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13章. ISMS の要求事項と構築（Lv.3 網羅的アプローチ）

章の目的
第 13 章では、情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する Lv.3 網羅的アプローチについて理解することを目的とします。
主な達成目標
◘ Lv.3 網羅的アプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

13-1. 【Lv.3 網羅的アプローチ】の概要

Lv.3 網羅的アプローチでは、フレームワークとして ISMS を用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。第 13 章では、ISMS における PDCA サイクルを回すために重要となる文書化の方法や、実施すべき事項について焦点を当てて説明していきます。

ISMS の要求事項に関連する文書化は重要ですが、あくまで手段であり目的ではありません。文書化と維持が目的化してしまうと、文書が形骸化し、情報セキュリティ対策としての意味がほとんどなくなってしまう場合があります。文書を精細に作り込むことより、ISMS マネジメントプロセスを取り入れ、PDCA サイクルを回していくことが大切です。ISMS に取り組み始めたときには理解できていても、文書作りを始めると文書化が目的になってしまうケースが多いため、注意が必要です。本来、ISMS の認証取得のために作成する文書は、実施すべきことを記述したものではなく、実際に実施していることを記述したものであるべきなのです。

Lv.3 網羅的アプローチ（網羅性のあるアプローチ方法）

概要	メリット	デメリット
網羅的なフレームワークとして ISMS を参考にします。ISMS のフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。	ISMS 要求事項の導入が可能です。	時間とコストがかかる。

13-2. 【Lv.3 網羅的アプローチ】フレームワークを参考とした実施手順

13-2-1. ISMS の概要（確立・運用・監視）

ISO/IEC 27001 各要求事項の概要

「1. 適用範囲」に記述されていますが、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの 7 項目となっています。

ISO/IEC 27001:2022 の構成	
1. 適用範囲 ISO/IEC 27001 は ISMS 運用のための要求事項を規定しており、本規格に適合するためには 4～10 に規定されるすべての事項に対応しなければならない。	**6. 計画** ISMS の計画を立てる際の要求事項。（PDCA サイクルの P「Plan」）
2. 引用規格 ISO/IEC 27001 は、ISO/IEC 27000（ISMS の概要と用語）を引用する。	**7. 支援** 構成員の教育など、ISMS 構築にあたり組織が構成員に行うべきサポートを要求している。
3. 用語および定義 ISO/IEC 27001 で用いる用語および定義は、ISO/IEC 27000 に定めている。	**8. 運用** ISMS を実行する際の要求事項。（PDCA サイクルの D「Do」）
4. 組織の状況 組織の内情や取り巻く状況、利害関係者のニーズを把握した上で ISMS の適用範囲を決定することを要求している。	**9. パフォーマンス評価** 適切な ISMS が構築・運用できているか評価する際の要求事項。（PDCA サイクルの C「Check」）
5. リーダーシップ トップマネジメントが主導して ISMS を構築することを要求している。（トップマネジメントが実施するべきことのまとめ）	**10. 改善** ISMS の是正処置やリスク、改善の機会、ISMS 認証の不適格があった場合の対処法。（PDCA サイクルの「Act」）

ISMS の確立、運用、監視

「第 11 章. セキュリティフレームワーク」でも記載した通り、ISMS は PDCA サイクルに則って運用することになります。Plan で ISMS を確立し、Do で導入および運用、Check で監視および見直し、Act で維持および改善を行います。ISMS の取組により、組織の情報セキュリティをより良くするために管理手段レベルでの解決を目指すことになります。同じ失敗を繰り返さない、あるいは現状を改善し続けるために、PDCA サイクルによって継続的な改善を図ることが重要です。

本テキストでは、Lv.3 網羅的アプローチとして必要な文書や項目を抜粋し、詳細に説明していきます。なお、ISMS の要求事項を定めている ISO/IEC 27001 の 1 から 3 はそれぞれ「1.適用範囲」「2.引用規格」「3.用語および定義」なので、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの 7 項目となっています。

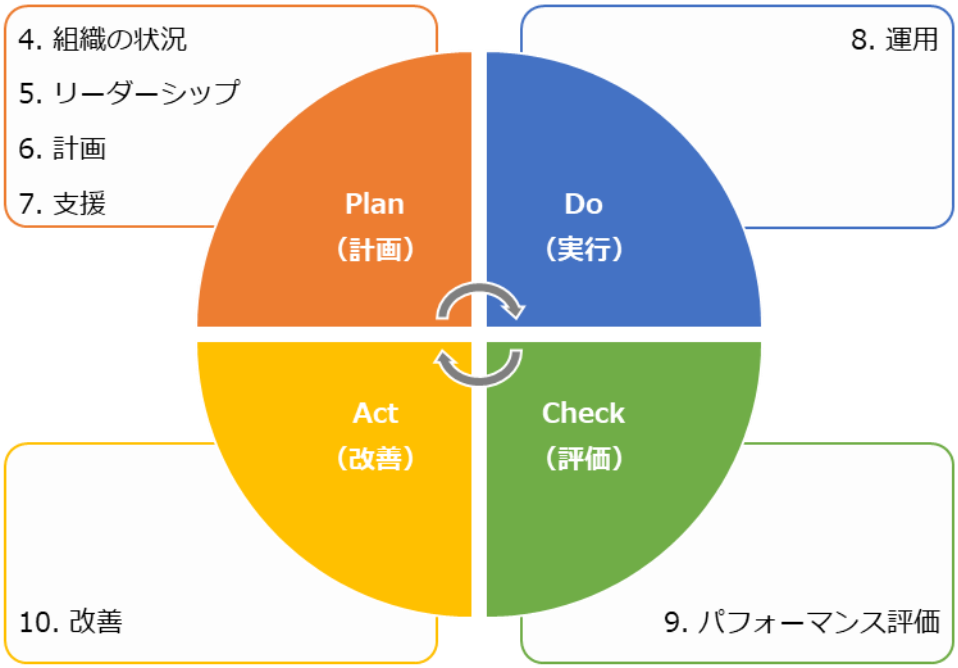


図 51. ISO/IEC 27001 の PDCA サイクル

13-2-2. ISMS：4. 組織の状況

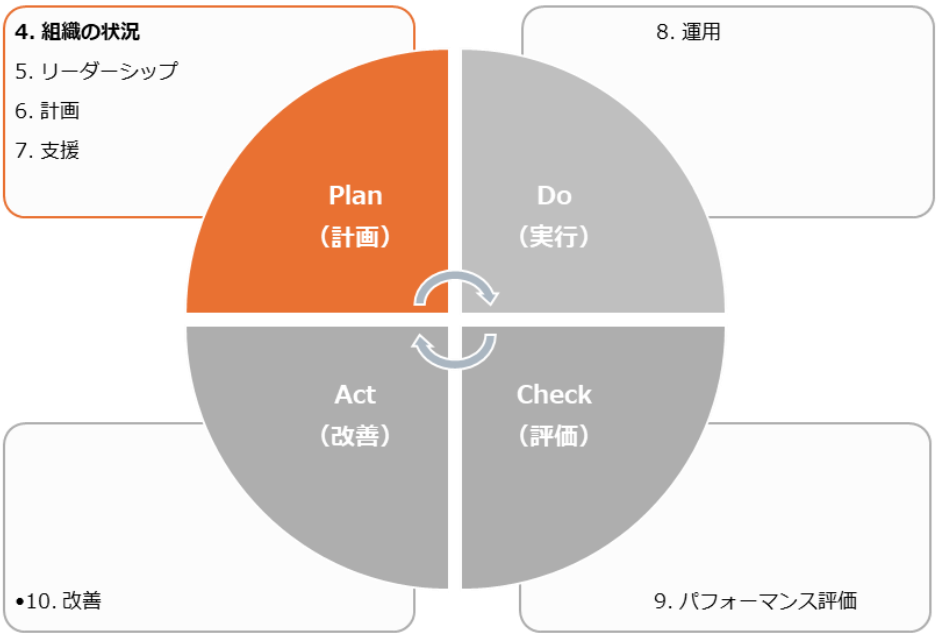
ISMS 構築の第一歩は、組織の状況を把握することにあります。組織が抱えている情報セキュリティ上の課題を明らかにするとともに、組織の利害関係者が情報セキュリティに関してどのようなニーズや期待を持っているのかを整理し、情報セキュリティに取り組む意義を確認します。それを踏まえて、「ISMS の適用範囲」を決定することになります。この「4.組織の状況」は、PDCA サイクルの「Plan（計画）」に位置していますが、組織内外の状況に応じて見直す必要があります。

4. 組織の状況	作成文書（例）
4.1 組織及びその状況の理解 ISMS を構築することにより解決したい課題（組織の目的に関連する内部課題、外部課題）を明確にします。	● 外部及び内部の課題
4.2 利害関係者のニーズ及び期待の理解 ISMS に関係する利害関係者（顧客、従業員、取引先など個人や組織）と、利害関係者から要求される情報セキュリティに関係する要求事項を明確にします。	● 利害関係者のニーズ及び期待

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 決定された外部課題・内部課題、利害関係者の要求事項と、業務内容や他の組織との情報のやり取り、ネットワーク構成などを考慮し、ISMS の適用範囲を合理的に決定します。	● ISMS 適用範囲 ● レイアウト図 ● ネットワーク図
4.4 情報セキュリティマネジメントシステム 決定した ISMS の適用範囲を対象に、PDCA サイクルに基づく ISMS を構築・運用します。	―

4.1 組織及びその状況の理解

作成する文書	● 外部および内部の課題



「組織及びその状況の理解」では、組織を取り巻く外部と内部の課題を整理することが求められています。ここで整理した課題を、ISMS の取組を通して解決していきます。また、組織のどの部分に対して ISMS を適用すべきなのかといった適用範囲を確定する際にも、課題を考慮することになります。なお、2025 年 5 月に「情報セキュリティ，サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項（追補 1）JIS Q 27001：2025（ISO/IEC 27001：2022＋Amd 1：2024）（JSA）」が発行されました。これにより組織は、気候変動が自社の課題となるかを決定する必要があります。

外部の課題

組織の外部に原因が存在する課題は、以下の情報をヒントに決定することができます。

- 国際、国内、地方または近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然および競争の環境
- 組織の目的に影響を与える主要な原動力および傾向
- 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の認知および価値観
- 気候変動

（例）

課題	リスク	機会
個人情報、機密情報の保護（ウイルス感染、情報漏えい、新たな脅威への対応）	情報セキュリティ事故の発生 →信用低下	情報の活用
外部委託先の被災	情報システム/サービスの停止	情報の活用

内部の課題

組織の内部に原因が存在する課題は、以下の情報をヒントに決定することができます。

- 統治、組織体制、役割およびアカウンタビリティ
- 方針、目的およびこれらを達成するために策定された戦略
- 資源および知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システムおよび技術）
- 情報システム、情報の流れおよび意思決定プロセス（公式および非公式の双方を含む。）
- 内部ステークホルダーとの関係並びに内部ステークホルダーの認知および価値観
- 組織文化
- 組織が採択した規格、指針およびモデル
- 契約関係の形態および範囲
- 気候変動による自然災害等の多発に伴う社員の出社困難

（例）

課題	リスク	機会
ISMS に関する理解の促進	理解不足による情報セキュリティ事故	体制強化
情報（紙、電子データ）の適切な取扱い	紛失、訪問先などに忘れ →信頼喪失	信頼向上
ノウハウ、お客様より預かる機密情報などの保護	機密情報の漏えい、ノウハウの流出	ビジネス機会の拡大
非常時の人員体制	出社人員不足による業務の一時停止	信頼向上

4.2 利害関係者のニーズ及び期待の理解

作成する文書	● 利害関係者のニーズ及び期待

「利害関係者のニーズ及び期待の理解」では、組織の利害関係者と、その利害関係者が要求する情報セキュリティに関する要求事項を明確化することが求められます。利害関係者には、顧客や従業員、取引先など、さまざまな個人や組織が含まれます。利害関係者に該当する範囲は広いため、組織が管理できる範囲で利害関係者からの要求事項を特定します。また、どの程度のセキュリティレベルで対策するのか、利害関係者とそのニーズから水準を設定することになります。また、「情報セキュリティ,サイバーセキュリティ及びプライバシー保護－情報セキュリティマネジメントシステム－要求事項（追補 1）JIS Q 27001：2025（ISO/IEC 27001：2022＋Amd 1：2024）（JSA）」により利害関係者から、気候変動に関連する課題についても対応を求められる可能性があります。

利害関係者のニーズ及び期待の記入例

利害関係者	情報セキュリティに関する要求事項	リスク	機会
取引先	適切な情報の取扱い	不適切な取扱いによる信頼低下 →案件減少	適切な対応による信頼向上 →受注の維持/増加
	法令順守	未順守による信頼低下 →案件減少	順守による信頼向上 →受注の維持/増加
株主	セキュリティインシデントの未然防止	セキュリティインシデントの発生 →ブランドイメージの低下	セキュリティインシデントの発生数減少 →ブランドイメージの向上
従業者	情報セキュリティに関する教育	機密情報/ノウハウの流出	組織の価値向上
	必要な情報へのアクセス	機密情報/ノウハウの流出	効果的・効率的な業務 →競争力アップ
	個人情報の保護	不適切な情報の取扱い →信頼低下	従業者から信頼向上 →人材の確保
国・自治体	法令・その他規範の順守	セキュリティインシデント発生時の不適切な対応 →社会的信頼の低下	社会的信頼の向上
全ての利害関係者	気候変動（自然災害）対応	非常時の対応不整備 →取引停止や従業者の退職等	適切な対応による信頼向上

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

作成する文書	● ISMS 適用範囲

	● レイアウト図 ● ネットワーク図

ISMS の適用範囲は、必ずしも会社全体とする必要はありません。特に大企業の場合には、特定の業務や特定の部門に限定して ISMS を構築することがあります。例えば、ある取引先の要請によって ISMS を構築する場合、その取引先と取引のある部門に適用範囲を限定するケースがあります。

中小企業の場合には、会社全体を適用範囲とすることが多いので、特段の理由がない限り、会社全体を適用範囲にするとよいでしょう。

「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」では、ISMS を適用するところと、そうではないところの境界およびその適用される範囲内で、規格の要求事項がどのように適用できるかを決定するよう要求しています。規格などの要求事項によって定められる改善すべき範囲を、適用範囲といいます。

適用範囲の決定に際しては、考慮しないといけない 3 つの事項があります。2 つはこれまでに説明した「外部および内部の課題」と「要求事項」です。もう 1 つは、「組織が実施する活動と、他の組織が実施する活動との間のインターフェースおよび依存関係」です。異なる部署や委託先など他の組織との業務プロセスにおける依存度を見ながら、適用範囲を広げるのか、分離しておくのかを検討することになります。

インターフェースおよび依存関係の記入例

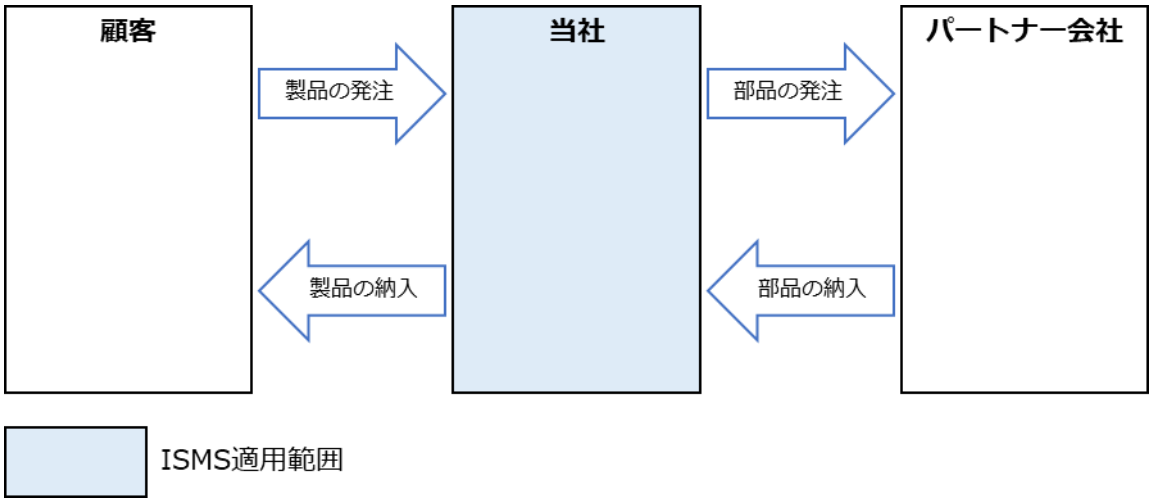


図 52. インターフェースおよび依存関係の記入例

適用範囲を組織の一部とした場合、同じ組織内に適用範囲の内と外という境界ができることになります。適用範囲の境界について、いくつかの観点から明確にしておく必要があります。

人的・組織的境界
組織におけるどの人、どの部門が適用範囲の内側に該当するのかを明確にします。それにより、同じ社内の人であっても、適用範囲外の人を外部の人として扱うといった配慮が必要にな

る場合があります。
物理的境界
適用範囲とする建物や施設、部屋といった空間を明確にします。扉や壁、パーティションなどの物理的な境界によって仕切られていることが望ましいです。
技術的境界
ネットワークにおいて、対象とする範囲を明確にします。物理的境界と同様に、適用範囲の IT 環境の境界を明らかにし、管理しなければならない情報システムや、ネットワークの対象や範囲を明確にする必要があります。
資産的境界
業務委託を受けていたり、組織の一部を適用範囲にしたりした場合に、資産的境界が生じる場合があります。顧客から情報や資源の提供を受けた際に、それを指定された管理方法により管理するのか、自組織の管理下となるのかといった場合や、適用範囲内の部門が保有する情報でも、組織全体で共有している場合にはどう管理するのかを明確にする必要があります。
事業的境界
事業（業務）においても対象を明確にします。事業は部門を横断する場合があるため、人的・組織的境界とも合わせて対象を検討し、適用範囲を明確にする必要があります。

物理的境界 レイアウト図（例）

物理的境界では、適用範囲とする空間を明確にし、境界線を記載します。そして境界線により区切られた空間ごとにセキュリティレベルを設定します。

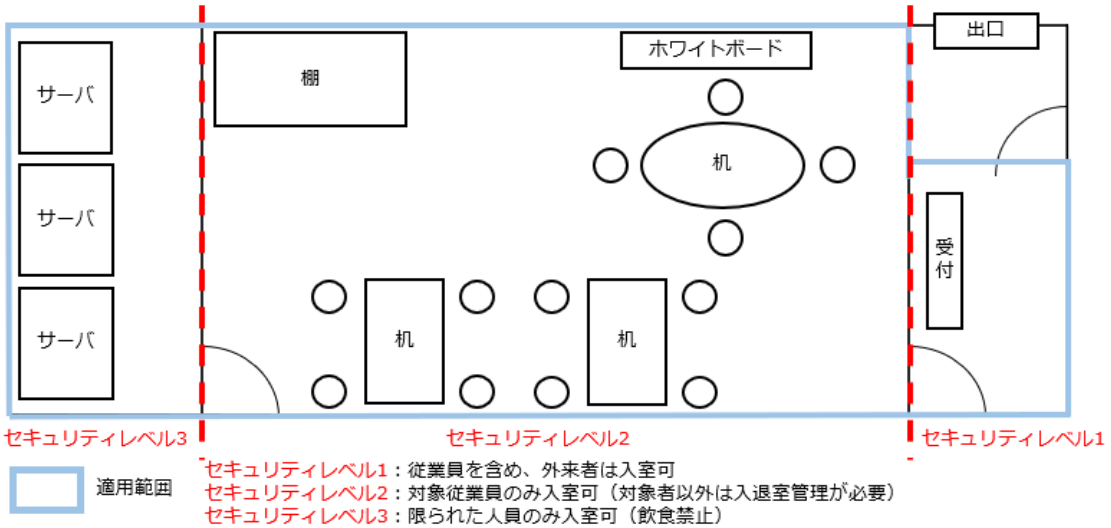


図 53. 適用範囲の例（物理的境界）

技術的境界 ネットワーク図（例）

ネットワークにおいて対象とする範囲を明確にするため、ネットワーク構成図を作成し、境界線を記載します。

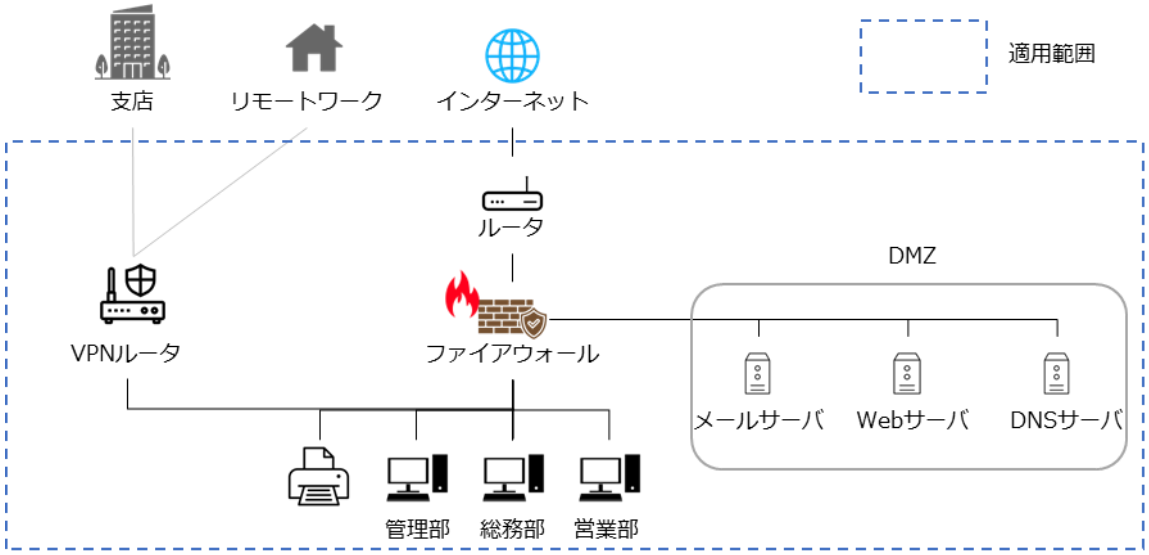
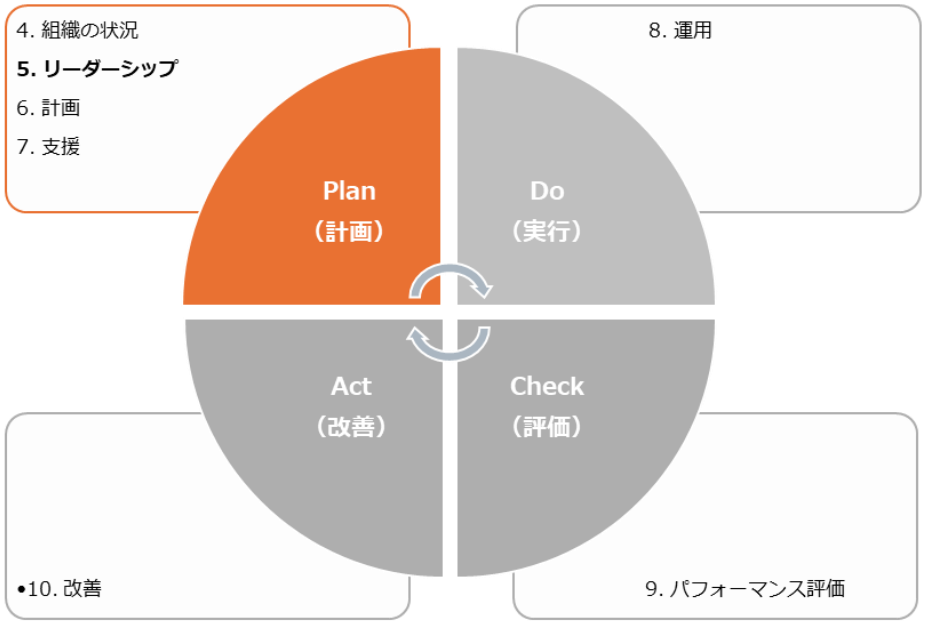


図 54. 適用範囲の例（技術的境界）

13-2-3. ISMS：5. リーダーシップ

「5. リーダーシップ」は、PDCA サイクルの「Plan（計画）」に位置しており、トップマネジメントに求められる要求事項を示しています。トップマネジメントとは、ISMS の適用範囲における最高責任者のことを指します。多くの場合、トップマネジメントは、組織の社長が担う傾向にあります。「5. リーダーシップ」は、PDCA サイクルの軸であり、PDCA サイクルを回すには、トップマネジメントのコミットメント（関与、制約）が重要になります。



5. リーダーシップ	作成文書（例）
5.1 リーダーシップ及びコミットメント トップマネジメントが責任を持って実行しなければならない事項が記載されています。	―
5.2 方針 トップマネジメントが、ISMS の目的や方向性、実施する内容について文書化し、「情報セキュリティ方針」を作成することを要求しています。	● 情報セキュリティ方針
5.3 組織の役割、責任及び権限 トップマネジメントは、ISMS を運用するために必要な役割や責任、権限を各要員に割り当て、どの要員がどのような役割や責任、権限を持っているかがわかる文書を作成することを要求しています。	● ISMS の運用組織図 ● 責任者または部門の名称と役割を明記した文書

5.1 リーダーシップ及びコミットメント

「リーダーシップ及びコミットメント」では、ISMS のトップマネジメントが責任を持たなければならないことを要求しています。トップマネジメントは、以下の事項について責任を持って必ず行う必要があります。

トップマネジメントが行う事項（要求事項）
情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする → 組織の事業の方向性に沿った情報セキュリティ方針と、情報セキュリティ目的を策定することを要求しています。※情報セキュリティ方針、情報セキュリティ目的については後述します。
組織のプロセスへの ISMS 要求事項の統合を確実にする → 自社の業務に、情報資産を管理する手順を組み込むことを要求しています。
ISMS に必要な資源が利用可能であることを確実にする → ISMS を構築・運用するために、必要な予算や人員など経営資源を確保しておくことを要求しています。
有効な情報セキュリティマネジメントおよび ISMS 要求事項への適合の重要性を伝達する → 従業員が ISMS を構築・運用し、情報資産を適切に管理することの重要性を十分に認識できるよう、周知することを要求しています。

ISMS がその意図した成果を達成することを確実にする
→ ISMS を構築・運用することにより得られる成果を明確にし、その成果を十分に得られるように取り組んでいくことを要求しています。

ISMS の有効性に寄与するよう人々を指揮し、支援する
→ ISMS を構築・運用できるようにするため、従業者に対して教育を受けさせたり、定めた決まりを認識・実施させたり、従業員の意見を聞いたりするなど、サポートすることを要求しています。

継続的改善を促進する
→ ISMS を構築・運用するにあたり、従業員が不便に感じていることなど、改善が必要だと考えられる場合には、改善を進めるよう要求しています。

その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する
→ 組織の規模や形態によって、トップマネジメントの指示が従業員に適切に伝わらない可能性があります。そのため、各部門の責任者が主導となり、従業員にトップマネジメントの指示を適切に伝え、ISMS を円滑に構築・運用できるようにすることを要求しています。

5.2 方針

作成する文書	● 情報セキュリティ方針

トップマネジメントは、組織の情報セキュリティに対する考え方や取組の姿勢を利害関係者に示すため、情報セキュリティ方針を文書として作成し、組織内に周知するとともに、必要に応じて、その他の利害関係者が入手できるようにします。例えば、保護するべき情報資産と保護すべき理由を明示し、利害関係者に周知します。

情報セキュリティ方針の作成方法

情報セキュリティ方針が満たさなければならない事項
a. 組織の目的に対して適切である
b. 情報セキュリティ目的を含むか、または情報セキュリティ目的の設定のための枠組みを示す
c. 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む
d. ISMS の継続的改善へのコミットメントを含む

a) 自社の経営理念に基づいた事業の目的や、情報セキュリティの必要性などを記載します。また、業務に関わる情報資産と、保護すべき理由などを記載します。

b) 情報セキュリティに関する目標を記載します。

情報セキュリティ方針（例）

【第X版】
【日付】
【社名】
【代表取締役社長 名前】

私たち【社名】は、【提供するサービス名】の提供を通じて、お客様、社員とその家族などすべてのステークホルダーの期待に応え、社会に貢献することを使命と考えています。

当社の事業活動において、お客様からお預かりする個人情報を含む多くの情報資産を活用しており、すべてのステークホルダーの期待に応えるためには、これらの情報資産を保護することは、経営上の最重要課題であると認識しています。

よって、私たちは、情報セキュリティ基本方針を策定し、本基本方針に基づいて、ISMSを構築・運用し、当社を取り巻く環境の変化を踏まえ、継続的改善に全社を挙げて取組むことをここに宣言します。

さらに、当社は、以下のセキュリティ目的を設定し、この目的を達成するための諸施策を確実に実施します。
- ✓ お客様との契約および法的または規制要求事項を尊重し遵守する。
- ✓ 情報セキュリティ事故を未然に防止する。
- ✓ 万一情報セキュリティ事故が発生した場合、影響を最小限にする。

以上

c) 自社の業務の特徴や課題を記載します。

d) ISMSに関する取組みを定期的に見直し、改善していく内容を記載します。

5.3 組織の役割、責任及び権限

作成する文書	● ISMS 運用組織図 ● 責任者または部門の名称と役割を明記した文書

「組織の役割、責任および権限」とは、ISMS を構築・運用するために、トップマネジメントが、組織内で役割を決め、責任と権限を割り当てることです。

ある程度の規模を超えた組織になると、ISMS の実際の運用担当者や責任者は、トップマネジメントから権限を委譲された人になります。そうすると、情報セキュリティに関する取組の実態を、トップマネジメントが十分把握していないという状況になりがちです。そうならないために、ISMS の実施状況をトップマネジメントに報告する仕組みやルールを作っておく必要があります。

ISMS 運用組織図の作成方法（例）

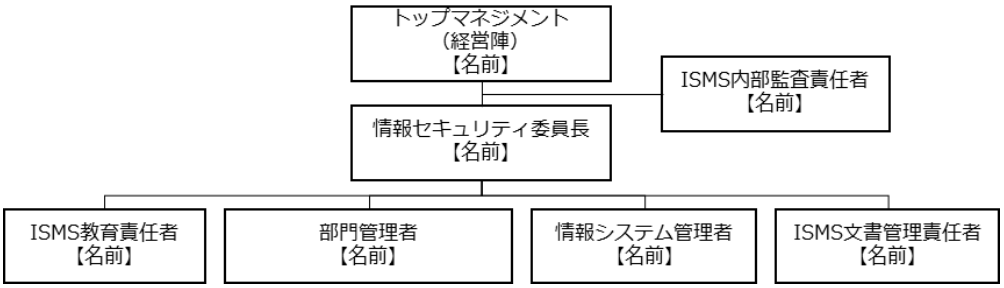


図 55. ISMS 運用組織図の例

ISMS の運用組織図を作成する流れを説明します。

1. トップマネジメントは、情報セキュリティ委員長を任命し、上記の事項に関する権限や責任を持たせる必要があります。そのため、トップマネジメントの下位に、情報セキュリティ委員長を配置します。
2. ISMS 内部監査責任者は、内部監査を実施する際の最高責任者であり、トップマネジメントの下位に設置します。
3. 情報セキュリティ委員長は、ISMS の実施・運用をするために必要な役割を持つ責任者を任命します。情報セキュリティ委員長の下位に各責任者を配置します。

責任者または部門の名称と役割を明記した文書化の方法（例）

名称	役割
情報セキュリティ委員長	ISMS の実施、運用について統括する
ISMS 内部監査責任者	ISMS とその実施状況に関わる監査を統括する
ISMS 教育責任者	ISMS に関する教育計画の立案と実施を行う
部門管理者（情報セキュリティ委員）	ISMS 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程・規則に従い、ISMS を維持するための安全管理対策を実施する
ISMS 文書管理責任者	ISMS に関する文書と記録などの維持・管理を行う

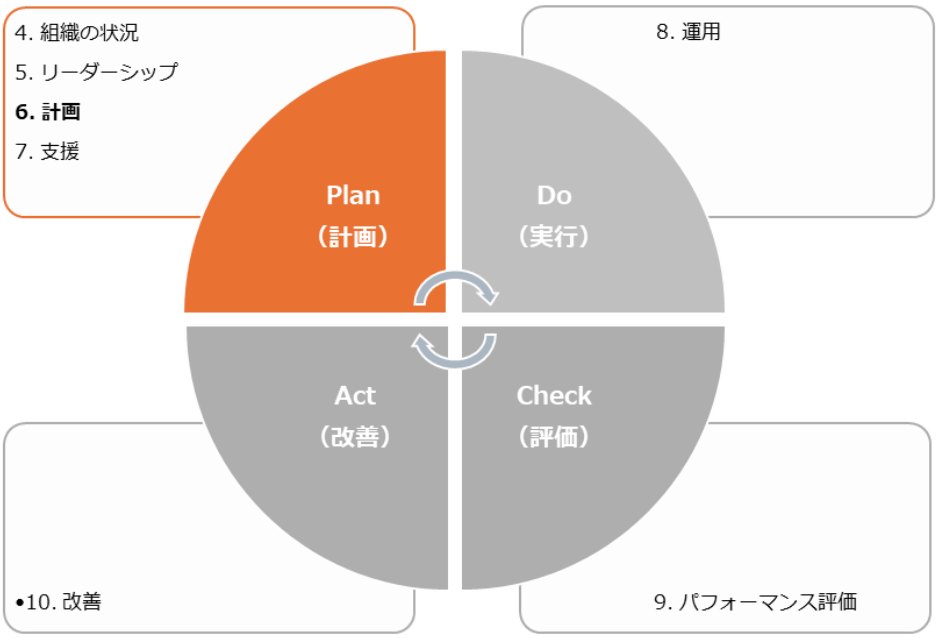
13-2-4. ISMS：6. 計画

「6. 計画」は、PDCA サイクルの「P（計画）」に位置しており、リスクマネジメントの確立、情報セキュリティにおけるリスクアセスメント、リスク対応、情報セキュリティ目的の管理に関する要求事項を示しています。

本項では、リスクマネジメントで作成する文書化の方法について解説します。リスクマネジメント手順については「12 章.リスクマネジメント」を参照してください。

6. 計画	作成文書（例）
6.1 リスク及び機会に対処する活動 **一般** 特定した内外部の課題と、利害関係者のニーズおよび期待を考慮して、リスク・機会（期待する状況や結果）を決定し、対処するための	● 資産目録（情報資産管理台帳） ● リスクアセスメント結果報告書

活動を明確にすることを要求しています。 **情報セキュリティリスクアセスメント** 組織や企業の資産に対する、情報セキュリティリスクアセスメントプロセスの確立を要求しています。 **情報セキュリティリスク対応** 情報セキュリティリスク対応の手順を確立することを要求しています。	● 適用宣言書 ● リスク対応計画
6.2 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティ目的を確立し、達成するための計画を策定することを要求しています。	● ISMS 有効性評価表
6.3 変更の計画策定 ISMS の変更が必要なときは、計画的な変更を要求しています。	—



6.1 リスク及び機会に対処する活動

作成する文書	● 資産目録（情報資産管理台帳） ● リスクアセスメント結果報告書 ● 適用宣言書 ● リスク対応計画

「リスク及び機会に対処する活動」とは、「ISMS の意図した成果を達成する」「ISMS の望ましくない影響を防止・低減する」「継続的改善を達成する」の 3 つを実現するために、妨げとなるよ

うな機会やリスクを発見し、対処することです。平たく言えば、情報セキュリティ上のリスクに対して、適切な対策を講じることにより、情報セキュリティを確保するための活動になります。具体的には「リスクアセスメントの実施」「リスク対応策の作成と実施」「リスク対応策の有効性評価」「継続的改善」といった活動が含まれます。

リスクアセスメントは、組織や企業の資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位付けをしていくプロセスになります。リスクアセスメントの実施により、リスクを評価し、事前にリスクを把握することにより必要な投資額を含め、企業が適切な対策を検討することが可能になります。

情報セキュリティのリスク基準を確立し、維持する
リスクアセスメントを実施するにあたり、リスクの重大性を評価するための目安となるリスク基準を決める必要があります。ISMS では、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むように明示されています。 ※「12-2-1. リスク基準の確立」を参照
情報セキュリティリスクを特定する
企業が掲げる目的・目標達成を阻害する可能性のあるリスクをすべて洗い出すことです。そのため、リスクの発生可能性や影響の大きさを考慮せず、少しでも企業に影響を与えそうなリスクを洗い出すことが目的となります。リスク特定として最終的な成果はリスク一覧表の作成になります。 ※「12-2-2. リスクの特定」を参照
情報セキュリティリスクを分析する
リスク特定により特定されたリスクに対して、リスク分析を行います。リスク分析を行うことで、「企業にとって対応が必要なリスクはどれか」、「優先的に対応しなければならないリスクは何か」といったことを判断します。リスク分析による結果を、「リスクアセスメント結果報告書」に記載します。 ※「12-2-3. リスクの分析」を参照
情報セキュリティリスクを評価する
リスク分析により算出したリスクレベルからリスク受容基準と比較し、リスク対策が必要か否かを判断します。また、算出したリスクレベルをもとに優先順位を付けます。 ※「12-2-4. リスクの評価」を参照

資産目録（情報資産管理台帳）、リスクアセスメント結果報告書は、ISO/IEC 27001:2022 の管理策「5.9 情報およびその他の関連資産の目録」に対応します。

資産目録（情報資産管理台帳）の作成方法（例）

資産目録（情報資産管理台帳）の作成方法は「12-2-2. リスクの特定」を参照してください。

リスクアセスメント結果報告書の作成方法（例）

作成した資産目録（情報資産管理台帳）から、リスクアセスメントの結果をまとめた「リスクアセスメント結果報告書」について説明します。

※下記表の「対応」の項目を記載するタイミングは、「8.運用」となります。

No	資産目録のNo	リスク特定					リスク分析（一次評価）			優先順位	リスク対応						二次評価		
		リスク源	影響領域	事象	原因	起こり得る結果	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応	重要度	被害発生可能性	リスクレベル
1	9	モバイル機器の利用ルールが十分に整備されていない	外部	持出中に重要な情報を紛失・盗難（機密性の喪失）	【事象】に対し【リスク源】である	機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	予定	2	1	2
2	40	教育が不十分なため従業者の意識が低い	全社	誤送信（機密性の喪失）	【リスク源】ため【事象】が発生	機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	予定	1	1	1
3	10、11、13、26、55	電子の情報分類／取り扱いが明確でない	外部	情報の紛失・盗難（機密性の喪失）	【リスク源】ため【事象】が発生	機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			・5.12 情報の分類、5.13 情報のラベル付け、分類ごとの情報の取扱いルール	予定	2	3	6

リスクアセスメント結果報告書には、以下の内容を記載します。

資産目録の No.	重要資産の項番を記載します。 重要資産は、資産目録（情報資産管理台帳）から「情報セキュリティリスクアセスメントを実施するための基準」で決定した基準をもとに選択します。例えば、機密性、完全性、可用性の項目について、評価値が 1 つでも 3 となった資産を重要資産とします。 ※リスクによっては資産目録の No は複数になることがありま

		す。 ※「情報セキュリティリスクアセスメントを実施するための基準」については、「12-2-1. リスク基準の確立」を参照してください。
リスク源		想定される脅威を記載します。 （例）モバイル機器の利用ルールが十分に整備されていないなど
影響領域		脅威が発生した場合の影響範囲を記載します。 （例）外部、全社など
事象		発生する可能性のある事象を記載します。 （例）持ち出し中に重要な情報を紛失・盗難（機密性の喪失）など
原因		事象が発生する原因を記載します。 （例）【事象】に対し【リスク源】のため【事象】が発生など
起こり得る結果		事象が発生した場合に起きる結果を記載します。 （例）機密情報などが漏えいし顧客に影響、信用喪失など
一次評価	**重要度**	算出方法は、「12-2-2. リスクの特定」を参照してください。
	被害発生可能性	算出方法は、「12-2-3. リスクの分析」を参照してください。
	リスクレベル	算出方法は、「12-2-3. リスクの分析」を参照してください。
優先順位		リスク受容基準をもとに、リスクレベルから優先順位づけを行います。 （例） 1：早急に対応、2：今期中に対応、3：今期対応が望ましい リスクレベル：9→優先順位：1 リスクレベル：4→優先順位：3 リスクレベル：6→優先順位：2
保有、低減、回避、移転		リスク対応により決定した対応について「●」を記載します。
管理策		リスク対応により決定した内容を記載します。 （例）モバイル機器の利用ルールを整備・強化など ※附属書 A の管理策のリストは包括的なものではないので、必要に応じてリストにない管理策を採用してもかまいません。
対応		管理策の実施状況を記載します。 ● 管理策を実施した場合は「済み」 ● 管理策を実施する予定がある場合は「予定」 ● 管理策を実施する予定が未定の場合は「未定」

二次評価	**重要度**	算出方法は、「12-2-2. リスクの特定」を参照してください。
	被害発生可能性	算出方法は、「12-2-3. リスクの分析」を参照してください。
	リスクレベル	算出方法は、「12-2-3. リスクの分析」を参照してください。

※「二次評価」とは、リスクに対する管理策の有効性評価をするために行うものです。リスク対応を実施した結果をもとに、情報資産に対する再評価を実施します。

適用宣言書の作成方法（例）

「適用宣言書」は、ISMS 認証を取得するすべての組織に作成が義務づけられています。認証を取得しない組織では、必須ではありませんが、情報セキュリティに対する取組を明確にするために「適用宣言書」を作成することが望ましいとされています。

適用宣言書は以下の内容を含むように作成します。

- 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
- 附属書 A に規定する管理策を除外した理由

管理目的および管理策			適用	実施・未実施	管理策を含めた理由 管理策を除外した理由	規程・手順書
5 組織的管理策						
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することが望ましい。	○	○	情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するため	情報セキュリティ方針
5.2	情報セキュリティの役割および責任	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、割り当てることが望ましい。	○	○	ISMS の構築・運用を円滑に行うため	情報セキュリティ手順書
5.3	職務の分離	相反する職務および責任範	○	○	許可されていないもしくは	情報セキュリティ

		囲は、分離することが望ましい。			意図しない変更または不正使用の危険性を低減するため	手順書
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することが望ましい。	○	○	ISMS の取組が、経営陣の経営戦略の一部であることを確実にするため	情報セキュリティ手順書
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することが望ましい。	○	○	セキュリティインシデントが発生したことを迅速に報告するため	情報セキュリティ手順書
…	…	…	…	…	…	…

適用宣言書には、以下の内容を含めます。

管理目的および管理策	ISO/IEC 27001 の附属書 A の管理策を記載します。 （例）5.1 情報セキュリティのための方針群など
適用	適用または適用除外を記載します。 （例）○：適用、×：適用除外
実施・未実施	実施したか否かを記載します。 （例）○：実施、未：未実施、ー：適用除外
管理策を含めた理由または管理策を除外した理由	管理策を行う場合も理由を記載します。 （例）情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するためなど
規程・手順書	管理策が含まれている規程または手順書を記載します。 （例）情報セキュリティ手順書 5.1.1、A-02 情報セキュリティ方針など

情報セキュリティリスク対応計画

「リスク対応計画」は、それぞれのリスクに対して、どのような管理策を、誰が、いつまでに、どのように実施するのかを表にまとめたものになります。

リスク対応計画の作成方法（例）

リスクアセスメント結果報告書から、リスク対応を行う管理策をすべて記載し、それぞれの具体

的な内容や、担当者などを記載します。リスク対応を行った場合、実績やリスク対応のステータスを記載する必要があります。

※下記表の「実績」と「ステータス」の項目を記載するタイミングは、「8.運用」となります。

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	ルール検討 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-	20XX/-/-	終了
2	教育訓練	ルール検討 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-		着手
3	情報の分類定義 分類ごとの情報の取扱いルール ラベリング	情報の分類定義 分類ごとの取扱いルール検討 関係者に周知	委員長	20XX/-/-	20XX/-/-			未着手

リスク対応計画では、以下の内容を記載します。

管理策	リスクアセスメント結果報告書の管理策を記載します。 （例）モバイル機器の利用ルールを整備・強化など
タスク	管理策を実施する上で、具体的な業務を記載します。 （例）ルール検討、関係者に周知
担当	管理策の担当者を記載します。 （例）委員長
予定	リスク対応予定の開始日と終了日を記載します。 （例） 開始：2024/08/10 終了：2024/09/29
実績	開始の箇所：実際にタスクを開始した日付を記載します。 終了の箇所：実際にタスクが完了した日付を記載します。
ステータス	タスクの進捗状況を記載します。 ● タスクが完了した場合は「終了」 ● タスクを実行中の場合は「着手」 ● タスクに着手していない場合は「未着手」

リスク所有者からの承認/残留している情報セキュリティリスクの受容

リスク対応計画と残留リスク（管理策の適用後に）は、リスク特定で決めたリスク所有者の承認

が必要になります。リスク所有者が承認する際は、記録をする必要があるため、ワークフローやチェック欄などを用います。

（例）承認プロセスとして、作成した書類にチェック欄（電子印欄など）を作成します。

作成	承認

作成者/更新者	【名前】	作成日/更新日	【日付】
承認者	【名前】	承認日	【日付】

6.2 情報セキュリティ目的及びそれを達成するための計画策定

作成する文書	● ISMS 有効性評価表

情報セキュリティ目的の基本要件として以下の要件を満たす必要があります。

- 情報セキュリティ方針と整合している
- （実行可能な場合）測定可能である
- 適用される情報セキュリティ要求事項, 並びにリスクアセスメント及びリスク対応の結果を考慮に入れる
- これを監視する
- これを伝達する
- 必要に応じて、更新する
- 文書化した情報として利用可能な状態にする

情報セキュリティ目的と、それを達成するための計画を ISMS 有効性評価表に記載します。
「8. 運用」で計画を実施し、「9. パフォーマンス評価」で評価を行います。

ISMS 有効性評価表の作成方法（例）

※下記表の「評価」の項目を記載するタイミングは、「9. パフォーマンス評価」となります。

【計画】
情報セキュリティ目的
お客様との契約および法的または規制要求事項を尊重し順守する
情報セキュリティ事故を未然に防止する
情報セキュリティ上の脅威から情報資産を保護する
当社 ISMS の意味を理解した活動の開始

評価指標

ISMS 教育受講／合格 100%（全従業者）
【備考】
取組みの初年度であるため、全従業者が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。

情報セキュリティ目的達成のための計画

実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業者が ISMS 教育を受講	ISMS 事務局長	20XX 年-月	受講者数および合格者数をカウントし、評価する

【評価】
評価日：【20XX/00/00】
情報セキュリティ目的達成に関する評価結果（凡例 ○：有効 ×：有効ではない）

結果：〇
備考：全従業員 e ラーニングでのテストを 100 点にて合格。有効性があるものと判断する。

ISMS 有効性評価表では、以下の内容を記載します。

情報セキュリティ目的	適用範囲（組織全体、各部署ごと）でのセキュリティ目的を記載します。 （例） 重大なセキュリティインシデントを発生させない、 マルウェア感染およびサイバー攻撃によるシステム停止の防止など
評価指標	測定可能な値を記載します。 （例）マルウェア感染の有無、システム停止の有無など
実施事項	情報セキュリティ目的を達成するための実施内容を記載します。 （例）ウイルス対策ソフトのインストール、標的型メール訓練の実施など
必要な資源	計画の責任者を記載します。 （例）部長各自など
責任者	計画の責任者を記載します。 （例）部長各自など
達成期限	計画の期限を記載します。 （例）年度末、2024 年 9 月など

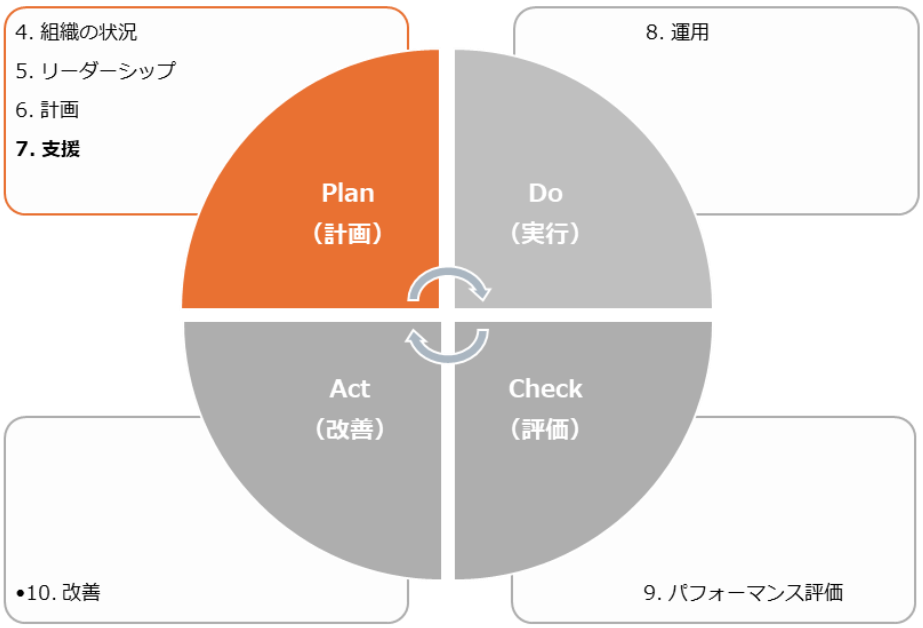
評価方法	具体的な評価方法を記載します。 （例）年度末に発生したセキュリティインシデントをカウントし、評価するなど
評価	情報セキュリティ目的達成に関する評価結果には、ISMS が有効だったか否かという結果を記載します。

13-2-5. ISMS：7. 支援

「7. 支援」は、PDCA サイクルの「Plan（計画）」に位置しており、ISMS の運用をサポートするための要求事項が規定されています。

7. 支援	作成文書（例）
7.1 資源 ISMS に必要な資源（人、物、金、情報）を決定し、提供します。	―
7.2 力量 ISMS 適用範囲の要員に求められる力量（知識、技能など）を定義し、要員が力量を備えているか評価を行います。力量評価の結果、力量が不足している場合は、力量を身に付けるための教育を計画し、実施します。教育の実施後、力量を取得・維持できたか確認テストを行います。最後に、実施した教育内容を記録として保持します。	● 力量確認表 ● 教育計画書 ● 理解度確認テスト ● 教育実施記録
7.3 認識 ISMS 適用範囲のすべての要員に、以下の内容を認識させる必要があります。 ● 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るメリットや、自身の業務と ISMS の関係、実施すべきセキュリティ対策 ● ISMS によって割り当てられた責任を果たさなかった際の影響	―
7.4 コミュニケーション ISMS を運用するにあたり、必要な意思疎通ができるプロセスを確立する必要があります。	―
7.5 文書化した情報 ISMS に必要な文書化した情報の作成、更新、管理についての要求	―

事項が記載されています。	



7.1 資源

ISMS の PDCA サイクルを回すために必要な資源を決定し、利用できるようにする必要があります。必要な資源を決定し提供することは、トップマネジメントが行う必要があります。（リーダーシップ及びコミットメントの箇所で要求されています。）

ISMSのPDCAサイクルを回すために必要となる資源を決定し、提供する

資源の具体例を以下に示します。例を参考に、ISMS の PDCA サイクルを回すために自社で必要となる資源を決定し、利用可能にします。

資源	具体例
人	ISMS を構築・運用するために必要となる要員 ISMS の推進体制の確立 必要に応じた外部の専門家など

物	情報を処理するための機器（サーバ、ネットワーク機器など） コミュニケーション手段（パソコン、スマホなど） 活動に必要な施設など
金	人、物の資源を確保するための予算 要員の教育費用 ISMS の維持費など
情報	文書化した情報 ISMS の PDCA サイクルを回すために有用な情報 情報セキュリティに関する最新情報など

7.2 力量

作成する文書	● 力量確認表 ● 教育計画書 ● 理解度確認テスト ● 教育実施記録

ISMS 適用範囲の要員に必要な力量（知識、技能など）を明確にし、実際に要員が力量を備えているか評価を行います。力量が不足している場合、力量を身に付けるための教育を計画し、実施する必要があります。教育の結果、力量が取得できたかを評価します。

力量確認表の作成方法（例）

要員の力量を評価し、確認するための力量確認表を作成する方法について説明します。

以下は、部門管理者の力量評価の例です。以下の手順で赤文字の箇所を自社の状況に合わせたものに修正することにより、自社に適した力量確認表を作成できます。

1. 要員ごとに、「組織の役割、責任及び権限」により割り当てられた役割や責任を果たすために必要となる力量を、「必要条件」として定義します。
2. 責任者として任命できるか否かを判断するための任命基準を定義します。
3. 定義された力量をどれほど備えているか、評価基準を決めて評価を行います。
4. 評価の結果、力量が不足している場合は教育・訓練を実施します。
5. 教育・訓練の実施後、どれほど改善できたか評価を行い、任命基準をもとに責任者として任命できるか判断します。

役割	部門管理者	**任命基準**	A	B	C
氏名	○○ ○○	**区分**	任命可	改善確認後任命可※	任命不可 再任命
A：項目のすべてが"3"以上。					

B：項目の"2"以下について改善の予定がある。
C：項目の"2"以下について改善の予定がない。
※改善確認までは暫定的に任命し、改善確認後に正式任命とする

	必要条件	評価	改善予定日	改善内容	改善後評価	改善確認日
1	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS 構築作業を通して獲得	3	20XX/-/-
2	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS 構築作業を通して獲得	3	20XX/-/-
3	情報セキュリティ全般に関する知識があること	2	20XX/-/-	ISMS 構築作業を通して獲得	3	20XX/-/-
4	公正な判断ができること	5				

評価基準	内容
5	十分な力量がある。指導・教育ができる
4	力量がある。支援なしに対応ができる
3	力量がある。他の支援により対応ができる
2	改善の余地がある
1	改善が必要

教育計画書の作成方法（例）

力量評価の結果をもとに、必要な力量を身に付けるための教育を計画します。以下の例をもとに、教育計画書の作成方法を説明します。

教育目的	ISO27001 認証取得のため
教育対象者	全従業者
教育方法	方法：e ラーニングによる自己学習、確認テスト。 委員会より、受講対象者に受講案内のメールを送付。 受講者は、案内にある URL から e ラーニングのシステムにアクセスし、受講（テキストのダウンロード）／確認テストを行う。

教育内容	ISMS に対する意識向上 当社の方針や手順について（情報セキュリティ基本方針など） ISMS の有効性に対する自らの貢献 ISMS 要求に適合しないことの意味 当社のルールの順守
実施期間	20XX 年-月-日（-）～20XX 年-月-日（-）
教育の有効性評価	情報セキュリティハンドブックを用いて教育を実施。 教育終了後、アンケート／確認テストを実施し記録に残す。 確認テストは、合格点は 100 点以上とする。 確認テストは、合格点に達するまで繰り返す。

教育計画書には、以下の内容を含めます。

教育目的	教育を実施する目的を記載します。
教育対象者	教育を受ける対象者を記載します。
教育方法	教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、e ラーニングなどさまざまあります。必要な力量を身に付けるために適切と考えられる方法を選択します。
教育内容	どのような教育を実施するのか、教育内容を記載します。
実施期間	教育を実施する期間を記載します。
教育の有効性評価	必要な力量を身に付けることができたか評価する方法を記載します。 明確に評価が可能であれば、どのような方法でも問題ないです。例えば、テストやアンケートの実施が挙げられます。次のページでテストの作成方法について説明します。

理解度確認テストの作成方法（例）

教育の実施後、必要な力量を身に付けることができたか評価するため、教育内容に関するテストを行うことが有効です。テストは、理解度が点数という数値で可視化されるため、評価がしやすく、多くの企業が実施しています。テストの作成例は以下の通りです。

次の【　　】に入る言葉として最も適したものを選びなさい（各 10 点）

設問			答え
【　　】とは、ISMS を構築・運用するための国際規格である。			C
A. ISO9001	B.ISO14001	C.ISO27001	
情報セキュリティという言葉は、一般的に、情報の【　　】、完全性、可用性を維持改善することと定義されている。			C

A. 信頼性	B.整合性	C.機密性	
2024 年度の当社の情報セキュリティ目標は、【　　】である。			
A.ISMS 教育受講／合格 100 %（全従業者）	B.予防処置の発行件数を四半期に 1 件以上	C.セキュリティインシデント発生件数／2 件以内	A
【　　】とは、企業や個人の情報を盗み取るため、特定の相手（企業組織や社員）をメールなどの手段で狙う攻撃のことです。			A
A. 標的型攻撃	B. ウイルス型攻撃	C. サイバー攻撃	
標的型メール攻撃の特徴はどれか。			
A. 支払う必要がない料金を振り込ませるために、債権回収会社などを装い無差別に送信される。	B. 件名や本文に、組織の担当者の業務に関係する内容が記述されている。	C. 偽のホームページにアクセスさせるために、金融機関などを装い無差別に送信される。	B

次の文章のうち正しいものには○、間違っているものには×を付けなさい（各 10 点）

設問	答え
⑥ ISMS では、情報資産とは、書類、データに加えて、ハードウェア、ソフトウェア、設備、ファームウェア（媒体など）、要員までも包括する。	○
⑦ 私物の外部記録媒体（USB メモリ、外づけ HDD など）の使用は原則禁止である。	○
⑧ 当社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情報を社外へ持ち出す場合は、責任者の許可を得て、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。	○
⑨ PC のログインパスワードは英数混合 8 文字以上のパスワードとする。	○
⑩ PC のパスワード付きスクリーンセーバの設定時間は、15 分以内とする。	×

実施日		**氏名**	
所属		**得点**	点/100 点

✓ テストは、選択問題や正誤形式にすることにより採点がしやすくなります。

✓ 教育内容に合った問題を考え、作成します。例えば、今回の教育内容に「当社のルールの順守」が含まれているため、⑥～⑩のような設問を作成します。

教育実施記録の作成方法（例）

教育を実施した際、実施記録を文書化する必要があります。以下の例をもとに、教育実施記録の作成方法を説明します。

教育の名称	ISMS 教育（基本方針、目標、ルール）
実施期間	20XX 年-月-日（-）～20XX 年-月-日（-）
実施方法	e ラーニング

使用テキスト	情報セキュリティハンドブック
教育の概要	情報セキュリティハンドブックなどによる ISMS に対する意識向上 ● 当社の方針や手順について（情報セキュリティ基本方針など） ● ISMS の有効性に対する自らの貢献 ● ISMS 要求に適合しないことの意味 ● 当社のルールの順守 学習後にテスト実施
受講対象者・部門	上記教育実施期間において在籍する全従業者
参加者	別紙：「教育受講者一覧」を参照
備考	特になし

教育実施記録には、以下のような内容を含めます。

教育の名称	どのような教育を実施したのか、教育テーマを記載します。
実施期間	教育を実施する期間を記載します。
教育方法	教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、e ラーニングなどさまざまあります。その中で、実際に実施した方法を記載します。
教育の概要	実施した教育の概要や、教育を実施した目的を記載します。
受講対象者・部門	教育を受講する対象者を記載します。
参加者	教育を実際に受講した者を記載します。以下の例のように、「教育の受講者一覧」を別紙で作成し、実施記録と分けて記載するとわかりやすくなります。

No	所属	氏名	受講日
1	営業	○○○○	20XX/-/-
2	管理	○○○○	20XX/-/-

7.3 認識

ISMS 適用範囲で働くすべての社員、従業員が情報セキュリティ方針を理解し、それを実現することの重要性を認識する必要があります。逆に、セキュリティ対策を実施せず、セキュリティ方針を実現できなかった場合、どのようなことが起きるのかについて理解する必要もあります。

具体的には、以下の内容について教育を行い、ISMS の重要性を十分理解させる必要があります。

- 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るメリットや、自身の業務と ISMS の関係、実施すべきセキュリティ対策の具体的な内容

- ISMS によって割り当てられた責任を果たさなかった場合の組織に与える影響

これらの内容について認識を持たせるために、教育や訓練を実施します。具体的な教育・訓練の実施手順は、「力量」や「コミュニケーション」で説明します。

力量

上記の内容について、各要員が認識しているか評価を行い、認識が不十分の場合は教育を実施し、認識させます。

コミュニケーション

情報提供・共有によって、上記の内容の認識を深めるようにします。

7.4 コミュニケーション

ISMS の PDCA サイクルを回すためには、内部および外部とのコミュニケーションを円滑に行う必要があります。そのため、組織内および組織外の関係者とコミュニケーションをとる手順などを定め、必要なときに円滑なコミュニケーションが行える体制を整えておくことが重要です。コミュニケーションの手順などには、以下の内容が含まれます。

- コミュニケーションの内容
- コミュニケーションの実施時期
- コミュニケーションの対象者
- コミュニケーションの方法

ISMS に関連するコミュニケーションをとる手順を確立した例を、以下に示します。例を参考に、自社の ISMS に対して PDCA サイクルを回す上で必要なコミュニケーションをとる手順を確立します。

内容	実施時期	対象者	実施者	方法
情報セキュリティ方針の伝達	随時	利害関係者	トップマネジメント（ISMS 事務局）	外部 ・当社 HP に公表 内部 ・ISMS 定期教育にて ・当社 HP に公表 ・社内掲示
各見直し結果の伝達	見直後、 1 週間以内	従業者	ISMS 事務局	承認後、ISMS 事務局より通達

セキュリティ調査結果の報告	依頼入手時	お客様	ISMS 事務局	・お客様より調査票などを入手した場合、主管部門にて回答を作成 ・ISMS 事務局責任者が確認の上、お客様に提出
セキュリティインシデントの伝達	発見時	ISMS 事務局	発見者	「情報セキュリティ手順書：セキュリティインシデント対応フロー」の通り
	適時	トップマネジメント	ISMS 事務局	同上
	適時	関係当局	ISMS 事務局	同上

内容	コミュニケーションで伝える情報
実施時期	伝えるタイミング
対象者	誰に伝えるのか、情報を伝える対象者
実施者	誰に伝えるのか、情報を対象者に伝える者
方法	情報を伝える手段

7.5 文書化した情報

ISMS に必要な文書化した情報の作成、更新、管理方法を決めます。

一般

以下の情報を ISMS に含める必要があります。

- ISO/IEC 27001 が要求する文書化した情報
- ISMS の有効性のために必要であると組織が判断した文書化した情報

以下は、ISO/IEC 27001 が要求する文書化した情報の一覧です。

文書化した情報	作成する項番
ISMS の適用範囲	「4. 組織の状況」で作成
情報セキュリティ方針	「5. リーダーシップ」で作成
リスクアセスメントプロセスに関わる文書化された情報	「6. 計画」で作成
リスク対応プロセスに関わる文書化された情報	
情報セキュリティ目的に関わる文書化された情報	

力量の証拠	「7. 支援」で作成
組織が決めた文書化された情報	
ISMS のプロセス実施に関わる文書化された情報	「8. 運用」で作成
リスクアセスメントの結果	
リスク対応の結果	
監視・測定の結果	「9. パフォーマンス評価」で作成
監査プログラムの実施、結果に関わる文書化された情報	
マネジメントレビューの結果	
不適合の内容と処置、処置の結果	「10. 改善」で作成

作成および更新

ISMS に必要な文書化した情報を作成・更新する際に、以下の事項を確実にする必要があります。

1. 適切な識別と記述

文書化した情報を識別できるよう、以下の例のように採番方法を決めたり、各文書には適切なタイトル、作成者、承認者、日付などを記載したりします。

文書の種類	採番方法
基本文書	A-□□（01 から採番を始める）
ISMS マニュアル	B-01
手順書	C-01
記録類	D-01
外部文書	採番せずに文書名、作成社名などの名称にて識別する

2. 適切な形式

文書化する情報を記載する媒体として、紙や電子データなどを指定し、適切な形式（文字、図表など）を用いて読みやすく、簡潔に記載します。

3. 適切なレビューと承認

文書化した情報は、適切な承認とレビューを行い策定します。

文書化した情報の管理

ISMS の文書化した情報を管理する必要があります。

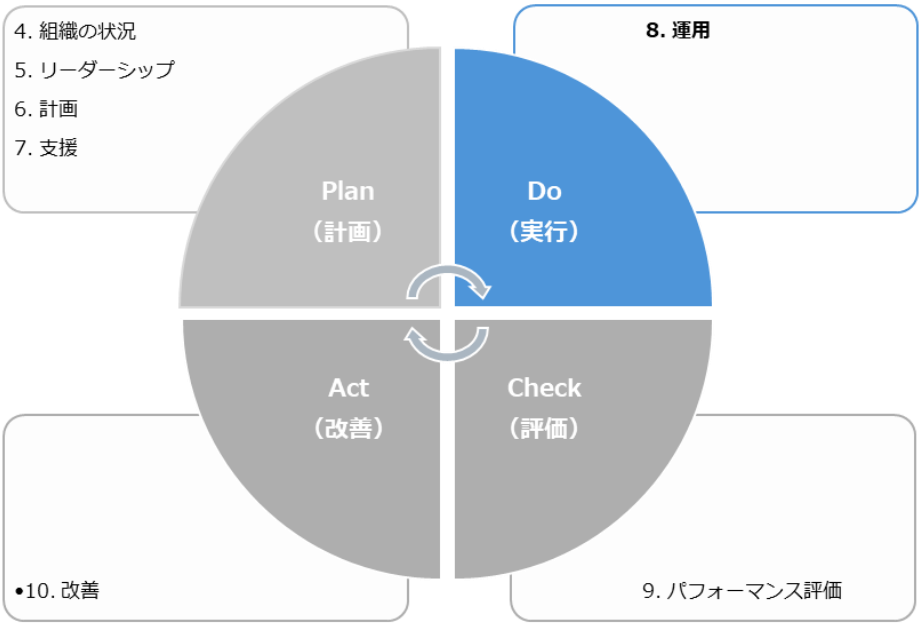
（管理方法の例）

文書化した情報は、ISMS 事務局責任者が、最新版を紙の媒体としてファイリングし、キャビネ

ットにて保管し、適用範囲内の対象者が必要なときに、必要なところで利用可能にする

13-2-6. ISMS：8. 運用

「8. 運用」は、PDCA サイクルの「Do（実行）」に位置しており、「6. 計画」で計画した活動や、要求事項を満たすための活動を実施し、管理します。そして、計画通りに実施した証拠となる情報を文書化し、保持する必要があります。



8. 運用	作成文書（例）
8.1 運用の計画及び管理 「6. 計画」で計画した活動や、要求事項を満たすための活動の実施状況を管理するための一覧表を作成します。	ISMS 年間計画表
8.2 情報セキュリティリスクアセスメント 「6. 計画」で定めたリスクアセスメントのプロセスを実施し、結果を文書化します。	リスクアセスメント結果報告書
8.3 情報セキュリティリスク対応 「6. 計画」で定めたリスク対応計画を実施し、結果を文書化します。	リスク対応計画

8.1 運用の計画及び管理

作成する文書	● ISMS 年間計画表

「6. 計画で決定した活動」および「要求事項を満たすための活動」を実施するにあたり必要な

プロセスを計画し、ISMS 年間計画表を作成します。ISMS 年間計画表は、「6. 計画で決定した活動」および「要求事項を満たすための活動」の実施状況を管理するための計画表です。

ISMS 年間計画表の作成方法

以下の例は、「6. 計画」で決定した活動に関する計画表の例です。

No	実施事項		文書名	スケジュール							
				2024 年 5 月				2024 年 6 月			
				8	15	22	29	5	12	19	26
6.1	「リスク及び機会に対処する活動」の検討	外部および内部の課題に対する活動の検討	外部および内部の課題								
		リスクアセスメントの実施	資産目録								
			リスクアセスメント結果報告書								
		リスク対応のための計画作成	適用宣言書								
		（アクションプランの作成）	リスク対応計画								
		管理策（ルール）の検討	情報セキュリティ手順書								
6.2	部門ごとに「情報セキュリティ目的及びそれを達成するための計画」を作成		ISMS 有効性評価表								

No	ISO/IEC 27001 の要求事項の項番を記載します。
実施事項	行う活動の内容を記載します。
文書名	実施事項で記載した活動を行う際に利用したり、作成したりする文書名を記載します。
スケジュール	実施事項を行う予定日を記載します。

ISMS の要求事項全体を示した計画表の例を紹介します。

前記の計画表は、ISMS の要求事項のうち「6.計画」の箇所だけを抜粋し、作成が必要な文書や、細かいスケジュールを示すことに焦点を当てたものですが、次の計画表は年間を通して実践すべき事項を記載したものとなっています。

期間	月	年に 1 回	月に 1 回	四半期に 1 回	随時
第 1 四半期	4 月	● 課題に対する活動の検討	● 入退記録の確認 ● 運用チェック	● バックアップされていることの確	● 「関係当局との連絡」体制の見直

			リストによる確認 ● バックアップされていることの確認 ● イベントログの確認 ● 利用者が利用可能なソフトウェアの確認	認 ● イベントログの確認	し ● 法令規制一覧表の確認
	5 月	● リスクアセスメントの実施	同上		
	6 月	● リスク対応のための計画作成（アクションプランの作成） ● 管理策（ルール）の検討	同上		
第 2 四半期	7 月	● 「情報セキュリティリスク対応」計画の実行	同上	同上	
	8 月	● ISMS の有効性の評価 ● 情報セキュリティパフォーマンス	同上		
	9 月	● 資産目録の見直し ● 情報の分類 ● アクセス権限の見直し	同上		
第 3 四半期	10 月	● システム開発の外部委託先の再審査	同上	同上	
	11 月	● 情報セキュリティ計画 ● 情報セキュリティ継続の検証・レビュー	同上		
	12 月	● 内部監査計画 ● 内部監査の実施 ● マネジメントレビュー ● 不適合及び是正処置のレビュー	同上		
第 4 四	1 月	● 主要メンバーの「力量」の評	同上	同上	

半期		価・証拠の文書化 ● 定期教育 ● UPS のバッテリーの確認			
	2 月	● 外部審査（審査機関による更新審査）の実施	同上		
	3 月	● 情報セキュリティのための方針群のレビュー ● 秘密保持契約書の確認	同上		

8.2 情報セキュリティリスクアセスメント

追記する文書	● リスクアセスメント結果報告書

リスクアセスメントを実施する際は、結果を「リスクアセスメント結果報告書」に追記します。

リスクアセスメント結果報告書の追記方法

リスクアセスメント結果報告書の「対応」の箇所に、管理策の実施状況を記載します。

「13-2-4. ISMS：6.計画」を参照してください。

8.3 情報セキュリティリスク対応

追記する文書	● リスク対応計画

リスク対応を実施する際は、結果を「リスク対応計画」に追記します。

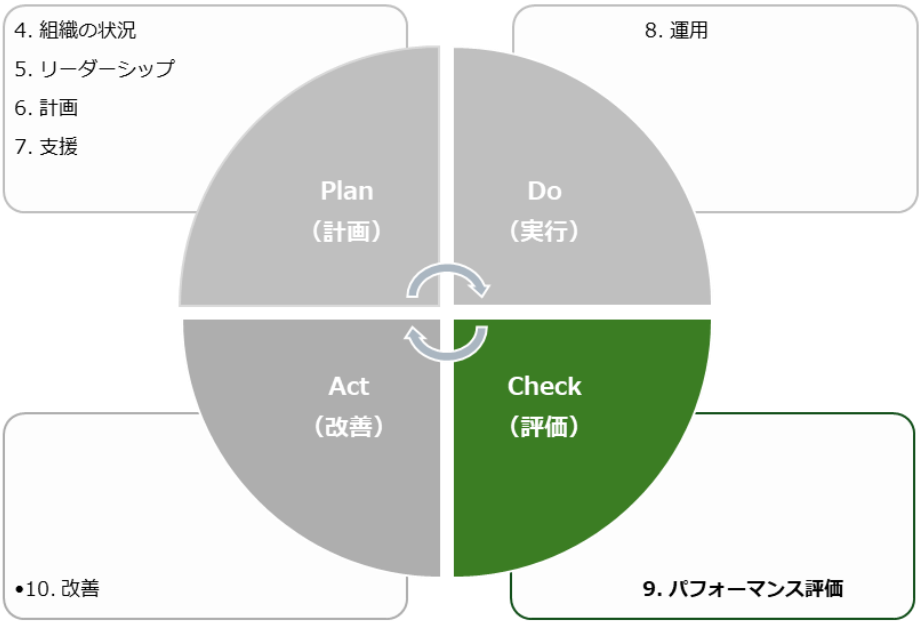
リスク対応計画の追記方法

リスク対応計画の「実績」、「ステータス」の箇所に記載します。

「13-2-4. ISMS：6.計画」を参照してください。

13-2-7. ISMS：9. パフォーマンス評価

「9. パフォーマンス評価」は、PDCA サイクルの「Check（評価）」に位置しており、定めた情報セキュリティ目標を達成するための取組（構築した ISMS）が有効であるか否かを評価します。



パフォーマンス評価	作成文書（例）
9.1 監視、測定、分析及び評価 情報セキュリティのパフォーマンスと、ISMS の有効性を評価します。	● ISMS 有効性評価表
9.2 内部監査 ISMS の適合性、有効性について、あらかじめ定めた間隔で監査を実施します。	● 内部監査チェックリスト ● 内部監査計画書 ● 内部監査結果報告書
9.3 マネジメントレビュー トップマネジメントが、ISMS の有効性を評価します。	● マネジメントレビュー報告書

9.1 監視、測定、分析及び評価

作成する文書	● ISMS 有効性評価表

ISMS の効果について判断するために、有効性評価を実施します。ISMS に沿って実施している活動が、情報セキュリティ目標の達成に繋がっているのか、有効に作用しているのかを評価し、課題があるのであれば改善することになります。PDCA サイクルによる継続したスパイラルアップによって、改善し続けることが重要です。計画時に定めた評価指標および評価方法により、ISMS が

有効だったか、そうではなかったかを判断します。この有効性の評価は、マネジメントレビューの際にトップマネジメントが実施することが効果的です。

ISMS 有効性評価表に記載する方法は、「13-2-4. ISMS：6. 計画」を参照してください。

9.2 内部監査

作成する文書	● 内部監査チェックリスト ● 内部監査計画書 ● 内部監査結果報告書

内部監査とは、社内のルールや扱っている文書が ISO/IEC 27001 の要求事項を満たしており、従業員などがそのルールを守って仕事をしているか否かをチェックすることです。内部監査結果報告書をもとに、マネジメントレビューで「自社の ISMS はこのままでいいのか」「自社の ISMS のどこに欠陥があり、どう修復しなくてはならないのか」を経営層が判断し、随時対策をとります。内部監査は一般的に以下のプロセスで進めます。

1. 内部監査員の選定

内部監査とは、組織内部において、専門的知識を持った人が、経営者や役員などの立場にない第三者として、ISMS が適切に構築され、適正に運用されているか否かを評価することです。内部監査員には、監査の公正さや客観性の観点から、監査対象となる部門に所属していない者を任命する必要があります。内部監査員に資格などは不要ですが、下記に当てはまるような人が適任です。社内に適した者がいない場合は、研修により内部監査員を育成したり、外部の専門家へ依頼したりするといった手段をとることが有効です。

- ISMS の内容を理解している人
- ISMS の内部監査の体制や実施方法といった手順に関する知識を有している人
- 自社の ISMS を把握している人
- 監査対象となる部署の業務内容を把握している人

2. 内部監査チェックリストの作成

内部監査員がチェックリストを作成します。事前にチェックリストを作成することにより、監査するべき範囲やポイントが明確になったり、チェック漏れを減らせたり、内部監査員ごとの偏った評価を防止したりといった効果が期待できます。また、チェックリストは内部監査を行った文書記録とすることができます。

内部監査チェックリストの作成方法（例）

ISMS の項目に沿ってチェック事項をまとめ、内部監査を実施の際には確認した ISMS の根拠となる確認結果や文書類を記録します。

監査項目	チェック事項	確認結果・文書類
4. 組織の状況		
4.1 組織及びその状況の理解	組織は、組織の目的に関連し、かつ、その ISMS の意図した成果を達成する組織の能力に影響を与える、外部および内部の課題を決定しているか。	外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解	次の事項を決定したか。 a）ISMS に関連する利害関係者 b）その利害関係者の、情報セキュリティに関連する要求事項	外部および内部の課題
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	ISMS の適用範囲は、文書化されているか。	ISMS マニュアル ISMS 適用範囲 レイアウト図 ネットワーク図
5. リーダーシップ		
5.1 リーダージップ及びコミットメント	トップマネジメントは、 a）情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしているか。	情報セキュリティ方針 質問で確認
5.2 方針	情報セキュリティ方針は、 e）文書化した情報として利用可能であるか。	情報セキュリティ方針

事前に作成する部分　　**監査時に記載する部分**

3. 内部監査の計画立案

内部監査の計画を立てます。いつ、誰が、どの部門の誰に、何についてチェックするか、といったことを事前に段取りしておきます。

内部監査計画書の作成方法（例）

監査概要	
監査名称	ISO27001 認証取得に関する内部監査
監査目的	ISO/IEC27001:2022 認証取得に向けた当社 ISMS の整備、運用状況を確認
監査テーマ	● 管理策の運用状況、および有効性の確認 ● 第一段階審査の指摘に対する改善状況の確認
監査方法	被監査部門に対するヒアリング、文書化された情報の閲覧、およびオフィスの視察
監査基準	JISQ27001:2022（ISO/IEC27001:2022）の要求事項、当社 ISMS マニュアル、および情報セキュリティ手順書

詳細監査計画				
No	被監査部門名	監査人	応対者	日時
1	情報システム部	○○　○○	△△　△△	20XX/-/- 00:00
2	管理部	○○　○○	△△　△△	20XX/-/- 00:00
3	営業部	○○　○○	△△　△△	20XX/-/- 00:00
4	総務部	○○　○○	△△　△△	20XX/-/- 00:00

内部監査結果報告（予定）	
報告予定日	20XX 年○月
報告手段	報告会の開催

監査概要	監査の名称、目的、テーマ、方法、基準を記載します。
詳細監査計画	監査の対象となる部門名、監査人名、監査への対応者名、監査実施の日時といった予定を記載します。
内部監査結果報告（予定）	監査結果の報告予定日と報告手段を記載します。

4. 内部監査の実施

内部監査計画に沿って、内部監査チェックリストを用いて監査を実施します。

5. 内部監査結果報告書の作成

内部監査の結果をとりまとめ、報告書を作成します。どの部署で、どのルールが守られなかったかといったことを明確にしておきます。内部監査結果報告書をもとに、経営層は自社の ISMS をどのようにするか判断することになるため、内容に不明瞭な点や不足があると、適切な見直しができなくなってしまうため、注意が必要です。

内部監査結果報告書の作成方法（例）

監査名称	ISO27001 認証取得に関する内部監査

<table>
<tr><td>監査実施日時</td><td colspan="3">20XX 年-月</td></tr>
<tr><td>監査目的</td><td colspan="3">ISO/IEC27001:2022 認証取得に向けた当社 ISMS の整備状況を確認</td></tr>
<tr><td colspan="4">監査体制</td></tr>
<tr><td>被監査部門①</td><td>情報システム部</td><td>監査人①</td><td>【名前】/【社名】</td></tr>
<tr><td>被監査部門②</td><td>管理部</td><td>監査人②</td><td></td></tr>
<tr><td>被監査部門③</td><td>営業部</td><td>監査人③</td><td></td></tr>
<tr><td>被監査部門④</td><td>総務部</td><td>監査人④</td><td></td></tr>
<tr><td rowspan="6">監査総評</td><td colspan="3">ISMS の整備状況を確認
当組織での ISMS は、ISO27001:2022 規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されなかった。全体として適切となる有効な仕組みにより運用を開始したと判断できる。
また社員の周知に関しては、ISMS 教育の実施などにより体制や方針などの周知を行っていた。
不適合・観察事項
一部ではあるが、対応が十分でない事項があったため○件を軽微な不適合、○件を観察事項とした。重大な不適合は、検出されなかった。

【軽微な不適合】</td></tr>
<tr><td>No</td><td>規格</td><td>内容</td></tr>
<tr><td>1</td><td>5.2 方針</td><td>規格では「情報セキュリティ方針は、次の事項を満たさなければならない。g）必要に応じて、利害関係者が入手可能である。」としている。しかし、「情報セキュリティ方針」について、お客様などの利害関係者が入手可能であることを確認できなかった。</td></tr>
<tr><td colspan="3">【観察事項】</td></tr>
<tr><td>No</td><td>規格</td><td>内容</td></tr>
<tr><td>1</td><td>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</td><td>ISMS マニュアルとネットワーク図で適用範囲の表現が同じであることの確認が難しい状況でした。ISMS マニュアルでは、ルータまで。ネットワーク図では、ONU まで。</td></tr>
<tr><td>2</td><td>7.3 認識</td><td>実施中の ISMS 教育の終了をお願いします。</td></tr>
<tr><td>備考
（フォローアップなど）</td><td colspan="3">次回の内部監査にて対応のフォローを行う</td></tr>
</table>

9.3 マネジメントレビュー

作成する文書	● マネジメントレビュー報告書

マネジメントレビューとは、経営者（トップマネジメント）が行うレビュー活動です。トップマネジメントは、内部監査の結果や利害関係者からのフィードバックをもとに、組織の ISMS が適切に運用されているか否かを判断し、必要に応じて改善方法を指示します。この活動は、少なくとも年に 1 回定期的に実施することが求められています。トップマネジメントに報告した内容（インプット）と、トップマネジメントの指示や提案（アウトプット）を文書化したものが、マネジメントレビュー報告書です。

インプット、アウトプットに含める必要がある内容は以下の通りです。

インプットに含める必要がある事項
1. 前回までの指示事項に対する処置の進捗や結果 トップマネジメントから前回指示された改善活動の進捗状況や結果を記載します。初回の場合は記載しません。
2. ISMS に関連する外部および内部の課題の変化 事業の変化、法規制の改正など、昨年と比べた外部および内部の課題の変化について記載します。
3. ISMS に関連する利害関係者のニーズおよび期待の変化 「顧客や取引先、従業員、株主など利害関係者からの情報セキュリティに関する要求」の変化について記載します。
4. 情報セキュリティパフォーマンスの実績報告 以下の内容について、報告します。 ● 不適合および是正処置 ➢ 不適合に対する是正処置の実施状況を報告します。 ● 監視および測定の結果 ➢ 情報セキュリティパフォーマンスや、ISMS の有効性についての監視、測定結果を報告します。 ● 監査結果 ➢ 内部監査の結果を報告します。 ● 情報セキュリティ目的の達成

- 情報セキュリティ目的の達成数や未達成数など、情報セキュリティ目的の達成状況を報告します。

5. 利害関係者からのフィードバック

利害関係者から、情報セキュリティに関する要望などについて、対応した結果を報告します。

6. リスクアセスメントの結果およびリスク対応計画の状況

リスクアセスメントにより、新しく特定したリスクや、リスク対応計画の進捗状況を報告します。

7. 継続的改善の機会

トップマネジメントに改善策を提案します。

アウトプットに含める必要がある事項

1. 継続的改善の機会

改善すべき内容について指示を記載します。

2. ISMS のあらゆる変更の必要性

ISMS に関して、次年度以降変更すべき内容について指示を記載します。

マネジメントレビュー報告書の作成方法（例）

出席者	トップマネジメント	【名前】	**日時**	20XX 年〇月
	情報セキュリティ委員長	【名前】		
	ISMS 内部監査責任者	【名前】		00：00～00：00

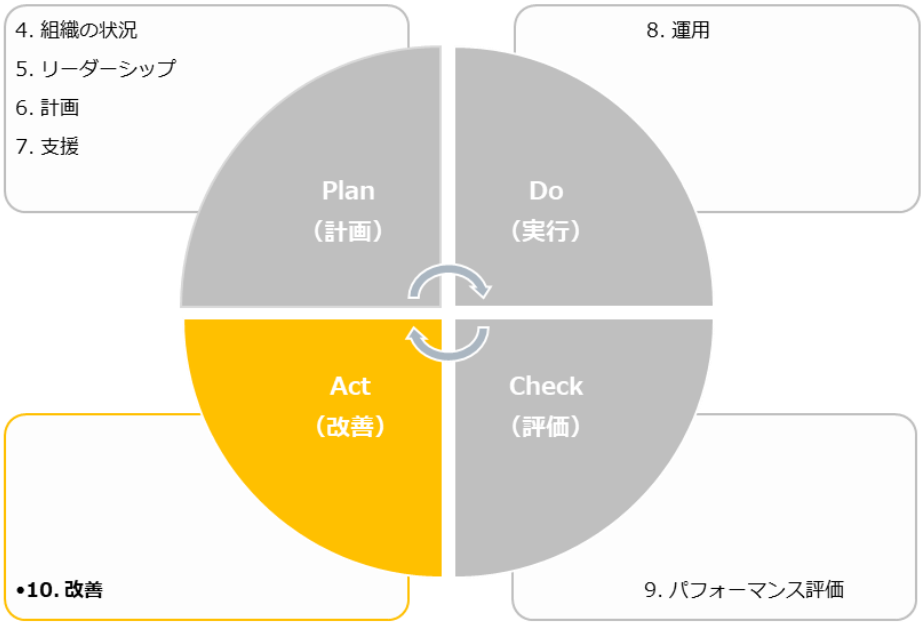
インプット（報告事項）			
1	前回までの指示事項に対する処置の進捗や結果	初回マネジメントレビューのためありません。	
2	ISMS に関連する外部および内部の課題の変化	「外部および内部の課題」にて報告の通りです。 その後、課題の変化は発生しておりません。	
3	ISMS に関連する利害関係者のニーズおよび期待の変化	お客様からの情報セキュリティに関する要求の変化はありませんでした。	
4	情報セキュリティパフォーマンスの実績報告	1）不適合および是正処置	20XX 年〇月に実施した初回の内部監査により検出された“観察事項”1 件は、是正対応中です。 今月末までに対応を予定しています。 そのほか現在対応中の不適合はありません。
		2）監視および測定の結果	次回のマネジメントレビューにて測定結果を報告します。

		3）監査結果	【内部監査】 20XX 年〇月に 1 回目の内部監査を実施し、主に ISMS の文書類整備状況の確認を行いました。 ①ISO27001 規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されませんでした。全体として適切な仕組みにより運用を開始したと判断します。 ②一部ではありますが、対応が十分でない事項があり、観察事項 1 件が検出されました。 詳細は、「内部監査結果報告書」（20XX 年〇月）にて報告の通りです。
		4）情報セキュリティ目的の達成	次回のマネジメントレビューにて報告します。
5	利害関係者からのフィードバック	お客様からのクレームは現状ありませんでした。	
6	リスクアセスメントの結果およびリスク対応計画の状況	【リスクアセスメントの状況】 「情報リスクアセスメント結果報告書」（20XX 年〇〇月〇〇日）にて報告の通りです。 【リスク対応計画の状況】 ● リスク対応計画にリストアップした管理策：〇件 ● 対応が終了した管理策：〇件 ● 対応が終了していない管理策 2 件は以下の通りです。 ※詳細は、「リスク対応計画」（作成：20XX 年〇〇月〇〇日、見直：20XX 年〇月）にて報告の通りです。	
7	継続的改善の機会	現状は ISMS を従業者が理解するための活動を主として行っています。	
アウトプット（トップマネジメントの指示事項）			
1	継続的改善の機会	現状認識している各課題を確実に実施すること。	
2	ISMS のあらゆる変更の必要性	コンサルタント会社のひな形にとらわれず、より当社の状況を反映した仕組み・ルールに見直しを行っていくこと。	

13-2-8. ISMS：10. 改善

「10. 改善」は、PDCA サイクルの「Act（改善）」に位置しており、ISMS の改善を行います。

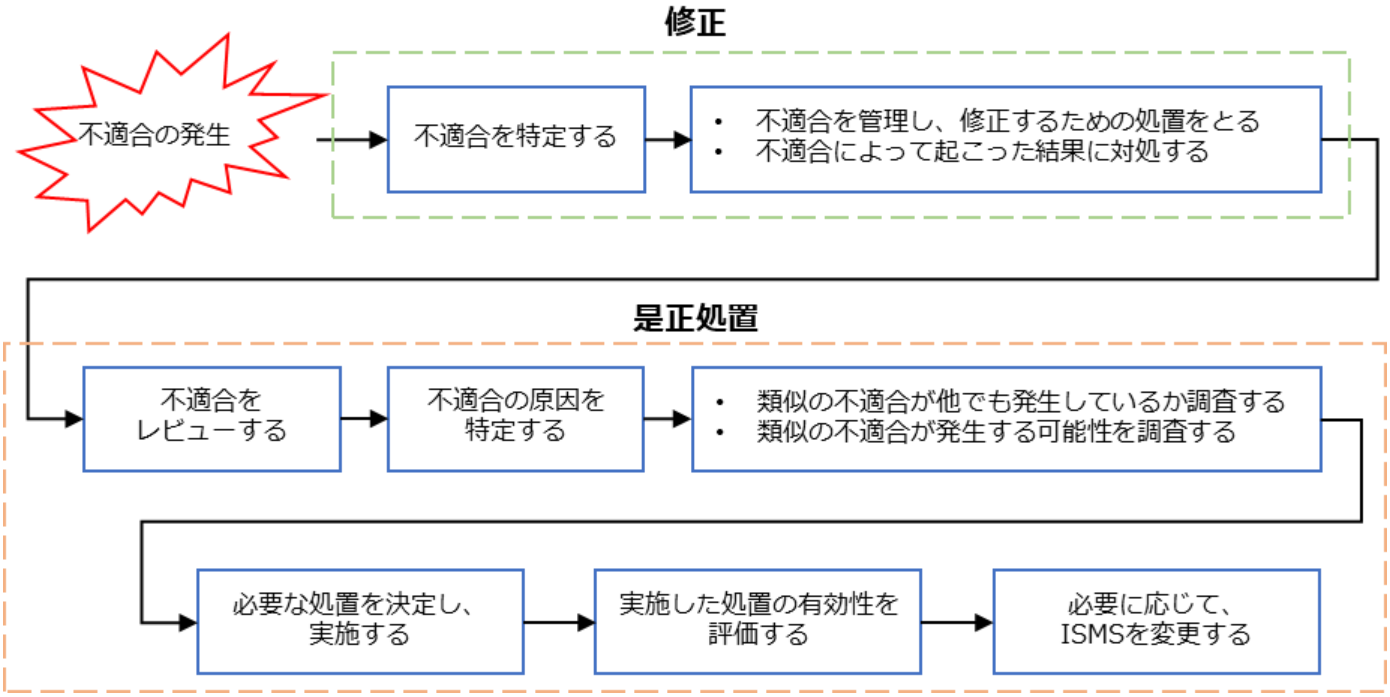
10. 改善	作成文書（例）
10.1 継続的改善 ISMS の PDCA サイクル（「4. 組織の状況」から「10. 改善」までの活動）を継続して実施し、情報セキュリティパフォーマンスを向上させるために必要となる改善を行っていきます。具体的には、情報セキュリティ方針や情報セキュリティ目的の計画、リスクアセスメントやリスク対応をもとに決定した管理策の実施を継続して行い、改善していきます。	―
10.2 不適合及び是正処置 不適合が発生した際に是正処置を実施します。不適合とは、ISMS の要求事項を満たしていないことです。具体的には、管理策の不備や未実施、セキュリティインシデントの発生などのことです。	● 是正要求書兼回答書



10.2 不適合及び是正処置

作成する文書	● 是正要求書兼回答書

審査で ISMS に不適合が検出された場合は、是正処置をしなければなりません。是正処置とは、不適合について、その原因を取り除き、再発防止を図る処置を指します。是正処置は以下の図に示したようなプロセスにより実施されます。



「不適合の性質および講じた処置」と「是正処置の結果」について、文書化した情報を残さなければなりません。そのため、内部監査で不適合が出た際は、是正要求書とその回答書を記載して保存することになります。

是正要求書兼回答書の作成方法（例）

前ページで説明した「不適合の性質および講じた処置」と「是正処置の結果」についての内容を記載します。

整理番号			00-00	対象部門	○○○○部門	発効日	20XX 年 - 月 - 日
入力情報	分類	監査	■	内部監査における指摘事項			
			□	外部機関が実施した監査における指摘事項（機関名：　　）			
			監査年月日	年 月 日		監査者	
			指摘のランク	観察事項		要求事項項番	7.2 力量
		監	□	セキュリティインシデントの関連した改善事項			

			□	外部の利害関係者からのニーズに基づく改善事項										
			□	内部において提案された改善事項										
			□	その他（　　）										
	内容	一部情報セキュリティ委員会担当者が仮任命のため、今後本任命を行っていく。											承認	作成
処置計画	修正	力量の確認。任命力量確認表の更新。												
		実施予定日		年		月		日						
	評価	類似の不適合の有無			無		発生する可能性		無					
		原因	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。											
		原因を除去するための計画の必要性			有		※有の場合原因除去の計画を記載							
	原因除去	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。											承認	作成
		実施予定日		年		月		日						
実施報告	内容	上記の通り、「ISMS 年間計画表」を修正し、運用チェックリストによる点検を実施した。											承認	作成
		実施完了日		年		月		日						
処置確認	確認	「ISMS 年間計画表」の修正、運用チェックリストによる点検記録を確認した。											承認	作成
		確認日		年		月		日						
	有効性	セキュリティ手順の実行、および技術的順守について、点検漏れのリスクが低減された。												
		評価日		年		月		日	フォロー監査の要・不要					

13-3. ISMS 文書体系（ISMS 構築・導入に必要な文書と記録）

13-3-1. ISMS 文書としての策定内容とポイント

対策基準を策定する際は、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するとよいでしょう。ただし、組織が対策基準を策定する際は、組織の業態や規模によって必要となる管理策は異なるので、取捨選択することが必要です。ISO/IEC 27001:2022 の附属書 A や ISO/IEC 27002:2022 は網羅的に管理策がリストアップされているので、自組織に必要のない管理策が含まれています。またその一方、このリストにない管理策が必要となるケースもあることに注意が必要です。自組織におけるサイバーセキュリティリスクを自ら考えて必要な管理策を選択するために、リスクアセスメントの手法を使用し、対策基準を策定します。

ISO/IEC 27001:2022 附属書 A の管理策		
カテゴリ	項目数（合計 93）	概要
組織的管理策	37	組織として取り組む必要のある管理策。例えば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取り組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。例えば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

対策基準策定時の注意点

ISMS の認証取得を目標にして情報セキュリティ対策を進めると、文書の整備が目的になり、本来の情報セキュリティ対策がおざなりになってしまい、ISMS が形骸化するケースが少なくありません。策定した管理策が継続的に実行されていくことが重要となります。
組織は、情報セキュリティリスクを適切にコントロールするために必要となる管理策の有効性を検討し、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
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

13-3-2. ISMS の要求事項および管理策

ISO/IEC 27001 の要求事項

ISO/IEC 27001 では、組織が効率的に ISMS の構築・実施・維持・継続的改善を行うとともに、情報セキュリティのリスクアセスメントおよびリスク対応を実現するために必要な要求事項を定めています。ISO/IEC 27001 の要求事項は、ISMS 認証を取得するには必ず対応しなければなりません。どのような内容が要求されているのか認識するため、各要求事項の概要について説明します。要求事項は、後述の PDCA サイクルと呼ばれる運用サイクルに落とし込むことにより、情報セキュリティマネジメントを実施することになります。

ISMS の運用プロセス

マネジメントシステムとは、組織の方針や目標を定めて、その目標を達成するために必要な、組織を管理する仕組みのことを指します。情報セキュリティのマネジメントシステムである ISMS も、組織によって定めた目標達成のための取組です。その目標は、情報セキュリティに関することや、会社が抱えている機密情報をどう保護していくのかという内容となります。その目標に向かってマネジメントを行っていくための方法として、要求事項を実施しながら、PDCA（Plan・Do・Check・Act）サイクルを繰り返し、スパイラルアップしていくことが、ISO/IEC 27001 では求められています。

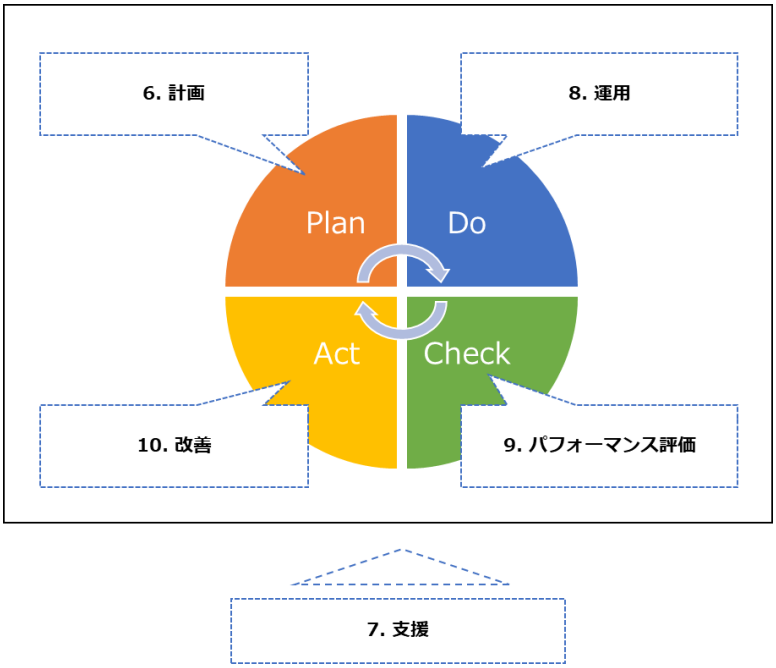


図 56. ISO/IEC 27001 の PDCA サイクル

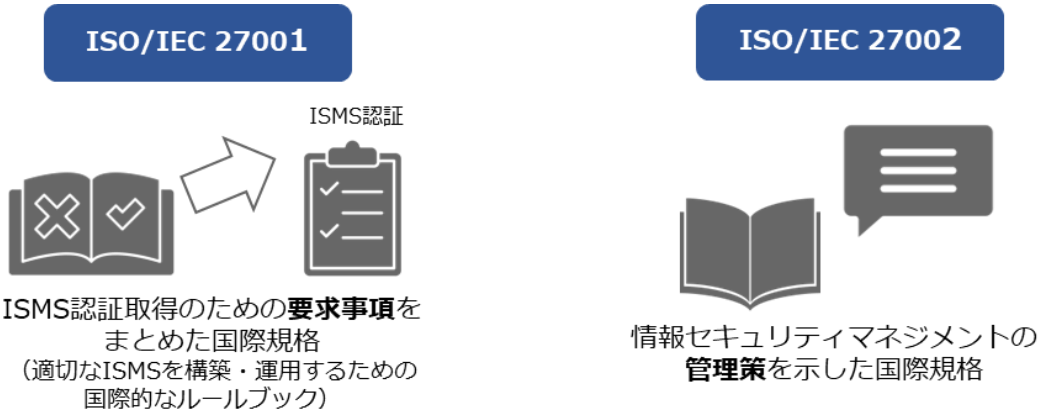
ISMS の管理策

ISO/IEC 27001 に記載されている要求事項をもとに、具体的な情報セキュリティマネジメントの管理策を示した規格として ISO/IEC 27002 があります。ISO/IEC 27001 の付属書 A は、この ISO/IEC 27002 の内容をそのまま取り入れたもので、情報セキュリティ上のリスクを低減するた

めの目的と、その目的を達成するための管理策で構成されています。

付属書 A は、ISMS の本文（ISO/IEC 27001 の規格要求事項）を補完するガイドラインとしての位置づけにあります。業務内容や ISMS の適用範囲によってはすべての管理策を適用することができない場合があり、その際には、適用できない理由を明確にし、採用しないという選択をすることができます。つまり、一律にすべての管理策を適用するのではなく、理由を含めて採用しない管理策を明示する必要があります。

ISO/IEC 27002 では、合計 93 種の管理策が「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る形で解説されています。



情報セキュリティ管理策		
カテゴリ	項目数	概要
組織的管理策	37	組織として取り組む必要のある管理策。例えば、情報セキュリティの方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取り組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。例えば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的対策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

ISO/IEC 27002 の箇条 5～8 は、93 種の ISMS 管理策で構成されています。以下の表は、それらの管理策標題の一覧です。詳細については「（別紙）ISO/IEC 27002:2022 管理策と目的」をご

確認ください。

組織的管理策	
5.1 情報セキュリティのための方針群	5.19 供給者関係における情報セキュリティ
5.2 情報セキュリティの役割及び責任	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
5.3 職務の分離	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
5.4 経営陣の責任	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
5.5 関係当局との連絡	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
5.6 専門組織との連絡	5.24 情報セキュリティインシデント管理の計画及び準備
5.7 脅威インテリジェンス	5.25 情報セキュリティ事象の評価及び決定
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	5.26 情報セキュリティインシデントへの対応
5.9 情報及びその他の関連資産の目録	5.27 情報セキュリティインシデントからの学習
5.10 情報及びその他の関連資産の利用の許容範囲	5.28 証拠の収集
5.11 資産の返却	5.29 事業の中断・阻害時の情報セキュリティ
5.12 情報の分類	5.30 事業継続のための ICT の備え
5.13 情報のラベル付け	5.31 法令，規制及び契約上の要求事項
5.14 情報転送	5.32 知的財産権
5.15 アクセス制御	5.33 記録の保護
5.16 識別情報の管理	5.34 プライバシー及び PII の保護
5.17 認証情報	5.35 情報セキュリティの独立したレビュー
5.18 アクセス権	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
	5.37 操作手順書

6.人的管理策	
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

7.物理的管理策	
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

8.技術的管理策	
8.1 利用者終端装置	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

ISMS の管理策における属性

ISO/IEC 27002 では、2022 年の改訂より「属性」という考え方が新たに追加されました。この「属性」についての各管理策としては「予防（preventive）」、「検知（detective）」、「是正（corrective）」のいずれかに分類され、またその特性によって「機密性」、「完全性」、「可用性」のいずれかに関連付けられています。さらに、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という 3 つの観点からも属性のグループ分けが行われています。「属性」という考え方が追加された結果、各管理策をより柔軟かつさまざまな場面に採用できるようになりました。

この「属性」という考え方は、他の組織や団体が発行するガイドラインなどとの親和性を高める効果も期待できます。例えば、「サイバーセキュリティ概念」では「識別、防御、検知、対応、復旧」という 5 つの属性値が示されていますが、これは米国国立標準研究所（NIST）が発行している CSF（サイバーセキュリティフレームワーク）でも採用されているものです。また、組織は自らの視点を作るために、独自の属性を作ることも可能です。

管理策タイプ
情報セキュリティインシデントの発生との関係において、リスクをいつどのように修正するかという観点から管理策を見る属性 ［属性値］予防、検知、是正
情報セキュリティ特性
情報のどの特性の維持に寄与するかという観点から管理策を見る属性 ［属性値］機密性、完全性、可用性
サイバーセキュリティ概念
ISO/IEC TS 27119 に記述されているサイバーセキュリティフレームワークで定義された、サイバーセキュリティ概念との関連付けの観点から管理策を見る属性 ［属性値］識別、防御、検知、対応、復旧
運用機能
実践者の情報セキュリティ機能の観点から管理策を見る属性 ［属性値］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
情報セキュリティドメインの観点から管理策を見る属性 ［属性値］ガバナンスおよびエコシステム、保護、防御、対応力

13-4. ISO/IEC27001 の審査準備と審査内容

13-4-1. ISO/IEC27001 の認証機関の選定と申し込み

認証取得の申請先

組織が ISO/IEC 27001 の認証を取得するためには、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）から認定された認証機関からの審査を受け、認証基準に適合していると認められる必要があります。

ISO/IEC27001（ISMS）における「認証」と「認定」は似た用語ですが、英語では”certification”と”accreditation”で異なる意味を持つ用語です。「認証」は組織の情報セキュリティマネジメントシステムが ISO 27001 の規格に適合していることを公的機関が証明することです。一方、「認定」は、審査機関が十分な審査能力をもち、かつ公平な審査が行われていることを証明する仕組みです。日本では ISMS-AC が ISMS の認証機関を認定しています。

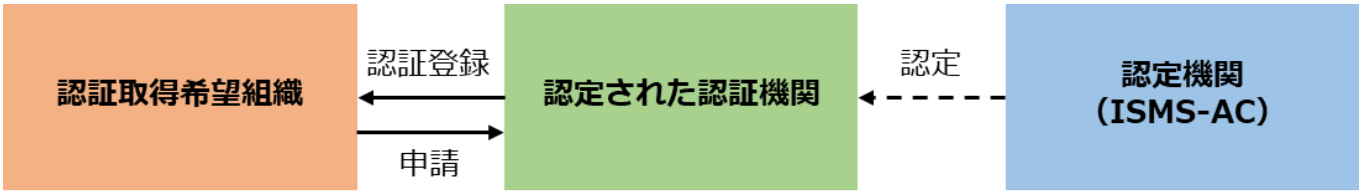


図 57. 認証取得の申請先

（出典）JIPDEC「ISMS/ITSMS/BCMS/CSMS 認証を取得するには」をもとに作成

認証機関の選択

認証取得を希望する組織は認定された認証機関の中から選んで申請します。

認定された認証機関は、ISMS-AC の Web ページに掲載されています。

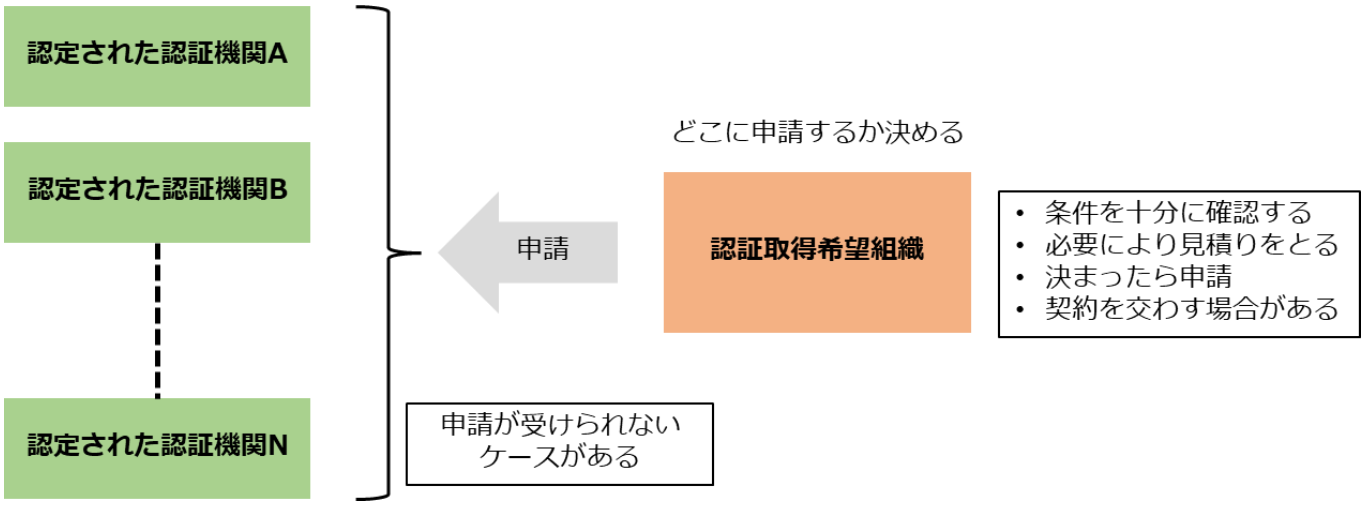


図 58. 認証機関の選択

（出典）JIPDEC「ISMS/ITSMS/BCMS/CSMS 認証を取得するには」をもとに作成

認定された認証機関は、業種による制限はありませんので、どの業種の組織でも審査することが

できます。しかし、審査において業種特有な専門的知識が必要な場合は、認証機関として審査を受付けない場合がありますので、事前に確認することが大切です。また、利害が絡む場合などでは審査を受付けられない場合があります。

認証機関を選択したら、認証審査・登録に関する条件について事前に確認し、合意されたら申請します。

認証登録に関わる料金は、適用範囲や受審組織の規模などの他、認証機関によっても異なります。見積りをとることもできます。

申請に必要な書類や様式などは、認証機関に確認します。

詳細理解のため参考となる文献（参考文献）	
ISMS 認証機関一覧	https://isms.jp/lst/isr/index.html

13-4-2. ISO/IEC27001 の審査事前準備

ISMS の構築

ISO/IEC 27001 に準拠した ISMS を実装するには、どのようなステップが必要なのか解説します。実装に際しては ISO/IEC 27001 の認証審査を受けることになります。そのため、審査対象となる ISMS の構築を実施し、実際の運用状況について記録することになります。

ISMS の構築	
ステップ	**概要**
適用範囲の決定	会社全体だけでなく、特定の部署・拠点のみといったように ISMS の範囲を限定することも可能なため、まずは適用範囲を決定します。
情報セキュリティ方針の策定	ISMS の基本的な指針として、会社の情報セキュリティ方針を策定します。
体制の確立	ISMS 管理責任者、ISMS 推進事務局、ISMS 内部監査チームなど、ISMS の運用体制を決定します。
ISMS 文書化	ISMS を運用・維持するための手順やガイドラインを文書化します。従業員や関係者が理解しやすく、利用・実践しやすい形式により作成することが重要です。
リスクアセスメントの実施	会社が持つ情報資産を洗い出し、それらに想定しうるリスクと対策を決定します。リスク

	アセスメントの結果は記録を作成します。
従業員の教育	ISMS の概要や手順、会社の情報セキュリティ方針について従業員に理解してもらうため、セキュリティ教育を実施します。教育の結果は記録を作成します。
内部監査	ISMS の運用がはじまった後に、定めたルールが適切に運用されているかを確認します。運用が不十分な場合はリスクの指摘やルールの見直しを行い、改善につなげます。内部監査の結果は記録を作成します。
マネジメントレビュー	内部監査の結果をもとに、会社の ISMS についての現状や課題、改善点などを経営陣に報告します。マネジメントレビューの結果は記録を作成します。

13-4-3. ISO/IEC27001 の審査（第一段・第二段）

ISMS 認証と ISMS 適合性評価制度

「ISMS 認証」とは、組織の構築した ISMS が ISO/IEC 27001 に基づいて適切に運用管理されているかを、第三者である ISMS 認証機関が、利害関係のない公平な立場から審査し証明することです。この認証を公正に運用するために、国際的な枠組みが定められており、これを「ISMS 適合性評価制度」と呼んでいます。この適合性評価制度は、以下の図に示したように「認証機関」「認定機関」「要員認証機関」から構成されています。

ISO/IEC 27001 は、ISMS 適合性評価制度において、第三者である認証機関が ISMS 認証を希望する組織の適合性を評価するための基準となります。認証審査においては、組織の ISMS が ISO/IEC27001 の標準に適合しているかが評価されることになります。

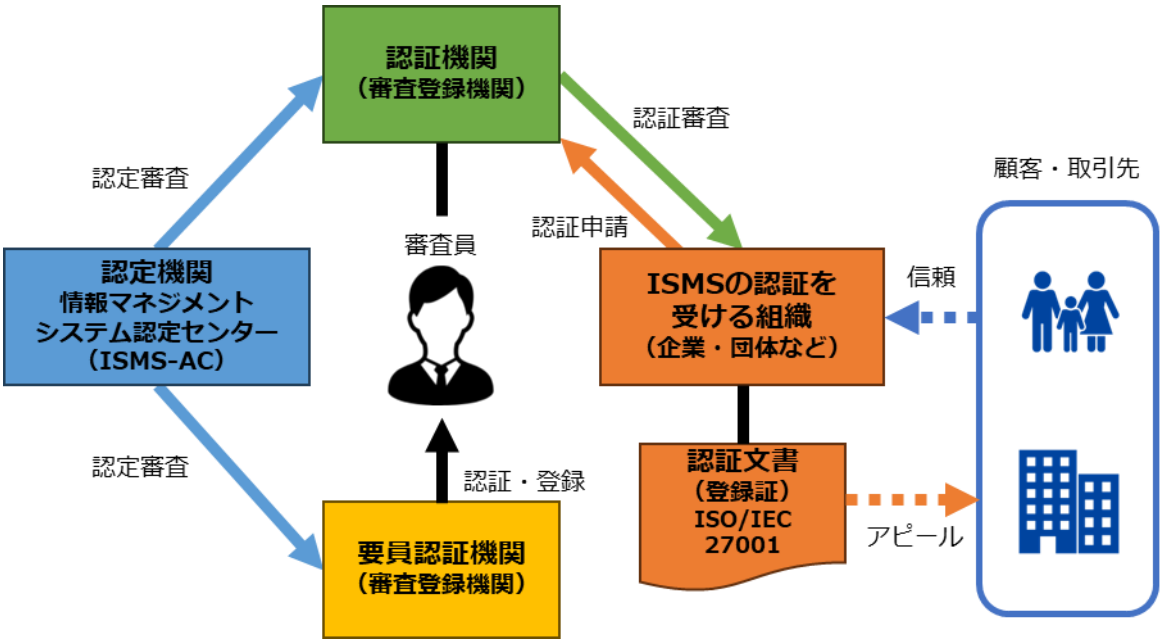


図 59. ISMS 適合性評価制度

（出典）ISMS-AC「ISMS 適合性評価制度」を基に作成

認定と認証

認定	認定機関が認証機関を審査し、認証を遂行する能力のあることを公式に承認する行為を認定といいます。日本における ISMS 適合性評価制度の認定機関は ISMS-AC です。ISMS-AC は、認証機関が適切に審査を実施できる体制・能力を持ち、かつ公正な審査を実施しているかを、国際規格に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けた ISMS 認証機関は、適切な ISMS 認証審査を実施することのできる、信頼のおける認証機関であることを意味します。
認証	第三者が文書で保証する手続きを認証といいます。 マネジメントシステム規格への適合性を保証する場合、認証の代わりに特に他と区別するため「審査登録」という用語を用いることがあります。この場合、認証の対象は、製品、サービスあるいはプロセスではなく、組織のマネジメントシステムそのものとなることに注意が必要です。

（出典）MSQA「ISMS 推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応 1.0 版」を基に作成

ISMS 認証審査プロセス

ISMS の認証審査は、大まかに以下のようなステップで進みます。

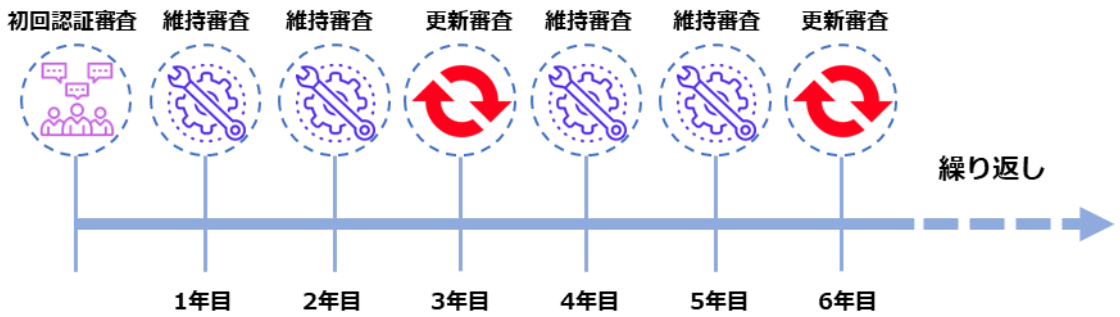
ステップ	申請	審査日程の確認	初回認証審査	認証登録	報告・公開
概要	新規取得する際、今までと異なる認証機関で受審する場合は、申請が必要です。	組織と認証機関との間で、審査日程の確認を行います。	新規の場合は原則として 1 次審査と 2 次審査の 2 回で実施されます。	審査の結果、適合していることが確認されると認証書が発行され、登録完了となります。	認証された旨が認証機関から ISMS-AC に報告され次第、ISMS-AC ホームページ上で公開されます。

なお、審査に要する期間や工数、申請方法、申請時の準備物、認証登録料金などは、認証機関によって異なります。ISMS 認証機関は、情報マネジメントシステム認定センター（ISMS-AC）のホームページで公開されているため、申請先選定の際は確認することが大切です。

13-4-4. ISO/IEC27001 の維持審査・再認証審査

ISMS 認証の維持および更新審査プロセス

ISMS 認証取得後も、維持・更新のための審査があります。年に 1 回以上の維持審査（サーベイランス審査）と、3 年ごとに認証の有効期限を更新するための全面的な審査（再認証審査）です。どちらにおいても、組織の ISMS が引き続き規格に適合し、有効に維持されているかが確認されます。



コラム

ISMS の導入：成功の鍵とよくある落とし穴

組織が顧客データや機密情報などの情報資産を守るためには、適切に情報セキュリティを確保する仕組みが必要となります。そのために、ISMS の導入と運用は重要になります。そこで、ISMS を導入・運用していく際に成功の鍵となるポイントと、陥りやすい失敗例をいくつか紹介します。

成功の鍵となるポイント

- トップマネジメントのコミットメント
  SMS の導入には経営陣からのコミットメントが不可欠です。経営層が情報セキュリティの重要性を理解し、リーダーシップを発揮することにより、組織全体が情報セキュリティの確保に向けて協力的になります。
- 従業員の教育と意識向上
  従業員への教育は、従業員に基本方針や対策基準などを理解させ、策定された実施手順を実践してもらうために重要です。定期的なトレーニングや教育プログラムを通じて、従業員が脅威に対処できるようにサポートしていくことが大切です。
- リスク評価と適切な対応策
  リスク評価を行い、特定のリスクに対して適切な対応策を策定することにより、情報資産の保護と事業の継続性を確保できます。

陥りやすい失敗例

- 実施手順の抽象性
  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。わかりやすい実施手順を策定し、従業員に浸透させることが重要です。
- 不十分な監査と改善の実施
  ISMS の運用において監査と改善を怠ってしまうと、新たな脅威に適応できず、セキュリティ体制が陳腐化してしまいます。定期的な監査と、その結果をもとにした改善活動を継続的に行うことが必要です。

ISMS の導入を成功させるためには、経営層のリーダーシップ、従業員の教育、リスクマネジメントの適切な実施が欠かせません。常に変化するセキュリティ環境に適応する柔軟性や継続的な改善が、組織の情報セキュリティを確保することにつながります。

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

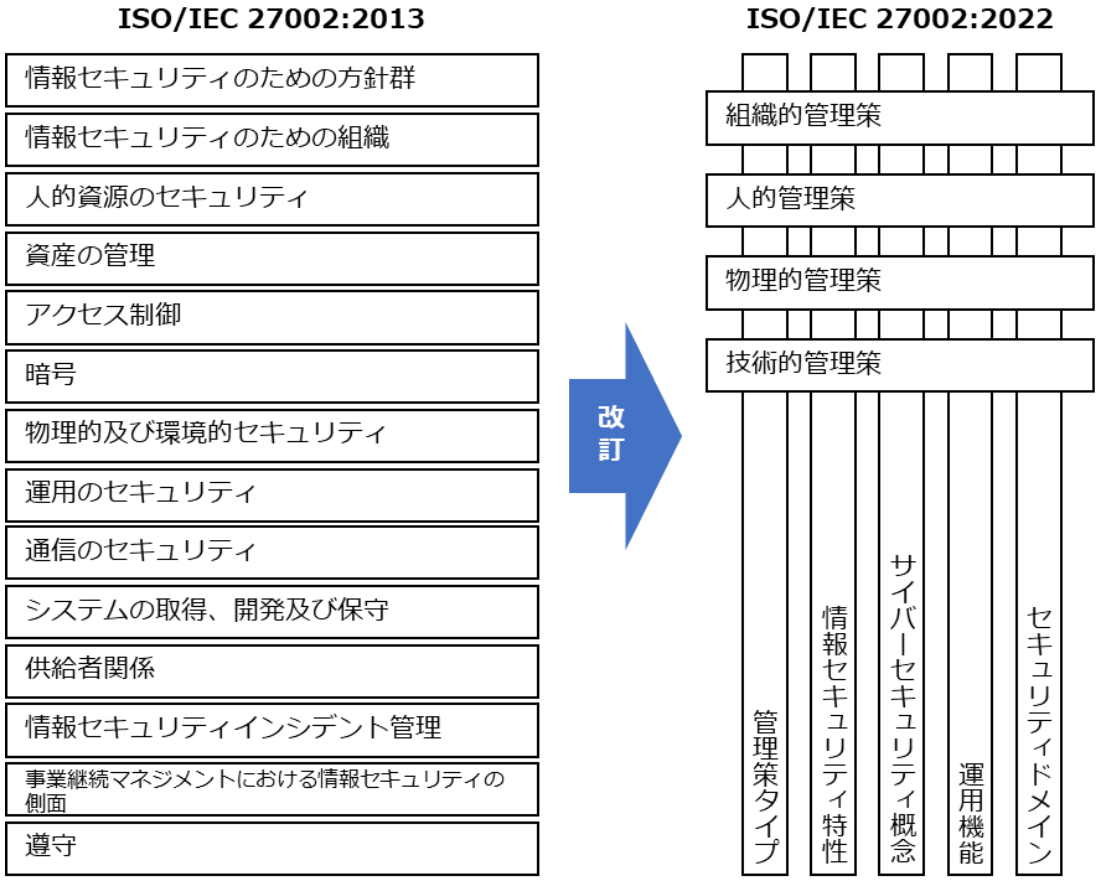
14-1-1. 管理策：ISO/IEC 27002

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。

（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

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。	

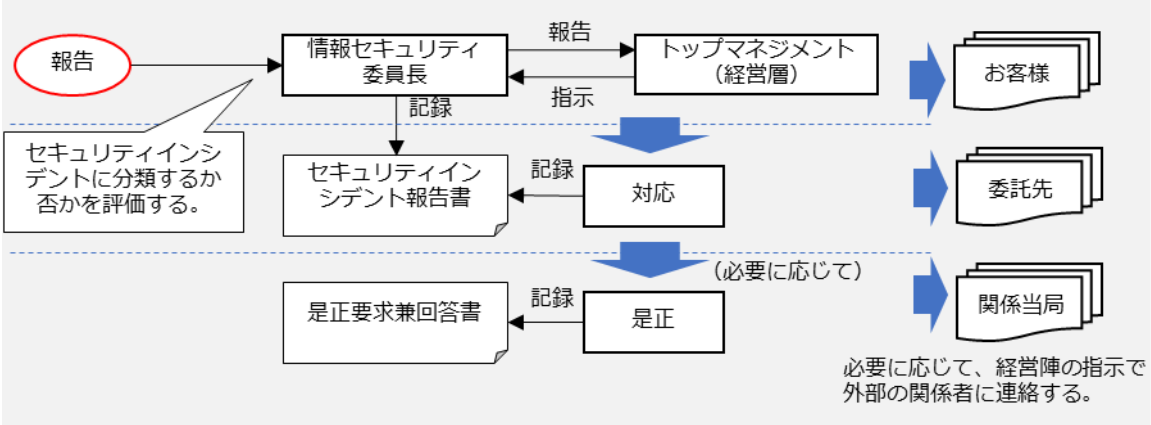
15-2-5. 情報セキュリティインシデント対応

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	社員または社内	顧客・取引先

	る可能性がある。）		
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

引用文献

ISMS/ITSMS/BCMS/CSMS認証を取得するには

https://www.jipdec.or.jp/project/smpo/ninsyou.html

ISMS適合性評価制度

https://isms.jp/isms.html

ISMS 推進マニュアル活用ガイドブック 2022 年 3.0 版

https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd

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

参考文

ISO/IEC 27001:2022

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

ISO/IEC 27002:2022

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

ISMS認証機関一覧

https://isms.jp/lst/isr/index.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/

■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。

13-3-2、15-1、15-2-6、15-2-7

■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。

13-1、13-2-1、13-2-2、13-2-3、13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、13-3-1、13-3-2、13-4-1、13-4-2、13-4-3、13-4-4、14-1-1、14-1-3、15-1

■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

■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。

13-3-2、14-1-2

■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。

13-3-2、15-1、15-2-8

■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

■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

■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。

13-3-2、15-1、15-2-1、15-2-3

■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。

13-3-1、13-3-2、15-2-1、15-2-7

■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。

13-2-6

■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

■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。

13-2-4、13-2-5、13-3-2、14-1-2、15-1、15-2-6、15-2-7

■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。

13-2-4、13-2-5、13-3-2、14-1-2、15-1

■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。

13-2-4、13-2-5、13-3-2、14-1-2、15-1

■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。

13-3-2、15-1、15-1、15-2-2

■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。

13-3-2、13-3-2、14-1-2、15-1、15-2-1、15-2-6、15-2-7、15-2-9

■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。

13-3-2

■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。

13-2-4、13-2-5

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の 調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される。

13-3-2

■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。

13-3-2、15-2-1

■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。

13-2-3、13-2-4、13-2-5、13-4-2、第13章コラム、15-2-6

■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。

13-3-2、14-1-2、15-1、15-2-1、15-2-5

■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。

13-2-5、15-2-7

■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。

13-2-5

■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。

13-3-1、13-3-2、14-1-2、15-2-1

■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。

13-2-2、13-2-4、13-2-5、13-2-8、13-3-2、14-1-2、15-1、15-2-1、15-2-4、15-2-5

■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

■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。

13-3-2

■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

■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。

13-2-3、13-2-6、13-2-7、13-2-8、13-4-2、15-2-1、15-2-9

■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

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている。

13-2-5

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある。

13-2-5

■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

■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

■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。

13-1、14-1-2

■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。

13-2-4、13-3-1、13-3-2、15-2-2、15-2-4

■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

■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

■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。

13-3-2

■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

■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。

13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、13-3-1、13-3-2、13-4-2、14-1-3、15-1、15-2-2

■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。

第13章コラム

東京都産業労働局