令和６年度

中小企業サイバーセキュリティ

社内体制整備事業

第３編　これからの企業経営で必要な IT 活用とサイバーセキュリティ対策　【レベル共通】
第４編　セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施　【レベル 1】
第５編　各種ガイドラインを参考にした対策の実施　【レベル 2】

第7章. セキュリティ対策の概要（全容）

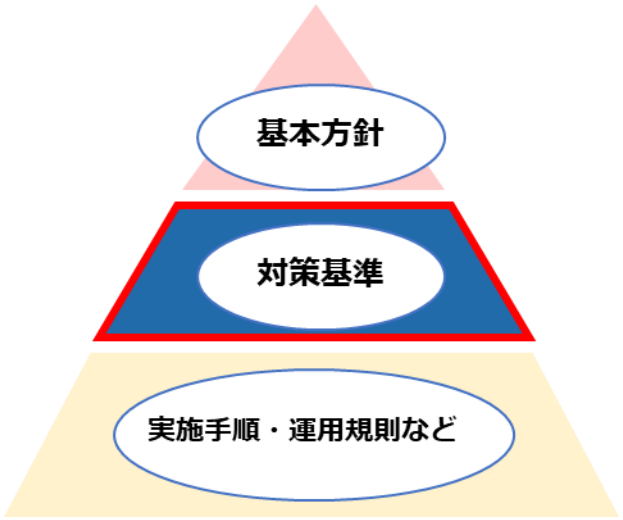
章の目的
第 7 章では、ISMS 認証を前提としたセキュリティ対策における基準を 3 段階にレベル分けし、各基準の手法について理解することを目的とします。
主な達成目標
◘ セキュリティ対策における複数のアプローチ方法と、それぞれのアプローチ手法の特徴について理解すること ◘ 各アプローチ手法について理解し、どのアプローチ手法を実施するべきか選択できるようになること

7-1. 対策基準の策定

7-1-1. セキュリティ対策のレベル

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・運用規則など」で構成されます。「基本方針」には、組織や企業の代表者の情報セキュリティに対する考え、必要性、取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程を記載します。「実施手順」には、対策基準ごとに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。



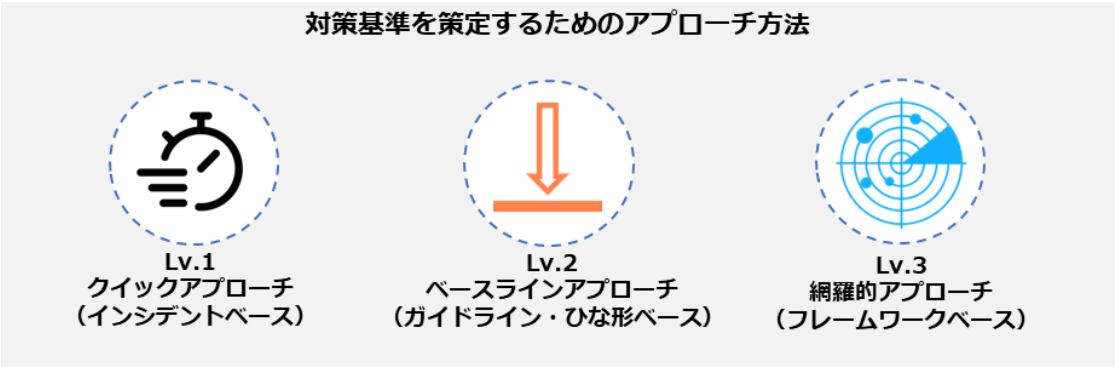
基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則など
対象者や用途によって必要な手続きを記述する

図 32. 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順守”. https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/12/

対策基準外部に公開することにより、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、



「2-3. 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。

7-1-2. セキュリティ対策のアプローチ方法

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。 低コスト、短期間で実施可能。包括的ではないが即効性がある。	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して暫定的対策を行う場合。
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型を参考とし、対策基準を策定。 規制遵守の観点から一定の安全性が確保できる。 コストパフォーマンスがよい。	組織的に一定以上の対策基準を策定する場合。 包括的な対策は過剰で、基本的な水準の対策が適切だと判断される場合。
Lv.3 網羅的アプローチ	脅威や攻撃手法に対して、網羅的なセキュリティ対策を講じることを目指すアプローチ手法。 ISMS 認証取得が可能なレベルを目指して、対策基準を策定。 コストが高くなる可能性があるが、組織のニーズに合わせた最適な対策が可能。	ISMS のフレームワークに沿った対策基準を策定する場合。 情報システムが重要な組織や機密性の高い情報を扱う組織など、高い水準の情報セキュリティが求められる場合。

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	• 小規模なセキュリティ対策や修正を迅速に実施可能。 • 低コストでリスクを軽減でき、コストパフォーマンスがよい。 • 流行中の攻撃の拡大や影響を最小限に抑えられる。 • リソースが限られていても実施可能。	• 包括的でないため、抜けが発生する可能性がある。 • 一時的な対策になりがちで、抜本的な対策にならない。 • 長期的にみると費用が嵩んでしまう場合がある。
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。 • ある程度の対策効果が見込め、コストパフォーマンスがよい。	• 最低基準を満たすだけなので、十分なセキュリティ水準が確保できない可能性がある。 • 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	• 組織のニーズに合わせた最適な対策が可能。 • リスクを徹底的に特定・分析できるので、高度なセキュリティ水準が実現できる。 • 長期的な視点で PDCA サイクルを回せる。 • 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。	• コスト（特に初期コスト）が高額になってしまうことが多い。 • リスク分析や対策の詳細設計に時間を要し、全体的なセキュリティ対策の実施が遅くなってしまう。

Lv.1 クイックアプローチ

Lv.1 クイックアプローチでは、さまざま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、重要情報の詐取など

2. 組織的対策
- ランサムウェア対応のためにセキュリティ管理体制を確立する
- インシデント対応のためにセキュリティ管理体制を整備する

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
- 公開サーバへの不正アクセス対策
- 共有サーバなど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

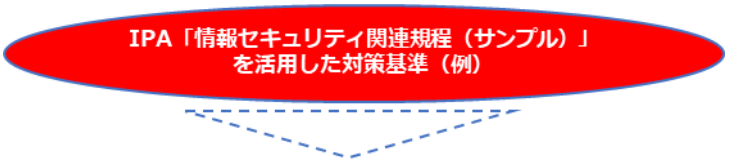
詳細理解のため参考となる文献（参考文献）	
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
マルウェア「ランサムウェア」の脅威と対策（対策編）	https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

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型を参考とし、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】を活用することにより、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 3.1 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）



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

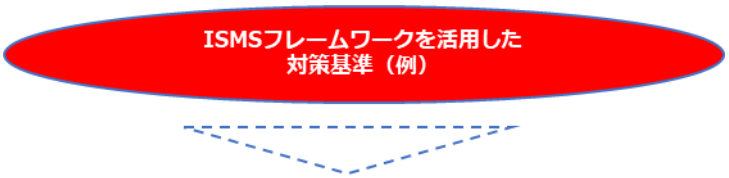
情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

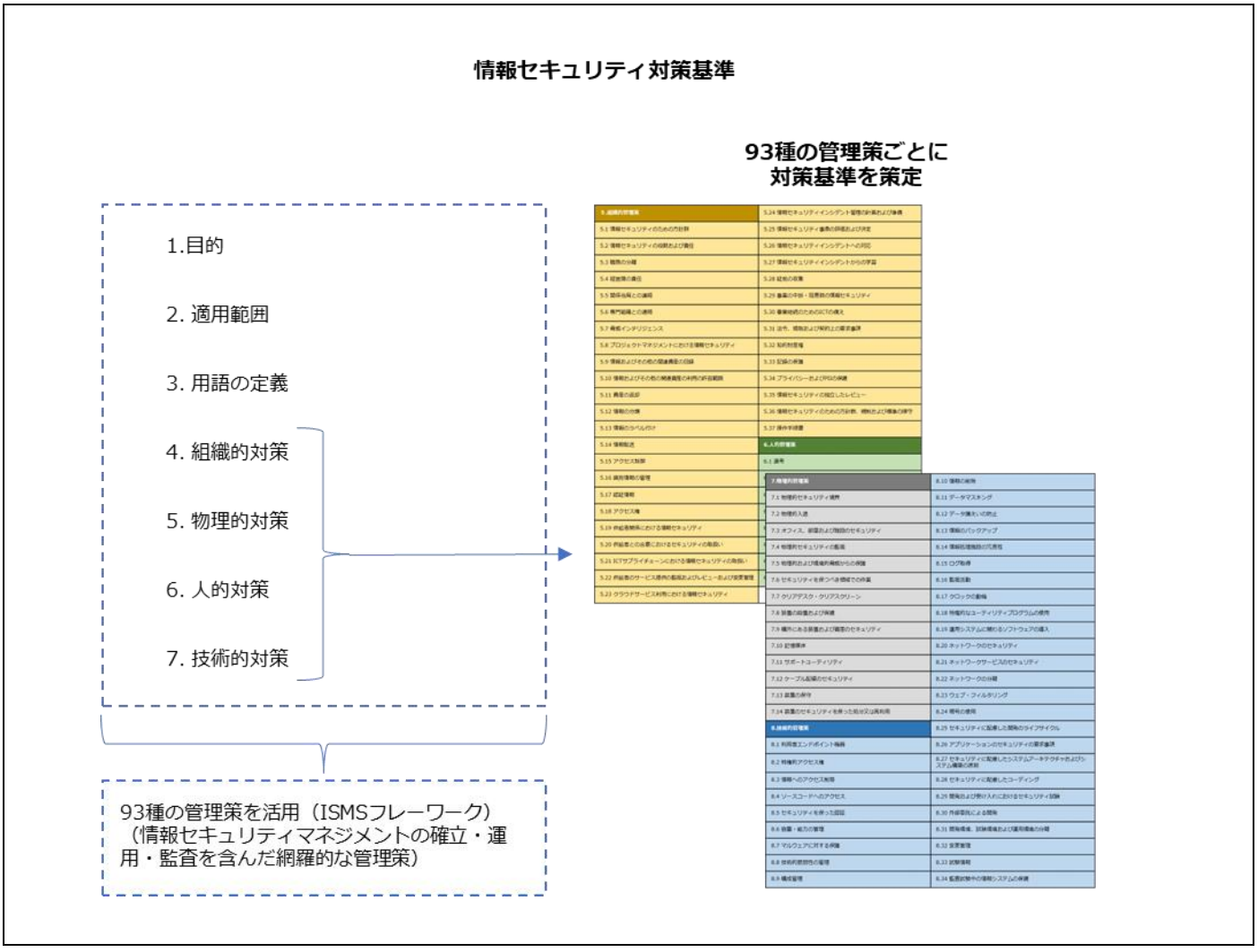
役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。

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（サンプル）	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

Lv.3 網羅的アプローチ

Lv.3 網羅的アプローチでは、ISMS 認証取得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8章. 用語定義および関係性と識別方法

章の目的
第 8 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

8-1. 用語の定義、脅威・脆弱性の識別

8-1-1. 用語の定義と関係性

企業や組織にはさまざま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、コンピュータウイルスなどのマルウェア、不正アクセス、DDoS 攻撃、窃盗や破壊行為などの犯罪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、情報システムやネットワーク、アプリケーション、セーフガード（管理策）、施設・設備などに存在する欠陥や弱点。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。
インシデント 事故・出来事のこと。セキュリティでは、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。コンピュータウイルスの感染、不正アクセスの発生、システム障害やネットワーク障害、情報システム関連の内部不正行為、災害や事故によるデータ・設備の損失など。
資産 組織にとって価値があるもの。
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） 脅威から情報資産を守るための対策や管理的・技術的手段。施設の入退室管理、監視カメラの設置、防犯装置の導入などの物理的な対策、ファイアウォール、アンチウイルスソフト、アクセス制御、暗号化、バックアップなどの技術的対策、情報セキュリティポリシーの策定、教育訓練の実施、インシデント対応手順の整備、監査の実施、担当者の資格管理、従業員教育、守秘義務の徹底などの管理的対策がある。

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と損害の度合い。
残留リスク さまざまな対策（セーフガード）を講じた後に残るリスク。残存リスクともいう。
リスク値 リスクの大きさのこと。「情報資産の重要度（あるいはリスクが顕在化したときの被害の大きさ）」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。高、中、低のような段階評価を用いる場合と定量的に計算する場合がある。

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

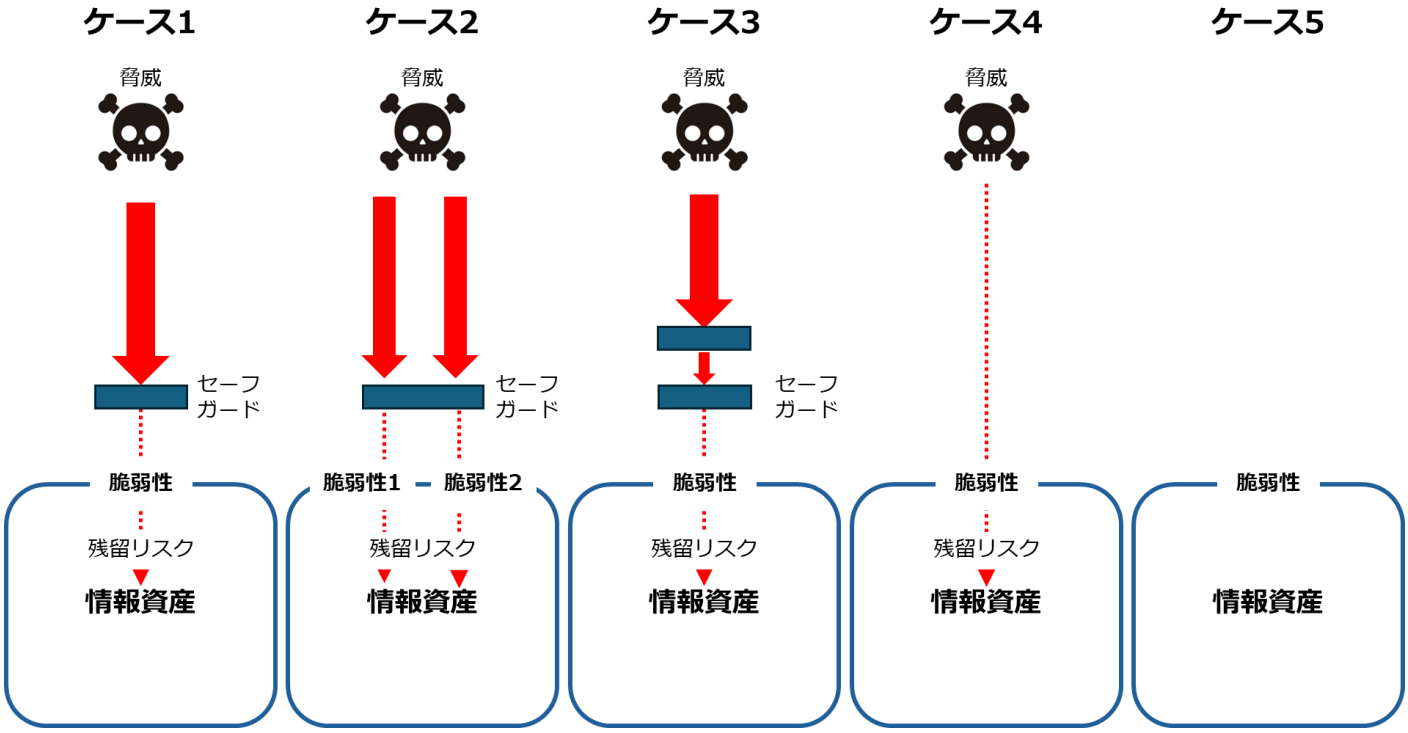


図 33.脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係

(出典)「ISO/IEC TR 13335-1」をもとに作成

ケース	図の説明	脅威	脆弱性	セーフガード（管理策）	リスク
ケース 1	**1 つのセーフガードが、リスクを低減することに効果的と見られる場合** 脆弱性に対応する脅威がありますが、セーフガードがある（セキュリティ対策がなされている）ので、リスクは残留リスクまで低減されています。	あり	あり	あり	低減

ケース 2	**1 つのセーフガードが、複数の脆弱性を悪用する脅威と関連するリスクを低減することに効果的と見られる場合** 複数の脆弱性があり、それを悪用する可能性のある脅威がありますが、1 つのセーフガード（セキュリティ対策）によってリスクを残留リスクまで低減できるケースです。	あり	あり (複数)	あり	低減
ケース 3	**複数のセーフガードの組み合わせが、リスクの低減に有効な場合** 脆弱性に対応する脅威がありますが、その脅威に対応する複数のセーフガードがあり（複数のセキュリティ対策がなされており）リスクは残留リスクまで低減されているケースです。一般的に、リスクを受容可能なレベルに低減するために、多数のセーフガードが必要になるケースは珍しくありません。	あり	あり	あり(多段)	低減
ケース 4	**脆弱性を悪用する可能性がある脅威があるが、そのリスクが受容可能とみなされる場合** リスクが受容可能なレベル以下であるため、セーブガード（セキュリティ対策）の必要がありません。	あり	あり	あり	受容
ケース 5	**脆弱性に対応する既知の脅威がない場合** 資産をとりまく情報システムなどの環境には脆弱性がありますが、それに対応する既知の脅威がないので、セーフガード（セキュリティ対策）の必要がないケースです（そもそもリスクもないことになります）。	なし	あり	あり	不明

（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	営業業務で必須の情報
脅威	社外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、従業員番号、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））

下記の図では「脅威」「脆弱性」「資産の価値」のいずれかが増加することにより、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。

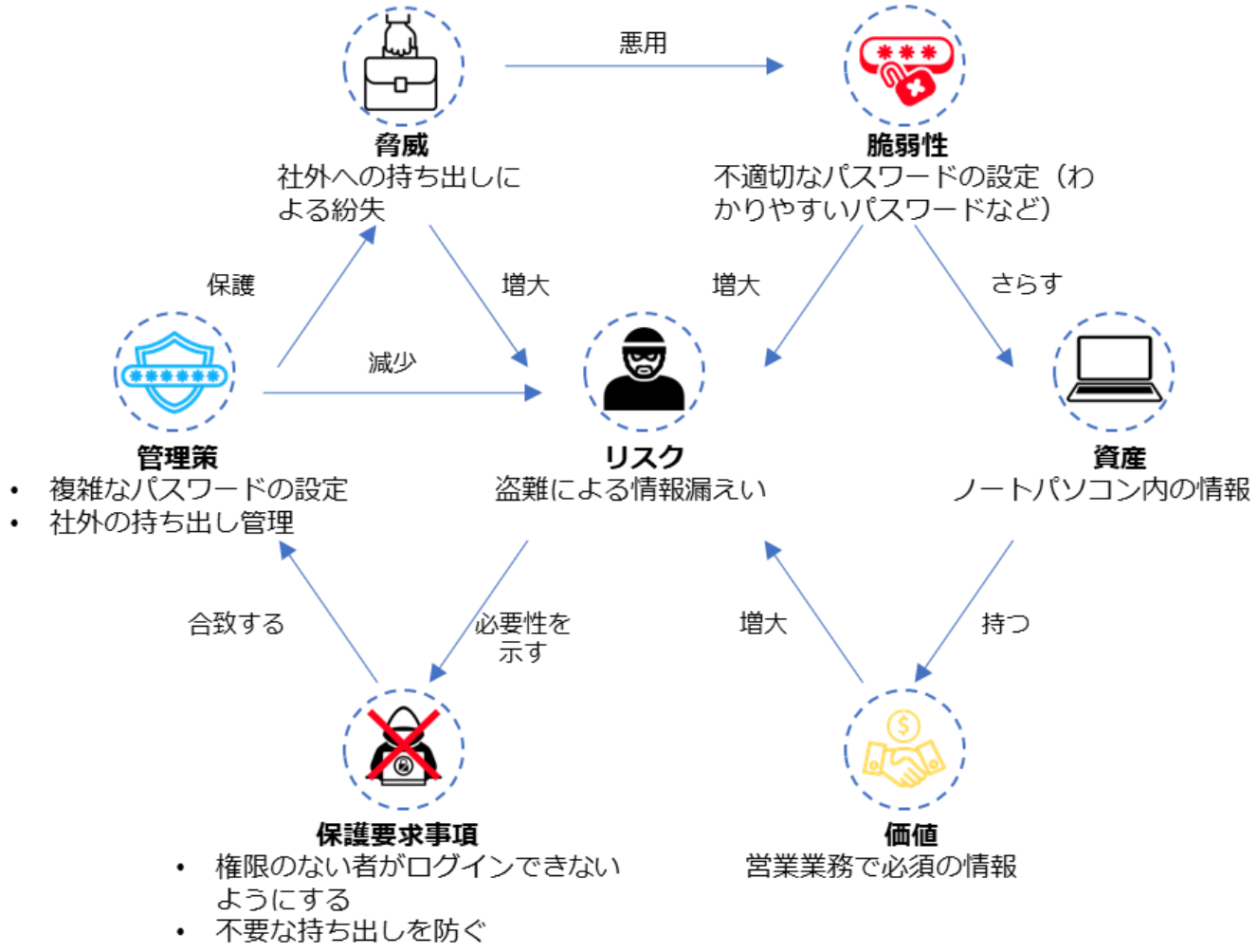


図 34. 脆弱性、リスクの関係の事例

8-1-2. 脅威の識別

脅威は「脆弱性」に付け入り顕在化することにより、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により、必要なセキュリティ対策を整理しやすくなります。

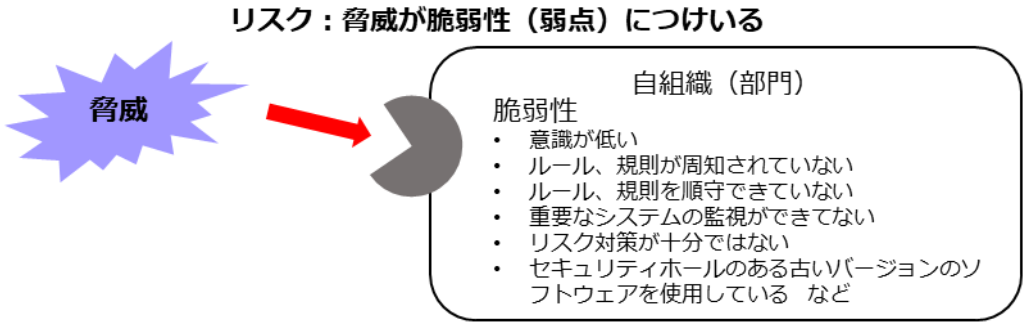


図 35. 脅威と脆弱性の関係

（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

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
	漏えい・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
許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	A/D

	アの使用	
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」をもとに作成

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、災害から回復すること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）漏えいする」という脅威が考えられます。このような脅威については、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えい者を罰すること、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セキュリティ対策が有効になります。漏えいを早期に検知するといったセキュリティ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ように、二回ずつ入力する、一定の範囲の値しか入力できないようにする、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」をもとに作成

8-1-3. 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。脅威と脆弱性がもたらすリスクを低減するためには、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意味することが多いため、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	脅威の例	脆弱性の識別
ハードウェア	システムの保守に関する違反	記憶媒体の不十分な保守/不適当な設置
	機器や媒体の破壊	定期的な交換計画の欠如
	粉塵（ダスト）、腐食、凍結	湿気、ホコリ、汚れに対する影響の受けやすさ
	使用時のミス	有効な構成変更管理の欠如
	電力供給の停止	電圧の変化に対する影響の受けやすさ
	気象現象	温度変化に対する影響の受けやすさ
	媒体や文書の盗難	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
ソフトウェア	不正アクセス	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
	使用時のミス	複雑なユーザーインタフェース
	使用時のミス	文書化の欠如
	不正アクセス	ユーザーの識別およ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
	データの違法な処理	不要なサービスが実行可能
	ソフトウェアの誤作動	効果的な変更管理の欠如
	恐怖、攻撃、妨害行為	管理されていないソフトウェアのダウンロードおよび使用

	装置又はシステムの故障	バックアップコピーの欠如

脆弱性の識別例

（出典）「ISO/IEC 27005」をもとに作成

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によって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。

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否か」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セキュリティ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セキュリティ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セキュリティ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セキュリティ対策につながります。

CIA の 3 要素に加えて上記の 4 要素も加えることにより、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

第 3 編では、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・運用規則など」）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、今後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。

本テキストを通じて、状況に応じて適切な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。

第9章. 具体的手順の作成（Lv.1 クイックアプローチ）

章の目的
第 9 章では、セキュリティインシデント事例を参考にするクイックアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。
主な達成目標
□　クイック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

9-1. 【Lv.1 クイックアプローチ】の概要

対策基準を策定し、具体的な実施手順を明確にすることにより、情報漏えいなどのリスク対策を行います。セキュリティ対策の内容を決めるためのアプローチ手法として、「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」があります。

本章では、「Lv.1 クイックアプローチ」における実施手順の作成方法について説明します。Lv.1 クイックアプローチは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。

Lv.1 クイックアプローチ（緊急性の高い事象に対応するための対策）

概要

報道される事例や情報セキュリティ 10 大脅威などから、発生する可能性が高いセキュリティインシデント事例や、セキュリティインシデントが発生した場合に被害が大きい事例を参考にし、対策基準や実施手順を策定します。

メリット

小規模なセキュリティ対策や修正を迅速に実施可能。
低コストでリスクを軽減でき、コストパフォーマンスがよい。
流行中の攻撃の拡大や影響を最小限に抑えられる。
リソースが限られていても実施可能。

デメリット

包括的でないため、抜けが発生する可能性がある。
一時的な対策になりがちで、抜本的な対策にならない。
長期的にみると費用が嵩んでしまうことがある。

セキュリティインシデント事例をもとに、リスクアセスメントの実施
（リスク特定、リスク分析、リスク評価）

9-2. 【Lv.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

Lv.1 クイックアプローチ

クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられるセキュリティインシデント事例を参考に、対策基準を策定します。決定した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。

対策基準・実施手順作成の手順

セキュリティインシデント事例をもとにリスクアセスメントを実施します。以下は、情報セキュリティ 10 大脅威 2024 にランクインしている「内部不正による情報漏えい」に関するセキュリティインシデント事例です。

事例：内部不正による情報漏えいの疑い（卸売業・小売業、従業員数 6~20 名以下）
被害内容 元従業員が退職前に大量にファイルをダウンロードしました。また、同従業員が使用していた PC の履歴が消去され、専門家でも復旧できない状態になっていました。 機密情報の持ち出しをした確定的な証拠が得られなかったため、結果的には被害届を提出しませんでした。しかし、この判断をするまでに 2 年かかりました。その間、弁護士に情報提供するために、多くの作業が必要になりました。例えば、経営者と総務担当は、情報漏えいしたと疑われる膨大なログを確認し、どれが機密情報に該当するかチェックする作業を強いられました。トラブル発生時は、人件費に加えて、心的負担も大きくかかりました。 **被害発生の原因** 社外からの脅威のセキュリティ対策としてウイルス対策ソフトウェアや電子メールへの対応、アクセス制限などは進めていたが、社内から発生する脅威のセキュリティ対策は不十分であったこと。

セキュリティインシデント事例：内部不正による情報漏えい

(出典) IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集- 」をもとに作成

リスク特定（例）

セキュリティインシデント事例を参考に、情報資産の洗い出しと、「機密性」「完全性」「可用性」の観点から重要度を算出します。セキュリティインシデント事例では、従業員が使用していた PC が悪用されていたため、以下の資産目録の例では「媒体・保存先」で従業員が使用する PC である情報資産を洗い出しています。そして、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。リスクアセスメントの詳細はこの後の「第 12 章. リスクマネジメント」を参照してください。

機密性・完全性・可用性の評価値は、1~3 で記載

重要度は、機密性・完全性・可用性いずれかの最大値

業務分類	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	機密性	完全性	可用性	重要度
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者の PC	3	3	2	3
経理	当社宛請求書	過去 3 年分	経理部	経理部長	経理部	経理担当者の PC	3	3	2	3
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者の PC	3	3	3	3

資産目録の例

（出典）IPA 「リスク分析シート」をもとに作成

リスク分析（例）

リスク特定で算出した重要度と、被害発生可能性からリスクレベルを算出します。被害発生可能性は、セキュリティインシデント事例と同様の被害がどの程度起きやすいかを考慮して算出します。

リスクレベルの算出方法	「リスクレベル」＝「重要度」×「被害発生可能性」

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	機密性	完全性	可用性	重要度	被害発生可能性	リスクレベル
人事	社員名簿	社員基本情報	人事部	人事部長	3	3	2	3	3	9
経理	当社宛請求書	過去 3 年分	経理部	経理部長	3	3	2	3	2	6
営業	顧客リスト	得意先	営業部	営業部長	3	3	3	3	2	6

リスク評価（例）

リスクレベルをもとに、必要なリスク対応を検討します。今回は、例としてリスク低減や回避を選択します。

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
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たり、リスクが顕在化したときの損失を他者に引き受けさせたりすること
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
リスク受容（保有）	セキュリティ対策を行わずにリスクを受け入れるということ

リスク評価をもとに対策基準・実施手順の作成

対策基準の策定（例）

リスク評価の結果を参考に対策基準を策定します。今回の例では、リスク低減や回避に関する対策基準を決定しています。対策基準の例は以下の通りです。

対策基準（例）
• 社内の機密情報に関する社内規程の策定 • 重要情報の管理、保護 • 物理的管理の実施 • 従業員向け研修の実施

実施手順の作成（例）

情報セキュリティ関連規程を参考に、実施手順を作成します。情報セキュリティ関連規程とは、情報セキュリティに関する社内規則の見本です。情報セキュリティ関連規程から、対策基準に合った規則を選択し、赤字の箇所を自社の状況に合わせて編集することにより、実施手順を作成します。

実施手順の作成（例）
機密情報に関する社内規程の策定 （例）従業員の責務 従業員は以下を遵守する • 従業員は、当社が営業秘密として管理する情報およびその複製物の一切を許可されていない組織、人に提供してはならない。 • 従業員は、当社の情報セキュリティ方針および関連規程を遵守する。違反時の懲戒については、就業規則に準じる。 • 従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が

交付を受けた資料またはそれらの複製物の一切を退職時に返還する。

- 従業員は、在職中に知り得た当社の営業秘密または業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

重要情報の管理、保護

（例）利用者アカウントの管理

利用者の認証に用いるアカウントが不要になる場合、システム管理者は、当該アカウントの削除または無効化を、当該アカウントが不要になった日の翌日までに実施する。

物理的管理の実施

（例）情報資産の社外持ち出し管理

情報資産を社外に持ち出す場合には、以下を実施する。

- 社外秘の場合は所属部門長の許可を得る。
- 極秘の場合は代表取締役の許可を得る。
- ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/データを暗号化する。
- スマホ、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
- USB メモリなどの小型電子媒体は、大きなタグをつける/ストラップで体やカバンに固定する/落としてもすぐにわかるように鈴をつける。
- 屋外でネットワークへ接続して極秘または社外秘の情報資産を送受信する場合は、暗号化する。
- 携行中は常に監視可能な距離を保つ。

従業員向けの研修

（例）情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。

対象者：全従業員

テーマ：以下は必須とする。

- 情報セキュリティ関連規程の説明（入社時、就業時）
- 最新の脅威に対する注意喚起（随時）
- 関連法令の理解（関連法令の公布・施行時）
- 個人情報の取扱いに関する留意事項
- コンプライアンス教育

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

編集後記

第 4 編では、対策基準から実施手順を策定する手法を説明するにあたり、クイックアプローチについて説明しました。

クイックアプローチは、実際のセキュリティインシデントの事例を踏まえ、自社での発生可能性や被害規模を慎重に検討し、対策基準や実施手順を策定していく手法です。この方法により、特に社会的に影響の大きい事案に対するセキュリティ対策を迅速かつ効果的に行うことができます。

サイバーセキュリティの脅威への対処の最初の段階として、緊急に大きなセキュリティホールを塞ぐには有効なアプローチとなります。

第 5 編では、ガイドブックやひな型を参照して迅速に対応できるベースラインアプローチについて解説します。

第10章. 具体的手順の作成（Lv.2 ベースラインアプローチ）

章の目的
第 10 章では、ガイドラインやひな型などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。
主な達成目標
□ ベースライン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

10-1. 【Lv.2 ベースラインアプローチ】の概要

「Lv.2 ベースラインアプローチ」における実施手順の作成方法について説明します。Lv.2 ベースラインアプローチは、ガイドラインなどを参考に、対策基準や実施手順を策定するアプローチ手法です。

Lv.2 ベースラインアプローチ（即効性のあるアプローチ手法）

概要

IPA や総務省などが発行しているガイドラインやひな型を参考に、対策基準や実施手順を策定します。

セキュリティ対策のガイドラインやひな型を参考にすることにより、組織全体で一貫性があり、セキュリティの最低基準を満たす対策基準や実施手順を策定します。

メリット

- 組織全体で一貫性を確保できる。
- 最低限実施すべきセキュリティ対策を講じることができる。
- ある程度の対策効果が見込め、コストパフォーマンスがよい。

デメリット

- 最低基準を満たすだけなので、十分なセキュリティ水準を確保できない可能性がある。
- ガイドラインやひな型は、一般的な組織を想定したものであるため、自社の組織やシステム、環境に見合ったものにするため、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必要がある。

10-2. 【Lv.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

10-2-1. 情報セキュリティ対策ガイドラインの活用

ベースラインアプローチでは、ガイドラインやひな型などの資料を参考に対策基準、実施手順を作成します。次のページから、以下の資料をもとに対策基準、実施手順を作成する流れを説明します。

- 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」
- NISC「インターネットの安全・安心ハンドブック Ver.5.0」
- 総務省「テレワークセキュリティガイドライン第 5 版」
- IPA「中小企業のためのクラウドサービス安全利用の手引き」
- IPA「情報セキュリティ関連規程」

各資料の概要は以下の通りです。

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」
「中小企業の情報セキュリティ対策ガイドライン」は、情報セキュリティ対策に取り組む際の、（1）経営者が認識し実施すべき指針、（2）社内において対策を実践する際の手順や手法をまとめたものです。経営者編と実践編で構成されており、中小企業の利用を想定しています。付録の「5 分でできる！情報セキュリティ自社診断」や「情報セキュリティハンドブック（ひな形）」を活用することにより、対策基準、実施手順を策定できます。
NISC「インターネットの安全・安心ハンドブック Ver.5.0」
「インターネットの安全・安心ハンドブック」は、サイバーセキュリティに関する基本的な知識を、身近な具体例を取り上げながら説明したものです。子供やシニアの方など、インターネットの一般利用者に加えて、中小企業なども活用できます。中小組織向けにある「インターネットの安全・安心ハンドブック Ver 5.00＜中小組織向け抜粋版＞」を活用することにより、対策基準、実施手順を策定できます。
総務省「テレワークセキュリティガイドライン第 5 版」
「テレワークセキュリティガイドライン」は、企業などがテレワークを導入する際のセキュリティ対策についての考え方や対策例を示したものです。テレワークを既に導入している場合は、自社のテレワーク環境がガイドラインに沿ったものであるのか検証できます。テレワークに関する「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場からそれぞれのセキュリティ対策について対策基準、実施手順を策定できます。
IPA「中小企業のためのクラウドサービス安全利用の手引き」
「中小企業のためのクラウドサービス安全利用の手引き」は、中小企業の情報セキュリティ対策ガイドラインの付録資料です。クラウドサービスを安全に利用するための手引きが記載され

ています。「クラウドサービス安全利用チェックシート」と「解説編」を参考にすることにより、クラウドサービス利用に関する対策基準、実施手順を策定できます。
IPA「情報セキュリティ関連規程」
「情報セキュリティ関連規程」は、自社に適した規程を作成するためのひな型です。ひな型に修正を加えることによって、対策基準、実施手順を策定します。1 から文書化する必要がないため、効率的に策定できます。

10-2-2. 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」の活用

対象者	• 中小企業および小規模事業者（業種は問わず、法人・個人事業主・各種団体も含む）の経営者と情報管理を統括する方 • セキュリティ対策を部分的に実施してきた企業 • 情報セキュリティに関する知識を十分に有した人材が不足している企業など
目的	• 情報セキュリティに関する組織的な取組を開始するため

本ガイドラインは、情報セキュリティに関する組織的な取組を行う際に活用できます。

本ガイドラインをもとに実施手順を策定する際は、「1. 実施状況の把握」「2. 対策の決定と周知」の手順で策定します。

1.実施状況の把握

「5 分でできる！情報セキュリティ自社診断」を利用し、現在のセキュリティ対策の実施状況を把握します。合計 25 問の設問に答えるだけでセキュリティ対策の実施状況が把握できます。設問の例（一部抜粋）は以下の通りです。

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	分からない
Part1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？	4	2	0	-1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1
	4	重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	-1

	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1

自社診断の設問（一部抜粋）

(出典) IPA「5 分でできる！情報セキュリティ自社診断」をもとに作成

「5 分でできる！情報セキュリティ自社診断」の使い方

- ✓ 経営者や情報システム担当者、部門長などセキュリティ対策の実施状況がわかる方が、25 問の設問に回答します。
- ✓ 事業所が複数ある、部署数が多いなど、1 人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
- ✓ 実施状況がわからない場合、各従業員に質問して、回答を総合して記入します。
- ✓ チェック欄の該当するもの 1 つに〇をつけて、「実施している…4 点」「一部実施している…2 点」「実施していない…0 点」「分からない…-1 点」で採点します。
- ✓ 全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「分からない」になっている項目を把握します。

詳細理解のため参考となる文献（参考文献）	
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
5 分でできる！情報セキュリティ自社診断	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

2.対策の決定と周知

診断結果をもとに「5 分でできる！情報セキュリティ自社診断」（解説編）を参考にし、実行すべきセキュリティ対策を検討・決定します。解説編の例（抜粋）は以下の通りです。

診断編 No.3	**パスワード管理**
強固なパスワードを使用する	
パスワードが推測や解析されたり、Web サービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。	
対策例	パスワードは 10 文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。 同じ ID・パスワードを複数サービス間で使い回さない。 テレワークで VPN やクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は多段階認証や多要素認証を利用する。

解説編の一例

(出典) IPA「5 分でできる！情報セキュリティ自社診断」をもとに作成

「5 分でできる！情報セキュリティ自社診断」（解説編）の使い方

- ✓ セキュリティ対策の検討と決定は、責任者・担当者と経営者が行います。
- ✓ 診断項目ごとにセキュリティ対策を実施しない場合に考えられる被害・事故や、防止するためのセキュリティ対策例を参考にして検討します。
- ✓ 検討するときには従業員の意見を聞き、職場環境や業務に適したセキュリティ対策を決定します。

セキュリティ対策の決定後、「情報セキュリティハンドブック（ひな形）」を利用し、従業員が実行するべき事項を周知します。情報セキュリティハンドブック（ひな形）は、自社診断の解説編に記載されているセキュリティ対策例と連動しています。ひな型を編集して決定したセキュリティ対策の内容を具体的に記述し、従業員に配付します。ひな型の記載例は以下の通りです。

実施手順の例：パスワードの管理

ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

編集前（ひな型）

○必須	×禁止
10 文字以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない

編集後

○必須	×禁止
16 文字以上の文字数で構成されている	従業員番号・名前・住所・電話番号・生年月日・辞書に載っている単語・他人に推測されやすい文字列は使わない

ひな形の修正例

(出典) IPA「情報セキュリティハンドブック（ひな形）」をもとに作成

「情報セキュリティハンドブック（ひな形）」の使い方

- ✓ 情報セキュリティハンドブックは、責任者・担当者が作成します。
- ✓ ひな型に記載された例文を編集して、決定したセキュリティ対策を社内ルールとして明文化します。
- ✓ 完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、セキュリティ対策を周知徹底します。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティハンドブック（ひな形）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

10-2-3. NISC「インターネットの安全・安心ハンドブック Ver.5.0」の活用

対象者	• 全従業員
目的	一人一人が能動的にサイバー空間における脅威を知り、サイバーセキュリティに対する素養・基本的な知識を身につけるため

本ハンドブックは、サイバー攻撃の手口やリスクを身近な具体例を取り上げながら説明しているため、専門知識を必要とせずセキュリティ対策を知ることができます。インターネットの利用者が実施すべき基本的なセキュリティ対策に加えて、中小組織向けのセキュリティ対策を記載しています。企業経営においてセキュリティ対策に投資すべき理由、企業特有のセキュリティ対策に必要なルール作りといった内容を説明しています。

以下では、第 1 章の「最低限実施すべきサイバーセキュリティ対策を理解しよう」を用いて、実施手順の作り方を説明します。

（例）①OS やソフトウェアは常に最新の状態にしておこう

インターネットの安全・安心ハンドブック記載

- OS 関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようにする。
- セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにする。
- サイバー攻撃で狙われやすいソフトウェアを重点的に更新する。
- 機器そのものの基本プログラムを更新するファームウェアもアップデートする。
- セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定する。
- アップデートが提供されなくなった OS やソフトウェアはセキュリティホールが見つかっても修正用アップデートが提供されず、攻撃に対して非常に脆弱なので、使用しないようにする。

自社の状況

- OS、セキュリティソフトは法人向けを利用しているため、アップデート管理は情報システム部が担当。
- 情報システム部がブラウザは古いバージョンを使わないように通知している。
- 自宅で使用しているリモート用 PC は、一般向けのソフトウェアがインストールされている。

実施手順

対象：PC

システム管理者は、アップデート管理として以下を実施する。

- システム管理者は月末に OS、セキュリティソフトの更新プログラムを適用する。緊急な場合は、従業員に通知し、更新プログラムを適用する。
- 従業員は、毎月 OS、セキュリティソフトの更新プログラムを適用する。確認方法はチェックリストを用いる。
- 従業員は、ブラウザのアップデートを適宜行い、バージョン○○以前のものは使用しない。
- システム管理者は○○日にセキュリティソフトのウイルス定義ファイルの更新を行う。

詳細理解のため参考となる文献（参考文献）	
インターネットの安全・安心ハンドブック Ver.5.00	https://security-portal.nisc.go.jp/guidance/handbook.html

10-2-4. 総務省「テレワークセキュリティガイドライン第 5 版」の活用

対象者	• 経営者 • システム・セキュリティ管理者 • テレワーク勤務者
目的	テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するため

本ガイドラインでは、セキュリティ対策を整理するため、13 個の対策分類にわかれています。「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場から対策分類ごとに具体的に実施すべき事項を示しています。以下では、「6.マルウェア対策」をもとに自社の状況からセキュリティ対策の実施手順の作成例を説明します。

（例）6. マルウェア対策

システム・セキュリティ管理者が実施すべき対策

- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
- セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能などを用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
- テレワーク端末に EDR を導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
- テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるよう

にする。

テレワーク勤務者が実施すべき対策

- 少しでも不審を感じたメール（添付ファイルや URL リンクなどを含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

自社の状況

- テレワーク端末には、法人向けのセキュリティ対策ソフトと EDR を導入しており、システム管理者はウイルス定義ファイルの更新などを一元管理できる。
- システム管理者は毎月○○日にセキュリティソフトのレポートを確認している。
- 不審なメールが来た場合は、情報システム部と上長に連絡するようにしている。

実施手順

テレワーク端末のマルウェア対策として以下を実施する。

- システム管理者は会社支給のテレワーク端末にセキュリティ対策ソフトと EDR をインストールし、一元管理する。
- システム管理者は、テレワーク端末のウイルス定義ファイルの自動更新とリアルタイムスキャンを設定する。
- システム管理者は毎月○○日にセキュリティソフトと EDR のレポートを確認し、不審な点があれば該当のテレワーク端末所有者に対して、確認を行う。
- 従業員は、不審を感じたメール（添付ファイルや URL リンクなどを含む。）は開かず、システム管理者と上長へ連絡する。

詳細理解のため参考となる文献（参考文献）	
テレワークセキュリティガイドライン第 5 版	https://www.soumu.go.jp/main_content/000752925.pdf

10-2-5. IPA「中小企業のためのクラウドサービス安全利用の手引き」の活用

対象者	• クラウドサービスを利用する企業
目的	クラウドサービスを安全に利用するため

本ガイドラインは、クラウドサービスを安全に利用するために活用できるガイドラインです。「利用するクラウドサービスを選定するとき」、「クラウドサービスを運用していくとき」、「クラ

ウドサービスのセキュリティ対策を検討するとき」のタイミングで活用することができます。本ガイドラインの使い方としては、「クラウドサービス安全利用チェックシート」でチェックを行います。また、「解説編」を参考に、利用者としての役割や責任を認識し、実施手順を策定します。

以下は、クラウドサービスの運用に関する設問例となります。

運用するときのポイント	
管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手もとに確保して必要なときに使えるようにしていますか？

解説編をもとに実施手順を作成します。以下は、チェックシートの設問「バックアップに責任を持つ」の実施手順（例）を記載します。自社の状況に合わせて赤文字の箇所を修正することによって、自社に適した実施手順を作成できます。

実施手順の例：バックアップに責任を持つ
バックアップの管理 サービス停止やデータの消失・改ざんなどに備え、重要情報を手もとに確保して、必要なときに使えるようにする。 会計データやホームページなど、消失や改ざんの影響が大きいものは以下の規則を遵守する □ クラウドサービスの拡張機能にバックアップがある場合は利用する □ 月に 1 度、社内の専用ハードディスクにバックアップを取得する □ 直前のバックアップよりもさらに過去の状態に遡って復元できるよう、2、3 ヶ月前に取得したバックアップを保存しておく

詳細理解のため参考となる文献（参考文献）	
付録 6：中小企業のためのクラウドサービス安全利用の手引き	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

10-2-6. IPA「情報セキュリティ関連規程」の活用

対象者	• 中小企業
目的	自社のリスクに応じたセキュリティ対策の規程を作成するため

情報セキュリティ関連規程とは、自社が対応すべきリスクとセキュリティ対策を検討し、文書化した規程のことです。企業をとりまくリスクは、事業内容や取扱う情報、職場環境、IT の利用状況などによって異なるため、汎用的な規程をそのまま使っても、自社に適さない場合があります。そこで情報セキュリティ関連規程を活用することによって、効率的に自社に適した規程を作成できます。

本ガイドラインを用いて、規程を作成する手順を説明します。

1.対応すべきリスクを特定する

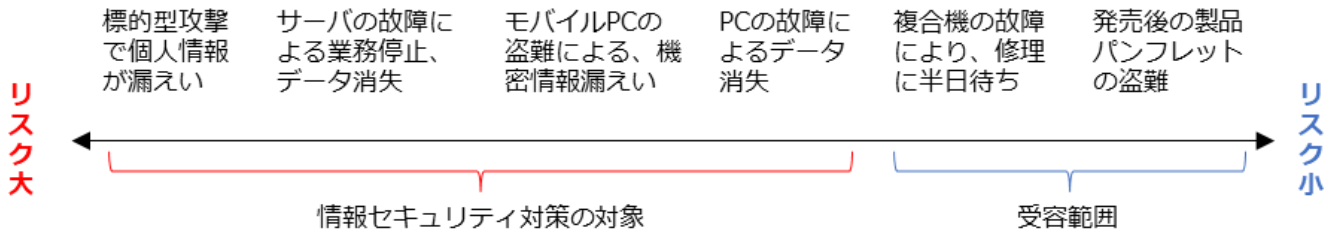
経営者が懸念する情報セキュリティの重大事故などを念頭に、何を起こさないようにするべきかを考えます。このとき、以下のような状況を併せて考えることにより、対応すべきリスクを把握します。

関連する業務や情報に関わる外部状況（法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など）、内部状況（経営方針・情報セキュリティ方針、セキュリティ管理体制、情報システムの利用状況など）

例
- 個人情報保護法への対応
- 取引先のセキュリティに対する要求への対応
- テレワーク時のセキュリティ対応
- 報道されている新たなサイバー攻撃への対応

2.セキュリティ対策の決定

すべてのリスクに対応しようとすると、セキュリティ対策費用が高額になったり、業務に支障をきたしたりする場合があります。そこで、いつ事故が起きてもおかしくない、事故が起きると大きな被害になるなど、リスクが大きなものを優先してセキュリティ対策を実施します。また、事故が起きる可能性が小さい、発生しても被害が軽微であるなど、リスクが小さなものは、現状のまま受容するなど、合理的に対応します。



3.規程の作成

「2. セキュリティ対策の決定」で対象としたリスクに対してセキュリティ対策を実施するため、文書化した規程を作成します。「中小企業の情報セキュリティ対策ガイドライン 付録 5 情報セキュリティ関連規程（サンプル）」を編集することによって、規程を作成することができます。以下では、「サーバの故障による業務停止、データ消失」に対するセキュリティ対策を文書化した規程の例を記載します。赤文字の箇所を修正することにより、自社に適した規程を作成します。

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
ファイルサーバ	ユーザーファイル	アプリケーションバックアップ機能	NAS サーバ
Web サーバ	ホームページ	同期ツール	NAS サーバ
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

＜保管＞

- NAS サーバ：施錠つきサーバラックに収納

情報セキュリティ関連規程の一例

(出典) IPA「情報セキュリティ関連規程（サンプル）」をもとに作成

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
DB サーバ	取引先に関するデータ	アプリケーションバックアップ機能	自社サーバ
Web サーバ	ホームページ	同期ツール	自社サーバ
発注管理システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドサービス上のサーバ

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

＜保管＞

- 自社サーバ：ハウジングサービスを利用し、サービス事業者の施設内に保管する

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

編集後記

第 5 編では、ガイドラインやひな型などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法を解説しました。

ベースラインアプローチは、ガイドラインやひな型などの既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定ができます。

ベースラインアプローチを用いることにより、組織全体で一貫性があり、セキュリティの最低基準を満たす対策基準や実施手順を策定できます。

第 6 編では、より漏れがない網羅的アプローチで用いる ISMS や、その他主要なフレームワークを解説します。

引用文献

情報セキュリティポリシーの順守（総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/12/
ISO/IEC TR 13335-1
https://www.iso.org/standard/39066.html
ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版
https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjo3ODgwMSwiY2F0ZWdvcnlOdW0iOjEwNzI0fQ==&pNo=1
ISO/IEC 27005
https://www.iso.org/standard/80585.html
2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf
リスク分析シート
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
5 分でできる！情報セキュリティ自社診断
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf
情報セキュリティハンドブック（ひな形）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx
情報セキュリティ関連規程（サンプル）
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

参考文献

情報セキュリティ 10 大脅威 2024

https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.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

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（サンプル）

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/

5 分でできる！情報セキュリティ自社診断

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf

情報セキュリティハンドブック（ひな形）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

インターネットの安全・安心ハンドブック Ver.5.00

https://security-portal.nisc.go.jp/guidance/handbook.html

テレワークセキュリティガイドライン第 5 版

https://www.soumu.go.jp/main_content/000752925.pdf

付録 6：中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

■AI

Artificial Intelligence の略。「AI（人工知能）」という言葉は、昭和 31 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。昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第 4 次 AI ブームに入ったとの見方もある）。「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

■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

■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

■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により、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

■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

■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

■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

■G ビズ ID

行政手続きなどにおいて手続き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さまざまな政府・自治体の法人向けオンライン申請が可能になる

■ICSCoE 中核人材育成プログラム

平成 29 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：Opera

tional 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

■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

■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

■IPS

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

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

■IP アドレス

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

■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

■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

■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

■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

■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

■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

■SASE（サシー）

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

■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

■SDP

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

■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

■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。

■SWG

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

■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により、盗聴やデータの改ざんを防ぐ。VPN を使用することによって、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

■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

■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

■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

■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

■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

■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、スマホ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

■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

■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

■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）

■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

■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

■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

■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

■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

■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、磁気的方法その他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、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

■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

■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。

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業の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にまとめた、民間事業者による安価なサービス。IPA は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■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

■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

■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

■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

■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

■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

■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

■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

■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

■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

■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

■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

■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、IPA と（一財）セキュリティ・キャンプ協議会が実施している

■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

■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

■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

■ゼロトラスト

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

■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」

■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

■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

■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

■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

■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

■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 ISO 27001 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

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある。

■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

■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

■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

■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

■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

■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さまざまである

■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

■踏み台

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

■フォレンジック

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

■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インターネット上の市場（闇市）

■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

■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、オープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

■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、ある基準に従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

■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

■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

■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

■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

■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

■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

■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