Q0001 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：基礎

「機密性・完全性・可用性／脅威・脆弱性」のうち「CIA」を確認する誤答分析で、学習者が候補「情報が正確で、意図しない変更や破壊がない状態を保つこと。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．完全性の説明である。
イ．機密性は、情報が許可されていない者へ開示・利用されないようにする性質である。
ウ．可用性の説明である。
エ．機密性の目的と反する。

答え・解説 正答：ア

ア：この説明は誤答候補「情報が正確で、意図しない変更や破壊がない状態を保つこと。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「認可された者だけが情報へアクセスできる状態を確保すること。」に対応するため、誤答候補「情報が正確で、意図しない変更や破壊がない状態を保つこと。」の問題点を直接説明していない。
ウ：この説明は別候補「必要なときに情報やシステムを利用できる状態を保つこと。」に対応するため、誤答候補「情報が正確で、意図しない変更や破壊がない状態を保つこと。」の問題点を直接説明していない。
エ：この説明は別候補「情報を必ず公開し、誰でも参照できるようにすること。」に対応するため、誤答候補「情報が正確で、意図しない変更や破壊がない状態を保つこと。」の問題点を直接説明していない。

総合解説：誤答候補「情報が正確で、意図しない変更や破壊がない状態を保つこと。」について、誤りの内容を説明できることが重要である。完全性の説明である。

対象：2026年度 / 基準日 2026-09-04

Q0002 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：基礎

「機密性・完全性・可用性／脅威・脆弱性」のうち「CIA」を、正答の根拠まで理解できているか確認する。候補「権限のない利用者がデータベースの振込先口座を改ざんした。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．主に可用性の問題である。
イ．完全性は情報や処理結果が正確かつ完全で、許可なく変更・破壊されていない性質を指す。
ウ．主に機密性の問題である。
エ．可用性を高める対策である。

答え・解説 正答：イ

ア：この説明は別候補「システム停止で正規利用者が業務画面を開けない。」に対応するため、正答候補「権限のない利用者がデータベースの振込先口座を改ざんした。」の根拠にはならない。
イ：この説明は正答候補「権限のない利用者がデータベースの振込先口座を改ざんした。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「機密文書が外部へ漏えいした。」に対応するため、正答候補「権限のない利用者がデータベースの振込先口座を改ざんした。」の根拠にはならない。
エ：この説明は別候補「バックアップサイトへ切り替えてサービスを継続した。」に対応するため、正答候補「権限のない利用者がデータベースの振込先口座を改ざんした。」の根拠にはならない。

総合解説：正答候補「権限のない利用者がデータベースの振込先口座を改ざんした。」を選ぶ根拠は次のとおりである。完全性は情報や処理結果が正確かつ完全で、許可なく変更・破壊されていない性質を指す。

対象：2026年度 / 基準日 2026-09-04

Q0003 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：基礎

「機密性・完全性・可用性／脅威・脆弱性」の「CIA」について、候補「重要サーバを冗長化し、障害時に別系統へ切り替えられるようにする。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．主に機密性の対策である。
イ．主に完全性確認の対策である。
ウ．冗長化やフェイルオーバは、必要なときにサービスを利用可能に保つ可用性向上策である。
エ．可用性向上策ではなく危険である。

答え・解説 正答：ウ

ア：この説明は別候補「データを暗号化し、復号鍵を権限者だけに配布する。」に対応するため、正答候補「重要サーバを冗長化し、障害時に別系統へ切り替えられるようにする。」の根拠にはならない。
イ：この説明は別候補「ファイルのハッシュ値を比較して改ざんを検知する。」に対応するため、正答候補「重要サーバを冗長化し、障害時に別系統へ切り替えられるようにする。」の根拠にはならない。
ウ：この説明は正答候補「重要サーバを冗長化し、障害時に別系統へ切り替えられるようにする。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全利用者に同じ管理者パスワードを共有する。」に対応するため、正答候補「重要サーバを冗長化し、障害時に別系統へ切り替えられるようにする。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。冗長化やフェイルオーバは、必要なときにサービスを利用可能に保つ可用性向上策である。

対象：2026年度 / 基準日 2026-09-04

Q0004 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：標準

「機密性・完全性・可用性／脅威・脆弱性」の「脅威と脆弱性」を復習している学習者が、候補「その弱点を探索して侵入を試みる攻撃者」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．これは影響である。
イ．保護対象となる資産である。
ウ．脆弱性は攻撃や事故に悪用され得る弱点であり、設定不備や弱い認証情報は代表例である。
エ．攻撃者は脅威源である。

答え・解説 正答：エ

ア：この説明は別候補「侵入成功によって顧客情報が漏えいする被害」に対応するため、誤答候補「その弱点を探索して侵入を試みる攻撃者」の問題点を直接説明していない。
イ：この説明は別候補「顧客情報を扱うWebサービス自体」に対応するため、誤答候補「その弱点を探索して侵入を試みる攻撃者」の問題点を直接説明していない。
ウ：この説明は別候補「不要な管理ポートの公開と初期パスワードの放置」に対応するため、誤答候補「その弱点を探索して侵入を試みる攻撃者」の問題点を直接説明していない。
エ：この説明は誤答候補「その弱点を探索して侵入を試みる攻撃者」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「その弱点を探索して侵入を試みる攻撃者」については、何が誤りかを明確にした上で正しい概念へ戻す。攻撃者は脅威源である。

対象：2026年度 / 基準日 2026-09-04

Q0005 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：標準

「機密性・完全性・可用性／脅威・脆弱性」のうち「攻撃対象領域」を確認する誤答分析で、学習者が候補「全てのサービスを同じ強権限アカウントで実行する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．侵害時の影響を拡大する。
イ．公開機能を最小化すると、攻撃者が利用できる入口や脆弱な機能の数を減らせる。
ウ．攻撃対象領域を広げる。
エ．検知・追跡能力を低下させる。

答え・解説 正答：ア

ア：この説明は誤答候補「全てのサービスを同じ強権限アカウントで実行する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「利用しないサービスやポートを停止し、必要な機能だけを公開する。」に対応するため、誤答候補「全てのサービスを同じ強権限アカウントで実行する。」の問題点を直接説明していない。
ウ：この説明は別候補「利用予定のない管理機能も全て公開しておく。」に対応するため、誤答候補「全てのサービスを同じ強権限アカウントで実行する。」の問題点を直接説明していない。
エ：この説明は別候補「ログ記録を停止する。」に対応するため、誤答候補「全てのサービスを同じ強権限アカウントで実行する。」の問題点を直接説明していない。

総合解説：誤答候補「全てのサービスを同じ強権限アカウントで実行する。」について、誤りの内容を説明できることが重要である。侵害時の影響を拡大する。

対象：2026年度 / 基準日 2026-09-04

Q0006 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：標準

「機密性・完全性・可用性／脅威・脆弱性」のうち「ゼロデイ」を、正答の根拠まで理解できているか確認する。候補「ゼロデイ脆弱性を利用した攻撃」を妥当と判断する根拠として最も適切な説明はどれか。

ア．候補を総当たりする攻撃である。
イ．修正策が十分に整う前に脆弱性が実際の攻撃へ使われる状況はゼロデイ攻撃として扱われる。
ウ．漏えい済み資格情報を他サービスへ試す攻撃である。
エ．正当な通信を再送して悪用する攻撃である。

答え・解説 正答：イ

ア：この説明は別候補「ブルートフォース攻撃」に対応するため、正答候補「ゼロデイ脆弱性を利用した攻撃」の根拠にはならない。
イ：この説明は正答候補「ゼロデイ脆弱性を利用した攻撃」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「パスワードリスト攻撃」に対応するため、正答候補「ゼロデイ脆弱性を利用した攻撃」の根拠にはならない。
エ：この説明は別候補「リプレイ攻撃」に対応するため、正答候補「ゼロデイ脆弱性を利用した攻撃」の根拠にはならない。

総合解説：正答候補「ゼロデイ脆弱性を利用した攻撃」を選ぶ根拠は次のとおりである。修正策が十分に整う前に脆弱性が実際の攻撃へ使われる状況はゼロデイ攻撃として扱われる。

対象：2026年度 / 基準日 2026-09-04

Q0007 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：標準

「機密性・完全性・可用性／脅威・脆弱性」の「CVEとCVSS」について、候補「CVEは脆弱性識別子、CVSSは脆弱性の深刻度を評価する指標として利用される。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．役割が逆で、CVEは鍵長指標でもない。
イ．いずれも製品名ではない。
ウ．CVEは個別脆弱性を参照する識別子であり、CVSSは深刻度評価に用いられる。
エ．事業継続の指標ではない。

答え・解説 正答：ウ

ア：この説明は別候補「CVSSが識別子で、CVEが暗号鍵長の指標である。」に対応するため、正答候補「CVEは脆弱性識別子、CVSSは脆弱性の深刻度を評価する指標として利用される。」の根拠にはならない。
イ：この説明は別候補「CVEもCVSSもウイルス対策製品名である。」に対応するため、正答候補「CVEは脆弱性識別子、CVSSは脆弱性の深刻度を評価する指標として利用される。」の根拠にはならない。
ウ：この説明は正答候補「CVEは脆弱性識別子、CVSSは脆弱性の深刻度を評価する指標として利用される。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「CVEはバックアップ世代、CVSSはRTOの単位である。」に対応するため、正答候補「CVEは脆弱性識別子、CVSSは脆弱性の深刻度を評価する指標として利用される。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。CVEは個別脆弱性を参照する識別子であり、CVSSは深刻度評価に用いられる。

対象：2026年度 / 基準日 2026-09-04

Q0008 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：標準

「機密性・完全性・可用性／脅威・脆弱性」の「多層防御」を復習している学習者が、候補「完全公開」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．一つの対策への依存であり逆である。
イ．DB設計の概念である。
ウ．異なる層の管理策を組み合わせ、一つの防御失敗が直ちに全面侵害へつながらないようにする考え方である。
エ．セキュリティ防御の考え方ではない。

答え・解説 正答：エ

ア：この説明は別候補「単一障害点への集中」に対応するため、誤答候補「完全公開」の問題点を直接説明していない。
イ：この説明は別候補「データ非正規化」に対応するため、誤答候補「完全公開」の問題点を直接説明していない。
ウ：この説明は別候補「多層防御（Defense in Depth）」に対応するため、誤答候補「完全公開」の問題点を直接説明していない。
エ：この説明は誤答候補「完全公開」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「完全公開」については、何が誤りかを明確にした上で正しい概念へ戻す。セキュリティ防御の考え方ではない。

対象：2026年度 / 基準日 2026-09-04

Q0009 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：応用

「機密性・完全性・可用性／脅威・脆弱性」のうち「リスク構成要素」を確認する誤答分析で、学習者が候補「漏えいだけが資産で、その他は全て同義である。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．異なる概念である。
イ．リスク分析では資産、脅威、脆弱性、影響を分けて考える。
ウ．分類が入れ替わっている。
エ．盗難は脅威事象、未暗号化は弱点である。

答え・解説 正答：ア

ア：この説明は誤答候補「漏えいだけが資産で、その他は全て同義である。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「顧客データは資産、盗難は脅威事象、暗号化未設定は脆弱性、漏えいは影響と整理できる。」に対応するため、誤答候補「漏えいだけが資産で、その他は全て同義である。」の問題点を直接説明していない。
ウ：この説明は別候補「顧客データが脅威、盗難が資産、暗号化未設定が影響である。」に対応するため、誤答候補「漏えいだけが資産で、その他は全て同義である。」の問題点を直接説明していない。
エ：この説明は別候補「PC盗難が脆弱性で、暗号化未設定が脅威源である。」に対応するため、誤答候補「漏えいだけが資産で、その他は全て同義である。」の問題点を直接説明していない。

総合解説：誤答候補「漏えいだけが資産で、その他は全て同義である。」について、誤りの内容を説明できることが重要である。異なる概念である。

対象：2026年度 / 基準日 2026-09-04

Q0010 4-1 セキュリティ基礎・リスク > 機密性・完全性・可用性／脅威・脆弱性 ｜ 難易度：応用

「機密性・完全性・可用性／脅威・脆弱性」のうち「責任追跡性」を、正答の根拠まで理解できているか確認する。候補「個人ごとの認証、権限管理、改ざん耐性を考慮した監査ログを組み合わせる。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．誰が操作したか追跡できない。
イ．個人識別、適切な認可、保護された操作記録により真正性や責任追跡性を高められる。
ウ．操作者の真正性を確認できない。
エ．証跡の完全性が失われる。

答え・解説 正答：イ

ア：この説明は別候補「全員で共有管理者IDを使い、ログを毎日削除する。」に対応するため、正答候補「個人ごとの認証、権限管理、改ざん耐性を考慮した監査ログを組み合わせる。」の根拠にはならない。
イ：この説明は正答候補「個人ごとの認証、権限管理、改ざん耐性を考慮した監査ログを組み合わせる。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「承認画面の認証を省略する。」に対応するため、正答候補「個人ごとの認証、権限管理、改ざん耐性を考慮した監査ログを組み合わせる。」の根拠にはならない。
エ：この説明は別候補「ログを利用者自身が自由に編集できるようにする。」に対応するため、正答候補「個人ごとの認証、権限管理、改ざん耐性を考慮した監査ログを組み合わせる。」の根拠にはならない。

総合解説：正答候補「個人ごとの認証、権限管理、改ざん耐性を考慮した監査ログを組み合わせる。」を選ぶ根拠は次のとおりである。個人識別、適切な認可、保護された操作記録により真正性や責任追跡性を高められる。

対象：2026年度 / 基準日 2026-09-04

Q0011 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：基礎

「リスクアセスメント・リスク対応」の「リスクアセスメント」について、候補「資産、脅威、脆弱性、発生可能性や影響などを評価し、優先して対応すべきリスクを明らかにすること。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．完全なゼロ化は通常現実的でない。
イ．目的全体ではない。
ウ．リスクアセスメントは意思決定に必要なリスク情報を整理し、対応優先順位の決定に役立てる。
エ．リスクを増大させ得る。

答え・解説 正答：ウ

ア：この説明は別候補「全てのリスクを必ずゼロにすること。」に対応するため、正答候補「資産、脅威、脆弱性、発生可能性や影響などを評価し、優先して対応すべきリスクを明らかにすること。」の根拠にはならない。
イ：この説明は別候補「CPU性能だけを測定すること。」に対応するため、正答候補「資産、脅威、脆弱性、発生可能性や影響などを評価し、優先して対応すべきリスクを明らかにすること。」の根拠にはならない。
ウ：この説明は正答候補「資産、脅威、脆弱性、発生可能性や影響などを評価し、優先して対応すべきリスクを明らかにすること。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全利用者へ管理者権限を与えること。」に対応するため、正答候補「資産、脅威、脆弱性、発生可能性や影響などを評価し、優先して対応すべきリスクを明らかにすること。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。リスクアセスメントは意思決定に必要なリスク情報を整理し、対応優先順位の決定に役立てる。

対象：2026年度 / 基準日 2026-09-04

Q0012 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：基礎

「リスクアセスメント・リスク対応」の「リスク回避」を復習している学習者が、候補「承認の上で現状リスクを受け入れる。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．リスク移転・共有に近い。
イ．リスク低減の例である。
ウ．リスク回避はリスクを生じさせる活動を開始しない、又は中止する対応である。
エ．リスク受容である。

答え・解説 正答：エ

ア：この説明は別候補「サイバー保険に加入する。」に対応するため、誤答候補「承認の上で現状リスクを受け入れる。」の問題点を直接説明していない。
イ：この説明は別候補「WAFを導入する。」に対応するため、誤答候補「承認の上で現状リスクを受け入れる。」の問題点を直接説明していない。
ウ：この説明は別候補「重大なリスクを伴う新サービスの提供自体を中止し、そのリスク源となる活動を行わない。」に対応するため、誤答候補「承認の上で現状リスクを受け入れる。」の問題点を直接説明していない。

エ：この説明は誤答候補「承認の上で現状リスクを受け入れる。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「承認の上で現状リスクを受け入れる。」については、何が誤りかを明確にした上で正しい概念へ戻す。リスク受容である。

対象：2026年度 / 基準日 2026-09-04

Q0013 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：基礎

「リスクアセスメント・リスク対応」のうち「リスク移転」を確認する誤答分析で、学習者が候補「リスク回避」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．活動そのものをやめる対応ではない。
イ．保険は損失負担の一部を第三者へ移すため、リスク移転・共有の代表例である。
ウ．事故確率や被害自体を直接減らす対策とは異なる。
エ．リスクを見つける工程である。

答え・解説 正答：ア

ア：この説明は誤答候補「リスク回避」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「リスク移転（共有）」に対応するため、誤答候補「リスク回避」の問題点を直接説明していない。
ウ：この説明は別候補「リスク低減」に対応するため、誤答候補「リスク回避」の問題点を直接説明していない。
エ：この説明は別候補「リスク識別」に対応するため、誤答候補「リスク回避」の問題点を直接説明していない。

総合解説：誤答候補「リスク回避」について、誤りの内容を説明できることが重要である。活動そのものをやめる対応ではない。

対象：2026年度 / 基準日 2026-09-04

Q0014 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：標準

「リスクアセスメント・リスク対応」のうち「定性評価」を、正答の根拠まで理解できているか確認する。候補「定性的リスク評価」を妥当と判断する根拠として最も適切な説明はどれか。

ア．金額や確率など数量を用いる。
イ．数値の金額や確率を厳密に算出せず、尺度やランクで相対評価する方法である。
ウ．暗号方式である。
エ．バックアップ方式である。

答え・解説 正答：イ

ア：この説明は別候補「定量的リスク評価」に対応するため、正答候補「定性的リスク評価」の根拠にはならない。
イ：この説明は正答候補「定性的リスク評価」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「公開鍵暗号」に対応するため、正答候補「定性的リスク評価」の根拠にはならない。
エ：この説明は別候補「差分バックアップ」に対応するため、正答候補「定性的リスク評価」の根拠にはならない。

総合解説：正答候補「定性的リスク評価」を選ぶ根拠は次のとおりである。数値の金額や確率を厳密に算出せず、尺度やランクで相対評価する方法である。

対象：2026年度 / 基準日 2026-09-04

Q0015 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：標準

「リスクアセスメント・リスク対応」の「ALE計算」について、候補「50万円」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．200万円÷0.25としている。
イ．適切な乗算になっていない。
ウ．ALEは一般にSLE×AROで見積もるので、200万円×0.25=50万円である。
エ．問題条件のAROと一致しない。

答え・解説 正答：ウ

ア：この説明は別候補「800万円」に対応するため、正答候補「50万円」の根拠にはならない。
イ：この説明は別候補「200万0.25円」に対応するため、正答候補「50万円」の根拠にはならない。
ウ：この説明は正答候補「50万円」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「25万円」に対応するため、正答候補「50万円」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ALEは一般にSLE×AROで見積もるので、200万円×0.25=50万円である。

対象：2026年度 / 基準日 2026-09-04

Q0016 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：標準

「リスクアセスメント・リスク対応」の「残留リスク」を復習している学習者が、候補「固有リスク」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．リスク残存量の用語ではない。
イ．RPOであり別概念である。
ウ．管理策で発生可能性や影響を低減しても完全には除去できず残るリスクを残留リスクという。
エ．管理策を考慮する前のリスクである。

答え・解説 正答：エ

ア：この説明は別候補「脆弱性識別子」に対応するため、誤答候補「固有リスク」の問題点を直接説明していない。
イ：この説明は別候補「復旧時点目標」に対応するため、誤答候補「固有リスク」の問題点を直接説明していない。
ウ：この説明は別候補「残留リスク」に対応するため、誤答候補「固有リスク」の問題点を直接説明していない。
エ：この説明は誤答候補「固有リスク」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「固有リスク」については、何が誤りかを明確にした上で正しい概念へ戻す。管理策を考慮する前のリスクである。

対象：2026年度 / 基準日 2026-09-04

Q0017 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：標準

「リスクアセスメント・リスク対応」のうち「固有リスク」を確認する誤答分析で、学習者が候補「回復時間目標」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．RTOである。
イ．管理策を適用する前のリスクを固有リスク、管理策適用後に残るものを残留リスクと区別する。
ウ．管理策適用後に残るリスクである。
エ．暗号技術である。

答え・解説 正答：ア

ア：この説明は誤答候補「回復時間目標」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「固有リスク」に対応するため、誤答候補「回復時間目標」の問題点を直接説明していない。
ウ：この説明は別候補「残留リスク」に対応するため、誤答候補「回復時間目標」の問題点を直接説明していない。
エ：この説明は別候補「電子署名」に対応するため、誤答候補「回復時間目標」の問題点を直接説明していない。

総合解説：誤答候補「回復時間目標」について、誤りの内容を説明できることが重要である。RTOである。

対象：2026年度 / 基準日 2026-09-04

Q0018 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：標準

「リスクアセスメント・リスク対応」のうち「リスク受容」を、正答の根拠まで理解できているか確認する。候補「権限者が受容を承認し、根拠と残留リスクを記録した上で監視を継続する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．適切な受容ではない。
イ．受容基準内のリスクは責任者の承認と記録を伴って保有する選択肢があり、継続監視も必要である。
ウ．基準や費用対効果を無視している。
エ．環境変化に応じ見直しが必要である。

答え・解説 正答：イ

ア：この説明は別候補「評価結果を隠し記録せず放置する。」に対応するため、正答候補「権限者が受容を承認し、根拠と残留リスクを記録した上で監視を継続する。」の根拠にはならない。
イ：この説明は正答候補「権限者が受容を承認し、根拠と残留リスクを記録した上で監視を継続する。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「受容基準に関係なく全業務を必ず停止する。」に対応するため、正答候補「権限者が受容を承認し、根拠と残留リスクを記録した上で監視を継続する。」の根拠にはならない。
エ：この説明は別候補「受容したので以後評価を永久に行わない。」に対応するため、正答候補「権限者が受容を承認し、根拠と残留リスクを記録した上で監視を継続する。」の根拠にはならない。

総合解説：正答候補「権限者が受容を承認し、根拠と残留リスクを記録した上で監視を継続する。」を選ぶ根拠は次のとおりである。受容基準内のリスクは責任者の承認と記録を伴って保有する選択肢があり、継続監視も必要である。

対象：2026年度 / 基準日 2026-09-04

Q0019 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：応用

「リスクアセスメント・リスク対応」の「リスク優先度」について、候補「まずAのリスク低減策を優先し、Bは受容根拠を確認して監視する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．リスクベースの優先付けになっていない。
イ．リスク差を無視している。
ウ．リスクの大きさと対策効果を考慮し、重大で低減効果の高いリスクへ資源を優先配分するのが合理的である。
エ．優先順位が逆である。

答え・解説 正答：ウ

ア：この説明は別候補「Bだけに全予算を使う。」に対応するため、正答候補「まずAのリスク低減策を優先し、Bは受容根拠を確認して監視する。」の根拠にはならない。
イ：この説明は別候補「AもBも評価せず同額を配分する。」に対応するため、正答候補「まずAのリスク低減策を優先し、Bは受容根拠を確認して監視する。」の根拠にはならない。
ウ：この説明は正答候補「まずAのリスク低減策を優先し、Bは受容根拠を確認して監視する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「Aは重大なので記録せず継続し、Bだけ停止する。」に対応するため、正答候補「まずAのリスク低減策を優先し、Bは受容根拠を確認して監視する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。リスクの大きさと対策効果を考慮し、重大で低減効果の高いリスクへ資源を優先配分するのが合理的である。

対象：2026年度 / 基準日 2026-09-04

Q0020 4-1 セキュリティ基礎・リスク > リスクアセスメント・リスク対応 ｜ 難易度：応用

「リスクアセスメント・リスク対応」の「第三者リスク」を復習している学習者が、候補「価格だけ比較しセキュリティや復旧条件は評価しない。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．利用者側の責任も残る。
イ．継続的確認が必要である。
ウ．外部委託では第三者依存が新たな脅威・影響経路となるため、提供者側の管理策や責任分界も評価する。
エ．重要なリスク要因を無視している。

答え・解説 正答：エ

ア：この説明は別候補「クラウド移行で自社のリスク責任は全て消えると考える。」に対応するため、誤答候補「価格だけ比較しセキュリティや復旧条件は評価しない。」の問題点を直接説明していない。
イ：この説明は別候補「契約後は管理状況を一切確認しない。」に対応するため、誤答候補「価格だけ比較しセキュリティや復旧条件は評価しない。」の問題点を直接説明していない。
ウ：この説明は別候補「自社資産だけでなく、委託先の可用性、データ保護、再委託、障害時対応、契約上の責任分界も評価する。」に対応するため、誤答候補「価格だけ比較しセキュリティや復旧条件は評価しない。」の問題点を直接説明していない。
エ：この説明は誤答候補「価格だけ比較しセキュリティや復旧条件は評価しない。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「価格だけ比較しセキュリティや復旧条件は評価しない。」については、何が誤りかを明確にした上で正しい概念へ戻す。重要なリスク要因を無視している。

対象：2026年度 / 基準日 2026-09-04

Q0021 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：基礎

「セキュリティ方針・BCP・ISMS」のうち「セキュリティ方針」を確認する誤答分析で、学習者が候補「バックアップ媒体名だけを定める。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．個別運用事項である。
イ．基本方針は組織としての方向性を明確にし、その下位に具体的な規程・手順・基準を展開する。
ウ．運用手順レベルである。
エ．組織方針として不適切である。

答え・解説 正答：ア

ア：この説明は誤答候補「バックアップ媒体名だけを定める。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「経営者の承認の下で、情報セキュリティに関する基本的な目的・方向性・責任を示す。」に対応するため、誤答候補「バックアップ媒体名だけを定める。」の問題点を直接説明していない。
ウ：この説明は別候補「特定サーバのIPアドレス一覧だけを記載する。」に対応するため、誤答候補「バックアップ媒体名だけを定める。」の問題点を直接説明していない。
エ：この説明は別候補「一人の担当者だけが知る非公式メモとする。」に対応するため、誤答候補「バックアップ媒体名だけを定める。」の問題点を直接説明していない。

総合解説：誤答候補「バックアップ媒体名だけを定める。」について、誤りの内容を説明できることが重要である。個別運用事項である。

対象：2026年度 / 基準日 2026-09-04

Q0022 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：基礎

「セキュリティ方針・BCP・ISMS」のうち「BCP」を、正答の根拠まで理解できているか確認する。候補「災害や重大障害が発生しても重要業務を許容範囲で継続し、又は目標時間内に復旧できるようにすること。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．障害発生を前提に継続・復旧を計画する。
イ．BCPは重大な中断に備え、重要業務の継続・復旧方針、代替手段、体制等を計画する。
ウ．BCPの主目的ではない。
エ．今回の条件・目的に照らすと適切な説明ではない。

答え・解説 正答：イ

ア：この説明は別候補「全ての障害を事前に完全排除すること。」に対応するため、正答候補「災害や重大障害が発生しても重要業務を許容範囲で継続し、又は目標時間内に復旧できるようにすること。」の根拠にはならない。
イ：この説明は正答候補「災害や重大障害が発生しても重要業務を許容範囲で継続し、又は目標時間内に復旧できるようにすること。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「日常のコーディング規約だけを定めること。」に対応するため、正答候補「災害や重大障害が発生しても重要業務を許容範囲で継続し、又は目標時間内に復旧できるようにすること。」の根拠にはならない。
エ：この説明は別候補「全利用者へ管理者権限を付与すること。」に対応するため、正答候補「災害や重大障害が発生しても重要業務を許容範囲で継続し、又は目標時間内に復旧できるようにすること。」の根拠にはならない。

総合解説：正答候補「災害や重大障害が発生しても重要業務を許容範囲で継続し、又は目標時間内に復旧できるようにすること。」を選ぶ根拠は次のとおりである。BCPは重大な中断に備え、重要業務の継続・復旧方針、代替手段、体制等を計画する。

対象：2026年度 / 基準日 2026-09-04

Q0023 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：基礎

「セキュリティ方針・BCP・ISMS」の「ISMS」について、候補「リスクに基づき管理策を計画・実施し、監視・見直しを通じて継続的に改善する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．継続的な見直しが必要である。
イ．経営層の関与が重要である。
ウ．ISMSは一度対策を導入して終わりではなく、環境・リスクの変化に応じて継続的に改善する。
エ．継続的管理が必要である。

答え・解説 正答：ウ

ア：この説明は別候補「最初に規程を作成したら以後は見直さない。」に対応するため、正答候補「リスクに基づき管理策を計画・実施し、監視・見直しを通じて継続的に改善する。」の根拠にはならない。
イ：この説明は別候補「セキュリティは情報システム部だけの責任で経営者は関与しない。」に対応するため、正答候補「リスクに基づき管理策を計画・実施し、監視・見直しを通じて継続的に改善する。」の根拠にはならない。
ウ：この説明は正答候補「リスクに基づき管理策を計画・実施し、監視・見直しを通じて継続的に改善する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「事故時だけ活動し平常時は管理しない。」に対応するため、正答候補「リスクに基づき管理策を計画・実施し、監視・見直しを通じて継続的に改善する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ISMSは一度対策を導入して終わりではなく、環境・リスクの変化に応じて継続的に改善する。

対象：2026年度 / 基準日 2026-09-04

Q0024 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：標準

「セキュリティ方針・BCP・ISMS」の「BIA」を復習している学習者が、候補「鍵生成」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．技術的脆弱性検出である。
イ．開発保守作業である。
ウ．BIAは業務中断による影響を分析し、重要業務、復旧優先度、必要な復旧目標等を定める基礎となる。
エ．暗号処理である。

答え・解説 正答：エ

ア：この説明は別候補「脆弱性スキャンだけ」に対応するため、誤答候補「鍵生成」の問題点を直接説明していない。
イ：この説明は別候補「ソースコード整形」に対応するため、誤答候補「鍵生成」の問題点を直接説明していない。
ウ：この説明は別候補「事業影響度分析（BIA）」に対応するため、誤答候補「鍵生成」の問題点を直接説明していない。
エ：この説明は誤答候補「鍵生成」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「鍵生成」については、何が誤りかを明確にした上で正しい概念へ戻す。暗号処理である。

対象：2026年度 / 基準日 2026-09-04

Q0025 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：標準

「セキュリティ方針・BCP・ISMS」のうち「RTO」を確認する誤答分析で、学習者が候補「障害時に失ってよいデータ量を時間で表す目標」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．RPOに近い。
イ．RTOは停止から復旧までに許容する目標時間を表す。
ウ．今回問われている論点には直接対応しない内容である。
エ．復旧時間目標ではない。

答え・解説 正答：ア

ア：この説明は誤答候補「障害時に失ってよいデータ量を時間で表す目標」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「業務やシステムを中断後、目標としてどの程度の時間までに復旧させるかを示す。」に対応するため、誤答候補「障害時に失ってよいデータ量を時間で表す目標」の問題点を直接説明していない。

ウ：この説明は別候補「暗号鍵長の目標」に対応するため、誤答候補「障害時に失ってよいデータ量を時間で表す目標」の問題点を直接説明していない。
エ：この説明は別候補「一日当たりの最大ログ件数」に対応するため、誤答候補「障害時に失ってよいデータ量を時間で表す目標」の問題点を直接説明していない。

総合解説：誤答候補「障害時に失ってよいデータ量を時間で表す目標」について、誤りの内容を説明できることが重要である。RPOに近い。

対象：2026年度 / 基準日 2026-09-04

Q0026 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：標準

「セキュリティ方針・BCP・ISMS」のうち「RPO」を、正答の根拠まで理解できているか確認する。候補「障害時に、原則として障害発生前2時間以内の時点までデータを復旧できるように設計する目標である。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．RTOに近い。
イ．RPOは復旧時点に関する目標で、どこまで過去の状態へ戻ることを許容するかを示す。
ウ．今回問われている論点には直接対応しない内容である。
エ．RPOの説明ではない。

答え・解説 正答：イ

ア：この説明は別候補「必ず2時間以内にシステム全体を再起動する。」に対応するため、正答候補「障害時に、原則として障害発生前2時間以内の時点までデータを復旧できるように設計する目標である。」の根拠にはならない。
イ：この説明は正答候補「障害時に、原則として障害発生前2時間以内の時点までデータを復旧できるように設計する目標である。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「2時間ごとにパスワードを変更する。」に対応するため、正答候補「障害時に、原則として障害発生前2時間以内の時点までデータを復旧できるように設計する目標である。」の根拠にはならない。
エ：この説明は別候補「障害が2時間以上続くことを禁止する契約である。」に対応するため、正答候補「障害時に、原則として障害発生前2時間以内の時点までデータを復旧できるように設計する目標である。」の根拠にはならない。

総合解説：正答候補「障害時に、原則として障害発生前2時間以内の時点までデータを復旧できるように設計する目標である。」を選ぶ根拠は次のとおりである。RPOは復旧時点に関する目標で、どこまで過去の状態へ戻ることを許容するかを示す。

対象：2026年度 / 基準日 2026-09-04

Q0027 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：標準

「セキュリティ方針・BCP・ISMS」の「文書体系」について、候補「情報セキュリティ基準・規程など、基本方針を具体化する下位文書」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．組織統制にならない。
イ．管理文書にならない。
ウ．基本方針は方向性を示し、具体的要求は規程や基準、実施方法は手順へ展開する。
エ．継続的な基準として不適切である。

答え・解説 正答：ウ

ア：この説明は別候補「個人メモだけに記載する。」に対応するため、正答候補「情報セキュリティ基準・規程など、基本方針を具体化する下位文書」の根拠にはならない。
イ：この説明は別候補「バイナリファイル内だけに埋め込む。」に対応するため、正答候補「情報セキュリティ基準・規程など、基本方針を具体化する下位文書」の根拠にはならない。
ウ：この説明は正答候補「情報セキュリティ基準・規程など、基本方針を具体化する下位文書」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「監査終了後に毎回削除する。」に対応するため、正答候補「情報セキュリティ基準・規程など、基本方針を具体化する下位文書」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。基本方針は方向性を示し、具体的要求は規程や基準、実施方法は手順へ展開する。

対象：2026年度 / 基準日 2026-09-04

Q0028 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：標準

「セキュリティ方針・BCP・ISMS」の「BCP訓練」を復習している学習者が、候補「訓練を行えば本番障害が物理的に発生しなくなる。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．今回問われている対象の目的には該当しない。
イ．今回の条件・目的に照らすと適切な説明ではない。
ウ．文書上の計画だけでは実効性を保証できないため、訓練で課題を発見し改訂する必要がある。
エ．障害自体をなくすものではない。

答え・解説 正答：エ

ア：この説明は別候補「監査ログを全削除するため。」に対応するため、誤答候補「訓練を行えば本番障害が物理的に発生しなくなる。」の問題点を直接説明していない。
イ：この説明は別候補「全利用者へ恒久管理者権限を与えるため。」に対応するため、誤答候補「訓練を行えば本番障害が物理的に発生しなくなる。」の問題点を直接説明していない。
ウ：この説明は別候補「連絡網、役割分担、代替手順、復旧手順が実際に機能するか検証し、不備を改善するため。」に対応するため、誤答候補「訓練を行えば本番障害が物理的に発生しなくなる。」の問題点を直接説明していない。
エ：この説明は誤答候補「訓練を行えば本番障害が物理的に発生しなくなる。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「訓練を行えば本番障害が物理的に発生しなくなる。」については、何が誤りかを明確にした上で正しい概念へ戻す。障害自体をなくすものではない。

対象：2026年度 / 基準日 2026-09-04

Q0029 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：応用

「セキュリティ方針・BCP・ISMS」のうち「BCP設計」を確認する誤答分析で、学習者が候補「同一機器内だけに保存すれば災害耐性が最も高い。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．同じ障害で失う可能性がある。
イ．厳しいRPOには短い間隔で更新を保護する仕組みが必要で、RTOには迅速な切替・復元方式も必要である。
ウ．最大約1日分失う可能性がある。
エ．事業継続の指標である。

答え・解説 正答：ア

ア：この説明は誤答候補「同一機器内だけに保存すれば災害耐性が最も高い。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「RPO=5分を満たしにくく、機器障害時の復旧にも弱いので、更新ログの継続保存や冗長化、別障害ドメインへの保管等を検討する必要がある。」に対応するため、誤答候補「同一機器内だけに保存すれば災害耐性が最も高い。」の問題点を直接説明していない。
ウ：この説明は別候補「1日1回のバックアップなら必ずRPO=5分を満たす。」に対応するため、誤答候補「同一機器内だけに保存すれば災害耐性が最も高い。」の問題点を直接説明していない。
エ：この説明は別候補「RTOとRPOは暗号鍵長の指標である。」に対応するため、誤答候補「同一機器内だけに保存すれば災害耐性が最も高い。」の問題点を直接説明していない。

総合解説：誤答候補「同一機器内だけに保存すれば災害耐性が最も高い。」について、誤りの内容を説明できることが重要である。同じ障害で失う可能性がある。

対象：2026年度 / 基準日 2026-09-04

Q0030 4-1 セキュリティ基礎・リスク > セキュリティ方針・BCP・ISMS ｜ 難易度：応用

「セキュリティ方針・BCP・ISMS」のうち「ISMSスコープ」を、正答の根拠まで理解できているか確認する。候補「対象範囲、資産、業務プロセス、関係者、法令・契約要求、リスクを見直し、必要な管理策と文書を更新する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．変更を反映していない。
イ．ISMSの対象範囲が変われば、境界・資産・要求事項・リスク評価など関連要素を再確認する必要がある。
ウ．履歴を失うべきではない。
エ．多面的確認が必要である。

答え・解説 正答：イ

ア：この説明は別候補「既存文書をそのまま使い、海外拠点は実態に関係なく無視する。」に対応するため、正答候補「対象範囲、資産、業務プロセス、関係者、法令・契約要求、リスクを見直し、必要な管理策と文書を更新する。」の根拠にはならない。
イ：この説明は正答候補「対象範囲、資産、業務プロセス、関係者、法令・契約要求、リスクを見直し、必要な管理策と文書を更新する。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「過去のリスク評価を全て削除する。」に対応するため、正答候補「対象範囲、資産、業務プロセス、関係者、法令・契約要求、リスクを見直し、必要な管理策と文書を更新する。」の根拠にはならない。
エ：この説明は別候補「スコープ変更はネットワーク速度だけの問題と考える。」に対応するため、正答候補「対象範囲、資産、業務プロセス、関係者、法令・契約要求、リスクを見直し、必要な管理策と文書を更新する。」の根拠にはならない。

総合解説：正答候補「対象範囲、資産、業務プロセス、関係者、法令・契約要求、リスクを見直し、必要な管理策と文書を更新する。」を選ぶ根拠は次のとおりである。ISMSの対象範囲が変われば、境界・資産・要求事項・リスク評価など関連要素を再確認する必要がある。

対象：2026年度 / 基準日 2026-09-04

Q0031 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：基礎

「共通鍵・公開鍵・鍵管理」の「共通鍵暗号」について、候補「暗号化と復号に共有する秘密鍵を用い、高速な大量データ暗号化に適しやすい。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．公開鍵暗号の特徴である。
イ．ハッシュは復号方式ではない。
ウ．共通鍵暗号は同じ秘密鍵を当事者間で安全に共有する必要があるが、一般に公開鍵暗号より高速である。
エ．共通鍵暗号の説明ではない。

答え・解説 正答：ウ

ア：この説明は別候補「暗号化鍵を誰にでも公開し、復号鍵だけ秘密にする。」に対応するため、正答候補「暗号化と復号に共有する秘密鍵を用い、高速な大量データ暗号化に適しやすい。」の根拠にはならない。
イ：この説明は別候補「秘密鍵を一切使わずハッシュ値だけで元データを復号する。」に対応するため、正答候補「暗号化と復号に共有する秘密鍵を用い、高速な大量データ暗号化に適しやすい。」の根拠にはならない。

ウ：この説明は正答候補「暗号化と復号に共有する秘密鍵を用い、高速な大量データ暗号化に適しやすい。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「暗号化と復号に必ず異なる二つの公開鍵だけを使う。」に対応するため、正答候補「暗号化と復号に共有する秘密鍵を用い、高速な大量データ暗号化に適しやすい。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。共通鍵暗号は同じ秘密鍵を当事者間で安全に共有する必要があるが、一般に公開鍵暗号より高速である。

対象：2026年度 / 基準日 2026-09-04

Q0032 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：基礎

「共通鍵・公開鍵・鍵管理」の「公開鍵暗号」を復習している学習者が、候補「受信者の秘密鍵を全送信者へ配布する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．機密性を確保できない。
イ．ハッシュは復号の仕組みではない。
ウ．公開鍵は配布可能で、対応する秘密鍵を保持する受信者だけが復号できるように利用する。
エ．秘密鍵を配布してはいけない。

答え・解説 正答：エ

ア：この説明は別候補「送信者の公開鍵で暗号化し、誰でも同じ公開鍵で復号する。」に対応するため、誤答候補「受信者の秘密鍵を全送信者へ配布する。」の問題点を直接説明していない。
イ：この説明は別候補「ハッシュ値を暗号鍵として必ず元データへ戻す。」に対応するため、誤答候補「受信者の秘密鍵を全送信者へ配布する。」の問題点を直接説明していない。
ウ：この説明は別候補「受信者の公開鍵で暗号化し、対応する受信者の秘密鍵で復号する。」に対応するため、誤答候補「受信者の秘密鍵を全送信者へ配布する。」の問題点を直接説明していない。
エ：この説明は誤答候補「受信者の秘密鍵を全送信者へ配布する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「受信者の秘密鍵を全送信者へ配布する。」については、何が誤りかを明確にした上で正しい概念へ戻す。秘密鍵を配布してはいけない。

対象：2026年度 / 基準日 2026-09-04

Q0033 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：基礎

「共通鍵・公開鍵・鍵管理」のうち「AES」を確認する誤答分析で、学習者が候補「利用者の生体情報を照合する認証方式である。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．暗号アルゴリズムである。
イ．AESはNISTのFIPS 197で標準化された共通鍵ブロック暗号である。
ウ．PKIの仕組みではない。
エ．ハッシュ標準ではない。

答え・解説 正答：ア

ア：この説明は誤答候補「利用者の生体情報を照合する認証方式である。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「代表的な共通鍵ブロック暗号であり、データ暗号化に利用される。」に対応するため、誤答候補「利用者の生体情報を照合する認証方式である。」の問題点を直接説明していない。
ウ：この説明は別候補「公開鍵証明書の失効一覧を配布するプロトコルである。」に対応するため、誤答候補「利用者の生体情報を照合する認証方式である。」の問題点を直接説明していない。
エ：この説明は別候補「一方向ハッシュ関数だけを定義する標準である。」に対応するため、誤答候補「利用者の生体情報を照合する認証方式である。」の問題点を直接説明していない。

総合解説：誤答候補「利用者の生体情報を照合する認証方式である。」について、誤りの内容を説明できることが重要である。暗号アルゴリズムである。

対象：2026年度 / 基準日 2026-09-04

Q0034 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：標準

「共通鍵・公開鍵・鍵管理」のうち「ハイブリッド暗号」を、正答の根拠まで理解できているか確認する。候補「データ本体は一時的な共通鍵で暗号化し、その共通鍵を受信者の公開鍵で保護して送る。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．一般的なハイブリッド方式の利点を生かさない。
イ．共通鍵暗号の高速性と、公開鍵暗号による鍵配送の利便性を組み合わせる代表的な構成である。
ウ．鍵漏えいで復号される。
エ．暗号化ではない。

答え・解説 正答：イ

ア：この説明は別候補「データ本体の各ビットを必ず公開鍵暗号で個別暗号化する。」に対応するため、正答候補「データ本体は一時的な共通鍵で暗号化し、その共通鍵を受信者の公開鍵で保護して送る。」の根拠にはならない。
イ：この説明は正答候補「データ本体は一時的な共通鍵で暗号化し、その共通鍵を受信者の公開鍵で保護して送る。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「共通鍵を平文で送信しデータだけ暗号化する。」に対応するため、正答候補「データ本体は一時的な共通鍵で暗号化し、その共通鍵を受信者の公開鍵で保護して送る。」の根拠にはならない。
エ：この説明は別候補「鍵を使わずファイル名を変更するだけで保護する。」に対応するため、正答候補「データ本体は一時的な共通鍵で暗号化し、その共通鍵を受信者の公開鍵で保護して送る。」の根拠にはならない。

総合解説：正答候補「データ本体は一時的な共通鍵で暗号化し、その共通鍵を受信者の公開鍵で保護して送る。」を選ぶ根拠は次のとおりである。共通鍵暗号の高速性と、公開鍵暗号による鍵配送の利便性を組み合わせる代表的な構成である。

対象：2026年度 / 基準日 2026-09-04

Q0035 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：標準

「共通鍵・公開鍵・鍵管理」の「鍵交換」について、候補「安全でない通信路上で、共有秘密を直接送らずに当事者間で共有鍵材料を合意すること。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．データ圧縮である。
イ．失効処理とは異なる。
ウ．鍵共有方式は秘密鍵そのものを送らず、暗号学的計算を用いて共通の秘密を導出するために使われる。
エ．攻撃手法である。

答え・解説 正答：ウ

ア：この説明は別候補「ファイルを圧縮して容量を減らす。」に対応するため、正答候補「安全でない通信路上で、共有秘密を直接送らずに当事者間で共有鍵材料を合意すること。」の根拠にはならない。
イ：この説明は別候補「公開鍵証明書を自動的に失効させる。」に対応するため、正答候補「安全でない通信路上で、共有秘密を直接送らずに当事者間で共有鍵材料を合意すること。」の根拠にはならない。
ウ：この説明は正答候補「安全でない通信路上で、共有秘密を直接送らずに当事者間で共有鍵材料を合意すること。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「パスワードを総当たりで探索する。」に対応するため、正答候補「安全でない通信路上で、共有秘密を直接送らずに当事者間で共有鍵材料を合意すること。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。鍵共有方式は秘密鍵そのものを送らず、暗号学的計算を用いて共通の秘密を導出するために使われる。

対象：2026年度 / 基準日 2026-09-04

Q0036 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：標準

「共通鍵・公開鍵・鍵管理」の「IVとnonce」を復習している学習者が、候補「暗号方式とは無関係なので省略してよい。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．鍵とIV/nonceは役割が異なる。
イ．固定再利用が危険な方式が多い。
ウ．IVやnonceの要件は方式ごとに異なるが、不適切な再利用は安全性を損なう場合がある。
エ．方式によっては必須である。

答え・解説 正答：エ

ア：この説明は別候補「必ず秘密鍵と同じ値を設定する。」に対応するため、誤答候補「暗号方式とは無関係なので省略してよい。」の問題点を直接説明していない。
イ：この説明は別候補「毎回固定値0を使えば全方式で最も安全になる。」に対応するため、誤答候補「暗号方式とは無関係なので省略してよい。」の問題点を直接説明していない。
ウ：この説明は別候補「方式の仕様に従い一意性や予測困難性など必要条件を満たす値を使用し、同一鍵で危険な再利用を避ける。」に対応するため、誤答候補「暗号方式とは無関係なので省略してよい。」の問題点を直接説明していない。
エ：この説明は誤答候補「暗号方式とは無関係なので省略してよい。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「暗号方式とは無関係なので省略してよい。」については、何が誤りかを明確にした上で正しい概念へ戻す。方式によっては必須である。

対象：2026年度 / 基準日 2026-09-04

Q0037 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：標準

「共通鍵・公開鍵・鍵管理」のうち「鍵ローテーション」を確認する誤答分析で、学習者が候補「鍵更新で暗号文が必ず短くなるため。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．圧縮目的ではない。
イ．鍵には生成・配布・利用・保管・更新・失効・廃棄のライフサイクル管理が必要である。
ウ．問われている関係や方向を逆に捉えた内容である。
エ．ローテーション自体が鍵管理の一部である。

答え・解説 正答：ア

ア：この説明は誤答候補「鍵更新で暗号文が必ず短くなるため。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「一つの鍵が長期間・大量データに使われ続けるリスクを抑え、漏えい時の影響範囲も限定しやすくするため。」に対応するため、誤答候補「鍵更新で暗号文が必ず短くなるため。」の問題点を直接説明していない。
ウ：この説明は別候補「更新後は過去暗号データを誰でも読めるようにするため。」に対応するため、誤答候補「鍵更新で暗号文が必ず短くなるため。」の問題点を直接説明していない。
エ：この説明は別候補「鍵管理を不要にするため。」に対応するため、誤答候補「鍵更新で暗号文が必ず短くなるため。」の問題点を直接説明していない。

総合解説：誤答候補「鍵更新で暗号文が必ず短くなるため。」について、誤りの内容を説明できることが重要である。圧縮目的ではない。

対象：2026年度 / 基準日 2026-09-04

Q0038 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：標準

「共通鍵・公開鍵・鍵管理」のうち「HSM」を、正答の根拠まで理解できているか確認する。候補「HSM等の耐タンパ性を考慮した専用装置内で鍵生成・利用を行い、秘密鍵の外部取り出しを制限する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．秘密性が失われる。
イ．重要秘密鍵は安全な暗号装置で保護し、鍵素材の露出を最小化することが有効である。
ウ．公開鍵暗号の前提が崩れる。
エ．漏えいリスクが高い。

答え・解説 正答：イ

ア：この説明は別候補「秘密鍵を全社員へメール添付で配布する。」に対応するため、正答候補「HSM等の耐タンパ性を考慮した専用装置内で鍵生成・利用を行い、秘密鍵の外部取り出しを制限する。」の根拠にはならない。
イ：この説明は正答候補「HSM等の耐タンパ性を考慮した専用装置内で鍵生成・利用を行い、秘密鍵の外部取り出しを制限する。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「秘密鍵を公開Webへ掲載する。」に対応するため、正答候補「HSM等の耐タンパ性を考慮した専用装置内で鍵生成・利用を行い、秘密鍵の外部取り出しを制限する。」の根拠にはならない。
エ：この説明は別候補「秘密鍵を平文共有フォルダへ保存する。」に対応するため、正答候補「HSM等の耐タンパ性を考慮した専用装置内で鍵生成・利用を行い、秘密鍵の外部取り出しを制限する。」の根拠にはならない。

総合解説：正答候補「HSM等の耐タンパ性を考慮した専用装置内で鍵生成・利用を行い、秘密鍵の外部取り出しを制限する。」を選ぶ根拠は次のとおりである。重要秘密鍵は安全な暗号装置で保護し、鍵素材の露出を最小化することが有効である。

対象：2026年度 / 基準日 2026-09-04

Q0039 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：応用

「共通鍵・公開鍵・鍵管理」の「前方秘匿性」について、候補「前方秘匿性（Forward Secrecy）」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．データ圧縮の性質である。
イ．DBの外部キー整合性である。
ウ．一時鍵を用いる設計では、長期秘密鍵の将来漏えいが過去セッション鍵へ直接波及しないようにできる。
エ．過去セッション保護の性質ではない。

答え・解説 正答：ウ

ア：この説明は別候補「可逆圧縮」に対応するため、正答候補「前方秘匿性（Forward Secrecy）」の根拠にはならない。
イ：この説明は別候補「参照整合性」に対応するため、正答候補「前方秘匿性（Forward Secrecy）」の根拠にはならない。
ウ：この説明は正答候補「前方秘匿性（Forward Secrecy）」の根拠に対応しており、今回の問いに合致する。

エ：この説明は別候補「単一署名」に対応するため、正答候補「前方秘匿性（Forward Secrecy）」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。一時鍵を用いる設計では、長期秘密鍵の将来漏えいが過去セッション鍵へ直接波及しないようにできる。

対象：2026年度 / 基準日 2026-09-04

Q0040 4-2 暗号・認証 > 共通鍵・公開鍵・鍵管理 ｜ 難易度：応用

「共通鍵・公開鍵・鍵管理」の「鍵管理総合」を復習している学習者が、候補「全システムで一つの鍵を永久共有し退職者にも保持させる。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．通常そのような復元はできない。
イ．追跡不能で危険である。
ウ．暗号の安全性はアルゴリズムだけでなく鍵管理に大きく依存するため、鍵ライフサイクル全体を統制する必要がある。
エ．影響範囲が広く管理不能である。

答え・解説 正答：エ

ア：この説明は別候補「鍵を紛失したら暗号文から必ず秘密鍵を再計算できると想定する。」に対応するため、誤答候補「全システムで一つの鍵を永久共有し退職者にも保持させる。」の問題点を直接説明していない。
イ：この説明は別候補「鍵操作ログを残さず誰でも自由に削除できるようにする。」に対応するため、誤答候補「全システムで一つの鍵を永久共有し退職者にも保持させる。」の問題点を直接説明していない。
ウ：この説明は別候補「鍵を用途別に識別し、保管・アクセス権・バックアップ・更新・失効・安全な廃棄まで手順化し、操作を監査できるようにする。」に対応するため、誤答候補「全システムで一つの鍵を永久共有し退職者にも保持させる。」の問題点を直接説明していない。
エ：この説明は誤答候補「全システムで一つの鍵を永久共有し退職者にも保持させる。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「全システムで一つの鍵を永久共有し退職者にも保持させる。」については、何が誤りかを明確にした上で正しい概念へ戻す。影響範囲が広く管理不能である。

対象：2026年度 / 基準日 2026-09-04

Q0041 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：基礎

「ハッシュ・電子署名・PKI」のうち「ハッシュ関数」を確認する誤答分析で、学習者が候補「公開鍵証明書を物理的に印刷する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．今回問われている対象の役割には該当しない。
イ．ハッシュ関数は任意長データからダイジェストを生成し、データの変更検知などに利用される。
ウ．復号目的ではない。
エ．ルーティング機能である。

答え・解説 正答：ア

ア：この説明は誤答候補「公開鍵証明書を物理的に印刷する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「入力データから固定長のダイジェストを求め、改ざん検知や電子署名処理などに利用する。」に対応するため、誤答候補「公開鍵証明書を物理的に印刷する。」の問題点を直接説明していない。
ウ：この説明は別候補「ダイジェストから元データを常に完全復号する。」に対応するため、誤答候補「公開鍵証明書を物理的に印刷する。」の問題点を直接説明していない。
エ：この説明は別候補「通信経路を自動的に選ぶ。」に対応するため、誤答候補「公開鍵証明書を物理的に印刷する。」の問題点を直接説明していない。

総合解説：誤答候補「公開鍵証明書を物理的に印刷する。」について、誤りの内容を説明できることが重要である。今回問われている対象の役割には該当しない。

対象：2026年度 / 基準日 2026-09-04

Q0042 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：基礎

「ハッシュ・電子署名・PKI」のうち「衝突耐性」を、正答の根拠まで理解できているか確認する。候補「同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難であること。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．復号の性質ではない。
イ．衝突耐性は異なる入力xとyについてH(x)=H(y)となる組を現実的に見つけにくい性質を指す。
ウ．有限長出力では理論上衝突は存在し得る。
エ．通常不要である。

答え・解説 正答：イ

ア：この説明は別候補「ハッシュ値から元入力を必ず一意に復号できること。」に対応するため、正答候補「同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難であること。」の根拠にはならない。
イ：この説明は正答候補「同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難であること。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「全ての異なる入力が数学的に絶対異なる無限長ハッシュになること。」に対応するため、正答候補「同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難であること。」の根拠にはならない。
エ：この説明は別候補「ハッシュ計算に公開鍵が必ず必要であること。」に対応するため、正答候補「同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難であること。」の根拠にはならない。

総合解説：正答候補「同じハッシュ値を持つ異なる二つの入力を見つけることが計算上困難であること。」を選ぶ根拠は次のとおりである。衝突耐性は異なる入力xとyについてH(x)=H(y)となる組を現実的に見つけにくい性質を指す。

対象：2026年度 / 基準日 2026-09-04

Q0043 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：基礎

「ハッシュ・電子署名・PKI」の「電子署名」について、候補「署名者の秘密鍵で生成した署名を、対応する公開鍵で検証する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．公開鍵は秘密ではなく署名生成は秘密鍵側で行う。
イ．署名者の公開鍵で検証する。
ウ．電子署名では署名者だけが保持する秘密鍵で署名を生成し、公開鍵で検証する。
エ．今回の条件・目的に照らすと適切な説明ではない。

答え・解説 正答：ウ

ア：この説明は別候補「署名者の公開鍵を全員で秘密共有して署名を生成する。」に対応するため、正答候補「署名者の秘密鍵で生成した署名を、対応する公開鍵で検証する。」の根拠にはならない。
イ：この説明は別候補「受信者の秘密鍵で署名を検証する。」に対応するため、正答候補「署名者の秘密鍵で生成した署名を、対応する公開鍵で検証する。」の根拠にはならない。
ウ：この説明は正答候補「署名者の秘密鍵で生成した署名を、対応する公開鍵で検証する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「ハッシュ値を削除すれば署名信頼性が高まる。」に対応するため、正答候補「署名者の秘密鍵で生成した署名を、対応する公開鍵で検証する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。電子署名では署名者だけが保持する秘密鍵で署名を生成し、公開鍵で検証する。

対象：2026年度 / 基準日 2026-09-04

Q0044 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：標準

「ハッシュ・電子署名・PKI」の「HMAC」を復習している学習者が、候補「可逆圧縮する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．攻撃者も変更後のハッシュを再計算できる。
イ．今回問われている論点には直接対応しない内容である。
ウ．HMACは共有秘密鍵とハッシュ関数を用いてメッセージ認証コードを生成し、完全性と鍵保有者による生成を確認する。
エ．メッセージ認証を提供しない。

答え・解説 正答：エ

ア：この説明は別候補「単なるSHA-256ハッシュを公開値として添付するだけ」に対応するため、誤答候補「可逆圧縮する。」の問題点を直接説明していない。
イ：この説明は別候補「DNSのTTLを短くする。」に対応するため、誤答候補「可逆圧縮する。」の問題点を直接説明していない。
ウ：この説明は別候補「HMACのような鍵付きメッセージ認証コード」に対応するため、誤答候補「可逆圧縮する。」の問題点を直接説明していない。
エ：この説明は誤答候補「可逆圧縮する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「可逆圧縮する。」については、何が誤りかを明確にした上で正しい概念へ戻す。メッセージ認証を提供しない。

対象：2026年度 / 基準日 2026-09-04

Q0045 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：標準

「ハッシュ・電子署名・PKI」のうち「ソルト」を確認する誤答分析で、学習者が候補「全利用者のハッシュ値を同一にするため。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．異なる値にするのが狙いである。
イ．ソルトは入力を個別化し、同一パスワードの識別やレインボーテーブル等の効率を低下させる。
ウ．必ずしも秘密である必要はない。
エ．問われている関係や方向を逆に捉えた内容である。

答え・解説 正答：ア

ア：この説明は誤答候補「全利用者のハッシュ値を同一にするため。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「同じパスワードでも異なるハッシュ値になり、事前計算表などを使った大量照合を困難にするため。」に対応するため、誤答候補「全利用者のハッシュ値を同一にするため。」の問題点を直接説明していない。
ウ：この説明は別候補「ソルト自体を秘密鍵として必ず利用者に隠すため。」に対応するため、誤答候補「全利用者のハッシュ値を同一にするため。」の問題点を直接説明していない。
エ：この説明は別候補「ハッシュ値から元パスワードを容易に復号するため。」に対応するため、誤答候補「全利用者のハッシュ値を同一にするため。」の問題点を直接説明していない。

総合解説：誤答候補「全利用者のハッシュ値を同一にするため。」について、誤りの内容を説明できることが重要である。異なる値にするのが狙いである。

対象：2026年度 / 基準日 2026-09-04

Q0046 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：標準

「ハッシュ・電子署名・PKI」のうち「公開鍵証明書」を、正答の根拠まで理解できているか確認する。候補「公開鍵とその所有主体に関する情報を、認証局の署名によって結び付ける。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．秘密鍵を配布してはいけない。
イ．X.509等の証明書は公開鍵と主体識別情報等を含み、認証局の署名によって結び付きの検証を可能にする。
ウ．認可は別途必要である。
エ．今回問われている論点には直接対応しない内容である。

答え・解説 正答：イ

ア：この説明は別候補「秘密鍵を証明書内に平文で格納して配布する。」に対応するため、正答候補「公開鍵とその所有主体に関する情報を、認証局の署名によって結び付ける。」の根拠にはならない。
イ：この説明は正答候補「公開鍵とその所有主体に関する情報を、認証局の署名によって結び付ける。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「証明書を使えば認可ルールが全て不要になる。」に対応するため、正答候補「公開鍵とその所有主体に関する情報を、認証局の署名によって結び付ける。」の根拠にはならない。
エ：この説明は別候補「DBのトランザクションログを圧縮するために使う。」に対応するため、正答候補「公開鍵とその所有主体に関する情報を、認証局の署名によって結び付ける。」の根拠にはならない。

総合解説：正答候補「公開鍵とその所有主体に関する情報を、認証局の署名によって結び付ける。」を選ぶ根拠は次のとおりである。X.509等の証明書は公開鍵と主体識別情報等を含み、認証局の署名によって結び付きの検証を可能にする。

対象：2026年度 / 基準日 2026-09-04

Q0047 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：標準

「ハッシュ・電子署名・PKI」の「証明書チェーン」について、候補「サーバ証明書から中間認証局を経て、信頼するルート認証局まで署名関係を検証する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．真正性を確認できない。
イ．秘密鍵を渡してはいけない。
ウ．PKIでは信頼の起点となるルートCAまでの認証パスを検証する。
エ．今回問われている論点には直接対応しない内容である。

答え・解説 正答：ウ

ア：この説明は別候補「サーバ証明書だけ見て発行者や署名を確認しない。」に対応するため、正答候補「サーバ証明書から中間認証局を経て、信頼するルート認証局まで署名関係を検証する。」の根拠にはならない。
イ：この説明は別候補「秘密鍵をサーバから取得して利用者側で検証する。」に対応するため、正答候補「サーバ証明書から中間認証局を経て、信頼するルート認証局まで署名関係を検証する。」の根拠にはならない。
ウ：この説明は正答候補「サーバ証明書から中間認証局を経て、信頼するルート認証局まで署名関係を検証する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「DNSのMXレコードだけで証明書署名を検証する。」に対応するため、正答候補「サーバ証明書から中間認証局を経て、信頼するルート認証局まで署名関係を検証する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。PKIでは信頼の起点となるルートCAまでの認証パスを検証する。

対象：2026年度 / 基準日 2026-09-04

Q0048 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：標準

「ハッシュ・電子署名・PKI」の「証明書失効」を復習している学習者が、候補「パスワードを毎回1文字短くする。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．ARPテーブルはIPアドレスとMACアドレスの対応確認に使う情報であり、証明書の失効状態は確認できない。
イ．証明書のファイルサイズを比較しても、失効状態は判断できない。
ウ．証明書は有効期限前でも失効し得るため、CRLやOCSPなどで失効状態を確認する。
エ．パスワードの文字数変更は認証情報の運用であり、証明書の失効確認とは関係しない。

答え・解説 正答：エ

ア：この説明は別候補「ARPテーブルだけを確認する。」に対応するため、誤答候補「パスワードを毎回1文字短くする。」の問題点を直接説明していない。
イ：この説明は別候補「証明書のファイルサイズだけを比較する。」に対応するため、誤答候補「パスワードを毎回1文字短くする。」の問題点を直接説明していない。
ウ：この説明は別候補「CRLやOCSPなどによる証明書失効状態の確認」に対応するため、誤答候補「パスワードを毎回1文字短くする。」の問題点を直接説明していない。
エ：この説明は誤答候補「パスワードを毎回1文字短くする。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「パスワードを毎回1文字短くする。」については、何が誤りかを明確にした上で正しい概念へ戻す。パスワードの文字数変更は認証情報の運用であり、証明書の失効確認とは関係しない。

対象：2026年度 / 基準日 2026-09-04

Q0049 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：応用

「ハッシュ・電子署名・PKI」のうち「署名と暗号化」を確認する誤答分析で、学習者が候補「電子署名だけで必ず内容を秘匿できる。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．署名だけでは通常機密性は確保しない。
イ．暗号化と電子署名は目的が異なるため、両要件がある場合は両者を組み合わせる。
ウ．今回問われている対象とは役割が異なる。
エ．暗号学的保護にならない。

答え・解説 正答：ア

ア：この説明は誤答候補「電子署名だけで必ず内容を秘匿できる。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「機密性のための暗号化と、真正性・完全性を確認する電子署名をそれぞれ適切に組み合わせる。」に対応するため、誤答候補「電子署名だけで必ず内容を秘匿できる。」の問題点を直接説明していない。
ウ：この説明は別候補「暗号化だけで送信者本人の署名を必ず証明できる。」に対応するため、誤答候補「電子署名だけで必ず内容を秘匿できる。」の問題点を直接説明していない。
エ：この説明は別候補「ファイル名変更だけで両要件を満たす。」に対応するため、誤答候補「電子署名だけで必ず内容を秘匿できる。」の問題点を直接説明していない。

総合解説：誤答候補「電子署名だけで必ず内容を秘匿できる。」について、誤りの内容を説明できることが重要である。署名だけでは通常機密性は確保しない。

対象：2026年度 / 基準日 2026-09-04

Q0050 4-2 暗号・認証 > ハッシュ・電子署名・PKI ｜ 難易度：応用

「ハッシュ・電子署名・PKI」のうち「PKI総合」を、正答の根拠まで理解できているか確認する。候補「署名値の数学的検証だけで十分とはいえず、証明書の有効性・失効状態・信頼チェーン等も含めて判断する必要がある。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．失効鍵の署名を信頼してしまう。
イ．PKIを用いた署名検証では、署名値だけでなく証明書が信頼でき有効であったかを確認することが重要である。
ウ．今回問われている論点には直接対応しない内容である。
エ．PKIの重要事項である。

答え・解説 正答：イ

ア：この説明は別候補「署名値が一致すれば証明書状態は常に無視してよい。」に対応するため、正答候補「署名値の数学的検証だけで十分とはいえず、証明書の有効性・失効状態・信頼チェーン等も含めて判断する必要がある。」の根拠にはならない。
イ：この説明は正答候補「署名値の数学的検証だけで十分とはいえず、証明書の有効性・失効状態・信頼チェーン等も含めて判断する必要がある。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「証明書失効で文書本文が自動暗号化される。」に対応するため、正答候補「署名値の数学的検証だけで十分とはいえず、証明書の有効性・失効状態・信頼チェーン等も含めて判断する必要がある。」の根拠にはならない。
エ：この説明は別候補「失効はDNSキャッシュだけの問題である。」に対応するため、正答候補「署名値の数学的検証だけで十分とはいえず、証明書の有効性・失効状態・信頼チェーン等も含めて判断する必要がある。」の根拠にはならない。

総合解説：正答候補「署名値の数学的検証だけで十分とはいえず、証明書の有効性・失効状態・信頼チェーン等も含めて判断する必要がある。」を選ぶ根拠は次のとおりである。PKIを用いた署名検証では、署名値だけでなく証明書が信頼でき有効であったかを確認することが重要である。

対象：2026年度 / 基準日 2026-09-04

Q0051 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：基礎

「認証・認可・アクセス制御」の「認証と認可」について、候補「前者が認証、後者が認可」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．役割が逆である。
イ．暗号化とは異なる。
ウ．認証は主体の本人性を確認し、認可は認証済み主体へ許可する操作や資源を決める。
エ．アクセス制御とは異なる。

答え・解説 正答：ウ

ア：この説明は別候補「前者が認可、後者が認証」に対応するため、正答候補「前者が認証、後者が認可」の根拠にはならない。
イ：この説明は別候補「前者も後者も暗号化」に対応するため、正答候補「前者が認証、後者が認可」の根拠にはならない。
ウ：この説明は正答候補「前者が認証、後者が認可」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「前者がバックアップ、後者が復元」に対応するため、正答候補「前者が認証、後者が認可」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。認証は主体の本人性を確認し、認可は認証済み主体へ許可する操作や資源を決める。

対象：2026年度 / 基準日 2026-09-04

Q0052 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：基礎

「認証・認可・アクセス制御」の「認証要素」を復習している学習者が、候補「パスワードとPIN」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．どちらも生体要素である。
イ．識別情報であり異なる秘密要素ではない。
ウ．パスワードは知識要素、トークンは所持要素で、異なる認証要素の組合せになる。
エ．どちらも知識要素である。

答え・解説 正答：エ

ア：この説明は別候補「指紋と顔認証」に対応するため、誤答候補「パスワードとPIN」の問題点を直接説明していない。
イ：この説明は別候補「社員番号と利用者名」に対応するため、誤答候補「パスワードとPIN」の問題点を直接説明していない。
ウ：この説明は別候補「パスワードとハードウェアトークン」に対応するため、誤答候補「パスワードとPIN」の問題点を直接説明していない。
エ：この説明は誤答候補「パスワードとPIN」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「パスワードとPIN」については、何が誤りかを明確にした上で正しい概念へ戻す。どちらも知識要素である。

対象：2026年度 / 基準日 2026-09-04

Q0053 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：基礎

「認証・認可・アクセス制御」のうち「最小権限」を確認する誤答分析で、学習者が候補「一度付与した権限は退職後も永久に残す。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．不要権限を削除すべきである。
イ．不要な権限を与えないことで誤操作やアカウント侵害時の影響範囲を抑える。
ウ．最小権限に反する。
エ．アクセス制御を放棄している。

答え・解説 正答：ア

ア：この説明は誤答候補「一度付与した権限は退職後も永久に残す。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「利用者やプロセスには、業務遂行に必要な最小限の権限だけを付与する。」に対応するため、誤答候補「一度付与した権限は退職後も永久に残す。」の問題点を直接説明していない。
ウ：この説明は別候補「全利用者に管理者権限を与える。」に対応するため、誤答候補「一度付与した権限は退職後も永久に残す。」の問題点を直接説明していない。
エ：この説明は別候補「権限設定せず全資源を公開する。」に対応するため、誤答候補「一度付与した権限は退職後も永久に残す。」の問題点を直接説明していない。

総合解説：誤答候補「一度付与した権限は退職後も永久に残す。」について、誤りの内容を説明できることが重要である。不要権限を削除すべきである。

対象：2026年度 / 基準日 2026-09-04

Q0054 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：標準

「認証・認可・アクセス制御」のうち「RBAC」を、正答の根拠まで理解できているか確認する。候補「RBAC（Role-Based Access Control）」を妥当と判断する根拠として最も適切な説明はどれか。

ア．複数属性を動的に評価する方式で、職務ロール中心ならRBACが直接的である。
イ．RBACは役割に権限を割り当て、利用者をロールへ所属させる方式で、職務単位の管理に向く。
ウ．権限割当を行わない。
エ．アクセス権モデルではない。

答え・解説 正答：イ

ア：この説明は別候補「ABACだけ」に対応するため、正答候補「RBAC（Role-Based Access Control）」の根拠にはならない。
イ：この説明は正答候補「RBAC（Role-Based Access Control）」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「暗号化だけ」に対応するため、正答候補「RBAC（Role-Based Access Control）」の根拠にはならない。
エ：この説明は別候補「バックアップ制御」に対応するため、正答候補「RBAC（Role-Based Access Control）」の根拠にはならない。

総合解説：正答候補「RBAC（Role-Based Access Control）」を選ぶ根拠は次のとおりである。RBACは役割に権限を割り当て、利用者をロールへ所属させる方式で、職務単位の管理に向く。

対象：2026年度 / 基準日 2026-09-04

Q0055 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：標準

「認証・認可・アクセス制御」の「ABAC」について、候補「ABAC（Attribute-Based Access Control）」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．動的な複数属性評価にはABACが適しやすい。
イ．証明書失効リストである。
ウ．ABACは主体・資源・環境などの属性に基づくポリシーでアクセス判断を行う。
エ．記憶装置冗長化である。

答え・解説 正答：ウ

ア：この説明は別候補「RBACだけで全条件を固定ロール化する。」に対応するため、正答候補「ABAC（Attribute-Based Access Control）」の根拠にはならない。
イ：この説明は別候補「CRL」に対応するため、正答候補「ABAC（Attribute-Based Access Control）」の根拠にはならない。
ウ：この説明は正答候補「ABAC（Attribute-Based Access Control）」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「RAID」に対応するため、正答候補「ABAC（Attribute-Based Access Control）」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ABACは主体・資源・環境などの属性に基づくポリシーでアクセス判断を行う。

対象：2026年度 / 基準日 2026-09-04

Q0056 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：標準

「認証・認可・アクセス制御」の「SSO」を復習している学習者が、候補「各サービスが同一パスワードを平文保存する必要がある。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．組み合わせて利用できる。
イ．認証後も認可が必要である。
ウ．SSOは利便性と認証統制を高められるが、認証基盤が重要な集中点となる。
エ．不要で危険である。

答え・解説 正答：エ

ア：この説明は別候補「SSOでMFAは技術的に禁止される。」に対応するため、誤答候補「各サービスが同一パスワードを平文保存する必要がある。」の問題点を直接説明していない。
イ：この説明は別候補「SSOを使えば認可設計は不要になる。」に対応するため、誤答候補「各サービスが同一パスワードを平文保存する必要がある。」の問題点を直接説明していない。
ウ：この説明は別候補「一度の認証で複数サービスへアクセスしやすくなる一方、認証基盤の侵害や停止の影響が大きくなるので強固な保護が必要である。」に対応するため、誤答候補「各サービスが同一パスワードを平文保存する必要がある。」の問題点を直接説明していない。
エ：この説明は誤答候補「各サービスが同一パスワードを平文保存する必要がある。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「各サービスが同一パスワードを平文保存する必要がある。」については、何が誤りかを明確にした上で正しい概念へ戻す。不要で危険である。

対象：2026年度 / 基準日 2026-09-04

Q0057 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：標準

「認証・認可・アクセス制御」のうち「OAuth/OIDC」を確認する誤答分析で、学習者が候補「OAuth 2.0では秘密鍵を全利用者へ配布する必要がある。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．そのような要件はない。
イ．OAuthは委任認可を扱い、OIDCはその上にIDトークン等を用いた認証レイヤを提供する。
ウ．Web認証・認可領域の仕様である。
エ．認証後にも権限制御が必要である。

答え・解説 正答：ア

ア：この説明は誤答候補「OAuth 2.0では秘密鍵を全利用者へ配布する必要がある。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「OAuth 2.0は主に認可の枠組みで、本人認証を標準化する用途ではOpenID Connectを組み合わせる。」に対応するため、誤答候補「OAuth 2.0では秘密鍵を全利用者へ配布する必要がある。」の問題点を直接説明していない。
ウ：この説明は別候補「OAuth 2.0は圧縮標準、OIDCは暗号鍵長規格である。」に対応するため、誤答候補「OAuth 2.0では秘密鍵を全利用者へ配布する必要がある。」の問題点を直接説明していない。
エ：この説明は別候補「OIDCを使うと認可は一切不要になる。」に対応するため、誤答候補「OAuth 2.0では秘密鍵を全利用者へ配布する必要がある。」の問題点を直接説明していない。

総合解説：誤答候補「OAuth 2.0では秘密鍵を全利用者へ配布する必要がある。」について、誤りの内容を説明できることが重要である。そのような要件はない。

対象：2026年度 / 基準日 2026-09-04

Q0058 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：標準

「認証・認可・アクセス制御」のうち「生体認証」を、正答の根拠まで理解できているか確認する。候補「本人を誤って拒否する本人拒否率（FRR）」を妥当と判断する根拠として最も適切な説明はどれか。

ア．一般に厳しくするとFARは低下方向である。
イ．判定を厳しくすると不正受入れは減りやすい一方、正当な本人まで拒否するFRRが増える傾向がある。
ウ．事業復旧時間である。
エ．脆弱性深刻度指標である。

答え・解説 正答：イ

ア：この説明は別候補「他人を誤って受け入れるFARだけが必ず増える。」に対応するため、正答候補「本人を誤って拒否する本人拒否率（FRR）」の根拠にはならない。
イ：この説明は正答候補「本人を誤って拒否する本人拒否率（FRR）」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「RTO」に対応するため、正答候補「本人を誤って拒否する本人拒否率（FRR）」の根拠にはならない。
エ：この説明は別候補「CVSS」に対応するため、正答候補「本人を誤って拒否する本人拒否率（FRR）」の根拠にはならない。

総合解説：正答候補「本人を誤って拒否する本人拒否率（FRR）」を選ぶ根拠は次のとおりである。判定を厳しくすると不正受入れは減りやすい一方、正当な本人まで拒否するFRRが増える傾向がある。

対象：2026年度 / 基準日 2026-09-04

Q0059 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：応用

「認証・認可・アクセス制御」の「特権ID」について、候補「個人を識別できる管理者認証、必要時だけの特権付与、操作記録・監査、資格情報の保護を組み合わせる。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．責任追跡性を低下させる。
イ．追跡困難になる。
ウ．特権IDは侵害時の影響が大きいため、共有を減らし、個人識別・最小権限・期限付き付与・証跡を整備する。
エ．最小権限に反する。

答え・解説 正答：ウ

ア：この説明は別候補「共有パスワードをさらに多くの人へ配布する。」に対応するため、正答候補「個人を識別できる管理者認証、必要時だけの特権付与、操作記録・監査、資格情報の保護を組み合わせる。」の根拠にはならない。
イ：この説明は別候補「管理操作ログを停止する。」に対応するため、正答候補「個人を識別できる管理者認証、必要時だけの特権付与、操作記録・監査、資格情報の保護を組み合わせる。」の根拠にはならない。
ウ：この説明は正答候補「個人を識別できる管理者認証、必要時だけの特権付与、操作記録・監査、資格情報の保護を組み合わせる。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全一般利用者にもroot権限を付与する。」に対応するため、正答候補「個人を識別できる管理者認証、必要時だけの特権付与、操作記録・監査、資格情報の保護を組み合わせる。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。特権IDは侵害時の影響が大きいため、共有を減らし、個人識別・最小権限・期限付き付与・証跡を整備する。

対象：2026年度 / 基準日 2026-09-04

Q0060 4-2 暗号・認証 > 認証・認可・アクセス制御 ｜ 難易度：応用

「認証・認可・アクセス制御」の「セッション管理」を復習している学習者が、候補「セッションIDを公開ログへ積極的に記録する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．別のリスクである。
イ．この対応は安全性やセキュリティ上のリスクを高めるため適切でない。
ウ．認証後のセッション管理に弱点があれば、攻撃者がセッションを奪って認証を迂回できる場合がある。
エ．漏えいリスクがある。

答え・解説 正答：エ

ア：この説明は別候補「MFAを使えばセッション管理の脆弱性は全て無関係になる。」に対応するため、誤答候補「セッションIDを公開ログへ積極的に記録する。」の問題点を直接説明していない。
イ：この説明は別候補「セッションIDを全利用者で共通にする。」に対応するため、誤答候補「セッションIDを公開ログへ積極的に記録する。」の問題点を直接説明していない。
ウ：この説明は別候補「強いログイン認証だけでは不十分で、セッションIDの十分なランダム性、更新、失効、Cookie保護なども必要である。」に対応するため、誤答候補「セッションIDを公開ログへ積極的に記録する。」の問題点を直接説明していない。
エ：この説明は誤答候補「セッションIDを公開ログへ積極的に記録する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「セッションIDを公開ログへ積極的に記録する。」については、何が誤りかを明確にした上で正しい概念へ戻す。漏えいリスクがある。

対象：2026年度 / 基準日 2026-09-04

Q0061 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：基礎

「マルウェア・ソーシャル・内部不正」のうち「ワーム」を確認する誤答分析で、学習者が候補「ファイル感染型ウイルス」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．一般に他のプログラムやファイルへ寄生して感染を広げる。
イ．ワームは単独で動作し、脆弱性等を利用してネットワーク上へ自己増殖する性質を持つ。
ウ．自己増殖を本質としない。
エ．マルウェアではない。

答え・解説 正答：ア

ア：この説明は誤答候補「ファイル感染型ウイルス」の問題点に対応しており、今回の誤解を直接修正できる。

イ：この説明は別候補「ワーム」に対応するため、誤答候補「ファイル感染型ウイルス」の問題点を直接説明していない。
ウ：この説明は別候補「トロイの木馬」に対応するため、誤答候補「ファイル感染型ウイルス」の問題点を直接説明していない。
エ：この説明は別候補「ルート証明書」に対応するため、誤答候補「ファイル感染型ウイルス」の問題点を直接説明していない。

総合解説：誤答候補「ファイル感染型ウイルス」について、誤りの内容を説明できることが重要である。一般に他のプログラムやファイルへ寄生して感染を広げる。

対象：2026年度 / 基準日 2026-09-04

Q0062 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：基礎

「マルウェア・ソーシャル・内部不正」のうち「ランサムウェア」を、正答の根拠まで理解できているか確認する。候補「ランサムウェア」を妥当と判断する根拠として最も適切な説明はどれか。

ア．広告表示を主目的とするソフトウェアである。
イ．ランサムウェアはデータ暗号化や端末ロック等で利用を妨げ、身代金を要求する。
ウ．開発ツールである。
エ．名前解決機能である。

答え・解説 正答：イ

ア：この説明は別候補「アドウェア」に対応するため、正答候補「ランサムウェア」の根拠にはならない。
イ：この説明は正答候補「ランサムウェア」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「コンパイラ」に対応するため、正答候補「ランサムウェア」の根拠にはならない。
エ：この説明は別候補「DNSリゾルバ」に対応するため、正答候補「ランサムウェア」の根拠にはならない。

総合解説：正答候補「ランサムウェア」を選ぶ根拠は次のとおりである。ランサムウェアはデータ暗号化や端末ロック等で利用を妨げ、身代金を要求する。

対象：2026年度 / 基準日 2026-09-04

Q0063 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：基礎

「マルウェア・ソーシャル・内部不正」の「トロイの木馬」について、候補「トロイの木馬」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．自己増殖・ネットワーク拡散が特徴である。
イ．証明書失効リストである。
ウ．有用・正規に見えるプログラムへ偽装して実行させる手法はトロイの木馬の典型である。
エ．暗号学的処理である。

答え・解説 正答：ウ

ア：この説明は別候補「ワーム」に対応するため、正答候補「トロイの木馬」の根拠にはならない。
イ：この説明は別候補「CRL」に対応するため、正答候補「トロイの木馬」の根拠にはならない。
ウ：この説明は正答候補「トロイの木馬」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「ハッシュ関数」に対応するため、正答候補「トロイの木馬」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。有用・正規に見えるプログラムへ偽装して実行させる手法はトロイの木馬の典型である。

対象：2026年度 / 基準日 2026-09-04

Q0064 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：標準

「マルウェア・ソーシャル・内部不正」の「フィッシング」を復習している学習者が、候補「SQLインジェクション」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．LAN上でARP情報を偽る攻撃である。
イ．メモリ境界を越えた書込み等を悪用する攻撃である。
ウ．信頼できる組織を装ったメールやWebサイトで認証情報等を詐取するのがフィッシングである。
エ．SQL生成へ悪意ある入力を注入する攻撃である。

答え・解説 正答：エ

ア：この説明は別候補「ARPスプーフィング」に対応するため、誤答候補「SQLインジェクション」の問題点を直接説明していない。
イ：この説明は別候補「バッファオーバフロー」に対応するため、誤答候補「SQLインジェクション」の問題点を直接説明していない。
ウ：この説明は別候補「フィッシング」に対応するため、誤答候補「SQLインジェクション」の問題点を直接説明していない。
エ：この説明は誤答候補「SQLインジェクション」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「SQLインジェクション」については、何が誤りかを明確にした上で正しい概念へ戻す。SQL生成へ悪意ある入力を注入する攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0065 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：標準

「マルウェア・ソーシャル・内部不正」のうち「スピアフィッシング」を確認する誤答分析で、学習者が候補「DNSラウンドロビン」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．名前解決を分散する方式である。
イ．特定の組織・個人に合わせて内容を作り込むフィッシングをスピアフィッシングという。
ウ．ポート状態を調べる技術である。
エ．バックアップ方式である。

答え・解説 正答：ア

ア：この説明は誤答候補「DNSラウンドロビン」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「スピアフィッシング」に対応するため、誤答候補「DNSラウンドロビン」の問題点を直接説明していない。
ウ：この説明は別候補「無差別なポートスキャン」に対応するため、誤答候補「DNSラウンドロビン」の問題点を直接説明していない。
エ：この説明は別候補「差分バックアップ」に対応するため、誤答候補「DNSラウンドロビン」の問題点を直接説明していない。

総合解説：誤答候補「DNSラウンドロビン」について、誤りの内容を説明できることが重要である。名前解決を分散する方式である。

対象：2026年度 / 基準日 2026-09-04

Q0066 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：標準

「マルウェア・ソーシャル・内部不正」のうち「内部不正」を、正答の根拠まで理解できているか確認する。候補「職務分掌を行い、登録・申請・承認など相互牽制が必要な権限を別担当へ分離する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．権限集中が進む。
イ．一人が一連の重要処理を完結できないよう権限を分けると、内部不正や誤操作を抑制・発見しやすい。
ウ．監査可能性を失う。
エ．操作追跡が困難になる。

答え・解説 正答：イ

ア：この説明は別候補「一人の担当者にさらに管理者権限を付与する。」に対応するため、正答候補「職務分掌を行い、登録・申請・承認など相互牽制が必要な権限を別担当へ分離する。」の根拠にはならない。
イ：この説明は正答候補「職務分掌を行い、登録・申請・承認など相互牽制が必要な権限を別担当へ分離する。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「承認ログを削除する。」に対応するため、正答候補「職務分掌を行い、登録・申請・承認など相互牽制が必要な権限を別担当へ分離する。」の根拠にはならない。
エ：この説明は別候補「全員で同じIDを共有する。」に対応するため、正答候補「職務分掌を行い、登録・申請・承認など相互牽制が必要な権限を別担当へ分離する。」の根拠にはならない。

総合解説：正答候補「職務分掌を行い、登録・申請・承認など相互牽制が必要な権限を別担当へ分離する。」を選ぶ根拠は次のとおりである。一人が一連の重要処理を完結できないよう権限を分けると、内部不正や誤操作を抑制・発見しやすい。

対象：2026年度 / 基準日 2026-09-04

Q0067 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：標準

「マルウェア・ソーシャル・内部不正」の「ボットネット」について、候補「ボットネット」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．PKIの主体である。
イ．分析用データ集合である。
ウ．攻撃者が遠隔制御する多数の感染端末の集合をボットネットと呼ぶ。
エ．記憶装置の冗長化構成である。

答え・解説 正答：ウ

ア：この説明は別候補「認証局」に対応するため、正答候補「ボットネット」の根拠にはならない。
イ：この説明は別候補「データマート」に対応するため、正答候補「ボットネット」の根拠にはならない。
ウ：この説明は正答候補「ボットネット」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「RAIDグループ」に対応するため、正答候補「ボットネット」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。攻撃者が遠隔制御する多数の感染端末の集合をボットネットと呼ぶ。

対象：2026年度 / 基準日 2026-09-04

Q0068 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：標準

「マルウェア・ソーシャル・内部不正」の「ルートキット」を復習している学習者が、候補「HSM」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．Web攻撃を検知・遮断する防御製品である。
イ．コンテンツ配信を分散する仕組みである。
ウ．ルートキットは侵害後の痕跡や不正活動を隠し、攻撃者の権限維持や潜伏に用いられる。
エ．暗号鍵保護の装置である。

答え・解説 正答：エ

ア：この説明は別候補「WAF」に対応するため、誤答候補「HSM」の問題点を直接説明していない。
イ：この説明は別候補「CDN」に対応するため、誤答候補「HSM」の問題点を直接説明していない。
ウ：この説明は別候補「ルートキット」に対応するため、誤答候補「HSM」の問題点を直接説明していない。

エ：この説明は誤答候補「HSM」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「HSM」については、何が誤りかを明確にした上で正しい概念へ戻す。暗号鍵保護の装置である。

対象：2026年度 / 基準日 2026-09-04

Q0069 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：応用

「マルウェア・ソーシャル・内部不正」のうち「ランサム初動」を確認する誤答分析で、学習者が候補「管理者資格情報を全端末へ配布する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．侵害範囲を拡大させ得る。
イ．感染拡大を抑える隔離と、インシデント対応体制への通報、証拠やログの保全を両立させることが重要である。
ウ．感染拡大を助長し得る。
エ．原因調査に必要な証拠を失う。

答え・解説 正答：ア

ア：この説明は誤答候補「管理者資格情報を全端末へ配布する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「組織の手順に従って感染端末をネットワークから隔離し、関係部署へ連絡し、証拠保全と影響範囲確認を進める。」に対応するため、誤答候補「管理者資格情報を全端末へ配布する。」の問題点を直接説明していない。
ウ：この説明は別候補「感染端末を接続したまま全共有フォルダを開く。」に対応するため、誤答候補「管理者資格情報を全端末へ配布する。」の問題点を直接説明していない。
エ：この説明は別候補「証拠となるログやファイルを全て削除する。」に対応するため、誤答候補「管理者資格情報を全端末へ配布する。」の問題点を直接説明していない。

総合解説：誤答候補「管理者資格情報を全端末へ配布する。」について、誤りの内容を説明できることが重要である。侵害範囲を拡大させ得る。

対象：2026年度 / 基準日 2026-09-04

Q0070 4-3 攻撃・脆弱性 > マルウェア・ソーシャル・内部不正 ｜ 難易度：応用

「マルウェア・ソーシャル・内部不正」のうち「MFA疲労」を、正答の根拠まで理解できているか確認する。候補「利用者教育、異常なMFA要求への検知・制限、条件付きアクセス、最小権限、アクセスログ監視を組み合わせる。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．一つの対策だけに依存する。
イ．人的対策だけでなく、認証要求の異常検知、アクセス制御、権限最小化、監視を重ねる多層防御が有効である。
ウ．認証強度が低下する。
エ．検知・調査能力を失う。

答え・解説 正答：イ

ア：この説明は別候補「社員教育だけ実施し技術対策を全て廃止する。」に対応するため、正答候補「利用者教育、異常なMFA要求への検知・制限、条件付きアクセス、最小権限、アクセスログ監視を組み合わせる。」の根拠にはならない。
イ：この説明は正答候補「利用者教育、異常なMFA要求への検知・制限、条件付きアクセス、最小権限、アクセスログ監視を組み合わせる。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「MFAを廃止してパスワードだけに戻す。」に対応するため、正答候補「利用者教育、異常なMFA要求への検知・制限、条件付きアクセス、最小権限、アクセスログ監視を組み合わせる。」の根拠にはならない。
エ：この説明は別候補「ログを記録しない。」に対応するため、正答候補「利用者教育、異常なMFA要求への検知・制限、条件付きアクセス、最小権限、アクセスログ監視を組み合わせる。」の根拠にはならない。

総合解説：正答候補「利用者教育、異常なMFA要求への検知・制限、条件付きアクセス、最小権限、アクセスログ監視を組み合わせる。」を選ぶ根拠は次のとおりである。人的対策だけでなく、認証要求の異常検知、アクセス制御、権限最小化、監視を重ねる多層防御が有効である。

対象：2026年度 / 基準日 2026-09-04

Q0071 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：基礎

「Web・アプリケーション攻撃」の「SQLインジェクション」について、候補「SQLインジェクション」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．ブラウザで悪意あるスクリプトを実行させる攻撃である。
イ．認証済み利用者へ意図しない要求を送らせる攻撃である。
ウ．信頼できない入力をSQLコードとして解釈させ、認証回避や不正参照・更新を狙う攻撃である。
エ．LAN上でARP情報を偽る攻撃である。

答え・解説 正答：ウ

ア：この説明は別候補「XSS」に対応するため、正答候補「SQLインジェクション」の根拠にはならない。
イ：この説明は別候補「CSRF」に対応するため、正答候補「SQLインジェクション」の根拠にはならない。
ウ：この説明は正答候補「SQLインジェクション」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「ARPスプーフィング」に対応するため、正答候補「SQLインジェクション」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。信頼できない入力をSQLコードとして解釈させ、認証回避や不正参照・更新を狙う攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0072 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：基礎

「Web・アプリケーション攻撃」の「XSS」を復習している学習者が、候補「パスワードリスト攻撃」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．SQLへの注入である。
イ．TCP資源を悪用するDoSである。
ウ．信頼できないデータをHTML等へ安全に出力せず、ブラウザでスクリプトとして実行させるのがXSSである。
エ．漏えい済み資格情報を試す攻撃である。

答え・解説 正答：エ

ア：この説明は別候補「SQLインジェクション」に対応するため、誤答候補「パスワードリスト攻撃」の問題点を直接説明していない。
イ：この説明は別候補「SYN Flood」に対応するため、誤答候補「パスワードリスト攻撃」の問題点を直接説明していない。
ウ：この説明は別候補「クロスサイトスクリプティング（XSS）」に対応するため、誤答候補「パスワードリスト攻撃」の問題点を直接説明していない。
エ：この説明は誤答候補「パスワードリスト攻撃」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「パスワードリスト攻撃」については、何が誤りかを明確にした上で正しい概念へ戻す。漏えい済み資格情報を試す攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0073 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：基礎

「Web・アプリケーション攻撃」のうち「CSRF」を確認する誤答分析で、学習者が候補「XSS」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．スクリプト注入・実行が中心である。
イ．CSRFは認証済みブラウザに意図しない状態変更リクエストを送らせる攻撃である。
ウ．DNS応答を偽情報へ汚染する。
エ．公開ポートを探索する。

答え・解説 正答：ア

ア：この説明は誤答候補「XSS」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「CSRF（Cross-Site Request Forgery）」に対応するため、誤答候補「XSS」の問題点を直接説明していない。
ウ：この説明は別候補「DNSキャッシュポイズニング」に対応するため、誤答候補「XSS」の問題点を直接説明していない。
エ：この説明は別候補「ポートスキャン」に対応するため、誤答候補「XSS」の問題点を直接説明していない。

総合解説：誤答候補「XSS」について、誤りの内容を説明できることが重要である。スクリプト注入・実行が中心である。

対象：2026年度 / 基準日 2026-09-04

Q0074 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：標準

「Web・アプリケーション攻撃」のうち「SQLi対策」を、正答の根拠まで理解できているか確認する。候補「入力値をSQL構文と分離するパラメータ化クエリ（prepared statement等）を用いる。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．攻撃文字列がSQL構文として解釈され得る。
イ．OWASPはデータをコマンド・クエリと分離する安全なAPIやパラメータ化を推奨している。
ウ．内部情報漏えいにつながる。
エ．侵害時の被害を拡大する。

答え・解説 正答：イ

ア：この説明は別候補「利用者入力をそのままSQL文字列へ連結する。」に対応するため、正答候補「入力値をSQL構文と分離するパラメータ化クエリ（prepared statement等）を用いる。」の根拠にはならない。
イ：この説明は正答候補「入力値をSQL構文と分離するパラメータ化クエリ（prepared statement等）を用いる。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「SQLエラーを詳細なスタックトレース付きで常時表示する。」に対応するため、正答候補「入力値をSQL構文と分離するパラメータ化クエリ（prepared statement等）を用いる。」の根拠にはならない。
エ：この説明は別候補「DBアカウントへ常に最高権限を付与する。」に対応するため、正答候補「入力値をSQL構文と分離するパラメータ化クエリ（prepared statement等）を用いる。」の根拠にはならない。

総合解説：正答候補「入力値をSQL構文と分離するパラメータ化クエリ（prepared statement等）を用いる。」を選ぶ根拠は次のとおりである。OWASPはデータをコマンド・クエリと分離する安全なAPIやパラメータ化を推奨している。

対象：2026年度 / 基準日 2026-09-04

Q0075 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：標準

「Web・アプリケーション攻撃」の「XSS対策」について、候補「出力先の文脈に応じて適切なエスケープ・エンコーディングを行い、必要に応じCSP等も併用する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．単純文字列置換だけでは不十分である。
イ．Cookie漏えいリスクを高める。
ウ．信頼できない入力がHTMLやJavaScriptとして解釈されないよう、出力文脈に応じたエンコーディングが重要である。
エ．XSS対策と無関係である。

答え・解説 正答：ウ

ア：この説明は別候補「<script>だけ削除すれば全XSSを防げる。」に対応するため、正答候補「出力先の文脈に応じて適切なエスケープ・エンコーディングを行い、必要に応じCSP等も併用する。」の根拠にはならない。
イ：この説明は別候補「全CookieからSecure属性を外す。」に対応するため、正答候補「出力先の文脈に応じて適切なエスケープ・エンコーディングを行い、必要に応じCSP等も併用する。」の根拠にはならない。
ウ：この説明は正答候補「出力先の文脈に応じて適切なエスケープ・エンコーディングを行い、必要に応じCSP等も併用する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「DBの外部キーを削除する。」に対応するため、正答候補「出力先の文脈に応じて適切なエスケープ・エンコーディングを行い、必要に応じCSP等も併用する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。信頼できない入力がHTMLやJavaScriptとして解釈されないよう、出力文脈に応じたエンコーディングが重要である。

対象：2026年度 / 基準日 2026-09-04

Q0076 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：標準

「Web・アプリケーション攻撃」の「CSRF対策」を復習している学習者が、候補「GETなら金銭送金など重要操作も無条件に実行する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．容易に再利用される。
イ．漏えいリスクが高い。
ウ．認証Cookieだけに依存せず、正規画面からの要求であることを追加検証することが重要である。
エ．CSRFリスクを高める。

答え・解説 正答：エ

ア：この説明は別候補「CSRFトークンを全利用者で固定の公開値にする。」に対応するため、誤答候補「GETなら金銭送金など重要操作も無条件に実行する。」の問題点を直接説明していない。
イ：この説明は別候補「認証CookieをURLへ常に付与する。」に対応するため、誤答候補「GETなら金銭送金など重要操作も無条件に実行する。」の問題点を直接説明していない。
ウ：この説明は別候補「予測困難なCSRFトークンの検証やSameSite Cookieなどを用い、意図しないクロスサイト要求を拒否する。」に対応するため、誤答候補「GETなら金銭送金など重要操作も無条件に実行する。」の問題点を直接説明していない。
エ：この説明は誤答候補「GETなら金銭送金など重要操作も無条件に実行する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「GETなら金銭送金など重要操作も無条件に実行する。」については、何が誤りかを明確にした上で正しい概念へ戻す。CSRFリスクを高める。

対象：2026年度 / 基準日 2026-09-04

Q0077 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：標準

「Web・アプリケーション攻撃」のうち「パストラバーサル」を確認する誤答分析で、学習者が候補「エラーにサーバの絶対パスを常時表示する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．内部情報を与える。
イ．利用者入力をそのままファイルパスとして使わず、許可対象を限定し正規化後のパス境界を確認することが重要である。
ウ．任意パスへ到達する危険がある。
エ．侵害時の影響が大きい。

答え・解説 正答：ア

ア：この説明は誤答候補「エラーにサーバの絶対パスを常時表示する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「利用可能なファイルをID等でホワイトリスト管理し、正規化後のパスが許可ディレクトリ外へ出ないことを検証する。」に対応するため、誤答候補「エラーにサーバの絶対パスを常時表示する。」の問題点を直接説明していない。
ウ：この説明は別候補「入力をそのままOSのパスへ連結する。」に対応するため、誤答候補「エラーにサーバの絶対パスを常時表示する。」の問題点を直接説明していない。
エ：この説明は別候補「Webサーバをroot権限で動かす。」に対応するため、誤答候補「エラーにサーバの絶対パスを常時表示する。」の問題点を直接説明していない。

総合解説：誤答候補「エラーにサーバの絶対パスを常時表示する。」について、誤りの内容を説明できることが重要である。内部情報を与える。

対象：2026年度 / 基準日 2026-09-04

Q0078 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：標準

「Web・アプリケーション攻撃」のうち「OSコマンド注入」を、正答の根拠まで理解できているか確認する。候補「可能ならシェルを介さない安全なAPIを使用し、必要な入力を厳格に制限してコマンドとデータを分離する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．追加コマンドを注入しやすくなる。
イ．信頼できない入力をシェルコマンドへ連結すると追加コマンド実行につながるため、安全なAPI利用が有効である。
ウ．被害を拡大する。
エ．情報漏えいにつながる。

答え・解説 正答：イ

ア：この説明は別候補「入力に任意の「;」や「&&」を許可する。」に対応するため、正答候補「可能ならシェルを介さない安全なAPIを使用し、必要な入力を厳格に制限してコマンドとデータを分離する。」の根拠にはならない。
イ：この説明は正答候補「可能ならシェルを介さない安全なAPIを使用し、必要な入力を厳格に制限してコマンドとデータを分離する。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「Webサーバを常に管理者権限で実行する。」に対応するため、正答候補「可能ならシェルを介さない安全なAPIを使用し、必要な入力を厳格に制限してコマンドとデータを分離する。」の根拠にはならない。
エ：この説明は別候補「コマンド実行結果を全て公開Webへ保存する。」に対応するため、正答候補「可能ならシェルを介さない安全なAPIを使用し、必要な入力を厳格に制限してコマンドとデータを分離する。」の根拠にはならない。

総合解説：正答候補「可能ならシェルを介さない安全なAPIを使用し、必要な入力を厳格に制限してコマンドとデータを分離する。」を選ぶ根拠は次のとおりである。信頼できない入力をシェルコマンドへ連結すると追加コマンド実行につながるため、安全なAPI利用が有効である。

対象：2026年度 / 基準日 2026-09-04

Q0079 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：応用

「Web・アプリケーション攻撃」の「SSRF」について、候補「SSRF（Server-Side Request Forgery）」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．ブラウザに認証済み要求を送らせる攻撃である。
イ．ブラウザ上でスクリプトを実行させる攻撃である。
ウ．SSRFはサーバを踏み台にして、本来外部から到達できない内部・ローカル・クラウドメタデータ等へリクエストさせる攻撃である。
エ．LAN上のARPキャッシュを偽装する攻撃である。

答え・解説 正答：ウ

ア：この説明は別候補「CSRF」に対応するため、正答候補「SSRF（Server-Side Request Forgery）」の根拠にはならない。
イ：この説明は別候補「XSS」に対応するため、正答候補「SSRF（Server-Side Request Forgery）」の根拠にはならない。
ウ：この説明は正答候補「SSRF（Server-Side Request Forgery）」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「ARPスプーフィング」に対応するため、正答候補「SSRF（Server-Side Request Forgery）」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。SSRFはサーバを踏み台にして、本来外部から到達できない内部・ローカル・クラウドメタデータ等へリクエストさせる攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0080 4-3 攻撃・脆弱性 > Web・アプリケーション攻撃 ｜ 難易度：応用

「Web・アプリケーション攻撃」の「Webセキュリティ総合」を復習している学習者が、候補「本番公開後に事故が起きた場合だけ考える。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．サーバ側検証・認可が必要である。
イ．過剰権限になる。
ウ．単一の入力検証だけでは複数種類の脆弱性を防げないため、設計・実装・テスト・運用を通じた多層のセキュア開発が必要である。
エ．設計段階から組み込むべきである。

答え・解説 正答：エ

ア：この説明は別候補「全対策をブラウザ側JavaScriptだけに任せる。」に対応するため、誤答候補「本番公開後に事故が起きた場合だけ考える。」の問題点を直接説明していない。
イ：この説明は別候補「全利用者を管理者として扱う。」に対応するため、誤答候補「本番公開後に事故が起きた場合だけ考える。」の問題点を直接説明していない。
ウ：この説明は別候補「安全なAPI・パラメータ化、出力エンコーディング、サーバ側認可、強固な認証・セッション管理、セキュリティテストをSDLCへ組み込む。」に対応するため、誤答候補「本番公開後に事故が起きた場合だけ考える。」の問題点を直接説明していない。
エ：この説明は誤答候補「本番公開後に事故が起きた場合だけ考える。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「本番公開後に事故が起きた場合だけ考える。」については、何が誤りかを明確にした上で正しい概念へ戻す。設計段階から組み込むべきである。

対象：2026年度 / 基準日 2026-09-04

Q0081 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：基礎

「ネットワーク・システム攻撃」のうち「DDoS」を確認する誤答分析で、学習者が候補「電子署名」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．今回問われている攻撃手法には該当しない。
イ．複数の分散した攻撃元からサービスへ負荷を集中させるDoSをDDoSという。
ウ．SQL構文への注入攻撃である。
エ．認証済みブラウザへ意図しない要求を送らせる。

答え・解説 正答：ア

ア：この説明は誤答候補「電子署名」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「DDoS攻撃」に対応するため、誤答候補「電子署名」の問題点を直接説明していない。

ウ：この説明は別候補「SQLインジェクション」に対応するため、誤答候補「電子署名」の問題点を直接説明していない。
エ：この説明は別候補「CSRF」に対応するため、誤答候補「電子署名」の問題点を直接説明していない。

総合解説：誤答候補「電子署名」について、誤りの内容を説明できることが重要である。今回問われている攻撃手法には該当しない。

対象：2026年度 / 基準日 2026-09-04

Q0082 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：基礎

「ネットワーク・システム攻撃」のうち「SYN Flood」を、正答の根拠まで理解できているか確認する。候補「SYN Flood」を妥当と判断する根拠として最も適切な説明はどれか。

ア．DNS同期の仕組みである。
イ．SYN FloodはTCP接続要求を大量に発生させ、半開状態等の管理資源を消費させるDoS攻撃である。

ウ．ブラウザ上の攻撃である。
エ．データ圧縮である。

答え・解説 正答：イ

ア：この説明は別候補「DNSゾーン転送」に対応するため、正答候補「SYN Flood」の根拠にはならない。
イ：この説明は正答候補「SYN Flood」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「XSS」に対応するため、正答候補「SYN Flood」の根拠にはならない。
エ：この説明は別候補「辞書圧縮」に対応するため、正答候補「SYN Flood」の根拠にはならない。

総合解説：正答候補「SYN Flood」を選ぶ根拠は次のとおりである。SYN FloodはTCP接続要求を大量に発生させ、半開状態等の管理資源を消費させるDoS攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0083 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：基礎

「ネットワーク・システム攻撃」の「ARPスプーフィング」について、候補「ARPスプーフィング（ARPポイズニング）」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．DNS真正性検証を支援する技術である。
イ．DBへの入力注入である。
ウ．ARP情報を偽装して通信を攻撃者端末へ迂回させ、盗聴や改ざんにつなげる攻撃である。
エ．総当たり攻撃である。

答え・解説 正答：ウ

ア：この説明は別候補「DNSSEC」に対応するため、正答候補「ARPスプーフィング（ARPポイズニング）」の根拠にはならない。
イ：この説明は別候補「SQLインジェクション」に対応するため、正答候補「ARPスプーフィング（ARPポイズニング）」の根拠にはならない。
ウ：この説明は正答候補「ARPスプーフィング（ARPポイズニング）」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「ブルートフォース」に対応するため、正答候補「ARPスプーフィング（ARPポイズニング）」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ARP情報を偽装して通信を攻撃者端末へ迂回させ、盗聴や改ざんにつなげる攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0084 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：標準

「ネットワーク・システム攻撃」の「DNSポイズニング」を復習している学習者が、候補「パスワードスプレー」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．IP-MAC対応を偽装する。
イ．Webページへスクリプトを注入する。
ウ．DNSキャッシュへ不正な対応情報を登録させると、正しいドメイン名でも偽IPへ誘導され得る。
エ．少数パスワードを多数IDへ試す。

答え・解説 正答：エ

ア：この説明は別候補「ARPスプーフィング」に対応するため、誤答候補「パスワードスプレー」の問題点を直接説明していない。
イ：この説明は別候補「XSS」に対応するため、誤答候補「パスワードスプレー」の問題点を直接説明していない。
ウ：この説明は別候補「DNSキャッシュポイズニング」に対応するため、誤答候補「パスワードスプレー」の問題点を直接説明していない。
エ：この説明は誤答候補「パスワードスプレー」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「パスワードスプレー」については、何が誤りかを明確にした上で正しい概念へ戻す。少数パスワードを多数IDへ試す。

対象：2026年度 / 基準日 2026-09-04

Q0085 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：標準

「ネットワーク・システム攻撃」のうち「MITM」を確認する誤答分析で、学習者が候補「証明書警告を常に無視する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．偽証明書を受け入れる危険がある。
イ．暗号化だけでなく接続先の真正性を証明書で検証することが中間者攻撃への防御に重要である。
ウ．盗聴・改ざんが容易になる。
エ．機密性を損なう。

答え・解説 正答：ア

ア：この説明は誤答候補「証明書警告を常に無視する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「TLSで通信を暗号化し、サーバ証明書のホスト名・信頼チェーン等を適切に検証する。」に対応するため、誤答候補「証明書警告を常に無視する。」の問題点を直接説明していない。
ウ：この説明は別候補「HTTPへ切り替える。」に対応するため、誤答候補「証明書警告を常に無視する。」の問題点を直接説明していない。
エ：この説明は別候補「全通信内容を公開SNSへコピーする。」に対応するため、誤答候補「証明書警告を常に無視する。」の問題点を直接説明していない。

総合解説：誤答候補「証明書警告を常に無視する。」について、誤りの内容を説明できることが重要である。偽証明書を受け入れる危険がある。

対象：2026年度 / 基準日 2026-09-04

Q0086 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：標準

「ネットワーク・システム攻撃」のうち「IPスプーフィング」を、正答の根拠まで理解できているか確認する。候補「IPスプーフィング」を妥当と判断する根拠として最も適切な説明はどれか。

ア．SQLへの入力注入である。
イ．IPヘッダの送信元アドレスを偽る攻撃をIPスプーフィングという。
ウ．UIを悪用するWeb攻撃である。
エ．DB障害回復の仕組みである。

答え・解説 正答：イ

ア：この説明は別候補「SQLインジェクション」に対応するため、正答候補「IPスプーフィング」の根拠にはならない。
イ：この説明は正答候補「IPスプーフィング」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「クリックジャッキング」に対応するため、正答候補「IPスプーフィング」の根拠にはならない。
エ：この説明は別候補「チェックポイント」に対応するため、正答候補「IPスプーフィング」の根拠にはならない。

総合解説：正答候補「IPスプーフィング」を選ぶ根拠は次のとおりである。IPヘッダの送信元アドレスを偽る攻撃をIPスプーフィングという。

対象：2026年度 / 基準日 2026-09-04

Q0087 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：標準

「ネットワーク・システム攻撃」の「ポートスキャン」について、候補「ポートスキャン」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．認証情報保護である。
イ．真正性・完全性確認である。
ウ．ポートスキャンは公開・応答するポートを調査し、動作中サービスや攻撃対象候補を把握する偵察行為である。
エ．バックアップ方式である。

答え・解説 正答：ウ

ア：この説明は別候補「パスワードハッシュ」に対応するため、正答候補「ポートスキャン」の根拠にはならない。
イ：この説明は別候補「電子署名」に対応するため、正答候補「ポートスキャン」の根拠にはならない。
ウ：この説明は正答候補「ポートスキャン」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「差分バックアップ」に対応するため、正答候補「ポートスキャン」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ポートスキャンは公開・応答するポートを調査し、動作中サービスや攻撃対象候補を把握する偵察行為である。

対象：2026年度 / 基準日 2026-09-04

Q0088 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：標準

「ネットワーク・システム攻撃」の「パスワードスプレー」を復習している学習者が、候補「パスワードリスト攻撃」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．DoS攻撃である。
イ．ファイルパス攻撃である。
ウ．多数アカウントに対して少数候補を分散して試すことで、アカウントロックを回避しながら突破を狙う。
エ．漏えい済みID・パスワード組を他サービスへ試す攻撃である。

答え・解説 正答：エ

ア：この説明は別候補「SYN Flood」に対応するため、誤答候補「パスワードリスト攻撃」の問題点を直接説明していない。
イ：この説明は別候補「ディレクトリトラバーサル」に対応するため、誤答候補「パスワードリスト攻撃」の問題点を直接説明していない。
ウ：この説明は別候補「パスワードスプレー攻撃」に対応するため、誤答候補「パスワードリスト攻撃」の問題点を直接説明していない。
エ：この説明は誤答候補「パスワードリスト攻撃」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「パスワードリスト攻撃」については、何が誤りかを明確にした上で正しい概念へ戻す。漏えい済みID・パスワード組を他サービスへ試す攻撃である。

対象：2026年度 / 基準日 2026-09-04

Q0089 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：応用

「ネットワーク・システム攻撃」のうち「ラテラルムーブメント」を確認する誤答分析で、学習者が候補「負荷分散」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．可用性技術である。
イ．初期侵入後に他ホストやアカウントへ移動して侵害範囲を広げる活動をラテラルムーブメントという。
ウ．DB論理設計である。
エ．鍵管理である。

答え・解説 正答：ア

ア：この説明は誤答候補「負荷分散」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「ラテラルムーブメント（横展開）」に対応するため、誤答候補「負荷分散」の問題点を直接説明していない。
ウ：この説明は別候補「データ正規化」に対応するため、誤答候補「負荷分散」の問題点を直接説明していない。
エ：この説明は別候補「鍵ローテーション」に対応するため、誤答候補「負荷分散」の問題点を直接説明していない。

総合解説：誤答候補「負荷分散」について、誤りの内容を説明できることが重要である。可用性技術である。

対象：2026年度 / 基準日 2026-09-04

Q0090 4-3 攻撃・脆弱性 > ネットワーク・システム攻撃 ｜ 難易度：応用

「ネットワーク・システム攻撃」のうち「ネットワーク防御総合」を、正答の根拠まで理解できているか確認する。候補「ネットワーク分離・アクセス制御、端末防御、最小権限、MFA、脆弱性管理、ログ監視を組み合わせる。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．横展開しやすくなる。
イ．侵入を完全に防げない前提で、横展開を制限し、資格情報悪用を難しくし、異常を検知できる多層防御が有効である。
ウ．検知・予防能力を低下させる。
エ．資格情報漏えいの影響が全社へ広がる。

答え・解説 正答：イ

ア：この説明は別候補「社内は安全と仮定し全端末間通信と管理ポートを無制限に許可する。」に対応するため、正答候補「ネットワーク分離・アクセス制御、端末防御、最小権限、MFA、脆弱性管理、ログ監視を組み合わせる。」の根拠にはならない。
イ：この説明は正答候補「ネットワーク分離・アクセス制御、端末防御、最小権限、MFA、脆弱性管理、ログ監視を組み合わせる。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「ログ停止とパッチ未適用を徹底する。」に対応するため、正答候補「ネットワーク分離・アクセス制御、端末防御、最小権限、MFA、脆弱性管理、ログ監視を組み合わせる。」の根拠にはならない。
エ：この説明は別候補「全社員へ同一管理者パスワードを配布する。」に対応するため、正答候補「ネットワーク分離・アクセス制御、端末防御、最小権限、MFA、脆弱性管理、ログ監視を組み合わせる。」の根拠にはならない。

総合解説：正答候補「ネットワーク分離・アクセス制御、端末防御、最小権限、MFA、脆弱性管理、ログ監視を組み合わせる。」を選ぶ根拠は次のとおりである。侵入を完全に防げない前提で、横展開を制限し、資格情報悪用を難しくし、異常を検知できる多層防御が有効である。

対象：2026年度 / 基準日 2026-09-04

Q0091 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：基礎

「FW・WAF・VPN・IDS/IPS等」の「FW基本」について、候補「定めたポリシーに基づいてネットワーク間又はホストの通信を許可・拒否する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．保存データ暗号化は別機能である。
イ．認証機能でありFWの基本機能ではない。
ウ．ファイアウォールは異なるセキュリティ境界間の通信を制御する。
エ．ポリシーに基づく制御にならない。

答え・解説 正答：ウ

ア：この説明は別候補「ファイルの内容を必ず暗号化して保存する。」に対応するため、正答候補「定めたポリシーに基づいてネットワーク間又はホストの通信を許可・拒否する。」の根拠にはならない。
イ：この説明は別候補「利用者の生体情報を照合する。」に対応するため、正答候補「定めたポリシーに基づいてネットワーク間又はホストの通信を許可・拒否する。」の根拠にはならない。
ウ：この説明は正答候補「定めたポリシーに基づいてネットワーク間又はホストの通信を許可・拒否する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全通信を無条件に許可する。」に対応するため、正答候補「定めたポリシーに基づいてネットワーク間又はホストの通信を許可・拒否する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ファイアウォールは異なるセキュリティ境界間の通信を制御する。

対象：2026年度 / 基準日 2026-09-04

Q0092 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：基礎

「FW・WAF・VPN・IDS/IPS等」の「WAF基本」を復習している学習者が、候補「CPU命令の実行順序」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．WAFの対象ではない。
イ．WAFはWebアプリケーション層の通信を解析し、SQLインジェクションやXSS等の攻撃検知・遮断に利用される。
ウ．物理セキュリティである。
エ．プロセッサ制御である。

答え・解説 正答：エ

ア：この説明は別候補「ディスク装置の物理故障」に対応するため、誤答候補「CPU命令の実行順序」の問題点を直接説明していない。
イ：この説明は別候補「HTTP/HTTPSを用いるWebアプリケーションへの攻撃通信」に対応するため、誤答候補「CPU命令の実行順序」の問題点を直接説明していない。
ウ：この説明は別候補「建物への不正侵入」に対応するため、誤答候補「CPU命令の実行順序」の問題点を直接説明していない。
エ：この説明は誤答候補「CPU命令の実行順序」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「CPU命令の実行順序」については、何が誤りかを明確にした上で正しい概念へ戻す。プロセッサ制御である。

対象：2026年度 / 基準日 2026-09-04

Q0093 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：基礎

「FW・WAF・VPN・IDS/IPS等」のうち「IDS/IPS」を確認する誤答分析で、学習者が候補「IDSとIPSは必ず全く同じ配置・動作をする。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．目的と動作方式が異なり得る。
イ．PKIの機能である。
ウ．バックアップ機能ではない。
エ．IDSは監視・検知、IPSはインラインでの遮断など能動的防御まで行う点が代表的な違いである。

答え・解説 正答：ア

ア：この説明は誤答候補「IDSとIPSは必ず全く同じ配置・動作をする。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「IDSは暗号鍵を発行し、IPSは証明書を失効させる。」に対応するため、誤答候補「IDSとIPSは必ず全く同じ配置・動作をする。」の問題点を直接説明していない。
ウ：この説明は別候補「IDSはバックアップ、IPSは復元を行う。」に対応するため、誤答候補「IDSとIPSは必ず全く同じ配置・動作をする。」の問題点を直接説明していない。
エ：この説明は別候補「IDSは主に侵入兆候の検知・通知を行い、IPSは検知に加えて通信遮断などの防御を自動実行できる。」に対応するため、誤答候補「IDSとIPSは必ず全く同じ配置・動作をする。」の問題点を直接説明していない。

総合解説：誤答候補「IDSとIPSは必ず全く同じ配置・動作をする。」について、誤りの内容を説明できることが重要である。目的と動作方式が異なり得る。

対象：2026年度 / 基準日 2026-09-04

Q0094 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：基礎

「FW・WAF・VPN・IDS/IPS等」のうち「VPN基本」を、正答の根拠まで理解できているか確認する。候補「VPN」を妥当と判断する根拠として最も適切な説明はどれか。

ア．LAN内論理分割であり公衆網越し通信の暗号化を直接提供しない。
イ．VPNは既存ネットワーク上に論理的な保護通信路を構成し、IPsec等で機密性・完全性等を提供できる。
ウ．アドレス変換であり通信内容の暗号化を保証しない。
エ．名前解決情報である。

答え・解説 正答：イ

ア：この説明は別候補「VLANだけ」に対応するため、正答候補「VPN」の根拠にはならない。
イ：この説明は正答候補「VPN」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「NATだけ」に対応するため、正答候補「VPN」の根拠にはならない。
エ：この説明は別候補「DNSキャッシュだけ」に対応するため、正答候補「VPN」の根拠にはならない。

総合解説：正答候補「VPN」を選ぶ根拠は次のとおりである。VPNは既存ネットワーク上に論理的な保護通信路を構成し、IPsec等で機密性・完全性等を提供できる。

対象：2026年度 / 基準日 2026-09-04

Q0095 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：標準

「FW・WAF・VPN・IDS/IPS等」の「ステートフルFW」について、候補「ステートフルインスペクションを行うファイアウォール」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．個々のパケット情報だけでは接続状態を直接利用できない。
イ．Webアプリ層の防御が中心で、一般TCP接続状態管理の代替ではない。
ウ．接続状態を追跡することで、確立済み通信に対応する戻りトラフィックを判断できる。
エ．鍵保護装置である。

答え・解説 正答：ウ

ア：この説明は別候補「単純な静的パケットフィルタだけで接続状態を一切保持しない方式」に対応するため、正答候補「ステートフルインスペクションを行うファイアウォール」の根拠にはならない。
イ：この説明は別候補「WAFだけ」に対応するため、正答候補「ステートフルインスペクションを行うファイアウォール」の根拠にはならない。
ウ：この説明は正答候補「ステートフルインスペクションを行うファイアウォール」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「HSM」に対応するため、正答候補「ステートフルインスペクションを行うファイアウォール」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。接続状態を追跡することで、確立済み通信に対応する戻りトラフィックを判断できる。

対象：2026年度 / 基準日 2026-09-04

Q0096 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：標準

「FW・WAF・VPN・IDS/IPS等」の「DMZ設計」を復習している学習者が、候補「DBの正規化を進めるため。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．主目的はセキュリティ境界の分離である。
イ．DMZは外部公開系と内部系の境界を分け、通信経路と許可ルールを限定する。
ウ．鍵長とは無関係である。
エ．DB論理設計とは別である。

答え・解説 正答：エ

ア：この説明は別候補「Webサーバを必ず高速化するため。」に対応するため、誤答候補「DBの正規化を進めるため。」の問題点を直接説明していない。
イ：この説明は別候補「公開サーバが侵害された場合でも、社内ネットワークへの直接到達を制限しやすくするため。」に対応するため、誤答候補「DBの正規化を進めるため。」の問題点を直接説明していない。
ウ：この説明は別候補「暗号鍵長を自動的に増やすため。」に対応するため、誤答候補「DBの正規化を進めるため。」の問題点を直接説明していない。
エ：この説明は誤答候補「DBの正規化を進めるため。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「DBの正規化を進めるため。」については、何が誤りかを明確にした上で正しい概念へ戻す。DB論理設計とは別である。

対象：2026年度 / 基準日 2026-09-04

Q0097 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：標準

「FW・WAF・VPN・IDS/IPS等」のうち「WAF限界」を確認する誤答分析で、学習者が候補「WAF導入後はアプリの脆弱性修正が不要になる。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．根本修正は必要である。
イ．今回問われている内容とは適用対象が異なる。
ウ．WAFは特定の攻撃パターンを検知・遮断できるが、アプリ設計・実装上の欠陥を全て解決するものではない。
エ．未知攻撃を完全保証できない。

答え・解説 正答：ア

ア：この説明は誤答候補「WAF導入後はアプリの脆弱性修正が不要になる。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「WAFは物理入退室管理を自動化する。」に対応するため、誤答候補「WAF導入後はアプリの脆弱性修正が不要になる。」の問題点を直接説明していない。
ウ：この説明は別候補「WAFは有効な補助防御だが、認証・認可不備や脆弱な業務ロジックを全て自動的に修正するものではない。」に対応するため、誤答候補「WAF導入後はアプリの脆弱性修正が不要になる。」の問題点を直接説明していない。
エ：この説明は別候補「WAFは必ず全てのゼロデイ攻撃を完全遮断する。」に対応するため、誤答候補「WAF導入後はアプリの脆弱性修正が不要になる。」の問題点を直接説明していない。

総合解説：誤答候補「WAF導入後はアプリの脆弱性修正が不要になる。」について、誤りの内容を説明できることが重要である。根本修正は必要である。

対象：2026年度 / 基準日 2026-09-04

Q0098 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：標準

「FW・WAF・VPN・IDS/IPS等」のうち「IPsecモード」を、正答の根拠まで理解できているか確認する。候補「トンネルモード」を妥当と判断する根拠として最も適切な説明はどれか。

ア．主にエンドホスト間でIPペイロードを保護する用途に使われる。
イ．トンネルモードでは元のIPパケットを新しいIPパケット内へカプセル化して保護するため、拠点間VPNでよく使われる。
ウ．IPsecの標準的なモード名ではない。
エ．IPsecのモードではない。

答え・解説 正答：イ

ア：この説明は別候補「トランスポートモードだけ」に対応するため、正答候補「トンネルモード」の根拠にはならない。
イ：この説明は正答候補「トンネルモード」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「平文モード」に対応するため、正答候補「トンネルモード」の根拠にはならない。
エ：この説明は別候補「ブロードキャストモード」に対応するため、正答候補「トンネルモード」の根拠にはならない。

総合解説：正答候補「トンネルモード」を選ぶ根拠は次のとおりである。トンネルモードでは元のIPパケットを新しいIPパケット内へカプセル化して保護するため、拠点間VPNでよく使われる。

対象：2026年度 / 基準日 2026-09-04

Q0099 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：標準

「FW・WAF・VPN・IDS/IPS等」の「IPS誤検知」について、候補「検知ルール、しきい値、例外設定、ログを確認し、誤検知と業務影響を評価して調整する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．原因分析が困難になる。
イ．防御機能を失う。
ウ．IPSは遮断を伴うため、シグネチャやしきい値の調整と継続的なログ確認が重要である。
エ．根拠なく業務を止めるのは不適切である。

答え・解説 正答：ウ

ア：この説明は別候補「検知ログを全削除する。」に対応するため、正答候補「検知ルール、しきい値、例外設定、ログを確認し、誤検知と業務影響を評価して調整する。」の根拠にはならない。
イ：この説明は別候補「全ルールを無条件に無効化する。」に対応するため、正答候補「検知ルール、しきい値、例外設定、ログを確認し、誤検知と業務影響を評価して調整する。」の根拠にはならない。
ウ：この説明は正答候補「検知ルール、しきい値、例外設定、ログを確認し、誤検知と業務影響を評価して調整する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「正常通信を攻撃と決め付けて利用者を停止する。」に対応するため、正答候補「検知ルール、しきい値、例外設定、ログを確認し、誤検知と業務影響を評価して調整する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。IPSは遮断を伴うため、シグネチャやしきい値の調整と継続的なログ確認が重要である。

対象：2026年度 / 基準日 2026-09-04

Q0100 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：標準

「FW・WAF・VPN・IDS/IPS等」の「VPN認証」を復習している学習者が、候補「全利用者に同じ共通パスワードを配布する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．MFAを組み合わせることで、パスワード単独漏えい時の不正接続リスクを低減できる。
イ．検知・追跡能力が低下する。
ウ．中間者攻撃等のリスクが高まる。
エ．漏えい時の影響が拡大する。

答え・解説 正答：エ

ア：この説明は別候補「VPN接続時に多要素認証を要求する。」に対応するため、誤答候補「全利用者に同じ共通パスワードを配布する。」の問題点を直接説明していない。
イ：この説明は別候補「VPN装置のログを停止する。」に対応するため、誤答候補「全利用者に同じ共通パスワードを配布する。」の問題点を直接説明していない。
ウ：この説明は別候補「証明書警告を無条件に無視する。」に対応するため、誤答候補「全利用者に同じ共通パスワードを配布する。」の問題点を直接説明していない。
エ：この説明は誤答候補「全利用者に同じ共通パスワードを配布する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「全利用者に同じ共通パスワードを配布する。」については、何が誤りかを明確にした上で正しい概念へ戻す。漏えい時の影響が拡大する。

対象：2026年度 / 基準日 2026-09-04

Q0101 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：応用

「FW・WAF・VPN・IDS/IPS等」のうち「境界多層設計」を確認する誤答分析で、学習者が候補「全機器を同一セグメントへ置き通信を無制限にする。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．侵害時の横展開が容易になる。
イ．WAFの守備範囲を超える。
ウ．各装置・機能は対象レイヤや目的が異なるため、単一製品へ依存せず組み合わせるのが合理的である。
エ．防御と監視を弱める。

答え・解説 正答：ア

ア：この説明は誤答候補「全機器を同一セグメントへ置き通信を無制限にする。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「WAF一台だけで全ネットワーク層・内部権限・物理対策まで代替する。」に対応するため、誤答候補「全機器を同一セグメントへ置き通信を無制限にする。」の問題点を直接説明していない。
ウ：この説明は別候補「ファイアウォール、WAF、IDS/IPS、DMZや内部セグメント分離を役割分担させて多層防御する。」に対応するため、誤答候補「全機器を同一セグメントへ置き通信を無制限にする。」の問題点を直接説明していない。
エ：この説明は別候補「FWを導入する代わりに全ログを削除する。」に対応するため、誤答候補「全機器を同一セグメントへ置き通信を無制限にする。」の問題点を直接説明していない。

総合解説：誤答候補「全機器を同一セグメントへ置き通信を無制限にする。」について、誤りの内容を説明できることが重要である。侵害時の横展開が容易になる。

対象：2026年度 / 基準日 2026-09-04

Q0102 4-4 セキュリティ実装・運用 > FW・WAF・VPN・IDS/IPS等 ｜ 難易度：応用

「FW・WAF・VPN・IDS/IPS等」のうち「VPN分割トンネル」を、正答の根拠まで理解できているか確認する。候補「社内向け通信とインターネット向け通信が同時に端末を通るため、端末侵害時の橋渡しリスクを評価し、端末防御やアクセス制御を強化する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．橋渡し経路になり得る。
イ．分割トンネルには性能・帯域上の利点がある一方、端末が複数ネットワークの接点になる点を考慮する必要がある。
ウ．そのような保証はない。
エ．端末脆弱性対策は引き続き必要である。

答え・解説 正答：イ

ア：この説明は別候補「スプリットトンネルなら端末が侵害されても社内へ影響しない。」に対応するため、正答候補「社内向け通信とインターネット向け通信が同時に端末を通るため、端末侵害時の橋渡しリスクを評価し、端末防御やアクセス制御を強化する。」の根拠にはならない。
イ：この説明は正答候補「社内向け通信とインターネット向け通信が同時に端末を通るため、端末侵害時の橋渡しリスクを評価し、端末防御やアクセス制御を強化する。」の根拠に対応しており、今回の問いに合致する。

ウ：この説明は別候補「許可すると通信は全て自動でエンドツーエンド署名される。」に対応するため、正答候補「社内向け通信とインターネット向け通信が同時に端末を通るため、端末侵害時の橋渡しリスクを評価し、端末防御やアクセス制御を強化する。」の根拠にはならない。
エ：この説明は別候補「VPN利用時は端末パッチが不要になる。」に対応するため、正答候補「社内向け通信とインターネット向け通信が同時に端末を通るため、端末侵害時の橋渡しリスクを評価し、端末防御やアクセス制御を強化する。」の根拠にはならない。

総合解説：正答候補「社内向け通信とインターネット向け通信が同時に端末を通るため、端末侵害時の橋渡しリスクを評価し、端末防御やアクセス制御を強化する。」を選ぶ根拠は次のとおりである。分割トンネルには性能・帯域上の利点がある一方、端末が複数ネットワークの接点になる点を考慮する必要がある。

対象：2026年度 / 基準日 2026-09-04

Q0103 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：基礎

「ログ・監視・インシデント・フォレンジック」の「ログ目的」について、候補「異常検知、インシデント調査、責任追跡、監査などに利用できる証跡を残すため。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．ログは保存領域を使用する。
イ．ログの主目的ではない。
ウ．認証・アクセス・システム・アプリ等のログは検知と事後調査の重要な情報源になる。
エ．ログは主に記録・検知・調査に使う。

答え・解説 正答：ウ

ア：この説明は別候補「記憶容量を必ずゼロにするため。」に対応するため、正答候補「異常検知、インシデント調査、責任追跡、監査などに利用できる証跡を残すため。」の根拠にはならない。
イ：この説明は別候補「暗号鍵を自動生成するため。」に対応するため、正答候補「異常検知、インシデント調査、責任追跡、監査などに利用できる証跡を残すため。」の根拠にはならない。
ウ：この説明は正答候補「異常検知、インシデント調査、責任追跡、監査などに利用できる証跡を残すため。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全攻撃をログだけで自動防止するため。」に対応するため、正答候補「異常検知、インシデント調査、責任追跡、監査などに利用できる証跡を残すため。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。認証・アクセス・システム・アプリ等のログは検知と事後調査の重要な情報源になる。

対象：2026年度 / 基準日 2026-09-04

Q0104 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：基礎

「ログ・監視・インシデント・フォレンジック」の「SIEM」を復習している学習者が、候補「PKI」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．ストレージ冗長化である。
イ．SIEMは多様なログ・イベントを集中管理し、検索、相関分析、アラート等に利用する。
ウ．コンテンツ配信基盤である。
エ．公開鍵基盤である。

答え・解説 正答：エ

ア：この説明は別候補「RAID」に対応するため、誤答候補「PKI」の問題点を直接説明していない。
イ：この説明は別候補「SIEM」に対応するため、誤答候補「PKI」の問題点を直接説明していない。
ウ：この説明は別候補「CDN」に対応するため、誤答候補「PKI」の問題点を直接説明していない。
エ：この説明は誤答候補「PKI」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「PKI」については、何が誤りかを明確にした上で正しい概念へ戻す。公開鍵基盤である。

対象：2026年度 / 基準日 2026-09-04

Q0105 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：基礎

「ログ・監視・インシデント・フォレンジック」のうち「フォレンジック」を確認する誤答分析で、学習者が候補「暗号鍵を公開Webへ掲載すること。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．無関係で危険である。
イ．証拠を失う可能性がある。
ウ．調査情報を失う。
エ．フォレンジックでは、データの保全、収集、検査、分析、報告などを適切な手順で行う。

答え・解説 正答：ア

ア：この説明は誤答候補「暗号鍵を公開Webへ掲載すること。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「感染端末を調査前に初期化すること。」に対応するため、誤答候補「暗号鍵を公開Webへ掲載すること。」の問題点を直接説明していない。
ウ：この説明は別候補「全ログを削除して容量を確保すること。」に対応するため、誤答候補「暗号鍵を公開Webへ掲載すること。」の問題点を直接説明していない。
エ：この説明は別候補「デジタル機器やログなどから事実関係を調査し、証拠性を意識してデータを収集・分析する。」に対応するため、誤答候補「暗号鍵を公開Webへ掲載すること。」の問題点を直接説明していない。

総合解説：誤答候補「暗号鍵を公開Webへ掲載すること。」について、誤りの内容を説明できることが重要である。無関係で危険である。

対象：2026年度 / 基準日 2026-09-04

Q0106 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：基礎

「ログ・監視・インシデント・フォレンジック」のうち「時刻同期」を、正答の根拠まで理解できているか確認する。候補「異なる機器のイベント発生順序を正確に関連付けやすくするため。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．時刻同期と暗号化は別機能である。
イ．ログ時刻が大きくずれると、因果関係や攻撃の時系列を誤って判断するおそれがある。
ウ．脆弱性修正にはならない。
エ．今回問われている論点には直接対応しない内容である。

答え・解説 正答：イ

ア：この説明は別候補「時刻同期でログ内容が自動暗号化されるため。」に対応するため、正答候補「異なる機器のイベント発生順序を正確に関連付けやすくするため。」の根拠にはならない。
イ：この説明は正答候補「異なる機器のイベント発生順序を正確に関連付けやすくするため。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「時刻同期すると全脆弱性が消えるため。」に対応するため、正答候補「異なる機器のイベント発生順序を正確に関連付けやすくするため。」の根拠にはならない。
エ：この説明は別候補「時刻同期でバックアップが不要になるため。」に対応するため、正答候補「異なる機器のイベント発生順序を正確に関連付けやすくするため。」の根拠にはならない。

総合解説：正答候補「異なる機器のイベント発生順序を正確に関連付けやすくするため。」を選ぶ根拠は次のとおりである。ログ時刻が大きくずれると、因果関係や攻撃の時系列を誤って判断するおそれがある。

対象：2026年度 / 基準日 2026-09-04

Q0107 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：標準

「ログ・監視・インシデント・フォレンジック」の「インシデント初動」について、候補「組織の手順に従い端末を必要に応じて隔離し、関係者へ連絡し、ログ・メモリ等の証拠保全と影響確認を進める。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．原因・影響調査が困難になる。
イ．被害拡大のおそれがある。
ウ．封じ込めと調査の両立が重要で、証拠を失わないよう計画的に対応する。
エ．侵害を拡大させ得る。

答え・解説 正答：ウ

ア：この説明は別候補「何も記録せず端末を即廃棄する。」に対応するため、正答候補「組織の手順に従い端末を必要に応じて隔離し、関係者へ連絡し、ログ・メモリ等の証拠保全と影響確認を進める。」の根拠にはならない。
イ：この説明は別候補「不審通信を見つけても永久に放置する。」に対応するため、正答候補「組織の手順に従い端末を必要に応じて隔離し、関係者へ連絡し、ログ・メモリ等の証拠保全と影響確認を進める。」の根拠にはならない。
ウ：この説明は正答候補「組織の手順に従い端末を必要に応じて隔離し、関係者へ連絡し、ログ・メモリ等の証拠保全と影響確認を進める。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全社員へ管理者資格情報を送る。」に対応するため、正答候補「組織の手順に従い端末を必要に応じて隔離し、関係者へ連絡し、ログ・メモリ等の証拠保全と影響確認を進める。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。封じ込めと調査の両立が重要で、証拠を失わないよう計画的に対応する。

対象：2026年度 / 基準日 2026-09-04

Q0108 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：標準

「ログ・監視・インシデント・フォレンジック」の「IOC活用」を復習している学習者が、候補「MTBF」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．復旧時点目標である。
イ．侵害の痕跡を示す技術的指標をIOCとして共有・検索し、影響範囲確認に利用する。
ウ．Common Criteriaの保証レベルに関する用語である。
エ．平均故障間隔である。

答え・解説 正答：エ

ア：この説明は別候補「RPO」に対応するため、誤答候補「MTBF」の問題点を直接説明していない。
イ：この説明は別候補「IOC（Indicator of Compromise）」に対応するため、誤答候補「MTBF」の問題点を直接説明していない。
ウ：この説明は別候補「EAL」に対応するため、誤答候補「MTBF」の問題点を直接説明していない。
エ：この説明は誤答候補「MTBF」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「MTBF」については、何が誤りかを明確にした上で正しい概念へ戻す。平均故障間隔である。

対象：2026年度 / 基準日 2026-09-04

Q0109 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：標準

「ログ・監視・インシデント・フォレンジック」のうち「ログ保全」を確認する誤答分析で、学習者が候補「攻撃者が自由に編集できる同一端末へだけ保存する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．証拠として必要な信頼性・完全性の確保が不十分である。
イ．調査できなくなる。
ウ．侵害端末上だけにログを置くと攻撃者に消去される可能性があるため、分離・保護した保管が有効である。
エ．機密情報漏えいにつながる。

答え・解説 正答：ア

ア：この説明は誤答候補「攻撃者が自由に編集できる同一端末へだけ保存する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「ログを毎分全削除する。」に対応するため、誤答候補「攻撃者が自由に編集できる同一端末へだけ保存する。」の問題点を直接説明していない。
ウ：この説明は別候補「ログ送信元から分離した集中ログ基盤へ転送し、アクセス制御や改ざん検知を行う。」に対応するため、誤答候補「攻撃者が自由に編集できる同一端末へだけ保存する。」の問題点を直接説明していない。
エ：この説明は別候補「全ログを匿名掲示板へ公開する。」に対応するため、誤答候補「攻撃者が自由に編集できる同一端末へだけ保存する。」の問題点を直接説明していない。

総合解説：誤答候補「攻撃者が自由に編集できる同一端末へだけ保存する。」について、誤りの内容を説明できることが重要である。証拠として必要な信頼性・完全性の確保が不十分である。

対象：2026年度 / 基準日 2026-09-04

Q0110 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：標準

「ログ・監視・インシデント・フォレンジック」のうち「チェーンオブカストディ」を、正答の根拠まで理解できているか確認する。候補「証拠の取扱経路と完全性を説明できるようにするため。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．問われている関係や方向を逆に捉えた内容である。
イ．チェーンオブカストディは証拠の管理履歴を明確にし、改ざん・取り違え等の疑義を減らす。
ウ．今回問われている対象の目的には該当しない。
エ．今回問われている論点には直接対応しない内容である。

答え・解説 正答：イ

ア：この説明は別候補「証拠を誰でも自由に書換えられるようにするため。」に対応するため、正答候補「証拠の取扱経路と完全性を説明できるようにするため。」の根拠にはならない。
イ：この説明は正答候補「証拠の取扱経路と完全性を説明できるようにするため。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「ディスク容量を増やすため。」に対応するため、正答候補「証拠の取扱経路と完全性を説明できるようにするため。」の根拠にはならない。
エ：この説明は別候補「ネットワーク帯域を確保するため。」に対応するため、正答候補「証拠の取扱経路と完全性を説明できるようにするため。」の根拠にはならない。

総合解説：正答候補「証拠の取扱経路と完全性を説明できるようにするため。」を選ぶ根拠は次のとおりである。チェーンオブカストディは証拠の管理履歴を明確にし、改ざん・取り違え等の疑義を減らす。

対象：2026年度 / 基準日 2026-09-04

Q0111 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：標準

「ログ・監視・インシデント・フォレンジック」の「メモリ保全」について、候補「揮発性情報は電源断で失われ得るため、必要なら手順に従ってメモリ等を取得してから電源操作を判断する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．通常はその情報・状態が保持されず、失われる点に注意が必要である。
イ．有用な情報源になり得る。
ウ．ライブフォレンジックでは揮発性データの価値と取得による変更影響を考慮して対応する。
エ．取得自体が状態を変えるため記録が必要である。

答え・解説 正答：ウ

ア：この説明は別候補「電源断してもRAM内容は永久に残る。」に対応するため、正答候補「揮発性情報は電源断で失われ得るため、必要なら手順に従ってメモリ等を取得してから電源操作を判断する。」の根拠にはならない。
イ：この説明は別候補「メモリ情報は攻撃調査に一切使えない。」に対応するため、正答候補「揮発性情報は電源断で失われ得るため、必要なら手順に従ってメモリ等を取得してから電源操作を判断する。」の根拠にはならない。
ウ：この説明は正答候補「揮発性情報は電源断で失われ得るため、必要なら手順に従ってメモリ等を取得してから電源操作を判断する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「取得ツールは証拠へ全く影響を与えない。」に対応するため、正答候補「揮発性情報は電源断で失われ得るため、必要なら手順に従ってメモリ等を取得してから電源操作を判断する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ライブフォレンジックでは揮発性データの価値と取得による変更影響を考慮して対応する。

対象：2026年度 / 基準日 2026-09-04

Q0112 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：標準

「ログ・監視・インシデント・フォレンジック」の「検知チューニング」を復習している学習者が、候補「全アラートを無条件に無効化する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．検知品質は誤検知と見逃しのバランスを見ながら運用改善する必要がある。
イ．業務影響が大きい。
ウ．検知能力を失う。
エ．真の攻撃も見えなくなる。

答え・解説 正答：エ

ア：この説明は別候補「アラートの根拠・頻度・業務影響を分析し、ルールやしきい値、例外、優先度を継続的に調整する。」に対応するため、誤答候補「全アラートを無条件に無効化する。」の問題点を直接説明していない。
イ：この説明は別候補「誤検知を全て本物の攻撃として停止処置する。」に対応するため、誤答候補「全アラートを無条件に無効化する。」の問題点を直接説明していない。
ウ：この説明は別候補「ログ収集を停止する。」に対応するため、誤答候補「全アラートを無条件に無効化する。」の問題点を直接説明していない。
エ：この説明は誤答候補「全アラートを無条件に無効化する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「全アラートを無条件に無効化する。」については、何が誤りかを明確にした上で正しい概念へ戻す。真の攻撃も見えなくなる。

対象：2026年度 / 基準日 2026-09-04

Q0113 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：応用

「ログ・監視・インシデント・フォレンジック」のうち「IRライフサイクル」を確認する誤答分析で、学習者が候補「インシデント対応はIT部門だけの秘密作業とし経営へ報告しない。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．重大事案では組織的意思決定が必要である。
イ．再発防止につながらない。
ウ．現行のNIST SP 800-61 Rev.3はインシデント対応をサイバーセキュリティリスク管理へ統合する考え方を示している。
エ．優先度や影響に応じた対応が必要である。

答え・解説 正答：ア

ア：この説明は誤答候補「インシデント対応はIT部門だけの秘密作業とし経営へ報告しない。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「復旧したら原因や教訓を記録せず終了する。」に対応するため、誤答候補「インシデント対応はIT部門だけの秘密作業とし経営へ報告しない。」の問題点を直接説明していない。
ウ：この説明は別候補「準備、検知・分析、対応・復旧だけでなく、得られた教訓を管理策・訓練・リスク評価の改善へ反映する。」に対応するため、誤答候補「インシデント対応はIT部門だけの秘密作業とし経営へ報告しない。」の問題点を直接説明していない。
エ：この説明は別候補「全ての事案で同一対応を機械的に適用し影響度を評価しない。」に対応するため、誤答候補「インシデント対応はIT部門だけの秘密作業とし経営へ報告しない。」の問題点を直接説明していない。

総合解説：誤答候補「インシデント対応はIT部門だけの秘密作業とし経営へ報告しない。」について、誤りの内容を説明できることが重要である。重大事案では組織的意思決定が必要である。

対象：2026年度 / 基準日 2026-09-04

Q0114 4-4 セキュリティ実装・運用 > ログ・監視・インシデント・フォレンジック ｜ 難易度：応用

「ログ・監視・インシデント・フォレンジック」のうち「フォレンジック整合性」を、正答の根拠まで理解できているか確認する。候補「書込みを抑制してイメージを取得し、取得時・解析前後にハッシュ値を記録・比較し、取扱履歴も残す。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．証拠状態を変化させる。
イ．原本保護、ハッシュによる完全性確認、管理履歴の記録を組み合わせることで証拠性を高められる。

ウ．完全性確認が弱い。
エ．取扱経路を説明できない。

答え・解説 正答：イ

ア：この説明は別候補「原本へ直接何度も書込みながら解析する。」に対応するため、正答候補「書込みを抑制してイメージを取得し、取得時・解析前後にハッシュ値を記録・比較し、取扱履歴も残す。」の根拠にはならない。
イ：この説明は正答候補「書込みを抑制してイメージを取得し、取得時・解析前後にハッシュ値を記録・比較し、取扱履歴も残す。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「ハッシュ値を記録せずファイル名だけで同一性を判断する。」に対応するため、正答候補「書込みを抑制してイメージを取得し、取得時・解析前後にハッシュ値を記録・比較し、取扱履歴も残す。」の根拠にはならない。
エ：この説明は別候補「取得者・時刻を記録しない。」に対応するため、正答候補「書込みを抑制してイメージを取得し、取得時・解析前後にハッシュ値を記録・比較し、取扱履歴も残す。」の根拠にはならない。

総合解説：正答候補「書込みを抑制してイメージを取得し、取得時・解析前後にハッシュ値を記録・比較し、取扱履歴も残す。」を選ぶ根拠は次のとおりである。原本保護、ハッシュによる完全性確認、管理履歴の記録を組み合わせることで証拠性を高められる。

対象：2026年度 / 基準日 2026-09-04

Q0115 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：基礎

「セキュア開発・クラウド・サプライチェーン」の「セキュアSDLC」について、候補「要件定義から設計、実装、テスト、リリース、保守までSDLC全体へセキュリティ活動を組み込む。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．早期対策ができない。
イ．多様な脆弱性に対応できない。
ウ．公開直前だけでなく開発ライフサイクル全体でリスクを減らすことが重要である。
エ．最小権限に反する。

答え・解説 正答：ウ

ア：この説明は別候補「本番公開後に事故が起きた時だけセキュリティを考える。」に対応するため、正答候補「要件定義から設計、実装、テスト、リリース、保守までSDLC全体へセキュリティ活動を組み込む。」の根拠にはならない。
イ：この説明は別候補「入力検証だけを唯一の対策とする。」に対応するため、正答候補「要件定義から設計、実装、テスト、リリース、保守までSDLC全体へセキュリティ活動を組み込む。」の根拠にはならない。
ウ：この説明は正答候補「要件定義から設計、実装、テスト、リリース、保守までSDLC全体へセキュリティ活動を組み込む。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「全開発者へ本番管理者権限を恒久付与する。」に対応するため、正答候補「要件定義から設計、実装、テスト、リリース、保守までSDLC全体へセキュリティ活動を組み込む。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。公開直前だけでなく開発ライフサイクル全体でリスクを減らすことが重要である。

対象：2026年度 / 基準日 2026-09-04

Q0116 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：基礎

「セキュア開発・クラウド・サプライチェーン」の「SAST/DAST」を復習している学習者が、候補「バックアップ」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．稼働中のアプリを動的に検査する。
イ．SASTはコード等を静的に解析する。DASTは稼働中アプリへ外部から働きかける動的テストである。
ウ．アドレス変換である。
エ．データ保護手法である。

答え・解説 正答：エ

ア：この説明は別候補「DAST」に対応するため、誤答候補「バックアップ」の問題点を直接説明していない。

イ：この説明は別候補「SAST（静的アプリケーションセキュリティテスト）」に対応するため、誤答候補「バックアップ」の問題点を直接説明していない。
ウ：この説明は別候補「NAT」に対応するため、誤答候補「バックアップ」の問題点を直接説明していない。

エ：この説明は誤答候補「バックアップ」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「バックアップ」については、何が誤りかを明確にした上で正しい概念へ戻す。データ保護手法である。

対象：2026年度 / 基準日 2026-09-04

Q0117 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：基礎

「セキュア開発・クラウド・サプライチェーン」のうち「SBOM」を確認する誤答分析で、学習者が候補「CRL」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．証明書失効リストである。
イ．事業影響度分析である。
ウ．復旧時点目標である。
エ．SBOMはソフトウェアを構成するコンポーネントや依存関係の可視化に利用される。

答え・解説 正答：ア

ア：この説明は誤答候補「CRL」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「BIA」に対応するため、誤答候補「CRL」の問題点を直接説明していない。
ウ：この説明は別候補「RPO」に対応するため、誤答候補「CRL」の問題点を直接説明していない。
エ：この説明は別候補「SBOM（Software Bill of Materials）」に対応するため、誤答候補「CRL」の問題点を直接説明していない。

総合解説：誤答候補「CRL」について、誤りの内容を説明できることが重要である。証明書失効リストである。

対象：2026年度 / 基準日 2026-09-04

Q0118 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：基礎

「セキュア開発・クラウド・サプライチェーン」のうち「共有責任」を、正答の根拠まで理解できているか確認する。候補「クラウド事業者と利用者でセキュリティ責任を分担し、サービス形態や契約に応じて責任範囲が異なる。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．利用者側責任が残る。
イ．クラウド利用でも利用者側のID管理、設定、データ保護などの責任が残る場合がある。
ウ．サービス形態に依存する。
エ．条件によって結果が異なるため、一律にはそのように判断できない。

答え・解説 正答：イ

ア：この説明は別候補「クラウド利用者には常に一切の責任がない。」に対応するため、正答候補「クラウド事業者と利用者でセキュリティ責任を分担し、サービス形態や契約に応じて責任範囲が異なる。」の根拠にはならない。
イ：この説明は正答候補「クラウド事業者と利用者でセキュリティ責任を分担し、サービス形態や契約に応じて責任範囲が異なる。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「事業者は常に利用者アプリの認可設定まで全て代行する。」に対応するため、正答候補「クラウド事業者と利用者でセキュリティ責任を分担し、サービス形態や契約に応じて責任範囲が異なる。」の根拠にはならない。
エ：この説明は別候補「責任分界は契約やサービス形態と無関係で一定である。」に対応するため、正答候補「クラウド事業者と利用者でセキュリティ責任を分担し、サービス形態や契約に応じて責任範囲が異なる。」の根拠にはならない。

総合解説：正答候補「クラウド事業者と利用者でセキュリティ責任を分担し、サービス形態や契約に応じて責任範囲が異なる。」を選ぶ根拠は次のとおりである。クラウド利用でも利用者側のID管理、設定、データ保護などの責任が残る場合がある。

対象：2026年度 / 基準日 2026-09-04

Q0119 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：標準

「セキュア開発・クラウド・サプライチェーン」の「脅威モデリング」について、候補「脅威モデリング」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．性能・可用性技術である。
イ．バックアップ方式である。
ウ．実装前に攻撃経路や資産を分析すると、設計上の弱点を早期に発見しやすい。
エ．DB設計である。

答え・解説 正答：ウ

ア：この説明は別候補「負荷分散」に対応するため、正答候補「脅威モデリング」の根拠にはならない。
イ：この説明は別候補「差分バックアップ」に対応するため、正答候補「脅威モデリング」の根拠にはならない。
ウ：この説明は正答候補「脅威モデリング」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「データ正規化」に対応するため、正答候補「脅威モデリング」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。実装前に攻撃経路や資産を分析すると、設計上の弱点を早期に発見しやすい。

対象：2026年度 / 基準日 2026-09-04

Q0120 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：標準

「セキュア開発・クラウド・サプライチェーン」の「秘密情報管理」を復習している学習者が、候補「ログにも秘密鍵全文を出力する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．漏えいリスクが高い。
イ．リポジトリへ秘密情報を残すと漏えい・履歴残存の危険があるため、専用管理と最小権限が重要である。
ウ．ローテーションが必要である。
エ．二次漏えいにつながる。

答え・解説 正答：エ

ア：この説明は別候補「秘密鍵をREADMEに記載して全員へ共有する。」に対応するため、誤答候補「ログにも秘密鍵全文を出力する。」の問題点を直接説明していない。
イ：この説明は別候補「秘密情報管理サービス等を利用し、コードから資格情報を分離し、必要最小限の権限とローテーションを適用する。」に対応するため、誤答候補「ログにも秘密鍵全文を出力する。」の問題点を直接説明していない。
ウ：この説明は別候補「一度公開した鍵を永久に使う。」に対応するため、誤答候補「ログにも秘密鍵全文を出力する。」の問題点を直接説明していない。
エ：この説明は誤答候補「ログにも秘密鍵全文を出力する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「ログにも秘密鍵全文を出力する。」については、何が誤りかを明確にした上で正しい概念へ戻す。二次漏えいにつながる。

対象：2026年度 / 基準日 2026-09-04

Q0121 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：標準

「セキュア開発・クラウド・サプライチェーン」のうち「依存関係管理」を確認する誤答分析で、学習者が候補「OSSなら脆弱性情報を無視してよい。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．OSSでも影響を受ける。
イ．実体の脆弱性は残る。
ウ．依存コンポーネントの可視化と脆弱性情報の継続監視はサプライチェーン管理の重要要素である。
エ．リスク評価に基づく対応が必要である。

答え・解説 正答：ア

ア：この説明は誤答候補「OSSなら脆弱性情報を無視してよい。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「脆弱性があってもSBOMから該当部品を消すだけで修正完了とする。」に対応するため、誤答候補「OSSなら脆弱性情報を無視してよい。」の問題点を直接説明していない。
ウ：この説明は別候補「自製品での利用有無・バージョン・到達可能性を確認し、修正版への更新や緩和策を優先度に応じて実施する。」に対応するため、誤答候補「OSSなら脆弱性情報を無視してよい。」の問題点を直接説明していない。
エ：この説明は別候補「影響確認せず全システム停止を永久継続する。」に対応するため、誤答候補「OSSなら脆弱性情報を無視してよい。」の問題点を直接説明していない。

総合解説：誤答候補「OSSなら脆弱性情報を無視してよい。」について、誤りの内容を説明できることが重要である。OSSでも影響を受ける。

対象：2026年度 / 基準日 2026-09-04

Q0122 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：標準

「セキュア開発・クラウド・サプライチェーン」のうち「クラウド設定」を、正答の根拠まで理解できているか確認する。候補「公開設定の禁止・検知ポリシー、IaCレビュー、CSPM等の継続監視、最小権限を組み合わせる。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．漏えいリスクが高い。
イ．クラウドでは設定ミスが大きなリスクになるため、予防と継続的検知を自動化することが有効である。
ウ．原因追跡が難しい。
エ．最小権限に反する。

答え・解説 正答：イ

ア：この説明は別候補「全ストレージを初期状態で公開する。」に対応するため、正答候補「公開設定の禁止・検知ポリシー、IaCレビュー、CSPM等の継続監視、最小権限を組み合わせる。」の根拠にはならない。
イ：この説明は正答候補「公開設定の禁止・検知ポリシー、IaCレビュー、CSPM等の継続監視、最小権限を組み合わせる。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「設定変更ログを記録しない。」に対応するため、正答候補「公開設定の禁止・検知ポリシー、IaCレビュー、CSPM等の継続監視、最小権限を組み合わせる。」の根拠にはならない。
エ：この説明は別候補「全利用者へ所有者権限を付与する。」に対応するため、正答候補「公開設定の禁止・検知ポリシー、IaCレビュー、CSPM等の継続監視、最小権限を組み合わせる。」の根拠にはならない。

総合解説：正答候補「公開設定の禁止・検知ポリシー、IaCレビュー、CSPM等の継続監視、最小権限を組み合わせる。」を選ぶ根拠は次のとおりである。クラウドでは設定ミスが大きなリスクになるため、予防と継続的検知を自動化することが有効である。

対象：2026年度 / 基準日 2026-09-04

Q0123 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：標準

「セキュア開発・クラウド・サプライチェーン」の「サプライヤ評価」について、候補「委託先の開発・脆弱性対応・アクセス管理・再委託・インシデント報告等を契約前後に評価し、継続監視する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．重要リスクを無視している。
イ．依存関係リスクが残る。
ウ．サプライチェーンリスクは調達時だけでなく、契約・運用・更新・終了まで管理する必要がある。
エ．継続監視が必要である。

答え・解説 正答：ウ

ア：この説明は別候補「価格だけで選定しセキュリティ条件を設けない。」に対応するため、正答候補「委託先の開発・脆弱性対応・アクセス管理・再委託・インシデント報告等を契約前後に評価し、継続監視する。」の根拠にはならない。
イ：この説明は別候補「再委託先は見えないので一切考慮しない。」に対応するため、正答候補「委託先の開発・脆弱性対応・アクセス管理・再委託・インシデント報告等を契約前後に評価し、継続監視する。」の根拠にはならない。
ウ：この説明は正答候補「委託先の開発・脆弱性対応・アクセス管理・再委託・インシデント報告等を契約前後に評価し、継続監視する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「契約締結後は委託先の状況変化を確認しない。」に対応するため、正答候補「委託先の開発・脆弱性対応・アクセス管理・再委託・インシデント報告等を契約前後に評価し、継続監視する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。サプライチェーンリスクは調達時だけでなく、契約・運用・更新・終了まで管理する必要がある。

対象：2026年度 / 基準日 2026-09-04

Q0124 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：標準

「セキュア開発・クラウド・サプライチェーン」の「ISMAP」を復習している学習者が、候補「JISECだけ」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．ISMAPは政府情報システムのためのクラウドサービスのセキュリティ評価制度である。
イ．DNSの真正性保護技術である。
ウ．脆弱性深刻度指標である。
エ．主にIT製品のISO/IEC 15408評価認証制度で、クラウドサービス登録制度とは異なる。

答え・解説 正答：エ

ア：この説明は別候補「ISMAP」に対応するため、誤答候補「JISECだけ」の問題点を直接説明していない。
イ：この説明は別候補「DNSSEC」に対応するため、誤答候補「JISECだけ」の問題点を直接説明していない。

ウ：この説明は別候補「CVSS」に対応するため、誤答候補「JISECだけ」の問題点を直接説明していない。
エ：この説明は誤答候補「JISECだけ」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「JISECだけ」については、何が誤りかを明確にした上で正しい概念へ戻す。主にIT製品のISO/IEC 15408評価認証制度で、クラウドサービス登録制度とは異なる。

対象：2026年度 / 基準日 2026-09-04

Q0125 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：応用

「セキュア開発・クラウド・サプライチェーン」のうち「CI/CD保護」を確認する誤答分析で、学習者が候補「ビルドログを削除し外部依存物を無検証で取得する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．改ざん検知が困難である。
イ．侵害と追跡不能のリスクが高い。
ウ．開発・ビルド・配布パイプライン自体を重要資産として保護し、成果物の完全性と出所を検証する必要がある。
エ．署名の信頼性を失う。

答え・解説 正答：ア

ア：この説明は誤答候補「ビルドログを削除し外部依存物を無検証で取得する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「CI/CDアカウントを全員で共有しMFAを無効化する。」に対応するため、誤答候補「ビルドログを削除し外部依存物を無検証で取得する。」の問題点を直接説明していない。
ウ：この説明は別候補「ビルド環境の分離、最小権限、MFA、依存物検証、署名・出所確認、監査ログ、秘密情報管理を行う。」に対応するため、誤答候補「ビルドログを削除し外部依存物を無検証で取得する。」の問題点を直接説明していない。
エ：この説明は別候補「署名鍵を公開リポジトリへ保存する。」に対応するため、誤答候補「ビルドログを削除し外部依存物を無検証で取得する。」の問題点を直接説明していない。

総合解説：誤答候補「ビルドログを削除し外部依存物を無検証で取得する。」について、誤りの内容を説明できることが重要である。改ざん検知が困難である。

対象：2026年度 / 基準日 2026-09-04

Q0126 4-4 セキュリティ実装・運用 > セキュア開発・クラウド・サプライチェーン ｜ 難易度：応用

「セキュア開発・クラウド・サプライチェーン」のうち「クラウド責任総合」を、正答の根拠まで理解できているか確認する。候補「事業者の管理策・認証・契約を確認するだけでなく、自社側の利用者権限、データ分類、設定、退職者アカウント、ログ監視も管理する。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．利用者側の認証・権限管理が必要である。
イ．クラウドの安全性は事業者側だけで完結せず、利用者側の設定・ID・データ利用も共有責任として重要である。
ウ．認証は個別利用設定の適切性を保証しない。
エ．ライフサイクル全体の管理が必要である。

答え・解説 正答：イ

ア：この説明は別候補「SaaSなら自社のID管理は不要である。」に対応するため、正答候補「事業者の管理策・認証・契約を確認するだけでなく、自社側の利用者権限、データ分類、設定、退職者アカウント、ログ監視も管理する。」の根拠にはならない。
イ：この説明は正答候補「事業者の管理策・認証・契約を確認するだけでなく、自社側の利用者権限、データ分類、設定、退職者アカウント、ログ監視も管理する。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「認証済み事業者なら全データを無条件に公開設定してよい。」に対応するため、正答候補「事業者の管理策・認証・契約を確認するだけでなく、自社側の利用者権限、データ分類、設定、退職者アカウント、ログ監視も管理する。」の根拠にはならない。
エ：この説明は別候補「契約終了後のデータ消去条件は確認不要である。」に対応するため、正答候補「事業者の管理策・認証・契約を確認するだけでなく、自社側の利用者権限、データ分類、設定、退職者アカウント、ログ監視も管理する。」の根拠にはならない。

総合解説：正答候補「事業者の管理策・認証・契約を確認するだけでなく、自社側の利用者権限、データ分類、設定、退職者アカウント、ログ監視も管理する。」を選ぶ根拠は次のとおりである。クラウドの安全性は事業者側だけで完結せず、利用者側の設定・ID・データ利用も共有責任として重要である。

対象：2026年度 / 基準日 2026-09-04

Q0127 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：基礎

「個人情報保護・セキュリティ関連法規」の「個人情報」について、候補「生存する個人に関する情報で、氏名等により特定の個人を識別できるものや、個人識別符号が含まれるもの。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．個人に関する情報でなければ個人情報には当たらない。
イ．個人識別性を持たない統計情報は通常個人情報とは扱われない。
ウ．個人情報は、生存する個人に関する情報のうち、特定個人を識別できるもの等を対象とする。
エ．個人情報の定義は生存する個人に関する情報を対象とする。

答え・解説 正答：ウ

ア：この説明は別候補「法人の売上高だけを記録した情報は常に個人情報である。」に対応するため、正答候補「生存する個人に関する情報で、氏名等により特定の個人を識別できるものや、個人識別符号が含まれるもの。」の根拠にはならない。
イ：この説明は別候補「完全に匿名化され、特定個人を識別できない統計値は常に個人情報である。」に対応するため、正答候補「生存する個人に関する情報で、氏名等により特定の個人を識別できるものや、個人識別符号が含まれるもの。」の根拠にはならない。
ウ：この説明は正答候補「生存する個人に関する情報で、氏名等により特定の個人を識別できるものや、個人識別符号が含まれるもの。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「死者だけに関する情報は法律上必ず個人情報に該当する。」に対応するため、正答候補「生存する個人に関する情報で、氏名等により特定の個人を識別できるものや、個人識別符号が含まれるもの。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。個人情報は、生存する個人に関する情報のうち、特定個人を識別できるもの等を対象とする。

対象：2026年度 / 基準日 2026-09-04

Q0128 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：基礎

「個人情報保護・セキュリティ関連法規」の「不正アクセス基本」を復習している学習者が、候補「パスワードを使う行為は全て同法の対象外である。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．無断の他人識別符号利用は不正アクセス行為に該当し得る。
イ．不正アクセス禁止法は、アクセス制御機能に対して他人の識別符号を不正に入力する行為等を禁止している。
ウ．情報通信ネットワーク上の不正アクセス等を対象とする。
エ．むしろ識別符号の不正利用が代表的対象である。

答え・解説 正答：エ

ア：この説明は別候補「本人の許可がなくても技術的にログインできれば常に合法である。」に対応するため、誤答候補「パスワードを使う行為は全て同法の対象外である。」の問題点を直接説明していない。
イ：この説明は別候補「不正アクセス禁止法上の不正アクセス行為に該当し得る。」に対応するため、誤答候補「パスワードを使う行為は全て同法の対象外である。」の問題点を直接説明していない。
ウ：この説明は別候補「不正アクセス禁止法は紙文書の誤字だけを規制する法律である。」に対応するため、誤答候補「パスワードを使う行為は全て同法の対象外である。」の問題点を直接説明していない。
エ：この説明は誤答候補「パスワードを使う行為は全て同法の対象外である。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「パスワードを使う行為は全て同法の対象外である。」については、何が誤りかを明確にした上で正しい概念へ戻す。むしろ識別符号の不正利用が代表的対象である。

対象：2026年度 / 基準日 2026-09-04

Q0129 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：標準

「個人情報保護・セキュリティ関連法規」のうち「利用目的」を確認する誤答分析で、学習者が候補「利用目的は事業者内部でも誰にも分からない状態にする。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．適切な管理・説明ができない。
イ．利用目的はできる限り特定する必要がある。
ウ．目的外利用には法令上の制約がある。
エ．個人情報保護では、利用目的の特定と、その範囲を踏まえた適切な取扱いが基本となる。

答え・解説 正答：ア

ア：この説明は誤答候補「利用目的は事業者内部でも誰にも分からない状態にする。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「将来何に使うか不明でも『何にでも利用する』とだけ定めれば常に十分である。」に対応するため、誤答候補「利用目的は事業者内部でも誰にも分からない状態にする。」の問題点を直接説明していない。
ウ：この説明は別候補「取得後は利用目的と無関係な用途へ自由に転用できる。」に対応するため、誤答候補「利用目的は事業者内部でも誰にも分からない状態にする。」の問題点を直接説明していない。
エ：この説明は別候補「利用目的をできる限り特定し、その目的の達成に必要な範囲で取り扱う。」に対応するため、誤答候補「利用目的は事業者内部でも誰にも分からない状態にする。」の問題点を直接説明していない。

総合解説：誤答候補「利用目的は事業者内部でも誰にも分からない状態にする。」について、誤りの内容を説明できることが重要である。適切な管理・説明ができない。

対象：2026年度 / 基準日 2026-09-04

Q0130 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：標準

「個人情報保護・セキュリティ関連法規」のうち「要配慮個人情報」を、正答の根拠まで理解できているか確認する。候補「病歴等の要配慮個人情報の取得は、法令上の例外を除き原則として本人同意が必要で、オプトアウトによる第三者提供も認められていない。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．原則同意が必要である。
イ．要配慮個人情報は不当な差別等につながるおそれから、一般の個人情報より慎重な取扱いが求められる。
ウ．病歴は代表例である。
エ．報告対象事態に該当し得る。

答え・解説 正答：イ

ア：この説明は別候補「要配慮個人情報は本人同意なしに常に自由取得できる。」に対応するため、正答候補「病歴等の要配慮個人情報の取得は、法令上の例外を除き原則として本人同意が必要で、オプトアウトによる第三者提供も認められていない。」の根拠にはならない。
イ：この説明は正答候補「病歴等の要配慮個人情報の取得は、法令上の例外を除き原則として本人同意が必要で、オプトアウトによる第三者提供も認められていない。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「病歴は要配慮個人情報には絶対含まれない。」に対応するため、正答候補「病歴等の要配慮個人情報の取得は、法令上の例外を除き原則として本人同意が必要で、オプトアウトによる第三者提供も認められていない。」の根拠にはならない。
エ：この説明は別候補「要配慮個人情報は漏えいしても報告対象となることはない。」に対応するため、正答候補「病歴等の要配慮個人情報の取得は、法令上の例外を除き原則として本人同意が必要で、オプトアウトによる第三者提供も認められていない。」の根拠にはならない。

総合解説：正答候補「病歴等の要配慮個人情報の取得は、法令上の例外を除き原則として本人同意が必要で、オプトアウトによる第三者提供も認められていない。」を選ぶ根拠は次のとおりである。要配慮個人情報は不当な差別等につながるおそれから、一般の個人情報より慎重な取扱いが求められる。

対象：2026年度 / 基準日 2026-09-04

Q0131 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：標準

「個人情報保護・セキュリティ関連法規」の「漏えい報告」について、候補「要配慮個人情報を含む漏えい等や、財産的被害のおそれ、不正目的のおそれ、1,000人を超える漏えい等。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．報告義務の要件と刑事罰を混同している。
イ．むしろ報告対象の代表例である。
ウ．個人の権利利益を害するおそれが大きい一定の事態では、委員会への報告と本人通知が義務となる。

エ．報告対象事態に含まれる。

答え・解説 正答：ウ

ア：この説明は別候補「どのような漏えいでも人数・内容・暗号化状況等に関係なく同一条件で必ず刑事罰になる。」に対応するため、正答候補「要配慮個人情報を含む漏えい等や、財産的被害のおそれ、不正目的のおそれ、1,000人を超える漏えい等。」の根拠にはならない。
イ：この説明は別候補「要配慮個人情報が含まれるほど報告義務から必ず除外される。」に対応するため、正答候補「要配慮個人情報を含む漏えい等や、財産的被害のおそれ、不正目的のおそれ、1,000人を超える漏えい等。」の根拠にはならない。
ウ：この説明は正答候補「要配慮個人情報を含む漏えい等や、財産的被害のおそれ、不正目的のおそれ、1,000人を超える漏えい等。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「不正目的の漏えいは本人の権利利益に影響しないので対象外である。」に対応するため、正答候補「要配慮個人情報を含む漏えい等や、財産的被害のおそれ、不正目的のおそれ、1,000人を超える漏えい等。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。個人の権利利益を害するおそれが大きい一定の事態では、委員会への報告と本人通知が義務となる。

対象：2026年度 / 基準日 2026-09-04

Q0132 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：標準

「個人情報保護・セキュリティ関連法規」の「助長行為」を復習している学習者が、候補「不正アクセス禁止法はアクセス管理者だけを処罰する法律である。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．助長行為も規制対象となり得る。
イ．同法は不正アクセス行為そのものだけでなく、一定の識別符号提供など助長行為も規制している。
ウ．典型的な識別符号である。
エ．不正アクセス行為者等を規制する。

答え・解説 正答：エ

ア：この説明は別候補「自分がログインしなければ、他人の識別符号提供は常に自由である。」に対応するため、誤答候補「不正アクセス禁止法はアクセス管理者だけを処罰する法律である。」の問題点を直接説明していない。
イ：この説明は別候補「不正アクセス行為を助長する行為として不正アクセス禁止法の規制対象となり得る。」に対応するため、誤答候補「不正アクセス禁止法はアクセス管理者だけを処罰する法律である。」の問題点を直接説明していない。
ウ：この説明は別候補「ID・パスワードは識別符号に含まれない。」に対応するため、誤答候補「不正アクセス禁止法はアクセス管理者だけを処罰する法律である。」の問題点を直接説明していない。
エ：この説明は誤答候補「不正アクセス禁止法はアクセス管理者だけを処罰する法律である。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「不正アクセス禁止法はアクセス管理者だけを処罰する法律である。」については、何が誤りかを明確にした上で正しい概念へ戻す。不正アクセス行為者等を規制する。

対象：2026年度 / 基準日 2026-09-04

Q0133 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：応用

「個人情報保護・セキュリティ関連法規」のうち「漏えい事案対応」を確認する誤答分析で、学習者が候補「漏えいの痕跡を消すためログを削除し、誰にも報告しない。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．調査を妨げ、法令上必要な対応も行えない。
イ．報告対象事態では本人通知が求められる。
ウ．要配慮個人情報を含み不正目的のおそれもあるため、技術的封じ込めだけでなく法令上の報告・通知を含めて対応する必要がある。
エ．原因が不正アクセスでも個人データ漏えいへの対応が必要である。

答え・解説 正答：ア

ア：この説明は誤答候補「漏えいの痕跡を消すためログを削除し、誰にも報告しない。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「要配慮個人情報なので本人通知は禁止されている。」に対応するため、誤答候補「漏えいの痕跡を消すためログを削除し、誰にも報告しない。」の問題点を直接説明していない。
ウ：この説明は別候補「被害拡大防止、事実関係・原因調査、影響範囲特定、再発防止を進め、報告対象事態として委員会への報告と本人通知等を行う。」に対応するため、誤答候補「漏えいの痕跡を消すためログを削除し、誰にも報告しない。」の問題点を直接説明していない。
エ：この説明は別候補「不正アクセスが原因なら個人情報保護法上の対応は一切不要である。」に対応するため、誤答候補「漏えいの痕跡を消すためログを削除し、誰にも報告しない。」の問題点を直接説明していない。

総合解説：誤答候補「漏えいの痕跡を消すためログを削除し、誰にも報告しない。」について、誤りの内容を説明できることが重要である。調査を妨げ、法令上必要な対応も行えない。

対象：2026年度 / 基準日 2026-09-04

Q0134 4-5 法務・標準・評価・監査 > 個人情報保護・セキュリティ関連法規 ｜ 難易度：応用

「個人情報保護・セキュリティ関連法規」のうち「基本法の位置付け」を、正答の根拠まで理解できているか確認する。候補「国のサイバーセキュリティ施策の基本理念、戦略、基本的施策、戦略本部等を定め、官民の連携を含む施策を総合的に推進する基本法である。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．基本法であり個別技術設定を網羅するものではない。
イ．同法は我が国のサイバーセキュリティ政策の基本的枠組みを定める法律で、個別企業の全セキュリティ義務を一つで網羅する法律ではない。
ウ．目的が異なる。
エ．多様な主体の連携を重視する。

答え・解説 正答：イ

ア：この説明は別候補「民間企業の全システム設定値を細部まで直接定める単一の技術仕様書である。」に対応するため、正答候補「国のサイバーセキュリティ施策の基本理念、戦略、基本的施策、戦略本部等を定め、官民の連携を含む施策を総合的に推進する基本法である。」の根拠にはならない。
イ：この説明は正答候補「国のサイバーセキュリティ施策の基本理念、戦略、基本的施策、戦略本部等を定め、官民の連携を含む施策を総合的に推進する基本法である。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「サイバーセキュリティとは無関係な税率だけを定める法律である。」に対応するため、正答候補「国のサイバーセキュリティ施策の基本理念、戦略、基本的施策、戦略本部等を定め、官民の連携を含む施策を総合的に推進する基本法である。」の根拠にはならない。
エ：この説明は別候補「国や重要インフラ等の連携を否定し、各主体を完全分離することを目的とする。」に対応するため、正答候補「国のサイバーセキュリティ施策の基本理念、戦略、基本的施策、戦略本部等を定め、官民の連携を含む施策を総合的に推進する基本法である。」の根拠にはならない。

総合解説：正答候補「国のサイバーセキュリティ施策の基本理念、戦略、基本的施策、戦略本部等を定め、官民の連携を含む施策を総合的に推進する基本法である。」を選ぶ根拠は次のとおりである。同法は我が国のサイバーセキュリティ政策の基本的枠組みを定める法律で、個別企業の全セキュリティ義務を一つで網羅する法律ではない。

対象：2026年度 / 基準日 2026-09-04

Q0135 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：基礎

「標準・認証・セキュリティ技術評価」の「ISO15408」について、候補「IT製品・システムのセキュリティ機能や保証を共通の基準で評価するための国際的な評価基準を提供する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．ITセキュリティ評価の基準である。
イ．今回問われている論点には直接対応しない内容である。
ウ．ISO/IEC 15408はCommon Criteriaとして、IT製品等のセキュリティ評価で共通の要求表現と評価の枠組みを提供する。
エ．規格の目的ではない。

答え・解説 正答：ウ

ア：この説明は別候補「企業の財務諸表だけを監査する基準である。」に対応するため、正答候補「IT製品・システムのセキュリティ機能や保証を共通の基準で評価するための国際的な評価基準を提供する。」の根拠にはならない。
イ：この説明は別候補「無線LANの周波数割当だけを定める。」に対応するため、正答候補「IT製品・システムのセキュリティ機能や保証を共通の基準で評価するための国際的な評価基準を提供する。」の根拠にはならない。
ウ：この説明は正答候補「IT製品・システムのセキュリティ機能や保証を共通の基準で評価するための国際的な評価基準を提供する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「バックアップ世代数を一律に定める法律である。」に対応するため、正答候補「IT製品・システムのセキュリティ機能や保証を共通の基準で評価するための国際的な評価基準を提供する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。ISO/IEC 15408はCommon Criteriaとして、IT製品等のセキュリティ評価で共通の要求表現と評価の枠組みを提供する。

対象：2026年度 / 基準日 2026-09-04

Q0136 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：基礎

「標準・認証・セキュリティ技術評価」の「ISMS認証」を復習している学習者が、候補「個々のファイアウォール製品の脆弱性を一件ずつ認証するだけの規格である。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．ISMS認証は個別製品の機能評価ではなく、組織のマネジメントシステムが要求事項へ適合するかを審査する。
イ．マネジメントシステム規格である。
ウ．絶対無事故を保証するものではない。
エ．組織のISMS要求事項である。

答え・解説 正答：エ

ア：この説明は別候補「組織の情報セキュリティマネジメントシステムに対する要求事項を示し、第三者認証の基準として用いられる。」に対応するため、誤答候補「個々のファイアウォール製品の脆弱性を一件ずつ認証するだけの規格である。」の問題点を直接説明していない。
イ：この説明は別候補「暗号アルゴリズムの鍵長だけを定める。」に対応するため、誤答候補「個々のファイアウォール製品の脆弱性を一件ずつ認証するだけの規格である。」の問題点を直接説明していない。
ウ：この説明は別候補「認証を取得すると全インシデントが発生しないことを保証する。」に対応するため、誤答候補「個々のファイアウォール製品の脆弱性を一件ずつ認証するだけの規格である。」の問題点を直接説明していない。
エ：この説明は誤答候補「個々のファイアウォール製品の脆弱性を一件ずつ認証するだけの規格である。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「個々のファイアウォール製品の脆弱性を一件ずつ認証するだけの規格である。」については、何が誤りかを明確にした上で正しい概念へ戻す。組織のISMS要求事項である。

対象：2026年度 / 基準日 2026-09-04

Q0137 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：標準

「標準・認証・セキュリティ技術評価」のうち「JISEC」を確認する誤答分析で、学習者が候補「Pマークだけ」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．個人情報保護マネジメントに関する制度で、製品CC評価とは異なる。
イ．政府情報システム向けクラウドサービス評価制度である。
ウ．JISECはIT関連製品のセキュリティ機能の適切性・確実性を第三者評価し、認証する国内制度である。
エ．DNSの暗号学的検証技術である。

答え・解説 正答：ア

ア：この説明は誤答候補「Pマークだけ」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「ISMAPだけ」に対応するため、誤答候補「Pマークだけ」の問題点を直接説明していない。
ウ：この説明は別候補「JISEC」に対応するため、誤答候補「Pマークだけ」の問題点を直接説明していない。

エ：この説明は別候補「DNSSEC」に対応するため、誤答候補「Pマークだけ」の問題点を直接説明していない。

総合解説：誤答候補「Pマークだけ」について、誤りの内容を説明できることが重要である。個人情報保護マネジメントに関する制度で、製品CC評価とは異なる。

対象：2026年度 / 基準日 2026-09-04

Q0138 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：標準

「標準・認証・セキュリティ技術評価」のうち「TOE」を、正答の根拠まで理解できているか確認する。候補「TOE（Target of Evaluation）」を妥当と判断する根拠として最も適切な説明はどれか。

ア．復旧時間目標である。
イ．TOEは評価対象として定義された製品・システム等を指す。
ウ．侵害指標である。
エ．事業影響度分析である。

答え・解説 正答：イ

ア：この説明は別候補「RTO」に対応するため、正答候補「TOE（Target of Evaluation）」の根拠にはならない。
イ：この説明は正答候補「TOE（Target of Evaluation）」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「IOC」に対応するため、正答候補「TOE（Target of Evaluation）」の根拠にはならない。
エ：この説明は別候補「BIA」に対応するため、正答候補「TOE（Target of Evaluation）」の根拠にはならない。

総合解説：正答候補「TOE（Target of Evaluation）」を選ぶ根拠は次のとおりである。TOEは評価対象として定義された製品・システム等を指す。

対象：2026年度 / 基準日 2026-09-04

Q0139 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：標準

「標準・認証・セキュリティ技術評価」の「ST」について、候補「ST（Security Target）」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．サービスレベル合意である。
イ．証明書失効リストである。
ウ．STは特定の評価対象に対するセキュリティ要求や評価対象の説明等を記述する。
エ．ソフトウェア部品表である。

答え・解説 正答：ウ

ア：この説明は別候補「SLA」に対応するため、正答候補「ST（Security Target）」の根拠にはならない。
イ：この説明は別候補「CRL」に対応するため、正答候補「ST（Security Target）」の根拠にはならない。
ウ：この説明は正答候補「ST（Security Target）」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「SBOM」に対応するため、正答候補「ST（Security Target）」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。STは特定の評価対象に対するセキュリティ要求や評価対象の説明等を記述する。

対象：2026年度 / 基準日 2026-09-04

Q0140 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：標準

「標準・認証・セキュリティ技術評価」の「PP」を復習している学習者が、候補「RPO」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．STは特定TOEに対する文書である。
イ．PPは特定の製品群・用途に対するセキュリティ要求を再利用可能な形で表現する。
ウ．脆弱性識別子である。
エ．復旧時点目標である。

答え・解説 正答：エ

ア：この説明は別候補「STだけ」に対応するため、誤答候補「RPO」の問題点を直接説明していない。
イ：この説明は別候補「PP（Protection Profile）」に対応するため、誤答候補「RPO」の問題点を直接説明していない。
ウ：この説明は別候補「CVE」に対応するため、誤答候補「RPO」の問題点を直接説明していない。
エ：この説明は誤答候補「RPO」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「RPO」については、何が誤りかを明確にした上で正しい概念へ戻す。復旧時点目標である。

対象：2026年度 / 基準日 2026-09-04

Q0141 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：応用

「標準・認証・セキュリティ技術評価」のうち「制度比較」を確認する誤答分析で、学習者が候補「どちらもCVSSの点数だけで第三者認証を代替する。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．CVSSは脆弱性深刻度指標で認証制度ではない。
イ．DNS保護技術であり認証制度ではない。
ウ．目的と制度が逆である。
エ．ISO/IEC 27001は組織のマネジメントシステム、ISO/IEC 15408はIT製品等のセキュリティ評価という対象の違いがある。

答え・解説 正答：ア

ア：この説明は誤答候補「どちらもCVSSの点数だけで第三者認証を代替する。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「組織Aも部門BもDNSSECだけを取得する。」に対応するため、誤答候補「どちらもCVSSの点数だけで第三者認証を代替する。」の問題点を直接説明していない。
ウ：この説明は別候補「組織AはJISEC製品認証だけ、部門BはBCPだけを使う。」に対応するため、誤答候補「どちらもCVSSの点数だけで第三者認証を代替する。」の問題点を直接説明していない。
エ：この説明は別候補「組織AはISO/IEC 27001に基づくISMS認証、部門BはISO/IEC 15408/Common Criteriaに基づく評価認証を検討する。」に対応するため、誤答候補「どちらもCVSSの点数だけで第三者認証を代替する。」の問題点を直接説明していない。

総合解説：誤答候補「どちらもCVSSの点数だけで第三者認証を代替する。」について、誤りの内容を説明できることが重要である。CVSSは脆弱性深刻度指標で認証制度ではない。

対象：2026年度 / 基準日 2026-09-04

Q0142 4-5 法務・標準・評価・監査 > 標準・認証・セキュリティ技術評価 ｜ 難易度：応用

「標準・認証・セキュリティ技術評価」のうち「クラウド評価制度」を、正答の根拠まで理解できているか確認する。候補「ISMAP」を妥当と判断する根拠として最も適切な説明はどれか。

ア．主にIT製品等のISO/IEC 15408評価認証であり、クラウドサービス登録制度とは異なる。
イ．ISMAPは政府情報システムのためのクラウドサービスのセキュリティ評価制度で、クラウドサービスリスト等が運用されている。
ウ．目的に応じてクラウドサービス評価も確認する。
エ．CVEとISMAP登録は別制度である。

答え・解説 正答：イ

ア：この説明は別候補「JISECだけ」に対応するため、正答候補「ISMAP」の根拠にはならない。
イ：この説明は正答候補「ISMAP」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「ISO/IEC 27001認証だけで、クラウドサービス固有の評価は一切確認不要とする。」に対応するため、正答候補「ISMAP」の根拠にはならない。
エ：この説明は別候補「CVE番号が一つもなければ自動的にISMAP登録済みと判断する。」に対応するため、正答候補「ISMAP」の根拠にはならない。

総合解説：正答候補「ISMAP」を選ぶ根拠は次のとおりである。ISMAPは政府情報システムのためのクラウドサービスのセキュリティ評価制度で、クラウドサービスリスト等が運用されている。

対象：2026年度 / 基準日 2026-09-04

Q0143 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：基礎

「セキュリティ監査・ガバナンス」の「監査目的」について、候補「リスクに基づくコントロールの整備・運用状況を独立かつ専門的な立場から検証・評価し、保証又は助言を行う。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．監査と業務執行は分ける必要がある。
イ．客観的根拠が必要である。
ウ．監査は情報セキュリティリスクのマネジメントが効果的に行われるよう、管理策の有効性を客観的に検証する。
エ．監査目的に反する。

答え・解説 正答：ウ

ア：この説明は別候補「監査人が被監査部門の業務を全て代行すること。」に対応するため、正答候補「リスクに基づくコントロールの整備・運用状況を独立かつ専門的な立場から検証・評価し、保証又は助言を行う。」の根拠にはならない。
イ：この説明は別候補「監査証拠を残さず主観だけで結論を決めること。」に対応するため、正答候補「リスクに基づくコントロールの整備・運用状況を独立かつ専門的な立場から検証・評価し、保証又は助言を行う。」の根拠にはならない。
ウ：この説明は正答候補「リスクに基づくコントロールの整備・運用状況を独立かつ専門的な立場から検証・評価し、保証又は助言を行う。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「監査対象の脆弱性を秘密にして改善させないこと。」に対応するため、正答候補「リスクに基づくコントロールの整備・運用状況を独立かつ専門的な立場から検証・評価し、保証又は助言を行う。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。監査は情報セキュリティリスクのマネジメントが効果的に行われるよう、管理策の有効性を客観的に検証する。

対象：2026年度 / 基準日 2026-09-04

Q0144 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：基礎

「セキュリティ監査・ガバナンス」の「独立性」を復習している学習者が、候補「利害関係が強いほど監査品質が必ず高まる。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．客観性・独立性を損なう。
イ．監査基準では外観上の独立性と精神上の独立性、客観性が重要とされる。
ウ．監査判断の独立性を失う。
エ．独立性の懸念が大きくなる。

答え・解説 正答：エ

ア：この説明は別候補「自分が設計・運用した対象を、自分の成果を守る立場で無条件に合格と判定する。」に対応するため、誤答候補「利害関係が強いほど監査品質が必ず高まる。」の問題点を直接説明していない。
イ：この説明は別候補「監査対象からの外観上の独立性に配慮し、偏向を排して公正・客観的に監査判断を行う。」に対応するため、誤答候補「利害関係が強いほど監査品質が必ず高まる。」の問題点を直接説明していない。
ウ：この説明は別候補「監査対象部門の指示どおり結論を書き換える。」に対応するため、誤答候補「利害関係が強いほど監査品質が必ず高まる。」の問題点を直接説明していない。
エ：この説明は誤答候補「利害関係が強いほど監査品質が必ず高まる。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「利害関係が強いほど監査品質が必ず高まる。」については、何が誤りかを明確にした上で正しい概念へ戻す。独立性の懸念が大きくなる。

対象：2026年度 / 基準日 2026-09-04

Q0145 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：標準

「セキュリティ監査・ガバナンス」のうち「監査証拠」を確認する誤答分析で、学習者が候補「担当者の『たぶん実施した』という記憶だけ。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．客観的な裏付けが弱い。
イ．証拠としての関連性がない。
ウ．監査結論は十分かつ適切な証拠に基づく必要があり、口頭説明だけでなく記録や観察等を組み合わせる。
エ．十分な根拠にならない。

答え・解説 正答：ア

ア：この説明は誤答候補「担当者の『たぶん実施した』という記憶だけ。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「監査対象とは無関係な広告資料。」に対応するため、誤答候補「担当者の『たぶん実施した』という記憶だけ。」の問題点を直接説明していない。
ウ：この説明は別候補「承認記録、権限一覧、変更履歴、レビュー結果など、実際の実施を裏付ける記録。」に対応するため、誤答候補「担当者の『たぶん実施した』という記憶だけ。」の問題点を直接説明していない。

エ：この説明は別候補「監査人の推測だけ。」に対応するため、誤答候補「担当者の『たぶん実施した』という記憶だけ。」の問題点を直接説明していない。

総合解説：誤答候補「担当者の『たぶん実施した』という記憶だけ。」について、誤りの内容を説明できることが重要である。客観的な裏付けが弱い。

対象：2026年度 / 基準日 2026-09-04

Q0146 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：標準

「セキュリティ監査・ガバナンス」のうち「監査計画」を、正答の根拠まで理解できているか確認する。候補「組織・システムのリスク特性を把握し、重要性や過去の問題、環境変化を踏まえて監査範囲と手続を定める。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．重要領域への資源配分が不十分になり得る。
イ．リスクの高い領域へ重点を置くリスクベースの監査計画が実効性を高める。
ウ．計画性・再現性を欠く。
エ．リスク変化を反映できない。

答え・解説 正答：イ

ア：この説明は別候補「全領域をリスクに関係なく同じ深さで機械的に監査する。」に対応するため、正答候補「組織・システムのリスク特性を把握し、重要性や過去の問題、環境変化を踏まえて監査範囲と手続を定める。」の根拠にはならない。
イ：この説明は正答候補「組織・システムのリスク特性を把握し、重要性や過去の問題、環境変化を踏まえて監査範囲と手続を定める。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「監査目的や範囲を決めず、その場で思いついた質問だけする。」に対応するため、正答候補「組織・システムのリスク特性を把握し、重要性や過去の問題、環境変化を踏まえて監査範囲と手続を定める。」の根拠にはならない。
エ：この説明は別候補「前年の計画を環境変化に関係なく永久に固定する。」に対応するため、正答候補「組織・システムのリスク特性を把握し、重要性や過去の問題、環境変化を踏まえて監査範囲と手続を定める。」の根拠にはならない。

総合解説：正答候補「組織・システムのリスク特性を把握し、重要性や過去の問題、環境変化を踏まえて監査範囲と手続を定める。」を選ぶ根拠は次のとおりである。リスクの高い領域へ重点を置くリスクベースの監査計画が実効性を高める。

対象：2026年度 / 基準日 2026-09-04

Q0147 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：標準

「セキュリティ監査・ガバナンス」の「サンプリング」について、候補「リスクと監査目的に応じて適切なサンプリング方法を設計し、母集団・抽出方法・結果を記録する。」を他の候補と区別する決め手として最も適切な説明はどれか。

ア．選択バイアスが強く証拠として不適切である。
イ．その判断を支持する根拠が示されておらず、妥当な説明とはいえない。
ウ．監査手続ではサンプリングを用いることがあり、偏りや代表性を考慮して結論を導く必要がある。
エ．母集団を歪める。

答え・解説 正答：ウ

ア：この説明は別候補「都合のよい正常記録だけを選び、抽出条件を残さない。」に対応するため、正答候補「リスクと監査目的に応じて適切なサンプリング方法を設計し、母集団・抽出方法・結果を記録する。」の根拠にはならない。
イ：この説明は別候補「一件も確認せず全件適正と断定する。」に対応するため、正答候補「リスクと監査目的に応じて適切なサンプリング方法を設計し、母集団・抽出方法・結果を記録する。」の根拠にはならない。
ウ：この説明は正答候補「リスクと監査目的に応じて適切なサンプリング方法を設計し、母集団・抽出方法・結果を記録する。」の根拠に対応しており、今回の問いに合致する。
エ：この説明は別候補「異常記録だけ除外してから抽出する。」に対応するため、正答候補「リスクと監査目的に応じて適切なサンプリング方法を設計し、母集団・抽出方法・結果を記録する。」の根拠にはならない。

総合解説：近接概念との区別では、正答候補に固有の根拠を押さえる。監査手続ではサンプリングを用いることがあり、偏りや代表性を考慮して結論を導く必要がある。

対象：2026年度 / 基準日 2026-09-04

Q0148 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：標準

「セキュリティ監査・ガバナンス」の「監査と執行」を復習している学習者が、候補「監査人が経営者に無断で本番システムを全面改修する。」を正答だと考えている。この誤解を直接修正するフィードバックとして最も適切な説明はどれか。

ア．監査はマネジメントの責任を代替するものではなく、評価・助言を通じて改善を支援する。
イ．管理責任は組織側にある。
ウ．監査目的に反する。
エ．業務執行責任との分離が必要である。

答え・解説 正答：エ

ア：この説明は別候補「監査人は根拠に基づき指摘・保証・助言を行い、管理者は是正措置を決定・実施する。」に対応するため、誤答候補「監査人が経営者に無断で本番システムを全面改修する。」の問題点を直接説明していない。
イ：この説明は別候補「管理者は監査指摘を読まず、監査人が全責任を負う。」に対応するため、誤答候補「監査人が経営者に無断で本番システムを全面改修する。」の問題点を直接説明していない。
ウ：この説明は別候補「重大不備でも監査報告へ記載しない。」に対応するため、誤答候補「監査人が経営者に無断で本番システムを全面改修する。」の問題点を直接説明していない。
エ：この説明は誤答候補「監査人が経営者に無断で本番システムを全面改修する。」の問題点に対応しており、今回の誤解を直接修正できる。

総合解説：誤答候補「監査人が経営者に無断で本番システムを全面改修する。」については、何が誤りかを明確にした上で正しい概念へ戻す。業務執行責任との分離が必要である。

対象：2026年度 / 基準日 2026-09-04

Q0149 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：応用

「セキュリティ監査・ガバナンス」のうち「独立性事例」を確認する誤答分析で、学習者が候補「独立性は外部監査にだけ必要で内部監査には一切不要である。」を選んだ。この選択を見直す理由として最も適切な説明はどれか。

ア．内部監査でも独立性・客観性への配慮が必要である。
イ．自己利益・自己レビューの脅威がある。
ウ．監査対象の設計・運用責任と監査機能が同一人物へ集中すると、精神上・外観上の独立性が損なわれるおそれがある。
エ．監査の信頼性を失う。

答え・解説 正答：ア

ア：この説明は誤答候補「独立性は外部監査にだけ必要で内部監査には一切不要である。」の問題点に対応しており、今回の誤解を直接修正できる。
イ：この説明は別候補「自分の設計なので最も客観的に無条件合格判定できる。」に対応するため、誤答候補「独立性は外部監査にだけ必要で内部監査には一切不要である。」の問題点を直接説明していない。
ウ：この説明は別候補「自己レビューによる独立性・客観性の懸念があるため、監査対象から独立した監査人の配置などを検討する。」に対応するため、誤答候補「独立性は外部監査にだけ必要で内部監査には一切不要である。」の問題点を直接説明していない。
エ：この説明は別候補「監査結果は証拠なしで開発責任者の希望どおりにする。」に対応するため、誤答候補「独立性は外部監査にだけ必要で内部監査には一切不要である。」の問題点を直接説明していない。

総合解説：誤答候補「独立性は外部監査にだけ必要で内部監査には一切不要である。」について、誤りの内容を説明できることが重要である。内部監査でも独立性・客観性への配慮が必要である。

対象：2026年度 / 基準日 2026-09-04

Q0150 4-5 法務・標準・評価・監査 > セキュリティ監査・ガバナンス ｜ 難易度：応用

「セキュリティ監査・ガバナンス」のうち「ガバナンス改善」を、正答の根拠まで理解できているか確認する。候補「経営層がリスク受容方針と責任を明確にし、重要指標・重大事案・監査結果・是正進捗を定期的に報告・監督する仕組みを整える。」を妥当と判断する根拠として最も適切な説明はどれか。

ア．経営判断に必要なリスク情報が届かない。
イ．情報セキュリティガバナンスでは経営層が方向性と監督責任を持ち、リスクや改善状況を可視化して意思決定することが重要である。
ウ．ガバナンスを損なう。
エ．責任と意思決定経路が不明確である。

答え・解説 正答：イ

ア：この説明は別候補「セキュリティ情報を現場だけで保持し経営へ一切報告しない。」に対応するため、正答候補「経営層がリスク受容方針と責任を明確にし、重要指標・重大事案・監査結果・是正進捗を定期的に報告・監督する仕組みを整える。」の根拠にはならない。
イ：この説明は正答候補「経営層がリスク受容方針と責任を明確にし、重要指標・重大事案・監査結果・是正進捗を定期的に報告・監督する仕組みを整える。」の根拠に対応しており、今回の問いに合致する。
ウ：この説明は別候補「監査指摘を全て削除してリスクがないように見せる。」に対応するため、正答候補「経営層がリスク受容方針と責任を明確にし、重要指標・重大事案・監査結果・是正進捗を定期的に報告・監督する仕組みを整える。」の根拠にはならない。
エ：この説明は別候補「責任者を定めず重大事案ごとに誰かが自主対応する。」に対応するため、正答候補「経営層がリスク受容方針と責任を明確にし、重要指標・重大事案・監査結果・是正進捗を定期的に報告・監督する仕組みを整える。」の根拠にはならない。

総合解説：正答候補「経営層がリスク受容方針と責任を明確にし、重要指標・重大事案・監査結果・是正進捗を定期的に報告・監督する仕組みを整える。」を選ぶ根拠は次のとおりである。情報セキュリティガバナンスでは経営層が方向性と監督責任を持ち、リスクや改善状況を可視化して意思決定することが重要である。

対象：2026年度 / 基準日 2026-09-04