平成 26 年度 秋期 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：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（Certificate Revocation List）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２　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，次の三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')）異なる二つのデータ（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３　正解：ア

「**クラウドサービス利用のための情報セキュリティマネジメントガイドライン**」の「序文　0.1 一般」に，「クラウド利用者の視点から JIS Q 27002（実践のための規範）の各管理策を再考し，クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として，このガイドラインを作成した」とある。したがって**ア**が正解。

●問４　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，発行の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，SSL/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署名する。

●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：ウ

CSIRT（Computer Security Incident Response Team：「シーサート」と読む）とは，企業・公的機関（国レベルを含む）などの組織内に設置され，コンピュータセキュリティインシデントに対応する活動を行う組織の総称である。攻撃やインシデントに関する情報，脆弱性情報等を収集・分析し，対応方針や手順の策定などの活動を行う。したがって**ウ**が正解。

●問７　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 で用いる三つの基準は次のとおり。

・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８　正解：ア

CRYPTREC（Cryptography Research and Evaluation Committees）とは，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，「電子政府」における調達のための推奨すべき暗号のリスト（電子政府推奨暗号リスト）を公表している。したがって**ア**が正解。

イ　NISC（内閣官房情報セキュリティセンター）の説明である。
ウ　JIPDEC（一般財団法人日本情報経済社会推進協会）の説明である。
エ　JCMVP（暗号モジュール試験及び認証制度）の説明である。

●問９　正解：イ

DNS サーバには，大きく分けるとコンテンツ機能とキャッシュ機能という二つの機能があり，各々の機能を提供する DNS サーバを「コンテンツサーバ」「キャッシュサーバ」という。キャッシュサーバは，再帰的な問合せに対し，必要に応じて他の DNS サーバに問合せを行い，その結果を問合せ元に返す。

DNS キャッシュポイズニング攻撃は，キャッシュサーバからの名前解決要求に対し，正常な応答に加えて悪意あるサイトに誘導するための不正な名前解決情報も付加して返すことで，キャッシュに登録させる攻撃である。そのようにしてキャッシュが汚染されたキャッシュサーバを利用したユーザが悪意あるサイトに誘導され，機密情報が盗まれるなどの被害を受ける。

DNS キャッシュポイズニング攻撃を成功させるためには，攻撃者は，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（DNS のリクエストを一意に識別するための ID）を本来の応答レコードと合致させる必要があるため，これらを固定することは非常に危険である。

再帰的な問合せは内部ネットワークからのものだけにするなど，キャッシュサーバを利用可能な IP アドレスの範囲を制限することは DNS キャッシュポイズニング攻撃への有効な対策となる。

したがって**イ**が正解。

●問 10　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（公開鍵基盤）における鍵の登録，検証，失効などを Web サービス上で行うプロトコルである。
エ　**XML Signature**（XML 署名）は，XML 文書にディジタル署名を行う技術仕様であり，Enveloped 署名，Enveloping 署名，Detached 署名の三つがある。

●問 11　正解：エ

問題文に該当するのは SSH（Secure SHell）であり，**エ**が正解。

SSH は，当初は rlogin，rsh など BSD 系 UNIX を起源とする r 系のコマンドや，X11，Telnet などを安全に行うための手段として使用されていたが，現在では FTP，POP3 など，暗号化機能を備えていないプロトコルを安全に使用する技術として広く使用されている。

ア　**IPsec**（IP security protocol）は，IP パケットをインターネット層でカプセル化し，暗号化するプロトコルである。
イ　**L2TP**（Layer 2 Tunneling Protocol）は，その名のとおり第 2 層（OSI 参照モデルではデータリンク層）におけるトンネリングプロトコルである。
ウ　**RADIUS**（Remote Authentication Dial-In User Service）は，リモートアクセス環境において，認証情報やアカウンティング情報をやりとりするプロトコルである。

●問 12　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あてに送ることにより，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。

●問 13　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。

●問 14　正解：エ

フォレンジックス（フォレンジックともいう）とは，事件や事故の証拠を収集し，裁判で立証する行為を意味する。**ディジタルフォレンジックス**（コンピュータフォレンジックスともいう）とは，データの改ざんや不正アクセスなどコンピュータに関する犯罪の法的な証拠性を明らかにするために，原因究明に必要な機器やデータ，ログなどを保全したり，収集・分析したりすることである。したがって**エ**が正解

●問 15　正解：ア

DKIM は，送信側 SMTP サーバがメールヘッダに付与したディジタル署名を受信側 SMTP サーバで検証することにより，発信元の正当性を確認する仕組みである。そのため，あらかじめ送信側ドメインの DNS サーバに正当なメールサーバの公開鍵を登録しておく必要がある。したがって**ア**が正解。

イ　SMTP-AUTH の説明である。
ウ　SPF（Sender Policy Framework）の説明である。
エ　OP25B（Outbound Port25 Blocking）の説明である。

●問 16　正解：ウ

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。

EAP は，次に示すように様々な認証方式に対応している。

・EAP-TLS

サーバとクライアント間で，ディジタル証明書による相互認証を行う方式。認証成立後には，TLS のマスタシークレットをもとにクライアントごとに異なる暗号鍵を生成・配布し，定期的に変更するため，無線 LAN のセキュリティを高めることができる。

・EAP-TTLS（EAP Tunneled TLS）

ディジタル証明書によるサーバ認証を行って EAP トンネルを確立後，そのトンネル内で様々な方式を用いてクライアントを認証する。

・EAP-PEAP（Protected EAP）

認証の仕組みは EAP-TTLS とほぼ同じだが，クライアントの認証は EAP 準拠の方式に限られる。

・EAP-MD5
MD5 によるチャレンジレスポンス方式によってパスワードを暗号化し，クライアントの認証のみを行う。

上記より，認証にクライアント証明書を用いるプロトコルは EAP-TLS である。したがってウが正解。

●問 17　正解：ウ

サンドボックスとは，ネットワークを通じて外部から受け取ったプログラム等を，セキュリティが確保された領域で動作させることによって，プログラムの影響がシステム全体に及ばないようにする仕組みである。したがってウが正解。

ア　WAF（Web Application Firewall）の説明である。
イ　ハニーポットの説明である。
エ　バインド機構の説明である。

●問 18　正解：エ

DNSSEC（DNS Security Extensions）は，DNS のセキュリティ拡張方式であり，次のような機能によって応答レコードの正当性と完全性を検証する。

・名前解決要求に対して応答を返す DNS サーバが，自身の秘密鍵を用いて応答レコードにディジタル署名を付加して送信する
・応答を受け取った側は，応答を返した DNS サーバの公開鍵を用いてディジタル署名を検証する

したがってエが正解。

●問 19　正解：エ

問題文に該当するのは**RADIUS**（Remote Authentication Dial-In User Service）であり，エが正解。
RADIUS は，リモートアクセス環境において，利用者の認証情報やアカウンティング情報，課金情報等を管理し，利用者の認証と利用記録を一元的に行う。

ア　**CHAP**（Challenge Handshake Authentication Protocol）は，PPP のリンク確立後，チャレンジレスポンス方式で認証するプロトコルである。
イ　**PAP**（Password Authentication Protocol）は，CHAP とは異なり，ユーザ ID とパスワードをそのまま暗号化せずに送信して認証するプロトコルである。
ウ　**PPP**（Point to Point Tunneling Protocol）は，PPP パケットを IP でカプセル化してトンネリングするプロトコルである。

●問 20　正解：エ

RFC 5322「Internet Message Format」の「2.1. General Description」中に次の記述があるように，空行の前後でヘッダと本体を分ける。

The body is simply a sequence of characters that follows the header section and is separated from the header section by an empty line (i.e., a line with nothing preceding the CRLF).

＜訳＞
本体はヘッダセクションに続く単純な文字の連続であり，空行（CRLF の前の何もない行）でヘッダセクションと分離される。

したがって**エ**が正解。

●問 21　正解：イ

デッドロックとは，例えば，データ A にロックをかけてからデータ B にロックをかけようとしているトランザクションと，その逆にデータ B にロックをかけてからデータ A にロックをかけようとしているトランザクションが同時に実行された場合に，互いに必要なデータをロックし合っているため，待ち状態になってしまうことをいう。

ア　A はアンロックを待っていないため，A が資源を解放すれば，B → C → D の順に実行される。
イ　D のみがアンロックを待っていないが，D が資源を解放しても A は C のアンロック待ち，C は B のアンロック待ち，B は A のアンロック待ちとなっているため，デッドロックの状態となっている。
ウ　B, C, D はいずれもアンロックを待っていないため，B, C, D が資源を解放すれば A が実行される。
エ　C はアンロックを待っていないため, C が資源を開放すれば, A, B, D が実行される。

したがって**イ**が正解。

●問 22　正解：エ

上位モジュールの代わりにテスト対象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。一方，下位モジュールの代わりとなってテスト対象モジュールから呼び出されるのが**スタブ**である。したがって**エ**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：ウ

JIS Q 20000-1：2012「サービスマネジメントシステム要求事項」では，「3 用語及び定義」「3.10 インシデント」において，「サービスに対する計画外の中断，サービスの品質の低下，又は顧客へのサービスにまだ影響していない事象」と定義している。解答群の中でこれに該当するのは「**アプリケーションの応答の大幅な遅延**」である。したがって**ウ**が正解。

●問 25　正解：ア

情報セキュリティ管理基準によらずとも，雇用の終了をもって守秘責任が解消されてしまうのは組織の情報管理の観点からすると問題であり，指摘事項に該当するのは明白である。参考までに経済産業省発行の「情報セキュリティ管理基準（平成 20 年改正版）」を参照すると，「4 人的資源のセキュリティ」「4.1 雇用前」「4.1.3 従業員，契約相手及び第三者の利用者は，契約上の義務の一部として，情報セキュリティに関する，これらの者の責任及び組織の責任を記載した雇用契約書に同意し，署名する」において，次のような記述がある。

4.1.3.2 雇用条件には，取扱いに慎重を要する情報へのアクセスが与えられる，すべての従業員，契約相手及び第三者の利用者による，情報処理施設へのアクセスが与えられる前の，秘密保持契約書又は守秘義務契約書への署名を含める
4.1.3.7 雇用条件には，組織の構外及び通常の勤務時間外に及ぶ責任（例えば，在宅勤務における責任）を含める
4.1.3.8 雇用条件には，従業員，契約相手及び第三者の利用者が組織のセキュリティ要求事項に従わない場合に取る処置を含める
4.1.3.9 従業員，契約相手及び第三者の利用者が情報セキュリティに関する雇用条件に同意することを確実にする仕組みを整備する
4.1.3.11 雇用終了後も，定められた期間は雇用条件に含まれる責任を継続する

また，「4.3 雇用の終了又は変更」「4.3.1 雇用の終了又は変更の実施に対する責任は，明確に定め，割り当てる」において，次のような記述がある。

4.3.1.1 雇用の終了に関する責任の伝達事項には，実施中のセキュリティ要求事項及び法的責任並びに，適切ならば，従業員，契約相手及び第三者の利用者の，雇用終了以降の一定期間継続する，秘密保持契約及び雇用条件に規定された責任を含める
4.3.1.2 雇用終了後もなお有効な責任及び義務を，従業員，契約相手及び第三者の利用者の契約に含める

したがって**ア**が正解。