平成 26 年度 春期 情報セキュリティスペシャリスト

＜午前Ⅱ　解答・解説＞

●問１　正解：イ

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ディジタル証明書が登録されたリストであり，当該ディジタル証明書と破棄された日時の対応が提示される。したがって**イ**が正解。

ディジタル証明書の有効性を検証する場合，証明書の署名の確認と併せて CRL に検証対象の証明書が記載されていないかを確認する必要がある。ただし，ディジタル証明書は有効期限が満了になった段階で CRL から削除されるため，有効期間中に失効されたとしても，最新の CRL にはその証明書の失効情報が含まれていない可能性もある。証明書の有効性を過去にさかのぼって検証する場合には，その時点での CRL を確認する必要がある。

●問２　正解：ウ

XML 署名（XML ディジタル署名）は，XML 文書にディジタル署名を行う技術であり，W3C（World Wide Web Consortium）と IETF（Internet Engineering Task Force）によって共同開発された。（RFC 3075）XML 署名では，署名対象や署名アルゴリズムなどを XML で記述する。また，署名の対象となる XML 文書（オブジェクト）全体だけでなく，オブジェクト中の指定したエレメントに対しても署名することができる。

XML 署名には，Enveloped 署名，Enveloping 署名，Detached 署名の 3 つがある。Enveloped 署名では，署名の対象となるオブジェクトの内部に署名が置かれる。Enveloping 署名では，署名の内部に署名の対象となるオブジェクトが置かれる。Detached 署名では，署名の対象となるオブジェクトと署名とが独立しており，オブジェクトは URI（Uniform Resource Identifier）によって参照される。したがって**ウ**が正解。

●問３　正解：ウ

EDoS 攻撃とは，ストレージ容量やトラフィック量に応じて課金されるクラウドの特性を悪用し，クラウド利用企業の経済的な損失を狙ってリソースを大量消費させる攻撃である。したがって**ウ**が正解。

●問４　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５　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もつ。したがって**イ**が正解。

●問６　正解：エ

ダイナミックパケットフィルタリング型のファイアウォールでは，最初にコネクションを確立する方向のみを意識した基本的な ACL を事前に登録しておき，実際に接続要求（TCP であれば SYN パケット）があると，個々の通信をセッション管理テーブルに登録するとともに必要なルールが動的に生成され，フィルタリング処理を行う。

セッション管理テーブルにより，通過したパケットの応答や，それに付随するコネクションなどを総合的に管理し，自動的に必要な処理を行う。セッションが終了すると，動的に生成したルールは破棄される。

従来のスタティックパケットフィルタリング型のファイアウォールでは，上りも下りも別個の通信としかとらえられなかったため，不正アクセスによって順序の矛盾したパケットが送られてきたとしても，該当する条件が ACL に登録されてさえいれば中継していた。一方，ダイナミックパケットフィルタリング型では，過去の通信の状態が記録されており，それと矛盾するパケットは不正パケットとして遮断することができる。したがって**エ**が正解。

●問７　正解：イ

ポリモーフィック（polymorphic：多形体，同質異像体）とは，同一の物質からなる結晶でありながら，構造が異なるために物性が異なっている結晶のことを意味する。**ポリモーフィック型ウイルス**とは，感染するごとに異なる暗号鍵を用いて自身を暗号化することによってコードを変化させ，パターンマッチング方式のウイルス対策ソフトで検知されないようにするタイプのウイルスである。したがって**イ**が正解。

●問８　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。

●問９　正解：エ

IP スプーフィング（IP 詐称）攻撃とは，偽の発信元 IP アドレスをセットしたパケットを送ることで，不正アクセスを試みる手口である。過去には，インターネット側にいる攻撃者が，送信元 IP アドレスにプライベートアドレスをセットしたパケットを送り付けることによって，ファイアウォールのアクセス制限をくぐり抜けて内部ネットワークへの侵入に成功したケースなどがあった。このような攻撃に対しては，外部ネットワークから内部ネットワークへのパケットの送信元 IP アドレスが，自組織の内部アドレス（プライベートアドレス）であった場合には破棄するのが有効である。したがって**エ**が正解。

●問 10　正解：ウ

cookie に Secure 属性をセットすると，HTTPS（HTTP over SSL/TLS）で通信している場合のみ当該 cookie を送信する。これにより，パケット盗聴によって cookie が盗まれるのを防ぐことが可能となる。したがって**ウ**が正解。

●問 11　正解：ウ

テンペスト（TEMPEST : Transient Electromagnetic Pulse Surveillance Technology）**攻撃**とは，パソコンのディスプレイ装置や接続ケーブルなどから放射される微弱な電磁波を傍受し，それを解析することによって，入力された文字や画面に表示された情報を盗む攻撃手法である。したがって**ウ**が正解。

テンペスト攻撃への対抗策としては，電磁波対策が施されたパソコンを使用する，電磁波を遮断する製品を使用する，電磁波遮断対策が施された部屋や施設内でパソコンを使用するなどの方法がある。

なお，パソコンなどが発する電磁波については，VCCI（情報処理装置等電磁波障害自主規制協議会）規格によって規制値が定められており，現在市販されている製品はこの規格をクリアしている。そのため，パソコンなどを購入時の状態で使用していればテンペスト攻撃への対策はある程度できていることになる。しかし，パソコンを改造したり，ハードディスクを増設したりするなどした場合には，VCCI の規制値以上の電磁波が放射される可能性がある。

●問 12　正解：ウ

TCP ポートに対するポートスキャンでは，対象ポートに SYN パケットを送り，その応答結果が"SYN/ACK"であればポートが開いていると判定し，"RST/ACK"であればポートが閉じていると判定する。

UDP ポートに対するポートスキャンでは，対象ポートに UDP パケットを送り，その結果，何の応答もなければポートが開いていると判定し，"port unreachable"が返ってきた場合はポートが閉じていると判定する。

したがって**ウ**が正解。

●問 13　正解：エ

ア　**EAP**（PPP Extensible Authentication Protocol）とは，PPP の認証機能を強化・拡張したユーザー認証プロトコルであり，IEEE 802.1X 規格を実装した標準的な認証プロトコルである。

イ　**RADIUS**（Remote Authentication Dial-In User Service）とは，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）とは，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。

したがって**エ**が正解。

●問 14　正解：エ

CWE 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ある。CWE では，SQL インジェクション，クロスサイトスクリプティングなど，脆弱性の種類（脆弱性タイプ）の一覧を体系化して提供している。したがって**エ**が正解。

●問 15　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**とは，ユーザーの入力データを基に，HTTP メッセージのレスポンス（メッセージヘッダ，メッセージボディ）を生成する Web アプリケーションにおいて，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などの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**（CSRF）とは，Web アプリケーションのユーザー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る。

エ　**セッションハイジャック**とは，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 16　正解：イ

WAF は，クロスサイトスクリプティング，SQL インジェクション，OS コマンドインジェクションなど，Web アプリケーションに対する攻撃を検出・排除することでセキュアな Web アプリケーション運用を実現する製品である。

WAF のブラックリストには，Web アプリケーションに対する攻撃の特徴を示す通信データのパターンを定義しておくことで，攻撃を検出し，該当する通信を遮断するか又は無害化する。

一方，WAF のホワイトリストには，正常な通信データのパターンを定義しておくことで，それに合致しない通信データを攻撃として検出する。したがって**イ**が正解。

●問 17　正解：ア

SSL2.0 など，旧バージョンの SSL で用いられている暗号方式は脆弱であるため，暗号化通信の内容を解読される可能性がある。**SSL に対するバージョンロールバック**とは，クライアントが TLS1.0 など SSL3.0 以降のプロトコルで通信しようとしているにもかかわらず，悪意のある通信仲介者が SSL の実装の脆弱性を悪用することにより，SSL2.0 での通信を強制し，暗号化通信の内容を解読しようと試みる攻撃である。したがって**ア**が正解。

●問 18　正解：エ

1 回当たりのファイルサイズが平均 1,000 バイトで，転送時にはファイルサイズの 30%に当たる各種制御情報が付加されるため，転送時のファイルサイズは平均 1,300 バイトとなる。

このファイルが平均 60 回／秒の頻度で 2 組のノード間で転送されることから，1 秒当たりのファイル転送サイズは次のように求められる。

1,300 バイト×　60×2＝156,000 バイト／秒≒1.2M ビット／秒

したがって，10M ビット／秒の LAN の利用率は 12%となり，**エ**が正解。

●問 19　正解：エ

問題文に該当するのは SIP（Session Initiation Protocol）であり，**エ**が正解。

SIP は，IP 電話などでセッションの確立，変更，切断といった一連の操作を制御するためのプロトコルである。

●問 20　正解：ア

インターネット VPN を実現するために用いられる技術としては，IPsec（Internet Protocol Security）や SSL（Secure Socket Layer）が代表的だが，ESP，AH などのプロトコルを含むのは **IPsec** である。

AH は，主に通信データの認証（メッセージ認証）のために使用されるプロトコルであり，通信データを暗号化する機能はない。一方 **ESP** は，通信データの認証と暗号化の両方の機能を提供するプロトコルである。したがって**ア**が正解。

●問 21　正解：エ

ア　外部キーの値は，その関係の中で一意である必要はない。
イ　外部キーと参照先の関係の候補キーとは比較可能でなければならない。
ウ　参照元の外部キーの値は，参照先の関係に一致している候補キーが存在している必要がある。
エ　正しい記述である。

したがって**エ**が正解。

●問 22　正解：ウ

UML（Unified Modeling Language）とは，オブジェクト指向型のソフトウェア開発における分析・設計段階で，システムをモデル化する際の表記方法を統一したものである。問題文に該当するのはシーケンス図であり，オブジェクト間のメッセージ送受信による相互作用を時系列的に表すのに用いる。したがって**ウ**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，一つ又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もっている必要がある。したがって**ウ**が正解。

●問 24　正解：ウ

各案の総合評価点を計算すると次のようになる。

案 1：(3×4＋2×2＋5×3)－(2×8＋4×3)＝3

案 2：(4×4＋4×2＋4×3)－(4×8＋1×3)＝1

案 3：(5×4＋2×2＋2×3)－(1×8＋5×3) ＝7

案 4：(2×4＋5×2＋4×3)－(5×8＋1×3)＝－13

この結果より，総合評価点が最も高い改善案は案 3 であることがわかる。したがって**ウ**が正解。

●問 25　正解：イ

ア　1 年以内に実現できる改善だけでなく，中長期的な取組みを要する改善についても計画に盛り込む必要がある。

イ　適切な記述である。

ウ　情報システムの機能面に絞らず，パフォーマンスやセキュリティなど，非機能面の改善についても計画に盛り込む必要がある。

エ　重要度や緊急度が高いものについては，必要に応じて新たに予算を確保して改善を実施することも検討すべきである。

したがって**イ**が正解。