IT資格道場

ISC2 Systems Security Certified Practitioner (SSCP) 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 公式 SSCP Certification Exam Outline（Effective Date: October 1, 2025・v10/2025・英語版・日本語版）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 Security Concepts and Practices [1.1/1.2/1.3/1.4/1.5/1.6/1.7/1.8]

- ISC2 倫理規定と組織の倫理規定 [1.1]
- セキュリティの基本概念 [1.2]
- セキュリティコントロールの種類と選び方 [1.3]
- 5 つの機能による分類と補償コントロール [1.4]
- 資産管理のライフサイクル [1.5]
- 変更管理と構成管理 [1.6]
- セキュリティ意識向上とトレーニング [1.7]
- 物理的セキュリティ運用との連携 [1.8]

サンプルはここまでです

SAMPLE

このテキストの位置づけ: 3 点セットの本編。**これだけで問題が解けるようになる**ことが目標で、仕組み・計算・用語の区別を合格ラインの深さで扱う。

進め方: ① 学習用を読む → ② 頻出度別で解き方を掴む → ③ 問題演習で腕試し → ④ 頻出度別に戻って再確認(試験直前もここ)。暗記用は空き時間や用語の再確認に使う。

SAMPLE

第1章 Security Concepts and Practices [1.1/1.2/1.3/1.4/1.5/1.6/1.7/1.8]

第1章は配点 16% で、7 分野のうち最も大きい 2 つの分野の一つです。範囲は次の 8 つの細目に分かれます。

- 1.1 倫理規定への準拠
- 1.2 セキュリティコンセプトの理解
- 1.3 セキュリティコントロールの特定と実装
- 1.4 機能的セキュリティコントロールの文書化と維持
- 1.5 資産管理ライフサイクルのサポートと実施
- 1.6 変更管理ライフサイクルのサポートまたは実施
- 1.7 セキュリティ意識向上とトレーニング
- 1.8 物理的セキュリティ運用との連携

後の章のアクセス制御、リスク、インシデント対応、暗号、ネットワーク、システムの問題は、この章の言葉を前提に書かれています。管理策の分類、資産の扱い、変更の手順を取り違えると、後の章の場面問題でも選択肢の違いが見えません。

ISC2 倫理規定と組織の倫理規定 [1.1]

ISC2 倫理規定の前文と 4 つの規範

ISC2 倫理規定（ISC2 Code of Ethics）は、ISC2 の認定を持つ者（会員）が全面的に守ると約束する行動の規則です。倫理委員会は、受験資格に関わる場面でも、この規定の適用を監督します。前文は、社会と公共の利益、依頼主

SAMPLE

（principals）への義務、仲間への義務の 3 つのために、最高の倫理水準を守り、守っていると見られることを求めます。続けて、この規定の厳守が認定の条件だと書きます。[1]

規範（canon）は 4 つです。

番号	規範	守る相手
I	社会、公共の利益、必要な公共の信頼と信用、そして基盤（インフラ）を守る	社会
II	誠実に、正直に、公正に、責任をもって、適法に行動する	行動の全般
III	依頼主に勤勉で有能なサービスを提供する	雇用主・顧客
IV	専門職を前進させ、守る	専門職の仲間

依頼主とは、認定を持つ者と雇用や契約の関係にある相手で、雇用主、顧客、発注元がこれにあたります。

後進の指導、知識の共有、資格の信頼を高める活動は、規範 IV（専門職を前進させ、守る）にあたります。

規範の優先順位と衝突の判断

4 つの規範は I から IV の番号順に並び、前文も社会、依頼主、仲間の順に義務を挙げます。現行の倫理規定の本文に、優先の順位を定める一文はありません。規範どうしがぶつかる場面は、この並びに沿って、社会の保護、誠実と適法、依頼主への奉仕、専門職の利益の順に考えると判断できます。

SAMPLE

ある会社の管理者が、顧客の個人情報が外部に流れた事故を、契約先に黙っているよう上司から命じられている場面です。依頼主である上司への忠実（規範 III）と、被害を受ける人々や社会の保護（規範 I）がぶつかっています。規範 I が先なので、命令に従って黙る選択は誤りです。適法に行動する規範 II も、隠すことを許しません。正しい動きは、組織内の報告経路（法務・コンプライアンス・経営層）に事実を上げて、通知を進めさせることです。専門職の評判のために仲間をかばう（規範 IV）選択も、規範 I と II に反するなら取れません。

顧客から、競合会社の従業員の私的なメールを、本人の同意なしに取得するツールを導入してほしいと頼まれているとします。依頼主へのサービス（規範 III）は、規範 II の「適法に行動する」の下に置かれます。違法な行為を引き受ければ、顧客への奉仕を理由にしても、規範 II を破ることになります。適切な対応は、違法な部分を断り、合法な方法（自社の通信の保全や、契約で認められた調査）を提案することです。依頼主の要望は、規範の順序を超えられません。

見分けのこつは、選択肢が守る相手を並べることです。社会を守る選択と、依頼主や仲間を守る選択が並んでいたら、前者が正解になり、後者は正解になりません。

SAMPLE

倫理違反の申し立て

倫理規定には、違反の苦情を扱う手続きが付いています。[2] 試験では、誰が何を申し立てられるかと、手続きの形が問われます。

違反を疑う規範	申し立てられる人
I と II	一般の人（誰でも）
III	依頼主（雇用や契約の関係にある相手）だけ

違反を疑う規範	申し立てられる人
IV	専門職の仲間（資格や免許を持ち、倫理規定にも従う人）だけ

どの場合も、申し立てる人は、行為によって自分が損害を受けたと主張する必要があります。手続きの形は次のとおりです。

- 苦情は書面で出す。書面と PDF の 2 通を提出する。
- 形は宣誓供述書（sworn affidavit）。ほかの形の訴えは検討されない。
- 少なくとも、相手方、問題の行為、違反した規範、申立人の立場、裏づけの証拠を書く。
- どの規範か分からない時も、できる範囲で書いて出してよい。

審査するのは ISC2 専門職行為（倫理）委員会（Professional Conduct (Ethics) Committee）です。規定の適用を監督し、勧告をまとめる常設の委員会で、調査機関ではありません。調べる権限も証言を強制する権限もないので、提出された書面と、自発的に出た証拠だけで判断します。一応の事実が示されなければ、苦情は終結します。

相手方（respondent）には、通知を受けた後 30 日で、宣誓供述書の形で反論や事情を出す権利があります。黙っていると、事実を争わない意思とみなされかねません。事実の争いが決着しない時は、疑わしきは相手方の利益になり、立証の責任は申立人にあります。委員会は勧告を理事会に出し、双方が 14 日で意見を出せます。処分は理事会が決め、その決定は最終です。[2]

間違えやすい点が 3 つあります。委員会は調査機関ではなく、書面だけを見ます。規範 III を申し立てられるのは依頼主だけで、一般の人には資格がありません。口頭や電話での訴えは受け付けられません。

SAMPLE

組織の倫理規定とISC2 倫理規定の関係

組織の倫理規定（organizational code of ethics）は、勤め先が従業員に課す行動規範です。典型の中身は、利益相反の申告、贈答や接待の制限、機密の扱い、不正の報告義務です。ISC2 の規定と組織の規定は、どちらも守る必要があり、片方だけで足りるわけではありません。ISC2 の規定を持つ者は、勤め先に雇われていても、認定の条件としてこの規定に縛られます。

組織の規定が ISC2 の規定より厳しければ、厳しい方に従います。組織の規定や上司の指示が ISC2 の規定に反するなら、規定を理由に断り、規範 I と II を守る方を選ぶほかありません。利益相反（たとえば自分の親族の会社を、公平な選定なしに委託先に選ぶこと）に気づいたら、自分の判断で黙って進めず、申告して判断を仰ぎます。不正を知った時の報告義務も、組織の報告経路に従って果たします。

たとえば、委託先の選定会議で、候補の 1 社が自分の親族の経営する会社だと分かりました。黙って評価に加われば、公平さが疑われ、規範 II の「公正に」に反します。正しい動きは、利益相反として上長や担当部署に申告し、その会社の評価と選定から外れることです。親族の会社が最も安く、技術的に優れていても、申告の義務は変わりません。申告した後の判断は、組織の規程に従います。

セキュリティの基本概念 [1.2]

機密性・完全性・可用性（CIA）

情報セキュリティの目標は、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の 3 つです。米国標準の FIPS 199 は、次のように定義します。[3]

SAMPLE

目標	定義	日本語版 PDF の訳
機密性	許可された者だけが情報にアクセスし、開示できるよう制限し、個人情報や企業秘密を守る	機密保持
完全性	情報が不正に変更・破壊されないよう守る。真正性と否認防止を含む	整合性
可用性	必要な時に、適時かつ確実に、情報にアクセスして使える	可用性

公式の日本語版 PDF は完全性を「整合性」と訳しますが、同じ語であり、本文では完全性と書きます。

FIPS 199 は、CIA の損失が与える影響を 3 段階に分けます。[4]

- 低: limited な悪影響（主な機能は果たせるが、効果は目に見えて落ちる）
- 中: serious な悪影響
- 高: severe または catastrophic な悪影響

1 つのシステムに複数の情報の種類がある時は、機密性、完全性、可用性のそれぞれで、最も高い値（high water mark）を、そのシステムの値にします。たとえば、情報 A が（機密性 低、完全性 中、可用性 低）、情報 B が（高、低、中）なら、システムは（高、中、中）になります。

損なわれたものを見分ける

見分けは、起きたことが「読まれた」「変わった」「使えない」のどれかで決まります。

SAMPLE

起きたこと	損なわれたもの	例
許可のない人に読まれた・見られた	機密性	顧客名簿の流出、メールの誤送信、肩越しののぞき見、公開 AI サービスへの社内資料の貼り付け
許可のない変更や意図しない変更が入った	完全性	振込先の書き換え、ログの改ざん、入力ミスによるデータ破損、AI の学習データへの混入
必要な時に使えなかった	可用性	DoS 攻撃、停電、機器の故障、ランサムウェアでファイルが開けない

ランサムウェアは、ファイルを暗号化されて使えなくなる点で可用性の損失です。攻撃者がデータを持ち出して公開すると脅す二重の恐喝では、機密性の損失も見逃せません。書き換えが誤操作でも悪意でも、変わったという事実は完全性の損失です。

複数の目標が同時に損なわれる場面もあります。従業員が顧客データを誤って公開フォルダに置いてしまった場合は、機密性の損失です。そのファイルを別の人が編集して数値を書き換えれば、完全性も損なわれるので、機密性だけの問題ではありません。サーバーが止まって顧客が閲覧できなければ、可用性の損失です。問題文が「主に損なわれた」と聞く時は、出来事の中心を 1 つだけ選びます。「すべて」と聞く時は、目標ごとに判定しなければなりません。原因の善悪では分けません。

守る側の管理策も、損なわれる性質ごとにほぼ決まります。機密性は暗号化・アクセス制御・分類、完全性はハッシュ・デジタル署名・変更管理・入力値の検証・職務の分掌、可用性は冗長化・バックアップ・無停電電源装置・DDoS 対策です。

SAMPLE

説明責任と監査証跡

説明責任（Accountability）は、実体の行為をその実体にだけ一意にたどれる性質で、誰がいつ何をしたかを本人に結びつけて追えることを指します。[5] 実現には 4 つの段階が連なります。

1. 識別: 誰であるかを名乗らせる（ユーザー ID）。
2. 認証: 名乗りが本物だと確かめる（パスワード、トークン、生体）。
3. 認可: 本人に許す操作を決める（権限）。
4. 記録（accounting）: 行為を監査ログに残す。

どれか 1 つでも欠けると、誰がやったか決まりません。共有アカウント（1 つの ID を複数人で使う）は、識別の段階で個人に結びつかないため、説明責任を壊します。管理者の操作を記録し、通常の作業用アカウントと管理用アカウントを分けるのも、誤用を見つけやすくする工夫です。[6] 監査証跡（audit trail）は、ログ自体が書き換えられないよう保護しなければ、証拠として使えません。

たとえば、データベースの管理者アカウント「admin」を 3 人で共有している組織で、顧客の記録が消され、ログには admin による削除が残っている場合を考えます。誰が消したかは、ログを見ても決まりません。識別が個人に結びつかず、説明責任が果たせない状態です。対策は、人ごとに個別のアカウントを発行し、管理者の権限は必要な時だけ昇格させ、操作を個人のアカウントに記録することです。パスワードを複雑にしても、共有そのものは解消しません。

否認防止

否認防止（Non-repudiation）は、ある人が実行した行為を、後から「やっていない」と否定できないようにする性質です。[7] 手段はデジタル署名と、改ざんで

SAMPLE

きないログです。デジタル署名は、署名者の身元の認証と、データが改ざんされていないことの確認に使います。[8]

完全性との違いが問われます。ハッシュは、データが変わっていないこと（完全性）を示しますが、誰が作ったかは示しません。攻撃者が内容を書き換えてハッシュも計算し直せるからです。共通鍵で作る認証コード（MAC）も、鍵を持つ双方が同じ値を作れるため、どちらが作ったかを第三者に証明できず、否認防止にはなりません。署名者だけが持つ秘密鍵で作るデジタル署名だけが、本人性まで示せます。完全性は「変わっていない」、真正性は「作った者が本物」、否認防止は「本人が後で否定できない」と並べて覚えます。

否認防止が成り立つ条件は、署名の鍵が本人だけに管理されていることと、記録が信頼できる形で残ることです。秘密鍵を共有していたり、管理者がログを書き換えられたりすれば、否認防止は成り立ちません。

たとえば、取引先が「その発注書は送っていない」と主張している場合を考えます。発注書のファイルが、保管してあったハッシュ値と一致すれば、内容が変わっていないことは示せます。しかし、取引先が送ったことは示せません。必要なのは、取引先の秘密鍵で署名された発注書か、取引先の本人確認を経た送信の記録です。完全性だけでは、否認を防げません。

最小特権と知る必要性

最小特権（Least privilege）は、業務に必要な最小限の権限だけを与える原則です。[9] 利用者だけでなく、プロセスにも当てはまります。必要がなくなった権限を、放置してはいけません。異動したのに前の部署の権限が残っている状態は、最小特権の違反です。

知る必要性（need to know）は、権限があっても、その情報を業務で知る必要がなければ見せない考え方で、最小特権と組み合わせます。最小特権が「どの

SAMPLE

操作を許すか」の幅を絞り、知る必要性が「どの情報を見せるか」の幅を絞ります。たとえば経理の部長は、経理の全システムを操作する権限があっても、人事の評価資料を見る必要はありません。

特権の時限付与は、管理者権限を常時持たせず、作業の間だけ与えて終われば戻す運用です。承認を経て、期間を切って昇格させ、操作を記録します。管理者権限を常時持たせたままでは、アカウントが乗っ取られた時の被害を抑えられません。

職務の分掌（SoD）

職務の分掌（公式の範囲の英語は Segregation of Duties、NIST SP 800-53 の AC-5 は Separation of Duties、略して SoD）は、重要な業務を複数の担当者に分け、1 人の不正や過失で完結しないようにする原則です。[9] 公式の日本語版は「業務の分掌」と書きます。分けた担当者が示し合わせる（共謀、collusion）と破れますが、共謀がなければ不正のリスクは下がります。

- 二人制御（two-person control）：重要な操作を、2 人が同時に関わって初めて実行できるようにする（金庫の鍵を 2 人が別々に持つ、承認者と実行者を分ける）。
- 職務の交代（job rotation）：同じ業務を長く同じ人に任せず、担当を替える。不正が続けにくくなり、前任の不正が後任に見つかる。
- 強制休暇（mandatory vacation）：一定期間、業務から離れさせる。その間に代理が処理して、不正の痕跡を見つける。

SoD は不正の予防、職務の交代と強制休暇は不正の発見に効きます。セキュリティ担当者がアクセス制御を管理し、監査機能まで管理しない、という分け方も SoD の例です。[9]

SAMPLE

経理担当者が、新しい取引先の登録と、その取引先への支払い承認の両方の権限を持っている場合を考えます。架空の取引先を登録して自分で承認すれば、1 人で不正が完結します。この場合、登録と承認を別の人に分けるのが正解で、パスワードを強くしても、操作ログを増やしても、不正は予防できません。ログを増やす対策は発見、分掌は予防、と機能も違います。すでに分掌が難しい小さな組織なら、承認の記録を上長が定期的に見直して補います（補償コントロールの考え方です）。

別の場面です。営業部から経理部へ異動した従業員が、営業のシステムの権限を持ち続けています。経理の権限も加わり、請求書の作成と入金の消し込みの両方が 1 人でできる状態です。最小特権の違反で、権限の積み上がりが分掌も崩しています。異動の時に、前の部署の権限を棚卸しして外す手順が、組織にありません。対策は、定期的な権限の見直しと、異動を起点にした権限の変更です。強制休暇を入れていれば、その間に代理が処理して、不正の痕跡に気づける場合もあります。

AI を使う仕組みの完全性

AI を使う仕組みでも、CIA は同じ枠で考えます。ここで追加される論点は、アルゴリズムの完全性（algorithmic integrity）で、AI の出力が信頼でき、改ざんされていないことを指します。[10]

完全性への攻撃の代表が、学習データへの細工（ポイズニング）です。学習データに不正な例を混ぜてモデルの判断を歪める攻撃で、学習のどの方式でも成り立ちます。[11] 守りは、学習データの出どころの管理、データへの書き込み権限の最小化、モデルとデータの変更の記録、出力の監視です。機密性の面では、公開 AI サービスに社内の機密を入力すると、情報が外部に出ます。可用性の面では、AI の判断に業務を頼る場合、AI の停止がそのまま業務の停止に

SAMPLE

ならないよう、備えなければなりません。モデルの更新が出力を変えることも多いので、更新は変更管理の対象にします（1.6 で扱います）。

たとえば、不正検知の AI の学習データに、攻撃者が「正常」と偽ったデータを少しずつ混ぜているとします。モデルは、その種の不正を見逃すようになります。入口はデータで、損なわれたのは AI の判断の信頼、つまりアルゴリズムの完全性で、機密性や可用性の問題ではありません。対応は、モデルの更新を止めて前の版に戻し、学習データの出どころを調べることです。

セキュリティコントロールの種類と選び方 [1.3]

セキュリティコントロール（管理策）は、実現の手段で 3 種類に分けます。この分類は「何で実現するか」を問い、後で扱う予防・発見などの分類は「何をするか」を問うので、2 つの軸は別物です。

技術的コントロールと物理的コントロール

技術的コントロール（technical controls）は、暗号化、アクセス制御、境界の保護、ログの記録と監視など、システムの機能で実現する管理策で、SP 800-53 では AC（アクセス制御）や AU（監査）などのファミリーに整理されます。[12]

管理策	働き	読み方
ファイアウォール	決めた規則で通信を通す・止める	境界で通信を選ぶ。通信の中身の悪意までは見ないものも多い
侵入検知システム（IDS）	通信やホストの動きを監視し、不審な動きを知らせる	見つけて知らせる。自分では止めない（止めるのは IPS）

SAMPLE

管理策	働き	読み方
アクセス制御リスト（ACL）	誰が、または何が、どの資源にどの操作をしてよいかの一覧	許可と拒否の表。上から順に評価するものが多い

ログの記録は、システムが出来事を記録して後から追えるようにするので、物理的管理策や管理的管理策には入りません。

物理的コントロール（physical controls）は、施錠、入退室管理、監視カメラ、フェンス、守衛など、物理的に守る管理策です。マントラップ（mantrap）は、2組の連動するドアの間の小さな空間です。1 枚目のドアが閉まってから 2 枚目が開くので、正規の人の後ろに付いて入る共連れ（tailgating）を防ぎます。SP 800-53 は同じ仕組みをアクセス制御の前室（vestibule）と呼び、共連れ（piggybacking）の防止を目的に挙げます。[13] 入口に守衛、鍵、バッジ、マントラップを重ねるように、物理の管理策も 1 層には頼りません。

管理的コントロールとポリシーの階層

管理的コントロール（administrative controls）は、方針、手順、教育、採用前の身元確認など、人とルールで実現する管理策です。公式の日本語版 PDF は「行政的コントロール」と訳しますが、一般の呼び名は管理的コントロールです。教育・研修は、技術でなく人とルールで守る管理的コントロールの代表です。

文書は、抽象から具体へ階層を成し、上位の文書を下位の文書が覆すことはありません。

文書	内容	守る義務
ポリシー（方針）	何を守るかを決める。経営が承認する高い水準の宣言	必須

SAMPLE

文書	内容	守る義務
スタンダード（標準）	方針を満たす具体的な水準（例: パスワードは 14 文字以上）	必須
ベースライン	最低限そろえる設定や構成の基準	必須
手順（procedure）	作業の具体的な順序	必須
ガイドライン	推奨や助言。従わなくても違反にはならない	任意

階層は、方針（何を守るか）、標準（守る水準）、手順（やり方）の順に具体化します。[14] 迷った時は、必須か任意か、抽象か具体かの 2 つで見分けるしかありません。経営が決める「何を」は方針、守る水準は標準、実際の操作の順序は手順で、3 つを取り違えてはいけません。

たとえば、「リモート接続には多要素認証を使う」は、何を守るかを決める文で、方針にあたります。「多要素認証は、パスワードとハードウェアトークンの組み合わせとし、トークンは 12 か月ごとに更新する」は標準です。「トークンを紛失した時の連絡先と、再発行の操作の順序」は手順です。「パスフレーズにすると覚えやすい」という助言は、ガイドラインです。ベースラインは、サーバーの OS に最低限そろえる承認済みの設定のことで、方針でも標準でもありません。

法令は外から課される義務で、守らなければ罰則や賠償が生じます。契約の条項は、契約相手との約束であり、守らなければ賠償や取引停止になります。規格（ISO/IEC 27001 など）は、採用すると決めた時に守る基準です。ISO/IEC 27001 は、情報セキュリティマネジメントシステム（ISMS）の要求事項を定めた国際規格で、認証の対象になります。ISO/IEC 27002 は、管理策の手引き

SAMPLE

（ガイダンス）で、認証の対象ではありません。[15] 要求事項（27001）と手引き（27002）の取り違えが、よく問われます。

コンプライアンス要件の評価

コンプライアンス要件の評価（assessing compliance requirements）は、組織に課される要件を拾い、管理策に結びつける作業です。次の順で進めます。

1. 適用される法令、契約、業界規格、社内規程を洗い出す（個人情報保護、決済カードの規格、取引先との契約など）。
2. 要件を管理策の言葉にそろえる（「アクセスを制限する」「ログを 1 年残す」）。
3. 今の管理策と比べ、足りない所（ギャップ）を見つける。
4. 足りない所に管理策を足すか、できない時は代替の管理策を置き、記録を残す。

要件の出どころによって、守れなかった時の結果が違います。法令違反は罰則、契約違反は賠償や取引停止、社内規程の違反は処分です。優先は、法令、契約、社内の順で、社内の決めごとが法令に優先することはありません。

たとえば、取引先との契約に「アクセスログを 1 年間保存する」とありますが、社内の標準は 90 日です。これはギャップで、契約違反の状態です。標準を 1 年に改め、保存容量を確保し、ログ基盤の設定を直して、直した証拠を残します。標準を直さずにログ基盤だけ延ばしても、文書と実態の食い違いは消えません。

デューケア（due care）は、組織が合理的な保護策を実際に実行することで、「やるべきことをやる」側です。デューディリジェンス（due diligence）は、リスクを事前に調べて確かめる活動で、「調べる」側です。[16] クラウドの委託先を選ぶ時、契約前に委託先の管理策を調べるのがデューディリジェンスで、契約後

SAMPLE

に管理策を実際に運用し確認し続けるのがデューケアです。調べただけで実行しなければ、デューケアが欠けています。

定期的な監査とレビュー

管理策は、置いて終わりではありません。定期的な監査とレビューで、置いてあるか（設計）、動いているか（運用）、効いているか（有効性）を確かめます。

種類	実施者	目的・特徴
内部監査	自組織の監査部門など	自己点検。改善が目的で、日常に近い
外部監査	組織の外の第三者	独立した評価。認証の取得や取引先への保証に使う

どちらも、監査する人が、監査される業務から独立していることが条件です。自分が設定した管理策を自分で監査しては、独立性が保てません。結果は発見事項（findings）として記録し、是正の担当者と期限を決めて、完了まで追います。

たとえば、内部監査で、退職者のアカウントが 30 日たっても無効になっていないという発見事項が出ています。担当は人事部門と IT 部門で、期限と是正の内容（退職日に自動で無効化する）を決めます。期限が来たら、監査部門が是正を確認して、完了を記録します。是正が遅れる時は、リスクとして経営層に報告しなければなりません。

管理策の有効性は指標で測ります。現行の SP 800-55 Vol.1（2024 年 12 月）は、指標を実装（置いたか）、有効性（狙いどおりに効いているか）、効率（どれだけ速く結果を返し、問題に対処できたか）、影響（ビジネスにどう効いたか）の 4 種類に分けます。取り下げられた Rev.1 は、有効性と効率を 1 つにまと

SAMPLE

めた 3 種類でした。[17] 継続的な監視（ISCM）は、脆弱性と脅威を常に把握し、リスクの判断を支える活動で、年 1 回の監査の間を埋めます。[18]

管理策の選び方

管理策は、リスクに見合うものを選びます。費用が守る資産の価値や期待される損失を超える管理策は、置く意味がありません。簡単な計算で確かめます。

項目	値
1 回の損失額（SLE）	100 万円
年間の発生率（ARO）	0.4（2.5 年に 1 回）
年間の期待損失（ALE = SLE × ARO）	40 万円
管理策を置いた後の ARO	0.1
置いた後の ALE	10 万円
管理策の年間の費用	15 万円

減る損失は 40 − 10 = 30 万円です。費用 15 万円を引いた正味の効果は 15 万円で、置く価値があります。減る損失が費用を下回る管理策は、費用対効果が悪いので採用しません。

もう 1 つの軸は多層防御（defense in depth）で、1 つの管理策に頼らず、物理、技術、管理の層を重ね、1 つが破られても次の層が止めます。同じ種類の管理策を 2 つ重ねるより、異なる種類を重ねた方が、同じ弱点で同時に破られにくくなります。

小さな医療法人が、患者の記録を扱う端末を入れた部屋への侵入を心配しています。予算に限りがあり、リスクの評価は高く、すべてを一度には置けません。ドアの電子錠だけなら技術と物理の 1 層です。そこに入退室の記録のレビ

SAMPLE

ュー（管理）と、持ち出しを禁じる規程と研修（管理）を重ねれば、層が増えます。高価なマントラップは、費用が見合わないなら採用しません。リスクに見合う別の管理策で下げ、選ぶ時はリスクの高さと費用の両方を見ます。

5 つの機能による分類と補償コントロール [1.4]

抑止・予防・発見・修正・補償

機能（何をするか）での分類は 5 つです。

機能	働き	例
抑止（Deterrent）	思いとどまらせる。実際には止めない	警告の看板、監視中の表示、解雇などの罰則の周知
予防（Preventative）	起きる前に止める	施錠、ファイアウォール、アクセス制御、職務の分掌、暗号化
発見（Detective）	起きたことに気づく	監査ログの確認、IDS、監視カメラの録画、入退室の監視
修正（Corrective）	起きた後に元へ戻す	バックアップからの復元、パッチの適用、ウイルスの除去、インシデント対応
補償（Compensating）	本来の管理策が置けない時の代わり	後で扱う

SP 800-53 の中では、入退室の許可を出入口で強制する PE-3 と、アクセスの許可を方針に従って強制する AC-3 が予防に当たります。入退室を監視して物理インシデントを見つける PE-6 は発見です。[19] 監視で見つけた問題に是正の行動を取るのは修正の機能で、予防や発見ではありません。

SAMPLE

違いは時点で見分け、起きる前に作用するなら抑止か予防、起きた最中か後に気づくなら発見、起きた後に戻すなら修正です。抑止と予防の違いは、行為者の心理に働くか、物理的・論理的に実際に止めるかです。警告の看板は抑止で、鍵のかかったドアは予防です。

同じ機器が場面で別の機能になる

分類は機器ではなく、働きで決まります。

機器	機能	理由
監視カメラ（見える位置・録画の表示あり）	抑止	映っていると知らせ、思いとどまらせる
監視カメラ（録画を後で確認する）	発見	起きたことを記録し、後から見つける
ログ	発見	起きたことを記録する。ログだけでは止めない
ファイアウォールの遮断	予防	通信を実際に止める
IDS	発見	見つけて知らせる。止めるのは IPS で、IPS は予防に近い
バックアップ	修正	損なわれたデータを元に戻す

同じカメラでも、ダミーのカメラは抑止にだけなり、発見はしません。問題文が「思いとどまらせる」と言えば抑止、「後から調べられる」と言えば発見です。

ある倉庫に監視カメラが付き、入口に「録画中」と掲示されています。夜間に侵入があり、翌朝の録画から犯人が特定された場合を考えます。掲示は侵入を思いとどまらせる抑止で、録画から特定できたのは発見です。この場合、カメラ

SAMPLE

は抑止と発見の両方の機能を持ちますが、侵入そのものは止まっていないので、予防は働いていません。再発の防止には、扉の補強（予防）を足さなければなりません。

実現の手段と機能の組み合わせ

1.3 の 3 種類（技術・物理・管理）と 5 つの機能は、別の軸で、1 つの管理策は、手段と機能の両方を持ちます。

管理策	手段	機能
ファイアウォールの遮断	技術的	予防
暗号化	技術的	予防
IDS	技術的	発見
バックアップからの復元	技術的	修正
施錠された扉	物理的	予防
録画を確認する監視カメラ	物理的	発見
警告の看板	物理的	抑止
セキュリティ教育	管理的	予防
方針違反への懲戒の周知	管理的	抑止
ログの定期レビュー（人が読む作業）	管理的	発見
インシデント対応手順	管理的	修正

問題が「技術的か」と聞く時は手段を、「予防的か発見的か」と聞く時は機能を見ます。ログの記録は技術的で発見、そのログを人が毎週読む作業は管理的で発見と、同じ発見でも手段が変わります。

SAMPLE

補償コントロール

補償コントロール（compensating controls）は、標準の管理策を置けない時に、同等かそれに近い保護を与える代わりの管理策です。[20] 管理的、運用的、技術的のどの種類でも構いません。補償と呼べる条件は、本来の管理策が置けない正当な理由があること、本来の管理策の狙いを満たす程度に保護が働くこと、その内容を文書にして残し、定期的に見直すことです。

たとえば、古い制御機器が、パスワードの複雑さの規則を満たせない場合を考えます。本来は機器を更新したいのですが、すぐにはできません。代わりに、その機器を専用のネットワークに隔離し、接続できる端末を絞り、操作を記録して毎週見直します。こうして、標準の管理策と同等に近い保護を別の手で与えます。カード情報を扱う決済の基準（PCI DSS）にも、同じ考え方があります。基準をそのまま満たせない時に、代わりの管理策で意図を満たし、理由と効果を文書にします。

補償は、本来の管理策を省く言い訳ではありません。置けない理由と、代わりの管理策で本来の狙いを満たせる根拠を文書に残します。定期的に見直し、本来の管理策を置けるようになったら置き換えを検討することも欠かせません。

管理策の文書化と維持

管理策は台帳（管理策の一覧）で管理し、各管理策に、目的、機能（予防・発見など）、種類（技術・物理・管理）、担当者、対象の資産、確認の頻度、直近の確認結果を書きます。台帳があれば、予防しかなく発見がない領域や、担当者のいない管理策を見つけられます。

たとえば、ファイル共有の行を見ると、予防の管理策（アクセス制御）はあっても、発見の管理策（アクセスログの確認）が空欄で、確認の担当者は退職済みです。この場合は、発見の管理策を足し、新しい担当者と確認の頻度（毎週な

SAMPLE

ど）を決め、台帳を更新します。足した後の見直しで、実際に確認の記録が残っていなければ、管理策は動いていません。

維持の作業は 3 つです。有効性を指標で測る、リスクや環境が変わった時に見直す、不要になった管理策を整理する。SP 800-53 の管理策ファミリーは、略称と番号（AC-2 など）で整理されており、台帳を作る時の分類に使えます。[19] 主な略称は AC（アクセス制御）、AT（意識向上と研修）、AU（監査と説明責任）、CM（構成管理）、PE（物理と環境）です。

資産管理のライフサイクル [1.5]

資産（ハードウェア、ソフトウェア、データ）は、手に入れる前から捨てた後まで、同じ流れで管理します。

段階	主な仕事
プロセス・計画・設計・開始（process, planning, design and initiation）	必要性と要件を決め、セキュリティ要件も最初に書く
開発／獲得（development / acquisition）	作る場合は安全な開発、買う場合は調達の審査
インベントリーとライセンス（inventory and licensing）	台帳に載せ、使用の権利を確かめる
実施と評価（implementation / assessment）	導入し、本番に出す前に設定と安全性を評価する
運用・保守・サポート終了（operation / maintenance / EOL）	パッチ、監視、サポートが切れた資産の扱い
アーカイブと保持（archival and retention）	要件に従って保管する
廃棄と破棄（disposal and destruction）	データを復元できない状態にして処分する

SAMPLE

流れの順は、計画、取得、導入、運用保守、廃棄です。サポートが切れた部品は、置き換えます（SP 800-53 の SA-22）。[21] 要件は最初の段階で決めるほど安く済み、運用の段階で後から足すほど高くつきます。問題で「どの段階で」と問われたら、要件の定義は計画と設計の段階です。

開発と獲得の段階のセキュリティ

自分で作る場合は、安全な開発の枠組みを使います。SP 800-218（SSDF）は、実践を 4 つのグループに分けます。

- 組織の準備（PO: Prepare the Organization）
- ソフトウェアの保護（PS: Protect the Software）
- 安全なソフトの作成（PW: Produce Well-Secured Software）
- 脆弱性への対応（RV: Respond to Vulnerabilities）

[22] DevSecOps は、開発（Dev）と運用（Ops）の流れの中に、セキュリティの確認を最初から組み込む考え方です。出荷の直前に検査するのでなく、コードを書く時、ビルドの時、導入の時に、自動のテスト（コードの解析、依存ライブラリの脆弱性の検査、設定の検査）を走らせます。見つかる時期が早いほど、直す費用は小さくなります。

試験は 3 つに分けます。

- 機能の試験: 仕様どおりに動くかを見る。
- セキュリティの試験: 悪意のある入力や権限の突破に耐えるかを見る。
- 受け入れ試験: 依頼した側が要件を満たすかを確かめる。

試験は本番と分けた環境で行い、本番の実データをそのまま使いません。

SAMPLE

買う場合は、調達の時点で要件を契約に入れます。確認する内容は次の 5 つです。

- 納入物のセキュリティ機能
- 脆弱性が見つかった時の修正の約束
- サポートの期間
- データの扱い
- 監査への協力

供給元が弱ければ、自社の守りも弱くなるので、委託先と部品の出どころを審査します。

たとえば、外部の会社に顧客管理アプリの開発を任せる時、契約に、脆弱性の検査と修正の約束、ソースコードの引き渡し、サポート期間が書かれていなければ、納品後に見つかった欠陥の修正費用を、自社が負うことになります。納品の前に、セキュリティの試験の結果を受け入れの条件にし、開発の途中でも、コードの検査の結果を共有してもらいます。調達の時点で要件を契約に入れなければ、後から求めても受け入れてもらえません。

資産の目録とライセンス

資産目録（インベントリー）は、守るべき機器とソフトを正確に把握する出発点で、SP 800-53 の CM-8 は、目録がシステムを正確に反映し、すべての構成部品を含めることを求めます。[21] CIS Controls でも、最初の 2 つが企業の資産の目録とソフトウェアの目録です。台帳にない機器（持ち込みや無断で導入された端末）には、パッチも監視も届きません。

ライセンスは、ソフトウェアを使う権利の条件です。

SAMPLE

種類	特徴	主なリスク
クローズドソース（商用）	提供元が条件を定める。台数、ユーザー数、用途に制限がある	契約を超えた利用（台数の超過）で、賠償や監査の指摘を受ける。修正は提供元の対応を待つ
オープンソース	ソースが公開される。無料でも、再配布などに条件が付く	条件を守らない利用（ライセンス違反）、部品の脆弱性に気づかず放置する、保守が止まった部品を使い続ける

ライセンスの違反は法的なリスクで、海賊版のソフトを使えば、権利の問題に加え、マルウェアを含む可能性も高まります。台帳には、ソフトの名前と版、ライセンスの種類と数、期限、担当者を載せ、実際の導入数と照合します。オープンソースの部品も、脆弱性の情報を追う対象なので、無料だからと台帳から外してはいけません。保守が止まった部品は、新しい脆弱性が見つかっても修正が出ず、知らせも来ないので、気づくのも遅れます。

たとえば、台帳には 50 本の購入記録がある設計用ソフトが、実際には 62 台に入っている場合です。超過した 12 台はライセンス違反で、監査で指摘されると、追加購入や賠償が必要になりかねません。反対に、購入したのに使われていない本数が見つかれば、更新の時に減らして、費用を下げられます。台帳と実際の導入数の照合は、リスクの管理と費用の管理の両方に効くので、省けません。

データの分類・ラベル・所有者と管理者

データの分類は、情報の重要度に応じて扱いの水準を決める仕組みで、組織ごとに公開、社内限り、機密、極秘のような段階を定めます。FIPS 199 の方式では、情報の種類ごとに CIA の損失の影響を低・中・高で見積もります。[4] 分類

SAMPLE

が決まれば、暗号化、アクセスの範囲、保管と廃棄の方法が、分類ごとに決まります。

ラベル付け（マーキング）は、分類や取り扱いの条件を、文書や媒体に表示して、扱う人に分かるようにする作業です。表示がなければ、扱う人は水準を知らず、守れません。

役割は 2 つに分かれます。

役割	内容	決める・やること
オーナー（所有者）	データの責任を負う側（多くは事業部門の長）	分類を決める。アクセスを許す人を決める。
カストディアン（管理者）	データを預かり、保護を実際に運用する側（多くは IT 部門）	決められた分類に従い、バックアップ、アクセスの設定、暗号化を運用する

分類を決めるのはオーナーで、カストディアンではありません。カストディアンは決められた水準を実装します。データを扱う一般の利用者（ユーザー）は、決められた規則に従います。

たとえば、人事部が持つ給与データを、IT 部門のバックアップ担当者が毎晩複製しています。給与データの分類を「機密」と決め、アクセスを許す人を決めるのは、人事部の長（オーナー）です。バックアップ担当者（カストディアン）は、決まった分類に従って暗号化と保管を運用し、分類を勝手に下げません。「重要でなさそうだから」と保管の暗号化を外すのは、権限の逸脱です。

データマスキングは、本物のデータを、見えない、使えない形に置き換える方法です（例: カード番号の一部を伏せる）。テストや画面表示で個人情報を守ります。個人を識別できなくなるまで個人情報を取り除く非識別化（de-identification）も、同じ目的の手法です。[23]

SAMPLE

サポート終了（EOL）の資産

サポートの終わった製品は、修正が出ません。新たな脆弱性が見つかっても、直す手段がなくなります。対処の順は 3 つです。

1. 置き換える（最優先）: サポートされる版や製品へ移す。
2. 置き換えられない間は隔離する: 専用のネットワークに閉じ、接続元と通信を絞り、監視する。補償コントロールの考え方です。
3. 延長サポートを買う: 提供元が有償で修正を続ける場合に限る。期間が限られるので、移行の計画と組み合わせる。

どの場合も、残すという判断をリスクとして記録し、承認を得ます。

工場の制御用 PC が、サポートの切れた OS で動いています。装置の認定の都合で、OS の更新が 2 年先にしかできません。インターネットから隔離し、接続できる端末を限り、USB 媒体の使用を禁じ、通信を監視して、更新までの暫定の補償とします。何もせずに残す、または認定を無視してすぐに更新する、のどちらも正解になりません。

アーカイブと保持の要件

保持（retention）は、データを残す期間の決まりです。法令や契約が最短の期間を定めることがあり、それより短く消すと違反になります。長く残しすぎるのにもリスクがあります。保管するデータが多いほど、漏えいした時の被害と、訴訟での開示の負担が大きくなります。保持期間を、必要な期間より長く設定してはいけません。過ぎたデータは廃棄します。

アーカイブは、普段使わないデータを、長期の保管へ移すことです。移した後も、機密性を保ち、必要な時に取り出せることが条件です。暗号化したアーカイブは、鍵も同じ期間保管します。鍵を先に失えば、データは取り出せません。媒体や形式の寿命も考え、読める形に移し替える計画を持ちます。訴訟や調

SAMPLE

査の対象のデータは、保持の期間が過ぎても、法的な保全（legal hold）で消去を止めます。

たとえば、7 年間の保存が法令で求められる記録を、5 年で消した場合は、保持の不足で違反になります。保存の期限が 3 年の業務記録を、10 年残していた場合は、保持の過剰です。期限が切れた個人情報が漏えいした時は、残していたこと自体が責められかねません。保持期間表（種類、期間、根拠、廃棄の方法）がなければ、判断の根拠がありません。保持期間表を作り、期限の来たものを自動で廃棄する運用なら、取りこぼしません。

媒体のサニタイズと破壊

廃棄や再利用の前に、媒体のデータを復元できない状態にする作業が、サニタイズ（sanitization）です。SP 800-88 の Rev.2（2025 年 9 月）が現行で、Rev.1（2014 年 12 月）に代わりました。[24] 方法は 3 つです。

方法	内容	媒体の状態
Clear（消去）	通常の読み書きの命令で新しい値を書き込む、または工場出荷の状態に戻す。簡単な復元に耐える	再利用できる
Purge（除去）	最新の研究室の技術でも復元できない状態にする	再利用できる可能性のある状態に残す
Destroy（破壊）	研究室の技術でも復元できず、媒体も再利用できない	再利用できない

Clear は、紙には使えません。Purge も、紙には使えません。紙（hard copy）は破壊です。Purge の中の暗号化消去（cryptographic erase）は、データを暗号化していた鍵を消して、データを読めなくする方法で、すばやく済みます。ただし、強い暗号が使われていて、鍵が適切に生成・管理されていなければ、成り

SAMPLE

立ちません。クラウドの記憶領域では、利用者が物理媒体に触れないので、暗号化消去が唯一の選択肢になることがあります。

消磁（degauss）は、強い磁界で磁気媒体のデータを消します。SSD などのフラッシュ媒体には効きません。最近の高い保磁力の媒体には力が足りない消磁装置も多く、Rev.2 は消磁を Destroy の認められた手法とは扱いません。破壊の物理的な手段は、粉砕（disintegrate）、焼却（incinerate）、溶解（melt）、微粉砕（pulverize）、細断（shred）です。曲げる、穴を開けるといった手段は、一部が読み取れる状態で残るおそれがあります。

上書き（overwrite）は、磁気ディスクでは Clear の代表です。SSD やフラッシュは、予備の領域や書き込みの平準化（wear levelling）で、利用者が書き込める範囲に全データがないため、上書きでは消えきりません。複数回の上書きは、SSD で保護がほとんど得られない場合があります。磁気ディスクの古い慣習をそのまま SSD に使うと、データが残ったままなのに消えたと思い込みかねません。

方法は、データの分類（低・中・高）、媒体の種類（磁気、フラッシュ、紙、クラウド）、再利用の予定の 3 つを見て決め、コストや環境への影響も考えます。

場面	選ぶ方法
内部で再利用する、機密の低いデータの PC	Clear
社外へ出す、機密の高いデータの SSD	Purge（機器の標準のサニタイズ命令、暗号化消去）、または Destroy
故障した、機密の高いデータの HDD	Destroy（機器が動かず Clear や Purge が効かないため）
紙の書類	Destroy（細断など）
クラウドの記憶領域	暗号化消去（鍵の破棄）

SAMPLE

退職者が使った、機密の高いデータの入った SSD 搭載のノート PC を、他部署で再利用する予定です。ファイルを削除して初期化する、または OS の標準のフォーマットだけでは、データは残ります。機器の標準のサニタイズ命令か暗号化消去による Purge を選びます。再利用の予定があるので、Destroy は選びません。Purge を適用した後で、結果を検証し、記録を残します。

検証と記録では、実施した日、担当者、媒体、方法、検証の結果を、サニタイズの証明書（certificate of sanitization）に書きます。[24]

変更管理と構成管理 [1.6]

変更管理の流れ

変更管理（change management）は、無秩序な変更が障害や脆弱性を生むのを防ぎ、いつでも元に戻せるようにする仕組みです。[25] 手順は次のとおりです。

1. 要求: 変更の理由、内容、対象、希望の日を記録する。
2. 影響の分析: セキュリティと運用への影響を調べる。
3. 承認: 権限のある者や委員会が可否を決める。
4. 試験: 本番とは別の環境で動作と安全性を確かめる。
5. 実施: 計画した時間帯に、手順どおりに適用する。
6. 検証: 狙いどおりに動き、管理策が損なわれていないか確かめる。
7. 記録と見直し: 結果を記録し、必要なら計画を直す。

順序は固定で、承認の前に影響を分析し、実施の前に試験します。試験と承認を飛ばして本番に入れると、障害や脆弱性の原因になります。SP 800-53 の CM-3 は、構成の管理対象の変更を、セキュリティとプライバシーの影響分析を明示的に考えたうえで、承認または却下することを求め、管理対象にする変

SAMPLE

更の種類を決めて記録すること、変更の記録を決めた期間残すことも求めます。[25]

役割と責任・CAB・緊急変更

役割	責任
申請者	変更の理由と内容を提出する
変更諮問委員会（CAB: Change Advisory Board）	提案を審査し、承認か却下を決める。構成管理委員会（CCB）と呼ぶ組織もある
実施者	承認された手順どおりに適用する
試験担当	試験し、結果を記録する
業務の責任者	業務への影響を判断し、停止の時間などに合意する

役割は分けて持ち、申請者が自分の変更を自分で承認し、自分で適用する体制は、職務の分掌に反します。承認者と実施者を分ければ、誤りや不正が１人で通りません。

コミュニケーションも仕事です。影響を受ける利用者に、日時、影響、問い合わせ先を事前に知らせ、終わったら完了を知らせます。監査では、変更の記録（誰が、いつ、なぜ、誰の承認で変えたか）が証拠になります。記録のない変更は、承認された変更とは扱われません。

緊急変更は、障害や脅威への急な対応で、通常の流れを待てない変更です。簡略化した承認で先に実施し、後から正式に記録して事後の審査を受けます。簡略化しても、承認と記録を飛ばしません。緊急を理由に、承認なしの変更を常態化させると、管理が崩れます。緊急変更の割合を定期的に見て、通常の

SAMPLE

手順で間に合う変更が緊急として通っていれば、事後の審査の記録から原因を調べ、通常の変更へ戻します。

セキュリティ影響分析と切り戻し

セキュリティ影響分析（security impact analysis）は、変更を実施する前に、セキュリティとプライバシーへの影響を分析することです（SP 800-53 の CM-4）。分析するのは、セキュリティかプライバシーの責任を持つ者です。[25] 見る点は、変更が既存の管理策を弱めないか、新しい脆弱性や攻撃面を作らないか、データの流れや権限が変わらないかです。たとえば、ファイアウォールの規則を 1 つ足す変更が、ほかの規則と合わさって、意図しない通信を通す場合があり、単独では気づけません。

切り戻し（rollback）の計画は、変更が失敗した時に元の状態へ戻す手順です。承認の前に用意します。SP 800-53 は、切り戻しに備えて、前の版のベースライン構成を残すことを求めます（CM-2(3)）。[25] 戻せない変更は、試験の段階で追加の対策を決めておきます。

たとえば、深夜に適用したパッチで、業務システムが起動しなくなる場合を考えます。変更記録に、承認者、試験の結果、前の版のベースラインの保存場所が残っていれば、実施者は計画の切り戻し手順に従い、前の構成へ戻せます。復旧の後は、試験の環境が本番と違っていた点などを原因として記録し、次の変更の試験条件を直します。試験で見つからなかった理由の分析は、再発の防止に効くので、省けません。

管理者が、緊急の依頼を受けて、チケットを起こさずに、本番のファイアウォールに規則を足したとします。作業は成功しても、承認も記録もありません。これは無承認の変更で、正しい対応は、変更を緊急変更として遅れて記録し、事後の審査で承認するかどうかを決めることです。検知は構成の監視が担い、承認の流れだけでは見つかりません。

SAMPLE

構成管理（CM）

構成管理（configuration management、CM）は、システムの構成を把握し、承認された状態を保つ仕組みです。変更管理は変更を承認して流す手続きで、構成管理は構成の状態を記録して維持する活動であり、2 つは互いに支え合います。

用語	内容
構成項目（CI）	管理の対象の部品（サーバー、OS、ソフト、設定ファイル、文書）
ベースライン	承認された安全な設定の基準。ここから外れていないかを監視する
構成のずれ（drift）	実際の設定が、ベースラインから外れた状態。無承認の変更や設定の誤りで起きる
最小機能（least functionality）	必要な機能、ポート、サービスだけを有効にし、攻撃対象を減らす
CIS ベンチマーク	OS やクラウドなどの安全な設定について、合意に基づいてまとめた設定の指針

承認された変更は、次回の比較で「ずれ」にならないよう、ベースラインも更新します。CIS ベンチマークは出発点で、SP 800-53 の CM-6 は、設定を「運用上の要件に合う最も制限の強い状態」で定めて文書にするよう求めます。業務の要件と両立しない項目は調整し、調整を文書にして承認した設定がベースラインになるので、承認された調整は「ずれ」ではありません。ベースラインとの定期的な比較で、承認されていない変更を見つけます。[26]

たとえば、サーバーのベースラインでは SSH を鍵認証だけにしていますが、定期の比較で、あるサーバーはパスワード認証も有効になっていました。変更の記録はありません。これは構成のずれで、無承認の変更の疑いがあります。

SAMPLE

対応は、承認された設定へ戻し、誰がいつ変えたかをログから調べ、必要なら正式な変更として申請し直すことです。同じ変更が複数のサーバーにあれば、変更管理の手続きが守られていない可能性も調べなければなりません。

機械学習モデルの更新と変更管理

機械学習（ML）のモデルの更新も、再学習するたびに出力が変わるので、変更管理の対象です。モデルの版、学習に使ったデータ、設定を記録し、再学習や入れ替えは、影響分析と承認と試験を経て本番に出します。入れ替え後は、出力の質と偏りを監視して、悪化したら前の版に戻します。本番で動くモデルの版もベースラインとして記録して定期的に本番の版と比べないと、承認を経ない入れ替えは後から確実には見つけられません。モデルは更新の周期が独特なので、コードの更新とは別の周期で、変更の計画を持ちます。[10]

セキュリティ意識向上とトレーニング [1.7]

意識向上・トレーニング・教育の違いと測り方

3 つの語は、目的が違います。

語	目的	例
意識向上（awareness）	気づかせる。全員が対象	ポスター、メール、ログイン画面の注意書き、短い動画
トレーニング（training）	業務に要る技能を身につけさせる。役割ごと	管理者向けの設定の実習、開発者向けの安全なコーディング
教育（education）	広く深い知識を与える。専門職の育成	学位の課程、資格の学習

SAMPLE

SP 800-50 の第 1 版は、この 3 つを学習の連続体として扱いました。2024 年の Rev.1 は、用語が現場で混乱するとして、ひとまとまりの学習プログラムと呼び、模擬演習、役割別、テーマ別の研修も含めて扱います。[27] 試験の選択肢では、3 つの違いは従来の定義で問われるので、気づかせるのが意識向上、技能を教えるのがトレーニング、広い知識を与えるのが教育、と覚えます。

対象を分けて、内容を合わせます。新入社員は入社時、全従業員は定期的に、管理職や委託先も含めて受けます（SP 800-53 の AT-2 は、管理職と委託先を含む利用者に、初回と定期の教育を求めます）。[28] 管理者、開発者、経営層には役割別の内容を足し、システムや脅威が変わった時にも随時更新します。

効果は、受講したかでなく、行動が変わったかで測ります。

指標	見るもの
受講率	全員が受けたか。最低限の確認
クリック率	模擬のフィッシングメールのリンクを押した割合。低いほどよい
報告率	不審なメールを報告した割合。高いほどよい
報告までの時間	受け取ってから報告までの短さ

行動の変化が目的なので、クリック率が下がっても、報告率が低いままなら、半分の成果です。押した人を罰するだけの運用は、報告をためらわせるので、よい結果になりません。報告しやすい仕組み（ワンクリックの報告ボタン、受付の窓口）がなければ、報告は集まりません。

たとえば、模擬のフィッシングで、クリック率が 30% から 10% に下がったとします。報告率は 5% のままです。クリックは減っても、不審なメールを報告する習慣は育っていません。本物の攻撃が来た時、押さずに済んだ人がいても、報

SAMPLE

告がなければ、ほかの人の被害は止まりません。次の施策は、報告ボタンを使いやすくすることと、報告した人を称えることです。

ソーシャルエンジニアリングとフィッシング

ソーシャルエンジニアリング（social engineering）は、人の心理を突いて、情報や操作を引き出す攻撃で、技術の突破でなく、人の判断の突破を狙います。利用される心理は、次の 4 つです。

- 権威（役員や IT 部門を名乗る）
- 緊急（今すぐ対応しないと止まる）
- 信頼（知り合いを装う）
- 親切（困っているので助けて）

手口	内容
フィッシング	信頼できる人や組織を装うメールで、リンクや添付ファイルを開かせる
スピアフィッシング	特定の個人や組織向けに、内容を作り込んだフィッシング
ホエーリング	経営層を狙ったスピアフィッシング
ビッシング（vishing）	電話による詐取
スミッシング（smishing）	SMS による詐取
プリテキスティング	偽の口実（調査員、取引先）で情報を聞き出す
ベイティング	餌（落とした USB 媒体、無料の配布物）で誘う
共連れ	正規の人の後ろについて、認証なしで入館する（1.8 で扱う）

SAMPLE

フィッシングは、信頼できる人や組織を装い、リンクや添付ファイルを開かせようとします。[29] 見分ける手がかりは、次の 4 つに絞れます。

- 差出人のアドレスの不一致
- 急がせる文面
- 不自然なリンク先
- 予期しない添付

疑わしい時は、開かず、リンクを押さず、決められた窓口に報告します。送り主への確認は、メールの返信でなく、別の経路（電話番号は、メールの記載でなく、登録済みのもの）で行います。

AI は文面を自然な日本語にし、個人向けの作り込みも安く大量にできるため、誤字や不自然な表現を見分けの手がかりにする教え方が古くなります。研修と手順書は、AI が書いた文面を前提に更新します。[10]

ソーシャルエンジニアリングへの備えは、訓練と仕組みの両方です。模擬のフィッシングメールを定期的に送り、押した人に学習の機会を返します。報告の窓口を整え、電話での本人確認の手順（コールバック）、物理の入退室の確認の手順を決めます。研修の内容は、CIS Controls の 14 番目の管理策（セキュリティ意識とスキルの研修）にも挙がっています。[30]

意識向上のコミュニケーション

意識向上の方法は、1 つに頼りません。次のような手段があります。[27]

- ポスターと社内の掲示板
- メールマガジン
- ログイン時の警告

SAMPLE

- 短い動画
- ロールプレイとサイバーレンジ（実習の環境）
- 模擬のフィッシング

同じ内容を、時期と媒体を変えて繰り返すと、記憶に残ります。月ごとにテーマを決め、事故や報道の事例を使い、自分の仕事に引きつけて伝えます。

卓上演習（テーブルトップ）

卓上演習（tabletop exercise）は、話し合いだけで進める演習です。関係者が会議室などに集まり、進行役が出す事故の筋書き（シナリオ）に、各自の役割で対応を話し合います。機器も資源も動かしません。[31]

進め方は、必要性の確認と日程、設計、資料づくり、実施、評価の順です。実施では、進行役が筋書きを少しずつ進め、状況の追加（インジェクト、たとえば「顧客データが外部に出ている」）を与え、参加者が判断と連絡を答えます。目的は、計画と役割の穴を見つけることで、参加者の採点ではありません。評価では、見つかった穴を行動項目にして、担当と期限を決め、計画を直します。

種類	内容
机上演習（tabletop）	議論が中心。機器を動かさない
機能演習（functional）	実際の手順の一部を、模擬の環境で動かし、役割と手順と資産を確かめる。範囲の広いものは、計画の全要素を扱う全面演習になる
全面演習（full-scale）	計画のすべての要素を、実際に近い環境で動かす

[31] 机上演習は軽く、開催しやすく、経営層も参加しやすいので、まず役割と連絡の流れを確かめるのに向きます。実際に切り替えて動くかどうかは、確かめ

SAMPLE

られません。確かめたい内容に合わせて、種類を選ばなければなりません。

物理的セキュリティ運用との連携 [1.8]

データセンターと施設の評価

データセンターや施設の評価（facility assessment）は、物理の面の弱点を見つける作業です。

項目	見ること	関連する管理策
立地	洪水や地震の危険、周辺の施設、人の通りやすさ	立地の選定（PE-23）
境界	フェンス、出入口の数、見通し、照明	入退室の管理（PE-3）
電源	無停電電源装置（UPS）、非常用発電機の有無と容量	非常用の電源（PE-11）
空調	温度、湿度の管理	環境の制御（PE-14）
消火	火災の検知と消火の設備。主電源が止まっても動く独立した電源	消火（PE-13）
入退室	許可者の一覧、監視、記録	PE-2、PE-3、PE-6

電源・消火・環境の 3 つは、SP 800-53 が管理策として定めています。[32] 無人で見通しの悪い出入口は、入館の権限を確かめる仕組み（PE-3）と、物理的なアクセスの監視（PE-6）を強めます。

- 非常用の電源（PE-11）：秩序ある停止（機器を安全に止める）などのために、無停電電源装置を備える。UPS は、秩序ある停止か、長期の代替電源

SAMPLE

（発電機など）への切り替えまでをつなぐ短期の電源で、長時間の停電には長期の代替電源を備える。

- 消火（PE-13）：独立した電源で動く、火災の検知と消火の設備を置いて保守する。
- 環境の制御（PE-14）：温度・湿度・気圧などを決めた水準に保つ。

評価は、単一障害点（1 つが壊れると全体が止まる箇所）を探す観点で行い、電源、空調、回線を二重化します。

たとえば、新しいデータセンターの候補地を、川の近くで安い A と、高台で少し高い B の 2 か所で比べます。A は洪水の危険が高く、地下に電源設備を置く設計です。B は水害の危険は低くても、非常用発電機の燃料の補給が難しい道路にあります。評価では、危険の大きさ、対策の費用、残る危険を並べて比べなければなりません。A は水害の対策（高い位置への設備、止水板）に費用がかかり、B は燃料の契約で補えます。決め手は、危険と対策を合わせた総額で、立地の安さだけでは決められません。

SAMPLE

入館証と訪問者管理

入館証（バッジ）は、入退室を制御し、記録する手段です。SP 800-53 の PE-2 は、施設に入ってよい者の一覧を作り、承認し、保守することを求めます。拡張として、役職や役割に応じた許可、2 種類の身分証の提示、付き添いなしの入館の制限もあります。[32] 入る許可は、必要な区域だけに絞ります（最小特権の物理版）。暗証の組み合わせや鍵は、知っていた者が異動・退職した時、鍵をなくした時、暗証が漏れた疑いがある時に変えます（PE-3）。

訪問者の記録（PE-8）は、施設の訪問者の記録を、決めた期間残すことです。記録に載せる内容は、訪問者の氏名と所属、署名、身分証の種類、訪問の日、入退出の時刻、用件、訪問先の氏名と所属です。記録は決めた頻度で見直し、

異常は決めた担当者に報告します。一般の人が立ち入れる区域には、記録は不要です。[32]

訪問者の受け入れは、次の順に進めます。

1. 事前に、来訪の目的と訪問先を登録する。
2. 受付で身分証を確認し、来訪者名簿に記入する。
3. 来訪者用の入館証を渡し、付き添いを付ける。
4. 付き添いの者が訪問先の区域まで同行し、区域内で目を離さない。
5. 退出時に入館証を回収し、退出の時刻を記録する。
6. 名簿を定期的に見直し、異常を報告する。

付き添いなしで、来訪者が機密区域に入る状態は、入退室の管理の違反です。

訪問者には、従業員と見た目で区別できる入館証を渡して付き添いを付け、保守の記録には、作業者の氏名、付き添いの氏名、持ち出した部品を書きます。

共連れ（tailgating）は、正規の人の後ろについて、認証なしで入館する手口です。防ぐのは、マントラップ（前室）、1 人ずつの通過を強いる回転式の扉、そして従業員の研修です。扉を開けて人を通す親切が弱点なので、「誰にでも入館証の提示を求める」習慣を作らなければ、研修だけでは防ぎきれません。[13] 物理の侵入テストは、フィッシング、共連れ、なりすましなど、人と警備の弱点を試します。

個人デバイスの制限

個人のデバイスは、データを持ち出す、撮影する、マルウェアを持ち込む経路になります。SP 800-53 の MP-7 は、決めた種類の媒体の使用を制限または禁

SAMPLE

止することを求め、私物の可搬記憶装置（USB 媒体など）もここで扱います。[33]

区域	例
サーバー室・機密区域	私物のスマートフォン、カメラ、USB 媒体の持ち込みを禁じる。入口にロッカーを置く
一般の執務室	私物の接続を許す条件を決める（登録、管理ソフトの導入、暗号化）
会議室	撮影や録音の可否を決める

禁止は、規程、入口の掲示、持ち込みの検査、端末側の制御（USB ポートの無効化）の組み合わせで実現します。規程だけでは、守られているか確かめられません。

物理と論理のセキュリティの連携

物理と論理の管理は、別々に動くと、すき間ができます。

退職の時は、入館証と ID を同時に止めます。異動の時は、ID を止めずに、論理と物理のアクセスの権限がまだ要るかを見直し、要らない分を外します（SP 800-53 の PS-5）。SP 800-53 の PS-4 は、雇用の終了時に、システムへのアクセスを決めた期間内に無効にし、認証の手段と資格情報を取り消し、入館証などの関連する資産を回収することを求めます。[34] 片方だけ止めると、入館証で入って物理の端末から操作する、または ID だけが残って遠隔から入る、という抜け道は塞がりません。

入退室のログとシステムのログは、突き合わせて見ます。サーバー室の入退室のログに記録のない時刻に、サーバー室の管理端末への操作が記録されていれば、共連れや入館証の貸し借りを疑えます。反対に、ある人が入館証でビ

SAMPLE

ルに入っているのに、同じ時刻に別の国から VPN で ID が使われていれば、ID の盗用を疑わなければなりません。

ある従業員が退職し、入館証の返却を受けましたが、人事から IT への連絡が遅れ、ID は 2 週間有効なままの場合を考えます。その間に、退職者の ID で業務システムにログインされた記録が見つかっています。入館証だけ回収して、物理の面を閉じても、論理の面が空いていたことが原因です。対策は、人事の退職手続きから、入館証の停止と ID の無効化を同時に起動する連携の手順を置き、退職の日付に合わせて自動で止めることです。

SAMPLE

サンプルはここまでです

続き(第2章〜巻末)は、ISC2 SSCP 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. ISC2 Code of Ethics（Preamble と Code of Ethics Canons）https://www.isc2.org/ethics ↩
2. ISC2 Ethical Complaint Procedures（Standing of Complainant・Form of Complaints・Professional Conduct Committee・Rights of Respondents・Findings and Recommendations・Disciplinary Action）https://www.isc2.org/ethics ↩ ↩2
3. NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2 Security Categories https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf ↩
4. NIST FIPS 199, 3 Security Categorization Applied to Information Systems（影響度の低・中・高と high water mark）https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf ↩ ↩2
5. RFC 4949, Internet Security Glossary, Version 2（accountability）https://www.rfc-editor.org/rfc/rfc4949.txt ↩
6. NIST SP 800-53 Rev. 5, AC-6 Least Privilege と AC-5 Separation of Duties（管理者の操作の分離）

SAMPLE

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩

7. NIST SP 800-63-4, Digital Identity Guidelines, Appendix（用語集 non-repudiation ）
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf ↩

8. NIST FIPS 186-5, Digital Signature Standard (DSS), 1 Introduction
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf ↩

9. NIST SP 800-53 Rev. 5, AC-5 Separation of Duties・AC-6 Least Privilege
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2 ↩3

10. ISC2 SSCP Certification Exam Outline, How is AI Security Incorporated into the SSCP Domains（Domain 1 の Algorithmic Integrity と ML モデルの更新周期）
https://www.isc2.org/certifications/sscp/sscp-certification-exam-outline ↩ ↩2 ↩3

11. NIST AI 100-2 E2025, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations（data poisoning）
https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2025.pdf ↩

12. NIST SP 800-53 Rev. 5, Chapter Two（管理策ファミリー AC・AT・AU・CM・PE ほか）
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩

SAMPLE

13. NIST SP 800-53 Rev. 5, PE-3(8) Access Control Vestibules https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2

14. NIST SP 800-12 Rev. 1, An Introduction to Information Security https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-12r1.pdf ↩

15. ISO/IEC 27001（ISMS の要求事項）https://www.iso.org/standard/27001 と ISO/IEC 27002（管理策の手引き）https://www.iso.org/standard/75652.html ↩

16. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, 4 Cloud Computing Outsourcing（due care）https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf と NIST SP 800-39, Managing Information Security Risk（due diligence）https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf ↩

17. NIST SP 800-55 Vol. 1, Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures, 3.3 Types of Measures https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-55v1.pdf（取り下げ済みの Rev. 1 の 3 種は https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf）↩

18. NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, 1

SAMPLE

Introduction
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf ↩

19. NIST SP 800-53 Rev. 5, PE-3 Physical Access Control・PE-6 Monitoring Physical Access・AC-3 Access Enforcement https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2

20. NIST CSRC Glossary, compensating security control https://csrc.nist.gov/glossary/term/compensating_security_control ↩

21. NIST SP 800-53 Rev. 5, SA-22 Unsupported System Components・CM-8 System Component Inventory https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2

22. NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1, 2 The Secure Software Development Framework https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf ↩

23. NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-122.pdf ↩

24. NIST SP 800-88 Rev. 2, Guidelines for Media Sanitization（2025 年 9 月）, 3 Summary of Sanitization Methods・3.1 Sanitization Methods・

SAMPLE

3.2 Use of Cryptography and Cryptographic Erase・Appendix C https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r2.pdf ↩ ↩2

25. NIST SP 800-53 Rev. 5, CM-3 Configuration Change Control・CM-4 Impact Analyses・CM-2(3) Retention of Previous Configurations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2 ↩3 ↩4

26. NIST SP 800-53 Rev. 5, CM-2 Baseline Configuration・CM-7 Least Functionality https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf と CIS Benchmarks https://www.cisecurity.org/cis-benchmarks ↩

27. NIST SP 800-50 Rev. 1, Building a Cybersecurity and Privacy Learning Program, 1 Introduction https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf ↩ ↩2

28. NIST SP 800-53 Rev. 5, AT-2 Literacy Training and Awareness https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩

29. CISA, Recognize and Report Phishing https://www.cisa.gov/secure-our-world/recognize-and-report-phishing ↩

30. CIS Critical Security Controls, Control 14: Security Awareness and Skills Training https://www.cisecurity.org/controls/cis-controls-list ↩

SAMPLE

31. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, 1 Introduction • 4 Tabletop Exercises • 5 Functional Exercises https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf ↩ ↩2

32. NIST SP 800-53 Rev. 5, PE-2 Physical Access Authorizations • PE-8 Visitor Access Records • PE-11 Emergency Power • PE-13 Fire Protection • PE-14 Environmental Controls • PE-23 Facility Location https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩ ↩2 ↩3

33. NIST SP 800-53 Rev. 5, MP-7 Media Use https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩

34. NIST SP 800-53 Rev. 5, PS-4 Personnel Termination https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf ↩

SAMPLE

ISC2 Systems Security Certified Practitioner (SSCP) 学習用テキスト(無料サンプル)

版

2026年11月版(ISC2 公式 SSCP Certification Exam Outline（Effective Date: October 1, 2025・v10/2025・英語版・日本語版）準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

ISC2、Systems Security Certified Practitioner（SSCP）および関連の名称は、ISC2, Inc. の商標または登録商標です。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。

本教材は公式シラバスの内容を基に作成したもので、ISC2, Inc. 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