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

セミナー内容

回数	テーマ
第1回	サイバーセキュリティを取り巻く環境および中小企業に 求められるサイバーセキュリティ対策
第2回	これからの企業経営で必要な攻めと守りのIT活用および サイバーセキュリティ対策
第3回	サイバーセキュリティに関する国の方針・施策および サイバー脅威の動向
第4回	サイバーセキュリティ対策におけるフレームワークの体系
第5回	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】

セミナー内容

回数	テーマ
第6回	セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】
第7回	組織として実施すべき具体的な対策事項・手順【実施手順・実施者マニュアルレベル①】
第8回	組織的対策と人的対策【実施手順・実施者マニュアルレベル②】
第9回	技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】
第10回	全体総括

1．セキュリティ対策基準の策定

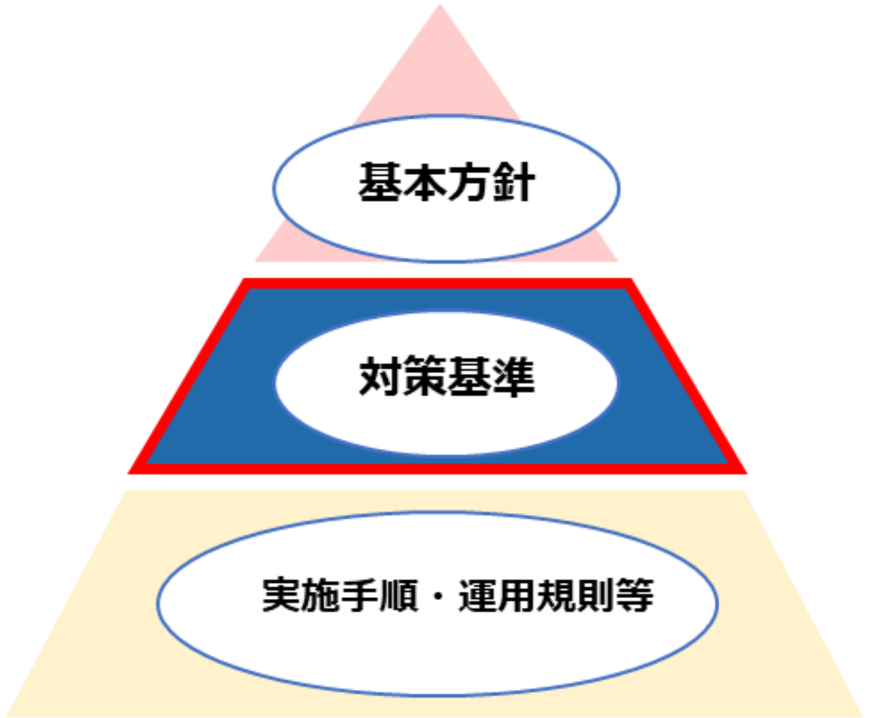
対策基準の策定

対策基準の策定

【参照：セミナーテキスト8-1-1.】
第8章 - 02

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の構成



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”

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

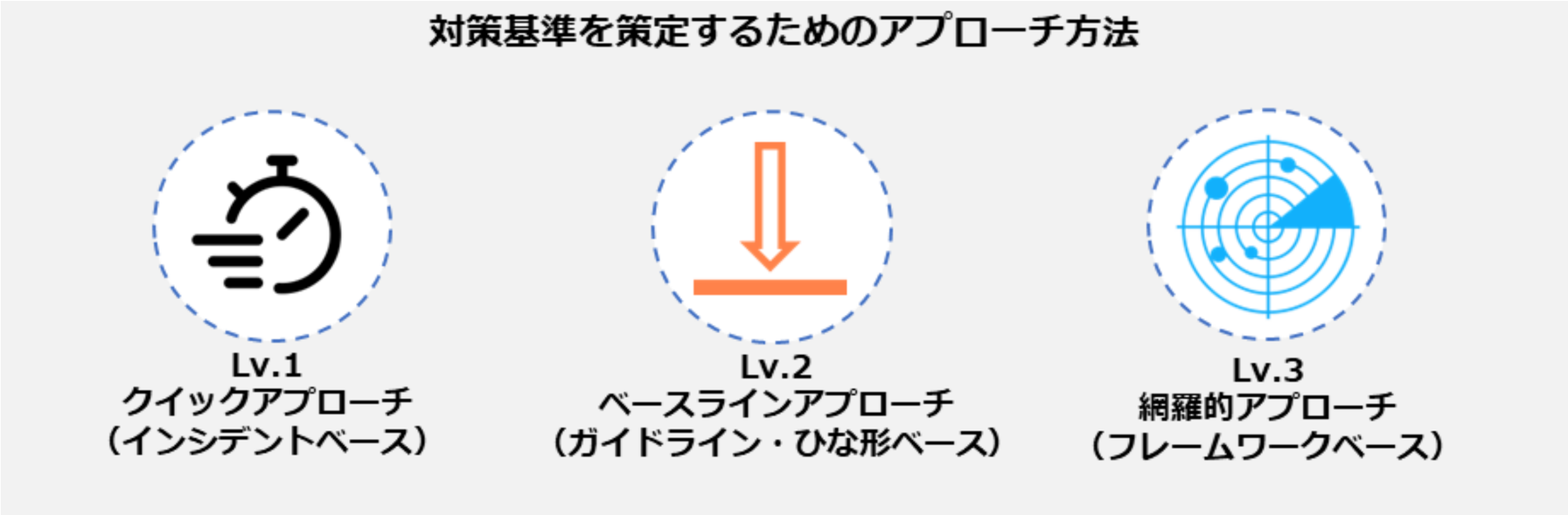
対象者や用途によって必要な手続きを記述する

対策基準の策定

【参照：セミナーテキスト8-1-1.】
第8章 - 02

対策基準のアプローチ方法

- 企業の現状を鑑み、次の段階的なアプローチ方法がある
  - 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【推奨】



対策基準の策定

【参照：セミナーテキスト8-1-2.】
第8章 - 03

対策基準のアプローチ概要

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。

対策基準の策定

【参照：セミナーテキスト8-1-2.】
第8章 - 03

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。

対策基準の策定

【参照：セミナーテキスト8-1-2.】
第8章 - 04

Lv.1 クイックアプローチ

【例】ランサムウェアに対する対策基準を作る

記載項目	内容
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のクリックを容易にしない • 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

対策基準の策定

【参照：セミナーテキスト8-1-2.】
第8章 - 05

Lv.2 ベースラインアプローチ

【例】 IPA「情報セキュリティ関連規程」を活用した対策基準

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。

1	組織的対策	改訂	20yy.mm.dd
適用範囲	全社・全従業員		

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

対策基準の策定

【参照：セミナーテキスト8-1-2.】
第8章 - 06

Lv.3 網羅的アプローチ

【例】 ISMSフレームワークを活用した対策基準

93種の管理策ごとに対策基準を策定する。

5.組織的管理策	5.24 情報セキュリティインシデント管理の計画および準備
5.1 情報セキュリティのための方針群	5.25 情報セキュリティ事象の評価および決定
5.2 情報セキュリティの役割および責任	5.26 情報セキュリティインシデントへの対応
5.3 職務の分離	5.27 情報セキュリティインシデントからの学習
5.4 経営陣の責任	5.28 証拠の収集
5.5 関係当局との連絡	5.29 事業の中断・阻害時の情報セキュリティ
5.6 専門組織との連絡	5.30 事業継続のためのICTの備え
5.7 脅威インテリジェンス	5.31 法令、規制および契約上の要求事項
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.32 知的財産権
5.9 情報およびその他の関連資産の目録	5.33 記録の保護
5.10 情報およびその他の関連資産の利用の許容範囲	5.34 プライバシーおよびPIIの保護
5.11 資産の返却	5.35 情報セキュリティの独立したレビュー
5.12 情報の分類	5.36 情報セキュリティのための方針群、規則および標準の順守
5.13 情報のラベル付け	5.37 操作手順書
5.14 情報転送	6.人的管理策
5.15 アクセス制御	6.1 選考
5.16 識別情報の管理	6.2 雇用条件
5.17 認証情報	6.3 情報セキュリティの意識向上、教育および訓練
5.18 アクセス権	6.4 懲戒手続き
5.19 供給者関係における情報セキュリティ	6.5 雇用の終了又は変更後の責任
5.20 供給者との合意におけるセキュリティの取扱い	6.6 秘密保持契約又は守秘義務契約
5.21 ICTサプライチェーンにおける情報セキュリティの取扱い	6.7 リモートワーク
5.22 供給者のサービス提供の監視およびレビューおよび変更管理	6.8 情報セキュリティ事象の報告
5.23 クラウドサービス利用における情報セキュリティ	

7.物理的管理策	8.10 情報の削除
7.1 物理的セキュリティ境界	8.11 データマスキング
7.2 物理的入退	8.12 データ漏えいの防止
7.3 オフィス、部屋および施設のセキュリティ	8.13 情報のバックアップ
7.4 物理的セキュリティの監視	8.14 情報処理施設の冗長性
7.5 物理的および環境的脅威からの保護	8.15 ログ取得
7.6 セキュリティを保つべき領域での作業	8.16 監視活動
7.7 クリアデスク・クリアスクリーン	8.17 クロックの同期
7.8 装置の設置および保護	8.18 特権的なユーティリティプログラムの使用
7.9 構外にある装置および資産のセキュリティ	8.19 運用システムに関わるソフトウェアの導入
7.10 記憶媒体	8.20 ネットワークのセキュリティ
7.11 サポートユーティリティ	8.21 ネットワークサービスのセキュリティ
7.12 ケーブル配線のセキュリティ	8.22 ネットワークの分離
7.13 装置の保守	8.23 ウェブ・フィルタリング
7.14 装置のセキュリティを保った処分又は再利用	8.24 暗号の使用
8.技術的管理策	8.25 セキュリティに配慮した開発のライフサイクル
8.1 利用者エンドポイント機器	8.26 アプリケーションのセキュリティの要求事項
8.2 特権的アクセス権	8.27 セキュリティに配慮したシステムアーキテクチャおよびシステム構築の原則
8.3 情報へのアクセス制限	8.28 セキュリティに配慮したコーディング
8.4 ソースコードへのアクセス	8.29 開発および受け入れにおけるセキュリティ試験
8.5 セキュリティを保った認証	8.30 外部委託による開発
8.6 容量・能力の管理	8.31 開発環境、試験環境および運用環境の分離
8.7 マルウェアに対する保護	8.32 変更管理
8.8 技術的ぜい弱性の管理	8.33 試験情報
8.9 構成管理	8.34 監査試験中の情報システムの保護

2. 管理策のテーマと属性

管理策の分類と構成

管理策の分類と構成

【参照：セミナーテキスト9-1-1.】
第9章 - 02

管理策：ISO/IEC27002

管理策
リスク対応のための対策のこと

ISO/IEC27002
ISO/IEC27001に記載されている要求事項を基に、さらに具体的なISMSの管理策を示した規格のこと。

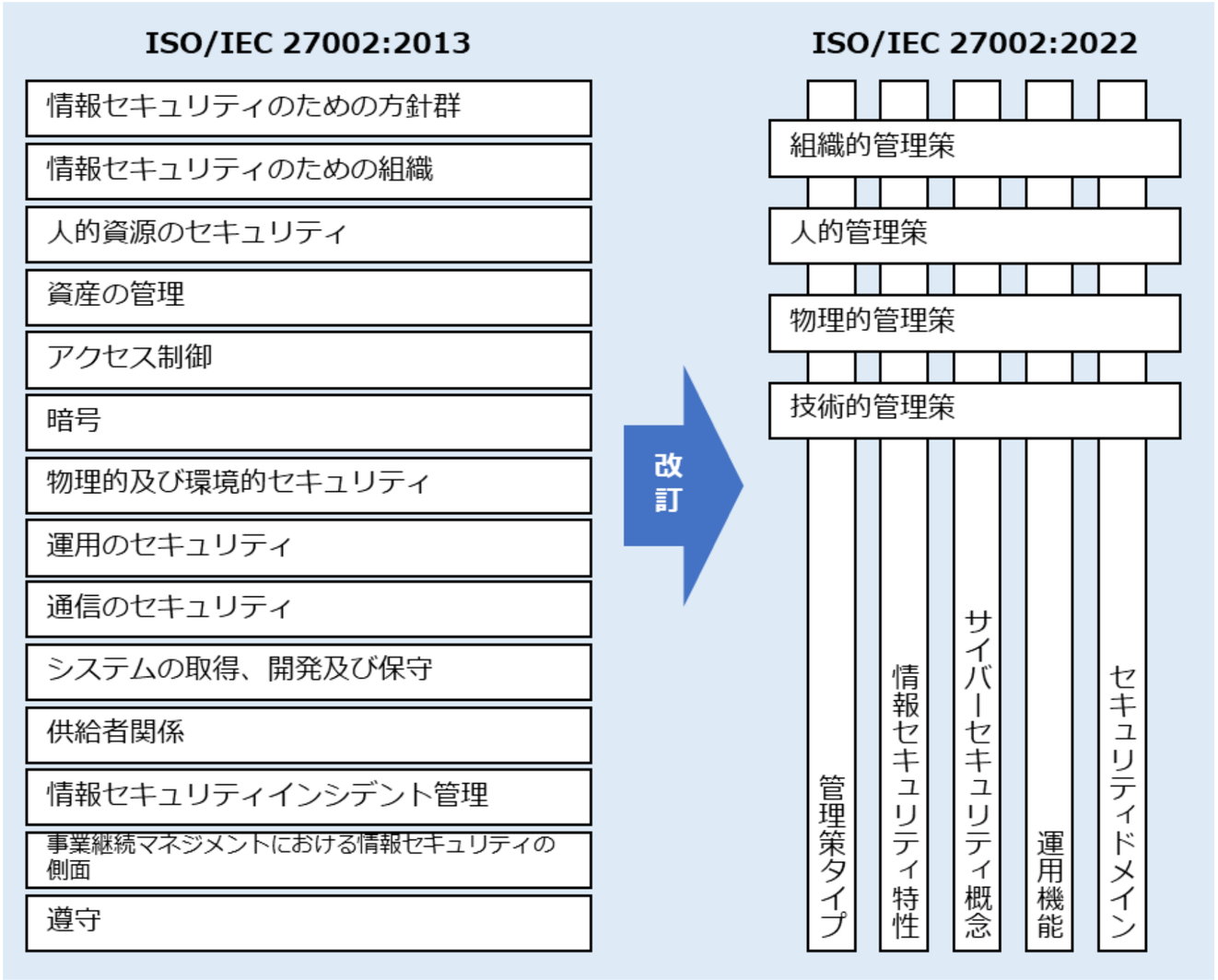
管理策の分類と構成

【参照：セミナーテキスト9-1-1.】
第9章 - 02

ISMS：2022年版

2013年版からの改定内容

- 管理策の項目数と章立てが変更され、テーマごとにカテゴリ分けされた
- 新たに属性の概念が導入された



管理策の分類と構成

【参照：セミナーテキスト9-1-2.】
第9章 - 03

テーマと属性

- ISO/IEC 27002の箇条5～8では、管理策が4つの分類（組織的・人的・物理的・技術的）に分けられ、これをテーマと呼ぶ。
- 各管理策に属性が付与し、より細かく見ることができる。

管理策の分類と構成

【参照：セミナーテキスト9-1-2.】
第9章 - 03

属性について

他の組織や団体が発行するガイドラインなどの考え方を取り入れているものもある

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	ー
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	ー

管理策の分類と構成

【参照：セミナーテキスト9-1-2.】
第9章 - 04

各テーマの管理策例示（組織的）

【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。

（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

管理策の分類と構成

【参照：セミナーテキスト9-1-2.】
第9章 - 04

各テーマの管理策例示（人的）

【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

管理策の分類と構成

【参照：セミナーテキスト9-1-2.】
第9章 - 05

各テーマの管理策例示（物理的）

【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。

（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

管理策の分類と構成

【参照：セミナーテキスト9-1-2.】
第9章 - 05

各テーマの管理策例示（技術的）

【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

3. 脅威、脆弱性、リスクの定義と関係性

用語の定義および関係性と識別方法

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-1.】
第10章 - 02

リスクマネジメントの理解に必要な用語の定義

用語	意味
リスク	目的に対する不確かさの影響
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
脆弱性	一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
管理策	リスクを修正する対策
保護要求事項	明示されている、通常暗黙のうちに了解されている又は義務として要求されている、ニーズ又は期待
資産	企業や組織などで保有している情報全般のこと。顧客情報や販売情報などの情報自体に加えて、ファイルやデータベースといったデータ、CD-ROMやUSB メモリなどのメディア、そして紙の資料も情報資産に含まれる

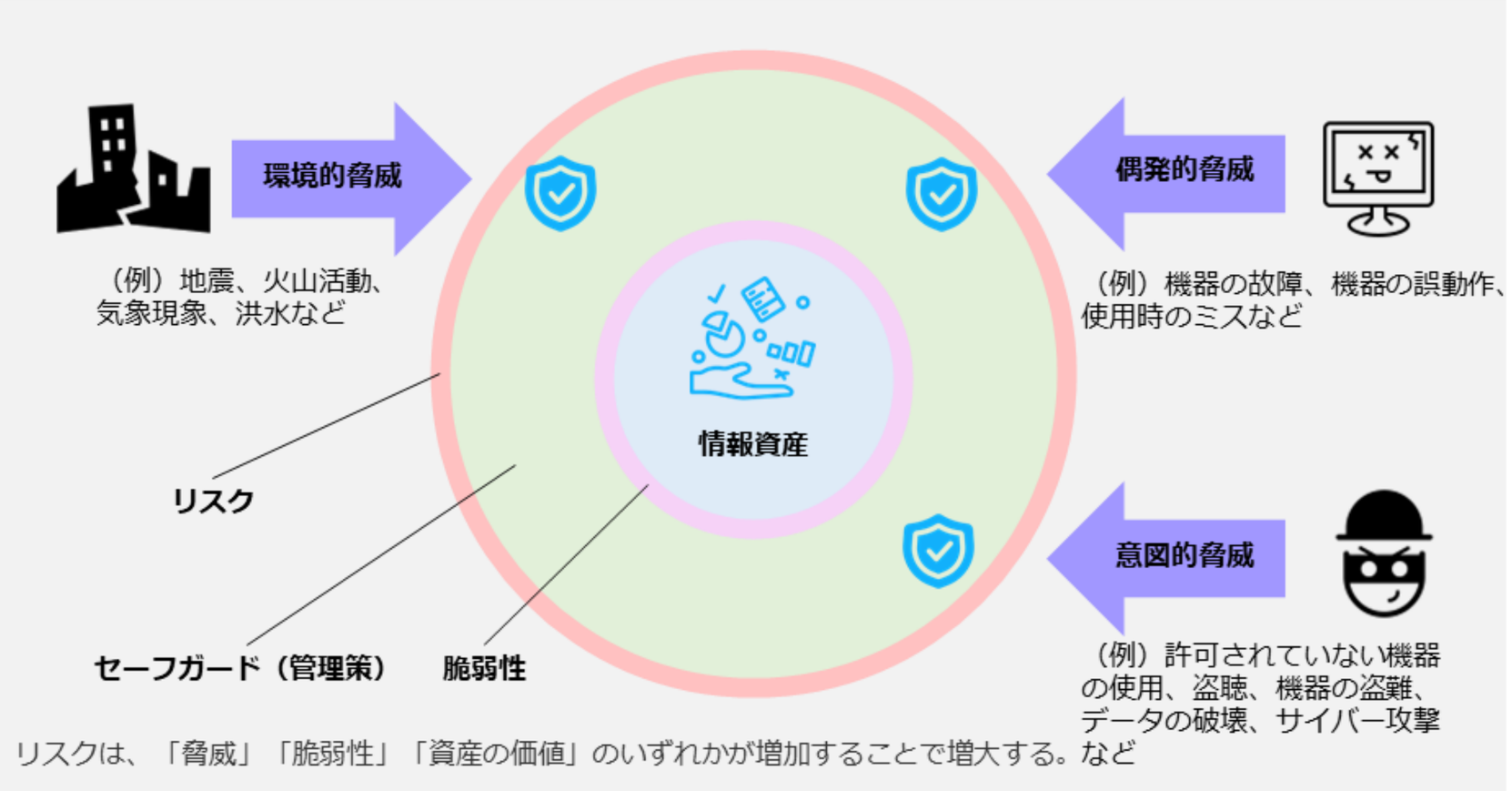
（出典）総務省「安心してインターネットを使うために 国民のためのサイバーセキュリティサイト 用語辞典」を基に作成

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-1.】
第10章 - 02

脅威、脆弱性、情報資産、セーフガード、リスクの関係

- 図にすると以下のようになる



脅威、脆弱性、情報資産、セーフガード、リスクの関係図

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-1.】
第10章 - 03

【例】業務用ノートPCのリスクマネジメント

- ノートPCに対して、各要素について検討する

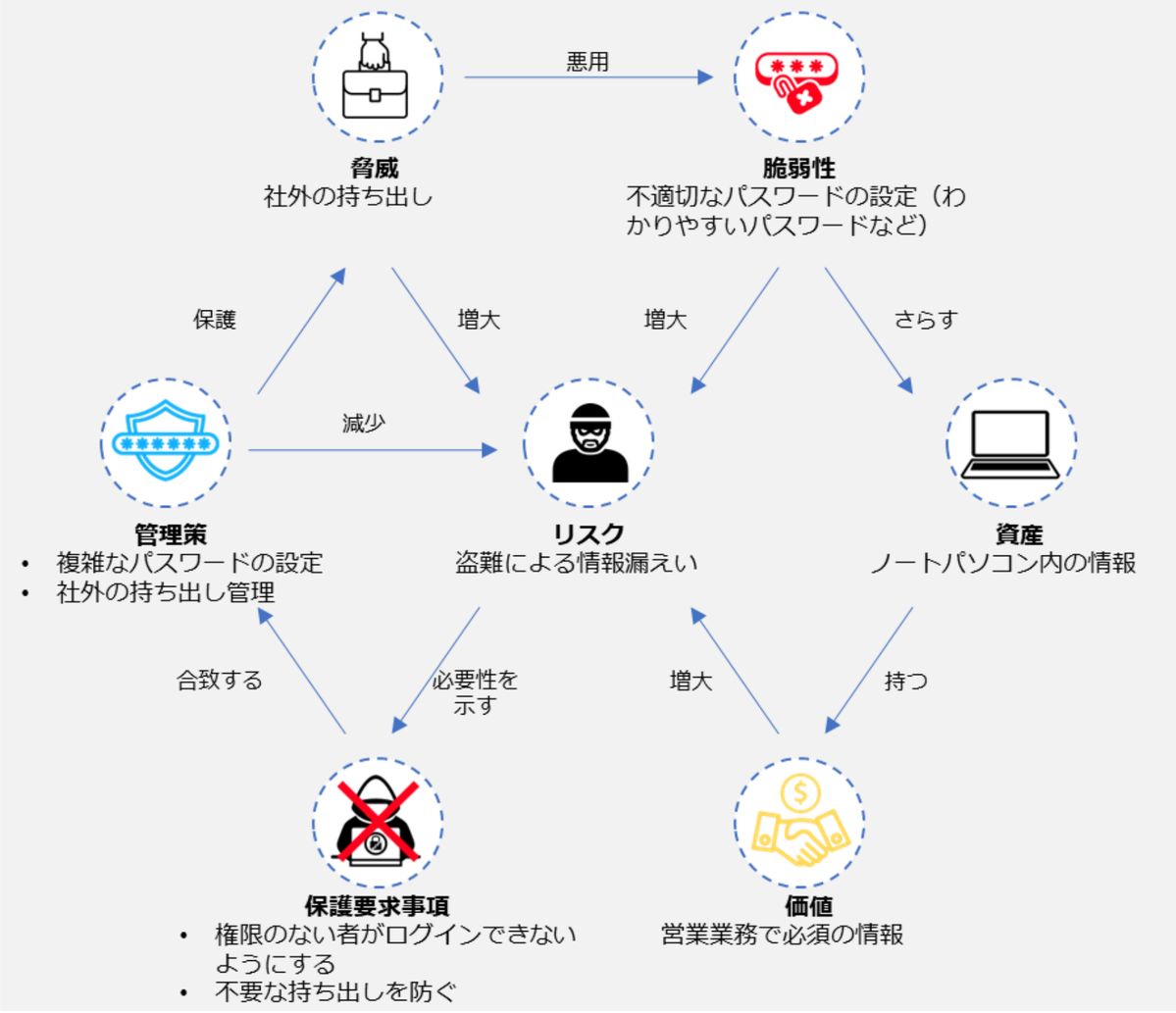
要素	内容
資産	ノートPC内の情報（データ）
価値	営業の業務で必須の情報
脅威	社外への持ち出し
リスク	盗難による情報漏えい
脆弱性	不適切なパスワードの設定（わかりやすい設定など）
保護要求事項	• 権限のないものがログインできないようにする • 不要な持ち出しを防ぐ
管理策	• 複雑なパスワードの設定（8.5 セキュリティを保った認証） • 社外の持ち出し管理（7.9 構外にある装置及び資産のセキュリティ（構外にある資産）

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-1.】
第10章 - 03

【例】業務用ノートPCのリスクマネジメント

- 関係性は次の通り



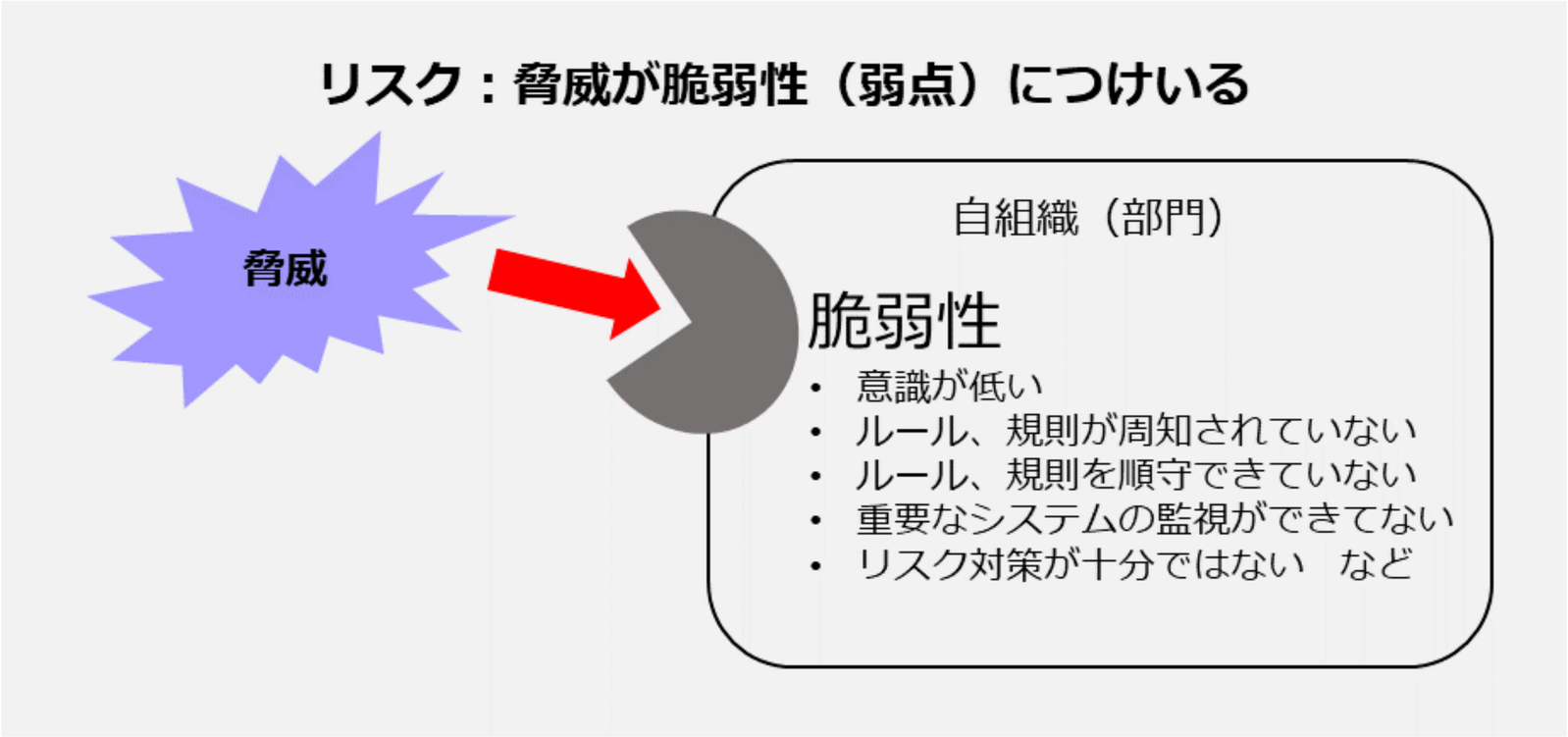
脆弱性、リスクの関係の事例

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-2.】
第10章 - 04

脅威の識別

- 脅威は「脆弱性」につけいり顕在化することで事故を起こす。



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

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-2.】
第10章 - 05

脅威の種類

- 脅威を区別することで、セキュリティ対策を整理しやすくなる

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)		被害：建物倒壊や火災による業務停止 対策：地震発生の可能性が低い場所を選択する、 災害からの回復対策を重視する
人為的脅威	意図的脅威 （Deliberate ➡ D）	被害：内部者による企業秘密の漏洩 対策：漏洩者を罰し、場合により損害賠償請求を行う 規程の明示と教育は抑止的対策の実施 漏洩の早期検知
	偶発的脅威 （Accidental ➡ A）	被害：入力ミスなどが原因の損害 対策：入力ミス防止の技術対策 2回入力 値の範囲制限 チェックデジットやチェックサムの設定

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

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-2.】
第10章 - 05

脅威の洗い出し

- 会社の資産に対し、脅威の識別を実施する
- 意図的脅威は、次の観点から判断する
  - 攻撃の動機や攻撃に必要なスキル
  - 利用可能なリソース
  - 資産の特性や魅力
  - 資産の脆弱性
- 偶発的脅威は次の観点から判断する
  - 人為的なミス
  - 誤動作

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

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-2.】
第10章 - 04

脅威の洗い出し

- 脅威を区別することで、セキュリティ対策を整理しやすくなる

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
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）コピーソフトウェアの使用	A, D

脅威の一覧表の例
（出典）「ISO/IEC 27005」を基に作成

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

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-3.】
第10章 - 06

脆弱性の識別

- 脆弱性を減らすためには適切な管理策の実施が必要
- 脆弱性は管理策の欠如を意味する
  - 例：
    脆弱性：アクセス権の誤った割り当て
    管理策：アクセス権の適切な設定
- 脆弱性は資産の性質から考えると識別しやすくなる
  - 例：クラウドサービス
    特性：インターネットがあればどこでも利用可能
    脆弱性：インターネットからの不正アクセス

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-3.】
第10章 - 06

脆弱性の識別例

類型	脆弱性	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

脆弱性の識別例
（出典）「ISO/IEC 27005」を基に作成

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-3.】
第10章 - 06

脆弱性の識別例

類型	脆弱性	脅威の例
ソフトウェア	離席時にログアウトしない	権限の濫用
	適切に削除されていない記憶媒体の処理または再利用	権限の濫用
	監査証跡の欠如	権限の濫用
	アクセス権の誤った割り当て	権限の濫用
	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	使用時のミス
	ユーザの認識及び認証メカニズムの欠如	権限の詐称
	不十分なパスワード管理	権限の詐称
	不要なサービスが実行可能	データの違法な処理
	開発者のための不明確又は不完全な仕様書	ソフトウェアの誤作動
	効率的な変更管理の欠如	ソフトウェアの誤作動
	管理されていないソフトウェアのダウンロード及び使用	ソフトウェアの改ざん
	バックアップコピーの欠如	ソフトウェアの改ざん

脆弱性の識別例
（出典）「ISO/IEC 27005」を基に作成

用語の定義および関係性と識別方法

【参照：セミナーテキスト10-1-3.】
第10章 - 06

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

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