【応用_午前_過去問】セキュリティ③

☆☆☆

IoTデバイスの耐タンパ性の実装技術とその効果に関する記述として，適切なものはどれか。

令和3年秋期　問40
101問目／選択範囲の問題数237問

ア　CPU処理の負荷が小さい暗号化方式を実装することによって，IoTデバイスとサーバとの間の通信経路での情報の漏えいを防止できる。

イ　IoTデバイスにGPSを組み込むことによって，紛失時にIoTデバイスの位置を検知して捜索できる。

ウ　IoTデバイスに光を検知する回路を組み込むことによって，ケースが開けられたときに内蔵メモリに記録されている秘密情報を消去できる。

エ　IoTデバイスにメモリカードリーダーを実装して，IoTデバイスの故障時にはメモリカードをIoTデバイスの予備機に差し替えることによって，IoTデバイスを復旧できる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ウ　“あなたの解答：エ”

❑解説

耐タンパ性とは、ハードウェアやソフトウェアのセキュリティレベルを表す指標で、外部からの物理的接触により機器内部の構造を不当に解析・改変したり、重要データを取り出そうとしたりする行為に対してどの程度の耐性を有するかを表します。タンパー（tamper）には「変更する」「改ざんする」「弄る」などの意味があります。

IoTデバイスの耐タンパ性は、機器内部の機密データの守秘性を高める、内部動作の解析を困難にする、分解すると壊れるようにすることで向上しますから、ケースを空けたときに秘密情報を消去する機構である「ウ」が適切となります。

ちなみに、IoTセキュリティガイドライン(ver1.0)では、耐タンパ性を高める対策例として以下を挙げています。

ハードウェアや構造設計による対策

- 機器を分解すると配線が切断されたり、インタフェースが破壊されたりすることで解析を妨げる設計
- 不要な非正規I/Fや露出した配線の除去
- 専用認証デバイスを接続しないと内部にアクセスできない設計
- 漏えい電磁波から内部処理を推定させないための電磁シールド
- チップや配線の内装化

データやソフトウェア設計による対策

- 盗難、紛失時に遠隔から端末をロックする機能の実装
- ソフトウェアの難読化、暗号化
- 機密データの暗号化、使用時のメモリなど在中時間の短縮
- 実行時のメモリ上でのプログラムやデータの改ざんの防止

☆☆

情報セキュリティ基本方針文書の取り扱いについて，ISMS認証基準に定められているものはどれか。

平成18年春期　問76
102問目／選択範囲の問題数237問

ア　一度決めた内容を変更せず，セキュリティ事故発生時に見直す。

イ　機密情報であるので関連する管理者だけに内容を教育する。

ウ　経営陣によって承認され，全従業員に公表し通知する。

エ　作成したメンバー自身で実施状況を点検する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ウ　“あなたの解答：ウ”

❑解説

情報セキュリティ基本方針は、組織の情報セキュリティマネジメントに対する基本的な考え方を示した文書です。
それぞれの記述をJIS Q 27001の規格に照らすと次のようになります。

ア “一度決めた内容を変更せず，セキュリティ事故発生時に見直す。”

内外の環境の変化を踏まえて定期的にレビューすることが要求されているため不適切です。

イ “機密情報であるので関連する管理者だけに内容を教育する。”

「組織は、ISMSに定義された責任を割り当てた要員すべてが、要求された職務を実施する力量をもつことを(教育・訓練などによって)確実にしなければならない」と定められているため不適切です。

ウ “経営陣によって承認され，全従業員に公表し通知する。”

正しい。ISMS認証基準では、経営陣の責任としてISMSの確立．導入，運用及び維持等に関与し、組織として情報セキュリティの実施責任を利害関係者に宣言(コミットメント)することを要求しています。

エ “作成したメンバー自身で実施状況を点検する。”

監査プロセスの客観性及び公平性を確実にするため「監査員は、自らの仕事を監査してはならない」と定められているため不適切です。

☆

暗号方式に関する説明のうち，適切なものはどれか。

平成29年春期　問38
103問目／選択範囲の問題数237問

ア　共通鍵暗号方式で相手ごとに秘密の通信をする場合，通信相手が多くなるに従って，鍵管理の手間が増える。

イ　共通鍵暗号方式を用いて通信を暗号化するときには，送信者と受信者で異なる鍵を用いるが，通信相手にその鍵を知らせる必要はない。

ウ　公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには，復号鍵を公開することによって，鍵管理の手間を減らす。

エ　公開鍵暗号方式では，署名に用いる鍵を公開しておく必要がある。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：エ”

❑解説

ア “共通鍵暗号方式で相手ごとに秘密の通信をする場合，通信相手が多くなるに従って，鍵管理の手間が増える。”

正しい。共通鍵暗号方式では通信の組合せの数だけ異なる鍵が必要になります。n人と暗号化通信を行う場合には、それぞれの相手と鍵を安全に共有し、n個の鍵を厳重に管理しなくてはなりません。

イ “共通鍵暗号方式を用いて通信を暗号化するときには，送信者と受信者で異なる鍵を用いるが，通信相手にその鍵を知らせる必要はない。”

共通鍵暗号方式における暗号化通信では暗号化と復号に同じ鍵を使用します。また、暗号化通信を行う前に通信当事者同士で安全に鍵を共有しておく必要があります。

ウ “公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには，復号鍵を公開することによって，鍵管理の手間を減らす。”

公開鍵暗号方式で暗号化通信を行う場合は、送信者が受信者の公開鍵でデータを暗号化し、受信者は自身の秘密鍵でデータを復号します。受信者は復号鍵を秘匿にし、暗号化鍵を公開しておきます。

エ “公開鍵暗号方式では，署名に用いる鍵を公開しておく必要がある。”

デジタル署名では、送信者が自身の秘密鍵で署名を生成し、受信者は送信者の公開鍵を用いて署名を検証します。署名に用いる鍵は秘密鍵ですので公開してはいけません。

☆☆

通信を要求したPCに対し，ARPの仕組みを利用して実現できる通信可否の判定方法のうち，最も適切なものはどれか。

平成26年秋期　問42
104問目／選択範囲の問題数237問

ア　PCにインストールされているソフトウェアを確認し，事前に許可されているソフトウェア以外がインストールされていない場合だけ通信を許可する。

イ　PCのMACアドレスを確認し，事前に登録されているMACアドレスである場合だけ通信を許可する。

ウ　PCのOSのパッチ適用状況を確認し，最新のパッチが適用されている場合だけ通信を許可する。

エ　PCのマルウェア対策ソフトの定義ファイルを確認し，最新になっている場合だけ通信を許可する。

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

イ　“あなたの解答：イ”

❑解説

ARP(Address Resolution Protocol)は、IPアドレスから対応する機器のMACアドレスを取得するプロトコルです。
無線LANルータなどでは、あらかじめMACアドレスを登録しておいた機器からのみの接続を許可する**MACアドレスフィルタリング**の機能を備えています。無線LANルータ側では接続を要求するPCのIPアドレスからARPを用いることで対応するMACアドレスを取得し、それを登録済みMACアドレスと比較することで正規の利用者以外からの接続を防止しています。

したがって適切な方法は「イ」です。

☆☆☆

DNSSECについての記述のうち，適切なものはどれか。

令和5年秋期　問45
105問目／選択範囲の問題数237問

ア　DNSサーバへの問合せ時の送信元ポート番号をランダムに選択することによって，DNS問合せへの不正な応答を防止する。

イ　DNSの再帰的な問合せの送信元として許可するクライアントを制限することによって，DNSを悪用したDoS攻撃を防止する。

ウ　共通鍵暗号方式によるメッセージ認証を用いることによって，正当なDNSサーバからの応答であることをクライアントが検証できる。

エ　公開鍵暗号方式によるデジタル署名を用いることによって，正当なDNSサーバからの応答であることをクライアントが検証できる。

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

エ　“あなたの解答：エ”

❑解説

DNSSEC(DNS Security Extensions)は、DNSにおける応答の正当性を保証するための拡張仕様です。DNSSECでは名前解決の応答パケットに**デジタル署名**を付加することで、正当な管理者によって生成された応答レコードであること、また応答レコードが改ざんされていないことの検証が可能になります。

DNSキャッシュポイズニング攻撃では、攻撃者が偽の応答パケットをキャッシュサーバに送り込み、それをキャッシュサーバが登録してしまうことによって攻撃が成立するので、DNSSECの導入はDNSキャッシュポイズニング攻撃への有効な対策となります。しかし、各DNSサーバのDNSSEC対応、電子署名に必要な鍵の管理や配布方法の確立、ルートやTLDの署名が必要なことなど、さまざまな課題があり、普及に当たっては今しばらく時間が必要です。

したがって適切な記述は「エ」です。

ア “DNSサーバへの問合せ時の送信元ポート番号をランダムに選択することによって，DNS問合せへの不正な応答を防止する。”

ソースポートランダマイゼーションの説明です。

イ “DNSの再帰的な問合せの送信元として許可するクライアントを制限することによって，DNSを悪用したDoS攻撃を防止する。”

DoS攻撃やキャッシュポイズニング攻撃を防止するための対策です。

ウ “共通鍵暗号方式によるメッセージ認証を用いることによって，正当なDNSサーバからの応答であることをクライアントが検証できる。”

メッセージ認証では通信相手の正当性を確認できません。

エ “公開鍵暗号方式によるデジタル署名を用いることによって，正当なDNSサーバからの応答であることをクライアントが検証できる。”

正しい。DNSSECの説明です。

☆

ゼロデイ攻撃の特徴はどれか。

平成27年秋期　問42
106問目／選択範囲の問題数237問

ア　セキュリティパッチが提供される前にパッチが対象とする脆弱性を攻撃する。

イ　特定のWebサイトに対し，日時を決めて，複数台のPCから同時に攻撃する。

ウ　特定のターゲットに対し，フィッシングメールを送信して不正サイトへ誘導する。

エ　不正中継が可能なメールサーバを見つけた後，それを踏み台にチェーンメールを大量に送信する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

ゼロデイ攻撃（zero-day attack）とは、あるOSやソフトウェアに脆弱性が存在することが判明し、ソフトウェアの修正プログラムがベンダーから提供されるより前に、その脆弱性を悪用して行われる攻撃のことを指します。

問題解決のための修正パッチが提供された日を1日目としたとき、それよりも前に行われた攻撃という意味で「ゼロデイ攻撃」と呼ばれます。

ア “セキュリティパッチが提供される前にパッチが対象とする脆弱性を攻撃する。”

正しい。ゼロデイ攻撃の特徴です。

イ “特定のWebサイトに対し，日時を決めて，複数台のPCから同時に攻撃する。”

DDoS攻撃の特徴です。

ウ “特定のターゲットに対し，フィッシングメールを送信して不正サイトへ誘導する。”

フィッシングの特徴です。

エ “不正中継が可能なメールサーバを見つけた後，それを踏み台にチェーンメールを大量に送信する。”

スパムメール送信行為の特徴です。外部からの不正中継を許可しているSMTPサーバはスパムメールの踏み台にされてしまいます。

☆☆☆

リスクマネジメントの実施内容を説明したものはどれか。

平成17年秋期　問78
107問目／選択範囲の問題数237問

ア　将来の損失発生の危険性は不確実なものであり，対策費の予算ではなく損失額を見積もる。

イ　投機的リスクとは経営主体の管理外で発生するリスクなので，内在するリスクは管理対象外とする。

ウ　リスクファイナンスでは，リスク分析，リスクコントロールなどのリスクマネジメントにかかる一切の費用の手当をする。

エ　リスク分析では純粋リスクにとどめず，投機的リスクも対象にする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

エ　“あなたの解答：ウ”

❑解説

ア “将来の損失発生の危険性は不確実なものであり，対策費の予算ではなく損失額を見積もる。”

リスクへの対応方法を判断するための情報として損失額、対策費の両方を見積もる必要があります。

イ “投機的リスクとは経営主体の管理外で発生するリスクなので，内在するリスクは管理対象外とする。”

リスクマネジメントではその特質に関わらずあらゆる種類のリスクを管理対象とします。

ウ “リスクファイナンスでは，リスク分析，リスクコントロールなどのリスクマネジメントにかかる一切の費用の手当をする。”

リスクファイナンスでは、リスクが顕在化したときの損失額や回復費用を他者に負担させます。

エ “リスク分析では純粋リスクにとどめず，投機的リスクも対象にする。”

正しい。情報セキュリティのためのリスク分析では純粋リスクのみを対象としますが、経営主体の立場で行うリスク分析では投機的リスクも対象にします。

☆☆

サーバにバックドアを作り，サーバ内で侵入の痕跡を隠蔽するなどの機能がパッケージ化された不正なプログラムやツールはどれか。

平成27年春期　問43
108問目／選択範囲の問題数237問

ア	RFID	イ	rootkit	ウ	TKIP	エ	web beacon

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：イ”

❑解説

ルートキット(rootkit)は、攻撃者がシステムへ不正侵入した後に侵入した痕跡を隠蔽したり、再び侵入するためのバックドアを設置するための機能をまとめたソフトウェア群です。ルートキットにはキーロガー、パスワード窃盗ツール、クレジットカードやオンラインバンキングの情報を盗むモジュール、DDoS攻撃用のボット、セキュリティソフトウェアを無効にする機能など、多数の悪意あるツールが含まれている可能性があります。

したがって「イ」が正解です。

ア “RFID”

RFID(Radio Frequency IDentification)は、ID情報を埋め込んだRFタグ(ICタグ)から電磁界や電波を用いて情報のやり取りを行う技術でICカードなどで使用されています。

イ “rootkit”

正しい。

ウ “TKIP”

Temporal Key Integrity Protocolの略。無線ネットワーク規格で使われているセキュリティプロトコルです。使用する鍵を一定時間ごとに更新することで暗号解読に対する耐性を高めた方式です。

エ “web beacon”

web beacon(Webビーコン)は、Webページに埋め込んだ見えないほどの小さな画像のことで、ユーザーの利用環境や滞在時間・ページ遷移などの情報を得たりするために設置されます。その情報の多くはアクセス解析などのために使用されています。

☆

JIS Q 31000:2010(リスクマネジメント－原則及び指針)における，残留リスクの定義はどれか。

平成27年春期　問41
109問目／選択範囲の問題数237問

ア	監査手続を実施しても監査人が重要な不備を発見できないリスク
イ	業務の性質や本来有する特性から生じるリスク
ウ	利益を生む可能性に内在する損失発生の可能性として存在するリスク
エ	リスク対応後に残るリスク

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

エ　“あなたの解答：エ”

❑解説

JIS Q 31000:2010は、リスクマネジメントに関する原則及び一般的な指針を示すJIS規格です。この中で残留リスクは次のように定義されています。

「リスク対応後に残るリスク」
注記1 残留リスクには、特定されていないリスクが含まれることがある。
注記2 残留リスクは、"保有リスク"としても知られている。

したがって「エ」が正解です。

ア “監査手続を実施しても監査人が重要な不備を発見できないリスク”

発見リスクの説明です。

イ “業務の性質や本来有する特性から生じるリスク”

固有リスクの説明です。

ウ “利益を生む可能性に内在する損失発生の可能性として存在するリスク”

投機リスクの説明です。

エ “リスク対応後に残るリスク”

正しい。残留リスク(保有リスク)の説明です。

☆☆☆☆

オープンリゾルバを悪用した攻撃はどれか。

令和4年秋期　問36
110問目／選択範囲の問題数237問

ア　ICMPパケットの送信元を偽装し，多数の宛先に送ることによって，攻撃対象のコンピュータに大量の偽のICMPパケットの応答を送る。

イ　PC内のhostsファイルにある，ドメインとIPアドレスとの対応付けを大量に書き換え，偽のWebサイトに誘導し，大量のコンテンツをダウンロードさせる。

ウ　送信元IPアドレスを偽装したDNS問合せを多数のDNSサーバに送ることによって，攻撃対象のコンピュータに大量の応答を送る。

エ　誰でも電子メールの送信ができるメールサーバを踏み台にして，電子メールの送信元アドレスを詐称したなりすましメールを大量に送信する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：エ”

❑解説

リゾルバ(resolver)は、利用者からの名前解決要求に対してネームサーバに問い合わせをし、結果をクライアントに返すソフトウェアです。オープンリゾルバとは、インターネット上で公開状態になっているリゾルバ、つまり外部の不特定多数からの問い合わせに対しても名前解決を処理するようになっている**DNSサーバ**を意味します。オープンリゾルバは攻撃の踏み台として悪用されてしまうことがあります。

DNS名前解決要求にはコネクションレスのUDPが使われるため、送信元や送信先の確認が行われません。このようなUDPの性質を悪用して、多数のオープンリゾルバに対して送信元IPアドレスを偽装したDNS名前解決要求を大量に行い、その応答結果を攻撃対象に送り付けることで攻撃対象をサービス不能に陥れるDDoS攻撃(DNSアンプ攻撃)があります。

ア “ICMPパケットの送信元を偽装し，多数の宛先に送ることによって，攻撃対象のコンピュータに大量の偽のICMPパケットの応答を送る。”

pingフラッド(ICMPフラッド)の説明です。オープンリゾルバは利用されません。

イ “PC内のhostsファイルにある，ドメインとIPアドレスとの対応付けを大量に書き換え，偽のWebサイトに誘導し，大量のコンテンツをダウンロードさせる。”

ファーミング攻撃の説明です。オープンリゾルバは利用されません。

ウ “送信元IPアドレスを偽装したDNS問合せを多数のDNSサーバに送ることによって，攻撃対象のコンピュータに大量の応答を送る。”

正しい。DNS名前解決要求を利用した攻撃なので、オープンリゾルバを悪用すると判断できます。

エ “誰でも電子メールの送信ができるメールサーバを踏み台にして，電子メールの送信元アドレスを詐称したなりすましメールを大量に送信する。”

外部からの不特定多数のオープンリレー(第三者中継)を許可しているメールサーバを悪用した攻撃です。

☆☆☆

SMTP-AUTH認証はどれか。

平成18年秋期　問74
111問目／選択範囲の問題数237問

ア　PASSコマンドの引数で用いられるパスワードをハッシュ値にして，その値でユーザー認証を行う。

イ　SMTPサーバへ電子メールを送信する前に電子メールを受信し，そのパスワード認証が行われたクライアントのIPアドレスに対して，一定時間だけ電子メールの送信を可能にする。

ウ　クライアントがSMTPサーバにアクセスするときにユーザー認証を行い，許可されたユーザーだけから電子メールを受け付ける。

エ　サーバはCAの公開鍵証明書をもち，クライアントから送信されたCAの署名付きクライアント証明書の妥当性を確認する。

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ウ　“あなたの解答：イ”

❑解説

電子メールを送信・転送するプロトコルであるSMTPには、

1. 送信処理と転送処理を同一の仕組みで扱っている
2. メールの投稿をするユーザーを認証する仕組みがない
3. 暗号化機能が標準で実装されていないため通信経路上を平文のメッセージが流れる

などの脆弱性があり、特に1，2の原因によって複数のメールサーバの第三者中継を利用した迷惑メールの温床となっていました。

SMTP-AUTH(SMTP-Authentication)は、メール投稿にあたってユーザー認証の仕組みがないSMTPにユーザー認証機能を追加した方式です。使用するにはメールサーバとクライアントの双方が対応していなければなりませんが、メール送信するときに「ユーザー名とパスワード」「チャレンジレスポンス」などで認証を行い、認証されたユーザーのみからのメール送信を許可することで不正な送信要求を遮断することができます。

ア “PASSコマンドの引数で用いられるパスワードをハッシュ値にして，その値でユーザー認証を行う。”

APOP(Authenticated POP)の説明です。

イ “SMTPサーバへ電子メールを送信する前に電子メールを受信し，そのパスワード認証が行われたクライアントのIPアドレスに対して，一定時間だけ電子メールの送信を可能にする。”

POP before SMTPの説明です。

ウ “クライアントがSMTPサーバにアクセスするときにユーザー認証を行い，許可されたユーザーだけから電子メールを受け付ける。”

正しい。SMTP-AUTHの説明です。

エ “サーバはCAの公開鍵証明書をもち，クライアントから送信されたCAの署名付きクライアント証明書の妥当性を確認する。”

DKIM(DomainKeys Identified Mail)の説明です。

☆

ISMSプロセスのPDCAモデルにおいて，PLANで実施するものはどれか。

平成19年秋期　問78
112問目／選択範囲の問題数237問

ア　運用状況の管理

イ　改善策の実施

ウ　実施状況に対するレビュー

エ　情報資産のリスクアセスメント

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

エ　“あなたの解答：エ”

❑解説

PDCA(ピーディーシーエー)は、Plan(計画)→Do(実行)→Check(評価)→Act(見直し・改善)の4段階を繰り返すことによって、業務を継続的に改善する手法です。

ISMS(情報セキュリティマネジメントシステム)におけるPDCAは次のような作業を行います。

Plan(計画)

・リスクアセスメントの実施
・情報セキュリティポリシーの策定　など

Do(実行)

・情報セキュリティポリシーに基づく対策の実施
・セキュリティ教育の実施　など

Check(評価)

・対策の実施状況の監査・評価・レビュー　など

Act(見直し・改善)

・情報セキュリティポリシーの見直し
・問題の是正・改善　など

上記から、各作業は以下のプロセスで実施するものと分類できます。

ア “運用状況の管理”

Do(実行)で実施する作業です。

イ “改善策の実施”

Act(見直し・改善)で実施する作業です。

ウ “実施状況に対するレビュー”

Check(評価)で実施する作業です。

エ “情報資産のリスクアセスメント”

正しい。Plan(計画)で実施する作業です。

☆

暗号方式の特徴のうち，適切なものはどれか。

平成19年春期　問71
113問目／選択範囲の問題数237問

ア　共通鍵暗号方式では，送信側と受信側で異なった鍵を用いるので，鍵の機密性が高い。

イ　共通鍵暗号方式では，通信相手ごとに異なった鍵を用いると，通信相手が多くなるに従って，鍵管理の手間が増える。

ウ　公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには，復号鍵を公開することによって，鍵管理の手間を減らす。

エ　公開鍵暗号方式では，署名に用いる鍵は公開しても構わない。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：イ”

❑解説

共通鍵暗号方式では、n人が相互に暗号化通信を行う場合「n×(n－1)÷2」種類の鍵が必要になります。(100人の場合で4950個)これに対して公開鍵暗号方式では「2n」個(100人の場合で200個)で済みます。
したがって共通鍵暗号方式を公開鍵暗号方式と比較した場合、鍵管理が煩雑になるという特徴があるといえます。

ア “共通鍵暗号方式では，送信側と受信側で異なった鍵を用いるので，鍵の機密性が高い。”

共通鍵暗号方式では送信側と受信側で同じ鍵を用います。

イ “共通鍵暗号方式では，通信相手ごとに異なった鍵を用いると，通信相手が多くなるに従って，鍵管理の手間が増える。”

正しい。

ウ “公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには，復号鍵を公開することによって，鍵管理の手間を減らす。”

公開鍵暗号方式では暗号化鍵を公開し、復号鍵は受信者自身が秘密鍵として厳重に管理します。

エ “公開鍵暗号方式では，署名に用いる鍵は公開しても構わない。”

デジタル署名では復号鍵で署名を行います。復号鍵は受信者が秘密鍵として管理しなくてはなりません。

☆☆

企業のDMZ上で1台のDNSサーバを，インターネット公開用と，社内のPC及びサーバからの名前解決の問合せに対応する社内用とで共用している。このDNSサーバが，DNSキャッシュポイズニングの被害を受けた結果，直接引き起こされ得る現象はどれか。

令和6年春期　問36
114問目／選択範囲の問題数237問

ア　DNSサーバのハードディスク上に定義されているDNSサーバ名が書き換わり，インターネットからDNSサーバに接続できなくなる。

イ　DNSサーバのメモリ上にワームが常駐し，DNS参照元に対して不正プログラムを送り込む。

ウ　社内の利用者が，インターネット上の特定のWebサーバにアクセスしようとすると，本来とは異なるWebサーバに誘導される。

エ　社内の利用者間の電子メールについて，宛先メールアドレスが書き換えられ，送信ができなくなる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：ウ”

❑解説

DNSキャッシュポイズニングは、DNSサーバからの名前解決要求があった場合に、正当なDNS応答よりも早く、偽の名前解決情報を含んだ応答を送りつけることで、そのDNSサーバに偽のキャッシュ情報（ドメイン名とIPアドレスの組み）を登録させる攻撃です。

社内のPCは外部のサイトにアクセスしようとする際に、DMZ上のサーバに名前解決を依頼しますが、この汚染されたDNSサーバは、偽のキャッシュ情報をもとに本来とは異なるサイトのIPアドレスを返します。これにより、社内のPCが攻撃者の指定した悪意のあるサイトへ誘導され、機密情報を盗まれるなどの被害が生じる可能性があります。

ア “DNSサーバのハードディスク上に定義されているDNSサーバ名が書き換わり，インターネットからDNSサーバに接続できなくなる。”

DNSサーバ名の書換えを行うわけではないので、DNSサーバにアクセスできなくなることはありません。

イ “DNSサーバのメモリ上にワームが常駐し，DNS参照元に対して不正プログラムを送り込む。”

DNSキャッシュポイズニングは、ワームに感染させる攻撃ではありません。

ウ “社内の利用者が，インターネット上の特定のWebサーバにアクセスしようとすると，本来とは異なるWebサーバに誘導される。”

正しい。DNSサーバに偽のDNSキャッシュ情報が登録されることで、そのキャッシュ情報を参照した利用者が本来とは別のサーバ(IPアドレス)に誘導されてしまいます。

エ “社内の利用者間の電子メールについて，宛先メールアドレスが書き換えられ，送信ができなくなる。”

偽のキャッシュ情報が登録されることで別のメールサーバに誘導され、メールの盗聴・改ざんを受ける可能性はありますが、電子メールの宛先アドレスが書き換えられることはありません。

☆

ボットネットにおけるC&Cサーバの役割として，適切なものはどれか。

令和2年秋期　問43
115問目／選択範囲の問題数237問

ア　Webサイトのコンテンツをキャッシュし，本来のサーバに代わってコンテンツを利用者に配信することによって，ネットワークやサーバの負荷を軽減する。

イ　外部からインターネットを経由して社内ネットワークにアクセスする際に，CHAPなどのプロトコルを中継することによって，利用者認証時のパスワードの盗聴を防止する。

ウ　外部からインターネットを経由して社内ネットワークにアクセスする際に，時刻同期方式を採用したワンタイムパスワードを発行することによって，利用者認証時のパスワードの盗聴を防止する。

エ　侵入して乗っ取ったコンピュータに対して，他のコンピュータへの攻撃などの不正な操作をするよう，外部から命令を出したり応答を受け取ったりする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：エ”

❑解説

C&Cサーバ(コマンド・コントロール・サーバ)は、マルウェアが侵入に成功したコンピュータ群(ボットネット)の動作を制御するために用いられる外部の指令サーバです。マルウェアはC&Cサーバからの指令を受けて、乗っ取ったコンピュータで悪意のある活動を行います。単純に外部から内部ネットワークに存在するマルウェアに対して通信を試みてもFWなどで遮断されてしまうため、マルウェア側からC&Cサーバに対して定期的に問い合わせを行い、その応答を使って指令を行う仕組みが用いられています。この仕組みを「コネクトバック通信」といいます。

したがって「エ」が適切な記述です。

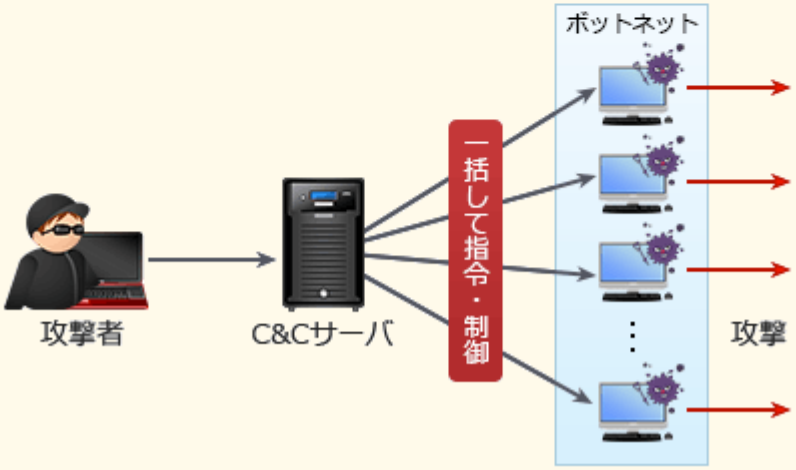


図　C&Cサーバ

ア “Webサイトのコンテンツをキャッシュし，本来のサーバに代わってコンテンツを利用者に配信することによって，ネットワークやサーバの負荷を軽減する。”

CDN(Contents Delivery Network)の役割です。

イ “外部からインターネットを経由して社内ネットワークにアクセスする際に，CHAPなどのプロトコルを中継することによって，利用者認証時のパスワードの盗聴を防止する。”

認証サーバの役割です。

ウ “外部からインターネットを経由して社内ネットワークにアクセスする際に，時刻同期方式を採用したワンタイムパスワードを発行することによって，利用者認証時のパスワードの盗聴を防止する。”

認証サーバの役割です。

エ “侵入して乗っ取ったコンピュータに対して，他のコンピュータへの攻撃などの不正な操作をするよう，外部から命令を出したり応答を受け取ったりする。”

正しい。C&Cサーバの役割です。

☆☆

経済産業省とIPAが策定した"サイバーセキュリティ経営ガイドライン(Ver1.1)"の説明はどれか。

平成29年春期　問39
116問目／選択範囲の問題数237問

ア　企業がIT活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき3原則と，情報セキュリティ対策を実施する上での責任者となる担当幹部に，経営者が指示すべき事項をまとめたもの

イ　経営者が，情報セキュリティについて方針を示し，マネジメントシステムの要求事項を満たすルールを定め，組織が保有する情報をCIAの観点から維持し，継続的に見直すためのプロセス及び管理策を体系的に規定したもの

ウ　事業体のITに関する経営者の活動を大きくITガバナンス(統制)とITマネジメント(管理)に分割し，具体的な目標と工程として37のプロセスを定義したもの

エ　世界的規模で生じているサイバーセキュリティ上の脅威に関して，企業の経営者を支援する施策を総合的かつ効果的に推進するための国の責務を定めたもの

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ア　“あなたの解答：ア”

❑解説

サイバーセキュリティ経営ガイドラインは、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」をまとめたものです。具体的には、経営者のリーダーシップの下での体制整備と対策の進め方、社会やステークホルダに対する情報開示のあり方などが取りまとめられています。

したがって適切な説明は「ア」です。

ア “企業がIT活用を推進していく中で，サイバー攻撃から企業を守る観点で経営者が認識すべき3原則と，情報セキュリティ対策を実施する上での責任者となる担当幹部に，経営者が指示すべき事項をまとめたもの”

正しい。サイバーセキュリティ経営ガイドラインの説明です。

イ “経営者が，情報セキュリティについて方針を示し，マネジメントシステムの要求事項を満たすルールを定め，組織が保有する情報をCIAの観点から維持し，継続的に見直すためのプロセス及び管理策を体系的に規定したもの”

情報セキュリティ方針の説明です。

ウ “事業体のITに関する経営者の活動を大きくITガバナンス(統制)とITマネジメント(管理)に分割し，具体的な目標と工程として37のプロセスを定義したもの”

COBITの説明です。

エ “世界的規模で生じているサイバーセキュリティ上の脅威に関して，企業の経営者を支援する施策を総合的かつ効果的に推進するための国の責務を定めたもの”

サイバーセキュリティ基本法の説明です。

参考URL: サイバーセキュリティ経営ガイドライン
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

☆☆

公開鍵暗号方式によるデジタル署名の手続とハッシュ値の使用方法のうち，適切なものはどれか。

平成19年春期　問72
117問目／選択範囲の問題数237問

ア　受信者は，送信者の公開鍵で署名を復号してハッシュ値を取り出し，元のメッセージを変換して求めたハッシュ値と比較する。

イ　送信者はハッシュ値を自分の公開鍵で暗号化して，元のメッセージとともに受信者に送る。

ウ　デジタル署名を付ける元になったメッセージは，署名を変換したハッシュ値から復元できる。

エ　元のメッセージ全体に対して公開鍵で暗号化を行い，ハッシュ値を用いて復号する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

デジタル署名の手順は次の通りです。

1. 送信者は、平文をハッシュ関数で圧縮したメッセージダイジェストを**送信者の秘密鍵**で暗号化し、平文と一緒に送信する。
2. 受信者は、受信したメッセージダイジェストを**送信者の公開鍵**で復号し、受信した平文をハッシュ関数で圧縮したものと比較する。
3. 一つの平文からハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、送信者から送られてきたメッセージダイジェストと、受信側でハッシュ化したメッセージダイジェストが同じなら、通信内容が改ざんされていないことが証明される。

ア “受信者は，送信者の公開鍵で署名を復号してハッシュ値を取り出し，元のメッセージを変換して求めたハッシュ値と比較する。”

正しい手順です。

イ “送信者はハッシュ値を自分の公開鍵で暗号化して，元のメッセージとともに受信者に送る。”

ハッシュ値の暗号化に使用するのは送信者の"秘密鍵"です。

ウ “デジタル署名を付ける元になったメッセージは，署名を変換したハッシュ値から復元できる。”

ハッシュ値は一方向性関数によって生成されるため、ハッシュ値からもとのメッセージを復元することはできません。

エ “元のメッセージ全体に対して公開鍵で暗号化を行い，ハッシュ値を用いて復号する。”

送信者が本文をハッシュ化したものに対して暗号化を行います。またハッシュ値は復号鍵として使用しません。

☆

WAFによる防御が有効な攻撃として，最も適切なものはどれか。

令和6年春期　問41
118問目／選択範囲の問題数237問

ア	DNSサーバに対するDNSキャッシュポイズニング
イ	REST APIサービスに対するAPIの脆弱性を狙った攻撃
ウ	SMTPサーバの第三者不正中継の脆弱性を悪用したフィッシングメールの配信
エ	電子メールサービスに対する大量，かつ，サイズの大きな電子メールの配信

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

イ　“あなたの解答：イ”

❑解説

WAF(Web Application Firewall)は、Webサーバの前段に配置し、通過するパケットのIPアドレスやポート番号だけでなくペイロード部(データ部分)をチェックすることで、Webアプリケーションに対する攻撃を検知し、遮断することが可能なファイアウォールです。例えば、Webブラウザからのリクエストパケットに**SQL**文の断片が含まれていたら、**SQL**インジェクションの可能性があるとして遮断するなどです。WAFは、多層防御の一環として、データの「入口」でのセキュリティを高めることを目的として設置されます。

WAFにより防御することができるのは、Webアプリケーションの脆弱性を狙った攻撃だけです。Webアプリケーションとは、HTTP(S)通信の仕組みを使いWebブラウザとWebサーバのやり取りによって機能を提供するアプリケーションなので、選択肢の中ではREST APIが正解となります。REST APIとは、HTTP(S)を使ったWeb APIシステムの設計モデルです。

ア　“DNSサーバに対するDNSキャッシュポイズニング”

DNSサーバに対する攻撃なので対象外です。DNSSECの導入などによって防御します。

イ　“REST APIサービスに対するAPIの脆弱性を狙った攻撃”

正しい。Webサーバに対する攻撃なので、WAFでの防御が有効です。

ウ　“SMTPサーバの第三者不正中継の脆弱性を悪用したフィッシングメールの配信”

メールサーバに対する攻撃なので対象外です。第三者不正中継は、メールサーバの設定で禁止することで防御します。

エ　“電子メールサービスに対する大量，かつ，サイズの大きな電子メールの配信”

メールサーバに対する攻撃なので対象外です。本肢の攻撃はメールボム(爆弾)と呼ばれ、スパムフィルタリングによって防御します。

☆

非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。

平成25年秋期　問38
119問目／選択範囲の問題数237問

ア	AES	イ	DSA	ウ	IDEA	エ	RSA

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：エ”

❑解説

RSA暗号(Rivest Shamir Adleman)は、桁数が大きい合成数の素因数分解が困難であることを安全性の根拠とした公開鍵暗号の一つです。数字の桁数がそのまま安全強度につながるため、実際のRSAでは合成数の元となる2つの数に300～1,000桁の非常に大きな素数が使用されます。

RSAという名称は、開発者であるRivest，Shamir，Adlemanの頭文字をとって名付けられました。

ア　“AES”

Advanced Encryption Standardの略。アメリカ合衆国の次世代暗号方式として規格化された共通鍵暗号方式です。

イ　“DSA”

Digital Signature Algorithmの略。離散対数問題を安全性の根拠とするElGamal署名を改良して開発された、デジタル署名方式の一つです。

ウ　“IDEA”

International Data Encryption Algorithmの略。PGPやSSHなどで使用される共通鍵暗号方式です。

エ　“RSA”

正しい。RSAは、非常に大きな数の素因数分解が困難なことを安全性の根拠としています。

☆

SQLインジェクションの説明はどれか。

平成22年春期　問43
120問目／選択範囲の問題数237問

ア　Webアプリケーションに悪意のある入力データを与えてデータベースの問合せや操作を行う命令文を組み立てて，データを改ざんしたり不正に情報取得したりする攻撃

イ　悪意のあるスクリプトが埋め込まれたWebページを訪問者に閲覧させて，別のWebサイトで，その訪問者が意図しない操作を行わせる攻撃

ウ　市販されているデータベース管理システムの脆弱性を利用して，宿主となるデータベースサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃

エ　訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送り，訪問者のブラウザで実行させる攻撃

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

SQLインジェクションとは、データベースを使ったWebアプリケーションシステムに対して、行われる攻撃手法です。入力フォームにSQL文の一部や不正な文字列を与えることでアプリケーションが想定していないSQL文を実行させ、データベースサーバを不正に操作する攻撃方法です。

この攻撃に対しては、入力値を適切にエスケープしたりBIND機構を使うことでが対策となります。DBMSやライブラリによってはエスケープ処理が自動化されているものもあり有用です。

ア “Webアプリケーションに悪意のある入力データを与えてデータベースの問合せや操作を行う命令文を組み立てて，データを改ざんしたり不正に情報取得したりする攻撃”

正しい。SQLインジェクション対策としてWeb入力フォームからのデータ内の危険文字列を「無害化」するサニタイジングという用語もチェックしておきましょう。

イ “悪意のあるスクリプトが埋め込まれたWebページを訪問者に閲覧させて，別のWebサイトで，その訪問者が意図しない操作を行わせる攻撃”

XSRF(クロスサイトリクエストフォージェリ)の説明です。攻撃者は第三者を攻撃用のWebページにアクセスさせ、意図した操作を行わせるための用意したHTTPリクエストを送信させます。

ウ “市販されているデータベース管理システムの脆弱性を利用して，宿主となるデータベースサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃”

ワームの一種 SQL Slammerの説明です。

エ “訪問者の入力データをそのまま画面に表示するWebサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送り，訪問者のブラウザで実行させる攻撃”

XSS(クロスサイトスクリプティング)の説明です。

☆

JIS Q 27000:2019(情報セキュリティマネジメントシステム用語)において，認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性として定義されているものはどれか。

令和5年秋期　問40
121問目／選択範囲の問題数237問

ア	機密性	イ	真正性	ウ	認証	エ	否認防止

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ア　“あなたの解答：ア”

❑解説

ア “機密性”

正しい。機密性(confidentiality)は、認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しないという特性と定義されています。要するに、アクセス権限がない人には情報を見せないということです。

イ “真正性”

真正性(authenticity)は、利用者、プロセス、システム、情報などの対象が、主張のとおり本物であることが明確である特性と定義されています。

ウ “認証”

認証(authentication)は、エンティティの主張する特性が正しいという保証の提供と定義されています。

エ “否認防止”

否認防止(non-repudiation)は、主張された事象又は処置の発生、及びそれらを引き起こしたエンティティを証明する能力と定義されています。

☆

電子的な方法を用いないで、緊急事態を装って組織内部の人間からパスワードや機密情報のありかを不正に聞き出して入手する行為は，どれに分類されるか。

平成17年春期　問75
122問目／選択範囲の問題数237問

ア	ソーシャルエンジニアリング	イ	トロイの木馬
ウ	パスワードクラック	エ	踏み台攻撃

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

ソーシャルエンジニアリングは、情報通信技術の方法を用いるのではなく、人のミスや心理的な隙に付け込むことでパスワードなどの秘密情報を不正に取得する方法の総称です。

関係者を装って電話でパスワードを聞き出す（なりすまし）、肩越しに画面やキー入力を見る（ショルダーハッキング）、プリンターやデスクやごみ箱に残された書類を漁る（トラッシング）などの行為がソーシャルエンジニアリングの代表例です。

したがって「ア」が正解です。

ア “ソーシャルエンジニアリング”

正しい。

イ “トロイの木馬”

トロイの木馬は、一見通常の動作をしているように見せかけておいて、裏ではOSの設定変更、パスワードの窃盗、外部からの遠隔操作の踏み台になるなどの悪意のある動作を秘密裏に行うコンピュータウィルスです。

ウ “パスワードクラック”

パスワードクラックは、パスワード認証を不正な手段で突破し、不正ログインを試みる行為です。

エ “踏み台攻撃”

踏み台攻撃は、サイバー犯罪者の支配下におかれたコンピュータを遠隔操作して、指令者の代わりに攻撃を行わせる行為です。

☆☆

Autorun.infを悪用したUSBワームの説明のうち，適切なものはどれか。

平成22年秋期　問43
123問目／選択範囲の問題数237問

ア　USB接続可能なICレコーダは，音声データを取り扱うものなので，USBワームに感染することはない。

イ　暗号化USBメモリは，メモリ上のデータが暗号化されているので，USBワームに感染することはない。

ウ　自動実行するワーム自体をUSBメモリ内のAutorun.infファイルに埋め込む。

エ　特定ワームのファイル名を登録したAutorun.infファイルをUSBメモリ内に生成する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：ウ”

❑解説

Autorun.infとは、CDやDVDなどの外部メディア内がPCに接続されたときに、内部にある特定のプログラムを自動実行するために記述されるテキストファイルです。通常ソフトウェアのインストールCDを挿入した際には自動でインストール画面が立ち上がりますが、これもAutorun.infの記述によるものです。

一般にCDやDVDだけと認識されているこの自動再生機能ですが、実際にはリムーバブルメディアなどにも適用可能です。USBワームはこれを悪用し、USBメモリがPCに接続された際にワーム本体が自動的に実行されるよう仕組んでいます。感染後は他の外部メディアやネットワーク上の他のPCに自身とAutorun.infをコピーし、さらに感染を広げていくという活動を行います。

対策としては、①出所不明のUSBメモリを使用しない、②信頼できないコンピュータではUSBメモリを使用しない、③USBメモリの自動実行をさせない、などが挙げられます。

ア　“USB接続可能なICレコーダは，音声データを取り扱うものなので，USBワームに感染することはない。”

たとえ音声データを取り扱う機器でも、記憶領域にワーム本体とAutorun.infが埋め込まれていれば感染を防ぐことはできません。

イ　“暗号化USBメモリは，メモリ上のデータが暗号化されているので，USBワームに感染することはない。”

暗号化されたデータは盗難時などには効果を発揮しますが、使用時のパスワードを入力すればデータは復号され通常と変わらない状態になるので、感染を防ぐことはできません。

ウ “自動実行するワーム自体をUSBメモリ内のAutorun.infファイルに埋め込む。”

USBワームが成立するためには、最低でもワーム本体とAutorun.infの2つが必要です。Autorun.infはテキスト形式の設定ファイルであり、ワーム本体を埋め込むことはできません。

エ “特定ワームのファイル名を登録したAutorun.infファイルをUSBメモリ内に生成する。”

正しい。

☆☆
※理屈

SSLによるクライアントとWebサーバ間の通信手順(1)～(5)において，a，bに入る適切な組合せはどれか。ここで，記述した手順は，一部簡略化している。

(1) クライアントからのSSLによる接続要求に対し，Webサーバは証明書をクライアントに送付する。

(2) クライアントは，保持している［ a ］によってこのサーバ証明書の正当性を確認する。

(3) クライアントは，共通鍵生成用のデータを作成し，サーバ証明書に添付された［ b ］によってこの共通鍵生成用データを暗号化し，Webサーバに送付する。

(4) 受け取ったWebサーバは，自らの秘密鍵によって暗号化された共通鍵生成用データを復号する。

(5) クライアントとWebサーバの両者は，同一の共通鍵生成用データによって共通鍵を作成し，これ以降の両者間の通信は，この共通鍵による暗号化通信を行う。

平成24年秋期　問33
124問目／選択範囲の問題数237問

	a	b
ア	クライアントの公開鍵	Web サーバの秘密鍵
イ	クライアントの秘密鍵	Web サーバの公開鍵
ウ	認証局の公開鍵	Web サーバの公開鍵
エ	認証局の公開鍵	Web サーバの秘密鍵

ア　イ　ウ　エ

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ウ　“あなたの解答：ウ”

❑解説

SSL(Secure Sockets Layer)は、通信の暗号化，デジタル証明書を利用した改ざん検出，ノード認証を含む統合セキュアプロトコルです。
OSI基本参照モデルのトランスポート層で動作するので，上位のアプリケーション層のプログラムから意識することなく利用できます。

[a]について
サーバ証明書(デジタル証明書)は、Webサーバが認証局に対して事前に登録申請を行い、Webサーバに対して発行されたもので、「サーバの公開鍵」に対して認証局のデジタル署名が付されています。
SSLの利用手順では、まずWebサーバからクライアントに対してサーバ証明書を送り、クライアントでは「**認証局の公開鍵**」を用いて、この証明書の正当性を確認し、Webサーバの認証を行います。(サーバ証明書に添付された「Webサーバの公開鍵」の正当性を確認する。)

∴ [a] **＝認証局の公開鍵**

[b]について
クライアントは、Webサーバを認証後、共通鍵生成用のデータをWebサーバと共有するために、自ら生成したデータを暗号化したものをWebサーバに送ります。
この際、サーバ証明書に添付された「**Webサーバの公開鍵**」を用いて暗号化したデータをWebサーバに送り、データを受け取ったWebサーバは「Webサーバの秘密鍵」で、このデータを復号し共通鍵生成用のデータを共有します。

∴ [b] **＝Webサーバの公開鍵**

その後、クライアントとWebサーバで共有した共通鍵生成用のデータから同一の共通鍵を生成し、以後はこの共通鍵を用いて暗号化通信を行います。

☆

手順に示すクライアントとサーバの処理と通信で可能になることはどれか。

〔手順〕

(1) サーバはクライアントから要求があるたびに異なる予測困難な値(チャレンジ)を生成して保持するとともに，クライアントへ送る。

(2) クライアントは利用者が入力したパスワードのメッセージダイジェストを計算し，(1)でサーバから送られた"チャレンジ"と合わせたものから，さらに，メッセージダイジェスト(レスポンス)を計算する。この"レスポンス"と利用者が入力した利用者IDをサーバに送る。

(3) サーバは，クライアントから受け取った利用者IDで利用者情報を検索して，取り出したパスワードのメッセージダイジェストと(1)で保持していた"チャレンジ"を合わせたものから，メッセージダイジェストを計算する(レスポンス照合データ)。この"レスポンス照合データ"とクライアントから受け取った"レスポンス"とを比較する。

平成24年春期　問39
125問目／選択範囲の問題数237問

ア	伝送上で発生したパスワードのビット誤りのサーバでの訂正
イ	伝送上で発生した利用者IDのビット誤りのサーバでの訂正
ウ	ネットワーク上でのパスワードの，漏えい防止とリプレイ攻撃の防御
エ	ネットワーク上での利用者IDの，漏えい防止とリプレイ攻撃の防御

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ウ　“あなたの解答：ウ”

❑解説

チャレンジレスポンス方式は、秘密にしている固定パスワードをネットワーク中に流さないようにすることで、パスワードの盗聴およびリプレイ攻撃を防止する仕組みです。

下図は手順を図式化したものです。

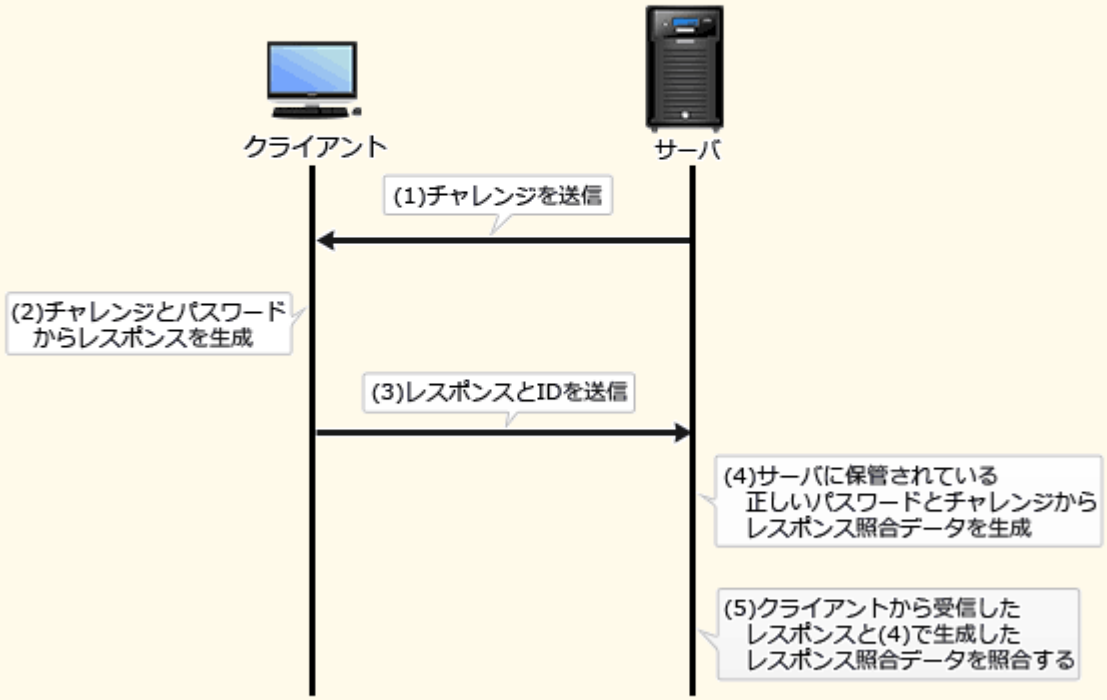


図　チャレンジレスポンス方式の流れ

このような手順をとることで次のような利点があります。

- 平文のパスワードがネットワークを流れることがない。
- ネットワークに送信されるレスポンスは、ハッシュ関数によって生成されたメッセージダイジェストなので盗聴されても元のパスワードを再現することが困難である。
- サーバからクライアントに送信されるチャレンジは毎回異なるので、ある時点のレスポンスを保存して後から送信しなおすことで不正な認証を試みるリプレイ攻撃が成功する可能性は非常に低い。

したがってこの手順によって可能なことは「ネットワーク上でのパスワードの，漏えい防止とリプレイ攻撃の防御」になります。

☆

サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち，適切なものはどれか。

平成25年秋期　問44
126問目／選択範囲の問題数237問

	辞書攻撃	スニッフィング	ブルートフォース攻撃
ア	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。
イ	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。
ウ	ランダムな値でパスワードを設定する。	ログインの試行回数に制限を設ける。	パスワードを平文で送信しない。
エ	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。

ア　イ　ウ　エ

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：イ”

❑解説

設問にある3つのパスワードクラック手法は次のようなものです。

辞書攻撃

辞書に載っている英単語、人名、パスワードによく使われる文字列などを大量に登録したリスト(辞書ファイル)を用意して、1つずつ試していくことでパスワードを解読しようとする攻撃手法。

スニッフィング

通信経路上を流れるパケットを盗聴して、その内容からパスワードの不正取得を試みる攻撃手法

ブルートフォース攻撃

パスワードとして設定可能な文字数と文字種の組合せを全て試すことで、パスワードの不正取得を試みる攻撃手法。パスワード長が短く、使用可能な文字種が少ない場合には、この手法によって破られる可能性が高くなってしまう。

それぞれの攻撃の性質を考えると、辞書攻撃には「ランダムな値でパスワードを設定する」、スニッフィングには「パスワードを平文で送信しない」、ブルートフォース攻撃には「ログイン試行回数に制限を設ける」が適切な対策となります。

したがって正解は「イ」です。

☆

ISMSにおけるリスク分析の方法の一つであるベースラインアプローチはどれか。

平成18年秋期　問77
127問目／選択範囲の問題数237問

ア　公表されている基準などに基づいて一定のセキュリティレベルを設定し，実施している管理策とのギャップ分析を行った上で，リスクを評価する。

イ　情報資産を洗い出し，それぞれの情報資産に対して資産価値，脅威，脆弱性及びセキュリティ要件を識別し，リスクを評価する。

ウ　複数のリスク分析方法の長所を生かして組み合わせ，作業効率や分析精度の向上を図る。

エ　リスク分析を行う組織や担当者の判断によって，リスクを評価する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ア　“あなたの解答：ア”

❑解説

ベースラインアプローチは、一般に公開されている基準やガイドライン，チェックリストを使用して**簡易的に**リスク分析を行う手法です。
アンケートやチェックリストの回答から、組織やシステムにおける問題点を洗い出すので時間やコストが少なくて済みますが、大まかな分析になってしまうことや質問の品質によって分析結果が左右されるというデメリットもあります。

基準として活用できるものとしては「ISO/IEC 27001」「情報セキュリティ管理基準」「システム管理基準」などがあります。

ア “公表されている基準などに基づいて一定のセキュリティレベルを設定し，実施している管理策とのギャップ分析を行った上で，リスクを評価する。”

正しい。ベースラインアプローチの説明です。

イ “情報資産を洗い出し，それぞれの情報資産に対して資産価値，脅威，脆弱性及びセキュリティ要件を識別し，リスクを評価する。”

詳細リスク分析の説明です。

ウ “複数のリスク分析方法の長所を生かして組み合わせ，作業効率や分析精度の向上を図る。”

組合せアプローチの説明です。

エ “リスク分析を行う組織や担当者の判断によって，リスクを評価する。”

非公式アプローチの説明です。

☆☆☆☆

Man-in-the-Browser攻撃に該当するものはどれか。

平成28年春期　問45
128問目／選択範囲の問題数237問

ア　DNSサーバのキャッシュを不正に書き換えて，インターネットバンキングに見せかけた偽サイトをWebブラウザに表示させる。

イ　PCに侵入したマルウェアが，利用者のインターネットバンキングへのログインを検知して，Webブラウザから送信される振込先などのデータを改ざんする。

ウ　インターネットバンキングから送信されたように見せかけた電子メールに偽サイトのURLを記載しておき，その偽サイトに接続させて，Webブラウザから口座番号やクレジットカード番号を入力させることで情報を盗み出す。

エ　インターネットバンキングの正規サイトに見せかけた中継サイトに接続させ，Webブラウザから入力された利用者IDとパスワードを正規サイトに転送し，利用者になりすましてログインする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：イ”

❑解説

Man-in-the-Browser攻撃(MITB)は、ユーザーPC内でプロキシとして動作するトロイの木馬(マルウェア)によってWebブラウザ～Webサーバ間の送受信をブラウザベースで盗聴・改ざんする攻撃です。インターネットバンキングへのログインを検知して、セッションを乗っ取り、振込先口座番号を差し替えることで預金を不正送金するなどの攻撃例があります。
同じく送受信を改ざんするMan-in-the-Middle攻撃と異なり、クライアント内で書換えが行われるためWebサーバ側で不正処理を拒否することが難しいという特徴があります。

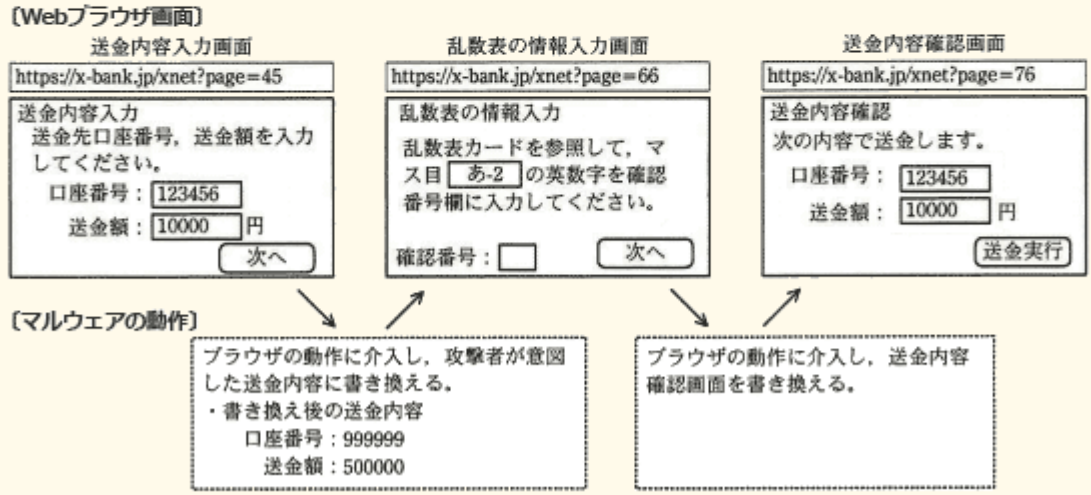


図　Man-in-the-Browser攻撃による不正送金被害の流れ(SC 26年春期午後Ⅰ問3より)

ア "DNSサーバのキャッシュを不正に書き換えて，インターネットバンキングに見せかけた偽サイトをWebブラウザに表示させる。"

DNSキャッシュポイズニング攻撃に該当します。

イ "PCに侵入したマルウェアが，利用者のインターネットバンキングへのログインを検知して，Webブラウザから送信される振込先などのデータを改ざんする。"

正しい。Man-in-the-Browser攻撃に該当します。

ウ "インターネットバンキングから送信されたように見せかけた電子メールに偽サイトのURLを記載しておき，その偽サイトに接続させて，Webブラウザから口座番号やクレジットカード番号を入力させることで情報を盗み出す。"

フィッシング攻撃に該当します。

エ "インターネットバンキングの正規サイトに見せかけた中継サイトに接続させ，Webブラウザから入力された利用者IDとパスワードを正規サイトに転送し，利用者になりすましてログインする。"

情報の搾取に中継サイトを使うMan-in-the-Middle攻撃(中間者攻撃)に該当します。

☆

JIS Q 27000:2019(情報セキュリティマネジメントシステム－用語)において定義されている情報セキュリティの特性に関する記述のうち，否認防止の特性に関する記述はどれか。

令和3年秋期　問39
129問目／選択範囲の問題数237問

ア	ある利用者があるシステムを利用したという事実が証明可能である。
イ	認可された利用者が要求したときにアクセスが可能である。
ウ	認可された利用者に対してだけ，情報を使用させる又は開示する。
エ	利用者の行動と意図した結果とが一貫性をもつ。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

否認防止(Non-Repudiation)は、情報セキュリティマネジメントの付加的な要素で、行った操作や発生した事象を後になって否認されないように証明できる能力のことです。ログの取得で必要な項目を確実に記録するとともに、完全性が損なわれないように保管することで確保できます。デジタル署名やタイムスタンプは否認防止に活用される技術です。
JIS Q 27000では「主張された事象又は処理の発生、及びそれを引き起こしたエンティティを証明する能力」と定義されています。

ア “ある利用者があるシステムを利用したという事実が証明可能である。”

正しい。否認防止の説明です。

イ “認可された利用者が要求したときにアクセスが可能である。”

可用性の説明です。

ウ “認可された利用者に対してだけ，情報を使用させる又は開示する。”

機密性の説明です。

エ “利用者の行動と意図した結果とが一貫性をもつ。”

信頼性の説明です。

☆☆☆

PCのストレージ上の重要なデータを保護する方法のうち，ランサムウェア感染による被害の低減に効果があるものはどれか。

令和5年秋期　問43
130問目／選択範囲の問題数237問

ア　WORM(Write Once Read Many)機能を有するストレージを導入して，そこに重要なデータをバックアップする。

イ　ストレージをRAID5構成にして，1台のディスク故障時にも重要なデータを利用可能にする。

ウ　内蔵ストレージを増設して，重要なデータを常時レプリケーションする。

エ　ネットワーク上のストレージの共有フォルダをネットワークドライブに割り当てて，そこに重要なデータをバックアップする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ア　“あなたの解答：イ”

❑解説

ア “WORM(Write Once Read Many)機能を有するストレージを導入して，そこに重要なデータをバックアップする。”

正しい。WORMとは、"write once"(書込みは1回だけ)の名称が示すように、一度書き込まれたデータは書換えや消去ができない読出し専用の状態になり、新たなデータの追記のみができるという記録方式です。DVD-R/BD-RなどがWORMなメディアの例です。WORM機能を有する記憶媒体に保存されたデータは書換えができないので、ランサムウェアによる暗号化から逃れることができます。このため、ランサムウェア対策として有効と言えます。

イ “ストレージをRAID5構成にして，1台のディスク故障時にも重要なデータを利用可能にする。”

RAID5はバックアップではないので、ランサムウェア対策のバックアップとしては使うことができません。ランサムウェアによりディスク内のファイルが暗号化されると、パリティビットは暗号化されたデータの冗長ビットに変わるためデータを復元することはできません。

ウ “内蔵ストレージを増設して，重要なデータを常時レプリケーションする。”

ランサムウェアは、感染したPCに接続されている記憶媒体上のデータすべてを暗号化しようとします。内蔵ストレージ内のレプリケーション(複製)も暗号化されてしまうため効果はありません。バックアップを保存する媒体は、常時接続とせずバックアップのときにだけPCと接続するのが鉄則です。

エ “ネットワーク上のストレージの共有フォルダをネットワークドライブに割り当てて，そこに重要なデータをバックアップする。”

ランサムウェアは、感染したPCからネットワークを介してアクセスできる外付けHDD、共有フォルダ、ファイルサーバなどにあるデータを暗号化しようとします。ネットワークストレージの共有フォルダに保存したバックアップは暗号化されてしまうため効果はありません。

☆☆☆

エクスプロイトキットの説明はどれか。

令和元年秋期　問42
131問目／選択範囲の問題数237問

ア　JPEGデータを読み込んで表示する機能をもつ製品に対して，セキュリティ上の問題を発生させる可能性のある値を含んだJPEGデータを読み込ませることによって，脆弱性がないかをテストするツール

イ　JVNなどに掲載された脆弱性情報の中に，利用者自身がPC又はサーバにインストールした製品に関する情報が含まれているかどうかを確認するツール

ウ　OSやアプリケーションソフトウェアの脆弱性を悪用して攻撃するツール

エ　Webサイトのアクセスログから，Webサイトの脆弱性を悪用した攻撃を検出するツール

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：エ”

❑解説

エクスプロイトキットは、複数のエクスプロイトコードをまとめ、ソフトウェアやOSに内在する脆弱性を確認したり、攻撃者がその脆弱性を悪用したりするツール群です。エクスプロイト(exploit)には、悪用という意味があります。

エクスプロイトコード

ソフトウェアの脆弱性を悪用した不正な動作を再現するために作成されたスクリプトやプログラムの断片

エクスプロイトキットが仕掛けられたWebサイトにアクセスすると、PC上の脆弱性が調べられ、その脆弱性を突く攻撃が行われます。最終的にはマルウェアがダウンロードされ、ランサムウェアやクリプトジャッキングの被害を受ける可能性があります。被害を受けないためにはPCで使用しているOSやソフトウェアを常に最新バージョンに更新しておくことが重要です。

ア　“JPEGデータを読み込んで表示する機能をもつ製品に対して，セキュリティ上の問題を発生させる可能性のある値を含んだJPEGデータを読み込ませることによって，脆弱性がないかをテストするツール”

ファジングツールの説明です。IPAでJPEG読込み機能のファジングを支援する「iFuzz Maker」というソフトウェアが公開されています。

イ　“JVNなどに掲載された脆弱性情報の中に，利用者自身がPC又はサーバにインストールした製品に関する情報が含まれているかどうかを確認するツール”

MyJVNバージョンチェッカ等の説明です。

ウ　“OSやアプリケーションソフトウェアの脆弱性を悪用して攻撃するツール”

正しい。エクスプロイトキットの説明です。

エ　“Webサイトのアクセスログから，Webサイトの脆弱性を悪用した攻撃を検出するツール”

SIEM(シーム)の説明です。SIEMではありませんが、IPAでWebサーバのアクセスログから攻撃の痕跡を探す「iLogScanner」というソフトウェアが公開されています。

☆

クロスサイトスクリプティングの手口に該当するものはどれか。

平成27年秋期　問36
132問目／選択範囲の問題数237問

ア　攻撃者が，スクリプトを用いてWebサイトのOSコマンドを呼び出し，任意のファイルの読出しや変更・削除などの不正操作をする。

イ　攻撃者が，スクリプトを用いて特定のPCへ大量に接続要求を送り出し，通信機能を停止させる。

ウ　攻撃者が用意したスクリプトでWebサイトのサービスポートに順次アクセスし，各ポートに対応するサービスに存在するセキュリティ上の弱点を探し出す。

エ　攻撃者が用意したスクリプトを，閲覧者のWebブラウザを介して脆弱なWebサイトに送り込み，閲覧者のWebブラウザ上でスクリプトを実行させる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：エ”

❑解説

クロスサイトスクリプティング(XSS)は、動的にWebページを生成するアプリケーションのセキュリティ上の不備を意図的に利用して、悪意のあるスクリプトを混入させることで、攻撃者が仕込んだ操作を実行させたり、別のサイトを横断してユーザーのクッキーや個人情報を盗んだりする攻撃手法です。
XSS脆弱性のあるWebアプリケーションでは、以下の影響を受ける可能性があります。

1. サイト攻撃者のブラウザ上で、攻撃者の用意したスクリプトの実行によりクッキー値を盗まれ、利用者が被害にあう。
2. 同様にブラウザ上でスクリプトを実行され、サイト利用者の権限でWebアプリケーションの機能を利用される。
3. Webサイト上に偽の入力フォームが表示され、フィッシングにより利用者が個人情報を盗まれる。

ア　“攻撃者が，スクリプトを用いてWebサイトのOSコマンドを呼び出し，任意のファイルの読出しや変更・削除などの不正操作をする。”

OSコマンドインジェクションの手口です。

イ　“攻撃者が，スクリプトを用いて特定のPCへ大量に接続要求を送り出し，通信機能を停止させる。”

DoS攻撃の手口です。

ウ　“攻撃者が用意したスクリプトでWebサイトのサービスポートに順次アクセスし，各ポートに対応するサービスに存在するセキュリティ上の弱点を探し出す。”

ポートスキャンの手口です。

エ　“攻撃者が用意したスクリプトを，閲覧者のWebブラウザを介して脆弱なWebサイトに送り込み，閲覧者のWebブラウザ上でスクリプトを実行させる。”

正しい。クロスサイトスクリプティングの手口です。

☆☆☆

公開鍵暗号方式を採用した電子商取引において，認証局(CA)の役割はどれか。

平成21年秋期　問39
133問目／選択範囲の問題数237問

ア　取引当事者の公開鍵に対するデジタル証明書を発行する。

イ　取引当事者のデジタル署名を管理する。

ウ　取引当事者のパスワードを管理する。

エ　取引当事者の秘密鍵に対するデジタル証明書を発行する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：エ”

❑解説

認証局(Certificaion Authority:CA)は、公開鍵暗号方式を用いたデータ通信において、利用者(主にサーバ)の公開鍵の正当性を保証するためのデジタル証明書を発行する第三者機関です。したがって正解は「ア」です。

また認証局はデジタル証明書を発行する以外にも、PKI(公開鍵基盤)における次の役割を担っています。

- CRL(証明書失効リスト)を発行する
- CPS(認証局運用規定)を公開する
- デジタル証明書を検証するための認証局の公開鍵を公開する
- 認証局の秘密鍵を厳重に管理する

☆☆☆

リスクベース認証の特徴はどれか。

令和3年春期　問39
134問目／選択範囲の問題数237問

ア　いかなる利用条件でのアクセスの要求においても，ハードウェアトークンとパスワードを併用するなど，常に二つの認証方式を併用することによって，不正アクセスに対する安全性を高める。

イ　いかなる利用条件でのアクセスの要求においても認証方法を変更せずに，同一の手順によって普段どおりにシステムにアクセスできるようにし，可用性を高める。

ウ　普段と異なる利用条件でのアクセスと判断した場合には，追加の本人認証をすることによって，不正アクセスに対する安全性を高める。

エ　利用者が認証情報を忘れ，かつ，Webブラウザに保存しているパスワード情報も使用できないリスクを想定して，緊急と判断した場合には，認証情報を入力せずに，利用者は普段どおりにシステムを利用できるようにし，可用性を高める。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：ア”

❑解説

リスクベース認証は、通常とは異なる利用環境(例えば、普段とは異なるIPアドレスやISP及びOSやWebブラウザ等)からの認証要求があった場合に、通常の認証に追加する形で別の認証を実施する方式です。不正ログインの可能性のあるアクセスに対してだけ追加の本人認証を行うため、一定の利便性を保ちつつ、異なる利用環境からの不正アクセスに対してセキュリティを高めることができます。

したがって適切な記述は「ウ」です。

ア “いかなる利用条件でのアクセスの要求においても，ハードウェアトークンとパスワードを併用するなど，常に二つの認証方式を併用することによって，不正アクセスに対する安全性を高める。”

二要素認証の説明です。

イ “いかなる利用条件でのアクセスの要求においても認証方法を変更せずに，同一の手順によって普段どおりにシステムにアクセスできるようにし，可用性を高める。”

RADIUS認証の説明です。

ウ “普段と異なる利用条件でのアクセスと判断した場合には，追加の本人認証をすることによって，不正アクセスに対する安全性を高める。”

正しい。リスクベース認証の説明です。

エ “利用者が認証情報を忘れ，かつ，Webブラウザに保存しているパスワード情報も使用できないリスクを想定して，緊急と判断した場合には，認証情報を入力せずに，利用者は普段どおりにシステムを利用できるようにし，可用性を高める。”

災害などの緊急時に認証なしで使えるようにする仕組みとして、公衆無線LAN（00000JAPANなど）の開放機能や"救済パスワード"がありますが、これらはリスクベース認証ではありません。

☆☆☆

パケットフィルタリング型ファイアウォールのフィルタリングルールを用いて，本来必要なサービスに影響を及ぼすことなく防げるものはどれか。

平成30年春期　問44
135問目／選択範囲の問題数237問

ア	外部に公開していないサーバへのアクセス
イ	サーバで動作するソフトウェアの脆弱性を突く攻撃
ウ	電子メールに添付されたファイルに含まれるマクロウイルスの侵入
エ	不特定多数のIoT機器から大量のHTTPリクエストを送り付けるDDoS攻撃

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ア　“あなたの解答：ア”

❑解説

パケットフィルタリングとは、通過するパケットのIPアドレス(送信元・送信先)やポート番号、通信の方向などの情報をもとに中継の可否を判断する方式です。ただし、パケットのペイロード(データ部分)に関してはチェックを行いません。

ア “外部に公開していないサーバへのアクセス”

正しい。外部に公開していないサービス、若しくは業務に不要なサービスのポートへの通信を遮断するルールを設定することで、必要なサービスに影響を与えることなく不正アクセスを防ぐことが可能です。

イ “サーバで動作するソフトウェアの脆弱性を突く攻撃”

IPアドレスとポート番号の組みを指定することで、脆弱性のあるソフトウェアへの攻撃を目的とする通信を遮断できますが、正当な処理要求についても遮断してしまうことになるため不適切です。

ウ “電子メールに添付されたファイルに含まれるマクロウイルスの侵入”

電子メールを転送するSMTP(TCP/25)に対する攻撃を防ぐことはできますが、それと同時に業務に必要なメール転送もできなくなってしまうため不適切です。

エ “不特定多数のIoT機器から大量のHTTPリクエストを送り付けるDDoS攻撃”

「ウ」と同様に、HTTP(TCP/80)宛の通信を遮断してしまうと、外部の利用者がWebサービスを利用できなくなってしまうため不適切です。

☆☆☆

インターネットとの接続において，ファイアウォールのNAPT機能によるセキュリティ上の効果はどれか。

令和元年秋期　問37
136問目／選択範囲の問題数237問

ア	DMZ上にある公開Webサーバの脆弱性を突く攻撃からWebサーバを防御できる。
イ	インターネットから内部ネットワークへの侵入を検知し，検知後の通信を遮断できる。
ウ	インターネット上の特定のWebサービスを利用するHTTP通信を検知し，遮断できる。
エ	内部ネットワークからインターネットにアクセスする利用者PCについて，インターネットからの不正アクセスを困難にすることができる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

エ　“あなたの解答：ウ”

❑解説

NAPT(Network Address Port Translation)は、プライベートIPアドレスとグローバルIPアドレスを1対1で相互変換するNATの考え方に、ポート番号でのクライアント識別を組み合わせた技術です。

NAPTが有効になっている場合、利用者PCがインターネットにアクセスしようとすると、NAPT機能をもつ機器等はプライベートIPアドレスをグローバルIPアドレスに変換すると同時に、送信元ポート番号を未使用の別の番号に書き換えてからインターネットに送出します(②)。そしてインターネットから内部ネットワークへのパケットが返ってくると、その送信先ポート番号を見て、送信先IPアドレスと送信先ポート番号を適切に書き換えて利用者PCに届けます(⑤)。

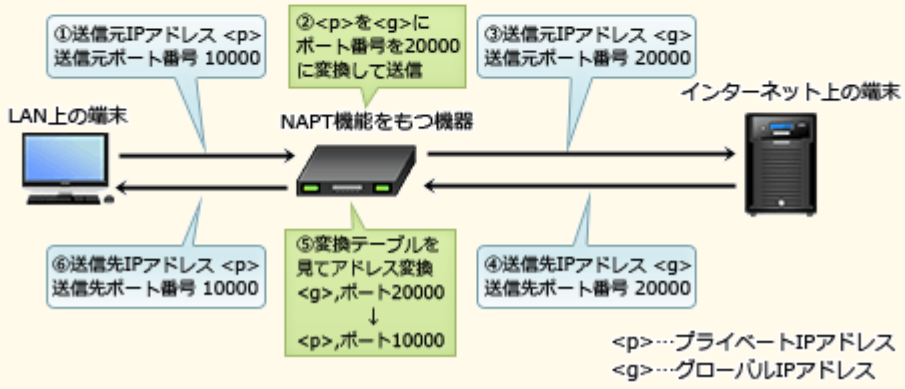


図　NAPTの仕組み

NAPT機能をもつ機器では、インターネット接続に使用中のポート番号を記憶しています。このため攻撃者が内部ネットワークへの不正アクセスを試みても、記憶しているポート番号以外に宛てたパケットは宛先不明としてすべて破棄されます。しかもNAPTで割り振られるポート番号は数万種あり、セッション確立の度に異なるため、攻撃者がピンポイントでポート番号を指定して利用者PCに不正アクセスすることは困難です。このように、NAPT機能には内部ネットワークを秘匿できるというセキュリティ上の副次的効果があります。

したがって「エ」の記述が適切です。

☆☆☆

NISTの定義によるクラウドサービスモデルのうち，クラウド利用企業の責任者がセキュリティ対策に関して表中の項番1と2の責務を負うが，項番3～5の責務を負わないものはどれか。

項番	責　務
1	アプリケーションに対して，データのアクセス制御と暗号化の設定を行う。
2	アプリケーションに対して，セキュアプログラミングと脆弱性診断を行う。
3	DBMS に対して，修正プログラム適用と権限設定を行う。
4	OS に対して，修正プログラム適用と権限設定を行う。
5	ハードウェアに対して，アクセス制御と物理セキュリティ確保を行う。

平成27年春期　問42
137問目／選択範囲の問題数237問

ア HaaS　イ IaaS　ウ PaaS　エ SaaS

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ウ　“あなたの解答：エ”

❑解説

NIST(米国国立標準技術研究所)による文書「クラウドコンピューティングの定義」では、クラウドコンピューティングのサービスモデル「SaaS」「PaaS」「IaaS」について以下のように定義しています。

SaaS(Software as a Service)

サービスの形で提供されるソフトウェア。
利用者に提供される機能は、クラウドのインフラストラクチャ上で稼動しているプロバイダ由来のアプリケーションである。アプリケーションには、クライアントの様々な装置から、ウェブブラウザのようなシンクライアント型インターフェイス（例えばウェブメール）、またはプログラムインターフェイスのいずれかを通じてアクセスする。**ユーザーは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、各アプリケーション機能ですら、管理したりコントロールしたりすることはない**。ただし、ユーザーに固有のアプリケーションの構成の設定はその例外となろう。

PaaS(Platform as a Service)

サービスの形で提供されるプラットフォーム。
利用者に提供される機能は、クラウドのインフラストラクチャ上にユーザーが開発したまたは購入したアプリケーションを実装することであり、そのアプリケーションはプロバイダがサポートするプログラミング言語、ライブラリ、サービス、およびツールを用いて生み出されたものである。**ユーザーは基盤にあるインフラストラクチャを、ネットワークであれ、サーバーであれ、オペレーティングシステムであれ、ストレージであれ、管理したりコントロールしたりすることはない。一方ユーザーは自分が実装したアプリケーションと、場合によってはそのアプリケーションをホストする環境の設定についてコントロール権を持つ。**

IaaS(Infrastructure as a Service)

サービスの形で提供されるインフラストラクチャ。
利用者に提供される機能は、演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースを配置することであり、そこで、ユーザーはオペレーティングシステムやアプリケーションを含む任意のソフトウェアを実装し走らせることができる。**ユーザーは基盤にあるインフラストラクチャを管理したりコントロールしたりすることはないが、オペレーティングシステム、ストレージ、実装されたアプリケーションに対するコントロール権を持ち**、場合によっては特定のネットワークコンポーネント機器（例えばホストファイアウォール）についての限定的なコントロール権を持つ。
※HaaS(Hardware as a Service)と同義

で強調した部分が利用者の責務について記述した部分です。各サービスの特徴をシンプルにまとめると次のようになります。

SaaS	事業者はアプリケーション以下を提供。利用者は機能を使い、 アプリケーションにおける設定(カスタマイズ)も可能。
PaaS	事業者はミドルウェア以下を提供。利用者はアプリケーションを用意し、 ミドルウェアにおける設定(カスタマイズ)も可能。
IaaS	1.事業者はOS以下を提供。利用者はミドルウェア以上を用意し、 OSにおける設定(カスタマイズ)も可能。 2.事業者はハードウェア、ネットワークを提供。利用者はOS以上を用意。

- 利用者が構築したアプリケーションについての責務を持つ
- OSやDBMSについて一部の権限は認められるが修正プログラムの適用までの責務はない

というレベルのクラウドサービスモデルは「PaaS」になります。

☆

デジタル署名などに用いるハッシュ関数の特徴はどれか。

平成24年春期　問38
138問目／選択範囲の問題数237問

ア　同じメッセージダイジェストを出力する異なる二つのメッセージが，容易に求められる。

イ　メッセージが異なっていても，メッセージダイジェストは同じである。

ウ　メッセージダイジェストからメッセージを復元することは困難である。

エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：ウ”

❑解説

ハッシュ関数は、任意の長さのデータを入力すると固定長のビット列(ハッシュ値、メッセージダイジェスト)を返す関数で、次のような特徴を持っています。

- 入力データが同じであれば、常に同じメッセージダイジェストが生成される。
- 入力データが少しでも異なっていれば生成されるメッセージダイジェストは大きく異なったものになる。
- メッセージダイジェストから元の入力データを再現することが困難である。
- 異なる入力データから同じメッセージダイジェストが生成される可能性が非常に低い。

このような特徴を応用して、ハッシュ関数は通信経路での改ざん検知、ユーザー認証、デジタル署名などの場面で利用されています。

主なハッシュ関数にはMD4(128ビット)、MD5(128ビット)、SHA1(160ビット)、SHA2(224～512ビット)などがあります。しかし、この中でMD4、MD5、SHA1は安全性が低くなってしまったため、現在ではより強度のあるSHA2の使用が推奨されています。

ア “同じメッセージダイジェストを出力する異なる二つのメッセージが，容易に求められる。”

同一のハッシュ値が生成される可能性は非常に低く、ハッシュ値から入力データへの逆算も難しいため求めることは困難です。

イ “メッセージが異なっていても，メッセージダイジェストは同じである。”

メッセージが少しでも異なっていれば生成されるメッセージダイジェストは大きく異なったものになります。

ウ “メッセージダイジェストからメッセージを復元することは困難である。”

正しい。ハッシュ関数は一方向性のアルゴリズムであるため結果から入力元を復元することは容易ではありません。

エ “メッセージダイジェストの長さはメッセージの長さによって異なる。”

使用するハッシュ関数が同じであれば生成されるメッセージダイジェストの長さは常に一定です。

☆

緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は，どれに分類されるか。

平成23年特別　問42
139問目／選択範囲の問題数237問

ア	ソーシャルエンジニアリング	イ	トロイの木馬
ウ	パスワードクラック	エ	踏み台攻撃

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：イ”

❑解説

ソーシャルエンジニアリング(Social Engineering)は、技術的な方法ではなく、人の心理的な弱みやミスに付け込んでパスワードなどの秘密情報を不正に取得する行為の総称です。

ソーシャルエンジニアリングの例として以下の行為があります。

なりすまし

管理者や関係者になりすまして秘密情報を不正取得する

ショルダーハッキング

モニター画面やキーボード操作を利用者の背後から盗み見て、ログイン情報等を不正取得する

トラッシング（スカベンジング）

ゴミ箱に捨てられているメモや書類を漁って秘密情報を不正取得する

のぞき見

FAXやプリンターに残された印刷物、オフィス内のメモ・付箋、机の上に放置された書類等から秘密情報を不正取得する

ア “ソーシャルエンジニアリング”

正しい。ソーシャルエンジニアリングの手口である「なりすまし」に該当します。

イ “トロイの木馬”

トロイの木馬は、一見正常に動作しているように見えますが、実際には裏でユーザーのキーストロークを盗んだり、バックドアとして機能したりするように巧妙につくりかえられたプログラムのことです。

ウ “パスワードクラック”

パスワードクラックは、設定されているパスワードを、様々な方法で不正に破ろうとする行為です。

エ “踏み台攻撃”

踏み台攻撃は、インターネット上にある多数のコンピュータに対して、あらかじめ攻撃プログラムを仕掛けておき、攻撃者からの命令で対象のサーバを攻撃させる手法です。意識しないうちに攻撃者から操作され、攻撃に加担させられてしまうことを「踏み台にされる」といいます。

☆

データベースで管理されるデータの暗号化に用いることができ，かつ，暗号化と復号とで同じ鍵を使用する暗号化方式はどれか。

平成28年秋期　問39
140問目／選択範囲の問題数237問

ア	AES	イ	PKI	ウ	RSA	エ	SHA-256

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

「暗号化と復号とで同じ鍵を使用する」という記述から、共通鍵暗号方式であることがわかります。共通鍵暗号方式であるのはAESのみです。

ア “AES”

正しい。**AES**(Advanced Encryption Standard)は、アメリカ合衆国の標準暗号規格として制定された共通鍵暗号方式です。暗号化と復号に同じ鍵を使用するため設問の条件を満たします。

イ “PKI”

Public Key Infrastructureの略で公開鍵基盤のことです。暗号方式ではないため不適切です。

ウ “RSA”

RSAは公開鍵暗号方式なので、暗号化と復号に異なる鍵を使用します。

エ “SHA-256”

SHA-256は、入力値をもとに256ビットのハッシュ値を生成するアルゴリズムです。ハッシュ化は一方向性の変換なのでデータの暗号化は行えますがハッシュ値から元のデータへの復号は困難です。

☆

パスワードクラック手法の一種である，レインボーテーブル攻撃に該当するものはどれか。

令和5年秋期　問36
141問目／選択範囲の問題数237問

ア　何らかの方法で事前に利用者IDと平文のパスワードのリストを入手しておき，複数のシステム間で使い回されている利用者IDとパスワードの組みを狙って，ログインを試行する。

イ　パスワードに成り得る文字列の全てを用いて，総当たりでログインを試行する。

ウ　平文のパスワードとハッシュ値をチェーンによって管理するテーブルを準備しておき，それを用いて，不正に入手したハッシュ値からパスワードを解読する。

エ　利用者の誕生日，電話番号などの個人情報を言葉巧みに聞き出して，パスワードを類推する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

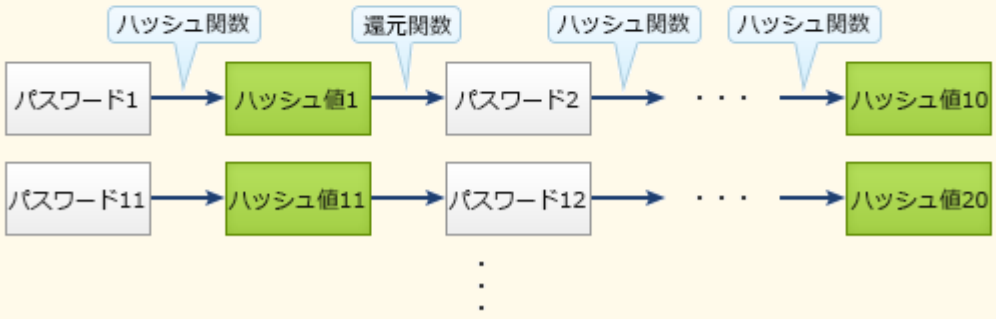
❑正解

ウ　“あなたの解答：ウ”

❑解説

レインボーテーブル攻撃は、ハッシュ値からパスワードを特定するための逆引き表（レインボーテーブル）を用いて、ハッシュ値の元となったパスワードを効率的に解読する手法です。

レインボーテーブルは、使用される文字種と文字数の組合せごとに作成されます。レインボーテーブル内では、パスワードとハッシュ値を数多くのチェーンとして管理しており、実際のテーブルにはチェーンの先頭であるパスワードと最後のハッシュ値だけを格納しておきます。



※還元関数…ハッシュ値からフォーマットを満たすパスワード文字列を生成する関数

図　レインボーテーブルのチェーン

先頭のパスワード	最後のハッシュ値
パスワード1	ハッシュ値10
パスワード11	ハッシュ値20
パスワード21	ハッシュ値30
パスワード31	ハッシュ値40
⋮	⋮

図　レインボーテーブル

解読対象のハッシュ値を入手したら、チェーンの各位置からチェーン化で行ったのと同様の計算を施し、チェーンの最後のハッシュ値を計算します。これがレインボーテーブルに格納されているハッシュ値のいずれかと一致すれば、対応するパスワードが存在するチェーンがわかる仕組みになっています。

ア "何らかの方法で事前に利用者IDと平文のパスワードのリストを入手しておき，複数のシステム間で使い回されている利用者IDとパスワードの組みを狙って，ログインを試行する。"

パスワードリスト攻撃の説明です。

イ "パスワードに成り得る文字列の全てを用いて，総当たりでログインを試行する。"

総当たり攻撃(ブルートフォースアタック)の説明です。

ウ "平文のパスワードとハッシュ値をチェーンによって管理するテーブルを準備しておき，それを用いて，不正に入手したハッシュ値からパスワードを解読する。"

正しい。レインボーテーブル攻撃の説明です。

エ "利用者の誕生日，電話番号などの個人情報を言葉巧みに聞き出して，パスワードを類推する。"

類推攻撃の説明です。

☆☆

暗号学的ハッシュ関数における原像計算困難性，つまり一方向性の性質はどれか。

令和3年春期　問40
142問目／選択範囲の問題数237問

ア　あるハッシュ値が与えられたとき，そのハッシュ値を出力するメッセージを見つけることが計算量的に困難であるという性質

イ　入力された可変長のメッセージに対して，固定長のハッシュ値を生成できるという性質

ウ　ハッシュ値が一致する二つの相異なるメッセージを見つけることが計算量的に困難であるという性質

エ　ハッシュの処理メカニズムに対して，外部からの不正な観測や改変を防御できるという性質

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

ハッシュ関数は、任意の長さのデータを入力すると固定長のビット列(ハッシュ値，メッセージダイジェスト)を返す関数で、次のような性質を持っています。

- 入力データが同じであれば、常に同じメッセージダイジェストが生成される。
- 入力データが少しでも異なっていれば生成されるメッセージダイジェストは大きく異なったものになる。
- メッセージダイジェストから元の入力データを再現することが困難である。
- 異なる入力データから同じメッセージダイジェストが生成される可能性が非常に低い。

このうち3つ目の「あるメッセージのハッシュ値を得ることは簡単にできるが、その逆は事実上できない」というハッシュ関数の一方向性を「原像計算困難性」といいます。したがって「ア」が適切な説明となります。

ちなみに「ウ」は、衝突発見困難性(強衝突耐性)を説明した文です。

☆☆☆

テンペスト技術の説明とその対策として，適切なものはどれか。

平成20年秋期　問75
143問目／選択範囲の問題数237問

ア　ディスプレイやケーブルなどから放射される電磁波を傍受し，内容を観察する技術であり，電磁波遮断が施された部屋に機器を設置することによって対抗する。

イ　データ通信の途中でパケットを横取りし，内容を改ざんする技術であり，デジタル署名による改ざん検知の仕組みを実装することによって対抗する。

ウ　マクロウイルスにおいて使われる技術であり，ウイルス対策ソフトを導入し，最新の定義ファイルを適用することによって対抗する。

エ　無線LANの信号から通信内容を傍受し，解析する技術であり，通信パケットを暗号化することによって対抗する。

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ア　“あなたの解答：ア”

❑解説

テンペスト技術は、モニターやキーボード，ネットワークケーブルなどから放射されている微弱な電磁波を傍受し解析することで元の情報の再現を試みる技術です。一般に知られている実験では、ブラウン管ディスプレイやケーブルから発生する電磁波を3m離れた地点で傍受して、表示されている画像を再現した例があります。

傍受を防ぐための対策としては、ブラウン管ディスプレイから液晶ディスプレイに切り替える，ケーブル等を電磁シールドで包む，PCを使用する部屋全体をシールドしてしまうなど、機器から放射される電磁波を極めて少量に抑える方法が効果的です。

☆☆☆

クロスサイトスクリプティング対策に該当するものはどれか。

平成30年秋期　問41
144問目／選択範囲の問題数237問

ア　WebサーバでSNMPエージェントを常時稼働させることによって，攻撃を検知する。

イ　WebサーバのOSにセキュリティパッチを適用する。

ウ　Webページに入力されたデータの出力データが，HTMLタグとして解釈されないように処理する。

エ　許容量を超えた大きさのデータをWebページに入力することを禁止する。

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

ウ　“あなたの解答：イ”

❑解説

クロスサイトスクリプティング(XSS)は、動的にWebページを生成するアプリケーションのセキュリティ上の不備を意図的に利用して、悪意のあるスクリプトを混入させることで、攻撃者が仕込んだ操作を実行させたり、別のサイトを横断してユーザーのクッキーや個人情報を盗んだりする攻撃手法です。

クロスサイトスクリプティングは、攻撃者が送り込んでくる文字列がHTMLドキュメントの一部となるように合成されて、その部分がブラウザによってスクリプトとして解釈される構文となることによって成立します。よって、プログラム中のデータをHTMLとして出力する際に、HTMLで特別な意味をもつ文字(<,>,",',&など)を実体参照に置き換えて無害化したり、HTMLタグを削除したりすることによりスクリプトとして解釈されないようにすることが重要です。

ア　“WebサーバでSNMPエージェントを常時稼働させることによって，攻撃を検知する。”

不正アクセス対策に該当します。XSSは正常なHTTP(S)パケットとしてWebサーバに届けられるので、SNMPエージェントで監視しても攻撃を検知することはできません。

イ　“WebサーバのOSにセキュリティパッチを適用する。”

OSのセキュリティホールを突く攻撃への対策に該当します。XSS脆弱性はWebアプリケーションの実装に基因するものなので、OSのアップデートは対策にはなりません。

ウ　“Webページに入力されたデータの出力データが，HTMLタグとして解釈されないように処理する。”

正しい。クロスサイトスクリプティング対策に該当します。

エ　“許容量を超えた大きさのデータをWebページに入力することを禁止する。”

バッファオーバーフロー対策に該当します。

☆☆☆

JPCERTコーディネーションセンターとIPAとが共同で運営するJVNの目的として，最も適切なものはどれか。

令和4年秋期　問40
145問目／選択範囲の問題数237問

ア　ソフトウェアに内在する脆弱性を検出し，情報セキュリティ対策に資する。

イ　ソフトウェアの脆弱性関連情報とその対策情報とを提供し，情報セキュリティ対策に資する。

ウ　ソフトウェアの脆弱性に対する汎用的な評価手法を確立し，情報セキュリティ対策に資する。

エ　ソフトウェアの脆弱性のタイプを識別するための基準を提供し，情報セキュリティ対策に資する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

イ　“あなたの解答：イ”

❑解説

JVNは(Japan Vulnerability Notes)は、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする**脆弱性対策情報ポータルサイト**です。脆弱性関連情報の受付と安全な流通を目的とした「情報セキュリティ早期警戒パートナーシップ」に基いて、2004年7月よりJPCERT コーディネーションセンターと独立行政法人情報処理推進機構(IPA)が共同で運営しています。
JVNに掲載されている情報は、脆弱性が確認された製品とバージョン、脆弱性の詳細や分析結果、製品開発者によって提供された対策や関連情報へのリンクなどで、対策にはパッチだけではなく回避策（ワークアラウンド）が掲載される事もあります（https://jvn.jp/nav/jvn.htmlより引用）。

したがって適切な説明は「イ」です。

ア “ソフトウェアに内在する脆弱性を検出し，情報セキュリティ対策に資する。”

MyJVNバージョンチェッカなどの説明です。

イ “ソフトウェアの脆弱性関連情報とその対策情報とを提供し，情報セキュリティ対策に資する。”

正しい。JVNの説明です。

ウ “ソフトウェアの脆弱性に対する汎用的な評価手法を確立し，情報セキュリティ対策に資する。”

CVSS(Common Vulnerability Scoring System)の説明です。

エ “ソフトウェアの脆弱性のタイプを識別するための基準を提供し，情報セキュリティ対策に資する。”

CWE(Common Weakness Enumeration)の説明です。

☆☆

SPF(Sender Policy Framework)を利用する目的はどれか。

平成27年春期　問44
146問目／選択範囲の問題数237問

ア	HTTP通信の経路上での中間者攻撃を検知する。
イ	LANへのPCの不正接続を検知する。
ウ	内部ネットワークへの不正侵入を検知する。
エ	メール送信のなりすましを検知する。

❑分類

テクノロジ系 » セキュリティ » セキュリティ実装技術

❑正解

エ　“あなたの解答：エ”

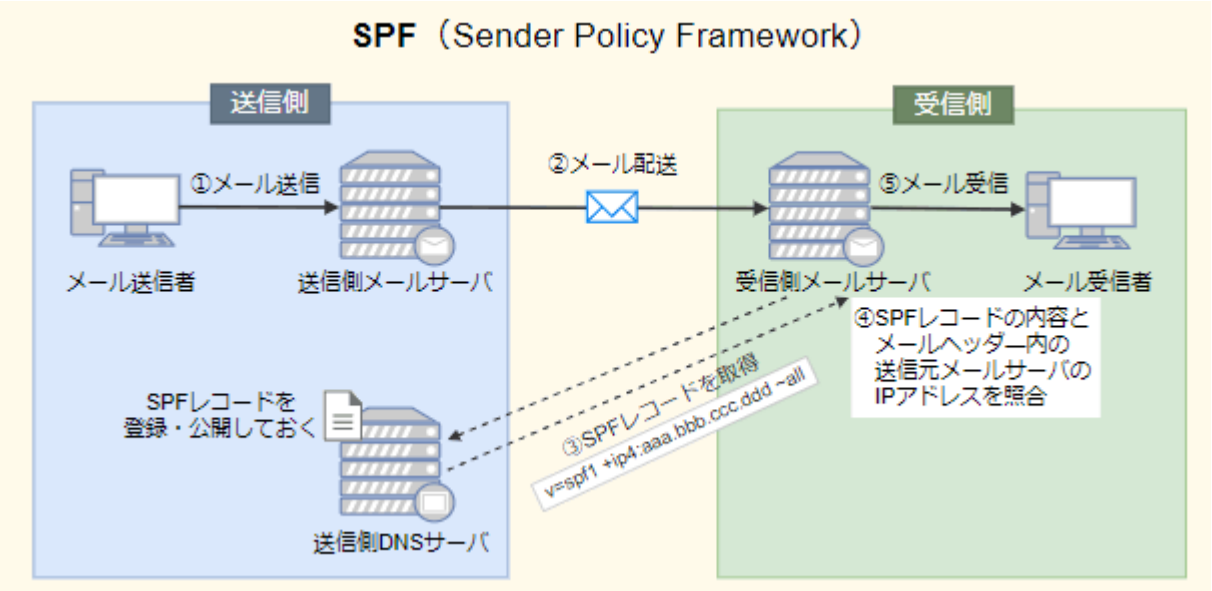
❑解説

SPF(Sender Policy Framework)は、メールを送信しようとしてきたメールサーバのIPアドレス情報を検証することで、正規のサーバからのメール送信であるかどうか確認することができる技術です。受信メールサーバ側がメールの送信元ドメインを管理するDNSサーバに問い合わせ、返されたIPアドレスが送信元メールサーバのIPアドレスと一致するかどうかでなりすましを検知します。

したがって「エ」が正解です。

SPFで送信元IPアドレスの検証を行う手順は以下のようになっています。

① 送信側は、送信側ドメインのDNSサーバのSPFレコード(又はTXTレコード)に正当なメールサーバのIPアドレスやホスト名を登録し、公開しておく。
② 送信側から受信側へ、SMTPメールが送信される。
③ 受信側メールサーバは、受信側ドメインのDNSサーバを通じて、MAIL FROMコマンドに記載された送信者メールアドレスのドメインを管理するDNSサーバに問い合わせ、SPF情報を取得する。
④ SPF情報との照合でSMTP接続してきたメールサーバのIPアドレスの確認に成功すれば、正当なドメインから送信されたと判断する。



☆☆☆

サイバーレスキュー隊(J-CRAT)の役割はどれか。

平成29年秋期　問42
147問目／選択範囲の問題数237問

ア　外部からのサイバー攻撃などの情報セキュリティ問題に対して，政府横断的な情報収集や監視機能を整備し，政府機関の緊急対応能力強化を図る。

イ　重要インフラに関わる業界などを中心とした参加組織と秘密保持契約を締結し，その契約の下に提供された標的型サイバー攻撃の情報を分析及び加工することによって，参加組織間で情報共有する。

ウ　セキュリティオペレーション技術向上，オペレータ人材育成，及びサイバーセキュリティに関係する組織・団体間の連携を推進することによって，セキュリティオペレーションサービスの普及とサービスレベルの向上を促す。

エ　標的型サイバー攻撃を受けた組織や個人から提供された情報を分析し，社会や産業に重大な被害を及ぼしかねない標的型サイバー攻撃の把握，被害の分析，対策の早期着手の支援を行う。

❑分類

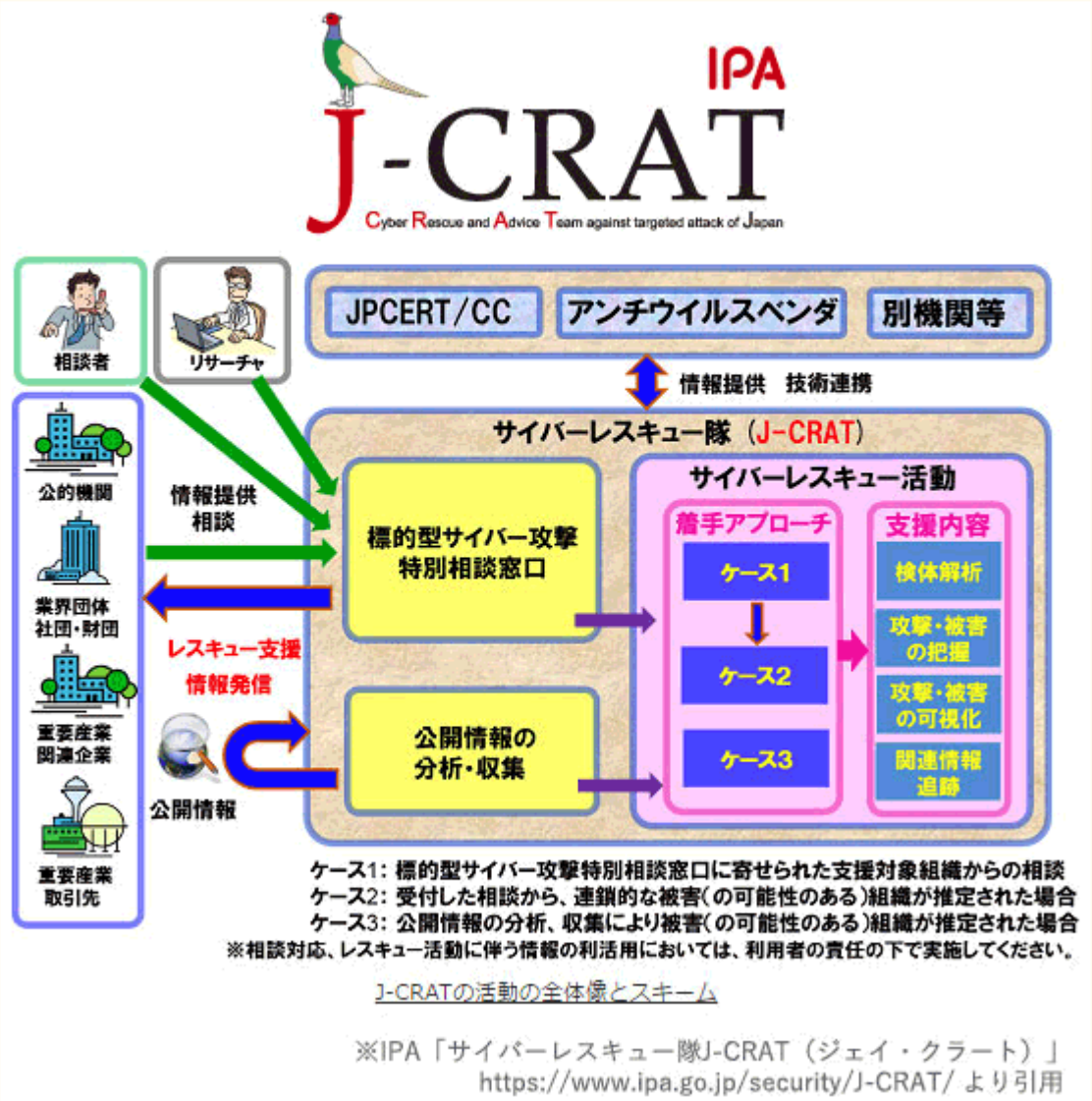
テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

エ　“あなたの解答：エ”

❑解説

サイバーレスキュー隊(J-CRAT)は、「標的型サイバー攻撃特別相談窓口」にて受け付けた相談や情報に対して調査分析を実施し、JPCERT/CCやセキュリティベンダー等と連携して助言や支援および情報共有を行うことで被害の低減と攻撃の拡大防止を図るIPAの取り組みです。



J-CRATの活動の全体像とスキーム

※IPA「サイバーレスキュー隊J-CRAT（ジェイ・クラート）」
https://www.ipa.go.jp/security/J-CRAT/ より引用

ア “外部からのサイバー攻撃などの情報セキュリティ問題に対して，政府横断的な情報収集や監視機能を整備し，政府機関の緊急対応能力強化を図る。”

内閣サイバーセキュリティセンター(NISC)の役割です。

イ “重要インフラに関わる業界などを中心とした参加組織と秘密保持契約を締結し，その契約の下に提供された標的型サイバー攻撃の情報を分析及び加工することによって，参加組織間で情報共有する。”

サイバー情報共有イニシアティブ(J-CSIP)の役割です。

ウ “セキュリティオペレーション技術向上，オペレータ人材育成，及びサイバーセキュリティに関係する組織・団体間の連携を推進することによって，セキュリティオペレーションサービスの普及とサービスレベルの向上を促す。”

日本セキュリティオペレーション事業者協議会(ISOG-J)の役割です。

エ “標的型サイバー攻撃を受けた組織や個人から提供された情報を分析し，社会や産業に重大な被害を及ぼしかねない標的型サイバー攻撃の把握，被害の分析，対策の早期着手の支援を行う。”

正しい。サイバーレスキュー隊(J-CRAT)の役割です。

☆☆☆

水飲み場型攻撃(Watering Hole Attack)の手口はどれか。

平成29年春期　問40
148問目／選択範囲の問題数237問

ア　アイコンを文書ファイルのものに偽装した上で，短いスクリプトを埋め込んだショートカットファイル(LNKファイル)を電子メールに添付して標的組織の従業員に送信する。

イ　事務連絡などのやり取りを行うことで，標的組織の従業員の気を緩めさせ，信用させた後，攻撃コードを含む実行ファイルを電子メールに添付して送信する。

ウ　標的組織の従業員が頻繁にアクセスするWebサイトに攻撃コードを埋め込み，標的組織の従業員がアクセスしたときだけ攻撃が行われるようにする。

エ　ミニブログのメッセージにおいて，ドメイン名を短縮してリンク先のURLを分かりにくくすることによって，攻撃コードを埋め込んだWebサイトに標的組織の従業員を誘導する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：イ”

❑解説

水飲み場型攻撃は、特定の組織や人に狙いを定める標的型攻撃の一つで、標的ユーザーが良く利用するWebサイトにドライブバイダウンロードのコードなどを仕込み、アクセスした標的ユーザーにマルウェアやウイルスを感染させる攻撃です。
一般的には標的対象のみに感染するマルウェアが用いられ、標的以外の第三者がアクセスしても何も起こらないため、脅威の存在やWebサイトの改ざんなどが発覚しにくくなっています。

「水飲み場型攻撃」の名称は攻撃者をライオンなどの肉食獣に、標的ユーザーが良く利用するWebサイトを草食獣が集まる水飲み場に見立て、肉食獣が水飲み場に来る獲物を待ち伏せする様子になぞらえています。

したがって正しい説明は「ウ」です。その他の選択肢も標的型攻撃の手法ですが、水飲み場攻撃の記述としては不適切です。

ドライブバイダウンロード

Webサイトにマルウェアやウイルスを仕込んでおき、利用者がアクセスすると同時に秘密裏に利用者のコンピュータにそれらをダウンロードさせたり実行させる攻撃手法

☆☆☆

ブラウザからWebサーバにアクセスするシステムのセキュリティに関する記述のうち，適切なものはどれか。

平成17年秋期　問76
149問目／選択範囲の問題数237問

ア　CGI又はサーブレットによって生成されたHTML文書は動的に変化するので，プロキシサーバでのキャッシュの内容が，本来の利用者以外に開示されることはない。

イ　SSLを使用すれば，通信経路上にプロキシサーバが存在していても，各利用者とWebサーバとの間での参照情報が，本来の利用者以外に開示されることはない。

ウ　複数の利用者が同一のパソコンを利用する場合，最初にHTTP基本認証を利用したログイン操作を行うようにすれば，ブラウザを起動したまま利用者が交代しても，本来の利用者以外に情報が開示されることはない。

エ　リバースプロキシは静的コンテンツのキャッシュができないので，それを使ってもクライアントへの応答時間が改善されることはない。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

イ　“あなたの解答：エ”

❑解説

ア “CGI又はサーブレットによって生成されたHTML文書は動的に変化するので，プロキシサーバでのキャッシュの内容が，本来の利用者以外に開示されることはない。”

本来の利用者以外でも同じURLでアクセスすればキャッシュの内容を知られてしまいます。

イ “SSLを使用すれば，通信経路上にプロキシサーバが存在していても，各利用者とWebサーバとの間での参照情報が，本来の利用者以外に開示されることはない。”

正しい。SSLではクライントのWebブラウザと通信相手のWebサーバ間の通信を暗号化するので、間にプロキシサーバが存在しても内容が漏えいすることはありません。
クライアント(Webサーバ)からSSLの接続要求を受け取ったプロキシは、通信の内容には介入せずデータをコピーしてWebサーバ(クライアント)に送信します。この動作を**SSLトンネリング**と呼びます。

ウ “複数の利用者が同一のパソコンを利用する場合，最初にHTTP基本認証を利用したログイン操作を行うようにすれば，ブラウザを起動したまま利用者が交代しても，本来の利用者以外に情報が開示されることはない。”

HTTP基本認証(Basic認証)では、一度認証されればブラウザを閉じるまではその認証はずっと有効なので、認証状態で放置されているブラウザが別ユーザーに使用されると非公開の情報を知られてしまう可能性があります。

エ “リバースプロキシは静的コンテンツのキャッシュができないので，それを使ってもクライアントへの応答時間が改善されることはない。”

リバースプロキシは静的コンテンツをキャッシュすることができます。キャッシュが存在し、有効期限が切れていない場合は、Webサーバに問い合わせることなくキャッシュをクライアントに返すので応答速度の改善が望めます。

☆

フィッシング(phishing)による被害はどれか。

平成23年秋期　問39
150問目／選択範囲の問題数237問

ア　インターネットからソフトウェアをダウンロードしてインストールしたところ，設定したはずのない広告がデスクトップ上に表示されるようになった。

イ　インターネット上の多数のコンピュータから，公開しているサーバに一斉にパケットが送り込まれたので，当該サーバが一時使用不能になった。

ウ　知人から送信されてきた電子メールに添付されていたファイルを実行したところ，ハードディスク上にあった全てのファイルを消失してしまった。

エ　"本人情報の再確認が必要なので入力してください"という電子メールで示されたURLにアクセスし，個人情報を入力したところ，詐取された。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

エ　“あなたの解答：エ”

❑解説

フィッシング(phishing)は、銀行やクレジットカード会社，ショッピングサイトなどの有名企業を装ったメールを送付し、個人情報を不正に搾取する行為です。メール本文内のハイパーリンクをクリックさせることで、本物そっくりな偽のWebサイトに誘導し、設置してある入力フォームに入力した情報などの個人情報を不正に収集するインターネットを用いた詐欺の一種です。

ア “インターネットからソフトウェアをダウンロードしてインストールしたところ，設定したはずのない広告がデスクトップ上に表示されるようになった。”

スパイウェアの１つであるアドウェアの説明です。

イ “インターネット上の多数のコンピュータから，公開しているサーバに一斉にパケットが送り込まれたので，当該サーバが一時使用不能になった。”

DDoS攻撃(Distributed Denial of Service attack，分散型サービス拒否攻撃)の説明です。

ウ “知人から送信されてきた電子メールに添付されていたファイルを実行したところ，ハードディスク上にあった全てのファイルを消失してしまった。”

電子メールによるウィルス被害の説明です。

エ “”本人情報の再確認が必要なので入力してください”という電子メールで示されたURLにアクセスし，個人情報を入力したところ，詐取された。”

正しい。