令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

組織として策定すべき対策基準及び
情報セキュリティの三大要素【対策基準レベル①】

サイバーセキュリティ
人材育成
社内体制整備支援

目次

第8章. セキュリティ対策基準の策定

8-1. 対策基準の策定

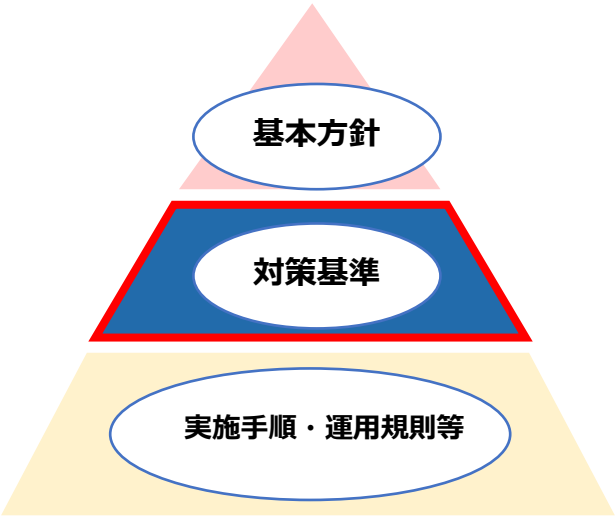
章の目的
第8章では、ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法について理解することを目的とします。

主な達成目標
◘ サイバーセキュリティ対策における複数のアプローチ方法と、それぞれのアプローチ手法の特徴について理解すること ◘ 各アプローチ手法について理解し、どのアプローチ手法を実施するべきか選択できるようになること

8-1-1. セキュリティ対策基準の概要

情報セキュリティポリシーは、一般的に「基本方針」「対策基準」「実施手順・運用規則等」で構成されます。「基本方針」には、組織や企業の代表者による情報セキュリティに対する考え、必要性、取り扱い方針などの宣言が含まれます。「対策基準」には、各業務や部署におけるセキュリティ対策をまとめた規定を記載します。「実施手順」には、対策基準ごとに、対策内容を具体的な手順として記載します。

以下では、「対策基準」策定方法の考え方について、説明します。



基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

図42. セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”.
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_04-3.html,(参照 2023-08-21).

対策基準を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たすことができます。ただし、対策基準で記載する内容は抽象度が高いため、具体的に実践で使用することは難しい内容です。実際に運用を行うためには、策定した対策基準に従って、実施手順などを作成する必要があります。

対策基準の内容を定める際は、網羅的なフレームワークを参考にすることが推奨されます。企業の現状、目標に応じてフレームワークを使用せずに段階的な対策基準の策定を行う場合は、「3-4-1. サイバーセキュリティアプローチ方法の概要」記載のアプローチ方法を参考にすることができます。アプローチ方法はレベルが上がるにつれ、網羅性も上がります。それぞれの特徴を次ページで説明します。

対策基準を策定するためのアプローチ方法

Lv.1
クイックアプローチ
（インシデントベース）

Lv.2
ベースラインアプローチ
（ガイドライン・ひな形ベース）

Lv.3
網羅的アプローチ
（フレームワークベース）

8-1-2. 対策基準策定のアプローチ方法

クイックアプローチ、ベースラインアプローチ、網羅的アプローチの概要、主な特徴と想定される適用ケースを説明します。

アプローチ手法	特徴	想定される適用ケース
Lv.1 クイックアプローチ	即時の対応や緊急事態への対処に適したアプローチ手法。 様々なインシデント事例内容を参考にし、対策基準を策定。	自社で発生する可能性が高い、または、発生したときの被害が大きいと考えられるインシデントに対処する場合。
Lv.2 ベースラインアプローチ	組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。 ガイドラインやひな形を参考とし、対策基準を策定。	組織的に一定以上の対策基準を策定する場合。
Lv.3 網羅的アプローチ	脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法。 ISMSなどの認証が可能なレベルを目指して、対策基準を策定。	ISMSのフレームワークに沿った対策基準を策定する場合。

メリット・デメリット

アプローチ手法	メリット	デメリット
Lv.1 クイックアプローチ	• 小規模な対策や修正を迅速に実施可能。 • 低コストでリスクを軽減。 • 進行中の攻撃の拡大や影響を最小限に抑えられる。	• 詳細な分析や検討が不十分な場合がある。 • 短期的な解決策に偏りがちになる。
Lv.2 ベースラインアプローチ	• 組織全体で一貫性を確保できる。 • 最低基準となるセキュリティ対策を講じることができる。	• 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
Lv.3 網羅的アプローチ	• 可能な限り多くの脅威や攻撃手法に対して対策を講じる。 • 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持できる。	• 全体的な実施には時間がかかる。

8-1-2. 対策基準策定のアプローチ方法

Lv.1 クイックアプローチ

Lv.1 クイックアプローチでは、様々なインシデント事例内容を参考にします。インシデント事例は、報道される事例、情報セキュリティ10大脅威、実際のインシデントなどから選択します。自社で発生する可能性が高いと考えられるインシデント事例や、実際に発生したときの被害が大きいと考えられるインシデント事例を参考にして、対策基準を策定することが重要です。以下は、情報セキュリティ10大脅威の『組織』に対する脅威で3年連続第1位になっている、ランサムウェアに対する対策基準の例です。

対策基準（例）

1. 対象とする脅威
ランサムウェアによる情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取等

2. 組織的対策
- 組織としてのランサムウェア対応体制の確立 ・インシデント対応体制を整備し対応する

3. 人的対策
- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- 提供元が不明なソフトウェアを実行しない
- 適切な報告/連絡/相談を行う

4. 物理的対策
- 適切なバックアップ運用を行う

5. 技術的対策
- 公開サーバーへの不正アクセス対策
- 共有サーバー等へのアクセス権の最小化と管理の強化
- 多要素認証の設定を有効にする
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

(出典) IPA「情報セキュリティ10大脅威 2023」を基に作成

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ10大脅威 2023	https://www.ipa.go.jp/security/10threats/10threats2023.html
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
マルウェア「ランサムウェア」の脅威と対策（対策編）	https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

8-1-2. 対策基準策定のアプローチ方法

Lv.2 ベースラインアプローチ

Lv.2 ベースラインアプローチでは、ガイドラインやひな形を参考とし、対策基準を策定します。IPAの「中小企業の情報セキュリティ対策ガイドライン」や以下の【参照資料】を活用することで、自社にあった対策基準を策定することできます。

【参照資料】
・リスク分析シート（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版（出典：IPA）
・情報セキュリティ関連規程（出典：IPA）
・自己点検チェックリスト（出典：個人情報保護委員会）

IPA「情報セキュリティ関連規程（サンプル）」を活用した対策基準（例）

1	組織的対策	改訂	20yy.mm.dd
適用範囲	全社・全従業員		

1.情報セキュリティのための組織
情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。

（出典）IPA「情報セキュリティ関連規程（サンプル）」を基に作成

詳細理解のため参考となる文献（参考文献）	
リスク分析シート	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
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/about.html
情報セキュリティ関連規程	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx
自己点検チェックリスト	https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

8-1-2．対策基準策定のアプローチ方法

Lv.3 網羅的アプローチ

Lv.3 網羅的アプローチでは、ISMSなどの認証が可能なレベルを目指して、対策基準を策定します。そのため、ISMSのフレームワークに沿って、技術的対策といった一部の内容ではなく、運用や監査についても対策基準に記載します。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティポリシーサンプル改版（1.0版）	https://www.jnsa.org/result/2016/policy/

第9章. 管理策のテーマと属性

9-1. 管理策の分類と構成

章の目的
第9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

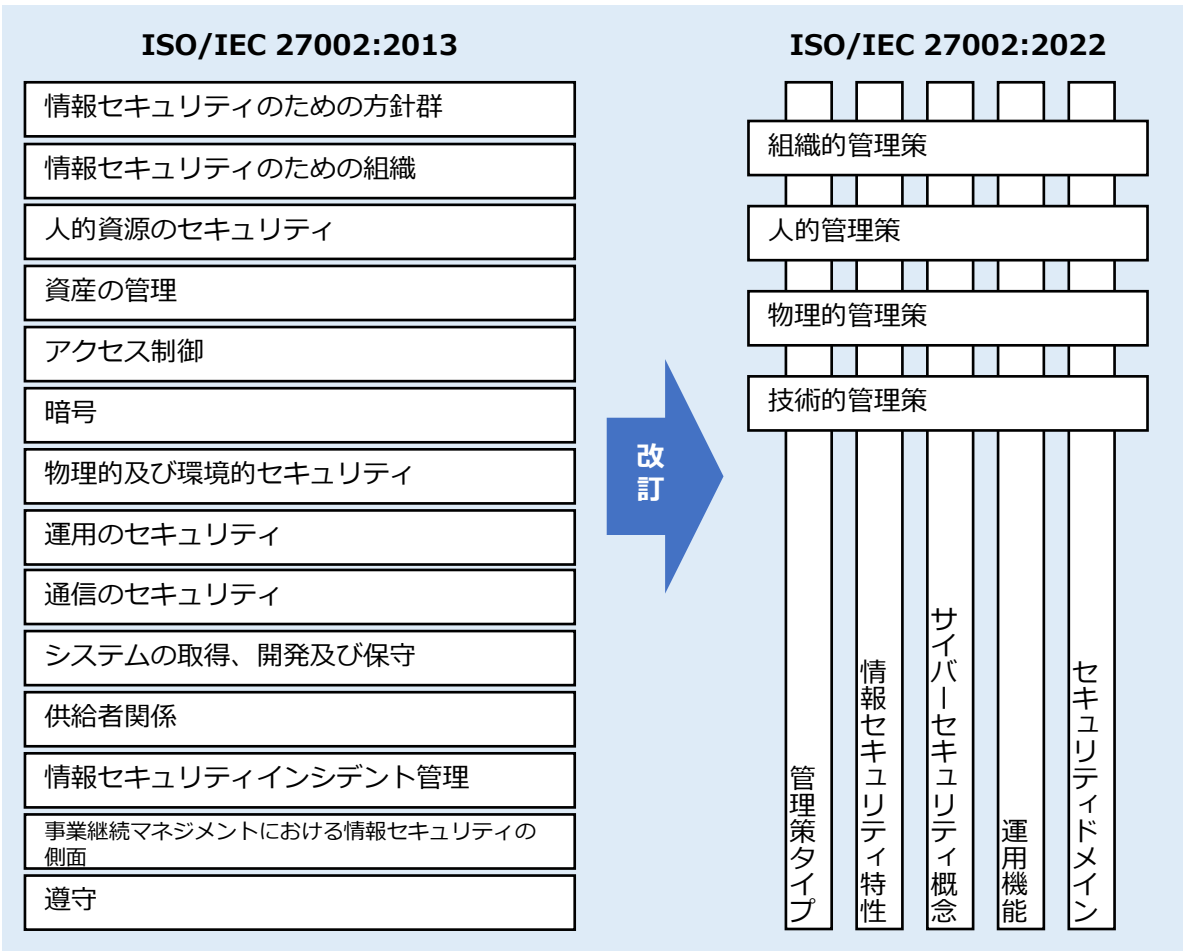
9-1-1. 管理策：ISO/IEC 27002

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、リスク対応のための対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、全管理策への目的の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つの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で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つけられています。 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。



9-1-2. 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。管理策の分類は様々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等
管理策タイプ	予防、検知、是正	―
情報セキュリティ特性	機密性、完全性、可用性	**ISO/IEC 27001**
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、法および遵守、情報セキュリティ事象管理、情報セキュリティ保証	**ISO/IEC 27002:2013**
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	―

9-1-2. 管理策のテーマと属性

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

9-1-2. 管理策のテーマと属性

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

第10章. 脅威、脆弱性、リスクの定義と関係性

10-1. 用語の定義および関係性と識別方法

章の目的
第10章では、ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を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

10-1-1. 用語の定義と関係性

企業や組織には様々なセキュリティ上の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するには、リスクマネジメントを行う必要があります。

リスクマネジメントを理解するために必要となる「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を説明します。次に、リスクを増大させる要因となる「脅威」や「脆弱性」の識別方法を説明します。

主な用語の定義

- ✓ **脅威**：システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。例えば、不正アクセス、DDoS攻撃のような意図的な人為的脅威、機器の故障や操作ミスのような偶発的な人為的脅威、地震や洪水のような環境的脅威がある。
- ✓ **脆弱性**：1つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。例えば、セキュリティホールと呼ばれるソフトウェアの欠陥・不具合。
- ✓ **情報資産の重要度**：機密性・完全性・可用性が損なわれた場合の事業に対する影響や、法律で安全管理義務があるなどの観点から、情報資産の重要度を判断する。
- ✓ **セーフガード（管理策）**：リスクを修正する対策。具体的には、リスクを除去あるいは許容できる範囲に制御するための手順や仕組みのこと。
- ✓ **リスク**：目的に対する不確かさの影響。情報セキュリティにおいては、脅威が組織に損害を与える可能性。
- ✓ **リスク値**：リスクの大きさのこと。「情報資産の重要度」と「機密性・完全性・可用性を損なう事象の発生確率」の積で求められる。

脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係を分かりやすく図で表すと以下のようになります。

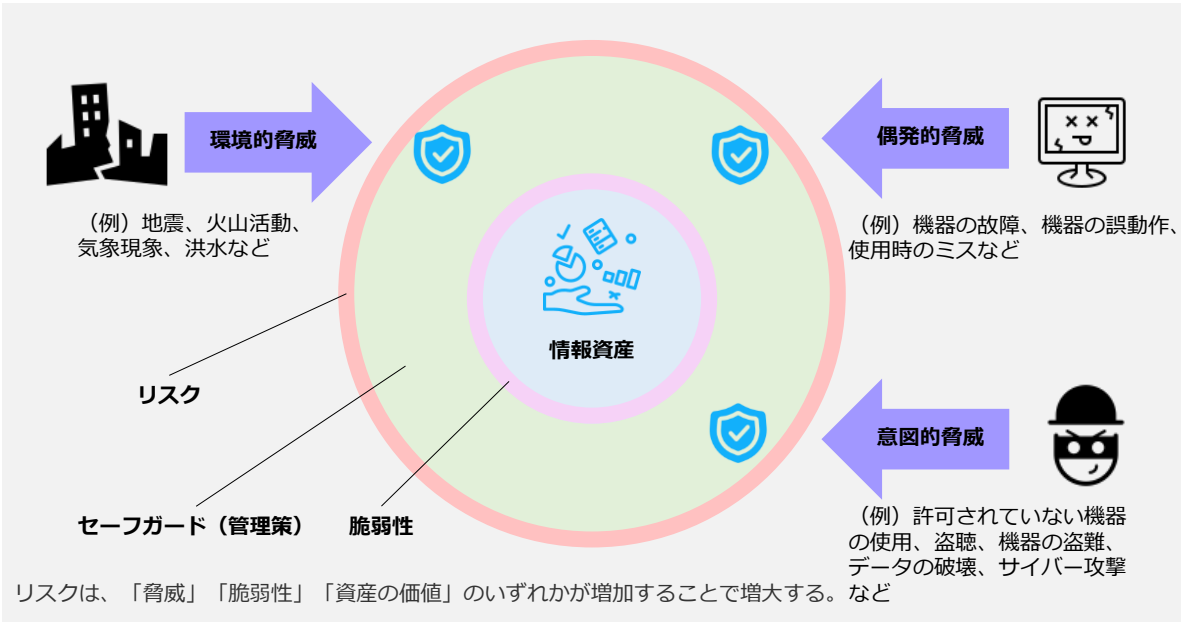


図43.脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係

10-1-1. 用語の定義と関係性

（例）業務用ノートパソコン

業務用ノートパソコンに関する脅威や脆弱性、管理策の関係について説明します。

資産	ノートパソコン内の情報
価値	営業の業務で必須の情報
脅威	社外への持ち出しによるノートパソコンの紛失
リスク	盗難による情報漏えい
脆弱性	不適切なパスワードの設定（例）わかりやすいパスワード：名前、社員番号、生年月日など
保護要求事項	• 権限のないものがログインできないようにする • 不要な持ち出しを防ぐ
管理策	• 複雑なパスワードの設定（8.5 セキュリティを保った認証） • 社外の持ち出し管理（7.9 構外にある装置及び資産のセキュリティ（構外にある資産））

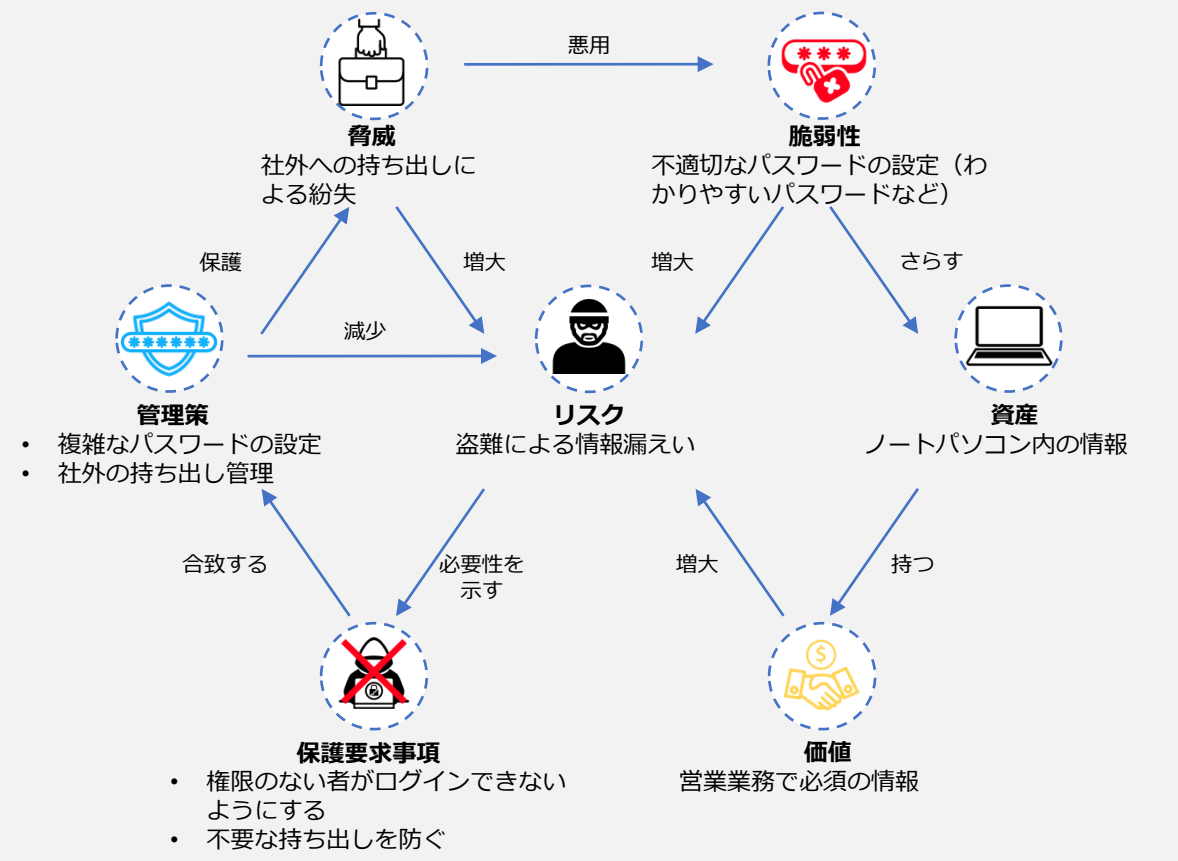


図44. 脆弱性、リスクの関係の事例

上記の図では「脅威」「脆弱性」「資産の価値」のいずれかが増加することで、リスクが増大することが示されています。リスクを減少させるためには、まず「脅威」、「脆弱性」、「資産の価値」を識別し、リスクに対する保護要求事項を明らかにします。そして、保護要求事項に合致するセーフガード（管理策）を適切に実施することが必要です。

10-1-2. 脅威の識別

脅威の識別

脅威は「脆弱性」につけいり顕在化することで、組織に損失や損害を与える事故を生じさせます。脅威を、人為的脅威（意図的脅威、偶発的脅威）と環境的脅威に区別して把握することで、必要なセキュリティ対策を整理しやすくなります。

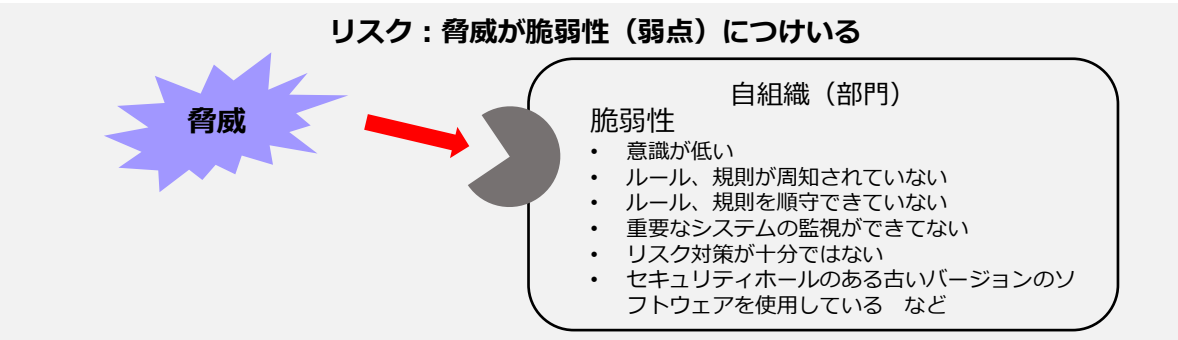


図45. 脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

類型	脅威	原因
物理的損傷	火災、水害、汚染、大事故、機器や媒体の破壊、粉塵、腐食、凍結	A/D/E
自然現象	気候、地震、火山活動、気象現象、洪水	E
重要なサービスの喪失	空調や給水システムの故障/電気通信機器の故障	A/D
	電力供給の停止	A/D/E
情報を危うくすること	遠隔スパイ行為、盗聴、媒体や文章の盗難、機器の盗難、再利用又は廃棄した媒体からの復元、ハードウェアの改ざん、位置検知	D
	漏洩・信頼できない情報源からのデータ・ソフトウェアの改ざん	A/D
技術的な故障	機器の故障、機器の誤動作、ソフトウェアの誤作動	A
	情報システムの飽和、情報システムの保守に関する違反	A/D
認可されていない行為	許可されていない機器の使用、ソフトウェアの不正コピー、データの破壊、データの違法な処理	D
	海賊版又は（不正）コピーソフトウェアの使用	A/D
機能を危うくすること	使用時のミス	A
	権限の乱用/権限の詐称	A/D
	要員の可用性に関する違反	A/D/E

A：偶発的脅威（Accidental）　D：意図的脅威（Deliberate）　E：環境的脅威（Environmental）

脅威の一覧表の例
（出典）「ISO/IEC 27005」を基に作成

10-1-2. 脅威の識別

脅威を洗い出すには自組織にある資産に対する脅威を識別して、前ページのようなリストを作成します。その際には、利用者や他の事業部の関係者、外部の専門家などから得られる、脅威に関する情報を活用することが大切です。

脅威の洗い出しの考え方として、意図的脅威は、攻撃の動機や必要なスキル、利用可能なリソースを考慮しつつ、資産の特性や魅力、脆弱性などから、どのような要因が脅威となるかを識別できます。一方で偶発的脅威は、環境や気候、人為的なミスや誤動作などから影響を及ぼす可能性を識別できます。

脅威の種類		想定される被害とセキュリティ対策
環境的脅威 (Environmental → E)		環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復する対策を重視する、などのセキュリティ対策が選択されることになります。
人為的脅威	**意図的脅威 (Deliberate → D)**	「（内部者が企業秘密を）漏洩する」という脅威が考えられます。この様な脅威については、当該行為が犯罪行為（不正競争防止法違反）であり、罰せられること、会社は企業規則により漏洩者を罰すること、場合によっては損害賠償請求を行うということを規程で明確に示し、教育を実施するという抑止的な対策が有効になります。漏洩を早期に検知するといった対策も重要になります。
	偶発的脅威 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じない様に、二回ずつ入力する、一定の範囲の値しか入力できない様にする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。

脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

10-1-3. 脆弱性の識別

脆弱性の識別

脆弱性があるだけでインシデントが発生するわけではありません。しかし、脆弱性は脅威を顕在化させ、インシデントの発生確率を高める可能性があります。脆弱性を減らすためには、適切な管理策を実施する必要があります。脆弱性は管理策の欠如を同時に意味しているため、脆弱性を識別することは必要な管理策を識別するのに役立ちます。例えば「アクセス権の誤った割当て」という脆弱性は、「アクセス権の適切な設定」という管理策の欠如を意味しています。

以下は、脆弱性を識別して一覧表にした例です。脆弱性の一覧表を作成する際は、脅威と関連付けて整理する必要があります。

類型	脆弱性の例	脅威の例
ハードウェア	記憶媒体の不十分な保守/不適当な設置	システムの保守に関する違反
	定期的な交換計画の欠如	機器や媒体の破壊
	湿気、ホコリ、汚れに対する影響の受けやすさ	粉塵（ダスト）、腐食、凍結
	有効な構成変更管理の欠如	使用時のミス
	電圧の変化に対する影響の受けやすさ	電力供給の停止
	温度変化に対する影響の受けやすさ	気象現象
	保護されない保管	媒体や文書の盗難
	廃棄時の注意の欠如	媒体や文書の盗難
	管理されないコピー作成	媒体や文書の盗難
ソフトウェア	監査証跡の欠如	不正アクセス
	アクセス権の誤った割当て	不正アクセス
	複雑なユーザインタフェース	使用時のミス
	文書化の欠如	使用時のミス
	ユーザの識別及び認証メカニズムの欠如	不正アクセス
	不十分なパスワード管理	不正アクセス
	不要なサービスが実行可能	データの違法な処理
	効果的な変更管理の欠如	ソフトウェアの誤作動
	管理されてないソフトウェアのダウンロード及び使用	恐怖。攻撃，妨害行為
	バックアップコピーの欠如	装置又はシステムの故障

脆弱性の識別例
（出典）「ISO/IEC 27005」を基に作成

脆弱性を識別する際に参考になる情報

- ISO/IEC 27001:2022の附属書A「管理目的及び管理策」
- ISO/IEC 27002:2022の管理策
- 情報セキュリティ管理基準　など

脆弱性は、資産の性質から考えることで簡単に識別できます。例えば、クラウドサービスは、「インターネットがあればどこでも利用可能」、「自社でデータを持たなくていい」といった性質を持ちます。同時にそれらの性質は「不正アクセス」「クラウドサービス停止によるデータの消失」という脅威に対する脆弱性があります。

コラム

情報セキュリティのCIA＋4要素

JIS Q 27000:2019で、情報セキュリティは「機密性（Confidentiality）」、「完全性（Integrity）」及び「可用性（Availability）」を維持することと定義されています。これら３つの要素（CIA）をバランスよく維持することは、セキュリティを担保する上では欠かせません。また、さらに以下の4つの要素を追加して、情報セキュリティの7要素とする場合もあります。より高度なISMSの構築につながる要素のため、ここで紹介します。

〇真正性 (Authenticity)
情報にアクセスする人や端末が「本当に許可されているかどうか」を確実にすることを指します。多要素認証やデジタル署名など、認証方法を強化することが対策として考えられます。

〇信頼性 (Reliability)
データやシステムを利用する際、意図した動作と結果が得られることを担保することを指します。不具合がないようにシステム構築を行うことや、ヒューマンエラーが起きないようなルール整備などが対策として考えられます。

〇責任追跡性 (Accountability)
情報へのアクセスが、誰によってどのような手順で行われたのかを後から証明できるようにしておくことを指します。ログの取得や、デジタル署名などが対策として考えられます。

〇否認防止性 (Non-repudiation)
問題発生後に、その原因となった人物から否定されないよう、後から証明できるようにしておくことを指します。先に説明した責任追跡性を担保することが対策につながります。

CIAの3要素だけでなく、上記の4要素も加えることで、より抜け漏れがないセキュリティ対策が期待できます。

編集後記

セミナーの5日目では、以下の内容について解説しました。（セキュリティポリシーの概要とサイバーセキュリティ対策のアプローチ方法、ISMSの管理策の概要、リスクマネジメントに関する用語について）このセミナーを通じて、状況に応じて適切なサイバーセキュリティ対策のアプローチ手法を選択できるようになり、またISMSの管理策の構造やリスクマネジメントで使用される用語を理解していただければと思います。

本テキストでは、最初にセキュリティポリシーの構成（「基本方針」「対策基準」「実施手順・運用規則等」）について説明しました。そして、企業が現在の状況や目標に合わせた「対策基準」を策定する際に活用できる、レベル感の異なる3つのアプローチ手法（ Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチ）を紹介しました。

その後、ISMSの管理策を示した規格であるISO/IEC 27002について説明しました。具体的には、ISO/IEC 27002に記載されている93の管理策は、テーマと呼ばれる4つのカテゴリ（「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」） に分類されることを説明しました。また、各管理策に属性というものが付与されたことで、管理策のフィルタリング、並び替え、提示がしやすくなったことを説明しました。

最後に、次回解説するリスクマネジメントを理解するために必要となる「リスク」、「脆弱性」、「脅威」といった用語の定義と関係性、さらに「脅威」、「脆弱性」の識別方法について説明しました。脅威や脆弱性、リスクなどの関係性は、図を用いて表し、具体例も合わせて説明しました。 また、「脅威」、「脆弱性」を識別し、一覧表を作成するための考え方を説明しました。

次回は、リスク基準の策定から、リスクマネジメントについて解説します。

（別紙）パスワードの作り方と管理方法

【複雑さを持つパスワードの作り方】

1. 単語ではなく、文章にする
　単語の場合、ディクショナリ検索でヒットする確率が上がるため、文章として考える

【例】
Cyber Security Keizoku Shien
↓
CyberSecurityKeizokuShien

2. 数字を入れる

CyberSecurityKeizokuShien0725

3. 単語の母音を削除し、読めなくする(aiueo)

CyberSecurityKeizokuShien0725
↓
CybrScrtyKzkShn0725

4. 特殊記号を数文字入れる
　#、%、@を単語の区切りに入れる

CybrScrtyKzkShn0725
↓
Cybr**#**Scrty**%**Kzk**@**Shn0725

5. サービス識別文字を入れる

【例】
　Tokyo ： t5
t5Cybr#Scrty%Kzk@Shn0725

6. 自分にしかわからない固定文字を入れる

　例　イニシャル
　　SH　→　$H
$Ht5Cybr#Scrty%Kzk@Shn0725

メモはベース部分のみ

$Ht5Cybr#Scrty%Kzk@Shn0725

【認証方式と管理】

- パスワードマネージャー（ソフトウェア）
  複雑なパスワードを生成し、管理するためのソフトウェア。
  端末間の同期を行うことで、複数のデバイスで共有できる。
- ワンタイムパスワード
  定期的に更新され、1度しか使用できないパスワード。
  パスワードは、専用のデバイスやソフトウェアで確認できる。
- PINコード方式
  パスワードとは異なり、デバイスに対する認証となるため、ネットワーク上を流れることがない。
- 公開鍵方式のパスキー
  公開鍵と秘密鍵を用いた2種類の鍵ペアで認証を行う方式

引用文献

情報セキュリティポリシーの内容

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_04-3.html

情報セキュリティ10大脅威 2023

https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

情報セキュリティ関連規程

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

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

JISC「JIS Q 27000 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

国民のためのサイバーセキュリティサイト | 用語辞典

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/glossary/glossary_01.html

JIPDEC ISMSユーザーズガイド –JIS Q 27001:2014(ISO/IEC 27001:2013)対応- -リスクマネジメント編-

https://m-p-o.co.jp/mpo/wp-content/uploads/2020/05/b823443df9d0ab703dd07bd352244f1d.pdf

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

https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjoyNzA3NTgsImNhdGVnb3J5TnVtIjo3MDMwfQ==&pNo=1

MSQA ISMS推進マニュアル活用ガイドブック2022_第1.0版

https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjo3ODgwMSwiY2F0ZWdvcnlOdW0iOjEwNzI0fQ==&pNo=1

ISO/IEC 27005:2022

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

参考文献

情報セキュリティ10大脅威 2023

https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

サイバー攻撃対応事例

https://security-portal.nisc.go.jp/dx/provinatack.html

マルウェア「ランサムウェア」の脅威と対策（対策編）

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

リスク分析シート

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx

サイバーセキュリティ経営ガイドラインVer 3.0

https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf

情報セキュリティ関連規程

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

自己点検チェックリスト

https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

情報セキュリティポリシーサンプル改版（1.0版）

https://www.jnsa.org/result/2016/policy/

用語集

■AI
Artificial Intelligenceの略。「AI（人工知能）」という言葉は、1956年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。1950年代後半から1960年代が第一次AIブーム、1980年代が第二次AIブーム、現在は2000年代からはじまる第三次AIブームである。
「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている
…… 1-1-1、4-1-1、4-2-2、4-2-5、5-2-1、5-2-2、5-2-3、6-1-1、6-1-3

■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
…… 2-3-2

■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
…… 2-1-3、6-1-3、7-5-3

■DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attackの略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることで、過剰な負荷をかけてサービスを利用できなくする攻撃手法
…… 2-2-2、2-2-5、第一回コラム、7-4-4

■DFFT
Data Free Flow with Trustの略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している
…… 5-2-1

■EDR
Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する
…… 2-2-4、2-2-5、3-1-1、3-4-1

■eKYC
electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと
…… 5-2-1

■GビズID
行政手続きなどにおいて手続を行う法人を認証するための仕組み。1つのID・パスワードで本人確認書類なしに様々な政府・自治体の法人向けオンライン申請が可能になる
…… 5-2-1

■ICSCoE中核人材育成プログラム
2017年4月にIPA内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている
…… 2-1-2

■ICT
Information and Communication Technologyの略。IT（情報技術）だけでなく、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
…… 4-1-2、5-2-1、7-2-2、7-3-1

用語集

■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、家電など様々な「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
…… 1-1-1、2-1-2、2-2-2、4-1-1、4-2-5、5-2-2、5-2-3、6-1-2、7-4-3、7-4-4

■IPS
Intrusion Prevention Systemの略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。
IPSは、異常を検知した場合、管理者に通知するだけではなく、その通信を遮断する
…… 2-2-2、3-4-2

■IPアドレス
コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。 IPアドレスは、127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれら4つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加だけでなく、情報セキュリティ機能の追加などの改良も加えられている
…… 2-3-1、6-2-2

■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、法令的な対策を含む、経営者を頂点とした総合的で組織的な取組み。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
…… 3-3-1、7-1-1、7-1-2、7-2-2、7-2-3、7-3-1、7-3-4、7-4-1、8-1-2、9-1-1

■ITリテラシー
コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能
…… 3-1-1

■LockBit2.0
「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される
…… 2-3-2

■NISC
National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当
…… 5-2-1、6-1-3

■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、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本も今後普及が見込まれる
…… 3-3-1、7-1-1、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-3-4

■RPA
Robotic Process Automationの略。定型的な業務をソフトウェアのロボットにより自動化すること
…… 4-2-3

■SASE（サシー）
Secure Access Service Edgeの略。2019年に提唱したゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウド上で統合して提供するサービス、また、その考え方・概念
…… 2-2-4

用語集

■SBOM（エスボム）
Software Bill of Materialsの略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOMは、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOMは、ソフトウェアのリスクを把握・管理するのに役立つ
…… 6-1-1

■SDP
Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、全ての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う
…… 2-2-5

■SECURITY ACTION
中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度
…… 2-1-2、3-2-1

■Society5.0
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）
…… 1-1-1、4-1-1、5-2-2、6-1-1、7-1-1、7-4-1、7-4-2、7-4-3

■SWG
Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することでセキュアな通信環境を実現
…… 2-2-4

■UTM
複数のセキュリティ対策機能を1つに集約した製品のこと。ウイルスや不正アクセスなど外部からの脅威から、内部のネットワークを包括的に保護できる
…… 3-1-1

■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。このようにVPNを使用することで、ユーザは物理的な専用線で通信しているかのような安全な通信を行うことができる
…… 2-1-3、2-2-2、2-2-5、2-3-1、2-3-2、2-3-3

■WAF（ワフ）
Web Application Firewallの略。 従来のファイアウォールが、IPアドレスとポート番号で通信を制御していたことに対して、Webアプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと
…… 2-2-2

■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を制限する機能のこと
…… 2-2-5、第一回コラム、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、9-1-1

■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で、システムの再構築や運用改善の参考情報となる
…… 2-2-4、7-3-1、7-4-5

■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
…… 2-1-3、2-2-1、2-2-5、2-3-2、3-2-3、3-3-1、第一回コラム

■アンダーグラウンドサービス
合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス
…… 2-1-3

■インターネットバンキング
インターネットを利用した銀行や金融機関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込や残高照会などの取引を行うことができる
…… 3-2-2

用語集

■ウイルス定義ファイル（パターンファイル）
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの
…… 3-2-2、3-2-3

■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
…… 7-2-1

■エンドポイントデバイス
ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）
…… 2-2-4

■改ざん
文書や記録などの全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
…… 2-1-2、5-2-2、6-1-3、7-4-4、8-1-2

■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
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2

■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
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2

■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
…… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2

■クラッキング
悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為
…… 第一回コラム

■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を確保することを任務とする、独立した機関のこと。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う行政機関（組織的には内閣府の外局）
…… 2-2-3、5-2-1、6-2-1、8-1-2

■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様々である。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。
…… 2-1-2、2-1-3、2-2-2、2-2-5、2-3-2、3-3-1、4-1-1、4-3-1、4-3-2、5-2-2、5-2-3、6-1-1、6-1-2、6-1-3、7-1-2、7-3-4、7-4-1、7-5-2、7-5-3

■サイバーセキュリティお助け隊サービス制度
中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービス
…… 2-1-2

■サイバーセキュリティ戦略
組織や企業がセキュリティに関する目標を達成するための計画やアプローチ
…… 3-3-1、5-1-1、6-1-1

■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
…… 3-3-1、7-1-1、7-1-2、7-4-1、7-4-2、7-4-3、7-4-4、7-4-5

用語集

■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
…… 3-3-1、7-1-1、7-1-2、7-4-1、7-4-2、7-4-3、7-4-4、7-4-5

■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
…… 2-1-3、2-2-2、2-2-4、4-1-1、4-2-4、4-3-2、5-1-1、5-2-2、6-1-1、6-1-2、6-1-3、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-4-1、7-4-2、7-4-3、7-4-5、7-5-1、7-5-2

■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
…… 3-3-1、7-2-1、7-2-2、7-3-4、7-4-4、7-5-1、8-1-2

■情報セキュリティの3要素「CIA」
情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ
…… 第一回コラム、第五回コラム

■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
…… 2-1-3、第一回コラム、6-1-3、7-2-1、第五回コラム

■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
…… 第一回コラム、6-1-1、6-1-3、7-2-1、7-4-2、7-4-3、7-4-4 、第五回コラム

■スクリーンロック
デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない
…… 2-2-2

■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
…… 2-1-1、2-1-3、2-2-1、2-2-2、2-2-4、2-2-5、2-3-1、2-3-2、2-3-3、3-3-1、第一回コラム、6-1-3、7-2-2、7-4-4、7-4-5、9-1-2、10-1-1

■脆弱性診断
システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること
…… 2-3-1

■責任追跡性
情報資産に対する参照や変更などの操作を、どのユーザが行ったものかを確認することができる特性
…… 第一回コラム、7-2-1 、第五回コラム

■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
…… 2-1-1、2-1-2、2-1-3、2-2-1、4-1-1、7-2-2、7-3-1、7-4-4、9-1-1、9-1-2

■セキュリティ・キャンプ
情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している
…… 2-1-2

用語集

■セキュリティホール
情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある
…… 3-3-1

■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のが一般的
…… 2-1-1、2-2-1、3-3-1、6-1-2、7-4-4、8-1-1

■ゼロデイ攻撃
OSやソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと
…… 2-1-3

■ゼロトラスト
従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、全てのネットワーク通信を信用できない領域として扱い、全ての通信を検知し認証するという新しいセキュリティの考え方
…… 2-2-4、4-1-3

■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」
…… 2-2-5

■ダークウェブ
特別な手法でないとアクセスできない、匿名性の高い非公開のWebサイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている
…… 2-1-3

■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
…… 2-2-5、2-3-3、8-1-2、第五回コラム

■データサイエンス
数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること
…… 1-1-1

■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）にするのがデジタイゼーション、音楽をダウンロード販売するのがデジタライゼーションである
…… 1-1-1、2-1-1、2-2-1、3-3-1、4-1-2、4-2-3、5-1-1、6-1-1、6-1-3、7-4-3

■デジタル情報
0、1、2のような離散的に（数値として）変化する量
…… 第一回コラム

■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
…… 3-3-1、7-2-1、7-3-1

用語集

■ビジネスメール詐欺
攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromiseとも略される
…… 2-1-3

■ビッグデータ
全体を把握することが困難な程、膨大な規模のデータ群
…… 1-1-1、5-2-2、5-2-3

■否認防止性
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
…… 第一回コラム 、第五回コラム

■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付きメール（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
…… 2-1-2、2-1-3

■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
…… 2-2-4

■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様々である
…… 2-3-1、3-4-1、3-4-2

■不正アクセス
利用権限を持たない悪意のあるユーザが、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、2000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
…… 2-1-1、2-1-2、2-1-3、2-2-1、2-2-2、2-2-3、2-2-5、2-3-1、4-3-2、5-2-1、7-4-4、8-1-2

■踏み台
不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ
…… 2-1-3、4-3-2

■フォレンジック
犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組みを指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる
…… 2-2-3、2-3-2

■ブラックマーケット
広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するネット上の市場（闇市）
…… 2-1-3

用語集

■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様々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「ひな形」としてまとめたもの
…… 2-2-4、3-3-1、7-1-1、7-1-2、7-2-1、7-3-1、7-3-2、7-4-1、8-1-1、8-1-2、9-1-2

■ブロックチェーン
複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する仕組み
…… 1-1-1

■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よい成果をもたらす方法論
…… 2-1-3、2-3-1、7-1-1

■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
…… 2-2-2、2-2-4、2-2-5、第一回コラム、7-2-2

■ミラサポコネクト
ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤
…… 5-2-1

■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にアクセスできる
…… 3-2-3

■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
…… 2-1-2、2-1-3、2-2-1、2-2-2、2-2-5、2-3-2、2-3-3、7-5-1、8-1-2

■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対策を講じる必要がある
…… 3-3-1、7-3-1、7-4-5、第四回コラム

■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
…… 2-3-2、3-3-1、7-3-2、7-4-5

■リモートデスクトップ接続
パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法
…… 2-2-2

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業