーネント、および情報システムサービスの開発者は、現行の開発プロセスの有効性／効率性について、品質目標を達成しているか、現在の脅威環境において必要なセキュリティ能力を備えているかの観点から検証する。

(7) 開発プロセス・標準・ツール | 自動化された脆弱性分析

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する:

(a) [指定：組織が定めたツール]を使用して、自動化された脆弱性分析を実施する

(b) 発見された脆弱性がどのように利用されうるかを判断する

(c) 発見された脆弱性に対するリスク軽減措置を決定する

(d) ツールからの出力情報と分析の結果を[指定： 組織が定めた職員または役職]に知らせる。

補足的ガイダンス：関連する管理策は、RA-5。

(8) 開発プロセス・標準・およびツール | 脅威 / 脆弱性情報の再利用

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、類似のシステム、コンポーネント、またはサービスに対する脅威のモデル化と脆弱性分析の結果を使用して、現行の開発プロセスに情報を与えることを要求する。

補足的ガイダンス：類似のソフトウェアアプリケーションで発見された脆弱性の分析は、開発中の情報システムに関連する設計または導入に関する問題を示す場合がある。類似の情報システムまたはシステムコンポーネントが、開発者組織内に存在することもある。信頼できる脆弱性情報は、たとえば、National Vulnerability Database などの、官民のさまざまな情報源から得られる。

(9) 開発プロセス・標準・ツール | 実データの使用

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発環境とテスト環境における実データの使用を許可制にし、文書化して、管理する。

補足的ガイダンス：実稼働前の環境で実データを使用することは、組織にとって重大なリスクとなりうる。組織は、情報システム・情報システムコンポーネント・情報システムサービスの開発とテストを行う際に、テストデータまたはダミーのデータを使用することによって、そうしたリスクを最小限に抑えることができる。

(10) 開発プロセス・標準・ツール | インシデント対応計画

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、インシデント対応計画を用意することを要求する。

補足的ガイダンス：情報システム、システムコンポーネント、および情報システムサービスの開発者向けのインシデント対応計画は、組織のインシデント対応計画に組み入れられ、これにより、そうでなければ組織がすぐに利用できないインシデント対応情報が提供される。そうした情報は、たとえば、市販の IT 製品にて発見された脆弱性に組織が対応する際に、非常に役立つだろう。関連する管理策は、IR-8。

(11) 開発プロセス、標準、およびツール | 情報システム / コンポーネントをアーカイブする

組織は、情報システムまたはシステムコンポーネントの開発者に対して、リリースまたは納品されるシステムまたはコンポーネントに、最終的なセキュリティレビューを裏付けるエビデンスが付随する場合には、それらすべてをアーカイブすることを要求する。

補足的ガイダンス：開発プロセスで生成された関連ドキュメントをアーカイブすることによって、情報システム／コンポーネントのアップグレードまたは変更の際にすぐに利用できる、有用なベースライン情報となる。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P2	**低** 選択されていない	**中** 選択されていない	**高** SA-15

SA-16 開発者が提供する訓練

管理策：組織は、情報システム・システムコンポーネント・情報システムサービスのいずれかを開発した者に対して、導入されているセキュリティ機能、管理策、および／またはメカニズムの正しい使い方と運用方法についての［指定：組織が定めた訓練］を実施する。

補足的ガイダンス：この管理策は、外部の開発者と内部の（社内の）開発者に適用される。職員の訓練は 、組織の情報システムに導入されているセキュリティ管理策の有効性を確保するためには必須の要素である。訓練の選択肢には、たとえば、教室スタイルの訓練、インターネットを使った／コンピュータを使った訓練、および実地訓練がある。組織は、また、職員に対する社内研修を実施する、またはセルフトレーニングを用意する目的で、訓練に必要な十分な資料を開発者に要求してもよい。組織は、必要なタイプの訓練を定めるが、セキュリティ機能、管理策、またはメカニズムが異なれば、必要な訓練も異なるだろう。関連する管理策は、AT-2・AT-3・SA-5。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P2	**低** 選択されていない	**中** 選択されていない	**高** SA-16

SA-17 開発者によるセキュリティアーキテクチャおよび設計

管理策：組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を満たす設計仕様書とセキュリティアーキテクチャ を作成することを要求する：

a. 組織のエンタープライズアーキテクチャ内に確立され、その一部となる、組織のセキュリティアーキテクチャに適合して、そのアーキテクチャを支援する

b. 必要なセキュリティ上の機能性、そして物理／論理コンポーネントに対するセキュリティ管理策の割り当てについて正確に、かつ完全に記述する

c. 必要なセキュリティ能力をもたらし、保護のための統一されたアプローチを実現するために、個々のセキュリティ機能、メカニズム、およびサービスがどのように連携するかについて述べる。

補足的ガイダンス：この管理策は主に外部の開発者を対象にしているが、内部（社内）開発にも使用できる。これとは対照的に、PL-8 は主に内部の開発者を対象にしていて、組織が情報セキュリティアーキテクチャを作成し、そうしたセキュリティアーキテクチャをエンタープライズアーキテクチャに組み入れる、あるいは密に結合させることを確実にするのに役立つ。この違いは、組織が情報システム、情報システムコンポーネント、または情報システムサービスの開発を外部組織に委託する場合で、かつ、組織のエンタープライズアーキテクチャと情報セキュリティにアーキテクチャへの適合を示すことが要求される場合に重要になる。関連する管理策は、PL-8・PM-7・SA-3・SA-8。

拡張管理策：

(1) 開発者によるセキュリティアーキテクチャおよび設計 | 形式的なポリシーモデル

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する：

(a) 開発プロセスに不可欠な活動として、実施されるべき［指定：組織が定めた、組織のセキュリティポリシーの要素］について記述する形式的なポリシーモデルを作成する

(b) 上述の形式的なポリシーモデル が内部で首尾一貫していて、実施された場合に、定められた組織のセキュリティポリシーの要素を実施するのに十分であることを証明する。

補足的ガイダンス：形式的なポリシーモデルは、形式言語を使用して特定の振る舞いまたはセキュリティポリシーについて記述したものであり、それらの振る舞い／ポリシーが正しいことを正式に証明する手段となる。情報システムのすべてのコンポーネントをモデル化できるわけではなく、形式仕様の範囲は、通常は特定の重要な振る舞いまたはポリシーに絞られる（例：任意でないアクセス制御ポリシー）。組織は、記述される振る舞い／ポリシーの性質と、利用可能なツールに基づいて、特定の形式的なモデル化のための言語とアプローチを選択する。形式的なモデル化のためのツールには、たとえば、Gypsy や Zed がある。

(2) 開発者によるセキュリティアーキテクチャおよび設計 | セキュリティ関連のコンポーネント

組織は、以下を実施することを要求する:

(a) ハードウェア・ソフトウェア・ファームウェアのうちセキュリティ関連のものを定義する

(b) ハードウェア・ソフトウェア・ファームウェアのうちセキュリティ関連のものの定義が完全であることを裏付ける根拠を示す。

補足的ガイダンス：ハードウェア・ソフトウェア・ファームウェアのうちセキュリティ関連のものは、情報システム・コンポーネント・サービスのいずれかの一部であり、ハードウェア・ソフトウェア・ファームウェアとして必要なセキュリティ特性を維持するために正しく機能することが求められるものである。関連する管理策は、SA-5。

(3) 開発者によるセキュリティアーキテクチャおよび設計 | 形式的なコレスポンデンス

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する:

(a) 開発プロセスに不可欠な活動として、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアに対する、例外処理、誤りメッセージ、および影響の観点からのインターフェースを規定する形式的な最高位の仕様書を作成する

(b) 上述の形式的な最高位の仕様書が形式的なポリシーモデルに適合することを、可能な範囲内で 証拠を介して、必要なれば付加的で形式張らないデモによって示す

(c) その形式的な最高位の仕様書がセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアに対するインターフェースをすべてカバーすることを、形式張らないデモによって示す

(d) その形式的な最高位の仕様書が、導入されているセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを正確に記述していることを示す

(e) その形式的な最高位の仕様書で扱われていないものの、厳密にはセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの一部である、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアメカニズムについて記述する。

補足的ガイダンス:コレスポンデンスは、モデル化を介して得られる保証の重要な部分である。コレスポンデンスは、実装がそのモデルを正確に変形したものであり、追加となるコードまたは実装の詳細がモデル化される振る舞いまたはポリシーに影響を及ぼさないことを示す。高レベルのセキュリティ特性が、形式的な情報システム記述によって満たされていることと、その形式的なシステム記述が、たとえばハードウェア記述などの、より低いレベルの記述によって正確に満たされていることとを示すには、形式的な手法を用いることができる。形式的な最高位の仕様書と形式的なポリシーモデルとの間の一貫性は、通常は十分に証明されない。したがって、そうした一貫性を示すには、形式的な手法と非形式的な手法の組み合わせが必要になるだろう。形式的な最高位の仕様書と実装との間の一貫性は、形式張らないデモの使用を必要とするだろう。なぜならば、仕様書が実装を正確に反映しているのを形式的な手法だけで証明するには、限りがあるからである。厳密にはセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの一部である、ハードウェア、ソフトウェア、およびファームウェアメカニズムには、たとえば、レジスタと、メモリーへの直接的な入力／メモリーからの直接的な出力とのマッピングがある。関連する管理策は、SA-5。

(4) 開発者によるセキュリティアーキテクチャおよび設計 | 非形式的なコレスポンデンス

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する:

(a) 開発プロセスに不可欠な活動として、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアに対する、例外処理、誤りメッセージ、および影響の観点からのインターフェースを規定する、非形式的で記述的な最高位の仕様書を作成する;

(b) 上述の記述的な最高位の仕様書が形式的なポリシーモデルに適合することを、[選択:非形式的なデモ、形式的な手法により生成された説得力のある論拠]をもって示す

(c) その記述的な最高位の仕様書がセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアに対するインターフェースをすべてカバーすることを、形式張らないデモによって示す

(d) その記述的な最高位の仕様書が、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアに対するインターフェースを正確に記述していることを示す

(e) その記述的な最高位の仕様書で扱われていないものの、厳密にはセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの一部である、セキュリティ関連のハードウェア・ソフトウェア・ファームウェアメカニズムについて記述する。

補足的ガイダンス:コレスポンデンスは、モデル化を介して得られる保証の重要な部分である。コレスポンデンスは、実装がそのモデルを正確に変形したものであり、追加となるコードまたは実装の詳細がモデル化される振る舞いまたはポリシーに影響を及ぼさないことを示す。記述的な最高位の仕様書（すなわち、上位レベル設計／下位レベル設計）と形式的なポリシーモデルとの間の一貫性は、通常は十分に証明されない。したがって、そうした一貫性を示すには、形式的な手法と非形式的な手法の組み合わせが必要になるだろう。厳密にはセキュリティ関連のハードウェア、ソフトウェア、およびファームウェアの一部である、ハードウェア、ソフトウェア、およびファームウェアメカニズムには、たとえば、レジスタと、メモリーへの直接的な入力／メモリーからの直接的な出力とのマッピングがある。関連する管理策は、SA-5。

(5) 開発者によるセキュリティアーキテクチャおよび設計 | 概念的にシンプルな設計

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、以下を実施することを要求する:

(a) 正確に定義された記号論を伴う完全で、かつ概念的にシンプルな保護メカニズムを使用できるよう、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを設計し、構造化する

(b) 本メカニズムを実現するために、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを内部で構造化する。

補足的ガイダンス:関連する管理策は、SC-3。

(6) 開発者によるセキュリティアーキテクチャおよび設計 | テスト構造

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、テストを容易にするために、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを構造化することを要求する。

補足的ガイダンス:関連する管理策は、SA-11。

(7) 開発者によるセキュリティアーキテクチャおよび設計 | 最小権限のための構造

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、最小権限によるアクセス制御を容易にするために、セキュリティ関連のハードウェア、ソフトウェア、およびファームウェアを構造化することを要求する。

補足的ガイダンス:関連する管理策は、AC-5・AC-6。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** 選択されていない	**高** SA-17

SA-18 改ざんの防止と検知

管理策:組織は、情報システム、システムコンポーネント、または情報システムサービスに対する改ざん防止プログラムを実施する。

補足的ガイダンス:改ざん防止テクノロジーおよび技法は、極めて重要な情報システム、システムコンポーネント、および IT 製品を改ざん、リバースエンジニアリング、および摩り替えなどの関連する数多くの脅威から保護するための、一定レベルの保護をそれらのシステム、コンポーネント、および製品に提供する。強力な識別と改ざん防止および／または改ざんの検知との組み合わせは、情報システム、コンポーネント、および製品の配送中や使用中に、それらを保護するのに不可欠である。関連する管理策は、PE-3・SA-12・SI-7。

拡張管理策:

(1) 改ざんの防止と検知 | システム開発ライフサイクルの各フェーズ

組織は、設計、開発、統合、運用、およびメンテナンスなどの、システム開発ライフサイクルの各フェーズにおいて、改ざん防止テクノロジーおよび技法を使用する。

補足的ガイダンス:組織は、改ざん防止と検知のためのハードウェア技法とソフトウェア技法の組み合わせを使用する。組織は、たとえば、敵対者にとってリバースエンジニアリングや改ざんがより困難で、かつ時間と費用のかかる作業となるよう、難読化や自己チェックを用いる。情報システムおよびシステムコンポーネントをカスタマイズすることで、摩り替えを検知しやすくなり、したがって摩り替え発生時の被害を最小限に抑えられる。関連する管理策は、SA-3。

(2) 改ざんの防止と検知 | 情報システム、コンポーネント、または機器の検査

組織は、[いずれかを指定：組織が定めた情報システム・システムコンポーネント・機器]を[選択（1つ以上）：ランダムに;[指定：組織が定めた頻度で]];[指定：組織が定めた 、検査が必要な兆候]があった場合に]検査し、改ざんの有無を確認する。

補足的ガイダンス：この拡張管理策は、物理的な改ざんと論理的な改ざんの両方を取り扱うものであり、通常は、組織によって管理された領域から持ち出される携帯機器、ノートパソコン、その他システムコンポーネントに適用される。検査が必要な兆候には、たとえば、リスクが高い場所への出張から個人が帰ってきた場合がある。関連する管理策は、SI-4。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SA-19 コンポーネントの真正性

管理策：組織は、

a. 偽造されたコンポーネントが情報システムに入り込むのを検知し防ぐための手段を含む、偽造防止ポリシーおよび手順を策定し実施する

b. 偽造された情報システムコンポーネントを[選択（1つ以上）：偽造されたコンポーネントの供給元・[指定：組織が定めた、外部の報告先機関]・[指定：組織が定めた職員または役職]]に報告する。

補足的ガイダンス：偽造されたコンポーネントの供給元には、たとえば、製造業者、開発者、ベンダー、および請負業者がある。偽造防止ポリシーおよび手順は、改ざん防止を支援し、悪質コードが挿入されることを防ぐための一定レベルの保護を提供する。外部の報告先機関には、たとえば、US-CERT がある。関連する管理策は、PE-3・SA-12・SI-7。

拡張管理策：

(1) コンポーネントの真正性 | 偽造防止のための訓練

組織は、偽造された情報システムコンポーネント（ハードウェア・ソフトウェア・ファームウェアを含む）を検知できるよう、[指定：組織が定めた職員または役職] を訓練する。

(2) コンポーネントの真正性 | 修復の対象のコンポーネントに対する構成管理

組織は、修復を待っている、あるいは既に修復されて、現場への復帰を待っている[指定：組織が定めた情報システムコンポーネント]に対する、構成管理を維持する。

(3) コンポーネントの真正性 | コンポーネントの廃棄

組織は、[指定：組織が定めた技法と手法]を用いて情報システムコンポーネントを廃棄する。

補足的ガイダンス：情報システムコンポーネントの適切な廃棄は、そうしたコンポーネントがグレーマーケットに入り込むのを防止するのに役立つ。

(4) コンポーネントの真正性 | 偽造防止のためのスキャニング

組織は、偽造された情報システムコンポーネントの有無を確認するために、[指定：組織が定めた頻度で]スキャンを実施する。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SA-20 重要なコンポーネントの受託開発

管理策:組織は、[指定:組織が定めた、極めて重要な情報システムコンポーネント]を再実装する、またはカスタム開発する。

補足的ガイダンス:組織は、特定の情報システムコンポーネントが、それらのコンポーネントに対する特定の脅威が存在する、またはコンポーネントに特定の脆弱性があり、最終的なリスクを十分に軽減できる実現可能なセキュリティ管理策がないが故に、信頼できないといったケースに当てはまるかどうかを確認する。そうしたコンポーネントの再実装またはカスタム開発は、より高位の保証の要求事項を満たすのに役立つ。これは、敵対者による標準攻撃が成功しないようにシステムコンポーネント(ハードウェア、ソフトウェア、およびファームウェアを含む)に対する変更を実施することによって、成し遂げられる。代替の供給源が利用できない場合で、かつ、極めて重要な情報システムコンポーネントの再実装またはカスタマイズを行わないことを組織が選択した場合には、追加の保護対策が実施されることが考えられる(例:強化された監査、ソースコードとシステムユーティリティに対するアクセスの制限、システムファイルとアプリケーションファイルが削除されるのを防止すること)。関連する管理策は、CP-2・SA-8・SA-14。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SA-21 開発者に対する審査

管理策:組織は、[指定:情報システム・システムコンポーネント・情報システムサービスのうちそしきが定めたもの]の開発者に対して、

a. 割り当てられた[指定:組織が定めた、政府の公務]によって定められる適切なアクセス権限を有すること

b. [指定:組織が定めた追加的な職員の審査基準]を満たすこと

の 2 つを満たすよう要求する。

補足的ガイダンス:情報システム、システムコンポーネント、または情報システムサービスは、アメリカ合衆国の国益および/または経済の安定にとって不可欠な極めて重要な活動に用いられる場合があるため、組織は開発者が信頼できることに強い関心を持っている。開発者に求められる信頼の度合は、導入後の情報システム/コンポーネント/サービスを利用する個人に求められる度合と同等である必要があるだろう。権限および職員の審査基準の例としては、クリアランスおよび十分な素性調査とともに、市民権および国籍がある。開発者の信用性は、また、会社の所有権や、開発中のシステム、コンポーネント、またはサービスの品質/信頼性に影響を与える可能性のあるエンティティとの間の関係をレビューし、分析することを含む。関連する管理策は、PS-3・PS-7。

拡張管理策:

(1) 開発者に対する審査 | 審査の有効性を確認する

組織は、情報システム、システムコンポーネント、または情報システムサービスの開発者に対して、必要なアクセス権限および審査基準が満たされるようにするための[指定:組織が定めた措置]を講じる。

補足的ガイダンス:必要なアクセス権限および職員の審査基準を満たすことは、たとえば、選択された情報システム、システムコンポーネント、または情報システムサービス上で開発活動を実施することが許可されている個人のリストを用意することを含む。そうしたリストが

あれば、組織は必要な権限および審査関連の要求事項を開発者が満たしているかどうかを確認できる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SA-22 サポートが得られないシステムコンポーネント

管理策:組織は、

a. 開発者、ベンダー、または製造業者からのサポートが得られなくなった情報システムコンポーネントを、別のものと入れ替えるとともに、

b. ミッション／業務ニーズを満たすのに必要なシステムコンポーネントに関して、サポートが得られなくなったものの、使用を継続する際には、その根拠を示し、許可を得た旨を文書化する。

補足的ガイダンス:情報システムコンポーネントの サポートは、たとえば、ソフトウェアパッチ、ファームウェアのアップデート、交換用部品、および保守契約を含む。サポートが得られないコンポーネント(例:ベンダーが重要なソフトウェアパッチの提供を終了した場合)は、現在インストールされているコンポーネントにおいて発見された新たな弱点を利用するための、十分な機会を敵対者に与えてしまう。サポートが得られないシステムコンポーネントの入れ替えにおける例外としては、極めて重要なミッション／業務の遂行能力を提供するシステムではあるが、利用できる新しいテクノロジーが存在しない場合や、交換用コンポーネントをインストールすることが1つの選択肢にならない程に、そのシステムが他のシステムから切り離されている場合がある。関連する管理策は、PL-2・SA-3。

拡張管理策:

(1) サポートが得られないシステムコンポーネント | 継続的なサポートのための代替の供給元

組織は、サポートが得られない情報システムコンポーネントに対する[選択(1つ以上):社内サポート・[指定:組織が定めた、外部プロバイダからのサポート]]を用意する。

補足的ガイダンス:この拡張管理策は、選択された情報システムコンポーネントに関して、開発者、ベンダー、または製造業者からのサポートが得られなくなったものの、それらのコンポーネントが引き続きミッション／業務に不可欠である場合の継続的なサポートの必要性に対処する。組織は、たとえば、極めて重要なソフトウェアコンポーネントに対するカスタマイズされたパッチを開発することによって社内サポートを確立したり、指定されたサポートが得られなくなったコンポーネントに対して契約関係を通じて継続的にサポートを行う、外部プロバイダが提供するサービスのセキュリティを確保することができる。そうした契約関係には、たとえば、オープンソースソフトウェアを提供する付加価値ベンダーがある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

「システムおよびサービスの調達」管理策

システム、コンポーネント、およびサービスの開発

信頼できる情報システムとサプライチェーンのセキュリティに重きが置かれるようになるにつれ、IT 業界に従事し、ミッション／業務の成功に必要なシステム、コンポーネント、およびサービスを得るために、情報セキュリティ要求事項を明確に、かつ、具体的に述べる能力を組織が有することが必須となる。そうした能力を組織が有することを確実にするために、本文書は「システムおよびサービスの調達」ファミリ（すなわち SA ファミリ）として、情報システム、IT 製品、および情報システムサービスの開発に関する要求事項を扱うセキュリティ管理策一式を記載している。したがって、SA ファミリ内の管理策の多くは、そうしたシステム、コンポーネント、およびサービスの開発者を対象としている。SA ファミリ内のセキュリティ管理策のスコープは、開発が組織の内部の職員によってなされるか、あるいは契約／調達プロセスを介して外部の開発者によってなされるかにかかわらず、すべてのシステム／コンポーネント／サービスの開発とそうした開発に携わる開発者を含むことを、組織が理解することが重要である。影響を受ける管理策には、SA-8, SA-10, SA-11、SA-15、SA-16、SA-17、SA-20,および SA-21 などがある。

ファミリ:システムおよび通信の保護

SC-1　システムおよび通信の保護のポリシーと手順

管理策:組織は、

a. 以下を策定、文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、システムおよび通信の保護のポリシー
   2. システムおよび通信の保護のポリシーと、関連する「システムおよび通信の保護」管理策の実施を容易にするための手順

b. 以下 の最新版をレビューし、更新する:
   1. システムおよび通信の保護のポリシーを[指定:組織が定めた頻度で]
   2. システムおよび通信の保護の手順を[指定:組織が定めた頻度で]。

補足的ガイダンス:この管理策は、SC ファミリ内の選択されたセキュリティ管理策とその拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12, 800-100

優先順位とベースライン管理策の割り当て:

P1	**低** SC-1	**中** SC-1	**高** SC-1

SC-2　アプリケーションの分割

管理策:情報システムは、ユーザの機能性(ユーザインターフェースサービスを含む)と、情報システムの管理面での機能性を分離する。

補足的ガイダンス:情報システムの管理面での機能性は、データベース・ネットワークコンポーネント・ワークステーション・サーバー等を管理するのに必要な機能を含み、通常は特権ユーザでのアクセスを必要とする。ユーザの機能性と、情報システムの管理面での機能性との分離は、物理的に、あるいは論理的に行うことができる。組織によるシステムマネジメント関連の機能性と、ユーザの機能性との分離は、それぞれに異なるコンピュータを使用する、異なる CPU(中央処理装置)を使用する、オペレーティングシステム上の異なるインスタンスを使用する、異なるネットワークアドレスを使用する、またはこれらの組合せ、あるいは、その他の方法によって行われる。分離のタイプには、たとえば、他の情報システムリソースの利用者に対して個別の認証方法を用いるウェブ管理用インターフェースがある。システム機能性とユーザの機能性を機能面で分離することは、ドメインが異なる管理用インターフェースを追加のアクセス制御を実施して分離することを含む。関連する管理策は、SA-4・SA-8・SC-3。

拡張管理策:

(1) アプリケーションの分割 | 特権ユーザ以外のユーザ向けのインターフェース

情報システムは、特権ユーザ以外のユーザ向けのインターフェースから、情報システムマネジメント関連の機能性が見えてしまうことを阻止する。

補足的ガイダンス:この拡張管理策は、管理に関わるオプション(例:アドミニストレータ権限)を一般ユーザが利用できないようにする(そうした情報にアクセスできなくするためによく使われる、灰色表示のオプションの使用を禁止することを含む)。そうした制限には、たとえば、ユーザがアドミニストレータ権限をもってセッションを確立するまで、管理に関わるオプションを見せないことがある。関連する管理策は、AC-3。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** SC-2	**高** SC-2

SC-3 セキュリティ機能の分離

管理策:情報システムは、セキュリティ機能を非セキュリティ機能から分離する。

補足的ガイダンス:情報システムは、(複数のパーティションやドメインを用いて実施される)分離境界を用いて、セキュリティ機能を非セキュリティ機能から分離する。そうした分離は、それらのセキュリティ機能を実施するハードウェア、ソフトウェア、およびファームウェアに対するアクセスを制御し、それらのハードウェア、ソフトウェア、およびファームウェアの完全性を保護する。情報システムは、たとえば、プロセッサリングまたはプロセッサモードによるセキュリティカーネルを配備するなど、さまざまな方法でコードの分離(すなわち、セキュリティ機能を非セキュリティ機能から分離すること)を実施する。カーネルコード以外のコードに関しては、セキュリティ機能の分離は、ディスク上のコードを保護する役割を果たすファイルシステム保護や、実行コードを保護する役割を果たすアドレス空間保護によってなされることが多い。情報システムはアクセス制御メカニズムを使用して、かつ、最小権限しか与えないといった機能を実施することによって、アクセスを制限する。理想としては、セキュリティ機能の分離境界の内側にあるコードすべてがセキュリティ関連であることが望ましいが、場合によっては分離境界の内側に非セキュリティ機能を配備する必要がある。関連する管理策は、AC-3・AC-6・SA-4・SA-5・SA-8・SA-13・SC-2・SC-7・SC-39。

拡張管理策:

(1) セキュリティ機能の分離 | ハードウェアの分離

情報システムは、基礎的なハードウェア分離メカニズムを使用して、セキュリティ機能の分離を実施する。

補足的ガイダンス:基礎的なハードウェア分離メカニズムには、たとえば、マイクロプロセッサ内に実装されることが多いハードウェアリング構造や、異なる属性(すなわち、読み込み可能な、書き込み可能な)を持つ論理的に異なるデータストレージオブジェクトをサポートするのに使用される、ハードウェアベースのアドレス分割がある。

(2) セキュリティ機能の分離 | アクセス / フロー制御機能

情報システムは、アクセス制御および情報フローの制御を行うセキュリティ機能を、非セキュリティ機能および他のセキュリティ機能から分離する。

補足的ガイダンス:セキュリティ機能の分離は、実施の結果として発生するが、それらの機能は引き続きスキャンおよびモニタリングが可能である。アクセス制御およびフロー制御の実施から切り離される可能性のあるセキュリティ機能には、監査・侵入検知・ウイルス対策機能等がある。

(3) セキュリティ機能の分離 | 非セキュリティ機能の数を最小限に抑える

組織は、セキュリティ機能を含む分離境界の内側に含まれる、非セキュリティ機能の数を最小限に抑える。

補足的ガイダンス：非セキュリティ機能をセキュリティ機能から厳密に分離することが実現可能でない場合には、セキュリティ機能境界の内側に含まれる非セキュリティ機能の数を最小限に抑えるための措置が必要である。分離境界の内側に含まれる非セキュリティ機能は、そうしたソフトウェアが境界の内側にあるという理由から、ソフトウェアにエラーや悪意がある場合に組織の情報システムのセキュリティ機能に影響を与えるため、セキュリティに関連するとみなされる。設計目標は、情報システム内で情報セキュリティを提供する部分の大きさと複雑さを最小限に抑えることである。情報システムのセキュリティ関連コンポーネントにおける非セキュリティ機能の数を最小限に抑えられれば、設計者と実装者は望まれるセキュリティ能力（通常、アクセス制御）をもたらすのに必要な機能に集中できる。また、分離境界の内側に含まれる非セキュリティ機能の数を最小限に抑えることによって、セキュリティポリシーの実施に関して信頼を要するコードの数を減らすことができ、このことが分かりやすさにもつながる。

(4) セキュリティ機能の分離 | モジュールの結合度と凝集度

組織は、モジュールの内部凝集度を最大限にし、モジュール間の結合度を最小限にする独立性の高いモジュールとしての、セキュリティ機能を実施する。

補足的ガイダンス：モジュール間の相互作用を減らすことは、セキュリティ機能を制約し、複雑さを管理するのに役立つ。結合度と凝集度の概念は、ソフトウェア設計におけるモジュール性の観点から重要である。結合度は、あるモジュールの他のモジュールへの依存度を示す。凝集度は、特定のモジュール内の異なる機能間の結びつきを示す。ソフトウェアエンジニアリングの優れた実践では、モジュールの分解、階層化、および最小化によって、複雑さを軽減・管理し、凝集度が高く、結合度が低いソフトウェアモジュールを生成する、といった取り組みがなされる。

(5) セキュリティ機能の分離 | 重層構造

組織は、設計の各層間の相互作用を最小限に抑えると同時に、下位層が上位層の機能性や正確さに依存しないようにする重層構造としての、セキュリティ機能を実施する。

補足的ガイダンス：セキュリティ機能間の相互作用を最小限に抑えることができ、ルーピングが発生しない階層からなる重層構造（すなわち、下位層の機能が、上位層の機能に依存しない）を導入することによって、セキュリティ機能の分離と複雑さの管理が容易になる。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** 選択されていない	**高** SC-3

SC-4 共有リソース内の情報

管理策：情報システムは、共有システムリソースを介して情報が不正に、あるいは誤って転送されないようにする。

補足的ガイダンス：この管理策は、共有システムリソース（例：レジスタ・メインメモリー・ハードディスク）が開放され情報システムに戻された後に、以前のユーザ／役職によるアクション（または以前のユーザ／役職の代わりに稼働するプロセスによるアクション）によって生成された情報（暗号化された情報も含む）が、それらのリソースに対するアクセスを取得した現在のユーザ／役職（または現在のプロセス）によって利用されないようにする。共有リソース内の情報の管理は、一般的に「オブジェクトの再利用」、または「残存情報の保護」と呼ばれている。この管理策

は、以下を取り扱わない:①表面上削除／除去されたものの実際には残っているデータである、残存情報②共有リソースを不正に操作し、情報フローの制限を破ること可能にしてしまう隠れチャネル(ストレージチャネルおよび／またはタイミングチャネルを含む)③単一のユーザ／役職によって利用される情報システムコンポーネント。関連する管理策は、AC-3・AC-4・MP-6。

拡張管理策:

(1) 共有リソース内の情報 | セキュリティレベル

[削除された:SC-4 に統合された]

(2) 共有リソース内の情報 | 処理している期間

情報システムは、システムの処理が異なる情報分類レベル間で、または異なるセキュリティカテゴリ間で明示的に切り替わる際の[指定:組織が定めた手順]に従って、共有リソースを介して情報が不正に転送されないようにする。

補足的ガイダンス:この拡張管理策は、たとえば多重レベルの処理が行われている最中や、分類レベル／セキュリティカテゴリがそれぞれに異なる情報を処理している期間に、情報システムの情報処理レベルに明確な変化が発生した場合に適用される。組織が定めた手順には、たとえば、電子的に記憶された情報に対する承認された無害化プロセスがある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** SC-4	**高** SC-4

SC-5 サービス妨害からの保護

管理策:情報システムは、[指定:組織が定めたセキュリティ対策]を実施することによって、以下のタイプのサービス妨害攻撃による影響から保護する、あるいはそうした影響を最小限に抑える:[指定:組織が定めたタイプのサービス妨害攻撃、またはそうした情報の情報源への参照]。

補足的ガイダンス:サービス妨害攻撃による影響を最小限に抑える、あるいは場合によっては、そうした影響をなくすためのテクノロジーは多様である。たとえば、境界保護装置を使用すれば、特定のタイプのパケットをフィルタリングによって通過させないようにすることができ、これにより組織の内部ネットワーク上の情報システムコンポーネントが、サービス妨害攻撃の影響を直に受けないようにすることができる。容量と帯域幅を増加し、サービスを二重化することは、サービス妨害攻撃に対する脆弱性の軽減につながる。関連する管理策は、SC-6・SC-7。

拡張管理策:

(1) サービス妨害からの保護 | 社内ユーザを限定する

情報システムは、個人が他の情報システムに対して[指定:組織が定めたサービス妨害攻撃]を仕掛けられないようにする。

補足的ガイダンス:個人がサービス妨害攻撃を 仕掛けられないようにするには、そうした攻撃に使われるメカニズムを利用できなくすることが求められる。懸念される個人には、たとえば、情報システムの侵害に成功し、そのシステムを第三者に対してサイバー攻撃を仕掛けるためのプラットフォームとして使用する、敵意を持った内部関係者、または外部敵対者がいる。組織は、個人が任意の情報にアクセスし、持ち出しが可能な媒体(すなわち、ネットワーク、無線スペクトル)を用いて情報を伝送できないようにする。組織は、また、個人が必要以上の情報システムリソースを使用できないようにする。サービス妨害攻撃を仕掛ける

能力を持つ個人に対する保護対策は、特定の情報システム上で、あるいは標的になりうるシステムへの進出を阻止できる境界装置上で実施することが可能である。

(2) サービス妨害からの保護 | 予備の容量 / 帯域幅 / その他の予備

情報システムは、予備の容量 / 帯域幅 / その他の予備を管理して、大量の情報を送りつけるタイプのサービス妨害攻撃による影響を最小限に抑える。

補足的ガイダンス：余剰容量を管理することによって、大量の情報を送りつける攻撃に対処するための十分な容量を確保できるようになる。余剰容量の管理は、たとえば、使用優先度を定めること、クオータ（割り当て可能な容量の上限）を設けること、またはパーティションを切ることを含む。

(3) サービス妨害からの保護 | 検知 / モニタリング

組織は、

(a) 情報システムに対するサービス妨害攻撃の兆候を発見するための［指定：組織が定めた、モニタリングツール］を使用する

(b) ［指定：組織が定めた情報システムリソース］をモニタリングして、効果的なサービス妨害攻撃を阻止するための十分なリソースが確保されているかどうかを判断する。

補足的ガイダンス：組織は、悪意ある攻撃によるサービス妨害がもたらすリスクを管理する際に、情報システムリソースの使用と容量について考慮する。サービス妨害攻撃は、外部の者によって仕掛けられる場合もあれば、内部関係者によって仕掛けられる場合もある。サービス拒否に影響されやすい情報システムリソースには、たとえば、物理的なディスク記憶装置、メモリー、および CPU サイクルがある。記憶装置の使用と容量に関連するサービス妨害攻撃を阻止するのによく使われる保護対策には、たとえば、ディスククオータを設けること、記憶容量の閾値に達した場合にアドミニストレータに自動で通知するよう、情報システムを設定すること、ファイル比較技術を用いて、利用可能な格納スペースを最大限にすること、およびシステムデータとユーザデータをそれぞれに別のパーティションに配置することがある。関連する管理策は、CA-7・SI-4。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P1	**低** SC-5	**中** SC-5	**高** SC-5

SC-6 リソースの可用性

管理策：情報システムは、［選択（1つ以上）：優先度、クオータ［指定：組織が定めたセキュリティ対策］］に従って、［指定：組織が定めたリソース］を割り当てることによって、リソースの可用性を保護する。

補足的ガイダンス：優先度による保護は、優先度が低いプロセスが、優先度がより高いプロセスを扱う情報システムを遅延させたり、妨げることがないようにするのに役立つ。クオータは、ユーザまたはプロセスが、あらかじめ定められたリソースの割当量を超えるリソースを取得できないようにする。この管理策は、単一のユーザ／役職によって利用される情報システムコンポーネントには適用されない。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SC-7 境界保護

管理策:情報システムは:

a. システムの外部境界、およびシステム内の主要な内部境界において通信をモニタリングし、制御する

b. 組織の内部ネットワークから[選択:物理的に; 論理的に]分離される、一般の人がアクセスできるシステムコンポーネントに対するサブネットワークを実施する

c. 組織のセキュリティアーキテクチャに従って配備された境界保護装置によって構成される管理されたインターフェースを介してのみ、外部ネットワークまたは情報システムに接続する。

補足的ガイダンス:管理されたインターフェースは、たとえば、セキュリティアーキテクチャ内で実現されるゲートウェイ、ルーター、ファイアウォール、ガード、ネットワークベースの悪質コード分析および仮想化システム、または暗号化トンネル(例:ファイアウォールを保護するルーター、または保護されたサブネットワーク上に存在するアプリケーションゲートウェイ)を含む。内部ネットワークから物理的に、あるいは論理的に切り離されているサブネットワークは、非武装地帯(DMZ)と呼ばれる。組織の情報システム内のインターフェースを制限する、または禁止することには、たとえば、管理されたインターフェース内の指定されたウェブサーバーに対する、外部からのウェブトラフィックを禁止することや、内部アドレスがスプーフィングされたものであると判断される外部トラフィックを禁止することがある。組織は、商用通信サービスの利用に関するセキュリティ管理策を導入する際には、それらのサービスに本来備わっている「共有」という性質を考慮する。商用通信サービスは通常、すべての法人顧客によって共有されるネットワークコンポーネントおよび統合管理システムをベースにしたものであり、第三者が提供するアクセスラインやその他のサービス要素を含む場合がある。そうした通信サービスは、セキュリティに関する契約規定があるにもかかわらず、リスクを増加させる要因となることもある。関連する管理策は、AC-4・AC-17・CA-3・CM-7・CP-8・IR-4・RA-3・SC-5・SC-13。

拡張管理策:

(1) 境界保護 | 物理的に切り離されたサブネットワーク

[削除された:SC-7 に統合された]

(2) 境界保護 | 一般からのアクセス

[削除された:SC-7 に統合された]

(3) 境界保護 | アクセスポイント

組織は、情報システムに対する外部からのネットワーク接続の数を制限する。

補足的ガイダンス:外部からのネットワーク接続の数を制限することで、内向け通信トラフィックと外向け通信トラフィックの包括的なモニタリングが容易になる。外部からのネットワーク接続の数を制限する 1 つの例として、Trusted Internet Connection の取り組みが挙げられる。

(4) 境界保護 | 外部通信サービス

組織は、

(a) 個々の外部通信サービスに対して、管理されたインターフェースを実施する

(b) 個々の管理されたインターフェースに対して、トラフィックフローポリシーを定める

(c) 個々のインターフェースを介して伝送される情報の機密性と完全性を保護する

(d) トラフィックフローポリシーが適用されない個々の例外を、それらを裏付けるミッション／業務の必要性と、その必要がある期間と共に、文書化する

(e) トラフィックフローポリシーが適用されない個々の例外を[指定：組織が定めた頻度で]レビューし、現時点で明確なミッション／業務の必要性によって裏付けられない例外を取り除く。

補足的ガイダンス：関連する管理策は、SC-8。

(5) 境界保護 | デフォルトで拒否/ 例外的に許可

管理されたインターフェースにおける情報システムは、ネットワーク通信トラフィックをデフォルトで拒否し、例外的に許可する（すなわち、「すべてを拒否」、「例外的に許可」）。

補足的ガイダンス：この拡張管理策は、内向けと外向けの両方のネットワーク通信トラフィックに適用される。「すべてを拒否」、「例外的に許可」のネットワーク通信トラフィックポリシーを実施することで、リクエストされた接続が不可欠であり、かつ許可されている場合のみ、接続が許可されるようになる。

(6) 境界保護 | 確認された不具合への対応

[削除された：SC-7(18)に統合された]

(7) 境界保護 | 遠隔装置上での分割トンネルを防止する

その情報システムと遠隔装置が併用される場合、システムは、その装置がシステムとの間で非リモート接続を複数同時に確立するのを阻止すると同時に、別の接続によって外部ネットワークのリソースにアクセスできないようにする。

補足的ガイダンス：この拡張管理策が遠隔装置（例：ノートパソコン）内で実施される場合には、それらの装置における分割トンネルを無効にする設定を通じて、また、それらの設定をユーザが容易に変更できないすることによって、上述の目的が成し遂げられる。この拡張管理策が情報システム内で実施される場合には、遠隔装置上の分割トンネル（または分割トンネルを許してしまう設定）の有無の確認を通じて、また、その遠隔装置が分割トンネルを使用している場合には接続を禁止することによって、上述の目的が成し遂げられる。分割トンネルは、たとえばプリンター／ファイルサーバーなどのローカル情報システムリソースと通信するリモートユーザにとって、好ましいものであるかも知れない。しかしながら、分割トンネルは、実際には不正な外部接続を許してしまうため、システムが攻撃を受けやすくなり、アタッカーからすれば組織の情報も引き出しやすくなる。リモート接続に仮想プライベートネットワーク(VPN)を使用する場合、適切なセキュリティ管理策も一緒に提供されるのであれば、VPNが非リモート接続のような接続を機密性と完全性の観点から効果的に扱えることに関して、十分な保証が組織に与えられるだろう。VPNは、遠隔装置からの非リモート通信経路を確立するための手段となる。ただし、適切に設定されたVPNを使用しているからといって、分割トンネルを阻止する必要がなくなるわけではない。

(8) 境界保護 | 認証されたプロキシサーバーにトラフィックをルーティングする

情報システムは、管理されたインターフェース上で認証されたプロキシサーバー経由で、[指定：組織が定めた内部通信トラフィック]を[指定：組織が定めた外部ネットワーク]にルーティングする。

補足的ガイダンス：外部ネットワークは、組織によって管理されないネットワークである。プロキシサーバーは、情報システムリソース（例：ファイル、接続、ウェブページ、またはサービス）をリクエストするクライアントの、仲介者しての役割を果たすサーバー（すなわち、情報システムまたはアプリケーション）である。プロキシサーバーへの初回の接続をもって確立されたクライアントリクエストは、複雑さを緩和するために評価されると同時に、このような仕組みは直接接続させないことによる追加の保護を提供する。ウェブコンテンツをフィルタリングできる機器は、インターネットアクセスを可能にする、最も一般的なプロキシサーバーの内の1つである。プロキシサーバーを使用すれば、個々の TCP セッションをログに記録する

ことができ、特定の URL、ドメイン名、および IP アドレスを遮断できる。ウェブプロキシは、組織が定めた、許可されている／許可されていないウェブサイトのリストを参照しながら設定することができる。関連する管理策は、AC-3・AU-2。

(9) 境界保護 | 脅威となる外向け通信トラフィックを禁止する

情報システムは:

(a) 外部情報システムに脅威をもたらす外向け通信トラフィックを検出し、拒否する

(b) 拒否された通信に関わっている社内ユーザの身元をチェックする。

補足的ガイダンス:内部アクションによる、外部情報システムを脅かす外向け通信トラフィックを検出することは、「エクストルージョン検知」と呼ばれることがある。管理されたインターフェースの一部としての、情報システム境界における「エクストルージョン検知」は、内向け／外向けの通信トラフィックを分析して、外部システムのセキュリティに対する、インサイダー脅威の兆候がないかどうかを探ることを含む。そうした脅威には、たとえば、サービス妨害攻撃を示すトラフィックや、悪質コードを含むトラフィックがある。関連する管理策は、AU-2・AU-6・SC-38・SC-44・SI-3・SI-4。

(10) 境界保護 | 不正な情報の引き出しを阻止する

組織は、管理されたインターフェースにわたって不正な情報の引き出しを阻止する

補足的ガイダンス:情報システムからの、不正な情報の引き出しを阻止するために組織が実施する保護対策には、たとえば、以下がある:①プロトコルフォーマットを厳密に遵守する②情報システムからの警告をモニタリングする③電子迷彩技術の使用をモニタリングする④明確に必要な場合を除き、外部ネットワークインターフェースとの接続を切る⑤パケットヘッダーを分解して、再度組み立てるならびに⑥トラフィックプロファイル解析を行って、組織内で予期されるトラフィックの量／タイプからの逸脱を検出する、または指令室へのコールバックを把握する。プロトコルフォーマットを厳密に遵守する必要がある機器には、たとえば、ディープパケットインスペクションを実施するファイアウォールや XML ゲートウェイがある。これらの機器は、アプリケーション層におけるプロトコルフォーマットと仕様の遵守状況を確認し、ネットワーク層またはトランスポート層で稼動している機器では発見されない脆弱性の特定に役立つ。この拡張管理策は、ドメイン間共通のソリューションと、情報フローに関する要求事項が課せられるシステムガードに密接に関連する。関連する管理策は、SI-3。

(11) 境界保護 | 内向け通信トラフィックを制限する

情報システムは、[指定:組織が定めた、許可されている宛先]にルーティングされる、[指定:組織が定めた、許可されている発信元]からの内向け通信のみ、許可する。

補足的ガイダンス:この拡張管理策は、発信元アドレスと宛先アドレスのペアから、許可されている通信であるかどうかを判断できるようにする。そうした判断は、たとえば、当該発信元アドレス／宛先アドレスのペアが、許可されている通信のリストに記載されているか、当該アドレスのペアが、許可されていないペアのリストに記載されていないか、あるいは許可されている発信元／宛先ペアに関するより一般的なルールなどの、いつくかの因子に基づく。関連する管理策jは、AC-3。

(12) 境界保護 | ホストベースの保護

組織は、[指定:組織が定めた情報システムコンポーネント]において、[指定:組織が定めた、ホストベースの境界保護メカニズム]を実施する。

補足的ガイダンス:ホストベースの境界保護メカニズムには、たとえば、ホストベースのファイアウォールがある。ホストベースの境界保護メカニズムを使用する情報システムコンポーネントには、たとえば、サーバー、ワークステーション、および携帯機器がある。

(13) 境界保護 | セキュリティツール / メカニズム / 支援コンポーネントの分離

組織は、管理されたインターフェースと、物理的に切り離されたサブネットワークを使用して、[指定:組織が定めた情報セキュリティツール、メカニズム、および支援コンポーネント]を情報システムの他の内部コンポーネントから分離する。

補足的ガイダンス:管理されたインターフェースと、物理的に切り離されたサブネットワークの使用は、たとえば、コンピューターネットワークの防衛機能と、極めて重要な業務処理用ネットワークを分離して、敵対者が組織の解析技術と科学捜査技術を見抜くことを防ぐのに有用である。関連する管理策は、SA-8・SC-2・SC-3。

(14) 境界保護 | 不正な物理接続から保護する

組織は、[指定:組織が定めた、管理されたインターフェース]における不正な物理接続から保護する。

補足的ガイダンス:異なるセキュリティカテゴリまたは分類レベルで稼動する複数の情報システムは、それらのシステムが組織の施設内のスペースを共有することもあることから、共通の物理面と環境面での管理策を使用するといったケースも考えられる。実際に、これらの個々の情報システムが、機器室、ワイヤリングクローゼット、およびケーブル配布パスを共有することも考えられる。不正な物理接続からの保護は、たとえば、明確に識別され、物理的に分離されているケーブルトレイ、コネクションフレーム、および管理されたインターフェースの各側面に対する配線盤と、それらのアイテムに対するアクセスを制限する物理アクセス制御によって成し遂げられる。関連する管理策は、PE-4・PE-19。

(15) 境界保護 | ルート権限でのネットワークアクセス

情報システムは、アクセス制御と監査を目的として、専用の、管理されたインターフェースを介して、すべてのネットワーク化された特権的アクセスをルーティングする。

補足的ガイダンス:関連する管理策は、AC-2・AC-3・AU-2・SI-4。

(16) 境界保護 | コンポーネント / 機器が発見されないようにする

情報システムは、管理されたインターフェースを構成するシステムコンポーネントが発見されないようにする。

補足的ガイダンス:この拡張管理策は、管理されたインターフェースの一部である、情報システムコンポーネントのネットワークアドレスが、ネットワーク上の機器を特定するのに使用される一般的なツールや技法によって発見されないようにする。ネットワークアドレスは、そうした発見のために利用することはできず(例:公開されていないネットワークアドレス、またはドメインネームシステムに参加していないネットワークアドレス)、アクセスするには予備的知識が必要である。難読化のための別の技法として、ネットワークアドレスを定期的に変更することが挙げられる。

(17) 境界保護 | プロトコルフォーマットの自動遵守

情報システムは、プロトコルフォーマットの遵守を確実にする。

補足的ガイダンス:プロトコルフォーマットを実施する情報システムコンポーネントには、たとえば、ディープパケットインスペクションを実施するファイアウォールや XML ゲートウェイがある。そうしたシステムコンポーネントは、アプリケーション層におけるプロトコルフォーマット/仕様(例:電気電子技術者協会)の遵守状況を確認し、ネットワーク層またはトランスポート層で稼動している機器では発見されない重大な脆弱性の特定に役立つ。関連する管理策は、SC-4。

(18) 境界保護 | フェールセキュア

情報システムは、境界保護装置の動作に不具合が発生した場合、安全に停止する。

補足的ガイダンス:フェールセキュアは、管理されたインターフェースにおける境界保護装置(例:一般的に非武装地帯と呼ばれる保護されたサブネットワーク上にあるルーター、ファイアウォール、ガード、およびアプリケーションゲートウェイ)の動作に不具合が発生した

場合でも、情報システムが意図したセキュリティ特性が有効でなくなるほど安全でない状態に陥らないようにする、情報システムメカニズムを使用することで実現される状況である。境界保護装置に不具合が発生しても、それらの装置にとって外部の情報が装置に入ることがないようにし、また、不正な情報の開示を許してしまうことがないようにする。関連する管理策は、CP-2・SC-24。

(19) 境界保護 | 組織によって設定されたホストではないホストからの通信を遮断する

情報システムは、エンドユーザと外部サービスプロバイダによって個別に設定される[指定:組織が定めた、通信クライアント]間の内向け／外向けの通信トラフィックを遮断する。

補足的ガイダンス:エンドユーザと外部サービスプロバイダによって個別に設定される通信クライアントには、たとえば、インスタントメッセージを送信するクライアントがある。トラフィックを遮断することは、許可されている機能を実施するために組織が設定する通信クライアントには適用されない。

(20) 境界保護 | 動的な分離 / 隔離

情報システムは、[指定:組織が定めた情報システムコンポーネント]を、そのシステムの他のコンポーネントから動的に分離する機能を提供する。

補足的ガイダンス:組織の情報システムの特定の内部コンポーネントを動的に分離できる機能は、出所が疑わしいコンポーネントを、より高い信頼を得ているコンポーネントから分離する(または区分けする)必要がある場合に有用である。コンポーネントを分離することで、組織の情報システムの攻撃の矢面を減らすことができる。選択された情報システムコンポーネントを分離することは、サイバー攻撃が発生し、成功した場合の被害を最小限に抑えるための手段でもある。

(21) 境界保護 | 情報システムコンポーネントの分離

組織は、[指定:組織が定めたミッションおよび／または業務機能]を支援する[指定:組織が定めた情報システムコンポーネント]を分離するための、境界保護メカニズムを導入する。

補足的ガイダンス:組織は、遂行するミッションおよび／または業務機能が異なる情報システムコンポーネントを分離してもよい。そうした分離は、システムコンポーネント間で許可されていない情報フローを制限し、選択されたコンポーネントに対してより高レベルの保護を展開する。境界保護メカニズムを使用してシステムコンポーネントを分離することによって、個々のコンポーネントに対する保護を強化し、それらのコンポーネント間の情報フローをより効果的に制御できるようになる。このタイプの強化された保護は、サイバー攻撃やエラーがもたらす被害を最小限に抑えてくれる。実際の分離の度合は、選択されるメカニズムによって異なる。境界保護メカニズムには、たとえば、システムコンポーネントを物理的に分離されたネットワークまたはサブネット上に振り分けるルーター、ゲートウェイ、ファイアウォール、サブネットワークを分離するためのドメイン間共通の機器、仮想化技術、異なる暗号鍵を使用して、システムコンポーネント間の情報フローを暗号化することがある。関連する管理策は、CA-9・SC-3。

(22) 境界保護 | 異なるセキュリティドメインに接続できるよう、分離されたサブネットを使用する

情報システムは、セキュリティドメインが異なるシステムを接続できるよう、分離されたネットワークアドレス(すなわち、分離されたサブネットワーク)を実施する。

補足的ガイダンス:情報システムを分割して複数のサブネットワーク上に配置することは、セキュリティカテゴリまたは分離レベルが異なる情報を含む複数のセキュリティドメインに対する、適切なレベルの保護を提供するのに役立つ。

(23) 境界保護 | プロトコル検証における不具合発生時の、送信者へのフィードバックを無効にする

情報システムは、プロトコルフォーマット検証における不具合発生時の、送信者へのフィードバックを無効にする。

補足的ガイダンス：プロトコルフォーマット検証における不具合発生時の、送信者へのフィードバックを無効にすることで、敵対者がそうした情報を取得するのを防げる。

参考文献：FIPS Publication 199・NIST Special Publications 800-41・NIST Special Publications 800-77

優先順位とベースライン管理策の割り当て：

P1	**低** SC-7	**中** SC-7 (3) (4) (5) (7)	**高** SC-7 (3) (4) (5) (7) (8) (18) (21)

SC-8 伝送される情報の機密性と完全性

管理策：情報システムは、伝送される情報の[選択（1つ以上）： 機密性; 完全性]を保護する。

補足的ガイダンス：この管理策は、内部ネットワークと外部ネットワークの両方に、そして情報が伝送されるあらゆるタイプの情報システムコンポーネントに適用される（例：サーバー・携帯機器・ノートパソコン・プリンター・コピー機・スキャナー・ファクシミリ装置）。管理された境界による物理面での保護の対象に含まれない通信経路は、傍受や改ざんに遭う可能性がある。組織の情報の機密性 および／または 完全性を保護することは、物理的な方法で（例：保護された流通システムを使用することによって）、あるいは論理的な方法で（例：暗号化技術を使用することによって）成し遂げられる。専用のサービス（すなわち、個々の顧客のニーズに対応できるサービス）ではなく、汎用のサービスとして伝送サービスを提供する民間プロバイダに組織が依存している場合には、伝送される情報の機密性／完全性を確保するのに必要なセキュリティ管理策の導入に関して、必要な保証を得ることが困難であるだろう。そうした状況では、組織は標準の商用通信サービスパッケージとして、どのようなタイプの機密性／完全性サービスが利用可能であるを確認する。適切な契約手段によって必要なセキュリティ管理策と、管理策の有効性に関する保証を得ることが不可能な場合／現実的でない場合には、組織は適切な補完的セキュリティ管理策を導入するか、あるいは、さらなるリスクを明示的に受け入れることになる。関連する管理策は、AC-17・PE-4。

拡張管理策：

(1) 伝送される情報の機密性と完全性 | 暗号化による、あるいは代替の物理面での保護

情報システムは、情報の伝送中に、[選択（1つ以上）： 不正な 情報の開示を防ぐ;情報に対する変更を検出する]ために、暗号メカニズムを導入する。ただし、[指定：組織が定めた、代替の物理面での対策]によって保護されている場合を除く。

補足的ガイダンス：伝送される情報を暗号化することで、その情報を不正な開示や変更から保護できる。情報の完全性を保護するのに用いられる暗号メカニズムには、たとえば、電子署名、チェックサム、およびメッセージ認証コードに共通に使用できる暗号ハッシュ関数がある。代替の物理面での対策には、たとえば、保護された流通システムがある。関連する管理策は、SC-13。

(2) 伝送される情報の機密性と完全性 | 伝送前 / 伝送後のハンドリング

情報システムは、情報の伝送の準備段階や受信時に、その情報の[選択（1つ以上）：機密性;完全性]を維持する。

補足的ガイダンス：情報は、たとえば、集約時、プロトコル変換地点において、圧縮／解答時などの、伝送の準備段階や受信時に誤って、あるいは悪意を持って開示または変更され

る可能性がある。このような不正な開示または変更は、情報の機密性または完全性を侵害する。関連する管理策は、AU-10。

(3) 伝送される情報の機密性と完全性 | メッセージの外側を暗号化によって保護する

情報システムは、メッセージの外側を保護するために、暗号メカニズムを導入する。ただし、[指定：組織が定めた、代替の物理面での対策]によって保護されている場合を除く。

補足的ガイダンス：この拡張管理策は、情報の不正な開示からの保護を取り扱う。メッセージの外側には、メッセージのヘッダー／ルーティング情報がある。この拡張管理策は、メッセージの外側が引き出されるのを阻止するものであり、内部ネットワークと外部ネットワークの両方に、あるいは許可されたユーザ以外からも見えてしまうリンクに適用される。ヘッダー／ルーティング情報は、場合によっては、暗号化されていない状態で伝送される。その理由としては、その情報が大きな価値を有することを組織が正しく認識していなかったり、情報の暗号化がネットワークの性能の低下や、コストの増加につながることを懸念していることが挙げられる。代替の物理面での対策には、たとえば、保護された流通システムがある。関連する管理策は、SC-12・SC-13。

(4) 伝送される情報の機密性と完全性 | 通信パターンを見えないようにする / 無作為化する

情報システムは、通信パターンを見えないようにする／無作為化するために、暗号メカニズムを導入する。ただし、[指定：組織が定めた、代替の物理面での対策]によって保護されている場合を除く。

補足的ガイダンス：この拡張管理策は、情報の不正な開示からの保護を取り扱う。通信パターンには、頻度・期間・量・予測可能性等がある。通信パターンの変化が、収集する価値のある情報を明らかにすることもある。とりわけ、組織の情報システムが支援するミッション／業務機能に関連する、他の入手可能な情報と組み合わさった場合には注意が必要である。この拡張管理策は、通信パターンに基づいて機密情報が引き出されるのを防ぐものであり、内部ネットワークと外部ネットワークの両方に、あるいは許可されたユーザ以外からも見えてしまうリンクに適用される。リンクを暗号化して、情報を連続的な、固定／ランダムパターンで伝送することで、システムの通信パターンに基づいて機密情報が引き出されるのを防げる。代替の物理面での対策には、たとえば、保護された流通システムがある。関連する管理策は、SC-12・SC-13。

参考文献：FIPS Publications 140-2・FIPS Publications 197・NIST Special Publications 800-52・NIST Special Publications 800-77・NIST Special Publications 800-81・NIST Special Publications 800-113・CNSS Policy 15・NSTISSI No. 7003

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** SC-8 (1)	**高** SC-8 (1)

SC-9 伝送中の機密性

[削除された：SC-8に統合された]

SC-10 ネットワークの切断

セキュリティ管理策：情報システムは、通信セッションの終了時、または通信セッションが[指定：組織が定めた時間]にわたってアクティブでない場合、そのセッションに関連するネットワーク接続を終了する。

補足的ガイダンス：このセキュリティ管理策は、内部ネットワークと外部ネットワークの両方に適用される。通信セッションに関連するネットワーク接続を終了する手段の例としては、オペレーティングシステムレベルで関連するTCP/IPアドレス／ポートのペアの割当てを解除すること、また

は複数のアプリケーションセッションが単一のオペレーティングシステムレベルのネットワーク接続を使用している場合には、アプリケーションレベルでネットワークの割当てを解除することを含む。アクティブでない時間は組織が定める場合があり、たとえばネットワークアクセスのタイプ別に定められたり、特定のネットワークアクセス向けに定められたりする。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低** 選択されていない	**中** SC-10	**高** SC-10

SC-11 高信頼パス

管理策:情報システムは、システムの以下のセキュリティ機能とユーザとの間に信頼できる通信経路を確立する:[指定:組織が定めたセキュリティ機能(少なくとも情報システムの認証および再認証を含む)]。

補足的ガイダンス:高信頼パスは、情報セキュリティポリシーを支援することに関して必要な保証をもって、ユーザが(入力装置を使用して)情報システムのセキュリティ機能と直接対話できるようにする仕組みである。この仕組みを有効にできるのは、ユーザまたは組織の情報システムのセキュリティ機能に限られる。高信頼パスを通るユーザレスポンスは、信頼できないアプリケーションによる変更または開示から保護される。組織は、情報システムのセキュリティ機能とユーザとの間で安定性の高い接続を要する場合(例:システムログオン時)に、高信頼パスを使用する。信頼できる通信経路の確立には、通常は参照モニターの概念を満たす実装が求められる。関連する管理策は、AC-16・AC-25。

拡張管理策:

(1) 高信頼パス | 論理的な切り離し

情報システムは論理的に切り離されていて、他の経路と区別できる、信頼できる通信経路を用意する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SC-12 暗号鍵の作成と管理

管理策:組織は、情報システム内で使用されている暗号技術向けの暗号鍵を[指定:鍵を生成・配布・保管・アクセス・破壊するにあたり組織が定めた要求事項]に従って作成・管理する。

補足的ガイダンス:暗号鍵の管理・作成は手作業で、あるいは手作業を伴う自動化されたメカニズムを用いて行える。組織は該当する連邦法・大統領命令・指令・規制・政策・標準・手引に従って鍵管理に関する要求事項を定義し、適切なオプション、レベル、およびパラメータを指定する。組織は承認されたトラストアンカーのみがトラストストアに含まれるよう、トラストストアを管理する。これは、組織の情報システムに対する可視性をもたらす証明書と、システムの内部処理に関連する証明書を含む。関連する管理策は、SC-13・SC-17。

拡張管理策:

(1) 暗号鍵の作成と管理 | 可用性

組織は、ユーザが暗号鍵を紛失した場合に、情報の可用性を維持する。

補足的ガイダンス:暗号鍵のエスクローは、鍵を紛失した場合(例:パスフレーズを忘れてしまったため)であっても可用性を確保するための一般的な方法である。

(2) 暗号鍵の作成と管理 | 対称鍵

組織は[選択:NIST の FIPS に準拠した NSA 認定の]鍵管理技術およびプロセスを用いて、対称の暗号鍵を生成・管理・配布する。

(3) 暗号鍵の作成と管理 | 非対称鍵

組織は[選択:NSA 認定の鍵管理技術およびプロセス; 認可された PKI Class 3 証明書またはあらかじめ配備された鍵マテリアル;ユーザの秘密鍵を保護する認可された PKI Class 3/Class 4 証明書およびハードウェアセキュリティトークン]を用いて、非対称の暗号鍵を生成・管理・配布する。

(4) 暗号鍵の作成と管理 | PKI 証明書

[削除された:SC-12 に統合された]

(5) 暗号鍵の作成と管理 | PKI 証明書/ ハードウェアトークン

[削除された:SC-12 に統合された]

参考文献:NIST Special Publications 800-56・NIST Special Publications 800-57

優先順位とベースライン管理策の割り当て:

P1	**低** SC-12	**中** SC-12	**高** SC-12 (1)

SC-13 暗号化による保護

管理策:情報システムは、該当する連邦法・大統領命令・指令・政策・規制・標準に従って、[指定:組織が定めた暗号の用途およびそれぞれの用途に必要な暗号技術]を実装する。

補足的ガイダンス:暗号技術は、機密情報や、CUI(管理されている、非機密扱いの情報)の保護、電子署名を行うこと、そうした情報に対して権限を与えられた個人が必要なアクセス権限を有するものの、必要な正式なアクセス許可を得ていない場合に情報を分離することなどの、さまざまなセキュリティソリューションを支援するのに使用できる。暗号技術は、また、乱数の生成やハッシュの生成を支援する。一般的に適用可能な暗号標準には、たとえば、FIPS によって有効性が確認された暗号技術と、NSA 認定の暗号技術がある。この管理策は組織に対して暗号技術の使用を要求するものではない。しかしながら、他のセキュリティ管理策の選択に応じて暗号技術が必要となる場合、組織は暗号の用途の各々と、必要な暗号技術を定義する(例:機密情報の保護には、NSA 認定の暗号技術を使用し、電子署名を行う際には、FIPS によって有効性が確認された暗号技術を使用する)。関連する管理策は、AC-2・AC-3・AC-7・AC-17・AC-18・AU-9・AU-10・CM-11・CP-9・IA-3・IA-7・MA-4・MP-2・MP-4・MP-5・SA-4・SC-8・SC-12・SC-28・SI-7。

拡張管理策:なし

(1) 暗号化による保護 | FIPS によって有効性が確認された暗号技術

[削除された:SC-13 に統合された]

(2) 暗号化による保護 | NSA 認定の暗号技術

[削除された:SC-13 に統合された]

(3) 暗号化による保護 | アクセスが正式に許可されていない個人

[削除された：SC-13 に統合された]

(4) 暗号化による保護 | 電子署名

[削除された：SC-13 に統合された]

参考文献：FIPS Publication 140・ウェブサイト http://csrc.nist.gov/cryptval および http://www.cnss.gov

優先順位とベースライン管理策の割り当て：

P1	**低** SC-13	**中** SC-13	**高** SC-13

SC-14 一般からのアクセスからの保護

[削除された：当該セキュリティ能力は、AC-2・AC-3・AC-5・AC-6・SI-3・SI-4・SI-5・SI-7・SI-10 によって提供されている]

SC-15 連携するコンピュータデバイス

管理策：情報システムは：

a. 以下の例外を除き、連携するコンピュータデバイスの遠隔でのアクティブ化を禁止する：[指定：組織が定めた、遠隔でのアクティブ化を許可せざるを得ない状況]

b. それらの機器に物理的に居合わせているユーザに対しては、使用を許可する旨を明示する。

補足的ガイダンス：連携するコンピュータデバイスには、たとえば、ネットワークでつながっているホワイトボード、カメラ、マイクがある。使用を許可する旨を明示する手段としては、たとえば連携するコンピュータデバイスがアクティブ化された時にユーザに信号で知らせることがある。関連する管理策は、AC-21。

拡張管理策：

(1) 連携するコンピュータデバイス | 物理的な切り離し

情報システムは、連携するコンピュータデバイスからの物理的な切り離しをユーザが簡単に実施できるようにする。

補足的ガイダンス：連携するコンピュータデバイスからの物理的な切り離しに失敗すると、組織の情報が侵害される恐れがある。連携コンピューティングセッションの終了後に、そうした機器からの物理的な切り離しを簡単に行える手段が用意されていれば、参加者は複雑で長ったらしい手順を踏むことなく、切り離し作業を行える。

(2) 連携するコンピュータデバイス | 内向け / 外向け通信トラフィックを遮断する

[削除された：SC-7 に統合された]

(3) 連携するコンピュータデバイス | 安全な作業領域内での無効化 / 撤去

組織は[指定：組織が定めた、安全な作業領域]内にある[指定：組織が定めた情報システムまたは情報システムコンポーネント]から、連携するコンピュータデバイスを撤去する、または無効にする。

補足的ガイダンス：情報システムまたは情報システムコンポーネントからの、連携するコンピュータデバイスの撤去または無効化に失敗すると、組織の情報が侵害される（例：会話が盗聴される）恐れがある。

(4) 連携するコンピュータデバイス | 現在の参加者を明示する

情報システムは、[指定：組織が定めたオンライン会議またはテレビ会議]への現在の参加者を明示する。

補足的ガイダンス:この拡張管理策は、権限のない個人が、他の参加者に気付かれずに連携コンピューティングセッションに参加するのを防止する。

参考文献:なし

優先順位とベースライ管理策ンの割り当て:

P1	**低** SC-15	**中** SC-15	**高** SC-15

SC-16

セキュリティ属性の伝送

管理策:情報システムは、[指定:組織が定めたセキュリティ属性]と、情報システム間で交換される情報およびシステムコンポーネント間で交換される情報とを対応付ける。

補足的ガイダンス:セキュリティ属性は、組織の情報システムまたはシステムコンポーネントに含まれる情報との明示的に、あるいは暗黙的に対応付けることができる。関連する管理策は、AC-3, AC-4・AC-16。

拡張管理策:

+セキュリティ属性の伝送 | 完全性検証

情報システムは、伝送されるセキュリティ属性の完全性を検証する。

補足的ガイダンス:この拡張管理策は、伝送される情報の完全性検証に、セキュリティ属性も対象として含まれるようにする。関連する管理策は、AU-10・SC-8。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** 選択されていない	**中** 選択されていない	**高** 選択されていない

SC-17 PKI 証明書

管理策:組織は、[指定:組織が定めた証明書に関するポリシー]に従って PKI 証明書を発行する、または承認されたサービスプロバイダから、PKI 証明書を取得する。

補足的ガイダンス:すべての証明書に対して、組織は、承認されたトラストアンカーのみが情報システムのトラストストアに含まれるよう、トラストストアを管理する。この管理策は、組織の情報システムに対する可視性をもたらす証明書と、システムの内部処理(例:アプリケーション特有のタイムサービス)に関連する証明書の両方を扱う。関連する管理策は、SC-12。

拡張管理策:なし

参考文献:OMB Memorandum 05-24・NIST Special Publications 800-32・NIST Special Publications 800-63

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** SC-17	**高** SC-17

SC-18 モバイルコード

管理策:組織は、

a. 許容できる／許容できないモバイルコードおよびモバイルコードテクノロジーを定義する
b. 許容できるモバイルコードおよびモバイルコードテクノロジーに関して、使用制限を定め、導入ガイダンスを作成する

c. 情報システムにおけるモバイルコードの使用を許可、モニタリング・管理する。

補足的ガイダンス：組織の情報システムにおけるモバイルコードの使用に関する意思決定は、そのコードが悪意を持って使用された場合にシステムに被害が及ぶ可能性に基づいて行われる。モバイルコードテクノロジーには、たとえば、Java・JavaScript・ActiveX・Postscript・PDF・Shockwave movies・Flash animations・VBScript がある。使用制限と導入ガイダンスは、サーバーにインストールされるモバイルコードとの選択および使用と、個々のワークステーションやデバイス（例：スマートフォン）にダウンロードされて実行されるモバイルコードの選択および使用に適用される。モバイルコードに関するポリシーおよび手順は、組織の情報システムに許容できないモバイルコードが調達または挿入されたり、そうしたコードが開発・実装されるを防ぐ手段も扱う。関連する管理策は、AU-2・AU-12・CM-2・CM-6・SI-3。

拡張管理策：

(1) モバイルコード | 許容できないコードを検知し、是正措置を取る

情報システムは、[指定：組織が定めた許容できないモバイルコード]を検知し、[指定：組織が定めた是正措置]を取る。

補足的ガイダンス：許容できないモバイルコードが検知された場合の是正措置には、たとえば遮断・隔離・アドミニストレータへの通知がある。遮断には、たとえば、文書作成ソフトを使って作成されたファイルにマクロが埋め込まれていて、それらのマクロが許容できないモバイルコードであると判断された場合に、ファイルの転送を阻止することが挙げられる。

(2) モバイルコード | 調達 / 開発 / 使用

組織は、情報システムに展開されるモバイルコードの調達、開発、使用が、[指定：組織が定めた、モバイルコードに関する要求事項]を満たすようにする。

(3) モバイルコード | ダウンロード / 実行を防止する

情報システムは、[指定：組織が定めた、許容できないモバイルコード]のダウンロード と実行を防止する。

(4) モバイルコード | 自動実行を防止する

情報システムは、[指定：組織が定めたソフトウェアアプリケーション]におけるモバイルコードの自動実行を防止し、そうしたコードが実施される前に取るべき[指定：組織が定めたアクション]を取る。

補足的ガイダンス：モバイルコードが実施される前に取るべきアクションには、たとえば、ユーザが電子メールの添付ファイルを開く前に、確認メッセージを表示することがある。モバイルコードの自動実行を防ぐ手段には、CD・DVD・USB などの持ち運び可能な記憶装置を使用できる情報システムコンポーネント上で、自動実行機能を無効にすることが挙げられる。

(5) モバイルコード | 閉ざされた環境でのみ実行を許可する

組織は、閉ざされた仮想マシン環境でのみ、許可されたモバイルコードの実行を許可する。

参考文献：NIST Special Publication 800-28・DoD Instruction 8552.01

優先順位とベースライン管理策の割り当て：

P2	**低**：選択されていない	**中**：SC-18	**高**：：SC-18

SC-19 ボイスオーバーインターネットプロトコル

管理策:組織は、

a. VoIP(Voice over Internet Protocol)テクノロジーが悪意を持って使用された場合に情報システムに被害が及ぶ可能性に基づいて、VoIP テクノロジーの使用制限を定め、導入ガイダンスを作成するとともに、

b. 情報システムにおける VoIP の使用を許可・モニタリング・管理する。

補足的ガイダンス:関連する管理策は、CM-6・SC-7・SC-15。

拡張管理策:なし

参考文献:NIST Special Publication 800-58

優先順位とベースライン管理策の割り当て:

P1	**低**:選択されていない	**中**:SC-19	**高**:SC-19

SC-20 セキュアな名前 / アドレス解決サービス(信頼できるソース)

管理策:情報システムは:

a. 名前/アドレス解決に関する外部からのクエリーへのレスポンスとして、信頼のおける名前解決データを返すと共に、データ元認証と完全性検証に関するアーチファクトを提供するとともに、

b. チャイルドゾーンのセキュリティ状態を示す手段を用意する。これは、分散型の、階層的な名前空間の一部として稼働している場合で、かつ、チャイルドがセキュアな解決サービスをサポートする場合に、親ドメインと子ドメイン間のトラストチェーンの検証を可能にする。

補足的ガイダンス:この管理策を適用することで、遠隔のインターネットクライアントなどの外部クライアントは、名前/アドレス解決サービスを使用して取得した、ネットワークアドレスに対するホスト/サービス名に関して、データ元認証と完全性検証に関する保証を獲られるようになる。名前/アドレス解決サービスを提供する情報システムには、たとえば、ドメインネームシステム(DNS)サーバーがある。上記外のアーチファクトには、たとえば、DNS Security (DNSSEC) 電子署名や暗号鍵がある。DNS リソースレコードは、信頼のおけるデータの一つの例である。チャイルドゾーンのセキュリティ状態を示す手段には、たとえば、DNS の委任署名者リソースレコード の使用が挙げられる。DNS に関するこれらのセキュリティ管理策は、OMB Memorandum 08-23 を反映する(また、この Memorandum から参照される)。ホスト/サービス名とネットワークアドレスの対応付けに DNS 以外のテクノロジーを使用する情報システムは、レスポンスデータの信頼性と完全性を保証するために他の手段を用意している。関連する管理策は、AU-10・SC-8・SC-12・SC-13・SC-21・SC-22。

拡張管理策:

(1) セキュアな名前 / アドレス解決サービス(信頼できるソース) | 子サブスペース

[削除された:SC-20 に統合された]

(2) セキュアな名前 / アドレス解決サービス(信頼できるソース) | データ元 / 完全性

情報システムは、名前/アドレス解決に関する内部からのクエリーへのレスポンスとして、データ元と完全性保護に関するアーチファクトを返す。

参考文献:OMB Memorandum 08-23・NIST Special Publication 800-81

優先順位とベースライン管理策の割り当て:

P1	**低** SC-20	**中** SC-20	**高** SC-20

SC-21 セキュアな名前 / アドレス解決サービス(再帰的な問合わせを行うリゾルバ / キャッシングリゾルバ)

管理策:情報システムは、信頼できるソースから受け取った名前／アドレス解決結果としてのレスポンスに対して、データ元認証とデータ完全性検証をリクエストし、実施する。、

補足的ガイダンス:名前解決サービスの各クライアントは、この検証を自ら実施するか、あるいは、認証されたチャネルを通じて信頼できる検証サービスプロバイダに依頼できる。ローカルクライアントに名前／アドレス解決サービスを提供する情報システムには、たとえば、再帰的な問合わせによって解決を図る DNS サーバーや、キャッシング型の DNS サーバーがある。DNS クライアントリゾルバの場合、リゾルバが DNSSEC 署名の検証を実施するか、あるいはクライアントが認証されたチャネルを通じて、再帰的な問合わせを行うリゾルバにそうした検証をリクエストする。ホスト／サービス名とネットワークアドレスの対応付けに DNS 以外のテクノロジーを使用する情報システムは、クライアントによるレスポンスデータの信頼性と完全性検証を可能にする、他の手段を用意している。関連する管理策は、SC-20・SC-22。

拡張管理策:なし

(1) セキュアな名前 / アドレス解決サービス(再帰的な問合わせを行うリゾルバ / キャッシングリゾルバ) | データ元 / 完全性

[削除された:SC-21 に統合された]

参考文献:NIST Special Publication 800-81

優先順位とベースライン管理策の割り当て:

P1	**低**:SC-21	**中**:SC-21	**高**:SC-21

SC-22 名前 / アドレス解決サービスの構成およびサービスの提供

管理策:組織に対して名前／アドレス解決サービスを集合的に提供する情報システムは、耐故障性を備えていて、内部／外部の役割分割を実施する。

補足的ガイダンス:名前／アドレス解決サービスを提供する情報システムには、たとえば、DNS サーバーがある。単一点障害を排除し、冗長性を高めるために、組織は少なくとも信頼のおける 2 つの DNS サーバーを用意して、1 つは一次サーバーとして、もう一つは二次サーバーとして使用する。さらに、これらのサーバーは、通常、互いに地理的に離れているサブネットワーク上に設置される(すなわち、物理的に同じ施設には設置されない)。役割分割のために、内部の役割を担う DNS サーバーは、組織内からの(すなわち、組織内のクライアントからの)名前／アドレスレ解決リクエストのみに対処する。外部の役割を担う DNS サーバーは、組織にとって外部の(すなわち、インターネットなど、外部ネットワーク上の)クライアントからの名前／アドレスレ解決リクエストのみに対処する。組織は、特定の役割を担う、信頼のおける DNS サーバーにアクセスできるクライアントを指定する(例:アドレスの範囲指定によって、明示的なリストによって)。関連する管理策は、SC-2・SC-20・SC-21・SC-24。

拡張管理策:なし

参考文献:NIST Special Publication 800-81

優先順位とベースライン管理策の割り当て:

P1	**低**:SC-22	**中**:SC-22	**高**:SC-22

SC-23 セッションの真正性

管理策:情報システムは、通信セッションの真正性を保護する。

補足的ガイダンス:この管理策は、パケットレベルではなく、セッションレベルでの通信の保護を扱うものであり(例:ウェブベースのサービスを提供するサービス指向型アーキテクチャにおけるセッション)、通信セッションの両端で通信相手の身元と、伝送される情報の有効性に関して信頼の根拠をもたらす。真正性の保護の例としていは、中間者(man-in-the-middle)攻撃／セッションの乗っ取りや、セッションに偽の情報を挿入することに対する保護が挙げられる。関連する管理策は、SC-8・SC-10・SC-11。

拡張管理策:

(1) セッションの真正性| ログアウト時に、セッション識別子を無効にする

情報システムは、ユーザがログアウトした時点で、あるいはその他のセッションが終了した時点で、セッション識別子を無効にする。

補足的ガイダンス:この拡張管理策は、過去に有効であったセッション ID を敵対者が取得して、使用し続けるのを阻止する。

(2) セッションの真正性 | ユーザが開始したログアウト / メッセージ表示

[削除された:AC-12(1)に統合された]

(3) セッションの真正性 | ランダム化を経た一意のセッション識別子

情報システムは、[指定:組織が定めた、ランダム要件]に従って、セッションごとに一意のセッション識別子を生成する。また、システムが生成したセッション識別子のみを認める。

補足的ガイダンス:この拡張管理策は、過去に有効であったセッション ID を敵対者が再利用するのを阻止する。一意のセッション識別子の生成にランダムの概念を取り入れることにより、これから先に生成されるセッション識別子を特定するための総当り攻撃(brute-force attack)に対して、防御が可能になる。関連する管理策は、SC-13。

(4) セッションの真正性 | ランダム化を経た一意のセッション識別子

[削除された:SC-23(3)に統合された]

(5) セッションの真正性 | 認可された認証局

情報システムは、確立された保護されるセッションの有効性確認を、[指定:組織が定めた認証局]にのみ許可する。

補足的ガイダンス:セキュアなセッションの確立を認証局に委ねる場合、たとえば、セキュアソケットレイヤー(SSL) 証明やトランスポート層セキュリティ(TLS)証明などが用いられる。これらの証明書は、各々の認証局による検証後に、ウェブクライアントとウェブサーバー間の保護されたセッションの確立を容易にする。関連する管理策は、SC-13。

参考文献:NIST Special Publications 800-52・NIST Special Publications 800-77・NIST Special Publications 800-95

優先順位とベースライン管理策の割り当て:

P1	**低**:選択されていない	**中**:SC-23	**高**:SC-23

SC-24 既知の状態に陥ること

管理策:情報システムは、[指定:組織が定めたタイプの不具合]が発生した場合に、[指定:組織が定めた、システム状態に関する情報]を保持したまま、[指定:組織が定めた既知の安全な状態]へと移行する。

補足的ガイダンス:既知の安全な状態に移行することは、組織のミッション／業務ニーズに応じてセキュリティ上の問題に対処することにつながる。組織の情報システムまたはシステムコンポーネントに不具合が発生しても、既知の安全な状態に移行することで、情報の機密性、完全性、または可用性の喪失を回避できる。また、システムが個人に害を及ぼしたり、器物を破損したりする状態に陥ることも阻止できる。情報システムの状態に関する情報を保持することで、システムを再開し、ミッション／業務プロセスが中断する期間を短くして、組織の運用モードに戻すことが容易になる。関連する管理策は、CP-2・CP-10・CP-12・ SC-7・SC-22。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低**:選択されていない	**中**:選択されていない	**高**:SC-24

SC-25 薄いノード

管理策:組織は、[指定:組織が定めた情報システムコンポーネント]の機能と情報の記憶を最小限に抑える。

補足的ガイダンス:機能を減らした／最小限に抑えた情報システムコンポーネントの開発(例:ディスクレスノードや、シンクライアントといったテクノロジー)は、すべてのユーザエンドポイントを保護する必要性を減少させると同時に、情報、情報システム、およびサービスがサイバー攻撃に晒される程度を減少させる。関連する管理策は、SC-30。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-26 ハニーポット

管理策:情報システムは、悪意ある攻撃を検知・回避・分析するために、そうした攻撃の標的となるように設計されたコンポーネントを含む。

補足的ガイダンス:ハニーポットは敵対者を魅了し、組織のミッション／業務機能を支援するシステムから目をそらさせるための「おとり」として設置される。ハニーポットをどのように使用するかによって、設置前に法律顧問室に助言を求めることが、必要になる場合がある。関連する管理策は、SC-30・SC-44・SI-3・SI-4。

拡張管理策:なし

(1) ハニーポット | 悪質コードの検出

[削除された:SC-35 に統合された]

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-27 プラットフォームに依存しないアプリケーション

管理策:情報システムは、[指定:組織が定めた、プラットフォームに依存しないアプリケーション]を含む。

補足的ガイダンス:プラットフォームは、ソフトウェアアプリケーションの実行に使用されるハードウェアとソフトウェアの組み合わせである。プラットフォームは以下を含む:①オペレーティングシステム② その基盤となるコンピューターアーキテクチャ、あるいは③両方。プラットフォームに依存しないアプリケーションとは、複数のプラットフォーム上で実行可能なアプリケーションである。そうしたアプリケーションは、複数のプラットフォーム上での移植性と再構成を促進し、特定のオペレーティングシステム上で稼働する情報システムが攻撃を受けている間にも、組織の重要な機能の可用性を向上させる。関連する管理策は、SC-29。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-28 保存されている情報の保護

管理策:情報システムは、[指定:組織が定めた、保存されている情報]の[選択(1つ以上):機密性; 完全性]を保護する。

補足的ガイダンス:この管理策は、保存されている情報の機密性と完全性を扱うものであり、その対象にはユーザ情報とシステム情報が含まれる。保存されている情報とは、情報システムのコンポーネントとして記憶装置上に置かれている情報である。保護を必要とするシステム関連情報には、たとえば、ファイアウォール・ゲートウェイ・侵入検知防止システム(およびフィルタリングを行うルーター)の設定またはルールセットとともに、オーセンティケータがある。組織は機密性と完全性の保護を実現するために、たとえば暗号メカニズムやファイル共有スキャンの使用など、異なるメカニズムを使用できる。完全性を保護する手段として、たとえば、追記型媒体の使用がある。企業は、オンライン記憶装置を使用している場合で、かつ保存されている情報を十分に保護できない場合や、挿入された悪質コードを検知するための継続的なモニタリングが不可能な場合には、代わりにセキュアなオフライン記憶装置を使用するなど、他のセキュリティ管理策を使用してもよい。関連する管理策は、AC-3・AC-6・CA-7・CM-3・CM-5・CM-6・PE-3・SC-8・SC-13・SI-3・SI-7。

拡張管理策:

(1) 保存されている情報の保護 | 暗号化による保護

情報システムは、[指定:組織が定めた情報システムコンポーネント]上の[指定:組織が定めた情報]に対する不正な開示や変更を阻止するために、暗号メカニズムを導入する。

補足的ガイダンス:暗号メカニズムの選択は、組織の情報の機密性と完全性を保護する必要性に基づいて行われる。メカニズムの強度は、その情報のセキュリティカテゴリおよび/または分類レベルに相応する。この拡張管理策は、大量の電子媒体が保管されている、「媒体の保管庫」として指定されているエリアに適用されるほか、通常は運用環境内の情報システムコンポーネントに関連する限られた量の媒体(例:持ち運び可能な記憶装置、携帯機器)にも適用される。組織は、記憶装置上のすべての情報を暗号化するか(すなわち、ディスク全体の暗号化)、あるいは特定のデータ構造(例:ファイル、レコード、フィールド)のみを暗号化するかを選択できる。保存されている情報を保護するために暗号メカニズムを使

用している組織は、暗号鍵管理ソリューションの導入も検討すべきである。関連する管理策は、AC-19・SC-12。

(2) 保存されている情報の保護 | オフライン記憶装置

組織は、[指定：組織が定めた情報]をオンライン記憶装置から除去し、安全な場所にあるオフライン記憶装置に保存する。

補足的ガイダンス：組織の情報をオンライン記憶装置から除去し、オフライン記憶装置に保存することにより、個人がネットワークを介してそうした情報に不正アクセスする可能性を排除できる。したがって組織には、そうした情報をオンライン記憶装置に保存して保護する代わりに、オフライン記憶装置に保存するといった選択肢がある。

参考文献：NIST Special Publications 800-56・NIST Special Publications 800-57・NIST Special Publications 800-111

優先順位とベースライン管理策の割り当て：

P1	**低**：選択されていない	**中**：SC-28	**高**：SC-28

SC-29 異種性

管理策：組織は、情報システムの導入にあたり、[指定：組織が定めた情報システムコンポーネント]に対して多様な情報技術を使用する。

補足的ガイダンス：組織の情報システムに、より多くの種類のる情報技術を使用することで、特定の技術が悪用されることによる影響を軽減することができ、また、サプライチェーン攻撃によって引き起こされる不具合などの、共通モード故障を防ぐことができる。多様な情報技術の使用は、また、敵対者が1つの情報システムコンポーネントを侵害するのに用いる手段が、他のシステムコンポーネントに対しても同様に効果的な手段となる可能性を減らし、結果として、敵対者が計画したサイバー攻撃を成功裏に実施するのに必要な作業要因も増加する。ただし、多様性の増大が、複雑さと管理オーバーヘッドを増加させ、最終的に誤りや許可されてない設定につながる可能性がある。関連する管理策は、SA-12・SA-14・SC-27。

拡張管理策：

(1) 異種性 | 仮想化技術

組織は、[指定：組織が定めた頻度で]変化する多様なオペレーティングシステムおよびアプリケーションの実装を支援するために、仮想化技術を使用する。

補足的ガイダンス：オペレーティングシステムとアプリケーションの頻繁な変更は、構成管理を困難にするが、そうした変更は敵対者がサイバー攻撃を成功裏に実施するのに必要な作業要因を増加させる。実際のオペレーティングシステム／アプリケーションを変更する代わりに、仮想オペレーティングシステム／アプリケーションを変更すれば、アタッカーが攻撃を成功させるのを阻止することができ、構成管理に必要な労力も軽減される。さらに、仮想化技術は組織による、信頼できないソフトウェアや出所が怪しいソフトウェアの隔離された実行環境への移動を可能にする。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低**：選択されていない	**中**：選択されていない	**高**：選択されていない

SC-30 隠匿および誤った方向に向けること

管理策:組織は、[指定:組織が定めた情報システム]に対して[指定:組織が定めた、隠匿、および誤った方向に向けるための技法]を[指定:組織が定めた時間周期]でを実施することによって、敵対者を混乱させ、誤った方向に向ける。

補足的ガイダンス:隠匿、および誤った方向に向けるための技法は、敵対者がサイバー攻撃を開始し、完了させるためのターゲッティング能力(すなわち、攻撃の機会と利用可能な攻撃の矢面)を低下させる。たとえば、仮想化技術は、組織が情報システムの外観を変えることを可能にし、アタッカーが複数のプラットフォームを用意することなく攻撃を成功させる可能性を減らす。たとえばランダム化、予測できなくすること(以下、不確実性)、仮想化などの、隠匿、および誤った方向に向けるための技法の使用の増加は、敵対者を混乱させ、誤った方向に向けるのに十分であり、トレードクラフト(スパイ活動に必要な知識や技術)が発見されたり、敵対者がトレードクラフトを露出してしまう可能性を高める。隠匿、および誤った方向に向けるための技法は、また、組織が主要なミッション/業務機能を成功裏に遂行できるよう、追加の時間を与えてくれる場合がある。隠匿、および誤った方向に向けるための技法に対応するのに必要な時間と労力を考慮すると、組織によるそうした技法の使用は非常に限られるだろう。関連する管理策は、SC-26・SC-29・SI-14。

拡張管理策:

(1) 隠匿、および誤った方向に向けること | 仮想化技術

[削除された:SC-29(1)に統合された]

(2) 隠匿、および誤った方向に向けること | ランダム化

組織は、組織の業務と資産にランダム化を取り入れるための[指定:組織が定めた技法]を使用する。

補足的ガイダンス:ランダム化は、サイバー攻撃を防ぐために組織が取るアクションに関して、敵対者側の不確実性度を増加させる。そうしたアクションは、敵対者が、極めた重要なミッション/業務機能を支援する組織の情報資源を正確に狙うことを阻止する。不確実性は、また、敵対者が攻撃を開始または継続するのを躊躇させる。ランダム化を伴う、誤った方向に向けるための技法には、たとえば、一日のうちでさまざまな時間に、さまざまな情報技術(例:ブラウザー、検索エンジン)や供給業者を使用し、組織の職員の役割と責任を交換しながら、所定のアクションを実施することがある。

(3) 隠匿、および誤った方向に向けること | 処理/ 保管拠点の変更

組織は、[指定:組織が定めた処理および/または保管]拠点を[選択:[指定:組織が定めた時間頻度で];ランダムな時間間隔で]変更する。

補足的ガイダンス:敵対者は、組織の極めて重要なミッション/業務機能と、それらのミッションと機能を支援する情報資源を標的にするが、その際、自身の存在とトレードクラフトがばれるリスクを最小限に抑えようとする。静的で、同質、かつ決定論的な情報システムは、敵対者にとっては少ないコストと労力でサイバー攻撃を成功させるのにうってつけのシステムであるため、敵対者の標的になりやすい。組織の処理拠点と保管拠点を変更(「ターゲットディフェンスの移動」と称されることもある)し、仮想化・分散処理・複製などの技法を使用することで、APT(advanced persistent threat)に対処できるようになる。これにより、極めて重要なミッション/業務機能を支援する情報資源(すなわち、処理および/または保管)を再配置することが可能になる。処置拠点および/または保管拠点の変更は、敵対者によるターゲッティング活動に不確実性をもたらす。この不確実性は敵対者の作業要因を増加させ、組織の情報システムに対する侵害を敵対者にとってより困難に、かつ時間のかかる作業とすることができ、組織の極めて重要なリソースを突き止めようとする敵対者が、トレードクラフトの諸側面をうっかり開示する可能性を高めることができる。

(4) 隠匿、および誤った方向に向けること | 誤った情報を与える

組織は、[指定：組織が定めた情報システムコンポーネント]のセキュリティ状態と対策に関して、現実身のある、誤った情報を与える。

補足的ガイダンス：この拡張管理策は、組織が実施しているセキュリティ対策の性質と範囲に関して、敵対者に誤った情報を与える。結果として、敵対者 は誤った（結果として効果的でない）攻撃技法を用いる可能性がある。敵対者を誤った方向に向ける一つの方法は、敵対者がアクセスしている、または標的にしていることが分かっている外部情報システムに関して、システムに導入されているセキュリティ管理策に関する誤った情報を与えることである。もう一つの方法は、組織の情報システムの実際の諸側面を模倣しているが、実際には古いソフトウェア構成などを使用する、敵対者を欺くためのネット（例：ハニーネット・仮想環境）を使用することである。

(5) 隠匿、および誤った方向に向けること | システムコンポーネントの隠匿

組織は、[指定：組織が定めた情報システムコンポーネント]を秘匿または隠匿するための[指定：組織が定めた技法]を使用する。

補足的ガイダンス：極めて重要な情報システムコンポーネントを秘匿する、外観を変える、または隠匿することで、敵対者がそうした資産を標的にし、成功裏に侵害する可能性を減らすことが可能になる。情報システムコンポーネントを秘匿および／または隠匿するために使用できる手段には、たとえば、ルーターの設定や、ハニーネットまたは仮想化技術の使用がある。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低**：選択されていない	**中**：選択されていない	**高**：選択されていない

SC-31 隠れチャネル分析

管理策：組織は、

a. カバート[選択（1つ以上）：ストレージ;タイミング]チャネルのための手段となりうる、情報システム内の通信の側面を特定するために、隠れチャネル分析を実施するとともに、

b. それらのチャネルの最大帯域幅を見積もる。

補足的ガイダンス：開発者は、隠れチャネルにつながる可能性のある、システムコン内の箇所を特定するのに最適な立場にある。隠れチャネル分析は、セキュリティドメインに跨る許可されていない情報の流れが疑われる場合に、重要な活動となる。たとえば、情報システムが、エクスポートが規制されている情報を含んでいる場合や、外部ネットワーク（すなわち、組織によって管理されないネットワーク）に接続されている場合が該当する。隠れチャネル分析は、マルチレベルセキュア(MLS)な情報システムや、マルチセキュリティレベル(MSL)のシステム、ドメインを跨るシステムに対して有効である。関連する管理策は、AC-3・AC-4・PL-2。

拡張管理策：

(1) 隠れチャネル分析 | 隠れチャネルをテストして、利用される可能性を特定する

組織は、特定された隠れチャネルをテストして、利用される可能性のあるチャネルを特定する。

(2) 隠れチャネル分析 | 最大帯域幅

組織は、特定されたカバート[選択（1つ以上）：ストレージ、タイミング] チャネルの最大帯域幅を[指定：組織が定めた値]まで下げる。

補足的ガイダンス：情報システム開発者は、特定されたカバートストレージ／タイミングチャネルの最大帯域幅を下げるのに最適な立場にある。

(3) 隠れチャネル分析 | システムの運用環境における帯域幅を測定する

組織は、情報システムの運用環境における[指定：組織が定めた、特定された隠れチャネル]の帯域幅を測定する。

補足的ガイダンス：この拡張管理策は、開発環境ではなく、運用環境における隠れチャネルの帯域幅を扱う。運用環境における隠れチャネルの帯域幅の測定は、どれだけの情報がひそかに流出すると、組織のミッション／業務機能に悪影響が及ぶかを判断するのに役立つ。隠れチャネルの帯域幅は、特定の運用環境から独立している環境（例：実験室または開発環境）で測定される場合には、大きく変わるだろう。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低**：選択されていない	**中**：選択されていない	**高**：選択されていない

SC-32 情報システムの分割

管理策：組織は、情報システムを[指定：組織が定めた情報システムコンポーネント]に分割して、[指定：組織が定めた、コンポーネントの物理的な分離が必要な状況]に基づいて、個別の物理ドメインまたは環境に配置する。

補足的ガイダンス：情報システムの分割は、「深層防護 (defense-in-depth)」という保護戦略の一部である。組織は、システムコンポーネントが、同室の個別のラック上にある、物理的に異なるコンポーネントから、あるいは別の部屋にある、よりクリティカルなコンポーネントから、もしくは、地理的にかなり離れている場所にある、最もクリティカルなコンポーネントから、どれだけ物理的に離れているかを特定する。セキュリティカテゴリが、ドメイン分割の適切な候補の選択に役立つ場合がある。管理されたインターフェース は、分割された情報システムコンポーネント間の、ネットワークアクセスや情報の流れを制限する。関連する管理策は、AC-4・SA-8・SC-2・SC-3・SC-7。

拡張管理策：なし

参考文献：FIPS Publication 199

優先順位とベースライン管理策の割り当て：

P0	**低**：選択されていない	**中**：選択されていない	**高**：選択されていない

SC-33 伝送準備段階での完全性

[削除された：SC-8 に統合された]

SC-34 変更できない実行可能プログラム

管理策：情報システムは、[指定：組織が定めた情報システムコンポーネント]において、以下を実施する：

a. ハードウェアによって読み出し専用になっている媒体から、稼働環境をロードして、実行する
b. ハードウェアによって読み出し専用になっている媒体から、[指定：組織が定めたアプリケーション]をロードして、実行する。

補足的ガイダンス:「稼働環境」という用語は、たとえば、オペレーティングシステム、管理アプリケーション、仮想マシンモニター(すなわち、ハイパーバイザ)などのモニターを含むアプリケーションをホストする特定コードである、と定義されている。稼働環境には、ハードウェアプラットフォーム上で直接実行できるアプリケーションも含まれる。ハードウェアによって読み出し専用になっている媒体には、たとえば、CD-R/DVD-Rディスクドライブや、ワンタイムプログラマブルROMがある。内容の変更ができない記憶装置を使用することで、読み出し専用イメージ作成時の、ソフトウェアの完全性を確保できる。プログラマブルROMの使用は、以下を満たす場合に、読み出し専用媒体として使用を認められる:①初回の書き込みから、メモリーを情報システムに挿入するまで、完全性が十分に保護されるかつ②メモリーが組織の情報システムにインストールされている最中に、メモリー内のプログラムが書き換えられるのを防ぐための、信頼できるハードウェア保護がなされている。関連する管理策は、AC-3・SI-7。

拡張管理策:

(1) 変更できない実行可能プログラム | 書き込み可能な記憶装置が使われないようにする

組織は、[指定:組織が定めた情報システムコンポーネント]に関して、コンポーネントの再スタートまたは電源のオン/オフに対する耐性を有する、書き込み可能な記憶装置が使われないようにする。

補足的ガイダンス:この拡張管理策は:①指定された情報システムコンポーネントに、書き込み可能な、永続記憶装置を介して悪質コードが挿入される可能性を排除するならびに②固定記憶装置と、取り外し可能な記憶装置の両方に適用され、後者の場合には、携帯機器向けのアクセス制御によって直接対処されるか、あるいは特定の制約が課せられる。関連する管理策は、AC-19・MP-7。

(2) 変更できない実行可能プログラム | 完全性の保護 / 読み出し専用媒体

組織は、情報を読み出し専用媒体に保存する前に、情報の完全性を保護する。また、情報が媒体に保存された後は、媒体を管理する。

補足的ガイダンス:セキュリティ対策は、情報システムに挿入される媒体の置き換えや、プログラムで制御できる読み出し専用媒体がシステムにインストールされる前に、媒体内のプログラムが書き換えられるのを防げるものでなければならない。そうしたセキュリティ対策には、たとえば、防止、検知、対応の組み合わせがある。関連する管理策は、AC-5・CM-3・CM-5・CM-9・MP-2・MP-4・MP-5・SA-12・SC-28・SI-3。

(3) 変更できない実行可能プログラム | ハードウェアベースの保護

組織は、

(a) [指定:組織が定めた情報システムファームウェアコンポーネント]に対して、ハードウェアベースの書き込み保護を実施する

(b) [指定:組織が定めた権限を有する個人]に対して、ファームウェアの変更を行えるようを手動で無効にし、運用モードに戻る前に書き込み保護を再度有効にするための、特定の手順を実施する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-35 ハニークライアント

管理策:情報システムは、悪質なウェブサイトおよび/またはウェブベースの悪質コードの特定に努めるコンポーネントを含む。

補足的ガイダンス:ハニークライアントは、そのコンポーネントがインターネットを積極的に探索し、外部ウェブサイトに含まれている悪質コード(例:ワーム)を検知する点で、ハニーポットとは異なる。ハニーポットと同様に、ハニークライアントも探査中に発見された、後に実行されることになっていた悪質コードが、組織の情報システムに悪影響を及ぼすのを防ぐための、なんらかの隔離メカニズム(例:仮想化)を必要とする。関連する管理策は、SC-26・SC-44・SI-3・SI-4。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-36 分散された処理 / 保管

管理策:組織は、[指定:組織が定めた処理／保管拠点]を複数の物理的なロケーションに分散する。

補足的ガイダンス:処理／保管拠点を複数の物理的なロケーションに分散することは、ある程度の冗長性またはオーバーラップを組織にもたらし、敵対者が組織の業務、資産、個人に悪影響を及ぼすのに必要な作業要因を増加させる。この管理策は、処理／保管拠点が1つしか存在しないケースを想定していない。したがって、並列の処理／保管に対応する。関連する管理策は、CP-6・CP-7。

拡張管理策:

(1) 分散された処理 / 保管 | ポーリング技術

組織は、ポーリング技術を使用して、[指定:組織が定めた、分散だれた処理／保管拠点]における不具合、エラー、または侵害を検知する。

補足的ガイダンス:分散された処理／保管拠点は、敵対者が情報または情報システムの機密性、完全性、または可用性 を成功裏に侵害する可能性を減らす。しかしながら、処理／保管拠点の分散は、敵対者が分散された拠点のうち、1 つ(あるいは複数)を侵害するのを防げるわけではない。ポーリングは、分散されている多くの拠点における処理結果および／または保管されている内容を比較し、その後、結果について採決を行う。ポーリングにより、分散された処理／保管拠点における不具合、エラー、または侵害を検知できる。関連する管理策は、SI-4。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-37 帯域外チャネル

管理策:組織は、[指定:組織が定めた情報、情報システムコンポーネント、または機器]を[指定:組織が定めた個人または情報システム]に届ける、または電子的に送る際に、[指定:組織が定めた、帯域外チャネル]を使用する。

補足的ガイダンス:帯域外チャネルには、たとえば、情報システムに対するローカル(ネットワークを介さない)アクセス、オペレーショナルトラフィック用のネットワークパスから物理的に切り離されているネットワークパス、米国郵便業務などの非電子パスがある。これは、所定のオペレーショナルトラフィックを実施する同一のチャネル(すなわち、帯域内チャネル)を使用する場合と

は対照的である。帯域外チャネルには、帯域内チャネルと同じ脆弱性／露出は存在しない。したがって、帯域内チャネルの機密性、完全性、または可用性が侵害されても、帯域外チャネルの侵害につながるわけではない。組織は、識別子／オーセンティケータ、ハードウェア、ファームウェア、ソフトウェアの構成管理の変更、暗号鍵管理情報、セキュリティアップデート、システム／データのバックアップ、メンテナンス情報、悪質コード防止対策のアップデートなど、組織の多くのアイテムを届ける、または電子的に送る際に、帯域外チャネルを使用できる。関連する管理策は、AC-2・CM-3・CM-5・CM-7・IA-4・IA-5・MA-4・SC-12・SI-3・SI-4・SI-7。

拡張管理策:

(1) 帯域外チャネル | 確実に届ける / 電子的に送る

組織は、[指定:組織が定めた個人または情報システム]のみが、[指定:組織が定めた情報または情報システムコンポーネントもしくは機器]を受け取るようにするための、[指定:組織が定めたキュリティ対策]を実施する。

補足的ガイダンス:特定の情報、情報システムコンポーネント、または機器]を指定された個人または情報システムのみが受け取るようにするために、組織が用いる技法や手段には、たとえば、政府発行の写真付きの身分証明書を所持している個人に対して、そうした身分証明書を掲示することを条件に、国際宅配便を使って認証コードを郵送することが挙げられる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-38 運用上のセキュリティ

管理策:組織は、システム開発ライフサイクル全体を通して組織の重要な情報を保護するための[指定:組織が定めた運用上のセキュリティ対策]を実施する。

補足的ガイダンス:運用上のセキュリティ(OPSEC)は組織的なプロセスであり、このプロセスによって、組織の機微な活動の計画と実施に関連する、通常は非機密扱いの情報を特定・管理・保護し、組織の能力や意図に関する情報を敵対者が求めても、拒否できる。運用上のセキュリティプロセスは、以下の 5 つのステップで構成される:①極めて重要な情報の特定(例:セキュリティ分類プロセス)②脅威分析③脆弱性分析④リスクアセスメントならびに⑤適切な対策の実施。運用上のセキュリティ対策は、組織の情報システムと、それらのシステムが稼働する環境の両方に適用される。運用上のセキュリティ 対策の例としては、重要な情報の機密性の保護に役立つ。そうした対策には、たとえば、情報システムコンポーネントや、IT 製品およびサービスの供給業者または供給業者の候補との間で、ならびに組織外の他のエレメントや個人との間で、情報共有を制限することが挙げられる。ミッション／業務の成功に不可欠な情報には、たとえば、ユーザ識別子、エレメントユーザー、供給業者、サプライチェーンプロセス、機能要件とセキュリティ要求事項、システム設計仕様書、テストプロトコル、セキュリティ管理策の実施詳細がある。関連する管理策は、RA-2・RA-5・SA-12。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-39 プロセスの分離

管理策:情報システムは、それぞれの実行プロセスに対して個別の実行ドメインを維持する。

補足的ガイダンス:情報システムは、それぞれの実行プロセスに対して、個別のアドレス空間を割り当てることによって、個別の実行ドメインを維持することが可能になる。情報システムのそれぞれのプロセスが個別のアドレス空間を有するため、プロセス間の通信はセキュリティ機能によって管理される形で実施され、あるプロセスが別のプロセスの実行コードを修正することはできない。それぞれの実行プロセスに対して個別の実行ドメインを維持する手段としては、たとえば、個別のアドレス空間を実施することがある。このような機能は、「マルチステートプロセッサ」技術を使用する市販のオペレーティングシステムに備わっている。関連する管理策は、AC-3・AC-4・AC-6・SA-4・SA-5・SA-8・SC-2・SC-3。

拡張管理策:

(1) プロセスの分離 | ハードウェアの分離

情報システムは、プロセスの分離を容易にするために、基盤となるハードウェアを分離する。

補足的ガイダンス:情報システムプロセスのハードウェアベースの分離は、通常、ソフトウェアベースの分離と比べて、侵害を受けにくい。したがって、分離が実施されることに関して、信頼が高い。基盤となるハードウェアを分離する仕組みには、たとえば、ハードウェアメモリーの管理がある。

(2) プロセスの分離 | スレッドの分離

情報システムは、[指定:組織が定めた、マルチスレッド処理]における各スレッドに対して、個別の実行ドメインを維持する。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低**:SC-39	**中**:SC-39	**高**:SC-39

SC-40 ワイヤレスリンクの保護

管理策:情報システムは、[指定:組織が定めたタイプの信号パラメータ攻撃、またはそうした攻撃の元]から外部と内部の[指定:組織が定めたワイヤレスリンク]を保護する。

補足的ガイダンス:本管理策は、権限を与えられた情報システムユーザではない個人に見えてしまう可能性のある、内部と外部のワイヤレス通信リンクに適用される。ワイヤレスリンクが十分に保護されていないと、ワイヤレスリンクの信号パラメータが敵対者に利用されてしまう可能性がある。機密情報を得る、サービス拒否を引き起こす、あるいは組織の情報システムの正規ユーザになりすますために、ワイヤレスリンクの信号パラメータを利用する方法は多く存在する。本管理策は、ワイヤレスシステムに特有の攻撃がもたらす影響を軽減する。専用のサービスではなく、汎用のサービスとして伝送サービスを提供する民間プロバイダに組織が依存している場合には、この管理策の実施が可能でない場合がある。関連する管理策は、AC-18・SC-5。

拡張管理策:

(1) ワイヤレスリンクの保護 | 電磁妨害

情報システムは、意図的な電磁妨害がもたらす影響対して[指定:組織が定めたレベルの保護]を実現するための暗号メカニズムを導入する。

補足的ガイダンス:この拡張管理策は、通信を拒否または妨害する意図的な通信妨害(ジャミング)から保護するためのものであり、耐ジャミング保護を実現するために使用されるワイヤレスの拡散スペクトル波形が、権限を与えられていない個人によって予測されないよう

にする。この拡張管理策は、また、同一のスペクトルを共有する正規の送信機による干渉に起因する、意図されないジャミングがもたらす影響の軽減に役立つ。ワイヤレスリンクの可用性レベルと、必要とされるパフォーマンス／暗号技術は、ミッション要求、予測される脅威、運用概念、および該当する法律、指令、規定、ポリシー、標準、ガイドラインに基づいて決定される。関連する管理策は、SC-12・SC-13。

(2) ワイヤレスリンクの保護 | 発見される可能性を減らす

情報システムは、ワイヤレスリンクが発見される可能性を[指定：組織が定めた低減レベル]まで低減するための暗号メカニズムを導入する。

補足的ガイダンス：この拡張管理策は、秘密通信や、無線送信機の地理的な位置が送信中に突き止められるのを防ぐのに必要である。この拡張管理策は、発見される可能性を減らすために使用される拡散スペクトル波形が、権限を与えられていない個人によって予測されないようにする。ワイヤレスリンクをどの程度発見しづらくするかは、ミッション要求、予測される脅威、運用概念、および該当する法律・指令・規制・政策・標準・ガイドラインに基づいて決定される。関連する管理策は、SC-12・SC-13。

(3) ワイヤレスリンクの保護 | 模倣による、あるいは操作による通信欺騙

情報システムは、信号パラメータに基づいた、模倣による、あるいは操作による通信欺騙を試みる無線送信を検知し、阻止するための暗号メカニズムを導入する。

補足的ガイダンス：この拡張管理策は、無線送信の信号パラメータが権限を与えられていない個人によって予測されないようにする。こうした予測不能は、信号パラメータのみに基づいた、模倣による、あるいは操作による通信欺騙の可能性を減らす。関連する管理策は、SC-12・SC-13。

(4) ワイヤレスリンクの保護 | 信号パラメータの特定

情報システムは、送信機の信号パラメータを使用して[指定：組織が定めた無線送信機]が特定されるのを防ぐための暗号メカニズムを導入する。

補足的ガイダンス：無線フィンガープリントは、送信機の追跡や、ミッション／ユーザ識別のために、送信機の一意の信号パラメータを特定して、送信機をフィンガープリントする技法である。この拡張管理策は、機密情報の探査を目的とした無線送信機の一意の識別から保護するためのものであり、信号パラメータのフィンガープリント防止のための変更が、権限を与えられていない個人によって予測されないようにする。この拡張管理策は、匿名が必要な場合に、ミッションを確実に成功させるのに役立つ。関連する管理策は、SC-12・SC-13。

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低**：選択されていない	**中**：選択されていない	**高**：選択されていない

SC-41 ポートおよび入出力装置に対するアクセス

管理策：組織は、[指定：組織が定めた情報システムまたは情報システムコンポーネント]上の[指定：組織が定めた接続ポートまたは入出力装置]を無効または撤去する。

補足的ガイダンス：接続ポートには、たとえば、USB や Firewire (IEEE 1394)がある。入出力(I/O)装置には、たとえば、CD や DVD ドライブがある。そうした接続ポートや入出力装置を物理的に無効にする、または撤去することは、情報システムから情報が取り出されるのを防ぎ、また、そうした接続ポートや入力／出力装置を介して悪質コードがシステムに挿入されるのを防ぐのに役立つ。

拡張管理策：なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-42 センサー機能およびデータ

管理策:情報システムは:

a. :[指定:組織が定めた、センサーの遠隔でのアクティブ化を許可せざるを得ない状況]の例外を除き、環境センサー機能の遠隔でのアクティブ化を禁止するとともに、

b. [指定:組織が定めたクラスのユーザ]に対して、センサーの使用を許可する旨を明示す。

補足的ガイダンス:この管理策は、携帯機器とみなされるタイプの情報システムまたはシステムコンポーネント(例:スマートフォン・タブレット・電子書籍端末)に適用されることが多い。これらのシステムは、多くの場合、システムが使用される環境に関するデータを収集・記録するセンサーを搭載している。携帯機器に搭載されているセンサーには、たとえば、カメラ・マイク・GPS メカニズム・加速度計がある。携帯機器に搭載されているセンサーは重要な働きをするが、ひそかにアクティブ化されると、そうした機器が敵対者にとっては、個人や組織に関する有益な情報を得るための手段になる。たとえば、携帯機器に搭載されている GPS 機能を遠隔でアクティブ化できると、敵対者にとっては、その機能を利用して個人の活動の追跡が可能になる。

拡張管理策:

(1) センサー機能およびデータ | 権限を与えられた個人または役職に報告する

組織は、[指定:組織が定めたセンサー]によって収集されるデータまたは情報が、権限を与えられた個人または役職にのみ報告されるよう、情報システムを設定する。

補足的ガイダンス:センサーが権限を与えられた個人(例:エンドユーザ)によってアクティブ化される場合であっても、センサーによって収集されたデータ/情報が権限のない個人に送られる可能性がある。

(2) センサー機能およびデータ | 許可されている用途

組織は、[指定:組織が定めたセンサー]によって収集されたデータ/情報が、許可されている用途にのみ使用されるよう、以下の対策を実施する:[指定:組織が定めた対策]。

補足的ガイダンス:特定の許可されている用途のために センサーによって収集された情報が、なんらかの許可されていない用途に悪用される可能性がある。たとえば、交通ナビゲーションを支援するのに使用される GPS センサーが、個人の活動を追跡するのに悪用される可能性がある。そうした活動を軽減するための対策には、たとえば、権限を与えられた個人が自身の権限を悪用しないよう、追加のトレーニング を実施すること、または(センサーによって収集されたデータ/情報が外部関係者によって維持管理される場合には)そうしたデータ/情報の使用に契約上の制約を課すことがある。

(3) センサー機能およびデータ | 機器の使用を禁止する

組織は、[指定:組織が定めた施設、エリア、またはシステム]において、[指定:組織が定めた、環境センサー機能]を有する機器の使用を禁止する。

補足的ガイダンス:たとえば組織は、機密情報が保管されている、あるいは機微な会話が行われる特定の施設、または施設内の管理された領域に、個人が携帯電話やデジタルカメラを持ち込むことを禁止できる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-43 使用制限

管理策:組織は、

a. [指定:組織が定めた情報システムコンポーネント]が悪意を持って使用された場合に、情報システムに被害が及ぶ可能性に基づいて、それらのコンポーネントの使用制限を定め、導入ガイダンスを作成するとともに、

b. 情報システムにおける、そうしたのコンポーネントの使用を許可のうえモニタリングを通じて管理する。

補足的ガイダンス:情報システムコンポーネントは、ハードウェアコンポーネント、ソフトウェアコンポーネント、ファームウェアコンポーネント(例:VoIP・モバイルコード・デジタル複写機・プリンター、スキャナー・光学装置・ワイヤレス技術・携帯機器)を含む。関連する管理策は、CM-6・SC-7。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SC-44 デトネーションチャンバー

管理策:組織は、[指定:組織が定めた情報システム、システムコンポーネント、またはロケーション]にデトネーションチャンバー機能を持たせる。

補足的ガイダンス:「動的な実行環境」としても知られる「デトネーションチャンバー」は、組織が隔離された環境、または仮想化されたサンドボックスといった安全な環境の中で、電子メールの添付ファイルを開いたり、信頼できない、または疑わしいアプリケーションを実行したり、URLリクエストを実行できるようにする。こうした保護された、隔離された実行環境は、添付ファイル／アプリケーションが悪質コードを含んでいるかどうかを判断する手段を提供する。本管理策は、「欺くためのネット」の概念と関連性があるものの、敵対者が稼働し、かつ、彼らのアクションを観測できるような長期的な環境の維持を意図していない。むしろ、悪質コードをすばやく検知し、そうしたコードがユーザの運用環境に伝播する可能性を減らす(または、そうした伝播を完全に防ぐ)ことを意図している。関連する管理策は、SC-7・SC-25・SC-26・SC-30。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

ファミリ:システムおよび情報の完全性

SI-1　システムおよび情報の完全性のポリシーと手順

管理策:組織は、

a. 以下を策定、文書化し、[指定:組織が定めた職員または役職]に配布する:
   1. 目的、適用範囲、役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスを取り扱う、システムおよび情報の完全性のポリシー
   2. システムおよび情報の完全性のポリシーと、関連する「システムおよび情報の完全性」管理策の実施を容易にするための手順
b. 以下の最新版をレビューし、更新する:
   1. システムおよび情報の完全性のポリシーを[指定: 組織が定めた頻度で]
   2. システムおよび情報の完全性の手順を[指定: 組織が定めた頻度で]。

補足的ガイダンス:この管理策は、SI ファミリ内の選択されたセキュリティ管理策とその拡張管理策を効果的に導入するためのポリシーと手順の策定を取り扱う。ポリシーと手順は、該当する連邦法・大統領命令・指令・規制・政策・標準・手引を反映する。組織レベルでのセキュリティプログラムのポリシーと手順は、システムに特化したポリシーと手順を不要にする可能性がある。このポリシーは、組織の全般的な情報セキュリティポリシーの一部として含めることもできれば、特定の組織の複雑な性質を反映して複数のポリシーによって表現することもできる。また、この手順は、一般的なセキュリティプログラムの一部として策定することもできれば、必要に応じて特定の情報システムに特化した形で策定することもできる。組織のリスクマネジメント戦略は、ポリシーと手順を策定する上で鍵となる。関連する管理策は、PM-9。

拡張管理策:なし

参考文献:NIST Special Publications 800-12 および NIST Special Publications 800-100

優先順位とベースライン管理策の割り当て:

P1	**低**:SI-1	**中**:SI-1	**高**:SI-1

SI-2　欠陥の修正

管理策:組織は、

a. 情報システムの欠陥を特定・報告・修正するのに合わせて、
b. 欠陥の修正に関連するソフトウェアアップデートとファームウェアアップデートをインストールする前に、有効性と副次的な悪影響の可能性についてテストするとともに、
c. セキュリティ関連のソフトウェアアップデートとファームウェアアップデートを、リリースされた時点から[指定:組織が定めた期間]内にインストールするのに加えて、
d. 組織の構成管理プロセスに欠陥修正を組み入れる。

補足的ガイダンス:組織は、公表されたソフトウェア欠陥(それらの欠陥に起因する潜在的な脆弱性を含む)による影響を受ける情報システムを特定し、この情報を組織指定の情報セキュリティに責任のある職員に報告する。セキュリティ関連のソフトウェアアップデートには、たとえば、パッチ、サービスパック、ホットフィックス、アンチウイルスシグナチャーがある。組織は、また、セキュリティアセスメント・(継続的な)モニタリング・インシデント対応活動・システムエラー処理時に発見された欠陥に対処する。組織は、組織の情報システムの発見された欠陥を修正する際に、CWE(Common Weakness Enumeration:共通脆弱性タイプ一覧)または CVE(Common Vulnerabilities and Exposures:共通脆弱性識別子)データベースなどの、利用可能なリソースを

活用する。継続的な構成管理プロセスに欠陥修正を組み入れることで、必要な／期待される修正活動を追跡・検証できる。追跡と検証が可能な欠陥修正活動には、たとえば、組織が US-CERT のガイダンスや、Information Assurance Vulnerability Alerts に従っているかどうかを確認することがある。組織が定めた、セキュリティ関連のソフトウェアおよびファームウェアのアップデート適用の期限は、情報システムのセキュリティカテゴリや、アップデートの重要度（すなわち、発見された欠陥に関連する脆弱性の重大さ）に基づいて決定される。欠陥修正のタイプによっては、他のタイプよりも多くのテストを必要とする。組織は、検討中の特定のタイプの欠陥修正活動に必要なテストとそのレベルを決定し、かつ、構成管理の対象となる変更について決定する。場合によっては、組織がソフトウェアアップデートやファームウェアアップデートのテストが必要でない、あるいは有用でないと判断することがある。たとえば、単一のアンチウイルスシグナチャーのアップデートを実施する場合が該当する。組織は、また、テストに関する意思決定において、セキュリティ関連のソフトウェアアップデートやファームウェアアップデートが、適切なデジタル署名を有する認定供給業者から取得したものであるかを確認する。関連する管理策は、CA-2・CA-7・CM-3・CM-5・CM-8・MA-2・IR-4・RA-5・SA-10・SA-11・SI-11。

拡張管理策:

(1) 欠陥の修正 | 一元的管理

組織は、欠陥修正プロセスを一元的に管理する.

補足的ガイダンス:ここでいう一元的管理とは、欠陥修正プロセスの組織全体にわたる管理と実施を意味する。一元的管理は、組織が定めた、一元的に管理される、欠陥修正のためのセキュリティ管理策を策定・導入・評価・認可のうえ、モニタリングすることを含む。

(2) 欠陥の修正 | 欠陥修正状況を判断するための自動化されたメカニズム

組織は、情報システムコンポーネントの欠陥修正状況を判断するための自動化されたメカニズムを[指定:組織が定めた頻度で]実施する。

補足的ガイダンス:関連する管理策は、CM-6・SI-4。

(3) 欠陥の修正 | 欠陥修正期限 / 是正措置のためのベンチマーク

組織は、

(a) 欠陥が発見されてから、欠陥が修正されるまでの時間を測定する

(b) 是正処置を取るための[指定:組織が定めたベンチマーク]を策定する。

補足的ガイダンス:この拡張管理策は、組織に対して、情報システムの欠陥が特定された場合に、そうした欠陥を修正するまでにかかる平均時間を割り出して、是正措置を取るための組織のベンチマーク（すなわち、時間枠）を策定することを求める。ベンチマークは、欠陥のタイプ別に、また、そうした欠陥が利用された場合の脆弱性の重大さに基づいて策定することができる。

(4) 欠陥の修正 | 自動化されたパッチ管理ツール

[削除された:SI-2 に統合された]

(5) 欠陥の修正 | 自動化されたソフトウェア / ファームウェアアップデート

組織は、[指定:組織が定めた情報システムコンポーネント]に[指定:組織が定めた、セキュリティ関連のソフトウェアアップデートやファームウェアアップデート]を自動でインストールする。

補足的ガイダンス:情報システムの完全性と可用性 への配慮から、組織は自動更新を実施する方法について慎重に検討する。組織はアップデートをできるだけ早くインストールする必要性と、構成管理を維持する必要性、そして自動更新がミッション／業務にもたらす影響とのバランスを鑑みる必要がある。

(6) 欠陥の修正 | 旧バージョンのソフトウェア / ファームウェアを削除する

組織は、[指定:組織が定めたソフトウェアコンポーネントとファームウェアコンポーネント]に関して、更新版をインストールした後に、削除する。

補足的ガイダンス:更新版がインストールされた後に、旧バージョンのソフトウェアコンポーネントやファームウェアコンポーネントがシステムに残っていると、敵対者に利用される可能性がある。IT 製品によっては、旧バージョンのソフトウェアやファームウェアを情報システムから自動的に削除する。

参考文献:NIST Special Publications 800-40・NIST Special Publications 800-128

優先順位とベースライン管理策の割り当て:

P1	**低**:SI-2	**中**:SI-2 (2)	**高**:SI-2 (1) (2)

SI-3 悪質コードからの保護

管理策:組織は、

a. 情報システムの入口点と出口点に、悪質コードを検知し、根絶するための防御メカニズムを導入する。

b. 組織の「構成管理のポリシーと手順」に従って、悪質コード防御メカニズムの新しいリリースが入手可能な場合はすぐに入手して、防御メカニズムを更新する

c. 悪質コード防御メカニズムを以下を満たすように設定する:

   1. 組織のセキュリティポリシーに従って情報システムの定期スキャンを[指定:組織が定めた頻度で]実施し、かつ、外部ソースからファイルをダウンロードした時点で、またはそうしたファイルを開いたり、実行した時点で、[選択(1つ以上):端点;ネットワークの入口点と出口点]におけるファイルのリアルタイムスキャンを実施する。

   2. 悪質コードが検出された場合に、[選択(1つ以上):悪質コードを遮断する;悪質コードを隔離する;アドミニストレータに通知する];[指定:組織が定めたアクション]]

d. 悪質コードの検出および隔離における誤判定と、結果として情報システムの可用性にもたらされる影響に対処する。

補足的ガイダンス:情報システムの入口点と出口点には、たとえば、ファイアウォール、電子メールサーバー、ウェブサーバー、プロキシサーバー、リモートアクセスサーバー、ワークステーション、ノートパソコン、携帯機器がある。悪質コードには、たとえば、ウイルス、ワーム、トロイの木馬、スパイウェアがある。悪質コードは、また、さまざまなフォーマット(例:UUENCODE、Unicode)にエンコードされ、圧縮ファイルや隠しファイルに含まれていたり、ステガノグラフィーを用いてファイルに埋め込まれていたりする。悪質コードは、たとえば、ウェブアクセス、電子メール、電子メールの添付ファイル、持ち運び可能な記憶装置など、さまざまな手段を使って運び込まれる。悪質コードの挿入は、情報システムの脆弱性を利用して行われる。悪質コード防御メカニズムには、たとえば、アンチウイルスシグナチャーの定義や、評判ベーステクノロジーがある。悪質コードの影響を抑える、または排除する技術や手法は多く存在する。広範囲の構成管理と、包括的なソフトウェア完全性のコントロールは、不正コードの実行を防ぐのに効果的である。市販のソフトウェアに加えて、特注のソフトウェアにも、悪質コードが存在する可能性がある。本管理策は、組織のミッション/業務機能に影響をもたらす論理爆弾、バックドア、およびその他のタイプのサイバー攻撃にも対処する。従来の悪質コード防御メカニズムでは、そうしたコードを常に検出できるわけではない。そのような場合、組織はソフトウェアが意図された機能以外の機能を実施しないようにするために、セキュアなコーディング、構成管理およびコントロール、信頼できる調達プロセス、モニタリング対策などの他の管理策に依存する。組織が、悪質コードが検出された場合に、いつもと違うアクションが必要だと判断する場合がある。たとえば、組織が定

期スキャン時に悪質コードが発見された場合に取るアクション、悪質なダウンロードが発見された場合に取るアクション、実行ファイルを開こうとした時に悪質な仕掛けが発見された場合に取るアクションを定義することが考えられる。関連する管理策は、CM-3・MP-2・SA-4・SA-8・SA-12・SA-13・SC-7・SC-26・SC-44・SI-2・SI-4・SI-7。

拡張管理策:

(1) 悪質コードからの保護 | 一元的管理

組織は、悪質コード防御メカニズムを一元的に管理する。

補足的ガイダンス:ここでいう一元的管理とは、悪質コード防御メカニズムの組織全体にわたる管理と実施を意味する。一元的管理は、組織が定めた、一元的に管理される、悪質コード防御のためのセキュリティ管理策を策定・導入・評価・認可のうえモニタリングすることを含む。関連する管理策は、AU-2・SI-8。

(2) 悪質コードからの保護 | 自動更新

情報システムは、悪質コード防御メカニズムを自動的に更新する。

補足的ガイダンス:悪質コード防御メカニズムには、たとえば、シグナチャー定義がある。情報システムの完全性と可用性への配慮から、組織は自動更新を実施する方法について慎重に検討する。関連する管理策は、SI-8。

(3) 悪質コードからの保護 | 特権ユーザ以外のユーザ

[削除された:AC-6(10)に統合された]

(4) 悪質コードからの保護 | 特権ユーザが指示した場合のみ、更新する

情報システムは、特権ユーザが指示した場合のみ、悪質コード 防御メカニズムを更新する。

補足的ガイダンス:この拡張管理策は、セキュリティまたは業務継続のために、指定された職員によって指示／承認された場合のみ更新を適用する組織に適した管理策である。関連する管理策は、AC-6・CM-5。

(5) 悪質コードからの保護 | 持ち運び可能な記憶装置

[削除された:MP-7 に統合された]

(6) 悪質コードからの保護 | テスト / 検証

組織は、

(a) 情報システムに、良く知られていて、害のない、広がり試験ではないテストケースを導入して、悪質コード 防御メカニズムを[指定:組織が定めた頻度で]テストする

(b) テストケースの検知と、インシデント報告が行われるかどうかを確認する。

補足的ガイダンス:関連する管理策は、CA-2・CA-7・RA-5。

(7) 悪質コードからの保護 | 署名ベースでない検知

情報システムは、シグナチャーベースでない悪質コード検知メカニズムを導入する。

補足的ガイダンス:シグナチャーベースでない検知メカニズムの例としては、経験則を使用して悪質コードの特性や振る舞いを検知、分析、記述し、シグナチャーがまだ用意されていない、または既存のシグナチャーが有効でない悪質コードに対する保護対策を実施することが挙げられる。これは、多形性の悪質コード(すなわち、複製時にシグナチャーを変えてしまうコード)を含む。この拡張管理策は、シグナチャーベースの検知メカニズムの使用を妨げるわけではない。

(8) 悪質コードからの保護 | 許可されていないコマンドを検知する

情報システムは、[指定:組織が定めた、情報システムのハードウェアコンポーネント]上のカーネルアプリケーションプログラミングインターフェース を介した[指定:組織が定めた、

許可されていないオペレーティングシステムコマンド] を検知し、[選択（1つ以上）: 警告を発する;コマンドの実行をチェックする;コマンドの実行を阻止する]。

補足的ガイダンス:この拡張管理策は、カーネルベースのインターフェース以外のクリティカルなインターフェース（例:仮想マシンと特権的なアプリケーションを伴うインターフェース）にも適用される。許可されていないオペレーティングシステムコマンドが発行される例としては、たとえばカーネル機能を実施するためのコマンドに関して、権限のない情報システムプロセスがコマンドを発行した、あるいは、発行してもおかしくないプロセスがコマンドを発行したものの、疑わしいといった場合がある。検知されるべき悪質なコマンドは、コマンドのタイプ、コマンドのクラス、コマンドのインスタンスのいずれか、または組み合わせによって定義することが可能である。ハードウェアコンポーネントは、コンポーネント、コマンドのタイプ、ネットワーク上の位置のいずれか、または組み合わせによって定義することが可能である。組織は、悪質なコマンドのタイプ／クラス／インスタンスの分類に応じて、異なるアクションを選択してもよい。関連する管理策は、AU-6。

(9) 悪質コードからの保護 | リモートコマンドの認証を行う

情報システムは、[指定:組織が定めたリモートコマンド]の認証を行うための[指定:組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス:この拡張管理策は、許可されていないコマンドと、許可されているコマンドのリプレイから保護するためのものである。この機能は、その喪失、誤作動、誤った指示、または悪用が即座の、および／または深刻な結果（例:死傷、物的損害、価値の高い資産または機微な情報の喪失、重要なミッション／業務機能の不具合）をもたらす、遠隔の情報システムにとって重要である。リモートコマンドの認証を保護するための保護対策は、情報システムが許可されたコマンドのみを受け入れて、意図された順番で実施することと、許可されていないコマンドを受け入れないことを確実にするのに役立つ。リモートコマンドの認証に、暗号メカニズムを使用することができる。関連する管理策は、SC-12・SC-13・SC-23。

(10) 悪質コードからの保護 | 悪質コード分析

組織は、

(a) 悪質コードの特性と振る舞いを分析するための[指定:組織が定めたツールと技法]を使用する

(b) 悪質コード分析の結果を組織のインシデント対応プロセスと、欠陥修正プロセスに組み入れる。

補足的ガイダンス:悪質コード分析のために選択されたツールと技法を使用することで、組織は敵対者のトレードクラフト（すなわち、戦術・技術・手順）と、悪質コードのインスタンスの機能性と意図を深く理解できるようになる。悪質コードの特性を理解することで、現在の脅威と将来の脅威に対して、より効果的に対応できるようになる。組織は、リバースエンジニアリング技法を用いて、あるいは実行コードの振る舞いをモニタリングすることによって分析を行うことができる。

参考文献:NIST Special Publication 800-83

優先順位とベースライン管理策の割り当て:

P1	**低**:SI-3	**中**:SI-3 (1) (2)	**高**:SI-3 (1) (2)

SI-4 情報システムの監視

管理策:組織は、

a. 以下を検知するために、情報システムをモニタリングする:

1. ［指定：組織が定めたモニタリング目標］に従って、攻撃および攻撃の兆候
2. 不正なローカル接続、ネットワーク接続、リモート接続

b. ［指定：組織が定めた技法や手法］を用いて、情報システムの不正な使用を検知する

c. モニタリング装置を①組織が定めた必須情報を収集できるよう、情報システム内に戦略的にかつ②組織にとって重要なトランザクションを追跡できるよう、システム内の臨時の箇所に設置する

d. 侵入モニタリングツールから得た情報を不正にアクセス、変更、削除されることから保護する

e. 組織の業務と資産、個人、他の組織、または国家に対するリスク増加の兆候がある場合には常に、法執行機関からの情報、諜報機関からの情報、またはその外の信頼できる情報源からの情報に基づいて、情報システムのモニタリング活動のレベルを上げる

f. 該当する連邦法・大統領命令・指令・政策・規制に従って、情報システムのモニタリング活動に関して、法律上の見解を得る

g. ［指定：組織が定めた、情報システムのモニタリング情報］を[指定：組織が定めた職員または役職]に［選択（1つ以上）：必要に応じて;［指定：組織が定めた頻度で］］伝える。

補足的ガイダンス：情報システムのモニタリングは、外部モニタリングと内部モニタリングを含む。外部モニタリングは、情報システムの境界（すなわち、ペリミタにおける防御や境界保護の一部）で発生するイベントの観測を含む。内部モニタリングは、情報システム内で発生するイベントの観測を含む。情報システムのモニタリングは、たとえば監査活動をリアルタイムで観測したり、アクセスパターン、アクセスの特徴、その外のアクションなどの、他のシステム側面を観測することによって実現できる。モニタリング目標は、イベントの選定を左右する。情報システムのモニタリング機能は、さまざまなツールや技法（例：侵入検知システム、侵入防止システム、悪質コード防御用のソフトウェア、スキャンツール、監査記録モニタリングソフト、ネットワークモニタリングソフト）を用いて実現できる。モニタリング装置の戦略的な配置の例としては、選択された境界や、クリティカルなアプリケーションがインストールされているサーバーファームの周辺が挙げられる。そうした場合、モニタリング装置は、通常は管理策 SC-7 と AC-17 が示す管理されたインターフェース上に設置される。組織が、米国国土安全保障省が提供する Einstein ネットワークモニタリング装置を導入することも考えられる。収集するモニタリング情報の詳細レベルは、組織のモニタリング目標と、そうした目標の達成を支援する情報システムの能力に基づいて決定される。重要なトランザクションの例としては、HTTP プロキシをバイパスする HTTP トラフィックがある。情報システムモニタリングは、組織の継続的なモニタリングとインシデント対応計画の不可欠な部分である。システムモニタリングサービスからの出力情報は、継続的なモニタリングとインシデント対応計画への入力情報となる。ネットワーク接続とは、ネットワークを介して情報をやりとりする機器との接続である（例：ローカルエリアネットワーク、インターネット）。リモート接続とは、外部ネットワークを介して情報をやりとりする機器との接続である（例：インターネット）。ローカル接続、ネットワーク接続、およびリモート接続は、有線であってり、無線であったりする。関連する管理策は、AC-3・AC-4・AC-8・AC-17・AU-2・AU-6・AU-7・AU-9・AU-12・CA-7・IR-4・PE-3・RA-5・SC-7・SC-26・SC-35・SI-3・SI-7。

拡張管理策：

(1) 情報システムのモニタリング | システム全体にわたる侵入検知システム

組織は、個々の侵入検知ツールを接続し、情報システム全体にわたる侵入検知システムとして設定する。

(2) 情報システムのモニタリング | リアルタイム分析のための自動化されたツール

組織は、エベントのリアルタイムに近い分析を支援する自動化されたツールを使用する。

補足的ガイダンス：自動化されたツールには、たとえば、組織の情報システムによって生成された警告や通知をリアルタイムで分析するためのホストベース、ネットワークベース、トラ

ンスポートベース、またはストレージベースのイベントモニタリングツールや、SIEM（Security Information and Event Management）テクノロジーがある。

(3) 情報システムのモニタリング | 自動化されたツールの統合

組織は、侵入検知ツールをアクセス制御メカニズムとフロー制御メカニズムに組み込むための自動化されたツールを使用する。こうしたツールを使用することで、攻撃の隔離と排除を支援するための、それらのメカニズムの再構成が可能になり、攻撃に迅速に対処できる。

(4) 情報システムのモニタリング | 内向け / 外向けの通信トラフィック

情報システムは、内向け／外向けの通信トラフィックを[指定：組織が定めた頻度で]モニタリングして、通常でない、または許可されていない活動または状況について確認する。

補足的ガイダンス：情報システムの内向け／外向けの通信トラフィックに関連する、通常でない／許可されていない活動または状況には、たとえば、組織の情報システム内に潜む悪質コードの存在を示す内向けトラフィック、またはシステムコンポーネント間で伝播する悪質コードの存在を示す内向けトラフィック、情報の不正利用、外部情報システムに対するシグナル発信がある。悪質コードのエビデンスは、侵害された可能性のある情報システム、または情報システムコンポーネントの特定に使用される。

(5) 情報システムのモニタリング | システムが生成する警告

情報システムは、以下のような侵害の兆候や、侵害の可能性の兆候がある場合に、[指定：組織が定めた職員または役職]に警告を発する。

補足的ガイダンス：警告は、たとえば、監査記録、または悪質コード防御メカニズム、侵入検知／防止メカニズムや、ファイアウォール、ゲートウェイ、ルーターなどの境界保護装置が生成する情報など、さまざまなソースから生成される。警告は、たとえば、電話、電子メールメッセージ、テキストメッセージなどで伝送される。通知リストに記載される職員には、たとえば、システムアドミニストレータ、ミッション／業務遂行の責任者、システム所有者、情報システムセキュリティ責任者がいる。関連する管理策は、AU-5・PE-6。

(6) 情報システムのモニタリング | 特権ユーザ以外のユーザを限定する

[削除された：AC-6(10)に統合された]

(7) 情報システムのモニタリング | 自動化された、疑わしいイベントに対する対応

情報システムは、発見された疑わしいイベントについて、[指定：組織が定めた、インシデント対応担当者（氏名および／または役職によって指定されている）]に通知する。

補足的ガイダンス：最も破壊的でないアクションの例として、人による応答を要請することが挙げられる。

(8) 情報システムのモニタリング | モニタリング情報の保護

[削除された：SI-4 に統合された]

(9) 情報システムのモニタリング | モニタリングツールのテスト

組織は、侵入モニタリングツールを[指定：組織が定めた頻度で]テストする。

補足的ガイダンス：侵入モニタリングツールのテストは、ツールが正しく機能することと、組織のモニタリング目標を満たすのを確実にするためにも必要である。テストの頻度は、組織が使用するツールと、ツールの設置方法によって変わる。関連する管理策は、CP-9。

(10) 情報システムのモニタリング | 暗号化された通信の可視性

組織は、[指定：組織が定めた、暗号化された通信トラフィック]が[指定：組織が定めた情報システムモニタリングツール]から見えるようにする。

補足的ガイダンス：組織は、通信トラフィックの暗号化と、通信トラフィックに対する可視性の確保といった、場合によっては矛盾する 2 つのニーズのバランスを鑑みる。組織によっては、通信トラフィックの機密性を確保する必要性が優勢される場合もあれば、ミッション保証

が、より重要な場合もある。組織は、可視性を確保する必要性が、内向けの暗号化されたトラフィック、外向けの暗号化されたトラフィック、あるいは内向けと外向けの組み合わせに適用されるかどうかを判断する。

(11) 情報システムのモニタリング | 通信トラフィックを分析し、異常の有無を確認する

組織は、情報システムの外部境界において、および選択された、[指定：組織が定めた、システムの内側のポイント（例：サブネットワーク、サブシステム）において、外向け通信トラフィックを分析し、異常の有無を確認する。

補足的ガイダンス：組織の情報システム内の異常には、たとえば、大きなファイルの転送、長期にわたる持続接続、通常でないプロトコルやポートの使用、疑わしい外部アドレスへの通信の試みがある。

(12) 情報システムのモニタリング |自動で警告を発する

組織は、以下のような、セキュリティに影響を及ぼす適切でない、または通常でない活動について、セキュリティ責任者に警告を発するための自動化されたメカニズムを使用する：[指定：組織が定めた、警告を誘発する活動]。

補足的ガイダンス：この拡張管理策は、組織によって生成され、自動化された手段を用いて伝送されるセキュリティアラートに焦点を当てている。SI-4 (5)が示す、情報システムが生成する警告（システムにとって内部である情報源（例：監査記録）に焦点が当てられる傾向にある）とは対照的に、この拡張管理策の情報源は、その他のエンティティ（例：疑わしい活動についての報告、インサイダー脅威についての報告）を含む。関連する管理策は、AC-18・IA-3。

(13) 情報システムのモニタリング | トラフィック / イベントパターンを分析する

組織は、

(a) 情報システムの通信トラフィック／イベントパターンを分析するとともに、

(b) よく見られるトラフィックパターンおよび／またはイベントを集約したプロファイルを作成するのに加えて、

(c) 上記で作成したトラフィック／イベントプロファイルを使用して、システムモニタリング装置の誤検出の数や、検出漏れの数を減らすためのチューニングを行う。

(14) 情報システムのモニタリング | ワイヤレスでの侵入検知

組織は、ワイヤレスの侵入検知システムを使用して、悪質なワイヤレス機器を特定し、情報システムに対する攻撃の試みや、侵害／侵入の可能性について確認する。

補足的ガイダンス：ワイヤレス信号は、組織が管理する施設の境界を越えて発せられる場合がある。組織は許可されていないワイヤレスアクセスポイントの徹底的なスキャンの実施を含む、不正なワイヤレス接続の調査を積極的に行う。スキャンは、許可されていないワイヤレスアクセスポイントがシステムに接続されているかどうかを確認するためにも、施設内の情報システムが設置されているエリアに限定するのではなく、必要に応じて施設の外のエリアも含めて実施する。関連する管理策は、AC-18・IA-3。

(15) 情報システムのモニタリング | 無線－有線通信

組織は、侵入検知システムを 使用して、無線ネットワークから有線ネットワークに移動するワイヤレス通信トラフィックをモニタリングする。

補足的ガイダンス：関連する管理策は、AC-18。

(16) 情報システムのモニタリング | モニタリング情報を相互に関連付ける

組織は、情報システムに導入されているモニタリングツールが生成する情報を相互に関連付ける。

補足的ガイダンス：さまざまなモニタリングツールが生成する情報を相互に関連付けることで、情報システムの活動に対する、より包括的な見解を得ることができる。通常は単独で機

能するモニタリングツール（例：ホストモニタリング、ネットワークモニタリング、ウイルス対策ソフト）を相互に関連付けることで、組織全体にわたる見解を得ることができると同時に、そうしなければ見えない攻撃パターンが明らかになる。さまざまなモニタリングツールの能力／制約を理解し、それらのツールが生成する情報の有用性をいかにして最大に引き出すかを理解することで、組織は、効果的なモニタリング計画を作成、実施し、維持できるようになる。関連する管理策は、AU-6。

(17) 情報システムのモニタリング | 総合的な状況認識

組織は、物理面での対策、サイバー対策、サプライチェーン 対策のモニタリングから得られる情報を相互に関連付けて、総合的な、組織全体にわたる状況認識を形成する。

補足的ガイダンス：この拡張管理策は、多様な情報源からのモニタリング情報を相互に関連付けることで、総合的な状況認識を形成するためのものである。物理面／サイバー／サプライチェーンのモニタリング活動の組み合わせから得られる総合的な状況認識は、高度なサイバー攻撃をより迅速に検知し、そうした攻撃に使用されている手法や技法を調査するための組織の能力を向上させる。さまざまなサイバーモニタリング情報を相互に関連付ける SI-4(16)とは対照的に、この拡張管理策は、サイバードメインを超えたモニタリングの結果を相互に関連付ける。そうしたモニタリングは、複数の攻撃ベクトルを跨いで稼働している、組織に対する攻撃を明らかにする。関連する管理策は、SA-12。

(18) 情報システムのモニタリング | トラフィックを分析し、情報の密かな取り出しを検知する

組織は、情報システムの外部境界（すなわち、システムペリミタ）において、および[指定：組織が定めた、システムの内側のポイント（例：サブネットワーク、サブシステム）において、外向け通信トラフィックを分析して、情報の密かな取り出しを検知する。

補足的ガイダンス：組織の情報の不正な取り出しに使用される密かな手段には、たとえば、ステガノグラフィーがある。

(19) 情報システムのモニタリング | 高いリスクをもたらす個人

組織は、[指定：組織が定めた情報源]によって、高レベルのリスクをもたらすことが判明された個人に対して、[指定：組織が定めた、追加のモニタリング]を実施する。

補足的ガイダンス：個人が高いリスクをもたらすことを示す兆候は、たとえば、人材記録、諜報機関、警察、および／またはその他の信頼できる情報源など、さまざまな情報源から得られる。個人に対するモニタリングは、組織内のそうしたモニタリングを実施している経営層、法律担当者、セキュリティ責任者、人材担当者との間で綿密に調整され、連邦法・大統領命令・政策・指令・規制・標準に準拠する。

(20) 情報システムのモニタリング | 特権ユーザ

組織は、特権ユーザに対して[指定：組織が定めた、追加のモニタリング]を実施する。

(21) 情報システムのモニタリング | 試験採用期間

組織は、[指定：組織が定めた、試験採用期間]に、対象者に対する[指定：組織が定めた、追加のモニタリング]を実施する。

(22) 情報システムのモニタリング | 許可されていないネットワークサービス

情報システムは、[指定：組織が定めた、認可／承認プロセス]を経て許可されていない／承認されていないネットワークサービスを検知し、[選択（1つ以上）：調査する; [指定：組織が定めた職員または役職]に警告を発する]]。

補足的ガイダンス：許可されていない／承認されていないネットワークサービスには、たとえば、組織による確認や有効性確認が行われておらず、したがって信頼できない、または有効なサービスに対して悪事を働く、サービス指向型アーキテクチャのサービスがある。関連する管理策は、AC-6・CM-7・SA-5・SA-9。

(23) 情報システムのモニタリング | ホストにベースの機器

組織は、[指定:組織が定めた情報システムコンポーネント]において[指定:組織が定めた、ホストベースのモニタリングメカニズム]を実施する。

補足的ガイダンス:ホストベースのモニタリングを実施できる情報システムコンポーネントには、たとえば、サーバー、ワークステーション、携帯機器がある。組織は、複数の IT 製品開発者からホストベースのモニタリングメカニズムを入手し、使用することを検討する。

(24) 情報システムのモニタリング | 侵害の兆候

情報システムは、侵害の兆候を発見、収集、配信し、利用する。

補足的ガイダンス:侵害の兆候は、組織の情報システム上で(ホストレベルで、またはネットワークレベルで)検知された侵入に関する、フォレンシックアーチファクトとなる。侵害の兆候は、侵害されたオブジェクトまたは情報システムに関する有益な情報を組織に提供する。ホストが侵害されたことを示す兆候には、たとえば、レジストリのキー値が勝手に設定されていることがある。ネットワークトラフィックが侵害されたことを示す兆候には、たとえば、マルウェア C&C サーバーの存在を示す URL エレメントまたはプロトコルエレメントがある。侵害の兆候の迅速な配信と対応は、情報システムと組織が同様の悪用または攻撃に対して脆弱である期間を減らし、情報セキュリティを向上させる。

参考文献:NIST Special Publications 800-61・NIST Special Publications 800-83・NIST Special Publications 800-92・NIST Special Publications 800-94・NIST Special Publications 800-137

優先順位とベースライン管理策の割り当て:

P1	**低**:SI-4	**中**:SI-4 (2) (4) (5)	**高**:SI-4 (2) (4) (5)

SI-5 セキュリティアラート、勧告、およびディレクティブ

管理策:組織は、

a. [指定:組織が定めた外部組織]から継続的に、情報システムのセキュリティアラート、勧告、およびディレクティブを受けるのと合わせて、

b. 必要であると考えられる場合に、初期のセキュリティアラート、勧告、およびディレクティブを生成するとともに、

c. セキュリティアラート、勧告、およびディレクティブを[選択(1つ以上):[指定: 組織が定めた職員または役職];[指定:組織が定めた、組織内のエレメント(部署、人)];[指定:組織が定めた外部組織]]に伝えるのに加えて、

d. 定められた時間枠に従ってセキュリティディレクティブを実施する、あるいはディレクティブの発行先の組織がディレクティブを遵守していない場合、不遵守の度合いを通知する。

補足的ガイダンス:US-CERT は、連邦政府機関全体にわたって状況認識を維持するために、セキュリティアラートおよび勧告を生成する。セキュリティディレクティブは OMB や、そうしたディレクティブを発行する責任と権限を有する指定された組織によって発行される。セキュリティディレクティブの遵守は、それらのディレクティブの多くが極めて重要であることと、ディレクティブがタイムリーに実施されない場合の組織の業務と資産、個人、他の組織、および国家にもたらされる直の負の影響を考慮すると重要である。外部組織には、たとえば、外部のミッション／業務パートナー、サプライチェーン パートナー、外部サービスプロバイダ、および提携している組織／支援組織がある。関連する管理策は、SI-2。

拡張管理策:

(1) セキュリティアラート、勧告、およびディレクティブ | 自動で警告と勧告を発する

組織は、組織全体にわたってセキュリティアラートおよび勧告情報が得られるようにする自動化されたメカニズムを使用する。

補足的ガイダンス:組織の情報システムと、それらのシステムが稼働する環境に対する、かなりの数の変更がなされる場合、組織のミッション／業務機能の成功に直接の利害関係を有する、組織のさまざまなエンティティ(部署・人)にセキュリティに関連する情報を伝える必要がある。セキュリティアラートと勧告が提供する情報によっては、情報セキュリティリスクの管理に関連する 3 つの層(ガバナンスレベル、ミッション／業務プロセス／エンタープライズアーキテクチャレベル、組織レベル)のうち、1 つ以上の層で変更が必要になる。

参考文献:NIST Special Publication 800-40

優先順位とベースライン管理策の割り当て:

P1	**低**:SI-5	**中**:SI-5	**高**:SI-5 (1)

SI-6 セキュリティ機能の検証

管理策:情報システムは:

a. [指定:組織が定めたセキュリティ機能]が正しく機能しているかどうかを検証するのと合わせて、

b. 上記の検証を[選択(1つ以上):[指定:組織が定めた、システムの遷移状態]に応じて;適切な権限を有するユーザによってコマンドが発行された時に;[指定:組織が定めた頻度で]]実施するとともに、

c. セキュリティ検証テストが失敗した場合に、[指定: 組織が定めた職員または役職]に知らせるのに加えて、

d. 異常が発見された場合に[選択(1つ以上): 情報システムをシャットダウンする;情報システムを再起動する;[指定:組織が定めた代替のアクション]を実施する]。

補足的ガイダンス:情報システムの遷移状態には、たとえば、システムの起動、再起動、シャットダウン、停止がある。情報システムが提供する通知には、たとえば、システムアドミニストレータに電子的な警告を発する、ローカルコンピュータのコンソールにメッセージを表示する、および／または 光などハードウェアによって示すことがある。関連する管理策は、CA-7・CM-6。

拡張管理策:

(1) セキュリティ機能の検証 | セキュリティテストの失敗についての通知

[削除された:SI-6 に統合された]

(2) セキュリティ機能の検証 | 分散テストを支援する自動化されたメカニズム

情報システムは、分散型のセキュリティテストの管理を支援する自動化されたメカニズムを使用する。

補足的ガイダンス:関連する管理策は、SI-2。

(3) セキュリティ機能の検証 | 検証結果を報告する

情報システムは、セキュリティ機能の検証結果を[指定:組織が定めた職員または役職]に報告する。

補足的ガイダンス:セキュリティ機能の検証結果に関心を抱く職員には、たとえば上級情報セキュリティ責任者、情報システムセキュリティ管理者、情報システムセキュリティ責任者がいる。関連する管理策は、SA-12・SI-4・SI-5。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低**:選択されていない	**中**:選択されていない	**高** :SI-6

SI-7　ソフトウェア・ファームウェア・情報の完全性

管理策:組織は、完全性検証ツールを使用して、[指定:(組織が定めた)ソフトウェア・(組織が定めた)ファームウェア・(組織が定めた)情報]に対する不正な変更を検知する。

補足的ガイダンス:ソフトウェア・ファームウェア・情報に対する不正な変更は、エラーまたは悪質な活動(例:改ざん)によって発生する。ソフトウェアには、たとえば、オペレーティングシステム(カーネル、ドライバなどの内部コンポーネントを含む)・ミドルウェア・アプリケーションがある。ファームウェアには、たとえば、BIOS(基本入出力システム)がある。情報は、たとえば、情報に関連するセキュリティ属性などのメタデータを含む。最新の完全性チェックメカニズム(例:パリティ検査・巡回冗長検査・暗号学的ハッシュ)と関連ツールを使用すれば、情報システムおよびホストされるアプリケーションの完全性を自動的にモニタリングできる。関連する管理策は、SA-12・SC-8・SC-13・SI-3。

拡張管理策:

(1) ソフトウェア、ファームウェア、および情報の完全性 | 完全性チェック

情報システムは、[指定:(組織が定めた)ソフトウェア・(組織が定めた)ファームウェア・(組織が定めた)情報]の完全性チェックを[選択(1つ以上):起動時;[指定:(組織が定めた)遷移状態に応じて、または(組織が定めた)セキュリティ関連イベント発生時に];[指定:組織が定めた頻度で]]実施する。

補足的ガイダンス:セキュリティ関連イベントには、たとえば、組織の情報システムが影響を受ける新たな脅威が確認された場合や、新しいハードウェア、ソフトウェア、またはファームウェアがインストールされた場合がある。遷移状態には、たとえば、システム起動・システム再起動・システムシャットダウン・システム停止がある。

(2) ソフトウェア・ファームウェア・情報の完全性 | 完全性違反の自動通知

組織は、完全性検証時に不一致が発見された場合に[指定:組織が定めた職員または役職]に通知する、自動化されたツールを使用する。

補足的ガイダンス:完全性の違反についてタイムリーに報告し、組織の職員に通知するための自動化されたツールを使用することは、効果的なリスク対応には必須条件となる。完全性の違反に注目する個人には、ミッション／業務遂行責任者・情報システム所有者・システムアドミニストレータ・ソフトウェア開発者・システムインテグレータ・情報セキュリティ責任者等がいる。

(3) ソフトウェア・ファームウェア・情報の完全性 | 一元的に管理される完全性検証ツール

組織は、一元的に管理される完全性検証ツールを使用する。

補足的ガイダンス:関連する管理策は、AU-3・SI-2・SI-8。

(4) ソフトウェア、ファームウェア、および情報の完全性 | 不正開封の跡がすぐ分かる梱包

[削除された:SA-12 に統合された]

(5) ソフトウェア、ファームウェア、および情報の完全性 | 自動化された、完全性違反に対する対応

情報システムは、完全性違反が発見された場合に、自動的に[選択(1つ以上):情報システムをシャットダウンする・情報システムを再起動する・[指定:組織が定めたセキュリティ対策]を実施する]]。

補足的ガイダンス：組織は、以下に基づいて、さまざまな完全性チェックと、異常に対する対応を定義してもよい：①情報システムのタイプごとに（例：ファームウェア、ソフトウェア、ユーザデータ）②特定の情報に対する（例：ブートファームウェア、特定のタイプのマシンのブートファームウェア）③それらの組み合わせ。組織の情報システム内で自動的に実施される保護対策の例としては、変更を元に戻す、情報システムを停止する、クリティカルなセキュリティファイルに対する不正な変更が発生した場合に、警告を発するなどが挙げられる。

(6) ソフトウェア、ファームウェア、および情報の完全性 | 暗号化による保護

情報システムは、ソフトウェア、ファームウェア、および情報に対する不正な変更を検出するために、暗号化メカニズムを実施する。

補足的ガイダンス：完全性を保護するために使用される暗号化メカニズムには、たとえば、デジタル署名と、非対称鍵暗号を使用して署名されたハッシュを計算して適用すること、ハッシュを生成するのに使用された鍵の機密性を保護すること、および公開鍵を使用してハッシュ情報を検証することがある。関連する管理策は、SC-13.

(7) ソフトウェア、ファームウェア、および情報の完全性 | 検知と対応の一体化

組織は、[指定：組織が定めた、情報システムに対するセキュリティ関連の変更]が不正に行われた場合の検知能力を、組織のインシデント対応能力に組み入れる。

補足的ガイダンス：この拡張管理策は、発見されたイベントが追跡・モニタリング・修正され、歴史的記録として記録されることを確実にする。歴史的記録を維持することは、長期間にわたって敵対者の活動を検知し、法的手段を取れるようにするためにも重要である。セキュリティ関連の変更には、たとえば、定められた設定の不正な変更や、情報システムの権限の不正な昇格がある。関連する管理策は、IR-4・IR-5・SI-4。

(8) ソフトウェア・ファームウェア・情報の完全性 | 重要なイベントのチェック機能

情報システムは、完全性違反の可能性がある場合には、イベントをチェックし、以下のアクションを開始できるようにする：[選択（1つ以上）：監査記録を生成する;現在のユーザに警告を発する;[指定： 組織が定めた職員または役職]に警告を発する;[指定：組織が定めたその他のアクション]を実施する]]。

補足的ガイダンス：組織は、完全性違反が発生した可能性のあるソフトウェアのタイプ、特定のソフトウェア、または情報に応じて、対応を選択する。関連する管理策は、AU-2・AU-6・AU-12。

(9) ソフトウェア、ファームウェア、および情報の完全性 | ブート処理を検証する

情報システムは、[指定：組織が定めた機器]のブート処理の完全性を検証する。

補足的ガイダンス：ブート処理の完全性を確保することは、機器を既知の状態／信頼できる状態で起動するためにも不可欠である。完全性検証メカニズムは、組織の職員に対して、信頼できるコードのみがブート処理時に実行されるのを保証する。

(10) ソフトウェア、ファームウェア、および情報の完全性 | ブートファームウェアの保護

情報システムは、[指定：組織が定めた機器]のブートファームウェアの完全性を保護するために、[指定：組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス：ブートファームウェアに対する不正な変更は、高度な標的型サイバー攻撃が原因である可能性がある。これらのタイプのサイバー攻撃が行われると、（そのファームウェアが破損している場合には）恒久的なサービス妨害につながることもあり、また（そのファームウェアに悪質コードが埋め込まれている場合には）悪質コードが長期間にわたって潜むことになる。機器が、組織の情報システム内のブートファームウェアの完全性を保護する手段には、たとえば以下がある：①ブートファームウェアに対するアップデートを実施する前に、アップデートの真正性と完全性を検証するならびに②許可されていないプロセスによる、ブートファームウェアに対する変更を阻止する。

(11)ソフトウェア、ファームウェア、および情報の完全性 | 権限が制限された、閉ざされた環境

組織は、[指定：組織が定めた、ユーザがインストールしたソフトウェア]に対して、権限が制限された、閉ざされた物理環境、または仮想マシン環境での実行を要求する。

補足的ガイダンス：組織は、供給元が疑わしい、あるいは悪質コードを含んでいる可能性のあるソフトウェアを検知する。このタイプのソフトウェアの場合、ユーザによるインストールは、悪質コードが実行された場合の被害を抑えるために、閉ざされた運用環境で行われる。

(12)ソフトウェア、ファームウェア、および情報の完全性 | 完全性検証

組織は、[指定：組織が定めた、ユーザがインストールしたソフトウェア]に関して、実行前に完全性検証が行われることを要求する。

補足的ガイダンス：組織は、ユーザがインストールしたソフトウェアに関して、実行前に完全性検証を行うことによって、悪質コードや、不正な変更に起因するエラーを含むコードが実施される可能性を減らす。組織は、ソフトウェアの完全性を検証するためのアプローチの現実性（ソフトウェア開発者／ベンダーの信頼性の検証にチェックサムを使用できるかを含む）について 検証する。

(13)ソフトウェア、ファームウェア、および情報の完全性 | 保護された環境内でのコードの実行

組織は、ソースコードを提供しない、保証が限られている（あるいは、全くない）供給元から入手したバイナリーコードまたはマシンコードの実行を、[指定：組織が定めた職員または役職]の明確な承認を得た上で、閉ざされた物理環境または仮想マシン環境でのみ許可する。

補足的ガイダンス：この拡張管理策は、バイナリーコードまたはマシンコード（市販のソフトウェア／ファームウェアおよびオープンソースソフトウェアを含む）を提供するすべての者に適用される。

(14)ソフトウェア、ファームウェア、および情報の完全性 | バイナリーコードまたはマシンコード

組織は、

(a) ソースコードを提供しない、保証が限られている（あるいは、全くない）供給元から入手したバイナリーコードまたはマシンコードの使用を禁止するとともに、

(b) ミッション／業務上やむをえない場合で、かつ運用認可責任者の承認を得らた場合に、ソースコード要件に対する例外を認める。

補足的ガイダンス：この拡張管理策は、バイナリーコードまたはマシンコード（市販のソフトウェア／ファームウェアおよびオープンソースソフトウェアを含む）を提供するすべての者に適用される。組織は、ソースコードを提供しない、保証が限られている（あるいは、全くない）ソフトウェア製品をアセスメントして、セキュリティ上の影響を確認する。このアセスメントは、これらのタイプのソフトウェア製品が多くの場合、組織がソースコードにアクセスできないためにレビュー、修正、または拡張が困難であるといった事実と、組織の代わりに修正を行うオーナーがいない可能性を念頭に行われる。関連する管理策は、SA-5。

(15)ソフトウェア・ファームウェア・情報の完全性 | コード認証

情報システムは、[指定：組織が定めたソフトウェアコンポーネントまたはファームウェアコンポーネント]のインストールに先立ち、コンポーネントの認証を行うための暗号メカニズムを導入する

補足的ガイダンス：暗号による認証は、たとえば、ソフトウェアコンポーネントまたはファームウェアコンポーネントが、組織が許可／承認した証明書を用いてデジタル署名されたかどうかを確認することを含む。コード署名は、悪質コードから保護するための有効な手段となる。

(16)ソフトウェア・ファームウェア・情報の完全性 | モニタリングなしのプロセスの実行に、タイムリミットを課す

組織は、モニタリングなしでのプロセスの実行が、[指定：組織が定めた期間]を超えるのを阻止する。

補足的ガイダンス：この拡張管理策は、プロセスに通常の実行期間が定められていて、組織がそうした期間を超過するといった状況に対処する。モニタリングには、たとえば、（オペレーティングシステムの）タイマー・自動応答・情報システムプロセスの異常発生時の手動でのモニタリングと対応がある。

参考文献：NIST Special Publications 800-147・NIST Special Publications 800-155

優先順位とベースライン管理策の割り当て：

P1	**低** 選択されていない	**中** SI-7 (1) (7)	**高** SI-7 (1) (2) (5) (7) (14)

SI-8 スパムからの保護

管理策：組織は、

a. 情報システムの入口点と出口点でスパム 防御メカニズムを実施して、迷惑メッセージを検知し、措置を講じるとともに、

b. 組織の「構成管理のポリシーと手順」に従って、スパム防御メカニズムの新しいリリースが入手可能な場合はすぐに入手して、防御メカニズムを更新する。

補足的ガイダンス：情報システムの入口点と出口点には、たとえば、ファイアウォール・電子メールサーバー・ウェブサーバー・プロキシサーバー・リモートアクセスサーバー・ワークステーション・携帯機器・ノートパソコン／ラップトップコンピュータがある。スパムは、たとえば、電子メール・（電子メールの）添付ファイル・ウェブアクセスなど、さまざまな手段を使って運び込まれる。スパム防御メカニズムには、たとえば、シグナチャーの定義がある。関連する管理策は、AT-2・AT-3・SC-5・SC-7・SI-3。

拡張管理策：

(1) スパムからの保護 | 一元的管理

組織は、スパム 防御メカニズムを一元的に管理する。

補足的ガイダンス：ここでいう一元的管理とは、スパム防御メカニズムの組織全体にわたる管理と実施を意味する。一元的管理には、組織が定めた一元的に管理されるスパム防御のためのセキュリティ管理策を策定・導入・評価・認可のうえモニタリングすることが含まれる。関連する管理策は、AU-3・SI-2・SI-7。

(2) スパムからの保護 | 自動更新

情報システムは、スパム 防御メカニズムを自動的に更新する。

(3) スパムからの保護 | 継続的に学ぶ能力

情報システムは、正規の通信トラフィックをより効果的に特定するために、学習機能を備えたスパム 防御メカニズムを導入する。

補足的ガイダンス：学習メカニズムには、たとえば、Bayesian フィルターがある。これは、ユーザが指定したトラフィックをアルゴリズムのパラメータに指定し直して、トラフィックの正確な分離を行うことで、そのトラフィックがスパムであるか、あるいは正規であるかを返答する。

参考文献：NIST Special Publication 800-45

優先順位とベースライン管理策の割り当て:

P2	**低**:選択されていない	**中**:SI-8 (1) (2)	**高**:SI-8 (1) (2)

SI-9 情報入力制限

[削除された:AC-2・AC-3・AC-5・AC-6 に統合された]

SI-10 入力情報の妥当性確認

管理策:情報システムは、[指定:組織が定めた、情報入力]の有効性をチェックする。

補足的ガイダンス:情報システムへの入力情報のシンタクスと意味(例:文字セット、長さ、数値の範囲、許容値)のチェックでは、入力情報が指定されたフォーマットや内容に適合しているかどうかを確認する。ソフトウェアアプリケーションは、通常、ソフトウェアモジュール/システムコンポーネント間の通信のための構造化されたメッセージ(すなわち、コマンドまたはクエリー)を使用する、明確に定義されたプロトコルに準拠する。構造化されたメッセージは、メタデータまたは制御情報に組み入れられている生データや構造化されていないデータを含む場合がある。ソフトウェアアプリケーションが、構造化されたメッセージを構築するためにアタッカーが入力した情報を、メッセージを適切にエンコードしないで使用した場合に、アタッカーによる悪質なコマンドまたは特殊な文字の挿入を許してしまい、データが制御情報またはメタデータとして解釈される可能性がある。その結果、改ざんされた出力情報を受け取るモジュールまたはコンポーネントが、誤った行動を取ったり、データを誤って解釈してしまう。インタープリターに渡される入力情報を事前に選別することによって、その情報が誤ってコマンドとして解釈されたるのを防ぐことができる。入力情報のチェックは、正確で正しい入力情報となることを保証し、クロスサイトスクリプティングやさまざまなインジェクション攻撃などの攻撃に対する防御策となる。

拡張管理策:

(1) 入力情報の妥当性確認 | 手動によるオーバーライド機能

情報システムは:

(a) [指定:組織が定めた入力情報]の有効性を確認するための、手動によるオーバーライド機能を提供するとともに、

(b) 手動によるオーバーライド機能の使用を、[指定:組織が定めた、権限を与えられた個人]に限定するのに加えて、

(c) 手動によるオーバーライド機能をチェックする。

補足的ガイダンス:関連する管理策は、CM-3・CM-5。

(2) 入力情報の妥当性確認 | エラーのレビュー / 解消

組織は、入力エラーがレビューされ、[指定:組織が定めた期間]内に解消されるようにする。

補足的ガイダンス:入力エラーを解消する方法には、たとえば、システムのエラーの原因を修正することや、修正した入力情報をもってトランザクションを再度サブミットすることがある。

(3) 入力情報の妥当性確認 | 予測可能な振る舞い

情報システムは、有効でない入力情報を受け取った場合に、組織の目的とシステムの目的に沿って、予想できる形で、かつ記載どおりに動作する。

補足的ガイダンス:組織の情報システムによく見られる脆弱性には、有効でない入力情報を受け取った場合に、予期せぬ形で動作することがある。この拡張管理策は、有効でない入力情報を受け取った場合も、予想できる形で動作するのを保証するためのものであり、

システムを予期せぬ副次的な悪影響を受けることなく既知の状態に戻すのを容易にする、情報システムレスポンスを指定する。

(4) 入力情報の妥当性確認 | やりとりをレビューし、タイミングを調整する

組織は、有効でない入力情報に対する適切な対処を決定する上で、情報システムコンポーネント間のやりとりのタイミングの調整に責任がある。

補足的ガイダンス:プロトコルインターフェースやタイミングインターフェースを介して、情報システムが受け取った有効でない入力情報 に対処することは、プロトコルスタック内の一つのプロトコルが、別のプロトコル上の誤ったレスポンスがもたらす影響を考慮する必要がある場合に、重要になる。たとえば、802.11 標準ワイヤレスネットワークプロトコルは、(たとえば、有効でないパケットが入力されて)パケットが喪失しても、TCP とはやりとりしない TCP は、パケットの喪失は混雑のためと考える。一方 802.11 リンク上では、パケットの喪失は、通常はリンク上の衝突またはノイズに起因して発生する。TCP が混雑を示すレスポンスを返すのであれば、衝突イベントに対して誤ったアクションを取るのは明らかである。敵対者は、有効でない入力情報を構築して悪影響を及ぼすために、プロトコルの許容できる個々の振る舞いを利用する可能性がある。

(5) 入力情報の妥当性確認 | 入力情報を信頼できる情報源と、認可されたフォーマットに限定する

組織は、入力情報の使用を[指定:組織が定めた、信頼できるソース]および/または[指定:組織が定めたフォーマット]に限定する。

補足的ガイダンス:この拡張管理策は、情報入力に対する「ホワイトリスト」の概念を適用する。情報入力の既知の信頼できる情報源と、そうした入力情報の許容できるフォーマットを指定することで、悪質な活動が行われる可能性を減せる。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低** 選択されていない	**中** SI-10	**高** SI-10

SI-11 エラー処理

管理策:情報システムは:

a. 敵対者によって利用される可能性のある情報を開示することなく、是正活動に必要な情報を提供する誤りメッセージを生成するとともに、

b. 誤りメッセージを[指定:組織が定めた職員または役職]にのみ開示する。

補足的ガイダンス:組織は、誤りメッセージの構造/内容を慎重に検討する。情報システムがエラー状態を検知し、対処できる度合いは、組織のポリシーおよび運用上の要求事項に基づいて決定される。敵対者によって利用される可能性のある情報には、たとえば、記録された情報から導出される(あるいは、はっきりと示される)ユーザ名やミッション/業務情報などの、うかつに入力されたパスワードによる誤ったログインの試みや、アカウント番号、社会保障番号、クレジットカード番号などの個人情報がある。さらに、誤りメッセージは、情報を伝送するための隠れチャネルを提供する場合がある。関連する管理策は、AU-2・AU-3・SC-31。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低**:選択されていない	**中**:SI-11	**高**:SI-11

SI-12 情報の処理および保持

管理策:組織は、情報システム内の情報と、そのシステムから出力された情報を該当する連邦法・大統領命令・指令・政策・規制・標準・運用上の要求事項に従って処理・保持する。

補足的ガイダンス:情報の処理および保持に関する要求事項は、情報のライフサイクル全体をカバーするが、場合によっては、情報システムの廃棄の後続ステップもカバーする。National Archives and Records Administration は、記録の保管に関する手引きを提供している。関連する管理策は、AC-16・AU-5・AU-11・MP-2・MP-4。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P2	**低**:SI-12	**中**:SI-12	**高**:SI-12

SI-13 予測可能な障害の防止

管理策:組織は、

a. 特定の運用環境における[指定:組織が定めた情報システムコンポーネント]の平均故障時間(MTTF)を定めるとともに、
b. 代替の情報システムコンポーネントと、[指定:組織が定めた、MTTF 置き換え基準]に沿って、アクティブなコンポーネントを予備コンポーネントに置き換える手段を用意する。

補足的ガイダンス:MTTF は、そもそも信頼性問題であるが、この管理策はセキュリティ能力をもたらす情報システムコンポーネントの不具合に対処する。故障率は、インストールに特化して考慮され、業界平均を意味するわけではない。組織は、MTTF の設定値に基づいて、情報システムコンポーネントの不具合がもたらす被害を考慮しながら、情報システムコンポーネントの置き換え基準を定める。アクティブモードなコンポーネントと予備コンポーネント間の権限の委譲が、安全性、運用の準備ができるていこと、またはセキュリティ能力(例:状態変数の維持)を低下させることはない。予備コンポーネントは、メンテナンス時や、復旧が失敗している場合を除き、常に利用可能である。関連する管理策は、CP-2・CP-10・MA-6。

拡張管理策:

(1) 予測可能な障害の防止 | コンポーネントの権限を委譲する

組織は、指定:組織が定めた割合の]平均故障時間より遅くならないよう、アクティブな情報システムコンポーネントから予備コンポーネントへの権限の委譲を行って、アクティブなコンポーネントをサービスから外す。

(2) 予測可能な障害の防止 | モニタリングなしのプロセスの実行に、タイムリミットを課す

[削除された:SI-7(16)に統合された]

(3) 予測可能な障害の防止 | コンポーネント間の手動での委譲

組織は、平均故障時間が[指定:組織が定めた期間]を超過した場合に、アクティブな情報システムコンポーネントと、予備コンポーネント間の権限の委譲を手動で開始する。

(4) 予測可能な障害の防止 | 予備コンポーネントのインストール / 通知

組織は、情報システムコンポーネントの不具合が発見された場合に、以下を実施する:

(a) 予備コンポーネントが[指定:組織が定めた期間]内に成功裏に、かつ 透過的にインストールされるようにする

(b) [選択(1つ以上):[指定:組織が定めたアラーム]をアクティブ化する; 情報システムを自動的にシャットダウンする]。

補足的ガイダンス:自動あるいは手動での、予備コンポーネントのアクティブなコンポーネントへの転換は、たとえば、アクティブなコンポーネントの不具合が発見された時点で実施される。

(5) 予測可能な障害の防止 | 障害迂回機能

組織は、情報システムに対して[選択:リアルタイムの・ほぼリアルタイムの][指定:組織が定めた障害迂回機能]を用意する。

補足的ガイダンス:障害迂回とは、一次情報システムの不具合発生時に、代替情報システムに自動的に切り替わることをいう。障害迂回機能には、たとえば、代替処理拠点での情報システムオペレーションのミラーリングや、組織の復旧時間によって定義される一定間隔での、データの定期的なミラーリングがある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SI-14 非永続性

管理策:組織は、既知の状態で開始され、[選択(1つ以上):使用中のセッションの終了時に[指定:組織が定めた頻度で]周期的に]]終了する、非永続的な[指定:組織が定めた情報システムコンポーネントおよびサービス]を実施する。

補足的ガイダンス:この管理策は、敵対者がサイバー攻撃を開始し、完了させるためのターゲッティング能力(すなわち、攻撃の機会と利用可能な攻撃の矢面)を著しく低下させることによって、APT (advanced persistent threats)によるリスクを低減する。選択された情報システムコンポーネントに対して「非永続性」の概念を実施することで、組織の情報システム、またはそれらのシステムが稼働する環境の脆弱性を利用するのに十分な時間を敵対者与えないよう、コンピュータリソースを特定の期間にわたって既知の状態に保つことができる。APT は、その能力、意図、ターゲッティング能力からしてハイエンドな脅威であるため、時間をかければサイバー攻撃が成功する可能性が一定の割合であると、組織は考える。非永続的な情報システムコンポーネントとサービスは、保護された情報を使用して必要に応じてアクティブ化され、周期的に、またはセッションの終了時に終了する。非永続性は、組織の情報システムの侵害または侵入を試みる敵対者の作業要因を増加させる。

非永続的なシステムコンポーネントは、たとえば、周期的に再イメージングされるコンポーネントや、一般に使用されるさまざまな仮想化技術を使用して実現できる。非永続的なサービス は、仮想マシンの一部として、あるいは物理マシン上のプロセスの新しいインスタンス(永続的あるいは非永続的)として、仮想化技術使用することで 実現できる。情報システムコンポーネント／サービスの定期的なリフレッシュがもたらす利点は、組織がコンポーネントまたはサービスの侵害が発生したかどうかを、はじめに判断する必要がないことである(組織にとって、その判断が困難であることが多い)。選択された情報システムコンポーネントとサービスのリフレッシュは、攻撃が意図する影響が広がるのを防ぐのに十分な頻度で、ただし、情報システムが不安定にならない頻度で実施される。場合によっては、クリティカルなコンポーネントやサービスのリフレッ

シュが、脆弱性を利用するための敵対者の能力を阻害するためにも、定期的に実施される。関連する管理策は、SC-30・SC-34。

拡張管理策:

(1) 非永続性 | 信頼できる情報源を利用したリフレッシュ

組織は、情報システムコンポーネントやサービスのリフレッシュ時に使用されるソフトウェアやデータが、[指定:組織が定めた、信頼できる情報源]から入手されるようにする。

補足的ガイダンス:信頼できる情報源には、たとえば、一度だけ書き込み可能な媒体、読み出し専用の媒体、選択されたオフラインのセキュアな保管場所がある。

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低** :選択されていない	**中**:選択されていない	**高** :選択されていない

SI-15 出力情報のフィルタリング

管理策:情報システムは、[指定:組織が定めた、ソフトウェアプログラムおよび／または アプリケーション]からの出力情報を検証して、期待される内容と一致しているかを確認する。

補足的ガイダンス:特定のタイプのサイバー攻撃(例:SQL インジェクション)は、予期せぬ出力情報、またはソフトウェアプログラムまたはアプリケーションからの通常期待される出力情報とは異なる出力情報を生成する。この拡張管理策は、無関係な内容を検知することと、そうした無関係な内容が表示されるのを防ぐこと、そして異常な振る舞いが発見された場合にモニタリングツールに警告を発することに焦点を当てている。関連する管理策は、SI-3・SI-4。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P0	**低**:選択されていない	**中**:選択されていない	**高**:選択されていない

SI-16 メモリーの保護

管理策:情報システムは、許可されていないコードの実行からメモリーを保護するための、[指定:組織が定めたセキュリティ対策]を実施する。

補足的ガイダンス:敵対者によっては、メモリー内のコードの実行が許されていない領域で、あるいは禁止されているメモリー領域でコードの実施を試みる攻撃をしかける。メモリーを保護するために導入されるセキュリティ対策には、たとえば、データ実行の防止や、アドレス空間のレイアウトのランダム化がある。データの実行を阻止するための対策は、ハードウェアによって、あるいはソフトウェアによって実施できる。後者の場合、強度がより高いメカニズムを提供するハードウェアを使用する。関連する管理策は、AC-25・SC-3。

拡張管理策:なし

参考文献:なし

優先順位とベースライン管理策の割り当て:

P1	**低**:選択されていない	**中**:SI-16	**高**:SI-16

SI-17　安全を保証するための手続き

管理策：情報システムは、[指定：組織が定めた障害]が発生した場合に、[指定：組織が定めた、フェイルセーフ手順]を実施する。

補足的ガイダンス：障害には、たとえば、クリティカルなシステムコンポーネント間、あるいはシステムコンポーネントと運用施設間の通信の喪失がある。フェイルセーフ手順には、たとえば、オペレータ職員に警告を発して、その後の取るべきステップに関する具体的な指示を出すこと（例：何もしない、システム設定を再構築する、プロセスをシャットダウンする、システムを再起動する、指定された職員に連絡を取る）がある。関連する管理策は、CP-12・CP-13・SC-24・SI-13。

拡張管理策：なし

参考文献：なし

優先順位とベースライン管理策の割り当て：

P0	**低**：選択されていない	**中**：選択されていない	**高**：選択されていない

1

付録 G

情報セキュリティプログラム

組織全体にわたる情報セキュリティプログラムマネジメント管理策

FISMA は、組織に対して、組織の業務と資産を支援する情報と情報システム（別の組織、請負業者、またはその他の業者によって提供される、または管理される情報やシステムを含む）の情報セキュリティを扱う、組織全体にわたる情報セキュリティプログラムを策定・、実施することを要求している。この付録に記載されている「情報セキュリティプログラムマネジメント（以下、PM）」管理策は、通常、組織レベルで実施され、組織内の個々の情報システムには対応しない。PM 管理策は、該当する連邦法・大統領命令・指令・政策・規制・標準への準拠を容易にする目的で策定された。これらの管理策は、FIPS Publication 200 に記載されている影響レベルのいずれにも対応しない。したがって、付録 D に記載されているセキュリティ管理策ベースラインのいずれにも対応しない。しかしながら、PM 管理策は、付録 F のセキュリティ管理策を補足するものであり、特定の情報システムに限定されない、プログラムに基づいた、組織全体にわたる情報セキュリティ要求事項に焦点を当てている。したがって PM 管理策は、情報セキュリティプログラムの管理には不可欠である。調整に関するガイダンスは、付録 F のセキュリティ管理策に適用されるのと同様の方法で、PM 管理策にも適用することができる。組織は、PM 管理策について策定・導入・アセスメント・認可・モニタリングに責任と説明責任のある1人の、あるいは複数の個人を指定する。組織は、「情報セキュリティプログラム計画書」に PM 管理策を記載する。組織全体にわたる情報セキュリティプログラム計画書は、組織のそれぞれの情報システムに対して作成された、個々のセキュリティ計画を補足する。それと同時に、個々の情報システムのセキュリティ計画と、情報セキュリティプログラムは、組織が導入するセキュリティ管理策の全体をカバーする。

セキュリティプログラム計画は、PM 管理策を文書化するのに加えて、付録 F の共通管理策として指定されてセキュリティ管理策（すなわち、組織の情報システムによって継承されるセキュリティ管理策）すべてを組織が、一元的に管理されるリポジトリに記載するための手段となる[111]。情報セキュリティプログラム計画書に記載されている PM 管理策と共通管理策は、リスクの管理に関して、情報システムの運用認可責任者と同じ、または同様の権限と責任を有する上級職員によって導入され、有効性がアセスメントされ[112]、認可される。アセスメントを通じて期待された効果が得られないと判断された PM 管理策と共通管理策については、行動計画とマイルストーンが作成され、維持管理される。PM 管理策と共通管理策も、組織内の個々の情報システムに導入されているセキュリティ管理策と同様に、継続的なモニタリングの対象となる。

表 G-1 は、付録 G に記載されている PM ファミリ内のセキュリティ管理策に関して、それぞれの管理策の概要を示している。組織は、PM 管理策をどの順番で導入するかを決定する際に、各管理策に対応する「優先順位コード」表記を使用することができる（すなわち、優先順位コード 1 [P1]管理策は、優先順位コード 2 [P2]管理策よりも導入の優先度が高く、優先順位コード 2 [P2]管理策は、優先順位コード 3 [P3]管理策よりも導入の優先度が高いということ）。

[111] 共通管理策とは、組織の単一の、あるいは複数の情報システムによって継承が可能なセキュリティ管理策であり、PM 管理策とは別のものである。

[112] PM 管理策と共通管理策のアセスメント手順に関しては、NIST Special Publication 800-53A を参照のこと。

2

表 G-1: PM 管理策

管理策番号	管理策名	優先順位	開始点としての管理策ベースライン		
			低	中	高
PM-1	情報セキュリティプログラム計画 書	P1	**組織全体にわたって導入される。 情報セキュリティプログラムを支援する。 セキュリティ管理策ベースラインに対応しない。 いずれのシステム影響レベルにも関連しない。**		
PM-2	上級情報セキュリティ責任者	P1			
PM-3	情報セキュリティリソース	P1			
PM-4	行動計画およびマイルストーンプロセス	P1			
PM-5	情報システム一覧	P1			
PM-6	情報セキュリティパフォーマンスの測定	P1			
PM-7	エンタープライズアーキテクチャ	P1			
PM-8	重要インフラ計画	P1			
PM-9	リスクマネジメント戦略	P1			
PM-10	セキュリティ認可プロセス	P1			
PM-11	ミッション／業務プロセスの定義	P1			
PM-12	インサイダー脅威に対する対策	P1			
PM-13	情報セキュリティ要員	P1			
PM-14	テスト、トレーニング、およびモニタリング	P1			
PM-15	セキュリティグループやセキュリティ団体と連絡を取り合う	P3			
PM-16	脅威意識向上のためのプログラム	P1			

注意書

組織は、組織の情報セキュリティプログラムの基盤を提供するための、PM 管理策を導入する必要がある。組織の情報システムにセキュリティ管理策を成功裏に導入するには、組織全体にわたる PM 管理策を成功裏に導入できなければならない。しかしながら、それぞれの組織が PM 管理策を実施する方法は、たとえば、組織の規模、複雑さ、ミッション／業務上の要求事項などの、組織の特性によって変わってくる。

PM-1　情報セキュリティプログラム計画書

管理策：組織は、

a. 組織全体にわたる情報セキュリティプログラム計画書を策定し、配布する：
   1. セキュリティプログラムの要求事項の概要を示し、それらの要求事項を満たすために導入が計画されている、あるいは導入されている PM 管理策と共通管理策について説明する
   2. 役割、責任、経営コミットメント、組織間の調整、およびコンプライアンスに関して、特定と割当てを含める
   3. 情報セキュリティのさまざまな側面（すなわち、技術面、物理面、職員による、サイバー物理面）に責任がある組織のエンティティ（部署、グループ、人）間の調整についてレビューする
   4. 組織の業務（ミッション、機能、イメージ、および評判を含む）、組織の資産、個人、他の組織、および国家に対するリスクに責任と説明責任のある上級職員による承認を得ている
b. 組織全体にわたる情報セキュリティプログラム計画書を［指定：組織が定めた頻度で］レビューする
c. 情報セキュリティプログラム計画書を、組織的な変更や、計画実施中に特定された問題、またはセキュリティ管理策アセスメント結果に基づいて更新する
d. 情報セキュリティプログラム計画書 を不正な開示や変更から保護する。

補足的ガイダンス：情報セキュリティプログラム計画書は、組織の自由裁量で、単一のドキュメントにまとめたり、複数のドキュメントに分けることができる。情報セキュリティプログラム計画書は、PM 管理策と、組織が定めた共通管理策について記述する。情報セキュリティプログラム計画書は、PM 管理策／共通管理策について十分な情報を提供する（「指定」ステートメントと「選択」ステートメントのパラメータの明示的な指定あるいは参照による指定を含む）。これにより、計画の意図に曖昧さを残さなずに準拠した実施が可能になり、計画が意図したとおりに実施された場合に生じるリスクの判断が可能になる。

個々の情報システムのセキュリティ計画と、組織全体にわたる情報セキュリティプログラム計画書の組み合わせは、組織に導入されているすべてのセキュリティ管理策を完全にカバーする。共通管理策は、通常は、組織の情報セキュリティプログラム計画書の付録に記載される。ただし、共通管理策が、情報システムの個別のセキュリティ計画書に含まれる場合（例：セキュリティ管理策が、組織全体にわたる境界保護を提供する侵入検知システムの一部として導入されていて、組織の単一の、あるいは複数の情報システムによって継承される場合）もある。組織全体にわたる情報セキュリティプログラム計画書は、共通管理策についての記述がどのセキュリティ計画書に含まれているかを示さなければならない。

組織には、共通管理策を単一のドキュメントに記載するか、あるいは複数のドキュメントに分けるかを選択できる柔軟性が与えられている。複数ドキュメントの場合、共通管理策について記載しているドキュメントは、情報セキュリティプログラム計画書に添付資料として含まれる。情報セキュリティプログラム計画書が複数のドキュメントを含む場合、組織は、各ドキュメント内にそれぞれの共通管理策について策定・導入・評価・認可・モニタリングする責任を負う職員が誰であるのかを明記する。たとえば、PE ファミリの「物理面と環境面での保護」に関するセキュリティ管理策が、特定の情報システムに対応するのではなく複数のシステムを支援する場合、組織が Facilities Management Office（施設管理局）に対して、それらの管理策について策定・導入・アセスメント・認可を要求することとともに、それらの管理策の継続的なモニタリングを要求することが考えられる。関連するセキュリティ管理策は、PM-8

拡張管理策：なし

参考文献：なし

PM-2　上級情報セキュリティ責任者

セキュリティ管理策：組織は、上級情報セキュリティ責任者を任命して、組織全体にわたる情報セキュリティプログラムの調整・開発・導入・維持管理に必要なミッションとリソースを与える。

補足的ガイダンス：このセキュリティ管理策に記載されている上級情報セキュリティ責任者は、組織の職員である。（該当する連邦法・大統領命令・指令・政策・規制に定義されているように）連邦政府機関では、この役職のことを「政府機関の上級情報セキュリティ責任者」と呼んでいる。組織によっては、この役職を「上級情報セキュリティ責任者」または「最高情報セキュリティ責任者」と呼んでいる。

拡張管理策：なし

参考文献：なし

PM-3　情報セキュリティリソース

セキュリティ管理策：組織は、

a. すべての資本計画と投資要請に、情報セキュリティプログラムの実施に必要なリソースが含まれるようにして、この要件に対するすべての例外を文書化するとともに、
b. ビジネスケース/Exhibit 300/Exhibit 53 を使用して、必要なリソースを記録するのに加えて、
c. 計画通りに、利用できる情報セキュリティリソースを確保する。

補足的ガイダンス：組織は、情報セキュリティへの取組に関して優秀な人材を育てることを検討し、必要なリソースを確保するために、必要に応じて専門分野別の専門家とリソースを割り当てる。組織は、資本計画や投資管理プロセスの情報セキュリティ関連の側面を管理・モニタリングする Investment Review Board（または類似のグループ）を指定し、権限を与えてもよい。関連するセキュリティ管理策は、PM-4・SA-2

拡張管理策：なし

参考文献：NIST Special Publication 800-65

PM-4　行動計画およびマイルストーンプロセス

セキュリティ管理策：組織は、

a. セキュリティプログラムの行動計画とマイルストーン、そして関連する情報システムが以下を満たすようにするためのプロセスを実施する：
    1. 策定され、維持管理される
    2. 組織の業務と資産、個人、他の組織、および国家に対するリスクに適切に対処するための、情報セキュリティの是正措置について文書化する
    3. OMB の FISMA 報告要件に従って、報告される。
b. 行動計画およびマイルストーンをレビューして、レビューして、組織のリスクマネジメント戦略と、リスク対応のためのアクションの組織全体にわたる優先順位に適合しているかどうかを確認する。

補足的ガイダンス：行動計画およびマイルストーンは、情報セキュリティプログラムの重要なドキュメントであり、OMB が規定する連邦報告要件の対象である。リスクマネジメント階層（すなわち、組織、ミッション／業務プロセス、および情報システム）内の 3 つのすべての層にわたる、組織全体にわたるリスク管理がますます強調されるようになっていることから、組織は行動計画とマイルストーンを組織的視点からとらえて、リスク軽減措置の優先順位付けを行い、行動計画とマイルストーンが組織の目標と目的に確実に適合するようにする。行動計画とマイルストーンの更新は、セキュリティ管理策アセスメントの結果および継続的モニタリング活動に基づいて実施

される。OMB の FISMA 報告に関するガイダンスは、組織の行動計画とマイルストーンに関する手引きを含む。関連するセキュリティ管理策は、CA-5。

拡張管理策：なし

参考文献：OMB Memorandum 02-01・NIST Special Publication 800-37

PM-5　情報システム一覧

セキュリティ管理策：組織は、組織の情報システムの一覧を作成し、維持管理する。

補足的ガイダンス：この管理策は、FISMAの一覧要件に対処する。OMBは、情報システム一覧の作成と、関連する報告要件に関する手引きを提供している。情報システム一覧の作成と報告要件に関しては、組織はOMB発行の年次FISMA報告ガイダンスを参照のこと。

拡張管理策：なし

参考文献：ウェブサイト http://www.omb.gov

PM-6　情報セキュリティパフォーマンスの測定

セキュリティ管理策：組織は、情報セキュリティパフォーマンスの測定方法を策定し、パフォーマンスをモニタリングし、測定結果を報告する。

補足的ガイダンス：パフォーマンスの測定は、成果に基づいたメトリクスを用いて行われる。この測定は、情報セキュリティプログラムと、プログラムを支援するために導入されているセキュリティ管理策の有効性または効率性の測定に使用される。

拡張管理策：なし

参考文献：NIST Special Publication 800-55

PM-7　エンタープライズアーキテクチャ

管理策：組織は、情報セキュリティと、結果として（組織の）業務・（組織の）資産・個人・他組織・国家にもたらされるリスクを考慮して、エンタープライズアーキテクチャを策定する。

補足的ガイダンス：組織が策定するエンタープライズアーキテクチャは、連邦エンタープライズアーキテクチャに準拠するよう調整される。情報セキュリティ要求事項および関連するセキュリティ管理策を組織のエンタープライズアーキテクチャに組み入れることは、システム開発ライフサイクルの早い段階でのセキュリティ考慮事項への対応を支援する。また、このような取組は組織のミッション／業務プロセスに直接的に、かつ明示的に関連する。セキュリティ要求事項を組み入れるためのこのプロセスは、組織のリスクマネジメント戦略と情報セキュリティ 戦略に適合する、必要不可欠な情報セキュリティアーキテクチャである、エンタープライズアーキテクチャにも組み入れられる。PM-7 の場合、情報セキュリティアーキテクチャは、「複数のシステムのうちの1つのシステム」レベル（組織全体にわたる）で策定される（すなわち、組織のすべての情報システムを代表する形）。PL-8 の場合、情報セキュリティアーキテクチャは、個々の情報システムを代表するレベルで策定されるが、同時に、組織向けに定義された情報セキュリティアーキテクチャにも適合する。セキュリティ要求事項とセキュリティ管理策の組み入れを最も効果的に実施するには、リスクマネジメントフレームワークが不可欠であるだけではなく、フレームワークを支援するセキュリティ標準およびガイドラインの適用が必須となる。Federal Segment Architecture Methodology は、情報セキュリティ要求事項およびセキュリティ管理策の双方をエンタープライズアーキテクチャに組み入れるに関する手引きである。関連するセキュリティ管理策は、PL-2・PL-8・PM-11・RA-2・SA-3。

拡張管理策：なし

参考文献：NIST Special Publication 800-39

PM-8　重要インフラ計画

セキュリティ管理策：組織は、「重要インフラと重要リソースを保護するための計画」の作成、文書化、更新における情報セキュリティ問題に対処する。

補足的ガイダンス：保護戦略は、重要資産と重要リソースの優先順位付けに基づく。重要インフラと重要リソースを定義し、関連する重要インフラ保護計画を作成するための要件と手引きは、該当する連邦法・大統領命令・指令・政策・規制・標準・指針に記載されている。関連するセキュリティ管理策は、PM-1・PM-9・PM-11・RA-3

拡張管理策：なし

参考文献：HSPD 7・National Infrastructure Protection Plan

PM-9　リスクマネジメント戦略

セキュリティ管理策：組織は、

a. 情報システムの運用と使用により生じる組織の業務と資産、個人、他の組織、および国家に対するリスクを管理するための、包括的な戦略を策定するとともに、
b. リスクマネジメント戦略を組織全体にわたって一貫性が保たれるように実施するのに加えて、
c. リスクマネジメント戦略を［指定：組織が定めた頻度で］、あるいは組織的変化に対処するために必要な場合にレビューし、更新する。

補足的ガイダンス：組織全体にわたるリスクマネジメント戦略は、例えば、組織のリスク許容度を明確に表現すること、受け入れられるリスクアセスメント方法、リスク緩和戦略、組織のリスク許容度と照らし合わせて、組織全体にわたってリスクを一貫して評価するためのプロセス、長期にわたってリスクをモニタリングするためのアプローチを含む。リスクエグゼクティブ機能の使用は、リスクマネジメント戦略の一貫した組織全体にわたる適用を容易にする。組織全体にわたるリスクマネジメント戦略は、組織にとって内外の他の情報源からのリスク関連情報をベースに策定してもよい。そうした場合には、リスクマネジメント戦略が広範囲にわたる包括的なものとなる。関連する管理策は、RA-3。

拡張管理策：なし

参考文献：NIST Special Publications 800-30・NIST Special Publications 800-39

PM-10　セキュリティ認可プロセス

セキュリティ管理策：組織は、

a. 組織の情報システムと、それらのシステムが稼働する環境のセキュリティ状態をセキュリティ認可プロセス全体を通して管理する（すなわち、文書化、追跡、および報告）とともに、
b. 組織のリスクマネジメントプロセス内の特定の役割と責任を担う個人を指定するのに加えて、
c. セキュリティ認可プロセスを組織全体にわたるリスクマネジメントプログラムに完全に組み入れる。

補足的ガイダンス：情報システムと運用環境のセキュリティ認可プロセスは、組織全体にわたるリスクマネジメントプロセスであるリスクマネジメントフレームワーク、および関連するセキュリティ標準とガイドラインの適用を必要とする。リスクマネジメントプロセス内の役割には、組織のリスクエグゼクティブ（機能）、それぞれの情報システムに指定された運用認可責任者、共通管理策の提供者を含む。セキュリティ認可プロセスは、組織の業務と資産、個人、他の組織、および

国家に対するリスクを把握し、受け入れるのを容易にするために、組織の継続的なモニタリングに組み入れられる。関連する管理策は、CA-6。

拡張管理策：なし

参考文献：NIST Special Publications 800-37・NIST Special Publications 800-39

PM-11 ミッション / 業務プロセスの定義

管理策：組織は、

a. 情報セキュリティと、結果として組織の業務、組織の資産、個人、他の組織、および国家にもたらされるリスクを考慮して、ミッション／業務プロセスを定義するとともに、

b. 定義されたッション／業務プロセスから生じる情報保護ニーズを特定して、達成可能な保護ニーズが得られるまでプロセスを修正する。

補足的ガイダンス：情報保護ニーズは、情報の侵害（機密性、完全性、または、可用性の喪失）が組織、個人、または国家にもたらす脅威に対抗するための、テクノロジーに依存しない必要な機能である。情報保護ニーズは、組織が定めるミッション／業務ニーズ、それらのニーズを満たすために選択されたミッション／業務プロセス、および組織のリスクマネジメント戦略から導出される。情報保護ニーズにより、組織にとって必要なセキュリティ管理策と、ミッション／業務プロセスを支援する関連情報システムが特定される。情報保護ニーズを定義する際には、情報の侵害が発生した場合の負の影響のレベルを把握する必要がある。セキュリティ分類プロセスは、そうした潜在的影響の判断に使用される。ミッション／業務プロセスの定義と、関連する情報保護に関する要求事項は、組織が組織のポリシーと手順に従って、組織によって文書化される。関連する管理策は、PM-7・PM-8・RA-2。

拡張管理策：なし

参考文献：FIPS Publication 199・NIST Special Publication 800-60

PM-12 インサイダー脅威に対する対策

セキュリティ管理策：組織は、複数の部門から選出された、インサイダー脅威に対するインシデント対応チームを含むインサイダー脅威によるインシデント対策を実施する。

補足的ガイダンス：機密情報を扱う組織は、大統領命令 13587 および National Policy on Insider Threat に従って、インサイダー脅威に対する対策を考案することが求められる。機密環境における、インサイダー脅威に対する対策に適用される標準およびガイドラインは、国家安全保障にかかわらないシステム内の CUI（管理されている、非機密扱いの情報）のセキュリティを高めるために使用することもできる。インサイダー脅威に対する対策は、インサイダー脅威関連の問題を特定するための技術情報と非技術情報の両方を一元的にまとめて、分析することによって、内部関係者による悪意のある活動を検知・防止するためのセキュリティ管理策を含む。組織の上級職員は、対策の実施とモニタリングに責任のある個人として、部門／政府機関の長によって任命される。一元的な組み入れと分析機能に加えて、インサイダー脅威に対する対策では少なくとも、部門／政府機関のインサイダー脅威に関するポリシーと実施計画を用意し、政府所有の機密扱いのコンピュータ上のそれぞれの職員をホストベースでモニタリングし、職員に対してインサイダー脅威に対する意識向上トレーニングを実施し、インサイダー脅威に対する分析を目的として部門／政府機関内のすべてのオフィス（例：人材・法律・物理的セキュリティ・情報技術・情報システムセキュリティに加えて、法執行職員によるセキュリティ）からの情報にアクセスできるようにし、部門／政府機関のインサイダー脅威に対する耐性の自己アセスメントを実施する。

インサイダー脅威に対する対策では、たとえばコンピュータセキュリティインシデント対応チームなど、すでに存在する可能性のあるインシデント対応チームの存在を活用できる。人材に関す

る記録は、この取組において、特に重要になる。なぜならば、そうした記録は、なんらかのタイプの内部犯罪が職場における非技術的な振る舞いによって発生した場合に、有力な証拠となるからである（例：不満を抱いている職員による振る舞い、あるいは同僚との衝突した職員による振る舞いの現行のパターン）。これらの前兆が、モニタリングに携わる組織の職員に情報を与えて、より的を絞った標的型のモニタリング活動を可能にする。法律チームによる参加は、すべてのモニタリング活動が、該当する法律・指令・政策・規制・標準・ガイドラインに従って実施されるようにするためにも、重要である。関連する管理策は、AC-6・AT-2・AU-6・AU-7- AU-10・AU-12・AU-13・CA-7・IA-4・IR-4・MP-7・PE-2・PS-3・PS-4・PS-5・PS-8・SC-7・SC-38・SI-4・PM-1・PM-14。

拡張管理策：なし

参考文献：Executive Order 13587

PM-13 情報セキュリティ要員

管理策：組織は、情報セキュリティ要員の育成とレベル向上のためのプログラムを作成する。

補足的ガイダンス：情報セキュリティ要員の育成とレベル向上のためのプログラムは、たとえば以下を含む：①情報セキュリティ上の職務とタスクの遂行に必要な知識とスキルレベルを定義すること②情報セキュリティ上の役割と責任を割り当てられた個人に対する役割ベースのトレーニングプログラムを用意することならびに③情報セキュリティ関連の職務に就いている者と、そうした職務の志願者の適正を評価して、育てること。そうした要員育成プログラムは、以下を促進するための情報セキュリティキャリアパスを含む：①情報セキュリティの専門化がその分野で昇進し、より大きな責任を担う職務に就くことならびに②組織が情報セキュリティ関連の職務を資格のある職員で埋めること。情報セキュリティ要員の育成とレベル向上のためのプログラムは、組織の「セキュリティ意識向上およびトレーニングプログラム」を補完する。情報セキュリティ要員の育成と レベル向上のためのプログラムは、組織の業務、資産、および職員を保護するために選ばれた職員の、重要な情報セキュリティ能力を育成し、制度化することに焦点を当てる。関連する管理策は、AT-2・AT-3。

拡張管理策：なし

参考文献：なし

PM-14 テスト、トレーニング、およびモニタリング

セキュリティ管理策：組織は、

a. 組織の情報システムに関連するセキュリティテスト、トレーニング、およびモニタリング活動が以下を満たすようにするためのプロセスを実施する：
    1. 策定され、維持管理される
    2. 引き続き、タイムリーに実施される
b. テスト、トレーニング、およびモニタリング計画をレビューして、組織のリスクマネジメント戦略と、リスク対応のためのアクションの組織全体にわたる優先順位に適合しているかどうかを確認する。

補足的ガイダンス：この管理策は、組織全体にわたって実施されるセキュリティテスト、トレーニング、およびモニタリング活動に対するモニタリングが行われることと、そうした活動が調整されることを確実にする。継続的モニタリングプログラム、リスクマネジメント階層の 3 つの層にわたる情報セキュリティ の実施、および共通管理策の広範な使用が重要であることから、組織は、さまざまなセキュリティ管理策を支援する継続的なアセスメントの一貫として日常的に実施される活動の、テストとモニタリングを調整し、強化する。セキュリティテストトレーニング活動では、通常は個々の情報システムや特定の役割に焦点が当てられるが、組織内のすべてのエンティティ

（部署、グループ、人）間の調整が必要となる。テスト、トレーニング、およびモニタリングの計画と活動は、脅威と脆弱性の最新のアセスメント結果に基づいて計画・実施される。関連する管理策は、AT-3・CA-7・CP-4・IR-3・SI-4。

拡張管理策：なし

参考文献：NIST Special Publications 800-16・NIST Special Publications 800-37・NIST Special Publications 800-53A・NIST Special Publications 800-137

PM-15 セキュリティグループやセキュリティ団体と連絡を取り合う

セキュリティ管理策：組織は、以下を目的として、セキュリティコミュニティ内の選択されたグループや団体との連絡を確立し、開始する。

a. 組織の職員に対する、継続的なセキュリティ教育とトレーニングを容易にする

b. 推奨されるセキュリティプラクティス、技法、テクノロジーについて情報を得る

c. 脅威、脆弱性、インシデントを含む、セキュリティ関連の最新情報を共有する。

補足的ガイダンス：セキュリティグループやセキュリティ団体と継続的に連絡を取り合うことは、テクノロジーと脅威が急速に変化する環境では最も重要である。セキュリティグループやセキュリティ団体には、例えば、特別利益団体、フォーラム、専門職協会、ニュースグループ、および／または類似の組織内のセキュリティ専門家で構成されるピアグループがある。組織は、組織のミッション／業務機能に基づいて、グループや団体を選択する。組織は、該当する連邦法・大統領命令・指令・政策・規制・標準・指針に従って、脅威・脆弱性、インシデントに関する情報を共有する。関連する管理策は、SI-5。

拡張管理策：なし

参考文献：なし

PM-16 脅威意識向上のためのプログラム

管理策：組織は、脅威意識向上のためのプログラム（組織を跨ぐ情報共有機能を含む）を実施する。

補足的ガイダンス：特に APT(advanced persistent threat) など、敵対者の手法が絶えず変化し、高度化するにつれて、敵対者が組織の情報システムの侵害または侵入に成功する可能性が高まっている。この問題に対処するための最良の技法の 1 つに、組織間で脅威情報を共有することがある。これは、例えば、組織が経験した脅威イベント（すなわち、戦術・技術・手順）や、特定のタイプの脅威に対して有効であることが判明した軽減策、脅威に関して入手した情報（すなわち、発生する可能性が高い脅威の兆候や、そうした脅威についての警告）を共有することを含む。脅威情報の共有は、二者間（例：政府と営利団体との連携、政府間の連携）で行われたり、より多くの組織間（例：脅威共有コンソーシアムに参加している組織）で行われたりする。脅威情報は、特殊な合意と保護を必要とする程、機密性が高い場合もあれば、機密性は高くなく、自由に共有される場合もある。なお、関連する管理策は、PM-12・PM-16。

拡張管理策：なし

参考文献：なし

1

付録 H

国際的なセキュリティ標準

この文書のセキュリティ管理策と、ISO/IEC 27001 および 15408 との対応

この付録に記載されているマッピングテーブルは、ISO/IEC 27001（題名：*"Information technology–Security techniques–Information security management systems–Requirements"*[113]）および ISO/IEC 15408（題名：*"Information technology -- Security techniques -- Evaluation criteria for IT security"*[114]）との関連でこの文書に記載されたセキュリティ管理策が通常適用される範囲について示した図表である。ISO/IEC 27001 は、あらゆるタイプの組織に適用されるものであり、ビジネスリスクという脈絡の中で、文書化された ISMS（情報セキュリティマネジメントシステム）の確立、導入、運用、モニタリング、レビュー、維持管理、および改善のための要求事項を規定している。NIST Special Publication 800-39 は、組織レベル、ミッション／業務プロセスレベル、および情報システムレベルでのリスクの管理に関する手引きを含んでおり、ISO/IEC 27001 との一貫性があり、連邦政府および受託業者向けの追加の実施詳細を示している。ISO/IEC 15408（「Common Criteria（コモンクライテリア）」としても知られている）は、情報システムや情報システムコンポーネント（すなわち、IT 製品）の開発者に対する機能要件と保証要件を規定するものである。付録 F の技術面でのセキュリティ管理策の多くは情報システムのハードウェアコンポーネント、ソフトウェアコンポーネント、およびファームウェアコンポーネント上で実施されるため、組織は ISO/IEC 15408 の要求事項に照らし合わせて評価された IT 製品を調達し、使用することが可能になり、組織にとって大きなメリットとなるだろう。そうした製品は、特定のセキュリティ管理策が正しく導入され、意図したとおりに運用され、システムのセキュリティ要求事項に対する適合性の観点から所望の結果を産出していることに関して証拠を提供する。

ISO/IEC 27001 との関連について記載された当初のマッピングテーブルは、この文書に記載された（セキュリティ管理策の）ベースライン管理策によって一義的に保護される対象を ISO/IEC 27001 の標準によって一義的に保護される対象と比較した結果について作成された図表である。また、このマッピングテーブルは、同等のセキュリティ管理策の要求事項を比較した図表である前に、セキュリティ管理策の相関関係を記載した図表である。

なお、この文書に記載されたセキュリティ管理策（または、ISO/IEC 27001 に記載された管理策としてマッピングされた管理策）は、2013 年に行われた ISO/IEC 27001 の改訂作業のなかで、ISO/IEC 27001 に記載された管理策としてマッピングされた管理策の趣旨に沿って（または、この文書に記載されたセキュリティ管理策の趣旨に沿って）実装されるのかどうかについて改めて評価された。

マッピング条件を満たすことができるようになるためには、マッピングされた管理策を実装することによって、マッピングされていない管理策を実装する場合と同等のセキュリティが担保されなければならない。ただし、そのことは、ある複数のセキュリティ管理策を組織がもっぱらこの文書に記載されたマッピングテーブルの内容によって同等のセキュリティを担保する管理策であると見なすということを意味するものではない。また、当初のマッピングテーブルから更新された図表は、マッピングテーブルとしてより正確な図表である一方、セキュリティ管理策の相

[113] ISO/IEC 27001 は、2005 年 10 月に ISO/IEC によって発行された。

[114] ISO/IEC 15408 は、2012 年 9 月に ISO/IEC によって発行された。

関関係として当該マッピングテーブルに表示された関係が常に一対一の対等な関係になるとは限らないため、若干主観によるマッピングテーブルであることを免れない。

マッピングを行うにあたっての課題とは、たとえば、

①この文書に記載された「contingency planning（緊急時対応計画）」と ISO/IEC 27001 の「business continuity（事業継続マネジメント）」は、全く同じではないが、類似の機能を有すると判断された

②2 つのセキュリティ管理策が類似のトピックを扱っているものの、状況・視点・コープのいずれかが異なるといったケースもある。情報フロー制御に関しては、Special Publication 800-53 ではソースオブジェクトとデスティネーションオブジェクトとの間のアクセスを、承認された権限をもって制御するといった広い意味で扱っているのに対し、ISO/IEC 27001 では相互接続されているネットワークドメインを制御するといった、より狭い意味で扱っている。表 H-2 は、逆の対応、すなわち、ISO/IEC 27001 のセキュリティ管理策側からの、Special Publication 800-53 のセキュリティ管理策への対応を示している

③ISO/IEC 27001 に記載されているセキュリティ管理策のうち情報セキュリティが果たす（または果たすべき）役割に関する A6.1.1 の管理策が「情報セキュリティが果たすべき役割を完全に定義・割り当てなければならない」という内容で策定されている一方、この文書に記載されているセキュリティ管理策のうち当該 A6.1.1 の管理策との相関関係がマッピングテーブルに記載されている管理策としてのセキュリティ認可のプロセスに関する PM-10 の管理策は 3 つの管理策から構成される管理策である

といった場合を指す。なお、この文書に記載された PM-10 のセキュリティ管理策を構成する 3 つの管理策のうち 1 つ目の管理策は「特定の役割を果たすことができるよう（組織が）特定の個人を割り当てる」という管理策であり、何ら情報が追加されないまま当該 PM-10 の管理策が上記 A6.1.1 の管理策の関連管理策となる場合、上記 A6.1.1 の管理策を実装しさえすれば当該 PM-10 の管理策によって保護される対象のセキュリティが完全に担保される（すなわち、役割が完全に定義・割り当てられる）ものと組織が誤認する可能性がある（ただし、当該 PM-10 の管理策を構成する 3 つの管理策のうち上記以外の残りの 2 つの管理策が策定されている場合を除く）ため、下記の表 H-1 および H-2 のそれぞれの内容が当該図表の向かって左側に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な内容である場合、当該図表の向って右側に記載された管理策には「*」の記号が添えられている。

なお、ISO/IEC 27001 に記載されたセキュリティ管理策の中には、この文書に記載されたセキュリティ管理策の拡張管理策にのみ相互に関係する場合がある。この場合においては、ISO/IEC 27001 に記載されたセキュリティ管理策は、ベースライン管理策によって保護される対象のセキュリティを担保する管理策ではなく、特定の拡張管理策によって保護される対象のセキュリティのみを担保する管理策であることから、当該拡張管理策は H-2 の表に列挙されている。また、セキュリティ管理策の拡張管理策が 1 つも策定されていない場合、ISO/IEC 27001 に記載されたセキュリティ管理策は、この文書に記載されたベースライン管理策によって保護される対象のセキュリティのみを保護する管理策となる。また、ISO/IEC 27002 に記載されたセキュリティ管理策は、基準である前に情報であることから、マッピング対象の管理策ではない。

下記の表 H-1 は、この文書に記載されたセキュリティ管理策と ISO/IEC 27001 に記載されたセキュリティ管理策との関連について、この文書に記載されたセキュリティ管理策の観点から記載されたマッピングテーブルである。当該マッピングテーブルは、この付録の冒頭に記載された導入部分の説明を参照のうえ利用されなければならない。

3

表 H-1:NIST SP 800-53 側からの ISO/IEC 27001 への対応

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
AC-1	アクセス制御のポリシーおよび手順	A.5.1.1・A.5.1.2・A.6.1.1・A.9.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
AC-2	アカウント管理	A.9.2.1・A.9.2.2・A.9.2.3・A.9.2.5・A.9.2.6のそれぞれに記載されたセキュリティ管理策
AC-3	アクセス制御の実施	A.6.2.2・A.9.1.2・A.9.4.1・A.9.4.4・A.9.4.5・A.13.1.1・A.14.1.2・A.14.1.3・A.18.1.3のそれぞれに記載されたセキュリティ管理策
AC-4	情報フロー制御の実施	A.13.1.3・A.13.2.1・A.14.1.2・A.14.1.3のそれぞれに記載されたセキュリティ管理策
AC-5	職務の分離	A.6.1.2のそれぞれに記載されたセキュリティ管理策
AC-6	最小権限	A.9.1.2・A.9.2.3・A.9.4.4・A.9.4.5のそれぞれに記載されたセキュリティ管理策
AC-7	ログオン試行の失敗	A.9.4.2に記載されたセキュリティ管理策
AC-8	システムの利用に関する通知	A.9.4.2に記載されたセキュリティ管理策
AC-9	前回のログオン(アクセス)に関する通知	A.9.4.2に記載されたセキュリティ管理策
AC-10	同時セッションの制御	(対応するものがない)
AC-11	セッションのロック	A.11.2.8・A.11.2.9のそれぞれに記載されたセキュリティ管理策
AC-12	セッションの終了	(対応するものがない)
AC-13	**(削除された)**	---
AC-14	識別または認証を必要としないアクション	(対応するものがない)
AC-15	**(削除された)**	---
AC-16	セキュリティ属性	(対応するものがない)
AC-17	リモートアクセス	A.6.2.1・A.6.2.2・A.13.1.1・A.13.2.1・A.14.1.2のそれぞれに記載されたセキュリティ管理策
AC-18	ワイヤレスアクセス	A.6.2.1・A.13.1.1・A.13.2.1 のそれぞれに記載されたセキュリティ管理策
AC-19	携帯機器に対するアクセス制御	A.6.2.1・A.11.2.6・A.13.2.1のそれぞれに記載されたセキュリティ管理策
AC-20	外部情報システムの使用	A.11.2.6・A.13.1.1・A.13.2.1のそれぞれに記載されたセキュリティ管理策
AC-21	情報共有	(対応するものがない)
AC-22	一般の人がアクセスできるコンテンツ	(対応するものがない)
AC-23	データマイニングからの保護	(対応するものがない)
AC-24	アクセス制御に関する決定	A.9.4.1*に記載されたセキュリティ管理策
AC-25	リファレンスモニタ	(対応するものがない)
AT-1	セキュリティ意識向上およびトレーニングのポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
AT-2	セキュリティ意識向上トレーニング	A.7.2.2・A.12.2.1のそれぞれに記載されたセキュリティ管理策
AT-3	役割に基づいたセキュリティトレーニング	A.7.2.2*に記載されたセキュリティ管理策
AT-4	セキュリティトレーニング記録	(対応するものがない)
AT-5	**(削除された)**	---
AU-1	監査および説明責任のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
AU-2	監査イベント	(対応するものがない)

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
AU-3	監査記録の内容	A.12.4.1*に記載されたセキュリティ管理策
AU-4	監査記録の記憶容量	A.12.1.3に記載されたセキュリティ管理策
AU-5	監査処理が失敗した時の対応	（対応するものがない）
AU-6	監査記録のレビュー、分析、報告	A.12.4.1・A.16.1.2・A.16.1.4のそれぞれに記載されたセキュリティ管理策
AU-7	監査量削減と報告書自動作成	（対応するものがない）
AU-8	タイムスタンプ	A.12.4.4に記載されたセキュリティ管理策
AU-9	監査情報の保護	A.12.4.2・A.12.4.3・A.18.1.3のそれぞれに記載されたセキュリティ管理策
AU-10	否認防止	（対応するものがない）
AU-11	監査記録の保管	A.12.4.1・A.16.1.7のそれぞれに記載されたセキュリティ管理策
AU-12	監査記録の生成	A.12.4.1・A.12.4.3のそれぞれに記載されたセキュリティ管理策
AU-13	情報開示のモニタリング	（対応するものがない）
AU-14	セッションの監査	A.12.4.1*に記載されたセキュリティ管理策
AU-15	代替監査機能	（対応するものがない）
AU-16	組織を跨る監査	（対応するものがない）
CA-1	セキュリティアセスメントおよび認可のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
CA-2	セキュリティアセスメント	A.14.2.8・A.18.2.2・A.18.2.3のそれぞれに記載されたセキュリティ管理策
CA-3	システムの相互接続	A.13.1.2・A.13.2.1・A.13.2.2のそれぞれに記載されたセキュリティ管理策
CA-4	（削除された）	---
CA-5	行動計画とマイルストーン	（対応するものがない）
CA-6	セキュリティ認可	（対応するものがない）
CA-7	継続的なモニタリング	（対応するものがない）
CA-8	侵入テスト	（対応するものがない）
CA-9	システムに対する内部接続	（対応するものがない）
CM-1	構成管理のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
CM-2	ベースライン構成	（対応するものがない）
CM-3	構成変更管理	A.12.1.2・A.14.2.2・A.14.2.3・A.14.2.4のそれぞれに記載されたセキュリティ管理策
CM-4	セキュリティ影響分析	A.14.2.3に記載されたセキュリティ管理策
CM-5	変更に対するアクセス制限	A.9.2.3・A.9.4.5・A.12.1.2・A.12.1.4・A.12.5.1のそれぞれに記載されたセキュリティ管理策
CM-6	設定項目	（対応するものがない）
CM-7	最小機能	A.12.5.1*に記載されたセキュリティ管理策
CM-8	情報システムコンポーネント一覧	A.8.1.1・A.8.1.2のそれぞれに記載されたセキュリティ管理策
CM-9	構成管理計画	A.6.1.1*に記載されたセキュリティ管理策
CM-10	ソフトウェアの使用制限	A.18.1.2に記載されたセキュリティ管理策
CM-11	ユーザによるソフトウェアのインストール	A.12.5.1・A.12.6.2のそれぞれに記載されたセキュリティ管理策
CP-1	緊急時対応計画のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
CP-2	緊急時対応計画	A.6.1.1・A.17.1.1・A.17.2.1のそれぞれに記載されたセキュリティ管理策

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
CP-3	緊急時対応トレーニング	A.7.2.2*に記載されたセキュリティ管理策
CP-4	緊急時対応計画のテスト	A.17.1.3に記載されたセキュリティ管理策
CP-5	（削除された）	---
CP-6	代替保管拠点	A.11.1.4・A.17.1.2・A.17.2.1のそれぞれに記載されたセキュリティ管理策
CP-7	代替処理拠点	A.11.1.4・A.17.1.2・A.17.2.1のそれぞれに記載されたセキュリティ管理策
CP-8	通信サービス	A.11.2.2・A.17.1.2のそれぞれに記載されたセキュリティ管理策
CP-9	情報システムのバックアップ	A.12.3.1・A.17.1.2・A.18.1.3のそれぞれに記載されたセキュリティ管理策
CP-10	情報システムの復旧と再構成	A.17.1.2に記載されたセキュリティ管理策
CP-11	代替通信プロトコル	A.17.1.2*に記載されたセキュリティ管理策
CP-12	セーフモード	（対応するものがない）
CP-13	代替のセキュリティメカニズム	A.17.1.2*に記載されたセキュリティ管理策
IA-1	識別および認証のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
IA-2	識別および認証（組織的ユーザ）	A.9.2.1に記載されたセキュリティ管理策
IA-3	デバイスの識別および認証	（対応するものがない）
IA-4	識別子の管理	A.9.2.1に記載されたセキュリティ管理策
IA-5	オーセンティケータの管理	A.9.2.1・A.9.2.4・A.9.3.1・A.9.4.3のそれぞれに記載されたセキュリティ管理策
IA-6	オーセンティケータのフィードバック	A.9.4.2に記載されたセキュリティ管理策
IA-7	暗号モジュールの認証	A.18.1.5に記載されたセキュリティ管理策
IA-8	識別および認証（組織的ユーザ以外のユーザ）	A.9.2.1に記載されたセキュリティ管理策
IA-9	サービスの識別および認証	（対応するものがない）
IA-10	適応性のある識別および認証	（対応するものがない）
IA-11	再認証	（対応するものがない）
IR-1	インシデント対応のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
IR-2	インシデント対応トレーニング	A.7.2.2*に記載されたセキュリティ管理策
IR-3	インシデント対応のテスト	（対応するものがない）
IR-4	インシデント対応	A.16.1.4・A.16.1.5・A.16.1.6のそれぞれに記載されたセキュリティ管理策
IR-5	インシデントモニタリング	（対応するものがない）
IR-6	インシデント報告	A.6.1.3・A.16.1.2のそれぞれに記載されたセキュリティ管理策
IR-7	インシデント対応の支援	（対応するものがない）
IR-8	インシデント対応計画	A.16.1.1に記載されたセキュリティ管理策
IR-9	情報流出対応	（対応するものがない）
IR-10	統合情報セキュリティ分析チーム	（対応するものがない）
MA-1	システムメンテナンスのポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
MA-2	管理されたメンテナンス	A.11.2.4*・A.11.2.5*のそれぞれに記載されたセキュリティ管理策
MA-3	メンテナンスツール	（対応するものがない）
MA-4	非局所的なメンテナンス	（対応するものがない）

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
MA-5	メンテナンス要員	（対応するものがない）
MA-6	タイムリーなメンテナンス	A.11.2.4に記載されたセキュリティ管理策
MP-1	媒体保護のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
MP-2	媒体に対するアクセス	A.8.2.3・A.8.3.1・A.11.2.9のそれぞれに記載されたセキュリティ管理策
MP-3	媒体のマーキング	A.8.2.2に記載されたセキュリティ管理策
MP-4	媒体の保管	A.8.2.3・A.8.3.1・A.11.2.9のそれぞれに記載されたセキュリティ管理策
MP-5	媒体の移動	A.8.2.3・A.8.3.1・A.8.3.3・A.11.2.5・A.11.2.6のそれぞれに記載されたセキュリティ管理策
MP-6	媒体の無害化	A.8.2.3・A.8.3.1・A.8.3.2・A.11.2.7のそれぞれに記載されたセキュリティ管理策
MP-7	媒体の使用	A.8.2.3・A.8.3.1のそれぞれに記載されたセキュリティ管理策
MP-8	媒体のダウングレード	（対応するものがない）
PE-1	物理面と環境面での保護のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
PE-2	物理アクセス権限	A.11.1.2*に記載されたセキュリティ管理策
PE-3	物理アクセス制御	A.11.1.1・A.11.1.2・A.11.1.3のそれぞれに記載されたセキュリティ管理策
PE-4	伝送媒体に対するアクセス制御	A.11.1.2・A.11.2.3のそれぞれに記載されたセキュリティ管理策
PE-5	出力装置に対するアクセス制御	A.11.1.2・A.11.1.3のそれぞれに記載されたセキュリティ管理策
PE-6	物理アクセスのモニタリング	（対応するものがない）
PE-7	（削除された）	---
PE-8	来客のアクセス記録	（対応するものがない）
PE-9	電力設備と電力ケーブル	A.11.1.4・A.11.2.1・A.11.2.2・A.11.2.3のそれぞれに記載されたセキュリティ管理策
PE-10	緊急遮断	A.11.2.2*に記載されたセキュリティ管理策
PE-11	非常用電源	A.11.2.2に記載されたセキュリティ管理策
PE-12	非常用照明	A.11.2.2*に記載されたセキュリティ管理策
PE-13	防火	A.11.1.4・A.11.2.1のそれぞれに記載されたセキュリティ管理策
PE-14	温度および湿度の管理	A.11.1.4, A.11.2.1, A.11.2.2のそれぞれに記載されたセキュリティ管理策
PE-15	浸水による被害からの保護	A.11.1.4・A.11.2.1・A.11.2.2のそれぞれに記載されたセキュリティ管理策
PE-16	搬入と搬出	A.8.2.3・A.11.1.6・A.11.2.5のそれぞれに記載されたセキュリティ管理策
PE-17	代替の仕事場	A.6.2.2・A.11.2.6・A.13.2.1のそれぞれに記載されたセキュリティ管理策
PE-18	情報システムコンポーネントの設置場所	A.8.2.3・A.11.1.4・A.11.2.1のそれぞれに記載されたセキュリティ管理策
PE-19	情報が漏れること	A.11.1.4・A.11.2.1のそれぞれに記載されたセキュリティ管理策
PE-20	資産のモニタリングと追跡	A.8.2.3*に記載されたセキュリティ管理策
PL-1	セキュリティ計画のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
PL-2	システムセキュリティ計画	A.14.1.1に記載されたセキュリティ管理策

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
PL-3	**(削除された)**	---
PL-4	行動規範	A.7.1.2・A.7.2.1・A.8.1.3のそれぞれに記載されたセキュリティ管理策
PL-5	**(削除された)**	---
PL-6	**(削除された)**	---
PL-7	運用におけるセキュリティ概念	A.14.1.1*に記載されたセキュリティ管理策
PL-8	情報セキュリティアーキテクチャ	A.14.1.1*に記載されたセキュリティ管理策
PL-9	一元的管理	(対応するものがない)
PS-1	職員によるセキュリティのポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
PS-2	役職ごとのリスク記号	(対応するものがない)
PS-3	職員の審査	A.7.1.1に記載されたセキュリティ管理策
PS-4	職員の雇用の終了	A.7.3.1・A.8.1.4のそれぞれに記載されたセキュリティ管理策
PS-5	職員の異動	A.7.3.1・A.8.1.4のそれぞれに記載されたセキュリティ管理策
PS-6	アクセス契約	A.7.1.2・A.7.2.1・A.13.2.4のそれぞれに記載されたセキュリティ管理策
PS-7	第三者職員によるセキュリティ	A.6.1.1*・A.7.2.1*のそれぞれに記載されたセキュリティ管理策
PS-8	職員に対する制裁	A.7.2.3に記載されたセキュリティ管理策
RA-1	リスクアセスメントのポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
RA-2	セキュリティカテゴリ	A.8.2.1に記載されたセキュリティ管理策
RA-3	リスクアセスメント	A.12.6.1*に記載されたセキュリティ管理策
RA-4	**(削除された)**	---
RA-5	脆弱性スキャン	A.12.6.1*に記載されたセキュリティ管理策
RA-6	科学的情報収集対策に関する調査	(対応するものがない)
SA-1	システムおよびサービスの調達のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
SA-2	リソースの割り当て	(対応するものがない)
SA-3	システム開発ライフサイクル	A.6.1.1・A.6.1.5・A.14.1.1・A.14.2.1・A.14.2.6のそれぞれに記載されたセキュリティ管理策
SA-4	調達プロセス	A.14.1.1・A.14.2.7・A.14.2.9・A.15.1.2のそれぞれに記載されたセキュリティ管理策
SA-5	情報システム文書	A.12.1.1*に記載されたセキュリティ管理策
SA-6	**(削除された)**	---
SA-7	**(削除された)**	---
SA-8	セキュリティエンジニアリング原則	A.14.2.5に記載されたセキュリティ管理策
SA-9	外部情報システムサービス	A.6.1.1・A.6.1.5・A.7.2.1・A.13.1.2・A.13.2.2・A.15.2.1・A.15.2.2のそれぞれに記載されたセキュリティ管理策
SA-10	開発者による構成管理	A.12.1.2・A.14.2.2・A.14.2.4・A.14.2.7のそれぞれに記載されたセキュリティ管理策
SA-11	開発者によるセキュリティテストおよび評価	A.14.2.7・A.14.2.8のそれぞれに記載されたセキュリティ管理策
SA-12	サプライチェーンの保護	A.14.2.7・A.15.1.1・A.15.1.2・A.15.1.3のそれぞれに記載されたセキュリティ管理策
SA-13	信用性	(対応するものがない)
SA-14	クリティカリティ分析	(対応するものがない)
SA-15	開発プロセス、標準、およびツール	A.6.1.5・A.14.2.1のそれぞれに記載されたセキュリティ管理策

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
SA-16	開発者が提供する訓練	（対応するものがない）
SA-17	開発者によるセキュリティアーキテクチャおよび設計	A.14.2.1・A.14.2.5のそれぞれに記載されたセキュリティ管理策
SA-18	改ざんの防止と検知	（対応するものがない）
SA-19	コンポーネントの真正性	（対応するものがない）
SA-20	重要なコンポーネントの受託開発	（対応するものがない）
SA-21	開発者に対する審査	A.7.1.1に記載されたセキュリティ管理策
SA-22	サポートが得られないシステムコンポーネント	（対応するものがない）
SC-1	システムおよび通信の保護のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
SC-2	アプリケーションの分割	（対応するものがない）
SC-3	セキュリティ機能の分離	（対応するものがない）
SC-4	共有リソース内の情報	（対応するものがない）
SC-5	サービス妨害からの保護	（対応するものがない）
SC-6	リソースの可用性	（対応するものがない）
SC-7	境界保護	A.13.1.1・A.13.1.3・A.13.2.1・A.14.1.3のそれぞれに記載されたセキュリティ管理策
SC-8	伝送される情報の機密性と完全性	A.8.2.3・A.13.1.1・A.13.2.1・A.13.2.3・A.14.1.2・A.14.1.3のそれぞれに記載されたセキュリティ管理策
SC-9	**（削除された）**	---
SC-10	ネットワークの切断	A.13.1.1に記載されたセキュリティ管理策
SC-11	高信頼パス	（対応するものがない）
SC-12	暗号鍵の作成と管理	A.10.1.2
SC-13	暗号化による保護	A.10.1.1・A.14.1.2・A.14.1.3・A.18.1.5のそれぞれに記載されたセキュリティ管理策
SC-14	**（削除された）**	---
SC-15	連携するコンピュータデバイス	A.13.2.1*に記載されたセキュリティ管理策
SC-16	セキュリティ属性の伝送	（対応するものがない）
SC-17	PKI 証明書	A.10.1.2に記載されたセキュリティ管理策
SC-18	モバイルコード	（対応するものがない）
SC-19	ボイスオーバーインターネットプロトコル	（対応するものがない）
SC-20	セキュアな名前／アドレス解決サービス（信頼できるソース）	（対応するものがない）
SC-21	セキュアな名前／アドレス解決サービス(再帰的な問合わせを行うリゾルバ／キャッシングリゾルバ)	（対応するものがない）
SC-22	名前／アドレス解決サービスの構成およびサービスの提供	（対応するものがない）
SC-23	セッションの真正性	（対応するものがない）
SC-24	既知の状態に陥ること	（対応するものがない）
SC-25	薄いノード	（対応するものがない）
SC-26	ハニーポット	（対応するものがない）
SC-27	プラットフォームに依存しないアプリケーション	（対応するものがない）
SC-28	保存されている情報の保護	A.8.2.3*に記載されたセキュリティ管理策

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
SC-29	異種性	（対応するものがない）
SC-30	隠匿、および誤った方向に向けること	（対応するものがない）
SC-31	隠れチャネル分析	（対応するものがない）
SC-32	情報システムの分割	（対応するものがない）
SC-33	**（削除された）**	---
SC-34	変更できない実行可能プログラム	（対応するものがない）
SC-35	ハニークライアント	（対応するものがない）
SC-36	分散された処理／保管	（対応するものがない）
SC-37	帯域外チャネル	（対応するものがない）
SC-38	運用上のセキュリティ	「A.12.x」の形式の項目に記載されたセキュリティ管理策
SC-39	プロセスの分離	（対応するものがない）
SC-40	ワイヤレスリンクの保護	（対応するものがない）
SC-41	ポートおよび入出力装置に対するアクセス	（対応するものがない）
SC-42	センサー機能およびデータ	（対応するものがない）
SC-43	使用制限	（対応するものがない）
SC-44	デトネーションチャンバー	（対応するものがない）
SI-1	システムおよび情報の完全性のポリシーと手順	A.5.1.1・A.5.1.2・A.6.1.1・A.12.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
SI-2	欠陥の修正	A.12.6.1・A.14.2.2・A.14.2.3・A.16.1.3のそれぞれに記載されたセキュリティ管理策
SI-3	悪質コードからの保護	A.12.2.1に記載されたセキュリティ管理策
SI-4	情報システムのモニタリング	（対応するものがない）
SI-5	セキュリティアラート、勧告、およびディレクティブ	A.6.1.4*に記載されたセキュリティ管理策
SI-6	セキュリティ機能の検証	（対応するものがない）
SI-7	ソフトウェア、ファームウェア、および情報の完全性	（対応するものがない）
SI-8	スパムからの保護	（対応するものがない）
SI-9	**（削除された）**	---
SI-10	入力情報の妥当性確認	（対応するものがない）
SI-11	エラー処理	（対応するものがない）
SI-12	情報の処理および保持	（対応するものがない）
SI-13	予測可能な障害の防止	（対応するものがない）
SI-14	非永続性	（対応するものがない）
SI-15	出力情報のフィルタリング	（対応するものがない）
SI-16	メモリーの保護	（対応するものがない）
SI-17	確実な手続き	（対応するものがない）
PM-1	情報セキュリティプログラム計画 書	A.5.1.1・A.5.1.2・A.6.1.1・A.18.1.1・A.18.2.2のそれぞれに記載されたセキュリティ管理策
PM-2	上級情報セキュリティ責任者	A.6.1.1*に記載されたセキュリティ管理策
PM-3	情報セキュリティリソース	（対応するものがない）
PM-4	行動計画およびマイルストーンプロセス	（対応するものがない）
PM-5	情報システム一覧	（対応するものがない）
PM-6	情報セキュリティパフォーマンスの測定	（対応するものがない）
PM-7	エンタープライズアーキテクチャ	（対応するものがない）

この文書に記載されたセキュリティ管理策		ISO/IEC 27001に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、ISO/IEC 27001に記載されたセキュリティ管理策がこの文書に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
PM-8	重要インフラ計画	（対応するものがない）
PM-9	リスクマネジメント戦略	（対応するものがない）
PM-10	セキュリティ認可プロセス	A.6.1.1*に記載されたセキュリティ管理策
PM-11	ミッション／業務プロセスの定義	（対応するものがない）
PM-12	インサイダー脅威に対する対策	（対応するものがない）
PM-13	情報セキュリティ要員	A.7.2.2*に記載されたセキュリティ管理策
PM-14	テスト、トレーニング、およびモニタリング	（対応するものがない）
PM-15	セキュリティグループやセキュリティ団体と連絡を取り合う	A.6.1.4に記載されたセキュリティ管理策
PM-16	脅威意識向上のためのプログラム	（対応するものがない）.

下記の表 H-2 は、この文書に記載されたセキュリティ管理策[115]と ISO/IEC 27001 に記載されたセキュリティ管理策との関連について、ISO/IEC 27001 に記載されたセキュリティ管理策の観点から記載されたマッピングテーブルである。当該マッピングテーブルは、この付録の冒頭に記載された導入部分の説明を参照のうえ利用されなければならない。

表 H-2：ISO/IEC 27001 側からの NIST SP 800-53 への対応

ISO/IEC 27001に記載されたセキュリティ管理策	この文書に記載されたセキュリティ管理策 注：「*」の記号が添えられた管理策は、この文書に記載されたセキュリティ管理策がISO/IEC 27001に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
A.5 Information Security Policies	
A.5.1 Management direction for information security	
A.5.1.1 Policies for information security	「XX-1」 の形式の項目に記載されたすべてのセキュリティ管理策
A.5.1.2 Review of the policies for information security	「XX-1」 の形式の項目に記載されたすべてのセキュリティ管理策
A.6 Organization of information security	
A.6.1 Internal organization	
A.6.1.1 Information security roles and responsibilities	CM-9・CP-2・PS-7・SA-3・SA-9・PM- 2・PM-10のそれぞれに記載されたセキュリティ管理策とともに、「XX-1」 の形式の項目に記載されたすべてのセキュリティ管理策
A.6.1.2 Segregation of duties	AC-5に記載されたセキュリティ管理
A.6.1.3 Contact with authorities	IR-6に記載されたセキュリティ管理
A.6.1.4 Contact with special interest groups	SI-5・PM-15のそれぞれに記載されたセキュリティ管理
A.6.1.5 Information security in project management	SA-3・SA-9・SA-15のそれぞれに記載されたセキュリティ管理策
A.6.2 Mobile devices and teleworking	
A.6.2.1 Mobile device policy	AC-17・AC-18・AC-19のそれぞれに記載されたセキュリティ管理策
A.6.2.2 Teleworking	AC-3・AC-17・PE-17のそれぞれに記載されたセキュリティ管理策
A.7 Human Resources Security	
A.7.1 Prior to Employment	
A.7.1.1 Screening	PS-3・SA-21のそれぞれに記載されたセキュリティ管理策
A.7.1.2 Terms and conditions of employment	PL-4・PS-6のそれぞれに記載されたセキュリティ管理策
A.7.2 During employment	
A.7.2.1 Management responsibilities	PL-4・PS-6・PS-7・SA-9のそれぞれに記載されたセキュリティ管理策
A.7.2.2 Information security awareness, education, and training	AT-2・AT-3・CP-3・IR-2・PM-13のそれぞれに記載されたセキュリティ管理策
A.7.2.3 Disciplinary process	PS-8に記載されたセキュリティ管理策
A.7.3 Termination and change of employment	
A.7.3.1 Termination or change of employment responsibilities	PS-4・PS-5のそれぞれに記載されたセキュリティ管理策
A.8 Asset Management	
A.8.1 Responsibility for assets	
A.8.1.1 Inventory of assets	CM-8に記載されたセキュリティ管理策

[115] 対応表 H-2 内の「XX-1 controls」という記載は、付録 F の各ファミリの最初のセキュリティ管理策を示している。すなわち、XX はプレースホルダーであり、2 文字から成るファミリ識別子によって置き換えられる。

ISO/IEC 27001に記載されたセキュリティ管理策	この文書に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、この文書に記載されたセキュリティ管理策がISO/IEC 27001に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
A.8.1.2 Ownership of assets	CM-8に記載されたセキュリティ管理策
A.8.1.3 Acceptable use of assets	PL-4に記載されたセキュリティ管理策
A.8.1.4 Return of assets	PS-4・PS-5のそれぞれに記載されたセキュリティ管理策
A.8.2 Information Classification	
A.8.2.1 Classification of information	RA-2に記載されたセキュリティ管理策
A.8.2.2 Labelling of Information	MP-3に記載されたセキュリティ管理策
A.8.2.3 Handling of Assets	MP-2・MP-4・MP-5・MP-6・MP-7・PE-16・PE-18・PE- 20・SC-8・SC-28のそれぞれに記載されたセキュリティ管理策
A.8.3 Media Handling	
A.8.3.1 Management of removable media	MP-2・MP-4・MP-5・MP-6・MP-7のそれぞれに記載されたセキュリティ管理策
A.8.3.2 Disposal of media	MP-6に記載されたセキュリティ管理策
A.8.3.3 Physical media transfer	MP-5に記載されたセキュリティ管理策
A.9 Access Control	
A.9.1 Business requirement of access control	
A.9.1.1 Access control policy	AC-1に記載されたセキュリティ管理策
A.9.1.2 Access to networks and network services	AC-3・AC-6のそれぞれに記載されたセキュリティ管理策
A.9.2 User access management	
A.9.2.1 User registration and de-registration	AC-2・IA-2・IA-4・IA-5・IA-8のそれぞれに記載されたセキュリティ管理策
A.9.2.2 User access provisioning	AC-2に記載されたセキュリティ管理策
A.9.2.3 Management of privileged access rights	AC-2・AC-3・AC-6・CM-5のそれぞれに記載されたセキュリティ管理策
A.9.2.4 Management of secret authentication information of users	IA-5に記載されたセキュリティ管理策
A.9.2.5 Review of user access rights	AC-2に記載されたセキュリティ管理策
A.9.2.6 Removal or adjustment of access rights	AC-2に記載されたセキュリティ管理策
A.9.3 User responsibilities	
A.9.3.1 Use of secret authentication information	IA-5に記載されたセキュリティ管理策
A.9.4 System and application access control	
A.9.4.1 Information access restriction	AC-3・AC-24のそれぞれに記載されたセキュリティ管理策
A.9.4.2 Secure logon procedures	AC-7・AC-8・AC-9・IA-6のそれぞれに記載されたセキュリティ管理策
A.9.4.3 Password management system	IA-5に記載されたセキュリティ管理策
A.9.4.4 Use of privileged utility programs	AC-3・AC-6のそれぞれに記載されたセキュリティ管理策
A.9.4.5 Access control to program source code	AC-3・AC-6・CM-5のそれぞれに記載されたセキュリティ管理策
A.10 Cryptography	
A.10.1 Cryptographic controls	
A.10.1.1 Policy on the use of cryptographic controls	SC-13に記載されたセキュリティ管理策
A.10.1.2 Key Management	SC-12・SC-17のそれぞれに記載されたセキュリティ管理策
A.11 Physical and environmental security	
A.11.1 Secure areas	
A.11.1.1 Physical security perimeter	PE-3*に記載されたセキュリティ管理策

ISO/IEC 27001に記載されたセキュリティ管理策	この文書に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、この文書に記載されたセキュリティ管理策がISO/IEC 27001に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
A.11.1.2 Physical entry controls	PE-2・PE-3・PE-4・PE-5のそれぞれに記載されたセキュリティ管理策
A.11.1.3 Securing offices, rooms and facilities	PE-3・PE-5のそれぞれに記載されたセキュリティ管理策
A.11.1.4 Protecting against external and environmental threats	CP-6・CP-7・PE-9・PE-13・PE-14・PE-15・PE-18・PE- 19のそれぞれに記載されたセキュリティ管理策
A.11.1.5 Working in secure areas	SC-42(3)*に記載されたセキュリティ管理策
A.11.1.6 Delivery and loading areas	PE-16に記載されたセキュリティ管理策
A.11.2 Equipment	
A.11.2.1 Equipment siting and protection	PE-9・PE-13・PE-14・PE-15・PE-18・PE-19のそれぞれに記載されたセキュリティ管理策
A.11.2.2 Supporting utilities	CP-8・PE-9・PE-10・PE-11・PE-12・PE-14・PE-15のそれぞれに記載されたセキュリティ管理策
A.11.2.3 Cabling security	PE-4・PE-9のそれぞれに記載されたセキュリティ管理策
A.11.2.4 Equipment maintenance	MA-2・MA-6のそれぞれに記載されたセキュリティ管理策
A.11.2.5 Removal of assets	MA-2・MP-5・PE-16のそれぞれに記載されたセキュリティ管理策
A.11.2.6 Security of equipment and assets off-premises	AC-19・AC-20・MP-5・PE-17のそれぞれに記載されたセキュリティ管理策
A.11.2.7 Secure disposal or reuse of equipment	MP-6に記載されたセキュリティ管理策
A.11.2.8 Unattended user equipment	AC-11に記載されたセキュリティ管理策
A.11.2.9 Clear desk and clear screen policy	AC-11・MP-2・MP-4のそれぞれに記載されたセキュリティ管理策
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	
A.12.1.1 Documented operating procedures	SA-5に記載されたセキュリティ管理策とともに、「XX-1」の形式の項目**に記載されたすべてのセキュリティ管理策**
A.12.1.2 Change management	CM-3・CM-5・SA-10のそれぞれに記載されたセキュリティ管理策
A.12.1.3 Capacity management	AU-4・CP-2(2)・SC-5(2)のそれぞれに記載されたセキュリティ管理策
A.12.1.4 Separation of development, testing, and operational environments	CM-4(1)*・CM-5*のそれぞれに記載されたセキュリティ管理策
A.12.2 Protection from malware	
A.12.2.1 Controls against malware	AT-2・SI-3のそれぞれに記載されたセキュリティ管理策
A.12.3 Backup	
A.12.3.1 Information backup	CP-9に記載されたセキュリティ管理策
A.12.4 Logging and monitoring	
A.12.4.1 Event logging	AU-3・AU-6・AU-11・AU-12・AU-14のそれぞれに記載されたセキュリティ管理策
A.12.4.2 Protection of log information	AU-9に記載されたセキュリティ管理策
A.12.4.3 Administrator and operator logs	AU-9・AU-12のそれぞれに記載されたセキュリティ管理策
A.12.4.4 Clock synchronization	AU-8に記載されたセキュリティ管理策
A.12.5 Control of operational software	
A.12.5.1 Installation of software on operational systems	CM-5・CM-7(4)・CM-7(5)・CM-11のそれぞれに記載されたセキュリティ管理策
A.12.6 Technical vulnerability management	

ISO/IEC 27001に記載されたセキュリティ管理策	この文書に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、この文書に記載されたセキュリティ管理策がISO/IEC 27001に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
A.12.6.1 Management of technical vulnerabilities	RA-3・RA-5・SI-2・SI-5のそれぞれに記載されたセキュリティ管理策
A.12.6.2 Restrictions on software installation	CM-11に記載されたセキュリティ管理策
A.12.7 Information systems audit considerations	
A.12.7.1 Information systems audit controls	AU-5*に記載されたセキュリティ管理策
A.13 Communications security	
A.13.1 Network security management	
A.13.1.1 Network controls	AC-3・AC-17・AC-18・AC-20・SC-7・SC-8・SC-10のそれぞれに記載されたセキュリティ管理策
A.13.1.2 Security of network services	CA-3・SA-9のそれぞれに記載されたセキュリティ管理策
A.13.1.3 Segregation in networks	AC-4・SC-7のそれぞれに記載されたセキュリティ管理策
A.13.2 Information transfer	
A.13.2.1 Information transfer policies and procedures	AC-4・AC-17・AC-18・AC-19・AC-20・CA-3・PE-17・SC-7・SC-8・SC-15のそれぞれに記載されたセキュリティ管理策
A.13.2.2 Agreements on information transfer	CA-3・PS-6・SA-9のそれぞれに記載されたセキュリティ管理策
A.13.2.3 Electronic messaging	SC-8に記載されたセキュリティ管理策
A.13.2.4 Confidentiality or nondisclosure agreements	PS-6に記載されたセキュリティ管理策
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	
A.14.1.1 Information security requirements analysis and specification	PL-2・PL-7・PL-8・SA-3・SA-4のそれぞれに記載されたセキュリティ管理策
A.14.1.2 Securing application services on public networks	AC-3・AC-4・AC-17・SC-8・SC-13のそれぞれに記載されたセキュリティ管理策
A.14.1.3 Protecting application services transactions	AC-3・AC-4・SC-7・SC-8・SC-13のそれぞれに記載されたセキュリティ管理策
A.14.2 Security in development and support processes	
A.14.2.1 Secure development policy	SA-3・SA-15・SA-17のそれぞれに記載されたセキュリティ管理策
A.14.2.2 System change control procedures	CM-3・SA-10・SI-2のそれぞれに記載されたセキュリティ管理策
A.14.2.3 Technical review of applications after operating platform changes	CM-3・CM-4・SI-2のそれぞれに記載されたセキュリティ管理策
A.14.2.4 Restrictions on changes to software packages	CM-3・SA-10のそれぞれに記載されたセキュリティ管理策
A.14.2.5 Secure system engineering principles	SA-8に記載されたセキュリティ管理策
A.14.2.6 Secure development environment	SA-3*に記載されたセキュリティ管理策
A.14.2.7 Outsourced development	SA-4・SA-10・SA-11・SA-12・SA-15のそれぞれに記載されたセキュリティ管理策
A.14.2.8 System security testing	CA-2・SA-11のそれぞれに記載されたセキュリティ管理策
A.14.2.9 System acceptance testing	SA-4・SA-12(7)のそれぞれに記載されたセキュリティ管理策
A.14.3 Test data	
A.14.3.1 Protection of test data	SA-15(9)*に記載されたセキュリティ管理策
A.15 Supplier Relationships	

ISO/IEC 27001に記載されたセキュリティ管理策	この文書に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、この文書に記載されたセキュリティ管理策がISO/IEC 27001に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
A.15.1 Information security in supplier relationships	
A.15.1.1 Information security policy for supplier relationships	SA-12に記載されたセキュリティ管理策
A.15.1.2 Address security within supplier agreements	SA-4・SA-12のそれぞれに記載されたセキュリティ管理策
A.15.1.3 Information and communication technology supply chain	SA-12に記載されたセキュリティ管理策
A.15.2 Supplier service delivery management	
A.15.2.1 Monitoring and review of supplier services	SA-9に記載されたセキュリティ管理策
A.15.2.2 Managing changes to supplier services	SA-9に記載されたセキュリティ管理策
A.16 Information security incident management	
A.16.1 Managing of information security incidents and improvements	
A.16.1.1 Responsibilities and procedures	IR-8に記載されたセキュリティ管理策
A.16.1.2 Reporting information security events	AU-6・IR-6のそれぞれに記載されたセキュリティ管理策
A.16.1.3 Reporting information security weaknesses	SI-2に記載されたセキュリティ管理策
A.16.1.4 Assessment of and decision on information security events	AU-6・IR-4のそれぞれに記載されたセキュリティ管理策
A.16.1.5 Response to information security incidents	IR-4に記載されたセキュリティ管理策
A.16.1.6 Learning from information security incidents	IR-4に記載されたセキュリティ管理策
A.16.1.7 Collection of evidence	AU-4*・AU-9*・AU-10(3)*・AU-11*のそれぞれに記載されたセキュリティ管理策
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	
A.17.1.1 Planning information security continuity	CP-2に記載されたセキュリティ管理策
A.17.1.2 Implementing information security continuity	CP-6・CP-7・CP-8・CP-9・CP-10・CP-11・CP-13のそれぞれに記載されたセキュリティ管理策
A.17.1.3 Verify, review, and evaluate information security continuity	CP-4に記載されたセキュリティ管理策
A.17.2 Redundancies	
A.17.2.1 Availability of information processing facilities	CP-2・CP-6・CP-7のそれぞれに記載されたセキュリティ管理策
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	
A.18.1.1 Identification of applicable legislation and contractual requirements	「XX-1」の形式の項目**に記載されたすべてのセキュリティ管理策**
A.18.1.2 Intellectual property rights	CM-10に記載されたセキュリティ管理策
A.18.1.3 Protection of records	AC-3・AC-23・AU-9・AU-10・CP-9・SC-8・SC-8(1)・SC-13・SC-28・SC-28(1)のそれぞれに記載されたセキュリティ管理策
A.18.1.4 Privacy and protection of personal information	付録 J に記載されたプライバシー管理策
A.18.1.5 Regulation of cryptographic controls	IA-7・SC-12・SC-13・SC-17のそれぞれに記載されたセキュリティ管理策
A.18.2 **Information security reviews**	
A.18.2.1 Independent review of information security	CA-2(1)・SA-11(3) のそれぞれに記載されたセキュリティ管理策

ISO/IEC 27001に記載されたセキュリティ管理策	この文書に記載されたセキュリティ管理策 注:「*」の記号が添えられた管理策は、この文書に記載されたセキュリティ管理策がISO/IEC 27001に記載されたセキュリティ管理策によって保護される対象のセキュリティを完全に担保するのに不十分な管理策である。
A.18.2.2 Compliance with security policies and standards	CA-2に記載されたセキュリティ管理策とともに、「XX-1」の形式の項目に記載されたすべてのセキュリティ管理策
A.18.2.3 Technical compliance review	CA-2に記載されたセキュリティ管理策

表 H-3 は、ISO/IEC 15408「Common Criteria(コモンクライテリア)」の機能要件と保証要件側からの、Special Publication 800-53 への対応を示している。この表は、セキュリティ要求事項とセキュリティ管理策の大まかな対応を示すものである(すなわち、この表は、ISO/IEC 15408 のセキュリティ要求事項が、対応するセキュリティ管理策によって完全に満たされる、あるいは部分的に満たされる、もしくは全く満たされない、のいずれに該当するかを判断するためのものではない。)しかしながら、この表は、対応のさらなる分析を行う際の出発点として役立つ。組織は、付録 F に記載されている特定のセキュリティ管理策が導入されている、評価され有効性が確認された特定の IT 製品が ISO/IEC 15408 のセキュリティ要求事項を満たしている場合であっても、そうした要求事項が情報システム(複数のコンポーネント製品で構成される場合もある)全体にわたって満たされているとは限らないことに、注意が必要である。表 H-3 内の特定の対応について説明する追加の情報は、NIAP(National Information Assurance Partnership)の以下のウェブサイトに記載されている:http://www.niap-ccevs.org

表 H-3:ISO/IEC 15408 側からの NIST SP 800-53 への対応

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
Functional Requirements			
FAU_ARP.1	**Security Audit Automatic Response** Security Alarms	AU-5	**監査処理が失敗した時の対応**
		AU-5 (1)	**監査処理が失敗した時の対応** 監査記録の記憶容量
		AU-5 (2)	**監査処理が失敗した時の対応** リアルタイムの警告
		AU-5 (3)	**監査処理が失敗した時の対応** トラフィック量の閾値を設定できるようにする
		AU-5 (4)	**監査処理が失敗した時の対応** 失敗した時のシャットダウン
		PE-6 (2)	**物理アクセスのモニタリング** 自動化された、侵入検知 / 対応
		SI-3	**悪質コードからの保護**
		SI-3 (8)	**悪質コードからの保護** 許可されていないコマンドを検知する
		SI-4 (5)	**情報システムのモニタリング** システムが生成する警告
		SI-4 (7)	**情報システムのモニタリング** 自動化された、疑わしいイベントに対する対応
		SI-4 (22)	**情報システムのモニタリング** 許可されていないネットワークサービス

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		SI-7 (2)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性違反の自動通知
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された、完全性違反に対する対応
		SI-7 (8)	**ソフトウェア、ファームウェア、および情報の完全性** 重要なイベントのチェック機能
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation	AU-2	**監査イベント**
		AU-3	**監査記録の内容**
		AU-3 (1)	**監査記録の内容** 追加の監査情報
		AU-12	**監査記録の生成**
FAU_GEN.2	**Security Audit Data Generation** User Identity Association	AU-3	**監査記録の内容**
FAU_SAA.1	**Security Audit Analysis** Potential Violation Analysis	SI-4	**情報システムのモニタリング**
FAU_SAA.2	**Security Audit Analysis** Profile-Based Anomaly Detection	AC-2 (12)	**アカウント管理** アカウントのモニタリング／通常でない使用
		SI-4	**情報システムのモニタリング**
FAU_SAA.3	**Security Audit Analysis** Simple Attack Heuristics	SI-3 (7)	**悪質コードからの保護** 署名ベースでない検知
		SI-4	**情報システムのモニタリング**
FAU_SAA.4	**Security Audit Analysis** Complex Attack Heuristics	SI-3 (7)	**悪質コードからの保護** 署名ベースでない検知
		SI-4	**情報システムのモニタリング**
FAU_SAR.1	**Security Audit Review** Audit Review	AU-7	**監査量削減と報告書自動作成**
FAU_SAR.2	**Security Audit Review** Restricted Audit Review	AU-9 (6)	**監査情報の保護** 読み出し専用アクセス
FAU_SAR.3	**Security Audit Review** Selectable Audit Review	AU-7	**監査量削減と報告書自動作成**
		AU-7 (1)	**監査量削減と報告書自動作成** 自動処理
		AU-7 (2)	**監査量削減と報告書自動作成** 自動での並べ替えと検索
FAU_SEL.1	**Security Audit Event Selection** Selective Audit	AU-12	**監査記録の生成**
FAU_STG.1	**Security Audit Event Storage** Protected Audit Trail Storage	AU-9	**監査情報の保護**
FAU_STG.2	**Security Audit Event Storage** Guarantees of Audit Data Availability	AU-9	**監査情報の保護** 代替監査機能
FAU_STG.3	**Security Audit Event Storage** Action In Case of Possible Audit Data Loss	AU-5	**監査処理が失敗した時の対応**
		AU-5 (1)	**監査処理が失敗した時の対応** 監査記録の記憶容量
		AU-5 (2)	**監査処理が失敗した時の対応** リアルタイムの警告

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		AU-5 (4)	**監査処理が失敗した時の対応** 失敗した時のシャットダウン
FAU_STG.4	**Security Audit Event Storage** Prevention of Audit Data Loss	AU-4	**監査記録の記憶容量**
		AU-5	**監査処理が失敗した時の対応**
		AU-5 (2)	**監査処理が失敗した時の対応** リアルタイムの警告
		AU-5 (4)	**監査処理が失敗した時の対応** 失敗した時のシャットダウン
FCO_NRO.1	**Non-Repudiation of Origin** Selective Proof of Origin	AU-10	**否認防止**
		AU-10 (1)	**否認防止** 身元の結び付け
		AU-10 (2)	**否認防止** 情報作成者の身元との結び付けを確認する
FCO_NRO.2	**Non-Repudiation of Origin** Enforced Proof of Origin	AU-10	**否認防止**
		AU-10 (1)	**否認防止** 身元の結び付け
		AU-10 (2)	**否認防止** 情報作成者の身元との結び付けを確認する
FCO_NRR.1	**Non-Repudiation of Receipt** Selective Proof of Receipt	AU-10	**否認防止**
		AU-10 (1)	**否認防止** 身元の結び付け
		AU-10 (2)	**否認防止** 情報作成者の身元との結び付けを確認する
FCO_NRR.2	**Non-Repudiation of Receipt** Enforced Proof of Receipt	AU-10	**否認防止**
		AU-10 (1)	**否認防止** 身元の結び付け
		AU-10 (2)	**否認防止** 情報作成者の身元との結び付けを確認する
FCS_CKM.1	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**暗号鍵の作成と管理**
FCS_CKM.2	**Cryptographic Key Management** Cryptographic Key Distribution	SC-12	**暗号鍵の作成と管理**
FCS_CKM.3	**Cryptographic Key Management** Cryptographic Key Access	SC-12	**暗号鍵の作成と管理**
FCS_CKM.4	**Cryptographic Key Management** Cryptographic Key Destruction	SC-12	**暗号鍵の作成と管理**
FCS_COP.1	**Cryptographic Operation** Cryptographic Operation	SC-13	**暗号化による保護**
FDP_ACC.1	**Access Control Policy** Subset Access Control	AC-3	**アクセス制御の実施**
		AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-3 (4)	**アクセス制御の実施** 任意のアクセス制御

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		AC-3 (7)	**アクセス制御の実施** 役割に基づいたアクセス制御
FDP_ACC.2	**Access Control Policy** Complete Access Control	AC-3	**アクセス制御の実施**
		AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-3 (4)	**アクセス制御の実施** 任意のアクセス制御
		AC-3 (7)	**アクセス制御の実施** 役割に基づいたアクセス制御
FDP_ACF.1	**Access Control Functions** Security Attribute Based Access Control	AC-3	**アクセス制御の実施**
		AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-3 (4)	**アクセス制御の実施** 任意のアクセス制御
		AC-3 (7)	**アクセス制御の実施** 役割に基づいたアクセス制御
		AC-16	**セキュリティ属性**
		SC-16	**セキュリティ属性の伝送**
FDP_DAU.1	**Data Authentication** Basic Data Authentication	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SI-7 (6)	**ソフトウェア、ファームウェア、および情報の完全性** 暗号化による保護
		SI-10	**入力情報の妥当性確認**
FDP_DAU.2	**Data Authentication** Data Authentication With Identity of Guarantor	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SI-7 (6)	**ソフトウェア、ファームウェア、および情報の完全性** 暗号化による保護
		SI-10	**入力情報の妥当性確認**
FDP_ETC.1	**Export from the TOE** Export of User Data without Security Attributes	（対応するものがない）.	
FDP_ETC.2	**Export from the TOE** Export of User Data with Security Attributes	AC-4 (18)	**情報フロー制御の実施** セキュリティ属性を結び付ける
		AC-16	**セキュリティ属性**
		AC-16 (5)	**セキュリティ属性** 出力装置に属性を表示する
		SC-16	**セキュリティ属性の伝送**
FDP_IFC.1	**Information Flow Control Policy**	AC-3	**アクセス制御の実施**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
	Subset Information Flow Control	AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-4	**情報フロー制御の実施**
		AC-4 (1)	**情報フロー制御の実施** オブジェクトのセキュリティ属性
FDP_IFC.2	**Information Flow Control Policy** Complete Information Flow Control	AC-3	**アクセス制御の実施**
		AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-4	**情報フロー制御の実施**
FDP_IFF.1	**Information Flow Control Functions** Simple Security Attributes	AC-3	**アクセス制御の実施**
		AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-4	**情報フロー制御の実施**
		AC-4 (1)	**情報フロー制御の実施** オブジェクトのセキュリティ属性
		AC-4 (2)	**情報フロー制御の実施** 処理ドメイン
		AC-4 (7)	**情報フロー制御の実施** 一方向フローメカニズム
		AC-16	**セキュリティ属性**
		SC-7	**境界保護**
FDP_IFF.2	**Information Flow Control Functions** Hierarchical Security Attributes	AC-3	**アクセス制御の実施**
		AC-3 (3)	**アクセス制御の実施** 必須のアクセス制御
		AC-4 (1)	**情報フロー制御の実施** オブジェクトのセキュリティ属性
		AC-16	**セキュリティ属性**
FDP_IFF.3	**Information Flow Control Functions** Limited Illicit Information Flows	SC-31	**隠れチャネル分析**
		SC-31 (2)	**隠れチャネル分析** 最大帯域幅
FDP_IFF.4	**Information Flow Control Functions** Partial Elimination of Illicit Information Flows	SC-31	**隠れチャネル分析**
		SC-31 (2)	**隠れチャネル分析** 最大帯域幅
FDP_IFF.5	**Information Flow Control Functions** No Illicit Information Flows	SC-31	**隠れチャネル分析**
		SC-31 (2)	**隠れチャネル分析** 最大帯域幅
FDP_IFF.6	**Information Flow Control Functions** Illicit Information Flow Monitoring	SC-31	**隠れチャネル分析**
		SI-4 (18)	**情報システムのモニタリング** トラフィック を分析し、情報の密かな取り出しを検知する
FDP_ITC.1	**Import from Outside of the TOE** Import of User Data without Security Attributes	AC-4 (9)	**情報フロー制御の実施** 人によるレビュー
		AC-4 (12)	**情報フロー制御の実施** データタイプ識別子

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FDP_ITC.2	**Import from Outside of the TOE** Import of User Data with Security Attributes	AC-4 (18)	**情報フロー制御の実施** セキュリティ属性を結び付ける
		AC-16	**セキュリティ属性**
		SC-16	**セキュリティ属性の伝送**
FDP_ITT.1	**Internal TOE Transfer** Basic Internal Transfer Protection	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		SC-5	**サービス妨害からの保護**
FDP_ITT.2	**Internal TOE Transfer** Transmission Separation by Attribute	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		SC-5	**サービス妨害からの保護**
		AC-4 (21)	**情報フロー制御の実施** 情報フローの物理的 / 論理的な分離
FDP_ITT.3	**Internal TOE Transfer** Integrity Monitoring	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された、完全性違反に対する対応
FDP_ITT.4	**Internal TOE Transfer** Attribute-Based Integrity Monitoring	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		AC-4 (21)	**情報フロー制御の実施** 情報フローの物理的 / 論理的な分離
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された、完全性違反に対する対応
FDP_RIP.1	**Residual Information Protection** Subset Residual Information Protection	SC-4	**共有リソース内の情報**
FDP_RIP.2	**Residual Information Protection** Full Residual Information Protection	SC-4	**共有リソース内の情報**
FDP_ROL.1	**Rollback** Basic Rollback	CP-10 (2)	**情報システムの復旧と再構成** トランザクションの回復
FDP_ROL.2	**Rollback** Advanced Rollback	CP-10 (2)	**情報システムの復旧と再構成** トランザクションの回復

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FDP_SDI.1	**Stored Data Integrity** Stored Data Integrity Monitoring	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
FDP_SDI.2	**Stored Data Integrity** Stored Data Integrity Monitoring and Action	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された完全性違反に対する対応
FDP_UCT.1	**Inter-TSF User Data Confidentiality Transfer Protection** Basic Data Exchange Confidentiality	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
FDP_UIT.1	**Inter-TSF User Data Integrity Transfer Protection** Data Exchange Integrity	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (6)	**ソフトウェア、ファームウェア、および情報の完全性** 暗号化による保護
FDP_UIT.2	**Inter-TSF User Data Integrity Transfer Protection** Source Data Exchange Recovery	（対応するものがない）.	
FDP_UIT.3	**Inter-TSF User Data Integrity Transfer Protection** Destination Data Exchange Recovery	（対応するものがない）.	
FIA_AFL.1	**Authentication Failure** Authentication Failure Handling	AC-7	**ログオン試行の失敗**
FIA_ATD.1	**User Attribute Definition** User Attribute Definition	AC-2	**アカウント管理**
		IA-2	**識別および認証（組織的ユーザ）**
FIA_SOS.1	**Specification of Secrets** Verification of Secrets	IA-5	**オーセンティケータの管理**
		IA-5 (1)	**オーセンティケータの管理** パスワードによる認証
		IA-5 (12)	**オーセンティケータの管理** 生体認証
FIA_SOS.2	**Specification of Secrets** TSF Generation of Secrets	IA-5	**オーセンティケータの管理**
		IA-5 (1)	**オーセンティケータの管理** パスワードによる認証
		IA-5 (12)	**オーセンティケータの管理** 生体認証
FIA_UAU.1	**User Authentication** Timing of Authentication	AC-14	**識別または認証を必要としないアクション**
		IA-2	**識別および認証（組織的ユーザ）**
		IA-8	**識別および認証（組織的ユーザ以外のユーザ）**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FIA_UAU.2	**User Authentication** User Authentication Before Any Action	AC-14	**識別または認証を必要としないアクション**
		IA-2	**識別および認証（組織的ユーザ）**
		IA-8	**識別および認証（組織的ユーザ）**
FIA_UAU.3	**User Authentication** Unforgeable Authentication	IA-2 (8)	**識別および認証（組織的ユーザ）** 特権アカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性
		IA-2 (9)	**識別および認証（組織的ユーザ）** 特権アカウントでないアカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性
FIA_UAU.4	**User Authentication** Single-Use Authentication Mechanisms	IA-2 (8)	**識別および認証（組織的ユーザ）** 特権アカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性
		IA-2 (9)	**識別および認証（組織的ユーザ）** 特権アカウントでないアカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性
FIA_UAU.5	**User Authentication** Multiple Authentication Mechanisms	IA-2 (1)	**識別および認証（組織的ユーザ）** 特権アカウントに対するネットワークアクセス
		IA-2 (2)	**識別および認証（組織的ユーザ）** 特権アカウントでないアカウントに対するネットワークアクセス
		IA-2 (3)	**識別および認証（組織的ユーザ）** 特権アカウントに対するローカルアクセス
		IA-2 (4)	**識別および認証（組織的ユーザ）** 特権アカウントでないアカウントに対するローカルアクセス
		IA-2 (6)	**識別および認証（組織的ユーザ）** 特権アカウントに対するネットワークアクセス - 切り離されたデバイス
		IA-2 (7)	**識別および認証（組織的ユーザ）** 特権アカウントでないアカウントに対するネットワークアクセス - 切り離されたデバイス
		IA-2 (11)	**識別および認証（組織的ユーザ）** リモートアクセス - 切り離されたデバイス
FIA_UAU.6	**User Authentication** Re-Authenticating	IA-11	**再認証**
FIA_UAU.7	**User Authentication** Protected Authentication Feedback	IA-6	**オーセンティケータのフィードバック**
FIA_UID.1	**User Identification** Timing of Identification	AC-14	**識別または認証を必要としないアクション**
		IA-2	**識別および認証（組織的ユーザ）**
		IA-8	**識別および認証（組織的ユーザ以外のユーザ）**
FIA_UID.2	**User Identification** User Identification Before Any Action	AC-14	**識別または認証を必要としないアクション**
		IA-2	**識別および認証（組織的ユーザ）**
		IA-8	**識別および認証（組織的ユーザ以外のユーザ）**
FIA_USB.1	**User-Subject Binding** User-Subject Binding	AC-16 (3)	**セキュリティ属性** 情報システムを介した属性の結び付けの維持
FMT_MOF.1	**Management of Functions in TSF**	AC-3 (7)	**アクセス制御の実施** 役割ベースのアクセス制御

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
	Management of Security Functions Behavior	AC-6	**最小権限**
		AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
FMT_MSA.1	**Management of Security Attributes** Management of Security Attributes	AC-6	**最小権限**
		AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
		AC-16 (2)	**セキュリティ属性** 許可された個人による属性値の変更
		AC-16 (4)	**セキュリティ属性** 許可された個人による属性の結び付け
		AC-16 (10)	**セキュリティ属性** 許可された個人による属性設定
FMT_MSA.2	**Management of Security Attributes** Secure Security Attributes	AC-16	**セキュリティ属性**
		CM-6	**設定項目**
		SI-10	**入力情報の妥当性確認**
FMT_MSA.3	**Management of Security Attributes** Static Attribute Initialization	（対応するものがない）.	
FMT_MSA.4	**Management of Security Attributes** Security Attribute Value Inheritance	（対応するものがない）.	
FMT_MTD.1	**Management of TSF Data** Management of TSF Data	AC-3 (7)	**アクセス制御の実施** 役割ベースのアクセス制御
		AC-6	**最小権限**
		AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
		AU-6 (7)	**監査記録のレビュー、分析、報告** 許可されているアクション
		AU-9 (4)	**監査情報の保護** 一部の特権ユーザのによるアクセス
FMT_MTD.2	**Management of TSF Data** Management of Limits on TSF Data	AC-3 (7)	**アクセス制御の実施** 役割ベースのアクセス制御
		AC-6	**最小権限**
		AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
FMT_MTD.3	**Management of TSF Data** Secure TSF Data	SI-10	**入力情報の妥当性確認**
FMT_REV.1	**Revocation** Revocation	AC-3 (7)	**アクセス制御の実施** 役割ベースのアクセス制御
		AC-3 (8)	**アクセス制御の実施** アクセス権限の取り消し
		AC-6	**最小権限**
		AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
FMT_SAE.1	**Security Attribute Expiration** Time-Limited Authorization	AC-3 (7)	**アクセス制御の実施** 役割ベースのアクセス制御
		AC-6	**最小権限**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions	（対応するものがない）.	
FMT_SMR.1	**Security Management Roles** Security Roles	AC-2 (7)	**アカウント管理** 役割ベースのスキーム
		AC-3 (7)	**アクセス制御の実施** 役割ベースのアクセス制御
		AC-5	**職務の分離**
		AC-6	**最小権限**
FMT_SMR.2	**Security Management Roles** Restrictions on Security Roles	AC-2 (7)	**アカウント管理** 役割に基づいたスキーム
		AC-3 (7)	**アクセス制御の実施** 役割に基づいたアクセス制御
		AC-5	**職務の分離**
		AC-6	**最小権限**
FMT_SMR.3	**Security Management Roles** Assuming Roles	AC-6 (1)	**最小権限** セキュリティ機能に対するアクセスを許可する
		AC-6 (2)	**最小権限** 非セキュリティ機能に対する特権的でないアクセス
FPR_ANO.1	**Anonymity** Anonymity	（対応するものがない）.	
FPR_ANO.2	**Anonymity** Anonymity Without Soliciting Information	（対応するものがない）.	
FPR_PSE.1	**Pseudonymity** Pseudonymity	（対応するものがない）.	
FPR_PSE.2	**Pseudonymity** Reversible Pseudonymity	（対応するものがない）.	
FPR_PSE.3	**Pseudonymity** Alias Pseudonymity	（対応するものがない）.	
FPR_UNL.1	**Unlinkability** Unlinkability	（対応するものがない）.	
FPR_UNO.1	**Unobservability** Unobservability	（対応するものがない）.	
FPR_UNO.2	**Unobservability** Allocation of Information Impacting Unobservability	（対応するものがない）.	
FPR_UNO.3	**Unobservability** Unobservability Without Soliciting Information	（対応するものがない）.	
FPR_UNO.4	**Unobservability** Authorized User Observability	（対応するものがない）.	
FPT_FLS.1	**Fail Secure** Failure with Preservation of Secure State	SC-7 (18)	**境界保護** フェールセキュア
		SC-24	**既知の状態に陥ること**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FPT_ITA.1	**Availability of Exported TSF Data** Inter-TSF Availability within a Defined Availability Metric	CP-10	**情報システムの復旧と再構成** 期間内に復旧する
		SC-5	**セキュリティ機能の分離**
		SC-5 (2)	**セキュリティ機能の分離** 予備の容量 / 帯域幅 / その他の予備
		SC-5 (3)	**セキュリティ機能の分離** 検知 / モニタリング
FPT_ITC.1	**Confidentiality of Exported TSF Data** Inter-TSF Confidentiality During Transmission	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
FPT_ITI.1	**Integrity of Exported TSF Data** Inter-TSF Detection of Modification	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された、完全性違反に対する対応
		SI-7 (6)	**ソフトウェア、ファームウェア、および情報の完全性** 暗号化による保護
FPT_ITI.2	**Integrity of Exported TSF Data** Inter-TSF Detection and Correction of Modification	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
		SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された、完全性違反に対する対応
		SI-7 (6)	**ソフトウェア、ファームウェア、および情報の完全性** 暗号化による保護
FPT_ITT.1	**Internal TOE TSF Data Transfer** Basic Internal TSF Data Transfer Protection	SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護
FPT_ITT.2	**Internal TOE TSF Data Transfer** TSF Data Transfer Separation	AC-4 (21)	**情報フロー制御の実施** 情報フローの物理的 / 論理的な分離
		SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化による、あるいは代替の物理面での保護

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FPT_ITT.3	**Internal TOE TSF Data Transfer** TSF Data Integrity Monitoring	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
		SI-7 (1)	**ソフトウェア、ファームウェア、および情報の完全性** 完全性チェック
		SI-7 (5)	**ソフトウェア、ファームウェア、および情報の完全性** 自動化された、完全性違反に対する対応
		SI-7 (6)	**ソフトウェア、ファームウェア、および情報の完全性** 暗号化による保護
FPT_PHP.1	**TSF Physical Protection** Passive Detection of Physical Attack	PE-3 (5)	**物理アクセス制御** 改ざん防止
		PE-6 (2)	**物理アクセスのモニタリング** 自動化された、侵入検知 / 対応
		SA-18	**改ざんの防止と検知**
FPT_PHP.2	**TSF Physical Protection** Notification of Physical Attack	PE-3 (5)	**物理アクセス制御** 改ざん防止
		PE-6 (2)	**物理アクセスのモニタリング** 自動化された、侵入検知 / 対応
		SA-18	**改ざんの防止と検知**
FPT_PHP.3	**TSF Physical Protection** Resistance to Physical Attack	PE-3 (5)	**物理アクセス制御** 改ざん防止
		SA-18	**改ざんの防止と検知**
FPT_RCV.1	**Trusted Recovery** Manual Recovery	CP-10	**情報システムの復旧と再構成**
		CP-12	**セーフモード**
FPT_RCV.2	**Trusted Recovery** Automated Recovery	CP-10	**情報システムの復旧と再構成**
		CP-12	**セーフモード**
FPT_RCV.3	**Trusted Recovery** Automated Recovery Without Undue Loss	CP-10	**情報システムの復旧と再構成**
		CP-12	**セーフモード**
FPT_RCV.4	**Trusted Recovery** Function Recovery	SI-6	**セキュリティ機能の検証**
		SI-10 (3)	**入力情報の妥当性確認** 予測可能な振る舞い
		SC-24	**既知の状態に陥ること**
FPT_RPL.1	**Replay Detection** Replay Detection	IA-2 (8)	**識別および認証（組織的ユーザ）** 特権アカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性
		IA-2 (9)	**識別および認証（組織的ユーザ）** 特権アカウントでないアカウントに対するネットワークアクセス - リプレイ攻撃に対する耐性
		SC-23	**セッションの真正性**
		SI-3 (9)	**悪質コードからの保護** リモートコマンドの認証を行う
FPT_SSP.1	**State Synchrony Protocol** Simple Trusted Acknowledgement	（対応するものがない）.	

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FPT_SSP.2	**State Synchrony Protocol** Mutual Trusted Acknowledgement	（対応するものがない）.	
FPT_STM.1	**Time Stamps** Reliable Time Stamps	AU-8	**タイムスタンプ**
FPT_TDC.1	**Inter-TSF TSF Data Consistency** Inter-TSF Basic Data Consistency	AC-16 (7)	**セキュリティ属性** 矛盾のない属性解釈
		AC-16 (8)	**セキュリティ属性** 結び付け技法 / テクノロジー
FPT_TEE.1	**Testing of External Entities** Testing of External Entities	SI-6	**セキュリティ機能の検証**
FPT_TRC.1	**Internal TOE TSF Data Replication Consistency** Internal TSF Consistency	SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
FPT_TST.1	**TSF Self Test** TSF Testing	SI-6	**セキュリティ機能の検証**
		SI-7	**ソフトウェア、ファームウェア、および情報の完全性**
FRU_FLT.1	**Fault Tolerance** Degraded Fault Tolerance	AU-15	**代替監査機能**
		CP-11	**代替通信プロトコル**
		SC-24	**セッションの真正性**
		SI-13	**予測可能な障害の防止**
		SI-13 (1)	**予測可能な障害の防止** コンポーネントの権限を委譲する
		SI-13 (2)	**予測可能な障害の防止** モニタリングなしのプロセスの実行に、タイムリミットを課す
		SI-13 (3)	**予測可能な障害の防止** コンポーネント間の手動での委譲
		SI-13 (4)	**予測可能な障害の防止** 予備コンポーネントのインストール / 通知
		SI-13 (5)	**予測可能な障害の防止** 障害迂回機能
FRU_FLT.2	**Fault Tolerance** Limited Fault Tolerance	AU-15	**代替監査機能**
		CP-11	**代替通信プロトコル**
		SC-24	**既知の状態に陥ること**
		SI-13	**予測可能な障害の防止**
		SI-13 (1)	**予測可能な障害の防止** コンポーネントの権限を委譲する
		SI-13 (2)	**予測可能な障害の防止** モニタリングなしのプロセスの実行に、タイムリミットを課す
		SI-13 (3)	**予測可能な障害の防止** コンポーネント間の手動での委譲
		SI-13 (4)	**予測可能な障害の防止** 予備コンポーネントのインストール / 通知
		SI-13 (5)	**予測可能な障害の防止** 障害迂回機能

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
FRU_PRS.1	**Priority of Service** Limited Priority of Service	SC-6	**リソースの可用性**
FRU_PRS.2	**Priority of Service** Full Priority of Service	SC-6	**リソースの可用性**
FRU_RSA.1	**Resource Allocation** Maximum Quotas	SC-6	**リソースの可用性**
FRU_RSA.2	**Resource Allocation** Minimum and Maximum Quotas	SC-6	**リソースの可用性**
FTA_LSA.1	**Limitation on Scope of Selectable Attributes** Limitation on Scope of Selectable Attributes	AC-2 (6)	**アカウント管理** 動的な権限管理
		AC-2 (11)	**アカウント管理** 使用条件
FTA_MCS.1	**Limitation on Multiple Concurrent Sessions** Basic Limitation on Multiple Concurrent Sessions	AC-10	**同時セッションの制御**
FTA_MCS.2	**Limitation on Multiple Concurrent Sessions** Per-User Limitation on Multiple Concurrent Sessions	AC-10	**同時セッションの制御**
FTA_SSL.1	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**セッションのロック**
		AC-11 (1)	**セッションのロック** パターンを隠して表示する
FTA_SSL.2	**Session Locking and Termination** User-Initiated Locking	AC-11	**セッションのロック**
		AC-11 (1)	**セッションのロック** パターンを隠して表示する
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination	AC-12	**セッションの終了**
		SC-10	**ネットワークの切断**
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination	AC-12 (1)	**セッションの終了** ユーザが開始したログアウト / メッセージ表示
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners	AC-8	**システムの利用に関する通知**
FTA_TAH.1	**TOE Access History** TOE Access History	AC-9	**前回のログオン(アクセス)に関する通知**
		AC-9 (1)	**前回のログオン(アクセス)に関する通知** ログオンの失敗
FTA_TSE.1	**TOE Session Establishment** TOE Session Establishment	AC-2 (11)	**アカウント管理** 使用条件
FTP_ITC.1	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel	IA-3 (1)	**デバイスの識別および認証** 暗号を用いた双方向認証
		SC-8	**伝送される情報の機密性と完全性**
		SC-8 (1)	**伝送される情報の機密性と完全性** 暗号化によるあるいは代替の物理面での保護
FTP_TRP.1	**Trusted Path** Trusted Path	SC-11	**高信頼パス**
Assurance Requirements			

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST Introduction** ST Introduction	SA-4	**調達プロセス**
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Conformance Claims** Conformance Claims	PL-2	**システムセキュリティ計画**
		SA-4 (7)	**調達プロセス** NIAP 認定の保護プロファイル
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition	PL-2	**システムセキュリティ計画**
		SA-4	**調達プロセス**
ASE_OBJ.1 EAL1	**Security Objectives** Security Objectives for the Operational Environment	PL-2	**システムセキュリティ計画**
		SA-4	**調達プロセス**
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Objectives** Security Objectives	PL-2	**システムセキュリティ計画**
		SA-4	**調達プロセス**
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Extended Components Definition** Extended Components Definition	（対応するものがない）.	
ASE_REQ.1 EAL1	**Security Requirements** Stated Security Requirements	PL-2	**システムセキュリティ計画**
		SA-4	**調達プロセス**
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Requirements** Derived Security Requirements	PL-2	**システムセキュリティ計画**
		SA-4	**調達プロセス**
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**TOE Summary Specification** TOE Summary Specification	PL-2	**システムセキュリティ計画**
		SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
ASE_TSS.2	**TOE Summary Specification**	PL-2	**システムセキュリティ計画**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
	TOE Summary Specification with Architectural Design Summary	SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ADV_ARC.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Architecture** Security Architecture Description	AC-25	**リファレンスモニタ**
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
		SA-18	**改ざんの防止と検知**
		SC-3	**セキュリティ機能の分離**
		SC-3 (1)	**セキュリティ機能の分離** ハードウェアの分離
		SC-3 (2)	**セキュリティ機能の分離** 非セキュリティ機能の数を最小限に抑える
		SC-41	**ポートおよび入出力装置に対するアクセス**
ADV_FSP.1 EAL1	**Functional Specification** Basic Functional Specification	SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
ADV_FSP.2 EAL2	**Functional Specification** Security-Enforcing Functional Specification	SA-4(1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_FSP.3 EAL3	**Functional Specification** Functional Specification With Complete Summary	SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_FSP.4 EAL4	**Functional Specification** Complete Functional Specification	SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_FSP.5 EAL5 EAL6	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Error Information	SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_FSP.6 EAL7	**Functional Specification** Complete Semi-Formal Functional Specification with Additional Formal Specification	SA-4 (1)	**調達プロセス** セキュリティ管理策の機能特性
		SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17 (3)	**開発者によるセキュリティアーキテクチャおよび設計** 形式的なコレスポンデンス
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_IMP.1 EAL4 EAL5	**Implementation Representation** Implementation Representation of the TSF	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
ADV_IMP.2 EAL6 EAL7	**Implementation Representation** Complete Mapping of the Implementation Representation of the TSF	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17 (3)	**開発者によるセキュリティアーキテクチャおよび設計** 形式的なコレスポンデンス
ADV_INT.1	**TSF Internals** Well-Structured Subset of TSF Internals	SA-8	**セキュリティエンジニアリング原則**
		SC-3 (3)	**セキュリティ機能の分離** 非セキュリティ機能の数を最小限に抑える
		SC-3 (4)	**セキュリティ機能の分離** モジュールの結合度と凝集度
		SC-3 (5)	**セキュリティ機能の分離** 重層構造
ADV_INT.2 EAL5	**TSF Internals** Well-Structured Internals	SA-8	**セキュリティエンジニアリング原則**
		SC-3 (3)	**セキュリティ機能の分離** 非セキュリティ機能の数を最小限に抑える
		SC-3 (4)	**セキュリティ機能の分離** モジュールの結合度と凝集度
		SC-3 (5)	**セキュリティ機能の分離** 重層構造
ADV_INT.3 EAL6 EAL7	**TSF Internals** Minimally Complex Internals	SA-8	**セキュリティエンジニアリング原則**
		SA-17 (5)	**開発者によるセキュリティアーキテクチャおよび設計** 概念的にシンプルな設計
		SC-3 (3)	**セキュリティ機能の分離** 非セキュリティ機能の数を最小限に抑える
		SC-3 (4)	**セキュリティ機能の分離** モジュールの結合度と凝集度
		SC-3 (5)	**セキュリティ機能の分離** 重層構造
		AC-25	**リファレンスモニタ**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
ADV_SPM.1 EAL6 EAL7	**Security Policy Modeling** Formal TOE Security Policy Model	SA-17 (1)	**開発者によるセキュリティアーキテクチャおよび設計** 形式的なポリシーモデル
		SA-17 (3)	**開発者によるセキュリティアーキテクチャおよび設計** 形式的なコレスポンデンス
ADV_TDS.1 EAL2	**TOE Design** Basic Design	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ADV_TDS.2 EAL3	**TOE Design** Architectural Design	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ADV_TDS.3 EAL4	**TOE Design** Basic Modular Design	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ADV_TDS.4 EAL5	**TOE Design** Semiformal Modular Design	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
		SA-17 (2)	**開発者によるセキュリティアーキテクチャおよび設計** セキュリティ関連のコンポーネント
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_TDS.5 EAL6	**TOE Design** Complete Semiformal Modular Design	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
		SA-17 (2)	**開発者によるセキュリティアーキテクチャおよび設計** セキュリティ関連のコンポーネント
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
ADV_TDS.6 EAL7	**TOE Design** Complete Semiformal Modular Design with Formal High-Level Design Presentation	SA-4 (2)	**調達プロセス** セキュリティ管理策の設計 / 導入に関する情報
		SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
		SA-17 (2)	**開発者によるセキュリティアーキテクチャおよび設計** セキュリティ関連のコンポーネント
		SA-17 (3)	**開発者によるセキュリティアーキテクチャおよび設計** 形式的なコレスポンデンス

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		SA-17 (4)	**開発者によるセキュリティアーキテクチャおよび設計** 非形式的なコレスポンデンス
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Operational User Guidance** Operational User Guidance	SA-5	**情報システム文書**
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Preparative Procedures** Preparative Procedures	SA-5	**情報システム文書**
ALC_CMC.1 EAL1	**CM Capabilities** Labeling of the TOE	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMC.2 EAL2	**CM Capabilities** Use of a CM System	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMC.3 EAL3	**CM Capabilities** Authorization Controls	CM-3	**構成変更管理**
		CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMC.4 EAL4 EAL5	**CM Capabilities** Production Support, Acceptance Procedures, and Automation	CM-3	**構成変更管理**
		CM-3 (1)	**構成変更管理** 変更を自動で文書化/ 報告 /禁止する
		CM-3 (3)	**構成変更管理** 変更を自動で実施する
		CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMC.5 EAL6 EAL7	**CM Capabilities** Advanced Support	CM-3	**構成変更管理**
		CM-3 (1)	**構成変更管理** 変更を自動で文書化/ 報告 /禁止する
		CM-3 (2)	**構成変更管理** 変更をテスト / 承認 / 文書化する
		CM-3 (3)	**構成変更管理** 変更を自動で実施する
		CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMS.1 EAL1	**CM Scope** TOE CM Coverage	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMS.2 EAL2	**CM Scope** Parts of the TOE CM Coverage	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMS.3 EAL3	**CM Scope** Implementation Representation CM Coverage	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
ALC_CMS.4 EAL4	**CM Scope** Problem Tracking CM Coverage	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_CMS.5 EAL5 EAL6 EAL7	**CM Scope** Development Tools CM Coverage	CM-9	**構成管理計画**
		SA-10	**開発者による構成管理**
ALC_DEL.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Delivery** Delivery Procedures	MP-5	**媒体の移動**
		SA-10 (1)	**開発者による構成管理** ソフトウェア / ファームウェアの完全性検証
		SA-10 (6)	**開発者による構成管理** 信頼できる配布
		SA-18	**改ざんの防止と検知**
		SA-19	**コンポーネントの真正性**
ALC_DVS.1 EAL3 EAL4 EAL5	**Development Security** Identification of Security Measures	SA-1	**システムおよびサービスの調達のポリシーと手順**
		SA-3	**システム開発ライフサイクル**
		SA-12	**サプライチェーンの保護**
ALC_DVS.2 EAL6 EAL7	**Development Security** Sufficiency of Security Measures	CM-5	**変更に対するアクセス制限**
		SA-3	**システム開発ライフサイクル**
		SA-12	**サプライチェーンの保護**
ALC_FLR.1	**Flaw Remediation** Basic Flaw Remediation	SA-10	**開発者による構成管理**
		SA-11	**開発者によるセキュリティテストおよび評価**
		SI-2	**欠陥の修正**
ALC_FLR.2	**Flaw Remediation** Flaw Reporting Procedures	SA-10	**開発者による構成管理**
		SA-11	**開発者によるセキュリティテストおよび評価**
		SI-2	**欠陥の修正**
ALC_FLR.3	**Flaw Remediation** Systematic Flaw Remediation	SA-10	**開発者による構成管理**
		SA-11	**開発者によるセキュリティテストおよび評価**
		SI-2	**欠陥の修正**
ALC_LCD.1 EAL3 EAL4 EAL5 EAL6	**Life-Cycle Definition** Developer Defined Life-Cycle Model	SA-3	**システム開発ライフサイクル**
		SA-15	**開発プロセス、標準、およびツール**
ALC_LCD.2 EAL7	**Life-Cycle Definition** Measurable Life-Cycle Model	SA-3	**システム開発ライフサイクル**
		SA-15	**開発プロセス、標準、およびツール**
ALC_TAT.1 EAL4	**Tools and Techniques** Well-Defined Development Tools	SA-15	**開発プロセス、標準、およびツール**
ALC_TAT.2 EAL5	**Tools and Techniques** Compliance with Implementation Standards	SA-15	**開発プロセス、標準、およびツール**
ALC_TAT.3 EAL6 EAL7	**Tools and Techniques** Compliance with Implementation Standards – All Parts	SA-15	**開発プロセス、標準、およびツール**
ATE_COV.1 EAL2	**Coverage** Evidence of Coverage	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
ATE_COV.2 EAL3 EAL4 EAL5	**Coverage** Analysis of Coverage	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する
ATE_COV.3 EAL6 EAL7	**Coverage** Rigorous Analysis of Coverage	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する
ATE_DPT.1 EAL3	**Depth** Testing: Basic Design	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する
ATE_DPT.2 EAL4	**Depth** Testing: Security Enforcing Modules	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する
ATE_DPT.3 EAL5 EAL6	**Depth** Testing: Modular Design	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する
ATE_DPT.4 EAL7	**Depth** Testing: Implementation Representation	SA-11	**開発者によるセキュリティテストおよび評価**
		SA-11 (7)	**開発者によるセキュリティテストおよび評価** テスト / 評価の範囲を確認する
ATE_FUN.1 EAL2 EAL3 EAL4 EAL5	**Functional Tests** Functional Testing	SA-11	**開発者によるセキュリティテストおよび評価**
ATE_FUN.2 EAL6 EAL7	**Functional Tests** Ordered Functional Testing	SA-11	**開発者によるセキュリティテストおよび評価**
ATE_IND.1 EAL1	**Independent Testing** Independent Testing – Conformance	CA-2	**セキュリティアセスメント**
		CA-2 (1)	**セキュリティアセスメント** 独立性を有するアセサー
		SA-11 (3)	**開発者によるセキュリティテストおよび評価** アセスメント計画 / エビデンスの独立検証
ATE_IND.2 EAL2 EAL3 EAL4 EAL5 EAL6	**Independent Testing** Independent Testing – Sample	CA-2	**セキュリティアセスメント**
		CA-2 (1)	**セキュリティアセスメント** 独立性を有するアセサー
		SA-11 (3)	**開発者によるセキュリティテストおよび評価** アセスメント計画 / エビデンスの独立検証
ATE_IND.3 EAL7	**Independent Testing** Independent Testing – Complete	CA-2	**セキュリティアセスメント**
		CA-2 (1)	**セキュリティアセスメント** 独立性を有するアセサー
		SA-11 (3)	**開発者によるセキュリティテストおよび評価** アセスメント計画 / エビデンスの独立検証
AVA_VAN.1 EAL1	**Vulnerability Analysis** Vulnerability Survey	CA-2 (2)	**セキュリティアセスメント** 特殊なアセスメント
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
		SA-11 (2)	**開発者によるセキュリティテストおよび評価** 脅威分析と脆弱性分析 / 欠陥の修正
		SA-11 (5)	**開発者によるセキュリティテストおよび評価** 侵入テスト
AVA_VAN.2 EAL2 EAL3	**Vulnerability Analysis** Vulnerability Analysis	CA-2 (2)	**セキュリティアセスメント** 特殊なアセスメント
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11 (2)	**開発者によるセキュリティテストおよび評価** 脅威分析と脆弱性分析 / 欠陥の修正
		SA-11 (5)	**開発者によるセキュリティテストおよび評価** 侵入テスト
AVA_VAN.3 EAL4	**Vulnerability Analysis** Focused Vulnerability Analysis	CA-2 (2)	**セキュリティアセスメント** 特殊なアセスメント
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11 (2)	**開発者によるセキュリティテストおよび評価**脅威分析と脆弱性分析 / 欠陥の修正
		SA-11 (5)	**開発者によるセキュリティテストおよび評価** 侵入テスト
AVA_VAN.4 EAL5	**Vulnerability Analysis** Methodical Vulnerability Analysis	CA-2 (2)	**セキュリティアセスメント** アセスメントタイプ
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11 (2)	**開発者によるセキュリティテストおよび評価**脅威分析と脆弱性分析 / 欠陥の修正
		SA-11 (5)	**開発者によるセキュリティテストおよび評価** 侵入テスト
AVA_VAN.5 EAL6 EAL7	**Vulnerability Analysis** Advanced Methodical Vulnerability Analysis	CA-2 (2)	**セキュリティアセスメント** アセスメントタイプ
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11 (2)	**開発者によるセキュリティテストおよび評価**脅威分析と脆弱性分析 / 欠陥の修正
		SA-11 (5)	**開発者によるセキュリティテストおよび評価** 侵入テスト
ACO_COR.1	**Composition Rationale** Composition Rationale	SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ACO_DEV.1	**Development Evidence** Functional Description	SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ACO_DEV.2	**Development Evidence** Basic Evidence of Design	SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ACO_DEV.3	**Development Evidence** Detailed Evidence of Design	SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ACO_REL.1	**Reliance on Dependent Component** Basic Reliance Information	SA-17	**開発者によるセキュリティアーキテクチャおよび設計**

ISO/IEC 15408の要求事項		この文書に記載されたセキュリティ管理策	
ACO_REL.2	**Reliance on Dependent Component** Reliance Information	SA-17	**開発者によるセキュリティアーキテクチャおよび設計**
ACO_CTT.1	**Composed TOE Testing** Interface Testing	SA-11	**開発者によるセキュリティテストおよび評価**
ACO_CTT.2	**Composed TOE Testing** Rigorous Interface Testing	SA-11	**開発者によるセキュリティテストおよび評価**
ACO_VUL.1	**Composition Vulnerability Analysis** Composition Vulnerability Review	CA-2	**セキュリティアセスメント**
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11	**開発者によるセキュリティテストおよび評価**
ACO_VUL.2	**Composition Vulnerability Analysis** Composition Vulnerability Analysis	CA-2	**セキュリティアセスメント**
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11	**開発者によるセキュリティテストおよび評価**
ACO_VUL.3	**Composition Vulnerability Analysis** Enhanced-Basic Composition Vulnerability Review	CA-2	**セキュリティアセスメント**
		CA-8	**侵入テスト**
		RA-3	**リスクアセスメント**
		SA-11	**開発者によるセキュリティテストおよび評価**

付録 I

オーバーレイテンプレート

特殊な状況に対応するために、またはコミュニティ全体にわたる利用のために、調整に関するガイダンスを適用する[116]

組織は、「オーバーレイ」の概念を用いて調整されたベースラインを策定する際に、以下のテンプレート（以下、このテンプレート）を使用できる[117]。このテンプレートは、あくまでも例を示すためのものであり、組織は、組織のニーズや策定するオーバーレイのタイプに応じて、他のフォーマットを使用したり、この付録のフォーマットを修正してもよい。オーバーレイの詳細レベルは、オーバーレイを開始する組織の自由裁量による。ただし、策定される調整されたベースライン管理策について適切な根拠と理由を示すのに十分な幅と深さを有することが求められる（オーバーレイの策定プロセスにおける、リスク情報を活用した意思決定を含む）。「オーバーレイ」の概念を用いたセキュリティ管理策のベースライン管理策の調整は、運用認可責任者の承認の対象となるセキュリティ計画の作成につながる。このテンプレートは、以下の 8 つのセクションで構成される：

- 指定
- オーバーレイの特徴
- 適用性
- オーバーレイの概要
- オーバーレイ管理策の詳細仕様
- 調整に関する考慮事項
- 定義
- 追加情報または指示

オーバーレイは、どのように使用できるか

リスクマネジメントフレームワーク（以下、RMF）において、オーバーレイはセクション 3.1 や、組織に特化した手引きに記載されている初期のセキュリティ分類プロセスが完了した後の、調整プロセスの一環として実施される。セキュリティ分類プロセスは、情報システムの影響レベルの特定につながり、その後、このセキュリティ管理策の付録 D のベースライン管理策から、開始点としてのセキュリティ管理策の一式を選択するのに使用される[118]。開始点としてのセキュリティ管理策一式が選択された後は、組織は、組織内の特定の状況により一層沿うようにセキュリティ管理策を修正・調整するための、調整プロセスを開始する。オーバーレイは、特殊な要求

[116] 「オーバーレイ」の概念を用いて生成された、調整されたベースラインは、さまざまな現場や刊行物（例：OMB ポリシー、CNSS Instructions、NIST Special Publications、業界標準、業界に特化した手引き）を介して発行される。オーバーレイの取組の一環として、付録 I の産業用制御システムとプロセス制御システムのセキュリティに関する旧版の手引きは、NIST Special Publication 800-82 に記載される予定である。

[117] 組織には、「オーバーレイ」の概念を用いてセキュリティ管理策ベースラインを調整することが推奨されるが、同じトピックに対して発散的なオーバーレイを生成することは、逆効果を生じさせる可能性がある。オーバーレイの概念が最も効果的になるのは、利益共同体が連携して、重複のない、合意に基づくオーバーレイを作成する時である。

[118] CNSS Instruction 1253 は、国家安全保障に関わるシステムに対するセキュリティ分類の手引きであると同時に、そうしたシステムに導入できるセキュリティ管理策ベースラインを規定している。

事項、ミッション／業務機能、テクノロジーまたは環境に対応するための、コミュニティ全体にわたる視点からの調整に関するガイダンスを提供する。オーバーレイは、情報システムの導入と維持管理に責任のあるシステム所有者に対して、セキュリティの専門家と、その他の主題の専門家によって策定された調整オプションを提供することによって、セキュリティ管理策選択の一様性と効率をもたらす。

オーバーレイを策定するのに使用できるオプションは広範囲にわたり、オーバーレイを策定する者は、自身が求める特異性に応じて選択できる。オーバーレイによっては、情報システムの主要コンポーネントや、それらのシステムが稼働する環境を形成するハードウェア、ファームウェア、ソフトウェアに関して、非常に具体的であったり、異なる環境に実装される大きなクラスの情報システムに適用できるよう、より抽象的であったりする。以下に示すテンプレートは、オーバーレイの一連の運用上のあらゆるレベルの特異性に対応する。

「特異性」が高いオーバーレイは、通常は、情報システムの所有者や運用環境に対する管理権限を有する組織によって策定される。組織は、セクション 3.2 に記載されているように、選択されたセキュリティ管理策ベースラインに対して、適切な調整活動を定める。特定の情報システムにオーバーレイを使用することを許す変数や条件の多くは、オーバーレイを適用する際の一貫性を確保するためにも、明確に示される。「特異性」がより低いオーバーレイは、大きなクラスの情報システムに適用する場合や、そのシステムの具体的な実施詳細について十分な情報が得られない場合には、セキュリティの専門家や、他の主題の専門家によって策定されることもある。「特異性」がより低いオーバーレイは、特定の情報システムに導入されるセキュリティ管理策一式をカスタマイズする場合など、追加の調整を必要とする場合がある。これらのオーバーレイでは、セキュリティ管理策内の「指定」ステートメントと「選択」ステートメント（すなわち、管理策の変数可変部分）の多くが、その情報システムを所有・運用する組織によって設定される。以下に、オーバーレイを構成する 8 つのセクションについて説明する。

指定

組織は、以下を用意して、オーバーレイを指定する：①オーバーレイの一意の名称②バージョン番号と日付③オーバーレイの策定に使用された NIST Special Publication 800-53 のバージョン④オーバーレイの策定に使用された他のドキュメント⑤著者または著者グループと、連絡先ならびに⑤どのタイプの承認を得たか。組織は、オーバーレイの有効期間と、NIST Special Publication 800-53 に対する変更や、組織に特化したセキュリティガイダンスの変更以外で、オーバーレイの更新を誘発するイベントを定義する。オーバーレイの更新を誘発する一意のイベントが存在しない場合、その旨をこのセクションに記載する。

オーバーレイの特徴

組織は、ユーザが自身のミッション／業務機能に最も適したオーバーレイを選択できるよう、オーバーレイの使用目的を定義する特徴について記述する。これは、例えば、以下についての記述を含む：①その情報システムが使用される予定の環境（例：アメリカ合衆国本土内の、保護された建物の中、無人宇宙船の中、機微情報または機密情報に対するアクセスを試みていることが判明している外国に出張中に、敵意を抱いているエンティティに接近している移動車両の中）②処理・保存・または伝送される予定の情報のタイプ（例：個人の識別情報と認証情報、財務管理情報・施設、海軍、設備管理情報、防衛情報および国家安全保障に関わる情報、システム開発情報）(iii)情報システムまたは、システムの一種（例：スタンドアロン型システム、産業用制御システム／プロセス制御システム、ドメインを跨ぐシステム）内の機能ならびに(iv)第

3 章に記載されている想定に含まれない一連の脅威から組織のミッション／業務機能、情報システム、情報、または個人を保護するのに役立つ、オーバーレイ に関連するその他の特徴。

適用性

組織は、特定の情報システム、または運用環境にオーバーレイが適用可能かどうかをユーザが判断しやすくするための判断基準を定める。典型的なフォーマットには、例えば、情報システム（関連するアプリケーションを含む）と、そのシステムが稼動する環境の特徴について、オーバーレイに適切なレベルの特異性をもって記述した質問リストや決定木がある。

オーバーレイの概要

組織は、オーバーレイの顕著な特徴について概要を示す。この概要は、たとえば、以下を含む：①オーバーレイの影響を受けるセキュリティ管理策と拡張管理策②オーバーレイ、セクション 3.2 に記載されている調整に関するガイダンス、または組織に特化した手引きの特徴や想定に基づいて、どのセキュリティ管理策／拡張管理策が選択され、どの管理策／拡張管理策が選択されないかを示すこと③新しい補足的ガイダンスやパラメータ値を含む、選択された管理策／拡張管理策ならびに④該当する連邦法・大統領命令・指令・指示・規制・政策のいずれかの標準の参照。

オーバーレイ管理策の詳細仕様

組織は、調整プロセスの一環として、オーバーレイ内のセキュリティ管理策／拡張管理策についての包括的に示す。これは、例えば、以下を含む：①特定のセキュリティ管理策／拡張管理策を選択する（選択しない）理由②オーバーレイや、オーバーレイを稼働させる予定の環境の特徴に対処するためのセキュリティ管理策／拡張管理策の補足的ガイダンスに対する変更、または新しい補足的ガイダンスの追加③セキュリティ管理策の「選択」ステートメントまたは「指定」ステートメントの一意のパラメータ値④セキュリティ管理策または拡張管理策が満たすべき具体的な法的要件および／または規制上の要件（FISMA の他に）⑤推奨される補完的管理策（必要に応じて）ならびに⑥追加機能の指定、メカニズムの強度の変更、実装オプションの追加または制限によって、管理策／拡張管理策の基本的な機能を拡張するための手引き。

調整に関する考慮事項

組織は、特定の情報システムに適用可能なセキュリティ管理策の一式を選択する際に、情報システム所有者と運用環境が調整プロセスにおいて考慮すべき情報を提供する。これは、オーバーレイが、選択されたセキュリティ管理策ベースライン管理策（セクション 3.1 に記載されているように）が想定する運用環境は異なる運用環境で利用される場合には、特に重要である。また、組織は、セキュリティ管理策ベースラインに対する複数のオーバーレイの使用に関する手引きを用意することで、オーバーレイの仕様とベースライン管理策との間で浮上する衝突に対処できるようになる。

定義

組織は、オーバーレイに固有の、関連する用語とそれらの定義を示す。用語と定義は、アルファベット順に記載する。オーバーレイに固有の用語または定義が存在しない場合は、その旨を本セクションに記載する。

追加情報または指示

組織は、前のセクションで扱っていないオーバーレイに関連する、追加の情報または指示を用意する。

付録 J

プライバシー管理策カタログ

プライバシー管理策、拡張管理策、および補足的ガイダンス

個人のプライバシーを保護する必要性は、政府の国民から情報を収集する必要性と、国民が情報がどのように使用・収集・維持管理され、必要な使用期間が過ぎたら廃棄されるかについて知らされる権利との、バランスを取るが要求され Privacy Act が制定された 1974 年と同様に、現在も重要になっている。これらの課題は、ヘルスケアサービス、金融サービス、その他のサービスがウェブを介して提供され、そうしたサービスの個人化が進んでいる民間部門でも共有されている。ソーシャルメディア・スマートグリッド・モバイル・クラウドコンピューティングの普及と、構造化されたデータ／メタデータ環境から、構造化されていないデータ／メタデータ環境への移行により、連邦政府組織にとってはプライバシーを保護することが非常に複雑かつ困難になっている。こうした課題は、機密性の確保に焦点を当てたプライバシー保護といった従来の IT セキュリティ視点を優に超えている。今日、個人の情報の完全性を管理し、個人の情報がオンデマンドで利用できるようにすることの重要性が増している。連邦政府は、情報セキュリティの範囲を超えるプライバシーに関する国民の期待に応えるためにも、プライバシーに対する視野を広げる必要がある。

個人情報[119]のプライバシーは、適切な法律・政策・手順・要求事項を満たすのに必要な管理策なしでは得られない基本的価値観である。個人のプライバシーと、プログラムや情報システムによって収集・使用・維持管理・共有・廃棄される彼らの個人情報を保護することは、連邦政府組織の基本的な責任である。また、プライバシーには、個人情報の共有を許すか否か、共有する時期、共有する情報の量、共有を許す状況について、各人が決定する権利が含まれる。今日のデジタル世界では、個人の効果的なプライバシーは、個人情報を処理・保存・伝送する情報システムと、それらのシステムが稼働する環境に導入される保護対策に依存する。情報セキュリティの基盤が無ければ、効果的なプライバシーは実現できない。プライバシーは、例えば、透明性・通知・選択の自由といった原則を含むため、単にセキュリティにとどまらない。

この付録は、プライバシーを保護するための構造化された管理策一式を示すものであり、個人情報（紙面上であるか、あるいは電子的形態であるかにかかわらず）のライフサイクル全体に関わるプライバシー管理策を選択し、導入する際に使用できる、ロードマップとなる。これらの管理策は、情報セキュリティとは異なるものの、高度に相関する価値として、情報プライバシ

[119] OMB Memorandum 07-16 は、個人情報を以下のように定義している：「個人の身元の識別や追跡に使用できる情報。そうした情報には、氏名、社会保障番号、生体記録のように、単独で特定の個人に結びつくものもあれば、生年月日と出生地、母親の旧姓などの他の個人情報または識別情報との組み合わせによって、特定の個人に結びつくものもある。」OMB Memorandum 10-22 は、さらに、「「個人情報」の定義は、単一のカテゴリーの情報またはテクノロジーに限定されるわけではない。むしろ、データ要素の使用または組み合わせを調べることによって個人が特定されてしまうリスクを、ケースバイケースでアセスメントすることを要求する。このアセスメントを実施する際には、個人情報でない情報が個人情報になりうることを政府機関が認識する事が重要である。具体的には、追加の情報が媒体や情報源を介して一般の人に渡った場合、その情報と他の利用可能な情報との組み合わせにより、個人が特定される可能性がある」と述べている。NIST Special Publication 800-122 は、本付録とは異なる、広い意味でプライバシーではなく機密性に焦点を当てた、「個人情報」の定義を記載している。組織の「個人情報」の定義は、考慮すべき追加の規制上の要件によって大きく変わるだろう。本付録のプライバシー管理策は、組織が「個人情報」をどのように定義するかにかかわらず、適用される。

ーに焦点を当てている。プライバシー管理策は、個人情報を保護し、適切に取り扱うために組織に導入される管理面、技術面、物理面での保護対策である[120]。組織は、個人情報の収集と使用を伴わない活動に携わることもあるが、それでもプライバシー問題や関連リスクは浮上する。プライバシー管理策は、そうした活動にも同様に適用され、プライバシーリスクを分析し、必要に応じてそうしたリスクを低減するために使用される。

この付録のプライバシー管理策は、1974 年に施行された Privacy Act、2002 に施行された E-Government Act のセクションに 208、および OMB ポリシーに含まれる FIPPs（Fair Information Practice Principles）[121]に基づいている。FIPPs は組織のプライバシー対策に対する国民の信頼を得ることと、組織がプライバシーインシデントによる目に見えるコストと、目に見えない被害を避けるのを支援することを目的としている。プライバシー管理策ファミリは、全部で 8 つであり、各ファミリは FIPPs のいずれかに対応する。プライバシーファミリは、政府機関の上級プライバシー責任者(SAOP)／最高プライバシー責任者(CPO)[122]の指揮と監督の下に、かつ、最高情報セキュリティ責任者・最高情報責任者・プログラム責任者・弁護士等の他関係者と連携して、組織レベル・省庁レベル・政府機関レベル・コンポーネントレベル・オフィスレベル・プログラムレベル・情報システムレベルのいずれかでで実施される。表 J-1 は、プライバシー管理策カタログ内のプライバシー管理策の概要を、セキュリティ管理策ファミリごとにまとめて記載している。

表 J-1: プライバシー管理策の概要（ファミリ別）

ID	プライバシー管理策
AP	**権限と目的**
AP-1	収集する権限
AP-2	目的を明確にする
AR	**説明責任、監査、およびリスクマネジメント**
AR-1	ガバナンスおよびプライバシープログラム
AR-2	プライバシー影響アセスメントとリスクアセスメント
AR-3	受託業者とサービスプロバイダに対するプライバシー要求事項
AR-4	プライバシーモニタリングおよびチェック
AR-5	プライバシー意識向上およびトレーニング
AR-6	プライバシー報告
AR-7	プライバシーを強化したシステム設計および開発

[120] 2010 年に、Federal CIO Council Privacy Committee は「*Best Practices: Elements of a Federal Privacy Program (Elements White Paper)*」と題する、プライバシープログラムを設計・実施するためのフレームワークを発行した。本付録のプライバシー管理策は、そのホワイトペーパーに記載されている多くの要素を取り入れている。組織は、そのホワイトペーパーに記載されているプライバシー管理策と手引きを使用して、組織全体にわたるプライバシープログラムを立ち上げたり、既存のプログラムを強化することができる

[121] FIPPsはプライバシーの一般的なフレームワークとして、アメリカ合衆国のみならず、国際的に広く受け入れられていて、連邦政府の法律やポリシーと、国際的な法律やポリシーに反映されている。多くの組織にとって、FIPPsはプライバシーリスクを分析し、適切な軽減戦略を決定する上で、基盤としての役割を果たす。FEA-SPP (Federal Enterprise Architecture Security and Privacy Profile)も、プライバシー管理策の策定に関する情報と資料を提供している。

[122] 連邦政府の各省と機関は、情報プライバシー問題に責任のある上級職員として、SAOP/CPO を任命している。OMB Memorandum 05-08 は、SAOPs/CPOs の任命に関する手引きである。本付録で使用されている「SAOP/CPO」という用語は、組織の上級プライバシーリーダーを指していて、その肩書は組織ごとに大きく異なる。

ID	プライバシー管理策
AR-8	開示についての説明
DI	**データの品質と完全性**
DI-1	データの品質
DI-2	データの完全性と、データ完全性委員会
DM	**データの最小化と保持**
DM-1	個人情報の最小化
DM-2	データの保持と廃棄
DM-3	テスト、トレーニング、調査における個人情報の使用を最小限に抑える
IP	**個人による参加と、個人の救済**
IP-1	同意
IP-2	個人によるアクセス
IP-3	救済
IP-4	苦情に対処する
SE	**セキュリティ**
SE-1	個人情報一覧
SE-2	プライバシーインシデント対応
TR	**透明性**
TR-1	プライバシーに関する通知
TR-2	記録システムによる通知と、Privacy Act の記述
TR-3	プライバシープログラム情報の配布
UL	**使用制限**
UL-1	内部使用
UL-2	第三者と情報を共有する

この付録のプライバシー管理策の構造と、この文書の付録 F および同付録 G のセキュリティ管理策の構造には、強い類似性がある。たとえば、管理策 AR-1 (Governance and Privacy Program)は、組織に対して、組織レベルまたはプログラムレベルで実施可能なプライバシー計画を策定することを求めている。これらの計画は、セキュリティ計画と共に使用することができ、その場合、組織のミッション／業務上の要求事項に加えて、組織が業務を行う環境に応じて適切なセキュリティ／プライバシー管理策の一式を選択する機会が組織に与えられる。情報セキュリティリスクの管理に用いられる基本概念を取り入れることで、遵守要件を満たすことができ、プライバシー管理策をリスクに基づいて費用対効果がより高くなるように実施できるようになる。標準化されたプライバシー管理策とアセスメント手順（管理策の有効性の評価のために策定される）は、組織が連邦政府のプライバシー要求事項を満たし、それらの要求事項に遵守していることを示すための、より統制のとれた構造化されたアプローチを提供する。

プライバシーに関する付録は、いつくかの重要な目的を果たす。この付録は:

- 該当する連邦法・大統領命令・指令・指示・規制・政策・標準・指針・組織の発令に組織が遵守するのを支援するベストプラクティスに基づいて構造化されたプライバシー管理策一式を掲載している
- 連邦政府の情報システム・プログラム・組織内で概念上や実施において重複する可能性のあるプライバシー要求事項とセキュリティ要求事項を満たすために、プライバシー管理策とセキュリティ管理策とのつながりと関係を確立する

- 連邦政府の情報システムならびにプログラムおよび組織に導入されるプライバシー管理策を選択・導入・評価・（継続的に）モニタリングする際に NIST リスクマネジメントフレームワークが適用できることを示す
- 連邦政府が制定したプライバシーに関する法律・政策・規制・指令・標準・ガイドライン要求事項を満たすといったシニアリーダー／上級管理者の目的が達成されるよう、連邦政府内のプライバシーに関わる職員とセキュリティに関わる職員との緊密な連携を促進する。

この付録の使い方

この文書に記載されているプライバシー管理策は、主に組織の SAOP/CPO によって使用されることを想定している。具体的には、SAOP/CPO がプログラムマネージャ、情報所有者／スチュワード、最高情報責任者、最高情報セキュリティ責任者、情報システム開発者／インテグレータ、リスクエグゼクティブと連携して、効果的なプライバシー保護およびプラクティス（すなわち、プライバシー管理策）をいかにしてうまく組織のプログラム、情報システム、それらのシステムが稼働する環境に組み入れるかを決定する際に使用する。プライバシー管理策は、個人情報について収集・使用・維持管理・共有・廃棄のいずれかを行う組織のプログラムやシステムに影響を与えるプライバシー要求事項を満たすための、組織の取組を容易にする。この文書の付録 F のセキュリティ管理策は、同じくこの文書の付録 D の低位、中程度の、高位ベースラインのいずれかに割り当てられる。一方、プライバシー管理策は、政府が制定した法律・ポリシー・指示・規制・ガイドライン・ベストプラクティスのうちプライバシーに関するものに従って、組織のプライバシー要求事項と、組織の情報システムやプログラムによって収集・維持管理される各人の個人情報を保護する必要性に基づいて選択・導入される。

組織は、法的権限と法律上と義務に基づいて、それぞれのミッション／業務ニーズと運用ニーズを満たせるよう、各プライバシー管理策を分析・適用する。導入すべきプライバシー管理策は、この分析の結果に応じて変わる（例：HIPAA (Health Insurance Portability and Accountability Act) に従って「保護されたエンティティ」として定義された組織には、この文書に列挙されていない追加の要求事項が課せられる。）この分析により、組織は法律やポリシーに準拠した情報プラクティスがレビューとともに必要な情報プラクティスを特定できるようになる。また、この分析により、組織は定義された具体的なニーズを組織レベル、ミッション／業務プロセスレベル、情報システムレベルで満たすために、プライバシー管理策を調整できるようになる。国家安全保障に関わる組織と捜査当局は、彼らの環境にどのようにしてプライバシー管理策を適用するかを決定する際に、それらの権限とプライバシー影響を考慮する。同様に、CIPSEA（Confidential Information Protection and Statistical Efficiency Act）の対象になる組織は、CIPSEA に適合するプライバシー管理策を導入する。すべての組織は、1974 に施行された Privacy Act、5 U.S.C. § 552a に適合するプライバシー管理策を導入する。ただし、例外や免除を受けられる場合がある。

この文書の付録 J に記載されているプライバシー管理策の拡張管理策セクションには、組織が成し遂げようと努力すべきベストプラクティスを記述しているが、必須ではない。組織は、どのような場合に、組織の特定のミッション／業務機能を支援するために拡張管理策を適用するかについて定める。セクション 3.2 と付録 I の手引きに従って策定される、プライバシー用のオーバーレイは、セキュリティ要求事項とプライバシー要求事項の両方が組織によって満たされるよう、付録のセキュリティ管理策のベースライン管理策を必要なプライバシー管理策をもって調整するのを容易にする。この文書の付録 F のセキュリティ管理策の多くは、組織の情報システムとそれらのシステムが稼働する環境における情報の機密性・完全性・可用性を保護するための基本的な情報保護、すなわち、強固で効果的なプライバシーを確保するのに不可欠な保護を提供する。

組織は、組織のプログラムや情報システム、それらのシステムが稼働する環境に導入される予定の、合意がなされたプライバシー管理策について文書化する。プライバシー管理策は、管理策を導入する組織の自由裁量により、個別のプライバシー計画に記載されたり、リスクマネジメントに関するその他のドキュメント（例：システムセキュリティ計画）に記載されたりする。組織は、また、プライバシー管理策どの程度正しく導入されているか、どの程度意図した通りに運用されているか、および指定されたプライバシー要求事項に対する適合性の観点から所望の結果をどの程度産出しているかを判断するための、適切なアセスメント方法を確立する。プライバシー管理策の評価は、SAOP/CPO が単独で実施する場合もあれば、情報セキュリティ責任者など、その他のリスクマネジメント責任者と共同で実施する場合もある。

導入に関するヒント

- 組織のプライバシー要求事項と、システムやプログラムによって収集・維持管理される各人の個人情報を保護する必要性に基づいて、プライバシー管理策を選択・導入する事
- 組織のリスクエグゼクティブ機能、ミッション／業務遂行の責任者、エンタープライズアーキテクチャ、最高情報責任者、SAOP/CPO、および最高情報セキュリティ責任者との間で、プライバシー管理策の選択と導入を調整する事
- この文書の付録 J のプライバシー管理策を付録 G の PM 管理策と同じ視点でとらえる事。すなわち、プライバシー管理策が、組織のそれぞれの情報システムに対して、システムの FIPS 199 分類のいかんにかかわらず導入される事を意味する。
- 個人や個人情報に対して、追加のプライバシー保護の必要性が示された場合には、任意の拡張管理策を選択・実施する。
- 法律・大統領命令・指令・政策・規制に含まれる例外や免除（例：法の執行または国家安全保障に関する考慮事項）に対応するプライバシー管理策を導入する。

FAMILY:権限と目的

このファミリは、組織が以下を実施するのを確実にする:① プライバシーに影響を与える、個人情報の収集または活動についての法的根拠を示すならびに②個人情報を収集する目的を組織の通知文書に記載する。

AP-1　収集権限

セキュリティ管理策:組織は、全般的に、あるいは特定のプログラム／情報システムの必要性を支援するために、個人情報の収集を使用・維持管理・共有とともに許可する法的権限を決定し、文書化する。

補足的ガイダンス:組織は、個人情報を収集する前に、予定されている個人情報の収集が法的に許可されているかどうかを確認する。プログラム責任者は、上級プライバシー責任者／最高プライバシー責任者および弁護士に個人情報を収集するあらゆるプログラム／活動に対する法的権限について、助言を求める。個人情報を収集するのに必要な権限は、SORN (System of Records Notice)および／または PIA(Privacy Impact Assessment:プライバシー影響アセスメント)、または Privacy Act Statements や「コンピュータマッチング契約」などのその他の関連ドキュメントに記載される。関連するセキュリティ管理策は、AR-2・DM-1・TR-1・TR-2。

拡張管理策:なし

参考文献:The Privacy Act of 1974 5 U.S.C. § 552a (e)・Section 208(c) E-Government Act of 2002 (P.L. 107-347)・OMB Circular A-130 付録 I

AP-2　目的の明確化

セキュリティ管理策:組織は、個人情報を収集・利用・維持管理・共有する目的を、プライバシーに関する通知文書に記載する。

補足的ガイダンス:法律用語は、多くの場合、個人情報の収集と使用を明示的に許可する。法律用語が広い意味で記述されていて、解釈が必要な場合、組織は、全般的な許可と個人情報の収集との間の強いつながりを確保するためにも、上級プライバシー責任者／最高プライバシー責任者と弁護士に助言を求める。具体的な目的が定まった場合、その目的は関連するプライバシーコンプライアンスドキュメント(例えば、PIA、SORN、収集時に(例えば、組織が個人情報を収集するのに使用するフォームを介して)提供される Privacy Act Statements があるが、これらに限定されない)に明確に記載される。また、個人情報の不正な収集または使用を回避するために、個人情報を扱う職員は、個人情報を収集するのに必要な権限・許可を得た上での個人情報の利用、通知文書の内容についてトレーニングを受ける。関連するセキュリティ管理策は、AR-2・AR-4・AR-5・DM-1・DM-2・TR-1・TR-2・UL-1・UL-2。

拡張管理策:なし

参考文献:The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)(A)-(B)・Sections 208(b), (c), E-Government Act of 2002 (P.L. 107-347)

FAMILY:説明責任・監査・リスクマネジメント

このセキュリティ管理策ファミリは、ガバナンス・モニタリング・リスクマネジメント・アセスメントの効果的なコントロールを通じて国民の信頼を高めると同時に、組織が該当するプライバシー保護要件を満たし、全般的なプライバシーリスクを最小限に抑えていることを示すのに役立つ。

AR-1 ガバナンスおよびプライバシープログラム

セキュリティ管理策:組織は、

a. プログラムや情報システムによる個人情報の収集・使用・維持管理・共有・廃棄に関して、該当する法規制に準拠するようにするための組織全体にわたるガバナンスおよびプライバシープログラムを作成・実施する上級プライバシー責任者／最高プライバシー責任者を任命するのと合わせて、

b. 連邦政府が規定したプライバシーに関する法律とポリシーをモニタリングし、プライバシープログラムに影響を与える変更の有無を確認するとともに、

c. 組織全体にわたるプライバシープログラムを導入・実施するのに必要な[指定:組織が定めた予算と要員]を確保し、十分なリソースを割り当てるのに加えて、

d. 該当するプライバシー管理策・ポリシー・手順を実施するための戦略的なプライバシー計画を作成するだけだはなく、

e. 個人情報を扱うプログラム、情報システム、テクノロジーに導入すべきプライバシー管理策とセキュリティ管理策を統治する組織のプライバシーポリシーおよび手順を策定・周知し、実施しながら、

f. プライバシー計画・ポリシー・手順を[指定:組織が定めた頻度で少なくとも 2 年に 1 度]更新する。

補足的ガイダンス:包括的なガバナンスおよびプライバシープログラムの作成と実施は、個人のプライバシーの保護に対する組織の説明責任とコミットメントを示すのに役立つ。説明責任は、上級プライバシー責任者／最高プライバシー責任者を任命して、多面的なプライバシープログラムを作成・実施するのに必要な権限、ミッション、リソース、責任を割り当てることから始まる。上級プライバシー責任者／最高プライバシー責任者は、情報セキュリティ責任者(必要な場合には、その他の職員も含めて)助言を求めた上で、①プライバシーポリシーおよび手順の策定、導入、実施を確実にする②個人情報を保護する上での役割と責任を定義する③個人情報の保有に関して、保有される情報の機微度を判断する④個人情報に適用される法律、規定、内部ポリシーを特定する⑤プライバシーベストプラクティスをモニタリングするならびに⑥指定されたプライバシー管理策への準拠をモニタリング／チャックする。

さらなる説明責任を果たすために、上級プライバシー責任者／最高プライバシー責任者は、組織のプライバシー要求事項と、それらの要求事項を満たすために導入が計画されている、あるいは導入されているプライバシー管理策とセキュリティ管理策について文書化するための、プライバシー計画を作成する。プライバシー計画は、組織がプライバシーを考慮して業務を行っていることに対する証拠となり、上級プライバシー責任者／最高プライバシー責任者によるリソース要請を支援する。組織構造・要求事項・リソースによって、単一の計画書で済む場合もれば、複数の計画書が必要な場合もあり、計画書の包括性も異なる。例えば、PIA や SORN などの、1 ページから成るプライバシー計画が、プライバシーポリシー、ドキュメント、そして既に導入されているセキュリティ管理策をカバーすする場合がある。包括的な計画は、本付録から選択されたプライバシー管理策ベースラインを含む場合があり、また以下を含む:①プライバシーリスクアセスメントを実施するためのプロセス②PIA と SORN を完了させるためのテンプレートとガイドライン③プライバシートレーニングおよび意識向上に関する要求事項④個人情報を処理する受

託業者に対する要求事項⑤不必要に個人情報が保有されるのを防ぐための計画ならびに⑥指定されたプライバシー管理策の導入に関して、年間達成目標の達成度を評価するためのフレームワーク。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a・E-Government Act of 2002 (P.L. 107-347)・Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541・OMB Memoranda 03-22・OMB Memoranda 05-08・OMB Memoranda 07-16・OMB Circular A-130・Federal Enterprise Architecture Security and Privacy Profile

AR-2　プライバシー影響アセスメントとリスクアセスメント

セキュリティ管理策：組織は、

a. 個人が個人情報を収集・共有・保存・伝送・使用・廃棄することにより生じるプライバシーリスクを評価するためプライバシーリスクマネジメントプロセスについて文書化のうえ実施するとともに、
b. プライバシーリスクをもたらす情報システム・プログラムをはじめその他の活動に対するPIA を該当する法律・OMB ポリシー・組織の既存のポリシーと手順に従って実施する。

補足的ガイダンス：組織のプライバシーリスクマネジメントプロセスは、個人情報を収集もしくは使用または維持管理・共有、または廃棄するすべてのミッション／業務プロセスのライフサイクル全体を通して実施される。リスクを管理するためのツールと手順は、組織のミッションとリソースに応じたものとなる。そうしたツールと手順は、PIA の実施を含むが、これに限定されない。PIA は、あるプロセスの結果として、プロセスとドキュメントを生成する。OMB Memorandum 03-22 は、組織が 2002 に施行された E-Government Act のプライバシー条項を実施する際に参照できる手引きである（情報システムに対する PIA が必要となる条件含む）である。組織によっては、法律またはポリシーによって、個人情報を扱う活動、またはプライバシーに影響を与える活動（例：プログラム・プロジェクト・規定）にも PIA 要件を課すことが要求される。PIA は、プライバシーリスクを特定し、その後、それらのリスクを低減するための方法を決定するために実施される。また、PIA は、プログラムまたは情報システムによる法律・規制・ポリシー要件への適合を確実にするために実施される。PIA は一般の人に対して、組織のプライバシー対策について知らせるのに役立つ。PIA は個人情報を収集または使用もしくは維持管理（または共有する情報システムもしくは個人情報を収集または使用もしくは維持管理または共有する情報プログラム）または個人情報を収集もしくは使用または維持管理もしくは共有するプロジェクトを開発または調達する前に実施され、新たなプライバシーリスクを生じさせる変更がなされた場合に、更新される。

拡張管理策：なし

参考文献：Section 208, E-Government Act of 2002 (P.L. 107-347)・Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541・OMB Memoranda 03-22・OMB Memoranda 05-08・OMB Memoranda 10-23

AR-3　受託業者とサービスプロバイダに対するプライバシー要求事項

セキュリティ管理策：組織は、

a. 受託業者とサービスプロバイダに対するプライバシーに関連して、役割・責任・アクセス要件を規定するとともに、
b. プライバシー要求事項を契約書と調達関連ドキュメントに記載する。

補足的ガイダンス：受託業者とサービスプロバイダは、情報提供者・情報処理者・情報システム開発・IT サービス・外部委託のそれぞれによるアプリケーションを提供する組織を含むが、これらに限定されない。組織は、このセキュリティ管理策の導入に影響を与える可能性のある法律・指令・ポリシー・規定について、弁護士・上級プライバシー責任者・最高プライバシー責任者と、受託業者側の責任者に助言を求める。関連するセキュリティ管理策は、AR-1・AR-5・SA-4。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a(m)・Federal Acquisition Regulation, 48 C.F.R. Part 24・OMB Circular A-130

AR-4　プライバシーモニタリングおよびチェック

セキュリティ管理策：組織は、プライバシー管理策と社内プライバシーポリシーを［指定：組織が定めた頻度で］モニタリング・チェックし、セキュリティ管理策が効果的に導入されていることを確認する。

補足的ガイダンス：説明責任を促進するために、組織は定期的なアセスメント（例：社内リスクアセスメント）を実施して、プライバシーコンプライアンスと、管理面・運用面・技術面でのセキュリティ管理策におけるギャップを特定・対処する。そうしたアセスメントは、組織による自己アセスメントであったり、第三者による監査であったりするが、出力情報として、プログラム・プロジェクト・情報システムにおいて特定されたコンプライアンスギャップについてのレポートが生成される。この付録に記載されているすべてのプライバシー管理策が、効果的に導入されていることを確認することに加えて、組織はそれらのセキュリティ管理策が以下を満たしているかどうかをアセスメントする：①プライバシーに関する考慮事項を個人情報・プログラム・情報システム・ミッション／業務プロセス、テクノロジーのライフサイクルに組み入れるためのプロセスを実施する②プライバシーに関連の法律・規制・政策に対する変更について把握する③個人情報を収集・維持管理するプログラム・情報システム・アプリケーションを追跡し、コンプライアンスを確認する④個人情報に対するアクセスを「知る必要がある」者に限定するならびに⑤個人情報の使用と維持管理は公示に記載されている法的に許可されている目的に適合する場合のみ許可される。

組織は、また、①個人情報のセキュリティ、適切な使用、喪失をチェックするためのテクノロジーを導入する②個人情報を含むドキュメントの物理的セキュリティを確認するためのレビューを実施する③委託業者がプライバシー要求事項を満たしているかどうかをアセスメントするならびに④アセスメントプロセスの一環として特定された是正措置が、チェックを通じて発覚した問題が是正されるまで、追跡され、モニタリングされるようにする。組織の上級プライバシー責任者／最高プライバシー責任者は、情報セキュリティ責任者との間でモニタリングおよびチェック活動を調整し、そうした活動の結果を上級管理者とモニタリング責任者に通知する。関連するセキュリティ管理策は、AR-6・AR-7・AU-1・AU-2・AU-3・AU-6・AU-12・CA-7・TR-1・UL-2。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a・Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541・Section 208, E-Government Act of 2002 (P.L. 107-347)・OMB Memoranda 03-22・OMB Memoranda 05-08・OMB Memoranda 06-16・OMB Memoranda 07-16・OMB Memoranda・OMB Circular A-130

AR-5　プライバシー意識向上およびトレーニング

セキュリティ管理策：組織は、

a. 職員がプライバシーに関する責任と手順について理解するのを確実にするための、包括的なトレーニングおよび意識向上戦略を立てて、実施・更新するとともに、

b. 基本的なプライバシートレーニングを[指定:組織が定めた頻度で(少なくとも年に 1 度)]実施する。また、個人情報に責任のある職員や、個人情報を扱う活動に責任のある職員に対して、的を絞った役割に基づいたプライバシートレーニングを実施するのに加えて、

c. 職員がプライバシー要求事項を満たす責任を受け入れることを[指定:組織が定めた頻度で(少なくとも年に 1 度)](手動で、または電子的に)確認する。

補足的ガイダンス:組織は、プライバシートレーニングおよび意識向上戦略を実施することで、プライバシー文化を促進する。プライバシートレーニングおよび意識向上プログラムは、通常、1974 年に施行された Privacy Act や、2002 年に施行された E-Government Act に従った責任とそうした責任を果たせなかった場合の影響、そして新たなプライバシーリスクを特定する方法、プライバシーリスクを軽減する方法、およびプライバシーインシデントについての報告をいつ、どのように行うかなど、広範囲のトピックスに焦点を当てる。プライバシートレーニングは、また、たとえば、プログラムまたは情報システムの PIA/SORN などの公示に記載されている、データの収集および使用に関する要求事項に焦点を当てる場合がある。具体的なトレーニング方法には、たとえば、以下がある:①必須の年に 1 度のプライバシー意識向上トレーニング②的を絞った、役割に基づいたトレーニング③ウェブサイト上のプライバシープログラム④マニュアル、ガイド、ハンドブック⑤スライドプレゼンテーション⑥イベント(例:「プライバシー意識向上)週間、「プライバシークリーンアップデー」⑦ポスターと小冊子ならびに⑧すべての職員と契約社員に、電子メールでメッセージを送信すること。組織は、法律・規定・ミッション・プログラム・業務プロセス、情報システムの要求事項に対する変更が生じた場合に、あるいはコンプライアンスのモニタリングおよびチェックの結果に基づいて、トレーニングを更新する。組織は、必要に応じて、既存の情報セキュリティトレーニングの一環としてプライバシートレーニングを実施してもよい。関連するセキュリティ管理策は、AR-3・AT-2・AT-3・TR-1。

拡張管理策:なし

参考文献:The Privacy Act of 1974, 5 U.S.C. § 552a(e)・Section 208, E-Government Act of 2002 (P.L. 107-347)・OMB Memoranda 03-22・OMB Memoranda 07-16

AR-6 プライバシー報告

セキュリティ管理策:組織は、プライバシーに関する法的要件と規制上の要件についての説明責任を果たすための、OMB・連邦議会・その他監視団体、そして必要な場合には、プライバシープログラムの進捗とコンプライアンスのモニタリングに責任のある上級管理者とその他の職員に対する報告書を作成・配布・適宜更新する。

補足的ガイダンス:組織は、内外のプライバシー報告を通じて、組織のプライバシープログラムの透明性と説明責任を促進する。報告は、また、組織が、プライバシーコンプライアンス要件への適合とプライバシー管理策の進捗を判断し、連邦政府全体にわたってパフォーマンスを比較し、ポリシーと導入における脆弱性とギャップを特定し、成功モデルを特定するのに役立つ。プライバシー報告のタイプには、以下がある:①OMB に対する上級プライバシー責任者による年に 1 度の報告②Implementing Regulations of the 9/11 Commission Act が要求する連邦議会への報告ならびに③組織の法的要件または社内ポリシーが要求する、その他の公的報告書。組織の上級プライバシー責任者/最高プライバシー責任者は、組織が、該当するすべてのプライバシー報告要件を満たすのを確実にするために、必要に応じて弁護士の助言を求める。

拡張管理策:なし

参考文献:The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347)・Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541・Section 803, 9/11 Commission Act, 42 U.S.C. § 2000ee-1・Section 804, 9/11 Commission Act, 42 U.S.C. § 2000ee-3・Section 522, Consolidated Appropriations Act of 2005 (P.L. 108-447)・OMB Memoranda 03-22・OMB Circular A-130

AR-7　プライバシーを強化したシステム設計および開発

セキュリティ管理策：組織は、プライバシー管理策が自動で実施されるよう、情報システムを設計する。

補足的ガイダンス：組織は、組織の情報システムを設計する際には可能な範囲内で、個人情報の収集・使用・保持・開示に必要なプライバシー管理策が自動で実施されるようにするための、技術とシステム機能を導入する。組織は、プライバシー管理策をシステム設計および開発に組み入れることで、個人情報に対するプライバシーリスクを低減し、情報システムの侵害や、その他のプライバシー関連インシデントが発生する可能性を減らせる。組織は、また、システムの定期的なレビューを実施して、Privacy Act へのコンプライアンスを維持するための更新の必要性について判断する。組織は、プライバシー管理策が自動で実施されるか否かにかかわらず、情報システムの使用と個人情報の共有を定期的にモニタリングし、そうした使用／共有が Privacy Act や、組織の公示に記載されている許可されている目的に適合しているかどうか、あるいはそれらの目的に適合する形で実施されているかどうかを確認する。関連するセキュリティ管理策は、AC-6・AR-4・AR-5・DM-2・TR-1。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a(e)(10)・Sections 208(b) and(c), E-Government Act of 2002 (P.L. 107-347)・OMB Memorandum 03-22

AR-8　開示についての説明

セキュリティ管理策：組織は、

a. 組織の管理下にある各記録システムに保存されている情報の開示について、
   (1) 記録が開示された日付、開示の性質と目的
   (2) 開示がなされた相手である個人または機関の名前と住所
   が含まれた正確な記述を保持する。
b. 開示についての記述を記録の存続期間または開示後 5 年間の、いずれか長い方に合わせて保持する。
c. その記録に名前が記載されている個人がリクエストした場合には、開示についての記述にアクセスできるようにする。

補足的ガイダンス：上級プライバシー責任者／最高プライバシー責任者は、定期的に組織の記録システムの管理者と連絡を取り合って、Privacy Act の規定に従って、記録の開示についての必要な記述が適切に維持管理され、記録に名前が記載されている個人に提供されるようにする。組織は、その開示が「知る必要がある」個人に対して行われた場合や、Freedom of Information Act に従って行われた場合、あるいは 5 U.S.C. § 552a(c)(3)に従って法執行機関に対して行われた場合には、開示についての記述を保持する必要はない。政府機関の長は、個人に対して開示についての記述を提供するといった要件から、特定の記録システムを免除するためのルールを策定・公示してもよい。関連するセキュリティ管理策は、IP-2。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (c)(1), (c)(3), (j), (k)

FAMILY: データの品質と完全性

このセキュリティ管理策ファミリは、組織が収集・維持管理するあらゆる個人情報が公示に記載されているそうした個人情報の使用目的に関して正確であることおよび関連性があることならびにタイムリーであることおよび完全であることを保証し、国民の信頼を高めるのに役立つ。

DI-1 データの品質

セキュリティ管理策:組織は、

a. 個人情報の収集または作成時に、可能な範囲内で、個人情報が正確であるかおよび関連性があるか(ならびにタイムリーであるかおよび完全であるか)を確認するのに合わせて、

b. 個人情報を収集する際には、可能な範囲内で、個人から直接収集するとともに、

c. 組織のプログラムまたはシステムによって使用される個人情報を[指定:組織が定めた頻度で]チェックして、情報が正確でないあるいは古い場合には修正するのに加えて、

d. 配布される情報の品質・実用性・客観性・完全性を確保し、最大限にするためのガイドラインを発行する

補足的ガイダンス:組織は、個人情報が正確であるか、また関連性があるかを確認するための妥当な措置を講じる。そうした措置の例として、アドレスが収集された(または情報システムに入力された)時に、自動化されたアドレス検証用 API を用いて、アドレスを編集・検証することが挙げられる。データの品質を保護するたの措置は、個人情報の性質と背景、個人情報をどのように使用するか、個人情報をどのように入手したかに基づく。連邦政府の福利厚生制度のもとで個人が受け取る権利または給付金もしくは権限についての決定に使用される個人情報が、正しいかどうかを検証するための措置は、機微度が劣る個人情報を検証するための措置よりも、より包括的である。個人または個人の正式代表者以外から入手した個人情報の検証には、追加の措置が必要になる可能性がある。

組織は、個人情報の機微度が十分に高い場合(例:個人情報が、自動更新のために年に 1 度実施される納税者の収入の再確認に使用される場合)には、そうした情報を更新するためのメカニズムを情報システムに組み入れると同時に、更新の頻度と手段を含む手順を策定する。関連するセキュリティ管理策は、AP-2・DI-2・DM-1・IP-3・SI-10。

拡張管理策:

(1) データの品質 | 個人情報 を検証する

組織は、個人、または個人の正式代表者に対して、個人情報の収集プロセスにおいて個人情報を検証することを要求する。

(2) データの品質 | 個人情報を再検証する

組織は、個人、または個人の正式代表者に対して、収集された個人情報が現在も正確であることを[指定:組織が定めた頻度で]再検証することを要求する。

参考文献:The Privacy Act of 1974, 5 U.S.C. § 552a (c) and (e)・Treasury and General Government Appropriations Act for Fiscal Year 2001 (P.L. 106-554), app C § 515, 114 Stat. 2763A-153-4・Paperwork Reduction Act, 44 U.S.C. § 3501; OMB Guidelines for Ensuring and Maximizing the Quality, Objectivity, Utility, and Integrity of Information Disseminated by Federal Agencies (October 2001)・OMB Memorandum 07-16。

DI-2　データの完全性と、データ完全性委員会

セキュリティ管理策：組織は、

a. 個人情報の完全性を既存のセキュリティ管理策を使用して確保するためのプロセスを文書化するとともに、

b. 組織の「コンピュータマッチング契約」[123]をモニタリングし、それらの合意が、Privacy Act のコンピュータマッチングに関する条項に適合するようにするために必要な場合には、Data Integrity Board を設立する。

補足的ガイダンス：連邦政府の福利厚生制度のもとで支給される金融支援または支払の申請者や受給者に関して、あるいは連邦政府の職員または給与に関する記録を比較するためのコンピュータによる比較に関して、他の組織との間で「コンピュータマッチング契約」を締結する組織あるいは参加する組織は、そうしたマッチングについての合意の導入をモニタリングし、調整する役割を果たす Data Integrity Board を設立する。多くの組織では、上級プライバシー責任者／最高プライバシー責任者が Data Integrity Board を指揮する。Data Integrity Board は、「コンピュータマッチング契約」に従って共有されるデータの品質と完全性の両方を維持するためのセキュリティ管理策が、確実に導入されるようにする。関連するセキュリティ管理策は、AC-1・AC-3・AC-4・AC-6・AC-17・AC-22・AU-2・AU-3・AU-6・AU-10・AU-11・DI-1・SC-8・SC-28・UL-2。

拡張管理策：

(1) データの完全性と、データ完全性委員会 | 「コンピュータマッチング契約」をウェブサイトに掲載する

組織は、「コンピュータマッチング契約」を組織のパブリックウェブサイトに掲載する。

参考文献：The Privacy Act of 1974, 5 U.S.C. §§ 552a (a)(8)(A), (o), (p), (u)・OMB Circular A-13 付録 I

[123] 組織は、自身がメンバーであるコンピュータマッチングプログラムに関連して、「コンピュータマッチング契約」を締結する。一部の例外はあるものの、コンピュータマッチングプログラムは、2 つ以上の自動化された記録システム間の、あるいは単一のそうした記録システムと連邦政府に関連しない記録を扱うシステムとの、コンピュータによる比較である。このプログラムの目的は、連邦政府の福利厚生制度のもとで支給される現金・現物・支払のいずれかに関するサービスの、申請者・受給者・参加者・提供者のいずれかによる法律および規制上の要求事項の継続的な遵守や資格の有無を確認する事、あるいは、連邦政府の職員または給与に関する記録を扱う 2 つ以上の自動化された記録システム間の、あるいは連邦政府の職員または給与に関する記録を扱う単一の記録システムと連邦政府に関連しない記録を扱うシステムとの、コンピュータによる比較を行うことにある。詳細は、Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. § 552a (a)(8)(A)を参照の事。

FAMILY:データの最小化と保有

このセキュリティ管理策ファミリは、組織が、データの最小化と保有に関する要求事項である、個人情報収集時の目的に関連し、かつ必要な個人情報のみを収集・使用・保有することを支援する。組織は、公示に記載されている目的を果たすのに必要な期間にわたって、NARA(National Archives and Records Administration)認定の記録保有に関するスケジュールに沿って、個人情報を保有する。

DM-1 個人情報の最小化

セキュリティ管理策:組織は、

a. 法的に許可されている収集目的を果たすために必要な、かつ関連する、最低限必要な個人情報 要素を特定するとともに、

b. 個人情報の収集と保有を、公示に記載されている目的に適合し、かつ情報提供者が同意した情報要素に限定するのに加えて、

c. 公示に記載されている個人情報のみが収集・保有されることを確実にし、かつ、その個人情報が法的に許可されている目的を果たすために引き続き必要であることを確認するために、個人情報の保有について初期評価と定期的なレビューを実施する。なお、レビューは[指定:組織が定めた頻度で(少なくとも年に 1 度)]行うこととし、スケジュールを立てて、スケジュールに従うこと

補足的ガイダンス:組織は、個人情報の収集が法規制によって許可されている目的に適合するよう、措置を講じる。組織の特定の業務プロセスを支援するために最低限必要な個人情報要素は、組織が収集することが許可されている個人情報であると考えられる。プログラム責任者は、上級プライバシー責任者/最高プライバシー責任者と弁護士に助言を求めた上で、法的に許可されている目的を果たすのに必要な情報システムまたは活動に対して、必要な個人情報要素を特定する。

組織は、可能な場合に、保有する個人情報の量を減らす事により、プライバシーリスクとセキュリティリスクをさらに低減できる。OMB Memorandum 07-16 は、組織に対して、個人情報の保有についての初期レビューと後続のレビューを実施すること、そして、保有されている情報が正確である事、関連性があること、タイムリーであること、および完全であることを最大限に保証することを要求している。組織には、OMB の規定に従って個人情報の保有を、文書化された、組織の事業目的を果たすのに必要な量に抑えることが求められている。OMB Memorandum 07-16 は、組織に対して、保有についての初期レビューを補足する定期的なレビューのスケジュールを立てて、Federal Register の公示、または組織のウェブサイトに掲載することを要求している。組織は、連邦記録責任者と連携して、組織が保有する個人情報の量を減らす作業が、NARA が規定する保管スケジュールが確実に適合されるようにする。

組織は、定期的な評価を実施することで、リスクを低減し、公示に記載されているデータのみが収集されるようにし、収集されたデータが公示に記載されている目的を果たすのに引き続き必要であり、かつ関連することを確認する。関連するセキュリティ管理策は、AP-1・AP-2・AR-4・IP-1・SE-1・SI-12・TR-1。

拡張管理策:

(1) 個人情報の最小化 | 個人情報 の検索 / 削除 / 編集 / 匿名化

組織は、実現可能で、かつテクノロジーの範囲内で、指定された個人情報を検索し、削除/編集する、および/または「匿名化」テクニックを使用して、保有されている情報の機微度を低下させ、開示によるリスクを低減することによって、そうした情報の使用を許可する。

補足的ガイダンス：NIST Special Publication 800-122 は匿名化に関する手引きを記載している。

参考文献：The Privacy Act of 1974, 5 U.S.C. §552a (e)・Section 208(b), E-Government Act of 2002 (P.L. 107-347)・OMB Memoranda 03-22・OMB Memoranda 07-16。

DM-2　データの保有と廃棄

セキュリティ管理策：組織は、

a. 個人情報の集合を公示に記載されている目的を果たすために、あるいは法律に従って、［指定：組織が定めた期間］にわたって保有するとともに、

b. 個人情報がどのように保存されているかにかかわらず、NARA 認定の記録保有スケジュールに従って、かつ、喪失、盗難、悪用、不正アクセスから保護される形で個人情報を廃棄・破壊・削除・匿名化のすべてを行う（またはそれらのいずれかを行う）のに加えて、

c. 個人情報（元情報とともに、複製またはアーカイブされた記録を含む）を安全に削除する、または破壊するための［指定：組織が定めた技法または手法］を用いる。

補足的ガイダンス：NARA は、連邦記録の廃棄に関わる保管スケジュールを提供している。プログラム責任者は、記録責任者や NARA と連携して、適切な保管期間と廃棄方法を定める。NARA が、組織に対して、運用上必要とされる期間よりも長く個人情報を保管することを要求する場合がある。そうした場合、組織はそうした要求事項を公示に記載する。保管の方法には、例えば、電子的・光媒体・紙面がある。

保有する個人情報の量を減らす方法には、たとえば、保有される個人情報のタイプを限定すること（例：社会保障番号を使用する必要がなくなった時点で、社会保障番号を削除する）、保有されている個人情報の、長期にわたる保有が必要でなくなった場合に、保有期間を短縮すること（この取組は、NARA の承認を必要とするため、組織の記録責任者と相談した上で実施される。上記のいずれの場合も、組織は、一般の人に対して、個人情報の保有に関する変更について知らせるために通知を行う（例：System of Records Notice を更新することによって)。

たとえば、DVD・CD・マイクロフィルム・マイクロフィッシュなどの読み出し専用のアーカイブが可能な媒体を使用することで、そうした媒体に保存されているデータベースごと破壊しない限り、個人記録を取り出せないようにすることが可能になる。関連するセキュリティ管理策は、AR-4・AU-11・DM-1・MP-1・MP-2・MP-3・MP-4・MP-5・MP-6・MP-7・MP-8・SI-12・TR-1。

拡張管理策：

(1) データの保有と廃棄 | システムの設定

組織は、可能な場合には、個人情報が収集、作成、または更新された日付と、承認された記録保管スケジュールに従って削除される／アーカイブされる予定の日付を記録するよう、情報システムを設定する。

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (e)(1), (c)(2)・Section 208 (e), E-Government Act of 2002 (P.L. 107-347)・44 U.S.C. Chapters 29, 31, 33・OMB Memorandum 07-16・OMB Circular A-130・NIST Special Publication 800-88

DM-3　テスト・トレーニング・調査における個人情報の使用を最小限に抑える

セキュリティ管理策：組織は、

a. テスト・トレーニング・研究における個人情報の使用を最小限に抑えるためのポリシーを作成するとともに、

b. テスト・トレーニング・研究に使用される個人情報を保護するためのセキュリティ管理策を導入する。

補足的ガイダンス：組織が新規アプリケーション／情報システムを実装する前に行う、アプリケーション／情報システムのテストには、個人情報が使用されることが多い。また、研究目的やトレーニングのために個人情報が使用される場合もある。テスト・研究・トレーニングに個人情報が使用される場合、そうした情報が不正に開示されるまたは悪用されるリスクが増加する。個人情報を使用せざるを得ない場合、組織は、関連するリスクを最小限に抑えるための対策を実施すると同時に、そうした目的に個人情報が使用されるのを承認し、使用される個人情報の量を制限する。組織は、テスト・トレーニング・研究における個人情報の使用が、情報収集時の本来の目的に適合することを確実にするためにも、上級プライバシー責任者・最高プライバシー責任者・弁護士の全員に助言を求める。

拡張管理策：

(1) テスト・トレーニング、調査における個人情報の使用を最小限に抑える | リスクを低減するためのテクニック

組織は、可能な場合には、研究・テスト・トレーニングに個人情報を使用する場合の、プライバシーリスクを最小限に抑えるためのテクニックを使用する。

補足的ガイダンス：個人情報のプライバシーリスクを最小限に抑えるためのテクニックには、例えば匿名化等がある。

参考文献：NIST Special Publication 800-122。

FAMILY:個人による参加と、個人の救済

このセキュリティ管理策ファミリは、個人情報の収集と使用に関して意思決定を行うプロセスに、個人を積極的に参加させる必要性に取り組む。このファミリのセキュリティ管理策は個人が個人情報にアクセスできるようにすると同時に、自身の個人情報を適宜訂正・修正させる手段を用意することによって、そうした個人情報に基づいた組織の決定について国民の信頼を向上させる。

IP-1 同意

セキュリティ管理策:組織は、

a. 可能な場合で、かつ適切な場合には、個人情報が収集される前に、情報提供者が自身の個人情報の収集、使用、維持管理、共有について承認する手段を用意するのと合わせて、

b. 個人情報の収集、使用、配布、保持を許可するあるいは許可しないかについての決定による影響を情報提供者が理解できるようにするための適切な手段を用意するとともに、

c. 可能な場合かつ適切な場合には、以前に収集された個人情報の新た使用または開示に先立って、情報提供者から同意を得るのに加えて、

d. 組織が個人情報を収集した時点で公示に記載されていなかった個人情報の使用に関して、情報提供者が承知していていることを確実にして、可能な場合には同意を得る。

補足的ガイダンス:同意は、個人が、自身の個人情報の収集と使用、そして個人のプライバシーに対するリスクを増加させるテクノロジーの使用に関する意思決定プロセスに、情報提供者が参加できるようにするために必須となる。同意を得るために、組織は個人に対して、個人情報の収集目的やテクノロジーの使用について適切に通知し、個人がそうした活動に対する同意を示す手段を用意する。組織は、運用ニーズを満たすために公示と同意メカニズムを調整する。組織は、例えば、公示の更新を通じて、情報提供者による認識と同意を実現する。

組織はオプトインまたはオプトアウトもしくは黙示の承諾といった形式で個人から同意を得る。オプトインによる同意は、推奨される方法であるが、常に実現できるとは限らない。オプトインでは個人が、組織による個人情報の収集または使用を許可するための肯定的なアクションを取る必要がある。例えばオプトインによる同意は、個人に対してウェブサイト上のラジオボタンを押すか、あるいは同意を示すドキュメントに署名することを必要とする。これとは対照的に、オプトアウトでは、個人がそうした個人情報の新たな収集／使用または継続的な収集／使用を禁止するためのアクションを取る必要がある。例えば、Federal Trade Commission の Do-Not-Call Registry は、個人が一方的な勧誘電話を受けたくない場合に、オプトアウトリストへの追加をリクエストできる仕組みである。黙示の承諾は、最も推奨されない方法であり、限られた状況でのみ使用すべきである。黙示の承諾では、個人が反対しない場合に、個人情報の収集または使用に同意したとみなす（例:防犯カメラが設置されいて、その旨を示す公示が壁などに貼られている建物の中に入って、留まる場合、個人がビデオ録画を無言で承諾する場合）。プログラムまたは情報システムの性質によっては、個人が、彼らが提供する個人情報のタイプと、そうした個人情報の使用を制限できるようにすることが適切な場合もある。組織の同意メカニズムには、個人が個人情報を提供しない場合の影響についての説明も含まれる。その場合の影響は、組織ごとに異なると考えられる。関連するセキュリティ管理策は、AC-2・AP-1・TR-1・TR-2。

拡張管理策:

(1) 同意 | 項目別の同意、または段階的な同意を支援するメカニズム

組織は、データの具体的な使用に関して、項目別の同意、または段階的な同意を支援するメカニズムを導入する。

補足的ガイダンス：組織が提供する項目別の選択肢の例として、個人がさまざまな目的の各々について知らされるのを望むか否かの項目を設けて、選択できるようにすることが挙げられる。この場合、組織は、組織の業務が個人の選択を遵守するのを確実にするための、同意メカニズムを構築する。

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (b), (e)(3)・Section 208(c), E-Government Act of 2002 (P.L. 107-347)・OMB Memoranda 03-22・OMB Memoranda 10-22。

IP-2 個人によるアクセス

セキュリティ管理策：組織は、

a. 個人が、記録システムに保存されている自身の個人情報にアクセスできるようにするのと合わせて、
b. Privacy Act 記録システムに保存されている記録にアクセスしたい場合に、どのようにリクエストしたらよいかを規定する、ルールと規定を公にするとともに、
c. SORN (System of Records Notices)にアクセスするための手順を公にするのに加えて、
d. Privacy Act リクエストを適切に処理するための、Privacy Act 要件と、OMB のポリシーおよびガイダンスに従う。

補足的ガイダンス：そうしたアクセスは、個人が、組織の記録システムに保存されている、自身に関する個人情報をレビューできるようにする。そうしたアクセスは、データに対するタイムリーかつ簡易化された費用のかからないアクセスを含む。記録に対するアクセスを許可するための組織のプロセスは、リソース・法的要件等、その他の要因によって変わる。組織の上級プライバシー責任者／最高プライバシー責任者は、弁護士の助言を受けた上で、Privacy Act の規定の内容に加えて、記録に対するアクセスリクエストを処理するプロセスに責任がある。記録のタイプによっては、アクセスを許可することが適切でない場合がある。政府機関の長は、Privacy Act のアクセスに関する条項から特定のシステムを免除するためのルールを策定・公示してもよい。また、民事訴訟または民事手続を目的として編集された情報には、個人はアクセスする資格がない。関連するセキュリティ管理策は、AR-8・IP-3・TR-1・TR-2。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. §§ 552a (c)(3), (d)(5), (e) (4); (j), (k), (t)・OMB Circular A-130

IP-3 救済

セキュリティ管理策：組織は、

a. 個人が、組織が維持管理する個人情報が正確でない場合に、情報を訂正／修正させるためのプロセスを用意するとともに、
b. 個人情報の訂正および／または修正について個人情報の正当な利用者（例：情報共有を行っている外部パートナー）に周知し、可能な場合で、かつ適切な場合に、訂正および／または修正の影響を受ける個人に対して、彼らの情報が訂正および／または修正された旨を通知するためのプロセスを確立する。

補足的ガイダンス：救済は、組織が保有する個人情報が正確であることに関して、個人が確認できるようにする。効果的な救済プロセスは、データの品質に対する組織のコミットメントとりわけデータが正確でない場合に個人に対する給付金やサービスの拒否につながるあるいは不適切な決断につながる業務機能において、そうしたコミットメントを示すのに役立つ。組織は、救済リクエストの範囲、要求されている変更、および変更による影響に基づいて、記録を訂正および／または修正すべきかどうかを自由裁量で判断する。不利な決定がなされた場合には、個人が抗議して、正確でない情報を修正させることも可能である。

効果的な救済のために、組織は①個人情報の収集を行っていることに関して、効果的に通知する②記録に対するアクセスをリクエストするためのプロセスとメカニズムについて、分かりやすい言葉で説明する③訂正／修正リクエストの発行に関する基準を作成する④リクエストを分析し、決定を下すためのリソースを用意する⑤データの集合を訂正／修正するための手段を用意する⑥正確でない情報をもとに下された決定についてレビューする。

組織の救済プロセスは、訂正／修正リクエストを拒否することが決定された個人に対して、そうした決定の理由、組織の決定に対する個人の異議を記録する手段、最初の決定に対する組織によるレビューをリクエストする手段と共に、決定内容を通知する。個人情報が訂正／修正される場合、組織は、その個人情報の正式な受取人が情報が訂正／修正されたことを知らされるようにするための措置を講じる。救済が他の組織から得た情報も対象に含む場合、救済プロセスには、その情報を収集した組織との間での調整が含まれる。関連するセキュリティ管理策は、IP-2・TR-1・TR-2・UL-2。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (d), (c)(4)・OMB Circular A-130

IP-4　苦情対応

セキュリティ管理策：組織は、組織のプライバシー対策に関して個人から寄せられる苦情・懸念・質問を受けて応じるためのプロセスを実施する。

補足的ガイダンス：個人から寄せられる苦情・懸念・質問は、最終的に運用モデル、テクノロジーの使用、データ収集プラクティス、およびプライバシー対策とセキュリティ対策を改善させる、外部入力の貴重な情報源として役立つ。組織は、一般の人が簡単にアクセスできて、簡単に使用できる「苦情申立て」メカニズムを用意する。このメカニズムには、苦情を申し立てる際に必要となるすべての情報（上級プライバシー責任者／最高プライバシー責任者、あるいは任命されて苦情を受ける職員の連絡先を含む）を含まれる。組織の苦情管理プロセスには、寄せられたすべての苦情がレビューされ、タイムリーかつ適切に対処されるようにするための追跡メカニズムが含まれる。関連するセキュリティ管理策は、AR-6・IP-3。

拡張管理策：

(1) 苦情に対処する | レスポンスタイム

組織は、苦情・懸念・質問として個人から寄せられるものに［指定：組織が定めた時間］内に応じる。

参考文献：OMB Circular A-130・OMB Memoranda 07-16・OMB Memoranda 08-09

FAMILY:セキュリティ

このセキュリティ管理策ファミリは、この管理策の付録 F のセキュリティ管理策を補完するものであり、組織が収集・維持管理する個人情報を喪失または不正アクセス(もしくは開示)から保護し、プライバシーインシデントに対処するための計画と対応が OMB のポリシーと手引きに適合するようにするための技術面・物理面・管理面での保護対策が実施されるようする。このセキュリティ管理策ファミリファミリ内のセキュリティ管理策の導入は、情報セキュリティ担当職員との間で調整され、既存の NIST Risk Management Framework に準拠するように実施される。

SE-1 個人情報一覧

セキュリティ管理策:組織は、

a. 個人情報を収集、使用、維持管理、または共有することが判明しているすべてのプログラムと情報システムの一覧を作成・維持管理し、[指定:組織が定めた頻度で]更新するとともに、

b. 個人情報を含むすべての新規情報システムまたは修正された情報システムの情報セキュリティ要求事項の規定を支援するために個人情報一覧が更新された場合には、最高情報責任者または情報セキュリティ責任者に一覧の最新版を渡す。

補足的ガイダンス:個人情報一覧は、組織がこのセキュリティ管理策の付録 F に従って個人情報を保護するための効果的な管理面・技術面・物理面でのセキュリティポリシーおよび手順を実施して、個人情報が開示されるリスクを軽減できるようにする。組織が個人情報一覧に必要な情報を収集するための1つの手段として、個人情報を含む情報システムの PIA から、以下の情報要素を抽出することが挙げられる:①特定されたシステムの各々の名称と頭字語②そのシステムに含まれる個人情報のタイプ③あらゆるタイプの個人情報の(情報システムと組み合わさった場合の)機微度の分類④個人情報が開示された場合に個人に及ぶ大きな被害、金銭的困難、迷惑、または不公平のリスクのレベルと、組織にもたらされる金銭的リスクまたは評判に関わるリスクのレベルの分類。組織が一覧を更新する際には、個人情報を創出する可能性のあるリンク可能なデータを特定する。関連するセキュリティ管理策は、AR-1・AR-4・AR-5・AT-1・DM-1・PM-5・UL-3。

拡張管理策:なし

参考文献:The Privacy Act of 1974, 5 U.S.C. § 552a (e) (10)・Section 208(b)(2), E-Government Act of 2002 (P.L. 107-347)・OMB Memorandum 03-22・OMB Circular A-130 の付録 I・FIPS Publication 199・NIST Special Publications 800-37・NIST Special Publications 800-122

SE-2 プライバシーインシデント対応

セキュリティ管理策:組織は、

a. プライバシーインシデント対応計画を作成・実施するとともに、

b. 組織のプライバシーインシデント対応計画に沿って、プライバシーインシデントに組織的かつ効果的に対応する。

補足的ガイダンス:このセキュリティ管理策の付録 F のインシデント対応(IR)ファミリが情報セキュリティに影響を与える広範囲のインシデントを扱うのに対して、このセキュリティ管理策は個人情報に関連するインシデントのみを扱うため、「プライバシーインシデント」という用語を使用している。組織のプライバシーインシデント対応計画は、上級プライバシー責任者/最高プライバシー責任者の指揮の下で作成される。プライバシーインシデント対応計画は、①プライバシーインシデント対応計画をレビュー・承認し、計画の実施に参加するいろいろな機能を果たすプライバ

シーインシデント対応チームを設立すること②組織や影響を受ける個人をモニタリングすることについての通知が適切であるかどうかを判断し、適切である場合には通知を行うためのプロセス③影響を受ける個人に及ぶ被害・金銭的困難・迷惑・不公平の程度を判断し、必要な場合には、そうしたリスクの低減措置を講じるための、プライバシーリスクアセスメントプロセス④プライバシーインシデントが発生した場合に、職員または契約社員が組織のインシデントマネジメント構造に沿って、情報セキュリティ責任者と上級プライバシー責任者／最高プライバシー責任者に速やかに報告するのを確実にするための初期手順ならびに⑤職員または契約社員が組織のプライバシーポリシーに従わない場合に、適切な管理職職員たはモニタリング責任者に報告するための手順の 5 つが盛り込まれたまれた計画がある。組織によっては、侵害発生時に監視組織に通知することが、法律またはポリシーによって求められている。組織は、また、プライバシーインシデント対応計画をセキュリティ計画インシデント対応計画に組み入れるか、あるいはそれらの計画を別々にするかを選択できる。関連するセキュリティ管理策は、AR-1・AR-4・AR-5・AR-6・AU-1～AU-14・IR-1～IR-8・RA-1。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (e), (i)(1), and (m)・Federal Information Security Management Act (FISMA) of 2002, 44 U.S.C. § 3541・OMB Memoranda 06-19・OMB Memoranda 07-16・NIST Special Publication 800-37

FAMILY:透明性

このファミリは、組織が、組織の情報プラクティスと、組織のプログラムや活動により生じるプライバシーへの影響について、公示することを確実にする。

TR-1 プライバシーに関する通知

セキュリティ管理策:組織は、

a. 以下に関して、一般人と個人に効果的に通知する:①個人情報の収集・使用・共有・保護・維持管理・廃棄を含むプライバシーに影響を与える活動②個人情報の収集に必要な権限③組織が個人情報をどのように使用するかについての個人情報を提供する側の選択肢(存在する場合)とそうした選択を行う場合と行わない場合の影響ならびに④個人情報にアクセスする手段と、個人情報 を訂正・修正させる手段

b. 以下について記述する:①組織が収集する個人情報と、そうした情報を組織が収集する目的②組織が個人情報 を社内でどのように使用するか③組織が、他の組織との間で個人情報を共有するか否か、共有する場合には、そうした他の組織のカテゴリーと、そうした共有の目的④個人情報の使用または共有に関して、個人が同意するか否かを選べるかどうか、どのようにしてそうした同意を行うか⑤個人が個人情報にアクセスする方法ならびに⑥個人情報がどのようにして保護されるのか

c. 個人情報に影響を与えるプラクティスまたはポリシーの変更を反映するために、あるいはプライバシーに影響を与える活動の変化を反映するために、変更後、可能な限り早く公示を修正する。

補足的ガイダンス:効果的な通知は、明確で、読みやすく、理解しやすいことから、読者は、組織が通常、個人情報をどのように使用するかについて理解し、個人情報を提供するに前に、十分な情報を得た上で提供の可否を決定できるようになる。効果的な通知は、また、組織が情報プラクティスを実施する際に取り組んだプライバシーに関する考慮事項を示すのに役立つ。組織は、SORN・PIA・ウェブサイトプライバシーポリシーなどの法律またはポリシーが要求する、さまざまな手段を用いて一般的な公示を行う。組織は、Privacy Act の定めるところにより、個人に対して紙面のあるいは組織が個人情報を収集するのに使用する電子フォーム上の、もしくは個人が保有する別のフォーム上の Privacy Act Statements を介して直接、通知を行う。

組織の上級プライバシー責任者／最高プライバシー責任者は、弁護士や、関連プログラムマネージャの助言をもとに、組織の公示に対する同意に責任がある。このセキュリティ管理策の公示要件は、組織が Privacy Act の公示に関する条項、the E-Government Act の PIA 要件、OMB 発行の連邦政府によるプライバシー通知に関する手引き、また該当する場合には、Information Sharing Environment (ISE)への参加に関するポリシー[124]に従った場合に満たされる。事前に通知することなく個人情報プラクティスまたはポリシーを変更することは、避けるべきであり、どうしても必要な場合は、上級プライバシー責任者／最高プライバシー責任者と弁護士に相談する。関連するセキュリティ管理策:AP-1・AP-2・AR-1・AR-2・IP-1・IP-2・IP-3・UL-1・UL-2。

拡張管理策:

(1) プライバシーに関する通知 | リアルタイムの、または階層化された通知

[124] Information Sharing Environment(ISE)は、テロ行為と国土安全保障に関する情報の共有を容易にするためのアプローチである。ISE は、Intelligence Reform and Terrorism Prevention Act of 2004, Public Law 108-458, 118 Stat. 3638 で定められている。詳細は、ISE の以下のウェブサイトを参照のこと: http://www.ise.gov

組織は、個人情報を収集する際に、リアルタイムの通知、および／または階層化された通知を行う。

補足的ガイダンス：リアルタイムの通知は、「収集した時点での通知」として定義されている。階層化された通知のアプローチでは、個人に対して、組織のプライバシーポリシーの要点の一覧を提供する。2 回目の通知は、より詳細な／具体的な情報を提供する。

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3), (e)(4)・Section 208(b), E-Government Act of 2002 (P.L. 107-347)・OMB Memoranda 03-22・OMB Memoranda 07-16・OMB Memoranda 10-22・OMB Memoranda 10-23・ISE Privacy Guidelines。

TR-2　記録システムによる通知と、PRIVACY ACT の記述

セキュリティ管理策：組織は、

a. 個人情報を含むシステムはプロセスのモニタリングが必要である。従って、そうしたシステムを保有する場合、SORN (Publishes System of Records Notices)を発行し、Federal Register に登録するとともに、

b. SORN を最新に保つのに加えて、

c. 情報の収集元である個人に対して追加の形式的な通知を行うために、個人情報を収集するためのフォーム上に、あるいは個人が保有する別のフォーム上に Privacy Act Statements を記載する。

補足的ガイダンス：組織は、収集され、記録システムに保存される個人情報に関して公示を行うための、SORN を発行する。そうした情報は、Privacy Act により、「政府機関の管理下にある記録の集まりであり、個人の名前や、識別番号、記号、その他の識別子を元に取り出される」と定義されている。SORN は、情報がどのように使用・維持管理され、修正されるかについて、また、システムの特定の部分が、法執行または国家安全上の理由により Privacy Act の対象から免除されるかについて説明する。Privacy Act Statements は、以下について通知する：①組織が個人情報を収集する権限を有すること②個人情報の提供が必須か、あるいは任意か③個人情報を使用する主な目的④情報の意図した開示（日常的な使用）ならびに⑤必要な情報のすべて、あるいは一部を提供しない場合の影響。情報が口頭で収集される場合、組織は、個人情報の収集を開始する前に Privacy Act Statement を熟読する（例えば、電話による聞き取りや調査を実施する場合）。関連するセキュリティ管理策は、DI-2。

拡張管理策：

(1) 記録システムによる通知と、PRIVACY ACT STATEMENTS | パブリックウェブサイトに掲載する

組織は SORN を組織のパブリックウェブサイトに掲載する。

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (e)(3)・OMB Circular A-130。

TR-3　プライバシープログラム情報の配布

セキュリティ管理策：組織は、

a. 一般の人が、組織のプライバシー対策に関する情報にアクセスできるようにし、また、組織の上級プライバシー責任者／最高プライバシー責任者と連絡を取れるようにするとともに、

b. プライバシー対策を、組織のウェブサイトや他の手段を介して一般の人が利用できるようにする。

補足的ガイダンス：組織は、組織のプライバシー対策に関して一般の人に周知するための、さまざまなメカニズムを導入する。そうしたメカニズムには、PIA・SORN・プライバシーレポート、一般の人がアクセスできるウェブページ、電子メールの送信、ブログ、定期的な刊行物（例：四半期ごとに発行されるニュースレターがあるが、これらに限定されない。組織は、組織のプライバシ

一対策に関する一般の人からのフィードバックや質問を受け付けるための、一般向けの電子メールアドレスおよび／または電話回線を用意する。関連するセキュリティ管理策は、AR-6。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a; Section 208, E-Government Act of 2002 (P.L. 107-347)・OMB Memoranda 03-22・OMB Memoranda 10-23

FAMILY:使用制限

このファミリは、組織が、組織の公示に記載されている個人情報のみを、あるいは記載された目的に適合する個人情報、もしくは法律で認められている個人情報のみを使用する。このファミリ内のセキュリティ管理策を導入することで、個人情報の使用の範囲が限定される。

UL-1 内部使用

セキュリティ管理策:組織は、組織内での個人情報の使用を、Privacy Act および／または公示に記載されている、許可されている目的に適合する場合のみ許可する。

補足的ガイダンス:組織は、個人情報の使用を、法的に許可されている目的に適合し、かつ、Privacy Act および／または公示に記載されている使用に適合する場合のみ許可するための措置を講じる。そうした措置は、組織による個人情報の使用をモニタリングとチェック、および組織の職員に対する、許可を得た上での個人情報の使用に関するトレーニングが含まれる。組織は、上級プライバシー責任者／最高プライバシー責任者と、必要な場合には、弁護士からの助言をベースにして、提案されている、個人情報の新たな使用を評価し、そうした使用が組織の権限の範囲に収まるかを確認するためのプロセスと手順を文書かする。組織は、必要な場合には、個人情報の新たな使用に関して、情報提供者の同意を得る。関連するセキュリティ管理策は、AP-2・AR-2・AR-3・AR-4・AR-5・IP-1・TR-1・TR-2。

拡張管理策:なし

参考文献:The Privacy Act of 1974, 5 U.S.C. § 552a (b)(1)

UL-2 第三者と情報を共有する

セキュリティ管理策:組織は、

a. 外部との個人情報の共有を Privacy Act および／または公示に記載されている、許可されている目的に適合する場合のみ、あるいはそれらの目的に適合する目的で行われる場合のみ、許可するのと合わせて、
b. 必要な場合には、第三者との間で、対象となる個人情報について記述のうえ個人情報を使用する目的を列挙する Memoranda of Understanding（もしくは Memoranda of Agreement または Letters of Intent もしくは Computer Matching Agreements 等の類似の契約）を締結するとともに、
c. 第三者との個人情報の共有をモニタリング、チェックし、職員に対して、許可を得た上での個人情報の共有と、許可を得ていない個人情報の使用または共有がもたらす影響について教育するのに加えて、
d. 第三者との間で提案されている、個人情報の共有の新たな事例を評価して、そうした共有が許可されているかどうか、追加の（あるいは新たな）公示が必要かどうかを判断する。

補足的ガイダンス:組織の上級プライバシー責任者／最高プライバシー責任者は、必要な場合には弁護士と協力して、公共部門の組織、国際的な組織、民間部門の組織など外部との間で提案されている、個人情報の共有についてレビューし、組織の既存の公示に記載されている使用に適合しているかどうかを確認し、適合する場合には承認する。外部との間で提案されている、個人情報の共有の新たな事例が現時点で、Privacy Actによって許可されていないおよび／または公示に記載されていない場合には、組織はそうした共有が公示に記載されている目的に適合するか否かを評価する。そうした共有が公示に記載されている目的に適合する場合には、組織は、PIA・SORN・ウェブサイトのプライバシーポリシーや、その他の公示をレビュー、更新し、再発行する。この際、新たな使用事例が存在する場合には、それらの事例ついての記述を

含めると同時に、必要かつ可能な場合には同意を得る。情報共有についての契約は、共有される情報の機微度に応じたセキュリティ保護も含む。関連するセキュリティ管理策は、AR-3・AR-4・AR-5・AR-8・AP-2・DI-1・DI-2・IP-1・TR-1。

拡張管理策：なし

参考文献：The Privacy Act of 1974, 5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o)・ISE Privacy Guidelines

謝辞

この付録は、NIST および Privacy Committee of the Federal Chief Information Officer (CIO) Council によって作成された。我々は、とりわけ Privacy Committee's Best Practices Subcommittee のメンバーと、Privacy Committee の Privacy Controls Appendix Working Group のメンバーである Claire Barrett 氏、Chris Brannigan 氏、Pamela Carcirieri 氏、Debra Diener 氏、Deborah Kendall 氏、Martha Landesberg 氏、Steven Lott 氏、Lewis Oleinick 氏、および Roanne Shaddox 氏には、Special Publication 800-53 の本付録の作成に役立つ見識をもたらし、技術顧問をしてくださったこと、そして全般的に寄与してくださったことに感謝の意を表する。また、Erika McCallister 氏、Toby Levin 氏、James McKenzie 氏、Julie McEwen 氏、および Richard Graubart 氏には、本プロジェクトに大きく寄与してくださったことに感謝する。さらに、Peggy Himes 氏と Elizabeth Lennon 氏には、極めて優れた管理支援に心から感謝する。著者は、また、公共および民間部門の個人、グループ、団体からいただいた多大な貢献にも心より感謝の意を表する。彼らの建設的で思慮深いコメントによって、この文書の全体的な質、完全さ、実用性が高められた。