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2回

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】

セミナー内容

編	テーマ
第1編	サイバーセキュリティを取り巻く背景
第2編	中小企業に求められるデジタル化の推進とサイバーセキュリティ対策
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
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
第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

編	テーマ
第6編	ISMS等のフレームワークの種類と活用法の紹介
第7編	ISMSの構築と対策基準の策定と実施手順
第8編	具体的な構築・運用の実践
第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第10編	全体総括

セミナー内容

第7章. セキュリティ対策の概要（全容）

第8章. 用語定義および関係性と識別方法

第9章. 具体的手順の作成（Lv.1 クイックアプローチ）

第10章. 具体的手順の作成（Lv.2 ベースラインアプローチ）

第7章. セキュリティ対策の概要（全容）

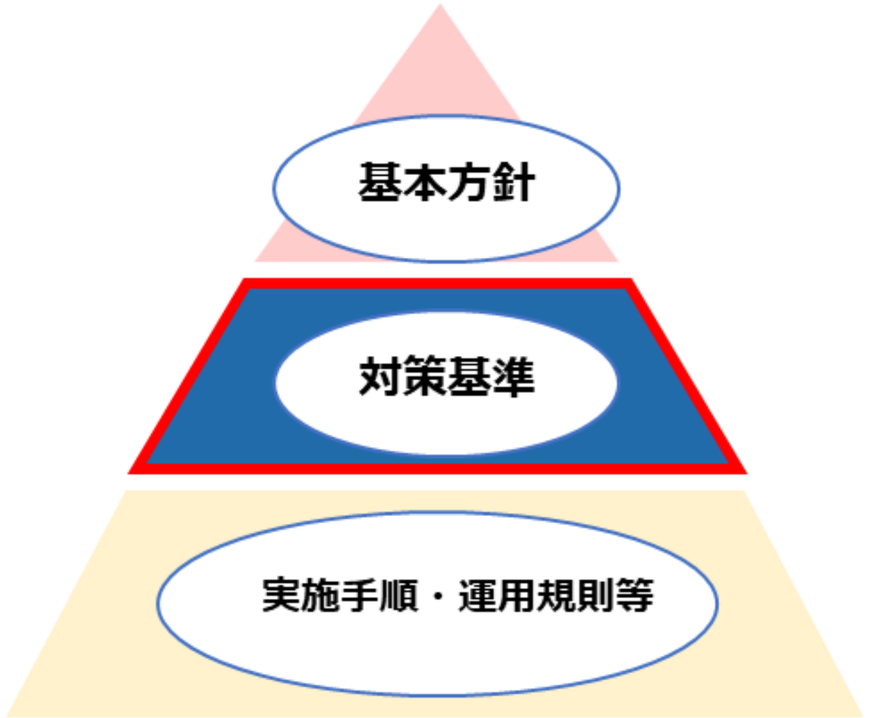
対策基準の策定

対策基準の策定

セキュリティ対策基準の概要

【参照：テキスト7-1-1.】
P3

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順守”

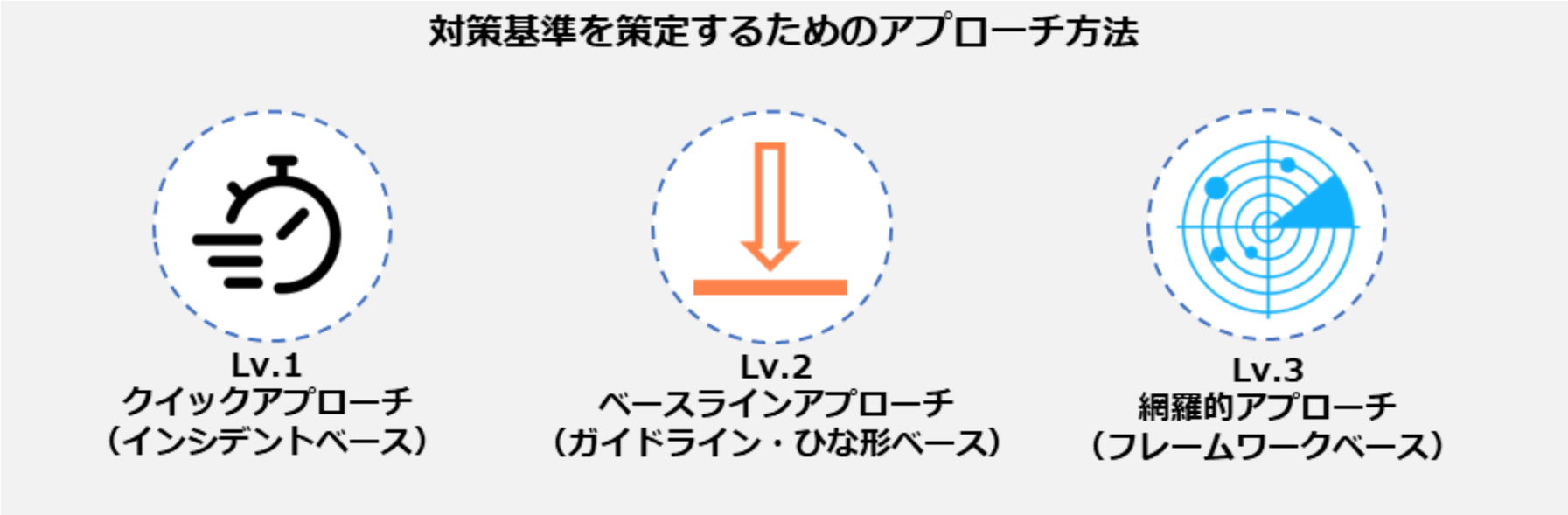
基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

対策基準の策定

対策基準のアプローチ方法

【参照：テキスト7-1-1.】
P3, P4

- 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

対策基準のアプローチ概要

【参照：テキスト7-1-2.】
P4, P5

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。 • さまざま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型を参考とし、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

メリット・デメリット

【参照：テキスト7-1-2.】
P4, P5

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。 • 流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

Lv.1 クイックアプローチ

【参照：テキスト7-1-2.】
P5, P6

【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、重要情報の詐取など
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

(出典) IPA「情報セキュリティ10大脅威 2024」をもとに作成

対策基準の策定

Lv.2 ベースラインアプローチ

【参照：テキスト7-1-2.】
P7, P8

【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）」をもとに作成

対策基準の策定

【参照：テキスト7-1-2.】
P8

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情報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

第8章. 用語定義および関係性と識別方法

用語の定義、脅威・脆弱性の識別

用語の定義、脅威・脆弱性の識別

用語の定義と関係性

【参照：テキスト8-1-1.】
P10, P11

主な用語の定義

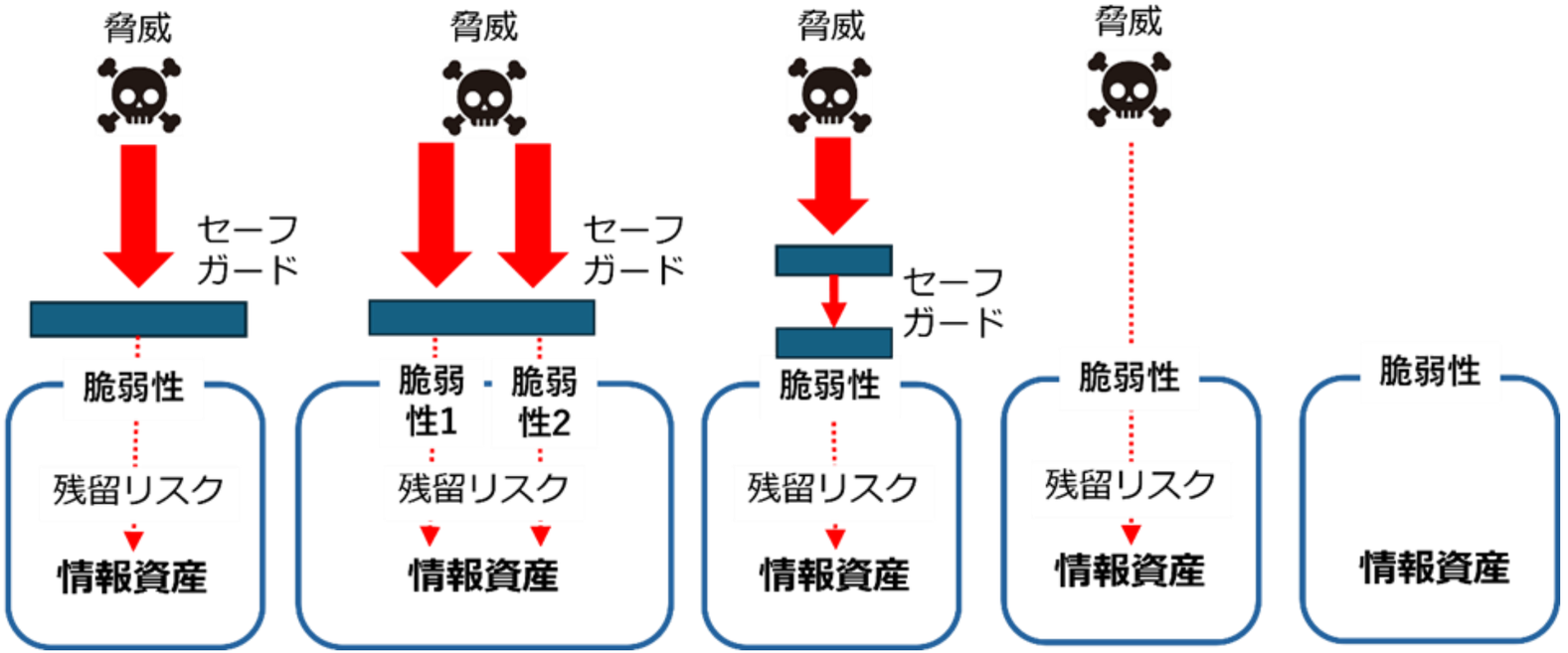
- 脅威
- 脆弱性
- インシデント
- 資産
- 資産情報の重要度
- セーフガード（管理策）
- リスク
- 残留リスク
- リスク値

用語の定義、脅威・脆弱性の識別

関係図

【参照：テキスト8-1-1.】
P11, P12

	ケース1	ケース2	ケース3	ケース4	ケース5
脅威	あり	あり	あり	あり	なし
セーフガード（管理策）	あり	あり	あり（多段）	あり	あり
脆弱性	あり	あり（複数）	あり	あり	あり
リスク	低減	低減	低減	受容	不明



用語の定義、脅威・脆弱性の識別

【例】業務用ノートPCのリスクマネジメント

【参照：テキスト8-1-1.】
P12, P13

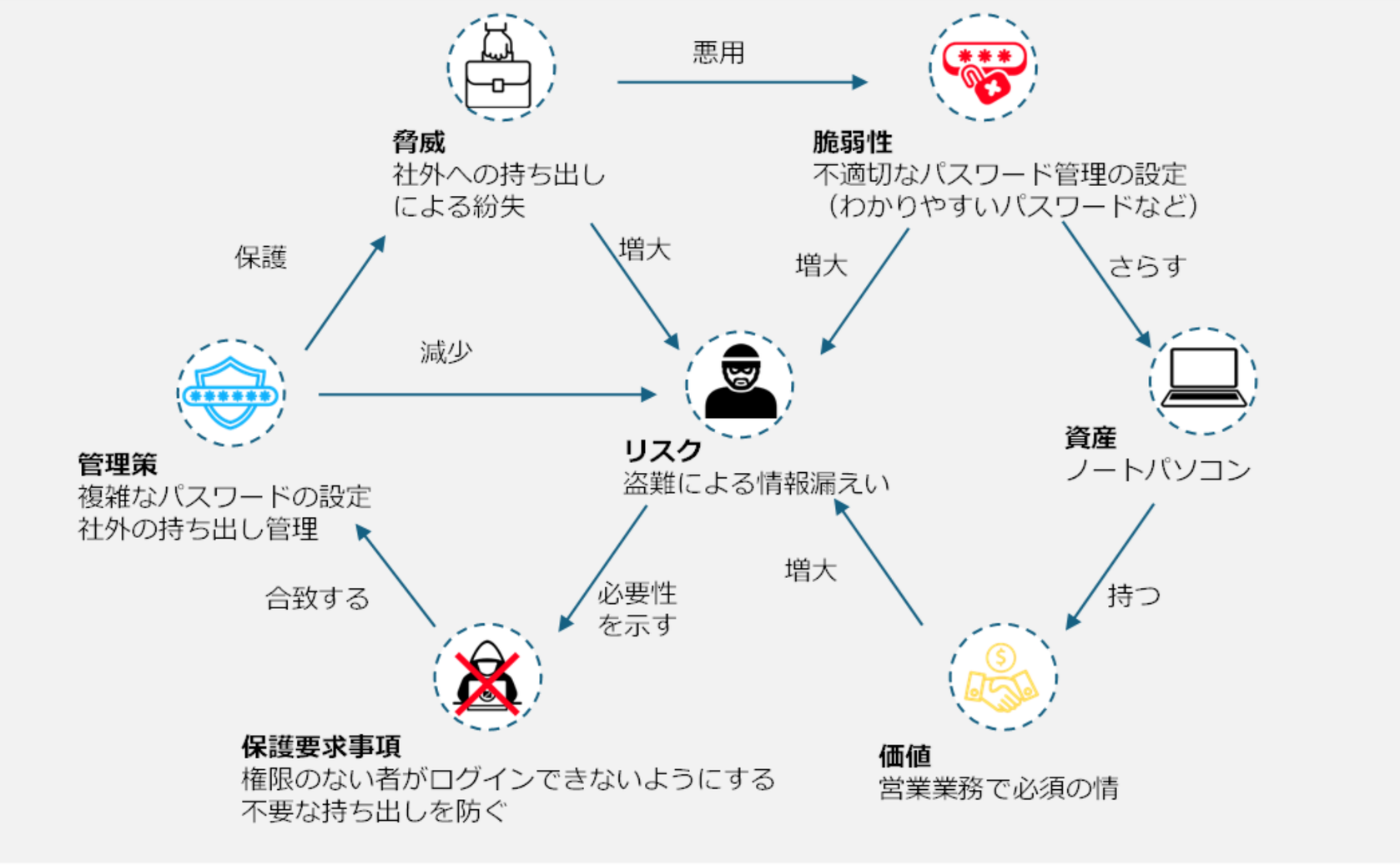
- ノートPCに対して、各要素について検討する

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、脅威・脆弱性の識別

【例】業務用ノートPCのリスクマネジメント

【参照：テキスト8-1-1.】
P13

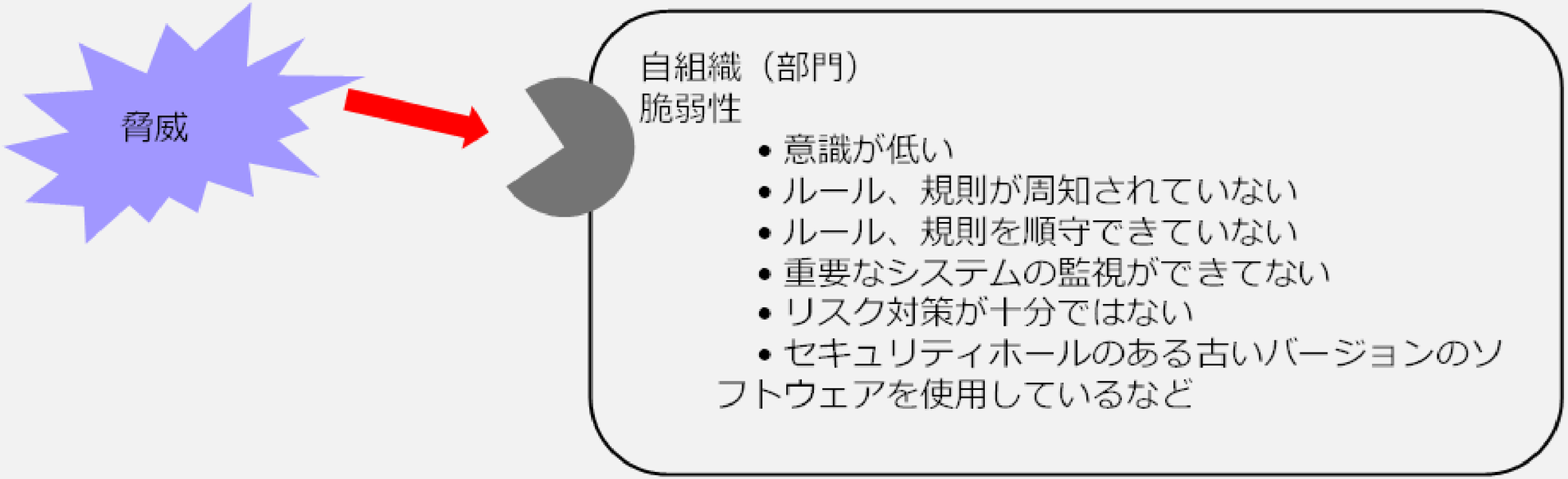


用語の定義、脅威・脆弱性の識別

脅威の識別

【参照：テキスト8-1-2.】
P14, P15

リスク：脅威が脆弱性（弱点）に付け入る



用語の定義、脅威・脆弱性の識別

脅威の種類

【参照：テキスト8-1-2.】
P15

- 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えい 対策：漏えい者を罰し、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 漏えいの早期検知
	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

用語の定義、脅威・脆弱性の識別

脆弱性の識別例

【参照：テキスト8-1-3.】
P16

類型	脅威の例	脆弱性
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

用語の定義、脅威・脆弱性の識別

脆弱性の識別例

【参照：テキスト8-1-3.】
P16

類型	脅威の例	脆弱性
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り当て
	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
	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

第9章. 具体的手順の作成（Lv.1 クイックアプローチ）

【Lv.1 クイックアプローチ】の概要

【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】の概要

クイックアプローチ

【参照：テキスト9-1.】
P21

概要

- 報道される事例や情報セキュリティ10大脅威を参考にする
- 発生する可能性が高いセキュリティインシデント事例を考慮する
- セキュリティインシデント発生時に被害が大きい事例を考慮する

メリット

- 低コストで効果的な対策が可能で、リソースが限られていても実施可能
- 流行中の攻撃に迅速に対応し、影響を最小限に抑えられる

デメリット

- 包括的でないため抜けが発生しやすく、一時的な対策になりがち
- 長期的には費用が増加する可能性がある

セキュリティインシデント事例を参考とした実施手順

対策基準・実施手順の作成手順

【参照：テキスト9-2.】
P22

インシデント事例

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。たとえば、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、人件費だけでなく、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を参考とした実施手順

リスクアセスメントの実施

【参照：テキスト9-2.】
P22, P23

リスク特定

- 対象となる資産情報の洗い出し
- 機密性、完全性、可用性の評価
- 重要度の算出

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

セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：テキスト9-2.】
P23

リスク分析

- 重要度と被害発生可能性から、リスクレベルを算出

「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	管理部署	媒体・保存先	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	人事部	人事担当者のPC	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	経理部	経理担当者のPC	3	3	2	3	2	6
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	2	6

セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：テキスト9-2.】
P24

リスク評価

- リスク対応を検討する

要素	内容
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する
リスク移転	リスクを他社に移す
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
リスク受容（保有）	セキュリティ対策を行わず、リスクを受け入れる

セキュリティインシデント事例を参考とした実施手順

対策基準の策定

【参照：テキスト9-2.】
P24

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

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：テキスト9-2.】
P24, P25

実施手順（例）

機密情報に関する社内規程の策定

- 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。

●
●
●

＜詳細はテキストP25、P26を参照＞

第10章. 具体的手順の作成（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】の概要

【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

【Lv.2 ベースラインアプローチ】の概要

ベースラインアプローチ

【参照：テキスト10-1.】
P28

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する
- 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する

メリット

- 組織全体で一貫性を確保できる
- コストパフォーマンスよく、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

デメリット

- 十分なセキュリティ水準を確保できない可能性がある
- ひな型は一般的なものであるため、自社に合わせて検討が必要

ガイドラインを参考とした実施手順

情報セキュリティ対策ガイドラインの活用

【参照：テキスト10-2-1.】
P29, P30

参考にするガイドラインの例

- 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」

ガイドラインを参考とした実施手順

中小企業の情報セキュリティ対策ガイドラインの活用

【参照：テキスト10-2-2.】
P30, P31, P32

対象者

- 中小企業および小規模事業者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

使い方

1. 実施状況の把握
2. 対策の決定と周知

ガイドラインを参考とした実施手順

インターネットの安全・安心ハンドブックの活用

【参照：テキスト10-2-3.】
P33, P34

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る
- サイバーセキュリティ対する素養・基本的な知識を身につける

使い方

1. ハンドブック記載内容を確認する
2. 自社の状況を把握する
3. 新たな実施手順を策定する

ガイドラインを参考とした実施手順

テレワークセキュリティガイドラインの活用

【参照：テキスト10-2-4.】
P34, P35

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する
- 安心してテレワークを導入・活用する

使い方

1. 立場ごとに分類された具体的に実施すべき項目を確認する
2. 自社の状況を把握する
3. 規程や手順に反映させる

ガイドラインを参考とした実施手順

【参照：テキスト10-2-5.】
P35, P36

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

使い方

1. クラウドサービス安全利用チェックシートを活用する
2. 解説編を参考に、利用者としての役割や責任を認識する
3. 実施手順を策定する

ガイドラインを参考とした実施手順

【参照：テキスト10-2-6.】
P36, P37, P38, P39

情報セキュリティ関連規程の活用

対象者

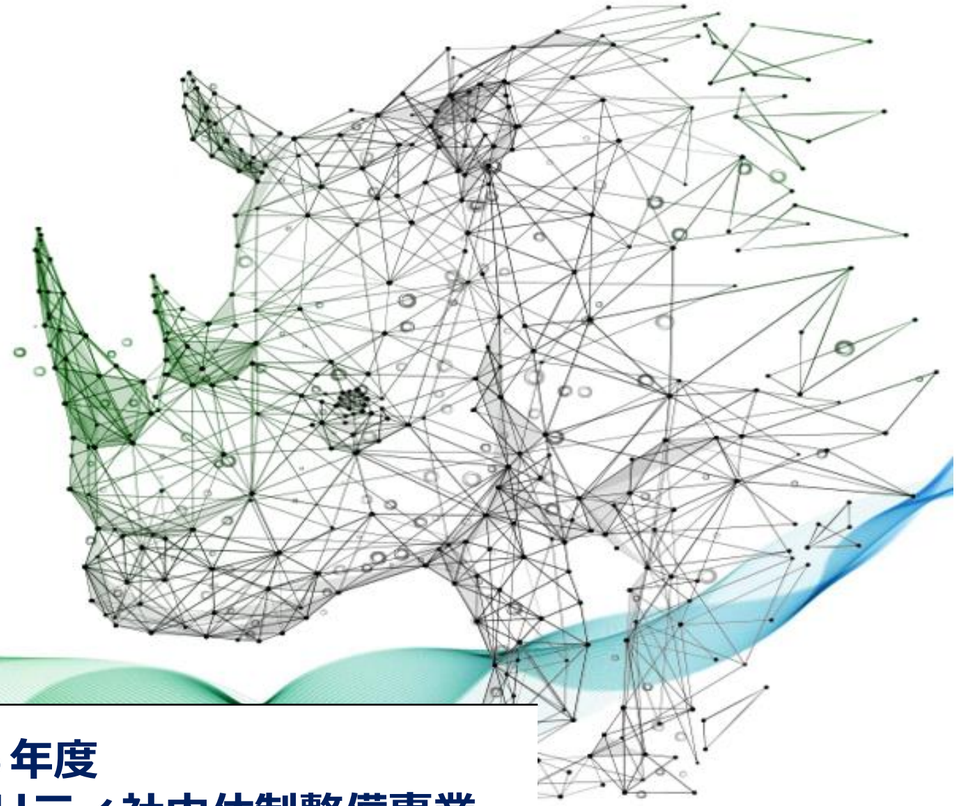
- 中小企業

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

使い方

1. 対応すべきリスクを特定する
2. セキュリティ対策の決定
3. 規程の作成



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