CompTIA.CAS-003J.v2021-10-19.q194

試験コード： CAS-003J
試験名称： CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-003日本語版)
認証ベンダー： CompTIA
無料問題の数： 194
バージョン： v2021-10-19
ページの閲覧量 : 580
問題集の閲覧量 : 19766
https://www.jpnshiken.com/shiken/CompTIA.CAS-003J.v2021-10-19.q194.html

質問: **1**
セキュリティエンジニアが新しいIoT製品を評価しています。この製品は、車両のODBIIポートとインターフェイスし、Bluetooth接続を使用して、データを車両内のオンボードデータロガーに中継します。データロガーは、カスタムUSBケーブルを介してのみデータを転送できます。エンジニアは、システムのセグメント間でメッセージを保護するために使用される暗号化実装に対してリレー攻撃が可能であると疑っています。エンジニアが分析を確認するために使用する必要があるツールは次のうちどれですか？
A. Wireless protocol analyzer
B. Log analysis and reduction tools
C. Binary decompiler
D. Network-based fuzzer
正解: **(**正解を表示します**)**

質問: **2**
エネルギー組織内のインフラストラクチャチームは調達プロセスの最後にいて、サービスを提供するベンダーのSaaSプラットフォームを選択しました。法的交渉の一環として、次のようないくつかの未解決のリスクがあります。
*エネルギー組織のセキュリティポリシーの内容と一致するデータ保持期間を確認する条項があります。
*データは、エネルギー組織の地理的な場所の外でホストおよび管理されます。
システムにアクセスするユーザーの数は少なく、機密データはSaaSプラットフォームでホストされません。プロジェクトのセキュリティコンサルタントが次のステップとして推奨するのは次のうちどれですか。
A. 識別されたリスクと結果を受け入れるために、エネルギー組織内のソリューション所有者を必要とします。
B. 調達プロセスを確認して、プロセスの終わりに向けたリスクの発見に関連して学んだ教訓を判断します。
C. 国内のプライバシー原則を受け入れ、保持期間を変更するようベンダーに依頼することにより、リスクを軽減します。

D. ソリューションがエネルギー組織のセキュリティポリシーを満たしていないため、セキュリティ免除を作成します。
正解: **A** (コメントを発表する)

質問: **3**
開発者は、SDLC中にピアの作業に関するフィードバックを提供する必要があります。コードの変更を確認している間、Webアプリケーションの開発者セッションIDトークンは、安全でない接続を介して送信されます。脆弱性を修正するために開発者が実装を推奨するコードスニペットは次のうちどれですか？
A）

```
Cookie cookie = new Cookie("primary");
cookie.secure(true);
```

B）

```
String input = request.getParameter ("input");
String character Pattern = "[./a-zA-Z0-9?"="&]";
If (! input. matches (character Pattern))
{
out.println ("Invalid Input");
}
```

C）

```
<webapp>
<session-con*g>
<session-timeout>15</session-timeout>
</session-con*g>
</webapp>
```

D）

```
<input type="text" maxlength="30" name="ecaSessionPW" size="40" readonly="true"
value='<%=ESAPI.encoder().encodeForHTML(request.getParameter("SessionPW"))%>'/>
```

A. オプションC
B. オプションB
C. オプションA
D. オプションD
正解: **C** (コメントを発表する)

質問: **4**
A社はB社と契約を結んでいます。
契約条件は、支払い条件、責任の制限、および知的財産権をカバーする文書で形式化されています。次のドキュメントのうち、これらの要素が含まれている可能性が最も高いのはどれですか
A. 会社A-B SLA v2.docx
B. A社−B NDA v03.docx
C. 会社A MOU v1.docx
D. A社OLA v1b.docx
E. 会社A MSA v3.docx
正解: (正解を表示します)

質問: **5**
解雇された従業員のAnnは、会社が発行したラップトップに個人の写真を残し、それらにアクセスすることはできなくなりました。アンは彼女の前のマネージャーに電子メールを送り、彼女の個人的な写真を取り戻すように頼みます。次のBESTのどれがマネージャがどのように対応すべきかを説明していますか？
A. ラップトップコンピュータがすでに消去されているかどうか、およびストレージチームが最近のバックアップを取得しているかどうかを確認して、データがまだ存在するかどうかを確認します。
B. ノートパソコンは会社のデータ専用であり、個人の写真を会社の資産に保存してはいけないことをAnnに通知します。
C. 法務部門および/または人事部門に相談し、雇用および解雇手続に関する会社の方針を確認してください。
D. 会社のラップトップからデータを流出させようとしている攻撃者からのなりすまし要求である可能性があるため、電子メールを報告してください。
正解: **(**正解を表示します**)**

質問: **6**
攻撃者は、データベースリスナーを調査することにより、企業のデータベース構造に関する情報を取得したいと考えています。
攻撃者は会社のデータベースを操作して、攻撃の実行を支援するために悪用される可能性のある脆弱性があるかどうかを確認しようとします。この種の攻撃を防ぐために、会社はデータベースを保護するために次のうちどれを行う必要がありますか？
A. データベースバナーをマスクする
B. Webおよびインターネットリソースを強化する
C. チャレンジベースの認証を実装する
D. データベース認証を強化し、テーブルアクセスを制限します
正解: **D (**コメントを発表する**)**

質問: **7**
次のうちどれが安全な環境で外部のビジネスベンダーによって提供されるメンテナンスのさまざまなレベルを定義するために使用される契約を説明しますか？
A. MOU
B. SLA
C. BIA
D. NDA
正解: **(**正解を表示します**)**

質問: **8**

情報セキュリティマネージャは、重要なネットワークデバイスの設定やトラブルシューティングに使用される接続が攻撃される可能性があることを懸念しています。マネージャは、ネットワークセキュリティエンジニアに以下の要件を満たすよう依頼しました。
* ネットワークエンジニアと重要なデバイス間のすべてのトラフィックを暗号化します。
* さまざまなネットワーキングプレーンをできるだけ分離する。
* アクセスポートが設定作業に影響を与えないようにしてください。
次のうちどれが、ネットワークセキュリティエンジニアにとって最も推奨されるものでしょうか。
A. コントロールプレーン保護を展開します。
B. AAAに証明書の使用を要求します。
C. TACACSだけを許可するように強制します。
D. 帯域外管理でSSHを使用します。
正解: (正解を表示します)

質問: **9**
銀行のセキュリティアナリストは、外部銀行のWebサイトで次のような匿名のヒントを受け取りました。
サポートされているプロトコル
TLS 1.0
SSL 3
SSL 2
Cipher suites supported
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA-ECDH p256r1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA-DH 1024bit
TLS_RSA_WITH_RC4_128_SHA
TLS_FALLBACK_SCSV non supported
POODLE
Weak PFS
OCSPステープルサポート
これらの調査結果を包括的に再現するために、アナリストは次のうちどれを使用すべきですか？
A. CAがサポートする暗号を確認し、HTTPプロキシを介した接続を検査します。
B. サーバー証明書を検査し、列挙のためのSSL / TLSハンドシェイクをシミュレートします。
C. OCSPレスポンダーを照会し、ユーザー証明書の失効情報を確認します。
D. エクスプロイトフレームワークを使用してPOODLE（SSLv3）攻撃を実行し、出力を検査します。
正解: (正解を表示します)

質問: **10**
コーポレートエグゼクティブのアンは、先進的で十分な資金を調達した手段を通じて競合他社が企業秘密を取得しようとする試みを増やす最近のターゲットになっています。アンは、旅行中に

ホテルの部屋で頻繁にラップトップを無人で物理的に安全な状態のままにします。セキュリティエンジニアは、ユーザートレーニングの必要性を最小限に抑えるAnnの実用的なソリューションを見つける必要があります。このシナリオのベストソリューションは次のうちどれですか？
A. Full disk encryption
B. An eFuse-based solution
C. Two-factor authentication
D. Biometric authentication
正解: **A** (コメントを発表する)

質問: **11**
コンサルタントは、企業とその従業員に関して収集される可能性のある情報を判断するために、企業の受動的な脆弱性評価を実施するために雇われます。コンサルタントがIT管理者の一人の名前を発見できれば、アセスメントは成功したと見なされます。次のうちどれが必要な情報を生成する可能性が最も高いですか？
A. Whois
B. 脆弱性スキャナー
C. 指紋
D. DNS列挙
正解: **A** (コメントを発表する)

質問: **12**
ユーザは、ホームネットワークを安全にすることについての勧告をセキュリティ専門家に尋ねる。ユーザーは最近、自宅を自動化するために、接続されたホームアシスタントと複数のIoTデバイスを購入しました。一部のIoTデバイスはウェアラブルであり、他のものはユーザーの自動車に取り付けられています。現在のホームネットワークは、ISP提供のルーターの背後にある単一のフラットネットワークとして構成されています。ルータには単一のIPアドレスがあり、ルータは着信トラフィックに対してNATを実行して、それを個々のデバイスにルーティングします。
次のセキュリティコントロールのうちどれがユーザーのプライバシー問題に対処し、ホームネットワークに最高レベルのセキュリティを提供しますか？
A. IoTデバイスのすべてのデフォルトパスワードを変更し、IoTデバイスとホームアシスタントのインターネットアクセスを無効にし、すべてのデバイスのルーティング可能なIPアドレスを取得し、すべてのネットワークトラフィックにIPv6およびIPSec保護を実装します。
B. ネットワークトラフィックを暗号的に分離できるファイアウォールをインストールすると、すべてのIoTデバイスにアクセスするために強力な認証が必要になり、時間帯の制限に基づいてホームアシスタントのネットワークアクセスが制限されます。
C. すべてのIoTデバイスがホームネットワークから削除されたときに機能しないように、すべてのIoTデバイスがジオフェンスモードに設定されていることを確認してください。アクティブに使用しない限り、ホームアシスタントを無効にし、ネットワークをセグメント化して各IoTデバイスに独自のセグメントを割り当てます。

D. ホームネットワークをセグメント化してユーザートラフィックとIoTデバイスからネットワークトラフィックを分離し、ホームアシスタントのセキュリティ設定で録音機能がサポートされないようにし、ルーターにファイアウォールルールをインストールしてトラフィックをホームアシスタントに制限します。可能。
正解: (正解を表示します)

質問: **13**
ペネトレーションテスターがリモートシステムにアクセスしようとしています。テスターは安全なログインページを表示でき、1つのユーザーアカウントと電子メールアドレスを知っていますが、まだパスワードを発見していません。
既知のアカウントのパスワードを取得する最も簡単な方法は次のうちどれですか？
A. Reverse engineering
B. Man-in-the-middle
C. Hash cracking
D. Social engineering
正解: (正解を表示します)

質問: **14**
最高情報セキュリティ責任者（CISO）は、組織全体のミッションクリティカルな機能のマネージャーに配布される調査を作成しました。この調査では、マネージャーは、ITが長期間停止した場合に、それぞれのユニットが稼働できる期間を決定する必要があります。組織が停止により金銭的損失を被っている調査の質問は次のうちどれに関連していますか？ （2つ選択してください）
A. 目標復旧時点
B. リカバリ時間の目標
C. リスク回避
D. ビジネスへの影響
E. リスク評価
F. 平均故障間隔
正解: (正解を表示します)

質問: **15**
CISO（最高情報セキュリティ責任者）がコンサルタントと協力して、次回の監査に先立ってギャップ評価を実施します。評価中に、組織がサードパーティのサービスプロバイダーによる規制順守を効果的に評価するための管理策を欠いていると判断された。次のうちどれがこのギャップに対処するために修正されるべきですか？
A. Privacy policy
B. Work breakdown structure
C. Audit report
D. Vendor management plan
E. Interconnection security agreement

正解: (正解を表示します)

質問: **16**
政府は、運用上のセキュリティを保護できない可能性のある技術の使用によって悪影響を受ける遠隔軍事任務に懸念を抱いています。この懸念を解消するために、次のような多くのソリューションが実装されています。
*はんだが家族と安全に通信できるようにする個人の電子メールおよびチャットセッションを含む、すべてのインバウンドおよびアウトバウンド通信のエンドツーエンド暗号化
*レイヤー7検査とTCP / UDPポート制限（TCPポート80と443および承認されたアプリケーションのみを許可するファイアウォールルールを含む）
*ミッション関連のツールとサイトのみを許可する承認済みのWebサイトとアプリケーションのホストベースのホワイトリスト
*送信元IPアドレスをスクランブルするために複数のプロキシサーバーを含めるための衛星通信の使用このシナリオで最も懸念されるのは次のうちどれですか？
A. 一般的なWebトラフィックに使用されている安全でないポート80
B. ミッションコントロールを使用したリアルタイム通信に悪影響を与える可能性のある通信遅延の影響
C. 外部の関係者と通信する際のはんだによる集中管理された軍事ネットワークとコンピューターの使用
D. はんだから電子メールで受信したジオタグ付き画像をソーシャルメディアに投稿する家族
正解: **D** (コメントを発表する)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu　**683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
電子メール管理者は、より適切なセキュリティ制御を利用して、フィッシング電子メールの数を減らす必要があります。次の構成はすでに実施されています。
*単語リストに基づくキーワードモック
* URLの書き換えと保護
*メッセージから実行可能ファイルを停止する
管理者が行うのに最適な構成変更は次のうちどれですか？
A. 受信した疑わしい電子メールごとに適切な正規表現ルールを構成します
B. 疑わしい受信メールをブロックするようにベイジアンフィルタリングを構成します
C. 疑わしいメールをブロックするためのより堅牢な単語リストを構成する

D. 添付ファイルを削除するようにメールゲートウェイを構成します
正解: (正解を表示します)

質問: **18**
ADを使用している会社は、サービスをLDAPからセキュアLDAPに移行しています。パイロットフェーズ中、サービスはLDAPを保護するために正しく接続されていません。ブロックは、トラブルシューティングセッションからの出力を除きます。



次のベストのうち、セキュアLDAPが機能しない理由を説明しているのはどれですか？ 2つ選択してください。)
A. セキュアLDAPサービスが開始されていないため、接続できません。
B. セキュアLDAPはTCPではなくUDPで実行する必要があります。
C. 会社が間違ったポートを使用しています。安全なLDAPのためにポート389を使用する必要があります。
D. Danvills.comはDDoSイネーター攻撃を受けており、OCSP要求に応答できません。
E. クライアントはデフォルトでidaptを信頼しない場合があります。
F. セキュアLDAPはワイルドカード証明書をサポートしていません。
G. クライアントはデフォルトでシカゴを信頼しない場合があります。
正解: (正解を表示します)

質問: **19**
最近のセキュリティ違反により、SQLデータベースにオンラインでアクセスできなくなりました。調査によると、SQLインジェクションの脆弱性により、データベースへの不正アクセスが可能であることが明らかになりました。将来この種の侵害を防ぐために、データベースをオンラインに戻す前に、次のセキュリティ管理策のどれを実行する必要がありますか。 2つ選んでください。)
A. セキュアストレージポリシー
B. 入力検証
C. 安全なコーディング標準
D. データベースアクティビティ監視
E. ブラウザのセキュリティ更新
F. Webアプリケーションファイアウォール
正解: (正解を表示します)

質問: **20**

BYODポリシーを採用した後、企業は管理されていないモバイルデバイスやラップトップからの新たなセキュリティの課題に直面しています。同社のIT部門では、次のような事件が多数発生しています。
* 重複したIPアドレス
* 不正なネットワーク機器
* 感染したシステムが会社のネットワークを探索している
次のうちどれが上記の問題を解決するために実装されるべきですか？　2つ選んでください。）
A. ポートセキュリティ
B. NAC
C. ヒップ
D. 経路保護
E. NIDS
正解: **(**正解を表示します**)**

質問: **21**
セキュリティアプライアンスベンダーは、一連のWebベースアプリケーションの防御のためのソリューションを要求しているRFPをレビューしています。このRFPは、パフォーマンス要件が非常に厳しい金融機関のものです。ベンダーはソリューションで対応したいと考えています。
回答する前に、ベンダーの資格に悪影響を与える可能性が最も高い要素は次のうちどれですか？
A. ベンダーが提案するソリューションは、RFPに示されているKPPを下回ります。
B. RFPは、ベンダーの自国以外に本社を置く金融機関によって発行されます。
C. このソリューションは、独自のデータモデルを使用した脅威情報共有機能を採用しています。
D. ベンダーが提案する全体的なソリューションは、RFPのTCOパラメーターよりも少ないです。
正解: **(**正解を表示します**)**

質問: **22**
法医学アナリストは、カーネルモジュールにバッファオーバーフローが存在すると疑っています。アナリストは次のコマンドを実行します。
dd if = / dev / ram = = / tmp / mem / dmp
その後、アナリストは関連する出力を確認します。
^ 34 ^＃AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA / bin / bash ^ 21 ^ 03＃45
しかし、アナリストは実行中のシェルの証拠を見つけることができません。アナリストがシェルのプロセスIDを見つけることができないのは、おそらく次のMOSTのどれですか？
A. コードは動的ライブラリを使用しています
B. NXビットが有効
C. シェルは難読化されています
D. システムはASLRを使用します
正解: **(**正解を表示します**)**

質問: **23**

組織の最高情報セキュリティ責任者 (CISO)は、企業全体でのクリアテキスト認証情報の送信に関与しています。セキュリティ評価が実施され、ポート80、389、および3268の使用が特定されました。CISOの懸念に最もよく対処するソリューションは次のうちどれですか。
A. クリアテキストを介して認証情報を送信するネットワーク間にVPNを展開します
B. HTTPSを強制します。LDAPSを有効にします。クリアテキストのグローバルカタログ通信を無効にします。
C. HTTPトラフィックをプロキシし、より安全なディレクトリサービスに移行します
D. 認証情報が含まれていると判断されたポートを無効にします
正解: **(**正解を表示します**)**

質問: **24**
セキュリティアナリストがログを確認し、従業員に発行された会社所有のコンピュータが多くのアラートを生成していることを発見し、アナリストがログイベントを確認し続け、別の不明なIPアドレスからの会社所有ではないデバイスが一般的に同じであることを発見しましたイベント。アナリストはこれらの発見をマネージャーに通知し、マネージャーはこれらの活動がすでに知られていると説明します。。。進行中のシミュレーション。このシナリオを考えると、アナリスト、従業員、およびマネージャーの役割は次のうちどれですか？
A. アナリストはレッドチームです
従業員は白人チームです
マネージャーはブルーチーム
B. アナリストはブルーチームです
従業員はレッドチームです
マネージャーは白いチームです
C. アナリストはレッドチームです
従業員はブルーチームです
マネージャーは白いチームです
D. アナリストは白人チームです
従業員はレッドチームです
マネージャーはブルーチーム
正解: **B (**コメントを発表する**)**

質問: **25**
ソフトウェア開発マネージャは、アジャイル開発方法を使用してプロジェクトを実行しています。
同社のサイバーセキュリティエンジニアは、プロジェクトの実稼働コードに悪用されている多数の脆弱性に気付いています。
問題の深刻度を減らすために、統合開発環境に加えて次の方法のうちどれを使用できますか？
A. 開発された機能ごとに侵入テストを実施する
B. 静的コードアナライザーを組み込んだ単体テストを実装する
C. 一般的なコーディングエラーに対する一連の基本的なチェックを開発する

D. ソフトウェア開発のウォーターフォール方式を採用
正解**: (**正解を表示します**)**

質問**: 26**
技術者は、ファイアウォールの自動システムから次のセキュリティ警告を受け取ります。
試合時間 :10/10/16 16:20:43
シリアル :002301028176
デバイス名 :COMPSEC1
タイプ :CORRELATION
Scrusex :domain \ samjones
Scr :10.50.50.150
Object_name :ビーコン検出
Object_id :6005
カテゴリー：危殆化したホスト
重大度：中
証拠 :ホストが動的DNSドメインに繰り返しアクセスした（17回）
アラートを確認した後、最良の分析は次のうちどれですか。
A. このアラートは、エンドポイントが感染している可能性があり、疑わしいホストに接続している可能性があることを示しています。
B. このアラートは、ユーザーが動的DNSを使用してセキュリティ対策を回避しようとしたことを示します。
C. ユーザーが無効なログインを何度も試行したため、このアラートはSIEMによって生成されました。
D. DNSは通常のネットワーク機能であるため、アラートは誤検知です。
正解**: (**正解を表示します**)**

質問**: 27**
2つの新しい技術的なSMBセキュリティ設定が実施されており、それらも安全な通信を強化するポリシーになっています。
ネットワーククライアント：通信にデジタル署名する
ネットワークサーバー：通信にデジタル署名する
時間に敏感なデータが含まれているレガシストレージアレイを持つリモートロケーションのストレージ管理者は、従業員が自分の部門の共有に接続できなくなったことを報告します。
情報セキュリティ管理者がデータの所有者に推奨する緩和策はどれですか。
A. クラウドサービスプロバイダーへの移行を提案して、遠隔地のリスクを軽減します。クラウドストレージの使用に関して、リモートロケーションに無期限のリスク例外を要求する
B. リスクを受け入れ、リモートロケーションの設定を元に戻し、レガシストレージデバイスをアップグレードできるようになるまでリモートロケーションファイルにリスク例外を設定します。
C. リスクを回避し、設定をそのままにして、従来の記憶装置を廃止する

D. リモートの場所へのリスクを許容し、従来の記憶装置はアップグレードされないため、設定を無期限に元に戻します。
正解: **(**正解を表示します**)**

質問: **28**
組織のコンプライアンスプログラムの一環として、管理者は強化チェックリストに記入し、潜在的な改善点を記録する必要があります。チェックリストの改善点を記録するプロセスは、おそらく次の要因によって推進されます。
A. 組織のソフトウェア開発ライフサイクル。
B. 継続的監視プログラムの一部としてのデータの収集。
C. インシデント対応に関連するポリシーの遵守。
D. オペレーティングシステムまたは業界の傾向の変化。
正解: **(**正解を表示します**)**

質問: **29**
会社は最近、新しいクラウドストレージソリューションを実装し、必要な同期クライアントをすべての会社のデバイスにインストールしました。数か月後、機密データの侵害が発見されました。根本原因分析は、紛失した個人のモバイルデバイスから発生したデータ侵害を示しています。
組織は、同様の侵害のリスクを減らすために、次のどのコントロールを実装できますか？
A. Cloud storage encryption
B. Hardware anti-tamper
C. Application containerization
D. Biometric authentication
正解: **(**正解を表示します**)**

質問: **30**
病院は、ローカルユーザーとリモートユーザーの両方の画像にアクセスするためにWebサーバーを必要とする新しい画像ソフトウェアを展開しています。Webサーバーでは、安全なLDAPを介したユーザー認証が可能です。情報セキュリティ責任者は、Nmapを使用して追加情報を収集することにより、サーバーがイメージングサーバーへの暗号化されていないアクセスを許可しないようにしたいと考えています。次のことを考えると。
*イメージングサーバーのIPは192.168.101.24です
*ドメインコントローラーのIPは192.168.100.1です
*クライアントマシンのIPは192.168.200.37です
これがWebサーバーで開いている唯一の投稿であることを確認するために使用する必要があるのは次のうちどれですか？
A. nmap "p 80,443,389,636 192.168.100.1
B. nmap "p 80,443 192.168.101.24
C. nmap "p" 192.168.101.24
D. nmap "p 80,389 192.168.200.37

正解: (正解を表示します)

質問: **31**
最高経営責任者（CEO）は、新しい最高情報セキュリティ責任者（CISO）に、同社のサイバーセキュリティ業務に対する機能強化のリストを提供するよう指示しました。その結果、CISOはセキュリティ運用と業界のベストプラクティスを一致させる必要性を認識しました。これを達成するために適切な次の業界参照のうちどれ？
A. OWASP
B. NIST
C. OSSM
D. PCI
正解: (正解を表示します)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu　**683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
大企業の財務部の一員であるアンは、彼女が受け取った不審な電子メールを情報セキュリティチームに送信しました。チームはアンからの電子メールを期待していなかった、そしてそれはZIP圧縮アーカイブの中にPDFファイルを含んでいる。
情報セキュリティの学びは、どのファイルが開かれたのかわからない。セキュリティチームのメンバーが空のPCを使ってZIPとPDFを開くのですが、これは悪用を仕掛けようとするソーシャルエンジニアリングの試みのようです。
次のうちどれが、この試みられた攻撃の潜在的な影響に関するより大きな洞察を提供するでしょうか？
A. 異常なトラフィックについてネットワークログを分析します。
B. エアギャップPCのプロトコルアナライザを使用します。
C. 文書に対してリバースエンジニアリングを実行します。
D. ユーザーのコンピュータに対してベースラインアナライザを実行します。
E. 金融機関のPCでウイルス対策スキャンを実行します。
正解: (正解を表示します)

質問: **33**
セキュリティアナリストは、従業員からセキュリティチームへの一連の疑わしい電子メールを調査しています。電子メールは現在のビジネスパートナーから送信されたようであり、画像やURL

は含まれていません。会社が代わりに使用するセキュリティツールによってメッセージから画像やURLが削除されることはなく、電子メールにはプレーンテキストで次のもののみが含まれています。

```
Test email sent from bp_app01 to external client_app01_mailing_list.
```

セキュリティアナリストは次のうちどれを実行する必要がありますか？

A. 境界ファイアウォールでビジネスパートナーのIPアドレスをブロックします。

B. ビジネスパートナーから発信されたすべてのメッセージを自動的に隔離するように電子メールゲートウェイを構成します。

C. ビジネスパートナのセキュリティ部門に連絡して、電子メールイベントについて警告します。

D. ゼロデイウイルスに感染した場合に備えて、影響を受ける従業員のデバイスをネットワークからプルします。

正解: **C** (コメントを発表する)

質問: **34**

最近の非常に大規模な企業合併に伴い、SOCがレビューする必要のあるログファイルの数は約3倍になりました。最高情報セキュリティ責任者（CISO）は、SOCにこれ以上スタッフを雇用することを許可されていませんが、ログレビュープロセスを自動化してSOCのノイズを減らす他の方法を探しています。SOCのログノイズを低減するのに最適なものは次のうちどれですか？

A. SIEM filtering

B. Machine learning

C. Outsourcing

D. Centralized IPS

正解: (正解を表示します)

質問: **35**

開発者は、次のコードスニペットを実装します。



コードスニペットが解決する脆弱性は次のうちどれですか？

A. セッション制限がありません

B. バッファオーバーフロー

C. 情報漏えい

D. SQLインジェクション

正解: (正解を表示します)

質問: **36**

システムモダナイゼーションプログラムの一部として、弱い暗号化アルゴリズムの使用が特定されています。ウェットサービスAPI APIを使用しているクライアントは、システムをアップグレードできず、一時的なものとして安全なアルゴリズムセットの使用をサポートします。回避策クラ

イアントはそのIPスペースを提供し、ネットワーク管理者はACLを介したAPIへのアクセスをクライアントが保持するIPスペースのみに制限します。この状況でのACLの使用例は次のうちどれですか？

A. 受け入れ
B. 評価
C. 回避
D. 転移
E. 緩和策

正解: **(**正解を表示します**)**

質問: **37**

セキュリティアセスメントの間、組織はネットワークセグメンテーションに対する不適切な管理について助言されます。査定者は、トラフィックをセグメント化するために組織がVLANに依存しているだけでは、規制基準に基づくセグメント化を提供するには不十分であると説明しています。

次のうちどれがより高いレベルのセグメンテーションを提供するためにVLANと共に実装することを検討すべきですか？

A. スパニングツリープロトコル
B. 弾性負荷分散
C. ネットワーク仮想化
D. アクセス制御リスト
E. エアギャップ

正解: **(**正解を表示します**)**

質問: **38**

次のコードスニペットを考えます。

```
SecCond = "1SS"
SecStatus = false
try {
if (SecStatus)
            SecCond = "2SS"
            console.log("ship to ship")
else
         SecCond = "normal operations"
         console.log("nothing to see here")
} catch (e) {
SecCond = "normal operations"
 console.log(e)
 console.log("Exception logged")
}
```

CompTIA

次の失敗モードのうちどれがコードが示すのでしょうか？

A. 停止
B. 開く
C. 安全

D. 例外
正解: **D** (コメントを発表する)

質問: **39**
以下のコードスニペットを考えます。

```
#include <stdio.h>
#include <stdlib.h>
int main(void) {
  char username[8];
  printf("Enter your username: ");
  gets(username)
  printf("\n";
if (username == NULL) {
  printf("you did not enter a username\n");
}
it strcmp(username, "admin") {
 printf("%s", "Admin user, enter your physical token value: ");
// rest of conditional logic here has been snipped for brevity
} else [
printf("Standard user, enter your password: ");
// rest of conditional logic here has been snipped for brevity
}
}
```

CompTIA
jpnshiken.com

次のMOSTの脆弱性タイプのうちどれに関して関係がありますか？
A. 管理者ユーザーにフォーマット文字列の脆弱性が存在しますが、標準ユーザーには存在しません。
B. 入力されたユーザーによって、コードパスが異なるハードコードされたユーザー名が異なります。

C. 短いユーザー名のみがサポートされています。これにより、資格情報が強制的に強制される可能性があります。
D. usernameパラメータのバッファオーバーフローにより、メモリ破損の脆弱性が引き起こされる可能性があります。
正解: (正解を表示します)

質問: **40**
情報セキュリティ管理者がギャップ分析を行い、その結果、リスクの高い脆弱性に対しては75%、中の脆弱性に対しては90%、低リスクの脆弱性に対しては10%のセキュリティ管理策が実施されています。確認されたギャップを埋めるためのロードマップを作成するために、保証チームは各脆弱性の悪用の可能性と、関連する各コントロールのビジネスへの影響を確認しました。どのコントロールを実装するかを決定するために、考慮すべき最も重要なものはどれですか。
A. BIA
B. KRI
C. KPI
D. GRC
正解: (正解を表示します)

質問: **41**
ある金融コンサルティング会社が最近、ルートキット経由でインストールされたマルウェアに関連するいくつかの有害な事件から回復しました。事件後分析が進行中であり、事件対応者とシステム管理者は再発のリスクを減らすための戦略を決定するために働いています。同社のシステムは最新のオペレーティングシステムを実行しており、UEFIとTPMを備えています。次のうちのどれがMOSTの予防的価値をもたらしますか？
A. パスワードの複雑さの要件を強化する
B. 測定起動を構成して使用する
C. ウイルス対策ソフトウェアと定義を更新します
D. GPOを更新して展開する
正解: (正解を表示します)

質問: **42**
最高情報セキュリティ責任者（CISO）は、次の外部のホスティングサービスに対して、マルウェア、セキュリティ保護されていないPII、およびヘルスケアデータのスキャンを要求します。
* 企業イントラネットサイト
* オンラインストレージアプリケーション
* Eメールとコラボレーションスイート
セキュリティポリシーも更新され、セキュリティチームは会社のイントラネットおよびオンラインストレージサイトからの企業データの一括ダウンロードをスキャンおよび検出できるようになりました。企業のセキュリティポリシーとCISOの要求に準拠するために必要なものはどれですか。

A. Port scanner
B. DLP agent
C. CASB
D. Application sandbox
E. SCAP scanner
正解: (正解を表示します)

質問: **43**
ある組織のネットワークエンジニアリングチームは最近、保存されているデータの機密性を確保するために新しいソフトウェア暗号化ソリューションを導入しました。これは、ストレージ内のデータ読み書き要求に300ミリ秒の待ち時間を追加し、業務に影響を及ぼします。
以下の代替アプローチのうちどれが意図したセキュリティ目標を達成しながらパフォーマンス要件に最もよく対処するでしょうか？
A. より効率的な暗号化ハッシュ関数を利用します。
B. HDDをSSDアレイに交換します。
C. マルチスレッドソフトウェアソリューションでFIFOパイプを使用します。
D. ハードウェアFDEまたはSEDソリューションを採用してください。
正解: (正解を表示します)

質問: **44**
企業のインターネット接続は通常、営業時間中に飽和状態になり、インターネットの可用性に影響を及ぼします。
会社では、すべてのインターネットトラフィックがビジネスに関連している必要があります。数時間にわたってトラフィックを分析した後、セキュリティ管理者は次のことを確認します。

Protocol	Usage	%
TCP/SSL	324Gb	85%
TCP/HTTP	37Gb	10%
UDP/DNS	10Gb	3%
Other	8GB	2%

TCP / SSLトラフィックに関連付けられたIPアドレスの大部分はCDNに解決されます。企業のセキュリティ要件を満たすために、管理者がCDNトラフィックに推奨する必要があるのは次のうちどれですか。
A. 認可されたMITMプロキシを使用してトラフィックをさらに調査します。
B. NetFlowデータを監視してCDNの使用を確認します
C. データの漏えいを防ぐためにアウトバウンドSSLトラフィックをブロックします。
D. CDNに関連付けられたパケットをドロップするIPSを実装します。
正解: (正解を表示します)

質問: **45**

最近の評価では、何人かのユーザーのモバイルデバイスが会社のセキュリティポリシーを満たさない古いバージョンのエンドポイントセキュリティソフトウェアを実行していることが判明しました。
ユーザーがネットワークにアクセスし、会社のセキュリティ要件を満たすことができるようにするために実行する必要があるのはどれですか？
A. パッチ管理
B. インシデント管理
C. 脆弱性評価
D. デバイス検疫
E. リスクアセスメント
正解: **(**正解を表示します**)**

質問: **46**
ある会社が、セキュリティエンジニアと契約して、クライアント向けWebポータルの侵入テストを実施します。次のうちどれが最も適切でしょうか。
A. ネットワーク列挙ツールを使用して、サーバーがロードバランサの背後で稼働しているかどうかを識別します。
B. ポートスキャナーでサイトをスキャンして、Webサーバー上で実行されている脆弱なサービスを特定します。
C. インターセプトプロキシを通じてWebサイトをスキャンし、コードインジェクションの対象となる領域を特定します。
D. サイトに対してプロトコルアナライザを使用して、データ入力をブラウザから再生できるかどうかを確認します。
正解: **B (**コメントを発表する**)**

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
組織は、ホストされているWebサーバーが最新バージョンのソフトウェアを実行していないことを懸念しています。次のうち、潜在的な脆弱性を特定するのに最も役立つのはどれですか？
A. nmap comptia.org -p 80 -sV
B. nslookup -port = 80 comptia.org
C. nc -1 -v comptia.org -p 80
D. hping3 -S comptia.org -p 80

正解: (正解を表示します)

質問: **48**
コードを分析した後、ある会社の2人の開発者がこれらのサンプルをセキュリティ運用マネージャーに持ち込みます。

```
Example Language: Java
# Java Web App ResourceBundle properties file
...
webapp.ldap.username=secretUsername
webapp.ldap.password=secretPassword
...
The following example shows a portion of a configuration file for an ASP.Net application.
Example Language: ASP.NET
...
<connectionStrings>
<add name="ud_DEV" connectionString="connectDB=uDB; uid=db2admin; pwd=password; dbalias=uDB;" providerName="System.Data.Odbc" />
</connectionStrings>
...
```

CompTIA jpnshiken.com

次のうちどれがこれらのコーディングの問題を最もよく解決しますか？
A. 特権アクセス管理システムを使用します
B. 管理者にパスワードを要求します。
C. PBKDF2でソルトハッシュを使用します。
D. パスワードの複雑さと長さを増やします
正解: (正解を表示します)

質問: **49**
政府機関は、いくつかのICS環境を運用および維持しています。ICS環境の1つを分類すると、中程度のベースラインが得られました。組織は、この分類に基づいて一連の適用可能なセキュリティ管理策を順守しています。
これが独自の環境であることを考えれば、他のセキュリティ管理策を検討する必要があるかどうかを判断するために、組織は次のうちどれを決定すべきですか
A. 現在のコントロールセット内の機能強化を確認します。
B. 連続監視をします。
C. 関連または必須のオーバーレイがないか確認してください。
D. ベースラインの高いコントロールセットに変更します。
正解: **D** (コメントを発表する)

質問: **50**
ソフトウェア開発会社は、ソフトウェア開発プロセスの一部として標準ライブラリの使用を検証したいと考えています。各開発者は、コードリポジトリに変更をコミットする前に単体テストを実行します。コミット後、ブランチの作成前に実行するのに最適なアクティビティは次のうちどれですか？
A. Webアプリケーションの脆弱性スキャン
B. 静的解析
C. 侵入テスト
D. ヒューリスティック分析
E. 動的解析

正解: (正解を表示します)

質問: **51**
スタッフは、不在時の時間に関連した異常な数のデバイス盗難を報告しています。会社が新しいソーシャルネットワーキングアプリを展開した後、すぐに盗難が増加しました。最高情報セキュリティ責任者（CISO）は、次のうちどれを実装することを推奨すべきですか？
A. 完全性制御
B. ジオロケーションプレゼンスプライバシー
C. NACはデバイスを隔離するためにチェックします
D. 自動位置チェックイン
正解: (正解を表示します)

質問: **52**
サイトの物理的評価を実施するためにペネトレーションテスターが契約されています。次のうちどれがこの関与の間に行われるべきソーシャルエンジニアリングの最も妥当な方法ですか？
A. ランダムに顧客の従業員に電話をかけ、問題解決のためにユーザーパスワードを要求するヘルプデスク技術者になりすます
B. コピー機のサービス技術者としてポーズをとっており、技術者にサービスコールを知らせるために機器が「電話をかけた」ことを示している
C. 会社の施設にアクセスするために偽の政府資格情報を取得し、法執行機関になりすます
D. 販売の電話を受ける場所にいる間に病気をシミュレートし、リスニングデバイスがインストールされたら回復する
正解: (正解を表示します)

質問: **53**
最高情報セキュリティ責任者（CISO）は、社内で開発され、組織のシステムを保護するために数年間使用されてきたシステム構成および強化ガイドを見直し、修正しています。CISOは、ガイドに改善を加えることができることを知っています。
次のうちどれが改訂プロセス中の最良の参照元になるでしょうか？
A. 内部セキュリティ評価報告
B. ベンダー固有の導入ガイド
C. 外部脆弱性スキャンレポート
D. CVEデータベース
E. 業界標準規格
正解: (正解を表示します)

質問: **54**
開発者は、ソーシャルメディアプラットフォームに追加するための新しい機能に取り組んでいます。新しい機能には、ユーザーが現在行っていることの写真をアップロードすることが含まれます。Data Privacy Officer（DPO）は、この新機能が原因で発生する可能性があるさまざまな種類の

悪用について懸念しています。DPOは、プラットフォームのユーザーの物理的な安全上の懸念に対処しなければ新機能をリリースできないと述べています。次のうちどれがDPOの懸念に最もよく対処できるでしょうか。
A. アップローダで利用可能なブロッキングオプションの増加
B. アップロードしたすべての写真に1時間の遅延を追加する
C. 写真をアップロードした人に公開しない
D. アップロードした写真ファイル内のすべてのメタデータを削除する
E. プラットフォーム上のすべての接続に対してTLSを強制する
正解: **(**正解を表示します**)**

質問: **55**
会社の人事部門は最近、独自のシャドーIT部門が、同じVM上で異なるラベルのデータタイプ（機密および制限付き）の混合をホストする10個のVMをスピンアップしました。次のクラウドと視覚化の考慮事項のどれがこれで提示された問題に最もよく対処しますかシナリオ？
A. 複数のデータ型をホストする単一のサーバーに関連する脆弱性を考慮する必要がありました。
B. IT部門が提供する共有ホスティングサービスに関連する脆弱性を考慮する必要がありました。
C. タイプ1とタイプ2のハイパーバイザーアプローチを検討する必要がありました
D. VM上で複数のデータ型をホストする単一のプラットフォームに関連する脆弱性を考慮する必要がありました
正解: **(**正解を表示します**)**

質問: **56**
新しい企業ポリシーでは、すべての従業員が個人のモバイルデバイス上の企業リソースにアクセスできる必要があります。情報保証マネージャーは、デバイスが紛失した場合の不注意による悪意のあるデータ開示の可能性を懸念し、ユーザーは企業の行き過ぎを懸念しています。次のコントロールのどれがこれらの懸念に対処し、会社のモバイルデバイスポリシーに反映されるべきですか？
A. 企業アプリケーションをコンテナに配置します
B. 会社のすべての通信でVPNを使用していることを確認します
C. すべてのデバイスでジオロケーションを有効にする
D. リモートワイピング機能をインストールする
正解: **A (**コメントを発表する**)**

質問: **57**
病院では、ネットワークに接続されたレガシーデスクトップを制御する機能的磁気共鳴画像（fMRI）スキャナーを使用しています。fMRIの製造元は、レガシーシステムのパッチ適用をサポートしません。レガシーデスクトップはTCPポート445でネットワークアクセス可能である必要があります。セキュリティ管理者は、レガシーシステムがエクスプロイトに対して脆弱であることを懸念しています。セキュリティを提供しながら、停止のリスクを低減するための最良の戦略は次のうちどれですか。

A. HIDSをインストールし、未使用のサービスを無効にします。
B. 既知の脆弱性に対する重要なセキュリティパッチのみを適用します。
C. アプリケーションのホワイトリストを有効にし、SMBを無効にします。
D. ネットワークをセグメント化し、制御されたインターフェースを構成する
正解: **D** (コメントを発表する)

質問: **58**
ある会社は、すべてのIT資産を管理し、IT活動のインシデントおよび問題管理ソリューションを提供するために使用されるアプリケーションを購入しています。会社は検索を2つの製品に絞り込みます。
アプリケーションAおよびアプリケーションB;すべての要件を満たしています。アプリケーションAは最も費用効果の高い製品ですが、最もリスクが高いため、会社はアプリケーションBを購入します。
リスク選好を決定する際に会社が使用した戦略のタイプは次のうちどれですか？
A. 緩和策
B. 転送
C. 受け入れ
D. 回避
正解: **C** (コメントを発表する)

質問: **59**
最近の停止に続いて、システム管理者はサーバーハードドライブの適切なベンチストックを決定するための調査を実施しています。次の指標のうち、手元に保持するハードドライブの数を決定するうえで管理者にとって最も価値のあるものはどれですか。
A. ALE
B. SLE
C. PRO
D. MTBF
E. TTR
正解: (正解を表示します)

質問: **60**
ベンダーがHTTPSおよびSSHのみを使用して新しい内部サーバーにアクセスし、ポータルのバックエンドシステムを管理するという要求が承認されました。内部ユーザーには、すべての内部WebサーバーへのHTTPおよびHTTPSアクセスが必要です。新しいサーバーとそのサブネットへの他のすべての外部アクセスは許可されていません。セキュリティマネージャは、適切なアクセスが設定されていることを確認する必要があります。

New internal server IP:	10.1.50.150
Vendor IP:	208.206.109.249
External development subnet:	108.109.110.0/28
Internal subnet:	10.1.10.0/24
Web team subnet:	10.1.40.0/24
Web server subnet:	10.1.50.0/24

以下は、そのサーバーに関連するファイアウォールのスニペットです（トップダウンモデルでアクセスが提供されます）。

Line #	Source address	Destination address	Port	Access type
1	10.1.40.0/24	10.1.50.0/24	Any	Permit
2	10.1.10.0/24	10.1.50.0/24	80	Permit
3	Any	10.1.50.0/24	Any	Deny
4	208.206.109.249	10.1.50.150	80, 22	Permit
5	10.1.40.0/24	108.109.110.0/28	80, 8080	Permit

適切なアクセスを許可するには、次のどの行を構成する必要がありますか？（2つ選択してください。）

A. Add port 22 to line 5.
B. Add port 443 to line 2.
C. Move line 3 below line 4 and add port 443 to line.
D. Add port 22 to line 2.
E. Move line 4 below line 5 and add port 80 to 8080 on line 2.
F. Add port 443 to line 5.
G. Move line 3 below line 4 and change port 80 to 443 on line 4.
正解: **(**正解を表示します**)**

質問: **61**
インフラチームは調達プロセスの最後にあり、ベンダーを選択しました。
最終交渉の一環として、以下を含む多くの未解決の問題があります。
1.補償条項が最大責任を特定しています
2.データは会社の地理的な場所以外でホストおよび管理されます。システムにアクセスするユーザー数は少なくなり、機密データはソリューションにホストされません。プロジェクトのセキュリティコンサルタントとして、プロジェクトのセキュリティコンサルタントは次のうちどれをNEXTステップとして推奨すべきですか？
A. セキュリティポリシーを満たしていないため、セキュリティ免除を作成してください
B. ソリューションの所有者に、特定されたリスクと影響を受け入れるように要求する
C. 調達プロセス全体を見直して、得られた教訓を判断する
D. ベンダーに国内のプライバシー原則を受け入れるように依頼することでリスクを軽減する
正解: **B (**コメントを発表する**)**

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
セキュリティアナリストは、組織に適用可能な外部のITセキュリティ問題のリストを作成するよう依頼されました。その目的は、さまざまな種類の外部アクター、それらの攻撃方法、およびビジネスに影響を与える可能性のある脆弱性の種類を示すことです。次に、最高情報セキュリティ責任者（CISO）が、このリストを取締役会に提示して、カバー範囲が不十分な分野の統制に対する資金提供を依頼します。
アナリストは次のどの運動タイプを実行すべきですか？
A. 外部からの脆弱性スキャンと侵入テストを実施する。
B. 脅威モデリングの演習を実施する。
C. 最近開示された脆弱性を要約してください。
D. 業界のベストプラクティスと最新のRFCを研究する。
正解: (正解を表示します)

質問: **63**
ソフトウェア開発会社は、ソフトウェアの問題が多数発生したため、最近顧客を失いました。これらの問題は、バッファオーバーフロー、ポインタ遅延などを含む整合性と可用性の欠陥に関連していました。コードの品質を改善するために、会社は次のうちどれを実装すべきですか？（2つ選択）。
A. コードのコメントとドキュメント
B. 継続的インテグレーション
C. 静的分析ツール
D. アプリケーションのコンテナ化
E. コードの難読化
F. 開発環境のアクセス制御
正解: (正解を表示します)

質問: **64**
侵害は、顧客のPIIが侵害されたインサイダーの脅威によって引き起こされました。侵害に続いて、主任セキュリティアナリストは、攻撃者が会社のリソースにアクセスするために使用した脆弱性を特定するように求められます。アナリストが脆弱性を修正するために使用する必要があるのは次のどれですか？
A. データ漏洩防止

B. 行動分析
C. プロトコルアナライザー
D. 根本原因分析
正解: **A** (コメントを発表する)

質問: **65**
ネットワーク管理者は、インターネット上のホストから時折攻撃される特定のサーバーを心配しています。サーバーは重要ではありません。ただし、攻撃はネットワークの残りの部分に影響を与えます。会社の現在のISPは費用対効果に優れていますが、ISPは報告された問題への対応が遅いです。管理者は、ISPとトラブルチケットを開くことなく、攻撃の影響をすぐに軽減できる必要があります。ISPは、特定のBGPコミュニティストリングでアドバタイズされた非常に小さなネットワークルートを受け入れます。管理者がこれらの攻撃の影響を緩和するBESRTの方法は次のうちどれですか？
A. ISPが提供するルート保護を使用して、インターネット上の信頼できるホストからのBGPルートのみを受け入れます。これにより、攻撃ホストからのトラフィックが破棄されます。
B. / 32ルートをISPにアドバタイズして、リモートトリガーのブラックホールを開始します。これにより、アップストリームプロバイダーの問題のあるサーバー宛てのトラフィックが破棄されます。
C. 2番目のローカルISPに冗長接続を追加して、1つの接続でサーバーが攻撃されている場合に冗長接続を使用できるようにします。
D. ISPと連携し、攻撃ホストの攻撃パターンを認識できるIPSフィルターをサブスクライブし、ローカルIPSデバイスでそれらのホストをブロックします。
正解: (正解を表示します)

質問: **66**
ある会社のチーフサイバーセキュリティアーキテクトが、内部の給与計算Webサイトにアクセスするために相互認証を構成したいと考えています。アーキテクトは、MITM攻撃に対する最良の防御策となる構成を決定するように管理チームに依頼しました。次の実装方法のうちどれが建築家の目標を最もよくサポートするでしょうか。
A. TLSを実装し、ハンドシェイク中にクライアントに独自の証明書の使用を要求します。
B. Webアプリケーションプロキシを設定し、HTTPSトランザクションの監視を開始します。
C. TLSセッションを復号化するように設定されている企業のDMZにリバースプロキシをインストールする。
D. ユーザー名/パスワード入力時に必要な入力としてチャレンジ/レスポンスプロンプトを利用します。
正解: (正解を表示します)

質問: **67**
組織は、脅威を通常のトラフィックやシステムへのアクセスと区別するのに苦労しています。セキュリティエンジニアは、データを集約し、環境全体で悪意のある攻撃者やその他の異常なアク

ティビティを特定するのに役立つメトリックを提供するシステムを推奨するように求められています。エンジニアが推奨するソリューションは次のうちどれですか？
A. IPS
B. UTM
C. Webアプリケーションファイアウォール
D. ファイル整合性モニター
E. SIEM
正解: **(**正解を表示します**)**

質問: **68**
SaaSベースの電子メールサービスプロバイダは、正当な顧客からIPネットブロックがブラックリストに載っていて電子メールを送信できないという報告を受け取ることがよくあります。SaaSは、影響を受ける顧客が通常より広いネットワーク範囲内のIPアドレスを持っており、同じIP範囲内の悪用された顧客の中にはスパムキャンペーンを実施した可能性があることを確認しています。
正当な顧客への影響を最小限に抑えるために、SaaSプロバイダーは次のどのアクションを実行するべきですか？
A. サービスプロバイダがサードパーティのブラックリストエントリを管理できないことを顧客に知らせます。顧客はブラックリストオペレータに直接手を差し伸べるべきです
B. ブラックリスト演算子との関係を確立して、幅広いエントリをより詳細なエントリに置き換え、誤ったエントリをすばやく整理できるようにします。
C. 電子メールブラックリストにエントリがあるすべての顧客アカウントの削除を実行します。これは敵対的な行動を強く示すものです。
D. 正当なトラフィックに影響を与えているため、ネットブロックが削除されていない場合、法務部門と協力してブラックリストオペレータに対する法的措置を脅かす
正解: **(**正解を表示します**)**

質問: **69**
システムエンジニアは、Webアプリケーションの脆弱性スキャンからの出力を確認しています。エンジニアは、データが信頼できないソースからアプリケーションに入力されており、クエリを動的に作成するために使用されていると判断しました。
次のコードスニペットのうち、SQLインジェクション攻撃からアプリケーションを最もよく保護するのはどれですか？
A）

```
String input = request.getParameter ("SeqNo");
String characterPattern = "[0-9a-zA-Z]";
If (! input. matches (characterPattern))
{
out.println ("Invalid Input");
}
```

B）

```
<input type="text" maxlength="30" name="ecsChangeFwdForm" size="40" readonly="true"
value='<%=ESAPI.encoder().encodeForHTML(request.getParameter("userName"))%>'/>
```

C）

```
catch (Exception e)
{
if(log.isDebugEnabled()) log.debug (context, EVENTS.ADHOC,
"Caught InvalidGSMException Exception --"
+ e.toString() );
}
```

D)

```
<asp:TextBox TabIndex="6" runat="server" Width="206px" MaxLength="11" TextMode="Password"></asp:TextBox>
```

A. オプションD
B. オプションC
C. オプションA
D. オプションB
正解: **(**正解を表示します**)**

質問: **70**
会社の請求処理部門には、個人の電子メールアドレスから多数の電子メール送信を受信するモバイルワーカーがいます。従業員は最近、請求フォームを承認する電子メールを受信しましたが、開いたときに従業員のラップトップに悪意のあるソフトウェアをインストールしました。
A. 電子メールにアクセスする前にすべてのラップトップがVPNに接続する必要がありました。
B. サンドボックス機能を使用してクラウドベースのコンテンツフィルタリングを実装します。
C. アプリケーションのホワイトリストを突き刺し、請求処理部門のラップトップのホワイトリストに電子メールクライアントのみを追加します。
D. メールゲートウェイをインストールして、受信メッセージをスキャンし、メールボックスに到達する前に添付ファイルを削除します。
正解: **(**正解を表示します**)**

質問: **71**
最近の事件で、機密データが開示され、その後、適切に保護されたクラウドベースのストレージプラットフォームを通じて破壊されました。インシデント対応の技術者は、経営陣と協力して、インシデントに関する重要なメトリックを伝えるアクション後のレポートを作成しています。
違反の影響を判断する上で、上級管理職にとって最も重要なのは次のうちどれですか？
A. 違反により存在する法的または規制上のエクスポージャー
B. 組織への侵害の可能性のあるレコードごとのコスト
C. 侵害されたレコードの数
D. データの復元に必要なダウンタイムの量
正解: **(**正解を表示します**)**

質問: **72**
組織はエンドポイントセキュリティソリューションを検討しています。製品を評価する場合、組織には次の要件があります。
*サーバー、ラップトップ、デスクトップのインフラストラクチャをサポート
*セキュリティリソースが限られているため、アクティブな保護機能を実装する

*セルフサービスで情報を分類し、ポリシーを適用する機能をユーザーに提供する
*保存データと使用データを保護
上記の要件を最もよく満たすエンドポイント機能は次のうちどれですか。 2つ選択してください。）
A. 権利管理
B. アプリケーションのホワイトリスト
C. エンドポイントの検出と応答
D. アンチウイルス
E. データ損失防止
F. ログ監視
正解: **(**正解を表示します**)**

質問: **73**
セキュリティ評価の後、最高情報セキュリティ責任者（CISO）が評価の結果を検討し、潜在的なリスク対策戦略を評価しています。CISOの評価の一環として、識別されたリスクに基づいて潜在的な影響の判断が行われます。対応行動に優先順位を付けるために、CISOは過去の経験を用いてばく露因子ならびに識別された脆弱性の外部からのアクセス可能性を考慮に入れる。
次のうちどれがCISOを実行していますか？
A. 定量的リスク評価
B. 学んだ教訓の文書化
C. ビジネスインパクトスコア
D. リスクの定性的評価
E. 脅威のモデル化
正解: **(**正解を表示します**)**

質問: **74**
セキュリティアナリストは、エンタープライズ資格情報管理ソフトウェアの実装に関して次の要件を受け取りました。
*ソフトウェアには個人までのトレーサビリティが必要です
*資格情報は常にベンダーに知られていない必要があります
* IDチェックアウト時に資格情報の変更を強制する必要があります
*複雑さの要件を実施する必要があります。
*ソフトウェアは、最大の可用性を備えた迅速かつ簡単にスケーラブルである必要があります。次のベンダー構成のうち、これらの要件を最もよく満たすのはどれですか。
A. 転送中に暗号化され、毎週取得されるバックアップとともに内部ネットワークサーバーに保存された資格情報
B. 転送中に暗号化され、ベンダーのクラウドに保存された資格情報。企業はキーを保持します。
C. 送信中に暗号化され、ベンダーのクラウドに保存、ハッシュ、ソルトされた資格情報。ベンダーがキー管理を処理します。
D. 各ローカルマシンに保存、ハッシュ、およびソルトされた資格情報

正解: (正解を表示します)

質問: **75**
ビデオゲーム開発者は、不正行為をしているプレーヤーの報告を受けています。すべてのゲームプレーヤーには、それぞれ1～10ポイントのスケールでランク付けされた5つの機能があり、合計10ポイントをバランスに使用できます。プレイヤーはいつでもこれらのポイントを機能間で移動できます。プログラミングロジックは次のとおりです。
*プレイヤーがポイントをある機能から別の機能に移動するように要求する
*ソース機能には、移動を可能にするのに十分なポイントが必要です
*移動後の移動先の能力は10を超えてはなりません
*ソース機能から宛先機能への移動が完了します。ゲームログのタイムスタンプは、転送プロセスの各ステップに約900ミリ秒かかることを示しています。ただし、不正行為をしているプレーヤーのタイムスタンプは、まったく同時に機能の転送を示しています。不正行為をしているプレイヤーは、複数の機能で10ポイントを獲得します。これらの機能の転送を許可するために悪用される可能性が最も高いのは、次のうちどれですか？
A. Memory leak
B. CSRF
C. Integer overflow
D. SQL injection
E. TOC/TOU
F. XSS
正解: (正解を表示します)

質問: **76**
組織は、従業員が自分のスマートフォンで企業のメールを受信できるようにしたいと考えています。セキュリティアナリストは、従業員のスマートフォンのファイルシステムに含まれる次の情報を確認しています。
FamilyPix.jpg
Taxreturn.tax
paystub.pdf
employeesinfo.xls
SoccerSchedule.doc
RecruitmentPlan.xls
Based on the above findings, which of the following should the organization implement to prevent further exposure? (Select two).
A. Side loading
B. Jailbreaking
C. Containerization
D. Rooting
E. Geofencing

F. Remote wiping
G. VPN
正解: **(**正解を表示します**)**

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
従業員が休暇中に、その従業員がネットワーク上で悪意のある活動に関与した疑いが生じます。セキュリティエンジニアは、従業員が職場に戻った後も調査を継続する必要があるかもしれないと懸念しています。この懸念を踏まえて、セキュリティエンジニアは、調査の整合性を維持するために次のうちどれを推奨する必要がありますか？
A. 従業員のネットワークドライブのイメージファイルを作成し、ハッシュとともに保存します
B. キーロガーをインストールして、従業員のコミュニケーションと連絡先をキャプチャします
C. 従業員に関連するすべてのドキュメントとコミュニケーションのアーカイブコピーを作成します
D. ネットワークインフラストラクチャデバイスのフォレンジックイメージを作成する
正解: **B (**コメントを発表する**)**

質問: **78**
セキュリティエンジニアが開発チームに組み込まれ、開発中の製品にセキュリティが組み込まれていることを確認します。セキュリティエンジニアは、開発者が特定のスケジュールポイントで適用される多数のセキュリティ要件によって妨げられないようにしたいと考えています。
次の解決策のどれがエンジニアの目標を達成しますか？
A. コードの品質を強化し、ウォーターフォール開発プロセスの要件定義フェーズに標準を再利用します。
B. 各開発チームリーダーのワークステーションにインストールされる一連の自動セキュリティテストを開発して実装する。
C. 開発チーム全体で毎週の単体テスト結果のレビューをスケジュールし、会議の合間にサプライズコードの検査でフォローアップします。
D. 開発者によってコミットされたコードの各部分を構築およびテストし、フィードバックを提供する統合ソフトウェアツールを展開します。
正解: **A (**コメントを発表する**)**

質問: **79**

組織の最高財務責任者（CFO）は、IT部門がCFOのアカウントをドメイン管理者グループに追加することを望んでいます。IT部門は、これは危険であると考えており、続行する前にセキュリティマネージャーからのサポートを求めています。次のBESTのうち、CFOにドメイン管理者アクセスを提供することに反対する議論を支持するのはどれですか？
A. 強制アクセス制御
B. 随意アクセス制御
C. データ分類
D. 職務の分離
正解: **(**正解を表示します**)**

質問: **80**
悪意のあるユーザーが同じハードウェアクラスター内で実行されている他の仮想マシンのルート権限を取得できる脆弱性が最近発表されました。次のクラウドベースのソリューションのどれがこの脆弱性について最も懸念されるべきですか？
A. Multitenant SaaS cloud
B. Single-tenant private cloud
C. Multitenant IaaS cloud
D. Single-tenant public cloud
E. Multitenant PaaS cloud
F. Single-tenant hybrid cloud
正解: **(**正解を表示します**)**

質問: **81**
セキュリティアナリストが、ルーキーがインストールされていることが判明したエンドポイントを確認しています。ルートキットは、エンドポイントのクリーンアップの複数回の試行、およびOSの再インストールの試行に耐えました。セキュリティアナリストは、他のエンドポイントで同様の問題が発生しないようにする方法を実装する必要があります。次のうちどれがこの目的を最もよく達成しますか？
A. マザーボードのTPMチップをリセットします。
B. 測定されたブート認証を利用します。
C. カスタムのマルウェア対策ルールを構成します。
D. 正常なメディアを使用してOSを再インストールします。
E. セキュアブートプロセスを実施します。
正解: **(**正解を表示します**)**

質問: **82**
病院で使用されている従来のWebアプリケーションは、12か月間アップグレードできません。新しい脆弱性がレガシーアプリケーションに発見され、ネットワーキングチームは緩和を任されています。

緩和のためのミドルウェアは、年間10万ドルの費用がかかります。次のうちどれがROIを決定するために計算されなければなりませんか？ （2つ選んでください。）
A. ARO
B. MTBF
C. ALE
D. RPO
E. RTO
正解: **(**正解を表示します**)**

質問: **83**
セキュリティ管理者は、BYOD環境で会社の電子メールとファイルへのアクセスを保護するためにMDMソリューションを実装したいと考えています。ソリューションは、次の要件をサポートする必要があります。
*会社の管理者は従業員の個人情報にアクセスできないようにする必要があります。
*ルート化されたデバイスまたはジェイルブレイクされたデバイスは、会社の機密情報にアクセスできないようにする必要があります。
次のベストのうち、関連するリスクに対処するのはどれですか？
A. コード署名
B. VPN
C. FDE
D. コンテナ化
正解: **A (**コメントを発表する**)**

質問: **84**
ベンダーは、グローバルな顧客向けにモバイルアプリケーションを開発します。モバイルアプリケーションは、ソース（モバイルデバイス）と宛先（組織のERPシステム）間のデータの高度な暗号化をサポートします。
ベンダーのコンプライアンスプログラムの一環として、次のうちどれを考慮することが重要ですか？
A. コントロールのエクスポート
B. モバイルトークン化
C. デバイスのコンテナ化
D. プライバシーポリシー
正解: **(**正解を表示します**)**

質問: **85**
製造会社は最近、ICSデバイスに対する攻撃から回復しました。その後、影響を受けるコンポーネントを分離することで攻撃対象を減らしました。同社は現在、検出機能の実装を望んでいます。機械学習に基づいたシステムを検討しています。次の機能のうち、主流の商用IDSにこのような新生技術を採用するドライバーを最もよく説明しているのはどれですか？

A. 論理プロトコルとメッセージング形式に基づいてトラフィックを分類する
B. 既知の不正な署名と動作を特定してトリガーする
C. 観察された動作に基づいてICSデバイスを自動的に再構成する
D. 通常の行動を訓練し、それからの逸脱を特定する
正解: **(**正解を表示します**)**

質問: **86**
サイバーセキュリティアナリストは、セキュリティを企業の姿勢で確認するために雇われています。サイバーセキュリティアナリストは、少数のIPアドレスからのSYNフラッドが原因で、非常に高いネットワーク帯域幅の消費に気付いています。次のうちどれがインシデント対応をサポートするために取るべき最良の行動でしょうか？
A. すべてのSYNパケットをブロックします。
B. ルーターに入力フィルタを適用します。
C. パケットキャプチャツールをインストールします。
D. 会社の帯域幅を広げます。
正解: **B (**コメントを発表する**)**

質問: **87**
ある会社が悪意のあるペイロードを含むと疑われるツールの分析を実行したいと考えています。法医学アナリストには次のスニペットが与えられます。
^ 32 ^ [34fda19 fd ^ 43gfd / home / user / lib / module.so.343jk ^ rfw 342fds43g
アナリストは次のうちどれを使用して悪質なペイロードの場所を特定しましたか？
A. ファズテスト
B. バイナリリバースエンジニアリング
C. コードデデュプリケータ
D. セキュリティコンテナ
正解: **(**正解を表示します**)**

質問: **88**
急成長している会社の最高経営責任者（CEO）は、もはやすべての従業員を知っているわけではなく、従業員によって会社の知的財産が盗まれるのではないかと心配しています。従業員は柔軟な時間帯でリモートで作業できるため、予測できないスケジュールが作成されます。会社全体で頻繁にシフトするニーズがあるため、役割の定義は不十分です。情報セキュリティチームによる次の新しいイニシアチブのうち、会社を最も安全に保護し、CEOの懸念を軽減するのはどれですか。
A. 従業員向けにシミュレートされたフィッシングキャンペーンを開始し、追加のセキュリティ意識向上トレーニングをフォローアップします。
B. 偽のパスワードを含むテキストドキュメントを含む会社のファイル共有とサーバーをシードし、その使用を監視します。
C. DLPを実装して、従業員アカウントと外部の関係者およびサービスの間のデータ転送を監視します

D. ユーザー行動監視ツールからのデータを報告し、セキュリティアナリストを割り当てて毎日それを確認します
正解: **C** (コメントを発表する)

質問: **89**
次の部門のうち、コンサルティング会社のエンジニアは、機密のある独自の顧客情報を保管するための管理要件と報告要件を決定する際に調整する必要がある部門はどれですか。
A. 財務
B. 弁護士
C. 販売
D. 人事
正解: (正解を表示します)

質問: **90**
企業のIT部門は現在、従来のパッチ適用を実行しており、サーバーの寿命は5年を超える可能性があります。セキュリティアーキテクトは、サーバーにパッチを適用するのではなく、サーバーを交換する免疫サーバーアーキテクチャに向けて会社を動かしています。開発、テスト、および本番用の静的サーバーを用意する代わりに、サーバーは環境間を動的に移動します。
このタイプのアーキテクチャに移行するために必要なものは次のうちどれですか？ (2つ選択してください。)
A. 自動展開
B. ネットワークセグメンテーション
C. Netflow
D. ロードバランサー
E. フォワードプロキシ
正解: (正解を表示します)

質問: **91**
スプリント中、開発者は、セキュリティの影響について変更の予想結果を徹底的に評価する責任があります。影響がある場合は、チームリーダーに報告する必要があります。ソースコードを変更する前に、チームリーダーに必要な情報を提供するために、次のうちどれを実行する必要がありますか？
A. リスク評価
B. ビジネス影響評価
C. 回帰テスト
D. データの抽象化
E. ユーザーストーリー開発
正解: (正解を表示します)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**

技術者は予算の制約のために古いSSLサーバーを使用し、PFSを有効にした後にパフォーマンスが劇的に低下していることを発見しました。技術者はパフォーマンスがそれほど劇的に低下した理由を特定できません。新しいバージョンのSSLサーバーは同じパフォーマンス低下を被りません。技術者にとって、セキュリティではなくパフォーマンスが最優先事項です。各システムのシステム仕様と構成を以下に示します。

	Old server	New server
Decryption chips	8	10
System RAM	16GB	8GB
Disk size	1TB	6TB
Algorithm	RSA	ECC
Connections	500	450

次のうちどれがパフォーマンスの低下の原因である可能性が最も高く、変更する必要がありますか？

A. メモリサイズ
B. RSAの使用
C. 復号化チップ
D. 接続要求
E. ECCの使用
F. ディスクサイズ

正解: (正解を表示します)

質問: **93**

研究者は、ランサムウェア攻撃で一般的に使用されている既存のマルウェアの新しい亜種と思われるものを特定するために取り組んでいますが、以前に評価されたマルウェアと同一ではありません。言語、ペイロードなど、多くの類似点があります。およびアルゴリズム。研究者が2つのバリアントのコードベースを安全に比較するのに役立つのは次のうちどれですか？

A. ソフトウェア定義ネットワーク
B. 脆弱性スキャナー
C. 仮想化されたサンドボックス
D. HTTPインターセプター

正解: (正解を表示します)

質問: **94**
次のシステムのうち、完璧な...機密性に関連するオープンな脆弱性があると判明した場合、最も危険にさらされるシステムはどれですか。
A. 仮想ホスト
B. VPNコンセントレーター
C. エンドポイント
D. SIEM
E. レイヤー2スイッチ
正解: **B (**コメントを発表する**)**

質問: **95**
薬局はその顧客に彼らの記録へのオンラインアクセスと請求書を見直して支払いをする能力を与えます。特別なプラットフォームに新たなSSLの脆弱性が発見され、攻撃者がこれらのサービスを提供するエンドユーザーとWebサーバー間のデータを取得する可能性があります。新しい脆弱性への投資後、提供するWebサービスはこの新しい脅威の影響を受けていると判断されました。次のデータタイプのうち、この新しい脅威に基づいて最も危険にさらされる可能性があるのはどれですか。 2つ選択）
A. 個人の健康情報
B. 知的財産
C. 従業員レコード
D. カード会員データ
E. 企業財務データ
正解: **(**正解を表示します**)**

質問: **96**
小さな会社の新しく作成されたWebサイトには、いくつかの設計上の欠陥があります。開発者は、さまざまなデジタル証明書を使用し、認証局を信頼するために、ActiveXスクリプトと完全に互換性のあるWebサイトを作成しました。
ただし、脆弱性テストでは、サンドボックスが有効になっていることが示されているため、ユーザーのコンピューター内のリソースへのコードのアクセスが制限されています。エラーの原因として最も可能性が高いのは次のうちどれですか？」
A. 開発者はファジーロジックを使用して、ポート80と443の両方が開いたときにWebブラウザーがどのように応答するかを決定しました
B. 開発者は、モバイルコードがネットワークを介して送信されることを考慮していませんでした。
C. 開発者は、信頼できない認証局で企業アカウントを確立しました。
D. 開発者が誤ってJavaアプレットを使用しました。
正解: **(**正解を表示します**)**

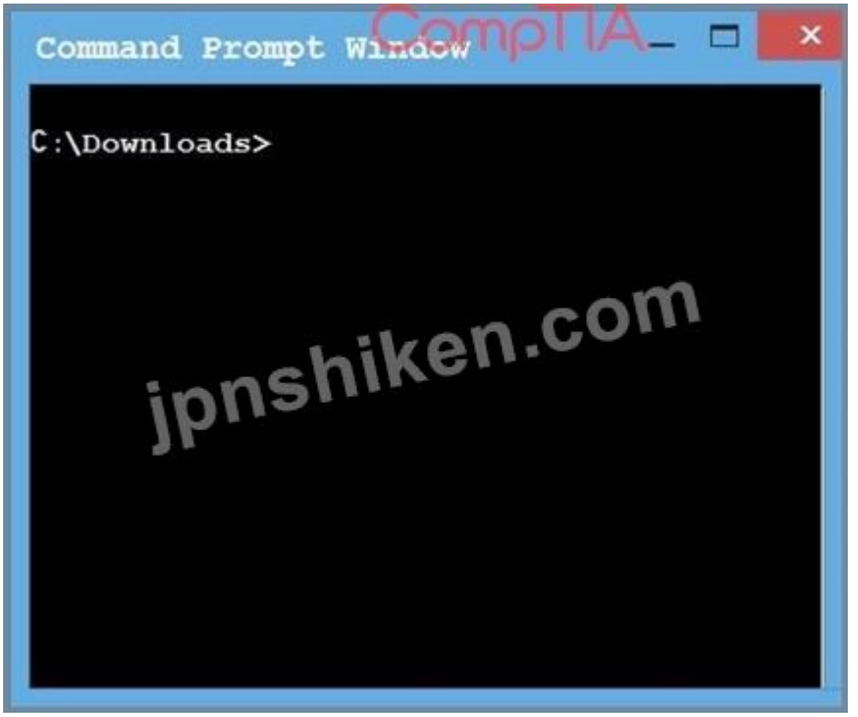
質問: **97**
セキュリティエンジニアは、個々のエンドポイントの固有の設定、および共通デバイスの共有設定ポリシーに適用されるため、会社のセキュリティポリシーへの準拠を評価する方法を確立する必要があります。

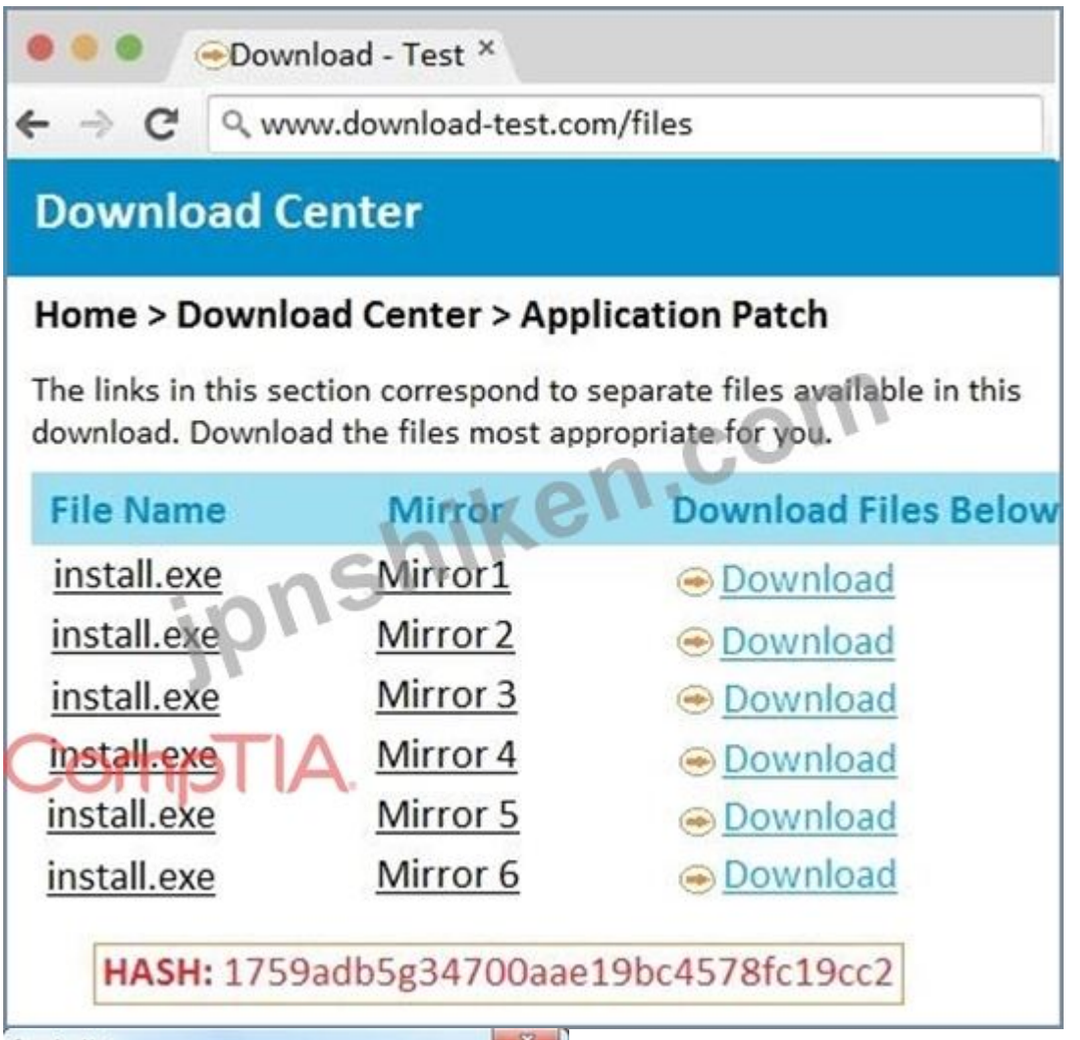
Policy	Device Type	% of Devices Compliant
Local Administration Accounts Renamed	Server	65%
Guest Account Disabled	Host	30%
Local Firewall Enabled	Host	80%
Password Complexity Enabled	Server	46%

CompTIA
jpnshiken.com

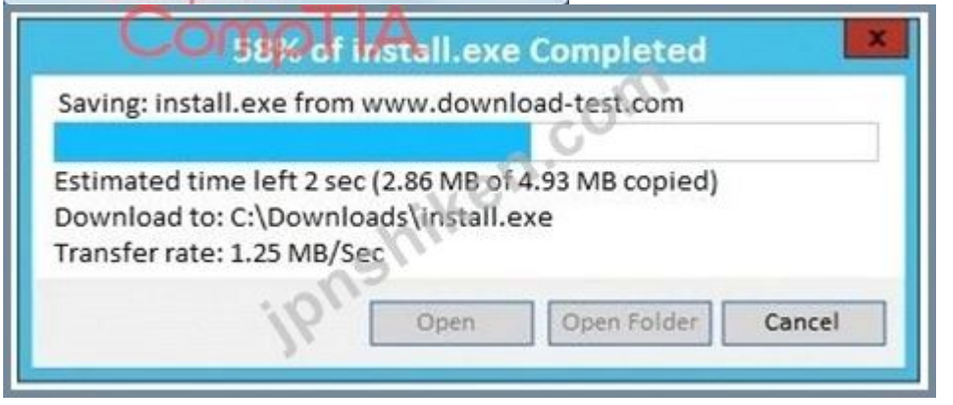
セキュリティエンジニアが上記の出力を生成するために使用しているツールはどれですか？
A. ポートスキャナ
B. SCAPスキャナー
C. SIEM
D. 脆弱性スキャナー
正解: (正解を表示します)

質問: **98**
管理者は、アプリケーションにパッチをインストールしたいと考えています。
指示
シナリオを前提として、最も安全な方法でパッチをダウンロード、検証、およびインストールします。
完了した最後のインストールが最終送信になります。
シミュレーションの初期状態に戻したい場合は、いつでも[すべてリセット]ボタンをクリックしてください。

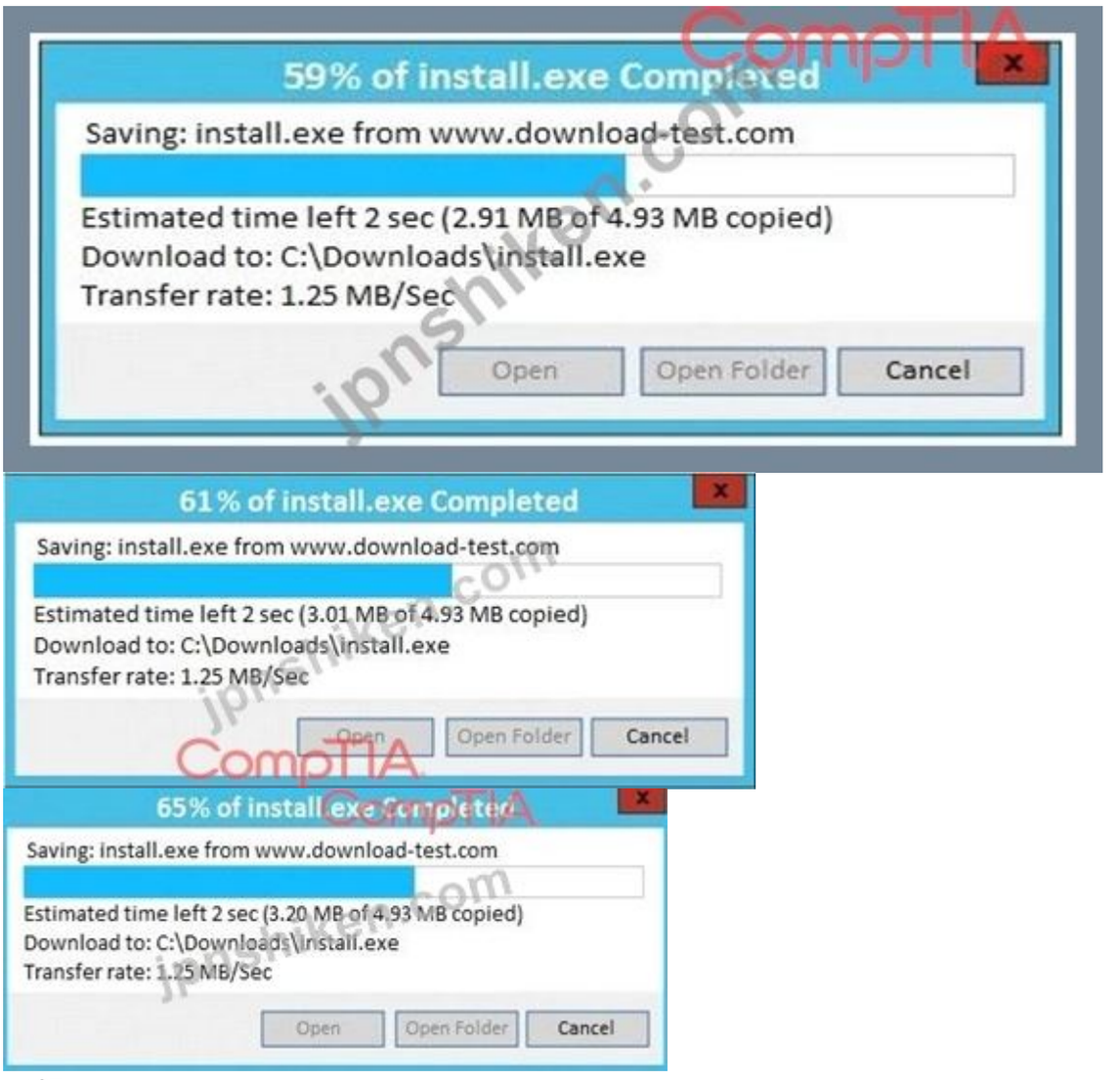








jpnshiken.com
CompTIA



正解:

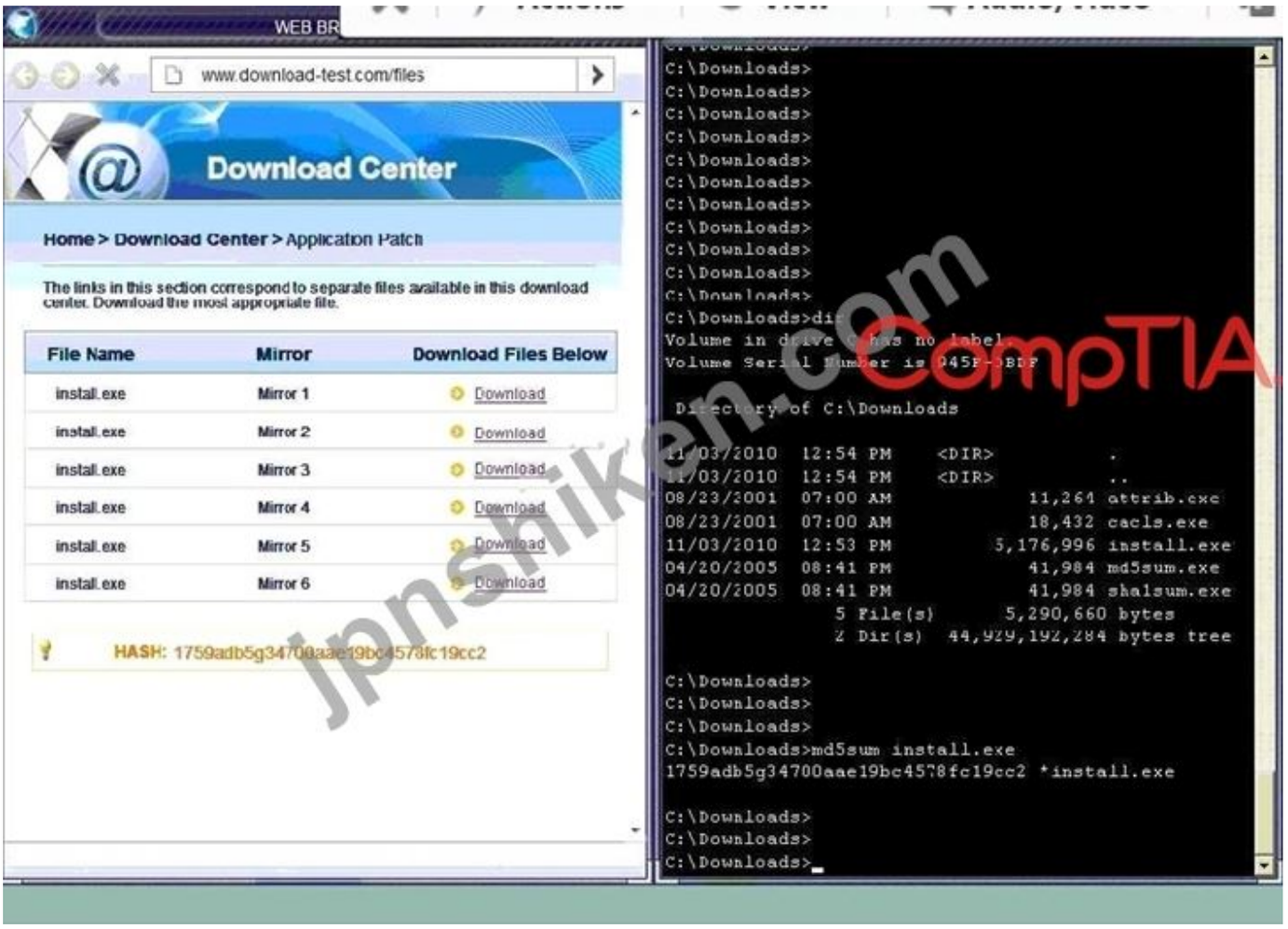
In this case the second link should be used (This may vary in actual exam). The first link showed the following error so it should not be used.



Also, Two of the link choices used HTTP and not HTTPS as shown when hovering over the links as shown:



Since we need to do this in the most secure manner possible, they should not be used.Finally, the second link was used and the MD5 utility of MD5sum should be used on the install.exe file as shown. Make sure that the hash matches.



Finally, type in install.exe to install it and make sure there are no signature verification errors.

質問: **99**

ある会社がDIPソリューションを展開し、ワークステーションとネットワークドライブをスキャンして、潜在的なPIIおよびペイメントカードデータを含むドキュメントを探しています。最初のスキャンの結果は次のとおりです。

Fileshare	PII findings	Payment card findings	Access permissions
Human resources	125,098	0	Administrator; DLP-Scan; HR_admins; HR-Staff; Help-Desk
Marketing	13,987	56	Administrator; DLP-Scan; Mrkt-Staff; Mrkt-Admin; Everyone
Payroll	456,765	1,236	Administrator; DLP-Scan; Payroll-Staff; Comptroller; Payroll-Admin; Internal-Audit
Accounts payable	13,873	978	Administrator; DLP-Scan; Comptroller; AP-Staff; AP-admin; Internal-Audit
Desktop support	0	0	Administrator; DLP-Scan; Help-Desk; Everyone

セキュリティ学習は、特定のファイルのデータ所有者をタイムリーに特定することができず、検出されたファイルのいずれかで悪意のあるアクティビティを疑うことはありません。データ所有者が正式に特定されるまで、固有のリスクに対処するのは次のうちどれですか？

A. 各ファイルのメタデータを検索してファイルの作成者を見つけ、リストされた作成者の個人用ドライブにファイルを転送します。
B. 買掛金および給与計算シェアから内部監査グループへのアクセスを削除します
C. ファイルをマーケティングシェアからセキュリティで保護されたドライブに移動します。
D. 共有ドライブ上のファイルを削除するようにDLPツールを構成します
正解: **(**正解を表示します**)**

質問: **100**
企業は、企業リソースから機密情報やデータにアクセスするために使用される新しく開発されたアプリケーションを保護したいと考えています。このアプリケーションはサードパーティ組織によって開発され、次のコントロールがないにもかかわらず、現在頻繁に使用されています。
*証明書のピン留め
*トークン化
*生体認証
同社はすでに次の管理を実装しています。
*完全なデバイス暗号化
* スクリーンロック
*デバイスのパスワード
*リモートワイプ
会社はデータ攻撃の傍受から防御したいと考えています会社は次の補償制御のどれを実装する必要がありますか？
A. 許可されたユーザーを認証するために帯域外の2番目の要素を実装する
B. 新しく開発したアプリケーションを使用する場合は、VPNの使用を強制します。
C. 会社の要件に従ってアプリケーションを無効にするジオフェンシングソリューションを実装します。
D. 追加の認証制御を必要とする安全なコンテナにアプリケーションをインストールします。
正解: **(**正解を表示します**)**

質問: **101**
セキュリティ管理者は、IPS-IDSシステムによって監視される特定のポートとIPアドレス、および会社と新しいビジネスパートナー間の境界ネットワーク上のファイアウォールの配置を確認しています。次のビジネスドキュメントのどれが、セキュリティ管理者が必要とするパラメータを定義します。確認？
A. ISA
B. BIA
C. MOU
D. NDA
正解: **B (**コメントを発表する**)**

質問: **102**

最近のセキュリティ評価では、Webアプリケーションがクリックジャッキングに対して脆弱である可能性があることが明らかになりました。アプリケーション開発者によると、修正は数か月先になる可能性があります。問題を軽減するために、セキュリティエンジニアがWebサーバーで設定する必要があるのは次のうちどれですか？
A. HttpOnly Cookieフィールド
B. 入力検証
C. ファイルのアップロードサイズの制限
D. X-Frame-Optionsヘッダー
正解: **(**正解を表示します**)**

質問: **103**
小規模な新興企業の最高経営責任者（CEO）は、ガバナンス、リスク管理、およびコンプライアンスに対処するためのセキュリティポリシーと評価を緊急に必要としています。同社にはリソースに制約のあるIT部門がありますが、情報セキュリティスタッフはいません。最高経営責任者（CEO）は、これを3ヶ月以内に完了するよう求めています。
次のうちどれが会社のニーズを満たすための最も費用対効果の高いソリューションでしょうか？
A. 情報セキュリティに関連するすべてのリスクを受け入れ、来年の年次理事会会議で再び問題を提起する。
B. 情報セキュリティのトレーニングを受けるIT担当者を1人選び、必要なすべてのポリシーと文書を社内で作成します。
C. スタートアップ企業の情報セキュリティ部門を運営する経験豊富なフルタイムの情報セキュリティチームを雇う。
D. コンサルタント会社にRFPを公開してから、要件を満たすことができる最も適切なコンサルタントを選択します。
正解: **D (**コメントを発表する**)**

質問: **104**
会社のポリシーに準拠するには、ファイアウォールルールを四半期ごとに確認する必要があります。複数の内部ネットワークの間にある内部ファイアウォールのレビューを行うように求められます。このファイアウォールの目的は、トラフィックをより安全にすることです。次の情報を前提として、以下にリストされているタスクを実行します。
信頼できないゾーン :0.0.0.0/0
ユーザーゾーン :USR 10.1.1.0/24
ユーザーゾーン :USR2 10.1.2.0/24
DBゾーン :10.1.4.0/24
Webアプリケーションゾーン :10.1.5.0/24
管理ゾーン :10.1.10.0 / 24
Webサーバー :10.1.5.50
MS-SQLサーバー :10.1.4.70
MGMTプラットフォーム :10.1.10.250

手順：必要なタスクを実行するには、DSTポート、SRCゾーン、プロトコル、アクション、またはルール順序の列を変更してください。ANYと入力して、すべてのポートを含めます。ファイアウォールACLはトップダウンで読み取られます。シミュレーション要件を満たしたら、[保存]をクリックします。シミュレーションが完了したら、[完了]ボタンを選択して送信してください。シミュレーションが送信されたら、[次へ]ボタンを選択して続行してください。

SRC Zone	SRC	SRC Port	DST Zone	DST	DST Port	Protocol	Action	Rule Order
UNTRUST	10.1.10.250	ANY	MGMT	ANY	ANY	ANY	PERMIT	↓
WEBAPP	10.1.5.50	ANY	DB	10.1.4.70	1433	UDP	DENY	↑ ↓
UNTRUST	ANY	ANY	ANY	ANY	ANY	TCP	PERMIT	↑ ↓
USER	10.1.1.0/24, 10.1.2.0/24	ANY	UNTRUST	ANY	80	TCP	PERMIT	↑ ↓
UNTRUST	ANY	ANY	WEBAPP	10.1.5.50	80	TCP	PERMIT	↑ ↓
DB	10.1.4.70	ANY	WEBAPP	10.1.5.50	ANY	ANY	DENY	↑

@ONSHIKEN.COM CompTIA

タスク1）管理プラットフォームがインターネットにアクセスできないようにするルールが追加されました。このルールは機能していません。ルールを特定し、この問題を修正します。
タスク2）SQLサーバーがWebサーバーからの要求のみを受信できるようにファイアウォールを構成する必要があります。
タスク3）Webサーバーは、企業ネットワークの内外のホストから暗号化されていない要求を受信できる必要があります。
タスク4）最終ルールが明示的な拒否であることを確認します。
タスク5）現在、ユーザーゾーンは暗号化されていないプロトコルを介してインターネットWebサイトにアクセスできます。ウェブサイトへのユーザーアクセスが安全なプロトコルのみを介して行われるようにルールを変更します。
手順：必要なタスクを実行するには、DSTポート、SRCゾーン、プロトコル、アクション、またはルール順序の列を変更してください。ANYと入力して、すべてのポートを含めます。ファイアウォールACLはトップダウンで読み取られます。シミュレーション要件を満たしたら、[保存]をクリックします。シミュレーションが完了したら、[完了]ボタンを選択して送信してください。シミュレーションが送信されたら、[次へ]ボタンを選択して続行してください。
正解:
Task 1: A rule was added to prevent the management platform from accessing the internet. This rule is not working. Identify the rule and correct this issue.
In Rule no. 1 edit the Action to Deny to block internet access from the management platform.
SRC Zone
SRC
SRC Port
DST Zone

DST
DST Port
Protocol
Action
UNTRUST
10.1.10.250
ANY
MGMT
ANY
ANY
ANY
DENY
Task 2: The firewall must be configured so that the SQL server can only receive requests from the web server.
In Rule no. 6 from top, edit the Action to be Permit.
SRC Zone
SRC
SRC Port
DST Zone
DST
DST Port
Protocol
Action
DB
10.1.4.70
ANY
WEBAPP
10.1.5.50
ANY
ANY
PERMIT
Task 3: The web server must be able to receive unencrypted requests from hosts inside and outside the corporate network.
In rule no. 5 from top, change the DST port to Any from 80 to allow all unencrypted traffic.
SRC Zone
SRC
SRC Port
DST Zone
DST
DST Port
Protocol

Action
UNTRUST
ANY
ANY
WEBAPP
10.1.5.50
ANY
TCP
PERMIT
Task 4: Ensure the final rule is an explicit deny
Enter this at the bottom of the access list i.e. the line at the bottom of the rule:
SRC Zone
SRC
SRC Port
DST Zone
DST
DST Port
Protocol
Action
ANY
ANY
ANY
ANY
ANY
ANY
TCP
DENY
Task 5: Currently the user zone can access internet websites over an unencrypted protocol. Modify a rule so that user access to websites is over secure protocols only.
In Rule number 4 from top, edit the DST port to 443 from 80
SRC Zone
SRC
SRC Port
DST Zone
DST
DST Port
Protocol
Action
USER
10.1.1.0/24 10.1.2.0/24
ANY

UNTRUST
ANY
443
TCP
PERMIT

質問: **105**
ある会社の評価を行うためにコンサルティング会社が雇われました。最初の段階では、侵入テスト担当者が次のような出力を提供するツールを使用しました。
TCP 80を開く
TCP 443がオープン
TCP 1434のフィルタリング
ペネトレーションテスターはその後、別のツールを使用して以下の要求を行いました。
GET / script / login.php？token = 45 $ MHT000MND876
GET / script/login.php?token=@#984DCSPQ%091DF
侵入試験機は次のどのツールを使用しましたか。
A. ログアナライザー
B. ポートスキャナー
C. HTTPインターセプター
D. ファザー
E. ブルートフォーサー
F. プロトコルアナライザ
正解: (正解を表示します)

質問: **106**
セキュリティ技術者が侵入テスト中にアプリケーションを悪用することに成功しました。この悪用の証拠として、セキュリティエンジニアはアプリケーション内でデータが侵害された方法のスクリーンショットを撮ります。スクリーンショットから以下の情報を与えます。



次のツールのうちどれがアプリケーションを悪用するために使用された可能性が最も高いですか？
A. エンジニアがサーバーに照会し、HTTPプロキシインターセプターを使用してデータを編集した
B. エンジニアはHTTPヘッダーをキャプチャしてから、JSONデータをバナーグラブツールに置き換えました
C. エンジニアは、curlを介して送信されたクロスサイトスクリプトを使用してデータを編集しました。
D. エンジニアはプロトコルアナライザでデータをキャプチャしてからデータを編集するためにPythonを利用しました
正解: **A** (コメントを発表する)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
医療機器会社は、その製造工場で新しいCOTSウイルス対策ソリューションを実装しています。新しいソフトウェアとの相互運用性について、すべての検証済みの機器および機器を再テストする必要があります。ソフトウェアと機器が設計どおりに機能していることを確認するのに最も適しているものはどれですか。
A. ユーザー受け入れテスト
B. 変更管理文書
C. ピアレビュー
D. 静的コード分析テスト
E. システム設計書
正解: (正解を表示します)

質問: **108**
ある企業は、攻撃時に回復力のあるセキュリティアーキテクチャを実装することを優先的に行っています。最近の事件では、攻撃者が暗号化の実装とVPNコンセントレータの潜在的な脆弱性を利用して、機密情報を危険にさらす可能性があります。これらの緊急の脆弱性に対するパッチがゆっくりとリリースされ、数週間から数か月の露出した脆弱な攻撃対象領域が残ります。次のアプローチのうち、同様の将来の攻撃時に企業の回復力を高めるのに最適なものはどれですか？
A. VPNコンセントレーターで使用される暗号暗号をアップグレードします
B. リモートVPNユーザーを本番LANから論理的にセグメント化します

C. さまざまなメーカーのアプライアンスとソフトウェアを実装する
D. オープンソースソフトウェアを最大化して、より迅速なパッチリリースの恩恵を受ける
正解: **(**正解を表示します**)**

質問: **109**
ある会社は、従業員のために出席者の多いオンプレミスのフィットネスクラブを運営しており、毎日約200人が参加しています。従業員は、センターのログインおよび出席プログラムをスマートフォンと同期させたいと考えています。フィットネスセンターの契約を管理する人事部は、セキュリティとプライバシーの要件の草案作成を支援するようにセキュリティアーキテクチャに依頼しました。これらのプライバシーの懸念に最もよく対処するのは次のうちどれですか？
A. コンテナ化を実装する
B. 生体認証を使用します。
C. 無許可のドメインブリッジをブロックします。
D. ジオロケーション/ジオフェンシングを利用します。
正解: **(**正解を表示します**)**

質問: **110**
ある会社がセキュリティコンサルタントと契約して、リモートホワイトボックス侵入テストを実行します。同社は、コンサルタントが本番サービスに悪影響を与えずにインターネット向けサービスに集中することを望んでいます。企業の攻撃面を特定するために最も使用する可能性が高いコンサルタントは次のうちどれですか。 2つ選択）
A. WHOISレジストリ
B. 内部ルーティングテーブル
C. DNSレコード
D. 会社のファイアウォールACL
E. ディレクトリサービスクエリ
F. Webクローラー
正解: **(**正解を表示します**)**

質問: **111**
新しいシステムの開発プロセスの一環として、組織は要件分析とリスク評価の実行を計画しています。この新しいシステムは、組織がデータ分析の実行に使用していたレガシーシステムを置き換えるものです。次のうちどれがプロジェクトのこの段階の間に経営者によって行われた活動の一部である可能性がありますか？
A. 応答時間が利害関係者に受け入れられることを確認するためのシステムの負荷テスト
B. 静的コード分析とすべてのアプリケーションコードの査読
C. システムのパフォーマンスとセキュリティに関する期待の検証
D. 展開中のレガシシステムとの相互運用性を評価するための回帰テスト
E. システムが正しく配備されていることを確認するための設計レビューおよびユーザー受け入れテスト

正解: **A** (コメントを発表する)

質問: **112**
適切なデータ保持ポリシーによって軽減できる攻撃は次のうちどれですか？
A. ごみ箱ダイビング
B. 水飲み場
C. マンインザブラウザ
D. スピアフィッシング
正解: (正解を表示します)

質問: **113**
セキュリティコンサルタントは、機密性の高いサイトの物理的なセキュリティを改善しており、レポートに含めるためにブランドのない建物の写真を撮っています。2週間後、セキュリティコンサルタントは電話を置き忘れ、1時間しか充電されません。携帯電話を見つけた人は、所有者を見つけて返品しようとしてMicroSDカードを取り外します。
人は電話から次のデータを抽出し、いくつかのファイルからEXIFデータを抽出します。
DCIM画像フォルダ
オーディオブックフォルダー
トレンツ
私のTAX.xls
Consultancy HR Manual.doc
カメラ :SM-G950F
露出時間 :1/60秒
場所 :3500 Lacey Road USA
次のベストのどれがセキュリティの問題を説明していますか？
A. MicroSDは暗号化されておらず、ジオタグ情報が含まれています。
B. MicroSDは暗号化されておらず、個人データも含まれています。
C. MicroSDには海賊版ソフトウェアが含まれており、暗号化されていません。
D. MicroSDには、個人データと仕事データが混在しています。
正解: **B** (コメントを発表する)

質問: **114**
会社のホストされたVM環境に新しいデータベースアプリケーションが追加されました。データベースユーザーがサーバーにリモートでアクセスできるように、ファイアウォールACLが変更されました。同社のクラウドセキュリティブローカーは、オンサイトのデータベースユーザーから異常を特定しました。さらに調査すると、セキュリティチームは、直接、ハイパーバイザやその他の機密データへのアクセスへのアクセスを提供するVM上のユーザのRANコードに気づきました。
VM環境内での将来の攻撃を軽減するために、セキュリティは次のうちどれを行うべきですか？（2つ選択してください。）

A. 境界NGFWをインストールします。
B. データベースVMのプロビジョニングを解除します。
C. VM分離を構成します。
D. ユーザーのアクセス権限を変更します。
すべてのエンドポイント上のF.アップデートウイルス定義。
E. は、適切なパッチをインストールします。
正解: (正解を表示します)

質問: **115**
侵入テスト担当者がComptia.orgで評価を実施しており、公衆インターネットに接続している間にコーヒーショップから次のコマンドを実行します。



侵入テスト担当者は、コマンド出力について次のうちどれを結論付ける必要がありますか？
A. 192.168.102.67はバックアップメールサーバーで、攻撃に対して脆弱な場合があります。
B. Comptia.org DNSサーバーのパブリックビューとプライベートビューが正しく設定されていません
C. Comptia.orgのDNS SPFレコードは更新されていません
D. Comptia.orgは古いメールサーバを実行しています。これはエクスプロイトに対して脆弱です。
正解: (正解を表示します)

質問: **116**
攻撃者は、地域全体の銀行機関の標的を危険にさらしています。地元の銀行の最高情報セキュリティ責任者（CISO）は、銀行が被害者になる前に攻撃を検出して防止したいと考えています。
CISOは次のどのアクションを実行する必要がありますか？
A. CASBソリューションを購入して、クラウドベースのアプリケーションとサービスへのアクセスを識別および制御し、それらをオンプレミスのレガシーセキュリティモニタリングと統合します
B. 銀行セクターの情報共有協会からの脅威インテリジェンスフィードを消費するようにIDSを構成するようにセキュリティエンジニアに指示します
C. クラウドベースの脅威分析を利用して、企業のB2Bおよびベンダートラフィックの異常な動作を特定します
D. 毎月、地方銀行協会のロビー活動グループ会議に出席して出席し、このトピックに関する議論を促進します。
正解: (正解を表示します)

質問: **117**
コアインシデント対応チームの一員であるファーストレスポンダは、ディレクトリ全体を暗号化するためにNASに呼びかけていた3つのホストを隔離するために急いでデータ損失を招いたランサムウェアの発生を封じ込めるために取り組んでいます。調査せずに直ちに閉鎖され、その後隔離された。
次のうちどれが逃しましたか？ 2つ選んでください。）
A. 一時ファイルシステムとスワップ空間
B. CPU、プロセス状態テーブル、およびメインメモリダンプ
C. ランサムウェアの暗号化を決定するための妥協の指標
D. 調査に必要なCoC情報
E. 既知のクリーンな状態にデータを復元するために必要な基本情報
正解: **(**正解を表示します**)**

質問: **118**
セキュリティエンジニアは、Web開発者が新しい企業Webアプリケーションを評価するのを支援しています。アプリケーションはインターネットに接続されるため、エンジニアは次の推奨事項を作成します。
htaccessファイルまたはサイト構成に以下を追加します。
またはロケーションブロックに追加します。

```
HeadereditSet_Cookie ^(.*)$ $1;HttpOnly;Secure
```

セキュリティエンジニアがCookieを介して達成しようとしているのは次のうちどれですか？ 2つ選択してください）
A. 一時的なCookieストレージ用にユーザーのドライブルートに一時スペースを作成します
B. CSRFを防ぐために、転送中にシーケンスIDをCookieセッションIDに追加します。
C. セッションIDが各Cookieリクエストで動的に生成されるようにします
D. Cookieが他のドメイン名に送信されないようにする
E. TLS接続を介した場合にのみCookieの作成または更新を許可する
F. 安全なローカルCookieストレージでプレーンテキストHTTP送信の使用を強制する
正解: **(**正解を表示します**)**

質問: **119**
セキュリティアナリストは、適切な技術管理設定とパラメータを選択する前に、次の企業要件を検討しています。
RTO :2日
RPO :36時間
MTTR :24時間
MTBF :60日
次の解決策のどれがRPOの要件に対処しますか？
A. リアルタイムSyslog機能を収集するSyslog機能

B. 毎日のスナップショットを実装するバックアップソリューション
C. 地域ごとに分散したクラウド環境
D. 5ナインのアップタイムを実現するロードバランサの背後にあるサーバーファーム
正解: **B** (コメントを発表する)

質問: **120**
安全な施設には、現在、単純なロックとキーによって制御されているサーバールームがあります。何人かの管理者が鍵のコピーを持っています。法令順守を維持するために、管理者のスマートフォン上のアプリケーションによって制御される2番目のロックを購入してインストールします。アプリケーションには、使用できるさまざまな認証方法があります。最も適切な方法を選択するための基準は次のとおりです。
*エンドユーザーに侵入することはできません
※2つ目の要素として活用する必要があります。
*情報共有は避ける必要があります
*他人受入率が低くなければなりません
次のベストのどれが基準を満たしていますか？
A. 複雑なパスコード
B. 顔認識
C. スワイプパターン
D. 指紋スキャン
E. トークンカード
正解: (正解を表示します)

質問: **121**
2つの異なる会社の最高経営責任者（CEO）は、それぞれの会社を合併するという非常にデリケートな見通しについて話し合っています。どちらも最高情報責任者（CIO）を招待して、安全かつデジタルで通信する方法を見極め、次の基準をまとめて決定します。
*メールサーバーとクライアントで暗号化する必要があります
*安全でないインターネット接続を介して送信するには問題がない
次の通信方法のうちどれが推奨されますか？
A. 両方のドメインでSTARTTLSを有効にします。
B. ドメイン間でTLSを強制します。
C. PGP暗号化メールを使用します。
D. DNSSECを利用するように両方のドメインを切り替えます。
正解: (正解を表示します)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試

験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu　**683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
2社の競合企業が、さまざまな攻撃者によるネットワークへの同様の攻撃を受けました。応答時間を短縮するために、両社は攻撃の発生源と方法に関する脅威情報を共有したいと考えています。次のビジネス文書のどれが、このエンゲージメントを文書化するのに最適でしょうか？
A. 業務提携契約
B. 覚書
C. サービスレベル契約
D. 相互接続セキュリティ契約
正解: **D (**コメントを発表する**)**
References:

質問: **123**
アナリストはSIEMで.cnドメイン名に変わった活動に気づいた。アナリストはトラフィックの内容を識別するために次のうちどれを使用すべきですか？
A. パケットキャプチャ
B. サービスの発見
C. ログレビュー
D. DNSハーベスティング
正解: **(**正解を表示します**)**

質問: **124**
組織は、次の管理マトリックスを確立しています。
次のコントロールセットは組織によって定義されており、集約的に適用されます。
PIIを含むシステムは、最小限の制御セットで保護されます。
医療データを含むシステムは、中程度のレベルで保護されています。
カード会員データを含むシステムは、高レベルで保護されています。
組織は、クライアントからのPIIと医療データを含むデータベースの機密を保護するシステムを展開する準備をしています。コントロールの分類に基づいて、次のコントロールのどれがこれらの要件を最もよく満たすでしょうか？
A. サーバールームへの近接カードアクセス、コンテキストベースの認証、UPS、およびデータベースサーバーのフルディスク暗号化。
B. 侵入検知機能、ネットワークベースのIPS、ジェネレーター、およびコンテキストベースの認証。
C. サーバールームのドアの暗号ロック、FDE、サージプロテクタ、およびすべてのアプリケーションコードの静的分析。

D. すべてのアプリケーション変更のピアレビュー、アプリケーションコードの静的分析、UPS、およびシステム全体の侵入テスト。
正解: **(**正解を表示します**)**

質問: **125**
技術者が、移動中に公衆インターネット接続を頻繁に利用するユーザーのために、モバイルデバイスマネージャでセキュリティオプションを構成しています。フルディスク暗号化が有効になっていることを確認した後、技術者は次のセキュリティ対策のうちどれを講ずるべきですか？ 2つ選んでください。）
A. 営業時間中にデバイスが長距離電話をかけるのを制限する
B. 常時接続VPNを実装する
C. 会社用パーティションと個人用パーティションのリモートワイプを発行する
D. すべてのモバイルデバイスのバックアップを暗号化する必要があります
E. すべてのモバイルデバイスがUSB OTGを使用して確実にバックアップされるようにする
正解: **(**正解を表示します**)**

質問: **126**
情報セキュリティ担当者は、1つのセキュアネットワークと1つのオフィスネットワークを担当します。最近の情報によると、ネットワーク間で同様のログイン認証情報があるため、攻撃者がセキュリティで保護されたネットワークにアクセスする可能性があります。情報を変更する必要があるユーザーを判断するために、情報セキュリティ担当者はツールを使用して両方のネットワーク上のハッシュ値でファイルをスキャンし、次のデータを受け取ります。

Corporate Network		Secure Network	
james.bond	asHU8$1bg	jbond	asHU8$1bg
tom.jones	wit4njyt%I	tom.jones	wit4njyt%I
dade.murphy	mUrpHTIME7	d.murph3	t%w3BT9)n
herbie.hancock	hh2016!#	hhanco	hh2016!#2
suzy.smith	1Li*#HFadf	ssmith	1LI*#HFadf

CompTIA
jpnshiken.com

ファイル内のハッシュ値からこの情報を収集するために使用されたツールはどれですか。
A. ファザー
B. 脆弱性スキャナー
C. パスワードクラッカー
D. プロトコルアナライザ
E. MD5ジェネレータ
正解: **E (**コメントを発表する**)**

質問: **127**
組織がWebサーバーを強化し、潜在的な攻撃者によって開示される可能性のある情報を削減しようとしています。セキュリティの分析...最近のWebサーバースキャンの脆弱性スキャン結果を確認しています。
スキャン結果の一部を以下に示します。
検索番号5144322
初めて検出された2015年11月10日09:00 GMT_0600
最終検出日 :2015年11月10日09:00 GMT_0600
CVSS base: 5
Access path: http://myorg.com/mailinglist.htm
Request: GET http://mailinglist.aspx?content=volunteer
Response: C:\Docments\MarySmith\malinglist.pdf
Which of the following lines indicates information disclosure about the host that needs to be remediated?
A. First Time detected 10 nov 2015 09:00 GMT_0600
B. Request: GET http://myorg.come/mailinglist.aspx?content=volunteer
C. Access path: http//myorg.com/mailinglist.htm
D. Finding#5144322
E. Response: C:\Docments\marysmith\malinglist.pdf
正解: **E (**コメントを発表する**)**

質問: **128**
企業がフィッシングおよびスピアフィッシングキャンペーンの被害者であるユーザーが一般的な銀行サイトのようなWebサイトリンクをクリックして、資格情報を誤って入力しているセキュリティエンジニアは、フィッシングを防止するか、その影響を軽減するために多層防御を使用することを決定します。セキュリティエンジニアが実装する必要があるのは次のどれですか？　2つ選択）
A. ログ監視
B. コンテンツフィルター
C. スパムフィルター
D. クライアント証明書
E. データ損失防止
F. ホスト侵入防止
正解: **B,C (**コメントを発表する**)**

質問: **129**
新しく採用されたセキュリティアナリストが、確立されたSOCチームに参加しました。企業指向を経てまもなく、Webベースのアプリケーションに対する新しい攻撃方法が一般に公開されました。セキュリティアナリストはすぐにこの新しい情報をチームリーダーにもたらしますが、チー

ムリーダーはそれを心配していません。次のうちどれがチームリーダーの地位のための最も可能性の高い理由ですか？

A. Webベースのアプリケーションは、独立したネットワークセグメント上にあります。

B. 会社の方針では、NIPSの署名は1時間ごとに更新する必要があります。

C. 攻撃の種類が組織の脅威モデルを満たしていません。

D. 組織はWebベースの脅威に関連するリスクを受け入れています。

正解: **(**正解を表示します**)**

質問: **130**

セキュリティ技術者が、元々最高情報セキュリティ責任者（CISO）から取締役会に送信されたレポートのコピーを受け取ります。

この報告書は、過去12か月間の以下のKPVKRIデータの概要を示しています。

Month	AV Fleet Coverage	AV Signature Updated	Detected Phishing Attempts	Infected Systems	Threat Landscape Rating	Number of Open Security Incidents
January	30%	100%	40	26	High	40
February	20%	100%	8	4	Low	40
March	40%	100%	2	3	Low	30
April	50%	98%	17	12	Medium	30
May	90%	98%	40	5	Low	20
June	95%	98%	10	13	Medium	30
July	95%	98%	25	13	Medium	30
August	95%	96%	8	15	Medium	40
September	95%	90%	9	10	Medium	50
October	95%	90%	20	4	Low	65
November	95%	98%	17	7	Low	75
December	95%	100%	5	22	High	85

CompTIA
Ipnshiken.com

次のBESTのどれが上記のデータから解釈されることができるかについて説明しますか？

A. 1.フリート全体のAVカバレッジが向上しました2。感染したシステムとAVの適用範囲との間に相関関係はありません。検出されたフィッシング攻撃と感染したシステムとの間に相関関係はありません4。脅威のランドスケープ評価と感染したシステムとの間に相関関係が存在するようです。セキュリティチームの有効性とパフォーマンスは低下しているようです。

B. 1. AVシグネチャカバレッジは常に高いままです2。フリート全体のAVカバレッジが向上しました3。フィッシング攻撃と感染したシステムとの間に相関関係が存在するようです4。脅威のランドスケープ評価とセキュリティチームのパフォーマンスの間には相関関係があります。検出されたフィッシング攻撃と感染したシステムとの間に相関関係はありません

C. 1.感染したシステムとAVの適用範囲との間に相関関係はありません2。フリート全体のAVカバレッジが向上しました3。フィッシング攻撃と感染したシステムとの間に相関関係が存在する

ようです4。脅威のランドスケープ評価とセキュリティチームのパフォーマンスとの間に相関関係はありません。検出されたフィッシング攻撃と感染したシステムの間には相関関係があります
D. 1.艦隊全体のAVカバレッジは減少しました2。感染したシステムとAVの適用範囲との間に相関関係はありません。フィッシング攻撃と感染したシステムとの間に相関関係が存在するようです4。脅威のランドスケープ評価とセキュリティチームのパフォーマンスとの間に相関関係はありません5。セキュリティチームの有効性とパフォーマンスは低下しているようです。
正解: **A** (コメントを発表する)

質問: **131**
セキュリティアナリストがクライアントの安全なネットワークに侵入しようとしています。アナリストには、現在使用されているパブリックIPアドレスのブロックを除いて、クライアントに関する事前情報は与えられませんでした。ネットワークの列挙後、アナリストの次のステップは次のことを実行することです。
A. グレーボックス侵入テスト
B. 赤いチーム演習
C. 脆弱性評価
D. 外部セキュリティ監査
E. リスク分析
正解: (正解を表示します)

質問: **132**
病院は、アプリケーションサーバーとアプリケーションのセグメントをサポートする仮想ホスト上のデータベースとの間のトラフィックにマルチキャストを必要とする従来の電子医療記録システムを使用しています。スイッチのアップグレード後、ハイパーバイザーとストレージの間の物理的な接続が確立されているにもかかわらず、電子カルテは利用できません。ネットワークチームは、マルチキャストトラフィックが電子カルテへのアクセスを回復できるようにする必要があります。ISMは、ネットワークチームがネットワーク上のマルチキャストトラフィックのフットプリントを減らす必要があると述べています。

VLAN	Description
201	Server VLAN1
202	Server VLAN2
400	Hypervisor Management VLAN
680	Storage Management VLAN
700	Database Server VLAN

CompTIA
jpnshiken.com

上記の情報を使用して、どのVLANでマルチキャストを有効にする必要がありますか。
A. VLAN 201、VLAN 202、VLAN 400、VLAN 680、VLAN 700
B. VLAN 201、VLAN 202、VLAN 400
C. VLAN 201、VLAN 202、VLAN 700
D. VLAN400、VLAN680、VLAN700

正解: (正解を表示します)

質問: **133**
組織で設定されているセキュリティポリシーでは、USBドライブを企業全体で使用することは禁止されており、それらをブロックするための適切な技術的管理が行われています。さまざまな場所からさまざまなコンピューティングリソースで作業できるようにするための方法として、何人かの営業スタッフが、IT部門の同意なしにWebベースのストレージソリューションにサインアップしました。ただし、オペレーション部門は、特定のビジネスパートナ伝票を送信するために同じサービスを使用する必要があります。
IT部門がこの動作を監視および制御することを許可するのは、どれが最も良いのでしょうか。
A. NGFWを設定する
B. vTPMを利用する
C. AAAを有効にする
D. WAFをインストールする
E. CASBの配置
正解: **E** (コメントを発表する)

質問: **134**
銀行の目的の1つは、セキュリティ意識の文化を浸透させることです。次のうちどれがこれを達成するのを助けることができるテクニックですか？ (2つ選んでください。)
A. 連続監視
B. 職務分離
C. フィッシングシミュレーション
D. ランチアンドラーニング
E. ブルーチーミング
F. ランダム監査
正解: **A,C** (コメントを発表する)

質問: **135**
次回の監査に備えて、最高情報セキュリティ責任者 (CISO)は、
実稼働サーバー上の1200の脆弱性が修正されます。セキュリティエンジニアは、最も危険なリスクを移行するためにリソースに優先順位を付けることができるように、どの脆弱性が悪用可能な実際の脅威を表すのかを判断する必要があります。CISOは、脆弱性スキャンの結果を使用してアクションの優先順位を設定しながら、セキュリティエンジニアが外部の脅威と同じように行動することを望んでいます。次のアプローチのどれが説明されていますか？
A. ブルーチーム
B. 赤いチーム
C. ブラックボックス
D. 白チーム
正解: (正解を表示します)

References:

質問: **136**
ある会社が営業時間を超えてヘルプデスクの可用性を拡張したいと考えています。最高情報責任者（CIO）は、電話に応答し、パスワードのリセットやリモートアシスタンスなどのTier 1の問題解決を提供するサードパーティのサービスでヘルプデスクを増強することにしました。セキュリティ管理者は、次のようなファイアウォールの変更を加えました。



管理者は、サードパーティ会社に適切なパスと資格情報を提供します。
次のうちどれがサードパーティへのアクセスを提供するために使用されている可能性がありますか。
A. WAYF
B. RADIUS
C. SAML
D. OpenID
E. LDAP
正解: (正解を表示します)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
企業ネットワーク上のサーバー（10.0.0.2）は、危険にさらされて別のネットワークセグメントに接続されている多数のマーケティングデスクトップからDoSを受けています。セキュリティエンジニアは、管理ルータに次の設定を実装します。

```
Router(config)# ip route 192.168.3.1 255.255.255.255 Null0
Router(config)# route-map DATA
Router(config-route-map)#match tag 101
Router(config-route-map)#set ip next-hop 192.168.3.1
Router(config-route-map)#set community no-export

Router(config-router)#redistribute static route-map DATA

Router(config)ip route 10.0.0.2 255.255.255.255 Null0 tag 101
```

エンジニアは次のうちどれを実装していますか？

A. 経路保護
B. アドレス空間レイアウトのランダム化
C. リモートトリガーされたブラックホール
D. 輸送セキュリティ
E. ポートセキュリティ
正解: **A** (コメントを発表する)

質問: **138**
ユーザーは、内部で開発されたWebアプリケーションが不規則に動作しており、応答出力に一貫性がないことを報告しています。この問題は、セキュリティを向上させるためにWebアプリケーションの依存関係パッチが適用された後に始まりました。
問題の特定に役立つ最も適切なツールは次のうちどれですか？

A. Vulnerability scanner
B. Fuzzer
C. SCAP scanner
D. HTTP interceptor
正解: (正解を表示します)

質問: **139**
会社のセキュリティポリシーには、2つの形式のネットワークベース認証を使用してリモート接続を検証する必要があると記載されています。また、ローカルの管理アカウントをリモートアクセスに使用しないでください。PKIは現在ネットワーク内で設定されていません。RSAトークンは、2FA認証に使用できるモバイルアプリケーションだけでなく、すべての従業員に提供されています。外部接続にセキュリティを提供するために、ネットワーク内に新しいNGFWがインストールされました。同社はVPN接続にも使用することを決定しました。次のうちどれを設定する必要がありますか？　2つ選んでください。）

A. 証明書ベースの認証
B. 802.1X
C. LDAP
D. RADIUS

E. TACACS+
F. ローカルユーザーデータベース
正解: **C,D** (コメントを発表する)

質問: **140**
セキュリティアナリストが毎週の電子メールレポートを確認し、内部のセキュリティアラート電子メールアドレスから毎日平均1.000の電子メールを受信していることを発見しました。次のうちどれを実装する必要がありますか？
A. システム管理者の職務の分離
B. ネットワーク監視サービスの調整
C. DoS攻撃の防止
D. 機械学習アルゴリズム
正解: (正解を表示します)

質問: **141**
SOCは、オープンWiFiゲストネットワークからの異常な量のトラフィックが、より広範なネットワーク速度低下と相関しているように見えることに気づきました。ネットワークチームはトラフィックをキャプチャできませんが、ネットワークサービスからのログは利用できます。
*ゲストネットワークのキャプティブポータルを介して最近認証されたユーザーはいません
* DDoS緩和システムは警告を発していません
* DNSリゾルバーログには非常に長いドメイン名が表示されます
次のうち、セキュリティアナリストが次に取るべき最善のステップはどれですか？
A. アクセスペントフォグを確認して、潜在的なゾンビサービスを特定します
B. 境界ファイアウォールでゲストネットワークからのすべてのアウトバウンドトラフィックをブロックします
C. ゲストネットワークのパスフレーズが変更されていないことを確認します。
D. ウイルス対策ログを検索して、侵害された会社のデバイスの証拠を探します
正解: (正解を表示します)

質問: **142**
ある企業は、悪意のあるDNS要求を陥没させるクラウドベースのセキュリティソリューションを実装したいと考えています。
セキュリティ管理者は、DNS要求をクラウドサーバーに送信するための技術的制御を実装しましたが、ユーザー定義のDNS手動設定を持つ可能性のあるすべてのマネージドエンドポイントとアンマネージドエンドポイントにソリューションを拡張したいと考えています。接続されているすべてのデバイスを保護しますか？
A）次のようにファイアウォールACLを実装します

```
PERMIT UDP ANY CLOUD_SERVER EQ 53
DENY UDP ANY ANY EQ 53
```

B）次のようにNATを実装します。

ORIGINAL				TRANSLATED			
SRC IP	SRC PORT	DST IP	DST PORT	SRC IP	SRC PORT	DST IP	DST PORT
SAME	SAME	SAME	53	PAT POOL	SAME	CLOUD SERVER	53

C）次のようにDHCPオプションを実装します。

```
DHCP DNS1: CLOUD_SERVER1
DHCP DNS2: CLOUD_SERVER2
```

D）次のようにポリシールーティングを実装します。

```
100 PERMIT UDP ANY ANY ANY 53
200 PERMIT UDP PAT_POOL ANY CLOUD_SERVER 53
IP ROUTE_MAP 200 200
```

A. オプションB
B. オプションC
C. オプションA
D. オプションD
正解: **D** (コメントを発表する)

質問: **143**
データベース管理者は、日常のタスクを実行するときにプライバシー原則を遵守し、実装する必要があります。管理者は、組織のシステム内に格納されているPIIの一意のインスタンスの数をできるだけ少なくするよう管理者に指示します。
次の原則のどれが実証されていますか？
A. データ最小化
B. PIIセキュリティ
C. 管理者の説明責任
D. レコードの透明度
正解: (正解を表示します)

質問: **144**
新しいセキュリティポリシーは、すべてのワイヤレスおよび有線認証に、すべての従業員がエンタープライズLAN内の内部リソースに接続するときに証明書を使用することを含める必要があります。新しいセキュリティポリシーに準拠するように構成する必要があるのは次のうちどれですか。 2つ選択してください）。
A. SSO
B. PKI
C. 新しい事前共有キー
D. 8021X
E. OAuth
F. プッシュベースの認証
正解: (正解を表示します)

質問: **145**
機密データの漏洩を心配しているセキュリティアナリストは次のようにレビューしています。
```
10:01:32. 384853 IP (tos 0x0, ttl 64, id 40587, offset 0, flags [DF], proto ICMP (1), length 1500
192.168.1.20 -> 100.61.100.2: ICMP echo reply, id 1592, seq 8, length 1500
```
次のツールのどれがアナリストがデータ漏洩が発生しているかどうかを確認することを可能にするでしょうか？
A. ファイル整合性モニタ
B. SCAPツール
C. ポートスキャナ
D. プロトコルアナライザ
正解: **(**正解を表示します**)**

質問: **146**
特定のジョブタスクに不可欠な情報のみを表示できるシステムの設計は、以下を使用して正常に実行できます。
A. 職務の分離
B. 役割ベースのアクセス制御
C. ジョブローテーション
D. 随意アクセス
E. 必須の休暇。
正解: **(**正解を表示します**)**

質問: **147**
ネットワークのセキュリティおよびストレージアプリケーションの最近の概要では、セキュリティ上の理由から分離する必要がある大量のデータが明らかにされています。以下は、ネットワーク上で構成されている重要なアプリケーションとデバイスです。
* ファイアウォール
* コアスイッチ
* RMサーバー
* 仮想環境
* NACソリューション
セキュリティマネージャはまた、すべての重要なアプリケーションからのデータを集約して、複数のソースからのイベントを関連付けることを望んでいます。重要なアプリケーションやデバイスでデータの集約とデータの分離を確実に実行するために、特定のアプリケーションで次のうちどれを設定する必要がありますか。 2を選択）
A. データの残り
B. ルーティングテーブル
C. ゾーン
D. ポート集約
E. ログ転送

F. NICチーミング
正解: **C,E (**コメントを発表する**)**

質問: **148**
組織は、ゼロデイ脅威の出現後すぐに、そのサイバーセキュリティ防御スイートを自動的に武装させたいと考えています。次のデータ標準のうち、組織がこの目的を達成するのに最も適したものをサポートするツールとサービスを取得することはできますか？
A. CWE
B. OVAL
C. XCCDF
D. CVE
E. STIX
正解: **(**正解を表示します**)**

質問: **149**
組織のモバイルデバイスインベントリは最近、デバイスのベースバンドを制御するために使用されるコードでゼロデイ脆弱性が識別されたという通知を提供しました。デバイスの製造元はパッチを迅速に処理していますが、展開には数か月かかりますさらに、最近海外旅行から戻ってきた数人のモバイルユーザーが、電話に不明なアプリケーションが含まれていると報告し、デバイスのパフォーマンスが低下していますユーザーはこれらのアプリケーションをアンインストールできませんでした。デバイス次の最も発生した可能性が高く、パッチがリリースされるまで緩和策を提供するのはどれですか？
A. 攻撃者が監視アプリケーションをダウンロードしました。影響を受けるデバイスの完全な出荷時設定へのリセットを実行します。
B. ユーザーがスピアフィッシングメールを開きました :サードパーティのアプリケーションストアを無効にし、実行前にすべての署名済みコードを検証します。
C. 認証されていないファームウェアがインストールされました。OTAアップデートとMDMを介したキャリアローミングを無効にしてください。
D. ユーザーが不適切にエンコードされた緊急ブロードキャストメッセージを受信したため、整合性が失われました。緊急ブロードキャストメッセージを無効にする
正解: **(**正解を表示します**)**

質問: **150**
SaaSプロバイダーは、データストレージをサービスとして提供することを決定しました。簡単にするために、同社はサービスを業界標準のAPIで利用できるようにし、パブリックインターネットでルーティングできるようにしたいと考えています。次のコントロールのうち、会社とその顧客の情報に最も保護を提供するのはどれですか？
A. 詳細なアプリケーションログ
B. 非標準ポートの使用
C. Webアプリケーションファイアウォール

D. 多要素認証
正解: **(**正解を表示します**)**

質問: **151**
インシデント対応の一環として、技術者が侵害されたシステムの画像を取得し、その画像をリモート画像サーバー（192.168.45.82）にコピーしています。システムドライブは非常に大きいですが、機密データは含まれていません。技術者は、このタスクを完了する時間が限られています。技術者が実行するのに最適なコマンドは次のうちどれですか？
A. tar cvf - / | ssh 192.168.45.82 "cat - > /images/image.tar"
B. dd if=/dev/mem | scp - 192.168.45.82:/images/image.dd
C. memdump /dev/sda1 | nc 192.168.45.82 3000
D. dd if=/dev/sda | nc 192.168.45.82 3000
正解: **(**正解を表示します**)**

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **152**
組織は、より良い顧客エンゲージメントとセルフサービスを可能にするためにWebサービスを改善しています。この組織には、ネイティブのモバイルアプリケーションと、第三者によって提供される報酬ポータルがあります。この企業は、一度ログインして各アプリケーション間でSSOを実行する機能を顧客に提供したいと考えています。アイデンティティの整合性は重要であるため、一貫した監査証跡を維持するためにそれをバックエンドシステムに伝播することができます。次の認証および承認の種類のうちどれが要件を満たしていますか？ （2つ選んでください。）
A. Social login
B. SPML
C. OAuth
D. XACML
E. SAML
F. OpenID connect
正解: **A,F (**コメントを発表する**)**

質問: **153**
大規模な公立大学では、最近、ネットワークに接続されたコンピューターに対するランサムウェア攻撃が増加しています。セキュリティエンジニアは、実行中の電子メールに一見無害なファイ

ルを受け取っているさまざまなスタッフメンバーを発見しました。次のうち、この攻撃方法を緩和するものはどれですか？
A. 組織のメールフィルタリングの改善
B. ユーザー認識トレーニングの実施
C. アプリケーションのホワイトリスト登録を有効にする
D. エンドポイントのマルウェア対策ソフトウェアのアップグレード
正解: **B** (コメントを発表する)

質問: **154**
SOCは、最近のインシデントの後、プロセスと手順を検討しています。このレビューでは、感染したホストの検疫が最善の行動であると判断するのに30分以上かかったことが示されています。これにより、マルウェアは封じ込められる前に追加のホストに拡散することができました。インシデント対応プロセスを改善するのに最適なのは次のうちどれですか？
A. 感染したホストの手動検疫の実装
B. ネットワークを信頼できるゾーンと信頼できないゾーンに分割する
C. 利用規定に関する追加のエンドユーザートレーニングを提供する
D. より良い決定ポイントでプレイブックを更新する
正解: (正解を表示します)

質問: **155**
グローバルなサイトを持つ企業は、いくつかの国の武器取引法の下で保護されている機密性の高い情報を処理し交換します。悪意のある国家が後援する活動が、地理的に異なるサイト間の暗号化の使用を標的としているという新しい情報があります。この組織は現在、サイト間のVPNでP-384、SHA-384、およびAES-256-GCMとともにECDSAとECDHを採用しています。次のうちどれが暗号実装を攻撃する企業の回復力を向上させる可能性が最も高いでしょうか。
A. サイト間で異なるベンダからの第二層VPNを追加します。
B. より強力な楕円曲線暗号化アルゴリズムを使用します。
C. 暗号化モジュールを提供しているベンダから暗号化モジュールを最新の状態に保ちます。
D. サイト間の各トンネルの内側（平文と外側（暗号文のセンサーを使用してIDSを実装します。
E. 認証済みのAES動作モードを使用するように暗号スイートをアップグレードします。
正解: (正解を表示します)

質問: **156**
セキュリティエンジニアが内部アプリケーションからの特定のURLをインターネット上で利用できるようにしています開発チームは以下を必要とします
* URLは、内部IPアドレスからのみアクセスできます
*特定の国は制限されています
* TLSが実装されています。

*システムユーザーは、ラウンドロビンで内部アプリケーションサービスに透過的にアクセスして、パフォーマンスを最大化します。セキュリティエンジニアが展開する必要があるのは次のうちどれですか7
A. トラフィックを転送するDNSと特定の外部URLのみが構成されたWAF
B. GeoIP制限と最小負荷検知トラフィック分散を備えたロードバランサー
C. トラフィックの方向付けにDNSを使用するジオフェンシングおよび証明書サービスを備えたアプリケーション対応ファイアウォール
D. IPACL制限と市販のPKI証明書を備えたロードバランサー
正解: **B** (コメントを発表する)

質問: **157**
インシデントレスポンダーは、フォレンジックの目的で実行中のマシンから揮発性メモリを包括的にキャプチャしたいと考えています。マシンは、Linux OSの最新リリースを実行しています。次の技術的アプローチのうち、このキャプチャを達成するための最も実現可能な方法はどれですか？
A. Use a loadable kernel module capture utility, such as LiME.
B. Run dd on/dev/mem.
C. Run the memdump utility with the -k flag.
D. Employ a stand-alone utility, such as FTK Imager.
正解: (正解を表示します)

質問: **158**
脅威アナリストは、HTTPログを調べているときに次のURLに気づきます。

脅威アナリストが目にしている攻撃の種類は次のうちどれですか？
A. SQLインジェクション
B. セッションハイジャック
C. CSRF
D. XSS
正解: **D** (コメントを発表する)

質問: **159**
ある企業が、管理された検出および応答サービスを実行するMSSPにアウトソーシングしています。MSSPでは、サーバーをログ集約としてネットワーク内に配置する必要があり、MSSPアナリストへのリモートアクセスを許可します。重要なデバイスはログをログアグリゲーターに送信し、そこでデータはマルチテナントクラウドにアーカイブされる前にローカルで12か月間保存されます。次に、データはログアグリゲートからMSSPデータセンターのパブリックIPアドレスに送信されて分析されます。
セキュリティエンジニアは、ソリューションのセキュリティを懸念しており、次の点に注意しています。

*重要なデバイスは、クリアテキストログをアグリゲーターに送信します。
*ログアグリゲーターはフルディスク暗号化を利用します。
*ログアグリゲーターはポート80を介して分析サーバーに送信します。
* MSSP分析では、MFAを使用したSSL VPNを利用して、ログアグリゲーターにリモートでアクセスします。
*データは、クラウドで実現される前に圧縮および暗号化されます。
次のうち、エンジニアの最大の関心事はどれですか？
A. 転送中のデータの暗号化
B. ログ集約サーバーによって導入されたハードウェアの脆弱性
C. リモートアクセスVPNからのネットワークブリッジ
D. クラウド内のマルチナンシーとデータの残骸
正解: (正解を表示します)

質問: **160**
サイバーセキュリティアナリストは、ビジネスが改善された電子メールフィルタリングシステムへの支出を正当化できる最大予算額を決定するのに役立つ次の表を作成しました。

Month	Total Emails Received	Total Emails Delivered	Spam Detections	Accounts Compromised	Total Business Loss Account Compromise
January	304	240	62	0	$0
February	375	314	58	1	$1000
March	360	289	69	0	$0
April	281	213	67	1	$1000
May	331	273	56	2	$2000
June	721	598	120	6	$6000

Filter	Yearly Cost	Expected Yearly Spam True Positives	Expected Yearly Account Compromises
ABC	$18,000	930	1
XYZ	$16,000	1200	4
GHI	$22,000	2400	0
TUV	$19,000	2000	2

次のうちどれがビジネスの予算のニーズを満たしていますか？
A. Filter TUV
B. Filter GHI
C. Filter XYZ
D. Filter ABC
正解: (正解を表示します)

質問: **161**
プロジェクトマネージャーは、ソフトウェア開発グループと協力して、組織の内部設計されたデータ分析ツールに関連するユーザーシナリオを収集および評価しています。利害関係者の入力を確認しながら、プロジェクトマネージャーは、さまざまな利害関係者のニーズと、プロジェクトがサポートする組織のコンプライアンス目標を正式に文書化したいと考えています。
次のうちどれを使用するのが最も適切でしょうか？
A. SRTM

B. Roles matrix
C. Peer review
D. BIA
正解: **A** (コメントを発表する)

質問: **162**
ある企業が社外のセキュリティコンサルタントを雇って、企業セキュリティのあらゆる側面について徹底的な見直しを実施しました。同社は特に、物理的なオフィスへの不正アクセスによってネットワークが侵害されることを懸念しています。次のうちどれが潜在的なリスクを評価するためにコンサルタントが実行されるべきですか？
A. 会社は潜在的なインサイダーの脅威を特定するためにアクセスログと従業員のソーシャルメディアフィードの内部監査を実施するべきです
B. コンサルタントはソーシャルエンジニアリングを通して物理的なオフィスへのアクセスを得ようとし、次にデータの漏洩を試みるべきです。
C. コンサルタントは、ログを見直し、脅威の可能性を評価するために、すべての物理的アクセス制御システムへのアクセスを許可されるべきです。
D. 会社は、物理的なオフィスへの不正アクセスを検出するために一時的なCCTVシステムをインストールする必要があります
正解: (正解を表示します)

質問: **163**
これまで、A社のリスク委員会は、最低限のリスク許容量でさえも嫌悪感を示していました。セキュリティエンジニアが、レガシーICS機器の導入を提案するリスクについての推奨事項を作成しています。このプロジェクトは企業に小さな脆弱性を導入するでしょう。この脆弱性によって企業がリスクにさらされることはそれほど多くなく、それに対して費用がかかる可能性があります。
次の戦略のうちどれが最初に承認されるべきですか？
A. 避ける
B. 転送する
C. 同意する
D. 軽減する
正解: **D** (コメントを発表する)

質問: **164**
新しいシステムの展開中に、実装チームは、新しいシステムをレガシシステムと統合するために使用されるAPIが正しく機能していないと判断します。さらに調査すると、システム間のデータ転送を保護するために使用されている暗号化アルゴリズムの設定が誤っていることがわかります。使用中の定義済みアルゴリズムのソースを特定するためにプロジェクトマネージャが使用するべきものはどれですか。
A. コードリポジトリ

B. セキュリティ要件のトレーサビリティマトリックス
C. ソフトウェア開発ライフサイクル
D. 実施ガイド
E. ロールマトリックス
F. データ設計図
正解: **(**正解を表示します**)**

質問: **165**
医用画像会社のシステム管理者は、汎用ファイルサーバーで保護された健康情報（PHI）を発見します。管理者は次のどの手順を実行する必要がありますか？
A. 法務部門に相談して、法的要件を決定してください。
B. 法務部門に相談するまで、ネットワークからすべてのPHIを削除します。
C. サーバーのMD5ハッシュを取得します。
D. すべてのPHIを独自のVLANで分離し、レイヤー2で分離したままにします。
正解: **(**正解を表示します**)**

質問: **166**
ビジネスは成長し、他の場所に分岐し始めています。別の国にオフィスを開くことを見越して、最高情報セキュリティ責任者（CISO）と法務チームは、新しいオフィスを開くためのデータに関して次の基準を満たす必要があることに同意します。
* 5年間の店舗課税関連文書
* 顧客の住所を暗号化形式で保存する
* 1年後に顧客情報を破棄する
* 顧客の本国のみでデータを保管する
CISOは、これらの要件を最もよく満たすために次のうちどれを実装すべきですか。
（3つ選んでください。）
A. バックアップポリシー
B. キャパシティプランニング方針
C. 暗号化規格
D. データ主権政策
E. 法令順守ポリシー
F. データ保持方針
G. データ分類基準
H. 利用規定
正解: **C,F,G (**コメントを発表する**)**

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試

験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **167**
ある会社のエンジニアは、特定の種類のデータを競合他社から保護する必要があると考えていますが、データの所有者はその情報は機密ではないと主張しています。情報セキュリティエンジニアが、企業のSANを保護するための管理策を実施しています。規制では、データを4つのグループに分類する必要があります。機密ではないが機密であるがアクセス可能である、機密であるが輸出規制、および極めて機密です。エンジニアは、データに関して次のどのアクションを実行する必要がありますか。
A. データに機密性はあるがエクスポート制御されているというラベルを付けます。
B. データに機密性のないラベルを付けます。
C. 機密性が高いがアクセス可能なデータにラベルを付けます。
D. データに機密性の高いラベルを付けます。
正解: **(**正解を表示します**)**

質問: **168**
ソフトウェア開発チームは、過去18か月間に、クライアントが製造を進めながら注文のステータスを確認できるようにする、新しいWebベースのフロントエンドの開発に費やしました。マーケティングチームは、2週間以内に新しいアプリケーションをクライアントに提示するための打ち上げパーティーを計画します。発売前に、セキュリティチームは危険な脆弱性を導入する可能性がある多数の欠陥を発見し、製造業で使用されるデータベースへの直接アクセスを可能にしました。開発チームは開発中にこれらの脆弱性を修正する計画はありませんでした。次のSDLCベストプラクティスのうち、開発チームが従うべきものはどれですか。
A. SRTMを使う
B. ユーザー受け入れテストを完了する
C. 回帰テストを実施する
D. システム設計文書の確認
正解: **(**正解を表示します**)**

質問: **169**
企業は、証明書認証用にSSLクライアントベースのVPNを構成しています。CAからの信頼されたルート証明書がファイアウォールにインポートされ、ファイアウォールのVPN構成が証明書認証用に構成されます。信頼できるCAからの署名付き証明書は、ユーザーデバイスに配布されます。CA証明書はエンドユーザーデバイスで信頼できるものとして設定され、VPNクライアントはエンドユーザーデバイスで構成されますエンドユーザーが接続しようとすると、ファイアウォールは短時間後に接続を拒否します。次のうちどれですか。ファイアウォールが接続を拒否する最も可能性の高い理由は何ですか？

A. ルーターでは、IPSecトラフィックをブリッジモードで許可する必要があります
B. ファイアウォールで、互換性のある暗号スイートを有効にする必要があります
C. CA内。SANフィールドをルートCA証明書に設定してから、再発行する必要があります
D. VPNクライアントでは、CARCLアドレスを手動で指定する必要があります
正解: **(**正解を表示します**)**

質問: **170**
セキュリティ評価中、アクティビティは2つのフェーズに分けられました。内部および外部の搾取セキュリティ評価チームは、企業の境界内の危険にさらされているボックスに移動する前に、外部の活動に厳しい時間制限を設定しました。
次の方法のうちどれがNEXTを採用する可能性が最も高い評価チームですか？
A. ソーシャルメディアの偵察の前兆として、侵入したボックスからネットワークをスキャンする
B. 侵入先からのピボット操作、企業内の横方向への移動、およびデータの漏洩とデバイスの侵害を試みる。
C. システムのさらなる侵害を可能にするためにネットワークの境界と範囲を特定するためのオープンソースのインテリジェンス収集。
D. 侵入先のボックスに物理的にアクセスすることを目的としてソーシャルエンジニアリング攻撃を試みる。
正解: **B (**コメントを発表する**)**

質問: **171**
組織は、クラウドでホストされた環境に移行するにつれて、シンクライアントアーキテクチャの使用を検討しています。セキュリティアナリストは、シンクライアントと仮想ワークステーションを使用することのセキュリティ上の利点について意見を述べるよう求められます。シンクライアントと仮想ワークステーションのこの組み合わせを使用することによるセキュリティ上の利点はどれですか。
A. シンクライアントのワークステーションは、簡単に侵害される可能性のあるストレージと周辺機器がないため、セキュリティの必要性ははるかに少なく、仮想ワークステーションはセキュリティが外部委託されているクラウドで保護されています。
B. 悪意のあるユーザーは、自分の物理的なシンクライアントワークステーションからデータを抽出する機会を減らすことになり、これによりローカル攻撃の有効性が低下します。
C. 悪意のある内部関係者は、保存されているデータを改ざんしてシステムの完全性に影響を与えることはありません。
D. すべてのシンクライアントはコア保護にTPMを使用し、仮想ワークステーションはコア保護にvTPMを使用し、どちらもクラウドホスト環境のセキュリティ上の優位性を高めます。
正解: **(**正解を表示します**)**

質問: **172**
経営陣は、組織の方針および手順に関する最近のリスク評価の結果を検討しています。リスク評価中に、バックグラウンドチェックに関連する手順が効果的に実施されていないと判断されま

す。このリスクに対応して、組織はバックグラウンドチェックに関連するポリシーと手順を改訂し、サードパーティを使用してすべての新入社員に対してバックグラウンドチェックを実行することを選択します。組織は次のどのリスク管理戦略を採用していますか？
A. 拒否
B. 避ける
C. 転送
D. 軽減する
E. 同意する
正解: **(**正解を表示します**)**

質問: **173**
セキュリティアナリストは、今後の侵入テストの準備のために会社についてオンライン調査を行っているときに、会社が公開していない投資家のウェブサイトで詳細な財務情報を発見します。アナリストはこの情報を最高財務責任者 (CFO) と共有し、最高財務責任者 (CFO) は、情報が正確であることを確認します。これは最近、取締役会で議論されました。詳細の多くは、モバイルデバイスでの転記を目的として、ボードの秘書が記録した逐語的なディスカッションコメントです。
将来、MOSTが同様の違反を防ぐ可能性が高いのは次のうちどれですか？
A. eFuse
B. VPN
C. Remote wipe
D. FDE
E. Geolocation
正解: **(**正解を表示します**)**

質問: **174**
組織の継続的な脆弱性評価プログラムの一環として、最高情報セキュリティ責任者 (CISO) は、さまざまな脅威について組織のシステム、人員、および施設を評価したいと考えています。評価の一環として、CISOは、独立したサイバーセキュリティ評価会社と協力してソーシャルを実行することを計画しています。組織の企業オフィスおよび遠隔地に対するエンジニアリングおよび物理的侵入テスト。
次の手法のうち、この評価の一部として最も採用される可能性が高いのはどれですか？ (3つ選択してください)。
A. 脆弱性スキャン
B. バッジスキミング
C. SQLインジェクション
D. TOC / TOUの活用
E. ビッシング
F. 特権の昇格
G. 不正APの置換
H. 共連れ

正解: **B,E,H** (コメントを発表する)

質問: **175**
セキュリティマネージャは、生産性への影響を最小限に抑えて従業員の活動を監視する機能を備えた管理を行うポリシーを実装したいと考えています。このシナリオに最適なポリシーは次のうちどれですか？
A. 必須の休暇
B. インシデント対応
C. 最小特権
D. 職務の分離
正解: (正解を表示します)

質問: **176**
大量のPIIを処理する組織では、PIIおよびその他の機密データを処理、保存、および送信できるモバイルデバイスを従業員に発行できます。セキュリティアセスメント担当者は、MDMがワイプコマンドを正常に発行した後に、デバイスストレージからの残りの機密データの回復と復号化を実演できます。
コントロールが利用可能であると仮定した場合、次のうちどれが将来の機密データの損失から保護するのが最もよいでしょうか。
A. 保存されている機密データの認証に、より強力なアルゴリズムを採用しているデバイスを発行する。
B. リモートワイプ中に吹き飛ばされるeFユースバックメモリスペースに保存されている機密データに暗号化キーを使用する。
C. PIIデータをラップし、キー情報をコンテナの暗号化されたアプリケーションスペースに直接格納するコンテナを実装します。
D. MDMによって発行されたリモートワイプコマンドを受信したときにブートローダバイナリを削除するデバイスを入手する。
正解: **C** (コメントを発表する)

質問: **177**
セキュリティマネージャが最近情報システムを分類しました。分類作業中に、マネージャは特定の情報タイプの整合性の喪失がビジネスに重大な影響を及ぼすと判断しました。これに基づいて、セキュリティマネージャはいくつかのソリューションの実装を推奨します。次のうちどれを組み合わせれば、このリスクを最も軽減できるでしょうか。 2を選択）
A. ブート認証
B. アクセス制御
C. 署名する
D. 検証
E. ホワイトリスト
正解: (正解を表示します)

質問: **178**
プロジェクトマネージャは、ソフトウェア開発グループと協力して、組織の内部で設計されたCRMツールに関連するユーザーストーリーを収集し評価します。要件を定義した後、プロジェクトマネージャは開発者の解釈とユーザーの要求の理解を検証したいと思います。次のうちどれがこの目的をサポートしますか？
A. ユーザー受け入れテスト
B. スクラム
C. ピアレビュー
D. 単体テスト
E. デザインレビュー
正解: **B** (コメントを発表する)

質問: **179**
セキュリティ管理者は、多層化され、多くのセキュリティテクノロジーを単一のプラットフォームに組み込むことができるNIPSを立ち上げたいと考えています。製品には、ウイルス対策、VPN、ファイアウォールサービスなどのさまざまな機能があり、タイムリーに更新できる必要があります。進化する脅威に対応します。要件を満たすために使用できるネットワーク防止システムの種類は次のうちどれですか？
A. エンタープライズファイアウォール
B. 統合脅威管理
C. アプリケーションファイアウォール
D. コンテンツベースのIPS
正解: **C** (コメントを発表する)

質問: **180**
銀行は、別の小さな銀行を取得するプロセスを開始しています。組織間で交渉が行われる前に、プロセスの最初のステップとして使用されるビジネスドキュメントは次のうちどれですか。
A. NDA
B. OLA
C. BPA
D. 覚書
正解: **A** (コメントを発表する)

質問: **181**
セキュリティ管理者は、従業員が個人用デバイスを企業ネットワークに接続することを懸念しています。そうすることは会社の方針に反します。ネットワークにはNACソリューションがありません。会社は、内部ネットワークに接続されているすべての会社所有デバイスのファイアウォールを無効にするGPOを使用しています。さらに、すべての会社所有デバイスは、デバイスのシリアル番号を使用する標準の命名規則を実装しています。セキュリティ管理者は、アクティブな個人

用デバイスを識別し、それらをネットワークから切断するためのカスタムスクリプトを記述したいのですが、このタスクを使用して、このタスクを最適に実行するにはどうすればよいですか。
A. AD認証ログ
B. 再帰的なDNSログ
C. DHCPログ
D. RADIUSログ
E. スイッチとルーターのARPテーブル
正解: (正解を表示します)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **182**
金融機関の情報セキュリティ担当者は、リスク管理担当者と協力して、すべてのセキュリティ管理が実施された後の金融機関の残存リスクの対処方法を決定しています。機関の非常に低いリスク許容度を考慮して、次の戦略のうちどれがベストでしょうか？
A. Transfer the risk.
B. Accept the risk.
C. Avoid the risk
D. Mitigate the risk.
正解: (正解を表示します)

質問: **183**
ヘルスケア企業は、サードパーティの研究者が有料でデータを利用できるようにすることで、患者に関して収集するデータの価値を高めたいと考えています。企業へのリスクを軽減するのに最適なものは次のうちどれですか。
A. レコード内の日付とタイムスタンプの情報をサニタイズします。
B. 研究者への転送中にすべてのデータが暗号化されていることを確認します
C. すべての研究者が秘密保持契約に署名して遵守するようにします
D. データへのすべてのアクセスをログに記録し、研究者と関連付けます
E. キー付き文字列を使用して識別可能な情報を匿名化します
正解: (正解を表示します)

質問: **184**

セキュリティアナリストは、サードパーティの侵入テスターによって最近実施されたエクスプロイトの成功の結果を読んでいます。テスターは、特権実行可能ファイルをリバースエンジニアリングしました。レポートでは、エクスプロイトの計画と実行がログとテストからの出力を使用して詳細に説明されています。ただし、エクスプロイトの攻撃ベクトルが欠落しているため、修復を推奨することは困難です。次の出力が与えられます：



浸透テスターは、おそらく以下を利用しました。

A. 整数オーバーフローの脆弱性

B. プレーンテキストのパスワード開示

C. バッファオーバーフローの脆弱性

D. TOC / TOUの脆弱性

正解: **D** (コメントを発表する)

質問: **185**

最高情報セキュリティ責任者（CISO）は最近、仕事を新しい業界に変えました。CISOの最初のタスクは、組織に関連する新しいリスク評価を作成することです。CISOが組織に関連するリスクを見つけるのに役立つのは、次のうちどれですか？（2つ選択してください。）

A. Conduct a regulatory audit.

B. Perform a penetration test.

C. Review the existing BIA.

D. Define the threat model.

E. Hire a third-party consultant.

F. Perform an attack path analysis.

正解: (正解を表示します)

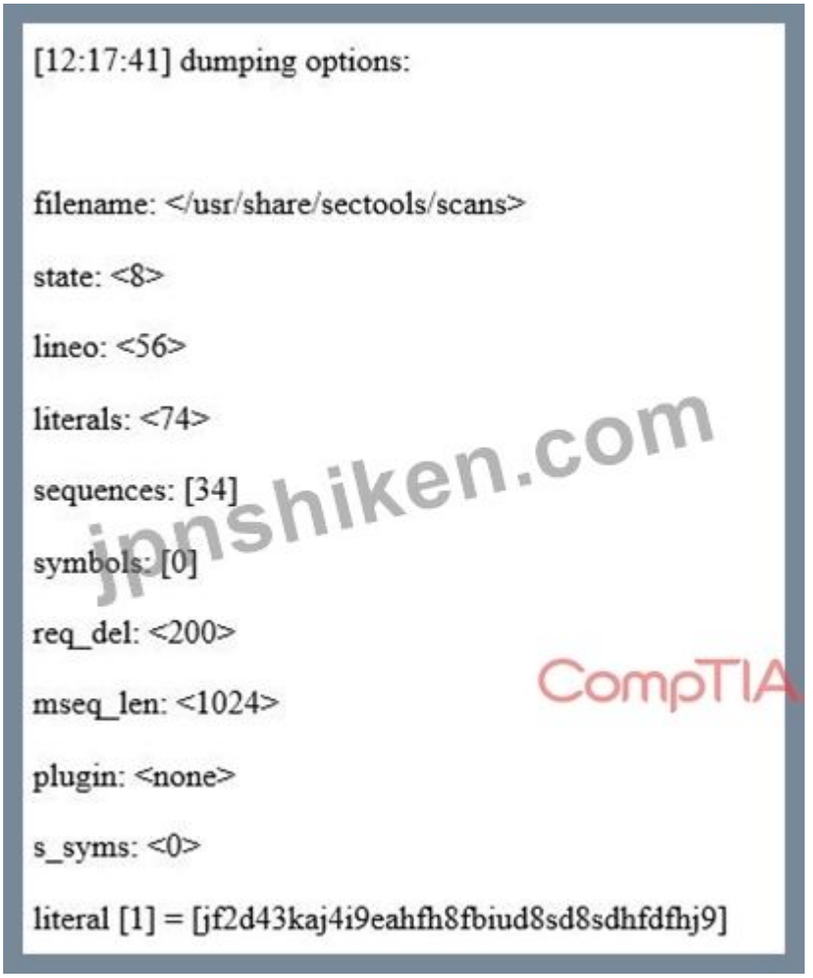
質問: **186**

コアルーターは、資格のあるバイパスによって操作され、すべてのネットワークトラフィックを、WiFiによってネットワークに接続された許可されていないユーザーの制御下でセカンダリルーターを介して送信します。

次のうち、この攻撃タイプが発生するリスクを減らすのに最適なものはどれですか？

A. 802.1XをWiFiインフラストラクチャのNACシステムとして展開します。
B. 帯域外チャネル経由でのみコアルーター管理インターフェイスへのアクセスを許可します。
C. コアルーターにアクセスできるユーザーアカウントに強力で複雑なパスワードポリシーを実装します。
D. コアルーターに接続されているスイッチング環境用のポートセキュリティ設定を追加します。
正解: **(**正解を表示します**)**

質問: **187**
Kaliのセキュリティツールからの次の出力があるとします。



jpnshiken.com
CompTIA

A. ネットワーク列挙子
B. SCAPスキャナー
C. ログ削減
D. ファザー
正解: **B (**コメントを発表する**)**

質問: **188**
セキュリティー管理者が、機密データを処理するTrustedSolarisサーバーを強化しています。データ所有者は次のセキュリティ要件を設定しました。
* データは内的な消費のためのものであり、外部の個人に配布することはできません
* システム管理者は、サーバーによって処理されたデータにアクセスできません。

* カーネルイメージの整合性が維持されている
次のホストベースのセキュリティコントロールのうちどれがデータ所有者の要件を最も強く強制しますか？ 3つ選んでください。）
A. DLP
B. データ暗号化
C. ホストベースのファイアウォール
D. HIDS
E. 測定ブーツ
F. 透かし
G. SELinux
正解: **(**正解を表示します**)**

質問: **189**
APIエンドポイントを使用した一連のWebサービスを対象にした侵入テストが行われています。APIは既存のWebアプリケーションサーバーでホストされます。新しいAPIの中には、認証されていないユーザーが利用できるものもありますが、認証されたユーザーだけが利用できるものもあります。以下のツールやアクティビティのうちどれが、侵入テスト担当者がエンゲージメント中に使用または使用する可能性が最も高いのでしょうか。 2つを選択する）
A. 代行受信プロキシ
B. リバースエンジニアリング
C. 静的コードアナライザ
D. ユーザー受け入れテスト
E. ポートスキャナー
F. 偵察会
正解: **A,F (**コメントを発表する**)**

質問: **190**
グローバルメーカーの運用プロセスの効率を高めるために、内部アプリケーションが開発されました。セキュリティバグを修正するために新しいコードが実装されましたが、操作が停止しました。経営陣は、セキュリティバグを修正することは、運用を継続することほど重要ではないと判断しました。
次のうち、失敗した修正の即時ロールバックをサポートするのはどれですか？ 2つ選択してください。）
A. バージョン管理
B. アジャイル開発
C. 継続的インテグレーション
D. 変更管理
E. ウォーターフォール開発
正解: **D (**コメントを発表する**)**

質問: **191**
セキュリティエンジニアは、既知のインシデントに続いてDNSサーバーを調べています。エンジニアは、次のコマンドをサーバーのシェル履歴の最新のエントリと見なします。
dd if=dev/sda of=/dev/sdb
次のうち、最も発生した可能性が高いのはどれですか？
A. サーバーのテープバックアップが実行されました。
B. DNSログファイルは期待どおりに毎日ロールされました
C. ハードドライブはインシデント後にフォーマットされました。
D. ドライブはフォレンジック分析のために複製されました。
正解: (正解を表示します)

質問: **192**
アナリストは、名前文字列に基づいて、アプリケーションのホワイトリスト登録が有効になっている、企業が所有し企業が管理するモバイルデバイスの動作を調査しています。デバイスが割り当てられている従業員は、承認された電子メールクライアントがブラウザーウィンドウを起動できる警告メッセージを表示しており、認識されていない電子メールアドレスを「作成」ウィンドウに追加していると報告します。
次のうち、アナリストが悪意のある動作を理解し、特徴付ける最良の機会を提供するのはどれですか？
A. ソースコードで静的コード分析を実行します。
B. モバイルアプリケーションの侵入テスト。
C. JTAGインターフェイスを介してデバイスファームウェアを分析します。
D. 暗号化ハッシュを使用するホワイトリストに変更します。
E. アプリケーションバイナリをリバースエンジニアリングします。
正解: (正解を表示します)

質問: **193**
地域ビジネスは来週深刻な冬の嵐を予想している。ITスタッフは、さまざまな状況への対処方法に関する企業ポリシーを検討していますが、見逃しているものや不完全なものもあります。このドキュメントのギャップを情報セキュリティマネージャに報告した後、すぐに文書が作成され、運用のダウンタイムを回避するためにさまざまな担当者が他の場所に移動します。これは次の例です。
A. リスク回避計画
B. 事件対応計画
C. 災害復旧計画
D. 事業継続計画
正解: (正解を表示します)

有効的な**CAS-003J**問題集はJPNTest.com提供され、**CAS-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-003J**試験問題集を提供します。JPNTest.com CAS-003J試験問題集はもう更新されました。ここで**CAS-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-003J-mondaishu **683**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」