IT資格道場

CISM 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)

CISM 試験範囲(ISACA 公式 CISM Exam Content Outline・2026年11月発効)準拠
2026年11月版

SAMPLE

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。

SAMPLE

目次

第1章 Information Security Governance [1.1.1/1.1.2/1.1.3/1.2.1/1.2.2/1.2.3/1.2.4]

- 事業体のガバナンスの基本と文化 [1.1.1]
- 法律、規制、契約上の要件 [1.1.2]
- 組織の構造、役割、責任 [1.1.3]
- 情報セキュリティ戦略の策定 [1.2.1]
- エンタープライズアーキテクチャ [1.2.2]
- 情報ガバナンスのフレームワークと標準 [1.2.3]
- 戦略計画（予算、リソース、ビジネス・ケース）[1.2.4]

サンプルはここまでです

SAMPLE

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、ISACA 公開の **CISM Exam Content Outline（2026 年 11 月 3 日発効）** です[1]。日本語版の受験者ガイドは、同じ範囲を「CISM試験内容の概要」と訳しています[2]。以下、ECO と呼びます。ECO は試験の範囲を、4 つの分野と 8 つの小区分、37 の細目で決めています。章と節の並びは ECO のままです。節見出しの末尾の `[1.1.1]` は細目の番号。公式の番号「1A1」の A を 1、B を 2 に置き換えた形です。

ECO には細目とは別に、分野に紐づかない補助タスクが 42 項目あります[1]。補助タスクとは、情報セキュリティマネージャーが仕事で行うことの一覧です。各節では、その節で扱う補助タスクを本文に織り込みました。

試験の基本は次のとおりです[2]。問題は 150 問で、試験時間は 240 分です。どの問題にも問題文と 4 つの選択肢があり、最も適切なものを 1 つ選びます。採点はスケールスコアの 200 から 800 点で、450 点以上が合格です。分野の比率は、1 情報セキュリティガバナンスが 18%、2 情報セキュリティリスク管理が 20%、3 情報セキュリティプログラムが 33%、4 インシデント管理が 29% です。日本語で受験できる[3]。

CISM の問題の中心は、用語の暗記ではありません。管理職の立場で「最初に何をするか」「最も適切なのはどれか」を選ぶ形です。そのため各章は、定義、判断の根拠になる順序や基準、間違えやすい点、場面の例の順に並べた。

SAMPLE

第1章 Information Security Governance [1.1.1/1.1.2/1.1.3/1.2.1/1.2.2/1.2.3/1.2.4]

分野 1 は、CISM の配点の 18% を占めます。1A の事業体のガバナンスと、1B の情報セキュリティ戦略に分かれます。問われるのは、組織の目的から戦略と投資を組み立て、経営層に判断を戻す力です。設定値や製品名はほとんど出ません。選択肢が割れたら、事業の目的に近いものと、責任を持つ人に判断を戻すものを選びます。

事業体のガバナンスの基本と文化 [1.1.1]

情報セキュリティガバナンスの目的

ISACA 用語集は、情報セキュリティガバナンスを、取締役会と経営層が負う責任と実務の集まりと定義します。狙いは 4 つです。戦略的な方向を示すこと。目標が達成されること。リスクが適切に管理されること。資源が責任を持って使われていることの確認です[4]。

NIST SP 800-100 は目的を次のように書きます。ミッションを支える適切な統制を、費用対効果よく先回りして実装し、変化するリスクを管理すること[5]。ISACA の用語集は、企業の情報と技術のガバナンス（EGIT）に期待する成果を 3 つ挙げます。便益の実現、リスクの最適化、資源の最適化です[4]。用語集は、この 3 つが釣り合った状態を、ガバナンスの主な目的である「価値の創造」と説明します[4]。

SAMPLE

3 つの成果	中身	取り違えやすい誤り
便益の実現	新しい便益を生み、今の便益を保って広げ、十分な価値を生まない取り組みや資産をやめる	技術的な高度さを目的にする
リスクの最適化	リスクを許容度の範囲に保つ	リスクをゼロにしようとする
資源の最適化	人・金・技術を、効果の大きい所へ配分する	全領域に均等に配る

NIST SP 800-39 は、リスク管理のガバナンスの成果を 5 つ挙げます。戦略との整合、リスク管理プロセスの実行、資源の効果的な配分、指標に基づく成果、投資の最適化による価値の提供です[6]。同じ文書は、ガバナンスの強さを、上級経営層の関与の最良の指標としています[6]。経営層が関与しない組織では、どれほど規程を整えても成果が出ません。

経営者は、サイバーセキュリティの優先事項と目標を定めるときに、期待を伝えます。伝える内容は、リスク選好、説明責任、資源についての期待です[7]。この期待が、現場の統制の強さと投資額の出発点になります。

組織の目的・使命とセキュリティの位置付け

セキュリティは、事業を支える機能です。CSF 2.0 の GOVERN は、リスク管理の判断を取り巻く状況の理解を求めます。状況とは、ミッション、ステークホルダーの期待、依存関係、法令・規制・契約上の要件です（GV.OC）。GV.OC-01 はミッションを理解してリスク管理に反映すること。GV.OC-02 は内外のステークホルダーの期待を把握することです[7]。統制の強さは、拠点や事業ごとの役割と影響の大きさで変えます。全社一律に最も厳しい統制をかけるのは、資源の

SAMPLE

最適化に反します。経営目標が変わったら、戦略の前提とのずれをリスクとして整理し、見直しを経営層に提案します。

たとえば、通販会社が、深夜の注文で売上の 4 割を得ています。管理者が全システムを夜間に止めて点検する案を出しました。この案は、セキュリティを目的にしてしまった例です。正しい動きは、売上への影響が最も小さい時間帯と方法を、事業部門と一緒に決めることです。統制を強くするだけの選択肢や、事業の目的を確認せずに技術を選ぶ選択肢は、不正解に回ります。

セキュリティ文化とリスク文化

用語集の「文化」は、行動、信念、前提、態度、物事の進め方の型です。「リスク文化」は、リスクを取ることへの態度を決める組織の共有された価値観と信念で、リスクや損失がどれだけ率直に報告され議論されるかも決めます[4]。CSF 2.0 の GV.RR-01 は、リーダーシップがサイバーリスクに責任と説明責任を持ち、リスクを意識し、倫理的で、継続的に改善する文化を育てるよう求めます[7]。

文化は、規程ではなく経営層の行動で決まります。報告した人を経営層が責めれば、インシデントの報告は減ります。SP 800-39 によれば、組織文化は、ガバナンス構造の変更（分散型からハイブリッドへの移行など）や、共通コントロールの選び方を、間接的に制約します[6]。変えるときの順序は、現状の把握、経営層による手本、教育と評価への反映、効果の測定です。戦略と文化が合わない時は、文化を評価して戦略の実施方法を合わせ、文化の側の改善も計画しなければなりません。合併や買収では、両社の文化の違いを評価し、経営層の方針の下で統合の方法を決めます。

隣の概念と並べると、違いが見えます。セキュリティ文化は、従業員がセキュリティを当然の行動として取る状態です。リスク文化は、リスクを隠さず報告できる状態まで含みます。管理者が一人でできるのは、現状の測定と、経営層への

SAMPLE

提案までで、それ以上は進められません。変える主体になれるのは経営層だけで、管理者ではありません。

リスク選好とリスク許容度

用語集の 3 つの定義は、試験で並べて問われます[4]。

用語	用語集の定義	例
リスク選好（appetite）	使命を追う中で、広い水準で受け入れてよいとする量	顧客の個人データの漏えいは受け入れない
リスク許容度（tolerance）	特定のリスクについて、経営が許す変動の幅	基幹システムの停止は月 4 時間まで
リスク容量（capacity）	組織の存続を危うくせずに耐えられる損失の客観的な大きさ	自己資本を超える損失は耐えられない

容量は外側の限界です。選好はその内側の方針で、許容度は個別のリスクに当てはめた数値の幅です。SP 800-39 は、許容度を、組織が受け入れられるリスクの水準または不確実性の度合いと定義します。組織文化を映し、損失の種類ごとに違い、上級経営者個人の主観にも強く左右されます[6]。CSF 2.0 の GV.RM-02 は、選好と許容度の表明を、策定し、伝達し、維持するよう求めます。経営はこれを基に優先順位と支出を決めます[7]。

決めるのは経営層です。管理者は材料を出し、決まった値を統制の強さに翻訳します。リスク評価で許容度を超えるリスクが見つかったとき、管理者が受け入れを決めることはできません。経営層に報告し、判断を求めます。許容度が文書になっていない組織では、最初に、経営層と許容度を決める作業を始めます。

SAMPLE

ガバナンスとマネジメントの違い

用語集は、ガバナンスの説明責任を次のように書きます。ステークホルダーのニーズ、条件、選択肢を評価する。優先順位付けと意思決定で方向を設定する。計画に対する業績、遵守、進捗を監視する。多くの組織で、責任を負うのは取締役会です[4]。用語集は、COBIT 2019 のガバナンスシステムの原則の 1 つとして、ガバナンスをマネジメントと区別することも挙げています[4]。

	ガバナンス	マネジメント
主体	取締役会と経営層	経営層の指示を受ける管理者
動詞	評価する、方向付ける、モニタリングする	計画する、構築する、運用する、監視する
例	リスク許容度の承認。戦略と予算の承認	プログラムの運営。統制の導入。インシデント対応

CSF 2.0 はこの区別を機能の並びで示します。GOVERN は、ほかの 5 機能（IDENTIFY・PROTECT・DETECT・RESPOND・RECOVER）の成果を何にするか、どう優先するかを決める機能です。決める材料は、ミッションとステークホルダーの期待です。CSF のコアは 6 機能で、GOVERN は 2.0 で加わりました[7]。CSF は、ガバナンスの活動を、サイバーセキュリティを全社的リスク管理（ERM）の戦略に組み込むうえで不可欠なものとしています[7]。

たとえば、取締役会が、侵入検知の製品の選定まで決めようとしたとします。これは役割の取り違えです。取締役会が決めるのは、許容度と戦略の方向です。製品の選定はマネジメントの側に属し、取締役会の仕事ではありません。管理者は、取締役会が方向を決められるよう、リスクと費用を事業の言葉で出します。

SAMPLE

リスク管理の枠付けと、この節の間違えやすい点

SP 800-39 は、リスク管理を 4 つの要素で説明します。枠付け（frame）、評価（assess）、対応（respond）、監視（monitor）です。最初の要素は枠付けで、リスクに基づく判断を行う環境、つまりリスクの文脈を定めます[6]。許容度と選好は、この枠付けの材料です。評価の前に枠付けが来るので、許容度が決まっていない状態でリスクの大小を判定しても、判断の物差しがありません。

取り違えは 4 つの型に集まります。

- リスクの最適化を、最小化と読む型。目的はゼロにすることではなく、許容度の範囲に保つことです
- 選好と許容度を、逆に覚える型。選好は広い方針の水準で、許容度は個別のリスクの変動の幅です
- 文化を規程で変えられると考える型。文化を決めるのは、経営層の行動です
- 許容度を管理者が決める型。決めるのは経営層で、管理者は材料を出します

新しいサービスの評価で、停止リスクが許容度（月 4 時間）を超える見込みと分かった場面を考えます。事業部門は、予定どおりの開始を求めている。管理者は、選択肢（対策の追加、範囲の縮小、許容度の見直しを諮ること、リスクの受け入れ）とその費用を示し、経営層に判断を求めます。管理者が独断で承認する案も、独断で差し止める案も、判断の権限を持たない点で誤りになります。

文化の場面では、現場がインシデントを報告したがらない状況を考えます。原因は、報告者が責められた経験にあった。管理者が規程を厳しくしても、報告はさらに減ってしまいます。経営層が、報告を評価し、責めない姿勢を行動で示し、その結果を測定する流れが、先に来ます。

SAMPLE

法律、規制、契約上の要件 [1.1.2]

要件の特定と台帳化

CSF 2.0 の GV.OC-03 は、サイバーセキュリティに関する法令・規制・契約上の要件（プライバシーと市民的自由の義務を含む）を理解し、管理することを求めます[7]。用語集の「コンプライアンス」は、法令・規制が定める要件と、契約上の義務や内部方針から生じる自発的な要件に従うこと、およびその遵守を示せることです[4]。

手順は 4 つです。

1. 適用される要件を洗い出して台帳に載せる
2. 各要件に責任者を付ける
3. 要件を統制に対応付ける
4. 遵守の状況を監視する

新しい要件が出た場面の最初の行動は、自社に適用されるかの判断です。範囲は法務と決め、統制の導入や予算の要求は、その後に回します。用語集には「相当の注意（due care）」と「デューデリジェンス」もあります。前者は、同じ能力を持つ合理的な人に期待される注意の水準。後者は、調査と確認を徹底して客観的に行うことです[4]。

個人データ保護の法令

GDPR は、EU の個人データ保護の規則です。第 5 条 2 項は、管理者に原則を守る責任を負わせ、遵守を実証できることを求めます。この義務が説明責任と呼ばれます。第 37 条は、次の 3 つの場合に、データ保護責任者（DPO）の指名を求めます。

- 公的機関が処理する場合

SAMPLE

- 中核業務が、大規模な定期的・体系的監視である場合
- 特別カテゴリのデータを、大規模に処理する場合

第 38 条 3 項は、DPO が最高経営層に直接報告する、と定めています。第 35 条 2 項は、データ保護影響評価（DPIA）の際、DPO を指名しているなら助言を求めると定めます[8]。

制裁金は 2 段階です。管理者・処理者の義務（第 25〜39 条など）の違反は、1,000 万ユーロか、全世界年間売上高の 2% のどちらか高い方が上限です。基本原則、データ主体の権利、第三国移転の違反は、2,000 万ユーロか 4% の高い方が上限です[8]。処理者が承認された行動規範や認証の仕組みを守っていることは、十分な保証を示す要素になります（第 28 条 5 項）[8]。

日本の個人情報保護法は、個人情報保護委員会が法令を公開しています[9]。管理者の対応は、取扱いの台帳、委託先の管理、漏えい時の報告体制の 3 つに集まります。DPO のような専任の責任者の指名は、GDPR が求める仕組みです。日本法の説明として DPO の指名義務を挙げる答えは、取り違えとなり、正解になりません。

侵害の通知義務

通知の期限は法ごとに違い、数字がそのまま問われます。

法令	最初の通知	続きの通知
GDPR 第 33 条	監督機関へ原則 72 時間以内。超えるなら遅延の理由を添える	処理者は侵害を知ったら、不当な遅滞なく管理者へ通知する（同条 2 項）
NIS2 第 23 条	重大インシデントを認識してから 24 時間以内に早期警告	認識してから 72 時間以内にインシデント通知。最終報告は通知から 1 か月以内

SAMPLE

法令	最初の通知	続きの通知
日本の個人情報保護法	報告対象事態を知った後、速やかに（把握している事項を報告）	知った日から 30 日以内。不正の目的のおそれがある事態は 60 日以内

8109

日本で報告が義務になる事態は、施行規則第 7 条の 4 つです。要配慮個人情報を含む漏えい等。不正に利用されると財産的被害が生じるおそれがある漏えい等。不正の目的をもって行われたおそれがある漏えい等。本人の数が 1,000 人を超える漏えい等です[9]。報告先は個人情報保護委員会で、本人への通知も要る（法第 26 条 1 項・2 項）[1112]。

通知の主体は、管理者（事業者）です。管理者が組織の中で行うことは、事実関係を早く正確に集めて、法務・DPO・経営層に上げ、期限に間に合わせることです。期限は気付いた時点から数えます。調査の完了を待ってから通知する運用は、成り立ちません。分かっている範囲で第 1 報を出し、続報で補います。

たとえば、委託先から、顧客のカード番号を含むデータが流出した可能性があると連絡が来ました。調査は続いている状況です。最初に、GDPR か日本法かなど、適用される法を法務と確認し、期限の起算点を決めます。次に、分かっている事実で第 1 報の準備を進めます。原因が確定するまで通知を止める案と、委託先に通知を任せきりにする案は、どちらも不適切です。通知の責任が管理者に残る点は、どちらの案でも変わりません。

NIS2 は、必須事業体と重要事業体の経営機関に、サイバーセキュリティリスク管理措置の承認と実施の監督を求め、違反の責任も問います（第 20 条）[10]。取締役会に責任が戻る点は、CISM の考え方と一致します。

SAMPLE

契約上の要件とコンプライアンスの監視

顧客との契約は、法律と並ぶ要件です。用語集によると、サービスレベルアグリーメント（SLA）は、提供者と顧客の間の合意で、サービスの最低限の達成目標と、その測り方を決めます。SLA が定めるのは何が提供されるかで、どう提供するかは定めません[4]。

PCI DSS は、決済カードの口座データを守るために PCI SSC が作った標準です。技術と運用の要件の基準線を示します。対象は、カード会員データや機密認証データを保存、処理、伝送する事業者と、その環境の安全に影響を与えうる事業者です[13]。PCI DSS は法律ではなく、カード取引の契約で課される要件です。違反の結果は、法による罰則ではなく、契約に基づく措置になります。

監視の方法は、要件ごとに指標を決めて測ること、定期的に自己評価と監査を行うこと、例外に承認者を決めて記録することの 3 つです。契約の要件を満たせなくなる見込みが出たら、相手先へ連絡する前に、現状と影響を評価します。

国境を越えるデータ、データの所在地、電子的証拠開示

用語集の「越境データ移転」は、データの発生地の外にある受領者への、個人データの移転です[4]。GDPR は、第三国への移転に、拘束的企業準則や、欧州委員会が採択した標準データ保護条項などの適切な保護措置を求めます[8]。クラウドの保管場所を選ぶとき、管理者はデータの所在地と、そこに適用される法律を確認します。所在地が変わると、適用される法律も変わります。

電子的証拠開示（e-discovery）は、訴訟や調査で、電子的に保存された情報を探し、保全し、提出する手続です。EDRM の説明では、リーガルホールドは、紛争に関わりうる情報を、収集してレビューするまで、または案件が終わるまで守る手続です。保全を実行するには、対象データの場所を知っている必要があります[14]。訴訟が見込まれる場面では、保全の対象の情報について、通常の

SAMPLE

保存期限による自動削除を止めます。用語集の「保存方針」は、データや記録を処分するまで、どれだけ保管するかの指針です[4]。保存方針が法令の保存期間より短い時は、対象の記録について、法令に合わせて方針を改めます。全記録へ一律に広げる必要はありません。

規制の変化への対応

規制は変わります。動向を監視する担当を決めます。変更が自社に与える影響を評価します。要件の台帳を更新し、統制を見直します。この流れを定常業務にしたものが、GV.OC-03 の「要件を理解して管理する」状態です[7]。新しい規制が出た場面の最初の行動は、影響の評価です。

管理者と処理者の違いと、この節の間違えやすい点

GDPR の用語では、管理者は処理の目的と手段を決める側で、処理者は管理者のために処理する側です。ISACA の用語集は、処理者を、管理者に代わって個人データを処理する者と定義します[4]。処理者が侵害に気付いたときの義務は、管理者への通知です。監督機関への通知は管理者の義務になります[8]。委託先に処理を任せても、管理者の責任は消えません。

数字と役割は、次の対応で取り違えやすい所です。GDPR の 72 時間は、監督機関への通知の期限です。NIS2 の 24 時間は、早期警告の期限であり、詳細な報告の期限ではありません。最終報告は、通知から 1 か月以内です。制裁金は、管理者・処理者の義務の違反が上限 1,000 万ユーロか 2%。原則、権利、第三国移転の違反が上限 2,000 万ユーロか 4% です。DPO の報告先は、最高経営層となる。

契約と法律が食い違う場面を考えます。顧客との契約は、侵害を知ってから 24 時間以内の通知を求めている。法定の期限は 72 時間とします。管理者の動きは、契約の期限も満たせる運用にすること。法定の期限を守るだけでは、

SAMPLE

契約の違反が残ってしまいます。通知の手順は、短い方の期限に合わせて設計することになります。

組織の構造、役割、責任 [1.1.3]

取締役会、経営層、運営委員会

SP 800-100 によれば、組織の長が、運営とガバナンスの最終責任を負います。ただし、情報セキュリティの権限と責任の置き方は、集中型か分散型かで変わります[5]。用語集の上級管理者は、プロセスに方針と全体の指針を与える人です。日々の監視と統制は通常担いません。資源の配分を指示する権限は持ちます[4]。

運営委員会（steering committee）は、日本語の用語集の訳です[15]。用語集の「セキュリティフォーラム」の説明では、全社の主要な部門の経営幹部が加わり、事業戦略に沿ったセキュリティ戦略の策定や、主要な施策の承認を担います。既存の経営の会議体が、この役を兼ねることもあります[4]。事業部門が入るので、セキュリティの判断が事業の言葉で行われます。

ガバナンス構造のモデルは 3 つです。SP 800-100 は基本モデルとして集中型と分散型を挙げ、SP 800-39 はハイブリッド型を加えます[56]。

モデル	特徴
集中型	権限、責任、意思決定が中央組織だけにある。強力で情報に通じた中央のリーダーシップが要る。組織全体の一貫性が生まれる
分散型	部門ごとに判断する。部門間の調整と信頼を高める取り組みがなければ、組織が変化の受け入れに時間をかけることがある

SAMPLE

モデル	特徴
ハイブリッド型	権限、責任、意思決定を中央と下位組織が分担する。中央は、共有基盤のように全社に及ぶ事項の方針を定める

実際の構造は、集中型と分散型を両端とする連続体のどこかにあります。完全な集中型や分散型は稀です[5]。どのモデルでも、リスク受容についての責任の割当と、説明責任を明確にすることが、有効なリスク管理に欠かせません[6]。SP 800-39 は、リスク管理を 3 つの層で行うとします。第 1 層が組織、第 2 層がミッションと業務プロセス、第 3 層が情報システムです。上位の判断が、下位の活動を方向づけます[6]。

SP 800-100 の役職の整理は次のとおりです[5]。

- CIO: 情報セキュリティ責任者（SAISO）を指名する。全社のプログラムと方針・手順を整え、遵守を確保する。有効性と是正の進捗を、年次で組織の長へ報告する
- CFO: 投資審査委員会と組織の長に対する、上級の財務アドバイザー。セキュリティ投資も所管に入る
- 内部監査・監察（IG）: 情報セキュリティの実務を評価し、脆弱性や見直しの必要性を特定する
- 個人情報保護責任者（CPO）: プライバシー遵守に責任を負い、セキュリティとプライバシーの要件が一方のために損なわれないよう均衡を保つ

CISO の役割と報告の経路

用語集は、CISO を、組織の情報セキュリティの責任者としています[4]。SP 800-53 は、SAISO を、全社の情報セキュリティプログラムを調整、策定、実装、維持する使命と資源を持つ者として任命するよう求めます[16]。SP 800-100 によれ

SAMPLE

ば、SAISO は情報セキュリティを主たる任務とし、コンプライアンスを支える組織を率います。インシデントを検知、報告、対応する手順の整備と実施も、SAISO の責任です[5]。プログラム計画は、リスクに責任と説明責任を負う上級職が承認します[16]。

報告の経路は、利益相反の観点から決まる。CISO が IT 部門長の下に置かれると、納期や費用を優先する圧力が、リスクの報告を弱めるおそれがあります。セキュリティの判断が IT 部門の目標に左右されない位置ほど、独立性が高くなります。経営層や取締役会への直接の経路も、独立性を支える要素になります。

たとえば、CISO が CIO の下にいて、CIO が稼働の遅れを避けるため、重大な脆弱性の報告を先送りさせようとしたとします。管理者が取る行動は、CIO の判断に従うことではありません。リスクを評価し、報告の経路を使って経営層にリスクを伝えます。逆に、独断で外部に公表する案や、黙って待つ案は、役割の範囲を外れます。

データ・情報資産の所有者と管理者

用語集によると、データ所有者は、組織内のデータの完全性、正確性、利用に責任を持つ個人です。データ管理者（カストディアン）は、電子データの保管と保護に責任を持つ個人や部門です[4]。

	所有者（オーナー）	管理者（カストディアン）
決めること	分類の水準。誰がアクセスしてよいか。保護の要件	決まった要件の実装と運用
典型	業務の責任者（営業部長など）	IT 部門、運用部門、ホスティング事業者

SAMPLE

分類は、データの感度の水準を割り当て、水準ごとの統制を定めることです[4]。分類を決めるのは所有者です。「IT 部長にデータの分類を決めてもらう」は、よくある誤りです。IT 部門はカストディアンとして、決まった保護を実装します。クラウド事業者にデータを預けても、所有者の責任は移りません。すべてのデータに最高の水準をかけると、価値の低いデータにも高い統制の費用がかかり、保護の濃淡が付きません。組織の再編などで所有者が不在になったデータは、そのデータを使う業務の責任者を新しい所有者に割り当て、分類と保護の要件を決め直してもらいます。

RACI と説明責任、職務の分離

用語集の RACI は、Responsible、Accountable、Consulted、Informed の頭文字です。Responsible は、活動を確実に完了させる人です。Consulted は意見を求められる人で、双方向の連絡です。Informed は進捗を知らされる人で、一方向の連絡です[4]。Accountable は、結果に最終的に責任を持つ人です。1 つの活動に 1 人とします。2 人にすると、責任の所在が曖昧になります。Responsible は複数でも構いません。

職務の分離（SoD）は、用語集では、取引の開始と記録、資産の保管を別々の個人に割り当てて、誤りや不正を防止または検出する基本的な内部統制です[4]。日本語の用語集は「職務の分掌」と「職務の分離」の両方を載せます[15]。1 人が変更の承認と実施の両方を持つと、不正や誤りを検出できません。小さな組織で分離が難しいときは、独立した人による確認を補完統制として置きます。

リスクオーナー、コントロールオーナー、事業部門の責任

用語集の定義は次のとおりです[4]。

SAMPLE

- リスクオーナー: リスクに基づく判断をする権限と説明責任を組織から与えられ、リスクが現実になったときの損失を負う人
- コントロールオーナー: コントロールに関する判断をする権限と説明責任を与えられ、コントロールが実装され、有効に動いていることに責任を持つ人

リスクの受容は、リスクオーナーが決めます。管理者は、リスクを特定し、評価し、助言します。事業部門のリスクを自分で受け入れることはできません。CSF 2.0 の GV.RR-02 は、サイバーリスク管理の役割、責任、権限を、確立し、伝達し、理解させ、強制するよう求めます[7]。事業部門の管理者は、自分の部門のリスクのオーナーとして、セキュリティの要件を守る責任を負います。

リスク・エグゼクティブと、この節の間違えやすい点

SP 800-39 のリスク・エグゼクティブは、組織全体のリスク管理を包括的に行うための機能的な役割です。特定の組織構造や個人を前提とせず、個人でも委員会でも構いません[6]。CISO と同じ意味ではありません。

取り違えが多いのは、次の 4 つです。

- Accountable を 2 人置くと、責任が曖昧になる
- 分類を決めるのは、IT 部門のカストディアンではなく、業務のオーナーである
- 変更を承認する人と実施する人が同じだと、職務の分離が崩れる
- リスクを受け入れる権限は、管理者ではなく、リスクオーナーにある

ある変更で、開発者が自分で本番環境へ反映し、自分で承認も行っていた場面を考えます。この状態は職務の分離に反しています。管理者が求めるのは、承認者と実施者を分けることでした。小さな組織で人が足りなければ、事後

SAMPLE

の独立した確認を補完統制として置きます。承認の記録を残すだけの案や、開発者を信頼して見過ごす案では、不正と誤りを検出できません。

もう 1 つ、データの責任の場面です。営業部のデータの保管をクラウド事業者に委託しました。事業者が障害を起こし、データが失われました。分類と保護の要件を決める責任は、委託後も営業部のオーナーに残ります。責任の転嫁を事業者に求めるだけでは、解決になりません。契約と監視で、要件の遵守を確認します。

情報セキュリティ戦略の策定 [1.2.1]

戦略の起点と、組織戦略への連動

SP 800-100 によれば、情報セキュリティ戦略は、組織の戦略計画、業績計画、IT 戦略計画を支えます。内容が上位の文書に明確にたどれる必要があります。戦略は、プログラムの開発、制度化、評価、改善を可能にする枠組みを定め、プログラムごとに使命、ビジョン、目標を書き、組織の使命との関係を示します[5]。情報セキュリティ戦略計画などの文書にまとめ、全社の戦略計画と整合させます。独立した文書である必要はなく、IT 戦略計画の 1 章でもかまいません。目標とその進捗を監視する業績指標も、戦略で定めます[5]。

起点は事業の目的です。脅威や製品が起点ではありません。「顧客の信頼を損なわずに海外へ展開する」という目的から、必要な保護の水準、投資の順序、測る指標を導きます。事業の方針が大きく変わった場面の最初の行動は、変わった目的の確認です。

リスク管理戦略は、別の文書です。SP 800-39 によれば、リスク管理戦略は、組織がリスクをどう評価し、対応し、監視するかを示します。前提、制約、リスク許容度、優先順位とトレードオフも明示する。リスク・エグゼクティブという機能（個人でも委員会でもよい）を置くと、戦略を全社で一貫して適用しやすくなり

SAMPLE

ます[6]。CSF 2.0 の GV.RM は、組織の優先事項、制約、許容度と選好の表明、前提を確立して伝えるよう求めます。GV.RM-01 は、リスク管理の目標をステークホルダーと合意して決めるよう求めます[7]。

現状と目標のギャップ分析、成熟度モデル、ロードマップ

CSF 2.0 の組織プロファイルは、現状と目標を、コアの成果で記述します。現在プロファイルは今達成している成果、目標プロファイルは優先して達成したい成果です。差を分析し、優先順位をつけた行動計画（リスク登録簿や POA&M など）で埋めます[7]。CSF 2.0 の手順を、現状と目標に分けて書くと、次の 5 つになります。

1. 現在プロファイルを作る
2. 目標プロファイルを作る。事業の目的と許容度から決める
3. 差を分析する
4. 優先順位をつけて行動計画を作り、ロードマップに並べる
5. 実施して、プロファイルを更新し、循環させる

用語集の能力成熟度モデル（CMM）は、効果的なプロセスの要素と、未成熟なプロセスから成熟したプロセスへ進む道筋を示すモデルです。5 段階で、レベル 1 が最も未成熟で混沌とした状態、レベル 5 が最も成熟した状態です[4]。目標は、全領域を最高にすることではありません。事業の目的とリスクに見合う水準を、領域ごとに決めます。

CSF の「ティア」は、成熟度の別名ではありません。組織のリスクのガバナンスと管理の実務について、厳格さを 4 段階で特徴づけます。Partial がティア 1、Risk Informed がティア 2、Repeatable がティア 3、Adaptive がティア 4 です。ティアは、組織のリスク管理手法を置き換えず、補完します[7]。

SAMPLE

戦略に影響する内部と外部の要因

用語集の SWOT は、内部の強みと弱みの監査と、外部の機会と脅威の環境調査を組み合わせた分析です[4]。内部の要因は、事業の変化、組織文化、人員と技能、予算、既存のシステムです。外部の要因には、技術の変化、規制、脅威の動向、取引先や顧客の要求が入る。

たとえば、経営層が、同業の会社の買収を決めたとします。買収先のシステムは、自社と標準が違っています。最初の行動は、買収の目的と、買収先の現状のリスクを把握し、戦略の見直しの要否を判断することです。買収先の統制を、直ちに自社の標準へ置き換える案は、順序が逆になります。戦略は、文書を作って終わりではありません。GV.OV-02 は、リスク管理戦略が組織の要件とリスクを網羅しているかを、見直して調整するよう求めます[7]。

SP 800-100 によれば、米国の連邦機関には GPRA という法律が、戦略計画を前回提出から 3 年以内に更新し、業績計画を毎年提出するよう求めています[5]。周期は組織ごとに決めます。定期の見直しと、大きな変化による臨時の見直しの 2 本立てが基本です。

戦略の要素と更新の契機

戦略の要素は、目的（使命、ビジョン、目標）、制約、資源、ロードマップ、業績指標です。SP 800-53 の PM-1 は、全社の情報セキュリティプログラム計画に、要件の概要、管理策、役割と責任と経営の関与、組織間の調整と遵守を含め、上級職が承認するよう求めます[16]。

更新の契機は、事業の変化、重大なインシデント、監査の指摘、規制の変更、技術の変化、指標が目標から外れたこと、の 6 つです。

SAMPLE

経営層の支持を得る方法

経営層の関与は、ガバナンスの強さの最良の指標です[6]。支持を得るには、事業の言葉で話すことです。「ファイアウォールの更新が必要」は、技術の言葉にとどまります。「受注システムが 3 日止まると、1 日 2,000 万円の売上を失うおそれがあります。許容度は 1 日なので、冗長化に 1,500 万円の投資を提案します」は、事業の言葉になります。リスク、価値、費用、選択肢を示し、経営層が判断できる形に整えるのが基本でした。CSF 2.0 は、サイバーセキュリティの用語を、経営層に通じるリスク管理の言葉へ翻訳することを、役割に挙げます[7]。

提案が通らなかった場面では、技術の説得を重ねません。残るリスクを経営層に明示して、受け入れの判断を記録してもらう流れになります。受け入れる権限は、リスクオーナーに属します。

ギャップ分析と成熟度の場面

経営層が「すべての領域で成熟度を最高の水準にせよ」と指示した場面を考えます。目標は、事業の目的とリスクに見合う水準を、領域ごとに決めるもの。管理者は、全領域を最高にする案をそのまま受けず、現状と目標のギャップを領域別に示し、費用と効果の大きい所から並べます。成熟度の高さは、それ自体が目的ではありません。

戦略とロードマップの関係は、戦略が方向と目的、ロードマップが時間軸の実施計画です。ロードマップだけ作って戦略を欠くと、投資が事業の目的とつながりません。戦略は、組織の戦略計画から追跡できることが条件です[5]。

SAMPLE

エンタープライズアーキテクチャ [1.2.2]

EA の定義と目的

用語集は、エンタープライズアーキテクチャ（EA）を、次の記述と定めます。事業システムの構成要素（または技術などその 1 つの要素）の根本的な設計。構成要素どうしの関係。それらが組織の目的を支える仕組み[4]。SP 800-39 によれば、EA は、ミッションと業務プロセス、情報資源の有効性を最大にするための経営の実践です。セキュリティ投資を含む投資と、測定可能な成果の改善を結びつけます。IT 資産を標準化、統合、最適化する機会も与えます[6]。層は、事業、データ、アプリケーション、技術の順に重なります。

セキュリティアーキテクチャは、EA の不可欠な一部です。システムの強靭性と、セキュリティ機能の実装に関する部分を指します。対策の配置は、多層防御と広域防御の考え方に沿います。多層防御は、防御を重ねて、攻撃者と資産の間に複数の障壁を置く実務です[4]。EA の参照モデル（パフォーマンス、ビジネス、サービスコンポーネント、データ、技術）ごとに、セキュリティアーキテクチャの版があります[6]。

EA の枠組み（TOGAF、ADM、Zachman）

TOGAF の ADM（アーキテクチャ開発手法）は、準備段階（Preliminary）と、A から H の 8 つのフェーズ、全体にわたる要件管理で成り立ちます[17]。

フェーズ	内容	セキュリティの関わり
準備	アーキテクチャの能力を作る準備。原則を決める	セキュリティの原則を組み込む
A ビジョン	範囲、ステークホルダー、ビジョン、承認	目的とリスクの把握
B 事業	事業アーキテクチャ	保護すべき事業の機能

SAMPLE

フェーズ	内容	セキュリティの関わり
C 情報システム	データとアプリケーションのアーキテクチャ	分類、アクセス制御
D 技術	技術アーキテクチャ	実装する対策
E 機会と解決策	提供の手段を特定。実装に直接関わる最初のフェーズ	対策の優先順位
F 移行計画	現状から目標へ。詳細な実装と移行の計画	移行中のリスク
G 実装ガバナンス	実装の監督	設計との適合の確認
H 変更管理	新しいアーキテクチャの変更を管理する手続	変更時のリスク評価

ADM は反復的で、フェーズの間でも、フェーズの内部でも繰り返します[17]。Zachman フレームワークは、通常 6×6 の分類表で描かれます。列は What、How、Where、Who、When、Why の 6 つの問いです。行の立場の名前は、版や資料によって違います[18]。TOGAF は進め方の手順を持ち、Zachman は成果物を分類する枠組みです。

セキュリティアーキテクチャを EA に整合させる

SP 800-53 の PM-7 は、セキュリティとプライバシー、組織と個人へのリスクを考慮して、EA を策定、維持するよう求めます。PL-8 は、システム単位のセキュリティ・プライバシーアーキテクチャを、全社のアーキテクチャ（PM-7）と整合させるよう求めます。あわせて、定めた頻度でアーキテクチャを見直して EA の変更を反映し、計画したアーキテクチャの変更を、セキュリティとプライバシーの計画、運用構想（CONOPS）、重要度の分析、組織の手順、調達と取得に反映するよう求めます。要件と対策を EA に統合すると、システム開発の全期間で考慮され、ミッションと業務プロセスに明示的に結びつきます[16]。

SAMPLE

SP 800-39 は、単一障害点を設計の早い段階で扱わなければ、各システムにその弱点が伝わると述べます。実際の障害で、ミッションと業務能力の喪失という深刻な結果を招きます。第 2 層の EA の判断は、第 3 層のシステム設計と、使える技術の種類に影響します[6]。関与の時期は、設計の段階です。完成後に付け足すより、設計の段階で入れるほうが、標準化も再利用もしやすくなります。SP 800-100 は、チーフ・エンタープライズ・アーキテクトに、情報セキュリティを EA の全層に統合することを促す責任があるとしています[5]。

SP 800-207 のゼロトラスト（ZT）は、ネットワークが侵害されている前提で、要求ごとに最小権限のアクセス判断を行い、不確実性を最小にする考え方の集まりです。ゼロトラストアーキテクチャ（ZTA）は、その概念を使い、構成要素の関係、ワークフロー、アクセスポリシーを決める企業のサイバーセキュリティ計画です[19]。SP 800-207 は基本原則を 7 つ挙げます。そのうち 2 つと、アクセスを許可する仕組みは次のとおりです。

- ネットワーク上の場所だけでは信頼しない。社内の端末からの要求にも、外部と同じ要件を課す
- アクセスはセッション単位で許可する。あるリソースの認証が、別のリソースへのアクセスを自動で許すことはない
- アクセスは、ポリシーエンジンとポリシー管理者からなるポリシー決定点（PDP）と、ポリシー実施点（PEP）を通じて許可する

EA のガバナンス

EA のガバナンスは 3 つで動かします。アーキテクチャの審査会、標準の技術の一覧、例外の手続です。新しいシステムは、審査会で、標準との適合とセキュリティ要件の織り込みを確認します。標準から外れる必要があるなら、リスクを評価し、承認者と期限を決めて、例外として記録します。TOGAF の ADM では、G が実装の監督、H が変更の統制を担います[17]。

SAMPLE

たとえば、事業部門が、審査を通さずに、独自のクラウドサービスを導入したとします。管理者は、サービスを直ちに止めるのではなく、リスクを評価して、標準への移行か例外としての承認かを、審査会に諮ります。EA のガバナンスは、標準を押し付ける仕組みではなく、例外を見える形で管理する仕組みになる。

ゼロトラストと、アーキテクチャの要件の取り込み

SP 800-207 は、ゼロトラストアーキテクチャの基本原則の 1 つとして、あらゆるデータ源と計算サービスをリソースとみなすことを挙げます[19]。SP 800-39 によれば、情報セキュリティアーキテクチャは、法令、指令、方針、規制、標準、ガイダンスのセキュリティ要件を、セグメントアーキテクチャへ取り込みます[6]。要件は、設計のときに入ります。

場面で考えます。社内ネットワークに接続した端末は信頼してよい、という設計方針の会社が、ゼロトラストへの移行を検討します。ゼロトラストでは、場所は信頼の根拠になりません。社内の端末にも、要求ごとに認証と認可を行い、アクセスはセッション単位で許可します。境界の防御を強化するだけの案や、社内ネットワークを信頼したまま認証を一度だけにする案は、前提が逆です。

情報ガバナンスのフレームワークと標準 [1.2.3]

COBIT

ISACA の COBIT 7 は、5 つのドメインと 40 の目標で、ガバナンスシステムを構成します。人、プロセス、技術の管理という複雑な作業を整理する、包括的なガバナンスの枠組みと位置づけられている。評価は、取締役会レベル、ハイレベル、詳細の 3 段階です[20]。COBIT 2019 のガバナンスシステムは、6 つの原則を掲げます。ステークホルダーへの価値の提供。包括的な取り組み。動的な

SAMPLE

ガバナンスシステム。ガバナンスとマネジメントの区別。組織の必要に合わせた調整。エンドツーエンドのガバナンスシステム。この 6 つです[4]。

COBIT は、ガバナンスの目標と、ガバナンスをマネジメントと分ける考え方の根拠になります。ISACA の用語集は、COBIT 2019 を、情報と技術（I&T）のガバナンスとマネジメントの、広く包括的な枠組みと説明します[4]。個々の目標の番号を覚える必要はありません。

ISO/IEC 27001 と 27002

ISO/IEC 27001 は、情報セキュリティマネジメントシステム（ISMS）の要求事項を定める規格です。組織が ISMS を確立し、実施し、維持し、継続的に改善するための要求事項を示します。何を行うべきかを主に書き、どう実現するかは書きません[21]。ISMS は、リスクアセスメントで必要なセキュリティの水準を決め、計画を持ち、資源を配分して運用する、マネジメントの仕組みです[21]。

本文は、すべての組織に適用が必要です。附属書 A の管理策は、事業の特性に応じて、適用を除外することもあります。除外の理由は、適用宣言書（SoA）に書きます。適用宣言書は、組織が適用する管理策を記述した文書化した情報です。適用した結果と理由、適用しない管理策とその理由を明記します[21]。

現行の版は、ISO/IEC 27001:2022 に、追補 1（2024 年、気候変動対応の変更）を併せたものです。日本では JIS Q 27001:2025 が、追補 1 に対応します[21]。ISO/IEC 27002:2022 は 2022 年 2 月に発行された管理策の指針です。93 の管理策を、組織的、人的、物理的、技術的の 4 つのテーマに分けます[2223]。27001 は要求事項で、認証の基準になります。27002 は手引です。情報セキュリティのガバナンスの手引には ISO/IEC 27014 があります[23]。

SAMPLE

NIST CSF 2.0

CSF 2.0 は、業種と規模を問わず、サイバーセキュリティリスクを管理し、低減するための枠組みです。サイバーセキュリティプログラムの成熟度にかかわらず使えます。コアは、機能、カテゴリ、サブカテゴリの階層で、6 つの機能（GOVERN、IDENTIFY、PROTECT、DETECT、RESPOND、RECOVER）を持ちます。GOVERN の下には 6 つのカテゴリがあります[7]。

カテゴリ	内容
GV.OC 組織の状況	ミッション、ステークホルダー、法令と契約上の要件
GV.RM リスク管理戦略	優先事項、制約、許容度、選好
GV.RR 役割、責任、権限	説明責任、文化、資源の配分
GV.PO 方針	方針の策定、伝達、見直し
GV.OV 監督	リスク管理戦略の結果の見直し
GV.SC サプライチェーン	サプライヤーのリスク管理

プロファイルには、現在と目標があります。ティアは 1 から 4 です。コミュニティプロファイルは、共通の関心を持つ複数の組織のために作られ、公開される、基準線の成果です。組織は、これを自分の目標プロファイルの土台に使えます[7]。SP 800-53 Rev.5 の管理策は、20 のファミリーに整理されています[16]。

枠組みの選び方と組み合わせ方

枠組みは手段で、どれか 1 つが最良という答えはありません。役割が違うため、組み合わせて使うのが普通です。

SAMPLE

枠組み	役割
COBIT	経営層向けのガバナンスの目標。ガバナンスとマネジメントの区別
ISO/IEC 27001	ISMS の要求事項。認証が取れる
ISO/IEC 27002	管理策の手引
NIST CSF 2.0	リスクに基づく成果の整理。現状と目標の比較
SP 800-53	管理策の詳細な一覧

選ぶ基準は、組織の状況です。見るのは、業種、規模、規制、顧客や取引先の要求。取引先が認証を求めるなら、ISO/IEC 27001 が優先です。経営層へ現状と目標を示す場面では、CSF のプロファイルが使いやすくなります。

たとえば、経営層が「競合が ISO の認証を取ったので、うちも全統制を同じにしたい」と言ったとします。管理者の動きは、認証の目的を確認し、自社のリスクと要求に合う範囲を決め、適用宣言書で適用と除外を整理することです。競合の統制を丸ごと写す案も、枠組みを使わず独自に決める案も、事業の目的と結びつきません。枠組みを入れただけでは、ガバナンスになりません。自社の目的に合わせて調整して、初めて機能します。

ガバナンスの枠組みの構築と運用

SP 800-100 によれば、組織は、使命を支え、現在と将来のセキュリティ要件を実装するため、正式な情報セキュリティガバナンス構造を確立すべきです。活動は、戦略計画、組織設計、役割と責任の設定、EA との統合、方針とガイダンスへの目標の文書化です。ガバナンスは、重要な役割と責任の特定に決定的な役割を持ちます。方針の策定、監督、継続的な監視にも影響します[5]。法務、

SAMPLE

財務、IT など分野ごとに組織されがちなガバナンスは、統一された取り組みで調整すると、全社で一貫します[6]。

運用では、文書を階層で整えます。用語集の方針は、必要な活動と禁止される活動を伝える文書です。標準は、承認された外部の標準化団体が定める義務的な要件です。手順は、特定の作業の手順を詳しく書いた文書です。ガイドラインは、手順より規定の少ない、やり方の説明です[4]。委員会と役割で意思決定し、指標で測り、報告し、見直す循環を回します。

枠組みの取り違えと、選ぶ場面

取り違えやすい点は 4 つあります。

- CSF のティアは、成熟度の別名ではない。ガバナンスと管理の実務の厳格さを表し、リスク管理手法の代わりでなく補完である
- ISO/IEC 27001 の認証を取った組織でも、附属書 A の管理策はリスクアセスメントの結果で選び、適用宣言書に理由を書く
- 27002 は手引で、認証の基準は 27001 である
- COBIT は、ガバナンスとマネジメントを分ける考え方の根拠になる

選ぶ場面では、問われている目的を見ます。

目的	選ぶ枠組み
取締役会に、ガバナンスの目標と責任の分け方を示す	COBIT
認証を求める取引先に応える	ISO/IEC 27001
現状と目標の差を、経営層に成果の形で示す	CSF のプロファイル
設計の段階で、要件を整理する	アーキテクチャの枠組み（TOGAF など）

SAMPLE

戦略計画（予算、リソース、ビジネス・ケース）[1.2.4]

ビジネスケースの要素と作り方

用語集のビジネスケースは、事業の投資をする根拠の文書です。投資を進めるかの意思決定を支え、投資の全期間を管理する運用の道具にもなります[4]。要素は、便益、費用、リスク、選択肢の比較です。用語集の費用対効果分析は、プラスの要因を足し、マイナスの要因を引いて、リスク対応を支えるビジネスケースを作る分析です[4]。

SP 800-100 の手順では、ビジネスケースに、前段の 3 つの局面の結果を裏づけとして含めます。優先順位をつけた是正措置の上位から最大 3 件を選び、完全な費用便益分析にかけます[5]。選択肢には、何もしない場合も入れます。何もしない場合のリスクが、比較の基準になるからです。

セキュリティ投資の評価（ROI、ROSI、TCO）

用語集の定義は次のとおりです[4]。

- ROI: プロセスや解決策の改善による便益と、実装の費用との比。価値を判断する
- NPV（正味現在価値）: 投資の税引後の割引率と、一定期間ごとの追加の支出（初期投資と運用費）と収入（費用の削減または収益）から計算する。公平な NPV には、導入後 5 年ほどまでの収入を含める
- TCO（総保有コスト）: 購入費に、ソフトウェア、ハードウェアとソフトウェアの更新、保守、技術サポート、訓練、利用者の活動の費用を加えたもの

セキュリティ投資の ROI（ROSI）は、便益を、対策で減る年間の予想損失とします。年間の予想損失（ALE）は、1 回の損失額（SLE）に、年間の発生頻度（ARO）を掛けた値です。数字で確かめます。

SAMPLE

	対策なし	対策 A	対策 B
1 回の損失（SLE）	6,000 万円	6,000 万円	3,000 万円
年間の頻度（ARO）	0.5	0.1	0.5
ALE	3,000 万円	600 万円	1,500 万円
便益（ALE の減少）		2,400 万円	1,500 万円
年間の費用		800 万円	500 万円
純便益		1,600 万円	1,000 万円
ROI（便益÷費用・用語集の定義）		300%	300%

用語集の定義どおり便益÷費用で計算すると、A も B も 300%（2,400÷800、1,500÷500）で同じです。純便益を費用で割る流儀もあり、その場合は両方 200% になります（1,600÷800、1,000÷500）。どちらの式でも、2 つの案の ROI は同じ値になります。比率が同じなら、予算が足りる限り、純便益の大きい A のほうがリスクを大きく減らせます。予算が 500 万円しかない場合、実行できるのは B だけになります。ROI だけで決めず、リスクの大きさ、予算、事業の目的と合わせて見ます。

TCO の例では、初期費用 2,000 万円と、年間の運用費 600 万円なら、3 年間の TCO は 3,800 万円になる。購入費だけを比べると、運用の費用を見落とします。

予算の計画と資源の配分

SP 800-100 は、資本計画・投資管理（CPIC）を、限られた予算を最優先のセキュリティ投資に配分し、資金の支出を管理する正式なプロセスと説明します。

SAMPLE

段階は、選定、統制、評価の 3 つ。投資のライフサイクル全体で、セキュリティを含めて規律を保ちます[5]。

段階	内容
選定（Select）	ミッションの必要性と改善の優先度で案件を評価する。便益、費用、リスクの基準で順位付けして、案件のポートフォリオを選ぶ。見直しの予定を決める
統制（Control）	運用中の投資が、当初の費用とスケジュールの節目に収まっているかを監視する
評価（Evaluate）	投資が、選定で決めた望ましい結果と実績目標を達成したかを問う

予算は、最も重要なセキュリティ投資から順に割り当てます。予算が尽きるか、優先事項が満たされるまで、次の層へ進みます[5]。例として、予算が 1,200 万円、優先順位の 1 位が 500 万円、2 位が 400 万円、3 位が 600 万円とします。1 位と 2 位で 900 万円を使うと、残りは 300 万円で、3 位に足りません。このときは、3 位の範囲を縮めるか、不足額と、見送ったときのリスクを経営層に報告します。優先順位の低い案件を先に埋めるのは、順序の逆です。

SP 800-53 の PM-3 は、プログラムに必要な資源を資本計画と投資要求に含め、例外を文書化するよう求めます。投資審査委員会（IRB）などの組織に、情報セキュリティの面を管理、監督させることもできます[16]。SP 800-100 は、IRB とポートフォリオ管理で、組織全体のビジネスケースを要件と優先事項に照らして優先順位をつけ、投資のポートフォリオを決める手順を示しています[5]。CSF 2.0 の GV.RR-03 は、リスク戦略、役割、責任、方針に見合う十分な資源の配分を求めます[7]。SP 800-100 によれば、分散型の構造では、部門レベルの SAISO の予算責任は、部門のセキュリティプログラムに及び、各運用部門のプログラムには及びません[5]。

SAMPLE

たとえば、経営層が、予算の削減を求めたとします。管理者の動きは、一律に削ることではありません。リスクの大きさと便益で優先順位を見直し、削った場合に残るリスクを経営層に示します。受け入れるかは、リスクオーナーが決めます。リスクの評価を示さずに、現場で自分の判断で投資を止めるのは誤りです。

人員、技能、外部資源の計画

用語集のアウトソーシングは、情報システムなどの業務を第三者が行う正式な合意です[4]。内製と外部委託を比べる軸は、業務の機密性、専門の技能を社内に持てるか、費用、管理の主導権、継続性の 5 つ。外部に委託しても、責任は委託元に残ります。戦略に必要な技能は、現状の技能とのギャップとして、計画に入れる。

戦略の進捗の管理

戦略はロードマップに落とし、マイルストーンを置き、定期的な見直しに掛けます。指標は、用語集の定義で使い分けます。KGI は、IT のプロセスが事業の要件を達成したかを、事後に示す指標です[4]。KRI は、重要なリスクを予測できる確率が高い、リスク指標の一部です[4]。用語集は、目標の SMART を「具体的、測定可能、達成可能、現実的、適時」、指標（メトリクス）の SMART を「具体的、測定可能、行動につながる、関連がある、適時」と、項目によって違う語で説明します[4]。

投資は、CPIC の統制の段階で費用とスケジュールを監視し、評価の段階で、選定で決めた成果が出たかを確認します[5]。計画と実績の差が大きいときは、原因を調べ、計画の変更を経営層に諮ります。

SAMPLE

投資の段階と、この節の場面

CPIC の 3 段階は、場面から見分けます。案件に優先順位をつけてポートフォリオを選ぶ作業は、選定です。運用中の投資が、当初の費用とスケジュールの節目に収まっているかを監視する作業は、統制です。導入が終わった投資が、選定で決めた望ましい結果と実績目標に達したかを確かめる作業は、評価です[5]。

ビジネスケースが経営層に却下された場面を考えます。理由は、投資の便益が経営層に見えなかったことでした。管理者は、技術の説明を増やす案を取りません。便益を、リスクの低減額と事業への影響の数字で示す。選択肢（何もしない場合を含む）を並べ、再提案します。費用だけを下げて同じ案を出す方法も、便益の説明にならないので不十分です。

投資の評価では、ROI と TCO の違いも問われる。ROI は便益と費用の比で、TCO は購入から運用までの総費用です。TCO を見ずに購入費だけで選ぶと、運用費の分だけ、ROI を実際より良く見積もってしまいます。NPV は、将来の収入と支出を割引率で現在の価値にして、投資の可否を判断する指標です[4]。

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、CISM 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。

Footnotes

1. ISACA「CISM Exam Content Outline」https://www.isaca.org/credentialing/cism/cism-exam-content-outline ↩ ↩2

2. ISACA「Certification Exams Candidate Guide」(CISM の問題数・時間・合格点・形式) https://www.isaca.org/-/media/files/isacadp/project/isaca/certification/exam-candidate-guides/2026/exam-candidate-guide.pdf ↩ ↩2

3. ISACA「Certified Information Security Manager (CISM)」認定ページ https://www.isaca.org/credentialing/cism ↩

4. ISACA Glossary https://www.isaca.org/resources/glossary ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16 ↩17 ↩18 ↩19 ↩20 ↩21 ↩22 ↩23 ↩24 ↩25 ↩26 ↩27 ↩28 ↩29 ↩30 ↩31 ↩32 ↩33 ↩34 ↩35 ↩36

5. NIST SP 800-100 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16 ↩17 ↩18 ↩19

SAMPLE

6. NIST SP 800-39 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16

7. NIST CSF 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6 ↩7 ↩8 ↩9 ↩10 ↩11 ↩12 ↩13 ↩14 ↩15 ↩16 ↩17

8. GDPR 第 5・28・33・35・37・38・83 条 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 ↩ ↩2 ↩3 ↩4 ↩5 ↩6

9. 個人情報保護法施行規則 第 7・8 条 https://laws.e-gov.go.jp/law/428M60020000003 ↩ ↩2 ↩3

10. NIS2 第 20・23 条 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 ↩ ↩2

11. 個人情報保護委員会 漏えい等報告 https://www.ppc.go.jp/personalinfo/legal/leakAction/ ↩

12. 個人情報保護法 第 26 条 https://laws.e-gov.go.jp/law/415AC0000000057 ↩

13. PCI DSS https://www.pcisecuritystandards.org/standards/pci-dss/ ↩

14. EDRM https://edrm.net/2022/03/the-ultimate-guide-to-a-defensible-litigation-hold-process/ ↩

15. ISACA CISM 用語集 日本語 https://www.isaca.org/-/media/files/isacadp/project/isaca/certific

SAMPLE

ation/cism/terminology/japanese_0922.pdf ↩ ↩2

16. NIST SP 800-53 Rev.5 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2 ↩3 ↩4 ↩5 ↩6

17. TOGAF Pocket Guide 第 6 章 https://pubs.opengroup.org/pocket-guides/togaf-pocket-guide/main/chap06.html ↩ ↩2 ↩3

18. Zachman Framework https://www.zachman.com/about-the-zachman-framework ↩

19. NIST SP 800-207 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf ↩ ↩2

20. ISACA COBIT 7 https://www.isaca.org/resources/cobit ↩

21. ISMS-AC https://isms.jp/isms/index.html ↩ ↩2 ↩3 ↩4

22. ISO/IEC JTC 1/SC 27 Journal 2025 https://committee.iso.org/files/live/sites/jtc1sc27/files/resources/Journal%202025.pdf ↩

23. JIPDEC 27000 ファミリー https://www.jipdec.or.jp/project/smpo/u71kba000000jjgv-att/27000family_20260518.pdf ↩ ↩2

SAMPLE

CISM 学習用テキスト(無料サンプル)

版

2026年11月版(CISM 試験範囲(ISACA 公式 CISM Exam Content Outline・2026年11月発効)準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

ISACA および CISM は、ISACA 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 ISACA が公開している試験内容の概要（ECO・受験者ガイド）などを基に作成したもので、ISACA 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。

SAMPLE