# Comptia Security+ Certification Exam (Japanese Version)

**1.** サイバーセキュリティの知識を持つ新任の取締役は、組織に影響を与えたインシデントの数を詳細に記した四半期レポートを取締役会に提出したいと考えています。システム管理者は、取締役会にデータを提示する方法を作成しています。システム管理者は次のどれを使用すべきでしょうか。

A. パケットキャプチャ

B. 脆弱性スキャン

C. メタデータ

D. ダッシュボード

**Answer(s):** D

---

**2.** 次のシナリオのうち、トークン化がプライバシー技術として最も適しているのはどれですか?

A. ソーシャルメディアのユーザーアカウントに疑似匿名化を提供する

B. 認証リクエストの2番目の要素として機能する

C. 既存の顧客がクレジットカード情報を安全に保管できるようにする

D. データをセグメント化してデータベース内の個人情報をマスキングする

**Answer(s):** C

---

**3.** ソフトウェア開発チームは、セキュリティ管理者に、ソフトウェアがリバースエンジニアリングされる可能性を減らすために使用すべき手法を推奨するよう依頼しました。セキュリティ管理者が推奨すべき手法は次のうちどれですか。

A. ソフトウェアにデジタル署名する

B. コードの難読化を実行する

C. サードパーティライブラリの使用を制限する

D. コンパイルフラグの使用

**Answer(s):** B

---

**4.** 重要なアプリケーション用の重要なパッチがリリースされたばかりで、システム管理者はパッチを必要とするすべてのシステムを特定しています。パッチを必要とするすべてのシステムが更新されるようにするには、次のどれを維持する必要がありますか?

A. 資産インベントリ

B. ネットワーク列挙

C. データ認証

D. 調達プロセス

**Answer(s):** A

---

**5.** ハッカーは、ユーザーが疑わしいリンクをクリックしたことによるフィッシング攻撃を通じてシステムにアクセスしました。このリンクによって、数週間にわたって潜伏していたランサムウェアがネットワーク全体に横展開されました。次のどれが拡散を緩和したでしょうか。

A. IPS

B. IDS

C. WAF

D. UAT

**Answer(s):** A

**6.** 年末のビジネス目標を急いで達成するため、IT 部門は新しいビジネス アプリケーションを実装するように指示されました。セキュリティ エンジニアはアプリケーションの属性を確認し、サイバーセキュリティの観点からデューデリジェンスを実行するために必要な時間が不十分であると判断しました。セキュリティ エンジニアの対応として最も適切なのは次のどれですか。

A. リスク許容度

B. リスク受容

C. リスクの重要性

D. リスク許容度

**Answer(s):** D

---

**7.** 次のトピックのうち、組織の SDLC に含まれる可能性が高いのはどれですか?

A. サービスレベル契約

B. 情報セキュリティポリシー

C. 侵入テストの方法論

D. ブランチ保護要件

**Answer(s):** D

---

**8.** セキュリティ ディレクターが企業の IT 環境内で脆弱性のパッチ適用を優先順位付けするために使用できるのは次のうちどれですか。

A. SOAR

B. CVSS

C. SIEM

D. CVE

**Answer(s):** B

---

**9.** さまざまな関係者が、セキュリティ インシデントや大規模災害などの特定の状況における仮想的な役割と責任について話し合うために会議を行っています。この会議を最もよく表すのは次のどれですか。

A. 侵入テスト

B. 業務継続計画

C. テーブルトップ演習

D. シミュレーション

**Answer(s):** C

---

**10.** 最近のセキュリティ侵害を調査しているときに、アナリストは、攻撃者が会社の Web サイトを介して SOL 感染によってアクセスしたことを発見しました。この問題の再発を防ぐために、アナリストは Web サイト開発者に次のどれを推奨する必要がありますか?

A. セキュアクッキー

B. 入力のサニタイズ

C. コード署名

D. ブロックリスト

**Answer(s):** B

---

**11.** 許容されるリスクの最大許容度を説明するのは次のどれですか?

A. リスク指標

B. リスクレベル

C. リスクスコア

D. リスク閾値

**Answer(s):** D

---

**12.** ある会社では、すべてのラップトップに資産目録ステッカーを貼り、従業員 ID と関連付けるようになりました。これらのアクションによって得られるセキュリティ上の利点は次のうちどれですか? (2 つ選択してください。)

A. ユーザーベースのファイアウォール ポリシーを適切なラップトップに正しく適用できます。

B. 従業員が組織を退職した場合でも、会社のデータを把握できます。

C. デバイス上でセキュリティ インシデントが発生した場合、適切な従業員に通知できます。

D. セキュリティ チームは、適切なデバイスにユーザー意識向上トレーニングを送信できるようになります。

E. ソフトウェア MFA トークンを構成するときに、ユーザーをデバイスにマッピングできます。

F. 侵入テストを実施する際、セキュリティ チームは目的のラップトップをターゲットにすることができます。

**Answer(s):** B,C

---

**13.** ある会社のエンドユーザーから、外部の Web サイトにアクセスできないという報告がありました。アナリストは、DNS サーバーのパフォーマンス データを調べたところ、CPU、ディスク、メモリの使用量は最小限であるものの、ネットワーク インターフェイスが受信トラフィックであふれていることを発見しました。ネットワーク ログには、このサーバーに送信された DNS クエリの数がわずかしか表示されていません。セキュリティ アナリストが見ている状況を最もよく表しているのは、次のどれですか。

A. 同時セッションの使用

B. セキュアDNS暗号化のダウングレード

C. パス上のリソース消費

D. 反射型サービス拒否

**Answer(s):** D

---

**14.** 管理者は、すべてのユーザー ワークステーションとサーバーに、拡張子 .ryk を含むファイルに関連付けられたメッセージが表示されていることに気付きました。システムに存在する感染の種類は次のどれですか。

A. ウイルス

B. トロイの木馬

C. スパイウェア

D. ランサムウェア

**Answer(s):** D

---

**15.** アーキテクトは、外部で JSON リクエストを使用してデータ転送の速度を上げたいという要求を持っています。

A. ウェブサイトホスト型ソリューション

B. クラウド共有ストレージ

C. 安全な電子メールソリューション

D. API を使用したマイクロサービス

**Answer(s):** D

---

**16.** 経営幹部チームは会社に災害復旧計画の策定を義務付けています。

A. ホットサイト

B. コールドサイト

C. フェイルオーバーサイト

D. 温かいサイト

**Answer(s):** B

---

**17.** セキュリティ マネージャーは、さまざまな種類のセキュリティ インシデントに対応するために使用する新しいドキュメントを作成しました。マネージャーが次に取るべきステップは次のどれですか。

A. 最大データ保持ポリシーを設定します。

B. ドキュメントをエアギャップネットワーク上に安全に保存します。

C. ドキュメントのデータ分類ポリシーを確認します。

D. チームで卓上演習を実施します。

**Answer(s):** D

---

**18.** 運用サーバーに影響を与えずに潜在的な攻撃者の活動を特定するために使用できるのは次のうちどれですか?

A. ハニーポット

B. ビデオ監視

C. ゼロトラスト

D. ジオフェンシング

**Answer(s):** A

---

**19.** ある会社は最近、従業員にリモートワークを許可することを決定しました。会社は VPN を使用せずにデータを保護したいと考えています。会社が実装すべきテクノロジーは次のうちどれですか?

A. セキュアウェブゲートウェイ

B. 仮想プライベートクラウドのエンドポイント

C. ディープパケットインスペクション

D. 次世代レーションファイアウォール

**Answer(s):** A

---

**20.** 最近、会社のシステムがランサムウェア攻撃を受けた後、管理者がログ ファイルを確認しました。

A. 補償

B. 探偵

C. 予防的

D. 修正

**Answer(s):** B

---