Sec01-02-57\_各種ガイドブックの内容要約\_法令・規則・規約

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

1. 施策・政策・統計
   1. サイバーセキュリティ基本法（2016年4月15日改正）
      1. 目的
         1. サイバーセキュリティに関する施策を総合的かつ効果的に推進し、 もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。
   2. 【校正中】サイバーセキュリティ戦略（案）（2018年6月2日NISC）

ドキュメントを参照: [18shiryou01.pdf](https://www.nisc.go.jp/conference/cs/dai18/pdf/18shiryou01.pdf)

* + 1. 目的を達成するため、 戦略が寄与する政策領域ごとに、 今後３年間に執るべき諸施策の目標や実施方針
    2. 「サイバーセキュリティ戦略（案）」の全体概要
       1. サブトピック  
          
    3. 1. 策定の趣旨・背景
       1. 1.1. サイバー空間がもたらすパラダイムシフト
       2. 1.2. 2015 年以降の状況変化
    4. 2. サイバー空間に係る認識
       1. 2.1. サイバー空間がもたらす恩恵
          1. (1) サイバー空間におけるサービスの進展と社会への定着
          2. (2) AI の劇的な進化
          3. (3) IoT の進展
       2. 2.2. サイバー空間における脅威の深刻化
          1. (1) 業務・機能・サービス障害による社会への多大な影響
          2. (2) 情報の毀損及び漏えいによる競争力低下
          3. (3) 金銭の窃取・詐取等の損害
    5. 3. 本戦略の目的
       1. 3.1. 基本的な立場の堅持
          1. (1) 基本法の目的
          2. (2) 基本的な理念
          3. (3) 基本原則

① 情報の自由な流通の確保

② 法の支配

③ 開放性

④ 自律性

⑤ 多様な主体の連携

* + - 1. 3.2. 目指すサイバーセキュリティの基本的な在り方
         1. (1) 目指す姿
         2. (2) ３つの観点

① サービス提供者の任務保証～業務・サービスの着実な遂行～

② リスクマネジメント～不確実性の評価と適切な対応～

③ 参加・連携・協働～個人・組織による平時からの対策と連携・協働～

* + 1. 4. 目的達成のための施策
       1. 4.1. 経済社会の活力の向上及び持続的発展
          1. ポイント

サイバー空間と実空間の一体化が加速的に進展する中、 「Society5.0」の実現に向け て、 グーバルな規模でこれまで取引がなかった異なる業種の企業間取引が生まれて いる。

また、 その取引自体が自動化されたものになるなど、 従来のサプライチェーン を超えた多様かつ流動的な形態を見せている。

そして、 このような形態においては、 サプライチェーンのつながりの端で起こったサイバーセキュリティの問題が、 実空間、 さらには、 経済社会全体にこれまで以上に広く波及し、 甚大な悪影響を及ぼすおそれ がある。

このようなリスクを認識し、 サプライチェーン全体を俯瞰した取組を推進す ることが不可欠である。

* + - * 1. 新たな価値創出を支えるサイバーセキュリティの推進

(1) 経営層の意識改革

(2) サイバーセキュリティに対する投資の推進

(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化

* + - * 1. 多様なつながりから価値を生み出すサプライチェーンの実現

(1) サイバーセキュリティ対策指針の策定

サプライチェーンにおけるつながりが多様かつ流動的な形態になる中、 サイバーセキュリティの確保を進めていくためには、 サプライチェーン全体に対して、 一貫性をもった必要な対策が実装されることが不可欠である。 また、 このような取組を通じて、 モノやサービスに関わる品質が新たな価値を生み出すことが期待される。

具体的には、

官民が連携して、 サプライチェーンにおける脅威を明確化し、 運用レベルでの対策が実施できるような業種横断的な指針を策定するとともに、 その普及を図る。

その際には、 中小企業を含めた事業者が実際に対策を行いやすくするため、 事業者の事情を踏まえた現実的に実施が可能な内容で、 かつ、 分かりやすいものとなるように十分に配慮する。

また、 事業者がリスクと対策費用のバランスを意識できるものとすることも重要である。

産業分野毎のサプライチェーンに関わるつながり方や守るべきもの、 脅威の差異を意識しつつ、 IoT 機器や組織等に求められる具体的な対応策を産業分野毎に示していく必要がある。

さらに、 サプライチェーンがグーバルに拡がる中で、 我が国における対策指針に基づくサイバーセキュリティ対策がグーバルに認められるようにするため、 海外におけるルール化の動きも反映する必要がある。

(2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

サプライチェーン全体としてのサイバーセキュリティを確保するためには、 製造される機器、 生成されて流通するデータ、 それらを利用したサービス等のサプライチェーンの構成要素における信頼の確保が不可欠である。

このため、 それぞれの構成要素がセキュリティ要件を満たした形で生成・流通されるよう、 要件の明確化を図るとともに、 その要件が満たされていることを確認等することにより信頼を創出する仕組みの構築が必要である。

また、 サプライチェーンにおける調達者が機器・サービス等の利用に際し、 その信頼を確認できるよう、 官民が連携して、 信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。

さらに、 これらがサプライチェーンのつながりにおいて、 連続的な仕組みとなるよう、 トレーサビリティ39を確認するための仕組みと、 創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する。

(3) 中小企業の取組の促進

中小企業は、 サイバー攻撃により、 金銭的な損害や信用の低下が生じた場合、 経営に与えるインパクトが大企業と比べて大きい。

また、 中小企業が踏み台となって自社のみならず取引先までサイバー攻撃の影響が拡大することも懸念されている。

一方、 中小企業は、 必ずしも高いサイバーセキュリティに関する知識やスキルを有しているとはいえず、 サイバーセキュリティに対して十分な投資を行うことが難しいという事情を踏まえた上で、 サイバーセキュリティ対策を推進する必要がある。

このため、 国は、 中小企業を対象として、 安全な情報システムの利活用モデルの提示を含む理解しやすいサイバーセキュリティ対策の事例集を作成するとともに、 サイバーセキュリティ保険の活用促進、 中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化を行う。

また、 官民が連携して、 サイバーセキュリティに取り組んでいる中小企業が、 それを自主的に宣言できる仕組みなどの可視化の取組を促進するとともに、 インセンティブの仕組みとの連携により、 効果的に中小企業のサイバーセキュリティを進めるための仕組み作りを行う。

* + - * 1. 安全なIoT システムの構築

(1) IoT システムにおけるサイバーセキュリティの体系の整備と国際標準化

これまで、

IoT システムのサイバーセキュリティ対策については、 官民が連携し、 ガイドラインの策定を始めとする安全なIoT システムの実現に向けた様々な取組を推進してきた。

今後は、 安全なIoT システムが価値を創出することに重点を置き、 一定の整合性・一貫性をもって戦略的に取り組む必要がある。

このため、

我が国がこれまで示してきた安全なIoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素41に基づき、 各主体の間で対策に係る基本理念、 目標、 方法、 期限等についての共通認識の醸成と、 各分野・各主体の役割や機能の明確化を図った上で、 自律的にサイバーセキュリティに関わる取組を進めつつ、 各主体が協働した取組を推進する。

また、 国は、 こうした取組を促すため、 官民の各主体が抱える課題42やそれぞれの取組について、 全体像が俯瞰できる形で可視化するとともに、 情報共有を行うための仕組みを構築する。

さらに、 IoT システムにおける価値創出の仕組みを、 我が国の安全・安心といった強みを活かしながらグーバルな規模で展開し、 安全なIoT システムの普及によって国際経済の発展に貢献するため、 官民が連携の下、 安全なIoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する。

(2) 脆弱性対策に係る体制の整備

IoT 機器に対するサイバー攻撃等の深刻化に対応するため、

ネットワークの安全・信頼性を確保する観点で、 産官学民及び民間企業相互間の連携と役割分担の下、 対策を推進することが重要である。

このため、 官民が連携して、 IoT 機器の脆弱性について、 設計・製造、 運用、 そして破棄までのライフサイクル全体を見通したサイバーセキュリティ対策や、 ネットワーク上の脆弱な IoT 機器の対策等のための体制整備が必要である。

ライフサイクルを見通した IoT 機器のサイバーセキュリティ対策については、

それぞれの機器の利用方法やサイバーセキュリティ上の脅威、 諸外国の検討状況や技術の進展の動向等を十分踏まえた上で、 機器製造事業者、 電気通信事業者、 利用者等の各々の主体の相互理解と連携の下で取り組むべきである。 その中で、 官民が連携して、 それぞれの IoT 機器について、 その特性や利用方法等を踏まえつつ必要なサイバーセキュリティの要件を整理し、 その要件を満たすIoT 機器の利用を推奨する。

また、 ネットワーク上の脆弱な IoT 機器の対策については、

パスワード設定に不備のある機器の調査・特定を行い、 電気通信事業者において当該機器の利用者への注意

喚起を円滑に行えるよう、 所要の制度整備を着実に進める。 また、 対策の実施に当たっては、 関係省庁等が一体となって、 電気通信事業者、 機器製造事業者等と連携して取り組む。

将来的には、

これらの我が国の対策をモデルとして、 国際的な連携や標準化等を通じて海外に展開し、 安全なネットワークの環境整備に貢献をしていく。

* + - 1. 4.2. 国民が安全で安心して暮らせる社会の実現
         1. 国民・社会を守るための取組

(1) 安全・安心なサイバー空間の利用環境の構築

(2) サイバー犯罪への対策

* + - * 1. 官民一体となった重要インフラの防護

(1) 行動計画に基づく主な取組

① リスクマネジメントの推進

② 安全基準等の改善・浸透

③ 深刻度評価基準

④ 官民の枠を超えた訓練・演習の実施

⑤ 制御系システムのセキュリティ対策

(2) 地方公共団体のセキュリティ強化・充実

* + - * 1. 政府機関等におけるセキュリティ強化・充実

(1) 情報システムのセキュリティ対策の高度化・可視化

① 情報システムの防御能力の向上と状態の把握

② 政府機関等における横断的な連携の高度化による被害の発生・拡大の防止

(2) クラウド化の推進等による効果的なセキュリティ対策

(3) 先端技術の活用による先取り対応への挑戦

(4) 監査を通じたサイバーセキュリティの水準の向上

(5) 組織的な対応能力の充実

* + - * 1. 大学等における安全・安心な教育・研究環境の確保

(1) 大学等の多様性を踏まえた対策の推進

(2) 大学等の連携協力による取組の推進

* + - * 1. 2020 年東京大会とその後を見据えた取組

(1) 2020 年東京大会に向けた態勢の整備

(2) 未来につながる成果の継承

* + - * 1. 従来の枠を超えた情報共有・連携体制の構築

(1) 多様な主体の情報共有・連携の推進

(2) 情報共有・連携の新たな段階へ

* + - * 1. 大規模サイバー攻撃事態等への対処態勢の強化
      1. 4.3. 国際社会の平和・安定及び我が国の安全保障への寄与
         1. 自由、 公正かつ安全なサイバー空間の堅持

(1) 自由、 公正かつ安全なサイバー空間の理念の発信

(2) サイバー空間における法の支配の推進

* + - * 1. 我が国の防御力・抑止力・状況把握力の強化

(1) 国家の強靱性の確保

① 任務保証

② 我が国の先端技術・防衛関連技術の防護

③ サイバー空間を悪用したテ組織の活動への対策

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応

② 信頼醸成措置

(3) サイバー空間の状況把握の強化

① 関係機関の能力向上

② 脅威情報連携

* + - * 1. 国際協力・連携

(1) 知見の共有・政策調整

(2) 事故対応等に係る国際連携の強化

(3) 能力構築支援

* + - 1. 4.4. 横断的施策
         1. 人材育成・確保

(1) 戦略マネジメント層の育成・定着

(2) 実務者層・技術者層の育成

(3) 人材育成基盤の整備

(4) 各府省庁におけるセキュリティ人材の確保・育成の強化

(5) 国際連携の推進

* + - * 1. 研究開発の推進

(1) 実践的な研究開発の推進

(2) 中長期的な技術・社会の進化を視野に入れた対応

* + - * 1. 全員参加による協働
    1. 5. 推進体制
  1. サイバーセキュリティ戦略（2015年9月4日閣議決定）
     1. 2020年代初頭までを見据えつつ、 サイバーセキュリティ政策の基本的な方向性を示す
     2. １ サイバー空間に係る認識
        1. サイバー空間は、 「無限の価値を産むフンティア」である人工空間であり、 人々の経済社会の活動基盤
        2. あらゆるモノがネットワークに連接され、 実空間とサイバー空間との融合が高度に深化した「連接融合情報社会(連融情報社会)」が到来。 同時に、 サイバー攻撃の被害規模や社会的影響が年々拡大、 脅威の更なる深刻化が予想
     3. ２ 目的
        1. 「経済社会の活力の向上及び持続的発展」、 「国民が安全で安心して暮らせる社会の実現」、 「国際社会の平和・安定及び我が国の安全保障」に寄与する。
        2. そのために、 「自由、 公正かつ安全なサイバー空間」を創出・発展させる
     4. ３ 基本原則
        1. ① 情報の自由な流通の確保② 法の支配③ 開放性④ 自律性⑤ 多様な主体の連携
     5. ４ 目的達成のための施策
        1. ①後手から先手へ／ ②受動から主導へ／ ③サイバー空間から融合空間へ
        2. 経済社会の活力の向上及び持続的発展
           1. ～ 費用から投資へ ～
           2. ■安全なIoTシステムの創出

安全なIoT活用による新産業創出

* + - * 1. ■セキュリティマインドを持った企業経営の推進

経営層の意識改革、 組織内体制の整備

* + - * 1. ■セキュリティに係るビジネス環境の整備

ファンドによるセキュリティ産業の振興

* + - 1. 国民が安全で安心して暮らせる社会の実現
         1. ～ 2020年・その後に向けた基盤形成 ～
         2. ■国民・社会を守るための取組

事業者の取組促進、 普及啓発、 サイバー犯罪対策

* + - * 1. ■重要インフラを守るための取組

防護対象の継続的見直し、 情報共有の活性化

* + - * 1. ■政府機関を守るための取組

攻撃を前提とした防御力強化、 監査を通じた徹底

* + - 1. 国際社会の平和・安定及び我が国の安全保障
         1. ～ サイバー空間における積極的平和主義～
         2. ■我が国の安全の確保

警察・自衛隊等のサイバー対処能力強化

* + - * 1. ■国際社会の平和・安定

国際的な「法の支配」確立、 信頼醸成推進

* + - * 1. ■世界各国との協力・連携

米国・ASEANを始めとする諸国との協力・連携

* + - 1. 横断的施策
         1. ■研究開発の推進

攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

* + - * 1. ■人材の育成・確保

ハイブリッド型人材の育成、 実践的演習、 突出人材の発掘・確保、 キャリアパス構築

* + 1. ５ 推進体制
       1. 官民及び関係省庁間の連携強化、 東京オリンピック・パラリンピック競技大会等に向けた対応
  1. サイバーセキュリティ2016【2016年サイバーセキュリティ戦略本部】

ドキュメントを参照: [cyber-security2016.pdf](https://www.nisc.go.jp/active/kihon/pdf/cyber-security2016.pdf)

* 1. 「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）」（2016年8月31日サイバーセキュリティ戦略本部決定）
     1. http://www.nisc.go.jp/active/general/kijun28.html

ドキュメントを参照: [kijun28.html](http://www.nisc.go.jp/active/general/kijun28.html)

* 1. 企業経営のためのサイバーセキュリティの考え方の策定について（2016年8月2日）【NISC】

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* + 1. http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* + 1. サイバーセキュリティ戦略本部

ドキュメントを参照: [index.html](http://www.nisc.go.jp/conference/cs/index.html)

* + - 1. http://www.nisc.go.jp/conference/cs/index.html

ドキュメントを参照: [index.html](http://www.nisc.go.jp/conference/cs/index.html)

* + 1. 経営層に期待される 認識 や経営戦略を企画する人材層に向けた実装のためのツールを示す
    2. 基本方針
       1. ーサイバーセキュリティは、 より積極的な経営への「投資」へー
       2. サイバーセキュリティをやむを得ない「費用」でなく、 積極的な経営への「投資」と位置づけ、 企業としての「挑戦」と、 それに付随する「責任」として取り組むことが期待される
    3. I.基本的考え方
       1. 二つの基本的認識
          1. ＜①挑戦＞

新しい製品やサービスを創造するための戦略の一環として考えていく

サブトピック

* + - * 1. ＜②責任＞

サイバーセキュリティに取り組むことは社会的な要求・要請であり、 自社のみならず社会全体の発展にも寄与する

* + - 1. 三つの留意事項
         1. ＜①情報発信による社会的評価の向上＞

「セキュリティ品質」を高め、 品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。

そのような取組に係る姿勢や方針を情報発信することが重要。

* + - * 1. ＜②リスクの一項目としてのサイバーセキュリティ＞

提供する機能やサービスを全うする（機能保証）という観点から、 リスクの一項目としてのサイバーセキュリティの視点も踏まえ、 リスクを分析し、 総合的に判断。

経営層のリーダーシップが必要。

* + - * 1. ＜③サプライチェーン全体でのサイバーセキュリティの確保＞

サプライチェーンの一部の対策が不十分な場合でも、 自社の重要情報が流出するおそれあり。

一企業のみでの対策には限界があるため、 関係者間での情報共有活動への参加等が必要。

* + 1. II.企業の視点別の取組
       1. ITの利活用やサイバーセキュリティへの取組において、 各企業の事業規模のみならず、 その認識の違いなどを踏まえて取り組んでいく必要がある
       2. ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業
          1. （積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）
          2. 【経営者に期待される認識】

積極的なITの利活用を推進する中で、 製品やサービスの「セキュリティ品質」を一層高め、 自社のブランド価値の向上につなげるべく、 システムの基盤におけるセキュリティの向上、 情報・データの保護、 製品等の安全品質向上に取り組む。

様々な関係者との協働が重要であるため、 情報提供に主体的に取り組む。

決して現存する標準や取り組みなどに満足することなく、 実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、 変革していく存在となることが期待される。

* + - * 1. 【実装に向けたツール】

IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）

自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

* + - 1. IT・セキュリティをビジネスの基盤として捉えている企業
         1. （IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）
         2. 【経営者に期待される認識】

経営者のリーダーシップによって、 社会的責任としてのサイバーセキュリティ対策に取り組む。

サプライチェーンやビジネスパートナー、 委託先を含めた対策を行う。

平時・緊急時のいずれにおいても、 情報開示などの適切なコミュニケーションを行う。

* + - * 1. 【実装に向けたツール】

サイバーセキュリティ経営ガイドライン

企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用

サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

* + - 1.  自らセキュリティ対策を行う上で、 事業上のリソースの制約が大きい企業
         1. （主に中小企業等でセキュリティの専門組織を保持することが困難な企業）
         2. 【経営者に期待される認識】

サプライチェーンを通じて中小企業等の役割はますます重要となる中、 消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、 取り組む。

外部の能力や知見を活用しつつ、 効率的に進める方策を検討する。

* + - * 1. 【実装に向けたツール】

効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）

 サイバーセキュリティに関する相談窓やセミナー、 地域の相談員等の活用

* 1. サイバーセキュリティ関連施策に関する平成29年度予算重点化方針

ドキュメントを参照: [yosanhoshin29.pdf](http://www.nisc.go.jp/active/kihon/pdf/yosanhoshin29.pdf)

* 1. サイバーセキュリティ政策の評価に係る基本方針

ドキュメントを参照: [cs\_hyouka\_houshin.pdf](http://www.nisc.go.jp/active/kihon/pdf/cs_hyouka_houshin.pdf)

* 1. 情報セキュリティ白書2017【2017年7月IPA】

ドキュメントを参照: [2017.html](https://www.ipa.go.jp/security/publications/hakusyo/2017.html)

* + 1. 序章 2016年度の情報セキュリティの概況
    2. 第1章 情報セキュリティインシデント・脆弱性の現状と対策
       1. 1.1 2016年度に観測されたインシデント状況
       2. 1.2 情報セキュリティインシデント別の状況と事例
       3. 1.3 攻撃・手の動向と対策
       4. 1.4 情報システムの脆弱性の動向
       5. 1.5 情報セキュリティ対策の状況
    3. 第2章 情報セキュリティを支える基盤の動向
       1. 2.1 日本の情報セキュリティ政策の状況
       2. 2.2 情報セキュリティ関連法の整備状況
       3. 2.3 国別・地域別の情報セキュリティ政策の状況
       4. 2.4 情報セキュリティ人材の現状と育成
       5. 2.5 情報セキュリティマネジメント
       6. 2.6 国際標準化活動
       7. 2.7 評価認証制度
       8. 2.8 情報セキュリティの普及啓発活動
       9. 2.9 情報セキュリティ産業の規模と成長の動向
       10. 2.10 その他の情報セキュリティの状況
    4. 第3章 個別テーマ
       1. 3.1 制御システムの情報セキュリティ
       2. 3.2 IoTの情報セキュリティ
       3. 3.3 スマートデバイスの情報セキュリティ
       4. 3.4 金融の情報セキュリティ
       5. 3.5 オリンピックに向けた情報セキュリティ対策
    5. 付録 情報セキュリティ10大脅威2017・資料・ツール
       1. 情報セキュリティ10大脅威2017
       2. 資料A 2016年のコンピュータウイルス届出状況
       3. 資料B 2016年のコンピュータ不正アクセス届出状況
       4. 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
       5. ツール 各ツールの紹介

1. ISMS
   1. 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】
      1.  管理的対策
         1. A.5 情報セキュリティのための方針群
            1. A.5.1 情報セキユリティのための経営陣の方向性

情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項並びに関連する法令及び規制に従って提示するため。

A.5.1.1 情報セキュリティのための方針群

情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知することが望ましい。

CSF

ガバナンス（ID.GV）

ID.GV-1 自組織の情報セキュリティポリシーを定めている。

A.5.1.2 情報セキュリティのための方針群のレビュー

情報セキュリティのための方針群は，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューすることが望ましい。

* + - 1. A.6 情報セキュリティのための組織
         1. A.6.1 内部組織

組織内で情報セキュリティの実施及び運用に着手し，これを統制するための管理上の枠組みを確立するため。

A.6.1.1 情報セキュリティの役割及び責任

全ての情報セキュリティの責任を定め，割り当てることが望ましい。

CSF

資産管理（ID.AM）

ID.AM-6

ガバナンス（ID.GV）

ID.GV-2

意識向上およびトレーニング（PR.AT）

PR.AT-2

PR.AT-3

PR.AT-4

PR.AT-5

検知プロセス（DE.DP）

DE.DP-1

伝達（RS.CO）

RS.CO-1

A.6.1.2 職務の分離

相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.6.1.3 関係当局との連絡

関係当局との適切な連絡体制を維持することが望ましい。

CSF

伝達（RS.CO）

RS.CO-2

A.6.1.4 専門組織との連絡

情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持することが望ましい。

CSF

リスクアセスメント（ID.RA）

ID.RA-2

A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ

プロジェクトの種類にかかわらず，プロジェクトマネジメントにおいては，情報セキュリティに取り組むことが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

* + - * 1. A.6.2 モバイル機器及びテレワーキング

モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

A.6.2.1 モバイル機器の方針

モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用することが望ましい。

A.6.2.2 テレワーキング

テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-3

* + - 1. A.8 資産の管理
         1. A.8.1 資産に対する責任

組織の資産を特定し，適切な保護の責任を定めるため。

A.8.1.1 資産目録

情報及び情報処理施設に関連する資産を特定することが望ましい。 また，これらの資産の目録を，作成し，維持することが望ましい。

CSF

資産管理（ID.AM）

ID.AM-1

ID.AM-2

A.8.1.2 資産の管理責任

目録の中で維持される資産は，管理されることが望ましい。

注6.1.2及び6.1.3では，情報セキュリティのリスクを運用管理することについて責任及び権限をもつ人又は主体をリスク所有者としている。 情報セキュリティにおいて，多くの場合，資産の管理責任を負う者はリスク所有者でもある。

CSF

資産管理（ID.AM）

ID.AM-1

ID.AM-2

A.8.1.3 資産利用の許容範囲

情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。

A.8.1.4 資産の返却

全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-11

* + - * 1. A.8.2 情報分類

組織に対する情報の重要性に応じて，情報の適切なレベルでの保護を確実にするため。

A.8.2.1 情報の分類

情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類することが望ましい。

CSF

資産管理（ID.AM）

ID.AM-5

A.8.2.2 情報のラベル付け

情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

保護技術（PR.PT）

PR.PT-2

A.8.2.3 資産の取り扱い

資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-1

PR.DS-2

PR.DS-3

PR.DS-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

保護技術（PR.PT）

PR.PT-2

* + - * 1. A.8.3 媒体の取扱い

媒体に保存された情報の認可されていない開示，変更，除去又は破壊を防止するため。

A.8.3.1 取外し可能な媒体の管理

組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

保護技術（PR.PT）

PR.PT-2

A.8.3.2 媒体の処分

媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

A.8.3.3 物理的媒体の輸送

情報を格納した媒体は，輸送の途中における，認可されていないアクセス，不正使用又は破損から保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

保護技術（PR.PT）

PR.PT-2

* + - 1. A.12 運用のセキュリティ
         1. A.12.1 運用の手順及び責任

情報処理設備の正確かつセキュリティを保った運用を確実にするため。

A.12.1.1 操作手順書

操作手順は，文書化し，必要とする全ての利用者に対して利用可能とすることが望ましい。

A.12.1.2 変更管理

情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.12.1.3 容量・能力の管理

要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整し，また，将来必要とする容量・能力を予測することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-4

A.12.1.4 開発環境、 試験環境及び運用環境の分離

開発環境，試験環境及び運用環境は，運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-7

* + - * 1. A.12.2 マルウェアからの保護

情報及び情報処理施設がマルウェアから保護されることを確実にするため。

A.12.2.1 マルウェアに対する管理策

マルウェアから保護するために，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-6

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-4

低減（RS.MI）

RS.MI-2

* + - * 1. A.12.3 バックアップ

データの消失から保護するため。

A.12.3.1 情報のバックアップ

情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-4

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-4

* + - * 1. A.12.4 ログ取得及び監視

A.12.4.1 イベントログ取得

利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューすることが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-3

分析 (RS.AN)

RS.AN-1

A.12.4.2 ログ情報の保護

ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護することが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

A.12.4.3 実務管理者及び運用担当者の作業ログ

システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューすることが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

分析 (RS.AN)

RS.AN-1

A.12.4.4 クロックの同期

組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは，単一の参照時刻源と同期させることが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

* + - * 1. A.12.5 運用ソフトウエアの管理

運用システムの完全性を確実にするため。

A.12.5.1 運用システムに関わるソフトウェアの導入

運用システムに関わるソフトウェアの導入を管理するための手順を実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-6

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

* + - * 1. A.12.6 技術的ぜい弱性管理

技術的ぜい弱性の悪用を防止するため。

A.12.6.1 技術的脆弱性の管理

利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得することが望ましい。 また，そのようなぜい弱性に組織がさらされている状況を評価することが望ましい。 さらに，それらと関連するリスクに対処するために，適切な手段をとることが望ましい。

CSF

リスクアセスメント（ID.RA）

ID.RA-1

ID.RA-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-12

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-8

低減（RS.MI）

RS.MI-3

A.12.6.2 ソフトウェアのインストールの制限

利用者によるソフトウェアのインストールを管理する規則を確立し，実施することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

* + - * 1. A.12.7 情報システムの監査に対する考慮事項

運用システムに対する監査活動の影響を最小限にするため。

A.12.7.1 情報システムの監査に対する管理

運用システムの検証を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意することが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

* + - 1. A.15 供給者関係
         1. A.15.1 供給者関係における情報セキュリティ

供給者がアクセスできる組織の資産の保護を確実にするため。

A.15.1.1 供給者関係のための情報セキュリティの方針

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化することが望ましい。

CSF

保守（PR.MA）

PR.MA-2

A.15.1.2 供給者との合意におけるセキュリティの取扱い

関連する全ての情報セキュリティ要求事項を確立し，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意することが望ましい。

A.15.1.3 ICTサプライチェーン

供給者との合意には，情報通信技術（以下，ICT という。 ）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-1

* + - * 1. A.15.2 供給者のサービス提供の管理

供給者との合意に沿って，情報セキュリティ及びサービス提供について合意したレベルを維持するため。

A.15.2.1 供給者のサービス提供の監視及びレビュー

組織は，供給者のサービス提供を定常的に監視し，レビューし，監査することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-1

保守（PR.MA）

PR.MA-2

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-6

A.15.2.2 供給者のサービス提供の変更に対する管理

関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。 ）を管理することが望ましい。

* + - 1. A.16 情報セキュリティインシデント管理
         1. A.16.1 情報セキュリティインシデントの管理及びその改善

セキュリティ事象及びセキュリティ弱点に関する伝達を含む，情報セキュリティインシデントの管理のための，一貫性のある効果的な取組みを確実にするため。

A.16.1.1 責任及び手順

情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-9

異常とイベント（DE.AE）

DE.AE-2

伝達（RS.CO）

RS.CO-1

A.16.1.2 情報セキュリティ事象の報告

情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告することが望ましい。

CSF

検知プロセス（DE.DP）

DE.DP-4

伝達（RS.CO）

RS.CO-2

A.16.1.3 情報セキュリティ弱点の報告

組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求することが望ましい。

A.16.1.4 情報セキュリティ事象の評価及び決定

情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定することが望ましい。

CSF

異常とイベント（DE.AE）

DE.AE-2

分析 (RS.AN)

RS.AN-4

A.16.1.5 情報セキュリティインシデントへの対応

情報セキュリティインシデントは，文書化した手順に従って対応することが望ましい。

CSF

対応計画（RS.RP）

RS.RP-1

分析 (RS.AN)

RS.AN-1

低減（RS.MI）

RS.MI-1

RS.MI-2

復旧計画（RC.RP）

RC.RP-1

A.16.1.6 情報セキュリティインシデントからの学習

情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いることが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-8

検知プロセス（DE.DP）

DE.DP-5

分析 (RS.AN)

RS.AN-2

改善（RS.IM）

RS.IM-1

A.16.1.7 証拠の収集

組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用することが望ましい。

CSF

分析 (RS.AN)

RS.AN-3

* + - 1. A.17 事業継続マネジメントにおける情報セキュリティの側面
         1. A.17.1 情報セキュリティ継続

情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むことが望ましい。

A.17.1.1 情報セキュリティ継続の計画

組織は，困難な状況（adverse situation）（例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-9

A.17.1.2 情報セキュリティ継続の実施

組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-4

PR.IP-9

A.17.1.3 情報セキュリティ継続の検証、 レビュー及び評価

確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-10

PR.IP-4

* + - * 1. A.17.2 冗長性

情報処理施設の可用性を確実にするため。

A.17.2.1 情報処理施設の可用性

情報処理施設は，可用性の要求事項を満たすのに十分な冗長性をもって，導入することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

* + - 1. A.18 順守
         1. A.18.1 法的及び契約上の要求事項の順守

情報セキュリティに関連する法的，規制又は契約上の義務に対する違反，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

A.18.1.1 適用法令及び契約上の要求事項の特定

各情報システム及び組織について，全ての関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組みを，明確に特定し，文書化し，また，最新に保つことが望ましい。

A.18.1.2 知的財産権

知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を実施することが望ましい。

A.18.1.3 記録の保護

記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-4

A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護

プライバシー及び PII の保護は，関連する法令及び規制が適用される場合には，その要求に従って確実にすることが望ましい。

CSF

検知プロセス（DE.DP）

DE.DP-2

A.18.1.5 暗号化機能に対する規制

暗号化機能は，関連する全ての協定，法令及び規制を順守して用いることが望ましい。

CSF

ガバナンス（ID.GV）

ID.GV-3

* + - * 1. A.18.2 情報セキュリティのレビュー

組織の方針及び手順に従って情報セキュリティが実施され，運用されることを確実にするため。

A.18.2.1 情報セキュリティの独立したレビュー

情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，あらかじめ定めた間隔で，又は重大な変化が生じた場合に，独立したレビューを実施することが望ましい。

A.18.2.2 情報セキュリティのための方針群及び標準の順守

管理者は，自分の責任の範囲内における情報処理及び手順が，適切な情報セキュリティのための方針群，標準類，及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューすることが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-12

A.18.2.3 技術的順守のレビュー

情報システムを，組織の情報セキュリティのための方針群及び標準の順守に関して，定めに従ってレビューすることが望ましい。

CSF

リスクアセスメント（ID.RA）

ID.RA-1

* + 1.  人的対策
       1. A.7 人的資源のセキュリティ
          1. A.7.1 雇用前

従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にするため。

A.7.1.1 選考

全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行うことが望ましい。 また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行うことが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-11

A.7.1.2 雇用条件

従業員及び契約相手との雇用契約書には，情報セキュリティに関する各自の責任及び組織の責任を記載することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

* + - * 1. A.7.2 雇用期間中

従業員及び契約相手が，情報セキュリティの責任を認識し，かつ，その責任を遂行することを確実にするため。

A.7.2.1 経営陣の責任

経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求することが望ましい。

CSF

ガバナンス（ID.GV）

ID.GV-2

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受け，また，定めに従ってその更新を受けることが望ましい。

CSF

意識向上およびトレーニング（PR.AT）

PR.AT-1

PR.AT-2

PR.AT-3

PR.AT-4

PR.AT-5

A.7.2.3 懲戒手続き

情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えることが望ましい。

* + - * 1. A.7.3 雇用の終了及び変更

雇用の終了又は変更のプロセスの一部として，組織の利益を保護するため。

A.7.3.1 雇用の終了又は変更に関する責任

雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め，その従業員又は契約相手に伝達し，かつ，遂行させることが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-11

* + 1.  物理的対策
       1. A.11 物理的及び環境的セキュリティ
          1. A.11.1 セキュリティを保つべき領

組織の情報及び情報処理施設に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。

A.11.1.1 物理的セキュリティ境界

取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界を定め，かつ，用いることが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-2

A.11.1.2 物理的入退管理策

セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-2

保守（PR.MA）

PR.MA-1

A.11.1.3 オフィス， 部屋及び施設のセキュリティ

オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用することが望ましい。

A.11.1.4 外部及び環境の脅威からの保護

自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

アクセス制御（PR.AC）

PR.AC-2

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.1.5 セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関する手順を設計し，適用することが望ましい。

A.11.1.6 受渡場所

荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理することが望ましい。 また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離すことが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-2

* + - * 1. A.11.2 装置

資産の損失，損傷，盗難又は劣化，及び組織の業務に対する妨害を防止するため。

A.11.2.1 装置の設置及び保護

装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.2.2 サポートユーティリティ（ライフライン事業者）

装置は，サポートユーティリティの不具合による，停電，その他の故障から保護することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-4

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.2.3 ケーブル配線のセキュリティ

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-4

アクセス制御（PR.AC）

PR.AC-2

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.2.4 装置の保守

装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守することが望ましい。

CSF

保守（PR.MA）

PR.MA-1

PR.MA-2

A.11.2.5 資産の移動

装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出さないことが望ましい。

CSF

保守（PR.MA）

PR.MA-1

A.11.2.6 構外にある装置及び資産のセキュリティ

構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用することが望ましい。

CSF

資産管理（ID.AM）

ID.AM-4

A.11.2.7 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した全ての装置は，処分又は再利用する前に，全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又はセキュリティを保って上書きしていることを確実にするために，検証することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

A.11.2.8 無人状態にある利用者装置

利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にすることが望ましい。

A.11.2.9 クリアデスク・クリアスクリーン方針

書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用することが望ましい。

CSF

保護技術（PR.PT）

PR.PT-2

* + 1.  技術的対策
       1. A.9 アクセス制御
          1. A.9.1 アクセス制御に対する業務上の要求事項

情報及び情報処理施設へのアクセスを制限するため。

A.9.1.1 アクセス制御方針

アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューすることが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

A.9.1.2 ネットワークおよびネットワークサービスへのアクセス

利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

保護技術（PR.PT）

PR.PT-3

* + - * 1. A.9.2 利用者アクセスの管理

システム及びサービスへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため。

A.9.2.1 利用者登録及び登録削除

アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.2.2 利用者アクセスの提供（プロビジョニング）

全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者アクセスの提供についての正式なプロセスを実施することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.2.3 特権的アクセス権の管理

特権的アクセス権の割当て及び利用は，制限し，管理することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.9.2.4 利用者の秘密認証情報の管理

秘密認証情報の割当ては，正式な管理プロセスによって管理することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.2.5 利用者アクセス権のレビュー

資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューすることが望ましい。

A.9.2.6 アクセス権の削除または修正

全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正することが望ましい。

* + - * 1. A.9.3 利用者の責任

利用者に対して，自らの秘密認証情報を保護する責任をもたせるため。

A.9.3.1 秘密認証情報の利用

秘密認証情報の利用時に，組織の慣行に従うことを，利用者に要求することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

* + - * 1. A.9.4 システム及びアプリケーションのアクセス制御

システム及びアプリケーションへの，認可されていないアクセスを防止するため。

A.9.4.1 情報へのアクセス制限

情報及びアプリケーションシステム機能へのアクセスは，アクセス制御方針に従って，制限することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.9.4.2 セキュリティに配慮したログオン手順

アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.4.3 パスワード管理システム

パスワード管理システムは，対話式とすることが望ましく，また，良質なパスワードを確実とするものが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.4.4 特権的なユーティリティプログラムの使用

システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.9.4.5 プログラムソースコードへのアクセス制御

プログラムソースコードへのアクセスは，制限することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

* + - 1. A.10 暗号
         1. A.10.1 暗号による管理策

情報の機密性，真正性及び／又は完全性を保護するために，暗号の適切かつ有効な利用を確実にするため。

A.10.1.1 暗号による管理策の利用方針

情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施することが望ましい。

A.10.1.2 鍵管理

暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施することが望ましい。

* + - 1. A.13 通信のセキュリティ
         1. A.13.1 ネットワークセキュリティ管理

ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため。

A.13.1.1 ネットワーク管理策

システム及びアプリケーション内の情報を保護するために，ネットワークを管理し，制御することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-3

PR.AC-5

データセキュリティ（PR.DS）

PR.DS-2

保護技術（PR.PT）

PR.PT-4

A.13.1.2 ネットワークサービスのセキュリティ

組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，セキュリティ機能，サービスレベル及び管理上の要求事項を特定し，また，ネットワークサービス合意書にもこれらを盛り込むことが望ましい。

A.13.1.3 ネットワークの分離

情報サービス，利用者及び情報システムは，ネットワーク上で，グループごとに分離することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-5

データセキュリティ（PR.DS）

PR.DS-5

* + - * 1. A.13.2 情報の転送

組織の内部及び外部に転送した情報のセキュリティを維持するため。

A.13.2.1 情報転送の方針及び手順

あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えることが望ましい。

CSF

資産管理（ID.AM）

ID.AM-3

アクセス制御（PR.AC）

PR.AC-3

PR.AC-5

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

保護技術（PR.PT）

PR.PT-4

A.13.2.2 情報転送に関する合意

合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱うことが望ましい。

A.13.2.3 電子的メッセージ通信

電子的メッセージ通信に含まれた情報は，適切に保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

A.13.2.4 秘密保持契約又は守秘義務契約

情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

* + - 1. A.14 システムの取得、 開発及び保守
         1. A.14.1 情報システムのセキユリティ要求事項

ライフサイクル全体にわたって，情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。 これには，公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

A.14.1.1 情報セキュリティ要求事項の分析及び仕様化

情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めることが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮

公衆ネットワークを経由するアプリケーションサービスに含まれる情報は，不正行為，契約紛争，並びに認可されていない開示及び変更から保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

PR.DS-6

A.14.1.3 アプリケーションサービスのトランザクションの保護

アプリケーションサービスのトランザクションに含まれる情報は，次の事項を未然に防止するために，保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

PR.DS-6

* + - * 1. A.14.2 開発及びサポートプロセスにおけるセキュリティ

情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため。

A.14.2.1 セキュリティに配慮した開発のための方針

ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.14.2.2 システムの変更管理手順

開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー

オペレーティングプラットフォームを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要なアプリケーションをレビューし，試験することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.14.2.4 パッケージソフトウェアに対する制限

パッケージソフトウェアの変更は，抑止し，必要な変更だけに限ることが望ましい。 また，全ての変更は，厳重に管理することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.14.2.5 セキュリティに配慮したシステム構築の原則

セキュリティに配慮したシステムを構築するための原則を確立し，文書化し，維持し，全ての情報システムの実装に対して適用することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.14.2.6 セキュリティに配慮したシステム開発環境

組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，適切に保護することが望ましい。

A.14.2.7 外部委託による開発

組織は，外部委託したシステム開発活動を監督し，監視することが望ましい。

CSF

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-6

A.14.2.8 システムセキュリティの試験

セキュリティ機能（functionality）の試験は，開発期間中に実施することが望ましい。

CSF

検知プロセス（DE.DP）

DE.DP-3

A.14.2.9 システムの受入れ試験

新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立することが望ましい。

* + - * 1. A.14.3 試験データ

試験に用いるデータの保護を確実にするため。

A.14.3.1 試験データの保護

試験データは，注意深く選定し，保護し，管理することが望ましい。

* + 1. ISMSになくCSFにある項目
       1. ID 特定
          1. 資産管理（ID.AM）
          2. ビジネス環境（ID.BE）

ID.BE-2

重要インフラとその産業分野における企業の位置付けを特定し、 伝達している。

ID.BE-3

企業のミッション、 目標、 活動に関して優先順位を定め、 伝達している。

* + - * 1. ガバナンス（ID.GV）

ID.GV-4

ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

* + - * 1. リスクアセスメント（ID.RA）

ID.RA-3

内外からの脅威を特定し、 文書化している。

ID.RA-4

ビジネスに対する潜在的な影響と、 その可能性を特定している。

ID.RA-6

リスクに対する対応を定め、 優先順位付けしている。

* + - * 1. リスク管理戦略（ID.RM）

ID.RM-1

リスク管理プロセスが自組織の利害関係者によって確立、 管理され、 承認されている。

ID.RM-2

自組織のリスク許容度を決定し、 明確にしている。

ID.RM-3

企業によるリスク許容度の決定が、 重要インフラにおける自組織の役割と、 その分野に特化したリスク分析の結果に基づいて行われている。

* + - 1. PR 防御
         1. アクセス制御（PR.AC）
         2. 意識向上およびトレーニング（PR.AT）
         3. データセキュリティ（PR.DS）
         4. 情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-7

保護プロセスを継続的に改善している。

* + - * 1. 保守（PR.MA）
        2. 保護技術（PR.PT）
      1. DE 検知
         1. 異常とイベント（DE.AE）

DE.AE-1

ネットワーク運用のベースラインと、 ユーザとシステム間の予測されるデータの流れを特定し、 管理している。

DE.AE-3

イベントデータを複数の情報源やセンサーから収集し、 相互に関連付けている。

DE.AE-4

イベントがもたらす影響を特定している。

DE.AE-5

インシデント警告の閾値を定めている。

* + - * 1. セキュリティの継続的なモニタリング (DE.CM)

DE.CM-1

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 ネットワークをモニタリングしている。

DE.CM-2

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 物理環境をモニタリングしている。

DE.CM-7

権限のない従業員、 接続、 デバイス、 ソフトウェアのモニタリングを実施している。

* + - * 1. 検知プロセス（DE.DP）
      1. RS 対応
         1. 対応計画（RS.RP）
         2. 伝達（RS.CO）

RS.CO-4

対応計画に従って、 利害関係者との間で調整を行っている。

RS.CO-5

サイバーセキュリティに関する状況認識を深めるために、 外部利害関係者との間で任意の情報共有を行っている。

* + - * 1. 分析 (RS.AN)
        2. 低減（RS.MI）
        3. 改善（RS.IM）

RS.IM-2

対応戦略を更新している。

* + - 1. RC 復旧
         1. 復旧計画（RC.RP）
         2. 改善（RC.IM）

RC.IM-1

学んだ教訓を復旧計画に取り入れている。

RC.IM-2

復旧戦略を更新している。

* + - * 1. 伝達（RC.CO）

RC.CO-1

: 広報活動を管理している

RC.CO-2

イベント発生後に評判を回復している。

RC.CO-3

復旧活動について内部利害関係者と役員、 そして経営陣に伝達している。

* 1. ISMSユーザーズガイド -JIS Q 27001:2014対応【2014年4月14日JIPDEC】

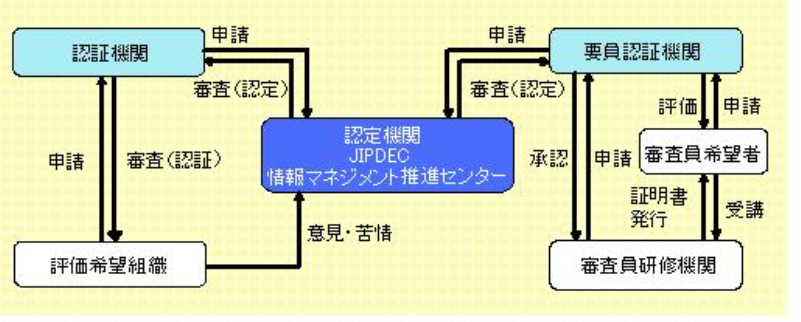
ドキュメントを参照: [JIP-ISMS111-30.html](https://isms.jp/JIP-ISMS111-30.html)

* 1. 情報セキュリティマネジメントシステム(ISMS) 適合性評価制度
     1. ISMS適合性評価制度とは
        1. JIS Q 27001:2014もしくはISO/IEC 27001:2013を認証基準とした情報セキュリティの運用管理に対する第三者評価制度である
     2. 認証審査
        1. 評価機関により、 JIS Q 27001:2014もしくはISO/IEC 27001:2013に基づいて認証審査が行われる
     3. JIPDEC
        1. 適合性評価制度に基づく適合性評価機関（認証機関）を認定する
           1. 適合性評価機関の認定、 不認定、 保留、 取消し又は一時停止等を審議する。
     4. 情報セキュリティ関連の調達時に提示する要件（例）
        1.  情報セキュリティマネジメントシステム(ISMS)適合性評価制度の認証機関により、 ISMS認証を取得した機関（企業、 部署）
           1. 補足：外部委託作業時及び内容に関してのセキュリティ要件ではないが、 作業時に情報セキュリティに対するルールを順守する意識が高いと想定される
     5. 参考資料
        1. 情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要
           1. https://www.isms.jipdec.or.jp/about/index.html

ドキュメントを参照: [index.html](https://www.isms.jipdec.or.jp/about/index.html)

* + - * 1. ISMS適合性評価制度の運用

ISMS適合性評価制度は、 組織が構築したISMSがJIS Q 27001（ISO/IEC 27001）に適合しているか審査し登録する「認証機関」、 審査員の資格を付与する「要員認証機関」、 及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みである。 なお、 審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。

サブトピック  


* + - 1. ISMS認証機関一覧
         1. https://www.isms.jipdec.or.jp/lst/isr/index.html

ドキュメントを参照: [index.html](https://www.isms.jipdec.or.jp/lst/isr/index.html)

* + - 1. ISMS認証取得組織検索
         1. https://www.isms.jipdec.or.jp/lst/ind/index.html

ドキュメントを参照: [index.html](https://www.isms.jipdec.or.jp/lst/ind/index.html)

* + - 1. サブトピック
  1. 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】
     1. 管理的対策
        1. A5.情報セキュリティのための方針群
           1. 情報セキユリティのための経営陣の方向性

情報セキュリティのための方針群

情報セキュリティのための方針群は， これを定義し， 管理層が承認し， 発行し， 従業員及び関連する外部関係者に通知しなければならない

情報セキュリティのための方針群のレビュー

情報セキュリティのための方針群は， あらかじめ定めた間隔で， 又は重大な変化が発生した場合に， それが引き続き適切， 妥当かつ有効であることを確実にするためにレビューしなければならない。

* + - 1. A6.情報セキュリティのための組織
         1. 内部組織

情報セキュリティの役割及び責任

全ての情報セキュリティの責任を定め， 割り当てなければならない

職務の分離

相反する職務及び責任範囲は組織の資産に対する， 認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために， 分離しなければならない。

関係当局との連絡

関係当局との適切な連絡体制を維持しなければならない。

専門組織との連絡

情報セキュリティに関する研究会又は会議、 及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。

プジェクトマネジメントにおける情報セキュリティ

プジェクトの種類にかかわらず， プジェクトマネジメントにおいては， 情報セキュリティに取り組まなければならない。

* + - * 1. モバイル機器及びテレワーキング

モバイル機器の方針

モバイル機器を用いることによって生じるリスクを管理するために、 方針及びその方針を支援するセキュリティ対策を採用しなければならない

テレワーキング

テレワーキングの場所でアクセス， 処理及び保存される情報を保護するために方針及びその方針を支援するセキュリティ対策を実施しなければならない。

* + - 1. A8.資産の管理
         1. 資産に対する責任

資産目録

情報，情報に関連するその他の資産及び情報処理施設を特定しなければならない。 また，これらの資産の目録を，作成し，維持しなければならない。

資産の管理責任

目録の中で維持される資産は，管理されなければならない。

注6.1.2及び6.1.3では，情報セキュリティのリスクを運用管理することについて責任及び権限をもつ人又は主体をリスク所有者としている。 情報セキュリティにおいて，多くの場合，資産の管理責任を負う者はリスク所有者でもある。

資産利用の許容範囲

情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない。

資産の返却

全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない。

* + - * 1. 情報分類

情報の分類

情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない。

情報のラベル付け

情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。

資産の取り扱い

資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない

* + - * 1. 媒体の取扱い

取外し可能な媒体の管理

組織が採用した分類体系に従って、 取外し可能な媒体の管理のための手順を実施しなければならない

媒体の処分

媒体が不要になった場合は、 正式な手順を用いて、 セキュリティを保って処分しなければならない

物理的媒体の輸送

情報を格納した媒体は，輸送の途中における，認可されていないアクセス、 不正使用又は破損から保護しなければならない。

* + - 1. A12.運用のセキュリティ
         1. 運用の手順及び責任

操作手順

変更管理

容量・能力の管理

開発環境、 試験環境及び運用環境の分離

* + - * 1. マルウェアからの保護

マルウェアに対する管理策

* + - * 1. バックアップ

情報のバックアップ

* + - * 1. グ取得及び監視

イベントグ取得

グ情報の保護

実務管理者及び運用担当者の作業グ

クックの同期

* + - * 1. 運用ソフトウエアの管理

運用システムに関わるソフトウェアの導入

* + - * 1. 技術的ぜい弱性管理

技術的脆弱性の管理

ソフトウェアのインストールの制限

* + - * 1. 情報システムの監査に対する考慮事項

情報システムの監査に対する管理

* + - 1. A15.供給者関係
         1. 供給者関係における情報セキュリティ

供給者関係のための情報セキュリティの方針

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。

供給者との合意におけるセキュリティの取扱い

関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセスラ処理，保存若しくは通信を行う，又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない

ICTサプライチェーン

供給者との合意には，情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない

* + - * 1. 供給者のサービス提供の管理

供給者のサービス提供の監視及びレビュー

組織は，供給者のサービス提供を定常的に監視し，レビューし，監査しなければならない。

供給者のサービス提供の変更に対する管理

関連する業務情報業務システム及び業務プセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。 ）を管理しなければならない。

* + - 1. A16.情報セキュリティインシデント管理
         1. 情報セキュリティインシデントの管理及びその改

責任及び手順

情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立しなければならない

情報セキュリティ事象の報告

情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告しなければならない。

情報セキュリティ弱点の報告

組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点はどのようなものでも記録し報告するように要求しなければならない。

情報セキュリティ事象の評価及び決定

情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定しなければならない。

情報セキュリティインシデントへの対応

情報セキュリティインシデントは，文書化した手順に従って対応しなければならない。

情報セキュリティインシデントからの学習

情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。

証拠の収集

組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。

* + - 1. A17.事業継続マネジメントにおける情報セキュリティの側面
         1. 情報セキュリティ継続

情報セキュリティ継続の計画

組織は，困難な状況（ adversesituation) （例えば，危機又は災害）における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。

情報セキュリティ継続の実施

組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない

情報セキュリティ継続の検証、 レビュー及び評価

確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証しなければならない。

* + - * 1. 冗長性

情報処理施設の可用性

情報処理施設は可用性の要求事項を満たすのに十分な冗長性をもって，導入しなければならない

* + - 1. A18.順守
         1. 法的及び契約上の要求事項の順守

適用法令及び契約上の要求事項の特定

知的財産権

記録の保護

プライバシー及び個人を特定できる情報（PII）の保護

暗号化機能に対する規制

* + - * 1. 情報セキュリティのレビュー

情報セキュリティの独立したレビュー

情報セキュリティのための方針群及び標準の順守

技術的順守のレビュー

* + 1. 人的対策
       1. A7.人的資源のセキュリティ
          1. 雇用前

選考

全ての従業員候補者についての経歴などの確認は， 関連する法令， 規制及び、 倫理に従って行わなければならない。 また， この確認は， 事業上の要求事項アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない

雇用条件

従業員及び契約相手との雇用契約書には， 情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。

* + - * 1. 雇用期間中

経営陣の責任

経営陣は， 組織の確立された方針及び手順に従った情報セキュリティの適用を全ての従業員及び契約相手に要求しなければならない

情報セキュリティの意識向上， 教育及び訓練

組織の全ての従業員， 及び関係する場合には契約相手は， 職務に関連する組織の方針及び手順についての， 適切な， 意識向上のための教育及び訓練を受けなければならず， また， 定めに従ってその更新を受けなければならない。

懲戒手続き

情報セキュリティ違反を犯した従業員に対して処置をとるための， 正式かつ周知された懲戒手続を備えなければならない

* + - * 1. 雇用の終了及び変更

雇用の終了又は変更に関する責任

雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定めその従業員又は契約相手に伝達し，かつ，遂行させなければならない。

* + 1. 物理的対策
       1. A11.物理的及び環境的セキュリティ
          1. セキュリティを保つべき領

物理的セキュリティ境界

物理的入退管理策

オフィス， 部屋及び施設のセキュリティ

外部及び環境の脅威からの保護

セキュリティを保つべき領域での作業

受渡場所

* + - * 1. 装置

装置の設置及び保護

サポートユーティリティ（ライフライン事業者）

ケーブル配線のセキュリティ

装置の保守

資産の移動

構外にある装置及び資産のセキュリティ

装置のセキュリティを保った処分又は再利用

無人状態にある利用者装置

クリアデスク・クリアスクリーン方針

* + 1. 技術的対策
       1. A9.アクセス制御
          1. アクセス制御に対する業務上の要求事項

アクセス制御方針

ネットワークおよびネットワークサービスへのアクセス

* + - * 1. 利用者アクセスの管理

利用者登録及び登録削除

利用者アクセスの提供（プビジョニング）

特権的アクセス権の管理

利用者の秘密認証情報の管理

利用者アクセス権のレビュー

アクセス権の削除または修正

* + - * 1. 利用者の責任

秘密認証情報の利用

* + - * 1. システム及びアプリケーションのアクセス制御

情報へのアクセス制限

セキュリティに配慮したグオン手順

パスワード管理システム

特権的なユーティリティプグラムの使用

プグラムソースコードへのアクセス制御

* + - 1. A10.暗号
         1. 暗号による管理策

暗号による管理策の利用方針

鍵管理

* + - 1. A13.通信のセキュリティ
         1. ネットワークセキュリティ管理

ネットワーク管理策

ネットワークサービスのセキュリティ

ネットワークの分離

* + - * 1. 情報の転送

情報転送の方針及び手順

情報転送に関する合意

電子的メッセージ通信

秘密保持契約又は守秘義務契約

* + - 1. A14.システムの取得、 開発及び保守
         1. 情報システムのセキユリティ要求事項

情報セキュリティ要求事項の分析及び仕様化

公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮

アプリケーションサービスのトランザクションの保護

* + - * 1. 開発及びサポートプセスにおけるセキュリティ

セキュリティに配慮した開発のための方針

システムの変更管理手順

オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー

パッケージソフトウェアに対する制限

セキュリティに配慮したシステム構築の原則

セキュリティに配慮したシステム開発環境

外部委託による開発

システムセキュリティの試験

システムの受入れ試験

* + - * 1. 試験データ

試験データの保護

1. NIST CSF　(重要インフラにおけるサイバーセキュリティフレームワーク)
   1. 重要インフラにおけるサイバーセキュリティフレームワーク1.0版（CSF)【2014年2月12日NIST】

ドキュメントを参照: [000038957.pdf](https://www.ipa.go.jp/files/000038957.pdf)

* + 1. フレームワークの概要
       1. フレームワークコア
       2. フレームワークインプレメンテーションティア
       3. フレームワークプロファイル
  1. CSF フレームワークコア
     1. ID 特定
        1. 資産管理（ID.AM）
           1. 組織が事業目的を達成することを可能にするデータ、 職員、 デバイス、 システム、 施設を特定し、 事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。
           2. ID.AM-1

企業内の物理デバイスとシステムの一覧を作成している。

参考情報

CCS CSC 1

COBIT 5 BAI09.01, BAI09.02

ISA 62443-2-1:2009 4.2.3.4

ISA 62443-3-3:2013 SR 7.8

 ISO/IEC 27001:2013 A.8.1.1

 ISO/IEC 27001:2013 A.8.1.2

NIST SP 800-53 Rev. 4 CM-8

* + - * 1. ID.AM-2

企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。

参考情報

CCS CSC 2

COBIT 5 BAI09.01, BAI09.02, BAI09.05

ISA 62443-2-1:2009 4.2.3.4

ISA 62443-3-3:2013 SR 7.8

 ISO/IEC 27001:2013 A.8.1.1

 ISO/IEC 27001:2013 A.8.1.2

NIST SP 800-53 Rev. 4 CM-8

* + - * 1. ID.AM-3

企業内の通信とデータの流れの図を用意している。

参考情報

CCS CSC 1

COBIT 5 DSS05.02

ISA 62443-2-1:2009 4.2.3.4

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9,

PL-8

* + - * 1. ID.AM-4

外部情報システムの一覧を作成している。

参考情報

COBIT 5 APO02.02

 ISO/IEC 27001:2013 A.11.2.6

NIST SP 800-53 Rev. 4 AC-20, SA-9

* + - * 1. ID.AM-5

リソース（例：ハードウェア、 デバイス、 データ、 ソフトウェア）を、 分類、 重要度、 ビジネス上の価値に基づいて優先順位付けしている。

参考情報

COBIT 5 APO03.03, APO03.04, BAI09.02

ISA 62443-2-1:2009 4.2.3.6

 ISO/IEC 27001:2013 A.8.2.1

NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14

* + - * 1. ID.AM-6

すべての従業員と第三者である利害関係者（例：供給業者、 顧客、 パートナー）に対して、 サイバーセキュリティ上の役割と責任を定めている。

参考情報

COBIT 5 APO01.02, DSS06.03

ISA 62443-2-1:2009 4.3.2.3.3

 ISO/IEC 27001:2013 A.6.1.1

NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

* + - 1. ビジネス環境（ID.BE）
         1. 自組織のミッション、 目標、 利害関係者、 活動を理解し、 優先順位付けを行っている; この情報はサイバーセキュリティ上の役割、 責任、 リスク管理上の意思決定を伝達するために使用される。
         2. ID.BE-1

サプライチェーンにおける企業の役割を特定し、 伝達している

参考情報

COBIT 5 APO08.04, APO08.05, APO10.03,

APO10.04, APO10.05

 ISO/IEC 27001:2013 A.15.1.3

 ISO/IEC 27001:2013 A.15.2.1

 ISO/IEC 27001:2013 A.15.2.2

NIST SP 800-53 Rev. 4 CP-2, SA-12

* + - * 1. ID.BE-2

重要インフラとその産業分野における企業の位置付けを特定し、 伝達している。

参考情報

COBIT 5 APO02.06, APO03.01

NIST SP 800-53 Rev. 4 PM-8

* + - * 1. ID.BE-3

企業のミッション、 目標、 活動に関して優先順位を定め、 伝達している。

参考情報

COBIT 5 APO02.01, APO02.06, APO03.01

ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6

NIST SP 800-53 Rev. 4 PM-11, SA-14

* + - * 1. ID.BE-4

重要サービスを提供する上での依存関係と重要な機能を把握している。

参考情報

 ISO/IEC 27001:2013 A.11.2.2

 ISO/IEC 27001:2013 A.11.2.3

 ISO/IEC 27001:2013 A.12.1.3

NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11,PM-8, SA-14

* + - * 1. ID.BE-5

重要サービスの提供を支援する、 レジリエンスに関する要求事項を定めている。

参考情報

COBIT 5 DSS04.02

 ISO/IEC 27001:2013 A.11.1.4

 ISO/IEC 27001:2013 A.17.1.1

 ISO/IEC 27001:2013 A.17.1.2

 ISO/IEC 27001:2013 A.17.2.1

NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

* + - 1. ガバナンス（ID.GV）
         1. 自組織に対する規制、 法律、 リスクと、 自組織の環境、 運用上の要求事項を管理しモニタリングするためのポリシー、 手順、 プロセスを理解しており、 サイバーセキュリティリスクの管理者に伝達している。
         2. ID.GV-1

自組織の情報セキュリティポリシーを定めている。

参考情報

COBIT 5 APO01.03, EDM01.01, EDM01.02

ISA 62443-2-1:2009 4.3.2.6

 ISO/IEC 27001:2013 A.5.1.1

NIST SP 800-53 Rev. 4 -1 controls from all families

* + - * 1. ID.GV-2

情報セキュリティ上の役割と責任について、 内部と外部パートナーとで調整・連携している。

参考情報

COBIT 5 APO13.12

ISA 62443-2-1:2009 4.3.2.3.3

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.1

NIST SP 800-53 Rev. 4 PM-1, PS-7

* + - * 1. ID.GV-3

プライバシーや市民の自由に関する義務を含む、 サイバーセキュリティに関する法規制上の要求事項を理解し、 管理している。

参考情報

COBIT 5 MEA03.01, MEA03.04

ISA 62443-2-1:2009 4.4.3.7

 ISO/IEC 27001:2013 A.18.1

NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)

* + - * 1. ID.GV-4

ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

参考情報

COBIT 5 DSS04.02

ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8,4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3

NIST SP 800-53 Rev. 4 PM-9, PM-11

* + - 1. リスクアセスメント（ID.RA）
         1. 企業は自組織の業務（ミッション、 機能、 イメージ、 評判を含む）、 自組織の資産、 個人に対するサイバーセキュリティリスクを把握している。
         2. ID.RA-1

資産の脆弱性を特定し、 文書化している。

参考情報

CCS CSC 4

COBIT 5 APO12.01, APO12.02, APO12.03,APO12.04

ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9,4.2.3.12

 ISO/IEC 27001:2013 A.12.6.1

 ISO/IEC 27001:2013 A.18.2.3

NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8,RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

* + - * 1. ID.RA-2

情報共有フォーラム／ソースより、 脅威と脆弱性に関する情報を入手している。

参考情報

ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

 ISO/IEC 27001:2013 A.6.1.4

NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5

* + - * 1. ID.RA-3

内外からの脅威を特定し、 文書化している。

参考情報

COBIT 5 APO12.01, APO12.02, APO12.03,APO12.04

ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12,PM-16

* + - * 1. ID.RA-4

ビジネスに対する潜在的な影響と、 その可能性を特定している。

参考情報

COBIT 5 DSS04.02

ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9,PM-11, SA-14

* + - * 1. ID.RA-5

リスクを判断する際に、 脅威、 脆弱性、 可能性、 影響を考慮している。

参考情報

COBIT 5 APO12.02

 ISO/IEC 27001:2013 A.12.6.1

NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

* + - * 1. ID.RA-6

リスクに対する対応を定め、 優先順位付けしている。

参考情報

COBIT 5 APO12.05, APO13.02

NIST SP 800-53 Rev. 4 PM-4, PM-9

* + - 1. リスク管理戦略（ID.RM）
         1. 自組織の優先順位、 制約、 リスク許容度、 想定を定め、 運用リスクの判断に利用している。
         2. ID.RM-1

リスク管理プロセスが自組織の利害関係者によって確立、 管理され、 承認されている。

参考情報

COBIT 5 APO12.04, APO12.05, APO13.02,BAI02.03, BAI04.02

ISA 62443-2-1:2009 4.3.4.2

NIST SP 800-53 Rev. 4 PM-9

* + - * 1. ID.RM-2

自組織のリスク許容度を決定し、 明確にしている。

参考情報

COBIT 5 APO12.06

ISA 62443-2-1:2009 4.3.2.6.5

NIST SP 800-53 Rev. 4 PM-9

* + - * 1. ID.RM-3

企業によるリスク許容度の決定が、 重要インフラにおける自組織の役割と、 その分野に特化したリスク分析の結果に基づいて行われている。

参考情報

NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11,SA-14

* + 1. PR 防御
       1. アクセス制御（PR.AC）
          1. 資産および関連施設へのアクセスを、 承認されたユーザ、 プロセス、 またはデバイスと、 承認された活動およびトランザクションに限定している。
          2. PR.AC-1

承認されたデバイスとユーザの識別情報と認証情報を管理している。

参考情報

CCS CSC 16

COBIT 5 DSS05.04, DSS06.03

ISA 62443-2-1:2009 4.3.3.5.1

ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

 ISO/IEC 27001:2013 A.9.2.1

 ISO/IEC 27001:2013 A.9.2.2

 ISO/IEC 27001:2013 A.9.2.4

 ISO/IEC 27001:2013 A.9.3.1

 ISO/IEC 27001:2013 A.9.4.2

 ISO/IEC 27001:2013 A.9.4.3

NIST SP 800-53 Rev. 4 AC-2, IA Family

* + - * 1. PR.AC-2

資産に対する物理アクセスを管理し、 保護している。

参考情報

COBIT 5 DSS01.04, DSS05.05

ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8

 ISO/IEC 27001:2013 A.11.1.1

 ISO/IEC 27001:2013 A.11.1.2

 ISO/IEC 27001:2013 A.11.1.4

 ISO/IEC 27001:2013 A.11.1.6

 ISO/IEC 27001:2013 A.11.2.3

NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9

* + - * 1. PR.AC-3

リモートアクセスを管理している。

参考情報

COBIT 5 APO13.01, DSS01.04, DSS05.03

ISA 62443-2-1:2009 4.3.3.6.6

ISA 62443-3-3:2013 SR 1.13, SR 2.6

 ISO/IEC 27001:2013 A.6.2.2

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20

* + - * 1. PR.AC-4

最小権限および職務の分離の原則を取り入れて、 アクセス権限を管理している。

参考情報

CCS CSC 12, 15

ISA 62443-2-1:2009 4.3.3.7.3

ISA 62443-3-3:2013 SR 2.1

 ISO/IEC 27001:2013 A.6.1.2

 ISO/IEC 27001:2013 A.9.1.2

 ISO/IEC 27001:2013 A.9.2.3

 ISO/IEC 27001:2013 A.9.4.1

 ISO/IEC 27001:2013 A.9.4.4

NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16

* + - * 1. PR.AC-5

適宜、 ネットワークの分離を行って、 ネットワークの完全性を保護している。

参考情報

ISA 62443-2-1:2009 4.3.3.4

ISA 62443-3-3:2013 SR 3.1, SR 3.8

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.1.3

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-4, SC-7

* + - 1. 意識向上およびトレーニング（PR.AT）
         1. 自組織の職員およびパートナーに対して、 関連するポリシー、 手順、 契約に基づいた、 情報セキュリティに関連する義務と責任を果たせるようにするために、 サイバーセキュリティ意識向上教育と、 十分なトレーニングを実施している。
         2. PR.AT-1

すべてのユーザに情報を周知し、 トレーニングを実施している。

参考情報

CCS CSC 9

COBIT 5 APO07.03, BAI05.07

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-2, PM-13

* + - * 1. PR.AT-2

権限を持つユーザが役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.02, DSS06.03

ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-3, PM-13

* + - * 1. PR.AT-3

第三者である利害関係者（例：供給業者、 顧客、 パートナー）が役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.03, APO10.04, APO10.05

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 PS-7, SA-9

* + - * 1. PR.AT-4

上級役員が役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.03

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-3, PM-13

* + - * 1. PR.AT-5

物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.03

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-3, PM-13

* + - 1. データセキュリティ（PR.DS）
         1. 情報と記録（データ）を情報の機密性、 完全性、 可用性を保護するために定められた自組織のリスク戦略に従って管理している。
         2. PR.DS-1

保存されているデータを保護している。

参考情報

CCS CSC 17

COBIT 5 APO01.06, BAI02.01, BAI06.01,

DSS06.06

ISA 62443-3-3:2013 SR 3.4, SR 4.1

 ISO/IEC 27001:2013 A.8.2.3

NIST SP 800-53 Rev. 4 SC-28

* + - * 1. PR.DS-2

伝送中のデータを保護している。

参考情報

CCS CSC 17

COBIT 5 APO01.06, DSS06.06

ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.2.1

 ISO/IEC 27001:2013 A.13.2.3

 ISO/IEC 27001:2013 A.14.1.2

 ISO/IEC 27001:2013 A.14.1.3

NIST SP 800-53 Rev. 4 SC-8

* + - * 1. PR.DS-3

資産について撤去、 譲渡、 廃棄プロセスを正式に管理している。

参考情報

COBIT 5 BAI09.03

ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1

ISA 62443-3-3:2013 SR 4.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.8.3.1

 ISO/IEC 27001:2013 A.8.3.2

 ISO/IEC 27001:2013 A.8.3.3

 ISO/IEC 27001:2013 A.11.2.7

NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16

* + - * 1. PR.DS-4

可用性を確保するのに十分な容量を保持している。

参考情報

COBIT 5 APO13.01

ISA 62443-3-3:2013 SR 7.1, SR 7.2

 ISO/IEC 27001:2013 A.12.3.1

NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

* + - * 1. PR.DS-5

データ漏えいに対する保護対策を実施している。

参考情報

CCS CSC 17

COBIT 5 APO01.06

ISA 62443-3-3:2013 SR 5.2

 ISO/IEC 27001:2013 A.6.1.2

 ISO/IEC 27001:2013 A.7.1.1

 ISO/IEC 27001:2013 A.7.1.2

 ISO/IEC 27001:2013 A.7.3.1

 ISO/IEC 27001:2013 A.8.2.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.9.1.1

 ISO/IEC 27001:2013 A.9.1.2

 ISO/IEC 27001:2013 A.9.2.3

 ISO/IEC 27001:2013 A.9.4.1

 ISO/IEC 27001:2013 A.9.4.4

 ISO/IEC 27001:2013 A.9.4.5

 ISO/IEC 27001:2013 A.13.1.3

 ISO/IEC 27001:2013 A.13.2.1

 ISO/IEC 27001:2013 A.13.2.3

 ISO/IEC 27001:2013 A.13.2.4

 ISO/IEC 27001:2013 A.14.1.2

 ISO/IEC 27001:2013 A.14.1.3

NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

* + - * 1. PR.DS-6

ソフトウェア、 ファームウェア、 および情報の完全性の検証に、 完全性チェックメカニズムを使用している。

参考情報

ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4,SR 3.8

 ISO/IEC 27001:2013 A.12.2.1

 ISO/IEC 27001:2013 A.12.5.1

 ISO/IEC 27001:2013 A.14.1.2

 ISO/IEC 27001:2013 A.14.1.3

NIST SP 800-53 Rev. 4 SI-7

* + - * 1. PR.DS-7

開発・テスト環境を実稼働環境から分離している。

参考情報

COBIT 5 BAI07.04

 ISO/IEC 27001:2013 A.12.1.4

NIST SP 800-53 Rev. 4 CM-2

* + - 1. 情報を保護するためのプロセスおよび手順（PR.IP）
         1. （目的、 範囲、 役割、 責任、 経営コミットメント、 組織間の調整を扱う）セキュリティポリシー、 プロセス、 手順を維持し、 情報システムと資産の保護の管理に使用している。
         2. PR.IP-1

情報技術／産業用制御システムのベースラインとなる設定を定め、 維持している。

参考情報

CCS CSC 3, 10

COBIT 5 BAI10.01, BAI10.02, BAI10.03,BAI10.05

ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3

ISA 62443-3-3:2013 SR 7.6

 ISO/IEC 27001:2013 A.12.1.2

 ISO/IEC 27001:2013 A.12.5.1,

 ISO/IEC 27001:2013 A.12.6.2

 ISO/IEC 27001:2013 A.14.2.2

 ISO/IEC 27001:2013 A.14.2.3

 ISO/IEC 27001:2013 A.14.2.4

NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

* + - * 1. PR.IP-2

システムを管理するためのシステム開発ライフサイクルを導入している。

参考情報

COBIT 5 APO13.01

ISA 62443-2-1:2009 4.3.4.3.3

 ISO/IEC 27001:2013 A.6.1.5

 ISO/IEC 27001:2013 A.14.1.1

 ISO/IEC 27001:2013 A.14.2.1

 ISO/IEC 27001:2013 A.14.2.5

NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8

* + - * 1. PR.IP-3

設定変更管理プロセスを導入している。

参考情報

COBIT 5 BAI06.01, BAI01.06

ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3

ISA 62443-3-3:2013 SR 7.6

 ISO/IEC 27001:2013 A.12.1.2

 ISO/IEC 27001:2013 A.12.5.1

 ISO/IEC 27001:2013 A.12.6.2

 ISO/IEC 27001:2013 A.14.2.2

 ISO/IEC 27001:2013 A.14.2.3

 ISO/IEC 27001:2013 A.14.2.4

NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

* + - * 1. PR.IP-4

情報のバックアップを定期的に実施、 保持し、 テストしている。

参考情報

COBIT 5 APO13.01

ISA 62443-2-1:2009 4.3.4.3.9

ISA 62443-3-3:2013 SR 7.3, SR 7.4

 ISO/IEC 27001:2013 A.12.3.1

 ISO/IEC 27001:2013 A.17.1.2

 ISO/IEC 27001:2013 A.17.1.3

 ISO/IEC 27001:2013 A.18.1.3

NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

* + - * 1. PR.IP-5

自組織の資産の物理的な運用環境に関するポリシーと規制を満たしている。

参考情報

COBIT 5 DSS01.04, DSS05.05

ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6

 ISO/IEC 27001:2013 A.11.1.4

 ISO/IEC 27001:2013 A.11.2.1

 ISO/IEC 27001:2013 A.11.2.2

 ISO/IEC 27001:2013 A.11.2.3

NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18

* + - * 1. PR.IP-6

ポリシーに従ってデータを破壊している。

参考情報

COBIT 5 BAI09.03

ISA 62443-2-1:2009 4.3.4.4.4

ISA 62443-3-3:2013 SR 4.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.8.3.1

 ISO/IEC 27001:2013 A.8.3.2

 ISO/IEC 27001:2013 A.11.2.7

NIST SP 800-53 Rev. 4 MP-6

* + - * 1. PR.IP-7

保護プロセスを継続的に改善している。

参考情報

COBIT 5 APO11.06, DSS04.05

ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8

NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

* + - * 1. PR.IP-8

保護技術の有効性について、 適切なパートナーとの間で情報を共有している。

参考情報

ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4

* + - * 1. PR.IP-9

対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、 管理している。

参考情報

COBIT 5 DSS04.03

ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1

 ISO/IEC 27001:2013 A.16.1.1

 ISO/IEC 27001:2013 A.17.1.1

 ISO/IEC 27001:2013 A.17.1.2

NIST SP 800-53 Rev. 4 CP-2, IR-8

* + - * 1. PR.IP-10

対応計画と復旧計画をテストしている。

参考情報

ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11

ISA 62443-3-3:2013 SR 3.3

 ISO/IEC 27001:2013 A.17.1.3

NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14

* + - * 1. PR.IP-11

人事に関わる対策にサイバーセキュリティ（例：アクセス権限の無効化、 従業員に対する審査）を含めている。

参考情報

COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05

ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2,　4.3.3.2.3

 ISO/IEC 27001:2013 A.7.1.1

 ISO/IEC 27001:2013 A.7.3.1

 ISO/IEC 27001:2013 A.8.1.4

NIST SP 800-53 Rev. 4 PS Family

* + - * 1. PR.IP-12

脆弱性管理計画を作成し、 実施している。

参考情報

 ISO/IEC 27001:2013 A.12.6.1

 ISO/IEC 27001:2013 A.18.2.2

NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

* + - 1. 保守（PR.MA）
         1. 産業用制御システムと情報システムのコンポーネントの保守と修理をポリシーと手順に従って実施している。
         2. PR.MA-1

自組織の資産の保守と修理は、 承認・管理されたツールを用いて、 タイムリーに実施し、 ログを記録している。

参考情報

COBIT 5 BAI09.03

ISA 62443-2-1:2009 4.3.3.3.7

 ISO/IEC 27001:2013 A.11.1.2

 ISO/IEC 27001:2013 A.11.2.4

 ISO/IEC 27001:2013 A.11.2.5

NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5

* + - * 1. PR.MA-2

自組織の資産に対する遠隔保守は、 承認を得て、 ログを記録し、 不正アクセスを防げる形で実施している。

参考情報

COBIT 5 DSS05.04

ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8

 ISO/IEC 27001:2013 A.11.2.4

 ISO/IEC 27001:2013 A.15.1.1

 ISO/IEC 27001:2013 A.15.2.1

NIST SP 800-53 Rev. 4 MA-4

* + - 1. 保護技術（PR.PT）
         1. 関連するポリシー、 手順、 契約に基づいて、 システムと資産のセキュリティと耐性・復旧力を確保するための、 技術的なセキュリティソリューションを管理している。
         2. PR.PT-1

ポリシーに従って監査記録／ログ記録の対象を決定、 文書化し、 そうした記録を実施して、 レビューしている。

参考情報

CCS CSC 14

COBIT 5 APO11.04

ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4

ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12

 ISO/IEC 27001:2013 A.12.4.1

 ISO/IEC 27001:2013 A.12.4.2

 ISO/IEC 27001:2013 A.12.4.3

 ISO/IEC 27001:2013 A.12.4.4

 ISO/IEC 27001:2013 A.12.7.1

NIST SP 800-53 Rev. 4 AU Family

* + - * 1. PR.PT-2

ポリシーに従って取り外し可能な外部記録媒体を保護し、 そうした媒体の使用を制限している。

参考情報

COBIT 5 DSS05.02, APO13.01

ISA 62443-3-3:2013 SR 2.3

 ISO/IEC 27001:2013 A.8.2.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.8.3.1

 ISO/IEC 27001:2013 A.8.3.3

 ISO/IEC 27001:2013 A.11.2.9

NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7

* + - * 1. PR.PT-3

最小機能の原則を取り入れて、 システムと資産に対するアクセスを制御している。

参考情報

COBIT 5 DSS05.02

ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1,　4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4

ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7

 ISO/IEC 27001:2013 A.9.1.2

NIST SP 800-53 Rev. 4 AC-3, CM-7

* + - * 1. PR.PT-4

通信ネットワークと制御ネットワークを保護している。

参考情報

CCS CSC 7

COBIT 5 DSS05.02, APO13.01

ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7

* + 1. DE 検知
       1. 異常とイベント（DE.AE）
          1. 異常な活動をタイムリーに検知し、 イベントがもたらす可能性のある影響を把握している。
          2. DE.AE-1

ネットワーク運用のベースラインと、 ユーザとシステム間の予測されるデータの流れを特定し、 管理している。

参考情報

COBIT 5 DSS03.01

ISA 62443-2-1:2009 4.4.3.3

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2,　SI-4

* + - * 1. DE.AE-2

攻撃の標的と手法を理解するために、 検知したイベントを分析している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8

ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2

 ISO/IEC 27001:2013 A.16.1.1

 ISO/IEC 27001:2013 A.16.1.4

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4

* + - * 1. DE.AE-3

イベントデータを複数の情報源やセンサーから収集し、 相互に関連付けている。

参考情報

ISA 62443-3-3:2013 SR 6.1

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

* + - * 1. DE.AE-4

イベントがもたらす影響を特定している。

参考情報

COBIT 5 APO12.06

NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4

* + - * 1. DE.AE-5

インシデント警告の閾値を定めている。

参考情報

COBIT 5 APO12.06

ISA 62443-2-1:2009 4.2.3.10

NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

* + - 1. セキュリティの継続的なモニタリング (DE.CM)
         1. サイバーセキュリティイベントを検知し、 保護対策の有効性を検証するために、 情報システムと資産を離散間隔でモニタリングしている。
         2. DE.CM-1

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 ネットワークをモニタリングしている。

参考情報

CCS CSC 14, 16

COBIT 5 DSS05.07

ISA 62443-3-3:2013 SR 6.2

NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7,CM-3, SC-5, SC-7, SI-4

* + - * 1. DE.CM-2

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 物理環境をモニタリングしている。

参考情報

ISA 62443-2-1:2009 4.3.3.3.8

NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20

* + - * 1. DE.CM-3

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 個人の活動をモニタリングしている。

参考情報

ISA 62443-3-3:2013 SR 6.2

 ISO/IEC 27001:2013 A.12.4.1

NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13,CA-7, CM-10, CM-11

* + - * 1. DE.CM-4

悪質なコードを検出できる。

参考情報

CCS CSC 5

COBIT 5 DSS05.01

ISA 62443-2-1:2009 4.3.4.3.8

ISA 62443-3-3:2013 SR 3.2

 ISO/IEC 27001:2013 A.12.2.1

NIST SP 800-53 Rev. 4 SI-3

* + - * 1. DE.CM-5

悪質なモバイルコードを検出できる。

参考情報

ISA 62443-3-3:2013 SR 2.4

 ISO/IEC 27001:2013 A.12.5.1

NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44

* + - * 1. DE.CM-6

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 外部サービスプロバイダの活動をモニタリングしている。

参考情報

COBIT 5 APO07.06

 ISO/IEC 27001:2013 A.14.2.7

 ISO/IEC 27001:2013 A.15.2.1

NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4

* + - * 1. DE.CM-7

権限のない従業員、 接続、 デバイス、 ソフトウェアのモニタリングを実施している。

参考情報

NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,　CM-8, PE-3, PE-6, PE-20, SI-4

* + - * 1. DE.CM-8

脆弱性スキャンを実施している。

参考情報

COBIT 5 BAI03.10

ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7

 ISO/IEC 27001:2013 A.12.6.1

NIST SP 800-53 Rev. 4 RA-5

* + - 1. 検知プロセス（DE.DP）
         1. 異常なイベントをタイムリーに、 かつ正確に検知するための検知プロセスおよび手順を維持し、 テストしている。
         2. DE.DP-1

説明責任を果たせるよう、 検知に関する役割と責任を明確に定義している。

参考情報

CCS CSC 5

COBIT 5 DSS05.01

ISA 62443-2-1:2009 4.4.3.1

 ISO/IEC 27001:2013 A.6.1.1

NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

* + - * 1. DE.DP-2

検知活動は必要なすべての要求事項を満たしている。

参考情報

ISA 62443-2-1:2009 4.4.3.2

 ISO/IEC 27001:2013 A.18.1.4

NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4

* + - * 1. DE.DP-3

検知プロセスをテストしている。

参考情報

COBIT 5 APO13.02

ISA 62443-2-1:2009 4.4.3.2

ISA 62443-3-3:2013 SR 3.3

 ISO/IEC 27001:2013 A.14.2.8

NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3,　PM-14, SI-3, SI-4

* + - * 1. DE.DP-4

イベント検知情報を適切な関係者に伝達している。

参考情報

COBIT 5 APO12.06

ISA 62443-2-1:2009 4.3.4.5.9

ISA 62443-3-3:2013 SR 6.1

 ISO/IEC 27001:2013 A.16.1.2

NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7,　RA-5, SI-4

* + - * 1. DE.DP-5

検知プロセスを継続的に改善している。

参考情報

COBIT 5 APO11.06, DSS04.05

ISA 62443-2-1:2009 4.4.3.4

 ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2,　RA-5, SI-4, PM-14

* + 1. RS 対応
       1. 対応計画（RS.RP）
          1. 検知したサイバーセキュリティイベントにタイムリーに対応できるよう、 対応プロセスおよび手順を実施し、 維持している。
          2. RS.RP-1

イベントの発生中または発生後に対応計画を実施している。

参考情報

COBIT 5 BAI01.10

CCS CSC 18

ISA 62443-2-1:2009 4.3.4.5.1

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8

* + - 1. 伝達（RS.CO）
         1. 法執行機関からの支援を必要に応じて得られるよう、 内外の利害関係者との間で対応活動を調整している。
         2. RS.CO-1

対応が必要になった時の自身の役割と行動の順番を従業員は認識している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.16.1.1

NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8

* + - * 1. RS.CO-2

定められた基準に沿って、 イベントを報告している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.5

 ISO/IEC 27001:2013 A.6.1.3

 ISO/IEC 27001:2013 A.16.1.2

NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8

* + - * 1. RS.CO-3

対応計画に従って情報を共有している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.2

 ISO/IEC 27001:2013 A.16.1.2

NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4

* + - * 1. RS.CO-4

対応計画に従って、 利害関係者との間で調整を行っている。

参考情報

ISA 62443-2-1:2009 4.3.4.5.5

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + - * 1. RS.CO-5

サイバーセキュリティに関する状況認識を深めるために、 外部利害関係者との間で任意の情報共有を行っている。

参考情報

NIST SP 800-53 Rev. 4 PM-15, SI-5

* + - 1. 分析 (RS.AN)
         1. 適切な対応を確実にし、 復旧活動を支援するために、 分析を実施している。
         2. RS.AN-1

検知システムからの通知を調査している。

参考情報

COBIT 5 DSS02.07

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7,

4.3.4.5.8

ISA 62443-3-3:2013 SR 6.1

 ISO/IEC 27001:2013 A.12.4.1

 ISO/IEC 27001:2013 A.12.4.3

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

* + - * 1. RS.AN-2

インシデントがもたらす影響を把握している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8

 ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4 CP-2, IR-4

* + - * 1. RS.AN-3

フォレンジクスを実施している。

参考情報

ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1

 ISO/IEC 27001:2013 A.16.1.7

NIST SP 800-53 Rev. 4 AU-7, IR-4

* + - * 1. RS.AN-4

対応計画に従ってインシデントを分類している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6

 ISO/IEC 27001:2013 A.16.1.4

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8

* + - 1. 低減（RS.MI）
         1. イベントの拡大を防ぎ、 その影響を緩和し、 インシデントを根絶するための活動を実施している。
         2. RS.MI-1

インシデントを封じ込めている。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6

ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 IR-4

* + - * 1. RS.MI-2

インシデントを低減している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10

 ISO/IEC 27001:2013 A.12.2.1

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 IR-4

* + - * 1. RS.MI-3

新たに特定された脆弱性に関して、 許容できるリスクである場合にはその旨を文書化し、 そうでない場合には低減している。

参考情報

 ISO/IEC 27001:2013 A.12.6.1

NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5

* + - 1. 改善（RS.IM）
         1. 現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、 自組織の対応活動を改善している。
         2. RS.IM-1

学んだ教訓を対応計画に取り入れている。

参考情報

COBIT 5 BAI01.13

ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4

 ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + - * 1. RS.IM-2

対応戦略を更新している。

参考情報

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + 1. RC 復旧
       1. 復旧計画（RC.RP）
          1. サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリーに復旧できるよう、 復旧プロセスおよび手順を実施し、 維持している。
          2. RC.RP-1

イベントの発生中または発生後に復旧計画を実施している。

参考情報

CCS CSC 8

COBIT 5 DSS02.05, DSS03.04

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8

* + - 1. 改善（RC.IM）
         1. 学んだ教訓を将来的な活動に取り入れることで、 復旧計画およびプロセスを改善している。
         2. RC.IM-1

学んだ教訓を復旧計画に取り入れている。

参考情報

COBIT 5 BAI05.07

ISA 62443-2-1:2009 4.4.3.4

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + - * 1. RC.IM-2

復旧戦略を更新している。

参考情報

COBIT 5 BAI07.08

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + - 1. 伝達（RC.CO）
         1. コーディネーティングセンター、 インターネットサービスプロバイダ、 攻撃システムのオーナー、 被害者、 その他のCSIRT、 ベンダなどの、 内外の関係者との間で復旧活動を調整している。
         2. RC.CO-1

広報活動を管理している。

参考情報

COBIT 5 EDM03.02

* + - * 1. RC.CO-2

イベント発生後に評判を回復している。

参考情報

COBIT 5 MEA03.02

* + - * 1. RC.CO-3

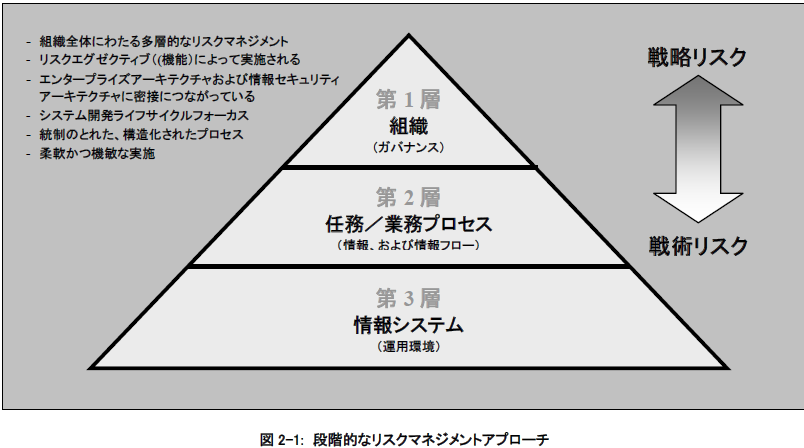
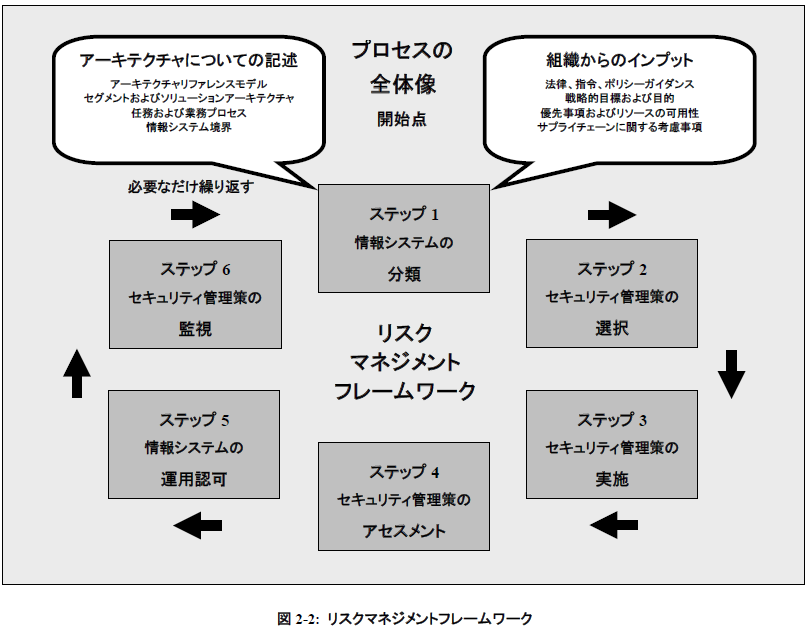
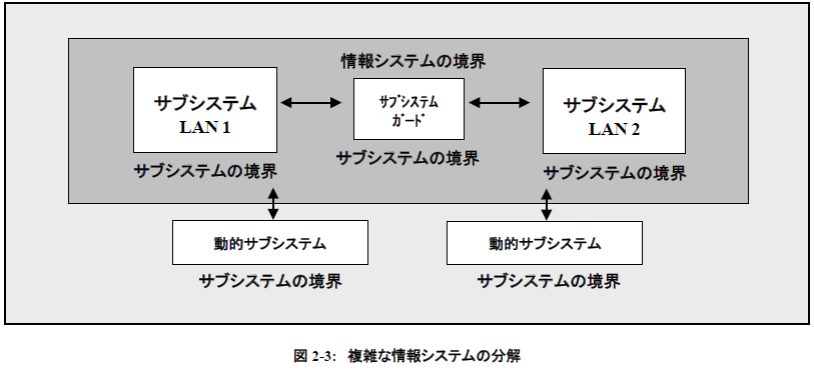
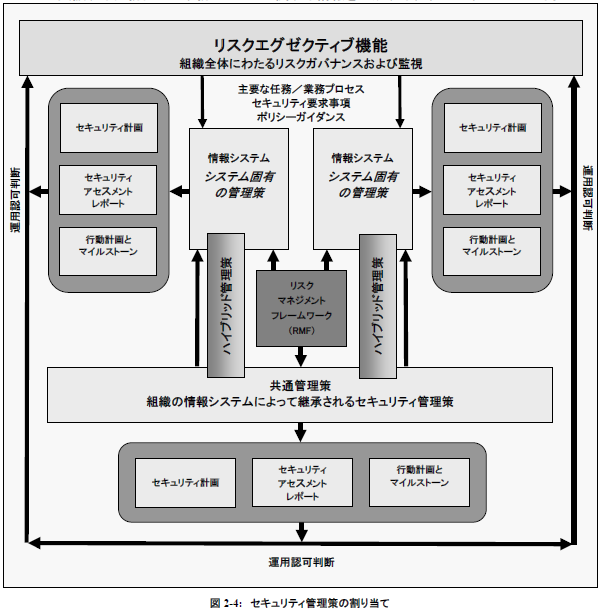
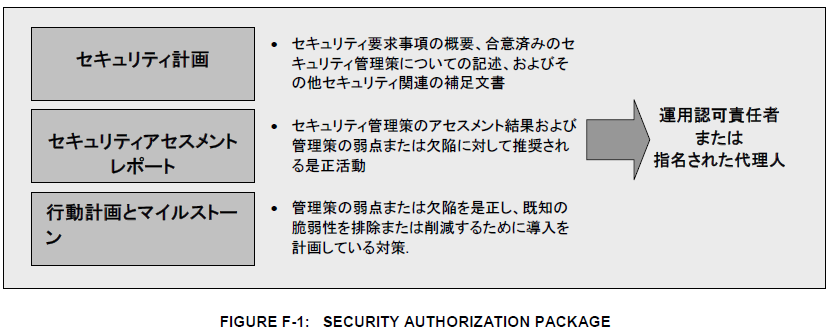
復旧活動について内部利害関係者と役員、 そして経営陣に伝達している。

参考情報

NIST SP 800-53 Rev. 4 CP-2, IR-4

1. NIST SP 800-37 (連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド： セキュリティライフサイクルによるアプローチ)
   1. 連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド： セキュリティライフサイクルによるアプローチ

ドキュメントを参照: [000025329.pdf](https://www.ipa.go.jp/files/000025329.pdf)

* 1. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  2. 第1章 はじめに
     1. 情報セキュリティの必要性とリスクを管理する必要性
        1. 公共および民間部門の情報システムに対する攻撃（複数）が成功した場合、 米国の国家安全上の利益および経済安全上の利益に深刻な、 または重大な被害が及ぶ可能性がある。 これらの脅威の危険性が重大であり、 かつ増大していることから、 組織内のあらゆる階層のリーダーが、 適切な情報セキュリティの確保、 および情報システム関連のセキュリティリスク8の管理における自身の責務を理解することが必要不可欠になる。
     2. 1.1 背景
        1. RMF（Risk Management Framework：リスクマネジメントフレームワーク）
           1. 堅牢で継続的監視プロセスの実施により、 リアルタイムに近いリスクマネジメントおよび情報システムの継続的な運用認可の概念を促進する。
           2. 主要な任務および業務上の機能をサポートする情報システムに関して、 費用対効果の高い、 リスクベースの意思決定を行うのに必要な情報をシニアリーダー提供するための、 オートメーション（automation）の利用を促進する。
           3. エンタープライズアーキテクチャおよびシステム開発ライフサイクルに情報セキュリティを組み入れる。
           4. セキュリティ管理策の選択、 実施、 アセスメント、 および監視、 ならびに情報システムの運用認可に重点を置く。
           5. リスクエグゼクティブ（機能）を通じて、 情報システムレベルのリスクマネジメントプロセスを、 組織レベルのリスクマネジメントプロセスにリンクする
           6. 組織の情報システムに導入され、 それらのシステムによって継承されるセキュリティ管理策（すなわち、 共通管理策）に対する責任と説明責任を定める。
     3. 1.2 目的および適用性
        1. 情報システム関連のセキュリティリスクの管理を、 組織の任務／業務上の目的、 およびリスクエグゼクティブ（機能）を通じてシニアリーダーが定めた全般的なリスク戦略に確実に適合させる。
        2. 必要なセキュリティ管理策を含む情報セキュリティ要求事項を、 組織のエンタープライズアーキテクチャおよびシステム開発ライフサイクルに確実に組み入れる。
        3. （継続的な監視を通じて）一貫性のある、 十分な情報に基づいた、 継続的なセキュリティ運用認可判断を支援すると同時に、 セキュリティおよびリスクマネジメント関連の情報の透明性、 ならびに互恵契約（reciprocity）11を支援する。
        4. 適切なリスク軽減戦略の実施により、 連邦政府内の情報および情報システムのセキュリティを向上させる。
        5. 本ガイドラインは、 国家安全保障にかかわるシステムに対する同様のガイドラインについても補足を行えるように、 技術的な観点から広範囲にわたって作成されたものであり、 そのようなシステムに対する政策権限を行使する適切な連邦政府職員による承認があれば、 そのようなシステムに適用することができる。
        6. 州政府、 地方政府、 および隊組織はもとより、 民間部門の組織においても、 必要に応じて本ガイドラインの使用を検討することが推奨される。
     4. 1.3 対象となる読者
        1. 任務／業務上のオーナーシップに責任を持つ者、 または、 受託者責任を持つ者（例：連邦政府機関の長、 最高経営責任者、 最高財務責任者）
        2. 情報システムの開発および統合に責任を持つ者（例：プログラムマネージャ、 IT製品の開発者、 情報システムの開発者、 情報システムのインテグレータ、 エンタープライズアーキテクト、 情報セキュリティアーキテクト）
        3. 情報システムおよび／またはセキュリティの管理／監督に責任を持つ者（例：シニアリーダー、 リスクエグゼクティブ、 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
        4. 情報システムおよびセキュリティ管理策のアセスメントおよび監視に責任を持つ者（例：システム評価者、 アセサー／アセスメントチーム、 検証および有効性確認を行う第三者アセサー、 監査官、 または情報システムのオーナー）
        5. 情報セキュリティの導入および運用に責任を持つ者（例：情報システムのオーナー、 共通管理策のプロバイダ、 情報のオーナー／スチュワード、 任務／業務のオーナー、 情報セキュリティアーキテクト、 情報システムセキュリティエンジニア／責任者）。
     5. 1.4 本文書の構成
        1. 第2章では、
           1. 情報システム関連のセキュリティリスクの管理に関連する基本概念を説明する。 内容には次のようなものが含まれる。 (i) リスクマネジメントに対する組織全体としての見解、 およびリスクマネジメントフレームワークの適用(ii) システム開発ライフサイクルへの情報セキュリティ要求事項の組み入れ(iii) 情報システム境界の確立、 および(iv) システム固有の管理策、 ハイブリッド管理策、 または共通管理策として分類されたセキュリティ管理策の、 情報システムへの割り当て。
        2. 第3章では、
           1. リスクマネジメントフレームワークを情報システムに適用するのに必要なタスクについて記述する。 内容には次のようなものが含まれる。 (i) 情報および情報システムの分類(ii) セキュリティ管理策の選択(iii) セキュリティ管理策の導入(iv) セキュリティ管理策の有効性のアセスメント(v) 情報システムの運用認可、 および(vi) 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状態の継続的な監視。
        3. （補足）付録 では、
           1. リスクマネジメントフレームワークの情報システムへの適用に関する追加情報を提供する。 内容には次のようなものが含まれる。
           2. (i) 参考文献(ii) 用語集(iii) 略語(iv) 役割と責任(v) RMFタスクの要約(vi) 情報システムのセキュリティ運用認可(vii) 情報システムのセキュリティ状態の監視(viii) 運用上のシナリオ(ix) 外部環境におけるセキュリティ管理策。
  3. 第2章 基本項目
     1. 2.1 統合された組織全体にわたるマネジメント
        1. サブトピック  
           
        2. サブトピック  
           
     2. 2.2 システム開発ライフサイクル
     3. 2.3 情報システム境界
        1. 2.3.1 情報システムの境界の設定
        2. 2.3.2 複雑な情報システムの境界
           1. サブトピック  
              
        3. 2.3.3 技術の変化および情報システム境界への影響
     4. 2.4 セキュリティ管理策の割り当て
        1. サブトピック  
           
  4. 第3章 プロセス
     1. リスクマネジメントフレームワークの適用
        1. リスクマネジメントフレームワークおよび関連するRMFタスクは、 情報システムのオーナーと共通管理策の提供者の両方に適用される。 情報システムの運用認可を支援するのに加えて、 RMFタスクは、 組織の情報システムが継承する共通管理策の選択、 開発、 実施、 アセスメント、 運用認可、 および継続的な監視を支援する。 共通管理策の提供者（組織にとって内部・外部の両方）によるRMFタスクの実施により、 共通管理策によって提供されるセキュリティ機能が、 情報の保護に関する彼らのニーズに適した保証レベルで、 情報システムオーナーによって継承される。 このアプローチでは、 情報システムおよび、 それらのシステムを支援するインフラに導入されるセキュリティ管理策の有効性の重要性を認識している。
        2. RMFの各タスクは、 シーケンシャルに記述されているが、 組織は、 組織が確立したマネジメントおよびシステム開発ライフサイクルプロセスに適合させるために、 あるいは、 タスクの実施に関して、 より費用対効果が高く効率的なソリューションを実現するために、 シーケンシャルな構造からの逸脱を選択してもよい。 タスクの順序付けがどうなっているかにかかわらず、 情報システムの運用を開始する前に実施すべき最後のステップは、 運用認可責任者がリスクを明示的に受容することである。 組織は、 RMFの特定のタスクを反復する形で実施したり、 システム開発ライフサイクルの異なるフェーズにおいて実施することもできる。 たとえば、 セキュリティ管理策アセスメントは、 システム開発時、 システム導入時、 およびシステム運用／保守時（継続的な監視の一環として）に実施される可能性がある。
        3. 組織は、 組織内の選択されたプロセスおよび活動の熟成度に基づいて、 RMFの特定のタスクに対しては、 大きな労力をかけて、 残りのタスクに対しては、 より少ないリソースを割り当ててもよい。 RMFは、 ライフサイクルをベースしているため、 情報システムやその運用環境に対する変更を組織がどのように管理するかによっては、 時間の経過とともに多くのタスクを再訪する必要性が生じる。 情報システムに対する情報セキュリティ関連リスクの管理は、 シニアリーダーが実施する、 組織全体にわたる大規模のリスクマネジメント活動の一部とみなされている。 RMFによって、 情報システムの運用および使用により生じるリスクを軽減するための統制のとれた構造化されたアプローチと、 極めて動的な運用環境において組織の主要な任務および業務を支援するのに必要な柔軟性と機敏さとの、 両方が同時に提供されなければならない。
     2. 3.1 RMFステップ1-情報システムの分類
        1. タスク1-1 セキュリティ分類
           1. 情報システムを分類し、 セキュリティ分類の結果をセキュリティ計画に記載する。
        2. タスク1-2 情報システムに関する記述
           1. 情報システム（システム境界を含む）について説明し、 その内容をセキュリティ計画に記載する。
        3. タスク1-3 情報システムの登録
           1. 組織内の適切な計画局／管理局に情報システムを登録する。
     3. 3.2 RMF ステップ 2-セキュリティ管理策の選択
        1. タスク2-1 共通管理策の明確化
           1. 組織の情報システムに対する共通管理策として組織が提供しているセキュリティ管理策を明確にし、 セキュリティ計画（またはそれと同等の文書）に記載する。
        2. タスク2-2 セキュリティ管理策の選択
           1. 情報システムに導入するセキュリティ管理策を選択し、 それらの管理策について、 セキュリティ計画に記載する。
        3. タスク2-3 監視戦略
           1. セキュリティ管理策の有効性、 ならびに、 情報システムおよびシステムの運用環境に対して提案されている、 あるいは、 実際に実施された変更を、 継続的に監視するための、 戦略を策定する。
        4. タスク2-4 セキュリティ計画の承認
           1. セキュリティ計画をレビューし、 承認する。
     4. 3.3 RMF ステップ 3-セキュリティ管理策の実施
        1. タスク3-1 セキュリティ管理策の実施
           1. セキュリティ計画に記載されているセキュリティ管理策を実施する。
        2. タスク3-2 セキュリティ管理策の文書化
           1. 必要に応じて、 セキュリティ管理策の実施について、 機能面での記述（予定しているインプット、 予想される挙動、 および予想されるアウトプットを含む）と併せて、 セキュリティ計画に記載する。
     5. 3.4 RMF ステップ 4-セキュリティ管理策のアセスメント
        1. タスク4-1 アセスメントの準備
           1. セキュリティ管理策のアセスメント計画を策定、 レビューし、 承認する。
        2. タスク4-2 セキュリティ管理策のアセスメント
           1. セキュリティアセスメント計画に記載されているアセスメント手順に従ってセキュリティ管理策をアセスメントする。
        3. タスク4-3 セキュリティアセスメントレポート
           1. セキュリティ管理策のアセスメントを通じて発見された問題、 導かれた結論および推奨事項を文書化した、 セキュリティアセスメントレポートを用意する。
        4. タスク4-4 是正活動
           1. セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、 セキュリティ管理策に対する初期の是正活動を実施し、 是正された管理策（複数）を適宜、 再アセスメントする。
     6. 3.5 RMF ステップ 5-情報システムの運用認可
        1. タスク5-1 行動計画とマイルストーン
           1. セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、 行動計画とマイルストーンを作成する（ただし、 既に実施されたすべての是正活動を除く）。
        2. タスク5-2 セキュリティ運用認可パッケージ
           1. セキュリティ運用認可パッケージをまとめて、 運用認可責任者に提出し、 裁定を仰ぐ。
        3. タスク5-3 リスクの判断
           1. 組織の業務（任務、 機能、 イメージ、 または評判を含む）、 組織の資産、 個人、 他の組織、 または国家に対するリスクを判断する。
        4. タスク5-4 リスクの受容
           1. 組織の業務、 組織の資産、 個人、 他の組織、 または国家に対するリスクが受容できるかどうかを判断する。
     7. 3.6 RMF ステップ 6-セキュリティ管理策の監視
        1. タスク6-1 情報システムやその運用環境に対する変更
           1. 情報システムおよびシステムの運用環境に対して提案されている、 あるいは、 実際に実施された変更がもたらすセキュリティへの影響を判断する。
        2. タスク6-2 継続的なセキュリティ管理策アセスメント
           1. 組織が定めた監視戦略に従って、 情報システムに導入される、 または情報システムによって継承される技術面、 管理面、 および運用面でのセキュリティ管理策の中から選択された管理策のサブセットをアセスメントする。
        3. タスク6-3 継続的な是正活動
           1. 継続的監視活動の結果、 リスクアセスメント結果、 および行動計画とマイルストーンにリストアップされている重要な項目に基づいて是正活動を実施する。
        4. タスク6-4 重要な更新
           1. 継続的監視プロセスの結果に基づいて、 セキュリティ計画、 セキュリティアセスメントレポート、 および行動計画とマイルストーンを更新する。
        5. タスク6-5 セキュリティ状況の報告
           1. 監視戦略に従って、 継続的に、 情報システムのセキュリティ状況（情報システムに導入されるセキュリティ管理策、 および情報システムによって継承されるセキュリティ管理策の有効性を含む）を運用認可責任者および組織内の他の適切な職員に報告する。
        6. タスク6-6 継続的なリスク判断および受容
           1. 監視戦略に従って、 情報システムのセキュリティ状況に関する報告内容（情報システムに導入される、 または情報システムによって継承されるセキュリティ管理策の有効性を含む）を継続的に見直すことによって、 組織の業務、 組織の資産、 個人、 他の組織、 または国家に対するリスクが、 ひきつづき受容可能か否かを判断する
        7. タスク6-7 情報システムの切り離しおよび廃止
           1. 必要に応じて、 情報システムの廃止戦略を実施する。 この戦略は、 システムがサービスから切り離された時に必要となる活動を実施するためのものである。
  5. 付録 A 参考文献
  6. 付録B 用語集
  7. 付録C 略語
  8. 付録D 役割と責任
     1. D.1 政府機関の長（最高経営責任者） （HEAD OF AGENCY （CHIEF EXECUTIVE OFFICER））
     2. D.2 リスクエグゼクティブ（機能） （RISK EXECUTIVE （FUNCTION））
     3. D.3 最高情報責任者（CHIEF INFORMATION OFFICER）
     4. D.4 情報のオーナー／スチュワード（INFORMATION OWNER/STEWARD）
     5. D.5 上級情報セキュリティ責任者（SENIOR INFORMATION SECURITY OFFICER）
     6. D.6 運用認可責任者（AUTHORIZING OFFICIAL）
     7. D.7 運用認可責任者が指名する代理人（AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE）
     8. D.8 共通管理策の提供者（COMMON CONTROL PROVIDER）
     9. D.9 情報システムのオーナー（INFORMATION SYSTEM OWNER）
     10. D.10 情報システムセキュリティ責任者（INFORMATION SYSTEM SECURITY OFFICER）
     11. D.11 情報セキュリティアーキテクト（INFORMATION SECURITY ARCHITECT）
     12. D.12 情報システムセキュリティエンジニア（INFORMATION SYSTEM SECURITY ENGINEER）
     13. D.13 セキュリティ管理策アセサー（SECURITY CONTROL ASSESSOR）
  9. 付録E RMFの各タスクの要約
  10. 付録F セキュリティ運用認可
      1. F.1 運用認可パッケージ（AUTHORIZATION PACKAGE）
         1. セキュリティ計画
         2. セキュリティアセスメントレポート
         3. 行動計画とマイルストーン
         4. 情報システムのセキュリティ分類
         5. セキュリティ管理策の具体的な弱点または欠陥
         6. セキュリティ管理策において特定された弱点または欠陥の重大性（すなわち、 それらの弱点または欠陥が、 情報システムの全体的なセキュリティ状態、 ならびに、 組織のリスクへの暴露65に及ぼす直接的／間接的な影響）
         7. 提案されている、 セキュリティ管理策に関して特定された弱点または欠陥に対処するためのリスク軽減アプローチ（たとえば、 リスク軽減活動の優先順位付け、 リスク軽減に必要なリソースの割り当て）、 および
         8. セキュリティ管理策の弱点または欠陥の一部の受容に関する組織の根拠。
         9. サブトピック  
            
      2. F.2 運用認可判断（AUTHORIZATION DECISIONS）
         1. 運用の認可
         2. 運用の不許可
      3. F.3 運用認可の判断文書（AUTHORIZATION DECISION DOCUMENT）
         1. 運用認可の判断
         2. 運用認可のための諸条件
         3. 運用認可の満了日
         4. リスクエグゼクティブ（機能）から得られる情報（提供される場合）
      4. F.4 継続的な運用認可（ONGOING AUTHORIZATION）
      5. F.5 タイプ運用認可（TYPE AUTHORIZATION）
      6. F.6 運用認可アプローチ（AUTHORIZATION APPROACHES）
  11. 付録G 継続的な監視
      1. G.1 監視戦略（MONITORING STRATEGY）
      2. G.2 監視すべきセキュリティ管理策の選択（SELECTION OF SECURITY CONTROLS FOR MONITORING）
      3. G.3 主要ドキュメントの更新および状況報告（KEY DOCUMENT UPDATES AND STATUS REPORTING）
  12. 付録H 運用上のシナリオ
  13. 付録I 外部環境におけるセキュリティ管理策

1. NIST SP 800-53 (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)
   1. 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

ドキュメントを参照: [000056415.pdf](https://www.ipa.go.jp/files/000056415.pdf)

* 1. NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 2013 年 4 月（2014 年 1 月 15 日時点での更新内容を含む）.
  2. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

ドキュメントを参照: [NIST.SP.800-53r4.](http://dx.doi.org/10.6028/NIST.SP.800-53r4.)

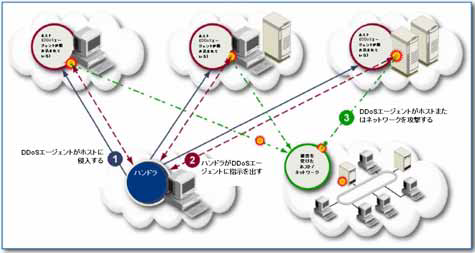
* 1. 第1 章はじめに
     1. 1.1 目的および適用範囲
     2. 1.2 対象と想定する読者
     3. 1.3 セキュリティ管理策に関する他の発行文書との関係
     4. 1.4 組織の責任
     5. 1.5 本文書の構成
  2. 第2 章基本事項
     1. 2.1 多層から成るリスクマネジメント
     2. 2.2 セキュリティ管理策の構造
     3. 2.3 セキュリティ管理策ベースライン
     4. 2.4 セキュリティ管理策の指定方法
     5. 2.5 外部サービスプロバイダ
     6. 2.6 保証と信用
     7. 2.7 改訂と拡張
  3. 第3 章プロセス
     1. 3.1 管理策ベースラインを選択する
     2. 3.2 ベースラインセキュリティ管理策を調整する
     3. 3.3 オーバーレイを作成する
     4. 3.4 管理策の選択プロセスを文書化する
     5. 3.5 新規に開発するシステムとレガシーシステム
  4. 付録 A 参考文献
  5. 付録 B 用語集
  6. 付録 C 略語
  7. 付録 D セキュリティ管理策ベースラインの要約
  8. 付録 E 保証と信用性
  9. 付録 F セキュリティ管理策カタログ
  10. 付録 G 情報セキュリティプログラム
  11. 付録 H 国政情報セキュリティ標準
  12. 付録 I オーバーレイテンプレート
  13. 付録 J プライバシー管理策カタログ

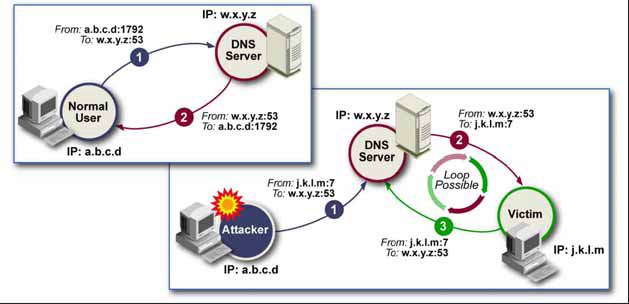
1. NIST SP 800-61 (コンピュータセキュリティインシデント対応ガイド)
   1. コンピュータセキュリティインシデント対応ガイドSP800-61 rev.1翻訳版【2008年03月NIST】

ドキュメントを参照: [000025341.pdf](https://www.ipa.go.jp/files/000025341.pdf)

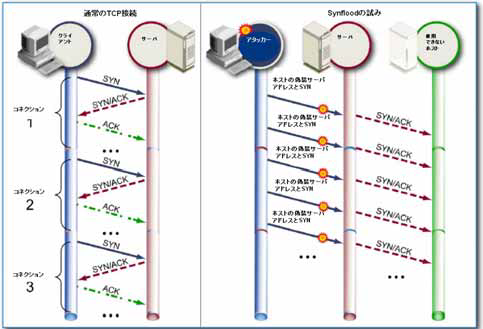
* 1. 要旨
     1. 1. はじめに
        1. 1.1. 権限
        2. 1.2. 目的および適用範囲
           1. 本書は、 事件に効果的かつ効率的に対応するための実用的な手引きとなることで、 各組織が情報セキュリティインシデントによるリスクを軽減するのに役立てることを意図したものである。
        3. 1.3. 対象とする読者
           1. CSIRT、 システム管理者とネットワーク管理者、 セキュリティスタッフ、 技術サポートスタッフ、 最高情 報責任者(CIO)、 コンピュータセキュリティプログラムマネージャ向け
        4. 1.4. ドキュメントの構成
     2. 2. コンピュータセキュリティインシデント対応能力の組織化
        1. 2.1. 事象と事件
        2. 2.2. インシデント対応の必要性
        3. 2.3. インシデント対応のポリシー、 計画および手順の作成
           1. 2.3.1. ポリシーの要素
           2. 2.3.2. 計画の要素
           3. 2.3.3. 手順の要素
           4. 2.3.4. 外部の関係者との情報共有

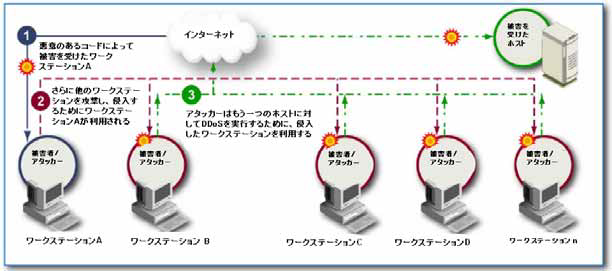
サブトピック  


* + - 1. 2.4. インシデント対応チームの構成
         1. 2.4.1. チームのモデル
         2. 2.4.2. チームモデルの選択
         3. 2.4.3. インシデント対応要員
         4. 2.4.4. 組織内の依存関係
      2. 2.5. インシデント対応チームのサービス
      3. 2.6. 推奨事項
    1. 3. 事件処理
       1. サブトピック  
          
       2. 3.1. 準備
          1. 3.1.1. 事件処理に備える
          2. 3.1.2. 事件の予防
       3. 3.2. 検知と分析
          1. 3.2.1. 事件の分類
          2. 3.2.2. 事件の兆候
          3. 3.2.3. 前兆と兆候のソース
          4. 3.2.4. 事件の分析
          5. 3.2.5. 事件の文書化
          6. 3.2.6. 事件の優先順位付け
          7. 3.2.7. 事件の通知
       4. 3.3. 封じ込め、 根絶、 復旧
          1. 3.3.1. 封じ込め戦略の選択
          2. 3.3.2. 証拠の収集と処理
          3. 3.3.3. アタッカーの特定
          4. 3.3.4. 根絶と復旧
       5. 3.4. 事件後の対応
          1. 3.4.1. 教訓
          2. 3.4.2. 収集された事件データの利用
          3. 3.4.3. 証拠の保管
       6. 3.5. 事件処理のチェックリスト
       7. 3.6. 推奨事項
    2. 4. サービス不能事件の処理
       1. 4.1. 事件の定義と例
          1. サブトピック  
             
          2. 4.1.1. リフレクタ攻撃

サブトピック  


* + - * 1. 4.1.2. アンプ(amplifier)攻撃
        2. 4.1.3. Flood攻撃

サブトピック  


* + - 1. 4.2. 準備
         1. 4.2.1. 事件処理の準備
         2. 4.2.2. 事件の予防
      2. 4.3. 検知と分析
      3. 4.4. 封じ込め、 根絶、 復旧
         1. 4.4.1. 封じ込め戦略の選択
         2. 4.4.2. 証拠の収集と処理
      4. 4.5. サービス不能事件の処理のためのチェックリスト
      5. 4.6. 推奨事項
    1. 5. 悪意のコードによる事件の処理
       1. 5.1. 事件の定義と例
          1. 5.1.1. ウイルス
          2. 5.1.2. ワーム
          3. 5.1.3. トロイの木馬
          4. 5.1.4. 悪意のあるモバイルコード
          5. 5.1.5. 混合攻撃
          6. 5.1.6. 追跡クッキー
          7. 5.1.7. 攻撃ツール
          8. 5.1.8. マルウェア以外の脅威
       2. 5.2. 準備
          1. 5.2.1. 事件処理の準備
          2. 5.2.2. 事件の予防
       3. 5.3. 検知と分析
       4. 5.4. 封じ込め、 根絶、 復旧
          1. 5.4.1. 封じ込め戦略の選択
          2. 5.4.2. 証拠の収集と処理
          3. 5.4.3. 根絶と復旧
       5. 5.5. 悪意のコードによる事件の処理のためのチェックリスト
       6. 5.6. 推奨事項
    2. 6. 不正アクセス事件の処理
       1. 6.1. 事件の定義と例
       2. 6.2. 準備
          1. 6.2.1. 事件処理の準備
          2. 6.2.2. 事件の予防
       3. 6.3. 検知と分析
       4. 6.4. 封じ込め、 根絶、 復旧
          1. 6.4.1. 封じ込め戦略の選択
          2. 6.4.2. 証拠の収集と処理
          3. 6.4.3. 根絶と復旧
       5. 6.5. 不正アクセス事件を処理するためのチェックリスト
       6. 6.6. 推奨事項
    3. 7. 不適切な使用による事件の処理
       1. 7.1. 事件の定義と例
       2. 7.2. 準備
          1. 7.2.1. 事件処理の準備
          2. 7.2.2. 事件の予防
       3. 7.3. 検知と分析
       4. 7.4. 封じ込め、 根絶、 復旧
       5. 7.5. 不適切な使用の事件を処理するためのチェックリスト
       6. 7.6. 推奨事項
    4. 8. 複合要素の事件の処理
       1. 8.1. 事件の定義と例
          1. サブトピック  
             
       2. 8.2. 準備、 検知、 分析
       3. 8.3. 封じ込め、 根絶、 復旧
       4. 8.4. 複合要素の事件を処理するためのチェックリスト
       5. 8.5. 推奨事項
  1. 付録
     1. 付録 A 推奨事項
        1. A.1 コンピュータセキュリティインシデント対応能力の組織化
           1. A.1.1 インシデント対応ポリシー、 計画、 および手順の作成

+ インシデント対応ポリシーを作成する

+ インシデント対応ポリシーをもとに、 インシデント対応計画を作成する

+ インシデント対応手順を作成する

+ 事件関連の情報共有に関するポリシーと手順を確立する

+ 適切な事件報告組織に、 事件についての関係情報を提供する

* + - * 1. A.1.2 インシデント対応チームの構成とサービス

+ インシデント対応チームモデルを選ぶ際には、 関係する要因を検討すること

+ インシデント対応チームには適切なスキルをもった人間を選ぶこと

+ 事件処理に参加してもらう必要がある、 組織内のほかのグループを明確にする

+ チームが提供するサービスを決める

* + - 1. A.2 準備
         1. + 事件処理で利用できそうなツールとリソースを入手する
         2. + ネットワーク、 システム、 アプリケーションを十分に安全な状態に保つことで、 事件の発生を予防する
         3. A.2.1 サービス不能事件

+ ファイアウォールルールセットを設定して、 リフレクタ攻撃を予防する

+ 境界ルーターを設定してアンプ攻撃を防ぐ

+ 組織のインターネットサービスプロバイダ(ISP)や二次プロバイダから、 ネットワークベースのDoS攻撃の処理において、 どういった支援が得られるのかを確認する

+ セキュリティソフトウェアを設定し、 DoS攻撃を検知する

+ ネットワーク境界で、 明示的に許可されていないすべての送受信トラフィックを拒否するように設定する

* + - * 1. A.2.2 悪意のコードの事件

+ 悪意のコードの問題について、 ユーザに自覚させる

+ ウイルス対策ソフトウェアベンダーの広報を読む

+ 重要なホストには、 ホスト型のIDPS(ファイル完全性チェッカーを含む)を配備する

+ ウイルス対策ソフトウェアを使用し、 最新のウイルスシグネチャを使って最新に保つ

+ 疑いのあるファイルをブロックするようにソフトウェアを設定する

+ 開かれているWindowsの共有を解除する

* + - * 1. A.2.3 不正アクセス事件

+ 侵入検知ソフトウェアを設定して、 不正なアクセスを取得しようという試みに対して警報を発生する

+ すべてのホストに対して、 ログの一元化のための設定を行う

+ 全ユーザにパスワードを変更させるための手順を確立する

+ ネットワーク境界で、 明示的に許可されていないすべての受信トラフィックを拒否するように設定する

+ モデムや仮想プライベートネットワーク(VPN)を含むすべてのリモートアクセス手段のセキュリティを高める

+ 公にアクセスできるサービスは、 安全な非武装地帯(DMZ)ネットワークセグメントに置く

+ ホスト上で不必要なサービスはすべて無効にし、 重要なサービスは分離する

+ ホストベースのファイアウォールソフトウェアまたはパーソナルファイアウォールを使用して、 各ホストが攻撃にさらされないようにする

+ パスワードポリシーの作成と実施

* + - * 1. A.2.4 不適切な使用の事件

+ 不適切な使用の事件の処理について、 組織の人事部および法務部と話し合う

+ 責任問題について組織の法務部と話し合う

+ 特定の種類の不適切な使用を検知するように侵入検知ソフトウェアを設定する

+ ユーザの活動に関する基本的な情報をログに記録する

+ すべての電子メールサーバを、 不正なメール中継で利用できないように設定する

+ すべての電子メールサーバでスパムフィルタリングを実行する

+ URLフィルタリングソフトウェアを実行する

* + - * 1. A.2.5 複合要素の事件

+ 一元化したログとイベント相関処理ソフトウェアを使用する

* + - 1. A.3 検知と分析
         1. + いくつもの種類のセキュリティソフトウェアが生成した警報を使って、 前兆や兆候を見つける
         2. + 外部の者が事件を報告する仕組みを確立する
         3. + 全システムにログと監査の基準レベルを義務付け、 重要なシステムではより高い基準レベルを義務付ける
         4. + ネットワークとシステムのプロファイル
         5. + ネットワーク、 システム、 アプリケーションの正常な動作を理解する
         6. + 一元化されたログ取得とログ保管ポリシーの作成
         7. + イベント相関処理の実施
         8. + すべてのホストの時刻を同期させておく
         9. + 情報の知識ベースの維持と利用
         10. + 経験が少ないスタッフのための診断マトリックスの作成
         11. + 事件が起きた疑いがある場合には、 すぐに全情報の記録を開始する
         12. + 事件データの保護
         13. + 影響のあるリソースの重要性や事件の技術的な影響に基づき、 ビジネスインパクトごとに事件に優先順位を付ける
         14. + 組織のインシデント対応ポリシーの中に、 事件報告に関する項目を盛り込む
      2. A.4 封じ込め、 根絶、 復旧
         1. + 事件を封じ込めるための戦略と手順の確立
         2. + 証拠収集と処理のための、 確立された手順に従うこと
         3. + 揮発性データを証拠としてシステムから取得する
         4. + ファイルシステムのバックアップではなく、 完全なフォレンジックディスクイメージを使って、 システムのスナップショットを取得する
         5. A.4.1 サービス不能事件

+ いくつかの対策を順に並べた封じ込め戦略を作成する

* + - * 1. A.4.2 悪意のコードの事件

+ 悪意のコードによる事件は、 できるだけ早く封じ込める

* + - * 1. A.4.3 不正アクセス事件

+ 変更管理情報をインシデント対応チームに提供する

+ リスク軽減とサービス維持のバランスを考えた封じ込め戦略を選択する

+ rootが奪取されたと思われるシステムはリストアまたは再インストールする

* + - * 1. A.4.4 複合要素の事件

+ 最初の事件を封じ込めてから、 事件のほかの要素の兆候を探す

* + - 1. A.5 事後活動
         1. + 大きな事件の後には反省会を開催する
         2. A.5.1 不正アクセス事件

+ 事件の各要素の処理に個別に優先順位を付ける

* + 1. 付録 B 事件処理のシナリオ
       1. B.1 シナリオの質問
          1. 準備:

1. あなたの組織では、 この活動を事件とみなしますか? もしそうなら、 この活動は、 組織のどのポリシーに違反していますか? (セクション2.1)

2. この種のインシデントの発生を防止し、 その影響を限定するために、 どのような措置を講じていますか？(セクション3.1.2)

* + - * 1. 検知と分析:

1. あなたの組織では、 インシデントのどんな前兆（あれば）を検知しますか？前兆があった場合、 あなたの組織はインシデントが起きる前に行動を起こそうとしますか？ (セクション3.2.2、 3.2.3)

2. あなたの組織では、 インシデントのどんな兆候を検知しますか？どの兆候があったらインシデントが起きた可能性があると考えますか？ (セクション3.2.2、 3.2.3)

3. インシデント対応チームは、 どうやってこのインシデントを分析し検証しますか？ (セクション3.2.4)

4. チームはこのインシデントを、 組織内のだれに／どのグループに報告しますか？ (セクション3.2.7)

5. インシデント対応チームは、 どのようにしてこのインシデントの対応に優先順位をつけますか？ (セクション3.2.6)

* + - * 1. 封じ込め、 根絶、 復旧:

1. このインシデントを封じ込めるために、 あなたの組織はどんな方策を採用しますか？この方策がほかよりも望ましいのはなぜですか？ (セクション3.3.1)

2. インシデントを封じ込めないと、 何が起きる可能性がありますか？ (セクション3.3.1)

3. あなたの組織では、 どんな証拠ソース(あれば)を取得しますか? 証拠はどのようにして取得しますか? どこに保管しますか? どれだけの期間保管しますか? (セクション3.2.5、 3.3.2、 3.4.3)

* + - * 1. 事後活動:

1. このインシデントに関する反省会にはだれが参加しますか？ (セクション3.4.1)

2. 将来同様のインシデントの発生を防ぐには何ができますか？ (セクション3.1.2)

3. 同様のインシデントの検知を向上させるためには何ができますか？ (セクション3.1.2)

* + - * 1. 一般的な質問:

1. このインシデントの対応には、 インシデント対応チームのメンバーが何人参加しますか？(セクション2.4.3)

2. インシデント対応チーム以外で、 組織内のどのグループがこのインシデントの処理に関連しますか？(セクション2.4.4)

3. チームからどの外部関係者にこのインシデントを報告しますか？いつ報告しますか？報告はどのように行いますか？ (セクション2.3.2)

4 . 外部関係者への連絡事項には、 ほかに何がありますか？ (セクション2 . 3 . 2 )

5. このインシデントへの対応にあたって、 どのツールやリソースを使用しますか？ (セクション3.1.1)

6. インシデントが別の日の別の時間（就業時間内と就業時間外）に起きていたら、 対応方法にどのような面で違いが生じていましたか？ (セクション2.4.2)

7. インシデントが物理的に別の場所（オンサイトとオフサイト）で起きていたら、 対応方法にどのような面で違いが生じていましたか？ (セクション2.4.2)

* + - 1. B.2 シナリオ
         1. シナリオ1: DNS (Domain Name System)サーバのサービス不能
         2. シナリオ2: 内部で生成されたスパム
         3. シナリオ3: ワームとDDoSエージェントへの感染
         4. シナリオ4: 盗まれたクレジットカード番号の使用
         5. シナリオ5: 侵入されたデータベースサーバ
         6. シナリオ6: ウイルスデマ情報
         7. シナリオ7: FTPサーバ上の不正なデータ
         8. シナリオ8: 外部へのDDoS攻撃
         9. シナリオ9: 給与支払い記録への不正アクセス
         10. シナリオ10: ハッキングツールのダウンロード
         11. シナリオ11: 消えたホスト
         12. シナリオ12: 在宅勤務の侵害
         13. シナリオ13: テロリストの脅威
         14. シナリオ14: フレームとポートスキャニング
         15. シナリオ15: ピアツーピアのファイル共有
         16. シナリオ16: 不明なワイヤレスアクセスポイント
    1. 付録 C 事件に関係するデータフィールド
       1. C.1 基本的なデータフィールド
          1. + 事件報告者の連絡先情報

- 名前

- 組織ユニット(機関、 部門、 部、 チーム)

- 電子メールアドレス

- 電話番号

- 場所(住所、 オフィスの部屋番号など)

* + - * 1. + 事件の詳細

- 事件を発見した日付と時刻(タイムゾーンを含む)

- 事件が発生した日付と時刻(タイムゾーンを含む)

- 事件の種類(サービス不能、 悪意のコード、 不正アクセス、 不適切な使用など)

- 事件の物理的な位置(市、 州など)

- 事件の現在の状態(攻撃が継続中など)

- 事件のソースや原因(わかる場合)。 ホスト名とIPアドレスを含む。

- 事件の説明(どうやって検知したか、 何が起きたかなど)

- オペレーションシステムの種類、 オペレーションシステムのバージョンおよびパッチレベル

- ウイルス対策ソフトウェアがインストールされ、 有効かつ最新になっているか(はい／いいえ)

- 影響を受けたリソースの説明(ネットワーク、 ホスト、 アプリケーション、 データなど)。 システムのホスト名とIPアドレス、 および機能を含む。

- 事件を緩和するための要素

- 事件の技術的な影響の見積(データ消去、 システムクラッシュ、 アプリケーション利用不可など)。 (セクション2.3.6を参照して、 事件の重大さの格付けと影響の格付けを行うこと)

- 実施した対応活動(ホストの停止、 ホストのネットワークからの切断など)

- 連絡するほかの組織(ソフトウェアベンダーなど)

- 事件の最中に侵害された個人情報(あれば)の種類

* + - * 1. + 一般的なコメント
      1. C.2 事件処理担当者のデータフィールド
         1. + インシデント対応の現在のステータス
         2. + 事件の概要
         3. + 事件処理活動

- すべての処理担当による活動の記録

* + - * 1. - 関連する全団体の連絡先情報

- 収集した証拠の一覧

* + - * 1. + 事件処理担当者のコメント
        2. + 事件の原因(アプリケーションの設定ミス、 ホストのパッチ未適用など)
        3. + 事件のコスト115
        4. + 事件のビジネスインパクト116
    1. 付録 D 用語集
    2. 付録 E 頭字語
    3. 付録 F 印刷されたリソース
    4. 付録 G オンラインのツールとリソース
    5. 付録 H よく聞かれる質問
    6. 付録 I 危機処理のステップ
       1. 以下に、 技術の専門家が重大な事件が発生したことを確信したものの、 組織に利用できるインシデント対応能力がない場合に実施すべき主なステップを示す。
       2. この付録は、 現在危機に直面していて、 このドキュメント全体を読む時間がないという人にとって、 基本的な参考資料となる。
       3. 1. すべてを記録に残すこと
          1. これには、 実行するあらゆる行動、 あらゆる証拠、 ユーザ、 システムオーナー、 事件に関係するその他の人とのあらゆる会話を含む。
       4. 2. 支援してくれる同僚を捜す
          1. 二人以上で協力すれば、 事件処理ははるかに容易になる。 たとえば、 ひとりが行動している間、 もう一人はそれを記録する。
       5. 3. 証拠を分析して事件が起きたことを確認する
          1. 必要に応じてさらに調査(インターネットサーチエンジン、 ソフトウェアマニュアルなど)し、 証拠をよく理解する。 組織内の技術専門家に連絡し、 助けを求める。
       6. 4. 事件が起きたと思われる場合には、 組織内の適切な人に通知する
          1. これには最高情報責任者(CIO)、 情報セキュリティ部門長、 ローカルセキュリティマネージャが含まれる。 事件の詳細をだれかと話す場合は慎重に行う。 その事件により個人情報が流出したと思われる場合は、 組織のデータ侵害ポリシーが規定する関係者に、 その旨を通知する。 知る必要がある人にしか話さないようにし、 十分安全な通信手段を使用する(アタッカーが電子メールサービスを侵害した場合、 事件に関する電子メールは送らないこと)。
       7. 5. US-CERT(政府の諸官庁と機関の場合)および／または他の外部組織に事件を通知する。
          1. まずは、 誤って機密情報を公開しないように、 事件に関して広報部、 法務部、 および／またはマネジメント層と話し合う。 その後、 US-CERTおよび／または他の外部組織に事件を報告し、 事件対応の支援を要請する。
       8. 6. 進行中の事件を止める
          1. そのための最も一般的な方法は、 影響を受けたシステムをネットワークから切断することである。 サービス不能(DoS)攻撃などでは、 ファイアウォールやルーターの設定を変更して、 事件の一部になっているネットワークトラフィックを止めなくてはならない場合もある。
       9. 7. 事件の証拠を保管する
          1. 影響を受けたシステムのバックアップを作成する(ファイルシステムのバックアップではなく、 ディスクイメージのバックアップが望ましい)。 また、 事件に関連する証拠が入ったログファイルをコピーする。
       10. 8. 事件のすべての影響を一掃する
           1. これには、 悪意のコードの感染ファイル、 不適切なデータ(海賊版ソフトウェアなど)、 トロイの木馬のファイル、 事件がもたらしたシステムへの変更に対する作業が含まれる。 システムが完全に侵害された場合は、 一から再構築するか、 正しいことがわかっているバックアップからリストアする。
       11. 9. 悪用されたすべての脆弱性を見つけて修正する
           1. 事件はオペレーティングシステムやアプリケーションの脆弱性を利用することで起きた可能性が高い。 そのような脆弱性を見つけて取り除くか軽減し、 再発しないようにすることが重要である。
       12. 10. 運用が通常に戻ったことを確認する
           1. 事件により影響を受けたデータ、 アプリケーション、 その他のサービスが通常の運用に戻ったことを確認する。
       13. 11. 最終レポートの作成
           1. このレポートには、 事件処理プロセスを詳述する。 また、 何が起きたかを要約し、 もし正式なインシデント対応能力があれば、 どれだけ早く状況を処理し、 リスクを軽減し、 被害を制限できたかも記載する。
    7. 付録 J 連邦政府機関による事件報告の分類

1. NIST SP 800-63 (電子的認証に関するガイドライン)
   1. 電子的認証に関するガイドライン Electronic Authentication Guideline
   2. 2017年に改訂された
      1. IDを利用する場面ごとのリスクに応じて検証プロセスの強度を選択するという考え方が導入された
      2. 「パスワードは定期変更すべき」「パスワードは複数の」文字種で混成すべき」などの、 従来は常識とされてきた対策についても、 実効性や技術の進展に合わせた見直しが図られてる
      3. パスワードに代わる認証手段として、 指紋や顔画面などを活用した生体認証や、 認証結果を完全にやりとりできる「FIDO」の普及が期待されている
      4. 携帯電話をWebサービス全般の汎用的な認証手段として利用するための「Mobile Connect」が注目されている
      5. FIDO(Fast Identity Onlinbe)
         1. 生体認証やデバイス認証などのパスワード認証に代わる認証方式を実現する際のフレームワーク
         2. 認証結果を公開鍵暗号方式により」ネットワーク上で安全にやりとりするための仕様が定められており、 認証に必要な秘密情報は認証を行う端末のみに保存され、 ネットワーク上での伝送やサーバーに保存する必要がない
      6. モバイル認証（GSMA Mobile Connect）
         1. 移動通信事業者（MNO:Mobile Network Operator）の業界団体であるGSMアソシエーション（GSMA）が普及を推進している、 携帯端末をWebサービスの認証機器として使用できるようにするための仕様「Mobile Connect」
   3. 文書
      1. SP 800-63-3
         1. Digital Identity Guidelines
         2. IDフレームワーク全体の概要、 リスクに応じた保証レベル(IAL/AAL/FAL)の選択
      2. SP 800-63-A
         1. Enrollment and Identity Proofing Requirements
         2. ID登録と身分確認におけるアイデンティティ保証レベル(IAL)の定義
      3. SP 800-63-B
         1. Authentication and Lifecycle Management
         2. 認証保証レベル(AAL)の導入と各認証方式に求められる要件、 脅威／プライバシー／ユーザビリティ面での考察ポイント
      4. SP 800-63-C
         1. Federation and Assertions
         2. 信頼関係を結んだシステム間での認証連携（フェデレーション）におけるフェデレーション保証レベル(FAL)の導入と各レベルに求められる要件、 プライバシーに考慮した属性連携
2. CSC20 （効果的なサイバー防御のための重要なセキュリティコントロール）
   1. 「Critical Security Controls for Effective Cyber Defense」（効果的なサイバー防御のための重要なセキュリティコントロール）は、 Version6.0が2015年10月に米国のCenter for Internet Securityから公開された。
   2. サイバー攻撃に対する重要なセキュリティ対策を20のコントロールに分類・優先度付けをしたもので、 極力自動化された技術的対策が主体となっている。
   3. CSC1 許可および無許可の機器のインベントリ
   4. CSC2 許可および無許可のソフトウェアのインベントリ
   5. CSC3 モバイル機器、 ラップトップ、 ワークステーション、 サーバにおけるハードウェアおよびソフトウェアのセキュアな構成
   6. CSC4 継続的な脆弱性診断と改修
   7. CSC5 管理者権限のコントロールされた使用
   8. CSC6 監査ログの保守、 監視、 および分析
   9. CSC7 電子メールとWebブラウザの保護
   10. CSC8マルウェア防御
   11. CSC9 ネットワークポート、 プロトコル、 サービスの制限およびコントロール
   12. CSC10 データ復旧能力
   13. CSC11 ファイアウォールやルーター、 スイッチなどのネットワーク機器のセキュアな構成
   14. CSC12 境界防御
   15. CSC13 データ保護
   16. CSC14 知る必要性に基づいた、 管理されたアクセス
   17. CSC15 無線のアクセスコントロール
   18. CSC16 アカウントのモニタリングおよびコントロール
   19. CSC17 不足を補完するためのセキュリティスキル評価および適切なトレーニング
   20. CSC18 アプリケーションソフトウェアのセキュリティ
   21. CSC19 インシデント対応と管理
   22. CSC20 ペネトレーションテストおよびレッドチームによる訓練
3. Top35 （標的型サイバー侵入の軽減戦略）
   1. 「Strategies to Mitigate Targeted Cyber Intrusions」(Top35 Mitigation Strategies)
   2. 「Strategies to Mitigate Targeted Cyber Intrusions」（標的型サイバー侵入の軽減戦略）は、 2014年2月に2014年版がオーストラリアの国防信号局から公開されています。 標的型攻撃を主な脅威と想定したセキュリティ対策を、 優先度順に35のカテゴリーで示したものです。
4. GDPR（General Data Protection Regulation：一般データ保護規則）
   1. GDPR（General Data Protection Regulation：一般データ保護規則）【個人情報保護委員会】

ドキュメントを参照: [GDPR](https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/)

* + 1. GDPR（General Data Protection Regulation：一般データ保護規則）
       1. EU（※）では、 EU域内の個人データ保護を規定する法として、 1995年から現在に至るまで適用されている「EUデータ保護指令（Data Protection Directive 95）」に代わり、 2016年4月に制定された「GDPR（General Data Protection Regulation：一般データ保護規則）」が2018年5月25日に施行されます。
       2. GDPRは個人データやプライバシーの保護に関して、 EUデータ保護指令より厳格に規定します。
       3. また、 EUデータ保護指令がEU加盟国による法制化を要するのに対し、 GDPRはEU加盟国に同一に直接効力を持ちます。
       4. ※ EU：EU加盟国及び欧州経済領域（EEA）の一部であるアイスランド、 ノルウェー、 リヒテンシュタイン
       5. なお、 EU各国の個人情報保護機関については、 こちらをご覧ください。

ドキュメントを参照: [EU-DPA](https://www.ppc.go.jp/enforcement/cooperation/cooperation/EU-DPA/)

* + 1. EU域外適用に関する影響
       1. GDPRはEU域外の事業者へも適用されます。 各組織・企業等の業務への影響について、 あらかじめ備えておく必要があります。
       2. 欧州委員会（European Commission）がWebサイトに掲載している資料の内、 以下の日本語仮訳を作成いたしましたので掲載いたします。
       3. Infographic（外部サイト（欧州委員会））

ドキュメントを参照: [index\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm)

* + - * 1. 日本語仮訳付PDF (PDF：1090KB) （中小企業向けの、 簡単にまとめられたGDPR説明）

ドキュメントを参照: [EC-Infographic.pdf](https://www.ppc.go.jp/files/pdf/EC-Infographic.pdf)

* + - 1. Fact Sheet "Questions and Answers-Data protection reform package"（外部サイト（欧州委員会））

ドキュメントを参照: [press-release\_MEMO-17-1441\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm)

* + - * 1. 日本語仮訳付PDF (PDF：318KB) （GDPRによるデータ保護改革案についての質疑応答概略）

ドキュメントを参照: [Factsheet-20170524QandA.pdf](https://www.ppc.go.jp/files/pdf/Factsheet-20170524QandA.pdf)

* + 1. 越境データ移転
       1. GDPRは、 EU域内の個人データのEU域外への移転について規定します。
       2. EU域内から域外へ個人データを移転するには、
       3. 十分な個人データ保護の保障
          1. （欧州委員会が、 データ移転先の国が十分なレベルの個人データ保護を保障していることを決定）
       4. BCR（Binding Corporate Rules：拘束的企業準則）の締結
          1. （企業グループで1つの規定を策定し、 データ移転元の管轄監督機関が承認）
       5. SCC（Standard Contractual Clauses：標準契約条項）の締結
          1. （データ移転元とデータ移転先との間で締結し、 欧州委員会が承認）
       6. 明確な本人同意
       7. 等、 一定の条件を満たさなくてはなりません。
    2. 日EU間の越境データ移転
       1. 我が国においては、 個人情報保護法が外国にある第三者への個人データの提供について規定しています。 個人データを越境移転するためには、
          1. 我が国と同等の水準にあると認められる個人情報保護制度を有している外国として委員会規則で定めるもの
          2. 必要な措置を継続的に講ずるため、 委員会規則に定める基準に適合する体制を整備している個人情報取扱事業者
          3. あらかじめ外国にある第三者への提供を認める旨の本人の同意がある場合
       2. 等、 一定の条件を満たさなくてはなりません。
       3. 日EU間においては、 双方の規定の下で、 相互に円滑な個人データ移転を行う環境を確保することを目指し、 当委員会と欧州委員会は対話を重ねてきています。
       4. 2017年12月14日には、 個人情報保護委員会熊澤委員と欧州委員会ヨウロバー委員が、 日EU間の個人データ移転について会談を行い、 双方の制度間の関連する相違点に対処するための、 法令改正を行わない形での解決策について確認するとともに、 今後、 その詳細について作業すること、 また、 2018年第一四半期に、 最終合意することを想定し、 委員レベルで会談をもつことで一致しました。
       5. 上記の会談について、 熊澤委員とヨウロバー委員は「共同プレスステートメント」 (PDF：149KB) を発出しました。

ドキュメントを参照: [291215\_pressstatement.pdf](https://www.ppc.go.jp/files/pdf/291215_pressstatement.pdf)

* + - 1. 「共同プレスステートメント」（2017年12月14日） (PDF：149KB)

ドキュメントを参照: [291215\_pressstatement.pdf](https://www.ppc.go.jp/files/pdf/291215_pressstatement.pdf)

* + 1. 参考（外部サイト）
       1. GDPR（欧州連合（EU）Webサイト）

ドキュメントを参照: [oj](http://eur-lex.europa.eu/eli/reg/2016/679/oj)

* + - 1. 2018 reform of EU data protection rules（欧州委員会（EC）Webサイト）

ドキュメントを参照: [2018-reform-eu-data-protection-rules\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)

* + - 1. Questions and Answers - GDPR - Factsheets 24 January 2018（欧州委員会（EC）Webサイト）

ドキュメントを参照: [press-release\_MEMO-18-387\_en.htm](http://europa.eu/rapid/press-release_MEMO-18-387_en.htm)

* + - 1. GDPRガイドライン（欧州委員会（EC）Webサイト）

ドキュメントを参照: [item-detail.cfm](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

* + - * 1. Guidelines on the right to "data portability", wp242rev.01\_en（PDF）
        2. Guidelines on Data Protection Officers ( DPOs ), wp243rev.01\_en（PDF）
        3. Guidelines on The Lead Supervisory Authority, wp244rev.01\_en（PDF）
        4. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01（PDF）
        5. Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, wp253（PDF）
        6. Guidelines on Data Protection Impact Assessment (DPIA), wp248（PDF）
        7. Guidelines on the right to "data portability"（PDF）

WP242 ANNEX-Frequently asked questions（PDF）

* + - * 1. Guidelines on Data Protection Officers ( DPOs ) （PDF）

WP243 ANNEX - Frequently asked questions（PDF）

* + - * 1. Guidelines for identifying a controller or processor's lead supervisory authority（PDF）

WP244 ANNEX II-Frequently asked questions（PDF）

* + - * 1. 未承認のガイドライン等については、 以下の欧州委員会（EC）Webサイトをご覧ください。

http://ec.europa.eu/newsroom/just/item-detail.cfm?item\_id=50083

ドキュメントを参照: [item-detail.cfm](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

* + - 1. Data Protection Reform - Factsheets 16 January 2017（EU加盟国の各国語）

ドキュメントを参照: [item-detail.cfm](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404)

* 1. 欧州連合における個人情報保護の枠組みGDPR、 その現状と対策のポイント【2017年08月01日富士通マーケティング】

ドキュメントを参照: [001.html](http://www.fujitsu.com/jp/group/fjm/mikata/column/sawa2/001.html)

* + 1. GDPRの概要
       1. 2016年5月4日付EU官報に掲載、 同年5月24日に発効、 行政罰を伴う適用開始は2018年5月25日であり、 ここからが実質の施行日となる。
       2. EUを含む欧州経済領域（EEA：EU加盟国28カ国＋アイスランド、 リヒテンシュタイン、 ノルウェー）域内で取得した「氏名」「メールドレス」「クレジットカード番号」などの個人データをEEA域外に移転することを原則禁止とする。 「個人」とは域内所在者のほか、 現地日系企業の現地採用従業員および日本から派遣される駐在員も含まれる点に注意。
       3. 個人データの範囲は、 職業上の電子メールアドレス、 オンライン識別子（IPアドレス／クッキー識別子）、 身体的、 生理学的、 遺伝子的、 精神的、 経済的、 文化的、 社会的固有性に関する要因も含まれる。
       4. EEA域内の現地法人・支店・駐在員を置くすべての企業・団体・機関が対象。
       5. EEA域内に上記支店などを置かない企業でも、 インターネット取引などで域内における所在者の個人情報を取得・移転する場合は適用対象となる。
       6. 個人情報の移転が適法となるのは、 十分性が認められる国・地域であるか、 適切な保護措置を取った場合とされるが、 十分性が認められた国は少なく、 日本企業は十分性が認められていないため、 保護措置を適切に施す必要がある。
       7. 違反の場合の制裁金は、 全世界年間売上高の4％以下または2000万ユーロ以下のいずれか高い方など。
       8. サイバーアタックなどで情報漏えいが発生したときの当局への報告や、 本人の求めに応じた個人情報の訂正などを怠った場合も制裁金の対象となることがある。
    2. 個人情報保護法との違い
       1. 前段に記述したとおり、 日本では個人情報の概念は氏名や住所などその人を特定できる情報という考え方になりますが、 GDPRではIDなど、 照合しないと個人が特定できないようなものも対象とされる点に注意が必要です。 また、 履歴データなども個人名がなければ問題なさそうに思えますが、 GDPRではこれも個人情報に該当します。
    3. GDPRが日本の企業に及ぼす影響
       1. 日本国内では本社と支店や系列企業の間での個人情報の移転は、 同じ企業内のセキュリティ措置で保護されていれば問題はありません。 しかし、 GDPR施行下では支店や系列企業内であってもEU域内から個人情報を移転することは原則できません。 ディスプレイで閲覧できる場合も移転とみなされる点に注意したいところです。
       2. 大きな影響を受けるのは、 EUを含めたEEA域内に支店や営業所、 系列企業などを持つグローバル企業でしょう。 現地採用の社員の個人情報はもちろん、 日本から出向している社員もEEA域内の事業所に勤務した場合は対象となるため、 扱いをルールに従ったものにしなければなりません。
       3. 海外に拠点を持つグローバル企業に限らず、 EEA域内の法人や団体とパートナー関係にある場合も注意しなければなりません。 GDPRの概要にも示したとおり、 日本のECサイトからEEA域内の在住者が購入をした場合も対象となるので、 技術提携や販売パートナーのような関係の企業との間においても十分な配慮が求められます。
    4. 日本企業の対応策
       1. 日本とは個人情報の定義や考え方が異なる点に留意し、 プライバシーポリシーに反映させる必要があります。 実務上、 EU域内の個人情報を移転する際は、 十分性があると認められていない日本では企業ごとに以下の手続きをしなければなりません。
          1. 「拘束的企業準則BCR（Binding Corporate Rules）」に準拠したルールを文書化して、 EUのデータ保護機関から承認を得る。 時間と費用を要するが承認されれば、 事業グループ内での地域を超えた個人情報の移動が、 ルールに従った範囲で可能となる。
          2. 「標準契約条項SCC（Standard Contractual Clauses）」はデータの移転を案件単位にして結ぶもので、 欧州委員会で決定された契約書のひな型であり、 当事者間でデータ移転契約として締結。 契約に即した履行体制が敷かれていることが前提である。 EU各国で条件が異なるため、 それぞれで事前承認取得などの作業が求められる。
       2. GDPRについてまとめてみました。 実質の施行となる2018年5月までに残された期間は余裕があるとはいえず、 この直前や施行されてから必要性に気づくのでは遅すぎます。 訪日旅客が増え、 東京オリンピックも近いため、 国内だけでサービス業を営む会社でもGDPRの内容を確認しておくことをお勧めします。
  1. EU一般データ保護規則（GDPR）の概要と企業が対応すべき事項【情報センサー2017年2月号】

ドキュメントを参照: [2017-02-05.html](https://www.eyjapan.jp/library/issue/info-sensor/2017-02-05.html)

* + 1. Ⅰ EU一般データ保護規則の概要
       1. 1. GDPRとは
          1. EU一般データ保護規則（General Data Protection Regulation：GDPR）は欧州連合（EU）における新しい個人情報保護の枠組みであり、 個人データ（personal data）の処理と移転に関するルールを定めた規則です。 1995年から適用されたEUデータ保護指令（Data Protection Directive 95）に代わり、 EU加盟諸国に対して直接効力が発生する法規制としてGDPRが2016年4月に制定されました。
       2. 2. GDPRの規制事項
          1. (1) 個人データの処理

個人データを処理するに当たり、 企業は管理者（Controller）として、 次のような規制事項を遵守することが求められます。

個人データの処理および保管に当たり、 適切な安全管理措置を講じなければならない。

処理を行う目的の達成に必要な期間を超えて個人データを保持し続けてはならない。

個人データの侵害（情報漏えい）が発生した場合、 企業はその旨を監督機関に対し72時間以内に通知しなければならない。

定期的に大量の個人データを取扱う企業などでは、 データ保護オフィサー（Data Protection Officer）を任命しなければならない。

* + - * 1. (2) 個人データの移転

EEA（欧州経済領域）の域内から域外への個人データの移転は原則として禁止され、 例えば日本のように欧州委員会によって適切な個人情報保護制度を有していると認められていない国への情報移転に当たっては、 企業は拘束的企業準則（Binding Corporate Rules）の策定、 標準契約条項（Standard Contract Clauses）の締結など、 適切な施策の下で一定の要件を満たす必要があります。

* + - * 1. (3) 基本的権利の保護

GDPRはデータ主体（Data Subject）すなわち本人の基本的権利を保護するという考え方が強く打ち出されています（GDPR第1条）。 例えば個人データの取得に際しては、 以下のようなルールが定められています。

企業は管理者として自らの身元や連絡先、 処理の目的、 第三者提供の有無、 保管期間、 データ主体の有する権利などについて、 明瞭で分かりやすい表現によりデータ主体に通知しなければならない。

企業は前記に関して明確な方法により同意を得るとともに、 データ主体が同意を自由に撤回することができる権利を適切に行使できるようにしなければならない。

個人データをデータ主体から直接取得していない場合、 企業は当該情報の入手先を本人に通知しなければならない。

こうした主な規制事項を含め、 GDPRでは全部で173項目の前文とともに99条にわたる規制事項がきめ細かく定められています。

* + 1. Ⅱ 日本企業への影響
       1. 1. 影響を受ける企業
          1. GDPRはEUで定められたルールですが、 以下のような場合は日本の企業であっても適用対象となり、 必ずしも無関係であるとは限らない点に注意が必要です。
          2. (1) EUに子会社、 支店、 営業所を有している企業

EU域内に所在地がある当該子会社などにとってGDPRは直接の適用対象であり、 当該企業は日本に本社を有している場合でも、 管理者としてGDPRへの対応が必要となります。

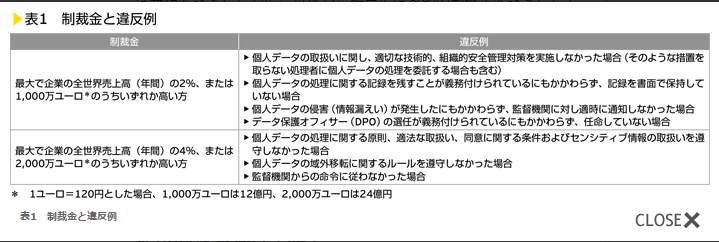
* + - * 1. (2) 日本からEUに商品やサービスを提供している企業

EU域内の個人（消費者）に対して日本から商品やサービスを提供している場合、 たとえEU域内に子会社などがなかったとしても、 当該企業は個人データの取得や処理に当たりGDPRに沿った手続を実施する必要があります。

* + - * 1. (3) EUから個人データの処理について委託を受けている企業

データセンター事業者やクラウドベンダーなどのように、 EU域内の企業から個人データの処理などを受託している日本企業の場合、 当該受託企業は処理者（Processor）として個人データの域外移転に関してGDPRが定めるルールに準拠する必要があります。

* + - 1. 2. 違反時のインパクト
         1. Ⅰ 2. で述べたように、 GDPRは適用対象となる企業に対しさまざまな義務を課すとともに、 違反した場合には多額の制裁金を課すことでルールの遵守を厳格に働きかけています（GDPR第83条）（＜表1＞参照）。
         2. 表1 制裁金と違反例

サブトピック  


最大で企業の全世界売上高（年間）の2%、 または1,000万ユーロのうちいずれか高いほう

個人データの取扱いに関し、 適切な技術的、 組織的安全管理対策を実施しなかった場合（そのような措置を取らない処理者に個人データの処理を委託する場合も含む）

個人データの処理に関する記録を残すことが義務付けられているにもかかわらず、 監督機関に対して適時に通知しなかった場合

個人データの侵害（情報漏えい）が発生したにもかかわらず、 監督機関に対し適時に通知しなかった場合

データ保護オフィサー（DPD）の選任が義務付けられているにもかかわらず、 任命していない場合

最大で企業の全世界売上高（年間）の4%、 または2,000万ユーロのうちいずれか高いほう

個人データの処理に関する原則、 適法な取扱い、 同意に関する条件およびセンシティブ情報の取扱いを遵守しなかった場合

個人データの域外移転に関するルールを遵守しなかった場合

監督機関からの命令に従わなかった場合

* + 1. Ⅲ GDPRへの対応に向けて
       1. 日本においても個人情報保護法が改正され、 2017年5月30日から全面施行となります。 しかし、 個人データを取扱う保護レベルとしては、 日本はいまだ欧州委員会による十分性の認定を受けるに至っていません。 このため、 日本企業が事業活動を積極的にグローバル展開していく中で、 個人データをEUとの間で円滑に流通させるためには、 各企業がGDPRに沿った対応について自主的に取り組む必要があります。
       2. GDPRの要求事項は多岐にわたるため、 企業は各条文の内容の理解にとどまらず自社の置かれている状況を適切に把握した上で、 次のような実務対応計画を慎重に進めていくことが望ましいと考えられます。
       3. 【準備フェーズ】
          1. 各拠点においてどのような個人データが存在し、 どのような経路で流通しているのかについて現状を調査する（データマッピング）。 その上でGDPR対応として必要な作業について担当部署、 作業ボリュームを把握することにより、 次フェーズに向けた全体計画およびスケジュールを決定する。
       4. 【対応フェーズ】
          1. 準備フェーズの計画に基づき、 GDPR対応として求められる個人データ保護の管理態勢（組織内の役割分担、 規程類の整備、 運用ルールの決定など）を構築し、 関係者に周知徹底する。
       5. 【運用フェーズ】
          1. 新たに制定した規程類、 ルールにのっとって適切に運用が行われているかどうかを評価し、 必要に応じて規程等の見直しまたは運用の改善を実施する。
       6. 以上を踏まえ、 企業は18年5月の適用開始に向けて、 限られた時間の中で効率的かつ速やかにGDPR対応を推進していくことが重要となってきます。