平成 30 年度 春期 情報処理安全確保支援士

＜午前Ⅱ解答・解説＞

●問 1　正解：ア

CVSS v3 の基本評価基準（Base Metrics）は，脆弱性そのものの特性を評価する基準であり，機密性，完全性，可用性に対する影響を，どこから攻撃が可能かといった攻撃元区分や，攻撃する際に必要な特権レベルなどの基準で評価する。したがって**ア**が正解。

●問 2　正解：イ

HTTP リクエストヘッダの「?user=;cat /etc/passwd」で，OS コマンドである「cat」を用いて「/etc/passwd」ファイルを表示しようとしていることから，攻撃者が悪用しようとしている脆弱性は OS コマンドインジェクションである。したがって**イ**が正解。

●問 3　正解：ア

XML 署名（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。XML 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（オブジェクト）全体だけでなく，オブジェクト中の指定した任意のエレメントに対してデタッチ署名することができる。したがって**ア**が正解。

●問 4　正解：ア

エクスプロイトコード（exploit code）は攻撃コードとも呼ばれ，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コードである。エクスプロイトコードは脆弱性の検証にも用いられる。したがって**ア**が正解。

●問 5　正解：エ

シングルサインオン（SSO）とは，認証を必要とする複数のシステムが存在する場合に，最初に 1 回認証に成功すれば，以降は利用するシステムが変わっても，認証プロセスを経ることなくそのまま利用できるようにする認証システムである。

ア　cookie を生成するのはサーバである。
イ　cookie の制約上，認証対象の各サーバを同一のドメインに配置する必要がある。
ウ　リバースプロキシを使った SSO については，認証対象の各サーバを配置するドメインに制約はない。
エ　正しい記述である。

●問 6　正解：ウ

ダイナミックパケットフィルタリング型のファイアウォールでは，最初にコネクションを確立する方向のみを意識した基本的なACLを事前に登録しておき,実際に接続要求(TCPであればSYNパケット）があると，個々の通信をセッション管理テーブルに登録するとともに必要なルールが動的に生成され，フィルタリング処理を行う。

セッション管理テーブルにより，通過したパケットの応答や，それに付随するコネクションなどを総合的に管理し，自動的に必要な処理を行う。セッションが終了すると，動的に生成したルールは破棄される。

従来のスタティックパケットフィルタリング型のファイアウォールでは，上りも下りも別個の通信としかとらえられなかったため，不正アクセスによって順序の矛盾したパケットが送られてきたとしても，該当する条件が ACL に登録されてさえいれば中継していた。一方，ダイナミックパケットフィルタリング型では，過去の通信の状態が記録されており，それと矛盾するパケットは不正パケットとして遮断することができる。したがって**ウ**が正解。

●問 7　正解：エ

ディジタル署名は，発信者（文書作成者）が，自分の秘密鍵を用いて文書のハッシュ値を暗号化してディジタル署名を生成し，元の文書とともに送信する。受信者は，発信者の公開鍵を用いてディジタル署名を復号するとともに，送られてきた文書のハッシュ値を求め，両者を比較することによって，発信者の正当性と文書が送信途中で改ざんされていないことを確認する。したがって**エ**が正解。

●問 8　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 9　正解：イ

バイオメトリクス（Biometrics : 生体情報）による認証として，指紋・掌紋・顔型・虹彩・声紋・筆跡等がある。いずれも経年変化が少ないことが特徴だが，特に成人の虹彩は経年変化がなく，認証デバイスでのパターン更新がほとんど不要である。したがって**イ**が正解。

●問 10　正解：エ

J-CSIP（Initiative for Cyber Security Information sharing Partnership of Japan）は，公的機関である IPA を情報ハブの役割として，参加組織間で検知された標的型サイバー攻撃等の情報共有を行うことで，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**エ**が正解。

●問 11　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。

ア　expires を指定したときの動作である。
イ　HttpOnly 属性を付けたときの動作である。
エ　path を指定したときの動作である。

●問 12　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 13　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 14　正解：イ

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**イ**が正解。

●問 15　正解：ア

ルートキットとは，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ルートキットと呼ばれている。したがって**ア**が正解。

●問 16　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 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。

ア　OS コマンドインジェクション対策である。
イ　セッションハイジャック対策である。
ウ　ディレクトリトラバーサル対策である。

●問 18　正解：ア

IP ヘッダのプロトコル番号は上位層のプロトコルを識別するための番号であり，IANA（Internet Assigned Numbers Authority）が管理している。ICMP メッセージのプロトコル番号は 1 であり，これにより IP パケットで送られているデータが ICMP メッセージであることを識別できる。したがって**ア**が正解。

●問 19　正解：ウ

IEEE 802.1Q はタグ VLAN の規格である。IEEE 802.1Q を有したスイッチにおいて，複数の VLAN に所属しているポートをトランクポートと呼ぶ。したがって**ウ**が正解。

●問 20　正解：イ

WebDAV（Web Distributed Authoring and Versioning）は，HTTP1.1 を拡張したプロトコルであり，ブラウザから Web サーバにファイルをアップロードしたり，ファイルのバージョン管理を行ったりすることなどができる。したがって**イ**が正解。

●問 21　正解：エ

システム障害発生時にデータベースの整合性を保ち，かつ最新のデータベース状態に復旧するためには，ログファイルへのコミット情報書込みが完了している必要がある。この仕組みは WAL（Write Ahead Log：ログ先行書込み）プロトコルと呼ばれる手法によって実現されている。WAL プロトコルにより，コミット済みであるが，システム障害等何らかの理由によりデータベースに書き込まれていない更新データをログファイルから回復することが可能となる。したがって**エ**が正解。

●問 22　正解：ウ

UML（Unified Modeling Language）とは，オブジェクト指向型のソフトウェア開発における分析・設計段階で，システムをモデル化する際の表記方法を統一したものである。UML では目的に応じて次のようなモデル図が用いられる。

オブジェクト図	：オブジェクト間の関係を表す。
クラス図	：クラス間の関係を表す。
コンポーネント図	：コンポーネント間の構造や依存関係を表す。
シーケンス図	：オブジェクト間のメッセージ送受信による相互作用を時系列的に表す。
ステートチャート図	：オブジェクトの状態遷移を表す。
ユースケース図	：ユーザなどシステムの外のオブジェクト（アクター）とシステムの相互作用を表す。

したがって**ウ**が正解。

●問 23　正解：エ

エクストリームプログラミング（XP:eXtreme Programming）とは，Kent Beck 氏らが考案・提唱しているソフトウェア開発手法であり，「アジャイルソフトウェア開発手法」と総称される，ソフトウェアを迅速かつ柔軟に開発する一連の手法を代表するものである。XP における"テスト駆動開発"では，プログラムを書く前にテストケースを作成する。したがって**エ**が正解。

●問 24　正解：ウ

4 月 1 日 0 時から 6 月 30 日 24 時までのサービス提供時間は次のようになる。

24h×30 日 ＋ 24h×31 日 ＋ 24h×30 日 ＝ 2,184h

ここからシステムバージョンアップ作業に伴う停止時間の 84 時間を除く。

2,184－84 ＝ 2,100h

ハードウェア故障によるシステム停止時間は 10 時間であるため，実際のサービス時間は 2,090 時間であり，可用性は次のようになる。

$$\frac{2{,}090}{2{,}100} \fallingdotseq 0.99523 = 99.52\%$$

したがって**ウ**が正解。

●問 25　正解：ア

更新ログを加工し，アプリケーションの機能を経由した正常な処理によるログとして残していたとすれば，ログの改ざん行為であり，重大な指摘事項に該当する。したがって**ア**が正解。