資料 4-2

重要インフラのサイバーセキュリティに係る
リスクマネジメント手引書
（骨子案）

令和４年12月22日

内閣官房内閣サイバーセキュリティセンター
重要インフラグループ

目次

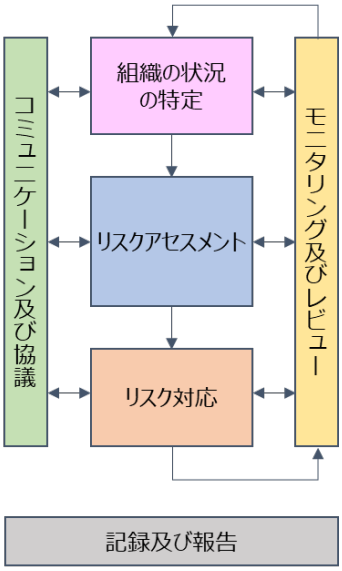
1. はじめに

1.1. 手引書策定の目的

- 情報通信技術の進歩や複雑な経済社会活動の相互依存関係の深化が進むなど、サイバー空間を取り巻く不確実性は絶えず変容かつ増大している。新しいサービスの創出機会等も拡大している一方で、サイバー攻撃等による情報漏えいやサービス停止の被害が増加するなど、サイバーセキュリティに関するリスクも拡大している。
- 国民生活や社会経済活動の基盤となるサービスを提供する重要インフラ事業者等においては、サイバーセキュリティに関するリスクを経営リスクの一つとして認識し、重要インフラを取り巻く情勢（システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まり等）を鑑みて、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応をより一層促進することとしている[1]。
- 本手引書は、サイバーセキュリティ部門（戦略マネジメント層、担当者層）向けに、リスクマネジメントの実施方法についての具体的な手順を含む基礎的なフレームワークを提供する。

1.2. 手引書の記載範囲

2. 本手引書では、組織の特性やリスクを把握するために必要な概念とその対処を具体化するためのリスク特定・分析・評価といった主要なプロセスに加え、活用が可能なリスクアセスメント以外のプロセスについても記載する。
    * コミュニケーション及び協議
    * 組織の状況の特定
    * リスクアセスメント（リスクの特定・分析・評価）
    * リスク対応
    * モニタリング及びレビュー
    * 記録及び報告
    * 主なセキュリティ対策



[1] 重要インフラのサイバーセキュリティに係る行動計画（2022 年６月 17 日サイバーセキュリティ戦略本部決定）

2.1. 手引書の適用範囲

（１）対象とする事業者等

本手引書は、重要インフラ事業者等による利活用を想定している。各事業分野や事業領域に特化したリスクマネジメント手法が既に確立している場合は、既存の手引書やガイドライン等を優先して利活用しつつ、必要に応じて本手引書の記載内容を補完的に利活用することが望まれる。

（２）リスクマネジメントの対象

本手引書におけるリスクマネジメントでは、重要インフラ事業者等が、そのサービス提供に必要な業務の遂行のために所有、使用又は管理する情報資産等に係る事象の結果（自然災害、サイバー攻撃等に起因する障害）から認識されるリスクを対象とする（※）。

（※）重要インフラ事業者等においては、サイバーセキュリティに関するリスク以外のリスクがあることも考えられる。本手引書では、スコープを限定したリスクマネジメントの手法を紹介しているが、実際にリスクの評価やリスク対応の選択肢の同定に係る意思決定を行う際には、サイバーセキュリティに関するリスク以外についても勘案し、総合的に考慮することが重要である。

3. リスクマネジメントのフレームワーク

3.1. 全体像

- NISC「機能保証のためのリスクアセスメント・ガイドライン」、NIST「重要インフラのサイバーセキュリティフレームワーク（CSF）」、ISO/IEC27001 をベースに構成している。
- 対象を従来のリスクアセスメントからリスクマネジメント全体に拡大し、コミュニケーション及び協議、モニタリング及びレビュー等に係る取組を追記した。
- 組織の状況把握からリスク対応の決定・改善に至る一連の取組[2]について、NIST CSF をベースに追記した。

3.2. 前提

- リスクの捉え方について、「目的に対する不確かさの影響」をリスクと捉える（ISO 31000:2018 における定義に準拠。）。

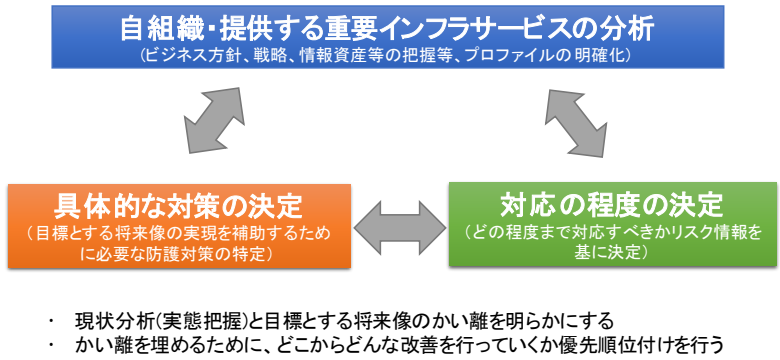
[2] NIST CSF では、「重要インフラの事業者及び運営者が自主的に利用できる、サイバーリスクの識別、評価、管理に役立つセキュリティ対策を含む、優先順位付けされた、柔軟な、繰り返し適用可能な、パフォーマンスベースの、費用対効果の高いアプローチ」とされている。

4. コミュニケーション及び協議

- リスクマネジメントのプロセスの初期段階において、サイバーセキュリティに関するリスクが影響を及ぼす可能性のある組織内外のステークホルダーを把握し、コミュニケーション及び協議のための体制を構築する。
- リスクマネジメントにおけるコミュニケーションには、分析したリスクをステークホルダーと共有や議論を行なうことに留まらず、リスクマネジメントの各ステップの活動を行う為に必要な分析に使用する最新の情報や手法に加えて、ステークホルダーの価値観等のリスク特定や評価に重要な情報の共有を行なうことも含まれる。
- ステークホルダーとのコミュニケーションにより、実施しているリスクマネジメントへの安心を高め、参加意識を高めることもできる。

5. 組織の状況の特定

- 自組織が直面するリスクとその程度を把握し、自組織の重要インフラサービス提供に係る特性の明確化に着手することから新たな改善をスタートする。
- 任務保証の考え方を踏まえ、自組織の特性を明確化する。



図：自組織に適した防護対策の実現（概念図）

5.1. 内部状況の把握

- 組織内部の要因により自組織の状況を把握するには、以下に例示する要素等について現状を把握する。
  - ＊ 現在の組織体制、経営戦略、セキュリティ方針
  - ＊ リスクマネジメント戦略、リスク許容度
  - ＊ 重要インフラサービスに係る情報システム、制御システム、データ
  - ＊ セキュリティ投資が可能な資源状況
  - ＊ リスク分析や対応に必要な技術や人的資源の把握
  - ＊ セキュリティリスクに対する、部署や立場による認識の差異
  - ＊ 従業員のセキュリティリテラシー

1) ビジョン、使命及び価値観
2) 組織統治、組織体制、役割及びアカウンタビリティ
3) 戦略、目的及び方針
4) 組織の文化
5) 組織が採用する規格、指針及びモデル
6) 資源及び知識として理解される能力（例えば、資本、時間、人員、知的財産、プロセス、システム、技術）
7) データ、情報システム及び情報の流れ

8) 内部ステークホルダーの認知及び価値観を考慮に入れた、内部ステークホルダーとの関係
9) 契約上の関係及びコミットメント
10) 相互依存及び相互関連

ISO 31000:2018 より、内部状況の例

5.2. 外部状況の把握

・ 組織外部の要因により自組織の状況を把握するには、以下に例示する要素等について現状を把握する。
  * 自組織が関連する法令の改正状況（事業法、個人情報保護法等）
  * 所管省庁や規制当局における基準の策定、改正状況
  * 関連団体における基準やガイドラインの策定、改正状況
  * 景気、為替、経済リスクが与えるセキュリティ投資への影響
  * 国外に拠点のある事業者における現地の法令、情勢等の状況
  * セキュリティ投資による優遇措置
  * 社会からのブランドイメージ
  * 重要インフラサービスの利用者に与える影響
  * 国内外におけるセキュリティインシデントの発生事例や、その報道等による社会からのセキュリティ認識の広まり
  * 株主や社会からの要求事項
  * 外部取引先との契約における、セキュリティに関する要求事項
  * 自組織が任務保証を達成するために必要な他の重要インフラサービス
  * 自組織と他組織の相互依存関係

1) 国際、国内、地方又は近隣地域を問わず、社会、文化、政治、法律、規制、金融、技術、経済及び環境に関する要因
2) 組織の目的に影響を与える、鍵となる原動力及び傾向
3) 外部ステークホルダーとの関係、並びに外部ステークホルダーとの認知、価値観、必要性及び期待
4) 契約上の関係及びコミットメント
5) ネットワークの複雑さ、及び依存関係

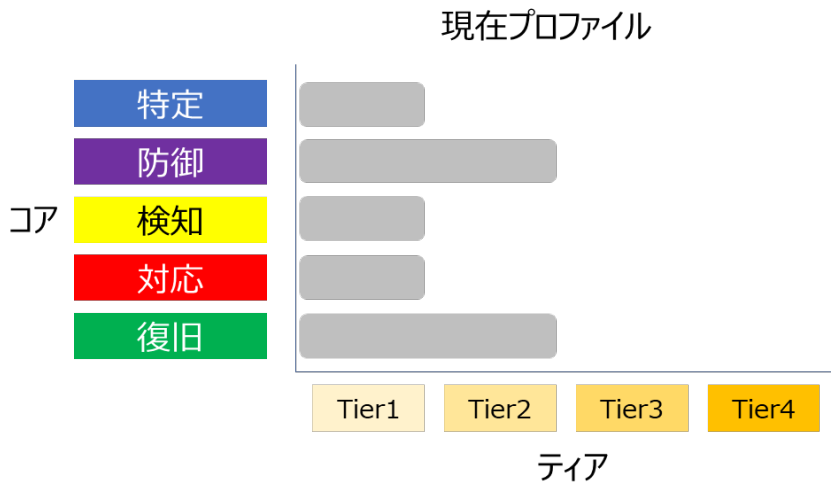
ISO 31000:2018 より、外部状況の例

5.3. 重要インフラサービス継続に係る特性の把握

・ 内部状況及び外部状況を踏まえた、以下に例示する自組織の重要インフラサービス継続に係る特性を把握、整理する。
  * 自組織のサービス停止が社会経済に与える影響
  * サービス継続に係る重要なシステムや機能
  * 重要なシステムや機能を支える業務
  * 業務を支える資源及び知識（予算、人員、設備、技術、資産の脆弱性情報）
  * 他の重要インフラとの相互依存関係
  * 重要インフラサービス障害時における、復旧までの許容可能な時間

5.4. 現在プロファイルの特定

・ 自組織の内部状況、外部状況及び重要インフラサービス継続に係る特性を踏まえ、自組織の現在のセキュリティ水準（現在プロファイル）を特定する。
・ セキュリティ水準の特定に当たっては、NIST サイバーセキュリティフレームワーク（CSF）、英国 Cyber Assessment Framework、C2M2、CIS Controls 等が参考となる。NIST CSF では、サイバーセキュリティの確保にあたり、コアと呼ばれる５つの区分（特定・防御・検知・対応・復旧）のセキュリティ対策と、ティアと呼ばれる対策の程度を例示している。



図：現在プロファイルの特定の概念図

表：NIST CSF に示されるティア（対応の程度）の例

Tier1	**・セキュリティ対策が未対応の状態。** ・リスクマネジメントプラクティスが定められておらず、リスク対処は場当たり的。 ・セキュリティリスクに関して意識が不足している。 ・情報共有のプロセスが存在しない。 ・ステークホルダーとは協力関係にない。
Tier2	**・セキュリティ対策は整備しているが、運用化まではできていない。** ・リスクマネジメントプラクティスは経営層に承認されているが、組織全体のポリシーにはなっていない。 ・サプライチェーン・リスクは把握しているものの対応はできない。
Tier3	**・セキュリティ対策は整備できており、定期的に見直しができる状態。** ・リスクマネジメントプラクティスが自組織のポリシーとなっており、またプラクティスは定期的に更新されている。 ・従業員は割り当てられた役割と責任を果たすための知識とスキルを持っている。 ・セキュリティ担当の役員と他の役員が定期的に他の役員とコミュニケーションを取っている。 ・ステークホルダーと協力関係にある。 ・サプライチェーン・リスクの対処ができる。
Tier4	**・セキュリティ対策は整備できており、適時に見直しができる状態。** ・組織全体のサイバーセキュリティマネジメントのアプローチが確立されている。 ・セキュリティリスクマネジメントが組織文化の一部となっている。 ・役員が示したビジョンを実践し、システムレベルでリスク分析を行っている。 ・事業目的、ミッションの変更に迅速かつ効果的に対処できる。 ・サプライチェーン・リスクをリアルタイムに近い情報で対処している。

6. リスクアセスメント

6.1. リスク分析手法の検討

・ 任務保証の観点から、原則としてリスクベースでの分析を実施する。

6.2. リスク基準の決定

・ リスクアセスメントの判断の目安となるリスク基準を決定する。

6.3. リスクアセスメントの実施目的の確認

・ 自組織の経営目標を踏まえたリスクアセスメントの目的を設定する。

6.4. 実施方針の確認

・ リスクアセスメントの実施目的の確認と合わせ、実施方針を設定する。

6.5. マススケジュールの策定

・ リスクアセスメントの実施方針として定めた各作業の実施時期を定め、リスクアセスメント活動全体の作業スケジュール（マススケジュール）を策定する。

6.6. 実施体制の構築

・ リスクアセスメントの実施方針及びマススケジュールを踏まえ、実施体制を構築する。
・ 経営層がリスクアセスメントの最高責任者となり、推進、管理を主導する。
・ 実施体制を構築後、各推進担当部門において、詳細スケジュールの策定及び要員計画（作業担当者の専任及び作業の割り当て）を行う。

6.7. リスクの特定

・ 任務保証の考え方を踏まえ、演繹的にリスク源の洗い出しを実施する。

6.8. リスクの分析

・ 事象の結果が及ぼす影響及び事象の発生頻度を評価し、リスク源ごとの残留リスクを導出する。

6.9. リスクの評価

・ リスク基準と残留リスクを踏まえ、リスク対応の実施対象を抽出する。

6.10. リスクアセスメントの妥当性確認・評価

・ リスクアセスメントの実施体制、実施手順、実施状況等が適切かつ十分であったかを評価する。

6.11. 制御システムのリスクアセスメント

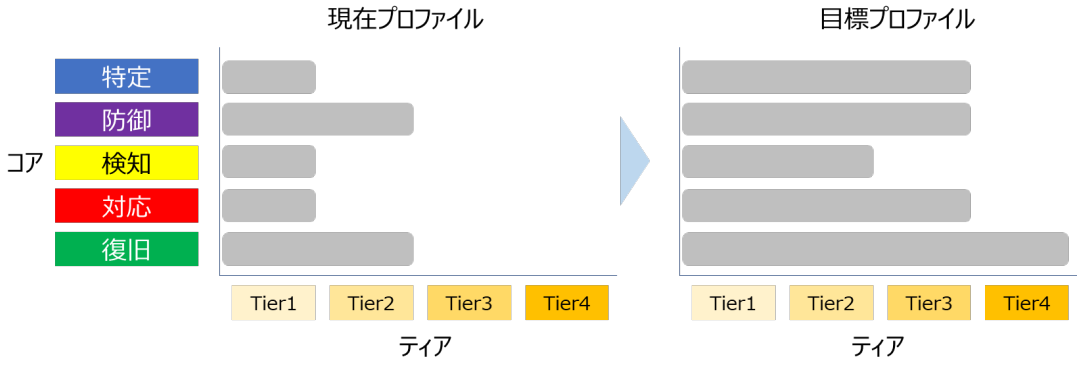
- 制御システムにおいては IPA「制御システムのセキュリティリスク分析ガイド」、ISO/IEC 62443「制御システムセキュリティに関する国際規格」、NIST-SP 800-82「産業用制御システム（ICS）セキュリティガイド」等を踏まえ、事業被害ベース[3]の脅威を想定したリスクアセスメントを実施する。
- 一般的に、制御システムは可用性（安全、安定稼働）が最優先される。パッチ適用やバージョンアップ、暗号化などのリスク低減策の実施が、制御システムの安定稼働に影響を与えると判断できる場合には、ログや通信の監視等の、代替策の実施によりリスク低減を図る。
- 制御システムに関するセキュリティ責任者を設置し、情報システムと制御システムの担当者間で適切なコミュニケーションをとる。

[3] システムで実現している事業やサービスに対して、事業被害とそのレベル、事業被害を引き起こす脅威の発生可能性、脅威に対する脆弱性の 3 つを評価指標として、リスクを評価する分析手法。

7. リスク対応

7.1. 目標プロファイルの作成

- 自組織の特性やサイバーセキュリティリスクの特定・分析・評価の結果を考慮し、目標とするセキュリティ水準（目標プロファイル）を作成する。
- 全ての項目で最高のセキュリティ水準を目指すのではなく、組織の置かれた状況やステークホルダーからの要求事項等を踏まえ、必要と思われるセキュリティ水準を設定する。



図：目標プロファイルの概念図

7.2. ギャップ分析と優先順位付け

- 現在のセキュリティ水準と目標とするセキュリティ水準の差異について分析する。
- 差異を解消し、目標とするセキュリティ水準に近づけるための取組について、組織方針に基づく動機、リスク、セキュリティ対策の費用対効果等を踏まえ、優先順位付けを行う。

7.3. リスク対応計画

- 優先順位付けを踏まえ、現在のセキュリティ水準と目標とするセキュリティ水準の差異に対して実施すべき取組をまとめたリスク対応計画を作成し、実施する。

8. モニタリング及びレビュー

8.1. モニタリング実施計画の策定と実施

- サイバーセキュリティ確保の取組の効果について、継続的に改善を行うため、リスク対応計画や、人材育成の進捗状況等をモニタリングする。継続的に実施するため、モニタリング及びレビューのプロセスを計画に組み込む。
- リスクの管理レベルが社会からの要求事項の変化に沿うよう、日々改善する。

8.2. 内部監査の実施

- サイバーセキュリティ確保の取組が適切な状態で維持していることを確認するため、内部監査人による定期的な監査を実施する。実施にあたっては必要に応じて、外部の専門知識を有する者の支援を受けて状況確認をする。

8.3. モニタリング及びレビュー結果の反映方針の策定

- モニタリング及び監査結果から、改善や見直しが必要な箇所を認識する。レビューに際し、内部環境、外部環境の変化や、関係主体からの要求事項も確認する。

9. 記録及び報告

9.1. 記録

- リスクマネジメントの検証、改善のため、各プロセスにおいて、記録を作成する。記録の作成に当たっては次の事項を考慮する。
  - 記録の作成及び維持管理の費用及び労力
  - 閲覧方法、検索の容易性及び保存媒体
  - 保有期間
- 記録を取ることを目的にするのではなく、利用目的に合わせて記録することが重要なことに留意する。

9.2. 報告

- ステークホルダーとのコミュニケーションの質を高めたり、経営層の意思決定を補助したりするために報告を実施する。報告に当たっては次の事項を考慮する。
  - それぞれのステークホルダーに特有の情報の必要性及び要求事項
  - 報告の費用、頻度及び適時性
  - 報告の方法
  - 情報と組織の目的及び意思決定との関連性

10. 対策項目

・ リスク評価の結果、重要度に応じて組織ごとにリスク対応を行うことが前提であるが、本項では分野共通的に必要度が高いと考えられる取組について記載する。

10.1. サプライチェーン・リスクへの対応

・ 製品・サービスの調達・利用にあたり、サイバーセキュリティに関する要求事項を整理する。
・ 不正機能等の埋め込みに係る脅威に対応する。
（リスク管理策例）
＊ 調達過程における一貫した品質管理が担保できることの選定基準への盛り込み
＊ 指定したセキュリティ要件が実装されているか、不正プログラムが混入していないかを確認する検査体制の構築
＊ 委託先が再委託先を監督し責任を負うことが可能な体制であるかの確認
＊ 再委託の禁止、又は再委託前に委託元の許可を得ることの契約要件への盛り込み
・ サービスの供給途絶に係る脅威に対応する。
（リスク管理策例）
＊ 部品の供給役務の継続提供の担保
＊ 供給者の事業計画や提供実績等の確認
＊ 委託先の事業実施場所の確認、立地条件の考慮
・ 外部サービスにおける情報の取扱いに係る脅威に対応する。
（リスク管理策例）
＊ 信用できるサービスの選定
＊ 情報の返却や抹消などに係る確認手段の設定
・ 海外拠点、グループ組織、取引先等を経由したサイバー攻撃に係る脅威に対応する。
（リスク管理策例）
＊ 第三者による評価検証結果の活用
＊ サプライチェーンとのネットワーク接続点におけるセキュリティの確認
・ NISC「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書」が参考になる。

10.2. 組織的対策

（資産管理）
・ 組織全体の資産目録を作成し、定期的に維持管理する。制御システムについても作

成する。重要な機器やサービス業務の機能維持・レジリエンス向上のため、全ての重要な資産の現在の詳細構成を記述した文書を策定し、維持管理する。

- 全てのシステム・ネットワーク構成を記述した文書（システム・ネットワーク構成図）を作成し、維持管理する。制御システムについても文書を作成する。構成図は定期的なレビューと更新を実施する。
- 新しいハードウェア、ソフトウェア、ファームウェアを導入する前に、承認を必要とする仕組みとし、組織の情報資産の可視性を高める。技術的に可能な場合、承認されたハードウェア、ソフトウェアのホワイトリストとも整合させ、維持管理する。

（運用管理）

- サイバーセキュリティに関する脅威情報を収集し、意思決定等に活用できるよう分析する。
- インターネットに接続されたシステムの既知の脆弱性（CVE 情報等）を、重要な資産から優先的にパッチ適用等により緩和する。パッチ適用が不可能もしくは、可用性や安全性を損なうおそれのある OT 資産については、NW の分離や監視等の代替手段を使用し、当該システムがインターネットからアクセスできないようにする。
- 従業員がシステムの脆弱性、誤設定、悪用可能な状態を発見した際に、セキュリティ担当者に速やかに報告できるようにする。報告手段は電子メールや Web フォーム等が一般的である。報告を受けた場合には、その重大性に応じて適切に対処する。

（インシデント管理）

- 一般的な脅威シナリオ及及び自組織固有の脅威シナリオに対応するセキュリティインシデント対応計画を策定し、年１回以上訓練を実施する。制御システムについても訓練を実施する。訓練で得られた教訓をもとにセキュリティインシデント対応計画を更新する。

10.3. 人的対策

- 組織の全ての従業員を対象としたトレーニングを年１回以上実施する。フィッシング、ビジネスメール詐欺、パスワードセキュリティなどの基本的な概念を網羅し、サイバーセキュリティに関する組織内文化を醸成する。
- サイバーセキュリティの基本的なトレーニングに加え、制御システムの運用、維持、保全の担当者は、制御システムに特化したサイバーセキュリティのトレーニングを年１回以上実施する。
- 雇用の終了又は変更後も有効なセキュリティに関する責任及び義務を定めて、従業員はその要求事項を遵守する。外部委託等の利害関係者に対しても同様の要求事項を伝達する。

10.4. 物理的対策

- 情報システムを収容する建物の屋根、壁、天井及び床を強固な構造物とし、外部に接する全ての扉を施錠する。入退室時におけるアクセスカード、生体認証等による認証の仕組みや、警備員、侵入者警報、監視カメラ等による監視システムを構築する。これにより、認可された要員だけが管理領域に入退できるようにする。
- 火災、洪水、地震等の自然災害や、爆発物、武器等による人的災害についてリスクアセスメントを実施し、災害対策や、ランダムな物品検査を実施する。
- 書類や取り外し可能な記録媒体について、セキュリティを保って保管し、不要になった場合にはセキュリティを保った仕組みを使用してそれらを破棄する。記憶媒体を持ち出す場合には認可を要求し、記憶媒体に位置追跡及び遠隔データ消去機能を実装する。

10.5. 技術的対策

（パスワード管理）

- ハードウェア、ソフトウェア等を使用する前に、製造元のデフォルトパスワードを変更する。制御システムについても、新規または将来のすべてのデバイスのデフォルト認証情報を変更する方針とする。これは、実現が容易なだけでなく、将来的にサイバー攻撃手法が変化した場合の潜在的なリスクも軽減される。ハードコードされている等、デフォルトパスワードの変更が不可能な場合、代替セキュリティ管理策を実施し、ログインのアクセスログを監視する。
- 自組織の情報資産に対して、パスワードの用途ごとに最小パスワード長及び複雑さを設定する。パスワードの用途は、「ログインパスワード」「パスワードロックされた圧縮ファイルや文書ファイル」「無線アクセスポイントへの接続」等がある。アカウントロックや多要素認証等、他の管理策との組み合わせを考慮して、パスワード長及び複雑さを設定する。
- 自組織のサービスや資産に関して、一意かつ個別のパスワードを設定する。利用者に対し、アカウント、アプリケーション、サービス等でパスワードを再利用させないようにする。

（アカウント管理）

- 失敗したログインを記録し、複数回連続して失敗したログインについてはセキュリティ担当者に通知されるようにする。短時間に連続して失敗したログインについては、アカウントロックされるよう設定する。
- ユーザーアカウントに管理権限を割り当てず、管理権限も用途ごとに設定する（バックアップ用、システム設定閲覧用、システム設定変更用等）

- ハードウェアベースの多要素認証技術[4]が利用可能な場合は有効にする。利用できない場合にはソフトウェアベース[5]を利用する。SMS による多要素認証は、他の選択肢が可能な場合を除きできるだけ避けるようにする。
- 離職者のアカウント管理として、すべてのバッジ、キーカード、トークン等を失効させ、安全に返却させる。離職者が保有するすべてのユーザーアカウントと、組織情報へのアクセスを無効にする。
- 個人情報及び認証情報を含む機微なデータは、暗号化して保存され、許可された管理者のみがアクセスできるようにする。

（ログ管理）

- アクセス及びセキュリティ関連のログを、検知及びインシデント対応で使用するために収集し、保存する。イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知する。ログ機能が非搭載の OT 資産については、OT 資産との間の通信ログを収集する。
- 収集したログはツールや中央システム（SIEM 等）に一元的に保存され、許可された管理者のみがアクセスできるようにする。ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定する。

（アクセス制御）

- 公開サーバなど、インターネット上の資産では、悪用可能なサービス（RDP、SSH、SMB 等）を使用しない。また、インターネットに接続された情報資産では、不要なアプリケーションやネットワークプロトコルはすべて無効化する。
- 運用上明示的に必要な場合を除き、OT 資産はインターネット上には配置しない。例外が存在する場合には承認、文書化し、悪用を防止する措置を具備する。悪用防止の措置として、多要素認証や VPN の活用、ロギングによる動作の監視等が挙げられる。また、OT ネットワークへの接続は、特定の機能のため明示的に許可された通信を除き、すべて拒否すること。IT と OT 間の必要な通信経路にはファイアウォール等中継装置を設置し、厳密に通信を監視する。中継となるファイアウォール装置の設定、脆弱性についても適切に維持管理する。

（暗号化）

- 転送中のデータを保護するために、適切な TLS 暗号化を導入する。非推奨や、脆弱

---

[4] 物理的な機器を使用して多要素認証を行う認証技術。ワンタイムパスワードトークン、USB セキュリティキー等がある。

[5] 特定の物理的な機器を使用するのではなく、ソフトウェアを使用して多要素認証を行う認証技術。例えば、スマートフォンのアプリケーションによる認証など。

な暗号化が使用されている資産を特定し、強度な暗号に更新する計画を立てて実施する。制御システムについては、遅延と可用性への影響を最小限にするため、通常はリモートや外部資産との通信について、可能であれば暗号化を行う。

- 暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照する。
- 完全性が求められる情報を取り扱う情報システムについては、STARTTLS、DMARC といった電子署名の付与及び検証を行う機能を設ける必要性の有無を検討する。

（マルウェアからの保護）

- マクロ等の埋め込みコードの実行をすべての機器において規定で無効とする。業務においてコードを実行する必要がある場合、許可されたユーザーが特定の状況化で実行できることを承認する仕組みを構築する。
- 被害が発生した際の、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、IPS[6]/プロキシサーバ（不審な外部通信の遮断）、EDR[7]（影響範囲の特定と被害端末の隔離）等がある。

（バックアップ）

- 運用に必要なシステムについて、年 1 回以上の定期的なバックアップを実施する。
- バックアップデータはバックアップ元のシステムとは切り離して保管し、データの重要度に応じて保存方法、保存期間を定める。また、定期的に復旧テストを実施する。
- 制御システムについては、設定、役割、PLC ロジック、設計図面、ツールについてもバックアップする。

---

[6] Intrusion Prevention System の略。ネットワークやサーバへの通信を監視し、不正なアクセスを検知して通信を遮断する不正侵入防止システム。

[7] Endpoint Detection and Response の略。従業員が利用する端末やサーバにおける不審な挙動を検知し、迅速に対応するためのセキュリティ対策のひとつ。