平成 25 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：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。RLO を利用してファイル名の拡張子を偽装することで,危険なファイルを安全な別な種類のファイルに見せかけて開かせる攻撃手口が知られている。したがって**エ**が正解。

●問２　正解：ア

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 ディジタル署名では,署名対象や署名アルゴリズム等を XML で記述する。また,署名の対象となる XML 文書全体だけでなく,文書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。したがって**ア**が正解。

イ　**エンベロープピング署名**は XML ディジタル署名の一つであり,対象となる XML 文書を署名の中に格納するため,複数の文書に対して一つの署名で済むのが特徴である。

ウ　**CMS** は一般的なディジタル署名で用いられている署名形式である。

エ　**ASN.1**（Abstract Syntax Notation One）は,データの構造や通信プロトコル等を記述する記法であり,CMS や S/MIME,SSL 等で用いられている。前述の通り,XML ディジタル署名では署名対象,署名アルゴリズム等を XML で記述する。

●問３　正解：イ

共通鍵暗号方式では,n 人の送受信者がそれぞれ秘密に暗号を使って通信を行うときに必要な鍵の数は次の式で求められる。

$${}_nC_2 = \frac{n(n-1)}{2}$$

したがって,100 人の場合には, $\frac{100\times99}{2}$ ＝ 4,950 個となり,**イ**が正解である。

なお,公開鍵暗号方式では,送受信者がそれぞれ秘密鍵と公開鍵の二つの鍵をもてばよいため,必要な鍵の数は,2n 個（100 人の場合には 200 個）となる。

●問４　正解：イ

WPA（Wi-Fi Protected Access）は無線 LAN のセキュリティを強化することを目的とした技術であり,無線 LAN の業界団体である Wi-Fi Alliance が 2002 年 10 月に発表した。**WPA2** は WPA の後継となる規格であり,Wi-Fi Alliance が 2004 年 9 月に発表した。WPA2 では暗号化アルゴリズムに **AES**（Advanced Encryption Standard）を採用した CCMP を使用する。したがって**イ**が正解。

●問５　正解：ウ

CVE（共通脆弱性識別子）は,その名が示す通り,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６　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,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。サイドチャネル攻撃の一種である**タイミング攻撃**は,暗号化や復号に要する時間の差異を精密に測定することにより,用いられている鍵を推測する手法である。したがって**ア**が正解。

●問７　正解：ア

テンペスト（Transient Electromagnetic Pulse Surveillance Technology：TEMPEST）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**ア**が正解。

テンペスト技術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,一般財団法人 VCCI 協会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,パソコン等を購入時の状態で使用していればテンペスト技術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８　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。

●問９　正解：ア

ブルートフォース攻撃とは,鍵や文字列として考えられるすべてのパターンを用いて暗号解読やパスワード破りを試みる攻撃手法である。総当たり攻撃とも呼ばれる。したがって**ア**が正解。

●問 10　正解：エ

"127.0.0.1"は,IPv4 においてローカルループバックアドレス,あるいは単にループバックアドレスと呼ばれ,そのホスト自身を指す特別な IP アドレスである。ループバックアドレスのホスト名には"localhost"が使われる。一方,IPv6 のループバックアドレスは"::1"（0:0:0:0:0:0:0:1）である。したがって**エ**が正解。

ア～ウのように,OS 提供元や PC 製造元,ウイルス定義ファイルの提供元等の FQDN に対応するアドレスが"127.0.0.1"として hosts ファイルに設定されていると,本来のサイトにアクセスできず,OS やウイルス定義ファイル等の更新が行われなくなってしまう。

●問 11　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 12　正解：ウ

SPF は,電子メールの送信元ドメインの DNS サーバにあらかじめ正当な SMTP サーバの IP アドレス（SPF レコード）を登録しておくことにより,送信元を詐称した電子メールを拒否する仕組みである。

電子メールを受信した SMTP サーバは,送信元の DNS サーバに問い合わせ,エンベロープ(SMTP プロトコルの MAIL FROM）のメールアドレスのドメインと送信サーバの IP アドレスの適合性を検証する。その結果,送信元の SMTP サーバの正当性が確認された場合のみメールを受け入れ,それ以外のメールは排除する。したがって**ウ**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

DNS amp 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 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 15　正解：ウ

SQL インジェクションとは,ユーザの入力データを元に 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。
・データベースのアカウントの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を導入する。

したがって**ウ**が正解。

●問 16　正解：エ

ディレクトリトラバーサル攻撃とは,ファイル名の入力を伴うアプリケーションに対して,ファイル名の先頭に“../”や“..¥”等を用いることにより,通常はアクセスできない不正なディレクトリにアクセスする攻撃手法である。対策としては,入力されたファイル名をチェックし,不正な文字列を取り除くことであるが,意図的にエンコードされた文字列が使われることなども多く,注意が必要である。したがって**エ**が正解。

●問 17　正解：ア

CSMA/CD(Carrier Sense Multiple Access with Collision Detection)**方式**とは,Ethernet に代表されるバス型ネットワークにおいて用いられているアクセス制御方式である。この方式では,ネットワークの利用率が高くなればなるほどパケット同士の衝突が発生する頻度が高くなるため,伝送待ち時間が増える傾向にある。一般に利用率が 20～30%に達すると衝突が増加し,

再送が繰り返されるため,伝送待ち時間が極端に長くなる。したがって**ア**が正解。

なお,**TDMA**（Time Division Multiple Access）**方式**とは,携帯端末などの無線通信において一つの周波数を短時間ずつ交代で複数の発信者で共有する方式である。

また,**トークンパッシング**とは,トークンと呼ばれる特殊なデータがネットワーク中を巡回し,送信を開始したいノードは,まずこのトークンを取得し,送信権を得てからデータを流す方式である。CSMA/CD のように衝突が発生しないため,トラフィックが増大しても伝送効率は低下しにくい。

●問 18　正解：エ

問題文は**リンクアグリゲーション**の説明である。したがって**エ**が正解。

ア　**スパニングツリー**とは,ループ状態になったネットワークにおいて,平常時は通信経路の一部をあえて使用不可状態にすることで,パケットが無限に循環するのを防止する技術である。平常時の経路に障害が発生した場合には,使用不可状態を自動的に解除して通信を再開する。

イ　**ブリッジ**はデータリンク層（第２層）でパケットの中継を行う装置である。

ウ　**マルチホーミング**とは,負荷分散や耐障害性の向上を目的として,複数の経路（ISP）を使ってインターネットなどの外部ネットワークに接続することである。

●問 19　正解：ア

問題文に該当するのは **IMAP4**（Internet Message Access Protocol）である。したがって**ア**が正解。

イ　**MIME**（Multipurpose Internet Mail Extension）は,電子メールで画像,音声,動画などのバイナリデータを扱うための拡張規格である。

ウ　**POP3**（Post Office Protocol）は,IMAP4 と同様に利用者端末がサーバから電子メールを受信するために使用するプロトコルであるが,選択したメールだけを利用者端末へ転送する機能や,サーバ上のメールを検索する機能などはない。

エ　**SMTP**（Simple Mail Transfer Protocol）は,電子メールを送信するために使用するプロトコルである。

●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：ウ

分散データベースシステムにおいては,データベースが分散されていることをユーザが意識することなく利用できる環境を提供する必要がある。これを**分散データベースシステムの透過性**という。透過性にはいくつかの要件があり,"分割に対する透過性"とは,一つの表が複数のサイトに分割して格納されていても,ユーザがそれを意識することなく利用できることである。したがって**ウ**が正解。

ア　**"移動に対する透過性"**の説明である。
イ　**"重複に対する透過性"**の説明である。
エ　**"位置に対する透過性"**の説明である。

●問 22　正解：ア

問題文に該当するのは**フールプルーフ**である。したがって**ア**が正解。

フールプルーフとは,不特定多数のユーザが操作しても誤動作などが起こりにくいように設計することである。

イ　**フェールセーフ**とは,システムに障害が発生した場合に,安全な方向に向かうように制御することである。
ウ　**フェールソフト**とは,システムに障害が発生した場合に,機能を縮退させて運用を継続することである。
エ　**フォールトトレラント**とは,機器を多重化することにより,高信頼性,高可用性を確保することである。

●問 23　正解：イ

要求が明確になっており,全機能を一斉に開発するのであれば,**ウォーターフォールモデル**が適している。

簡易なシステムを実装して動作を評価しながら要求を明確にし,その後全機能を一斉に開発するのは**プロトタイピングモデル**である。

最初に要求が確定した部分だけを開発し,その後に要求が確定した部分を逐次追加していくのは**進化的モデル**である。

したがって**イ**が正解。

●問 24　正解：ウ

IT サービスマネジメントの問題管理プロセスは,インシデントをはじめ,IT サービスにおける問題の根本原因を追究して解決するとともに,再発防止策を策定することを目的としている。インシデントにつながる可能性のある事象や予兆について管理し,問題の発生を未然に防ぐことも重要な役割である。

プロアクティブな活動とは,問題の発生に備え,事前に行う活動のことであるから,過去のインシデントの記録を分析し,今後起こりそうなインシデントを予測することがこれに該当する。

したがって**ウ**が正解。

●問 25　正解：イ

SaaS（Software as a Service）はクラウドコンピューティングの提供形態の一つであり,クラウドサービス事業者がアプリケーションを提供し,ユーザ企業は必要なアプリケーションを選択して利用する。SaaS の利用者環境からシステム監査人が評価できるのはアプリケーションの利用者 ID である。したがって**イ**が正解。