

IT 資格道場

ISC2 Certified in Cybersecurity (CC) 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 Certified in Cybersecurity (CC) Certification Exam Outline (Effective
Date: September 1, 2026・v01/2026・英語版・日本語版) 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

第1章 Security Principles [1.1/1.2/1.3/1.4/1.5]

機密性・完全性・可用性 (CIA) [1.1]
認証・認可・アカウンティング (AAA) [1.1]
否認防止 [1.1]
プライバシー [1.1]
リスクの用語 [1.2]
リスク管理のライフサイクル [1.2]
リスク評価: 定性と定量 [1.2]
リスクへの対応: 回避・受容・軽減・移転 [1.2]
リスク選好・許容度・残存リスク [1.2]
リスク登録簿とリスクの所有者 [1.2]
AIを導入する時のリスク [1.2]
規制と法律 [1.3]
ポリシー・標準・手順・ガイドライン [1.3]
フレームワークとガイドライン [1.3]
組織のポリシーの種類 [1.3]
AIもポリシーと法令の対象 [1.3]
技術的・管理的・物理的制御 [1.4]
制御の働き: 予防・検知・是正ほか [1.4]
制御の選び方と組み合わせ [1.4]
ISC2倫理規定 [1.5]
職業上の行動規範 [1.5]
デューケアとデューディリジェンス [1.5]

サンプルはここまでです

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 Principles [1.1/1.2/1.3/1.4/1.5]

第1章は、CCの出題で最大の24%を占める分野です。採点の対象になる問題は最低75問で、75問で数えると18問前後がここから出る計算です（CAT 方式のため、問題数は受験者ごとに変わります）。細目は次の5つです。

- 1.1 サイバーセキュリティの基本概念
- 1.2 リスク管理
- 1.3 ガバナンス
- 1.4 セキュリティ制御
- 1.5 専門家の倫理

後の章の認証、ネットワーク、インシデント対応は、すべてこの章の言葉を前提に問われます。定義を一語ずつ正確に持っていれば、後の章の問題で迷う場面が減ります。逆に、ここで言葉の境目があいまいなままだと、選択肢の言い換えに引っかかりかねません。

機密性・完全性・可用性 (CIA) [1.1]

CIA は、守る対象の情報について「何が守られていればよいか」を3つに分けた考え方です。機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) の頭文字を並べたもので、CIAトライアドとも呼びます。

機密性

(許可された者だけが読める)



完全性

可用性

(不正に変えられない) (必要な時に使える)

米国標準の FIPS 199 は、3つを次のように定義します。[^c1-1]

- **機密性:** 情報へのアクセスと開示に許可された制限を保つこと
- **完全性:** 情報が不適切に変更・破壊されるのを防ぐこと。真正性と否認防止を含む
- **可用性:** 情報に適時かつ確実にアクセスし、使えること

損なわれたものを見分ける

試験の中心は、場面を読んで「どれが損なわれたか」を判定する問題です。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。

起きたこと	損なわれたもの	具体例
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サービスへ社内資料を貼り付けた

起きたこと	損なわれたもの	具体例
許可のない変更、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の学習データへの不正な混入
必要な時に使えなかった	可用性	DoS攻撃、ランサムウェアでファイルが開けない、停電、機器の故障

守る制御も、性質ごとに決まっています。

守る性質	代表的な制御
機密性	暗号化、アクセス制御、データの分類
完全性	ハッシュ、デジタル署名、変更管理、入力値の検証、職務の分離
可用性	冗長化、バックアップ、無停電電源装置、DDoS対策

完全性とハッシュ

ハッシュは、データから固定長の短い値を計算する一方向の関数です。元のデータが1文字でも変わると、出てくる値はまるで別物になり、元の値と見比べても似たところはありません。次の値は Python の hashlib で実際に計算したSHA-256の先頭16桁です。

```
SHA-256("abc") = ba7816bf8f01cfea...
SHA-256("abd") = a52d159f262b2c6d...
```

最後の1文字が違っただけで、先頭からまったく違う値になります。保管時の値と今の値を比べて一致すれば、その間にデータは変わっていません。ハッシュが示すのは保管した時点からの変化だけで、保管した時点で既に誤っていた値の正しさは示しません。ハッシュの役割は改ざんの**検知**で、改ざんを防ぐ力はありません。暗号化でもありません。値から元のデータには戻せず、中身を隠す働きもないからです。「ハッシュ化で機密性を守る」という選択肢は誤りです。

ハッシュだけでは、誰が作ったかも分かりません。攻撃者がデータを書き換え、ハッシュも計算し直して置き換えれば、一致してしまうからです。ハッシュだけでは、この穴は埋まりません。埋めるのは、後で扱うデジタル署名です。

完全性には、データだけでなくシステムの完全性もあります。承認されていないソフトウェアが入った状態や、設定が勝手に変わった状態は、システムの完全性の損失です。AIでは、学習データに細工をしてモデルの判断をゆがめるポイズニング(汚染)が、完全性への攻撃にあたります。[^c1-2]

可用性と冗長化

可用性は使える時間の割合(稼働率)で表し、1年を8,760時間とすると、稼働率ごとの停止時間の上限は次のとおりです。

稼働率	1年で許される停止
99%	約87.6時間
99.9%	約8.76時間
99.99%	約52.6分

停止時間の上限は $8,760 \text{時間} \times (1 - \text{稼働率})$ で求め、たとえば99.5%なら、 $8,760 \times 0.005 = 43.8 \text{時間}$ です。9が1つ増えるごとに、許される停止時間は10

分の1に減ります。この差を埋めるのが冗長化で、同じ働きの機器や経路を複数用意し、1つが壊れても残りが引き継げるようにします。停電しても、無停電電源装置 (UPS) があれば機器はすぐには止まりません。UPS は、停電した時に電池から電気を送り、機器を一定時間動かし続ける装置です。

可用性を損なう事象は、攻撃ではありません。災害、停電、機器の故障、設定ミス、容量不足も含みます。攻撃では、次の2つの言葉を区別します。

- **DoS (サービス拒否) 攻撃:** 大量のリクエストでサービスを使えなくする攻撃
- **DDoS攻撃:** 複数の発信元から行うDoS攻撃

場面から判定する

実際の問題は、3つが混ざった場面が出るので、判定は「最も直接的に何が起きたか」で決めます。

ランサムウェアで業務ファイルが暗号化され、開けなくなった場面は、可用性の損失です。直接の問題は、業務ファイルを必要な時に使えなくなったことからです。攻撃者がさらに「払わなければ盗んだデータを公開する」と脅したなら、持ち出されたデータについては機密性の損失になります。問いが「最も直接的に」を聞いているのか、「すべて」を聞いているのかは、読み落としてはいけません。

営業担当が顧客リストの金額欄を誤って書き換えて保存した場面は、完全性の損失です。悪意の有無は関係しません。許可された人の誤操作でも、情報が正しくなくなれば、完全性は損なわれます。

暗号化したノートPCが盗まれた場面では、機密性は暗号化が守ります。ただし端末が手元から消えたので、そこにしかなかったデータは可用性を失います。バックアップがあれば復旧でき、これが可用性の制御です。1つの出来事が

複数の性質に響く例で、暗号化しているから全部安全という選択肢は成り立ちません。

複合の場面は、「最も直接的に」を基準に決めます(次の表)。

場面	最も直接的に損なわれたもの	理由
従業員が顧客名簿をUSBメモリにコピーし、電車に置き忘れた	機密性	許可のない第三者に読まれるおそれが生じた
夜間バッチの設定ミスで、本番データベースの金額列が上書きされた	完全性	データが正しくない値に変わった
給与システムのサーバが故障し、給与計算が3日止まった	可用性	必要な時に使えなかった
退職者のアカウントが残り、元従業員が社内資料を閲覧した	機密性	許可のない者が読んだ。認可の管理の不備が原因

問いが「どの制御がこの損失を防ぐか」の形なら、損なわれた性質に対応する制御を選びます。暗号化は機密性、ハッシュと署名は完全性、冗長化とバックアップは可用性です。アクセス制御のように、機密性と完全性の両方に効く制御もあります。

FIPS 199 は、CIAの損失が組織に与える影響を、次の3段階に分けます。[^c1-1]

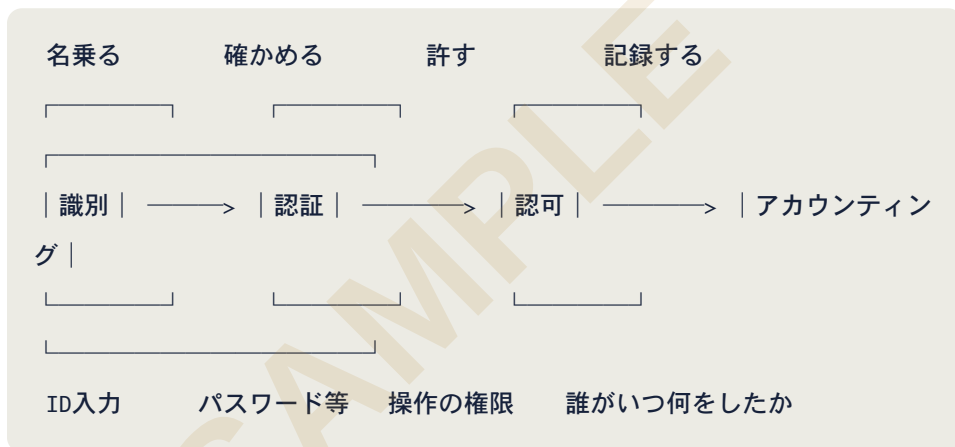
- 低: 限定的な悪影響
- 中: 重大な悪影響

- **高**: 深刻または壊滅的な悪影響

影響が高い情報ほど、強い制御を選びます。

認証・認可・アカウントिंग(AAA) [1.1]

AAA は、システムが人や機器を扱う時の働きを、認証 (Authentication)、認可 (Authorization)、アカウントिंग (Accounting) の3つに分けたものです。ここに、認証の前の段階である識別を加えて、4つの順序で理解します。



- **識別**: 利用者が自分のIDを名乗ること
- **認証**: 名乗った身元が正しいかを、パスワードや鍵などの認証子で確かめる処理[^c1-3]
- **認可**: 認証できた主体に、どの資源へどんな操作を許すかを与えること。認証の後に行う[^c1-4]
- **アカウントング**: 誰がいつ何をしたかを記録し、後から追跡できるようにすること。監査ログが土台になる[^c1-5]

順序は、識別、認証、認可、アカウントングです。認証が通っても、認可がなければ操作はできません。社員Aが正しいパスワードでログインできても、人事デ

一タへの権限を持たなければ、人事データは開けません。この場面で働かなかったのは、認可です。

この区別は場面で問われ、「ログインはできたが、ファイルが開けない」なら認可の問題、「ログインできない」なら識別か認証の問題、「誰が削除したか分からない」ならアカウンティングの問題です。

認証の3つの要素

認証に使う情報は、3種類に分かれます。

要素	意味	例
知識	知っているもの	パスワード、PIN、秘密の質問の答え
所有	持っているもの	スマートフォン、ICカード、ハードウェアトークン、ワンタイムパスワードの生成器
生体	本人の特徴	指紋、顔、虹彩、声

2種類以上の要素を組み合わせるのが**多要素認証(MFA)**です。^[^c1-6] 数えるのは要素の**種類**で、手順の回数ではありません。パスワードと秘密の質問の答えは、どちらも知識です。2つ使っても多要素にはならず、単要素を2回繰り返しただけです。パスワードとスマートフォンへのコード、パスワードと指紋は、種類が違うので多要素です。

MFAを使っている場合でも、安全が保証されるわけではありません。利用者をだましてコードを入力させるフィッシングや、承認の通知を連続で送って根負けさせる攻撃があります。MFAは強い制御ですが、他の制御と組み合わせて使います。

アカウントティングと共有アカウント

アカウントティングが成り立つ条件は、操作とそれを行った人が1対1で結びつくことです。1つのIDを数人で使い回す共有アカウントでは、ログに「adminが削除した」と残っても、誰が削除したかは分かりません。共有アカウントは、アカウントティングと、次に述べる否認防止の両方を弱めます。対策は、1人に1つの一意のIDを持たせることです。

否認防止 [1.1]

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、手段はデジタル署名とログです。
[^c1-7]

デジタル署名は、次の手順で働きます。[^c1-8]

- 1. 署名者が、データのハッシュを自分の秘密鍵で署名する
- 2. 受け取った側が、署名者の公開鍵で署名を検証する
- 3. 検証が通れば、署名者の身元と、署名後にデータが変わっていないことを確かめられる

検証が通らなければ、署名者が違うか、署名の後にデータが変えられたかを疑います。秘密鍵は署名者だけが持つので、署名者は後から否定しにくくなります。

隣概念と並べて区別します。

概念	守るもの	時点
認証	今この場の本人確認	操作の前
完全性	データが変わっていないこと	保管と転送の間

概念	守るもの	時点
否認防止	行為を否定できない証拠	操作の後

共通鍵による暗号化は、否認防止になりません。同じ鍵を持つ人が複数いて、誰が作ったのか区別できないからです。署名は、鍵が1人にしかないという前提で成り立ちます。

否認防止を支えるログは、改ざんできない形で残す必要があります。管理者が自分で消せるログは、証拠になりません。ログを別のサーバに転送する、書き込みだけを許す設定にする、といった制御で書き換えを防ぎます。

AIが行った操作も同じ扱いで、AIエージェントが人に代わってメールを送ったり設定を変えたりする場合は、人とは別のIDを割り当て、その操作をログに残します。そうしておかなければ、後から「AIが何をしたか」「誰の指示で動いたか」を追跡できません。

プライバシー [1.1]

プライバシーは、個人が、自分の情報の扱われ方をコントロールできることです。守る対象は個人を識別できる情報で、これを**PII (個人を特定できる情報)**と呼びます。PIIは、次の2つのどちらかにあたる情報です。[^c1-9]

- 単独で本人を識別・追跡できる情報: 氏名、生体情報
- 他の情報と結びついて、本人を特定できる情報

EUのGDPRは、識別された、または識別可能な自然人に関するあらゆる情報を「個人データ」と呼びます。[^c1-10] 住所や電話番号だけでなく、本人と結びつくIPアドレスやオンライン識別子も含まれます。

機密性との違い

機密性とプライバシーは近いものの、同じではありません。機密性は、情報へのアクセスを許可された者だけに制限することです。プライバシーは、個人が、自分の情報がどう集められ、使われ、共有されるかに関わる権利です。

ある会社が顧客の個人情報を暗号化し、アクセスできる従業員も絞っているとしします。機密性は守られていますが、顧客が同意した目的はメールマガジンの配信だけだったのに、その情報を無断で他社へ販売したなら、プライバシーは侵害されています。守る仕組みが働いていても、**同意と利用目的**に反した使い方が許されるわけではありません。

プライバシーを守る基本は、次の3つです。

- **最小化:** 必要な範囲だけ集める
- **目的の限定:** 集めた目的の範囲で使う
- **本人の同意:** 集める前と、目的を変える前に得る

AIとプライバシー

AIの学習データに個人情報が含まれる場合も、同じ考え方が当てはまります。学習データの安全性と完全性は、AIの出力の正確さと信頼性を左右します。個人情報を含むデータは、収集から保管、利用まで、保護と最小化が要ります。[^c1-11]

従業員が公開されているAIサービスに、顧客情報や社内の機密資料を入力する場面も出題されます。入力した情報は外部のサービスの管理下に置かれ、学習に使われる可能性があるため、機密性とプライバシーの両方に響きかねません。組織のポリシーで入力してよい情報の範囲を決め、利用者に伝えるのが対策です。

リスクの用語 [1.2]

リスク管理の問題は、用語の取り違えを突いてきます。7つの言葉を、洪水の例とITの例で区別します。

用語	意味	洪水の例	ITの例
資産	守る価値のあるもの	倉庫の商品	顧客データベース
脆弱性	脅威に悪用され得る弱点	堤防が低い	パッチ未適用のサーバ
脅威	悪影響を与え得る事象や状況	大雨	マルウェア、不正アクセス
脅威の主体	脅威を起こす者や原因	台風	攻撃者、内部の不満を持つ従業員
可能性	その事象の起きやすさ	年に1回起きる	公開された脆弱性は悪用されやすい
影響	起きた時の被害の大きさ	商品が全滅する	顧客情報が流出する
リスク	影響と可能性から測る不確かさ	洪水で商品を失う恐れ	流出が起きる恐れ

NISTは、脅威と脆弱性を次のように定義します。[^c1-12]

- **脅威:** 組織の運営や資産に悪影響を与え得る事象や状況
- **脆弱性:** 脅威に悪用され得る、システムや手順や管理上の弱点

リスクは、悪い出来事が起きた時の影響と、起きる可能性から測ります。脅威、脆弱性、資産の組み合わせで考えます。[^c1-13] 3つの関係から、次の性質が導かれます。

- 脆弱性があっても、それを悪用する脅威がなければ、リスクは低い
- 脅威が強くても、脆弱性が塞がれていれば、リスクは低い
- 資産の価値が低ければ、どちらがあっても影響が小さく、リスクは低い

間違えやすいのは脆弱性と脅威です。サーバにパッチが当たっていない状態は**脆弱性**で、それを悪用しようとする攻撃者や攻撃は**脅威**です。「攻撃者」を脆弱性と答えると誤りになります。情報漏えいが実際に起きた後の状態は、リスクではなく**インシデント**です。リスクはまだ起きていない不確かさであり、起きた後の状態を指しません。

リスク管理のライフサイクル [1.2]

リスク管理は一度やって終わりではなく、繰り返し回します。流れは、特定、評価、対応、監視・見直しの4段階で、監視の結果が次の特定に戻ります。特定では、守る資産と、脅威と脆弱性を洗い出して一覧にします。見直しを止めると、後から現れた脅威や弱点が一覧に入りません。



特定 —> 評価 —> 対応 —> 監視・見直し

(何が危ないか)(どれくらいか)(どうするか)(効いているか)

NIST SP 800-39 の枠組みは、リスクのフレーミング、評価、対応、監視の4つで、これを繰り返し回します。[^c1-14] CCの細目名「リスク管理のライフサイクル」は、この流れにあたります。手順の名前はNISTの文書ごとに範囲が違い、混ぜてはいけません。

手順	範囲	段階
SP 800-39 のリスク管理	組織全体	フレーミング、評価、対応、監視
SP 800-30 のリスク評価	評価の1段階	準備、実施、結果の伝達、評価の維持
SP 800-37 のRMF	システムへの適用	下の7ステップ

SP 800-30 の手順は、リスク管理の中の「評価」を細かく分けたものです。
[^c1-15] NIST RMF (リスク管理フレームワーク) は、システムに適用する7つのステップで、次の順に進みます。[^c1-16]

- 1. Prepare (準備)
- 2. Categorize (システムの分類)
- 3. Select (管理策の選択)
- 4. Implement (管理策の実装)
- 5. Assess (管理策の評価)
- 6. Authorize (運用の認可)
- 7. Monitor (運用中の監視)

順序を並べ替える問題が出るので、英単語の頭文字ではなく流れて覚えます。
まず準備して、システムを分類し、必要な管理策を選び、実装し、効いているか評価し、運用を認可し、運用中は監視する流れです。

リスク評価: 定性と定量 [1.2]

リスク評価は、リスクの大きさを測って優先順位を付ける作業です (SP 800-30)。測り方は3つあり、NISTも定量的、定性的、半定量的を挙げています。
[^c1-17]

方法	測り方	強み	弱み
定性的	高・中・低などの段階で測る	速い。数字がなくてもできる	評価者の主観が入る
定量的	金額や確率の数字で測る	費用対効果を数字で比べられる	根拠になるデータが要る
半定量的	0～100などの点数の尺度で測る	両者の中間	点数が正確な数字に見える

可能性×影響のマトリクス

定性評価で最もよく使うのは、可能性と影響を3段階で見て掛け合わせる表です。低を1、中を2、高を3として積を出すと、次のようになります。

	影響 低(1)	中(2)	高(3)
可能性 低(1)	1	2	3
可能性 中(2)	2	4	6
可能性 高(3)	3	6	9

右下の9が最優先で、高×高にあたります。左上の1は、最も後回しにできます（低×低）。点数の高い順に対応を決めるのが、優先順位づけです。[^c1-18]可能性が低くて影響が高いものは3で、可能性が高くて影響が低いものも3です。同じ点でも、中身が違うことは見落とせません。

定量評価の計算

金額で測る定量評価では、次の式を使う方法があります。

- **資産価値 (AV):** 資産の金額
- **曝露係数 (EF):** 1回の事象で資産の何割を失うか

- **単一損失予測 (SLE):** $AV \times EF$
- **年間発生率 (ARO):** 1年に何回起きるか
- **年間損失予測 (ALE):** $SLE \times ARO$

例を計算します。資産価値が200万円のシステムで、1回の事故で25%を失い、事故が2年に1回 ($ARO=0.5$) 起きるとします。SLEは200万円 $\times$ 0.25で50万円、ALEは50万円 $\times$ 0.5で25万円です。

対策を入れて事故が $ARO=0.1$ に減るなら、新しいALEは50万円 $\times$ 0.1で5万円になり、減る額は年20万円です。この対策の年間費用が30万円だと、20万円の効果に30万円かかるので、10万円の赤字になり、導入しても割に合いません。費用が12万円なら8万円の黒字になり、**対策費用が減らせる損失より小さければ、導入する価値がある**と判断します。

リスクへの対応:回避・受容・軽減・移転 [1.2]

リスクの大きさを測ったら、どう扱うかを決めなければなりません。NISTは、受容、回避、軽減(低減)、共有または移転の4つを挙げており、[1-14] CCでは「回避・受容・軽減・移転」と覚えます。

対応	中身	具体例
回避	リスクの原因となる活動をやめる	危険な機能の提供をやめる、リスクの高い地域での営業をやめる
受容	何もせず、起きた時の損失を受け入れる	対策費用が損失より大きく、許容できる範囲なので、そのままにする
軽減	対策を入れて可能性が影響を下げる	パッチを当てる、MFAを導入する、バックアップを取る

対応	中身	具体例
移転	損失の負担を第三者に渡す	サイバー保険に入る、運用を委託して契約で補償を求める

選び方の目安は、まず影響と可能性が許容できるかを見ることです。許容度の範囲に収まるなら、受容します。収まらなくても、費用をかけて下げられるなら軽減、損失の負担だけ外へ出したいなら移転、活動自体の価値が小さいなら回避です。

迷いやすいのは、移転と回避、移転と軽減の境目です（保険が典型）。保険に入っても、事故の可能性も影響の大きさも変わりません。変わるのは損失を誰が負担するかで、これが移転です。対策で可能性か影響を下げれば、軽減になります。

移転しても、情報を守る責任や評判への影響は組織に残ります。「外部委託したので責任もなくなった」という選択肢は誤りです。リスクは、費用を渡せても、責任までは渡せません。

場面で選び方を確かめます。**場面A:** 新サービスで健康データを集める機能を計画したが、法令に対応する費用が機能の利益を上回る。この機能は提供をやめるのが回避にあたり、リスクの原因である活動そのものがなくなります。**場面B:** 社内の古い備品管理システムに脆弱性が見つかったが、扱うデータは備品の数だけで、止まっても業務に支障がない。影響が小さく許容度の範囲なので、対策費用をかけずに受容します。**場面C:** 大規模なDDoS攻撃による売上の損失が心配で、自社の設備だけでは防ぎきれない。DDoS対策のサービスを契約するのは軽減、損失を補償するサイバー保険に入るのは移転で、両方を組み合わせることもあります。**場面D:** MFAを導入した後も、残存リスクが

許容度を超えている。受容はできないので、追加の軽減策を検討します。軽減策に費用が見合わないなら、移転か、その活動の回避に進みます。

リスク選好・許容度・残存リスク [1.2]

リスク対応の判断に使う言葉が、4つあります。

- **リスク選好**: 組織が目標を追うために、進んで取るリスクの全体的な量や姿勢。新規事業に積極的か、慎重かという経営の方針にあたる
- **リスク許容度**: 組織が受け入れてよいと考えるリスクの水準や不確実さの度合い。選好の範囲のなかの具体的な線引き[^c1-19]
- **内在リスク**: 対策をとる前の、もともと持っているリスク
- **残存リスク**: 対策をとった後になお残るリスク[^c1-20]

選好は方向、許容度は具体的な限度と覚えます。内在リスクから対策の効果を引いたものが、残存リスクです。残存リスクは、許容度と照らして受容するかを決めます。

残存リスクが許容度を超えているなら、受容できません。追加の対策か、移転か、回避を選びます。許容度以下なら受容して、監視を続けます。残存リスクをゼロにする選択肢は、費用の面で現実的でないので誤りです。

リスク登録簿とリスクの所有者 [1.2]

リスク登録簿は、特定したリスクを1つずつ記録する一覧表で、主な項目は次のとおりです。

- リスクの説明と、関係する資産
- 脅威と脆弱性
- 可能性、影響、点数

- 対応方針 (回避・受容・軽減・移転) と、その進み具合
- リスクの所有者
- 見直しの日付

リスクの所有者は、そのリスクを管理し、対応に責任を持つ人です。セキュリティ担当者とは限らず、そのリスクの元になる業務を担う部門の責任者が就くのが原則です。顧客データのリスクなら、データを使う部門の責任者が所有者になり、セキュリティ部門が所有者になるわけではありません。セキュリティ部門は、助言と支援をします。

登録簿は、状況が変わるたびに更新します。重要なリスクは、経営層に報告します。受容するかどうかの最終判断も、経営層の役割です。所有者が決まっていないリスクは、誰も対応しないまま残りがねません。そのため、リスクを登録簿に載せる時は、まず所有者を決めます。

AIを導入する時のリスク [1.2]

AIを導入すると、既存の資産とは違うリスクが加わります。登録簿に載せて、通常のリスクと同じ手順で管理します。

- 学習データを汚染して判断をゆがめる攻撃 (ポイズニング): 完全性のリスク [^c1-2]
- 学習に使ったデータや、入力されたデータが外へ漏れること: 機密性とプライバシーのリスク
- 学習データの偏りで、出力が特定の人々に不利になること: 公平性のリスク

NISTのAIリスク管理フレームワークは、信頼できるAIの特性として、妥当性と信頼性、安全、セキュリティとレジリエンス (回復力)、説明責任と透明性、説明

可能性と解釈可能性、プライバシーの強化、公平性(有害な偏りの管理)を挙げ、これらの観点でAIのリスクを測り、管理するとしています。[^c1-21] 時間が経ってモデルの精度が落ちる劣化も、登録簿に載せる対象です。

規制と法律 [1.3]

ガバナンスは、組織がセキュリティを経営の方針に沿って動かし、責任を明らかにする仕組みで、その外側の枠になるのが規制と法律です。

- **法律:** 国や地域の議会が定める
- **規制:** 法律に基づいて、監督当局や業界の団体が定める

どちらも**外から課される義務**で、守らなければ罰金や営業停止などの罰則があります。組織が自分で決める方針や手順とは、ここが違います。組織は、法令を選んで守ることはできません。

GDPR

GDPR (EU一般データ保護規則) は、EUの個人データ保護の規則です。データの処理には、第5条の原則が定められています。[^c1-22]

原則	意味
適法・公正・透明	適法な根拠があり、本人に分かる形で処理する
目的の限定	決めた目的の範囲で使う
データの最小化	目的に必要な範囲だけ集める
正確性	正確に保ち、誤りは直す
保存の制限	必要な期間を過ぎたら持たない

原則	意味
完全性と機密性	適切な安全管理措置で、不正な処理や紛失、破壊から守る
アカウントビリティ	上の原則を守っていることを示せる

GDPRで押さえておく数字は、制裁金の上限と通知の期限です。

違反の制裁金は、2段階あります。

- **重い違反** (処理の原則、本人の権利、第三国への移転など): 最大2,000万ユーロ、または全世界の年間売上高の4%のうち**高い方**^[^c1-23]
- **軽い違反** (管理者の義務や安全管理など): 最大1,000万ユーロ、または年間売上高の2%のうち**高い方**

売上高が1億ユーロの会社なら、4%は400万ユーロにしかならず、2,000万ユーロのほうが高いので、上限は2,000万ユーロです。売上高が10億ユーロなら、4%は4,000万ユーロで、こちらが上限になります。「高い方」を取る点は、計算の問題で試されます。

個人データの侵害は、遅滞なく、可能な場合は**知ってから72時間以内**に監督機関へ通知します(自然人の権利と自由へのリスクが生じそうにない侵害は除きます)。72時間を過ぎても、通知が免除されるわけではありません。遅れた理由を添えます。^[^c1-24] たとえば10月23日の9時30分に侵害に気づいたなら、期限は10月26日の9時30分です。数え始めるのは気づいた時刻で、侵害が起きた時刻ではありません。委託先(処理者)は、侵害を知ったら遅滞なく管理者へ知らせます。

本人には**削除権(忘れられる権利)**があり、一定の場合に自分の個人データの消去を求められます。^[^c1-25] 本人の求めを、組織の都合だけで無視する

ことはできません。

HIPAA

HIPAAは、米国の医療情報を守る法律です。対象は、医療機関や保険者などの「対象事業体 (covered entity)」と、その業務を受託する「業務提携者 (business associate)」です。守る情報は、個人を識別できる医療情報で、**保護対象保健情報 (PHI)** と呼びます。^[^c1-26] 医療情報が対象という点で、個人データ全般を対象にするGDPRとは範囲が違います。

業種や地域によって適用される法令が変わるため、1つの法令だけで足りるとは限りません。場面に「医療情報」とあればHIPAA、「EU居住者の個人データ」とあればGDPRを疑います。どちらも法令なので、従う義務があり、組織の方針で緩められません。

ポリシー・標準・手順・ガイドライン [1.3]

組織内の文書は、抽象度の高い順に並べると階層になります。

方針（ポリシー）	— 何を守るか、誰が責任を持つか	（経営層が承認）
標準（スタンダード）	— どの水準で守るか	（必須の具体的な要件）
手順（プロシージャ）	— どのやり方で実行するか	（操作の順序）
ガイドライン	— 守ると望ましい助言	（強制ではない）

方針は何を守るかを経営の言葉で示し、標準は守る水準を具体的に定め、手順は実際の操作の順序を書きます。方針から手順へ向かうほど具体的になり

ます。方針は変わりにくく、手順は技術の変化に合わせて頻繁に変わります。

文書	内容	強制力	例
方針	目的、範囲、責任	必須	「情報を分類し、分類に応じて保護する」
標準	守る水準、要件	必須	「パスワードは12文字以上にする」
手順	作業の順序	必須	「退職者のアカウントを無効にする手順」
ガイドライン	推奨される進め方	任意	「安全なパスワードの作り方の助言」

ガイドラインだけが強制ではなく、従わなくても違反にはなりません。方針、標準、手順には、従う義務があります。場面では、文書の種類を当てる形で出ます。「経営層が承認した、情報を守る基本の考え方」は方針、「パスワードは12文字以上」という水準は標準、「手順書」は手順です。「状況に合わせて参考にする助言」はガイドラインです。

組織の標準と、ISOなどの外部規格

「標準(規格)」という言葉は、2つの意味で使われるので、取り違えてはいけません。組織内の標準は、通常はその組織の中で必須です。[^c1-27] NISTも、国や国際機関の規格と取り違えないよう、注意を添えています。ISOのような外部の規格は、それ自体に法的な強制力はありません。組織が採用して認証を受けたり、契約で求められたりして、初めて効力を持ちます。

まとめて区別すると、法令は外から課される義務、外部規格やガイドラインは推奨、方針は組織の決めごと、手順は具体的な操作の順序です。[^c1-28] こ

の区別が曖昧なままでは、文書の種類を問う問題は解けません。

フレームワークとガイドライン [1.3]

フレームワークは、セキュリティ対策を体系的に進めるための枠組みで、組織が自分に合わせて使います。

NIST CSF 2.0

NISTサイバーセキュリティフレームワーク (CSF) 2.0は、6つの機能で構成します。[^c1-29]

機能	内容	場面の手がかかり
Govern (統治)	リスク管理の戦略、期待、方針を定め、伝える。2.0で追加	方針や役割を決める
Identify (特定)	組織の現在のリスクを理解する	資産とリスクを洗い出す
Protect (防御)	リスクを管理する安全策を使う	対策を入れる、教育する
Detect (検知)	攻撃や侵害の可能性を見つけて分析する	ログを監視して異常に気づく
Respond (対応)	検知したインシデントに対処する	インシデントを封じ込める
Recover (復旧)	影響を受けた資産と業務を元に戻す	バックアップから復元する

Govern は2.0で新しく加わった機能で、図の中央に置かれ、ほかの5つの結果を方向づけます。[^c1-36] CSFには、目標に合わせて選んだ内容をまとめるプロファイルと、取り組みの成熟度を表すティア (Partial、Risk Informed、

Repeatable、Adaptive) もあります。ティアは Tier 1 の Partial から Tier 4 の Adaptive へ、成熟度が上がる順に並びます。

CIS Controls

CIS Controls v8は、18の重要なセキュリティ管理策で構成し、[^c1-30] 資産の棚卸し、データ保護、アカウント管理、ログ管理、マルウェア対策、データ復旧、インシデント対応管理などが並びます。組織の規模と資源に応じて優先度を定める仕組みがあります (実装グループ IG1、IG2、IG3)。

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**を定めた国際規格で、認証の対象になります。ISO/IEC 27002は、情報セキュリティの管理策を説明する**手引き(ガイダンス)**です。[^c1-31] 27001は「ISMSをこう作る」という要求、27002は「管理策の具体的な考え方」という手引きです。認証の対象になるのは27001のほうです (認証を受けると言う時は27001を指す)。

位置づけを3つ並べます。

- **CSF:** リスク管理を6つの機能の順に整理する枠組み
- **CIS Controls:** 優先順位の付いた、具体的な18の管理策の一覧
- **ISO/IEC 27001:** 認証を受けられる管理体制 (ISMS) の規格

いずれも法律ではなく、組織が自主的に採用します。採用していなくても、法令違反にはなりません。

組織のポリシーの種類 [1.3]

組織が定めるポリシーは、対象によって種類があります。

- **データの取り扱いポリシー**: 情報を分類し、分類ごとに保管、共有、廃棄のルールを定める
- **パスワードポリシー**: 長さ、複雑さ、変更の条件、使い回しの禁止を定める
- **許容される利用ポリシー (AUP)**: 会社の機器やネットワークを何に使ってよいか、してはいけないかを定める
- **BYODポリシー**: 私物の端末を業務に使う条件 (登録、暗号化、紛失時の遠隔消去など) を定める
- **プライバシーポリシー**: 個人情報情報をどう集め、使い、守るかを本人に示す
- **変更管理ポリシー**: システムの変更を、申請、審査、承認、記録の手順を踏んで行わせる

場面では、ポリシーの名前を当てる形で出ます。私物のスマートフォンで社内メールを見たい従業員に条件を示すのはBYOD、会社のPCで私的なサイトを見てよいかを決めるのはAUPです。承認なしにサーバの設定を変えて障害が起きた場合は、変更管理ポリシーの違反です (承認の手順を飛ばしたため)。

AIもポリシーと法令の対象 [1.3]

AIを使うことにも、既存のポリシーと法令がそのまま及び、個人データを扱うならGDPRなどの対象です。AIが出した判断の理由を説明できること (透明性) と、特定の人々に不利にならないこと (偏りのない扱い) が求められます。
[^c1-21]

組織は、AIの利用範囲、入力してよい情報、出力の確認方法をポリシーに定めます。AUPやデータの取り扱いポリシーに含めるのが基本です。AIだからといって、例外にはなりません。

技術的・管理的・物理的制御 [1.4]

セキュリティ制御は、リスクを下げるために入れる対策の総称です。実装の方法によって、3つに分けます。

技術的制御 (システムの機能)	管理的制御 (人とルール)	物理的制御 (物理的に守る)
暗号化	ポリシー	施錠
ファイアウォール	研修	入退室バッジ
アクセス制御	身元確認	監視カメラ
MFA・ログ	職務の交替	警備員

- **技術的制御** (論理的制御とも呼ぶ): システムの機能で実現する制御。暗号化、ファイアウォール、アクセス制御リスト、多要素認証、ログ監視が例 [^c1-32]
- **管理的制御**: 人とルールで実現する制御。方針、手順、教育、採用前の身元確認、職務の交替、強制休暇が例
- **物理的制御**: 物理的に守る制御。施錠、入退室管理、監視カメラ、フェンス、警備員が例

ログは、システムが出来事を記録して後から追跡できるようにする技術的制御です。職務の交替(担当を定期的に入れ替える)と強制休暇(一定期間は必ず休ませる)は、管理的制御です。担当が変わると、前任者が隠していた不正が表に出るので、どちらも不正の検知に効きます。

共連れ(前の人について扉を通り抜けること)は、物理的制御の定番の論点で、防ぐには、1人ずつしか通れないマントラップ(二重扉)や回転式の扉を使います(共連れ防止)。

NISTのSP 800-53は、管理策を「AC-2」のように、ファミリーの略称と番号で整理しています。[^c1-32] 略称は、AC(アクセス制御)、AT(意識向上と教育)、AU(監査と説明責任)、CM(構成管理)、PE(物理的・環境的保護)、PS(人員のセキュリティ)などです。略称を見れば、その管理策が技術的、管理的、物理的のどれに近いかを推測できます。

最小権限と職務の分離

2つの原則は、制御の設計で繰り返し出るので、取り違えてはいけません。**最小権限**は、業務に必要な最小限の権限だけを与える原則です。**職務の分離**は、不正や誤りを防ぐために、1つの業務を複数の人に分け、1人で完結させないことです。たとえば、支払いの申請者と承認者を別の人にします。2人が結託しない限り、不正は通りません。どちらも管理的制御ですが、システムのアクセス権限として実装される場合もあります。[^c1-32]

見分けのコツ

同じ対策でも、見方によって種類が変わります。種類は「何が実現しているか」で決めます。

パスワードを12文字以上にするという決まりは、文書に書けば管理的制御、システムの設定で強制すれば技術的制御です。研修は教育なので管理的制御の

代表で、ログを取る仕組みは技術的制御です。

AIシステムも、技術、管理、物理の制御を組み合わせる点は変わりません。データセンターにあるGPUサーバには、入退室管理や施錠のような物理的制御も要ります。[^{^c1-11}]

制御の働き：予防・検知・是正ほか [1.4]

制御は、実装の方法とは別に、**働き**でも分類します。

働き	役割	例
予防	起きる前に止める	ファイアウォール、施錠、MFA、アクセス制御
検知	起きたことに気づく	ログの監視、監視カメラ、侵入検知、強制休暇
是正	起きた被害や見つかった欠陥（脆弱性・設定の誤り）を直す	パッチの適用、感染端末の隔離、不正アカウントの無効化
抑止	「やめよう」と思わせる	警告の看板、監視カメラがあること、懲戒の規定
補償	本来の制御の代わりに別の策で補う	MFAを入れられない古い機器を隔離し、通信を監視する
復旧	平常の状態に戻す	バックアップからの復元、代替拠点への切り替え

予防は起きる前に止め、検知は起きたことに気づき、是正は被害を元に戻します。本来の策ができない時は、補完的な管理策が別の策で代わりを務めます。[^{^c1-32}]

実装の種類と働きを掛け合わせる

ひとつの対策には、実装の種類と働きの両方があります。次の表は、よく出る組み合わせです。

対策	実装の種類	主な働き
ファイアウォール	技術的	予防
侵入検知システム	技術的	検知
バックアップからの復元	技術的	復旧
研修	管理的	予防
強制休暇	管理的	検知
監視カメラ	物理的	検知 (抑止にもなる)
施錠	物理的	予防
警備員	物理的	予防、抑止

監視カメラは、映像に残して後から確認できるので、検知にあたります。カメラがあるのを見て思いとどまらせる効果は、抑止です。問題文が何を問うかで、答えは1つに決まります(検知か抑止か)。「事件の後に確認できる」とあれば検知、「設置してあるだけで悪事を思いとどまる」とあれば抑止を選びます。

制御の選び方と組み合わせ [1.4]

1つのリスクに、種類の違う制御を重ねるのが基本です。1つの制御は破られる可能性があり、その時にもう1つが止めるので、この重ね方を**多層防御**と呼びます。物理の面でも、入口に守衛、鍵、バッジ、マントラップを重ねます(どれか1つでは足りません)。^[^c1-32]

場面で考えます。サーバ室に権限のない人が入り込むのを防ぎたい場合です。次のように重ねます。

- 入退室バッジのリーダーを扉に付ける: 物理的な予防
- 扉をマントラップにして、1人ずつしか通れなくする: 物理的な予防 (共連れ対策)
- 入室の記録を残して、後から確認できるようにする: 技術的な検知
- 入室できる人を定めて、研修する規定を置く: 管理的な予防

バッジを持つ人の後ろについて入る共連れには、バッジのリーダーだけでは弱いので、マントラップを足します。こうして物理、技術、管理の制御が重なり、1つが破られても残りが働きます。

補償的制御の使いどころ

本来入れるべき制御が、技術の都合や費用で入れられないことがあり、製造設備の古い制御機器がMFAに対応していない場合が典型です。MFAを入れる代わりに、その機器を他のネットワークから分離し、アクセスできる端末を限定し、通信を常時監視するのが補償的制御で、目的であるアクセスの保護を別の手段で満たします。

補償的制御は、本来の制御より弱くてよいわけではありません。NIST SP 800-53 は、補償的制御を、本来の管理策の代わりに使い、同等か、それに匹敵する保護を与える管理策と定義しています。「対応できないので何もしない」は補償になりません。

制御を選ぶ時は、リスクの大きさ、制御の費用、運用の負担をあわせて見ます。守る資産の価値より高い制御は、釣り合いません。前に見た費用対効果の考え方と同じです。

ISC2倫理規定 [1.5]

ISC2倫理規定は、ISC2の認定資格を持つ者が守る行動の基準で、前文と4つの規範からできています。前文は、社会と公共の利益、依頼主への義務、互いへの義務を守るために、高い倫理基準に従うことを求めています。規定を厳守することは、認定を維持する条件です。[^c1-33]

4つの規範は次のとおりです。

1. 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
2. 誠実に、正直に、公正に、責任をもって、適法に行動する
3. 依頼主 (principals) に勤勉かつ有能なサービスを提供する
4. 専門職を前進させ、守る

依頼主 (principals) は、認定者を雇う雇用主や、業務を頼む顧客のことです。

順序には意味がある

ISC2 の倫理規定のページには、規範どうしの優先順位を定める文はありません。[^c1-33] 規範は社会、自分の誠実さ、依頼主、専門職の順に並んでおり、場面問題では、先に並ぶ規範を重く見て判断します。公共の安全を守る規範1を、依頼主への義務を定める規範3より重く見るのがその例です。覚え方は、外側から内側へ向かう順で、社会、自分の誠実さ、依頼主、専門職の順に並んでいます。

順序そのものを問う問題は、並べ替えや、場面から規範を選ぶ形で出ます。「依頼主のため」と答えたい場面でも、公共の利益や違法性が絡めば、規範1か2が上に来ます(規範3は下)。

苦情の申し立て

倫理規定の違反について、ISC2に苦情を申し立てるルールも定められており、苦情を出せる人は規範によって異なります。

規範	苦情を出せる人
I・II	一般の人
III	依頼主だけ
IV	ほかの専門職（資格や免許を持ち、倫理規定に従う人）だけ

苦情は書面で、宣誓供述書の形で出します。申し立てる側は、まず違反されたとする規範を特定し、それを書いた宣誓供述書をまとめてから ISC2 に出します。[^c1-33] 苦情を扱うのは、規定の適用を監督する常設の倫理委員会で、審査を助ける役割です。委員会は、自分で調査を行う機関ではありません。

場面の判断

規範どうしがぶつかる場面や、違反を見た場面が、難しい問題の中心です。判断の基準は、規範の順序と、「適法か」「誠実か」の2点です。

上司が違法な指示を出した場面。顧客データを、本人の同意なく外部へ売るよう指示された、とします。規範3は依頼主（雇用主）に尽くすことを求めますが、規範2は適法に行動することを求めます。先に並ぶ規範2を重く見て、指示には従いません。違法な指示を断り、必要なら上位の部署や法務へ報告するのが正しい動きです。

依頼主の利益と公共の安全が衝突する場面。契約先の工場で、制御システムの重大な欠陥が見つかったとします。依頼主は公表したくありません。公共の安全に関わるなら、先に並ぶ規範1を規範3より重く見ます。安全に関わる事

実を隠さず、適切な当局や関係者へ伝える方向で動きます。守秘は大切ですが、公共の安全よりは下に来ます。

同僚の違反を見た場面。同僚が、受験者に試験問題を横流ししていると知ったとします。規範4は、専門職の信頼を守ることを求めます。見て見ぬふりはできず、まず適切な窓口 (ISC2の倫理委員会や上司) へ報告します。身内をかばう判断は、最も直接には規範4に反します。

利益相反の場面。評価を依頼された製品の販売会社から、謝礼を受け取っているとします。評価の公正さを損ねるおそれがあるので、規範2に反します。利益相反は、開示するか、その評価から外れます。黙って続けるのは許されません。

職業上の行動規範 [1.5]

倫理規定のほかに、組織が定める倫理方針と、専門家としての行動規範があります。中心は3つです。

- **守秘:** 業務で知った情報を、許可なく他に漏らさない
- **誠実:** 事実を偽らず、利益のために判断をゆがめない
- **能力の範囲で働く:** 自分に力のない仕事を、力があるかのように引き受けない

足りない時は、断るか、支援を求めます。依頼主に「勤勉かつ有能な」サービスを提供する規範3が根拠です。

組織の倫理方針は、倫理規定より具体的な、日々の行動を定める文書です。利益相反の申告、贈答品の受け取りの上限、通報窓口の使い方などが入ります。方針が倫理規定より厳しいなら、組織の方針も守らなければなりません。規定を満たしていても、方針に違反すれば、組織の中では違反になります。

デューケアとデューディリジェンス [1.5]

2つの言葉は似ていて、取り違いやすい組です。

- **デューディリジェンス**: リスクを事前に調べて確かめる調査。「調べる」側 [^c1-34]
- **デューケア(善良な管理者の注意義務)**: 組織が合理的な保護策を実際に実行すること。「やるべきことをやる」側[^c1-35]

	デューディリジェンス	デューケア
意味	調べて確かめる	保護策を実行し続ける
時点	実行の前	実行の中
例	クラウド事業者の管理体制を契約前に調べる	契約後に、決めた管理策を運用し、監視する

覚え方は、diligence の「調査」と、careの「実行」です。調査だけして実行しなければ、注意義務は果たせていません。

AIを導入する時の上層部の責任も、同じ形です。導入前に、AIが使うデータ、偏り、漏えいのリスクを調べます(デューディリジェンス)。導入後は、利用ルールを定めて監督を続けます(デューケア)。リスクが高いと分かっているが何もしなければ、注意義務を怠ったことになります。AIの導入では、透明性と偏りのなさが求められ、これを守ることが倫理規定の遵守にもつながります。
[^c1-21] 透明性は、AIが何を根拠に判断したかを説明できること、偏りのなさは、特定の集団に不利な結果を出さないことで、どちらも欠かせません。

サンプルはここまでです

続き(第2章～巻末)は、ISC2 CC 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

ISC2 Certified in Cybersecurity (CC) 学習用テキスト(無料サンプル)

版

2026年10月版(ISC2 公式 Certified in Cybersecurity (CC) Certification Exam Outline
(Effective Date: September 1, 2026・v01/2026・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、Certified in Cybersecurity (CC) 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。