

情報・サイバーセキュリティ管 理士 学習用テキスト

出題範囲の42細目を全部——読んで理解する1冊目

無料サンプル(第1章まで)

情報・サイバーセキュリティ管理士認定試験(旧 情報セキュリティ管理士認定試験) 出題範囲
(2026年2月度試験からの範囲)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

この教材群の使い方(3点セット)

この試験の出題範囲と、このテキストの構成

用語の書き方についてのお断り

第1章 Ⅰ.情報セキュリティ総論

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

情報セキュリティの3要素 [1.1]

情報セキュリティの7要素 [1.2]

守るべき情報資産 [1.3]

リスクマネジメント [1.4]

リスクアセスメント [1.5]

リスク対応 [1.6]

組織における情報セキュリティ対策 [1.7]

情報セキュリティマネジメントシステム [1.8]

情報セキュリティ関連法規 [1.9]

ストラテジ [1.10]

QC七つ道具 [1.11]

新QC七つ道具 [1.12]

サンプルはここまでです

この教材群の使い方(3点セット)

種類	役割
① 学習用テキスト	これだけで問題が解けるようになる本編
② 頻出度別ノート	テキストを読んだら次はこれ。頻出順に絞った問題と解説で「解ける」に橋渡し。試験直前の最終チェックにも
③ 暗記用ノート	覚えるべき要点だけを一問一答に凝縮。空き時間の反復と用語の再確認用

使い方: 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)。暗記用は本線には入れず、空き時間や用語の再確認に並走させます。

このテキストの位置づけ: ①の学習用テキストです。ここを通読して、これだけで問題が解けるようになるのが目標。

この試験の出題範囲と、このテキストの構成

情報・サイバーセキュリティ管理士認定試験は、全日本情報学習振興協会が実施する民間資格の試験です。2026年2月度の試験から、試験名が「情報セキュリティ管理士認定試験」から変わりました。検索には旧名のほうが多く出るので、本文は両方の名を併記します。

出題の形と、2026年2月度の試験からの範囲の変更は次のとおりです。

- 形式：180問・120分のマークシート方式。○×(2択)が80問、4択が100問
- 範囲から外れた分野：コンピュータの一般知識(旧 IV)
- 加わった5項目：Web攻撃対策、ログ・インシデント対応、クラウド・API、ランサムウェア・標的型攻撃、サプライチェーン攻撃

出題範囲は次の3分野。

分野	問数	内容	このテキスト
I 情報セキュリティ 総論	40問	3要素、リスクマネジメント、ISMS、法規、QC	第1章
II 脅威と情報セキュリティ対策	40問	人・委託先・入退管理・障害・事業継続	第2章
III サイバーセキュリティ対策	100問	認証、不正プログラム、攻撃と対策、暗号、クラウド	第3章

各節の見出しの末尾にある [1.1] のような記号は、出題範囲の細目の番号。出題範囲の表と見比べると、どの細目を読んでいるかが分かります。法令・指針の名前と数字(期間・罰則・年数)は、末尾の「商標と出典」にまとめた資料で確かめた値。

試験の要綱は改められることがあります。受験前に公式サイトで最新の出題範囲を確認する。

用語の書き方についてのお断り

旧名と新名、略称と正式名、日本語名と英語名が混ざるときは、最初に正式名を書き、略称を括弧で添えます。試験では略称で問われることが多い。両方を結びつけて覚える。

SAMPLE

第1章 I .情報セキュリティ総論

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

情報セキュリティの3要素 [1.1]

情報セキュリティは、機密性・完全性・可用性の3つを保つことです。頭文字からC.I.A と呼びます。[^c1-1]

要素	定義	損なわれた状態
機密性 (Confidentiality)	認可されていない個人・エンティティ・プロセスに、情報を使用させず開示しない特性	情報が見られた、漏れた
完全性 (Integrity)	正確さ及び完全さの特性	書き換えられた、誤りや欠落が混じった
可用性 (Availability)	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性	使えない、見られない

エンティティは実体・主体のことで、人・組織・設備・ソフトウェア・物理的媒体を含みます。完全性は、情報そのものが改ざんされないことに加えて、情報を処理する方法が守られること(手順の遵守、システムが勝手に変更されないこと)も含みます。可用性は、自然災害やシステムダウンで使えなくなることからの保護に関係します。[^c1-2]

事例問題は「何が起きたか」で判定します。起こした者が社内の従業員でも外部の攻撃者でも、要素は結果で決まります。情報が見られた・漏れたなら機密性、書き換えられた・誤りが混じったなら完全性、使えなくなったなら可用性です。ノートパソコンの紛失で顧客名簿が第三者の手に渡れば機密性、売上データが誤って上書きされれば完全性、サーバの故障で受注画面が開けなければ可用性が損なわれています。複数の要素が同時に損なわれる事故も珍しくありません。ランサムウェ

アは、暗号化で可用性を奪い、窃取を伴えば機密性まで奪います。問題文が指す結果は、一つずつ数えなければなりません。情報が漏れただけで内容が正確なままなら、完全性は損なわれていません。示されていない要素を足してはいけません。

暗号化は、定められた手順でデータを変換し、他人に内容が分からないようにする技術で、復号すれば元に戻せます。機密性を守ります。[^c1-3]

改ざん検知（ハッシュ値の照合や電子署名の検証）は完全性を、バックアップや冗長化（機器や回線の二重化）は可用性を守ります。暗号化はデータの消失を防ぎませんし、バックアップは盗難を防ぎません。

対策の例	守る要素
アクセス権の設定、暗号化、入退室管理、持出しの禁止	機密性
ハッシュ値の照合、電子署名の検証、入力チェック、変更履歴の記録	完全性
バックアップ、機器や回線の冗長化、無停電電源装置、事業継続計画	可用性

電子署名は、完全性（改ざんがないこと）と否認防止の両方を支えます。対策は要素同士で綱引きになることがあり、片方だけを強めれば済む話ではありません。バックアップを増やせば可用性は上がりますが、複製が増えるぶん漏えいの経路も増え、機密性の管理が難しくなります。問題文が「どの要素を優先した対策か」を聞くときは、対策が直接防ぐ事故を見ます。

リスクを下げる方向は2つあります。起こりやすさを下げる例は入退室の厳重な管理、影響度を下げる例はバックアップ頻度を増やすことです。[^c1-2]

情報セキュリティの7要素 [1.2]

JIS Q 27000:2019 は、情報セキュリティを「情報の機密性・完全性・可用性を維持すること」と定め、注記で真正性・責任追跡性・否認防止・信頼性などの特性の維持を含めることもあります。3要素に、この4つを加えたものを7要素と呼びます。中核は3要素で、4つは追加の特性です。[^c1-2]

追加の要素	定義	見分けの言い回し
真正性 (Authenticity)	エンティティが、それが主張するとおりのものであるという特性	なりすましでないと確認できる
責任追跡性 (Accountability)	利用者・システムの行動を一意に追跡できること	誰がいつ何をしたかが記録から分かる
否認防止 (Non-repudiation)	送信者 (受信者) があとから送信 (受信) の事実や内容を否定できないよう、証拠を残すこと[^c1-33]	あとで送っていないとは言えない
信頼性 (Reliability)	意図する行動と結果とが一貫しているという特性	同じ入力で毎回同じ結果になる

否認防止は電子署名で実現します。電子署名は、秘密鍵で作成して公開鍵で検証する仕組みで、送信元のなりすましやメッセージの改ざんがないことの検証と否認防止ができます。[^c1-32] 責任追跡性は、JIS Q 27000 の定義の注記に名前が挙がる特性です。ISMS ユーザーズガイドが定義を引用しているのは真正性・否認防止・信頼性の3つだけで、責任追跡性の定義は引用していません。責任追跡性は、ログの記録と利用者の識別が前提だと覚えると事例問題に使えます。[^c1-2]

3要素との区別が問われます。まず3要素で判断します。なりすましや事後の否定が論点なら、追加の特性を疑います。ログインしてきた人が本人かを確認める話は真正性、あとから「私は送っていない」と言わせない話は否認防止です。3要素だけで

は、この2つは説明できません。送ったこと自体を本人に否定させない話は否認防止、操作の主を記録から辿る話は責任追跡性です。

場面	損なわれた要素
盗まれた ID とパスワードで、社員になりすましたログインが成功した	真正性 (同時に機密性)
取引先が「その注文メールは送っていない」と主張し、送信の証拠が残っていない	否認防止
設定が変更されたが、誰がいつ変更したか記録がなく追跡できない	責任追跡性
同じ入力なのに、実行のたびに計算結果が違う	信頼性
顧客名簿の金額欄が書き換えられた	完全性
障害でシステムが半日使えなかった	可用性

追加の特性は、3要素のどれかに言い換えられる場合があります。なりすましは機密性の問題とも見え、迷う人が少なくありません。その場合は、問題文が「本人であること」を問題にしているのか、「情報が漏れたこと」を問題にしているのかで決めます。

JIS Q 27000 は、ISMS で使う用語を定める規格です。[^c1-2][^c1-5]

用語	定義
情報セキュリティ事象	情報セキュリティ方針への違反や管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム・サービス・ネットワークの状態に関連する事象
情報セキュリティインシデント	望まない・予期しない単独又は一連の情報セキュリティ事象で、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いものの

用語	定義
管理策	リスクを修正する対策。リスクを修正するあらゆるプロセス・方針・仕掛け・実務・その他の処置を含み、常に意図した効果を発揮するとは限らない
リスクマネジメント	リスクについて、組織を指揮統制するための調整された活動

事象とインシデントの違いは、事象が起きただけの段階か、事業に影響しうる確率が高い段階かです。事象が起きただけの段階は、インシデントとは呼びません。被害につながる確率が高い事象が、インシデントです。

守るべき情報資産 [1.3]

情報資産は、守る対象になる情報とそれを扱う資産の全体です。種類は、情報（顧客データ・設計書・契約書）、ソフトウェア（業務アプリ・OS）、物理的資産（サーバ・PC・USB メモリ・書類・施設）、サービス（クラウド・通信回線）、人（従業員とその知識・力量）、無形資産（評判・信用・ブランド）です。

JIS Q 27002 の 5.9 は、情報及びその他の関連資産の目録を、情報資産、ハードウェア、ソフトウェア、仮想マシン (VM)、施設、要員、力量、機能、記録に関する動的な目録の集まりとみてよいと述べています。単一のリストである必要はありません。資産の場所も、必要に応じて含めます。[^c1-6]

洗い出しは、パソコンの中身や引き出しを探すのではなく、日常の業務でどんな電子データや書類を使っているかを考えて行います。洗い出しの対象には、電子データや書類のほか、人（従業員とその知識・力量）やサービスも含みます。結果は「情報資産管理台帳」に記入します。[^c1-4]

JIS Q 27002 の 5.9.1 は、資産を特定して情報セキュリティの観点から重要度を決めること、目録を正確で最新に保つことを求めています。定期的なレビューや、設置・変更・除去のプロセスでの自動更新で、正確性を確保します。[^c1-6]

目録の粒度は、組織のニーズに合わせます。ライフサイクルが短い VM インスタンスのように、特定のインスタンスを文書化できない場合もあります。[^c1-6]

台帳の評価は、中小企業ガイドラインの3つの手順で行います。[^c1-4]

1. 資産ごとに、機密性・完全性・可用性が損なわれたときの事業への影響を、評価値 3～1 で記入する。
2. 3つの評価値のうち最大の値を、その資産の重要度にする。
3. 次に当てはまる資産は、算定結果に関わらず重要度を 3 にする。事故で法的責任を問われる場合、取引先・顧客・個人に大きな影響が出る場合、企業の存続を左右しかねない場合、個人情報を含む場合である。

機密性が 1、完全性が 2、可用性が 3 の資産なら、重要度は 3 です。平均は取りません。

資産には管理責任者を割り当てます。5.9.7～5.9.11 によると、割り当ては資産の生成時又は組織への移転時に行い、管理責任者が職務を離れる・変わるときは再割り当てします。

管理責任者は、目録の作成、分類と保護、分類の定期レビューなどに責任を負います。[^c1-6]

情報の分類と取扱いに移ります。JIS Q 27002 の 5.12 は、機密性・完全性・可用性及び利害関係者の要求事項に基づく組織のニーズに従って分類するとしています。分類は、侵害が組織に与える影響のレベルで決め、各レベルには意味をもつ名称を付けます。価値や重要度が変われば、結果を更新します。[^c1-6]

5.13 のラベル付けは、分類体系に従い、あらゆる形式の情報・関連資産に適用できる手順で行います。ラベルは容易に認識でき、媒体の種類に応じて添付場所・方法を示します。秘密でない情報はラベル付けを省略でき、ラベル付けできない場合の取扱いも定めます。[^c1-6]

機密区分の例は、「社外秘情報」と「公開情報」などです。法律で安全管理が義務付けられているもの、守秘義務の対象、営業秘密、限定提供データとして指定されたものは重く扱います。[^c1-4]

政府統一基準の格付は、機密性が 3・2・1 の 3 区分、完全性が 2・1、可用性が 2・1 の 2 区分です。機密性 2 と 3 を「要機密情報」、完全性 2 を「要保全情報」、可用性 2 を「要安定情報」と呼び、いずれかに当たれば「要保護情報」です。取扱制限は、複製禁止・持出禁止・配布禁止・暗号化必須・読後廃棄など、格付に応じた具体的な取扱い方を示すものです。[^c1-5]

権利で守られる情報は3つです。個人情報とは、生存する個人に関する情報で、氏名・生年月日などで特定の個人を識別できるもの、又は個人識別符号を含むものです。死者の情報は対象外です。[^c1-19]

営業秘密は、秘密として管理されている生産方法・販売方法その他の事業活動に有用な技術上又は営業上の情報で、公然と知られていないものです。要件は秘密管理性・有用性・非公知性です。限定提供データは、業として特定の者に提供する情報として電磁的方法により相当量蓄積・管理されている技術上又は営業上の情報で、営業秘密を除きます。[^c1-7]

知的財産（著作権・産業財産権）は 1.9 で扱います。企業がこれらを漏えいさせた場合は、法的責任と取引先への責任を免れません。

情報	守る要件	企業の責任
個人情報	生存する個人を識別できること	安全管理措置、従業員・委託先の監督、漏えい等の報告 (1.9)
営業秘密	秘密管理性・有用性・非公知性の3つ	アクセス制限や秘密表示で秘密として管理する。管理が欠ければ保護されない

情報	守る要件	企業の責任
限定提供データ	業として特定の者に提供し、電磁的方法で相当量蓄積・管理されている	不正取得等が不正競争に当たる
知的財産	著作物・発明・意匠・商標など	他者の権利を侵害しない。自社の権利を守る

リスクマネジメント [1.4]

中小企業ガイドラインは、リスク値を重要度と被害発生可能性の積で表し、被害発生可能性を脅威の起こりやすさと脆弱性のつけ込みやすさから算出します。脅威が脆弱性を利用してどの程度被害をもたらすかを示す指標です。[^c1-4]

用語	意味
脅威	被害をもたらす原因（不正アクセス・地震・内部不正）
脆弱性	脅威につけ込まれる弱点（パッチ未適用・施錠なし）
リスク	目的に対する不確かさの影響。影響とは期待されていることからの乖離で、好ましいもの・好ましくないものの両方があり得る
リスク源	リスクを生じさせる要素
影響	期待されていることからの乖離。好ましいもの・好ましくないもの、又はその両方があり、機会又は脅威を示したり、もたらしたりすることがある

JIS Q 31000:2019 のリスクの定義は、悪い結果だけを指しません。好ましい乖離も含まれます。[^c1-2] 詳細リスク分析では、情報資産ごとに資産価値・脅威・脆弱性・セキュリティ要件の4つを識別し、リスク基準に照らして評価します。[^c1-5] ISMS 6.1.2 c) は、リスクの特定を、情報の機密性・完全性・可用性の喪失に伴う視

点で行うことを要求します。資産・脅威・脆弱性ベースのリスクアセスメントも、具体的な方法の一つとして有効です。[^c1-2]

リスクの特定では、リスク源、影響を受ける領域、事象、これらの原因と起こり得る結果を挙げます。リスク源が組織の管理下にあるか否かにかかわらず行います。[^c1-2]

JIS Q 31000:2019 のプロセスは、次の要素で構成されます。コミュニケーション及び協議 (6.2)、リスク基準 (6.3.4)、リスクアセスメント (6.4)、リスク対応の選択肢 (6.5.2)、モニタリング及びレビュー (6.6) です。リスクアセスメントは、リスク特定・リスク分析・リスク評価を網羅するプロセス全体を指します。モニタリング及びレビューは、プロセスの設計・実施・結末の質と効果を保証し改善することで、計画、情報の収集と分析、結果の記録、フィードバックの提供を含みます。[^c1-5]

ISMS 6.1.2 の流れは、リスク基準の確立、一貫性・妥当性の確保、リスクの特定、リスクの分析、リスクの評価の順です。リスク分析は結果と起こりやすさの組合せでリスクレベルを決めます。評価はリスク基準と比較して、対応の必要性和優先順位を決めます。[^c1-2]

リスク基準は、目的に照らして、取ってもよいリスク又は取ってはならないリスクの大きさ及び種類の規定です。[^c1-5]

中小企業ガイドラインのリスク値の区分例は、9～6 が大 (深刻な事故の可能性大)、4 が中 (重大な事故の可能性有)、3～1 が小 (事故の可能性小、起きても受容範囲) です。[^c1-4]

リスク受容基準は、リスクを受容するかどうかの判断基準です。受容の意思決定は、リスクに責任と権限を負うリスク所有者が行います。資産のオーナーはリスク所有者でもることが多くあります。[^c1-2]

残留リスクは、リスク対応後に残るリスクです。ISMS の 6.1.3 f) は、リスク所有者がリスク対応計画と残留リスクを承認することを求めます。残留リスクのレベルが

許容可能かを判断し、許容できなければ新たな対応を策定する、循環するプロセスです。[^c1-2]

サイバーセキュリティ経営ガイドラインの指示4は、サイバー保険の活用や専門ベンダーへの委託を含むリスク対応計画を策定させ、対応後の残留リスクを識別させます。[^c1-9]

対応後はモニタリング及びレビューを行い、さらなる改善を図ることが望ましいとされます。リスクアセスメントは、あらかじめ定めた間隔で、又は重大な変更の提案・重大な変化の発生の際に実施し、結果の文書化した情報を保持します(8.2)。[^c1-5][^c1-2]

重要度3の顧客台帳で被害発生可能性が3なら、リスク値は $3 \times 3 = 9$ で「大」です。リスク受容基準が「リスク値4以下は受容」の組織で、多要素認証の導入などにより被害発生可能性が1に下がったとします。リスク値は $3 \times 1 = 3$ で、基準以下なので受容できます。残ったリスクが残留リスクで、リスク所有者が対応計画と一緒に承認します。承認するのはセキュリティ担当者ではありません。

リスクアセスメント [1.5]

リスクアセスメントは3段で進みます。リスク特定、リスク分析、リスク評価の順です。リスク特定は、リスク源・影響を受ける領域・事象(周辺状況の変化を含む)・原因・起こり得る結果を挙げ、リスクの包括的な一覧を作る段です。この段で特定されなかったリスクは、以降の分析から外れます。[^c1-2]

リスク分析は、リスクレベルを決める段です。リスク評価は、分析結果をリスク基準と比較して受容可能かを決め、対応の意思決定を助ける段です。結果として、既存の管理策を維持するだけという判断もありえます。[^c1-5][^c1-2]

分析のアプローチは4つです。[^c1-5]

アプローチ	中身	利点	欠点
ベースラインアプローチ	既存の基準をリスク基準として、運用がそれを満たすかで評価する	簡単	選ぶ基準によって要求水準が高すぎ・低すぎになりうる
非形式的アプローチ	担当者やコンサルタントの知見・経験で評価する	短時間でできる	属人的な判断に偏るおそれがある
詳細リスク分析	資産価値・脅威・脆弱性・セキュリティ要件を識別して評価する	厳密に評価できる	工数と費用が多くかかる
組合せアプローチ	ベースラインアプローチと詳細リスク分析を併用する	互いの欠点を補う (作業の効率化と分析精度の向上)	運用の設計が要る

成熟度が十分でない組織は、簡易なベースラインから始めるのが現実的です。重要な資産だけ詳細に分析する、というのが組合せアプローチの典型です。[^c1-5]

場面	向くアプローチ
小規模な組織で、まず全体の水準を既存の基準にそろえたい	ベースラインアプローチ
専門家の経験で、短時間に当たりを付けたい	非形式的アプローチ
基幹システムなど重要な資産だけ、脅威と脆弱性まで厳密に見たい	詳細リスク分析
全体はベースラインで済ませ、重要な資産だけ詳細に見たい	組合せアプローチ

分析の方法は、定性的分析・半定量的分析・定量的分析、又はそれらの組合せで行えます。リスクの種類・利用可能な情報・結果の使い道を反映して選び、リスク基準と矛盾しないようにします。[^c1-2]

定性的評価の例は、脅威事象の発生可能性と負の影響の可能性を「非常に低い／低い／中間／高い／非常に高い」の5段階でマトリクスにして、総合的な可能性を決める方法です (NIST SP800-30 rev1 由来)。^[^c1-5]

定量的評価は、リスクを金額で表します。一般に、1回の損失額に年間の発生頻度を掛けた年間予想損失額 (ALE) で示します。

方法	表し方	利点	欠点
定性的	高・中・低、5段階など	数値データが無くて も使え、短時間でできる	評価者の判断で結果 が変わる
半定量的	点数や指数	順位付けと優先順位 付けがしやすい	点数の差が実際の損失の差を表すとは限らない
定量的	金額 (年間予想損失額など)	対策費との比較ができる	発生頻度や被害額のデータが要る

例: 顧客データベースが漏えいすると、1回あたり 3,000 万円の損失が出る。発生は年 0.2 回 (5年に1回) と見込む。年間予想損失額は $3,000 \text{ 万円} \times 0.2 = 600 \text{ 万円}$ 。年 400 万円かかる対策で発生を年 0.05 回に下げられるなら、対策後は $3,000 \text{ 万円} \times 0.05 = 150 \text{ 万円}$ 。低減額は $600 - 150 = 450 \text{ 万円}$ で、対策費 400 万円を上回るなので、対策に投資する価値がある (差し引き 50 万円)。

低減額が対策費を下回るなら、投資は割に合いません。そのときは保有 (受容) が合理的な選択になります。

リスク値の算出は、資産ベースの3段階で行います。重要度 (3～1) と被害発生可能性 (3～1) を掛けます。被害発生可能性は、脅威と脆弱性から決めます。^[^c1-4]

評価	脅威(起こりやすさ)	脆弱性(つけ込みやすさ)
3	いつ発生してもおかしくない	対策を実施していない(ほぼ無防備)
2	特定の状況で発生(年に数回程度)	部分的に対策を実施している
1	通常は発生しない	必要な対策をすべて実施している

被害発生可能性は3高(いつ発生してもおかしくない)・2中(年に数回程度)・1低(通常は発生しない)です。[^c1-4]

例として、重要度3の顧客台帳で被害発生可能性が3なら、リスク値は $3 \times 3 = 9$ で「大」です。重要度2で被害発生可能性が2なら4で「中」です。

手順は3段です。手順1は情報資産の洗い出し(重要度)、手順2はリスク値の算定(重要度 × 被害発生可能性)、手順3は情報セキュリティ対策の決定で、リスク値の大きいものから対策を検討します。[^c1-4]

リスク対応 [1.6]

リスク対応の選択肢は4つです。中小企業ガイドラインは、低減・保有・回避・移転と呼びます。[^c1-4]

選択肢	一言	例
低減	対策を導入・強化して脆弱性を改善し、事故の可能性を下げる	パッチ適用、入退室管理
保有(受容)	現状維持。受容できる、対策費が損害額を上回る場合は何もしない	被害額が小さい資産を対策しない

選択肢	一言	例
回避	仕事のやり方を変えるなどして、リスクの源そのものをなくす	個人情報を送送完了後すぐに消去する、ネットバンキング専用パソコンを設けメール・Web閲覧とUSBメモリを禁止する
移転	自社より有効な対策を行っている、あるいは補償能力がある他社のサービスを使い、負担を下げる	決済代行でカード番号を非保持化する、業務システムを外部クラウドへ移す、サイバー保険に加入する

JIS Q 27001 の説明では、選択肢は低減・受容（保有）・回避・共有の4つです。共有が、中小企業ガイドラインの「移転」に当たります。情報セキュリティでは、基本的にリスクを低減する方向でアプローチします。[^c1-2]

回避は、リスク対応を考えてもコストの割にベネフィットが得られない場合に、業務を廃止したり資産を破棄したりしてリスクを避けることです。保有は、リスクが組織の方針及びリスク基準を明らかに満たす場合に、情報に基づいた選択として意識的・客観的に受け入れます。何もしていないのとは違い、判断を記録します。[^c1-2]

事例から選ぶときは、起きた変化の方向を見ます。

場面	対応	理由
ウイルス対策ソフトを全 PC に入れ、パッチを自動適用にした	低減	脆弱性を直し、事故の可能性を下げた
個人情報の取得をやめ、既存データも廃棄した	回避	リスクの源をなくした
ネットバンキング専用 PC を設け、メールと Web 閲覧を禁止した	回避	感染の経路をなくした

場面	対応	理由
決済代行サービスに任せ、カード番号を自社で持たなくした	移転	他社の対策に預けた
サイバー保険に加入した	移転	損害の負担を保険会社に分けた
損害額が小さい資産を、リスク基準に照らして対策せず現状のまま使う	保有	判断して受け入れた

取り違えやすい点が3つあります。1つ目は、保険やクラウドへの移行を低減と取り違えることです。どちらも事故の可能性は下げません。負担や責任の一部を他者に預ける移転です。2つ目は、何もしないことをすべて保有と呼ぶことです。保有は、基準に照らして意識的に受け入れた場合だけを指します。気づかず放置している状態は保有ではありません。3つ目は、移転しても責任が消えないことです。委託先の管理は自社に残ります。[^c1-4]

リスク対応計画は、ISMS の 6.1.3 a～f の6段階で作ります。[^c1-2]

1. リスク対応の選択肢を選定する。
2. 必要な管理策を決定する。
3. 決めた管理策を附属書Aと比較する。
4. 適用宣言書を作成する。
5. リスク対応計画を策定する。
6. 計画と残留リスクについて、リスク所有者の承認を得る。

適用宣言書は、ISMS で適用する管理策を記述した文書化された情報です。適用した管理策とその理由、適用しない場合の理由、附属書A以外から独自に追加した管理策の内容と理由も書きます。[^c1-13] 附属書Aの管理策は適用除外が可能です。除外した理由が求められます。箇条4～10の要求事項は例外が認められま

せん。ISMS ユーザーズガイドと ISMS-AC は「除外の原則」の例として、ISMS の能力・責任に影響しない、情報セキュリティ目的と相反しない、関連法規や規制の要求事項でない、という条件がすべて満たされる場合にのみ除外する、という考え方を示しています。[^c1-2][^c1-13]

サイバー保険は、情報漏えいに限らず損害を補償します。補償の対象は、損害賠償責任（賠償費用・争訟費用等）、事故対応費用（原因調査、コールセンター設置、記者会見、見舞金、法律相談、再発防止策の策定等）、利益損害・営業継続費用で、個人情報漏えい保険より広い範囲です。金銭的補償のほか、相談サービスなどを付けるものもあります。保険は移転の手段で、リスクは消えないため残留リスクとして識別します。[^c1-9]

SECURITY ACTION の宣言、プライバシーマークや ISMS などの認証取得、適切な情報管理体制の導入があると、保険料が割引になる保険もあります。[^c1-4]

外部委託による移転（共有）も同じで、委託先の管理は自社に残ります。[^c1-4]

組織における情報セキュリティ対策 [1.7]

情報セキュリティポリシーは、基本方針・対策基準・実施手順の3階層で構成します。政府統一基準の整理では、対策基準と実施手順を総称して情報セキュリティ関係規程と呼びます。対策基準は、リスク評価の結果を踏まえ、情報セキュリティ委員会の審議を経て定めます。[^c1-5]

階層	中身	変わりやすさ
基本方針	組織の方針を宣言する。管理体制の整備、法令・ガイドライン等の順守、セキュリティ対策の実施、継続的改善が記載項目の例。決まった書き方はなく、従業員や顧客など関係者に周知する	変わりにくい

階層	中身	変わりやすさ
対策基準	基本方針を実現するための遵守事項を定める	中間
実施手順	対策基準に定められた対策内容を、個別の情報システムや業務で実施するために、あらかじめ定める具体的な手順	変わりやすい

基本方針は経営者が決め、実施手順は現場が使う文書です。「パスワードは 12 文字以上」は対策基準、「新入社員のアカウントは次の画面でこう設定する」は実施手順に当たります。[^c1-4]

組織体制では、経営者が最終責任を負います。経営者が責任者となる担当幹部（CISO 等）に指示する形がサイバーセキュリティ経営ガイドラインの考え方で、経営者は「3原則」を認識し、CISO 等に「重要10項目」を指示して実行させます。[^c1-11]

情報セキュリティ委員会等には経営層も参加します。資源配分や方針は経営の判断が要るためです。基本方針や資源配分を審議し、決定内容の記録、全社への周知とフォローを徹底します。担当する役職員・部署の役割と責任を文書化し、平時と有事の連絡先リストを整備します。[^c1-4]

CSIRT (Computer Security Incident Response Team) は、機関内で発生した情報セキュリティインシデントに対処するために設置された体制です。[^c1-5]

規程類は、人を縛る文書です。JIS Q 27002 の 6.2 は、雇用契約書に情報セキュリティに関する要員と組織の責任を記載し、秘密情報へアクセスする前に秘密保持契約書 (守秘義務契約書) への署名を求めることが望ましいとしています。[^c1-6]

6.4 の懲戒手続は、情報セキュリティ方針違反の事前確認を待って開始します。違反の内容・重大さ、故意か偶発か、初回か再発か、教育・訓練を受けていたかを考慮して、段階別に対応します。抑止力としても使います。[^c1-6]

内部不正防止ガイドラインは、解雇等の懲戒処分に備えて就業規則等の内部規程を整備し、正式な懲戒手続を用意するよう求めています。誓約書（秘密保持誓約書）は、役職員に重要情報を保護する義務があることを理解させるために、入社時以外にも昇格・配置転換・プロジェクトの開始時や終了時など適切な機会に提出を求めます。[^c1-12]

教育・訓練と周知は、6.3 によると定期的 to 実施します。新しい要員や異動者にも開始時に適用し、終了時に理解の評価を行ってプログラムの有効性を確認します。[^c1-6]

内部不正防止ガイドラインは、全役職員に繰り返し実施し、教育内容を定期的に見直すとしています。受講状況と理解度を記録します。職位や契約形態に応じたレベルで行い、特にシステム管理者には規範意識を高める教育を行います。[^c1-12]

点検と監査は区別します。点検は自らの対策が実施されているかを確かめることで、結果は経営者に報告し、経営者の意図するセキュリティ対策が実現できているかを確認します。[^c1-4]

内部監査は、ISMS が適切に運用され継続的に改善されることを保証する重要なプロセスです。主な役割は、適合性の評価、運用の有効性確認、問題点や改善点の特定、継続的改善の促進、客観的な評価の提供です。[^c1-2]

情報セキュリティ監査は、独立した立場の者が基準に照らして評価する点が、現場の点検と違います。

活動	実施者	目的
自己点検	現場の担当者・部門	自らの対策が実施されているかを確かめる
内部監査	自組織の中の、監査対象から独立した者	ISMS の適合性と運用の有効性を評価し、継続的改善を促す (ISMS の 9.2)

活動	実施者	目的
外部監査・認証審査	組織の外の第三者	基準への適合を客観的に評価する。ISMS 認証では認証機関が審査する
マネジメントレビュー	トップマネジメント	ISMS が引き続き適切かを見直す (9.3)

内部監査と自己点検の違いは、実施者の独立性です。現場が自分の業務を確かめるのが点検、監査対象から独立した者が評価するのが監査です。

情報セキュリティマネジメントシステム [1.8]

ISMS (情報セキュリティマネジメントシステム) は、リスクマネジメントのプロセスを適用して、機密性・完全性・可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与える仕組みです。[^c1-13]

JIS Q 27001:2023 (ISO/IEC 27001:2022) は、箇条0～10と附属書Aで構成されます。箇条4～10は例外が認められません。[^c1-2]

箇条	内容
0～3	序文・適用範囲・引用規格・用語
4 組織の状況	4.1 組織及びその状況の理解、4.2 利害関係者のニーズ及び期待の理解、4.3 ISMS の適用範囲の決定、4.4 ISMS
5 リーダーシップ	トップマネジメントの責任
6 計画策定	6.1.1 一般 (リスクと機会の決定)、6.1.2 情報セキュリティリスクアセスメント、6.1.3 情報セキュリティリスク対応 (適用宣言書とリスク対応計画を策定)、6.2 情報セキュリティ目的、6.3 変更の計画策定

箇条	内容
7 支援	資源・力量・認識・コミュニケーション・文書化した情報
8 運用	運用の計画策定と実施
9 パフォーマンス評価	9.1 監視・測定・分析・評価、9.2 内部監査、9.3 マネジメントレビュー
10 改善	10.1 継続的改善、10.2 不適合及び是正処置
附属書A	管理策の一覧

PDCA は箇条に対応します。附属書SL (マネジメントシステム規格の共通構造) は「6章が Plan、8章が Do、9章が Check、10章が Act」の構成で、27001:2022 も同じです。条文に「PDCA モデル」の語は明記されませんが、PDCA のアプローチが考慮されています。[^c1-2]

段階	箇条	活動
Plan	6	リスクアセスメント・リスク対応・目的の計画策定
Do	8	運用の計画策定と実施
Check	9	監視・測定・内部監査・マネジメントレビュー
Act	10	継続的改善・是正処置

運用では、リスク分析とリスク対応について PDCA サイクルを定め、計画を定期的に見直します。例えば年1回リスク分析をやり直し、リスクの変化に応じてリスク対応を検討します。リスクが減少した場合は、対応が過剰にならないよう調整します。[^c1-2]

内部監査は 9.2、マネジメントレビューは 9.3 で、どちらも Check に入ります。是正処置は Act です。

附属書A の管理策は、2022 版 (JIS Q 27001:2023) で 114 から 93 に整理され、管理策の箇条は 14 (5～18) から 4 (5～8) になりました。[^c1-2]

箇条	分類	項番	数
5	組織的管理策	5.1～5.37	37
6	人的管理策	6.1～6.8	8
7	物理的管理策	7.1～7.14	14
8	技術的管理策	8.1～8.34	34

合計 93 です。分け方のルールは JIS Q 27002:2024 の 4.2 にあり、個人に関係すれば人的、物理的対象に関係すれば物理的、技術に関係すれば技術的、それ以外は組織的に分類します。[^c1-6][^c1-2] 管理策には5つの属性が付き、その一つの管理策タイプは、予防（インシデントの発生を予防）、検知（発生時に機能）、是正（発生後に機能）の3つです。[^c1-2]

附属書A の各分類に入る代表的な管理策です。[^c1-6]

分類	管理策の例
5 組織的	5.1 情報セキュリティのための方針群、5.9 情報及びその他の関連資産の目録、5.12 情報の分類、5.13 情報のラベル付け、5.15 アクセス制御、5.19 供給者関係における情報セキュリティ、5.24～5.28 インシデント管理、5.31 法令、規制及び契約上の要求事項
6 人的	6.1 選考、6.2 雇用条件、6.3 意識向上、教育及び訓練、6.4 懲戒手続、6.6 秘密保持契約又は守秘義務契約、6.7 リモートワーク、6.8 情報セキュリティ事象の報告

分類	管理策の例
7 物理的	7.1 物理的セキュリティ境界、7.2 物理的入退、7.7 クリアデスク・クリアスクリーン、7.10 記憶媒体、7.14 装置のセキュリティを保った処分又は再利用
8 技術的	8.5 セキュリティを保った認証、8.7 マルウェアに対する保護、8.13 情報のバックアップ、8.14 情報処理施設・設備の冗長性、8.15 ログ取得、8.20 ネットワークセキュリティ、8.24 暗号の利用、8.28 セキュリティに配慮したコーディング

分類は「誰に・何に関わるか」で決まります。入退室のカードは物理的、認証の仕組み(8.5)は技術的、パスワードの強度(5.17 認証情報)は組織的、入社時の誓約は人的、方針の策定は組織的で、一つの管理策が二つの分類に入ることはありません。クラウドの利用は組織的(5.23)、委託先との合意も組織的(5.20)です。

ISMS 適合性評価制度は三者で成り立ちます。認証機関(審査登録機関)が組織を審査し、認定機関(ISMS-AC)が認証機関を ISO/IEC 27006 に照らして認定し、要員認証機関が審査員を認証・登録します。申請先は ISMS-AC ではなく、認定された認証機関です。認証範囲は組織の必要に応じて定めてよく、全社である必要はありません。認証の有効期限は 3 年です。初回審査は第一段階・第二段階の 2 段階で行います。以後、年 1 回以上のサーベイランス審査と、3 年ごとの再認証審査があります。[^c1-14]

規格の版も出ます。ISO/IEC 27001:2022 への移行期限は、2022 年 10 月 31 日から 3 年後の 2025 年 10 月 31 日まででした。日本語版は JIS Q 27001:2023 です。追補1(気候変動)に対応する JIS Q 27001:2025 が 2025 年に制定されました。JIS Q 27001:2025 は追補1の改正内容だけを示し、JIS Q 27001:2023 はこれにより JIS Q 27001:2025 となります。[^c1-15][^c1-16]

27001 は認証の対象になる要求事項で、27002 は認証の対象にならない手引です。[^c1-17][^c1-14][^c1-18]

名称	中身
ISO/IEC 27002:2022 (JIS Q 27002:2024)	管理策の選定・実施・管理のベストプラクティス集。27001 附属書A と整合する。JIS 版は 2024 年 6 月制定
ISO/IEC 27017 (JIS Q 27017:2016)	ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範。JIS 版は 2016 年 12 月制定。ISO/IEC 27017 は 2026 年 7 月 27 日に ISO/IEC 27017:2026 として改訂された。ISMS クラウドセキュリティ認証の認証基準 (JIP-ISMS517-1.0) は ISO/IEC 27017:2015 に基づくもので、JIPDEC が改訂版を作成中。ISO/IEC 27001 への適合も求められる
ISO/IEC 27701:2025	プライバシー情報マネジメントシステム (PIMS) の要求事項と手引。2025 年版は ISO/IEC 27001 の拡張ではなく、ISMS とは独立したマネジメントシステム規格になった
プライバシーマーク制度	JIS Q 15001:2023 をベースにした審査基準で、個人情報保護マネジメントシステムを評価し、使用を認める。付与の有効期間は 2 年間

ISMS 認証は 3 年、プライバシーマークは 2 年です。ISMS は情報全般の管理、プライバシーマークは個人情報に絞った管理を評価します。

情報セキュリティ関連法規 [1.9]

出題は、事例を法律に当てはめる形で出ます。支払用カードの電磁的記録を不正に作る行為が、刑法の「支払用カード電磁的記録不正作出等」に当たるかを問う出題があります。法律ごとの守備範囲を混同すると、事例を当てはめられません。

法律	守るもの
個人情報保護法	個人情報の取扱い

法律	守るもの
不正アクセス禁止法	ID・パスワード等による制限の突破とその周辺行為
不正競争防止法	営業秘密・商品表示・ドメイン名など事業上の利益
刑法	コンピュータ犯罪(ウイルス・業務妨害・詐欺・カード)
著作権法・産業財産権	創作物・発明・デザイン・商標
電子署名法・電子帳簿保存法・e-文書法	電子文書の真正性と保存
サイバーセキュリティ基本法	国・事業者・国民の責務の枠組み
情報流通プラットフォーム対処法	ネット上の権利侵害への対処
特定電子メール法	広告宣伝メール
番号法	マイナンバー

事例	当てはまる法律・条文
退職した元社員が、在職中に持ち出した顧客名簿を競合会社に売った	不正競争防止法(営業秘密の不正取得・使用・開示)
他人のIDとパスワードを入力して、社内システムにログインした	不正アクセス禁止法(第3条)
銀行を装ったサイトを作り、利用者にIDとパスワードの入力を求めた	不正アクセス禁止法(第7条、入力要求)
入手した他人のIDを、別の人に渡した	不正アクセス禁止法(第5条、不正提供)
他人のパソコンで勝手に動作するプログラム(ウイルス)を作成した	刑法(不正指令電磁的記録に関する罪)
他人のネットバンキングの口座に不正にログインして送金した	刑法(電子計算機使用詐欺罪)

事例	当てはまる法律・条文
Web サーバに大量の不正な指令を送り、店の営業を止めた	刑法（電子計算機損壊等業務妨害罪）
ATM のカード情報を読み取り、偽のカードを作った	刑法（支払用カード電磁的記録不正作出等）
本人の同意なく、顧客の個人データを他社に提供した	個人情報保護法（第27条、第三者提供の制限）
従業員が、他人のマイナンバーを無断で集めて保管した	番号法（第20条）
購入したソフトを、自社の全 PC にライセンス数を超えて複製した	著作権法
同意を得ていない相手に、広告メールを一斉送信した	特定電子メール法
掲示板の中傷投稿の発信者を特定したい	情報流通プラットフォーム対処法（発信者情報の開示）
紙の領収書をスキャンして電子化して保存する	e-文書法（通則法）・電子帳簿保存法

個人情報保護法

用語	内容
個人情報（第2条第1項）	生存する個人に関する情報で、氏名・生年月日などの記述等により特定の個人を識別できるもの（他の情報と容易に照合でき識別できるものを含む）、又は個人識別符号を含むもの [^c1-19]
要配慮個人情報（第2条第3項）	本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実など、不当な差別・偏見が生じないよう特に配慮を要するもの。取得にはあらかじめ本人の同意が必要（第20条第2項）

用語	内容
仮名加工情報	他の情報と照合しない限り特定個人を識別できない加工情報
匿名加工情報	識別できず復元もできない加工情報
個人関連情報	個人情報・仮名加工情報・匿名加工情報のいずれにも当たらない、生存する個人に関する情報
個人データ(第16条)	個人情報データベース等を構成する個人情報
保有個人データ	事業者が開示・訂正・利用停止などを行う権限を有する個人データ

事業者の義務は、利用目的の特定・目的外利用の制限(第17条・第18条)、安全管理措置(第23条)、従業員の監督(第24条)、委託先の監督(第25条)、第三者提供の制限(第27条第1項)です。利用目的はできる限り特定し、変更は変更前と関連性を有すると合理的に認められる範囲を超えられません。本人の同意なく、利用目的の達成に必要な範囲を超えて取り扱ってはなりません。第三者提供は、あらかじめ本人の同意を得ないで個人データを提供してはなりません。法令に基づく場合、人の生命・身体・財産の保護で同意が困難な場合などは例外です。[^c1-19]

漏えい等の報告は、次のいずれかに当たる事態(発生又はそのおそれ)が必要です(施行規則第7条)。[^c1-20]

- 1. 要配慮個人情報を含む漏えい等
- 2. 財産的被害が生じるおそれのある漏えい等(クレジットカード番号など)
- 3. 不正の目的によるおそれのある漏えい等(不正アクセス等)
- 4. 本人の数が千人を超える漏えい等

報告は、事態を知った後速やかに行い(速報)、知った日から 30 日以内に確報を出します。3 の不正の目的によるおそれのある事態は 60 日以内です(施行規則第8条)。本人への通知も必要です(法第26条第2項)。[^c1-20][^c1-19] 罰則は、個

個人情報保護委員会の命令に違反すると1年以下の拘禁刑又は100万円以下の罰金です(第178条)。不正な利益を図る目的でのデータベース等の提供・盗用は、1年以下の拘禁刑又は50万円以下の罰金です(第179条)。第178条・第179条の違反が法人の業務に関して行われると、行為者を罰するほか、法人にも1億円以下の罰金刑が科されます(第184条の両罰規定)。^[^c1-19]

不正アクセス禁止法

不正アクセス行為(第2条第4項)は3類型です。^[^c1-21]

1. 他人の識別符号を入力して、制限された利用をできる状態にする。
2. 識別符号以外の情報・指令(セキュリティホール攻撃)を入力して、制限を免れる。
3. 他の特定電子計算機のアクセス制御により制限された電子計算機に、制限を免れる情報・指令を入力する。

禁止行為は、第3条が不正アクセス行為、第4条が他人の識別符号の不正取得、第5条が識別符号の不正提供(助長行為)、第6条が他人の識別符号の不正保管、第7条が識別符号の入力要求(フィッシング)です。第4条～第7条は、不正アクセス行為(ログイン)に及ばなくても、取得・提供・保管・入力要求の行為だけで成立します。罰則は、第3条違反が3年以下の拘禁刑又は100万円以下の罰金(第11条)です。第4条・第6条・第7条違反と、情を知った識別符号の提供(第5条)は、1年以下の拘禁刑又は50万円以下の罰金(第12条)です。その他の第5条違反は30万円以下の罰金です(第13条)。アクセス管理者には努力義務があります(第8条)。識別符号又はこれを確認するための符号の適正な管理に努め、アクセス制御機能の有効性を常に検証し、必要なら速やかに高度化など必要な措置を講ずるよう努めます。努力義務で、罰則はありません。被害を受けた管理者の申出があれば、都道府県公安委員会が再発防止のための援助を行います(第9条)。法は、被害を受けた管理者に公安委員会への届出を義務づけておらず、援助は管理者の申出に応じて行われます。^[^c1-21]

不正競争防止法

営業秘密の3要件は、秘密として管理されている(秘密管理性)、事業活動に有用な技術上又は営業上の情報である(有用性)、公然と知られていない(非公知性)です(第2条第6項)。1つでも欠けると営業秘密として保護されません。「社外秘」と書かれていても、実際にアクセス制限がなければ秘密管理性を欠きえます。[^c1-7]

不正競争行為の主な類型は第2条第1項に並びます。1号は周知な商品等表示の混同惹起、2号は著名な商品等表示の冒用、3号は他人の商品形態の模倣、4～10号は営業秘密の不正取得・使用・開示、11～16号は限定提供データの不正取得等、17・18号は技術的制限手段の無効化、19号はドメイン名の不正取得・使用、20号は誤認惹起表示、21号は信用毀損です。[^c1-7] 営業秘密侵害罪は、不正取得・領得・使用・開示で 10 年以下の拘禁刑若しくは 2000 万円以下の罰金(又は併科)です(第21条)。法人には 5 億円以下の罰金で、海外での使用等の加重類型は 10 億円以下です(第22条)。[^c1-7]

刑法

罪	条	行為	法定刑
不正指令電磁的記録に関する罪	168条の2	正当な理由なく、意図に反する動作をさせる不正な指令の電磁的記録(コンピュータウイルス)を作成・提供	3 年以下の拘禁刑又は 50 万円以下の罰金
同(取得・保管)	168条の3	取得・保管	2 年以下の拘禁刑又は 30 万円以下の罰金

罪	条	行為	法定刑
電子計算機損壊等業務妨害罪	234条の2	人の業務に使用する電子計算機・電磁的記録の損壊、虚偽の情報・不正な指令の付与などで業務を妨害。未遂も罰する	5年以下の拘禁刑又は100万円以下の罰金
電子計算機使用詐欺罪	246条の2	人の事務処理に使用する電子計算機に虚偽の情報・不正な指令を与え、財産権の得喪等に係る不実の電磁的記録を作るなどして財産上不法の利益を得る	10年以下の拘禁刑（罰金の選択肢なし）
支払用カード電磁的記録に関する罪	163条の2	電磁的記録の不正作出	10年以下の拘禁刑又は100万円以下の罰金
同（所持）	163条の3	不正作出カードの所持	5年以下又は50万円以下
同（取得・提供）	163条の4	情報の取得（スキミング等）・提供	3年以下又は50万円以下
電磁的記録不正作出罪	161条の2	事務処理を誤らせる目的で、権利・義務・事実証明に関する電磁的記録を不正に作る	5年以下の拘禁刑又は50万円以下の罰金（公務所・公務員の作るべきものは10年以下又は100万円以下）

事例の見分けは対象で行います。ウイルスを作った・渡したなら不正指令電磁的記録、ネットバンキングの口座を不正操作して送金させたなら電子計算機使用詐欺、サーバを止めて店の営業を妨げたなら電子計算機損壊等業務妨害、カードの

磁気情報を不正に作ったなら支払用カード電磁的記録不正作出です。他人の ID でログインしただけなら、刑法ではなく不正アクセス禁止法の領域です。[^c1-22]

著作権法と産業財産権

著作権は、創作の時に発生し、登録などの方式を要しません（無方式主義、第17条第2項）。存続期間は、原則として著作者の死後 70 年を経過するまでです。共同著作物は、最終に死亡した著作者の死後 70 年です（第51条）。法人等の発意に基づき従業者が職務上作成し、法人等の名義で公表する著作物の著作者は、別段の定めがなければ法人等です（職務著作、第15条）。プログラムの著作物は、公表名義の要件がありません（第15条第2項）。プログラムの複製物の所有者は、自ら電子計算機で実行するために必要と認められる限度で複製できます（第47条の3）。侵害の罰則は、10 年以下の拘禁刑若しくは 1000 万円以下の罰金（又は併科）が基本で、法人には 3 億円以下の罰金刑です（第119条・第124条）。[^c1-23]

産業財産権	存続期間	発生
特許権	出願日から 20 年	設定登録
実用新案権	出願日から 10 年	設定登録
意匠権	出願日から 25 年（関連意匠は基礎意匠の出願日から 25 年）	設定登録
商標権	設定登録日から 10 年（更新登録の申請で更新できる）	設定登録

商標だけ、起算点が出願日ではなく登録日です。更新できるのも商標だけです。[^c1-24]

電子署名法・電子帳簿保存法・e-文書法

電子署名法の電子署名（第2条第1項）は、電磁的記録に記録された情報について行う措置で、その情報が措置を行った者の作成に係るものであることを示すため

のもの、かつ、改変が行われていないかどうかを確認できるもの、の両方を満たします。本人による電子署名（本人だけが行えるよう符号・物件を適正に管理しているもの）が行われている電磁的記録は、真正に成立したものと推定されます（第3条）。認証業務（第2条第2項）は、自らが行う電子署名について、利用者が電子署名を行ったものであることを確認するために用いられる事項が、その利用者に係るものであることを証明する業務です。[^c1-25]

電子帳簿保存法は、国税関係帳簿は最初の記録段階から一貫して電子計算機で作成する場合、国税関係書類は一貫して電子計算機で作成する場合に、財務省令に従って電磁的記録の保存で書面の保存に代えられるとします（第4条）。電子取引を行ったときは、取引情報に係る電磁的記録を保存しなければなりません（第7条、令和4年1月1日以後の電子取引から適用）。[^c1-26] e-文書法（通則法）は、法令で書面保存が義務づけられているもの（主務省令で定めるものに限る）を、書面に代えて電磁的記録で保存できるとし（第3条）、電磁的記録での保存は書面で保存したものとみなされます。書面による作成が義務づけられているものも、電磁的記録で作成できます（第4条）。[^c1-27]

サイバーセキュリティ基本法と情報流通プラットフォーム対処法

サイバーセキュリティ基本法は、サイバーセキュリティを、電磁的方式で記録・発信・伝送・受信される情報の漏えい・滅失・毀損の防止など安全管理に必要な措置と、情報システム・情報通信ネットワークの安全性・信頼性確保のための措置が講じられ、その状態が適切に維持管理されていることと定義します（第2条）。条の見出しは、国（第4条）・地方公共団体（第5条）・重要社会基盤事業者（第6条）・サイバー関連事業者その他の事業者（第7条）・教育研究機関（第8条）が「責務」、国民（第9条）だけが「努力」です。施策を策定し、及び実施する責務を有すると定めるのは国と地方公共団体だけで、事業者・教育研究機関・国民の条は、中身が「努めるものとする」の形です。重要社会基盤事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性への関心と理解を深め、自主的かつ積極的に確保に努め、国や地方公共団体の施策に協力するよう努めます。[^c1-28]

情報流通プラットフォーム対処法の正式名称は「特定電気通信による情報の流通によって発生する権利侵害等への対処に関する法律」で、旧プロバイダ責任制限法です。損害賠償責任の制限、発信者情報の開示、発信者情報開示命令事件の手続、大規模特定電気通信役務提供者の義務を定めます。被侵害者は、開示関係役務提供者に発信者情報の開示を請求できます(第5条)。裁判手続は第8条以下で、提供命令・消去禁止命令などもあります。大規模特定電気通信役務提供者には、総務大臣が指定し(第20条)、指定から3か月以内に届出(第21条)、被侵害者からの申出の受付方法の公表(第22条)、遅滞なく調査(第23条)、申出を受けた日から14日以内の総務省令で定める期間内に結果を申出者に通知(第25条)、という義務があります。[^c1-29]

特定電子メール法と番号法

特定電子メールは、営利を目的とする団体及び営業を営む場合における個人が、自己又は他人の営業につき広告又は宣伝を行うための手段として送信する電子メールです(第2条)。原則はオプトイン方式で、あらかじめ送信に同意した(求めた)者などにしか送れません。例外は、メールアドレスを通知した者、取引関係にある者、アドレスを公表している団体や営業を営む個人です(第3条)。同意を得た送信者は、求め・同意があったことを証する記録を保存します。受信拒否の通知を受けたら、その意思に反して送信してはなりません(第3条第2項・第3項)。送信者の氏名又は名称、受信拒否の通知を受けるための電子メールアドレス又はURLなどは、受信者の端末画面に正しく表示します(第4条)。送信者情報を偽った送信(第5条違反)と措置命令違反は、1年以下の拘禁刑又は100万円以下の罰金で、法人には3000万円以下の罰金刑です(第34条・第37条)。[^c1-30]

番号法で、個人番号は住民票コードを変換して得られ、住民票に係る者を識別するために指定される番号です。特定個人情報とは、個人番号(に代わる符号を含む)を内容に含む個人情報です(第2条)。何人も、第19条各号に当たる場合を除き、他人に個人番号の提供を求めてはならず(第15条)、特定個人情報を提供してはならず(第19条)、収集・保管してはなりません(第20条)。個人番号利用事務実施者

及び個人番号関係事務実施者は、漏えい・滅失・毀損の防止その他の適切な管理のために必要な措置を講じなければなりません(第12条)。罰則は、特定個人情報ファイルを正当な理由なく提供した事務従事者が4年以下の拘禁刑若しくは200万円以下の罰金(又は併科)、個人番号を不正な利益目的で提供・盗用した場合が3年以下の拘禁刑若しくは150万円以下の罰金です(第48条・第49条)。^[^c1-31]

拘禁刑の上限の比較

上限	罪・違反
10 年以下	営業秘密侵害罪、電子計算機使用詐欺罪、支払用カード電磁的記録の不正作出、著作権侵害
5 年以下	電子計算機損壊等業務妨害罪、電磁的記録不正作出罪(一般)、不正作出カードの所持
4 年以下	番号法:特定個人情報ファイルの正当な理由のない提供
3 年以下	不正アクセス行為(第3条)、不正指令電磁的記録の作成・提供、番号法:個人番号の不正な利益目的の提供・盗用、カード情報の取得・提供
2 年以下	不正指令電磁的記録の取得・保管
1 年以下	個人情報保護委員会の命令違反、不正アクセス禁止法の第4条・第6条・第7条違反、特定電子メール法の送信者情報の偽り

電子計算機使用詐欺罪だけは、罰金の選択肢がありません。

ストラテジ [1.10]

経営戦略の手法

SWOT 分析は、自社の事業の状況を、強み (Strengths)、弱み (Weaknesses)、機会 (Opportunities)、脅威 (Threats) の4項目で整理して分析する方法です。事業の戦略方針が明確になります。強みと弱みは自社の内部、機会と脅威は外部の環境に属します。[^c1-34]

バランススコアカード (BSC) は、業績を財務だけでなく4つの視点から評価する手法です。基本は、顧客の視点、財務の視点、内部プロセスの視点、学習と成長の視点で、その他の視点を独自に設定することもできます。視点ごとに目標・指標を設定します。財務の視点は「財務面で成功するために出資者にどう行動すべきか」、顧客の視点は「ビジョンと戦略の達成に向け顧客にどう行動すべきか」を問います。[^c1-35]

PPM (プロダクト・ポートフォリオ・マネジメント) は、事業を市場成長率と市場シェアの2軸で4つに分け、資源配分を決める手法です。

成長率が高くシェアも高い事業が「花形」、成長率が低くシェアが高い事業が「金なる木」、成長率が高くシェアが低い事業が「問題児」、成長率もシェアも低い事業が「負け犬」です。金なる木で稼いだ資金を、問題児や花形へ振り向けるのが基本の考え方です。

プロジェクトマネジメント

用語	定義
WBS (Work Breakdown Structure)	プロジェクト全体を詳細な作業に分割する手法。ゴール (開発すべき製品) を細かな成果物に階層的に詳細化し、成果物ごとに必要な作業を配置する[^c1-36]

用語	定義
PERT (Program Evaluation and Review Technique)	WBS で洗い出した作業を組み合わせ、プロジェクトを最短で終了させる計画を立てる手法。作業の順番 (並行か順次か) からスケジュールを立案する[^c1-36]
クリティカルパス	PERT 上でプロジェクトの達成期間を決めている一連の作業。作業の開始から終了までの経路のうち最長のもの。この上の作業が遅れると、プロジェクト全体が遅れる[^c1-36]

アローダイアグラム (矢線図) は、作業を矢線、作業の区切りを結合点で表します。アローダイアグラム法は、米海軍の OR チームで開発された PERT 図と同様の手法で、JIS 2018 で「アロー・ダイヤグラム法」から「アローダイアグラム法」に表記が改められました。[^c1-37] 作成手順は11段です。

1. テーマを決める。
2. 作業を列挙する。
3. 作業名をカード化する。
4. 順序関係を決める。
5. カードを配置する。
6. 結合点・矢線・番号を付ける。
7. 所要日数を見積もる。
8. 最早結合点日程を求める。
9. 最遅結合点日程を求める。
10. 全余裕を求める。
11. クリティカルパスを表示する。

具体例で見ます。作業 A (3日) の後に、作業 B (4日) と作業 C (6日) が並行し、どちらも終わると作業 E (2日) に進む計画です。経路は A→B→E が $3+4+2=9$ 日、

A→C→E が $3+6+2=11$ 日です。最長の A→C→E がクリティカルパスで、全体の所要は 11 日になります。B は C より 2 日短いので、2 日まで遅れても全体に影響しません。この 2 日が余裕です。クリティカルパス上の作業に余裕はありません。出題も、この「最長の経路を選ぶ」形です。

作業 C が 3 日遅れて 9 日かかると、A→C→E は $3+9+2=14$ 日になり、全体が 14 日に伸びます。作業 B が 3 日遅れて 7 日かかった場合は、A→B→E が $3+7+2=12$ 日です。これはクリティカルパスの 11 日を超えるので、全体が 1 日伸びて 12 日になり、クリティカルパスが入れ替わります。余裕の 2 日以内の遅れは、全体に影響しません。

内部統制・IT ガバナンス・コンプライアンス

内部統制は、次の4つの目的が達成されているとの合理的な保証を得るために、業務に組み込まれ、組織内の全員が遂行するプロセスです。金融庁の基準が示します。[^c1-38]

目的	内容
業務の有効性及び効率性	事業活動の目的の達成のため、業務の有効性と効率性を高める
報告の信頼性	組織内及び組織の外部への報告（非財務情報を含む）の信頼性を確保する。財務諸表と財務諸表に重要な影響を及ぼす情報の信頼性（財務報告の信頼性）を含む（2023年の改訂）
事業活動に関わる法令等の遵守	法令やルールを守る
資産の保全	資産の取得、使用及び処分が正当な手続及び承認の下に行われるよう図る

基本的要素は6つです。統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング（監視活動）、IT（情報技術）への対応です。[^c1-38]

用語	何を守り、整えるか
内部統制	4つの目的(業務の有効性及び効率性、報告の信頼性、法令等の遵守、資産の保全)を達成する仕組み。資産の保全は、情報資産の保護とも重なる
情報セキュリティガバナンス	トップマネジメントが、評価・指示・モニタ・コミュニケーションで情報セキュリティを統治する枠組み
IT ガバナンス	経営者が IT の利用を方向付け、統制する枠組み
コンプライアンス	法令・規範・契約上の要求事項の順守

情報セキュリティガバナンスは、評価・指示・モニタ・コミュニケーションの各プロセスで構成されます。トップマネジメントと各 ISMS の責任者が、各プロセスで実行する内容を定めます。目的は6つです(情報セキュリティ管理基準 3.2)。^[^c1-6]

- 1. 組織体全体の統合された包括的情報セキュリティの確立
- 2. リスクに基づく取組による意思決定
- 3. 投資の方向性の設定
- 4. 内部・外部の要求事項への適合
- 5. セキュリティに積極的な文化の醸成
- 6. パフォーマンスが現在及び将来の要求を満たす確実化

コンプライアンスは法令・規範の順守です。JIS Q 27002 の 5.31 は、情報セキュリティに関連する法令・規制・契約上の要求事項と、それを満たすための組織の取組を特定し、文書化し、最新に保つことを管理策とし、目的は順守の確実化です。^[^c1-6]

システム監査

システム監査は、システム監査人がシステムの運用状況等を点検・評価し、ガバナンスやマネジメント等について一定の保証や助言を行う取組です。システムの信頼性を確保し、企業の信用を高めます。[^c1-39]

経済産業省が策定・公表した基準は2つに分かれます。システム監査基準は、監査人の行為規範と監査手続の規則を定めます。システム管理基準は、監査の判断の尺度（組織体制や開発・運用・保守等の基準）を定めます。昭和60年1月に策定され、平成8年・平成16年・平成30年の改訂を経て、令和5年（2023年）4月にも改訂されています。[^c1-39]

システム監査の進め方は、体制整備、監査計画の策定、監査の実施（証拠の入手と評価、調書の作成、結論の形成）、報告、改善提案のフォローアップの順です。基準の構成もこの順に並んでいます。

システム監査基準（令和5年）の構成は12基準で、[1]システム監査の属性に係る基準（基準1～5：権限と責任等の明確化、専門的能力の保持と向上、ニーズの把握と品質の確保、監査の独立性と客観性の保持、監査の能力及び正当な注意と秘密の保持）、[2]実施に係る基準（6 監査計画の策定、7 監査計画の種類、8 監査証拠の入手と評価、9 監査調書の作成と保管、10 監査の結論の形成）、[3]報告に係る基準（11 監査報告書の作成と報告、12 改善提案（及び改善計画）のフォローアップ）です。システム管理基準（令和5年）は、Ⅰ ITガバナンス編とⅡ ITマネジメント編の2編で構成されます。ITマネジメント編の中身は、推進・管理体制、プロジェクト管理、企画プロセス、開発プロセス、運用プロセス、保守プロセス、廃棄プロセス、外部サービス管理、事業継続管理、人的資源管理の10項目。[^c1-39]

サイバーセキュリティ経営ガイドライン

対象は大企業及び中小企業（小規模事業者を除く）の経営者です。経営者が認識すべき「3原則」（Ver3.0）は3つです。[^c1-11]

1. リスクを経営課題と認識し、リーダーシップのもとで対策を進める。

2. 自社だけでなく、国内外の拠点・ビジネスパートナー・委託先などサプライチェーン全体に目配りする。
3. 平時と緊急時の双方で、関係者と積極的にコミュニケーションをとる。

経営者が責任者となる担当幹部(CISO 等)に指示する「重要10項目」は、1 リスクの認識・対応方針の策定、2 リスク管理体制の構築、3 資源(予算・人材)の確保、4 リスクの把握と対応計画の策定、5 効果的に対応する仕組みの構築、6 PDCA による継続的改善、7 インシデント緊急対応体制の整備、8 事業継続・復旧体制の整備、9 サプライチェーン全体の状況把握と対策、10 情報の収集・共有・開示の促進です。指示1は、サイバーセキュリティリスクを経営者が責任を負うべき経営リスクと認識し、対応方針(セキュリティポリシー)を策定して対外的に宣言することです。指示4は、リスク対応計画を策定させ、対応後の残留リスクを識別させることです。[^c1-11][^c1-9]

QC七つ道具 [1.11]

QC七つ道具は、主に数値データを解析する手法です。層別・パレート図・特性要因図・グラフ・チェックシート・ヒストグラム・散布図・管理図の8つを、グラフと管理図を1つの手法として数えて「七つ」とします。[^c1-40]

パレート図

不良・クレーム・故障などの件数や損失金額を原因別・状況別に分類し、データ数の大きい順に並べて、棒グラフと累積曲線で表した図です。少数の重点項目と多数の軽微項目を定量的に把握します。使い方は重点指向(大きな問題に絞る)と、効果の確認(改善前後の図を並べて比較)です。[^c1-41]

描き方は、棒を大きい順に左から並べて棒の間をあけず、「その他」は大きさに関係なく右端に置きます。累積比率の折れ線(パレート曲線)の始点は左縦軸の0、右側縦軸は0~100%です。[^c1-41]

例として、不良原因別の件数が A 40、B 25、C 15、D 10、その他 10 (合計 100) なら、累積比率は 40%、65%、80%、90%、100% です。上位3項目で 80% を占めるので、A・B・C に絞って対策します。

「その他」が D より大きくても右端に置きます。

特性要因図

特性 (結果) と要因 (原因) の関係を整理した図で、石川馨が考案しました。形から「魚の骨」とも呼ばれ、海外では Ishikawa Diagram です。作り方は次の順です。

1. 特性を決める。
2. 特性を「悪さ」で表現する。
3. 大骨を 4M や 5M1E で分類する (4～6本が適当)。
4. 中骨・小骨を、「それはなぜか」を繰り返して出す。
5. 記入もれと因果の逆転をチェックする。
6. 影響の大きい要因に○印を付ける。

4M は Man (作業者)・Machine (機械・設備)・Material (原材料)・Method (方法) で、5M1E は 4M に Measurement (測定) と Environment (環境) を加えたものです。[^c1-42]

連関図法との違いは、連関図が特性要因図の異なる大骨から出た中骨・小骨の要因の相互関係を、論理的に矢印で結んだものだという点です。作成のルールが少なく、自由に表現できます。[^c1-43]

ヒストグラムと散布図

ヒストグラムは、横軸にデータの値をとり、最大値と最小値を含む等間隔の区間を作り、各区間のデータ数を縦軸にとった図です。別名は「柱状図」で、工程のばらつきやロットの把握に使います。[^c1-44]

区間の数はデータ数の平方根 $\sqrt{n}$ を目安にします。 $n=100$ なら 10 区間です。区間の幅は測定単位の整数倍にし、最初の区間の境界値は「最小値 - 測定単位/2」で求めます。[^c1-44]

散布図は、要因と特性のように、2つの対になったデータの関係を表した図です。要因を横軸、特性を縦軸にとり、点の散らばり方で相関を読み取ります。右上がり为正の相関、右下がりを負の相関、傾向が見られないのが相関なしです。[^c1-45]

型には、正の相関、正の相関がありそう、相関なし、負の相関がありそう、負の相関の5種類があります。対のデータは30組以上集めます。相関がなければ他の要因を探します。[^c1-45]

管理図

統計的に決めた管理線（中心線と上下2本の管理限界線）を記入した折れ線グラフです。シューハート博士が考案しました。工程が安定した状態のばらつきと、異常によるばらつきを判定します。使用目的で2つに分かれ、解析用管理図は工程の現状把握や要因解析に、管理用管理図は安定状態にある工程が今後も安定を保っているかの判定に使います。管理用は、解析用の管理線を延長して打点します。[^c1-46]

種類は8つです。計量値用が $\bar{X}$ - R ・ $\bar{X}$ - $\bar{R}$ ・ $\bar{X}$ - R_s ・ $\bar{X}$ - s の4種類、計数値用が np ・ p ・ c ・ u の4種類です。群の大きさ n は 2~6（できれば4~5）、群の数 k は 20~25 以上を集めます。[^c1-46]

重さや長さのような連続量なら計量値、不良個数や欠点数のような数えるデータなら計数値です。

チェックシート・層別・グラフ

チェックシートは、データを集めやすいように、記入欄や項目名をあらかじめ書き込んだ用紙です。目的別に設計した調査用（不良項目別、工程分布調査用、欠点位置調査用、不良原因調査用）と、点検確認用があります。不良項目別は、不良を見

つけるたびに項目の欄に印を付け、どの不良がどれだけ出たかを調べる用紙です。工程分布調査用は、あらかじめ数値を書いた用紙に印を付けて、分布の姿を見る用紙。欠点位置調査用は、製品の概略図に欠点の位置と数を記入して、発生位置を一目で見る用紙です。不良原因調査用は、多くの不良原因を一つの用紙にまとめて、原因をつかむ用紙。[^c1-47]

層別は、データを機械別・作業別・原料別などの特徴でグループ(層)に分けて、層による違いを調べる考え方で、「分けると分かる」と言われます。層間の違いが現れれば、層別がうまくいったことになります。切り口は7つで、人別・機械・装置別、原材料別、作業方法別、時間別、環境別、その他(運送方法・包装・良品/不適合品など)です。時間別は、時間・午前と午後・曜日・日や月や年のように、時間でデータを分ける切り口です。昼勤と夜勤、月初と月末で分けるのも時間別。[^c1-40]

グラフは、折れ線グラフが時間的推移、棒グラフが項目間の大小比較を表し、円グラフ、帯グラフ、レーダーチャートなどがあります。使用目的では、解析用・管理用・計画用・統計用・計算用に分かれます。[^c1-48]

知りたいこと	使う道具
どの原因・項目が大きいのか、どこに絞るか	パレート図
結果に関わる要因を洗い出して整理したい	特性要因図
データのばらつきの形、規格に収まるか	ヒストグラム
2つの量に関係があるか	散布図
工程が安定しているか、異常がないか	管理図
データを漏れなく集めたい、点検したい	チェックシート
機械別・人別などで違いがあるか	層別
時間の推移や項目の大小を示したい	グラフ

新QC七つ道具 [1.12]

新QC七つ道具 (N7) は、親和図法・連関図法・系統図法・マトリックス図法・アローダイアグラム法・PDPC法・マトリックス・データ解析法の7手法です。主に言語データを用い、計画段階 (管理のサイクルの Plan) で活用します。QC七つ道具が数値データの解析なのに対し、N7 は言語データの整理です。[^c1-49]

言語データは3種類あります。事実データは事実をありのままに表し、推定データは一部の事実から新たな発想・推定を述べ、意見データは主張・意志・賛否を述べます。事実認識や原因探索には事実データ、方策の展開には推定データが推奨されます。[^c1-49]

手法	使いどころ	要点
親和図法	モヤモヤして整理できない問題の所在・形態を明らかにする	言語データを相互の親和性 (何となく似ている感じ) でまとめる。カード寄せで作る [^c1-50]
連関図法	原因－結果、目的－手段などが複雑に絡み合う事柄の原因の究明	因果関係のある要因を矢線で結び、問題解決の糸口を見つける。テーマは「○○が○○しないのはなぜか」の形[^c1-43]
系統図法	目的を果たす手段を系統的に追求して対策を見出す	目的→手段を多段に枝分けさせせる樹形図。方策展開型と構成要素展開型の2タイプ [^c1-51]
マトリックス図法	問題に関連する要素同士を組み合わせることで解決の方向を見出す	行・列の交点で関連の有無・度合いを見て優先順位を決める。L型・T型・Y型・X型などの型がある[^c1-52]

手法	使いどころ	要点
アローダイアグラム法	最適な日程計画を立て、進度を効率よく管理する	作業と作業を矢線で結んで順序関係を表す。工期短縮の検討や並行作業の分析にも使う。PERT 図と同様の手法 [[^] c1-37]
PDPC法	事態の進展とともにいろいろな結果が想定される問題で、望ましい結果に至るプロセスを定める	Process Decision Program Chart (過程決定計画図) [[^] c1-53]
マトリックス・データ解析法	多くの要因からなるマトリックス・データの特徴をとらえる	変数間の相関を手がかりに、互いに無相関な少数の総合特性値 (主成分) に変換する。多変量解析の主成分分析法に当たる[[^] c1-54]

PDPC法には2タイプがあります。逐次展開型は、実施に入ってから出る問題に対応して計画を充実させていきます。強制連結型は、重大事態につながるあらゆる事態を読み切り、各事態に対策を考えて重大事態を未然に防ぎます。[[^]c1-53]

マトリックス・データ解析法は、N7 の中で唯一、数値を基に複雑な計算を伴う手法です。計算はソフトに任せ、考え方を理解して主成分の意味づけ (ネーミング) をします。[[^]c1-54]

親和図法は「似たものを集めて問題の形を見る」手法で、連関図法は「原因を矢印で結んで根本を探る」手法です。系統図法は目的から手段を「枝分かれで展開」し、マトリックス図法は「2つの軸の交点で関連を見る」手法です。アローダイアグラム法は作業の順序と日程を、PDPC法は不測の事態への備えを扱います。

サンプルはここまでです

続き(第2章～巻末)は、情報・サイバーセキュリティ管理士 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

情報・サイバーセキュリティ管理士 学習用テキスト(無料サンプル)

版

2026年10月版(情報・サイバーセキュリティ管理士認定試験(旧 情報セキュリティ管理士認定試験)
出題範囲(2026年2月度試験からの範囲)準拠)

発行

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

お問い合わせ

info@shikaku-doujou.com

「情報セキュリティ管理士認定試験」「情報・サイバーセキュリティ管理士認定試験」は、一般財団法人 全日本情報学習振興協会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。

本教材は公式の出題範囲(2026年2月度試験からの範囲)の内容を基に作成したもので、一般財団法人 全日本情報学習振興協会との提携・承認関係はありません。実際の試験問題の転載・復元は行っていません。

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。