0001 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：基礎

「機密性・完全性・可用性・基本概念」の「機密性」を確認する。次の判断「許可された者だけが情報へアクセスできる状態を維持すること。」が適切である根拠として、最も直接的な説明はどれか。

ア. 機密性は情報へのアクセスを許可された主体に限定する性質である。
イ. 「情報が許可なく改ざんされていない状態を維持すること。」は完全性の説明である。
ウ. 「必要なときに情報やサービスを利用できる状態を維持すること。」は可用性の説明である。
エ. 匿名化はプライバシー保護手法の一つで、機密性そのものの定義ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「情報が許可なく改ざんされていない状態を維持すること。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「必要なときに情報やサービスを利用できる状態を維持すること。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「利用者の操作履歴を必ず匿名化すること。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「機密性」について、結論だけでなく正答理由を説明できるかを確認する。機密性は情報へのアクセスを許可された主体に限定する性質である。 情報セキュリティの基本は機密性・完全性・可用性を区別して理解することである。

基準：2026年度 / 2026-09-04

0002 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：標準

「機密性・完全性・可用性・基本概念」の演習で「否認防止（Non-Repudiation）だけ。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 完全性は情報が正確で完全であり、不正に変更されていないことを重視する。
イ. 否認防止は行為の事実を後から否定できないようにする性質である。
ウ. 機密性はアクセス制御や秘匿に関する性質である。
エ. 可用性は必要時に利用できることを重視する。

答え・解説 正答：イ

ア：この説明は元の論点では「完全性（Integrity）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「機密性（Confidentiality）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「可用性（Availability）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「完全性」について、誤答肢のどこが不適切かを説明できるかを確認する。否認防止は行為の事実を後から否定できないようにする性質である。 改ざん検知やアクセス権管理は完全性を守る代表的な手段となる。

基準：2026年度 / 2026-09-04

0003 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：基礎

「可用性」に関する理解を確認する。「責任追跡性（Accountability）だけ。」という判断の問題点を説明しているものはどれか。

ア. 真正性は主体や情報が本物であることを確かめる性質である。
イ. 可用性は情報やサービスを必要なときに利用可能な状態へ保つことを意味する。
ウ. 責任追跡性は行為主体を追跡できる性質である。
エ. 機密性は不正な閲覧を防ぐ性質である。

答え・解説 正答：ウ

ア：この説明は元の論点では「真正性（Authenticity）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「可用性（Availability）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「機密性（Confidentiality）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「可用性」について、誤答肢のどこが不適切かを説明できるかを確認する。責任追跡性は行為主体を追跡できる性質である。 冗長化やバックアップ、障害対策は可用性確保に役立つ。

基準：2026年度 / 2026-09-04

0004 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：標準

「機密性・完全性・可用性・基本概念」を復習している。「スループット。」が正答にならない理由として最も適切なものはどれか。

ア. 可用性は利用可能性に関する性質である。
イ. 圧縮率はデータ量の指標である。
ウ. 真正性は主体や情報源が主張どおり本物であることを確認する性質である。
エ. スループットは性能指標である。

答え・解説 正答：エ

ア：この説明は元の論点では「可用性。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「圧縮率。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「真正性（Authenticity）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「なりすまし対策」について、誤答肢のどこが不適切かを説明できるかを確認する。スループットは性能指標である。 認証や電子署名は真正性の確認に利用される。

基準：2026年度 / 2026-09-04

0005 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：応用

「責任追跡性を理解する」ために、「責任追跡性（Accountability）。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. 責任追跡性は行為と実行主体を対応付けて追跡できる性質である。
イ. 可用性の中心はサービス継続である。
ウ. 秘匿化は情報を見えにくくする対策である。
エ. 圧縮効率とは無関係である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「可用性だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「秘匿化だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「圧縮効率。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「ログ」について、結論だけでなく正答理由を説明できるかを確認する。責任追跡性は行為と実行主体を対応付けて追跡できる性質である。 監査ログやアクセスログは責任追跡性の確保に重要である。

基準：2026年度 / 2026-09-04

0006 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：標準

「機密性・完全性・可用性・基本概念」の「電子署名」を確認する。次の選択「可用性。」が不適切である理由として、最も直接的な説明はどれか。

ア. 負荷分散は性能・可用性向上の技術である。
イ. 可用性はサービス利用可能性である。
ウ. 否認防止は後から行為の事実を否定できないようにする性質である。
エ. 圧縮はデータ量削減である。

答え・解説 正答：イ

ア：この説明は元の論点では「負荷分散。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「否認防止（Non-Repudiation）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「圧縮。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「電子署名」について、誤答肢のどこが不適切かを説明できるかを確認する。可用性はサービス利用可能性である。 電子署名やタイムスタンプは否認防止に利用される。

基準：2026年度 / 2026-09-04

0007 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：基礎

「機密性・完全性・可用性・基本概念」の演習で「一つの強力なパスワードだけに全ての防御を依存する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. アクセス制御解除は防御にならない。
イ. バックアップは重要だが、それだけで侵入を防ぐことはできない。
ウ. 単一対策への依存はその対策が破られた際に脆弱である。
エ. 多層防御では境界、端末、認証、監視など複数の防御策を組み合わせる。

答え・解説 正答：ウ

ア：この説明は元の論点では「全てのアクセス制御を解除して監視だけを行う。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「バックアップだけ実施し、侵入防止対策は一切行わない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「一つの対策が破られても他の対策で被害を防げるよう、異なる防御策を複数層で組み合わせる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「Defense in Depth」について、誤答肢のどこが不適切かを説明できるかを確認する。単一対策への依存はその対策が破られた際に脆弱である。 異なる管理策を重ねることで単一障害点のような防御上の弱点を減らす。

基準：2026年度 / 2026-09-04

0008 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：標準

「設計段階から対策」に関する理解を確認する。「フェイルオーバだけ。」という判断の問題点を説明しているものはどれか。

ア. リリース直前だけの後付け対策とは異なる。
イ. 通信品質方式の話ではない。
ウ. セキュリティバイデザインは開発初期からセキュリティ要件を組み込む考え方である。
エ. フェイルオーバは可用性対策の一つである。

答え・解説 正答：エ

ア：この説明は元の論点では「後付け暗号化だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ベストエフォート通信。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「セキュリティバイデザイン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「設計段階から対策」について、誤答肢のどこが不適切かを説明できるかを確認する。フェイルオーバは可用性対策の一つである。 早期工程でリスクを考慮すると設計変更コストを抑えつつ体系的な対策を実装しやすい。

基準：2026年度 / 2026-09-04

0009 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：応用

「機密性・完全性・可用性・基本概念」の演習で「プライバシーバイデザイン。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. プライバシーバイデザインは企画・設計段階から個人情報保護を組み込む考え方である。
イ. ゼロデイ攻撃は未修正脆弱性を狙う攻撃である。
ウ. スケールアウトは性能拡張の方式である。
エ. 圧縮は情報量削減技術である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「ゼロデイ攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「スケールアウト。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「データ圧縮。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「個人情報保護」について、結論だけでなく正答理由を説明できるかを確認する。プライバシーバイデザインは企画・設計段階から個人情報保護を組み込む考え方である。 データ最小化や目的明確化はプライバシー配慮の重要な観点となる。

基準：2026年度 / 2026-09-04

0010 セキュリティ基礎・リスク > 機密性・完全性・可用性・基本概念 ｜ 難易度：標準

「CIAのトレードオフを理解する」ために、「可用性と機密性は必ず両立できないため、どちらか一方を完全に捨てる。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 復旧データが正しいことを確保する完全性も重要である。
イ. 複数要件をバランスよく満たすのがセキュリティ設計である。
ウ. 遠隔複製は可用性を高める一方、保管箇所が増えるため機密性対策も必要である。
エ. 複製先の不正閲覧リスクが高まる。

答え・解説 正答：イ

ア：この説明は元の論点では「災害対策では完全性を考慮する必要がない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「可用性向上だけでなく、複製先でのアクセス制御や暗号化も行い機密性を維持する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「複製先は多いほどよいのでアクセス制御は不要である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「機密性・完全性・可用性・基本概念」の「可用性と機密性」について、誤答肢のどこが不適切かを説明できるかを確認する。複数要件をバランスよく満たすのがセキュリティ設計である。 CIAは独立して考えるだけでなく、システム要件に応じてバランスよく確保する。

基準：2026年度 / 2026-09-04

0011 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：基礎

「脅威・脆弱性・攻撃者」の「基本概念」を確認する。次の選択「脆弱性は必ず攻撃者そのものを指す。」が不適切である理由として、最も直接的な説明はどれか。

ア. 脅威は安全状態ではない。
イ. 脅威は事故・攻撃・災害など損失要因、脆弱性はシステムや組織の弱点である。
ウ. 脆弱性は弱点であり攻撃者そのものではない。
エ. 両者は区別される。

答え・解説 正答：ウ

ア：この説明は元の論点では「脅威は対策済みの安全な状態だけを指す。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「脅威は損害を生じさせる要因で、脆弱性は脅威に悪用され得る弱点である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「脅威と脆弱性は完全に同じ意味である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「基本概念」について、誤答肢のどこが不適切かを説明できるかを確認する。脆弱性は弱点であり攻撃者そのものではない。 リスクは情報資産、脅威、脆弱性などの組合せで考える。

基準：2026年度 / 2026-09-04

0012 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：標準

「脅威・脆弱性・攻撃者」の演習で「CPUキャッシュミス。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 暗号方式の安全性とは別問題である。
イ. DB設計とは無関係である。
ウ. 教育や行動上の弱点は人的脆弱性に分類できる。
エ. 性能問題である。

答え・解説 正答：エ

ア：この説明は元の論点では「暗号アルゴリズムの危殆化だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「データベース正規化不足。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「人的脆弱性。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「教育不足」について、誤答肢のどこが不適切かを説明できるかを確認する。性能問題である。 セキュリティは技術だけでなく人的・組織的対策を組み合わせる必要がある。

基準：2026年度 / 2026-09-04

0013 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：基礎

「内部犯」に関する理解を確認する。「内部不正。」という結論を支持する説明として最も適切なものはどれか。

ア. 組織内部の権限保有者が意図的に不正を行うのは内部不正である。
イ. 自然災害ではない。
ウ. サービス妨害攻撃とは異なる。
エ. 故障による偶発事象ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「自然災害。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「外部DoS攻撃だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「偶発的な機器故障。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「内部犯」について、結論だけでなく正答理由を説明できるかを確認する。組織内部の権限保有者が意図的に不正を行うのは内部不正である。 内部不正対策では最小権限、職務分掌、監査ログ、教育などが重要となる。

基準：2026年度 / 2026-09-04

0014 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：標準

「脅威・脆弱性・攻撃者」を復習している。「予防・検知・是正。」が正答にならない理由として最も適切なものはどれか。

ア. 不正のトライアングルは機会、動機、正当化で説明される。
イ. 管理策のタイプである。
ウ. 「機密性・完全性・可用性。」はCIA三要素である。
エ. サイバーセキュリティ活動の要素の一部に近い。

答え・解説 正答：イ

ア：この説明は元の論点では「機会・動機・正当化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「機密性・完全性・可用性。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「識別・防御・復旧。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「機会・動機・正当化」について、誤答肢のどこが不適切かを説明できるかを確認する。管理策のタイプである。 内部不正を減らすには、特に不正を実行しにくい環境を作って機会を減らすことが重要である。

基準：2026年度 / 2026-09-04

0015 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：応用

「ゼロデイ攻撃を理解する」ために、「SQLの結合。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 辞書攻撃は辞書語などをパスワード候補に使う。
イ. 修正策が行き渡る前の未知・未修正脆弱性を狙う攻撃をゼロデイ攻撃という。
ウ. データベース操作である。
エ. 総当たり攻撃は候補を網羅的に試す。

答え・解説 正答：ウ

ア：この説明は元の論点では「辞書攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ゼロデイ攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「総当たり攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「未修正脆弱性」について、誤答肢のどこが不適切かを説明できるかを確認する。データベース操作である。 ゼロデイ対策では多層防御、振る舞い検知、影響緩和策などが重要になる。

基準：2026年度 / 2026-09-04

0016 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：標準

「脅威・脆弱性・攻撃者」の「ポートスキャン」を確認する。次の選択「正規化。」が不適切である理由として、最も直接的な説明はどれか。

ア. 電子署名は真正性・完全性確認に利用する。
イ. バックアップは復旧対策である。
ウ. ポートスキャンは開いているポートやサービスを調査する攻撃準備・調査行為である。
エ. DB設計技法である。

答え・解説 正答：エ

ア：この説明は元の論点では「電子署名。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「バックアップ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ポートスキャン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「ポートスキャン」について、誤答肢のどこが不適切かを説明できるかを確認する。DB設計技法である。 不要なサービスを停止し、監視で異常なスキャンを検知することが対策となる。

基準：2026年度 / 2026-09-04

0017 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：基礎

「脅威・脆弱性・攻撃者」を復習している。「金銭奪取。」と判断できる理由として最も適切なものはどれか。

ア. 身代金要求は金銭獲得を目的とする典型例である。
イ. サービス可用性を高める行為ではない。
ウ. データ品質改善でもない。
エ. 法令遵守とは逆の犯罪行為である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「可用性向上。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「データ品質改善。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「法令遵守。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「金銭目的」について、結論だけでなく正答理由を説明できるかを確認する。身代金要求は金銭獲得を目的とする典型例である。 攻撃者の種類や動機を把握すると想定脅威の整理に役立つ。

基準：2026年度 / 2026-09-04

0018 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：標準

「取引先経由」に関する理解を確認する。「単純な停電。」という判断の問題点を説明しているものはどれか。

ア. ストレージ断片化とは無関係である。
イ. 電源障害ではない。
ウ. 取引先やソフトウェア供給経路を悪用する攻撃はサプライチェーン攻撃に該当する。
エ. 更新経路が侵害されているため正常更新ではない。

答え・解説 正答：イ

ア：この説明は元の論点では「物理ディスク断片化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「サプライチェーンを介した攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「内部統制とは無関係な正常更新。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「取引先経由」について、誤答肢のどこが不適切かを説明できるかを確認する。電源障害ではない。 自組織だけでなく委託先・供給元のセキュリティもリスク管理対象となる。

基準：2026年度 / 2026-09-04

0019 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：応用

「脅威・脆弱性・攻撃者」を復習している。「ARPスプーフィング。」が正答にならない理由として最も適切なものはどれか。

ア. メモリ境界を越える書込みを悪用する攻撃であり別物である。
イ. DNSを使った負荷分散方式である。
ウ. ARPの対応関係を偽装する攻撃である。
エ. 生成AIへの指示系統を悪用し、意図しない動作を誘導するのがプロンプトインジェクションである。

答え・解説 正答：ウ

ア：この説明は元の論点では「バッファオーバーフローだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「DNSラウンドロビン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「プロンプトインジェクション。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「プロンプトインジェクション」について、誤答肢のどこが不適切かを説明できるかを確認する。ARPの対応関係を偽装する攻撃である。 AI利用時も入力データの信頼性、権限分離、出力検証などの対策が必要になる。

基準：2026年度 / 2026-09-04

0020 セキュリティ基礎・リスク > 脅威・脆弱性・攻撃者 ｜ 難易度：標準

「脆弱性管理の必要性を理解する」ために、「多要素認証。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 署名技術でもない。
イ. 性能拡張方式でもない。
ウ. 組織の正式な管理外で利用されるITサービスや機器をシャドーITという。
エ. 認証方式ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「デジタル署名。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「スケールアウト。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「シャドーIT。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「脅威・脆弱性・攻撃者」の「シャドーIT」について、誤答肢のどこが不適切かを説明できるかを確認する。認証方式ではない。 シャドーITは情報資産の所在把握やアクセス管理を難しくし、組織的な脆弱性となり得る。

基準：2026年度 / 2026-09-04

0021 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「特定・分析・評価」を確認する。次の判断「リスクを特定し、分析し、組織の基準に照らして評価する。」が適切である根拠として、最も直接的な説明はどれか。

ア. リスクアセスメントは一般にリスク特定、リスク分析、リスク評価の流れで行う。
イ. 資産特定は対策後ではなく前段階で重要である。
ウ. 全リスクを無条件に受容するのは適切でない。
エ. 事前評価がリスク管理の目的である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「対策を実施した後に資産を初めて特定する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「全リスクを無条件に受容する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「障害が起きるまで何も調査しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「特定・分析・評価」について、結論だけでなく正答理由を説明できるかを確認する。リスクアセスメントは一般にリスク特定、リスク分析、リスク評価の流れで行う。 アセスメント結果を基にリスク対応を選定する。

基準：2026年度 / 2026-09-04

0022 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」の演習で「ルーティングテーブル。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. CPU命令仕様とは無関係である。
イ. ネットワーク経路情報である。
ウ. 情報資産台帳は保護対象となる資産を識別・管理するために用いる。
エ. 名前解決結果の一時保存である。

答え・解説 正答：イ

ア：この説明は元の論点では「CPU命令表。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「情報資産台帳。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「DNSキャッシュ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「資産特定」について、誤答肢のどこが不適切かを説明できるかを確認する。ネットワーク経路情報である。 何を守るか明確でなければ、リスク評価や対策の優先順位付けができない。

基準：2026年度 / 2026-09-04

0023 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

「リスクマトリックス」に関する理解を確認する。「ページ置換。」という判断の問題点を説明しているものはどれか。

ア. 負荷分散・スケジューリング方式である。
イ. 発生可能性と影響度の区分を組み合わせる方法は定性的なリスク評価に広く用いられる。
ウ. メモリ管理方式である。
エ. 暗号方式である。

答え・解説 正答：ウ

ア：この説明は元の論点では「ラウンドロビン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「リスクマトリックスを用いた定性的評価。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「公開鍵暗号。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「リスクマトリックス」について、誤答肢のどこが不適切かを説明できるかを確認する。メモリ管理方式である。 数値データが十分でない場合でも共通基準で相対的な優先順位を付けられる。

基準：2026年度 / 2026-09-04

0024 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」を復習している。「400万円。」が正答にならない理由として最も適切なものはどれか。

ア. 1回当たり損失額そのもので、年間頻度を考慮していない。
イ. 頻度の扱いが誤っている。
ウ. 200万円×0.2=40万円である。
エ. 計算が10倍大きい。

答え・解説 正答：エ

ア：この説明は元の論点では「200万円。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「1,000万円。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「40万円。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「リスクアセスメント・リスク対応」の「ALE」について、誤答肢のどこが不適切かを説明できるかを確認する。計算が10倍大きい。 定量的評価では損失額と発生頻度を用いて年間損失の期待値を求めることがある。

基準：2026年度 / 2026-09-04

0025 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

「リスク回避を理解する」ために、「リスク回避。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. リスク源となる活動をやめることでリスクそのものを避けるのがリスク回避である。
イ. リスク保有は残るリスクを受け入れる対応である。
ウ. リスク共有は保険や委託などで負担を分担する。
エ. 検知は管理策のタイプでありリスク対応分類とは異なる。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「リスク保有。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「リスク共有。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「リスク検知だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「業務中止」について、結論だけでなく正答理由を説明できるかを確認する。リスク源となる活動をやめることでリスクそのものを避けるのがリスク回避である。 回避は影響・可能性を下げる対策とは異なり、活動そのものを中止する選択である。

基準：2026年度 / 2026-09-04

0026 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「管理策導入」を確認する。次の選択「リスク無視。」が不適切である理由として、最も直接的な説明はどれか。

ア. 管理策を導入して発生可能性や影響を下げるのはリスク低減である。
イ. リスク管理を放棄しているわけではない。
ウ. 対象業務をやめていないため回避ではない。
エ. 何も対策せず受容する対応ではない。

答え・解説 正答：イ

ア：この説明は元の論点では「リスク低減（リスクコントロール）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「リスク回避。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「リスク保有だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「管理策導入」について、誤答肢のどこが不適切かを説明できるかを確認する。リスク管理を放棄しているわけではない。 技術的・人的・物理的な管理策を組み合わせてリスクレベルを下げる。

基準：2026年度 / 2026-09-04

0027 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」の演習で「脆弱性診断。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. リスク特定はアセスメント工程である。
イ. 保険により経済的損失の一部を第三者と分担するためリスク共有に該当する。
ウ. 脆弱性診断は評価・対策手段である。
エ. 活動そのものをやめる対応ではない。

答え・解説 正答：ウ

ア：この説明は元の論点では「リスク特定。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「リスク共有（移転）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「リスク回避。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「保険・委託」について、誤答肢のどこが不適切かを説明できるかを確認する。脆弱性診断は評価・対策手段である。 保険へ移しても事故自体の発生を防ぐわけではないため、低減策との併用が必要である。

基準：2026年度 / 2026-09-04

0028 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

「受容」に関する理解を確認する。「リスク特定。」という判断の問題点を説明しているものはどれか。

ア. 活動を停止していないため回避ではない。
イ. 第三者へ移していない。
ウ. 基準内の残留リスクを認識して受け入れることをリスク保有という。
エ. 特定は対応ではなく評価前段階である。

答え・解説 正答：エ

ア：この説明は元の論点では「リスク回避。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「リスク移転だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「リスク保有。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「リスクアセスメント・リスク対応」の「受容」について、誤答肢のどこが不適切かを説明できるかを確認する。特定は対応ではなく評価前段階である。 リスク保有は『何もしない』ではなく、根拠を持って受容を決定し監視することが重要である。

基準：2026年度 / 2026-09-04

0029 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」の演習で「残留リスク。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. 対策後にも残るリスクを残留リスクという。
イ. 固有リスクは対策前のリスクを指す文脈で用いられる。
ウ. 実務上すべてのリスクをゼロにすることは困難である。
エ. 一般的な正式用語ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「固有リスクだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ゼロリスク。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「バックアップリスク。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「対策後リスク」について、結論だけでなく正答理由を説明できるかを確認する。対策後にも残るリスクを残留リスクという。 残留リスクが受容可能かを再評価し、必要なら追加対策を行う。

基準：2026年度 / 2026-09-04

0030 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

「リスク所有者を理解する」ために、「DNS管理者だけ。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 攻撃者はリスク管理責任者ではない。
イ. DNS担当者が必ず全リスク所有者になるわけではない。
ウ. リスク所有者は対象リスクに対する説明責任と権限を持つ主体である。
エ. 認証局は証明書を発行・管理する組織である。

答え・解説 正答：イ

ア：この説明は元の論点では「攻撃者。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「リスク所有者。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「認証局だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「リスクアセスメント・リスク対応」の「責任主体」について、誤答肢のどこが不適切かを説明できるかを確認する。DNS担当者が必ず全リスク所有者になるわけではない。 リスク対応の実効性を高めるには責任者を明確にすることが重要である。

基準：2026年度 / 2026-09-04

0031 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：基礎

「共通鍵・公開鍵暗号」の「同一鍵」を確認する。次の選択「暗号化には公開鍵、復号には必ず別の秘密鍵を用いる。」が不適切である理由として、最も直接的な説明はどれか。

ア. 暗号化には鍵を用いる。
イ. 公開鍵は公開して利用することを前提とする。
ウ. 「暗号化には公開鍵、復号には必ず別の秘密鍵を用いる。」は公開鍵暗号の基本的な説明である。
エ. 共通鍵暗号では送信者と受信者が同じ秘密鍵を共有する。

答え・解説 正答：ウ

ア：この説明は元の論点では「鍵を使わずに暗号化する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「公開鍵だけを秘密に保管する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「暗号化と復号に同じ秘密鍵を用いる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「同一鍵」について、誤答肢のどこが不適切かを説明できるかを確認する。「暗号化には公開鍵、復号には必ず別の秘密鍵を用いる。」は公開鍵暗号の基本的な説明である。 共通鍵暗号は高速だが、相手ごとの鍵配送・管理が課題となる。

基準：2026年度 / 2026-09-04

0032 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：標準

「共通鍵・公開鍵暗号」の演習で「全利用者が同じ秘密鍵を共有する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 秘密鍵を安全でない方法で配布する必要はない。
イ. 公開鍵は公開して使える。
ウ. 公開鍵暗号では数学的に関連する公開鍵と秘密鍵の対を用いる。
エ. 全員で同一秘密鍵を共有する方式ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「暗号鍵をネットワークへ平文で配布することを前提とする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「公開鍵も秘密鍵も必ず非公開にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「公開鍵と秘密鍵の対を用い、一方の鍵で行った処理を対応する他方の鍵で検証・復号する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「共通鍵・公開鍵暗号」の「鍵対」について、誤答肢のどこが不適切かを説明できるかを確認する。全員で同一秘密鍵を共有する方式ではない。 公開鍵暗号は鍵配送問題の緩和や電子署名に利用される。

基準：2026年度 / 2026-09-04

0033 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：基礎

「処理速度」に関する理解を確認する。「共通鍵暗号方式。」という結論を支持する説明として最も適切なものはどれか。

ア. 共通鍵暗号は公開鍵暗号より計算負荷が小さく、大量データの暗号化に向く。
イ. 公開鍵暗号は一般に処理負荷が高い。
ウ. 電子署名は暗号化そのものが主目的ではない。
エ. ハッシュは一方向関数で復号できない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「公開鍵暗号方式だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「電子署名だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ハッシュ関数だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「処理速度」について、結論だけでなく正答理由を説明できるかを確認する。共通鍵暗号は公開鍵暗号より計算負荷が小さく、大量データの暗号化に向く。 実際の通信では公開鍵暗号で鍵を安全に共有し、共通鍵暗号で本文を処理することが多い。

基準：2026年度 / 2026-09-04

0034 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：標準

「共通鍵・公開鍵暗号」を復習している。「公開鍵暗号では認証ができないため。」が正答にならない理由として最も適切なものはどれか。

ア. 共通鍵暗号はデータ暗号化に適している。
イ. 公開鍵暗号やPKIは認証にも利用される。
ウ. ハイブリッド暗号は鍵共有の利便性と大量データ処理の高速性を両立する。
エ. 遅くすることが目的ではない。

答え・解説 正答：イ

ア：この説明は元の論点では「共通鍵暗号ではデータを暗号化できないため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「公開鍵暗号で安全に共通鍵を共有し、実データは高速な共通鍵暗号で処理するため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「全データを二重に暗号化して必ず処理を遅くするため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「鍵共有」について、誤答肢のどこが不適切かを説明できるかを確認する。公開鍵暗号やPKIは認証にも利用される。 現代のセキュア通信では複数の暗号技術を役割分担させる。

基準：2026年度 / 2026-09-04

0035 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：応用

「AESの位置づけを理解する」ために、「ハッシュ関数そのものである。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 証明書形式でもない。
イ. AESはAdvanced Encryption Standardで、共通鍵ブロック暗号として広く利用される。
ウ. ハッシュ関数ではない。
エ. 公開鍵暗号ではない。

答え・解説 正答：ウ

ア：この説明は元の論点では「電子証明書の形式である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「代表的な共通鍵ブロック暗号方式である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「代表的な公開鍵暗号方式である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「ブロック暗号」について、誤答肢のどこが不適切かを説明できるかを確認する。ハッシュ関数ではない。 暗号方式の分類ではAESとRSAを混同しないことが重要である。

基準：2026年度 / 2026-09-04

0036 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：標準

「共通鍵・公開鍵暗号」の「公開鍵暗号」を確認する。次の選択「データ圧縮専用の方式である。」が不適切である理由として、最も直接的な説明はどれか。

ア. AESなどの共通鍵ブロック暗号とは異なる。
イ. DNS情報ではない。
ウ. RSAは公開鍵暗号方式として暗号化や電子署名に利用される。
エ. 圧縮方式ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「共通鍵ブロック暗号だけに使われる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「DNSレコードの一種である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「公開鍵暗号や電子署名で利用される代表的な方式である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「共通鍵・公開鍵暗号」の「公開鍵暗号」について、誤答肢のどこが不適切かを説明できるかを確認する。圧縮方式ではない。 公開鍵暗号では鍵長や安全性、用途に応じた方式選択が必要である。

基準：2026年度 / 2026-09-04

0037 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：基礎

「共通鍵・公開鍵暗号」を復習している。「所有者以外へ漏えいしないよう厳重に保護する。」と判断できる理由として最も適切なものはどれか。

ア. 秘密鍵が漏えいすると復号やなりすましに悪用されるため厳重な保護が必要である。
イ. 公開するのは公開鍵である。
ウ. 利用者ごとに適切に管理すべきである。
エ. 平文で無制限に複製するのは危険である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「公開Webページへ掲載する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「全社員で同じ秘密鍵を共有する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「バックアップを含め平文でどこにでもコピーする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「秘密鍵保護」について、結論だけでなく正答理由を説明できるかを確認する。秘密鍵が漏えいすると復号やなりすましに悪用されるため厳重な保護が必要である。 暗号の安全性はアルゴリズムだけでなく鍵の生成・保管・更新・廃棄にも依存する。

基準：2026年度 / 2026-09-04

0038 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：標準

「鍵更新」に関する理解を確認する。「ログを全て削除する。」という判断の問題点を説明しているものはどれか。

ア. 鍵の危殆化時は利用停止・交換し、影響分析を行う必要がある。
イ. ログ削除は調査を妨げる。
ウ. 漏えい鍵の継続利用は危険である。
エ. 鍵対の安全性が失われている可能性がある。

答え・解説 正答：イ

ア：この説明は元の論点では「当該鍵を失効・交換し、必要に応じて影響範囲を調査する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「そのまま永久に使い続ける。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「公開鍵だけを削除して秘密鍵を使い続ける。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「鍵更新」について、誤答肢のどこが不適切かを説明できるかを確認する。ログ削除は調査を妨げる。 鍵管理では有効期間、ローテーション、失効手続を事前に定める。

基準：2026年度 / 2026-09-04

0039 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：応用

「共通鍵・公開鍵暗号」を復習している。「データを必ず可逆圧縮するため。」が正答にならない理由として最も適切なものはどれか。

ア. 公開鍵と秘密鍵を変換する仕組みではない。
イ. 暗号利用モードは複数ブロックをどのように連携して暗号化するかを定める。
ウ. 圧縮方式ではない。
エ. 鍵は必要である。

答え・解説 正答：ウ

ア：この説明は元の論点では「公開鍵を秘密鍵へ変換するため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ブロックごとの処理方法を定め、同一平文パターンがそのまま暗号文へ現れるなどの弱点を避けるため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「暗号鍵を完全に不要にするため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「共通鍵・公開鍵暗号」の「同一平文パターン」について、誤答肢のどこが不適切かを説明できるかを確認する。圧縮方式ではない。 アルゴリズムだけでなく安全なモードや初期値の利用も重要である。

基準：2026年度 / 2026-09-04

0040 暗号・認証 > 共通鍵・公開鍵暗号 ｜ 難易度：標準

「ストレージ暗号化の目的を理解する」ために、「CPU性能を向上させる。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. マルウェア感染防止とは別対策である。
イ. ネットワークDoS対策ではない。
ウ. ストレージ暗号化は保存データの機密性を守る対策である。
エ. 性能向上が目的ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「マルウェア感染を完全に防ぐ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「WebサイトへのDDoS攻撃を防ぐ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「PCや記憶媒体を紛失・盗難された場合でも、保存データを読み取られにくくする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「共通鍵・公開鍵暗号」の「紛失対策」について、誤答肢のどこが不適切かを説明できるかを確認する。性能向上が目的ではない。 保存時暗号化では鍵の管理と端末認証も重要となる。

基準：2026年度 / 2026-09-04

0041 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：基礎

「ハッシュ・電子署名・証明書」の「一方向性」を確認する。次の判断「任意長の入力から固定長の値を生成し、元データへ戻すことが困難である。」が適切である根拠として、最も直接的な説明はどれか。

ア. ハッシュ関数は一方向性を持ち、固定長のダイジェストを生成する。
イ. 復号可能な暗号とは異なる。
ウ. 同じ入力には同じハッシュ値を返す。
エ. 通常のハッシュ計算には秘密鍵を必要としない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「出力から必ず元データを完全復元できる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「同じ入力でも毎回必ず異なる値を返す。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「暗号鍵がなければ計算できない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「一方向性」について、結論だけでなく正答理由を説明できるかを確認する。ハッシュ関数は一方向性を持ち、固定長のダイジェストを生成する。 完全性確認やパスワード保存、電子署名などで利用される。

基準：2026年度 / 2026-09-04

0042 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：標準

「ハッシュ・電子署名・証明書」の演習で「復号。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. ネットワーク経路選択である。
イ. 復号は暗号文から平文を得る処理である。
ウ. 異なる入力が同じダイジェストになることをハッシュ衝突という。
エ. 認可は権限を与える処理である。

答え・解説 正答：イ

ア：この説明は元の論点では「ルーティング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「衝突。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「認可。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「ハッシュ衝突」について、誤答肢のどこが不適切かを説明できるかを確認する。復号は暗号文から平文を得る処理である。 安全なハッシュ関数には衝突を現実的に見つけにくい性質が求められる。

基準：2026年度 / 2026-09-04

0043 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：基礎

「ハッシュ方式」に関する理解を確認する。「共通鍵暗号方式である。」という判断の問題点を説明しているものはどれか。

ア. 失効確認にはCRLやOCSPが使われる。
イ. 認証局は組織・主体である。
ウ. AESなどとは異なる。
エ. SHA-256はハッシュ関数で、256ビットのハッシュ値を生成する。

答え・解説 正答：ウ

ア：この説明は元の論点では「公開鍵証明書の失効通知方式である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「認証局そのものである。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「SHA-2系列の暗号学的ハッシュ関数である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「ハッシュ方式」について、誤答肢のどこが不適切かを説明できるかを確認する。AESなどとは異なる。 用途に応じて現在安全性が認められているハッシュ方式を選択する。

基準：2026年度 / 2026-09-04

0044 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：標準

「ハッシュ・電子署名・証明書」を復習している。「データの機密性だけ。」が正答にならない理由として最も適切なものはどれか。

ア. 可用性対策ではない。
イ. 圧縮とも無関係である。
ウ. 電子署名はハッシュと公開鍵暗号等を用いて完全性と署名者の真正性を確認する。
エ. 署名そのものは内容の秘匿を主目的としない。

答え・解説 正答：エ

ア：この説明は元の論点では「サーバの可用性だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「データ圧縮率だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「署名後にデータが改ざんされていないことと、署名者が対応する秘密鍵の保有者であること。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「完全性・真正性」について、誤答肢のどこが不適切かを説明できるかを確認する。署名そのものは内容の秘匿を主目的としない。 電子署名は否認防止にも役立つ。

基準：2026年度 / 2026-09-04

0045 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：応用

「署名生成・検証の鍵を理解する」ために、「署名者の秘密鍵。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. 署名者は自身だけが保有する秘密鍵を使って署名を生成する。
イ. 公開鍵は検証側が利用する。
ウ. 受信者の秘密鍵では署名者本人を証明できない。
エ. 認証局の公開鍵は証明書検証などに使う。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「署名者の公開鍵。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「受信者の秘密鍵。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「認証局の公開鍵だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「秘密鍵署名」について、結論だけでなく正答理由を説明できるかを確認する。署名者は自身だけが保有する秘密鍵を使って署名を生成する。 秘密鍵を安全に保護することが署名の信頼性に直結する。

基準：2026年度 / 2026-09-04

0046 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：標準

「ハッシュ・電子署名・証明書」の「公開鍵検証」を確認する。次の選択「受信者自身の秘密鍵だけ。」が不適切である理由として、最も直接的な説明はどれか。

ア. 電子署名の基本は公開鍵暗号の鍵対を利用する。
イ. 受信者の秘密鍵は署名検証には用いない。
ウ. 署名者の公開鍵で署名を検証する。
エ. 秘密鍵は署名者が保護すべきである。

答え・解説 正答：イ

ア：この説明は元の論点では「共通鍵暗号の共有鍵だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「署名者の公開鍵。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「署名者の秘密鍵。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「公開鍵検証」について、誤答肢のどこが不適切かを説明できるかを確認する。受信者の秘密鍵は署名検証には用いない。 公開鍵が本当に署名者のものかを証明書等で確認することも重要である。

基準：2026年度 / 2026-09-04

0047 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：基礎

「ハッシュ・電子署名・証明書」の演習で「Webコンテンツを圧縮する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. DHCPの役割である。
イ. 証明書は公開鍵の帰属を認証局が保証するために使われる。
ウ. 圧縮機能ではない。
エ. 秘密鍵を公開するものではない。

答え・解説 正答：ウ

ア：この説明は元の論点では「IPアドレスを自動割当てする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「公開鍵とその所有者の識別情報を結び付け、認証局の署名でその関係を証明する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「秘密鍵を全利用者へ配布する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「公開鍵の帰属」について、誤答肢のどこが不適切かを説明できるかを確認する。圧縮機能ではない。 PKIでは証明書を通じて公開鍵を信頼して利用できるようにする。

基準：2026年度 / 2026-09-04

0048 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：標準

「証明書失効」に関する理解を確認する。「ARPテーブル。」という判断の問題点を説明しているものはどれか。

ア. IPv4名前解決情報である。
イ. Web状態保持データである。
ウ. CRLはCertificate Revocation Listで、失効した証明書の一覧を提供する。
エ. IPとMACの対応表である。

答え・解説 正答：エ

ア：この説明は元の論点では「DNS Aレコード。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「HTTP cookie。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「CRL。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「証明書失効」について、誤答肢のどこが不適切かを説明できるかを確認する。IPとMACの対応表である。 証明書は有効期限内でも危殆化時には失効確認が必要である。

基準：2026年度 / 2026-09-04

0049 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：応用

「ハッシュ・電子署名・証明書」の演習で「OCSP。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. OCSPは証明書の失効状態をオンラインで確認するためのプロトコルである。
イ. メール送信用である。
ウ. ネットワーク管理用である。
エ. ファイル転送用である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「SMTP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「SNMP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「FTP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「オンライン失効確認」について、結論だけでなく正答理由を説明できるかを確認する。OCSPは証明書の失効状態をオンラインで確認するためのプロトコルである。 CRLとOCSPはいずれも証明書失効確認に関係するが、利用方式が異なる。

基準：2026年度 / 2026-09-04

0050 暗号・認証 > ハッシュ・電子署名・証明書 ｜ 難易度：標準

「タイムスタンプを理解する」ために、「RAID。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. タイムスタンプは特定時刻にデータが存在したことと、その後の非改ざん性の確認に利用される。
イ. ストレージ冗長化方式である。
ウ. IPアドレス変換技術である。
エ. IP設定配布プロトコルである。

答え・解説 正答：イ

ア：この説明は元の論点では「タイムスタンプ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「NAT。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「DHCP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ハッシュ・電子署名・証明書」の「時刻証明」について、誤答肢のどこが不適切かを説明できるかを確認する。ストレージ冗長化方式である。 電子署名とタイムスタンプを組み合わせることで長期的な証拠性を高められる。

基準：2026年度 / 2026-09-04

0051 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：基礎

「認証・PKI・多要素認証」の「Authentication/Authorization」を確認する。次の選択「どちらも暗号化だけを指す。」が不適切である理由として、最も直接的な説明はどれか。

ア. 説明が逆である。
イ. Authenticationは本人確認、Authorizationはアクセス権付与である。
ウ. 暗号化とは別概念である。
エ. 役割は異なる。

答え・解説 正答：ウ

ア：この説明は元の論点では「認証は権限付与だけを行い、認可は本人確認だけを行う。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「認証は利用者が誰かを確認し、認可はその利用者に何を許可するかを決める。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「認証と認可は完全に同じ意味である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「Authentication/Authorization」について、誤答肢のどこが不適切かを説明できるかを確認する。暗号化とは別概念である。 安全なシステムでは認証後に適切な認可を行う必要がある。

基準：2026年度 / 2026-09-04

0052 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：標準

「認証・PKI・多要素認証」の演習で「公開鍵暗号だけ。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 同じ要素を複数回使うだけとは異なる。
イ. 利用者を識別している。
ウ. パスワードは記憶要素、スマートフォンは所有要素で異なる要素を組み合わせている。
エ. 暗号方式の分類ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「同一要素だけの多段階認証。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「匿名認証。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「多要素認証。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「認証・PKI・多要素認証」の「異なる要素」について、誤答肢のどこが不適切かを説明できるかを確認する。暗号方式の分類ではない。 多要素認証では記憶・所有・生体など異なる要素を組み合わせる。

基準：2026年度 / 2026-09-04

0053 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：基礎

「知識・所有・生体」に関する理解を確認する。「指紋。」という結論を支持する説明として最も適切なものはどれか。

ア. 指紋は身体的特徴を利用する生体要素である。
イ. パスワードは記憶要素である。
ウ. ICカードは所有要素である。
エ. 秘密の質問も記憶要素に分類される。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「パスワード。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ICカード。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「秘密の質問の答え。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「知識・所有・生体」について、結論だけでなく正答理由を説明できるかを確認する。指紋は身体的特徴を利用する生体要素である。 多要素認証では異なるカテゴリの要素を組み合わせる。

基準：2026年度 / 2026-09-04

0054 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：標準

「認証・PKI・多要素認証」を復習している。「一度決めたパスワードを永久に変更しない。」が正答にならない理由として最も適切なものはどれか。

ア. 第三者へ公開すべきではない。
イ. 固定パスワードとは異なる。
ウ. OTPは毎回または一定時間ごとに変化し、再利用攻撃を難しくする。
エ. 利用者ごとに適切に生成される。

答え・解説 正答：イ

ア：この説明は元の論点では「公開Webページに表示して利用する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「一度限り又は短時間だけ有効な値を使い、盗聴された認証情報の再利用リスクを下げる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「全利用者が同じ値を共有する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「再利用防止」について、誤答肢のどこが不適切かを説明できるかを確認する。固定パスワードとは異なる。 OTPだけでもフィッシング等のリスクは残るため、認証方式全体の設計が必要である。

基準：2026年度 / 2026-09-04

0055 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：応用

「FIDOの特徴を理解する」ために、「利用者のパスワードを全サイトで同じ値に統一する。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 秘密鍵は端末側で保護される。
イ. メール送信を必須としない。
ウ. パスワード使い回しを推奨するものではない。
エ. FIDOは公開鍵暗号を利用し、認証器側の秘密鍵をサーバへ渡さずに認証できる。

答え・解説 正答：ウ

ア：この説明は元の論点では「秘密鍵をサーバへ平文で送信する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「認証時に必ずメール本文へパスワードを書く。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「端末側の秘密鍵を外部へ送らず、公開鍵暗号を利用してサーバへ認証する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「パスワードレス」について、誤答肢のどこが不適切かを説明できるかを確認する。パスワード使い回しを推奨するものではない。 フィッシング耐性の高いパスワードレス認証として利用される。

基準：2026年度 / 2026-09-04

0056 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：標準

「認証・PKI・多要素認証」の「本人拒否率」を確認する。次の選択「FAR（他人受入率）。」が不適切である理由として、最も直接的な説明はどれか。

ア. 平均故障間隔である。
イ. 有効期間や寿命を表す用語である。
ウ. FRRはFalse Rejection Rateで本人を誤って拒否する割合である。
エ. FARは他人を本人として誤受入れする割合である。

答え・解説 正答：エ

ア：この説明は元の論点では「MTBF。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「TTL。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「FRR（本人拒否率）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「認証・PKI・多要素認証」の「本人拒否率」について、誤答肢のどこが不適切かを説明できるかを確認する。FARは他人を本人として誤受入れする割合である。 閾値調整では一般にFARとFRRのトレードオフが生じる。

基準：2026年度 / 2026-09-04

0057 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：基礎

「認証・PKI・多要素認証」を復習している。「FAR（他人受入率）。」と判断できる理由として最も適切なものはどれか。

ア. FARはFalse Acceptance Rateで他人を誤受入れする割合である。
イ. FRRは本人を誤拒否する割合である。
ウ. 復旧時間目標である。
エ. CPU性能指標である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「FRR（本人拒否率）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「RTO。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「CPI。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「他人受入率」について、結論だけでなく正答理由を説明できるかを確認する。FARはFalse Acceptance Rateで他人を誤受入れする割合である。 セキュリティを厳しくするほどFARは下がりやすいが、FRRが上がる場合がある。

基準：2026年度 / 2026-09-04

0058 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：標準

「CA」に関する理解を確認する。「HTTP通信を圧縮する。」という判断の問題点を説明しているものはどれか。

ア. ルーティング機能ではない。
イ. 圧縮機能ではない。
ウ. CAは証明書の発行、更新、失効などを管理する信頼主体である。
エ. 秘密鍵公開は行わない。

答え・解説 正答：イ

ア：この説明は元の論点では「ルータの経路を計算する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「申請者の確認を行い、公開鍵と主体の関係を証明するデジタル証明書を発行・管理する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「全利用者の秘密鍵を公開する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「CA」について、誤答肢のどこが不適切かを説明できるかを確認する。圧縮機能ではない。 PKIの信頼はCAの適切な本人確認と秘密鍵管理に依存する。

基準：2026年度 / 2026-09-04

0059 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：応用

「認証・PKI・多要素認証」を復習している。「cookie。」が正答にならない理由として最も適切なものはどれか。

ア. ネットワーク設定情報である。
イ. ルート証明書は証明書チェーンの信頼の基点となる。
ウ. Web状態保持情報である。
エ. 秘密鍵は証明書ではなくサーバ側で保護される。

答え・解説 正答：ウ

ア：この説明は元の論点では「DHCPリース情報。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ルート証明書。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「サーバの秘密鍵。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「認証・PKI・多要素認証」の「トラストアンカー」について、誤答肢のどこが不適切かを説明できるかを確認する。Web状態保持情報である。 ルートCAから中間CA、サーバ証明書へ続く署名連鎖を検証して信頼性を確認する。

基準：2026年度 / 2026-09-04

0060 暗号・認証 > 認証・PKI・多要素認証 ｜ 難易度：標準

「SSOを理解する」ために、「CAPTCHAだけ。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. OTPは認証情報の一種でありSSOそのものではない。
イ. 負荷分散方式である。
ウ. SSOは一度の認証結果を複数サービスで利用する仕組みである。
エ. CAPTCHAは自動化されたアクセスか人間かの判定に使う。

答え・解説 正答：エ

ア：この説明は元の論点では「ワンタイムパスワードだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「DNSラウンドロビン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「シングルサインオン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「認証・PKI・多要素認証」の「シングルサインオン」について、誤答肢のどこが不適切かを説明できるかを確認する。CAPTCHAは自動化されたアクセスか人間かの判定に使う。 SSOは利便性を高める一方、認証基盤の保護やセッション管理が重要になる。

基準：2026年度 / 2026-09-04

0061 攻撃と技術的対策 > 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注入」を確認する。次の判断「SQLインジェクション。」が適切である根拠として、最も直接的な説明はどれか。

ア. SQLインジェクションは入力値を通じてSQL構文を不正に改変する攻撃である。
イ. XSSはブラウザ上でスクリプトを実行させる攻撃である。
ウ. DNS情報を偽装する攻撃である。
エ. サービス妨害攻撃である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「クロスサイトスクリプティング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「DNSキャッシュポイズニング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「DoS攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「SQL注入」について、結論だけでなく正答理由を説明できるかを確認する。SQLインジェクションは入力値を通じてSQL構文を不正に改変する攻撃である。 SQLインジェクション対策ではプレースホルダを用いたパラメータ化クエリなどが有効である。

基準：2026年度 / 2026-09-04

0062 攻撃と技術的対策 > 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」の演習で「データベースの全利用者へ管理者権限を与える。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. プレースホルダを使うと入力値をSQL構文として解釈させにくくできる。
イ. 最小権限の原則に反する。
ウ. 攻撃文字列をSQL構文へ混入させる危険な実装である。
エ. 情報漏えいの抑制には役立つ場合があるが根本対策ではない。

答え・解説 正答：イ

ア：この説明は元の論点では「SQL文と値を分離し、プレースホルダを用いたパラメータ化クエリを利用する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「入力値をそのままSQL文字列へ連結する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「エラーメッセージを詳しく表示するだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「プレースホルダ」について、誤答肢のどこが不適切かを説明できるかを確認する。最小権限の原則に反する。 入力検証と併せて、SQLを文字列連結しない実装が重要である。

基準：2026年度 / 2026-09-04

0063 攻撃と技術的対策 > Webアプリケーション攻撃 ｜ 難易度：基礎

「スクリプト注入」に関する理解を確認する。「パスワードリスト攻撃。」という判断の問題点を説明しているものはどれか。

ア. LAN内のARP情報を偽装する攻撃である。
イ. XSSはWebページへ悪意あるスクリプトを混入し、閲覧者のブラウザで実行させる。
ウ. 漏えい済み認証情報を使い回す攻撃である。
エ. CSRFは認証済み利用者のブラウザに意図しない要求を送らせる攻撃である。

答え・解説 正答：ウ

ア：この説明は元の論点では「ARPスプーフィング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「クロスサイトスクリプティング（XSS）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「CSRF。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「スクリプト注入」について、誤答肢のどこが不適切かを説明できるかを確認する。漏えい済み認証情報を使い回す攻撃である。 出力時のエスケープや適切なContent Security Policyなどが対策となる。

基準：2026年度 / 2026-09-04

0064 攻撃と技術的対策 > 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」を復習している。「管理者権限でブラウザを実行する。」が正答にならない理由として最も適切なものはどれか。

ア. 攻撃コードを実行させる原因となる。
イ. 認証情報漏えいリスクを高める。
ウ. 出力エスケープにより入力値を実行可能なHTMLやスクリプトとして解釈させにくくする。
エ. 被害を拡大する可能性がある。

答え・解説 正答：エ

ア：この説明は元の論点では「全入力をそのままHTMLとして解釈させる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「cookieへパスワードを平文保存する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「出力先の文脈に応じてHTML特殊文字などを適切にエスケープする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「Webアプリケーション攻撃」の「出力エスケープ」について、誤答肢のどこが不適切かを説明できるかを確認する。被害を拡大する可能性がある。 XSS対策では出力文脈に応じたエスケープが基本となる。

基準：2026年度 / 2026-09-04

0065 攻撃と技術的対策 > Webアプリケーション攻撃 ｜ 難易度：応用

「CSRFを理解する」ために、「クロスサイトリクエストフォージェリ（CSRF）。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. CSRFは認証済み利用者のブラウザに意図しないリクエストを送信させる。
イ. スクリプト注入そのものとは異なる。
ウ. DB問い合わせ構文を不正変更する攻撃である。
エ. 公開ポート調査である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「XSSだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「SQLインジェクション。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ポートスキャン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「意図しない要求」について、結論だけでなく正答理由を説明できるかを確認する。CSRFは認証済み利用者のブラウザに意図しないリクエストを送信させる。 CSRFトークンやSameSite属性などが対策となる。

基準：2026年度 / 2026-09-04

0066 攻撃と技術的対策 > 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「パス操作」を確認する。次の選択「クリックジャッキング。」が不適切である理由として、最も直接的な説明はどれか。

ア. DNS応答の真正性を確認する技術である。
イ. 透明な画面要素を重ねるなどして誤クリックを誘う攻撃である。
ウ. パス表現を悪用して想定外のファイルへアクセスする攻撃である。
エ. セッションIDの扱いを悪用する攻撃である。

答え・解説 正答：イ

ア：この説明は元の論点では「DNSSEC。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「ディレクトリトラバーサル。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「セッション固定。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「パス操作」について、誤答肢のどこが不適切かを説明できるかを確認する。透明な画面要素を重ねるなどして誤クリックを誘う攻撃である。 ファイル名の正規化、許可リスト、アクセス権制御などで対策する。

基準：2026年度 / 2026-09-04

0067 攻撃と技術的対策 > 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」の演習で「ARPキャッシュ更新。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 署名技術の問題に限定されない。
イ. 配信性能の問題である。
ウ. LANアドレス解決の動作である。
エ. シェルのメタ文字などを悪用して意図しないOSコマンドを実行させる攻撃である。

答え・解説 正答：ウ

ア：この説明は元の論点では「電子署名偽造だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「CDNキャッシュミス。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「OSコマンドインジェクション。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「コマンド注入」について、誤答肢のどこが不適切かを説明できるかを確認する。LANアドレス解決の動作である。 可能ならシェル呼出しを避け、固定APIを使い、入力を厳格に検証する。

基準：2026年度 / 2026-09-04

0068 攻撃と技術的対策 > Webアプリケーション攻撃 ｜ 難易度：標準

「透明UI」に関する理解を確認する。「ブルートフォース攻撃。」という判断の問題点を説明しているものはどれか。

ア. 自己拡散型マルウェアの感染である。
イ. 過去の認証データなどを再送する攻撃である。
ウ. クリックジャッキングは画面表示を欺いて意図しないクリックを誘導する。
エ. 認証候補を総当たりする攻撃である。

答え・解説 正答：エ

ア：この説明は元の論点では「ワーム感染。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「リプレイ攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「クリックジャッキング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「Webアプリケーション攻撃」の「透明UI」について、誤答肢のどこが不適切かを説明できるかを確認する。認証候補を総当たりする攻撃である。 frame-ancestorsやX-Frame-Optionsなどで埋込みを制限する対策がある。

基準：2026年度 / 2026-09-04

0069 攻撃と技術的対策 > 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」の演習で「HTTPSを利用し、cookieへSecureやHttpOnlyなど適切な属性を設定する。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. HTTPSと適切なcookie属性は盗聴やスクリプトからの取得リスク低減に役立つ。
イ. URLはログや参照元へ残る可能性がある。
ウ. 固定IDは他人のセッションへ容易に侵入できる。
エ. 長すぎる有効期間は盗用時の危険を増やす。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「セッションIDをURLへ常に平文表示する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「全利用者で同じ固定セッションIDを使う。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「セッション有効期限を無期限にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「Secure/HttpOnly」について、結論だけでなく正答理由を説明できるかを確認する。HTTPSと適切なcookie属性は盗聴やスクリプトからの取得リスク低減に役立つ。 セッションIDは十分なランダム性を持たせ、ログイン時の再生成や期限管理も重要である。

基準：2026年度 / 2026-09-04

0070 攻撃と技術的対策 > Webアプリケーション攻撃 ｜ 難易度：標準

「WAFの役割を理解する」ために、「DHCPサーバ。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. ストレージ制御を行う。
イ. IP設定配布を行う。
ウ. WAFはHTTP/HTTPS通信を解析しWebアプリ向け攻撃を検知・遮断する。
エ. UPSは停電対策である。

答え・解説 正答：イ

ア：この説明は元の論点では「RAIDコントローラ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「WAF。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「UPS。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「Webアプリケーション攻撃」の「Web防御」について、誤答肢のどこが不適切かを説明できるかを確認する。IP設定配布を行う。 WAFは有効な補助対策だが、脆弱なアプリケーション実装そのものの修正も必要である。

基準：2026年度 / 2026-09-04

0071 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：基礎

「ネットワーク・エンドポイント攻撃」の「サービス妨害」を確認する。次の選択「データ圧縮。」が不適切である理由として、最も直接的な説明はどれか。

ア. DB設計技法である。
イ. DoSはサービス提供を妨害して可用性を損なう攻撃である。
ウ. データ量削減処理である。
エ. 真正性・完全性確認技術である。

答え・解説 正答：ウ

ア：この説明は元の論点では「正規化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「DoS攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「電子署名。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「サービス妨害」について、誤答肢のどこが不適切かを説明できるかを確認する。データ量削減処理である。 DoS対策ではレート制限、冗長化、フィルタリングなどを組み合わせる。

基準：2026年度 / 2026-09-04

0072 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：標準

「ネットワーク・エンドポイント攻撃」の演習で「SQLの副問合せ。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 通常アクセスではない。
イ. 公開鍵基盤である。
ウ. DDoSは多数の送信元から分散してサービス妨害を行う。
エ. DB検索機能である。

答え・解説 正答：エ

ア：この説明は元の論点では「単一端末だけからの通常アクセス。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「PKI。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「DDoS攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「分散攻撃」について、誤答肢のどこが不適切かを説明できるかを確認する。DB検索機能である。 ボットネットがDDoSの送信基盤として悪用されることがある。

基準：2026年度 / 2026-09-04

0073 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：基礎

「送信元偽装」に関する理解を確認する。「IPスプーフィング。」という結論を支持する説明として最も適切なものはどれか。

ア. 送信元IPアドレスを偽ることをIPスプーフィングという。
イ. DNSデータの署名検証技術である。
ウ. 一方向変換技術である。
エ. 復旧対策である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「DNSSEC。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ハッシュ化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「バックアップ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「送信元偽装」について、結論だけでなく正答理由を説明できるかを確認する。送信元IPアドレスを偽ることをIPスプーフィングという。 入口・出口フィルタリングなどが偽装パケット対策として用いられる。

基準：2026年度 / 2026-09-04

0074 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：標準

「ネットワーク・エンドポイント攻撃」を復習している。「ラウンドロビン。」が正答にならない理由として最も適切なものはどれか。

ア. 偽DNS情報をキャッシュさせることで名前解決を改ざんする攻撃である。
イ. 負荷分散方式である。
ウ. 正常なARP処理ではない。
エ. ファイル転送方式である。

答え・解説 正答：イ

ア：この説明は元の論点では「DNSキャッシュポイズニング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「ARP正常更新。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「FTPパッシブモード。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「偽DNS応答」について、誤答肢のどこが不適切かを説明できるかを確認する。負荷分散方式である。 DNSSECはDNSデータの真正性確認に利用され、こうした改ざん対策に関係する。

基準：2026年度 / 2026-09-04

0075 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：応用

「中間者攻撃を理解する」ために、「ランサムウェア。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. DB入力を悪用する攻撃である。
イ. MITMは通信経路上で双方を欺き、盗聴や改ざんを行う。
ウ. データ暗号化等で身代金を要求するマルウェアである。
エ. パスワード候補を辞書から試す攻撃である。

答え・解説 正答：ウ

ア：この説明は元の論点では「SQLインジェクション。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「中間者攻撃（MITM）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「辞書攻撃。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「MITM」について、誤答肢のどこが不適切かを説明できるかを確認する。データ暗号化等で身代金を要求するマルウェアである。 TLS証明書の適切な検証はMITM対策として重要である。

基準：2026年度 / 2026-09-04

0076 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：標準

「ネットワーク・エンドポイント攻撃」の「パケットフィルタリング」を確認する。次の選択「DBビュー。」が不適切である理由として、最も直接的な説明はどれか。

ア. データ要約を生成する関数である。
イ. プログラム翻訳ツールである。
ウ. ファイアウォールは通信ルールに基づいて境界でトラフィックを制御する。
エ. 仮想表である。

答え・解説 正答：エ

ア：この説明は元の論点では「ハッシュ関数。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「コンパイラ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ファイアウォール。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「パケットフィルタリング」について、誤答肢のどこが不適切かを説明できるかを確認する。仮想表である。 境界防御だけでなく内部セグメント分離にもファイアウォールを活用できる。

基準：2026年度 / 2026-09-04

0077 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：基礎

「ネットワーク・エンドポイント攻撃」を復習している。「IDSは侵入を検知・通知し、IPSは検知に加えて通信遮断などの防止動作を行う。」と判断できる理由として最も適切なものはどれか。

ア. IDSは検知、IPSはインラインで遮断まで行う点が代表的な違いである。
イ. 役割は異なる。
ウ. 暗号・圧縮専用装置ではない。
エ. IPSも通信を監視して攻撃判定する。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「IDSとIPSは完全に同じで、どちらも検知しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「IDSは暗号化専用、IPSは圧縮専用である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「IPSはネットワーク監視を一切行わない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「検知と防止」について、結論だけでなく正答理由を説明できるかを確認する。IDSは検知、IPSはインラインで遮断まで行う点が代表的な違いである。 誤検知時の影響も考慮し、配置やルールを調整する必要がある。

基準：2026年度 / 2026-09-04

0078 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：標準

「端末監視」に関する理解を確認する。「DNSサーバ。」という判断の問題点を説明しているものはどれか。

ア. ストレージ冗長化方式である。
イ. 名前解決サーバである。
ウ. EDRはEndpoint Detection and Responseで、端末上の活動を監視し検知・対応を支援する。
エ. 負荷分散装置である。

答え・解説 正答：イ

ア：この説明は元の論点では「RAID5。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「EDR。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ロードバランサ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「端末監視」について、誤答肢のどこが不適切かを説明できるかを確認する。名前解決サーバである。 EDRは従来型マルウェア対策だけでは捉えにくい侵害後の挙動分析にも有効である。

基準：2026年度 / 2026-09-04

0079 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：応用

「ネットワーク・エンドポイント攻撃」を復習している。「修正プログラムを永久に適用しない。」が正答にならない理由として最も適切なものはどれか。

ア. 認証強度を下げる。
イ. 調査や監視を困難にする。
ウ. 未修正状態が長く続き攻撃リスクが増える。
エ. 既知脆弱性には提供された修正プログラムを適切に適用することが基本対策である。

答え・解説 正答：ウ

ア：この説明は元の論点では「管理者パスワードを共有する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「全ログを削除する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「影響確認の上でセキュリティパッチを適切に適用する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「修正プログラム」について、誤答肢のどこが不適切かを説明できるかを確認する。未修正状態が長く続き攻撃リスクが増える。 資産・脆弱性情報を把握し、優先度を付けてパッチ管理する。

基準：2026年度 / 2026-09-04

0080 攻撃と技術的対策 > ネットワーク・エンドポイント攻撃 ｜ 難易度：標準

「DMZを理解する」ために、「VLANを使わない単一LAN。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 自端末を示すアドレス概念である。
イ. 仮想記憶領域である。
ウ. DMZは外部公開サーバを内部ネットワークから分離して配置する領域である。
エ. 分離を行わない構成は侵害時の内部到達リスクが高まる。

答え・解説 正答：エ

ア：この説明は元の論点では「ループバック。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「スワップ領域。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「DMZ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ネットワーク・エンドポイント攻撃」の「公開サーバ分離」について、誤答肢のどこが不適切かを説明できるかを確認する。分離を行わない構成は侵害時の内部到達リスクが高まる。 DMZとファイアウォールルールを組み合わせ、外部・DMZ・内部間の通信を最小限に制御する。

基準：2026年度 / 2026-09-04

0081 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：基礎

「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「自己増殖」を確認する。次の判断「ワーム。」が適切である根拠として、最も直接的な説明はどれか。

ア. ワームは独立して自己増殖しネットワーク等へ拡散できる。
イ. マクロウイルスは文書のマクロ機能などへ感染する。
ウ. キーロガーは入力情報を記録する。
エ. 証明書でありマルウェアではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「マクロウイルスだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「キーロガー。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ルート証明書。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「自己増殖」について、結論だけでなく正答理由を説明できるかを確認する。ワームは独立して自己増殖しネットワーク等へ拡散できる。 マルウェアは感染・拡散方法や目的に応じて分類される。

基準：2026年度 / 2026-09-04

0082 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：標準

「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の演習で「デジタル証明書。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. ネットワーク管理通知である。
イ. 証明書である。
ウ. トロイの木馬は正規ソフトを装って実行させるなど、利用者を欺いて侵入する。
エ. 自己増殖の有無など性質が異なる。

答え・解説 正答：イ

ア：この説明は元の論点では「SNMP Trap。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「トロイの木馬。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ワームだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「偽装プログラム」について、誤答肢のどこが不適切かを説明できるかを確認する。証明書である。 信頼できない配布元からのソフト実行を避けることが対策の一つとなる。

基準：2026年度 / 2026-09-04

0083 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：基礎

「身代金要求」に関する理解を確認する。「ルートキット。」という判断の問題点を説明しているものはどれか。

ア. ネットワークサービスでありマルウェアではない。
イ. ランサムウェアはデータ利用を妨害し身代金を要求する。
ウ. 存在隠蔽や権限維持に使われることがある。
エ. 情報収集を主目的とするマルウェアの総称である。

答え・解説 正答：ウ

ア：この説明は元の論点では「DNSサーバ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ランサムウェア。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「スパイウェアだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「身代金要求」について、誤答肢のどこが不適切かを説明できるかを確認する。存在隠蔽や権限維持に使われることがある。 暗号化だけでなく情報窃取と公開脅迫を組み合わせる二重脅迫もある。

基準：2026年度 / 2026-09-04

0084 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：標準

「マルウェア・ランサムウェア・ソーシャルエンジニアリング」を復習している。「バックアップを一切取得しない。」が正答にならない理由として最も適切なものはどれか。

ア. 本番侵害時にバックアップまで暗号化される危険がある。
イ. 復元できることを定期検証する必要がある。
ウ. 分離されたイミュータブルなバックアップ等はランサムウェアによる同時破壊を防ぎやすい。
エ. 復旧手段を失う。

答え・解説 正答：エ

ア：この説明は元の論点では「本番サーバと同じ資格情報で常時書換え可能な一つのバックアップだけを置く。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「毎回バックアップの復元確認を省略する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「本番環境から分離され、攻撃者が容易に削除・暗号化できないバックアップを複数世代保持する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「バックアップ」について、誤答肢のどこが不適切かを説明できるかを確認する。復旧手段を失う。 3-2-1ルールなどを参考に、複数媒体・別場所・オフライン等を組み合わせる。

基準：2026年度 / 2026-09-04

0085 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：応用

「フィッシングを理解する」ために、「フィッシング。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. フィッシングは信頼できる組織を装い認証情報や金銭を詐取する。
イ. サービス妨害攻撃である。
ウ. メモリ破壊を利用する攻撃である。
エ. DB設計手法である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「DoS。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「バッファオーバーフロー。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「SQL正規化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「偽サイト」について、結論だけでなく正答理由を説明できるかを確認する。フィッシングは信頼できる組織を装い認証情報や金銭を詐取する。 送信元だけを信用せずURLや証明書、正規アプリからのアクセスを確認することが重要である。

基準：2026年度 / 2026-09-04

0086 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：標準

「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「SMS詐欺」を確認する。次の選択「パッチ適用。」が不適切である理由として、最も直接的な説明はどれか。

ア. SMSを利用するフィッシングをスミッシングという。
イ. 防御策である。
ウ. 電話音声を利用するフィッシングをビッシングという。
エ. 公開サービス調査である。

答え・解説 正答：イ

ア：この説明は元の論点では「スミッシング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「ビッシング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ポートスキャン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「SMS詐欺」について、誤答肢のどこが不適切かを説明できるかを確認する。防御策である。 通信手段がメール以外でもソーシャルエンジニアリング攻撃は成立する。

基準：2026年度 / 2026-09-04

0087 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：基礎

「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の演習で「ブルートフォース攻撃だけ。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. DNS保護技術である。
イ. BECは業務上の信頼関係を悪用し送金や情報提供を要求する詐欺である。
ウ. 認証候補の総当たり攻撃である。
エ. DB攻撃である。

答え・解説 正答：ウ

ア：この説明は元の論点では「DNSSEC。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ビジネスメール詐欺（BEC）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「SQLインジェクション。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「経営者なりすまし」について、誤答肢のどこが不適切かを説明できるかを確認する。認証候補の総当たり攻撃である。 高額送金ではメールだけでなく別経路で本人確認する業務手続が有効である。

基準：2026年度 / 2026-09-04

0088 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：標準

「APT」に関する理解を確認する。「データ圧縮。」という判断の問題点を説明しているものはどれか。

ア. 攻撃ではない。
イ. 正常運用である。
ウ. APTはAdvanced Persistent Threatで、特定標的へ持続的・組織的に攻撃する。
エ. 圧縮処理である。

答え・解説 正答：エ

ア：この説明は元の論点では「単純な偶発故障。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「通常のソフト更新。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「APT。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「APT」について、誤答肢のどこが不適切かを説明できるかを確認する。圧縮処理である。 標的型攻撃ではメール、脆弱性悪用、認証情報窃取など複数手法が連鎖することがある。

基準：2026年度 / 2026-09-04

0089 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：応用

「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の演習で「ビヘイビア法（振る舞い検知）。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. 振る舞い検知は実行時の不審な動作パターンから未知脅威も検出できる可能性がある。
イ. 未知マルウェアには一致パターンが存在しない場合がある。
ウ. 名前解決である。
エ. ストレージ冗長化方式である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「既知パターンだけに完全依存する方式。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「DNS正引き。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「RAID1。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「振る舞い検知」について、結論だけでなく正答理由を説明できるかを確認する。振る舞い検知は実行時の不審な動作パターンから未知脅威も検出できる可能性がある。 パターンマッチング、ヒューリスティック、振る舞い検知を組み合わせて検出力を高める。

基準：2026年度 / 2026-09-04

0090 攻撃と技術的対策 > マルウェア・ランサムウェア・ソーシャルエンジニアリング ｜ 難易度：標準

「ソーシャルエンジニアリング対策を理解する」ために、「緊急と言われたので直ちに伝える。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 被害を拡大する。
イ. 認証情報漏えいにつながる。
ウ. ソーシャルエンジニアリングでは緊急性や権威を装って判断を急がせるため、別経路で本人確認する。
エ. 確認なしの送信は危険である。

答え・解説 正答：イ

ア：この説明は元の論点では「同僚のパスワードもまとめて伝える。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「パスワードを伝えず、社内で定めた正規の連絡先へ自分から確認する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「本人確認せず秘密情報をメールでも送る。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「マルウェア・ランサムウェア・ソーシャルエンジニアリング」の「本人確認」について、誤答肢のどこが不適切かを説明できるかを確認する。認証情報漏えいにつながる。 技術対策だけでなく教育、手続、報告ルートの整備が人的攻撃への重要な対策となる。

基準：2026年度 / 2026-09-04

0091 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：基礎

「アクセス制御・ID管理」の「権限最小化」を確認する。次の選択「業務上不要な共有フォルダも全て閲覧可能にする。」が不適切である理由として、最も直接的な説明はどれか。

ア. 最小権限では業務に必要な範囲へ権限を限定する。
イ. 過剰権限となり、侵害時の影響を大きくする。
ウ. need-to-knowの考え方に反する。
エ. 役割変更時には権限の見直しが必要である。

答え・解説 正答：ウ

ア：この説明は元の論点では「利用者の業務遂行に必要な最小限の権限だけを付与する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「全利用者へ管理者権限を付与する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「一度付与した権限は異動や退職後も変更しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「権限最小化」について、誤答肢のどこが不適切かを説明できるかを確認する。need-to-knowの考え方に反する。 アクセス制御では、必要な主体に必要な資源への必要な操作だけを認めることが基本である。

基準：2026年度 / 2026-09-04

0092 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：標準

「アクセス制御・ID管理」の演習で「フェイルオーバ。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 職務分掌は重要処理を複数の役割へ分離し、不正や誤りを抑制する。
イ. SSOは一度の認証で複数サービスを利用する仕組みである。
ウ. 情報量削減技術である。
エ. 障害時の切替えである。

答え・解説 正答：エ

ア：この説明は元の論点では「職務分掌。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「シングルサインオン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「データ圧縮。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「アクセス制御・ID管理」の「権限分離」について、誤答肢のどこが不適切かを説明できるかを確認する。障害時の切替えである。 相反する権限を同一人物へ集中させないことは内部不正対策として有効である。

基準：2026年度 / 2026-09-04

0093 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：基礎

「役割ベース」に関する理解を確認する。「RBAC。」という結論を支持する説明として最も適切なものはどれか。

ア. RBACはRole-Based Access Controlで、役割を介して権限を管理する。
イ. DACは所有者などが裁量的に権限設定する方式である。
ウ. アクセス制御モデルではない。
エ. ABACは属性に基づいて判断する方式である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「DACだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ハッシュ化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ABACだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「役割ベース」について、結論だけでなく正答理由を説明できるかを確認する。RBACはRole-Based Access Controlで、役割を介して権限を管理する。 組織の職務と権限を対応付けやすいため、大規模なID管理で利用される。

基準：2026年度 / 2026-09-04

0094 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：標準

「アクセス制御・ID管理」を復習している。「RAID1。」が正答にならない理由として最も適切なものはどれか。

ア. RBACは役割を中心に権限を管理する。
イ. ストレージのミラーリング方式である。
ウ. キューの処理方式である。
エ. ABACはAttribute-Based Access Controlで、主体・資源・環境などの属性に基づいて認可する。

答え・解説 正答：イ

ア：この説明は元の論点では「RBACだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「FIFO。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ABAC。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「属性ベース」について、誤答肢のどこが不適切かを説明できるかを確認する。ストレージのミラーリング方式である。 属性を組み合わせることで、状況に応じた細かなアクセス制御を実現できる。

基準：2026年度 / 2026-09-04

0095 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：応用

「IDライフサイクル管理を理解する」ために、「退職後もアカウントを無期限に有効にする。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 不要アカウントを残すと不正利用の入口になるため速やかな無効化が必要である。
イ. 退職後の利用を継続させる対応は不適切である。
ウ. 退職者アカウントはセキュリティリスクとなる。
エ. 権限拡大はリスクをさらに高める。

答え・解説 正答：ウ

ア：この説明は元の論点では「必要な業務引継ぎを確認した上で、不要となったアカウントや権限を速やかに無効化・削除する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「パスワードだけを本人に返却して利用継続を認める。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「管理者権限へ昇格させてから放置する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「退職者アカウント」について、誤答肢のどこが不適切かを説明できるかを確認する。退職者アカウントはセキュリティリスクとなる。 ID管理では入社・異動・休職・退職などのライフサイクルに合わせて権限を変更する。

基準：2026年度 / 2026-09-04

0096 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：標準

「アクセス制御・ID管理」の「管理者アカウント」を確認する。次の選択「管理者IDはネットワーク通信ができないから。」が不適切である理由として、最も直接的な説明はどれか。

ア. 特権IDにも強固な認証が必要である。
イ. 特権は必要な管理作業に限定し、通常利用アカウントと分離するのが望ましい。
ウ. むしろ特権操作は厳格にログ監視すべきである。
エ. 特権IDでも通信は可能である。

答え・解説 正答：エ

ア：この説明は元の論点では「特権IDはパスワードを設定できないから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「特権を必要としない操作まで高権限で行うと、誤操作や侵害時の影響が拡大するから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「特権IDではログを取得できないから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「アクセス制御・ID管理」の「管理者アカウント」について、誤答肢のどこが不適切かを説明できるかを確認する。特権IDでも通信は可能である。 特権アクセス管理では利用目的、承認、時間、操作記録などを厳格に管理する。

基準：2026年度 / 2026-09-04

0097 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：基礎

「アクセス制御・ID管理」を復習している。「パスワード総当たり攻撃を困難にする。」と判断できる理由として最も適切なものはどれか。

ア. 試行回数を制限することで自動化されたパスワード推測を抑制できる。
イ. 暗号化機能ではない。
ウ. DB設計とは無関係である。
エ. 一時ロックや段階的遅延が一般的で、永久削除が目的ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「通信内容を暗号化する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「データベースを正規化する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「正規利用者の権限を永久に削除する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「総当たり対策」について、結論だけでなく正答理由を説明できるかを確認する。試行回数を制限することで自動化されたパスワード推測を抑制できる。 ロックアウトはDoS的な悪用にも注意し、MFAや監視などと組み合わせる。

基準：2026年度 / 2026-09-04

0098 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：標準

「権限棚卸し」に関する理解を確認する。「全利用者へ権限を追加するだけにする。」という判断の問題点を説明しているものはどれか。

ア. 権限利用状況の確認が難しくなる。
イ. 過剰権限を増やす。
ウ. ライフサイクル管理が機能しない。
エ. アクセスレビューにより現職務と権限の不一致を発見できる。

答え・解説 正答：イ

ア：この説明は元の論点では「ログを取得しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「異動情報をID管理へ反映しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「利用者と付与権限の棚卸しを行い、不要権限を削除する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「権限棚卸し」について、誤答肢のどこが不適切かを説明できるかを確認する。過剰権限を増やす。 付与時だけでなく継続的な棚卸しが最小権限維持に必要である。

基準：2026年度 / 2026-09-04

0099 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：応用

「アクセス制御・ID管理」を復習している。「共有IDにすると必ず通信速度が低下する。」が正答にならない理由として最も適切なものはどれか。

ア. 個人別IDでなければ、監査ログから誰が操作したかを追跡しにくい。
イ. むしろID数は減る。
ウ. 通信速度とは直接関係しない。
エ. 共有IDで暗号化が必ず無効になるわけではない。

答え・解説 正答：ウ

ア：この説明は元の論点では「操作を実行した個人を特定しにくくなり、責任追跡性が低下する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「パスワード総数が増え過ぎる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「暗号化が自動的に無効になる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「アクセス制御・ID管理」の「個人識別性」について、誤答肢のどこが不適切かを説明できるかを確認する。通信速度とは直接関係しない。 特権操作では個人識別できるIDを用い、必要に応じて承認・記録を行うことが重要である。

基準：2026年度 / 2026-09-04

0100 セキュリティ管理・運用 > アクセス制御・ID管理 ｜ 難易度：標準

「条件付きアクセスを理解する」ために、「全端末から無条件で管理者権限を許可する。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 機密性を損なう。
イ. 端末状態や場所など環境属性を認可判断へ利用することでリスクに応じた制御ができる。
ウ. 侵害済み端末からも同じ条件で許可される。
エ. 最小権限に反する。

答え・解説 正答：エ

ア：この説明は元の論点では「公開鍵を使わず全通信を平文にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「利用者だけでなく端末や接続状況も評価する条件付きアクセス。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「認証済みなら接続元を一切評価しない固定許可。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「アクセス制御・ID管理」の「リスクベース制御」について、誤答肢のどこが不適切かを説明できるかを確認する。最小権限に反する。 アクセス制御はIDだけでなく利用コンテキストを含めて設計すると防御力を高められる。

基準：2026年度 / 2026-09-04

0101 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：基礎

「ログ・監視・脆弱性管理」の「監査証跡」を確認する。次の判断「不審な活動の検知や、事故発生後の原因・影響範囲の調査に利用する。」が適切である根拠として、最も直接的な説明はどれか。

ア. ログは監視・調査・監査の証拠として利用される。
イ. 圧縮は保存効率の手段であって主目的ではない。
ウ. 性能向上機能ではない。
エ. ログを非表示にすることが目的ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「保存データを必ず圧縮する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「CPU性能を向上させる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「利用者の操作を全て非表示にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「監査証跡」について、結論だけでなく正答理由を説明できるかを確認する。ログは監視・調査・監査の証拠として利用される。 認証、権限変更、設定変更、通信など重要イベントを適切に記録することが重要である。

基準：2026年度 / 2026-09-04

0102 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：標準

「ログ・監視・脆弱性管理」の演習で「全ログの時刻情報を削除する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. ファイル名の一致だけでは時系列を比較できない。
イ. 時刻を削除すると調査が困難になる。
ウ. 任意設定では時系列の整合が取れない。
エ. 時刻同期により複数機器のイベントを時系列で相関分析しやすくなる。

答え・解説 正答：イ

ア：この説明は元の論点では「ログファイル名だけを同じにする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「サーバごとに任意の時刻へ設定する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「NTPなどを用いてシステム時刻を同期する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「NTP」について、誤答肢のどこが不適切かを説明できるかを確認する。時刻を削除すると調査が困難になる。 インシデント調査では正確なタイムスタンプが重要な証拠情報になる。

基準：2026年度 / 2026-09-04

0103 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：基礎

「ログ相関分析」に関する理解を確認する。「コンパイラ。」という判断の問題点を説明しているものはどれか。

ア. SIEMはSecurity Information and Event Managementで、ログ集約・分析・アラートを行う。
イ. IP設定配布プロトコルである。
ウ. プログラム翻訳ツールである。
エ. ストレージ冗長化方式である。

答え・解説 正答：ウ

ア：この説明は元の論点では「SIEM。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「DHCP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「RAID。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「ログ相関分析」について、誤答肢のどこが不適切かを説明できるかを確認する。プログラム翻訳ツールである。 個別機器だけでは見つけにくい攻撃も、複数ログを関連付けることで検知しやすくなる。

基準：2026年度 / 2026-09-04

0104 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：標準

「ログ・監視・脆弱性管理」を復習している。「ログを利用者のPCへ自由にコピーさせる。」が正答にならない理由として最も適切なものはどれか。

ア. ログを分離保管しアクセス制御することで侵入先からの改ざんリスクを下げられる。
イ. 侵害された管理者権限で証拠を消されやすい。
ウ. 調査証拠を失う。
エ. 管理統制が弱くなる。

答え・解説 正答：エ

ア：この説明は元の論点では「ログを別の保護されたサーバへ転送し、書込み権限を限定して改ざんを困難にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「ログを侵害対象サーバだけに保存し、管理者なら自由に削除できるようにする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「全てのログ取得を停止する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ログ・監視・脆弱性管理」の「改ざん防止」について、誤答肢のどこが不適切かを説明できるかを確認する。管理統制が弱くなる。 ログの機密性だけでなく完全性と保存性も確保する必要がある。

基準：2026年度 / 2026-09-04

0105 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：応用

「誤検知と見逃しを区別できる」ために、「フォールスポジティブ。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. 正常事象を異常と誤判定するのがフォールスポジティブである。
イ. 情報源が本物かを示す性質である。
ウ. 対策後に残るリスクである。
エ. 実際の攻撃を正常と誤判定して見逃すのがフォールスネガティブである。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「真正性。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「残留リスク。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「フォールスネガティブ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「フォールスポジティブ」について、結論だけでなく正答理由を説明できるかを確認する。正常事象を異常と誤判定するのがフォールスポジティブである。 監視ルールは誤検知と見逃しのバランスを見ながら継続的に調整する。

基準：2026年度 / 2026-09-04

0106 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：標準

「ログ・監視・脆弱性管理」の「既知脆弱性検査」を確認する。次の選択「アクセスログを全て削除する。」が不適切である理由として、最も直接的な説明はどれか。

ア. 問題発見の機会を減らす。
イ. 監視・調査能力を低下させる。
ウ. バックアップは復旧策であり脆弱性検出ではない。
エ. 脆弱性スキャンは既知脆弱性や設定上の問題を広く検出するために用いる。

答え・解説 正答：イ

ア：この説明は元の論点では「ソースコードを一切確認せず運用する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「バックアップだけを取得する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「脆弱性スキャン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「既知脆弱性検査」について、誤答肢のどこが不適切かを説明できるかを確認する。監視・調査能力を低下させる。 スキャン結果は誤検知もあり得るため、影響度や資産重要度と合わせて確認する。

基準：2026年度 / 2026-09-04

0107 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：基礎

「ログ・監視・脆弱性管理」の演習で「利用者のパスワード強度だけを測定する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. CVSSは脆弱性の深刻度を数値化・評価するための共通指標である。
イ. DB設計指標ではない。
ウ. パスワード専用指標ではない。
エ. 通信性能指標でもない。

答え・解説 正答：ウ

ア：この説明は元の論点では「脆弱性の技術的な深刻度を共通尺度で評価する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「データベースの正規化度を評価する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「ネットワーク帯域を測定する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「深刻度評価」について、誤答肢のどこが不適切かを説明できるかを確認する。パスワード専用指標ではない。 実際の対応優先度はCVSSだけでなく、悪用状況、資産重要度、露出状況なども考慮する。

基準：2026年度 / 2026-09-04

0108 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：標準

「リスクベース修正」に関する理解を確認する。「発見順だけで機械的に決める。」という判断の問題点を説明しているものはどれか。

ア. 資産価値は影響度に直結する。
イ. リスクベースで優先度を決めることで限られた資源を重大リスクへ集中できる。
ウ. 低スコアでも環境や悪用状況によって対応が必要な場合がある。
エ. 発見順はリスクを反映しない。

答え・解説 正答：エ

ア：この説明は元の論点では「重要システムかどうかは考慮しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「脆弱性の深刻度、実際の悪用状況、対象資産の重要度や外部公開状況を総合して判断する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「CVSSが低ければ外部公開サーバでも必ず無期限に放置する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ログ・監視・脆弱性管理」の「リスクベース修正」について、誤答肢のどこが不適切かを説明できるかを確認する。発見順はリスクを反映しない。 脆弱性管理は発見、評価、優先順位付け、修正、確認を継続的に行う。

基準：2026年度 / 2026-09-04

0109 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：応用

「ログ・監視・脆弱性管理」の演習で「SBOM。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. 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を一覧化する。
イ. Web状態保持情報である。
ウ. ストレージのストライピング方式である。
エ. メール配送先情報である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「HTTP cookie。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「RAID0。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「DNS MXレコード。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「ソフトウェア構成把握」について、結論だけでなく正答理由を説明できるかを確認する。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を一覧化する。 ソフトウェア構成を把握しておくと、サプライチェーン上の脆弱性影響を調べやすい。

基準：2026年度 / 2026-09-04

0110 セキュリティ管理・運用 > ログ・監視・脆弱性管理 ｜ 難易度：標準

「ペネトレーションテストを理解する」ために、「単純なバックアップ復元。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 認証管理の一対策にすぎない。
イ. 復旧テストである。
ウ. 性能・保存効率の試験である。
エ. ペネトレーションテストは実攻撃に近い手法で侵入可能性や影響を評価する。

答え・解説 正答：イ

ア：この説明は元の論点では「定期パスワード変更だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「データ圧縮試験。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ペネトレーションテスト。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ログ・監視・脆弱性管理」の「侵入可能性評価」について、誤答肢のどこが不適切かを説明できるかを確認する。復旧テストである。 脆弱性スキャンより踏み込んだ検証を行うため、明確な許可・範囲・手順が必要である。

基準：2026年度 / 2026-09-04

0111 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：基礎

「インシデント対応・バックアップ・事業継続」の「インシデント対応組織」を確認する。次の選択「DNSルートサーバ。」が不適切である理由として、最も直接的な説明はどれか。

ア. CSIRTはComputer Security Incident Response Teamで、インシデント対応を組織的に行う。
イ. CAは認証局である。
ウ. DNS階層の名前解決基盤である。
エ. データベース管理システムである。

答え・解説 正答：ウ

ア：この説明は元の論点では「CSIRT。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「CA。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「DBMS。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「インシデント対応組織」について、誤答肢のどこが不適切かを説明できるかを確認する。DNS階層の名前解決基盤である。 CSIRTは平常時から連絡網や対応手順、外部機関との連携を準備しておく。

基準：2026年度 / 2026-09-04

0112 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：標準

「インシデント対応・バックアップ・事業継続」の演習で「証拠を確認せず全ログを削除する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 被害をさらに拡大する。
イ. 隔離は横展開や情報流出を抑える封じ込め策となる。
ウ. 被害拡大の可能性がある。
エ. 原因調査に必要な証拠を失う。

答え・解説 正答：エ

ア：この説明は元の論点では「攻撃者へ管理者パスワードを送る。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「組織の手順に従って対象端末をネットワークから隔離し、必要な証拠を保全する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「感染端末をそのまま業務利用し続ける。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「封じ込め」について、誤答肢のどこが不適切かを説明できるかを確認する。原因調査に必要な証拠を失う。 インシデント対応では封じ込めと証拠保全を両立させることが重要である。

基準：2026年度 / 2026-09-04

0113 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：基礎

「証拠保全」に関する理解を確認する。「デジタルフォレンジックス。」という結論を支持する説明として最も適切なものはどれか。

ア. デジタルフォレンジックスはデジタル証拠を適切に扱い、事実関係を分析する。
イ. DB設計技法である。
ウ. IP設定要求の中継機能である。
エ. 負荷分散である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「正規化。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「DHCPリレー。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「ロードバランシング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「証拠保全」について、結論だけでなく正答理由を説明できるかを確認する。デジタルフォレンジックスはデジタル証拠を適切に扱い、事実関係を分析する。 証拠の完全性や取得手順の記録を保つことが重要である。

基準：2026年度 / 2026-09-04

0114 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：標準

「インシデント対応・バックアップ・事業継続」を復習している。「3台のサーバを同じディスクへバックアップする。」が正答にならない理由として最も適切なものはどれか。

ア. 日数のルールではない。
イ. 同一障害点に集中すると共通原因で失う恐れがある。
ウ. 別場所保管の要件を満たさない。
エ. 3-2-1ルールは複数コピー、異なる媒体、別場所という多重化の考え方である。

答え・解説 正答：イ

ア：この説明は元の論点では「データを3日ごとに1回だけ上書きする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「バックアップを2個作り、両方とも本番と同じ場所へ置く。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「データを合計3コピー保持し、2種類の媒体に保存し、1コピーを別場所に保管する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「複数コピー」について、誤答肢のどこが不適切かを説明できるかを確認する。同一障害点に集中すると共通原因で失う恐れがある。 ランサムウェアや災害への備えでは、オフライン・イミュータブル化も有効である。

基準：2026年度 / 2026-09-04

0115 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：応用

「RPOを理解する」ために、「CVSS。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. RPOはRecovery Point Objectiveで、復旧すべきデータ時点の目標である。
イ. RTOは業務・システムを復旧させるまでの目標時間である。
ウ. 脆弱性深刻度指標である。
エ. 平均故障間隔である。

答え・解説 正答：ウ

ア：この説明は元の論点では「RPO。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「RTO。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「MTBF。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「許容データ損失」について、誤答肢のどこが不適切かを説明できるかを確認する。脆弱性深刻度指標である。 RPOが短いほど、より頻繁なバックアップやレプリケーションが必要になる。

基準：2026年度 / 2026-09-04

0116 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：標準

「インシデント対応・バックアップ・事業継続」の「復旧時間目標」を確認する。次の選択「TTL。」が不適切である理由として、最も直接的な説明はどれか。

ア. RTOはRecovery Time Objectiveで、停止から復旧までの目標時間を表す。
イ. データ損失許容点の目標である。
ウ. 生体認証の他人受入率である。
エ. 有効期間などを表す値である。

答え・解説 正答：エ

ア：この説明は元の論点では「RTO。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「RPO。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「FAR。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「復旧時間目標」について、誤答肢のどこが不適切かを説明できるかを確認する。有効期間などを表す値である。 事業継続計画では業務重要度に応じてRTOとRPOを設定する。

基準：2026年度 / 2026-09-04

0117 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：基礎

「インシデント対応・バックアップ・事業継続」を復習している。「災害や重大障害が発生しても重要業務を継続し、又は目標時間内に復旧できるよう計画する。」と判断できる理由として最も適切なものはどれか。

ア. BCPはBusiness Continuity Planで、重要業務の継続・早期復旧を目的とする。
イ. コスト削減だけが目的ではない。
ウ. 認証運用だけを扱う計画ではない。
エ. 事故ゼロを保証するものではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「システム開発費を必ず0にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「日常のパスワード変更だけを定める。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「全ての事故を必ず発生させない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「重要業務継続」について、結論だけでなく正答理由を説明できるかを確認する。BCPはBusiness Continuity Planで、重要業務の継続・早期復旧を目的とする。 BCPでは代替拠点、人員、連絡、IT復旧など業務全体を考慮する。

基準：2026年度 / 2026-09-04

0118 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：標準

「復旧可能性」に関する理解を確認する。「復元テストはログ監視を禁止するために行う。」という判断の問題点を説明しているものはどれか。

ア. 実際の復元可能性を検証しなければならない。
イ. 監視を禁止する目的ではない。
ウ. 一般にテスト用環境で確認できる。
エ. 取得成功と復旧成功は同じではなく、破損や手順不備があり得る。

答え・解説 正答：イ

ア：この説明は元の論点では「バックアップ成功なら復元は必ず保証されるため本来不要である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「復元するとバックアップが必ず消えるから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「実際に必要なデータを所定時間内に復元できることを確認するため。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「復旧可能性」について、誤答肢のどこが不適切かを説明できるかを確認する。監視を禁止する目的ではない。 バックアップは『取得した』だけでなく『復元できる』ことまで確認して初めて有効である。

基準：2026年度 / 2026-09-04

0119 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：応用

「インシデント対応・バックアップ・事業継続」を復習している。「正規化。」が正答にならない理由として最も適切なものはどれか。

ア. 重大度に応じて上位責任者や専門部門へ報告・判断を引き上げることをエスカレーションという。
イ. 通信のカプセル化技術である。
ウ. DB設計技法である。
エ. 故障時安全設計である。

答え・解説 正答：ウ

ア：この説明は元の論点では「エスカレーション。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「トンネリング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「フェイルセーフ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「エスカレーション」について、誤答肢のどこが不適切かを説明できるかを確認する。DB設計技法である。 インシデント対応では重大度分類と連絡先を事前に定めておくことが重要である。

基準：2026年度 / 2026-09-04

0120 セキュリティ管理・運用 > インシデント対応・バックアップ・事業継続 ｜ 難易度：標準

「事後レビューを理解する」ために、「証拠とログを全て削除する。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 組織学習を妨げる。
イ. 事後レビューにより対応プロセスの弱点を発見して改善できる。
ウ. 原因を把握しなければ再発防止策を立てにくい。
エ. 将来の監査や改善に必要な証拠を失う。

答え・解説 正答：エ

ア：この説明は元の論点では「インシデントを無かったことにする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「教訓を手順や管理策へ反映し、同種事故の再発防止と対応力向上につなげる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「原因調査を禁止する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「インシデント対応・バックアップ・事業継続」の「再発防止」について、誤答肢のどこが不適切かを説明できるかを確認する。将来の監査や改善に必要な証拠を失う。 インシデント管理は復旧で終わらず、振り返りと改善まで含めて継続的に成熟させる。

基準：2026年度 / 2026-09-04

0121 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：基礎

「セキュアプロトコル・クラウド・IoTセキュリティ」の「通信路保護」を確認する。次の判断「通信相手の認証や通信内容の暗号化・改ざん検知によって通信路を保護する。」が適切である根拠として、最も直接的な説明はどれか。

ア. TLSは通信相手の認証、機密性、完全性の確保に利用される。
イ. DB設計とは無関係である。
ウ. 圧縮方式ではない。
エ. IP設定配布はDHCPの役割である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「データベース表を正規化する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ファイルを必ず可逆圧縮する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「IPアドレスを端末へ自動配布する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「通信路保護」について、結論だけでなく正答理由を説明できるかを確認する。TLSは通信相手の認証、機密性、完全性の確保に利用される。 HTTPSではHTTPをTLS上で利用してWeb通信を保護する。

基準：2026年度 / 2026-09-04

0122 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：標準

「セキュアプロトコル・クラウド・IoTセキュリティ」の演習で「Telnetを暗号化なしで利用する。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. FTPは主にファイル転送用である。
イ. Telnetは通信内容が平文となるため安全な遠隔管理には不向きである。
ウ. SNMP Trapは管理イベント通知である。
エ. SSHは遠隔ログインやコマンド実行を暗号化して保護する。

答え・解説 正答：イ

ア：この説明は元の論点では「FTPだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「SNMP Trapだけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「SSH。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「安全な遠隔管理」について、誤答肢のどこが不適切かを説明できるかを確認する。Telnetは通信内容が平文となるため安全な遠隔管理には不向きである。 管理用プロトコルでは認証情報や操作内容を保護できる方式を選ぶ。

基準：2026年度 / 2026-09-04

0123 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：基礎

「IP層保護」に関する理解を確認する。「Webブラウザのcookie形式である。」という判断の問題点を説明しているものはどれか。

ア. IPsecはIP層で通信保護を行い、拠点間VPNなどに利用される。
イ. メール圧縮方式ではない。
ウ. Web状態保持情報ではない。
エ. DB制約とは無関係である。

答え・解説 正答：ウ

ア：この説明は元の論点では「IP層でパケットの認証や暗号化を行い、VPNなどで通信を保護する技術である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「電子メール本文だけを圧縮する方式である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「データベースの主キー制約である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「IP層保護」について、誤答肢のどこが不適切かを説明できるかを確認する。Web状態保持情報ではない。 IPsecはアプリケーションに依存しにくいネットワーク層のセキュリティ技術である。

基準：2026年度 / 2026-09-04

0124 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：標準

「セキュアプロトコル・クラウド・IoTセキュリティ」を復習している。「SMTP。」が正答にならない理由として最も適切なものはどれか。

ア. ストレージ冗長化方式である。
イ. WPA3は無線LANの認証・暗号化に関するセキュリティ規格である。
ウ. Web通信プロトコルである。
エ. メール送信プロトコルである。

答え・解説 正答：エ

ア：この説明は元の論点では「RAID5。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「WPA3。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「HTTP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「無線LAN保護」について、誤答肢のどこが不適切かを説明できるかを確認する。メール送信プロトコルである。 無線LANでは強固な暗号方式だけでなく、認証情報やアクセスポイント設定も適切に管理する。

基準：2026年度 / 2026-09-04

0125 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：応用

「送信ドメイン認証を理解する」ために、「SPF、DKIM、DMARC。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. SPFは送信元サーバ、DKIMは署名、DMARCは認証結果に基づくポリシーや報告に関係する。
イ. ファイル転送技術の組合せである。
ウ. ストレージ・メモリ・電源の可用性技術である。
エ. IP設定・アドレス解決・変換の技術である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「FTP、TFTP、SFTP。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「RAID、ECC、UPS。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「DHCP、ARP、NAT。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「SPF/DKIM/DMARC」について、結論だけでなく正答理由を説明できるかを確認する。SPFは送信元サーバ、DKIMは署名、DMARCは認証結果に基づくポリシーや報告に関係する。 送信ドメイン認証はなりすましメール対策の重要な一部である。

基準：2026年度 / 2026-09-04

0126 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：標準

「セキュアプロトコル・クラウド・IoTセキュリティ」の「共有責任」を確認する。次の選択「クラウドでは暗号化を実施できないから。」が不適切である理由として、最も直接的な説明はどれか。

ア. 認証サービスは利用できる。
イ. 暗号化機能も利用できる。
ウ. 安全性は構成・運用・サービス内容に依存し一律に決まらない。
エ. クラウドでは提供者と利用者の責任範囲を明確にし、それぞれが管理策を実施する。

答え・解説 正答：イ

ア：この説明は元の論点では「クラウドでは認証機能を利用できないから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「クラウドサービスは必ずオンプレミスより危険だから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「サービスモデルに応じて、利用者にもアカウント・権限・データ・設定などを適切に管理する責任が残るから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「共有責任」について、誤答肢のどこが不適切かを説明できるかを確認する。暗号化機能も利用できる。 クラウド利用では責任共有モデルを理解し、設定不備や過剰権限を防ぐことが重要である。

基準：2026年度 / 2026-09-04

0127 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：基礎

「セキュアプロトコル・クラウド・IoTセキュリティ」の演習で「管理者用アクセスキーをソースコードへ平文で埋め込む。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 最小権限と定期的な設定レビューにより公開設定ミスを防ぎやすい。
イ. 情報漏えいや改ざんの危険が高い。
ウ. 認証情報漏えいにつながる。
エ. 監査・異常検知能力を下げる。

答え・解説 正答：ウ

ア：この説明は元の論点では「公開範囲を必要な利用者だけに限定し、権限設定を定期的に確認する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「インターネット上の全利用者へ匿名書込みを許可する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「アクセスログを無効にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「ストレージ公開設定」について、誤答肢のどこが不適切かを説明できるかを確認する。認証情報漏えいにつながる。 クラウドでは設定変更が容易なため、構成管理と継続的な監視が重要になる。

基準：2026年度 / 2026-09-04

0128 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：標準

「初期パスワード」に関する理解を確認する。「センサ精度が必ず低下するから。」という判断の問題点を説明しているものはどれか。

ア. 共通既定パスワードは大量侵害の入口となり得る。
イ. 消費電力とは直接関係しない。
ウ. IP重複の直接原因ではない。
エ. センサ精度とも無関係である。

答え・解説 正答：エ

ア：この説明は元の論点では「一つの認証情報が知られると多数機器へ不正ログインされる可能性があるから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「機器の消費電力が必ず増えるから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「IPアドレスが自動的に重複するから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「初期パスワード」について、誤答肢のどこが不適切かを説明できるかを確認する。センサ精度とも無関係である。 機器ごとの認証情報、初回変更、不要サービス停止などがIoTの基本対策となる。

基準：2026年度 / 2026-09-04

0129 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：応用

「セキュアプロトコル・クラウド・IoTセキュリティ」の演習で「更新ファイルのデジタル署名を機器側で検証し、正当な提供元のものだけ適用する。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. 署名検証により更新元の真正性とファイル完全性を確認できる。
イ. 防御機能を失う。
ウ. 改ざんやなりすましを検知できない。
エ. 悪意あるファームウェアを受け入れる危険がある。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「署名検証機能を無効にする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「通信経路と更新ファイルの完全性を一切確認しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「更新ファイルを入手元に関係なく自動実行する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「署名検証」について、結論だけでなく正答理由を説明できるかを確認する。署名検証により更新元の真正性とファイル完全性を確認できる。 IoTでは長期運用を考慮し、安全な更新配布と署名検証の仕組みを用意する。

基準：2026年度 / 2026-09-04

0130 実装・法務・標準 > セキュアプロトコル・クラウド・IoTセキュリティ ｜ 難易度：標準

「セキュアブートを理解する」ために、「データベースビュー。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. IP設定要求の中継機能である。
イ. DBの仮想表である。
ウ. 名前解決を利用する分散方式である。
エ. セキュアブートは起動コードの署名などを検証し、信頼されたコードだけを実行する。

答え・解説 正答：イ

ア：この説明は元の論点では「DHCPリレー。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「DNSラウンドロビン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「セキュアブート。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュアプロトコル・クラウド・IoTセキュリティ」の「起動時検証」について、誤答肢のどこが不適切かを説明できるかを確認する。DBの仮想表である。 端末・IoT機器では起動時から信頼の連鎖を確保することが重要である。

基準：2026年度 / 2026-09-04

0131 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：基礎

「セキュリティ関連法規・個人情報保護」の「不正アクセス行為」を確認する。次の選択「著作権法だけ。」が不適切である理由として、最も直接的な説明はどれか。

ア. 他人の識別符号などを悪用した不正アクセスを禁止する法律である。
イ. 労働条件に関する法律である。
ウ. 著作物保護が主目的であり、この行為を直接扱う中心法規ではない。
エ. 道路交通に関する法律である。

答え・解説 正答：ウ

ア：この説明は元の論点では「不正アクセス行為の禁止等に関する法律。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「労働基準法。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「道路交通法。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「不正アクセス行為」について、誤答肢のどこが不適切かを説明できるかを確認する。著作物保護が主目的であり、この行為を直接扱う中心法規ではない。 FEでは不正アクセス禁止法の対象となる行為を、単なる利用規約違反などと区別して理解する。

基準：2026年度 / 2026-09-04

0132 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：標準

「セキュリティ関連法規・個人情報保護」の演習で「認証情報は自由に第三者へ配布してよい。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 通信路の暗号化と行為の適法性は別問題である。
イ. 不正アクセスを助長する目的で識別符号を提供する行為は規制対象となる。
ウ. 対象は秘密鍵だけに限られない。
エ. 認証情報の無断提供は重大なリスクである。

答え・解説 正答：エ

ア：この説明は元の論点では「通信が暗号化されていれば常に適法となる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「不正アクセスを助長する行為として法的問題となり得る。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「本人の秘密鍵でなければ法的問題は一切生じない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「認証情報提供」について、誤答肢のどこが不適切かを説明できるかを確認する。認証情報の無断提供は重大なリスクである。 認証情報の取扱いは技術面だけでなく法的・組織的ルールにも従う必要がある。

基準：2026年度 / 2026-09-04

0133 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：基礎

「マルウェア作成」に関する理解を確認する。「不正指令電磁的記録に関する罪。」という結論を支持する説明として最も適切なものはどれか。

ア. いわゆるコンピュータウイルス作成罪などは不正指令電磁的記録に関する罪として規定される。
イ. 要件が異なる。
ウ. 分野が異なる。
エ. この行為を直接扱う中心的な犯罪類型ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「業務上過失致死罪だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「道路運送法違反。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「名誉毀損罪だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「マルウェア作成」について、結論だけでなく正答理由を説明できるかを確認する。いわゆるコンピュータウイルス作成罪などは不正指令電磁的記録に関する罪として規定される。 セキュリティ関連法規では、攻撃手法だけでなく不正プログラム作成・提供にも法的規制があることを理解する。

基準：2026年度 / 2026-09-04

0134 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：標準

「セキュリティ関連法規・個人情報保護」を復習している。「個別Webサイトのパスワード長だけを定める法律である。」が正答にならない理由として最も適切なものはどれか。

ア. 暗号方式を一つに固定する法律ではない。
イ. 特定サイトのパスワード仕様だけを規定するものではない。
ウ. DB設計とは無関係である。
エ. サイバーセキュリティ基本法は国全体の施策推進に関する基本的枠組みを定める。

答え・解説 正答：イ

ア：この説明は元の論点では「全ての暗号アルゴリズムを一つに統一する法律である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「データベースの正規化方法を定める法律である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「国のサイバーセキュリティ施策の基本理念や関係主体の責務などを定める基本法である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「基本法」について、誤答肢のどこが不適切かを説明できるかを確認する。特定サイトのパスワード仕様だけを規定するものではない。 基本法と、個別の禁止行為や義務を定める法律を区別することが重要である。

基準：2026年度 / 2026-09-04

0135 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：応用

「個人情報の定義を理解する」ために、「死亡者に関する情報は他の情報との関係を問わず常に同法上の個人情報となる。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 個人情報は生存する個人に関する情報で、氏名などにより特定個人を識別できるもの等を含む。
イ. 法人そのものの情報は個人情報の定義とは異なる。
ウ. 法の定義は生存する個人を対象とする。
エ. 公開情報であっても定義に該当すれば個人情報となり得る。

答え・解説 正答：ウ

ア：この説明は元の論点では「生存する個人に関する情報で、特定の個人を識別できるものなどを含む。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「法人名だけは必ず個人情報になる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「公開済み情報は特定個人を識別できても個人情報にならない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「生存する個人」について、誤答肢のどこが不適切かを説明できるかを確認する。法の定義は生存する個人を対象とする。 情報の公開・非公開だけでなく、特定個人を識別できるかなど法上の定義で判断する。

基準：2026年度 / 2026-09-04

0136 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：標準

「セキュリティ関連法規・個人情報保護」の「識別子」を確認する。次の選択「会社の部署コードだけを必ず指す。」が不適切である理由として、最も直接的な説明はどれか。

ア. 表示用コードとは無関係である。
イ. 個人識別符号は法令で定められた、個人を識別するための一定の符号である。
ウ. 個人識別性のない任意文字列が当然に該当するわけではない。
エ. 部署識別だけでは個人識別符号とは限らない。

答え・解説 正答：エ

ア：この説明は元の論点では「Webページの色指定コードだけを指す。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「特定の個人を識別できるように変換された身体的特徴の符号や、公的に個人へ割り当てられた番号等のうち法令で定めるものをいう。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「全てのランダムなファイル名をいう。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「識別子」について、誤答肢のどこが不適切かを説明できるかを確認する。部署識別だけでは個人識別符号とは限らない。 個人識別符号を含む情報は、他の要件を満たす場合に個人情報として扱われる。

基準：2026年度 / 2026-09-04

0137 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：基礎

「セキュリティ関連法規・個人情報保護」を復習している。「要配慮個人情報。」と判断できる理由として最も適切なものはどれか。

ア. 病歴などは要配慮個人情報に含まれる代表例である。
イ. 個人を識別できない統計情報とは性質が異なる。
ウ. 通信上の識別情報である。
エ. 暗号技術の用語である。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「匿名の統計値だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ネットワークアドレス。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「公開鍵。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「慎重な取扱い」について、結論だけでなく正答理由を説明できるかを確認する。病歴などは要配慮個人情報に含まれる代表例である。 要配慮個人情報は取得や取扱いについて通常の個人情報より慎重なルールが設けられている。

基準：2026年度 / 2026-09-04

0138 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：標準

「漏えい防止」に関する理解を確認する。「従業員教育は安全管理措置と無関係である。」という判断の問題点を説明しているものはどれか。

ア. 技術だけで全ての事故を防ぐことはできない。
イ. 人的安全管理は重要な要素である。
ウ. アクセス制御は技術的安全管理に関係する。
エ. 個人情報保護委員会のガイドラインでは複数の観点から安全管理措置を整理している。

答え・解説 正答：イ

ア：この説明は元の論点では「技術的対策だけを実施すれば他の対策は不要である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「アクセス権管理は安全管理措置には含まれない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「組織的・人的・物理的・技術的な対策などを、リスクに応じて適切に講じる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「漏えい防止」について、誤答肢のどこが不適切かを説明できるかを確認する。人的安全管理は重要な要素である。 安全管理は組織・人・物理・技術を組み合わせて継続的に実施する。

基準：2026年度 / 2026-09-04

0139 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：応用

「セキュリティ関連法規・個人情報保護」を復習している。「収集した情報は必ず全て第三者へ公開する。」が正答にならない理由として最も適切なものはどれか。

ア. 個人情報の利用目的はできる限り明確に特定することが基本である。
イ. 無制限利用を前提とする考え方ではない。
ウ. 第三者公開を原則とするものではない。
エ. 利用目的の通知・公表等に関するルールがある。

答え・解説 正答：ウ

ア：この説明は元の論点では「利用目的をできる限り特定し、その目的との関係を意識して適正に取り扱う。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「将来何に使うか決めず無制限に利用できるようにする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「利用目的は本人にも社内にも一切示さないことが原則である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「目的外利用防止」について、誤答肢のどこが不適切かを説明できるかを確認する。第三者公開を原則とするものではない。 必要な情報を目的に沿って適切に扱うことが個人情報保護の基本となる。

基準：2026年度 / 2026-09-04

0140 実装・法務・標準 > セキュリティ関連法規・個人情報保護 ｜ 難易度：標準

「匿名加工情報の基本を理解する」ために、「加工前の個人情報と全く同じ内容をそのまま公開する。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 匿名加工情報は個人を識別できず、元の個人情報を復元できないよう加工する。
イ. 単純な置換で容易に元へ戻せるなら要件を満たさない。
ウ. 可逆暗号化だけでは匿名加工情報の定義を満たすとは限らない。
エ. 無加工公開ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「特定の個人を識別できず、元の個人情報を復元できないよう所定の加工を施した情報である。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「氏名だけを別名に置換すれば必ず元に戻せる状態でも匿名加工情報となる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「個人情報を暗号化しただけで復号鍵を保持していても必ず匿名加工情報となる。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「セキュリティ関連法規・個人情報保護」の「再識別困難化」について、誤答肢のどこが不適切かを説明できるかを確認する。無加工公開ではない。 仮名加工情報と匿名加工情報は再識別可能性や法的取扱いが異なるため区別する。

基準：2026年度 / 2026-09-04

0141 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：基礎

「ISMS・監査・ガバナンス」の「リスクベース管理」を確認する。次の判断「組織が自らの情報セキュリティリスクを評価し、必要な管理策を選択・運用して継続的に改善する。」が適切である根拠として、最も直接的な説明はどれか。

ア. ISMSは組織のリスクに基づいて管理策や運用を体系的に管理するマネジメントシステムである。
イ. 単一製品の導入だけでマネジメントシステムにはならない。
ウ. 経営・業務・人・技術を含む組織的な取組が必要である。
エ. 組織の状況やリスクは異なるため一律ではない。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「暗号化製品を導入すればISMSが自動的に完成する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「情報セキュリティを情報システム部門だけの問題として扱う。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「全組織へ同じ技術対策だけを無条件に適用する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「リスクベース管理」について、結論だけでなく正答理由を説明できるかを確認する。ISMSは組織のリスクに基づいて管理策や運用を体系的に管理するマネジメントシステムである。 ISMSは個別技術だけでなく、方針、責任、リスク管理、評価、改善を一体として扱う。

基準：2026年度 / 2026-09-04

0142 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：標準

「ISMS・監査・ガバナンス」の演習で「HTTP/1.1だけ。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 品質マネジメントシステムの規格でありISMS認証基準ではない。
イ. Web通信プロトコルである。
ウ. Ethernetに関する規格である。
エ. JIS Q 27001はISO/IEC 27001と整合するISMSの要求事項規格で、ISMS認証基準として用いられる。

答え・解説 正答：イ

ア：この説明は元の論点では「JIS Q 9001だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「IEEE 802.3だけ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「JIS Q 27001（ISO/IEC 27001）。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「JIS Q 27001」について、誤答肢のどこが不適切かを説明できるかを確認する。Web通信プロトコルである。 2026年時点のISMS適合性評価制度ではJIS Q 27001が認証基準として位置付けられている。

基準：2026年度 / 2026-09-04

0143 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：基礎

「トップマネジメント」に関する理解を確認する。「現場担当者だけが非公開で作成し経営層は関与しない。」という判断の問題点を説明しているものはどれか。

ア. 方針は組織の方向性とコミットメントを示す上位文書である。
イ. 環境変化に応じて見直しが必要である。
ウ. 経営の関与が重要である。
エ. 個別製品一覧だけでは方針にならない。

答え・解説 正答：ウ

ア：この説明は元の論点では「経営上の方向性や情報セキュリティへの取組姿勢を示し、組織内の活動の基礎とする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「一度作成すれば組織変更やリスク変化があっても見直さない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「技術製品の型番一覧だけを記載する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「トップマネジメント」について、誤答肢のどこが不適切かを説明できるかを確認する。経営の関与が重要である。 方針、規程、手順へ段階的に具体化して組織全体へ展開する。

基準：2026年度 / 2026-09-04

0144 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：標準

「ISMS・監査・ガバナンス」を復習している。「利用可能な管理策を理由なく全て導入する。」が正答にならない理由として最も適切なものはどれか。

ア. 他社の状況と自組織のリスクは異なる。
イ. 管理策は組織のリスクと要求事項に基づいて選定する。
ウ. 高リスクなら費用を含め適切な対応判断が必要である。
エ. 全管理策の無条件導入は合理的ではない。

答え・解説 正答：エ

ア：この説明は元の論点では「他社が使っている管理策だけをそのままコピーする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「リスクアセスメントとリスク対応の結果に基づき、必要な管理策を選択する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「費用がかかる管理策はリスクに関係なく全て除外する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ISMS・監査・ガバナンス」の「リスク対応」について、誤答肢のどこが不適切かを説明できるかを確認する。全管理策の無条件導入は合理的ではない。 リスクベースで必要性を説明できることがISMS運用の重要点である。

基準：2026年度 / 2026-09-04

0145 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：応用

「内部監査の独立性を理解する」ために、「客観性や独立性が損なわれ、問題を適切に評価できないおそれがあるから。」という判断の根拠を確認したい。最も適切な説明はどれか。

ア. 監査では監査対象からの客観性を確保することが重要である。
イ. 監査証拠に基づく評価が必要である。
ウ. 監査結果の公開範囲は目的・規程による。
エ. 知識があること自体が問題ではなく、自己監査による利害関係が問題となる。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「内部監査では証拠を使ってはいけないから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「監査結果は必ず外部公開する必要があるから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「担当者は業務内容を知り過ぎているため法律で必ず監査禁止だから。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「自己監査回避」について、結論だけでなく正答理由を説明できるかを確認する。監査では監査対象からの客観性を確保することが重要である。 独立性を確保した監査体制により、形骸化した自己評価を避けやすくなる。

基準：2026年度 / 2026-09-04

0146 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：標準

「ISMS・監査・ガバナンス」の「客観的証拠」を確認する。次の選択「暗号鍵。」が不適切である理由として、最も直接的な説明はどれか。

ア. ネットワーク経路情報の一種である。
イ. 認証・暗号化に使う情報であり監査証拠の総称ではない。
ウ. 一時保存領域である。
エ. 監査証拠は監査所見や結論を裏付ける客観的な情報である。

答え・解説 正答：イ

ア：この説明は元の論点では「ルーティングテーブル。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「キャッシュ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「監査証拠。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「客観的証拠」について、誤答肢のどこが不適切かを説明できるかを確認する。認証・暗号化に使う情報であり監査証拠の総称ではない。 監査では十分かつ適切な証拠を収集し、事実に基づいて評価する。

基準：2026年度 / 2026-09-04

0147 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：基礎

「ISMS・監査・ガバナンス」の演習で「暗号化。」を選ぶと誤答になる。その理由として最も適切なものはどれか。

ア. 監査サンプリングは母集団の一部を抽出し、合理的な監査証拠を得る方法である。
イ. 監査対象を消してしまう。
ウ. 機密性対策である。
エ. 可用性対策である。

答え・解説 正答：ウ

ア：この説明は元の論点では「監査サンプリング。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「全件削除。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
エ：この説明は元の論点では「フェイルオーバ。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「サンプリング」について、誤答肢のどこが不適切かを説明できるかを確認する。機密性対策である。 抽出方法や件数が偏ると結論の信頼性へ影響するため、目的に応じて設計する。

基準：2026年度 / 2026-09-04

0148 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：標準

「経営層評価」に関する理解を確認する。「パケットキャプチャだけ。」という判断の問題点を説明しているものはどれか。

ア. DB問合せ処理である。
イ. マネジメントレビューはトップマネジメントがISMSの適切性・有効性等を評価する活動である。
ウ. ネットワーク調査行為である。
エ. 技術的な通信解析だけではない。

答え・解説 正答：エ

ア：この説明は元の論点では「SQL結合。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は元の論点では「マネジメントレビュー。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「ポートスキャン。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。

総合解説：この問題は「ISMS・監査・ガバナンス」の「経営層評価」について、誤答肢のどこが不適切かを説明できるかを確認する。技術的な通信解析だけではない。 経営層が評価結果を改善や方針・資源へ反映することでISMSを継続的に機能させる。

基準：2026年度 / 2026-09-04

0149 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：応用

「ISMS・監査・ガバナンス」の演習で「原因を分析し、再発を防ぐため手順・責任・確認方法を改善し、その有効性を確認する。」を正しい判断として採用した。その理由を最も適切に説明しているものはどれか。

ア. 是正処置は不適合の原因を除去し、再発を防止することを目的とする。
イ. 監査証跡の削除は不適切である。
ウ. 継続的改善に反する。
エ. 個別修正だけでは根本原因が残る可能性がある。

答え・解説 正答：ア

ア：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
イ：この説明は元の論点では「監査記録を削除して指摘を無かったことにする。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
ウ：この説明は元の論点では「同じ不備が再発しても対応しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「指摘された1件だけ直して原因を調べない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「再発防止」について、結論だけでなく正答理由を説明できるかを確認する。是正処置は不適合の原因を除去し、再発を防止することを目的とする。 原因分析、対策実施、有効性確認まで行うことで改善を定着させる。

基準：2026年度 / 2026-09-04

0150 実装・法務・標準 > ISMS・監査・ガバナンス ｜ 難易度：標準

「情報セキュリティガバナンスを理解する」ために、「技術対策だけを選び事業リスクは考慮しない。」という選択の誤りを検討する。最も適切な説明はどれか。

ア. 最終的な経営責任まで委譲することはできない。
イ. 事業目標やリスクとの整合が必要である。
ウ. 平常時から継続的な監督が必要である。
エ. ガバナンスでは経営が方向性を示し、責任を明確にして監督する。

答え・解説 正答：イ

ア：この説明は元の論点では「セキュリティを全て現場へ丸投げし、経営は結果を確認しない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
イ：この説明は、設問中の判断を評価するための直接の根拠を示しており、今回の問いに適切である。
ウ：この説明は元の論点では「事故発生時だけ一時的に関与し、平常時の監督は行わない。」に対応する内容であり、今回指定された判断の直接の根拠ではない。
エ：この説明は元の論点では「事業目標とリスクを踏まえて方針・責任・資源配分を決め、セキュリティ活動を監督する。」に対応する内容であり、今回指定された判断の直接の根拠ではない。

総合解説：この問題は「ISMS・監査・ガバナンス」の「経営責任」について、誤答肢のどこが不適切かを説明できるかを確認する。事業目標やリスクとの整合が必要である。 情報セキュリティを経営課題として扱い、組織全体の管理体系へ組み込むことが重要である。

基準：2026年度 / 2026-09-04