Q001 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

セキュリティバイデザインの考え方として最も適切なものはどれか。
ア．企画・要件定義などの早い段階からセキュリティを設計へ組み込み、ライフサイクル全体で継続的に扱う。
イ．リリース直前に脆弱性診断だけを実施し、その結果だけで安全性を判断する。
ウ．利用者が必要に応じて安全な設定へ変更することを前提に、初期設定は利便性を最優先する。
エ．インシデント発生後にのみセキュリティ要件を追加し、それ以前は機能要件だけを管理する。

正答・4肢解説・総合解説

正答：ア．企画・要件定義などの早い段階からセキュリティを設計へ組み込み、ライフサイクル全体で継続的に扱う。
ア：後工程での追加対策だけに依存せず、初期段階からセキュリティ要件と設計判断へ反映する考え方である。
イ：診断は重要だが、設計段階からの組込みを代替できず、セキュリティバイデザインの趣旨ではない。
ウ：安全性を利用者任せにする考え方はSecure by Defaultにも反しやすい。
エ：事後対応だけでは設計上の欠陥を早期に抑制できない。
総合解説：IPAは企画・要件定義でセキュリティ要件を定義し、設計・実装・テストへつなげる能力を求めている。SSDFもセキュリティ実務をSDLCへ統合することを重視する。

Q002 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

Secure by Defaultの設計例として最も適切なものはどれか。
ア．全ての管理機能を初期状態でインターネットへ公開し、利用者へ閉鎖手順を案内する。
イ．新規導入時は不要な外部公開機能を無効にし、必要な機能だけを管理者が明示的に有効化する。
ウ．初期パスワードを全製品で同一にし、導入後の変更を推奨するだけにする。
エ．監査ログを既定で停止し、障害が起きた場合だけ利用者が有効化する。

正答・4肢解説・総合解説

正答：イ．新規導入時は不要な外部公開機能を無効にし、必要な機能だけを管理者が明示的に有効化する。
ア：安全化の負担を利用者へ転嫁しており、Secure by Defaultとは逆である。
イ：初期状態から安全側に倒し、利用者が追加設定をしなくても過度な露出を避ける設計である。
ウ：共通の既定資格情報は不正利用を招きやすく、安全な既定値ではない。
エ：必要なセキュリティ機能を既定で無効にする設計は安全側とはいえない。
総合解説：Secure by Defaultは、利用者が高度な知識を持たなくても初期状態で合理的に安全であることを狙う。CISAも安全化の負担を顧客だけに負わせないことを重視している。

Q003 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

業務アプリケーションからデータベースへ接続するアカウントの設計として、最小権限の原則に最も合致するものはどれか。
ア．将来の機能追加に備えてDB管理者権限を付与しておく。
イ．権限管理を簡単にするため、全アプリケーションで同じ高権限アカウントを共用する。
ウ．アプリケーションが実際に必要とする表・操作だけに権限を限定し、管理者権限は付与しない。
エ．読み取り専用処理であっても、更新・削除権限を含む標準ロールを一律に付与する。

正答・4肢解説・総合解説

正答：ウ．アプリケーションが実際に必要とする表・操作だけに権限を限定し、管理者権限は付与しない。
ア：将来の可能性だけを理由に過剰な権限を付与するのは最小権限に反する。
イ：共有高権限アカウントは侵害時の影響と追跡困難性を増大させる。
ウ：必要な業務機能を満たす最小限の権限へ限定することで、侵害時の影響範囲を抑える。
エ：不要な更新・削除権限は付与すべきではない。
総合解説：最小権限は、主体に必要な権限だけを付与する基本原則である。設計時点でサービスアカウントやAPI権限の境界を明確にする。

Q004 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

多層防御（defense in depth）の説明として最も適切なものはどれか。
ア．最も強力な一つの製品へ全ての防御を集約し、他の対策を省略する。
イ．同一の設定ミスを持つ同一製品を複数台並べれば十分である。
ウ．侵入後の復旧だけを重視し、予防や検知は不要とする。
エ．単一の対策が突破されても直ちに重大事故へ至らないよう、独立性のある複数の対策を重ねる。

正答・4肢解説・総合解説

正答：エ．単一の対策が突破されても直ちに重大事故へ至らないよう、独立性のある複数の対策を重ねる。
ア：単一対策への集中は、その対策の失敗が全体の失敗になりやすい。
イ：同じ弱点を共有する対策の単純な複製は、独立した防御層とは限らない。
ウ：多層防御は特定の一段階だけへ偏る考え方ではない。
エ：予防・検知・抑止・回復など複数層の対策で、単一障害点への依存を減らす考え方である。
総合解説：設計では認証、認可、ネットワーク分離、暗号化、監視などを組み合わせ、どれか一つが破られても被害を限定できる構造を目指す。

Q005 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

社内向け管理APIを新規設計する。攻撃対象領域（attack surface）を小さくする施策として最も適切なものはどれか。
ア．外部から不要な管理APIを公開せず、管理ネットワークから必要なエンドポイントだけへ到達可能にする。
イ．全管理APIを公開した上で、URLを推測しにくい名前に変更する。
ウ．全APIを公開し、異常が起きた場合だけログで追跡する。
エ．管理APIに説明用の詳細なバージョン情報を常時表示する。

正答・4肢解説・総合解説

正答：ア．外部から不要な管理APIを公開せず、管理ネットワークから必要なエンドポイントだけへ到達可能にする。
ア：不要な公開面と到達経路を減らすことで、攻撃者が試行できる入口を縮小できる。
イ：秘密のURL名だけではアクセス制御にならず、公開面そのものは残る。
ウ：検知は必要だが、不要な公開面を削減する予防策にはならない。
エ：不要な技術情報の公開は攻撃者の偵察を助ける場合がある。
総合解説：攻撃対象領域の削減では、不要な機能・ポート・インタフェース・権限をなくし、必要なものだけを限定公開する。

Q006 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

認可サービスとの通信に失敗した場合の業務APIの振る舞いとして、機密データ保護を優先する設計はどれか。
ア．業務継続を優先し、認可確認ができない要求は全て許可する。
イ．認可結果を確認できない要求は拒否し、必要に応じて限定的な障害応答を返す。
ウ．最後に成功した別利用者の認可結果を再利用する。
エ．認可処理自体を削除し、アプリケーション画面の表示制御だけに任せる。

正答・4肢解説・総合解説

正答：イ．認可結果を確認できない要求は拒否し、必要に応じて限定的な障害応答を返す。
ア：認可障害がそのままアクセス制御の迂回経路になる。
イ：認可不能時にアクセスを許可しないfail-closedの設計で、機密性を優先できる。
ウ：主体が異なる認可結果の流用は不正アクセスを招く。
エ：表示制御はサーバ側の認可を代替できない。
総合解説：フェールセーフ設計では故障時の安全側の状態を定義する。ただし可用性要件との両立が必要で、どの機能を閉じるかはリスクに基づき設計する。

Q007 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

脅威分析で「盗まれた一般利用者アカウントから大量の顧客データを一括取得される」シナリオが重大と評価された。設計要件への反映として最も適切なものはどれか。
ア．脅威分析書を保管するだけで、既存要件は変更しない。
イ．全利用者へ一括取得権限を付与して運用を単純化する。
ウ．利用者単位の認可に加え、一括取得権限の分離、取得量制御、異常な大量取得の監視を要件化する。
エ．大量取得が起きても事後に利用者へ注意喚起することだけを要件とする。

正答・4肢解説・総合解説

正答：ウ．利用者単位の認可に加え、一括取得権限の分離、取得量制御、異常な大量取得の監視を要件化する。
ア：分析結果を要件や設計へ反映しなければリスク低減につながらない。
イ：脅威シナリオの成立条件を強める方向であり不適切である。
ウ：具体的な脅威シナリオから、権限制御・利用制限・検知という複数の設計要件へ落とし込んでいる。
エ：事後注意だけでは予防・検知・影響限定が不足する。
総合解説：脅威分析は文書化で終わらず、認証・認可・監視・データ保護など検証可能なセキュリティ要件へ変換する必要がある。

Q008 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

セキュリティ要件として最も検証しやすい記述はどれか。
ア．システムは十分に安全でなければならない。
イ．必要に応じてログを残すことが望ましい。
ウ．最新のセキュリティ技術をできるだけ利用する。
エ．管理者権限の操作は全件監査ログへ記録し、利用者ID・対象・操作結果・時刻を含める。

正答・4肢解説・総合解説

正答：エ．管理者権限の操作は全件監査ログへ記録し、利用者ID・対象・操作結果・時刻を含める。
ア：「十分に安全」の判定基準がなく、受入れテストへ直接つなげにくい。
イ：「必要に応じて」「望ましい」では適用条件と必須性が曖昧である。
ウ：「最新」「できるだけ」が曖昧で、具体的な検証基準にならない。
エ：対象、条件、記録項目が具体的で、レビューやテストで達成可否を確認できる。
総合解説：良いセキュリティ要件は、対象・条件・期待結果が明確で追跡・検証できる。後続の設計、実装、テストとのトレーサビリティも重要である。

Q009 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

新しいSaaSの管理者向け機能を設計している。Secure by Designの観点から最も望ましい方針はどれか。
ア．高リスク機能は安全な既定設定と明確な警告を用意し、保護機能を有効にするための追加購入や複雑な手順を前提にしない。
イ．高リスク機能の防御は全てオプションにし、利用者が自力で設定できる場合だけ保護する。
ウ．既定では誰でも管理機能へ接続できるようにし、運用開始後に必要なら制限する。
エ．脆弱性情報は製品評価が下がるため、修正後も利用者へ知らせない。

正答・4肢解説・総合解説

正答：ア．高リスク機能は安全な既定設定と明確な警告を用意し、保護機能を有効にするための追加購入や複雑な手順を前提にしない。
ア：顧客の安全を製品設計の責任として扱い、安全化の負担を利用者だけへ転嫁しない方針である。
イ：安全性を顧客の知識や作業へ過度に依存させる。
ウ：初期状態の露出が高く、安全な既定値になっていない。
エ：透明性と適切な情報提供を欠き、利用者のリスク判断を妨げる。
総合解説：CISAのSecure by Designは顧客のセキュリティ成果に製造者が責任を持つ考え方を示す。設計・既定値・運用支援を一体として考える。

Q010 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

要件からテストまでのセキュリティ・トレーサビリティを確保する主な目的はどれか。
ア．各工程の文書名を同じにして、内容の対応確認を不要にする。
イ．脅威や要件が、どの設計・実装・テストで満たされるかを追跡し、抜けや変更影響を確認できるようにする。
ウ．開発後に要件文書を削除し、ソースコードだけを正本にする。
エ．全ての脅威を同じ重要度として扱い、優先順位付けを行わない。

正答・4肢解説・総合解説

正答：イ．脅威や要件が、どの設計・実装・テストで満たされるかを追跡し、抜けや変更影響を確認できるようにする。
ア：文書名の統一だけでは要件と実装・テストの対応を保証できない。
イ：要求と実装・検証の対応関係を維持すると、未実装や未検証の要件を発見しやすい。
ウ：要件の根拠や変更影響を追跡しにくくなる。
エ：トレーサビリティは優先順位付けを否定するものではない。
総合解説：トレーサビリティは、脅威→要件→設計→実装→テスト→結果の関係を追える状態にする。変更時の影響分析にも有効である。

Q011 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

既存システムの制約で一部通信を直ちに強い相互認証へ変更できない。セキュリティバイデザインの観点から次の対応として最も適切なものはどれか。
ア．完全な対策ができないため、認証に関する要件自体を削除する。
イ．現状動いているので、リスク評価を行わず無期限に現行方式を使う。
ウ．残存リスクを明示し、到達元制限・監視強化・認証移行計画などの代替管理策と期限を設けて段階的に解消する。
エ．相互認証へ変えられない代わりに、利用者向け画面の配色を変更する。

正答・4肢解説・総合解説

正答：ウ．残存リスクを明示し、到達元制限・監視強化・認証移行計画などの代替管理策と期限を設けて段階的に解消する。
ア：制約があることはリスクや要件を消す理由にはならない。
イ：残存リスクの評価・受容・解消計画がなく、管理された設計判断ではない。
ウ：制約を無視せず、リスクを可視化して補完策と解消計画を組み合わせる現実的な設計判断である。
エ：当該脅威に対するリスク低減効果がない。
総合解説：セキュリティ要件は制約とともに扱う。実現困難な場合でも、残存リスク、補完管理策、責任者、期限を明確にして追跡可能にする。

Q012 4-1 セキュリティ要件・設計 / セキュリティバイデザイン

リリース直前に、インターネット公開APIで認証回避につながる高影響の欠陥が再現された。納期は厳しい。最も適切な判断はどれか。
ア．納期を優先して出荷し、問題は利用者から報告された後に対応する。
イ．欠陥情報をテスト記録から削除し、リリース判定に影響させない。
ウ．認証回避が再現しても、他のテストが合格していれば自動的に合格扱いとする。
エ．事前に定義したリリース基準に照らして出荷を止め、修正・再テストまたは承認された例外処理を経てから判断する。

正答・4肢解説・総合解説

正答：エ．事前に定義したリリース基準に照らして出荷を止め、修正・再テストまたは承認された例外処理を経てから判断する。
ア：既知の高影響欠陥を放置した出荷は顧客リスクを不当に高める。
イ：証跡の隠蔽となり、適切なリスク判断を妨げる。
ウ：重大欠陥の性質を考慮しない単純な総数評価は不適切である。
エ：重大なセキュリティ欠陥を、納期だけを理由に基準外で出荷しない。例外が必要なら権限者によるリスク判断を記録する。
総合解説：Secure by Designでは品質ゲートと例外管理を事前定義し、重大な既知欠陥を経営・事業上の都合だけで黙認しない仕組みが重要である。

Q013 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

プライバシーバイデザインの考え方として最も適切なものはどれか。
ア．個人に関するデータの利用目的やリスクを企画・設計段階から検討し、必要な保護をシステムへ組み込む。
イ．個人データの利用開始後に苦情が出た場合だけ保護策を追加する。
ウ．法令で明示的に禁止されていない個人データは、目的を決めず全て収集する。
エ．プライバシーは利用規約だけの問題なので、システム要件には含めない。

正答・4肢解説・総合解説

正答：ア．個人に関するデータの利用目的やリスクを企画・設計段階から検討し、必要な保護をシステムへ組み込む。
ア：事後対応ではなく、事業・システムの設計段階からプライバシー保護を組み込む考え方である。
イ：事後対応に限定しており、設計段階からの組込みという考え方に合わない。
ウ：目的や必要性を検討せず収集範囲を広げることはプライバシーリスクを高める。
エ：データ処理、アクセス、保存、削除など技術要件にも反映する必要がある。
総合解説：IPAはプライバシーバイデザインを要件定義で扱う知識として挙げる。個人情報保護委員会も事業の設計段階で個人の権利利益保護を組み込む考え方を示している。

Q014 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

新サービスで位置情報と購買履歴を新たに組み合わせて利用する予定である。PIAを実施する時期として最も適切なものはどれか。
ア．サービス終了後にのみ実施し、過去の判断を記録する。
イ．本格実装・運用開始前の企画や変更設計の段階で実施し、結果を要件や設計へ反映する。
ウ．個人情報漏えいが発生した場合だけ実施する。
エ．実装完了後、リリース当日に形式的な承認のためだけ実施する。

正答・4肢解説・総合解説

正答：イ．本格実装・運用開始前の企画や変更設計の段階で実施し、結果を要件や設計へ反映する。
ア：終了後では設計変更によるリスク低減へつなげられない。
イ：PIAはリスクを事前に特定・評価し、回避・低減策を設計へ反映するため早期実施が有効である。
ウ：PIAは事故後の原因分析だけを目的とする手法ではない。
エ：設計へ反映する余地が乏しく、事前評価としての効果が弱い。
総合解説：個人情報保護委員会は、個人情報等の収集を伴う事業の開始や変更に際し、事前に影響を評価するPIAを説明している。

Q015 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

配送状況通知アプリで、通知機能の提供に氏名と配送先だけで足りることが確認できた。データ最小化の観点で最も適切な要件はどれか。
ア．将来使う可能性があるため、取得可能な属性は全て必須入力にする。
イ．収集項目は増やすが、画面上では利用目的を表示しない。
ウ．通知機能に不要な生年月日や勤務先は収集せず、必要な項目だけを取得する。
エ．不要なデータも永久保存すれば再収集が不要なので安全である。

正答・4肢解説・総合解説

正答：ウ．通知機能に不要な生年月日や勤務先は収集せず、必要な項目だけを取得する。
ア：具体的な必要性がないデータまで収集するとプライバシーリスクが増える。
イ：透明性も最小化も満たさない。
ウ：目的達成に不要な個人データを収集しないことで、漏えいや不適切利用時の影響を抑えられる。
エ：不要な長期保存は侵害時の影響や管理負担を増やす。
総合解説：プライバシー要件では、収集項目、利用目的、保存期間、アクセス主体などをデータライフサイクルに沿って具体化する。

Q016 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

キャンペーン応募者の連絡先は当選通知と問い合わせ対応のためにだけ利用する。要件定義として最も適切なものはどれか。
ア．将来の分析に使える可能性があるため、明確な目的なく無期限保存する。
イ．保存期間は決めず、ストレージ容量が不足したときだけ古いデータを削除する。
ウ．削除要件は運用部門に任せ、システム側では削除機能を設けない。
エ．利用目的と業務上必要な期間を踏まえて保存期間を定め、期間満了後の削除または適切な匿名化を要件化する。

正答・4肢解説・総合解説

正答：エ．利用目的と業務上必要な期間を踏まえて保存期間を定め、期間満了後の削除または適切な匿名化を要件化する。
ア：目的と必要性が不明確な無期限保存はリスクを増やす。
イ：技術的都合だけでは適切な保持・削除基準にならない。
ウ：要件として定義しなければ適切な削除を継続的に実施しにくい。
エ：保存期間と廃棄まで含めたライフサイクル管理により、不要な保有を避ける。
総合解説：個人データは取得から利用、共有、保存、削除までを通じて管理する。必要以上の保持を避け、削除の実現方法と確認方法も設計する。

Q017 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

新サービスのプライバシー要件を定義する際、最初に整備する情報として特に有効なものはどれか。
ア．どの個人データを、どこから取得し、どの処理・保存先・第三者提供先へ流すかを示したデータフロー。
イ．画面の配色一覧だけを作り、データ処理の流れは確認しない。
ウ．サーバのCPU型番だけを一覧化し、個人データの所在は確認しない。
エ．開発者の勤続年数だけを記録し、外部委託先へのデータ移転は対象外にする。

正答・4肢解説・総合解説

正答：ア．どの個人データを、どこから取得し、どの処理・保存先・第三者提供先へ流すかを示したデータフロー。
ア：データの流れを把握すると、収集・利用・保存・共有の各段階でリスクと必要な管理策を検討しやすい。
イ：配色はデータ処理リスクの把握に直接役立たない。
ウ：ハードウェア情報だけでは個人データの処理経路を把握できない。
エ：第三者や委託先を含むデータの流れを把握する必要がある。
総合解説：データマッピングは、個人データがどこで収集・処理・保存・共有されるかを可視化し、PIAや要件定義の基礎になる。

Q018 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

人事システムで従業員の健康関連情報を扱う。プライバシー保護の観点から適切な要件はどれか。
ア．社内利用なので全従業員が閲覧できるようにする。
イ．業務上必要な担当者だけにアクセスを限定し、閲覧・変更の記録を残して不適切な利用を追跡できるようにする。
ウ．利便性を優先し、共有アカウントで全担当者が同じ資格情報を使用する。
エ．情報を暗号化すればアクセス権限は不要とする。

正答・4肢解説・総合解説

正答：イ．業務上必要な担当者だけにアクセスを限定し、閲覧・変更の記録を残して不適切な利用を追跡できるようにする。
ア：社内であっても目的と職務に応じたアクセス制限が必要である。
イ：アクセスを必要最小限に限定し、利用の説明責任を支える監査証跡を確保する要件である。
ウ：主体を識別できず、最小権限や追跡性を損なう。
エ：暗号化は重要だが、正規利用者間の不適切アクセスを防ぐ認可の代替にはならない。
総合解説：プライバシー要件は法務文書だけでなく、アクセス制御、監査ログ、保存期間、データ移転など具体的なシステム要件へ変換する。

Q019 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

個人を直接識別する氏名を別の識別子へ置き換え、対応表を厳格に分離保管する設計について、最も適切な説明はどれか。
ア．氏名を削除した時点で、どのような状況でも完全に匿名になる。
イ．識別子へ置き換えるとアクセス制御や漏えい対策は不要になる。
ウ．識別性を低減する有効な措置になり得るが、対応表などにより再び個人へ結び付けられる可能性があるため、単純に「完全匿名」とは扱えない。
エ．置換後のデータは元データより必ず高い精度になる。

正答・4肢解説・総合解説

正答：ウ．識別性を低減する有効な措置になり得るが、対応表などにより再び個人へ結び付けられる可能性があるため、単純に「完全匿名」とは扱えない。
ア：他の属性や対応情報から再識別できる場合があり、一律にはいえない。
イ：再識別や対応表の漏えいなどのリスクが残るため保護は必要である。
ウ：識別子置換はリスク低減策だが、再識別可能性や対応情報の管理を考慮する必要がある。
エ：精度向上は識別子置換の目的ではない。
総合解説：プライバシー保護技術は、再識別可能性や利用目的を踏まえて評価する。ラベルだけで安全性を決めず、データと対応情報の管理を設計する。

Q020 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

PIAで「退会後も個人データが不要に残り続ける」リスクが指摘された。最も適切な後続対応はどれか。
ア．PIA報告書へ記載した時点で対応完了とし、システム要件は変更しない。
イ．利用者が削除を希望しない限り、目的に関係なく永久保存する。
ウ．削除対象を開発者が都度判断し、共通ルールは作らない。
エ．退会処理に保存期間・削除対象・例外保持条件を定義し、実装とテスト項目へ結び付けて追跡する。

正答・4肢解説・総合解説

正答：エ．退会処理に保存期間・削除対象・例外保持条件を定義し、実装とテスト項目へ結び付けて追跡する。
ア：評価結果を設計へ反映しなければリスクは残る。
イ：必要性を超えた保持を正当化できない。
ウ：属人的な判断では一貫性や検証可能性が低い。
エ：PIAの発見事項を検証可能な要件へ変換し、実装・テストまで追跡できる。
総合解説：PIAの価値は、発見したプライバシーリスクを具体的な要件・管理策・テストへつなげる点にある。

Q021 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

既存サービスで取得していた利用履歴を、新たに信用スコアリングへ利用したいという企画が出た。要件定義前の対応として最も適切なものはどれか。
ア．新しい処理目的・対象者への影響・必要データ・共有先などを再評価し、必要に応じてPIAや既存の説明・同意・管理策を見直す。
イ．同じデータを使うので、目的が変わっても既存の評価を無条件に流用する。
ウ．技術的に実装できることだけ確認し、個人への影響は運用開始後に検討する。
エ．スコアリング結果を秘密にすれば、入力データの利用目的は検討不要である。

正答・4肢解説・総合解説

正答：ア．新しい処理目的・対象者への影響・必要データ・共有先などを再評価し、必要に応じてPIAや既存の説明・同意・管理策を見直す。
ア：利用目的や処理方法の重要な変更はプライバシーリスクを変えるため、既存評価をそのまま流用せず再評価する。
イ：データが同じでも利用目的や影響が変わればリスクは変化する。
ウ：プライバシー影響を設計前に検討できない。
エ：出力の秘匿だけでは目的変更に伴うプライバシーリスクを解消できない。
総合解説：プライバシーリスクはデータ種類だけでなく、目的、処理、共有、個人への影響で変わる。重要な変更では再評価して要件を更新する。

Q022 4-1 セキュリティ要件・設計 / プライバシーバイデザイン・要件定義

混雑傾向の統計だけを提供する機能で、個々の利用者を長期間追跡する必要はない。プライバシーリスクを抑える設計として最も適切なものはどれか。
ア．将来の別用途に備え、全利用者の詳細な位置履歴を無期限に保存する。
イ．目的達成に必要な粒度へ集約し、個人単位の識別子や詳細履歴を可能な範囲で保持しない。
ウ．統計表示に不要でも、端末識別子を外部公開データへ含める。
エ．個人単位データを全従業員へ配布し、分析の自由度を高める。

正答・4肢解説・総合解説

正答：イ．目的達成に必要な粒度へ集約し、個人単位の識別子や詳細履歴を可能な範囲で保持しない。
ア：現在の目的に不要な詳細データの長期保有はリスクを増やす。
イ：機能目的に不要な個人単位の追跡を減らすことで、データ侵害や二次利用による影響を低減できる。
ウ：不要な識別子の公開は再識別や追跡リスクを高める。
エ：利用目的とアクセス範囲を必要以上に広げている。
総合解説：プライバシーバイデザインでは、機能目的を満たしつつ収集・保持・共有する個人データを最小化する設計が重要である。

Q023 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

セキュリティ観点のアーキテクチャレビューで「信頼境界（trust boundary）」を確認する主な目的はどれか。
ア．システムの画面色を領域ごとに統一するため。
イ．全コンポーネントを同じ権限で動作させるため。
ウ．異なる信頼レベルの領域をまたぐデータや処理を特定し、境界で必要な認証・認可・検証などを確認する。
エ．ネットワーク機器の購入価格を比較するため。

正答・4肢解説・総合解説

正答：ウ．異なる信頼レベルの領域をまたぐデータや処理を特定し、境界で必要な認証・認可・検証などを確認する。
ア：表示デザインの統一は信頼境界確認の目的ではない。
イ：信頼差を無視した権限統一は侵害時の影響を拡大し得る。
ウ：信頼境界は脅威が顕在化しやすい箇所であり、境界通過時の制御を設計レビューするために重要である。
エ：コスト比較だけでは境界上のセキュリティ制御を評価できない。
総合解説：アーキテクチャレビューではデータフロー、信頼境界、外部インタフェース、権限境界を把握し、境界ごとの制御が脅威に対応しているか確認する。

Q024 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

外部システムと連携するAPI仕様のセキュリティレビューで優先して確認すべき事項はどれか。
ア．API名が短く覚えやすいかだけを確認する。
イ．開発者のPC性能が十分かだけを確認する。
ウ．レスポンスの文字色が統一されているかだけを確認する。
エ．通信相手の認証、操作ごとの認可、入力検証、通信保護、エラー時の振る舞いを仕様として確認する。

正答・4肢解説・総合解説

正答：エ．通信相手の認証、操作ごとの認可、入力検証、通信保護、エラー時の振る舞いを仕様として確認する。
ア：名称の使いやすさだけではセキュリティ要件を評価できない。
イ：開発端末性能はAPI境界のセキュリティ仕様とは別論点である。
ウ：表示上の統一だけでは認証や認可の欠陥を検出できない。
エ：外部境界では不正主体や不正入力を前提に、認証・認可・入力・通信・失敗時制御を確認する必要がある。
総合解説：仕様レビューでは、境界を越える主体・データ・プロトコル・例外経路を明確にし、セキュリティ要件が具体的に記述されているかを確認する。

Q025 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

全ての認証要求が1台の認証サーバに集中し、その障害時は全サービスへログインできない設計である。レビュー上の指摘として最も適切なものはどれか。
ア．認証サーバが可用性上の単一障害点になっているため、要件に応じて冗長化や障害時動作を設計する必要がある。
イ．認証サーバはセキュリティ機能なので、可用性を考慮する必要はない。
ウ．障害時は認証を無条件で迂回して全利用者を許可すればよい。
エ．サーバ名を非公開にすれば単一障害点の問題は解消する。

正答・4肢解説・総合解説

正答：ア．認証サーバが可用性上の単一障害点になっているため、要件に応じて冗長化や障害時動作を設計する必要がある。
ア：認証基盤の単一障害はサービス全体の可用性に波及するため、信頼性設計とセキュリティを合わせて評価する。
イ：セキュリティ機能自体の障害も可用性リスクになり得る。
ウ：可用性確保のために認証を外すと重大な機密性・完全性リスクを生む。
エ：名称秘匿は構成上の単一障害点を解消しない。
総合解説：セキュリティアーキテクチャはCIAを総合的に扱う。冗長化だけでなく、障害時にfail-open/fail-closedのどちらが適切かも業務リスクに基づき決める。

Q026 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

インターネット公開Web層と重要データベースを同一セグメントに置く構成と比べ、両者を適切に分離する主な利点はどれか。
ア．分離すると全ての脆弱性が自動的に消滅する。
イ．Web層が侵害された場合でも、DBへの到達経路と許可通信を限定し、横展開や被害拡大を抑えやすい。
ウ．分離すれば認証や認可は不要になる。
エ．分離すると監視ログを取得する必要がなくなる。

正答・4肢解説・総合解説

正答：イ．Web層が侵害された場合でも、DBへの到達経路と許可通信を限定し、横展開や被害拡大を抑えやすい。
ア：分離は被害限定策であり、アプリやDB自身の脆弱性を消すものではない。
イ：セグメンテーションは侵害後の移動や不要通信を制約し、信頼境界を明確にする。
ウ：ネットワーク制御と主体・操作レベルの認証認可は別の防御層である。
エ：境界通信の監視はむしろ重要になる。
総合解説：アーキテクチャレビューでは、公開面から重要資産までの経路を確認し、必要最小限の通信だけが許可されているか評価する。

Q027 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

設計書に「外部IDプロバイダから返される属性値は信頼できるので、アプリ側では検証しない」とある。レビューで最も適切な指摘はどれか。
ア．外部サービスは常に安全なので、検証処理は削除した方がよい。
イ．属性値は画面に表示しないので、認可に使う場合も検証不要である。
ウ．発行元・署名・対象者・有効期限などを検証し、受け取った属性が認可判断に使える条件を明確にすべきである。
エ．通信を暗号化すれば、受信した属性の発行元や対象者確認は不要である。

正答・4肢解説・総合解説

正答：ウ．発行元・署名・対象者・有効期限などを検証し、受け取った属性が認可判断に使える条件を明確にすべきである。
ア：外部依存にも誤設定・侵害・不正トークンなどのリスクがある。
イ：表示有無と認可判断の信頼性は別問題である。
ウ：外部サービスを利用しても信頼条件は暗黙にせず、どの証拠をどこで検証するかを仕様化する必要がある。
エ：TLSは通信路を保護するが、アプリケーションレベルのトークン検証を代替しない。
総合解説：外部依存との境界では、何を信頼し、どの条件を検証し、失敗時にどう振る舞うかを明示する。暗黙の信頼は設計上の弱点になる。

Q028 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

入退室管理システムの設計レビューで、通信障害時の振る舞いを決める。最も適切な考え方はどれか。
ア．セキュリティでは常に全扉を施錠するのが正解で、避難要件は考えなくてよい。
イ．可用性を優先し、障害時は全ての扉を無条件に開放する。
ウ．障害時動作は運用時に現場判断すればよく、設計書には記載しない。
エ．守る対象と人命・業務継続への影響を評価し、扉ごとにfail-safe/fail-secureの要件を明示する。

正答・4肢解説・総合解説

正答：エ．守る対象と人命・業務継続への影響を評価し、扉ごとにfail-safe/fail-secureの要件を明示する。
ア：人命安全や法令上の避難要件を無視した設計は不適切である。
イ：重要区画まで一律開放すると不正侵入リスクが高まる。
ウ：事前に要件を決めないと一貫した安全な動作を保証できない。
エ：単純に全箇所を閉鎖または開放するのではなく、安全・防災・セキュリティ要件の優先度を場所ごとに決める。
総合解説：フェールセーフ/フェールセキュアは文脈依存であり、守るべき安全性・機密性・可用性の優先順位を明確にして設計する。

Q029 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

決済APIの仕様書には認証方式と暗号化方式があるが、「同一注文への二重決済防止」や「再送時の扱い」が記載されていない。最も適切なレビュー指摘はどれか。
ア．通信・認証だけでなく、リプレイや重複実行を含む業務ロジック上の安全性を要件化し、冪等性や一意性確認などを検討すべきである。
イ．TLSを使っていれば二重決済は発生しないため、仕様追加は不要である。
ウ．二重決済は利用者の操作ミスなので、システム設計では扱わない。
エ．API名を変更すれば再送攻撃を防止できる。

正答・4肢解説・総合解説

正答：ア．通信・認証だけでなく、リプレイや重複実行を含む業務ロジック上の安全性を要件化し、冪等性や一意性確認などを検討すべきである。
ア：セキュリティは暗号・認証だけではなく、業務処理の状態遷移や再送による不正・誤処理も対象となる。
イ：TLSは通信路を保護するが、重複要求や業務ロジックの誤処理を防ぐものではない。
ウ：再送や攻撃を含めシステム側で防止すべき重要な完全性要件である。
エ：名称変更では同一要求の再実行を制御できない。
総合解説：仕様レビューでは技術要素だけでなく、資産・状態遷移・例外・再送・競合などの業務ロジック上の脅威も確認する。

Q030 4-1 セキュリティ要件・設計 / アーキテクチャ・仕様レビュー

オンプレミスの単一アプリを、API Gateway・複数マイクロサービス・外部SaaSを使う構成へ変更する。既存のセキュリティレビュー結果の扱いとして最も適切なものはどれか。
ア．機能要件が同じならセキュリティ構造も同じなので、再レビューは不要である。
イ．新しい信頼境界、サービス間認証、外部依存、秘密情報、データフローを再整理し、脅威分析と要件を更新する。
ウ．API Gatewayがあるため、各サービスの認証・認可は不要とする。
エ．外部SaaSは契約済みなので、データ移転や権限設定はレビュー対象外とする。

正答・4肢解説・総合解説

正答：イ．新しい信頼境界、サービス間認証、外部依存、秘密情報、データフローを再整理し、脅威分析と要件を更新する。
ア：機能が同じでも構成・境界・依存先が変われば脅威は変化する。
イ：アーキテクチャ変更により攻撃面と信頼関係が変わるため、過去のレビューをそのまま適用せず再評価が必要である。
ウ：ゲートウェイだけでは内部サービス間の全ての信頼問題を解消できない。
エ：外部依存もシステム全体のリスクと要件に含める必要がある。
総合解説：大きな構成変更では、データフロー図や信頼境界を更新し、設計前提と脅威モデルを再検証する。

Q031 4-2 セキュア実装 / セキュアコーディング

利用者が指定した顧客IDで検索する処理を実装する。SQLインジェクション対策として最も適切な実装はどれか。
ア．入力値をSQL文字列へ直接連結し、問題が起きたらログで確認する。
イ．SQL文を難読化し、利用者に見えないようにする。
ウ．SQL文と入力値を分離し、プレースホルダへ値をバインドするパラメータ化クエリを用いる。
エ．DBアカウントを管理者権限にしてSQLエラーを減らす。

正答・4肢解説・総合解説

正答：ウ．SQL文と入力値を分離し、プレースホルダへ値をバインドするパラメータ化クエリを用いる。
ア：文字列連結はSQLインジェクションの原因になり得る。
イ：SQLの秘匿は入力値の構文解釈を防がない。
ウ：入力値をSQL構文として解釈させにくくし、コードとデータの境界を保てる。
エ：過剰権限は侵害時の被害を拡大させる。
総合解説：セキュアコーディングでは、入力をコードとして解釈させないAPIを優先する。パラメータ化できない識別子などは別途allowlist等で制御する。

Q032 4-2 セキュア実装 / セキュアコーディング

HTML本文へ利用者入力を表示する実装で、XSS対策として基本となる考え方はどれか。
ア．全入力から半角英数字を削除する。
イ．危険そうな文字列を数個だけ置換すれば全ての文脈で安全になる。
ウ．TLSを使用すればブラウザ内でのスクリプト実行を防げる。
エ．出力先の文脈に応じたエンコーディングを行い、入力をコードではなくデータとして扱わせる。

正答・4肢解説・総合解説

正答：エ．出力先の文脈に応じたエンコーディングを行い、入力をコードではなくデータとして扱わせる。
ア：正規データまで壊し、XSSの全ての文脈を安全にできない。
イ：文脈依存の解釈があるため、単純なブラックリストだけでは不十分である。
ウ：TLSは通信路を保護するが、レスポンス内のXSSを防止しない。
エ：HTML、属性、JavaScript、URLなど文脈ごとに適切な出力処理を行う必要がある。
総合解説：入力検証と出力エンコーディングは役割が異なる。XSS対策では出力文脈に適したエンコーディングや安全なAPIを用いる。

Q033 4-2 セキュア実装 / セキュアコーディング

本番Web APIで予期しない例外が発生した場合の実装として最も適切なものはどれか。
ア．利用者には一般化したエラー応答を返し、詳細なスタックトレースや内部情報は保護されたサーバ側ログへ記録する。
イ．例外オブジェクトの全内容、SQL文、内部パスをそのまま利用者へ返す。
ウ．エラー情報を一切記録せず、HTTP 200だけを返す。
エ．本番では全例外を握りつぶし、処理成功とみなす。

正答・4肢解説・総合解説

正答：ア．利用者には一般化したエラー応答を返し、詳細なスタックトレースや内部情報は保護されたサーバ側ログへ記録する。
ア：利用者への情報露出を抑えつつ、運用者が原因調査できる証跡を残す。
イ：内部構造や技術情報の漏えいにつながり、攻撃者の偵察を助ける。
ウ：障害や攻撃兆候の調査が困難になり、応答コードも実態と一致しない。
エ：データ不整合や不正処理を見逃す危険がある。
総合解説：安全なエラー処理は、外部への詳細情報開示を抑え、内部では調査に必要な情報を適切に保護して記録する。

Q034 4-2 セキュア実装 / セキュアコーディング

整数で受け取る件数パラメータを配列サイズ計算へ利用する。安全な実装として最も適切なものはどれか。
ア．数値として変換できれば上限なく受け入れる。
イ．型の範囲、最小値・最大値、演算時のオーバーフローを確認してからサイズ計算へ使う。
ウ．負数でも内部で絶対値に変換するため無条件に受け入れる。
エ．クライアント側JavaScriptで検査するのでサーバ側検査は省略する。

正答・4肢解説・総合解説

正答：イ．型の範囲、最小値・最大値、演算時のオーバーフローを確認してからサイズ計算へ使う。
ア：極端な値や演算オーバーフローによる異常動作を防げない。
イ：入力値単体だけでなく、後続演算でのオーバーフローや異常な資源確保も考慮する。
ウ：仕様外値の暗黙変換は予期しない挙動を招く。
エ：クライアント側処理は改変可能であり、サーバ側でも検証が必要である。
総合解説：セキュア実装では、長さ・範囲・型・符号・演算結果などの境界条件を明示して検証する。

Q035 4-2 セキュア実装 / セキュアコーディング

ファイル変換機能で外部プログラムを呼び出す必要がある。OSコマンドインジェクションのリスクを下げる実装として最も適切なものはどれか。
ア．利用者入力をそのままコマンド文字列へ連結する。
イ．危険文字を一つだけ削除すれば全OSで安全とみなす。
ウ．可能ならシェルを介さないAPIを使い、引数を構造化して渡し、許可された値だけを受け入れる。
エ．コマンド実行ユーザをrootにして権限不足エラーを避ける。

正答・4肢解説・総合解説

正答：ウ．可能ならシェルを介さないAPIを使い、引数を構造化して渡し、許可された値だけを受け入れる。
ア：入力がシェル構文として解釈される可能性がある。
イ：構文やエンコーディングは多様で、単純な単一文字除去では不十分である。
ウ：シェルのメタ文字解釈を避け、引数とコマンドの境界を保つことで注入リスクを下げる。
エ：侵害時の影響を最大化するため逆効果である。
総合解説：外部コマンド実行は必要性自体を見直し、どうしても必要ならシェル回避、引数分離、allowlist、最小権限を組み合わせる。

Q036 4-2 セキュア実装 / セキュアコーディング

利用者が指定した文書IDに対応するファイルをダウンロードさせる機能を実装する。最も安全な設計はどれか。
ア．利用者が送った相対パスをそのままopen関数へ渡す。
イ．パス中の文字列「../」を一度だけ削除すれば全て安全である。
ウ．OSの全ファイルへ読取権限を付与し、アクセス失敗をなくす。
エ．外部入力を直接ファイルパスにせず、許可済みIDをサーバ側で管理するファイルへ対応付け、基準ディレクトリ外へ出ないことを保証する。

正答・4肢解説・総合解説

正答：エ．外部入力を直接ファイルパスにせず、許可済みIDをサーバ側で管理するファイルへ対応付け、基準ディレクトリ外へ出ないことを保証する。
ア：ディレクトリトラバーサルにより任意ファイルへ到達され得る。
イ：エンコーディングや正規化、入れ子表現などで回避される可能性がある。
ウ：侵害時に読み取れる範囲を拡大する。
エ：利用者入力から任意パスを構成しないことで、../などを使った意図しないファイル参照を防ぎやすい。
総合解説：ファイルアクセスでは識別子と実パスを分離し、許可範囲を固定する設計が有効である。最小権限も併用する。

Q037 4-2 セキュア実装 / セキュアコーディング

画像アップロード機能の実装として、セキュリティ上最も適切なものはどれか。
ア．拡張子だけでなく許可形式を検証し、サーバ側でファイル名を再生成し、実行領域から分離して保存する。
イ．利用者が指定したファイル名と保存先をそのまま使用する。
ウ．Content-Typeヘッダがimageなら内容検証なしで受け入れる。
エ．アップロード先をWeb実行ディレクトリに固定し、実行権限も付与する。

正答・4肢解説・総合解説

正答：ア．拡張子だけでなく許可形式を検証し、サーバ側でファイル名を再生成し、実行領域から分離して保存する。
ア：ファイル種別・名称・保存場所を制御し、アップロードファイルがコードとして実行される可能性を抑える。
イ：パス操作や危険な拡張子、上書きなどのリスクがある。
ウ：クライアントが送るContent-Typeは偽装できる。
エ：悪意あるファイルが実行されるリスクを高める。
総合解説：アップロードはサイズ、形式、内容、ファイル名、保存場所、アクセス権を複数層で制御する必要がある。

Q038 4-2 セキュア実装 / セキュアコーディング

外部から受信したデータをアプリケーションオブジェクトへ復元する処理で最も適切な方針はどれか。
ア．受信データが署名されていなくても、任意オブジェクトを自動生成する。
イ．信頼できないデータから任意クラスを生成する仕組みを避け、必要なデータ構造だけを明示的に解析・検証する。
ウ．復元エラーが出ないよう、全ての型を許可リストへ自動追加する。
エ．入力サイズだけ確認すれば、オブジェクト生成の安全性は保証できる。

正答・4肢解説・総合解説

正答：イ．信頼できないデータから任意クラスを生成する仕組みを避け、必要なデータ構造だけを明示的に解析・検証する。
ア：悪意ある型や処理が実行される危険がある。
イ：危険なオブジェクト生成や副作用を避け、受入れ可能な構造を限定する。
ウ：許可範囲が無制限に広がり、制御にならない。
エ：サイズ検査だけでは危険な型や処理の実行を防げない。
総合解説：デシリアライズでは信頼境界を意識し、不要な汎用オブジェクト復元を避ける。データ形式を限定し、型・値・構造を検証する。

Q039 4-2 セキュア実装 / セキュアコーディング

認証APIのデバッグログへ記録する情報として最も不適切なものを避ける実装はどれか。
ア．障害解析のため、平文パスワードを毎回ログへ保存する。
イ．アクセストークン全文を通常ログへ出力し、全開発者が閲覧できるようにする。
ウ．認証結果や相関IDは記録するが、パスワード・秘密鍵・完全なアクセストークンは記録しない。
エ．秘密鍵をBase64化して記録すれば秘密ではなくなる。

正答・4肢解説・総合解説

正答：ウ．認証結果や相関IDは記録するが、パスワード・秘密鍵・完全なアクセストークンは記録しない。
ア：認証秘密の漏えいにつながる重大な実装である。
イ：トークンの不正利用につながり得る。
ウ：調査に必要な証跡と秘密情報保護を両立する。秘密そのものをログへ残すとログ侵害時の被害が大きい。
エ：Base64は符号化であり、機密性を提供しない。
総合解説：ログはセキュリティ上重要だが、秘密情報や不要な個人データを記録しない。必要ならマスキングや識別子化を行う。

Q040 4-2 セキュア実装 / セキュアコーディング

アプリケーションで暗号機能が必要な場合、一般に推奨される実装方針はどれか。
ア．アルゴリズムを秘密にすれば安全なので、独自暗号を自作する。
イ．暗号鍵をソースコードへ埋め込めば実装が単純なので最も安全である。
ウ．乱数は実行時刻をそのまま使えば暗号用途に十分である。
エ．検証された標準アルゴリズムと実績ある暗号ライブラリを使い、独自暗号方式の設計を避ける。

正答・4肢解説・総合解説

正答：エ．検証された標準アルゴリズムと実績ある暗号ライブラリを使い、独自暗号方式の設計を避ける。
ア：方式の秘匿に依存する設計は第三者検証が難しく、安全性を保証しにくい。
イ：ソース流出や閲覧権限から鍵が露出しやすい。
ウ：予測可能な値は暗号鍵やトークン生成に適さない。
エ：暗号は実装上の落とし穴が多く、独自方式は安全性評価が難しい。標準化・検証済みの方式を適切な設定で使う。
総合解説：暗号ではアルゴリズム選定だけでなく、鍵管理、乱数、モード、パラメータ、エラー処理を含めて安全なライブラリの推奨方法に従う。

Q041 4-2 セキュア実装 / セキュアコーディング

在庫1個の商品に対し、複数リクエストが同時に購入処理を行う可能性がある。完全性を守る実装として最も適切なものはどれか。
ア．在庫確認と減算を一貫性のあるトランザクションや原子的処理として実行し、競合時の再試行・失敗条件を定める。
イ．各リクエストが在庫を読み取った後、同期なしで個別に減算する。
ウ．画面上の購入ボタンを一度だけ押せるようにすればサーバ側同期は不要である。
エ．競合が起きたら在庫数を負数のまま保存する。

正答・4肢解説・総合解説

正答：ア．在庫確認と減算を一貫性のあるトランザクションや原子的処理として実行し、競合時の再試行・失敗条件を定める。
ア：確認と更新の間に他処理が割り込む競合を防ぎ、状態遷移の整合性を保つ。
イ：同じ在庫を複数処理が同時に購入可能と判断する競合が起こり得る。
ウ：複数クライアントや直接API呼出しは防げない。
エ：データ完全性を損なう。
総合解説：セキュアコーディングでは入力だけでなく、並行処理によるTOCTOUや競合状態も考慮し、重要な状態更新を原子的に扱う。

Q042 4-2 セキュア実装 / セキュアコーディング

アプリケーションが多数のOSSライブラリを利用している。セキュア開発として最も適切な方針はどれか。
ア．ビルドのたびに無条件で最新バージョンを取得し、内容確認を行わない。
イ．使用する依存関係とバージョンを把握・固定し、既知脆弱性や更新情報を継続監視して検証後に更新する。
ウ．一度動作した依存ライブラリは、脆弱性が公表されても永久に更新しない。
エ．直接利用するライブラリだけ確認し、推移的依存関係は管理対象外にする。

正答・4肢解説・総合解説

正答：イ．使用する依存関係とバージョンを把握・固定し、既知脆弱性や更新情報を継続監視して検証後に更新する。
ア：予期しない破壊的変更や供給網リスクを招く。
イ：依存関係を資産として管理し、再現可能なビルドと脆弱性対応を両立する。
ウ：既知脆弱性を放置することになる。
エ：推移的依存にも脆弱性や改ざんリスクが存在する。
総合解説：依存関係はバージョン、出所、脆弱性、更新可否を追跡する。固定だけでも自動最新化だけでも不十分で、検証された更新プロセスが必要である。

Q043 4-2 セキュア実装 / セキュアコーディング

外部入力を扱う低レベル言語の処理で、バッファ境界を越える書込みリスクを下げる方針として最も適切なものはどれか。
ア．入力が通常は短いので、長さ検査を削除して処理を高速化する。
イ．配列の終端を越えてもOSが必ず安全に補正すると仮定する。
ウ．長さを明示的に扱う安全なAPIや境界検査を用い、可能ならメモリ安全性を高める言語・ライブラリを選択する。
エ．例外が起きたら再実行すれば安全性は確保できる。

正答・4肢解説・総合解説

正答：ウ．長さを明示的に扱う安全なAPIや境界検査を用い、可能ならメモリ安全性を高める言語・ライブラリを選択する。
ア：攻撃者は想定外の長さを送れるため危険である。
イ：境界外アクセスはクラッシュやコード実行につながり得る。
ウ：入力長と格納先容量の不一致を防ぐ実装と、危険なAPIを避ける設計が重要である。
エ：脆弱性自体を解消していない。
総合解説：メモリ破壊系の欠陥は重大な影響を持つ。安全な抽象化、境界検査、コンパイラ保護、レビュー・テストを組み合わせる。

Q044 4-2 セキュア実装 / セキュアコーディング

重要な権限判定関数が予期しない例外を返した。アプリケーションの実装として最も適切なものはどれか。
ア．例外時は管理者権限を付与して処理を継続する。
イ．例外内容と設定ファイルのパスを全て利用者へ返す。
ウ．権限判定をスキップし、呼出し元が正しいと仮定する。
エ．権限を付与せず安全側に失敗させ、必要な監視情報を残し、利用者には内部詳細を露出しない。

正答・4肢解説・総合解説

正答：エ．権限を付与せず安全側に失敗させ、必要な監視情報を残し、利用者には内部詳細を露出しない。
ア：例外を権限昇格へ結び付ける重大な欠陥になる。
イ：内部情報の漏えいにつながる。
ウ：認可制御を迂回する。
エ：認可不能を許可へ変換せず、同時に調査可能性を確保するfail-closedな実装である。
総合解説：セキュア実装では、異常系・例外系でもセキュリティ不変条件が保たれることを確認する。正常系だけの実装では不十分である。

Q045 4-2 セキュア実装 / 入力検証・認可・セッション管理

Webアプリケーションの入力検証として最も適切な方針はどれか。
ア．外部から受け取る値はサーバ側で仕様に沿って検証し、可能ならデータフローの早い段階で不正値を拒否する。
イ．ブラウザのJavaScriptで検証しているため、サーバ側では検証しない。
ウ．社内システムからの入力は常に正しいので検証対象外とする。
エ．不正入力でも一旦DBへ保存し、月末にまとめて検査する。

正答・4肢解説・総合解説

正答：ア．外部から受け取る値はサーバ側で仕様に沿って検証し、可能ならデータフローの早い段階で不正値を拒否する。
ア：クライアント側検証はUX向上には有効だが改変可能なので、信頼境界を越えたサーバ側で検証する必要がある。
イ：攻撃者はクライアント側検証を回避できる。
ウ：内部・取引先システムも侵害や誤動作の可能性がある。
エ：不正データが後続処理へ流れ、影響が拡大し得る。
総合解説：OWASPは信頼できない全ての入力を検証し、できるだけ早い段階で不正な形式を拒否する考え方を示している。

Q046 4-2 セキュア実装 / 入力検証・認可・セッション管理

国コードとしてJP、US、DEの3値だけを受け付けるAPIの入力検証として最も適切なものはどれか。
ア．既知の危険文字列だけをblacklistで除外し、それ以外は全て許可する。
イ．許可される3値を明示したallowlistと照合し、それ以外を拒否する。
ウ．文字列長が2文字なら全て許可する。
エ．エラーになった値だけ後から個別に禁止リストへ追加する。

正答・4肢解説・総合解説

正答：イ．許可される3値を明示したallowlistと照合し、それ以外を拒否する。
ア：本来の仕様外値まで受け入れ、未知の回避表現にも弱い。
イ：仕様上許可される値が明確な場合、許可集合を定義する方が抜けの少ない検証を行いやすい。
ウ：ZZなど仕様外の値も通過する。
エ：事後的で網羅性に乏しい。
総合解説：入力仕様が限定できる場合は、型・長さ・範囲・列挙値など期待される形を肯定的に定義して検証する。

Q047 4-2 セキュア実装 / 入力検証・認可・セッション管理

認証済み利用者が他人の請求書IDをURLへ指定して閲覧できてしまう。主に不足している制御はどれか。
ア．パスワードの文字数を増やすことだけ。
イ．請求書IDを長い数字へ変更することだけ。
ウ．請求書ごとに、その利用者が当該資源を閲覧する権限を持つか確認する認可。
エ．画面上のリンクを非表示にすることだけ。

正答・4肢解説・総合解説

正答：ウ．請求書ごとに、その利用者が当該資源を閲覧する権限を持つか確認する認可。
ア：認証強化だけでは他人資源へのアクセス制御欠如を解消しない。
イ：識別子を推測しにくくしても認可の代替にはならない。
ウ：ログイン済みであることと、特定資源へアクセスできることは別であり、各要求で認可を確認する必要がある。
エ：直接URL/APIを呼ばれた場合のサーバ側認可が必要である。
総合解説：認証は主体確認、認可はその主体が操作を許されるかの判断である。資源単位・操作単位でサーバ側認可を行う。

Q048 4-2 セキュア実装 / 入力検証・認可・セッション管理

新しい管理APIの認可ルールを設計する。deny by defaultの方針として最も適切なものはどれか。
ア．明示的に禁止された操作だけ拒否し、未定義の操作は全て許可する。
イ．エラー時は利便性のため全権限を与える。
ウ．管理画面にリンクがない操作は認可確認を省略する。
エ．明示的に許可された主体・操作だけを通し、どのルールにも一致しない要求は拒否する。

正答・4肢解説・総合解説

正答：エ．明示的に許可された主体・操作だけを通し、どのルールにも一致しない要求は拒否する。
ア：ルール漏れがそのまま不正許可になる。
イ：異常系が権限昇格経路になる。
ウ：UI非表示はアクセス制御ではない。
エ：未定義・想定外のケースを暗黙に許可しないため、ルール漏れが権限付与につながりにくい。
総合解説：認可は最小権限、deny by default、毎要求の検証を基本とする。未定義状態を安全側に倒す。

Q049 4-2 セキュア実装 / 入力検証・認可・セッション管理

利用者がログイン時に一般ユーザ権限だったが、その後アカウントが停止された。重要操作APIの実装として最も適切なものはどれか。
ア．重要操作ごとに現在の権限・アカウント状態をサーバ側で確認し、停止後の要求を拒否する。
イ．ログイン時に認証済みなら、セッション終了まで権限変更を一切反映しない。
ウ．画面から操作ボタンを消せばAPI側の確認は不要である。
エ．停止情報はクライアント側Cookieだけで保持し、利用者が送った値を信頼する。

正答・4肢解説・総合解説

正答：ア．重要操作ごとに現在の権限・アカウント状態をサーバ側で確認し、停止後の要求を拒否する。
ア：ログイン時の一回の判定だけに依存せず、重要な各要求で最新の認可状態を確認する。
イ：停止や権限剥奪が即時に効かず、不要なアクセスが継続する。
ウ：APIを直接呼ばれる可能性がある。
エ：クライアント側値は改変可能である。
総合解説：認可判断は信頼できるサーバ側情報を使い、各要求またはリスクに応じた頻度で最新状態を評価する。

Q050 4-2 セキュア実装 / 入力検証・認可・セッション管理

ログイン前に発行したセッションIDを、ログイン成功後もそのまま使い続ける実装がある。適切な改善はどれか。
ア．ログイン後も同じIDを永久に使い続ける。
イ．認証成功や権限レベル変更時にセッションIDを再生成し、旧IDを無効化する。
ウ．セッションIDをURLへ付与して共有しやすくする。
エ．セッションIDを利用者名そのものにする。

正答・4肢解説・総合解説

正答：イ．認証成功や権限レベル変更時にセッションIDを再生成し、旧IDを無効化する。
ア：セッション固定化の危険が残る。
イ：攻撃者が事前に知るセッションIDを被害者へ固定しても、認証後のIDが変われば乗っ取りを防ぎやすい。
ウ：履歴・ログ・Referer等から漏えいしやすい。
エ：予測可能で機密情報も含み、不適切である。
総合解説：セッションIDは認証や権限変更の境界で更新し、推測困難で意味を持たない値として管理する。

Q051 4-2 セキュア実装 / 入力検証・認可・セッション管理

認証セッションCookieへHttpOnly属性を付与する主な目的はどれか。
ア．CookieをTLS通信だけで送信するため。
イ．クロスサイト要求でCookie送信を制御するため。
ウ．ブラウザ上のJavaScriptからCookieへアクセスされにくくし、XSS発生時のセッションID窃取リスクを低減する。
エ．Cookie内容を自動的に暗号化してサーバでも読めなくするため。

正答・4肢解説・総合解説

正答：ウ．ブラウザ上のJavaScriptからCookieへアクセスされにくくし、XSS発生時のセッションID窃取リスクを低減する。
ア：これは主にSecure属性の役割である。
イ：これは主にSameSite属性が関係する。
ウ：HttpOnlyはスクリプトからのCookie読取りを制限する防御層である。
エ：HttpOnlyは暗号化機能ではない。
総合解説：Secure、HttpOnly、SameSiteは目的が異なる。Cookie属性を組み合わせ、TLS、セッション更新、タイムアウト等と多層で保護する。

Q052 4-2 セキュア実装 / 入力検証・認可・セッション管理

アイドルタイムアウトの実装として最も適切なものはどれか。
ア．ブラウザのJavaScript表示だけでタイムアウトし、サーバは同じIDを無期限に受け入れる。
イ．タイムアウト後も旧IDを再送すれば自動的に復活させる。
ウ．管理者セッションだけは利便性のため永久に有効にする。
エ．一定時間操作がないセッションをサーバ側で失効させ、失効後の同じセッションIDを受け付けない。

正答・4肢解説・総合解説

正答：エ．一定時間操作がないセッションをサーバ側で失効させ、失効後の同じセッションIDを受け付けない。
ア：クライアント側処理を迂回すればセッションを継続できる。
イ：失効の意味がなくなる。
ウ：高権限ほど長期セッションのリスクは高い。
エ：タイムアウトは攻撃者がクライアント側時刻を改変して延長できないよう、サーバ側で強制する。
総合解説：アイドル・絶対・更新タイムアウトをリスクに応じて定め、サーバ側で失効を強制する。

Q053 4-2 セキュア実装 / 入力検証・認可・セッション管理

長時間ログイン状態を維持できるサービスで、登録済み振込先を変更する機能を追加する。最も適切なセッション設計はどれか。
ア．変更時に利用者のリスク状態を確認し、必要に応じて再認証や追加認証を要求してから実行する。
イ．ログイン済みなら何日前のセッションでも追加確認なしで変更できる。
ウ．変更APIはURLを長くすれば追加認証は不要である。
エ．確認画面を表示すればサーバ側の再認証は不要である。

正答・4肢解説・総合解説

正答：ア．変更時に利用者のリスク状態を確認し、必要に応じて再認証や追加認証を要求してから実行する。
ア：高リスク操作では、既存セッションが乗っ取られている可能性を考慮し、再認証で保証を高める。
イ：古い・盗まれたセッションから重要設定を変更されるリスクが高い。
ウ：URLの推測困難性は本人確認の代替にならない。
エ：画面表示だけでは攻撃者によるAPI実行を防げない。
総合解説：パスワード変更、支払先変更、アカウント回復など高リスク操作では再認証やステップアップ認証を検討する。

Q054 4-2 セキュア実装 / 入力検証・認可・セッション管理

SaaSで利用者は自社テナント内のデータだけ閲覧できる。APIが受け取るtenant_idをそのまま検索条件に使う設計の改善として最も適切なものはどれか。
ア．tenant_idが整数なら他テナント値でも受け入れる。
イ．認証済み主体から許可テナントをサーバ側で導出し、要求された資源がそのテナントに属するか毎回確認する。
ウ．画面上で他テナントIDを表示しなければAPI側確認は不要である。
エ．テナントIDを連番からUUIDへ変えるだけで認可確認を削除する。

正答・4肢解説・総合解説

正答：イ．認証済み主体から許可テナントをサーバ側で導出し、要求された資源がそのテナントに属するか毎回確認する。
ア：形式が正しくても認可されているとは限らない。
イ：クライアントが送るテナント識別子を権限根拠にせず、信頼できる主体情報と資源所有関係で認可する。
ウ：利用者はリクエストを直接変更できる。
エ：推測困難性はアクセス権の検証を代替しない。
総合解説：マルチテナントでは主体・テナント・資源の関係をサーバ側で強制する。識別子の難読化だけでは越境アクセスを防げない。

Q055 4-2 セキュア実装 / 秘密情報・鍵管理

APIキーやDBパスワードをソースコードへ直接埋め込むことを避ける主な理由はどれか。
ア．ソースコードへ埋め込むと暗号アルゴリズムが自動的に弱くなるため。
イ．ハードコードするとプログラムの実行速度が必ず大幅に低下するため。
ウ．リポジトリの閲覧・複製・履歴・ビルド成果物などを通じて秘密が広範囲へ露出し、失効や更新も難しくなるため。
エ．ソースコードは必ず公開される法律上の義務があるため。

正答・4肢解説・総合解説

正答：ウ．リポジトリの閲覧・複製・履歴・ビルド成果物などを通じて秘密が広範囲へ露出し、失効や更新も難しくなるため。
ア：問題の中心はアルゴリズムではなく秘密情報の露出とライフサイクル管理である。
イ：性能ではなく機密性と管理性が主な問題である。
ウ：コードと秘密情報を分離すると、アクセス制御、監査、ローテーション、失効を独立して行いやすい。
エ：そのような一般的義務はなく、技術的な秘密管理リスクが理由である。
総合解説：秘密情報はコードや一般設定ファイルから分離し、専用の秘密管理基盤や安全な注入方式を使う。漏えい時に速やかに失効・更新できる設計が重要である。

Q056 4-2 セキュア実装 / 秘密情報・鍵管理

専用のSecrets Managerを利用する利点として最も適切なものはどれか。
ア．全利用者が同じ秘密を自由に閲覧できるようにする。
イ．秘密を暗号化せず、チャットへ貼り付けて配布する。
ウ．一度登録した秘密を永久に変更できなくする。
エ．秘密の保管・アクセス制御・監査・ローテーションを集中管理し、アプリへ必要時に限定して提供しやすい。

正答・4肢解説・総合解説

正答：エ．秘密の保管・アクセス制御・監査・ローテーションを集中管理し、アプリへ必要時に限定して提供しやすい。
ア：集中管理は共有拡大ではなく、必要最小限のアクセス制御を実現するために使う。
イ：露出範囲が増え、監査・失効も困難になる。
ウ：漏えいや期限切れに対応できず、ライフサイクル管理に反する。
エ：秘密のライフサイクル管理をコードから分離し、一貫した制御を適用できる。
総合解説：秘密管理では保管だけでなく、誰がいつ取得したかの監査、短命化、ローテーション、失効、可用性も設計する。

Q057 4-2 セキュア実装 / 秘密情報・鍵管理

複数マイクロサービスが同じ秘密管理基盤を利用する。最小権限の設計として最も適切なものはどれか。
ア．各サービスの実行IDごとに必要な秘密だけを読み取れるポリシーを付与し、不要な一覧・更新権限は与えない。
イ．全サービスへ全秘密の読取・更新・削除権限を付与する。
ウ．アクセス制御をなくし、秘密の名前を推測困難にする。
エ．開発・本番の秘密を一つの共有アカウントで管理し、利用者識別を行わない。

正答・4肢解説・総合解説

正答：ア．各サービスの実行IDごとに必要な秘密だけを読み取れるポリシーを付与し、不要な一覧・更新権限は与えない。
ア：サービス単位で権限を分離すると、一つのサービスが侵害された際の秘密漏えい範囲を限定できる。
イ：侵害時の影響範囲が大きく、誤操作も起こりやすい。
ウ：名前の秘匿は認可の代替にならない。
エ：環境分離と追跡性を損なう。
総合解説：秘密管理でも主体ごとの最小権限、環境分離、監査が基本である。管理権限と利用権限を分けることも有効である。

Q058 4-2 セキュア実装 / 秘密情報・鍵管理

本番APIキーが誤って公開リポジトリへコミットされたことが判明した。最優先の対応として最も適切なものはどれか。
ア．最新コミットから文字列を削除すれば、同じキーを使い続けてよい。
イ．当該キーを失効・ローテーションし、利用履歴を調査した上で安全な秘密管理方法へ移行する。
ウ．公開先へ削除依頼だけを送り、キーは変更しない。
エ．キー名を変更し、値は同じまま利用する。

正答・4肢解説・総合解説

正答：イ．当該キーを失効・ローテーションし、利用履歴を調査した上で安全な秘密管理方法へ移行する。
ア：過去履歴や外部キャッシュから既に取得されている可能性がある。
イ：履歴から文字列を消すだけでは既に取得された秘密を無効化できないため、失効・更新が必要である。
ウ：削除完了を待つ間も不正利用され得る。
エ：秘密値が同じなら漏えい状態は解消しない。
総合解説：秘密漏えい時は「見えなくする」だけでは不十分である。失効・ローテーション、影響調査、根本原因修正まで行う。

Q059 4-2 セキュア実装 / 秘密情報・鍵管理

暗号鍵管理のライフサイクルに含めるべき事項として最も適切なものはどれか。
ア．鍵を一度生成したら永久に使い続け、失効手順は定めない。
イ．鍵の保管場所だけ決め、誰が利用できるかは管理しない。
ウ．鍵の生成、配布・保管、利用、更新、失効、必要な保管期間、最終的な破棄を管理する。
エ．鍵を削除したかどうかは記録せず、各担当者へ任せる。

正答・4肢解説・総合解説

正答：ウ．鍵の生成、配布・保管、利用、更新、失効、必要な保管期間、最終的な破棄を管理する。
ア：漏えい・アルゴリズム変更・利用期限などへ対応できない。
イ：アクセス制御がなければ鍵の機密性を維持できない。
ウ：鍵は生成時だけでなく、使用期間全体と利用終了後まで管理する必要がある。
エ：追跡性と一貫性が不足する。
総合解説：NIST SP 800-57は鍵素材の保護とライフサイクル管理を扱う。用途、期間、権限、バックアップ、失効・破棄を設計する。

Q060 4-2 セキュア実装 / 秘密情報・鍵管理

同じ秘密鍵を複数の異なる用途へ無制限に使い回すことを避ける主な理由はどれか。
ア．鍵を分けると暗号化されたデータが必ず読めなくなるため。
イ．暗号鍵は数が少ないほど常に安全だから。
ウ．同一鍵を使うとネットワーク帯域が必ず増加するため。
エ．用途ごとに必要な保護や有効期間が異なり、一つの鍵の漏えいが複数機能へ波及するため。

正答・4肢解説・総合解説

正答：エ．用途ごとに必要な保護や有効期間が異なり、一つの鍵の漏えいが複数機能へ波及するため。
ア：適切な鍵管理をすれば用途分離しても必要な復号は行える。
イ：数だけで安全性は決まらず、用途分離は重要な設計原則である。
ウ：主な問題はセキュリティ上の影響範囲とライフサイクル管理である。
エ：鍵用途を分離すると、侵害範囲を限定し、個別にローテーション・失効しやすい。
総合解説：暗号鍵は目的に応じて分離し、必要な権限と利用期間を限定する。鍵暗号化鍵とデータ暗号化鍵を分ける設計もその一例である。

Q061 4-2 セキュア実装 / 秘密情報・鍵管理

CI/CDで本番環境へデプロイするための資格情報が必要である。最も適切な設計はどれか。
ア．短命な資格情報やワークロードIDを利用し、パイプライン実行時に必要な権限だけを取得し、利用を監査する。
イ．本番管理者の長期パスワードをCI設定ファイルへ平文保存する。
ウ．全開発者へ本番の共通秘密鍵を配布し、個人識別を行わない。
エ．資格情報が漏えいしても、ビルドが成功していれば変更しない。

正答・4肢解説・総合解説

正答：ア．短命な資格情報やワークロードIDを利用し、パイプライン実行時に必要な権限だけを取得し、利用を監査する。
ア：長期固定秘密を配布するより、短命・最小権限・監査可能な資格情報の方が漏えい時の影響を抑えやすい。
イ：漏えい時の影響が大きく、ローテーションや追跡も難しい。
ウ：最小権限と説明責任を損なう。
エ：漏えいした秘密は不正利用される前提で失効・更新すべきである。
総合解説：CI/CDの秘密管理は、長期固定秘密を減らし、短命化、ワークロード認証、環境分離、監査、ローテーションを組み合わせる。

Q062 4-2 セキュア実装 / 秘密情報・鍵管理

重要データの復号鍵を1人の管理者PCだけに保存しており、そのPC故障で復旧不能になる懸念がある。最も適切な改善はどれか。
ア．鍵を社内共有フォルダへ平文コピーし、誰でも取得できるようにする。
イ．鍵を適切に保護した管理基盤で冗長化・バックアップし、復旧手順とアクセス統制を定めて定期的に検証する。
ウ．鍵を一切バックアップせず、障害時はデータを諦める。
エ．復旧鍵をチャットへ投稿し、検索できるようにする。

正答・4肢解説・総合解説

正答：イ．鍵を適切に保護した管理基盤で冗長化・バックアップし、復旧手順とアクセス統制を定めて定期的に検証する。
ア：可用性は上がっても機密性を大きく損なう。
イ：鍵の機密性だけでなく可用性も要件であり、安全なバックアップと復旧テストが必要である。
ウ：業務要件が復旧を必要とする場合、可用性設計として不十分である。
エ：秘密情報の露出範囲が広がり不適切である。
総合解説：鍵管理では機密性・完全性・可用性のバランスが必要である。バックアップ鍵も本番鍵と同等に保護し、復旧可能性を検証する。

Q063 4-3 テスト・脆弱性対応 / セキュリティテスト計画

セキュリティテスト計画を作成する際の基本として最も適切なものはどれか。
ア．テスト担当者が当日に思いついた項目だけを実施する。
イ．機能テストが合格すればセキュリティテストは不要とする。
ウ．セキュリティ要件や脅威分析結果を基に、何をどの方法で検証し、どの結果を合格とするかを定める。
エ．リリース後の事故件数だけをテスト結果として扱う。

正答・4肢解説・総合解説

正答：ウ．セキュリティ要件や脅威分析結果を基に、何をどの方法で検証し、どの結果を合格とするかを定める。
ア：再現性や網羅性がなく、重要な要件が未検証になり得る。
イ：正常系の機能成立だけでは攻撃・誤用・権限制御等を検証できない。
ウ：テストは要件を満たしているか検証する活動であり、脅威・要件・試験項目・判定基準を対応付ける必要がある。
エ：事前の検証計画になっていない。
総合解説：IPAはセキュリティ機能のテスト計画書をレビューする能力を求める。テスト計画は要件、脅威、対象、手法、環境、判定基準、証跡を明確にする。

Q064 4-3 テスト・脆弱性対応 / セキュリティテスト計画

セキュリティテストの実施時期として最も適切な方針はどれか。
ア．全てのセキュリティテストを本番公開後に初めて実施する。
イ．設計段階ではセキュリティを扱わず、脆弱性診断だけに任せる。
ウ．一度合格したら、その後の変更では再テストしない。
エ．設計レビュー、コード解析、結合・システムテストなど、開発ライフサイクルの複数段階へ組み込む。

正答・4肢解説・総合解説

正答：エ．設計レビュー、コード解析、結合・システムテストなど、開発ライフサイクルの複数段階へ組み込む。
ア：重大欠陥を利用者へ露出する前に検出できない。
イ：設計欠陥は後工程の診断だけで十分に検出・修正できない場合がある。
ウ：変更によって既存制御が壊れる可能性がある。
エ：早い段階で欠陥を発見し、後工程では実装済み制御を動的に検証するなど、段階ごとに適した手法を使う。
総合解説：OWASP WSTGやNIST SSDFは、セキュリティ検証を開発ライフサイクルへ統合する考え方を示す。単発の終盤診断だけでは不十分である。

Q065 4-3 テスト・脆弱性対応 / セキュリティテスト計画

セキュリティテストにおけるネガティブテストの説明として最も適切なものはどれか。
ア．不正形式、権限外操作、異常な順序など想定外の入力や操作でも、安全に拒否・処理できることを確認する。
イ．正常な入力だけを繰り返し、機能仕様どおり動くかだけ確認する。
ウ．テストを実施せず、設計書の存在だけ確認する。
エ．全ての入力を同じ値に固定し、境界条件を避ける。

正答・4肢解説・総合解説

正答：ア．不正形式、権限外操作、異常な順序など想定外の入力や操作でも、安全に拒否・処理できることを確認する。
ア：正常な利用だけでなく、誤用・悪用・境界値で制御が破れないかを確認する。
イ：これは主に正常系機能テストであり、ネガティブテストの趣旨ではない。
ウ：実装された制御の異常系挙動を確認できない。
エ：想定外条件の耐性を検証できない。
総合解説：セキュリティ制御は異常系で破綻しやすい。拒否時の状態、エラー情報、ログ、権限維持なども合わせて確認する。

Q066 4-3 テスト・脆弱性対応 / セキュリティテスト計画

開発・テスト環境で個人情報を扱う必要がある。最も適切な方針はどれか。
ア．テスト環境なので本番DBを全量コピーし、全開発者へ自由に配布する。
イ．可能な限り合成・匿名化されたテストデータを使い、実データが必要な場合は本番相当の保護と利用制限を適用する。
ウ．個人情報はテスト用途なら保護不要とみなす。
エ．テスト完了後もコピーした実データを無期限に各端末へ残す。

正答・4肢解説・総合解説

正答：イ．可能な限り合成・匿名化されたテストデータを使い、実データが必要な場合は本番相当の保護と利用制限を適用する。
ア：漏えい・目的外利用のリスクを大きくする。
イ：テスト環境は本番より管理が緩くなりやすいため、不要な実データ持込みを避け、必要時も保護要件を下げない。
ウ：環境名だけでデータの機微性は変わらない。
エ：不要な保持と管理外コピーが増える。
総合解説：テスト計画にはデータ準備、環境分離、アクセス権、ログ、廃棄まで含める。プライバシー要件とも整合させる。

Q067 4-3 テスト・脆弱性対応 / セキュリティテスト計画

SASTとDASTを組み合わせる理由として最も適切なものはどれか。
ア．両者は完全に同じ情報を解析するため、結果を二重化するためだけに使う。
イ．SASTを導入すれば実行環境の設定不備は必ず全て検出できる。
ウ．ソース等を解析するSASTと、実行中アプリを外部から評価するDASTでは検出しやすい欠陥が異なり、相互補完できるため。
エ．DASTを導入すればソース内の到達困難な欠陥も必ず全て特定できる。

正答・4肢解説・総合解説

正答：ウ．ソース等を解析するSASTと、実行中アプリを外部から評価するDASTでは検出しやすい欠陥が異なり、相互補完できるため。
ア：解析対象と検出特性は異なる。
イ：実行時・構成上の問題はSASTだけでは捉えにくい。
ウ：単一手法で全ての脆弱性を検出できないため、設計レビュー、SAST、DAST、手動テスト等を目的別に組み合わせる。
エ：動的テストは実行経路や入力到達性に依存し、網羅性に限界がある。
総合解説：ツールごとに誤検知・見逃し・対象範囲が異なる。目的と開発段階に応じた複数手法の組合せが現実的である。

Q068 4-3 テスト・脆弱性対応 / セキュリティテスト計画

一般利用者と管理者がいるAPIの認可テストとして最も適切なものはどれか。
ア．管理者で正常操作できることだけ確認し、一般利用者からの不正操作は試さない。
イ．管理者メニューが非表示なら認可テストを省略する。
ウ．レスポンス時間だけ測定し、権限判定結果は確認しない。
エ．一般利用者が管理者用操作を直接API呼出ししても拒否されることや、他利用者資源へIDを変えてもアクセスできないことを確認する。

正答・4肢解説・総合解説

正答：エ．一般利用者が管理者用操作を直接API呼出ししても拒否されることや、他利用者資源へIDを変えてもアクセスできないことを確認する。
ア：権限境界が破れていないか検証できない。
イ：UI制御はAPI認可の代替ではない。
ウ：認可制御の有効性を評価できない。
エ：画面表示ではなく、資源・操作・主体の組合せでサーバ側認可を検証する。
総合解説：認可テストでは水平・垂直権限逸脱、直接オブジェクト参照、未認証アクセス、失敗時挙動などを含める。

Q069 4-3 テスト・脆弱性対応 / セキュリティテスト計画

独自バイナリプロトコルを解析するサーバについて、想定外入力への耐性を効率よく確認したい。追加するテストとして最も適切なものはどれか。
ア．構造を考慮したファジング等で多数の異常・境界入力を自動生成し、クラッシュや異常状態を検出する。
イ．正常なサンプル1件だけを毎回送信する。
ウ．サーバの画面色だけを確認する。
エ．テストを行わず、クラッシュ報告が来るまで待つ。

正答・4肢解説・総合解説

正答：ア．構造を考慮したファジング等で多数の異常・境界入力を自動生成し、クラッシュや異常状態を検出する。
ア：パーサや境界処理は多様な入力組合せで欠陥が出るため、ファジングが有効な場合がある。
イ：異常入力や境界条件の探索範囲が狭い。
ウ：プロトコル処理の安全性を検証できない。
エ：本番利用者へリスクを転嫁する。
総合解説：ファジングは大量・多様な入力でパーサや境界処理の欠陥を発見する手法である。クラッシュの再現、原因特定、回帰テスト化まで行う。

Q070 4-3 テスト・脆弱性対応 / セキュリティテスト計画

過去に修正した認証回避バグについて、修正版リリース後の開発で最も適切な対応はどれか。
ア．一度直したバグは再発しない前提で、テスト項目から削除する。
イ．再発を検知できる自動または再現可能なテストを回帰テストへ追加し、関連変更のたびに実行する。
ウ．修正内容を口頭共有するだけで、再現手順は残さない。
エ．重大バグだけはテストせず、本番監視で発見する。

正答・4肢解説・総合解説

正答：イ．再発を検知できる自動または再現可能なテストを回帰テストへ追加し、関連変更のたびに実行する。
ア：リファクタリングや機能追加で再導入される可能性がある。
イ：修正だけで終えず、同じ欠陥が再導入された場合に早期検出できる仕組みを残す。
ウ：継続的な検証が難しくなる。
エ：利用者へ再発リスクを露出する。
総合解説：脆弱性対応では根本原因を分析し、類似箇所の確認と回帰テスト化によって再発防止へつなげる。

Q071 4-3 テスト・脆弱性対応 / セキュリティテスト計画

セキュリティテスト結果をリリース判定へ使う。判定基準として最も適切なものはどれか。
ア．脆弱性が1件でもあれば内容に関係なく永久にリリース禁止とする。
イ．重大度に関係なく100件未満なら自動的に合格とする。
ウ．重大度・悪用可能性・露出・代替策などに基づき、未解決欠陥を許容できる条件と例外承認手順を事前に定める。
エ．納期が近ければ未解決欠陥を全て合格扱いにする。

正答・4肢解説・総合解説

正答：ウ．重大度・悪用可能性・露出・代替策などに基づき、未解決欠陥を許容できる条件と例外承認手順を事前に定める。
ア：現実的なリスク判断や例外処理ができない。
イ：件数だけでは影響や悪用可能性を評価できない。
ウ：単なる件数ではなくリスクに基づく基準と例外管理を明確にすると、一貫した判断を行いやすい。
エ：事前基準を無視し、リスク受容の説明責任を欠く。
総合解説：品質ゲートにはリスク基準、責任者、例外承認、期限、補完策を含める。重大欠陥は少数でも優先度が高い。

Q072 4-3 テスト・脆弱性対応 / セキュリティテスト計画

自社アプリが外部ライブラリとSaaS APIへ依存している。セキュリティテスト計画として最も適切なものはどれか。
ア．自社が書いていないコードやサービスは安全と仮定し、全て対象外にする。
イ．ライブラリ名だけ確認し、実際のバージョンは記録しない。
ウ．SaaSは契約済みなので、付与権限の妥当性を確認しない。
エ．自社コードだけでなく、依存関係の既知脆弱性、設定、権限、インタフェース、障害時の影響も対象へ含める。

正答・4肢解説・総合解説

正答：エ．自社コードだけでなく、依存関係の既知脆弱性、設定、権限、インタフェース、障害時の影響も対象へ含める。
ア：第三者依存にも脆弱性や設定不備が存在する。
イ：脆弱性影響判定や再現性が低くなる。
ウ：過剰権限は自社側の設計・設定リスクとなる。
エ：システム全体の安全性は外部依存にも左右されるため、契約・設定・利用方法を含めて検証する。
総合解説：セキュリティテストは自社コードの境界を越えて、依存コンポーネント・クラウド設定・外部連携を含む実システム構成を対象にする。

Q073 4-3 テスト・脆弱性対応 / セキュリティテスト計画

本番に近い環境で外部事業者へペネトレーションテストを依頼する。開始前に最も重要な事項はどれか。
ア．対象範囲、許可する手法、禁止事項、実施時間、停止条件、連絡先、データ取扱いを明確に合意する。
イ．対象範囲を伝えず、可能な限り自由に攻撃してもらう。
ウ．緊急連絡先を定めず、障害時もテストを継続する。
エ．テストで取得した機密データの保管・削除条件を決めない。

正答・4肢解説・総合解説

正答：ア．対象範囲、許可する手法、禁止事項、実施時間、停止条件、連絡先、データ取扱いを明確に合意する。
ア：攻撃的テストは可用性やデータへ影響し得るため、Rules of Engagementを事前に定義する必要がある。
イ：誤って対象外システムや第三者へ影響を与える危険がある。
ウ：重大影響を拡大させる可能性がある。
エ：テスト自体が情報漏えい源になり得る。
総合解説：ペネトレーションテストは技術力だけでなく、権限・範囲・安全管理・証跡・報告・データ保護を明文化して実施する。

Q074 4-3 テスト・脆弱性対応 / セキュリティテスト計画

テスト環境ではWAF・認証連携・クラウド権限設定を省略しており、本番だけに存在する。リリース前の評価として最も適切なものはどれか。
ア．アプリのコードが同じなら構成差分はセキュリティへ影響しない。
イ．本番との差分を明確にし、本番固有の構成・連携・権限についても安全な方法で検証またはレビューする。
ウ．テスト環境で合格したため、本番設定は確認不要とする。
エ．本番だけの設定は文書化せず、担当者の記憶に任せる。

正答・4肢解説・総合解説

正答：イ．本番との差分を明確にし、本番固有の構成・連携・権限についても安全な方法で検証またはレビューする。
ア：認証・WAF・権限など構成はセキュリティに直接影響する。
イ：環境差分が大きいとテスト合格が本番安全性を示さないため、本番相当性と差分管理が必要である。
ウ：本番固有の誤設定を見逃す。
エ：再現性とレビュー可能性が低い。
総合解説：セキュリティテスト計画では環境差分を把握し、コードだけでなく設定・外部サービス・ネットワーク・ID連携を含めた本番条件を評価する。

Q075 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

組織的なパッチ管理プロセスとして最も適切なものはどれか。
ア．利用者から障害報告が出た端末だけ、担当者の判断で随時更新する。
イ．全パッチを内容確認なしで本番へ同時適用し、失敗時の復旧方法は用意しない。
ウ．対象資産と更新情報を把握し、リスクに基づき優先順位を付け、取得・検証・展開・適用確認まで管理する。
エ．脆弱性情報は収集せず、OSのメジャー更新時だけ対処する。

正答・4肢解説・総合解説

正答：ウ．対象資産と更新情報を把握し、リスクに基づき優先順位を付け、取得・検証・展開・適用確認まで管理する。
ア：組織的な資産把握や優先順位付けがなく、漏れが生じやすい。
イ：業務影響や互換性を考慮せず、可用性リスクが高い。
ウ：パッチ管理は単なるインストール作業ではなく、識別から検証までの継続的なプロセスである。
エ：重大なセキュリティ更新を長期間放置し得る。
総合解説：NIST SP 800-40 Rev.4は、パッチ管理を識別・優先順位付け・取得・適用・検証を含む予防保守として扱う。資産管理と例外管理も前提となる。

Q076 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

セキュリティ構成ベースラインを定める主な目的はどれか。
ア．全システムを同一機種へ統一しなければならないから。
イ．構成情報を一度作成したら更新しないため。
ウ．障害時に全てのセキュリティ設定を無効化するため。
エ．承認された標準構成を明確にし、逸脱や無許可変更を検出・評価できる基準を作る。

正答・4肢解説・総合解説

正答：エ．承認された標準構成を明確にし、逸脱や無許可変更を検出・評価できる基準を作る。
ア：ベースラインは必ずしも同一機種化を意味しない。
イ：変更に応じて承認済みベースラインも維持・更新する必要がある。
ウ：安全な標準状態を定義するものであり、無効化を目的としない。
エ：基準構成があることで、現在状態との差分や変更の妥当性を継続的に確認できる。
総合解説：NIST SP 800-128は、セキュリティ重視の構成管理でベースライン、変更管理、監視を重視する。

Q077 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

同日に複数のセキュリティ更新が公開された。最優先で評価すべき対象を決める考え方として最も適切なものはどれか。
ア．脆弱性の深刻度だけでなく、実際の悪用状況、資産の露出、業務重要度、代替策などを合わせて判断する。
イ．公開日が新しい順だけで決め、資産の重要度は考慮しない。
ウ．スコアが同じなら全て同じ期限でよく、外部公開かどうかは無視する。
エ．利用者数が少ないシステムは、機密情報を扱っていても永続的に更新不要とする。

正答・4肢解説・総合解説

正答：ア．脆弱性の深刻度だけでなく、実際の悪用状況、資産の露出、業務重要度、代替策などを合わせて判断する。
ア：CVSS等の技術的深刻度だけでは組織固有のリスクを表せないため、実環境の露出と影響を加味する。
イ：新しさだけではリスクの大きさを判断できない。
ウ：攻撃可能性や露出によって優先度は変わる。
エ：利用者数だけで重大性は決まらない。
総合解説：パッチ優先順位は脆弱性の性質と資産文脈を組み合わせる。悪用中・外部公開・重要資産などは優先度を高める要因になる。

Q078 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

重要業務サーバへ緊急パッチを適用する。可用性と安全性を両立する対応として最も適切なものはどれか。
ア．緊急なので事前確認・復旧手段・適用確認を全て省略する。
イ．影響を可能な範囲で事前検証し、バックアップやロールバック手順を準備して適用し、適用後にバージョン・機能・脆弱性解消を確認する。
ウ．パッチファイルをダウンロードした時点で適用済みと記録する。
エ．一度適用コマンドが成功したら、再起動やバージョン確認は不要とする。

正答・4肢解説・総合解説

正答：イ．影響を可能な範囲で事前検証し、バックアップやロールバック手順を準備して適用し、適用後にバージョン・機能・脆弱性解消を確認する。
ア：業務停止や未適用を見逃す可能性がある。
イ：緊急時でも適用失敗や互換性問題を想定し、復旧と適用確認まで含めて管理する。
ウ：取得とインストールは別であり、実際の適用を確認できない。
エ：適用が完了していない、または期待どおり動作しない可能性がある。
総合解説：パッチ管理は「入れたつもり」を避けるため、適用結果と残存リスクを確認する。重要系では復旧計画も不可欠である。

Q079 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

悪用中の重大脆弱性に対する緊急設定変更が必要になった。変更管理として最も適切なものはどれか。
ア．緊急なので誰でも本番設定を自由に変更し、記録は残さない。
イ．通常承認に数週間かかるため、悪用中でも変更を禁止する。
ウ．緊急変更手順に従って必要な承認と記録を簡略化しつつ確保し、実施後に妥当性・影響・恒久対応をレビューする。
エ．変更後のレビューは不要とし、恒久対応も検討しない。

正答・4肢解説・総合解説

正答：ウ．緊急変更手順に従って必要な承認と記録を簡略化しつつ確保し、実施後に妥当性・影響・恒久対応をレビューする。
ア：無許可変更や原因追跡不能につながる。
イ：リスクが高い場合に迅速な例外手続が必要である。
ウ：緊急性を理由に統制を完全に外すのではなく、迅速さと追跡性を両立する。
エ：一時対策が不適切なまま残る可能性がある。
総合解説：緊急変更はスピードを上げても、誰が何をなぜ変えたか、結果はどうだったかを追跡できるようにする。事後レビューも重要である。

Q080 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

クラウドサーバの実構成が、承認済みテンプレートから徐々にずれている。最も適切な対応はどれか。
ア．動作している限り差分を記録せず放置する。
イ．実構成を常に正しいものとして扱い、ベースラインを自動的に無条件で追随させる。
ウ．差分が出たら原因確認なしでサーバを削除する。
エ．構成差分を継続監視し、正当な変更か確認してベースラインを更新するか、無許可の逸脱を是正する。

正答・4肢解説・総合解説

正答：エ．構成差分を継続監視し、正当な変更か確認してベースラインを更新するか、無許可の逸脱を是正する。
ア：不要なポートや権限などの逸脱が蓄積し得る。
イ：無許可変更まで標準化してしまう。
ウ：業務影響と変更の正当性を評価していない。
エ：構成ドリフトを放置せず、承認状態との比較と変更履歴で統制する。
総合解説：構成管理では、承認済み基準と実状態の差分を把握し、変更の正当性を確認して是正または基準更新する。

Q081 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

高リスクな本番設定変更について、職務分離の観点から望ましい運用はどれか。
ア．変更提案者とは別の権限者が内容とリスクを確認し、承認後に実施し、結果を記録する。
イ．一人の担当者が提案・承認・実施・監査を全て行う。
ウ．承認記録を残さず口頭だけで済ませる。
エ．本番変更は誰でも行える共通アカウントだけを使う。

正答・4肢解説・総合解説

正答：ア．変更提案者とは別の権限者が内容とリスクを確認し、承認後に実施し、結果を記録する。
ア：重要変更を一人で提案・承認・実施できる状態を避け、誤操作や不正変更のリスクを下げる。
イ：相互牽制が働かず、不正やミスの発見が難しい。
ウ：後から変更の根拠や責任を追跡しにくい。
エ：主体識別と説明責任を損なう。
総合解説：変更管理では、リスクに応じた承認、職務分離、個人識別可能な操作、変更証跡を組み合わせる。

Q082 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

脆弱なミドルウェアの緊急更新が公開されたが、組織内のどのサーバがその製品を使っているか分からない。根本的な改善として最も適切なものはどれか。
ア．影響資産が分からないので、更新情報を無視する。
イ．ソフトウェア・バージョン・所有者・用途などの資産情報を維持し、脆弱性情報と影響資産を迅速に対応付けられるようにする。
ウ．全サーバを毎回初期化し、製品利用状況は記録しない。
エ．担当者の記憶だけで影響確認を続ける。

正答・4肢解説・総合解説

正答：イ．ソフトウェア・バージョン・所有者・用途などの資産情報を維持し、脆弱性情報と影響資産を迅速に対応付けられるようにする。
ア：脆弱性が残り続ける。
イ：パッチ適用対象を特定するには、資産・ソフトウェアの可視化が前提となる。
ウ：業務影響が大きく、資産把握の問題も解決しない。
エ：属人的で漏れや更新遅延が起こりやすい。
総合解説：資産インベントリはパッチ・脆弱性・構成管理の基礎である。製品名、バージョン、公開範囲、重要度、責任者等を追跡する。

Q083 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

重要業務で利用するOSがベンダサポート終了となり、今後セキュリティ更新が提供されない。最も適切な対応はどれか。
ア．現在動作しているので、無期限にそのまま利用する。
イ．サポート終了製品なら脆弱性は公表されないので安全とみなす。
ウ．移行計画を優先して策定し、完了までの間は分離・アクセス制限・監視等の補完策を適用し、残存リスクを管理する。
エ．製品名を社内文書から削除すればリスクはなくなる。

正答・4肢解説・総合解説

正答：ウ．移行計画を優先して策定し、完了までの間は分離・アクセス制限・監視等の補完策を適用し、残存リスクを管理する。
ア：新たな脆弱性に対する修正が得られず、リスクが増える。
イ：公表や攻撃の有無にかかわらず更新不能という構造的リスクがある。
ウ：更新不能な製品は時間とともにリスクが蓄積するため、恒久的な移行と暫定対策を組み合わせる。
エ：実システムの脆弱性は変わらない。
総合解説：EOL/EOS製品はパッチ管理上の重大課題である。期限・予算・責任者を持つ移行計画と、移行までの補完管理策が必要である。

Q084 4-3 テスト・脆弱性対応 / パッチ・構成・変更管理

セキュリティ強化の設定変更後、認証サービスが停止した。事前の変更計画に含めるべきだった事項として最も重要なものはどれか。
ア．変更内容だけ決め、失敗時は現場で考える。
イ．変更後の確認は利用者から苦情が出るまで行わない。
ウ．変更履歴を削除し、誰が何をしたか分からなくする。
エ．変更前状態へのロールバック条件・手順、依存サービスの確認、成功判定と監視方法を定めておく。

正答・4肢解説・総合解説

正答：エ．変更前状態へのロールバック条件・手順、依存サービスの確認、成功判定と監視方法を定めておく。
ア：停止時間が延び、誤った復旧操作のリスクが高まる。
イ：異常の早期検出ができない。
ウ：原因分析と再発防止を妨げる。
エ：変更は成功だけでなく失敗を前提に設計し、迅速かつ安全に戻せるようにする。
総合解説：変更管理は計画、評価、承認、実施、検証、記録、必要に応じたロールバックまで一連で扱う。

Q085 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

PSIRT（Product Security Incident Response Team）の中心的な役割として最も適切なものはどれか。
ア．自組織が提供する製品・サービスの脆弱性について、受付、評価、修正調整、情報公開などを組織横断で推進する。
イ．社内の給与計算だけを担当する。
ウ．外部からの脆弱性報告を受け付けず、社内発見分だけを扱う。
エ．製品の営業価格だけを決定する。

正答・4肢解説・総合解説

正答：ア．自組織が提供する製品・サービスの脆弱性について、受付、評価、修正調整、情報公開などを組織横断で推進する。
ア：PSIRTは製品セキュリティ脆弱性のリスクを扱い、開発・法務・サポート等と連携して対応する。
イ：製品セキュリティ脆弱性対応とは関係しない。
ウ：外部報告を受ける窓口や調整もPSIRTの重要な機能になり得る。
エ：PSIRTの中心的役割ではない。
総合解説：FIRSTはPSIRTを、組織が生産・販売する製品等のセキュリティ脆弱性リスクの特定・評価・処置に焦点を当てる組織機能として説明する。

Q086 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

製品ベンダが脆弱性開示ポリシー（VDP）と報告窓口を公開する主な目的はどれか。
ア．脆弱性報告を禁止し、発見者との連絡を断つため。
イ．外部研究者などが発見した脆弱性を安全かつ明確な経路で報告でき、調整された修正・開示へつなげるため。
ウ．全ての報告を確認せず自動的に公開するため。
エ．製品の広告メール配信用アドレスを増やすため。

正答・4肢解説・総合解説

正答：イ．外部研究者などが発見した脆弱性を安全かつ明確な経路で報告でき、調整された修正・開示へつなげるため。
ア：報告を受けられないと未知のリスクを把握しにくい。
イ：報告方法、対象範囲、期待する対応などを示すことで、脆弱性情報を適切に受け取りやすくなる。
ウ：影響評価や修正調整を行わない即時公開が目的ではない。
エ：脆弱性開示の目的とは無関係である。
総合解説：CISAは製品セキュリティ上の悪い慣行として、適切なVDPがないことを挙げる。明確な報告チャネルと調整された開示方針が重要である。

Q087 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

外部研究者から製品脆弱性の報告を受けた直後、PSIRTが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．内容を読まずに全報告を同じ優先度で処理する。
イ．報告者の所属だけで正誤を決め、技術内容は確認しない。
ウ．再現条件、影響を受ける製品・バージョン、想定影響、悪用状況、報告者との連絡手段などを確認する。
エ．対象製品を確認せず、全顧客へ一律に緊急停止を要求する。

正答・4肢解説・総合解説

正答：ウ．再現条件、影響を受ける製品・バージョン、想定影響、悪用状況、報告者との連絡手段などを確認する。
ア：重大度や悪用可能性に応じた優先順位付けができない。
イ：技術的再現性や影響を評価する必要がある。
ウ：事実関係と影響範囲を整理し、優先順位と対応方針を決めるための情報を収集する。
エ：影響範囲を特定せず過剰対応するのは不適切である。
総合解説：トリアージでは報告の妥当性、再現性、影響製品、深刻度、悪用の有無などを整理し、修正や調整の優先順位を決める。

Q088 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

同じ製品で2件の脆弱性が確認された。Aは低影響で悪用困難、Bは認証不要で遠隔から悪用され実被害も確認されている。対応順として最も適切なものはどれか。
ア．受付順だけで処理し、Bも通常の待ち行列へ置く。
イ．脆弱性番号の数字が小さい方だけを優先する。
ウ．どちらも製品が動作しているため対応しない。
エ．Bを緊急対応として優先し、影響顧客への軽減策・修正版・情報提供を迅速に調整する。

正答・4肢解説・総合解説

正答：エ．Bを緊急対応として優先し、影響顧客への軽減策・修正版・情報提供を迅速に調整する。
ア：実悪用中の重大リスクへ十分に対応できない。
イ：番号はリスクの大きさを示さない。
ウ：脆弱性リスクを無視している。
エ：実悪用、到達性、影響の大きさを考慮するとBの緊急度が高い。
総合解説：PSIRTは重大脆弱性や実悪用中の問題へ迅速に対応できる体制が必要である。スコアだけでなく現実の攻撃状況と顧客影響を加味する。

Q089 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

製品脆弱性の修正版を準備中で、外部報告者も公表を希望している。PSIRTの対応として最も適切なものはどれか。
ア．報告者・開発・法務・サポート等と連携し、修正や軽減策の準備状況を踏まえて調整された開示時期と内容を決める。
イ．報告者との連絡を断ち、脆弱性の存在を永久に隠す。
ウ．修正も軽減策もない状態で、影響確認せず機密な技術詳細を即時に全公開する。
エ．公表内容は営業部門だけで決め、技術的正確性を確認しない。

正答・4肢解説・総合解説

正答：ア．報告者・開発・法務・サポート等と連携し、修正や軽減策の準備状況を踏まえて調整された開示時期と内容を決める。
ア：利用者が対策できる情報と修正をできるだけ同期させ、関係者間のコミュニケーションを管理する。
イ：利用者のリスク判断と対策を妨げ、信頼も損なう。
ウ：利用者が防御できないまま悪用可能性を高める場合がある。
エ：誤った影響情報や対処方法を案内する危険がある。
総合解説：調整された脆弱性開示では、修正・軽減策・影響範囲・公開情報を関係者と調整し、利用者が行動できる形で正確に伝える。

Q090 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

入力検証不足による重大脆弱性を1か所修正した。PSIRT・開発チームの次の対応として最も適切なものはどれか。
ア．該当箇所だけ直し、同じパターンの他コードは確認しない。
イ．同種実装が他にもないか横断確認し、原因となった開発ルール・レビュー・テストの不足を改善して再発防止へつなげる。
ウ．脆弱性を発見したテストを削除し、今後検出されないようにする。
エ．開発手順は一切見直さず、同じ原因の脆弱性が出たら都度対応する。

正答・4肢解説・総合解説

正答：イ．同種実装が他にもないか横断確認し、原因となった開発ルール・レビュー・テストの不足を改善して再発防止へつなげる。
ア：類似脆弱性が残る可能性がある。
イ：個別パッチだけでなく、欠陥が生まれた根本原因と類似箇所を扱うことで将来の脆弱性を減らせる。
ウ：再発を見逃すことになる。
エ：根本原因を放置している。
総合解説：NIST SSDFは脆弱性の根本原因を特定し、将来の再発を防ぐ改善へ反映することを重視する。回帰テスト化やコーディング規約更新も有効である。

Q091 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

実悪用中の脆弱性に対して緊急修正版を作成した。配布前の対応として最も適切なものはどれか。
ア．緊急なのでビルドできた時点で無検証で配布する。
イ．どのバージョンが影響するか確認せず、全顧客へ同じ手順を案内する。
ウ．修正の有効性と副作用を重点的に検証し、影響バージョン、更新方法、回避策、既知の制約を明確にして配布する。
エ．回避策が存在しても利用者には知らせない。

正答・4肢解説・総合解説

正答：ウ．修正の有効性と副作用を重点的に検証し、影響バージョン、更新方法、回避策、既知の制約を明確にして配布する。
ア：修正不十分や重大な回帰を見逃す可能性がある。
イ：不要な変更や誤対応を招き得る。
ウ：緊急性が高くても、誤った修正で障害や未解決を生まないよう最低限の検証と正確な情報提供が必要である。
エ：修正版適用までのリスク低減機会を失わせる。
総合解説：PSIRTの緊急対応でも、修正の妥当性、影響範囲、利用者が取れる行動を整理する。迅速さと正確性の両立が必要である。

Q092 4-3 テスト・脆弱性対応 / 脆弱性ハンドリング・PSIRT

PSIRTが毎回同じ種類の脆弱性対応で混乱し、修正・告知に時間がかかっている。改善策として最も適切なものはどれか。
ア．経験者一人だけに全判断を集中し、手順書や代替要員を作らない。
イ．報告件数を減らすため、外部窓口を閉鎖する。
ウ．事後レビューを禁止し、同じ問題でも毎回ゼロから対応する。
エ．受付・トリアージ・重大度判定・開発連携・CVE/告知・緊急対応などの標準プロセスと役割を定義し、訓練・振り返りで継続改善する。

正答・4肢解説・総合解説

正答：エ．受付・トリアージ・重大度判定・開発連携・CVE/告知・緊急対応などの標準プロセスと役割を定義し、訓練・振り返りで継続改善する。
ア：属人化し、欠勤・退職時に機能しなくなる。
イ：未把握の脆弱性が増え、リスクを隠すだけである。
ウ：学習と継続改善ができない。
エ：属人的な都度対応から、再現可能なサービス・役割・エスカレーションへ標準化することで応答力を高められる。
総合解説：FIRSTのPSIRT Services Frameworkは、PSIRTが提供し得るサービスや能力を整理している。標準化、役割分担、関係部門連携、訓練、改善が成熟化に有効である。

Q093 4-4 監視・ログ管理 / SOC・SIEM

SOC（Security Operation Center）の役割として最も適切なものはどれか。
ア．組織のセキュリティ事象を継続的に監視し、検知した事象を分析・トリアージして、必要に応じて対応部門へエスカレーションする。
イ．製品開発の売上目標だけを策定する。
ウ．全ての脆弱性を自動的に修正し、人の判断を不要にする。
エ．監査ログを削除して保存容量を最小化する。

正答・4肢解説・総合解説

正答：ア．組織のセキュリティ事象を継続的に監視し、検知した事象を分析・トリアージして、必要に応じて対応部門へエスカレーションする。
ア：SOCは監視と分析を継続し、インシデントの疑いを早期に見つけて適切な対応へつなぐ運用機能である。
イ：SOCの主目的は事業計画ではなくセキュリティ監視・分析である。
ウ：SOCは検知・分析・連携が中心であり、全脆弱性の自動修正を保証するものではない。
エ：ログは検知・調査の基礎であり、適切な保管が必要である。
総合解説：IPAはSOC、セキュリティ監視、ログの取得・分析を支援士の知識・技能として挙げる。SOCは検知だけでなく、事象の評価と関係部門への連携まで含む運用体制として設計する。

Q094 4-4 監視・ログ管理 / SOC・SIEM

SIEMを導入する主な目的として最も適切なものはどれか。
ア．利用者のパスワードを平文で一元保存する。
イ．複数の機器やサービスからログを集約し、検索・相関分析・可視化・アラート生成を行いやすくする。
ウ．サーバの冗長化だけを実現する。
エ．ソースコードを自動生成して脆弱性をなくす。

正答・4肢解説・総合解説

正答：イ．複数の機器やサービスからログを集約し、検索・相関分析・可視化・アラート生成を行いやすくする。
ア：認証秘密の平文保存はSIEMの目的ではなく危険である。
イ：SIEMは異なるログ源を集中管理し、横断的な相関分析や検知を支援する。
ウ：冗長化は可用性設計であり、SIEMの中心機能ではない。
エ：SIEMはログ分析基盤であり、コード生成ツールではない。
総合解説：ログを一元化することで、単一機器のログでは見えにくい攻撃の連鎖や異常を横断的に把握しやすくなる。

Q095 4-4 監視・ログ管理 / SOC・SIEM

SIEMとSOARの役割の説明として最も適切なものはどれか。
ア．SIEMはバックアップ専用、SOARは暗号鍵管理専用である。
イ．SIEMとSOARは同一概念で、機能上の区別はない。
ウ．SIEMは主にログの集約・相関・検知を担い、SOARは手順化された対応のオーケストレーションや自動化を支援する。
エ．SOARはログを保存せず、必ず人手のみで対応するための仕組みである。

正答・4肢解説・総合解説

正答：ウ．SIEMは主にログの集約・相関・検知を担い、SOARは手順化された対応のオーケストレーションや自動化を支援する。
ア：いずれもそのような専用製品ではない。
イ：一般にSIEMは分析・検知、SOARは対応自動化・連携の比重が高い。
ウ：両者は連携することが多いが、中心的な役割は異なる。
エ：SOARは自動化やワークフロー連携を支援する。
総合解説：監視運用では、SIEMで検知したアラートをSOARやチケット管理と連携し、定型的な確認・通知・封じ込めを効率化する設計がある。

Q096 4-4 監視・ログ管理 / SOC・SIEM

海外IPからのVPNログイン成功直後に、同一利用者のクラウド管理画面で特権操作が行われた。SOCの初動として最も適切なものはどれか。
ア．アラートが1件だけなので無条件に無視する。
イ．直ちに全社の全アカウントを永久停止し、調査は行わない。
ウ．VPNログだけを削除して誤検知を防ぐ。
エ．VPN、IdP、クラウド監査ログを時系列で突合し、利用者・端末・送信元・認証状況を確認して、侵害の可能性をトリアージする。

正答・4肢解説・総合解説

正答：エ．VPN、IdP、クラウド監査ログを時系列で突合し、利用者・端末・送信元・認証状況を確認して、侵害の可能性をトリアージする。
ア：重大な侵害の初期兆候を見逃す可能性がある。
イ：影響確認前の過剰対応で業務影響が大きく、根拠も得られない。
ウ：証跡を失い、調査不能になる。
エ：単一アラートだけで断定せず、関連ログを相関させて事実関係と影響範囲を評価するのが適切である。
総合解説：SOCのトリアージでは複数のログ源を相関し、利用者・端末・時間・送信元・操作内容を確認する。必要に応じて本人確認やセッション失効などへつなげる。

Q097 4-4 監視・ログ管理 / SOC・SIEM

新しいSaaSの監査ログをSIEMへ取り込むことになった。最初に行うべき設計として最も適切なものはどれか。
ア．重要なイベント、利用者ID、時刻、送信元、結果など必要な項目を定義し、共通形式への正規化と欠損・遅延の監視方法を決める。
イ．全フィールドを意味確認せず文字列1項目へ連結する。
ウ．保存容量を節約するため、成功・失敗の結果を削除する。
エ．取り込み後の欠損や遅延は監視せず、アラートだけを信頼する。

正答・4肢解説・総合解説

正答：ア．重要なイベント、利用者ID、時刻、送信元、結果など必要な項目を定義し、共通形式への正規化と欠損・遅延の監視方法を決める。
ア：ログを取り込むだけでなく、検知に必要なフィールド品質と運用監視まで設計する必要がある。
イ：相関や検索が困難になり、検知品質が低下する。
ウ：認証や操作の成否は分析上重要な情報になり得る。
エ：ログ停止により検知不能でも気付けない。
総合解説：中央集約では、ログソースごとの意味を保ちながら正規化し、収集状態そのものも監視する。

Q098 4-4 監視・ログ管理 / SOC・SIEM

SOCで大量のアラートが発生している。優先順位付けとして最も適切なものはどれか。
ア．件数が多いルールだけを常に最優先にする。
イ．検知の信頼度だけでなく、対象資産の重要度、権限、悪用可能性、実被害の兆候などを合わせて評価する。
ウ．最も古いアラートから機械的に処理し、重大度は見ない。
エ．資産情報や利用者権限は分析に使わない。

正答・4肢解説・総合解説

正答：イ．検知の信頼度だけでなく、対象資産の重要度、権限、悪用可能性、実被害の兆候などを合わせて評価する。
ア：件数の多さとリスクの大きさは一致しない。
イ：同じ検知でも重要サーバと検証端末では事業影響が異なるため、コンテキストを加味した優先順位付けが必要である。
ウ：緊急性の高い事象を後回しにする危険がある。
エ：影響度判断に重要なコンテキストを失う。
総合解説：効率的な監視には、検知シグナルへ資産・ID・脅威情報などの文脈を付加し、限られた分析資源を高リスク事象へ集中させることが重要である。

Q099 4-4 監視・ログ管理 / SOC・SIEM

新しい検知ルールが毎日数千件の誤検知を出し、SOCが重要アラートを見落とし始めた。改善策として最も適切なものはどれか。
ア．ルールを永久に無効化し、代替検知は用意しない。
イ．誤検知を減らすため全ログ収集を停止する。
ウ．誤検知の原因を分析し、対象範囲・閾値・例外条件を根拠付きで調整し、変更後も既知の攻撃シナリオを検知できるか検証する。
エ．アラート数を減らすため重大度を全て最低に固定する。

正答・4肢解説・総合解説

正答：ウ．誤検知の原因を分析し、対象範囲・閾値・例外条件を根拠付きで調整し、変更後も既知の攻撃シナリオを検知できるか検証する。
ア：本来検知すべき攻撃まで見逃す可能性がある。
イ：監視能力そのものを失う。
ウ：単にルールを無効化するのではなく、検知性能と運用負荷の両方を評価してチューニングする。
エ：優先順位付けが機能しなくなる。
総合解説：検知ルールは継続的に評価・改善する。チューニングでは、誤検知率だけでなく真陽性の維持と検知漏れのリスクを確認する。

Q100 4-4 監視・ログ管理 / SOC・SIEM

夜間SOCが、重要サーバで未知の管理者アカウント作成と外部送信を同時に検知した。分析担当者だけで長時間調査を続ける運用の問題点として最も適切なものはどれか。
ア．夜間は全アラートを翌営業日まで保留するのが原則なので問題ない。
イ．未知アカウントは必ず正当なので調査不要である。
ウ．外部送信を検知した時点でログを削除すれば問題は解決する。
エ．重大度や影響に応じた明確なエスカレーション基準がないと、封じ込め判断や関係部門への連絡が遅れる。

正答・4肢解説・総合解説

正答：エ．重大度や影響に応じた明確なエスカレーション基準がないと、封じ込め判断や関係部門への連絡が遅れる。
ア：重大事象まで一律保留すると被害拡大につながる。
イ：正当性は確認が必要で、外部送信との組合せは高リスクである。
ウ：証跡破壊であり、対応を悪化させる。
エ：重大インシデント候補は、SOC内だけで抱えず、定めた基準でCSIRT・システム責任者等へ迅速に連携する必要がある。
総合解説：監視設計には、検知後のトリアージ、重大度判定、エスカレーション、連絡先、対応権限まで含める。

Q101 4-4 監視・ログ管理 / SOC・SIEM

SIEM基盤自体が障害で停止した場合にも重大イベントの検知を継続したい。設計として最も適切なものはどれか。
ア．重要ログのバッファリングや代替参照経路、SIEM収集停止を検知する監視、復旧後の再送・欠損確認を用意する。
イ．SIEMが止まったらログ生成元も全て停止させる。
ウ．収集停止はアラートが出ないので正常とみなす。
エ．復旧後は停止期間のログを破棄し、現在分だけ見る。

正答・4肢解説・総合解説

正答：ア．重要ログのバッファリングや代替参照経路、SIEM収集停止を検知する監視、復旧後の再送・欠損確認を用意する。
ア：監視基盤は単一障害点になり得るため、収集停止そのものを検知し、ログ損失を抑える設計が必要である。
イ：業務停止を招き、証跡も失う。
ウ：監視の盲点が生じる。
エ：停止期間に発生した事象を調査できない。
総合解説：ログ管理基盤にも可用性と監視が必要である。収集遅延・欠損の検知、ローカル保持、再送などで観測可能性を維持する。

Q102 4-4 監視・ログ管理 / SOC・SIEM

既知の攻撃手法に対するSOCの検知カバレッジを継続的に改善したい。最も適切な進め方はどれか。
ア．導入済みルール数だけを増やし、検知対象や品質は評価しない。
イ．重要な脅威シナリオごとに必要なテレメトリと検知ルールを対応付け、演習や実インシデントの結果から欠落を見直す。
ウ．過去に事故がなかったログ源は全て永久に廃止する。
エ．検知テストは本番影響が怖いため一切実施しない。

正答・4肢解説・総合解説

正答：イ．重要な脅威シナリオごとに必要なテレメトリと検知ルールを対応付け、演習や実インシデントの結果から欠落を見直す。
ア：数が多くても重要な攻撃を検知できるとは限らない。
イ：脅威シナリオ、ログ源、ルール、対応手順を関連付け、実証結果に基づいてギャップを更新するのが有効である。
ウ：将来の攻撃や新たな利用形態を見逃す可能性がある。
エ：ルールが実際に機能するか確認できない。
総合解説：検知エンジニアリングでは、脅威に対する観測可能性とルール有効性をテストし、継続的に改善する。

Q103 4-4 監視・ログ管理 / ログ設計・相関分析

認証イベントのログ項目として、後日の調査に最も有用な組合せはどれか。
ア．パスワードそのもの、秘密鍵そのもの、セッションCookieの全値。
イ．画面の背景色、フォント、利用者の好みだけ。
ウ．時刻、利用者識別子、送信元、対象システム、認証の成否、認証方式。
エ．成功件数の月合計だけで、個別イベントは記録しない。

正答・4肢解説・総合解説

正答：ウ．時刻、利用者識別子、送信元、対象システム、認証の成否、認証方式。
ア：秘密情報をログへ記録すると漏えいリスクが高まる。
イ：認証事象の追跡にはほとんど役立たない。
ウ：誰が、いつ、どこから、何に対して、どのような結果になったかを追跡できる項目が基本となる。
エ：個々の事象の時系列調査ができない。
総合解説：ログ設計では調査・検知に必要な属性を確保しつつ、パスワードや鍵など不要な機密情報を記録しない。

Q104 4-4 監視・ログ管理 / ログ設計・相関分析

アプリケーションログへ原則として記録すべきでない情報はどれか。
ア．処理結果を示す成功・失敗コード。
イ．追跡用の要求ID。
ウ．アプリケーション名とイベント種別。
エ．利用者の平文パスワードやAPI秘密鍵など、認証に使える秘密情報。

正答・4肢解説・総合解説

正答：エ．利用者の平文パスワードやAPI秘密鍵など、認証に使える秘密情報。
ア：検知やトラブルシュートに有用である。
イ：分散処理の相関に役立つ。
ウ：ログの意味を識別する基本情報である。
エ：ログは広く集約・参照されることがあるため、認証秘密を記録すると二次漏えいの原因になる。
総合解説：必要最小限の記録と機密情報のマスキングを設計し、ログ自体も保護対象として扱う。

Q105 4-4 監視・ログ管理 / ログ設計・相関分析

Webフロント、API、データベースに処理が分かれるシステムで、1件の利用者要求を横断追跡したい。最も適切な方法はどれか。
ア．要求ごとに一意な相関IDを付与し、各コンポーネントのログへ同じIDを引き継いで記録する。
イ．各サーバが無関係な連番を付け、対応表は持たない。
ウ．全ログの時刻を日付だけに丸める。
エ．追跡性を下げるため利用者IDも要求IDも全て削除する。

正答・4肢解説・総合解説

正答：ア．要求ごとに一意な相関IDを付与し、各コンポーネントのログへ同じIDを引き継いで記録する。
ア：時刻だけよりも一意なIDを併用することで、並行処理が多い環境でも同一トランザクションを追跡しやすい。
イ：サーバ間の同一要求を結び付けにくい。
ウ：粒度が粗く、並行要求を区別できない。
エ：インシデント調査が困難になる。
総合解説：分散システムでは、トレースIDや要求IDなどの共通識別子を設計し、時刻や利用者情報と組み合わせて相関分析する。

Q106 4-4 監視・ログ管理 / ログ設計・相関分析

短時間に「多数の認証失敗→認証成功→権限昇格→大量ダウンロード」というイベントが発生した。分析として最も適切なものはどれか。
ア．各イベントを完全に独立とみなし、関連性を調べない。
イ．同一利用者・送信元・端末などをキーに時系列で相関し、単発イベントではなく一連の攻撃シナリオとして評価する。
ウ．大量ダウンロードだけを見て、直前の認証や権限変更は破棄する。
エ．イベント順序は不要なので時刻を全て削除する。

正答・4肢解説・総合解説

正答：イ．同一利用者・送信元・端末などをキーに時系列で相関し、単発イベントではなく一連の攻撃シナリオとして評価する。
ア：攻撃の連鎖を見逃す。
イ：攻撃は複数イベントの連鎖として現れることがあり、相関によって検知の信頼度を高められる。
ウ：侵入経路や原因分析に必要な情報を失う。
エ：時系列分析ができなくなる。
総合解説：相関分析では、共通キーと時間窓を用いて複数ログを結び付け、攻撃の文脈を把握する。

Q107 4-4 監視・ログ管理 / ログ設計・相関分析

ログの保持期間を決める方針として最も適切なものはどれか。
ア．保存容量がある限り全ログを無期限保存し、目的や個人情報を考慮しない。
イ．障害がなければ当日中に全ログを消す。
ウ．法令・契約・社内規程、調査に必要な期間、脅威の潜伏期間、保存コストなどを踏まえてログ種別ごとに定める。
エ．保持期間は利用者ごとに自由入力させる。

正答・4肢解説・総合解説

正答：ウ．法令・契約・社内規程、調査に必要な期間、脅威の潜伏期間、保存コストなどを踏まえてログ種別ごとに定める。
ア：不要な長期保持はコストやプライバシー・漏えいリスクを増やす。
イ：後日のセキュリティ調査ができなくなる。
ウ：全ログ一律ではなく、目的とリスクに基づく保持設計が必要である。
エ：組織的な証跡管理ができない。
総合解説：ログ保持は可用性だけでなく、調査可能性、法的義務、データ最小化、コストのバランスを取る。

Q108 4-4 監視・ログ管理 / ログ設計・相関分析

全てのデバッグログを常時収集した結果、重要ログの検索が遅くなり保存費も急増した。改善策として最も適切なものはどれか。
ア．重要ログを含め全て停止する。
イ．検索性能を上げるため時刻と利用者IDを削除する。
ウ．保存費を抑えるためログを非暗号化で公開ストレージへ置く。
エ．検知・監査・障害解析に必要なイベントと粒度を定義し、高頻度デバッグ情報は必要時だけ有効化するなど収集方針を最適化する。

正答・4肢解説・総合解説

正答：エ．検知・監査・障害解析に必要なイベントと粒度を定義し、高頻度デバッグ情報は必要時だけ有効化するなど収集方針を最適化する。
ア：検知・調査能力を失う。
イ：相関に必要な情報を失う。
ウ：機密性・完全性を損なう。
エ：ログは多ければ多いほど良いとは限らず、利用目的とコストに応じた設計が必要である。
総合解説：ログ方針ではイベント選定、粒度、フィルタリング、保存層を設計し、分析価値を維持しながら過剰収集を抑える。

Q109 4-4 監視・ログ管理 / ログ設計・相関分析

攻撃者がログ転送エージェントを停止した場合でも、監視担当が早期に気付けるようにしたい。最も適切な設計はどれか。
ア．各ログ源の最終受信時刻・期待イベント量・エージェント状態を監視し、一定時間受信がない場合にもアラートを出す。
イ．アラートはログが届いた時だけ作り、無受信は常に正常とみなす。
ウ．ログ転送エージェントの状態は攻撃者にも変更できるよう権限を広げる。
エ．転送停止後のローカルログも自動削除する。

正答・4肢解説・総合解説

正答：ア．各ログ源の最終受信時刻・期待イベント量・エージェント状態を監視し、一定時間受信がない場合にもアラートを出す。
ア：「イベントが来ない」こと自体を異常として監視することで、意図的停止や障害による盲点を検知できる。
イ：収集停止を検知できない。
ウ：停止や改変を容易にする。
エ：証跡回復の可能性を失う。
総合解説：ログ管理では収集経路の健全性も監視対象である。欠損・遅延・急減を検知し、調査できるようにする。

Q110 4-4 監視・ログ管理 / ログ設計・相関分析

通常時は1時間に数回しか管理者操作がないシステムで、深夜に数百回の管理操作が発生した。最も適切な分析はどれか。
ア．件数が多いだけで必ず侵害と断定し、確認を省略する。
イ．通常時のイベント量・時間帯・利用主体をベースラインとして比較し、変更作業予定や正当な自動処理の有無も確認する。
ウ．通常時との比較は不要で、ログの文字数だけを見る。
エ．深夜のイベントは全て除外して監視しない。

正答・4肢解説・総合解説

正答：イ．通常時のイベント量・時間帯・利用主体をベースラインとして比較し、変更作業予定や正当な自動処理の有無も確認する。
ア：正当な一括作業の可能性を排除できない。
イ：異常量は有力な兆候だが、業務変更など正当な理由もあり得るため、ベースラインとコンテキストを併用する。
ウ：行動異常を評価できない。
エ：攻撃が夜間に行われる可能性を見逃す。
総合解説：相関・異常分析では正常パターンを理解し、資産・利用者・変更予定などの文脈で判断する。

Q111 4-4 監視・ログ管理 / ログ設計・相関分析

複数製品のログをSIEMの共通スキーマへ変換する際、設計上最も重要な点はどれか。
ア．同名フィールドなら意味確認せず必ず同じ項目へ入れる。
イ．変換後の値だけを残し、元ログとの対応を一切持たない。
ウ．元ログの意味を確認し、利用者・IP・イベント結果など対応関係を定義しつつ、必要に応じて原本も追跡できるよう保持する。
エ．全てのIPアドレスを0.0.0.0へ置換する。

正答・4肢解説・総合解説

正答：ウ．元ログの意味を確認し、利用者・IP・イベント結果など対応関係を定義しつつ、必要に応じて原本も追跡できるよう保持する。
ア：製品ごとに意味や形式が異なることがある。
イ：解析誤りの検証や詳細調査が難しくなる。
ウ：誤ったフィールドマッピングは相関や検知を誤らせるため、意味の整合性と原本への追跡性が重要である。
エ：相関に必要な送信元・宛先情報を失う。
総合解説：正規化は単なる形式変換ではない。検知に必要な意味を正確に保持し、変換ルールの品質を管理する。

Q112 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

セキュリティログを取得する機器で時刻同期が重要な主な理由はどれか。
ア．ログの保存容量を必ず半分にできるため。
イ．全ての攻撃を自動的に防止できるため。
ウ．暗号鍵の長さを自動的に増やすため。
エ．複数機器のイベント順序を正しく比較し、インシデントの発生経緯を時系列で再構成しやすくするため。

正答・4肢解説・総合解説

正答：エ．複数機器のイベント順序を正しく比較し、インシデントの発生経緯を時系列で再構成しやすくするため。
ア：時刻同期自体にそのような効果はない。
イ：時刻同期は検知・調査を支援するが攻撃防止そのものではない。
ウ：時刻同期と鍵長は別の問題である。
エ：時刻がずれると同じ攻撃の関連イベントが逆順に見えるなど、相関分析や証跡評価を誤る。
総合解説：IPAはNTPを含む時刻同期を明示している。正確な時刻はログ相関、証跡、インシデント調査の前提となる。

Q113 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

複数地域のクラウドサービスからログを集約する際、時刻の扱いとして最も適切なものはどれか。
ア．タイムゾーンやUTCとの対応が分かる形式で記録し、相関時に共通の時間基準へ正規化する。
イ．タイムゾーン情報を削除し、全て同じ文字列時刻として扱う。
ウ．時刻は不要なので日付だけ記録する。
エ．ログ源ごとに時計を意図的に数時間ずらす。

正答・4肢解説・総合解説

正答：ア．タイムゾーンやUTCとの対応が分かる形式で記録し、相関時に共通の時間基準へ正規化する。
ア：地域ごとのローカル時刻だけでは夏時間やタイムゾーン差で誤解が生じるため、共通基準に変換可能であることが重要である。
イ：同じ表示でも実際の時刻が異なる可能性がある。
ウ：短時間の攻撃連鎖を追跡できない。
エ：相関分析を困難にする。
総合解説：監査記録は一貫した時間基準へ対応付けられることが望ましい。

Q114 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

侵害されたサーバ上の攻撃者がローカルログを削除するリスクを低減したい。最も適切な対策はどれか。
ア．アプリ管理者に集中ログの削除権限も無制限に与える。
イ．ログを迅速に別の保護された集中ログ基盤へ転送し、書込み権限を分離して改ざん・削除を制限する。
ウ．ログはサーバの同じディスクにだけ保存する。
エ．検知後に全ログを上書きして容量を確保する。

正答・4肢解説・総合解説

正答：イ．ログを迅速に別の保護された集中ログ基盤へ転送し、書込み権限を分離して改ざん・削除を制限する。
ア：侵害時にログまで消されやすくなる。
イ：攻撃対象とログ保管先を分離し、ログへの変更権限を限定することで証跡の残存性を高める。
ウ：サーバ侵害や障害と同時に失う可能性がある。
エ：証拠保全に反する。
総合解説：NISTのAU管理策は監査情報の保護やアクセス制限を扱う。集中化、分離、暗号学的保護、書込み制御などを組み合わせる。

Q115 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

本番システム管理者が、自分の操作記録を自由に削除できる設定になっている。改善策として最も適切なものはどれか。
ア．管理者なら全ログを自由に変更できるのが望ましい。
イ．ログへのアクセス制御を廃止し、全社員に削除権限を与える。
ウ．通常のシステム管理権限と監査ログの変更・削除権限を分離し、必要最小限の担当者だけに付与する。
エ．監査ログ自体を取得しない。

正答・4肢解説・総合解説

正答：ウ．通常のシステム管理権限と監査ログの変更・削除権限を分離し、必要最小限の担当者だけに付与する。
ア：不正操作の隠蔽が可能になる。
イ：改ざん・消失リスクがさらに高まる。
ウ：監査対象者が自分の証跡を自由に変更できないよう職務・権限を分離することで説明責任を高める。
エ：操作追跡や不正検知ができない。
総合解説：ログは単に取得するだけでなく、閲覧・変更・削除の権限を管理し、監査機能を保護する必要がある。

Q116 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

パスワードスプレーを検知したい。単一アカウントの連続失敗だけを見るより適切なルールはどれか。
ア．同一アカウントの1秒間100回失敗だけを唯一の条件にする。
イ．認証成功ログだけを見て失敗ログは破棄する。
ウ．送信元や時間を一切使わず、月間失敗件数だけを見る。
エ．一定時間内に同一送信元から多数の異なるアカウントへ少数回ずつ認証失敗が発生するパターンを集計する。

正答・4肢解説・総合解説

正答：エ．一定時間内に同一送信元から多数の異なるアカウントへ少数回ずつ認証失敗が発生するパターンを集計する。
ア：低頻度で複数アカウントを狙う手法を見逃しやすい。
イ：試行パターンを把握できない。
ウ：リアルタイム性と攻撃単位の相関が弱い。
エ：パスワードスプレーはアカウントロックを避けるため、複数アカウントへ低頻度で試すことがある。送信元と時間窓を用いた集計が有効である。
総合解説：検知ルールは攻撃手法の特徴に合わせ、適切なキーと時間窓、閾値を設計する。

Q117 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

定期バックアップ用サービスアカウントの大量アクセスが毎晩アラートになる。例外設定として最も適切なものはどれか。
ア．対象アカウント・実行元・時間帯・処理内容を限定した例外にし、変更時は再評価し、例外外の挙動は引き続き検知する。
イ．サービスアカウントに関する全イベントを永久に監視対象外にする。
ウ．夜間のログを全て捨てる。
エ．例外理由を記録せず誰でも追加できるようにする。

正答・4肢解説・総合解説

正答：ア．対象アカウント・実行元・時間帯・処理内容を限定した例外にし、変更時は再評価し、例外外の挙動は引き続き検知する。
ア：正当な業務を考慮しつつ、例外範囲を最小化して攻撃者の悪用余地を減らす。
イ：侵害されても検知できなくなる。
ウ：他の攻撃も見逃す。
エ：ルールの形骸化につながる。
総合解説：検知チューニングでは、例外を具体的かつ監査可能にし、定期的に妥当性を見直す。

Q118 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

SIEMの高重要度ルールを大幅に変更する。変更管理として最も適切なものはどれか。
ア．本番へ直接反映し、結果が悪ければ履歴なしで上書きする。
イ．検知目的と想定イベントを文書化し、代表的な正常・攻撃データでテストしてから段階的に展開し、変更後の真陽性・誤陽性を監視する。
ウ．変更前後のテストは一切しない。
エ．誤検知をゼロにするためルールを「何も検知しない」にする。

正答・4肢解説・総合解説

正答：イ．検知目的と想定イベントを文書化し、代表的な正常・攻撃データでテストしてから段階的に展開し、変更後の真陽性・誤陽性を監視する。
ア：影響分析やロールバックが困難になる。
イ：検知ルールも本番制御の一部であり、変更により検知漏れやアラート洪水が起こり得るため検証が必要である。
ウ：検知不能や誤検知増加を事前に把握できない。
エ：監視目的を失う。
総合解説：ルールの版管理、テスト、承認、段階展開、ロールバックは監視品質の維持に有効である。

Q119 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

あるサーバだけ時計が20分進んでおり、SIEMでは「情報持出し」が「認証成功」より先に記録されて見える。最も適切な対応はどれか。
ア．表示順が正しいと決めつけ、認証ログを改ざんと断定する。
イ．全ログの時刻を手作業で同じ値に上書きする。
ウ．時刻同期状態とログのタイムゾーンを確認し、補正可能な範囲を明示して時系列を再構成するとともに、同期障害自体を是正する。
エ．時刻同期の問題はセキュリティに無関係なので放置する。

正答・4肢解説・総合解説

正答：ウ．時刻同期状態とログのタイムゾーンを確認し、補正可能な範囲を明示して時系列を再構成するとともに、同期障害自体を是正する。
ア：時計ずれという既知の事実を無視している。
イ：原証跡を失い、根拠も不明になる。
ウ：誤った時刻をそのまま信頼すると攻撃経路を誤認する。同期状態の確認と補正根拠の記録が必要である。
エ：相関・証拠評価に重大な影響がある。
総合解説：時刻同期はログ分析の基盤である。補正する場合も原ログを保持し、補正根拠を記録して調査の再現性を確保する。

Q120 4-4 監視・ログ管理 / 時刻同期・証跡保護・検知ルール

重大インシデントの調査中、監査ログに攻撃者の操作痕跡が見つかった。証跡保全として最も適切な対応はどれか。
ア．見やすくするため原ログを直接編集し不要行を削除する。
イ．担当者が個人USBへ無記録でコピーして持ち帰る。
ウ．調査が終わる前に保存期間を短縮して自動削除する。
エ．原ログを変更せずアクセス制御された形で保全し、必要なコピーを作成してハッシュや取扱記録などで完全性・追跡性を確保しながら分析する。

正答・4肢解説・総合解説

正答：エ．原ログを変更せずアクセス制御された形で保全し、必要なコピーを作成してハッシュや取扱記録などで完全性・追跡性を確保しながら分析する。
ア：原証跡の完全性を損なう。
イ：管理不能で漏えい・改ざんリスクが高い。
ウ：必要な証跡を失う。
エ：分析のために原本を直接編集せず、完全性と取扱経緯を確認できるようにする。
総合解説：監査情報は不正な変更や削除から保護し、インシデント時は証拠としての完全性・取扱履歴を意識して保全する。

Q121 4-5 運用・レジリエンス / バックアップ・復旧

バックアップと冗長化の違いとして最も適切なものはどれか。
ア．冗長化は主にサービス継続を高め、バックアップは消失・破損・誤更新したデータを過去時点へ復元するために用いる。
イ．冗長化があれば過去データのバックアップは常に不要である。
ウ．バックアップはサービスを無停止にするためだけの仕組みである。
エ．両者は完全に同じ概念である。

正答・4肢解説・総合解説

正答：ア．冗長化は主にサービス継続を高め、バックアップは消失・破損・誤更新したデータを過去時点へ復元するために用いる。
ア：冗長化だけでは誤削除や暗号化されたデータが複製されることがあり、バックアップの代替にはならない。
イ：誤削除やランサムウェアによる破壊が冗長系へ反映される可能性がある。
ウ：主目的はデータやシステムの復元である。
エ：目的と故障モードへの効果が異なる。
総合解説：レジリエンスでは冗長化とバックアップを別の対策として組み合わせる。

Q122 4-5 運用・レジリエンス / バックアップ・復旧

RPO（Recovery Point Objective）が表すものとして最も適切なものはどれか。
ア．サービス復旧までに許容される最大停止時間。
イ．障害時にどの時点までデータを戻せれば許容できるかという、許容可能なデータ損失量を時間で表した目標。
ウ．バックアップ媒体の暗号鍵長。
エ．システムの年間稼働率だけを示す値。

正答・4肢解説・総合解説

正答：イ．障害時にどの時点までデータを戻せれば許容できるかという、許容可能なデータ損失量を時間で表した目標。
ア：これはRTOに近い。
イ：例えばRPOが1時間なら、原則として最大1時間程度のデータ損失を想定してバックアップ等を設計する。
ウ：RPOとは関係しない。
エ：RPOはデータ復旧点に関する目標である。
総合解説：RPOはバックアップ頻度やレプリケーション方式の設計に影響する。

Q123 4-5 運用・レジリエンス / バックアップ・復旧

RTO（Recovery Time Objective）が表すものとして最も適切なものはどれか。
ア．許容できるデータ損失量を時間で表す目標。
イ．1日に取得するログ件数。
ウ．障害発生後、対象サービスや業務を許容時間内に復旧させるための時間目標。
エ．暗号アルゴリズムの処理時間。

正答・4肢解説・総合解説

正答：ウ．障害発生後、対象サービスや業務を許容時間内に復旧させるための時間目標。
ア：これはRPOに近い。
イ：RTOとは無関係である。
ウ：RTOは復旧手順、代替環境、要員、冗長化などの設計に影響する。
エ：復旧目標時間ではない。
総合解説：RTOとRPOは異なる目標であり、BIAなどに基づいて業務・システムごとに定める。

Q124 4-5 運用・レジリエンス / バックアップ・復旧

バックアップ運用で定期的な復元テストが必要な主な理由はどれか。
ア．バックアップ容量を必ずゼロにできるため。
イ．ログを削除するため。
ウ．RTOとRPOを不要にするため。
エ．バックアップが取得できていても、破損・設定不備・鍵不足・手順不備により実際には復元できない可能性があるため。

正答・4肢解説・総合解説

正答：エ．バックアップが取得できていても、破損・設定不備・鍵不足・手順不備により実際には復元できない可能性があるため。
ア：復元テストにその効果はない。
イ：復元テストの目的ではない。
ウ：復元テストは目標達成可能性を確認する手段である。
エ：取得成功だけでは復旧可能性を保証できないので、復元して検証する必要がある。
総合解説：レジリエンスではバックアップの存在ではなく、必要な時間内に正しく戻せることを確認する。

Q125 4-5 運用・レジリエンス / バックアップ・復旧

ランサムウェア感染時にバックアップまで暗号化される事態を抑えたい。最も適切な対策はどれか。
ア．本番環境から常時書換え可能な経路だけに依存せず、オフライン・イミュータブル等の保護されたコピーを持ち、管理権限も分離する。
イ．本番管理者の同じ資格情報で全バックアップも削除可能にする。
ウ．バックアップは本番サーバの同じボリュームにだけ置く。
エ．復旧できるかどうかは確認せずコピーだけ増やす。

正答・4肢解説・総合解説

正答：ア．本番環境から常時書換え可能な経路だけに依存せず、オフライン・イミュータブル等の保護されたコピーを持ち、管理権限も分離する。
ア：攻撃者が本番の高権限を得ても全バックアップを破壊しにくいよう、障害・権限・保存先の分離を行う。
イ：侵害時にバックアップまで破壊されやすい。
ウ：同一障害や暗号化の影響を受けやすい。
エ：不良コピーを増やしても復旧性は保証されない。
総合解説：2026年のNISTランサムウェアプロファイルも、バックアップを含む復旧能力の整備と検証を重視する。

Q126 4-5 運用・レジリエンス / バックアップ・復旧

高頻度更新されるデータベースを、単純なファイルコピーだけでバックアップしたところ復元時に不整合が生じた。改善策として最も適切なものはどれか。
ア．稼働中ファイルをランダムな順序でコピーし続ける。
イ．DBMSが提供する整合性を考慮したバックアップ機能やスナップショット、ログ連携を用い、復元手順まで検証する。
ウ．復元時にエラーが出てもデータを強制上書きする。
エ．バックアップ対象からトランザクション情報を必ず除外する。

正答・4肢解説・総合解説

正答：イ．DBMSが提供する整合性を考慮したバックアップ機能やスナップショット、ログ連携を用い、復元手順まで検証する。
ア：整合性の保証がない。
イ：更新途中のファイルを無秩序にコピーすると、アプリケーション整合性を満たさない可能性がある。
ウ：破損や不整合を悪化させる。
エ：復旧に必要な場合があり一律除外は不適切である。
総合解説：バックアップ方式はデータの更新特性と整合性要件に合わせる。復元テストではアプリケーションが正常に動作することまで確認する。

Q127 4-5 運用・レジリエンス / バックアップ・復旧

バックアップを強固に暗号化していたが、災害で鍵管理サーバも同時に失われ復号できなかった。改善策として最も適切なものはどれか。
ア．暗号化をやめてバックアップを公開保存する。
イ．鍵は担当者1人の記憶だけに依存する。
ウ．バックアップ暗号鍵や復号手段も復旧対象として、適切に保護された別障害領域の保管・復旧手順を設計する。
エ．鍵管理サーバとバックアップを同じ単一障害点に置く。

正答・4肢解説・総合解説

正答：ウ．バックアップ暗号鍵や復号手段も復旧対象として、適切に保護された別障害領域の保管・復旧手順を設計する。
ア：機密性を損なう。
イ：属人化し、喪失時に復旧できない。
ウ：データだけでなく復号に必要な鍵・設定・資格情報も回復可能でなければバックアップは利用できない。
エ：同時喪失リスクが残る。
総合解説：復旧設計ではデータ、システム構成、鍵、資格情報、依存サービスを含めて必要資産を特定する。

Q128 4-5 運用・レジリエンス / バックアップ・復旧

データ破損が発生したが、破損に気付くまで3日かかり、その間の毎日バックアップにも破損データが含まれていた。改善策として最も適切なものはどれか。
ア．毎回前回バックアップを即時削除し、1世代だけにする。
イ．破損検知を避けるためバックアップ検証を行わない。
ウ．本番データを削除してバックアップだけを使う。
エ．複数世代のバックアップを保持し、復旧ポイントを選べるようにするとともに、バックアップの健全性を監視する。

正答・4肢解説・総合解説

正答：エ．複数世代のバックアップを保持し、復旧ポイントを選べるようにするとともに、バックアップの健全性を監視する。
ア：過去の正常時点へ戻れない。
イ：不良バックアップを長期間保持する危険がある。
ウ：可用性と業務継続を損なう。
エ：最新1世代だけでは、潜伏していた破損や誤操作がバックアップへ反映された場合に戻れない。
総合解説：保持世代や復旧ポイントは、RPO、検知遅延、法的要件、容量を踏まえて設計する。

Q129 4-5 運用・レジリエンス / バックアップ・復旧

業務アプリ、DB、認証基盤、DNSの全てが停止した。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、認証や名前解決、DBなど上位サービスが必要とする基盤から優先順位を付けて復旧する。
イ．名前順にサーバを起動し、依存関係は考慮しない。
ウ．最も重要でない検証端末から復旧し、基幹機能は最後にする。
エ．依存関係は障害時に初めて調べればよい。

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、認証や名前解決、DBなど上位サービスが必要とする基盤から優先順位を付けて復旧する。
ア：復旧は単純なサーバ一覧順ではなく、業務重要度と技術的依存関係を考慮する必要がある。
イ：起動しても必要サービスへ接続できず復旧が進まない可能性がある。
ウ：業務復旧目標に合わない。
エ：復旧時間が延びる。
総合解説：BIAとシステム依存関係を組み合わせ、復旧順序・前提条件・担当をプレイブック化する。

Q130 4-5 運用・レジリエンス / バックアップ・復旧

侵害後にバックアップから復元する直前の確認として最も適切なものはどれか。
ア．最も新しいバックアップなら無条件に安全とみなす。
イ．バックアップの完全性、取得時点、マルウェア混入の可能性、復号可能性を確認し、信頼できる復旧点を選ぶ。
ウ．バックアップの取得日時は確認しない。
エ．復元後の検証は不要である。

正答・4肢解説・総合解説

正答：イ．バックアップの完全性、取得時点、マルウェア混入の可能性、復号可能性を確認し、信頼できる復旧点を選ぶ。
ア：侵害後に取得されたバックアップには攻撃者の変更が含まれる可能性がある。
イ：バックアップ自体が破損・侵害されている可能性を考慮し、復元前に健全性を検証する。
ウ：侵害前後の判断ができない。
エ：不正状態や破損が残る可能性がある。
総合解説：NIST CSF 2.0は復旧に使用するバックアップ等の完全性確認と、復元した資産の完全性確認を回復成果として示している。

Q131 4-5 運用・レジリエンス / バックアップ・復旧

侵入時点が不明なため、バックアップに攻撃者の永続化設定が含まれる可能性がある。安全な復旧方針として最も適切なものはどれか。
ア．最新バックアップを無条件で全台へ復元し、監視は停止する。
イ．攻撃者が使った資格情報をそのまま継続利用する。
ウ．侵害範囲と侵入時点を分析し、信頼できる基準イメージや検証済みバックアップから復旧し、資格情報更新・脆弱性修正・監視強化後に業務へ戻す。
エ．原因不明のまま復旧完了と宣言する。

正答・4肢解説・総合解説

正答：ウ．侵害範囲と侵入時点を分析し、信頼できる基準イメージや検証済みバックアップから復旧し、資格情報更新・脆弱性修正・監視強化後に業務へ戻す。
ア：永続化や脆弱性を再導入する危険がある。
イ：再侵入を許す可能性がある。
ウ：単純に最新バックアップへ戻すだけでは再侵害する可能性がある。復旧は根本原因への対処と検証を伴う。
エ：再発防止と安全性確認が不足している。
総合解説：サイバー事象からの回復では、単なるデータ復元ではなく、安全な状態への復旧、完全性確認、再発防止を組み合わせる。

Q132 4-5 運用・レジリエンス / バックアップ・復旧

設計上はRTO4時間だが、過去の復元訓練では毎回8時間かかっている。最も適切な対応はどれか。
ア．計画書に4時間と書いてあるので実測8時間でも問題なしとする。
イ．訓練をやめれば未達が見えなくなるので解決する。
ウ．RTOを記録から削除し、復旧時間を測らない。
エ．実測結果を基にボトルネックを特定し、手順自動化、代替環境、要員、バックアップ方式等を改善して再テストするか、事業側と目標を再合意する。

正答・4肢解説・総合解説

正答：エ．実測結果を基にボトルネックを特定し、手順自動化、代替環境、要員、バックアップ方式等を改善して再テストするか、事業側と目標を再合意する。
ア：実際の復旧能力が目標を満たしていない。
イ：リスクを隠すだけである。
ウ：業務要件との整合を評価できない。
エ：紙上の目標だけでなく、演習で達成可能性を確認し、達成できない場合は対策または目標の見直しが必要である。
総合解説：復旧計画はテスト・演習・実事象から学び継続改善する。

Q133 4-5 運用・レジリエンス / BCP・可用性・冗長化

BIA（Business Impact Analysis）の主な目的として最も適切なものはどれか。
ア．業務停止による影響や許容停止時間、重要資源・依存関係を把握し、復旧優先順位や継続要件を決める。
イ．全てのパスワードを一括変更すること。
ウ．脆弱性スキャンの実行だけを行うこと。
エ．データセンタの温度だけを測ること。

正答・4肢解説・総合解説

正答：ア．業務停止による影響や許容停止時間、重要資源・依存関係を把握し、復旧優先順位や継続要件を決める。
ア：BIAは全システムを同じ優先度で復旧するのではなく、業務影響に基づき復旧目標を決めるために用いる。
イ：BIAの目的ではない。
ウ：BIAは事業影響と継続要件の分析である。
エ：一部の設備情報に限定されない。
総合解説：継続計画では、まず重要業務と影響を把握し、その結果をRTO/RPOや復旧戦略へ反映する。

Q134 4-5 運用・レジリエンス / BCP・可用性・冗長化

単一障害点（SPOF）の説明として最も適切なものはどれか。
ア．故障しても全く影響しない予備部品。
イ．その一要素が故障すると、代替経路や冗長系がなくサービス全体が停止し得る構成要素。
ウ．バックアップの世代数を表す指標。
エ．利用者のパスワード強度だけを示す指標。

正答・4肢解説・総合解説

正答：イ．その一要素が故障すると、代替経路や冗長系がなくサービス全体が停止し得る構成要素。
ア：単一障害点ではない。
イ：SPOFを特定して冗長化や代替手段を設けることは可用性向上の基本である。
ウ：SPOFとは無関係である。
エ：可用性構成の概念ではない。
総合解説：冗長化ではサーバだけでなく電源、ネットワーク、認証、DNS、クラウドリージョン等の依存関係も確認する。

Q135 4-5 運用・レジリエンス / BCP・可用性・冗長化

BCPとITの災害復旧（DR）の関係として最も適切なものはどれか。
ア．BCPはバックアップ媒体の暗号化方式だけを定める。
イ．DRがあれば業務部門の代替手順や連絡計画は不要である。
ウ．BCPは重要業務を継続・再開するための全体計画であり、DRはその中でITシステムやデータを復旧するための要素の一つである。
エ．BCPとDRは互いに無関係である。

正答・4肢解説・総合解説

正答：ウ．BCPは重要業務を継続・再開するための全体計画であり、DRはその中でITシステムやデータを復旧するための要素の一つである。
ア：BCPの範囲はより広い。
イ：ITが復旧するまでの業務継続や関係者調整も必要である。
ウ：業務継続には人員、拠点、連絡、代替手順なども含まれ、IT復旧だけでは完結しない。
エ：DRはBCP/継続計画と密接に関連する。
総合解説：NISTの継続計画ガイドは、情報システム継続計画と他の緊急・事業継続計画との関係を扱う。

Q136 4-5 運用・レジリエンス / BCP・可用性・冗長化

Webサーバを2台に増やしたが、両方が同じ電源装置と同じスイッチに接続されている。可用性上の問題として最も適切なものはどれか。
ア．サーバが2台なら全ての障害に耐えられる。
イ．同じラックに置くほど地理的冗長性が高まる。
ウ．電源やネットワークは可用性に影響しない。
エ．サーバは冗長でも電源やネットワークが単一障害点のままで、共通故障により2台同時停止する可能性がある。

正答・4肢解説・総合解説

正答：エ．サーバは冗長でも電源やネットワークが単一障害点のままで、共通故障により2台同時停止する可能性がある。
ア：共通インフラの故障には耐えられない。
イ：同じ故障領域に集約される。
ウ：サービス提供の前提となる。
エ：冗長化では個々の台数ではなく、障害領域と依存関係を分離できているかを確認する。
総合解説：高可用性設計では、電源、ネットワーク、ストレージ、認証、DNS等も含めて単一障害点を除去する。

Q137 4-5 運用・レジリエンス / BCP・可用性・冗長化

待機系サーバは構築済みだが、3年間一度も切替試験をしていない。最も適切な対応はどれか。
ア．計画した条件でフェイルオーバー試験を行い、切替時間、データ整合性、依存サービス、戻し手順を確認する。
イ．障害発生まで待ち、本番で初めて切り替える。
ウ．待機系は動かすと壊れるので、ログインも禁止する。
エ．切替試験ではデータ整合性を確認しない。

正答・4肢解説・総合解説

正答：ア．計画した条件でフェイルオーバー試験を行い、切替時間、データ整合性、依存サービス、戻し手順を確認する。
ア：存在するだけの待機系は、設定差異や容量不足で実際には機能しない可能性がある。
イ：未検証の問題が本番障害時に顕在化する。
ウ：健全性や設定差異を確認できない。
エ：サービスが起動してもデータ不整合があれば復旧とはいえない。
総合解説：継続計画は定期的にテスト・訓練し、結果を改善へ反映する。

Q138 4-5 運用・レジリエンス / BCP・可用性・冗長化

「別拠点」として2つのデータセンタを用意したが、同じ洪水想定区域で同一通信局舎に依存していた。評価として最も適切なものはどれか。
ア．住所が異なれば共通故障は絶対に起きない。
イ．地理的に別住所でも共通災害や共通インフラに依存しており、想定する障害に対する独立性が不足している可能性がある。
ウ．遠隔拠点ではバックアップや通信回線は不要である。
エ．共通通信局舎への依存は可用性を必ず高める。

正答・4肢解説・総合解説

正答：イ．地理的に別住所でも共通災害や共通インフラに依存しており、想定する障害に対する独立性が不足している可能性がある。
ア：同じ災害やインフラ障害の影響を受けることがある。
イ：冗長拠点は距離だけでなく、電力・通信・災害・運用などの共通故障要因を評価する必要がある。
ウ：復旧に必要なデータ・接続が必要である。
エ：むしろ単一障害点になり得る。
総合解説：代替サイトや冗長化は、想定リスクに対して十分に分離された故障領域を持つよう設計する。

Q139 4-5 運用・レジリエンス / BCP・可用性・冗長化

通常時は2系統で50%ずつ処理しているが、片系停止時に残り1系統の最大容量を超えることが分かった。最も適切な対応はどれか。
ア．冗長系が2台あるという事実だけで十分とする。
イ．片系停止時は監視を止めて負荷を見えなくする。
ウ．障害時の必要負荷を満たす容量設計を見直し、縮退運転の優先サービスや追加容量も含めて負荷試験する。
エ．障害時ほど全ての低優先業務を増やす。

正答・4肢解説・総合解説

正答：ウ．障害時の必要負荷を満たす容量設計を見直し、縮退運転の優先サービスや追加容量も含めて負荷試験する。
ア：容量不足を解決していない。
イ：実際の処理能力は改善しない。
ウ：冗長系が存在しても、障害時に必要な容量がなければ目標可用性を満たせない。
エ：重要サービスの容量を圧迫する。
総合解説：可用性設計は故障時の性能・容量まで含めて検証し、必要に応じて優先業務への資源配分を計画する。

Q140 4-5 運用・レジリエンス / BCP・可用性・冗長化

災害時に全機能を維持する資源がない。BCP上の対応として最も適切なものはどれか。
ア．全機能を同じ優先度で無理に維持し、重要業務も共倒れにする。
イ．災害時の優先順位は当日の担当者の勘だけで決める。
ウ．低優先機能の停止条件は誰にも知らせない。
エ．重要業務を優先し、低優先機能を一時停止・制限する縮退運転を事前に定義して、関係者へ手順を共有する。

正答・4肢解説・総合解説

正答：エ．重要業務を優先し、低優先機能を一時停止・制限する縮退運転を事前に定義して、関係者へ手順を共有する。
ア：事業影響を拡大する可能性がある。
イ：判断の遅れや不整合を招く。
ウ：運用混乱を招く。
エ：限られた資源で重要機能を継続するため、優先順位と許容できるサービス低下を事前に定める。
総合解説：BIAで重要業務を把握し、代替手段や縮退運転を継続計画に盛り込む。

Q141 4-5 運用・レジリエンス / BCP・可用性・冗長化

クラウドをマルチAZ構成にしたが、全AZで同じIdPと同じDNSサービスに依存している。レジリエンス評価として最も適切なものはどれか。
ア．AZ障害への耐性は高まっても、共通IdPやDNSが停止すると全体が利用不能になるため、依存サービスを含むエンドツーエンドの障害分析が必要である。
イ．マルチAZなら上位・下位の依存サービスは一切考慮不要である。
ウ．IdPとDNSは可用性に影響しない。
エ．冗長化は台数が多いほど必ず独立性が高い。

正答・4肢解説・総合解説

正答：ア．AZ障害への耐性は高まっても、共通IdPやDNSが停止すると全体が利用不能になるため、依存サービスを含むエンドツーエンドの障害分析が必要である。
ア：個別レイヤの冗長化だけでなく、サービスチェーン全体の単一障害点・共通モード故障を確認する。
イ：共通依存先が単一障害点になり得る。
ウ：認証や名前解決が失われると利用不能になり得る。
エ：同じ依存先を共有すれば共通故障が残る。
総合解説：レジリエンス設計では、アプリだけでなく認証、名前解決、ネットワーク、鍵、監視などの依存関係を含めて障害シナリオを評価する。

Q142 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

組織支給のリモートワーク端末の基本運用として最も適切なものはどれか。
ア．利用者が更新を永久に拒否できるようにする。
イ．標準構成を定め、OS・アプリ更新、マルウェア対策、暗号化、監視、設定逸脱の管理を継続する。
ウ．セキュリティ設定は利用者ごとに完全自由とし、基準を設けない。
エ．端末紛失時の対策は不要とする。

正答・4肢解説・総合解説

正答：イ．標準構成を定め、OS・アプリ更新、マルウェア対策、暗号化、監視、設定逸脱の管理を継続する。
ア：既知脆弱性が残る。
イ：端末を支給して終わりではなく、ライフサイクルを通じた構成・更新・監視が必要である。
ウ：組織としてリスク管理できない。
エ：外部利用では紛失・盗難リスクも考慮する。
総合解説：NISTはテレワーク端末を含むクライアント機器を想定脅威に対して保護し、関連ポリシーを整備することを推奨している。

Q143 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

ノートPCのフルディスク暗号化が主に低減するリスクはどれか。
ア．フィッシングメールを必ず受信しなくなる。
イ．全てのWeb攻撃を防止する。
ウ．端末の紛失・盗難時に、ストレージを取り外すなどして保存データを読み取られるリスク。
エ．バックアップが不要になる。

正答・4肢解説・総合解説

正答：ウ．端末の紛失・盗難時に、ストレージを取り外すなどして保存データを読み取られるリスク。
ア：ディスク暗号化はメール受信を防ぐ機能ではない。
イ：保存データ保護が中心であり、Web攻撃対策の代替ではない。
ウ：適切な認証と鍵保護を前提に、保存データの機密性を高める。
エ：暗号化とバックアップは目的が異なる。
総合解説：モバイル端末は物理的に持ち出されるため、紛失・盗難を前提とした保存データ保護が重要である。

Q144 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

一般利用者の端末でローカル管理者権限を常時付与しない主な理由はどれか。
ア．管理者権限がないとインターネットへ接続できないから。
イ．管理者権限を外すとログが自動的に全削除されるから。
ウ．管理者権限は暗号鍵と同じ意味だから。
エ．マルウェアや誤操作が高い権限でシステム設定を変更する範囲を抑え、被害を限定するため。

正答・4肢解説・総合解説

正答：エ．マルウェアや誤操作が高い権限でシステム設定を変更する範囲を抑え、被害を限定するため。
ア：一般にそのような必須条件ではない。
イ：そのような関係はない。
ウ：権限と暗号鍵は異なる概念である。
エ：業務上必要な操作に権限を限定し、管理操作は別の管理手段で行うことが望ましい。
総合解説：リモート端末でも最小権限、標準構成、管理者操作の分離を維持する。

Q145 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

社員が会社支給ノートPCを出張先で紛失した。初動として最も適切なものはどれか。
ア．紛失を速やかに報告させ、端末識別、アカウント・トークンの失効、遠隔ロック/ワイプ可否、保存データの影響を手順に従って評価する。
イ．見つかるまで数週間待ち、アカウントはそのまま使う。
ウ．報告を避けるため資産台帳から端末を削除する。
エ．暗号化されていれば認証トークンの失効は常に不要である。

正答・4肢解説・総合解説

正答：ア．紛失を速やかに報告させ、端末識別、アカウント・トークンの失効、遠隔ロック/ワイプ可否、保存データの影響を手順に従って評価する。
ア：紛失端末は物理アクセスを受ける前提で、認証情報とデータのリスクを迅速に減らす。
イ：不正利用の時間を与える。
ウ：インシデント管理と追跡を妨げる。
エ：ログイン済み状態やトークンが悪用される可能性を考慮すべきである。
総合解説：端末管理には紛失・盗難時の報告、遠隔制御、認証情報失効、影響評価を含む手順が必要である。

Q146 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

社外から管理システムへアクセスさせる運用として最も適切なものはどれか。
ア．管理画面をインターネットへ無制限公開し、パスワード1つだけにする。
イ．組織が承認したリモートアクセス経路を用い、強固な認証、端末状態確認、最小権限、ログ記録を組み合わせる。
ウ．個人の未管理端末から管理者共有アカウントで接続させる。
エ．リモートアクセスのログを取得しない。

正答・4肢解説・総合解説

正答：イ．組織が承認したリモートアクセス経路を用い、強固な認証、端末状態確認、最小権限、ログ記録を組み合わせる。
ア：攻撃面が大きく認証強度も不足しやすい。
イ：通信の保護だけでなく、利用者認証、端末信頼性、権限、監視を組み合わせることが重要である。
ウ：端末・IDの追跡性と防御が弱い。
エ：不正利用の検知・調査が困難になる。
総合解説：NIST SP 800-46はリモートアクセス技術だけでなく、端末、認証、ポリシーを含めて保護することを扱う。

Q147 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

VPN接続中の端末が、社内ネットワークとインターネットへ同時に直接通信するスプリットトンネルを許可している。評価として最も適切なものはどれか。
ア．スプリットトンネルは必ず全ての攻撃を防止する。
イ．VPN利用中は端末側のセキュリティ対策は不要になる。
ウ．利便性や帯域面の利点はあるが、未信頼ネットワークと社内接続の橋渡しとなるリスクがあるため、脅威モデルに基づき制御する。
エ．ネットワーク経路は脅威モデルに影響しない。

正答・4肢解説・総合解説

正答：ウ．利便性や帯域面の利点はあるが、未信頼ネットワークと社内接続の橋渡しとなるリスクがあるため、脅威モデルに基づき制御する。
ア：むしろ追加の攻撃経路になり得る。
イ：端末は依然として攻撃対象である。
ウ：常に禁止・常に許可ではなく、端末保護、経路制御、監視、業務要件を踏まえて判断する。
エ：接続経路は攻撃面に直接影響する。
総合解説：リモートアクセスでは、端末が同時に接続するネットワークや通信経路を含めてリスク評価する。

Q148 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

BYODを許可する場合、個人データへの過度な干渉を避けつつ組織データを保護したい。最も適切な対策はどれか。
ア．端末内の全個人写真を常時会社サーバへ送信する。
イ．業務データを個人クラウドへ自由に同期させる。
ウ．紛失時に業務データだけを消す機能は使わず、管理も行わない。
エ．業務用コンテナや管理プロファイルで組織データ・アプリを論理分離し、業務領域に対する暗号化・コピー制御・選択的ワイプを行う。

正答・4肢解説・総合解説

正答：エ．業務用コンテナや管理プロファイルで組織データ・アプリを論理分離し、業務領域に対する暗号化・コピー制御・選択的ワイプを行う。
ア：業務目的を超えた侵襲的管理になり得る。
イ：組織の管理外へデータが流出しやすい。
ウ：組織データを保護できない。
エ：個人領域と業務領域を分けることで、組織データ保護と利用者プライバシーの両立を図りやすい。
総合解説：BYODでは、端末全体を組織所有端末と同じように扱えない場合があり、業務データの分離と管理範囲を明確にすることが重要である。

Q149 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

社員が空港の公衆Wi-Fiから業務を行う必要がある。組織の運用として最も適切なものはどれか。
ア．未信頼ネットワークとして扱い、承認済みの保護されたリモートアクセス、強固な認証、端末ファイアウォール等を用い、不要な共有機能を無効にする。
イ．SSID名が会社名に似ていれば安全とみなす。
ウ．公衆Wi-FiではOS更新や端末保護を無効化する。
エ．業務システムの管理パスワードを周囲と共有する。

正答・4肢解説・総合解説

正答：ア．未信頼ネットワークとして扱い、承認済みの保護されたリモートアクセス、強固な認証、端末ファイアウォール等を用い、不要な共有機能を無効にする。
ア：外部ネットワークを信頼せず、通信・端末・認証の防御を重ねる。
イ：偽アクセスポイントの可能性がある。
ウ：端末の防御を弱める。
エ：認証情報漏えいにつながる。
総合解説：リモートワークでは、利用場所やネットワークを前提に脅威モデルを作り、安全な通信経路と端末保護を適用する。

Q150 4-5 運用・レジリエンス / エンドポイント・リモートワーク運用

在宅勤務端末が社内LANへ数か月接続しないため、パッチ配布とEDR監視が遅延している。改善策として最も適切なものはどれか。
ア．出社するまで更新・監視を全て停止する。
イ．インターネット経由でも認証された管理基盤へ安全に接続できる仕組みを用意し、更新・ポリシー・監視状態を継続的に確認する。
ウ．利用者に管理者権限を与え、好きなソフトを自由に入れてもらう。
エ．EDRが通信できない状態を正常とみなし、欠損を監視しない。

正答・4肢解説・総合解説

正答：イ．インターネット経由でも認証された管理基盤へ安全に接続できる仕組みを用意し、更新・ポリシー・監視状態を継続的に確認する。
ア：既知脆弱性や侵害の検知遅延が長期化する。
イ：端末管理を社内LAN接続時だけに依存すると、長期リモート端末が管理外になりやすい。
ウ：構成逸脱やマルウェアリスクを高める。
エ：侵害やエージェント停止を見逃す。
総合解説：リモートワーク運用では、端末が社内にいない期間も更新、構成管理、セキュリティ監視を維持できる管理経路が重要である。