中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

第 7 編　　ISMS の構築と対策基準の策定と実施手順【レベル 3】

東京都産業労働局

第14章. ISMS の管理策

章の目的
第 14 章では、ISO/IEC 27002 における管理策の分類と構成について理解することを目的とします。
主な達成目標
◘ ISMS の管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

14-1. 管理策の分類と構成

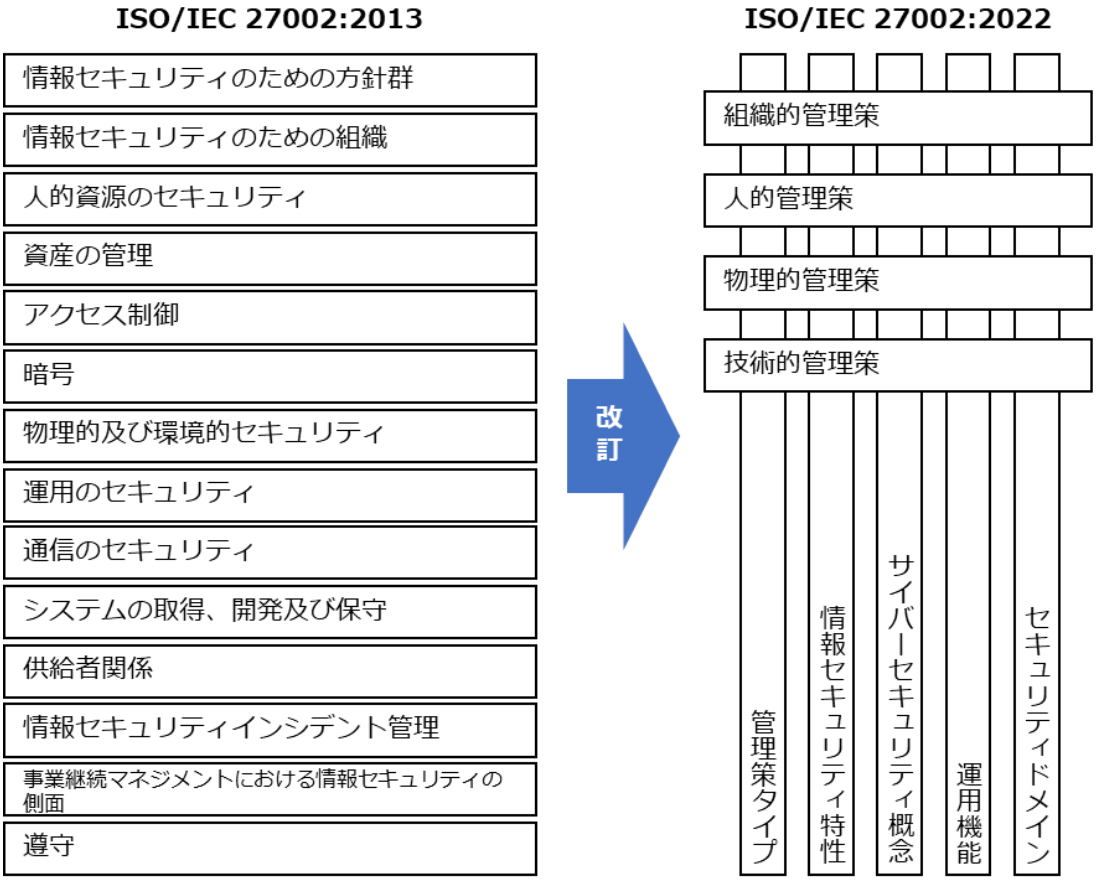
14-1-1. 管理策：ISO/IEC 27002

ISO/IEC 27001 に記載されている要求事項をもとに、さらに具体的な ISMS の管理策を示した規格が ISO/IEC 27002 です。管理策とは、リスク対応策のことを指します。企業は ISMS を導入する際、ISO/IEC 27002 にある管理策から、自社に合ったものを選択し、対策基準として導入することになります。

ISO/IEC 27002 は、2022 年に改訂がありました。その際の変更点としては、管理策の項目数と章立ての変更、テーマおよび属性の導入、全管理策に目的を追加などがあります。管理策の数は、2013 年版では 14 分野 114 項目でしたが、2022 年版ではいくつかが統合されて 82 項目になり、新しく 11 項目が追加され、合計で 93 項目となりました。

2022 年版では、この 93 の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4 カテゴリに分類されています（箇条 5～8）。

また、2022 年版では「属性（attribute）」という新しい概念が導入されました。各管理策には、属性値がハッシュタグにより表示されるようになっています。例えば、管理策のタイプには、予防・検知・是正の 3 つの属性値があります。この他、情報セキュリティ特性、サイバーセキュリティ概念、運用機能、セキュリティドメインの観点からも属性値が付けられています。これらの属性を参考にして、組織に必要な情報セキュリティ対策を選択することになります。



14-1-2. 管理策のテーマと属性

ISO/IEC 27002 の箇条 5～8 に示される 4 種の管理策での分類（組織的・人的・物理的・技術的）を、テーマと呼びます。管理策の分類はさまざまな考え方がありますが、多くの組織に共通であると考えられる最低限の分類としてこの 4 つが採用されています。テーマとは別の視点で、より細かに管理策を見るのに際しては、属性という機能があります。各管理策に属性が付与されたことにより、検索性が向上し、管理策のフィルタリング、並び替え、提示がしやすくなりました。

管理策の属性には、他の組織や団体が発行するガイドラインなどにおける考え方を取り入れているものがあります。「サイバーセキュリティ概念」では、サイバーセキュリティフレームワークにおける、フレームワークコアの 5 つの機能分類がそのまま属性値となっています。また、「運用機能」の属性値は、2022 年の改訂前における ISO/IEC 27002 での管理策の分類がもとになっています。

管理策の属性	属性値	関連するガイドラインなど
管理策タイプ	予防、検知、是正	ー
情報セキュリティ特性	機密性、完全性、可用性	ISO/IEC 27001:2022
サイバーセキュリティ概念	識別、防御、検知、対応、復旧	サイバーセキュリティフレームワーク
運用機能	ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティ、セキュリティ	ISO/IEC 27002:2022

	を保った構成、識別情報およびアクセスの管理、脅威および脆弱性の管理、継続、供給者関係のセキュリティ、法および順守、情報セキュリティ事象管理、情報セキュリティ保証	
セキュリティドメイン	ガバナンスおよびエコシステム、保護、防御、対応力	ー

各テーマより管理策の例示（組織的/人的）

【組織的管理策】5.2 情報セキュリティの役割及び責任

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防	#機密性 #完全性 #可用性	#識別	#ガバナンス	#ガバナンス及びエコシステム #対応力

管理策	情報セキュリティの役割及び責任を、組織の要求に従って定め、割り当てることが望ましい。
目的	組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。

【人的管理策】6.8 情報セキュリティ事象の報告

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#検知	#機密性 #完全性 #可用性	#検知	#情報セキュリティ事象管理	#防御

管理策	組織は、要員が発見した又は疑いを持った情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設けることが望ましい。
目的	要員が、特定可能な情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。

各テーマより管理策の例示（物理的/技術的）

【物理的管理策】7.4 物理的セキュリティの監視

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防 #検知	#機密性 #完全性 #可用性	#防御 #検知	#物理的セキュリティ	#保護 #防御

管理策	施設は、認可されていない物理的アクセスについて継続的に監視することが望ましい。
目的	認可されていない物理的アクセスを検知し、抑止するため。

【技術的管理策】8.16 監視活動

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#検知 #是正	#機密性 #完全性 #可用性	#検知 #対応	#情報セキュリティ事象管理	#防御

管理策	情報セキュリティインシデントの可能性がある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じることが望ましい。
目的	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

14-1-3. 対策基準と実施手順の作成方法

管理策から自社に必要な対策を適用宣言書として選択して対策基準を作成し、実施手順を作成できるようにする手順を説明します。

- 管理策の決定：リスクアセスメントの結果を考慮して、適切なリスク対応を選定します。選定したリスク対応の選択肢に基づいて、実施に必要なすべての管理策を決定します。管理策は、

ISO/IEC 27001 の附属書 A から選択できます。附属書 A に適切な管理策がない場合は、独自に追加の管理策を選択できます。

- 管理策の検証：決定した管理策を、ISO/IEC 27001 の付属書 A に規定された管理策と比較し、自社にとって必要な管理策が見落とされていないか検証します。

- 適用宣言書の作成：適用宣言書を作成します。適用宣言書とは、ISMS に関連してその組織が適用する管理策を記述した、文書化された情報のことです。適用宣言書に含める事項は以下の通りです。
  - 必要な管理策
  - それらの管理策を含めた理由
  - それらの管理策を実施しているか否か
  - 付属書 A に規定する管理策を除外した理由

- 実施手順の作成：管理策（対策基準）をもとに具体的な実施手順を作成します。実施手順は、組織の内部文書として作成します。従業員が具体的に何を順守して行動すればよいか理解できるよう、わかりやすく策定するよう心掛けることが大切です。

第15章. 組織的対策

章の目的
第 15 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。
主な達成目標
◘　組織的管理策をもとに、対策基準を策定する手順を理解すること ◘　策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

15-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に記載された合計 93 項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
5.1 情報セキュリティのための方針群		5.20 供給者との合意におけるセキュリティの取扱い	
5.2 情報セキュリティの役割及び責任		5.21 ICT サプライチェーンにおける情報セキュリティの管理	
5.3 職務の分離		5.22 供給者のサービス提供の監視、レビュー及び変更管理	
5.4 経営陣の責任		5.23 クラウドサービス利用における情報セキュリティ	
5.5 関係当局との連絡		5.24 情報セキュリティインシデント管理の計画策定及び準備	
5.6 専門組織との連絡		5.25 情報セキュリティ事象の評価及び決定	
5.7 脅威インテリジェンス		5.26 情報セキュリティインシデントへの対応	
5.8 プロジェクトマネジメントにおける情報セキュリティ		5.27 情報セキュリティインシデントからの学習	
5.9 情報及びその他の関連資産の目録		5.28 証拠の収集	
5.10 情報及びその他の関連資産の利用の許容範囲		5.29 事業の中断・阻害時の情報セキュリティ	
5.11 資産の返却		5.30 事業継続のための ICT の備え	
5.12 情報の分類		5.31 法令、規制及び契約上の要求事項	

5.13 情報のラベル付け		5.32 知的財産権	
5.14 情報転送		5.33 記録の保護	
5.15 アクセス制御		5.34 プライバシー及び PII の保護	
5.16 識別情報の管理		5.35 情報セキュリティの独立したレビュー	
5.17 認証情報		5.36 情報セキュリティのための方針群、規則及び標準の順守	
5.18 アクセス権		5.37 操作手順書	
5.19 供給者関係における情報セキュリティ			

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMS に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）

5.1 情報セキュリティのための方針群

情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューしなければならない。

5.2 情報セキュリティの役割及び責任

情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てなければならない。

5.3 職務の分離

相反する職務および責任範囲は、分離しなければならない。

5.4 経営陣の責任

経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求しなければならない。

5.5 関係当局との連絡

組織は、関係当局との連絡体制を確立および維持しなければならない。

5.6 専門組織との連絡

組織は、情報セキュリティに関する研究会または会議、および情報セキュリティの専門家からの協会・団体との連絡体制を確立し維持しなければならない。

5.7 脅威インテリジェンス

情報セキュリティの脅威に関連する情報を収集および分析し、脅威インテリジェンスを構築しなければならない。

5.8 プロジェクトマネジメントにおける情報セキュリティ

情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

5.9 情報及びその他の関連資産の目録

管理責任者を含む情報およびその他の関連資産の目録を作成し、維持しなければならない。

5.10 情報及びその他の関連資産の利用の許容範囲

情報およびその他の関連資産の利用並びに取扱い手順の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。

5.11 資産の返却

要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却しなければならない。

5.12 情報の分類

情報は、機密性、完全性、可用性および関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類しなければならない。

5.13 情報のラベル付け

情報のラベル付けに関する適切な一連の手順は、「5.12 情報の分類」で確立した分類体系に従って策定し、実施しなければならない。

5.14 情報転送

情報転送の規則、手順または合意を、組織内および組織と他の関係者との間のすべての種類の転送設備に関して備えなければならない。

5.15 アクセス制御

情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、業務および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。

5.16 識別情報の管理

組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てなければならない。

5.17 認証情報

認証情報の割り当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

5.18 アクセス権

情報およびその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針および規則に従って、提供、レビュー、変更および削除しなければならない。

5.19 供給者関係における情報セキュリティ

供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定義し実施しなければならない。

5.20 供給者との合意における情報セキュリティの取扱い

供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意をとらなければならない。

5.21 ICT サプライチェーンにおける情報セキュリティの管理

ICT 製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。

5.22 供給者のサービス提供の監視、レビュー及び変更管理

サービスの供給者の情報セキュリティの実践およびサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。

5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスの取得、利用、管理および終了のプロセスを、組織の情報セキュリティ要求事項に従って定めなければならない。

5.24 情報セキュリティインシデント管理の計画及び準備

セキュリティインシデント管理のプロセス、役割および責任を定義、確立および伝達し、セキュリティインシデント管理の計画を定めなければならない。

5.25 情報セキュリティ事象の評価及び決定

情報セキュリティ事象に対して、セキュリティインシデントに分類するか否かを決定するための評価を実施しなければならない。

5.26 情報セキュリティインシデントへの対応

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

5.27 情報セキュリティインシデントからの学習

セキュリティインシデントから得られた知識を、情報セキュリティ管理策を強化し、改善するために用いなければならない。

5.28 証拠の収集

情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を定め、実施しなければならない。

5.29 事業の中断・阻害時の情報セキュリティ

事業の中断・阻害時に情報セキュリティを適切なレベルに維持するための方法を定めなければならない。

5.30 事業継続のための ICT の備え

事業継続の目的および ICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持および試験しなければならない。

5.31 法令・規制及び契約上の要求事項

情報セキュリティに関する法令や契約事項を特定・文書化し、順守しなければならない。

5.32 知的財産権

知的財産権を保護するための適切な手順を実施しなければならない。

5.33 記録の保護

記録を、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。

5.34 プライバシー及び PII の保護

適用される法令、規制および契約上の要求事項に従って、プライバシーの維持および PII の保護に関する要求事項を特定し、満たさなければならない。

5.35 情報セキュリティの独立したレビュー

情報セキュリティおよびその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。

5.36 情報セキュリティのための方針群、規則及び標準の順守

組織の情報セキュリティ方針、トピック固有の個別方針、規則および標準を順守していることを定期的にレビューしなければならない。

5.37 操作手順書

情報処理設備の操作手順を文書化し、必要な要員に対して利用可能な状態としなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

One Point

対策基準を策定する際のポイント

ISO/IEC 27001:2022 附属書 A の中には、中小企業にとっては負担が大きい管理策があります。ISO/IEC 27001:2022 附属書 A に適切な管理策がない場合は、独自の管理策を追加することができます。組織の状況を考慮し、適切な対策基準を策定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

15-2. 組織的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順例を、それぞれ紹介します。実施手順は、組織の内部文書として作成します。実施手順が抽象的で理解しづらい場合、従業員は具体的に何を順守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。従業員に対してわかりやすい実施手順を策定するよう心掛けることが大切です。

実施手順を策定する際は、ISO/IEC 27002 に記載されている各管理策の手引きが参考になります。手引きの内容をもとに、実施手順の例を紹介します。この例と、ISO/IEC 27002 の内容を参考に、自社に適した実施手順を策定してください。

15-2-1. 情報化・サイバーセキュリティ・個人情報保護

情報化・サイバーセキュリティ・個人情報保護に関連する実施手順の例を紹介します。

【5.1 情報セキュリティのための方針群】

実施手順（例）
情報セキュリティ委員会は、「情報セキュリティ方針」などの情報セキュリティに関する方針を定義し、トップマネジメント（経営層）の承認を得る。また、情報セキュリティ委員会は、情報セキュリティに関する方針を適用範囲内の全従業者に公表する。また、「情報セキュリティ方針」は外部関係者にも公表する。 情報セキュリティ委員会は、「情報セキュリティ方針」以外の情報セキュリティのための方針群を、本手順において定める。方針群には以下を含める。 ● モバイル機器の方針 ● テレワーキング ● アクセス制御方針 ● 暗号による管理策の利用方針 ● クリアデスク・クリアスクリーン ● 情報転送の方針（および手順） ● セキュリティに配慮した開発のための方針 ● 供給者関係のための情報セキュリティの方針
ワンポイントアドバイス 情報セキュリティに関する方針は、関連する従業員および利害関係者に認識されることが大切です。

【5.2 情報セキュリティの役割及び責任】

実施手順（例）

トップマネジメント（経営層）は、情報セキュリティに関連する役割を持つ情報セキュリティ委員会、内部監査責任者に対して、以下の責任および権限を割り当てる。また、トップマネジメント（経営層）は、これらの役割、責任および権限を従業者に伝達する。情報セキュリティの運用に際し、トップマネジメント（経営層）は、情報セキュリティ委員会の設置および運営を実施する。

情報セキュリティ委員会の役割は以下の通り。

a. リスク対応計画の策定
b. 情報セキュリティ実行体制の構築
c. 選択された管理策の実施
d. 教育・訓練
e. 運用の管理
f. 経営資源の管理
g. 情報セキュリティ事象・セキュリティインシデントの管理
h. 関連当局との連絡（警察・審査機関・コンサル会社・取引先・委託先など）

情報セキュリティ委員会の役割と、責任および権限は以下の通り。

- **情報セキュリティ委員会責任者**
  管理策の実施・運用について統括する。管理策の成果をトップマネジメント（経営層）に報告する。
- **教育責任者**
  管理策に関する教育計画の立案と実施を行う。
- **部門管理者（運用委員）**
  情報セキュリティの部門代表者として、部門を管理する。
- **情報システム管理者**
  情報システム部門の管理者で、情報システム管理に関する規定・規則に従い、情報セキュリティを維持するための安全管理対策を実施する。
- **文書管理責任者**
  管理策に関する文書や記録などの維持・管理を行う。

内部監査責任者の責任および権限は以下の通り。
内部監査責任者は、管理策とその実施状況に関わる監査を統括する責任と権限を有する。

ワンポイントアドバイス
従業員が少ない場合は、文書管理責任者と教育責任者を同じ者にするなど、役割を兼任させて体制を構築することも有効です。

【5.3 職務の分離】

実施手順（例）
a. 当組織は、申請者または作業者と、承認者を分離するように組織設計する。 b. 従業員の制約により兼任せざるを得ない場合、別部門などから監視を受けることを条件に、兼任できる。
ワンポイントアドバイス 小さな組織で、職務の分離が困難である場合には、他の管理策（例：活動の監視、監査証跡、管理層からの監督）を考慮することが大切です。

【5.4 経営陣の責任】

実施手順（例）
トップマネジメント（経営層）はすべての従業者に対し、情報セキュリティ方針、各実施手順、並びにその他情報セキュリティに関する要求事項の順守を求める。
ワンポイントアドバイス 情報セキュリティ方針、各実施手順、その他情報セキュリティに関する要求事項が、すべての従業員に認識されることが大切です。

【5.5 関係当局との連絡】

実施手順（例）
情報セキュリティ委員会は、関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。
ワンポイントアドバイス セキュリティインシデントを、時機を失せずに報告するために、関係当局の連絡方法を明確にすることが大切です。

連絡先一覧表（例）

関係当局	連絡手段	URL	主目的
【IPA】コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口	ウイルス発見・感染の届出 virus@ipa.go.jp 不正アクセスの届出 crack@pa.go.jp	https://www.ipa.go.jp/security/todokede/crack-virus/about.html	ウイルス感染や、不正アクセスによる被害を報告するため。
【IPA】情報セキュリティ安心相談窓口	TEL:03-5978-7509 （受付時間 10:00～	https://www.ipa.go.jp/security/anshin/ab	ウイルス感染や不正アクセスに関する技術的

	12:00、13:30～17:00 土日祝日・年末年始は除く）anshin@ipa.go.jp	out.html	な内容の相談に対して、アドバイスをもらうため。
【警視庁】サイバー犯罪相談窓口	TEL:03-5805-1731 受付時間：午前 8 時 30 分から午後 5 時 15 分まで（平日のみ）	https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html	サイバー犯罪被害について相談するため。
【個人情報保護委員会】個人情報・マイナンバーの漏えい報告	Web フォームで報告	https://www.ppc.go.jp/personalinfo/legal/leakAction/	個人情報、マイナンバーの漏えいに対処するため。
【JPCERT/CC】インシデント対応依頼	Web フォームまたは、以下のメールアドレスに報告 info@jpcert.or.jp	https://www.jpcert.or.jp/form/	セキュリティインシデント対応を支援してもらうため。

【5.6 専門組織との連絡】

実施手順（例）
情報セキュリティ委員会は、専門組織およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。
ワンポイントアドバイス 脆弱性や攻撃など情報セキュリティに関する情報を適時入手するために、入手方法を明確にすることが大切です。

連絡先一覧表（例）

専門組織	**情報の入手方法**	**URL**	**主目的**
【IPA】重要なセキュリティ情報	Web ページを閲覧	https://www.ipa.go.jp/security/security-alert/2025/index.html	危険性が高いセキュリティ上の問題と対策に関する最新情報を収集するため。
【IPA】ランサムウェア対策特設ページ	Web ページを閲覧	https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html	ランサムウェア対策に関する最新情報を収集するため。

【個人情報保護委員会】注意情報一覧	Web ページを閲覧	https://www.ppc.go.jp/news/careful_information/?category=39	セキュリティ・個人情報・マイナンバーに関する、注意事項を把握するため。
【JPCERT/CC】注意喚起	Web ページを閲覧	https://www.jpcert.or.jp/at/2025.html	脆弱性に関する最新情報を収集するため。

【5.8 プロジェクトマネジメントにおける情報セキュリティ】

実施手順（例）

a. プロジェクト管理者は、プロジェクトにおける必要な管理策を特定する。
b. プロジェクトにおける必要な管理策は、プロジェクト終了後も考慮する。
c. プロジェクト管理者は、情報セキュリティ責任者を任命する。
d. 情報システム管理者は、業務用情報システムの導入・改善にあたっては、必要に応じて情報セキュリティ上の要求事項を、要件定義書や提案依頼書などにより文書化する。
文書には下記から必要な事項を含める。
- 情報システムの設置場所（環境・障害からの対策を含む）に関する事項
- 無停電電源装置などのサポートユーティリティに関する事項
- 保守契約に関する事項
- システムの冗長化に関する事項
- 通信、データの安全対策に関する事項
- 受け入れテストに関する事項
- アクセス権限に関する事項

ワンポイントアドバイス

プロジェクトが提供する製品またはサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の個別方針および規制から順守すべき要求事項を決定することが大切です。

【5.12 情報の分類】

実施手順（例）

情報は一般・社外秘・関係者外秘で分類する。
情報セキュリティ委員会は、情報の分類を最低年 1 回見直す。

ワンポイントアドバイス

分類は、情報の侵害が組織に与える影響のレベルによって決定できます。分類体系により定義されたレベルには、分類体系の適用において意味をなすような名称を付けることが大切です。

情報の分類（例）

分類	内容
一般	下記以外
社外秘	関係者外秘以外の機密事項であり、当組織の従業者に対してのみ開示が許されるもの。（取引先に開示する必要があるものは除く。）または情報セキュリティに関わる規定・手順書類。
関係者外秘	情報が外に漏れることによって、当組織が重大な損失もしくは不利益を受けるような恐れのある機密事項であり、職務上の限られた関係者のみに開示を許すもの。関係者が明示的に定められていない場合、関係者とは、情報を直接配布された者を指す。

【5.13 情報のラベル付け】

実施手順（例）

従業員は、取扱う情報が一般・社外秘・関係者外秘の区分のうち、どれに該当するか認識できる必要がある。

書類の分類を容易に認識できない場合は、以下のいずれかの方法により適切なラベル付けを行う。

a. 分類をシールなどの色により識別する。
b. ファイルなどに分類を記入（またはスタンプ）することで識別する。
c. 分類ごとに収納場所を分ける。

ワンポイントアドバイス

ラベル付けは、「5.12 情報の分類」で確立した分類体系を反映していることが大切です。

【5.14 情報転送】

実施手順（例）

a. 重要な情報を外部に送信する場合は、セキュアなファイル共有サービスを利用する。やむを得ずファイル共有サービスが利用できない場合は、受信者と合意した上で、メールに添付して送信する。
b. 重要な情報を外部に FAX にて送信する場合は、入力した番号と、名刺や送り状を照合し、間違えがないことを確認してからスタートボタンを押す。また頻繁に送信する送り先は短縮ダイヤルに登録する。
c. 認可されていない者に聞かれる可能性がある場所で、重要な情報を口頭で伝えることは禁じる。
d. 重要な情報を外部に郵送する場合は、配達記録郵便や宅配便など配達記録が残る手段をとる。
e. 重要な情報を格納した媒体は、手渡しを原則とし、やむを得ず郵送する場合は、十分な梱

包により媒体を保護する。

f. 個人情報の授受記録
- 紙や記憶媒体による個人情報の受け渡しに際しては、送付票や受領証などで受け渡しの完了を確認する。
- 電子メールにより個人情報の受け渡しを行う際には、送信済みメールおよび、受領確認の返信メールのいずれかまたは両方を受け渡し記録とする。

g. 電子メールの利用
- 電子メールは会社所定のソフトを使用し、その利用は業務上必要な場合に限定する。
- 社外メーリングリストへの参加は、原則禁止とする。
- 重要な情報（社外秘以上）はメール本文に記載して送信せず、a に従う。

h. 情報転送に関する合意
- 情報の転送先との間で、情報転送の手段について、あらかじめ合意を得る。
- 重要な情報を外部にメール添付または FAX にて送信する場合は、必要に応じて送信予告、到着確認の電話を掛ける。
- 宅配便業者を利用する場合は、会社が指定する業者を利用する。

i. 電子的メッセージ通信
- 当組織の Web サイトに入力する情報の通信は、SSL/TLS により行う。
- 電子データによる個人情報をインターネット経由で送受信する際は、SSL/TLS などの暗号化対策やパスワード設定などの措置を講じる。

ワンポイントアドバイス

情報転送は、電子的な転送、物理的記憶媒体での送付および口頭での伝達によって行われる場合があります。情報転送の規則、手順を定めることが大切です。

【5.15 アクセス制御】

実施手順（例）

a. 業務に必要な者のみが情報にアクセスできるようにし、アクセス権限および操作権限は、認められた場合以外は与えないようにする。

b. 社内 LAN は、情報システム管理者の承認を得た従業員、装置に限り接続する。

c. 社内の情報システムへの外部からのアクセスは、ファイアウォールなどによって通信を制限する。

d. 外部から社内のサーバに接続する場合、VPN 接続を使用する。

e. 無線 LAN は物理的・論理的な認証、通信の暗号化などを施した上で利用する。

f. サーバ室へ入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁じる。

g. サーバ室は、常時施錠可能とし、入退資格のない者の立ち入りを禁じる。

ワンポイントアドバイス

アクセス制御規則を定めるには、「明確に許可していないことは、原則的に禁止する」という最も特権の小さい前提に基づいた規則を設定するようにすることが大切です。

【5.16 識別情報の管理】

実施手順（例）

a. 情報システムの利用者登録および登録削除は、当該利用者の属する部門長が申請し、情報システム管理者の承認を得る。

b. 利用者登録は業務上必要な範囲で従業者に付与する。

ワンポイントアドバイス

識別情報が不要になった場合、識別情報は時機を失せずに無効化または削除することが大切です。

【5.17 認証情報】

実施手順（例）

a. 情報システム管理者は、利用者に仮パスワードを発行する場合、利用者本人のみが知ることができる方法で通知する必要がある。

b. 情報システム管理者は、利用者に対し、仮パスワードを直ちに変更することを要求し、通知する。

c. 秘密認証情報の利用

- 利用者は、英数字と記号を混在した 10 文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。利用者は、英数字と記号を混在した 10 文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。
- 他人に容易に推測されるようなわかりやすいパスワードの使用を禁じる。
- 他のサービスと重複するパスワードの利用を禁じる。
- 各システムにおける管理者 ID のパスワードは、情報システム管理者において厳重に管理する必要がある。
- 利用者および情報システム管理者は、パスワードの代替もしくは補完のために、指紋などの生体認証、IC カード認証などの機器による認証方式も採用できるものとする。

d. パスワード管理システム

- パスワードの入力は対話式とする。
- パスワードをシステムに記憶させることは禁じる。

ワンポイントアドバイス

パスワードを認証情報として使用する場合、IPA などが推奨している強力なパスワードの作り方を参考にすることが大切です。

【5.18 アクセス権】

実施手順（例）
a. 利用者のアクセス権は、重要情報に対しては必要最小限の者がアクセスするという原則のもとに、情報システム管理者が検討し、設定を行う。 b. 情報システム管理者は、定期的（最低年 1 回）および必要時にアクセス権限の棚卸および見直しを行う。 c. 退職者が発生した際は、業務に支障がないよう調整し、速やかに該当アカウントを削除する必要がある。申請は、当該従業員が最後に所属した部門の長がアクセス権限の削除を申請し、情報システム管理者、またはその指名する従業員が削除する。 d. 他部署への移動が生じた際は、a の手順に従い削除する。また、新規のアクセス権限は移動先部門の長が申請し、同様の手順に従い登録する。
ワンポイントアドバイス 物理的および論理的なアクセス権の定期的レビューでは、同じ組織内での異動、昇進、降格、退職後の利用者のアクセス権、および特権的アクセス権の認可について考慮することが大切です。

15-2-2. 脅威インテリジェンス

脅威インテリジェンスに関連する実施手順の例を紹介します。

【5.7 脅威インテリジェンス】

実施手順（例）
既存または新たな脅威に関する情報を、次に示す専門機関から収集する。 ● IPA ● JVN（Japan Vulnerability Notes） ● JPCERT/CC ● ISAC（Information Sharing and Analysis Center） ● 個人情報保護委員会 収集する情報は、以下のようなものとする。 ● 変化する脅威の状況に関する情報（例：攻撃者や攻撃の種類） ● 攻撃の方法、使用されるツールや技術に関する情報 ● 特定の攻撃に関する詳細な情報 収集した情報を分析する。 脅威が、自組織にどのような影響を及ぼすか把握するために、収集した情報をもとにリスクアセスメントを実施する。 リスク低減の処置を実施する。

リスクアセスメントの結果をもとに、ファイアウォール・侵入検知システム・マルウェア対策ソリューションなど、技術的に予防、検知を行うための管理策を採用する。
ワンポイントアドバイス 情報の収集から、リスク低減処置を実施するまでの手順を明確にすることが大切です。

15-2-3. 情報資産台帳作成・維持実施

情報資産台帳作成・維持実施に関連する実施手順の例を紹介します。

【5.9 情報及びその他の関連資産の目録】

実施手順（例）
情報セキュリティ委員会は「資産目録」を作成し、当組織における重要な資産を識別する。また「資産目録」を「年間計画表」に従い、最低年 1 回見直す。 情報セキュリティ委員会は「資産目録」において特定した資産に対し、同目録上に管理責任者（リスク所有者）を記載することにより管理責任を明確にする。
ワンポイントアドバイス 資産の管理責任を個人またはグループに割り当て、管理責任を明確にすることが大切です。

【5.10 情報及びその他の関連資産の利用の許容範囲】

実施手順（例）				
情報の区分ごとの取扱いルールを以下に示す。 情報の区分は「5.12 情報の分類」で、ラベル表示については「5.13 情報のラベル付け」で定める。				
文書・メディアなどの場合	**管理区分**	**関係者外秘**	**社外秘**	**一般**
	ラベル表示	責任者に一任	責任者に一任	不要
	利用者	関係する部署・プロジェクトに所属する従業者	当組織の従業者	誰でも可
	再配布	関係する部署・プロジェクト内に限る	社内に限る	特別な配慮不要
	保管場所	施錠された場所	責任者に一任	
	コピーの使用	必要のある者に限定	社内に限る	
	FAX 送信	関係する部署・プロジェクト内に限る	社内に限る	
	裏紙使用※1	禁止	禁止	
	社外便	透かして内容が見えないようにする。※2		

	社外での携行	責任者の許可を得た者のみ携行を許可する。※3		
	廃棄（文書）※4	シュレッダー・焼却・溶解のいずれか	責任者に一任	
	廃棄処（媒体）	廃棄、再利用前の内容を消去する。		
	※1 個人情報の記された書類の再利用は禁じる。 ※2 紙や記憶媒体による個人情報を、郵便や宅配便などにより移送するときは、誤配、紛失などの危険を最小限にするため、ポストへの施錠、受け取り確認が可能な移送手段の選択などの措置を講じる。 ※3 個人情報を外部へ持ち出す際は、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。 ※4 紙に記された個人情報の廃棄は、シュレッダーによる裁断・焼却・溶解いずれかの方法により処分する。また、廃棄前の一時保管場所からの紛失・盗難防止のため、重要書類は即廃棄する。			

システム内情報	管理区分	関係者外秘	社外秘	一般
	アクセス制御	個人またはグループでのアクセス制御	責任者に一任	特別な配慮不要
	個人 PC への保管	責任者に一任	責任者に一任	
	サーバへの保管	アクセス制限	責任者に一任	
	コピー（複製）※1	コピーの管理	責任者に一任	
	メール	添付ファイルにパスワード		
	※1 コピーは、バックアップの必要上および業務上やむを得ない場合の必要最小限の範囲にとどめるものとする。 ※2 取引先との合意がある場合は、その合意に従う。			

ワンポイントアドバイス

許容できる行動、許容できない行動を明確に定めることが大切です。

【5.11 資産の返却】

実施手順（例）
情報セキュリティ委員会は、退職者が発生した際に、以下の対応を部門長に要求し、実施されたことを確認する。 名刺、社員証、ID カードなどの返却 会社が支給したノート PC や携帯電話などの返却 紙で保管する書類の返却、または廃棄
ワンポイントアドバイス

返却するすべての情報およびその他の関連資産を明確に特定し、文書化することが大切です。

15-2-4. クラウドサービス利用

クラウドサービス利用に関連する実施手順の例を紹介します。

【5.23 クラウドサービスの利用における情報セキュリティ】

実施手順（例）	
クラウドサービスを導入する際、以下の評価表をもとにクラウドサービスを評価し、自社のセキュリティ要件事項を満たしているか確認する。	
評価表	
クラウドサービス提供者名	**サービス内容**
取得している認証	
□ ISO/IEC 27001 □ ISO/IEC 27017	
セキュリティ対策内容	**評価**
クラウドサービスに対して、マルウェア対策を行っているか。	
クラウドサービスのバックアップを行っているか。	
サービス解約時のデータの取扱い方法が明確になっているか。	
サービス稼働率、障害発生頻度、障害発生時の復旧時間など、サービス品質は問題ないか。	
データがどの国や地域に配置されたサーバに保存されているか確認したか。	
サービスの利用方法について問い合わせることができるか。	
クラウドサービス提供者の責任範囲を確認したか。	
クラウドサービスのセキュリティインシデント発生時に通知がくるかどうか確認したか。	
ワンポイントアドバイス クラウドサービスの利用は、クラウドサービス提供者とクラウドサービス利用組織との間の情報セキュリティに関する責任の共有および分担、共同作業を伴う可能性があります。クラウドサービス提供者と、クラウドサービス利用組織の両方の責任を適切に定義し、実践することが大切です。	

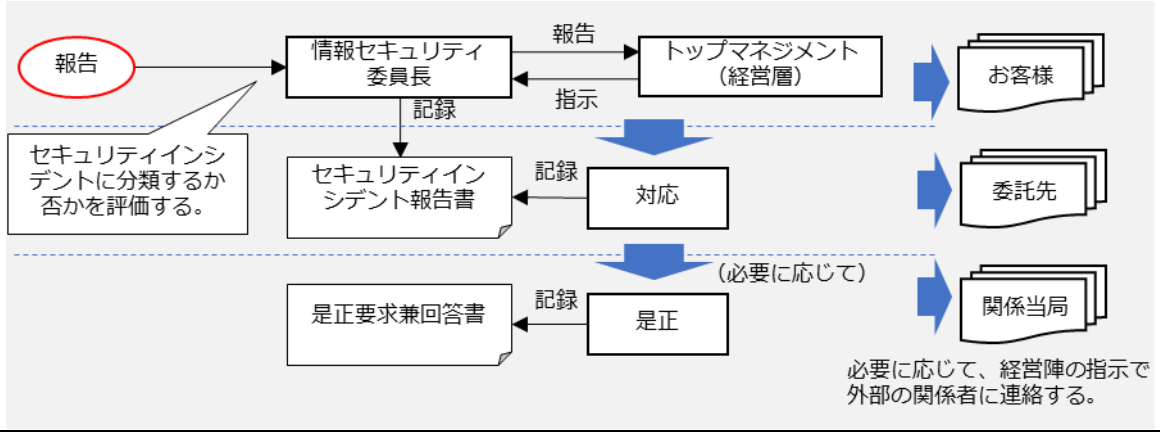
15-2-5. 情報セキュリティインシデント対応

情報セキュリティインシデント対応に関連する実施手順の例を紹介します。

【5.24 情報セキュリティインシデント管理の計画策定及び準備】

実施手順（例）

セキュリティインシデントへの対応は、以下の手順で行う。
管理層の責任のもと、以下の手順を関係者に伝達する。



ワンポイントアドバイス

セキュリティインシデントへの対応を実行するために役割および責任を決定し、関連する関係者に効果的に伝達することが大切です。

【5.25 情報セキュリティ事象の評価及び決定】

実施手順（例）

セキュリティの弱点、脅威に気付いた場合もしくは疑いを持った場合は、情報セキュリティ委員会に報告する。この際、自己で解決することよりも報告を優先させる。
情報セキュリティ事象の評価は、以下の表に従い、部門管理者（情報セキュリティ委員会メンバー）が行う。
・大、中の項目に該当する情報セキュリティ事象は、セキュリティインシデントとして分類する。
・項目の大、中、小の順に優先順位を付ける。

ワンポイントアドバイス

情報セキュリティ事象をセキュリティインシデントに分類する基準を明確に定めることが大切です。

優先順位

項目	小	中	大
分類	ヒヤリハット・事象	インシデント	インシデント
最終的に被害が及ぶ範囲	現状、事件・事故の発生には及ばない。（将来、被害が発生する可能性がある。）	社員または社内	顧客・取引先

連絡先	情報セキュリティ委員長	情報セキュリティ委員長	情報セキュリティ委員長 トップマネジメント（経営層） 外部関係者

【5.26 情報セキュリティインシデントへの対応】

実施手順（例）

セキュリティインシデントへの対応手順は以下の表に従う。

	影響度	小	中・大
セキュリティインシデントへの対応手順	ウイルス感染時	● 感染した PC を、組織内のネットワークから切り離す。 ● 発生する可能性がある被害をシステム担当者に報告する。	● 感染した PC を、組織内のネットワークから切り離す。 ● 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
	不正アクセス発生時	● ネットワークを遮断する。 ● 重要なデータを隔離する。 ● ログインできる場合は、早急にパスワードを変更する。 ● 発生する可能性がある被害をシステム担当者に報告する。	● ネットワークを遮断する。 ● 重要なデータを隔離する。 ● ログインできる場合は、早急にパスワードを変更する。 ● システムやアプリケーションを停止する。 ● 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
	情報破壊発生時	● 発見次第、発生する可能性がある被害を部門長に報告する。	● 発見した事実をできるだけ速やかに部門長に連絡する。
	情報改ざん発生時	同上	同上
	情報漏えい発生時	同上	同上
	サービス停止時・機器故障など	同上	同上

ワンポイントアドバイス

セキュリティインシデント対応に関する手順を確立し、すべての関連する利害関係者に伝達することが大切です。

【5.27 情報セキュリティインシデントからの学習】

実施手順（例）
a. 情報セキュリティ委員会は、セキュリティインシデントを管理・分析し、問題があれば、計画を立ててトップマネジメント（経営層）へ提議する。計画には、解決に向けての処置方法・費用・実施予定日・責任者を明確にする。 b. 将来のセキュリティインシデントの起こりやすさや影響を減らすため、情報セキュリティ委員会は、セキュリティインシデントから得られた知識を活かして「6.3 情報セキュリティの意識向上、教育及び訓練」を強化・改善する。
ワンポイントアドバイス セキュリティインシデントの形態、規模および費用を定量化および監視するための手順を確立することが大切です。

【5.28 証拠の収集】

実施手順（例）
情報セキュリティ委員会は、情報システムの事故が特定の個人、または組織に起因するもので、事後処置が法的処置に及ぶ可能性のある場合には、必要な証拠の収集、保全に努める。
ワンポイントアドバイス 懲戒処置および法的処置のために情報セキュリティ事象に関連する証拠を取扱う場合は、内部の手順を定めて従うことが大切です。

15-2-6. 事業継続計画策定

事業継続計画策定に関連する実施手順の例を紹介します。

【5.29 事業の中断・阻害時の情報セキュリティ】

実施手順（例）
a. 資産のリスク分析 b. 「資産目録（情報資産管理台帳）」で特定した情報資産のうち、可用性の評価値が 3 の重要資産を情報セキュリティ継続のリスク分析対象とする。 ※ 可用性の評価値は、「12-2-2. リスク特定」で記載している方法により算出する。 c. a において登録した資産に対して、以下のリスクについて考慮する。 ● 地震・火災・洪水などの自然災害 ● 人的なミス ● システム障害 ● 健康上の問題 d. b のリスクが生じた際に影響を受ける業務プロセスを特定し、リスクが発生した場合のシナリオを作成する。

e. リスクが生じた場合の影響度と、リスクが発生する可能性について検討し、検討結果に基づき優先順位を決定する。
f. d において、優先順位が高いと判断したものに対して「事業継続計画書」を作成し、トップマネジメント（経営層）の承認を得る。
g. 「事業継続計画書」には以下の内容を含む。

- 実行開始条件（リスクシナリオの発生）
- 非常時手順（発生時の連絡手順）
- 回復手順（復旧のための手順）
- 回復目標（目標時間を必要に応じて決定）
- 再開手順（回復後のリハーサル手順）
- 試験のスケジュール
- 教育（教育が必要な場合はその計画）

h. 策定した計画および手続きについて試験を実施し、試験の結果、必要があると判断した場合は計画を更新する。試験は以下のいずれかの方法、またはその組み合わせにより行う。

- 机上試験
- 模擬試験
- 技術的回復試験
- 代替施設における回復試験
- 供給者施設およびサービスの試験

i. 情報セキュリティ委員会は、事業継続に関する試験を最低年 1 回、継続的に実施する。

ワンポイントアドバイス

事業の中断または阻害時に、重要な事業プロセスの情報セキュリティを維持または復旧するために、計画を策定、実施、試験、レビューおよび評価することが大切です。

【5.30 事業継続のための ICT の備え】

実施手順（例）

a. ビジネスインパクト分析（不測のインシデントによって業務やシステムが停止した場合、会社の事業にどのような影響があるかを分析すること）を行い、事業継続が困難な状況を特定する。
b. 事業が中断・停止になった際の対応手順を策定し、文書化する。
c. 策定した対応手順が有効であることを確実にするため、あらかじめ定めた間隔（年 1 回以上）で試験を実施し検証する。

ワンポイントアドバイス

組織が ICT サービス事業の中断・阻害を管理する方法を詳述した対応および復旧手順を含む ICT 継続計画を、演習および試験を通じて定期的に評価、または経営陣が承認することが大切です。

15-2-7. 法的、規制および契約上の要件

法的、規制および契約上の要件に関連する実施手順の例を紹介します。

【5.19 供給者関係における情報セキュリティ】

実施手順（例）
a. 当組織における供給者には、以下がある。 ● ISP、電話サービス、IT 機器などのサービス提供者 ● 情報システムの開発・保守における外部委託先 ● 会計、税務、法律などの専門サービス提供者 ● 清掃業者、廃棄業者 ● クラウドサービス b. 情報セキュリティ委員会は、部外者・外部組織からのオフィスエリアや情報システムへのアクセスを許可する際に生じる可能性があるリスクを考慮し、情報セキュリティ上の要求事項を明確にする。
ワンポイントアドバイス 供給者が提供する製品およびサービスの使用に関連するセキュリティリスクに対処するためのプロセスおよび手順を特定し、実施することが大切です。

【5.20 供給者との合意における情報セキュリティの取扱い】

実施手順（例）
a. 提供されるサービスの利用は、次の手順に従い行う。 1. 「委託先審査票」による評価・選定を行う。 2. 情報セキュリティ要求事項を考慮し、次の事項を含む契約を締結する。 ● 機密保持契約などの情報の取扱いに関する契約 ● 使用許諾に関する取り決め、コードの所有権および知的所有権（開発の場合） ● 実施される作業場所および入退室管理 ● 外部委託先が不履行となった場合の預託契約に関する取り決め 3. 情報セキュリティ委員会は、「5.19 供給者関係における情報セキュリティ」において検討したリスクを考慮し、必要に応じて第三者との間で契約を締結する。 b. クラウドサービスを介して重要資産を取扱う際は、利用者は多要素認証を有効にしてセキュリティを強化する必要がある。
ワンポイントアドバイス 組織と供給者の間で情報セキュリティ要求事項を満たす義務に関し、当事者間で合意を確立し、文書化することが大切です。

【5.21 ICT サプライチェーンにおける情報セキュリティの管理】

実施手順（例）
a. ICT 製品・サービスの供給者との契約には、必要に応じて再委託に関する事項を盛り込む。 b. クラウドサービスの利用にあたっては、クラウドサービス提供者の事業継続性、および以下のサービスに関する情報セキュリティ事項を考慮の上、クラウドサービスを選定する。 ● サービスの導入実績、信頼性 ● 利用者サポート機能 ● 利用終了後のデータの扱い ● サービスの可用性 c. 暗号化など、通信経路の安全対策
ワンポイントアドバイス 信頼できる供給源から ICT を取得する手順を明確にすることが大切です。

【5.31 法令・規制及び契約上の要求事項】

実施手順（例）
a. 情報セキュリティ委員会は、当組織が順守すべき法令、規制、および契約上の要求事項を識別し、「情報セキュリティに関する法令規制一覧表」に記載する。「情報セキュリティに関する法令規制一覧表」は最低年 1 回見直す。 b. 情報セキュリティ委員会は、当組織の従業者が「情報セキュリティに関する法令規制一覧表」を、必要に応じていつでも参照できる状態にする。 c. 特定した要求事項を満たすために、必要に応じて教育などのテーマとする。 d. 暗号化した装置を輸出する場合、または海外に持ち出す場合、該当する法規制について調査を行い、必要であれば対応を行う。
ワンポイントアドバイス 総務省の Web サイト「国民のためのサイバーセキュリティサイト サイバーセキュリティ関連の法律・ガイドライン」で、サイバーセキュリティに関する代表的な法律が紹介されています。

情報セキュリティに関連する法律（例）	概要
特定電子メールの送信の適正化等に関する法律	利用者の同意を得ずに広告、宣伝または勧誘などを目的とした電子メールの送信を禁止している。
電子署名及び認証業務に関する法律	「本人による一定の条件を満たす電子署名」がなされた文書は、本人の手書署名・押印がある文書と同様、真正に成立したものと推定されることが定めら

	れている。
著作権法	プログラムやマニュアル、ホームページなどは、著作権の対象であり、無断での複製は、著作権法の侵害になる。
不正アクセス禁止法	不正アクセス行為や、不正アクセス行為につながる識別符号（ID、パスワード）の不正取得・保管行為、不正アクセス行為を助長する行為などを禁止している。
刑法	無断でデータを改ざん・破壊する行為や、虚偽の金融機関を名乗ったサイトや電子メールを使い、金銭をだまし取るような行為などは、刑法に違反する。

詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ関連の法律・ガイドライン	https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/legal

15-2-8. 知的財産、データ、プライバシー

知的財産、データ、プライバシーに関連する実施手順の例を紹介します。

【5.32 知的財産権】

実施手順（例）
a. 知的財産権を保護するためのルールを策定し、組織内で教育・啓発活動を行う。 b. 知的財産権を侵害する行為を禁止する。 c. 知的財産権を侵害する行為が発生した場合には、速やかに是正措置を講じる。 d. ソフトウェアなどの使用許諾計画を順守する。 e. 情報システム管理者は、パッケージソフトウェアのライセンス管理を適切に行う。
ワンポイントアドバイス 知的財産権には、ソフトウェアまたは文書の著作権、意匠権、商標権、特許権およびソースコード使用許諾権が含まれます。

【5.33 記録の保護】

実施手順（例）
当組織における記録は、関連する法令に基づき次表の保存期間にわたり、消失、破壊、改ざん、不正なアクセス、流失などがないように適切に保存する。
ワンポイントアドバイス 記録は、記録の種類（会計記録、商取引記録、人事記録、法的記録など）によって分類し、それぞれに保存期間の詳細と、物理的または電子的な保存が可能な保存媒体の種類を記載するこ

とが大切です。

記録の種類と保存期間

記録の種類	保存期間
■定款 ■登記関係書類 ■訴訟関係書類 ■特許など知的所有権に関する書類 ■社則・社規	永久
■「商業帳簿」 会計帳簿（日記帳、仕訳帳、総勘定元帳）、貸借対照表、損益計算書、附属明細書 ■「営業に関する重要な書類」 株主名簿、社債原簿、株主総会議事録、取締役会議事録、営業報告書、利益処分案（損失処理案）、このほか紛争が生じた場合に重要な証拠となり得る書類（例：契約書）	10 年
■仕訳帳、総勘定元帳、現金出納帳、固定資産台帳、売掛帳、買掛帳、経費帳 ■棚卸表、貸借対照表、損益計算書、決算に関して作成された書類 ■注文書、契約書、送り状、領収書、見積書、その他これらに準ずる書類（例：請求書）	7 年
■給与所得者の扶養控除など（異動）申告書 ■給与所得者の保険料控除申告書兼給与所得者の配偶者特別控除申告書 ■源泉徴収簿	
■財産形成非課税貯蓄申込書・移動申請書	5 年
■雇用保険被保険者に関する書類	4 年
■労働者名簿 ■賃金台帳 ■雇入・解雇・災害補償・賃金その他労働関係に関する重要な書類	3 年
■労働保険料の徴収に関する書類	
■労災保険に関する書類	
■安全委員会議事録 ■衛生委員会議事録 ■安全衛生委員会議事録	
■健康保険に関する書類	2 年
■厚生年金保険に関する書類	
■雇用保険に関する書類	

【5.34 プライバシー及び PII の保護】

実施手順（例）
個人情報は、「5.10 情報およびその他の関連資産の利用の許容範囲」の取扱いルールに従い、厳重に取扱う。
ワンポイントアドバイス プライバシーの保持および PII 保護のための手順を策定および実施することが大切です。

15-2-9. セキュリティ対策状況の点検・監査・評価・認証

セキュリティ対策状況の点検・監査・評価・認証に関連する実施手順の例を紹介します。

【5.22 供給者のサービス提供の監視、レビュー及び変更管理】

実施手順（例）
a. 情報セキュリティ委員会は、サービスの供給者に対して、あらかじめ定められた頻度（最低年 1 回）において契約の履行状況ならびに「委託先審査票」による順守状況の確認を行う。 b. サービスの供給者との間で契約内容やサービスレベルに変更があった場合、変更点を受け入れることができるか否かを検証し、契約内容の見直しを実施する。
ワンポイントアドバイス サービスの提供において不完全な点があった場合は、適切な処置をとることが大切です。

【5.35 情報セキュリティの独立したレビュー】

実施手順（例）
a. 年に 1 度、内部監査により独立したレビューを行う。 b. 以下に例示する、情報セキュリティに影響のある変化が生じた場合も、内部監査により独立したレビューを行う。 ● 事業の追加/変更、業務手順の大幅な変更 ● 住所変更、拠点の新設 ● 情報セキュリティに関する主たる担当者の変更 ● 関係する法令・規制、または契約の大幅な変更
ワンポイントアドバイス 独立したレビューにおいて、情報セキュリティに関して取組が不十分であると明確になった場合には、経営陣は是正処理を発議することが大切です。

【5.36 情報セキュリティのための方針群、規則及び標準の順守】

実施手順（例）
a. 情報セキュリティ委員会は、セキュリティに関する手順や実施標準が正しく実施されていることを確実にするため、「運用チェックリスト」にて、定期的（3 ヶ月ごと）に点検を行

う。

b. 情報セキュリティ委員会（入退管理責任者）は、入退記録が適切にとられているか否かを月に 1 度確認する。また、入退管理が有効かつ適切に実施されていることを定期的に確認し、不備が発見された場合は速やかに是正の処置をとる必要がある。

c. 情報システム管理者は、技術的な順守事項が正しく実施されていることを確実とするため、上記の a、b に従い点検する。

ワンポイントアドバイス

是正処置が完了しない場合は、確認時に進捗状況を報告することが大切です。

【5.37 操作手順書】

実施手順（例）

情報処理設備の正確、かつ、セキュリティを保った運用を確実とするために、次の事項を明記した手順書を文書化し、必要に応じて利用者が参照できるようにする。

システムが故障した場合の再起動および回復の手順

a. 記憶媒体の取扱い手順

b. バックアップの取得手順

c. 保守手順

d. 容量、能力、パフォーマンスおよびセキュリティなどの監視手順

ワンポイントアドバイス

操作手順書は必要に応じてレビューし、更新することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

第16章. 人的対策

章の目的
第 16 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標
◘ 人的管理策をもとに、対策基準を策定する手順を理解すること ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

16-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
6.1 選考		6.5 雇用の終了又は変更後の責任	
6.2 雇用条件		6.6 秘密保持契約又は守秘義務契約	
6.3 情報セキュリティの意識向上、教育及び訓練		6.7 リモートワーク	
6.4 懲戒手続		6.8 情報セキュリティ事象の報告	

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMS に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）

6.1 選考

従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。

6.2 雇用条件

雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。

6.3 情報セキュリティの意識向上、教育及び訓練

従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。

6.4 懲戒手続

情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。

6.5 雇用の終了又は変更後の責任

雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、明確にしなければならない。

6.6 秘密保持契約又は守秘義務契約

組織の要求事項を反映した秘密保持契約または守秘義務契約を従業員や外部の関係者と締結しなければならない。

6.7 リモートワーク

要員が遠隔で作業する場合は、セキュリティ対策を実施しなければならない。

6.8 情報セキュリティ事象の報告

情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告できる仕組みを設けなければならない。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

16-2. 人的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引きを参考に、自社に適した実施手順を策定してください。

16-2-1. スクリーニング

【6.1 選考】

実施手順（例）
従業者の募集・採用プロセスは以下の点を考慮のうえ行う。 a. 取得した履歴書、スキルシートなどから業務上の要求事項に対する適合を判断し、選考を行う。 b. 採用時の面接などにおける態度や言葉遣いなどから倫理観を判断し、選考を行う。 c. 役員や管理職の採用に関しては、過去の信用情報など、より詳細な調査を行う場合があるが、この際は本人の同意を得たうえで行う。
ワンポイントアドバイス 選考プロセスはフルタイム、パートタイム、臨時スタッフを含むすべての従業員に対して実行することが大切です。

16-2-2. 雇用契約書

【6.2 雇用条件】

実施手順（例）
情報セキュリティに関する責任を理解し、情報セキュリティ方針を守ることを従業員に誓約させるため、雇用契約書に、情報セキュリティに関する事項を盛り込み、誓約書に署名を求める。
ワンポイントアドバイス 従業員に、情報セキュリティに関する雇用条件を同意させることが大切です。

16-2-3. 懲戒手続き

【6.4 懲戒手続】

実施手順（例）
従業者が故意または過失により情報を漏えいした場合、または情報セキュリティ上の遵守事項に違反した場合は、罰則の対象とする。
ワンポイントアドバイス

懲戒手続は、関連する法令、規制、契約および事業上の要求事項を考慮に入れることが大切です。

16-2-4. 雇用の終了または変更後の責任

【6.5 雇用の終了又は変更後の責任】

実施手順（例）
情報セキュリティの観点から、雇用の終了または変更後も従業員が守るべき義務や責任（例えば守秘義務）について定め、雇用時の誓約書に盛り込むと同時に、雇用の終了または変更時に再確認する。
ワンポイントアドバイス 雇用の終了または変更を管理する手続では、終了または変更後にどの情報セキュリティの責任および義務を引き続き有効とすることが望ましいかを定義することが大切です。

16-2-5. 守秘義務または秘密保持契約

【6.6 秘密保持契約又は守秘義務契約】

実施手順（例）
a. 当組織の従業者は、当組織との間で機密情報に関する秘密保持の契約を締結する。なお、同契約には原契約の終了後も一定期間、秘密保持の義務が課せられる旨の条項を含める。 b. 当組織との委託先との間で、必要に応じて秘密保持の契約を締結する。 c. 情報セキュリティ委員会は、年に一度、情報セキュリティ要求事項に照らして、秘密保持契約書の妥当性を検証する。
ワンポイントアドバイス 秘密保持契約または守秘義務契約に関する要求事項は、定期的または要求に影響する変化が発生した場合に、レビューすることが大切です。

【6.3 情報セキュリティの意識向上、教育及び訓練】

実施手順（例）
a. すべての従業者は、職務に関連する方針および手順についての適切な、意識向上のための教育および訓練を受ける必要がある。 b. 当組織では従業者が次の事項に関して認識を持てるよう教育・訓練を実施する。 ● 情報セキュリティ方針 ● 情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティに対する自らの貢献 ● ISO/IEC 27001 の要求事項に適合しないことの意味 c. 教育計画は情報セキュリティ委員会が作成し、トップマネジメント（経営層）が承認する。

d. 当組織の主な教育を以下に示す。（以下の教育は「教育実施記録」に残す。）

- ●新任部門管理者（運用委員）

  新任の情報セキュリティ委員会メンバーに実施する。

- ●入社時・社内異動者の教育（適時）

  新入社員、中間採用者に対して、入社時にセキュリティ教育を実施する。

- ●定期教育（「年間計画表」に基づく）

  年に最低 1 回、適用範囲内の従業者に対して、情報セキュリティの理解、再確認と改善、向上のための教育を実施する。

- ●再教育

  セキュリティ違反者および情報セキュリティに関する低理解度の従業者に対して、再教育を実施し、違反の再発防止に努める。

- ●実施した教育の有効性評価

上記の教育実施後理解度調査などを実施し、実施した教育の有効性について評価を行う。

ワンポイントアドバイス

知識が伝わったこと、並びに意識向上、教育および訓練プログラムの有効性を確認するため、意識向上、教育および訓練の活動終了時に、従業員理解の評価を行うことが大切です。

16-2-6. リモートワーク実施手順

【6.7 リモートワーク】

実施手順（例）

a. リモートワークは、情報セキュリティ委員長の承認を得たものに限って行える。

b. リモートワークにて使用する PC は、会社から貸与した PC とし、家族などの同居人と共有することは禁じる。

c. リモートワークにて使用する PC は、アンチウイルスソフトを導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。

d. リモートワークにて使用する PC に、ファイル交換ソフトなどの不正なソフトウェアをインストールすることは禁じる。

e. 社内ネットワークへは VPN にて接続する。

ワンポイントアドバイス

リモートワークで個人所有の PC を使用する場合は、管理方法や接続方法について実施手順を記載することが大切です。

16-2-7. 情報セキュリティイベントの報告

【6.8 情報セキュリティ事象の報告】

実施手順（例）
情報セキュリティ事象は、「5.25 情報セキュリティ事象の評価及び決定」に従って報告し、評価を行う。
ワンポイントアドバイス すべての従業員が情報セキュリティ事象を報告する連絡先を認識し、報告の仕組みはできるだけ簡単で使いやすく、いつでも利用できるようにすることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

第17章. 物理的対策

章の目的
第 17 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標
◘ 物理的管理策をもとに、対策基準を策定する手順を理解すること ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

17-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
7.1 物理的セキュリティ境界		7.8 装置の設置及び保護	
7.2 物理的入退		7.9 構外にある資産のセキュリティ	
7.3 オフィス、部屋及び施設のセキュリティ		7.10 記憶媒体	
7.4 物理的セキュリティの監視		7.11 サポートユーティリティ	
7.5 物理的及び環境的脅威からの保護		7.12 ケーブル配線のセキュリティ	
7.6 セキュリティを保つべき領域での作業		7.13 装置の保守	
7.7 クリアデスク・クリアスクリーン		7.14 装置のセキュリティを保った処分又は再利用	

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMS に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）
7.1 物理的セキュリティ境界 情報およびその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。 **7.2 物理的入退** セキュリティを保つべき領域は、適切な入退管理策および立寄り場所によって保護しなければ

ならない。

7.3 オフィス、部屋及び施設のセキュリティ

オフィス、部屋および施設に対する物理的セキュリティを設計し、実装しなければならない。

7.4 物理的セキュリティの監視

施設は、認可されていない物理的アクセスについて継続的に監視しなければならない。

7.5 物理的及び環境的脅威からの保護

自然災害およびその他の意図的または意図的でない、インフラストラクチャーに対する物理的脅威などの物理的および環境的脅威に対する保護を設計し、実装しなければならない。

7.6 セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施しなければならない。

7.7 クリアデスク・クリアスクリーン

書類および取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施しなければならない。

7.8 装置の設置及び保護

装置は、セキュリティを保って設置し、保護しなければならない。

7.9 構外にある資産のセキュリティ

構外にある資産を保護しなければならない。

7.10 記憶媒体

記憶媒体は、組織における分類体系および取扱いの要求事項に従って、取得、使用、移送および廃棄のライフサイクルを通して管理しなければならない。

7.11 サポートユーティリティ

情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。

7.12 ケーブル配線のセキュリティ

電源ケーブル、データ伝送ケーブルまたは情報サービスを支援するケーブルの配線は、傍受、妨害または損傷から保護しなければならない。

7.13 装置の保守

装置は、情報の可用性、完全性、機密性を維持することを確実にするために、正しく保守しなければならない。

7.14 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した装置は、処分または再利用する前に、すべての取扱いに慎重を要するデータおよびライセンス供与されたソフトウェアを消去していること、またはセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

17-2. 物理的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順例を紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引きを参考に、自社に適した実施手順を策定してください。

17-2-1. 物理的なセキュリティ境界

【7.1 物理的セキュリティ境界】

実施手順（例）
a. 当組織は、「レイアウト図」により、セキュリティ境界を定義する。 ※レイアウト図は、「13-2-2. ISMS:4. 組織の状況」の「4-3.情報セキュリティマネジメントシステムの適用範囲の決定」内の「物理的境界 レイアウト図（例）」を参照 b. 重要な情報資産がある領域の入退を制限し、入退資格を有さない者の立ち入りを制限する。
ワンポイントアドバイス 許可されていない者の物理アクセスを防ぐために、入口に「関係者以外立入禁止」の表示や、入退制限の標識をつけるなどの工夫は効果的です。 

17-2-2. 入退室認証システム

【7.2 物理的入退】

実施手順（例）
a. 入退を行う対象者に対して、入退資格を設け、資格を持たない者の立ち入りを禁じる。入退資格は、従業者証またはセキュリティカードを交付することにより付与し、他人への貸借は禁じる。 b. 外来者の訪問は、原則として、「入退受付票」に氏名、身元、入退時刻を記録し、面談者が面会確認の押印または署名を行い、退出するまでエスコートする。 c. 宅配便などの荷物を受け取る場合は、各オフィスの入口より外で行うことを原則とし、例外的にオフィス内への入室を認める場合は、必ず応対者がエスコートする。
ワンポイントアドバイス 荷物の受け取り場所は、重要な情報処理設備から離れた場所に設定することが大切です。

【7.3 オフィス、部屋及び施設のセキュリティ】

実施手順（例）

a. 各事業場は常時施錠可能とし、入退資格を持たない者の立ち入りを禁じる。やむを得ず施錠可能でない事業場においては、重要な情報はキャビネットに収納し施錠するなど、厳重な管理を行う。
b. 施錠、開錠は、原則として従業者が行う。
c. 入退を許可された外来者に対しては、原則として従業者が随行し、立ち入り場所を制限する。
d. 秘密の情報または活動が外部から見えないよう、ブラインドやパーティションを設置する。

ワンポイントアドバイス

活動内容や PC のモニタなどが外部から見えたり、聞こえたりすることがないよう、外部来場者の動線ルートを事前に決めておくことが大切です。

17-2-3. 物理的セキュリティの監視

【7.4 物理的セキュリティの監視】

実施手順（例）

a. 組織の施設は、監視カメラ、侵入者警報を設置し、認可されていないアクセスや、疑わしい行動を検知する。無人の領域には、必ず監視カメラおよび侵入者警報を設置する。
b. 監視カメラ、侵入者警報の動作確認をするため、3 か月に 1 回点検を実施する。

ワンポイントアドバイス

無人の領域は、警報器を設置することが大切です。

17-2-4. 物理的および環境的脅威からの保護

【7.5 物理的及び環境的脅威からの保護】

実施手順（例）

a. 各フロアには、火災報知器、消火器を設置する。
b. サーバ付近に段ボールなどの燃えやすいものを置くことを禁じる。
c. サーバの転倒対策として設置位置を工夫する。必要に応じて、転倒防止器具を利用するなどの対策を行う。

ワンポイントアドバイス

ハザードマップなどにより自社の地理的な脅威を把握し、災害時における具体的対策を講じて

おくことが重要です。

【7.6 セキュリティを保つべき領域での作業】

実施手順（例）

a. サーバ室には、スマートフォンやボイスレコーダー、カメラなど撮影や録音ができるものや、USB メモリなどサーバの情報をダウンロードできる機器の持ち込みは禁じる。
b. セキュリティを保つべき領域は常時施錠し、入退資格を持たない者の立ち入りを禁じる。

ワンポイントアドバイス

セキュリティを保つべき領域での作業ルールが適切に守られているか確認することが大切です。

【7.7 クリアデスク・クリアスクリーン】

実施手順（例）

a. クリアデスク
   - 離席時や帰宅時には、重要情報や個人情報を含む書類や記憶媒体を机上やその周辺に放置しない。
   - 書類やデータは、重要なものとそうでないものを区別して整理する。
   - プリンタ、コピーに出力した印刷分は放置せず速やかに取り出す。

b. クリアスクリーン
   - 利用者は、食事やトイレ、会議などにより自席を離れる場合には、コンピュータのログアウト（ログオフ）やスクリーンロックを行い、第三者がコンピュータを操作したり、画面を盗み見たりできないようにする。
   - ログイン ID、パスワードを机上に貼付することは禁じる。

ワンポイントアドバイス

クリアデスク、クリアスクリーンについてのルールが適切に守られているか、チェックシートなどにより徹底することも効果的です。

【7.8 装置の設置及び保護】

実施手順（例）

a. スイッチ、無線 LAN アクセスポイントなどは、人目につくところや通行量の多い場所を避けて設置する。
b. サーバは、サーバ室など隔離されたエリアに設置する。隔離されていないエリアに設置す

る場合は、ラックなどへ収容する。
c. サーバが設置されたエリアでの飲食、喫煙は禁じる。
d. サーバが設置されたエリアの温度、湿度を監視し、サーバに悪影響を与えない状態を維持する。

ワンポイントアドバイス
サーバ周辺に水などの配管などが通っていないか、確認することが大切です。

17-2-5. オフプレミスの資産のセキュリティ

【7.9 構外にある資産のセキュリティ】

実施手順（例）

a. 社外にノート PC などを持ち出す場合は、
   ① ログインパスワードを設定する。
   ② 必要のない機密情報、個人情報を格納しない。
   ③ 格納するファイルは暗号化する（パスワードをつける）。
   ④ OS・ソフトウェアが最新バージョンになっており、セキュリティソフトが入っていることを確認する。
   ⑤ ノート PC などが入ったカバンなどを交通機関の網棚などには置かず、常時携帯する。
b. 公共交通機関を利用する際に、顧客情報や個人情報など、重要な情報をノート PC や社用携帯で閲覧することは禁じる。

ワンポイントアドバイス
公共交通機関を利用する際に、装置（例：スマートフォン、ノート PC など）上の情報をのぞき見られるリスクから保護することが大切です。

17-2-6. 機器のメンテナンス

【7.10 記憶媒体】

実施手順（例）

a. 外づけの記録媒体を持ち出し・持ち込みする場合は、事前に許可を得た上で行う。また、不使用時は、キャビネットに施錠保管を行う。
b. 記憶媒体に収納する情報は必要最小限なものとし、必要のない機密情報や個人情報、会社の重要情報は保存しない。
c. 格納するファイルは暗号化して（パスワードをつけて）保存する。

d. 外部記憶媒体や、重要な情報が記された文書を机上や、棚上などに放置することは禁じる。
e. 私有の外部記憶媒体を持ち込む場合、社有の外部記憶媒体を持ち出す場合は、該当部門の責任者および情報システム管理者の許可を得る。
f. 外部記憶媒体によるデータを受け渡しは、データの内容に応じてセキュリティを確保できるような受け渡し方法をとる。
g. お客様の USB メモリなどの記憶媒体を預かった場合は、使用する前に必ずアンチウイルスソフトによりスキャンを行う。
h. 不要な媒体を処分する場合は、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。
i. 媒体を輸送する場合は、必要に応じて梱包などにより保護するとともに、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。
j. サーバ、ネットワーク機器（スイッチ、ルータなど）の設置場所を、情報システム管理者の許可なく移動することは禁じる。
k. 当組織の資産および顧客から預かった資産を、情報セキュリティ委員長の許可なく無断で持ち出すことは禁じる。

ワンポイントアドバイス

USB メモリやハードディスクなどの記憶媒体に加えて、紙の文書に対してもセキュリティ対策を行うことが大切です。

【7.11 サポートユーティリティ】

実施手順（例）

a. 情報システム管理者は、必要に応じて無停電電源装置を設置する。無停電電源装置は、ランプの確認などにより、バッテリーの寿命が尽きていないことや、緊急時の切り替えが問題なく行えるかを定期的に確認する。
b. 情報システム管理者は、フロア（装置の設置場所）が適切な温度に保たれていることを適時確認する。

ワンポイントアドバイス

停電対策として無停電電源装置に加えて、補助発電装備を利用することも有効です。

【7.12 ケーブル配線のセキュリティ】

実施手順（例）

a. 人が通る箇所のケーブル配線は、できるだけ床下か天井に配線する。床上に配線する場合

には、モール、ケーブルカバーによる保護を行う。
b. 配線ケーブルに異常がないか、3 か月に 1 回点検を行う。
c. 誤接続を防止するために、ケーブルにラベルをつける、役割ごとに色の異なるケーブルを使う。
d. ケーブル配線図を作成するとともに、機器の増設や移設により配線が変更になった場合には配線図を更新する。

ワンポイントアドバイス

周辺機器の増設や移設に際して、ケーブル類の適正化を確認することが大切です。

【7.13 装置の保守】

実施手順（例）

サーバ、ネットワーク機器など主要な装置は、製造元から提供されたマニュアルを参照し、製造元が推奨する頻度にて点検、保守を行い、記録する。

ワンポイントアドバイス

装置の点検・保守が定期的に実施され、記録されているか確認することが大切です。

【7.14 装置のセキュリティを保った処分又は再利用】

実施手順（例）

a. PC を処分する場合は、従業員が各自で処理せず、情報システム管理者に処理を依頼する。情報システム管理者は、ハードディスクなどの記憶媒体については、物理的破壊もしくは、完全消去により処分する。
b. 上記以外の方法により、処分する必要があると認められる場合、事前に情報セキュリティ委員長の承認を得ることを要するものとする。
c. 情報システム管理者は、装置を再利用する場合、不要な情報を完全に消去し、またライセンス供与されたソフトウェアが消去されたことを確認の上、再利用する。

ワンポイントアドバイス

廃棄・再利用する際、情報を消去する責任者と手順を定めることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

17-3. BYOD、MDM

17-3-1. BYOD（Bring Your Own Device）導入に向けて

関連する主な管理策
6.3、6.7、7.9、8.1、8.7

BYOD の概念や、導入に向けたポイント、運用手順を説明します。

BYOD（Bring Your Own Device）

BYOD とは、個人が私物として所有している端末（PC やスマートフォンなど）を業務に使う利用形態のことです。従来は、業務で使用する端末は企業が購入し、従業員に貸与することが一般的でした。しかし、使い慣れた端末を利用できることによる働きやすさの実現や、端末購入コストの削減などの観点から、従業員が持つ私物のデバイスを業務に利用する BYOD が導入されるようになりました。

BYOD の主なメリット・デメリット

メリット	デメリット
● コスト削減 企業は、端末の調達や管理にコストがかかりません。故障した際の修理費用や老朽化した端末の入替も基本的には個人負担となります。 ● 使い慣れた端末の業務利用 従業員は、自分の使い慣れた端末を使用でき、操作方法や設定などを新たに覚える必要がないため作業効率があがります。また、仕事用とプライベート用に分けて端末を複数台持つ必要がなくなります。	● シャドーIT ルールの整備や技術的な対策を講じないと、シャドーIT が増加してしまう恐れがあります。 ● セキュリティリスク 個人の端末では、さまざまな Web サイトやアプリケーションを利用することがあるため、ウイルス感染や不正アクセスといった被害にあう可能性が高くなります。

BYOD を運用する際のポイント

BYOD を運用する際は、適切なルールを策定し、周知することが重要です。また、ルールに加えて、技術的な対策を講じることも重要です。

運用手順（例）
a. BYOD に関する使用ルールや禁止事項を決めて周知する。 b. BYOD で使用する機器については管理者に申請し、許可を得る。 c. BYOD で使用する機器が紛失した場合の対応フローを策定し、周知する。 d. BYOD で行える業務範囲やリモートアクセスの権限を設定する。 e. 社内ネットワークへは、VPN を利用する場合のみ接続できるようにする。 f. 必要以上に業務データを蓄積させない。（保存可能なデータに関するルールを決める。） g. 業務で使用する PC は、EDR を導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。 h. 業務で使用する PC に、ファイル共有ソフトなどの不正なソフトウェアをインストールすることは禁じる。

17-3-2. MDM（Mobile Device Management）導入のポイント

関連する主な管理策
6.7、7.9、8.1

MDM の概念や、導入に向けたポイント、運用手順について説明します。

MDM（Mobile Device Management）
MDM とは、企業が保有しているモバイル端末（スマートフォンやタブレットなど）を一元管理できるシステムのことです。オフィスの外にあるデバイスも管理できます。ポリシー（パスワードの長さやロック画面の解除方法、インストールできるアプリケーションの制限など）を従業員のモバイル端末に適用し、違反した場合に警告を行ったり管理者に通知したりできます。また、万が一紛失や盗難があった際には、位置情報の確認や遠隔でモバイル端末の画面をロックしたり、リモートワイプ（端末に保存されているデータを遠隔で初期化する機能）したりすることができ、機密情報を守れます。

MDM を導入する際のポイント	
コスト・費用	MDM は導入して終わりではなく、維持費がかかります。自社の予算に合わせた確認をすることが大切です。
対応している OS の確認	すべての OS に対応している MDM もあれば、一部のみに対応している MDM もあります。導入する MDM が、自社で使用している端末の OS に対応しているか確認することが大切

	です。
サポート体制	MDM の導入時や導入後の運用サポートなどが受けられるか確認することが大切です。
利用者の意見を反映した社内ルールの策定、および MDM の選定	MDM は情報セキュリティの向上や業務効率化に役立ちますが、いくつか注意点があります。例えば、紛失・盗難されたデバイスがネットワークに接続されていない場合には、初期化などのリモート制御ができません。また、MDM による制限が厳しくなりすぎると、使い勝手が悪くなり利用者から不満がでる可能性があります。利用者の意見を聞きながら、社内ルールの策定や MDM の選定を進めることが重要です。

MDM の運用手順について説明します。

運用手順（例）

a. モバイル端末の紛失・盗難時の対応
   1. 従業員は、モバイル端末を紛失・盗難にあった場合は、速やかに情報セキュリティ管理者に報告する。
   2. 情報セキュリティ管理者は、従業員からモバイル端末の紛失・盗難の報告を受けた場合、速やかにリモートでモバイル端末の画面をロックし、位置情報を確認する。
   3. 情報セキュリティ管理者は、モバイル端末の位置情報が確認できず、発見が困難であると想定される場合、リモートワイプを実施し、モバイル端末内のデータを削除する。

b. 業務で新たにアプリケーションが必要になった場合、情報セキュリティ管理者に連絡し、インストールの許可をもらう。

第18章. 技術的対策

- ◘ 技術的管理策をもとに、対策基準を策定する手順を理解すること
- ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること
- ◘ Security by Design、ゼロトラスト・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること

18-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
8.1 利用者エンドポイント機器		8.18 特権的なユーティリティプログラムの使用	
8.2 特権的アクセス権		8.19 運用システムに関わるソフトウェアの導入	
8.3 情報へのアクセス制限		8.20 ネットワークのセキュリティ	
8.4 ソースコードへのアクセス		8.21 ネットワークサービスのセキュリティ	
8.5 セキュリティを保った認証		8.22 ネットワークの分離	
8.6 容量・能力の管理		8.23 ウェブ・フィルタリング	
8.7 マルウェアに対する保護		8.24 暗号の使用	
8.8 技術的ぜい弱性の管理		8.25 セキュリティに配慮した開発のライフサイクル	
8.9 構成管理		8.26 アプリケーションのセキュリティの要求事項	
8.10 情報の削除		8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	
8.11 データマスキング		8.28 セキュリティに配慮したコーディング	

8.12 データ漏えいの防止		8.29 開発及び受入れにおけるセキュリティ試験	
8.13 情報のバックアップ		8.30 外部委託による開発	
8.14 情報処理施設の冗長性		8.31 開発環境、試験環境及び運用環境の分離	
8.15 ログ取得		8.32 変更管理	
8.16 監視活動		8.33 試験情報	
8.17 クロックの同期		8.34 監査試験中の情報システムの保護	

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMS に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）

8.1 利用者エンドポイント機器

利用者エンドポイントデバイスに保存されている情報、処理される情報、または利用者エンドポイントデバイスを介してアクセス可能な情報を保護しなければならない。

8.2 特権的アクセス権

特権的アクセス権の割り当ておよび利用は、制限し、管理しなければならない。

8.3 情報へのアクセス制限

情報およびその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。

8.4 ソースコードへのアクセス

ソースコード、開発ツール、ソフトウェアライブラリへの読取りおよび書込みアクセスを、適切に管理しなければならない。

8.5 セキュリティを保った認証

セキュリティを保った認証技術および手順を、情報へのアクセス制限およびアクセス制御に関するトピック固有の方針に基づいて備えなければならない。

8.6 容量・能力の管理

現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。

8.7 マルウェアに対する保護

マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。

8.8 技術的脆弱性の管理

利用中の情報システムの技術的脆弱性に関する情報を獲得しなければならない。また、そのような脆弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。

8.9 構成管理

ハードウェア、ソフトウェア、サービスおよびネットワークのセキュリティ構成を含む構成を確立、文書化、実装、監視し、レビューしなければならない。

8.10 情報の削除

情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。

8.11 データマスキング

データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。

8.12 データ漏えいの防止

データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存、送信するシステム、ネットワークおよびその他の装置に適用しなければならない。

8.13 情報のバックアップ

合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップを維持し、定期的に検査しなければならない。

8.14 情報処理施設の冗長性

情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性を持って、導入しなければならない。

8.15 ログ取得

活動、例外処理、過失、その他の関連する事象を記録したログを取得、保存、保護し、分析しなければならない。

8.16 監視活動

セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。

8.17 クロックの同期

組織が使用する情報処理システムのクロックは、国の原子時計から配信される時刻に基づくクロックと同期させなければならない。

8.18 特権的なユーティリティプログラムの使用

システムおよびアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。

8.19 運用システムに関わるソフトウェアの導入

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。

8.20 ネットワークのセキュリティ

システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。

8.21 ネットワークサービスのセキュリティ

ネットワークサービスのセキュリティ機能、サービスレベルおよびサービスの要求事項を特定し、実装し、監視しなければならない。

8.22 ネットワークの分離

情報サービス、利用者および情報システムは、組織のネットワーク上でグループごとに分離しなければならない。

8.23 ウェブ・フィルタリング

悪意のあるコンテンツにさらされることを減らすために、外部 Web サイトへのアクセスを管理しなければならない。

8.24 暗号の使用

暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。

8.25 セキュリティに配慮した開発のライフサイクル

ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。

8.26 アプリケーションのセキュリティの要求事項

アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。

8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、すべての情報システムの開発活動に対して適用しなければならない。

8.28 セキュリティに配慮したコーディング

セキュリティに配慮したコーディングの原則を、ソフトウェア開発に適用しなければならない。

8.29 開発及び受入れにおけるセキュリティ試験

セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。

8.30 外部委託による開発

組織は、外部委託したシステム開発に関する活動を指揮、監視し、レビューしなければならない。

8.31 開発環境、試験環境及び運用環境の分離

開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。

8.32 変更管理

情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。

8.33 試験情報

テスト用情報は、適切に選定、保護、管理しなければならない。

8.34 監査試験中の情報システムの保護

運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

18-2. 技術的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

18-2-1. エンドポイントデバイス

【8.1 利用者エンドポイント機器】

実施手順（例）

a. モバイル機器を社外に持ち出す場合、ログインパスワードを設定する。
b. 必要のない機密情報、個人情報などは、モバイル機器に格納しない。
業務上必要のある機密情報や個人情報をモバイル機器に格納する場合は、暗号化する。（パスワードをつける。）
c. モバイル機器を利用者が限定されない無償の WiFi スポットなどへ接続することは禁じる。
- 携帯電話・スマートフォンの管理
社有の携帯電話・スマートフォン（以下「社有携帯電話など」という）を使用する者は、紛失、破損しないよう丁寧かつ慎重に扱う。
- 社有携帯電話などを使用する者は、使用者本人以外が操作できないよう、パスワードを設定して保護する。
- 持ち歩く際は、ストラップをつけるなどの紛失・盗難防止策を必要に応じて講じる。
- 電車やバスの中、その他公共の場所における使用は控え、個人情報やその他機密情報を他者に聞かれないよう十分配慮する。
- 私有の携帯電話・スマートフォンを業務で使用する場合は、情報システム管理者の承認を要する。また、社有携帯電話などと同様の安全対策を実施する。

d. 利用者はノート PC に対して、パスワードつきのスクリーンセーバを設定し、のぞき見を防止する。スクリーンセーバの設定時間は 10 分以内とする。

ワンポイントアドバイス

利用者終端装置（携帯、スマートフォン、ノート PC など、ユーザーが情報処理サービスにアクセスするために使用するさまざまなデバイス）の取扱いに関する規則を定めることが大切です。

18-2-2. 特権アクセス権

【8.2 特権的アクセス権】

実施手順（例）
a. 特権的アクセス権は特定の者に付与し、管理対象システムとその保有者を明確にする。 b. 半年に 1 回、または組織に何か変更があった際、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任、力量の点で今も適格であるか否かを検証する。
ワンポイントアドバイス 特権的アクセス権は一般の利用者よりも多くの権限が付与されているため、悪用されると影響が大きいです。ID 付与に際しては、厳格かつ安全な管理のもとに運用されることが大切です。

18-2-3. アクセス制限

【8.3 情報へのアクセス制限】

実施手順（例）
a. 情報システム管理者は、取扱いに慎重を要する情報へのアクセス権限を、必要な者のみに割り当てる。 b. 未知の利用者識別情報または匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。
ワンポイントアドバイス 情報およびその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止することが大切です。

【8.4 ソースコードへのアクセス】

実施手順（例）
ソースコードや設計書、仕様書などの関連書類は、アクセス権で管理されたフォルダに厳重に保管する。
ワンポイントアドバイス ソースコードが変更される、または開発環境の一部のデータが認可されていない人物によって取り出される可能性をなくすため、ソースコードへのアクセスを適切に制御することが大切です。

18-2-4. 安全な認証

【8.5 セキュリティを保った認証】

実施手順（例）

重要な情報システムにアクセスする際は、パスワードに加えて、多要素認証を使用し、不正アクセスの可能性を減らす。

ワンポイントアドバイス

多要素認証では、知識（パスワード、秘密の質問など）、所持物（スマートフォン、IC カードなど）、生体情報（指紋、声紋など）のうち、2 つ以上を組み合わせて認証することで、認可されていないアクセスの可能性を減らします。

18-2-5. キャパシティ管理

【8.6 容量・能力の管理】

実施手順（例）

a. 情報システム管理者は、コンピュータやネットワークの応答時間など、その負荷状況について、業務を通じて問題がないか否かを確認する。CPU やメモリ、ハードディスクなどの外部記憶装置の使用率など、リソースの使用状況を定期的に監視する。
b. リソースの使用状況に応じてリソースの割り当てを調整すると同時に、将来必要となる容量や能力を予測し、システムのパフォーマンスを維持するため、必要なリソースを事前に確保する。
c. 情報システム管理者は、問題が発見された場合、速やかに原因の究明を行い、情報セキュリティ委員会に報告する。
d. 情報セキュリティ委員会は、情報システム管理者に対策を指示し、必要に応じて経営陣に報告する。
e. 情報システム管理者は、中長期的な業務量の増減を考慮し、将来的にシステムに必要な容量を予測し、必要であればトップマネジメントに報告する。

ワンポイントアドバイス

クラウドサービスを利用することで、特定のアプリケーションおよびサービスで利用できる資源を、要求に応じて迅速に拡張・削減することができます。

18-2-6. マルウェアに対する保護

【8.7 マルウェアに対する保護】

実施手順（例）

a. ネットワークに接続するすべてのパソコン、サーバ上に情報システム管理者が指定したアンチウイルスソフトを導入する。
b. アンチウイルスソフトを常時設定にし、ファイルへのアクセスおよび電子メールの受信時に常時スキャンできる設定を行う。
c. 常時スキャンに加えて情報システム管理者が指定した期間に一度、ファイル全体に対するスキャンを行う。
d. 自動でウイルス定義ファイルの更新が行われるように設定する。
e. 標的型メール対応
   - メールの添付書類やメール中のリンクは、原則として（送信者に確認するなどの方法で）安全が確認できるまで開かない。
   - ファイルの拡張子を表示させる設定とし、添付ファイルの拡張子が、通常使用しない内容の場合、ファイルの参照を禁じる。
     通常使用しないファイルの拡張子の例：.exe、.pif、.scr

ワンポイントアドバイス

基本的な対策として、社内パソコンのウイルス定義ファイルが常に最新版に更新されているかの確認を徹底することが重要です。

18-2-7. 技術的脆弱性の管理

【8.8 技術的脆弱性の管理】

実施手順（例）

a. 情報セキュリティ委員会および情報システム管理者は、技術的な脆弱性のニュースを常に意識し、時期を失せず効果的に外部の攻撃を防御する。
b. OS やアプリケーションには常に最新のセキュリティパッチを適用する。ただし、検証の結果、業務上支障があると認められる場合には、他の方法により脆弱性に対処する。

ワンポイントアドバイス

セキュリティパッチは、正当な供給元から取得したもののみを使用することが大切です。

18-2-8. 構成管理

【8.9 構成管理】

実施手順（例）

システムの構成要素とその相互関係を理解し管理するため、台帳や構成管理ツールを用いて、ハードウェア、ソフトウェア、ネットワーク機器、設定ファイルなど、システムを構成するすべての要素の情報を把握する。

ワンポイントアドバイス

ハードウェア・ソフトウェア・サービス・ネットワークが、必要とされるセキュリティ設定により正しく機能し、認可されていない変更や誤った変更によって構成が変えられないようにすることが大切です。

18-2-9. 情報の削除

【8.10 情報の削除】

実施手順（例）

a. 業務上必要がなくなったデータは速やかに削除する。
b. 記憶媒体上のデータを削除する際は、データ消去ソフトを使用し、復元できないよう、完全に削除する。
c. ハードディスクを廃棄する際は、磁気データ消去装置を用いてハードディスクのデータを削除してから廃棄する。

ワンポイントアドバイス

取扱いに慎重を要する情報などの機密情報については、必要がなくなった時点で速やかに削除することが大切です。情報を保有していることがリスクなので、不要な情報は持ちつづけないことが重要です。

18-2-10. データ保護

【8.11 データマスキング】

実施手順（例）

保有している情報をマーケティング分析などの目的で二次利用する場合には、個人情報や重要情報が推測できない形に加工した上で利用する。

ワンポイントアドバイス

取扱いに慎重を要するデータ（個人情報や重要情報）の保護が必要である場合、データマスキ

ング・仮名化・匿名化などの手法を使用して保護することが大切です。これにより、データが万が一漏えいしても、その内容を第三者に理解されることを防げます。

【8.12 データ漏えいの防止】

実施手順（例）

a. 漏えいから保護する情報を特定し、分類する。
b. ファイル共有ソフトの使用を禁じる。
c. 重要な情報が画面に表示されている場合は、スクリーンショットや写真を撮ることを禁じる。
d. ファイアウォールや IDS、IPS などによって不正アクセスを防止する。「8.20 ネットワークのセキュリティ」に従う。
e. 重要データについてアクセス制限を設ける。「8.3 情報へのアクセス制限」に従う。
f. 重要データは暗号化して保管する。「8.24 暗号の使用」に従う。

ワンポイントアドバイス

個人やシステムによる情報の認可されていない開示・抽出を検出し、防止することが大切です。

18-2-11. バックアップ

【8.13 情報のバックアップ】

実施手順（例）

a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてシステムおよびデータのバックアップを行う。
b. バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。
c. 情報システム管理者は、バックアップが確実に行われており、障害時に復元が可能か否かを月に 1 度チェックする。

ワンポイントアドバイス

クラウドサービスを利用している場合は、クラウド環境にあるデータのバックアップも作成しているか確認することが大切です。ランサムウェア対策として、バックアップは 2 つ作成し、1 つはネットワークから隔離したオフサイトで保管することが大切です。

18-2-12. 冗長化

【8.14 情報処理施設の冗長性】

実施手順（例）

a. 情報システムは、可用性に関する業務上の要求事項を明確にし、必要に応じて予備の機器を用意して二重化を行い、冗長性をもたせる。
b. 緊急の場合、速やかに予備の機器に切り替えられるよう、動作確認を月に 1 回行う。

ワンポイントアドバイス

冗長な構成要素および処理活動を常に作動させておくか、緊急の場合に自動または手動で作動させるかを確認します。常に作動させておく場合は、稼動状況を確認することが大切です。

18-2-13. ロギング

【8.15 ログ取得】

実施手順（例）

a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてログの取得を行う。
b. 情報システム管理者は、必要に応じてログの定期的なチェックを行う。
c. ログは、情報システム管理者またはその指名する担当がアクセスできるようにする。
d. 情報システム管理者は、運用担当者がサーバで行った作業を確認する。確認は、作業ログ、または日報・サーバ作業記録の閲覧により行う。

ワンポイントアドバイス

セキュリティインシデントの分析、警告および調査のために、システム間のログを相関づけられるようにすべてのシステムが同期した時刻源（8.17 クロックの同期を参照）を持つことが重要です。

18-2-14. 監視

【8.16 監視活動】

実施手順（例）

ファイアウォール・IDS・IPS のログを常に監視し、異常な動作を検知した場合は速やかに対応する。

ワンポイントアドバイス

通常時およびピーク時のシステム使用率や、各利用者または利用者グループの通常のアクセス時間・アクセス場所・アクセス頻度を考慮して正常な行動・動作の基準を確立し、基準に照ら

して異常を監視することが大切です。

18-2-15. クロック同期

【8.17 クロックの同期】

実施手順（例）

a. 情報システム管理者は、クライアント PC やサーバなどすべての情報システムについてクロックを同期させる。
b. すべての情報システムのクロックを同期させるために、NTP を使用する。

ワンポイントアドバイス

イベントログは、調査や法令や懲戒が関わる場合の証拠として必要となる可能性があり、不正確な監査ログは証拠の信頼性を損なう可能性があります。コンピュータ内のクロックを正しく設定し、イベントログの正確さを確実にすることが重要です。

18-2-16. 特権ユーティリティの使用

【8.18 特権的なユーティリティプログラムの使用】

実施手順（例）

a. ユーティリティプログラムの使用は、原則として OS 標準機能のみ許可する。
b. その他のユーティリティプログラムが必要となった場合は、情報システム管理者の承認を得た上で利用する。

ワンポイントアドバイス

情報システムの大半には、パッチ適用・ウイルス対策・バックアップ・ネットワークツールなど、システムやアプリケーションによる制御を無効にできる 1 つ以上のユーティリティプログラムが組み込まれています。不要なユーティリティプログラムは、すべて除去・無効化することが大切です。また、特権的ユーティリティの中には、データベースの中身を、その整合性を気にすることなく強制的に書き換えることができる機能や、他の利用者の権限でデータを操作できる機能をもったものがあります。こうした特権的なユーティリティを野放しにすると組織の情報セキュリティが保てなくなるため、厳しく利用を管理する必要があります。

18-2-17. ソフトウェア管理

【8.19 運用システムに関わるソフトウェアの導入】

実施手順（例）

a. 運用システムに、開発用のコードを導入しない。

b. PC を含む社内の情報システムで使用するソフトウェアは、原則情報システム管理者によって指定されたもののみ使用し、それ以外のソフトウェアを使用する場合は、事前に許可を得るものとする。他社が開発したソフトウェアを利用する場合、その開発会社が要求している条件やスペックを満たす環境で運用する。
c. 情報システム管理者は、利用者がインストール可能なソフトウェアを定期的に見直す。
d. 利用者は認可されていないソフトウェアをインストールしてはならず、業務上、必要な場合は、情報システム管理者の承認を得た上でインストールする。
e. ファイル共有ソフトなど、ウイルス感染や不正アクセスなどの原因となりやすいソフトウェアのインストールを禁じる。

ワンポイントアドバイス

組織は、利用者がインストールできるソフトウェアの種類について、厳密な規則を定めて施行することが大切です。

【8.25 セキュリティに配慮した開発のライフサイクル】

実施手順（例）

セキュリティに配慮した開発のための方針を以下に記す。
a. 開発の初期段階でセキュリティ要件を明確化する。
b. 開発環境は、「8.31 開発環境、試験環境及び運用環境の分離」の「b. セキュリティに配慮した開発環境」に従う。
c. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
d. 開発したシステムに脆弱性がないかテストする。
e. 開発文書（仕様書、設計書、テスト仕様など）は、必要最低限の者だけがアクセスできるようにする。
f. 受託開発または客先への派遣による開発では、クライアントから提示のあったセキュリティの方針・ルールなどに従う。

ワンポイントアドバイス

ソフトウェアやシステムのセキュリティに配慮した開発のための規則を定めることが大切です。

【8.26 アプリケーションのセキュリティの要求事項】

実施手順（例）

a. アプリケーションを取得する際、リスクアセスメントを通じてアプリケーションの情報セ

キュリティ要求事項を決定する。必要に応じて、情報セキュリティの専門家の支援を受け、情報セキュリティ要求事項を決定する。

b. セキュリティに配慮したシステムを構築するための原則は、以下の通りとする。
   - 情報セキュリティ事象を防止・検知し、対応するために必要な管理策を分析すること。
   - 情報セキュリティ要求事項を満たすための費用・時間・複雑さを考慮すること。

ワンポイントアドバイス

ネットワークを介してアクセス可能なアプリケーションは、ネットワークに関連した脅威を受けやすいため、リスクアセスメントの実施や、管理策を決定することが大切です。

【8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則】

実施手順（例）

a. 社内使用の情報システムおよび外部向けに提供する情報システムの開発に際しては、情報セキュリティ事項を明確にし、要件定義として記録する。
b. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
c. 開発したシステムに脆弱性がないかテストする。

ワンポイントアドバイス

セキュリティに配慮したシステム構築の原則および確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするため、定期的にレビューすることが大切です。

【8.28 セキュリティに配慮したコーディング】

実施手順（例）

a. ユーザーが入力したデータを確認し、問題がある場合は読み込まないようにする。
b. セキュリティ上の問題を発見しやすくするため、設計は可能な限りシンプルにする。
c. ユーザーには必要最小限の権限・機能を与える。
d. 他のシステムに送信するデータは、サニタイズ（特殊文字を一般的な文字に変換すること）を行い、不正操作を防止する。

ワンポイントアドバイス

コーディングの原則が定められていない場合、コードの書き方がそれぞれ異なってしまうことで、コードが読みづらく、脆弱性が生まれる危険性があります。セキュリティに配慮したコーディングの規則を定め、コードの書き方を統一することが大切です。

【8.29 開発及び受入れにおけるセキュリティ試験】

実施手順（例）

a. 情報システムのセキュリティテストは、運用に移行する前に行う。
b. システムの受入れ試験
   - 情報システムの導入または改修の際は、受入れ時に動作確認を行う。
   - 必要に応じて受入れテストの仕様書を作成し、確認を行う。
   - 必要に応じて、コード分析ツールや脆弱性スキャナのような自動化ツールを利用し、セキュリティに関連する欠陥を修正する。
   - 受入れ試験の結果は、受入れ部門の管理者および情報システム管理者が承認する。

ワンポイントアドバイス

効果的な試験を確実にするために、試験環境、ツール、技術の試験および監視も考慮する必要があります。

【8.30 外部委託による開発】

実施手順（例）

情報システムの開発を外部に委託する場合の手順は以下に従う。
a. 「委託先審査票」によって委託先を評価、選定、およびあらかじめ定められた頻度（最低年 1 回）で再審査し、また、契約の履行状況を監視する。
b. 委託先との契約を締結する。（契約書には情報セキュリティ要求事項を含める。）
c. 成果物の品質および正確さを評価するため、「8.29 開発及び受入れにおけるセキュリティ試験」に定める「b. システムの受入れ試験」を実施する。

ワンポイントアドバイス

外部委託したシステム開発に関する活動を随時、指導、監視およびレビューすることが大切です。

【8.31 開発環境、試験環境及び運用環境の分離】

実施手順（例）

a. 情報システムの開発に際しては、開発・テスト環境と本番環境を、物理的・論理的に分割する。
   - セキュリティに配慮した開発環境
     開発は、開発業務を行わない従業員から分離した場所およびシステムにて行う。また開発環境は、運用環境から分離する。
   - ソースコードおよび設定ファイルは、不意の消去や改ざんから保護するため、必要最

小限の者だけがアクセスできるようにする。

ワンポイントアドバイス

開発および運用環境に変更を加える際は、組織としての事前レビューおよび承認を徹底することが大切です。

【8.32 変更管理】

実施手順（例）

a. 変更管理は以下のプロセスで行う。
   1. 変更の承認
      変更を行う前にその変更の必要性、変更が及ぼす影響、変更によるリスクの変動について評価し、情報システム管理者の承認を得る。
   2. 変更のテスト
      変更を適用する前に、情報システムへの影響を確認するためにテストを行う。
   3. 変更の監査
      変更後に変更が適切に行われたか否かを監査によって確認する。

b. 情報システム管理者は、サーバに周辺機器を接続する場合や、サービスパックを適用する場合、事前に情報収集し、問題の有無を確認する。万が一、適用後に問題が生じた場合は、再インストールすることで問題解決を即座に実施する。

c. OS やパッケージソフトウェアを変更する際は、情報システム管理者はテスト機や予備機を用いて、現在の情報システムが変更後の OS 上で問題なく動作するかを検証する。

d. パッケージソフトウェアのカスタマイズを原則として禁じる。万が一、修正を行う場合は、動作上の影響およびベンダーから将来的に受けるサポートへの影響を考慮し、情報システム管理者の許可を得る。

ワンポイントアドバイス

変更管理手順は、情報の機密性、完全性、可用性を確実にするために、設計の初期段階からその後のすべての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装することが大切です。

【8.33 試験情報】

実施手順（例）

a. テストデータとして個人情報を使用することを禁じる。

b. 実データをテストデータとして使用する場合は、情報システム管理者の承認を得てから使用する。テスト終了後は、実データを直ちに削除し、情報システム管理者に対して報告す

る。

ワンポイントアドバイス

テストデータは、注意深く選定し、保護し、管理することが大切です。

【8.34 監査試験中の情報システムの保護】

実施手順（例）

a. 情報システムの監査は、システム停止のリスクを考慮し、営業時間外もしくは休日を利用して実施することを原則とする。
b. 情報システムのメンテナンスなどにより情報システムの稼動を停止する場合は、業務への影響を及ぼさない範囲または時間帯で行うように計画する。

ワンポイントアドバイス

運用システムのアセスメントを伴う監査活動およびその他の保証活動を計画し、試験者と管理層の間で合意することが大切です。

18-2-18. ネットワークセキュリティ

【8.20 ネットワークのセキュリティ】

実施手順（例）

a. ネットワーク図および装置（例：ルータ、スイッチ）の構成ファイルを含む文書を最新に維持する。
b. 社内ネットワークへ接続する際は、情報システム管理者の承認を受け、指示された手順に従う。
c. 情報システム管理者は、ネットワークにおける社外との境界にはファイアウォールを設けるなど、不正侵入対策を施す。
d. ネットワーク装置のファームウェアの定期的なアップデートを行う。
e. 他人の ID、パスワードで、社内ネットワークに接続することを禁じる。
f. 一旦、社内ネットワークから切り離したパソコンなどは、ウイルスチェックなどの安全確認を行ってから再接続する。
g. 持ち込みおよび私有 PC 利用の場合は、社内ネットワークに接続しない。やむを得ず接続する場合は、情報システム管理者が指定するソフトウェアによりウイルスチェックを行う。
h. 無線 LAN を使用する場合は、情報システム管理者の承認を得て、暗号化、接続パソコンの認証など、十分な安全対策を実施する。
i. 不特定が利用できる公衆無線 LAN や WiFi スポットに接続することは禁じる。

ワンポイントアドバイス
ネットワークや、ネットワークをサポートする情報処理施設における情報を、ネットワークを通じた危険から保護することが大切です。

【8.21 ネットワークサービスのセキュリティ】

実施手順（例）

a. 利用しているネットワークサービスを特定する。
b. 情報システム管理者は、ネットワークサービスを利用する場合は、ネットワークサービス提供者と SLA を締結する。

ワンポイントアドバイス
ネットワークサービスには、接続・プライベートネットワークサービスおよびネットワークセキュリティ管理のためのソリューション（ファイアウォール、IDS など）が含まれます。

18-2-19. ネットワークの分離

【8.22 ネットワークの分離】

実施手順（例）

a. インターネットと社内 LAN との境界にファイアウォールを設置する。
b. メール、Web サーバなどの公開サーバは、社内のネットワークと分離する。
c. ゲスト用の無線アクセスネットワークを、社内用の無線アクセスネットワークから分離する。

ワンポイントアドバイス
各領域の境界は、明確に定めることが大切です。ネットワーク領域間のアクセスが認められる場合は、境界にファイアウォールなどを設けて制御することが大切です。

18-2-20. Web フィルタリング

【8.23 ウェブ・フィルタリング】

実施手順（例）

フィルタリングソフトを利用し、業務上不必要な Web サイト、危険性のある Web サイトへアクセスすることを防ぐ。

ワンポイントアドバイス
システムがマルウェアによって危険にさらされることを防ぐために、認可されていないウェブ資源へのアクセスを防止することが大切です。

18-2-21. 暗号の使用

【8.24 暗号の使用】

実施手順（例）

a. 暗号利用のための規則

- SSL/TLS
  当組織の Web サイトの通信は、SSL/TLS を用いて暗号化する。
- 無線 LAN
  無線 LAN の通信は暗号化し、暗号化の規格は脆弱性の報告されていない安全な方法とする。

b. 鍵の管理

- SSL/TLS
  情報システム管理者は、証明書に対する秘密鍵を適切に管理する。
- 無線 LAN
  アクセスポイントの管理者画面は、情報システム管理者のみがアクセスでき、そのパスワードを厳重に管理する。

c. 重要データの暗号化

- 暗号化の対象とするデータを選定する。
- 利用する暗号の種類を決める。
- 暗号鍵のライフサイクルに関する方針を策定する。
- 暗号の管理責任者を定める。

ワンポイントアドバイス

業務や情報セキュリティ要求事項に従い、暗号に関連する法令・規制・契約上の要求事項を考慮し、情報の機密性・真正性・完全性を保護するための暗号の適切かつ効果的な使用を確実に履行することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

18-3. 実施手順を適用するセキュリティ概念

18-3-1. Security by Design

関連する主な管理策

5.1、5.7、5.9、5.19、5.20、5.24、5.26~5.29、5.37、8.9、8.15、8.16、8.22、8.25~8.34

Security by Design とは「情報セキュリティを企画、設計段階から組み込むための方策」で、開発プロセスの最初の段階からセキュリティを考慮することで、開発システムのセキュリティを確保するという考え方です。従来のように、後づけでセキュリティ機能を追加したり、システムの導入直前に脆弱性診断などを実行したりする方法の場合、手戻りが多発することがあり、結果的に開発コストが増大する可能性があります。企画・設計の段階からセキュリティ対策を行うことで、手戻りが少なくなり、コストの削減につながり、保守性のよいシステム・ソフトウェアになります。

図 60. セキュリティ対策の実施タイミング

Security by Design 導入のメリット

- 手戻りが少なくなり、納期を守れる

- コストを削減できる
- 保守性の高いソフトウェアができる

Security by Design の工程ごとに実施内容を紹介します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

実施手順（例）	選択すべき管理策（例）
セキュリティリスク分析 ● システムで取扱う重要情報のフローやライフサイクルがわかる内容を記載したシステムプロファイルの作成（ステークホルダー、実施業務、他システムとの連携方法などがわかるように作成） ● システムプロファイルに基づくセキュリティ脅威の特定 ● セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施 ● リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソースなど）	5.1 情報セキュリティのための方針群 5.9 情報及びその他の関連資産の目録
セキュリティ要件定義 ● 遵守すべきセキュリティ標準（セキュリティベースライン）やリスク分析結果などに基づく、システムとして満たすべきセキュリティ要件の定義（機能、非機能面）	8.26 アプリケーションのセキュリティの要求事項
セキュア調達 ● セキュリティ要件に基づいて、調達仕様におけるセキュリティ仕様策定 ● セキュリティ仕様に関する、委託先との責任範囲の明確化 ● 委託先に求めるセキュリティ管理基準の策定 ● セキュリティ仕様を満たす能力を有した安全な委託先の選定 ● 不正侵入の経路となるバックドアなどが含まれていない、継続的なサポートを受けられる安全なプロダクトの選定	5.19 供給者関係における情報セキュリティ 5.20 供給者との合意における情報セキュリティの取扱い
セキュリティ設計 ● セキュリティ設計の実施	8.27 セキュリティに配慮したシステムアーキテクチャ及びシ

➢ アプリケーションセキュリティ ➢ OS セキュリティ ➢ ミドルウェアセキュリティ ➢ ネットワークセキュリティ ➢ クラウドセキュリティ ➢ 物理セキュリティ ➢ セキュリティ運用（平時、有事）	ステム構築の原則
セキュリティ実装 ● 設計に基づくシステムにおけるセキュリティ機能の実装 ● セキュリティ設計に基づくアプリケーションのセキュアコーディング ● セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施（堅牢化、要塞化） ➢ OS セキュリティ ➢ ミドルウェアセキュリティ ➢ ネットワークセキュリティ ➢ クラウドセキュリティ ➢ 物理セキュリティ	8.28 セキュリティに配慮したコーディング
セキュリティテスト ● セキュリティ機能テストの実施（単体テスト、結合テスト、システムテストなど） ● 脆弱性診断の実施 ➢ Web アプリケーション脆弱性診断 ➢ プラットフォーム脆弱性診断 ➢ スマートフォンアプリケーション診断 ➢ 高度セキュリティ診断（ペネトレーションテスト、レッドチーム演習など） ● 機能テストで検出されたバグの是正対応 ● 脆弱性診断で検出された脆弱性に対する、リスクベースの是正対応	8.29 開発及び受入れにおけるセキュリティ試験 8.33 試験情報 8.34 監査試験中の情報システムの保護
セキュリティ運用準備 ● セキュリティ運用体制の確立 ● 下記項目に対応したセキュリティ運用手順の整備 平時の運用	5.24 情報セキュリティインシデント管理の計画及び準備 5.29 事業の中断・阻害時の情報セキュリティ

➢ 構成管理、変更管理 ➢ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ➢ 脅威情報収集、自システムへの影響分析 ➢ CVSS などに基づく、リスクに応じた脆弱性対応 ➢ 定期的な脆弱性診断の実施 有事の運用 ➢ インシデント対応 ● システム運用において人的ミスが発生する可能性のある箇所の洗い出し、是正 ● 有事を想定したセキュリティ運用訓練の実施	8.9 構成管理 8.32 変更管理 8.19 運用システムに関わるソフトウェアの導入
セキュリティ運用 ● セキュリティ運用を行う要員の教育/訓練の実施、重要な情報を取扱う要員のスクリーニング（要員のスキルや行動特性などを考慮） ● セキュリティ運用の実施（下記） 平時の運用 ➢ 構成管理、変更管理 ➢ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ➢ 脅威情報収集、自システムへの影響分析、是正対応 ➢ CVSS などに基づく、リスクに応じた脆弱性対応 ➢ 定期的な脆弱性診断の実施 有事の運用 ➢ インシデント対応	5.7 脅威インテリジェンス 5.26 情報セキュリティインシデントへの対応 5.29 事業の中断・阻害時の情報セキュリティ 5.37 操作手順書 8.9 構成管理 8.15 ログ取得 8.16 監視活動 8.32 変更管理

Security by Design 実施における留意事項

- 工程間でセキュリティ対策の不整合が起きないように注意すること
- 組織として考慮すべきリスクや組織能力を踏まえて実現可能なレベルで実施し、PDCA サイクルを回しながら成熟度を高めていくこと

詳細理解のため参考となる文献（参考文献）	
セキュリティ・バイ・デザイン導入指南書	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/security-by-design.html
DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

18-3-2. ゼロトラスト、境界防御モデル

関連する主な管理策

5.9、5.15~5.23、5.29~5.30、8.1~8.3、8.15~8.16、8.21、8.32

ゼロトラストの定義

ゼロトラスト（ZT）は、従来の境界線によるセキュリティ対策とは異なり、ネットワーク内のすべてのデバイスやユーザーを信頼せず、あらゆるアクセスをゼロから検証するという考え方です。これにより、内部からの脅威や、一度内部に侵入された場合の被害を最小限に抑えることを目指します。具体的には、多要素認証、最小権限の原則、継続的な監視など、複数のセキュリティ対策を組み合わせることで、アクセス制御を強化します。

境界防御モデルとゼロトラストの違い

境界防御モデルは、信用する領域（社内）と信用しない領域（社外）に境界を設け、組織が守るべき情報資産は信用する境界内部に存在するという前提をもとに、境界線でセキュリティ対策を講じることで、境界外部からの脅威を防ぐという考え方です。

一方、ゼロトラストは、「境界」の概念をなくし、守るべき情報資産にアクセスするものはすべて確認し、認証・認可を行うことで脅威を防ぐという考え方です。

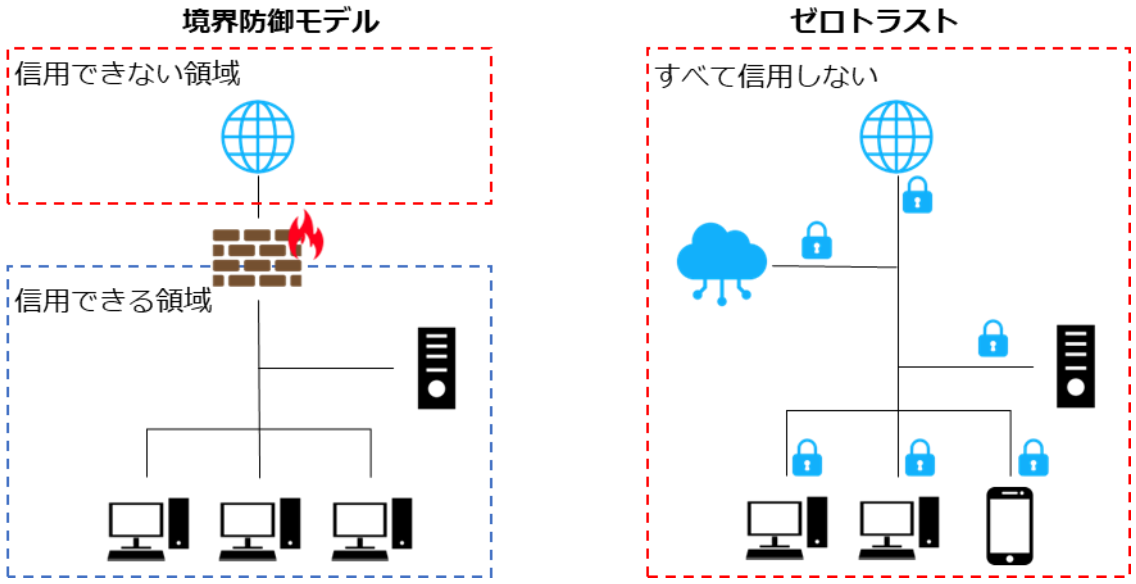


図 61. 境界防御モデルとゼロトラストの概要図

現在、クラウドサービスの普及やモバイル端末の活用、テレワークによる働き方の多様化により、内部と外部を隔てる「境界」そのものが曖昧になりつつあります。その結果、従来の社内・社外の境界でセキュリティ対策を行う「境界防御モデル」では、サイバー攻撃やマルウェア感染などの脅威から情報資産を守ることが難しくなってきています。こうした問題を解決するものとして、「ゼロトラスト」という考え方が注目されています。

One Point

ゼロトラストと境界防御の関係

ゼロトラストは、境界防御モデルで守ることが困難な脅威に対して適用する対策ではあるもの

の、「境界防御モデルを排除する考え」ではありません。強固なセキュリティを構築するにあたり、すでに用いられている境界防御モデルを活かすことが大切です。

ゼロトラスト導入に向けた進め方

準備工程

ゼロトラストを導入する準備として、資産（デバイスやネットワークなど）、主体（ユーザー・権限など）、ビジネスプロセスについて詳細に理解する必要があります。ゼロトラストを導入する準備として、資産、主体、データフロー、ワークフローの調査を行います。

ゼロトラスト導入プロセス

準備工程を実施した以降は、次のプロセスで進めます。

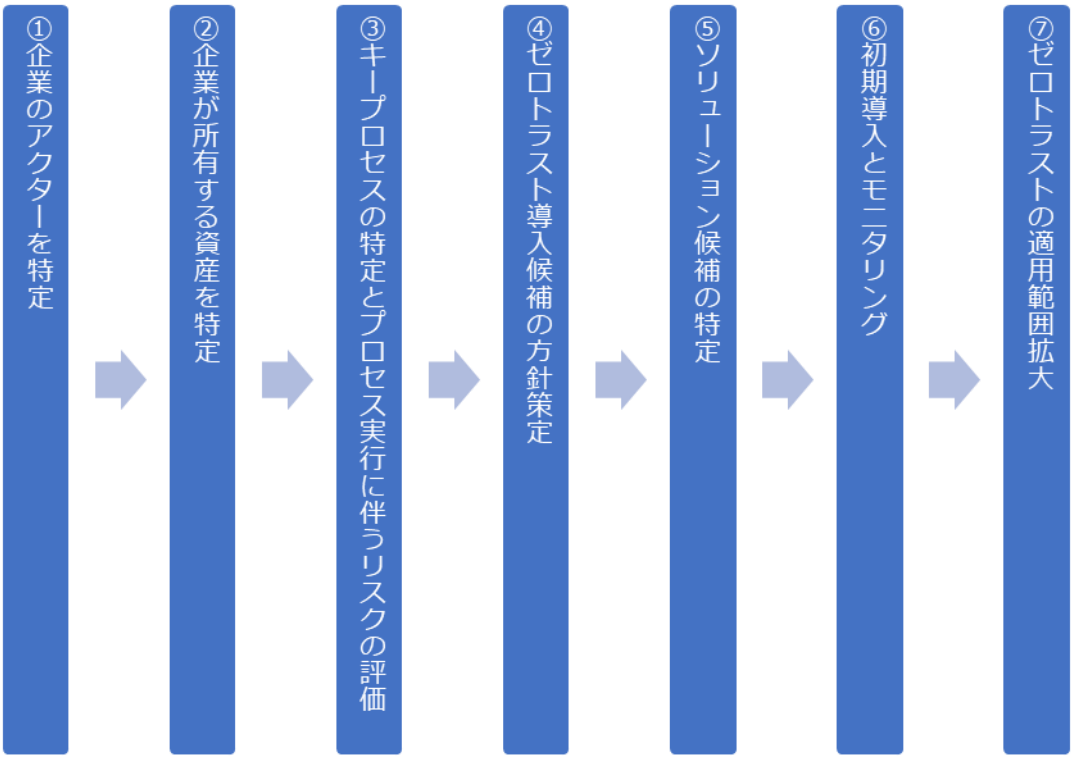


図 62. ゼロトラスト導入プロセス

（出典）IPA「ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～ 」をもとに作成

詳細理解のため参考となる文献（参考文献）	
ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

ゼロトラスト導入の各プロセスで実施すべき内容を説明します。

1.企業のアクターを特定

企業の主体には、ユーザーに紐づいたアカウントと、サービスに紐づいたアカウントの両方が含まれることがあります。どのユーザーにどのレベルの権限を与えるのかは精査が必要です。基本的には、必要な対象に必要な権限だけ与えるという最小権限の考え方で整理します。

2.企業が所有する資産を特定

ゼロトラスト・アーキテクチャ（ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシーなどを含むサイバーセキュリティ計画のこと）は、デバイスを識別して管理する機能が必要であり、企業内のデバイスはもちろん、企業所有ではないデバイスについても識別し、監視する機能が必要です。よって、企業の情報にアクセスするデバイスについては、「シャドーIT」も含めて可能な限り資産化する必要があります。なお、企業によって可視化されているもの（例：MAC アドレス、IP アドレス）と、管理者のデータ入力による追加分も含まれます。

3.キープロセスの特定とプロセス実行に伴うリスクの評価

業務プロセス、データフロー、および組織のミッションにおけるそれらの関係（プロセス）を特定します。次に信用度レベルをつけ、ゼロトラストへ移行するプロセスを決めます。認証・認可の判断を導入することによる失敗のリスクを考慮し、初めはビジネスインパクトの低いビジネスプロセスから開始するとよいでしょう。ある程度、認証・認可の挙動を掴んでから対象を広げていくことで、リスクを抑えることができます。

4.ゼロトラスト導入候補の方針策定

資産またはワークフローを特定したら、影響を受ける対象をすべて特定します。（上流リソース（例：ID 管理システム）、下流リソース（例：セキュリティ監視）、エンティティ（例：主体ユーザー）。次に企業管理者は、候補となるビジネスプロセスで使用されるリソースの信用度レベルの重みを決定します。それらを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定します。

5.ソリューション候補を特定

④で策定した内容をもとに、導入箇所に適するソリューション、製品を検討します。製品、ソリューションについては後述します。

6.初期導入とモニタリング

初期導入時には、適用したポリシーや初期動作の確認を含め、監視モードで運用することが推奨されます。初期導入後はしばらくシステムの動作を監視し、必要に応じて、システムの安全性を保ちつつ、業務効率を最大化するために調整を行います。

7.ゼロトラストの適用箇所拡大

運用フェーズに入ったら、ネットワークや資産の監視は継続し、トラフィックの記録を行います。これらを実施していく中で、ポリシーの変更や適用箇所の拡大を適宜実施していきます。ポリシー変更などを実施する場合は、深刻な問題にならないように行います。

ゼロトラスト導入に向けた実施手順（例）

「ゼロトラスト導入に向けた進め方」で説明したプロセスをもとに、ゼロトラストを導入するための実施手順を、例を用いて説明します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

実施手順（例）	選択すべき管理策（例）
準備工程 新たに導入する必要のあるプロセスやシステムを判断することおよびアクセスの認証・認可を正しく行うため、現在の運用状況を把握する。 a. 情報システム管理者は、次の事項を調査し、詳細に理解する。 ● 資産（デバイスやネットワークなど） ● 主体（ユーザー・権限など） b. 経営者は、次の事項を調査し、詳細に理解する。 ● ビジネスプロセス	5.9 情報及びその他の関連資産の目録 5.16 識別情報の管理 5.18 アクセス権 8.2 特権的アクセス権
① 企業のアクターを特定 a. 情報システム管理者は、業務に必要な者のみ情報へアクセスできる権限を与える。 b. アクセス権限および操作権限は、認められた場合以外は与えないようにする。	5.15 アクセス制御 5.16 識別情報の管理 5.17 認証情報 5.18 アクセス権 8.2 特権的アクセス権 8.3 情報へのアクセス制限
② 企業が所有する資産を特定 a. デバイスを識別して管理する。 企業の情報にアクセスするデバイスは、シャドーIT を含めて、すべて識別して管理する。 b. シャドーIT は可能な限り資産化する。	5.9 情報及びその他の関連資産の目録 8.1 利用者終端装置

③ キープロセスの特定とプロセス実行に伴うリスクの評価 a. 業務プロセス、データフロー、組織のミッションにおける業務プロセスとデータフローの関係（プロセス）を特定する。 b. 特定したプロセスのうち、ゼロトラストに移行するプロセスを決定する。 認証・認可の判断を導入することによる失敗のリスクを考慮し、初めは組織の事業に与える影響が低いビジネスプロセスを選択し、徐々に対象を広げる。	5.29 事業の中断・阻害時の情報セキュリティ 5.30 事業継続のための ICT の備え
④ ゼロトラスト導入候補の方針策定 a. 資産、プロセスの特定後、ゼロトラストの導入により影響を受ける対象をすべて特定する。 ● 上流リソース（例：ID 管理システム） ● 下流リソース（例：セキュリティ監視） ● エンティティ（例：主体ユーザー） b. ゼロトラスト導入候補となるビジネスプロセスで使用されるリソースの重要さを決定する。 c. リソースの重要さを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定する。	5.9 情報及びその他の関連資産の目録
⑤ ソリューション候補を特定 ④で策定した内容をもとに、導入箇所に適するソリューションを検討する。	5.19 供給者関係における情報セキュリティ 5.20 供給者との合意における情報セキュリティの取扱い 5.21 ICT サプライチェーンにおける情報セキュリティの管理 5.22 供給者のサービス提供の監視、レビュー及び変更管理 5.23 クラウドサービスの利用における情報セキュリティ 8.21 ネットワークサービス

	のセキュリティ
⑥ 初期導入とモニタリング a. ソリューションの初期導入時は、実際に通信の遮断は行わず、適用したポリシーや初期動作の確認を行う。 b. 動作に問題がないことを確認後、運用を開始する。	8.16 監視活動
⑦ ゼロトラストの適用箇所拡大 a. 運用開始後は、ネットワークや資産の監視は継続しつつ、トラフィックの記録を行う。 b. トラフィックを記録していく中で、ポリシーの変更や適用箇所の拡大を適宜実施する。 c. ポリシー変更を実施する場合は、影響が問題にならないように確認する。	8.15 ログ取得 8.16 監視活動 8.32 変更管理

ゼロトラストを実装するための主な技術要素

ゼロトラストを実装するために必要となる主な技術要素（製品、ソリューション）について説明します。

CASB（Cloud Access Security Broker）

CASB とは、クラウドサービスの利活用における情報セキュリティのコンセプトですが、それを実装した製品も CASB と呼ばれます。CASB は、以下の 4 機能を備えています。

- 可視化
  - クラウドストレージへの不審なアップロードやダウンロードの監視や、シャドーIT の検知を行います。
- データセキュリティ
  - アクセス権限の逸脱や機密情報の持ち出しをチェックし、ブロックします。
- コンプライアンス
  - セキュリティに関する基準やポリシーを満たしていることを監査します。
- 脅威防御
- セキュリティ脅威の検出、分析や防御を行います。

SWG（Secure Web Gateway）

SWG は、外部ネットワークに対するすべてのアクセスを中継することで、危険なコンテンツをブロック・フィルタリングするセキュリティ製品です。物理的なアプライアンスとして提供

されるものもありますが、クラウド型のソリューションが一般的です。利用者によるリスクの高い行為や許可されていない操作をブロックして、エンドポイントデバイスと社内ネットワークの安全性を保ちます。SWG の主な機能は、次の通りです。

- リスクの高い URL や IP アドレスへのアクセスの遮断
- マルウェアの検出とブロック
- アプリケーション制御

ZTNA（Zero Trust Network Access）

ZTNA は、ユーザー認証によって、特定のサービスやアプリケーションへの安全なアクセスを提供する仕組みです。VPN と異なり、ネットワーク全体へのアクセスを許可するのではなく、特定のサービスやアプリケーションのみの利用を許可します（ユーザーが許可されていないサービスなどは表示されず、利用もできません）。必要最小限の権限を付与することで、セキュリティを向上することができます。

FWaaS（Firewall as a Service）

FWaaS とは、ファイアウォールやその他ネットワークセキュリティの機能をクラウドサービスで提供するソリューションです。URL フィルタリングや IPS、アプリケーション制御の機能を持ち、セキュリティを高めます。FWaaS は、オンプレミス型のファイアウォールよりもネットワークの変更に柔軟に対応できます。

SDP（Software Defined Perimeter）

SDP の機能はほぼ ZTNA と同じで、ユーザーに特定のサービスやアプリケーションへの安全なリモートアクセスを提供します。SDP は、ネットワークの内部と外部の境界（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更することにより安全にデータを転送する技術のことです。従来のファイアウォールの概念をソフトウェア上に持ち、利用者がどこにいても動的にアクセスを制御します。

18-3-3. SASE

SASE（Secure Access Service Edge）とは、「ネットワーク機能」と「セキュリティ機能」をまとめて提供する仕組みです。「ネットワーク機能」と、接続の安全性を確保する「セキュリティ機能」をまとめて 1 つの製品として提供します。

SASE に含まれる主な機能に以下のものがあります。

ネットワーク機能

- SD-WAN（Software Defined - Wide Area Network）

※SD-WAN については、「18-3-4. ネットワーク制御（Network as a Service）」で説明します。

セキュリティ機能

- SWG（Secure Web Gateway）
- CASB（Cloud Access Security Broker）
- FWaaS（Firewall as a Service）
- ZTNA（Zero Trust Network Access）

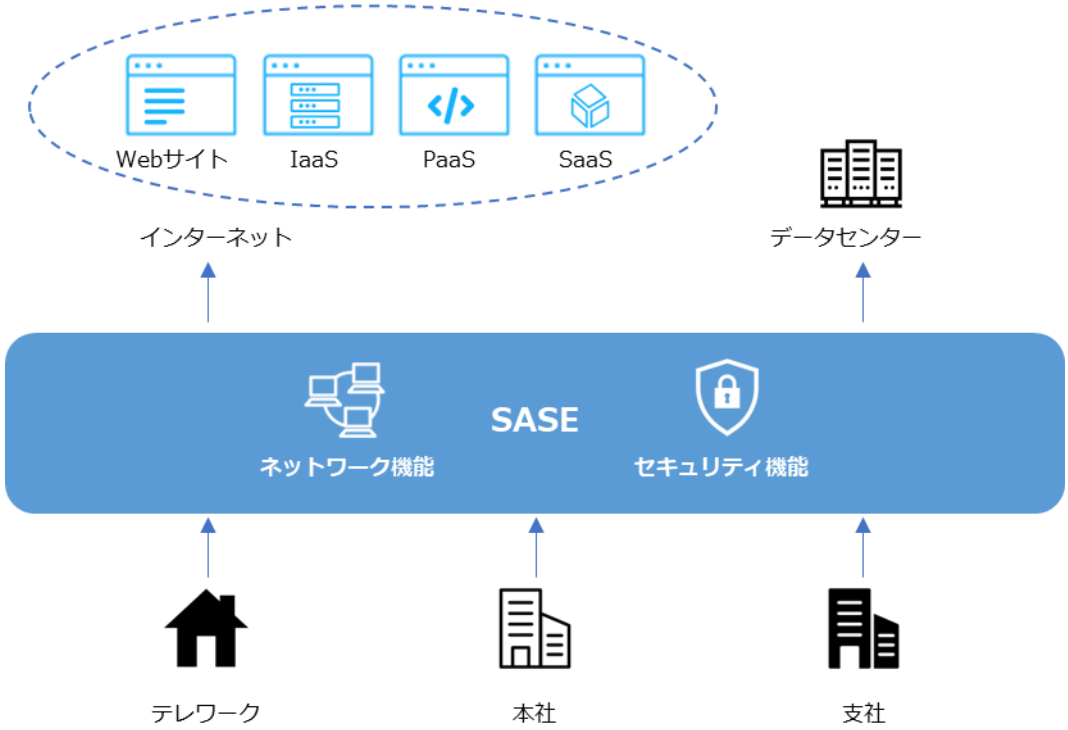


図 63. SASE のイメージ図

ゼロトラスト導入事例

概要
地方銀行は、個人顧客向けサービス以外にも、法人顧客向けサービスの充実を図っています。法人向け営業力強化方策の 1 つとして、営業職員にモバイル端末を配布し、場所を問わずに行内システムにアクセスを可能にすることになりました。そこで、高いセキュリティが求められる金融機関のリモートアクセス環境として、ゼロトラストネットワークアクセス機能を備えた「ZTNA」を導入しました。結果、安全で安定したリモートアクセスが可能となり、業務効率化と営業力強化を実現しました。

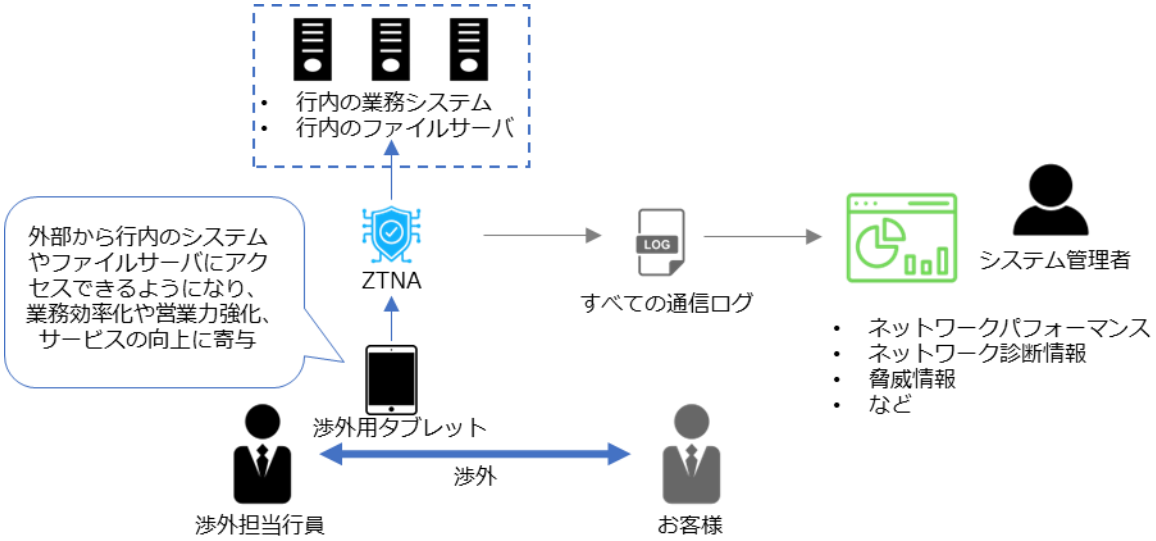


図 64. 事例のイメージ図

導入前の課題

営業力強化に向けてモバイル端末の必要性が高まり、次の課題があげられました。

- 行内だけの運用だったモバイル端末活用を、いつでもどこでも働ける環境に拡大すること。
- 渉外用タブレットは、外から行内システムやファイルサーバにアクセスできる必要があること。
- 外部でモバイル端末を利用するためには、セキュリティや性能の担保が必要であること。

選定の決め手

次の事項が導入の決め手となりました。

- リモートアクセスとセキュリティのゼロトラスト機能が一体になっていること。
- 動作検証でリモートアクセス時の速度・安定性が高いこと。

導入後の効果

導入後の効果は次の通りです。

- 営業職員が行内に戻らず業務を遂行できるようになり、業務が効率化したこと。
- 許容した内容や業務だけの通信に限定できるので、安心して使用できること。
- 今後は渉外用タブレットを活用した業務改革の推進が見込まれること。

詳細理解のため参考となる文献（参考文献）	
（参考資料 1）民間企業におけるゼロトラスト導入事例	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf

18-3-4. ネットワーク制御（Network as a Service）

関連する主な管理策
5.23、6.7、8.20~8.24

ネットワーク制御を説明するにあたって、クラウドサービスについて説明します。

クラウドサービスとは、サービス事業者がハードウェアの機能（サーバ、ハードディスクなど）、プラットフォームの機能（データベースやプログラム実行環境など）、ソフトウェアなどを、ネットワーク経由で利用者に提供するサービスのことです。利用者は、どの端末からでもさまざまなサービスを利用することができます。クラウドサービスの利用形態には、主に「IaaS＝アイアース」、「PaaS＝パース」、「SaaS＝サーズ」があります。また、「NaaS＝ナース」と呼ばれるネットワークインフラを提供するサービスもあります。

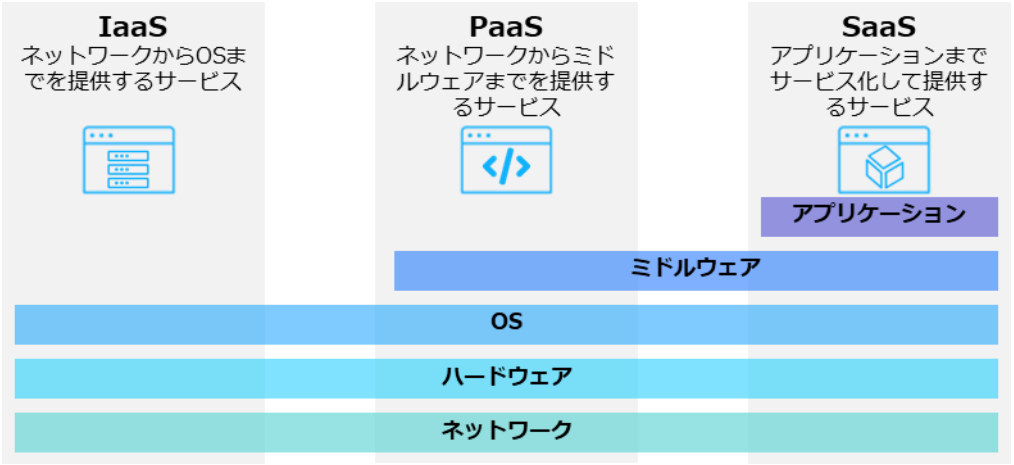


図 65. クラウドサービス利用形態の概要図

IaaS（Infrastructure as a Service）

IaaS とは、インターネット経由でネットワークやサーバ（CPU・メモリ・ストレージ）などのハードウェアやインフラ機能を提供するサービスのことです。IaaS を利用することで、従来は自社で購入、構築し、運用する必要があったハードウェアやインフラの機能を、必要なときに必要なだけ利用できます。

PaaS（Platform as a Service）

PaaS とは、インターネット経由でアプリケーションサーバやデータベースなどのアプリケーションを実行するためのプラットフォーム機能を提供するサービスのことです。PaaS を利用することで、アプリケーションの開発前段階で必要な開発環境の準備（サーバの設置や OS やミドルウェアのインストールと設定、ネットワークの設定など）を省略できます。

SaaS（Software as a Service）

SaaS とは、インターネット経由で電子メール、顧客管理、財務会計などのアプリケーションソフトの機能を提供するサービスのことです。アカウントを持っていれば、インターネット経由でどこからでもアクセスすることができたり、チームでファイルやデータを共有できたりします。

NaaS（Network as a Service）

NaaS とは、インターネット経由でネットワークインフラを提供するサービスのことです。NaaS の導入により、ネットワーク環境の変更に柔軟に対応できるようになります。NaaS に含まれる主要な機能として、SDN、SD-WAN などがあります。

SDN・SD-WAN

クラウドサービスや Web 会議、リモートワークの普及に伴い、ネットワーク回線にアクセスが集中し、通信速度が低下したり、サービスへの接続ができなくなったりするなどの問題があります。その解決策として SDN を応用した SD-WAN があります。SDN、SD-WAN について説明します。

SDN（Software Defined Networking）

SDN とは、ソフトウェアを用いてネットワーク構成を動的に変更することです。ネットワークを構成している機器（ルータやサーバ、スイッチなど）を、ソフトウェアを介して一括制御することで、機器設定やネットワーク構成を柔軟に変更できます。SDN のメリットは、ネットワーク機器に対して一括で設定を行えることです。従来のルータ、スイッチといった物理的なネットワーク機器・製品は、1 台ごとに個別に設定を行う必要があり、大規模なネットワーク構成を変更する際には、大きな作業負荷がかかりました。しかし、SDN を用いてネットワークを制御することで、管理が 1 か所で行えるようになるため、ネットワーク機器・製品ごとに個別設定が不要になり、作業負荷が大幅に軽減できます。

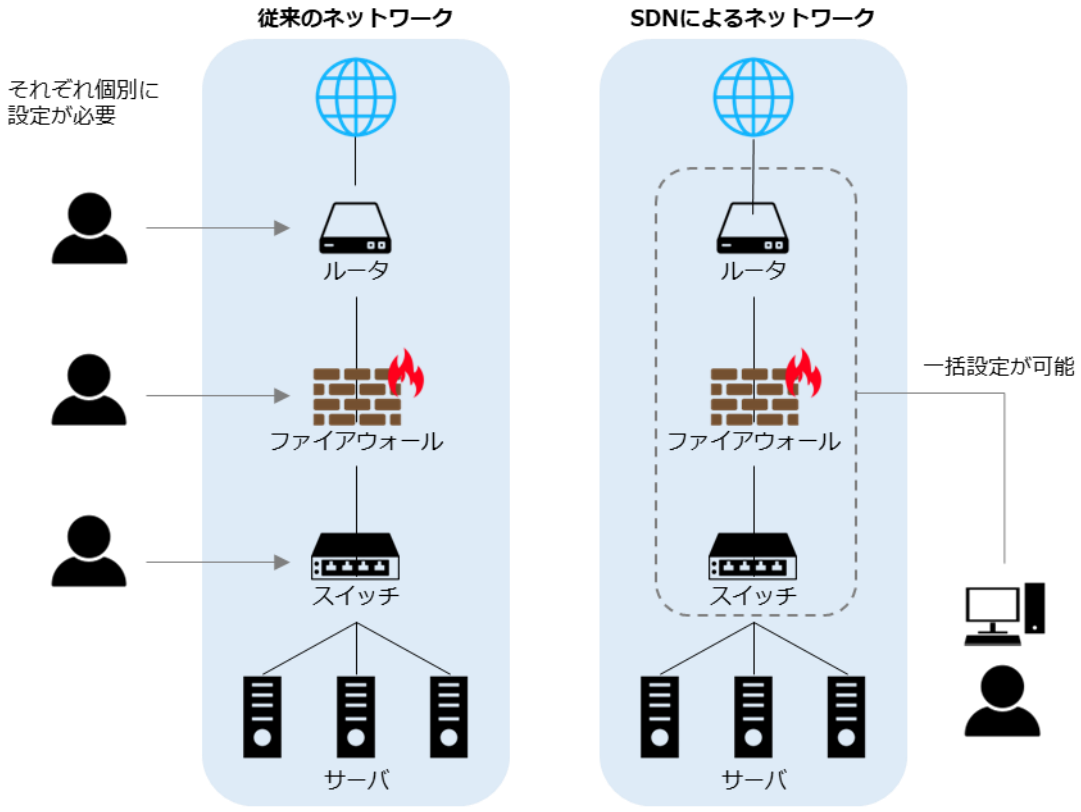


図 66. 従来のネットワークと SDN によるネットワークの比較

SD-WAN（Software Defined-Wide Area Network）

SD-WAN とは、ネットワークをソフトウェアで制御する SDN を、物理的なネットワーク機器で構築した WAN に適用する技術のことです。企業の拠点間接続や、クラウド接続などにおいて柔軟なネットワーク構成を実現したり、ネットワーク上で発生する通信を適切に制御したりすることができます。

例えば、拠点間の通信には閉域網（不特定多数のユーザーが利用するインターネットとは異なり、関係者のみが接続できる通信回線）を使用し、信頼できるクラウドサービスには直接外部インターネットへ接続するように切り替えることで、トラフィックの最適化が行えます。

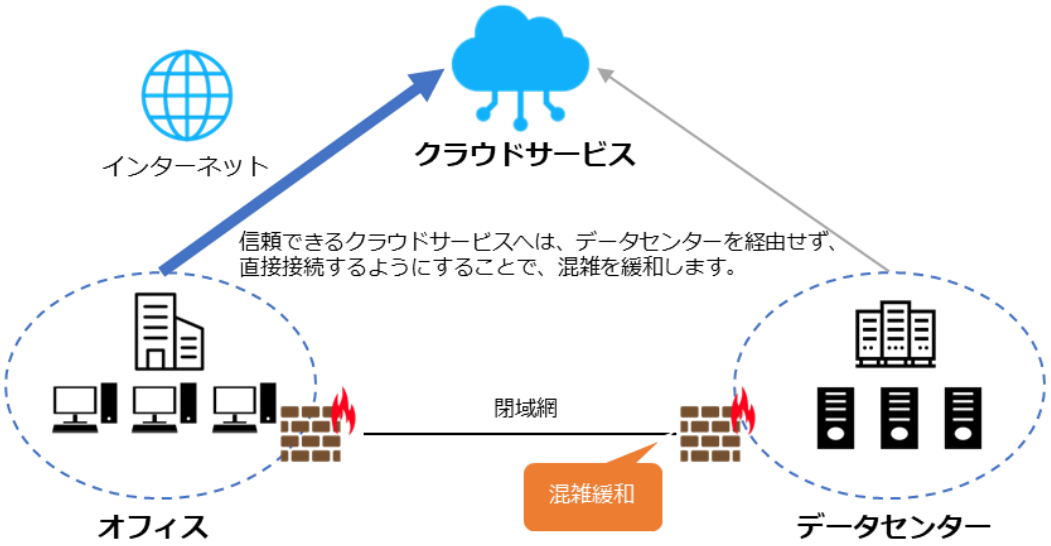


図 67. SD-WAN で実現できることの例

VPN

個人情報などの重要なデータをインターネット経由で扱う機会が増えたことや、サイバー攻撃の手口が年々巧妙化しているなどの状況を背景に、VPN が注目されています。

VPN（Virtual Private Network）

インターネット上で安全性の高い通信を実現するための手法です。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぎます。VPN を使用することで、ユーザーは物理的な専用線で通信しているかのような安全な通信を行えます。

図 68. VPN の概要図

18-3-5. セキュリティ統制（Security as a Service）

関連する主な管理策

5.1、5.9、5.15～5.18、5.23～5.28、8.1～8.5

セキュリティ統制とは、組織が情報資産を守るために採用するセキュリティ対策や仕組みになります。機密性、完全性、可用性などの情報セキュリティの目標を達成するために監視、記録を行い

統制します。

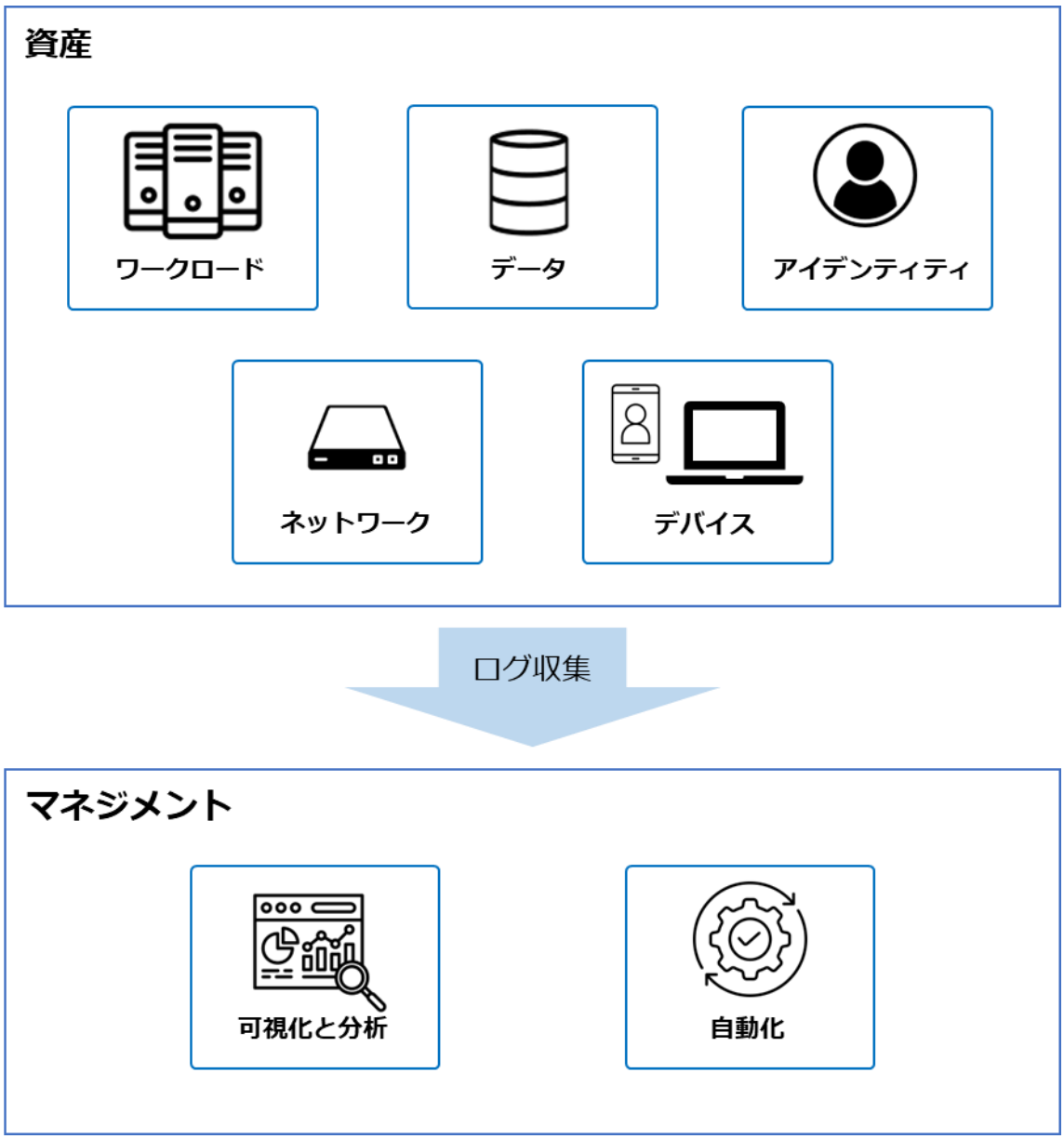


図 69. セキュリティ統制の概要図

以下は、セキュリティ統制を確立するための実施例となります。

実施内容（例）	選択すべき管理策（例）
リスク評価と分析 ● 組織内の情報資産やプロセスを評価し、セキュリティリスクを特定 ● リスクの重要度や影響を評価し、優先順位づけ	5.9 情報及びその他の関連資産の目録
ポリシーの策定 ● セキュリティポリシーを作成し、組織内での適用範囲や	5.1 情報セキュリティのための方針群

要件を定義 ● ポリシーは法規制や業界のガイドラインに準拠	
技術的対策の実施 ● 資産に対してセキュリティ対策の実施 ➢ ワークロード ➢ データ ➢ アイデンティティ ➢ ネットワーク ➢ デバイスなど	5.15 アクセス制御 5.16 識別情報の管理 5.17 認証情報 5.18 アクセス権 5.23 クラウドサービスの利用における情報セキュリティ
監視と評価 ● セキュリティ対策の効果を監視し、定期的な評価の実施 ● セキュリティインシデントが発生した場合は、原因を分析し、対策の改善	5.25 情報セキュリティ事象の評価及び決定 5.27 情報セキュリティインシデントからの学習 5.28 証拠の収集 8.15 ログ取得 8.16 監視活動
変更管理 ● システムやポリシーに変更があった場合、セキュリティに影響を与えないように変更管理プロセスを確立	8.32 変更管理
対応計画の策定 ● セキュリティインシデントが発生した場合の対応計画を策定し、迅速かつ効果的に対処	5.24 情報セキュリティインシデント管理の計画及び準備 5.26 情報セキュリティインシデントへの対応

SECaaS（Security as a Service）

SECaaS はセキュリティをサービスとして提供します。組織がセキュリティに関する機能をクラウドベースのサービスプロバイダから提供される形態で利用します。従来では、オンプレミスで利用していたセキュリティ機能をクラウド上に移行し、サブスクリプションで利用することが可能になります。

SECaaS のメリット

- コスト最適化
- スケーラビリティ
- 変化への柔軟な対応

- 冗長性
- 高い可用性
- 障害耐性

セキュリティ統制を確立するために実施することができる技術を紹介します。

ネットワークセキュリティ	
SWG（Secure Web Gateway）	Web アクセスを中継するプロキシの一種で、危険なサイトやコンテンツへのアクセスを遮断するセキュリティ機能をクラウドサービスとして実施。
SDP（Software Defined Perimeter）	アクセス制御をソフトウェアで制御し、認証とアクセス制御を接続ごとに行うことで、動的なマイクロセグメンテーションおよびセキュアなリモートアクセスを実現。
デバイスセキュリティ	
EDR（Endpoint Detection and Response）	パソコンやサーバ、スマートフォンなどのエンドポイントデバイスに侵入したマルウェアやランサムウェアなどを検出し、通知するシステム。マルウェア感染後の被害拡大防止に有効。
EPP（Endpoint Protection Platform）	パソコンやサーバ、スマートフォンなどのエンドポイントデバイスへのマルウェアの侵入を防御するソリューション。未知のマルウェアの検知・駆除にも対応。
アイデンティティセキュリティ	
IAM（Identity and Access Management）	情報システムのユーザーID を管理・認証・認可。
FIDO（Fast Identity Online）	ID/パスワード方式に代わる認証技術。指紋や虹彩といった生体情報、公開鍵暗号、端末 ID、ワンタイムパスワードなどを利用した認証方法がある。
ワークロードセキュリティ	
CWPP（Cloud Workload Protection Platform）	クラウド上コンテナ（実行環境）や仮想マシンなどに導入し、クラウドワークロード（クラウド上で実行されるプログラムやアプリケーション）の監視と保護を行うソリューション。

データセキュリティ	
DLP （Data Loss Prevention）	情報漏えい防止を目的とするセキュリティツール。従来のシステムと異なり、データそのものを監視して情報漏えいを防ぐため、高い効果が期待できる。
可視化と分析	
CASB （Cloud Access Security Broker）	クラウドサービスの脆弱性対策ソリューション。クラウドサービスの利用状況を可視化すると同時にクラウド環境への不正アクセス検知と防御も可能。
SIEM （Security Information and Event Management）	ファイアウォールや IDS/IPS などから出力されるログやデータを一元的に集約し、集約したデータを組み合わせて相関分析を行うことにより、サイバー攻撃やマルウェア感染などのセキュリティインシデントをリアルタイムで検知。
CSPM （Cloud Security Posture Management）	クラウド環境の設定状況を可視化し、あらかじめ設定したルールに基づいて、不適切な設定や脆弱性の有無を検知。
自動化	
SOAR （Security Orchestration Automation and Response）	セキュリティインシデントの監視、データの収集・分析、対応などのセキュリティ運用業務を自動化・効率化する技術。

FIDO（Fast Identity Online）

FIDO は、従来のパスワードによる認証方式に代わる、パスワードを使わない「パスワードレス認証」を実現する技術です。認証には、公開鍵暗号方式を利用したデジタル署名の仕組みが用いられます。

デジタル署名による送信者確認の仕組み

デジタル署名では公開鍵と秘密鍵、2 つの鍵を使用します。公開鍵は公開される誰でも取得できる鍵で、秘密鍵は本人だけが保持している鍵です。秘密鍵で署名したデータは、対となる公開鍵で検証できます。この仕組みを利用し、受信者は送られてきたデータが間違いなく送信者本人から送

図 70. デジタル署名による送信者確認の仕組み

られてきたか確認できます。

FIDO2

FIDO2 とは、パスワードレス認証の技術仕様です。FIDO2 では、端末で生体認証行い、利用者を認証します。サーバとは、デジタル署名による本人確認の仕組みを用いて認証します。サーバ側には公開鍵、端末側には秘密鍵が保管され、鍵同士がペアとなります。正式サイトを偽装したフィッシングサイトがログインを求めても、ペアとなる鍵がないためログインを防げます。FIDO2 を利用したパスキーという仕組みでは、認証資格情報を複数の端末で同期できるため、機種変更や端末紛失などの場合に、一からの作成する必要はありません。

メリット

- 認証に必要な秘密情報（秘密鍵）は、認証を行う端末側のみに保存され、利用する際は指紋認証や顔認証などによって本人確認を行うため、パスワードを覚える必要がありません。
- パスワードや認証に必要な機密情報がインターネットに流れず、サーバ側で保存されないため、漏えいのリスクが低減されます。

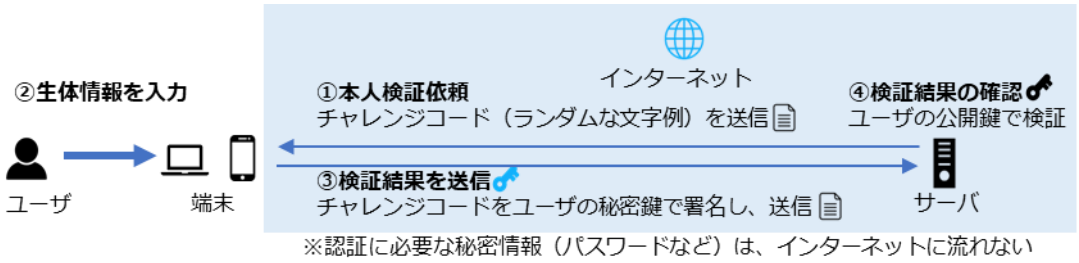


図 71. FIDO2 の仕組み

① 本人検証依頼

サーバは、ユーザーの端末に向けてチャレンジコード（ランダムな文字列）を送信します。

② 生体情報を入力

ユーザーは生体情報を入力し、端末はユーザーを認証します。

③ 検証結果を送信

ユーザーの認証に成功したら、端末はチャレンジコードをユーザーの秘密鍵で署名し、サーバへ送信します。

④検証結果の確認

サーバは、署名されたチャレンジコードを受け取ったら、ユーザーの公開鍵で検証します。検証に成功するとユーザーのログインを受入れ、認証完了となります。

18-4. インシデント対応

関連する主な管理策
5.5、5.6、5.24~5.28、6.8

インシデント発生時の対応

セキュリティインシデントが発生した際の基本的な対応の流れは、「第５章．事例を知る：重大なインシデント発生から課題解決まで」で説明した「1．検知・初動対応」、「2．報告・公表」、「3．復旧・再発防止」です。インシデント対応の実施手順について、ウイルス感染が起きた際の例を用いて説明します。

実施手順（例）	
①検知・初動対応	検知と連絡受付： ● パソコンの動作異常やウイルス対策ソフトの警告が表示された場合、ウイルス感染の可能性があるため、情報セキュリティ責任者に報告する。 ● ウイルスが添付されたメールを受け取った外部から通知を受けて発覚した場合も、情報セキュリティ責任者に報告する。 ● 内部から外部への不正な通信、外部からの意図しない通信や、一時的な大量の通信、ウイルスに関係する特定サイトへのアクセスなどは、ウイルス感染を疑う。 初動対応： ● 感染したパソコンやサーバの利用を停止し、ネットワークから切り離す。
②報告・公表	第二報以降・最終報： ● 影響を及ぼした取引先や顧客に対して、セキュリティインシデントに関する報告を行う。 ● ウイルス感染による影響によって、業法などで報告が求められる場合は所管の省庁へ報告する。 ● ウイルス感染やランサムウェア感染の場合は、IPA の届出窓口へ届け出る。
③復旧・再発防止	調査・対応： ● 他のパソコンやサーバがウイルスに感染していないか、ウイルス対策ソフトの定義ファイルを最新にしてからチェックする。 ● ウイルス対策ソフトに従ってウイルスを駆除する。 ● ウイルス駆除ができない場合、OS のクリーンインストールを実施し、すべてのプログラムを入れ直す。 復旧：

	● ウイルスの駆除が確認できたら、対象のパソコンやサーバをネットワークに接続し、復旧する。

インシデント対応の実施手順について、ウイルス感染が起きた際の例
（出典）IPA「中小企業のためのセキュリティインシデント対応の手引き」をもとに作成

詳細理解のため参考となる文献（参考文献）	
中小企業のためのセキュリティインシデント対応の手引き	https://www.meti.go.jp/policy/netsecurity/sme_incident.html

フォレンジック

インシデント対応の「復旧・再発防止」のステップでは、訴訟対応などを見越して事実関係を裏づける情報や証拠を保全し、必要に応じてフォレンジックを行います。

フォレンジックとは

フォレンジックとは、セキュリティインシデントが起きた際に、コンピュータやネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を調査・解析する技術・手法・手続きを指します。

フォレンジックを行う際の注意点

フォレンジックを行う必要がある際は、専門の調査会社に依頼する選択肢も考慮することが大切です。なぜなら、フォレンジックには専門知識が必要であり、自社で対応しようとすると、証拠となるデータの収集・保全が困難になる可能性があるためです。例えば、データのコピーが客観的証拠として認められない可能性や、誤操作によるデータの破損などがあります。事前に相談する専門の調査会社を決めておくことが大切です。

セキュリティインシデント発生直後の対応についての実施手順策定

フォレンジックに関して、「証拠保全ガイドライン」が参考になります。想定読者として、「フォレンジックに関する専門知識を習得しているとは限らないが、専門事業者または捜査機関に引き継ぐために証拠保全手続きを行う可能性のある担当者」が含まれています。

セキュリティインシデント発生直後の初動対応についての実施手順を、例を用いて説明します。セキュリティインシデントが検知された、または発生していたことが明らかになった直後は、証拠保全を適切かつ円滑に実施するため、次の事項を実施することが大切です。

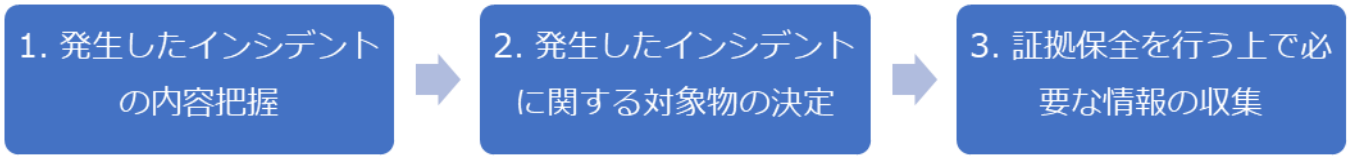


図 72. インシデント発生直後の対応の流れ

詳細理解のため参考となる文献（参考文献）	
証拠保全ガイドライン第 10 版	https://digitalforensic.jp/home/act/products/df-guideline-10th/

実施手順（例）

1. 発生したインシデントの内容把握

発生したインシデントを把握します。

インシデントの種類

- 情報流出・データ破壊
- 不正アクセス、不正プログラムの実行
- 操作・設定ミスなど

検知・発覚のきっかけ

- ログのレビュー・監視
- 内部通報
- 不正検知システムなど

発生時刻

- システム時計の正確性について確認

初動対処の開始までの記録

発生したインシデントの検知・発覚から、報告または対処依頼連絡までの時間およびその間のインシデントに対する対処の有無について記録をとります。

- 発生したインシデントを知る人物および人数
- インシデント対象物の確保の有無

インシデントの対象物を確保していた場合

対象物を確保した日時、人物（役職）、場所、確保時の対象物（および周辺）に対する行為、確保後の対象物に対する対処（の有無）とその内容を記録します。

インシデントの対象物を確保していない場合
対象物を確保する（予定の）日時と場所、確保時の対象物（およびその周辺）の状態を詳細に記録します。

2. 発生したインシデントに関する対象物の決定

対象物に対する情報収集および対象物の絞り込み

- 発生したインシデントに関する対象物の種類および個数を確認します。
  - コンピュータ（タブレット型、ノート型、デスクトップ型、サーバ型）
  - ネットワーク機器（ルータ、ファイアウォール、IDS、IPS）
  - HDD、SSD など
- 発生したインシデントに関する対象物の状態（いつどこに存在していたかなど）を確認します。
- 発生したインシデントに関する対象物の使い始めと終わり、および使用頻度を確認します。
- 発生したインシデントに関する対象物の使用者、および管理者を確認します。
- 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器、および文書の有無を確認します。

対象物の選定と優先順位づけ

- 保全を行う前の対象物（デバイス）を選定し、その理由を明確にします。
- （対象物が複数ある場合）取扱う対象物の優先順位をつけ、その理由を明確にします。

3. 証拠保全を行う上で必要な情報の収集

対象物の情報

- 対象物の形状、個数、物理的な状態を確認します。
  - 対象物のラベル情報（メーカー、型番、モデル名、記憶容量など）
  - ケーブルの接続状況
  - 通常環境下で視認可能な物理的破損、損傷の有無など
- HDD、SSD、ストレージメディアの記憶容量、インタフェースの状況を確認します。
- セキュリティ設定の有無を確認します。
  - HDD、SSD のパスワードロック
  - HDD、SSD 全体暗号化または一部のファイル・フォルダの暗号化
  - PC 周辺のワイヤストッパー、ロッカーなど

第19章. セキュリティ対策状況の有効性評価

章の目的
第 19 章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組として、監査について理解することを目的とします。

主な達成目標
◘　内部監査および外部監査の重要性について理解すること

19-1. 内部監査

内部監査とは、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実施されているかをチェックすることです。セキュリティのルールを整備して日が浅いうちは、関係者がルールを理解し、遵守しながら仕事ができているかを重視して判断します。運用に慣れてきたら、設けられた社内のルールや使っている文書の内容が適切か、その有効性を判断していきます。内部監査の視点を適合性から有効性へと移していくことで、**ルールが形骸化し、目的が見失われている状態になることを防げる**でしょう。

内部監査の進め方は、「13-2-7. ISMS：9. パフォーマンス評価」を参照してください。

19-2. 外部監査

外部監査とは、組織に所属しない外部の監査人が行う監査を指します。セキュリティの外部監査では、企業が保有する情報資産を守るための体制や環境が整っているかを第三者がチェックすることになります。情報漏えいやサイバー攻撃などのリスクに対して、外部監査を受けることはセキュリティ対策として有効な手段の 1 つです。近年では取引先企業を乗っ取り、そこを踏み台にしてメインターゲットとなる企業にサイバー攻撃を仕掛ける「サプライチェーン攻撃」が頻繁に起こっており、中小企業が大企業に対する攻撃の踏み台として狙われる可能性が高まっています。

情報セキュリティ監査を受ければ、**自社のセキュリティ対策が正しく行われているか否か確認でき、不十分な点を洗い出して迅速に対処することが可能になります。**顧客や取引先に、セキュリティ対策を適切に行っていることがアピールできるので、会社や事業の規模も考慮しつつ、監査を受けることは重要です。経済産業省は、情報セキュリティの管理・監査について、2 つの基準を発表しています。

管理基準・監査基準

情報セキュリティ管理基準
組織における情報セキュリティマネジメントの円滑で効果的な確立を目指し、マネジメントサイクルの構築から具体的な管理策まで、包括的な適用範囲を定めたものです。この管理基準は「マネジメント基準」と「管理策基準」の 2 項目から構成されています。 **マネジメント基準** 情報セキュリティマネジメントの計画・実行・点検・処置に必要な実施すべき事項が提示されています。 **管理策基準** リスク対応方針に従って管理策を選択する際の選択肢が提示されています。
情報セキュリティ監査基準
情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範です。監査の品質を一定の水準に保ち、有効かつ効率的に実施できるように「一般基準」「実施基準」「報告基準」の 3 項目を提示しています。 **一般基準** 監査人としての適格性および監査業務上の遵守事項を定めています。 **実施基準** 監査計画の立案および監査手続きの適用方法を中心に、監査実施上の枠組みを定めています。

報告基準

監査報告にかかる留意事項と、監査報告書の記載方式を定めています。

情報セキュリティ管理基準は、JIS Q 27001 をもとに策定されています。そのため、Lv.3 網羅的アプローチを実施することで、外部監査に対応することも可能となります。

詳細理解のため参考となる文献（参考文献）	
経済産業省「情報セキュリティ監査制度」	https://www.meti.go.jp/policy/netsecurity/is-kansa/
情報セキュリティ監査基準 Ver1.0（平成 15 年経済産業省告示第 114 号）	https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf
情報セキュリティ管理基準（平成 28 年経済産業省告示第 37 号）	https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

コラム

実施手順の文書化に関するポイント

実施手順を文書化する際のポイントをいくつか紹介します。

- 明確な手順と責任の割り当て
  実施手順を文書化する際、手順が、誰が、いつ、どのように実施するのかを明確にすることが重要です。実施手順が適切に実施されるようにするためには、文書の各手順に関連する責任者を明記することが有効です。
- フローチャートや図の活用
  文字に加えて、フローチャートや図などを用いて手順を視覚的に示すことにより、手順の流れや関係性を理解しやすくできます。また、複雑なプロセスをわかりやすく表現できるため、実施者が迷わずに手順を進められるようになります。
- 定期的なレビューと更新
  実施手順は、絶えず変化する環境に適応させる必要があります。新たな脅威や法規制などへ対応させていくために、定期的なレビューや更新を行い、実施手順が常に効果的なものである状態を維持していくことが大切です。

実施手順の文書化は、組織がセキュリティ対策を行っていく上で必要です。実施手順を組織全体に浸透させ、形骸化させず有効な状態を維持するためには、責任者を明記したり、視覚的な表現を組み合わせてわかりやすい手順を記載したり、定期的にレビューしたりすることが大切です。

編集後記

第 7 編では、 ISMS の管理策を参考に、対策基準・実施手順を策定する手順について解説しました。紹介した 対策基準・実施手順の例は、そのまま組織に適用できるものではないため、紹介した例と ISO/IEC 27002 の内容を参考に、自社にあった対策基準・実施手順を策定していただければと思います。文書化・更新は重要ですが、本来の目標は文書化ではなく、効果的なセキュリティ対策の計画と実行にあることを忘れないようにしてください。

第 8 編では、 具体的な構築・運用の実践について説明します。

引用文献

ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド

https://isms-society.stores.jp/items/632a57a42e7452256400d84b

ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u000002klo-att/000092243.pdf

参考文献

ISO/IEC 27001:2022

https://www.iso.org/standard/27001

ISO/IEC 27002:2022

https://www.iso.org/standard/75652.html

サイバーセキュリティ関連の法律・ガイドライン

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/legal/

セキュリティ・バイ・デザイン導入指南書

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/security-by-design.html

DS-200政府情報システムにおけるセキュリティ・バイ・デザインガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u000002klo-att/000092243.pdf

（参考資料1）民間企業におけるゼロトラスト導入事例

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf

中小企業のためのセキュリティインシデント対応の手引き

https://www.meti.go.jp/policy/netsecurity/sme_incident.html

証拠保全ガイドライン第10版

https://digitalforensic.jp/home/act/products/df-guideline-10th/

経済産業省「情報セキュリティ監査制度」

https://www.meti.go.jp/policy/netsecurity/is-kansa/

情報セキュリティ監査基準 Ver1.0（平成15年経済産業省告示第114号）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Audit_Annex04.pdf

情報セキュリティ管理基準（平成28年経済産業省告示第37号）

https://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard_H28.pdf

■CVSS

Common Vulnerability Scoring Systemの略。情報システムの脆弱性に対するオープンで汎用的な評価手法のこと。ベンダーに依存しない共通の評価方法を提供している。CVSSを用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる。ベンダー、セキュリティ専門家、管理者、ユーザーなどの間で、脆弱性に関して共通の言葉で議論できるようになる。

18-3-1

■EDR

Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する。

17-3-1、18-3-5

■ICT

Information and Communication Technology の略。IT（情報技術）に加えて、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる。

15-1、15-2-6、15-2-7
18-3-2

■IDS

Intrusion Detection Systemの略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPSと異なり、不正アクセスや異常な通信をブロックする機能はない。

18-2-10、18-2-14、18-2-18、18-3-5、18-4

■IPS

Intrusion Prevention Systemの略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPSは、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する。

18-2-10、18-2-14、18-3-2、18-3-5、18-4

■IP アドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IPアドレスは、127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら4つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている。

18-3-2

■ISAC

Information Sharing and Analysis Centerの略。業界内での情報共有・連携を図る組織のこと。国内では、金融や交通、電力、ICTなどの分野にISACがある。ICT-ISACでは、ICT分野の情報セキュリティに関する情報（インシデント情報を含

む。）の収集・調査・分析を行っている。
15-2-2

■ISMS
Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取り組み。組織が ISMS を構築するための要求事項をまとめた国際規格が ISO/IEC 27001（国内規格は JIS Q 27001）であり、審査機関の審査に合格すると「ISMS 認証」を取得できる。
14-1-1、14-1-3、15-1、16-1、17-1、17-2-1、18-1、19-1

■ISP
個人や企業などに対してインターネットに接続するためのサービスを提供する事業者のこと。ユーザーはISPと契約し、回線を用いてISPが運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる。
15-2-7

■JPCERT/CC
日本におけるセキュリティインシデントなどの報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている組織。政府機関や企業などから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる。
15-2-1、15-2-2

■JVN
Japan Vulnerability Notes の略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと。
15-2-2

■MAC アドレス
Media Access Control address の略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される。
18-3-2

■NIST サイバーセキュリティフレームワーク（CSF）
米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている。日本においても、今後普及が見込まれる。
14-1-2

■NTP
Network Time Protocolの略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている。
18-2-15

■PII
Personally Identifiable Informationの略。「個人を特定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と 1 対 1 に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号に

加えて、使命、生年月日、住所、勤務先などの情報もPIIに含まれる。

15-1、15-2-8

■SASE（サシー）

Secure Access Service Edgeの略。令和元年に提唱されたゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念。

18-3-3

■SDP

Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザーの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う。

18-3-2、18-3-5

■SLA

Service Level Agreementの略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの。

18-2-18

■SSL/TLS

WebサーバとWebブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去にはSSLが使われていたが、脆弱性が発見されたため、TLS（v.1.2以降）への移行が進んでおり、今ではSSLは使われなくなってきている。しかし、歴史的経緯でSSLの用語が広く普及しているため、本テキストでは「SSL/TLS」と表記す。

15-2-1、18-2-21

■SWG

Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することによりセキュアな通信環境を実現。

18-3-2、18-3-3、18-3-5

■VPN

Virtual Private Networkの略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぐ。VPNを使用することで、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる。

15-2-1、16-2-6、17-3-1、18-3-2、18-3-4

■WAN

Wide Area Networkの略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にあるLAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートなWANを構築

する場合には、通信事業者に依頼する必要がある。

18-3-4

■アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと。

15-1、15-2-1、15-2-3、18-1、18-3-2、18-3-5

■アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することにより、システムの再構築や運用改善の参考情報となる。

18-1

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること。

15-2-1、15-2-7、17-2-5、17-2-6、18-2-1、18-2-10、18-2-18、18-2-21、18-3-4、18-4

■イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと。

18-2-15

■エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと

18-3-2

■エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（パソコン、プリンタ、スキャナ、スマートフォン、仮想マシン、サーバ、IoT デバイスなど）

18-1、18-3-2、18-3-5

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT 分野においては、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為。

15-1、15-2-5、15-2-7、15-2-8、18-2-11、18-2-13、18-2-17、18-3-4

■可用性

許可された者だけが必要な時にいつでも情報や情報資産にアクセスできる特性。

15-1、15-2-6、15-2-7、17-1、18-1、18-2-12、18-2-17、18-3-5

■完全性

参照する情報が改ざんされていなく、正確である特性。

14-1-2、15-1、17-1、18-2-17、18-2-21、18-3-5

■機密性

許可された者だけが情報や情報資産にアクセスできる特性。

14-1-2、15-1、17-1、18-2-17、18-2-21、18-3-5

■脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている。

15-1、15-1、15-2-2、18-3-1

■供給者

組織に対して、製品・サー

ビスを供給する企業または個人のこと。製品の場合、PCやサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある。

14-1-2、15-1、15-2-1、15-2-6、15-2-7、15-2-9、18-3-1、18-3-2

■クリーンインストール

すでにインストールされているOSを削除した上で、新しくOSを再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある。

18-4

■コーディング

プログラミング言語でソースコードを書くこと。

18-1、18-2-17、18-3-1

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行っている。

15-2-1、15-2-2

■サイバー攻撃

インターネットを通じて、別の企業や組織、国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマホから、企業のサーバやデータベース、国の重要インフラまでさまざまである。ネット社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。

18-3-2、18-3-4、18-3-5、19-2

■サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調を挙げている。

15-2-1、17-1、17-2-6

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる。

18-2-9

■シャドーIT

従業員が業務に使用するIT機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの。

17-3-1、18-3-2

■情報資産

企業や組織などが所有している情報全般のこと。情報資産には顧客情報や販売情報などの情報自体に加え、ファイルや

データベースといったデータ、CD-ROMやUSBメモリなどの記録メディア、紙媒体の資料も含まれる。

15-2-6、17-2-1、18-3-2、18-3-5、19-2

■情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。

情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される。

14-1-2、15-1、15-2-1、15-2-5、16-1、16-2-7、18-2-17、18-3-5

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある。

18-2-21

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性。

15-2-7、18-2-15

■スクリーンセーバ

離席時にPCの画面の内容を盗み見されることを防ぐ機能のこと。PCに対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする。

18-2-1

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない。

17-2-4

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと。

14-1-2、15-2-1、18-1、18-2-7、18-2-17、18-2-21、18-3-1、18-3-5

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること。

18-3-1

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当。

14-1-2、15-1、15-2-1、15-2-4、15-2-5、18-1、18-2-13、18-3-1、18-3-5、18-4

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準など

を具体的に記載することが一般的。

18-3-5

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方。

18 章、18-3-2、18-3-3

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1から作る必要がなくなり、効率的に開発を行うことができる。

18-1

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」。

15-2-2、18-2-18、18-3-2、18-3-5

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年ではFIDO2と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている。

15-2-7、18-2-4、18-3-2

■データマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする

18-1、18-2-10

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと。

18-3-2、18-3-4

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する。

15-2-1、15-2-9、19-1

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行

する必要がある。

15-2-6

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハード ウェアを指す。パソコンの OSに付随しているもの、セキュリティソフトウェアに付いているもの、専用のハードウェアになっているものなど形態はさまざまである。

15-2-1、15-2-2、18-2-10、18-2-14、18-2-18、18-2-19、18-3-2、18-3-5、18-4

■ファイル共有ソフト

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある。

17-3-1、18-2-10、18-2-17

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる。

18-4

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている。

15-2-1、15-2-5、15-2-7、17-3-1、18-2-4、18-2-10、18-2-11、18-2-13、18-2-17、18-3-5、18-4

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ。

19-2

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報

システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの。

14-1-2

■プロキシ

クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Webサーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる。

18-3-5

■ペネトレーションテスト

ネットワークに接続されたシステムの安全性を検証するテスト手法。すでに知られているサイバー攻撃手法を使って実際にシステムに侵入や攻撃を試みることで攻撃耐性を確認する。

18-3-1

■マルウェア

パソコンやスマホなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる。

15-2-2、15-2-4、16-2-6、17-3-1、18-1、18-2-6、18-2-20、18-3-2、18-3-5

■ミドルウェア

OSとアプリケーションの中間に位置するソフトウェアのこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる。

18-3-1、18-3-4

■無線 LAN

LANはLocal Area Networkの略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線LANを通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる。

15-2-1、17-2-4、18-2-18、18-2-21

■無停電電源装置

UPSとも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる。

15-2-1、17-2-6

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある。

18-1、18-2-16

■ランサムウェア

悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する。

15-2-1、18-2-11、18-3-5
18-4

■リスクアセスメント

組織に存在するリスクを認識し、リスクの大きさの評価を行い、そのリスクが許容できるかどうかを決定するプロセスを指す。リスク対応を行うときの優先度の根拠となるリスクレベルを決定する活動である。

14-1-3、15-1、15-2-2、16-1、17-1、18-1、18-2-17

■リスク評価

組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス。

18-3-5

東京都産業労働局