Q001 3-1 Web・アプリケーション攻撃 / SQLインジェクション

WebアプリケーションでSQLインジェクションが成立しやすい実装はどれか。
ア．利用者入力を文字列連結してSQL文を組み立て、そのままDBMSへ実行させる。
イ．SQL文とデータ値を分離してパラメータ化クエリで実行する。
ウ．DB接続アカウントへ必要最小限の権限だけを与える。
エ．入力値とは無関係な固定SQLだけを実行する。

正答・4肢解説・総合解説

正答：ア．利用者入力を文字列連結してSQL文を組み立て、そのままDBMSへ実行させる。
ア：利用者入力がSQL文の構文として解釈され得るため、意図しない検索・更新などにつながる。
イ：値がSQL構文として解釈されないよう分離する代表的な対策である。
ウ：被害軽減策として有効だが、脆弱な文字列連結を成立させる要因ではない。
エ：外部入力がSQL構文へ混入しなければ、この原因によるSQLインジェクションは成立しにくい。
総合解説：SQLインジェクションの本質は、データとして扱うべき入力とSQLコードの境界が崩れることにある。第一選択はパラメータ化クエリであり、最小権限などを重ねて防御する。

Q002 3-1 Web・アプリケーション攻撃 / SQLインジェクション

SQLインジェクション対策としてプリペアドステートメント（パラメータ化クエリ）が有効な主な理由はどれか。
ア．利用者入力に含まれる英数字を全て削除するため。
イ．SQLの構造と入力値を分離してDBMSへ渡し、入力値をSQL構文として解釈させにくくするため。
ウ．DBMSの監査ログを自動的に暗号化するため。
エ．アプリケーションの全権限をDB管理者権限へ昇格するため。

正答・4肢解説・総合解説

正答：イ．SQLの構造と入力値を分離してDBMSへ渡し、入力値をSQL構文として解釈させにくくするため。
ア：パラメータ化クエリは文字の削除処理ではなく、SQL構造と値の分離である。
イ：プレースホルダへ値を束縛することで、コードとデータの境界を保つ。
ウ：ログ暗号化は別の管理策であり、SQLインジェクション防止の原理ではない。
エ：権限昇格は被害を拡大し得るため逆効果である。
総合解説：安全性を高めるには、パラメータ化できない識別子等はallowlistで制御し、DBアカウントも最小権限にする。

Q003 3-1 Web・アプリケーション攻撃 / SQLインジェクション

SQLインジェクション対策として「利用者入力からシングルクォートだけを削除する」方式の評価として最も適切なものはどれか。
ア．シングルクォートさえ削除すれば全DBMSで完全に防止できる。
イ．入力検証はSQLインジェクション対策では一切使ってはならない。
ウ．入力表現やDBMS・文脈によって回避され得るため、それだけに依存せずパラメータ化クエリを基本とする。
エ．SQLインジェクションは暗号化通信を使えば発生しない。

正答・4肢解説・総合解説

正答：ウ．入力表現やDBMS・文脈によって回避され得るため、それだけに依存せずパラメータ化クエリを基本とする。
ア：SQL構文や入力文脈は多様であり、特定文字の除去だけで完全防止はできない。
イ：列名や並び順などパラメータ化しにくい箇所ではallowlist検証が有効である。
ウ：特定文字の除去は抜け道や文字コード差異を生みやすく、根本対策として脆弱である。
エ：TLSは通信路を保護するが、サーバ側SQLの組立て不備は残る。
総合解説：ブラックリスト型の文字除去より、パラメータ化クエリとallowlist、最小権限を組み合わせる方が堅牢である。

Q004 3-1 Web・アプリケーション攻撃 / SQLインジェクション

商品検索用WebアプリのDB接続アカウントに、検索対象表のSELECT権限だけを与えた。SQLインジェクション対策上の効果として最も適切なものはどれか。
ア．SQL文の文字列連結が自動的にパラメータ化される。
イ．利用者のブラウザでXSSが実行されなくなる。
ウ．DBMSの脆弱性が全て修正される。
エ．脆弱性そのものを除去するわけではないが、攻撃が成立した場合に更新・削除などへ被害が広がる範囲を抑えられる。

正答・4肢解説・総合解説

正答：エ．脆弱性そのものを除去するわけではないが、攻撃が成立した場合に更新・削除などへ被害が広がる範囲を抑えられる。
ア：権限設定はSQL生成方法を変更しない。
イ：DB権限はブラウザ上のXSS対策ではない。
ウ：アクセス権付与はパッチ適用の代替ではない。
エ：最小権限は侵害後の影響を限定する防御層である。
総合解説：根本対策は安全なクエリ実装だが、DB権限、ネットワーク分離、監視を組み合わせることで多層防御になる。

Q005 3-1 Web・アプリケーション攻撃 / SQLインジェクション

Blind SQLインジェクションの説明として最も適切なものはどれか。
ア．DBの値が画面に直接表示されなくても、応答の真偽や時間差などの挙動を手掛かりに情報を推測する攻撃である。
イ．DBのバックアップ媒体を物理的に盗み出す攻撃である。
ウ．常に同一LAN内のARP表を書き換える攻撃である。
エ．ブラウザにスクリプトを保存して実行させる攻撃だけを指す。

正答・4肢解説・総合解説

正答：ア．DBの値が画面に直接表示されなくても、応答の真偽や時間差などの挙動を手掛かりに情報を推測する攻撃である。
ア：エラーや結果セットが直接返らない状況でも、観測可能な差を利用して情報を推定する。
イ：これは物理的な情報窃取でありSQLインジェクションではない。
ウ：ARPスプーフィングの説明に近い。
エ：保存型XSSの説明に近い。
総合解説：SQLインジェクションは「画面にSQLエラーが出るか」だけで判断できない。挙動差を利用する推論型も存在するため、安全なクエリ実装が必要である。

Q006 3-1 Web・アプリケーション攻撃 / SQLインジェクション

注文管理システムでSQLインジェクションが成立し、アプリ用DBアカウントにSELECT・UPDATE・DELETE権限が付与されていた。想定すべき影響として最も適切なものはどれか。
ア．必ずOSのカーネル権限を取得される。
イ．閲覧可能な情報の漏えいに加え、権限の範囲で注文データの改ざんや削除が行われる可能性がある。
ウ．通信がTLSならデータベースへの影響は発生しない。
エ．攻撃者はデータの閲覧しかできず、更新・削除は絶対にできない。

正答・4肢解説・総合解説

正答：イ．閲覧可能な情報の漏えいに加え、権限の範囲で注文データの改ざんや削除が行われる可能性がある。
ア：SQLインジェクションだけで必ずOS最高権限になるとは限らない。
イ：攻撃による影響は、脆弱なSQLの位置とDB接続アカウントが持つ権限に左右される。
ウ：TLSは通信路を保護するが、アプリが不正SQLをDBへ送れば影響する。
エ：DBアカウントに更新・削除権限があれば、その権限が悪用される可能性がある。
総合解説：脆弱性の根本修正とともに、DB接続権限を業務上必要な範囲に限定することで被害を抑える。

Q007 3-1 Web・アプリケーション攻撃 / SQLインジェクション

利用者が検索結果の並び替え項目を選択できる機能で、ORDER BY句の列名を動的に切り替えたい。安全な実装として最も適切なものはどれか。
ア．利用者が送った列名文字列を無加工でORDER BYの後ろへ連結する。
イ．列名をBase64にしてから無条件でSQLへ連結する。
ウ．利用可能な列名をサーバ側の固定リストへ対応付けし、許可した識別子だけをSQLへ組み込む。
エ．DBアカウントを管理者権限へ変更してエラーを減らす。

正答・4肢解説・総合解説

正答：ウ．利用可能な列名をサーバ側の固定リストへ対応付けし、許可した識別子だけをSQLへ組み込む。
ア：SQL構文へ外部入力を直接混入させ、インジェクションの原因になる。
イ：符号化は信頼性検証にならず、復号後に危険な入力を扱う問題が残る。
ウ：列名など値パラメータとして束縛できない要素は、利用者入力をそのまま使わずallowlistで限定する。
エ：攻撃時の影響を拡大する。
総合解説：「値」はパラメータ化、「SQL構造を変える識別子」は固定対応表やallowlist、という切り分けが重要である。

Q008 3-1 Web・アプリケーション攻撃 / SQLインジェクション

ストアドプロシージャを使っていればSQLインジェクション対策として常に安全だ、という説明の評価として適切なものはどれか。
ア．正しい。ストアドプロシージャは入力内容に関係なくSQL構文を一切実行しない。
イ．正しい。ストアドプロシージャを使うとDB権限が不要になる。
ウ．誤りだが、理由はTLS証明書が利用できなくなるからである。
エ．誤りである。プロシージャ内部で外部入力を連結して動的SQLを生成すれば、SQLインジェクションが生じ得る。

正答・4肢解説・総合解説

正答：エ．誤りである。プロシージャ内部で外部入力を連結して動的SQLを生成すれば、SQLインジェクションが生じ得る。
ア：ストアドプロシージャもSQLを実行し、動的SQLの組立てが不適切なら脆弱になり得る。
イ：実行には適切なDB権限が必要であり、権限管理も重要である。
ウ：TLS証明書の利用可否とは別の問題である。
エ：安全性は「ストアドプロシージャを使うか」だけでなく、内部で値をどのようにSQLへ渡すかで決まる。
総合解説：安全に構築されたストアドプロシージャは対策になり得るが、内部で危険な文字列連結を行わないことが前提である。

Q009 3-1 Web・アプリケーション攻撃 / SQLインジェクション

本番WebサイトがDBMS名、テーブル名、SQL文の一部を含む詳細なエラーを利用者へ返している。改善策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を返し、詳細情報はアクセス制御されたサーバ側ログへ記録する。
イ．詳細エラーを表示しておけばSQLインジェクション自体を防げる。
ウ．SQLインジェクション対策として全てのログを停止する。
エ．エラー画面にDB管理者パスワードを表示して利用者へ対処を依頼する。

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を返し、詳細情報はアクセス制御されたサーバ側ログへ記録する。
ア：詳細エラーは攻撃者の偵察を助ける可能性がある一方、運用者には調査用情報が必要なので表示先を分離する。
イ：情報開示は防御ではなく、攻撃者の手掛かりを増やすことがある。
ウ：調査・監視能力を失うため不適切である。
エ：重大な秘密情報漏えいである。
総合解説：エラー情報の露出を抑えつつ、根本対策であるパラメータ化クエリを実施する。表示抑制だけでは脆弱性は解消しない。

Q010 3-1 Web・アプリケーション攻撃 / SQLインジェクション

既存WebアプリにSQLインジェクション脆弱性が見つかり、WAFを導入した。最も適切な評価はどれか。
ア．WAFを置けば脆弱なSQL文字列連結を永久に修正しなくてよい。
イ．WAFは攻撃パターンの遮断など補助的な防御になり得るが、アプリ側の安全なクエリ実装への修正を代替しない。
ウ．WAFはDBバックアップの世代管理を行う装置なのでSQLインジェクションとは無関係である。
エ．WAFを導入するとDBアカウントは常に管理者権限にすべきである。

正答・4肢解説・総合解説

正答：イ．WAFは攻撃パターンの遮断など補助的な防御になり得るが、アプリ側の安全なクエリ実装への修正を代替しない。
ア：防御装置だけに依存すると回避や設定不備の影響を受ける。
イ：WAFには回避や誤検知の可能性があり、脆弱性の根本原因はコード側に残る。
ウ：WAFはHTTP/HTTPS等のWeb通信を検査し、Web攻撃の緩和に利用される。
エ：最小権限に反する。
総合解説：緊急時の仮想パッチとしてWAFを使う場合でも、コード修正・権限見直し・監視を計画する。

Q011 3-1 Web・アプリケーション攻撃 / SQLインジェクション

ORM（Object-Relational Mapping）を利用しているWebアプリのSQLインジェクション対策について正しい説明はどれか。
ア．ORMを採用した時点でSQLインジェクションは理論上不可能になる。
イ．ORMではデータベースを利用しないためSQLインジェクションと無関係である。
ウ．ORMを使っていても、生SQLやクエリ文字列へ利用者入力を直接連結する機能を使えば脆弱性が生じ得る。
エ．ORMでは入力検証や権限設計を行ってはならない。

正答・4肢解説・総合解説

正答：ウ．ORMを使っていても、生SQLやクエリ文字列へ利用者入力を直接連結する機能を使えば脆弱性が生じ得る。
ア：実装方法によっては危険な動的クエリを作成できる。
イ：ORMはDBアクセスを抽象化する仕組みであり、SQLを利用することが多い。
ウ：ORMは安全なAPI利用を支援するが、危険な機能や誤用まで自動的に排除するとは限らない。
エ：多層防御として入力検証や最小権限は依然重要である。
総合解説：フレームワークやORMの「安全な既定値」を理解し、危険な生クエリAPIを必要最小限にすることが重要である。

Q012 3-1 Web・アプリケーション攻撃 / SQLインジェクション

Webアクセスログに、検索機能へ不自然なSQL構文断片を繰り返し送る試行が記録されている。初動として最も適切なものはどれか。
ア．証跡を残さないため関連ログを直ちに全削除する。
イ．攻撃文字列が見えた時点で必ずDB全件漏えいと断定する。
ウ．利用者入力を全てDB管理者権限で再実行して再現する。
エ．アプリ・WAF・DBログを保全して影響範囲を確認し、脆弱な入力経路の有無を調査した上で、必要に応じて遮断と修正を行う。

正答・4肢解説・総合解説

正答：エ．アプリ・WAF・DBログを保全して影響範囲を確認し、脆弱な入力経路の有無を調査した上で、必要に応じて遮断と修正を行う。
ア：調査に必要な証跡を失い、影響確認が困難になる。
イ：試行と成功は区別し、実際の応答・DB操作等を確認する必要がある。
ウ：本番環境で危険な操作を行うべきではない。
エ：攻撃試行の検知だけで侵害有無は確定しないため、証跡保全と実装確認を並行する。
総合解説：検知後は、試行・成功・影響を区別し、ログとDB変更履歴を用いて事実に基づき判断する。

Q013 3-1 Web・アプリケーション攻撃 / XSS・CSRF

反射型XSS（Reflected XSS）の典型的な特徴はどれか。
ア．リクエストに含まれた不正な入力が応答HTMLへ安全化されず反映され、利用者のブラウザでスクリプトとして実行される。
イ．攻撃コードが必ずデータベースへ永続保存された後、全利用者に配信される。
ウ．認証済み利用者のブラウザに勝手に状態変更リクエストを送らせるだけの攻撃である。
エ．サーバに任意の内部URLへアクセスさせる攻撃である。

正答・4肢解説・総合解説

正答：ア．リクエストに含まれた不正な入力が応答HTMLへ安全化されず反映され、利用者のブラウザでスクリプトとして実行される。
ア：反射型XSSは、入力がその応答へ「反射」されることで成立する。
イ：これは保存型XSSの典型に近い。
ウ：これはCSRFの説明に近い。
エ：これはSSRFの説明である。
総合解説：XSS対策では、出力先の文脈に応じたエンコーディングや安全なDOM API、必要に応じたHTMLサニタイズを用いる。

Q014 3-1 Web・アプリケーション攻撃 / XSS・CSRF

掲示板の投稿本文がサニタイズされずDBに保存され、閲覧した利用者のブラウザで不正スクリプトが実行された。この脆弱性の分類として最も適切なものはどれか。
ア．CSRF
イ．保存型XSS（Stored XSS）
ウ．DNSキャッシュポイズニング
エ．DDoS

正答・4肢解説・総合解説

正答：イ．保存型XSS（Stored XSS）
ア：CSRFは利用者のブラウザに意図しない状態変更要求を送らせる攻撃であり、保存されたスクリプト実行とは異なる。
イ：攻撃文字列がサーバ側に永続保存され、後から複数利用者へ配信されるため保存型XSSに該当する。
ウ：DNS応答の偽装・汚染に関する攻撃である。
エ：大量トラフィック等で可用性を低下させる攻撃である。
総合解説：保存型XSSは多数の閲覧者へ継続的に影響し得るため、入力の性質に応じたサニタイズと出力エンコーディングが重要である。

Q015 3-1 Web・アプリケーション攻撃 / XSS・CSRF

XSS対策として、HTML本文・HTML属性・JavaScript文字列・URLなどで同じエスケープ処理を一律に使う方針の評価として最も適切なものはどれか。
ア．適切である。HTMLエンティティ化だけで全てのJavaScript文脈も安全になる。
イ．不適切だが、理由はTLS通信を使えなくなるからである。
ウ．不適切である。出力先の文脈ごとに必要なエンコーディングや安全なAPIが異なる。
エ．適切である。ブラウザは危険な文字列を常に自動削除する。

正答・4肢解説・総合解説

正答：ウ．不適切である。出力先の文脈ごとに必要なエンコーディングや安全なAPIが異なる。
ア：JavaScript文脈では別の解釈規則があるため、一律処理は危険である。
イ：TLSの利用可否とは別の問題である。
ウ：HTML、属性、JavaScript、URLでは解釈規則が異なるため、文脈に合わないエンコーディングは回避され得る。
エ：ブラウザが全ての不正なデータを安全化してくれるわけではない。
総合解説：XSS対策は「入力を全部削る」より、出力時に文脈を意識して安全な形に変換することが基本である。

Q016 3-1 Web・アプリケーション攻撃 / XSS・CSRF

DOM Based XSSの説明として最も適切なものはどれか。
ア．必ずDBMSのSQL解析器で発生する。
イ．認証済みCookieを自動送信するブラウザ仕様だけで成立する。
ウ．DNSサーバのキャッシュだけを書き換える。
エ．ブラウザ側JavaScriptが信頼できないデータを危険なDOM操作へ渡し、クライアント側で不正スクリプト実行につながる。

正答・4肢解説・総合解説

正答：エ．ブラウザ側JavaScriptが信頼できないデータを危険なDOM操作へ渡し、クライアント側で不正スクリプト実行につながる。
ア：SQL解析器ではなくブラウザ側DOM操作が中心である。
イ：これはCSRFの成立条件に関係する説明である。
ウ：DNS攻撃とは異なる。
エ：サーバ応答が直接悪性スクリプトを生成しなくても、クライアント側のsourceとsinkの組合せで成立し得る。
総合解説：innerHTMLなど危険なsinkへの未検証データ投入を避け、textContent等の安全なAPIや適切なサニタイズを使う。

Q017 3-1 Web・アプリケーション攻撃 / XSS・CSRF

WebサイトにContent Security Policy（CSP）を導入する目的として最も適切なものはどれか。
ア．実行可能なスクリプト等の読み込み元を制約し、XSSが存在した場合の悪用可能性を低減する補助防御として利用する。
イ．SQL文を自動的にパラメータ化する。
ウ．CSRFトークンをサーバ側で自動生成する仕様である。
エ．TLS証明書の失効を確認する仕組みである。

正答・4肢解説・総合解説

正答：ア．実行可能なスクリプト等の読み込み元を制約し、XSSが存在した場合の悪用可能性を低減する補助防御として利用する。
ア：CSPは強力な緩和策だが、出力エンコーディングやサニタイズなど根本対策の代替ではない。
イ：CSPはブラウザ側コンテンツ実行制御であり、SQL生成には作用しない。
ウ：CSPはCSRFトークン機構ではない。
エ：証明書失効確認とは別の仕組みである。
総合解説：XSSの根本修正に加え、CSPを多層防御として用いると、攻撃成功時の影響を抑えられる場合がある。

Q018 3-1 Web・アプリケーション攻撃 / XSS・CSRF

Cookieベースのセッションを使うWebアプリでCSRFが成立する基本的な理由として最も適切なものはどれか。
ア．攻撃者が必ず利用者のCookie値そのものを知っているから。
イ．ブラウザが対象サイトへのリクエストに認証Cookieを自動付与するため、偽造リクエストでも本人の権限で処理され得る。
ウ．DBMSが全てのHTTPリクエストをSQLとして解釈するから。
エ．CSRFはDNSSECを無効化するとだけ発生するから。

正答・4肢解説・総合解説

正答：イ．ブラウザが対象サイトへのリクエストに認証Cookieを自動付与するため、偽造リクエストでも本人の権限で処理され得る。
ア：CSRFではCookie値を直接取得できなくても、ブラウザの自動送信を悪用できる。
イ：サーバ側が「利用者が意図して送った要求か」を検証しなければ、第三者サイトから誘導された要求を区別できないことがある。
ウ：HTTPとSQLは別の処理層である。
エ：DNSSECの有無はCSRF成立条件ではない。
総合解説：状態変更処理ではCSRFトークン、SameSite、Origin/Referer検証等を設計し、GETを状態変更に使わない。

Q019 3-1 Web・アプリケーション攻撃 / XSS・CSRF

送金処理にCSRFトークンを導入する場合の設計として最も適切なものはどれか。
ア．全利用者で固定値「1234」を共有する。
イ．トークンを検証せず、画面に表示するだけにする。
ウ．攻撃者が予測・取得しにくい値を利用者セッション等に結び付け、状態変更リクエストでサーバ側検証する。
エ．状態変更処理を全てGETへ変更しトークンを廃止する。

正答・4肢解説・総合解説

正答：ウ．攻撃者が予測・取得しにくい値を利用者セッション等に結び付け、状態変更リクエストでサーバ側検証する。
ア：推測可能かつ全員共通では攻撃者も容易に付与できる。
イ：サーバ側検証がなければ防御にならない。
ウ：CSRFトークンは、ブラウザが自動送信するCookieだけでは得られない追加の要求真正性を確認するために使う。
エ：GETを状態変更に使うとリンクや外部埋込み等から意図せず実行されるリスクが高まる。
総合解説：フレームワーク標準のCSRF保護がある場合は適切に利用し、独自実装ではトークン生成・保管・検証を慎重に設計する。

Q020 3-1 Web・アプリケーション攻撃 / XSS・CSRF

CookieのSameSite属性を設定したため、他のCSRF対策は一切不要だという判断として最も適切なものはどれか。
ア．正しい。SameSiteを一度設定すればXSSもSQLインジェクションも防げる。
イ．正しい。SameSiteはサーバのDB権限を最小化する機能である。
ウ．誤りだが、SameSiteはWi-Fi暗号方式だからである。
エ．過信すべきではない。SameSiteは有効な防御層だが、アプリの要件やブラウザ挙動を踏まえ、CSRFトークン等と組み合わせる。

正答・4肢解説・総合解説

正答：エ．過信すべきではない。SameSiteは有効な防御層だが、アプリの要件やブラウザ挙動を踏まえ、CSRFトークン等と組み合わせる。
ア：SameSiteはCookie送信制御であり、XSSやSQLiの根本対策ではない。
イ：DB権限とは無関係である。
ウ：SameSiteはHTTP Cookie属性である。
エ：SameSiteはクロスサイトcookie送信を制御するが、全ての利用形態で単独完全防御を保証するものではない。
総合解説：Cookieベース認証では、Secure・HttpOnly・SameSiteの適切な設定に加え、CSRFトークンや再認証等をリスクに応じて組み合わせる。

Q021 3-1 Web・アプリケーション攻撃 / XSS・CSRF

XSSとCSRFの関係について最も適切な説明はどれか。
ア．XSSが成立すると、正規サイトのオリジン内でスクリプトを実行できるため、CSRF対策を迂回される場合がある。
イ．CSRF対策を導入するとXSSの出力エンコーディングは不要になる。
ウ．XSSとCSRFは完全に同一の攻撃で、区別する意味がない。
エ．XSSはネットワーク帯域を枯渇させる攻撃だけを指す。

正答・4肢解説・総合解説

正答：ア．XSSが成立すると、正規サイトのオリジン内でスクリプトを実行できるため、CSRF対策を迂回される場合がある。
ア：CSRFトークンがあっても、XSSで正規ページ上のトークンや処理を悪用される可能性があるため、両方の脆弱性を防ぐ必要がある。
イ：CSRF対策はXSSの根本原因を解消しない。
ウ：成立条件・攻撃経路・主な対策が異なる。
エ：それはDoS/DDoSの説明に近い。
総合解説：XSSは「ブラウザ内でコードを実行させる」、CSRFは「利用者の認証状態を利用して意図しない要求を送らせる」という違いを押さえる。

Q022 3-1 Web・アプリケーション攻撃 / XSS・CSRF

Cookie認証されたWeb APIが、Content-TypeやOriginを確認せず外部サイトからの単純なフォームPOSTでも口座設定を変更できる。改善策として最も適切なものはどれか。
ア．外部サイトからのPOSTも全て正規利用者の意思とみなし許可する。
イ．状態変更要求にCSRF保護を適用し、必要に応じてCSRFトークンやOrigin検証、SameSite設定を組み合わせる。
ウ．APIのレスポンス本文をBase64に変える。
エ．DBを読み取り専用にして全ての業務更新を停止する。

正答・4肢解説・総合解説

正答：イ．状態変更要求にCSRF保護を適用し、必要に応じてCSRFトークンやOrigin検証、SameSite設定を組み合わせる。
ア：攻撃者が利用者のブラウザを介して状態変更を起こせる。
イ：Cookieが自動送信される設計では、クロスサイトからの偽造要求をサーバ側で拒否する仕組みが必要である。
ウ：レスポンス表現の符号化はCSRF対策にならない。
エ：業務要件を失う過剰対応で、適切なCSRF防御ではない。
総合解説：CSRFの対策設計は、認証情報がどのように送信されるかと、状態変更リクエストをどう識別するかを基準に考える。

Q023 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

SSRF（Server-Side Request Forgery）の説明として最も適切なものはどれか。
ア．利用者のブラウザだけでHTMLを改ざんしてスクリプトを実行する攻撃である。
イ．大量端末から帯域を枯渇させる攻撃だけを指す。
ウ．利用者が指定したURLなどをサーバが取得する機能を悪用し、サーバから内部ネットワークや想定外の宛先へリクエストを送らせる攻撃である。
エ．DBへSQL構文を混入させる攻撃である。

正答・4肢解説・総合解説

正答：ウ．利用者が指定したURLなどをサーバが取得する機能を悪用し、サーバから内部ネットワークや想定外の宛先へリクエストを送らせる攻撃である。
ア：これはXSSの説明に近い。
イ：これはDDoSの説明である。
ウ：SSRFでは攻撃者自身から直接到達できない内部サービスへ、脆弱なサーバを中継点としてアクセスさせることがある。
エ：これはSQLインジェクションである。
総合解説：画像取得、Webhook、URLプレビュー等の「サーバが外部URLへアクセスする機能」はSSRFの入口になり得るため、宛先制御とネットワーク分離が重要である。

Q024 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

業務上、Webhook送信先が社内の3つの固定サービスに限定されている。SSRF対策として最も適切なものはどれか。
ア．利用者が入力した任意URLへ接続し、失敗した時だけ警告する。
イ．URL文字列に「http」が含まれていれば全て安全と判断する。
ウ．DNS解決結果を確認せず、利用者入力をOSコマンドへ連結する。
エ．送信先のホスト名やIP、必要なプロトコルをサーバ側allowlistで限定し、検証後の宛先だけへ接続する。

正答・4肢解説・総合解説

正答：エ．送信先のホスト名やIP、必要なプロトコルをサーバ側allowlistで限定し、検証後の宛先だけへ接続する。
ア：内部サービスや不正宛先への接続を許してしまう。
イ：スキームだけでは宛先の安全性を確認できない。
ウ：SSRFに加えて別のインジェクションリスクを招く。
エ：接続先が事前に限定できる場合は、allowlistによる明示的許可が強い対策になる。
総合解説：SSRF対策は、アプリ層の宛先検証だけでなく、ファイアウォール等でサーバから不要な内部・外部宛先へ到達できないようにする多層防御が有効である。

Q025 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

SSRF対策として最初のURLだけallowlist確認し、その後のHTTPリダイレクト先は無条件で追従する実装の評価として適切なものはどれか。
ア．危険である。許可済みURLから攻撃者が制御する別宛先へ転送され、検証を迂回される可能性がある。
イ．安全である。最初のURLが許可されていれば後続宛先は常に安全である。
ウ．危険だが、理由はSQL文が自動的に実行されるからである。
エ．安全である。HTTP 3xx応答はブラウザだけが処理しサーバHTTPクライアントは扱えない。

正答・4肢解説・総合解説

正答：ア．危険である。許可済みURLから攻撃者が制御する別宛先へ転送され、検証を迂回される可能性がある。
ア：OWASPはSSRF対策で、リダイレクト追従の制御を重要な論点としている。
イ：リダイレクト先は元URLと異なるため、再検証なしでは安全を保証できない。
ウ：主な問題は接続先検証の迂回でありSQLとは直接関係しない。
エ：多くのHTTPクライアントは設定によりリダイレクトを追従できる。
総合解説：URL検証では、初回入力だけでなく解決後IP、IPv4/IPv6、リダイレクト後宛先なども脅威モデルに含める。

Q026 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

ログイン画面が「このメールアドレスは登録されていません」と「パスワードが違います」を明確に分けて表示している。主なリスクはどれか。
ア．SQLインジェクションを必ず防止できる。
イ．攻撃者が有効なアカウント名を列挙しやすくなり、パスワード攻撃やフィッシングの対象選定に利用される。
ウ．利用者のCookieが自動的に暗号化される。
エ．DDoS攻撃の帯域を必ず増加させる。

正答・4肢解説・総合解説

正答：イ．攻撃者が有効なアカウント名を列挙しやすくなり、パスワード攻撃やフィッシングの対象選定に利用される。
ア：エラーメッセージの設計はSQLi防止とは別である。
イ：認証エラーの差異はアカウント存在確認の手掛かりになり得る。
ウ：認証エラー表示はCookie暗号化機能ではない。
エ：主な論点はアカウント列挙である。
総合解説：外部向け応答は必要以上にアカウント存在を示さず、内部ログでは運用に必要な詳細を保持するという分離が有効である。

Q027 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

パスワードスプレー攻撃の特徴として最も適切なものはどれか。
ア．一つのアカウントに対して非常に多数のパスワード候補を連続試行することだけを指す。
イ．DNS応答を書き換えて偽サイトへ誘導する攻撃である。
ウ．少数のよく使われるパスワード候補を、多数の異なるアカウントに対して試す。
エ．サーバへ任意URLを取得させる攻撃である。

正答・4肢解説・総合解説

正答：ウ．少数のよく使われるパスワード候補を、多数の異なるアカウントに対して試す。
ア：これは典型的なオンラインブルートフォースの説明に近い。
イ：DNS攻撃とは異なる。
ウ：一つのアカウントへ大量候補を試す方式よりロックアウト閾値を回避しやすい場合がある。
エ：SSRFの説明である。
総合解説：対策にはMFA、侵害済みパスワードの利用抑止、レート制御、異常な分散ログイン試行の監視などがある。

Q028 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

セッション固定攻撃（Session Fixation）の説明として最も適切なものはどれか。
ア．多数の端末から同時に大量通信を送り帯域を枯渇させる。
イ．データベースのSQL文へ入力を混入する。
ウ．無線APと同じSSIDを名乗るだけで必ず成立する。
エ．攻撃者が知っているセッションIDを被害者に使用させ、被害者のログイン後も同じIDが有効なままなら、その認証済みセッションを悪用する。

正答・4肢解説・総合解説

正答：エ．攻撃者が知っているセッションIDを被害者に使用させ、被害者のログイン後も同じIDが有効なままなら、その認証済みセッションを悪用する。
ア：これはDDoSである。
イ：これはSQLインジェクションである。
ウ：Evil Twin等の無線攻撃とは別である。
エ：ログイン等の権限変化時にセッションIDを再生成しない実装が主な危険要因になる。
総合解説：認証前後でセッションIDを更新し、サーバが発行していないIDを受理しないことが固定化対策の重要点である。

Q029 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

WebアプリのセッションCookieがJavaScriptから読み取り可能で、HTTPSでもSecure属性が設定されていない。改善策として最も適切なものはどれか。
ア．HTTPSを前提にSecure属性を付け、不要なJavaScript参照を防ぐHttpOnly属性を設定し、セッションIDの漏えい経路を減らす。
イ．セッションIDをURLへ常時埋め込み、リンクで共有する。
ウ．全利用者で同じ固定セッションIDを使う。
エ．セッションCookieの有効期限を永久にする。

正答・4肢解説・総合解説

正答：ア．HTTPSを前提にSecure属性を付け、不要なJavaScript参照を防ぐHttpOnly属性を設定し、セッションIDの漏えい経路を減らす。
ア：Cookie属性だけで全ての攻撃を防げるわけではないが、盗難や誤送信のリスクを下げる基本策である。
イ：ログやReferer等へ漏えいしやすくなる。
ウ：一人のID漏えいが全員へ波及し、識別もできない。
エ：盗難時の悪用可能期間を長くする。
総合解説：セッションIDは認証情報に相当するため、十分な予測困難性、Secure/HttpOnly/SameSite、タイムアウト、ログアウト時失効などを組み合わせる。

Q030 3-1 Web・アプリケーション攻撃 / SSRF・認証・セッション攻撃

利用者がログイン済みであっても、パスワード変更や送金先追加など高リスク操作の直前に再認証を求める主な目的はどれか。
ア．SQLインジェクションを防ぐためにSQL構文を再認証する。
イ．盗まれた・放置されたセッションだけで重要操作を実行されるリスクを低減する。
ウ．DNSSECの署名鍵を更新するため。
エ．WebサーバのCPU利用率を下げるため。

正答・4肢解説・総合解説

正答：イ．盗まれた・放置されたセッションだけで重要操作を実行されるリスクを低減する。
ア：再認証は利用者本人性の再確認でありSQLi対策ではない。
イ：認証済みセッションが常に本人操作であるとは限らないため、重要イベントでは認証の鮮度を高める。
ウ：DNSSEC鍵管理とは無関係である。
エ：主目的は重要操作の不正利用抑止である。
総合解説：再認証やステップアップ認証は、認証状態の乗っ取りを前提にした防御として、特に機密操作で有効である。

Q031 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

DoS攻撃とDDoS攻撃の一般的な違いとして最も適切なものはどれか。
ア．DoSは必ず暗号化通信を使い、DDoSは暗号化を使わない。
イ．DDoSはデータの機密性だけを狙い、可用性には影響しない。
ウ．DDoSは複数の分散した送信元から同時に攻撃を行うため、単一送信元のDoSより送信元遮断だけでの対処が難しい場合が多い。
エ．DoSはWebだけ、DDoSはDNSだけを対象とする。

正答・4肢解説・総合解説

正答：ウ．DDoSは複数の分散した送信元から同時に攻撃を行うため、単一送信元のDoSより送信元遮断だけでの対処が難しい場合が多い。
ア：暗号化の有無はDoS/DDoSの分類条件ではない。
イ：DoS/DDoSの主目的はサービス可用性の低下である。
ウ：DDoSではボットネット等の多数端末が使われ、帯域や処理資源を集中的に消費させる。
エ：対象プロトコルやサービスは限定されない。
総合解説：DoS/DDoSは可用性を狙う攻撃であり、帯域、ネットワーク機器、OS、アプリケーションなど複数層の資源が標的になり得る。

Q032 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

ボリューム型DDoS攻撃の主な狙いとして最も適切なものはどれか。
ア．利用者のブラウザへJavaScriptを保存する。
イ．DBのSQL構文へ入力を混入する。
ウ．証明書の秘密鍵を必ず解読する。
エ．大量のトラフィックでインターネット回線や上流ネットワークの帯域を飽和させ、正規通信を通しにくくする。

正答・4肢解説・総合解説

正答：エ．大量のトラフィックでインターネット回線や上流ネットワークの帯域を飽和させ、正規通信を通しにくくする。
ア：XSSの説明である。
イ：SQLインジェクションの説明である。
ウ：DDoSの主目的ではない。
エ：サーバ処理能力より前段の回線容量がボトルネックになる場合がある。
総合解説：ボリューム型への対処では、上流ISPやDDoS緩和サービス、CDN/Anycast等と連携し、組織回線へ到達する前に吸収・除去することが重要になる。

Q033 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

反射型DDoS攻撃の説明として最も適切なものはどれか。
ア．攻撃者が送信元IPを被害者のIPに詐称して第三者サーバへ要求を送り、その応答を被害者へ集中させる。
イ．被害者端末の画面を鏡像表示して操作を妨害する攻撃である。
ウ．Webサーバに内部URLへ接続させる攻撃である。
エ．利用者の認証Cookieを固定する攻撃である。

正答・4肢解説・総合解説

正答：ア．攻撃者が送信元IPを被害者のIPに詐称して第三者サーバへ要求を送り、その応答を被害者へ集中させる。
ア：第三者の公開サービスが「反射器」として利用され、攻撃者自身のアドレスを隠しながら応答を被害者へ向ける。
イ：ネットワーク上の反射とは意味が異なる。
ウ：これはSSRFである。
エ：これはセッション固定化に関係する。
総合解説：反射型DDoSを成立させにくくするには、送信元アドレス詐称を抑えるネットワーク対策や、不必要に公開された反射可能サービスの制限が重要である。

Q034 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

増幅型DDoSで「増幅」が意味するものとして最も適切なものはどれか。
ア．攻撃者のCPUクロックを物理的に高くする。
イ．攻撃者が送る比較的小さな要求に対して、第三者サービスからより大きな応答を被害者へ送らせ、攻撃トラフィック量を増やす。
ウ．パスワード文字数を増やして認証を突破する。
エ．暗号鍵を長くして復号を高速化する。

正答・4肢解説・総合解説

正答：イ．攻撃者が送る比較的小さな要求に対して、第三者サービスからより大きな応答を被害者へ送らせ、攻撃トラフィック量を増やす。
ア：増幅の意味はネットワーク応答量の拡大である。
イ：要求と応答のサイズ差を悪用して、攻撃者側の送信量より大きな負荷を被害者側へ生じさせる。
ウ：認証攻撃とは異なる。
エ：暗号鍵長とは無関係である。
総合解説：DNS等のUDPサービスが反射・増幅に悪用されることがあるため、不要な公開やオープンリゾルバを避けることが重要である。

Q035　3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

TCP接続要求が大量に到達し、サーバが多数の半開き接続状態を保持して新規接続を受けにくくなった。想定される攻撃として最も適切なものはどれか。
ア．保存型XSS
イ．SQLインジェクション
ウ．SYN flood
エ．セッション固定

正答・4肢解説・総合解説

正答：ウ．SYN flood
ア：ブラウザでのスクリプト実行を狙う攻撃であり、TCP半開き接続とは異なる。
イ：DBへの不正SQL実行を狙う攻撃である。
ウ：TCPの接続確立処理を大量に発生させ、接続状態管理資源を消費させる代表的なDoS手法である。
エ：Webセッション IDの扱いを悪用する攻撃である。
総合解説：SYN cookie等のOS・ネットワーク機能、レート制御、上流緩和を組み合わせる。攻撃規模が回線容量を超える場合はサーバ単体対策だけでは不十分である。

Q036　3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

Webサーバへの通信量自体は極端に大きくないが、検索・帳票生成などCPU負荷の高いURLへ大量の正規形式HTTPリクエストが送られ、処理能力が枯渇している。最も適切な分類はどれか。
ア．DNSキャッシュポイズニング
イ．ARPスプーフィング
ウ．保存型XSS
エ．アプリケーション層DoS/DDoS

正答・4肢解説・総合解説

正答：エ．アプリケーション層DoS/DDoS
ア：DNS応答の信頼性を悪用する攻撃であり、Web処理資源枯渇とは異なる。
イ：同一ネットワーク内のARP対応付けを偽装する攻撃である。
ウ：閲覧者ブラウザ上のスクリプト実行を狙う。
エ：帯域ではなく、アプリケーションの高コスト処理やバックエンド資源を狙って枯渇させる攻撃である。
総合解説：HTTPが正規形式でも攻撃になり得るため、リクエスト単価、利用者・IP・セッション単位のレート、キャッシュ、WAF/CDN等を組み合わせて対処する。

Q037 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

大規模DDoSに対して「送信元IPを1件ずつ手作業でFWに追加すれば十分」という方針の評価として最も適切なものはどれか。
ア．不十分になりやすい。送信元が多数・変動・詐称される場合があり、上流での緩和や自動化されたレート制御等が必要になる。
イ．十分である。DDoSの送信元は必ず1台だけだから。
ウ．不十分だが、理由はFWがIPアドレスを扱えないから。
エ．十分である。送信元IPは攻撃中に絶対変化しない。

正答・4肢解説・総合解説

正答：ア．不十分になりやすい。送信元が多数・変動・詐称される場合があり、上流での緩和や自動化されたレート制御等が必要になる。
ア：DDoSでは分散性のため個別IPブロックが追いつかない場合がある。
イ：DDoSは複数の分散送信元を用いる攻撃である。
ウ：FWはIPアドレスを条件に制御できるが、規模・変動への追随が課題になる。
エ：ボットネットや詐称等により変動し得る。
総合解説：防御は攻撃規模とボトルネック位置に合わせて行う。回線飽和型では、組織境界より上流でのスクラビングが必要になる。

Q038 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

ログインAPIへの大量リクエストでアプリケーションが高負荷になっている。レート制限を導入する際の説明として最も適切なものはどれか。
ア．レート制限を1件設定すればどんな規模の回線飽和攻撃も必ず防げる。
イ．単位時間当たりの要求数を利用者・IP・トークン等で制御し負荷を抑えられるが、分散送信元や正規利用集中との区別も考慮する必要がある。
ウ．レート制限は通信を暗号化するための仕組みである。
エ．正規利用者には負荷が一切ないため閾値設計は不要である。

正答・4肢解説・総合解説

正答：イ．単位時間当たりの要求数を利用者・IP・トークン等で制御し負荷を抑えられるが、分散送信元や正規利用集中との区別も考慮する必要がある。
ア：回線到達前に帯域が飽和する攻撃にはサーバ側レート制限が間に合わない。
イ：レート制限は有効な一層だが、DDoSでは一つのキーだけに依存すると回避や誤遮断が起きる。
ウ：主目的は要求頻度の制御である。
エ：閾値が厳しすぎると正規利用を妨げる。
総合解説：レート制限は、WAF/CDN、キャッシュ、キュー制御、上流緩和等と組み合わせて防御する。

Q039 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

CDNやAnycast構成がDDoS耐性向上に役立つ理由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全て同一にするため。
イ．SQL文を自動的に安全化するため。
ウ．トラフィックを複数拠点へ分散・吸収し、オリジンサーバへ直接集中する負荷を軽減できるため。
エ．DNSSECを無効化して応答を高速化するため。

正答・4肢解説・総合解説

正答：ウ．トラフィックを複数拠点へ分散・吸収し、オリジンサーバへ直接集中する負荷を軽減できるため。
ア：認証設定とは関係しない。
イ：SQLインジェクションの根本修正にはならない。
ウ：広域の配信・緩和基盤へ負荷を分散することで、単一拠点の処理能力や回線だけに依存しにくくなる。
エ：DNSSEC無効化がDDoS対策の原理ではない。
総合解説：オリジンIPの直接露出を避け、CDN経由以外の到達を制限する等、アーキテクチャ全体で設計する必要がある。

Q040 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

クラウド環境のDDoS対策を「オートスケールだけ」に依存する方針として最も適切な評価はどれか。
ア．完全である。オートスケールを使えばDDoSで費用は一切増えない。
イ．危険なのは、オートスケールするとTLSが使えなくなるからである。
ウ．完全である。DBや外部APIも必ず無限にスケールする。
エ．負荷吸収には役立つ場合があるが、攻撃トラフィックに合わせて資源・費用が増大するため、上流緩和やレート制御等も必要である。

正答・4肢解説・総合解説

正答：エ．負荷吸収には役立つ場合があるが、攻撃トラフィックに合わせて資源・費用が増大するため、上流緩和やレート制御等も必要である。
ア：従量課金環境では攻撃負荷が費用増大につながる場合がある。
イ：TLS利用可否とは別の問題である。
ウ：各構成要素には容量・制約がある。
エ：可用性だけでなく、コスト枯渇やバックエンドの非スケール資源も考慮する。
総合解説：DDoS対策は容量拡張、攻撃識別、緩和、コスト制御、復旧手順をセットで考える。

Q041 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

DDoSの早期検知のため、平常時のネットワーク・アプリ指標を収集する主な目的はどれか。
ア．通常のトラフィック量、接続数、要求率、エラー率等からの異常な逸脱を把握しやすくするため。
イ．平常値を記録すると攻撃トラフィックが自動的に暗号化されるため。
ウ．ログを保存しないで済むため。
エ．全ての負荷上昇を攻撃と断定するため。

正答・4肢解説・総合解説

正答：ア．通常のトラフィック量、接続数、要求率、エラー率等からの異常な逸脱を把握しやすくするため。
ア：攻撃判定には単なる絶対値だけでなく、そのサービスの通常パターンを知ることが重要である。
イ：ベースラインは暗号化機能ではない。
ウ：検知・事後分析にはログやメトリクスが必要である。
エ：正規イベントや障害による増加もあるため、追加分析が必要である。
総合解説：帯域だけでなく、SYN/ACK比率、HTTPステータス、特定URL集中、国・ASN分布等の複数指標を相関すると判断精度が上がる。

Q042 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

攻撃トラフィックで自社インターネット回線が飽和し、境界FWへ到達する前から正規通信が失われている。最優先で検討すべき対処はどれか。
ア．社内PCのスクリーンセーバー時間を短くする。
イ．ISPやDDoS緩和事業者と連携し、上流側で攻撃トラフィックを除去・迂回させる。
ウ．DBのSELECT権限を増やす。
エ．利用者ブラウザのCookieを削除する。

正答・4肢解説・総合解説

正答：イ．ISPやDDoS緩和事業者と連携し、上流側で攻撃トラフィックを除去・迂回させる。
ア：回線飽和には効果がない。
イ：自社回線自体が飽和している場合、回線の内側にあるFWで遮断しても正規通信を回線へ戻せない。
ウ：DDoS緩和とは無関係である。
エ：回線レベルの攻撃を止められない。
総合解説：DDoS対応計画には、事前の連絡先、緩和サービス切替手順、BGP/DNS変更、証跡保全を含めておく。

Q043 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

DDoS緊急対応で対象IPへの通信をブラックホールルーティングする場合の説明として最も適切なものはどれか。
ア．対象サービスの可用性を必ず向上させ、正規利用者だけを通す。
イ．SQLインジェクションを自動修正する。
ウ．攻撃トラフィックを捨てて他サービスへの波及を抑えられる一方、対象IPへの正規通信も到達しなくなる。
エ．DNSキャッシュを暗号化する方式である。

正答・4肢解説・総合解説

正答：ウ．攻撃トラフィックを捨てて他サービスへの波及を抑えられる一方、対象IPへの正規通信も到達しなくなる。
ア：通常のブラックホールでは対象宛通信をまとめて破棄する。
イ：ルーティング制御とSQL脆弱性は別である。
ウ：サービスを一時的に犠牲にしてネットワーク全体を守る最終的な緩和策の一つである。
エ：DNS暗号化方式ではない。
総合解説：RTBH等は被害拡大を止める選択肢だが、業務影響が大きいため、より選択的なスクラビング等と優先順位を決めておく。

Q044 3-2 ネットワーク・インフラ攻撃 / DDoS・DoS

DDoSが収束した後に行う事後対応として最も適切なものはどれか。
ア．攻撃時ログを全て削除し、記録を残さない。
イ．今後の対策として全サービスを永久停止する。
ウ．攻撃元IPが一つでも見つかれば、他のデータは調べない。
エ．ピークトラフィック、攻撃ベクトル、緩和開始までの時間、誤遮断、サービス影響を分析し、閾値・連絡手順・容量計画を改善する。

正答・4肢解説・総合解説

正答：エ．ピークトラフィック、攻撃ベクトル、緩和開始までの時間、誤遮断、サービス影響を分析し、閾値・連絡手順・容量計画を改善する。
ア：再発防止や原因分析に必要な証跡を失う。
イ：業務継続を損なう過剰対応である。
ウ：DDoSは複数ベクトル・送信元を使うことがあり、全体分析が必要である。
エ：復旧だけで終了せず、事実に基づいて防御と運用を改善することが再発時の対応速度を高める。
総合解説：DDoS対応能力は技術設備だけでなく、連絡系統、ベンダ連携、演習、サービス優先順位の設計で大きく変わる。

Q045 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

中間者攻撃（MITM）の説明として最も適切なものはどれか。
ア．通信当事者の間に攻撃者が介在し、通信を盗聴・改ざん・なりすましながら双方には正規相手と通信しているように見せる攻撃である。
イ．多数端末から大量トラフィックを送り可用性だけを低下させる攻撃。
ウ．SQL文へ利用者入力を混入する攻撃。
エ．ファイルを暗号化して身代金を要求する攻撃。

正答・4肢解説・総合解説

正答：ア．通信当事者の間に攻撃者が介在し、通信を盗聴・改ざん・なりすましながら双方には正規相手と通信しているように見せる攻撃である。
ア：MITMでは通信路上の位置を悪用し、機密性・完全性・真正性を損なう可能性がある。
イ：これはDDoSの説明である。
ウ：これはSQLインジェクションである。
エ：ランサムウェアの説明である。
総合解説：TLS等を使う際も、証明書検証やホスト名検証を無視するとMITMを許す可能性がある。

Q046 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

利用者が公衆Wi-Fi上でHTTPSサイトへ接続した際、ブラウザが証明書不一致を警告したが無視して接続を続けた。最も懸念すべきことはどれか。
ア．SQLインジェクションが必ず発生する。
イ．偽の証明書や別ホストの証明書を使った中間者へ接続し、通信を盗聴・改ざんされる可能性がある。
ウ．公衆Wi-FiではHTTPSを使うと必ずDDoSになる。
エ．証明書警告は通信速度だけに関する通知で、セキュリティ上の意味はない。

正答・4肢解説・総合解説

正答：イ．偽の証明書や別ホストの証明書を使った中間者へ接続し、通信を盗聴・改ざんされる可能性がある。
ア：証明書警告とSQLiは直接の因果関係がない。
イ：TLSの安全性は暗号化だけでなく、相手が正しいサーバであることの検証にも依存する。
ウ：HTTPS利用自体がDDoSを引き起こすわけではない。
エ：証明書検証エラーは相手認証の失敗を示す重要な警告である。
総合解説：証明書チェーン、期限、ホスト名等の検証を正しく行い、検証エラーを安易に無効化しない。

Q047 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

ARPスプーフィング（ARP poisoning）の説明として最も適切なものはどれか。
ア．DNSのMXレコードを使ってメール本文を暗号化する。
イ．サーバのSQLクエリを文字列連結する。
ウ．同一LAN上で偽のARP情報を送信し、他端末にIPアドレスと攻撃者MACアドレスの誤った対応を学習させる。
エ．ブラウザCookieのSameSite属性を書き換える攻撃である。

正答・4肢解説・総合解説

正答：ウ．同一LAN上で偽のARP情報を送信し、他端末にIPアドレスと攻撃者MACアドレスの誤った対応を学習させる。
ア：ARPとは無関係である。
イ：SQLインジェクションの原因である。
ウ：攻撃者をゲートウェイ等として誤認させれば、通信の中継・盗聴・妨害につながり得る。
エ：HTTP Cookieとは別層の攻撃である。
総合解説：ARPには強い認証機構がないため、スイッチ側の動的ARP検査やポートセキュリティ、暗号化通信などの多層対策が用いられる。

Q048 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

同一セグメント内で「デフォルトゲートウェイIPに対応するMACアドレスが短時間に変化する」事象が観測された。優先して疑うべきものはどれか。
ア．保存型XSS
イ．SQLインジェクション
ウ．CSRF
エ．ARPスプーフィングや不正なL2機器によるARP情報の改ざん。

正答・4肢解説・総合解説

正答：エ．ARPスプーフィングや不正なL2機器によるARP情報の改ざん。
ア：ブラウザ上のスクリプト実行でありARP表の変動とは直接関係しない。
イ：DBクエリへの入力混入でありL2アドレス対応とは異なる。
ウ：認証Cookieを利用した偽造HTTP要求である。
エ：ゲートウェイのIP-MAC対応が不自然に変動するのはARP poisoningの兆候になり得る。
総合解説：正規の冗長化や機器交換でもMACが変わる場合があるため、スイッチログ・ARP表・機器構成と照合して判断する。

Q049 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

DNSキャッシュポイズニングによる代表的な影響はどれか。
ア．再帰DNSのキャッシュに偽の名前解決情報を混入させ、利用者を攻撃者が用意したIPアドレスへ誘導する。
イ．利用者端末のファイルを必ず暗号化して身代金を要求する。
ウ．DBMSへ不正なSQLを送る。
エ．CPUを過熱させる物理攻撃だけを指す。

正答・4肢解説・総合解説

正答：ア．再帰DNSのキャッシュに偽の名前解決情報を混入させ、利用者を攻撃者が用意したIPアドレスへ誘導する。
ア：利用者が正しいドメイン名を入力しても誤ったIPへ接続させられる可能性がある。
イ：ランサムウェアの説明である。
ウ：SQLインジェクションである。
エ：DNSの名前解決情報を狙う攻撃である。
総合解説：DNSSECはDNSデータの真正性・完全性を検証し、偽応答を受理しにくくするための重要な対策である。

Q050 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

DNSSECがDNSキャッシュポイズニング対策として有効な理由はどれか。
ア．DNS問い合わせを必ず匿名化し、接続先リゾルバにも内容を見えなくするため。
イ．DNSデータへ暗号学的署名を付け、検証側が信頼連鎖を確認することで改ざん・偽造された応答を検出しやすくするため。
ウ．全DDoSトラフィックを自動的に遮断するため。
エ．ARP表を暗号化するため。

正答・4肢解説・総合解説

正答：イ．DNSデータへ暗号学的署名を付け、検証側が信頼連鎖を確認することで改ざん・偽造された応答を検出しやすくするため。
ア：問い合わせの機密性はDoH/DoT等の別技術の主な役割である。
イ：DNSSECは応答のデータ起源認証と完全性を提供する。
ウ：DNSSECだけで可用性攻撃を防ぐことはできない。
エ：DNSSECはARPには作用しない。
総合解説：DNSSECと暗号化DNSは目的が異なる。前者は応答データの真正性・完全性、後者は主にクライアントとリゾルバ間の通信保護を担う。

Q051 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

利用者のルータ設定が改ざんされ、正規とは異なる攻撃者管理のDNSリゾルバを使わされていた。この事象の説明として最も適切なものはどれか。
ア．SQLインジェクションによりDBのORDER BY句だけが改ざんされた。
イ．CSRFトークンが不足しているだけで必ず発生する。
ウ．DNS設定のハイジャックにより、名前解決そのものを攻撃者のリゾルバへ誘導されている。
エ．TLS 1.3の仕様として正しい動作である。

正答・4肢解説・総合解説

正答：ウ．DNS設定のハイジャックにより、名前解決そのものを攻撃者のリゾルバへ誘導されている。
ア：DNS設定とは関係しない。
イ：ルータ管理画面への攻撃経路としてCSRF等が使われる可能性はあるが、事象の分類はDNS設定ハイジャックである。
ウ：キャッシュの一部レコードだけを汚染する場合とは異なり、利用するリゾルバ設定自体が変更されている。
エ：正規DNS設定が不正に変更されるのは正常動作ではない。
総合解説：ルータ管理認証、ファームウェア更新、設定変更監視、信頼できるDNSリゾルバの利用などを組み合わせる。

Q052 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

組織の端末が既知の悪性ドメインへ名前解決しようとした際に、組織のDNSサービスで遮断・監視したい。この目的に合う考え方はどれか。
ア．全てのDNSSEC検証を無効化する。
イ．端末のARPキャッシュを永久固定し、DNSを使わない。
ウ．メールのDKIM署名を削除する。
エ．Protective DNSを用いて、脅威情報やポリシーに基づき悪性・疑わしいドメインへの解決を制御する。

正答・4肢解説・総合解説

正答：エ．Protective DNSを用いて、脅威情報やポリシーに基づき悪性・疑わしいドメインへの解決を制御する。
ア：真正性検証を弱めるため不適切である。
イ：実用性と可用性を損ない、Protective DNSの代替ではない。
ウ：メール認証を弱めるだけである。
エ：DNSは多くの通信の前段にあるため、悪性宛先への接続を早期に抑止する防御点として利用できる。
総合解説：Protective DNSは悪性通信を抑止する一層であり、端末防御、ネットワーク監視、アクセス制御等と組み合わせる。

Q053 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

端末が組織管理外の外部DoHリゾルバを自由に利用できる状態のセキュリティ上の論点として最も適切なものはどれか。
ア．盗聴耐性は高まる一方、組織のDNSポリシー・悪性ドメイン遮断・ログ監視を迂回される可能性がある。
イ．DoHを使うとDNS応答の署名検証が必ず無効になる。
ウ．DoHを使うとSQLインジェクションが自動的に防止される。
エ．DoHは無線LANの電波暗号化方式である。

正答・4肢解説・総合解説

正答：ア．盗聴耐性は高まる一方、組織のDNSポリシー・悪性ドメイン遮断・ログ監視を迂回される可能性がある。
ア：暗号化DNSは通信の機密性を向上させるが、どのリゾルバを信頼し管理するかという運用設計が必要である。
イ：DoHとDNSSECは独立して併用できる。
ウ：WebアプリのSQL実装とは無関係である。
エ：DoHはHTTPS上でDNSを運ぶ仕組みである。
総合解説：組織では信頼できる暗号化DNSリゾルバを指定し、エンドポイントポリシーやネットワーク制御と整合させることが重要である。

Q054 3-2 ネットワーク・インフラ攻撃 / MITM・ARP・DNS攻撃

社内LANでARPスプーフィングによるMITMを懸念している。対策の組合せとして最も適切なものはどれか。
ア．TLSを廃止し、全通信を平文にする。
イ．スイッチ側のL2保護機能を有効化し、重要通信はTLS等で相手認証と暗号化を行い、不自然なARP変化も監視する。
ウ．全端末へ同じ管理者パスワードを設定する。
エ．ARPログを全て削除して検知を避ける。

正答・4肢解説・総合解説

正答：イ．スイッチ側のL2保護機能を有効化し、重要通信はTLS等で相手認証と暗号化を行い、不自然なARP変化も監視する。
ア：盗聴・改ざんの影響を大きくする。
イ：一つの層が突破されても通信内容や相手認証を守れるよう、多層防御を構成する。
ウ：認証侵害時の影響を拡大する。
エ：攻撃兆候の把握を困難にする。
総合解説：L2で完全に防げない場合でも、TLS等のエンドツーエンド保護を正しく検証すればMITMによる内容の盗聴・改ざんを抑えられる。

Q055 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

無線LANにおけるEvil Twin攻撃の説明として最も適切なものはどれか。
ア．DNSサーバのキャッシュへ偽レコードを混入する攻撃。
イ．Webサーバに内部URLへ接続させる攻撃。
ウ．正規アクセスポイントと同じ又は紛らわしいSSIDを持つ偽アクセスポイントを設置し、利用者を誤接続させて通信を盗聴・誘導する。
エ．DBのSQL文へ入力を混入する攻撃。

正答・4肢解説・総合解説

正答：ウ．正規アクセスポイントと同じ又は紛らわしいSSIDを持つ偽アクセスポイントを設置し、利用者を誤接続させて通信を盗聴・誘導する。
ア：DNSキャッシュポイズニングの説明である。
イ：SSRFの説明である。
ウ：利用者がSSID名だけで接続先を判断すると、攻撃者のAPへ接続してしまう可能性がある。
エ：SQLインジェクションである。
総合解説：企業WLANでは強固な認証方式、サーバ証明書検証、不要な自動接続の抑止、不正AP監視等を組み合わせる。

Q056 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

従業員が私物の無線ルータを社内LANへ無断接続し、弱い設定のWi-Fiを提供している。主な問題と対策として最も適切なものはどれか。
ア．問題はない。社内LANに接続されていれば自動的に企業セキュリティ設定になる。
イ．対策は全てのメールへDKIM署名を付けるだけでよい。
ウ．対策はDBのSELECT権限を追加することである。
エ．管理外の接続経路が生まれて境界防御を迂回されるため、不正APの検出・接続制御・設置禁止方針を運用する。

正答・4肢解説・総合解説

正答：エ．管理外の接続経路が生まれて境界防御を迂回されるため、不正APの検出・接続制御・設置禁止方針を運用する。
ア：私物APの暗号・認証・管理設定は企業管理外である。
イ：メール認証は無線AP制御の代替にならない。
ウ：無線LANの脅威とは無関係である。
エ：無許可APは既存のネットワーク設計や認証ポリシーの外側に新たな入口を作る。
総合解説：WLANは設計・構築時だけでなく、継続的な不正AP検知や構成監視まで含めて管理する。

Q057 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

経理担当者へ「取引先の振込先が変更された」とするメールが届き、表示名は取引先だが送信ドメインが似た別ドメインだった。最も適切な対応はどれか。
ア．メール記載の連絡先を使わず、既知の正規連絡先で取引先へ別経路確認し、送信ドメインや認証結果も確認する。
イ．メールに記載された新しい電話番号へだけ確認し、そのまま振り込む。
ウ．表示名が正しければ送信元ドメインは確認しなくてよい。
エ．添付ファイルを無条件に開けば送信者の正当性を確認できる。

正答・4肢解説・総合解説

正答：ア．メール記載の連絡先を使わず、既知の正規連絡先で取引先へ別経路確認し、送信ドメインや認証結果も確認する。
ア：ビジネスメール詐欺では、表示名や文面だけでなく、ドメイン・送信経路・業務手続の検証が重要である。
イ：攻撃者が連絡先も用意している可能性がある。
ウ：表示名は偽装できるため不十分である。
エ：マルウェア感染の危険がある。
総合解説：送金・認証情報・緊急依頼など高リスク業務は、メールだけで完結させず独立した確認手順を設ける。

Q058 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

SPF・DKIM・DMARCを適切に導入したため、フィッシングメールは今後100%届かないという説明の評価として最も適切なものはどれか。
ア．正しい。DMARCがあれば全ての悪性添付を自動削除する。
イ．誤りである。送信ドメイン偽装の抑止には有効だが、類似ドメイン、正規アカウント侵害、本文中の詐欺など別手法は残る。
ウ．誤りだが、理由はSPFがSQLインジェクションを引き起こすからである。
エ．正しい。DKIM署名があればメール内容は必ず善意である。

正答・4肢解説・総合解説

正答：イ．誤りである。送信ドメイン偽装の抑止には有効だが、類似ドメイン、正規アカウント侵害、本文中の詐欺など別手法は残る。
ア：DMARCは主に送信ドメイン認証ポリシーと報告を扱う。
イ：メール認証は重要な防御層だが、内容検査、URL対策、MFA、業務手続、利用者教育等と組み合わせる。
ウ：SPFとSQLiは無関係である。
エ：正規ドメインやアカウントが侵害されれば悪性内容にも正規署名が付く可能性がある。
総合解説：「送信元認証に成功した」ことと「メール内容が安全である」ことを区別する。

Q059 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

インターネット公開のVPN装置で、短時間に多数の国からパスワード試行が観測された。対策として最も適切なものはどれか。
ア．管理者パスワードを全従業員で共有する。
イ．ログ保存を停止して攻撃者に見えなくする。
ウ．MFAを導入し、不要な公開範囲を絞り、レート制御・異常ログイン監視・既知侵害資格情報対策を組み合わせる。
エ．VPN装置の更新を止め、設定を永久固定する。

正答・4肢解説・総合解説

正答：ウ．MFAを導入し、不要な公開範囲を絞り、レート制御・異常ログイン監視・既知侵害資格情報対策を組み合わせる。
ア：認証情報漏えい時の影響と追跡困難性を増す。
イ：監視・調査能力を失う。
ウ：リモートアクセスは外部から直接狙われるため、単一パスワードだけに依存しない防御が重要である。
エ：既知脆弱性の悪用リスクを高める。
総合解説：VPN/RDP等のリモート入口は、認証だけでなくパッチ、端末状態、最小権限、ネットワーク分離を含めて守る。

Q060 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

RDPなどの管理用リモートデスクトップをインターネットへ直接公開する場合のリスクとして最も適切なものはどれか。
ア．直接公開すればセキュリティ装置を経由しないので安全になる。
イ．RDPを公開するとメールのDKIM署名が強化される。
ウ．強いパスワードがあればパッチ適用は不要になる。
エ．認証試行や既知脆弱性の直接的な攻撃面になるため、VPN・ゼロトラスト型アクセス・MFA・送信元制限などで露出を減らすべきである。

正答・4肢解説・総合解説

正答：エ．認証試行や既知脆弱性の直接的な攻撃面になるため、VPN・ゼロトラスト型アクセス・MFA・送信元制限などで露出を減らすべきである。
ア：防御層を減らし、攻撃面を増やす。
イ：無関係である。
ウ：認証と脆弱性対策は別の防御層である。
エ：管理サービスは高い権限へつながるため、公開範囲を必要最小限にする。
総合解説：リモートアクセス設計では、誰が・どの端末から・どの資源へ・どの条件で接続できるかを明示して制御する。

Q061 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

従業員の私物端末から社内システムへのリモートアクセスを許可する場合、最も重要な考慮事項はどれか。
ア．端末のパッチ、マルウェア対策、暗号化、認証、紛失時対応など組織管理外端末のリスクを評価し、接続条件を定める。
イ．私物端末なら企業情報は漏えいしないため管理不要である。
ウ．端末のOS更新はセキュリティと無関係である。
エ．接続時の認証を廃止すると利便性と安全性が同時に高まる。

正答・4肢解説・総合解説

正答：ア．端末のパッチ、マルウェア対策、暗号化、認証、紛失時対応など組織管理外端末のリスクを評価し、接続条件を定める。
ア：BYODでは端末の所有者が組織でないため、管理可能範囲とデータ保護要件を明確にする必要がある。
イ：私物端末でも企業データを扱えば漏えいリスクがある。
ウ：既知脆弱性対策として重要である。
エ：不正アクセスリスクを大幅に高める。
総合解説：リモートアクセスは通信路だけでなく、接続元端末の信頼性とデータ保存先まで含めて設計する。

Q062 3-2 ネットワーク・インフラ攻撃 / 無線LAN・メール・リモートアクセス攻撃

出張者が公共Wi-Fiから業務システムへアクセスする場合の対策として最も適切なものはどれか。
ア．暗号化を避けてHTTPを使えばMITMを防げる。
イ．正規APを確認し、HTTPS等の相手認証付き暗号化通信や組織指定の安全なリモートアクセス方式を用い、証明書警告を無視しない。
ウ．SSID名が有名企業名なら証明書警告を無視してよい。
エ．同じパスワードを全サービスで使えば接続確認が簡単になる。

正答・4肢解説・総合解説

正答：イ．正規APを確認し、HTTPS等の相手認証付き暗号化通信や組織指定の安全なリモートアクセス方式を用い、証明書警告を無視しない。
ア：平文通信は盗聴・改ざんされやすい。
イ：公共無線は同一ネットワーク上の盗聴・偽AP・MITM等を想定し、アプリ層・VPN等で通信を保護する。
ウ：SSIDは偽装可能であり、TLS警告を無視すべきではない。
エ：一つの漏えいが複数サービスへ波及する。
総合解説：公共Wi-Fiを全面禁止するか否かではなく、脅威モデルに応じて端末・認証・通信経路を多層で保護する。

Q063 3-3 マルウェア・標的型攻撃 / ランサムウェア

ランサムウェアの典型的な挙動として最も適切なものはどれか。
ア．DNS応答に電子署名を付けて真正性を高める。
イ．Webページ出力を文脈別にエンコードする。
ウ．端末やサーバのデータを暗号化して利用不能にしたり、データを窃取して公開を脅したりし、金銭を要求する。
エ．DBのクエリをパラメータ化して実行する。

正答・4肢解説・総合解説

正答：ウ．端末やサーバのデータを暗号化して利用不能にしたり、データを窃取して公開を脅したりし、金銭を要求する。
ア：DNSSECの説明でありランサムウェアではない。
イ：XSS対策である。
ウ：近年は暗号化だけでなく、窃取データの公開を組み合わせる二重恐喝も想定する必要がある。
エ：SQLインジェクション対策である。
総合解説：ランサムウェア対策は侵入防止だけでなく、侵害を前提にした分離・監視・バックアップ・復旧訓練まで含める。

Q064 3-3 マルウェア・標的型攻撃 / ランサムウェア

ランサムウェア被害の初期侵入経路として想定すべきものの組合せはどれか。
ア．DNSSEC署名の正しい検証、TLS証明書の正常更新、バックアップの復元成功。
イ．パラメータ化クエリ、MFA、最小権限。
ウ．時刻同期、ログ保全、構成管理。
エ．フィッシング、侵害済み認証情報、外部公開サービスの脆弱性など。

正答・4肢解説・総合解説

正答：エ．フィッシング、侵害済み認証情報、外部公開サービスの脆弱性など。
ア：いずれも通常は防御・正常運用であり初期侵入経路ではない。
イ：代表的な防御策である。
ウ：これらも防御・運用管理策である。
エ：CISAのガイダンスでは、複数の一般的な初期アクセス経路を想定した予防策が求められる。
総合解説：一つの侵入経路だけを塞ぐのではなく、メール、認証、公開資産、端末を横断して防御する。

Q065 3-3 マルウェア・標的型攻撃 / ランサムウェア

ランサムウェア対策としてバックアップを用意していたが、本番環境と同じ管理者資格情報で常時オンライン接続されていた。最も重要な改善はどれか。
ア．本番侵害から分離されたバックアップを用意し、削除・改ざんに強い保管方式と別管理の認証を採用し、定期的に復元試験する。
イ．バックアップを一つだけ残し、本番サーバと同じ共有フォルダへ保存する。
ウ．復元試験を行わず、取得ジョブの成功ログだけを確認する。
エ．バックアップ管理者を全従業員へ付与する。

正答・4肢解説・総合解説

正答：ア．本番侵害から分離されたバックアップを用意し、削除・改ざんに強い保管方式と別管理の認証を採用し、定期的に復元試験する。
ア：攻撃者が本番管理権限を得た際にバックアップまで破壊できる設計では、復旧手段として弱い。
イ：同時侵害・暗号化の影響を受けやすい。
ウ：実際に復元できる保証にならない。
エ：破壊・誤操作のリスクを高める。
総合解説：バックアップは「存在すること」ではなく、侵害から独立して保護され、必要時間内に復元できることが重要である。

Q066 3-3 マルウェア・標的型攻撃 / ランサムウェア

侵害端末で、攻撃者がOSの回復用コピーやスナップショットを削除しようとしている。ランサムウェア攻撃の文脈で最も妥当な解釈はどれか。
ア．正常なDNSSEC運用の一環である。
イ．被害者の復旧手段を妨害し、暗号化後の回復を困難にする意図が疑われる。
ウ．SQLインジェクションを防ぐために必要な標準処理である。
エ．WebブラウザのCookieを安全にするための操作である。

正答・4肢解説・総合解説

正答：イ．被害者の復旧手段を妨害し、暗号化後の回復を困難にする意図が疑われる。
ア：DNSSECとは無関係である。
イ：ランサムウェア攻撃では、復旧機能やバックアップの破壊が影響拡大の一部として行われることがある。
ウ：SQLi対策ではない。
エ：Cookie設定とは無関係である。
総合解説：回復機能への不審な変更は高優先度で監視し、端末隔離や証跡保全を検討する。

Q067 3-3 マルウェア・標的型攻撃 / ランサムウェア

複数端末で短時間に大量のファイル拡張子変更と暗号化らしい書込みが検知された。初動として最も適切なものはどれか。
ア．全端末のログを削除して暗号化処理だけを観察する。
イ．感染端末を共有ネットワークへ接続したまま再起動を繰り返す。
ウ．影響端末をネットワークから隔離し、横展開を抑えながら必要な証跡を保全し、インシデント対応手順を開始する。
エ．攻撃者へ直ちに管理者資格情報を送って復号を依頼する。

正答・4肢解説・総合解説

正答：ウ．影響端末をネットワークから隔離し、横展開を抑えながら必要な証跡を保全し、インシデント対応手順を開始する。
ア：証跡を失い、原因・影響範囲調査が困難になる。
イ：拡散や証拠消失の可能性がある。
ウ：暗号化が進行中なら拡散防止を急ぐ一方、調査に必要なログ・メモリ等の保全も考慮する。
エ：被害拡大につながる不適切な行為である。
総合解説：隔離の方法は環境に応じて決め、ネットワーク・ID・共有ストレージなど横展開経路も同時に制御する。

Q068 3-3 マルウェア・標的型攻撃 / ランサムウェア

ランサムウェア被害時に身代金を支払えば必ず安全に復旧できる、という説明として最も適切な評価はどれか。
ア．正しい。支払い後は攻撃者が技術的に再接続できなくなる。
イ．正しい。支払いを行えば流出済みデータは物理的に必ず消去される。
ウ．誤りだが、理由はランサムウェアがネットワーク攻撃ではなく自然災害だからである。
エ．誤りである。復号鍵やデータ削除の保証はなく、再攻撃や法的・制裁上の問題も含めて専門家と評価すべきである。

正答・4肢解説・総合解説

正答：エ．誤りである。復号鍵やデータ削除の保証はなく、再攻撃や法的・制裁上の問題も含めて専門家と評価すべきである。
ア：侵入経路や残存アカウントが残れば再侵害され得る。
イ：攻撃者側コピーの削除を検証できない場合がある。
ウ：ランサムウェアはサイバー攻撃である。
エ：攻撃者との約束に技術的・法的な保証はなく、支払いだけを復旧戦略にしてはならない。
総合解説：復旧計画は、バックアップ、再構築、認証情報変更、侵入経路修正、法務・当局連携などを含める。

Q069 3-3 マルウェア・標的型攻撃 / ランサムウェア

ランサムウェアの「二重恐喝」に備える際、暗号化対策だけで不十分な理由はどれか。
ア．攻撃者が暗号化前に機密データを窃取し、復旧できても公開・売却を脅して金銭を要求する場合があるため。
イ．二重恐喝では必ずDNSSECを無効化するため。
ウ．二重恐喝はバックアップ容量を二倍にするだけの運用用語だから。
エ．暗号化されたデータは攻撃者が事前に窃取できないから。

正答・4肢解説・総合解説

正答：ア．攻撃者が暗号化前に機密データを窃取し、復旧できても公開・売却を脅して金銭を要求する場合があるため。
ア：可用性だけでなく機密性侵害も同時に扱う必要がある。
イ：DNSSECの有無は二重恐喝の定義ではない。
ウ：データ窃取と暗号化・恐喝を組み合わせる攻撃である。
エ：暗号化前に外部送信される可能性がある。
総合解説：DLPや外部通信監視、権限分離、データ分類、流出時の通知・法務対応もランサムウェア計画へ含める。

Q070 3-3 マルウェア・標的型攻撃 / ランサムウェア

VPN資格情報の漏えいがランサムウェア侵入の一因になった。再発防止としてMFAを導入する評価として最も適切なものはどれか。
ア．MFAを入れれば全ランサムウェアが実行不能になる。
イ．資格情報だけを盗まれた攻撃への耐性を高める有効な対策だが、脆弱性悪用や端末感染など他経路もあるため単独では十分でない。
ウ．MFAはバックアップ復元速度だけを上げる仕組みである。
エ．MFA導入後はVPN装置の更新を停止してよい。

正答・4肢解説・総合解説

正答：イ．資格情報だけを盗まれた攻撃への耐性を高める有効な対策だが、脆弱性悪用や端末感染など他経路もあるため単独では十分でない。
ア：マルウェア実行や脆弱性悪用そのものを直接防ぐわけではない。
イ：MFAは認証侵害の一部を抑える重要策だが、パッチ・端末防御・アクセス制御なども必要である。
ウ：認証強化が主目的である。
エ：既知脆弱性対策は別途必要である。
総合解説：初期アクセス経路を複数想定し、認証・公開資産・メール・端末を横断して対策する。

Q071 3-3 マルウェア・標的型攻撃 / ランサムウェア

一台の端末がランサムウェアに感染した場合に、ファイルサーバや管理ネットワークへの横展開を抑える設計として最も適切なものはどれか。
ア．全端末を同一フラットネットワークに置き、相互通信を全許可する。
イ．バックアップサーバを利用者端末から管理者権限で常時マウントする。
ウ．業務・管理・バックアップ等を必要に応じてセグメント分離し、端末から到達できるサービスと権限を最小限にする。
エ．管理者アカウントを一般作業へ常用する。

正答・4肢解説・総合解説

正答：ウ．業務・管理・バックアップ等を必要に応じてセグメント分離し、端末から到達できるサービスと権限を最小限にする。
ア：横展開を容易にする。
イ：感染時にバックアップも破壊されやすい。
ウ：ネットワーク到達性と認証権限を絞ることで、一台の侵害が組織全体へ波及する可能性を低減できる。
エ：資格情報窃取時の影響を大きくする。
総合解説：セグメンテーションは万能ではないため、最小権限、管理者資格情報分離、EDR、監視と組み合わせる。

Q072 3-3 マルウェア・標的型攻撃 / ランサムウェア

バックアップからシステムを復元する前に実施すべきこととして最も適切なものはどれか。
ア．感染原因を調べず、同じ侵害済み環境へ即座に全バックアップを書き戻す。
イ．復元後も盗まれた可能性のある管理者パスワードを変更しない。
ウ．ログを全て消去してから原因調査を始める。
エ．侵入経路や残存マルウェア・不正アカウントを特定し、脆弱性修正や認証情報変更など再侵害防止策を講じた上でクリーンな環境へ復元する。

正答・4肢解説・総合解説

正答：エ．侵入経路や残存マルウェア・不正アカウントを特定し、脆弱性修正や認証情報変更など再侵害防止策を講じた上でクリーンな環境へ復元する。
ア：再感染・再暗号化の危険が高い。
イ：攻撃者が再利用できる可能性がある。
ウ：調査証跡を失う。
エ：原因を残したまま復元すると、復旧直後に再度侵害される可能性がある。
総合解説：復旧は単なるデータ戻しではなく、侵害原因の除去、信頼できる状態の再構築、監視強化まで含む。

Q073 3-3 マルウェア・標的型攻撃 / ランサムウェア

ランサムウェア対応訓練を定期実施する主な目的として最も適切なものはどれか。
ア．技術担当・経営・法務・広報・外部事業者の役割と連絡手順、復旧優先順位を事前に検証し、実際の初動を迅速化する。
イ．訓練をすればバックアップを作らなくてもよくなる。
ウ．訓練では必ず本番データを暗号化して停止させる。
エ．訓練の目的は身代金支払い額を事前に決めることだけである。

正答・4肢解説・総合解説

正答：ア．技術担当・経営・法務・広報・外部事業者の役割と連絡手順、復旧優先順位を事前に検証し、実際の初動を迅速化する。
ア：ランサムウェアは技術問題だけでなく事業継続・法務・対外説明を伴うため、組織横断の準備が必要である。
イ：訓練は技術的復旧資源の代替ではない。
ウ：安全なシナリオで実施でき、本番破壊は不要である。
エ：主目的は対応能力と意思決定の検証である。
総合解説：机上演習と技術復旧訓練を組み合わせ、訓練で見つかった課題を手順・構成へ反映する。

Q074 3-3 マルウェア・標的型攻撃 / ランサムウェア

予算が限られる中、外部公開VPNは単一パスワード認証、バックアップは本番と同一資格情報、OSには未適用の重大パッチがある。優先すべき方針として最も適切なものはどれか。
ア．壁紙を統一することを最優先し、認証とパッチは翌年度まで保留する。
イ．重大な初期侵入・復旧阻害リスクを減らすため、VPNのMFA・脆弱性修正と、バックアップの分離・復元試験を優先して実施する。
ウ．バックアップを削除してストレージ費用を減らす。
エ．全利用者へ管理者権限を付与して復旧を簡単にする。

正答・4肢解説・総合解説

正答：イ．重大な初期侵入・復旧阻害リスクを減らすため、VPNのMFA・脆弱性修正と、バックアップの分離・復元試験を優先して実施する。
ア：重大な攻撃面を放置するため不適切である。
イ：侵入を防ぐ対策と、侵入後に復旧できる対策の両方を高優先で進める。
ウ：復旧能力を失う。
エ：侵害時の影響を拡大する。
総合解説：リスクベースで、悪用可能性・影響・復旧可能性を見て対策を優先順位付けする。

Q075 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

標的型攻撃の一般的な特徴として最も適切なものはどれか。
ア．必ず大量トラフィックだけを送り回線を飽和させる。
イ．必ず物理施設へ侵入して端末を盗む。
ウ．特定の組織・人物・業務を狙い、事前調査や社会的背景を利用して侵入し、目的達成まで段階的に活動する。
エ．対象を選ばず全世界へ同じ広告だけを表示する。

正答・4肢解説・総合解説

正答：ウ．特定の組織・人物・業務を狙い、事前調査や社会的背景を利用して侵入し、目的達成まで段階的に活動する。
ア：これはDDoSの典型的な目的である。
イ：物理侵入を伴う場合もあるが、標的型攻撃の必須条件ではない。
ウ：不特定多数への無差別攻撃と比べ、対象に合わせた誘導・侵入手法が用いられることがある。
エ：標的性の説明と逆である。
総合解説：標的型攻撃では、メール・認証情報・外部公開資産・取引先など複数の入口を想定し、侵入後の横展開や情報窃取も監視する。

Q076 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

スピアフィッシングの説明として最も適切なものはどれか。
ア．無差別に同一文面を大量送信することだけを指す。
イ．DNSサーバのキャッシュを偽情報で汚染する攻撃である。
ウ．WebサーバのCPUを大量HTTPで枯渇させる攻撃である。
エ．特定の受信者や組織に合わせて、氏名・部署・取引関係などを利用した説得力のある内容で誘導するフィッシングである。

正答・4肢解説・総合解説

正答：エ．特定の受信者や組織に合わせて、氏名・部署・取引関係などを利用した説得力のある内容で誘導するフィッシングである。
ア：それは一般的な大量フィッシングに近い。
イ：DNSキャッシュポイズニングである。
ウ：アプリケーション層DoSの説明である。
エ：対象に関する情報を使うことで、受信者が正規の連絡と誤認しやすくする。
総合解説：対策はメールフィルタだけでなく、MFA、業務手続による独立確認、添付・URL検査、利用者教育を組み合わせる。

Q077 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

サプライチェーン攻撃の説明として最も適切なものはどれか。
ア．標的組織が信頼して利用するソフトウェア、更新経路、委託先、サービス提供者などを侵害し、その信頼関係を経由して標的へ影響を及ぼす。
イ．社内LANでARP表だけを書き換える攻撃に限定される。
ウ．利用者のブラウザCookieだけを削除する攻撃である。
エ．必ず自然災害による物流停止を意味する。

正答・4肢解説・総合解説

正答：ア．標的組織が信頼して利用するソフトウェア、更新経路、委託先、サービス提供者などを侵害し、その信頼関係を経由して標的へ影響を及ぼす。
ア：直接標的だけでなく、製品・サービスの開発・配布・運用に関わる第三者が攻撃面になる。
イ：サプライチェーン攻撃はより広い供給・委託関係を狙う。
ウ：定義と無関係である。
エ：サイバー領域ではICT製品・サービスの供給網を通じたリスクを含む。
総合解説：C-SCRMでは、供給者のリスク評価、契約要件、製品真正性、更新経路、脆弱性対応、監視などをライフサイクル全体で扱う。

Q078 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

正規ベンダの署名付き更新サーバが侵害され、悪性コードを含む更新パッケージが顧客へ配布された。この事象の分類として最も適切なものはどれか。
ア．反射型DDoS
イ．ソフトウェアサプライチェーン攻撃
ウ．CSRF
エ．SQLインジェクション

正答・4肢解説・総合解説

正答：イ．ソフトウェアサプライチェーン攻撃
ア：第三者サーバの応答を被害者へ反射する可用性攻撃とは異なる。
イ：利用者が信頼する正規の配布経路が悪用され、複数顧客へ影響が波及するためである。
ウ：認証済みブラウザに意図しないリクエストを送らせる攻撃である。
エ：DBクエリへの入力混入である。
総合解説：署名が存在していても、署名鍵やビルド・配布基盤自体が侵害されれば悪性更新が正規に見える可能性があるため、開発・署名・配布環境の保護が重要である。

Q079 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

重要システムの運用を外部SaaS事業者へ委託する際、セキュリティ確認として最も適切なものはどれか。
ア．大手事業者なら契約前のセキュリティ確認は一切不要である。
イ．委託すれば自組織はインシデント対応計画を持たなくてよい。
ウ．委託先のセキュリティ体制、下請け・再委託、インシデント通知、脆弱性対応、データ取扱い等をリスクに応じて評価し契約へ反映する。
エ．価格だけを比較し、データ保護要件は契約後に決める。

正答・4肢解説・総合解説

正答：ウ．委託先のセキュリティ体制、下請け・再委託、インシデント通知、脆弱性対応、データ取扱い等をリスクに応じて評価し契約へ反映する。
ア：規模だけでリスクを判断できない。
イ：委託先障害・侵害時にも自組織の対応が必要である。
ウ：第三者に業務を移しても、自組織の事業リスクまで消えるわけではない。
エ：重要なセキュリティ条件は調達・契約段階で明確にする必要がある。
総合解説：C-SCRMは技術製品だけでなく、サービス提供者や再委託を含む依存関係を可視化して管理する。

Q080 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

SBOM（Software Bill of Materials）のセキュリティ上の主な価値として最も適切なものはどれか。
ア．SBOMがあれば全コンポーネントの脆弱性が自動的に修正される。
イ．SBOMはDDoSトラフィックを吸収するネットワーク装置である。
ウ．SBOMは利用者パスワードを保管する方式である。
エ．ソフトウェアを構成するコンポーネントや依存関係の把握を助け、脆弱性公表時に影響調査を迅速化できる。

正答・4肢解説・総合解説

正答：エ．ソフトウェアを構成するコンポーネントや依存関係の把握を助け、脆弱性公表時に影響調査を迅速化できる。
ア：SBOMは主に可視化情報であり、修正そのものは別工程である。
イ：ソフトウェア構成情報でありネットワーク装置ではない。
ウ：認証情報管理とは異なる。
エ：依存部品の可視性を高めることで、どの製品が影響を受けるかを特定しやすくする。
総合解説：SBOMは有用だが、完全性・更新頻度・部品の脆弱性評価・署名・ビルド環境保護など他の供給網対策と組み合わせる必要がある。

Q081 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

ソースコード管理は改ざんされていないが、CI/CDビルドサーバが侵害され、生成物へ悪性コードが混入した。重要な教訓として最も適切なものはどれか。
ア．ソースコードだけでなく、ビルド・署名・配布の各工程を信頼境界として保護し、生成物の来歴と完全性を検証する必要がある。
イ．Gitリポジトリが無事なら生成物は必ず安全である。
ウ．ビルドサーバはインターネットへ管理ポートを全開放すべきである。
エ．生成物の署名鍵をCIログへ平文出力する。

正答・4肢解説・総合解説

正答：ア．ソースコードだけでなく、ビルド・署名・配布の各工程を信頼境界として保護し、生成物の来歴と完全性を検証する必要がある。
ア：供給網攻撃では、開発パイプライン自体が改ざん点になり得る。
イ：ビルド工程での混入を見逃す。
ウ：攻撃面を増大させる。
エ：鍵漏えいにより悪性生成物への正規署名を許す可能性がある。
総合解説：開発・ビルド・署名・配布を分離し、最小権限、秘密管理、監査ログ、再現可能性等で信頼性を高める。

Q082 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

一人の利用者端末の侵害後、通常その利用者がアクセスしない複数サーバへ管理プロトコルで接続試行が始まった。最も適切な評価はどれか。
ア．正常なDNSSEC署名検証だけで必ず発生する。
イ．侵害端末を起点とした横展開（Lateral Movement）の兆候として高優先で調査する。
ウ．利用者がWebページを閲覧しただけなので調査不要である。
エ．バックアップ取得の成功を意味するため必ず安全である。

正答・4肢解説・総合解説

正答：イ．侵害端末を起点とした横展開（Lateral Movement）の兆候として高優先で調査する。
ア：DNSSECとは無関係である。
イ：標的型攻撃では初期侵入後に資格情報や管理機能を使って他端末・サーバへ移動することがある。
ウ：通常外の管理接続は重要な異常である。
エ：接続元・宛先・認証情報等の文脈を確認する必要がある。
総合解説：EDR、認証ログ、ネットワークログを相関し、資格情報窃取や横展開経路を調査する。

Q083 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

保守ベンダに常設VPNと広範な管理者権限を与えている。サプライチェーン侵害に備えた改善として最も適切なものはどれか。
ア．ベンダ全員で共通の管理者IDを使い、24時間接続可能にする。
イ．委託先通信は監査対象外にする。
ウ．接続元・時間・対象資産を限定し、MFA、個別アカウント、必要時のみの特権付与、操作ログを適用する。
エ．保守の便宜のためネットワーク分離を全て解除する。

正答・4肢解説・総合解説

正答：ウ．接続元・時間・対象資産を限定し、MFA、個別アカウント、必要時のみの特権付与、操作ログを適用する。
ア：追跡性と最小権限を損なう。
イ：第三者アクセスこそ監視・証跡が重要である。
ウ：委託先アカウントが侵害された場合の影響を最小化するため、信頼を無条件に与えない。
エ：侵害時の横展開を容易にする。
総合解説：第三者アクセスは、自社社員と同等以上に認証・権限・時間・経路・監査を明確化する。

Q084 3-3 マルウェア・標的型攻撃 / 標的型・サプライチェーン攻撃

利用中のソフトウェアベンダから「特定バージョンの更新パッケージが改ざんされた可能性がある」と通知を受けた。最も適切な初動はどれか。
ア．通知を無視し、次回定期更新まで何もしない。
イ．全社のログを削除して容量を空ける。
ウ．影響有無を確認せず全従業員へ管理者権限を付与する。
エ．影響バージョンの利用状況を資産情報から特定し、ベンダのIOC・修正版・回避策を確認し、ログ保全と侵害有無の調査を優先する。

正答・4肢解説・総合解説

正答：エ．影響バージョンの利用状況を資産情報から特定し、ベンダのIOC・修正版・回避策を確認し、ログ保全と侵害有無の調査を優先する。
ア：既に侵害可能性があるため影響確認が必要である。
イ：IOC照合や侵害調査に必要な証跡を失う。
ウ：被害拡大につながる。
エ：サプライチェーン事象では、どの製品・版・期間が影響するかを迅速に特定できる資産可視性が重要である。
総合解説：SBOM・ソフトウェア資産台帳・構成管理が整っていると、供給網インシデントの影響範囲特定を迅速化できる。

Q085 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

マルウェアにおけるC2（Command and Control）通信の主な目的はどれか。
ア．侵害端末と攻撃者側インフラの間で命令を受け取り、実行結果や収集情報を送るなど遠隔制御を行う。
イ．DNSSECの信頼連鎖を検証するため。
ウ．DBのSQL文をパラメータ化するため。
エ．バックアップ媒体を暗号化して保管するため。

正答・4肢解説・総合解説

正答：ア．侵害端末と攻撃者側インフラの間で命令を受け取り、実行結果や収集情報を送るなど遠隔制御を行う。
ア：MITRE ATT&CKではCommand and Controlは侵害システムを制御するための通信を表す戦術である。
イ：DNS真正性検証の機能でありC2の目的ではない。
ウ：SQLi対策である。
エ：バックアップ保護とC2は別である。
総合解説：C2はHTTP(S)、DNS、クラウドサービス等の一般的通信に紛れる場合があるため、宛先だけでなく頻度・プロセス・通信パターンを分析する。

Q086 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

端末が深夜も一定間隔で、利用実績のない外部ドメインへ少量のHTTPS通信を繰り返している。調査上の観点として最も適切なものはどれか。
ア．HTTPSなので悪性通信の可能性はゼロと判断する。
イ．C2ビーコンの可能性を考え、送信元プロセス、宛先評判、周期性、DNS・EDRログを相関して調査する。
ウ．一定間隔の通信は全てマルウェアと断定し即座に全社停止する。
エ．DBのSELECT権限を追加して通信量を増やす。

正答・4肢解説・総合解説

正答：イ．C2ビーコンの可能性を考え、送信元プロセス、宛先評判、周期性、DNS・EDRログを相関して調査する。
ア：攻撃者もTLSを利用できる。
イ：周期的な少量通信はC2のチェックインに見られることがあるが、正規アップデータ等との区別が必要である。
ウ：正規ソフトも周期通信するため追加文脈が必要である。
エ：C2調査とは無関係である。
総合解説：C2検知では単一IOCだけでなく、周期性、親子プロセス、ドメイン年齢、通信先、送信量など複数の特徴を組み合わせる。

Q087 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

攻撃者がC2通信にHTTPSやDNSなど一般的プロトコルを使う理由として最も適切なものはどれか。
ア．HTTPSを使うと攻撃者のコードが自動的に正規署名されるため。
イ．DNSを使うと端末の管理者権限が必ず付与されるため。
ウ．通常業務通信に紛れやすく、ネットワーク境界で単純にプロトコル自体を遮断しにくいため。
エ．一般プロトコルは監視ログを一切生成できないため。

正答・4肢解説・総合解説

正答：ウ．通常業務通信に紛れやすく、ネットワーク境界で単純にプロトコル自体を遮断しにくいため。
ア：TLS暗号化とコード署名は別である。
イ：DNS利用だけで権限昇格は起きない。
ウ：MITRE ATT&CKでも、一般的なアプリケーション層プロトコルへC2を埋め込む技術が整理されている。
エ：DNS・プロキシ・FW等でログを取得できる。
総合解説：防御側は、許可プロトコルの中でも不審な宛先・利用プロセス・データ量・頻度を監視する必要がある。

Q088 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

「ファイルレスマルウェア」という表現の説明として最も適切なものはどれか。
ア．ネットワーク通信を一切行わないマルウェアだけを指す。
イ．必ずBIOSを書き換えるハードウェア攻撃である。
ウ．暗号化ファイルを作るランサムウェアだけの別名である。
エ．悪性活動の全部又は一部をメモリ上や既存の正規ツール・スクリプト機能で実行し、従来型の悪性実行ファイルをディスクへ残さない又は最小化する手法を指す。

正答・4肢解説・総合解説

正答：エ．悪性活動の全部又は一部をメモリ上や既存の正規ツール・スクリプト機能で実行し、従来型の悪性実行ファイルをディスクへ残さない又は最小化する手法を指す。
ア：ファイルレスでもC2通信を行う場合がある。
イ：ファイルレスの定義とは異なる。
ウ：ランサムウェアに限定されない。
エ：「ファイルが一切存在しない」という絶対的な意味ではなく、ディスク上の典型的なマルウェアファイルへの依存を減らす攻撃手法を指すことが多い。
総合解説：検知ではファイルハッシュだけでなく、プロセス挙動、スクリプト実行、メモリ、親子プロセス、ネットワーク通信を観測する。

Q089 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

通常はOffice文書を閲覧するだけの端末で、文書閲覧プロセスからPowerShellが起動し、難読化されたコマンドを実行後に外部通信を開始した。最も適切な評価はどれか。
ア．不審なPowerShell悪用の可能性が高く、親子プロセス、コマンドライン、スクリプトログ、外部通信を保全して調査する。
イ．PowerShellは正規ツールなので悪用される可能性はない。
ウ．難読化されていれば必ず正規管理処理である。
エ．外部通信がHTTPSなら調査不要である。

正答・4肢解説・総合解説

正答：ア．不審なPowerShell悪用の可能性が高く、親子プロセス、コマンドライン、スクリプトログ、外部通信を保全して調査する。
ア：MITRE ATT&CKはPowerShellを攻撃者が実行・ダウンロード・メモリ上実行に悪用し得る技術として整理している。
イ：正規管理ツールも攻撃者に悪用される。
ウ：難読化は悪性活動で検知回避に使われることがある。
エ：TLS上でも悪性C2は成立する。
総合解説：正規ツールの悪用は単純なファイルブロックでは見つけにくいため、実行文脈と行動連鎖を監視する。

Q090 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

管理者以外が通常利用しない端末群で、WMIを介したリモートプロセス起動が複数ホストへ連続している。最も適切な判断はどれか。
ア．WMIは監視情報の読み取り専用なのでプロセス起動には使えない。
イ．WMIを悪用した実行や横展開の可能性を考え、実行元アカウント、対象ホスト、生成プロセス、関連通信を調査する。
ウ．WMI通信は必ずDNSSECで署名されるので安全である。
エ．WMIを使った通信は全てバックアップ処理である。

正答・4肢解説・総合解説

正答：イ．WMIを悪用した実行や横展開の可能性を考え、実行元アカウント、対象ホスト、生成プロセス、関連通信を調査する。
ア：WMIは管理操作やコマンド実行に利用できる。
イ：WMIは正規管理機能だが、攻撃者がローカル・リモートのコマンド実行に悪用できる。
ウ：DNSSECとは無関係である。
エ：業務文脈を確認する必要があり一律に正常とは言えない。
総合解説：WMI・PowerShell等の正規管理機能は必要な利用者・端末へ制限し、異常な使用を行動ベースで検知する。

Q091 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

マルウェア検知を「ディスク上の既知悪性ファイルハッシュ照合だけ」に限定する方針の評価として最も適切なものはどれか。
ア．十分である。全ての攻撃は必ず既知の実行ファイルをディスクへ保存する。
イ．不十分だが、理由はハッシュ値がネットワーク帯域を必ず枯渇させるからである。
ウ．不十分である。メモリ上実行、スクリプト、正規ツール悪用、未知ファイルなどを見逃すため、行動・プロセス・メモリ・通信監視を組み合わせる必要がある。
エ．十分である。PowerShellやWMIは攻撃者が利用できない。

正答・4肢解説・総合解説

正答：ウ．不十分である。メモリ上実行、スクリプト、正規ツール悪用、未知ファイルなどを見逃すため、行動・プロセス・メモリ・通信監視を組み合わせる必要がある。
ア：その前提は成り立たない。
イ：主な問題は検知範囲の不足である。
ウ：シグネチャは既知脅威に有効だが、ファイルレスや変種への可視性を補完する必要がある。
エ：正規ツールが悪用される事例は多数ある。
総合解説：EDR等では、ファイル情報に加えてプロセスツリー、コマンドライン、メモリ挙動、接続先を組み合わせて検知する。

Q092 3-3 マルウェア・標的型攻撃 / C2・ファイルレスマルウェア

既知のC2ドメインへの通信をDNSで遮断したところ、端末の外部通信は止まった。次の対応として最も適切なものはどれか。
ア．C2が止まればマルウェアは必ず自動消滅するため調査不要である。
イ．遮断後は全ログを削除する。
ウ．同じC2ドメインをallowlistへ追加して再接続させる。
エ．遮断だけで完了とせず、通信していた端末を特定して隔離・調査し、侵入経路、永続化、資格情報窃取、横展開の有無を確認する。

正答・4肢解説・総合解説

正答：エ．遮断だけで完了とせず、通信していた端末を特定して隔離・調査し、侵入経路、永続化、資格情報窃取、横展開の有無を確認する。
ア：端末内の悪性コードや永続化が残る可能性がある。
イ：原因・範囲調査に必要な証跡を失う。
ウ：攻撃者との通信を再開させる危険がある。
エ：C2遮断は被害抑止に有効だが、端末内の侵害状態そのものを除去したことにはならない。
総合解説：IOC遮断は封じ込めの一手段であり、根本原因と侵害範囲を確認して根絶・復旧へ進む必要がある。

Q093　3-4 脆弱性評価・診断 / CVE・CVSS・CWE

CVE IDの主な役割として最も適切なものはどれか。
ア．公開された個々の脆弱性を一意に参照し、組織や製品をまたいで同じ問題を識別できるようにする。
イ．脆弱性の深刻度を0.0〜10.0の数値だけで表す。
ウ．プログラム上の弱点を言語非依存で分類する。
エ．全ての脆弱性に対して修正版プログラムを配布する。

正答・4肢解説・総合解説

正答：ア．公開された個々の脆弱性を一意に参照し、組織や製品をまたいで同じ問題を識別できるようにする。
ア：CVEは公開脆弱性に共通の識別子を与え、関係者が同一の問題を参照できるようにする仕組みである。
イ：深刻度のスコアリングはCVSSの役割であり、CVE IDそのものの役割ではない。
ウ：弱点の分類体系はCWEの役割である。
エ：CVE Programは識別・定義・カタログ化を行うもので、修正版の配布主体ではない。
総合解説：CVEは『どの脆弱性か』を共有するための識別体系である。深刻度はCVSS、弱点の種類はCWEというように役割を区別する。

Q094　3-4 脆弱性評価・診断 / CVE・CVSS・CWE

CVEとCWEの関係について最も適切な説明はどれか。
ア．CVEとCWEは同一の識別体系で、番号だけが異なる。
イ．CVEは個別の公開脆弱性を識別し、CWEはその背景にあるソフトウェア・ハードウェア上の弱点の種類を分類する。
ウ．CWEは脆弱性の公開日を示し、CVEは攻撃者グループを示す。
エ．CVEは設定ミスだけを、CWEは暗号技術だけを扱う。

正答・4肢解説・総合解説

正答：イ．CVEは個別の公開脆弱性を識別し、CWEはその背景にあるソフトウェア・ハードウェア上の弱点の種類を分類する。
ア：両者は別のプログラムであり、目的も粒度も異なる。
イ：CVEは具体的な脆弱性レコード、CWEは弱点の共通語彙であり、両者は粒度と目的が異なる。
ウ：CWEは弱点分類であり、CVEも攻撃者グループの識別体系ではない。
エ：対象領域はそのように限定されていない。
総合解説：脆弱性の管理では、CVEで個別案件を特定し、CWEで根本的な弱点パターンを捉えると、修正だけでなく再発防止にもつなげやすい。

Q095 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

CVSS v4.0におけるSupplemental Metricsの説明として適切なものはどれか。
ア．必ずBase Scoreを2倍にする。
イ．CVE IDを自動採番するための項目である。
ウ．脆弱性の追加的な特性を伝えるために用いるが、最終CVSSスコアそのものは変更しない。
エ．脆弱性の修正済み・未修正だけを表し、他の特性は扱わない。

正答・4肢解説・総合解説

正答：ウ．脆弱性の追加的な特性を伝えるために用いるが、最終CVSSスコアそのものは変更しない。
ア：Supplemental Metricsはスコアを直接増減しない。
イ：CVE IDの採番とCVSSのメトリクスは別の仕組みである。
ウ：CVSS v4.0仕様ではSupplemental Metricsは追加情報を提供するが、最終スコアに影響しない。
エ：Supplemental Metricsは複数の補助的特性を表現でき、修正状況だけに限定されない。
総合解説：CVSS v4.0ではBase、Threat、EnvironmentalとSupplementalを区別する。Supplementalは状況理解を助けるが、スコア計算への影響は持たない。

Q096 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

CVSSベクタ文字列を記録しておく利点として最も適切なものはどれか。
ア．脆弱性のソースコード全体を暗号化して格納できる。
イ．CVE Recordの公開を取り消すための署名として使う。
ウ．攻撃者の実名と所在地を一意に特定できる。
エ．スコアの根拠となる各メトリクス値を圧縮した形で共有でき、数値だけより評価条件を追跡しやすい。

正答・4肢解説・総合解説

正答：エ．スコアの根拠となる各メトリクス値を圧縮した形で共有でき、数値だけより評価条件を追跡しやすい。
ア：CVSSベクタはソースコード格納形式ではない。
イ：ベクタは取消署名ではなく評価値の表現である。
ウ：CVSSは脆弱性特性を評価する仕組みであり、攻撃者属性を識別しない。
エ：ベクタ文字列には評価に用いたメトリクス値が含まれるため、単一スコアより判断根拠を確認しやすい。
総合解説：脆弱性評価では『スコアだけ』でなくベクタも残すと、攻撃元区分、必要権限、影響等の評価前提を再確認できる。

Q097 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

同じCVSS Base Scoreの脆弱性AとBがある。Aはインターネット公開された基幹システムに存在し、Bは隔離された検証端末にのみ存在する。修正優先順位の判断として最も適切なものはどれか。
ア．Base Scoreだけで同順位とせず、資産重要度、実際の露出、利用可能な攻撃情報、既存対策など環境・脅威の文脈を加えて判断する。
イ．CVE番号の数字が小さい方を必ず先に直す。
ウ．同じBase Scoreなら資産の用途に関係なく常に同順位とする。
エ．隔離端末の脆弱性は将来接続されても永久に無視してよい。

正答・4肢解説・総合解説

正答：ア．Base Scoreだけで同順位とせず、資産重要度、実際の露出、利用可能な攻撃情報、既存対策など環境・脅威の文脈を加えて判断する。
ア：同じBase特性でも、組織環境での影響や現実の脅威状況は異なるため、運用上の優先順位は文脈を加えて決める必要がある。
イ：CVE IDの数値大小は深刻度や優先度を意味しない。
ウ：Base Scoreだけでは組織固有の重要度や露出を表し切れない。
エ：現状の露出が低くても、構成変更や利用状況に応じて再評価が必要である。
総合解説：CVSSは優先順位付けの重要な材料だが、組織固有のリスク判断を完全に代替するものではない。EnvironmentalやThreatの観点、資産価値、露出、補完統制を併せる。

Q098 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

複数製品で別々のCVEが発生したが、調査するといずれも境界外書込みに起因していた。組織横断の再発防止策を検討する際に最も有用な整理はどれか。
ア．CVE番号の末尾が同じものだけを同一原因とみなす。
イ．各CVEをCWEの弱点分類へ対応付け、共通する根本原因に対してコーディング規約・レビュー・テストを改善する。
ウ．CVSSスコアが違えば同じ弱点分類になることはない。
エ．脆弱性の種類を無視し、全てネットワーク機器交換で対処する。

正答・4肢解説・総合解説

正答：イ．各CVEをCWEの弱点分類へ対応付け、共通する根本原因に対してコーディング規約・レビュー・テストを改善する。
ア：CVE IDの番号構造は根本原因の同一性を示さない。
イ：個別CVEをCWEへマッピングすると、共通の弱点パターンを捉えて開発工程の再発防止策へつなげやすい。
ウ：同じCWEに属しても、環境や影響によってCVSS評価は異なり得る。
エ：原因に対応しない一律対策では再発防止にならない。
総合解説：CVEは個別事象、CWEは弱点パターンである。両者を結び付けると、修正管理と根本原因分析を別レベルで実施できる。

Q099 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

CVSS v4.0のThreat Metricsが主に表そうとするものはどれか。
ア．脆弱性を発見した研究者の所属組織だけである。
イ．組織固有の機密性・完全性・可用性要求だけである。
ウ．時間とともに変化し得る、現実の脅威状況に関する要素である。
エ．CVE IDを発行したCNAの国籍である。

正答・4肢解説・総合解説

正答：ウ．時間とともに変化し得る、現実の脅威状況に関する要素である。
ア：研究者の所属はCVSS Threat Metricsではない。
イ：組織固有の要求はEnvironmental側で扱う。
ウ：CVSS v4.0ではThreat Metricsにより、脆弱性を取り巻く現実の脅威状況をBaseとは分けて扱う。
エ：CNAの国籍はCVSS評価項目ではない。
総合解説：Baseは脆弱性固有の特性を中心に表し、Threatは変化し得る脅威状況、Environmentalは組織固有の環境を反映するという分担を押さえる。

Q100 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

CVE Recordが存在することから直ちに断定できる内容として不適切なものはどれか。
ア．公開された脆弱性を共通の識別子で参照できる。
イ．複数の組織が同じ脆弱性について情報交換しやすくなる。
ウ．関連するベンダ情報や評価情報を別ソースで突合する起点になり得る。
エ．その脆弱性に対する修正プログラムが、全ての利用環境向けに既に提供済みである。

正答・4肢解説・総合解説

正答：エ．その脆弱性に対する修正プログラムが、全ての利用環境向けに既に提供済みである。
ア：これはCVE Programの主要目的に合致する。
イ：共通識別子により調整や情報共有が容易になる。
ウ：CVE IDは他の脆弱性情報源を関連付けるキーとして利用できる。
エ：CVEは脆弱性を識別・記述するための記録であり、全環境向け修正版の提供完了を保証しない。
総合解説：CVE Recordは重要な識別基盤だが、修正可否、悪用状況、適用影響などはベンダ情報や他の信頼できる情報源で確認する。

Q101 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

SOCが脆弱性修正のSLAをCVSS Base Scoreだけで一律に決めている。インターネット非公開でも機密データを扱うシステムや、逆に公開されていても強い補完統制があるシステムが混在している。改善策として最も適切なものはどれか。
ア．CVSSのベクタ・Threat/Environmentalの観点に加え、資産重要度、到達可能性、悪用状況、補完統制を明示した優先順位基準へ改める。
イ．CVE IDの発行順だけでSLAを決める。
ウ．全脆弱性を必ず同日中に修正し、業務影響は考慮しない。
エ．CVSSを完全に廃止し、担当者の直感だけで決める。

正答・4肢解説・総合解説

正答：ア．CVSSのベクタ・Threat/Environmentalの観点に加え、資産重要度、到達可能性、悪用状況、補完統制を明示した優先順位基準へ改める。
ア：脆弱性固有の評価と組織固有のリスクを分けて取り込み、判断根拠を説明可能にするのが適切である。
イ：発行順はリスクの大きさを表さない。
ウ：無差別な期限設定は可用性や変更リスクを無視し、現実的なリスク管理にならない。
エ：標準化された評価指標を捨てるのではなく、文脈と組み合わせるのが望ましい。
総合解説：CVSSは共通尺度として有用だが、実運用では『脆弱性の特性×組織環境×脅威状況』で優先順位を決める。

Q102 3-4 脆弱性評価・診断 / CVE・CVSS・CWE

脆弱性管理台帳に『個別脆弱性の識別』『深刻度評価』『根本的な弱点分類』の3項目を持たせたい。対応する組合せとして最も適切なものはどれか。
ア．個別識別=CVSS、深刻度評価=CWE、弱点分類=CVE。
イ．個別識別=CVE、深刻度評価=CVSS、弱点分類=CWE。
ウ．個別識別=CWE、深刻度評価=CVE、弱点分類=CVSS。
エ．3項目ともCVEだけで完全に表現する。

正答・4肢解説・総合解説

正答：イ．個別識別=CVE、深刻度評価=CVSS、弱点分類=CWE。
ア：3者の役割が入れ替わっている。
イ：CVE、CVSS、CWEはそれぞれ識別・評価・弱点分類という補完的な役割を持つ。
ウ：CWEは弱点分類、CVEは個別識別、CVSSはスコアリングである。
エ：CVEだけでは深刻度の標準評価や弱点分類の役割を代替できない。
総合解説：3つの標準を競合関係ではなく補完関係として使うと、脆弱性の追跡、優先順位付け、開発工程の改善を一つの台帳で結び付けられる。

Q103 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

一般的な脆弱性スキャンとペネトレーションテストの違いとして最も適切なものはどれか。
ア．脆弱性スキャンは必ずソースコードを読み、ペネトレーションテストは必ず読まない。
イ．ペネトレーションテストは承認不要だが、脆弱性スキャンだけ承認が必要である。
ウ．脆弱性スキャンは潜在的な弱点を広く検出することを重視し、ペネトレーションテストは定めた範囲で実際の悪用可能性や攻撃経路を検証する。
エ．両者は名称だけが異なり、目的・手法・成果物は完全に同じである。

正答・4肢解説・総合解説

正答：ウ．脆弱性スキャンは潜在的な弱点を広く検出することを重視し、ペネトレーションテストは定めた範囲で実際の悪用可能性や攻撃経路を検証する。
ア：どちらも実施形態は多様であり、この区分では説明できない。
イ：能動的なセキュリティテストはいずれも適切な承認と範囲定義が必要である。
ウ：両者は目的と深さが異なり、スキャン結果を踏まえて手動検証や攻撃連鎖を確認することがある。
エ：テストの深さや目的、手動検証の程度などに違いがある。
総合解説：診断手法は一つで全てを保証できない。スキャン、設定確認、手動テスト、ペネトレーションテストを目的に応じて組み合わせる。

Q104 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

本番ネットワークに対するペネトレーションテストを開始する前に最も重要な事項はどれか。
ア．テスト担当者だけで対象を当日に決める。
イ．検知されないよう運用部門には一切知らせないことを常に必須とする。
ウ．成果物を残さないことを優先する。
エ．対象、期間、許可する手法、禁止事項、連絡先、停止条件などを含む承認済みのスコープとルールを明確にする。

正答・4肢解説・総合解説

正答：エ．対象、期間、許可する手法、禁止事項、連絡先、停止条件などを含む承認済みのスコープとルールを明確にする。
ア：無断の範囲変更は業務影響や法的問題を生み得る。
イ：演習目的によって秘匿範囲は変わるが、正当な承認・緊急連絡体制は必要である。
ウ：結果、証跡、影響、推奨対策を記録することが重要である。
エ：能動テストは障害やデータ影響を生む可能性があるため、事前承認とRules of Engagementの明確化が不可欠である。
総合解説：テストの技術より先に、権限・スコープ・停止条件・情報取扱いを定める。これが安全性と法的正当性の前提になる。

Q105 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

脆弱性スキャナが重大度Highの結果を出した場合の対応として適切なものはどれか。
ア．資産・バージョン・設定・到達可能性などを確認し、必要に応じて手動検証して真偽と実際の影響を評価する。
イ．Highなら必ず実際に悪用可能なので検証は不要である。
ウ．Highは全て誤検知なので無視する。
エ．スコアを下げるためスキャナのルールを削除する。

正答・4肢解説・総合解説

正答：ア．資産・バージョン・設定・到達可能性などを確認し、必要に応じて手動検証して真偽と実際の影響を評価する。
ア：自動スキャンには誤検知や環境依存の差があるため、重要な結果は裏付けを取る。
イ：自動判定だけで実環境の悪用可能性を断定できない。
ウ：重大な真の脆弱性を見逃す危険がある。
エ：結果を見えなくしても脆弱性は解消しない。
総合解説：自動診断は効率的だが、最終的なリスク判断では証拠、構成、露出、業務影響を確認する。

Q106 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

認証情報を用いた脆弱性スキャン（credentialed scan）の特徴として最も適切なものはどれか。
ア．必ず攻撃コードを実行し、管理者権限を奪取する。
イ．対象ホストへ正当にログインしてローカルのパッケージや設定を確認できるため、外部からの観測だけでは分かりにくい情報も評価しやすい。
ウ．ネットワークに接続せず、紙の設計書だけを読む。
エ．認証情報を使うため、結果に誤りが生じる可能性はゼロになる。

正答・4肢解説・総合解説

正答：イ．対象ホストへ正当にログインしてローカルのパッケージや設定を確認できるため、外部からの観測だけでは分かりにくい情報も評価しやすい。
ア：認証付きスキャンは必ずしも侵入・権限奪取を行うものではない。
イ：認証付きスキャンは内部状態へアクセスできるため、パッチや設定の確認精度を高められる場合がある。
ウ：これは認証付きスキャンの説明ではない。
エ：認証付きでも検出漏れや誤判定はあり得る。
総合解説：外部視点と内部視点は補完関係にある。目的と権限に応じて認証付き・非認証スキャンを使い分ける。

Q107 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

24時間稼働の決済システムへ負荷の高い診断を実施したい。最も適切な計画はどれか。
ア．診断精度を上げるため、予告なく最大並列数で全ポートへ攻撃する。
イ．本番では一切の診断をしてはならず、永続的に未確認のままとする。
ウ．業務影響を事前評価し、許可された時間帯・レート・対象・停止条件を設定し、監視担当と連絡できる体制で実施する。
エ．障害が起きても原因調査をしないことを事前合意する。

正答・4肢解説・総合解説

正答：ウ．業務影響を事前評価し、許可された時間帯・レート・対象・停止条件を設定し、監視担当と連絡できる体制で実施する。
ア：本番障害を誘発する危険があり、承認済みルールに反する可能性が高い。
イ：本番固有の問題を確認する必要がある場合もあり、リスクを管理したテスト計画が重要である。
ウ：本番テストは可用性への影響を管理しながら、承認済み条件内で実施する必要がある。
エ：停止・復旧・エスカレーション手順を明確にするべきである。
総合解説：セキュリティテスト自体がリスク源になり得る。安全な実施条件、監視、停止判断、バックアウト手順を計画に含める。

Q108 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

脆弱性診断で認証回避が見つかり、開発部門から『修正済み』との連絡を受けた。クローズ前の対応として最も適切なものはどれか。
ア．担当者が修正済みと言えば証拠なしで即時クローズする。
イ．脆弱性が直っていても、同じ報告を永久に未解決のまま残す。
ウ．再テストでは元の脆弱性と無関係なサービスを停止することだけ確認する。
エ．元の再現手順で脆弱性が解消したことを再テストし、関連機能に新たな問題がないか必要な回帰確認も行う。

正答・4肢解説・総合解説

正答：エ．元の再現手順で脆弱性が解消したことを再テストし、関連機能に新たな問題がないか必要な回帰確認も行う。
ア：修正の有効性が検証されていない。
イ：再テストで解消を確認できれば、証跡を残して適切に状態更新する。
ウ：修正対象と影響範囲を直接確認すべきである。
エ：修正報告だけでなく、実際の再テストで是正の有効性を確認する。
総合解説：脆弱性管理は『発見→修正依頼』で終わらず、『是正確認→記録→必要な回帰確認』まで閉ループにする。

Q109 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

ポートスキャンで管理用サービスが外部公開されていることが分かった。この事実だけからの評価として最も適切なものはどれか。
ア．露出は攻撃面の拡大を示すため調査対象だが、それだけで『侵害済み』や『必ず脆弱』と断定せず、認証方式・バージョン・設定・到達制御を確認する。
イ．ポートが開いていれば必ず既に侵害されている。
ウ．管理用サービスは外部公開されていてもセキュリティ評価の対象外である。
エ．ポート番号だけで使用中ソフトウェアの正確なバージョンと設定を必ず特定できる。

正答・4肢解説・総合解説

正答：ア．露出は攻撃面の拡大を示すため調査対象だが、それだけで『侵害済み』や『必ず脆弱』と断定せず、認証方式・バージョン・設定・到達制御を確認する。
ア：公開サービスの発見は重要な観測結果だが、脆弱性の成立や侵害事実は追加検証が必要である。
イ：開放ポートだけで侵害事実は確定しない。
ウ：管理面は高権限につながるため重要な評価対象である。
エ：ポート番号から断定はできず、追加の情報収集が必要である。
総合解説：診断では『観測事実』『推定』『確認済み脆弱性』『侵害証拠』を区別して報告すると、過大評価・過小評価を避けやすい。

Q110 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

単体では中程度の脆弱性が複数見つかった。Aで一般利用者権限を得た後、Bで権限昇格し、Cを経由して機密DBへ到達できる可能性がある。評価として最も適切なものはどれか。
ア．個々がCriticalでないので組合せは無視する。
イ．個別スコアだけでなく、許可された範囲で攻撃連鎖の成立条件と到達可能な影響を検証し、複合リスクとして報告する。
ウ．影響を示すため本番機密DBの全データを必ず外部へ持ち出す。
エ．脆弱性BだけをCVE番号順に並べ直せば攻撃連鎖の評価になる。

正答・4肢解説・総合解説

正答：イ．個別スコアだけでなく、許可された範囲で攻撃連鎖の成立条件と到達可能な影響を検証し、複合リスクとして報告する。
ア：連鎖による権限拡大や重要資産到達を見落とす。
イ：複数の弱点を組み合わせると単体評価を超える影響になるため、攻撃経路を含めて評価する。
ウ：必要最小限の検証とルール遵守が原則で、実データ持出しは不要かつ危険である。
エ：攻撃経路は前提条件と到達可能性の連鎖を評価する必要がある。
総合解説：ペネトレーションテストの価値の一つは、個別指摘を越えて『どこまで到達できるか』を検証できる点にある。ただし承認範囲と安全性を守る。

Q111 3-4 脆弱性評価・診断 / 脆弱性診断・ペネトレーションテスト

外部診断会社から『危険な脆弱性あり』という一文だけの報告を受けた。適切な改善要求はどれか。
ア．製品名や対象を削除し、危険という表現だけを強くする。
イ．全ての指摘を同じ重大度にして説明を省く。
ウ．対象、観測証拠、再現条件、影響、重大度根拠、推奨対策、必要に応じて再テスト方法を記載させる。
エ．再現条件を一切残さず、担当者の記憶だけで管理する。

正答・4肢解説・総合解説

正答：ウ．対象、観測証拠、再現条件、影響、重大度根拠、推奨対策、必要に応じて再テスト方法を記載させる。
ア：対応対象が特定できず、実務的な報告にならない。
イ：リスク差が分からず、優先順位付けができない。
ウ：修正・優先順位付け・再現確認に使える具体的な報告が必要である。
エ：証拠と再現性が失われ、検証・監査が困難になる。
総合解説：診断結果は単なる一覧ではなく、技術者が再現・修正し、管理者が優先順位を判断できるだけの根拠を持つべきである。

Q112 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

SAST（Static Application Security Testing）の説明として最も適切なものはどれか。
ア．実行中Webアプリへ外部からHTTPリクエストだけを送って評価する。
イ．ランダム入力を大量投入してクラッシュだけを探すことと同義である。
ウ．人手による脅威モデリングを完全に自動化する標準である。
エ．アプリケーションを実行せず、ソースコードや中間表現などを解析して潜在的なセキュリティ欠陥を探す。

正答・4肢解説・総合解説

正答：エ．アプリケーションを実行せず、ソースコードや中間表現などを解析して潜在的なセキュリティ欠陥を探す。
ア：これはDASTの代表的な形である。
イ：これはファジングの一形態に近い。
ウ：SASTはコード解析手法であり、脅威モデリングそのものではない。
エ：SASTは静的なコード解析を用いるホワイトボックス寄りの手法で、実装段階から適用しやすい。
総合解説：SASTは早期導入しやすい一方、実行時の状態や業務文脈を十分に理解できない場合がある。

Q113 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

DAST（Dynamic Application Security Testing）の特徴として最も適切なものはどれか。
ア．実行中のアプリケーションに外部から入力やリクエストを与え、応答を観測して脆弱性を検出する。
イ．ソースコードを一行も実行せずにデータフローだけ解析する。
ウ．CVE IDを発行するためだけの審査である。
エ．バックアップ媒体の復元速度だけを測る。

正答・4肢解説・総合解説

正答：ア．実行中のアプリケーションに外部から入力やリクエストを与え、応答を観測して脆弱性を検出する。
ア：DASTはソースコードを直接参照せず、実行中アプリケーションの外部挙動を評価するブラックボックス型の手法である。
イ：これはSASTの特徴である。
ウ：DASTは脆弱性検出のテスト手法でありCVE発行手続ではない。
エ：これはレジリエンスや復旧テストでありDASTではない。
総合解説：DASTは実際の配置・設定を含む挙動を評価できるが、内部コードの位置特定や未到達経路の分析には限界がある。

Q114 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

ファジングの基本的な考え方として最も適切なものはどれか。
ア．既知の正しい入力だけを1回送信し、正常終了だけ確認する。
イ．大量の多様な入力、境界値、予期しない形式などを自動的に与え、クラッシュや異常応答などから欠陥を探す。
ウ．ソースコードの著作権表示だけを確認する。
エ．攻撃者の氏名をOSINTで特定する。

正答・4肢解説・総合解説

正答：イ．大量の多様な入力、境界値、予期しない形式などを自動的に与え、クラッシュや異常応答などから欠陥を探す。
ア：異常入力や広い入力空間を探索するというファジングの狙いを満たさない。
イ：人手で全入力を試す代わりに、多数の入力を生成・投入して異常を探索する。
ウ：セキュリティ欠陥探索とは関係がない。
エ：これは脅威インテリジェンスの領域である。
総合解説：ファジングは入力空間が大きい箇所やパーサ、プロトコル処理などの欠陥発見に有効だが、異常の原因分析と再現確認が必要である。

Q115 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

SASTツールが大量の警告を出した。対応として最も適切なものはどれか。
ア．全警告が必ず脆弱性なので、内容を見ず全コードを書き直す。
イ．誤検知が1件でもあればSASTを永久に廃止する。
ウ．データフローや実際の呼出し条件を確認して真の脆弱性かをトリアージし、ルール調整や手動レビューと組み合わせる。
エ．警告数を減らすため、重要ルールを無条件に無効化する。

正答・4肢解説・総合解説

正答：ウ．データフローや実際の呼出し条件を確認して真の脆弱性かをトリアージし、ルール調整や手動レビューと組み合わせる。
ア：自動解析には誤検知があり、優先順位や根拠確認が必要である。
イ：限界を理解して補完的に利用するのが適切である。
ウ：SASTは効率的だが誤検知を含み得るため、結果の文脈検証が必要である。
エ：見かけの件数だけ減らしてもリスク低減にはならない。
総合解説：自動ツールは『判断を支援するもの』として使う。高リスク経路を優先し、誤検知抑制と真陽性の見逃し防止を両立する。

Q116 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

DASTがSASTより直接確認しやすい事項はどれか。
ア．実行されないコード中に存在する潜在的な危険関数への全データフロー。
イ．コンパイル前ソースコードに含まれる到達不能な秘密値の全箇所。
ウ．設計書に記載されていない将来要件。
エ．実際に配置されたWebアプリケーションのHTTP応答、認証挙動、セキュリティヘッダ、サーバ設定に起因する外部から観測可能な問題。

正答・4肢解説・総合解説

正答：エ．実際に配置されたWebアプリケーションのHTTP応答、認証挙動、セキュリティヘッダ、サーバ設定に起因する外部から観測可能な問題。
ア：未実行経路のコード解析はSASTの方が向く。
イ：ソースに直接アクセスしないDASTでは把握しにくい。
ウ：DASTは将来要件を推測する手法ではない。
エ：DASTは稼働中システムへ外部からアクセスするため、デプロイ後の挙動を直接確認しやすい。
総合解説：SASTは内部コード、DASTは稼働中の外部挙動という観点が異なる。どちらか一方だけで包括的な保証にはならない。

Q117 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

CIではSASTを実施しているが、本番相当環境での認証設定ミスやリバースプロキシ設定不備が繰り返し発生している。改善策として最も適切なものはどれか。
ア．SASTを継続しつつ、本番相当環境へDASTや設定検証を追加し、コードと実行環境の両面を確認する。
イ．SASTの警告閾値だけを下げ、実行環境は確認しない。
ウ．DASTだけに切り替え、ソースコード中の潜在欠陥は確認しない。
エ．セキュリティテストを廃止し、本番障害が出たときだけ調べる。

正答・4肢解説・総合解説

正答：ア．SASTを継続しつつ、本番相当環境へDASTや設定検証を追加し、コードと実行環境の両面を確認する。
ア：コード解析だけではデプロイ後設定の問題を十分に検出できないため、動的検証を補完する。
イ：設定ミスの検出範囲は改善しない。
ウ：今度は静的解析の利点を失う。
エ：予防的検証を失い、リスクが高まる。
総合解説：異なる観点のテストを重ねるDefense in Depthが有効である。SAST、DAST、SCA、設定検査、手動レビューは役割が異なる。

Q118 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

ファジング中に同じ入力で再現するクラッシュが見つかった。次の対応として最も適切なものはどれか。
ア．クラッシュしたという事実だけで必ず遠隔コード実行可能と断定する。
イ．再現入力を保存し、スタックトレースやメモリ状態などを解析して原因とセキュリティ影響を評価し、修正後に再テストする。
ウ．再現入力を削除して二度と検証できないようにする。
エ．異常が出たのでファザーの実行ログを全て破棄する。

正答・4肢解説・総合解説

正答：イ．再現入力を保存し、スタックトレースやメモリ状態などを解析して原因とセキュリティ影響を評価し、修正後に再テストする。
ア：クラッシュと任意コード実行は同義ではない。
イ：クラッシュは手掛かりであり、再現性と根本原因、悪用可能性を分析して初めて脆弱性評価につながる。
ウ：原因分析と修正確認が困難になる。
エ：入力・ログ・環境情報はトリアージに重要である。
総合解説：ファジングは『異常を見つける』工程であり、その後に最小再現、原因特定、重大度評価、回帰テストを行う。

Q119 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

送金APIは入力値の型や認証処理に問題がないが、『承認者自身が自分の申請を承認できる』という業務ルール違反がある。検出方法として最も適切なものはどれか。
ア．ファジングでランダム文字列を増やせば必ず職務分離違反を検出できる。
イ．CVE IDを取得すれば自動的に承認フローが修正される。
ウ．自動SAST/DASTだけに依存せず、権限モデルと業務要件を理解した手動コードレビュー・シナリオテストを組み合わせる。
エ．TLSを有効化すれば承認ロジックの欠陥は消える。

正答・4肢解説・総合解説

正答：ウ．自動SAST/DASTだけに依存せず、権限モデルと業務要件を理解した手動コードレビュー・シナリオテストを組み合わせる。
ア：入力異常探索だけでは業務ルールの意味を理解できない。
イ：CVEは識別体系であり、アプリケーションロジックを修正しない。
ウ：業務ロジック欠陥は文脈理解が必要で、自動ツールだけでは見逃しやすい。
エ：通信路保護と業務認可ロジックは別問題である。
総合解説：セキュリティテストでは機械的な弱点検出と、人が理解する業務文脈の両方が必要である。

Q120 3-4 脆弱性評価・診断 / SAST・DAST・ファジング

新規Webサービスで、開発初期からコード欠陥を早く検出し、結合後には実際のWeb挙動を確認し、入力処理の頑健性も広く試したい。組合せとして最も適切なものはどれか。
ア．全工程でCVE検索だけ行い、実システムのテストはしない。
イ．本番公開後にだけSASTを1回実施し、それ以外は不要とする。
ウ．DASTをソースコードが存在しない設計段階だけで実施する。
エ．実装段階でSAST、稼働するテスト環境でDAST、入力処理やパーサ等にはファジングを適用し、結果を統合してトリアージする。

正答・4肢解説・総合解説

正答：エ．実装段階でSAST、稼働するテスト環境でDAST、入力処理やパーサ等にはファジングを適用し、結果を統合してトリアージする。
ア：既知脆弱性情報だけでは自社実装・設定の欠陥を検証できない。
イ：早期検出・実行環境・入力頑健性の目的を満たさない。
ウ：DASTには動作する対象が必要である。
エ：各手法の観測点が異なるため、SDLCの適切な位置に配置して補完する。
総合解説：テスト戦略は手法名ではなく、どの工程で何を観測したいかから設計する。

Q121 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

Lockheed MartinのCyber Kill Chainで、攻撃者が標的へ悪性ファイルやリンクなどを届ける段階はどれか。
ア．Delivery（配送）。
イ．Reconnaissance（偵察）。
ウ．Installation（インストール）。
エ．Actions on Objectives（目的達成行動）。

正答・4肢解説・総合解説

正答：ア．Delivery（配送）。
ア：Deliveryは攻撃用コンテンツを標的へ届ける段階である。
イ：標的に関する情報を収集する段階である。
ウ：標的環境へ悪性コンポーネント等を設置する段階である。
エ：攻撃者が最終目的に向けた行動を実施する段階である。
総合解説：Cyber Kill Chainは侵入活動を複数段階で捉え、早い段階で妨害できれば後続の目的達成を阻止しやすいという分析枠組みである。

Q122 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

MITRE ATT&CKにおけるtactic（戦術）の意味として最も適切なものはどれか。
ア．特定製品に存在するCVE番号だけを表す。
イ．攻撃者がその行動を行う戦術的な目的、すなわち『なぜ（why）』を表す。
ウ．ログファイルの保存形式を表す。
エ．CVSSのBase Scoreを算出する数式を表す。

正答・4肢解説・総合解説

正答：イ．攻撃者がその行動を行う戦術的な目的、すなわち『なぜ（why）』を表す。
ア：tacticは脆弱性識別子ではない。
イ：ATT&CKのtacticは攻撃者の目標・目的を表し、techniqueはその目的を達成する方法を表す。
ウ：ATT&CKの戦術概念とは異なる。
エ：ATT&CKとCVSSは目的が異なる。
総合解説：ATT&CKを読むときは、tactic=目的、technique/sub-technique=方法、procedure=実際の攻撃者やソフトウェアによる具体的実装例、という粒度を意識する。

Q123 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

MITRE ATT&CKの説明として最も適切なものはどれか。
ア．全ての攻撃を必ず7段階の直線順序で表す唯一のモデルである。
イ．脆弱性の深刻度を0〜10で算定する仕組みである。
ウ．実世界で観測された攻撃者の戦術・技術を整理した、公開利用可能な知識ベースである。
エ．電子証明書の失効情報を配布するプロトコルである。

正答・4肢解説・総合解説

正答：ウ．実世界で観測された攻撃者の戦術・技術を整理した、公開利用可能な知識ベースである。
ア：7段階の直線モデルはCyber Kill Chainの説明に近く、ATT&CKは行動技術をマトリクス等で整理する。
イ：それはCVSSの役割である。
ウ：ATT&CKは実観測に基づく攻撃行動の共通語彙・知識ベースとして利用される。
エ：ATT&CKはPKIプロトコルではない。
総合解説：ATT&CKは検知ルール、脅威ハンティング、対策カバレッジ、インシデント分析などで共通語彙として使える。

Q124 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

MITRE ATT&CKのInitial AccessとExecutionの違いとして適切なものはどれか。
ア．Initial Accessはデータ持出し、Executionはバックアップ復元を意味する。
イ．両者は常に同一イベントであり区別する意味がない。
ウ．Executionは攻撃前の企業情報収集だけを意味する。
エ．Initial Accessは標的環境へ最初の足掛かりを得る目的、Executionは悪性コードやコマンドを実行する目的を表す。

正答・4肢解説・総合解説

正答：エ．Initial Accessは標的環境へ最初の足掛かりを得る目的、Executionは悪性コードやコマンドを実行する目的を表す。
ア：それぞれのtacticの意味と一致しない。
イ：同時に起こる場合があっても分析上の目的は異なる。
ウ：攻撃前情報収集はReconnaissanceに該当する。
エ：侵入の入口を得ることと、コードを動かすことは別の戦術的目的として整理される。
総合解説：ATT&CKでは攻撃を目的別に分解して観測するため、同じアラートでもどの戦術・技術に対応するかを整理すると検知の抜けを分析しやすい。

Q125 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

インシデントでPowerShellの不審実行が確認され、ATT&CKの特定techniqueへマッピングできた。この事実だけから『特定APTグループの犯行』と断定する判断は適切か。
ア．不適切である。同じtechniqueは複数の攻撃者や管理用途でも使われ得るため、帰属には追加の証拠と複数の一致点が必要である。
イ．適切である。1つのtechniqueは世界で1グループしか使えない。
ウ．適切である。ATT&CK IDは攻撃者の実名を暗号化した値である。
エ．不適切だが、理由はATT&CKがネットワーク防御に一切使えないからである。

正答・4肢解説・総合解説

正答：ア．不適切である。同じtechniqueは複数の攻撃者や管理用途でも使われ得るため、帰属には追加の証拠と複数の一致点が必要である。
ア：ATT&CKマッピングは行動を共通語彙で表すもので、単一techniqueが攻撃者の一意識別子になるわけではない。
イ：ATT&CKのtechniqueは多くの攻撃者が共有して使用し得る。
ウ：ATT&CK IDは戦術・技術等を識別するIDである。
エ：ATT&CKは防御・検知・脅威分析に広く利用できる。
総合解説：行動マッピングとアトリビューションは別問題である。帰属ではインフラ、時系列、マルウェア、被害対象、複数TTPなどの総合評価が必要になる。

Q126 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

ATT&CKでCommand and Control（C2）とExfiltrationを区別する説明として最も適切なものはどれか。
ア．C2は必ずデータ破壊、Exfiltrationは必ずパスワード変更を意味する。
イ．C2は侵害端末との制御通信を確立・維持する目的、Exfiltrationは標的環境からデータを持ち出す目的を表す。
ウ．C2とExfiltrationは完全に同義で、ATT&CKでも区別されない。
エ．Exfiltrationは攻撃前のOSINTだけを意味する。

正答・4肢解説・総合解説

正答：イ．C2は侵害端末との制御通信を確立・維持する目的、Exfiltrationは標的環境からデータを持ち出す目的を表す。
ア：それぞれの戦術目的と一致しない。
イ：両者が同じ通信路を使う場合でも、戦術的な目的は異なる。
ウ：ATT&CKでは別のtacticとして整理される。
エ：攻撃前の情報収集はReconnaissanceである。
総合解説：ネットワーク分析では『通信がある』だけでなく、その通信が制御、収集、持出しなど何の目的を担うかを他ログと併せて判断する。

Q127 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

侵害された一般社員PCから、盗まれた資格情報を使って別サーバへ接続し、さらに管理サーバへ移動した。この行動をATT&CKの観点で最も直接的に表すtacticはどれか。
ア．Reconnaissance（偵察）。
イ．Resource Development（攻撃資源開発）。
ウ．Lateral Movement（横展開）。
エ．Impact（影響）。

正答・4肢解説・総合解説

正答：ウ．Lateral Movement（横展開）。
ア：攻撃前の情報収集が主目的ではない。
イ：攻撃用インフラ等の準備が主目的ではない。
ウ：侵害済み環境内で別のシステムへ移動して到達範囲を広げる行動はLateral Movementに該当する。
エ：破壊・妨害等の最終的影響が主目的の記述ではない。
総合解説：横展開では認証ログ、リモートサービス利用、端末間通信を相関させると、侵害の広がりを把握しやすい。

Q128 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

SOCの検知ルールはマルウェア実行には多いが、Credential AccessやLateral Movementに対応するルールがほとんどない。改善策として最も適切なものはどれか。
ア．検知件数を増やすため同じルールを名前だけ変えて複製する。
イ．ATT&CKを使うと全攻撃を自動防止できるので、ログ収集を停止する。
ウ．不足領域を無視し、既に多いExecutionだけをさらに増やす。
エ．既存ルールをATT&CKのtactic/techniqueへマッピングしてカバレッジの偏りを可視化し、優先脅威に対する不足検知を追加する。

正答・4肢解説・総合解説

正答：エ．既存ルールをATT&CKのtactic/techniqueへマッピングしてカバレッジの偏りを可視化し、優先脅威に対する不足検知を追加する。
ア：カバレッジの質は改善しない。
イ：ATT&CKは知識ベースであり、自動的な防御製品ではない。
ウ：既知の偏りを放置することになる。
エ：ATT&CKを共通分類として使うと、検知が集中している領域と空白を体系的に確認できる。
総合解説：マッピングは目的ではなく、脅威シナリオに対する観測可能性・検知可能性を改善するための手段として使う。

Q129 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

Cyber Kill ChainとMITRE ATT&CKの使い分けとして最も適切なものはどれか。
ア．Kill Chainで侵入活動を大きな段階として捉え、ATT&CKで各段階に現れる具体的な戦術・技術を詳細化するなど、補完的に使える。
イ．両者は同じ管理団体が同一仕様として発行しており、用語も完全に同じである。
ウ．ATT&CKは脆弱性スコア、Kill Chainは暗号アルゴリズムの標準である。
エ．Kill Chainを使う場合はATT&CKの利用が禁止される。

正答・4肢解説・総合解説

正答：ア．Kill Chainで侵入活動を大きな段階として捉え、ATT&CKで各段階に現れる具体的な戦術・技術を詳細化するなど、補完的に使える。
ア：両者は粒度や構造が異なるため、どちらか一方を絶対視せず分析目的に応じて組み合わせられる。
イ：Lockheed MartinのKill ChainとMITRE ATT&CKは別の枠組みである。
ウ：いずれもその説明には当たらない。
エ：相互排他的な規格ではない。
総合解説：高レベルの攻撃ライフサイクルと、詳細な行動技術の辞書を組み合わせると、説明・検知・対策設計の粒度を調整しやすい。

Q130 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

実際の攻撃が、資格情報窃取と横展開を何度も往復しながら進行した。『攻撃は必ず一方向の7段階を一度ずつ通る』と仮定して分析する問題点はどれか。
ア．直線モデルを使うとログの時刻が必ず消える。
イ．現実の攻撃は段階を飛ばしたり反復したり並行したりするため、直線順序だけに固定すると行動の再訪や複数経路を見落とし得る。
ウ．7段階モデルではCVE番号を保存できないためだけである。
エ．実攻撃は必ず1段階しかないので、7段階は多すぎる。

正答・4肢解説・総合解説

正答：イ．現実の攻撃は段階を飛ばしたり反復したり並行したりするため、直線順序だけに固定すると行動の再訪や複数経路を見落とし得る。
ア：モデル利用自体がログを削除するわけではない。
イ：Kill Chainは有用な抽象化だが、全ての現実攻撃が厳密な単一線形順序になるとは限らない。
ウ：主な問題は攻撃進行の複雑さを過度に単純化する点にある。
エ：実攻撃は複数行動を含み得る。
総合解説：分析モデルは現実を簡略化する。モデルの前提を理解し、必要ならATT&CKや攻撃グラフ、タイムライン分析で補完する。

Q131 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

EDRで不審スクリプト実行、認証ログで複数サーバへの接続、プロキシで外部への周期通信が確認された。ATT&CKを使う最も適切な分析はどれか。
ア．周期通信だけを見て他ログを削除する。
イ．1つでもATT&CKに対応すれば自動的に全端末を侵害済みと断定する。
ウ．各観測をExecution、Lateral Movement、Command and Controlなどの戦術・技術へ対応付け、時系列と端末間関係を統合して攻撃経路と検知抜けを整理する。
エ．ATT&CK IDをCVE IDへ置き換えれば攻撃経路が完成する。

正答・4肢解説・総合解説

正答：ウ．各観測をExecution、Lateral Movement、Command and Controlなどの戦術・技術へ対応付け、時系列と端末間関係を統合して攻撃経路と検知抜けを整理する。
ア：複数ソースの相関情報を失う。
イ：マッピングと侵害事実の確定は別であり、証拠に基づく範囲評価が必要である。
ウ：ATT&CKは異なるログの観測を攻撃者行動の共通語彙へ変換し、全体像の整理に使える。
エ：ATT&CK技術とCVE脆弱性は異なる種類の情報である。
総合解説：ATT&CKはアラート分類に留めず、複数証跡を行動連鎖として関連付けると、調査優先順位や不足データを明確にできる。

Q132 3-5 脅威分析・インテリジェンス / サイバーキルチェーン・MITRE ATT&CK

脅威分析で優先するATT&CK technique群を決めた後、対策の有効性を評価したい。最も適切な進め方はどれか。
ア．technique名を一覧に書けば対策済みとみなす。
イ．全techniqueを同じ重要度で扱い、組織の脅威モデルは考慮しない。
ウ．検知テストを避け、製品カタログの記載だけで判断する。
エ．各techniqueに対し必要なテレメトリ、予防策、検知ロジック、対応手順を対応付け、演習やテストで実際に観測・検知・対応できるか確認する。

正答・4肢解説・総合解説

正答：エ．各techniqueに対し必要なテレメトリ、予防策、検知ロジック、対応手順を対応付け、演習やテストで実際に観測・検知・対応できるか確認する。
ア：名前の対応付けだけでは実際の予防・検知能力を保証しない。
イ：優先脅威や資産特性に応じた重点化が必要である。
ウ：実環境で期待する証跡と検知が得られるか検証するべきである。
エ：ATT&CKマッピングを具体的な防御能力と検証へ結び付けることで、形式的な一覧から実効性評価へ進められる。
総合解説：ATT&CKは防御能力を説明・比較する共通語彙として有用だが、最終的には自組織環境でのテストが必要である。

Q133 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

OSINT（Open Source Intelligence）の説明として最も適切なものはどれか。
ア．一般に公開されている情報源を収集・評価・分析し、意思決定に使える情報へ整理する活動である。
イ．対象組織へ必ず侵入して非公開ファイルを取得する活動である。
ウ．暗号鍵を総当たりで解読する手法だけを指す。
エ．CVE番号をCVSSへ変換する計算式である。

正答・4肢解説・総合解説

正答：ア．一般に公開されている情報源を収集・評価・分析し、意思決定に使える情報へ整理する活動である。
ア：公開Web、公開技術データベース、公開文書などはOSINTの代表的な情報源になり得る。
イ：無断侵入は公開情報の分析であるOSINTとは異なる。
ウ：OSINTは暗号解読手法の名称ではない。
エ：OSINTと脆弱性スコアリングは別概念である。
総合解説：公開情報でも組み合わせると機微情報になり得るため、情報源・取得時刻・信頼性・法的条件を意識して扱う。

Q134 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

公開検索エンジンや公開証明書データベースだけを調べる行為と、対象IPへ直接ポートスキャンする行為の違いとして適切なものはどれか。
ア．どちらも対象へ同じパケットを送るため完全に同一である。
イ．前者は公開情報源の検索であり、後者は対象インフラへ通信を送る能動的な偵察である。
ウ．公開情報検索だけが必ず違法で、ポートスキャンは常に無条件で合法である。
エ．能動スキャンはOSINTより必ず情報量が少ない。

正答・4肢解説・総合解説

正答：イ．前者は公開情報源の検索であり、後者は対象インフラへ通信を送る能動的な偵察である。
ア：公開データベース検索は対象へ直接接続しない場合がある。
イ：ATT&CKでもSearch Open Technical Databases等とActive Scanningは別の偵察技術として整理される。
ウ：法的評価は状況・権限・法域に依存し、このように一律ではない。
エ：取得できる情報量は対象・手法によるため一律に比較できない。
総合解説：偵察手法を分類すると、対象への接触有無、検知可能性、承認要件、リスクを区別しやすい。

Q135 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

STIXとTAXIIの関係として最も適切なものはどれか。
ア．STIXは暗号方式、TAXIIはパスワードハッシュ方式である。
イ．STIXとTAXIIはCVE IDを採番する同一サービスの別名である。
ウ．STIXはサイバー脅威情報を構造化して表現する言語・データモデルで、TAXIIはそのような脅威情報を交換するためのアプリケーション層プロトコルである。
エ．TAXIIは脆弱性スコア、STIXはOSのパッチ番号だけを表す。

正答・4肢解説・総合解説

正答：ウ．STIXはサイバー脅威情報を構造化して表現する言語・データモデルで、TAXIIはそのような脅威情報を交換するためのアプリケーション層プロトコルである。
ア：いずれもその種の暗号アルゴリズムではない。
イ：CVE Programとは別の標準である。
ウ：『何をどう表すか』と『どう交換するか』の役割が補完的である。
エ：両者の役割を誤っている。
総合解説：STIXで脅威情報の構造をそろえ、TAXIIでAPIベースの交換を行う構成が代表的である。

Q136 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

自社名で検索したところ、公開コードリポジトリに古いAPIキーらしき文字列が見つかった。防御側の対応として最も適切なものはどれか。
ア．公開情報なので機密情報である可能性はゼロとして無視する。
イ．検索結果を隠すためリポジトリを削除するだけで、キーは永続利用する。
ウ．漏えいしたキーを全社員へメールで再配布する。
エ．真に自社の有効な秘密情報かを確認し、有効なら失効・ローテーションし、利用ログを調査して公開経路と再発防止策を是正する。

正答・4肢解説・総合解説

正答：エ．真に自社の有効な秘密情報かを確認し、有効なら失効・ローテーションし、利用ログを調査して公開経路と再発防止策を是正する。
ア：公開されてしまった秘密情報は機密性を失っている可能性があり、速やかな確認が必要である。
イ：既に取得されている可能性があるため、削除だけでは不十分である。
ウ：漏えい範囲を拡大する。
エ：公開リポジトリは攻撃者も検索できるため、漏えい候補を単なる検索結果で終わらせず秘密管理へつなげる。
総合解説：OSINTは攻撃者だけでなく防御側も外部露出の発見に使える。秘密は『削除』だけでなく『失効・置換・利用確認』まで行う。

Q137 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

単なるIPアドレス一覧ではなくSTIX形式で脅威情報を共有する利点として適切なものはどれか。
ア．Indicator、Malware、Threat Actor等のオブジェクトと関係を構造化し、指標の意味や関連文脈を機械処理しやすくできる。
イ．共有する全IPアドレスを自動的に安全なアドレスへ変更する。
ウ．STIXを使えば情報源の誤りや陳腐化が絶対に発生しない。
エ．STIXは画像ファイル専用形式なので、脅威情報の関係は表せない。

正答・4肢解説・総合解説

正答：ア．Indicator、Malware、Threat Actor等のオブジェクトと関係を構造化し、指標の意味や関連文脈を機械処理しやすくできる。
ア：STIXはIOC単体だけでなく、脅威情報の文脈と関係を共通構造で表せる。
イ：STIXは防御装置そのものではない。
ウ：構造化しても情報品質・有効期限の管理は必要である。
エ：STIXは脅威・観測情報を構造化するための仕様である。
総合解説：IOCは寿命が短い場合がある。STIXで関連するマルウェア、キャンペーン、観測時刻、関係等を持たせると分析価値が高まる。

Q138 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

複数組織間でSTIX 2.1の脅威情報をAPI経由で継続的に交換したい。適した標準はどれか。
ア．CVSS 4.0。
イ．TAXII 2.1。
ウ．CWE。
エ．Cyber Kill Chain。

正答・4肢解説・総合解説

正答：イ．TAXII 2.1。
ア：CVSSは脆弱性の特性・深刻度を評価する仕組みである。
イ：TAXII 2.1はサイバー脅威情報を簡潔かつスケーラブルに交換するRESTful APIを定義する。
ウ：CWEは弱点分類であり情報交換プロトコルではない。
エ：攻撃段階を理解するフレームワークで、API交換プロトコルではない。
総合解説：STIXをデータ表現、TAXIIを交換プロトコルとして組み合わせる構成を理解しておく。

Q139 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

OSINTで見つけた『悪性IP一覧』を出典・観測時刻・根拠を確認せず、FWで永久遮断する運用の評価として最も適切なものはどれか。
ア．適切である。インターネット上のIPは所有者も用途も永久に変わらない。
イ．不適切だが、理由はOSINTが防御用途に一切利用できないからである。
ウ．不適切である。IPの再割当てや誤判定があり得るため、出典、観測時刻、信頼度、組織内観測と照合し、有効期限や見直しを設けるべきである。
エ．適切である。公開された情報は必ず100%正確である。

正答・4肢解説・総合解説

正答：ウ．不適切である。IPの再割当てや誤判定があり得るため、出典、観測時刻、信頼度、組織内観測と照合し、有効期限や見直しを設けるべきである。
ア：IPの用途や割当ては変化し得る。
イ：OSINTは防御にも有用だが、品質評価が必要である。
ウ：脅威インテリジェンスは鮮度と文脈が重要で、IOCを恒久的な真実として扱うと副作用が生じる。
エ：公開情報にも誤り・古さ・文脈不足があり得る。
総合解説：情報源のprovenance、観測時刻、confidence、expirationを管理し、内部ログと突合して使うと、IOC運用の精度が上がる。

Q140 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

TAXIIで受け取ったSTIX Indicatorを自動遮断へ直結させたところ、誤遮断が増えた。改善策として最も適切なものはどれか。
ア．STIX形式なら必ず正しいので、誤遮断は利用者側の責任として無視する。
イ．全Indicatorを永久に遮断し、失効管理を廃止する。
ウ．TAXIIを使うと暗号化が不要になるため、共有経路の認証を外す。
エ．情報源の信頼度、観測時刻、Indicatorの有効期間、内部観測との一致、対象資産への影響を評価し、一定条件のみ自動化する。

正答・4肢解説・総合解説

正答：エ．情報源の信頼度、観測時刻、Indicatorの有効期間、内部観測との一致、対象資産への影響を評価し、一定条件のみ自動化する。
ア：データ形式は真偽を保証しない。
イ：IOCは陳腐化し得るため副作用が増える。
ウ：交換基盤自体の認証・通信保護も必要である。
エ：標準化された形式・交換手段と、情報の正確性・自動対処の妥当性は別問題である。
総合解説：CTIの自動化では『機械可読』と『自動実行して安全』を区別する。信頼スコア、期限、適用範囲、ロールバックを設計する。

Q141 3-5 脅威分析・インテリジェンス / OSINT・STIX/TAXII

あるドメインが攻撃インフラの疑いを持たれている。公開DNS履歴、証明書情報、公開マルウェア分析、社内プロキシログを使って調査する方法として最も適切なものはどれか。
ア．各情報の観測時刻・出典・一致点を比較し、同じインフラやキャンペーンに結び付くか仮説として評価し、単一情報だけで帰属を断定しない。
イ．検索結果の先頭1件だけで攻撃者の実名を確定する。
ウ．観測時刻が異なっても全データを同時点の事実として扱う。
エ．社内ログはOSINTではないので、相関分析に使ってはならない。

正答・4肢解説・総合解説

正答：ア．各情報の観測時刻・出典・一致点を比較し、同じインフラやキャンペーンに結び付くか仮説として評価し、単一情報だけで帰属を断定しない。
ア：複数の独立情報を相関し、時間軸と信頼性を確認することで分析の確度を高める。
イ：単一OSINTの断片だけでは帰属の確度が不足する。
ウ：インフラは変化するため時系列を無視すると誤推論につながる。
エ：公開情報と内部観測を組み合わせることで、自組織への影響評価ができる。
総合解説：脅威分析では、情報源の独立性・鮮度・信頼性を明示し、事実と推測を分けて結論を記録する。

Q142 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

脅威モデリングの実施時期として最も適切な考え方はどれか。
ア．本番侵害が起きた後に一度だけ実施し、それ以前は不要である。
イ．設計段階などSDLCの早期から実施し、アーキテクチャや脅威が変わったときに更新する。
ウ．初版を作ったらシステム変更があっても更新してはならない。
エ．脆弱性スキャナがあれば脅威モデリングは常に不要である。

正答・4肢解説・総合解説

正答：イ．設計段階などSDLCの早期から実施し、アーキテクチャや脅威が変わったときに更新する。
ア：早期に設計上の脅威を見つける利点を失う。
イ：脅威モデリングは早期に行うと設計変更コストを抑えやすく、継続的に維持することが望ましい。
ウ：脅威モデルはシステムとともに更新する必要がある。
エ：設計・信頼境界・業務文脈の脅威はスキャンだけでは十分に扱えない。
総合解説：脅威モデルは納品物ではなく、設計判断を支える生きたモデルとして扱う。

Q143 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

脅威モデリングでデータフロー図と信頼境界を明示する主な理由はどれか。
ア．図を作れば自動的に全脆弱性へパッチが適用されるから。
イ．信頼境界は暗号鍵の長さだけを示す線だから。
ウ．データや処理がどこを通り、どの境界で信頼条件や権限が変化するかを可視化して、攻撃面と必要な対策を検討しやすくする。
エ．データフローはネットワーク帯域の課金額だけを計算するため。

正答・4肢解説・総合解説

正答：ウ．データや処理がどこを通り、どの境界で信頼条件や権限が変化するかを可視化して、攻撃面と必要な対策を検討しやすくする。
ア：図は分析のためのモデルであり、修正を自動実施しない。
イ：信頼境界は信頼レベルや制御条件が変わる境界を表す。
ウ：脅威モデルでは対象システムを分解し、データフロー、主体、データストア、信頼境界などを理解することが重要である。
エ：セキュリティ上の情報の流れと境界を理解する目的がある。
総合解説：信頼境界をまたぐ入力、認証・認可、暗号化、検証、ログなどは特に脅威検討の重点になる。

Q144 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

利用者が自分のJWTのrole値を書き換え、一般利用者から管理者として処理を実行できた。この脅威をSTRIDEで最も直接的に分類するものはどれか。
ア．Information Disclosure。
イ．Denial of Service。
ウ．Repudiation。
エ．Elevation of Privilege（権限昇格）。

正答・4肢解説・総合解説

正答：エ．Elevation of Privilege（権限昇格）。
ア：主な事象は情報の閲覧ではなく不正な権限獲得である。
イ：可用性を妨害する事象ではない。
ウ：行為の否認や監査不能が主な問題ではない。
エ：本来持たない高い権限を得る行為はSTRIDEのElevation of Privilegeに該当する。
総合解説：STRIDEは脅威を漏れなく考えるためのプロンプトであり、実際のシステム文脈に当てはめて具体的な対策へ落とし込む。

Q145 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

既存システムへ外部SaaS連携と新しいAPI Gatewayを追加した。脅威モデルの扱いとして最も適切なものはどれか。
ア．新しいデータフロー、信頼境界、認証方式、外部依存関係を反映して脅威モデルを更新し、追加脅威と管理策を再評価する。
イ．初期版が承認済みなら、新しい外部接続はモデルへ追加しない。
ウ．変更のたびに過去の全脅威を削除してゼロから扱う。
エ．SaaSを使えば責任が全て外部へ移るので脅威分析は不要になる。

正答・4肢解説・総合解説

正答：ア．新しいデータフロー、信頼境界、認証方式、外部依存関係を反映して脅威モデルを更新し、追加脅威と管理策を再評価する。
ア：アーキテクチャ変更は攻撃面や信頼関係を変えるため、既存モデルの前提を見直す必要がある。
イ：モデルと実システムが乖離し、重要な脅威を見落とす。
ウ：既存の有効な知見を維持しつつ差分を評価する方が実務的である。
エ：利用組織側に残る設定、ID、データ、統合部分のリスクがある。
総合解説：脅威モデルは構成管理と連携させ、重要変更をトリガにレビューする仕組みにすると陳腐化を防げる。

Q146 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

攻撃グラフ（attack graph）を利用する主な利点として最も適切なものはどれか。
ア．全ての脆弱性を1件として数え、経路や前提条件を無視する。
イ．複数の脆弱性、権限、ネットワーク到達性などを組み合わせ、重要資産へ至る複数段階の攻撃経路を分析できる。
ウ．ネットワーク構成に関係なく全ホストが常に直接接続されていると仮定する。
エ．攻撃者の実名をグラフから自動的に断定する。

正答・4肢解説・総合解説

正答：イ．複数の脆弱性、権限、ネットワーク到達性などを組み合わせ、重要資産へ至る複数段階の攻撃経路を分析できる。
ア：攻撃グラフの価値は連鎖・到達可能性を扱う点にある。
イ：個別脆弱性の数だけでなく、脆弱性がどのように連鎖して侵入を深めるかを表現できる。
ウ：実際の到達性・制御条件をモデルへ反映する必要がある。
エ：攻撃グラフは主に潜在経路・リスク分析のためのもので、帰属を自動確定しない。
総合解説：単独では低〜中程度の弱点でも、組み合わせると重要資産へ到達できる場合がある。攻撃経路分析はこうした累積効果を可視化する。

Q147 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

攻撃グラフ上で、重要DBへ到達する5本の攻撃経路のうち4本が同じ踏み台サーバを通る。対策優先順位として合理的なものはどれか。
ア．最も利用されない経路だけを強化し、共通の踏み台は無視する。
イ．攻撃経路が複数ある場合は対策不能なので何もしない。
ウ．その踏み台サーバの脆弱性・権限・到達制御を改善すると複数経路を同時に遮断できるため、影響と実現性を確認して優先候補にする。
エ．DBのデータを削除して攻撃者の目的をなくす。

正答・4肢解説・総合解説

正答：ウ．その踏み台サーバの脆弱性・権限・到達制御を改善すると複数経路を同時に遮断できるため、影響と実現性を確認して優先候補にする。
ア：複数経路をまとめて減らす機会を逃す。
イ：経路の共通条件を断つことで全体リスクを下げられる場合がある。
ウ：多くの経路が集中する要素は、対策効果が大きいチョークポイントになり得る。
エ：業務資産を破壊することは適切なセキュリティ対策ではない。
総合解説：攻撃経路分析では『最も重大な単一脆弱性』だけでなく、複数経路に共通する条件や権限を探すと効率的なリスク低減策を選びやすい。

Q148 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

脅威モデルで100件の脅威候補が出た。優先順位付けとして最も適切なものはどれか。
ア．発見順だけで上から対応する。
イ．全て同じ重大度として扱い、資産重要度を考慮しない。
ウ．数が多いので全件を削除し、脅威ゼロとして記録する。
エ．発生可能性、影響、露出、既存管理策、必要な対策コスト等を一貫した基準で評価し、重要資産への脅威から優先する。

正答・4肢解説・総合解説

正答：エ．発生可能性、影響、露出、既存管理策、必要な対策コスト等を一貫した基準で評価し、重要資産への脅威から優先する。
ア：発見順はリスクを表さない。
イ：限られた資源を効果的に配分できない。
ウ：モデルから消しても現実の脅威は消えない。
エ：脅威モデルは列挙で終わらせず、対応判断へつなげる必要がある。
総合解説：優先順位はモデル固有の精密な数値より、判断基準を明確にし、対策の根拠を追跡できることが重要である。

Q149 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

重要サーバにはCritical脆弱性がないが、低権限端末→共有サービスアカウント→管理セグメントという複数段階で到達できることが分かった。評価として最も適切なものはどれか。
ア．個別脆弱性の最大スコアだけで安全と判断せず、権限・到達性・認証関係を含む経路全体の成立可能性と影響を評価する。
イ．Critical脆弱性が1件もないので、重要サーバへの侵入経路は存在しないと断定する。
ウ．経路上の認証関係は脆弱性ではないので分析から必ず除外する。
エ．攻撃経路分析はCVSSの代わりにCVE番号を足し算するだけでよい。

正答・4肢解説・総合解説

正答：ア．個別脆弱性の最大スコアだけで安全と判断せず、権限・到達性・認証関係を含む経路全体の成立可能性と影響を評価する。
ア：攻撃グラフ研究が示すように、複数の弱点が組み合わさることで重要資産へ到達するリスクが生じ得る。
イ：複数の中小リスクや権限関係の連鎖で到達できる場合がある。
ウ：攻撃経路は脆弱性だけでなく権限・到達性等の前提条件も重要である。
エ：経路の因果関係や前提条件を扱う必要がある。
総合解説：ネットワーク全体のリスクは、個別の脆弱性一覧の単純集計では表し切れない。攻撃経路と重要資産への到達可能性を合わせて評価する。

Q150 3-5 脅威分析・インテリジェンス / 脅威モデリング・攻撃経路分析

脅威モデルでは『外部Web→アプリ→DB』だけを想定していたが、インシデント調査で『端末→クラウド管理ID→DB』という別経路が判明した。最も適切な対応はどれか。
ア．モデルと一致しない実ログを誤りとして削除する。
イ．実インシデントの経路を脅威モデルへ反映し、前提・信頼境界・ID権限を更新して、同様の経路に対する予防・検知策を追加する。
ウ．一度承認した脅威モデルは監査証跡のため永久に変更してはならない。
エ．新経路は偶然なので、予防・検知の改善は不要とする。

正答・4肢解説・総合解説

正答：イ．実インシデントの経路を脅威モデルへ反映し、前提・信頼境界・ID権限を更新して、同様の経路に対する予防・検知策を追加する。
ア：現実の証拠をモデルに合わせて捨てるのは逆である。
イ：現実の観測をモデルへフィードバックすることで、脅威モデルの網羅性と実効性を改善できる。
ウ：履歴を残しつつ現状へ更新する必要がある。
エ：再発・類似経路の可能性を評価し対策へつなげるべきである。
総合解説：脅威モデルは設計時の仮説であり、診断・インシデント・運用変更から得た知見を戻して継続的に改善する。