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 6 編　　ISMS などのフレームワークの種類と活用法の紹介　【レベル 3】

東京都産業労働局

第11章. セキュリティフレームワーク

章の目的
第 11 章では、ISMS をはじめとしたサイバーセキュリティ対策における代表的なフレームワークを理解し、それぞれの内容について知識を身につけることを目的とします。
主な達成目標
◘ サイバーセキュリティ対策においてフレームワークを活用することの重要性について理解すること ◘ 各フレームワークの目的や必要性などの特徴について理解すること

11-1. セキュリティフレームワークの概要

11-1-1. セキュリティフレームワークの役割と重要性

セキュリティフレームワークの概要およびその利用メリットについて説明します。

セキュリティフレームワークとは
セキュリティ対策を行うために定義された指針やセキュリティ対策基準、ガイドライン、ベストプラクティス集のことを指します。自社におけるセキュリティリスクを評価・管理し、適切なセキュリティ対策を計画、実装、管理するための基盤となります。

セキュリティフレームワークを使用するメリット	
効果的なセキュリティ対策 フレームワークを使用することにより、セキュリティ対策の抜け漏れを防ぎ、効果的かつ適切なセキュリティ対策を行うことが可能となります。	**信頼性の確保** 認証制度が存在するフレームワークの場合、そのフレームワークにしたがってセキュリティ対策を実装し、第三者機関から認証を受けることにより、取引先や顧客からの信頼獲得につながります。

代表的なセキュリティフレームワーク	
ISMS（情報セキュリティマネジメントシステム） **ISO/IEC27001:2022、ISO/IEC 27002:2022** ● 網羅的なセキュリティフレームワーク	
ISO/IEC 27017:2015 ● クラウドサービス	**サイバーセキュリティフレームワーク（CSF）2.0** ● 幅広い組織向け
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver.1.0 ● Society 5.0 における産業社会	**サイバーセキュリティ経営ガイドライン Ver3.0** ● 経営者を中心としたセキュリティ対策
PCI DSS（国際的なクレジット産業向けのデータセキュリティ基準）v4.0.1 ● クレジットカード産業	**個人情報保護マネジメントシステム（PMS）JIS Q 15001:2023 準拠 ver1.0** ● 個人情報保護
CIS Controls version 8.1 ● 具体的なサイバー攻撃アプローチ	**ISA/IEC 62443** ● 産業オートメーションおよび制御システム

フレームワーク使用上のポイント

上記のようにフレームワークは数多くの種類がありますが、まずは業種業態を問わず、セキュリティ対策の全体の枠組みと網羅的な対策項目を提示している ISMS をベースとするとよいでしょう。そして必要に応じて、業種業態や重点領域ごとに特に注力すべき内容が詳細化されている各種フレームワークの内容で補完することが大切です。

11-1-2. フレームワーク選択の重要性

ISMS（情報セキュリティマネジメントシステム） ISO/IEC27001:2022、ISO/IEC 27002:2022
● **網羅的なセキュリティフレームワーク** **発行元：ISO/IEC** 情報の機密性、完全性、可用性を保護するための体系的な仕組みであり、技術的対策に加えて、従業員の教育や訓練、組織体制の整備などが含まれています。必ずしも、組織全体で適用する必要はなく、組織の必要に応じて、適用範囲を決定できるという特徴があります。[1]

ISO/IEC 27017:2015	サイバーセキュリティフレームワーク（CSF）2.0
● **クラウドサービス** **発行元：ISO/IEC** クラウドサービスに関する情報セキュリティ対策を実施するためのガイドライン規格で、ISO/IEC27002 をベースに作成されています。この規格は、クラウドサービスの提供者とクラウドサービスの利用者の両方を対象としています。クラウドサービスに関するリスクの低減や、クラウドサービスを適切に利用する組織体制を確立できます。 また、情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC 27001 の取組を ISO/IEC 27017 で強化することによって、クラウドサービスにも対応した情報セキュリティ管理体制を構築することができます。	● **幅広い組織向け** **発行元：NIST** CSF は、組織がサイバーセキュリティリスクを管理する際の指針を提供するものです。CSF は、組織の規模や業界を問わず（産業界、学術界、政府および非営利組織を含む）組織におけるサイバーセキュリティリスクの管理と低減に役立つよう設計されています。 CSF の下位概念に位置づけられているのが SP800 シリーズ（SP 800-53/SP 800-171/SP 800-161 など）となります。 CSF2.0、SP800 シリーズの内容については後述します。

1 ISMS-AC「ISMS 適合性評価制度」 https://isms.jp/doc/JIP-ISMS120-62.pdf

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver.1.0	サイバーセキュリティ経営ガイドライン Ver3.0
● **Society 5.0 における産業社会** **発行元：経済産業省** ISMS、CSF の概念を包含したフレームワークであり、サイバー空間におけるセキュリティ対策から、サイバー空間とフィジカル空間のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理しています。 Society5.0 を意識したセキュリティリスクとその対策方法について記述されている特徴があります。 リスク源を適切に捉えるために産業社会を 3 層構造と 6 つの構成要素で捉えており、産業界が自らのセキュリティ対策に活用できるよう、対策例がまとめられています。	● **経営者を中心としたセキュリティ対策** **発行元：経済産業省/独立行政法人情報処理推進機構（IPA）** サイバー攻撃の多様化・巧妙化に伴い、サイバー攻撃から企業を守るために必要なことをまとめたガイドラインです。ISMS のフレームワークがベースとなっており、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある 3 原則と、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO など）に指示すべき重要 10 項目をまとめているという特徴があります。[2] サイバー攻撃から企業を守る観点で、“サイバーセキュリティは経営問題”と定義し、経営者を中心とした組織的な対策の見直し・強化を求めています。
PCI DSS（国際的なクレジット産業向けのデータセキュリティ基準）v4.0.1	**個人情報保護マネジメントシステム（PMS）JIS Q 15001:2023 準拠 ver1.0**
● **クレジットカード産業** **発行元：PCI SSC** クレジットカード情報を取扱うすべての事業者に対して国際カードブランド 5 社が共同で策定した、クレジットカードの取扱いにおけるセキュリティの国際基準です（Payment Card Industry Data Security Standard の略）。[3] カード会員情報を適切に管理するため、ネットワークアーキテクチャ、ソフトウェアデザイン、セキュリティマネジメント、ポリシー、プロシジャなどに関する基準が 12 の要件として規定されています。	● **個人情報保護** **発行元：JIPDEC** 組織が業務上取扱う個人情報を安全で適切に管理するための仕組みです。JIS Q 15001 によって要求事項が定められています。この規格は、事業者が個人情報を適切に取扱う方法を規定したもので、プライバシーの保護を直接の目的とはしていません。しかし、意図しない個人情報の取扱いが抑制されることにより、結果的にプライバシーも保護されます。[4] 個人情報保護マネジメントシステム（PMS）の基本的な仕組みは、個人情報保護方針を定め、この方針に基づき「PDCA サイクル」を

2 経済産業省「サイバーセキュリティ経営ガイドラインと支援ツール」 https://www.meti.go.jp/policy/netsecurity/mng_guide.html
3 経済産業省「クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性」 https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf
4 JIPDEC「「個人情報」と「プライバシー」の違い」 https://privacymark.jp/system/course/theme1/03.html

	実行することになります。
CIS Controls version 8.1	**ISA/IEC 62443**
● **具体的なサイバー攻撃アプローチ** **発行元：CIS** サイバー攻撃の現状と傾向を踏まえて、組織が実施すべきサイバーセキュリティ対策とその優先順位を決めるためのフレームワークで、あらゆる企業が取るべき最も基本的で重要な対応に重点を置いています。ネットワークの詳細設定や、ログの管理など、具体的で技術的な対策が中心となっている特徴があります。 多岐にわたる対策の中から、自社（組織）が実施すべき対策と、その優先順位を導くためのアプローチを提示したフレームワークとなります。	● **産業オートメーションおよび制御システム** **発行元：ISA/IEC** 産業用自動制御システム（Industrial Automation and Control Systems）に対するセキュリティ対策とプロセス要件を定めた一連の国際標準規格です。ISO/IEC 27001 などではカバーしきれない、工場やプラントにおける制御システムのセキュリティを網羅的に対象としています。また、セキュリティ確保の対象は、ソフトウェア・ハードウェアを含む制御関連のデータ処理基盤であるシステムに加えて、システムの運用に関わる「人」と「業務」も対象となっている特徴があります。

11-2. 情報セキュリティマネジメントシステム（ISMS）［ISO/IEC27001:2022, 27002:2022］

ISMS とは、情報セキュリティマネジメントシステム（Information Security Management System）の略称で、組織の情報セキュリティリスクを適切に管理するための仕組みのことです。ISMS に関する国際規格がフレームワークとして存在していることから、ISMS はセキュリティフレームワークの中でも代表的なものとなっています。ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性および可用性をバランスよく維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにあります。[5]また、ISMS には技術的対策に加えて、従業員の教育・訓練、組織体制の整備なども含まれます。

情報セキュリティの 3 要素

機密性（Confidentiality）
権限のない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しないこと（情報に対するアクセスを適切に管理すること）

完全性（Integrity）
情報が正確であり、完全である状態を保持すること

可用性（Availability）
情報を必要なときに使えるようにしておくこと

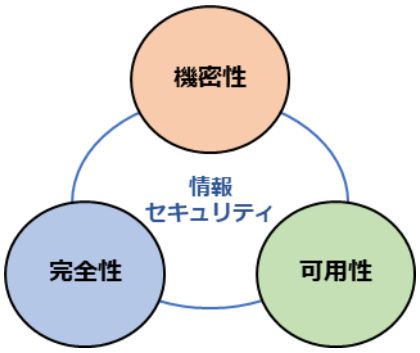


図 37. 情報セキュリティの 3 要素
（出典）ISMS-AC「ISMS 適合性評価制度」をもとに作成

One Point

情報セキュリティの 7 要素
情報セキュリティには、上記で紹介した 3 要素に加えて、「真正性（Authenticity）」「信頼性（Reliability）」「責任追跡性（Accountability）」「否認防止（non-repudiation）」という 4 つの拡張要素があります。これらは、情報にアクセスする人が本当にアクセスするべき人であるかを担保することや、システムが確実に目的の動作をすること、誰がどのような手順で情報にアクセスしたかを追跡できるようにすること、また、情報が後から否定されない状況を作ることにより情報セキュリティを確保するものです。

ISMS のための要求事項をまとめた国際規格が、ISO/IEC 27001 です。組織が ISMS を確立し、実施し、維持し、継続的に改善するための要求事項の提供を目的として作成されています。ISMS

5 ISMS-AC「ISMS とは」 https://isms.jp/isms/

の確立および実施について、組織の行うべき事項が項目ごとに記述されたものとなっており、この規格は以下のために用いることができます。[6]

組織のマネジメントおよび業務プロセスを取り巻くリスクの変化への対応

JIS Q 27001（ISO/IEC 27001）では、組織は、自らのニーズおよび目的、情報セキュリティ要求事項、組織が用いているプロセス、並びに組織の規模および構造を考慮して、ISMS の確立および実施を行います。これは、多くの情報を取扱うようになっている、現代の組織のマネジメントおよび業務プロセスを取り巻くリスクの変化に対応できるように、組織基盤を構築する抜本的な業務改革をする目的に適しています。

情報セキュリティ要求事項を満たす組織の能力を内外で評価するための基準

JIS Q 27001（ISO/IEC 27001）は、情報セキュリティ要求事項を満たす組織の能力を、パフォーマンス評価および内部監査などにより、組織の内部で評価する基準としても、取引先の顧客などから受ける第二者監査、あるいは、審査登録機関による認証のための第三者監査の基準としても用いることができます。

（出典）ISMS-AC「ISMS とは」　https://isms.jp/isms

One Point

ISO/IEC 27001 と JIS Q 27001

ISMS に関する規格には、ISO/IEC 27001 とは別に JIS Q 27001 があります。国際規格である ISO/IEC に対して、JIS は日本産業規格となり、日本における任意の国家規格です。JIS Q 27001 は、ISO/IEC 27001 を日本語に訳したものとなり ISO と JIS による規格内容の違いはありません。

6 ISMS-AC「ISMS とは」　https://isms.jp/isms/

11-3. NIST サイバーセキュリティフレームワーク（CSF）

11-3-1. NIST サイバーセキュリティフレームワーク（CSF）の概要

CSF の概要および ISMS との関係性について説明します。CSF の最新版は、2.0 です。CSF2.0 は、中小企業を含むあらゆる組織で利用されるよう設計されています。

CSF2.0 は ISMS を補完し、組織のセキュリティ対策を強化するための有用なツールとなります。ISMS を補完する形で、ISMS をベースに必要に応じて CSF を取り込むことが重要です。

CSF2.0 とは
CSF2.0 は、あらゆる組織がサイバーセキュリティリスクを管理する際の指針を提供するものです。CSF2.0 は、どのような組織でもサイバーセキュリティへの取組をより深く理解し、評価し、優先順位をつけ、各方面に周知するために利用できます。CSF2.0 の実施方法は画一的ではなく、組織ごとに異なります。各組織には共通のリスクと固有のリスクの両方があり、また、組織によってリスク選好度やリスク許容度、具体的なミッション、ミッションを達成するための目的もさまざまであるためです。CSF2.0 をしっかりと理解し、自組織に適した形で実施することが重要です。

CSF2.0 の 3 つの構成要素（コア、ティア、プロファイル）

CSF は、組織がセキュリティ対策を継続的に改善するため、①コア（サイバーセキュリティ対策の一覧）、②ティア（対策状況を数値化するための成熟度評価基準）、③プロファイル（サイバーセキュリティ対策の現状とあるべき姿を記述するためのフレームワーク）の 3 つの要素で構成されています。

「コア」の概要
コアとは、一定の分類で定められたセキュリティ管理策の一覧のことです。 コアは、「識別」「防御」「検知」「対応」「復旧」「ガバナンス」の 6 つの機能に分類されます。各機能の下には複数のカテゴリが存在し、各カテゴリはそれぞれ複数のサブカテゴリを有します。
「ティア」の概要
組織におけるサイバーセキュリティガバナンスと管理の成熟度を評価するための階層（tier）です。 指標階層は 4 段階あり、次の通りです。 ● ティア 1：実施しているが、まだ部分的／基本的なレベル ● ティア 2：ある程度定型化されているがポリシーにはなっていない ● ティア 3：ポリシーとして確立しており、繰り返し適用可能なレベル ● ティア 4：サイバーセキュリティリスク管理が組織文化の一部となっている
「プロファイル」の概要

フレームワークのカテゴリおよびサブカテゴリに基づき、サイバーセキュリティリスクに対する期待される効果を現すものです。 サイバーセキュリティリスクへの対応状況として、「あるべき姿」と「現在の姿」をまとめたものです。「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整します。

詳細理解のため参考となる文献（参考文献）	
The NIST Cybersecurity Framework（CSF）2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

「コア」

コアとは、業種・業態や企業規模に依存しない共通のサイバーセキュリティ対策の一覧を定義したものです。「ガバナンス」「識別」「防御」「検知」「対応」「復旧」の 6 つの機能に分類されます。

ガバナンス機能は、他の 5 つの機能（識別、防御、検知、対応、復旧）の目標達成や組織内の優先順位づけをするためのものと定義され、CSF2.0 の中心的機能と位置づけられています。

各機能の下には複数のカテゴリが存在し、合計 22 個あります。また、各カテゴリにはそれぞれ複数のサブカテゴリが存在しており、サブカテゴリは合計で 106 個あります。

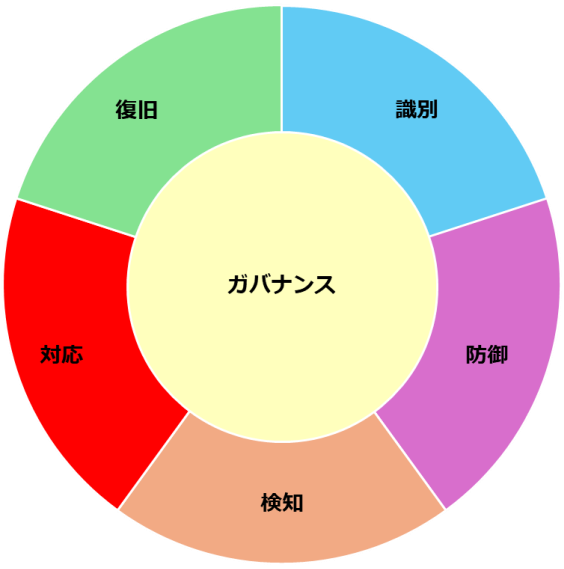


図 38. CSF2.0 のコア

（出典）「The NIST Cybersecurity Framework（CSF）2.0」をもとに作成

機能	説明	カテゴリ
ガバナンス	組織におけるサイバーセキュリティリスクマネジメントの戦略、期待事項、およびポリシーを確立し、周知し、モニタリングする。	● 組織的文脈 ● リスクマネジメント戦略 ● 役割/責任/権限 ● ポリシー ● 監督 ● サイバーセキュリティサプライチェーンリスクマネジメント
識別	組織の資産（情報システム、人、データ・情報など）、組織を取り巻く環境、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを特定し理解を深める。	● 資産管理 ● リスクアセスメント ● 改善
防御	重要サービスの提供が確実に行われるよう適切な保護対策を検討し実施する。	● アイデンティティ管理とアクセス制御 ● 意識向上およびトレーニング ● データセキュリティ ● プラットフォームセキュリティ ● 技術インフラのレジリエンス
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し実施する。	● 継続的モニタリング ● 有害イベントの分析
対応	サイバーセキュリティインシデントに対処するための適切な対策を検討し実施する。	● インシデントマネジメント ● インシデント分析 ● インシデント対応の報告とコミュニケーション ● インシデント軽減
復旧	サイバーセキュリティインシデントにより影響を受けた機能やサービスをインシデント発生前の状態に戻すための適切な対策を検討し実施する。これには、レジリエンスを実現するための計画の策定・維持も含む。	● インシデント復旧計画の実行 ● インシデント復旧のコミュニケーション

「ガバナンス」機能のサブカテゴリ（例）

カテゴリ	サブカテゴリ
組織的文脈	GV.OC-01：組織のミッションが理解され、サイバーセキュリティリスクマネジメントについて伝えている。
	GV.OC-02：内部と外部の利害関係者が理解され、サイバーセキュリティリスクマネジメントに関するそれら利害関係者のニーズと期待事項が理解および考慮されている。
	GV.OC-03：サイバーセキュリティに関する法的要求事項、規制上の要求事項、および契約上の要求事項（プライバシーと市民的自由の義務を含む）が理解され管理されている。
	GV.OC-04：外部の利害関係者が組織に依存または期待する重要な目的、能力およびサービスが理解され周知されている。
	GV.OC-05：組織が依存する成果、能力、およびサービスが理解され周知されている。

「ティア」

ティアとは、組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したものです。指標は以下の 4 段階があります。各ティアの定義は、組織に応じて柔軟にアレンジすることが可能です（以下の表は一例です）。また、必ずしもすべてのカテゴリにおいて最高レベル（ティア 4）を目指す必要はありません。ビジネス特性や情報資産の実態などに応じて、カテゴリごとに目指すべきティアを設定しましょう。

ティア 1：実施しているが、まだ部分的／基本的なレベル セキュリティ対策は経験に基づいて実施される。セキュリティ対策は組織として整備されていなく場当たり的に実施されている。
ティア 2：ある程度定型化されているがポリシーにはなっていない セキュリティ対策はセキュリティリスクを考慮して実施されているが、組織として方針や標準が定められてはいない、あるいは非公式に存在する。
ティア 3：ポリシーとして確立しており、繰り返し適用可能なレベル セキュリティ対策は組織の方針・標準として定義、周知されており、脅威や技術の変化に伴い方針・標準は定期的に更新される。
ティア 4：サイバーセキュリティリスク管理が組織文化の一部となっている 組織で標準化されたセキュリティ対策は、脅威や技術の変化、組織における過去の教訓やセキュリティ対策に関するメトリックスなどを参考に、継続的かつタイムリーに調整される。

サイバーセキュリティリスクへの対応状況を評価する例

識別：セキュリティ対策が必要なリソースを明確にする

	ティア 1	ティア 2	ティア 3	ティア 4
資産管理 事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が特定され管理されていますか？				

防御：ルールを策定し、セキュリティリスクをコントロールする

	ティア 1	ティア 2	ティア 3	ティア 4
意識向上およびトレーニング サイバーセキュリティ意識向上教育とトレーニングが実施されていますか？				

検知：事故の発生を即時に把握するための仕組みをつくる

	ティア 1	ティア 2	ティア 3	ティア 4
異常とイベント 異常な活動は検知されており、異常がもたらす潜在的な影響を把握していますか？				

対応：事故に対する対策を用意する

	ティア 1	ティア 2	ティア 3	ティア 4
対応計画の策定 検知したセキュリティ事故に対応できるように対応プロセスおよび手順が準備されていますか？				

復旧：システムを正常な状態に戻すための必要なタスクを明確にする

	ティア 1	ティア 2	ティア 3	ティア 4
復旧計画の作成 セキュリティ事故による影響を受けたシステムや資産を復旧できる復旧プロセスおよび手順となっていますか？				

「プロファイル」

プロファイルとは、機能・カテゴリ・サブカテゴリについて、組織ごとに考慮すべき点を踏まえて調整し、整理したものです。組織はプロファイルを用いることにより、サイバーセキュリティ対

策の現在の状態（現在の姿）と、目標の状態（あるべき姿）を明らかにすることができます。そして「現在の姿」と「あるべき姿」を比較することによって、サイバーセキュリティマネジメント上の目標を達成する上で、解消が必要なギャップを知ることができます。

「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整します。

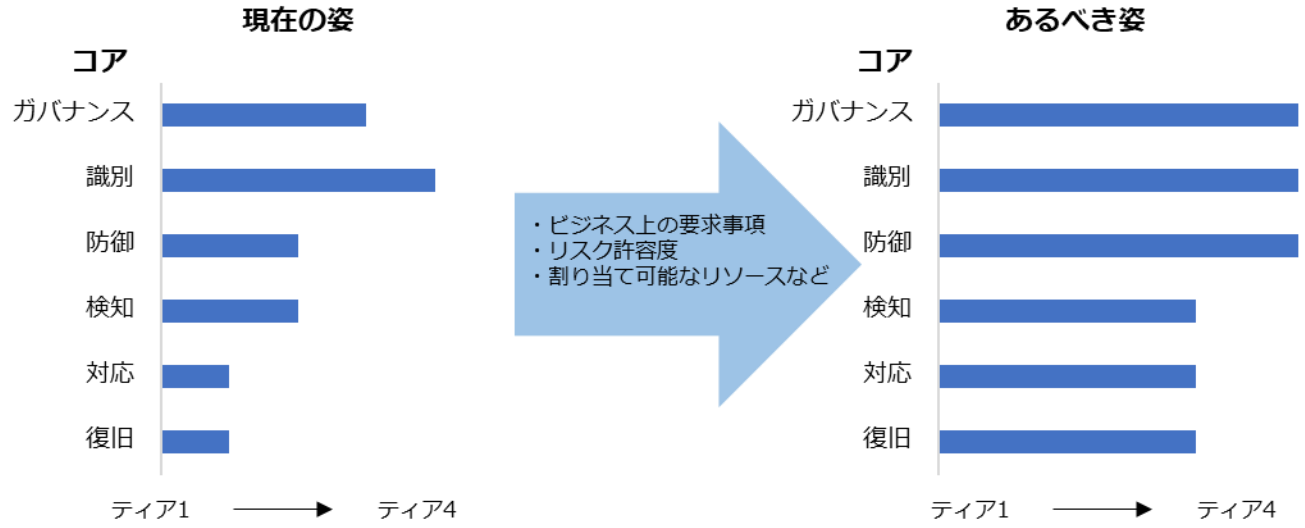


図 39. プロファイルの活用イメージ

（出典）デジタル庁「政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート」をもとに作成

NIST サイバーセキュリティフレームワーク（CSF）2.0 の特徴

令和 6 年 2 月 26 日、NIST サイバーセキュリティフレームワークが 1.1 から 2.0 に改訂されました。CSF2.0 の主な特徴は、以下の通りです。

フレームワークの適用範囲の拡大

CSF 2.0 は、組織の規模や業種に関係なく、中小企業を含むあらゆる組織で利用されるよう再設計されました。以前の CSF 1.0,1.1 は、重要インフラ（病院、発電所など）の安全保障を目的に策定されたものでした。

新たな機能「ガバナンス」の追加

CSF2.0 では、コアの 5 つの機能（特定・防御・検知・対応・普及）に、「ガバナンス」が新たに追加されました。

ガバナンスは、5 つの機能の中心に位置づけられています。ガバナンスは、組織のミッションと利害関係者の期待に沿って、他の 5 つの機能の成果の達成と優先順位をつけるための方法を示します。

フレームワーク活用のためのコンテンツ強化

CSF の実装を支援するためのさまざまな参考情報が、NIST の Web サイトに公開されました。

- クイック・スタート・ガイド（Quick-Start Guide）
  中小企業などの特定のニーズに対応した専用のガイダンスを提供しています。

文書名	利用方法
Small Business Quick-Start Guide	中小企業、特にサイバーセキュリティ計画があまり整っていないまたは全くない企業が、CSF2.0 を使用してサイバーセキュリティリスク管理戦略を開始するためのポイントを理解するために利用できます。
A Guide to Creating Community Profiles	フレームワークを実装するために、コミュニティプロファイルの作成と使用に関する考慮事項を理解するために利用できます。コミュニティプロファイルとは、多数の組織間で共有される、サイバーセキュリティリスクを低減するための関心、目標、成果を記述したものです。
Quick-Start Guide for Creating and Using Organizational Profiles	CSF 2.0 を実装するための現状および目標プロファイルの作成と使用に関する考慮事項を理解するために利用できます。
Quick-Start Guide for Using the CSF Tiers	CSF 2.0 のティアをプロファイルに適用し、自身のサイバーセキュリティリスクのガバナンスおよび管理成果の厳密さを特徴付けるために利用できます。
Quick-Start Guide for Cybersecurity Supply Chain Risk Management（C-SCRM）	サイバーセキュリティサプライチェーンリスク管理（C-SCRM）の概要と、C-SCRM が CSF とどのように関連しているのか理解するために利用できます。 C-SCRM の機能を実装する組織は、このガイドに加えて、参照されている追加文書も併せて確認することが推奨されます。
Enterprise Risk Management Quick-Start Guide	エンタープライズリスクマネジメントの実務者が、組織のサイバーセキュリティリスクマネジメントを改善するために、CSF2.0 で提供される成果の活用方法を理解するために利用できます。

- 参考情報（Informative References）
  参考情報を利用することにより、目標達成に役立つ他のガイドラインやリソースを知ることができます。
- 実装例（Implementation Examples）
  実装例を利用することにより、特定のサブカテゴリをどのように実装するかのベストプラクティス（最良の方法）を知ることができます。

- NIST Cybersecurity Framework（CSF）2.0 Reference Tool
  NIST CSF 2.0 リファレンスツールを利用すると、ユーザーは CSF 2.0 コア（機能、カテゴリ、サブカテゴリ、実装例）を探索できます。このツールは、人間と機械が読み取り可能な形式（JSON および Excel）でコアを提供します。さらに、ユーザーは主要な検索用語を使用してコアの一部を表示し、エクスポートすることが可能です。これにより、ユーザーは自分のニーズに合わせて情報を探しやすくなります。

サプライチェーンリスクマネジメントの強化

CSF2.0 では、新機能「ガバナンス」の下に新しいカテゴリ（GV.SC：サイバーセキュリティサプライチェーンリスクマネジメント）が設けられました。GV.SC カテゴリの下には 10 個のサブカテゴリが定義され、CSF1.1 に比べてサプライチェーンのリスク管理に必要な対策が増加しました。

詳細理解のため参考となる文献（参考文献）	
Small Business Quick-Start Guide	https://doi.org/10.6028/NIST.SP.1300
A Guide to Creating Community Profiles	https://doi.org/10.6028/NIST.CSWP.32.ipd
Quick-Start Guide for Creating and Using Organizational Profiles	https://doi.org/10.6028/NIST.SP.1301
Quick-Start Guide for Using the CSF Tiers	https://doi.org/10.6028/NIST.SP.1302.ipd
Quick-Start Guide for Cybersecurity Supply Chain Risk Management（C-SCRM）	https://doi.org/10.6028/NIST.SP.1305.ipd
Enterprise Risk Management Quick-Start Guide	https://doi.org/10.6028/NIST.SP.1303.ipd
CSF 2.0 Informative References	https://www.nist.gov/informative-references
CSF 2.0 Implementation Examples	https://www.nist.gov/document/csf-20-implementations-pdf
NIST Cybersecurity Framework（CSF）2.0 Reference Tool	https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

11-3-2. NIST SP 800

NIST SP 800 シリーズと CSF の関連性

CSF は、NIST が定義するサイバーセキュリティ対策アプローチの中で最も上位に位置づけられており、セキュリティ管理手法の概念や管理方針・体制の整備など包括的な内容が記載されています。CSF の下位概念に位置づけられているのが、NIST SP 800 シリーズです。実施すべきタスクと手順、推奨技術の特定など、セキュリティ管理の手法について具体的に明記されています。

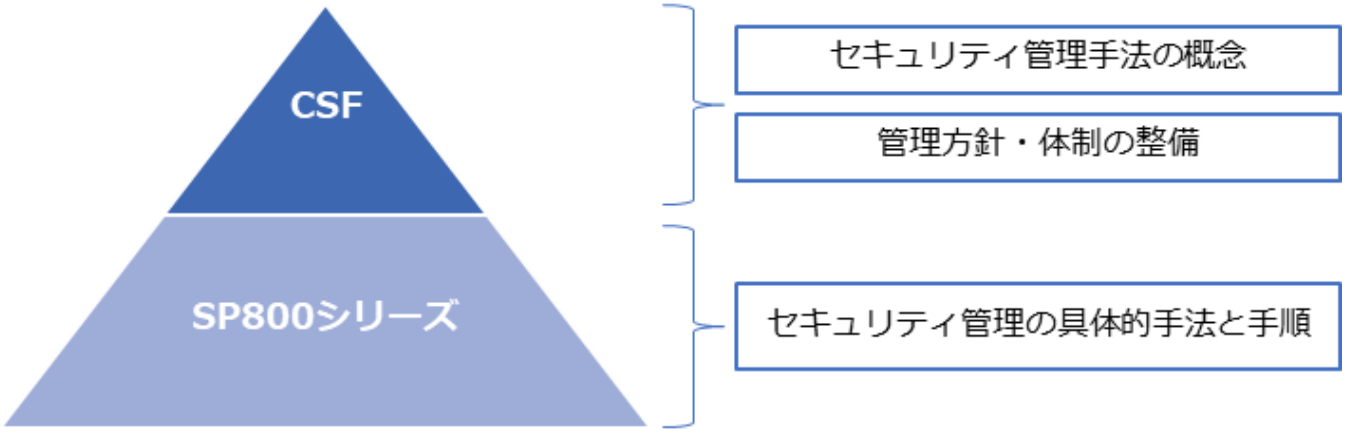


図 40. CSF と SP800 シリーズの関係

NIST SP 800-53、NIST SP 800-171、NIST SP 800-161

NIST SP 800 シリーズの中から、ガイドラインの一部を紹介します。

NIST SP 800-53
米国政府内の情報システムをより安全なものにし、効果的にリスク管理するためのガイドラインのことです。対象は連邦政府機関で、政府の機密情報（CI：Classified information）の保護を目的としています。
NIST SP 800-171
NIST SP 800-53 から民間企業・組織向けに要件を抽出したものです。サプライチェーンに存在する、業務委託先や関連企業のすべてが準拠すべきセキュリティ基準を示しています。対象は、多くの民間企業・組織で、政府の機密情報以外の重要情報（CUI：Controlled Unclassified Information）の保護を目的としています。
NIST SP 800-161
調達から販売・供給までの一連のサプライチェーンに起因するさまざまなリスクに対して、組織として対応するためのガイドラインです。業務委託先や関連企業におけるセキュリティ対策を目的としています。

NIST SP 800-53 と NIST SP 800-171 は、以下のように保護する情報と対策を行う組織が異なりますが、どちらも密接に関連しているため 2 つ同時に参照する必要があります。

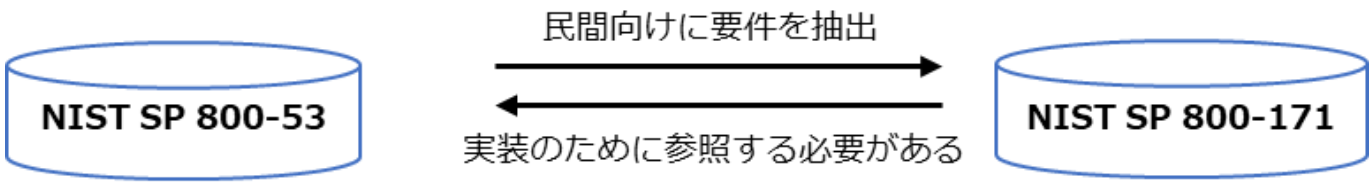


図 41. NIST SP 800-53 と NIST SP 800-171 の関係

11-3-3. ISMS との関連性

CSF と ISMS の主な関係性を説明します。

CSF と ISMS の主な共通点
汎用性が高い ISMS と CSF は、汎用性が高く、あらゆる組織で使用することができます。まずは ISMS をベースにして情報セキュリティ対策を行い、必要に応じて CSF の内容を取り入れるとよいでしょう。
サイバーセキュリティ対策方法 ISMS と CSF はどちらも「識別」「防御」「検知」「対応」「復旧」といったサイバーセキュリティ対策を挙げています。

任意性がある

ISMS と CSF はどちらも、提示しているすべてのセキュリティ対策を取り入れることは求めていないため、何を取り入れるかはそれぞれの組織で決定可能です。

CSF と ISMS の主な相違点
第三者認証制度の有無 ISMS には、第三者機関による認証制度（適合性評価制度）が存在します。これに対して、CSF にはそのような認証制度はありません。そのため、情報セキュリティ対策を行っていることを顧客や取引先に対して客観的に示すためには、ISMS を構築して認証を受けることが有効です。
目標への到達手段 ISMS は、PDCA サイクルをまわすことにより、情報セキュリティマネジメント体制を構築する一方、CSF では特に PDCA サイクルをまわすといった記載はありません。CSF の「プロファイル」では、現在の状況と理想の状況とのギャップを明確にすることにより、取るべき対応策の優先順位を決めて、それにしたがって実施していくことになります。

11-4. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

概要

Society5.0 の到来で、サイバー空間とフィジカル空間が融合することによって、これまでにはなかったさまざまな新たな価値（モノやサービス）が提供されることになります。

サプライチェーンは、従来の形（例：調達→生産→物流→販売）から、サイバー空間とフィジカル空間のつながりや、サイバー空間のデータのつながりを考える必要がある形へと変化していくことになります。このような新たな形のサプライチェーンは、『価値創造過程（バリュークリエイションプロセス）』と定義されています。

製品を製造して消費者に販売するまでが従来のサプライチェーンだとした場合、バリュークリエイションプロセスでは、消費者の使用データの収集やシステムのアップデートなどを通じて消費者との関係が継続します。サイバー空間とフィジカル空間の接点のすべてがサイバー攻撃の対象となると考えられ、工場のシステムに加えて、製品そのものに対する攻撃、個人情報などのデータを蓄積した本社に対する攻撃が行われる危険性があります。

このような新たなサプライチェーンの概念に求められるセキュリティへの対応指針として、政府は『サイバー・フィジカル・セキュリティ対策フレームワーク』（CPSF）を策定しました。

CPSF は、ISMS や CSF のフレームワークの内容を包含しつつ、サイバー空間とフィジカル空間双方のセキュリティ対策に対応したフレームワークとなっています。

目的と適用範囲

CPSF の主な目的は、新たな産業社会におけるバリュークリエイションプロセス全体の理解、リスク源の明確化、必要なセキュリティ対策全体像の整理を行うことです。従来のサプライチェーンに適用可能なセキュリティ対策に加えて、新たな産業社会の変化から生じる特有の対策も含まれています。

本フレームワークの適用範囲としては、新たな産業社会におけるバリュークリエイションプロセス全体となります。企業が本フレームワークを参考にし、自社の実態に合わせて、適切なセキュリティ対策を実施することが重要です。

CPSF に含まれる対策
● 従来型サプライチェーンにおいても適用可能な対策 ● 新たな産業社会に変化したからこそ新たに対応が必要な対策

- 新たな産業社会におけるバリュークリエイションプロセス全体が適用範囲
- それぞれの組織に応じてセキュリティ対策を選定することが可能

従来のサプライチェーンに対するセキュリティの考え方では、セキュリティ対応を行っている組織間の取引であれば、サプライチェーン全体の信頼性が確保される「組織マネジメントの信頼性」

に基点が置かれていました。

しかしながら、Society5.0 では、従来のサプライチェーンのように、組織のマネジメントの信頼性に基点を置くことだけでは、バリュークリエイションプロセスの信頼性を確保することが困難となります。IoT 機器を使用した場合、フィジカル空間のさまざまな情報はデジタル化され・サイバー空間へ取り込まれ、新たな価値が生み出されます。その一方で、マネジメントルールを徹底しただけでは、サイバー空間に取り込んだデータの適切な保護といった信頼性を確保することはできなくなります。

バリュークリエイションプロセスの信頼性を確保するためには、セキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要になります。そのため、CPSF では、バリュークリエイションプロセスが発生する産業社会を 3 つの層、バリュークリエイションプロセスに関与する構成要素を 6 つに整理し、CPSF の基本構成としました。3 つの層でリスク源を洗い出し、6 つの構成要素で各リスク源に対する対策要件および具体的な対策例を示します。

3 層構造モデル

各層における信頼性の基点は以下の通りです。

第 1 層	企業（組織）のマネジメントの信頼性
第 2 層	サイバー空間とフィジカル空間のつながりにおける、要求される情報の正確性に応じて適切な正確さで情報が変換される“転写”機能の信頼性
第 3 層	サイバー空間のつながりにおける、データの信頼性

[第 3 層]サイバー空間におけるつながり
自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保
[第 2 層]フィジカル空間とサイバー空間のつながり
フィジカル空間・サイバー空間を正確に”転写”する機能の信頼性を確保 （現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラなどの信頼）
[第 1 層]企業間のつながり
適切なマネジメントを基盤に各主体の信頼性を確保

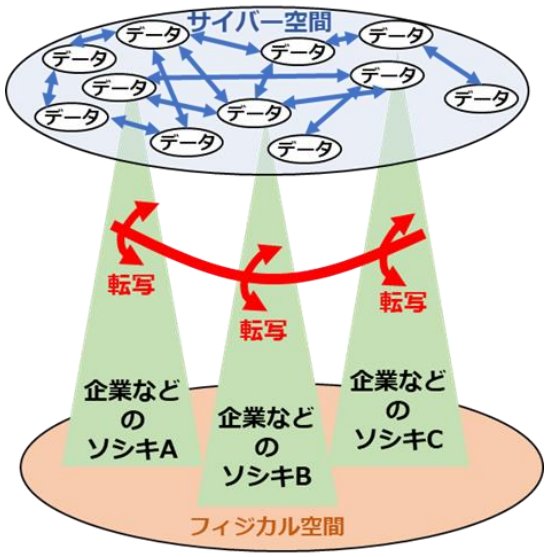


図 42. 層構造モデルと各層における信頼性

（出典）経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークの概要」をもとに作成

11-5. サイバーセキュリティ経営ガイドライン

11-5-1. サイバーセキュリティ経営ガイドライン

経営者が主体となってサイバーセキュリティ対策を実施する際に、経済産業省と独立行政法人情報処理推進機構（IPA）が共同で発行している「サイバーセキュリティ経営ガイドライン」が参考になります。本ガイドラインでは、経営者がサイバーセキュリティ対策を実行する際に認識するべき事項と、サイバーセキュリティ対策の責任者（CISO など）に指示するべき事項を包括的にまとめています。

平成 29 年の Ver2.0 の公開以降、企業のサイバーセキュリティ対策を取り巻く環境が変化しました。そのため、最新の状況への認識と対策の実践が可能となるように内容が見直され、令和 5 年に Ver3.0 が最新版として公開されました。

企業のサイバーセキュリティ対策を取り巻く環境の変化	
テレワークの活用	テレワークなどのデジタル環境の活用を前提とする働き方の多様化
サイバー空間とフィジカル空間のつながり	インターネットなどのサイバー空間と現物の取引を行うフィジカル空間のつながりの緊密化と、それに伴うリスクの顕在化
セキュリティ対象の変化・拡大	情報資産だけでなく、制御系を含むデジタル基盤の保護がサイバーセキュリティの対象となる変化と拡大
ランサムウェアの被害	ランサムウェアによる被害の顕在化により、企業におけるサイバーセキュリティに関する被害は情報漏えいに留まらず、企業の事業活動の停止へと影響が拡大
サプライチェーンを介した被害拡大	国内外のサプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえた、サプライチェーン全体を通じた対策の必要性の高まり
ESG 投資の拡大	ESG（Environment, Society, Governance）投資の拡大により、コーポレートガバナンスおよび ERM（エンタープライズリスクマネジメント）の改善に向けた取組に対する関心の高まり

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

次のページからは、サイバーセキュリティ対策に取り組む上で、経営者が認識するべき事項と実行するべき事項を紹介し、経営目線でのサイバーセキュリティ対策について全体像を説明します。また、経営者とセキュリティ担当者それぞれの立場に応じて、具体的に行うべきことについて説明した後、サイバーセキュリティ対策を実践するための手順を説明します。

One Point

サイバーセキュリティ対策は企業の価値増大への投資

サイバーセキュリティ対策はやむを得ない「費用」と考えるのではなく、「投資」と位置づけることが重要です。なぜなら、サイバーセキュリティ対策は、企業活動における損失やコストを減らし、企業の価値を維持・増大させるために必要だからです。サイバーセキュリティに関するリスクを経営リスクの一環として取り入れ、適切な対策に投資することによって、リスクを許容可能な範囲まで低減させることができます。企業としては、この取組を通じて社会的責任を果たし、経営者はこの責務を認識する必要があります。

経営者が認識するべき 3 原則

経営者は、以下の 3 原則を認識し、対策を進める必要があります。

原則 1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
原則 2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先など、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
原則 3	平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営の重要 10 項目

経営者は、以下の重要 10 項目について、サイバーセキュリティ対策を実施する上での責任者や担当部署（CISO、サイバーセキュリティ担当者など）への指示を通じて組織に適した形で確実に実施させる必要があります。これらは、組織のリスクマネジメントの責任を担う経営者が、単なる指示ではなく、自らの役割として発信する必要があります。リスク対策に関する実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応など、多くのことを通じてリーダーシップを発揮することが求められます。

経営者がリーダーシップをとったセキュリティ対策の推進
サイバーセキュリティリスクの管理体制構築 指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定 指示 2 サイバーセキュリティリスク管理体制の構築 指示 3 サイバーセキュリティ対策のための資源（予算、人材など）確保
サイバーセキュリティリスクの特定と対策の実装 指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 指示 5 サイバーセキュリティリスクに効果的に対応する仕組みの構築 指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善
インシデント発生に備えた体制構築

指示 7 インシデント発生時の緊急対応体制の整備 指示 8 インシデントによる被害に備えた事業継続・復旧体制の整備
サプライチェーンセキュリティ対策の推進
指示 9 ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握および対策
ステークホルダーを含めた関係者とのコミュニケーションの推進
指示 10 サイバーセキュリティに関する情報の収集、共有および開示の促進

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

サイバーセキュリティ経営の重要 10 項目の概要

経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO など）に指示すべき「重要 10 項目」のポイントと、対策例の一部を紹介します。

指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

- サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定させる。
- 策定した対応方針を対外的な宣言として公表させる。

対策例

- 経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取ったセキュリティポリシーを策定する。その際、製造、販売、サービス等、事業が立脚している全ての基盤（設備、システム、情報等の資産、流通プロセス等）に影響を及ぼすと考えられるサイバーセキュリティリスクに応じた対応方針を検討する。

指示 2 サイバーセキュリティリスク管理体制の構築

- サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構成させる。
- サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。

対策例

- 役割遂行に求められる責任や専門性、人的資源の状況に応じて、組織内要員で対応すべきものと外部の専門サービスに委託すべきものとの切り分けを行う。
- 取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築、運用されているかを監査する。

指示 3 サイバーセキュリティ対策のための資源（予算、人材等）確保

- サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組ませる。
- 全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。

対策例

- 事業が立脚している全ての基盤の安全性の担保のために必要なサイバーセキュリティ対策を明確にし、それに要する費用を確保する。
- 従業員向けやセキュリティ担当者向けなどの研修等のための予算を確保し、継続的に役割に応じたセキュリティ教育を実施する。
- セキュリティ対策業務に従事する人材のみならず、デジタル部門、事業部門、管理部門等のあらゆる業務に従事する人材に、「プラス・セキュリティ」知識・スキルの習得を促す。

指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

- 事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
- サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダーへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

対策例

- 組織における情報のうち、経営戦略の観点から守るべき情報を特定し、それらがどこに保存され、どこで扱われているかを把握する。その際、自社の営業秘密を外部のクラウドサービスで管理したり、テレワーク等の新しい働き方を導入したりしていることの影響を適切に反映させる。

指示 5 サイバーセキュリティリスクに効果的に対応する仕組みの構築

- サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。
- 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

対策例

- 重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施する。
- 従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。

指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善

- リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用させる。
- 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- 株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

対策例

- 必要に応じて、ISO/IEC 27001 規格に基づく ISMS など、国際標準となっている PDCA マネジメントシステムの認証を活用する。

指示 7 インシデント発生時の緊急対応体制の整備

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRT 等）を整備させる。
- 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- インシデント発生時の対応について、適宜実践的な演習を実施させる。

対策例

- インシデント発生時の体制整備、ルール整備にあたって、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照しながら、社内理解を深める。
- インシデントの発生を想定した緊急対応に関する演習を役員に対して定期的に実施し、緊急時にどのような手順で初動対応を行うべきかについて、全ての関係者が体験を通じて理解する。

指示 8 インシデントによる被害に備えた事業継続・復旧体制の整備

- インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- 制御系も含めた BCP との連携等、組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。
- 業務停止等からの復旧対応について、対象を IT 系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

対策例

- 設備投資計画を立案する際に、事業継続に影響をもたらす要因として、自然災害やパンデミック等にサイバーセキュリティリスクを加え、その対策を要求仕様等に反映させる。
- 定期的な復旧演習の実施により、復旧対応に関わる関係者がその手順について、体験を通じて理解する。

指示 9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

- サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。
- ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

対策例

- 系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等が SECURITY ACTION を実施していることを確認する。なお、ISMS 等のセキュリティマネジメント認証を取得していることがより効果的である。

指示 10 サイバーセキュリティに関する情報の収集、共有及び開示の促進
● 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。 ● 入手した情報を有効活用するための環境整備をさせる。 対策例 ● 株主やステークホルダーとの対話、広報による一般向け情報開示等の機会において、サイバーセキュリティインシデントに備えた日頃の取組等の情報開示に積極的に取り組む。 ● 中小企業の場合は、商工会議所、商工会等を通じて地元で情報共有を行うことのできる相手を確保する。 ● 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参考に、インシデントに備え、サイバーセキュリティ専門組織との情報共有や被害に係る情報の公表を行うにあたっての観点について、あらかじめ理解しておく。

詳細理解のため参考となる文献（参考文献）	
サイバー攻撃被害に係る情報の共有・公表ガイダンス	https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

11-5-2. サイバーセキュリティ経営ガイドラインの読み方

ここでは「経営者」、「情報セキュリティ対策の責任者（CISO など）」それぞれの立場から、本ガイドラインの内容を実践する際の役割、認識するべきことについて記載します。

対象者	経営者
役割	● 「3 原則」の理解 ● 重要 10 項目について、情報セキュリティ対策の責任者（CISO など）に指示を出す ● リーダーシップの発揮
認識すべきこと	**ERM（エンタープライズリスクマネジメント）にサイバー攻撃のリスクを含めること** 現在、企業活動の多くは IT に依存しています。そのため、内部統制システムの構築や、コーポレートガバナンス・コードに基づく開示と対話などにおいて、サイバー攻撃のリスクを考慮する必要があります。 **サプライチェーン上のリスクを認識すること** 現在、サプライチェーンの多様化が進み、サイバー攻撃の起点は広く拡散しています。したがって、サプライチェーン全体を考慮したリスクマネジメントが必要です。

	サイバーセキュリティ対策は担当者に丸投げしてはいけない 経営者は、インシデント発生時に法的・社会的責任を負い、事業停止や新たな脅威に対処するための経営判断を迫られることがあります。そのため、経営者は、サイバーセキュリティ対策を担当者に丸投げせずに、自ら主体的に取り組む必要があります。 **サイバーセキュリティ対策は投資と位置づけること** サイバーセキュリティ対策への投資では、直接的な収益を算出することは困難です。しかし、サイバーセキュリティ対策への投資は、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、将来の事業活動・成長に必須な投資でもあります。

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

One Point

ERM（エンタープライズリスクマネジメント）とは

企業が直面するリスクに対して、企業全体で管理することです。国際競争や情報技術の急速な進化により、企業が直面するリスクも多様化しています。このような状況下で、従来の部門ごとにリスクに対して管理するのではなく、企業全体で管理することが重要です。

対象者	情報セキュリティ対策を実施する上で責任者となる担当幹部 （CISO など）
役割	● 重要 10 項目を理解すること ● 経営者に対して適宜状況報告を行い、経営者が適切な判断を行うために必要な情報を提供すること
認識すべきこと	経営者から指示される以下の事項に関して、より具体的な取組を検討し、セキュリティ担当者に対して指示する必要があること ● サイバーセキュリティリスクの管理体制構築 ● サイバーセキュリティリスクの特定と対策の実装 ● インシデント発生に備えた体制を構築 ● サプライチェーンセキュリティ対策の推進 ● ステークホルダーを含めた関係者とのコミュニケーションの推進

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

11-5-3. サイバーセキュリティ経営ガイドラインの実践の流れ

サイバーセキュリティ経営ガイドラインの活用手順

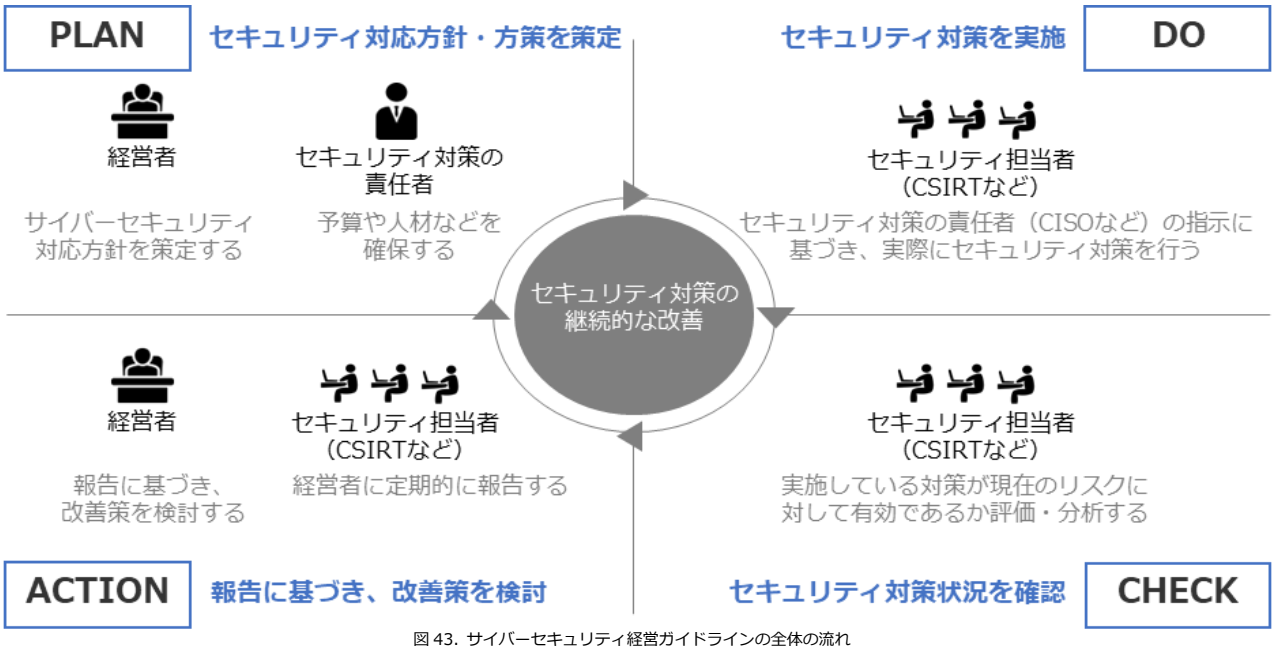


図 43. サイバーセキュリティ経営ガイドラインの全体の流れ

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

PLAN

はじめに、サイバーセキュリティ対応方針・方策を策定します。

- 経営者は、3 原則を認識した上でサイバーセキュリティ対応方針を策定します。
- セキュリティ対策の責任者（CISO など）は、経営者の指示に基づき、リスクを許容範囲内に抑制するための方策を検討し、必要となる資源（予算や人材など）を確保します。

DO

セキュリティ担当者（CSIRT など）は、セキュリティ対策の責任者（CISO など）の指示に基づき、実際にセキュリティ対策を行っていきます。具体的には以下の作業を行います。

- リスクの把握や対応計画の策定
- サイバー攻撃の防御や検知
- 分析などの保護対策の実施
- 緊急時の対応体制を整備、事業継続、復旧体制の整備

CHECK

実施しているセキュリティ対策がリスクに対して有効であるか評価・分析をします。

- セキュリティ担当者（CSIRT など）は、サイバーセキュリティ経営ガイドライン付録の「サイバーセキュリティ経営チェックシート」や「サイバーセキュリティ経営可視化ツール」を活用し、経営者が指示した事項の実践状況をチェックします。

ACTION

セキュリティ担当者（CSIRT など）は、経営者に指示された事項の実践状況について、CISO を通じて経営者に報告し、経営者は報告をもとに改善策を検討します。

- 新たなサイバーセキュリティリスクの発見などにより、追加の対応が必要な場合には、対処方針を修正します。

第12章. リスクマネジメント

章の目的
第 12 章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方について学ぶことを目的とします。
主な達成目標
◘ リスクマネジメントの意義について理解すること ◘ リスクマネジメントプロセスの全体像を理解すること ◘ リスクアセスメント、リスク対応のプロセスを理解すること

12-1. リスクマネジメント：概要

12-1-1. リスクマネジメントプロセス（ISO31000）

企業や組織にはさまざまなリスクが存在しています。これらのリスクを効率的に管理し、発生する可能性がある損失を回避したり低減したりするプロセス全体のことを「リスクマネジメント」と言います。

リスクマネジメントの国際規格として ISO 31000 があります。ISO 31000 では、リスクマネジメントを「原則」「枠組み」「プロセス」の 3 つの要素から構成されるものとして捉えています。

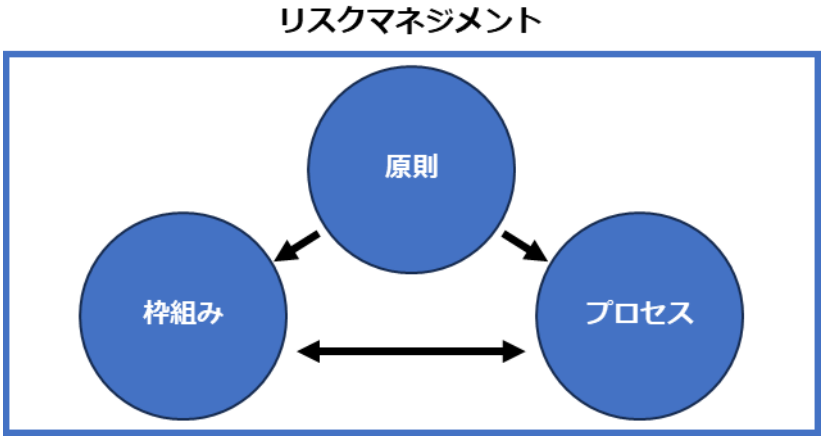


図 44. リスクマネジメントの 3 要素

原則	リスクマネジメントを実施する際に、組織が取り組むべき事項です。 「統合」「体系化及び包括」「組織への適合」「包含」「動的」「利用可能な最善の情報」「人的及び文化的要員」「継続的改善」で構成されています。
枠組み	リスクマネジメントを組織全体に定着させるための仕組みです。 「統合」「設計」「実施」「評価」「改善」で構成されています。
プロセス	リスクマネジメントに取り組む上で実施すべき、一連の活動です。 「コミュニケーション及び協議」「適用範囲、組織の状況及び基準」「リスクアセスメント」「リスク対応」「モニタリング及びレビュー」「記録作成及び報告」で構成されています。

実際にリスクに対応していくにあたっては、リスクマネジメントプロセスにおける「リスクアセスメント」が必須事項となります。リスクアセスメントとは、組織や企業が抱える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づけをしていくプロセスのことを表します。リスクアセスメントの実施により、個々の資産が持つリスクと、リスクに対する管理策、および管理策に投じるべき費用の識別が期待できます。また、リスクを評価するということは情報資産の持つ固有の弱点や脅威を明確にする過程を含みます。そのため、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、適切な対策を検討することが可能になります。

12-1-2. 情報セキュリティリスクマネジメント（ISO/IEC27005）

ISO/IEC 27005 は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。先に説明した ISO31000 と整合性がありますが、情報セキュリティに特化した内容になっています。この規格は、組織の情報資産を安全に保つことに焦点が当てられており、情報セキュリティリスクの特定、分析、評価、対応、管理、レビューなどを実施するための手引きになっています。中小企業を含むすべての組織における情報セキュリティリスクのマネジメントに有用です。

ISO/IEC 27005 の情報セキュリティリスクマネジメントプロセスは、ISO 31000 の一般的なリスクマネジメントプロセスに基づいており、リスクの特定、リスクの評価、リスクの対処およびリスクの監視とコントロールに関するステップから構成されます。以下の図で示すように情報セキュリティリスクマネジメントプロセスは循環しており、反復的に実施されるものです。組織を取り巻く環境の変化や組織内の変化に応じて、新しいリスクが発生したり、既存のリスクが変化したりする上に、リスクへの対処法も進化するからです。特に、リスクマネジメントプロセスに含まれているリスクアセスメントは、リスク対応の方策や、対応の優先順位づけの前提になる重要な工程です。

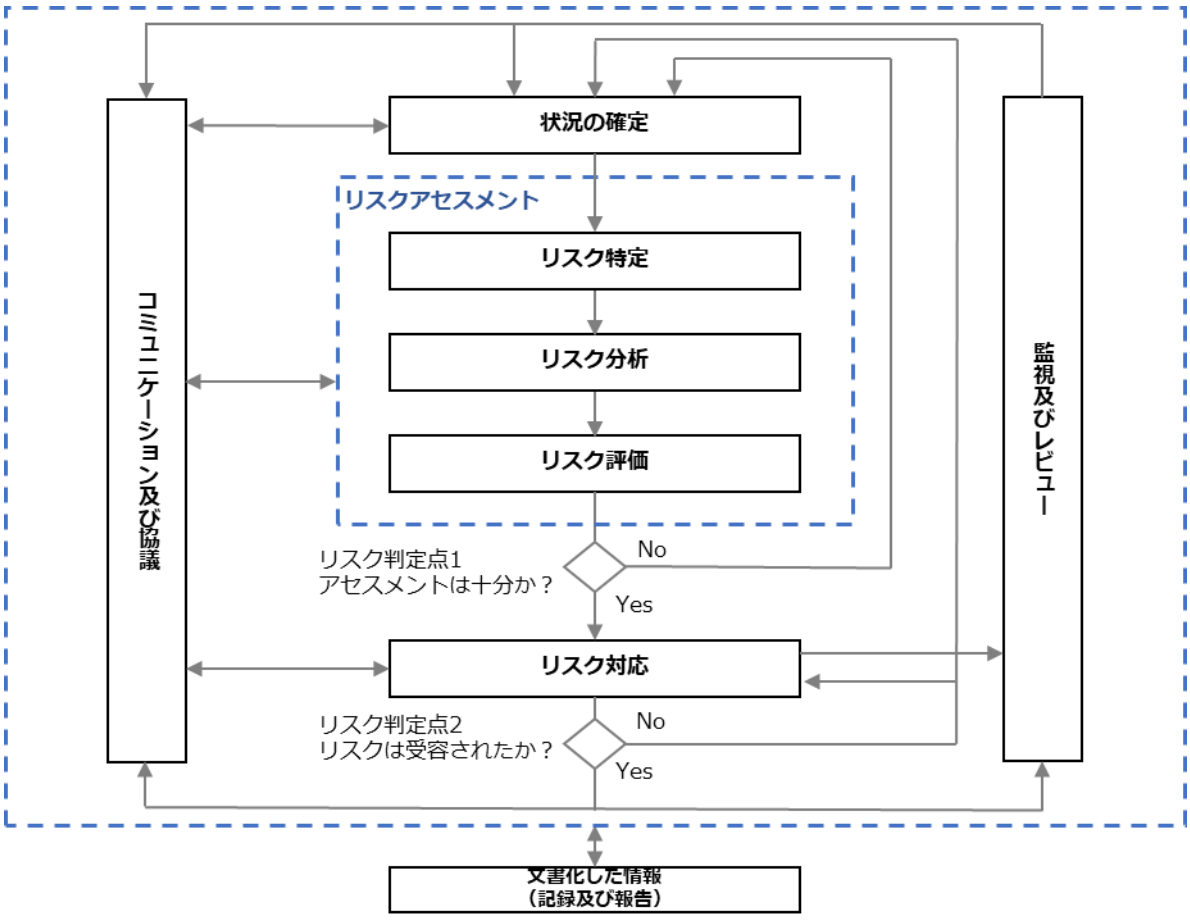


図 45. 情報セキュリティマネジメントプロセスの概要

（出典）ISO/IEC「ISO/IEC 27005:2022」をもとに作成

リスクアセスメントからリスク対応までの流れを表す図を記載します。リスク対応を実施する過程では、「低減」「移転」「回避」「受容（保有）」の４つ選択があり、それらの選択は以下の図で示すプロセスで行われます。

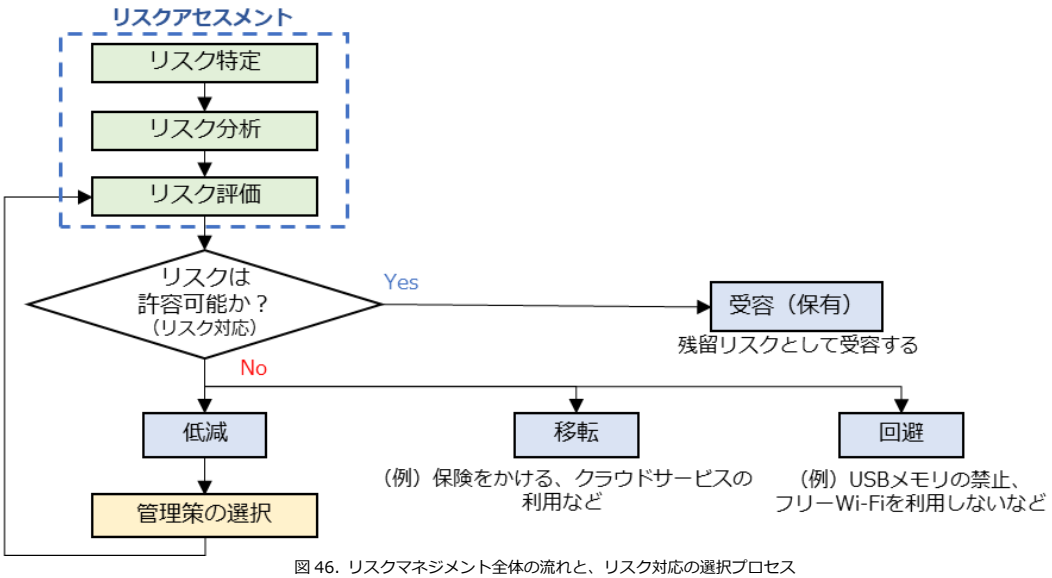


図 46. リスクマネジメント全体の流れと、リスク対応の選択プロセス

リスクを低減する
自社で実行できる情報セキュリティ対策を導入ないし強化することによって、脆弱性を改善し、事故が起きる可能性を下げます。
リスクを受容（保有）する
事故が発生しても受容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。
リスクを回避する
仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。 （例） ● 従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する。 ● インターネットバンキングに使用するパソコンでメールや Web サイトの閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールや Web サイトの閲覧に利用せず、USB メモリ、外付け HD D も接続を禁止する。 リスクレベルが大きく自社の対策だけでは不十分であったり、多額の費用がかかり、実施できなかったりする場合は「リスクの移転」を検討します。
リスクを移転する
自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することにより自社の負担を下げます。

（例）

- 商品を販売する Web サイトではクレジットカード番号を非保持化し、代金の決済はセキュリティ対策を十分行っている外部の決済代行サービスに変更する。
- 社内のサーバで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する。
- 情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する。

（出典）IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」をもとに作成

12-1-3. ISO/IEC 27001 におけるリスクマネジメント手順

ISO/IEC 27005 は、情報セキュリティリスクマネジメントの手法を提供する規格であり、ISO/IEC 27001（ISMS）は情報セキュリティマネジメントシステムの設計と実装に関する規格です。つまり、ISO/IEC 27001 は情報セキュリティマネジメントシステムの枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているのが、ISO/IEC 27005 になります。ISO/IEC 27001（ISMS）の活動は、ISO/IEC 27005 におけるリスクマネジメントプロセスと関連付けて整理することが可能です。

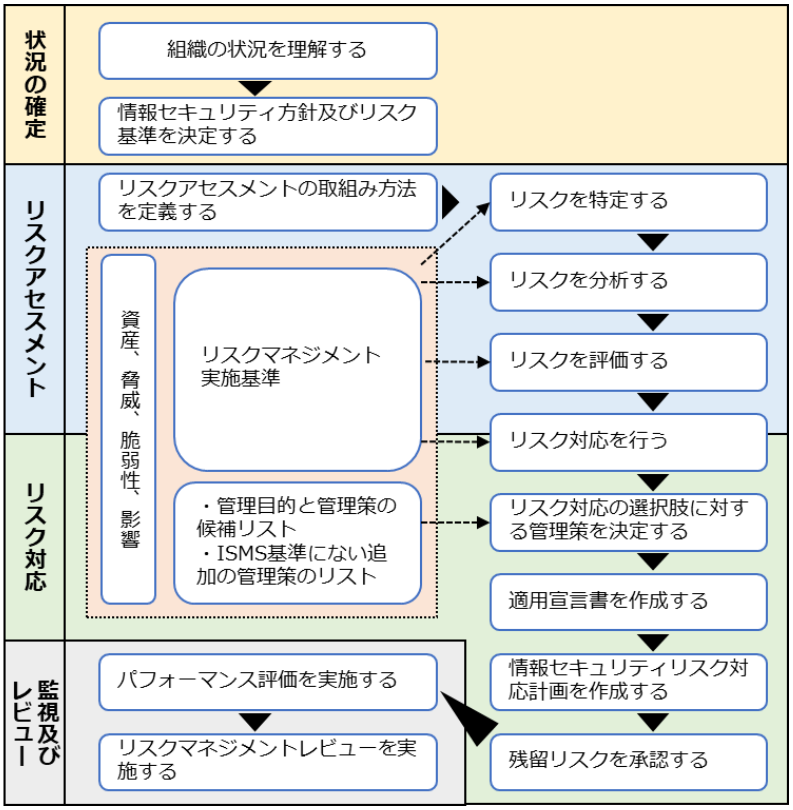


図 47. ISMS におけるリスクアセスメントおよびリスク対応に関する作業の概要

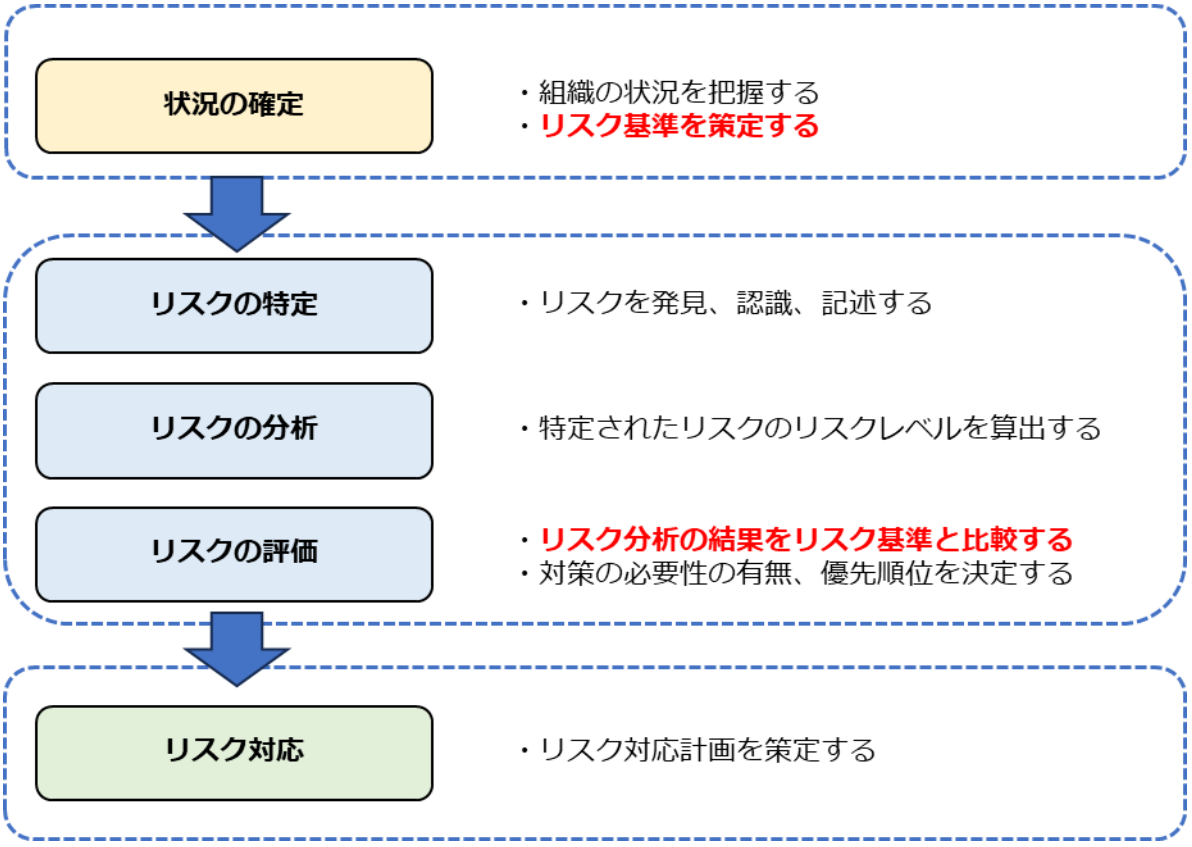
12-2. リスクマネジメント：リスクアセスメント

12-2-1. リスク基準の確立

必要なリスク基準

リスクアセスメントを実施するにあたって、リスクの重大性を評価するための目安となる条件を決める必要があります。その条件のことをリスク基準と言います。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」を含むよう明示されています。

リスク受容基準
どの程度のリスクであれば受け入れることが可能かの判断基準です。 あるリスクに対して、どの程度のレベル感や優先順位でリスク対応を実施するのか、リスクが顕在化した際にどの程度の大きさまでなら許容するのかを明確にする必要があります。
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
いつ、どのようなときにリスクアセスメントを実施するのかを決める要件です。 リスクアセスメントの実施条件や実施時期、タイミングや頻度などを明確にする必要があります。



12-2-2. リスクの特定

リスク特定

リスクアセスメントの 1 つ目のプロセスである「リスク特定」について説明します。リスク特定とは、「リスクを発見、認識及び記述するプロセス」[7]のことです。リスク特定を実施するために一般的に使用されるアプローチは「資産ベースのアプローチ」および「事象ベースのアプローチ」の 2 つがあります。

【情報セキュリティリスクの特定および記述】

アプローチ手法	概要	メリット	デメリット
資産ベースのアプローチ	● 資産、脅威及び脆弱性の検査を通じてリスクを特定しアセスメントを行う。 ● 資産は、その種類及び優先度にしたがって主要資産及び支援資産として特定できる。 ● 脅威は、資産の脆弱性につけ込み、対応する情報の機密性、完全性または可用性を侵害する。 ● 資産のリストを作成することが望ましい。	● 資産、脅威及び脆弱性のすべての有効な組み合わせを ISMS の適用範囲で列挙することができれば、理論上はすべてのリスクが特定される。	● 情報資産が増えたときに、資産のリストの行数が多くなる。 ● 同様のリスクを繰り返し記載したりしなければならない場合がある。
事象ベースのアプローチ	● 事象及び結果の評価を通じてリスクを特定し、アセスメントを行う。 ● 事象及び結果は、トップマネジメントから見た懸念、リスク所有者及び	● 詳細なレベルで資産を特定することに多大な時間を費やすことなく、高いレベルまたは戦略的なシナリオを確立することができる。	● 網羅性において、資産ベースのアプローチに劣る。

7 JISC 日本産業標準調査会「JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

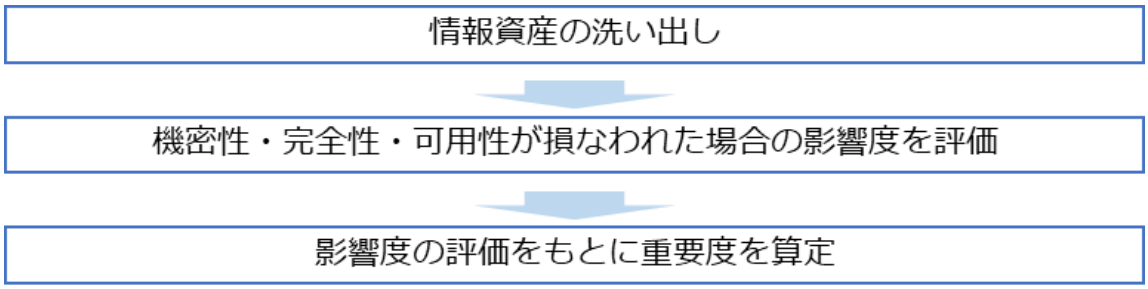
	組織の状況を決定する際に特定された要求事項によって発見できる。		

（出典）ISO/IEC「ISO/IEC 27005:2022」をもとに作成

リスク所有者の特定	● 特定されたリスクに対し、リスク所有者を関連付ける。 ● リスク所有者は、トップマネジメント、セキュリティ委員会、プロセス所有者、機能所有者、部門マネージャーおよび資産所有者など、リスクマネジメントに権限を持つ人とする（通常、組織内で一定の権限を持つ人が選ばれる）。

リスク特定（資産ベースのアプローチ）

資産ベースのアプローチでは、はじめに情報資産を洗い出し（資産目録の作成）、その過程でリスク所有者を特定します。リスク所有者とは、リスクが顕在化した際に責任を取る人のことを指します。その後、情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合、事業にどれほど影響があるか評価を行い、重要度を判断します。



情報資産の洗い出し（例）

情報資産の洗い出しでは、業務で利用する電子データや書類などを特定し、資産目録を作成します。洗い出した情報資産は、「営業」「人事」「経理」など管理部門ごとに分類します。企業活動に大きな影響を与えかねない重要な情報を、できる限り漏れないように洗い出すことが重要です。影響がほとんどない情報であれば、漏れても大きな問題はありません。情報資産の洗い出しの粒度は、細かすぎると管理が大変ですが、逆に粗いと次のリスク分析が難しくなります。そのため、適度な粒度にすることが重要です。以下は、情報資産のリストアップ例です。

No	情報分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先
1	人事	従業員名簿	従業員基本情報	人事部	人事部長	人事部	事務所PC

2	人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部長	人事部	書類
3	経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	経理部長	人事部	事務所 PC
4	経理	当社宛請求書	当社宛請求書の原本（過去 3 年分）	総務部	経理部長	総務部	書類
5	経理	発行済請求書控え	当社発行の請求書の控え（過去 3 年分）	総務部	経理部長	総務部	書類
6	営業	顧客リスト	得意先（直近 5 年間に実績があるもの）	営業部	営業部長	営業部	可搬電子媒体
7	営業	受注伝票	受注伝票（過去 10 年分）	営業部	営業部長	営業部	社内サーバ
8	営業	受注契約書	受注契約書原本（過去 10 年分）	営業部	営業部長	営業部	書類

資産目録の例

（出典）IPA「リスク分析シート」をもとに作成

電子化された情報を洗い出す際は、「普段パソコンで見ているこのデータは、どこに保存されているのだろう」というように、社内の IT 機器や利用しているクラウドサービスを思い浮かべて記入します。また、複数の組織を持つ企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

資産目録を作成する際、情報資産を情報、情報を支援する資産として「主要/事業資産」と「支援資産」2 つのカテゴリに分類して整理する方法も有効です。

「主要/事業資産」

「主要/事業資産」とは、「組織にとって価値のある情報又はプロセス」[8]のことです。主要資産は、「事業プロセス及び事業活動」と「情報」の 2 つに分けられます。

「事業プロセス及び事業活動」の例

- その損失又は低下によって、組織の使命達成が不可能となるプロセス
- 機密プロセス又は専有技術を伴っているプロセス
- 修正された場合、組織の使命の達成に大きく影響するプロセス
- 組織が契約、法令又は規則の要求事項を遵守するために必要となるプロセス

「情報」の例

8 ISO「ISO/IEC 27005:2022」 https://www.iso.org/standard/80585.html

- 組織の使命又は事業の遂行に不可欠の情報
- プライバシーに関する国内法に言う意味で、特別に定義することができる個人情報
- 戦略的方向性によって決定される目的の達成に必要となる戦略情報
- 収集、保管、処理、送信に長時間を要する高コスト情報および高い取得費用を伴う情報

「支援資産」

「支援資産」とは、「1 つ以上の事業資産の基礎となる情報システムの構成要素」[9]のことです。

「支援資産」の例

- ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織

（出典）MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

One Point

情報資産のグループ化

ISMS 適用範囲に存在する情報資産を洗い出す作業は、負荷が非常に大きくなりやすいです。そこで、資産価値や保管形態、保管期間や用途などが同じものを 1 つのグループとしてまとめて管理することにより、作業負荷を軽減したり、作業を効率化したりすることができます。

（例）事務所内のパソコンで会計ソフトウェアや表計算ソフトウェアを使って帳簿を作成している場合

- 仕訳帳
- 総勘定元帳
- 現金出納帳
- 当座預金出納帳
- 小口現金出納帳
- 仕訳帳
- 売上帳

情報資産名称：「会計データ」
「会計データバックアップ」
（バックアップを取っている場合）など

媒体・保存先：「事務所PC」（会計ソフトの保存先）
「可搬電子媒体」
（USBメモリがバックアップ保存先）

機密性・完全性・可用性が損なわれた場合の影響度を評価

情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合の事業への影響度を評価します。

具体例として、以下の評価基準を参考に「機密性」「完全性」「可用性」それぞれの評価値（3～1）を決定します。

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	個人情報（個人情報保護法で定義） 特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影	取引先から秘密として提供された情報 取引先の製品・サービスに関わる非

9 ISO「ISO/IEC 27005:2022」 https://www.iso.org/standard/80585.html

		響がある	公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	自社の独自技術・知識 取引先リスト 特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	自社製品カタログ ホームページ掲載情報
完全性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	個人情報（個人情報保護法で定義） 特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	取引先から処理を委託された会計情報 取引先の口座情報 顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	自社の会計情報 受発注・決済・契約情報 ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	廃版製品カタログデータ
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	顧客に提供している EC サイト 顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	製品の設計図 商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	廃版製品カタログ

情報資産の機密性・完全性・可用性に基づく重要度の定義

（出典）IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」をもとに作成

影響度の評価をもとに重要度を算定

重要度の算出例を説明します。重要度は「機密性」「完全性」「可用性」いずれかの評価値の最大値で判断します。なお、事故が起きると法的責任を問われたり、取引先、顧客、個人に大きな影響があったり、事業に深刻な影響を及ぼすなど、企業の存続を左右しかねない場合や、個人情報を含

む場合は、前項の算定結果に関わらず、重要度は 3 とします。

重要度	情報資産の価値・事故の影響の大きさ
3	事故が起きると、「法的責任を問われる」「取引先、顧客、個人に大きな影響がある」「事業に深刻な影響を及ぼす」など、企業の存続を左右しかねない
2	事故が企業の事業に重大な影響を及ぼす
1	事故が発生しても事業にほとんど影響はない

重要度の判断例：自社のホームページ（電子データ）		評価値
「機密性」	公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない	⇒ 1
「完全性」	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられたりすると顧客や閲覧者に被害が発生し、信用を失う	⇒ 3
「可用性」	サーバの障害などでアクセスできなくなると、来店客が減少し、売上も減少する	⇒ 3
➡完全性と可用性の評価値 3 が最大値なので、重要度は評価値：3		

重要度の判断例

（出典）IPA 「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」をもとに作成

One Point

重要度を判断する際のポイント

- 重要度の判断は、立場や見識によっても異なることがあるので、情報資産管理台帳に記入する前に「重要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。
- 情報資産の「重要度」は、時間経過とともに変化することがありますが、現時点の評価値を記入します。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。

リスク特定（事象ベースのアプローチ）

事象ベースのアプローチでは、従業者の業務プロセスを起点にリスクを特定します。それにより、詳細なレベルで資産を特定することに多大な時間を費やすことなく、戦略的なシナリオを確立することができます。その結果、組織は自らのリスク対応の取組を、重大なリスクに集中させることができます。

前述の資産ベースのアプローチに比べると網羅性に劣るというデメリットはありますが、その分、日々の業務をもとにして洗い出すため、現実的なリスクを洗い出すことができるというメリットがあります。また、資産ベースのアプローチの際、情報資産の洗い出しにより出てきた主要資産（事業プロセスおよび事業活動）に対しても、事象ベースのアプローチでリスク特定が可能です。

1.リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること（リスク）もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 （例） 「ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ」
2.リスク所有者の特定	1.で特定されたリスクの所有者を記載します。

リスク	評価値			重要度	リスク所有者
ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ	機密性	情報が漏えいする類の事象ではない	1	3	○○○○
	完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
	可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響を及ぼす事象である	3		

事象ベースのアプローチによるリスク特定の例

（出典）MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

上記内容でリスク特定を実施した後、特定されたリスクおよび「重要度」に対して後述のリスク分析を実施します。

12-2-3. リスクの分析

リスク分析（例）

特定されたリスクに対して「リスク分析」を行います。リスク分析とは、「リスクの性質を理解し、リスクレベルを決定するプロセス」[10]のことです。リスクレベル（リスクの大きさ）は、優先的・重点的に対策が必要な情報資産を把握するために使用されます。リスクレベル（リスクの大きさ）を算定するにはさまざまな方法があります。算定方法の一例を以下に示します。

10 JISC 日本産業標準調査会「JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

「リスクレベル」 ＝ 「重要度」（※リスク特定で算出方法を説明） × 「被害発生可能性」

被害発生可能性の算出方法

「被害発生可能性」とは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の 2 つの数値を「被害発生可能性の換算表」に当てはめて算出します。

起こりやすさ（脅威）		つけ込みやすさ（脆弱性）	
3	通常の状況で脅威が発生する（いつ発生してもおかしくない）	3	対策を実施していない（ほぼ無防備）
2	特定の状況で脅威が発生する（年に数回程度）	2	部分的に対策を実施している（一部対策を実施）
1	通常の状況で脅威が発生することはない（通常発生しない）	1	必要な対策をすべて実施している（対策を実施）

被害発生可能性の換算表		つけ込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

被害発生可能性の算出例

脅威の起こりやすさ：「2」、脆弱性のつけ込みやすさ：「2」

➡ 被害発生可能性は「1」：通常の状況で被害が発生することはない

脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「2」

➡ 被害発生可能性は「2」：特定の状況で被害が発生する（年に数回程度）

脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「3」

➡ 被害発生可能性は「3」通常の状況で被害が発生する（いつ発生してもおかしくない）

12-2-4. リスクの評価

リスク評価

リスク評価とは、「特定・評価したそれぞれのリスクが、受容可能か否かを評価するプロセス」のことです。リスク分析で算出したリスクレベルを、リスク基準（リスク受容基準）と比較し、リスク対策が必要か否か判断します。また、リスクレベルをもとに対策の優先順位をつけます。

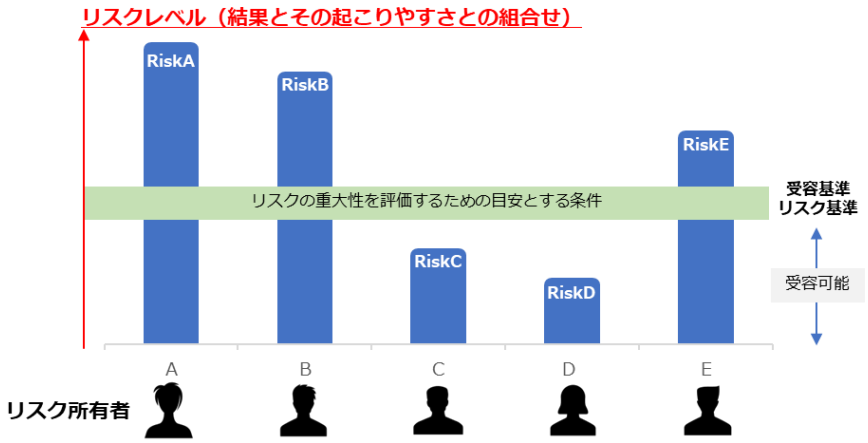


図 48. リスク評価の概要図

（出典）MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

リスク評価（例）

「重要度」 × 「被害発生可能性」でリスクレベルを算出し、リスク評価を行います。例として、算出したリスクレベルを以下の表に当てはめて行います。

リスクレベルの評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

※リスクレベル＝「重要度」×「被害発生可能性」

※赤色、黄色、青色の網掛けは以下のリスク受容基準を示す

リスク受容基準（例）

リスクレベル	リスク評価	記述
低（青）	そのままで受容可能	それ以上の活動なしにリスクを受容可能
中（黄）	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高（赤）	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい。そうでない場合、活動の

（出典）ISO/IEC「ISO/IEC 27005:2022」をもとに作成

		全部又は一部を拒否することが望ましい

また、情報セキュリティリスクの場合、以下の図で示す考え方をすることが多いです。以下の図では、発生頻度が高く被害が非常に大きいものについては「回避」、発生頻度は低いが被害が大きいものについては「移転」、発生頻度は高いが被害が大きくないものについては「低減」を検討するという考え方を示しています。

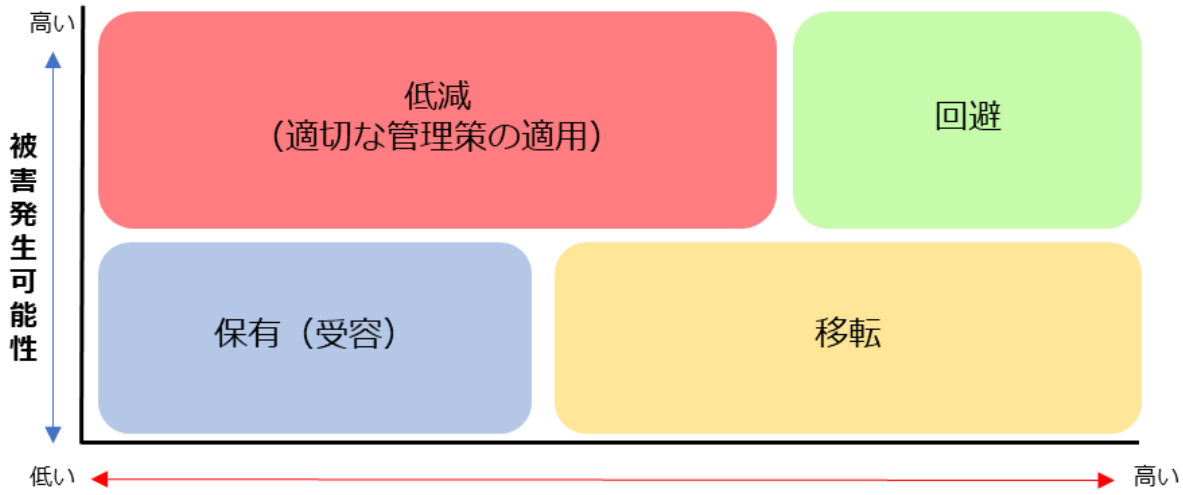


図 49. 情報セキュリティリスクの考え方

（出典）JNSA「2-4 リスクアセスメントとリスク対応」 https://www.jnsa.org/ikusei/01/02-04.html

12-3. リスクマネジメント：リスク対応

リスク対応プロセス

リスク対応とは、「リスクを修正するプロセス」[11]のことです。リスクアセスメントプロセスの結果に基づいており、リスク基準に基づき対応すべき優先順位づけされたリスクに対応する内容となります。

1. 適切な情報セキュリティリスク対応の選択肢の選定	
リスク対応の選択肢は以下の通りです。	
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。例えば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して自分たちの責任範囲外にし、リスクが顕在化したときの損失を他者に引き受けさせることです。例えばクラウドサービスのサーバを利用することによって、サーバが破壊されたり盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。
2. 情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策の決定	
ISO/IEC 27001:2022 の附属書 A、ISO/IEC 27017 などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な全ての管理策を決定します。	
3. 決定した管理策と ISO/IEC 27001:2022 附属書 A の管理策との比較	
必要な全ての管理策を、ISO/IEC 27001:2022 附属書 A に挙げられている管理策と比較します。	
4. 適用宣言書の作成	
必要な全ての管理策と、その理由及び実施状況を文書化します。適用宣言書に含まれる全ての	

11 JISC 日本産業標準調査会「JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

管理策の実施状況は、“実施された”、“一部実施された”または“実施されていない”として記述できます。

5. 情報セキュリティリスク対応計画

組織がリスクに対応する必要性を含んだリスク対応計画を作成します。リスク対応計画とは、組織のリスク受容基準を満たすようにリスクを修正するための計画のことです。
組織の必要な管理策を実施するためのプロジェクト計画とは、リスクを修正するために管理策が環境と相互にどのように作用するかを記述した設計計画のことです。

6. リスク所有者による承認

リスク所有者は、リスク対応計画を承認します。

7. 残留している情報セキュリティリスクの受容

リスク所有者は、残留リスクが受容可能か否かを判断し、決定します。

（出典）ISO/IEC「ISO/IEC 27005:2022」をもとに作成

リスク対応プロセス（例）

例：自社のホームページ（電子データ）

リスクの内容

不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失ったりする

リスク対応

リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）

対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する
対応する管理策：5.15 アクセス制御

対策基準の策定（対策基準の例）

技術的対策

- 公開サーバへの不正アクセス対策
- 公開サーバへのアクセス権の最小化と管理の強化
- 多要素認証の設定の有効化

残留リスク

残留リスクとは、「リスク対応後に残っているリスク」[12]のことです。残留リスクを受容するためには、リスク所有者の承認が必要になります。受容可能だと判断された残留リスクであっても、資産の価値や脅威、脆弱性など環境の変化に合わせて、リスクレベル（リスクの大きさ）を見直し、必要に応じて追加のリスク対応を行う必要があります。

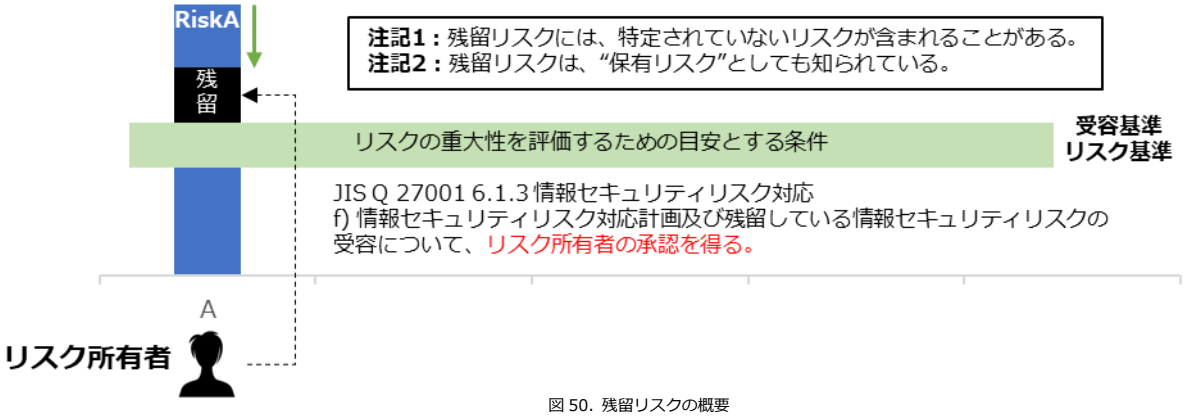


図 50. 残留リスクの概要

（出典）MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

12 JISC 日本産業標準調査会」JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

編集後記

第 6 編では、①ISMS をはじめとしたサイバーセキュリティ対策における代表的なフレームワーク、②リスクマネジメントやリスクアセスメントの手法、リスク対応の考え方について説明しました。

セキュリティ対策はやみくもに進めると、対策が複雑になり、余計に手間がかかり、内容に抜け漏れが発生する可能性があります。漏れなく効果的に対策を実施するために、セキュリティフレームワークを使用し、自社の課題・目的に即した対応方針を選択する必要があることを、11 章を通じて理解していただければと思います。

組織を取り巻く環境や組織が持つ情報資産の変化に応じてリスクもまた流動的に変化するため、リスクマネジメントプロセスを繰り返し実施していくことが重要です。リスクマネジメントはセキュリティ対策にとって欠かせないものですが、顕在化していないリスクについて考えることは、容易ではありません。リスクマネジメントプロセスにおける各段階での考え方や手法、フレームワークを用いることにより、円滑なリスク特定、分析と対応策の検討を実施できることを、12 章を通じて理解していただければと思います。

次回は、Lv.3 網羅的アプローチで使用する ISMS の要求事項や構築などについて説明します。

引用文献

ISMS-AC ISMS 適合性評価制度

https://isms.jp/doc /JIP-ISMS120-62.pdf

経済産業省 サイバーセキュリティ経営ガイドラインと支援ツール

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

経済産業省 クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性

https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf

JIPDEC「個人情報」と「プライバシー」の違い

https://privacymark.jp/system/course/theme1/03.html

ISMS-AC ISMS とは

https://isms.jp/isms/

デジタル庁 政府情報システムにおける サイバーセキュリティフレームワーク導入に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf

経済産業省　サイバー・フィジカル・セキュリティ対策フレームワークの概要

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.pdf

経済産業省 サイバーセキュリティ経営ガイドライン Ver3.0

https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

ISO/IEC「ISO/IEC 27005:2022」

https://www.iso.org/standard/80585.html

IPA 中小企業の情報セキュリティ対策ガイドライン第 3.1 版

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

JISC 日本産業標準調査会 JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語

https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

中小企業の情報セキュリティ対策ガイドライン第3.1版付録7リスク分析シート（全7シート）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
MSQA ISMS推進マニュアル活用ガイドブック 2022年 1.0版
https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd
JNSA 2-4 リスクアセスメントとリスク対応
https://www.jnsa.org/ikusei/01/02-04.html

参考文献

The NIST Cybersecurity Framework (CSF) 2.0

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Small Business Quick-Start Guide

https://doi.org/10.6028/NIST.SP.1300

A Guide to Creating Community Profiles

https://doi.org/10.6028/NIST.CSWP.32.ipd

Quick-Start Guide for Creating and Using Organizational Profiles

https://doi.org/10.6028/NIST.SP.1301

Quick-Start Guide for Using the CSF Tiers

https://doi.org/10.6028/NIST.SP.1302.ipd

Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)

https://doi.org/10.6028/NIST.SP.1305.ipd

Enterprise Risk Management Quick-Start Guide

https://doi.org/10.6028/NIST.SP.1303.ipd

CSF 2.0 Informative References

https://www.nist.gov/informative-references

CSF 2.0 Implementation Examples

https://www.nist.gov/document/csf-20-implementations-pdf

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

サイバー攻撃被害に係る情報の共有・公表ガイダンス

https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

用語集

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画。

11-5-1

■CSIRT（シーサート）

Computer Security Incident Response Teamの略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う。

11-5-1、11-5-3

■IoT（アイ・オー・ティー）

Internet of Thingsの略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと。

11-4

■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組。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。

11-1-1、11-1-2、11-2、11-3-1、11-3-3、11-4、11-5-1、12-1-3、12-2-1、12-2-2、

■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。

11-1-1、11-1-2、11-3-1、11-3-2、11-3-3、11-4

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度。

11-5-1

■Society5.0

日本が目指すべき未来社会の姿として、平成28年に閣議決定された「第5期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている。

11-1-1、11-1-2、11-4

■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。

11-3-1、12-3

■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。

12-2-2

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口やATMに出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる。

12-1-2

■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。

11-2

■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分野では、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。

12-2-2、12-3

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性。

11-1-2、11-2、12-2-2

■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。

11-1-2、11-2、12-2-2

■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。

11-1-2、11-2、12-2-2

■限定提供データ

不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、および管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。

12-2-2

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに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ートフォンから、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。デジタル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。

11-1-1、11-1-2、11-4、11-5-1、11-5-2、11-5-3、12-2-2

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク。

11-1-1、11-1-2、11-4

■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。

11-3-1、11-3-2、11-4、11-5-1、11-5-2

■情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報。

11-3-1、11-5-1、12-1-1、12-1-2、12-2-2、12-2-3

■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。

11-2

■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。

11-1-1、11-2、11-4

■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。

12-1-2、12-2-2、12-2-3、12-3

■責任追跡性

情報資産に対する参照や変更などの操作を、どのユーザーが行ったものかを確認することができる特性。

11-2

■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。

11-3-1、11-5-1

■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。

11-5-1

■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。

12-3

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードをCD（コンパクトディスク）にすること

がデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである。

11-4

■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。

11-2

■否認防止

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性。

11-2

■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。

12-2-2、12-3

■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。

11-1-1、11-1-2、11-2、11-3-1、11-4

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論。

11-1-1、11-3-1

■マルウェア

パソコンやスマートフォン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。

12-2-2

■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。

11-5-1

■リスクアセスメント

企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外は何らかのセキュリティ対策を講じる必要がある。

11-3-1、12-1-1、12-1-2、12-2-1、12-2-2、12-3

■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。

12-2-4、12-3

東京都産業労働局