

IT 資格 道 場

CISSP 学習用テキスト

予備知識ゼロから合格ラインへ——読んで理解する1冊目

無料サンプル(第1章まで)

ISC2「CISSP Certification Exam Outline」(2024年4月15日発効・日本語版の試験概要も同日付) 準拠
2026年10月版

ご利用にあたって

- このテキストは「IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルも著作物です。転載・改変しての再配布・二次販売はできません。
- AI モデルの学習データとしてのご利用(学習目的の入力・データセット化を含む)はできません。
- 製品版(学習用テキスト・頻出度別ノート・暗記用ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

目次

試験の骨組みと、このテキストの読み方 [0]

試験の基本情報

8つの分野と重み

読み方

第1章 Security and Risk Management

[1.1/1.2/1.3/1.4/1.5/1.6/1.7/1.8/1.9/1.10/1.11/1.12]

職業倫理の理解、遵守、推進 [1.1]

セキュリティの概念の理解、適用 [1.2]

セキュリティガバナンス原則の評価および適用 [1.3]

法律、規制、コンプライアンス [1.4]

調査の種類の要件の理解（行政、刑事、民事、規制、業界の標準など） [1.5]

セキュリティポリシー、規格、手続き、ガイドラインの開発、文書化、実装 [1.6]

事業継続性（BC）要件の特定、分析し、評価、優先順位付け及び実施 [1.7]

人事セキュリティのポリシーと手続きへの貢献と執行 [1.8]

リスク管理の概念の理解および適用 [1.9]

脅威モデリングの概念と方法論の理解および適用 [1.10]

サプライチェーンリスク管理（SCRM）に関する概念の適用 [1.11]

セキュリティ意識、教育、トレーニングプログラムの確立および維持 [1.12]

サンプルはここまでです

3冊の使い方は、ダウンロード欄の案内を参照してください。

このテキストの骨組みは、ISC2 が公開している **CISSP Certification Exam Outline (2024 年 4 月 15 日発効)** です[^c0-1]。日本語版の範囲も同じ日付の版で、重みも同じです[^c0-2]。以下、試験概要と呼びます。試験概要は、試験の範囲を 8 つの分野と 62 の細目で決めています。章は分野、節は細目の並び順のまま。節見出しの末尾にある [1.1] は細目の番号。

CISSP の問題は、用語を知っているかよりも、場面を読んで「どの管理策を選ぶか」「最初にやることは何か」を決める力を測る。そのため各節は、定義、読み方、隣の仕組みとの違い、間違いやすい点の順に書きました。難しい問が出やすい細目には、場面を読んで判断する段落を置いています。

試験の骨組みと、このテキストの読み方 [0]

試験の基本情報

項目	内容
版	CISSP Certification Exam Outline (2024 年 4 月 15 日発効) [^c0-1]
方式	コンピュータ適応型テスト (CAT) です。英語、ドイツ語、現代スペイン語、日本語、簡体字中国語の試験で使われます[^c0-1]
問題数	100～150 問 です。採点されない事前テストの問題が 25 問含まれ、どれかは見分けられません[^c0-3]
試験時間	最大 3 時間 です[^c0-1]
見直し	できません。答えを確定したら前の問題には戻れません[^c0-3]
合格点	1000 点満点中 700 点 です[^c0-1]
出題形式	選択方式と、高度で革新的な問題です。後者には、チャートや表を使う問題、計算問題、順序回答、ドラッグアンドドロップ、ホットスポット、シナリオ、動画を使う問題が含まれる場合があります[^c0-4]
日本語	日本語で受験できます[^c0-5]
受験料	日本は「Americas and all other regions」の区分で、749 米ドルです[^c0-6]
受験資格	8 分野のうち 2 分野以上で、通算 5 年の実務経験が要ります。学位が承認された資格で 1 年を免除されます。経験が足りない合格者は Associate of ISC2 になれます[^c0-1]

CAT は、答えるたびに受験者の能力を推定し、次の問題を選びます。推定が十分に決まった時点で試験が終わるため、問題数は人によって 100 問から 150 問まで変わります[^c0-3]。このコースの模擬試験は、上限の 150 問・3 時間で作ってあります。本番は 100～150 問のどこかで終わる形式です。時間配分の練習のために、模擬試験は最も長い場合に合わせました。

形式ごとの出題数は、ISC2 が公表していません。模擬試験の形式の内訳は、このコースが決めた推定です。本番の内訳を示すものではありません。

8 つの分野と重み

章	分野	重み	細目
第1章	セキュリティとリスク マネジメント (Security and Risk Management)	16%	12
第2章	資産のセキュリティ (Asset Security)	10%	6
第3章	セキュリティ アーキテ クチャとエンジニアリ ング (Security Architecture and Engineering)	13%	10
第4章	通信とネットワークセ キュリティ (Communication and Network Security)	13%	3
第5章	アイデンティティとア クセスの管理 (IAM)	13%	6

章	分野	重み	細目
第6章	セキュリティの評価とテスト (Security Assessment and Testing)	12%	5
第7章	セキュリティ運用 (Security Operations)	13%	15
第8章	ソフトウェア開発セキュリティ (Software Development Security)	10%	5

重みは、試験概要の CAT の分野別の平均の割合です[^c0-1]。細目の数と重みは比例しません。第4章は細目が3つしかありませんが、重みは第3章と同じ 13% あります。

読み方

- 最初から順に読む必要はありません。重みの大きい分野と、自分の経験が薄い分野から読んでください。
- 計算や手順の問題は、本文の例を自分で手を動かして解き直すと定着する。
- 「最も適切」「最初に」を問う問題では、技術的に正しい答えが複数並ぶ。リスクの管理は経営の責任であり、人命の安全が最優先であり、まず状況を確認してから動く、という筋が判断の軸になる。

第1章 Security and Risk Management

[1.1/1.2/1.3/1.4/1.5/1.6/1.7/1.8/1.9/1.10/1.11/1.12]

職業倫理の理解、遵守、推進 [1.1]

ISC2 職業倫理規定

ISC2 職業倫理規定 (ISC2 Code of Professional Ethics) は、認定を受けた人が守る行動の決まりです。前文は、社会の安全と福祉、共通の善、依頼者への義務、相互の義務が、最高の倫理的な行動の基準を守ingことを求めると述べます。規定の厳守は認定の条件なので、守れなければ認定を失うことがあります。[^c1-1]

本文は 4 つの規範 (canon) で、覚える形は次のとおりです。

規範	内容	一言で
規範 1	社会、共通の善、必要な公共の信頼と信用、インフラを守る	社会
規範 2	名誉ある、誠実な、公正な、責任ある、合法的行動をとる	行動
規範 3	依頼者 (principals) に勤勉で有能なサービスを提供する	依頼者
規範 4	専門職を発展させ、守る	専門職

規範は 1 から 4 の順に優先します。規範どうしが衝突したら、上の規範を取ります。この順位は、規範どうしの衝突は規範の順に解くとした、規定の旧版に添えられた指針から続く考え方だ。依頼者の指示 (規範 3) が社会への害 (規範 1) につながるなら、断ります。雇用主の利益や自分の昇進が、社会の安全より先に来ることはありません。

違反の申し立てにも形があります。申立人は書面で ISC2 の倫理委員会に出し、宣誓供述書の形をとります。委員会は自分では調査せず、自発的に出された書面の証拠だけを見ます。申し立てられる人は規範で決まります。

- 規範 1 と 2: 一般の人なら誰でも
- 規範 3: 依頼者（雇用主や契約の相手）だけ
- 規範 4: 認定か免許を持ち、自分も倫理規定に従う専門家だけ

受験資格の数字も出ます。8 分野のうち 2 分野以上で通算 5 年以上の実務経験が要り、学位か承認された資格があれば 1 年まで免除されます。経験が足りない合格者は Associate of ISC2 になり、6 年以内に 5 年を満たします。[[^]c1-2]

規範の使い方

問は、場面を示して「最初にすべきこと」や「最も適切な行動」を選ばせる形で出ます。判断は規範の順に行います。

1. 人命、社会、公共の信頼に害が及ぶか（規範 1）
2. 自分の行動が誠実で合法か（規範 2）
3. 依頼者への勤勉で有能なサービスか（規範 3）
4. 専門職の評判を守る行動か（規範 4）

場면을 3 つ見ます。1 つ目は、顧客が依頼した診断で、顧客の別の違法行為が見つかった場合です。顧客への守秘（規範 3）より、違法行為による社会への害を止めること（規範 1・2）が先に立ちます。まず依頼者の上位の責任者や法務に知らせ、必要なら当局への通報を検討します（要否は法務が判断）。

2 つ目は、経験のない技術の導入を頼まれた場合です。規範 3 は「有能な」サービスを求めるので、できると言って引き受け、失敗して顧客に損害を与える行動は規範に反します。引き受ける前に限界を伝え、専門家の支援を手配します（規範 3）。3 つ目は、同じ認定を持つ同僚が資格の偽りを行っていたと知った場合です。規範

4 は黙認を認めず、ISC2 への申し立てを支持します。仲間の不正を庇う行動は、専門職を守ることになりません。

組織の規定と ISC2 規定の関係にも注意します。組織の規定が ISC2 規定より緩い場合は、厳しい側の ISC2 規定を守ります。勤務外の行動に規定が及ばないわけではありません。認定は個人に与えられた資格だからです。

組織の倫理規定

組織の倫理規定は、その会社の従業員が守る行動の決まりです。ISC2 の規定は専門家個人に課され、組織の規定は雇用関係で課されます。両方が衝突する時は、規範の優先順位を基準にします(上の規範が先)。

倫理方針は、経営層が承認して全員に周知します。整える物は3つです。

- 違反の報告窓口(内部通報)と、報告した人を不利益から守る仕組み
- 調査と記録の手順
- 職位に関係なく同じ基準で行う処分

基準が人によって変わる運用は、規定そのものへの信頼を損ないます。

申し立てと誤答の型

申し立ての場面で確かめます。顧客 A 社が、請け負ったコンサルタントの成果の水増しに気づきました。依頼者である A 社は、規範 3 の違反として申し立てられます。第三者の一般の人には、規範 3 の申し立ての資格がありません。同じ水増しが社会への害(規範 1)や不誠実(規範 2)にあたるなら、一般の人も申し立てられます。申立人の資格は、どの規範の違反かで決まります。

選択肢の誤答には、決まった型があります。

- 雇用主の利益を最優先にする(規範 1 より下の判断)
- 問題を自分で処理して、誰にも知らせない(組織の報告経路を使わない)

- 外部へ暴露する前に、組織内の手順を試さない
- 規定がないことを理由に、何もしない(規範は法令や社内規則が空白でも働く)

最も適切な答えは、たいてい、社会への害を防ぎ、誠実に、組織の正規の経路で、記録を残して進める行動です。

セキュリティの概念の理解、適用 [1.2]

機密性・完全性・可用性(CIA)

情報セキュリティの 5 つの柱は、機密性、完全性、可用性、真正性、否認防止です。2024 年版の範囲は 5 つ全部を挙げています。[^c1-2]

最初の 3 つを CIA と呼びます。

- **機密性:** 許可されていない者に情報を開示しない性質[^c1-4]
- **完全性:** 情報が不正に変更、破壊されていない性質[^c1-3]
- **可用性:** 許可された者が、必要な時に確実に情報へアクセスし利用できる性質[^c1-3]

どの性質を損なう事象かを見分ける問がよく出ます。

事象	損なわれる性質	主な管理策
顧客名簿の持ち出し、盗聴	機密性 (開示)	暗号化、アクセス制御
帳簿の不正な書き換え、ファイルの破壊	完全性 (変更・破壊)	ハッシュ、署名、変更管理
DDoS、停電、ランサムウェアによる暗号化	可用性 (利用の妨害)	冗長化、バックアップ

ランサムウェアは両方に効きます。データの暗号化は可用性を奪い、窃取してから脅す二重恐喝なら機密性も失われます。「最も直接の影響」を問われたら、攻撃者

が実際に手を付けた側を選びます(暗号化なら可用性)。

柱どうしは緊張関係になることもあります。強い暗号化は機密性を高めますが、鍵を失うと可用性を損ないます。冗長化は可用性を高める一方で、複製が増えるぶん機密性の管理の対象も増えます。どれを優先するかは事業の要求が決めます(救急の医療なら可用性、機密の財務データなら機密性)。

FIPS 199 は、影響度を機密性、完全性、可用性ごとに低、中、高の3段階で決めます。システム全体の影響度の水準は、3つの中で最も高いものを取ります(高水位・high water mark。システム全体を1つの水準にまとめるのはFIPS 200の定めです)。給与システムの機密性が高、完全性が中、可用性が低なら、区分は「高」で、平均を取って「中」にすることはありません。1つの性質の損失でも最大の影響が起こり得るからです。[^c1-3]

真正性と否認防止

真正性(authenticity)は、情報や利用者が、名乗るとおりの本物であることです。完全性は「変わっていない」、真正性は「本物の出どころである」と分けて覚えます。偽の送信者から届いた改ざんのないメールは、完全性は保たれていますが、真正性は保たれません。

否認防止(nonrepudiation)は、行為をした者が後でその行為を否定できないようにする保証です。NIST SP 800-53のAU-10は、作成、送信、受信、承認といった行為について、否定できない証拠を示すよう求めています。実現の手段はデジタル署名で、署名は秘密鍵を持つ本人だけが作れるので、後から「送っていない」とは言えません。[^c1-4][^c1-5]

間違えやすい点があります。共通パスワードや共有アカウントは、誰の行為か特定できないので否認防止を壊します。ハッシュだけでも否認防止にはなりません。ハッシュは誰でも計算できるからです。

見分けの手がかりを表にします。

記述	柱
権限のない者が読めた	機密性
値や記録が書き換えられた	完全性
システムが使えなくなった	可用性
送信者が偽者だった、偽の証明書だった	真正性
実行者が「やっていない」と否認できる状態だった	否認防止

FIPS 199 の定義では、不適切な変更と破壊はどちらも完全性の側で、情報やシステムへのアクセスと利用の妨害が可用性の側です。[^c1-3]

管理策の選び方

要件から管理策を選ぶ問では、柱と手段を組にして考えます。

要件	手段	理由
送信者が後で否認できないようにする	デジタル署名	秘密鍵を持つ本人だけが作れる
通信中の改ざんだけを検知する	ハッシュ、メッセージ認証	変更があれば値が変わる
相手が本物だと確かめる	認証、証明書	名乗りを裏づける
読めなくする	暗号化	鍵を持たない者に開示しない
止まっても動き続ける	冗長化、バックアップ	利用できる状態を保つ

共有鍵を使うメッセージ認証は、完全性と送信元の確認には使えますが、否認防止にはなりません。鍵を持つ双方が同じ値を作れるので、どちらが作ったかを第三者に示せないからです。

場面で確かめます。経理システムのログに、誰かが金額を書き換えた跡が見つかりました。書き換えは完全性の損失です。誰が書き換えたかを示せないなら、否認防止も欠けています。原因がログの共有アカウントなら、対策は、個人ごとのアカウントと、ログ自体の改ざん防止の2つです(片方では足りません)。

影響度の水準

FIPS 199 は、影響度の低、中、高を、組織や個人への悪影響の大きさに定めています。

- 低: 限定的な悪影響 (任務の能力は落ちるが、主要な機能は果たせる。小さな資産の損害、小さな財務の損失)
- 中: 重大な悪影響 (任務の能力が大きく落ちる。大きな資産の損害、大きな財務の損失。ただし、人命や生命に関わる重い傷害は含まない)
- 高: 深刻または壊滅的な悪影響

問では、場面の損害の大きさから水準を選びます。業務は続けられるが効率が下がる程度なら低、主要な機能の有効性が大きく落ちるなら中、機能を果たせなくなるほどなら高です。[^c1-3]

セキュリティガバナンス原則の評価および適用 [1.3]

事業戦略・目標・使命とセキュリティ機能の整合

セキュリティは事業を支える機能です。計画は、事業の戦略、目標、使命 (mission) に合わせて立てるもので、事業から離れて立てることはありません。順序は、事業の目的を先に確かめ、そのための資産とリスクを特定し、管理策を選ぶ形で、管理策を先に決めて事業を合わせる順は逆です。

計画は3つの時間軸に分かれます。

- 戦略計画: 長期 (数年) の方向を決める
- 戦術計画: 戦略を1年ほどの施策に落とす

- 運用計画: 日々の作業の手順にする

経営層が戦略を承認し、セキュリティ部門が戦術と運用へ分解します。方針の流れは上から下で、経営が承認した方針に沿って標準や手順が作られます。この方式をトップダウンと呼びます。現場が先に作って上に認めさせるボトムアップは、経営の支持を得にくく、全社に行き渡りません。セキュリティの責任を IT 部門だけに置くのも誤りで、リスクの受容は事業の判断なので、経営の責任とします。

セキュリティの目標は、事業の目標に合わせて決めます。「売上の 7 割をオンライン販売が占める」なら、可用性と決済情報の保護が最優先です。目標は測定できる形(停止時間の上限、検知までの時間)で置き、経営へ報告します。予算の要求は、事業の損失の大きさに裏づけないと通りません。

事業と衝突する要求が来た場面を見ます。新サービスの公開を急ぐ事業部が、セキュリティの評価を省くよう求めたとします。評価を省く決定は、経営層が残るリスクを承認して初めて許されるもので、担当者の一存では決まりません。セキュリティ担当者が独断で止めることも、黙って通すこともありません。リスクを数字で示し、経営が受容するかを判断する形にします。

組織のプロセス

買収(acquisition)では、相手の管理策、負債(未解決の脆弱性や法令違反)、脅威を引き継ぎます。統合の前に相手のセキュリティを評価し、接続は評価の後にします。評価の前に直接つなぐと、相手の脅威が自社へ入ります(接続は後)。**売却・分離(divestiture)**では、資産、アカウント、データを切り分けます。引き継ぐ先へ渡すものと自社から消去するものを計画し、残ったアクセス権を閉じます。分離する事業部のアカウント、共有ストレージ、証明書、クラウドの契約は、洗い出しの対象です。個人データの移転は、契約と法令が許す範囲に限られます。[^c1-27]

ガバナンス委員会(セキュリティ運営委員会)は、経営層と各部門の責任者で構成します。方針を承認し、優先順位を決め、資源を配分し、リスクの受容を判断します。実務の担当者が決める場ではありません。

組織の役割と責任

役割	責任
上級管理者	最終責任 (説明責任)。方針を承認し、資源を出す
CISO	セキュリティの計画と運営。経営への報告
データ所有者	データの分類と保護の水準を決める
管理者 (カストディアン)	所有者の決定に沿って、日々の保護を実施する
監査人	管理策の有効性を、独立の立場で確かめる

責任と説明責任は別です。実務を部下や外部へ任せても、説明責任は上級管理者に残ります。分類を決めるのはデータ所有者で、バックアップや暗号化を実際に行うのは管理者です。管理者が自分の判断で分類を変えることはできません。データ所有者は通常、事業部の責任者であり、IT 部門の人ではありません。IT 部門は、所有者の決定に従って保護を実施する側です。

監査人は、監査の対象に利害を持たないことが条件です。自分が設計した管理策を自分で監査すると、独立性が崩れます。

場面で確かめます。

- 顧客データを「機密」に分類するかを決める: データ所有者
- 分類に従ってアクセス権を設定する: 管理者
- セキュリティ投資の予算を決める: 上級管理者
- 計画を立てて経営へ報告する: CISO
- 設計どおり動いているかを独立して確かめる: 監査人

ガバナンスとマネジメントの違い

ガバナンスは、組織の方向を決め、成果とリスクを監督する働きで、取締役会や経営層が担います。マネジメントは、決まった方向に沿って計画し、実行し、運用する働きです。

COBIT 2019 は、この 2 つを分けて整理した枠組みです。EDM (評価・指示・監視) がガバナンスで、APO (調整・計画・組織化)、BAI (構築・調達・実装)、DSS (提供・サービス・サポート)、MEA (監視・評価・アセスメント) がマネジメントです。[^c1-9]

セキュリティ管理のフレームワーク

枠組み	種類	覚える数字・中身
ISO/IEC 27001:2022	ISMS の要求事項 (認証の基準)	附属書 A は 93 個、4 テーマ (組織 37・人 8・物理 14・技術 34)
ISO/IEC 27002:2022	管理策の実施の手引き	認証の基準ではない
NIST CSF 2.0 (2024-02)	成果の枠組み	6 機能 (統治・特定・防御・検知・対応・復旧)
NIST SP 800-53 Rev.5	管理策のカタログ	20 ファミリ
COBIT 2019	IT のガバナンスとマネジメント	40 の目標、5 つの領域
SABSA	セキュリティアーキテクチャ	6 層 × 6 つの問いの表
PCI DSS v4.0.1	カード会員データの保護	12 の要件
FedRAMP	米連邦政府のクラウド承認	低・中・高のベースライン (2026 年の新規則では Class A～D の区分)

ISO/IEC 27001 は、組織が ISMS を運用していることを第三者が認証する時の基準です。27002 は附属書 A の各管理策の詳しい手引きで、認証の対象ではありません。

せん。「認証を受ける」なら 27001、「実施の方法を知りたい」なら 27002 と選びます。[^c1-7][^c1-8]

NIST CSF 2.0 の 6 機能は、統治 (Govern)、特定 (Identify)、防御 (Protect)、検知 (Detect)、対応 (Respond)、復旧 (Recover) です。2.0 で統治が加わりました。統治は残り 5 つの中心に置かれ、方針、役割、リスク戦略を扱います。[^c1-6]

SP 800-53 Rev.5 の 20 ファミリは、AC、AT、AU、CA、CM、CP、IA、IR、MA、MP、PE、PL、PM、PS、PT、RA、SA、SC、SI、SR です。Rev.5 でプライバシー (PT) とサプライチェーンのリスク管理 (SR) が加わりました。AC はアクセス制御、IR はインシデント対応、PS は人事セキュリティのように、2 文字から中身が引けるようにします。[^c1-4]

COBIT 2019 は ISACA の枠組みで、40 の目標を持ちます。EDM が「経営が決める側」、残りの 4 領域が「実行側」です。SABSA は事業の要件から順に下ろす設計の枠組みで、文脈、概念、論理、物理、構成要素、運用の 6 層を、何を、なぜ、どう、誰が、どこで、いつの 6 つの問いと組にします。[^c1-9][^c1-10]

PCI DSS は、カード会員データを扱う事業者向けの標準で、現行は v4.0.1 です。v4.0 で新設された要件のうち将来日付とされた分は、2025 年 3 月 31 日から必須になりました。法律ではなく、カードブランドとの契約で強制されます。FedRAMP は、米連邦政府が使うクラウドサービスを承認する制度で、FIPS 199 の影響度 (低・中・高) に応じた SP 800-53 のベースラインで評価してきました。2026 年の統合規則 (CR26) では、影響度の代わりに Class A～D の区分を使います (Class と影響度は 1 対 1 には対応しません)。[^c1-11][^c1-12]

選び方は、場面ごとに次の表のとおりです。

場面	選ぶ枠組み
第三者の認証 (ISMS 認証) を受けたい	ISO/IEC 27001

場面	選ぶ枠組み
経営層と共通の言葉でリスクと対策を整理したい	NIST CSF 2.0
管理策を具体的に選んで文書化したい	NIST SP 800-53 とベースライン
IT のガバナンスを事業の目標へ結びつけたい	COBIT 2019
事業の要件から、アーキテクチャを設計したい	SABSA
カード決済を扱う	PCI DSS
米連邦政府へクラウドサービスを提供する	FedRAMP

SP 800-53 の管理策は、ベースライン (SP 800-53B) の形で選びます。システムの影響度が低、中、高のどれかで、使うベースラインが決まります。そのまま使わず、組織の事情に合わせて調整する作業を**テーラリング**と呼びます。

- 共通管理策の指定
- 適用範囲の考慮 (scoping)
- 補償管理策の選択
- パラメータへの値の割り当て
- 追加の管理策での補強

根拠なく管理策を外すことは許されません。外した理由は、リスクに基づく判断として文書に残します。[^c1-33]

1 つの組織が複数の枠組みを併用するのはよくあります。カード決済のあるクラウド事業者が、ISO/IEC 27001 の認証を持ち、PCI DSS にも適合させ、内部の整理に SP 800-53 を使う形がその例です。重なる要件は、1 つの管理策で複数の枠組みを満たすよう統合します (二重に作らない)。

デューケアとデューディリジェンス

デューケア (due care) は、合理的な人が同じ立場で払う注意を、実際に払うことです。行動の側で、パッチを当てる、方針を作る、教育を行うといった実行が当たります。

デューディリジェンス (due diligence) は、その注意が足りているかを調べ、確かめ続けることです。調査と維持の側で、委託先を契約の前に評価する、脆弱性診断を定期的に行うといった確認が当たります。[^c1-4]

見分け方は1つで、「やった」ならデューケア、「調べた・確かめた」ならデューディリジェンスです。デューケアを欠くと、注意義務違反(過失)を問われます。委託先の評価を契約の前に行うのは、デューディリジェンスです。評価に沿った管理策を自社が実施するのは、デューケアです(実行の側)。

説明責任が残る場面

クラウド事業者にデータを預けた企業が、事業者の設定ミスで顧客データを漏えいさせた場面を考えます。実務は事業者が行っていても、顧客に対する説明責任は、データを預けた企業(データ所有者)に残ります。委託できるのは実施であり、責任そのものではありません。企業は、委託の前に事業者を評価し(デューディリジェンス)、契約で要件と監査の権利を定めます。委託の後も、確かめ続けなければなりません。

セキュリティ責任者を新しく任命された場面では、最初の仕事が問われます。最初は技術の導入ではありません。事業の目標、既存の方針、法令の要件、現在のリスクを把握し、そのうえで経営と合意した優先順位に従って計画を作ります。経営の支持と事業の理解が先で、管理策の購入は後になります(購入が先ではありません)。

文書と責任の連鎖もそろえて覚えます。

1. 経営層が、事業の使命と目標に沿った戦略とポリシーを承認する

- 2. セキュリティ部門が、標準、ベースライン、手順へ落とす
- 3. データ所有者が分類を決め、管理者が実施する
- 4. 監査人が、実施の有効性を独立して確かめる
- 5. 結果を経営へ報告し、方針と戦略へ戻す

どの段も、経営の承認と支持が土台です。

CSF 2.0 の使い方と ISMS の文書

NIST CSF 2.0 は、成果を示す枠組みで、達成の方法までは定めません。組織は、プロファイルを作って、現在の状態 (Current) と目標の状態 (Target) を、CSF の成果で記述します。ティア (Tiers) は、リスクの統治と管理の厳格さを段階で示します。現在と目標の差が、改善の計画の元になります。[^c1-6]

ISO/IEC 27001 の認証を目指す組織は、リスクアセスメントを行い、リスク対応計画を作り、適用宣言書 (SoA) に、附属書 A の管理策のうち何を採用し何を除外するかと、その理由を記録します。附属書 A の 93 個を全部実施する義務はなく、リスクの評価に基づいて選びます。[^c1-7]

法律、規制、コンプライアンス [1.4]

サイバー犯罪とデータ侵害

サイバー犯罪は、不正アクセス、データの窃取、詐欺などの法令違反として扱われ、国ごとに法が違います。組織は、拠点のある国と顧客のいる国の両方の法に従います (片方だけでは足りません)。侵害が起きた時の通知は、誰へ、いつまでにと
いう期限が法令で決まっており、実務の問になります。

法令	通知の相手	期限
GDPR 33 条	監督機関	知った時から 72 時間以内 (遅れたら理由を添える)

法令	通知の相手	期限
GDPR 34 条	本人	本人の権利と自由に高いリスクがあれば、遅滞なく
日本の個人情報保護法	個人情報保護委員会	速報は知った時から概ね 3～5 日以内、確報は 30 日以内（不正の目的のおそれは 60 日以内）
HIPAA 侵害通知規則	本人	不当な遅れなく、発見から遅くとも 60 日以内

GDPR の 72 時間は、「侵害に気づいた時」から数えます。10 月 2 日（金）9 時に気づいたなら、期限は 10 月 5 日（月）9 時で、土日は数えから外れません。侵害がリスクを生みそうにない時は、監督機関への通知は要りません。本人への通知は、高いリスクがある時だけ必要です。リスクがあれば監督機関へ、高いリスクなら本人へも、と 2 段で覚えます。[^c1-13]

日本では、個人情報保護委員会への報告が、速報と確報の 2 回あります。確報の期限は、知った日を 1 日目として数えます。10 月 2 日（金）に知ったなら、速報は 10 月 7 日ごろまでです。確報は 30 日目の 10 月 31 日ですが、土曜日なので翌開庁日の 11 月 2 日（月）までになります（期限の日が土日・祝日・年末年始なら翌開庁日）。不正の目的で行われたおそれがある漏えい等は、確報が 60 日以内で、60 日目の 11 月 30 日（月）までです。本人への通知も要ります。[^c1-15]

HIPAA は、本人への通知を、不当な遅れなく、発見から遅くとも 60 日以内に求めます。同じ州の住民が 500 人を超える場合は、報道機関にも知らせます。500 人以上の侵害は、本人への通知と同時に保健福祉省（HHS）へ知らせます。500 人未満なら記録を残し、その年の終わってから 60 日以内にまとめて報告します。[^c1-16]

ライセンスと知的財産

権利	守るもの	期間(米国／日本)
著作権	表現(コード、文章、図)。創作と同時に生じる	著作者の死後 70 年。職務著作は公表から 95 年か創作から 120 年の短い方(米)
特許	発明(新規性、進歩性)	出願から 20 年(実用特許)
商標	名前、ロゴ。出所を示す	米国は使用を続ける限り更新、日本は登録から 10 年で更新できる
営業秘密	秘密として管理する情報	期間の定めなし。秘密である限り守られる

営業秘密になる条件は 3 つで、秘密として管理していること、事業に有用であること、公然と知られていないことです。特許は出願で内容が公開されるので、秘密にしたい技術は営業秘密で守ります。管理が崩れて公になれば、保護は消えます。秘密保持契約(NDA)とアクセス制限が、管理していた証拠になります。[^c1-17]

守る手段の選び方です。独自の製法で、他社が簡単に再現できないなら、営業秘密が向きます。他社が独自に発明したり、製品を分解して再現したりする可能性が高いなら、特許が向きます。営業秘密は、他社が独自に同じものを開発する行為を止められません。

著作権は、ソースコードや文書を創作と同時に保護します。登録は要りません。守られるのは表現だけで、アイデアは含まれません。商標は、商品やサービスの出所を示す名前やロゴを守り、更新して使い続けます。従業員が職務で書いたコードの著作権は、職務著作として会社に帰属するのが通常です(個別の契約がなければ)。

ソフトウェアのライセンスの主な形態は、次のとおりです。

- 商用の許諾

- オープンソース(利用と改変を認める条件つき)
- フリーウェア(無償だが著作権は残る)
- シェアウェア(試用後に支払う)
- EULA(利用許諾契約)

ライセンスの条件を超えた複製は、著作権の侵害です。

輸出入の管理

暗号の技術は軍事にも使えるので、輸出が管理されます。

ワッセナー・アレンジメントは、通常兵器と汎用品・技術(暗号を含む)の輸出管理を定めた国際的な取り決めで、参加は 42 か国です。法的な拘束力はありません。各国が国内法で実施します。米国の管理は 2 本立てで、汎用品と暗号は商務省産業安全保障局(BIS)の EAR、防衛品目は国務省の ITAR の担当です。[^c1-18][^c1-31]

出題は「暗号を使ったソフトを海外の拠点へ送る時、何を確かめるか」の形になります。答えは、輸出元の国の管理規則と、送り先の国の輸入規則の両方を確かめることです。

国境を越えたデータの流れ

GDPR は、EU の個人データを EU の外へ移す手段を、条文で 4 つ決めています。

1. 十分性認定(45 条): 欧州委員会が移転先の国の保護水準を十分と認めた場合は、追加の手続きなしで移せる
2. 適切な保護措置(46 条): 標準契約条項(SCC)などを契約に組み込む(認定を受けた行動規範や認証に、拘束力のある約束を添える形も含む。認定のない自主規約は当たらない)
3. 拘束的企業準則(BCR・47 条): 多国籍企業のグループ内で守る規則を、監督機関が承認する

4. 特定の場合の例外 (49 条): 本人の明示の同意など、限られた場合

日本は、欧州委員会の十分性認定の対象に入っています。EU から日本への移転は、追加の手続きなしで行えます。[^c1-34]

場面で確かめます。EU の顧客の個人データを、十分性認定のない国のデータセンターへ移したい場合です。取引相手との個別の契約には、SCC を組み込めば足りません (承認は不要)。グループ内の多数の移転には、監督機関の承認を受けた BCR を整えます。BCR は承認に時間がかかりますが、承認後はグループ内の移転に広く使えます。本人の同意 (49 条) は例外なので、日常の大量の移転の根拠にはなりません。[^c1-13]

プライバシーの法令

GDPR は、EU 域内の人の個人データを扱う組織に、その所在地を問わず及びます (EU 域外の組織には、EU 域内の人へ商品やサービスを提供する場合と、その人の行動を監視する場合に及ぶ。3 条 2 項)。役割は 3 つです。

- 管理者 (controller): 処理の目的と手段を決める者
- 処理者 (processor): 管理者に代わって処理する者
- データ主体: 識別される自然人

25 条は、データ保護をバイ・デザイン (設計の段階から) とバイ・デフォルト (初期設定で最小限) で組み込むよう求めます。

5 条は、処理の原則を 7 つ挙げます。適法・公正・透明、目的の限定、データの最小化、正確性、保存の制限、完全性と機密性、そして遵守を示せる責任 (accountability) です。データ主体には、アクセス、訂正、削除 (17 条)、処理の制限、持ち運び、異議の権利があります。

高いリスクのある処理の前には、データ保護影響評価 (DPIA) を行います (35 条)。公的機関や、大規模な監視などの中核業務を持つ組織は、データ保護責任者 (DPO) を指名します (37 条)。

管理者と処理者の関係は契約で結びます。処理者が侵害を知ったら、管理者へ遅滞なく知らせます。72 時間の時計は管理者が気づいた時から動きます。EDPB の指針は、処理者から知らされた時に管理者が気づいたとみなすのを原則とする。クラウド事業者 (処理者) からの通知が遅れると、顧客企業 (管理者) の調査と判断がそのぶん遅れるので、契約には、通知の期限を短く決めておきます。[^c1-13]

制裁金は 2 段です。83 条 5 項の重い側 (基本原則、本人の権利、越境移転の違反) は、2,000 万ユーロか、前年の全世界の売上の 4% の、どちらか高い方です。売上 6 億ユーロの会社は 4% が 2,400 万ユーロなので上限は 2,400 万ユーロ、売上 3 億ユーロの会社は 4% が 1,200 万ユーロなので 2,000 万ユーロが上限です。軽い側 (83 条 4 項) は 1,000 万ユーロか売上の 2% の高い方です。[^c1-13]

法令	地域	覚える特徴
GDPR	EU	72 時間通知、制裁金は最大 2,000 万ユーロか売上 4%
CCPA (CPRA で改正)	カリフォルニア州	知る・削除・訂正・販売や共有のオプトアウト・機微な情報の利用の制限・差別されない
PIPL	中国	個人情報の保護法。国外への提供に条件がある
POPIA	南アフリカ	個人情報の保護法
個人情報保護法	日本	個人情報保護委員会へ速報と確報

CCPA の 6 つの権利は、知る権利、削除する権利、訂正する権利、販売や共有をオプトアウトする権利、機微な個人情報の利用を制限する権利、差別されない権利です。訂正と機微な情報の制限は CPRA が加えました。[^c1-14]

契約・法令・業界標準・規制の要件

SOX 法 (2002 年) は、米国の上場企業の財務報告の正確さと内部統制を求めます。404 条が、経営者による内部統制の評価と監査人の意見を要求します。IT の統制 (アクセス管理、変更管理) は財務報告に影響するので、IT 部門も対象に入ります。[^c1-19]

GLBA は、米国の金融機関に、顧客情報の保護 (Safeguards Rule) とプライバシー通知を求めます。HIPAA は、医療情報 (PHI) を扱う組織に、安全管理と侵害通知を課します。[^c1-20]

法令は法律で強制され、違反は罰則です。業界標準 (PCI DSS など) は契約で強制され、違反は取引の停止や制裁金です。「法令ではないから従わなくてよい」とは限りません。契約の条件になっていれば、守る義務があります。

法令の種類にも違いがあります。

- 刑事法: 国家が犯罪を罰する
- 民事法: 当事者の間の損害を扱い、賠償が主な救済
- 行政法: 規制当局の権限に基づき、制裁金や是正命令を使う

1 つの侵害で、これらが同時に動くことがあります。

多国籍の SaaS 事業者が、EU、米国、日本の顧客のデータを含む侵害を受けた場面です。各国の期限は同時に動き、GDPR は 72 時間、日本は速報が 3~5 日、HIPAA は 60 日です。実務では、最も短い期限に合わせた手順を用意します (通知の要否は法務が判断)。複数の法令が衝突したら、最も厳しい要件を満たす形に揃えます (法務が判断)。

通知の免除と侵害の定義

GDPR の個人データの侵害 (personal data breach) は、偶発的か違法かを問わず、個人データの破壊、紛失、改変、許可されない開示やアクセスにつながる、セキ

セキュリティの違反です。紛失や改変も含むので、盗まれた場合に限りません。

本人への通知(34条)には、免除があります。侵害を受けたデータが、暗号化などで権限のない者に解読できない状態だった場合は、本人への通知は要りません。侵害の後に講じた措置で、高いリスクがもう生じそうにない状態にした場合なども同じです。ただし、監督機関への通知(33条)は、別の判断になります。リスクの有無を評価して決めます。暗号化が、通知の義務を軽くする代表的な管理策です。[^{c1-13}]

HIPAAにも同じ考え方があります。通知の対象は、保護されていない(unsecured)保護対象保健情報の侵害です。暗号化などで保護された情報は、通知の対象から外れます。[^{c1-16}]

場面です。従業員のPCが盗まれ、中に顧客の個人データがありました。ディスク全体が暗号化されていて、鍵はPCに保管されていませんでした。解読できない状態なので、本人への通知は免除される可能性が高くなります。暗号化がなければ、期限内に監督機関へ、高いリスクなら本人にも通知します。最初の対応は、何が入っていたかを確定し、法務と共に適用される法令を特定することです。

法令の問に答える順序

法令の問は、技術の詳細より、手順を問います。

1. どの国、どの州の法令が適用されるかを特定する(拠点、顧客の所在、データの所在)
2. 通知や報告の義務の有無と期限を確かめる
3. 証拠を保全し、事実を確定する
4. 経営と法務の判断で、通知と対外対応を行う

どの法令を適用するかを決める前に、規制当局や顧客へ連絡してはいけません。事実が定まらないまま通知すると、誤った内容を訂正する負担が生じます。ただし、期限は事実の確定を待たずに動き始めるので、並行して進めます。

処理の適法性と同意

GDPR の 6 条は、個人データの処理が適法になる根拠を、次の 6 つに限っています。

- 本人の同意
- 契約の履行 (または契約前の手続き) に必要な処理
- 法的義務の遵守に必要な処理
- 本人や他の人の生命に関わる利益の保護
- 公共の利益や公的権限の行使
- 正当な利益 (本人の権利が優先する場合を除く)

同意を根拠にする場合、同意は特定の目的ごとに、明確な肯定の行動で示され、撤回もできる必要があります。契約の履行に必要な処理 (注文の発送に住所を使う) は、同意がなくても適法です。根拠を決めずにデータを集めるのが、最も典型的な違反の入口です。[^c1-13]

調査の種類と要件の理解 (行政、刑事、民事、規制、業界の標準など) [1.5]

調査の種類と立証の基準

調査は、誰が、何の違反を、どの基準で調べるかで 5 つに分かれます。立証の基準が厳しいほど、証拠の扱いも厳しくなる関係にあります。

種類	調べる対象	立証の基準	主導する者
刑事	法律違反 (犯罪)	合理的な疑いを超える (最も厳しい)	法執行機関
民事	当事者間の争い (契約、損害)	証拠の優越 (どちらがもっともらしいか)	当事者
行政 (管理)	組織内の方針違反、運用の問題	組織が決める (最も緩い)	組織

種類	調べる対象	立証の基準	主導する者
規制	規制当局の定める規則への違反	規制による	規制当局
業界標準	PCI DSS など業界の基準への適合	契約による	契約の相手（審査機関など）

刑事が「合理的な疑いを超える」、民事が「証拠の優越」です（行政は組織が基準を決めます）。

社員が就業規則に違反してデータを持ち出した場面で考えます。

- 社内の処分を決める調査: 行政
- 持ち出されたデータで顧客に損害が出て、訴えられた場合: 民事
- 不正アクセス禁止法の違反として、警察が動いた場合: 刑事

1つの事件が、同時に複数の種類の調査になることもあります。行政の調査で得た証拠だけでは、刑事の立証に足りません。基準が最も緩い調査の結論を、最も厳しい場へそのまま持ち込めないからです。

業界標準の調査は、法の強制ではなく契約に基づきます。カード情報の侵害が起きますと、カードブランドや決済代行が指定した審査機関が調べます。法律で調べられるのではなく、契約の義務として受け入れる調査です。[^c1-11]

調査の開始の判断

法執行機関や規制当局へ連絡するかどうかは、慎重に決めます。連絡すると、調査の主導権が組織の手を離れます。証拠として押収され、業務が止まり、事実が公開されることもあります。連絡は経営の判断で、法務と一緒に決めます。現場の担当者が単独で連絡することはありません。

ただし、法令が通報を義務づける場合（個人データの侵害、重大インシデントなど）は、判断の余地がありません。通報の期限を守る方を優先します。通報の要否

が不明な時は、まず法務へ相談します。証拠の保全は、連絡の判断を待たずに始めます。後で刑事の事件に発展しても使えるよう、扱いの記録(保管の連鎖)を残します(誰が、いつ、何を受け取ったか)。

調査を始める時は、法務の関与を先に確保します。法務が判断するのは、証拠の収集の範囲、従業員のプライバシー、通報の義務です。従業員の通信を調べるには、ポリシーで監視の同意を得ていることが前提になります。同意がなければ、得た証拠が使えなくなるだけでなく、会社が責任を問われます。調査の存在は、対象者や関係のない従業員へ漏らしません。

場面での判断

内部不正の疑いが見つかった場面を順に見ます。

1. 法務と人事に報告し、調査の権限を確保する
2. 疑いの対象者に知らせず、アカウントのログとデータを保全する
3. 調査の種類を決める(社内処分だけか、刑事告訴や民事訴訟を見込むか)
4. 外部に連絡する要否を経営と法務が判断する
5. 結果を記録し、必要な処分と再発防止につなげる

刑事や民事を見込む場合は、証拠の扱いを最初から厳格にします。調査の途中で証拠に手を加えると、後で証拠として使えなくなります。調査担当者は、対象者から独立した立場の人にします(対象者の上司が調べると、利害が衝突します)。

セキュリティポリシー、規格、手続き、ガイドラインの開発、文書化、実装

[1.6]

文書の階層

文書	性質	内容
ポリシー	強制	経営の意思。何をなぜ守るかを書く。技術の細部は書かない
標準	強制	ポリシーを満たす必須の技術や製品の決まり
ベースライン	強制	システムごとの最低限の設定水準
手順	強制	作業の具体的な順序
ガイドライン	推奨(任意)	標準が無い場面での進め方の助言

上から下へ具体になります。ポリシーが「個人情報情報は暗号化して保存する」と書くと、標準が「AES-256 を使う」と決めます。ベースラインは「このサーバーでは暗号化を有効にした状態を最低とする」と置き、手順が「設定画面を開き、次の順に操作する」と書きます。ガイドラインだけが任意で、従わなくても違反にはなりません。

[^c1-4]

見分け方は次のとおりです。

- 経営が出し、変わりにくい: ポリシー
- 必ず守る技術や製品の決まり: 標準
- 必ずこの順で行う: 手順
- できればこの方法で: ガイドライン

場面で確かめます。

- 全社の方針として「重要情報は暗号化する」と決める: ポリシー
- 暗号方式として「AES-256 を使う」と決める: 標準
- ノート PC の設定水準として「ディスクの暗号化を有効にする」と置く: ベースライン
- 設定画面での操作の順序: 手順
- 「迷ったら TLS 1.3 を選ぶとよい」という助言: ガイドライン

新しい OS を導入する時に直す文書は、使う OS の設定水準（ベースライン）と作業の手順で、経営の意思を示すポリシーは変えなくて済みます。ポリシーに製品名を書いておくと、製品を替えるたびに経営の承認が要ります。この理由で、ポリシーは技術の細部を含みません。

ポリシーの策定・承認・周知・見直し

ポリシーは、策定、承認、周知、実施、見直しの順で回ります。

1. 目的と範囲を決め、関係部門の意見を集めて案を作る
2. 上級管理者が承認する（承認がなければ強制力がない）
3. 全員へ周知し、同意や確認の記録を残す
4. 実施し、違反の扱いも明示する
5. 定期的に見直す

見直しは、年に 1 回程度の定期と、事業、法令、技術が大きく変わった時に行います。SP 800-53 は、各ファミリの先頭の管理策 (-1) で、方針と手順を定義した頻度で見直すよう求めます。見直した結果は、経営が再び承認します。周知されていないポリシーは、従業員が知らなかったと主張でき、処分の根拠として弱くなります。
[^c1-4]

例外は、承認の手続きを置いて扱います。例外を申請した部署が、リスクと代替の管理策を示し、責任者が期限つきで承認します。例外が際限なく許されると、ポリ

シーが形骸化します。例外の一覧を定期的に確かめ、期限の切れた例外は閉じます(違反の場合の措置も、ポリシーに明記)。

見直しの順序

新しい法令が施行され、個人情報の保存の期間に新しい要件が加わった場面です。最初に直すのはポリシー(経営の意思)で、保存の期間に関する方針を承認し直します。次に標準(保存の期間の具体的な値)、手順(削除の作業)の順で改訂します。技術の細部は標準以下で変わるので、ポリシーが変わるのは、経営の意思が変わる時だけです。改訂のたびに、周知と同意の記録を更新します(古い版の記録は残す)。

事業継続性(BC)要件の特定、分析し、評価、優先順位付け及び実施 [1.7]

事業影響度分析(BIA)とMTD・RTO・RPO・WRT

BIA は、業務が止まった時の影響を分析し、復旧の優先度を決める作業で、SP 800-34 は 3 段で進めます。

- 1. 業務の過程と、復旧の優先度(重要度)を決める
- 2. 資源の要件を特定する
- 3. システムの資源の復旧の優先度を決める

BIA で決める時間と量の指標は 4 つです。[^c1-21]

指標	意味	何を決めるか
MTD(最大許容停止時間)	業務が止まっても許される最長の時間	復旧の方式の選択
RTO(目標復旧時間)	システムを戻すまでに許される時間	復旧技術の選択。MTD より短い
RPO(目標復旧時点)	失ってよいデータの量を時間で表したもの	バックアップの間隔

指標	意味	何を決めるか
WRT (作業復旧時間)	システムを戻した後、データの確認と業務の再開に要する時間	RTO と合わせて MTD に収める

SP 800-34 は、RTO が MTD を超えてはならないと述べます。データの再処理など、システムが戻った後に要する時間があるなら、その時間を RTO に足して MTD の内側に収めます。この考え方から、RTO に WRT を足した時間が MTD 以下になる関係が使われます。足した時間が MTD と等しい場合も、以下なので収まります (MTD 8 時間・WRT 2 時間なら、RTO 6 時間で $6+2=8$ 時間となり、収まります)。RPO は MTD の一部ではありません。別の軸で、「どれだけのデータ損失に耐えられるか」で決まります。

計算で確かめます。MTD が 8 時間、RTO が 5 時間、WRT が 2 時間なら、 $5+2=7$ 時間で MTD に収まります。RTO が 7 時間なら $7+2=9$ 時間で 8 時間を超えるので、RTO を縮める復旧方式へ替えます。RPO が 4 時間なのに、バックアップが 6 時間ごとなら、最悪 6 時間分のデータを失い、RPO を満たしません。バックアップを 4 時間以内の間隔にするか、レプリケーションに替えます。

復旧方式の選択は、RTO で決まります。RTO が短いほど費用が上がります。

- ホットサイト: 直ちに切り替えられる
- ウォームサイト: 準備に時間がかかる
- コールドサイト: 機材の手配から始まる

RTO が数時間ならホットかウォームを検討します。RPO が 24 時間なら夜間の日次バックアップで足り、数分なら同期のレプリケーションが要ります。RTO が数分で RPO がほぼゼロなら、ホットサイトと同期の複製が必要で、費用は最も高くなります。

BIA は、事業部門の責任者から聞き取りを行って進めます。IT 部門だけで決めるはいけません。業務が止まった時の影響（収益の損失、顧客の離反、法令の違反、評判）を、時間とともに増える形で見ます。影響が許容できない水準に達する時点が MTD です。システムの資源と、システム間の依存も特定します（人、設備、データ、外部のサービス）。

優先順位の計算で確かめます。システム A（MTD 4 時間）、B（MTD 24 時間）、C（MTD 72 時間）があり、B は A のデータに依存するとします。復旧は A、B、C の順で、MTD の順と依存の順が一致します。仮に B の MTD が A より短くても、A が戻らなければ B は動けないので、依存先の A が先です。優先順位は業務の影響が大きい順に決まります（システム部門の都合や台数の多さは関係ありません）。

BC 計画の範囲と体制

BC 計画は、上級管理者の承認と資源（予算と人員）の配分が先に要ります。経営の支持がなければ、計画は作っても実行されません。SP 800-34 は、計画の作成と保守を 7 段の過程で示します。[^c1-21]

1. 方針の策定
2. BIA の実施
3. 予防の管理策の特定
4. 復旧の戦略の作成
5. 計画の作成
6. 計画の試験、訓練、演習
7. 計画の保守

BIA は 2 番目で、方針の次です。方針で範囲と責任を決めてから分析に入ります。計画は作って終わりではなく、試験と訓練で確かめ、結果を改訂へ戻し、その後も変化に合わせて保守します。事業継続マネジメントシステム（BCMS）の要求事項は、ISO 22301 が定めています。[^c1-32]

事業継続計画（BCP）は、重要な業務を災害の最中でも続ける、組織全体の計画です。災害復旧計画（DRP）は、IT のシステムとデータを復旧する、BCP の一部です。BCP は人の安全の確保、代替の拠点、顧客への連絡を含み、DRP は復元や代替サイトへの切り替えの手順を扱います。DRP だけでは、事業は続きません。

計画の範囲は、BIA で特定した重要な業務に絞ります。すべてを守ろうとすると、資源が足りず、肝心の業務に届きません。計画は承認した責任者の名で出し、定期的な訓練で実効性を確かめ、結果を改訂へ戻します。

外部への依存関係

自社の業務は、取引先、クラウド、通信、電力に依存します。外部の依存が止まれば、自社の MTD を超える停止になり得ます。BIA で外部の依存関係を洗い出し、委託先の RTO が自社の MTD に合うかを確認めます。

- 契約に復旧時間（SLA）を入れる
- 委託先の BC 計画の提出や共同の訓練を求める
- 1 社だけに依存せず、代替の調達先を持つ

1 社だけに依存する構成は単一障害点になります。

復旧方式を選ぶ計算

選択の場面を数字で確かめます。ある業務の MTD は 8 時間、WRT は 3 時間です。復旧方式の候補は 3 つあります。

方式	RTO	年間費用
ホットサイト	1 時間	3,000 万円
ウォームサイト	12 時間	800 万円
コールドサイト	72 時間	200 万円

ウォームは RTO が 12 時間で、MTD の 8 時間を超えるので使えません。コールドは当然使えません。ホットの RTO 1 時間に WRT 3 時間を足すと 4 時間で、MTD に収まります。MTD を満たす案はホットだけなので、費用が高くても選びます。MTD を満たすことが先で、満たす案の中から費用の低い案を選びます。費用の安い案を先に選ぶ順序は誤りです。

MTD が 24 時間まで緩められるなら、ウォームの $12 + 3 = 15$ 時間で収まります（その場合の話）。費用は年 2,200 万円下がります（3,000 - 800）。MTD は事業部門が決める値なので、IT 部門が RTO の都合で勝手に緩めてはいけません。事業部門の責任者が、停止の影響を承知したうえで決めます。

計画を試験した結果、RTO を超えたことが分かった場面では、計画と復旧の手段を改善します。MTD を超える結果が出たなら、MTD を緩める前に、手順の見直しや方式の変更を検討します（直した後に再び試験します）。

外部の依存と MTD の差

自社の注文システムの MTD は 3 時間です。クラウド事業者の契約上の復旧時間（RTO）は 4 時間でした。このままでは、事業者の障害の場面で MTD を 1 時間超えます。対応の選択肢は 3 つあります。

- 事業者と、復旧時間を 3 時間未満に縮める契約を結び直す
- 代替の事業者や、別の領域（リージョン）への切り替えを用意する
- 超過を経営が承認し、受容する（MTD の見直しは事業部門が決める）

最初にすることは、差を事業部門の責任者に伝えて、どの選択肢を取るか判断してもらうことです。IT 部門が黙って MTD を延ばしたり、契約を無視したりしてはいけません。

人事セキュリティのポリシーと手続きへの貢献と執行 [1.8]

候補者の選考と採用

採用の前に、職務の重さに応じて、身元、経歴、資格、信用を確かめます (SP 800-53 の PS-3・人の審査)。管理者権限や機密情報を扱う職務ほど、確認を厚くします。本人の同意を得て、法令の範囲で行います。経歴の照会は、採用した後ではなく採用の前です。確認の厚さは職務で決め、全員に最大の調査をかけることはありません。[^c1-4]

雇用契約とポリシーに基づく要件

入社時に、秘密保持契約 (NDA)、利用規定 (AUP)、利益相反の申告を結びます (PS-6 アクセスの合意)。署名した記録は、後で違反を処分する時の根拠になります。契約には、退職後も秘密を守る義務が続くことを明記します。

入社・異動・退職の手続き

場面	すること
入社	役割に必要な最小限の権限を与える。教育を受けさせる
異動	新しい職務に要らない権限を外す (権限の蓄積を防ぐ・PS-5)
退職	アクセスを止め、資産と認証情報を回収し、秘密保持の義務を再確認する (PS-4)

退職の手順には順序があります。

1. 解雇の通告と同時に、その直前にアクセスを停止する
2. 資産 (PC、鍵、バッジ) と認証情報を回収する
3. 退職面接で、秘密保持の義務を再確認する

システム管理者が懲戒解雇される場面で考えます。人事が本人へ通告する時刻に合わせて、アカウントの停止を実行します。通告の前に本人が気づくと、データの削除や持ち出しの機会が生まれます。通告の後に停止しても、その間に操作できてしまいます。正しい順序は、通告と同時か直前の停止です（共有アカウントのパスワードの変更も忘れません）。

異動の場面では、経理から営業へ移った社員に経理の権限が残ると、権限の蓄積が起きます。1人が購買の起票と承認の両方の権限を持つと、職務分掌が崩れます。異動の手続きには、旧職務の権限の棚卸しと削除を組み込みます（PS-5）。
[^c1-4]

人事の管理策として、次の3つが使われます。どれも、1人に権限が集中する状態を避けるための手段です。

- 職務分掌: 重要な作業を1人に任せず、複数人で分ける
- ジョブローテーション: 担当を入れ替えて、不正を見つけやすくする
- 強制休暇: 休暇中に別の人が見て、不正を表に出す

ベンダー・コンサルタント・請負業者との契約と管理

外部の人員にも、従業員と同じ要件を契約で課します（PS-7）。契約に入れる物は5つです。

- NDA
- アクセスの範囲
- 監査の権利
- 事故の報告の義務
- 契約終了時のデータの返却と消去

外部の人員には必要な範囲だけの権限を与え、活動を監視します。契約を結んだだけでは足りません。履行を継続して確かめます。

手続きの順序の判断

新しい請負業者の技術者に、本番環境のアクセスを与える場面です。順序は次のとおりです。

1. 契約を結び、NDA と利用規定に署名してもらう
2. 必要な身元の確認を行う
3. 教育を受けてもらう
4. 職務に必要な最小限の権限だけを与える
5. 契約期間に合わせて、アクセスの期限を設定する

NDA の署名より前に、機密に触れさせてはいけません。急ぎを理由に、署名やアクセス権の承認を後回しにしても、リスクは消えません。契約が終わったら、アクセスを止め、返却と消去を確かめます。

リスク管理の概念の理解および適用 [1.9]

脅威と脆弱性の識別

資産、脅威、脆弱性、リスクは、次の関係にあります。

- 脅威 (threat): 損害を起こし得る原因 (攻撃者、災害)
- 脆弱性 (vulnerability): 脅威に突かれる弱点
- リスク: 脅威が脆弱性を突いて資産に影響を与える可能性と、影響の大きさ

脅威か脆弱性のどちらかが無ければ、リスクは低くなります。[^c1-23]

具体例です。脅威は「攻撃者による SQL インジェクション」、脆弱性は「入力の検証がない」、資産は「顧客データベース」です。入力を検証する管理策で脆弱性を減らせば、リスクは下がります。台風 (脅威) は止められません。対応は、脆弱性 (建物の耐水性) と影響 (バックアップの有無) を下げる形になります。

管理策を入れる前のリスクを固有リスク (inherent risk)、入れた後に残るリスクを残存リスク (residual risk) と呼びます。

- リスク選好 (risk appetite): 組織が目標のために進んで引き受けるリスクの大きさ
- リスク許容度 (tolerance): 許容できる逸脱の幅

対応の決定は、組織のリスク許容度に沿って経営が行います。リスクの情報は、リスク登録簿 (register) に、内容、可能性、影響、対応、責任者、期限として残します。
[^c1-23]

定量的リスク分析

用語	式	意味
AV (資産価値)	与えられる	資産の金額
EF (暴露係数)	与えられる	1 回の事象で資産が失われる割合
SLE (単一損失予想額)	$AV \times EF$	1 回の損失額
ARO (年間発生率)	与えられる	1 年に起きる回数
ALE (年間損失予想額)	$SLE \times ARO$	1 年あたりの損失額

資産価値 5,000 万円、EF 40%、ARO 0.25 (4 年に 1 回) なら、SLE は $5,000 \text{ 万円} \times 0.4 = 2,000 \text{ 万円}$ 、ALE は $2,000 \text{ 万円} \times 0.25 = 500 \text{ 万円}$ です。[^c1-23]

管理策の価値は、(導入前の ALE - 導入後の ALE) - 管理策の年間費用で測ります。正なら導入の価値があります。

計算例を 3 つ見ます。

- 年間 180 万円の管理策で ARO が 0.25 から 0.05 に下がる場合: 導入後の ALE は $2,000 \text{ 万円} \times 0.05 = 100 \text{ 万円}$ 、価値は $(500 - 100) - 180 = 220 \text{ 万}$

円で正

- 管理策の費用が年 450 万円の場合: $(500 - 100) - 450 = -50$ 万円で、導入すれば損
- EF だけを 10% に下げる管理策 (年 180 万円) の場合: ALE は $5,000 \text{ 万円} \times 0.1 \times 0.25 = 125 \text{ 万円}$ 、価値は $(500 - 125) - 180 = 195 \text{ 万円}$

もう 1 つの資産で確かめます。資産価値 8,000 万円の顧客システムで、EF 25%、ARO 0.5 (2 年に 1 回) なら、SLE は 2,000 万円、ALE は 1,000 万円です。年 400 万円のバックアップ強化で EF を 5% に下げると、SLE は 400 万円、ALE は 200 万円です。価値は $(1,000 - 200) - 400 = 400 \text{ 万円}$ です (導入に価値あり)。

2 つの管理策を比べる時は、費用を引いた後の純価値が大きい方を選びます。管理策 X の価値が 400 万円、Y が 250 万円なら X を選びます。費用が安い方を選ぶのでも、ALE の減る額が大きい方を選ぶのでもありません。

間違えやすい点があります。

- ARO は「1 年あたりの回数」で、10 年で 3 回なら 0.3、5 年に 1 回なら 0.2、年に 2 回なら 2
- 「資産価値」と「SLE」を取り違えると、桁が外れる
- 管理策の費用は、導入した年の費用ではなく、年あたりの費用で ALE と比べる
- 複数の資産を持つ時は、資産ごとに計算して合計する

定性的リスク分析とリスク評価の範囲

定性的分析は、数字の代わりに、高、中、低や 1～5 の段階で、可能性と影響を評価します。可能性 × 影響の表 (リスクマトリクス) で優先順位を決め、可能性 4、影響 4 の 16 を、可能性 3、影響 5 の 15 より先に扱います。金額が決まらない場合や、速さを優先する場合に向きます。

専門家の判断に頼るので、評価者の主観が入る点は避けられません。定量的分析は金額で比べられますが、データが要ります。実務では組み合わせ、定性で絞り込んで、重要なリスクだけを定量で分析します。数字で経営に説明したいなら定量、データが乏しく早く順位を付けたいなら定性です。

評価の範囲 (scope) は、最初に決めます。どの資産、どの脅威、どの事業を対象にするかを決め、経営の承認を得ます (承認が先)。範囲を決めずに始めると、分析が終わらないか、重要な資産が抜けます (範囲の承認が先)。

SP 800-30 は、リスクマネジメントを 4 つの要素 (フレーム、評価、対応、監視) で捉えます。評価は 4 段で進みます。

- 1. 準備
- 2. 実施
- 3. 結果の伝達
- 4. 維持

[^c1-23]

リスク対応

対応	中身	例
低減 (軽減)	管理策で、発生の可能性が影響を下げる	パッチ、暗号化
移転 (共有)	損失を他者に負わせる	保険、外部委託の契約
回避	リスクのある活動をやめる	サービスの廃止
受容	経営が承認して、そのまま引き受ける	費用が見合わない小さなリスク

SP 800-37 と SP 800-30 は、対応を、受容、回避、低減、共有、移転と呼びます。試験では、低減、移転、回避、受容の 4 つで覚えれば足ります。受容は、経営が承認し

て文書に残すことが条件です。リスクを無視するのは対応ではありません。保険に入ってもリスクは消えず、損失が他者へ移るだけで、評判への影響などは残ります。残存リスクは、経営が受容できる水準以下まで下げます。[^c1-22]

選択の場面です。ALE が 500 万円で、管理策が年 180 万円、導入後の ALE が 100 万円なら、低減を選びます。ALE が 30 万円で管理策が年 100 万円なら、受容を選びます（経営が承認して文書に残す）。ALE が 500 万円で、保険料が年 60 万円、免責が 200 万円なら、移転を検討します。ただし保険会社は、管理策の水準を条件にすることが多く、条件を満たさなければ支払いが減ります。毎年大きな赤字を生む訴訟の元になる事業は、やめる回避が選択肢です。

サイバー保険は移転の手段で、管理策の代わりにはなりません。

管理策の種類

機能による分類は、次のとおりです。[^c1-4]

種類	機能	例
予防	事象が起きないようにする	ファイアウォール、アクセス制御、職務分掌
発見（検知）	起きたことに気づく	IDS、ログの監視、監視カメラ
是正	起きた事象の影響を直す	パッチ、ウイルスの駆除、インシデント対応
抑止	実行を思いとどまらせる	警告の掲示、監視カメラの存在の告知
回復	通常の状態に戻す	バックアップからの復元、DR サイト
補償	他の管理策の不足を補う	承認者が不在の時の代替の確認
指示	望ましい行動を指示する	方針、手順書

実装による分類は 3 つです。

- 管理的: 方針、手順、教育
- 技術的 (論理): 暗号、ファイアウォール
- 物理的: 錠、柵、警備員

1 つの管理策に、機能と実装の 2 つの分類が付きます。監視カメラは、物理的な発見の管理策で、存在を知らせれば抑止にもなります。ファイアウォールは技術的な予防、職務分掌は管理的な予防です。

見分け方は、事象との前後です。

- 事象の前: 予防か抑止
- 最中や直後に気づく: 発見
- その後に直す: 是正
- 元に戻す: 回復
- 本来の管理策ができない時の代わり: 補償

管理策の評価・継続的な監視と測定・報告

管理策は、導入した後に、有効かを評価します。セキュリティ管理策とプライバシー管理策の両方が対象です。評価は、面談 (interview)、文書や設定の確認 (examine)、試験 (test) の 3 つの方法を組み合わせます。面談だけでは、実際の動作を確かめたことになりません。結果は、承認の判断と残存リスクの見直しに使います。

RMF の承認は、権限のある責任者 (承認者) が、リスクを受け入れて運用を許可する段階です。システム管理者や、評価を行った人が承認するわけではありません。承認は期限つきで、継続的監視の結果で見直されます。

継続的監視 (SP 800-137・ISCM) は、組織のリスクの判断を支えるために、管理策と脅威を継続して監視する仕組みです。年に 1 回の評価では、間にある変化を捉

えられません。脆弱性の情報、構成の変更、ログ、脅威の情報を集め、変化がリスクに与える影響を見ます。測定の指標(メトリクス)を決め、定期的に集めます。[^c1-24]

報告は、内部(経営層、委員会)と外部(規制当局、顧客、監査人)に分かれ、受け手に合わせます。取締役会には、事業へ及ぶリスクと必要な決定を、事業の言葉で簡潔に伝えます。規制当局には、法令が求める形式で報告します。技術の詳細を並べても、意思決定には使えません。

継続的な改善

リスク成熟度モデルは、組織のリスク管理の成熟度を段階で示し、上の段階へ高める指針になります。段階の低い組織や部門から順に引き上げるのが、指針の使い方です。場当たりの初期の段階から、定義され、管理され、最適化される段階へ進むのが典型です(旧 CMM の並び。CMMI では「管理」の段が「定義」の段より前に来ます)。測定した結果を次の計画へ戻し、改善を繰り返します。

リスクフレームワーク

NIST RMF (SP 800-37 Rev.2) は、7 段です。[^c1-22]

1. 準備 (Prepare)
2. 分類 (Categorize)
3. 選択 (Select)
4. 実装 (Implement)
5. 評価 (Assess)
6. 承認 (Authorize)
7. 監視 (Monitor)

分類は、FIPS 199 の影響度(低・中・高)でシステムを区分する段です。選択は、SP 800-53 のベースラインから管理策を選び、必要に応じて調整する段になります。

承認するのは技術担当ではなく、組織の責任者です。分類の前に選択はできず、評価の前に実装が要ります(順序の確認が出ます)。

ISO 31000:2018 は、リスクマネジメントの指針で、過程を次の順に示します。

- 1. 伝達と協議
- 2. 範囲・状況・基準の設定
- 3. リスクアセスメント(特定、分析、評価)
- 4. リスク対応
- 5. 監視とレビュー
- 6. 記録と報告

ISO/IEC 27005 は、情報セキュリティのリスク管理の手引きで、27001 が求めるリスクアセスメントを支えます。[^c1-32]

複数の資産の優先順位

資産が複数ある場面です。

資産	資産価値	EF	ARO	SLE	ALE
顧客データベース	5,000 万円	40%	0.25	2,000 万円	500 万円
公開 Web サイト	2,000 万円	100%	1	2,000 万円	2,000 万円
社内メール	500 万円	20%	2	100 万円	200 万円

資産価値が最も大きいのは顧客データベースですが、ALE が最も大きいのは公開 Web サイトです。年あたりの損失の見込みが最大の資産に、優先して管理策を入れます(資産価値の大きさだけで順位を付けてはいけません)。発生の頻度(ARO)が高いと、1 回の損失が同じでも年の損失が大きくなります。

リスク対応の手順

リスク評価の結果が、経営のリスク許容度を超えた場面では、次の手順で進めます。

1. 対応の選択肢(低減、移転、回避、受容)を挙げる
2. 各案の費用と、下がるリスクの大きさを比べる
3. 経営が対応を選び、承認する
4. 実施し、残存リスクを測る
5. 残存リスクを経営が受容するか確かめ、文書に残す
6. 継続的監視で、前提の変化を追う

担当者が自分の判断でリスクを受容してはいけません。受容できる権限を持つのは、そのリスクの結果を負う事業の責任者や上級管理者です。残存リスクがなお許容度を超えるなら、追加の対応を検討します(受容は最後の手段)。

RMF の順序の判断

RMF の各段の作業は、順序で問われます。

- 分類: システムの影響度を FIPS 199 で決める(ここが基礎)
- 選択: 分類の結果(低、中、高)に合うベースラインから管理策を選ぶ
- 評価: 実装した後に行う
- 承認: 評価の結果を受けて、承認者が運用を許可するか決める
- 監視: 運用開始後に変化を追い、重大な変化があれば前の段へ戻る

承認は、評価の前にも、実装の前にもできません。準備の段は、組織とシステムの両方のレベルで行います。リスクの許容度や優先順位を組織が決めておくと、個別のシステムで決める作業が軽くなります。

脅威の発生源

脅威を洗い出す時は、発生源の型で漏れを防ぎます。SP 800-30 は、脅威の発生源を次の型で整理しています。[^c1-23]

- 敵対的な攻撃 (サイバーや物理の攻撃)
- 人の過失 (操作の誤りや、やるべきことの抜け)
- 組織が管理する資源の構造的な故障 (ハードウェア、ソフトウェア、環境の制御)
- 環境の影響 (自然災害や、人為の災害)

敵対的な脅威は、攻撃者の意図と能力から可能性を見積もります。それ以外の脅威は、過去の発生の記録から見積もります。過失や故障は、攻撃者がいなくても起きます。脅威の一覧には必ず入れます (入れ忘れが多い)。

脅威モデリングの概念と方法論の理解および適用 [1.10]

脅威モデリングの手法

脅威モデリングは、システムの設計の段階で、起こり得る攻撃を洗い出し、対策を決める作業です。完成してから見つけるより、設計の段階で直す方が安く済みます。主な手法は、次の表の 5 つです (名前と中身の対応が問われます)。

手法	中身
STRIDE	脅威を 6 種類に分類する (Microsoft)
PASTA	攻撃のシミュレーションとリスクの分析を、7 段で進める
VAST	アジャイルの開発と大きな組織に合わせた、自動化しやすい手法
DREAD	脅威を 5 つの観点で点数づけする

手法	中身
攻撃ツリー	攻撃者の目標を根に置き、達成の手段を枝に分けた図

STRIDE は次の 6 つの頭文字で、損なわれる性質に対応させて覚えます。[^c1-25]

- なりすまし (Spoofing)
- 改ざん (Tampering)
- 否認 (Repudiation)
- 情報漏えい (Information disclosure)
- サービス拒否 (Denial of service)
- 権限昇格 (Elevation of privilege)

STRIDE	損なわれる性質	対策
なりすまし	真正性	認証
改ざん	完全性	ハッシュ、署名、アクセス制御
否認	否認防止	ログ、デジタル署名
情報漏えい	機密性	暗号化、アクセス制御
サービス拒否	可用性	冗長化、レート制限
権限昇格	認可	最小権限、入力の検証

PASTA は、攻撃者の視点 (Attack Simulation) で、事業への影響まで届くのが特徴です。7 段を順に進めます。

1. 目標の定義
2. 技術の範囲の定義
3. アプリケーションの分解

4. 脅威の分析
5. 脆弱性の分析
6. 攻撃のモデル化
7. リスクと影響の分析

DREAD は、5 つの観点を点数にして、平均で優先順位を決めます。

- 損害 (Damage)
- 再現性 (Reproducibility)
- 悪用のしやすさ (Exploitability)
- 影響を受ける利用者 (Affected users)
- 発見のしやすさ (Discoverability)

5 つの点が 8、6、7、9、4 なら、平均は 6.8 です。点のつけ方が評価者の主観に左右されるのが弱点で、OWASP の解説は、数字の順位づけの主観を避けるため、高・中・低の評価を勧めています。[^c1-26]

攻撃ツリーは、頂点に攻撃者の目標 (例: 顧客データを盗む) を置き、達成の手段 (SQL インジェクション、内部者の持ち出し) へ枝分かれさせます。経路ごとに、成功の難しさや費用を付けると、最も安く攻略できる経路が分かります。「口座の残高を書き換える」を根にして、必要な前提 (認証の突破、API の脆弱性) を枝に広げ、最も弱い経路に対策を置く使い方が典型です。

手法の選び方

場面で選びます。

- 設計の段階で、脅威を網羅的に洗い出したい: STRIDE (データフロー図の各要素に 6 種類を当てはめるので、漏れが出にくい)
- 事業への影響まで含め、攻撃者の視点で段階を踏んで評価したい: PASTA
- 多数のチームが速いサイクルで評価する、アジャイルの開発: VAST

- 洗い出した脅威に優先順位を付けたい: DREAD、または可能性 × 影響
- 攻撃者の最終目標から、経路を逆にたどりたい: 攻撃ツリー

手法は競合しません。STRIDE で洗い出し、DREAD で順位を付け、攻撃ツリーで経路を掘り下げる併用もあります。

脅威モデリングの進め方

進め方は、OWASP の解説では 4 つの高い段で示されます。[^c1-26]

1. 作業の範囲を決める: 対象を分解し、データフロー図で、資産、入口、信頼の境界を描く
2. 脅威を特定する: STRIDE などで分類し、リスクの大きさで順位を付ける
3. 対策と緩和策を決める
4. 作業を評価する: 洗い出しと対策に漏れがないかを確認する

場面で確かめます。オンライン注文の仕組みで、利用者のブラウザと注文サーバーの間に信頼の境界があります。この境界を越えるデータのやり取りで、次の脅威が洗い出されます。

- なりすまし: なりすました注文
- 改ざん: 途中の金額の書き換え
- 情報漏えい: 通信の盗聴

対策は、認証、署名か TLS、サーバー側での金額の再計算です。分解で境界を見つけ損ねると、その境界の脅威が丸ごと抜けます。

「何を作っているか」「何が悪くなり得るか」「それに何をするか」「うまくできたか」の 4 つの問いで考える進め方もあり、分解に当たる問いが最初に来ます。

脅威モデリングは、1 度で終わりません。設計が変わったら更新し、リリースの後に出了脆弱性や新しい攻撃手法もモデルへ戻します。対策は、設計の段階で入れる

方が、リリース後に直すより費用が小さくなります。

分類の問い方

STRIDE の問は、場面から種類を選ばせる形が多くなります。

- 偽の送信元で管理者になります: なりますし
- 通信の途中で金額を書き換える: 改ざん
- 操作ログが無く、本人が「やっていない」と主張できる: 否認
- 暗号化されていない通信を盗聴される: 情報漏えい
- 大量のリクエストでサービスを止める: サービス拒否
- 一般利用者が管理者の機能を使えるようになる: 権限昇格

否認は、実行者を特定できる記録が無いことで成立します。権限昇格は、認証を破る話ではなく、認証された後に権限が広がる話です。

サプライチェーンリスク管理 (SCRM) に関する概念の適用 [1.11]

製品・サービスの取得に伴うリスク

サプライチェーンのリスク管理 (C-SCRM) は、製品やサービスの調達から廃棄までの、供給網の脅威を扱います。NIST SP 800-161 Rev.1 が手引きです。[^c1-27]

取得に伴う脅威は、3つの型で出ます。

- 改ざん (tampering): 流通の途中で、部品や製品に細工される
- 偽造品 (counterfeit): 本物を装った模倣品が混じる
- インプラント (implant): 不正な機能 (バックドア) が埋め込まれる

供給元の信頼が崩れると、自社で正しく設定しても防げません。

リスク軽減策

取得の前に、供給者を評価します。第三者の評価（監査報告、認証）を求め、契約に最低限のセキュリティ要件とサービスレベル要件（SLA）を入れます。取得した後も、継続して監視します（評価は契約の前だけでは終わりません）。SP 800-53 の SR ファミリが、この管理策を定めています。[^c1-4]

供給者を 1 社に絞らず、複数から調達すれば、1 社の侵害や停止の影響を減らせます。受け取りの際に、封印や出荷の記録を確かめ、公式の経路の外で入手した機器は使いません。

海外の部品メーカーから、ネットワーク機器を調達する場面です。取引の前に、メーカーの第三者評価を確かめます。契約には、最低限のセキュリティ要件（脆弱性の通知、パッチの提供、部品の出所の説明）と、修理や交換の期限（SLA）を入れます。公式の販売経路の外にある中古品や並行輸入品は避けます（偽造や改ざんの危険が高いため）。

シリコンの信頼の基点・PUF・SBOM

ハードウェアの信頼の基点（Root of Trust・RoT）は、常に信頼される前提の部品で、ファームウェアの保護、検知、回復の起点になります。SP 800-193 は、更新、検知、回復の 3 つの信頼の基点を定めています。シリコン（チップ）の中に信頼の基点を置くと、その上の起動の連鎖（chain of trust）を、順に検証できます（検証の連鎖）。

機器の起動時にファームウェアの改ざんを確かめたい場面では、チップ内蔵の RoT が最初の段階で署名を検証し、その検証を次の段階へ連鎖させる形が使われます（起動の最初が信頼の起点）。[^c1-28]

PUF（Physically Unclonable Function・物理的に複製不可能な機能）は、製造のばらつきから、機器ごとに固有の値を生む回路です。同じ設計でも、同じ値は得られません。鍵を保存せずに機器を識別できるので、偽造品の対策になります。

SBOM (Software Bill of Materials) は、ソフトウェアを構成する部品の一覧です。CISA は、入れ子になった「材料のリスト」だと説明しています (ソフトウェアの部品の一覧)。形式には SPDX や CycloneDX があります。新しい脆弱性 (例: ある部品の欠陥) が公表された時、SBOM があれば、自社の製品がその部品を含むかをすぐ調べられます。SBOM は脆弱性を直す物ではなく、影響の範囲を知る物です (供給者から取得し、受け入れの条件にします)。^[^c1-29]

場面での判断

調達したソフトウェアの部品に重大な脆弱性が公表された場面では、手順は次の順です。

1. SBOM で、自社のどの製品が、どの版の部品を使うかを特定する
2. リスク (外部から到達できるか、悪用されているか) を評価して、優先順位を付ける
3. 供給者の修正版を適用する (なければ、設定による緩和や部品の置き換えを検討する)

供給者の通知の速さは、契約の評価基準になります。

信頼の基点の場面では、ハードウェアのセキュリティを、ソフトウェアで後から付け足すことはできないと考えます。最初に信頼できる土台がなければ、その上で検証した結果も信頼できません。

取得の判断の順序

製品を取得する時の判断は、リスクの大きさに厳しさを変えます。重要なシステムに使う部品は、供給者の評価を厚くし、監査の権利を契約に入れます。重要度の低い消耗品は、簡素な確認で足ります。評価の結果、要件を満たさない供給者には、改善を求めるか、別の供給者を探します。契約を結んでから評価する順序は逆です (評価が先)。

セキュリティ意識、教育、トレーニングプログラムの確立および維持 [1.12]

意識向上・訓練・教育の違いと方法

区分	目的	対象
意識向上 (awareness)	注意を向けさせる	全員
訓練 (training)	職務の技能を身につけさせる	役割別
教育 (education)	理解を深め、判断できるようにする	専門職

この 3 区分は、SP 800-50 の旧版の考え方です。2024 年の Rev.1 は、3 つを別の区分とせず、サイバーセキュリティとプライバシーの学習プログラム (CPLP) として一体で扱います。段階は、計画と戦略、分析と設計、開発と実施、評価と改善の 4 つです。3 区分の違いを問う問にも、一体の学習プログラムとして問う問にも備えて、両方を知っておきます。[^c1-30]

方法は、対象に合わせて選びます。全員向けには、ポスター、メール、短い動画の意識向上を使います。経理や開発などの役割別には、職務に合った訓練を行います。セキュリティ担当者が、攻撃の分析の技能を身につける専門の学びは、教育にあたります。

- フィッシング演習: 模擬のメールを送り、開封、クリック、報告の行動を測る
- セキュリティチャンピオン: 各部署 (開発チームなど) に置く推進役で、現場の相談窓口になる
- ゲーミフィケーション: 得点や順位を使い、参加の意欲を高める

新入社員には入社時に基本の研修、管理者権限を持つ人には追加の訓練、経営層には事業と責任の観点の短い話が向きます。役員を狙った詐欺が増えているなら、役員向けの内容を足します。

新しい技術と動向を取り込む内容の定期見直し

内容は定期的に見直します。暗号資産の詐欺、AI を使った偽の音声や文面、ブロックチェーンに関わるリスク、新しいフィッシングの手口を、教材に加えます。1 度作った教材を使い続けても、現在の脅威には合いません。

プログラムの有効性評価

有効性は、受講率だけでは測れません。受講したことと、行動が変わったことは別です。SP 800-50 Rev.1 は、受講の完了率に加え、フィッシング演習のクリックと報告の測定を挙げます。クリック率が下がり、報告率が上がるなら、行動が変わっています。[^c1-30]

場面で確かめます。研修の受講率が 100% でも、フィッシング演習のクリック率が下がらないなら、研修は有効ではありません。クリック率の推移、報告率、インシデントの件数、問い合わせの内容の変化を、継続して測り、結果を教材の改善へ戻します。クリックした人を罰するより、報告した人を認める方が、報告が増えます。

計画を立てる順序

教育プログラムを新しく作る場面では、順序が問われます。

1. 教育の需要を把握する（誰が、どの職務で、どのリスクにさらされているか）
2. 目標と測定の指標を決める
3. 内容と方法を選ぶ
4. 実施する
5. 測定して改善する

教材を先に作ってから需要を探すと、的を外します。経営の支持を得て、予算と時間を確保することも、最初の段階です。

サンプルはここまでです

続き(第2章～巻末)は、CISSP 問題集のご購入で、頻出度別ノート・暗記用ノートと合わせて3点すべてダウンロードできます。

SAMPLE

CISSP 学習用テキスト(無料サンプル)

版

2026年10月版(ISC2「CISSP Certification Exam Outline」(2024年4月15日発効・日本語版の試験概要も同日付) 準拠)

発行

IT資格道場(<https://www.shikaku-doujou.com>)

お問い合わせ

info@shikaku-doujou.com

「CISSP」はISC2(International Information System Security Certification Consortium, Inc.)の登録商標です。記載されているその他の会社名・製品名・サービス名は、各社の商標または登録商標です。

本教材はISC2 公式の試験範囲(CISSP Certification Exam Outline・2024年4月15日発効)と公開されている規格・文書を基に作成したもので、ISC2 との提携・承認関係はありません。

本文・図表・設問はすべてオリジナルの著作物です。無断での転載・複製・再配布・二次販売はできません。お気づきの点はinfo@shikaku-doujou.com までご連絡ください。