平成 29 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：エ

CRL は，ディジタル証明書の悪用や誤発行などの不測事態が発生したことによって有効期限内に破棄する必要が生じた証明書が登録されたリストであり，当該証明書のシリアル番号，失効した日時が掲載される。CRL に登録された証明書の情報は，当該証明書の有効期限が満了になった段階で CRL から削除される。したがって**エ**が正解。

●問 2　正解：ウ

OCSP（Online Certificate Status Protocol）とは，ディジタル証明書の失効情報をリアルタイムで確認する仕組みである。OCSP を実装したサーバを OCSP レスポンダ（OCSP サーバ）といい，CA（Certification Authority）や VA（Validation Authority）が運営する。クライアントは OCSP レスポンダに問い合わせることによって，自力で CRL を取得したり照合したりする手間を省くことができる。したがって**ウ**が正解。

●問 3　正解：ア

問題文に該当するのは SAML（Security Assertion Markup Language）である。SAML とは，異なる Web サーバ間において，ユーザ ID・パスワード・公開鍵等の認証情報やアクセス制御情報，属性情報等を安全に交換するためのプロトコルである。XML 関連の標準化団体である OASIS（Organization for the Advancement of Structured Information Standards）によって策定された。SAML では，認証や認可に関する情報等を格納する XML ベースの証明書（Assertion）の仕様や，Assertion を交換するためのプロトコルを標準化することで，シングルサインオンのための基盤を提供している。したがって**ア**が正解。

イ　SOAP（Simple Object Access Protocol）は，XML と HTTP などをベースとしており，他のコンピュータ上にあるデータやサービスを呼び出すためのプロトコルである。

ウ　XKMS（XML Key Management Specification）は，XML をベースとして PKI の鍵情報の取得や管理を行うための仕様である。

エ　XML Signature は，XML 文書にディジタル署名を行う技術である。

●問 4　正解：エ

ハッシュ関数は，任意の長さの入力データ（x）をもとに，固定長のビット列（ハッシュ値：y＝H(x)）を生成する関数（H(x)）である。ハッシュ関数には，次の 3 つの性質が求められる。入力データを「メッセージ」，求められるハッシュ値を「メッセージダイジェスト」ともいう。

・衝突発見困難性
　同一のハッシュ値を生成する（H(x)＝H(x')）異なる 2 つのデータ(x, x')を求めることが計算量的に困難であること
・第 2 原像計算困難性
　データ(x)と，それに対するハッシュ値(y＝H(x))が与えられたとき，同じハッシュ値を生成する（y＝H(x')）データ(x')を求めることが計算量的に困難であること
・原像計算困難性（一方向性）
　ハッシュ値(y＝H(x))が与えられたとき，それを生成するデータ(x)を求めることが計算量的に困難であること

これらは，衝突発見困難性→第 2 原像計算困難性→原像計算困難性（一方向性）の順により困難となる。

ア　最大の計算量は 256 の 2 乗ではなく，2 の 256 乗である。
イ　原像計算困難性（一方向性）に関する記述である。
ウ　原像計算困難性（一方向性）に関する記述である。
エ　適切な記述である。

したがって**エ**が正解。

●問 5　正解：エ

ソフトウェアやハードウェアの脆弱性を悪用して攻撃するために作成されたプログラムを**エクスプロイトコード**（exploit code）と呼ぶ。したがって**エ**が正解。

●問 6　正解：ウ

カミンスキー攻撃とは，セキュリティ研究者の Dan Kaminsky 氏によって考案・公表された DNS キャッシュポイズニング攻撃の一種である。攻撃者は，汚染情報を登録したいドメイン名と同じドメインかつ存在しない FQDN の名前解決要求を行うことで，従来よりも効率良く攻撃を成立させる手法である。

攻撃を成功させるためには，攻撃者は，送信ポート番号（名前解決要求の送信元ポート

番号であり，応答時のあて先ポート番号となる)，トランザクション ID を本来の応答レコードと合致させる必要がある。しかし，送信ポート番号，あて先ポート番号ともに 53 番に固定する設定となっている DNS サーバは数多く存在し，攻撃を容易にさせている。また，トランザクション ID が 16 ビット（最大 65,536 通り）であることも攻撃を容易にさせている。

そのため, DNS の送信元ポート番号をランダム化(ソースポートランダマイゼーション)することで，カミンスキー攻撃をはじめとした DNS キャッシュポイズニング攻撃が成功する確率を大きく低減することができる。したがって**ウ**が正解。

●問 7　正解：ア

Smurf 攻撃とは，最終的なターゲットホストの IP アドレスを発信元アドレスとして偽装した ICMP 応答要求（ICMP echo request）を，攻撃に加担させる（踏み台）ネットワークセグメントのブロードキャストアドレス宛に送ることにより，大量の ICMP 応答（ICMP echo reply）パケットを発生させ，サービスを妨害する攻撃手法である。したがって**ア**が正解。

イ　SYN Flood 攻撃の説明である。
ウ　UDP Flood 攻撃の説明である。
エ　メールボム（e-mail bomb）の説明である。

●問 8　正解：イ

問題文に該当するのはサイドチャネル攻撃である。**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**イ**が正解。

●問 9　正解：エ

ステートフルインスペクションは，パケットフィルタリングを拡張した方式である。「ステートフル」とは，個々のセッションの状態を管理して，常にその情報に基づいてフィルタリングを行うという意味であり，受け付けたパケットをセッションの状態に照らし合わせて通過させるか遮断させるかを判断する。したがって**エ**が正解。

●問 10　正解：イ

ディジタル証明書は ITU-T 勧告の X.509 に定義されており，発行に際には申請者の公開鍵に対して認証局（CA）がディジタル署名を付す。ディジタル証明書は，TLS プロトコルで通信データの暗号化のための鍵交換や通信相手の認証に利用されるほか，S/MIME にお

けるメールの暗号化やディジタル署名等にも利用されている。したがって**イ**が正解。

ア　X.509 で規定されている。
ウ　申請者の公開鍵に対して認証局がディジタル署名する。
エ　下位層の認証局の公開鍵に対してルート認証局の秘密鍵でディジタル署名する。

●問 11　正解：イ

JIS Q 27000:2014**「情報セキュリティマネジメントシステムー用語」**では，是正処置（corrective action）を「不適合の原因を除去し，再発を防止するための処置」と定義している。したがって**イ**が正解。

●問 12　正解：エ

ア　脆弱性の説明である。
イ　脅威の説明である。
ウ　リスク評価の説明である。
エ　正しい記述である。なお，リスク特定には，過去のデータ，理論的分析，情報に基づいた意見，専門家の意見及びステークホルダのニーズを含むことがある。

したがって**エ**が正解。

●問 13　正解：ア

問題文に該当するのは CVSS（Common Vulnerability Scoring System：**共通脆弱性評価システム**）である。CVSS は，IT 製品の脆弱性に対するオープンで汎用的な評価手法であり，ベンダに依存しない共通の評価方法を提供している。CVSS で用いる 3 つの基準は次の通り。

・基本評価基準（Base Metrics）
　脆弱性そのものの特性を評価する基準。機密性，完全性，可用性に対する影響を評価し，CVSS 基本値（Base Score）を算出する。

・現状評価基準（Temporal Metrics）
　脆弱性の現状の深刻度を評価する基準。攻撃コードの出現有無や対策情報が利用可能であるかといった基準で評価し，CVSS 現状値（Temporal Score）を算出する。

・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。攻撃によ

る被害の大きさや対象製品の使用状況といった基準で評価し， CVSS 環境値（Environmental Score）を算出する。

したがって**ア**が正解。

●問 14　正解：エ

問題文の攻撃手法は，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 Web アプリケーションに対する不正な処理要求を行わせる手法であり，**クロスサイトリクエストフォージェリ**（Cross-Site Request Forgeries：CSRF）と呼ばれる。CSRF による被害を防ぐためには，Web アプリケーションのユーザ認証機能やセッション管理機能を強化し，不正なリクエストを受け付けないようにする必要がある。具体的には，次のようなものがある。

・POST メソッドを使用し，hidden フィールドに秘密情報をセットする
・確定処理の直前で再度パスワードを入力させる
・Referrer を用いてリンク元の正当性を確認する
・重要な操作を行った後で，その内容を登録アドレスにメール送信する

したがって**エ**が正解。

●問 15　正解：イ

OP25B（Outbound Port25 Blocking）とは，ISP（Internet Services Provider）が動的 IP アドレスを割り当てたネットワークから，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。したがって**イ**が正解

●問 16　正解：エ

ディジタルフォレンジックスで証拠を収集する際には，揮発性の高いものから順に進める必要がある。

RFC3227「証拠収集とアーカイビングのためのガイドライン」によれば，揮発性の順序について，次のように例示されている。（上のものほど揮発性が高い）

① レジスタ，キャッシュ
② ルーティングテーブル，arp キャッシュ，プロセステーブル，カーネル統計，メモリ
③ テンポラリファイルシステム
④ ディスク

⑤ 当該システムと関連する遠隔ロギングと監視データ
⑥ 物理的設定，ネットワークトポロジ
⑦ アーカイブ用メディア

a は⑤，b は⑦，c は④，d は②に該当するため，保全の順序は d → c → a → b となる。したがって**エ**が正解。

●問 17　正解：エ

ア　EAP（PPP Extensible Authentication Protocol）は，IEEE 802.1X 規格に基づき，PPP の認証機能を強化・拡張したユーザ認証プロトコルである。
イ　RADIUS（Remote Authentication Dial-In User Service）は，ネットワーク利用者の認証と利用記録を一元的に行うシステムである。
ウ　SSID（Service Set ID）は，同じ無線 LAN アクセスポイントに接続する通信端末をグループ化するために設定された論理的な名称である。
エ　正しい記述である。

●問 18　正解：ア

ルータは，コリジョン（複数の機器が同時にデータを創出したことによるデータの衝突）や，ブロードキャストを他のネットワークセグメントには中継しない。したがって**ア**が正解。

●問 19　正解：イ

100×10^6 ビット／秒の LAN の伝送効率が 50%であるため，実質的な伝送速度は 50×10^6 ビット／秒 である。

また，ピーク時のクライアント 1 台の通信量である 600×10^3 バイト／分 を「ビット／秒」に換算すると，80×10^3 ビット／秒 となる。

前者を後者で割れば，業務を滞りなく遂行できるクライアント数が求められる。

$$\frac{50\times10^6}{80\times10^3} = \frac{5000}{8} = 625$$

したがって**イ**が正解。

●問 20　正解：イ

サブネットマスクとは，IP アドレスのうち，上位何ビットまでがネットワークアドレスであるかを表すものであり，255.255.255.224 を 2 進数で表すと次のようになる。

11111111.11111111.11111111.11100000

これは，1 オクテット目から 4 オクテット目の上位 3 ビットまでがネットワークアドレスで，4 オクテット目の下位 5 ビットがホストアドレスであることを表している。

198.51.100.90 の場合，4 オクテット目の 90 を 2 進数で表すと 01011010 となるが，この中で下位 5 ビットの 11010 がホストアドレスとなり，これを 10 進数で表すと 26 となる。したがって**イ**が正解。

●問 21　正解：ウ

ア　誤差逆伝播法の調整作業は出力層から入力層に向かって行われる。

イ　サポートベクタマシンは機械学習におけるパターン認識手法の一つであり，大量計算には向かない。

ウ　正しい記述である。

エ　過学習とは，機械学習等において，過度の学習を行った場合，未知のデータに対して正しく答えを出力できなくなる現象である。

●問 22　正解：エ

JIS X 25010:2013 では，システム利用時の品質特性について，有効性，効率性，満足性，リスク回避性，利用状況網羅性の 5 つに分類しており，各特性は，関係する副特性の集合から構成される。

満足性とは，「製品又はシステムが明示された利用状況において使用されるとき，利用者ニーズが満足される度合い」であり，その副特性を次のように定義している。

●実用性
利用の結果及び利用の影響を含め，利用者が把握した目標の達成状況によって得られる利用者の満足の度合い。

●信用性
利用者又は他の利害関係者がもつ，製品又はシステムが意図したとおりに動作するという確信の度合い。

●快感性
個人的なニーズを満たすことから利用者が感じる喜びの度合い。

●快適性
利用者が（システム又はソフトウェアを利用する時の）快適さに満足する度合い。

ア　快感性の説明である。
イ　快適性の説明である。
ウ　信用性の説明である。
エ　実用性の説明である。

したがって**エ**が正解。

●問 23　正解：ウ

このようなケースにおいて，著作権の帰属に関する特段の取決めがない場合，開発したソフトウェアの著作権は原則として請負人に帰属する。したがって**ウ**が正解。

●問 24　正解：ウ

フェールソフトとは，システムの一部に障害が発生した場合に，システム全体の停止とならないように，正常な部分でシステムの運用を継続することである。したがって**ウ**が正解。

ア　フォールトトレラントの例である。
イ　フェールセーフの例である。
エ　フールプルーフの例である。

●問 25　正解：ア

システム監査基準において，「システム監査人は，システム監査を客観的に実施するために，監査対象から独立していなければならない。監査の目的によっては，被監査主体と身分上，密接な利害関係を有することがあってはならない。」とされている。

内部監査において，過去に在籍していた部門に対する監査にメンバを従事させる場合，一定の期間を置くのは適切な措置である。したがって**ア**が正解。