【応用_午前_過去問】セキュリティ⑤

チャレンジレスポンス認証方式に該当するものはどれか。

令和4年春期　問38
201問目／選択範囲の問題数237問

ア　固定パスワードを，TLSによる暗号通信を使い，クライアントからサーバに送信して，サーバで検証する。

イ　端末のシリアル番号を，クライアントで秘密鍵を使って暗号化し，サーバに送信して，サーバで検証する。

ウ　トークンという装置が自動的に表示する，認証のたびに異なる数字列をパスワードとしてサーバに送信して，サーバで検証する。

エ　利用者が入力したパスワードと，サーバから受け取ったランダムなデータとをクライアントで演算し，その結果をサーバに送信して，サーバで検証する。

❑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：ア”

❑解説

チャレンジレスポンス方式は、通信経路上に固定パスワードを流さないようにすることで、盗聴によるパスワードの漏えいやリプレイアタックを防止する認証方式です。

チャレンジレスポンス方式では以下の手順で認証を行います。

(1) サーバは、クライアントから要求があるたびに異なる乱数値(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と(1)でサーバから送られた"チャレンジ"から所定の方法でレスポンスを計算する。

(3) クライアントは、(2)で生成した"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。

(4) 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と(1)で保持していた"チャレンジ"を用いてクライアントと同じ手順でレスポンスを生成する（レスポンス照合データ）。

(5) サーバは、"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"を比較し、両者が一致すれば認証成功とする。

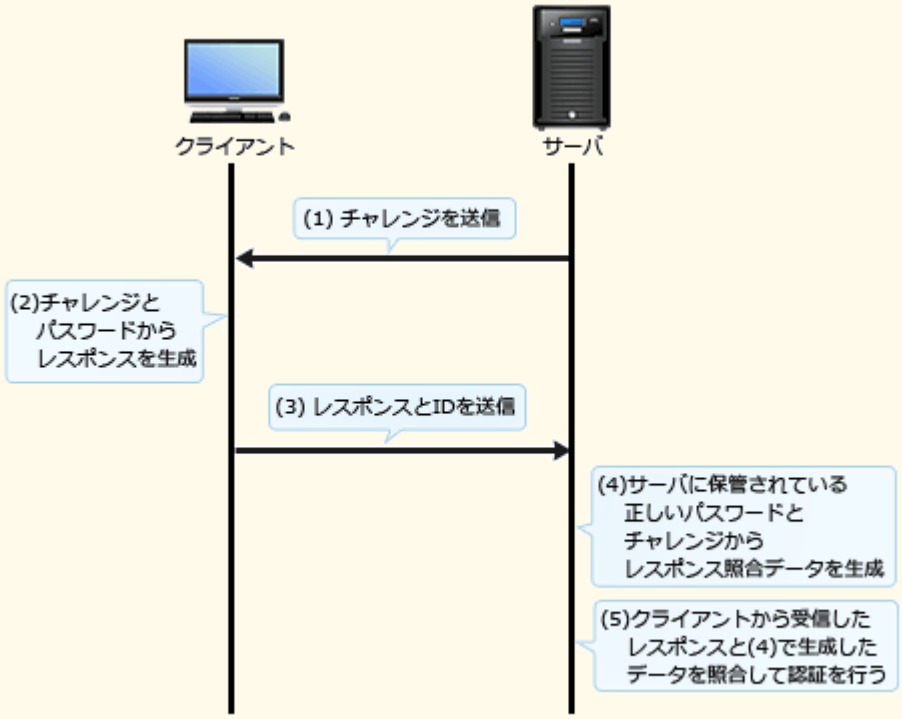


図　チャレンジレスポンス方式の手順

ア “固定パスワードを，TLSによる暗号通信を使い，クライアントからサーバに送信して，サーバで検証する。”

チャレンジレスポンス方式では、固定パスワードとサーバから送信された乱数(チャレンジ)を組み合わせたものをハッシュ化又は暗号化してサーバに返信します。

イ “端末のシリアル番号を，クライアントで秘密鍵を使って暗号化し，サーバに送信して，サーバで検証する。”

端末のシリアル番号は送信しません。端末ごとに固有の番号を使用するといつも同じ認証データが使われることになるので、リプレイアタックを受ける可能性があります。

ウ “トークンという装置が自動的に表示する，認証のたびに異なる数字列をパスワードとしてサーバに送信して，サーバで検証する。”

時刻同期式ワンタイムパスワードの説明です。チャレンジレスポンス方式ではトークンは不要です。

エ “利用者が入力したパスワードと，サーバから受け取ったランダムなデータとをクライアントで演算し，その結果をサーバに送信して，サーバで検証する。”

正しい。チャレンジレスポンス認証方式の特徴です。

Xさんは，Yさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容は秘密にする必要があるので，公開かぎ暗号方式を使って暗号化して送信したい。電子メールの内容を暗号化するのに使用するかぎはどれか。

平成17年春期　問70
202問目／選択範囲の問題数237問

ア	Xさんの公開かぎ	イ	Xさんの秘密かぎ
ウ	Yさんの公開かぎ	エ	Yさんの秘密かぎ

❑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

公開鍵暗号方式は、受信者の公開鍵と秘密鍵の鍵ペアを使用して暗号化／復号を行う暗号化方式です。送信者は、受信者の公開鍵を使って暗号化したデータを送信し、受信者は自分の秘密鍵を使ってデータを復号します。

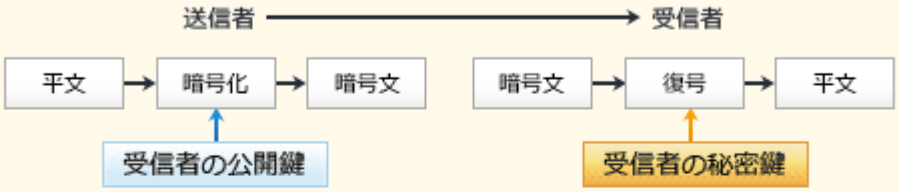


図　公開鍵暗号通信

公開鍵暗号方式では「暗号化は誰でもできるが、正しく復号できるのは正当な受信者だけ」です。もしデータが途中で傍受されても、第三者には復号できないので機密性が確保されます。また、通信相手が複数いても必要となる鍵の組合せが1つでいいので、共通鍵暗号方式の短所である鍵共有の手間および鍵数の多さという点が改善されています。

ただし共通鍵暗号方式と比較したとき、暗号化・復号するのに要する計算量が非常に多いため処理に時間が掛かる短所もあります。このためインターネット通信に使われるSSL/TLSやS/MIMEのように、両方式を組み合わせたハイブリッド方式を採用している通信規格もあります。

設問のケースでは、Xさんが送信者、Yさんが受信者に当たるので、暗号化に使用する鍵は受信者である**Yさんの公開かぎ**になります。

ポリモーフィック型マルウェアの説明として，適切なものはどれか。

平成30年春期　問39
203問目／選択範囲の問題数237問

ア　インターネットを介して，攻撃者がPCを遠隔操作する。

イ　感染ごとにマルウェアのコードを異なる鍵で暗号化することによって，同一のパターンでは検知されないようにする。

ウ　複数のOS上で利用できるプログラム言語でマルウェアを作成することによって，複数のOS上でマルウェアが動作する。

エ　ルートキットを利用して，マルウェアに感染していないように見せかけることによって，マルウェアを隠蔽する。

❑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：ウ”

❑解説

ポリモーフィック(Polymorphic)は「多様な形」という意味で、**ポリモーフィック型マルウェア**は、パターンマッチングによる検出を免れるため、感染の度に異なる暗号化/復号ルーチンで暗号化を行うなどして、自身のプログラムコードを都度変化させるマルウェアです。**ミューテーション型**ともいいます。

マルウェア定義ファイルによるパターンマッチングでは検知することができないので、検出にはマルウェアの活動を監視して判定を行う「ヒューリスティック法」や「ビヘイビア法」などの行動検知型の手法を利用する必要があります。

ア “インターネットを介して，攻撃者がPCを遠隔操作する。”

ボットやRAT(Remote Access Tool)の説明です。

イ “感染ごとにマルウェアのコードを異なる鍵で暗号化することによって，同一のパターンでは検知されないようにする。”

正しい。ポリモーフィック型マルウェアの説明です。

ウ “複数のOS上で利用できるプログラム言語でマルウェアを作成することによって，複数のOS上でマルウェアが動作する。”

マルチプラットホーム型マルウェアの説明です。

エ “ルートキットを利用して，マルウェアに感染していないように見せかけることによって，マルウェアを隠蔽する。”

ステルス型マルウェアの説明です。

WAFの説明はどれか。

ア　Webアプリケーションへの攻撃を検知し，阻止する。

イ　Webブラウザの通信内容を改ざんする攻撃をPC内で監視し，検出する。

ウ　サーバのOSへの不正なログインを監視する。

エ　ファイルへのマルウェア感染を監視し，検出する。

❑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

WAF(Web Application Firewall)は、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。チェックされる内容には「URLパラメータ」や「クッキーの内容」などのHTTPヘッダー情報や、「POSTデータの内容」などのメッセージボディ部などがあります。
本来、Webシステムへの攻撃はWebアプリケーション側で対処すべき問題ですが、脆弱性のないWebアプリケーションを作成するためには専門的な知識や技術が必要であるため、全てのWebアプリケーションのセキュリティ対策を万全にすることは難しいのが現実です。WAFはこのようなセキュリティ対策の不十分さを補完し、Webアプリケーションの堅牢性を高める役割をもちます。

ア “Webアプリケーションへの攻撃を検知し，阻止する。”

正しい。WAFの説明です。

イ “Webブラウザの通信内容を改ざんする攻撃をPC内で監視し，検出する。”

SSL/TLSの機能です。WAFはWebサーバの前段に設置されます。

ウ “サーバのOSへの不正なログインを監視する。”

HIDS(ホスト型IDS)の説明です。

エ “ファイルへのマルウェア感染を監視し，検出する。”

ウイルス対策ソフトの説明です。

無線LANにおいて，事前にアクセスポイントに登録した端末以外の接続を制限するためのものはどれか。

平成21年秋期　問42
205問目／選択範囲の問題数237問

ア	AES	イ	IEEE 802.11b
ウ	MACアドレスフィルタリング	エ	TKIP

❑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

MACアドレスフィルタリングは、無線LANのアクセスポイントに正当なユーザーのMACアドレスを登録しておくことで、正当なユーザー以外のアクセスを拒否する機能です。

ア “AES”

Advanced Encryption Standardの略。アメリカ合衆国の新暗号規格として規格化された共通鍵暗号方式です。

イ “IEEE 802.11b”

IEEE 802.11bは、IEEEにより策定された無線LAN規格の1つです。

ウ “MACアドレスフィルタリング”

正しい。

エ “TKIP”

Temporal Key Integrity Protocolの略。無線LAN規格で使われているセキュリティプロトコルで、WEPの脆弱性を克服した方式です。

情報セキュリティにおけるエクスプロイトコードの説明はどれか。

ア　同じセキュリティ機能をもつ製品に乗り換える場合に，CSV形式など他の製品に取り込むことができる形式でファイルを出力するプログラム

イ　コンピュータに接続されたハードディスクなどの外部記憶装置や，その中に保存されている暗号化されたファイルなどを閲覧，管理するソフトウェア

ウ　セキュリティ製品を設計する際の早い段階から実際に動作する試作品を作成し，それに対する利用者の反応を見ながら徐々に完成に近づける開発手法

エ　ソフトウェアやハードウェアの脆弱性を検査するために作成されたプログラム

❑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：イ”

❑解説

エクスプロイトコード(Exploit Code)とは、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を指す言葉です。

このようなプログラムは、善意の第三者や製品開発元の間で安全に流通している状況であれば問題ありませんが、世の中に出回ると攻撃方法の詳細が広く知られることになり、攻撃者が個人や企業、組織などへの攻撃を実行する際に悪用することが可能になります。実際に様々な脆弱性に対して攻撃が成功するように、複数のエクスプロイトコードをまとめた**エクスプロイトキット**というツールも存在し、攻撃に利用されています。

したがって「エ」が正解です。

エクスプロイトコードは、多くの場合、悪意を持ったマルウェアのことを指しますが、セキュリティ向上目的での研究材料や脆弱性検査のために作成された実証用コードという意味でも用いられます。

ア “同じセキュリティ機能をもつ製品に乗り換える場合に，CSV形式など他の製品に取り込むことができる形式でファイルを出力するプログラム”

データ移行プログラムの説明です。

イ “コンピュータに接続されたハードディスクなどの外部記憶装置や，その中に保存されている暗号化されたファイルなどを閲覧，管理するソフトウェア”

ファイル管理ツールの説明です。

ウ “セキュリティ製品を設計する際の早い段階から実際に動作する試作品を作成し，それに対する利用者の反応を見ながら徐々に完成に近づける開発手法”

プロトタイプモデルの説明です。

エ “ソフトウェアやハードウェアの脆弱性を検査するために作成されたプログラム”

正しい。エクスプロイトコードの説明です。

TLSのクライアント認証における次の処理a～cについて，適切な順序はどれか。

処理	処理の内容
a	クライアントが，サーバにクライアント証明書を送付する。
b	サーバが，クライアントにサーバ証明書を送付する。
c	サーバが，クライアントを認証する。

令和3年春期　問45
207問目／選択範囲の問題数237問

ア　a → b → c

イ　a → c → b

ウ　b → a → c

エ　c → a → b

❑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

TLSでは、サーバ認証の終了後、オプションでクライアント証明書によるクライアント認証を行う機能があります。クライアント認証を実施する際の、クライアントとサーバの間のメッセージのやり取りとしては以下の手順となります。

① サーバは、クライアントにサーバ証明書を送付するときに、クライアント証明書の提示を要請する（b）

② クライアントは、サーバにクライアント証明書を送付する（a）

③ サーバは、クライアント証明書を検証して、クライアントを認証する（c）

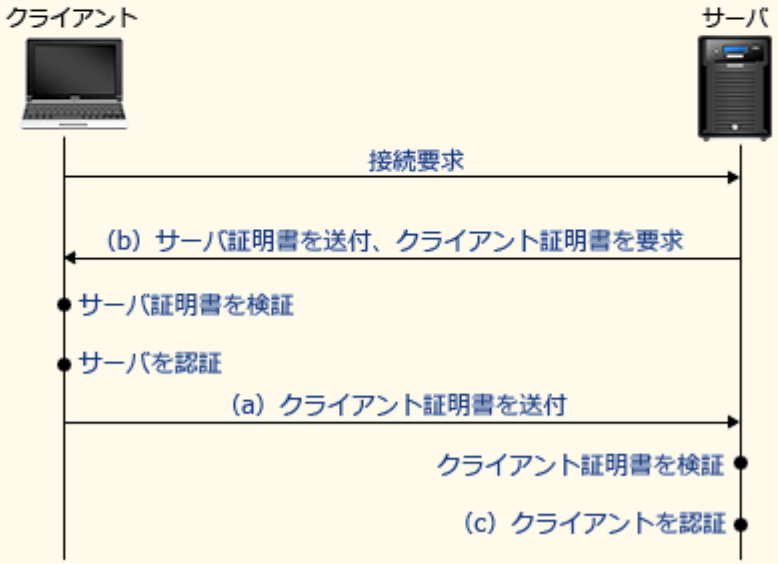


図　TLSのクライアント認証のシーケンス

したがって「b → a → c」の手順が適切です。

ICカードの耐タンパ性を高める対策はどれか。

令和6年春期　問44
208問目／選択範囲の問題数237問

ア　ICカードとICカードリーダーとが非接触の状態で利用者を認証して，利用者の利便性を高めるようにする。

イ　故障に備えてあらかじめ作成した予備のICカードを保管し，故障時に直ちに予備カードに交換して利用者がICカードを使い続けられるようにする。

ウ　信号の読出し用プローブの取付けを検出するとICチップ内の保存情報を消去する回路を設けて，ICチップ内の情報を容易には解析できないようにする。

エ　利用者認証にICカードを利用している業務システムにおいて，退職者のICカードは業務システム側で利用を停止して，他の利用者が利用できないようにする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ウ　“あなたの解答：イ”

❑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(tamper)は"改ざんする"という意味です。

ア “ICカードとICカードリーダーとが非接触の状態で利用者を認証して，利用者の利便性を高めるようにする。”

システムの使用性を高めるための対策であり、ICカードの耐タンパ性は向上しません。

イ “故障に備えてあらかじめ作成した予備のICカードを保管し，故障時に直ちに予備カードに交換して利用者がICカードを使い続けられるようにする。”

システムの信頼性を高めるための対策であり、ICカードの耐タンパ性は向上しません。

ウ “信号の読出し用プローブの取付けを検出するとICチップ内の保存情報を消去する回路を設けて，ICチップ内の情報を容易には解析できないようにする。”

正しい。解読や偽造に対して物理的に情報を保護する機能なので、耐タンパ性を高める対策に該当します。

エ “利用者認証にICカードを利用している業務システムにおいて，退職者のICカードは業務システム側で利用を停止して，他の利用者が利用できないようにする。”

システムのセキュリティを高めるための対策であり、ICカードの耐タンパ性は向上しません。

自社の中継用メールサーバで，接続元IPアドレス，電子メールの送信者のメールアドレスのドメイン名，及び電子メールの受信者のメールアドレスのドメイン名から成るログを取得するとき，外部ネットワークからの第三者中継と判断できるログはどれか。ここで，AAA.168.1.5 と AAA.168.1.10 は自社のグローバルIPアドレスとし，BBB.45.67.89 と BBB.45.67.90 は社外のグローバルIPアドレスとする。a.b.c は自社のドメイン名とし，a.b.d と a.b.e は他社のドメイン名とする。また，IPアドレスとドメイン名は詐称されていないものとする。

	接続元 IP アドレス	電子メールの送信者のメールアドレスのドメイン名	電子メールの受信者のメールアドレスのドメイン名
ア	AAA.168.1.5	a.b.c	a.b.d
イ	AAA.168.1.10	a.b.c	a.b.c
ウ	BBB.45.67.89	a.b.d	a.b.e
エ	BBB.45.67.90	a.b.d	a.b.c

ア　イ　ウ　エ

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ウ　“あなたの解答：ウ”

❑解説

第三者中継とは、メールサーバが、本来行うべきではない外部ネットワークの第三者から別の第三者へのメール転送を中継してしまうことです。インターネットに公開されているメールサーバが第三者中継を許す設定になっていると、スパムメールの温床になったり、スパムメールの発信・中継元としてブラックリストに載ってしまい、正規のメールの送受信に影響を与えるおそれがあります。

設問の条件に従って、各ログのIPアドレスとドメイン名を分類すると以下のようになります。

	接続元 IP アドレス	電子メールの送信者のメールアドレスのドメイン名	電子メールの受信者のメールアドレスのドメイン名
ア	AAA.168.1.5　社内	a.b.c　自社	a.b.d　他社
イ	AAA.168.1.10　社内	a.b.c　自社	a.b.c　自社
ウ	BBB.45.67.89　社外	a.b.d　他社	a.b.e　他社
エ	BBB.45.67.90　社外	a.b.d　他社	a.b.c　自社

表に書き入れてみると一目瞭然で、接続元IPアドレス、電子メールの送信者のドメイン名、電子メールの受信者のドメイン名がすべて自社と無関係である「ウ」が第三者中継を示すログとわかります。

WAFの説明として，適切なものはどれか。

平成28年春期　問40
210問目／選択範囲の問題数237問

ア　DMZに設置されているWebサーバへ外部から実際に侵入を試みる。

イ　WebサーバのCPU負荷を軽減するために，TLSによる暗号化と復号の処理をWebサーバではなく専用のハードウェア上で行う。

ウ　システム管理者が質問に答える形式で，自組織の情報セキュリティ対策のレベルを診断する。

エ　特徴的なパターンが含まれるかなどWebアプリケーションへの通信内容を検査して，不正な操作を遮断する。

❑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

パケットフィルター型ファイアウォールは、通過するパケットのヘッダー部に含まれるIPアドレスとポート番号を見て通過の可否を判断しますが、XSSやSQLインジェクション，OSコマンドインジェクションなどの正当なHTTP通信に則って仕掛けられた攻撃(ポート80宛てのパケット)は防ぐことができません。

WAF(Web Application Firewall)では、パケットのヘッダー部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これらの攻撃を検知し、遮断することが可能です。

ア “DMZに設置されているWebサーバへ外部から実際に侵入を試みる。”

ペネトレーションテスト(侵入テスト)の説明です。

イ “WebサーバのCPU負荷を軽減するために，TLSによる暗号化と復号の処理をWebサーバではなく専用のハードウェア上で行う。”

SSL/TLSアクセラレータの説明です。

ウ “システム管理者が質問に答える形式で，自組織の情報セキュリティ対策のレベルを診断する。”

IPAで公開されている「情報セキュリティ対策自己診断テスト」の説明です。

エ “特徴的なパターンが含まれるかなどWebアプリケーションへの通信内容を検査して，不正な操作を遮断する。”

正しい。WAFの説明です。

パケットフィルタリング型ファイアウォールがルール一覧に示したアクションに基づいてパケットを制御する場合，パケットAに対する処理はどれか。ここで，ファイアウォールでの処理は，ルール一覧に示す番号の1から順に行い，一つのルールが適用された場合には残りのルールは適用されない。

ルール一覧

番号	送信元アドレス	送信先アドレス	プロトコル	送信元ポート	送信先ポート	アクション
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注　*は任意のパターンを表す。

パケットA

送信元アドレス	送信先アドレス	プロトコル	送信元ポート	送信先ポート
10.1.2.3	10.2.3.4	TCP	2100	25

平成20年春期　問75

211問目／選択範囲の問題数237問

ア　番号1によって，通過が禁止される。

イ　番号2によって，通過が許可される。

ウ　番号3によって，通過が許可される。

エ　番号4によって，通過が禁止される。

❑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

パケットフィルタリング方式は、通過するパケットの送信先／送信元IPアドレス，送信先／送信元ポート，プロトコルなどのヘッダー情報を検証することでパケットの通過の可否を判断する手法です。

ルールの上から順にパケットAの情報にマッチするか確認していきます。ルール内の*(アスタリスク)はすべての値にマッチという意味です。

ルール1の送信元アドレスは、10.1.2.3なのでパケットAと一致します。さらにルール1のほかの項目はすべての値にマッチする*なので、パケットAにはルール1が適用され通過が禁止されます。「一つのルールが適用された場合には残りのルールは適用されない」という条件からルール1適用後、他のルールについては無視されることになります。

Webサーバにおいて，機密情報を記載したページが第三者に不正利用されることを防止するためのセキュリティ対策のうち，最も適切なものはどれか。

ア　Webサーバの受信用のポート番号を標準ポート番号から変更する。

イ　機密情報を記載したページでは，アクセス時に利用者認証を要求する。

ウ　機密情報を記載したページのURLは非公開にし，関係者だけに伝える。

エ　ドメイン名をDNSに登録せず，IPアドレスの直接入力だけでアクセスさせる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

イ　“あなたの解答：イ”

❑解説

第三者の不正利用を防止するには、正当な権限をもつユーザーのみに対して情報資産の利用を許可するような仕組みが実装されていることが重要です。
したがってアクセス時に利用者認証を行う「イ」の対策が適切です。

その他の対策は、攻撃者がWebサーバへのアクセスすることを難しくしますが、正当な権限を持たない者がアクセスできてしまうため不適切です。

SMTP-AUTHにおける認証の動作を説明したものはどれか。

ア　SMTPサーバは，クライアントがアクセスしてきた場合に利用者認証を行い，認証が成功したとき電子メールを受け付ける。

イ　サーバは認証局のデジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する。

ウ　電子メールを受信した際にパスワード認証が成功したクライアントのIPアドレスは，一定時間だけSMTPサーバへの電子メールの送信が許可される。

エ　パスワードを秘匿するために，パスワードからハッシュ値を計算して，その値で利用者が電子メールを受信する際の利用者認証を行う。

❑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

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 “SMTPサーバは，クライアントがアクセスしてきた場合に利用者認証を行い，認証が成功したとき電子メールを受け付ける。”

正しい。SMTP-AUTHによる認証動作です。

イ “サーバは認証局のデジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する。”

SMTP over SSL(TLS)によるサーバ/クライアントの相互認証です。

ウ “電子メールを受信した際にパスワード認証が成功したクライアントのIPアドレスは，一定時間だけSMTPサーバへの電子メールの送信が許可される。”

POP before SMTPによる認証動作です。

エ “パスワードを秘匿するために，パスワードからハッシュ値を計算して，その値で利用者が電子メールを受信する際の利用者認証を行う。”

APOP(Authenticated POP)による認証動作です。

セキュアOSを利用することによって期待できるセキュリティ上の効果はどれか。

令和5年春期　問37
214問目／選択範囲の問題数237問

ア　1回の利用者認証で複数のシステムを利用できるので，強固なパスワードを一つだけ管理すればよくなり，脆弱なパスワードを設定しにくくなる。

イ　Webサイトへの通信路上に配置して通信を解析し，攻撃をブロックすることができるので，Webアプリケーションソフトウェアの脆弱性を悪用する攻撃からWebサイトを保護できる。

ウ　強制アクセス制御を設定することによって，ファイルの更新が禁止できるので，システムに侵入されてもファイルの改ざんを防止できる。

エ　システムへのログイン時に，パスワードのほかに専用トークンを用いて認証が行えるので，パスワードが漏えいしても，システムへの侵入を防止できる。

❑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

ウ　“あなたの解答：エ”

❑解説

セキュアOSは、軍事機密や国家機密などを守るために作られたトラステッドOSをルーツとし、価格や使い勝手などの面を一般的な使用に適した形で開発されたOSです。セキュアOSには、トラステッドOSで要求されていた「最小特権」と「強制アクセス制御」という機能が取り入れられていて、高いセキュリティが実現されています。

最小特権

特権を付与する際に、全部の操作に対して特権を与えるのではなく、特権を細かく分割し、実行する必要のある操作に限定して特権を与える仕組み。管理者アカウントによる不必要な操作や権限の乱用を防ぎ、管理者アカウントが乗っ取られたときの被害を小さくする

強制アクセス制御（MAC：Mandatory Access Control）

ファイルやディレクトリの設定でアクセス制御を行うのではなく、システム全体のアクセス制御を記述したセキュリティポリシーが設定され、管理者アカウントを含むすべてのアカウントやプロセスがそれに強制的に従う仕組み。ファイル所有者や管理者アカウントによりファイル等のアクセス権が変更されるのを防ぐ

ア　“1回の利用者認証で複数のシステムを利用できるので，強固なパスワードを一つだけ管理すればよくなり，脆弱なパスワードを設定しにくくなる。”

シングルサインオンによるセキュリティ効果です。

イ　“Webサイトへの通信路上に配置して通信を解析し，攻撃をブロックすることができるので，Webアプリケーションソフトウェアの脆弱性を悪用する攻撃からWebサイトを保護できる。”

WAF(Web Application Firewall)によるセキュリティ効果です。

ウ　“強制アクセス制御を設定することによって，ファイルの更新が禁止できるので，システムに侵入されてもファイルの改ざんを防止できる。”

正しい。強制アクセス制御の説明なので、セキュアOSによるセキュリティ効果です。

エ　“システムへのログイン時に，パスワードのほかに専用トークンを用いて認証が行えるので，パスワードが漏えいしても，システムへの侵入を防止できる。”

多要素認証によるセキュリティ効果です。

内部ネットワークのPCからインターネット上のWebサイトを参照するときに，DMZに設置したVDI(Virtual Desktop Infrastructure)サーバ上のWebブラウザを利用すると，未知のマルウェアがPCにダウンロードされるのを防ぐというセキュリティ上の効果が期待できる。この効果を生み出すVDIサーバの動作の特徴はどれか。

令和4年春期　問44
215問目／選択範囲の問題数237問

ア　Webサイトからの受信データを受信処理した後，IPsecでカプセル化し，PCに送信する。

イ　Webサイトからの受信データを受信処理した後，実行ファイルを削除し，その他のデータをPCに送信する。

ウ　Webサイトからの受信データを受信処理した後，生成したデスクトップ画面の画像データだけをPCに送信する。

エ　Webサイトからの受信データを受信処理した後，不正なコード列が検知されない場合だけPCに送信する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ウ　“あなたの解答：エ”

❑解説

VDI(Virtual Desktop Infrastructure)は、サーバ内にクライアントごとの仮想マシンを用意して仮想デスクトップ環境を構築する技術です。利用者はネットワークを通じてVDIサーバ上の仮想デスクトップ環境に接続し、クライアントPCにはVDIサーバからの操作結果画面のみが転送される仕組みになっています。

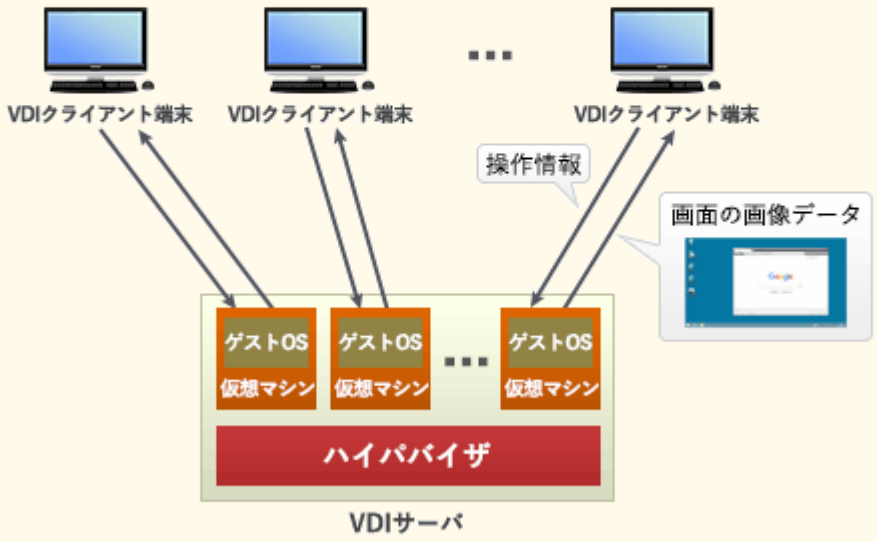


図　VDIの仕組み

この仕組みにより、クライアントがインターネット上のサイトと直接的な通信を行わなくなるので、クライアントPCをインターネットから分離できます。もし利用者の操作により不正なマルウェアをダウンロードしてしまったとしても、それが保存されるのはVDIサーバ上の仮想環境ですので、クライアントPCへの感染を防げます。汚染された仮想環境を削除してしまえば内部ネットワークへの影響もありません。

VDIサーバからPCに送信されるのは「デスクトップ画面の画像データ」のみです。したがって正解は「ウ」です。

企業内情報ネットワークやサーバにおいて，通常のアクセス経路以外で，侵入者が不正な行為に利用するために設置するものはどれか。

平成21年春期　問41
216問目／選択範囲の問題数237問

ア	VoIPゲートウェイ	イ	ストリクトルーティング
ウ	バックドア	エ	フォレンジック

❑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

バックドア(backdoor)は、直訳すれば「裏口」若しくは「勝手口」となりますが、防犯・犯罪学上等では「正規の手続きを踏まずに内部に入る事が可能な侵入口」のことを指します。コンピュータシステムにおいては、本来はIDやパスワードを使って通信を制限したり、使用権を確認するコンピュータの機能を無許可で利用するために、コンピュータ内に（他人に知られる事無く）設けられた通信接続の機能などがバックドアと呼ばれます。
直接的な攻撃だけでなくウィルスなどによっても設置されるシステム上の抜け道であり、攻撃者のシステムへの不正侵入を容易にしてしまいます。具体例としてはポートの設定変更などが挙げられます。

ア “VoIPゲートウェイ”

公衆電話網と他のIPネットワークなどの間に設置され、情報の送受信やプロトコル変換を行う機器です。

イ “ストリクトルーティング”

通信パケットの転送経路を、送信側のルータで指定する方法です。

ウ “バックドア”

正しい。

エ “フォレンジック”

セキュリティインシデントの発生時に、原因究明のために必要な電子的記録を収集解析することです。

暗号方式に関する記述のうち，適切なものはどれか。

令和2年秋期　問42
217問目／選択範囲の問題数237問

ア　AESは公開鍵暗号方式，RSAは共通鍵暗号方式の一種である。

イ　共通鍵暗号方式では，暗号化及び復号に同一の鍵を使用する。

ウ　公開鍵暗号方式を通信内容の秘匿に使用する場合は，暗号化に使用する鍵を秘密にして，復号に使用する鍵を公開する。

エ　デジタル署名に公開鍵暗号方式が使用されることはなく，共通鍵暗号方式が使用される。

❑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

ア “AESは公開鍵暗号方式，RSAは共通鍵暗号方式の一種である。”

記述とは逆で、AESは共通鍵暗号方式、RSAは公開鍵暗号方式です。

イ “共通鍵暗号方式では，暗号化及び復号に同一の鍵を使用する。”

正しい。共通鍵暗号方式は、名前のとおり、暗号化と復号に同一（共通）の鍵を使用します。錠をかけるのと開けるのとで同じ鍵を使用する、玄関のドアのようなイメージです。

ウ “公開鍵暗号方式を通信内容の秘匿に使用する場合は，暗号化に使用する鍵を秘密にして，復号に使用する鍵を公開する。”

公開鍵暗号方式では、暗号化鍵を公開し、復号鍵は厳重に管理します。暗号化は誰でもできますが、復号できるのは正当な受信者だけなので、通信の機密性が確保される仕組みです。

エ “デジタル署名に公開鍵暗号方式が使用されることはなく，共通鍵暗号方式が使用される。”

デジタル署名は、共通鍵暗号方式ではなく公開鍵暗号方式を応用した技術です。暗号化通信とは異なり、送信者が秘密鍵で暗号化したデータを、受信者が公開鍵で復号して検証することで、正当な送信者から送信されたデータであることを確認できます。

	共通鍵暗号方式	公開鍵暗号方式
暗号化と復号の鍵	同じ	異なる
鍵の配送	手間が掛かる	必要なし
処理速度	速い	遅い
n人の相互暗号化通信に必要となる鍵数	n(n－1)／2	2n
秘密として管理すべき鍵	両方の共通鍵	秘密鍵のみ
代表的なアルゴリズム	AES，3DES，Blowfish	RSA，楕円曲線暗号，エルガマル暗号

パケットフィルタリング型ファイアウォールが，通信パケットの通過を許可するかどうかを判断するときに用いるものはどれか。

平成31年春期　問44
218問目／選択範囲の問題数237問

ア　Webアプリケーションに渡されるPOSTデータ

イ　送信元と宛先のIPアドレスとポート番号

ウ　送信元のMACアドレス

エ　利用者のPCから送信されたURL

❑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

ファイアウォールには幾つかの方式がありますが、**パケットフィルタリング型**は、パケットのヘッダー部分に含まれる「送信元/宛先IPアドレス」「送信元/宛先ポート番号」「通信の方向」などの情報と、FW内部のフィルタリングルールを比較することでパケット通過の可否を決定する方式です。ここでいうヘッダー部分とは、IPヘッダー又はTCP/UDPヘッダーを指します。

したがって「イ」が適切な記述です。

ISP"A"管理下のネットワークから別のISP"B"管理下の宛先へSMTPで電子メールを送信する。電子メール送信者がSMTP-AUTHを利用していない場合，スパムメール対策OP25Bによって遮断される電子メールはどれか。

平成28年秋期　問37
219問目／選択範囲の問題数237問

ア　ISP"A"管理下の固定IPアドレスから送信しようとしたが，受信者の承諾を得ていない広告の電子メール

イ　ISP"A"管理下の固定IPアドレスから送信しようとしたが，送信元IPアドレスがDNSで逆引きできなかった電子メール

ウ　ISP"A"管理下の動的IPアドレスからISP"A"のメールサーバを経由して送信された電子メール

エ　ISP"A"管理下の動的IPアドレスからISP"A"のメールサーバを経由せずに直接送信された電子メール

❑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

OP25B(Outbound Port 25 Blocking)は、名前の通り、外向き(インターネット方向)のポート25番宛て(SMTP)パケットを遮断することでスパムメールを防ぐ仕組みです。
ISP管理下の動的IPアドレスからの電子メール送信について、管理外ネットワークのメールサーバへSMTP通信を禁止することで、ISPのメールサーバを介さずに外部のオープンリレーサーバと直接コネクションを確立して送信されるスパムメールを防ぎます。

OP25Bでは、1.動的IPアドレスからの送信である，2.ISPのメールサーバを経由しない　という2つの条件を満たした場合のみTCP/25宛てのパケットを遮断します。

またISPのメールサーバを経由しない場合であっても

1. 固定IPからの送信
2. SMTP-AUTHで認証済ノードからの送信

についてはOP25Bの影響を受けません。

したがって「エ」のみがOP25Bによって遮断される電子メールということになります。

ファイアウォールの方式に関する記述のうち，適切なものはどれか。

ア　アプリケーションゲートウェイ方式では，アプリケーションのプロトコルごとにゲートウェイ機能の設定が必要である。

イ　サーキットゲートウェイ方式では，コマンドの通過可否を制御する。

ウ　トランスポートゲートウェイ方式では，アプリケーションのプロトコルに依存するゲートウェイ機能を提供する。

エ　パケットフィルタリング方式では，電子メールの中に含まれている単語によるフィルタリングが可能である。

❑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：ア”

❑解説

ア “アプリケーションゲートウェイ方式では，アプリケーションのプロトコルごとにゲートウェイ機能の設定が必要である。”

正しい。アプリケーションゲートウェイ方式では、アプリケーション層レベルでコネクションを中継するため、HTTP，FTP，SMTPなどアプリケーションプログラムごとに別々の中継プログラムを用意する必要があります。

イ “サーキットゲートウェイ方式では，コマンドの通過可否を制御する。”

サーキットゲートウェイ方式は、ペイロード部をチェックしないためアプリケーション層レベルの情報である"コマンド"によるフィルタリングには対応していません。

ウ “トランスポートゲートウェイ方式では，アプリケーションのプロトコルに依存するゲートウェイ機能を提供する。”

トランスポートゲートウェイ方式は、トランスポート層レベルでコネクションを中継するため、アプリケーションプログラムの形式に依存することはありません。

エ “パケットフィルタリング方式では，電子メールの中に含まれている単語によるフィルタリングが可能である。”

パケットフィルタリング方式は、パケットのヘッダー部の内容に基づいてフィルタリングを行う方式です。電子メールの内容はパケットのペイロード部に格納されているためパケットフィルタリングではその内容をチェックすることができません。

サンドボックスの仕組みについて述べたものはどれか。

平成25年春期　問44
221問目／選択範囲の問題数237問

ア　Webアプリケーションの脆弱性を悪用する攻撃に含まれる可能性が高い文字列を定義し，攻撃であると判定した場合には，その通信を遮断する。

イ　侵入者をおびき寄せるために本物そっくりのシステムを設置し，侵入者の挙動などを監視する。

ウ　プログラムの影響がシステム全体に及ぶことを防止するために，プログラムが実行できる機能やアクセスできるリソースを制限して動作させる。

エ　プログラムのソースコードでSQL文の雛(ひな)形の中に変数の場所を示す記号を置いた後，実際の値を割り当てる。

❑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：ウ”

❑解説

サンドボックス(Sandbox)は、外部から受け取ったプログラムを保護された領域で動作させることによってシステムが不正に操作されるのを防ぎ、セキュリティを向上させる仕組みです。
JavaアプレットやAdobe Flash、Webブラウザのプラグインなどでは外部プログラムの機能を制限することで脆弱性を低減させています。子供を安全である砂場(サンドボックス)内だけで遊ばせるイメージからこう呼ばれています。

ア　“Webアプリケーションの脆弱性を悪用する攻撃に含まれる可能性が高い文字列を定義し，攻撃であると判定した場合には，その通信を遮断する。”

WAF(Web Application Firewall)の仕組みです。

イ　“侵入者をおびき寄せるために本物そっくりのシステムを設置し，侵入者の挙動などを監視する。”

ハニーポットの仕組みです。

ウ　“プログラムの影響がシステム全体に及ぶことを防止するために，プログラムが実行できる機能やアクセスできるリソースを制限して動作させる。”

正しい。サンドボックスの仕組みです。

エ　“プログラムのソースコードでSQL文の雛(ひな)形の中に変数の場所を示す記号を置いた後，実際の値を割り当てる。”

SQLインジェクション対策であるバインド機構またはプレースホルダの仕組みです。

ファジングに該当するものはどれか。

ア　Webサーバに対し，ログイン，閲覧などのリクエストを大量に送り付け，一定時間内の処理量を計測して，DDoS攻撃に対する耐性を検査する。

イ　ソフトウェアに対し，問題を起こしそうな様々な種類のデータを入力し，そのソフトウェアの動作状態を監視して脆弱性を発見する。

ウ　パスワードとしてよく使われる文字列を数多く列挙したリストを使って，不正にログインを試行する。

エ　マークアップ言語で書かれた文字列を処理する前に，その言語にとって特別な意味をもつ文字や記号を別の文字列に置換して，脆弱性が悪用されるのを防止する。

❑分類

テクノロジ系 » セキュリティ » セキュリティ技術評価

❑正解

イ　“あなたの解答：イ”

❑解説

ファジング(fuzzing)とは、検査対象のソフトウェア製品に「ファズ（英名：fuzz）」と呼ばれる問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで(未知の)脆弱性を検出する検査手法です。

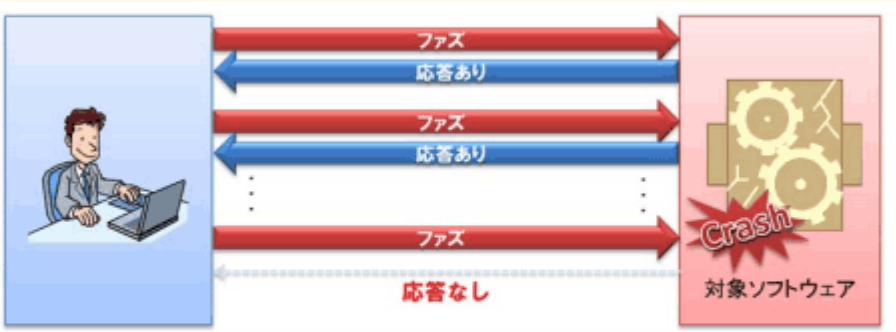


図 2.1-1 ファジングによる脆弱性検出イメージ

IPA資料「ファジング活用の手引き」より引用
http://www.ipa.go.jp/files/000051628.pdf

ファジングは、ファズデータの生成、検査対象への送信、挙動の監視を自動で行うファジングツール(ファザー)と呼ばれるソフトウェアを使用して行います。開発ライフサイクルにファジングを導入することで「バグや脆弱性の低減」「テストの自動化・効率化によるコスト削減」が期待できるため、大手企業の一部で徐々に活用され始めています。

ア “Webサーバに対し，ログイン，閲覧などのリクエストを大量に送り付け，一定時間内の処理量を計測して，DDoS攻撃に対する耐性を検査する。”

負荷テストやDDoS演習に関する記述です。

イ “ソフトウェアに対し，問題を起こしそうな様々な種類のデータを入力し，そのソフトウェアの動作状態を監視して脆弱性を発見する。”

正しい。ファジングに関する記述です。

ウ “パスワードとしてよく使われる文字列を数多く列挙したリストを使って，不正にログインを試行する。”

辞書攻撃に関する記述です。

エ “マークアップ言語で書かれた文字列を処理する前に，その言語にとって特別な意味をもつ文字や記号を別の文字列に置換して，脆弱性が悪用されるのを防止する。”

サニタイジング(エスケープ処理)に関する記述です。

JIS Q 27002における情報資産に対する脅威の説明はどれか。

平成22年春期　問41
223問目／選択範囲の問題数237問

ア　情報資産に害をもたらすおそれのある事象の原因

イ　情報資産に内在して，リスクを顕在化させる弱点

ウ　リスク対策に費用をかけないでリスクを許容する選択

エ　リスク対策を適用しても解消しきれず残存するリスク

❑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

ア　“あなたの解答：ア”

❑解説

JIS Q 27002は、組織のセキュリティ運用体制をISO/IEC 27002の日本語訳として規定されています。情報セキュリティマネジメントシステム (ISMS) を立ち上げ、実装し、運用するための情報セキュリティ管理に関するベストプラクティスを提供します。

JIS Q 27001 では、脅威 (threat)は「システムまたは組織に損害を与える可能性があるインシデントの潜在的な原因」として定義しています。

ア “情報資産に害をもたらすおそれのある事象の原因”

正しい。脅威の説明です。

イ “情報資産に内在して，リスクを顕在化させる弱点”

脆弱性の説明です。

ウ “リスク対策に費用をかけないでリスクを許容する選択”

リスク保有の説明です。

エ “リスク対策を適用しても解消しきれず残存するリスク”

残存リスクの説明です。

パスワードに使用できる文字の種類の数をM，パスワードの文字数をnとするとき，設定できるパスワードの理論的な総数を求める数式はどれか。

平成29年秋期　問39
224問目／選択範囲の問題数237問

ア　M^n

イ　$\frac{M!}{(M-n)!}$

ウ　$\frac{M!}{n!(M-n)!}$

エ　$\frac{(M+n-1)!}{n!(M-1)!}$

❑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

数字4桁のパスワードを考えると

文字種の数："0～9" の10種類

文字数：4文字

となり、この条件では"0000"～"9999"の10,000種類の組合せが存在します。同様に数字6文字であれば、

文字種の数："0～9" の10種類

文字数：6文字

パスワードの組合せ：1,000,000種類

となります。これらの例を一般化してパスワードの総数を表す式を考えると、「10×10×10×10＝10,000」、「10×10×10×10×10×10＝1,000,000」というように文字種の数**M**を文字数**n**回だけ乗じた数であると導けます。したがってM^nが適切な数式です。

毎回参加者が変わる100名程度の公開セミナにおいて，参加者が持参する端末に対して無線LAN接続環境を提供する。参加者の端末以外からのアクセスポイントへの接続を防止するために効果があるセキュリティ対策はどれか。

平成25年春期　問43
225問目／選択範囲の問題数237問

ア　アクセスポイントがもつDHCPサーバ機能において，参加者の端末に対して動的に割り当てるIPアドレスの範囲をセミナごとに変更する。

イ　アクセスポイントがもつURLフィルタリング機能において，参加者の端末に対する条件をセミナごとに変更する。

ウ　アクセスポイントがもつ暗号化機能において，参加者の端末とアクセスポイントとの間で事前に共有する鍵をセミナごとに変更する。

エ　アクセスポイントがもつプライバシーセパレータ機能において，参加者の端末へのアクセス制限をセミナごとに変更する。

❑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

ウ　“あなたの解答：ア”

❑解説

ア “アクセスポイントがもつDHCPサーバ機能において，参加者の端末に対して動的に割り当てるIPアドレスの範囲をセミナごとに変更する。”

参加者のものではない端末に対して、DHCPからIPアドレスが割り振られるのを防ぐことはできません。

イ “アクセスポイントがもつURLフィルタリング機能において，参加者の端末に対する条件をセミナごとに変更する。”

URLフィルタリングは、特定のWebサイトへのアクセスを遮断する機能ですが、アクセスポイント自体への接続を拒否できるわけではありません。

ウ “アクセスポイントがもつ暗号化機能において，参加者の端末とアクセスポイントとの間で事前に共有する鍵をセミナごとに変更する。”

正しい。無線LANにおいてはアクセスポイントと子機のもつ暗号化キーが一致した場合のみ通信を開始します。これを利用しセミナ参加者の正規の端末にだけ正しい暗号化キーを設定することでアクセスポイントへの不正アクセスを遮断することができます。

エ “アクセスポイントがもつプライバシーセパレータ機能において，参加者の端末へのアクセス制限をセミナごとに変更する。”

プライバシーセパレータは、同じアクセスポイントに接続している子機同士のアクセスを禁止する機能ですが、アクセスポイント自体への接続を拒否できるわけではありません。

セキュリティ対策で利用するCRLに記載されるデータはどれか。

ア　スパムメールの発信元及びメールの不正中継を行うドメインの名前

イ　デジタル証明書の有効期間内に認証局の廃止などによって失効した自己署名証明書及び相互認証証明書

ウ　有効期間内に失効したデジタル証明書のシリアル番号

エ　利用者に対して与えられた情報資源へのアクセス権限リスト

❑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

CRL(Certificate Revocation List：証明書失効リスト)は、公開鍵基盤(PKI)において失効した(信用性のない)公開鍵証明書のリストです。信用性がなくなる失効理由としては、秘密鍵の漏洩・紛失、証明書の被発行者の規則違反などで、どれも認証の役に立たなくなったということが共通しています。

CRLは、PKIを使用したアプリケーションが証明書の有効性を検証するために使われています。

電子メールに用いられるS/MIMEの機能はどれか。

ア　ウイルスの検出

イ　改ざんされた内容の復元

ウ　スパムメールのフィルタリング

エ　内容の暗号化とデジタル署名の付与

❑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

S/MIME(Secure MIME)は、電子メールを盗聴や改ざんなどから守るために米国RSA Data Security社によって開発された技術で、公開鍵暗号技術を使用して「認証」「改ざん検出」「暗号化」などの機能を電子メールソフトに提供するものです。

したがって「エ」が適切です。

脆弱性検査手法の一つであるファジングはどれか。

ア　既知の脆弱性に対するシステムの対応状況に注目し，システムに導入されているソフトウェアのバージョン及びパッチの適用状況の検査を行う。

イ　ソフトウェアのデータの入出力に注目し，問題を引き起こしそうなデータを大量に多様なパターンで入力して挙動を観察し，脆弱性を見つける。

ウ　ベンダーや情報セキュリティ関連機関が提供するセキュリティアドバイザリなどの最新のセキュリティ情報に注目し，ソフトウェアの脆弱性の検査を行う。

エ　ホワイトボックス検査の一つであり，ソフトウェアの内部構造に注目し，ソースコードの構文をチェックすることによって脆弱性を見つける。

❑分類

テクノロジ系 » セキュリティ » セキュリティ技術評価

❑正解

イ　“あなたの解答：イ”

❑解説

ファジング(fuzzing)とは、検査対象のソフトウェア製品に「ファズ（英名：fuzz）」と呼ばれる問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで(未知の)脆弱性を検出する検査手法です。

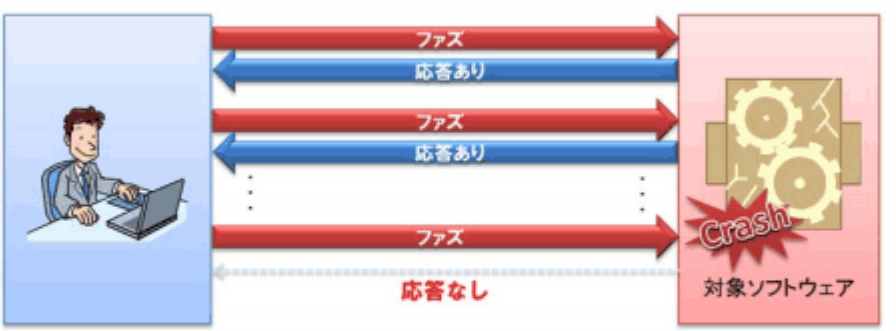


図 2.1-1 ファジングによる脆弱性検出イメージ

IPA資料「ファジング活用の手引き」より引用
http://www.ipa.go.jp/files/000051628.pdf

ファジングは、ファズデータの生成、検査対象への送信、挙動の監視を自動で行うファジングツール(ファザー)と呼ばれるソフトウェアを使用して行います。開発ライフサイクルにファジングを導入することで「バグや脆弱性の低減」「テストの自動化・効率化によるコスト削減」が期待できるため、大手企業の一部で徐々に活用され始めています。

ア “既知の脆弱性に対するシステムの対応状況に注目し，システムに導入されているソフトウェアのバージョン及びパッチの適用状況の検査を行う。”

バージョンチェックツールの説明です。

イ “ソフトウェアのデータの入出力に注目し，問題を引き起こしそうなデータを大量に多様なパターンで入力して挙動を観察し，脆弱性を見つける。”

正しい。ファジングの説明です。

ウ “ベンダーや情報セキュリティ関連機関が提供するセキュリティアドバイザリなどの最新のセキュリティ情報に注目し，ソフトウェアの脆弱性の検査を行う。”

JVNなどが提供する脆弱性対策情報データベースなどを活用した検査です。

エ “ホワイトボックス検査の一つであり，ソフトウェアの内部構造に注目し，ソースコードの構文をチェックすることによって脆弱性を見つける。”

ソースコードセキュリティ検査ツールの説明です。

参考URL: IPA 脆弱性対策：ファジング
https://www.ipa.go.jp/security/vuln/fuzzing/contents.html

https://www.ipa.go.jp/security/vuln/fuzzing/contents.html

ブルートフォース攻撃に該当するものはどれか。

ア　WebブラウザとWebサーバの間の通信で，認証が成功してセッションが開始されているときに，Cookieなどのセッション情報を盗む。

イ　コンピュータへのキー入力を全て記録して外部に送信する。

ウ　使用可能な文字のあらゆる組合せをそれぞれパスワードとして，繰り返しログインを試みる。

エ　正当な利用者のログインシーケンスを盗聴者が記録してサーバに送信する。

❑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：ウ”

❑解説

ブルートフォース攻撃は、パスワードクラックや暗号鍵の解読に用いられる手法の1つで、特定の文字数および文字種で設定される可能性のあるすべての組合せを試すことで不正ログインを試みる攻撃手法です。総当たり攻撃とも呼ばれます。
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、この手法によって認証を不正に突破されてしまう危険性が高くなります。

ア “Webブラウザとwebサーバの間の通信で，認証が成功してセッションが開始されているときに，Cookieなどのセッション情報を盗む。”

セッションハイジャックの説明です。

イ “コンピュータへのキー入力を全て記録して外部に送信する。”

キーロガーの説明です。

ウ “使用可能な文字のあらゆる組合せをそれぞれパスワードとして，繰り返しログインを試みる。”

正しい。ブルートフォース攻撃の説明です。

エ “正当な利用者のログインシーケンスを盗聴者が記録してサーバに送信する。”

リプレイアタックの説明です。

ソーシャルエンジニアリングに分類される手口はどれか。

平成22年秋期　問39
230問目／選択範囲の問題数237問

ア　ウイルス感染で自動作成されたバックドアからシステムに侵入する。

イ　システム管理者などを装い，利用者に問い合わせてパスワードを取得する。

ウ　総当たり攻撃ツールを用いてパスワードを解析する。

エ　バッファオーバーフローなどのソフトウェアの脆(ぜい)弱性を利用してシステムに侵入する。

❑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

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

選択肢の中で、技術的な方法ではなく、人の心の隙を狙って秘密情報を窃取しようとする行為は「イ」だけです。

DNSSECで実現できることはどれか。

令和6年春期　問37
231問目／選択範囲の問題数237問

ア　DNSキャッシュサーバが得た応答の中のリソースレコードが，権威DNSサーバで管理されているものであり，改ざんされていないことの検証

イ　権威DNSサーバとDNSキャッシュサーバとの通信を暗号化することによる，ゾーン情報の漏えいの防止

ウ　長音"ー"と漢数字"一"などの似た文字をドメイン名に用いて，正規サイトのように見せかける攻撃の防止

エ　利用者のURLの入力誤りを悪用して，偽サイトに誘導する攻撃の検知

❑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：イ”

❑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、次の手順によって応答レコードが改ざんされておらず、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を検証します。

1. DNSキャッシュサーバは、DNSコンテンツ(権威)サーバに対してドメイン問合せを行う（通常と同じ）
2. DNSコンテンツサーバは、ドメイン応答に自身のデジタル署名を付加してDNSキャッシュサーバに送信する
3. 応答を受け取ったDNSキャッシュサーバは、DNSコンテンツサーバの公開鍵を使用してデジタル署名を検証し、内容の正当性を確認する

DNSSECで実現できることは、権威DNSサーバの応答レコードの正当性、完全性の確認なので、「ア」が適切な記述です。

ア “DNSキャッシュサーバが得た応答の中のリソースレコードが，権威DNSサーバで管理されているものであり，改ざんされていないことの検証”

正しい。応答中に含まれるリソースレコードが改ざんされておらず、DNSサーバ上で管理されていることが確認できます。

イ “権威DNSサーバとDNSキャッシュサーバとの通信を暗号化することによる，ゾーン情報の漏えいの防止”

DNSSECには暗号化の仕組みがありません。ゾーン情報の暗号化には、DNS over TLS(DoT)やDNS over HTTPS(DoH)が用いられます。

ウ “長音”ー”と漢数字”一”などの似た文字をドメイン名に用いて，正規サイトのように見せかける攻撃の防止”

DNSSECでは防げません。利用者が混同するおそれのある類似ドメインに対しては、紛争処理機関に対してドメイン名紛争処理を申し立て、取消や移転処分を求めるのが有効です。なお、正当なドメインに似せたドメインを用いる攻撃は、ドッペルゲンガードメインと呼ばれます。

エ “利用者のURLの入力誤りを悪用して，偽サイトに誘導する攻撃の検知”

DNSSECでは防げません。なお、URLの入力ミス・打ち間違いに乗じて偽サイトに誘導する行為は、タイポスクワッティングと呼ばれます。

暗号機能を実装したIoT機器における脅威のうち，サイドチャネル攻撃に該当するものはどれか。

令和5年秋期　問41
232問目／選択範囲の問題数237問

ア　暗号化関数を線形近似する式を導き，その線形近似式から秘密情報の取得を試みる。

イ　機器が発する電磁波を測定することによって秘密情報の取得を試みる。

ウ　二つの平文の差とそれぞれの暗号文の差の関係から，秘密情報の取得を試みる。

エ　理論的にあり得る復号鍵の全てを機器に入力して秘密情報の取得を試みる。

❑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

サイドチャネル攻撃は、対象の動作状況を観察し、漏洩電磁波・電力消費等のサイドチャネル情報から暗号鍵推定等を行う非破壊型解析攻撃の総称です。サイドチャネル(Side Channel)には、非正規の入出力経路という意味があります。具体的な攻撃方法としては、故障利用攻撃、タイミング攻撃や電力解析攻撃、電磁波解析攻撃などがあります。

故障利用攻撃

デバイスに限定的な障害を故意に与え、デバイスの計算誤りから秘密情報を解析する手法

タイミング攻撃

暗号処理のタイミングが暗号鍵の論理値に依存して変化することに着目し、暗号化や復号に要する時間の差異を統計的に解析して暗号鍵を推定する手法

電力解析攻撃

消費電力の変化に着目して鍵や処理内容の解析を試みる手法

電磁波解析攻撃（テンペスト攻撃）

機器が発する電磁波を測定することによって秘密情報の取得を試みる手法

ア “暗号化関数を線形近似する式を導き，その線形近似式から秘密情報の取得を試みる。”

暗号化関数の線形近似式を発見することを基本とした「線形解読法」の説明です。

イ “機器が発する電磁波を測定することによって秘密情報の取得を試みる。”

正しい。サイドチャネル攻撃の一つである「電磁波解析攻撃」の説明です。

ウ “二つの平文の差とそれぞれの暗号文の差の関係から，秘密情報の取得を試みる。”

入力値の差分が出力値の差分にどのような影響を与えるかを分析して解読を試みる「差分解読法」の説明です。

エ “理論的にあり得る復号鍵の全てを機器に入力して秘密情報の取得を試みる。”

ブルートフォース攻撃(総当たり攻撃)の説明です。

JIS Q 31000:2019(リスクマネジメント－指針)において，リスク特定で考慮することが望ましいとされている事項はどれか。

令和6年春期　問40
233問目／選択範囲の問題数237問

ア　結果の性質及び大きさ

イ　残留リスクが許容可能かどうかの判断

ウ　資産及び組織の資源の性質及び価値

エ　事象の起こりやすさ及び結果

❑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：ア”

❑解説

JIS Q 31000では、リスク特定では次の要素やそれら同士の関係を考慮することが望ましいとしています。

①有形及び無形のリスク源、②原因及び事象、③脅威及び機会、④脆弱性及び能力、⑤外部及び内部の状況の変化、⑥新たに発生するリスクの指標、⑦**資産及び組織の資源の性質及び価値**、⑧結果及び結果が目的に与える影響、⑨知識の限界及び情報の信頼性、⑩時間に関連する要素、⑪関与する人の先入観・前提及び信条

リスクは組織の状況と離れて認識されるものではなく、その事象の可能性がリスクであるかどうか、そのリスクの重要性は常に組織の内外の状況との関係で認識されます。このためリスク特定に当たっては、リスクの顕在化により影響を受ける、資産・組織の資源の性質・価値を考慮する必要があります。

ア “結果の性質及び大きさ”

リスク分析で考慮するべき事項です。

イ “残留リスクが許容可能かどうかの判断”

リスク対応で考慮するべき事項です。

ウ “資産及び組織の資源の性質及び価値”

正しい。リスク特定で考慮するべき事項です。

エ “事象の起こりやすさ及び結果”

リスク分析で考慮するべき事項です。

DNSキャッシュサーバに対して外部から行われるキャッシュポイズニング攻撃への対策のうち，適切なものはどれか。

ア　外部ネットワークからの再帰的な問合せにも応答できるように，コンテンツサーバにキャッシュサーバを兼ねさせる。

イ　再帰的な問合せに対しては，内部ネットワークからのものだけを許可するように設定する。

ウ　再帰的な問合せを行う際の送信元のポート番号を固定する。

エ　再帰的な問合せを行う際のトランザクションIDを固定する。

❑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

DNSキャッシュポイズニング攻撃は、DNSキャッシュサーバに偽のDNS情報をキャッシュとして登録させることで、利用者を偽のWebサイトに誘導する攻撃です。

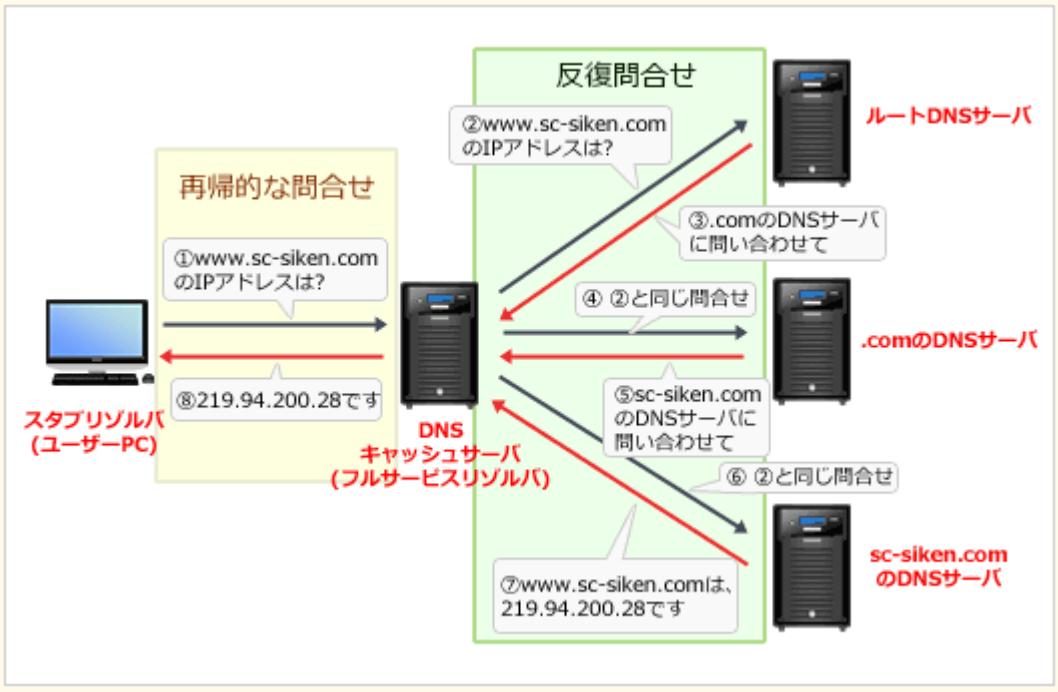
まず設問に登場する「再帰的な問合せ」について確認しておきます。DNSの名前解決はその性質によって「再帰的な問合せ」と「反復(非再帰的)問合せ」に区別されます。

再帰的な問合せ

リゾルバから名前解決要求を受けたDNSサーバが他のDNSサーバに代理して問合せを行い、最終的な結果をリゾルバに返す必要のある問合せのこと

反復問合せ

リゾルバから再帰的問合せを受けたDNSサーバが、それを解決できるまで繰り返し他のDNSサーバに行う問合せのこと



この2つの問合せの違いを踏まえて、攻撃者がDNSキャッシュサーバに偽のキャッシュ情報を登録させる手順を追ってみます。

① 攻撃者は、キャッシュサーバに対して偽の再帰的な問合せを行い反復問合せを強制的に生じさせる。

② キャッシュサーバは、コンテンツサーバに対して反復問合せを行う。

③ 攻撃者は、コンテンツサーバが正規の応答を返すよりも先にキャッシュサーバへ偽の応答を送りつける。

④ キャッシュサーバは、攻撃者から送られた偽の応答を正規のものと判断しキャッシュに登録する。この時点でDNSクエリは解決済なのでコンテンツサーバから送られた正規の応答は破棄される。

DNSキャッシュポイズニングは、上記のように外部から攻撃目的で送られた再帰的な問合せをキャッシュサーバが処理してしまうことから始まります。再帰的問合せの役割は、内部ネットワークのホストが外部ネットワークに接続する際の名前解決であり、原則として外部からの再帰的な問合せに応じる必要はないはずですから、**再帰的な問合せを受け付けるホストを内部ネットワークだけに限定する**ことがキャッシュポイズニング攻撃への対策となります。
また、DNSでは送信元のIPアドレスとポート番号、トランザクションIDの全てが一致しないと、キャッシュサーバはコンテンツサーバからの正しい応答として認めない仕組みを備えています。このためDNSキャッシュポイズニングが成立するためには、反復問合せに対する偽の応答メッセージに含まれる各情報を正規の応答と一致させる必要があります。DNSの設定で、ポート番号やトランザクションIDが固定されていたり推測されやすいものになっていたりすると、パケットの偽装が容易になり攻撃に対して脆弱になってしまいます。

ア "外部ネットワークからの再帰的な問合せにも応答できるように，コンテンツサーバにキャッシュサーバを兼ねさせる。"

キャッシュサーバは外部からの再帰的な問合せに応じない設定にする必要があります。

イ "再帰的な問合せに対しては，内部ネットワークからのものだけを許可するように設定する。"

正しい。

ウ "再帰的な問合せを行う際の送信元のポート番号を固定する。"

送信元のポート番号を固定しても、外部からの再帰的な問合せに対して効果はありません。

エ "再帰的な問合せを行う際のトランザクションIDを固定する。"

トランザクションIDを固定しても、外部からの再帰的な問合せに対して効果はありません。

人間には読み取ることが可能でも，プログラムでは読み取ることが難しいという差異を利用して，ゆがめたり一部を隠したりした画像から文字を判読させ入力させることで，人間以外による自動入力を排除する技術はどれか。

平成26年春期　問36
235問目／選択範囲の問題数237問

ア	CAPTCHA	イ	QRコード
ウ	短縮URL	エ	トラックバックping

❑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

CAPTCHA(キャプチャ)は、チャレンジレスポンス型テストの一種で、認証の際に異なる歪んだ文字や数字を表示し、書かれている文字を入力させる仕組みです。
人間は多少の歪んだ文字列であれば認識できますが、プログラム処理でこれを読み取ることは非常に困難です※。これを利用して、自動プログラムで無差別に投稿するスパム行為や、サーバに負荷が掛かる短時間での連続リクエストの送信を抑制する目的で設置されます。

ア “CAPTCHA”

正しい。

イ “QRコード”

QRコードは、携帯電話でのURLの読取りや、販売店や工場における在庫管理などにも利用される二次元コードの規格です。

ウ “短縮URL”

短縮URLは、長くなりがちなURLを20文字程度に短縮する仕組みです。リダイレクトを利用することで本来のURLに接続できるようになっています。

エ “トラックバックping”

トラックバックpingは、ブログシステムに組み込まれている機能の1つで、他のブログページへのハイパーリンクを設置した際に、そのハイパーリンクを設置した事実やその設置ページの情報をリンク先ブログに通知する仕組みです。

※現在ではAI技術の進展により単純な歪み程度は判別されてしまうため、より複雑化したものでなければスパム防止の効果は望めません。

TPM(Trusted Platform Module)に該当するものはどれか。

令和5年春期　問41
236問目／選択範囲の問題数237問

ア　PCなどの機器に搭載され，鍵生成，ハッシュ演算及び暗号処理を行うセキュリティチップ

イ　受信した電子メールが正当な送信者から送信されたものであることを保証する送信ドメイン認証技術

ウ　ファイアウォール，侵入検知，マルウェア対策など，複数のセキュリティ機能を統合したネットワーク監視装置

エ　ログデータを一元的に管理し，セキュリティイベントの監視者への通知及び相関分析を行うシステム

❑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：ウ”

❑解説

TPM(Trusted Platform Module)は、PCのマザーボード上に直付けされるセキュリティチップで、暗号化と復号、鍵ペアの生成と管理、ハッシュ値の計算、乱数生成、デジタル署名の生成・検証などの機能を有します。

TPMによって提供されるセキュリティ機能には以下のようなものがあります。

- OSやアプリケーションの改ざん検知
- 端末認証
- プラットフォームの整合性の検証
- ストレージ全体の暗号化

したがって「ア」が適切です。

ア “PCなどの機器に搭載され，鍵生成，ハッシュ演算及び暗号処理を行うセキュリティチップ”

正しい。TPMの説明です。

イ “受信した電子メールが正当な送信者から送信されたものであることを保証する送信ドメイン認証技術”

SPF(Sender Policy Framework)の説明です。

ウ “ファイアウォール，侵入検知，マルウェア対策など，複数のセキュリティ機能を統合したネットワーク監視装置”

UTM(Unified Threat Management，統合脅威管理)の説明です。

エ “ログデータを一元的に管理し，セキュリティイベントの監視者への通知及び相関分析を行うシステム”

SIEM(Security Information and Event Management)の説明です。

"政府情報システムのためのセキュリティ評価制度(ISMAP)"の説明はどれか。

令和5年春期　問39
237問目／選択範囲の問題数237問

ア　個人情報の取扱いについて政府が求める保護措置を講じる体制を整備している事業者などを評価して，適合を示すマークを付与し，個人情報を取り扱う政府情報システムの運用について，当該マークを付与された者への委託を認める制度

イ　個人データを海外に移転する際に，移転先の国の政府が定めた情報システムのセキュリティ基準を評価して，日本が求めるセキュリティ水準が確保されている場合には，本人の同意なく移転できるとする制度

ウ　政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価，登録することによって，政府のクラウドサービス調達におけるセキュリティ水準の確保を図る制度

エ　プライベートクラウドの情報セキュリティ全般に関するマネジメントシステムの規格にパブリッククラウドサービスに特化した管理策を追加した国際規格を基準にして，政府情報システムにおける情報セキュリティ管理体制を評価する制度

❑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

"政府情報システムのためのセキュリティ評価制度(ISMAP：イスマップ)"は、国際標準等を踏まえて政府が策定したセキュリティ基準に基づき、各基準が適切に実施されているかを第三者が監査するプロセスを経て、クラウドサービスを登録する国の制度です。登録されたサービスは「ISMAPクラウドサービスリスト（以下、本リスト）」として公開され、政府機関は本リストに掲載されたサービスから調達を行うことが原則となっています。また民間事業者においても本リストを参照することで、クラウドサービスの適切な活用が推進されることが期待されています。

国が政府情報システムを整備する際に、クラウドサービスの利用を第一候補とする方針(クラウド・バイ・デフォルト原則)を受け、政府機関等におけるクラウドサービスの導入に当たって、統一的な安全性評価基準のもとで情報セキュリティ対策が十分に行われているサービスを円滑に導入できるように立ち上げられたものです。

したがって「ウ」が適切な説明です。

ア “個人情報の取扱いについて政府が求める保護措置を講じる体制を整備している事業者などを評価して，適合を示すマークを付与し，個人情報を取り扱う政府情報システムの運用について，当該マークを付与された者への委託を認める制度”

プライバシーマーク制度に関する記述です。

イ “個人データを海外に移転する際に，移転先の国の政府が定めた情報システムのセキュリティ基準を評価して，日本が求めるセキュリティ水準が確保されている場合には，本人の同意なく移転できるとする制度”

個人情報保護法が定める、外国にある第三者に個人データを提供する場合の規制制度に関する記述です。

ウ “政府が求めるセキュリティ要求を満たしているクラウドサービスをあらかじめ評価，登録することによって，政府のクラウドサービス調達におけるセキュリティ水準の確保を図る制度”

正しい。ISMAPの説明です。

エ “プライベートクラウドの情報セキュリティ全般に関するマネジメントシステムの規格にパブリッククラウドサービスに特化した管理策を追加した国際規格を基準にして，政府情報システムにおける情報セキュリティ管理体制を評価する制度”

クラウドセキュリティ認証に関する記述です。