平成28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：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：ア

A 社ドメイン配下のランダムなサブドメイン名に関する大量の問合せを，第三者の DND キャッシュサーバに分散して送信した場合，当該 DNS キャッシュサーバのキャッシュには名前解決情報は登録されていないため，A 社ドメインの権威 DNS サーバに大量の問合せが集中し，サービス不能状態に陥る可能性がある。したがって**ア**が正解。

●問３　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４　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５　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６　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

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９　正解：ア

カウントの値と時刻データを入力値としており，(7)に「(4)の出力について，必要とする分の数を得るまで(2)～(6)を繰り返す」とある。このような処理を行って出力するのは擬似乱数である。したがってアが正解。

イ　ディジタル証明書は，発行の際に申請者の公開鍵に対して認証局（CA）の秘密鍵でディジタル署名を付与する。
ウ　ハッシュ値は，対象となるデータをハッシュ関数で演算して出力した固定長のビット列である。
エ　メッセージ認証コード（Message Authentication Code : MAC）は，通信データの改ざん有無を検知し，完全性を保証するために通信データから生成する固定長のコード（ビット列）である。MAC には，ブロック暗号を用いた CMAC（Cipher-based MAC），ハッシュ関数を用いた HMAC などがある。

●問 10　正解：イ

J-CSIP（Initiative for Cyber Security Information sharing Partnership of Japan）は，公的機関である IPA（情報処理推進機構）を情報ハブ（集約点）の役割として，参加組織間で情報共有を行い，高度なサイバー攻撃対策につなげていく取組みである。したがってイが

正解。

●問 11　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 12　正解：イ

DNS キャッシュポイズニング攻撃とは，DNS 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，当該 DNS サーバのキャッシュに（不正な名前解決情報を）登録させる攻撃である。

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），DNS ヘッダ内のトランザクション ID（DNS の問合せ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。そのため，これらを固定せずにランダムな値に変更することは有効な対策となる。したがって**イ**が正解。

●問 13　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 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

ア　ステガノグラフィの説明である。
イ　ペネトレーションテストの説明である。

ウ　ソーシャルエンジニアリングの説明である。

●問 15　正解：ア

ping は，ICMP（Internet Control Message Protocol）を用いて指定したコンピュータが接続可能であるかどうか等を確認するプログラムであるため，これに応答しないようにするためには ICMP を“通過禁止”に設定する必要がある。したがって**ア**が正解。

イ　FTP（File Transfer Protocol）が使用するポートである。
ウ　POP3（Post Office Protocol v3）が使用するポートである。
エ　NTP（Network Time Protocol）が使用するポートである。

●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，サーバ証明書，クライアント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-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。

・EAP-FAST（Flexible Authentication via Secure Tunneling）

Cisco Systems 社による認証プロトコルであり，EAP-TTLS とほぼ同様の方式でクライアントを認証するが，FAST ではディジタル証明書を用いず，DH（Diffie-Hellman）鍵交換によって TLS セッションを確立する方式も使用可能である。

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：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 18　正解：ウ

SSID（Service Set ID）とは，最長 32 オクテットのネットワーク識別子であり，無線 LAN アクセスポイントを識別するために用いられる。ESSID（Extended Service Set ID）とも呼ばれる。したがってウが正解。

●問 19　正解：イ

DHCP（Dynamic Host Configuration Protocol）は，ネットワークに接続されたコンピュータに対して，IP アドレス，サブネットマスク，DNS サーバアドレス，ゲートウェイアドレス等の必要な情報を動的に割り当てるプロトコルである。

DHCP クライアントと DHCP サーバ間でやり取りされるメッセージの順序は，次の通りである。

①DHCP DISCOVER

クライアントが DHCP サーバを見つけるために“DHCP DISCOVER”メッセージをブロードキャストで送信する。

②DHCP OFFER

“DHCP DISCOVER”メッセージを受け取った DHCP サーバが，割り当てる候補となる IP アドレス，サブネットマスク等の情報を“DHCP OFFER”メッセージで通知する。

③DHCP REQUEST

クライアントが，“DHCP OFFER”メッセージで通知された IP アドレスを正式に取得することを“DHCP REQUEST”メッセージで DHCP サーバに要求する。

④DHCP ACK

クライアントから要求のあった IP アドレスが割り当て可能であった場合には，DHCP サーバは確認応答として，“DHCP ACK”メッセージで IP アドレス，サブネットマスク等の情報を通知する。

したがって**イ**が正解。

●問 20　正解：エ

サブミッションポートは，迷惑メール対策として SMTP ポートの代わりに投稿専用のポートとして使用する。したがって**エ**が正解。

ボットなどが迷惑メールを送信する際に，ISP（Internet Services Provider）のメールサーバを経由せず，直接送信先のメールサーバの 25 番ポートに接続して SMTP コネクションを確立する手口が用いられたため，これを OP25B（Outbound Port25 Blocking）により遮断する対策が行われるようになった。

OP25B とは，ISP 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。

OP25B が設定されている環境で正当な利用者が自社のメールサーバなどと直接 SMTP コネクションを確立してメールを送信する必要がある場合には，25 番ポートではなくサブミッションポートを使用する必要がある。

サブミッションポートへアクセスしてきたユーザを SMTP-AUTH によって認証することで，ボットなどからの投稿を受け付けないようにするほか，TLS によって通信を秘匿化することも可能である（Submission over TLS）。

●問 21　正解：ア

ア～エの値を入力パラメタにセットすると，WHERE 句はそれぞれ次のようになる。

ア　WHERE ユーザ名 = '' OR '--' = '--';
イ　WHERE ユーザ名 = '' OR ユーザ名 = 'ユーザ名';
ウ　WHERE ユーザ名 = '-- OR 1 = 1';
エ　WHERE ユーザ名 = '¥' OR 1 = 1 ';--';

アは，"OR '--' = '--'"が常に真となるため，"アカウント"表の全ての行が取得される。
イは，ユーザ名が空か"ユーザ名"という文字列であることが条件となるため，どの行も取得されない。
ウは，"--"以降はコメントとなった結果，ユーザ名が空であることが条件となるため，どの行も取得されない。
エは，"¥"の後のシングルクォートがエスケープされ，"--"以降がコメントとなった結果，ユーザ名が"¥' OR 1 = 1 "という文字列であることが条件となるため，どの行も取得されない。

したがって**ア**が正解。

●問 22　正解：イ

フェールセーフとは，システムに何らかの障害が発生した場合に安全な方向に向かうように設計しておくことで，被害を最小限にする方法である。例えば，ファイアウォールに障害が発生した場合に，全てのパケットが通過できないようにするのはフェールセーフである。

ア　フールプルーフの考えに基づいた設計である。
イ　フェールセーフの考えに基づいた設計である。
ウ　フェールソフトの考えに基づいた設計である。
エ　フォールトトレランス（“フォールトトレラント”とも呼ばれる）の考えに基づいた設計である。

したがって**イ**が正解。

●問 23　正解：エ

ペアプログラミングとは，2 人のプログラマがペアとなり，相談やレビューを行うことで品質の向上や知識の共有を図る開発手法である。したがって**エ**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：イ

システム管理基準（平成 16 年 10 月 8 日策定）は，組織体が経営戦略に沿って情報システム戦略を立案し，その戦略に基づいた効果的な情報システム投資と，リスクを低減するためのコントロールを適切に整備・運用するための実践規範となるものである。
システム管理基準の前文に次の記述がある。

組織体が情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は，以下の通りである。
・情報システムが，組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが，組織体の目的を実現するように安全，有効かつ効率的に機能するため
・情報システムが，内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが，関連法令，契約又は内部規程等に準拠するようにするため

したがって**イ**が正解。