# 平成 27 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：ア**

**EV**（Extended Validation）**SSL 証明書**とは，CA と Web ブラウザベンダで構成する業界団体である「CA/Browser フォーラム」が定めた Web サーバ用のディジタル証明書である。従来のディジタル証明書よりも，発行に当たっての審査基準を厳しく設定しているため，EV 証明書を所有するサイトは通常の証明書を所有するサイトよりも信頼性が高いといえる。

**サブジェクトフィールド**は，認証の対象となる組織の情報が記載されるフィールドであり，Organizational Name には Web サイト運営団体の正確な名称が記載される。したがって**ア**が正解。

**●問２　正解：ウ**

**EAP-TLS** は，サーバとクライアント（サプリカント）間で，ディジタル証明書による相互認証を行う方式である。EAP は，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り，無線 LAN 環境のセキュリティを強化する技術として普及しているほか，有線 LAN においてもクライアントの正当性や安全性を認証する技術として用いられている。したがって**ウ**が正解。

**●問３　正解：エ**

**RLO** とは，ファイル名の文字の並びを右から左に向かって読むように変更する Unicode の制御文字であり，通常はアラビア語などを表記する際に使われる。これを悪用することで，ファイル名の拡張子を偽装する手口が知られている。

例.「議事録 exe.doc」
⇒　実際には「議事録[RLO]cod.exe」となっている。

したがって**エ**が正解。

**●問４　正解：ア**

**VA**（証明書有効性検証局）とは，次のような役割を担っているシステムや機関である。

・ディジタル証明書の失効情報の集中管理
・CA（Certification Authority：認証局）の公開鍵で署名を検証
・ディジタル証明書内に記載された有効期限の確認
・CRL（Certificate Revocation List）の確認
・ディジタル証明書の失効状態についての問合せへの応答

したがって**ア**が正解。

イ　CA の役割である。
ウ　AA（Attribute Authority：属性認証局）の役割である。
エ　RA（Registration Authority：登録局）の役割である。

**●問５　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６　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，当該証明書と破棄された日時の対応が提示される。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７　正解：ウ**

**CVE**（共通脆弱性識別子）は，その名が示すとおり，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８　正解：ウ**

**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。

電子政府推奨暗号リストとは，CRYPTREC によって安全性及び実装性能が確認された暗号技術のうち，市場における利用実績が十分であるか，今後の普及が見込まれると判断され，当該技術の利用を推奨するもののリストである。したがって**ウ**が正解。

**●問９　正解：ウ**

IPsec は，次のような特徴をもっている。

・IP パケットをインターネット層でカプセル化し，暗号化する方式である
・上位層のアプリケーションに依存せずに暗号化通信が可能であるため，ユーザは暗号化通信を行っていることを意識する必要がない

・IPv4，IPv6 のどちらでも利用することができ，IPv6 では IPsec の実装が必須である
・暗号化アルゴリズムを特定せず，DES，3DES など，様々な暗号化アルゴリズムを利用できるようになっている
・IPsec では，パケットを暗号化する対象部分によって，トランスポートモードとトンネルモードという二つの方式が提供されている
・トランスポートモードは，IP パケットのデータ部分のみを暗号化する方式である
・トンネルモードは，IP ヘッダとデータ部分をまとめてカプセル化して暗号化する方式である
・IPsec における鍵交換プロトコルとしては，ISAKMP/Oakley（ISAKMP：Internet Security Association and Key Management Protocol）方式を使った IKE（Internet Key Exchange）が標準となっており，ポート番号 500/UDP を使用する
・IPsec における代表的な通信プロトコルとして，AH（Authentication Header：認証ヘッダ）と ESP（Encapsulating Security Payload：暗号化ペイロード）がある
・AH は，主に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
・ESP は，メッセージ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**ウ**が正解。

**●問 10　正解：ア**

**NTP を使った増幅型の DDoS 攻撃**（「**NTP リフレクター攻撃**」と呼ばれる）では，NTP サーバが過去にやりとりした 600 件のアドレスを回答する「monlist」コマンド（状態確認機能）により，増幅率を数十倍から数百倍にまで高めるという手口が使われている。そのため，その後リリースされた NTP のサーバプログラムでは，このコマンドを脆弱であるとして無効にしている。したがって**ア**が正解。

**●問 11　正解：ア**

**ダークネット**とは，インターネット上で到達可能であり，かつ特定のホストに割り当てられていない（未使用）IP アドレス空間のことである。通常はダークネットに対してパケットが流れることはないが，マルウェアが感染対象を探査するパケットや，感染対象の脆弱性を攻撃するためのパケット，IP アドレスを詐称した DDoS 攻撃を被っているホストからの応答パケットなどが流れる。したがって**ア**が正解。

**●問 12　正解：エ**

**rootkit** とは，侵入に成功した攻撃者が，その後の不正な活動を行いやすくするために，自身の存在を隠ぺいすることを目的として使用するソフトウェアなどをまとめたパッケージの呼称（俗称）である。当初は，UNIX 系のシステムに侵入して root 権限を手に入れた侵入者が，システム管理者に見つかることなく，root 権限を保持して活動できるようにするためのツールのことであったが，現在では Windows など"root"というアカウントが存在

しない環境で同様な働きをするツールも rootkit と呼ばれている。したがってエが正解。

**●問 13　正解：エ**

**ベイジアンフィルタリング**（Bayesian Filtering）とは，ベイズの定理を応用することにより，迷惑メールの特徴を自己学習し，統計的に解析して判定するフィルタリング手法である。学習量の増加に伴い，フィルタリングの精度が向上する。したがってエが正解。

**●問 14　正解：ア**

**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権威 DNS サーバ（コンテンツサーバ）の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権威 DNS サーバが，自身の秘密鍵を用いて応答したリソース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，応答を返した権威 DNS サーバの公開鍵を用いてリソースレコードが改ざんされていないことを検証する

したがってアが正解。

**●問 15　正解：ア**

**DNS amp 攻撃**とは，DNS サーバ（キャッシュサーバ）に対し，発信元アドレスを攻撃のターゲットとなるホストのアドレスに詐称し，かつ応答メッセージのサイズが大きくなる（増幅される）クエリを送ることにより，その応答メッセージによってターゲットホストをサービス不能状態に陥らせる攻撃である。DNS リフレクション攻撃とも呼ばれる。DNS amp 攻撃の対策としては，DNS サーバをキャッシュサーバとコンテンツサーバに分離し，キャッシュサーバはインターネット側からのリクエストには応じないようにするのが有効である。したがってアが正解。

**●問 16　正解：イ**

**SMTP-AUTH**は，SMTP にユーザ認証機能を追加した方式であり，クライアントが SMTP サーバにアクセスしたときにユーザアカウントとパスワードによる利用者認証を行うことで，許可された利用者だけから電子メールの送信を受け付ける。したがってイが正解。

ア　OP25B（Outbound Port25 Blocking）の説明である。
ウ　POP before SMTP の説明である。
エ　SPF（Sender Policy Framework）の説明である。

**●問 17　正解：エ**

**SQL インジェクション**とは，ユーザの入力データをもとに SQL 文を編集してデータベ

ース（DB）に発行し，その結果を返す仕組みになっている Web ページにおいて，不正な SQL 文を入力することで DB を操作したり，DB に登録された個人情報等を不正に取得したりする攻撃手法である。SQL インジェクションへの対策には，次のようなものがある。

＜Web アプリケーションの実装における対策＞
・バインド機構（※）を利用する
・ユーザの入力データ中に含まれる，SQL 文として意味をもつ文字をエスケープ処理する

＜Web アプリケーションの実装以外の対策＞
・クライアントに送る Web サーバのエラーメッセージを必要最小限にする
・DB のアカウントがもつ DB アクセス権限を必要最小限にする
・Web アプリケーションファイアウォール（WAF）を導入する

※変数部分にプレースホルダと呼ばれる特殊文字（「?」など）を使用して SQL 文の雛形をあらかじめ用意しておき，後からそこに実際の値を割り当てて SQL 文を完成させる方法。

したがって**エ**が正解。

**●問 18　正解：ア**

**TCP ヘッダ**には，送信元ポート番号，宛先ポート番号，シーケンス番号，確認応答番号，ウィンドウサイズなどの情報が含まれる。したがって**ア**が正解。イ～エはいずれも IP ヘッダに含まれる情報である。

**●問 19　正解：ウ**

16 個のサブネットを使用するには，$2^4 = 16$ で，ネットワークアドレス部として第 4 オクテットの上位 4 ビットが必要であることから，サブネットマスクを 2 進数で表すと 11111111.11111111.11111111.11110000 となる。これを 10 進数で表記すると 255.255.255.240 となる。したがって**ウ**が正解。

**●問 20　正解：ウ**

**HTTP のヘッダ部**には，リクエスト／レスポンスの内容に応じた情報が入る。主なヘッダ情報として次のようなものがある。

・Authorization：認証方式や認証情報（リクエスト時）
・Referer：リンク元の URL 情報（リクエスト時）
・User-Agent：ブラウザの名称やバージョン情報（リクエスト時）
・Cookie：クライアントが Web サーバに提示するクッキー（リクエスト時）
・Content-Type：送信するファイルや文字セットの種類（リクエスト／レスポンス時）
・Server：Web サーバのプログラム名やバージョン情報（レスポンス時）

・Set-Cookie：Web サーバがクライアントにセットするクッキー（レスポンス時）
・Location：次に参照（リダイレクト）させる先の URI 情報（レスポンス時）

したがってウが正解。

**●問 21　正解：イ**

**2 相コミット**は，コミットを開始する一人の調停者と，複数の参加者によって行われる。まず，調停者が参加者全員に対してコミットの可否を問い合わせる。その結果，すべての参加者が了承した場合はコミットが成立し，調停者はコミットの決定を参加者に送る。一方，一つでも拒否があればコミットは成立せず，調停者はロールバックの決定を参加者に送る。調停者が参加者からの了承／拒否を受信後，決定内容（コミット／ロールバック）を参加者に送る前に障害が発生すると，その回復処理が終わらない限り，参加者全員がコミットもロールバックも行えない事態が起こる可能性がある。したがってイが正解。

**●問 22　正解：ウ**

**共通フレーム**は，ソフトウェアの企画から設計・開発・運用・保守・廃棄までのライフサイクルプロセス全般に対して，共通の物差し（フレーム）を規定することによって，ソフトウェアの取得者と供給者間の取引を明確化することを目的としている。

共通フレームによれば，システム要件の評価は，次の基準を考慮して行うこととされている。

(a) 取得ニーズへの追跡可能性
(b) 取得ニーズとの一貫性
(c) テスト計画性
(d) システム方式設計の実現可能性
(e) 運用及び保守の実現可能性

なお，ア，イ，エはいずれもシステム方式の評価における基準となる項目である。
したがってウが正解。

**●問 23　正解：エ**

**マッシュアップ**（Mashup）とは，既存の複数のサービスやコンテンツ等を組み合わせることで，新たなサービスを創出することである。例えば，API が公開された既存の複数の Web サービスを組み合わせることで，複合的な機能をもった新たな Web サービスを短期間で開発することなどが可能となる。したがってエが正解。

**●問 24　正解：ウ**

**データセンタにおけるコールドアイル**（cold aisle）とは，空調機からの冷気が通る部分のことである。通常データセンタでは，空調機からの冷気と IT 機器からの熱排気を分離す

るため，ラックの前面（吸気面）同士を向き合わせて配置する。このとき，ラックの前面同士に挟まれた冷気の通る部分がコールドアイルである。これに対し，ラックの IT 機器からの熱排気が通る部分をホットアイル（hot aisle）という。したがってウが正解。

**●問 25　正解：ウ**

入金管理システムから売掛金管理システムへのデータ受渡しの正確性及び網羅性を確保するには，入金額及び入金データ件数のコントロールトータルをチェックするのが有効である。これにより，入金データファイルのデータが重複や欠落なく処理され，入金額も一致していることを確認できる。したがってウが正解。

ア　ランツーランコントロール（R2R）とは，主に製造の分野において，入力データと出力結果のずれ等を認識し，補正を行っていくことで生産性や品質を高める手法である。

イ　売掛金管理システムのマスタ更新がいつの時点で行われたかを確認するための機能である。

エ　入金管理システムへの入力データの書式や内容，データの範囲等が妥当であるかを確認するコントロールである。