0001 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：基礎

マルウェア対策ソフトの役割として、最も適切なものはどれか。

ア：既知の特徴や挙動などを利用して、不審なプログラムの検知・隔離・削除を支援する。

イ：OSやアプリケーションの脆弱性をすべて自動的に修正する。

ウ：利用者のアクセス権を職務に応じて承認する。

エ：障害発生時に必ずバックアップからデータを復元する。

答え・解説 正答：ア

ア：マルウェア対策製品はシグネチャや挙動分析などを用いて、悪性プログラムの検知や処置を支援します。

イ：マルウェア対策製品とパッチ管理は別の役割であり、脆弱性修正を全て代替するものではありません。

ウ：アクセス権の付与・承認はID・アクセス管理の領域です。

エ：バックアップ復元は復旧対策であり、マルウェア対策ソフトの主機能ではありません。

総合解説：マルウェア対策は重要ですが、単独では十分ではありません。パッチ管理、最小権限、メール・Web対策、バックアップ、監視などと組み合わせる多層的な運用が必要です。

対象：2026年度 / 基準日 2026-09-05

0002 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：基礎

セキュリティパッチを適用する主な目的として、最も適切なものはどれか。

ア：ログの保存期間を自動的に無期限へ変更する。

イ：ソフトウェアやファームウェアに存在する既知の脆弱性などを修正し、悪用されるリスクを低減する。

ウ：全利用者へ管理者権限を付与する。

エ：バックアップデータを暗号化せず公開する。

答え・解説 正答：イ

ア：パッチ適用の主目的ではありません。

イ：セキュリティパッチは既知の欠陥・脆弱性の修正を目的とし、攻撃機会の低減に役立ちます。

ウ：むしろ最小権限に反し、リスクを高めます。

エ：パッチ管理とは無関係で、情報漏えいリスクを高めます。

総合解説：パッチ管理は単なる「更新ボタンを押す作業」ではなく、対象の把握、優先順位付け、適用、結果確認まで含む継続的な管理活動です。

対象：2026年度 / 基準日 2026-09-05

0003 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：基礎

組織的なパッチ管理で、パッチ配布後に行うべき作業として最も適切なものはどれか。

ア：配布通知を送信した時点で全端末への適用完了とみなす。

イ：更新失敗を隠すために管理ログを削除する。

ウ：対象端末に実際に適用されたかを確認し、未適用端末や失敗端末を把握する。

エ：再起動が必要な更新でも、利用者へ知らせず永久に延期する。

答え・解説 正答：ウ

ア：通知や配布指示だけでは実際の適用を保証できません。

イ：失敗原因の追跡を妨げ、監査性も損ないます。

ウ：配布指示だけで完了とせず、適用結果を検証することが重要です。

エ：必要な再起動を無期限に延期すると脆弱性が残存します。

総合解説：パッチ管理では「取得・配布」と「適用済みであることの検証」を分けて管理します。資産台帳や管理ツールと照合し、未適用状態を見逃さないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0004 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：標準

同日に複数の脆弱性修正が公開された。緊急適用の優先順位を決める考え方として、最も適切なものはどれか。

ア：公開日が古いものから機械的に適用し、悪用状況や資産重要度は考慮しない。

イ：すべて同じ優先度とし、重要サーバと検証端末を区別しない。

ウ：CVSSなどの数値が同じなら、必ず全システムで同じ期限に適用する。

エ：脆弱性の深刻度だけでなく、実際の悪用状況、インターネット公開の有無、資産の重要度、代替策の有無などを総合して決める。

答え・解説 正答：エ

ア：古さだけでは現在のリスクを適切に表せません。

イ：資産の重要度や露出度を無視すると、限られた対応資源を有効に使えません。

ウ：同一脆弱性でも利用状況や公開範囲、業務影響によりリスクは異なります。

エ：リスクベースで、脆弱性と資産・露出・脅威状況を組み合わせて優先します。

総合解説：パッチ優先度は脆弱性スコアだけでなく「その組織でどれだけ悪用され得るか」で判断します。重要資産・外部公開・悪用確認済みなどは優先度を上げる要因です。

対象：2026年度 / 基準日 2026-09-05

0005 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：標準

基幹システムへ重要なセキュリティパッチを適用する際の運用として、最も適切なものはどれか。

ア：緊急度を踏まえつつ、可能な範囲で互換性確認やバックアップ・ロールバック手順を準備して適用する。

イ：セキュリティパッチなら業務影響は発生しないと決めつけ、復旧策を用意しない。

ウ：検証が必要という理由で、悪用が確認されている重大脆弱性も無期限に放置する。

エ：適用前にバックアップを削除し、旧状態へ戻せないようにする。

答え・解説 正答：ア

ア：パッチ適用による障害も業務リスクなので、緊急度と変更リスクの双方を管理します。

イ：更新によって互換性問題や停止が起こる可能性があります。

ウ：検証と迅速なリスク低減を両立させる必要があります。

エ：障害時の復旧可能性を下げる不適切な運用です。

総合解説：パッチ管理はセキュリティと可用性のトレードオフを管理する活動です。事前検証、復旧手段、適用後確認、緊急時の代替緩和策を組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0006 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：標準

利用中製品のゼロデイ脆弱性が公表されたが、修正パッチはまだ提供されていない。最も適切な対応はどれか。

ア：パッチがないため何もできないとして、外部公開を含め現状を維持する。

イ：ベンダ情報を確認し、影響機能の停止、公開範囲の縮小、アクセス制限などの暫定緩和策を講じ、修正版公開を継続監視する。

ウ：全ログを停止し、攻撃の記録が残らないようにする。

エ：脆弱性情報を見なかったことにして、資産台帳から製品を削除する。

答え・解説 正答：イ

ア：暫定緩和策が可能な場合があり、無対応は適切ではありません。

イ：パッチがない場合でも攻撃面を減らす補完策でリスクを下げ、更新情報を追跡します。

ウ：検知・調査能力を失うため逆効果です。

エ：資産管理を歪めてもリスクは消えません。

総合解説：ゼロデイ対応では、公式な緩和策、ネットワーク隔離、機能無効化、WAF等の補完策などを検討し、パッチ公開後に速やかに評価・適用します。

対象：2026年度 / 基準日 2026-09-05

0007 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：標準

OSがベンダのサポート終了を迎え、今後セキュリティ更新が原則提供されない。最も適切な対応方針はどれか。

ア：更新が来ないので脆弱性も新たに発生しないと考え、そのまま使い続ける。

イ：サポート終了製品へ全社員の管理者権限を集約する。

ウ：移行計画を立ててサポート対象製品へ更新し、移行までの間は隔離やアクセス制限などの補完策でリスクを抑える。

エ：ログ保存を停止すれば攻撃者に見つからないと考える。

答え・解説 正答：ウ

ア：サポート終了後も新たな脆弱性が発見・悪用される可能性があります。

イ：侵害時の影響を増大させます。

ウ：更新が受けられない製品は脆弱性が残存しやすいため、恒久的には移行が必要です。

エ：ログ停止は検知能力を下げるだけです。

総合解説：EOL/EOS製品は「パッチ管理できない」という構造的なリスクを持ちます。延命が必要でも、移行期限と補完統制を明確にします。

対象：2026年度 / 基準日 2026-09-05

0008 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：標準

業務アプリがマルウェア対策ソフトで検知されたが、誤検知の可能性もある。最も適切な初動はどれか。

ア：業務で使うファイルなら必ず安全なので、全社で同名ファイルを永久除外する。

イ：検知端末のログを削除して、アラートをなかったことにする。

ウ：マルウェア対策ソフトを全端末からアンインストールする。

エ：安易に除外設定せず、検知内容、ファイルの由来・署名・ハッシュ、ベンダ情報等を確認し、安全性を評価してから例外可否を判断する。

答え・解説 正答：エ

ア：業務利用の有無だけでは安全性を保証できません。

イ：原因分析と再発検知を妨げます。

ウ：一つの誤検知疑いに対して防御機能を全廃するのは過剰です。

エ：誤検知の可能性があっても、未検証で除外すると本物のマルウェアを許可する危険があります。

総合解説：例外設定は攻撃面を広げるため、根拠と範囲を限定します。署名や配布元、検体分析、ベンダ確認など複数の証拠で評価します。

対象：2026年度 / 基準日 2026-09-05

0009 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：応用

ランサムウェア被害を想定した日常運用として、最も適切な組合せはどれか。

ア：パッチ管理、最小権限、マルウェア検知、復元可能性を確認したバックアップ、監視を組み合わせる。

イ：バックアップだけ取得すれば、侵入経路や認証情報の窃取は考えなくてよい。

ウ：パッチだけ適用すれば、フィッシングや認証情報悪用への対策は不要である。

エ：マルウェア対策製品を導入したら、ログ監視や復元テストは不要である。

答え・解説 正答：ア

ア：ランサムウェアは侵入・横展開・暗号化・窃取を伴う場合があるため、多層的な予防・検知・復旧策が有効です。

イ：バックアップは復旧には有効ですが、侵入や情報窃取を防ぐものではありません。

ウ：侵入経路は脆弱性だけではありません。

エ：単一製品では検知漏れや復旧失敗に備えられません。

総合解説：ランサムウェア対策では、予防・検知・対応・復旧を一連の運用として設計します。特にバックアップは取得だけでなく、分離・保護と復元テストが重要です。

対象：2026年度 / 基準日 2026-09-05

0010 日常のセキュリティ運用 > マルウェア対策・パッチ管理 ｜ 難易度：応用

装置メーカーから、特定パッチを適用すると認定アプリが動作しなくなるため当面適用しないよう指示された。最も適切な管理はどれか。

ア：メーカー指示があるので資産台帳から対象装置を削除し、管理対象外にする。

イ：未適用の理由・対象・期限・リスクを記録し、ネットワーク制限などの代替策を設け、定期的に解消可否を見直す。

ウ：適用できないパッチが一つあるため、以後すべての更新を停止する。

エ：未適用情報を誰にも共有せず、担当者個人の記憶だけで管理する。

答え・解説 正答：イ

ア：資産を隠しても脆弱性リスクは残ります。

イ：例外は放置せず、承認されたリスクとして代替策と期限を持って管理します。

ウ：他の修正まで停止するとリスクが拡大します。

エ：引継ぎや監査ができず、例外が恒久化しやすくなります。

総合解説：業務都合で即時適用できない場合も、リスク受容・代替統制・期限・見直しを明確にします。これは「適用できない＝管理しない」ではありません。

対象：2026年度 / 基準日 2026-09-05

0011 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：基礎

セキュリティ運用におけるログの主な用途として、最も適切なものはどれか。

ア：利用者の記憶を完全に不要にする。

イ：脆弱性そのものを自動的に修正する。

ウ：システムで発生した事象を記録し、異常検知、障害・インシデント調査、監査などに利用する。

エ：バックアップデータの代わりに業務データを復元する。

答え・解説 正答：ウ

ア：ログだけですべての状況や意図を再現できるわけではありません。

イ：ログは記録・分析の基盤であり、脆弱性修正はパッチ等の役割です。

ウ：ログは事象の記録であり、検知・分析・説明責任の基盤になります。

エ：ログは通常、業務データの完全なバックアップではありません。

総合解説：どのログを何の目的で取得するかを事前に定義することが重要です。取得しているだけで確認されなければ、検知や調査に十分活用できません。

対象：2026年度 / 基準日 2026-09-05

0012 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：基礎

認証システムで、成功ログだけでなく失敗ログも取得する主な理由として最も適切なものはどれか。

ア：失敗ログがあると認証処理そのものが不要になるため。

イ：失敗ログを公開すれば利用者のパスワードが強化されるため。

ウ：成功ログを取得できなくするため。

エ：総当たり攻撃や不正なログイン試行などの兆候を検知・調査しやすくするため。

答え・解説 正答：エ

ア：ログは認証処理を代替しません。

イ：ログ公開は情報漏えいにつながる可能性があります。

ウ：成功・失敗の両方を目的に応じて取得することが重要です。

エ：失敗の連続や異常な発生元は攻撃兆候になり得るため、失敗ログも重要です。

総合解説：IPAの実務例でもアクセス失敗のログ取得が挙げられています。成功だけでなく失敗も含めることで、攻撃兆候や誤設定の分析精度が上がります。

対象：2026年度 / 基準日 2026-09-05

0013 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：基礎

複数システムのログを突き合わせてインシデントの時系列を分析するために、特に重要な運用はどれか。

ア：各システムの時計を信頼できる時刻源へ同期し、タイムゾーンも含めて時刻情報を管理する。

イ：各端末の時計を利用者が自由に変更できるようにする。

ウ：ログから時刻情報を削除して保存容量を減らす。

エ：異なるシステムは必ず別のタイムゾーンで記録する。

答え・解説 正答：ア

ア：時刻がずれているとイベントの前後関係を誤って解釈するおそれがあります。

イ：時刻のばらつきが増え、相関分析が困難になります。

ウ：時系列分析に不可欠な情報を失います。

エ：統一的に比較できるルールが必要で、意図的な不統一は不適切です。

総合解説：ログ相関では「誰が・何を・いつ・どこで」が重要です。時刻同期とタイムゾーン管理は、原因分析や証拠性を高める基本運用です。

対象：2026年度 / 基準日 2026-09-05

0014 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：標準

侵害されたサーバ上のローカルログだけに依存する問題と、その改善策の組合せとして最も適切なものはどれか。

ア：ログ消去を防ぐには、ログ取得自体を停止する。

イ：攻撃者にログを消去される可能性があるため、重要ログを別システムへ転送して集中保管する。

ウ：ローカルログだけを同じディスクに複製すれば、侵害時の消去に十分耐えられる。

エ：ログを利用者が自由に編集できる共有フォルダへ置く。

答え・解説 正答：イ

ア：検知・調査能力を失うため逆効果です。

イ：侵害対象とログ保管先を分離すると、ログ改ざん・消去のリスクを低減できます。

ウ：同一侵害範囲内では複製も消去される可能性があります。

エ：完全性とアクセス制御を損ないます。

総合解説：IPAの実務例でも、対象システムとは別の場所へログを保管する考え方が示されています。重要ログは集中管理し、アクセス権と改ざん防止も考慮します。

対象：2026年度 / 基準日 2026-09-05

0015 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：標準

SIEMの利用目的として、最も適切なものはどれか。

ア：すべてのOS脆弱性を自動修正する。

イ：利用者の本人確認を生体認証だけで必ず実施する。

ウ：複数の機器・システムからログを集約し、相関分析やルールに基づく異常検知を支援する。

エ：データベースのバックアップを唯一の保存先として代替する。

答え・解説 正答：ウ

ア：パッチ管理の役割とは異なります。

イ：SIEMは認証方式そのものではありません。

ウ：SIEMは多様なログを集中管理し、相関分析やアラート生成を支援します。

エ：ログ分析基盤と業務データのバックアップは別の目的です。

総合解説：SIEMは「ログを集める箱」だけではなく、相関・検索・アラートなどにより大量ログから意味のある兆候を抽出するために使います。適切なルールと運用体制が必要です。

対象：2026年度 / 基準日 2026-09-05

0016 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：標準

ログの保管期間を決める考え方として、最も適切なものはどれか。

ア：保存容量がある限り、内容を問わず永久保存すれば常に最善である。

イ：容量節約のため、すべて1日で削除する。

ウ：担当者ごとに気分で削除日を変える。

エ：調査に必要な期間、法令・契約・社内規程、システム容量、機密性などの要件を踏まえて定める。

答え・解説 正答：エ

ア：不要な長期保存はコストや情報漏えいリスクを増やす場合があります。

イ：インシデントが後から判明した場合に調査できないおそれがあります。

ウ：一貫性と監査性がなく、管理できません。

エ：ログの価値とコスト・規制要件を踏まえ、目的に合う保管期間を設計します。

総合解説：ログ保管は「長ければ長いほど良い」と単純には決まりません。調査・監査に必要な期間を確保しつつ、個人情報や機密情報の扱いも統制します。

対象：2026年度 / 基準日 2026-09-05

0017 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：標準

通常時には深夜の管理者ログインがほぼないシステムで、深夜に多数の管理者ログインが発生した。監視上の考え方として最も適切なものはどれか。

ア：通常の利用パターンからの逸脱として調査対象にし、正当な作業か不正利用かを確認する。

イ：深夜という理由だけで必ず侵害と断定し、証拠確認なしに全システムを初期化する。

ウ：ログイン成功なので正常とみなし、発生元や対象を確認しない。

エ：通常と違うログは監視ノイズなので自動削除する。

答え・解説 正答：ア

ア：ベースラインとの差分は異常の手掛かりになりますが、アラートだけで攻撃と断定せず確認します。

イ：異常は調査の起点であり、即断による過剰対応は避けます。

ウ：正規資格情報が悪用される可能性もあります。

エ：異常を見逃すおそれがあります。

総合解説：異常検知は「通常状態」を知っているほど有効です。時間帯、発生元、対象アカウント、操作内容などを組み合わせて判断します。

対象：2026年度 / 基準日 2026-09-05

0018 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：標準

監視システムのアラートが多すぎて重要な警告が埋もれている。最も適切な改善はどれか。

ア：アラートをすべて無効化する。

イ：誤検知の原因を分析し、重要度、閾値、除外条件を根拠付きで調整し、見逃しが増えていないかも検証する。

ウ：担当者が多忙なので全アラートを自動的に正常扱いにする。

エ：閾値を最大値に固定し、発報しないことを成功とする。

答え・解説 正答：イ

ア：重要インシデントの検知まで失います。

イ：アラートチューニングはノイズ削減と検知能力の両方を評価する必要があります。

ウ：確認を省略すると真の異常を見逃します。

エ：発報ゼロは検知能力が失われている可能性があります。

総合解説：監視の品質はアラート数の少なさではなく、必要な兆候を適切に検知・処理できるかで評価します。チューニング後も定期的に有効性を見直します。

対象：2026年度 / 基準日 2026-09-05

0019 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：応用

VPNで海外IPからログイン成功した直後、同一利用者が社内ファイルサーバから大量ダウンロードし、その後クラウドへ大容量通信を行った。最も適切な分析はどれか。

ア：各ログは別システムなので関連付けず、単独で正常なら調査を終了する。

イ：通信量が多いので、誰のアカウントか確認せずサーバを廃棄する。

ウ：VPN認証、ファイルアクセス、外向き通信の各ログを時系列で相関し、資格情報悪用や情報持出しの可能性を調査する。

エ：海外IPという理由だけでログを削除し、利用者へ知らせない。

答え・解説 正答：ウ

ア：相関を無視すると複合的な攻撃を見逃します。

イ：過剰対応であり、事実確認と範囲特定が先です。

ウ：単一ログでは正常に見えても、複数イベントの組合せで攻撃シナリオが浮かぶことがあります。

エ：証拠を失い、原因分析もできません。

総合解説：インシデント分析では認証・端末・ファイル・ネットワーク・クラウドなど異なるログを関連付けます。アカウント、IP、時刻、端末IDなどをキーに追跡します。

対象：2026年度 / 基準日 2026-09-05

0020 日常のセキュリティ運用 > ログ取得・監視・分析 ｜ 難易度：応用

特権管理者が不正操作を行った場合でも追跡できるログ設計として、最も適切なものはどれか。

ア：特権管理者だけが自分のログを自由に削除できるようにする。

イ：特権操作は信頼できるのでログを取得しない。

ウ：ログを対象サーバの一時フォルダだけに保存し、自動消去を1時間にする。

エ：操作対象システムとは別の保管先へログを転送し、ログの削除・変更権限を運用管理者から分離して限定する。

答え・解説 正答：エ

ア：不正の隠蔽が可能になり、監査性が失われます。

イ：高権限操作ほど監査ログが重要です。

ウ：侵害時に容易に消去され、調査可能期間も不足します。

エ：操作する権限と監査記録を消せる権限を分離すると、ログ完全性を高められます。

総合解説：ログの機密性・完全性・可用性も保護対象です。特権操作の記録を独立した保管先へ転送し、職務分離や改ざん検知を組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0021 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：基礎

アクセス権管理における最小権限の原則として、最も適切なものはどれか。

ア：利用者やプロセスに、業務遂行に必要な最小限の権限だけを付与する。

イ：全利用者へ管理者権限を与え、問い合わせを減らす。

ウ：一度付与した権限は退職後も永久に残す。

エ：重要操作は誰でも匿名で実行できるようにする。

答え・解説 正答：ア

ア：不要な権限を減らすことで、誤操作やアカウント侵害時の影響を限定します。

イ：権限過剰となり、侵害時の被害を拡大させます。

ウ：不要となった権限は迅速に削除すべきです。

エ：識別・認証・説明責任を損ないます。

総合解説：アクセス権は「便利だから多めに」ではなく、職務上の必要性に基づいて付与します。権限付与後も定期的なレビューが必要です。

対象：2026年度 / 基準日 2026-09-05

0022 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：基礎

定期的なアクセス権レビューを行う主な目的として、最も適切なものはどれか。

ア：利用者のパスワードを管理者が一覧で閲覧する。

イ：現在の職務・所属・必要性と照合し、不要・過剰・不適切な権限を見つけて是正する。

ウ：ログを削除して監査対象を減らす。

エ：すべての権限を毎回追加する。

答え・解説 正答：イ

ア：パスワードそのものの共有・閲覧は不適切です。

イ：人事異動や業務変更で権限が陳腐化するため、定期レビューが必要です。

ウ：監査性を損ないます。

エ：レビューの目的は必要性の確認と過剰権限の是正です。

総合解説：レビューでは、アカウントの有効性、所属、役割、特権、最終利用状況などを確認します。申請時に正しくても、時間経過で不要になる権限があります。

対象：2026年度 / 基準日 2026-09-05

0023 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：基礎

退職者のアカウント管理として、最も適切なものはどれか。

ア：引継ぎに便利なので無期限に有効のまま残す。

イ：退職後は本人の端末だけ回収し、クラウドアカウントは放置する。

ウ：退職・契約終了のタイミングに合わせて不要なアカウントや認証資格情報を速やかに無効化する。

エ：パスワードだけ同僚へ渡し、同じアカウントを使い続ける。

答え・解説 正答：ウ

ア：不要なアカウントは攻撃面になります。

イ：クラウド等の論理アカウントも無効化対象です。

ウ：離職後の認証情報が残ると、不正利用されるリスクがあります。

エ：本人性と責任追跡が失われます。

総合解説：人事イベントとID管理を連携し、退職・契約終了・長期休職などに応じてアクセス権を更新します。共有や放置を避けます。

対象：2026年度 / 基準日 2026-09-05

0024 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：標準

営業部から経理部へ異動した利用者について、最も適切なアクセス権処理はどれか。

ア：旧部署と新部署の権限をすべて累積させる。

イ：異動後も一切見直さず、定年まで同じ権限を維持する。

ウ：本人が希望する権限を承認なしで自由に追加する。

エ：新しい職務に必要な権限を付与するとともに、旧職務で不要になった営業部向け権限を削除する。

答え・解説 正答：エ

ア：権限肥大化につながります。

イ：職務と権限が不一致になります。

ウ：権限付与には業務上の必要性と承認が必要です。

エ：異動時は権限追加だけでなく旧権限の剥奪が重要です。

総合解説：異動時に古い権限を残す「権限の蓄積」は典型的な管理不備です。付与と剥奪をセットで処理します。

対象：2026年度 / 基準日 2026-09-05

0025 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：標準

複数担当者が同じ管理者IDとパスワードを共有している。主な問題として最も適切なものはどれか。

ア：誰がどの操作を行ったか追跡しにくく、認証情報漏えい時の影響範囲も大きくなる。

イ：共有すれば各担当者の操作がより正確に識別できる。

ウ：共有IDならパスワード変更は不要になる。

エ：共有IDは最小権限を自動的に満たす。

答え・解説 正答：ア

ア：共有IDは個人単位の説明責任を弱めます。

イ：一つのIDを共有すると個人識別が困難になります。

ウ：共有でも認証情報の保護と更新は必要です。

エ：権限の大きさとは別問題です。

総合解説：原則として個人を識別できる管理者アカウントを用い、特権利用を記録・監視します。共通IDが不可避な場合は追加の統制が必要です。

対象：2026年度 / 基準日 2026-09-05

0026 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：標準

長期間利用されていないアカウントを発見した。最も適切な対応はどれか。

ア：利用されていないほど安全なので永久に残す。

イ：所有者と業務上の必要性を確認し、不要なら無効化・削除し、必要なら理由を記録して継続管理する。

ウ：パスワードを公開して、誰でも再利用できるようにする。

エ：所有者不明でも管理者権限を追加する。

答え・解説 正答：イ

ア：監視されにくい不要アカウントはリスクになります。

イ：休眠アカウントは攻撃者に悪用されても気づきにくいため、定期的な見直しが重要です。

ウ：不正アクセスの原因になります。

エ：必要性不明の権限拡大は不適切です。

総合解説：アカウント棚卸では最終利用日時や所有者を確認し、不要アカウントを整理します。自動無効化ルールを設ける場合も業務要件と整合させます。

対象：2026年度 / 基準日 2026-09-05

0027 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：標準

通常利用者権限と管理者権限のレビュー頻度・深さについて、最も適切な考え方はどれか。

ア：管理者は信頼されているのでレビュー対象外にする。

イ：通常利用者より管理者の監査ログを少なくする。

ウ：高い権限ほど侵害時の影響が大きいため、特権アカウントはより厳格に必要性・利用状況・保有者を確認する。

エ：特権を一度付与したら、役割変更があっても削除しない。

答え・解説 正答：ウ

ア：内部不正や資格情報侵害のリスクがあるため除外すべきではありません。

イ：特権操作はむしろ重点的に監視する対象です。

ウ：リスクに応じたレビュー強度が必要です。

エ：不要な特権は速やかに削除すべきです。

総合解説：特権アカウントは重要操作が可能なため、最小化、個人紐付け、定期再認証、ログ監視などを強化します。

対象：2026年度 / 基準日 2026-09-05

0028 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：標準

障害対応のため外部ベンダへ一時的な管理者権限を付与する。最も適切な運用はどれか。

ア：緊急対応なら承認も期限も不要として、恒久的に残す。

イ：ベンダ担当者全員で同じ管理者パスワードを共有する。

ウ：作業後はログを削除して情報を残さない。

エ：作業目的・対象・承認者・有効期限を定め、作業後に権限を削除し、操作ログを確認する。

答え・解説 正答：エ

ア：一時例外が恒久権限化するリスクがあります。

イ：個人追跡が困難になります。

ウ：事後確認や説明責任を失います。

エ：一時権限は必要最小限・期限付き・監視付きで管理します。

総合解説：緊急時にも統制を完全に外すのではなく、迅速な承認手順、時間制限、対象限定、事後レビューなどでリスクを管理します。

対象：2026年度 / 基準日 2026-09-05

0029 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：応用

規程には「退職者IDを即日停止する」とあるが、実際には数週間残る例が複数見つかった。最も適切な評価はどれか。

ア：規程の存在だけでは統制が有効とはいえず、実際の運用実績を確認して停止プロセスの不備を是正する必要がある。

イ：規程があるので、実施されていなくても統制は十分と判断する。

ウ：退職者IDの残存を隠すため棚卸を中止する。

エ：すべての現役利用者IDも停止して帳尻を合わせる。

答え・解説 正答：ア

ア：設計された統制と実際に運用されている統制を区別して評価します。

イ：運用されなければリスク低減効果はありません。

ウ：不備を把握できず、リスクが継続します。

エ：業務停止を招く過剰対応で、原因改善になりません。

総合解説：自己点検や監査では「ルールがあるか」だけでなく「実際に守られ、期待した効果を出しているか」を証拠で確認します。

対象：2026年度 / 基準日 2026-09-05

0030 日常のセキュリティ運用 > アクセス権レビュー・運用状況点検 ｜ 難易度：応用

四半期ごとにアクセス権レビューを実施しているが、誰が何を確認し、どの権限を削除したか記録していない。改善として最も適切なものはどれか。

ア：口頭で実施したと担当者が覚えていれば記録は不要とする。

イ：レビュー対象、確認者、判断結果、是正内容、実施日を記録し、後から追跡できるようにする。

ウ：削除した権限をすぐ再付与し、記録との差異をなくす。

エ：レビュー資料を一般公開し、全利用者の権限を誰でも閲覧可能にする。

答え・解説 正答：イ

ア：担当者交代や監査時に客観的な確認ができません。

イ：レビューの証跡があれば、実施の事実と判断根拠を確認できます。

ウ：不適切な権限を復活させることになります。

エ：権限情報自体の機密性も考慮する必要があります。

総合解説：運用点検は、実施結果を証跡として残すことで継続的改善や監査に利用できます。記録の閲覧権限や保管期間も管理します。

対象：2026年度 / 基準日 2026-09-05

0031 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：基礎

セキュリティ運用における「イベント」と「インシデント」の関係として、最も適切なものはどれか。

ア：ログに記録された事象はすべて重大インシデントである。

イ：インシデントは必ず外部攻撃だけを指し、誤送信や内部不正は含まれない。

ウ：イベントは観測された事象であり、その中で組織のセキュリティ方針や業務へ悪影響を与えるものがインシデントとして扱われる。

エ：イベントは発生後に記録できない事象だけを指す。

答え・解説 正答：ウ

ア：正常なログインなどの通常イベントも多数あります。

イ：人的ミスや内部不正もインシデントになり得ます。

ウ：すべてのイベントがインシデントではなく、評価して対応対象を判断します。

エ：ログ等に記録される事象もイベントです。

総合解説：検知段階では多数のイベントから、影響・確度・緊急度を評価してインシデントを識別します。用語の区別はトリアージの基礎です。

対象：2026年度 / 基準日 2026-09-05

0032 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：基礎

従業員が不審メールの添付ファイルを開き、直後にPCの挙動がおかしくなった。最も適切な行動はどれか。

ア：自分で問題を隠し、翌月の定例会まで待つ。

イ：証拠を消すためメールとログをすべて削除する。

ウ：同僚全員へ添付ファイルを転送して再現させる。

エ：定められた窓口へ速やかに報告し、組織の初動手順に従う。

答え・解説 正答：エ

ア：対応が遅れ、被害が拡大する可能性があります。

イ：調査に必要な情報を失います。

ウ：被害を拡大させる危険があります。

エ：早期報告により、被害拡大防止や調査開始を早められます。

総合解説：利用者が異常を感じたときに迷わず報告できる窓口と手順を用意することが重要です。報告者を責める文化は早期検知を妨げます。

対象：2026年度 / 基準日 2026-09-05

0033 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：基礎

インシデント対応におけるエスカレーションの主な目的として、最も適切なものはどれか。

ア：影響や緊急度に応じて、必要な権限・専門性・意思決定を持つ上位者や関係部門へ速やかに引き上げる。

イ：担当者が責任を避けるため、内容を確認せず全件を社長へ送る。

ウ：報告件数を減らすため、重大事象も担当者だけで処理する。

エ：インシデントの記録を削除する。

答え・解説 正答：ア

ア：重大事象を適切な意思決定レベルへ上げることで、迅速な対応と調整が可能になります。

イ：基準のない無差別なエスカレーションは業務を阻害します。

ウ：必要な意思決定が遅れます。

エ：エスカレーションは記録削除ではありません。

総合解説：エスカレーション基準には、重要資産、影響範囲、顧客影響、法務・広報対応の必要性などを定めておくと有効です。

対象：2026年度 / 基準日 2026-09-05

0034 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：標準

EDRから「疑わしいPowerShell実行」のアラートが1件出た。最も適切な初動はどれか。

ア：アラートが1件だけなので無条件に無視する。

イ：端末、利用者、実行コマンド、親プロセス、通信先などを確認し、正規作業か不正活動かを評価する。

ウ：PowerShellはすべて攻撃なので、全社PCを即廃棄する。

エ：アラートを消すためEDRを停止する。

答え・解説 正答：イ

ア：単一アラートでも重大な活動の可能性があります。

イ：アラートは調査の起点であり、文脈を確認して確度と影響を判断します。

ウ：正規利用もあるため、事実確認なしの過剰対応です。

エ：検知能力を失います。

総合解説：検知ツールのアラートは、利用者・端末・プロセス・ネットワークなどの文脈で評価します。誤検知と見逃しの双方を考慮します。

対象：2026年度 / 基準日 2026-09-05

0035 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：標準

同じ種類のマルウェア検知でも、一般PC1台と基幹認証サーバで発生した場合の扱いとして最も適切なものはどれか。

ア：マルウェア名が同じなら必ず同じ重大度にする。

イ：一般PCの方が台数が少ないので常に重大とする。

ウ：資産の重要度や影響範囲を考慮し、基幹認証サーバでの検知をより高い優先度で評価・エスカレーションする。

エ：サーバは常時稼働しているのでインシデント対象外とする。

答え・解説 正答：ウ

ア：資産価値や影響範囲を無視しています。

イ：台数だけで重大度は決まりません。

ウ：同じ脅威でも対象資産の重要度で事業影響は変わります。

エ：重要サーバこそ侵害時の影響が大きくなり得ます。

総合解説：トリアージでは脅威の種類だけでなく、資産重要度、影響、拡大可能性、機密情報の有無などを総合して優先順位を決めます。

対象：2026年度 / 基準日 2026-09-05

0036 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：標準

インシデントの初期報告に含める情報として、最も適切な組合せはどれか。

ア：推測だけで攻撃者の氏名を断定し、それ以外の情報は書かない。

イ：発見日時や対象を記録せず「何か変」とだけ伝える。

ウ：対応履歴を残さず、担当者の記憶だけに任せる。

エ：発見日時、発見者、対象、症状・観測事実、実施済み対応、影響の見込み、連絡先など、現時点で確認できる事実を整理する。

答え・解説 正答：エ

ア：根拠のない断定は判断を誤らせます。

イ：切り分けや時系列分析に必要な情報が不足します。

ウ：引継ぎや説明責任が困難になります。

エ：初期報告は確定していない事項を区別しつつ、対応判断に必要な事実を共有します。

総合解説：初期段階では不明点があって当然です。「確認済み事実」「仮説」「未確認」を分けて伝えると、意思決定の精度が上がります。

対象：2026年度 / 基準日 2026-09-05

0037 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：標準

1回の認証失敗、1件の不審DNS照会、1回の外向き通信だけでは判断しにくい。これらが同一端末で短時間に連続した場合の扱いとして最も適切なものはどれか。

ア：複数の兆候を相関し、単独では低重要度でも攻撃シナリオとして成立するかを追加調査する。

イ：各兆候が単独で重大でないため、組合せも必ず正常とする。

ウ：すべての低重要度ログを保存せず即削除する。

エ：一つでも不審なら証拠なしで全社員を不正者と断定する。

答え・解説 正答：ア

ア：弱い兆候の組合せで侵害の確度が高まることがあります。

イ：相関によって意味が変わる可能性があります。

ウ：後の相関分析ができなくなります。

エ：過剰で根拠のない判断です。

総合解説：インシデント検知では、複数データソースの相関が重要です。単一イベントの評価と、攻撃チェーン全体の評価を区別します。

対象：2026年度 / 基準日 2026-09-05

0038 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：標準

取引先から「御社ドメインを名乗る不審メールが届いた」と連絡があった。最も適切な対応はどれか。

ア：社外からの情報はすべて無視する。

イ：外部通報もインシデント検知の入力として記録し、メールヘッダや送信元、アカウント侵害の有無などを確認する。

ウ：連絡者へ不審メールを全社員へ転送するよう依頼する。

エ：自社ドメインが表示されているだけで必ずメールサーバ侵害と断定する。

答え・解説 正答：イ

ア：外部通報から自組織の侵害が判明することがあります。

イ：監視システム以外の外部通報も重要な認知経路です。

ウ：被害拡大につながる可能性があります。

エ：送信元詐称の可能性もあり、調査が必要です。

総合解説：インシデントは内部監視だけでなく、顧客・取引先・外部CSIRTなどから認知することがあります。通報窓口と受付手順を整備します。

対象：2026年度 / 基準日 2026-09-05

0039 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：応用

重大インシデントが休日深夜に発生しても初動を遅らせないための準備として、最も適切なものはどれか。

ア：休日は誰も対応しないことを前提に、月曜まで待つ。

イ：担当者一人の私物スマートフォン番号だけに依存し、代替連絡先を持たない。

ウ：緊急連絡先、当番・代替担当、重大度基準、権限委譲を事前に定め、定期的に連絡網を確認する。

エ：連絡網を作成したら、異動や退職があっても更新しない。

答え・解説 正答：ウ

ア：重大インシデントでは被害が拡大する可能性があります。

イ：単一障害点になり、担当者不在時に連絡できません。

ウ：時間外でも誰が判断・対応するかを事前に決めておくことで初動遅延を減らせます。

エ：連絡先が陳腐化し、緊急時に機能しません。

総合解説：インシデント対応計画は平常時に整備・演習します。特に時間外の連絡網、意思決定権限、外部支援先を確認しておくことが重要です。

対象：2026年度 / 基準日 2026-09-05

0040 インシデント検知・初動 > 兆候・発見・報告・エスカレーション ｜ 難易度：応用

アラートを調査した結果、正規の管理作業と判明した。最も適切な処理はどれか。

ア：正常と分かったので調査記録をすべて削除する。

イ：一度誤検知だったため、その検知ルールを無条件に永久停止する。

ウ：正規作業者を攻撃者として外部公表する。

エ：確認した根拠と判断を記録してクローズし、同種の不要アラートが多い場合は検知ルールの改善を検討する。

答え・解説 正答：エ

ア：将来の比較や説明責任に使えなくなります。

イ：将来の真の攻撃を見逃す可能性があります。

ウ：事実に反する公表は不適切です。

エ：誤検知でも判断過程を残すことで、監査・再評価・チューニングに利用できます。

総合解説：クローズ時も「なぜ正常と判断したか」を記録します。誤検知傾向はルール改善に使い、検知感度を維持しながらノイズを減らします。

対象：2026年度 / 基準日 2026-09-05

0041 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：基礎

インシデント対応におけるトリアージの目的として、最も適切なものはどれか。

ア：事象の確度、影響、緊急度などを評価し、対応すべきかと優先順位を決める。

イ：すべての端末を無条件に初期化する。

ウ：ログを削除して調査件数を減らす。

エ：被害の大小に関係なく全件を同じ順番で処理する。

答え・解説 正答：ア

ア：限られた対応資源を重大な事象へ適切に配分するための評価です。

イ：事実確認や優先順位付けをせずに一律処置することではありません。

ウ：証拠を失います。

エ：トリアージは優先順位付けのために行います。

総合解説：トリアージでは、対象資産、業務影響、攻撃継続性、機密情報、拡大可能性などを確認して優先度を設定します。

対象：2026年度 / 基準日 2026-09-05

0042 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：基礎

インシデント対応における封じ込めの主な目的として、最も適切なものはどれか。

ア：原因を調べずにすべての証拠を消す。

イ：攻撃や被害の拡大を抑え、影響範囲を限定しながら調査・復旧へつなげる。

ウ：攻撃者が自由に横展開できる状態を維持する。

エ：再発防止策を永久に不要にする。

答え・解説 正答：イ

ア：調査能力を失います。

イ：封じ込めは侵害の拡大防止を目的とする段階です。

ウ：封じ込めと逆の行為です。

エ：封じ込めは一時的な対応を含み、根絶・改善も必要です。

総合解説：封じ込めには端末隔離、アカウント停止、通信遮断、セグメント制御などがあります。業務影響と証拠保全を考慮して選びます。

対象：2026年度 / 基準日 2026-09-05

0043 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：基礎

同じ部署のPCだけが同時に不審な通信を始めた。切り分けの考え方として最も適切なものはどれか。

ア：1台だけを確認し、他端末は必ず無関係とする。

イ：端末名をすべて変更し、原因分析を終了する。

ウ：共通するネットワーク、配布ソフト、認証情報、メールなどの要因を確認し、影響範囲と共通原因を絞り込む。

エ：ネットワーク図を見ず、部署情報も無視する。

答え・解説 正答：ウ

ア：同時発生なら横展開や共通侵入経路の確認が必要です。

イ：名称変更では侵害原因を除去できません。

ウ：複数端末に共通する条件から侵入経路や範囲を推定します。

エ：共通点の把握に有用な情報を捨てることになります。

総合解説：切り分けでは「共通点」と「差分」を使って範囲を絞ります。ユーザー、端末、ネットワーク、時間帯、配布物、認証などを比較します。

対象：2026年度 / 基準日 2026-09-05

0044 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：標準

端末でマルウェア感染が強く疑われ、外部C2通信も確認された。最も適切な初動はどれか。

ア：感染疑い端末から他端末へファイルを共有して比較する。

イ：通信を継続させたまま数週間様子を見る。

ウ：調査前にログとメモリをすべて消去する。

エ：必要な調査・業務影響を考慮しつつ、ネットワークから論理的に隔離して外部通信や横展開を抑える。

答え・解説 正答：エ

ア：感染拡大の危険があります。

イ：攻撃者の活動継続を許す可能性があります。

ウ：証拠を失うおそれがあります。

エ：端末隔離は被害拡大防止に有効で、EDRのネットワーク隔離などを利用できる場合があります。

総合解説：隔離は封じ込めの代表策です。ただし電源断や完全遮断が揮発性証拠を失う場合もあるため、手順と優先度を定めます。

対象：2026年度 / 基準日 2026-09-05

0045 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：標準

複数端末でファイル暗号化が始まり、共有フォルダにも被害が広がっている。最も適切な初動はどれか。

ア：感染・疑い端末や影響セグメントを隔離し、共有資源へのアクセスを制限して暗号化と横展開の拡大を抑える。

イ：暗号化が終わるまで待ち、通信を維持する。

ウ：バックアップサーバを感染端末へ新たに書込み可能で接続する。

エ：ログを停止してディスク負荷を下げる。

答え・解説 正答：ア

ア：ランサムウェアでは拡大速度が速いため、影響範囲を限定する封じ込めが重要です。

イ：被害が拡大します。

ウ：バックアップまで暗号化される危険があります。

エ：調査・検知能力を失います。

総合解説：ランサムウェア初動では横展開とバックアップ被害を防ぎます。隔離後に影響範囲、侵入経路、認証情報悪用の有無を調査します。

対象：2026年度 / 基準日 2026-09-05

0046 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：標準

クラウド管理者アカウントの資格情報漏えいが疑われる。最も適切な封じ込めはどれか。

ア：パスワードを変更せず、利用者へ注意するだけで終える。

イ：影響を確認しつつアカウントを無効化または資格情報を更新し、既存セッションやトークンも必要に応じて失効させる。

ウ：同じパスワードを別の管理者IDにも設定する。

エ：ログイン履歴を削除してからアカウントを継続利用する。

答え・解説 正答：イ

ア：攻撃者が資格情報を使い続ける可能性があります。

イ：パスワード変更だけで既存セッションが残るサービスもあるため、認証セッション全体を考慮します。

ウ：侵害範囲を広げます。

エ：調査証拠を失い、侵害継続の危険があります。

総合解説：アカウント侵害ではパスワード、APIキー、トークン、MFA設定、復旧用情報など、利用可能な認証手段を総合的に無効化・再発行します。

対象：2026年度 / 基準日 2026-09-05

0047 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：標準

脆弱なWeb機能が悪用されている。恒久修正には数日かかる。最も適切な対応はどれか。

ア：恒久修正まで何もせず公開を続ける。

イ：暫定策を入れたら恒久修正は不要とする。

ウ：まず対象機能の停止やWAFルール、アクセス制限などで短期封じ込めを行い、並行して恒久修正と復旧計画を進める。

エ：Webサーバの名前だけ変更して攻撃を止める。

答え・解説 正答：ウ

ア：攻撃継続の可能性があります。

イ：暫定策には限界があり、根本原因の解消が必要です。

ウ：迅速な暫定策と根本的な恒久対策を段階的に使い分けます。

エ：脆弱性そのものは残ります。

総合解説：インシデント対応では短期的な被害抑制と長期的な根絶を分けて計画します。暫定策の副作用や解除条件も記録します。

対象：2026年度 / 基準日 2026-09-05

0048 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：標準

製造ライン制御サーバの侵害が疑われるが、即時停止すると安全上重大な影響が出る可能性がある。最も適切な考え方はどれか。

ア：セキュリティ事案なら必ず即時電源断し、物理安全は考慮しない。

イ：業務影響があるので、侵害兆候を永久に無視する。

ウ：担当者一人だけで停止を決め、運用責任者へ連絡しない。

エ：安全・業務影響とサイバーリスクを関係部門で評価し、代替運転や段階隔離など実行可能な封じ込め方法を決定する。

答え・解説 正答：エ

ア：人命や設備安全を損なう可能性があります。

イ：攻撃継続のリスクがあります。

ウ：重大な業務判断には適切な権限と関係部門調整が必要です。

エ：封じ込めは常に単純な電源断ではなく、現実の安全性・可用性を考慮して決めます。

総合解説：封じ込め戦略は資産特性に応じます。ITとOT、医療、公共サービスなどでは、安全性や事業継続を含めた意思決定が重要です。

対象：2026年度 / 基準日 2026-09-05

0049 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：応用

1台のPCからドメイン管理者資格情報の窃取痕跡が見つかった。最も適切な初動方針はどれか。

ア：当該PCだけでなく、管理者資格情報が使用された他端末・サーバ・認証ログを確認し、必要に応じて資格情報を失効して横展開を封じ込める。

イ：1台のPCを再起動すれば必ず解決するとして、他システムを調べない。

ウ：管理者資格情報を同じ値のまま全端末へ配布する。

エ：認証ログを削除して横展開の痕跡を消す。

答え・解説 正答：ア

ア：高権限資格情報の侵害は広い範囲へ影響し得るため、利用履歴と範囲を追跡します。

イ：資格情報が既に悪用されている可能性があります。

ウ：攻撃者の利用可能範囲を広げます。

エ：範囲特定ができなくなります。

総合解説：侵害された資格情報は「端末内の問題」ではなく組織全体の認証基盤へ波及する可能性があります。アカウント・認証・端末の両面で封じ込めます。

対象：2026年度 / 基準日 2026-09-05

0050 インシデント検知・初動 > トリアージ・切り分け・封じ込め ｜ 難易度：応用

公開リポジトリにクラウドのAPIキーが誤って含まれていたことが判明した。最も適切な初動はどれか。

ア：リポジトリから文字列を削除しただけで、キーはそのまま使い続ける。

イ：該当キーを速やかに失効・再発行し、利用ログを確認して不正利用の有無と影響範囲を調査する。

ウ：キーの権限を管理者へ昇格して監視しやすくする。

エ：ログを見ず、課金額が増えていなければ不正利用なしと断定する。

答え・解説 正答：イ

ア：既に複製・取得されている可能性があり、削除だけでは不十分です。

イ：公開済み資格情報は取得された前提で扱い、失効と利用履歴確認を行います。

ウ：漏えい時の影響を増大させます。

エ：情報アクセス等、課金に表れない悪用もあり得ます。

総合解説：クラウド資格情報漏えいでは、認証情報の失効、権限見直し、監査ログ確認、関連シークレットの探索を迅速に行います。

対象：2026年度 / 基準日 2026-09-05

0051 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：基礎

デジタルフォレンジックスの説明として、最も適切なものはどれか。

ア：すべての証拠を削除して復旧を早める活動である。

イ：攻撃者へ報復するための活動である。

ウ：デジタル機器やログ等から、事象の解明に必要なデータを適切に収集・保全・分析・報告する活動である。

エ：バックアップだけを取得し、分析を一切行わない活動である。

答え・解説 正答：ウ

ア：証拠保全と逆です。

イ：フォレンジックスの目的ではありません。

ウ：インシデント調査では、証拠の完全性を意識してデータを扱います。

エ：取得だけでなく検査・分析・報告まで含まれます。

総合解説：フォレンジックスは法執行だけでなく、組織内部のインシデント原因分析や被害範囲特定にも利用されます。手順と権限を定めて実施します。

対象：2026年度 / 基準日 2026-09-05

0052 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：基礎

取得したディスクイメージの完全性を確認する方法として、最も適切なものはどれか。

ア：ファイル名を「証拠」に変更するだけで完全性を保証する。

イ：分析のたびに元データを直接編集する。

ウ：ハッシュ値を記録せず、担当者の記憶だけに頼る。

エ：取得時にハッシュ値を計算・記録し、分析用コピーでも一致を確認する。

答え・解説 正答：エ

ア：名称変更では内容の改変有無を検証できません。

イ：原本の完全性が損なわれます。

ウ：客観的な完全性確認ができません。

エ：ハッシュ値はデータが取得後に変更されていないことを検証する手掛かりになります。

総合解説：証拠取得では原本と分析用コピーを区別し、ハッシュや取得手順、日時、担当者を記録します。

対象：2026年度 / 基準日 2026-09-05

0053 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：基礎

デジタル証拠の「誰が、いつ、どこで、どのように取り扱ったか」を継続して記録する主な目的はどれか。

ア：証拠の管理経路と完全性を説明できるようにし、不適切な取扱いや改変の疑いを減らす。

イ：証拠を誰でも自由に持ち出せるようにする。

ウ：証拠の内容を一般公開する。

エ：分析担当者を匿名にし、責任を追跡できなくする。

答え・解説 正答：ア

ア：取扱履歴を記録することで、証拠がどのように管理されたかを追跡できます。

イ：管理統制を弱めます。

ウ：機密性を損なう可能性があります。

エ：説明責任を低下させます。

総合解説：証拠保全では、取得・移送・保管・分析の各段階を記録します。組織の手順や法務要件に従って管理します。

対象：2026年度 / 基準日 2026-09-05

0054 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：標準

感染疑い端末の電源を切る前に取得を検討すべき情報として、揮発性が高いものはどれか。

ア：長期保管済みの紙の契約書だけ。

イ：メモリ上のプロセス、ネットワーク接続、ログオンセッションなど、電源断で失われ得る情報。

ウ：封印済みのオフラインバックアップ媒体だけ。

エ：公開Webサイトの会社概要だけ。

答え・解説 正答：イ

ア：端末の揮発性データではありません。

イ：揮発性データは電源断や状態変化で消失する可能性があります。

ウ：電源断で消える端末上の揮発性情報とは異なります。

エ：端末の一時的状態を表す証拠ではありません。

総合解説：証拠取得では揮発性の高い情報を優先する場合があります。ただし組織の手順と技術的・法的要件に従い、取得による状態変化も記録します。

対象：2026年度 / 基準日 2026-09-05

0055 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：標準

ディスク証拠を分析する際の原則として、最も適切なものはどれか。

ア：分析効率を上げるため、原本上のファイルを自由に編集する。

イ：原本とコピーを区別せず同じラベルで管理する。

ウ：可能な限り原本を保全し、取得したイメージや複製を分析対象にして原本への変更を避ける。

エ：分析後に原本のハッシュ値を初めて計算し、取得前の状態と同じと仮定する。

答え・解説 正答：ウ

ア：証拠改変となり得ます。

イ：取り違えの原因になります。

ウ：原本を直接操作すると証拠の完全性が損なわれるおそれがあります。

エ：取得時点の完全性確認ができません。

総合解説：フォレンジックでは、取得、ハッシュ、保管、分析用コピー作成などの手順を標準化します。原本へのアクセスは最小限にします。

対象：2026年度 / 基準日 2026-09-05

0056 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：標準

複数国のクラウドサービスと端末ログを時系列で統合する際の注意として、最も適切なものはどれか。

ア：表示されている時刻をすべて同じタイムゾーンだと仮定する。

イ：時刻情報を削除してIPアドレスだけで順序を決める。

ウ：端末時計がずれていても必ずクラウド時刻と一致するとみなす。

エ：各ログのタイムゾーン、時刻同期状況、夏時間等を確認し、共通基準へ正規化して比較する。

答え・解説 正答：エ

ア：ログごとに時刻基準が異なる場合があります。

イ：時系列分析に必要な情報を失います。

ウ：同期不良があればずれます。

エ：タイムスタンプの意味をそろえないとイベント順序を誤ります。

総合解説：フォレンジック分析では、タイムラインの精度が重要です。時刻源やタイムゾーンの差を明示し、不確実性も記録します。

対象：2026年度 / 基準日 2026-09-05

0057 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：標準

削除済みファイルや未割当て領域も含めてディスク全体を調査したい。最も適切な取得方法はどれか。

ア：可能な場合、フォレンジックイメージとしてディスクの内容をセクタ等の単位で取得する。

イ：エクスプローラで見えるファイルだけをコピーし、それ以外は存在しないとみなす。

ウ：証拠ディスクを初期化してからコピーする。

エ：スクリーンショットだけで全ディスクの証拠を代替する。

答え・解説 正答：ア

ア：単純なファイルコピーでは未割当て領域などを取得できないため、目的に応じてイメージ取得を使います。

イ：削除ファイル等の痕跡を見逃す可能性があります。

ウ：証拠を破壊します。

エ：表示されていないデータやメタデータを取得できません。

総合解説：取得方法は調査目的に合わせます。全体イメージが必要な場合と、対象ログ・ファイルだけで足りる場合を区別し、過剰収集にも注意します。

対象：2026年度 / 基準日 2026-09-05

0058 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：標準

不審な画面表示をスクリーンショットで保存した。フォレンジック上の扱いとして、最も適切なものはどれか。

ア：スクリーンショットが1枚あれば、他の証拠は一切不要である。

イ：画面状態の補助記録として有用だが、ログやメモリ、ファイル、メタデータ等の取得を代替するものではない。

ウ：画像に時刻が写っていれば、ファイル改変の有無も自動的に証明できる。

エ：スクリーンショットを撮った後は元端末を自由に改変してよい。

答え・解説 正答：イ

ア：調査目的によっては多様なデータが必要です。

イ：スクリーンショットだけでは背後の技術情報や時系列を十分に保存できません。

ウ：スクリーンショットだけでは原データの完全性を証明できません。

エ：証拠保全の観点から不適切です。

総合解説：フォレンジックでは一つの証拠形式に依存せず、複数のデータソースを組み合わせます。取得目的と証拠価値を明確にします。

対象：2026年度 / 基準日 2026-09-05

0059 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：応用

従業員端末のフォレンジック調査を行う際のガバナンスとして、最も適切なものはどれか。

ア：調査担当者が興味を持った個人データを無制限に収集してよい。

イ：権限確認は不要で、すべての私物端末も自動的に押収する。

ウ：組織の規程、法務・プライバシー要件、調査権限、対象範囲を確認し、必要最小限のデータを適切な手順で取得する。

エ：調査対象者へ無断で証拠を書き換え、結果を都合よく整える。

答え・解説 正答：ウ

ア：目的外・過剰な収集は不適切です。

イ：法務・契約・規程上の問題が生じ得ます。

ウ：技術的に取得可能でも、権限やプライバシーを無視してよいわけではありません。

エ：証拠の完全性と倫理に反します。

総合解説：フォレンジックは技術だけでなく、権限、プライバシー、労務、契約等の統制が必要です。事前に手順と相談先を定めます。

対象：2026年度 / 基準日 2026-09-05

0060 インシデント検知・初動 > 証拠保全・デジタルフォレンジックス ｜ 難易度：応用

稼働中サーバからメモリや接続情報を取得すると、取得ツール自体がプロセスやアクセス時刻を変化させる可能性がある。最も適切な対応はどれか。

ア：取得行為は絶対に何も変えないと仮定し、手順を記録しない。

イ：影響を隠すため取得ログを削除する。

ウ：証拠変化を避けるため、どのようなインシデントでも一切データを取得しない。

エ：取得による影響を理解し、使用ツール・手順・時刻・担当者を記録して、分析時にその変化を区別できるようにする。

答え・解説 正答：エ

ア：実際には状態が変化することがあります。

イ：透明性と再現性を損ないます。

ウ：調査不能になります。

エ：ライブ取得では完全に無影響にすることが難しいため、取得行為の影響を記録することが重要です。

総合解説：デジタル証拠取得は対象へ何らかの影響を与える場合があります。完全性を高めるには、標準手順、検証済みツール、詳細な作業記録が重要です。

対象：2026年度 / 基準日 2026-09-05

0061 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：基礎

インシデントの被害範囲を特定する主な目的として、最も適切なものはどれか。

ア：影響を受けた資産・アカウント・データ・業務を把握し、必要な封じ込め・復旧・通知の対象を決める。

イ：最初に見つかった1台だけを対象にし、他の影響を調べない。

ウ：被害範囲を広く見せるため、無関係なシステムも必ず含める。

エ：原因分析をせず、全システムを同じ対応にする。

答え・解説 正答：ア

ア：範囲特定は対応の優先順位と後続措置を正しく決める基盤です。

イ：横展開や共通原因を見逃す可能性があります。

ウ：事実に基づく範囲評価が必要です。

エ：過剰・不足のある対応になり得ます。

総合解説：被害範囲は端末数だけでなく、アカウント、データ、クラウド、取引先接続、業務プロセスなど複数の観点で評価します。

対象：2026年度 / 基準日 2026-09-05

0062 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：基礎

インシデントの影響評価として、最も適切なものはどれか。

ア：CPU使用率だけで重大度を決める。

イ：機密性・完全性・可用性への影響に加え、業務停止、顧客、法令・契約、財務、評判なども確認する。

ウ：データ漏えいがなければ、可用性停止は影響ゼロとする。

エ：売上への影響だけを見て、機密情報の漏えいは評価しない。

答え・解説 正答：イ

ア：一つの技術指標だけでは事業影響を判断できません。

イ：技術的影響と事業影響の両方を評価することが重要です。

ウ：可用性の喪失も重大な影響になり得ます。

エ：機密性・法令・顧客影響等も重要です。

総合解説：情報セキュリティインシデントはCIAのいずれか、または複数を損ないます。復旧優先順位は事業影響と組み合わせて判断します。

対象：2026年度 / 基準日 2026-09-05

0063 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：基礎

Webサーバが改ざんされた事案で、「不正なファイルが置かれていた」という事実と「未修正の脆弱性が悪用された」という事実の関係として、最も適切なものはどれか。

ア：不正ファイルを削除すれば、侵入原因は必ず解消したといえる。

イ：脆弱性は結果であり、不正ファイルが根本原因である。

ウ：前者は観測された結果・症状であり、後者は侵入経路となった原因候補である。

エ：原因分析では観測事実を記録する必要はない。

答え・解説 正答：ウ

ア：脆弱性や盗まれた資格情報が残っていれば再侵入されます。

イ：一般に因果関係が逆です。

ウ：症状を消すだけでなく、侵入を可能にした根本要因を特定する必要があります。

エ：原因仮説を検証する基礎として事実記録が必要です。

総合解説：原因分析では「何が起きたか」「どう入ったか」「なぜ防げなかったか」を分けて考えます。根絶・再発防止には原因まで掘り下げることが重要です。

対象：2026年度 / 基準日 2026-09-05

0064 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：標準

インシデントの原因分析でタイムラインを作成する主な利点はどれか。

ア：時刻を削除してイベントの順序を分からなくする。

イ：最初に見つかったイベントを必ず侵入開始点と断定する。

ウ：一つのログだけで全ての事象を完全に説明できると仮定する。

エ：認証、プロセス実行、通信、ファイル操作などの前後関係を整理し、侵入・横展開・持出しの流れを検証できる。

答え・解説 正答：エ

ア：分析精度が下がります。

イ：検知時刻と侵入時刻は異なる場合があります。

ウ：複数のログや証拠を相関する必要があります。

エ：時系列をそろえることで因果関係や欠落期間を分析しやすくなります。

総合解説：タイムラインは仮説検証の道具です。最初の兆候より前のログも確認し、侵害開始時刻や攻撃者の滞在期間を見積もります。

対象：2026年度 / 基準日 2026-09-05

0065 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：標準

侵害端末から悪性ドメイン名とファイルハッシュが見つかった。次の調査として最も適切なものはどれか。

ア：組織内のDNS・プロキシ・EDR等で同じドメインやハッシュの出現を検索し、他の侵害端末候補を特定する。

イ：侵害端末だけで見つかったので、他端末には絶対に存在しないとする。

ウ：IOCを全社公開チャットへ無制限に貼り、機密性を考慮しない。

エ：ハッシュが一致したファイルを調べず、すべて正常とみなす。

答え・解説 正答：ア

ア：既知の侵害指標を横断検索することで影響範囲を広げて確認できます。

イ：共通攻撃や横展開の可能性があります。

ウ：情報共有には範囲・機密性・必要性を考慮します。

エ：IOC一致は調査対象とするべきです。

総合解説：IOCは範囲特定に有用ですが、単独で確定証拠とは限りません。文脈や追加証拠と組み合わせて評価します。

対象：2026年度 / 基準日 2026-09-05

0066 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：標準

侵害された利用者IDが複数サーバへログインしていた。被害範囲分析として最も適切なものはどれか。

ア：ログイン成功はすべて正規利用とみなし、調査しない。

イ：認証ログ、接続元、時刻、実行操作を確認し、正規利用と不正利用を区別しながらアクセス先と変更内容を追跡する。

ウ：利用者IDを削除したら過去のアクセス先調査は不要とする。

エ：全サーバのログを削除し、利用者へ聞き取りだけ行う。

答え・解説 正答：イ

ア：盗まれた資格情報でも正常に認証できるため不十分です。

イ：アカウント単位で横断的に利用履歴を追うと、侵害範囲を把握しやすくなります。

ウ：既に変更・窃取されたデータがある可能性があります。

エ：客観的証拠を失います。

総合解説：認証情報の侵害では「どこで使われたか」「何をしたか」を追跡します。パスワード変更だけで影響分析を終了しないことが重要です。

対象：2026年度 / 基準日 2026-09-05

0067 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：標準

公開Webサーバ1台が既知脆弱性を悪用されて侵害された。同じ製品・バージョンを利用する他サーバもある。最も適切な対応はどれか。

ア：最初の1台を修復すれば他サーバは確認不要とする。

イ：製品名を変更して資産台帳に登録し直す。

ウ：資産台帳等で同じ脆弱性を持つサーバを特定し、侵害兆候の確認と緩和・修正を横断的に行う。

エ：他サーバのログを停止して攻撃を見えなくする。

答え・解説 正答：ウ

ア：同じ脆弱性が残っています。

イ：実際の脆弱性は解消しません。

ウ：共通脆弱性があれば他資産も同じ攻撃の対象になり得ます。

エ：検知能力を下げます。

総合解説：原因が共通する場合、個別復旧だけでなく同一条件を持つ全資産へ調査・是正を広げます。資産管理の精度が重要です。

対象：2026年度 / 基準日 2026-09-05

0068 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：標準

侵害サーバに機密ファイルが置かれていた。情報流出の有無を判断する方法として、最も適切なものはどれか。

ア：機密ファイルがあるだけで、必ず全データが流出したと断定する。

イ：外向き通信が少なければ、圧縮やクラウド経由の可能性を考えず流出なしと断定する。

ウ：調査が難しいのでログを削除し、流出なしとして報告する。

エ：ファイルアクセス、外向き通信、プロキシ・クラウドログ、攻撃者の操作履歴など複数の証拠を確認し、流出の可能性と不確実性を評価する。

答え・解説 正答：エ

ア：証拠なしの断定は不適切です。

イ：多様な持出し経路があり得ます。

ウ：事実と異なる判断につながります。

エ：機密ファイルが存在するだけでは流出を断定できず、アクセス・転送の証拠を調べます。

総合解説：情報流出評価では、証拠が不十分な場合も「確認できたこと・できないこと」を区別して報告します。過大・過小評価の双方を避けます。

対象：2026年度 / 基準日 2026-09-05

0069 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：応用

フィッシングで資格情報が窃取され、不正ログインが発生した。再発防止につながる原因分析として最も適切なものはどれか。

ア：メールが届いた経路、利用者判断、MFAの有無、条件付きアクセス、検知・報告手順など、複数の管理策がなぜ突破・未機能だったかを分析する。

イ：利用者一人を責めて終了し、技術・運用対策は見直さない。

ウ：パスワードを変更したので原因分析は不要とする。

エ：フィッシングは完全に防げないため、教育やMFAは無意味とする。

答え・解説 正答：ア

ア：「利用者がクリックした」で終わらず、組織的な防御と検知の弱点まで確認します。

イ：同様の攻撃が再発する可能性があります。

ウ：侵入を可能にした弱点が残ります。

エ：複数の対策で発生確率・影響を下げられます。

総合解説：根本原因分析は個人責任の追及だけではなく、プロセス・技術・組織要因の改善につなげるために行います。

対象：2026年度 / 基準日 2026-09-05

0070 分析・復旧 > 被害範囲・影響・原因分析 ｜ 難易度：応用

ログ欠損があり、侵入開始時刻を特定できない。分析報告として最も適切なものはどれか。

ア：証拠がない時刻を断定して、報告書を簡潔にする。

イ：確認できた最古の侵害兆候、欠損期間、推定範囲、判断根拠を示し、確定事項と推定事項を明確に分ける。

ウ：分からない点があるので、確認済み事実も全て無効とする。

エ：ログ欠損を隠し、完全な調査ができたと説明する。

答え・解説 正答：イ

ア：誤った断定は対応判断を誤らせます。

イ：証拠不足を隠さず、不確実性を明示する方が意思決定に有用です。

ウ：部分的に確かな情報は利用できます。

エ：説明責任と信頼性を損ないます。

総合解説：インシデント分析では完全な証拠が得られないことがあります。確度や前提、欠損を明示し、追加調査で更新可能な形にします。

対象：2026年度 / 基準日 2026-09-05

0071 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：基礎

インシデント対応における「根絶」の説明として、最も適切なものはどれか。

ア：影響端末をネットワークから切り離すだけで終了する。

イ：調査ログを削除する。

ウ：マルウェア、侵害アカウント、脆弱な設定、永続化機構など、侵害を継続・再発させる原因を除去する。

エ：報告書の表紙だけを作る。

答え・解説 正答：ウ

ア：隔離は主に封じ込めであり、根本原因が残る場合があります。

イ：証拠を失います。

ウ：根絶は単なる一時隔離ではなく、攻撃者の足場や原因を取り除く段階です。

エ：根絶とは無関係です。

総合解説：根絶では悪性ファイル削除だけでなく、脆弱性修正、資格情報再発行、設定是正、永続化の除去などを含めます。

対象：2026年度 / 基準日 2026-09-05

0072 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：基礎

侵害後のデータ復元で最も重要な考え方はどれか。

ア：最新なら内容を確認せず必ず安全とみなす。

イ：復元前にバックアップを感染端末へ書込み可能で接続する。

ウ：バックアップの復元テストは不要とする。

エ：侵害前の信頼できる時点のバックアップを選び、マルウェア混入や改ざんがないことを確認して復元する。

答え・解説 正答：エ

ア：最新バックアップが侵害後に取得されている場合があります。

イ：バックアップまで破壊される危険があります。

ウ：実際に復元できるか事前・事後の検証が必要です。

エ：侵害後のバックアップや感染済みバックアップを戻すと再感染する可能性があります。

総合解説：バックアップは「存在」だけでなく、隔離・完全性・復元可能性・復元時点を確認します。侵害の開始時刻推定も重要です。

対象：2026年度 / 基準日 2026-09-05

0073 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：基礎

侵害システムを業務へ戻す前に行うべき確認として、最も適切なものはどれか。

ア：原因・悪性要素が除去され、必要な修正が適用され、機能と監視が正常であることを検証する。

イ：画面が表示されたら即座に全利用者へ公開する。

ウ：監視を停止してから再接続する。

エ：原因が不明でも、復旧を急ぐため同じ脆弱な構成のまま戻す。

答え・解説 正答：ア

ア：再開前に再侵入・再感染のリスクが許容可能まで下がっているかを確認します。

イ：機能表示だけでは安全性を確認できません。

ウ：再発兆候を検知できなくなります。

エ：再侵入の可能性が高まります。

総合解説：復旧は「動けば終わり」ではありません。根絶・修正・検証・監視を経て、業務所有者と合意した再開基準を満たします。

対象：2026年度 / 基準日 2026-09-05

0074 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：標準

管理者資格情報が窃取された可能性がある。復旧時の対応として最も適切なものはどれか。

ア：同じパスワードを再設定して復旧完了とする。

イ：影響を受けた資格情報を失効・再発行し、依存するサービスアカウントやトークン等も漏れなく見直す。

ウ：アカウント名だけ変更し、認証トークンはそのまま残す。

エ：認証情報の窃取が疑われても、アクセスログを見ない。

答え・解説 正答：イ

ア：攻撃者が既知の値を再利用できます。

イ：一つのパスワード変更だけでは関連資格情報が残る場合があります。

ウ：既存トークンが悪用される可能性があります。

エ：影響範囲特定が不十分です。

総合解説：資格情報侵害ではパスワード、秘密鍵、APIキー、セッショントークン、復旧コードなどを体系的に洗い出して再発行します。

対象：2026年度 / 基準日 2026-09-05

0075 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：標準

多数システムが停止したインシデントから復旧する。最も適切な順序の決め方はどれか。

ア：担当者が好きなシステムから順に復旧する。

イ：依存関係を無視し、上位アプリだけ先に起動する。

ウ：事業影響、依存関係、RTO等を踏まえ、重要サービスとその前提システムから段階的に復旧する。

エ：重要度に関係なくファイル名順で復旧する。

答え・解説 正答：ウ

ア：業務優先度と一致しません。

イ：必要な認証・DB等が未復旧ならサービスできません。

ウ：復旧順序は技術的な簡単さだけでなく、事業優先度と依存関係で決めます。

エ：事業影響を反映していません。

総合解説：大規模復旧ではBIAや継続計画で定めた優先度を活用します。認証、ネットワーク、DB等の依存関係も考慮します。

対象：2026年度 / 基準日 2026-09-05

0076 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：標準

高度な侵害で、OSのどこまで改ざんされたか確信できない。復旧方法として最も適切な考え方はどれか。

ア：見つかった悪性ファイル1個だけ削除すれば必ず安全になる。

イ：侵害の深さに関係なく、再構築は常に禁止する。

ウ：安全性を確認せず、侵害端末のイメージを全端末へ配布する。

エ：信頼できる状態を証明できない場合は、既知の安全なイメージから再構築する方が確実性を高められる。

答え・解説 正答：エ

ア：未知の永続化や追加改ざんが残る可能性があります。

イ：リスクに応じて再構築が適切な場合があります。

ウ：被害を拡大します。

エ：深い侵害では悪性要素の取り残しを避けるため再構築が選ばれる場合があります。

総合解説：復旧方法は侵害の深さと証拠、再構築コスト、復旧時間で判断します。「信頼できる状態へ戻せるか」が重要です。

対象：2026年度 / 基準日 2026-09-05

0077 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：標準

侵害サーバを復旧してネットワークへ戻した直後の運用として、最も適切なものはどれか。

ア：一定期間、関連IOC、認証、通信、プロセス等を重点監視し、再侵入や残存活動の兆候を確認する。

イ：復旧したので監視ルールを全て解除する。

ウ：復旧ログを削除してディスクを軽くする。

エ：同じ脆弱な設定へ戻し、変化を避ける。

答え・解説 正答：ア

ア：復旧直後は根絶漏れや再攻撃の有無を確認する重要な期間です。

イ：再発を見逃す可能性があります。

ウ：検証・追跡情報を失います。

エ：再侵入リスクが残ります。

総合解説：復旧後の監視は、対応が有効だったかを検証する工程でもあります。再発兆候があれば再度分析・封じ込めへ戻ります。

対象：2026年度 / 基準日 2026-09-05

0078 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：標準

ランサムウェア被害から復旧する際、バックアップ運用として最も適切なものはどれか。

ア：通常時からバックアップを全利用者が削除可能にする。

イ：侵害範囲から分離されたバックアップを保全し、復元前に完全性と復元可能性を確認する。

ウ：復元テストを行わず、バックアップがあるという表示だけを信頼する。

エ：感染端末の自動同期先だけを唯一のバックアップにする。

答え・解説 正答：イ

ア：攻撃者や誤操作で失われる危険があります。

イ：バックアップが攻撃者から到達可能だと暗号化・削除される可能性があります。

ウ：実際に復元できない可能性があります。

エ：暗号化が同期される可能性があります。

総合解説：ランサムウェア対策ではバックアップの分離、権限制御、複数世代、復元テストが重要です。復旧時には侵害前の安全な時点を選びます。

対象：2026年度 / 基準日 2026-09-05

0079 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：応用

重大インシデント後、技術担当者は「サーバは起動した」と報告したが、業務部門はデータ整合性を確認できていない。最も適切な判断はどれか。

ア：OSが起動した時点で自動的に全面再開する。

イ：業務部門の確認は不要とし、技術担当者一人で決定する。

ウ：技術的稼働だけで再開せず、データ整合性、必要なセキュリティ対策、業務手順を確認し、権限者が再開を承認する。

エ：整合性確認を省略する代わりにログを削除する。

答え・解説 正答：ウ

ア：業務データや統制の確認が不足しています。

イ：事業影響を適切に評価できない可能性があります。

ウ：業務再開は技術部門だけでなく業務所有者を含む判断です。

エ：リスクを増やします。

総合解説：復旧完了の定義を事前に決め、セキュリティ・機能・データ・業務の各観点を確認します。再開後も監視を継続します。

対象：2026年度 / 基準日 2026-09-05

0080 分析・復旧 > 根絶・復元・業務再開 ｜ 難易度：応用

マルウェアを削除しパッチを適用した後、同じ端末で再び不審通信が発生した。最も適切な対応はどれか。

ア：一度根絶作業をしたので、再発ログは誤りとして削除する。

イ：不審通信先を許可リストへ登録してアラートを止める。

ウ：端末名だけ変更して再調査を終了する。

エ：根絶が不完全だった可能性を考え、永続化、別侵入経路、盗まれた資格情報、同一ネットワーク上の感染源を再調査する。

答え・解説 正答：エ

ア：再侵入・残存活動を見逃します。

イ：攻撃通信を許可する危険があります。

ウ：原因は解消されません。

エ：再発は根本原因や範囲特定が不十分だった兆候です。

総合解説：インシデント対応は直線的ではなく、復旧後の兆候によって分析・封じ込め・根絶へ戻ることがあります。検証とフィードバックが重要です。

対象：2026年度 / 基準日 2026-09-05

0081 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：基礎

インシデント報告書に記載する内容として、最も適切なものはどれか。

ア：発生・検知の経緯、影響、対応、根拠となる事実、未確定事項、今後の対策などを整理する。

イ：担当者の感想だけを書き、発生日時や影響を記載しない。

ウ：不明点をすべて断定して見栄えを整える。

エ：証拠となる記録を報告後すぐ全て削除する。

答え・解説 正答：ア

ア：後から経緯と判断を追跡できるよう、事実と対応履歴を構造化します。

イ：意思決定や再発防止に利用できません。

ウ：誤情報を生みます。

エ：監査・法務・改善のための記録が失われます。

総合解説：インシデント報告は単なる結果報告ではなく、意思決定、説明責任、再発防止の基礎資料です。更新履歴も残します。

対象：2026年度 / 基準日 2026-09-05

0082 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：基礎

調査途中のインシデントについて関係者へ説明するとき、最も適切な方法はどれか。

ア：原因が不明でも最もありそうな攻撃者を断定する。

イ：確認済み事実、推定、未確認事項を区別し、今後更新する前提で伝える。

ウ：不確実な点が一つでもあれば、確認済み事実も共有しない。

エ：担当者ごとに異なる内容を自由に外部発信する。

答え・解説 正答：イ

ア：根拠のない断定は不適切です。

イ：不確実性を明示することで誤解や誤った意思決定を減らせます。

ウ：必要な意思決定が遅れる可能性があります。

エ：情報不整合が生じます。

総合解説：インシデント中は情報が変化します。確度を明示し、更新時刻と情報源を管理すると、関係者の共通認識を保ちやすくなります。

対象：2026年度 / 基準日 2026-09-05

0083 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：基礎

外部公表が必要となる可能性のある重大インシデントで、CSIRT以外に連携すべき部門の例として最も適切なものはどれか。

ア：CSIRTだけで全て決定し、経営層や広報へ知らせない。

イ：技術部門と無関係な外部SNS利用者だけに相談する。

ウ：経営層、法務、広報、個人情報・コンプライアンス、業務部門など、事案に応じた関係者。

エ：誰にも共有せず、担当者個人で公表する。

答え・解説 正答：ウ

ア：重大な事業判断を適切に行えない可能性があります。

イ：組織の責任ある意思決定になりません。

ウ：技術対応だけでなく法的・契約的・顧客対応の判断が必要になるため部門横断の連携が重要です。

エ：統制された発信になりません。

総合解説：事前にコミュニケーション計画と役割を定め、重大時の意思決定・承認ルートを明確にします。

対象：2026年度 / 基準日 2026-09-05

0084 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：標準

情報漏えいの可能性があるが、対象件数はまだ調査中である。外部発表の考え方として最も適切なものはどれか。

ア：件数が不明なので、根拠なく最大件数を確定値として発表する。

イ：調査が完全終了するまで、どのような法的・契約上の通知義務も無視する。

ウ：担当者ごとに異なる推定値をSNSへ投稿する。

エ：法令・契約・社内方針と緊急性に従い、確認済みの範囲を公表し、未確定事項は未確定と明示して必要に応じ更新する。

答え・解説 正答：エ

ア：誤情報になります。

イ：要件によっては迅速な通知が必要な場合があります。

ウ：情報の一貫性を損ないます。

エ：公表の正確性と適時性を両立させる必要があります。

総合解説：外部コミュニケーションは法務・広報等と調整し、単一の承認済み情報源を使います。更新が必要なら訂正・追記を明示します。

対象：2026年度 / 基準日 2026-09-05

0085 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：標準

利用者アカウント情報の漏えいが確認され、パスワード再設定が必要になった。利用者への案内として最も適切なものはどれか。

ア：何が起きたか、影響対象、必要なパスワード変更やMFA確認など、利用者が取るべき具体的な行動を分かりやすく伝える。

イ：専門用語だけを並べ、利用者が何をすべきか書かない。

ウ：漏えいを隠すため、利用者へ何も知らせずアカウントを放置する。

エ：全利用者のパスワードをメール本文に平文で送る。

答え・解説 正答：ア

ア：受け手が自ら被害低減できる情報を提供することが重要です。

イ：実際の被害低減につながりにくい案内です。

ウ：必要な防御行動が取れません。

エ：新たな情報漏えいリスクになります。

総合解説：関係者対応では、事実、影響、対処方法、問い合わせ窓口を明確にします。受け手別に必要情報を整理します。

対象：2026年度 / 基準日 2026-09-05

0086 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：標準

重大インシデント発生時に、監督機関、警察、JPCERT/CC、保険会社など外部組織への連絡が必要になる場合がある。最も適切な準備はどれか。

ア：外部連絡は担当者の気分で決め、記録しない。

イ：自組織に適用される法令・契約・保険条件を整理し、連絡条件、窓口、期限、承認者を事前に手順化する。

ウ：どのインシデントでも必ず同じ外部機関へ全情報を無条件提供する。

エ：契約上の通知条件はセキュリティ部門に関係ないので確認しない。

答え・解説 正答：イ

ア：一貫性・期限遵守・説明責任を損ないます。

イ：緊急時に初めて調べると遅延するため、平常時に連絡要件を整理します。

ウ：必要性や機密性、法的要件を考慮すべきです。

エ：契約違反や対応遅延につながる可能性があります。

総合解説：外部報告先は事案ごとに異なります。法務・コンプライアンスと連携し、連絡先と手順を最新に保ちます。

対象：2026年度 / 基準日 2026-09-05

0087 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：標準

自社の侵害により取引先との共有アカウントが悪用された可能性がある。最も適切な対応はどれか。

ア：自社内の問題なので取引先へ一切知らせない。

イ：詳細未確認のまま取引先を攻撃者と断定して公表する。

ウ：取引先へ必要な事実と推奨対処を速やかに共有し、資格情報変更やアクセス遮断などを共同で調整する。

エ：共有資格情報をそのまま使い続け、ログだけ削除する。

答え・解説 正答：ウ

ア：取引先側に影響が及ぶ可能性があります。

イ：根拠のない断定です。

ウ：相互接続がある場合、片側だけの対応ではリスクが残ります。

エ：悪用継続の危険があります。

総合解説：サプライチェーンや委託先との接続では、連絡先と責任分担を契約・手順で事前に整理します。インシデント時は共同で封じ込めます。

対象：2026年度 / 基準日 2026-09-05

0088 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：標準

インシデント対応中、広報、営業、サポートが別々の数字を顧客へ伝え始めた。最も適切な改善はどれか。

ア：各部門が独自の推測を優先し、統一しない。

イ：数字の違いを隠すため、記録を全て削除する。

ウ：最も大きい数字を常に採用し、根拠確認をしない。

エ：承認済みの最新情報を管理する単一の情報源と発信責任者を定め、更新時に関係部門へ同期する。

答え・解説 正答：エ

ア：顧客混乱と信頼低下につながります。

イ：原因を追跡できなくなります。

ウ：正確性が確保できません。

エ：発信の不一致を防ぐには、情報の版管理と承認ルートが重要です。

総合解説：重大インシデントでは情報更新が頻繁です。状況報告の版、時刻、承認者、配布先を管理し、一貫したコミュニケーションを維持します。

対象：2026年度 / 基準日 2026-09-05

0089 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：応用

インシデント収束後の事後レビューで、最も適切な活動はどれか。

ア：うまくいった点・失敗した点・根本原因・検知や連絡の課題を整理し、改善策に担当者と期限を設定して追跡する。

イ：原因を個人の責任だけにして、技術・手順の改善は行わない。

ウ：収束したので記録を破棄し、振り返りを行わない。

エ：改善策を大量に列挙するだけで、担当者や期限を決めない。

答え・解説 正答：ア

ア：教訓を具体的な改善タスクへ落とし込み、実施状況まで確認することが重要です。

イ：再発防止につながりにくい方法です。

ウ：同じ問題を繰り返す可能性があります。

エ：実行されず形骸化しやすくなります。

総合解説：インシデント対応は継続的改善の入力です。検知ルール、教育、設計、契約、連絡網、バックアップなど幅広い統制へ教訓を反映します。

対象：2026年度 / 基準日 2026-09-05

0090 分析・復旧 > 報告・情報公開・関係者対応 ｜ 難易度：応用

経営層へ重大インシデントを報告する際の内容として、最も適切なものはどれか。

ア：マルウェアの16進ダンプだけを数百ページ提示し、事業影響は説明しない。

イ：技術詳細を必要な範囲に整理し、事業影響、対応状況、残存リスク、必要な意思決定、今後の見通しを明示する。

ウ：不明点を隠し、復旧時刻を根拠なく確約する。

エ：重大な残存リスクを報告せず、収束したように見せる。

答え・解説 正答：イ

ア：経営判断に必要な情報が不足します。

イ：経営層には事業判断に必要な情報を簡潔かつ正確に提示することが重要です。

ウ：誤った期待と意思決定を招きます。

エ：リスク受容や追加投資の判断ができません。

総合解説：経営報告では、確定事実と不確実性、選択肢とリスクを示します。技術チームと経営層の情報粒度を調整することもCSIRTの重要な役割です。

対象：2026年度 / 基準日 2026-09-05

0091 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：基礎

重要データのバックアップにおける「3-2-1ルール」の説明として、最も適切なものはどれか。

ア：運用データを含め3つのコピーを持ち、2種類の異なる媒体に保存し、そのうち1つを異なる場所に保管する。

イ：3日に1回バックアップし、2年間保存し、1人の管理者だけが利用する。

ウ：3台の同型ディスクに同じ筐体内で複製し、2つを常時接続し、1つを同じラックに保管する。

エ：本番データを1つだけ保持し、2種類の暗号方式で暗号化し、3個の鍵を作る。

答え・解説 正答：ア

ア：3-2-1ルールは、コピー数・媒体の多様化・保管場所の分離によって同時喪失のリスクを下げる考え方です。

イ：3-2-1の数字は取得間隔・保存年数・管理者数を表すものではありません。

ウ：同一場所・同一障害ドメインに集中すると、災害やランサムウェアで同時に失う可能性が残ります。

エ：3-2-1は暗号方式や鍵数を示すルールではありません。

総合解説：3-2-1ルールはバックアップの単一障害点を減らす基本原則です。重要データでは、オフライン化・イミュータブル化や復元試験も組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0092 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：基礎

バックアップの一部をオフサイトに保管する主な目的として、最も適切なものはどれか。

ア：バックアップの暗号化を不要にする。

イ：火災・水害・盗難などで主拠点と同時にバックアップまで失うリスクを低減する。

ウ：RPOを必ずゼロにする。

エ：障害発生時の原因分析を不要にする。

答え・解説 正答：イ

ア：オフサイト保管であっても機密性保護は必要で、暗号化が不要になるわけではありません。

イ：地理的・物理的に保管場所を分離することで、同一拠点の災害や物理事故による同時喪失を抑えます。

ウ：RPOはバックアップやレプリケーションの頻度・方式に左右され、保管場所だけではゼロになりません。

エ：保管場所を分けても、障害やインシデントの原因分析は必要です。

総合解説：オフサイト化は「同じ場所にある本番とバックアップが一度に失われる」リスクへの対策です。

対象：2026年度 / 基準日 2026-09-05

0093 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：基礎

ランサムウェア対策としてバックアップを保護する方法の説明として、最も適切なものはどれか。

ア：バックアップ先を本番と同じ管理者アカウントだけで管理し、常時書込み可能にする。

イ：バックアップを取得したら復元試験は行わず、保存成功のログだけを確認する。

ウ：重要なバックアップの一部を攻撃者から直接到達しにくいオフライン又はイミュータブルな状態で保持し、復元可能性を定期確認する。

エ：ランサムウェアはバックアップを攻撃しないので、本番と同一共有フォルダに置く。

答え・解説 正答：ウ

ア：本番側の資格情報が侵害された場合にバックアップまで削除・暗号化される危険が高まります。

イ：保存成功と復元成功は同義ではありません。定期的な復元試験が必要です。

ウ：常時接続されたバックアップだけに依存せず、改ざん・削除されにくいコピーを持ち、実際に戻せることを確認するのが重要です。

エ：ランサムウェアは到達可能なバックアップを暗号化・削除することがあります。

総合解説：CISAはオフライン・暗号化・イミュータブルなバックアップと定期的な復元確認を推奨しています。

対象：2026年度 / 基準日 2026-09-05

0094 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：標準

WORM（Write Once Read Many）型ストレージの特徴として、最も適切なものはどれか。

ア：保存したデータを自動的に匿名化して個人情報ではなくする。

イ：全ての保存データを自動的に公開情報へ変更する。

ウ：ネットワーク障害時に必ず別拠点へ通信経路を切り替える。

エ：書き込んだデータを所定の条件・保持期間中は変更や削除しにくくし、読み出しを可能にする。

答え・解説 正答：エ

ア：WORMは匿名化技術ではありません。

イ：WORMは公開範囲を変更する技術ではありません。

ウ：これは冗長化・フェイルオーバーの説明で、WORMの機能ではありません。

エ：WORMは書込み後の改ざん・削除を制限することで、データ完全性や保存性を高める技術です。

総合解説：WORMはバックアップの改ざん耐性を高める選択肢ですが、機密性は別途暗号化やアクセス制御で保護します。

対象：2026年度 / 基準日 2026-09-05

0095 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：標準

バックアップ運用で「取得成功」の記録だけでなく、定期的なリストア試験を行う理由として最も適切なものはどれか。

ア：媒体破損、設定不備、鍵不足、手順不備などにより、保存済みでも実際には復元できない状態を検出するため。

イ：バックアップ容量を常に本番容量の半分以下にするため。

ウ：全システムのRTOを自動的にゼロにするため。

エ：復元後のセキュリティ確認を不要にするため。

答え・解説 正答：ア

ア：バックアップの存在だけでは復旧可能性を保証できず、リストア試験でデータと手順の有効性を確認します。

イ：復元試験の目的は容量削減ではありません。

ウ：試験は復旧能力を検証しますが、RTOを自動的にゼロにはしません。

エ：復元後もマルウェア残存や設定不備などの確認が必要です。

総合解説：「バックアップがある」と「必要な時間内に正しく復元できる」は別問題です。復元試験は事業継続の実効性確認に直結します。

対象：2026年度 / 基準日 2026-09-05

0096 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：標準

業務データのRPOを「最大1時間分のデータ損失まで許容」と設定した。単純な定期バックアップだけで対応する場合、最も整合的な運用はどれか。

ア：バックアップは月1回でよいが、媒体を3種類にする。

イ：障害時の失われる更新量が目標を超えにくいよう、少なくともRPOを満たせる頻度でバックアップを取得する。

ウ：RPOはバックアップ頻度と無関係なので、年1回でもよい。

エ：RPOを満たすため、バックアップの暗号化を解除する。

答え・解説 正答：イ

ア：媒体の多様化は重要でも、月1回では1時間RPOを満たせません。

イ：RPOはどの時点までデータを戻せればよいかという目標であり、バックアップ頻度はその達成可否に直接影響します。

ウ：定期バックアップ方式では取得間隔がデータ損失量に影響します。

エ：暗号化の有無はRPO達成のための取得間隔とは別論点です。

総合解説：RPOから逆算してバックアップ・レプリケーション方式と頻度を設計します。

対象：2026年度 / 基準日 2026-09-05

0097 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：標準

バックアップを複数世代保持する利点として、最も適切なものはどれか。

ア：バックアップの機密性対策を一切行わなくてよくなる。

イ：どの世代でも必ずマルウェアが存在しないと保証できる。

ウ：破損や不正変更の発見が遅れ、最新バックアップにも問題が含まれている場合に、より前の正常時点へ戻せる可能性を高める。

エ：本番システムの冗長化が不要になる。

答え・解説 正答：ウ

ア：世代管理と機密性保護は別です。

イ：複数世代でも感染済みの可能性はあり、復元前の検証が必要です。

ウ：複数世代があれば、問題発生前の復元点を選べる余地が広がります。

エ：バックアップと可用性の冗長化は役割が異なります。

総合解説：世代管理は誤更新・破損・侵害の発見遅延に備える基本策です。

対象：2026年度 / 基準日 2026-09-05

0098 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：標準

ランサムウェア攻撃で本番側の管理者アカウントが奪取されるリスクを考慮したバックアップ管理として、最も適切なものはどれか。

ア：運用を簡単にするため全従業員へバックアップ削除権限を付与する。

イ：本番とバックアップで共有する管理者パスワードを文書に平文で保存する。

ウ：バックアップ装置の監査ログを無効にして操作痕跡を残さない。

エ：バックアップ基盤の管理権限を必要最小限にし、本番環境と同一資格情報への過度な依存を避ける。

答え・解説 正答：エ

ア：最小権限に反し、誤操作・内部不正・侵害時の被害を拡大します。

イ：資格情報漏えい時の影響を拡大します。

ウ：異常操作の検知・追跡が困難になります。

エ：資格情報や権限を分離すると、本番の侵害がそのままバックアップ削除へ連鎖するリスクを低減できます。

総合解説：バックアップそのものだけでなく、バックアップを変更・削除できる権限と資格情報を守る必要があります。

対象：2026年度 / 基準日 2026-09-05

0099 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：応用

A社では毎晩バックアップジョブが「成功」と表示されるが、半年間リストア試験をしていない。重要システムの復旧確実性を高める改善として最も適切なものはどれか。

ア：代表データやシステムを隔離された検証環境で定期的に復元し、完全性と手順、所要時間を確認する。

イ：ジョブログを保存しているので、復元試験を永久に省略する。

ウ：バックアップ先の削除権限を利用者全員へ付与する。

エ：復元に失敗した場合に備えて、原因を調べずバックアップ世代を全削除する。

答え・解説 正答：ア

ア：復元試験により、データの可読性だけでなく手順・依存関係・時間目標まで実践的に検証できます。

イ：ジョブ成功ログだけでは実際の復元可能性を保証できません。

ウ：誤削除や攻撃による破壊のリスクを高めます。

エ：原因究明前の全削除は利用可能な復元点まで失うおそれがあります。

総合解説：復旧能力は「作ったバックアップ」を実際に戻して初めて検証できます。

対象：2026年度 / 基準日 2026-09-05

0100 事業継続・バックアップ > バックアップ・3-2-1ルール・WORM ｜ 難易度：応用

B社は本番サーバと同一ネットワーク上のNASへ毎日1世代だけバックアップしている。ランサムウェアと拠点災害の双方に備える改善として最も適切なものはどれか。

ア：NASを同じネットワークにもう1台追加し、同じ管理者資格情報で同時同期するだけにする。

イ：複数コピー・異なる媒体・別拠点を組み合わせ、少なくとも一部をオフライン又はイミュータブルにし、複数世代と復元試験を運用する。

ウ：本番サーバのディスク容量を増やし、バックアップを廃止する。

エ：バックアップ先を暗号化せず、誰でも読み書きできる共有フォルダに変更する。

答え・解説 正答：イ

ア：同一ネットワーク・同一資格情報では同じ攻撃で両方が侵害される可能性があります。

イ：単一NAS・単一世代・同一拠点は複数の共通原因障害に弱いため、分散・改ざん耐性・世代・復元確認を組み合わせるべきです。

ウ：容量拡張はデータ破損・攻撃・災害に対するバックアップの代替ではありません。

エ：機密性・完全性とも悪化し、攻撃時の被害を拡大します。

総合解説：バックアップ設計では、障害ドメインの分離、改ざん耐性、世代管理、復元試験を組み合わせて考えます。

対象：2026年度 / 基準日 2026-09-05

0101 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：基礎

BCPとBCMの関係について、最も適切なものはどれか。

ア：BCPは暗号鍵管理だけを定め、BCMは暗号方式を選ぶ活動である。

イ：BCPは緊急時の事業継続・復旧の計画であり、BCMはその計画を含め、平時から継続的に事業継続能力を管理・改善する活動である。

ウ：BCPとBCMはどちらもバックアップ媒体の製品名である。

エ：BCMは事故発生後だけ実施し、平時の準備はBCPに含めない。

答え・解説 正答：イ

ア：BCP/BCMは事業継続に関する概念で、暗号技術だけを扱うものではありません。

イ：BCMは計画作成だけでなく、分析、対策、教育、演習、見直しを継続するマネジメント活動です。

ウ：いずれも製品名ではありません。

エ：BCMは平時から継続的に準備・改善する活動です。

総合解説：事業継続は「計画書を作って終わり」ではなく、BCMとして訓練・評価・改善を回すことが重要です。

対象：2026年度 / 基準日 2026-09-05

0102 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：基礎

BIAを実施する際に優先して把握すべき内容として、最も適切なものはどれか。

ア：全ての脆弱性に同じCVSS値を付ける。

イ：バックアップデータを自動的に暗号化する。

ウ：業務停止が時間経過とともに与える影響や重要業務・依存関係を把握し、復旧優先順位や目標設定の根拠にする。

エ：利用者のパスワードを定期変更させるだけの活動である。

答え・解説 正答：ウ

ア：BIAは脆弱性スコアリングの手法ではありません。

イ：BIAは分析活動であり暗号化機能ではありません。

ウ：BIAは停止影響を分析して重要な業務・資源を識別し、継続・復旧戦略の基礎を作ります。

エ：認証運用は一部の対策であり、BIAの目的ではありません。

総合解説：BIAの結果はRTO/RPO、代替手段、復旧順序、必要資源の検討につながります。

対象：2026年度 / 基準日 2026-09-05

0103 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：基礎

RTO（Recovery Time Objective）の説明として、最も適切なものはどれか。

ア：復旧時に許容するデータ損失量を時間で表した目標である。

イ：バックアップを保管する法定年数である。

ウ：暗号鍵を更新する周期である。

エ：中断後、対象業務やシステムを目標とする水準まで復旧させるまでの目標時間である。

答え・解説 正答：エ

ア：これはRPOの説明です。

イ：RTOは保存年限ではありません。

ウ：RTOは鍵管理の周期ではありません。

エ：RTOは「いつまでに復旧させるか」という時間目標です。

総合解説：RTOは業務停止の許容度と復旧能力の両方を踏まえて設定します。

対象：2026年度 / 基準日 2026-09-05

0104 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：標準

RPO（Recovery Point Objective）の説明として、最も適切なものはどれか。

ア：障害発生時に、どの時点までのデータを復元できればよいかを表す目標で、許容できるデータ損失量を時間の観点で示す。

イ：障害発生からシステム再開までの目標時間である。

ウ：災害復旧拠点までの物理距離である。

エ：インシデント報告書の作成期限である。

答え・解説 正答：ア

ア：RPOは復旧させるデータの時点に関する目標です。

イ：これはRTOの説明です。

ウ：RPOは距離の指標ではありません。

エ：RPOは報告期限ではありません。

総合解説：RPOが短いほど、より頻繁なバックアップやレプリケーションなどが必要になり、一般にコストも増えます。

対象：2026年度 / 基準日 2026-09-05

0105 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：標準

複数業務が同時停止した場合の復旧優先順位を決める方法として、最も適切なものはどれか。

ア：サーバ名のアルファベット順だけで決める。

イ：BIAで確認した停止影響、重要度、時間的制約、他業務への依存関係などを基に優先順位を決める。

ウ：機器価格が安い順だけで決める。

エ：担当者が最も使い慣れているシステムを必ず最優先にする。

答え・解説 正答：イ

ア：事業影響を反映できません。

イ：復旧順序はシステム担当者の感覚だけでなく、事業影響と依存関係に基づいて決めます。

ウ：価格だけでは業務重要度を判断できません。

エ：個人の慣れではなく事業影響を基準にします。

総合解説：重要業務の復旧には、認証、ネットワーク、データベースなど前提サービスの依存関係も考慮します。

対象：2026年度 / 基準日 2026-09-05

0106 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：標準

短いRTOと短いRPOを要求される重要システムの継続対策を検討する際、最も適切な考え方はどれか。

ア：RTO/RPOに関係なく、全システムで年1回のバックアップだけに統一する。

イ：RPOが短いほどバックアップ頻度を下げる。

ウ：目標を満たせるよう、冗長化・レプリケーション・バックアップ頻度・代替拠点などを組み合わせ、コストとのバランスを評価する。

エ：RTOを満たすにはログを全て削除する。

答え・解説 正答：ウ

ア：重要度や目標が異なるのに一律方式では要件を満たせない可能性があります。

イ：一般には逆で、短いRPOにはより高頻度な保護が必要です。

ウ：RTO/RPOは技術方式の選定条件となり、必要水準と費用のトレードオフを評価します。

エ：ログ削除は復旧時間目標の達成策ではありません。

総合解説：目標値を決めるだけでなく、それを満たす設計・運用・演習まで落とし込むことが重要です。

対象：2026年度 / 基準日 2026-09-05

0107 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：標準

BCPを策定した後に定期的な訓練・演習を行う主な理由として、最も適切なものはどれか。

ア：一度演習すれば以後の組織変更やシステム変更を無視できるため。

イ：演習を行えば全てのインシデントを完全に防止できるため。

ウ：演習では失敗を記録せず、成功した点だけを残すため。

エ：連絡網、判断手順、代替手段、復旧手順などが実際に機能するか確認し、見つかった課題を改善するため。

答え・解説 正答：エ

ア：環境変化に応じて計画・演習は更新が必要です。

イ：演習は対応能力を高めますが事故をゼロに保証しません。

ウ：課題や失敗を記録して改善につなげることが重要です。

エ：文書だけでは実効性を確認できないため、演習で人・手順・技術の弱点を把握します。

総合解説：訓練・演習はBCMの継続的改善の中心であり、BIAやRTO/RPOの妥当性確認にも役立ちます。

対象：2026年度 / 基準日 2026-09-05

0108 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：標準

業務システムAのRTOを2時間と設定したが、Aが依存する認証基盤BのRTOは8時間である。この状態への評価として最も適切なものはどれか。

ア：Aの復旧にBが必須なら、依存関係を踏まえてBのRTOや代替手段を見直さないとAのRTOを達成できない可能性が高い。

イ：AのRTOは2時間なので、Bが8時間停止してもAは必ず2時間で利用できる。

ウ：RTOは文書上の目標なので依存関係は考慮しなくてよい。

エ：AとBのログ保存期間を同じにすればRTOの矛盾は自動的に解消する。

答え・解説 正答：ア

ア：個別システムの目標だけでなく、前提サービスを含む復旧連鎖を整合させる必要があります。

イ：Bが必須なら実際の利用再開はBの復旧に制約されます。

ウ：実現可能性を伴わない目標では事業継続に役立ちません。

エ：ログ保存期間と復旧時間の依存関係は別論点です。

総合解説：BIAでは業務・システム間の依存関係を明らかにし、復旧順序と目標を整合させます。

対象：2026年度 / 基準日 2026-09-05

0109 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：応用

受注システムは「停止は4時間以内、データ損失は最大15分相当まで」と事業部門が要求している。最も適切な解釈はどれか。

ア：RTOは15分、RPOは4時間である。

イ：RTOは4時間、RPOは15分を目標とし、それを満たせる復旧方式とデータ保護方式を設計・検証する。

ウ：RTOとRPOはいずれも4時間である。

エ：RTO/RPOはバックアップ媒体の種類だけで決まり、業務要件は不要である。

答え・解説 正答：イ

ア：RTOとRPOを逆にしています。

イ：停止許容時間はRTO、許容データ損失の時間幅はRPOに対応します。

ウ：データ損失要件15分が反映されていません。

エ：事業要求・BIAを根拠に設定します。

総合解説：RTO/RPOは事業側の影響許容度から導き、技術設計と復旧試験で実現性を確認します。

対象：2026年度 / 基準日 2026-09-05

0110 事業継続・バックアップ > BCP・BCM・BIA・RTO・RPO ｜ 難易度：応用

全システムにRTO=0、RPO=0を一律要求すると非常に高コストになることが分かった。BCMとして最も適切な対応はどれか。

ア：コストが高いので全システムのBCPを廃止する。

イ：目標値を達成できなくても、文書に0と書いておけばよい。

ウ：BIAで業務影響と重要度を再確認し、必要なシステムに相応の目標を設定して、費用対効果を含め経営判断する。

エ：全システムで同じ復旧方式しか認めない。

答え・解説 正答：ウ

ア：事業継続リスクを無視する対応です。

イ：実現可能性のない目標は有効な計画になりません。

ウ：重要度に応じて目標を差別化し、リスクとコストをバランスさせるのが現実的です。

エ：業務重要度・要件に応じた方式選択が必要です。

総合解説：BCMでは事業影響に基づき優先順位を付け、実現可能で説明可能な継続戦略を選びます。

対象：2026年度 / 基準日 2026-09-05

0111 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：基礎

システム冗長化とバックアップの関係について、最も適切なものはどれか。

ア：冗長化していればバックアップは常に不要である。

イ：バックアップがあればサービス停止は必ずゼロになる。

ウ：冗長化は停止時間の短縮に有効だが、誤削除やランサムウェアによるデータ破壊が複製される場合があるため、独立したバックアップも必要である。

エ：冗長化はデータの機密性を自動的に保証する。

答え・解説 正答：ウ

ア：論理的な破損や攻撃が冗長系にも同期されるため、バックアップは必要です。

イ：復元には時間を要し、可用性の冗長化とは異なります。

ウ：可用性向上の冗長化と、過去時点へ戻すバックアップは目的が異なり、相互に代替できません。

エ：冗長化の主目的は可用性であり、機密性は別対策です。

総合解説：冗長化・バックアップ・代替拠点は、それぞれ異なる障害に備えるため組み合わせます。

対象：2026年度 / 基準日 2026-09-05

0112 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：基礎

フェイルオーバーの説明として、最も適切なものはどれか。

ア：障害時に全バックアップを削除する処理である。

イ：暗号鍵を利用者間で共有する仕組みである。

ウ：脆弱性情報へCVE番号を付与する仕組みである。

エ：稼働中の系に障害が発生したとき、待機系など別の系へ処理を切り替えることでサービス継続を図る仕組みである。

答え・解説 正答：エ

ア：バックアップ削除ではありません。

イ：認証・鍵管理とは別です。

ウ：CVE識別とは無関係です。

エ：フェイルオーバーは障害時の切替により可用性を高めます。

総合解説：自動フェイルオーバーでも、切替条件、データ整合性、復帰手順などを事前に検証する必要があります。

対象：2026年度 / 基準日 2026-09-05

0113 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：基礎

広域災害に備えてDRサイトを設ける際の考え方として、最も適切なものはどれか。

ア：主拠点と同一災害で同時に停止しにくいよう、電力・通信・地理などの共通障害要因を考慮して分離する。

イ：主拠点と同じ建物の同じフロアに置けば広域災害に強くなる。

ウ：DRサイトではバックアップや復旧手順を用意しなくてよい。

エ：DRサイトを設ければBIAは不要になる。

答え・解説 正答：ア

ア：物理的距離だけでなく、電力系統や通信経路など共通依存も確認します。

イ：同一建物では共通原因による同時停止リスクが高いです。

ウ：代替拠点でもデータ・手順・人員の準備が必要です。

エ：必要な復旧水準を決めるためBIAは依然重要です。

総合解説：DR戦略では共通障害モードを避け、目標RTO/RPOを満たす接続・データ同期・切替方法を設計します。

対象：2026年度 / 基準日 2026-09-05

0114 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：標準

災害復旧訓練でバックアップからシステムをリストアした。確認事項として最も適切なものはどれか。

ア：復元コマンドが終了した時点で、内容確認なしに成功とする。

イ：データ完全性、アプリケーション動作、認証・ネットワーク等の依存関係、復旧所要時間を確認する。

ウ：復元後はログを消去し、問題の痕跡を残さない。

エ：認証基盤や外部接続は復旧対象外として常に無視する。

答え・解説 正答：イ

ア：処理終了だけでは整合性や業務利用可否を保証できません。

イ：ファイルが読めるだけでなく、業務サービスとして機能し目標時間を満たすかを確認します。

ウ：復旧検証や監査のためログは重要です。

エ：依存サービスがなければ業務システムが使えない場合があります。

総合解説：復旧訓練は、技術的な復元と業務再開の両方を検証します。

対象：2026年度 / 基準日 2026-09-05

0115 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：標準

災害復旧用のランブック（手順書）を整備する利点として、最も適切なものはどれか。

ア：復旧作業を一人の記憶だけに依存できる。

イ：システム変更後も内容を更新しなくてよい。

ウ：緊急時に必要な担当、前提条件、実施順序、確認点、連絡先などを標準化し、属人化と手戻りを減らせる。

エ：復旧に必要な資格情報を誰でも読める形で本文へ平文記載する。

答え・解説 正答：ウ

ア：むしろ属人化を避けるために手順書を整備します。

イ：構成変更に応じて手順書も更新が必要です。

ウ：復旧時は時間制約と混乱が大きいため、実行可能な手順書が重要です。

エ：機密情報は適切な秘密管理とアクセス制御が必要です。

総合解説：ランブックは訓練で実行し、実際に使える内容か継続的に改善します。

対象：2026年度 / 基準日 2026-09-05

0116 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：標準

業務アプリケーションが認証基盤、DNS、データベースに依存している。復旧計画として最も適切なものはどれか。

ア：アプリケーションだけを最初に復元し、依存サービスは存在しないものとして扱う。

イ：復旧順序は毎回無作為に決める。

ウ：バックアップのファイル名順に復旧する。

エ：依存関係を洗い出し、必要な基盤サービスを先行又は並行して復旧できる順序と手順を設計する。

答え・解説 正答：エ

ア：依存関係を無視すると業務再開が遅れます。

イ：事前にBIAや依存関係を基に計画すべきです。

ウ：ファイル名では業務依存関係を表せません。

エ：アプリケーションだけ復元しても依存サービスが停止していれば利用できません。

総合解説：復旧順序は事業優先順位と技術依存の両方から設計します。

対象：2026年度 / 基準日 2026-09-05

0117 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：標準

ランサムウェア被害後にバックアップから復元する際の注意点として、最も適切なものはどれか。

ア：復元元と復旧先が安全か確認し、侵害要因を除去したクリーンな環境へ復元して再感染を防ぐ。

イ：原因が不明でも本番ネットワークへ直ちに全端末を再接続する。

ウ：バックアップが存在すれば、脆弱性修正や資格情報変更は不要である。

エ：復元速度を優先し、整合性確認を一切しない。

答え・解説 正答：ア

ア：感染済みバックアップや侵害された認証情報をそのまま戻すと再侵害につながるため、復旧前後の安全確認が必要です。

イ：再感染や横展開を招く可能性があります。

ウ：侵入経路が残れば再発する可能性があります。

エ：破損・感染したデータを戻す危険があります。

総合解説：復旧は「元に戻す」だけでなく、安全な状態へ戻すことが重要です。

対象：2026年度 / 基準日 2026-09-05

0118 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：標準

2台のサーバを冗長化したが、同じ電源装置と同じネットワークスイッチ1台に接続している。評価として最も適切なものはどれか。

ア：サーバが2台なら周辺機器の単一障害点は考慮不要である。

イ：サーバ自体は二重化されても、電源装置やスイッチが単一障害点となり、可用性目標を満たせない可能性がある。

ウ：同じスイッチを使うほどネットワーク障害への耐性が高くなる。

エ：冗長化はバックアップデータの機密性を自動的に高める。

答え・解説 正答：イ

ア：共通部品が落ちれば2台ともサービス不能になります。

イ：冗長化はシステム全体の障害経路を見て、共通部品の単一障害点を除く必要があります。

ウ：単一スイッチは共通障害点です。

エ：冗長化と機密性は別の管理目的です。

総合解説：冗長設計ではサーバ、電源、ネットワーク、ストレージ、拠点などの障害ドメインを確認します。

対象：2026年度 / 基準日 2026-09-05

0119 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：応用

C社の重要システムはRTO=3時間だが、これまで復旧訓練で所要時間を測っていない。最も適切な改善はどれか。

ア：文書に3時間と書いてあるので、測定せず達成済みとみなす。

イ：復旧時間が長い場合は、測定結果を削除して記録を残さない。

ウ：実際の復旧手順を訓練し、各工程の時間を測定して3時間以内に業務再開できるか確認し、超過要因を改善する。

エ：RTOを守るため復旧データの完全性確認を全て省略する。

答え・解説 正答：ウ

ア：目標値の記載だけでは実現性を証明できません。

イ：課題を隠すと改善につながりません。

ウ：RTOは目標値だけでなく、演習で実現性を測定・検証する必要があります。

エ：不正確な復旧では業務再開の目的を満たせません。

総合解説：復旧能力は訓練で測定し、ボトルネックを改善して目標とのギャップを縮めます。

対象：2026年度 / 基準日 2026-09-05

0120 事業継続・バックアップ > 災害復旧・冗長化・リストア確認 ｜ 難易度：応用

D社は別拠点へリアルタイムレプリケーションしているが、過去時点の独立バックアップはない。誤削除やランサムウェアと拠点災害の双方に備えるには、最も適切な改善はどれか。

ア：レプリケーションがあるのでバックアップは一切不要とする。

イ：両拠点を同一電源・同一通信経路だけに依存させる。

ウ：復旧手順は本番障害が起きるまで一度も試さない。

エ：別拠点レプリケーションに加え、過去時点へ戻せる独立した複数世代バックアップを保持し、切替とリストアの双方を訓練する。

答え・解説 正答：エ

ア：誤削除や暗号化が複製されると両拠点のデータを失う可能性があります。

イ：共通原因障害への耐性が低下します。

ウ：未検証手順は実際の障害時に失敗するリスクが高いです。

エ：レプリケーションは可用性に有効ですが、論理的な破壊まで同期される場合があるため、時点復旧可能なバックアップも必要です。

総合解説：DRは可用性とデータ保護を分けて設計し、複数の障害シナリオで検証します。

対象：2026年度 / 基準日 2026-09-05

0121 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：基礎

インシデント対応後に「教訓（lessons learned）」を整理する主な目的として、最も適切なものはどれか。

ア：インシデントの記録を全て削除し、再検証できなくする。

イ：発生した事実を関係者から隠すことだけを目的とする。

ウ：一度の成功事例を全てのインシデントへ無条件に適用する。

エ：対応中に判明した弱点や有効だった施策を整理し、将来の方針・手順・技術・訓練の改善へ反映する。

答え・解説 正答：エ

ア：記録は原因分析や改善、説明責任のため重要です。

イ：隠蔽は改善や適切な報告を妨げます。

ウ：状況やリスクに応じて教訓を評価する必要があります。

エ：教訓整理は個人の責任追及ではなく、組織の対応能力を改善するために行います。

総合解説：NISTは復旧計画を過去の事象から学んで継続的に改善することを重視しています。

対象：2026年度 / 基準日 2026-09-05

0122 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：基礎

再発防止を目的とする「是正処置」の本質を示す選択肢を選べ。

ア：不適合や問題の原因を除去し、同じ問題が再発する可能性を低減するための処置である。

イ：問題の記録を削除して、発生しなかったことにする。

ウ：原因に関係なく全ての利用者を処分する。

エ：復旧した時点で原因分析や改善を必ず終了する。

答え・解説 正答：ア

ア：応急処置で症状だけを消すのではなく、原因に働きかけるのが是正処置の中心です。

イ：記録削除は原因除去ではありません。

ウ：根本原因に基づかない処置は適切ではありません。

エ：復旧後も再発防止の分析・改善が必要です。

総合解説：是正処置は原因分析、具体的な対策、担当・期限、効果確認まで一連で管理します。

対象：2026年度 / 基準日 2026-09-05

0123 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：基礎

再発したフィッシング事故を分析する。利用者の操作以外に確認すべき観点はどれか。

ア：被害者の名前だけを記録し、技術的・手続的要因は調べない。

イ：利用者の操作だけでなく、メール防御、認証方式、報告手順、教育内容、権限設計など複数の要因を確認する。

ウ：「注意不足」という結論だけで分析を終了する。

エ：メールログや認証ログを確認せず、全て同じ原因と決めつける。

答え・解説 正答：イ

ア：原因の全体像を把握できません。

イ：単一の個人ミスに帰結させず、人・プロセス・技術の要因を構造的に分析します。

ウ：具体的な再発防止策につながる原因分析になりません。

エ：事実に基づく分析が必要です。

総合解説：根本原因分析では、人だけでなく制御の欠落や運用設計も確認し、再発可能性を下げる対策へつなげます。

対象：2026年度 / 基準日 2026-09-05

0124 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：標準

インシデント後レビューで改善課題が10件抽出された。これらを確実に実行へ移すために必要な管理はどれか。

ア：一覧を作るだけで責任者も期限も決めない。

イ：重大度に関係なく全項目を同じ優先度にする。

ウ：各課題に優先度、責任者、期限、実施内容を割り当て、完了状況と効果を追跡する。

エ：完了報告を受けたら効果確認をせず永久に閉じる。

答え・解説 正答：ウ

ア：実行責任が曖昧になります。

イ：リスクに応じた優先順位付けが必要です。

ウ：具体的な責任と期限がなければ、改善項目が未実施のまま残りやすくなります。

エ：実施後の有効性確認も重要です。

総合解説：改善計画は「誰が・何を・いつまでに・どう確認するか」を明確にします。

対象：2026年度 / 基準日 2026-09-05

0125 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：標準

是正処置をクローズする前に確認すべき事項はどれか。

ア：処置を実施した記録だけを残し、結果は確認しない。

イ：問題が再発しても同じ処置を無条件に続ける。

ウ：評価のためのログや測定値を全て破棄する。

エ：再発指標、監査結果、テスト、訓練などで処置が意図した効果を発揮しているか確認する。

答え・解説 正答：エ

ア：実効性が不明なままです。

イ：効果が不十分なら見直しが必要です。

ウ：効果検証の証拠を失います。

エ：実施しただけでなく、原因低減に効いたかを検証して初めて改善の実効性を評価できます。

総合解説：是正処置は、実施→有効性確認→必要に応じ追加改善まで追跡します。

対象：2026年度 / 基準日 2026-09-05

0126 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：標準

インシデントで連絡先の古さによりエスカレーションが遅れた。再発防止として最も適切なものはどれか。

ア：連絡網の更新責任と定期確認手順を定め、対応手順書を更新し、演習で連絡経路を再検証する。

イ：今回だけ口頭で新しい番号を共有し、文書は更新しない。

ウ：連絡遅延を避けるため、今後は一切報告しない。

エ：連絡先が古かった事実を削除し、レビュー対象から外す。

答え・解説 正答：ア

ア：原因に対して運用ルールと訓練の両面を改善することで再発可能性を下げます。

イ：時間が経つと再び情報が陳腐化する可能性があります。

ウ：インシデント対応を悪化させます。

エ：教訓を失い改善につながりません。

総合解説：再発防止は単発対応ではなく、制度・文書・教育・演習へ定着させることが重要です。

対象：2026年度 / 基準日 2026-09-05

0127 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：標準

攻撃メールを利用者が開く前に気付き報告したため被害は発生しなかった。この事例の扱いとして最も適切なものはどれか。

ア：被害がないので記録も分析も一切しない。

イ：被害がなくても、検知・報告が機能した点と攻撃が到達した経路を分析し、必要な改善や教育へ活用する。

ウ：報告した利用者を処分して今後の報告を抑制する。

エ：攻撃メールの送信元を信頼リストへ登録する。

答え・解説 正答：イ

ア：将来の予防に役立つ情報を失います。

イ：ニアミスも防御の有効性や弱点を学ぶ材料になります。

ウ：報告文化を損ない早期検知を弱めます。

エ：逆に攻撃を通しやすくなります。

総合解説：実被害だけでなくヒヤリハットも、予防策と検知能力の改善に活用できます。

対象：2026年度 / 基準日 2026-09-05

0128 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：標準

インシデント対応プロセスの改善効果を継続的に把握する指標として、最も適切なものはどれか。

ア：担当者の好き嫌いだけを指標にする。

イ：測定値が悪い期間だけ記録から除外する。

ウ：検知から報告・封じ込めまでの所要時間、再発件数、訓練での達成率など、目的に結び付く測定可能な指標を用いる。

エ：件数や時間を一切測らず、感覚だけで改善を判断する。

答え・解説 正答：ウ

ア：客観的な改善評価になりません。

イ：評価を歪め、課題を隠します。

ウ：改善目標に結び付く指標を継続測定することで、対策の効果やボトルネックを把握できます。

エ：改善の有効性を客観評価しにくくなります。

総合解説：指標は多ければよいのではなく、改善したい能力に対応し、継続して比較可能であることが重要です。

対象：2026年度 / 基準日 2026-09-05

0129 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：応用

同一部署で不審メール起因のアカウント侵害が2回発生した。前回は注意喚起メールだけで終了していた。今回の再発防止として最も適切なものはどれか。

ア：前回と同じ注意喚起文を送るだけで、他の対策は検討しない。

イ：被害端末を交換すれば原因分析は不要とする。

ウ：再発件数をゼロに見せるため、今回の事故を記録しない。

エ：原因分析をやり直し、MFA、メール防御、権限、教育、報告手順など必要な管理策をリスクに応じて組み合わせ、効果を確認する。

答え・解説 正答：エ

ア：既に効果が不十分だった可能性が高いです。

イ：資格情報や手順上の弱点が残る可能性があります。

ウ：正確な記録と改善を妨げます。

エ：注意喚起だけで再発した事実を踏まえ、技術・運用・人的対策を複合的に見直すべきです。

総合解説：再発した場合は、前回の是正処置の有効性も検証し、必要なら対策を追加・変更します。

対象：2026年度 / 基準日 2026-09-05

0130 再発防止・継続的改善 > 再発防止・教訓・是正処置 ｜ 難易度：応用

再発防止のため緊急に新しい監視ツールを全社導入する案が出た。継続的改善として最も適切な進め方はどれか。

ア：対策の効果だけでなく、権限、個人情報、性能、運用負荷など新たなリスクを評価し、変更管理の下で導入・検証する。

イ：緊急対策なので設定検証や権限設計を一切省略する。

ウ：効果が不明でも、導入したことだけを成功指標にする。

エ：監視ログを誰でも閲覧できるようにして運用を簡単にする。

答え・解説 正答：ア

ア：是正処置そのものが新しいリスクや障害を生む可能性があるため、変更影響を評価します。

イ：新たなセキュリティ事故や業務障害を招く可能性があります。

ウ：改善の目的達成を確認できません。

エ：ログに機微情報が含まれる可能性があり、最小権限が必要です。

総合解説：継続的改善では、改善策による副作用や新しいリスクも含めて管理します。

対象：2026年度 / 基準日 2026-09-05

0131 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：基礎

情報セキュリティ管理におけるPDCAの説明として、最も適切なものはどれか。

ア：方針・目標・計画を定め、実施し、結果を評価し、その結果に基づいて改善するサイクルを継続する。

イ：計画を一度作成したら、環境が変化しても永久に変更しない。

ウ：事故が起きた場合だけPlanを行い、平時は何もしない。

エ：Doだけを繰り返し、評価や改善を行わない。

答え・解説 正答：ア

ア：PDCAは計画→実行→評価→改善を繰り返し、管理の有効性を高める考え方です。

イ：継続的改善と相反します。

ウ：平時から計画・実施・評価・改善を回します。

エ：CheckとActが欠けています。

総合解説：PDCAは規程や管理策を固定化せず、リスクや組織環境の変化へ追随させるために用います。

対象：2026年度 / 基準日 2026-09-05

0132 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：基礎

新年度開始前、リスク評価を基にセキュリティ目標・管理策・責任を決めることになった。この場面で行う内容として適切なものはどれか。

ア：策定済み対策を実際に展開・運用する。

イ：監視結果や監査結果を評価する。

ウ：リスクや要求事項を踏まえて情報セキュリティ目標、管理策、実施計画、責任などを定める。

エ：評価で判明した不備を是正し、計画を更新する。

答え・解説 正答：ウ

ア：これは主にDoに該当します。

イ：これは主にCheckに該当します。

ウ：Planでは達成したい状態と、そのための方針・計画を具体化します。

エ：これは主にActに該当します。

総合解説：Planの品質が低いと、後続の実施・評価も目的からずれます。

対象：2026年度 / 基準日 2026-09-05

0133 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：基礎

策定済みの教育計画や技術対策を現場へ展開する段階で、実施すべき内容はどれか。

ア：管理策の有効性を監査結果で評価する。

イ：計画した管理策、教育、手順、技術対策などを実施・運用する。

ウ：リスク評価に基づいて目標を設定する。

エ：不適合原因を踏まえて制度を改定する。

答え・解説 正答：イ

ア：これはCheckの活動です。

イ：Doは計画を実行に移す段階です。

ウ：これはPlanに該当します。

エ：これはActに該当します。

総合解説：Doでは「実施した」という記録を残し、後の評価につなげることも重要です。

対象：2026年度 / 基準日 2026-09-05

0134 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：標準

対策導入から一定期間が経過した。KPIや監査結果を用いて確認すべき活動はどれか。

ア：評価を行わず、新しい対策を導入し続ける。

イ：経営目標やリスクを踏まえて計画を立てる。

ウ：発見した課題に対する是正処置を実行する。

エ：ログ・KPI・自己点検・監査などを用いて、管理策が計画どおり実施され有効かを評価する。

答え・解説 正答：エ

ア：Checkが欠け、効果や問題を把握できません。

イ：Planの活動です。

ウ：Actに該当します。

エ：Checkは客観的な証拠に基づき実施状況と有効性を確認する段階です。

総合解説：Checkでは不備の発見だけでなく、目標達成度や管理策の有効性を確認します。

対象：2026年度 / 基準日 2026-09-05

0135 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：標準

評価の結果、目標未達と手順上の不備が判明した。次の改善サイクルへつなげる行動はどれか。

ア：評価結果や事故・監査の教訓を踏まえて是正処置や改善を実施し、必要に応じて方針・手順・計画を更新する。

イ：決めた計画を実施するだけで評価結果は反映しない。

ウ：新しい脅威が出ても規程は変更しない。

エ：評価結果が悪い場合は記録を削除する。

答え・解説 正答：ア

ア：ActはCheckで得た結果を次の改善へつなげる段階です。

イ：Doだけで改善循環になりません。

ウ：変化に追随できません。

エ：改善の根拠を失います。

総合解説：Actの結果は次のPlanへつながり、継続的な改善サイクルになります。

対象：2026年度 / 基準日 2026-09-05

0136 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：標準

情報セキュリティ規程を見直す契機として、最も適切なものはどれか。

ア：制定後は一切見直さず、古い内容を守り続ける。

イ：規程の文字数を減らしたいときだけ見直す。

ウ：重大インシデント、法令・契約変更、組織再編、新技術導入、監査結果、脅威環境の変化などがあったとき。

エ：事故が起きても規程に原因がなければ記録を残さない。

答え・解説 正答：ウ

ア：陳腐化して実務や要求事項と乖離する可能性があります。

イ：見直しはリスク・要求・有効性を根拠に行います。

ウ：規程は環境変化に適合し続ける必要があり、定期レビューとイベント起点のレビューを組み合わせます。

エ：事故から得た教訓を広く評価すべきです。

総合解説：規程レビューでは、単に文言を変えるのではなく、現行リスクと業務実態に適合しているか確認します。

対象：2026年度 / 基準日 2026-09-05

0137 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：標準

情報セキュリティ規程を改定する際の管理として、最も適切なものはどれか。

ア：担当者が個人PC上で無承認に上書きし、版履歴を残さない。

イ：変更内容、承認者、施行日、版番号を管理し、対象者へ周知して旧版との混同を防ぐ。

ウ：新旧版を同じ名称で配布し、どちらが有効か示さない。

エ：改定内容を管理者だけが知り、利用者には周知しない。

答え・解説 正答：イ

ア：改定の正当性や追跡性を失います。

イ：正式な変更管理と周知により、誰がどの版に従うべきか明確にします。

ウ：現場で誤ったルールが使われるおそれがあります。

エ：実際の遵守につながりません。

総合解説：規程は統制文書として、承認・版管理・周知・教育まで一体で管理します。

対象：2026年度 / 基準日 2026-09-05

0138 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：標準

監査で多数の改善事項が見つかった。改善計画の優先順位付けとして、最も適切なものはどれか。

ア：発見順だけで優先順位を固定する。

イ：実施が簡単な項目だけを優先し、重大な課題を無期限に残す。

ウ：担当者が好む対策だけを選ぶ。

エ：リスクの大きさ、悪用可能性、対象資産の重要度、法令・契約要求、実施難易度などを総合して決める。

答え・解説 正答：エ

ア：リスクの大小を反映できません。

イ：重大リスクへの対応が遅れます。

ウ：客観的な根拠が不足します。

エ：全項目を同一扱いせず、事業リスクと要求事項に基づいて資源を配分します。

総合解説：改善計画では、優先順位・責任者・期限・必要資源・効果確認方法を具体化します。

対象：2026年度 / 基準日 2026-09-05

0139 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：応用

内部監査で「退職者アカウントの削除が遅い」と指摘された。PDCAに沿った対応として最も適切なものはどれか。

ア：原因を分析して手順・責任・期限を見直し、是正策を実施し、その後の削除状況を測定して有効性を確認する。

イ：監査報告書を削除して指摘自体を消す。

ウ：対象の1アカウントだけ削除し、原因や手順は見直さない。

エ：監査部門へ削除作業を全て移管し、業務部門の責任をなくす。

答え・解説 正答：ア

ア：指摘を受けて修正するだけでなく、原因→是正→効果確認まで回すことで再発防止につながります。

イ：問題は解消せず、説明責任も損ないます。

ウ：同じ問題が再発する可能性が残ります。

エ：役割設計を検討せず責任転嫁するだけでは適切ではありません。

総合解説：PDCAでは監査結果をCheckの入力とし、Actで是正し、次のPlan/Doへ反映します。

対象：2026年度 / 基準日 2026-09-05

0140 再発防止・継続的改善 > 規程見直し・PDCA・改善計画 ｜ 難易度：応用

E社はISMS認証取得後、3年間規程・リスク評価・訓練を変更していない。一方でクラウド利用と生成AI利用が大きく増えた。最も適切な評価はどれか。

ア：認証を一度取得すれば新技術のリスク評価は不要である。

イ：新しいサービスは全て自動的に安全なので規程変更は不要である。

ウ：認証取得時点の状態を維持するだけでは不十分で、変化した資産・脅威・利用形態を再評価し、規程・管理策・教育を更新すべきである。

エ：規程を変更すると監査対象になるので、変化があっても旧規程を固定する。

答え・解説 正答：ウ

ア：認証は継続的な適合・改善を不要にするものではありません。

イ：利用形態に応じたリスク評価が必要です。

ウ：継続的改善とは、環境やリスクの変化へ管理体系を適応させ続けることです。

エ：実態と規程の乖離がリスクになります。

総合解説：セキュリティ管理は一度完成するものではなく、事業・技術・脅威の変化に合わせて更新し続けます。

対象：2026年度 / 基準日 2026-09-05

0141 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：基礎

JVN（Japan Vulnerability Notes）の説明として、最も適切なものはどれか。

ア：企業の財務諸表だけを公開するデータベースである。

イ：日本で使用されるソフトウェア等の脆弱性関連情報と対策情報を提供する脆弱性対策情報ポータルである。

ウ：全ての脆弱性を自動修正するパッチ配布ソフトである。

エ：電子証明書を発行する認証局である。

答え・解説 正答：イ

ア：JVNは脆弱性情報のポータルです。

イ：JVNはIPAとJPCERT/CCが共同運営し、影響製品、想定影響、対策などを提供します。

ウ：情報提供が主目的で、自動修正ツールではありません。

エ：JVNは認証局ではありません。

総合解説：脆弱性情報は信頼できる一次・公的情報源から収集し、自組織の資産との関連を確認します。

対象：2026年度 / 基準日 2026-09-05

0142 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：基礎

JVN iPediaの利用目的として、最も適切なものはどれか。

ア：従業員の勤怠情報を記録するために使う。

イ：バックアップを自動的にWORM化するために使う。

ウ：インターネット接続を暗号化するVPNとして使う。

エ：国内外で公開されるソフトウェア製品の脆弱性対策情報を検索・収集し、自組織で利用する製品の対策検討に役立てる。

答え・解説 正答：エ

ア：勤怠管理サービスではありません。

イ：ストレージ機能ではありません。

ウ：VPNサービスではありません。

エ：JVN iPediaはJVNやNVD等の情報を集約する脆弱性対策情報データベースです。

総合解説：大量の脆弱性情報から自組織に関係するものを効率よく把握するため、資産台帳と組み合わせて活用します。

対象：2026年度 / 基準日 2026-09-05

0143 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：基礎

CVEとCVSSの違いについて、最も適切なものはどれか。

ア：CVEは脆弱性を一意に識別するための識別子、CVSSは脆弱性の技術的な深刻度などを評価するためのスコアリング体系である。

イ：CVEはバックアップ方式、CVSSは暗号方式である。

ウ：CVEとCVSSはどちらも製品の販売価格を示す。

エ：CVEは攻撃者の氏名、CVSSは被害企業名を示す。

答え・解説 正答：ア

ア：識別子と深刻度評価は役割が異なります。

イ：どちらもバックアップ・暗号方式の名称ではありません。

ウ：価格指標ではありません。

エ：そのような個人・企業識別情報ではありません。

総合解説：脆弱性管理ではCVE等で対象を識別し、CVSSだけでなく利用状況や悪用状況も踏まえて優先度を決めます。

対象：2026年度 / 基準日 2026-09-05

0144 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：標準

脆弱性対応の優先順位を決める際、CVSS基本値だけを見る方法の問題点として、最も適切なものはどれか。

ア：CVSSは脆弱性識別子なので深刻度を全く表さない。

イ：CVSSを使うとパッチを適用できなくなる。

ウ：自組織が影響製品を使っているか、外部公開されているか、実悪用されているか、重要資産かなどの文脈を反映できない。

エ：CVSSはバックアップ復旧時間だけを示す。

答え・解説 正答：ウ

ア：CVSSは深刻度評価の体系であり、CVEが識別子です。

イ：CVSS自体がパッチ適用を妨げるわけではありません。

ウ：技術的深刻度は重要な入力ですが、組織固有の露出・資産価値・脅威状況と組み合わせる必要があります。

エ：復旧時間の指標ではありません。

総合解説：脆弱性対応は「高スコア順」だけでなく、実際の悪用、露出、資産重要度、代替策などを加味します。

対象：2026年度 / 基準日 2026-09-05

0145 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：標準

CISAのKnown Exploited Vulnerabilities（KEV）Catalogを脆弱性管理に利用する意義として、最も適切なものはどれか。

ア：KEVに載っていない脆弱性は絶対に安全と判断できる。

イ：実環境で悪用が確認された脆弱性という情報を、対応優先度を判断する入力の一つとして利用できる。

ウ：KEVはバックアップ媒体の互換性一覧である。

エ：KEV掲載時点で自組織への侵入が確定したことを意味する。

答え・解説 正答：イ

ア：未掲載でも危険な脆弱性はあり、他の情報も評価する必要があります。

イ：KEVは実悪用の事実に着目したカタログで、優先順位付けに有用です。

ウ：脆弱性の実悪用に関するカタログです。

エ：掲載は実悪用が存在することを示しますが、自組織の侵害を直接証明するものではありません。

総合解説：「悪用実績」は技術的深刻度とは別の重要な脅威情報で、資産の該当性と組み合わせて判断します。

対象：2026年度 / 基準日 2026-09-05

0146 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：標準

重大な脆弱性情報を受け取った際の初動として、最も適切なものはどれか。

ア：製品を使っているか確認せず、全従業員のPCを廃棄する。

イ：脆弱性情報の見出しだけを見て、詳細な対象バージョンを確認しない。

ウ：自組織の資産台帳を更新せず、担当者の記憶だけで対象を探す。

エ：影響製品・バージョン・構成条件を確認し、資産台帳やスキャン結果と突合して自組織の該当資産を特定する。

答え・解説 正答：エ

ア：過剰かつ根拠のない対応です。

イ：誤った適用判断につながります。

ウ：漏れや誤認が起こりやすくなります。

エ：脆弱性情報が自組織に適用されるかを確認してから、優先度と対策を具体化します。

総合解説：情報収集だけでは不十分で、資産の該当性を迅速に判断できる管理体制が重要です。

対象：2026年度 / 基準日 2026-09-05

0147 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：標準

SNSで「特定製品に緊急脆弱性がある」という未確認情報が拡散している。担当者の対応として最も適切なものはどれか。

ア：ベンダー、JVN、IPA、JPCERT/CC、CISAなど信頼できる情報源で事実・対象・対策を確認し、必要に応じ暫定防御を検討する。

イ：SNS投稿だけを根拠に全サービスを永久停止する。

ウ：公式情報が出るまで一切の監視強化もできないと決める。

エ：投稿者のフォロワー数だけで脆弱性の真偽を判定する。

答え・解説 正答：ア

ア：速報性と正確性を両立するため、複数の信頼できる一次・公的情報源で確認します。

イ：影響と真偽を確認せず過剰対応するのは適切ではありません。

ウ：高リスクの兆候があれば暫定的な監視・防御を検討できます。

エ：信頼性の根拠として不十分です。

総合解説：脅威情報は出所、更新日時、技術的根拠、自組織への関連性を評価して利用します。

対象：2026年度 / 基準日 2026-09-05

0148 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：標準

JVNの脆弱性レポートにおける「解決策」と「回避策（ワークアラウンド）」の違いとして、最も適切なものはどれか。

ア：回避策を実施すれば、将来の正式パッチは常に不要になる。

イ：解決策はログを削除する方法、回避策は監査を中止する方法である。

ウ：解決策はパッチ適用や更新などで脆弱性自体を解消する方法で、回避策は脆弱性を残したまま悪用可能性や影響を一時的に低減する方法である。

エ：解決策と回避策は必ず同一内容である。

答え・解説 正答：ウ

ア：回避策は暫定的で、根本修正が必要な場合があります。

イ：そのような定義ではありません。

ウ：回避策は正式修正までの暫定措置として有効な場合がありますが、脆弱性そのものが消えたとは限りません。

エ：目的と効果が異なります。

総合解説：緊急時は回避策で露出を下げつつ、正式修正の適用計画を管理することがあります。

対象：2026年度 / 基準日 2026-09-05

0149 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：応用

外部から「このIPアドレスは攻撃に使われた」というIoC情報を受け取った。最も適切な扱いはどれか。

ア：一致が1件あれば、調査せず全システムが侵害済みと断定する。

イ：出所や鮮度を確認し、自組織ログとの照合、通信の文脈、誤検知可能性を評価して監視・遮断等の判断材料にする。

ウ：IoCは一度取得すれば永久に有効なので更新日時を確認しない。

エ：自組織ログとの照合はせず、情報を保存するだけにする。

答え・解説 正答：イ

ア：共有サービスや再利用IPなど誤判定の可能性があり、追加調査が必要です。

イ：IoCは有力な手掛かりですが、単独で侵害確定とは限らず、文脈と証拠を組み合わせて評価します。

ウ：脅威インフラは変化するため鮮度が重要です。

エ：情報を行動につなげるためには関連性の評価が必要です。

総合解説：脅威インテリジェンスは、信頼性・鮮度・関連性・実行可能性を評価して活用します。

対象：2026年度 / 基準日 2026-09-05

0150 再発防止・継続的改善 > 脅威情報・脆弱性情報・動向の収集と評価 ｜ 難易度：応用

F社は脆弱性情報を担当者が月末に手作業で検索しており、緊急情報の見落としが起きた。改善として最も適切なものはどれか。

ア：月末検索を維持し、緊急情報は翌月まで待つ。

イ：情報量が多いので、全ての脆弱性情報を読むことをやめる。

ウ：通知を受けたら対象製品の有無を確認せず、全システムを停止する。

エ：信頼できる情報源の通知・フィードを継続購読し、資産台帳と突合して重要度・悪用状況・露出を評価し、担当・期限を付けて対応を追跡する。

答え・解説 正答：エ

ア：高リスク脆弱性への対応が遅れる可能性があります。

イ：リスクベースのフィルタリング・優先順位付けが必要です。

ウ：資産該当性とリスクを評価して判断すべきです。

エ：情報収集を継続プロセス化し、資産との関連付けから対策完了まで管理することで見落としを減らせます。

総合解説：脆弱性管理は「情報収集→該当性確認→優先順位付け→対策→完了確認」の継続的な運用です。

対象：2026年度 / 基準日 2026-09-05