The CIS Critical Security Controls

for

Effective Cyber Defense

Version6.1

効果的なサイバー防御のための

CIS クリティカルセキュリティコントロール

Translated by NRI SecureTechnologies, Ltd.

The Center for Internet Security（CIS）
効果的なサイバー防御のための
CIS クリティカルセキュリティコントロール
バージョン 6.0
2015 年 10 月 15 日

The CIS Critical Security Controls for Effective Cyber Defense

イントロダクション

現在、いわゆるサイバー防御の発達段階において、私たちは非常に興味深い時期を迎えています。大規模なデータ損失、知的財産の盗用、クレジットカードの不正利用、個人情報の盗難、プライバシー侵害、サービス拒否などが、サイバースペースでは日常的な出来事になっています。

皮肉にも、防御する側として私たちが利用できるものは非常に多く、セキュリティツールやテクノロジー、セキュリティ標準、トレーニングや研修、認定資格、脆弱性データベース、ガイダンス、ベストプラクティス、セキュリティコントロールカタログ、無数のセキュリティチェックリスト、ベンチマーク、推奨事項や勧告に至るまで、膨大な数にのぼります。また、脅威への理解を助けるものとして、脅威情報フィード、レポート、ツール、警告サービス、規格、脅威共有フレームワークなどが登場しました。その上になお、セキュリティ要件、リスク管理フレームワーク、コンプライアンス体制、規定も存在します。セキュリティ担当者にとってみれば、インフラ保護のために必要な情報には事欠かないのです。

ところが、こうしたテクノロジーや情報、およびその管理は、文字通り「膨大な選択肢による混沌（Fog of More）」をもたらしています。オプションや優先事項、意見、要求が競合することで、企業は麻痺し、重要な活動が妨げられてしまうおそれがあります。ビジネスは複雑さの度合いを増し、依存度は拡大し、ユーザのモバイル化が進み、そして脅威は進化していきます。新しいテクノロジーは大きなメリットはもたらしますが、それは同時に、データやアプリケーションが様々な場所に分散されることを意味し、その多くは組織インフラの外に置かれることになります。このような複雑に相互接続した世界において、自社だけの問題としてセキュリティを検討できる企業などないのです。

では、私たちは、一般社会をはじめ、業界、企業体、あるいはパートナー関係や連合組織といったコミュニティとして、優先的活動の決定や相互サポートを目指して一致団結し、急速に変化する問題と、無数とも言えるその対応策に臨む必要がありますが、それにあたって持つべき知識やテクノロジーを最新に保ち続けていくには、一体どうしたらよいでしょうか。取り組むべき最も重要な領域とは何なのでしょうか。企業はリスク管理プログラムの充実に向けた第一歩をどう踏み出したらよいでしょうか。新たに起こる例外的脅威をすべて追跡するのでも、基本事項を怠るのでもなく、むしろ基本事項のロードマップに沿って、評価と改善の指針を得るにはどうしたらよいでしょうか。最も効果的な防御対策とはどのようなものでしょうか。

このような課題に対応することを目的とし、本 CIS CSC は開発され、現在推進されています。当初は「Fog of More」を切り開く草の根活動として始まりましたが、現在はあらゆる企業がとるべき最も基本的かつ重要な対応に重点を置いています。ここでの**価値**は、知識とデータによって決定されます。これはすなわち、現在企業を悩ます攻撃を防御し、警戒し、対処する能力を得ることにほかなりません。

CIS 主導の下、個人ユーザおよび団体の国際コミュニティによって、CIS CSC（以下、「コントロール」とする）は以下の趣旨で形作られてきました。

- 攻撃と攻撃者に関する知見を共有し、根本的原因を特定し、これらの情報から各種防御対策を策定する。
- 実施例をドキュメント化し、問題解決ツールを共有する。
- 脅威の進化、攻撃者の能力、不正侵入のトレンドを追跡する。
- 法規制フレームワークにコントロールを紐付け、全体的な優先事項を特定して集中的に取り組む。
- ツール、作業支援機能、翻訳を共有する。
- 共通課題（初期アセスメント、実装ロードマップの策定など）を特定し、個人や個々の組織

としてではなくコミュニティとして解決に取り組む。

こうした活動が、単なる対策案に留まらない、高度に的を絞り優先順位付けされた対策として、本コントロールを形成しています。コミュニティ全体からなるサポートネットワークがこのような活動を実施、利用、拡張可能なものとし、業界や政府のあらゆるセキュリティ要件に準拠しています。

The Center for Internet Security, Inc.(CIS)は、サイバーセキュリティにおけるベストプラクティスの特定、開発、評価、促進および維持、世界レベルのサイバーセキュリティソリューションの提供、サイバーインシデントの回避や有事の早期対応、さらに、サイバースペース上に信頼環境を実現するためのコミュニティ構築とその主導をミッションとする、501c3非営利組織です。

詳しくは、<http://www.cisecurity.org/>をご覧ください。

CIS CSC が効果的である理由：方法論と貢献者

CIS CSC は、実際に行われた攻撃や効果的な防御対策から情報を収集し、エコシステム上のあらゆる構成員（企業、政府機関、個人ユーザ）が所属する多くのセクター（政府、電力、防衛、金融、運輸、学術、コンサルティング、セキュリティ、IT）のあらゆる担当者（脅威への対応者やアナリスト、技術者、脆弱性診断者、ツール開発者、ソリューションプロバイダー、防御スタッフ、ユーザ、ポリシー策定者メーカー、監査者など）を交え、本コントロールを適用し運用することができるようにするべくとりまとめた知識が反映されています。こうした組織のトップ専門技術者は、実際のサイバー攻撃に対する防御経験から得られた幅広い知識を蓄積し、攻撃を防止または追跡する最良の防御テクニックをまとめた合意リストを作成します。これにより、本コントロールは、最もよく見られる攻撃から最も高度なサイバー攻撃に至るまで、さまざまな攻撃を検知、防止し、またこれに対応し、被害を軽減する上で最も効果的かつ具体的な技術対策をまとめたものとなっています。

これらのコントロールは、システムに対する初期のセキュリティ侵害をブロックするだけではなく、すでにセキュリティ侵害を受けているマシンの検知や、攻撃者によるさらなる活動の防止・阻止にも対応します。これらのコントロールで特定された防御対策は、デバイスの設定強化で初期の攻撃対象範囲を狭め、セキュリティ侵害を受けたマシンを特定することで組織ネットワーク内の長期的脅威に対処し、攻撃者によって埋め込まれた悪意あるコードによるコマンド＆コントロールを阻止し、維持や改善が可能で、適応性と継続性を備えた防御対応機能を確立します。

CIS CSC には、5 つの重要なサイバー防御システムが反映されています。それらの主な基本事項は次のとおりです。

攻撃から防御を学ぶ：システムを侵害した実際の攻撃に関する知識を活用することで、このような経験から継続的に学び、効果的かつ実用的な防御対策を構築するための基盤を提供します。既知の攻撃を阻止できる効果が明らかになっているコントロールだけを組み込みます。

優先順位化：最大のリスク低減効果と、最も危険な脅威要因に対する保護が得られ、かつ目的のコンピューティング環境に適切に実装できるコントロールに対して、最初に投資を行います。

メトリクス：必要な調整を迅速に特定、実装できるようにする目的で組織内でのセキュリティ対策の効果を測定するべく、経営幹部、IT 専門技術者、監査担当者、セキュリティ担当者すべてが、理解できる共通メトリクスを確立します。

継続的な診断とリスク低減：現在のセキュリティ対策の効果をテスト、検証し、次の段階での優先事項を推進するため、継続的な測定を実施します。

自動化：防御を自動化することで、組織のコントロールおよび関連するメトリクスに対する準拠度を、信頼性および拡張性の高い継続的な方法で測定できるようにします。

導入にあたり

CIS CSC は、組織が現在のセキュリティ状況を評価、改善するために取り入れることのできる比較的少数のアクションリストであり、優先順位付けがなされ、入念な検討を経てサポート体制が整えられています。また、「自社としては何をすべきか」から、より大規模なセキュリティ対策の強化を目指した「一人ひとりが何を行わなくてはならないか」へと課題を進化させています。

ただし、その内容においても優先度においても、単一のソリューションがあらゆる状況に対応できるというものではありません。各自のビジネス、データ、システム、ネットワーク、インフラストラクチャにとって不可欠な事項を理解し、事業や経営を成功に導く機能に影響を与えるかもしれない攻撃者の活動を考慮しなくてはなりません。比較的少数であっても、すべてのコントロールを 1 度に実施することはできないため、評価、実装、およびプロセス管理の計画を策定する必要があります。

セキュリティ対策を成功させるには、コントロール CSC1 から CSC5 までが不可欠であり、これらが最初に実施されるべきコントロールであるとお考えください。これらは「Foundation Cyber Hygiene」（基本サイバー予防策）と呼ばれ、攻撃から組織を守る強固な基盤を作るために実施しなければならない基本事項です。例えばこれは、CIS CSC パートナーの 1 つである米国国土安全保障省（DHS）の Continuous Diagnostic and Mitigation (CDM) Program（継続的診断およびリスク軽減プログラム）が取り入れている方法です。オーストラリア通信電子（ASD）のパートナーが策定した「Top Four Strategies to Mitigate Targeted Intrusions」（攻撃侵入を軽減するための 4 大戦略）[1]でも、同様の方法が提案されています。このドキュメントは、効果が実証され高い評価を得ているサイバー防御対策集であり、CIS CSC とも密接に対応しています。また、US CERT（米コンピュータ緊急レスポンスチーム）の内容とも調和しています。

上記内容を、低コストかつ利用しやすく分かりやすい形で活用できる、CIS の「National Cyber Hygiene Campaign」(Appendix D および www.cisecurity.org)もご検討ください。

CIS CSC の現バージョン

本コントロールは、脅威環境に関する具体的知識や、通信やデータの依存を受ける、市場に存在する現在の技術に基づいて開発されました。本コントロールの主なメリットの 1 つは、これらが不変のコントロールではないということです。本コントロールは定期的に更新また状況に応じて調整され、最新のセキュリティ課題に対応します。現バージョンには、すべてのコントロールおよびサブコントロールの精度、必要性、簡潔性、関連性を確保するための検討、考慮事項が反映されています。

バージョン 5.1 からバージョン 6.0 への改訂には、以下の内容が含まれます。

- 「管理者権限のコントロール下での使用」の優先度を上げ、章順を変更（コントロール 12 からコントロール 5 に移動）。
- コントロール 19：「安全なネットワークエンジニアリング」の削除。
- コントロール 7：「E メールと Web ブラウザの保護」の追加。
- コントロール「群」に基づく分類スキームの追加と「クイックウィン」カテゴリーの削除。

[1] http://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

- グループコントロールに以下の 3 つのカテゴリーを新規追加。
  - システム
  - ネットワーク
  - アプリケーション
- NIST の Cybersecurity Framework、National Hygiene Campaign for Cyber Hygiene およびセキュリティーガバナンスに関する Appendix の追加。

バージョン 6.0 からバージョン 6.1 への改訂には、以下の内容が含まれます。

- 優先順位付けやプランニングをする上での補完指標として、各サブコントロールに「Foundational」（基本的な対策となる項目かどうか）と「Advanced」（より高度なコントロールかどうか）を追記。
- いくつかの誤字、フォーマットエラーを修正。
- 各コントロール、サブコントロールの文言や順番は一切変更なし。

技術的内容に加え、コントロールの発行元と名称が変更されました。2015 年、CIS は The Council on Cybersecurity（サイバーセキュリティ協議会）と合併したため、現在は「CIS CSC」と呼ばれています。

他の参考文献

本コントロールの真の力は、最善の実施案リストを作ることではなく、優先順位付け、アイデアの共有および総体的アクションを通して、セキュリティ強化を行う個人ユーザおよび企業からなるコミュニティの経験を利用することにあります。

そのため CIS は、私たち全員がお互いから学ぶための媒体および情報センターとしての役割を果たしています。以下の参考文献やその他補足資料については、CIS までお問合せください。

- 本コントロールから正式なリスク管理フレームワーク（FISMA、ISO など）の幅広いバリエーションへの変換
- 企業での導入事例
- ベンダーのホワイトペーパーやその他本コントロールに対応している資料へのリンク
- NIST Cybersecurity Framework と整合する文献

本ドキュメントの構成

本ドキュメントの各コントロールの概要では、以下の要素を説明します。

- 攻撃の防御や攻撃の存在を特定する際のコントロールの重要性**（このコントロールが重要である理由）**と、このコントロールが実施されない状況が攻撃者によってどのように悪用されるかを説明します。
- 組織がこのコントロールを実装し、自動化し、その効果を測定するために行う具体的なアクション（「サブコントロール」）をリスト化して記載します。
- 実装と自動化を可能にする手順とツール。
- 実装構成要素を示すサンプルの**エンティティ関係図**。

本ドキュメントに加え、CIS が提供する「A Measurement Companion to the CIS Critical Security Controls」（CIS CSC に伴う対策）を強く推奨します。

謝辞

Center for Internet Security（CIS）は、本コントロール作成にあたり、無償で協力、貢献いただいた多くのセキュリティ専門家に対し、謝意を表します。本バージョンに協力してくださった多くの方々には、例年、その専門知識でお力添えをいただいています。時間をかけ、専門知識をご提供くださった方々に、心から感謝申し上げます。また、本作業に多大なご貢献をいただいた SANS Institute には、特に御礼を申し上げるものです。

CSC1: 許可されたデバイスと無許可のデバイスのインベントリ

ネットワーク上のすべてのハードウェアデバイスを能動的に管理（イベントリ作成、追跡、修正）し、アクセス権限を許可されたデバイスだけに付与します。また、無許可のデバイスや管理されていないデバイスを検出し、これらのデバイスがアクセス権限を取得することを防止します。

このコントロールが重要である理由

世界中に潜んでいる攻撃者は、標的とした組織のアドレススペースを継続的にスキャンし、新規システムや保護されていないシステムがネットワークに接続されるのを待ち構えています。そして、企業ネットワークに接続したり切断したりを繰り返しながら、パッチやセキュリティが最新版に更新されていないデバイス（特にラップトップ）を探し出します。ある日の夜にネットワーク上にインストールされ、翌日まで未設定のまま適切なセキュリティ更新パッチが適用されずにいるハードウェアは、攻撃に利用されてしまうことがあります。内部アクセスをすでに取得していれば、攻撃者はインターネットからは見えないデバイスをも利用して、内部のジャンプポイントや標的を物色します。攻撃者のアクセスによって企業業務のセキュリティが影響を受けることを防ぐためには、企業ネットワークに接続する追加システム（デモシステム、一時的テストシステム、ゲストネットワークなど）は慎重に管理されるか、あるいは隔離されなければなりません。

従業員が職場に個人所有のデバイスを持ち込んでネットワークに接続する、いわゆる BYOD（bring your own device：私的デバイスの活用）は、新しい技術が登場するにつれてごく普通の光景になっていきます。こうした個人デバイスはすでにセキュリティを侵害されているおそれがあり、内部リソースを感染させることに利用されてしまう可能性があります。

すべてのデバイスを管理コントロールすることは、システムのバックアップと復旧を計画、実施する上で重要な役割を果たすのです。

CSC1: 許可されたデバイスと無許可のデバイスのインベントリ				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**1.1**	自動化された資産インベントリ検出ツールを適用し、これを使用して組織のパブリックネットワークおよびプライベートネットワークに接続されたシステムの予備の資産インベントリを作成します。IPｖ4 または IPｖ6 のネットワークアドレス範囲をスキャンするアクティブツールおよびトラフィックの分析に基づいてホストを特定するパッシブツールの両方を採用する必要があります。	**Y**	継続モニタリングプログラムの一部として、アクティブツールとパッシブツールを複合的に使用する。
System	**1.2**	DHCP を使用して動的にアドレスを割りあてている場合は、システムに対して動的ホスト構成プロトコル(DHCP)サーバのロギング機能を適用して資産インベントリを改善し、このDHCP情報から不明なシステムを検知します。	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	1.3	機器の取得に伴ってインベントリシステムが新規に更新され、承認されたデバイスがネットワークに接続されることを確認します。	Y	
System	1.4	少なくともネットワークアドレス、マシン名、各システムの目的、および各デバイスの責任を負う資産所有者、各デバイスに関連付けられた部門を記録して、ネットワークに接続されたすべてのシステムおよびネットワークデバイス自体の資産インベントリを保守します。このインベントリには、デスクトップ、ラップトップ、サーバ、ネットワーク機器（ルータ、スイッチ、ファイアウォールなど）、プリンタ、ストレージエリアネットワーク、VoIP（Voice over IP）電話、マルチホームアドレス、仮想アドレスなど、ネットワーク上に IP（Internet Protocol）アドレスを持つすべてのシステムが含まれている必要があります。作成する資産インベントリには、デバイスがポータブルデバイス／パーソナルデバイスであるかどうかに関するデータも含める必要があります。携帯電話、タブレット、ラップトップなど、データの保管または処理が可能なポータブル電子機器は、組織のネットワークに接続しているかどうかに関係なく特定する必要があります。	Y	
System	1.5	ネットワークに接続できるデバイスを制限しコントロールするために、802.1x によるネットワークレベル認証を適用します。許可されているシステムと無許可のシステムを判別するために、802.1x をインベントリデータに結びつける必要があります。	Y	認証メカニズムは、ハードウェアインベントリ管理と密接に紐づく。
System	1.6	プライベートネットワークへの接続前に、クライアント証明書を使用してシステムを検証および認証します。		Y

CSC1 手順およびツール

このコントロールには、ライフサイクル全体を通じてハードウェアのインベントリおよびすべての関連情報を管理し把握するプロセスと符合した、技術面と手順面での活動が求められます。これは、情報、ソフトウェア、ハードウェアを含むビジネスプロセスの各コンポーネントについて、情報や資産の管理責任者を置くことによるビジネスガバナンスにもつながります。大規模で包括的な企業向け製品を利用して IT 資産インベントリを保守する組織もあります。あるいは、適切なツールでネットワークを走査してデータを収集し、結果をデータベースで独立管理している企業もあります。

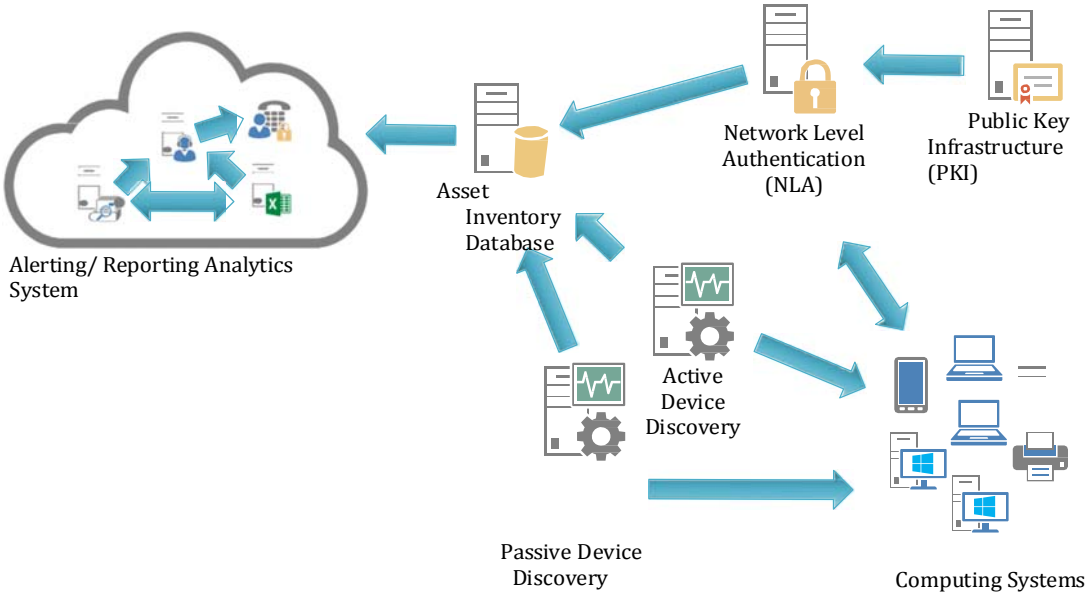
正確な最新の IT 資産情報を維持するということは、プロセスが常に動いているということです。組織は、定期的にアクティブスキャンを実施し、ネットワーク接続デバイスを識別するさまざまなパケットタイプを送信できます。こうしたスキャンを行うならば、ネットワークのロード履歴と容量を確認して定期スキャンを行うのに適切な帯域幅があることを、あらかじめ検証しなければなりません。インベントリスキャンを実施するに当たっては、スキャンツールが従来の ping パケット（ICMP エコー要求）を送信し、特定 IP アドレスのシステムを識別することを目的として ping 応答を待つことがあります。一部のシステムは、従来の ping に加えインバウンド ping パケットをブロックするため、スキャナは伝送コントロールプロトコル（TCP）の同期（SYN）または確認（ACK）パケットを利用して、ネットワーク上のデバイスを特定することもできます。スキャナによっては、ネットワーク上にあるデバイスの IP アドレスを特定したうえで、強固なフィンガープリント機能を使って検出されたマシンのオペレーティングシステムタイプを判別します。

ネットワークを走査するアクティブスキャンツールに加え、ある種の資産識別ツールは、ネットワークインタフェース上で受動待機して、デバイスがトラフィックを送出するとその存在を感知します。このようなパッシブツールは、ネットワーク内の重要な場所にあるスイッチスパンポートに接続でき、スイッチを通過するすべてのデータを表示します。そのため、これらのスイッチを経由して通信するシステムを特定できるチャンスを最大限に得ることができます。

また多くの組織は、スイッチやルータなどのネットワーク資産から、ネットワークに接続されたマシンに関する情報を取得します。ツールは安全に認証され暗号化されたネットワーク管理プロトコルを使用して、ネットワークデバイスから MAC アドレスなどの情報を取得できます。それらデバイスは、組織のサーバ、ワークステーション、ラップトップ、およびその他デバイスの資産インベントリに紐づいています。MAC アドレスを確認したら、適切に構成されている認証システムだけをネットワークに接続できるよう、スイッチには 802.1x と NAC を実装する必要があります。

ワイヤレスデバイス（および有線のラップトップ）は、定期的にネットワークに接続したり切断したりするので、現在利用可能なシステムのインベントリは常に変動します。同様に仮想マシンは、シャットダウンや一時停止時に資産インベントリで追跡することが困難になることがあります。さらに、仮想プライベートネットワーク（VPN）技術を使ってネットワークにアクセスするリモートマシンは、ネットワークに一時的に接続してから、切断することがあります。IP アドレスを使用する各マシンは、物理マシンであっても仮想マシンであっても、組織の資産インベントリに登録されなくてはなりません。

CSC1 システムエンティティ関係図



CSC2: 許可されたソフトウェアと無許可のソフトウェアのインベントリ

ネットワーク上のすべてのソフトウェアを能動的に管理（イベントリ作成、追跡、修正）し、許可されたソフトウェアだけをインストールし、実行可能とします。無許可のソフトウェアや管理されていないソフトウェアを検出し、不正なソフトウェアのインストールと実行を防止します。

このコントロールが重要である理由

攻撃者は標的とした組織を継続的にスキャンし、リモートから悪用可能な脆弱性を抱えるバージョンのソフトウェアを探します。また、一部の攻撃者は、悪意のある Web ページ、文書ファイル、メディアファイル、およびその他のコンテンツを自身の Web ページや信頼できるサードパーティーサイトから配布します。疑いを持たない被害者が脆弱なブラウザやその他のクライアント側プログラムを使用してこのコンテンツにアクセスすると、攻撃者は被害者のマシンを侵害し、長期にわたってシステムのコントロールを可能にするバックドアプログラムやボットをインストールします。一部の巧妙な攻撃者は、ゼロデイエクスプロイトを利用することがあります。ソフトウェアベンダーからはパッチがまだリリースされていない、存在が公になる前の脆弱性が利用されるのです。組織に適用されているソフトウェアを適切に把握あるいは管理していない状態では、資産を適切に保護することなどできません。

こうした管理が不十分なマシンは、業務に必要のないソフトウェアを実行しているか（潜在的なセキュリティ上の不具合を招く）、あるいはシステムのセキュリティが侵害された後で攻撃者によって導入されたマルウェアを実行している可能性が高いのです。1 台のマシンが悪用されてしまうと、そのマシンは攻撃者の足がかりとなり、侵害されたシステムとそこに接続する他のシステムからも機密情報が収集されるという例が多く見られます。さらに侵害されたマシンは、攻撃者がネットワークおよびその連携ネットワーク全体を移動するための拠点としても利用されます。このように攻撃者は、たった 1 台のマシンを起点として急速に多くのマシンを侵害することがあります。完全なソフトウェアインベントリを持たない組織は、脆弱なソフトウェアやマルウェアを実行しているシステムを見つけることができず、問題の軽減や、攻撃者の一掃に取り組むことができません。

すべてのソフトウェアを管理コントロールすることは、システムのバックアップと復旧を計画、実施する上で重要な役割を果たすのです。

CSC2: 許可されたソフトウェアと無許可のソフトウェアのインベントリ				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**2.1**	さまざまな種類と用途のサーバ、ワークステーション、ラップトップを含む各タイプのシステムについて、企業内で許可されているソフトウェアと各種のシステムで必要とされているバージョンのリストを考案します。このリストは、許可されているソフトウェアが変更されていないかどうかを検証するファイル完全性チェックツールでモニタする必要があります。	**Y**	ファイルの完全性は、継続モニタリングプログラムの一部として、検証される。

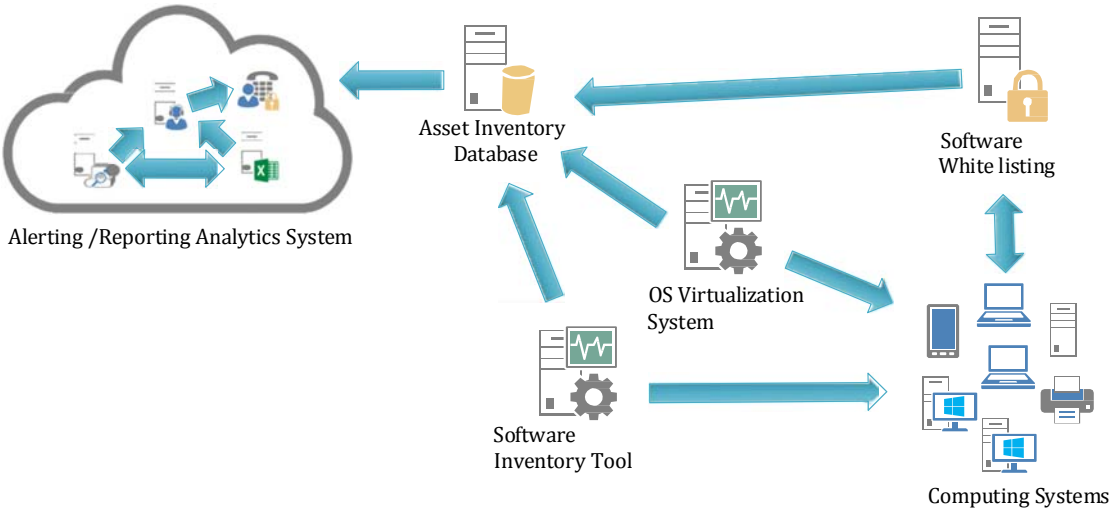
Family	CSC	Control Description	Foun-dational	Advanced
System	2.2	アプリケーションのホワイトリストテクノロジーを適用します。ホワイトリストテクノロジーでは、システムに対してホワイトリストに登録されているソフトウェアのみの実行を許可し、その他すべてのソフトウェアの実行を防止します。ホワイトリストは（ホワイトリストベンダーから入手可能であり）非常に広範囲に及ぶ場合もありますが、一般的なソフトウェアを使用している場面で不便と感じることはありません。一部の専用システム（必要なビジネス機能に要するプログラムがごく少数であるシステム）では、ホワイトリストが限定的な場合もあります。	Y	（EXE や MSI のような）実行バイナリに、（DLL のような）ホワイトリストアプリケーションライブラリを追加する。
System	2.3	サーバ、ワークステーション、ラップトップを含む、使用中の各オペレーティングシステムタイプに対応したソフトウェアインベントリツールを組織全体に適用します。ソフトウェアインベントリシステムは、オペレーティングシステムおよびオペレーティングシステム上にインストールされたアプリケーションのバージョンを追跡する必要があります。すべてのデバイスとそれに関連するソフトウェアとを一元的に追跡できるよう、ソフトウェアインベントリを各関連ハードウェア資産インベントリに紐付けます。	Y	ハードウェアとソフトウェアインベントリ管理は、密接に紐づき、集中的に運用される。
System	2.4	仮想マシンやネットワークから隔離されたシステムを使用して、必要であるがリスクが高く、ネットワーク接続された環境内にインストールすべきではないアプリケーションを分離して実行する必要があります。		Y

CSC2 手順およびツール

市販のホワイトリストツール、ポリシーまたはアンチウイルススイートや Windows に付属のアプリケーション実行ツールを組み合わせることで、ホワイトリスト機能を実装できます。市販のソフトウェアと資産インベントリツールは一般に入手可能で、現在、多くの企業で利用されています。これらツールの最も優れたものには、企業で利用される数百もの一般アプリケーションのインベントリチェックが用意されています。インストールされている各プログラムについてパッチレベルで情報を取得することによって最新バージョンであることを確認し、共通プラットフォーム一覧仕様に見られるような標準アプリケーション名を活用します。

ホワイトリストを実装している機能は、現在多くのエンドポイントセキュリティスイートに組み込まれています。また、市販のソリューションでは、アプリケーションのホワイトリストとブラックリストとともに、アンチウイルス、アンチスパイウェア、パーソナルファイアウォール、およびホストベースの侵入検知システム（IDS）と侵入防御システム（IPS）をバンドルする傾向が高まっています。特に、ほとんどのエンドポイントセキュリティソリューションは、特定の実行可能ファイル名、ファイルシステムの場所、暗号化ハッシュを調べ、保護されたマシンでアプリケーションの実行を許可するかどうかを決定できます。これらの中で最も有効なツールは、実行可能ファイルのパス、ハッシュ、または正規表現マッチングに基づいたカスタムホワイトリストを提供します。一部には、特定ユーザが特定時刻に特定プログラムのみを実行するための規則を管理者が定義できるようにするグレイリスト機能も組み込まれています。

CSC2 システムエンティティ関係図



CSC3: モバイルデバイス、ラップトップ、ワークステーションおよびサーバに関するハードウェアおよびソフトウェアのセキュアな設定

攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な設定管理および変更管理プロセスを使用して、ラップトップ、サーバ、およびワークステーションのセキュリティ設定を確立、実装し、能動的に管理（追跡、報告、修正）します。

このコントロールが重要である理由

メーカーやリセラーから納品された時点でのオペレーティングシステムやアプリケーションのデフォルト設定は、通常導入のしやすさや使いやすさに配慮されており、セキュリティが考慮されていません。基本的なコントロール、空いているサービスおよびポート、デフォルトアカウントやパスワード、古い（脆弱な）プロトコル、プリインストールされている不要なソフトウェアなどはすべて、デフォルト状態では悪用される可能性があります。

適切なセキュリティプロパティで構成設定を開発することは、個人ユーザの能力の域を超えた複雑な作業であり、適切な判断には何百万通りもの分析が必要になる可能性があります（以下の手順およびツールのセクションにセキュアな設定に関する参考リソースが記載されています）。ソフトウェアの更新やパッチの適用、新たなセキュリティ脆弱性の出現、あるいは、新規ソフトウェアのインストールや新しい運用要件への対応に合わせて設定を「調整」するなど、こうした機会に伴ってセキュリティが「低下」することを避けるためには、強力な初期設定が施されインストールされていたとしても、継続的な設定管理を行う必要があります。このように管理を行わなければ、ネットワークにアクセス可能なサービスとクライアントソフトウェアの両方を悪用する機会を攻撃者に与えてしまうことになります。

CSC3: ハードウェアおよびソフトウェアのセキュアな設定				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**3.1**	ご使用のオペレーティングシステムおよびソフトウェアアプリケーションの標準的なセキュア設定を確立し、この設定を使用します。標準イメージは、基盤となるオペレーティングシステムと、システムにインストールされているアプリケーションを強化したものである必要があります。これらのイメージは、定期的に検証して更新し、最近の脆弱性と攻撃経路の観点からセキュリティ設定を更新する必要があります。	**Y**	
System	**3.2**	厳密な設定管理に従い、組織に適用されているすべての新規システムを構築するために使用されるセキュアなイメージをビルドします。セキュリティを侵害された既存のシステムには、セキュアなビルドでイメージを再適用する必要があります。このイメージに対する定期的な更新または例外を、組織の変更管理プロセスに統合する必要があります。組織で使用するワークステーション、サーバ、およびその他のシステムタイプすべてに対してイメージを作成する必要があります。	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	3.3	安全に設定されたサーバにマスターイメージを格納する必要があります。継続的に検証を実行できる完全性チェックツールと変更管理を使用して、イメージに対して許可された変更のみを行うようにします。あるいは、これらのマスターイメージを本番ネットワークから隔離したオフラインのイメージストレージサーバに格納し、本番ネットワーク上で使用する際はセキュアなメディアでオフラインマシンからコピーしたコピーイメージを使用します。	Y	マスターイメージのファイルの完全性は、継続モニタリングプログラムの一部として検証される。
System	3.4	サーバ、ワークステーション、ネットワークデバイス、および類似した機器のリモート管理はすべて、セキュアなチャネルを介して行います。TELNET、VNC、RDP などのプロトコルや、強力な暗号化をアクティブにサポートしないその他のプロトコルは、SSL、TLS や IPSEC などの二次暗号化チャネルを介して実行する場合のみ使用します。	Y	
System	3.5	ファイル完全性チェックツールを使用して、重要なシステムファイル（機密システムとアプリケーション実行可能ファイル、ライブラリ、および構成を含む）が変更されていないことを確認します。レポートシステムは定期的な変更および予期される変更を報告し、通常とは異なる変更または予期しない変更を強調して示し、アラートを生成する必要があります。また、レポートシステムは時系列に設定変更の履歴を表示し、変更を実行したユーザ(su コマンドや sudo コマンドを使用してユーザ ID が切り替えられた場合は、元のログインアカウントを含む)を示すことができる必要があります。この完全性チェックは、疑わしいシステム変更（ファイルまたはディレクトリの所有者または許可の変更、悪意ある活動を隠すために使用される可能性がある代替データストリームの使用など）を特定し、重要なシステム領域へのファイルの追加（これは、攻撃者が残した悪意あるペイロードや、バッチ配布プロセスで不適切に追加されたファイルを示す可能性があります）を検出する必要があります。	Y	重要なシステムファイルのファイル完全性は、継続モニタリングプログラムの一部として検証される。
System	3.6	リモートテストで測定できるすべてのセキュアな設定要素を確認し、無許可の変更が行われた場合にアラートを出す自動化設定モニタシステムを実装し、テストを行います。これには、新たな待機ポート、新たな管理者ユーザ、グループやローカルポリシーオブジェクトの変更（該当する場合）、システムで実行中の新たなサービスの検出も含まれます。レポート作成や脆弱性等の統合管理の効率化を図るために、Security Content Automation Protocol(SCAP) に準拠したツールを可能な限り常に使用します。	Y	
System	3.7	スケジュールされた定期的な間隔でシステムに対し構成設定を自動的に実施、再適用するシステム設定管理ツール（Microsoft Windows システムの Active Directory グループポリシーオブジェクト、UNIX システムの Puppet など）を適用します。これらのツールは、スケジュール、手動操作、またはイベントドリブンで構成設定の再適用をトリガーできる必要があります。	Y	

CSC3 手順およびツール

組織は、各ソフトウェアシステムのセキュリティベースラインを新規開発するのではなく、公式に開発されたセキュリティベンチマーク、セキュリティガイド、チェックリストなどを入念に吟味し、サポートが受けられるものを使って開発する必要があります。優れた参考リソースを以下に示します。

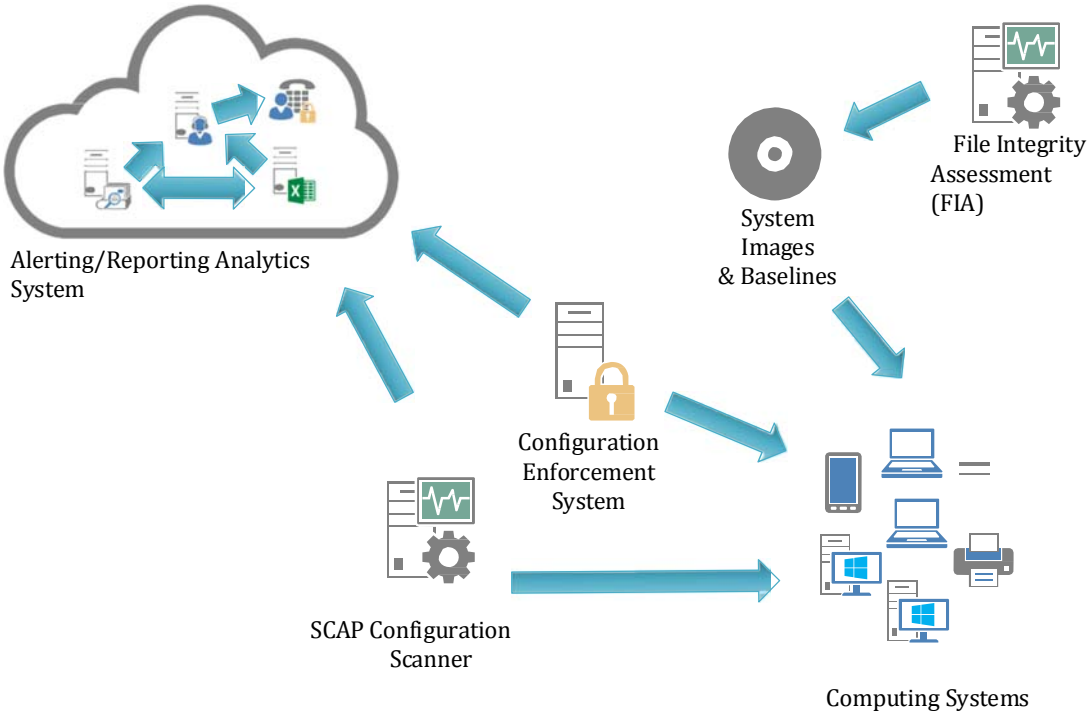
- TheCenterforInternetSecurityBenchmarksProgram(www.cisecurity.org)
- TheNISTNationalChecklistProgram(checklists.nist.gov)

こうしたベースラインは、ローカルポリシーやローカル要件に合わせて拡大あるいは調整が必要になります。ただし追って実施される審査や監査に向けて、逸脱とその根拠は文書に記録しておかなくてはなりません。

構成が複雑な企業では、1 つのセキュリティベースライン設定（企業全体のすべてのワークステーションを対象とした 1 つのインストールイメージなど）を確立することが現実的ではないか、または受け入れ難いことが起こりがちです。予定している適用（DMZ への Web サーバの導入と、内部ネットワークへの電子メールサーバまたはその他のアプリケーションサーバの導入など）に伴うリスクや必要とされる機能に対応するため、適切な強化に基づいて異なる標準イメージをサポートする必要が生じることがあります。各標準イメージのセキュリティプロパティをより適切に理解、管理するためには、使用する標準イメージの数を最小限に抑えてください。ただしこの場合、組織は複数のベースラインを管理できる体制を整えている必要があります。

市販あるいは無償の設定管理ツールを採用して、管理対象マシンのオペレーティングシステムやアプリケーションの設定を測定し、標準イメージ設定からの逸脱を特定することができます。一般的な設定管理ツールは、各被管理システムにインストールされたエージェントを組み合わせるか、または管理者認証情報で各被管理マシンにリモートログインすることでエージェントなしのシステムチェックをしています。また、リモートセッションを開始し、一時エージェントまたはダイナミックエージェントをターゲットシステムに展開してスキャンし、その後エージェントを削除するというハイブリッド方式が採用されることもあります。

CSC3 システムエンティティ関係図



CSC4: 継続的な脆弱性診断および修復

継続的に新たな情報を取得、評価し、この情報に基づいて措置を講じることで、脆弱性を特定して修復し、攻撃チャンスを最小限に抑えます。

このコントロールが重要である理由

サイバー防御担当者は、新しい情報（ソフトウェア更新、パッチ、セキュリティ勧告、脅威の報告など）が絶え間なく流入する状況で活動しなければなりません。脆弱性を理解し管理することは継続して行わなければならない活動であり、長い時間と高い注意力、そして多大なリソースを必要とします。

攻撃者も同じ情報を入手できるため、新しい情報が得られてから修正が行われるまでにできる隙を突かれてしまうことがあります。例えば、研究者が新たな脆弱性を報告すると、攻撃者（「武器化」、攻撃の開始、脆弱性を突く）、ベンダー（パッチまたはシグネチャおよびアップデートの開発と公開）、および防御者（リスク評価、パッチの修正確認テスト、インストール）といったすべての当事者が競争を始めます。

脆弱性をスキャンして発見された不具合にあらかじめ手を打たなければ、組織はコンピュータシステムが侵害を受ける高い可能性にさらされてしまうことになります。防御者は、修復の規模を組織全体に拡大し、競合する優先事項と突き合わせて対応を優先付けする際に、特有の課題に直面し、場合によっては思わぬ副次的影響が発生することがあります。

CSC4: 継続的な脆弱性診断および修復				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**4.1**	ネットワーク上のすべてのシステムに対し、毎週またはこれよりも高い頻度で自動化された脆弱性スキャンツールを実行します。最も重要な脆弱性の優先リストと、システム管理者と各部門がリスクを削減する際の効果を比較したリスクスコアを、各担当システム管理者に配付します。SCAP により検証済みの脆弱性スキャナを使用します。このスキャナは、コードベースの脆弱性（Common Vulnerabilities and Exposures（共通脆弱性識別子）の項目で説明されている脆弱性など）と、構成ベースの脆弱性（Common Configuration Enumeration（共通セキュリティ設定一覧）プロジェクトにより列挙されている脆弱性）の両方を検出します。	**Y**	脆弱性リスクスコアは、集中的に計測され、管理されるとともに、アクションプランに取り込みます。
System	**4.2**	イベントログを脆弱性スキャンの情報と関連付けます。これには 2 つの目標があります。最初に、担当者は、通常の脆弱性スキャンツール自体のアクティビティが記録されていることを確認する必要があります。次に、担当者は、攻撃検知イベントを前述の脆弱性スキャン結果と関連付けて、特定のエクスプロイトが既知の脆弱な標的に対して使用されたかどうかを判別する必要があります。	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	4.3	セキュリティ構成を分析するために各エンドシステムでローカルに実行されているエージェントを使用するか、テストするシステムで管理権限を付与されているリモートスキャナを使用して、脆弱性スキャンを認証モードで実行します。認証済みの脆弱性スキャン専用のアカウントを使用します。このアカウントは、その他の管理作業には使用してはならず、また特定の IP アドレスで特定のマシンに関連付ける必要があります。承認されている従業員のみが脆弱性管理ユーザインターフェイスにアクセスできるようにし、役割が各ユーザに適用されるようにします。	Y	
System	4.4	発生しつつあるリスクを常に認識できるようにするため、脆弱性情報提供サービスに登録し、このサービスから得られる情報を使用して組織の脆弱性スキャンアクティビティを最低限でも毎月更新します。あるいは、使用する脆弱性スキャンツールを、関連するすべての重要なセキュリティ脆弱性に対応できるよう定期的に更新します。	Y	
System	4.5	オペレーティングシステムやソフトウェア／アプリケーションの自動化パッチ管理ツールとソフトウェア更新ツールを、このツールを使用でき安全であるすべてのシステムに適用します。パッチは、適切に隔離されたシステムを含むすべてのシステムに適用する必要があります。	Y	
System	4.6	スキャンアクティビティに関連するログと関連付けられている管理者アカウントをモニタし、すべてのスキャンアクティビティと、権限付きアカウントを介した関連アクセスが、正当なスキャンの時間枠でのみ実行されていることを確認します。	Y	
System	4.7	バックツーバック脆弱性スキャンの結果を比較して、パッチを適用するか、補正コントロールを実装するか、適度なビジネスリスクを文書化して受容するかによって、脆弱性が対処されたことを確認する必要があります。このような既存の脆弱性に関するビジネスリスクの受容は、定期的に見直しを行い、新たな補正コントロールまたは後続のパッチが以前に受容した脆弱性に対処できるかどうか、または状況が変化しリスクが高まったかどうかを判別する必要があります。	Y	
System	4.8	脆弱性の悪用可能性と潜在的な影響に基づいて脆弱性のリスクを評価するプロセスを確立し、適切な資産グループ（DMZ サーバ、内部ネットワークサーバ、デスクトップ、ラップトップなど）に基づいて分割します。最初に、最もリスクの高い脆弱性にパッチを適用します。組織への影響を最小限に抑えるには、段階的なロールアウトが適用でき、リスク評価レベルに基づいてパッチ適用予定を策定します。		

CSC4 手順およびツール

システムのセキュリティ設定評価には、多くの脆弱性スキャンツールが利用可能です。リモート側で管理されるスキャンアプリケーションを利用した商用サービスが有効だと認識済みの企業もあるでしょう。組織の複数部門、場合によっては組織全体にわたって発見された脆弱性の定義を標準化するのに役立つよう、セキュリティの不具合を測定し、業界で認知されている 1 つ以上の脆弱性、設定、およびプラットフォーム分類スキームや言語（CVE、CCE、OVAL、CPE、CVSS、XCCDF）を使用してカテゴリー化された脆弱性と問題にその不具合をマップする、脆弱性スキャンツールの利用をお勧めします。

ログイン認証情報なしで実行可能なスキャンより、スキャンシステムにユーザ認証情報を使ってログインし設定を行えるツールの方が、より包括的なスキャンを実行することができます。また、組織のシステムが多様化するとともに各ベンダーのパッチサイクルも変動することになるので、スキャンアクティビティの頻度も合わせて増やさなくてはなりません。

脆弱性と誤設定をネットワーク全体にわたって検査するスキャンツールに加え、さまざまな無償・有償ツールでも、インストールされているローカルマシンのセキュリティ構成と設定を評価することができます。こうしたツールは、許可されていない設定変更や、管理者がうっかり入れ込んでしまったセキュリティの脆弱性を詳細に把握するのに役立ちます。

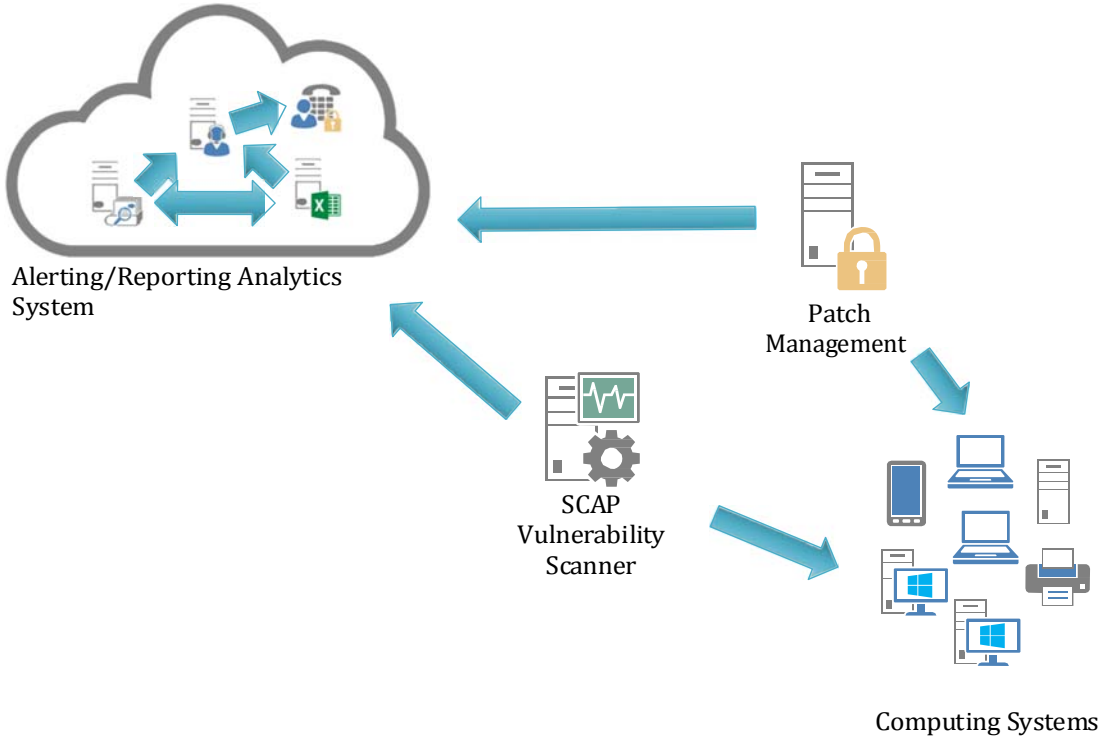
効率的な組織であれば、脆弱性スキャナを課題管理チケット発行システムにリンクさせ、問題の修正状況を自動的にモニタして報告し、低減されていない重大な脆弱性をより高位の管理職レベルに対して可視化し、問題が確実に解決されるようにします。

最も効果的な脆弱性スキャンツールは、新旧のスキャン結果を比較し、時間経過とともに環境内の脆弱性がどのように変化したかを判別します。セキュリティ担当者は、これらの機能を利用して、毎月脆弱性の傾向分析を実施します。

スキャンツールがパッチ未適用のシステムの脆弱性を見つけ出したら、セキュリティ担当者は、システムのパッチ公開から、脆弱性スキャンの実行までに要した時間を測定し、文書化する必要があります。この時間枠が、組織が設定した特定パッチの適用におけるベンチマークの限界を超えている場合、セキュリティ担当者は遅延を記録し、システムとそのパッチについての逸脱が公式に文書化されていたかどうかを見極める必要があります。文書化されていなかった場合、セキュリティチームは経営層と協力して、パッチ適用プロセスを改善する必要があります。

さらに、一部の自動パッチ適用ツールは、ベンダーまたは管理者によるエラーが原因で、特定のパッチを検知またはインストールしないことがあります。このために、すべてのパッチチェックは、Web サイトで各ベンダーが発表したパッチリストとシステムパッチ間で一致させる必要があります。

CSC4 システムエンティティ関係図



CSC5: 管理権限のコントロールされた使用

コンピュータ、ネットワーク、アプリケーションの管理権限の使用、割り当て、設定を追跡／管理／防止／修正するためのプロセスとツールです。

このコントロールが重要である理由

管理権限の誤使用は、攻撃者が標的とする企業内に侵入するための主たる手段となります。極めてよく使われる 2 つの攻撃テクニックがあり、これらはコントロールされていない管理権限を利用します。まず 1 つ目は、権限ユーザとして実行しているワークステーションユーザを騙し、悪意のある電子メールの添付ファイルを開かせるか、悪意のある Web サイトからファイルをダウンロードさせ開かせるか、または自動的にブラウザを悪用する攻撃者コンテンツをホストしている Web サイトにアクセスさせるという手口です。ファイルまたはエクスプロイトには実行可能コードが含まれており、このコードは被害者のマシンで自動的に実行されるか、攻撃者のコンテンツを実行するようユーザを騙すことによって実行されます。被害者のユーザアカウントに管理権限が付与されている場合、攻撃者は、被害者のマシンを完全にコントロールし、キーストロークロガー、スニファー、およびリモートコントロールソフトウェアをインストールして、管理者パスワードとその他の機密データを見つけ出すことができます。類似の攻撃は電子メールで行われます。管理者がうっかり感染した添付ファイルを含む電子メールを開くことで、他のシステムを攻撃するために使用されるネットワーク内の起点を得るという手口がこれにあたります。

攻撃者が使用する 2 つ目の一般的テクニックは、管理ユーザのパスワードの推測またはクラッキングによって権限を昇格させ、ターゲットマシンへのアクセスを取得します。管理権限が厳密ではなく広く分散されている場合、または重要性の低いシステムで使用されているパスワードと同一なら、攻撃者はより容易にシステムを完全にコントロールすることができます。攻撃者が管理権限を侵害するための手段として利用できるアカウントがより多く存在するためです。

CSC5: 管理権限のコントロールされた使用				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	5.1	管理権限を最小限に抑え、必要な場合にのみ管理アカウントを使用します。管理者権限の使用に焦点を当てて監査を行い、異常な動作をモニタします。	Y	
System	5.2	自動化ツールを使用して、すべての管理アカウントのインベントリを作成し、デスクトップ、ラップトップ、およびサーバで管理権限を持つ各ユーザが上級管理者によって承認されていることを確認します。	Y	
System	5.3	ネットワーク接続された環境内に新規のデバイスを適用する前に、アプリケーション、オペレーティングシステム、ルータ、ファイアウォール、無線アクセスポイント、およびその他のシステムのデフォルトで設定されているパスワードをすべて、管理者レベルのアカウントに対応した値に変更する必要があります。	Y	

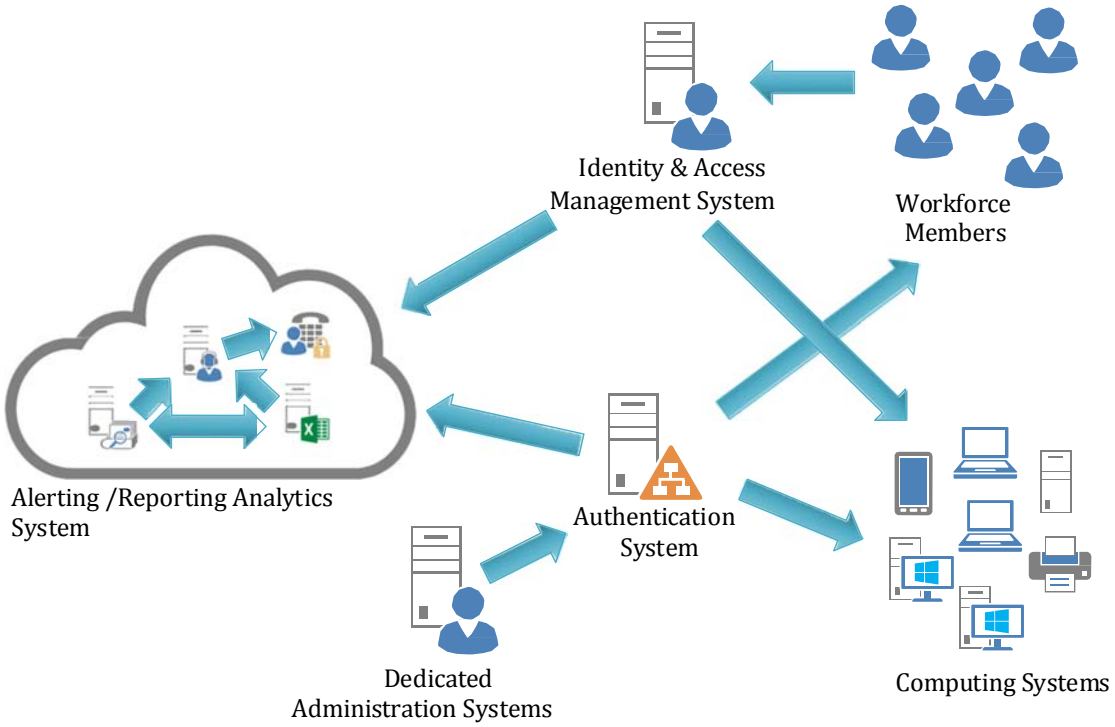
Family	CSC	Control Description	Foun-dational	Advanced
System	5.4	ドメイン管理者グループにアカウントが追加または削除されたとき、または新しいローカル管理者アカウントがシステムに追加されたときに、ログエントリを発行してアラートを送信するようシステムを構成します。	Y	
System	5.5	管理者アカウントへのログインが失敗したときに、ログエントリを発行してアラートを送信するようシステムを構成します。	Y	
System	5.6	すべての管理アクセス（ドメイン管理アクセスを含む）に対して多要素認証を使用します。多要素認証にはさまざまな手法（証明書付きスマートカードの使用、1 回限りのパスワード（OTP）、トークン、生体認証など）が使用できます。	Y	
System	5.7	多要素認証を使用していない場合、ユーザアカウントには長いパスワードを使用します(14 文字以上)。	Y	
System	5.8	管理者に対し、システムにアクセスするときには完全にログに記録される非管理者アカウントを使用することを義務付けます。その後、管理者は管理権限なしでマシンにログオンしてから、Linux／UNIX では sudo、Windows では RunAs、およびその他のシステムでは類似した他の機能などのツールを使用して管理権限に移行する必要があります。	Y	
System	5.9	管理者は、すべての管理者タスクや昇格タスクをする際には専用のマシンを使用します。専用マシンは組織の主要なネットワークからは隔離され、インターネットアクセスを許可しないようにします。また、専用マシンは電子メールを読んだり、文書を作成したり、インターネットで情報を閲覧したりといった用途には使用されないようにします。		Y

CSC5 手順およびツール

組み込みオペレーティングシステム機能は、個々のシステムでローカルまたドメインコントローラ全体の両方で、スーパーユーザ権限を持つアカウントのリストを抽出できます。高権限アカウントを持つユーザが、日常的な Web や電子メールの閲覧にそのアカウントを使用していないことを確認するには、セキュリティ担当者が実行されているプロセスのリストを定期的に収集し、Web ブラウザまたは電子メールブラウザが高権限で実行されているかどうかを判別する必要があります。そのような情報収集は、高権限ユーザがマシンで実行している何十にも及ぶ Web ブラウザや電子メールブラウザ、文書編集プログラムを検索できるよう、短いシェルスクリプトを使ってスクリプト化することができます。一部の正当なシステム管理活動において、短期間ならこうしたプログラムの実行が必要になることがありますが、管理権限で長期間または頻繁に使用している場合は、管理者がこのコントロールに準拠していないことを示している可能性があります。

強固なパスワード要件を施行するに、最小のパスワード長を組み込みオペレーティングシステムの機能で設定し、ユーザが短いパスワードを選択することを防ぎます。複雑なパスワードを強制する（パスワードを偽似乱数の文字列にするよう義務付ける）には、組み込みオペレーティングシステムで設定するか、あるいはパスワードの複雑さを義務付けるサードパーティーツールを適用しても構いません。

CSC5 システムエンティティ関係図



CSC6: 監査ログの保守、監視および分析

イベント監査ログを収集、管理、分析します。これは、攻撃を検知、理解し、攻撃からの被害を復旧する上で役立ちます。

このコントロールが重要である理由

セキュリティロギングと分析が欠如していると、攻撃者の所在や悪意のあるソフトウェア、マシンが受けた被害痕跡の隠ぺいを許してしまいます。システムが侵害されたことを被害者が認識した場合でも、保護された完全なロギングレコードがなければ、攻撃の詳細やそれに続く攻撃者の行動を知ることができません。しっかりとした監査ログがなければ、いつまでも攻撃に気づくことができず、受けたダメージを修復することさえできないかもしれません。

時としてロギングレコードが、攻撃を証明する唯一の証拠にもなります。多くの組織は、コンプライアンス目的で監査記録をとります。しかし、こうした組織は監査ログをめったに確認せず、システム侵害を認識していないという事実が、攻撃者に利用されてしまいます。未検査のログファイルに攻撃の証拠が記録されていたとしても、ログ分析プロセスが不完全であったり、プロセス自体が存在しなければ、攻撃者の存在は標的組織内で誰にも知られることないため、数ヶ月あるいは数年にもわたって被害者のマシンがコントロールされてしまいます。

CSC6: 監査ログの保守、監視および分析				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**6.1**	ログ内のタイムスタンプが整合するように、すべてのサーバとネットワーク機器が定期的に時刻情報を取得する同期化された時刻ソースを、少なくとも 2 つ組み込みます。	**Y**	
System	**6.2**	各ハードウェアデバイスと、インストールされているソフトウェアの監査ログ設定を検証して、ログに日付、タイムスタンプ、ソースアドレス、宛先アドレス、および各パケットやトランザクションのさまざまなその他の有用な要素が含まれていることを確認します。システムでは、syslog エントリなどの標準化された形式や、Common Event Expression イニシアチブによって概略されている形式でログを記録する必要があります。システムが標準化された形式でログを生成できない場合は、ログを標準化された形式に変換するためにログ正規化ツールを適用できます。	**Y**	
System	**6.3**	ログを格納するすべてのシステムに、生成されるログに十分なストレージスペースがあることを定期的に確認して、ログ循環間隔の間にログファイルがいっぱいにならないようにします。ログは、定期的にアーカイブしてデジタル署名を付す必要があります。	**Y**	
System	**6.4**	セキュリティ担当者やシステム管理者が、ログにおける異常を特定する隔週のレポートを作成します。その後、異常を積極的に確認して、判明した内容を文書化する必要があります。	**Y**	

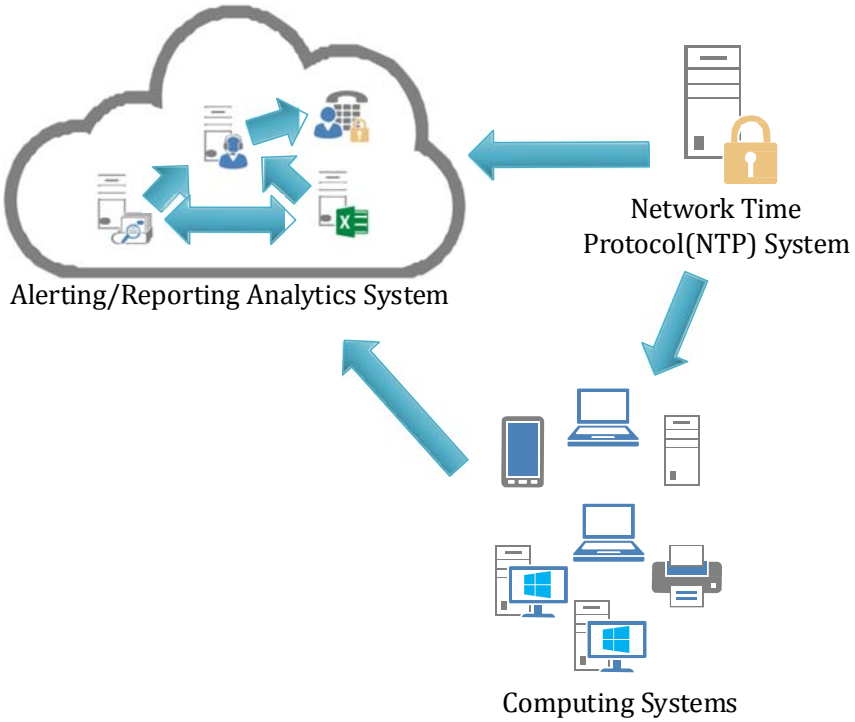
Family	CSC	Control Description	Foun-dational	Advanced
System	6.5	ファイアウォール、ネットワークベースの IPS、インバウンドおよびアウトバウンドプロキシなどのネットワーク境界デバイスが、それらに到着するすべてのトラフィック（許可されるトラフィックとブロックされるトラフィックの両方）を詳細に記録するよう構成します。	Y	
System	6.6	複数のマシンからのログの集約と統合、およびログの関連付けと分析のために、SIEM（Security Incident and Event Management）ツールまたはログ分析ツールを適用します。システム管理者とセキュリティ担当者は、SIEM ツールを使用して特定のシステムから共通するイベントのプロファイルを抽出できるようにする必要があります。これにより、異常なアクティビティに焦点を当てて、誤検知を防止し、より迅速に異常を特定して、意味のないアラートによる膨大な分析を回避するように検知を調整することができます。	Y	

CSC6 手順およびツール

無償または商用のオペレーティングシステム、ネットワークサービス、およびファイアウォールテクノロジーのほとんどには、ロギング機能が備わっています。こうしたロギングを実行して、ログを集中型ロギングサーバに送信する必要があります。ファイアウォール、プロキシ、およびリモートアクセスシステム（VPN、ダイヤルアップなど）はすべて詳細ロギング用に設定し、追加調査が必要な場合にロギングで得られるすべての情報を保存しておかなくてはなりません。さらに、ユーザが適切な権限を持たないリソースにアクセスしようとしたときにアクセスコントロールログを作成できるよう、オペレーティングシステム（特定にサーバのオペレーティングシステム）を設定する必要があります。こうしたロギングが実施されているかどうかを評価するには、ログを定期的にスキャンして、CSC1 で作成した資産インベントリと比較し、ネットワークにアクティブに接続されている各管理対象項目が定期的にログを生成していることを確認しなければなりません。

ログの確認を目的とした SIM/SEM ソリューションなどの分析プログラムは有益ですが、監査ログを分析するために採用されている機能は、個人による大まかな検査を含め、非常に詳細にわたります。続いて行われる手作業の検査における監査ログの有用性は、実際の相関ツールのおかげです。こうしたツールは巧妙な攻撃の特定に役立つことがあります。ただし、これらのツールは、熟練した情報セキュリティ担当者とシステム管理者の代用となる万能薬ではありません。自動化されたログ分析ツールを使用したとしても、攻撃を特定して理解するためには、時として人間の専門知識と直感が必要になります。

CSC6 システムエンティティ関係図



CSC7: 電子メールと Web ブラウザの保護

攻撃者が Web ブラウザや電子メールシステム利用者の行動を操作して行う攻撃の対象範囲や機会を最小限に抑えます。

このコントロールが重要である理由

Web ブラウザや電子メールクライアントは、技術的な複雑性や柔軟性が高く、ユーザや他のシステムおよび Web サイトと直接的なやり取りがあることから、侵入や攻撃の入口として非常によく使われます。ユーザを惑わし欺くコンテンツを作ってリスクを大幅に高める行動を取らせ、悪意のあるコードの注入や重要データの漏えい、その他の攻撃を可能にします。

CSC7: 電子メールと Web ブラウザの保護				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**7.1**	完全にサポートされている Web ブラウザと電子メールクライアントのみ組織内で実行可能であることを確認します。最新のセキュリティ機能と修正を使うために、ベンダーから提供される最新のブラウザのみ使用するのが理想的です。	**Y**	
System	**7.2**	必要のない、あるいは許可されていないブラウザや電子メールクライアントのプラグインもしくはアドオンアプリケーションをアンインストールするか無効にします。各プラグインはアプリケーションと URL のホワイトリストを使用し、事前承認されたドメインのアプリケーションの使用のみ許可します。	**Y**	
System	**7.3**	すべての Web ブラウザと電子メールクライアントにおいて不必要なスクリプト言語の使用を制限します。例としては、ActiveX や JavaScript 等をサポートする必要のないシステム上での言語の使用を指します。	**Y**	
System	**7.4**	悪意のある可能性のあるアクティビティの特定をしたり、インシデントハンドラーが侵害されている可能性のあるシステムを特定するのを補助するために、オンサイト・モバイルデバイス問わず、組織の各システムからのすべての URL リクエストのログを取得します。	**Y**	モバイルデバイスを含みます。
System	**7.5**	各システムに 2 つの別個のブラウザ設定を適用します。1 つの設定はすべてのプラグインや不必要なスクリプト言語の使用を無効にし、機能を制限して一般的な Web サイトの閲覧のみに使用されます。もう 1 つの設定は特定の Web サイトへアクセスするために必要な機能のみの設定を許可します。	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
System	7.6	組織から承認されていない Web サイトへの接続を制限するネットワークベースの URL フィルタを維持・適用します。URL フィルタが最新の Web サイトカテゴリ定義に更新されるように URL カテゴライズサービスに登録します。分類されていない Web サイトはデフォルト設定でブロックします。このフィルタリングは、仮想的であろうとなかろうと各システムに適用します。	Y	
System	7.7	電子メールメッセージがスプーフされる可能性を減らすためには、Sender Policy Framework（SPF）を実装します。SPF レコードを DNS に適用することで、メールサーバで受信者側の検証を有効にすることができます。	Y	
System	7.8	組織の電子メールゲートウェイに到着するすべての電子メールの添付ファイルをスキャンし、悪意のあるコードや、ビジネスにとって不要なファイルタイプを含む電子メールをブロックします。このスキャンは、電子メールがユーザの受信箱に入る前に行う必要があります。このフィルタには、電子メールのコンテンツフィルタと We コンテンツフィルタが含まれます。	Y	

CSC7 手順およびツール

Web ブラウザ

今日の Web ブラウザの多くは、基本的なセキュリティ機能を備えていますが、セキュリティの一面だけに頼るのは適切ではありません。Web サーバはレイヤー群で構成されており、複数の角度から攻撃される可能性があります。あらゆる Web ブラウザの基盤となるのはオペレーティングシステムであり、そのセキュリティ確保の秘訣は至って単純です。つまり、最新のセキュリティパッチで更新し続けるのです。古いパッチを実行しているサーバは被害に遭うため、最新のパッチが適切にインストールされている状況を確保してください。

Web サーバで実行するすべてのソフトウェアコンポーネントを更新してください。DNS サーバや VNC のようなリモート管理ツール、あるいはリモートデスクトップといった必須ではないものは、すべて無効にするか削除するべきです。リモート管理ツールが必須である場合は、デフォルトのパスワードや簡単に推測できるパスワードの使用は避けてください。これは、リモートアクセスツールだけでなく、ユーザアカウント、スイッチおよびルータにもいえることです。

フレキシブルなファイアウォールの設置は、セキュリティ侵害に対する最強の防御策の 1 つです。Web サーバが攻撃の対象になると、脆弱性が修復される前にその弱点を突くべく、攻撃者は即座にハッキングツールまたはマルウェアのアップロードを試みます。適切なアンチウイルスパッケージがなければ、長期にわたってセキュリティ侵害が見つからないことも考えられます。

サイバー犯罪者は悪意を持ってクッキーを不正利用することができます。第三者のクッキーをブロックするようにブラウザの設定を変更することで、このリスクを軽減させることができます。オートコンプリートやオートフィル機能は、最近入力した情報を保持するため、キーボード入力の手間が軽減されます。しかし、ログインでオートコンプリートを利用していると、ラップトップの紛失や盗難時に大きなリスクが生じてしまいます。また、アドオンを極限まで最少に制限することで、攻撃の可能範囲を狭めます。アドオンはマルウェアの隠れ蓑となるため、ブラウザに対する攻撃の機会が増大

してしまうのです。プロンプトなしでアドオンをインストールしないようにブラウザを設定してください。

普及度の高いブラウザは、フィッシングやマルウェアサイトのデータベースを利用して、最もよく見られる脅威に対抗しています。必ずコンテンツフィルタを有効にしてください。また、ポップアップブロッカーを有効にしてください。ポップアップは目障りというだけでなく、埋め込みマルウェアを直接ホストしたり、あるいはソーシャルエンジニアリングの技法でユーザを欺いて何かをクリックさせてしまいます。お使いのブラウザでは、必ずポップアップブロックを有効にしてください。

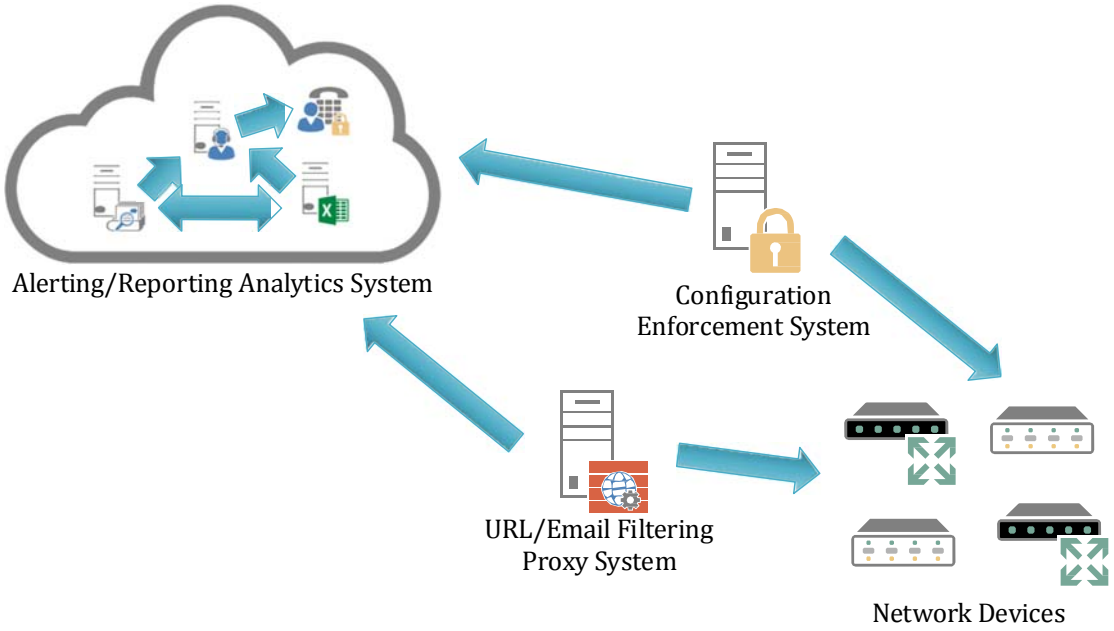
電子メール

電子メールは、人がコンピュータを使って行う中で最も双方向性の高い作業の 1 つであり、適切な行動を推奨することが技術的な設定に劣らず重要になります。

一般な用語やフレーズが含まれるパスワードは簡単に破られます。複雑なパスワードを確実に作成してください。文字、数字、特殊文字を組み合わせれば、十分に複雑なパスワードになります。パスワードは、45～60 日ごとに定期的に変更するべきです。

二要素認証は、ユーザが本物であることを保証し、攻撃範囲を狭めるもう 1 つの方法です。スパムフィルタリングツールを利用すれば、お使いのネットワークに入ってくる悪意のあるメールを大幅に減らすことができます。メール送信元のドメインが本物であることを確認する Sender Policy Framework を利用すれば、スパムやフィッシング行為の減少につながります。暗号化ツールをインストールして電子メールや通信を保護することで、ユーザやネットワークベースのセキュリティレイヤーをさらに増やすことができます。

CSC7 システムエンティティ関係図



CSC8: マルウェア対策

企業内の複数ポイントで悪意のあるコードのインストール、感染拡大、実行をコントロールし、自動化機能を活用して迅速な防御対策の更新、データ収集、修正を可能にします。

このコントロールが重要である理由

マルウェアは、システム、デバイス、データを攻撃することを目的として作成されたソフトウェアのことを指し、インターネットを利用する上で避けて通るこのとのできない脅威です。すばやく移動と変化を繰り返し、エンドユーザのデバイス、電子メールの添付ファイル、Web ページ、クラウドサービス、ユーザによる操作、リムーバブルメディアなど、さまざまなポイントから侵入します。最近のマルウェアは、防御対策を回避したり、防御対策そのものを攻撃あるいは無効にしたりすることもあります。

マルウェアの防御対策は、こうしたダイナミックな環境において、大規模な自動化、迅速な更新、そしてインシデント対応のようなプロセスとの統合を通じて機能するようにしなければなりません。マルウェアの移動を検知して止めるか、マルウェアの実行をコントロールするため、攻撃点となる可能性がある複数のポイントにマルウェア防御対策を適用する必要があります。エンタープライズエンドポイントセキュリティスイートは、すべての管理対象システムにおいて、すべての防御対策がアクティブであり、最新であることを確認できる管理機能を備えています。

CSC8: マルウェア対策				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**8.1**	自動化ツールを利用して、アンチウイルス、アンチスパイウェア、パーソナルファイアウォール、およびホストベースの IPS 機能のあるワークステーション、サーバ、およびモバイルデバイスを継続的にモニタします。すべてのマルウェア検知イベントを、企業のアンチマルウェア管理ツールとイベントログサーバに送信する必要があります。	**Y**	
System	**8.2**	ファイルのレピュテーションに関する情報を蓄積する集中型インフラストラクチャを提供するアンチマルウェアソフト（レピュテーション機能を所持するアンチマルウェアソフト）、もしくは管理者からすべてのマシンに対して手動でシグネチャの更新が実施できるアンチマルウェアソフトを採用します。アンチマルウェアソフトのシグネチャを更新適用した後に、自動化されたシステムは、各システムがシグネチャを更新したことを確認する必要があります。	**Y**	
System	**8.3**	外部デバイスの利用を、承認され文書化された業務要件に限定します。外部デバイスの使用と、使用しようとした操作をモニタします。USB トークン（サムドライブ）や USB ハードドライブ、CD／DVD、FireWire デバイス、外部のシリアル拡張テクノロジー接続デバイス、マウントによるネットワーク共有などの取り外し可能なメディアから、コンテンツが自動実行されないように、ラップトップ、ワークステーション、サーバを設定します。取り外し可能なメディアの挿入時に、そのメディアに対してアンチマルウェアスキャンを自動的に実行するようにシステムを構成します。	**Y**	（ロギングに加えて）外部デバイスの使用を能動的にモニタします。

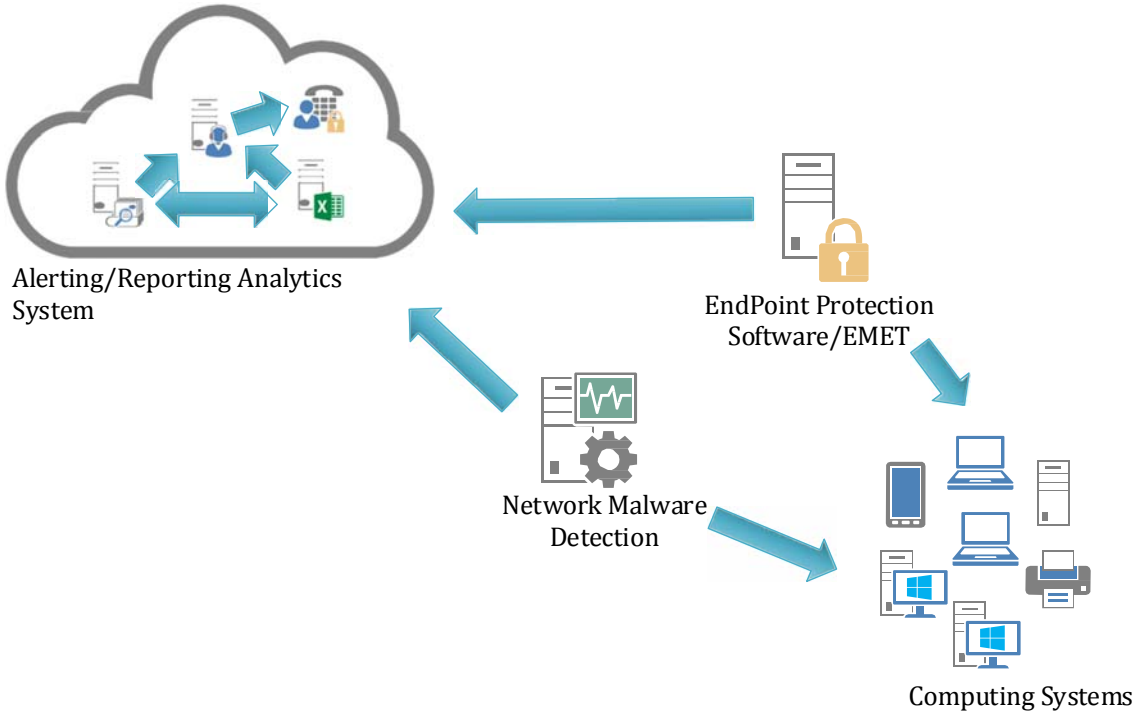
Family	CSC	Control Description	Foun-dational	Advanced
System	8.4	データ実行防止（DEP）、アドレス空間配置のランダム化（ASLR）,仮想化/コンテナ化などの悪用防止機能を有効にします。保護強化のため、さまざまなアプリケーションや実行ファイルに保護を適用するように構成できる Enhanced Mitigation Experience Toolkit （EMET）などの機能を適用します。	Y	
System	8.5	ネットワークベースのアンチマルウェアツールを使用して、すべてのネットワークトラフィックで実行可能ファイルを特定し、シグネチャベースの検知以外の技術を使用して、悪意のあるコンテンツがエンドポイントに到着する前に、このようなコンテンツを特定して除外します。		Y
System	8.6	既知の悪意のある C2 ドメインを検索するホストを検知するために、ドメインネームシステム（DNS）クエリのロギングを有効にします。	Y	

CSC8 手順およびツール

組織は自動化機能を利用して、常に最新のアンチウイルスシグネチャを維持します。エンタープライズエンドポイントセキュリティスイートに組み込まれている管理機能を使用して、アンチウイルス、アンチスパイウェア、およびホストベースの IDS 機能がすべての管理対象システムでアクティブになっていることを確認します。組織は自動化されたアセスメントを毎日実行して結果を確認し、上記のような保護が有効になっていないシステム、および最新のマルウェア定義がないシステムを見つけ、リスクを低減します。

無償または商用のハニーポットと tarpit ツールを適用して、環境内の攻撃者を特定している企業もあります。セキュリティ担当者は、ハニーポットと tarpit を継続的にモニタし、トラフィックがこれらのツールに送信されているかどうか、またアカウントのログインが試行されているかどうかを判別します。こうしたイベントを検出した場合、セキュリティ担当者はその後の追加調査に向け、このトラフィックを発生させたソースアドレスと、攻撃に関連するその他の詳細を収集しなければなりません。

CSC8 システムエンティティ関係図



CSC9: ネットワークポート、プロトコル、およびサービスの制限およびコントロール

攻撃者に対して脆弱性が利用可能である期間を最小限に抑えるため、ネットワーク接続デバイスのポート、プロトコルおよびサービスの継続的な運用を管理（追跡／コントロール／修正）します。

このコントロールが重要である理由

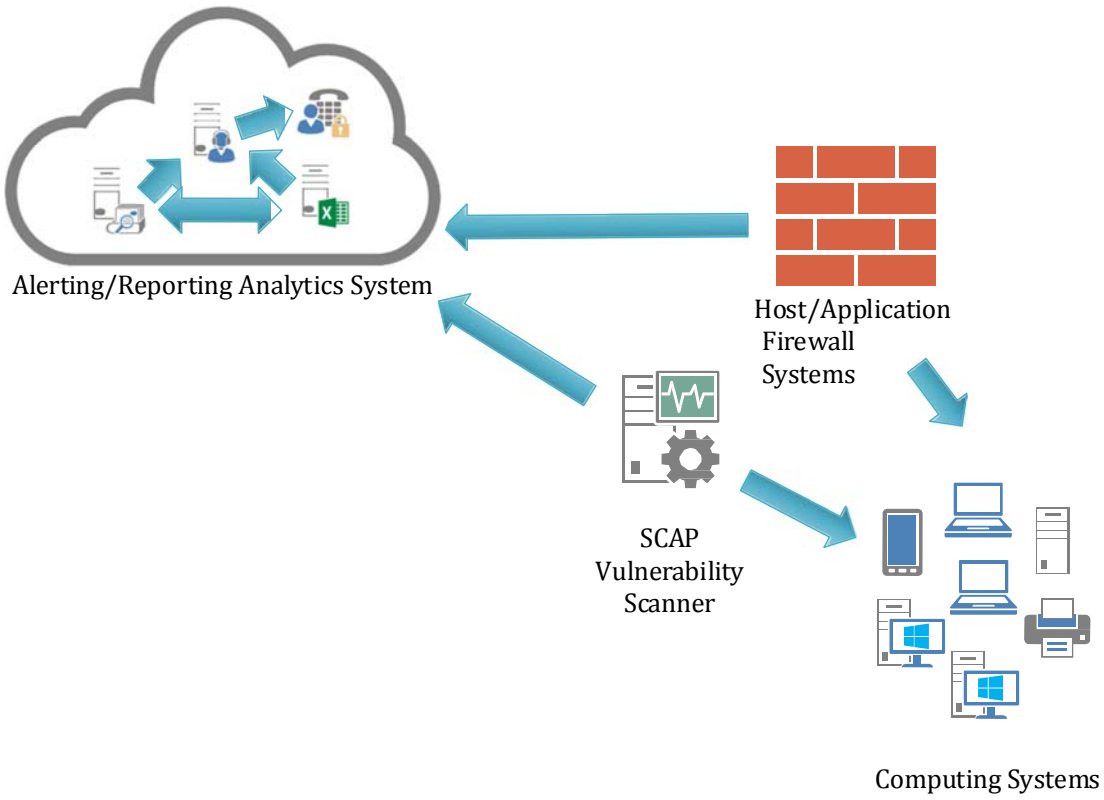
攻撃者は、リモートからアクセス可能で、攻撃に弱いネットワークサービスを探します。よく見られる例には、設定が不完全な Web サーバ、メールサーバ、ファイル・プリントサービス、特定のサービスに対するビジネスニーズもなくさまざまなデバイスにデフォルトでインストールされるドメインネームシステム（DNS）サーバがあります。多くのソフトウェアパッケージでは、メインソフトウェアパッケージのインストール時に、各サービスが自動的にインストールされ、有効にされますが、サービスが有効になっていることがユーザや管理者に通知されません。攻撃者は、こうした問題点を洗い出し、サービスの悪用を試みます。多くの場合はデフォルトのユーザ ID とパスワード、もしくは広く普及しているエクスプロイトコードを試行します。

CSC9: ネットワークポートの制限およびコントロール				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**9.1**	検証済みの業務要件に対応したポート、プロトコル、サービスのみが各システムで稼働していることを確認します。	**Y**	
System	**9.2**	明示的に許可されるサービスとポートを除くすべてのトラフィックをドロップするデフォルトの拒否ルールを使用して、ホストベースのファイアウォールまたはポートフィルタツールをエンドシステムに適用します。	**Y**	
System	**9.3**	すべての重要なサーバに対して自動化されたポートスキャンを定期的に実行して、既知の有効なベースラインと比較します。組織の承認済みベースラインにリストされていない変更が検出された場合には、アラートが生成され、レビューされる必要があります。	**Y**	
System	**9.4**	インターネットまたは信頼できないネットワークから可視できるサーバをすべて確認して、業務目的で必要ない場合は、内部 VLAN に移動して、プライベートアドレスを指定します。	**Y**	
System	**9.5**	DNS、ファイル、メール、Web、およびデータベースサーバなどの重要なサービスは、別個の物理ホストマシンまたは論理ホストマシンで操作します。		**Y**
System	**9.6**	サーバに送信されるトラフィックを確認・検証するために、アプリケーションファイアウォールを重要なサーバの前に設置します。無許可のサービスまたはトラフィックをブロックして、アラートを生成する必要があります。		**Y**

CSC9 手順およびツール

ポートスキャンツールを使用して、一連の対象システムにおいてどのサービスがネットワーク上で稼働しているかを判別します。優れているポートスキャナは、開いているポートを判別することに加えて、そのポートで稼働するサービスとプロトコルのバージョンを特定するように設定できます。サービスとそのバージョンのリストは、資産管理システム内のサーバとワークステーションごとに、組織で必要なサービスのインベントリと突き合わせて比較されます。最近これらのポートスキャナに追加された機能としては、前回のスキャン以降にネットワーク上のスキャン済みマシンで行われたサービスの変更を判別して、セキュリティ担当者が時間経過による相違を特定できるようにするものもあります。

CSC9 システムエンティティ関係図



CSC10: データ復旧能力

本プロセスとツールは、重要情報を適切にバックアップするとともに、実証済みの手法でタイムリーに情報を復旧します。

このコントロールが重要である理由

攻撃者がマシンを侵害する場合、その多くは設定とソフトウェアに大きな変更が加えられます。侵害されたマシンに格納されているデータに対してわずかな手を加え、汚染情報で組織の有効性を脅かす攻撃者も存在します。信頼できるデータ復旧能力を持たない組織にとって、マシンに加えられたすべての影響を取り除くことは、攻撃者を発見できたとしても非常に困難になってしまう可能性があります。

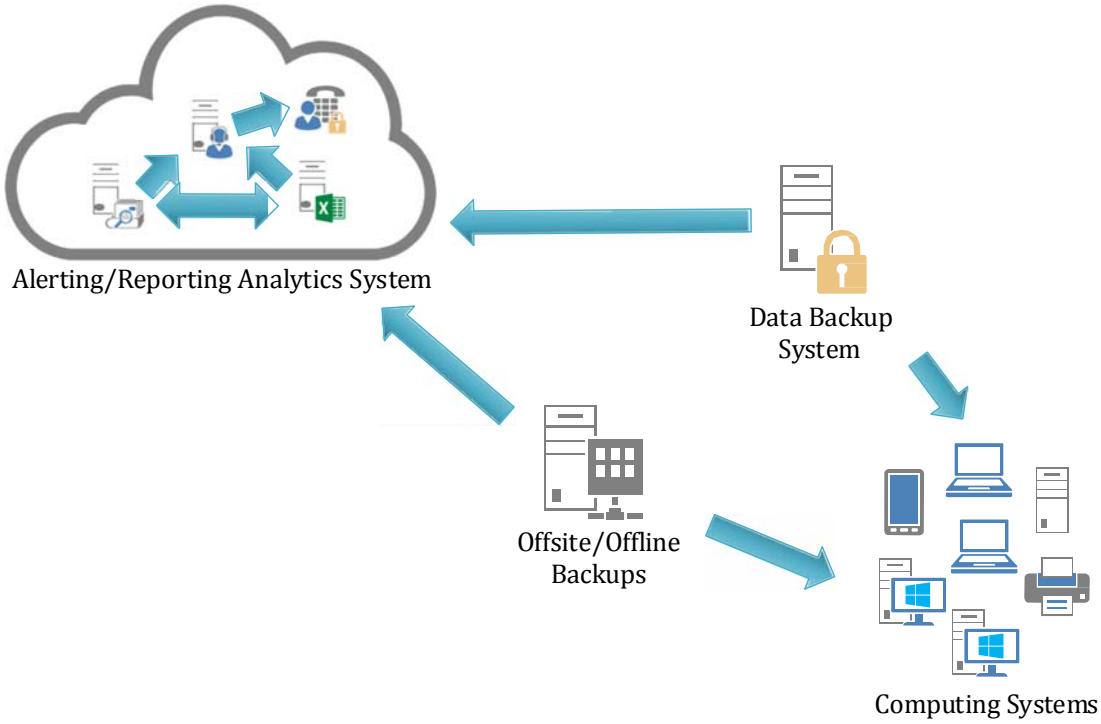
CSC10: データ復旧能力				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
System	**10.1**	各システムが少なくとも毎週自動的にバックアップされること、および機密情報が格納されているシステムではバックアップがより頻繁に実行されることを確認します。システムをバックアップから迅速に復元できるようにするには、マシンのオペレーティングシステム、アプリケーションソフトウェア、およびデータを、全体的なバックアップ手順に含める必要があります。システムのこれら 3 つのコンポーネントは、同じバックアップファイルに含めたり、同じバックアップソフトウェアを使用したりする必要はありません。常に複数のバックアップが存在している必要があります。これにより、マルウェアに感染した場合に、感染以前に存在した元のバージョンから復旧できます。すべてのバックアップポリシーは、規制上のまたは行政機関の要件に準拠している必要があります。	**Y**	
System	**10.2**	バックアップが正しく動作することを確認するため、データ復旧プロセスを実行してバックアップメディアのデータをテストする作業を定期的に実行する必要があります。	**Y**	
System	**10.3**	バックアップの保管時、およびバックアップをネットワーク上で移動するときに、物理セキュリティまたは暗号化によってバックアップが正しく保護されるようにします。これには、リモートバックアップやクラウドサービスなどが含まれます。	**Y**	
System	**10.4**	主要システムには少なくとも 1 つのバックアップ先があり、このバックアップ先がオペレーティングシステム呼び出しによって継続的にアドレス指定可能ではないことを確認します。これにより、アドレス指定可能なすべてのデータ共有（バックアップ先を含む）のデータを暗号化または損傷させる CryptoLocker などのような攻撃のリスクが低減します。	**Y**	

CSC10 手順およびツール

テストチームは四半期に 1 度（あるいは、新規バックアップ機器の購入時は必ず）、テストベッド環境でシステムバックアップの復元を試行することで、無作為にバックアップサンプルを評価しておくべきです。復元されたシステムを検査し、バックアップからのオペレーティングシステム、アプリケーション、およびデータがすべて完全で機能していることを確認する必要があります。

マルウェアに感染してしまったら、復元プロセスでは、感染前のバックアップバージョンを使用しなければなりません。

CSC10 システムエンティティ関係図



CSC11: ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定

攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な設定管理および変更管理プロセスを適用してネットワークインフラの機器設定を確立、実装し、能動的に管理（追跡、報告、修正）します。

このコントロールが重要である理由

メーカーやリセラーから納品された時点でのネットワークインフラ機器のデフォルト設定は通常、導入のしやすさや使いやすさに配慮されており、セキュリティが考慮されていません。起動しているサービスや空いているポート、デフォルトのアカウント名（サービスで利用するアカウントを含む）、デフォルトパスワード、古い（脆弱な）プロトコルのサポート、あらかじめインストールされている不要なソフトウェアなどは、すべてデフォルトの状態では悪用される可能性があります。

特定の業務にユーザが必要とするからという理由で例外を設けてしまうと、ネットワークデバイスは設定上の安全性が徐々に低下し、攻撃者に付け込まれてしまいます。時として、例外は適用されてから不要になり、そのまま放置されることがあります。また、例外を設けるセキュリティリスクが、関連する業務要件に照らし合わせて正しく分析されず、測定されない場合もあり、このようなリスクは時間の経過に伴ってその安全性が変化することもあります。攻撃者は、脆弱なデフォルト設定や、ファイアウォール、ルータ、スイッチのセキュリティホールを探し、防御を突破して侵入するために悪用します。脆弱性を悪用してネットワークに侵入し、ネットワークのトラフィックをリダイレクトし、送信中の情報を傍受します。その結果、攻撃者は機密データへのアクセス権を取得し、重要な情報を改ざんし、場合によっては侵害した 1 台のマシンを使用してネットワーク上の信頼できる別のシステムを装います。

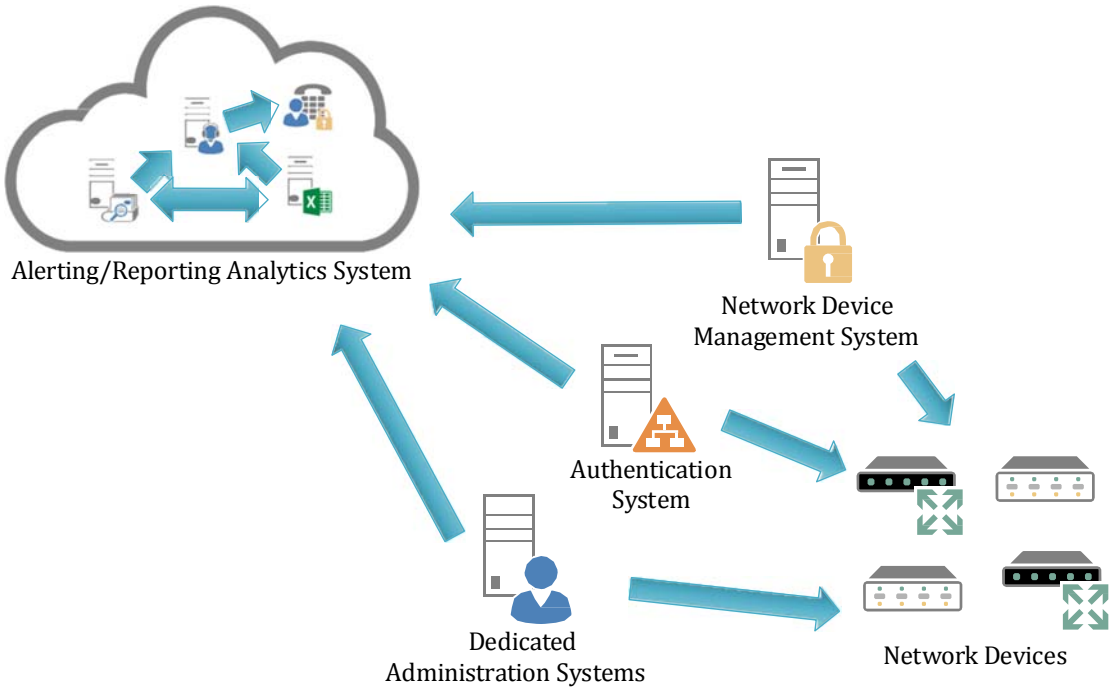
CSC11: ネットワーク機器のセキュアな設定				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Network	**11.1**	**組織で使用中の各種ネットワーク機器用に定義された標準のセキュアな設定と、ファイアウォール、ルータ、およびスイッチの設定とを比較します。そのような機器のセキュリティ設定は、組織の変更管理委員会によって文書化、確認、および承認される必要があります。 標準の設定からの逸脱、または標準の設定への更新をすべて文書化して、変更管理システムで承認する必要があります。**	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Network	**11.2**	ネットワークセキュリティ機器（ファイアウォール、ネットワークベースの IPS など）に対して、トラフィックの通過を許可する設定をセキュアな標準設定に追加する場合には、各変更の特定された業務上の理由、そのビジネスニーズの責任を負う特定の個人の名前、ニーズの予期される期間とともに、構成管理システムに文書化して記録する必要があります。	**Y**	
Network	**11.3**	自動ツールを使用して標準の機器設定を検証し、変更を検知します。そのようなファイルの変更はすべてログを取り、セキュリティ担当者に自動的に報告する必要があります。	**Y**	
Network	**11.4**	二要素認証および暗号化されたセッションを使用してネットワーク機器を管理します。	**Y**	
Network	**11.5**	すべてのネットワーク機器上でセキュリティ関連の更新をインストールするときには、常に最新の安定したバージョンをインストールします。	**Y**	
Network	**11.6**	ネットワークエンジニアは、すべての管理者タスクや昇格タスクをする際は専用のマシンを使用します。専用マシンは組織の主要なネットワークからは隔離され、インターネットアクセスを許可しないようにします。また、専用マシンは電子メールを読んだり、文書を作成したり、インターネットで情報するためには使用されないようにします。		**Y**
Network	**11.7**	ネットワークインフラの構成管理は、業務ネットワークとは異なる管理用のセグメントを通じて行う必要があります。VLAN を別にするか、できれば物理的に完全に異なるネットワークを使用します。	**Y**	

CSC11 手順およびツール

一部の組織では、商用ツールを使用してネットワークフィルタリングルールを評価し、自組織の基準と整合しているか矛盾があるかを評価します。このようなツールには、ネットワークフィルタリングの自動妥当性チェック、ネットワーク機器で意図しないサービスを許可する可能性があるルールセットの検索機能、アクセスコントロールリスト（ACL）のエラー検索機能などを備えています。ファイアウォールルールセット、ルータの ACL、その他フィルタリングに大きな変更を行うたびに、これらのツールを使って再評価を行います。

CSC11 システムエンティティ関係図



CSC12: 境界防御

異なる信頼レベルのネットワーク間を流れる情報の中から、セキュリティ上問題となるデータを検出／防止／修正します。

このコントロールが重要である理由

DMZ システムだけでなく、ワークステーションやノート PC などインターネットからコンテンツを取得できるシステムは、すべてインターネットを介して攻撃者からの攻撃を受ける可能性があります。犯罪グループや国家が組織的に攻撃を行う場合、まず始めに境界システムやネットワークデバイス、およびインターネットにアクセスするクライアントマシンの設定やアーキテクチャ上の脆弱性を利用して、組織内部へのアクセスを試みます。そして、これらのマシンの操作を乗っ取ることで、組織内のより深い場所に入り込み、情報の盗聴、改ざんを行い、あるいは組織内ホストに対し攻撃を仕掛けるべく常駐態勢を作り上げます。加えて、多くの攻撃はエクストラネットとも呼ばれるビジネスパートナーとのネットワーク間で行われます。こうして攻撃者は、エクストラネットの境界にある脆弱なシステムを悪用して、ある組織のネットワークから別のネットワークへと渡り歩きます。

侵害されたマシンへの攻撃とその証拠を探すことでコンテンツを監視し、ネットワーク境界からトラフィックのフローを制御するためには、ファイアウォール、プロキシ、DMZ 境界ネットワーク、およびネットワークベースの IPS と IDS を利用して、境界防御を多層化する必要があります。また、インバウンドトラフィックとアウトバウンドトラフィックの両方をフィルタにかけることが重要です。

組織内や組織間の相互接続性が拡大し、無線テクノロジーが急速に普及した結果、内部ネットワークと外部ネットワーク間の境界線がなくなりつつあることに注意する必要があります。これら不鮮明な境界は、攻撃者が境界システムをバイパスしながらネットワーク内へのアクセスを取得することを許してしまいます。ただし、不鮮明な境界であっても、有効なセキュリティの適用は、異なる脅威レベル、ユーザセット、コントロールレベルを持つネットワークを区別するよう慎重に設定された境界防御に、依然として依存しています。内部ネットワークと外部ネットワークの境界が不鮮明になりつつある状況でも、境界ネットワークの効果的な多層防御は、攻撃の成功数低減に役立ち、境界制限をバイパスするための方法を考案した攻撃者に対し、セキュリティ担当者が集中して対処することを可能します。

CSC12: 境界防御				
Family	CSC	Control Description	Foun-dational	Advanced
Network	12.1	既知の悪意のある IP アドレス（ブラックリスト）との通信を拒否する（またはデータフローを制限する）か、信頼できるサイト（ホワイトリスト）にアクセスを制限します。bogon ソース IP アドレス（ルーティング不能であるか、未使用の IP アドレス）からネットワークにパケットを送信して、ネットワーク境界から伝送されないことを確認することによって、定期的にテストを実行できます。bogon アドレスのリストは、インターネットでさまざまなソースから公的に入手可能です。これは、インターネットを通過する正当なトラフィックには使用すべきではない一連の IP アドレスを示しています。	Y	
Network	12.2	DMZ ネットワークでは、モニタシステム（IDS センサーに組み込むか、または別個のテクノロジーとして適用される）を構成して、少なくともパケットヘッダ情報、できればネットワーク境界宛のトラフィックまたはネットワーク境界を通過するトラフィックの完全なパケットヘッダとペイロードを記録します。ネットワーク上のすべてのデバイスからイベントを関連付けることができるように、正しく構成されたセキュリティ情報イベント管理（SIEM）システムまたはログアナリティクスシステムにこのトラフィックを送信する必要があります。	Y	
Network	12.3	インターネットとエクストラネットの DMZ システムおよびネットワーク上に、異常な攻撃メカニズムを探し、これらのシステムの侵害を検知するネットワークベースの IDS センサーを導入します。ネットワークベースの IDS センサーは、シグネチャ、ネットワーク振る舞い分析、またはトラフィックを分析するためのその他のメカニズムを使用して、攻撃を検知できます。	Y	
Network	12.4	ネットワークベースの IPS デバイスを適用し、既知の不正なシグニチャまたは攻撃の動作をブロックすることで、IDS を補完します。攻撃は自動化されるため、IDS などの方法では多くの場合、誰かが攻撃に対応するまでにかかる時間が長くなります。正しく構成されたネットワークベースの IPS は、不正なトラフィックを自動的にブロックします。ネットワークベースの IPS 製品を評価するときには、シグネチャベースの検知（仮想マシンやサンドボックス方式など）以外の手法を含めて検討します。	Y	

Family	CSC	Control Description	Foun-dational	Advanced
Network	**12.5**	インターネットへのすべての通信トラフィックが DMZ ネットワーク上の少なくとも 1 つのプロキシを通過する必要があるように、ネットワーク境界を設計して実装します。プロキシでは、ネットワークトラフィックを解読し個々の TCP セッションを記録して、ブラックリストを実施するために特定の URL、ドメイン名、および IP アドレスをブロックし、プロキシからアクセスできる許可されたサイトのホワイトリストを適用し、その他のサイトすべてをブロックすることができる必要があります。組織は、アウトバウンドトラフィックを、企業の境界にある認証済みのプロキシサーバからインターネットに強制的に流す必要があります。	**Y**	
Network	**12.6**	すべてのリモートログインアクセス（VPN、ダイヤルアップ、および内部システムへのログインを許可するその他の形式のアクセスを含む）で二要素認証を使用する必要があります。	**Y**	
Network	**12.7**	内部ネットワークにリモートからログインする企業のデバイスはすべて企業により管理され、その構成、インストールされているソフトウェア、およびパッチレベルがリモートで管理されます。サードパーティーのデバイス（請負業者／ベンダー）の場合、企業ネットワークへのアクセスに関する最小限のセキュリティ標準を公開し、アクセスを許可する前にセキュリティスキャンを実行します。		**Y**
Network	**12.8**	無許可の VPN 接続や、無線、ダイヤルアップモデム、またはその他のメカニズムで企業ネットワークとその他のネットワークに接続されているデュアルホームホストなど、DMZ をバイパスするインターネットへのバックチャネル接続を定期的にスキャンします。		**Y**
Network	**12.9**	異常なアクティビティを検知するため、NetFlow 収集および分析機能を DMZ ネットワークフローに適用します。	**Y**	
Network	**12.10**	ファイアウォールを経由してデータを流出させる隠れたチャネルを特定するには、多数の市販のファイアウォールに組み込まれているファイアウォールセッション追跡メカニズムを使用して、特定の組織とファイアウォール装置で異常に長時間続いている TCP セッションを特定するように設定し、これらの長いセッションに関連付けられているソースアドレスと宛先アドレスを担当者に通知する必要があります。		**Y**

CSC12 手順およびツール

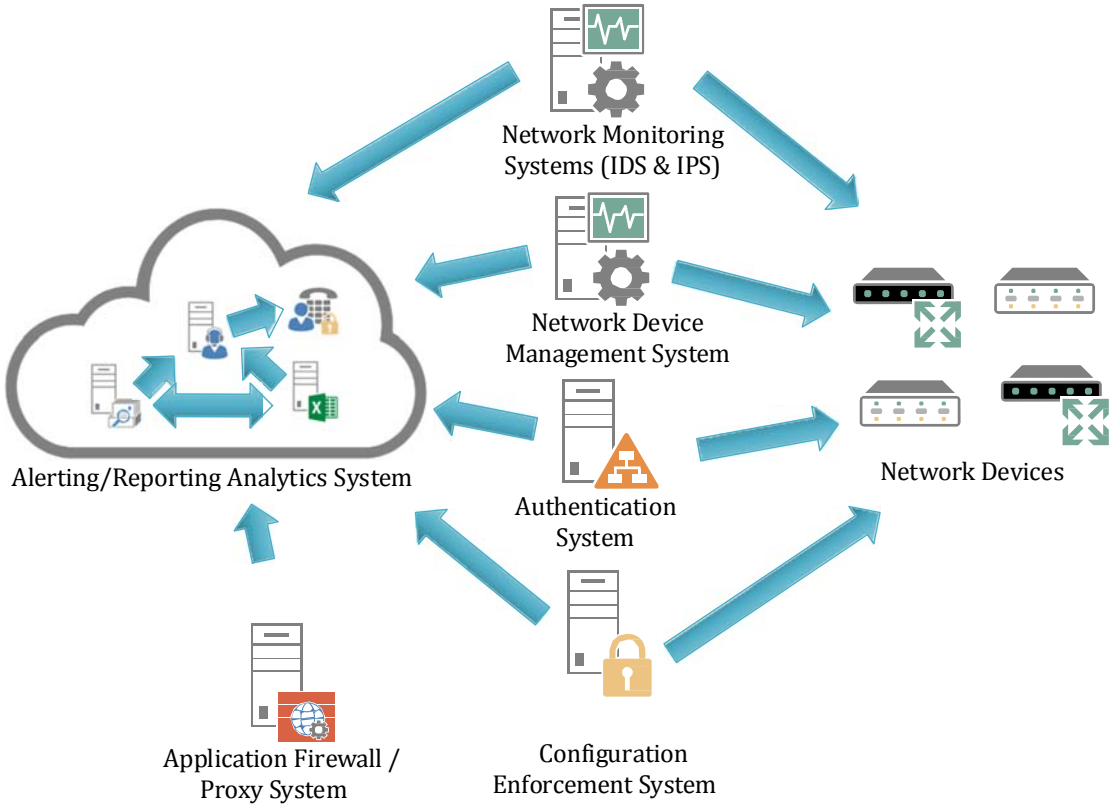
このコントロールに含まれている境界防御は、CSC10 に基づいて構築されています。追加の推奨事項は、全体的なアーキテクチャとインターネットと内部ネットワーク境界点の両方の実装に重点を置いています。ネットワークに入った侵入者の多くは最も重要なマシンを標的にしようとするため、内部ネットワークの分割がこのコントロールの中心となります。通常、内部ネットワークの保護は、内部の攻撃者に対する防御を目的として施されるものではありません。ネットワーク間で基本レベルのセキュリティ分割を構築して、プロキシとファイアウォールで各セグメントを保護することでも、侵入者によるネットワークの他の部分へのアクセスを大幅に低減することができます。

無償または商用の IDS とスニファーを利用して、このコントロールの 1 つの要素を実装し、DMZ と内部システムを標的にした外部ソースからの攻撃、および内部システムから DMZ またはインターネットに対して行われた攻撃を探し出すことができます。情報セキュリティ担当者は、これらのセンサーに対して脆弱性スキャンツールを実行することで定期的にセンサーをテストし、スキャナトラフィックが適切なアラートを挙げることを確認しなければなりません。キャプチャされた IDS センサーのパケットを、毎日自動化スクリプトを利用して確認し、ログのボリュームが予期したパラメータ内にあること、またログが正しくフォーマットされていて破損していないことを確認する必要があります。

さらに、Hypertext Transfer Protocol （HTTP）プロキシをバイパスする HTTP トラフィックを探すため、パケットスニファーを DMZ に適用しなければなりません。トラフィックを定期的に、例えば週に 1 回 3 時間サンプリングすることによって、情報セキュリティ担当者はソースも宛先も DMZ プロキシではない HTTP トラフィックを検索することができます。このようなトラフィックは、プロキシ使用の要件がバイパスされていることを示します。

許可された DMZ をバイパスするバックチャネル接続を特定するために、ネットワークセキュリティ担当者は、アウトバウンドアクセスをテストする受信側として使用するインターネットにアクセス可能なシステムを構築することができます。このシステムは無償または商用のパケットスニファーで構成されます。次にセキュリティ担当者は、組織の内部ネットワーク上にあるさまざまなポイントに送信テストシステムを接続して、容易に特定可能な送信トラフィックを、インターネット上で盗聴している受信側に送信します。これらのパケットは、テストに使用されたカスタムファイルを含んでいるペイロードによって、無償または商用のツールを使用して生成可能です。パケットが受信側システムに到達したら、パケットのソースアドレスを組織に許可されている許容可能な DMZ アドレスと突き合わせて検査する必要があります。ソースアドレスが、正当な登録済み DMZ に含まれていないことがわかった場合は、パケットが送信側から受信側システムに送信される際に使用したパスを判別するために、トレースルートツールを使用してさらなる詳細情報を収集することができます。

CSC12 システムエンティティ関係図



CSC13: データ保護

データの不正持ち出しを防止し、不正に持ち出されたデータの影響を低減し、機密情報の機密性と完全性を確保するためのプロセスとツールです。

このコントロールが重要である理由

データは多くの場所に散在しています。暗号化、完全性保護、データ損失防止の技術を組み合わせて使用することが、このようなデータの保護を実現する最良の方法です。組織内でクラウドコンピューティングとモバイルアクセスへの移行が進んでいくに伴い、データ侵害の影響を低減する一方で、データの不正持ち出しを制限し、不正持ち出しの発生が報告されるよう十分な対応をとることが重要です。

データの移動や保存に際してデータの暗号化を採用することで、データ侵害を低減できます。これが機能するのは、暗号化処理に関連するプロセスと技術が適切に管理されている場合です。この例として、さまざまなデータ保護アルゴリズムに使用される暗号鍵の管理があります。鍵の生成、使用、破棄のプロセスは、NIST SP 800-57 などの標準で定義されている実証済みプロセスに基づいている必要があります。

社内で使用する製品に、広く知られ綿密に検査された暗号アルゴリズムが、NIST の規定どおりに実装されていることを十分に確認する必要があります。また、データ保護の強度の点で組織が遅れをとらないようにするため、社内で使用するアルゴリズムと鍵のサイズを毎年評価することをお勧めします。

データをクラウドに移行する組織では、クラウドのマルチテナント環境でデータに適用されるセキュリティコントロールを理解し、暗号化コントロールと鍵のセキュリティを適用する上で最も適切な手続きを決定することが重要です。可能であれば、ハードウェアセキュリティモジュール（HSM）などの保護されたコンテナに鍵を保管することをお勧めします。

データを暗号化することで、万が一データが侵害された場合でも、重要なリソースなしでは平文にアクセスできないことが保証されます。ただし、何よりもまず、データ不正持ち出しの脅威を低減するコントロールを導入しなければなりません。多くの攻撃がネットワークを介して行われる一方で、機密情報が格納されているラップトップやその他デバイスの物理的盗難が絡む攻撃もあります。しかもほとんどの場合、被害者はデータの流出を監視していなかったため、機密データがシステムから流出していたことに気づきません。攻撃者への流出を最小限に抑えるため、ネットワーク境界間の電子的および物理的データ移動は、細心の注意が払われなければなりません。

組織が保護されたデータまたは機密データに対するコントロールを失うことは、事業運営にとって深刻な脅威となり、場合によっては国家の安全を揺るがす脅威にもなり得ます。窃盗やスパイ活動の結果として一部のデータが漏えいするか損失する場合、これらの問題の大部分は、データの正しい取扱いを十分に理解していないこと、効果的なポリシーアーキテクチャが欠落していること、そしてユーザエラーに起因しています。特に記録保全の実践が適切でないか存在しない場合、訴訟中の電子情報開示などの正当な活動の結果としてさえ、データ損失が発生することもあります。

「データ損失防止」（DLP）は、コンテンツの詳細な検査と集中型の管理フレームワークによって、使用中のデータ（エンドポイントアクション）、移動中のデータ（ネットワークアクション）、および保存データ（データストレージ）の特定、監視、および保護する人、プロセス、システムを対象とした包括的な取り組みを指します。過去数年にわたり、関心の対象と投資の対象が、ネットワーク保護からネットワーク内のシステム保護およびデータ自体の保護へと顕著に変化しています。DLP コントロールはポリシーに基づいており、機密データの分類、企業全体での機密データの発見、コントロールの強化、さらにポリシーへの準拠を確実にするためのレポート作成と監査を含んでいます。

CSC13: データ保護				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Network	**13.1**	データのアセスメントを実施し、暗号化および完全性コントロールを適用する必要がある機密情報を特定します。	**Y**	
Network	**13.2**	機密データを保持するモバイルデバイスとシステムに、認可されたハードドライブ暗号化ソフトウェアを適用します。	**Y**	
Network	**13.3**	ネットワーク境界を越えてデータを取り出そうとする不正な試行を発見し、そのような転送をブロックし、情報セキュリティ担当者にアラートを送信するため、特定の機密情報（個人識別情報）、キーワード、およびその他の文書の特性をモニタする自動化ツールをネットワーク境界に展開します。		**Y**
Network	**13.4**	自動化ツールを使用してサーバマシンの定期的なスキャンを実行し、機密データ（個人識別情報、健康に関する情報、クレジットカード情報、および機密情報）がシステムに平文で存在するかどうかを判別します。機密情報の存在を示すパターンを検索するこれらのツールは、ビジネスプロセスまたは技術的なプロセスが機密情報を置き去りにしていないか、もしくは機密情報を漏洩させていないかを特定するのに役立ちます。		**Y**
Network	**13.5**	USB トークンまたは USB ハードドライブが必要でない業務要件の場合、それらの機器にデータを書き込まないようにシステムを構成します。そのようなデバイスが必要な場合は、アクセスする特定の USB デバイスのみを（シリアル番号またはその他の固有のプロパティに基づいて）許可するようにシステムを構成でき、そのようなデバイスに格納されているすべてのデータを自動的に暗号化できるエンタープライズソフトウェアを使用する必要があります。許可されるすべてのデバイスのインベントリはメンテナンスされる必要があります。		**Y**

Family	CSC	Control Description	Foun-dational	Advanced
Network	13.6	ネットワークベースの DLP ソリューションを使用して、ネットワーク内のデータのフローをモニタおよびコントロールします。通常のトラフィックパターンを超える異常はすべて記録され、このような異常に対処するための適切な措置を行う必要があります。		Y
Network	13.7	組織の外へ出るトラフィックをすべて監視して、暗号化の許可されない使用をすべて検出します。攻撃者は多くの場合、暗号化されたチャネルを使用して、ネットワークセキュリティデバイスを迂回します。そのため、組織は不正な接続を検出して、その接続を終了し、感染したシステムを修復できることが不可欠です。		Y
Network	13.8	既知のファイル転送および電子メールによる情報流出の可能性のある Web サイト（Web メール）へのアクセスをブロックします。		Y
Network	13.9	ホストベースのデータ漏えい防止（DLP）ソフトウェアを使用して、サーバからデータがコピーされるときにも ACL を適用します。ほとんどの組織では、データへのアクセスは、サーバに実装されている ACL によってコントロールされます。データをデスクトップシステムにコピーした後では ACL は適用されなくなり、ユーザがデータを誰にでも送信できます。		Y

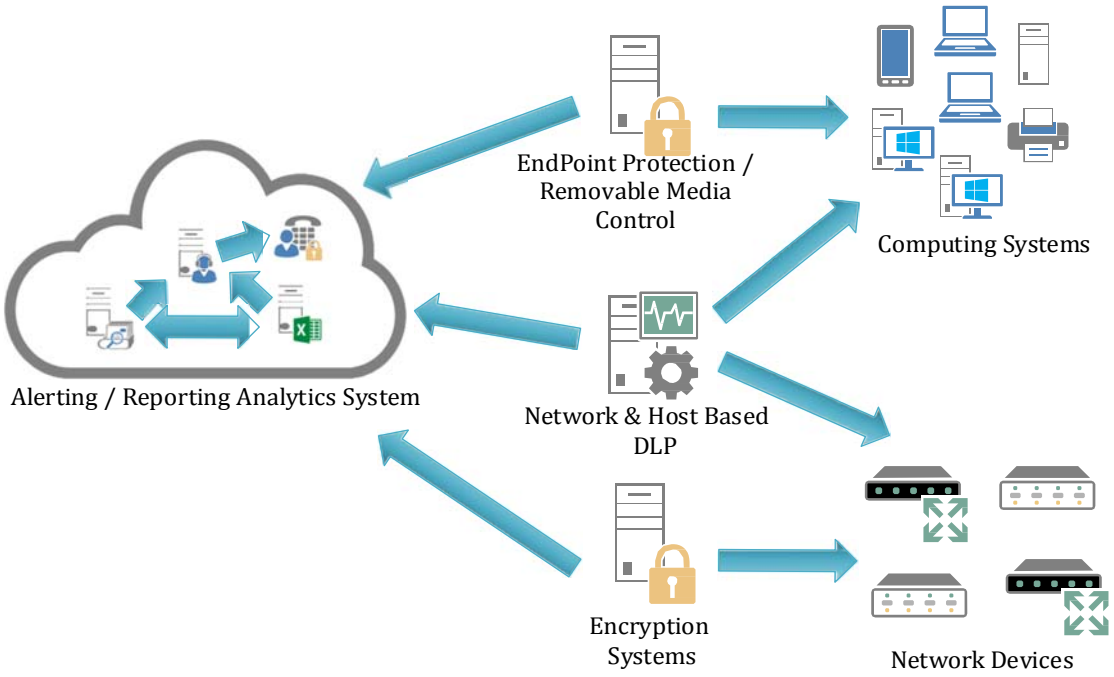
CSC13 手順およびツール

社内での暗号化と鍵の管理をサポートし、クラウドおよびモバイル環境で暗号化コントロールを実装するための商用ツールを利用することができます。

鍵管理に関連するライフサイクルプロセスと役割および責務の定義は、組織ごとに実施しなければなりません。

不正持ち出しの試行を発見したり、機密情報を保持している保護されたネットワークに関連するその他の疑わしいアクティビティを検出するには、商用の DLP ソリューションが利用可能です。こうしたツールを導入している組織は、ログを注意深く調査し、組織から機密情報を承認なしに伝送しようとする試行（正常にブロックした試行も含む）が検出されたなら、これを追跡しなければなりません。

CSC13 システムエンティティ関係図



CSC14: Need-to-Know に基づいたアクセスコントロール

許可された分類に基づき、どのユーザ、コンピュータ、アプリケーションが重要な資産（情報、リソース、システムなど）へのアクセスを必要とし、アクセス権限を持つべきであるかに関する正式な決定内容に従い、これら資産への保護されたアクセスを追跡／制御／防止／修正するためのプロセスとツールです。

このコントロールが重要である理由

最重要データを慎重に特定して、内部ネットワーク上で公開されている重要性の低い情報と切り離す措置をとっていない組織があります。多くの環境において社内ユーザは、すべてか、あるいはほとんどの重要資産にアクセスできます。機密性の高い資産には、物理システムを管理制御するシステム（例：SCADA）が含まれていることもあります。攻撃者は、こうしたネットワークに侵入すると、ほとんど阻止されることなく重要情報をたやすく見つけて持ち出すか、物理的損害を与えるか、運用を妨害することができてしまいます。例えば、過去2年で見られた注目度の高いいくつかの侵害事例では、はるかに重要性が低いデータと同一サーバに格納され同じアクセスレベルが設定されている機密データに対し、攻撃者はアクセスすることができています。また、企業ネットワークへのアクセスを利用して物理資産にアクセスし、損害を与えた例もあります。

CSC14: Need to Know に基づいたアクセスコントロール				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**14.1**	サーバ上に保管されている情報のラベルや重要度に応じて、ネットワークを分割します。すべての機密情報は、権限のあるユーザのみが特定の業務上必要なシステムにのみ通信するようにファイアウォールを設定した別個の VLAN 上に保管します。	**Y**	
Application	**14.2**	信頼性の低いネットワークを介した機密情報の通信は、すべて暗号化通信を使用する必要があります。情報が信頼レベルの低いネットワークを通過する場合は、常に情報を暗号化する必要があります。	**Y**	
Application	**14.3**	すべてのネットワークスイッチはネットワーク上の機器がサブネット上のその他の機器に直接通信する機能を制限し、攻撃者が攻撃したシステムの周辺システムへ攻撃（横断的侵害）できなくなるように、分割したワークステーションネットワークへの Private Virtual Local Area Networks (VLANs)を有効にします。	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Application	**14.4**	システム上に保管されているすべての情報は、ファイルシステム、ネットワーク共有、クレーム(Kerberos チケット内に入れる情報)、アプリケーションやデータベースのアクセスコントロールリストを使用して守られています。これらの管理は許可されたユーザのみが必要に応じ情報にアクセスできるという原則を徹底させます。	**Y**	
Application	**14.5**	システム上に保管されている機密情報は暗号化されており、情報にアクセスするためにはオペレーティングシステムに組み込まれていない第二の認証メカニズムを要します。		**Y**
Application	**14.6**	非公開のデータへのアクセスに関する詳細な監査ロギングと、機密データに対する特殊な認証を実装します。	**Y**	
Application	**14.7**	組織が定期的にアクセスしないアーカイブデータやシステムは組織のネットワークから分離します。これらのシステムは時折システムを必要とする事業部からネットワークから隔離されたスタンドアロンシステムとして使われるか、完全に仮想化され必要な時まで電源を切られている必要があります。	**Y**	

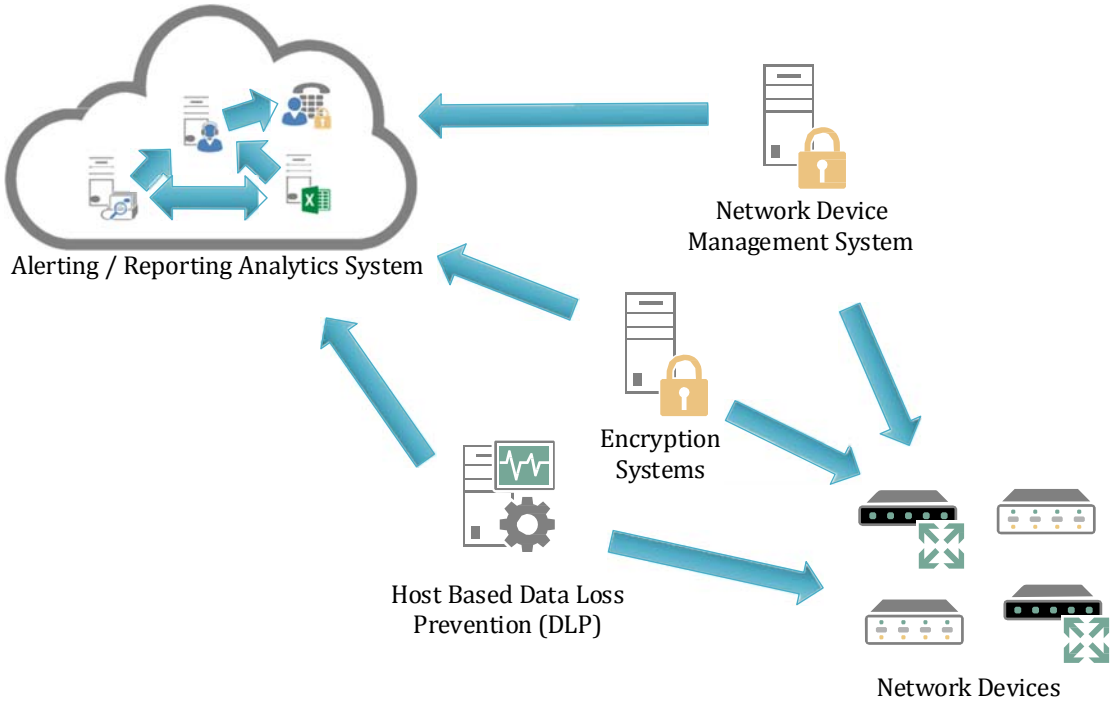
CSC14 手順およびツール

重要なのは、何が機密情報なのか、どこに存在するのか、そしてアクセスする必要があるのは誰なのかについて、組織が理解するということです。組織は機密レベルを得るために、データの主なタイプと組織に対する全体的な重要度をリスト化してまとめる必要があります。この分析を用いて、組織全体のデータ分類スキームを作成します。基本レベルでは、パブリック（機密扱いではない）とプライベート（機密扱い）の 2 つのレベルにデータ分類スキームが分かれます。プライベート情報を特定したら、侵害された場合に組織が受ける影響に基づいてさらにプライベート情報を分類することができます。

データの機密性を特定したら、ビジネスアプリケーションとこれらのアプリケーションを格納している物理サーバにトレースバックする必要があります。続いて、同じ機密レベルのシステムが同一ネットワークに配置され、異なる信頼レベルのシステムからは分離されるよう、ネットワークを分割しなければなりません。可能であれば、ファイアウォールで各セグメント間に配置しアクセスをコントロールします。信頼度が低いネットワークをデータが通過する場合は、暗号化しなければなりません。

ユーザグループごとに業務要件を策定し、その業務を遂行するためにグループがアクセスする必要がある情報を判別します。要件に基づいて、各業務に必要なセグメントまたはサーバにのみ、アクセス権を付与する必要があります。アクセスを追跡し、何者かがアクセスしてはならないデータにアクセスしている状況を調査することができるよう、すべてのサーバで詳細ロギング機能を有効にしておかなくてはなりません。

CSC14 システムエンティティ関係図



CSC15: 無線アクセスコントロール

本プロセスとツールは、無線ローカルエリアネットワーク（LAN）、アクセスポイント、無線クライアントシステムのセキュリティの使用状況を追跡／管理／防止／修正するために利用されます。

このコントロールが重要である理由

大規模なデータ窃盗は、攻撃者が物理的な建物の外部から組織への無線 LAN アクセスを取得することから始まり、組織内部のアクセスポイントに無線接続することで組織のセキュリティ境界をバイパスします。出張中の職員が所持する無線クライアントは、飛行機での移動中やインターネットカフェの利用中に、リモートエクスプロイトによって日常的に感染します。こうして悪用されたシステムは、その後に標的となる組織のネットワークに再接続した際、バックドアとして利用されます。ネットワーク上に未承認の無線アクセスポイントが発見されたという事例はいまだに後を絶ちません。これらは内部ネットワークへ無制限にアクセスできるように埋め込まれ、時には隠されているのです。直接の物理接続を必要としないため、無線デバイスは、攻撃者が標的とする環境への長期のアクセスを維持する上で便利な攻撃手段なのです。

CSC15: 無線アクセスコントロール				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Network	**15.1**	ネットワークに接続されている各無線デバイスが、文書に記録されている接続所有者と定義済みの業務要件を参照し、許可された構成とセキュリティプロファイルに一致することを確認します。組織は、そのような構成とプロファイルのない無線デバイスへのアクセスを拒否する必要があります。	**Y**	
Network	**15.2**	有線ネットワークに接続されている無線アクセスポイントを検知するよう、ネットワーク脆弱性スキャンツールを設定します。特定されたデバイスは、許可された無線アクセスポイントのリストと照合して一致する必要があります。無許可の不正なアクセスポイントは機能しないようにする必要があります。	**Y**	
Network	**15.3**	無線侵入検知システム（WIDS）を使用して、不正な無線デバイスを特定し、攻撃の試行と成功した侵害を検知します。WIDS に加えて、すべての無線トラフィックは、有線ネットワークを通過する際に WIDS によってモニタする必要があります。		**Y**
Network	**15.4**	無線アクセスを必要とする固有の業務要件が特定されている場合、承認された無線ネットワークへのアクセスのみを許可するように、クライアントマシンで無線アクセスを設定する必要があります。無線による業務にそぐわないデバイスでは、ハードウェア構成（基本的な入力／出力システムまたは拡張可能なファームウェアインターフェイス）で無線アクセスを無効にします。		**Y**

Family	CSC	Control Description	Foun-dational	Advanced
Network	**15.5**	すべての無線トラフィックが、Advanced Encryption Standard （AES）以上の暗号化と WiFi Protected Access2 （WPA2）以上の保護の両方に対応していることを確認します。	**Y**	
Network	**15.6**	無線ネットワークでクレデンシャル（認証情報）の保護と相互認証を提供するExtensible Authentication Protocol-Transport Layer Security（EAP／TLS）などの認証プロトコルを使用していることを確認します。	**Y**	
Network	**15.7**	無線クライアントのピアツーピア無線ネットワーク機能は無効にします。	**Y**	
Network	**15.8**	（Bluetooth のような）デバイスの無線周辺アクセスは、文書化された業務要件で必要な場合を除き、無効にします。	**Y**	
Network	**15.9**	BYOD システムやその他の信頼できないデバイス向けに、別の仮想ローカルエリアネットワーク（VLAN）を構築します。この VLAN からのインターネットアクセスは、少なくとも企業トラフィックと同じ境界を通過する必要があります。この VLAN から企業へのアクセスは、信頼できないアクセスとして扱われ、フィルタリングと監査を受ける必要があります。	**Y**	

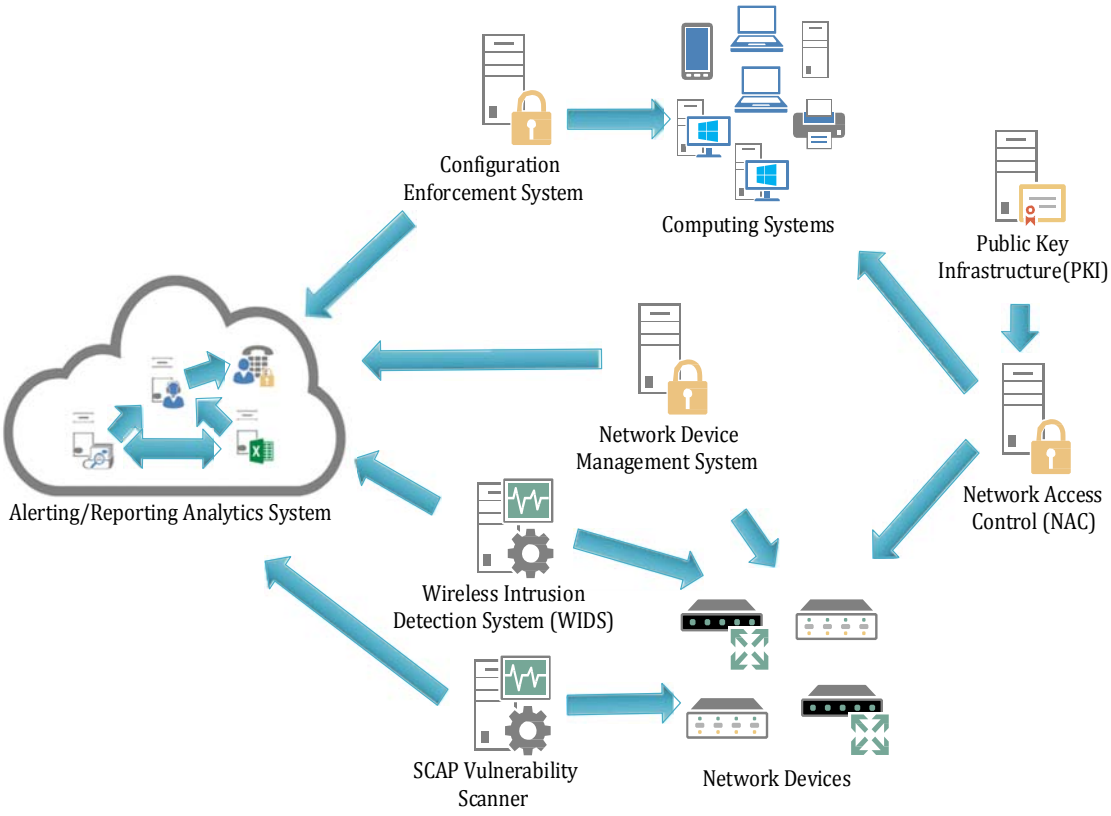
CSC15 手順およびツール

有効な対策をとっている組織では、商用の無線侵入検知システムとともに、無線スキャン、検知、発見ツールを実行しています。

さらに、セキュリティチームは、施設の境界内からの無線トラフィックを定期的にキャプチャし、無償および商用の分析ツールを利用して、無線トラフィックの伝送に使用されているプロトコルあるいは暗号化が、組織に義務付けられているよりも弱いものであるかどうかを判別しなければなりません。弱い無線セキュリティ設定を使用しているデバイスが特定された場合、そのデバイスが組織の資産インベントリに含まれていることを確認すべきであり、こうしたデバイスはよりセキュアに再設定するか、あるいは組織ネットワークへのアクセスを拒否する必要があります。

また、セキュリティチームは、有線ネットワーク上でリモート管理ツールを用い、管理対象システムに接続されている無線機能やデバイスに関する情報を取得しなければなりません。

CSC15 システムエンティティ関係図



CSC16: アカウントの監視およびコントロール

システムアカウントおよびアプリケーションアカウントのライフサイクル（アカウントの作成、使用、休止、削除）を能動的に管理し、攻撃者に悪用される機会を最小限に抑えます。

このコントロールが重要である理由

攻撃者は、アクティブでない正規ユーザアカウントを見つけ出して悪用し、正規ユーザになりすますことを頻繁に行うため、ネットワーク監視者による攻撃活動の発見を難しくしてしまいます。契約を終了した請負業者や従業員のアカウント、またレッドチームテスト用に正式に設定されながらその後削除されていないアカウントがたびたびこうした方法で悪用されます。さらに、一部の悪意のある社内関係者や元従業員が、契約満了後にシステムログに残されていたアカウントにアクセスして、承認外の行為や、場合によっては悪意ある行為を目的として組織のコンピュータシステムと機密データへのアクセスを維持していることがあります。

CSC16: アカウントの監視およびコントロール				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**16.1**	すべてのシステムアカウントを見直して、ビジネスプロセスと所有者に関連付けることができないアカウントをすべて無効にします。	**Y**	
Application	**16.2**	すべてのアカウントに有効期限が設定されていることを確認し、一般ユーザに変更が加えられないようにします。	**Y**	
Application	**16.3**	従業員または請負業者の解約時にアカウントを即時に無効にすることで、システムアクセスを失効するプロセスを確立して、そのプロセスに従います。アカウントを削除する代わりに無効にすることで、監査証跡を保持できます。	**Y**	
Application	**16.4**	すべてのアカウントの使用を定期的にモニタし、標準の未使用期間の経過後にユーザを自動的にログオフします。	**Y**	
Application	**16.5**	無人のワークステーションへのアクセスを制限するため、システムのスクリーンロックを設定します。	**Y**	
Application	**16.6**	アカウントの使用状況をモニタして休止アカウントであるかどうかを判別し、ユーザまたはユーザのマネージャに通知します。このようなアカウントが不要である場合はアカウントを無効化します。あるいは、例外（システム復旧または継続的な運用に必要なベンダー保守用アカウントなど）を文書化してモニタします。マネージャが現在の従業員と請負業者を、管理対象スタッフの各アカウントと照合することを義務付けます。その後、セキュリティまたはシステム管理者は、正当な従業員または請負業者に割り当てられていないアカウントを無効にする必要があります。	**Y**	

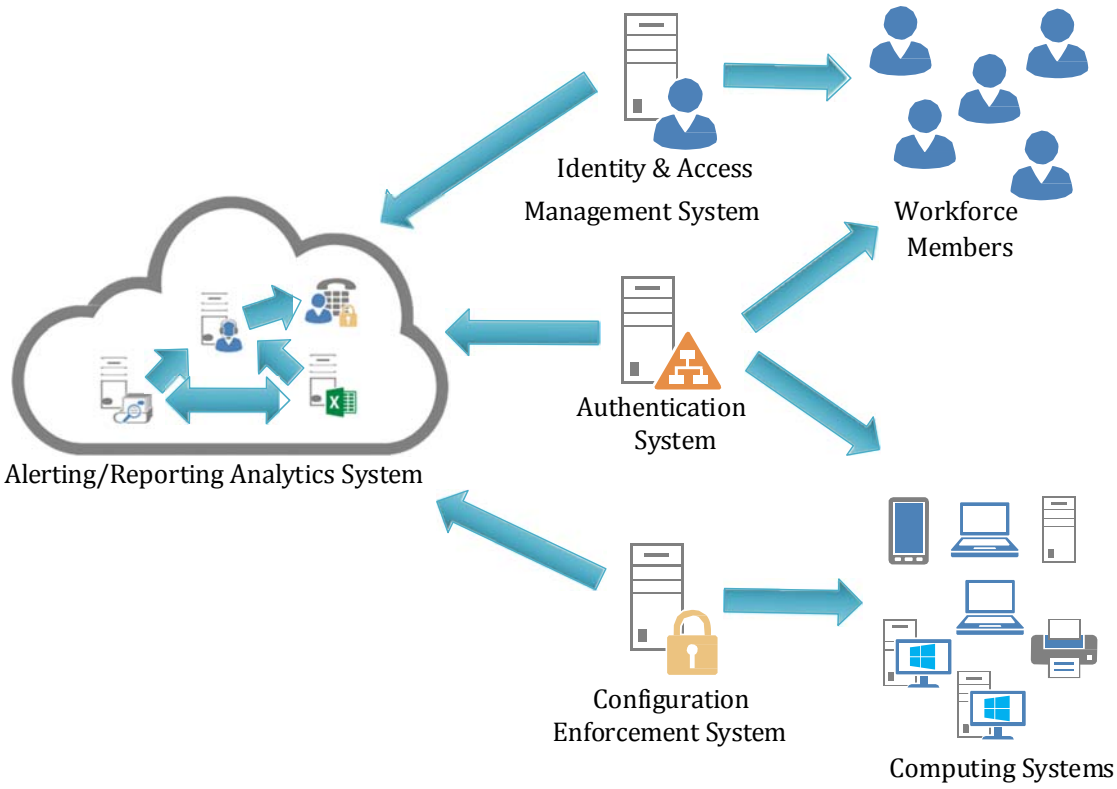
Family	CSC	Control Description	Foun-dational	Advanced
Application	**16.7**	アカウントロックアウト機能を使用し、設定されているログイン失敗回数に達した後に、アカウントが標準の期間にわたってロックされるように設定します。	**Y**	
Application	**16.8**	監査ログによって実効性のないアカウントへのアクセスの試行をモニタします。	**Y**	
Application	**16.9**	すべてのアカウントへのアクセスが、集中型認証ポイント（Active Directory または LDAP）を経由するように設定します。また、ネットワークデバイスとセキュリティデバイスを集中型認証に対応するように設定します。	**Y**	
Application	**16.10**	各ユーザの業務時間帯および利用時間を判別して、各ユーザの標準的なアカウントの使用をプロファイルする必要があります。通常の時間帯以外の時間帯にログインしたユーザと、通常の利用時間を超えているユーザを示すレポートを生成する必要があります。これには、ユーザが通常作業するコンピュータ以外のコンピュータからユーザクレデンシャル（認証情報）を使用した場合にフラグを付けることが含まれます。		**Y**
Application	**16.11**	機密データまたは機密システムへのアクセス権限があるすべてのユーザアカウントには、多要素認証を義務付けます。多要素認証は、証明書、スマートカード、ワンタイムパスワード（OTP）、トークン、生体認証などを使用して実施できます。	**Y**	
Application	**16.12**	多要素認証を使用していない場合、ユーザアカウントには長いパスワードを使用します(14 文字以上)。	**Y**	
Application	**16.13**	すべてのアカウントユーザ名と認証情報がネットワーク上で送信される際に暗号化チャネルを介していることを確認します。	**Y**	
Application	**16.14**	すべてのパスワードファイルが暗号化およびハッシュ化されており、ルート権限または管理者権限なしではアクセスできないことを確認します。システム上でパスワードファイルへのアクセスをすべて監査します。	**Y**	

CSC 16 手順およびツール

ほとんどのオペレーティングシステムには、アカウントの利用情報を記録する機能が組み込まれていますが、こうした機能は時としてデフォルトで無効になっています。機能が備わっていて有効であったとしても、デフォルトではシステムアクセスに関して細部にわたる詳細が提供されるわけではありません。セキュリティ担当者は、アカウントアクセスに関するより詳細な情報を記録するようシステムを設定し、社内開発のスクリプトやサードパーティーのログ分析ツールを利用することで、情報を分析することができ、さまざまなシステムのユーザアクセスをプロファイルすることができます。

アカウントは入念に追跡しなければなりません。休止アカウントはすべて無効にして、最終的にはシステムから削除する必要があります。アクティブアカウントは、すべてシステムの承認ユーザにトレースバックされなければなりません。また、パスワードが強固で定期的に変更されていることを確認します。さらに、攻撃者がシステムを利用して組織から情報を抜き取る可能性を最小限に抑えるため、一定時間システムを利用していないユーザはログアウトされなければなりません。

CSC16 システムエンティティ関係図



CSC17: スキル不足を補う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

組織内の全ての職務について、事業とそのセキュリティに不可欠な職務を優先しながら、企業防衛に必要とされる具体的知識、スキル、能力を洗い出します。その上で、現状との差を評価し不足を特定するための全体計画を作成し実施します。そして、セキュリティポリシー、組織計画、トレーニングおよびセキュリティリテラシープログラムを通じて改善を進めます。

このコントロールが重要である理由

サイバーセキュリティとは主として技術上の課題であると考えられがちですが、人間の行動もまた、企業にとっての成否を左右する重要な要素を構成しています。システムの設計、実装、運用や利用、管理に関するどの段階においても、人間が重要な役割を果たしています。例えば、システム開発者やプログラマは、システムライフサイクルの早い段階に根本的な脆弱性を改善できる機会を理解していないかもしれません。IT 運用専門スタッフは、IT のアーティファクトやログに含まれるセキュリティの問題に気づかない可能性があります。エンドユーザは、フィッシングなどのソーシャルエンジニアリングスキームに感染しやすいかもしれません。セキュリティアナリストは、新しい情報の波についていくのが大変です。経営層やシステム担当者は、全体的な運用／ミッションのリスクでサイバーセキュリティが担う役割を測ることができず、適切な投資判断をするための妥当な方法を見出せないかもしれません。

攻撃者は、組織にこうした課題があることを熟知しており、これを悪用する不正行為を計画します。例えば、不用心なユーザを狙って正常なメールに見せかけたフィッシングメールを用意周到に作成する、セキュリティポリシーとテクノロジーのギャップに着目し実際は施行されていないポリシーを悪用する、パッチの適用やログの定期確認が行われる前を狙って攻撃する、セキュリティ上重要ではないと判断され管理が不十分なシステムを踏み台としたりボットとして悪用する、といったことを行います。

こうした基本的脆弱性に対処する手段を持たずして、いかなるサイバー防御の取組みもサイバーリスクに対して有効とは言えません。逆にいうと、関係者に適切なサイバーセキュリティの習慣を持たせれば、大幅に組織のセキュリティを向上させることができるのです。

CSC17: スキル不足を補う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				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**17.1**	従業員に必要なスキルと、従業員が守っていない行動に対するギャップ分析を実施します。この情報を使用して、全従業員を対象としたベースライントレーニングと意識向上のためのロードマップを策定します。	**Y**	

Family	CSC	Control Description	Foun-dational	Advanced
Application	17.2	スキルギャップを解決するためのトレーニングを提供します。可能であれば、上級職員がトレーニングを実施します。あるいは、外部の講師を招き、使用する例が実際の業務に直接関連するようにオンサイトトレーニングを実施します。トレーニングを受ける従業員の数が少ない場合は、ギャップ解消のためにトレーニングカンファレンスへの参加やオンライントレーニングを利用します。	Y	
Application	17.3	セキュリティ意識向上プログラムを実施します。このプログラムは、（1）個人のアクションによってブロック可能な不正侵入で一般に使用される手法のみに重点を置き、（2）従業員にとって利用しやすい短期間のオンラインプログラムとして提供され、（3）最新の攻撃テクニックを反映するため頻繁に（少なくとも毎年）更新され、（4）すべての従業員が少なくとも毎年受講し修了するよう義務付けられ、（5）従業員の修了状況が確実にモニタされるようにします。	Y	
Application	17.4	従業員が疑わしい電子メールのリンクをクリックするかどうか、または電話をかけてきた発信者を認証するための適切な手順に従わずに機密情報を提供するかどうかを確認するテストを定期的に実施することで、セキュリティ意識レベルを確認、改善します。このテストで不合格となった従業員を対象に、トレーニングを実施する必要があります。	Y	
Application	17.5	従業員が疑わしい電子メールのリンクをクリックするかどうか、または電話をかけてきた発信者を認証するための適切な手順に従わずに機密情報を提供するかどうかを確認するテストを定期的に実施することで、セキュリティ意識レベルを確認、改善します。このテストで不合格となった従業員を対象に、トレーニングを実施する必要があります。		Y

CSC17 手順およびツール

組織全体に対する有効なトレーニングプログラムとは、従業員のトレーニングについて考えられていることと合わせて、組織全体としてセキュリティポリシーと導入されている技術を考慮していることが必要です。可能であれば、セキュリティポリシーに技術的な対策とその測定を取り入れ、それでも不足する部分を解消するためにトレーニングを実施します。技術的な管理策は、従業員が誤った行動をとる機会を抑制し、最小限に抑えることに集約させます。そのため、従業員のトレーニングでは技術的に管理できない事項に重点を置き、訓練を行います。

費用対効果を高めるために、セキュリティトレーニングは、優先度が高く、トピックが絞られ、具体的で、さらに測定可能なものを用意するべきです。セキュリティトレーニングを優先させるカギとなるのは、その企業の使命や事業の成果にとって、セキュリティ上不可欠な職務と役割を明確にすることです。国土安全保障省の長官によるサイバースキルタスクフォース 2012（the 2012 Task Force on Cyber Skills）の活動を参照することは、こうしたミッションクリティカルな職務を特定する 1 つの方法といってよいでしょう。

1）システム・ネットワークペネトレーションテスター
2）アプリケーションペネトレーションテスター
3）セキュリティモニタリング・イベントアナリスト

4）インシデントレスポンスの専門担当者
5）カウンターインテリジェンスアナリスト／インサイダースレットアナリスト
6）リスク評価エンジニア
7）セキュアプログラマおよびコードレビュアー
8）セキュリティエンジニア／アーキテクチャおよび設計担当者
9）セキュリティエンジニア／運用担当者
10）上級フォレンジックアナリスト

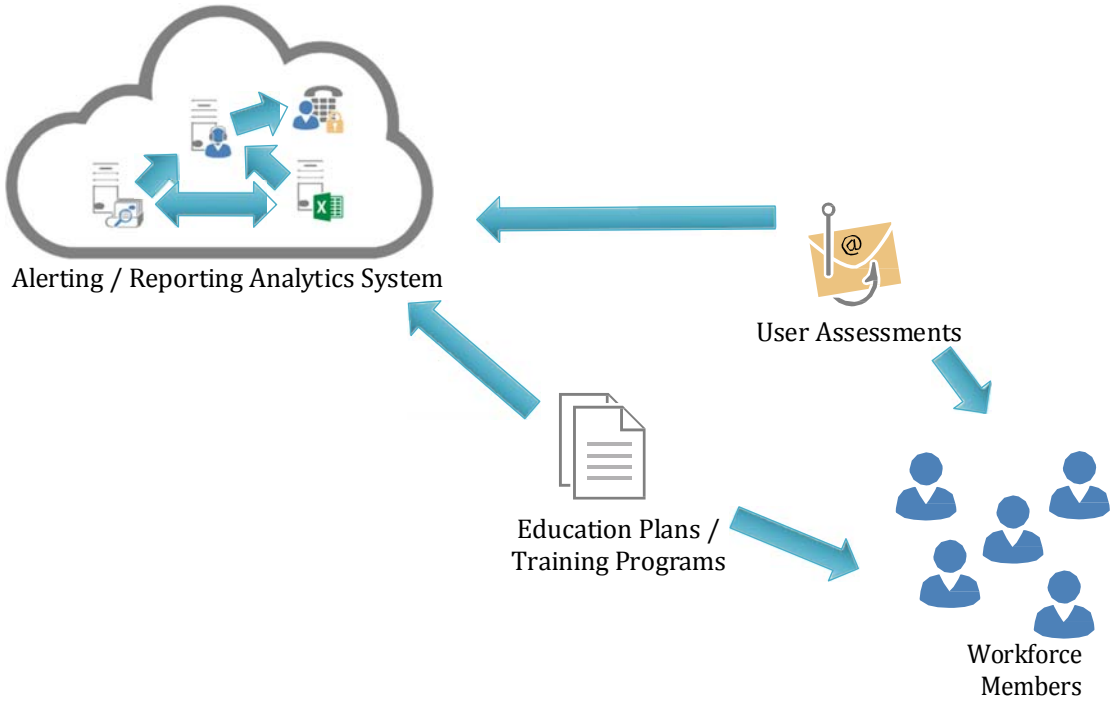
米国立標準技術研究所（NIST）から発行された国家サイバーセキュリティ・ワークフォース・フレームワーク（National Cybersecurity Workforce Framework）にて、企業や政府組織における一般的な職務と関連付けされた包括的なサイバーセキュリティの役割分類が参照できます。

全ユーザに対する一般的なセキュリティリテラシー教育も必要です。ただし、この種のトレーニングも各職務に合わせて調整して、組織を危険にさらす行動に重点を置いた内容にします。そして、トレーニングの評価を行い、改善していく必要があります。

スキルを向上させるには、従業員にも雇用者にも知識の充足度やギャップの度合い示す評価を開示し、その効果を測定することが重要になります。ギャップが測定されたなら、その職務上必要とされるスキルを改善しなければならない従業員の指導を、十分なスキルを持つ従業員に依頼することができます。さらに、セキュリティに関する教育計画を策定し、ギャップを解消して従業員の対応を最善なものに維持し続けることができます。

このトピックのすべてを詳しく扱うことは、本 Critical Security Controls の範疇を超えていますが、CIS が発行する「the Cybersecurity Workforce Handbook」(www.cisecurity.org)をご参照いただければ、企業セキュリティのための従業員の最適化に関する基本手順が記載されています。

CSC17 システムエンティティ関係図



CSC18: アプリケーションソフトウェアセキュリティ

ソフトウェアにおけるセキュリティ上の脆弱性を防止、検出、修正するため、社内開発ソフトウェアと社外調達したソフトウェアすべてのセキュリティライフサイクルを管理します。

このコントロールが重要である理由

Web ベースのアプリケーションソフトウェアやその他のアプリケーションソフトウェアで見つかった脆弱性は、しばしば攻撃者に悪用されます。脆弱性の原因には、コードの誤記、論理エラー、未達成要件、異常や不測の状況に対するテストの未実施など、さまざまな点が挙げられます。具体的なエラーの例として、ユーザ入力のサイズをチェックしていない、不要だが悪意のある可能性がある文字シーケンスを入力ストリームから除去していない、変数の初期化とクリアを行っていない、ずさんなメモリ管理でソフトウェアの一部が不具合を起こし、関係のない（セキュリティ上より重要な）部分にまで影響を及ぼしてしまうことなどがあります。このような脆弱性に関する膨大な公開情報および非公開情報は、攻撃者にも防御者にも入手可能であり、このような脆弱性を「武器化(weaponization)」して、エクスプロイトの作成を可能にするツールや技術が出回っています。攻撃者は、脆弱なマシンのコントロールを取得するために、バッファーオーバーフローや SQL インジェクション攻撃、クロスサイトスクリプティング、クロスサイトリクエストフォージェリ、コードのクリックジャックといった特定のエクスプロイトを使用できます。ある攻撃では、SQL インジェクションによって 100 万を超える Web サーバが、これらのサイトの閲覧者をマルウェアに感染させる悪意あるエンジンに変えられました。この攻撃では、州政府および他の組織の信頼できる Web サイトが攻撃者によって侵害され、これらの Web サイトにアクセスした何十万ものブラウザにマルウェア感染を引き起こしました。多くの Web アプリケーションおよび Web 以外のアプリケーションの脆弱性が定期的に発見されています。

CSC18: アプリケーションソフトウェアセキュリティ				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**18.1**	取得したすべてのアプリケーションソフトウェアについて、使用しているバージョンがベンダーによってサポートされているかどうかを確認します。サポートされていない場合は、最新バージョンに更新し、関連するパッチとベンダーのセキュリティ勧告をすべてインストールします。	**Y**	
Application	**18.2**	クロスサイトスクリプティングや SQL インジェクション、コマンドインジェクション、ディレクトリトラバーサル攻撃など（これに限定されない）、一般的な Web アプリケーション攻撃に対して、Web アプリケーションを通過するすべてのトラフィックを検査する Web アプリケーションファイアウォール（WAF）を導入することによって、Web アプリケーションを保護します。Web ベースではないアプリケーションでは、特定のアプリケーションタイプ用のアプリケーションファイアウォールが使用可能な場合は、そのようなアプリケーションファイアウォールを導入する必要があります。トラフィックが暗号化されている場合は、デバイスを暗号化の背後に配置するか、または分析の前にトラフィックを復号できる必要があります。いずれのオプションも適切ではない場合は、ホストベースの Web アプリケーションファイアウォールを導入する必要があります。	**Y**	暗号化/トンネル化されたトラフィックに対応するには、より綿密な計画とリソースが必要です。

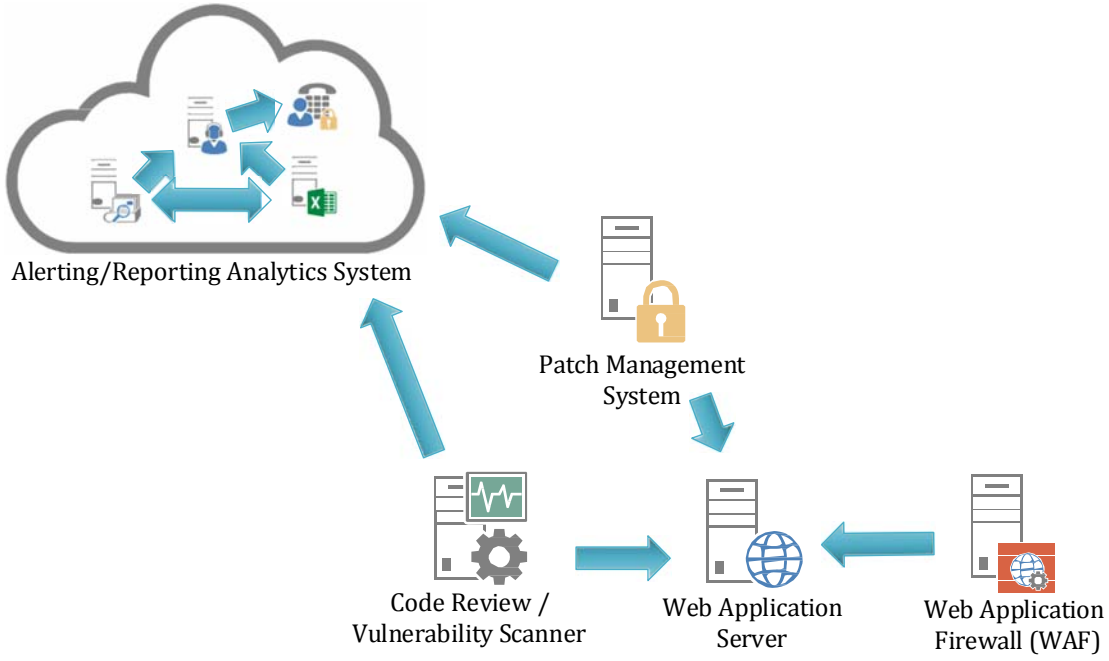
Family	CSC	Control Description	Foun-dational	Advanced
Application	18.3	自社開発ソフトウェアの場合、すべての入力(サイズ、データ型、許容される範囲またはフォーマットを含む)に関する明示的なエラーチェックが実行され、文書化されていることを確認します。	Y	
Application	18.4	自社で開発した Web アプリケーションとサードパーティーから入手した Web アプリケーションに対して、リリースする前に自動化リモート Web アプリケーションスキャナを使用してテストし、一般的なセキュリティ脆弱性の有無を確認します。このテストは、アプリケーションの更新が実施されるときには必ず実行し、また定期的に繰り返し実行します。特に、アプリケーションソフトウェアの入力検証および出力エンコードルーチンを確認してテストする必要があります。	Y	
Application	18.5	エンドユーザに対してシステムエラーメッセージを表示しないようにします（出力サニタイズ）。	Y	
Application	18.6	本番環境と非本番環境それぞれに別個の環境を維持します。一般に、監視下にない状況で開発者が本番環境へアクセスできないようにします。	Y	
Application	18.7	データベースを使用するアプリケーションについては、標準の強化設定テンプレートを使用します。重要なビジネスプロセスの一部であるシステムもすべてテストする必要があります。	Y	
Application	18.8	すべてのソフトウェア開発担当者が、特定の開発環境向けのセキュアなコードを書くトレーニングを受講できるようにします。	Y	
Application	18.9	自社開発のアプリケーションの場合、開発成果物（サンプルデータとスクリプト、未使用のライブラリ、コンポーネント、デバッグコード、ツール）が、実際に導入されたソフトウェアに含まれておらず、本番環境でこれらの成果物にアクセスできないことを確認します。	Y	

CSC18 手順およびツール

アプリケーション（社内開発アプリケーションおよび社外調達したアプリケーション）のセキュリティは、社内全体のポリシー、技術、各ユーザの役割をカバーする包括的なプログラムを必要とする複雑さを伴います。正式なリスク管理フレームワークおよびプロセスによって広く定義されているか、またはそれらが必要とされることが多くあります。

このトピックを包括的に説明することは、本 Critical Security Controls の対象範囲外です。ただし、CSC6 におけるアクションは、アプリケーションソフトウェアセキュリティを強化するための具体的かつ優先度の高い手順を示しています。また、このトピックを詳しく解説している優れたリソースの活用をお勧めします。例としては、DHS "Build Security In" Program （buildsecurityin.us-cert.gov）や The Open Web Application Security Project （OWASP）（http://www.owasp.org）などがあります。

CSC18 システムエンティティ関係図



CSC19: インシデントレスポンスと管理

組織の情報と信頼を保護するため、攻撃を迅速に検知し、損害を効果的に食い止め、攻撃者の存在を根絶し、ネットワークとシステムの完全性を復元するためのインシデントレスポンス基盤（計画、明確な役割、トレーニング、コミュニケーション、管理／監督）を策定、実装します

このコントロールが重要である理由

サイバーインシデントは日常的に発生しています。十分な資金があり、先進の技術を導入している大規模な企業でさえ、頻発する攻撃とその複雑性への対応に苦慮しています。企業に対するサイバー攻撃とは、「もし起こったら」ではなく「いつ起こるか」という問題なのです。

インシデントが発生してから、企業が正しく事態を理解し、管理し、復旧できるようにする適切な手順や報告、データ収集、管理責任、法的措置、コミュニケーション戦略を策定するようでは遅すぎます。インシデントレスポンス計画がなければ、組織は初期段階で攻撃を発見できないばかりか、攻撃が検知された場合においても、損害を最小限に抑え、攻撃者の存在を根絶し、セキュアな方法で復旧するための適切な手順に従うことができません。結果として、攻撃者はさらに大きな影響を組織に与え、より深刻な損害を引き起こし、より多くのシステムを侵害し、そしておそらくは、有効なインシデントレスポンス計画が実施されている場合に比べてより多くの重要な情報を流出させるでしょう。

CSC19: インシデントレスポンスと管理				
Family	**CSC**	**Control Description**	**Foun-dational**	**Advanced**
Application	**19.1**	インシデントに対応する担当者の役割の定義を含むインシデントレスポンス手順を策定し、文書化していることを確認します。この手順ではインシデントハンドリングのフェーズが定義される必要があります。	**Y**	
Application	**19.2**	コンピュータおよびネットワークインシデントを処理するための役職と職務を特定の個人に割り当てます。	**Y**	
Application	**19.3**	重要な意思決定の役割を果たすことによってインシデントハンドリングプロセスをサポートする管理担当者を定義します。	**Y**	
Application	**19.4**	システム管理者およびその他の担当者が異常な事象をインシデントハンドリングチームに報告するために必要な時間、そのような報告のための仕組み、およびインシデント通知に含める情報の種類に関する組織全体の標準を考案する必要があります。この報告には、組織がコンピュータインシデントに取り組むためのすべての法的要件または規制要件に従って、適切な地域緊急対応チーム(Community Emergency Response Team：CERT) へ通知することも含まれます。	**Y**	

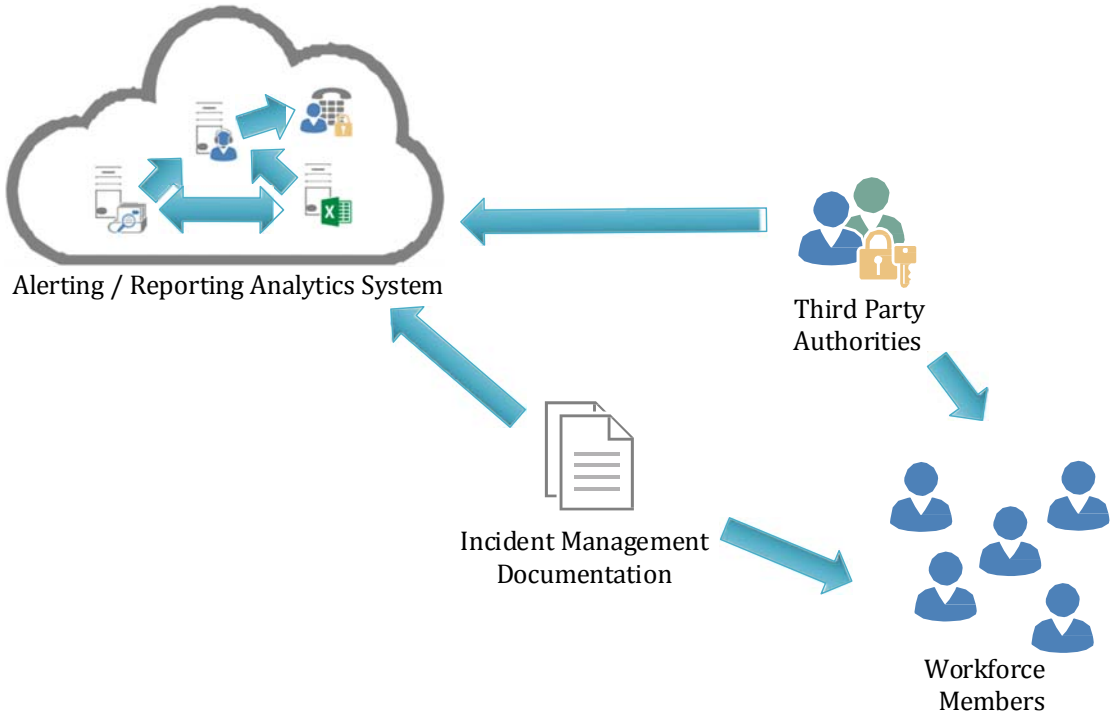
Family	CSC	Control Description	Foun-dational	Advanced
Application	19.5	セキュリティインシデントの報告に使用するサードパーティーの連絡先に関する情報を収集、保持します。（security@organization.com といった電子メールアドレスや http://organization.com/security といった Web ページなど）	Y	
Application	19.6	従業員と請負業者を含むすべての担当者を対象に、インシデントハンドリングチームへのコンピュータの異常とインシデントの報告に関する情報を公開します。そのような情報は、普段から従業員意識向上活動に組み込む必要があります。	Y	
Application	19.7	インシデントハンドリングチームに関連する担当者を対象にインシデントシナリオセッションを定期的に実施して、脅威とリスク、インシデントハンドリングチームを支援する上での担当者の責務を担当者が理解していることを確認します。	Y	

CSC19 手順およびツール

詳細なインシデントレスポンス手順の定義後に、インシデントレスポンスチームは、定期的なシナリオベースのトレーニングに参加し、組織が直面する脅威と脆弱性に合わせて細かく調整された一連の攻撃シナリオに取り組む必要があります。これらのシナリオは、チームメンバーがインシデントレスポンスチームにおける各自の役割を理解し、インシデントレスポンスに備える助けとなります。

このトピック全体を詳しく扱うことは、本Critical Security Controlsの対象範囲を越えています。ただし、CSC18におけるアクションは、企業セキュリティを強化するための具体的かつ優先度の高い手順を示していますし、それらは包括的インシデントレスポンス計画に組み込まれるべきものです。

CSC19 システムエンティティ関係図



CSC20: ペネトレーションテストおよびレッドチームの訓練

攻撃者の目的と活動をシミュレーションして、組織の防御対策（技術、プロセス、担当者）の全体的な強度をテストします。

このコントロールが重要である理由

防御設計と意図、実装、保守が適切であっても、その間にあるギャップが、攻撃者に悪用されてしまいがちです。例として、脆弱性が公表された後にベンダーからパッチが公開され、そして実際に各マシンにインストールされるまでの間の時間差や、善意から策定されたのみで実施メカニズムがないポリシー（特に、ユーザによるリスクの高いアクションを制限するための拘束力がないポリシー）、すなわち、適切な設定やその他の対策を企業全体に適用できていない状態であったり、もしくはネットワークへの接続と切断を繰り返すマシンに適用できていない状態であったり、さらには、複数の防御ツール間の相互作用や、セキュリティに影響する標準的なシステム運用での相互作用を理解できていない状態などがあります。

また、適切な防御を実現するには、技術面での防御、適切なポリシーとガバナンスに関する包括的なプログラム、そして従業員による適切なアクションが必要です。テクノロジーが継続的に発展し、新しい攻撃者のノウハウが定期的に表れる複雑な環境では、組織はその防御対策を定期的にテストし、ギャップを洗い出し、対応態勢を評価する必要があります。

ペネトレーションテストは、社内で特定可能な脆弱性を見つけ出し評価することから始めます。これを補完するため、攻撃者が特に組織のセキュリティ目標（特定の知的財産の保護など）をどのように妨害できるか、または特定の攻撃側の目標（秘密のコマンドコントロールインフラストラクチャの確立など）がどのように達成されるかを明らかにするテストを設計、実行します。判明した結果から、さまざまな脆弱性のビジネスリスクについて深く理解できます。

レッドチームの訓練は、組織の対応態勢の改善、防御担当者に行うトレーニングの改善、および現在のパフォーマンスレベルの検査を目的として、組織のポリシー、プロセス、防御対策全体にわたって取り組みます。独立したレッドチームは、脆弱性の存在、すでに実施されている防御対策および低減コントロール、さらには将来の実装のために計画されている防御対策および低減コントロールの有効性に関する価値のある客観的な見識を提供できます。

CSC20: ペネトレーションテストおよびレッドチームの訓練				
Family	CSC	Control Description	Foun-dational	Advanced
Application	20.1	定期的な外部および内部ペネトレーションテストを実施して、企業システムを悪用するために使用できる脆弱性と攻撃の経路を特定します。ペネトレーションテストは、部外者からの攻撃と内部関係者からの攻撃の両方をシミュレートするために、ネットワーク境界外（つまり、インターネットまたは組織周囲の無線周波数）からと、その境界内（つまり、内部ネットワーク上）から実行する必要があります。	Y	
Application	20.2	ペネトレーションテストの実施に使用するユーザアカウントとシステムアカウントが、正当な目的に限って使用されることと、テスト終了後に除去されるかまたは通常の機能に戻ることを確認するため、これらのアカウントをすべてコントロール・モニタする必要があります。	Y	
Application	20.3	定期的にレッドチームの訓練を実施して、攻撃を特定して阻止できるか、または迅速かつ効果的に対応できるかについて、組織の準備状況をテストします。	Y	
Application	20.4	攻撃者にとって有用な保護されていないシステム情報や成果物が存在しているかどうかを確認するためのテストを組み込みます。確認対象はネットワーク図、構成ファイル、古いペネトレーションテストのレポート、パスワード、システム運用に重要な情報を含む電子メールや文書などを含みます。	Y	
Application	20.5	複合型の攻撃を念頭に置いて、目標マシンまたは標的の資産を特定し、ペネトレーションテスト自体の明確な目標を策定します。多くの APT スタイルの攻撃では、複数の攻撃経路が使用されます。この場合、ソーシャルエンジニアリングと Web またはネットワークの悪用が組み合わされることがよくあります。ピボットによる攻撃または複数軌道による攻撃を捕捉するレッドチームの手動テストまたは自動化されたテストでは、セキュリティ態勢と重要な資産へのリスクがより現実的に評価されます。	Y	
Application	20.6	脆弱性スキャンツールとペネトレーションテストツールを連携して使用します。脆弱性スキャンの評価結果に基づいて、ペネトレーションテストを実施します。	Y	
Application	20.7	可能な際には常に、公開されていて機械処理が可能な形式(SCAP など)でレッドチームの活動結果を記録します。長期にわたってレッドチームの訓練の結果を比較できるように、結果を判別するための採点法を検討します。		Y
Application	20.8	特定のペネトレーションテストと、監視コントロールやデータ獲得、その他のコントロールシステムに対する攻撃など、本番環境で一般にテストできない要素に対するレッドチームによる攻撃テストのために、本番環境を模倣したテストベッドを作成する必要があります。		Y

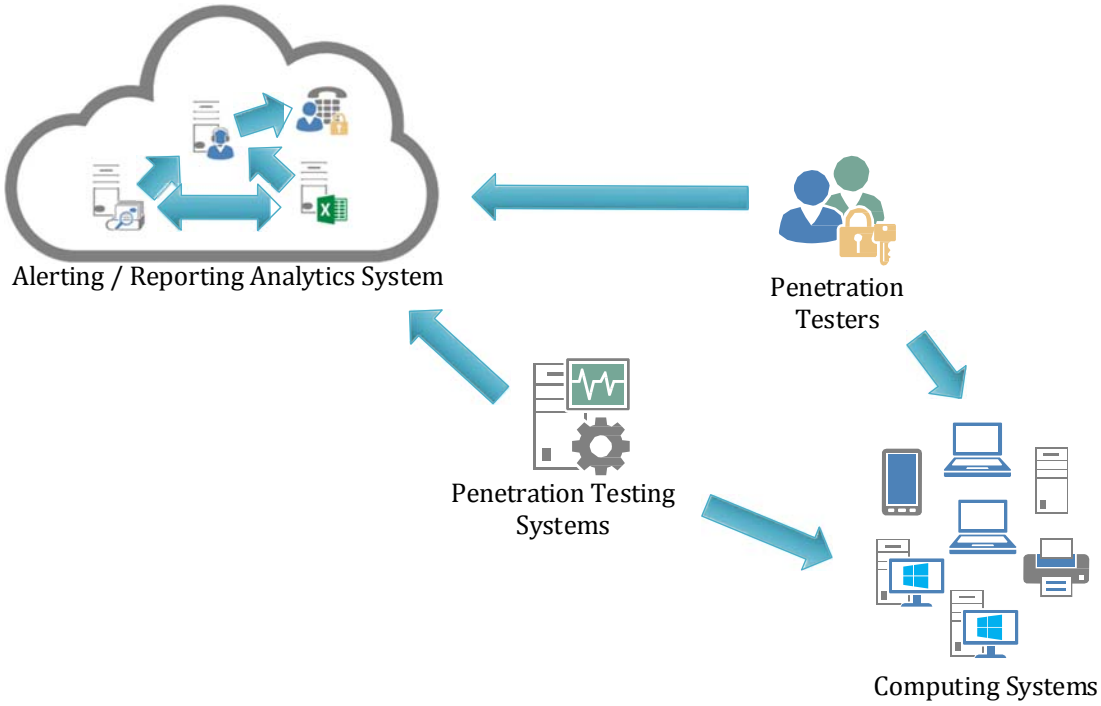
CSC20 手順およびツール

ペネトレーションテストとレッドチームの編成が大きな価値をもたらすのは、基本的な防御対策がすでに施行されており、包括的かつ継続的なセキュリティ管理／改善プログラムの一部として実施される場合に限られます。正式なリスク管理フレームワークおよびプロセスによって、これらが指定されているか、あるいは必要とされることがあります。

ペネトレーションテストとレッドチームの分析に対する取組みの範囲とルールは、各組織において明確に定義されなければなりません。そのようなプロジェクトの範囲には、少なくとも組織の最重要機密情報が格納されているシステムと本番稼働用処理機能を備えたシステムを含める必要があります。その他重要度の低いシステムも、より重要度の高い標的を侵害するための踏み台として利用されることがないかどうかを確認するためにテストするとよいでしょう。ペネトレーションテストとレッドチームの分析に関する作業ルールには、少なくともテストの日数、期間、全体的なテスト方法が記載される必要があります。

このトピック全体を詳しく扱うことは、本 Critical Security Controls の対象範囲を超えていますが、この CSC20 に記載したアクションは、企業のセキュリティを強化し、包括的ペネトレーションテストとレッドチームプログラムに組み込むべき、具体的かつ優先度の高い手順を示しています。

CSC20 システムエンティティ関係図



Appendix A: CIS Critical Security Controls の攻撃モデルの進化

背景

CIS Critical Security Controls（以下「コントロール」）は、その開始時から*「攻撃から防御を学ぶ」*という基本信条を持っていました。つまり、システムのセキュリティを侵害したことのある実際の攻撃（悪意ある者による「攻撃」）を知ることが、防御策の価値を測る上で重要な要素になっているということです。やりたいことや、やらなければならないことがすべて可能とは限りませんので、サイバー防御は、防御用リソースから最大限の価値を生み出すために最初に何をするべきかという優先度に従って行わなければなりません。**価値**を最適に判断できるのは攻撃者です。今、攻撃者はどんな攻撃をしているのでしょうか。それを防ぐために最も有効で拡張可能なアクションは何でしょうか。

本コントロールには、実際の攻撃と、多くの分野の様々な立場の専門家から集めた効果的な防御方法に関する知識が反映されています。本コントロールのために、多くの大手ベンダーの脅威レポートから攻撃データを検討・分析し、幅広く存在している脅威に対して本コントロールが十分に機能することを確認しました。我々は、このプロセスを CIS Critical Security Controls の**「コミュニティ攻撃モデル（Community Attack Model）」**と呼んでいます。現実世界から攻撃に関する関係情報を収集し、防御策に簡単かつ信頼性のある形で紐づけできるように内容をまとめるプロセスです。「コミュニティ」とは、参加者および情報源の広がりや、本プロセスを運用している共有リソースを指します。さらに、これらはコミュニティ全体が直面している脅威、つまり、攻撃者が具体的に成功した内容を文書化したものであることも強調しておきます。具体的な攻撃が今すぐ襲い掛かってくることはないかもしれませんが、いつでもその可能性はあるのです。

攻撃と脅威を理解するためのコミュニティアプローチ

コミュニティ攻撃モデルは、適切に文書化された権威ある「現実世界」のデータソースであるベライゾンのデータ漏洩/侵害調査報告書（ベライゾンDBIR 2013年版/2014年版/2015年版）から該当する項目を検証の上、内容を補足して作成されました。ベライゾンチームが主な分析を実施した後、CISが結成したボランティアチームがベライゾンチームと協力し、過去のデータで確認された最重要攻撃分類を直接本コントロールと紐づけ（サブコントロール）したものが、ベライゾンDBIR推奨の重要な部分を構成しています。先般、2015年シマンテックインターネットセキュリティレポートおよび2015年HPサイバーリスクレポートとの調整を図った年次報告書を使用して、同様の紐づけ作業が完了しました。この方法により、これらのデータ先導型の年次報告書の読者は、簡単かつ一貫性のある方法で、本コントロール内の一致する内容を確認できるようになっています。

本ワークフローに関する重要ポイントは以下です。

- 個々の攻撃に関するデータからではなく、ベンダーの分類または攻撃の概要レベルから紐づけが行われています。

- データは、ベンダーのビジネスモデル（インシデントレスポンス、マネージドセキュリティ、アンチマルウェアセンサー、スレットインテリジェンスなど）によって作成されているため、各内容は不完全ですが、そのエコシステムサンプルに関して適切に文書化されたものとなっています。
- 通常、ベンダーが使用する分類は説話形式であり、標準的な形式でも分類法でもありません。推奨事項も大抵は説話形式で記述されているため、具体的な防御フレームワークと紐づけされていません。そのため、あるベンダーの報告書とどのコントロールが一致するかを確認するには、議論や分析判断が必要になります。

本攻撃情報の利用や適切な防御策の選択は、脆弱性、脅威およびその結果を理解するための広範な**「基本リスク評価」**（個々の企業が迅速かつ価値の高い結果を出せるアクションを行うためのスタートポイントとして使用でき、コミュニティ全体で共通のアクションの基礎も提供するもの）の一部として確認できます。

運用可能な攻撃モデルの構築

本コントロール関連のコミュニティの規模や多様性の進化、また環境がさらに複雑化するのに伴い、私たちは本モデルの拡張性や再現性を上げ、他のコミュニティにも適用でき、正式なセキュリティフレームワークとの間でより一貫性のとれた内容に進化させなければなりません。すべては、私たちがここに至らしめた協力と公共の利益を旨とする精神を忘れることなく行われなければなりません。

一企業として、または企業コミュニティとしてこの問題に対応するかどうかにかかわらず、攻撃者に関連する新情報を見つけ出すために継続的かつ再現性のあるプロセスを作成・運用し、該当する環境への影響を評価して重要な意思決定を行い、対策をとらなければなりません。こうすることで、戦術的にも戦略的にも最高の投資方法を判断できるようになるでしょう。

有効なモデルには、多くの重要な要素があります。

- 信頼できる公開ソースから取得したデータに基づくべきだが、特殊知識（特定分野だけに当てはまるなど）または限定知識（機密扱いや契約によって制限されているなど）も利用可能とするべき。
- 優先度に対応し、正式なリスク管理フレームワークと一致した方法によって攻撃から対策（コントロール）へと転換する、しっかりと定義されたプロセスが用意されているべき。
- 過去の防御策の検証と新しい情報の評価が可能な継続的「更新」サイクルが用意されているべき。
- 低コストであるべきであり、可能であればコミュニティ全体でコストを共有すべき。
- 他者に対し自由に実証でき、譲渡可能であるべき（自らのリスクは、常に他者のリスクでもある）。

このように CIS Critical Security Controls を進化させることで、上記ガイドラインに従い、継続的に本コントロールを充実させ、更新していくことが可能なのです。これにより、脅威レポートの数や種類が増え、他のフレームワークに紐づける攻撃の標準分類や分類法が進化し、マルチステート ISAC（Multi-State Information Sharing and Analysis Center、MS-ISAC）の利用など、既存の情報共有手段を活用することができます。

Appendix B: 攻撃タイプ

これまで、Critical Security Controls を開発するにあたっては、以下の攻撃タイプが第一義的に検討されてきました。これらの攻撃タイプは、本コントロールの網羅性を確保するべく、逆に本コントロールに対しても紐づけが行われました。この方法は、CIS コミュニティ攻撃モデルを選択した結果、段階的に撤廃されつつあります。

攻撃の概要
攻撃者は、テストまたは実験システムを含む、未保護の新規システムを継続的にスキャンし、こうしたシステムの脆弱性を不正利用して侵害します。
攻撃者は、インターネット上でアクセス可能な（時として内部の）ウェブサイトに悪意あるコンテンツを頒布し、対象マシン上で実行されているパッチ処理が未完で、セキュリティ設定が不適切なクライアントソフトウェアの脆弱性を不正利用します。
攻撃者は、継続的に脆弱性の高いソフトウェアを詳細にスキャンし、その脆弱性を利用して対象マシンを侵害します。
攻撃者は、現在感染しているマシンまたはセキュリティが侵害されているマシンを利用し、社内ネットワーク全体で他に脆弱なマシンを特定し、これを悪用します。
攻撃者は、セキュリティよりも使いやすさを優先しているシステムの脆弱なデフォルト設定を悪用します。
攻撃者は、継続的な脆弱性評価や効果的修正が行われないために脆弱であるという認識がない組織において、重要パッチが未適用のシステムに見られる新たな脆弱性を悪用します。
攻撃者は、企業の有効性の測定や継続的改善を行うための防御策を実施していない対象組織のセキュリティを侵害します。
攻撃者は、悪意あるコードを利用して対象マシンを侵害し、機密データを取得して他のシステムに拡散、時にはシグニチャベースのアンチウイルスツールを無効化あるいは回避するコードを巧みに利用します。
攻撃者は、業務には必要のないことが多い対象システム上でリモートアクセス可能なサービスを詳細にスキャンし、攻撃ルートを用意して組織のセキュリティを侵害します。
攻撃者は、SQL インジェクション、クロスサイトスクリプティング、同様のツールなどの攻撃ベクトルを介して、脆弱なアプリケーションソフトウェア、特にウェブアプリケーションを悪用します。
攻撃者は、対象組織の内部ネットワークに侵入するために無線アクセスポイントの脆弱性や、機密情報を盗むために無線クライアントシステムの脆弱性を悪用します。
攻撃者は、セキュリティ関連のスキルや認識不足を突いてソーシャルエンジニアリングの手口でユーザやシステム管理者を欺きます。
攻撃者は、特定の短期業務ニーズのために、おそらくは一時的に例外を認めたが後日削除されることなく、徐々にセキュリティ設定が弱化したネットワークデバイスの脆弱性を悪用し、そこに侵入します。

攻撃者は、管理者権限を持つユーザを欺いてフィッシングメールの添付を開かせるか、インターネットウェブサイト上の攻撃者のコンテンツに移動させ、被害者のマシン上で攻撃者の悪意あるコードまたは改ざんを完全な管理者権限で実行します。
攻撃者は、インターネットでアクセス可能な DMZ ネットワーク上の境界システムを悪用して足が掛かりとし、内部ネットワークのより深部までアクセスできるようにします。
攻撃者は、不要または保護されていない接続、脆弱なフィルタリング機能、重要システムや業務機能から分離されていない箇所を探し出し、適切に設計されていないネットワークアーキテクチャを悪用します。
攻撃者は、ロギングやログレビューがないためセキュリティが侵害されているシステムで、長時間、検知されることなく活動します。
攻撃者は、機密情報を適切に特定せず保護をしていない、あるいは機密情報を通常情報と分けていない組織の機密文書にアクセスします。
攻撃者は、自身が残したアカウントも含め、一時雇用者、請負業者、元従業員などが残した非アクティブアカウントを侵害します。
攻撃者は、パスワードの推測やパスワード解析、権限昇格の脆弱性を突くといった攻撃で被害マシンの権限を昇格させ、システム管理者としての権限を取得し、企業内の他のマシンにも被害を広げるために利用します。
攻撃者は、企業システムの内部にアクセスし、被害組織に検知されることなく機密情報を収集し盗取します。
攻撃者は、システムを侵害し、重要データを改ざんするため、汚染された情報が組織の有効性を危険にさらす可能性があります。
攻撃者は、効果的対応能力を持たない組織内で検知されずに活動しますが、たとえ検知されたとしても、攻撃阻止、攻撃者の存在根絶、セキュアな業務環境の回復が不可能になっていることがあります。

Appendix C: 重要インフラのサイバーセキュリティを改善する NIST フレームワーク

2014 年 2 月のリリース以来、*重要インフラのサイバーセキュリティを向上させる NIST フレームワーク（The NIST Framework for Improving Critical Infrastructure Cyubersecurity）*は、重要なインフラ（また、それ以上のもの）のサイバーセキュリティに関する全国的議論の主要部分を占め、国内外の大規模かつ具体的なセキュリティ向上に向けた重要な一歩となりました。CIS は、本フレームワークの開発に積極的に参加しました。CIS Critical Security Controls は、具体的な実装を促進することにおいて有用な「参考情報」の 1 つとして参照されています。

本フレームワークは、その名前のとおり「意思決定や判断の際に取り入れる一連の原理やアイデアなど」（参照: MacMillan Dictionary）であり、個々の企業や企業コミュニティ全体に、セキュリティ関連の目標や向上に関する議論を取りまとめ、実施し、促進させるための手段を提供します。しかし、ここには具体的なリスク管理プロセスは含まれておらず、アクションの優先順位も指定されていません。「意思決定や判断」は、これを採用する側が具体的な状況や背景に合わせて管理しなければなりません。

大多数の企業にとって、こうした課題を解決するための最良の方法は、企業ごとではなく、コミュニティ全体で課題に取り組むことだと考えます。これは、CIS 非営利モデルの本質であり、CIS Critical Security Controls、CIS セキュリティ設定ベンチマークおよび National Cyber Hygiene Campaign のようなプロジェクトによって体現されています。全員が成功に至ることができるよう、私たちは一丸となって、重要なアクションを特定し、情報を生み出し、ツールを共有し、そして障害を取り除いていく必要があります。

この精神の下、CIS は絶え間なく本フレームワークの進化をサポートし、またコミュニティが、NIST のサイバーセキュリティフレームワークと合致したアクションメカニズムとして CIS Critical Security Controls の内容、プロセス、優先順位を活用できるように支援していきます。

以下に、コミュニティが本フレームワークを活用できるよう CIS が維持している実用的なサポート例をご紹介します。この表では、Critical Security Controls（バージョン 6.0）と NIST CSF（バージョン 1.0）の Core Functions and Categories（主な役割とカテゴリ）から最も関連のある項目との紐づけが行われています。

	Cybersecurity Framework (CSF) Core				
CIS Critical Security Controls (V6.0)	**Identify**	**Protect**	**Detect**	**Respon**	**Recover**
CSC1: Inventory of Authorized and Unauthorized Devices	AM				
CSC2: Inventory of Authorized and Unauthorized Software	AM				

	Cybersecurity Framework (CSF) Core				
CIS Critical Security Controls (V6.0)	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
CSC3: Secure Configuration of End user devices		IP			
CSC4: Continuous Vulnerability Assessment and Remediation	RA		CM	MI	
CSC5: Controlled Use of Administrative Privileges		AC			
CSC6: Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
CSC7: Email and Web Browser Protections		PT			
CSC8: Malware Defense		PT	CM		
CSC9: Limitation and Control of Network Ports, Protocols, and Service		IP			
CSC10: Data Recovery Capability					RP
CSC11: Secure Configuration of Network Devices		IP			
CSC12: Boundary Defense			DP		
CSC13: Data Protection		DS			
CSC14: Controlled Access Based on Need to Know		AC			
CSC15: Wireless Access Control		AC			
CSC16: Account Monitoring and Control		AC	CM		
CSC17: Security Skills Assessment and Appropriate Training		AT			
CSC18: Application Software Security		IP			
CSC19: Incident Response and Management			AE	RP	
CSC20: Penetration Tests and Red Team Exercises				IM	IM

Appendix D: The National Cyber Hygiene Campaign

The National Cyber Hygiene Campaign（全米サイバー予防キャンペーン）は、CIS Critical Security Controls を簡易な記述で入手しやすく、低コストで実装可能な基礎を提供することを目的として開発されました。本コントロールにはコミュニティにとっての優先度や対策が用意され、サイバー防御における難しい課題は既に単純化されていますが、非常に基礎的なレベルからセキュリティに取り組み始める企業も多いのです。

このキャンペーンは、すべての企業や行政のリーダーが答えられるであろう、いくつかの基本的な質問から始まります。

- 自組織のシステムやネットワークに何が接続されているかご存知ですか？（CSC 1）
- 自組織のシステムやネットワーク上でどのソフトウェアを実行しているか（または実行しようとしているか）ご存知ですか？（CSC 2）
- 「既知の優れた」設定を用いて、継続的にシステムを管理していますか？（CSC 3）
- 「既知の不適切な」ソフトウェアの検出および管理を継続的に行っていますか？（CSC 4）
- 管理者権限を持つ人物によるセキュリティ設定の変更、バイパスまたは上書きを制限し、それをトラッキングしていますか？（CSC 5）

これらの質問や、それに答えるために必要なアクションは、本キャンペーンの優先度トップ 5 に**「カウント、設定、コントロールパッチ、再現」**という「わかりやすい言葉」で記載されています。このキャンペーンに対応すべく、実装をガイドするドキュメントと「ツールキット」がボランティアによって作成されました。

言葉としては単純で分かりやすいのですが、各質問の裏側にはアクションプランを伴う主なコントロールが紐づけされています。このキャンペーンは、CIS Critical Security Controls から最初の 5 つ、オーストラリア通信電子局（ASD）の「Top Four Strategies to Mitigate Targeted Intrusions」（攻撃侵入を軽減するための 4 大戦略）、および国土安全保障省（DHS）の「Continuous Diagnostic and Mitigation (CDM)」（継続的診断およびリスク軽減）プログラムと整合するように設計されています。これにより、キャンペーンの優先事項に対し強力で防御を可能とする基盤と、そうした基礎的活動を経て防御を進化させるための道筋、そして多数の専門家、ユーザ、ベンダーからなるコミュニティの支援が得られることになります。

The National Campaign for Cyber Hygiene は、CIS（MS ISAC のホーム）と National Governor's Association Homeland Security Advisory Council (GHSAC) によって、多くの州、自治体、民族、地域政府の横断的な基本サイバーセキュリティプログラムとして共同採用され、あらゆる公的組織や民間組織にツールキットやリソースを提供しています。
*詳しくは、*www.cisecurity.org *をご覧ください。*

Appendix E: クリティカルガバナンスコントロールと CIS Critical Security Controls

サイバーセキュリティガバナンスは経営陣や幹部の重要な責務であり、全体的な企業ガバナンスの一部として統合されていなければなりません。その性質は常に変化するため、サイバーセキュリティガバナンスはサイバーセキュリティの*運用*フレームワークとも調整する必要があります。

効果的ガバナンスの実施には、自社の情報セキュリティプログラムから何が期待できるのか、経営陣が明確に理解していなければなりません。実施にあたりどのように指揮を執るか把握し、実施済みのセキュリティプログラムの現状を評価して、効果的なセキュリティプログラムの戦略と目的を決定する必要があります。

CIS Critical Security Controls の活用方法

本コントロールは、組織のネットワークや最重要データに対する攻撃を検知し回避するための実用的かつ自動化された活動です。経営陣から見たビジネス上のリスクと、そうしたリスクを管理するための具体的アクションや運用管理に関する技術的な見地とのギャップを埋めることで、企業のセキュリティガバナンスプログラムをサポートしています。経営陣が抱える主な情報セキュリティリスク関連の懸念を、具体的なセキュリティ改善プログラムや現場スタッフの日々のセキュリティ業務に反映させることができます。これにより、企業全体にわたってのリスク管理により良く適合させることができるのです。また、本コントロールは、専門家とベンダーで構成された大規模コミュニティにより作成、サポートされているので、セキュリティ改善に向けた効果測定や交渉のための具体的かつサポートされたオープンなベースラインが得られます。実質的にも、あらゆる公式規制、ガバナンスおよび監視フレームワークとも整合した内容になっています。

ガバナンスから CIS Critical Security Controls へ

企業の情報リスク管理能力を向上させるため、企業ガバナンス上の懸念と実施するセキュリティコントロールとを協調させるための手順をいくつかご紹介します。実施すべき主な CIS Critical Security Controls の例を取り上げていますが、これらに限定されるものではありません。

カバナンス項目 1: *組織の最重要情報資産と、そのセキュリティが侵害された場合に事業またはミッションに与える影響を特定します。*

> 情報は、現代のいかなる企業にとっても不可欠であり、情報の移動、保存および管理は、情報技術の利用と密接な関係にあります。そのため、以下の CIS Critical Security Controls が、情報の流れ、提示、用途を管理するシステムコンポーネントをトラッキングし、コントロールするための主な手段となります。
>
> **CSC1—許可されたデバイスと無許可のデバイスのインベントリ**
>
> **CSC2—許可されたソフトウェアと無許可のソフトウェアのインベントリ**

ガバナンス項目 2: *情報に絡むサイバー関連の既知の脆弱性を管理し、リスク管理に必要なセキュリティポリシーを確実に実施します。*

最低限、情報技術およびプロセスにおける*既知*の不具合や脆弱性について、その多くを発見および管理できるようにしなければなりません。以下の CIS Critical Security Controls は、対策、管理、報告が可能な責任ある活動のベースラインを確立する主な方法です。

CSC3: ハードウェアおよびソフトウェアのセキュアな設定

CSC4: 継続的な脆弱性評価および修復

ガバナンス項目 3: *組織の情報にとっての主たる脅威を明確に特定し、実施している防御策の脆弱性を評価します。*

組織の情報、システム、およびプロセスに対する脅威は、常に進化しています。以下の CIS Critical Security Controls は、対策、管理、報告が可能な責任ある活動のベースラインを確立する主な方法です。

CSC8: マルウェア対策

CSC20: ペネトレーションテストおよびレッドチームの訓練

ガバナンス項目 4: *最重要情報にアクセスできる人物を確認・コントロールします。*

適切な人物が企業データへのアクセス権を持ち、権限の厳格な管理が確保されていることで、内外からの未承認アクセスによる脅威の影響を軽減することができます。以下の CIS Critical Security Controls は、ニーズの特定やアクセス管理について責任ある活動のベースラインを確立する主な方法です。

CSC5: 管理権限のコントロールされた使用

CSC14: Need-to-Know に基づいたアクセスコントロール

情報セキュリティの主たる目的は、組織への悪影響を許容可能なリスクレベルにまで下げることにあります。そのため、極めて重要な対策には、企業が経験した情報セキュリティ関連事故の悪影響が包含されます。効果的なセキュリティプログラムは、影響が軽減されていることが傾向として見られます。定量的対策に、継時的影響の傾向分析を含めることが可能です。

包括的ガバナンス戦略の開発

CIS Critical Security Controls からは、サイバー防御のための主たる*技術的*コントロールを計画、優先順位付け、実施するための効果的な手段が得られますが、CIS Critical Security Controls の最適な活用方法は、総体的な情報ガバナンスプログラム、つまり技術的コントロールの実施内容を補足するポリシー、スタンダードおよびガイドラインにも対応したプログラムの一部とすることです。例えば、ネットワーク上に存在するデバイスのインベントリ管理は、重要な技術上のベストプラクティスですが、組織はさらに、従業員にこうしたコントロールの目的、期待される結果、そして企業の利益を守るために果たしている役割を明確に伝えるポリシーやプロセスを定義し、公開しなければなりません。

包括的ガバナンス戦略を開発するために有益なフレームワークを以下にご紹介します。私たちの経験に基づき、効果的な情報保証プログラムを構築しサポートする際の影響を考慮して、優先度の高いものからリストしています。

エグゼクティブスポンサーシップ: 職務や職責、運営委員会を明記した情報保証憲章を開発し、取締役会向けの状況説明を行い、経営陣からのサポートと指導を確保します。

情報保証プログラム管理: 予算計画などの管理やリソース割り当てコントロール、およびエグゼクティブスポンサーシップの下で情報保証プログラムを統制する際の優先順位を定義します。

情報保証ポリシーとスタンダード管理: セキュリティコントロールを完遂するための詳しいガイドラインを提供するため、ポリシーやスタンダードを定義・文書化し、防御策の一貫性を促進します。

データ分類: アナログまたは物理資産を含むデータ資産を特定、優先順位付けして分類します。

リスク管理: 価値の高いデータ資産の最適な防御方法に対する優先的な判断に基づき、配慮に富み目的が明確な防御戦略を特定します。

コンプライアンスとリーガル管理: 組織に課された規制および契約要件に基づいて、コンプライアンス要件に対処します。

セキュリティアウェアネスと教育: すべての従業員に対する教育計画を確立し、従業員の責務の一部として情報資産の保護に必要なスキルが備わることを確実にします。

監査と評価管理: 情報保証の取組みが、定義済みのスタンダードと適合していることを確認し、その取組みを支援する監査と評価を行うことでリスク管理を行います。

職員と人材管理: 人によるデータ資産の扱い方を管理するため、職員や人材のコントロールを明確にします。人と技術のコントロールは、情報資産の防御にとって必要不可欠です。

予算とリソース管理: 効率的に防御を行うため、適切な人材を割り当てます。防御のために情報保証のための基盤は不可欠ですが、予算と人材がなければ、計画を効率的に実現させることはできません。

物理セキュリティ: データ資産の論理的なセキュリティ基盤を整備するために、データ資産を保存する設備、建物、場所を保護します。

インシデントレスポンス管理: 有事の際の対応方法に関する管理計画を明確にします。これは、事業継続や災害管理の一部として機能します。

事業継続と災害復旧管理: 業務に対し発生し得る障害に起因して被る可能性のある損失を軽減するための復旧コントロールを明確にします。

調達管理とベンダー管理: データ資産の防御において、関係各社と連携します。本コントロールは、組織がサードパーティーやベンダーと協力してデータ資産を守る方法を定義しています。

変更管理と構成管理: 組織の情報資産を防御するために、システムに対する変更、とりわけ設定の変更を、手順に従った正式な方法で評価し、承認または却下し、記録します。

組織は、本ドキュメント内で別途定義されている技術的コントロールと平行して、これらのガバナンスコントロールを実施することが推奨（また、多くの場合は要求）されます。技術関連のコントロールと管理関連のコントロールは、いずれも組織の防御構造において同様に重要な柱と見なされなければなりません。

Appendix F: CIS Critical Security Controls のプライバシー影響評価（PIA）に向けて

はじめに

企業がサイバーセキュリティに対し有効な方針をとることで、個人のプライバシーを侵害する必要はありませんし、実際のところ、侵害するべきではありません。プライバシーを守るために、多くの法律、規制、ガイドラインおよび推奨事項が存在し、多くの場合、組織が本コントロールを適用すれば、既存のプライバシーポリシーにも適応することになります。

最低限でも、本コントロールの使用は、*公正な情報処理原則（FIP）*[2]やプライバシーバイデザイン[3]に詳述されている一般原則に準拠させるべきです。本コントロールを採用するすべての企業は、関連システムのプライバシー影響評価を行い（そして、それを関係者と共有し）、本コントロールの実施時に適切な保護が提供されることを確実にすべきです。また、すべての企業は、サイバーセキュリティに対する自社の姿勢に重要な変更が加わる際に、これらの評価を定期的に検討すべきです。ここでは、具体的なコントロールの実施に伴って考えられる主なプライバシー関連リスクを評価、軽減し、また個人のプライバシーに対する本コントロールの全体的な影響を評価することが目的です。

本コントロールを実施する際にプライバシー影響評価を行う企業の取組みや、プライバシーや本コントロールに関するより一般的な参照スタンダードの確立に向けた取組みを支援するため、CIS では、技術専門家とプライバシー専門家を招集し、各コントロールの検討とベストプラクティスの提案を行っています。

以下のフレームワークでは、この取組みを支援し、プライバシー影響評価に考えられる内容をまとめます。

CIS Critical Security Controls のプライバシー影響評価

I. 概要

各コントロールの目的をまとめ、実際または潜在的に個人情報が関わる部分について、正当な理由を記載します。

- 可能な限り、本コントロールを実施するために、どのような技術、手順およびデータフローが用いられているか特定してください。全般的に、本コントロールによって、どのように情報が収集・保存されるか簡単に説明してください。本コントロールで収集されるデータの種類と、このデータから導き出される情報の種類を特定してください。本コントロールによる個人を特定できる情報（PII）の収集および使用方法について説明する際は、その PII の収集から廃棄までのライフサイクルを詳しく説明した代表的な流れを含めてください。

[2] http://www.dhs.gov/publication/fair-information-practice-principles-fipps および http://www.nist.gov/nstic/NSTIC-FIPPs.pdf をご覧ください。

[3] https://www.privacybydesign.ca をご覧ください。本 Annex に記載するアプローチは、アメリカ合衆国の公共セクターにおけるアプローチを重く取り上げていますが、全ての業界に適応可能です。

- プライバシーデータを保護し、承認されないアクセスまたは不用意なデータ開示のリスクを軽減するために必要な対策を説明してください。ここでは、プライバシーについて考えられるリスクをすべてリストするのではなく、本コントロールを実施することで発生し得るプライバシーリスクの総体的な概念を提示してください。
- 企業内および外部共有パートナーの両方において、本コントロールを実施した結果発生する可能性のある個別および所定の情報共有を説明してください。また、そのような外部共有が、元々収集していた情報と両立し得るのか、さらに、この共有に対応するためにどのような契約が必要になるかについても説明してください。

II. 関係当局

本コントロールによる情報の収集または使用を許可する、または反対に制限する、あるいは禁止する司法当局または企業ポリシーを特定してください。

- 上記で特定した情報の収集権限を含め、本コントロールの運用を統制する司法当局および規制当局をリストしてください。司法および規制当局がどのように情報の収集や使用を許可または制限するか、または地理的な保存要件をどのように統制するか説明してください。本コントロールが個人を特定できる情報（PII）を収集する可能性がある場合は、そのような収集を許可する具体的な司法当局を特定してください。
- 企業の担当部門は、親会社や子会社、パートナー、代理店の権限を信用できていますか。
- 海外のユーザや組織、政府機関から、本コントロールで収集した情報を受け取った可能性はありますか。ある場合、その収集を支援または統制するための国際合意、契約、プライバシーポリシーまたは覚書（MOU）は存在しますか。

III. コントロール関連情報の特性化

本コントロールが収集、使用、発信または維持するデータの種類を特定してください。

- 各コントロールに関して、情報収集源となる技術ソース、ログまたは個人のカテゴリーを特定し、各カテゴリーに関して、本コントロールに対応するために収集、使用または保存される可能性のある PII をリストしてください。
  - ここに該当する情報には（ただし、これらに制限されません）、氏名、生年月日、住所、電話番号、社会保障番号、電子メールアドレス、母親の旧姓、医療記録の管理 ID、銀行口座番号、健康保険の受益者、その他の口座番号、免許証または他の許可証番号、ナンバープレートを含む自動車識別 ID、婚姻履歴、住民または犯罪歴情報、医療記録、デバイス識別子やシリアル番号、教育記録、生体認証識別子、顔写真、または、その他あらゆる独特の ID 番号または特徴が含まれます。
- 本コントロール、またはそれに基づき稼働しているシステムの出力として、収集したデータから新しい情報が生成される場合（例えば、スコア、分析結果またはレポートなど）、この新情報にプライバシーの問題が絡む可能性はありますか。ある場合、新たに生成された情報について、上記と同じ分析を行ってください。
- 本コントロールが商用ソースまたは公的に得られるデータからの情報を使用して他の収集データを補足している場合、この情報の使用方法を説明してください。
  - 商用データには、情報収集サイト（Lexis Nexis、脅威フィード、マルウェアデータベースなど）や、元来は民間組織が情報収集しているソーシャルネットワークソースからの情報が含まれます。
  - 公的に得られるデータには、インターネットから取得した情報、ニュースフィード、ま

たは商用の情報収集サイトではなく、裁判記録など州または自治体機関から直接受け取った、州または自治体の公式記録などが含まれます。
    - この補足されたデータに関係して、プライバシーの問題が発生し得るデータが生まれる状況を特定してください。そのような状況がある場合、新たに生成される情報に上記と同様の分析を行ってください。
- コントロール情報のプライバシー関連リスクを特定し説明した上で、その緩和策を説明してください。特定のリスクは、収集源または収集方法に固有の問題かもしれません。
- 以下の公平な情報処理原則（FIPs）を検討してください。
    - *目的特定の原則*: 本コントロールによる PII の収集が、企業のサイバーセキュリティ関連ニーズとどのように絡んでいるか説明してください。
    - *最小化の原則*: 当該 PII データは、本コントロールの具体的な目的を達成するにあたり、直接関係していますか。あるいは、必要なものですか。
    - *個人参加の原則*: 本コントロールは、可能かつ実用の範囲内で、個人から直接 PII を収集していますか。

IV. コントロール関連情報の使用

本コントロールによる PII またはプライバシー保護データの用途を説明してください。本コントロールによるこのデータの使用方法と理由を説明してください。

- 企業が内外で収集した情報または保持している情報について、起こり得る使用方法をリストしてください。さまざまなデータ要素の使用方法と理由を説明してください。例えば、何らかの理由で社会保障番号を収集する場合、なぜ収集する必要があるのか、どのように使用するのかを説明してください。情報の適切な取扱いを確保するために取り入れている手順や保護の種類、ユーザ通知を提供するために必要なポリシーを説明してください。
- 本コントロールでは、技術を活用して、データベースの電子検索、クエリまたは分析を行い、予測パターンや例外を発見したり特定したりしていますか。している場合、どのような結果が得られるのか、またプライバシー関連の問題が発生する可能性があるか説明してください。
- 一部のコントロールでは、ユーザからの問合せやプログラムされた機能に応じて大量の情報処理が必要です。本コントロールは、以前には特定不能であったものの、アナリストまたは他の従業員による追加調査の必要性が生まれるデータの特定に役立つかもしれません。一部のコントロールは、他のデータ種類、マッチング、関係性分析、スコアリング、報告またはパターン分析に至る複雑な分析作業を行うようにデザインされています。
- リンク分析、スコアリングまたはその他の分析を含め、上記の用途で生成される結果について話し合ってください。こうした結果は、情報システムによってデータで生成されるか、アナリストレビューによって手動で生成されます。こうした結果には、プライバシー関連の問題が絡んでいますか。
- 企業内または企業に関係する他のオフィスまたは部署で、生成されたデータを受け取る場所はありますか。そのようなオフィスまたは部署がこのデータの使用や収集を行うことにプライバシー関連の問題はありますか。
- 以下の FIP を検討してください。
    - *透明性の原則*: PIA および関連のポリシーは、本コントロールによって生成された情報の使用について明記していますか。
    - *使用制限の原則*: システムに含まれる情報の使用は、本コントロールのミッションに関係していますか。

V. セキュリティ

本コントロールに対応している情報システムのセキュリティ計画を策定してください。

- 本コントロールに送られるプライバシー保護データや本コントロールから生成されるプライバシー保護データを守る適切な物理、人材、IT その他の保護対策を確実にするべく、本コントロール実施時における適切なガイダンスは用意されていますか。
- 以下の FIP を検討してください。
  - *セキュリティの原則*: そのセキュリティは、該当の保護データに対し適切かつ妥当ですか。

VI. 通知

本コントロールの実施、収集した PII、情報の使用に同意する権利、および（可能な場合）情報提供を却下する権利について、個人への通知が義務化されているか確認します。

- 企業が情報収集前の個人への通知をどのように義務付けているか定義します。
- 企業は、個人から情報を収集する前に、従業員、顧客、株主および他の関係者に書面または口頭で通知を提供することがあります。アメリカ合衆国政府では、そのような通知に、掲載済みのプライバシーポリシー、プライバシー保護法の声明書、プライバシー影響評価または*アメリカ合衆国連邦広報*に公開されている Statement of Records Notice (SORN)を含めることができます。顧客から情報を収集する民間企業では、公的に取得できるプライバシーポリシーが利用されます。本コントロールで情報収集する可能性のある個人には、どのような通知が妥当であるか説明してください。
- 通知を提供しなくてよい、またはできない場合、通知が必要なケースまたは通知を免除できる場合を定義してください。特定の法律に準拠する際に、通知が適切でないケースがあるかもしれません。その場合企業は、収集時に個人に直接通知を行うことで、どのように法律の目的が損なわれるのか説明します。
- 提供した通知がどのように本コントロールの目的や宣言されている用途に適合しているかを話し合ってください。最初の収集時に提示した通知が、その情報について記載されている用途にどう一致しているか説明してください。本コントロールを実施することで、通知が不十分な場合や、拒否あるいは同意の可能性に関わるリスクがどのように緩和されるか説明してください。
- 以下の FIP を検討してください。
  - *透明性の原則*: 本コントロールは、個人に十分な通知を提供することを認めていますか。
  - *用途制限の原則*: その情報は、個人に直接または公示を通じて提供された通知にある目的に限って使用されていますか。情報がその通知に明記された目的でしか使用されないことを確保するため、どのような手順が取り入れられていますか。
  - *個人参加の原則*: 情報の種類や、情報のセキュリティ、保持、廃棄などに対するコントロールといった通知の目的等も含んだアクセスや訂正などの救済について、企業は個人に通知を提供することが義務付けられていますか。

VII. データ保持

収集した情報や本コントロールで生成された情報を統制するため、適切な権限者（経営陣など）の許可を必要とする記録保持ポリシーの開発要件はありますか。

- 回答を提出する際、以下の FIP を検討してください。
  - *最小限の原則*: 本コントロールは、宣言されている目的に必要な情報しか使用させないようにできますか。本コントロールは、特定の目的を達成するために必要か、関係する場合に限り、保持している PII を管理するようにできますか。
  - *データ品質と完全性の原則*: PIA は、無関係か不要になったと判断される PII の破棄方法について、組織が要請するポリシーや手順を説明していますか。

VIII. 情報共有

本コントロールに対応するために必要とされる企業内外との情報共有範囲を説明してください。外部共有には、他企業、ベンダー、民間の業界グループまたは連邦、州、自治体、民族および地域政府、および他国の政府や公的機関との共有を含みます。

- 本コントロールに該当する一般的な州または自治体機関あるいは民間組織の種類をリストしてください。具体的な団体名ではありません。
- 組織が通常業務の一環として情報共有を行うために必要とされる契約を説明してください。
- 企業外で情報を共有することで発生し得るプライバシー関連のリスクを話し合ってください。そうしたリスクはどのように緩和できますか。
- 情報の共有が、記載されている目的や本コントロールのための初回収集時の用途にどのように適合しているか話し合ってください。

IX. 補償

企業は、本コントロールの実施時に、個人の PII が不適切に、あるいは不注意で開示されたか不正利用された場合、個人がその補償を求める手順を用意していなくてはなりません。こうした手順では、収集したデータや使用方法について個人が訴訟を起こすことを認めることもあります。

- FIP の *個人参加の原則*に該当する以下の問題を検討してください。
  - ある目的で取得された PII が、個人が知ることなく他の目的に使用されることを防ぐメカニズムを適用できますか。

X. 監査と説明責任

本コントロールに対応するためには、どのような技術あるいはポリシーベースの保護またはセキュリティ対策が必要になるか説明してください。情報共有手順、特殊アクセス規制等のコントロールなど、技術的およびポリシー保護の検討内容も含めてください。

- 本コントロールでは、自己監査が可能か、サードパーティーによる監査を許可しているか、あるいは適切な監視機関によるリアルタイムまたはフォレンジックレビューが可能かを話し合ってください。
- 本コントロールに対応している IT システムは、情報が不正利用された場合にそれを自動的に検知するツールを備えていますか？
- 本コントロールの全般または個別事項に関連して、どのようなプライバシートレーニング要件をユーザに提供するべきか、情報処理手順や情報の機密性も含めて説明してください。収

集した PII または本コントロールで生成された PII にアクセスできる個人にその情報を適切に扱わせるため、どのようなトレーニングを行うべきか説明してください。

- 情報共有契約、コントロール情報の新たな用途および他者によるコントロール情報への新規アクセスについて検討し、承認するために必要なプロセスと手順を話し合ってください。

Appendix G：CIS Critical Security Controls のカテゴライズ

イントロダクション

CIS CSC の Version6 を作成したときの大きな変化の 1 つは、各サブコントロールのカテゴリー（クイックウィン、可視化/特定、強化された情報セキュリティ構成と予防措置、高度なサブコントロール）の削除でした。これらのカテゴリーは、いくつかの理由で問題があるとされていましたし、使用するには一貫性がないことが指摘されていました。

しかし、その一方で、各コントロールの導入計画において優先順位付けするためにはカテゴリーがあった方がよく、特に導入計画を経営陣に説明する場合にも有用であることも指摘されていました。そこで、再度それらの視点に立ち返ってみることにしました。加えて、真に「高度」で時間とリソースというかなりの投資を必要とするサブコントロールを識別する際の助言も求められていました。

本ドキュメントでは、「Foundational（基本事項）」と「Advanced（高度な事項）」を区別するために、いくつかの補足説明を付加しつつ、それぞれのサブコントロールに対して以前と同様の分類スキームを提供するようにしています。

説明

CIS CSC のバージョン 5 では、それぞれのサブカテゴリーは以下の分類に分かれていました。

- **クイックウィン**：財務、手続き、アーキテクチャ、技術の面で環境を大きく変更することなくリスクを大幅に低減するサブコントロール、または最も一般的な攻撃に対する実質的かつ即時のリスク低減を実現するサブコントロール（ほとんどのセキュリティ対応組織がこれらの重要なコントロールを優先的に実施します）。
- **可視化／特定**： 組織がそのネットワークとコンピュータシステムを監視して、攻撃の試みの検知、侵入した位置の特定、すでに侵害されているマシンの特定、侵入した攻撃者の活動の中断、および攻撃元に関する情報の取得を行うためのプロセス、アーキテクチャ、および技術的な能力を改善するための手段。
- **強化された情報セキュリティ構成と予防措置**：攻撃者にとってメリットとなる可能性のある、システム管理者やエンドユーザによる不十分なセキュリティ慣習の防止を中心に、セキュリティ上の脆弱性の数と規模を低減し、ネットワークコンピュータシステムの運用を改善します。
- **高度なサブコントロール**：適用が困難であるか、適用コストが高いか、または商品化されたセキュリティソリューションより高度なスキルを持つ担当員を必要とする新たなテクノロジーまたは手続きの使用により実現する高度なセキュリティを提供するサブコントロールです。

バージョン 6.1 では、寄り単純に 2 つの分類システムにしました。その出発点として、ほとんどのサブコントロールが繰り越されているバージョン 5 から作業を始めました。

- **Foundational**：これらは、組織のネットワークやコンピュータシステムに対して、攻撃を検知し、攻撃起点を発見し、すでに侵害されたマシンを特定し、攻撃の拡散を断ち切り、攻撃元の情報を取得するといった一連のモニタリングを達成するために、プロセスやアーキテクチャ、技術的能力に対して不可欠な改善策を提供します。これらは、ともすると攻撃者に優位性を与えてしまうようなシステム管理者やエンドユーザの不適切な行動にも焦点をあてながら、ネットワーク化されたコンピュータシステムの運用を改善させ、セキュリティに関する脆弱性の件数と影響範囲を減少させます。
- **Advanced**：これらは、セキュリティレベルを最大水準にするために新たな技術やプロシージャを利用するサブコントロールです。しかし、このコントロールを導入するには、一般に普及してい

るセキュリティソリューションを採用する場合と比較して、導入が容易でなかったり、費用が高額だったり、高い技術スキルを有する人材が必要だったりします。

個々のサブコントロールのいくつかには、どちらかのカテゴリーに厳格には当てはまらない用語や表現、解釈が含まれているという指摘も受けていますので、プライマリとなるカテゴリー（Foundation もしくは Advanced の表中に「Y」で示しています。）を設定し、サブコントロールの他の側面を明確に分離するために文章を追加しました。

例えば、Foundational と定義されているサブコントロールであっても、高度なセキュリティプログラム上に構築しようとしているものであれば、注釈をつけています。これはお世辞にもエレガントなソリューションとはいえませんが、サブコントロールの大幅な改訂を行わずに有用なガイダンスを提供したいと思った結果です。CIS CSC を採用する組織は、CSC の段階的な実装に向けたロードマップを作成するために、現在置かれている状況下、技術的水準、リスクマネジメント等を鑑みながら各サブコントロールを解釈し、アクションを起こす必要があるのです。