Japan Information Security
Management Systems User Group

# どっちで考える？リスクアセスメント

## ～「資産ベース」と「シナリオベース」の使い分け～

日本ISMSユーザグループインプリメンテーション研究会

北村俊樹　(JNSA特別会員 情報処理安全確保支援士会)

本発表は私個人の考察であり、所属各団体を代表するものではありません。

# リスクアセスメント、何から始めますか？

～資産ベースとシナリオ／イベントベースをどう使い分けるか～

**「資産を洗い出して評価する」**方法もあれば、
**「実際に何が起きるか」**をシナリオで考える方法もあります。

**資産ベース**

**何を守るか？**

**シナリオ／イベント**

**何が起きるか？**

では、どちらを使えばよいのか？

**今日は「見えているものの違い」から考えていきます**

# まず、「何を守るのか」を整理


**資産ベースの出発点は「守る対象を全体として把握する」こと**

# 資産ベースで「何が分かる」のか？

01
**何を守るか**
情報・プロセス

02
**どこにあるか**
保存先・媒体

03
**何が重要か**
重要度

04
**何が弱いか**
脅威・脆弱性

05
**リスク**

全体を俯瞰し、**「重要な資産は何か」**「**どこにリスクがあるか**」を整理できる

**資産ベース ＝ リスクの「地図」を作る**

# しかし、資産ベースだけでは「何が起きるか」が見えにくい

## 資産ベースで分かること

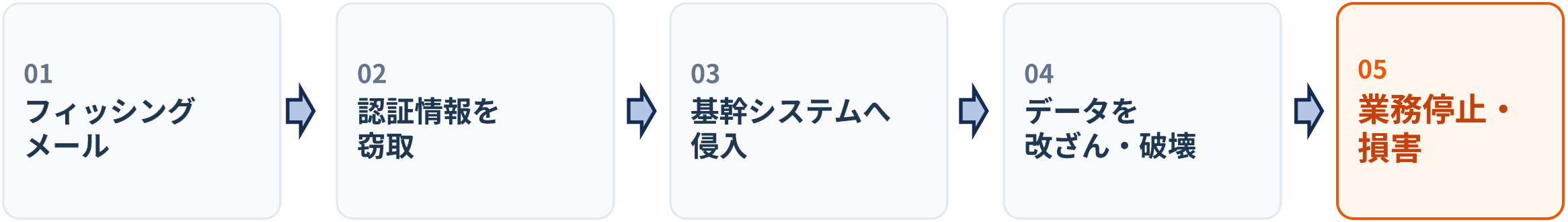
- 守るべき情報・事業プロセス
- 保存先・媒体
- 重要度
- 脅威・脆弱性とリスク

## 資産ベースだけでは見えにくいこと

- 攻撃・事故がどう進展するか
- 複数資産にまたがる影響
- 発生から被害までの連鎖
- 具体的なシナリオに沿った対策

**ポイント：脅威・脆弱性を「選んで数値化」するだけでは、現実のリスクの進展が十分に見えない**

# そこで、シナリオ／イベントベースで「何が起きるか」を追う




誰が ・ どこから ・ どうする ・ 何が起きる

**発生 → 進展 → 影響を可視化することで、「具体的な対策」を考えやすくなる**

# 資産ベースとイベントベースは、見ているものが違う

| 資産ベース | シナリオ／イベントベース |
| --- | --- |
| 何を守るか？ | 何が起きるか？ |
| ・情報・事業プロセス<br>・保存先・サポート資産<br>・重要度<br>・脅威・脆弱性<br>・資産ごとのリスク | ・攻撃・事故の発生<br>・事象の進展<br>・複数資産への連鎖<br>・最終的な事業影響<br>・シナリオに沿った対策 |
| リスクの「地図」を作る | 地図上で「何が起きるか」を追う |

→ だから、次のステップでは両者を組み合わせる

# だから、両者を組み合わせる

① 資産ベース

全体を俯瞰
重要な資産・プロセスを特定

② シナリオベース

重要資産に
具体的な脅威を当てはめる

③ リスクを再確認

影響・発生可能性を
シナリオで見直す

④ リスク対応

何を・なぜ・どこまで
守るかを決める

「網羅性」＋「具体性」＝ 対策の優先順位と意思決定につなげる

**リスク値を計算して終わらせない**

# ここからは参考資料

# リスクアセスメントの対象

**JIS Q 27002:2024**

**3.1.2**

**資産**(asset)

組織にとって価値のある全てのもの

注釈1 情報セキュリティにおいては,次の2種類の資産を区別することが可能である。

- 主要資産
  - 情報
    - 事業プロセス(3.1.27)及び活動
- (主要資産が依存する)全ての種類のサポート資産。例えば,次がある。
    - ハードウェア
  - ソフトウェア
  - ネットワーク
  - 要員(3.1.20)
  - サイト
  - 組織の構造

＊ 日本産業標準調査会(JISC)のHPの「JIS検索」から、本文を閲覧できます。https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html

# 資産ベースのアプローチ

中小企業の情報セキュリティ対策ガイドラインより

# 資産ベースのアプローチ


- 中小企業の情報セキュリティ対策ガイドラインでは、ISO/IEC 27005を参考にしており資産ベースのリスク分析の説明がある。
- リスク値の算定においては、脅威と脆弱性を数値化する必要があるが、脅威と脆弱性を特定する方法が明確に書かれていない。

# 資産ベース：網羅的な「静」の分析

- 特徴: 資産管理台帳に基づき、すべての資産をフラットに評価する。
- メリット: 漏れがない。客観的な数値で優先順位がつけやすい。
- 出典：中小企業の情報セキュリティガイドライン P.44～45

【表 5】リスク値の算定基準

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

×掛け算

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

| | | |
|---|---|---|
| 被害発生可能性 | 3高 | 通常の状況で被害が発生する（いつ発生してもおかしくない） |
| | 2中 | 特定の状況で被害が発生する（年に数回程度） |
| | 1低 | 通常の状況で被害が発生することはない |

| | | |
|---|---|---|
| リスク値 | 9～6 大 | 深刻な事故が起きる可能性大 |
| | 4 中 | 重大な事故が起きる可能性有 |
| | 3～1 小 | 事故が起きる可能性小、起きても被害は受容範囲 |

# 中小企業の情報セキュリティ対策ガイドライン

- STEP3はSCS評価制度の★3・★4に相当。
- リスクアセスメントは、STEP4に登場。

| STEP | 取り組みの目安 | 想定している企業の例 |
|---|---|---|
| STEP1<br>(P20) | すべての企業が実施すべき基本的なセキュリティ対策であり、「情報セキュリティ６か条」を活用し、自社の業務・情報・従業員・取引先を守る必要最低限の対策から始めます。 | STEP を目指すきっかけ<br>●アナログ中心だったが、近年業務にITを取り入れ始めた<br><br>企業をとりまく状況<br>●周囲の取引先でセキュリティ被害が発生し、その脅威を身近に感じた　等 |
| STEP2<br>(P22) | 基本的なセキュリティ対策を組織的に取り組むために、「5分でできる！情報セキュリティ自社診断」を活用し、自社の弱みを把握し基本的対策を決定するとともに、組織としての情報セキュリティ基本方針を作成します。 | STEP を目指すきっかけ<br>●業務の効率化や情報共有促進のために、ITシステムの本格導入を進めている<br><br>企業をとりまく状況<br>●セキュリティ対策が標準化されず、従業員の属人的な対応となっていた　等 |
| STEP3<br>(P26) | 組織的な取り組みを強化し、セキュリティ対策に本格的に取り組む企業は、必要に応じて外部専門家を交え、セキュリティに関する体制を整備し、基本的な組織的対策や技術的な防御対策を実施します。 | STEP を目指すきっかけ<br>●取引先からの要請を受けて、高度なセキュリティ対策が必要となった<br><br>企業をとりまく状況<br>●日常的に受発注をしているなど、取引先企業が必要不可欠な存在となっている　等 |
| STEP4<br>(P42) | より強固で広範囲なセキュリティ対策のためには、人的・組織的な対策だけでなく、必要に応じて外部専門家を交えてリスク分析を行い、技術的な対策の強化により包括的なセキュリティ対策を実施します。 | STEP を目指すきっかけ<br>●外部監査への対応や基準達成のため、従来以上に厳格なセキュリティ対策が必要となった<br><br>企業をとりまく状況<br>●企業活動においてITやデジタル技術が欠かせない存在となり、DXを積極的に推進している　等 |

# リスクアセスメントはSCS評価制度★３・★４の要求にはない

3. 構築する評価制度

## [参考] ISMS適合性評価制度と本制度の比較

- 本制度(★３・★４)は、代表的な脅威を参考に効果の高い管理策を抽出するベースラインアプローチを採用。
- ★５段階では、組織におけるリスクベースの改善プロセスを整備した上で、システムへの具体的な対策実装が必要であり、ISMS適合性評価制度との整合に配慮しつつ、令和８年度以降具体的なあり方等を検討する予定。

| | ISMS適合性評価制度 | ★５ 要求事項（イメージ） | 本制度(★３・★４) |
|---|---|---|---|
| 目的 | ・組織が運用する情報セキュリティマネジメントシステム(ISMS)が、国際規格に基づいて適切に運用管理されていることを第三者が公平な立場から審査し証明するための、国際的に整合の取れた枠組みを確保・維持すること | | ・サプライチェーン全体でのサイバーレジリエンスの向上<br>・部品供給、業務委託等のビジネスサプライチェーンを通じたサイバーリスク(※)への対応を重視<br>(※)事業・サービスの供給途絶リスク、機密情報の漏えい改ざんリスク、取引先等を踏み台とした不正侵入リスク等 |
| 取得範囲 | ・ISMSを運用する「組織」が対象<br>(組織の単位は、管理する情報に応じて、認証取得を希望する組織が対象範囲を決定する。一企業内の特定部門のほか、グループ企業全体を認証範囲とすることもある。) | システムへの具体的な対策実装 | ・「インターネットに接続している自社IT基盤」が対象(一般的に、IT基盤が外部からの不正侵入やNW横展開の足掛かりとなるため、リスクの高いシステムとして制度側で指定)<br>・取引先管理の観点を盛り込み |
| 採用する管理策 | ・リスクアセスメント結果に基づいて、リスク対策のために必要な情報セキュリティ管理策を組織が決定する。<br>・ISO/IEC27001(JISQ27001)附属書Aを参照し、情報セキュリティ管理策(組織的・人的・物理的・技術的)に漏れがないかどうかを確認する。 | ＋<br>組織におけるマネジメントシステムの確立 | ・代表的な脅威や国内外制度を参考に、効果の高い管理策を業界横断的なコンセンサスとして設定することを目指す。<br>★３：取引上の要請に応えるために最低限必要な対策<br>★４：侵害の早期発見・拡大防止等に必要な対策 |
| 審査の観点 | ・ISO/IEC 27001で規定されている要求事項に適合したISMSが構築・運用できているか | | ・各段階(★３・★４)で求める具体的なセキュリティ対策が実装されているか |
| 特徴 | ■ リスクアセスメント結果に基づき、組織自らが適切な管理策を決定<br>■ 認証により、組織的に対策を維持・向上させる仕組み(マネジメントシステム)が構築できていることを証明 | ISMS取得後★を取得<br>相互補完的な制度として両輪で発展<br>★取得後ISMSを取得 | ■ 代表的な脅威・リスクを前提に、具体的な対策や範囲が決められているため、何をするか迷うことが少ない<br>■ システムへの対策実装を、第三者評価で確認(★４) |

28

# ガイドラインのSTEP４　より強固にするための対策

### (1)資産ベースのリスク分析
「資産管理台帳(サンプル)」(付録6)の「リスク値算定」シートを活用した、各企業の状況に応じてリスクを特定する資産ベースのリスク分析について説明します。

### (2)技術的対策例と活用
様々な技術的対策について説明します。自社の環境に合わせて活用してください。

### (3)セキュリティサービス例と活用
情報セキュリティに関する外部サービスを説明します。情報セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用です。

### (4)ウェブサイトの情報セキュリティ
ウェブサイトを安全に構築し、運用するためのポイントを説明します。

### (5)クラウドサービスの情報セキュリティ
クラウドサービスを安全に利用するためのポイントを説明します。

### (6)テレワークの情報セキュリティ
テレワークを安全に実施するためのポイントを説明します。

### (7)セキュリティインシデント対応
セキュリティインシデント発生時の対応に関するポイントを説明します。情報セキュリティにおいても、事業継続の観点から被害を最小化し、早期に復旧するために、インシデントを想定した備えを行う必要性があります。

**③資産ベースのリスク分析**
情報資産ごとに「資産価値」「脅威」「脆弱性」を識別し、対策を検討する方法。個々の情報資産に適した対策が可能だが手間がかかる。
例)システムを構成する各資産(サーバー、端末、通信機器等)に対して、「資産価値」「脅威」「脆弱性」の3つを評価指標として、対策を検討・実施する。

### (1)資産ベースのリスク分析
各企業の状況に応じてリスクを特定する資産ベースのリスク分析の実施方法について解説します。自社の情報資産や関連する機器等を一覧化して管理するための**「資産管理台帳（サンプル)」(付録6)**の「リスク値算定」シートを活用しながら、以下の手順で行います。

**手順１ 情報資産の洗い出し** → **手順２ リスク値の算定** → **手順３ 情報セキュリティ対策の決定**

- STEP4は、（1）の手順３で、（2）～（7）のセキュリティ対策を決定する構成となっている。

# STEP４の手順１

## 手順1 情報資産の洗い出し

### どのような情報資産があるか洗い出して重要度を判断する

業務で利用する電子データや書類を**「資産管理台帳（サンプル）」（付録６）**の情報資産管理台帳に記入します。記入した情報資産ごとに漏えいや改ざん、誤びゅう（誤記、計算違い）が起きたり、必要な時に利用できないときの、事業への影響の観点から重要度を判断します。

業種、事業内容、IT 環境によって保有する情報資産は異なるため、**「資産管理台帳（サンプル）」（付録６）**の「台帳記入例」・「重要度定義」シートを参考に、以下の要領で作業を進めます。

**①情報資産管理台帳の作成**

パソコンのハードディスクや机の引き出しを見るのではなく、日常どのような電子データや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。

**②情報資産ごとの機密性・完全性・可用性の評価**

機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなど、評価値３～１を記入します。

**③機密性・完全性・可用性の評価値から重要度を算定**

重要度は、機密性、完全性、可用性いずれかの最大値で判断します。前項の作業で「情報資産管理台帳」の所定欄に記入した機密性･完全性･可用性の評価値をもとに、重要度を算定します。

- 情報を洗い出し、資産管理台帳に情報を記載してその重要度を算定する。

# STEP４の手順１

情報資産管理台帳

| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 管理者名 | 管理者連絡先 | 媒体・保存先 | 評価値 機密性 | 評価値 完全性 | 評価値 可用性 | 重要度 | 保存期限 | 登録日 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | ○○ ○ | 090-XXXX-XXXX | 事務所PC | 3 | 1 | 1 | 3 | | 2026/4/1 |
| 人事 | 健康診断の結果 | 雇入時・定期健康診断 | 人事部 | 人事部 | ○○ ○ | 090-XXXX-XXXX | 書類 | 3 | 3 | 2 | 3 | 5年 | 2026/4/1 |
| 経理 | 給与システムデータ | 税務署提出用源泉徴収票 | 給与計算担当 | 人事部 | ○○ ○ | 090-XXXX-XXXX | 事務所PC | 3 | 3 | 2 | 3 | 7年 | 2026/4/1 |
| 経理 | 当社宛請求書 | 当社宛請求書の原本（過去3年分） | 総務部 | 総務部 | △△ △ | 090-XXXX-XXXX | 書類 | 2 | 2 | 2 | 2 | | 2026/4/1 |
| 共通 | 電子メールデータ | Gmailに転送 | 担当者 | 総務部 | △△ △ | 090-XXXX-XXXX | 社外サーバー | 3 | 3 | 3 | 3 | | 2026/4/1 |
| 営業 | 顧客リスト | 得意先（直近５年間に実績があるもの） | 営業部 | 営業部 | ×× × | 090-XXXX-XXXX | 可搬電子媒体 | 3 | 2 | 2 | 3 | | 2026/4/1 |
| 営業 | 顧客リスト | 得意先（直近５年間に実績があるもの） | 営業部 | 営業部 | ×× × | 090-XXXX-XXXX | モバイル機器 | 3 | 2 | 2 | 3 | | 2026/4/1 |
| 営業 | 受注契約書 | 受注契約書原本（過去10年分） | 営業部 | 営業部 | ×× × | 090-XXXX-XXXX | 書類 | 2 | 3 | 2 | 3 | | 2026/4/1 |
| 営業 | 製品カタログ | 現役製品カタログ一式 | 営業部 | 営業部 | ×× × | 090-XXXX-XXXX | 社内サーバー | 1 | 2 | 2 | 2 | | 2026/4/1 |
| 調達 | 委託先リスト | 外部委託先（直近５年間に実績があるもの） | 総務部 | 総務部 | □□ □ | 090-XXXX-XXXX | 社内サーバー | 1 | 2 | 2 | 2 | | 2026/4/1 |
| ❶技術 | ❷製品設計図 | ❸現役製品の設計図 | ❹開発部 | ❺開発部 | ❻●●● | ❼090-XXXX-XXXX | ❽書類 | ❾3 | 3 | 3 | 3 | ❿ | ⓫2026/4/1 |

- 情報資産管理台帳には、情報の媒体・保存先が記載される。
- 情報に対して重要度が決定される。

# STEP４の手順２

**手順2　リスク値の算定**

**優先的・重点的に対策が必要な情報資産を把握する**

手順１で洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定します。リスク値を算定するにはいろいろな方法がありますが、本ガイドラインでは「重要度」と「被害発生可能性」の２つの数値の掛け算で行います。「被害発生可能性」は「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の２つの数値から算出します。これは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。

**リスク値 ＝ 重要度 × 被害発生可能性**

**重要度 ＝ 手順1にて算定**
**被害発生可能性 ＝ 脅威･脆弱性から算定**

**4.「リスク値算定」シートの利用方法**

簡易リスク分析の手順を以下に示します。中小企業の情報セキュリティ対策ガイドラインP.45～47でも説明していますので参照して下さい。
対策の優先度を決めるため、情報資産ごとにリスク値（リスクの大きさ）を算定します。リスク値は「重要度」「脅威」「脆弱性」の数値から算定します。重要度は【手順１】で算定しているので、ここでは脅威と脆弱性を算定します。

- 媒体・保存先に対して、脅威・脆弱性から発生可能性を算定する。

# STEP４の手順２

- 脅威と脆弱性は、情報の媒体・保存先ごとに決定される。

リスク値算定シート

| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 評価値 機密性 | 評価値 完全性 | 評価値 可用性 | 重要度 | 保存期限 | 登録日 | 現状から想定されるリスク 脅威の発生頻度 | 現状から想定されるリスク 脆弱性 | 現状から想定されるリスク 被害発生可能性 | | 現状から想定されるリスク リスク値 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | 書類 | | | | | | | 3: 通常の状況で脅威が発生する（いつ発生し | 3: 対策を実施していない（ほぼ | 3 | 可能性：高 | 0 | リスク小 |
| | | | | | 可搬電子媒体 | | | | | | | 3: 通常の状況で脅威が発生する（いつ発生し | 2: 部分的に対策を実施している | 2 | 可能性：中 | 0 | リスク小 |
| | | | | | 事務所PC | | | | | | | 3: 通常の状況で脅威が発生する（いつ発生し | 1: 必要な対策をすべて実施して | 1 | 可能性：低 | 0 | リスク小 |
| | | | | | モバイル機器 | | | | | | | 2: 特定の状況で脅威が発生する（年に数回程 | 3: 対策を実施していない（ほぼ | 2 | 可能性：中 | 0 | リスク小 |
| | | | | | 社内サーバー | | | | | | | 2: 特定の状況で脅威が発生する（年に数回程 | 2: 部分的に対策を実施している | 1 | 可能性：低 | 0 | リスク小 |
| | | | | | 社外サーバー | | | | | | | 2: 特定の状況で脅威が発生する（年に数回程 | 1: 必要な対策をすべて実施して | 1 | 可能性：低 | 0 | リスク小 |
| | | | | | | | | | | | | 1:通常の状況で脅威が発生することはない | 3: 対策を実施していない（ほぼ | 1 | 可能性：低 | | |
| | | | | | | | | | | | | 1:通常の状況で脅威が発生することはない | 2: 部分的に対策を実施している | 1 | 可能性：低 | | |
| | | | | | | | | | | | | 1:通常の状況で脅威が発生することはない | 1: 必要な対策をすべて実施して | 1 | 可能性：低 | | |

媒体・保存先
プルダウンから選択

脅威の発生頻度
脆弱性
プルダウンから選択

# STEP４の手順２

**(1)「脅威」の識別**

媒体・保存先ごとの脅威が、対策を講じない場合にどのくらいの頻度で発生する可能性があるかを、「脅威の発生頻度」欄のドロップダウンリストから1～3のいずれかを選択します。

| ドロップダウンリスト | 解説 |
|---|---|
| **1:通常の状況で脅威が発生することはない** | 通常業務を行っている状態では発生しない、または発生する可能性が極めて低い場合は「1」を選択します。<br>例）業務でモバイル機器を使っていないので「モバイル機器」に考えられる脅威は「1」である。 |
| **2:特定の状況で脅威が発生する（年に数回程度）** | 頻度は少ないが、たまに必要だったり、通常とは異なる環境で業務を行うことがあり、そのような特定の状況で発生する可能性がある場合は「2」を選択します。<br>例）月末の繁忙時に私有のUSBメモリでデータを持ち帰り、自宅のノートパソコンで業務を行っている人がいるので「可搬電子媒体」「モバイル機器」に考えられる脅威は「2」である。 |
| **3:通常の状況で脅威が発生する（いつ発生してもお** | 日常的に、典型的な脅威が発生しうる業務を行っている、または、これまでに何度か発生したことがある場合は「3」を選択します。<br>例）取引先や顧客との重要情報のやりとりは、全て電子メールにファイルを添付して送受信しているので「事務所PC」「モバイル機器」「社外サーバー（メールサーバー）」の脅威は「3」である。 |

**(2)「脆弱性」の認識**

情報セキュリティ対策の実施状況を、「脆弱性」欄のドロップダウンリストから1～3のいずれかを選択します。

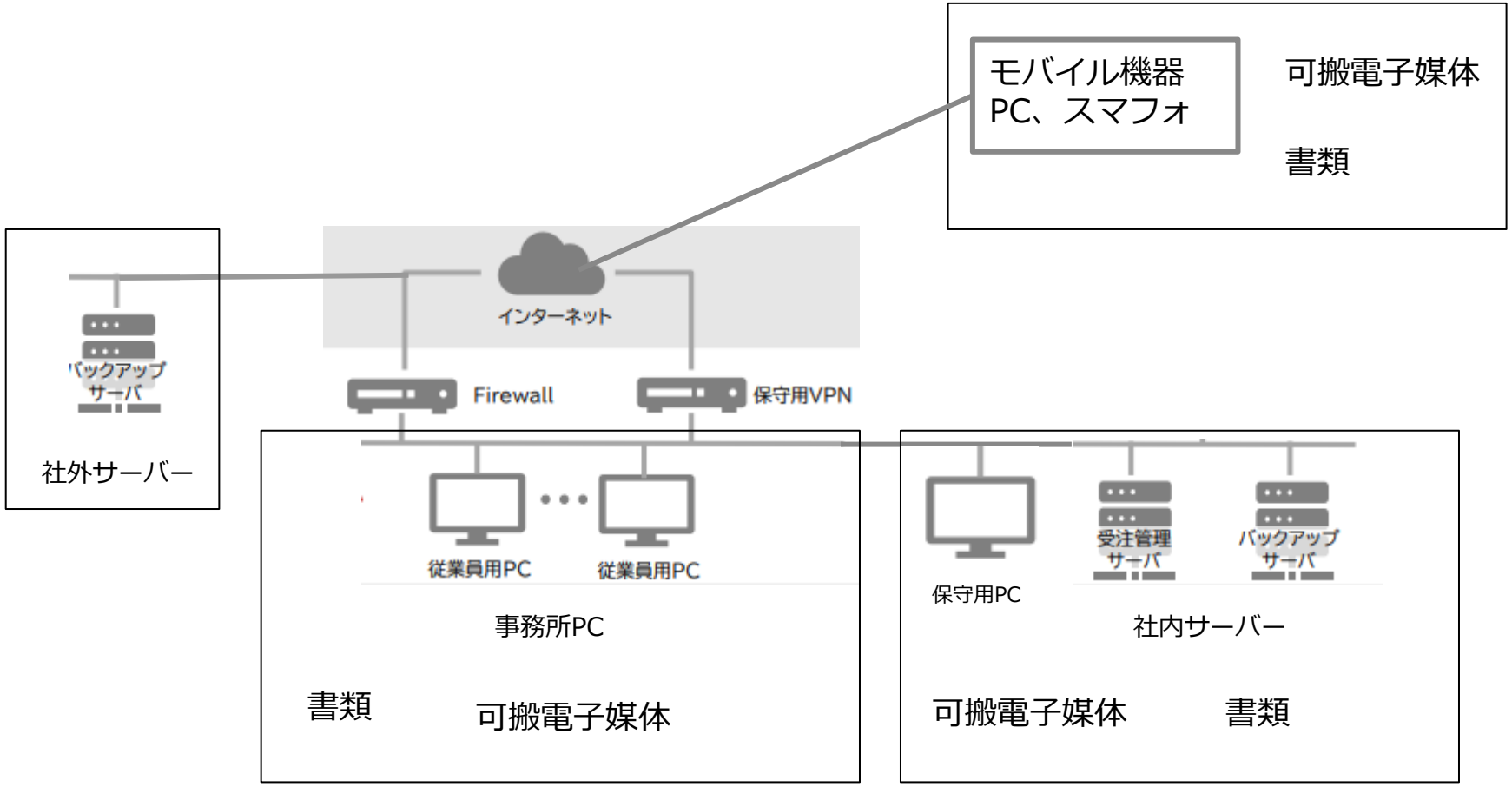
| ドロップダウンリスト | 解説 |
|---|---|
| **1:必要な対策をすべて実施している** | 情報セキュリティ診断項目の通りか、それ以上の対策を実施している場合は「1」を選択します。 |
| **2:部分的に対策を実施している** | 情報セキュリティ診断項目の一部か、実施状況が不十分である場合は「2」を選択します。 |
| **3:対策を実施していない（ほぼ無防備）** | 情報セキュリティ診断項目を全く実施していないか、実施しているかどうかが分からない場合は「3」を選択します。 |

- 媒体・保存先ごとに脅威と脆弱性を１～３で算定する。
- そのためには、脅威を特定し、脅威に対する脆弱性を特定する必要がある。
- この作業についての説明はガイドライン本体ではなく付録に説明がある。

# STEP４の手順２　実際のところは。。。複雑

プルダウン

- 書類
- 可搬電子媒体
- 事務所PC
- モバイル機器
- 社内サーバー
- 社外サーバー

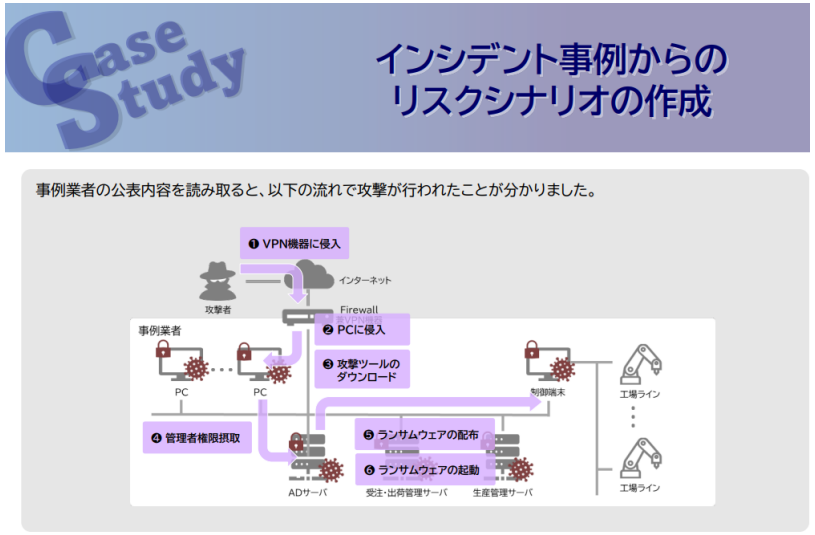


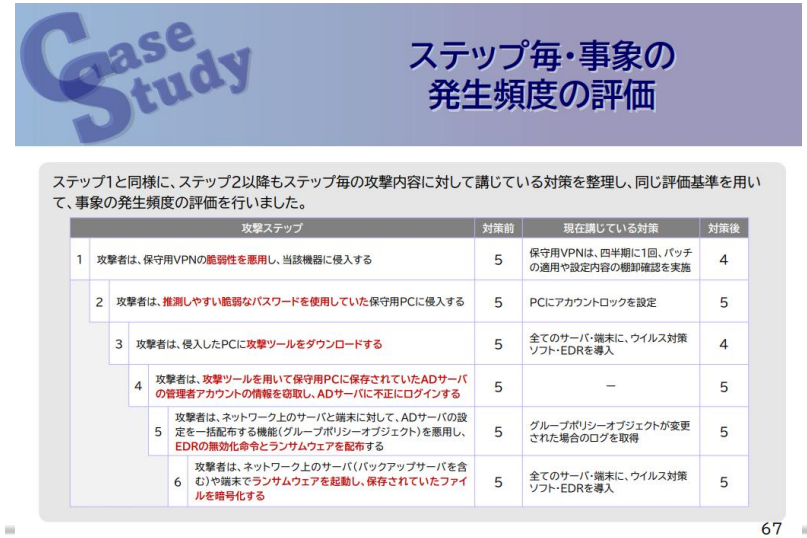
# シナリオベースのアプローチ

NCOの「リスクアセスメント実践ラーニングキット」より

# シナリオベース：具体的な「動」の分析

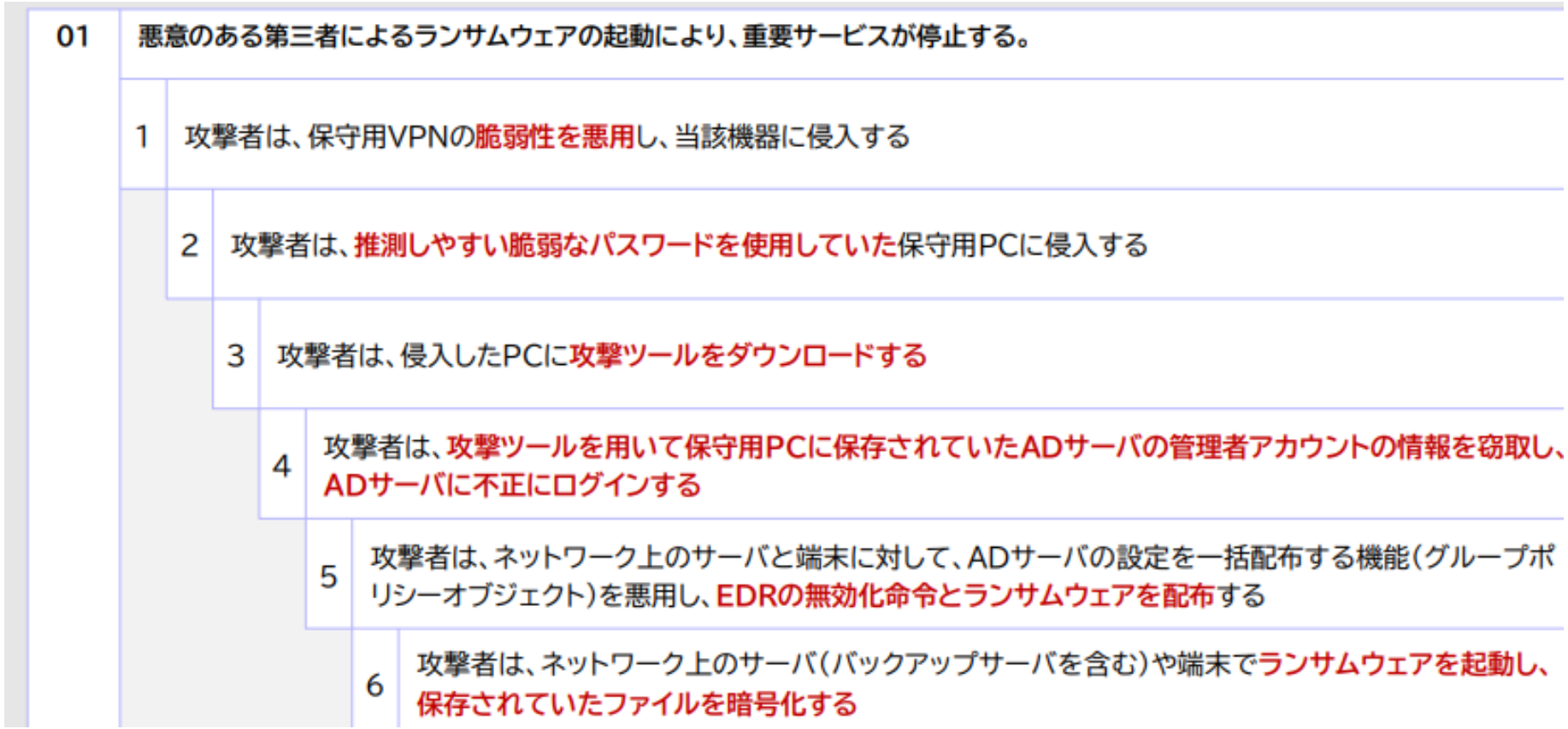
- 考え方: 「何が起きるか？」という物語（シナリオ）を描く
  - 誰が: 悪意のある部外者、ミスをした従業員
  - どこから: フィッシングメール、公開サーバーの弱点
  - どうする: IDを盗み、基幹システムに侵入してデータを破壊
- 特徴: 発生から損害までの「プロセス」を可視化する。
- メリット: 現場の納得感が強い。具体的な対策（防御策）が見えやすい。
- 出典：リスクアセスメント実践ラーニングキット P.41～45



# シナリオベースのアプローチ

- イベントをステップ１～ステップ６のシナリオとしてステップ毎にリスク評価



# 参考情報のリンク

- 中小企業の情報セキュリティ対策ガイドライン 第4.0版
  - https://www.ipa.go.jp/security/guide/sme/about.html
  - 本編
    - https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0.pdf
  - 付録6：資産管理台帳（サンプル）(全9シート)
    - https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_6.xlsx

- リスクアセスメント実践ラーニングキット ～自己学習、研修教材～
  - https://security-portal.cyber.go.jp/guidance/nco_risk.html
  - 自主学習用コンテンツ
    - https://security-portal.cyber.go.jp/assets/images/guidance/risk/risk_asses_learning_kit.pdf
  - 解説・研修展開マニュアル
    - https://security-portal.cyber.go.jp/assets/images/guidance/risk/risk_asses_manual.pdf

# ディスカッション：皆さんの実務で例えば。。。

① ISMSのリスクアセスメントでは、どちらを起点にしていますか？

② 資産ベースで見えない部分を、シナリオベースで補うことは有効ですか？

③ 実務上、シナリオをどこまで作り込むべきでしょうか？