平成 30 年度 秋期 情報処理安全確保支援士

＜午前Ⅱ解答・解説＞

●問 1　正解：ア

AES（Advanced Encryption Standard）は、DES（Data Encryption Standard）の後継として米国政府が採用した共通鍵暗号方式である。AES のブロック長は 128 ビットで、使用する鍵の長さは 128, 192, 256 ビットの中から選択することができる。段数（ラウンド数）は鍵長により、10 段、12 段、14 段となる。したがって**ア**が正解。

●問 2　正解：ウ

CVE（共通脆弱性識別子）は、その名が示す通り、脆弱性を識別するための識別子である。CVE は個別の製品に含まれる脆弱性を対象としており、米国政府の支援を受けた非営利団体の MITRE 社が採番している。したがって**ウ**が正解。

●問 3　正解：エ

ブロックチェーンとは、ハッシュ関数の技術を用いて、取引の記録を複数のコンピュータ間で相互に共有・検証しながら鎖のように連結していく仕組みである。したがって**エ**が正解。

●問 4　正解：ア

システムリソースに対する攻撃、ネットワーク帯域に対する攻撃など、種類の異なる複数の DDoS 攻撃を同時に行う手法をマルチベクトル型 DDoS 攻撃と呼ぶ。したがって**ア**が正解。

●問 5　正解：ア

FIPS 140-2（Federal Information Processing Standardization 140-2：連邦情報処理規格 140-2）は、米国連邦政府の省庁等各機関が利用する暗号モジュールに関するセキュリティ要件を規定した文書である。したがって**ア**が正解。

●問 6　正解：ア

サイバーセキュリティ経営ガイドラインは，大企業及び中小企業のうち、IT に関するシステムやサービス等を供給する企業及び経営戦略上 IT の利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、経済産業省と IPA が策定したガイドラインである。2015 年 12 月に初版である Ver1.0 が公表された後、毎年改訂が行われており、2017 年 11 月に Ver2.0 が公表された。

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」、及び経営者がサイバー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」をまとめているほか、付録として、サイバーセキュリティ経営チェックシートやインシデント発生時に組織内で整理しておくべき事項などがある。したがって**ア**が正解。

●問 7　正解：ア

解答群の中で、UDP に該当するのは DNS である。DNS リフレクタ攻撃（DNS リフレクション攻撃、DNS amp 攻撃とも呼ばれる）とは、DNS サーバ（キャッシュサーバ）に対し、発信元アドレスを攻撃のターゲットとなるホストのアドレスに詐称し、かつ応答メッセージのサイズが大きくなるクエリを送ることにより、その応答メッセージによってターゲットホストをサービス不能状態に陥らせる攻撃であるしたがって**ア**が正解。

●問 8　正解：ア

EDSA（Embedded Device Security Assurance）は、組込み機器である制御機器を評価対象とした認証制度である。 EDSA における評価項目は、「通信ロバストネス（堅牢性）試験（CRT)」、「機能セキュリティ評価（FSA)」、「ソフトウェア開発セキュリティ評価（SDSA)」の 3 項目である。したがって**ア**が正解。

●問 9　正解：ア

MITB 攻撃は、ブラウザの動作に介入し、インターネットバンキングの送金内容を勝手に書き換えて不正な送金を行う手法である。MITB への有効な対策として、トランザクション署名がある。トランザクション署名とは、送金時にトークン（携帯認証装置）を用いて署名情報を生成し、口座番号、金額とともに送信することで、取引の内容が通信の途中で改ざんされていないことを検証する技術である。したがって**ア**が正解。

●問 10　正解：ウ

クラウドコンピューティングにおける各サービス区分は次のようになっている。

SaaS(Software as a Service)
利用者に提供される機能はクラウドのインフラ上で稼動しているアプリケーションであり、利用者が OS などのインフラを管理したりコントロールしたり、アプリケーションの設定をしたりすることはできない。

PaaS(Platform as a Service)
利用者に提供される機能はクラウドのインフラ上に利用者が開発もしくは購入したアプ

リケーションを実装することである。利用者は OS などのインフラを管理したり、ミドルウェアの設定等を行ったりすることはないが、自分が実装したアプリケーションに対する各種設定、セキュリティ対策等を行う。

IaaS(Infrastructure as a Service)、HaaS（Hardware as a Service）
利用者に提供される機能は CPU、ストレージ等のインフラである。利用者は OS やミドルウェア、ストレージ容量等を選択してサーバ環境を構築し、OS やミドルウェアに対する各種設定等を行う。

上記により、問題文に該当するのは PaaS である。したがって**ウ**が正解。

●問 11　正解：エ

Mirai は、IP カメラなどの IoT 機器に感染を広げ、C&C サーバからの指令を受けて大規模な DDoS 攻撃を行うマルウェアである。多くの IoT 機器が、工場出荷時の脆弱なパスワードが設定されたままで設置されていたことが、Mirai による感染が広がる原因となった。したがって**エ**が正解。

●問 12　正解：エ

HSTS は、Web サイトが、HTTPS でアクセスしたブラウザに対し、当該ドメイン（サブドメインにも適用可能）への次回以降のアクセスにおいて、「max-age」で指定した有効期限（秒単位）まで、HTTPS の使用を強制させる機構である。HSTS は、HTTPS の応答ヘッダに「Strict-Transport-Security」を指定することによって有効になる。したがって**エ**が正解。

●問 13　正解：イ

問題文に該当するのは OS コマンドインジェクションであり、イが正解。OS コマンドインジェクションは、Perl の open 関数、system 関数、PHP の exec 関数など、OS コマンドや外部プログラムの呼出しを可能にするための関数を利用することで、任意の命令を実行したり、ファイルの読出し、変更、削除などを行ったりする攻撃手法である。

ア　HTTP ヘッダインジェクションは、HTTP ヘッダ内に不正なデータを入力することで、任意のヘッダフィールドやメッセージボディを追加したり、複数のレスポンスに分割したりする攻撃を行う手法である。
ウ　クロスサイトリクエストフォージェリは、Web アプリケーションのユーザ認証やセッション管理の不備を突いて、サイトの利用者に不正な処理要求を行わせる手法である。

エ　セッションハイジャックは、クライアントとサーバの正規のセッションの間に割り込んで、そのセッションを奪い取る行為である。

●問 14　正解：ウ

SMTP-AUTH は、SMTP にユーザ認証機能を追加した方式であり、クライアントが SMTP サーバにアクセスしたときにユーザアカウントとパスワードによる利用者認証を行うことで、許可された利用者だけから電子メールの送信を受け付ける。したがって**ウ**が正解。

ア　OP25B（Outbound Port25 Blocking）の説明である。
イ　SPF（Sender Policy Framework）の説明である。
エ　POP before SMTP の説明である。

●問 15　正解：ウ

TLS（Transport Layer Security）では、ディジタル証明書を用いて、クライアント、サーバ間で相互認証を行うことが可能である。ディジタル証明書を個人を認証する目的で使用する場合には、IC カードや USB デバイスなどにディジタル証明書を格納することで、PC を限定せずに使用することができる。したがって**ウ**が正解。

●問 16　正解：ア

PGP（Pretty Good Privacy）は、1991 年に米国の Philip R. Zimmermann 氏によって開発された電子メールの暗号化ツールである。PGP では基本的な暗号化アルゴリズムとして、RSA と IDEA が用いられており、ユーザ（メールアドレス）ごとに公開鍵を用意する。

S/MIME（Secure Multipurpose Internet Mail Extensions）は米国 RSA Security 社によって開発された暗号化電子メール方式である。S/MIME は不特定多数のユーザ間で安全性、信頼性の高い通信を行うことを想定しているため、利用にあたって各ユーザは公開鍵を生成し、ディジタル証明書（S/MIME 証明書）を取得する必要がある。

SMTP over TLS は、メールクライアントとメールサーバ間の SMTP 通信、もしくはメールサーバ間の SMTP 通信を TLS で暗号化する仕組みであり、メールサーバごとに公開鍵を生成し、ディジタル証明書を取得する必要がある。

したがって**ア**が正解。

●問 17　正解：イ

IEEE 802.1X とは、ネットワーク環境においてユーザ認証を行うための規格である。IEEE 802.1X に準拠した認証システムは、クライアントであるサプリカント、アクセスポイントや LAN スイッチなど、認証の窓口となる機器であるオーセンティケータ、認証サーバ

（RADIUS サーバなど）から構成される。認証サーバに RADIUS を用いる場合には、オーセンティケータが RADIUS クライアントとなる。したがって**イ**が正解。

●問 18　正解：ア

TCP の 3 ウェイハンドシェイクとは、「3 ウェイ」の名が示すように、次の①～③の 3 回のパケット送信によってコネクションを確立する方式である。

① SYN（要求元が送信）
② SYN+ACK（要求先が送信）
③ ACK（要求元が送信）

したがって**ア**が正解。

●問 19　正解：ウ

クラスDのIPアドレスはマルチキャスト通信に用いられる。マルチキャストとは、TCP/IPプロトコルにおいて同時に複数のノードを指定してデータを送信する技術であり、UDP による動画のリアルタイム配信などの用途に用いられる。マルチキャストに対し、単一のノードにデータを送信することを"ユニキャスト"、同一ネットワーク上のすべてのノードに同時にデータを送信することを"ブロードキャスト"という。したがって**ウ**が正解。

●問 20　正解：ウ

無線 LAN の各規格の周波数帯域を次に示す。

IEEE 802.11b　2.4GHz 帯
IEEE 802.11a　5GHz 帯
IEEE 802.11g　2.4GHz 帯
IEEE 802.11n　2.4GHz 帯, 5GHz 帯
IEEE 802.11ac 5GHz 帯

したがって**ウ**が正解。

●問 21　正解：エ

最初の 3 行の SQL 文で実表"取引先"の所在地が'東京'であるビューを生成し、次の 2 行では、GRANT 文を用いて利用者"8823"に対し、生成したビューの参照権限を付与している。したがって**エ**が正解。

●問 22　正解：イ

上位層であるアプリケーション層及びミドルウェア層の単体テストが終了している場合には、スタブを用いてトップダウン型の結合テストを行うのが適切である。スタブは、未完成の下位モジュールの代わりとなってテスト対象の上位モジュールから呼び出される役割を持つ。一方、未完成の上位モジュールの代わりにテスト対象の下位モジュールに引数を渡して呼び出すのがドライバである。したがって**イ**が正解。

●問 23　正解：ウ

SOA（Service Oriented Architecture：サービス指向アーキテクチャ）とは、業務の機能を「サービス」という単位で実装し、それらを組み合わせることによってシステムを構築する考え方である。サービスは、一つまたは複数のアプリケーションをコンポーネント化したものであり、外部から呼び出すためのインターフェイスを持っている必要がある。

サービス間の関係を疎結合にすることで、各サービスの独立性が高まり、業務の変化に対応しやすくなる。サービスを設計する際にはこの点を十分考慮する必要ある。したがって**ウ**が正解。

●問 24　正解：ウ

JIS Q 20000-1：2012 の「6.6.3 情報セキュリティの変更及びインシデント」において、次のような要求事項が挙げられている。

6.6.3 情報セキュリティの変更及びインシデント

次を特定するために，変更要求を評価しなければならない。

a) 新たな情報セキュリティリスク，又は変化した情報セキュリティリスク

b) 既存の情報セキュリティ基本方針及び管理策への潜在的影響

したがって**ウ**が正解。

ア　「9.1 構成管理」における要求事項である。

イ　「8.2 問題管理」における要求事項である。

エ　「9.2 変更管理」における要求事項である。

●問 25　正解：ウ

自社が提供する Web サービスの信頼性に責任を負うのは、当該企業の経営者である。保証業務の実施者は外部監査人であり、その報告書の想定利用者は Web サービス利用者である。表の A～D のうち、この組合せとなっているのは C である。したがって**ウ**が正解。