【応用_午前_過去問】セキュリティ②

☆

メッセージの送受信における署名鍵の使用に関する記述のうち，適切なものはどれか。

令和4年春期　問39
51問目／選択範囲の問題数237問

ア　送信者が送信者の署名鍵を使ってメッセージに対する署名を作成し，メッセージに付加することによって，受信者が送信者による署名であることを確認できるようになる。

イ　送信者が送信者の署名鍵を使ってメッセージを暗号化することによって，受信者が受信者の署名鍵を使って，暗号文を元のメッセージに戻すことができるようになる。

ウ　送信者が送信者の署名鍵を使ってメッセージを暗号化することによって，メッセージの内容が関係者以外に分からないようになる。

エ　送信者がメッセージに固定文字列を付加し，更に送信者の署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようになる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

ア “送信者が送信者の署名鍵を使ってメッセージに対する署名を作成し，メッセージに付加することによって，受信者が送信者による署名であることを確認できるようになる。”

正しい。デジタル署名の手順です。署名は、メッセージのダイジェストを送信者の秘密鍵で暗号化したものです。受信者は、まず署名を送信者の公開鍵でダイジェストに復号します。秘密鍵を所有するのはダイジェストを作成した送信者だけなので、正しく復号できれば送信者が署名をしたことを確認できます。

イ “送信者が送信者の署名鍵を使ってメッセージを暗号化することによって，受信者が受信者の署名鍵を使って，暗号文を元のメッセージに戻すことができるようになる。”

送信者の署名鍵(秘密鍵)で暗号化されたメッセージは、送信者の公開鍵でしか復号できません。暗号化通信で暗号化に使うのは受信者の公開鍵です。

ウ “送信者が送信者の署名鍵を使ってメッセージを暗号化することによって，メッセージの内容が関係者以外に分からないようになる。”

署名鍵は秘密鍵です。秘密鍵で暗号化したメッセージは公開鍵を使えば誰でも復号することができてしまうので、メッセージの機密性を確保することはできません。

エ “送信者がメッセージに固定文字列を付加し，更に送信者の署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようになる。”

デジタル署名で確認できるのは改ざんがあったかどうかであり、改ざん部位の特定はできません。

☆☆☆

送信者がメッセージからブロック暗号(方式)を用いて生成したメッセージ認証符号(MAC: message authentication code)をメッセージとともに送り，受信者が受け取ったメッセージからMACを生成して，送られてきたMACと一致することを確認するメッセージ認証で使用される鍵の組合せはどれか。

平成18年春期　問74
52問目／選択範囲の問題数237問

	送信者	受信者
ア	受信者と共有している共通鍵	送信者と共有している共通鍵
イ	受信者の公開鍵	受信者の秘密鍵
ウ	送信者の公開鍵	受信者の秘密鍵
エ	送信者の秘密鍵	受信者の公開鍵

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

ア　“あなたの解答：イ”

❑解説

MAC(Message Authentication Code)は、通信内容の改ざんの有無を検証し、完全性を保証するために通信データから生成される固定長のビット列です。
MACの生成には、共通鍵暗号を用いたもの(DES-MACやAES-MAC)とハッシュ関数を用いたもの(HMAC)がありますが、設問ではブロック暗号を用いてMACを生成しているので共通鍵暗号を用いた方式であることがわかります。

したがって生成と検証に使用されるのは「共有している共通鍵」が適切です。

☆☆

パスワードリスト攻撃に該当するものはどれか。

平成27年春期　問39
53問目／選択範囲の問題数237問

ア　一般的な単語や人名からパスワードのリストを作成し，インターネットバンキングへのログインを試行する。

イ　想定され得るパスワードとそのハッシュ値との対のリストを用いて，入手したハッシュ値からパスワードを効率的に解析する。

ウ　どこかのWebサイトから流出した利用者IDとパスワードのリストを用いて，他のWebサイトに対してログインを試行する。

エ　ピクチャパスワードの入力を録画してリスト化しておき，それを利用することでタブレット端末へのログインを試行する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：ア”

❑解説

パスワードリスト攻撃は、複数のサイトで同様のID・パスワードの組合せを使用している利用者が多いという傾向を悪用したもので、あるサイトに対する攻撃などによって得られたIDとパスワードのリストを用いて、別のサイトへの不正ログインを試みる攻撃です。

この攻撃に対しては、利用者側で「パスワードの使いまわしをやめる」ことや、管理者側で「2段階認証を行う」「ログイン履歴を表示し利用者に確認してもらう」などの対策が考えられます。

ア “一般的な単語や人名からパスワードのリストを作成し，インターネットバンキングへのログインを試行する。”

辞書攻撃の説明です。

イ “想定され得るパスワードとそのハッシュ値との対のリストを用いて，入手したハッシュ値からパスワードを効率的に解析する。”

レインボーテーブル攻撃の説明です。

ウ “どこかのWebサイトから流出した利用者IDとパスワードのリストを用いて，他のWebサイトに対してログインを試行する。”

正しい。パスワードリスト攻撃の説明です。

エ “ピクチャパスワードの入力を録画してリスト化しておき，それを利用することでタブレット端末へのログインを試行する。”

ピクチャパスワードとは、任意の画像上とその画像上で行われるタッチジェスチャーやマウスのポインティング操作などの組合せで認証を行う方式です。パスワードリスト攻撃は、特定の端末ではなくWebサービスへの不正ログインを狙う攻撃なので誤りです。

☆☆☆

無線LANを利用するとき，セキュリティ方式としてWPA2を選択することで利用される暗号化アルゴリズムはどれか。

平成26年秋期　問41
54問目／選択範囲の問題数237問

ア	AES	イ	ECC	ウ	RC4	エ	RSA

❑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：エ”

❑解説

WPA2(Wi-Fi Protected Access 2)は、無線LANのセキュリティプロトコル「WPA」の脆弱性を改善した次期バージョンです。暗号化アルゴリズムが、WEP、WPAで使用されていた脆弱性のある「RC4」からNIST標準の「AES」に変更され、解読攻撃に対する耐性が高められています。

したがって「ア」が適切です。

☆

安全なWebアプリケーションの作り方について，攻撃と対策の適切な組合せはどれか。

平成26年春期　問40
55問目／選択範囲の問題数237問

	攻撃	対策
ア	SQL インジェクション	SQL 文の組立てに静的プレースホルダを使用する。
イ	クロスサイトスクリプティング	任意の外部サイトのスタイルシートを取り込めるようにする。
ウ	クロスサイトリクエストフォージェリ	リクエストに GET メソッドを使用する。
エ	セッションハイジャック	利用者ごとに固定のセッション ID を使用する。

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

ア　“あなたの解答：ア”

❑解説

Webアプリケーションに対するそれぞれの攻撃手法を確認しておきましょう。

SQLインジェクション

Webアプリケーションに対してデータベースへの命令文を構成する不正な入力データを与え、Webアプリケーションが想定していないSQL文を意図的に実行させることで、データベースを破壊したり情報を不正取得したりする攻撃。

クロスサイトスクリプティング

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、サイト間を横断して悪意のあるスクリプトを混入させることでユーザーのクッキーを盗むなどの攻撃を行う行為。

クロスサイトリクエストフォージェリ

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手法。会員制サイトでログイン状態であるときに会員情報の変更や商品の注文画面への直接リンクを踏ませる(またはスクリプトでリダイレクトする)などの意図しない不正な処理要求を行わせる行為がこれに該当する。

セッションハイジャック

認証が完了してセッションを開始しているブラウザとWebサーバの間の通信において、Cookieやセッション情報を盗むことで、対象セッションを通信当事者以外が乗っ取る攻撃手法。

ア 正しい。**プレースホルダ**は、SQL文中のユーザー入力を割り当てる部分に特殊文字(?など)を使用したひな形を用意し、後から実際の値を割り当てる機構です。後から割り当てる値は、SQL文の特殊文字がエスケープされた完全な数値または文字列として扱われるため安全に実行することができます。

イ スタイルシートには"expression"文のようにJavaScriptを直接記述できる部分があるため、不用意に別ドメインのCSSを読込むと悪意のあるスクリプトによってXSSの被害を受ける可能性があります。またスタイルシートの"import"文によってスクリプトファイルがダウンロードさせてしまうおそれもあります。
これらの脅威は2020年現在はブラウザによりブロックされることがほとんどです。しかし、スタイルシートはWebページのデザインを指定する言語ですが、設定できる範囲は広く、悪意を持って使用すれば任意の要素を消したり、出現させたりというようにページの表示を改ざんすることも可能です（CSSインジェクション）。この観点からも信用できない外部CSSは読む込むべきではないと言えます。

ウ GETメソッドを使用すると、URLから秘密情報を読みとられたり改ざんされたりという可能性が高くなるのでPOSTメソッドを使用すべきです。
GETやPOSTというのはWebブラウザからサーバへのパラメータの受け渡し型の違いです。GETメソッドは、"hoge.php?mode=new&uid=34632847"というようにURLの後ろにパラメータを付加して送信する方式、POSTメソッドは、パラメータをメッセージボディにセットしサーバに渡す方式です。

エ 固定のセッションIDはセッションハイジャックのターゲットになりやすいので危険です。

☆☆☆

JPCERTコーディネーションセンターの説明はどれか。

令和3年春期　問42
56問目／選択範囲の問題数237問

ア　産業標準化法に基づいて経済産業省に設置されている審議会であり，産業標準化全般に関する調査・審議を行っている。

イ　電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり，総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される。

ウ　特定の政府機関や企業から独立した組織であり，国内のコンピュータセキュリティインシデントに関する報告の受付，対応の支援，発生状況の把握，手口の分析，再発防止策の検討や助言を行っている。

エ　内閣官房に設置され，我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ウ　“あなたの解答：ウ”

❑解説

JPCERTコーディネーションセンター(JPCERT/CC)は、インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっています。
特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいます。

引用元:JPCERTコーディネーションセンター「JPCERT/CCについて」
https://www.jpcert.or.jp/about/

ア “産業標準化法に基づいて経済産業省に設置されている審議会であり，産業標準化全般に関する調査・審議を行っている。”

日本産業標準調査会(JISC)の説明です。

イ “電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり，総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される。”

CRYPTRECの説明です。

ウ “特定の政府機関や企業から独立した組織であり，国内のコンピュータセキュリティインシデントに関する報告の受付，対応の支援，発生状況の把握，手口の分析，再発防止策の検討や助言を行っている。”

正しい。JPCERT/CCの説明です。

エ “内閣官房に設置され，我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である。”

NISC(内閣サイバーセキュリティセンター)の説明です。

SSHの説明はどれか。

ア　MIMEを拡張した電子メールの暗号化とデジタル署名に関する標準

イ　オンラインショッピングで安全にクレジット決済を行うための仕様

ウ　対称暗号技術と非対称暗号技術を併用して電子メールの暗号化，復号の機能をもつ電子メールソフト

エ　リモートログインやリモートファイルコピーのセキュリティを強化したツール及びプロトコル

❑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

SSH(Secure Shell)は、公開鍵暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルであり、SSLと同様にトランスポート層とアプリケーション層で通信を暗号化します。

当初はrlogin，rshやTelnetを安全に利用する手段として用いられていましたが、現在ではポートフォワーディング機能を用いることで、**POP3**や**FTP**などネットワーク上に平文のパスワードが流れてしまう既存のプロトコルを安全に利用する技術としても広く利用されています。

ポートフォワーディング

ローカルホストの任意のポートに送信したデータを、リモートホストの特定ポートへ転送する機能

ア　“MIMEを拡張した電子メールの暗号化とデジタル署名に関する標準”

S/MIME(Secure Multipurpose Internet Mail Extensions)の説明です。

イ　“オンラインショッピングで安全にクレジット決済を行うための仕様”

SET(Secure Electronic Transaction)の説明です。

ウ　“対称暗号技術と非対称暗号技術を併用して電子メールの暗号化，復号の機能をもつ電子メールソフト”

PGP(Pretty Good Privacy)の説明です。

エ　“リモートログインやリモートファイルコピーのセキュリティを強化したツール及びプロトコル”

正しい。SSHの説明です。

☆☆☆

コンピュータウイルスの検出，機能の解明，又は種類の特定をする方法について，適切な記述はどれか。

平成18年秋期　問7
58問目／選択範囲の問題数237問

ア　暗号化された文書中のマクロウイルスを検出するにはパターンマッチング方式が有効である。

イ　逆アセンブルは，バイナリタイプの新種ウイルスの機能を解明するのに有効な手法である。

ウ　不正な動作を識別してウイルスを検知する方式は，ウイルス名を特定するのに最も有効である。

エ　ワームは既存のファイルに感染するタイプのウイルスであり，その感染の有無の検出にはファイルの大きさの変化を調べるのが有効である。

❑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

イ　“あなたの解答：ア”

❑解説

実行ファイルをアセンブリ言語に逆変換することを**逆アセンブル**といいます。
ソースコードを入手することができないソフトウェアでも、機械語ではなくプログラマが理解しやすいアセンブリ言語に変換することで内部の動作を解析することができるようになります。

ア “暗号化された文書中のマクロウイルスを検出するにはパターンマッチング方式が有効である。”

パターンマッチングは、「パターンファイル」「ウイルス定義ファイル」等を用いて、何らかの特徴的なコードをパターンとしてウイルス検査対象と比較することで検出する手法ですが、暗号化されたウィルスには効果を発揮しません。

イ “逆アセンブルは，バイナリタイプの新種ウイルスの機能を解明するのに有効な手法である。”

正しい。

ウ “不正な動作を識別してウイルスを検知する方式は，ウイルス名を特定するのに最も有効である。”

不正な動作を識別してウイルスを検知する方式はビヘイビア法といい、既知のウイルスの亜種を検知するのに有効です。

エ “ワームは既存のファイルに感染するタイプのウイルスであり，その感染の有無の検出にはファイルの大きさの変化を調べるのが有効である。”

ワームは宿主を必要とせず自己複製を行う機能をもっているので、ファイルサイズの検査は有効ではありません。

☆

クロスサイトスクリプティングの手口はどれか。

平成30年春期　問37
59問目／選択範囲の問題数237問

ア　Webアプリケーションのフォームの入力フィールドに，悪意のあるJavaScriptコードを含んだデータを入力する。

イ　インターネットなどのネットワークを通じてサーバに不正にアクセスしたり，データの改ざんや破壊を行ったりする。

ウ　大量のデータをWebアプリケーションに送ることによって，用意されたバッファ領域をあふれさせる。

エ　パス名を推定することによって，本来は認証された後にしかアクセスが許可されていないページに直接ジャンプする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑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 “Webアプリケーションのフォームの入力フィールドに，悪意のあるJavaScriptコードを含んだデータを入力する。”

正しい。クロスサイトスクリプティングの手口です。

イ “インターネットなどのネットワークを通じてサーバに不正にアクセスしたり，データの改ざんや破壊を行ったりする。”

クラッキングの手口です。

ウ “大量のデータをWebアプリケーションに送ることによって，用意されたバッファ領域をあふれさせる。”

バッファオーバーフロー攻撃の手口です。

エ “パス名を推定することによって，本来は認証された後にしかアクセスが許可されていないページに直接ジャンプする。”

ディレクトリトラバーサル攻撃の手口です。

☆☆☆☆☆

攻撃にHTTP over TLS(HTTPS)が使われた場合に起こり得ることはどれか。

平成29年春期　問44
60問目／選択範囲の問題数237問

ア　HTTPSを使ったSQLインジェクション攻撃を受けると，Webアプリケーションでデータベースへの不正な入力をチェックできないので，悪意のあるSQLが実行されてしまう。

イ　HTTPSを使ったクロスサイトスクリプティング攻撃を受けると，Webブラウザでプログラムやスクリプトを実行しない設定にしても実行を禁止できなくなるので，悪意のあるWebサイトからダウンロードされたプログラムやスクリプトが実行されてしまう。

ウ　HTTPSを使ったブルートフォース攻撃を受けると，ログイン試行のチェックができないので，Webアプリケーションでアカウントロックなどの対策が実行できなくなってしまう。

エ　攻撃者が社内ネットワークに仕掛けたマルウェアによってHTTPSが使われると，通信内容がチェックできないので，秘密情報が社外に送信されてしまう。

❑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

HTTPSを使用したとき、通信データが暗号化されるのは「クライアントとサーバの間」です。Webサーバは暗号化されたデータを平文のHTTPリクエストに復号した後、リクエストに応じた処理を行います。

ア “HTTPSを使ったSQLインジェクション攻撃を受けると，Webアプリケーションでデータベースへの不正な入力をチェックできないので，悪意のあるSQLが実行されてしまう。”

Webサーバで処理される際のHTTPリクエストは平文の状態です。このためSQLの実行前にクライアントからの入力データをチェック／無害化できます。

イ “HTTPSを使ったクロスサイトスクリプティング攻撃を受けると，Webブラウザでプログラムやスクリプトを実行しない設定にしても実行を禁止できなくなるので，悪意のあるWebサイトからダウンロードされたプログラムやスクリプトが実行されてしまう。”

クライアント側でJavaScriptを無効にしていれば、JavaScriptのコードが実行されることはありません。

ウ “HTTPSを使ったブルートフォース攻撃を受けると，ログイン試行のチェックができないので，Webアプリケーションでアカウントロックなどの対策が実行できなくなってしまう。”

Webサーバで処理される際のHTTPリクエストは平文の状態です。このためWebサーバ側で攻撃対象のIDやリクエスト主の情報を把握し、ロックアウト等の措置をとることが可能です。

エ “攻撃者が社内ネットワークに仕掛けたマルウェアによってHTTPSが使われると，通信内容がチェックできないので，秘密情報が社外に送信されてしまう。”

正しい。HTTPSではクライアントーサーバ間の通信が暗号化されます。このため、もし通信経路上にプロキシサーバ等が介在したとしても内容のチェックはできません。

完全性を脅かす攻撃はどれか。

平成24年秋期　問40
61問目／選択範囲の問題数237問

ア　Webページの改ざん

イ　システム内に保管されているデータの持出しを目的とした不正コピー

ウ　システムを過負荷状態にするDoS攻撃

エ　通信内容の盗聴

❑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

完全性（Integrity）は、情報セキュリティマネジメントで管理すべき要素の一つで、「情報の正確さ完全さ」を示す特性です。具体的には、情報に矛盾がなく完備され、最新であり、改ざん、破壊されていない状態で維持されている度合いをいいます。

また「完全性」とともに情報セキュリティマネジメントの三要素と位置付けられている特性に「機密性」と「可用性」があります。

機密性（Confidentiality）

許可されていないユーザーやシステムに対して情報を使用させず、開示しない特性。許可された正規のユーザーだけが情報にアクセスできる度合いを示す

可用性（Availability）

ユーザーが要求したときにシステムが利用可能である特性。障害がなくシステムが正常に稼働し続けることの度合いを示す

各選択肢の事例がどの要素を脅かすものかを考えます。

ア “Webページの改ざん”

正しい。改ざんによる情報の破壊は、完全性を低下させる事象です。

イ “システム内に保管されているデータの持出しを目的とした不正コピー”

許可されていない者に情報が漏れるので、機密性を脅かす攻撃です。

ウ “システムを過負荷状態にするDoS攻撃”

サービス停止を引き起こすDoS攻撃は、可用性を脅かす攻撃です。

エ “通信内容の盗聴”

許可されていない者に情報が漏れるので、機密性を脅かす攻撃です。

☆☆☆

不正利用を防止するためにメールサーバ(SMTPサーバ)で行う設定はどれか。

平成19年秋期　問72
62問目／選択範囲の問題数237問

ア　ゾーン転送のアクセス元を制御する。

イ　第三者中継を禁止する。

ウ　ディレクトリに存在するファイル名の表示を禁止する

エ　特定のディレクトリ以外でのCGIプログラムの実行を禁止する。

❑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

イ　“あなたの解答：ア”

❑解説

SMTP(Simple Mail Transfer Protocol)を使用した一部のメールサーバソフトウェアは、誰からのメールでも受け付けるというの初期設定になっていました。さらにSMTPには、投稿者を認証する仕組みがないためにネットワーク外の第三者から別の第三者へのメールを無制限に受け付け中継してしまいます。
このような第三者中継を禁止することで迷惑メールの発信者などの不正利用からメールサーバを防ぐことができます。

ア “ゾーン転送のアクセス元を制御する。”

存在するホストとそのIPアドレスが知られるのを防ぐためにDNSサーバに行う設定です。

イ “第三者中継を禁止する。”

正しい。メールサーバに行う設定です。

ウ “ディレクトリに存在するファイル名の表示を禁止する”

Webサーバでディレクトリにアクセスしたときにファイルの一覧が表示されてしまうのを防ぐための対策です。

エ “特定のディレクトリ以外でのCGIプログラムの実行を禁止する。”

Webサーバに行うパーミッション(アクセス権)設定の説明です。

☆☆☆

ICカードの情報の解読や偽造に対して，物理的に情報を保護するための機能を示すものはどれか。

平成19年春期　問75
63問目／選択範囲の問題数237問

ア	SECE	イ	インターロック
ウ	インボリューション	エ	耐タンパ性

❑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

エ　“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。

ア　“SECE”

Secure Electronic Commerce Environmentの略。オンライン決済の通信を行う際の国際標準的プロトコルであるSET(Secure Electronics Transaction)を日本独自に拡張したプロトコルです。

イ　“インターロック”

インターロックは、誤操作や確認不足から機器に生じる誤作動を防止する安全機構です。「すべての扉が閉まっていなければ機械が動作を開始しない仕組みにする」などがその例です。

ウ　“インボリューション”

インボリューションは、共通鍵暗号のブロック暗号方式において解読されにくい暗号文を生成するためのデータランダム化のテクニックです。

エ　“耐タンパ性”

正しい。

☆☆☆
※解説読み込む

利用者PCがボットに感染しているかどうかをhostsファイルの改ざんの有無で確認するとき，hostsファイルが改ざんされていないと判断できる設定内容はどれか。ここで，hostsファイルには設定内容が1行だけ書かれており，利用者及びシステム管理者は，これまでにhostsファイルを変更していないものとする。

平成27年春期　問45
64問目／選択範囲の問題数237問

	設定内容	説　明
ア	127.0.0.1　a.b.com	a.b.com は利用者 PC の OS 提供元の FQDN を示す。
イ	127.0.0.1　c.d.com	c.d.com は利用者 PC の製造元の FQDN を示す。
ウ	127.0.0.1　e.f.com	e.f.com はウイルス定義ファイルの提供元の FQDN を示す。
エ	127.0.0.1　localhost	localhost は利用者 PC 自身を示す。

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

エ　“あなたの解答：エ”

❑解説

hostsファイルは、TCP/IPを利用するコンピュータにおいてIPアドレスとホスト名の対応を記述するファイルです。hostsファイルでは「IPアドレス ホスト名」の形式で1つの行につき1つの対応を記述します。

IPアドレス「127.0.0.1」は、現在使用している自分自身のコンピュータ(localhost)を指定する特別なアドレス(ローカル・ループバック・アドレス)です。つまり「127.0.0.1」の対応ホストとして「localhost」以外が設定されている「ア」「イ」「ウ」は改ざんが行われた可能性があると判断できます。よって正解は「エ」になります。

Windows環境ではDNSの設定よりもhostsファイルの設定が優先されるので、攻撃者によりhostsファイルが改ざんされると不正なURLへ誘導されたり、攻撃の踏み台にされたりするなどの被害が発生する可能性があります。

☆☆☆

Webアプリケーションにおけるセキュリティ上の脅威と対策の適切な組合せはどれか。

平成26年秋期　問40
65問目／選択範囲の問題数237問

ア　OSコマンドインジェクションを防ぐために， Webアプリケーションが発行するセッションIDを推測困難なものにする。

イ　SQLインジェクションを防ぐために，Webアプリケーション内でデータベースへの問合せを作成する際にバインド機構を使用する。

ウ　クロスサイトスクリプティングを防ぐために，外部から渡す入力データをWebサーバ内のファイル名として直接指定しない。

エ　セッションハイジャックを防ぐために，Webアプリケーションからシェルを起動できないようにする。

❑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：ウ”

❑解説

問題文に登場するそれぞれの攻撃手法は次のようなものです。

OSコマンドインジェクション

ユーザーの入力をもとにOSのコマンドを発行して処理を行うWebアプリケーションに対して、不正なコマンドを渡すことで任意のファイルに対する読出し、変更、削除、パスワードの取得などを行う攻撃。OSコマンドの呼出しに使われる関数は、C、Perl、PHPの `exec` や `system` 、入力値としてコマンドを許しているPerlの `open` 関数などがある

SQLインジェクション

Webアプリケーションに対してデータベースへの命令文を構成する不正な入力データを与え、Webアプリケーションが想定していないSQL文を意図的に実行させることで、データベースを破壊したり情報を不正取得したりする攻撃

クロスサイトスクリプティング

動的にWebページを生成するアプリケーションに対して、セキュリティ上の不備を突いた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、別のサイトを介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

セッションハイジャック

認証が完了しているWebブラウザとWebサーバの間の通信を傍受するなどして、Cookieやセッション IDなどのセッション情報を盗み取ることで、第三者が対象セッションを乗っ取る攻撃

ア "OSコマンドインジェクションを防ぐために， Webアプリケーションが発行するセッションIDを推測困難なものにする。"

セッションハイジャックを防ぐための対策です。

イ "SQLインジェクションを防ぐために，Webアプリケーション内でデータベースへの問合せを作成する際にバインド機構を使用する。"

正しい。SQLインジェクションは、利用者が入力した値をそのままSQL文の一部として使ってしまうことで攻撃が成立します。プレースホルダは、利用者入力部分に特殊文字（?など）を割り当てたSQL文のひな形を用意し、特殊文字部分には実行時にエスケープ処理された値を割り当てる仕組みです。SQLインジェクションを狙った不正な文字が含まれていたとしても、SQL文の命令文の一部ではなく、単なる値として認識されるため安全に実行することができます。

```
//PHPにおけるプレースホルダの一例
$uid = $_POST["userid"];
$sql = 'SELECT * FROM USER WHERE uid = ?' //?がプレースホルダ
$pdo = new PDO($dbh, $user, $password);
$stmt = $pdo->prepare($sql);
$stmt->execute([$uid]); //?に値を割り当てて実行
```

ウ "クロスサイトスクリプティングを防ぐために，外部から渡す入力データをWebサーバ内のファイル名として直接指定しない。"

ディレクトリトラバーサル攻撃を防ぐための対策です。ディレクトリトラバーサル攻撃は、Webサーバの非公開ファイルへのアクセスを試みる攻撃です。

エ "セッションハイジャックを防ぐために，Webアプリケーションからシェルを起動できないようにする。"

OSコマンドインジェクションを防ぐための対策です。

☆☆☆

IoT推進コンソーシアム，総務省，経済産業省が策定した"IoTセキュリティガイドライン(ver1.0)"における"要点17. 出荷・リリース後も安全安心な状態を維持する"に対策例として挙げられているものはどれか。

令和3年秋期　問37
66問目／選択範囲の問題数237問

ア　IoT機器及びIoTシステムが収集するセンサーデータ，個人情報などの情報の洗い出し，並びに保護すべきデータの特定

イ　IoT機器のアップデート方法の検討，アップデートなどの機能の搭載，アップデートの実施

ウ　IoT機器メーカー，IoTシステムやサービスの提供者，利用者の役割の整理

エ　PDCAサイクルの実施，組織としてIoTシステムやサービスのリスクの認識，対策を行う体制の構築

❑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：ア”

❑解説

IoTセキュリティガイドラインは、IoT特有の性質とセキュリティ対策の必要性を踏まえて、IoT機器やシステム、サービスについて、その関係者がセキュリティ確保等の観点から求められる基本的な取組を、セキュリティ・バイ・デザインを基本原則としつつ明確化するものです。

IoT機器の開発から IoTサービスの提供までの流れを、「方針」「分析」「設計」「構築・接続」「運用・保守」の5つの段階に分けた上で、それぞれの段階に対するセキュリティ対策指針を示すとともに、指針ごとに具体的な要点を挙げ、ポイントと解説、対策例を記載しています。

大項目	指針	要点
方針	指針1 IoT の性質を考慮した基本方針を定める	要点 1. 経営者が IoT セキュリティにコミットする
		要点 2. 内部不正やミスに備える
分析	指針2 IoT のリスクを認識する	要点 3. 守るべきものを特定する
		要点 4. つながることによるリスクを想定する
		要点 5. つながりで波及するリスクを想定する
		要点 6. 物理的なリスクを認識する
		要点 7. 過去の事例に学ぶ
設計	指針3 守るべきものを守る設計を考える	要点 8. 個々でも全体でも守れる設計をする
		要点 9. つながる相手に迷惑をかけない設計をする
		要点 10. 安全安心を実現する設計の整合性をとる
		要点 11. 不特定の相手とつなげられても安全安心を確保できる設計をする
		要点 12. 安全安心を実現する設計の検証・評価を行う
構築・接続	指針4 ネットワーク上での対策を考える	要点 13. 機器等がどのような状態かを把握し、記録する機能を設ける
		要点 14. 機能及び用途に応じて適切にネットワーク接続する
		要点 15. 初期設定に留意する
		要点 16. 認証機能を導入する
運用・保守	指針5 安全安心な状態を維持し、情報発信・共有を行う	要点 17. 出荷・リリース後も安全安心な状態を維持する
		要点 18. 出荷・リリース後も IoT リスクを把握し、関係者に守ってもらいたいことを伝える
		要点 19. つながることによるリスクを一般利用者に知ってもらう
		要点 20. IoT システム・サービスにおける関係者の役割を認識する
		要点 21. 脆弱な機器を把握し、適切に注意喚起を行う

図　IoTセキュリティガイドライン(ver1.0)におけるセキュリティ対策指針一覧

IoTセキュリティガイドライン(ver1.0) P12から引用
https://www.soumu.go.jp/main_content/000428393.pdf

本問の要点は、出荷・リリース後に関するものですから運用・保守段階に行うべき対策例を選ぶことになります。

ア "IoT機器及びIoTシステムが収集するセンサーデータ，個人情報などの情報の洗い出し，並びに保護すべきデータの特定"

"分析"段階における"要点3. 守るべきものを特定する"の対策例です。
本ガイドラインでは、IoTの安全安心の観点で、守るべき本来機能や情報、つなげるための機能について特定することとしており、その対策例として、IoT機器・システムが収集するセンサーデータや個人情報（プライバシー含む）、所有する設計情報などの技術情報の洗い出しが挙げられています。

イ "IoT機器のアップデート方法の検討，アップデートなどの機能の搭載，アップデートの実施"

正しい。"運用・保守"段階における"要点17. 出荷・リリース後も安全安心な状態を維持する"の対策例です。
本ガイドラインでは、IoTシステム・サービスの提供者等は、IoT機器のセキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用することとしており、その対策例として、アップデート方法の検討、アップデート等の機能の搭載、アップデートの実施が挙げられています。

ウ "IoT機器メーカー，IoTシステムやサービスの提供者，利用者の役割の整理"

"運用・保守"段階における"要点20. IoTシステム・サービスにおける関係者の役割を認識する"の対策例です。
本ガイドラインでは、IoT機器メーカーやIoTシステム・サービス提供者及び一般利用者の役割を整理することとしており、その対策例として、IoT機器メーカーやIoTシステム・サービス提供者及び利用者の役割の整理が挙げられています。

エ "PDCAサイクルの実施，組織としてIoTシステムやサービスのリスクの認識，対策を行う体制の構築"

"方針"段階における"要点1. 経営者がIoTセキュリティにコミットする"の対策例です。
本ガイドラインでは、経営者は、「サイバーセキュリティ経営ガイドライン」を踏まえた対応を行う。IoTセキュリティの基本方針を企業として策定し社内に周知するとともに、継続的に実現状況を把握し、見直していく。また、そのために必要な体制・人材を整備することとしており、その対策例として、PDCAサイクルを回し、組織としてIoTシステム・サービスのリスクを認識し対策を行う体制を構築・維持することが挙げられています。

☆☆☆

Webサイトにおいて，クリックジャッキング攻撃の対策に該当するものはどれか。

令和3年春期　問37
67問目／選択範囲の問題数237問

ア　HTTPレスポンスヘッダーにX-Content-Type-Optionsを設定する。

イ　HTTPレスポンスヘッダーにX-Frame-Optionsを設定する。

ウ　入力にHTMLタグが含まれていたら，HTMLタグとして解釈されないほかの文字列に置き換える。

エ　入力文字数が制限を超えているときは受け付けない。

❑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

クリックジャッキングは、攻撃者が用意したWebページの前面に透明化した別のWebページを重ねることでユーザーを視覚的にだまし、正常に視認できるWebページ上をクリックさせることで、透明化したWebページのコンテンツを操作させる攻撃です。ユーザーのクリックを奪うという攻撃の特徴からクリック・ジャッキングと呼ばれます。

図4 2つの部品を重ねるイメージ
※IPA資料より引用

ア “HTTPレスポンスヘッダーにX-Content-Type-Optionsを設定する。”

"X-Content-Type-Options"は、ブラウザによるMIMEスニッフィングの有効・無効を指示するためのHTTPヘッダーで、値として"nosniff"を指定することがクロスサイトスクリプティングへの対策になります。
MIMEスニッフィングとは、WebサーバからMIMEタイプ（メディアの種類）が指定されないなどの理由でリソースのMIMEタイプが不明なとき、ブラウザがリソースのバイトストリームを調べ、MIMEタイプを推定する機能です。これが有効になっていると、攻撃者がJSONや画像内に埋め込んだスクリプトを不正に実行してしまうおそれがあります。これを防止するためのヘッダーが"X-Content-Type-Options"です。

イ “HTTPレスポンスヘッダーにX-Frame-Optionsを設定する。”

正しい。"X-Frame-Options"は、フレーム要素（<frame>または<iframe>）を使用したコンテンツ表示を許可するかどうか指示するためのHTTPヘッダーで、値として"DENY(拒否)"または"SAMEORIGIN"を指定することがクリックジャッキング攻撃への対策となります。
クリックジャッキング攻撃は、別サイトのHTMLをフレーム要素で読込み、それを透明化して罠サイトの上に重ね合わせるため、フレーム要素を使用した他サイトの表示を禁止すれば防ぐことができます。

ウ “入力にHTMLタグが含まれていたら，HTMLタグとして解釈されないほかの文字列に置き換える。”

クロスサイトスクリプティングへの対策です。入力値に含まれる特殊文字を無害化する処理をサニタイジングと言います。

エ “入力文字数が制限を超えているときは受け付けない。”

バッファオーバーフロー攻撃への対策です。

☆☆

アクセス制御に用いる認証デバイスの特徴に関する記述のうち，適切なものはどれか。

平成28年秋期　問41
68問目／選択範囲の問題数237問

ア　USBメモリにデジタル証明書を組み込み，認証デバイスとする場合は，利用するPCのMACアドレスを組み込む必要がある。

イ　成人には虹(こう)彩の経年変化がなく，虹彩認証では，認証デバイスでのパターン更新がほとんど不要である。

ウ　静電容量方式の指紋認証デバイスでは，LED照明を設置した室内において正常に認証できなくなる可能性がある。

エ　認証に利用する接触型ICカードは，カード内のコイルの誘導起電力を利用している。

❑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 “USBメモリにデジタル証明書を組み込み，認証デバイスとする場合は，利用するPCのMACアドレスを組み込む必要がある。”

デジタル証明書が格納されたUSBメモリは、それ自体が鍵の役割を果たします。このためMACアドレスを組み込まなくても、USBメモリを挿し込みさえすればどのPCでも認証を受けられます。

イ “成人には虹(こう)彩の経年変化がなく，虹彩認証では，認証デバイスでのパターン更新がほとんど不要である。”

正しい。虹彩認証は、眼球の特徴で本人認証を行うバイオメトリクス認証技術です。虹彩とは、眼球の黒目部分、瞳孔の外側にある円状の部分のことで、その部分のしわのパターンが個人ごとに異なることを認証に利用しています。
虹彩認証の精度はメガネやコンタクトレンズを着用してもほとんど低下しません。年を経ると変化する顔や声と異なり、一度登録した虹彩パターンは生涯にわたって利用可能です。

ウ “静電容量方式の指紋認証デバイスでは，LED照明を設置した室内において正常に認証できなくなる可能性がある。”

認証デバイスに直に触れて指紋を読み取るため、室内の明るさは問題になりません。光源が認証精度に影響するのは顔認証や虹彩認証です。

エ “認証に利用する接触型ICカードは，カード内のコイルの誘導起電力を利用している。”

非接触型ICカードの説明です。接触型ICカードは、読み取り機に挿入した際に表面の金メッキの端子部分から外部電源が供給される仕組みになっています。これに対して非接触型ICカードは、読取り機の磁界を通過する際の誘導起電力を利用しています。

※その他選択肢

暗号化や認証機能をもち，遠隔にあるコンピュータに安全にログインするためのプロトコルはどれか。

平成29年秋期　問43
69問目／選択範囲の問題数237問

ア	L2TP	イ	RADIUS	ウ	SSH	エ	TLS

❑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

ア “L2TP”

Layer 2 Tunneling Protocolの略。OSI基本参照モデルの第2層におけるトンネリングプロトコルです。PPPなどのデータリンク層のフレームをIPヘッダーでカプセル化することで、ルータを越えた複数の拠点間でフレームのやり取りを実現します。暗号化の機能はないため必要に応じてIPsecと併用する必要があります。

イ “RADIUS”

Remote Authentication Dial In User Serviceの略。認証情報、認証手続および利用ログの記録（アカウンティング）をネットワーク上のサーバに一元化することを目的とした認証プロトコルです。

ウ “SSH”

正しい。**SSH**(Secure SHell)は、公開鍵暗号や認証の技術を利用して、リモートコンピュータと安全に通信するためのプロトコルです。
ネットワークを介して遠隔地のコンピュータを操作する「rlogin」や「rsh」などのUNIX系コマンドや「TELNET」などを安全に利用するための方式です。また、ポートフォワーディング機能を使って、FTP、POP、SMTPなどの暗号化機能をもたないプロトコルを安全に利用する手段としても使用されています。

エ “TLS”

Transport Layer Securityの略。ノード認証、暗号化通信、改ざん検知などのセキュリティ機能をOSI基本参照モデルのトランスポート層レベルで提供するプロトコルです。

SQLインジェクション対策として行う特殊文字の無効化操作はどれか。

平成20年春期　問70
70問目／選択範囲の問題数237問

ア	クロスサイトスクリプティング	イ	サニタイジング
ウ	パケットフィルタリング	エ	フィッシング

❑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

サニタイジング(sanitizing)は、ユーザーの入力値を受け取り処理するWebアプリケーションにおいて、入力データ中のスクリプトやコマンドとして特別な意味を持つ文字があった場合、HTML出力やコマンド発行の直前でエスケープ処理し無害化する操作です。

ア “クロスサイトスクリプティング”

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。

イ “サニタイジング”

正しい。

ウ “パケットフィルタリング”

パケットフィルタリングは、パケットのIPアドレスやポート番号によって通過の可否を判断しますが、データ部については検証を行わないので正当なHTTPリクエストに攻撃文を含めるSQLインジェクションを防ぐことはできません。

エ “フィッシング”

フィッシングは、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。

☆☆☆

サイドチャネル攻撃に該当するものはどれか。

令和4年秋期　問37
71問目／選択範囲の問題数237問

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量(処理時間，消費電流など)やエラーメッセージから，攻撃対象の秘密情報を得る。

イ　企業などの秘密情報を不正に取得するソーシャルエンジニアリングの手法の一つであり，不用意に捨てられた秘密情報の印刷物をオフィスの紙ごみの中から探し出す。

ウ　通信を行う2者間に割り込み，両者が交換する情報を自分のものとすり替えることによって，その後の通信を気付かれることなく盗聴する。

エ　データベースを利用するWebサイトに入力パラメータとしてSQL文の断片を送信することによって，データベースを改ざんする。

❑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：ウ”

❑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 “暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量(処理時間，消費電流など)やエラーメッセージから，攻撃対象の秘密情報を得る。”

正しい。サイドチャネル攻撃の説明です。

イ “企業などの秘密情報を不正に取得するソーシャルエンジニアリングの手法の一つであり，不用意に捨てられた秘密情報の印刷物をオフィスの紙ごみの中から探し出す。”

スキャベンジングの説明です。

ウ “通信を行う2者間に割り込み，両者が交換する情報を自分のものとすり替えることによって，その後の通信を気付かれることなく盗聴する。”

MITM攻撃(Man in the middle attack：中間者攻撃)の説明です。

エ “データベースを利用するWebサイトに入力パラメータとしてSQL文の断片を送信することによって，データベースを改ざんする。”

SQLインジェクションの説明です。

☆☆☆
※解説読む

クラウドのサービスモデルをNISTの定義に従ってIaaS，PaaS，SaaSに分類したとき，パブリッククラウドサービスの利用企業が行うシステム管理作業において，PaaSとSaaSでは実施できないが，IaaSでは実施できるものはどれか。

平成28年春期　問42
72問目／選択範囲の問題数237問

ア	アプリケーションの利用者ID管理
イ	アプリケーションログの取得と分析
ウ	仮想サーバのゲストOSに係るセキュリティの設定
エ	ハイパーバイザに係るセキュリティの設定

❑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

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フェース（例えばウェブメール）、またはプログラムインタフェー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。

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。

3つのモデルのうち唯一"OSに対するコントロール権"を持つIaaSが「OSに係るセキュリティの設定」を実施可能です。

ア "アプリケーションの利用者ID管理"

全てのモデルで実施可能です。

イ "アプリケーションログの取得と分析"

全てのモデルで実施可能です。

ウ "仮想サーバのゲストOSに係るセキュリティの設定"

正しい。IaaSのみが実施可能です。

エ "ハイパーバイザに係るセキュリティの設定"

ハイパーバイザはハードウェア上で稼働する1つ以上のバーチャルマシンを制御するプログラムで、事業者側が管理します。したがってハイパーバイザに係るセキュリティの設定は全てのサービスモデルで実施できません。

参考URL:NISTによるクラウドコンピューティングの定義(PDF)
http://www.ipa.go.jp/files/000025366.pdf

https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025366.pdf

☆☆☆

デジタルフォレンジックスでハッシュ値を利用する目的として，適切なものはどれか。

平成25年秋期　問43
73問目／選択範囲の問題数237問

ア　一方向性関数によってパスワードを変換して保存する。

イ　改変された証拠を復元する。

ウ　証拠と原本との同一性を証明する。

エ　パスワードの盗聴の有無を検証する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ウ　“あなたの解答：ア”

❑解説

デジタルフォレンジクスとは、不正アクセスや情報漏えいなどのセキュリティインシデントの発生時に、原因究明や法的証拠を明らかにするために対象となる電子的記録を収集・解析することです。

ハッシュ関数は、長い文章やデータを固定長のビット列に圧縮する一方向性の関数で、圧縮された値をハッシュ値と呼びます。この技術は、ハッシュ値にデジタル署名を付して、本人性と文書の真正性の証明に利用したり、証拠の保全・開示に広く利用されています。

ア “一方向性関数によってパスワードを変換して保存する。”

パスワードを平文ではなくハッシュ値に変換して保存するのは、盗聴や漏えいなどにより第三者に知られても解読できないようにするための対策です。

イ “改変された証拠を復元する。”

ハッシュ関数は一方向性なのでハッシュ値からもとのデータを復元することはできません。

ウ “証拠と原本との同一性を証明する。”

正しい。

エ “パスワードの盗聴の有無を検証する。”

ハッシュ値には盗聴の有無を検知する仕組みはありません。

☆

日本情報処理開発協会のプライバシーマーク制度について説明したものはどれか。

平成17年春期　問76
74問目／選択範囲の問題数237問

ア　OECDのプライバシーガイドラインに準拠している公的機関及び民間事業者を認定する制度

イ　個人情報を売買する事業者が一定の基準を満たしていること認定する制度

ウ　個人情報を保有している事業者に個人情報保護措置の概要を登録させる制度

エ　事業者が個人情報の取扱いを適切に行うための体制などを整備していることを認定する制度

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

エ　“あなたの解答：エ”

❑解説

プライバシーマーク制度は、企業や団体等(事業者)の事業活動における個人情報の取り扱いについて、資格を持った審査員が査定を行い、適切な管理体制であると評価された事業者にプライバシーマークの使用を認める制度で、平成10年4月より一般財団法人日本情報経済社会推進協会(JIPDEC)が運用しています。任意で実施している第三者認証制度で法的根拠はありませんが、個人情報保護体制のアピールや競合他社との差別化、消費者や取引先からの信頼獲得などのメリットがあり、取得する組織が増加しています。

図　プライバシーマーク見本

ア　“OECDのプライバシーガイドラインに準拠している公的機関及び民間事業者を認定する制度”

認定ではJIS Q 15001（個人情報保護マネジメントシステム要求事項）、及びJIPDECのプライバシーマーク付与適格性審査基準に適合しているかどうかが判断基準となります。OECDのプライバシーガイドラインは、経済協力開発機構により採択されたプライバシー保護と個人データの国際流通についてのガイドラインで、世界各国の個人情報保護に関する法律の基本原則となっています。

イ　“個人情報を売買する事業者が一定の基準を満たしていること認定する制度”

認定の対象は個人情報を適切に取り扱っている事業者です。

ウ　“個人情報を保有している事業者に個人情報保護措置の概要を登録させる制度”

個人情報保護措置の概要を登録させる制度ではありません。

エ　“事業者が個人情報の取扱いを適切に行うための体制などを整備していることを認定する制度”

正しい。プライバシーマーク制度の説明です。

☆☆☆

デジタル証明書が失効しているかどうかをオンラインで確認するためのプロトコルはどれか。

令和4年秋期　問38
75問目／選択範囲の問題数237問

ア	CHAP	イ	LDAP	ウ	OCSP	エ	SNMP

❑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

OCSP(Online Certificate Status Protocol)は、デジタル証明書の失効情報をオンライン確認し、デジタル証明書の有効性をリアルタイムで検証するプロトコルです。

クライアントは、確認対象となるデジタル証明書のシリアル番号をOCSPレスポンダに送信し、有効性検証の結果を受け取ります。この仕組みを利用することで、クライアント自身がCRLを取得・検証する手間を省くことができます。

ア “CHAP”

Challenge Handshake Authentication Protocolの略。チャレンジレスポンス方式を使用した安全性の高い認証方式で、PPP接続で利用されます。

イ “LDAP”

Lightweight Directory Access Protocolの略。ディレクトリサービス(LANなどのコンピュータネットワーク上にあるユーザー情報、接続されているプリンターなどの資源を記憶し、検索しやすいようにまとめたもの)に対するアクセスを提供するプロトコルです。

ウ “OCSP”

正しい。OCSPはデジタル証明書が失効しているかどうかをオンラインで確認するためのプロトコルです。

エ “SNMP”

Simple Network Management Protocolの略。TCP/IPネットワーク上でネットワーク上の機器の情報を収集して、監視や制御を行うためのプロトコルです。

☆☆☆

情報セキュリティにおけるサンドボックスの説明はどれか。

平成31年春期　問43
76問目／選択範囲の問題数237問

ア　OS，DBMS，アプリケーションソフトウェア，ネットワーク機器など多様なソフトウェアや機器が出力する大量のログデータを分析する。

イ　Webアプリケーションの入力フォームへの入力データに含まれるHTMLタグ，JavaScript，SQL文などを他の文字列に置き換えることによって，入力データ中に含まれる悪意のあるプログラムの実行を防ぐ。

ウ　Webサーバの前段に設置し，不特定多数のPCから特定のWebサーバへのリクエストに代理応答する。

エ　不正な動作の可能性があるプログラムを特別な領域で動作させることによって，他の領域に悪影響が及ぶのを防ぐ。

❑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

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AdobeFlash、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。最近では、仮想環境として構築したサンドボックスが、未確認ファイルや不審ファイルの動作確認に使えることから標的型攻撃への対策としても注目を集めています。サンドボックスとは「砂場」のことであり、子供を安全が確保された場所内だけで遊ばせるイメージからこう呼ばれています。

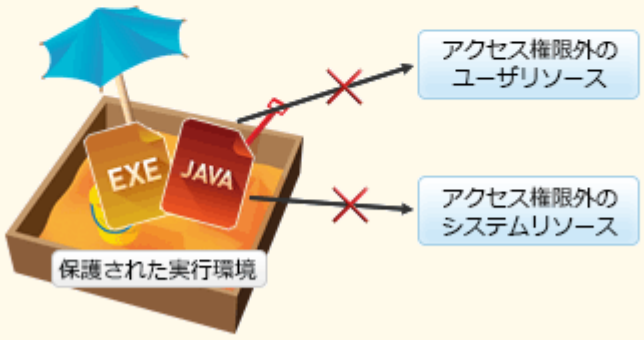


図　サンドボックス機構の概念

したがって適切な記述は「エ」です。

ア　“OS，DBMS，アプリケーションソフトウェア，ネットワーク機器など多様なソフトウェアや機器が出力する大量のログデータを分析する。”

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

イ　“Webアプリケーションの入力フォームへの入力データに含まれるHTMLタグ，JavaScript，SQL文などを他の文字列に置き換えることによって，入力データ中に含まれる悪意のあるプログラムの実行を防ぐ。”

サニタイジングやエスケープ処理の説明です。

ウ “Webサーバの前段に設置し，不特定多数のPCから特定のWebサーバへのリクエストに代理応答する。”

リバースプロキシの説明です。

エ “不正な動作の可能性があるプログラムを特別な領域で動作させることによって，他の領域に悪影響が及ぶのを防ぐ。”

正しい。サンドボックスの説明です。

☆☆

所有者と公開鍵の対応付けをするのに必要なポリシーや技術の集合によって実現される基盤はどれか。

平成24年春期　問36
77問目／選択範囲の問題数237問

ア	IPsec	イ	PKI
ウ	ゼロ知識証明	エ	ハイブリッド暗号

❑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

PKI(Public Key Infrastructure，公開鍵基盤)は、公開鍵と秘密鍵のペアが真の所有者のものであるかを第三者機関である**CA**(Certification Authority，認証局)が審査し、申請者の公開鍵に対して**デジタル証明書**を発行することで保証を実現するための仕組みです。デジタル証明書には審査済みの公開鍵が含まれ、CAのデジタル署名が付されています。公開鍵の利用者は認証局の公開鍵を用いてこのデジタル署名の正当性を検証することで公開鍵の正当性を確認することができます。

ア　“IPsec”

Security Architecture for IPの略。IP(Internet Protocol)を拡張してセキュリティを高めたプロトコルで、改ざんの検知，通信データの暗号化，送信元の認証などの機能をOSI基本参照モデルのネットワーク層レベル(TCP/IPモデルではインターネット層)で提供します。

イ　“PKI”

正しい。

ウ　“ゼロ知識証明”

ゼロ知識証明は、チャレンジレスポンス方式のように平文のパスワードを直接送信しなくても、論理的思考の積み立てによって相手の真正性を確認する作業のことです。(チャレンジレスポンス方式では、パスワードではなくチャレンジコードとレスポンスコードのやり取りによって認証を行います。)

エ　“ハイブリッド暗号”

ハイブリッド暗号は、公開暗号方式を用いて共通鍵を他方へ安全に配送し、以後はその共通鍵を使用して暗号化通信を行う方式です。SSLやS/MIMEで採用されています。

☆☆☆

次に示すような組織の業務環境において，特定のIPセグメントのIPアドレスを幹部のPCに動的に割り当て，一部のサーバへのアクセスをそのIPセグメントからだけ許可することによって，幹部のPCだけが当該サーバにアクセスできるようにしたい。利用するセキュリティ技術として，適切なものはどれか。

〔組織の業務環境〕

- 業務ではサーバにアクセスする。サーバは，組織の内部ネットワークからだけアクセスできる。
- 幹部及び一般従業員は同一フロアで業務を行っており，日によって席が異なるフリーアドレス制を取っている。
- 各席には有線LANポートが設置されており，PCを接続して組織の内部ネットワークに接続する。
- ネットワークスイッチ1台に全てのPCとサーバが接続される。

令和5年春期　問45
78問目／選択範囲の問題数237問

ア	IDS	イ	IPマスカレード
ウ	スタティックVLAN	エ	認証VLAN

❑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

認証VLANは、VLANの方式の1つで、ネットワークの接続前にMACアドレス認証、IDとパスワード認証、IEEE 802.1xなどでユーザーを特定し、ユーザーごとに所属すべきVLANに振り分けることで端末のグルーピングを行います。これにより接続ポート単位やアドレス単位というグルーピングができない場合でも、VLANに対応させることができます。

ア “IDS”

Intrusion Detection Systemの略。ネットワークやホストをリアルタイムで監視し、異常を検知した場合に管理者に通知するなどの処置を行う侵入検知システムです。

イ “IPマスカレード”

IPマスカレードは、プライベートIPアドレスとポート番号の組合せでクライアントを識別することで、1つのグローバルIPアドレスで複数の端末をインターネットに接続可能とする技術です。NAPTとも呼ばれます。

ウ “スタティックVLAN”

スタティックVLANは、スイッチの接続ポートに基づいてグルーピングする方法です。ポートベースVLANとも呼ばれます。設問ではフリーアドレス制が採用されていて、どの人がどのポートを利用するかが決まっていないため、ポートベースの割当てではセキュリティレベルを分けることはできません。

エ “認証VLAN”

正しい。フリーアドレス制や無線アクセスポイントなどのように、接続ポートでVLANを識別できない場合でも、認証VLANを利用することによりユーザーごとに適切なVLANを割り当てることができます。

☆

デジタル署名を利用する目的はどれか。

平成18年春期　問72
79問目／選択範囲の問題数237問

ア　受信者が署名用の鍵を使って暗号文を元の平文に戻すことができるようにする。

イ　送信者が署名用の鍵を使って作成した署名を平文に付加することによって，受信者が送信者を確認できるようにする。

ウ　送信者が署名用の鍵を使って平文を暗号化し，平文の内容を関係者以外に分からないようにする。

エ　送信者が定数を付加した平文を署名用の鍵を使って暗号化し，受信者が復号した定数を確認することによって，メッセージの改ざん部位を特定できるようにする。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：イ”

❑解説

デジタル署名は、公開鍵暗号方式を使って通信内容が改ざんされていないことを保証する技術で、受信者側で「発信者が正当であるか」と「改ざんの有無」の2点を確認できます。
デジタル署名の利用によって受信者が確認する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　“受信者が署名用の鍵を使って暗号文を元の平文に戻すことができるようにする。”

デジタル署名は平文を暗号化するものではありません。また受信者がメッセージダイジェストの復号に使用するのは送信者の公開鍵です。

イ　“送信者が署名用の鍵を使って作成した署名を平文に付加することによって，受信者が送信者を確認できるようにする。”

正しい。

ウ　“送信者が署名用の鍵を使って平文を暗号化し，平文の内容を関係者以外に分からないようにする。”

デジタル署名は平文を暗号化するものではありません。

エ　“送信者が定数を付加した平文を署名用の鍵を使って暗号化し，受信者が復号した定数を確認することによって，メッセージの改ざん部位を特定できるようにする。”

平文に付加するメッセージダイジェストは平文をハッシュ化したものを署名用の秘密鍵で暗号化したものです。

☆

盗まれたクレジットカードの不正利用を防ぐ仕組みのうち，オンラインショッピングサイトでの不正利用の防止に有効なものはどれか。

令和3年秋期　問42
80問目／選択範囲の問題数237問

ア　3Dセキュアによって本人確認する。

イ　クレジットカード内に保持されたPINとの照合によって本人確認する。

ウ　クレジットカードの有効期限を確認する。

エ　セキュリティコードの入力によって券面認証する。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

ア　“あなたの解答：ア”

❑解説

ア “3Dセキュアによって本人確認する。”

正しい。3Dセキュアは、オンライン決済時に本人のみが知る情報（パスワードや属性情報等）を入力させることで、利用者本人が取引を行っていることを確認する仕組みです。カードを盗まれたとしても、パスワードは本人しか知らないのでオンラインでの不正利用を防止できます。

イ “クレジットカード内に保持されたPINとの照合によって本人確認する。”

PIN（暗証番号）は、オフライン決済時にIC対応カードを決済端末に挿入し、ICチップからカード情報を読み込んで照合する方法です。ICチップ内の情報を読み出すことが前提となっているため、オンライン決済の認証には使えません。

ウ “クレジットカードの有効期限を確認する。”

有効期限はカード券面に記載されているため、盗まれたカードの不正利用対策にはなりません。

エ “セキュリティコードの入力によって券面認証する。”

セキュリティコードは、カード券面の「セキュリティコード（数字3～4桁）」を入力し、カードが真正であることを確認する方法です。セキュリティコードはカード券面に記載されているため、盗まれたカードの不正利用対策にはなりません。

☆☆☆

スパイウェアによって引き起こされた情報の漏えいに該当するものはどれか。

平成17年春期　問72
81問目／選択範囲の問題数237問

ア　暗号化せずに電子メールを送信したところ，ネットワーク上で内容が読み取られてしまった。

イ　インターネットに接続したところ，パソコン内の利用者情報が知らないうちに送信されてしまった。

ウ　パスワードを忘れてしまったという電話に対して，システム管理者が教えたのでパスワードが他人に知られてしまった。

エ　パソコンをそのまま破棄したところ，磁気媒体上に残存していたデータが読み取られてしまった。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

イ　“あなたの解答：ア”

❑解説

スパイウェア(Spyware)は、利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴及びキーストロークなどの情報を秘密裏に収集し、勝手に外部の組織や個人に送信する不正プログラムです。
ユーザーに気付かれずに情報を収集することが目的であるため、ウイルスの特徴であるシステムの改ざんやファイルの破壊などの目立つ活動は行わないことが多く、インストールされていることをユーザーが気付きにくいようになっています。

ア “暗号化せずに電子メールを送信したところ，ネットワーク上で内容が読み取られてしまった。”

盗聴(スニッフィング)による被害です。

イ “インターネットに接続したところ，パソコン内の利用者情報が知らないうちに送信されてしまった。”

正しい。スパイウェアによる被害です。

ウ “パスワードを忘れてしまったという電話に対して，システム管理者が教えたのでパスワードが他人に知られてしまった。”

ソーシャルエンジニアリングによる被害です。

エ “パソコンをそのまま破棄したところ，磁気媒体上に残存していたデータが読み取られてしまった。”

スキャビンジング行為による被害です。

☆

OSI基本参照モデルのネットワーク層で動作し，"認証ヘッダー(AH)"と"暗号ペイロード(ESP)"の二つのプロトコルを含むものはどれか。

令和3年秋期　問43
82問目／選択範囲の問題数237問

ア	IPsec	イ	S/MIME	ウ	SSH	エ	XML暗号

❑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

IPsec(IP Security)は、IP(Internet Protocol)を拡張してセキュリティを高めたプロトコルで、改ざんの検知、通信データの暗号化、送信元の認証などの機能をOSI基本参照モデルのネットワーク層レベル(TCP/IPモデルではIP層)で提供します。IPsecを用いれば上層のアプリケーションに依存せずに暗号化通信を行えるため、VPNの構築に利用されます。
IPsecはプロトコル群の総称であり、認証、暗号化、鍵交換などの複数のプロトコルを含みます。そのうち、認証を担うプロトコルが**AH**(Authentication Header)、認証と暗号化を担うプロトコルが**ESP**(Encapsulated Security Payload)です。

どの規格もデータの暗号化を担いますが、ネットワーク層で動作するのはIPsecだけです。したがって「ア」が正解です。

ア　“IPsec”

正しい。

イ　“S/MIME”

Secure MIMEの略。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規格です。

ウ　“SSH”

Secure Shellの略。公開鍵暗号や認証の技術を利用してリモートコンピュータと安全に通信するためのアプリケーション層のプロトコルです。

エ　“XML暗号”

XML暗号は、XML文書の一部分を暗号化するための規格です。

☆☆☆

スパムメール対策として，サブミッションポート(ポート番号587)を導入する目的はどれか。

令和5年春期　問44
83問目／選択範囲の問題数237問

ア　DNSサーバにSPFレコードを問い合わせる。

イ　DNSサーバに登録されている公開鍵を使用して，デジタル署名を検証する。

ウ　POP before SMTPを使用して，メール送信者を認証する。

エ　SMTP-AUTHを使用して，メール送信者を認証する。

❑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：ウ”

❑解説

スパムメールは、追跡やブロックのリスクを避けるために、自身のISPのメールサーバを介さずに直接外部のメールサーバとコネクションを確立して、送信されることが普通です。このようなスパムメールの送信をブロックするため、ISPでは、ISP外部のメールサーバと直接コネクションを確立しようとする外向きの通信をブロックする**OP25B**（Outbound Port 25 Blocking）という対策を行っています。OP25Bが実施されていると、たとえ正当な利用者であっても、通常の"25/TCP"のSMTP通信を使って外部のメールサーバと直接コネクションを確立することができなくなります。これにより、外出先で自分が契約しているISPのメールサーバから送信できないなどの問題が生じます。

サブミッションポートは、SMTPを拡張したプロトコルであり、利用者のメールソフト(メーラー)からメールサーバに対して、メールの送信を依頼するときに使用する**送信専用のポート番号**です。通常のメール送信に使われるSMTP(25/TCP)と異なり、**SMTP-AUTH**による送信者認証が用意されているため、メールサーバは認証を受けた利用者からのメールのみを送信することが可能となります。これによりスパマーの悪用を防ぎつつ、外部のメールサーバを使用したメール送信を可能にしています。

したがって、サブミッションポートの導入目的は「SMTP-AUTHによる送信者認証」が適切です。

☆☆

サイバーキルチェーンの偵察段階に関する記述として，適切なものはどれか。

令和4年春期　問37
84問目／選択範囲の問題数237問

ア　攻撃対象企業の公開Webサイトの脆弱性を悪用してネットワークに侵入を試みる。

イ　攻撃対象企業の社員に標的型攻撃メールを送ってPCをマルウェアに感染させ，PC内の個人情報を入手する。

ウ　攻撃対象企業の社員のSNS上の経歴，肩書などを足がかりに，関連する組織や人物の情報を洗い出す。

エ　サイバーキルチェーンの2番目の段階をいい，攻撃対象に特化したPDFやドキュメントファイルにマルウェアを仕込む。

❑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

サイバーキルチェーンは、サイバー攻撃の手順を攻撃者の視点からいくつかの段階に分けモデル化したものです。攻撃の段階としては、偵察、武器化、配送、攻撃、インストール、遠隔操作、目的達成という7段階が一般的です。攻撃者の視点からサイバー攻撃を見ることで、各段階における防御策の立案に役立てることができます。多層防御を施すことでサイバーキルチェーンを断ち切ることが重要です。

偵察

標的に関する情報を収集して調査する

武器化

攻撃のためのマルウェアを用意する

配送

メールやWebサイトを使って標的にマルウェアを送信／配信する、または標的のシステムに侵入する

攻撃

標的がマルウェアを実行する

インストール

標的がマルウェアに感染する

遠隔操作

マルウェアを介して標的のサーバを操作可能になる

目的達成

秘密情報を得る、サービス停止、改ざんなど攻撃者の目的を達成する

ア “攻撃対象企業の公開Webサイトの脆弱性を悪用してネットワークに侵入を試みる。”

配送段階に関する記述です。

イ “攻撃対象企業の社員に標的型攻撃メールを送ってPCをマルウェアに感染させ，PC内の個人情報を入手する。”

配送～目的達成段階に関する記述です。

ウ “攻撃対象企業の社員のSNS上の経歴，肩書などを足がかりに，関連する組織や人物の情報を洗い出す。”

正しい。偵察段階に関する記述です。

エ “サイバーキルチェーンの2番目の段階をいい，攻撃対象に特化したPDFやドキュメントファイルにマルウェアを仕込む。”

武器化段階に関する記述です。

☆☆☆

完全一致によるパターンマッチング方式のウイルス対策ソフトは，ウイルス単体の特徴あるコード列を照合に用いる。そのコード列の長さと検出の関係はどれか。

平成20年春期　問74
85問目／選択範囲の問題数237問

ア　コード列が長いほど，ウイルスの亜種を検出する可能性も高くなる。

イ　コード列が長いほど，未知のウイルスを検出する可能性が高い。

ウ　コード列が短いほど，ウイルス名を正しく特定する可能性が高い。

エ　コード列が短いほど，正常なプログラムを誤検出する可能性が高くなる。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ対策

❑正解

エ　“あなたの解答：イ”

❑解説

パターンマッチング方式は、コンピュータウイルスやワームを検出するための代表的な方式で、そのウイルスが持つ特徴的なコードをパターン(シグネチャコード|ウィルス定義ファイル)として検査対象のファイルと比較することでウイルスの検出を試みます。検出できるウイルスはパターンファイルに定義されているものに限るので、定義されていないものや次々と亜種が作られるもの、未知のウイルスなどを検出することは困難です。

パターンのコード列が短いとそのウィルスの亜種を検出できる可能性が高くなりますが誤報が多く、コード列が長いと誤報は少なくなりますが、亜種や未知のウィルスを検出することは難しくなります。

☆☆☆

OCSPクライアントとOCSPレスポンダとの通信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38
86問目／選択範囲の問題数237問

ア　デジタル証明書全体をOCSPレスポンダに送信し，その応答でデジタル証明書の有効性を確認する。

イ　デジタル証明書全体をOCSPレスポンダに送信し，その応答としてタイムスタンプトークンの発行を受ける。

ウ　デジタル証明書のシリアル番号，証明書発行者の識別名(DN)のハッシュ値などをOCSPレスポンダに送信し，その応答でデジタル証明書の有効性を確認する。

エ　デジタル証明書のシリアル番号，証明書発行者の識別名(DN)のハッシュ値などをOCSPレスポンダに送信し，その応答としてタイムスタンプトークンの発行を受ける。

❑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

OCSP(Online Certificate Status Protocol)は、リアルタイムでデジタル証明書の失効情報を検証し、有効性を確認するプロトコルです。OCSPクライアントは、確認対象となるデジタル証明書の**シリアル番号**等をOCSPレスポンダに送信し、**有効性検証の結果**を受け取ります。この仕組みを利用することで、クライアント自身がCRL(証明書失効リスト)を取得・検証する手間を省くことができます。

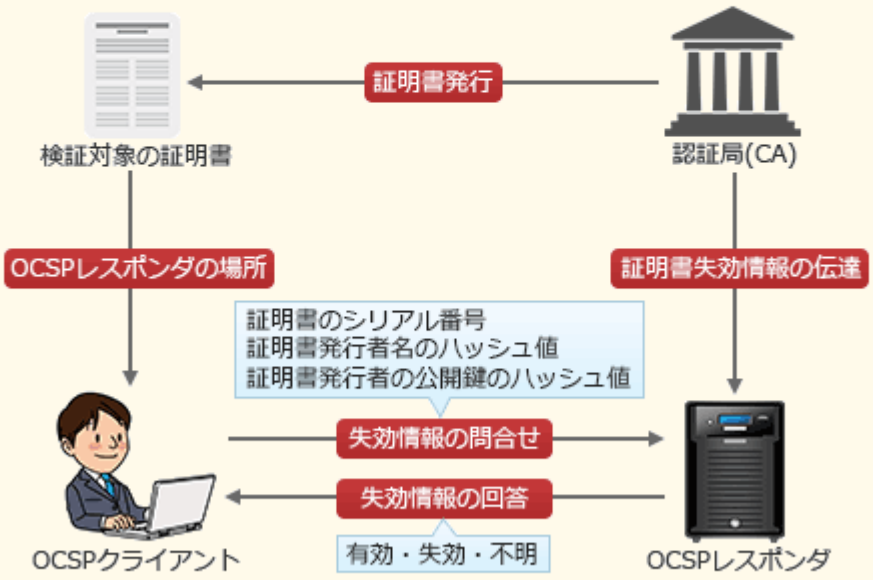


図　OCSPの概要

したがって適切な説明は「ウ」です。

☆☆
※常識的に考えたら解ける？

情報システムのリスク分析における作業①～⑤の，適切な順序はどれか。

① 損失の分類と影響度の評価

② 対策の検討・評価と優先順位の決定

③ 事故態様の関連分析と損失額予想

④ 脆弱性の発見と識別

⑤ 分析対象の理解と分析計画

平成19年春期　問77
87問目／選択範囲の問題数237問

ア	④→⑤→②→③→①	イ	④→⑤→③→②→①
ウ	⑤→④→②→③→①	エ	⑤→④→③→①→②

❑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

選択肢をみると1，2番目が④と⑤のどちらかになる事がわかります。常識的に考えて⑤「(リスク)分析計画」後に④「脆弱性の発見」が来るのが適当と考えられるので1，2番目は⑤→④になります。
続く3番目の作業ですが選択肢から②と③のどちらかが当てはまることがわかります。②「優先順位の決定」は、③「損失額予想」の結果を考慮して決まるので3番目の作業は③が適切です。
最後の4，5番目の作業には残された①と②のどちらかが当てはまります。②「優先順位の決定」は、先程と同様に①「損失の分類と影響度の評価」の結果を考慮して決まるので①→②の順序が適切です。

これらをまとめると適切な作業順序は「⑤→④→③→①→②」となります。

☆☆☆

ソフトウェアの既知の脆弱性を一意に識別するために用いる情報はどれか。

令和5年春期　問40
88問目／選択範囲の問題数237問

ア　CCE(Common Configuration Enumeration)

イ　CVE(Common Vulnerabilities and Exposures)

ウ　CVSS(Common Vulnerability Scoring System)

エ　CWE(Common Weakness Enumeration)

❑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：エ”

❑解説

CVE(共通脆弱性識別子)は、一般に知られている個々の脆弱性ごとに採番された識別子です。世界各国の製品開発企業、セキュリティ関連企業、脆弱性検査ツールや脆弱性対策情報提供サービスにおいて、脆弱性を識別するために使用されています。採番の形式は CVE-[西暦年号]-[4桁以上の数字] です。

ア “CCE(Common Configuration Enumeration)”

CCE(共通セキュリティ設定)は、コンピュータのセキュリティ設定項目ごとに付けられた識別子です。

イ “CVE(Common Vulnerabilities and Exposures)”

正しい。CVEは、脆弱性ごとに付けられている識別子です。

ウ “CVSS(Common Vulnerability Scoring System)”

CVSS(共通脆弱性評価システム)は、情報システムの脆弱性の深刻度を同一の基準のもとで定量的に評価する共通的な手法です。

エ “CWE(Common Weakness Enumeration)”

CWE(共通脆弱性タイプ)は、ソフトウェアの脆弱性の種類を識別するための共通基準です。

☆

暗号方式のうち，共通鍵暗号方式はどれか。

平成28年春期　問37
89問目／選択範囲の問題数237問

ア	AES	イ	ElGamal暗号	ウ	RSA	エ	楕円曲線暗号

❑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

AES(Advanced Encryption Standard)は、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。アメリカの旧国家暗号規格であったDES(Data Encryption Standard)の鍵長が56ビットであったのに対して最大256ビットの鍵長を利用することが可能で強度が高くなっています。
日本でも「電子政府推奨暗号リスト」に掲載されているほか、無線LANの暗号化規格WPA2の暗号化方式としても採用されています。

ア “AES”

正しい。

イ “ElGamal暗号”

ElGamal暗号は、非常に大きな数の離散対数問題を解くことが困難であることを利用した公開鍵暗号方式です。共通鍵を安全に共有する方法であるDiffie-Hellman法の技術を暗号化方式に応用したものです。

ウ “RSA”

RSAは、けた数の大きな数の素因数分解に膨大な時間がかかることを利用した公開鍵暗号方式です。

エ “楕円曲線暗号”

楕円曲線暗号は、楕円曲線上の離散対数問題を解くことが困難であることを利用した公開鍵暗号方式です。

☆☆☆☆

JPCERTコーディネーションセンター"CSIRTガイド(2021年11月30日)" では，CSIRTを機能とサービス対象によって六つに分類しており，その一つにコーディネーションセンターがある。コーディネーションセンターの機能とサービス対象の組合せとして，適切なものはどれか。

令和5年秋期　問39
90問目／選択範囲の問題数237問

	機能	サービス対象
ア	インシデント対応の中で，CSIRT 間の情報連携，調整を行う。	他の CSIRT
イ	インシデントの傾向分析やマルウェアの解析，攻撃の痕跡の分析を行い，必要に応じて注意を喚起する。	関係組織，国又は地域
ウ	自社製品の脆弱性に対応し，パッチ作成や注意喚起を行う。	自社製品の利用者
エ	組織内 CSIRT の機能の一部又は全部をサービスプロバイダとして，有償で請け負う。	顧客

ア　イ　ウ　エ

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ管理

❑正解

ア　“あなたの解答：ウ”

❑解説

一般的にCSIRTといえば「組織内CSIRT」を指すことが多いのですが、広義のCSIRTは活動範囲の違いによって以下の6種類に分類されます。

組織内CSIRT

組織内のセキュリティインシデントに対応する

国際連携CSIRT

国を代表する形でインシデント対応のための連絡窓口として活動する

コーディネーションセンター

協力関係にある他のCSIRTとの情報連携や調整を行う

分析センター

インシデントの傾向分析、マルウェア解析、痕跡分析、注意喚起などを行う

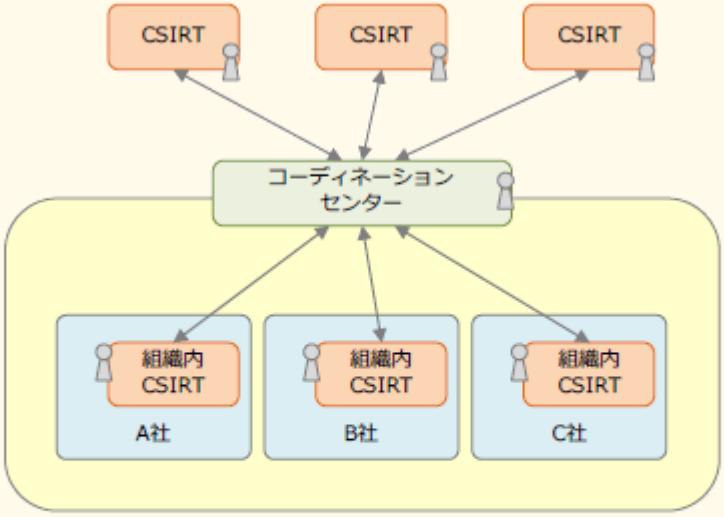
ベンダーチーム

自社製品の脆弱性に対応し、パッチを作成したり注意喚起をしたりする

インシデントレスポンスプロバイダ

セキュリティベンダーやSoCなどの、CSIRT機能の一部を顧客から有償で請け負う事業者

CSIRTガイドではコーディネーションセンターについて「サービス対象は協力関係にある**他のCSIRT**。インシデント対応においてCSIRT間の情報連携、調整を行なう。グループ企業間の連携を担当する」と説明しています。



[図 1.2-3 コーディネーションセンターのサービスモデル]

「CSIRTガイド」より引用
https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf

したがって、サービス対象が「他のCSIRT」である「ア」が適切です。

ア 正しい。コーディネーションセンターに該当します。

イ 分析センターに該当します。

ウ ベンダーチームに該当します。

エ インシデントレスポンスプロバイダに該当します。

☆

セキュリティ関連のプロトコルに関する記述のうち，適切なものはどれか。

平成19年春期　問56
91問目／選択範囲の問題数237問

ア　IPsecは，PPPの認証用のプロトコルの一つである。

イ　PAPは，LAN間接続やダイヤルアップ接続を行う際のユーザー認証に，暗号を使用したプロトコルである。

ウ　PPPは，暗号技術を導入してセキュリティを強化した電子メールシステムのプロトコルである。

エ　SSLは，Webサーバとブラウザとの間でデータを暗号化して転送する場合に使用することができるプロトコルである。

❑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

ア “IPsecは，PPPの認証用のプロトコルの一つである。”

IPsecは、IP(Internet Protocol)を拡張してセキュリティを高め、改ざんの検知，通信データの暗号化，送信元の認証などの機能をOSI基本参照モデルのネットワーク層レベル(TCP/IPモデルではインターネット層)で提供するプロトコルです。

イ “PAPは，LAN間接続やダイヤルアップ接続を行う際のユーザー認証に，暗号を使用したプロトコルである。”

PAP(Password Authentication Protocol)は、CHAP(Challenge Handshake Authentication Protocol)とともにPPPの認証で使用されるプロトコルです。

ウ “PPPは，暗号技術を導入してセキュリティを強化した電子メールシステムのプロトコルである。”

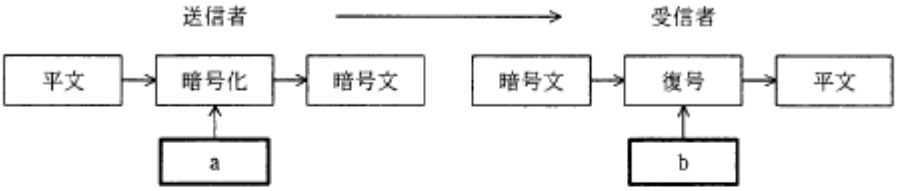
PPP(Point-to-Point Protocol)は、電話回線を通じてコンピュータをネットワークに接続するダイヤルアップ接続でよく使われる、2点間を接続してデータ通信を行うための通信プロトコルです。

エ “SSLは，Webサーバとブラウザとの間でデータを暗号化して転送する場合に使用することができるプロトコルである。”

正しい。SSL(Secure Sockets Layer)は、主にWebブラウザとWebサーバ間でデータを安全にやり取りするための業界標準プロトコルとして使用されてます。

☆

図は公開かぎ暗号方式による機密情報の送受信の概念図である。a，bに入れるかぎの適切な組合せはどれか。



平成17年秋期　問71
92問目／選択範囲の問題数237問

	a	b
ア	受信者の公開かぎ	受信者の秘密かぎ
イ	受信者の秘密かぎ	受信者の公開かぎ
ウ	送信者の公開かぎ	受信者の秘密かぎ
エ	送信者の秘密かぎ	受信者の公開かぎ

ア　イ　ウ　エ

❑分類

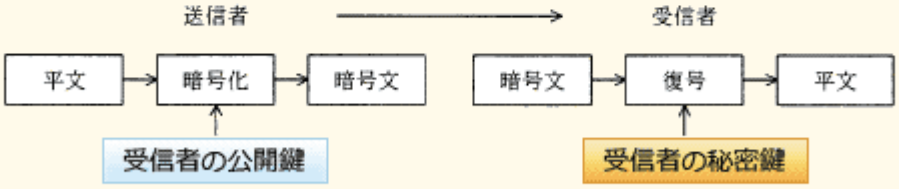
テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：ア”

❑解説

公開鍵暗号方式で暗号化通信を行う場合には、送信者が**受信者の公開かぎ**で平文を暗号化し、受信者が**受信者の秘密かぎ**で復号する手順になります。



a ＝受信者の公開かぎ、 b ＝受信者の秘密かぎ になるため「ア」の組合せが適切です。

☆☆

ソーシャルエンジニアリング手法を利用した標的型攻撃メールの特徴はどれか。

平成25年春期　問40
93問目／選択範囲の問題数237問

ア　件名に"未承諾広告※"と記述されている。

イ　件名や本文に，受信者の業務に関係がありそうな内容が記述されている。

ウ　支払う必要がない料金を振り込ませるために，債権回収会社などを装い無差別に送信される。

エ　偽のホームページにアクセスさせるために，金融機関などを装い無差別に送信される。

❑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

標的型攻撃メールは、差出人を取引先企業や官公庁や知人など信頼性のある人に偽装し、さらに、受信者の興味を引く件名や本文を使用することによって、ウイルスを仕込んだ添付ファイルを開かせたり、ウイルスに感染させるWebサイトのリンクをクリックさせるように巧妙に誘導する攻撃手法です。
この攻撃は、**メールの件名・本文にあたかもその企業・組織の業務に関係があるような内容を記述し受信者を錯覚させる**という人間の心理的な隙をつくソーシャルエンジニアリングの要素をもっています。

以前からあったような不特定多数のメールアドレスに対して無差別に送信されるものとは異なり、特定の企業･組織を狙い打ちする目的をもったメール攻撃であるため「標的型」攻撃メールと呼ばれます。

ア　“件名に"未承諾広告※"と記述されている。”

スパムメールの特徴です。

イ　“件名や本文に，受信者の業務に関係がありそうな内容が記述されている。”

正しい。標的型攻撃メールの特徴です。

ウ　“支払う必要がない料金を振り込ませるために，債権回収会社などを装い無差別に送信される。”

架空請求詐欺メールの特徴です。

エ　“偽のホームページにアクセスさせるために，金融機関などを装い無差別に送信される。”

フィッシング詐欺メールの特徴です。

☆☆☆

コンピュータ犯罪の手口の一つであるサラミ法はどれか。

平成18年春期　問77
94問目／選択範囲の問題数237問

ア　回線の一部に秘密にアクセスして他人のパスワードやIDを盗み出してデータを盗用する方法である。

イ　ネットワークを介して送受信されている音声やデータを不正に傍受する方法である。

ウ　不正行為が表面化しない程度に，多数の資産から少しずつ詐取する方法である。

エ　プログラム実行後のコンピュータ内部又はその周囲に残っている情報をひそかに探索して，必要情報を入手する方法である。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ウ　“あなたの解答：ウ”

❑解説

サラミ法は、銀行口座などの多数の資産から、不正行為が表面化しない程度に少しずつ搾取する行為です。

ア “回線の一部に秘密にアクセスして他人のパスワードやIDを盗み出してデータを盗用する方法である。”

不正アクセスやなりすましの説明です。

イ “ネットワークを介して送受信されている音声やデータを不正に傍受する方法である。”

盗聴の説明です。

ウ “不正行為が表面化しない程度に，多数の資産から少しずつ詐取する方法である。”

正しい。サラミ法の説明です。

エ “プログラム実行後のコンピュータ内部又はその周囲に残っている情報をひそかに探索して，必要情報を入手する方法である。”

スキャビンジング(ゴミ箱あさり)の説明です。

☆☆☆

基本評価基準，現状評価基準，環境評価基準の三つの基準で情報システムの脆弱性の深刻度を評価するものはどれか。

令和3年秋期　問41
95問目／選択範囲の問題数237問

ア	CVSS	イ	ISMS	ウ	PCI DSS	エ	PMS

❑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

ア　“あなたの解答：ア”

❑解説

CVSS(Common Vulnerability Scoring System，共通脆弱性評価システム)は、情報システムの脆弱性に対する汎用的な評価手法で、これを用いることで脆弱性の深刻度を同一の基準のもとで定量的に比較することが可能です。

CVSSでは次の3つの基準ごとに0.0から10.0までのスコアを付け、脆弱性を評価します。

基本評価基準 (Base Metrics)

脆弱性自体の深刻度を評価する指標。機密性、可用性、完全性への影響の大きさや、攻撃に必要な条件などの項目から算出され、時間の経過や利用者の環境で変化しない。

現状評価基準 (Temporal Metrics)

脆弱性の現在の深刻度を評価する基準。攻撃を受ける可能性、利用可能な対応策のレベルなどの項目から算出され、時間の経過により変化する。

環境評価基準 (Environmental Metrics)

製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する基準。二次被害の可能性や影響を受ける範囲などの項目から算出され、製品利用者ごとに変化する。

深刻度	スコア
緊急	9.0～10.0
重要	7.0～8.9
警告	4.0～6.9
注意	0.1～3.9
なし	0

図　CVSS v3によるスコアと深刻度レベル

ア "CVSS"

正しい。

イ "ISMS"

Information Security Management Systemの略。情報セキュリティマネジメントシステムの整備・管理・運用に関する仕組みでJIS Q 27001 (ISO/IEC 27001)の基となっています。

ウ "PCI DSS"

Payment Card Industry(PCI)データセキュリティ基準(DSS)は、カード会員のデータセキュリティを強化し、均一なデータセキュリティ評価基準の採用をグローバルに推進するためにクレジットカードの国際ブランド大手5社共同(VISA，MasterCard，JCB，AmericanExpress，Diners Club)により策定された基準です。

エ "PMS"

Personal information protection Management Systemの略。個人情報保護マネジメントシステムの整備・管理・運用に関する仕組みです。

参考URL：　共通脆弱性評価システムCVSS概説
http://www.ipa.go.jp/security/vuln/CVSS.html

https://www.ipa.go.jp/security/vuln/scap/cvss.html

☆

楕円曲線暗号の特徴はどれか。

令和5年秋期　問37
96問目／選択範囲の問題数237問

ア	RSA暗号と比べて，短い鍵長で同レベルの安全性が実現できる。
イ	共通鍵暗号方式であり，暗号化や復号の処理を高速に行うことができる。
ウ	総当たりによる解読が不可能なことが，数学的に証明されている。
エ	データを秘匿する目的で用いる場合，復号鍵を秘密にしておく必要がない。

❑分類

テクノロジ系 » セキュリティ » 情報セキュリティ

❑正解

ア　“あなたの解答：イ”

❑解説

楕円曲線暗号(ECC：Elliptic Curve Cryptography)は、楕円曲線上の点の演算を用いた公開鍵暗号方式です。1985年に発明されました。楕円曲線によって定義された有限可換群上の離散対数問題を解く際の計算量の多さを安全性の根拠とし、同じ強度を想定した場合、RSAより鍵長を短くできる利点があります。ビットコインで採用されている暗号方式として有名です。

2023年現在、RSAの鍵長は2,048ビット以上を使用することが推奨されています。公開鍵暗号方式は暗号化・復号に要する計算量が多いため、RSAの鍵長は処理負荷の面でネックとなっています。代わりに、鍵長が少なくて済む楕円曲線暗号へのニーズが高まってきています。特に組込みシステムやIoTデバイスなどの資源に制約のある環境では有効な選択肢となります。

ア “RSA暗号と比べて，短い鍵長で同レベルの安全性が実現できる。”

正しい。楕円曲線暗号の特徴です。RSAの鍵長2,048ビットで実現できる暗号強度を、楕円曲線暗号では鍵長224ビットで実現できます。

イ “共通鍵暗号方式であり，暗号化や復号の処理を高速に行うことができる。”

楕円曲線暗号は公開鍵暗号方式です。

イ “共通鍵暗号方式であり，暗号化や復号の処理を高速に行うことができる。”

楕円曲線暗号は公開鍵暗号方式です。

ウ “総当たりによる解読が不可能なことが，数学的に証明されている。”

不可能なわけではありません。現実的に有効な時間での解読が難しいことを安全性の根拠にしています。

エ “データを秘匿する目的で用いる場合，復号鍵を秘密にしておく必要がない。”

他の公開鍵暗号方式と同様に、暗号化通信で用いる場合には、暗号化鍵を公開し、復号鍵を秘密にします。

☆☆

問題を引き起こす可能性があるデータを大量に入力し，そのときの応答や挙動を監視することによって，ソフトウェアの脆弱性を検出するテスト手法はどれか。

令和5年秋期　問46
97問目／選択範囲の問題数237問

ア　限界値分析　　イ　実験計画法　　ウ　ファジング　　エ　ロードテスト

❑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

ウ　“あなたの解答：ウ”

❑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。

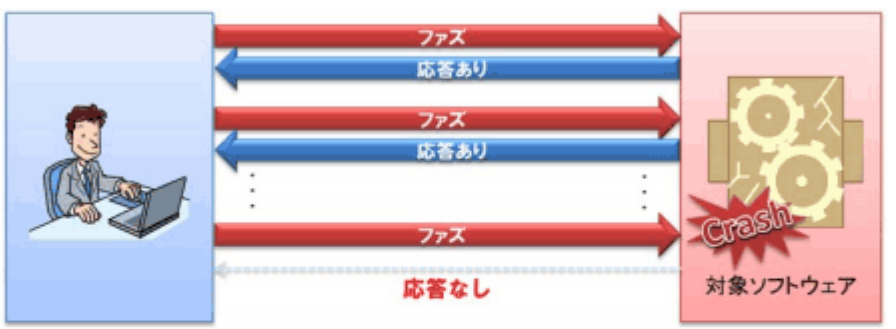


図 2.1-1 ファジングによる脆弱性検出イメージ

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。

したがって「ウ」が正解です。

ア “限界値分析”

限界値分析は、一般的に問題が発生する可能性の高い限界値や境界値を入力して、問題が発生しないかどうかを検証する手法です。

イ “実験計画法”

実験計画法は、確認すべき複数の要因をうまく組み合わせることによって、なるべく少ない実験回数で効率的に検証する手法です。

ウ “ファジング”

正しい。ファジングは、様々な不正確なデータを入力として送り、ソフトウェアが意図しない動作をしないかどうか検証する手法です。

エ “ロードテスト”

ロードテストは、通常想定される運用条件下の高負荷をかけた状態でソフトウェアを動作させ、問題が発生しないかどうかを検証する手法です。

☆☆

ウイルス検知手法の一つであるビヘイビア法を説明したものはどれか。

平成24年秋期　問42
98問目／選択範囲の問題数237問

ア　ウイルスの特徴的なコード列が検査対象プログラム内に存在するかどうかを調べて，もし存在していればウイルスとして検知する。

イ　各ファイルに，チェックサム値などウイルスではないことを保証する情報を付加しておき，もし保証する情報が検査対象ファイルに付加されていないか無効ならば，ウイルスとして検知する。

ウ　検査対象ファイルのハッシュ値と，安全な場所に保管してあるその対象の原本のハッシュ値を比較して，もし異なっていればウイルスとして検知する。

エ　検査対象プログラムを動作させてその挙動を監視し，もしウイルスによく見られる行動を起こせばウイルスとして検知する。

❑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

エ　“あなたの解答：エ”

❑解説

ビヘイビア法は、ウイルスの実際の感染・発病動作を監視して検出する手法です。

感染・発病動作として「書込み動作」「複製動作」「破壊動作」等の動作そのものの異常を検知する場合だけでなく、感染・発病動作によって起こる環境の様々な変化を検知することによる場合もこの手法に分類されます。例えば、「例外ポート通信・不完パケット・通信量の異常増加・エラー量の異常増加」「送信時データと受信時データの量的変化・質的変化」等がそれにあたります。

この他にもウィルス検出技術には次のようなものがあります。

コンペア法

ウイルスの感染が疑わしい対象(検査対象)と安全な場所に保管してあるその対象の原本を比較し、異なっていれば感染を検出する手法。

パターンマッチング法

「パターンデータ」「ウイルスパターン」「パターンファイル」「ウイルス定義ファイル」等を用いて、何らかの特徴的なコードをパターンとしてウイルス検査対象と比較することで検出する手法。

チェックサム法/インテグリティチェック法

検査対象に対して別途ウイルスではないことを保証する「チェックサム」「デジタル署名」等の情報を付加し、保証がないか無効であることで検出する手法。

ヒューリスティック法

ウイルスのとるであろう動作を事前に登録しておき、検査対象コードに含まれる一連の動作と比較して検出する手法。

問題文のそれぞれの記述とウィルス検出技術を合わせると次のようになります。

ア “ウイルスの特徴的なコード列が検査対象プログラム内に存在するかどうかを調べて，もし存在していればウイルスとして検知する。”

パターンマッチング法の説明です。

イ “各ファイルに，チェックサム値などウイルスではないことを保証する情報を付加しておき，もし保証する情報が検査対象ファイルに付加されていないか無効ならば，ウイルスとして検知する。”

チェックサム法の説明です。

ウ “検査対象ファイルのハッシュ値と，安全な場所に保管してあるその対象の原本のハッシュ値を比較して，もし異なっていればウイルスとして検知する。”

コンペア法の説明です。

エ “検査対象プログラムを動作させてその挙動を監視し，もしウイルスによく見られる行動を起こせばウイルスとして検知する。”

正しい。ビヘイビア法の説明です。

☆☆

組織的なインシデント対応体制の構築や運用を支援する目的でJPCERTコーディネーションセンターが作成したものはどれか。

令和4年秋期　問39
99問目／選択範囲の問題数237問

ア　CSIRTマテリアル

イ　ISMSユーザーズガイド

ウ　証拠保全ガイドライン

エ　組織における内部不正防止ガイドライン

❑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

CSIRTマテリアルは、組織的なインシデント対応体制である「組織内CSIRT」の構築を支援する目的で作成されたガイドラインです。構想フェーズ、構築フェーズ、運用フェーズの3部構成になっていて、ITセキュリティに対応するための情報およびノウハウが提示されています。CSIRTマテリアルはJPCERT/CCのWebサイトで閲覧可能です。

ア “CSIRTマテリアル”

正しい。CSIRTマテリアルは、組織内CSIRT(インシデント対応チーム)の構築を支援する目的でJPCERT/CCが作成したガイドラインです。

イ “ISMSユーザーズガイド”

ISMSユーザーズガイドは、ISMS認証基準の要求事項について一定の範囲でその意味するところを説明しているガイドです。JIPDECによって作成されています。

ウ “証拠保全ガイドライン”

証拠保全ガイドラインは、電磁的証拠の保全手続きの参考として、様々な事案について広く利用できるように策定された指針です。デジタル・フォレンジック研究会によって作成されています。

エ “組織における内部不正防止ガイドライン”

組織における内部不正防止ガイドラインは、組織が管理する情報と情報システムに対する内部不正の防止、および不正行為発生時の早期発見と拡大防止のための体制の整備を推進するための指針です。IPAによって作成されています。

☆

取引履歴などのデータとハッシュ値の組みを順次つなげて記録した分散型台帳を，ネットワーク上の多数のコンピュータで同期して保有し，管理することによって，一部の台帳で取引データが改ざんされても，取引データの完全性と可用性が確保されることを特徴とする技術はどれか。

平成30年秋期　問44
100問目／選択範囲の問題数237問

ア	MAC(Message Authentication Code)
イ	XML署名
ウ	ニューラルネットワーク
エ	ブロックチェーン

❑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

ブロックチェーンは、仮想通貨(暗号通貨)の基盤技術であり、"ブロック"と呼ばれる幾つかの取引データをまとめた単位をハッシュ関数で鎖のように繋ぐことによって、台帳を形成し、P2Pネットワークで管理する技術です。**分散型台帳技術**とも呼ばれます。

日本ブロックチェーン協会では、(広義の)ブロックチェーンを次のように定義しています。
「電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を広義のブロックチェーンと呼ぶ」

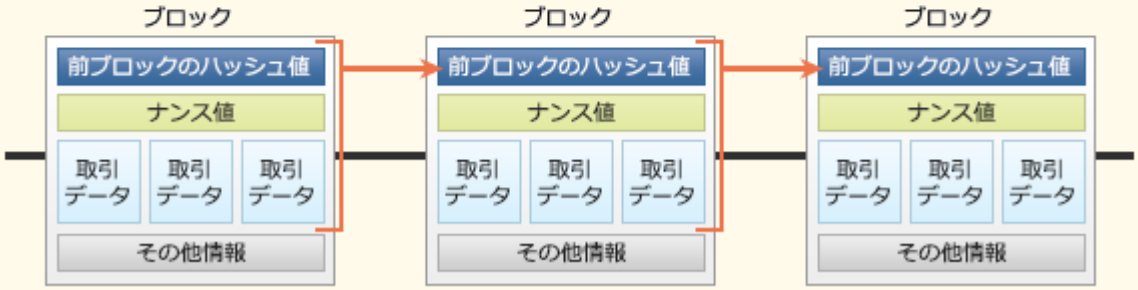


図　ブロックチェーン

ア　"MAC(Message Authentication Code)"

MAC(メッセージ認証符号)は、通信データとシークレットデータからハッシュ関数や共通鍵暗号を用いて生成される固定長のデータで、メッセージの改ざんの検知に用いられます。

イ　"XML署名"

XML署名は、XML文書にデジタル署名を埋め込むため仕様でRFC3075として標準化されています。デジタル署名と同様に完全性、認証、否認防止などのセキュリティ機能を提供します。

ウ “ニューラルネットワーク”

ニューラルネットワークは、脳機能に見られるいくつかの特性を計算機上のシミュレーションによって表現することを目指した数学モデルです。

エ “ブロックチェーン”

正しい。