平成 29 年度 春期 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

SSL/TLS の**ダウングレード攻撃**とは，中間者攻撃によってバージョンの古い脆弱な暗号スイートの使用を強制し，暗号化通信の解読を試みるものである。攻撃者は SSL/TLS の暗号化通信の確立プロセスに介在することにより，この攻撃を成立させる。したがって**ウ**が正解。

●問３　正解：ア

サイドチャネル攻撃とは，耐タンパ性を備えた IC カードや TPM（Trusted Platform Module）などに対し，物理的に破壊することなく，暗号化処理時の消費電力など外部から観察可能な情報や，外部から操作可能な手段を利用して暗号鍵/復号鍵などの機密情報を奪取する手法である。したがって**ア**が正解。

イ　スキャベンジング（scavenging）の説明である。
ウ　中間者攻撃（Man-in-the-Middle Attack）の説明である。
エ　SQL インジェクションの説明である。

●問４　正解：イ

TPM は，耐タンパ性に優れたセキュリティチップであり，通常マザーボードに直付けする形で PC に搭載されている。TPM は，暗号化に用いる鍵ペアの生成・格納，暗号化・復号処理の実行などの機能を持つ。したがって**イ**が正解。

●問５　正解：ウ

セッション ID の固定化攻撃とは，ターゲットユーザに対して攻撃者が生成したセッション ID を含む不正な URL を送りつけることで意図的にセッションを確立させ，そのセッションをハイジャックするというものである。セッション ID の固定化攻撃は次のように実行される。

ア　攻撃者がターゲットとなる Web サイトのログイン画面などにアクセスし，実際に発行されたセッション ID（例：98765）を入手する

イ　入手したセッション ID を含む URL（例：;sessionid=98765）をリンク先としてセットしたフィッシングメールをターゲットユーザに送付する（もしくは他の手段でその URL をクリックさせる）

ウ　ターゲットユーザがそのリンクをクリックし（そのセッション ID を使って），ターゲットサイトにログインする

エ　攻撃者も同じセッション ID を使ってターゲットサイトへのアクセスに成功し，正規のユーザになりすまして不正な操作などを行う

したがって**ウ**が正解。

●問６　正解：イ

DNS 水責め攻撃とは，問合せ元のアドレスや問合せ対象ドメインの制限なく名前解決要求に応じ状態（オープンリゾルバ）となっている DNS キャッシュサーバに対し，攻撃対象のドメインのランダムなサブドメイン名を大量に発生させ，不正な名前解決要求を行う手法である。これにより，攻撃対象ドメインの権威 DNS サーバ（コンテンツサーバ）を過負荷にさせる。したがって**イ**が正解。

●問７　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８　正解：イ

NIST（National Institute of Standards and Technology：米国国立標準技術研究所）では，クラウドコンピューティングのサービスモデルについて概ね次のように定義している。

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。

したがって**イ**が正解。

●問 9　正解：エ

リスク回避とは，リスク発生の根本原因（作業，事象など）を排除することによってリスクを処理する方法である。たとえば，インターネットからのサイバー攻撃を受けるリスクを処理するために，インターネットへの接続自体を取りやめることなどがリスク回避に該当する。問題文のア～エの中では，**エ**の内容がリスク回避に該当する。

ア：リスク受容に該当する。
イ：リスク低減に該当する。
ウ：リスク移転に該当する。

●問 10　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 11　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 12　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 13　正解：ウ

フォールスネガティブとは，本来検知すべき事象（攻撃，不正行為等）を見逃してしまうことである。解答群の中でウイルス対策ソフトでのフォールスポジティブに該当するのは，ウイルスに感染しているファイルをウイルスに感染していないと判断することである。したがって**ウ**が正解。

これに対し，本来検知する必要のない事象を誤って検知してしまうことを**フォールスポジティブ**という。

●問 14　正解：ア

OAuth2.0 は，信頼関係にある複数のサービス間で，セキュアに認可情報をやり取りする仕組み（API）を提供する。

OAuth2.0 の API を提供しているサービスを「resource server」と呼び，本問では Web サービス A が該当する。一方，resource server が提供する API を利用するサービスを「client」と呼び，本問では Web サービス B が該当する。また，認可情報を付与する利用者を「resource owner」と呼ぶ。

利用者の認可の下，Web サービス B が Web サービス A 上のリソースへの限定的なアクセス権を取得しようとする際には，Web サービス A が，利用者を認証・認可した上で Web サービス B に対してアクセストークンを発行する。したがって**ア**が正解。

●問 15　正解：イ

OP25B（Outbound Port25 Blocking）とは，ISP が動的 IP アドレスを割り当てた（ISP 管理下の）ネットワークから，当該 ISP のメールサーバを経由せずに，ISP 管理外のネットワーク（外向き）に直接出ていく 25 番ポート宛のパケット（SMTP）を遮断する方式である。このようなパケットは，ISP 管理外のネットワークに向けたスパムメールである可能性が高い。したがって**イ**が正解。

●問 16　正解：ウ

サンドボックスとは，システムの実環境に影響が及ばないように，機能やアクセスできるリソースを制限したプログラム実行環境である。仮想環境上のサンドボックスで不審なプログラムを実行させ，その振る舞いからマルウェアかどうかを判定するなどの用途で使用されている。したがって**ウ**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：イ

ICMP Flood 攻撃（Ping Flood 攻撃）とは，ターゲットとなるサーバに対し，ICMP echo request（ping コマンド）を大量に送り続けることにより，当該サーバが接続されている回線を過負荷状態にして正常なアクセスを妨害する攻撃である。したがって**イ**が正解。

ア　HTTP GET Flood 攻撃（Connection Flood 攻撃の一種）の説明である。
ウ　SYN Flood 攻撃の説明である。
エ　Connection Flood 攻撃の説明である。

●問 19　正解：ア

イーサネットインタフェースには，送信端子，受信端子の割り当ての違いにより，**MDI** と **MDI-X** の 2 種類があり，MDI と MDI-X を接続する場合には**ストレートケーブル**，MDI 同士，あるいは MDI-X 同士を接続する場合には**クロスケーブル**を使用する場合がある。

Automatic MDI/MDI-X は，ストレートケーブル，クロスケーブルのどちらを使用しても，コネクタの送信端子と受信端子が正しい組合せになるように自動的に切り替える機能である。したがって**ア**が正解。

●問 20　正解：ア

問題文に該当するのはCSMA/CA（Carrier Sense Multiple Access/Collision Avoidance）であり，**ア**が正解。

IEEE 802.11a，IEEE 802.11b はいずれも無線 LAN の規格である。

有線 LAN とは異なり，無線 LAN 環境では通信の衝突を検出できないため，各ホストは自分が通信する際に，まず他のホストが通信していないことを確認（Carrier Sense）した後，ランダムな長さの待ち時間をとってから送信を開始することで，通信の衝突を回避（Collision Avoidance）する仕組みとなっている。

●問 21　正解：ア

SQL の **GRANT 文**は，ユーザに対し，テーブル，ビューなどのオブジェクトに関する特定の権限を付与する。既に何らかの権限を有していた場合には，それに追加される。

GRANT 文の基本的な構文は次の通り。

GRANT 権限名 ON オブジェクト名 TO ユーザ名;

- 権限名に"ALL"もしくは"ALL PRIVILEGES"と記述すると，SELECT 権限，UPDATE 権限，INSERT 権限，DELETE 権限などのすべての権限をユーザに付与することになる。
- ユーザ名に"PUBLIC"を指定すると，すべてのユーザに権限を付与することになる。
- "WITH GRANT OPTION"を指定すると，権限を他のユーザに付与する権限をユーザに対して与えることができる。

したがって**ア**が正解。

●問 22　正解：ア

JIS X 25010:2013（システム及びソフトウェア品質モデル）では，製品品質を 8 つの特性（機能適合性，信頼性，性能効率性，使用性，セキュリティ，互換性，保守性及び移植性）に分類しており，各特性は，関係する副特性の集合から構成される。

ア　適切な記述である。
イ　性能効率性に関する記述である。
ウ　使用性に関する記述である。

エ　信頼性に関する記述である。

したがってアが正解。

●問 23　正解：イ

DTCP-IP（Digital Transmission Content Protection over Internet Protocol）は，著作権保護されたコンテンツを伝送するためのプロトコルである。DLNA（Digital Living Network Alliance）とともに使用され，接続する機器間で相互認証し，コンテンツ保護が行える場合に録画再生を可能にする。したがってイが正解。

●問 24　正解：エ

フルバックアップを取得する時間間隔を 2 倍にしてもフルバックアップで取得するデータの量は変わらないため，1 回当たりの磁気テープ使用量や平均実行時間は変わらない。

一方，フルバックアップを取得する時間間隔を 2 倍にすると，その間に行われたデータの追加・変更・削除等のログ情報は約 2 倍になるため，当該ログ情報によって復旧するときの処理時間も平均して約 2 倍になる。したがってエが正解。

●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。