情報システムにおける

セキュリティ コントロール ガイドライン

Ver.1.0

2022 年 5 月

一般社団法人ソフトウェア協会 Software ISAC

目次

1 序言

1.1 はじめに

情報セキュリティコントロールガイドライン（以下、「本ガイドライン」といいます。）は、組織における「セキュアな情報システムの維持」を目的とした要件と管理策のフレームワークを確立するため、Software ISAC のコミュニティ主導の取り組みにより策定されたガイドラインであり、情報システムの開発や運用設計の際に必要となる機能的および非機能的なセキュリティ管理策の定義を適切に行うためのさまざまな工夫がなされています。ここでいう「コントロール」とは情報セキュリティ維持のため対策事項であり、組織のネットワークやデバイス、データといった情報資産の識別、保護、検出、対応、復旧のために実践すべき事項を列挙しています。

本ガイドラインは、システム運用のライフサイクルを通して、さまざまな組織のニーズに答えられるようにセキュリティ面での管理策をまとめてあります。経営者とシステム管理者は、本ガイドラインを活用することで、自組織でのセキュリティ管理の充実度を知ることができ、現状と比較することで、将来のセキュリティ管理の優先順位の決定や、予算の獲得の根拠とするなど、新規に開発するシステムにおけるセキュリティ管理体制の過不足を発見することが可能となります。

残念ながら、本ガイドラインがあらゆる組織に対して完全なセキュリティ管理を提供できるとは考えていません。サイバーセキュリティの脅威は組織毎に異なり、さまざまな状況に対応できるような汎用化はほとんど困難といっても良いでしょう。しかし、ランサムウェアなどの被害を防ぐ、データの改ざんを防ぐ、電子メールから飛び込んでくる標的型攻撃を防ぐ、などのヒントを見つけることは可能です。
技術的に詳細な設定については、IPA 「情報システム開発契約のセキュリティ仕様作成のためのガイドライン」[1] を活用し、運用面や管理面での日々の業務の在り方については本ガイドラインをご活用下さい。

今後も、情報セキュリティコントロールガイドラインは、Software ISAC のコミュニティの主導によって更新されていきます。コミュニティでの建設的な意見と、トピックの充実のために、読者のご協力をお待ちしています。

1.2 ガイドラインの内容

本ガイドライン Ver.1 では、米国カルフォルニア州が「合理的なセキュリティ対策」として認定した、米国 CIS[2] Control v8 のキャッチアップを行った上で、証明書の管理などの CIS Control[3] での不足分を補う項目を紹介しています。CIS Control は、識別、保護、検出、対処、復旧といったセキュリティ管理のプロセスごとに項目が構成されていますが、本ガイドライン Ver.1 では、アカウント、ソフトウェア、データ、機器、ネットワークという単位で各々に識別、保護、検出、対処、復旧についてのプロセスについて紹介しています。また、セキュリティトレーニングとインデント対応のための組織が実践すべきプロセスも例示しています。

---

[1] https://www.softwareisac.jp/ipa/

[2] https://www.cisecurity.org/

[3] 日本語版の解説 https://www.lac.co.jp/lacwatch/people/20211025_002766.html

本ガイドラインの構成は、今後のフィードバックを得て将来的には変わる可能性はありますが、システム管理者だけでなく、経営者にとって分かりやすいセキュリティ管理単位として考慮しました。
各章では、冒頭に「管理プロセスを確立する」とあり、例えばネットワークの管理プロセスとしての、細分化された管理項目を解説しています。当然、組織によって管理手法や粒度は異なるものの、一般論として、どのような管理を行えばよいのかは、「管理プロセスを確立する」を読むだけで、IT 知識に乏しい経営者であってもおおよその理解が可能でしょう。
また、殆どのプロセスの確立の責任者は経営者として定義しています。これは、組織のセキュリティ管理において、経営者が一定の理解と責任を負うことで、組織全体のセキュリティコントロールの理解と浸透を狙っています。

個々の管理策の多くは、システム管理者が責任者となっています。現在のサイバーセキュリティの状況を考えると、場合によっては、さらに細かい粒度で対処する必要があります。その意味では、いわゆる「一人情シス」では、こなしきれない仕事量となることでしょう。しかし、セキュリティの維持を目的とするならば必要な仕事量であり、言い換えれば、そのような組織は根本的なリソース不足の課題を解決するべきであるということができます。

組織の規模に応じて、各管理策にはレベルを付与しています。「一人情シス」でも、可能な範囲の項目から着手し、責任者である経営との相互理解を深め、適宜、リソースの拡充を図ることが重要です。また、可能な限り、拡充されるリソースとしては、人員ではなく「自動化」であることが望まれます。機器の購入申請や承認、台帳管理にはワークフローが有効でしょうし、資産管理ツールを活用することで情報資産の取得が容易になります。自動化によって、セキュリティ管理が継続的なものになり、全体の負担も軽減されることとなります。

1.3 情報システムにおけるセキュリティ コントロール ガイドライン ライセンス

2　本ガイドラインの考え方と利用方法

本ガイドラインの基本的な考え方と、利用方法を解説します。

2.1 本ガイドランの考え方

以下に本ガイドラインが拠り所とする原則を解説します。プロセスの策定や実行時に判断に迷った場合など、本ガイドラインの適用が難しい局面での参考としてください。

2.1.1　識別の優先

識別されていない情報資産は保護できません。保護されていない情報資産は検出、対処、復旧が不可能です。つまり、識別されていない資産が組織内に存在した場合、その時点で組織は侵害されてしまうリスクが高いといわざるを得ません。

2.1.2　最小特権

権限というものは、常に必要最小限の権限しか付与されないという事が既定（Default）である必要があります。特に特権である管理者権限は期間的に限定的に付与されるべきです。万が一、永続的に管理者権限が付与されたアカウントが侵害を受けると、侵入者は管理者権限であらゆる操作が可能となってしまいます。そのため、特権が付与されなければならない機器、ソフトウェア、アプリケーション、Debugger、ツールは、厳格に管理され、ログを取得し異常の検出に努めなければなりません。

2.1.3　知る権利に基づくアクセス制御

すべてのデータは「知る権利」に基づきアクセス権が付与されるべきであり、たとえシステム管理者であっても、「知る権利」がなければアクセスできないのは当然のことです。システム管理とデータへのアクセス権は別であり、例えばバックアップオペレーターがユーザーのメールボックスを閲覧できてはなりません。また、高い権限を有するアカウントは、常時、監査されなければなりません。

2.1.4　攻撃表面の最小化

電子メール、Web 閲覧、仮想ネットワーク（VPN）接続は業務に必要な行為であり、特に VPN はコロナ禍によってかなり普及しました。一方で、攻撃側からみれば、これらは組織に侵入するために都合の良い接続点であり、当然、攻撃の対象となります。VPN がランサムウェアの主要な侵入口となっていることは周知の事実です。そのため、これらの接点への管理者業務を実施する場合は、限定的なアクセス制限と厳格な認証が必要となります。また、利用されていないソフトウェアコンポーネント、リモート操作ツール、コーデック、特権ユーティリティ、スクリプト等をアンインストールすることで、ソフトウェアの悪用や脆弱性の悪用の可能性が低くなります。

2.2 レベル

本ガイドラインは、組織の規模やミッションに応じて、L1、L2、L3 のレベルが割り当てられています。概ね、L1 は情報漏洩による被害が少ないと考えられる組織であり、L2 以上は大量の個人情報や重要な機密情報が存在していることを想定しています。

レベル	システム管理者	大量の個人情報や機密情報の存在
L1	システム管理者は他の業務と兼務、もしくは常駐していない	存在していない
L2	専従のシステム管理者が常駐	大量の個人情報、重要な機密情報が存在している
L3	専従のシステム管理者が常駐	CSIRT が設置されている

L3 は L2 と L1 のプロセスや要求事項をすべて満たすべきであり、L2 は L1 のプロセスや要求事項を満たさなければなりません。反対に、自らの組織を L1 と定義しても、リソースが許すのであれば、L2、L3 の項目を選択し、管理することは望ましい事といえます。

2.3 利用する前に

本ガイドラインは、最初に組織に応じた具体的な防御項目の選択、次いで、選択した防御項目の管理策の策定と実行を促すことを目的としています。そのため、取り組み当初は、厳格な PDCA サイクルの確立を目的にせず、状況に応じた柔軟な管理体制を立ち上げることを推奨します。

例えば、全組織のすべてのルーターなどのネットワーク機器の脆弱性管理を考えてみます。1,000 台以上の PC を保有している組織であれば、ネットワーク機器の所在と使用状況を把握し、ファームウェアのバージョンを取得するには、専従者がいても相当の工数がかかるでしょう。具体的には、サーバールームやフロア単位でのネットワーク機器の一覧の作成を行い、その後、拠点単位といった情報収の積み重ねとなるはずです。また、ネットワーク経由でルーターの設定が確認できない場合、現地に赴く必要があります。このように、脆弱性管理ひとつをとってみても膨大な作業が待ち受けており、一斉にロバストな環境を手に入れることは困難です。従って、リスクが小さいと判断されるものは劣後させ、リスクが高いものから、可能な範囲で小さな成功を積み上げ、最終的にプロセスを確立することを目指します。

故に、規程集を策定したり、承認プロセスを作ることを目的とせず、また、特定のシステムや管理者に権限を集中させるのが目的ではないことを念頭に置きましょう。

３章以降は、以下の構成となっています。各章はアカウント、ソフトウェア、セキュア開発、データ、機器、ネットワークの管理プロセスの確立と、トレーニング、インシデント対応のプロセス確立について述べています。

3 章　組織のアカウント管理プロセスを確立する
4 章　組織のソフトウェア管理プロセスを確立する
5 章　組織のデータ管理プロセスを確立する
6 章　組織の機器管理プロセスを確立する
7 章　組織のネットワーク管理プロセスを確立する
8 章 セキュア開発プロセスの確立
9 章 セキュリティトレーニングプロセスの確立
10 章 インシデント対応プロセスの確立

繰り返しになりますが、最初に各章冒頭の「プロセスの確立」の内容を簡単に理解した上で、それ以降の「プロセスの実行」項目を可能な範囲で実践し、最終的に、可能な範囲で自動化されたプロセスの確立を目指すことを推奨します。

2.4 利用方法

2.4.1　プロセスの確立

以下の例に基づき、解説します。

4　　組織のソフトウェア管理プロセスを確立する（プロセスの確立/経営層/L1）

組織が承認した、組織の機器にインストールできる、もしくは利用できるソフトウェア（これには、スクリプト、OSS、ライブラリ、クラウド、外部サービスを含む）の受け入れ、使用許可、脆弱性管理から廃棄までの管理プロセスを確立し、実行する。これには、所属、管理者、利用者、機器、利用目的を伴う申請、リスク評価、承認、ソフトウェア部品表管理 (SBOM)、受け入れ、設定・構築、アクセスコントロール、実行制御、ログ収集と保管、脆弱性管理、運用方法、保守、廃棄が含まれる。ソフトウェアの特性に応じた運用を慎重に検討する。例えば、電子メールや Web 閲覧は脅威の入り口になるため、利用者が管理者権限で運用することは避けなければならないし、これらの重要資産にアクセスできる環境での操作は制限されるべきである。保守が伴う場合は、期限、現地対応、リモート保守などの方法や、外部要員の立ち入りやアクセス、保存されているデータのアクセスの有無、証明書の場合は有効期限と更新計画などが、受け入れの際に明確になっていなければならない。

各章の冒頭には「~管理プロセスを確立する」とあり、管理プロセスの確立の概要、考え方や注意点が述べられています。括弧の中には「プロセスの確立」「経営者」「L1」とありますが、それぞれ、目的と責任者とレベルを表します。

管理プロセスは、組織の防御のための多数の管理策の集合といえます。例えば、システムを自ら開発する組織であれば「ソフトウェア部品表管理 (SBOM)」による OSS の管理が必要となってくるでしょうが、パ

ッケージソフトを利用するだけの組織であれば、「ソフトウェア部品表管理（SBOM)」は不要です。このように組織のおかれている状況に合わせてプロセスを確立させます。

2.4.2　プロセスの実行

以下の例に基づき、解説します。

4.1　　ソフトウェア管理

4.1.1　承認されたソフトウェア（プロセスの実行/システム管理者/L1）

組織によって承認されたソフトウェア以外のソフトウェアは使用してはならない。未承認のソフトウェアはすべてアンインストールしなければならない。可能であればソフトウェア実行制御機能を用いて、組織が承認したソフトウェアやコマンド、ライブラリ等だけが実行できるようにする。また、これには、ソフトウェア、コマンド等のリスク評価が含まれる。これは、ベンダーが非推奨としたコマンドや、明示的に必要とされない限りブロックすべきコマンドリストを用いて、定期的に評価を行う。

4.1.2　ソフトウェアのサポート状況の確認（プロセスの実行/システム管理者/L1）

組織が承認したソフトウェア、ライブラリ等の脆弱性情報や保守終了を月次で管理する。併せて、保守が終了したソフトウェア等を継続使用する場合の、防御設定や監視等の手順も含める。

「4.1.1 承認されたソフトウェア（プロセスの実行/システム管理者/L1）」では、承認されたソフトウェア以外は、アンインストールしなければなりません。小規模な組織では、インストールされたソフトウェアの一覧の監査で済みますが、大規模な組織では資産管理ソフト等の利用によって、未承認ソフトウェアの検出が必要となってきます。

また、「可能であれば」という条件付きでソフトウェア実行制御機能を利用して、リスク評価されたホワイトリスト、ブラックリストの適用を推奨しています。「Microsoft が推奨するブロックの規則」[4] では、不要であれば明示的に停止すべき Windows のコマンドが紹介されています。こうした情報を参考にして、悪用されるコマンドのブロックを見直します。

「4.1.2 ソフトウェアのサポート状況の確認（プロセスの実行/システム管理者/L1）」では、ソフトウェアのサポート状況を月次で管理することが求められています。やむなくサポート切れのソフトウェアを使用せざるを得ない場合、ネットワークの切り離しやリムーバブルメディアの利用の禁止や、ログ監視による異常の検出などの防御策が考えられますが、こうした対策も併せて管理することが求められています。

2.5 システム管理者の取り組み

最初に、各「プロセスの実行」と、組織のセキュリティ管理の状況を照らし合わせます。最初は、管理の粒度にはこだわらず、実施しているのか、実施していないのか、といった程度の評価で十分でしょう。もし、実施済であるならば、自動化や管理の細分化や連携を考えてみてはどうでしょうか。また、実施していない項目があれば、その項目を実施しなかった場合のリスクや脅威を評価して優先度を決定し、優先度の高い項目の実施を阻害する要因やリソースの不足を調査します。とりわけ、重要情報の「識別」と「保護」を最初に重点的に取り組むことを強く推奨します。

---

4 https://docs.microsoft.com/ja-jp/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

セキュリティ管理のすべてが、完全に完璧に実施されることは困難といわざるを得ません。しかし、組織の従業員、経営者の理解があれば、日々の業務の積み重ねで確実に結実するでしょう。その意味において、セキュリティ管理と業務遂行のバランスが重要です。リスクや脅威を組織と共有し、組織全体で課題解決を図らなければなりません。

2.6 経営者の取り組み

セキュリティ知識の少ない経営者は、まず、システム管理者に対して、L1 の項目がどの程度実現できているかを質問するとよいでしょう。そして、実現できていないプロセスについて、理由や制限事項を共有することが重要です。実現できていないプロセスのリスクや課題を共有し、そのプロセスが重要資産や個人情報にどのように影響を及ぼすかを説明させ、また、発生する可能性を検討し、経営者自らが優先順位をつけて実施を促すべきです。

場合によってはシステム管理者がプロセスを理解できない場合があるかもしれません。そうした場合は、第三者のアドバイスやコンサルティングを受けるべき項目となります。セキュリティコンサルタントや、セキュリティ製品ベンダーに提案を依頼するのも良いでしょう。

組織によってはリソースが不足し、また、予算が限られるケースがあるでしょう。そのような場合は、機密情報に最も影響を与える、優先順位の高いプロセスの実現に集中すべきです。その意味で、実現された項目を単純な実現率などで評価するのは意味がなく、優先順位の質と量をバランスよく評価することが必要です。

セキュリティの管理プロセスによっては現業に支障をきたしたり、生産性を下げることがあり得ます。現場は、業務の遂行に障害となるプロセスの導入に反対するかもしれません。このような場合は、優先順位の高い機密情報に影響があった場合の、組織のダメージやリスクを経営者自ら説明することが重要です。システム管理者と現場の協働と協調がなければ、セキュリティの維持は困難です。

3 組織のアカウント管理プロセスを確立する（プロセスの確立/経営層/L1）

組織のすべてのアカウントの作成、変更、廃棄プロセスを確立し、実行する。ユーザーアカウントには、一般ユーザーアカウント、管理者アカウントとシステムが利用するサービスアカウントがある。これには、少なくともアカウント名に対する個人名もしくは、管理者名、メールアドレス、所属、サービスアカウントの場合はそのシステム、有効期間（開始/終了）、可能な範囲でアカウント作成の申請者、アカウントの有効/無効、無効の場合の理由、最終アクセス日、長期間アクセスのないアカウント、ログ要件などを一覧として管理する必要がある。アカウント作成・廃棄は承認プロセスを経なければならず、ユーザーアカウントの原始データは人事システムと連携することが望まれる。組織のニーズに従って外部パートナーへのアカウント付与は、適切な承認管理がされなければならない。すべてのアカウントは定期的な監査を行い正当性をチェックする。

（互換性：CIS Ctrl 5.1 Establish and Maintain an Inventory of Accounts）

3.1 アカウント管理

3.1.1 承認されたアカウント（プロセスの実行/システム管理者/L1）

アカウントの開設、権限付与、グループの参加、これらの変更、改廃等は、すべて組織の承認を得なければならない。

3.1.2 一元化されたアカウント管理（プロセスの実行/システム管理者/L1）

アカウント管理は、ID 管理システム、ディレクトリ等で一元管理しなければならない。

3.1.3 デフォルトアカウントの変更（プロセスの実行/システム管理者/L1）

可能な限り、すべての機器、ソフトウェアのデフォルトアカウントは使用せずに変更する。多要素認証が使用できない場合、可能な限り長く漏洩していないパスフレーズを使用する。

3.1.4 独立した管理者アカウント（プロセスの実行/システム管理者/L1）

管理者アカウントは管理業務だけに使用されなければならず、一般業務に使用されてならない。

3.2 アカウント保護

3.2.1 認証認可システムの管理（プロセスの実行/システム管理者/L1）

最低半期に一度、すべてのユーザーアカウント、管理者アカウントの使用目的、権限、変更の有無を評価する。これには、ディレクトリ、Radius、802.1X、WPA、VPN、クラウドサービス、SOAP、Auth、SMTP-AUTH などが含まれる。

3.2.2 管理者アカウントにおける多要素認証（プロセスの実行/システム管理者/L1）

可能な限り管理者アカウントは MFA を使用しなければならない。管理者アカウントは共有されてはならず、必ず、個人に紐づき、否認が防止されなければならない。

3.2.3 限定された特権付与（プロセスの実行/システム管理者/L1）

永続的な特権の付与は限定されなければならず、原則として、特権は、目的と有効期限を限定し付与されなければならない。

3.2.4　最小権限での運用（プロセスの実行/システム管理者/L1）

一般業務は最小権限で実行されなければならない。一般業務を行うユーザーアカウントが管理者もしくは管理者グループに所属してはならず、管理者権限で一般業務を実行してならない。管理者権限は時限的に付与されるべきで、永続的に付与されてはならない。

3.2.5　アカウントの無効化（プロセスの実行/システム管理者/L1）

ユーザーが 2 週間以上の休職、長期休暇、若しくは退職する場合は、組織の承認を得て無効化しなければならない。退職の場合、実質的な業務に携わらなくなる日をもって無効化する。

3.2.6　長期間使用されなかったアカウント（プロセスの実行/システム管理者/L1）

30 日間使用されなかったアカウントについて、その理由を監査する。休職、退職等に応じて、無効化、削除を速やかに行う。削除する場合は、180 日間を目安に無効化したのちに削除する。削除の際は、アカウントと紐づいているデータへのアクセス権限に注意する。

3.2.7　漏洩パスワードの検証（プロセスの実行/システム管理者/L1）

組織が使用しているパスワードが漏洩していないか、4 半期に 1 回以上チェックする。漏洩が判明した場合は、即座に改訂する。漏洩がない限り、定期的変更を求めず、複雑性を求めない。16 桁以上のパスフレーズを推奨する。パスフレーズは、3 つ以上の単語の組合せなどとする。

3.2.8　多要素認証の導入（プロセスの実行/システム管理者/L2）

組織のすべてのアカウントに可能な限り多要素認証（MFA）を使用する。MFA が使用可能なら PIN は 6 桁以上とする。MFA が使用できない場合は 16 桁以上のパスフレーズを設定する。パスワードはすべてユニークでなければならない。

3.3 アクセス制御

3.3.1　一元化されたアクセスコントロール管理（プロセスの実行/システム管理者/L1）

アクセスコントロール管理は、ID 管理システム、ディレクトリ等で一元管理しなければならない。

3.3.2　知る必要に基づくアクセス制御（プロセスの実行/システム管理者/L1）

組織のデータの特性に基づいた知る必要に基づくアクセス制御を設定する。これにはファイル、データベース、アプリケーション、クラウド、サービス等での認証と読取、書込、変更、削除などの操作権限、ログの取得、バックアップ及び復旧の権限設定が含まれる。

3.3.3　サービスアカウントの管理（プロセスの実行/システム管理者/L2）

システムが利用するサービスアカウントの使用目的、権限、変更の有無を評価する。システムがサービスアカウントのパスワードを自動変更しない場合、四半期に一度、推測困難なパスワードを更新する。

3.3.4　役割ベースのアクセス制御（プロセスの実行/システム管理者/L2）

役職、職務に応じたアクセス権を設定し文書化して管理し、役割ベースのアクセス制御を実行する。組織内の異動や職務が変わった場合は、確実にアクセス権が変更されていることを検証しなければならない。兼務で職位が異なる場合のアクセス権については慎重に検討する。

4 組織のソフトウェア管理プロセスを確立する（プロセスの確立/経営層/L1）

組織が承認した、組織の機器にインストールできる、もしくは利用できるソフトウェア（これには、スクリプト、OSS、ライブラリ、クラウド、外部サービスを含む）の受け入れ、使用許可、脆弱性管理から廃棄までの管理プロセスを確立し、実行する。これには、所属、管理者、利用者、機器、利用目的を伴う申請、リスク評価、承認、ソフトウェア部品表管理 (SBOM)、受け入れ、設定・構築、アクセスコントロール、実行制御、ログ収集と保管、脆弱性管理、運用方法、保守、廃棄が含まれる。ソフトウェアの特性に応じた運用を慎重に検討する。例えば、電子メールや Web 閲覧は脅威の入り口になるため、管理者権限で運用されることは避けなければならないし、これらの重要資産にアクセスできる環境での操作は制限されるべきである。保守が伴う場合は、期限、現地対応、リモート保守などの方法や、外部要員の立ち入りやアクセス、保存されているデータのアクセスの有無、証明書の場合は有効期限と更新計画などが、受け入れの際に明確になっていなければならない。

4.1 ソフトウェア管理

4.1.1 承認されたソフトウェア（プロセスの実行/システム管理者/L1）

組織によって承認されたソフトウェア以外のソフトウェアは使用してはならない。未承認のソフトウェアはすべてアンインストールしなければならない。可能であればソフトウェア実行制御機能を用いて、組織が承認したソフトウェアやコマンド、ライブラリ等だけが実行できるようにする。また、これには、ソフトウェア、コマンド等のリスク評価が含まれる。これは、ベンダーが非推奨としたコマンドや、明示的に必要とされない限りブロックすべきコマンドリストを用いて、定期的に評価を行う。

4.1.2 ソフトウェアのサポート状況の確認（プロセスの実行/システム管理者/L1）

組織が承認したソフトウェア、ライブラリ等の脆弱性情報や保守終了を月次で管理し、対応するプロセスを確立し実行する。これには、保守が終了したソフトウェア等を継続使用する場合のプロセスも含まれる。

4.1.3 承認された署名済みスクリプト（プロセスの実行/システム管理者/L1）

ソフトウェア実行制御機能や電子署名を用いて、組織が承認したスクリプトだけが実行できるようにする。明示的に必要とされていない限り、スクリプトは実行禁止とする。スクリプトの実行は組織の承認が必要であり、承認のための受け入れ、リスク評価、承認、廃棄までのプロセスを管理し、実行する。

4.1.4 安全なソフトウェアの設定構成（プロセスの実行/システム管理者/L1）

組織の機器、オペレーティングシステム、アプリケーションの安全に構成する。これには、暗号化、脆弱な初期設定の変更や、脆弱なプロトコルなどが明示的に使用禁止に設定するなどが含まれる。

4.1.5 不要なソフトやサービスのアンインストール（プロセスの実行/システム管理者/L1）

組織の機器、ソフトウェアの不要なサービスをアンインストールする。これには、ファイル共有、Web サービス、管理機能、ゲームアプリケーション、メールアプリケーション、Video 再生やコーデック、スクリプトなどが含まれる。

4.1.6 時刻同期（プロセスの実行/システム管理者/L1）

ソフトウェアの時刻を同期する。可能であれば、3 つのタイムソースを設定する。判定が困難になるためタイムソースを 2 つ指定することはしない。

4.1.7　資産管理ツールによるソフトウェアの検出（プロセスの実行/システム管理者/L2）

資産管理ツールを利用し、機器や機器にインストールされたソフトウェアを検出し、未承認ソフトウェアや脆弱性のあるバージョンの対処を最低でも月に 1 回以上行う。

4.2 マルウェア、脅威対策

4.2.1　マルウェア対策の実行（プロセスの実行/システム管理者/L1）

マルウェア対策ソフトを設定し、実行する。これには、端末、サーバー、スマートフォン、IoT 機器、複合機などが含まれるがこれに限らない。マルウェア対策ソフトが設定できない機器の一覧が作成され、代替策が実施されていること。ソフトウェアの動作に影響がある場合は、ソフトウェアの改修を実施する。

4.2.2　マルウェア対策ソフトの自動更新（プロセスの実行/システム管理者/L1）

すべてのマルウェア対策ソフトのパターンファイルは最低 1 日に 1 回以上、自動更新されなければならない。

4.2.3　マルウェア対策ソフトの一元管理・監視（プロセスの実行/システム管理者/L1）

マルウェア対策ソフトは一元管理・監視されなければならない。

4.2.4　振る舞い検知と AMSI に対応したマルウェア対策ソフト（プロセスの実行/システム管理者/L1）

マルウェア対策ソフトは振る舞い検知機能や、マルウェア対策スキャンインターフェース（AMSI）を搭載しているものを使用することが望ましい。これらの機能が正しく動作していることを確認する。

4.2.5　脅威情報の入手（プロセスの実行/システム管理者/L2）

情報共有が許可されている機関、組織、コミュニティから継続的に脅威情報や脆弱性情報を入手する。入手した情報は TLP 等に従って管理されなければならない。
これには、犯罪者たちの活動状況、ランサムウェアなどが利用する脆弱性や侵入経路、売買されるマルウェアや資格情報（ID/PW、IP アドレス）、標的型攻撃が利用するテクニックなどが含まれるがこれに限ったものではない。得られた情報をもとに強化設定を行い、ユーザーに共有し注意喚起をするなどが含まれる。

4.2.6　セキュリティイベントの閾値の見直し（プロセスの実行/システム管理者/L2）

組織のセキュリティイベント対策管理プロセスに基づき、月次 1 回以上、セキュリティ警告等の閾値を見直す。これには、最新の攻撃手法の分析情報や組織内のセキュリティ警告のトレンド分析に基づく必要がある。

4.3 ソフトウェアの保護

4.3.1　オペレーティングシステムの自動更新（プロセスの実行/システム管理者/L1）

オペレーティングシステムの修正プログラムはリリース後、速やかに自動的に適用されなければならない。但し、デグレード（直し壊し）の恐れがある場合は、この限りではない。

4.3.2　アプリケーションの自動更新（プロセスの実行/システム管理者/L1）

アプリケーションの修正プログラムはリリース後、速やかに自動的に適用されなければならない。但し、デグレード（直し壊し）の恐れがある場合は、この限りではない。

4.3.3　ソフトウェアの脆弱性管理（プロセスの実行/システム管理者/L1）

組織のすべてのソフトウェア（ファームウェアも含まれる）の脆弱性管理を実行する。これには、脆弱性情報や適用情報の入手、適用すべきシステムの一覧、適用しなかった場合のリスクの評価、修正プログラムのテスト適用、バックアップと本番適用、代替策の適用、当該システムの切り離し、切り戻し、運用停止、変更管理などが含まれる。

4.3.4　適切なログの保存（プロセスの実行/システム管理者/L1）

組織の監査ログプロセスに基づき、ソフトウェアのログが適切なストレージに保存されていることを月次 1 回以上確認する。

4.3.5　ブラウザと電子メールの運用ルール（プロセスの実行/システム管理者/L1）

組織のブラウザと電子メールの運用ルールを策定し、実行する。これには、ブラウザと電子メールクライアントの脆弱性管理と、ユーザートレーニングが含まれる。

4.3.6　ブラウザと電子メールのアドオン管理（プロセスの実行/システム管理者/L1）

組織のブラウザと電子メールの運用ルールに基づき、組織が承認したブラウザ、電子メールクライアントのアドオン、拡張機能だけが使用されているかを四半期に 1 回以上監査する。

4.3.7　DMARC 対応した電子メール（プロセスの実行/システム管理者/L1）

組織の電子メールに Sender Policy Framework (SPF) と DomainKeys Identified Mail (DKIM) を導入し、Domain-based Message Authentication, Reporting, and Conformance (DMARC) を検証する。

4.3.8　電子メールでブロックされるファイル（プロセスの実行/システム管理者/L1）

組織の電子メールサーバー、電子メールクライアントで .scr、.exe、.pif、.cpl など などの実行形式やマクロファイルをブロックする。

4.3.9　電子メールサーバーでのスピアフィッシング対策（プロセスの実行/システム管理者/L1）

組織の電子メールサーバーに対してサンドボックスを設定し、悪意ある添付ファイルのスキャンや埋め込みリンクのスキャンを導入、維持する。

4.3.10 コマンドラインのログ収集（プロセスの実行/システム管理者/L1）

コマンドラインのログを収集する。これには、BASH、Windows コマンドライン、PowerShell などが含まれる。コマンドラインのログには ID/Password や組織の重要なアカウント情報が含まれる場合があるため、慎重なアクセス権限設定を行い、暗号化や保存先のセグメントを変更するなどの措置を講じる。

4.3.11 リムーバブルメディアの自動実行の無効化（プロセスの実行/システム管理者/L1）

リムーバブルメディアの自動実行機能、自動再生機能を無効にする。

4.3.12 エクスプロイト防止機能の有効化（プロセスの実行/システム管理者/L1）

OS もしくはマルウェア対策ソフトが提供するエクスプロイト防止機能を有効にする。

4.3.13 証明書のライフサイクル管理と保護（プロセスの実行/システム管理者/L1）

各種証明書のライフサイクル管理を行う。有効期限が切れた際の影響を事前に把握し、適切に更新、失効されること。認証用証明書、署名用証明書などの証明書は、ハードウェアトークン、TPM 等のハードウェアで保護する。秘密鍵はエクスポートできないように設定する。P12 形式の証明書はオフラインで保存され、適切なパスフレーズが設定されなければならない。

4.3.14 外部公開されたアプリケーションの多要素認証（プロセスの実行/システム管理者/L1）

可能な限り、外部公開されている組織のアプリケーション、クラウドサービス等は MFA を使用しなければならない。

4.4 クラウド

4.4.1 組織の利用しているクラウドサービス管理プロセスを確立する（プロセスの確立/経営層/L1）

組織が利用しているクラウドサービス、外部サービスの管理プロセスを確立し、実行する。これにはソフトウェア管理プロセスに加えて、サービス利用開始、終了の承認、サービス名、管理インターフェースの URL、管理者アカウント、利用部門、利用者、サポート連絡先、SLA、費用、データやアカウントの保護、ソフトウェア部品表管理、ネットワーク要件、ログ要件、認証要件、データ廃棄要件、バックアップ要件、脆弱性管理、クラウドサービスのコンプライアンス適合評価などが含まれる。

4.4.2 クラウド管理インターフェースの保護（プロセスの実行/システム管理者/L1）

組織が利用しているクラウドサービスの管理インターフェースのアクセス制限を行う。これには、多要素認証の採用、接続元 IP アドレス制限、長いパスフレーズの採用、管理担当者ごとの異なる ID の割り当て、管理担当者のロール付与、全体管理者の限定的付与などを実行する。

4.4.3 クラウドサービスの廃止手順の策定（プロセスの実行/システム管理者/L1）

サービスの廃止手順を定め、実行する。これには、アカウントの無効化、インスタンスの廃止、データの安全な廃棄、フローやマイクロサービスの廃止などがある。

4.4.4 クラウドサービスの監視（プロセスの実行/システム管理者/L1）

サービスの正常性、機能更新、機能廃止、不具合、脆弱性及び代替手段などを継続的に取得し、評価、対処する。

4.4.5 クラウドサービスのログ収集（プロセスの実行/システム管理者/L1）

組織の監査ログプロセスに基づき、脅威の検出を目的として、クラウドサービスや外部サービスの異常なイベントを検出する。これには、ログオン失敗、権限変更、Kernel による実行阻止、不正なアクセス、異常なコマンドラインなどがある。可能な限り自動化すること。

4.4.6　クラウドサービスの監査（プロセスの実行/システム管理者/L2）

年に 1 回以上サービスのセキュリティ要件に基づく、データ保護、アクセス管理、データ廃棄、ログ要件、監査要件について、組織の定めた要件に沿っているかを監査する。組織の要件を満たさない場合は、サービスを中止、廃棄するか、もしくは保護手段を確立し、継続的に監査を実行する。

4.4.7　クラウドサービスの情報セキュリティレベルの評価（プロセスの実行/システム管理者/L2）

年に 1 回以上、サービスごとに対する、機密性、完全性、可用性を評価する。

4.4.8　クラウドサービスのコンプライアンス適合状況の評価（プロセスの実行/システム管理者/L2）

年に 1 回以上、サービスのコンプライアンス適合状況を把握し、組織のコンプライアンスとの整合性を評価する。これには、マイナンバー法、個人情報の保護に関する法律などの法律や自治体の定めた条例、ISMAP、FISC、PCIDSS、GDPR、ISO 27001/27017/27018 等との整合性が含まれる。

4.5 ソフトウェアの検出

4.5.1　組織内のソフトウェアの脆弱性スキャン（プロセスの実行/システム管理者/L2）

月次 1 回以上、脆弱性スキャナーを使用して、組織内の資産に脆弱性が存在しないこと、安全な設定が維持されていることを確認する。可能であれば、脆弱性スキャナーには SCAP 準拠のものを使用する。

4.5.2　公開されているソフトウェア脆弱性スキャン（プロセスの実行/システム管理者/L2）

月 1 回以上、脆弱性スキャナーを使用して、外部に公開している組織の資産に脆弱性が存在しないこと、安全な設定が維持されていることを確認する。

4.5.3　ホストベースのファイアウォールのログ収集（プロセスの実行/システム管理者/L2）

組織の監査ログプロセスに基づき、ホストベースのファイアウォールのログを収集し、異常を検出する。これには、廃棄されたパケットや正常なパケットが含まれる。ログは適切にローテーションされなければならない。

4.6 ソフトウェアへの対処

4.6.1　未承認ソフトウェアへの対処（プロセスの実行/システム管理者/L1）

組織が承認していないソフトウェア、ライブラリの使用を禁止する規程を整備し、実効性を担保するための規程と監査方法を確立し、実行する。

4.6.2　修正プログラムや代替措置が提供されない脆弱性（プロセスの実行/システム管理者/L2）

修正プログラムや代替措置が提供されない脆弱性が発生した場合の、リスク評価、保護、監視、改修措置を計画し、実行する。

5　組織のデータ管理プロセスを確立する（プロセスの確立/経営層/L1）

組織のデータの特性に基づいた管理プロセスを確立し、実行する。これには、保存場所、デバイス、ネットワーク経路、機密度、暗号化、知る必要に基づくアクセス制限（これにはドキュメント、ファイル、データベース、アプリケーション、クラウド、サービス等での認証と読取、書込、変更、削除などの操作権限とログ収集と保管が含まれる）、バックアップの方法、場所と復旧及びその権限、保存期間、法定要件、重要資産や個人情報を示すラベリング、データの流れと廃棄に関する要件をまとめる。また、長期間アクセスのないデータの廃棄手順を定め、実効性を担保する。重要資産、個人情報等は、アクセス制御管理プロセスとともに定期的に監査する。

5.1 データの識別・管理

5.1.1　データにラベルを付与する（プロセスの実行/システム管理者/L1）

データにラベルを付与し、分類する。ラベルには、「極秘」、「秘密」、「関係者外秘」、「公開」などがあげられるが、情報が漏洩した際の事業上の影響をもとに策定される必要がある。ラベルに基づき、例えばアプリケーションが「個人情報取扱中」のメッセージや、アイコンを表示したり、自動的に暗号化するなどに活用される。

5.1.2　データの保存期間と廃棄（プロセスの実行/システム管理者/L1）

データの保存期間を定め、必要に応じて保存期間を延長、もしくは廃棄を行う。廃棄には、バックアップの廃棄が含まれる。

5.1.3　クラウドサービスが取り扱うデータの管理（プロセスの実行/システム管理者/L1）

半期に 1 回、サービスごとに、データの機密度、データ量、利用するソフトウェアやシステム、保存期間、法規制の影響、サービス停止や情報漏洩が発生した場合の事業への影響と対応策などを検討し、実行する。

5.1.4　機密データの監査（プロセスの実行/システム管理者/L1）

機密度の高いデータは一覧を作成し、アクセス制限の監査を行う。機密データは重要性に応じて、四半期、半期、1 年に 1 回以上、重要性の見直しを行う。

5.1.5　不可逆的な廃棄（プロセスの実行/システム管理者/L1）

データを不可逆的に廃棄する。機密性の高いデータが保存されたストレージに関しては、別途、ストレージの廃棄基準を策定し、それに従う。

5.1.6　ドキュメント管理（プロセスの実行/L1）

組織のアプリケーションで管理されていないドキュメントデータの管理を実行する。これには、手書きの申込書や、アプリケーションから出力された紙のデータや書類、電子ワークフロー、電子メール、SNS に添付されたファイル、コミュニケーションツールで共有されるファイルなどがある。重要資産、個人情報などのラベリングや鍵のかかる保管方法、廃棄方法について監査する。

5.1.7　データ損失防止（プロセスの実行/システム管理者/L2）

データ損失防止機能などにより、機密情報を保護し、把握する。これには、不適切な共有や、本来権限のないユーザーによる上書きや変更、個人情報やクレジットカード情報の電子メール送信などがある。

5.2 データの保護

5.2.1 機密データのアクセスログ（プロセスの実行/システム管理者/L1）

機密データのアクセスログを取得する。これには、読み込み、書き出し、変更、削除などの操作と、アクセス権限の追加、変更、削除などが含まれる。

5.2.2 機密データの暗号化（プロセスの実行/システム管理者/L1）

組織のデータ管理プロセスに基づき、ストレージの機密データを暗号化する。機密度と知る必要に基づくアクセス制限に応じて、共通鍵暗号、公開鍵暗号などを適切に選択する。暗号スイートや暗号化手法は、半年に 1 回見直す。

5.2.3 機密データの分離（プロセスの実行/システム管理者/L1）

機密性の高いデータと機密性の低いデータを分離して処理および保存する。ネットワーク分離と通信中の暗号化も考慮される必要がある。

5.2.4 重要資産に対する詳細ログの構成（プロセスの実行/システム管理者/L1）

組織の監査ログプロセスに基づき、重要資産に対する詳細なアクセスログを構成する。可能な限り、タイムスタンプ、アクセス先 IP アドレス、アクセス元 IP アドレス、ユーザー名、マシン名、イベントソース、アクセス内容を含める。

5.2.5 バックアップデータの暗号化（プロセスの実行/システム管理者/L2）

バックアップデータを暗号化する。

5.3 バックアップ

5.3.1 バックアップからの復旧プロセスの確立（プロセスの確立/システム管理者/L1）

組織のデータのバックアップと復旧プロセスを確立し、実行する。これには、システムごとにランサムウェアに汚染された場合を想定し、バックアップするデータやデータベースの特定、バックアップのタイミングと頻度、バックアップの冗長性、復旧の手順、優先順位、バージョン管理、他のシステムとの整合性の確保、バックアップデータの保管先や保護、トレーニングなどが含まれる。

5.3.2 バックアップの自動化（プロセスの実行/システム管理者/L1）

バックアップのスケジュール、バージョン、保存場所、保存期間を決定し、自動化する。

5.3.3 バックアップの冗長化（プロセスの実行/システム管理者/L1）

データの重要度に応じて、異なるセグメントやクラウドへの隔離、オフラインでの保存を実施する。

5.3.4 復旧テスト（プロセスの実行/システム管理者/L1）

半期に 1 回以上、バックアップデータからの復旧をテストする。

5.4 データの検出

5.4.1　機密データの不正アクセスの検出（プロセスの実行/システム管理者/L1）

組織の機密データのログから、不正なアクセスを検出する。機密データの重要度に応じて、日次、週次、月次で検出する。

5.5 データの対処

5.5.1　不正アクセスへの対処（プロセスの実行/システム管理者/L1）

不正なアクセスを行ったアカウントの無効化とアクセス範囲、漏洩、改ざん等を調査し、対処する。アクセス権限の取得の原因を調査し、対処する。

6　組織の機器管理プロセスを確立する（プロセスの確立/経営層/L1）

組織のデータを扱う PC、サーバー、仮想マシン、スマートフォン、ネットワーク機器、IC カードリーダー、USB デバイス、Bluetooth デバイス、ストレージ、IoT デバイス、監視カメラ、センサー、複合機、プリンター、その他の機器等の管理プロセスを確立し、実行する。これには、所属、管理者、利用者、利用目的、ネットワーク情報等を伴う申請、リスク評価、承認、受け入れ、設定・構築、ログ収集と保管、脆弱性管理、保守、廃棄までの規程やルール整備が含まれる。デバイスの特性に応じた管理を検討しなければならない。例えば組織のスマートフォンや持出可能な PC にはリモートワイプの設定や、紛失、盗難の場合の申請や処理のための規程整備が求められる。保守を伴う場合は、期限、センドバック、現地対応、リモート保守などの方法や、外部要員の立ち入りやアクセス、保存されているデータのアクセスの有無などが受け入れの際に明確になっていなければならない。

6.1 デバイス管理

6.1.1　機器の受入と資産管理（プロセスの実行/システム管理者/L1）

デバイスの特性に応じた受入プロセスを実行する。これには、デバイスの特性に応じた管理者、利用者、目的、ネットワーク情報、リスク評価、管理方法を伴う申請と、管理者による承認、文書化、特性に応じた実際の管理がなされなければならない。

6.1.2　機器の廃棄（プロセスの実行/システム管理者/L1）

デバイスの特性に応じた廃棄を行う。廃棄にあたっては、デバイスの特性に応じ、メモリ、ストレージ、設定情報を初期化しなければならない。

6.1.3　時刻同期（プロセスの実行/システム管理者/L1）

組織の監査ログプロセスに基づき、端末、サーバー、スマートフォン、IoT 機器等の時刻を同期する。可能であれば、3 つのタイムソースを設定する。

6.1.4　監査ログの設定と保存期間（プロセスの実行/システム管理者/L1）

監査ログを最低過去 1 年分保持する。可能であれば、定期的にオフサイトもしくはオフラインに移動し保全する。

6.1.5　機器のリスク評価（プロセスの実行/システム管理者/L2）

機器の特性に応じたリスク評価を行い、保護方法を決定する。可用性、完全性、真正性の確保の観点から、人的、物理的、技術的なリスクを分析する。例えば、物理的な制限のある入退出が制限されたサーバールームに設置されたファイアウォールと、業務執行フロアに設置された LAN 接続された複合機、ゲストフロアのゲスト用無線 LAN 機器、共用 EPS に設置されたルーターでは、それぞれ人的、物理的、技術的な保護の方法は異なる。

6.2 デバイスの保護

6.2.1　デバイスの脆弱性管理（プロセスの実行/システム管理者/L1）

組織のすべてのデバイスのファームウェアの脆弱性管理を実行する。これには、脆弱性情報や適用情報の入手、適用すべきシステムの一覧、適用しなかった場合のリスクの評価、修正プログラムのテスト適用、バックアップと本番適用、代替策の適用、当該システムの切り離し、切り戻し、運用停止、変更管理などが含まれる。

6.2.2　安全なデバイスの設定構成（プロセスの実行/システム管理者/L1）

デバイスを安全に構成する。これには、暗号化、脆弱な初期設定の変更や、脆弱なプロトコルなどが明示的に使用禁止に設定するなどが含まれる。

6.2.3　デバイスのロックアウト（プロセスの実行/システム管理者/L1）

すべての端末とサーバー、スマートフォンはデバイスのロックアウトを設定する。15 分以内に 5 回以上、認証に失敗した場合は、15 分間以上ロックアウトする。

6.2.4　スマートフォンのリモート・ワイプ・プロセス（プロセスの実行/システム管理者/L1）

組織のスマートフォンのリモート・ワイプ・プロセスを確立し、実行する。ノート PC、スマートフォンは紛失、盗難、退職退社などの必要に応じてリモートワイプできなければならない。

6.2.5　自動ロック（プロセスの実行/システム管理者/L1）

すべての機器、端末、サーバーは、15 分以上操作されていない状態が続いた場合、ロックされなければならない。スマートフォンは 2 分でロックされなければならない。ロック解除は認証を必要とする。

6.2.6　ストレージの暗号化（プロセスの実行/システム管理者/L1）

端末、サーバーのストレージを暗号化する。これは、ストレージデバイスを他の端末、サーバーに接続され、内容の読み出しを防ぐものである。暗号鍵はハードウェア（TPM、HSM)に保存されることが望ましい。

6.2.7　リムーバブルメディアの暗号化（プロセスの実行/システム管理者/L1）

リムーバブルメディアに記録されるデータはすべて暗号化する。

6.2.8　スマートフォンの組織データの分離（プロセスの実行/システム管理者/L1）

BYOD を導入している場合は、必要に応じてスマートフォンは組織データと個人データを分離できるよう設定する。

6.2.9　リモートアクセスにおける多要素認証（プロセスの実行/システム管理者/L1）

組織のネットワークに VPN 等でリモートアクセスする場合は、MFA を使用しなければならない。

6.3 デバイスの検出

6.3.1　サーバーのファイアウォールとログ（プロセスの実行/システム管理者/L1）

すべてのサーバーは必要最低限のポートだけが許可されるように、ファイアウォールが設定され、ログが取得され、異常を検出しなければならない。

6.3.2　端末のファイアウォールとログ（プロセスの実行/システム管理者/L1）

すべての端末は必要最低限のポートだけが許可されるように、ファイアウォールが設定され、重要度に応じてログが取得され、異常を検出しなければならない。

6.3.3　リムーバルメディアの自動スキャン（プロセスの実行/システム管理者/L1）

マルウェア対策ソフトはリムーバブルメディアが接続された際に自動スキャンをしなければならない。

6.3.4　ホストベースの侵入防止リューションの監視（プロセスの実行/システム管理者/L2）

資産の重要度、機密性に応じてホストベースの侵入検知システムによる監視を行う。

6.3.5　DHCP ログに基づくデバイスの検出（プロセスの実行/システム管理者/L2）

組織のネットワーク管理プロセスに基づき、DHCP のログを分析し、許可されていないデバイスを検出し、対処する。

6.4 デバイスの対処

6.4.1　未承認デバイスへの対処（プロセスの実行/システム管理者/L1）

組織が承認していないデバイスの使用を禁止する規程を整備し、実効性を担保するための規程と監査方法を確立し、実行する。

7 組織のネットワーク管理プロセスを確立する（プロセスの確立/経営層/L1）

組織のネットワークに接続されるルーター、ファイアウォール、UTM などのネットワーク管理プロセスを確立し、実行する。これには、機器管理プロセスに加えて、組織全体のネットワーク構成図と変更管理、機器、SDN 等のソフトウェア構成、バージョン、リビジョン等の一覧と重要資産のセグメント情報や、802.1X の構成、VLAN、ルーティング情報、VPN の構成、VPN クライアントソフト等の脆弱性管理、ログの収集と保管と、現在の構成を確実に再現できる文書の整備、ネットワークへの変更が文書に適切に反映されるような管理プロセスが含まれる。ネットワークの特性に応じた管理を検討しなければならない。例えば、ルーターやファイアウォールの管理コンソールへの接続は限定されなければならず、脆弱性対策のために、現行の構成のバックアップとバージョンアップの手順や廃棄の手順が確立されなければならない。

7.1 ネットワークの管理

7.1.1 ネットワークの認証・認可・監査の一元管理（プロセスの実行/システム管理者/L1）

可能な限りネットワークの認証・認可・監査は、アカウント管理と統合する。

7.1.2 ネットワーク監査ログ（プロセスの実行/システム管理者/L1）

組織のすべてのネットワークの取得すべき監査ログを定め、取得、保存、分析等の管理プロセスを確立し、実行する。これには、ルーターやファイアウォールなどのネットワークデバイス、無線 LAN、IoT デバイスなどの syslog、イベントログなどがあるがこれに限定されるものではない。

7.1.3 適切にセグメント化されたネットワーク（プロセスの実行/システム管理者/L1）

資産の重要度、機密性に応じてネットワークセグメント間の通信制御を行う。これにはポートフィルタリング、IP アドレス、アプリケーションによる通信の許可、制限などが含まれる。

7.1.4 セキュアなネットワークの管理（プロセスの実行/システム管理者/L1）

ネットワークインフラを安全に管理する。これには、VLAN による接続、SSH、HTTPS などの暗号化された接続や、物理的な管理、セグメント、ルーティング、冗長構成などによる可用性の維持が含まれる。

7.1.5 時刻同期（プロセスの実行/システム管理者/L1）

組織の監査ログプロセスに基づき、ネットワークデバイスの時刻を同期する。可能であれば、3 つのタイムソースを設定する。

7.2 ネットワークの保護

7.2.1 ネットワークデバイスの脆弱性管理（プロセスの実行/システム管理者/L1）

組織のすべてのネットワークデバイスの OS、ファームウェアの脆弱性管理プロセスを実行する。これには、脆弱性情報や適用情報の入手、適用すべきシステムの一覧、適用しなかった場合のリスクの評価、修正プログラムのテスト適用、バックアップと本番適用、代替策の適用、当該システムの切り離し、切り戻し、運用停止、変更管理などが含まれる。

7.2.2　セキュアな通信プロトコルの使用（プロセスの実行/システム管理者/L1）

組織のネットワーク管理プロセスに基づき、可能な限りセキュアな通信プロトコルを使用して接続する。これには、802.1X 認証（EAP-TLS、PEAP）、WPA2/3 Enterprise Mode などがある、

7.2.3　有線 LAN の保護（プロセスの実行/システム管理者/L1）

ゲストエリアの有線 LAN にゲストが接続できないように物理的保護をする。

7.2.4　通信における機密データの暗号化（プロセスの実行/システム管理者/L1）

ネットワーク通信中の機密データを TLS 等で暗号化する。TLS バージョン及び暗号スイートや暗号化手法は、半年に 1 回見直す。

7.2.5　安全なネットワークデバイスの設定構成（プロセスの実行/システム管理者/L1）

組織のネットワーク機器の安全な構成を設定する。これには脆弱な初期設定の変更や、脆弱なプロトコルを明示的に使用禁止に設定するなどの保護が含まれる。

7.2.6　ゲストエリアネットワークの保護（プロセスの実行/システム管理者/L1）

ゲストエリアの有線 LAN にゲストが接続できないように物理的保護をする。ゲストエリアの社内用無線 LAN とゲスト用無線 LAN を論理的に分離し、ゲストが社内用無線 LAN に接続できないように保護する。可能であれば、社内無線 LAN は証明書を利用した認証にする。

7.2.7　信頼できる DNS（プロセスの実行/システム管理者/L1）

信頼性が高く、悪意のあるサイトの名前解決を行わない DNS をフォワーダーとして設定する。信頼性については、単一障害点がない（Primary と Secondary が同一セグメントや SA に配置されていない、異なる TLD に配置）などが含まれる。

7.2.8　DNS フィルタリング（プロセスの実行/システム管理者/L1）

組織のすべての資産で DNS フィルタリングを使用し、悪意あるドメインへの名前解決を行わない。

7.2.9　リモートデバイス接続の認証（プロセスの実行/システム管理者/L1）

リモートデバイスは、組織の VPN や認証システムで認証されなければならない。

7.2.10　分離されたネットワーク経由の管理インターフェース（プロセスの実行/システム管理者/L2）

管理インターフェースは論理的もしくは物理的に分離されたネットワーク経由か、制限されたネットワークで接続しなければならない。接続端末は、限定されなければならず、一般業務の利用は禁止されなければならない。通信は必ず適切な暗号スイートで暗号化されなければならず、半期に 1 回、暗号スイートの設定を見直さなければならない。SSH やリモートデスクトップ接続などの接続クライアント、サーバーの設定が含まれる。

7.2.11　独立した管理用ネットワークでの接続と多要素認証（プロセスの実行/システム管理者/L2）

サーバーや機器の管理操作は、物理的、論理的に分離されたネットワークを経由して行われなければならない。分離されたネットワークでは、業務ネットワークから分離されており、保守に必要なポートだけが許

可されたインターネット接続が設定されなければならない。管理用端末は専用であり、管理端末は多要素認証が維持されており、Web ブラウザ、電子メールの利用や一般業務は禁止されていなければならない。

7.2.12 URL フィルタリング（プロセスの実行/システム管理者/L2）

組織のすべての資産で、URL フィルタリングを使用し、悪意あるサイトへの接続を行わない。

7.2.13 リモート接続する機器の正常性の確保（プロセスの実行/システム管理者/L2）

組織の遠隔拠点の機器や、リモートで組織に接続する端末、サーバー、スマートフォン、IoT デバイス、カメラ等のリモートアクセス制御基準を実行する。これには、アンチウイルスソフトの構成、脆弱性管理、安全な設定構成、必要最小限の実行権限、アクセス可能な組織の資産やクラウドサービスなどの正常性チェックが含まれる。BYOD を許可する場合は、正常性を確実に担保するか、必要最小限のアクセス制御を行うべきである。

7.2.14 ネットワーク侵入防止ソリューションの導入（プロセスの実行/システム管理者/L2）

資産の重要度、機密性に応じてネットワーク侵入防止システムを導入する。

7.2.15 ホストベースの侵入防止リューションの導入（プロセスの実行/システム管理者/L2）

資産の重要度、機密性に応じてホストベースの侵入防止システムを導入する。

7.2.16 802.1x 認証の導入（プロセスの実行/システム管理者/L2）

802.1X 認証によるデバイス認証、ユーザー認証を実施し、アクセスログを収集し、分析、対応する。可能な限り、802.1X 認証はアカウント管理と統合する。

7.2.17 アプリケーション型ファイアウォールの導入（プロセスの実行/システム管理者/L3）

組織のセキュリティイベント対策管理プロセスに基づき、資産の重要度、機密性に応じてアプリケーション型ファイアウォール(プロキシ型ファイアウォール）等を導入し、外部-内部、内部-内部の通信を制御する。

7.3 ネットワークの検出

7.3.1 監査ログの取得監査（プロセスの実行/システム管理者/L1）

組織の監査ログプロセスに基づき、必要とされるログが有効に取得され、ログに対して適切な権限が設定されていることを月次 1 回以上確認する。

7.3.2 ネットワーク機器のアクティブ検出（プロセスの実行/システム管理者/L2）

PING、NMAP などを使用し、ネットワークに接続されている機器を特定し、許可されていないデバイスを検出し、対処する。

7.3.3 ネットワーク侵入検知システムによる監視（プロセスの実行/システム管理者/L2）

資産の重要度、機密性に応じてネットワーク侵入検知システムによる監視を行う。

7.3.4 DNS クエリログの収集（プロセスの実行/システム管理者/L2）

組織の監査ログプロセスに基づき、スタブリゾルバの DNS クエリのログを収集する。

7.3.5　URL リクエストログの収集（プロセスの実行/システム管理者/L2）

組織の監査ログプロセスに基づき、URL リスクエストのログを収集する。

7.3.6　ログの一元管理（プロセスの実行/システム管理者/L2）

可能な限りログの収集と保存を一元化する。

7.3.7　ネットワーク機器のパッシブ検出（プロセスの実行/システム管理者/L3）

Wireshark, pktmon などを使用し、ネットワークに接続されている機器を特定し、許可されていないデバイスを検出し、対処する。

7.3.8　外部侵入テストの実施（プロセスの実行/システム管理者/L3）

年に 1 回以上、インターネットに公開されているデバイス、ネットワーク、ソフトウェアへの外部侵入テストを実施する。外部侵入テストは内部構造が漏洩したことを前提に、外部仕様に対するテストを行うことが望ましい。

7.3.9　内部侵入テストの実施（プロセスの実行/システム管理者/L3）

年に 1 回以上、内部侵入・漏洩テストを実施する。これには、知る必要性に基づくデータのアクセス制御の設定検証や、内部構造が漏洩したことを前提に、社内システムの外部仕様に対するテストを行うことが望ましい。

7.3.10 ログの詳細な自動監査（プロセスの実行/システム管理者/L3）

脅威の検出を目的として、組織内の異常なイベントを検出する。これには、ログオン失敗、権限変更、Kernel による実行阻止、不正なアクセス、異常なコマンドラインなどがある。可能な限り自動化すること。

7.4 ネットワークの対処

7.4.1　不正なネットワーク機器への対処（プロセスの実行/システム管理者/L3）

検出された不正なネットワーク機器を是正もしくは排除する。その際、ネットワーク機器の構成を保全し、不正なルーティングや許可されていないポート等を調査し、対処する。

7.4.2　脆弱性への対処（プロセスの実行/システム管理者/L3）

侵入テスト、自動監査等で発見された脆弱性を是正する。この際、脆弱性をもたらした原因を調査し、根本的な再発防止策を講じる。

8 セキュア開発プロセスの確立（プロセスの確立/システム管理者・開発責任者/L2）

組織のセキュアなアプリケーション開発プロセスを確立し、実行する。これには、セキュアなアプリケーション設計基準、セキュアコーディングガイドラインの作成もしくは選定、開発者トレーニング、開発の承認、SBOM 管理、フレームワーク管理、ソースコード管理、データ保護管理、脆弱性対応プロセスに基づく脆弱性管理、出荷判定基準、テスト基準などが含まれる。

8.1 セキュア開発プロセス

8.1.1 セキュアアプリケーション開発プロセスの実行（プロセスの実行/開発責任者/L2）

要件定義時点から OWASP ASVS v4 等を参照し、Security by Design を実践する。外注する場合は、折衝段階で、ASVS などのコーディングガイドラインを指定すること。

8.1.2 開発標準の維持（プロセスの実行/開発責任者/L2）

組織の開発標準を維持する。これには、用語の統一、最小特権原則の適用、プロセスの進捗評価の統一、入出力モジュールの統一や共通化、バリデーションルール（形式検証、論理検証、出力検証、）やフェイルセーフの規定、安全でない既定値の修正、ハードコードしてはいけない情報と安全な保存方法、必要最小限の構成方法などが含まれる。用語やプロセス定義については、共通フレーム 2013（ISO/IEC 12207：2008、JIS X 0160：2012、IPA 刊）を参考にする。

8.1.3 設計における脅威モデリング（プロセスの実行/開発責任者/L2）

アプリケーションの設計時に脅威モデリングを行い、セキュリティ評価を実施する。これには、ネットワーク構成、機器、サーバー、OS、開発環境、開発標準、開発フレームワーク、暗号化方式、データの保管・格納方式、ログ取得と保護などを総合的に評価する。

8.1.4 安全なコンポーネントの選定（プロセスの実行/システム管理者/L2）

安全なソフトウェアコンポーネントを選定し、採用する。これには、実績のある脆弱性対応が継続されている開発フレームワークやライブラリの採用、ソースコードの評価、脆弱性の評価などが含まれる。

8.1.5 信頼できるセキュリティ・コンポーネントの採用（プロセスの実行/開発責任者/L2）

認証・認可、暗号化、ログは、信頼できる OS の機能、コンポーネント若しくは開発フレームワークの機能を採用する。

8.1.6 インフラの強化設定（プロセスの実行/開発責任者/L2）

OS、DB、アプリケーション、コンテナ、Web サーバー、クラウド、SaaS、PaaS、サービスなどの強化設定を実施する。これには、最小権限設定、互換性維持による脆弱な設定の修正、脆弱なプロトコルの使用禁止、管理インターフェースの強化、セキュリティポリシー設定、ログの取得と保護、暗号化されていない認証や通信の禁止、スクリプトの禁止、統計情報などの外部送信の禁止、認証情報のキャッシュの禁止などが含まれる。

8.1.7 本番環境と開発環境の分離（プロセスの実行/開発責任者/L2）

開発環境と本番環境は異なる環境で管理する。開発環境のネットワークセキュリティは本番環境と同等以上のものとし、開発関係の資料、仕様書、データなどの漏洩、意図せぬ公開が起きないよう保護する。

8.1.8　コードレビューの実施（プロセスの実行/開発責任者/L2）

開発中のアプリケーションのコードレビューを行い、組織の承認を得る。コードレビューには、解析ツールや複数人による複数の第三者の人的解析が含まれる。

8.2 ペネトレーションテスト

8.2.1　重要システムのペネトレーションテスト（プロセスの実行/開発責任者/L2）

重要なデータを扱うシステムに対してペネトレーションテストを実施する。これには、ホワイトボックステスト、ブラックボックステストと、内部構造を理解した上での外部からのグレーボックステストが含まれる。

8.2.2　攻撃手法に対する防御・検出（プロセスの実行/システム管理者/L2）

組織に応じたペネトレーションテストプロセスに基づき、テストで使用された攻撃手法の防御や検出方法を検討し、実行する。

8.2.3　ペネトレーションテスト（プロセスの実行/システム管理者/L3）

組織に応じたペネトレーションテストを実行する。これには、組織内外のネットワーク、機器、サーバー、端末、IoT 機器、Web アプリケーション、API、クラウドシステム、複合機、入退出システムと施設などに対する、侵入、サービス停止、C&C、水平展開などの評価と、脆弱性が発見された場合の回避策の検討、実施が含まれる。

8.2.4　ペネトレーションテストでの課題の対応（プロセスの実行/システム管理者/L3）

組織に応じたペネトレーションテストプロセスに基づき、抽出された課題を修正する。課題の重大性にもとに、優先順位を決定し、修正までの代替策の適用や保護、監視を行う。

8.3 アプリケーションの対処

8.3.1　アプリケーションの脆弱性評価（プロセスの実行/システム管理者/L2）

アプリケーションの脆弱性の深刻度評価を実施する。これには、システムやデータの重要性や業務への影響度を加味した、修正の優先順位付け、修正までの保護策の適用、代替策の適用、アクセス管理や監視、出荷判定基準へのフィードバックなどが含まれる。

8.3.2　アプリケーションの SBOM 管理（プロセスの実行/開発責任者/L2）

アプリケーションごとの SBOM を作成し、月次単位で更新する。これには、ソフトウェアコンポーネントの名称、エディション、バージョン、ビルド、ソースコードもしくはバイナリなどの形式、リリース日などの版管理と、取得したリポジトリ、フォークの有無、コンポーネントに対する修正、組織内のソース管理場所などが含まれ、脆弱性対応プロセスと連携する。外注の場合は、サプライチェーン全体で SBOM 管理を求める。

8.3.3　アプリケーションの脆弱性の原因究明（プロセスの実行/開発責任者/L2）

アプリケーションの脆弱性の発生原因の分析、究明を行う。脆弱性を単にコーディングミスとせず、その失敗を招いた構造的な要因、すなわち仕様書の品質や誤解をまねく表現、前提とする要件の理解不足・連絡不足、教育不足、組織内外の連絡不足、仕様決定の先送り、仕様変更による手戻り、強行なスケジュール、杜撰なテスト体制、出荷判定基準などを洗い出すことが含まれる。

9 セキュリティトレーニングプロセスの確立（プロセスの確立/経営層/L1）

組織のセキュリティトレーニングプロセスを確立し、実行する。これには、最新の攻撃手法やソーシャルエンジニアリングの共有、サイバー攻撃の事例紹介、組織の認証方法や暗号化の危殆化につながる行為、セキュリティパッチの適用やアンチウイルスの更新、データのバックアップ、データのラベリングとそれに応じた保護などがあげられる。スキルを測定し、必要に応じて再教育し、人事情報として管理する。トレーニングは、経営者層（秘書を含む）、管理者層、従業員層（パートタイマーを含む）、IT 管理者・開発者層、外注業者に分け、それぞれの業務上のリスク視点で年に 1 回以上実施されなければならない。

9.1 ソーシャルエンジニアリングに関する教育（プロセスの実行/システム管理者/L1）

フィッシングやソーシャルエンジニアリングの手法、組織でソーシャルエンジニアリングが発生しやすいケースとその防止方法を教育する。これには、実際のフィッシングメールの紹介や、電子メールに埋め込まれた Web リンクの確認方法、ショルダーハッキング、電子メールでの信頼関係の構築などがあげられる。

9.2 認証方法に関する教育（プロセスの実行/システム管理者/L1）

組織が採用している認証方法の弱点や、危殆化につながる行為とその防止方法を教育する。

9.3 データの取扱いに関する教育（プロセスの実行/システム管理者/L1）

機密データ、組織外秘データ、公開データ等のラベルに基づく、取扱い規程を教育する。電子データと紙、ホワイトボードなどの物理的な記録について教育する。

9.4 データ露出に関する教育（プロセスの実行/システム管理者/L1）

誤送信やデバイスの紛失などのデータ露出の際の対応方法、リモートワイプ、データ消去の依頼などについて教育する。

9.5 脆弱性対応更新プログラムなどに関する教育（プロセスの実行/システム管理者/L1）

ファームウェア、セキュリティ更新プログラム、アンチウイルスのパターンファイルが最新であることを確認する方法について教育する。併せて組織内に情報共有のためのサイトやツールを設けて、最新情報を提供する。

9.6 安全でないネットワークに関する教育（プロセスの実行/システム管理者/L1）

安全でないネットワークの識別方法や、パブリックネットワークや家庭内ネットワークに接続した際の禁止行為を教育する。

9.7 BYOD に関する教育（プロセスの実行/システム管理者・人事責任者/L1）

個人所有の機器、スマートフォン、家庭内ネットワークの正常性維持のための情報、禁止行為を教育する。

9.8 セキュアコーディングに関する教育（プロセスの実行/開発責任者/L2）

半期に 1 回以上、開発要員に対してセキュアコーディングの教育を行う。これには、最新のセキュアコーディングガイドラインの内容、傾向や、脆弱性を作りこまない手法などの教育とともに、コーディングでは守れない前提となる設定や構成についても正確な理解を得る。理解度の評価を行うとともに、継続的にセキュアコーディングのノウハウ共有のコミュニティを形成する。

9.9 脆弱な設定・運用に関する教育（プロセスの実行/システム管理者/L2）

情報漏洩やサイバー攻撃につながる脆弱な設定や運用に対して、積極的な情報共有を行うよう教育する。別途、報奨制度を設けても良い。

9.10 役職の特性に応じたセキュリティに関する教育（プロセスの実行/システム管理者/L2）

経営者層、管理者層、従業員層、IT 管理者・開発者層ごとのセキュリティ教育を実施する。経営者層（秘書を含む）は機密データを取り扱うことからソーシャルエンジニアリングや電子メール、SNS の取扱いなどについて解説する。管理者層は従業員を含めたサイバーセキュリティの意識向上が事業継続の重要な要素であることを認識させ、業務よりもセキュリティを優先する課題抽出能力の向上に主眼を置く。従業員についても、サイバーセキュリティが事業継続に多大な影響を及ぼすことを認識させ、かつ、インシデントやインシデントにつながる業務の発見を奨励するよう教育する。IT 管理者及び開発者は、サイバーセキュリティインシデントを招く管理者権限の行使が伴うことから、ジャストインタイム権限や権限の最小化などについての情報共有を主眼とし、どうすればリスクを最小化できるかについて教育やディスカッションを展開することが望まれる。

10 インシデント対応プロセスの確立（プロセスの確立/経営層/L1）

10.1　インシデント報告（プロセスの実行/システム管理者/L1）

組織の従業員がインシデントを発見した際の報告手順を定め、実行する。あらかじめ想定できるインシデントの種類に基づき、最低限必要な情報と必要な情報の粒度、報告先、報告手段などを含めた書式の整備と、実効性を担保するための教育が望まれる。

10.2　インシデント発生時の保全（プロセスの実行/システム管理者/L1）

インシデント発生時の保全方法を定める。インシデントの原因がマルウェアの場合、アンチウイルスソフトのスキャンやシャットダウンを行う事で、マルウェアの手がかりを失い、結果として、アンチウイルスソフトのパターンファイルの作成が困難になる場合がある。アンチウイルスによる駆除ができないと、PC、サーバー等を初期化する必要が出てくる。このため、初動での保全方法を専門家と協議し、定めておく。これには、ネットワークの停止、パスワードの変更、セキュリティグループの追加や変更、ログの保全、時系列での対応記録の作成なども含まれる。

10.3　事業継続計画（BCP：Business Continuity Plan）の実行（プロセスの実行/経営者/L1）

現状の BCP を見直す、または環境の変化に追従するための事業継続戦略（BCM：Business Continuity Management）を確立するために事業継続戦略システム（BCMS：Business Continuity Management System）を策定し、実行する。これには、BCM における情報セキュリティマネジメントシステムの知見を持った専門家とのサポート契約や、サイバーセキュリティ版 BCP の策定と、それに基づくサイバーインシデント対応の準備と訓練、インシデント外部パートナーに対する適切な情報の提供(保全を含む)と、パートナーに対し、的確に状況を説明できる最低限の知見などが含まれる。例えば、パートナーとの契約により、本ガイドラインや情報セキュリティマネジメントシステム（ISMS：Information Security Management System）もしくはサブセットを実践し、情報資産、構成情報、設定情報、ログ管理、脆弱性対応状況を管理する力を継続的に向上させる、情報システムの調達及び刷新に関しては、本ガイドラインや ISMS に必要な情報の提供(ドキュメント、ツールなど)に協力を怠らないベンダー、協力会社を選定するなどがある。格段、注意すべき点として、本ガイドラインや ISMS は不断の努力により、常に見直し実践すべきものであり、手続き・規程（プロセス）確立や認定取得が目的となってはならない。

10.4　インシデント発生時の連絡先（プロセスの実行/システム管理者/L1）

経営者とシステム管理者は最低限、インシデント発生時に信頼できる初動体制を確保できる外部パートナーの選定を済ませなければならない。また、社内共有情報と社外共有情報の基準を定め、基準に沿ったコミュニケーションを行う。社内共有情報には、一般従業員、対応スタッフ、経営層などが考えられ、知る必要に基づく情報が提供されるべきである。社外共有情報には、顧客、所轄官公庁、警察、弁護士、保険会社、マスメディアとインシデント対応に協力する外部セキュリティ関連企業があり、それぞれに、定期的に更新されたリストに基づき知る必要に基づく情報が提供されるべきである。いずれも、2 次被害を拡大させない

ための技術的な手順や、復旧に向けた活動状況の継続的な広報が、信頼回復向けた重要なプロセスと位置付けなければならない。

10.5　インシデント発生後のレビュー（プロセスの実行/システム管理者/L1）

インシデント発生から復旧までのプロセスをすべてレビューし、課題抽出を行い、改善する。

10.6　インシデント発生時の通常経路外の情報共有（プロセスの実行/システム管理者/L2）

電子メール、情報共有システムが使用不能になったことを想定し、社内外への情報共有のための手段を確立し、半期に 1 回、テストを行う。

10.7　インシデント発生時の広報体制（プロセスの実行/システム管理者/L2）

コンプライアンス違反があった際の、原因、改善、復旧、将来に向けた保護措置に関する広報体制と発表方法を検討し、組織として確立する。

10.8　インシデント対応の演習（プロセスの実行/システム管理者/L2）

予め想定できるインシデントをもとに、社内組織の役割をシミュレーションし、演習を実施し、フィードバックに基づく改善を施す。

10.9　インシデントとイベントの定義（プロセスの実行/システム管理者/L2）

インシデントとイベントを区別するための客観的な数値や事象の重大性を定義し、見直す。これにはあってはならないログやプライバシーの侵害などの事実や、ノイズと判断されるログ、情報漏洩につながらない操作ミスや公開情報の誤送信などの定義が含まれる。