Q001 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

組織内CSIRTを新設する際、最初に明確化すべき事項として最も適切なものはどれか。
ア．CSIRTの使命、サービス対象（コンスティチュエンシー）、権限、提供サービスを文書化する。
イ．市販のSIEM製品を先に選定する。
ウ．全社員をCSIRT専任要員に任命する。
エ．外部公開用の事故報告書の書式だけを作成する。

正答・4肢解説・総合解説

正答：ア．CSIRTの使命、サービス対象（コンスティチュエンシー）、権限、提供サービスを文書化する。
ア：使命・対象・権限が曖昧だと、誰が何を判断しどこまで対応するかが不明確になるため、体制設計の基礎として先に定義する。
イ：SIEMは支援ツールであり、体制の使命や権限を代替しない。
ウ：全社員を専任にする必要はなく、必要な役割と要員を設計する。
エ：報告書式は一要素にすぎず、CSIRT全体の役割定義より先ではない。
総合解説：使命・対象・権限が曖昧だと、誰が何を判断しどこまで対応するかが不明確になるため、体制設計の基礎として先に定義する。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q002 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

FIRSTのCSIRT Services Frameworkの位置付けとして最も適切なものはどれか。
ア．すべてのCSIRTに同一の組織図を義務付ける国際規格である。
イ．CSIRTが提供し得るサービスや機能を整理した高レベルの枠組みであり、全CSIRTが全サービスを提供することを要求するものではない。
ウ．CSIRT用の侵入検知製品の技術仕様書である。
エ．法執行機関だけが利用できる証拠保全手順書である。

正答・4肢解説・総合解説

正答：イ．CSIRTが提供し得るサービスや機能を整理した高レベルの枠組みであり、全CSIRTが全サービスを提供することを要求するものではない。
ア：組織図を一律に規定するものではない。
イ：FIRSTの枠組みは共通語彙とサービス整理を目的とし、各チームは使命と対象に応じて必要なサービスを選択する。
ウ：製品仕様ではなく、サービスと機能のフレームワークである。
エ：CSIRT全般の運用改善を支援するもので、法執行機関限定ではない。
総合解説：FIRSTの枠組みは共通語彙とサービス整理を目的とし、各チームは使命と対象に応じて必要なサービスを選択する。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q003 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTとPSIRTの役割の違いとして最も適切なものはどれか。
ア．CSIRTは製品脆弱性だけを扱い、PSIRTは社内ネットワークだけを扱う。
イ．両者は名称が違うだけで役割は完全に同一である。
ウ．CSIRTは主に組織の情報システムやサービスのインシデント対応を担い、PSIRTは自組織が提供する製品・サービスの脆弱性や製品セキュリティ問題への対応を担う。
エ．PSIRTは人事部門に限定された内部不正調査チームである。

正答・4肢解説・総合解説

正答：ウ．CSIRTは主に組織の情報システムやサービスのインシデント対応を担い、PSIRTは自組織が提供する製品・サービスの脆弱性や製品セキュリティ問題への対応を担う。
ア：役割の方向が逆である。
イ：FIRSTはPSIRT固有のサービス領域を別枠で整理している。
ウ：CSIRTとPSIRTには共通点もあるが、主な対象は組織環境と製品セキュリティで異なる。
エ：PSIRTは製品セキュリティインシデント対応チームであり、人事部門限定ではない。
総合解説：CSIRTとPSIRTには共通点もあるが、主な対象は組織環境と製品セキュリティで異なる。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q004 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTのインシデントトラッキングシステムに持たせる情報として、対応の追跡可能性を最も高めるものはどれか。
ア．最終的な復旧日時だけを記録する。
イ．担当者の私的メモだけに経緯を残す。
ウ．インシデントごとに異なる記録様式を自由に使う。
エ．受付時刻、事象概要、担当者、判断、実施した対応、証拠・関連チケット、状態遷移を一貫して記録する。

正答・4肢解説・総合解説

正答：エ．受付時刻、事象概要、担当者、判断、実施した対応、証拠・関連チケット、状態遷移を一貫して記録する。
ア：最終日時だけでは判断経緯や対応内容を追跡できない。
イ：私的メモは共有性・継続性が低く、正式記録として不十分である。
ウ：様式がばらばらだと集約・検索・比較が難しくなる。
エ：対応の履歴と根拠を時系列で追える記録は、引継ぎ、監査、事後分析に有効である。
総合解説：対応の履歴と根拠を時系列で追える記録は、引継ぎ、監査、事後分析に有効である。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q005 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTの権限をあらかじめ規程化する主な理由として最も適切なものはどれか。
ア．緊急時に、端末隔離や通信遮断などの判断を誰がどの条件で実施できるかを明確にし、対応遅延や越権を防ぐため。
イ．すべてのインシデントで経営者の口頭承認を不要にするためだけ。
ウ．CSIRTが法務・広報・事業部門の権限を恒久的に代行するため。
エ．ログを取得しなくてもよいようにするため。

正答・4肢解説・総合解説

正答：ア．緊急時に、端末隔離や通信遮断などの判断を誰がどの条件で実施できるかを明確にし、対応遅延や越権を防ぐため。
ア：権限・承認経路を事前定義すると、重大事象での迅速性と統制を両立できる。
イ：承認要否は事案や権限設計によるため、常に不要にすることが目的ではない。
ウ：関係部門との役割分担は維持し、CSIRTが恒久的に代行するわけではない。
エ：権限規程は証拠・ログ取得の必要性をなくさない。
総合解説：権限・承認経路を事前定義すると、重大事象での迅速性と統制を両立できる。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q006 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

24時間対応が必要な組織で、CSIRTの連絡体制として最も適切な設計はどれか。
ア．代表者1名の個人携帯だけを唯一の連絡手段とする。
イ．一次連絡先と代替連絡先、時間外の当番・呼出し、連絡不能時のエスカレーション経路を定義する。
ウ．平日日中のメール受信だけで運用する。
エ．緊急連絡先を文書化せず、担当者同士の記憶に任せる。

正答・4肢解説・総合解説

正答：イ．一次連絡先と代替連絡先、時間外の当番・呼出し、連絡不能時のエスカレーション経路を定義する。
ア：1名・1端末への依存は可用性が低い。
イ：単一障害点を避け、時間外でも必要な担当へ到達できる冗長な連絡設計が重要である。
ウ：24時間要件に対して平日日中だけでは不足する。
エ：属人的な記憶は引継ぎや緊急時に機能しにくい。
総合解説：単一障害点を避け、時間外でも必要な担当へ到達できる冗長な連絡設計が重要である。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q007 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

重大インシデント対応でCSIRTだけでは判断できない事項が生じた。最も適切な対応はどれか。
ア．CSIRTだけで法的義務や対外公表を最終決定する。
イ．技術調査が終わるまで他部門には一切知らせない。
ウ．法務、広報、個人情報保護、事業部門、経営層など必要な関係者を事前定義した体制に基づき招集する。
エ．関係者を毎回その場で探し、役割は決めない。

正答・4肢解説・総合解説

正答：ウ．法務、広報、個人情報保護、事業部門、経営層など必要な関係者を事前定義した体制に基づき招集する。
ア：法的・広報上の決定権は通常CSIRT単独にはない。
イ：早期の連携が必要な事案では、調査完了まで秘匿すると対応が遅れる。
ウ：インシデント対応は技術だけで完結せず、法務・広報・事業継続など横断的な判断が必要になる。
エ：事前の役割定義がないと招集と意思決定が遅れる。
総合解説：インシデント対応は技術だけで完結せず、法務・広報・事業継続など横断的な判断が必要になる。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q008 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTの訓練として、実運用上の弱点を発見しやすいものはどれか。
ア．規程を作成した後は演習を行わない。
イ．セキュリティ担当者だけが用語集を暗記する。
ウ．過去のインシデント報告書を保管するだけで訓練とみなす。
エ．実際の連絡網、判断基準、技術手順、経営層への報告まで含めた机上演習や実動演習を定期的に行う。

正答・4肢解説・総合解説

正答：エ．実際の連絡網、判断基準、技術手順、経営層への報告まで含めた机上演習や実動演習を定期的に行う。
ア：文書化だけでは実行時の問題を検証できない。
イ：用語学習だけでは連携や意思決定を検証できない。
ウ：報告書の保管は学習資源にはなるが、訓練そのものではない。
エ：演習は手順の実行可能性、連絡の遅延、役割の曖昧さなどを事前に発見する手段になる。
総合解説：演習は手順の実行可能性、連絡の遅延、役割の曖昧さなどを事前に発見する手段になる。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q009 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTのサービス対象（コンスティチュエンシー）を明確にする効果として最も適切なものはどれか。
ア．どの組織・システム・利用者からの事象を受け付け、誰にどのサービスを提供するかの境界を明確にできる。
イ．攻撃者の身元を必ず特定できる。
ウ．すべてのインシデントを同じ優先度にできる。
エ．CSIRTが外部機関との連携を禁止できる。

正答・4肢解説・総合解説

正答：ア．どの組織・システム・利用者からの事象を受け付け、誰にどのサービスを提供するかの境界を明確にできる。
ア：サービス対象の定義は受付範囲と責任境界を明確にし、期待値調整にも役立つ。
イ：攻撃者特定は別の調査課題であり保証されない。
ウ：優先度は影響や緊急性で変える必要がある。
エ：外部連携の要否とは別概念である。
総合解説：サービス対象の定義は受付範囲と責任境界を明確にし、期待値調整にも役立つ。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q010 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

PSIRTが製品脆弱性の外部報告を受け付ける仕組みを整備する際、最も重要な設計はどれか。
ア．報告者の氏名が不明なら全て自動破棄する。
イ．報告窓口、受付後の評価・担当割当て、開発部門との連携、修正版やアドバイザリ公開までのプロセスを定義する。
ウ．脆弱性報告は営業部門だけで処理し、開発部門には伝えない。
エ．修正版ができる前に影響確認なしで全情報を公開する。

正答・4肢解説・総合解説

正答：イ．報告窓口、受付後の評価・担当割当て、開発部門との連携、修正版やアドバイザリ公開までのプロセスを定義する。
ア：匿名・仮名報告でも有用な情報が含まれる可能性があり、一律破棄は不適切である。
イ：PSIRTは受領から評価、修正調整、情報提供までを一貫して扱える体制が必要である。
ウ：技術評価や修正には開発部門との連携が必要である。
エ：公開時期や内容はリスクと調整を踏まえて判断する。
総合解説：PSIRTは受領から評価、修正調整、情報提供までを一貫して扱える体制が必要である。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q011 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTの活動指標を設計する考え方として最も適切なものはどれか。
ア．件数が多いほどCSIRTの品質が高いと一律に評価する。
イ．平均対応時間だけを唯一のKPIとし、重大度は考慮しない。
ウ．受付件数だけでなく、検知・対応の所要時間、再発、サービス品質、関係者満足など複数の観点を使命に合わせて用いる。
エ．測定可能な指標は運用を硬直化させるため一切持たない。

正答・4肢解説・総合解説

正答：ウ．受付件数だけでなく、検知・対応の所要時間、再発、サービス品質、関係者満足など複数の観点を使命に合わせて用いる。
ア：件数は攻撃状況や検知能力にも左右され、品質そのものではない。
イ：重大度を無視した平均時間だけでは適切な評価にならない。
ウ：単一指標は誤った行動を誘発し得るため、目的とサービスに対応した複数指標で改善を見る。
エ：測定は継続改善の材料になるため、適切に設計すべきである。
総合解説：単一指標は誤った行動を誘発し得るため、目的とサービスに対応した複数指標で改善を見る。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q012 6-1 CSIRT・初動対応 / CSIRT・PSIRT体制

CSIRTの体制変更後に最も優先して実施すべき確認はどれか。
ア．旧連絡網を残したまま、利用者には変更を知らせない。
イ．役職名だけ変更し、権限や手順は確認しない。
ウ．インシデントが実際に起きるまで新体制を試さない。
エ．新しい役割分担、連絡先、権限、エスカレーション経路が文書と実運用の双方で機能するかを演習で確認する。

正答・4肢解説・総合解説

正答：エ．新しい役割分担、連絡先、権限、エスカレーション経路が文書と実運用の双方で機能するかを演習で確認する。
ア：旧情報の放置は誤連絡や対応遅延の原因になる。
イ：名称だけでなく権限・責任・手順の整合が必要である。
ウ：本番事故を最初のテストにするのはリスクが高い。
エ：体制変更は連絡断や権限の空白を生みやすいため、文書更新と演習による検証が必要である。
総合解説：体制変更は連絡断や権限の空白を生みやすいため、文書更新と演習による検証が必要である。 CSIRT/PSIRT体制では、使命・対象・権限・役割分担を平常時に明確化し、演習と指標で運用能力を改善することが重要である。

Q013 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

セキュリティ監視で異常な通信を検知した。トリアージの最初の目的として最も適切なものはどれか。
ア．事象がインシデントに該当する可能性、影響範囲、緊急性、必要な初動を短時間で評価する。
イ．原因を完全に特定するまで対応を開始しない。
ウ．全ての事象を重大インシデントとして扱う。
エ．ログを削除して誤検知かどうかを確認する。

正答・4肢解説・総合解説

正答：ア．事象がインシデントに該当する可能性、影響範囲、緊急性、必要な初動を短時間で評価する。
ア：トリアージは限られた情報で優先順位と次の行動を決めるための初期評価である。
イ：完全な原因究明は後続調査で行うもので、初動を遅らせてはならない。
ウ：一律に重大扱いすると資源配分を誤る。
エ：ログ削除は調査・証拠保全を損なう。
総合解説：トリアージは限られた情報で優先順位と次の行動を決めるための初期評価である。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q014 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

同時に三つのアラートが発生した。優先順位付けで最も重視すべき観点はどれか。
ア．アラートが発生した時刻の早い順だけで処理する。
イ．業務への影響、対象資産の重要度、被害拡大の可能性、攻撃の進行状況などを総合する。
ウ．検知製品の画面上で赤色のものだけを処理する。
エ．担当者が詳しい技術のアラートを優先する。

正答・4肢解説・総合解説

正答：イ．業務への影響、対象資産の重要度、被害拡大の可能性、攻撃の進行状況などを総合する。
ア：先着順だけでは重大事象を後回しにする可能性がある。
イ：優先度は組織への影響と緊急性に基づいて決めるべきである。
ウ：製品表示は参考情報であり、組織の事業影響を直接表すとは限らない。
エ：担当者の得意分野ではなくリスクに基づいて判断する。
総合解説：優先度は組織への影響と緊急性に基づいて決めるべきである。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q015 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

EDRが重要サーバで不審なPowerShell実行を検知したが、現時点で被害は確認できていない。最も適切なトリアージはどれか。
ア．被害が確認できないので自動的に誤検知と判断する。
イ．重要サーバなので証拠を確認せず直ちに初期化する。
ウ．サーバの重要度、実行元、親子プロセス、通信先、認証状況などを確認し、悪性の可能性と影響を評価する。
エ．PowerShellは正規機能なので調査不要とする。

正答・4肢解説・総合解説

正答：ウ．サーバの重要度、実行元、親子プロセス、通信先、認証状況などを確認し、悪性の可能性と影響を評価する。
ア：被害未確認は無害を意味しない。
イ：初期化は証拠と業務影響を失うため、適切な判断・保全なしに行うべきではない。
ウ：正規ツールの悪用もあり得るため、文脈を確認して悪性度と影響を評価する。
エ：正規ツールでも攻撃に利用され得る。
総合解説：正規ツールの悪用もあり得るため、文脈を確認して悪性度と影響を評価する。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q016 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

同じ攻撃元から複数端末に似たアラートが発生している。トリアージで最も適切な対応はどれか。
ア．各端末を互いに無関係として別々に閉じる。
イ．最初の1台だけ調べ、他は無視する。
ウ．アラート件数が多いので全て誤検知とみなす。
エ．個別アラートだけでなく、共通IOC、時間帯、利用アカウント、通信先を相関し、一つの侵害キャンペーンとしての広がりを確認する。

正答・4肢解説・総合解説

正答：エ．個別アラートだけでなく、共通IOC、時間帯、利用アカウント、通信先を相関し、一つの侵害キャンペーンとしての広がりを確認する。
ア：関連性を無視すると横展開を見逃す。
イ：1台だけではスコープを過小評価し得る。
ウ：件数の多さは誤検知の根拠にならない。
エ：相関により同一攻撃の範囲や侵入経路を早く把握できる可能性がある。
総合解説：相関により同一攻撃の範囲や侵入経路を早く把握できる可能性がある。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q017 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

ランサムウェアによるファイル暗号化が継続中であることを確認した。トリアージ上の扱いとして最も適切なものはどれか。
ア．被害が進行中で拡大可能性が高いため、重大度を高く評価し、封じ込めを含む緊急対応へ移す。
イ．暗号化完了まで待ってから調査する。
ウ．身代金額が判明するまで優先度を決めない。
エ．バックアップがあるので低優先度とする。

正答・4肢解説・総合解説

正答：ア．被害が進行中で拡大可能性が高いため、重大度を高く評価し、封じ込めを含む緊急対応へ移す。
ア：進行中の破壊・暗号化は影響拡大を止める必要があり、高い緊急性を持つ。
イ：待機すれば被害が増える可能性がある。
ウ：身代金額は重要情報になり得るが、進行中被害の優先判断を待つ理由にはならない。
エ：バックアップがあっても侵害拡大や情報窃取の可能性がある。
総合解説：進行中の破壊・暗号化は影響拡大を止める必要があり、高い緊急性を持つ。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q018 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

トリアージで「影響は大きいが、攻撃が停止しており拡大兆候がない事象」と「影響はまだ小さいが、急速に横展開中の事象」を比較する際に適切な考え方はどれか。
ア．現在の被害額だけで機械的に決める。
イ．現在の影響だけでなく、被害拡大の速度や将来影響も含めて優先度を判断する。
ウ．検知時刻の早い方を必ず優先する。
エ．影響がまだ小さい事象は常に後回しにする。

正答・4肢解説・総合解説

正答：イ．現在の影響だけでなく、被害拡大の速度や将来影響も含めて優先度を判断する。
ア：被害額単独では緊急性を捉えられない。
イ：優先度は影響と緊急性の双方で見る必要があり、進行中の拡大は重要な判断材料である。
ウ：先着順はリスクベースの優先付けではない。
エ：小さい現時点影響でも急速拡大中なら高優先度になり得る。
総合解説：優先度は影響と緊急性の双方で見る必要があり、進行中の拡大は重要な判断材料である。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q019 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

重大度分類の基準を平常時に定義しておく利点として最も適切なものはどれか。
ア．すべての事象を自動的に同じ手順で処理できる。
イ．誤検知を完全になくせる。
ウ．担当者ごとの判断ばらつきを抑え、必要な対応レベルやエスカレーションを迅速に決めやすくする。
エ．攻撃者を自動的に特定できる。

正答・4肢解説・総合解説

正答：ウ．担当者ごとの判断ばらつきを抑え、必要な対応レベルやエスカレーションを迅速に決めやすくする。
ア：重大度に応じて手順は変わり得るため、完全に同一化するものではない。
イ：誤検知は残り得る。
ウ：明文化された基準は一貫したトリアージと迅速な連携に役立つ。
エ：重大度基準は攻撃者帰属を自動化しない。
総合解説：明文化された基準は一貫したトリアージと迅速な連携に役立つ。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q020 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

クラウド管理者アカウントで通常と異なる地域からのログインを検知した。最も適切な初期評価はどれか。
ア．地域が異なるだけで直ちにアカウントを削除する。
イ．MFA成功なら侵害は絶対にないと判断する。
ウ．ログイン成功なので正常とみなす。
エ．本人利用の可能性を確認しつつ、認証ログ、MFA結果、操作履歴、権限、関連セッションを確認して侵害の可能性を評価する。

正答・4肢解説・総合解説

正答：エ．本人利用の可能性を確認しつつ、認証ログ、MFA結果、操作履歴、権限、関連セッションを確認して侵害の可能性を評価する。
ア：削除は業務影響が大きく、事実確認と適切な封じ込め判断が必要である。
イ：MFAもフィッシングやセッショントークン窃取などで突破される可能性がある。
ウ：成功ログイン自体が侵害結果である場合もある。
エ：異常な地域は手掛かりであり、他の認証・操作情報と合わせて判断する。
総合解説：異常な地域は手掛かりであり、他の認証・操作情報と合わせて判断する。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q021 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

脆弱性スキャナが多数の古い脆弱性を報告したが、同時に外部公開サーバで実際の悪用痕跡が見つかった。インシデント対応の優先判断として最も適切なものはどれか。
ア．実際の悪用痕跡がある対象を侵害の可能性が高いものとして優先調査し、並行して他対象への横展開も確認する。
イ．CVSSが最も高い古い脆弱性だけを調べる。
ウ．スキャナの件数が多いので悪用痕跡は無視する。
エ．全脆弱性の修正が終わるまで侵害調査を開始しない。

正答・4肢解説・総合解説

正答：ア．実際の悪用痕跡がある対象を侵害の可能性が高いものとして優先調査し、並行して他対象への横展開も確認する。
ア：実悪用の証拠は緊急性が高く、影響範囲の確認が必要である。
イ：CVSSは重要な参考だが、実悪用・資産重要度・露出状況も考慮する。
ウ：件数の多さは侵害証拠を軽視する理由にならない。
エ：修正だけでは侵害の有無や残存アクセスを確認できない。
総合解説：実悪用の証拠は緊急性が高く、影響範囲の確認が必要である。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q022 6-1 CSIRT・初動対応 / トリアージ・優先順位付け

トリアージ結果が「情報不足」で判断不能だった場合の最も適切な対応はどれか。
ア．情報不足なのでチケットを閉じる。
イ．判断に必要な追加ログや関係者情報を特定して収集し、暫定的なリスクに応じて監視・隔離などの予防的措置も検討する。
ウ．結論が出るまで一切の対策を禁止する。
エ．担当者の直感だけで正常と記録する。

正答・4肢解説・総合解説

正答：イ．判断に必要な追加ログや関係者情報を特定して収集し、暫定的なリスクに応じて監視・隔離などの予防的措置も検討する。
ア：情報不足は無害の根拠ではない。
イ：不確実性自体を管理し、必要な追加情報と暫定措置を明確にすることが重要である。
ウ：高リスクなら調査中でも合理的な暫定対策が必要になる。
エ：判断根拠を記録せず直感だけで閉じるのは追跡性がない。
総合解説：不確実性自体を管理し、必要な追加情報と暫定措置を明確にすることが重要である。 トリアージでは、確認済み事実と不確実性を整理し、事業影響・緊急性・被害拡大可能性を踏まえて優先度と次の行動を決める。

Q023 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

インシデント連絡・報告フローを事前に定める際、最も重要な要素はどれか。
ア．担当者が都度自由に連絡先を決める。
イ．全ての事象を社外へ即時公開する。
ウ．事象の重大度や種類ごとに、誰が誰へ、どの期限・手段で、何を報告するかを定める。
エ．技術担当者だけに情報を限定し、経営層への経路は設けない。

正答・4肢解説・総合解説

正答：ウ．事象の重大度や種類ごとに、誰が誰へ、どの期限・手段で、何を報告するかを定める。
ア：都度判断だけでは属人化し、重要な連絡漏れが起きやすい。
イ：公開要否は法令・契約・影響などに基づいて判断する。
ウ：報告先・条件・内容・手段を事前定義すると、緊急時の迷いと遅延を減らせる。
エ：重大事象では経営判断が必要な場合があり、経営層への経路も必要である。
総合解説：報告先・条件・内容・手段を事前定義すると、緊急時の迷いと遅延を減らせる。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q024 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

侵害が疑われるメールシステムについて、攻撃者が社内メールを閲覧できる可能性がある。CSIRTの連絡手段として最も適切なものはどれか。
ア．通常の社内メールだけを使い続ける。
イ．公開SNSで調査内容を共有する。
ウ．連絡を全て停止し、復旧後にまとめて伝える。
エ．侵害の影響を受けていないことを確認した代替チャネルを用いて、必要な関係者と連絡する。

正答・4肢解説・総合解説

正答：エ．侵害の影響を受けていないことを確認した代替チャネルを用いて、必要な関係者と連絡する。
ア：攻撃者に対応状況を知られる可能性がある。
イ：公開SNSは機微情報の漏えいにつながる。
ウ：必要な連絡を止めると封じ込めや意思決定が遅れる。
エ：通常チャネル自体が侵害されている可能性がある場合、独立した安全な連絡経路が必要である。
総合解説：通常チャネル自体が侵害されている可能性がある場合、独立した安全な連絡経路が必要である。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q025 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

インシデント発生直後、原因がまだ確定していない段階で経営層へ報告する内容として最も適切なものはどれか。
ア．確認済み事実、未確認事項、現時点の影響評価、実施中の対応、次回更新予定を区別して報告する。
イ．推測を確定事実として断定する。
ウ．原因が完全に確定するまで何も報告しない。
エ．技術ログを説明なしで全件転送するだけにする。

正答・4肢解説・総合解説

正答：ア．確認済み事実、未確認事項、現時点の影響評価、実施中の対応、次回更新予定を区別して報告する。
ア：事実と仮説を分け、意思決定に必要な情報と不確実性を明示することが重要である。
イ：誤った断定は判断や対外説明を誤らせる。
ウ：重大事案では早期の状況共有が必要である。
エ：経営層には影響や判断事項を整理して伝える必要がある。
総合解説：事実と仮説を分け、意思決定に必要な情報と不確実性を明示することが重要である。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q026 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

顧客情報漏えいの可能性があるインシデントで、外部報告の要否を判断する最も適切な方法はどれか。
ア．CSIRT担当者の経験だけで決める。
イ．適用法令、監督官庁の要求、契約上の通知義務、影響範囲を法務・関係部門と確認する。
ウ．技術的に復旧できれば外部報告は不要とする。
エ．顧客から問い合わせが来るまで検討しない。

正答・4肢解説・総合解説

正答：イ．適用法令、監督官庁の要求、契約上の通知義務、影響範囲を法務・関係部門と確認する。
ア：個人の経験だけでは法的・契約上の義務を見落とす。
イ：外部報告義務は事案・法令・契約で異なるため、法務等と確認して判断する。
ウ：復旧と通知義務は別問題である。
エ：期限付きの通知義務がある場合、問い合わせ待ちでは遅れる。
総合解説：外部報告義務は事案・法令・契約で異なるため、法務等と確認して判断する。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q027 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

重大インシデントのエスカレーション基準として最も適切な設計はどれか。
ア．担当者の気分で毎回決める。
イ．金銭被害が確定した場合だけに限定する。
ウ．重要サービス停止、機密情報流出、法令・契約影響、被害拡大可能性など、経営判断が必要になる条件を具体化する。
エ．技術担当者が解決不能になった時だけ上げる。

正答・4肢解説・総合解説

正答：ウ．重要サービス停止、機密情報流出、法令・契約影響、被害拡大可能性など、経営判断が必要になる条件を具体化する。
ア：属人的な基準は一貫性を欠く。
イ：金銭以外にも重大な影響はある。
ウ：事業・法令・社会的影響を含む条件を明確にすると、重大事案を適時に上位判断へつなげられる。
エ：技術解決の可否だけでなく、経営判断が必要な事案は早期エスカレーションすべきである。
総合解説：事業・法令・社会的影響を含む条件を明確にすると、重大事案を適時に上位判断へつなげられる。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q028 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

複数の部門がインシデント状況を別々の表計算ファイルで管理し、内容が食い違っている。改善策として最も適切なものはどれか。
ア．各部門の記録を統合せず、そのまま対外発表に使う。
イ．最も新しそうなファイルを毎回勘で選ぶ。
ウ．記録を残さず口頭連絡だけに切り替える。
エ．承認されたインシデント管理記録を単一の正本として定め、更新責任と共有範囲を明確にする。

正答・4肢解説・総合解説

正答：エ．承認されたインシデント管理記録を単一の正本として定め、更新責任と共有範囲を明確にする。
ア：矛盾した情報をそのまま使うと誤報につながる。
イ：選定根拠がなく再現性がない。
ウ：口頭だけでは追跡性と引継ぎ性が低下する。
エ：単一の信頼できる記録を設けると、状況認識と意思決定の不整合を抑えられる。
総合解説：単一の信頼できる記録を設けると、状況認識と意思決定の不整合を抑えられる。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q029 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

夜間の重大インシデントで担当交代が必要になった。引継ぎとして最も適切なものはどれか。
ア．確認済み事実、未解決事項、実施済み対応、保全済み証拠、次の判断点を記録し、後任と確認する。
イ．口頭で「だいたい対応済み」とだけ伝える。
ウ．調査中の仮説だけを事実として引き継ぐ。
エ．前任者の端末にしか記録を残さない。

正答・4肢解説・総合解説

正答：ア．確認済み事実、未解決事項、実施済み対応、保全済み証拠、次の判断点を記録し、後任と確認する。
ア：構造化した引継ぎは対応の重複・漏れ・誤認を減らす。
イ：曖昧な口頭説明では重要情報が失われる。
ウ：仮説と事実の混同は誤判断につながる。
エ：共有できない個人端末だけの記録は継続性が低い。
総合解説：構造化した引継ぎは対応の重複・漏れ・誤認を減らす。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q030 6-1 CSIRT・初動対応 / 連絡・報告・エスカレーション

外部CSIRTやJPCERT/CCなどと連携する際の情報共有として最も適切なものはどれか。
ア．内部ログを無条件で全て公開する。
イ．共有目的と必要性を確認し、機密性・個人情報・契約上の制約を考慮して必要な範囲の情報を安全に共有する。
ウ．外部機関とは一切情報共有しない。
エ．情報の正確性を確認せず、推測も含めて拡散する。

正答・4肢解説・総合解説

正答：イ．共有目的と必要性を確認し、機密性・個人情報・契約上の制約を考慮して必要な範囲の情報を安全に共有する。
ア：無条件の全量公開は機密・個人情報などの問題を生む。
イ：外部連携は有効だが、共有範囲・取扱い・正確性を管理する必要がある。
ウ：連携を禁止すると支援や脅威情報を活用できない。
エ：未確認情報の拡散は混乱と誤対応を招く。
総合解説：外部連携は有効だが、共有範囲・取扱い・正確性を管理する必要がある。 連絡・報告では、事実と仮説を分け、重大度に応じた報告先・手段・期限を事前定義して追跡可能な形で共有する。

Q031 6-2 インシデント分析 / ログ・ネットワーク調査

複数機器のログを突合する際に、最初に確認すべき事項として最も適切なものはどれか。
ア．ログ件数の多い機器だけを残す。
イ．時刻の差は無視して文字列順に並べる。
ウ．各機器の時刻同期状況、タイムゾーン、ログ時刻の基準を確認し、同一の時間軸で比較できるようにする。
エ．最も新しいログだけを使い、古いログは捨てる。

正答・4肢解説・総合解説

正答：ウ．各機器の時刻同期状況、タイムゾーン、ログ時刻の基準を確認し、同一の時間軸で比較できるようにする。
ア：件数だけで重要性は判断できず、必要な証拠を失う。
イ：時刻差を無視すると相関分析を誤る。
ウ：時刻がずれていると、因果関係や攻撃順序を誤って判断するため、時間軸の正規化が重要である。
エ：攻撃の前後関係を確認するには過去ログも必要である。
総合解説：時刻がずれていると、因果関係や攻撃順序を誤って判断するため、時間軸の正規化が重要である。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q032 6-2 インシデント分析 / ログ・ネットワーク調査

フィッシング後の侵害範囲を調べる際、エンドポイント、DNS、プロキシのログを組み合わせる主な利点はどれか。
ア．一つのログだけで攻撃者本人を法的に特定できる。
イ．複数ログを使うと必ず誤検知がゼロになる。
ウ．DNSログだけで端末上の全プロセスを復元できる。
エ．端末上の実行、名前解決、外部通信を時系列で関連付け、感染端末や通信先を多面的に確認できる。

正答・4肢解説・総合解説

正答：エ．端末上の実行、名前解決、外部通信を時系列で関連付け、感染端末や通信先を多面的に確認できる。
ア：ログは有力な証拠だが、攻撃者個人の法的特定を自動保証しない。
イ：複数証拠でも誤検知の可能性は残る。
ウ：DNSログは名前解決を示すが、端末上の全プロセスは示さない。
エ：異なる観測点を組み合わせることで単一ログでは見えない攻撃経路や範囲を補完できる。
総合解説：異なる観測点を組み合わせることで単一ログでは見えない攻撃経路や範囲を補完できる。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q033 6-2 インシデント分析 / ログ・ネットワーク調査

FWログに外部IPアドレスへの通信が記録されていた。NAT環境で送信元端末を特定するために追加で重要となる情報はどれか。
ア．当該時刻のNAT変換ログや内部送信元IP・ポートの対応情報。
イ．外部IPアドレスのWHOIS情報だけ。
ウ．FWの製造年月日。
エ．宛先国の時差だけ。

正答・4肢解説・総合解説

正答：ア．当該時刻のNAT変換ログや内部送信元IP・ポートの対応情報。
ア：NAT越しでは複数端末が同じグローバルIPを共有し得るため、時刻とポートを含む変換対応が必要になる。
イ：WHOISは外部宛先の情報であり、内部端末の特定には不足する。
ウ：製造年月日は通信元特定に直接関係しない。
エ：時差だけでは内部端末を識別できない。
総合解説：NAT越しでは複数端末が同じグローバルIPを共有し得るため、時刻とポートを含む変換対応が必要になる。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q034 6-2 インシデント分析 / ログ・ネットワーク調査

DHCPを利用する社内ネットワークで、過去のある時刻に特定IPアドレスを使っていた端末を調べたい。最も有用な情報はどれか。
ア．現在のIPアドレス一覧だけを見る。
イ．DHCPのリース記録と端末識別情報を対象時刻に対応付ける。
ウ．DNSの外部権威サーバのSOAレコードだけを見る。
エ．ルータの機種名だけを見る。

正答・4肢解説・総合解説

正答：イ．DHCPのリース記録と端末識別情報を対象時刻に対応付ける。
ア：現在の割当ては過去時点と異なる可能性がある。
イ：DHCP環境ではIP割当てが時間で変わるため、過去時点のリース記録が端末対応付けに重要である。
ウ：SOAレコードは内部端末のDHCP割当てを示さない。
エ：機種名から利用端末は特定できない。
総合解説：DHCP環境ではIP割当てが時間で変わるため、過去時点のリース記録が端末対応付けに重要である。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q035 6-2 インシデント分析 / ログ・ネットワーク調査

ネットワーク調査でフルパケットキャプチャとフローデータを比較した説明として最も適切なものはどれか。
ア．フローデータには常にHTTP本文まで全て保存される。
イ．フルパケットは通信相手のIPアドレスを記録できない。
ウ．フルパケットは通信内容を詳細に確認できる可能性がある一方、フローデータは通信の組合せや量などを比較的少ない容量で把握しやすい。
エ．両者は保存する情報が完全に同一である。

正答・4肢解説・総合解説

正答：ウ．フルパケットは通信内容を詳細に確認できる可能性がある一方、フローデータは通信の組合せや量などを比較的少ない容量で把握しやすい。
ア：一般的なフローデータは通信メタデータ中心で、本文全体を保持しない。
イ：フルパケットには通常IPヘッダなども含まれる。
ウ：両者は粒度と保存コストが異なり、目的に応じて使い分ける。
エ：保持情報は同一ではない。
総合解説：両者は粒度と保存コストが異なり、目的に応じて使い分ける。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q036 6-2 インシデント分析 / ログ・ネットワーク調査

DNSログで、端末が短時間に多数のランダム文字列のサブドメインを問い合わせている。調査として最も適切なものはどれか。
ア．ランダム文字列だけを根拠に即座にDGAと断定する。
イ．DNSログは攻撃調査に使えないので無視する。
ウ．問い合わせ先が応答していれば正常と判断する。
エ．正常な業務・CDN等の可能性も考慮しつつ、端末プロセス、問い合わせ先ドメイン、頻度、他端末の状況を相関して異常性を評価する。

正答・4肢解説・総合解説

正答：エ．正常な業務・CDN等の可能性も考慮しつつ、端末プロセス、問い合わせ先ドメイン、頻度、他端末の状況を相関して異常性を評価する。
ア：類似挙動は正規サービスでも起こり得るため断定は早い。
イ：DNSログは外部通信やC2候補の調査に有用である。
ウ：応答有無だけでは正当性を判断できない。
エ：特徴的なDNS挙動は手掛かりになるが、文脈を相関して判断する必要がある。
総合解説：特徴的なDNS挙動は手掛かりになるが、文脈を相関して判断する必要がある。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q037 6-2 インシデント分析 / ログ・ネットワーク調査

Webプロキシログからマルウェアの外部通信を調べる際、確認項目として最も適切なものはどれか。
ア．送信元端末・利用者、宛先URL/ドメイン、時刻、HTTPメソッド、応答コード、転送量などを相関する。
イ．プロキシの設置場所の床面積だけを確認する。
ウ．HTTP応答コードだけで感染端末を確定する。
エ．利用者情報は調査に不要なので常に破棄する。

正答・4肢解説・総合解説

正答：ア．送信元端末・利用者、宛先URL/ドメイン、時刻、HTTPメソッド、応答コード、転送量などを相関する。
ア：複数の属性を組み合わせると、異常な宛先や通信パターンと端末・利用者を関連付けやすい。
イ：物理的な床面積は通信調査に関係しない。
ウ：応答コード単独では感染を確定できない。
エ：適法かつ必要な範囲で利用者との対応付けが重要な場合がある。
総合解説：複数の属性を組み合わせると、異常な宛先や通信パターンと端末・利用者を関連付けやすい。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q038 6-2 インシデント分析 / ログ・ネットワーク調査

FWの拒否ログが大量にあるが、侵入成功の有無を判断したい。最も適切な考え方はどれか。
ア．拒否ログがあれば侵入成功は絶対にない。
イ．拒否ログだけでなく、許可通信、サーバ・認証・EDRなどのログも確認して成功した通信や後続活動を調べる。
ウ．拒否ログの件数が多ければ必ず侵入済みである。
エ．FWログを削除して新しいログだけを見る。

正答・4肢解説・総合解説

正答：イ．拒否ログだけでなく、許可通信、サーバ・認証・EDRなどのログも確認して成功した通信や後続活動を調べる。
ア：FW以外の経路や許可ルールが存在し得る。
イ：拒否ログは遮断した試行を示すにとどまり、別経路や許可通信で成功していないか確認が必要である。
ウ：試行件数だけでは侵入成功を示さない。
エ：過去ログ削除は調査を妨げる。
総合解説：拒否ログは遮断した試行を示すにとどまり、別経路や許可通信で成功していないか確認が必要である。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q039 6-2 インシデント分析 / ログ・ネットワーク調査

なりすましメールの送信経路を調査する際、メール本文以外で有用な情報はどれか。
ア．添付ファイルの表示名だけを見る。
イ．件名の文字数だけで送信者を断定する。
ウ．Receivedヘッダ、Message-ID、認証結果、送信元関連ヘッダなどを確認し、経路と認証状況を分析する。
エ．受信者のメールソフトの壁紙設定を調べる。

正答・4肢解説・総合解説

正答：ウ．Receivedヘッダ、Message-ID、認証結果、送信元関連ヘッダなどを確認し、経路と認証状況を分析する。
ア：表示名は容易に偽装でき、単独では不十分である。
イ：件名の長さから送信者は特定できない。
ウ：メールヘッダには配送経路や認証結果など調査に有用な情報が含まれる。
エ：壁紙設定は送信経路に関係しない。
総合解説：メールヘッダには配送経路や認証結果など調査に有用な情報が含まれる。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q040 6-2 インシデント分析 / ログ・ネットワーク調査

TLSで暗号化された外部通信をネットワーク側から調査する場合、復号できなくても利用できる情報として最も適切なものはどれか。
ア．暗号化されていれば一切の調査は不可能である。
イ．暗号化通信は全て正常とみなす。
ウ．TLSの利用だけを根拠にマルウェア通信と断定する。
エ．接続先IP、ポート、通信時刻、通信量、接続頻度などのメタデータを他ログと相関する。

正答・4肢解説・総合解説

正答：エ．接続先IP、ポート、通信時刻、通信量、接続頻度などのメタデータを他ログと相関する。
ア：暗号化は内容可視性を下げるが調査手段を全て失わせるわけではない。
イ：攻撃者も正規利用者もTLSを使う。
ウ：TLS利用だけでは悪性の根拠にならない。
エ：本文が見えなくても、通信メタデータや端末側ログから挙動を分析できる。
総合解説：本文が見えなくても、通信メタデータや端末側ログから挙動を分析できる。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q041 6-2 インシデント分析 / ログ・ネットワーク調査

侵害端末から別セグメントへの横展開が疑われる。ネットワーク調査として最も適切なものはどれか。
ア．境界FW、認証、EDR、フロー等から対象端末の通信先と認証利用を確認し、関連端末へ調査範囲を広げる。
イ．侵害端末の画面だけを見て終了する。
ウ．外部インターネット通信だけ調べ、内部通信は除外する。
エ．横展開の可能性は復旧後まで調べない。

正答・4肢解説・総合解説

正答：ア．境界FW、認証、EDR、フロー等から対象端末の通信先と認証利用を確認し、関連端末へ調査範囲を広げる。
ア：横展開では内部通信・認証・端末挙動の相関が重要で、スコープ拡大を確認する必要がある。
イ：画面表示だけでは内部活動を把握できない。
ウ：内部通信が主要な手掛かりになる場合がある。
エ：復旧前に範囲を把握しないと再侵害につながる。
総合解説：横展開では内部通信・認証・端末挙動の相関が重要で、スコープ拡大を確認する必要がある。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q042 6-2 インシデント分析 / ログ・ネットワーク調査

SIEMで「外部からのVPNログイン→特権昇格→大量データ転送」の相関ルールが発報した。最も適切な初動調査はどれか。
ア．相関ルールが発報したので侵害確定として証拠確認を省略する。
イ．各イベントの時刻、同一利用者・端末か、転送先、正当な業務変更の有無を確認し、一連の侵害シナリオとして評価する。
ウ．大量転送だけを単独で見て他イベントを無視する。
エ．ルール名だけを変更してアラートを閉じる。

正答・4肢解説・総合解説

正答：イ．各イベントの時刻、同一利用者・端末か、転送先、正当な業務変更の有無を確認し、一連の侵害シナリオとして評価する。
ア：ルールは誤検知し得るため裏付けが必要である。
イ：相関アラートは有力な手掛かりだが、関連イベントの整合と業務文脈を確認して判断する。
ウ：一連の流れを捉えることが相関分析の価値である。
エ：名前変更は事象評価にならない。
総合解説：相関アラートは有力な手掛かりだが、関連イベントの整合と業務文脈を確認して判断する。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q043 6-2 インシデント分析 / ログ・ネットワーク調査

パケットキャプチャで通信の片方向しか確認できない。原因として考慮すべきものはどれか。
ア．TCP通信では必ず片方向しか流れない。
イ．暗号化を使うと復路パケットが消える。
ウ．非対称ルーティングや取得位置の違いにより、往路と復路が別経路を通っている可能性。
エ．DNSを利用すると片方向通信になる。

正答・4肢解説・総合解説

正答：ウ．非対称ルーティングや取得位置の違いにより、往路と復路が別経路を通っている可能性。
ア：TCPは双方向の通信を行う。
イ：暗号化はパケット自体を消さない。
ウ：ネットワーク構成によっては往路と復路が異なるため、観測点で片側しか見えないことがある。
エ：DNS利用が非対称通信を必ず生むわけではない。
総合解説：ネットワーク構成によっては往路と復路が異なるため、観測点で片側しか見えないことがある。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q044 6-2 インシデント分析 / ログ・ネットワーク調査

ログ分析で攻撃時刻の前後だけを極端に狭く切り出すリスクとして最も適切なものはどれか。
ア．ログ容量が必ず増える。
イ．タイムゾーンが自動的に修正される。
ウ．暗号化通信が自動復号される。
エ．侵入準備、認証情報窃取、横展開、持続化など前後に離れて発生した関連活動を見落とす可能性がある。

正答・4肢解説・総合解説

正答：エ．侵入準備、認証情報窃取、横展開、持続化など前後に離れて発生した関連活動を見落とす可能性がある。
ア：切出し範囲を狭めれば容量は通常減る。
イ：時間範囲はタイムゾーン補正を自動化しない。
ウ：ログ期間設定と復号は無関係である。
エ：攻撃は複数段階・長期間に及ぶことがあり、時間範囲を狭めすぎるとスコープを過小評価する。
総合解説：攻撃は複数段階・長期間に及ぶことがあり、時間範囲を狭めすぎるとスコープを過小評価する。 ログ・ネットワーク調査では、時刻・端末・利用者・通信先を複数の観測点で相関し、単一ログの限界を補いながら侵害範囲を特定する。

Q045 6-2 インシデント分析 / マルウェア解析

未知の実行ファイルを解析する際、静的解析と動的解析の組合せとして最も適切なものはどれか。
ア．まずハッシュ、ヘッダ、文字列、インポートなどを静的に確認し、必要に応じて隔離した解析環境で実行挙動を観察する。
イ．本番端末で直接実行し、挙動を見る。
ウ．静的解析だけで必ず全挙動を把握できる。
エ．ファイル名が正常なら解析を終了する。

正答・4肢解説・総合解説

正答：ア．まずハッシュ、ヘッダ、文字列、インポートなどを静的に確認し、必要に応じて隔離した解析環境で実行挙動を観察する。
ア：静的・動的解析は相補的であり、安全な環境で組み合わせると理解を深められる。
イ：本番環境での実行は感染拡大や情報漏えいの危険がある。
ウ：難読化や実行時生成により静的解析だけでは見えない挙動がある。
エ：ファイル名は容易に偽装できる。
総合解説：静的・動的解析は相補的であり、安全な環境で組み合わせると理解を深められる。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q046 6-2 インシデント分析 / マルウェア解析

マルウェア検体を動的解析する環境として最も適切なものはどれか。
ア．社内の重要サーバで直接実行する。
イ．本番環境から隔離し、通信やスナップショットを制御できる専用サンドボックスを使用する。
ウ．個人の私物PCで管理者権限を付けて実行する。
エ．バックアップのない本番端末で挙動を見る。

正答・4肢解説・総合解説

正答：イ．本番環境から隔離し、通信やスナップショットを制御できる専用サンドボックスを使用する。
ア：重要サーバへの直接実行は被害を拡大し得る。
イ：隔離環境なら本番への影響を抑えつつ、プロセス・ファイル・レジストリ・通信などを観察できる。
ウ：私物PCは管理・証拠保全・安全性の面で不適切である。
エ：本番端末での実行はリスクが高い。
総合解説：隔離環境なら本番への影響を抑えつつ、プロセス・ファイル・レジストリ・通信などを観察できる。マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q047 6-2 インシデント分析 / マルウェア解析

あるファイルのSHA-256ハッシュが既知マルウェアと一致した。最も適切な解釈はどれか。
ア．ハッシュ一致だけで全端末が感染したと断定できる。
イ．ハッシュが一致すれば攻撃者の身元まで分かる。
ウ．同一バイト列のファイルである可能性が極めて高く、有力な識別情報になるが、影響範囲や実行有無は別途確認する。
エ．ハッシュ値はファイル内容と無関係なので意味がない。

正答・4肢解説・総合解説

正答：ウ．同一バイト列のファイルである可能性が極めて高く、有力な識別情報になるが、影響範囲や実行有無は別途確認する。
ア：一つの検体一致から全端末感染は導けない。
イ：攻撃者帰属には追加証拠が必要である。
ウ：暗号学的ハッシュはファイル識別に有用だが、感染範囲や実行状況はログ等で確認する必要がある。
エ：ハッシュは内容から計算されるため識別に利用できる。
総合解説：暗号学的ハッシュはファイル識別に有用だが、感染範囲や実行状況はログ等で確認する必要がある。マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q048 6-2 インシデント分析 / マルウェア解析

静的解析で意味のある文字列やインポート情報がほとんど見つからない検体がある。考えられる理由として最も適切なものはどれか。
ア．必ず無害なテキストファイルである。
イ．OSが自動的に解析結果を消去した。
ウ．ハッシュ計算をしたため文字列が消えた。
エ．パッキング、暗号化、難読化により、実行前の状態ではコードや文字列が隠されている可能性がある。

正答・4肢解説・総合解説

正答：エ．パッキング、暗号化、難読化により、実行前の状態ではコードや文字列が隠されている可能性がある。
ア：情報が少ないことは無害の証明ではない。
イ：通常の静的解析でOSが結果を自動消去するわけではない。
ウ：ハッシュ計算は元ファイルを書き換えない。
エ：マルウェアは解析妨害のためパッキングや難読化を使うことがあり、動的解析やアンパックが必要になる場合がある。
総合解説：マルウェアは解析妨害のためパッキングや難読化を使うことがあり、動的解析やアンパックが必要になる場合がある。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q049 6-2 インシデント分析 / マルウェア解析

PE形式の疑わしい実行ファイルを静的解析する際、インポート情報を確認する目的として最も適切なものはどれか。
ア．ファイルが利用しようとするAPIから、ファイル操作、通信、プロセス操作などの機能を推測する手掛かりを得る。
イ．攻撃者の住所を直接特定する。
ウ．ファイルの実行履歴を必ず全て復元する。
エ．証明書がなくても正規ソフトと断定する。

正答・4肢解説・総合解説

正答：ア．ファイルが利用しようとするAPIから、ファイル操作、通信、プロセス操作などの機能を推測する手掛かりを得る。
ア：インポートAPIは機能推測の手掛かりになるが、難読化や動的解決で隠されることもある。
イ：API情報から攻撃者の住所は分からない。
ウ：静的なインポート情報だけで実行履歴は復元できない。
エ：署名や証明書の有無だけで正当性を断定できない。
総合解説：インポートAPIは機能推測の手掛かりになるが、難読化や動的解決で隠されることもある。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q050 6-2 インシデント分析 / マルウェア解析

マルウェア解析で外部ドメインへの定期通信を確認した。インシデント対応への活用として最も適切なものはどれか。
ア．解析端末だけで観察し、他環境には共有しない。
イ．通信先や周期などをIOC・挙動情報として監視に反映し、他端末に同様の通信がないか探索する。
ウ．通信先ドメインが見つかった時点で攻撃者本人を確定する。
エ．ドメイン名だけを根拠に全通信を永久遮断する。

正答・4肢解説・総合解説

正答：イ．通信先や周期などをIOC・挙動情報として監視に反映し、他端末に同様の通信がないか探索する。
ア：他端末調査へ活用しないと被害範囲を見落とす。
イ：解析結果を検知・スコープ調査へ還元すると、同一侵害の横断探索に役立つ。
ウ：インフラ情報だけで攻撃者個人を確定できない。
エ：共有サービス等の可能性もあり、影響評価と更新可能な対策が必要である。
総合解説：解析結果を検知・スコープ調査へ還元すると、同一侵害の横断探索に役立つ。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q051 6-2 インシデント分析 / マルウェア解析

ファイルレスマルウェアが疑われ、ディスク上に明確な実行ファイルが見つからない。調査として最も適切なものはどれか。
ア．ディスクにファイルがないので感染なしと判断する。
イ．端末を直ちに電源断し、メモリ情報を失ってから調べる。
ウ．メモリ、プロセス、コマンド履歴、スクリプト実行、EDRテレメトリなど揮発性・実行時情報を重点的に確認する。
エ．ファイル名検索だけで調査を完了する。

正答・4肢解説・総合解説

正答：ウ．メモリ、プロセス、コマンド履歴、スクリプト実行、EDRテレメトリなど揮発性・実行時情報を重点的に確認する。
ア：ディスク上の実行ファイル不在は無害の証明ではない。
イ：電源断で揮発性情報を失う可能性がある。
ウ：ファイルレス攻撃はメモリや正規ツールを利用するため、実行時情報が重要な証拠になる。
エ：ファイル名検索だけでは把握できない。
総合解説：ファイルレス攻撃はメモリや正規ツールを利用するため、実行時情報が重要な証拠になる。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q052 6-2 インシデント分析 / マルウェア解析

検体が仮想環境では活動せず、実機に近い環境でだけ不審通信を行う。考えられる解析回避として最も適切なものはどれか。
ア．DNSSECによる正規の名前検証。
イ．バックアップの世代管理。
ウ．アクセス制御リストによる通常の認可。
エ．仮想化やサンドボックスの特徴を検出して挙動を変えるアンチVM・アンチサンドボックス機能。

正答・4肢解説・総合解説

正答：エ．仮想化やサンドボックスの特徴を検出して挙動を変えるアンチVM・アンチサンドボックス機能。
ア：DNSSECはDNS応答の検証技術であり解析回避ではない。
イ：世代管理はバックアップ運用である。
ウ：ACLは認可制御でありマルウェアの解析回避とは異なる。
エ：マルウェアは解析環境を検知して休眠するなど、動的解析回避を行うことがある。
総合解説：マルウェアは解析環境を検知して休眠するなど、動的解析回避を行うことがある。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q053 6-2 インシデント分析 / マルウェア解析

マルウェア検体を他の解析担当者へ渡す際に最も適切な取扱いはどれか。
ア．検体を誤実行されにくい安全な形式で暗号化・アクセス制御し、ハッシュ、入手元、日時、取扱履歴を記録して受け渡す。
イ．メール本文に実行ファイルをそのまま添付して全社員へ送る。
ウ．検体名だけ伝え、ハッシュや入手元は記録しない。
エ．検体を共有フォルダの誰でも実行できる場所に置く。

正答・4肢解説・総合解説

正答：ア．検体を誤実行されにくい安全な形式で暗号化・アクセス制御し、ハッシュ、入手元、日時、取扱履歴を記録して受け渡す。
ア：検体は危険物として扱い、誤実行防止と完全性・追跡性を確保する必要がある。
イ：無差別送信は感染リスクを高める。
ウ：識別・追跡情報がないと同一検体か確認しにくい。
エ：広範な実行権限は事故につながる。
総合解説：検体は危険物として扱い、誤実行防止と完全性・追跡性を確保する必要がある。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q054 6-2 インシデント分析 / マルウェア解析

マルウェア解析結果として作成する報告に含める内容として最も有用なものはどれか。
ア．「危険だった」という感想だけを記載する。
イ．検体識別情報、観察した挙動、生成・変更物、通信先、持続化、検知・封じ込めに使える指標、解析上の限界を整理する。
ウ．検体のファイル名だけを記載する。
エ．解析環境や観察条件を全て省略する。

正答・4肢解説・総合解説

正答：イ．検体識別情報、観察した挙動、生成・変更物、通信先、持続化、検知・封じ込めに使える指標、解析上の限界を整理する。
ア：感想だけでは他担当者が検証・活用できない。
イ：再現性と対応への活用を高めるには、観察事実・条件・指標・限界を構造化して示す必要がある。
ウ：ファイル名だけでは挙動や対策に結び付かない。
エ：解析条件がないと結果の解釈を誤る可能性がある。
総合解説：再現性と対応への活用を高めるには、観察事実・条件・指標・限界を構造化して示す必要がある。 マルウェア解析では、安全な隔離環境を用い、静的・動的・メモリ等の分析を組み合わせ、結果をIOCや封じ込め・検知改善へ還元する。

Q055 6-2 インシデント分析 / フォレンジック・証拠保全

デジタルフォレンジックでChain of Custodyを維持する主な目的として最も適切なものはどれか。
ア．証拠ファイルの容量を小さくする。
イ．攻撃者のIPアドレスを自動的に特定する。
ウ．証拠を誰が、いつ、どこで、どのように取得・保管・移送・分析したかを追跡できるようにし、取扱いの一貫性を示す。
エ．全ての証拠を公開情報にする。

正答・4肢解説・総合解説

正答：ウ．証拠を誰が、いつ、どこで、どのように取得・保管・移送・分析したかを追跡できるようにし、取扱いの一貫性を示す。
ア：Chain of Custodyは圧縮手法ではない。
イ：攻撃者特定を自動化する仕組みではない。
ウ：取扱履歴を連続して記録することで、証拠の真正性・完全性に関する説明可能性を高める。
エ：証拠には機密情報が含まれ得るため公開を目的としない。
総合解説：取扱履歴を連続して記録することで、証拠の真正性・完全性に関する説明可能性を高める。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q056 6-2 インシデント分析 / フォレンジック・証拠保全

稼働中のPCのディスクを保全する際、原本への書込みを避けるために用いる手段として最も適切なものはどれか。
ア．原本ディスク上で直接ファイル整理を行う。
イ．証拠取得前に不要そうなログを削除する。
ウ．原本を通常業務用PCに接続して自由に編集する。
エ．状況に応じてフォレンジック用イメージを取得し、可能な場合は書込み防止機構を用いて原本の変更を抑える。

正答・4肢解説・総合解説

正答：エ．状況に応じてフォレンジック用イメージを取得し、可能な場合は書込み防止機構を用いて原本の変更を抑える。
ア：直接編集は証拠を改変する。
イ：削除は重要証拠を失う可能性がある。
ウ：通常接続でOSがメタデータを書き換える可能性もある。
エ：原本変更を最小化し、複製物で分析することが証拠保全の基本である。
総合解説：原本変更を最小化し、複製物で分析することが証拠保全の基本である。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q057 6-2 インシデント分析 / フォレンジック・証拠保全

フォレンジックイメージ取得前後にハッシュ値を計算する目的として最も適切なものはどれか。
ア．取得した複製が対象データと一致していることや、その後に変更されていないことを検証する材料にする。
イ．暗号化されたデータを復号する。
ウ．削除ファイルを必ず復元する。
エ．攻撃経路を自動的に図示する。

正答・4肢解説・総合解説

正答：ア．取得した複製が対象データと一致していることや、その後に変更されていないことを検証する材料にする。
ア：ハッシュ比較はデータ完全性の検証に利用できる。
イ：ハッシュは復号鍵ではない。
ウ：ハッシュ計算自体には削除ファイル復元機能はない。
エ：攻撃経路の自動推定を行うものではない。
総合解説：ハッシュ比較はデータ完全性の検証に利用できる。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q058 6-2 インシデント分析 / フォレンジック・証拠保全

電源が入ったままの侵害端末で、暗号鍵やネットワーク接続など揮発性情報が重要と判断された。最も適切な考え方はどれか。
ア．必ず即時に電源コードを抜く。
イ．電源断で失われる情報の価値と、ライブ取得による証拠変更リスクを比較し、手順に従って必要な揮発性情報を先に保全する。
ウ．揮発性情報は証拠にならないので無視する。
エ．全ての端末で同じ順序を無条件に適用する。

正答・4肢解説・総合解説

正答：イ．電源断で失われる情報の価値と、ライブ取得による証拠変更リスクを比較し、手順に従って必要な揮発性情報を先に保全する。
ア：即時電源断が常に最善とは限らない。
イ：ライブ取得には副作用があるが、メモリ等は電源断で失われるため、状況に応じた判断が必要である。
ウ：揮発性情報も侵害分析に重要な証拠になり得る。
エ：システム状態・暗号化・法的要件により保全方法は変わる。
総合解説：ライブ取得には副作用があるが、メモリ等は電源断で失われるため、状況に応じた判断が必要である。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q059 6-2 インシデント分析 / フォレンジック・証拠保全

証拠保全の作業記録として最も適切なものはどれか。
ア．担当者名だけを記録する。
イ．最終報告書があれば取得時の記録は不要とする。
ウ．取得日時、担当者、対象機器識別情報、使用ツール・手順、ハッシュ、保管場所、受渡し履歴を記録する。
エ．作業の失敗や再試行は記録しない。

正答・4肢解説・総合解説

正答：ウ．取得日時、担当者、対象機器識別情報、使用ツール・手順、ハッシュ、保管場所、受渡し履歴を記録する。
ア：担当者名だけでは対象・方法・完全性を説明できない。
イ：取得時記録は後から補完できない情報を含む。
ウ：再現性と追跡性のため、取得条件と取扱履歴を具体的に残す。
エ：失敗や再試行も証拠への影響を説明するため記録すべきである。
総合解説：再現性と追跡性のため、取得条件と取扱履歴を具体的に残す。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q060 6-2 インシデント分析 / フォレンジック・証拠保全

クラウドサービス上のインシデントで証拠保全を行う際の注意点として最も適切なものはどれか。
ア．物理ディスクを自社で必ず持ち出せると仮定する。
イ．クラウドでは証拠保全は不可能と判断する。
ウ．ログ保持期間を確認せず、数か月後に取得すればよいと考える。
エ．自組織が取得できるログ・スナップショットの範囲、クラウド事業者が保持する記録、保存期間、取得手続きを事前に確認する。

正答・4肢解説・総合解説

正答：エ．自組織が取得できるログ・スナップショットの範囲、クラウド事業者が保持する記録、保存期間、取得手続きを事前に確認する。
ア：共有基盤の物理媒体を利用者が自由に取得できるとは限らない。
イ：APIログやスナップショットなど保全可能な証拠はある。
ウ：保存期間が短いログは時間経過で失われる可能性がある。
エ：クラウドでは責任分界と取得可能性がオンプレミスと異なるため、証拠源と手続きを把握する必要がある。
総合解説：クラウドでは責任分界と取得可能性がオンプレミスと異なるため、証拠源と手続きを把握する必要がある。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q061 6-2 インシデント分析 / フォレンジック・証拠保全

複数地域のログでタイムゾーン表記が異なる。フォレンジックのタイムライン作成で最も適切な方法はどれか。
ア．原記録の時刻情報とタイムゾーンを保持した上で、分析用にUTCなど共通基準へ正規化する。
イ．全ての時刻から一律9時間を引く。
ウ．タイムゾーン情報を削除して時刻だけ比較する。
エ．最も遅い時刻を基準に他ログを並べ替える。

正答・4肢解説・総合解説

正答：ア．原記録の時刻情報とタイムゾーンを保持した上で、分析用にUTCなど共通基準へ正規化する。
ア：原情報を保持しつつ共通時間軸へ変換すると、異なる地域・機器のイベントを正確に相関しやすい。
イ：一律補正は地域や夏時間などを誤る可能性がある。
ウ：タイムゾーンを失うと正確な変換ができない。
エ：時刻の大小だけでは基準差を補正できない。
総合解説：原情報を保持しつつ共通時間軸へ変換すると、異なる地域・機器のイベントを正確に相関しやすい。フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q062 6-2 インシデント分析 / フォレンジック・証拠保全

証拠取得時に専門性の高いストレージ装置があり、誤操作でデータを失う懸念がある。最も適切な対応はどれか。
ア．担当者が未経験でも本番装置で試行錯誤する。
イ．自組織の力量を超える場合は、デジタルフォレンジックや法的措置の専門家へ早期に相談・依頼する。
ウ．証拠保全を諦めて装置を初期化する。
エ．装置の電源状態や構成を記録せず持ち運ぶ。

正答・4肢解説・総合解説

正答：イ．自組織の力量を超える場合は、デジタルフォレンジックや法的措置の専門家へ早期に相談・依頼する。
ア：試行錯誤は証拠を改変・消失させる危険がある。
イ：IPAシラバスも専門性が必要な状況で専門家への依頼を扱っており、証拠毀損リスクを下げる判断が重要である。
ウ：初期化は証拠を失う。
エ：状態記録なしの移動は再現性とChain of Custodyを損なう。
総合解説：IPAシラバスも専門性が必要な状況で専門家への依頼を扱っており、証拠毀損リスクを下げる判断が重要である。 フォレンジックでは、証拠の完全性・追跡性を維持し、揮発性や環境特性を考慮して原本への影響を最小化しながら保全・分析する。

Q063 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

インシデント対応における「封じ込め」と「根絶」の違いとして最も適切なものはどれか。
ア．封じ込めは原因究明、根絶は経営報告だけを意味する。
イ．封じ込めと根絶は同じ作業で区別する必要がない。
ウ．封じ込めは被害拡大を抑える措置であり、根絶はマルウェア、侵害アカウント、持続化手段など原因となる要素を除去する。
エ．根絶は必ず全システムの廃棄を意味する。

正答・4肢解説・総合解説

正答：ウ．封じ込めは被害拡大を抑える措置であり、根絶はマルウェア、侵害アカウント、持続化手段など原因となる要素を除去する。
ア：原因究明や報告は関連するが、両用語の定義ではない。
イ：目的と作業内容が異なるため区別が必要である。
ウ：NIST CSF 2.0でもContainとEradicateを区別し、拡大抑制と原因要素の除去を別の活動として扱う。
エ：根絶方法は事案に応じ、全廃棄が必須ではない。
総合解説：NIST CSF 2.0でもContainとEradicateを区別し、拡大抑制と原因要素の除去を別の活動として扱う。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q064 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

マルウェア感染端末から社内への横展開が継続している。初期の封じ込めとして最も適切なものはどれか。
ア．感染端末をそのまま利用し続ける。
イ．全ログを削除して通信量を減らす。
ウ．原因が完全に判明するまで何も遮断しない。
エ．業務影響と証拠保全を考慮しつつ、感染端末または該当ネットワークを隔離して横展開を止める。

正答・4肢解説・総合解説

正答：エ．業務影響と証拠保全を考慮しつつ、感染端末または該当ネットワークを隔離して横展開を止める。
ア：利用継続は被害を拡大させ得る。
イ：ログ削除は調査を妨げる。
ウ：完全な原因究明を待つと被害が広がる可能性がある。
エ：進行中の横展開では、合理的な範囲で通信を止めて被害拡大を抑えることが優先される。
総合解説：進行中の横展開では、合理的な範囲で通信を止めて被害拡大を抑えることが優先される。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q065 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

管理者アカウントの認証情報窃取が判明した。封じ込め・根絶として最も適切な対応はどれか。
ア．侵害セッションやトークンを無効化し、認証情報を安全に再発行し、関連権限・アクセス履歴と同一資格情報の使い回しを確認する。
イ．パスワード変更だけで調査を終了する。
ウ．アカウント名だけ変更し、既存セッションは維持する。
エ．同じパスワードを再設定する。

正答・4肢解説・総合解説

正答：ア．侵害セッションやトークンを無効化し、認証情報を安全に再発行し、関連権限・アクセス履歴と同一資格情報の使い回しを確認する。
ア：認証情報侵害では、資格情報だけでなく既存セッション、トークン、権限利用、横展開を含めて対処する必要がある。
イ：セッションや持続化が残る可能性がある。
ウ：アカウント名変更だけでは侵害済みトークン等を無効化できない。
エ：同じ秘密を再利用すると侵害状態を解消できない。
総合解説：認証情報侵害では、資格情報だけでなく既存セッション、トークン、権限利用、横展開を含めて対処する必要がある。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q066 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

C2通信が確認された端末群に対して、通信先をFWで遮断した。次に必要な対応として最も適切なものはどれか。
ア．通信が止まったのでインシデントを即時終了する。
イ．遮断を封じ込めの一部と位置付け、端末内のマルウェアや持続化、侵入経路、他の通信先を調査して根絶する。
ウ．遮断ルールを解除して通信再開を待つ。
エ．C2ドメイン以外の調査は不要とする。

正答・4肢解説・総合解説

正答：イ．遮断を封じ込めの一部と位置付け、端末内のマルウェアや持続化、侵入経路、他の通信先を調査して根絶する。
ア：表面的に通信が止まっても感染状態が残る可能性がある。
イ：通信遮断だけでは端末内の侵害要素が残るため、根絶とスコープ確認が必要である。
ウ：不用意な解除は再侵害を招く。
エ：代替C2や横展開が存在する可能性がある。
総合解説：通信遮断だけでは端末内の侵害要素が残るため、根絶とスコープ確認が必要である。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q067 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

ランサムウェア被害でバックアップが利用可能である。復元を始める前に優先すべき事項として最も適切なものはどれか。
ア．感染中のネットワークへ直ちに全バックアップを接続する。
イ．原因を確認せず暗号化端末へ上書き復元する。
ウ．侵害範囲と侵入経路を確認し、攻撃者のアクセスやマルウェアの持続化を封じ込め・根絶してから安全な復元に移る。
エ．復元後は監視を弱める。

正答・4肢解説・総合解説

正答：ウ．侵害範囲と侵入経路を確認し、攻撃者のアクセスやマルウェアの持続化を封じ込め・根絶してから安全な復元に移る。
ア：バックアップ自体が攻撃対象になる可能性がある。
イ：侵入経路を残すと再発し得る。
ウ：侵害要素が残ったまま復元すると再暗号化・再侵害されるため、復旧前の封じ込め・根絶が重要である。
エ：復旧後はむしろ再発兆候を重点監視する。
総合解説：侵害要素が残ったまま復元すると再暗号化・再侵害されるため、復旧前の封じ込め・根絶が重要である。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q068 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

封じ込め策を選ぶ際のトレードオフとして最も適切なものはどれか。
ア．最も強い遮断策を常に無条件で選ぶ。
イ．業務影響だけを考え、セキュリティ影響は無視する。
ウ．証拠保全と封じ込めは両立できないため、必ず一方を諦める。
エ．被害拡大防止の効果と、事業停止、証拠喪失、攻撃者への察知などの副作用を比較して選ぶ。

正答・4肢解説・総合解説

正答：エ．被害拡大防止の効果と、事業停止、証拠喪失、攻撃者への察知などの副作用を比較して選ぶ。
ア：一律の全面停止が最適とは限らない。
イ：セキュリティ影響を無視すると被害が拡大する。
ウ：計画と優先順位付けにより両立を図る。
エ：封じ込めは状況依存で、短期・長期の影響を比較して意思決定する必要がある。
総合解説：封じ込めは状況依存で、短期・長期の影響を比較して意思決定する必要がある。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q069 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

一部サーバだけに侵害兆候があるが、同一管理ネットワークから多数サーバへアクセスできる構成である。封じ込めとして最も適切な検討はどれか。
ア．侵害端末の隔離に加え、管理経路やネットワークセグメントの一時制限を検討し、横展開経路を抑える。
イ．侵害サーバの画面をロックするだけにする。
ウ．外部通信だけ止め、内部管理経路は必ず維持する。
エ．全社員のインターネットを永久停止する。

正答・4肢解説・総合解説

正答：ア．侵害端末の隔離に加え、管理経路やネットワークセグメントの一時制限を検討し、横展開経路を抑える。
ア：攻撃経路が共有管理ネットワークに及ぶ場合、横展開の経路そのものを制限する必要がある。
イ：画面ロックはネットワーク横展開を防がない。
ウ：内部管理経路が攻撃に使われる可能性を無視している。
エ：必要範囲を評価せず恒久全面停止するのは過剰である。
総合解説：攻撃経路が共有管理ネットワークに及ぶ場合、横展開の経路そのものを制限する必要がある。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q070 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

クラウドメールのアカウント乗っ取りで、パスワード変更後も不正アクセスが続いている。追加対応として最も適切なものはどれか。
ア．パスワードを同じ値に戻す。
イ．既存セッション、リフレッシュトークン、アプリ連携・OAuth同意、転送設定などを確認し、不正なものを失効・削除する。
ウ．端末の壁紙を変更する。
エ．メール件名を全て削除する。

正答・4肢解説・総合解説

正答：イ．既存セッション、リフレッシュトークン、アプリ連携・OAuth同意、転送設定などを確認し、不正なものを失効・削除する。
ア：同じパスワードへの戻しは改善にならない。
イ：クラウドアカウントではパスワード以外のセッションや委任設定が持続化に使われることがある。
ウ：壁紙は認証状態に関係しない。
エ：件名削除は不正セッションを無効化しない。
総合解説：クラウドアカウントではパスワード以外のセッションや委任設定が持続化に使われることがある。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q071 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

破壊型マルウェアがバックアップ管理サーバにも到達しようとしている。最も適切な封じ込めはどれか。
ア．バックアップ管理サーバを感染端末と同じネットワークへ追加接続する。
イ．全バックアップを削除して攻撃対象をなくす。
ウ．バックアップ基盤を攻撃経路から隔離し、管理認証情報を保護・必要に応じて変更し、バックアップの完全性を確認する。
エ．バックアップの状態確認を復旧後まで行わない。

正答・4肢解説・総合解説

正答：ウ．バックアップ基盤を攻撃経路から隔離し、管理認証情報を保護・必要に応じて変更し、バックアップの完全性を確認する。
ア：接続拡大は攻撃面を増やす。
イ：削除は復旧可能性を自ら失う。
ウ：復旧資産を保護することはレジリエンス上重要で、攻撃者の到達経路を遮断して完全性を確認する。
エ：早期確認が復旧計画の判断に必要である。
総合解説：復旧資産を保護することはレジリエンス上重要で、攻撃者の到達経路を遮断して完全性を確認する。封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q072 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

インターネット公開サーバの既知脆弱性が侵入経路だった。根絶策として最も適切なものはどれか。
ア．脆弱性パッチだけ適用し、侵害痕跡は調べない。
イ．Webシェルだけ削除し、脆弱性は残す。
ウ．サーバ名だけ変更して再公開する。
エ．脆弱性を修正・緩和し、侵害による不正アカウントやWebシェル等を除去し、同種の露出が他資産にないか確認する。

正答・4肢解説・総合解説

正答：エ．脆弱性を修正・緩和し、侵害による不正アカウントやWebシェル等を除去し、同種の露出が他資産にないか確認する。
ア：侵害要素が残る可能性がある。
イ：侵入経路が残れば再侵害される。
ウ：名称変更は脆弱性や侵害状態を解消しない。
エ：侵入経路と侵害後の持続化の双方を解消し、同様の弱点を横断確認する必要がある。
総合解説：侵入経路と侵害後の持続化の双方を解消し、同様の弱点を横断確認する必要がある。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q073 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

封じ込めのために一時的なFWルールを追加した。長期対応として最も適切なものはどれか。
ア．一時ルールの目的・期限・責任者を記録し、根本対策後に必要性を再評価して恒久設定へ整理または削除する。
イ．一時ルールは無期限に残す。
ウ．誰が追加したか記録しない。
エ．根本対策を行わず一時ルールだけで終了する。

正答・4肢解説・総合解説

正答：ア．一時ルールの目的・期限・責任者を記録し、根本対策後に必要性を再評価して恒久設定へ整理または削除する。
ア：緊急変更は技術的負債や意図しない遮断を残し得るため、事後に構成管理へ戻す必要がある。
イ：無期限放置は運用リスクになる。
ウ：追跡性が失われる。
エ：暫定策だけでは根本原因が残る可能性がある。
総合解説：緊急変更は技術的負債や意図しない遮断を残し得るため、事後に構成管理へ戻す必要がある。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q074 6-3 封じ込め・復旧・再発防止 / 封じ込め・根絶

第三者サービス用APIキーの漏えいが判明した。最も適切な根絶対応はどれか。
ア．キーの表示名だけ変更する。
イ．漏えいしたキーを失効し、新しいキーを安全に発行・保管し、利用ログと権限を確認して過剰権限や不正利用を是正する。
ウ．漏えいキーを残したまま監視だけ強化する。
エ．同じキーを別ファイルへコピーして利用する。

正答・4肢解説・総合解説

正答：イ．漏えいしたキーを失効し、新しいキーを安全に発行・保管し、利用ログと権限を確認して過剰権限や不正利用を是正する。
ア：表示名変更では秘密値は無効化されない。
イ：秘密情報漏えいでは失効・再発行と利用状況確認が必要で、権限最小化も再発防止に寄与する。
ウ：有効な漏えいキーを残すと継続悪用され得る。
エ：コピーしても漏えい状態は解消しない。
総合解説：秘密情報漏えいでは失効・再発行と利用状況確認が必要で、権限最小化も再発防止に寄与する。 封じ込めは被害拡大の抑制、根絶は侵害要素と侵入経路の除去が目的であり、事業影響・証拠保全とのトレードオフを管理する。

Q075 6-3 封じ込め・復旧・再発防止 / 復旧・回復

侵害システムをバックアップから復元する際、最も重要な前提確認はどれか。
ア．最も新しいバックアップであれば内容確認は不要である。
イ．バックアップが存在すれば復元テストは不要である。
ウ．利用するバックアップが侵害前の信頼できる時点のもので、完全性と復元可能性が確認されていること。
エ．感染した端末に接続できれば信頼できると判断する。

正答・4肢解説・総合解説

正答：ウ．利用するバックアップが侵害前の信頼できる時点のもので、完全性と復元可能性が確認されていること。
ア：最新でも侵害済みデータを含む可能性がある。
イ：復元できることは実際のテストで確認する必要がある。
ウ：侵害後に取得されたバックアップや汚染されたバックアップを戻すと再侵害につながるため、時点・完全性・復元性の確認が必要である。
エ：接続可否はバックアップの信頼性を示さない。
総合解説：侵害後に取得されたバックアップや汚染されたバックアップを戻すと再侵害につながるため、時点・完全性・復元性の確認が必要である。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q076 6-3 封じ込め・復旧・再発防止 / 復旧・回復

RTOとRPOの違いとして最も適切なものはどれか。
ア．RTOは暗号鍵長、RPOはパスワード長を表す。
イ．RTOとRPOはどちらもバックアップ媒体の容量を表す。
ウ．RPOは必ず0でなければならず、RTOは無制限でよい。
エ．RTOはサービスを復旧させるまでの目標時間、RPOは許容できるデータ損失を時間軸で示す目標である。

正答・4肢解説・総合解説

正答：エ．RTOはサービスを復旧させるまでの目標時間、RPOは許容できるデータ損失を時間軸で示す目標である。
ア：暗号強度の指標ではない。
イ：容量ではなく時間に関する復旧目標である。
ウ：事業要件とコストを踏まえて設定され、常に0や無制限ではない。
エ：RTOとRPOは復旧計画で異なる要求を表し、復旧順序やバックアップ設計に影響する。
総合解説：RTOとRPOは復旧計画で異なる要求を表し、復旧順序やバックアップ設計に影響する。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q077 6-3 封じ込め・復旧・再発防止 / 復旧・回復

大規模インシデント後、全システムを同時に復旧できない。最も適切な復旧順序の決め方はどれか。
ア．業務重要度、依存関係、RTO、セキュリティ上の前提条件を踏まえ、重要サービスから段階的に復旧する。
イ．システム名の五十音順に復旧する。
ウ．担当者が最も好きなシステムから復旧する。
エ．最も容量の小さいサーバだけを優先する。

正答・4肢解説・総合解説

正答：ア．業務重要度、依存関係、RTO、セキュリティ上の前提条件を踏まえ、重要サービスから段階的に復旧する。
ア：復旧は事業優先度と技術依存関係に基づいて計画する必要がある。
イ：名称順は事業影響と無関係である。
ウ：個人の好みは客観的な基準にならない。
エ：容量だけでは業務重要性を評価できない。
総合解説：復旧は事業優先度と技術依存関係に基づいて計画する必要がある。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q078 6-3 封じ込め・復旧・再発防止 / 復旧・回復

復旧したサーバを本番ネットワークへ再接続する前の確認として最も適切なものはどれか。
ア．OSが起動すれば即時に再接続する。
イ．必要な修正・ハードニング、認証情報の更新、マルウェアや持続化の不存在、業務機能とログ監視の正常性を確認する。
ウ．利用者が急いでいればセキュリティ確認を省略する。
エ．監視機能を無効にして負荷を下げてから再接続する。

正答・4肢解説・総合解説

正答：イ．必要な修正・ハードニング、認証情報の更新、マルウェアや持続化の不存在、業務機能とログ監視の正常性を確認する。
ア：起動可否だけでは侵害除去を確認できない。
イ：復旧は単に起動することではなく、安全に業務へ戻せる状態を検証してから再接続する。
ウ：緊急時でも再侵害防止の最低限の確認が必要である。
エ：復旧直後は重点監視が重要である。
総合解説：復旧は単に起動することではなく、安全に業務へ戻せる状態を検証してから再接続する。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q079 6-3 封じ込め・復旧・再発防止 / 復旧・回復

インシデントから復旧した直後の監視として最も適切なものはどれか。
ア．復旧したので監視を停止する。
イ．通常ログを削除して容量を空ける。
ウ．侵害時に観測したIOCやTTP、再侵害の兆候、異常認証・通信を一定期間重点的に監視する。
エ．侵害と無関係な指標だけを見る。

正答・4肢解説・総合解説

正答：ウ．侵害時に観測したIOCやTTP、再侵害の兆候、異常認証・通信を一定期間重点的に監視する。
ア：監視停止は再発を見逃す。
イ：ログ削除は追跡性を損なう。
ウ：復旧直後は根絶漏れや再侵害を検知するため、インシデントに関連した監視を強化する。
エ：関連兆候を監視しなければ復旧の妥当性を確認しにくい。
総合解説：復旧直後は根絶漏れや再侵害を検知するため、インシデントに関連した監視を強化する。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q080 6-3 封じ込め・復旧・再発防止 / 復旧・回復

ランサムウェア侵害で、1か月前のバックアップは正常だが、その時点ですでに攻撃者が潜伏していた可能性がある。最も適切な復旧方針はどれか。
ア．バックアップが暗号化されていなければ必ず安全とみなす。
イ．最も新しいバックアップだけを無条件に使う。
ウ．バックアップから戻せば根本原因対策は不要とする。
エ．バックアップ時点の侵害有無をログやIOCで検証し、必要ならより古いクリーンな時点を選び、脆弱性や認証情報も是正して復元する。

正答・4肢解説・総合解説

正答：エ．バックアップ時点の侵害有無をログやIOCで検証し、必要ならより古いクリーンな時点を選び、脆弱性や認証情報も是正して復元する。
ア：暗号化されていなくてもWebシェルや不正アカウントが含まれる場合がある。
イ：新しさと安全性は同義ではない。
ウ：復元と侵入経路の是正は両方必要である。
エ：潜伏期間がある攻撃ではバックアップにも侵害要素が含まれる可能性があり、クリーン時点の確認が必要である。
総合解説：潜伏期間がある攻撃ではバックアップにも侵害要素が含まれる可能性があり、クリーン時点の確認が必要である。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q081 6-3 封じ込め・復旧・再発防止 / 復旧・回復

認証基盤、DNS、業務アプリが相互依存している環境での復旧計画として最も適切なものはどれか。
ア．サービス依存関係を事前に整理し、基盤サービスの復旧順序と代替手段を含む復旧シーケンスを設計する。
イ．各担当が独立に好きな順で復旧する。
ウ．業務アプリだけ先に起動し、依存サービスは考慮しない。
エ．依存関係は障害発生後に初めて調べる。

正答・4肢解説・総合解説

正答：ア．サービス依存関係を事前に整理し、基盤サービスの復旧順序と代替手段を含む復旧シーケンスを設計する。
ア：依存関係を無視すると、単体で復旧してもサービス全体が利用できないため、順序設計が必要である。
イ：独立作業では前提サービス不足で手戻りが起きる。
ウ：認証や名前解決がなければアプリが正常動作しない場合がある。
エ：平常時に把握しておく方が迅速で確実である。
総合解説：依存関係を無視すると、単体で復旧してもサービス全体が利用できないため、順序設計が必要である。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q082 6-3 封じ込め・復旧・再発防止 / 復旧・回復

代替サイトへフェイルオーバーした後、元サイトへ戻す際に最も注意すべき点はどれか。
ア．元サイトが起動した瞬間に無条件で切り戻す。
イ．フェイルオーバー中に更新されたデータの整合性と同期状態を確認し、切戻し手順・停止時間・ロールバック条件を管理する。
ウ．代替サイトで更新されたデータは全て捨てる。
エ．データ整合性は復旧と無関係なので確認しない。

正答・4肢解説・総合解説

正答：イ．フェイルオーバー中に更新されたデータの整合性と同期状態を確認し、切戻し手順・停止時間・ロールバック条件を管理する。
ア：起動だけではデータ整合性を保証しない。
イ：切戻しではデータの分岐や欠落を防ぐため、同期・整合性と手順管理が重要である。
ウ：業務更新を無条件に破棄すると情報損失になる。
エ：復旧品質の中心的な確認事項である。
総合解説：切戻しではデータの分岐や欠落を防ぐため、同期・整合性と手順管理が重要である。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q083 6-3 封じ込め・復旧・再発防止 / 復旧・回復

復旧完了の判定基準として最も適切なものはどれか。
ア．サーバの電源ランプが点灯することだけ。
イ．CSIRTが疲れた時点で終了とする。
ウ．業務機能、セキュリティ管理策、データ完全性、性能、監視、利用部門の確認など、事前に定めた受入基準を満たすこと。
エ．エラー画面が出なければログ確認は不要とする。

正答・4肢解説・総合解説

正答：ウ．業務機能、セキュリティ管理策、データ完全性、性能、監視、利用部門の確認など、事前に定めた受入基準を満たすこと。
ア：電源状態だけでは業務機能を確認できない。
イ：担当者の疲労は完了基準ではない。
ウ：復旧はサービスとセキュリティの両面で受入基準を満たして初めて完了と判断できる。
エ：見かけ上正常でもログに異常が残る可能性がある。
総合解説：復旧はサービスとセキュリティの両面で受入基準を満たして初めて完了と判断できる。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q084 6-3 封じ込め・復旧・再発防止 / 復旧・回復

長時間の復旧作業中に利用部門への説明が必要である。最も適切な情報提供はどれか。
ア．復旧完了まで一切連絡しない。
イ．毎回異なる担当者が推測を含む時刻を約束する。
ウ．技術ログだけを利用部門へ大量送付する。
エ．復旧対象、現時点の状態、利用可能な代替手段、次の更新時刻、未確定事項を整理し、定期的に更新する。

正答・4肢解説・総合解説

正答：エ．復旧対象、現時点の状態、利用可能な代替手段、次の更新時刻、未確定事項を整理し、定期的に更新する。
ア：無連絡は業務判断を困難にする。
イ：根拠のない復旧時刻の断定は信頼を損なう。
ウ：利用部門には業務影響と選択肢を分かりやすく伝える必要がある。
エ：利用者が業務継続を判断できるよう、確定情報と不確実性を区別した定期更新が有効である。
総合解説：利用者が業務継続を判断できるよう、確定情報と不確実性を区別した定期更新が有効である。 復旧では、信頼できる復旧元、依存関係、RTO/RPO、再接続前の安全性、復旧後の重点監視を含めて段階的に業務を回復する。

Q085 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

インシデント後の根本原因分析で、「利用者がフィッシングメールを開いた」だけを原因として終了する問題点はどれか。
ア．なぜ単一の利用者操作が侵害拡大につながったか、認証・権限・検知・教育・技術対策など背景要因を十分に分析できていない。
イ．利用者の操作は一切調べてはならないから。
ウ．フィッシングは情報セキュリティインシデントではないから。
エ．根本原因分析では技術要因だけを扱うから。

正答・4肢解説・総合解説

正答：ア．なぜ単一の利用者操作が侵害拡大につながったか、認証・権限・検知・教育・技術対策など背景要因を十分に分析できていない。
ア：直接のきっかけと組織・技術上の根本要因を分けて分析すると、再発防止策を広く設計できる。
イ：利用者操作も事実として調べるが、それだけに責任を帰すのは不十分である。
ウ：フィッシングは侵害の起点になり得る。
エ：人的・プロセス・技術要因を横断して分析する必要がある。
総合解説：直接のきっかけと組織・技術上の根本要因を分けて分析すると、再発防止策を広く設計できる。 再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q086 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

事後レビューの進め方として最も適切なものはどれか。
ア．失敗した担当者名だけを一覧化して終了する。
イ．個人の責任追及だけに偏らず、事実に基づいて手順・技術・体制・意思決定の改善点を抽出する。
ウ．問題点を記録すると責任問題になるため議事録を残さない。
エ．成功した点は再発防止に関係ないので分析しない。

正答・4肢解説・総合解説

正答：イ．個人の責任追及だけに偏らず、事実に基づいて手順・技術・体制・意思決定の改善点を抽出する。
ア：個人責任だけでは構造的な弱点が残る。
イ：学習を目的に事実と仕組みを評価することで、具体的な改善につなげやすい。
ウ：記録がないと改善の追跡ができない。
エ：有効だった対応も標準化・強化の材料になる。
総合解説：学習を目的に事実と仕組みを評価することで、具体的な改善につなげやすい。 再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q087 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

再発防止策を決めた後の管理として最も適切なものはどれか。
ア．対策案を会議で読み上げた時点で完了とする。
イ．全ての対策を無期限の検討事項にする。
ウ．各対策に責任者、期限、優先度、完了条件を割り当て、進捗と有効性を追跡する。
エ．誰が実施するか決めず、善意に任せる。

正答・4肢解説・総合解説

正答：ウ．各対策に責任者、期限、優先度、完了条件を割り当て、進捗と有効性を追跡する。
ア：合意だけでは実装されない。
イ：期限がなければ先送りされやすい。
ウ：改善事項を実行可能なアクションとして管理し、完了と効果を確認することが再発防止につながる。
エ：責任者不明では実施・追跡が困難である。
総合解説：改善事項を実行可能なアクションとして管理し、完了と効果を確認することが再発防止につながる。再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q088 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

インシデント調査で、攻撃開始から検知まで長期間かかっていたことが分かった。再発防止として最も適切なものはどれか。
ア．検知が遅れた事実を記録から削除する。
イ．同じ検知ルールを変更せず使い続ける。
ウ．再発防止は復旧担当だけに任せ、SOCには共有しない。
エ．見逃したログや挙動を分析し、必要なログ取得、相関ルール、監視範囲、脅威ハンティング、要員手順を改善する。

正答・4肢解説・総合解説

正答：エ．見逃したログや挙動を分析し、必要なログ取得、相関ルール、監視範囲、脅威ハンティング、要員手順を改善する。
ア：不都合な事実を消すと学習機会を失う。
イ：同じ弱点を残すことになる。
ウ：SOCや監視担当との共有が必要である。
エ：検知ギャップを具体化して監視設計へフィードバックすると、同種攻撃の早期発見につながる。
総合解説：検知ギャップを具体化して監視設計へフィードバックすると、同種攻撃の早期発見につながる。 再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q089 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

再発防止として新しいEDRルールを追加した。対策の有効性確認として最も適切なものはどれか。
ア．想定した攻撃挙動を安全なテストや演習で再現し、検知・通知・初動まで機能するか確認する。
イ．設定を保存しただけで有効とみなす。
ウ．本番で同じ攻撃が再発するまで確認しない。
エ．アラート件数が0なら必ず成功と判断する。

正答・4肢解説・総合解説

正答：ア．想定した攻撃挙動を安全なテストや演習で再現し、検知・通知・初動まで機能するか確認する。
ア：管理策は導入だけでなく、期待した結果を出すかを検証する必要がある。
イ：設定存在だけでは動作を保証しない。
ウ：実攻撃待ちは検証として不適切である。
エ：0件は攻撃がない、または検知できていない可能性もある。
総合解説：管理策は導入だけでなく、期待した結果を出すかを検証する必要がある。 再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q090 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

インシデント対応手順の改善として最も適切なものはどれか。
ア．事後レビューは保管だけして手順を変えない。
イ．実際に発生した判断遅延や連絡漏れを基に、プレイブック、連絡網、判断基準を更新し、その内容を訓練へ反映する。
ウ．対応手順は一度作れば恒久的に変更しない。
エ．新手順をCSIRT管理者だけが知っていればよい。

正答・4肢解説・総合解説

正答：イ．実際に発生した判断遅延や連絡漏れを基に、プレイブック、連絡網、判断基準を更新し、その内容を訓練へ反映する。
ア：保管だけでは同じ問題が再発する。
イ：教訓を文書・訓練・運用へ戻すことで継続的な対応能力向上につながる。
ウ：脅威・組織・システムは変化するため見直しが必要である。
エ：関係者への周知と訓練がなければ実行できない。
総合解説：教訓を文書・訓練・運用へ戻すことで継続的な対応能力向上につながる。 再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q091 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

CSIRTの対応時間指標を改善する際の注意点として最も適切なものはどれか。
ア．全てのチケットを即時クローズすれば指標改善とみなす。
イ．長時間かかった重大事案は統計から除外する。
ウ．平均時間だけを短縮することを目的にせず、重大度別の品質、封じ込めの妥当性、再発率なども合わせて評価する。
エ．時間指標だけでCSIRTの有効性を完全評価できる。

正答・4肢解説・総合解説

正答：ウ．平均時間だけを短縮することを目的にせず、重大度別の品質、封じ込めの妥当性、再発率なども合わせて評価する。
ア：見かけ上の数値だけ改善し、実際の対応品質を損なう。
イ：恣意的除外は指標の信頼性を損なう。
ウ：時間短縮だけを追うと拙速な終了を誘発し得るため、品質や結果を含む複数指標で見る必要がある。
エ：単一指標では複雑な対応能力を十分に表せない。
総合解説：時間短縮だけを追うと拙速な終了を誘発し得るため、品質や結果を含む複数指標で見る必要がある。再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q092 6-3 封じ込め・復旧・再発防止 / 根本原因分析・再発防止

ある攻撃では侵害に至らなかったが、設定不備により危険な通信が許可されかけた。再発防止として最も適切な扱いはどれか。
ア．被害が出ていないため記録も分析もしない。
イ．実害がないので設定不備を残す。
ウ．攻撃者が再度試すまで対策しない。
エ．重大なニアミスとして原因と制御の弱点を分析し、設定・監視・レビュー手順の改善へ反映する。

正答・4肢解説・総合解説

正答：エ．重大なニアミスとして原因と制御の弱点を分析し、設定・監視・レビュー手順の改善へ反映する。
ア：記録しなければ同じ弱点を見逃す。
イ：設定不備を放置すると次回は侵害に至る可能性がある。
ウ：再攻撃を待つ必要はない。
エ：未遂事象も管理策の弱点を示す重要な学習材料であり、実害が出る前に改善できる。
総合解説：未遂事象も管理策の弱点を示す重要な学習材料であり、実害が出る前に改善できる。 再発防止では、直接のきっかけだけでなく技術・手順・体制上の根本要因を分析し、改善策の実装・検証・教育まで追跡する。

Q093 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

あるWebシステムは「インターネット→WAF→Webサーバ→APサーバ→DBサーバ」の順に接続されている。運用端末からの保守接続は、VPN接続後に踏み台サーバを経由することだけが許可され、Webサーバへのインターネットからの SSH接続は禁止されている。緊急パッチ適用時の作業方法として、要件に最も適合するものはどれか。
ア．運用端末からVPNに接続し、踏み台サーバを経由して対象サーバへ保守接続する。
イ．作業時間を短縮するため、WebサーバのSSHを一時的にインターネットへ公開する。
ウ．WAFの管理画面からDBサーバへ直接ログインしてパッチを適用する。
エ．APサーバにパッチファイルを置き、Web利用者の通信に混ぜてDBサーバへ転送する。

正答・4肢解説・総合解説

正答：ア．運用端末からVPNに接続し、踏み台サーバを経由して対象サーバへ保守接続する。
ア：構成図と運用要件で定めた管理経路を維持でき、緊急時でもインターネットからの直接SSHを新たに許可しないため適切である。
イ：明示的に禁止された経路を例外扱いで開放すると、要件違反になり攻撃面も増える。
ウ：WAFはWeb通信の防御装置であり、記載されたDB保守経路ではない。
エ：利用者向け通信経路を保守用途へ転用する方法は構成・運用要件に反し、管理経路の統制も失う。
総合解説：科目B型のシナリオでは、一般論よりも問題文に明示された接続経路・禁止事項・運用条件を優先して判断する。緊急対応でも、定義済みの管理経路を逸脱する場合は追加リスクが生じる。

Q094 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

外部SaaSから社内APIへ通知を受ける仕組みを設計している。要件は「送信元を認証すること」であり、SaaS事業者からは「送信元IPアドレスは固定されず、予告なく変更される場合がある」と説明された。この条件から導く設計判断として最も適切なものはどれか。
ア．現在観測できたSaaSのIPアドレスだけを恒久的に許可する。
イ．固定IPアドレスの許可リストだけに依存せず、メッセージ署名や相互認証など送信主体を検証できる方式を採用する。
ウ．送信元認証を行わず、HTTPSで暗号化されていれば十分とする。
エ．社内APIをインターネットへ全面公開し、SaaS側の善意に任せる。

正答・4肢解説・総合解説

正答：イ．固定IPアドレスの許可リストだけに依存せず、メッセージ署名や相互認証など送信主体を検証できる方式を採用する。
ア：IPアドレスが変更されるという前提に反し、正規通信が停止するか、運用で恒常的な例外対応が必要になる。
イ：送信元IPが固定されないという制約のため、IPアドレスだけでは要求された送信元認証を安定して満たせない。別の認証要素を設計する必要がある。
ウ：通信路暗号化は送信主体の正当性を自動的に保証するものではなく、要件を満たさない。
エ：アクセス制御を放棄しており、要求された認証を実装していない。
総合解説：要求は達成すべき性質、制約は設計の選択肢を狭める条件である。科目Bでは両者を切り分け、制約の下でも要求を満たす代替策を選ぶ。

Q095 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

設計資料では、DBサーバ用サブネットにはインターネット向けのデフォルトルートがなく、APサーバからDBポートへの通信だけが許可されている。しかし、インシデント調査で「DBサーバから外部IPアドレスへの通信」が記録された。最初の確認として最も適切なものはどれか。
ア．設計資料が正しい前提で、ログは必ず誤記録だと結論付ける。
イ．DBサーバを直ちに廃棄し、新規サーバへ置き換える。
ウ．現行のルート設定、FW設定、NAT構成が設計資料どおりかを実機・現行設定で確認する。
エ．外部IPアドレスの所有者だけを調べ、ネットワーク構成は確認しない。

正答・4肢解説・総合解説

正答：ウ．現行のルート設定、FW設定、NAT構成が設計資料どおりかを実機・現行設定で確認する。
ア：資料とログのどちらが誤っているかは未確定であり、検証前に一方を排除してはいけない。
イ：封じ込めが必要な場合はあるが、構成矛盾の原因確認前に廃棄すると証拠や原因情報を失うおそれがある。
ウ：観測事実と設計資料が矛盾しているため、まず資料が現状を正しく表しているか、構成変更や例外経路がないかを確認する必要がある。
エ：通信先情報だけでは、DBから外部への経路が存在した理由を説明できない。
総合解説：構成図は重要な前提だが、常に実環境と一致するとは限らない。ログ・設定・資産情報など複数の証拠を照合し、現行構成を再確認してから攻撃経路を推定する。

Q096 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

顧客データを扱うサービスにはRTO 30分の要件がある。一方、契約上「顧客データは国内リージョンの外へ保存してはならない」という制約がある。災害対策構成として最も適切なものはどれか。
ア．最も遠い海外リージョンへ常時レプリケーションする。
イ．所在制約を優先し、バックアップも冗長化も一切行わない。
ウ．RTOを満たすため、契約条件を無視して任意のリージョンへ複製する。
エ．国内の別リージョンまたは契約で許容された国内拠点に待機系と復旧データを準備し、切替手順を検証する。

正答・4肢解説・総合解説

正答：エ．国内の別リージョンまたは契約で許容された国内拠点に待機系と復旧データを準備し、切替手順を検証する。
ア：災害分離には有効でも、顧客データを国外へ保存しないという明示的制約に反する。
イ：RTO 30分の可用性要件を満たせない可能性が高い。
ウ：非機能要件を満たすために契約上の制約を無視することはできない。
エ：可用性を高めつつ、データ所在の制約を守る必要があるため、許容範囲内の別障害ドメインへ冗長化するのが適切である。
総合解説：設計判断では、単一の要件だけでなく、可用性・法務・契約・データ所在など複数の制約を同時に満たす必要がある。矛盾する場合は、設計で解消するか、正式な要件変更手続が必要になる。

Q097 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

全社システムはIdPによるSSOとMFAを必須としている。ただし、IdP障害時でも基幹システムへ最低限の復旧操作が必要である。設計レビューで最も適切な指摘はどれか。
ア．非常用アカウントの利用条件、保管方法、承認、監視、利用後の資格情報変更を明文化し、通常経路とは分離して設計する。
イ．MFA必須という方針があるので、IdP障害時の復旧操作は一切できない設計にする。
ウ．非常用アカウントを全管理者で共有し、パスワードを変更しない。
エ．非常用アカウントはログを残さないことで機密性を高める。

正答・4肢解説・総合解説

正答：ア．非常用アカウントの利用条件、保管方法、承認、監視、利用後の資格情報変更を明文化し、通常経路とは分離して設計する。
ア：IdP障害時の復旧要件と通常時の強固な認証要件を両立させるには、例外経路を無統制に設けず、用途・権限・監査を限定した非常用アクセスとして管理する必要がある。
イ：可用性・復旧要件を満たせず、業務継続上の要求を無視している。
ウ：共有・固定資格情報は追跡性と秘密性を低下させ、非常用経路のリスクを高める。
エ：非常用アクセスこそ厳格な監査証跡が必要であり、ログを残さない設計は不適切である。
総合解説：例外要件は「例外だから統制不要」ではない。通常統制を迂回する非常用経路には、限定権限、強い保管、承認、監視、定期試験など追加統制を設ける。

Q098 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

社員PCは共通のNATゲートウェイを経由してインターネットへ接続する。外部サービスから「10時15分に送信元グローバルIP Xから不正アクセスがあった」と通知されたが、社内ではNATゲートウェイの変換ログを保存していない。どの情報不足が調査を最も直接的に妨げるか。
ア．社員食堂の座席表。
イ．該当時刻のグローバルIP・ポートと社内端末のプライベートIP・ポートを対応付けるNAT変換記録。
ウ．WebサイトのCSSファイル。
エ．会社案内の組織図だけ。

正答・4肢解説・総合解説

正答：イ．該当時刻のグローバルIP・ポートと社内端末のプライベートIP・ポートを対応付けるNAT変換記録。
ア：ネットワーク通信元の特定には直接結び付かない。
イ：多数端末が同じグローバルIPを共有する構成では、NAT変換記録がないと外部観測から内部端末へ一意にたどれない場合がある。
ウ：表示内容の資産であり、NAT変換の対応関係を示さない。
エ：所属情報は後続調査に役立つ場合があるが、通信元端末の特定にはまずネットワーク証跡が必要である。
総合解説：ログ設計は「取れるものを保存する」のではなく、想定する調査・検知・説明責任から必要項目を定める。NATやプロキシなどアドレスを変換・集約する装置のログは、追跡性に直結する。

Q099 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

モバイルアプリ→API Gateway→複数の業務APIという構成である。モバイルアプリはHTTPヘッダに「role=admin」などの値を付けられる。業務APIの認可設計として最も適切なものはどれか。
ア．roleヘッダがadminなら無条件で管理操作を許可する。
イ．TLSを利用しているので、roleヘッダの内容も自動的に正しいとみなす。
ウ．検証済みのトークンやサーバ側の権限情報から利用者の権限を決定し、クライアントが任意に設定できるroleヘッダを認可根拠にしない。
エ．API Gatewayを経由していれば、業務API側では一切認可しない。

正答・4肢解説・総合解説

正答：ウ．検証済みのトークンやサーバ側の権限情報から利用者の権限を決定し、クライアントが任意に設定できるroleヘッダを認可根拠にしない。
ア：攻撃者がヘッダを改変できれば権限昇格できるため不適切である。
イ：TLSは通信路を保護するが、正規クライアントが送る任意入力の正当性まで保証しない。
ウ：クライアント側で改変できる値は信頼境界の外にあり、認可判断の根拠にはできない。サーバ側で検証可能な認証・権限情報を使う必要がある。
エ：ゲートウェイ側の統制だけに依存すると、内部経路や設定不備による迂回時の影響が大きくなる。
総合解説：構成図では、どこが信頼境界か、どの情報を誰が生成し検証するかを読む。認可は利用者が自由に操作できない、検証済みの情報に基づいて行う。

Q100 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

社内OAネットワークと製造設備ネットワークはFWで分離されている。両ネットワークへ接続できるのは、管理用ジャンプサーバとパッチ配布サーバだけである。OA端末でマルウェア感染が発生した場合、製造設備側への波及可能性を評価する際に最優先で確認すべき資産はどれか。
ア．製造設備と無関係な公開Webサイトの画像サーバ。
イ．社員の私物スマートフォンの機種名だけ。
ウ．OAネットワークのプリンタ用紙残量。
エ．両ネットワークへ到達可能なジャンプサーバとパッチ配布サーバの認証・通信・更新状態。

正答・4肢解説・総合解説

正答：エ．両ネットワークへ到達可能なジャンプサーバとパッチ配布サーバの認証・通信・更新状態。
ア：両ネットワーク間の接続経路に位置せず、今回の波及経路の評価優先度は低い。
イ：直接の接続条件が示されておらず、境界を越える経路の確認より優先度は低い。
ウ：セキュリティ上の接続経路や認証状態を示さない。
エ：分離境界をまたぐ経路を持つ資産は攻撃経路の橋渡し点になり得るため、その防御状態と侵害有無が波及評価の中心になる。
総合解説：「分離されている」という記述だけで安全と結論付けず、境界を越える例外通信・二重接続資産・管理経路を確認する。科目Bでは図中の例外経路が重要な手掛かりになる。

Q101 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

不正アクセス調査のため認証ログを1年間保持する要件がある。一方で、ログに含む個人情報は必要最小限にし、閲覧者を限定するという要件もある。最も適切な設計はどれか。
ア．調査に必要な識別子・時刻・結果などを定義し、不要な属性を記録せず、保管ログをアクセス制御・改ざん防止の下で1年間保持する。
イ．個人情報を避けるため、認証ログを一切記録しない。
ウ．調査に使う可能性を考えて、利用者の全入力内容を無期限に保存する。
エ．1年間保存する代わりに、誰でも閲覧できる共有フォルダへ置く。

正答・4肢解説・総合解説

正答：ア．調査に必要な識別子・時刻・結果などを定義し、不要な属性を記録せず、保管ログをアクセス制御・改ざん防止の下で1年間保持する。
ア：保持期間だけでなく、取得項目の最小化と閲覧統制を組み合わせることで、調査可能性とプライバシー要件を同時に満たせる。
イ：1年間の調査ログ保持要件を満たさない。
ウ：必要最小限という要件と保持期間要件の双方に反する。
エ：保持期間を満たしても、閲覧者を限定する要件を満たさない。
総合解説：複数要件は一方を犠牲にして満たすのではなく、データ最小化、保持期間、アクセス制御、完全性保護などを組み合わせて両立させる。

Q102 6-4 科目Bシナリオ判断 / 要求・制約・構成図の読解

IaaS上に業務システムを構築する。クラウド事業者は物理設備と基盤を管理するが、利用企業はOS設定、IAM、ネットワーク設定、アプリケーションを管理する契約である。「クラウド事業者が安全なので、管理者権限の棚卸しは不要」とする設計判断の問題点として最も適切なものはどれか。
ア．IaaSでは利用企業は物理データセンターの入退室管理だけを担当する。
イ．契約上利用企業が管理するIAMは利用企業自身の責任範囲であり、クラウド事業者の基盤対策だけでは管理者権限の統制を代替できない。
ウ．クラウドでは責任分界という概念は存在しない。
エ．管理者権限は可用性だけの問題であり、セキュリティとは無関係である。

正答・4肢解説・総合解説

正答：イ．契約上利用企業が管理するIAMは利用企業自身の責任範囲であり、クラウド事業者の基盤対策だけでは管理者権限の統制を代替できない。
ア：記載された契約では物理基盤は事業者側であり、利用企業側の責任範囲の説明も逆である。
イ：構成・契約から責任境界を読み取ると、IAMは利用企業側の管理対象である。事業者の責任範囲と利用者の責任範囲を混同してはいけない。
ウ：クラウドでもサービスモデルや契約に応じた責任分担が存在する。
エ：過大な管理権限や不適切なIAMは機密性・完全性・可用性に重大な影響を与える。
総合解説：科目Bの構成・契約読解では、「誰が何を管理するか」を明示的に切り分ける。外部委託やクラウド利用でも、利用者側に残る責任はなくならない。

Q103 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

外部公開VPN装置では既知の重大脆弱性は確認されていないが、利用者アカウントにMFAがなく、退職者の認証情報が一部残存していた。VPN接続後は管理用セグメントへ到達できる。外部攻撃者の攻撃経路として最も優先して評価すべきものはどれか。
ア．VPN装置の筐体を外部から物理的に分解する経路だけを評価する。
イ．社内プリンタの用紙切れから管理セグメントへ侵入する経路を評価する。
ウ．漏えい・残存した認証情報でVPNへログインし、管理用セグメントへ到達する経路。
エ．VPNの暗号アルゴリズム名だけを見て、認証・到達範囲は評価しない。

正答・4肢解説・総合解説

正答：ウ．漏えい・残存した認証情報でVPNへログインし、管理用セグメントへ到達する経路。
ア：インターネット越しの攻撃シナリオとして現実性が低く、提示された認証上の弱点を無視している。
イ：提示された情報から技術的な因果関係がない。
ウ：脆弱性の有無だけでなく、認証情報の悪用可能性と接続後に得られる到達範囲を組み合わせると、現実的で影響の大きい経路になる。
エ：攻撃経路は単一要素ではなく、初期侵入から権限・到達先まで連鎖で評価する必要がある。
総合解説：攻撃経路の評価では、脅威主体が利用可能な入口、成立条件、得られる権限、次の到達先を連鎖として見る。CVSSや装置種別だけでなく、認証・権限・ネットワーク到達性を組み合わせる。

Q104 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

利用者Aがフィッシングメールのリンクから偽サイトへ誘導された。その後、Aのクラウドアカウントで見覚えのないOAuthアプリへの同意が記録され、数時間後に大量のファイル閲覧が発生した。最も整合する攻撃経路はどれか。
ア．大量ファイル閲覧が先に起き、その結果としてフィッシングメールが生成された。
イ．OAuthアプリは権限を持たないので、同意記録は調査対象外である。
ウ．端末の電源ケーブルが抜けたことが、クラウドファイル閲覧の直接原因である。
エ．フィッシングを起点に利用者の認証・同意を悪用し、OAuthアプリの権限でクラウドデータへ継続アクセスした。

正答・4肢解説・総合解説

正答：エ．フィッシングを起点に利用者の認証・同意を悪用し、OAuthアプリの権限でクラウドデータへ継続アクセスした。
ア：提示された時系列と逆であり、因果関係の説明にもならない。
イ：OAuthアプリは付与されたスコープに応じてデータへアクセスできるため、同意内容は重要な手掛かりである。
ウ：提示されたクラウド上の認証・同意イベントと関係しない。
エ：時系列上、偽サイトへの誘導、OAuth同意、ファイル閲覧が連続しており、認証・権限付与を悪用したクラウド上の攻撃経路として整合する。
総合解説：クラウドの攻撃経路では、パスワード窃取だけでなく、トークンやアプリ同意など権限委任の悪用も考える。時系列と権限の変化を追うことが重要である。

Q105 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

公開WebアプリにSSRF脆弱性があり、その実行環境からインスタンスメタデータサービスへ到達できる。Webアプリに付与されたクラウドロールは、機密情報を保存するオブジェクトストレージの読み取り権限を持つ。最も重要な攻撃経路はどれか。
ア．SSRFでメタデータサービスへアクセスし、一時的な認証情報を取得して、そのロール権限で機密ストレージを読み取る経路。
イ．Webアプリの画面色を変更し、その色からストレージ内容を推測する経路。
ウ．SSRFがあるため、IAMロールの権限範囲は確認しなくてよい。
エ．ストレージが暗号化されていれば、正規ロール権限での読み取りも必ず不可能になる。

正答・4肢解説・総合解説

正答：ア．SSRFでメタデータサービスへアクセスし、一時的な認証情報を取得して、そのロール権限で機密ストレージを読み取る経路。
ア：SSRF、メタデータ到達性、過大なIAM権限が連鎖すると、公開Webアプリの脆弱性からクラウドデータへ到達できる。
イ：技術的な到達関係がなく、提示された脆弱性と権限を利用していない。
ウ：SSRF後に何へ到達できるかはロール権限で大きく変わるため、権限範囲の確認が不可欠である。
エ：暗号化は権限を持つ正規サービスからの復号・読み取りを通常可能にするため、過大権限の問題を消さない。
総合解説：攻撃経路は「一つの脆弱性」ではなく、到達性と権限の連鎖で評価する。SSRFを入口として認証情報へ到達し、その権限が機密資産へつながるかを確認する。

Q106 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

CI/CD環境では外部レジストリから依存パッケージを取得し、ビルドサーバが本番用成果物を生成する。ビルドサーバにはコード署名鍵を利用できる権限があり、成果物は署名済みであれば本番へ自動配布される。攻撃経路として最も重大なものはどれか。
ア．公開Webサイトの背景画像を変更するだけで、署名鍵を使わず本番バイナリを置き換える経路。
イ．依存パッケージを侵害し、ビルド工程で悪性コードを混入させ、正規の署名権限で署名された成果物として本番へ配布する経路。
ウ．ビルドサーバが署名鍵を利用できるため、依存パッケージの完全性確認は不要である。
エ．署名済みであれば内容は必ず安全なので、攻撃経路は存在しない。

正答・4肢解説・総合解説

正答：イ．依存パッケージを侵害し、ビルド工程で悪性コードを混入させ、正規の署名権限で署名された成果物として本番へ配布する経路。
ア：提示された自動配布条件と署名要件を満たさず、主要な信頼経路を説明していない。
イ：外部依存、ビルド環境、署名権限、自動配布が直列につながるため、一点の侵害が信頼された成果物として本番へ波及する経路になる。
ウ：署名はビルドされた成果物に正当性の外観を与えるため、むしろビルド前の供給元検証が重要になる。
エ：侵害されたビルド環境が正規鍵を利用できれば、悪性内容でも正規署名され得る。
総合解説：サプライチェーン攻撃では、どの段階が次段階から信頼されているかを追う。ビルド・署名・配布が自動化されているほど、上流の侵害が下流へ広く伝播する可能性がある。

Q107 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

社内LANはほぼフラットで、複数端末に同一のローカル管理者パスワードが設定されている。1台の端末で認証情報窃取型マルウェアが検知された。ランサムウェアの横展開経路として最も優先して確認すべきものはどれか。
ア．端末の壁紙ファイルを順番に閲覧して暗号鍵を生成する経路。
イ．ネットワーク分離が十分であると仮定し、他端末への到達性を確認しない。
ウ．窃取した管理者資格情報を再利用し、SMBやリモート管理機能を使って他端末へ展開する経路。
エ．管理者資格情報の共通利用は影響しないので、DNS名だけを調査する。

正答・4肢解説・総合解説

正答：ウ．窃取した管理者資格情報を再利用し、SMBやリモート管理機能を使って他端末へ展開する経路。
ア：横展開の成立条件と関係がない。
イ：問題文ではフラットなLANとされており、仮定が事実に反する。
ウ：共通管理者パスワードと広い相互到達性がそろうと、1台の侵害から資格情報再利用による横展開が成立しやすい。
エ：資格情報再利用は横展開の重要な成立条件であり、無視できない。
総合解説：攻撃経路は、侵害済み資産から次の資産へ移るために必要な到達性・認証情報・サービスを確認する。フラットネットワークと共通特権資格情報の組合せは横展開リスクを高める。

Q108 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

企業のDNSには promo.example.jp が外部SaaSのホスト名を指すCNAMEとして残っているが、そのSaaS契約は既に解約され、SaaS側では同じ識別子を第三者が取得できる状態である。主要なリスクはどれか。
ア．CNAMEが存在するだけで、企業のルートドメインの秘密鍵が自動的に漏えいする。
イ．SaaS契約を解約したので、DNSレコードが残っていても一切影響しない。
ウ．DNSレコードは表示速度だけに関係し、セキュリティには関係しない。
エ．第三者がSaaS側の識別子を取得し、企業ドメイン配下のpromo.example.jpを自分のコンテンツへ向ける経路。

正答・4肢解説・総合解説

正答：エ．第三者がSaaS側の識別子を取得し、企業ドメイン配下のpromo.example.jpを自分のコンテンツへ向ける経路。
ア：CNAME設定そのものからルートドメインの秘密鍵が漏れるわけではない。
イ：参照だけが残ることで、外部サービス側の再取得可能性が攻撃経路になる。
ウ：名前解決先を第三者に制御されると、フィッシングやコンテンツ改ざんなどに利用され得る。
エ：DNS側の参照が残り、参照先サービスの所有権が失われているため、第三者が信頼されたサブドメインを支配できる可能性がある。
総合解説：攻撃経路分析では、技術資産だけでなく外部サービスの所有状態も見る。DNSと外部サービスのライフサイクルがずれると、信頼関係が攻撃者へ移る場合がある。

Q109 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

二つの脆弱性AとBがある。AはCVSSが高いが、隔離された検証環境にあり外部から到達できない。BはCVSSがAより低いが、インターネット公開システムにあり、侵害すると顧客データ管理系へ到達できる。優先リスク評価として最も適切なものはどれか。
ア．CVSSだけで決めず、到達可能性、悪用可能性、資産重要度、後続の攻撃経路と事業影響を含めてAとBを比較する。
イ．CVSSが高いAを常に無条件で最優先とする。
ウ．CVSSが低いBは、インターネット公開であっても評価対象外とする。
エ．どちらも脆弱性なので、資産価値やネットワーク構成を調べる必要はない。

正答・4肢解説・総合解説

正答：ア．CVSSだけで決めず、到達可能性、悪用可能性、資産重要度、後続の攻撃経路と事業影響を含めてAとBを比較する。
ア：リスク評価では脆弱性の深刻度だけでなく、脅威事象が成立する条件と影響を組み合わせる必要がある。Bが実際の攻撃経路上で高いリスクとなる可能性もある。
イ：CVSSは脆弱性の深刻度指標であり、組織固有の到達性や事業影響を単独では表さない。
ウ：外部到達性や後続資産への経路によって実リスクが高くなる場合がある。
エ：リスクは脆弱性だけでは決まらず、脅威、成立条件、影響、既存管理策を含めて評価する。
総合解説：脆弱性スコアは重要な入力だが、リスクそのものではない。科目Bでは、システム固有の構成、資産重要度、攻撃者の到達経路、既存対策を組み合わせて優先度を判断する。

Q110 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

外部委託者の正規アカウントが窃取された。対象アプリは、利用者認証に加えて「管理対象端末であること」「端末が基準準拠であること」をアクセス条件としている。攻撃者は個人所有端末から正しいIDとパスワードだけで接続を試みた。想定どおり統制が働く場合、どこで攻撃経路が止まるか。
ア．正しいパスワードを知っていれば、端末条件は必ず無視される。
イ．認証情報が正しくても、端末状態の条件を満たさないためアプリへのアクセス許可段階で遮断される。
ウ．攻撃者は必ず物理データセンターへ侵入しなければならない。
エ．アカウントが正規のものなら、端末の準拠状態を確認する意味はない。

正答・4肢解説・総合解説

正答：イ．認証情報が正しくても、端末状態の条件を満たさないためアプリへのアクセス許可段階で遮断される。
ア：端末条件をアクセス判断に組み込む設計と矛盾する。
イ：本人確認だけでなく端末状態も継続的なアクセス判断に使う設計では、窃取資格情報だけでは条件を満たせない。
ウ：問題の攻撃経路はリモートアクセスであり、物理侵入は必要条件ではない。
エ：資格情報窃取を想定すると、複数の文脈要素を使うことが攻撃経路の遮断に役立つ。
総合解説：攻撃経路分析では「どの管理策がどの段階で成立条件を崩すか」を確認する。複数条件によるアクセス判断は、単一の資格情報漏えいからの侵入経路を狭める。

Q111 6-4 科目Bシナリオ判断 / リスク・攻撃経路の特定

同日のログは次の順だった。09:02 WAFがSQLインジェクションを遮断、09:35 海外IPから社員BのVPNログイン成功、09:41 Bの端末を経由した管理サーバへのRDP接続、09:50 管理サーバから複数ホストへコマンド実行。初期侵入経路として最も整合するものはどれか。
ア．09:02のSQLインジェクションが成功し、WAF遮断ログは成功を意味する。
イ．09:50のコマンド実行が原因で、09:35のVPNログインが過去に発生した。
ウ．社員BのVPN認証情報が悪用され、VPN経由で内部へ侵入した可能性。
エ．海外IPという情報だけで、攻撃者が社員B本人でないと断定できる。

正答・4肢解説・総合解説

正答：ウ．社員BのVPN認証情報が悪用され、VPN経由で内部へ侵入した可能性。
ア：「遮断」と記録されているため、追加証拠なしに成功と判断するのは不適切である。
イ：時系列の因果関係が逆である。
ウ：WAFの攻撃は遮断されている一方、その後にVPN成功と内部横展開が連続しているため、VPN認証を起点とする経路が時系列に最も整合する。
エ：異常の手掛かりにはなるが、VPNログと他の認証・端末情報を合わせて確認する必要がある。
総合解説：科目Bのログ読解では、単一の目立つアラートに引っ張られず、成功・失敗、時刻、主体、次の行動をつなげて経路を推定する。

Q112 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

インターネット公開中の業務Webサーバに認証不要のRCE脆弱性が見つかり、同脆弱性の悪用が外部で観測されている。ベンダ修正パッチは提供済みで、適用には15分程度の停止が必要である。最も適切な対応はどれか。
ア．次回の年次メンテナンスまで何もせず待つ。
イ．パッチは適用せず、脆弱性の存在を社内で秘密にする。
ウ．サービス停止を避けるため、ログ取得も止める。
エ．事業影響を確認したうえで緊急変更手続を用いて早期にパッチを適用し、適用までの間は可能な緩和策と監視を行う。

正答・4肢解説・総合解説

正答：エ．事業影響を確認したうえで緊急変更手続を用いて早期にパッチを適用し、適用までの間は可能な緩和策と監視を行う。
ア：悪用中の重大脆弱性を長期間露出させることになり、リスクに見合わない。
イ：情報を隠しても技術的な露出は減らず、対応遅延の原因になる。
ウ：検知能力を下げるだけで、脆弱性の悪用可能性は下がらない。
エ：公開範囲が広く悪用も観測されているため、短時間の計画停止より侵害リスクが高い。変更統制を維持しつつ迅速に修正するのが適切である。
総合解説：対策の優先順位は脆弱性の深刻度だけでなく、公開状況、悪用事実、資産重要度、変更影響、代替緩和策を組み合わせて決める。緊急時でも変更手続と事後確認を省略しない。

Q113 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

ある組織では標的型メール訓練とEDRは導入済みだが、バックアップは本番ネットワークから常時書き込み可能で、過去1年間復元試験をしていない。ランサムウェア対策に追加予算を一つ優先投入する場合、最も適切なものはどれか。
ア．改ざん・削除されにくいバックアップ方式へ改善し、定期的な復元試験で実際に回復できることを確認する。
イ．メール訓練のポスターを毎日貼り替えることだけに全予算を使う。
ウ．バックアップを本番サーバと同じ認証情報で常時マウントし続ける。
エ．復元試験を省略し、バックアップ成功ログだけを信頼する。

正答・4肢解説・総合解説

正答：ア．改ざん・削除されにくいバックアップ方式へ改善し、定期的な復元試験で実際に回復できることを確認する。
ア：予防・検知だけでなく回復能力が弱点になっているため、攻撃者から分離されたバックアップと復元試験を優先する合理性が高い。
イ：教育は有効でも、提示された重大な回復上の弱点を改善しない。
ウ：侵害時にバックアップも同時に暗号化・削除されるリスクを高める。
エ：バックアップ取得成功と実際の復元可能性は同義ではない。
総合解説：リスクベースの優先順位付けでは、既存対策と残る弱点を確認する。ランサムウェアでは、回復可能性を実証できるバックアップと復旧手順が重要である。

Q114 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

営業担当者のノートPC紛失時に、保存済み顧客ファイルの内容を第三者に読まれるリスクを直接低減したい。最も直接的な対策はどれか。
ア．WebアプリのWAFルールを追加する。
イ．端末のストレージを強固に暗号化し、鍵を適切な認証で保護する。
ウ．社内DNSキャッシュ時間を短くする。
エ．サーバ室のUPS容量を増やす。

正答・4肢解説・総合解説

正答：イ．端末のストレージを強固に暗号化し、鍵を適切な認証で保護する。
ア：インターネット経由のWeb攻撃対策であり、紛失端末内の保存データ保護には直接効かない。
イ：端末を物理的に取得された場合でも、保存データを復号できなければ機密性侵害を抑えられるため、脅威に直接対応する。
ウ：端末紛失時の保存データ機密性とは関係しない。
エ：可用性対策であり、紛失したノートPCのデータ読み取りリスクを直接下げない。
総合解説：対策比較では、保護対象・脅威・攻撃段階を一致させる。目的が「紛失した端末内のデータを読ませない」であれば、保存データ暗号化が最も直接的である。

Q115 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

APIのBearerトークンがクライアント端末から窃取され、攻撃者が有効期限内にAPIを呼び出した。再発防止策として最も適切な組合せはどれか。
ア．APIサーバの背景画像を変更し、利用者に注意を促す。
イ．トークンの有効期間を無期限にして再認証を減らす。
ウ．漏えいトークンを速やかに失効できる仕組み、短い有効期間、端末側の安全な保管、異常利用の監視を組み合わせる。
エ．通信をHTTPSにしているので、端末内でのトークン保管方法は考慮しない。

正答・4肢解説・総合解説

正答：ウ．漏えいトークンを速やかに失効できる仕組み、短い有効期間、端末側の安全な保管、異常利用の監視を組み合わせる。
ア：資格情報の悪用を防ぐ技術的な効果がない。
イ：漏えい時に攻撃者が長期間利用できるため逆効果である。
ウ：Bearerトークンは所持者が利用できるため、漏えい時の有効時間を抑え、失効・保管・監視を組み合わせることが直接的である。
エ：HTTPSは通信路を保護するが、端末内からの窃取リスクは別に管理する必要がある。
総合解説：同じ「認証」でも、パスワード窃取とトークン窃取では有効な対策が異なる。原因となった資格情報の種類と利用方式に合わせて、失効・寿命・保管・監視を設計する。

Q116 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

数百Gbps級のボリューム型DDoSにより、企業拠点のインターネット回線自体が飽和している。自社FWのCPU使用率はまだ低い。最も効果が期待できる対策はどれか。
ア．自社LAN内のPCにパーソナルFWを追加するだけで対応する。
イ．WAFで特定のURLパターンだけを拒否する。
ウ．インシデント中は監視を停止し、帯域を節約する。
エ．通信が自社回線へ到達する前に、ISPやDDoSスクラビングサービス、CDN等の上流で攻撃トラフィックを吸収・除去する。

正答・4肢解説・総合解説

正答：エ．通信が自社回線へ到達する前に、ISPやDDoSスクラビングサービス、CDN等の上流で攻撃トラフィックを吸収・除去する。
ア：外部回線の帯域飽和を解消できない。
イ：アプリケーション層攻撃には有効な場合があるが、回線飽和型の大量トラフィックには不十分である。
ウ：監視停止による帯域削減は限定的で、攻撃緩和にもならず状況把握を悪化させる。
エ：回線自体が飽和しているため、自社設備に到達してから遮断しても帯域枯渇は解消しない。上流での緩和が必要である。
総合解説：対策案は攻撃がボトルネックにしている層に合わせる。ボリューム型DDoSで回線が飽和している場合、自社境界より上流で吸収・フィルタリングする必要がある。

Q117 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

運用担当者は障害対応のため本番環境へ管理者権限が必要だが、恒常的な特権付与による内部不正リスクが問題になっている。業務要件を満たしつつリスクを下げる対策として最も適切なものはどれか。
ア．申請・承認に基づくJIT型の特権付与やPAMを用い、利用時間と対象を限定し、操作を記録・監視する。
イ．障害対応を不可能にするため、全管理者権限を永久に廃止する。
ウ．管理者アカウントを全員で共有して承認手続を不要にする。
エ．特権操作のログを削除し、担当者の心理的負担を減らす。

正答・4肢解説・総合解説

正答：ア．申請・承認に基づくJIT型の特権付与やPAMを用い、利用時間と対象を限定し、操作を記録・監視する。
ア：必要時の権限を残しつつ、恒常的な特権を減らして追跡性を高められるため、業務と統制の両立に適している。
イ：業務要件を満たさず、可用性・復旧に支障が出る。
ウ：誰が操作したか追跡できず、内部不正リスクを高める。
エ：監査証跡を失い、抑止・検知・調査能力を下げる。
総合解説：優先順位付けでは「リスクをゼロにする」だけでなく、業務上必要な機能を維持しながら残留リスクを下げる対策を選ぶ。最小権限、時間限定、承認、監視を組み合わせる。

Q118 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

製造設備の制御端末に重大な脆弱性が見つかったが、ベンダ検証の都合で3か月間パッチを適用できない。設備停止も困難である。最も適切な暫定対応はどれか。
ア．パッチできないので、脆弱性情報を無視して通常運用を続ける。
イ．対象端末を必要最小限の通信へ分離し、不要サービスを停止し、許可通信を限定して監視を強化し、正式パッチ適用計画を管理する。
ウ．設備停止が難しいため、インターネットから直接管理できるよう公開する。
エ．監視ログを削除し、障害の発見を遅らせる。

正答・4肢解説・総合解説

正答：イ．対象端末を必要最小限の通信へ分離し、不要サービスを停止し、許可通信を限定して監視を強化し、正式パッチ適用計画を管理する。
ア：既知リスクを放置しており、暫定的な低減策も講じていない。
イ：修正まで時間がある場合でも、到達性と悪用条件を下げる補完策を組み合わせ、残るリスクを監視しながら恒久対策へつなぐ必要がある。
ウ：攻撃面を広げ、脆弱性悪用の可能性を高める。
エ：検知・調査能力を低下させるため不適切である。
総合解説：恒久対策がすぐ取れない場合は、ネットワーク分離、サービス削減、アクセス制御、監視などの補完策でリスクを下げ、期限・責任者付きで修正計画を追跡する。

Q119 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

機密データを扱うSaaS候補企業が「監査結果の提示もセキュリティ条項への合意もできない」と回答した。代替事業者は存在するが、導入は1か月遅れる。最も適切な判断はどれか。
ア．導入が早いので、リスク評価も契約確認もせず採用する。
イ．候補企業が有名なら、監査・契約条件は一切不要とする。
ウ．情報の重要度と委託リスクを再評価し、必要な保証を得られないなら代替事業者や業務設計の変更を検討し、正式なリスク判断を行う。
エ．担当者個人が口頭で「大丈夫」と判断し、記録を残さない。

正答・4肢解説・総合解説

正答：ウ．情報の重要度と委託リスクを再評価し、必要な保証を得られないなら代替事業者や業務設計の変更を検討し、正式なリスク判断を行う。
ア：機密データの委託リスクを把握・管理できない。
イ：企業知名度は個別サービスの統制を保証しない。
ウ：委託先管理では、必要なセキュリティ保証を契約・評価で確認する。納期だけを理由に、説明不能なリスクを暗黙受容すべきではない。
エ：組織としてのリスク判断・説明責任・再評価ができない。
総合解説：対策案比較では、技術対策だけでなく契約、委託先選定、業務変更、リスク受容を含めて比較する。重要リスクの受容は適切な権限者が根拠を記録して行う。

Q120 6-4 科目Bシナリオ判断 / 対策案比較・優先順位付け

SIEMの「管理者権限での夜間ログイン」ルールが、夜間バッチ運用の正規管理者によって毎日大量に発報し、重要なアラートが埋もれている。最も適切な改善はどれか。
ア．誤検知が多いのでルールを完全に削除し、夜間の特権ログインを一切監視しない。
イ．正規バッチの詳細を確認せず、全管理者アカウントを例外登録する。
ウ．アラート件数を減らすため、SIEMのログ受信自体を停止する。
エ．正規バッチのアカウント・時間帯・接続元などの文脈を条件に組み込み、例外を限定しつつ、それ以外の夜間特権利用は検知し続ける。

正答・4肢解説・総合解説

正答：エ．正規バッチのアカウント・時間帯・接続元などの文脈を条件に組み込み、例外を限定しつつ、それ以外の夜間特権利用は検知し続ける。
ア：重要な異常も検知できなくなり、検知能力を過度に失う。
イ：例外範囲が広すぎて、不正な特権利用も見逃すおそれがある。
ウ：他の検知・調査にも必要なログを失うため不適切である。
エ：検知目的を保ったまま正常パターンを具体的に除外し、資産や主体の文脈を使ってシグナル対雑音比を改善するのが適切である。
総合解説：優先順位付けは「アラートを減らすこと」ではなく、重要な異常を見つけやすくすることが目的である。正常パターンを限定的に除外し、資産重要度や主体情報を使ってルールを調整する。

Q121 6-5 科目B総合演習 / 技術×管理の複合事例

クラウドストレージが誤って公開設定となり、外部から顧客データが閲覧された可能性がある。設定変更は担当者が個人判断で行い、レビュー記録もない。再発防止まで含む対応として最も適切なものはどれか。
ア．公開設定を直ちに是正してアクセス状況を調査し、設定変更の承認・レビュー・継続監視を導入する。
イ．公開設定だけ戻し、誰がなぜ変更したかは調べない。
ウ．顧客データを削除してログも消去する。
エ．クラウド利用を全面禁止し、今回の設定原因は分析しない。

正答・4肢解説・総合解説

正答：ア．公開設定を直ちに是正してアクセス状況を調査し、設定変更の承認・レビュー・継続監視を導入する。
ア：技術的な露出を止めるだけでなく、無レビュー変更という管理上の原因も是正しなければ同種事故が再発し得る。
イ：目前の露出は止まるが、変更管理上の原因が残る。
ウ：証拠や影響確認に必要な情報を失い、説明責任も果たせない。
エ：過剰な対処であり、根本原因と必要な統制の特定にならない。
総合解説：科目Bの複合事例では、技術的な封じ込め、影響調査、変更管理・承認・監視など管理面の是正を一連で考える。

Q122 6-5 科目B総合演習 / 技術×管理の複合事例

決算処理中に基幹システムがランサムウェア被害を受けた。バックアップは存在するが、直近の復元試験は失敗している。経営部門は「最短で復旧してほしい」と要求している。最も適切な対応はどれか。
ア．復元試験に失敗していても、確認せず全システムへ一括復元する。
イ．感染範囲を封じ込め、バックアップの完全性と復元可能性を検証したうえで、事業優先順位に沿ってクリーンな環境へ段階的に復旧する。
ウ．決算期なので封じ込めを行わず、感染端末もネットワークへ接続したままにする。
エ．業務影響を考慮せず、すべてのシステムを同じ優先度で復旧する。

正答・4肢解説・総合解説

正答：イ．感染範囲を封じ込め、バックアップの完全性と復元可能性を検証したうえで、事業優先順位に沿ってクリーンな環境へ段階的に復旧する。
ア：バックアップが利用可能か不明で、失敗や再感染のリスクが高い。
イ：速度だけを優先して汚染や不完全なバックアップを本番へ戻すと再侵害やデータ損失を招く。業務優先順位と技術的信頼性を両立させる必要がある。
ウ：被害拡大の可能性を高める。
エ：重要業務や依存関係に基づく復旧優先順位が必要である。
総合解説：復旧は単なる再起動ではない。安全な復旧点、バックアップの完全性、依存関係、事業優先順位を確認し、監視しながら段階的に戻す。

Q123 6-5 科目B総合演習 / 技術×管理の複合事例

自社製品に認証不要のRCE脆弱性が外部研究者から報告された。修正版はまだ開発中で、公開環境での悪用は未確認である。PSIRTの初期対応として最も適切なものはどれか。
ア．悪用が未確認なので、研究者への返信も記録も行わない。
イ．修正版がない段階で、検証せず全顧客へ「必ず侵害されている」と通知する。
ウ．報告を検証・トリアージし、影響製品と緩和策を整理し、修正計画と関係者への通知・開示方針を調整する。
エ．技術チームだけで処理し、サポート・法務・広報などの関係者には一切共有しない。

正答・4肢解説・総合解説

正答：ウ．報告を検証・トリアージし、影響製品と緩和策を整理し、修正計画と関係者への通知・開示方針を調整する。
ア：未悪用でも重大な脆弱性なら検証・追跡が必要である。
イ：未確認事実を断定すると誤情報になる。
ウ：PSIRTでは脆弱性の真偽・影響を技術評価したうえで、修正、暫定緩和、顧客コミュニケーションを一体で管理する。
エ：顧客影響や開示を伴う場合、必要な関係者との連携が不可欠である。
総合解説：製品脆弱性対応は、技術検証だけでなく、修正計画、暫定対策、顧客通知、開示調整を含む横断的な活動である。

Q124 6-5 科目B総合演習 / 技術×管理の複合事例

営業部が未承認のSaaSへ顧客情報を保存していることが判明した。即時停止すると商談中の業務が大きく混乱する。最も適切な対応はどれか。
ア．業務が便利なので、今後も無期限に未承認利用を黙認する。
イ．証拠を残さずSaaSアカウントを削除し、顧客データの所在確認もしない。
ウ．営業部全員を懲戒すれば、技術・契約上の是正は不要とする。
エ．保存情報・利用者・契約条件・アクセス権を把握してリスクを評価し、必要な保護と移行計画を決め、承認済み環境へ段階的に移す。

正答・4肢解説・総合解説

正答：エ．保存情報・利用者・契約条件・アクセス権を把握してリスクを評価し、必要な保護と移行計画を決め、承認済み環境へ段階的に移す。
ア：組織としてリスクと契約条件を管理できない。
イ：データ残存や影響確認ができなくなる。
ウ：原因となる承認手続や代替環境などの改善が残る。
エ：無条件放置も即時遮断だけも不十分である。実態把握、リスク評価、法務・契約確認、業務移行を組み合わせる必要がある。
総合解説：複合事例では、人の行動だけを責めず、利用実態、データ、契約、アクセス、代替手段、承認プロセスを含めて是正する。

Q125 6-5 科目B総合演習 / 技術×管理の複合事例

保守委託先のVPNアカウントが侵害され、自社ネットワークへの不正接続に使われた。委託契約にはインシデント通知と協力義務が定められている。最も適切な対応はどれか。
ア．当該アクセスを停止・資格情報を失効して影響を調査し、契約上の連絡経路で委託先と証拠・原因・再発防止策を協議する。
イ．委託先の問題なので、自社のVPNログや到達先を調査しない。
ウ．委託先との契約関係を理由に、侵害アカウントをそのまま有効にする。
エ．原因調査前にすべての委託先を同一に危険と判断し、証拠を破棄する。

正答・4肢解説・総合解説

正答：ア．当該アクセスを停止・資格情報を失効して影響を調査し、契約上の連絡経路で委託先と証拠・原因・再発防止策を協議する。
ア：自社側の封じ込めと、委託先側の原因究明・再発防止を契約に基づいて同時に進める必要がある。
イ：自社への侵入影響を把握できない。
ウ：被害拡大を防ぐ封じ込めを怠っている。
エ：個別事実に基づく評価と証拠保全が必要である。
総合解説：サプライチェーン・委託先インシデントでは、自社環境の封じ込めと影響分析に加えて、契約上の通知・協力・是正要求を使い外部組織と連携する。

Q126 6-5 科目B総合演習 / 技術×管理の複合事例

SOCでは1日1万件のアラートが発生し、担当者が重要アラートを見落とした。調査すると、低重要度資産の既知正常動作による誤検知が多数を占めていた。再発防止として最も適切なものはどれか。
ア．担当者へ「もっと注意するように」と伝えるだけで終える。
イ．検知ルールを資産重要度や正常動作の文脈で調整し、優先度基準・エスカレーション手順・要員配置も見直す。
ウ．重要アラートも含めて全ての検知ルールを停止する。
エ．アラート件数を減らすため、低重要度資産のログ収集を無条件で全部廃止する。

正答・4肢解説・総合解説

正答：イ．検知ルールを資産重要度や正常動作の文脈で調整し、優先度基準・エスカレーション手順・要員配置も見直す。
ア：構造的なアラート過多と優先度設計が改善されない。
イ：技術的なルール品質と運用上の処理能力の双方が問題であり、片方だけでなく優先度・手順・体制まで改善する必要がある。
ウ：検知能力を失い、本来の目的を達成できない。
エ：調査や他の検知に必要なログまで失う可能性がある。
総合解説：SOC運用では、検知精度、優先順位、処理手順、人員・自動化を一体で設計する。見落としの根本原因が量と優先度なら、個人注意だけでは再発防止にならない。

Q127 6-5 科目B総合演習 / 技術×管理の複合事例

公開APIのTLS証明書が期限切れになり、複数顧客の接続が停止した。証明書は担当者個人の表計算だけで管理され、引継ぎもなかった。最も適切な再発防止策はどれか。
ア．期限切れのたびに顧客から連絡が来るのを待つ。
イ．証明書の有効期限を記録しないことで管理負荷を減らす。
ウ．証明書・鍵の資産台帳、所有者、更新期限、通知・自動更新、更新後確認を組織的なライフサイクルとして管理する。
エ．担当者個人の記憶だけに依存し、引継ぎ資料を作らない。

正答・4肢解説・総合解説

正答：ウ．証明書・鍵の資産台帳、所有者、更新期限、通知・自動更新、更新後確認を組織的なライフサイクルとして管理する。
ア：受動的で、可用性影響を繰り返す。
イ：期限管理ができず、再発可能性が高まる。
ウ：技術的には証明書更新が必要だが、再発原因は属人的な資産・期限管理にもあるため、所有者と更新プロセスを制度化する必要がある。
エ：属人化を強め、同じ原因を残す。
総合解説：複合事例では、障害を直すだけでなく、資産台帳、責任者、期限監視、自動化、変更確認など運用プロセスへ落とし込む。

Q128 6-5 科目B総合演習 / 技術×管理の複合事例

本番DBで不審なデータ削除があり、操作は共有のroot相当アカウントで行われていた。5人の運用担当者が同じパスワードを知っている。最も適切な対応はどれか。
ア．誰が操作したか不明なので、調査をせず全員を同じ責任とする。
イ．共有パスワードをそのままにして、ログだけ削除する。
ウ．共有アカウントを増やして、担当者ごとに別名の共有IDを作る。
エ．関連ログを保全して影響と操作経路を調査し、共有資格情報を安全に変更したうえで、個人識別可能な特権アカウントとPAMへ移行する。

正答・4肢解説・総合解説

正答：エ．関連ログを保全して影響と操作経路を調査し、共有資格情報を安全に変更したうえで、個人識別可能な特権アカウントとPAMへ移行する。
ア：事実確認と証拠に基づく調査が必要である。
イ：再利用リスクと追跡不能性を残し、証拠も失う。
ウ：個人単位の識別・最小権限・承認という根本課題を解決しない。
エ：まず証跡を保ちつつ封じ込めを行い、恒久的には共有アカウントによる追跡不能性を解消する必要がある。
総合解説：特権インシデントでは、証拠を失わずに資格情報を封じ込め、誰が何をしたか追跡できる認証・承認・記録へ改善する。

Q129 6-5 科目B総合演習 / 技術×管理の複合事例

開発者がクラウドAPIキーを公開Gitリポジトリへ誤ってコミットした。数分後に削除コミットを行ったが、キー自体はまだ有効である。最も適切な対応はどれか。
ア．キーを直ちに失効・再発行し、利用ログを確認し、今後はSecrets Managerやコミット前検査などで秘密情報をコードから分離する。
イ．最新コミットから消えたので、キーは安全になったと判断する。
ウ．キーを長期間有効のままにし、漏えいの有無は調べない。
エ．再発防止として、全ソースコードのレビューを禁止する。

正答・4肢解説・総合解説

正答：ア．キーを直ちに失効・再発行し、利用ログを確認し、今後はSecrets Managerやコミット前検査などで秘密情報をコードから分離する。
ア：履歴から文字列を消すだけでは、既に取得されたキーの悪用を止められない。資格情報そのものを無効化し、漏えい有無を確認する必要がある。
イ：リポジトリ履歴や外部取得済みコピーに残っている可能性がある。
ウ：悪用可能な資格情報を残すことになる。
エ：秘密管理の改善にはならず、品質・セキュリティ確認を弱める。
総合解説：秘密情報漏えいでは、削除より失効が優先される。即時の資格情報ローテーション、利用確認、保管方式と開発プロセスの改善まで行う。

Q130 6-5 科目B総合演習 / 技術×管理の複合事例

取引先を装ったメールにより、経理担当者が振込先を変更し送金した直後に詐欺の疑いが判明した。最も適切な初動と再発防止の組合せはどれか。
ア．メールを削除して忘れ、金融機関には連絡しない。
イ．金融機関へ速やかに連絡して組戻し等の可能性を確認し、メール・認証ログを保全し、振込先変更を別経路で確認する手続を強化する。
ウ．全メール利用を恒久的に禁止する。
エ．送金した担当者だけを処分し、振込手続や認証ログは見直さない。

正答・4肢解説・総合解説

正答：イ．金融機関へ速やかに連絡して組戻し等の可能性を確認し、メール・認証ログを保全し、振込先変更を別経路で確認する手続を強化する。
ア：資金回収機会と証拠を失う。
イ：金銭被害の拡大防止、攻撃経路の調査、業務プロセス上の再発防止を同時に進める必要がある。
ウ：業務継続性を損なう過剰対応で、振込変更確認という根本統制も整理していない。
エ：攻撃が成立した業務・技術上の原因を残す。
総合解説：BECのような複合事例では、技術ログだけでなく送金業務の統制が重要である。緊急連絡、証拠保全、本人確認・変更確認手続の改善を組み合わせる。

Q131 6-5 科目B総合演習 / 技術×管理の複合事例

工場のIoT機器に既知脆弱性があるが、メーカーは修正版を提供していない。機器は生産上不可欠で、直ちに撤去できない。最も適切な対応はどれか。
ア．修正版がないので、脆弱性の存在をリスク台帳から削除する。
イ．利便性向上のため、機器をインターネットへ直接公開する。
ウ．到達性を最小化するネットワーク分離・通信許可制・監視を実施し、代替機器や更新計画を作成し、残留リスクを権限者が期限付きで判断する。
エ．現場担当者一人の口頭判断で永久にリスクを受容する。

正答・4肢解説・総合解説

正答：ウ．到達性を最小化するネットワーク分離・通信許可制・監視を実施し、代替機器や更新計画を作成し、残留リスクを権限者が期限付きで判断する。
ア：未解決リスクを見えなくするだけで、実際の危険は減らない。
イ：到達性を広げ、悪用可能性を高める。
ウ：技術的な補完策で現在のリスクを下げつつ、恒久対策と残留リスクの正式な管理を行う必要がある。
エ：重要な残留リスクは適切な権限者が根拠・期限・条件を記録して判断すべきである。
総合解説：修正不能・停止不能の資産では、補完的管理策、監視、更新計画、残留リスク受容を一つの管理サイクルとして扱う。

Q132 6-5 科目B総合演習 / 技術×管理の複合事例

企業買収後、被買収企業のネットワークを本社へ接続する計画がある。被買収企業では資産台帳が不完全で、MFA未導入、複数のサポート切れOSが残っている。最も適切な統合方針はどれか。
ア．統合を急ぐため、評価せず本社LANへ全面接続する。
イ．被買収企業の全システムを即日廃棄し、業務影響は考慮しない。
ウ．会社が別だった時期の問題なので、買収後のセキュリティ責任は存在しない。
エ．資産・ID・脆弱性・接続経路を先に評価し、必要な隔離・認証強化・更新を行ったうえで段階的に本社ネットワークへ統合する。

正答・4肢解説・総合解説

正答：エ．資産・ID・脆弱性・接続経路を先に評価し、必要な隔離・認証強化・更新を行ったうえで段階的に本社ネットワークへ統合する。
ア：未知のリスクを直接本社へ持ち込む可能性がある。
イ：現実的でなく、必要な事業継続とリスク低減のバランスを欠く。
ウ：統合後の事業・システムリスクとして管理する必要がある。
エ：未知の資産や弱い認証をそのまま信頼境界へ入れると、本社側へリスクが伝播する。接続前評価と段階的統合が必要である。
総合解説：M&Aや組織統合では、技術接続の前に資産・ID・脆弱性・依存関係を把握し、信頼境界を段階的に広げる。

Q133 6-5 科目B総合演習 / 経営層・関係者への指導・助言

取締役会から「セキュリティ状況を一枚で示してほしい」と依頼された。SOCにはアラート件数や未修正CVE件数が多数ある。経営層への報告として最も適切なものはどれか。
ア．重要な事業・資産ごとに主要リスクシナリオ、想定影響、現在の対策、残留リスク、必要な意思決定を要約する。
イ．SIEMの生ログを加工せず全件印刷して提出する。
ウ．CVE件数だけを示し、対象資産や影響は説明しない。
エ．問題があっても不安を与えないため、リスク情報をすべて隠す。

正答・4肢解説・総合解説

正答：ア．重要な事業・資産ごとに主要リスクシナリオ、想定影響、現在の対策、残留リスク、必要な意思決定を要約する。
ア：経営層が必要とするのは技術イベントの羅列ではなく、事業影響と意思決定につながるリスク情報である。
イ：情報量が多すぎ、重要度や事業影響が分からず意思決定に結び付きにくい。
ウ：脆弱性数だけでは組織固有のリスクや優先順位を示せない。
エ：経営判断に必要な情報を欠き、適切なリスク受容・投資判断ができない。
総合解説：経営層向け助言では、技術指標を事業リスクへ翻訳する。何が起こり得るか、どの業務へ影響するか、何を決める必要があるかを明確にする。

Q134 6-5 科目B総合演習 / 経営層・関係者への指導・助言

社長が「来年度のセキュリティ目標はインシデント0件にする。0件なら対策成功とみなす」と提案した。支援士としての助言で最も適切なものはどれか。
ア．事故0件を唯一の目標とし、検知件数が増えたらSOCを評価下げする。
イ．インシデント件数だけでなく、リスク低減、検知・対応時間、復旧能力、重大事象の影響など複数指標を用い、残留リスクを経営として管理する。
ウ．目標設定自体をやめ、セキュリティ状況を測定しない。
エ．発生した事故を記録しなければ0件を達成できると助言する。

正答・4肢解説・総合解説

正答：イ．インシデント件数だけでなく、リスク低減、検知・対応時間、復旧能力、重大事象の影響など複数指標を用い、残留リスクを経営として管理する。
ア：検知能力向上で発見件数が増える場合もあり、逆インセンティブになる。
イ：インシデント件数は外部脅威や検知能力にも左右され、0件だけでは安全性を評価できない。予防・検知・対応・回復を含む指標が必要である。
ウ：改善や経営判断のためには適切な指標が必要である。
エ：リスクを隠すだけで、実際の安全性や説明責任を損なう。
総合解説：サイバーリスクは完全にゼロにできない。経営には、残留リスクを理解したうえで、予防だけでなく検知・対応・回復まで含むレジリエンスを測る指標を示す。

Q135 6-5 科目B総合演習 / 経営層・関係者への指導・助言

過去2年間重大インシデントが発生していないため、CFOが「セキュリティ予算を半減しても安全性は変わらない」と主張している。最も適切な助言はどれか。
ア．事故がないので、全セキュリティ対策を停止してよい。
イ．予算は多いほど必ず安全なので、リスク評価なしに無制限に増額する。
ウ．事故未発生だけでは将来リスクや統制有効性を証明できないため、脅威動向、資産重要度、管理策の有効性、演習結果などを基に投資判断する。
エ．判断材料はCFOの印象だけで十分で、技術・事業データは不要である。

正答・4肢解説・総合解説

正答：ウ．事故未発生だけでは将来リスクや統制有効性を証明できないため、脅威動向、資産重要度、管理策の有効性、演習結果などを基に投資判断する。
ア：将来リスクや既存対策が事故を抑えていた可能性を無視している。
イ：費用対効果や事業リスクに基づく優先順位が必要である。
ウ：事故件数は結果指標の一つであり、運が良かった可能性や未検知の可能性もある。予防・検知・復旧能力を含む根拠が必要である。
エ：組織的なリスク判断には客観的な根拠が必要である。
総合解説：経営助言では、単一の結果指標を因果関係と誤解しない。リスク評価、統制の有効性、演習・監査、脅威変化を合わせて投資判断を支援する。

Q136 6-5 科目B総合演習 / 経営層・関係者への指導・助言

事業部長が、売上に重要な旧システムの脆弱性について「今期は改修しないので受容したい」と相談してきた。支援士の助言として最も適切なものはどれか。
ア．担当エンジニアが個人判断で永久に受容し、経営には報告しない。
イ．改修しないなら、脆弱性を資産台帳から削除する。
ウ．受容したリスクは今後一切見直さない。
エ．想定シナリオ、事業影響、既存・追加対策、残留リスクを文書化し、適切なリスク所有者が期限・見直し条件付きで受容判断する。

正答・4肢解説・総合解説

正答：エ．想定シナリオ、事業影響、既存・追加対策、残留リスクを文書化し、適切なリスク所有者が期限・見直し条件付きで受容判断する。
ア：重要な事業リスクの受容権限と説明責任を満たさない。
イ：記録を消してもリスクは残る。
ウ：脅威・資産・事業条件は変化するため、見直し条件や期限が必要である。
エ：リスク受容は単なる未対応ではなく、残留リスクを理解し、権限者が根拠をもって意思決定し、再評価できる状態にする必要がある。
総合解説：助言のポイントは、技術担当者が経営判断を代行しないこと。リスクの内容と選択肢を可視化し、権限あるリスク所有者の判断を支援する。

Q137 6-5 科目B総合演習 / 経営層・関係者への指導・助言

顧客情報漏えいの可能性があるが、調査は継続中で件数は確定していない。営業部から「今すぐ全顧客に100万件漏えいしたと断定して発表しよう」と提案された。最も適切な助言はどれか。
ア．法務・広報・経営・インシデント対応部門で、確定事実と未確定事項を区別し、法令・契約上の要件と被害抑止を踏まえて適時に通知内容を決める。
イ．調査が完全に終わるまで、法令上の期限があっても一切連絡しない。
ウ．営業部だけで公表内容を決め、法務・経営・技術部門とは共有しない。
エ．証拠保全より先にログを削除し、情報を少なくしてから公表する。

正答・4肢解説・総合解説

正答：ア．法務・広報・経営・インシデント対応部門で、確定事実と未確定事項を区別し、法令・契約上の要件と被害抑止を踏まえて適時に通知内容を決める。
ア：迅速性は重要だが、未確認情報を断定すると誤報になる。必要な通知期限を守りながら、事実・不確実性・利用者が取るべき行動を整理する。
イ：通知要件や被害拡大防止を無視する可能性がある。
ウ：法的義務、事実確認、事業影響を横断的に判断できない。
エ：調査・説明責任に必要な証拠を失う。
総合解説：関係者への助言では、速度と正確性を両立し、確定事実と推測を分ける。通知・公表は法務、広報、経営、技術の連携事項である。

Q138 6-5 科目B総合演習 / 経営層・関係者への指導・助言

経営会議で「委託先の危険度は、保有する製品の最高CVSS値だけで順位付けすればよい」と提案された。最も適切な助言はどれか。
ア．最高CVSS値だけで全委託先を評価し、業務内容は見ない。
イ．CVSSに加えて、委託業務の重要度、扱う情報、接続権限、代替可能性、委託先の管理策・インシデント対応能力などを含めて評価する。
ウ．委託先は社外なので、自社のリスク評価対象から除外する。
エ．委託先の自己申告だけを無条件で信頼し、契約・監査・証跡を確認しない。

正答・4肢解説・総合解説

正答：イ．CVSSに加えて、委託業務の重要度、扱う情報、接続権限、代替可能性、委託先の管理策・インシデント対応能力などを含めて評価する。
ア：同じ脆弱性でも接続範囲や扱うデータによって組織への影響は異なる。
イ：委託先リスクは脆弱性一件の技術スコアだけでは表せない。自社との依存関係と事業影響を含む評価が必要である。
ウ：委託を通じたリスクは自社の事業・情報へ影響する。
エ：必要な保証を確認できず、管理策の実効性を判断できない。
総合解説：経営層には、サプライチェーンのリスクを「外部の問題」ではなく、自社の業務依存・データ・アクセスの問題として説明する。

Q139 6-5 科目B総合演習 / 経営層・関係者への指導・助言

経営者が「サイバー保険に加入すれば、MFAやバックアップへの投資は不要になる」と考えている。最も適切な助言はどれか。
ア．保険加入後は、セキュリティ対策を全て停止しても契約上必ず補償される。
イ．保険はリスク管理と無関係なので、加入効果を一切評価しない。
ウ．保険は一部の財務損失を移転できても、業務停止・信用低下・適用除外などの残留リスクは残るため、予防・検知・復旧対策を継続する。
エ．保険料が高ければ、技術対策より必ず優れた対策である。

正答・4肢解説・総合解説

正答：ウ．保険は一部の財務損失を移転できても、業務停止・信用低下・適用除外などの残留リスクは残るため、予防・検知・復旧対策を継続する。
ア：補償条件・免責があり得るうえ、業務停止や信用への影響は保険だけで解消できない。
イ：財務影響の移転手段として評価対象になり得る。
ウ：保険はリスク対応手段の一つだが、技術・運用上のリスクを消滅させるものではない。補償条件や免責も含めて残留リスクを管理する必要がある。
エ：費用と効果、補償範囲、残留リスクを比較して判断すべきである。
総合解説：経営助言では、リスク低減・回避・移転・受容を区別する。保険による移転後も、残る業務・信用・法的・技術的リスクを説明する。

Q140 6-5 科目B総合演習 / 経営層・関係者への指導・助言

前年度比で平均検知時間は大幅に短縮したが、同じ原因によるインシデントが繰り返し発生している。経営層への説明として最も適切なものはどれか。
ア．検知時間が短くなったので、再発件数は無視してよい。
イ．再発があるので、検知時間改善は価値がないと結論付ける。
ウ．指標同士は比較できないため、今後は一切測定しない。
エ．検知能力は改善している一方、根本原因の是正や管理策の有効性に課題があるため、再発率や是正完了率も合わせて追跡する。

正答・4肢解説・総合解説

正答：エ．検知能力は改善している一方、根本原因の是正や管理策の有効性に課題があるため、再発率や是正完了率も合わせて追跡する。
ア：同じ原因の再発は是正が機能していない可能性を示す。
イ：検知改善自体は有益であり、別の改善課題と区別して評価する。
ウ：複数指標を組み合わせることで改善サイクルを評価できる。
エ：一つの指標改善だけで全体を成功と評価せず、検知後の是正・再発防止まで含めた結果を見る必要がある。
総合解説：経営層には、先行・結果指標を単独で見ず、因果関係を仮説として検証する形で示す。検知、対応、是正、再発防止を一連で評価する。

Q141 6-5 科目B総合演習 / 経営層・関係者への指導・助言

新サービス公開直前に重大な設計上の弱点が見つかった。修正には2週間必要だが、事業部は予定どおり公開したい。支援士として最も適切な対応はどれか。
ア．修正延期、機能限定、補完対策付き公開などの選択肢について、攻撃成立条件・事業影響・残留リスクを示し、適切なリスク所有者の意思決定を支援する。
イ．セキュリティ部門だけで事業影響を無視して公開中止を決定する。
ウ．納期を優先し、弱点の内容を誰にも知らせず公開する。
エ．公開後に考えることにして、暫定対策も監視も行わない。

正答・4肢解説・総合解説

正答：ア．修正延期、機能限定、補完対策付き公開などの選択肢について、攻撃成立条件・事業影響・残留リスクを示し、適切なリスク所有者の意思決定を支援する。
ア：技術担当が独断で事業判断を代行せず、対策案と残留リスクを比較可能な形で提示するのが専門家として適切である。
イ：重大リスクなら中止が妥当な場合もあるが、意思決定権限と事業影響を含む正式な判断が必要である。
ウ：リスクを隠したまま受容させることになり、適切な判断ではない。
エ：既知リスクを無管理で残す。
総合解説：支援士の助言は「技術的に正しい一案を押し付ける」ことではなく、事業条件とリスクを整理し、意思決定者が比較できるよう支援することにある。

Q142 6-5 科目B総合演習 / 長文ケース・時間配分

2027年度新制度案では、情報処理安全確保支援士試験の科目Bは120分・12問とされている。受験開始時の時間配分方針として最も合理的なものはどれか。
ア．最初の1問に120分すべてを使い、残りは見ない。
イ．1問当たり約10分を一つの目安としつつ、難易度に応じて調整し、未回答確認や見直しのための時間も残す。
ウ．すべての問題に必ず秒単位で同じ時間を使い、難易度差は無視する。
エ．時間を確認すると集中が切れるので、終了時刻まで一度も残り時間を見ない。

正答・4肢解説・総合解説

正答：イ．1問当たり約10分を一つの目安としつつ、難易度に応じて調整し、未回答確認や見直しのための時間も残す。
ア：全12問に取り組む機会を失うため、時間配分として不適切である。
イ：120分を12問で割ると単純平均は10分だが、問題の重さは均一とは限らない。平均を目安にしつつ、難問への滞留を避けて見直し時間を確保する方が合理的である。
ウ：問題ごとの読解量や判断量が異なり得るため、硬直的な配分は不合理である。
エ：長文・複数問題の試験では、進捗確認が時間切れ防止に役立つ。
総合解説：科目Bの時間配分に公式の「1問10分ルール」があるわけではない。120分・12問という公表値から得られる平均を目安にし、問題量と残り時間に応じて柔軟に調整する学習戦略である。

Q143 6-5 科目B総合演習 / 長文ケース・時間配分

科目B形式の長文ケースに、組織概要、ネットワーク構成、ログ表、契約条件が記載されている。設問は「最優先で封じ込めるべき経路」を問うている。読み進め方として最も適切なものはどれか。
ア．設問を読まず、本文の全単語を暗記してから考える。
イ．契約条件だけを読み、ネットワーク構成とログは無視する。
ウ．設問の要求語を確認し、攻撃経路・到達性・事業影響に関係する構成図とログを中心に読み、必要に応じて他の記述へ戻る。
エ．最初に目に入った専門用語だけで答えを決め、本文へ戻らない。

正答・4肢解説・総合解説

正答：ウ．設問の要求語を確認し、攻撃経路・到達性・事業影響に関係する構成図とログを中心に読み、必要に応じて他の記述へ戻る。
ア：時間を使う割に、設問と無関係な情報まで保持しようとして効率が悪い。
イ：封じ込めるべき攻撃経路の判断には技術的な到達性や事象が必要である。
ウ：長文全体を均等に暗記するより、設問が何を求めているかを先に把握して関連情報を抽出する方が、判断根拠を整理しやすい。
エ：設問の根拠をシナリオ内の複数情報から確認する必要がある。
総合解説：科目Bでは、設問要求→関連箇所→根拠の照合という順に読むと、長文でも必要情報を見失いにくい。一般知識より問題文の具体条件を優先する。

Q144 6-5 科目B総合演習 / 長文ケース・時間配分

ある設問で「パッチ適用」と「ネットワーク分離」のどちらも一般には有効だが、本文には「ベンダ検証のため90日間パッチ適用禁止」と明記されている。最も適切な判断方法はどれか。
ア．一般にパッチが最善なので、本文の禁止条件を無視してパッチを選ぶ。
イ．二つとも一般に有効なので、必ず複数正答だと決めつける。
ウ．本文の条件は読まず、用語の印象だけで決める。
エ．本文の制約を優先し、90日間はパッチ以外の補完策を選び、恒久的なパッチ計画は別途管理する。

正答・4肢解説・総合解説

正答：エ．本文の制約を優先し、90日間はパッチ以外の補完策を選び、恒久的なパッチ計画は別途管理する。
ア：設問の前提条件に反する。
イ：資格ブートキャンプでは正答1つに標準化しており、設問の制約で最適解を絞る。
ウ：ケース問題では明示条件が正答選択の主要根拠になる。
エ：一般論で有効な対策でも、シナリオの明示制約に反するならその時点の最適解ではない。制約下で実行可能な代替策を選ぶ。
総合解説：長文ケースで選択肢がどれももっともらしく見えるときは、対象時点、禁止条件、責任範囲、事業影響などの限定条件を探す。

Q145 6-5 科目B総合演習 / 長文ケース・時間配分

長文ケースには、FWログがJST、クラウド監査ログがUTC、端末ログが5分進んだローカル時刻で記録されていると明記されている。攻撃の順序を判断する際に最も適切な方法はどれか。
ア．各ログのタイムゾーンと既知の時刻ずれを補正して同じ基準時刻にそろえ、その後に事象を並べる。
イ．表示された時計文字列だけを大小比較し、タイムゾーンは無視する。
ウ．端末ログだけを正しいと仮定し、他のログを捨てる。
エ．ログの時刻は調査に使えないので、全て削除する。

正答・4肢解説・総合解説

正答：ア．各ログのタイムゾーンと既知の時刻ずれを補正して同じ基準時刻にそろえ、その後に事象を並べる。
ア：異なる時刻基準をそのまま比較すると順序を誤認する。まず正規化し、補正根拠を残してから因果関係を評価する。
イ：同じ瞬間でも表記が異なるため、誤った時系列になる。
ウ：複数証拠の突合という利点を失い、端末時計のずれも無視する。
エ：補正可能な時刻情報は時系列分析に重要である。
総合解説：長文ケースの表は、列名・単位・タイムゾーン・注記まで読む。時系列は攻撃経路や初動判断の基礎になるため、基準をそろえてから比較する。

Q146 6-5 科目B総合演習 / 長文ケース・時間配分

科目Bの残り時間が15分で、未処理の設問が4問ある。1問目だけが特に難しく、3分考えても決め手がない。最も合理的な進め方はどれか。
ア．難問が解けるまで15分すべてを使い、他3問は見ない。
イ．現時点の根拠を整理して一旦印を付け、残り3問にも回答時間を確保し、余れば難問へ戻る。
ウ．時間が少ないので、本文を読まず4問すべて同じ選択肢にする。
エ．残り時間を使わず、すぐ試験を終了する。

正答・4肢解説・総合解説

正答：イ．現時点の根拠を整理して一旦印を付け、残り3問にも回答時間を確保し、余れば難問へ戻る。
ア：全体の回答機会を失う可能性が高い。
イ：一つの難問に残り時間を集中すると、他の設問へ取り組む機会を失う。残り時間と未処理数を見て配分を切り替えるのが合理的である。
ウ：根拠に基づく判断を放棄している。
エ：未処理問題に取り組める時間を自ら捨てる。
総合解説：時間配分は正答内容とは別の試験技能である。難問への滞留を管理し、全設問を確認する機会を確保する。

Q147 6-5 科目B総合演習 / 長文ケース・時間配分

長文ケースの冒頭で「本問では『重要端末』を、製造停止に直結する端末と定義する」と記載されている。一般社内規程では別の定義を使っている。設問で重要端末の優先復旧対象を問われた場合、最も適切な判断はどれか。
ア．自分の勤務先の社内規程の定義を優先し、問題文の定義を無視する。
イ．一般辞書の意味だけで判断し、本文の定義は読まない。
ウ．この設問では本文中の定義を用い、製造停止に直結する端末を重要端末として扱う。
エ．定義がある問題は解けないと判断し、必ず未回答にする。

正答・4肢解説・総合解説

正答：ウ．この設問では本文中の定義を用い、製造停止に直結する端末を重要端末として扱う。
ア：受験者ごとに前提が変わり、設問の共通条件を崩す。
イ：問題文が明示的に範囲を限定しているため不適切である。
ウ：ケース問題では、問題文が用語の範囲を明示している場合、その定義が設問解釈の前提になる。
エ：明示定義はむしろ判断基準を与える情報である。
総合解説：長文ケースでは、冒頭の定義、注記、前提条件が後続設問の基準になる。外部知識は補助として使い、問題文の定義を上書きしない。

Q148 6-5 科目B総合演習 / 長文ケース・時間配分

構成図の凡例には「実線＝現在稼働中の通信」「破線＝来期導入予定の通信」とある。インシデントは今月発生した。破線で描かれた新SIEM連携について、現在の検知能力を評価する際の扱いとして最も適切なものはどれか。
ア．図に描かれているものは全て現在稼働中とみなす。
イ．破線だけを現在稼働中とみなし、実線を将来予定とする。
ウ．構成図の凡例は意味がないので、見ずに回答する。
エ．破線は未導入なので現在の管理策としては数えず、現行の実線構成で取得できるログと検知能力を評価する。

正答・4肢解説・総合解説

正答：エ．破線は未導入なので現在の管理策としては数えず、現行の実線構成で取得できるログと検知能力を評価する。
ア：凡例の明示条件に反する。
イ：凡例を逆に解釈している。
ウ：凡例は線や記号の意味を定義する重要な情報である。
エ：図の凡例によって時間軸が区別されているため、将来予定を現行対策として扱うとリスク評価を誤る。
総合解説：科目Bの図表読解では、凡例、注記、時点、単位を確認する。将来計画と現行統制を混同すると、存在しない対策を前提に判断してしまう。

Q149 6-5 科目B総合演習 / 長文ケース・時間配分

見直し時間に入ったところ、ある設問が「最も不適切なもの」を選ぶ問題だったことに気付いた。最も有効な確認はどれか。
ア．設問の「適切／不適切」などの要求語を再確認し、選んだ肢がその要求に対応しているかを根拠とともに照合する。
イ．最初に選んだ肢は必ず正しいと考え、設問文は読み直さない。
ウ．選択肢の長さだけで正答を変更する。
エ．設問の要求語は無視し、覚えている用語が多い肢を選ぶ。

正答・4肢解説・総合解説

正答：ア．設問の「適切／不適切」などの要求語を再確認し、選んだ肢がその要求に対応しているかを根拠とともに照合する。
ア：知識が合っていても設問の極性を読み違えると誤答になる。見直しでは要求語と選択肢の対応を確認する価値が高い。
イ：読み違いを発見する機会を失う。
ウ：長さは正誤の根拠にならない。
エ：何を問われているかと関係なく判断している。
総合解説：長文試験の見直しでは、全てを最初から解き直すより、未回答、迷い、設問の肯否、選択肢番号の転記など誤りやすい点を優先確認する。

Q150 6-5 科目B総合演習 / 長文ケース・時間配分

一つの長文ケースに設問1と設問2がある。設問2には「設問1の対策を既に実施した後とする」という追加条件がある。設問2を解くときの考え方として最も適切なものはどれか。
ア．設問1で使った前提を永久に固定し、設問2の追加条件は無視する。
イ．設問2の追加条件を反映して状態を更新し、設問1時点の構成をそのまま前提にしない。
ウ．設問1の自分の解答が正しいか不安なので、設問2は本文を読まず同じ肢を選ぶ。
エ．同一ケース内では前提が変わることはないと決めつける。

正答・4肢解説・総合解説

正答：イ．設問2の追加条件を反映して状態を更新し、設問1時点の構成をそのまま前提にしない。
ア：設問2の明示条件に反する。
イ：同じケースでも設問ごとに時点や前提が変わることがある。追加条件を読み落とすと、既に解消されたリスクを再評価するなど判断を誤る。
ウ：設問2固有の要求と条件を検討していない。
エ：問題文が追加条件を明示している場合は状態が変わる。
総合解説：長文ケースでは、設問ごとの「時点」「前提」「対策実施済み」「仮定」を確認する。前の設問の状態を無意識に引きずらないことが重要である。