平成 27 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：ア

AES（Advanced Encryption Standard）は，DES（Data Encryption Standard）の後継として米国政府が採用したブロック暗号方式である。AES のブロック長は 128 ビットで，使用する鍵の長さは 128，192，256 ビットの中から選択することができる。段数（ラウンド数）は鍵長により，10 段，12 段，14 段となる。したがって**ア**が正解。

●問２　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**イ**が正解。

●問３　正解：エ

ステートフルインスペクションは，パケットフィルタリングを拡張した方式である。「ステートフル」とは，個々のセッションの状態を管理して，常にその情報に基づいてフィルタリングを行うという意味であり，受け付けたパケットをセッションの状態に照らし合わせて通過させるか遮断させるかを判断する。したがって**エ**が正解。

●問４　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５　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６　正解：ウ

ISO/IEC 15408 を評価基準とする**"IT セキュリティ評価及び認証制度"**は，IT 関連製品や

情報処理システムのセキュリティ品質を評価する。対象となるのは，OS，アプリケーションプログラムなどのソフトウェアをはじめ，通信機器，OA 機器，情報家電など，セキュリティ機能を備えた全ての IT 関連製品や，それらを組み合わせた一連の情報システムである。したがってウが正解。

●問７　正解：ウ

リスク回避とは，リスク発生の根本原因（作業，事象など）を排除することによってリスクを処理する方法である。例えば，インターネットからの不正アクセスを受けるリスクを処理するために，インターネットへの接続自体を取りやめることなどがリスク回避に該当する。問題文のア～エの中では，ウの内容がリスク回避に該当する。

ア　リスク低減に該当する。
イ　リスク移転に該当する。
エ　リスク受容に該当する。

●問８　正解：ウ

水飲み場型攻撃とは，攻撃者がターゲットとなる組織の従業員が日ごろ頻繁に利用している Web サイト（水飲み場）を改ざんして攻撃コードを埋め込むことで，同組織の従業員がアクセスしたときだけ攻撃を行い，マルウェアに感染させる手口である。したがってウが正解。

●問９　正解：ア

米国の組織犯罪研究者である Donald R.Cressey の「**不正のトライアングル**」理論によれば，不正行為は，「動機」「機会」「正当化」の三つがそろったときに発生すると考えられている。

ア　正しい記述である。
イ　内部統制の構成要素であり，“不正のトライアングル”とは無関係である。
ウ　“動機”の説明である。
エ　“正当化”の説明である。

したがってアが正解。

●問 10　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。

ア　HTTP GET Flood 攻撃（Connection Flood 攻撃の一種）の説明である。
ウ　SYN Flood 攻撃の説明である。
エ　Connection Flood 攻撃の説明である。

●問 11　正解：イ

VLAN は，スイッチに接続されたホストを幾つかのグループに分けることで仮想的に作り出された LAN である。物理的な接続にとらわれずに，スイッチの設定を変更することで自由自在にグループを作成することができるため，このように呼ばれている。

VLAN を構築すると，個々の VLAN は別個のネットワークとなるため，ブロードキャストパケットも送信されなくなる。これにより，アドレス情報の不要な流出のリスクを低減できる。したがって**イ**が正解。

●問 12　正解：エ

クロスサイトスクリプティング（Cross-Site Scripting：XSS）とは，ユーザ情報登録や問合せ受付の入力確認画面など，ユーザが入力したデータを元に，Web アプリケーションが動的に HTML を作成するページにおいて，入力データのチェックの不備を突いてクライアント環境で不正なスクリプトを実行させる攻撃手法である。XSS への対策としては，入力データを処理する Web アプリケーションにおいて，入力データに“<”，“>”，“&”などのメタキャラクタが存在した場合には，それらを無効にする処理（エスケープ処理）を行う必要がある。したがって**エ**が正解。

●問 13　正解：ウ

Cookie に Secure 属性をセットすると，HTTPS（HTTP over 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 14　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。

●問 15　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 16　正解：ア

PC に感染したダウンローダ型ウイルスは，インターネット上の悪意ある Web サイト等にアクセスし，他のウイルスをダウンロードする。これを防ぐ対策として有効なのは，URL フィルタを用いてインターネット上の不正 Web サイトへの接続を遮断することである。したがって**ア**が正解。

●問 17　正解：ウ

OAuth2.0 は，信頼関係にある複数のサービス間で，セキュアに認可情報をやり取りする仕組み（API）を提供する。

OAuth2.0 の API を提供しているサービスを「OAuth Server」と呼び，本問では Web サービス B が該当する。一方，OAuth Server が提供する API を利用するサービスを「OAuth Client」と呼び，本問では Web サービス A が該当する。また，認可情報を付与する利用者を「Resource Owner」と呼び，本問では利用者 C が該当する。

「Resource Owner」である利用者 C の承認の下，「OAuth Client」である Web サービス A がリソース D への限定的なアクセス権限を取得しようとする際には，「OAuth Server」である Web サービス B が，利用者 C を認証した上で Web サービス A に対してアクセストークンを発行する。したがって**ウ**が正解。

●問 18　正解：ア

DNS の MX（Mail Exchange）**レコード**には，当該 DNS サーバが管理するドメイン（ゾーン）への電子メールを受け付けるサーバの名前が登録されている。したがって**ア**が正解。

●問 19　正解：エ

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，パケットが無限に循環（ループ）するのを防止する技術である。ネットワークを構成する複数のブリッジ間で BPDU（Bridge Protocol Data Unit）と呼ばれる制御情報を交換し合うことで，平常時に使用するルート（通信経路）を決定するとともに，一部の通信ポートをあえて使用不可状態にすることで，パケットがループするのを防ぐ。また，平常時のルートに障害が発生した場合には迂回ルートを決定し，通信を再開する。したがって**エ**が正解。

●問 20　正解：エ

TFTP（Trivial File Transfer Protocol）は，ユーザ認証機能のない簡易な FTP であり，UDP を用いる。したがって**エ**が正解。

●問 21　正解：イ

問題文に該当するのはデータクレンジングであり，**イ**が正解。

データクレンジングにより，業務システムごとに異なっているデータの属性や形式，コード体系等を統一し，データウェアハウスを構築する。

●問 22　正解：エ

ソフトウェア開発における**リポジトリ**（倉庫，貯蔵庫）とは，仕様書やプログラム，テスト結果など，ソフトウェア開発や保守に関する各種の成果物を格納し，一元管理するデータベースのことをいう。成果物を一元管理することによって，開発・保守の作業効率を高めることができる。したがって**エ**が正解。

●問 23　正解：ア

特許法では，他者が特許を出願するより前に同一の内容の発明を独自に発明し，実施していた，もしくは実施の準備をしていたと認められる者に対しては，「先使用による通常実施権（先使用権）」として，その実施が認められている。したがって**ア**が正解。

イ　組込み機器であることによる特別な制限等はなく，ソフトウェアも特許権で保護される。

ウ　特許権を取得した後であっても，無効審査請求によって無効となる場合がある。

エ　独自開発した技術であっても，先行特許と同一の技術であれば特許権の侵害になる。

●問 24　正解：ア

ア　正しい記述である。

イ　情報システム部門だけで判断するのではなく，出力帳票を利用している部門に確認した上で判断する必要がある。

ウ　情報システム部門だけで判断するのではなく，入力伝票等を起票した部門に確認した上で判断する必要がある。

エ　データ入力処理で誤りがあった場合等に備えて保存しておく必要がある。

●問 25　正解：ア

監査証拠とは，監査人が収集又は作成し，監査報告書において指摘事項又は指摘しないことの根拠として評価した資料のことである。したがって**ア**が正解。