平成28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

RADIUS（Remote Authentication Dial-In User Service）やその後継となる DIAMETER は，認証（Authentication），認可（Authorization），課金（Accounting）を行うプロトコルである。したがって**ア**が正解。

なお，"diameter"（直径）は，単語の"radius"（半径）から付けられた名称である。

●問２　正解：エ

NTP リフレクション攻撃とは，NTP を使った増幅型の DDoS 攻撃であり，NTP サーバが過去にやり取りした 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。したがって**エ**が正解。

●問３　正解：イ

POODLE（Padding Oracle On Downgraded Legacy Encryption）は，その名の通り，パディング処理の不備を突いて暗号化通信を解読する攻撃である。したがってイが正解。

●問４　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５　正解：エ

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**エ**が正解。

●問６　正解：ウ

リスクベース認証とは，送信元 IP アドレスなど利用者の環境を分析し，普段とは異なるネットワークからのアクセスであった場合に，追加で利用者に関する登録情報を入力させて認証を行うことである。したがって**ウ**が正解。

●問７　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８　正解：ア

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。したがって**ア**が正解。

イ　NISC（内閣官房情報セキュリティセンター）の説明である。
ウ　JIPDEC（一般財団法人日本情報経済社会推進協会）の説明である。
エ　JCMVP（暗号モジュール試験及び認証制度）の説明である。

●問９　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 10　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。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ため，鍵の違いによって演算の処理時間に差異が生じないようにすることが対策となる。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：ア

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**ア**が正解。

●問 13　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 14　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-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 15　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 16　正解：ウ

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**ウ**が正解。

ア　OP25B（Outbound Port25 Blocking）の説明である。
イ　SPF（Sender Policy Framework）の説明である。
エ　POP before SMTP 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 文として意味を持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 のアカウントが持つ 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

ア　正しい記述である。
イ　ゾーン転送とは，プライマリ DNS サーバとセカンダリ DNS サーバが登録内容を同期させるため，定期的に行う通信である。
ウ　ドメイン名に対応する IP アドレスを求めることを正引きという。
エ　CNAME はホスト名の別名を指定する資源レコードであり，ドメイン名を管理する

DNS サーバを指定する資源レコードは NS である。

したがって**ア**が正解。

●問 19　正解：ア

TCP の 3 ウェイハンドシェイクとは，「3 ウェイ」の名が示すように，次の①～③の 3 回のパケット送信によってコネクションを確立する方式である。

① SYN（要求元が送信）
② SYN+ACK（要求先が送信）
③ ACK（要求元が送信）

したがって**ア**が正解。

●問 20　正解：ウ

ア　TCP は OSI 基本参照モデルのトランスポート層の機能である
イ　ウィンドウ制御の単位はバイトである。
ウ　正しい記述である。
エ　TCP ヘッダにはデータの順序を示すシーケンス番号があり，それによって正しい順序で受信データを処理できる。

したがって**ウ**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メン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

システム方式設計では，複数のシステム間における処理やデータの流れ，連携方法などの仕様等を決定し，システム結合テストにおける要求事項が定義される。

ソフトウェア方式設計では，システムで使用するソフトウェア間のインタフェース，連携方法などの仕様等を決定し，ソフトウェア結合テストにおける要求事項が定義される。

ソフトウェア詳細設計では，個々のソフトウェアの機能の詳細仕様を決定し，ユニットテスト（単体テスト）における要求事項が定義される。

したがって**ウ**が正解。

●問 23　正解：イ

最初にコアな部分を開発し，順次機能を追加していくのであれば，**段階的モデル**（インクリメンタルモデル）が適している。段階的モデルでは，最初にシステム全体の要件定義を行い，要求された機能をいくつかに分割して段階的にリリースする。

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。

要求に不明確な部分がある場合には，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**進化的モデル**が適している。

したがって**イ**が正解。

●問 24　正解：ア

JIS Q 20000-1：2012「サービスマネジメントシステム要求事項」では，「3 用語及び定義」-「3.10 インシデント」において「サービスに対する計画外の中断，サービスの品質の低下，又は顧客へのサービスにまだ影響していない事象」と定義している。解答群の中でこれに該当するのは「IT サービス応答時間の大幅な超過」である。したがって**ア**が正解。

●問 25　正解：エ

システム管理基準は，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「Ⅳ．運用業務」「４．データ管理」において，「データへのアクセスコントロール及びモニタリングは，有効に機能すること。」「データの利用状況を記録し，定期的に分析すること」などの記述がある。

データベースに対する不正アクセスの防止・発見を目的としたアクセスコントロールについてシステム管理基準への準拠性を確認する監査手続としては，利用者のデータベースに対するアクセス記録を出力し，内容を調査することが適切である。したがって**エ**が正解。