

問1 DNSSEC (DNS Security Extensions) の機能はどれか。

- ア DNS キャッシュサーバの設定によって再帰的な問合せの受付範囲が最大限になるように拡張する。
- イ DNS サーバから受け取るリソースレコードに対するデジタル署名を利用して、リソースレコードの送信者の正当性とデータの完全性を検証する。
- ウ ISP などのセカンダリ DNS サーバを利用して DNS コンテンツサーバを二重化することで名前解決の可用性を高める。
- エ 共通鍵暗号技術とハッシュ関数を利用したセキュアな方法で、DNS 更新要求が許可されているエンドポイントを特定し認証する。

問2 セキュアハッシュ関数 SHA-256 を用いて、32 ビット、256 ビット、2,048 ビットの三つの長さのメッセージからハッシュ値を求めたとき、それぞれのメッセージのハッシュ値の長さはどれか。

単位 ビット

メッセージの長さ	32	256	2,048
ア	32	256	256
イ	32	256	2,048
ウ	256	256	256
エ	256	256	2,048

問3 A社のWebサーバは、認証局で生成したWebサーバ用のデジタル証明書を使ってSSL/TLS通信を行っている。PCがA社のWebサーバにSSL/TLSを用いてアクセスしたときにPCが行う処理のうち、サーバのデジタル証明書を手に入れた後に、認証局の公開鍵を利用して行うものはどれか。

- ア 暗号化通信に利用する共通鍵を生成し、認証局の公開鍵を使って暗号化する。
- イ 暗号化通信に利用する共通鍵を認証局の公開鍵を使って復号する。
- ウ デジタル証明書の正当性を認証局の公開鍵を使って検証する。
- エ 利用者が入力して送付する秘匿データを認証局の公開鍵を使って暗号化する。

問4 SSLを使用して通信を暗号化する場合、SSL-VPN装置に必要な条件はどれか。

- ア SSL-VPN装置は、FQDN又はIPアドレスを含むデジタル証明書を組み込む必要がある。
- イ SSL-VPN装置は、装置メーカーが用意した機種固有のデジタル証明書を組み込む必要がある。
- ウ SSL-VPN装置は、装置メーカーから提供される認証局を利用する必要がある。
- エ 同一ドメイン内で複数拠点にSSL.VPN装置を設置する場合は、同一のデジタル

証明書を利用する必要がある。

問5 ISP “A” 管理下のネットワークから別の ISP “B” 管理下の宛先へ SMTP で電子メールを送信する。電子メール送信者が SMTP-AUTH を利用していない場合、スパムメール対策 OP25B によって遮断される電子メールはどれか。

- ア ISP “A” 管理下の固定 IP アドレスから送信されたが、受信者の承諾を得ていない広告の電子メール
- イ ISP “A” 管理下の固定 IP アドレスから送信されたが、送信元 IP アドレスが DNS で逆引きできなかった電子メール
- ウ ISP “A” 管理下の動的 IP アドレスから ISP “A” のメールサーバを経由して送信された電子メール
- エ ISP “A” 管理下の動的 IP アドレスから ISP “A” のメールサーバを経由せずに送信された電子メール

問6 100 人の送受信者が共通鍵暗号方式で、それぞれが相互に暗号化通信を行うときに必要な共通鍵の総数は幾つか。

- ア 200
- イ 4,950
- ウ 9,900
- エ 10,000

問7 IP アドレスに対する MAC アドレスの不正な対応関係を作り出す攻撃はどれか。

- ア ARP スプーフィング攻撃
- イ DNS キャッシュポイズニング攻撃
- ウ URL エンコーディング攻撃
- エ バッファオーバーフロー攻撃

問8 DNS サーバに格納されるネットワーク情報のうち、第三者に公開する必要のない情報が攻撃に利用されることを防止するための、プライマリ DNS サーバの設定はどれか。

- ア SOA レコードのシリアル番号を更新する。
- イ 外部の DNS サーバにリソースレコードがキャッシュされる時間を短く設定する。
- ウ ゾーン転送を許可する DNS サーバを限定する。
- エ ラウンドロビン設定を行う。

問9 サービス不能攻撃 (DoS) の一つである Smurf 攻撃の特徴はどれか。

- ア ICMP の応答パケットを大量に発生させる。
- イ TCP 接続要求である SYN パケットを大量に送信する。
- ウ サイズの大きい UDP パケットを大量に送信する。

エ サイズの大きい電子メールや大量の電子メールを送信する。

問 10 表に示すテーブル X, Y へのアクセス要件に関して, JIS Q 27001:2006 (ISO/IEC 27001:2005) が示す“完全性”の観点からセキュリティを脅かすおそれのあるアクセス権付与はどれか。

- ア GRANT INSERT ON Y TO A イ GRANT INSERT ON Y TO B
ウ GRANT SELECT ON X TO A エ GRANT SELECT ON X TO B

問 11 テンペスト (TEMPEST) 攻撃を説明したものはどれか。

- ア 故意に暗号化演算を誤動作させて正しい処理結果との差異を解析する。
イ 処理時間の差異を計測し解析する。
ウ 処理中に機器から放射される電磁波を観測し解析する。
エ チップ内の信号線などに探針を直接当て, 処理中のデータを観測し解析する。

問 12 ダウンローダ型ウイルスが PC に侵入した場合に, インターネット経路で他のウイルスがダウンロードされることを防ぐ対策のうち, 最も有効なものはどれか。

- ア 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。
イ インターネットから内部ネットワークに向けた要求パケットによる不正侵入行為を IPS で破棄する。
ウ スпамメール対策サーバでインターネットからのスパムメールを拒否する。
エ メールフィルタで他サイトへの不正メール発信を遮断する。

問 13 ルートキット (rootkit) を説明したものはどれか。

- ア OS の中核であるカーネル部分の脆弱性を分析するツール
イ コンピュータがウイルスやワームに感染していないことをチェックするツール
ウ コンピュータやルータのアクセス可能な通信ポートを外部から調査するツール
エ 不正侵入して OS などに不正に組み込んだものを隠蔽する機能をまとめたツール

問 14 スпамメールの対策である DKIM (DomainKeys Identified Mail) の説明はどれか。

- ア 送信側メールサーバでデジタル署名を電子メールのヘッダに付与して, 受信側メールサーバで検証する。
イ 送信側メールサーバで利用者が認証されたとき, 電子メールの送信が許可される。
ウ 電子メールのヘッダや配送経路の情報から得られる送信元情報を用いて, メール送信元の IP アドレスを検証する。

エ ネットワーク機器で、内部ネットワークから外部のメールサーバの TCP ポート 25 番への直接の通信を禁止する。

問 15 IPsec の AH に関する説明のうち、適切なものはどれか。

- ア IP 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、トンネルモードの方式がある。
- イ 暗号化アルゴリズムや暗号化鍵のライフタイムが設定される管理テーブルで、期間を過ぎると新しいデータに更新される。
- ウ 暗号化アルゴリズムを決定し、暗号化鍵を動的に生成する鍵交換プロトコルで、暗号化通信を行う。
- エ データの暗号化は行わず、SPI、シーケンス番号、認証データを用い、完全性の確保と認証を行う。

問 16 Web アプリケーションの脆弱性を悪用する攻撃手法のうち、Per1 の system 関数や PHP の exec 関数など外部プログラムの呼出しを可能にするための関数を利用し、不正にシェルスクリプトや実行形式のファイルを実行させるものはどれに分類されるか。

- ア HTTP ヘッダインジェクション
- イ OS コマンドインジェクション
- ウ クロスサイトリクエストフォージェリ
- エ セッションハイジャック

問 17 DNS の MX レコードで指定するものはどれか。

- ア エラーが発生したときの通知先のメールアドレス
- イ 送信先ドメインのメールサーバ
- ウ 複数の DNS サーバが動作しているときのマスク DNS サーバ
- エ メーリングリストを管理しているサーバ

問 18 コンピュータとスイッチングハブの間、又は 2 台のスイッチングハブの間を接続する複数の物理回線を論理的に 1 本の回線に束ねる技術はどれか。

- ア スパニングツリー
- イ ブリッジ
- ウ マルチホーミング
- エ リンクアグリゲーション

問 19 電源オフ時に IP アドレスを保持することができない装置が、電源オン時に自装置の MAC アドレスから自装置に割り当てられている IP アドレスを知るために用いるデータリンク層のプロトコルで、ブロードキャストを利用するものはどれか。

ア ARP

イ DHCP

ウ DNS

エ RARP

問 20 TCP ヘッダに含まれる情報はどれか。

ア 宛先ポート番号

イ パケット生存時間 (TTL)

ウ 発信元 IP アドレス

エ プロトコル番号

問 21 次数が n の関係 R には、属性なし (ϕ) も含めて異なる射影は幾つあるか。

ア n

イ $2n$

ウ n^2

エ 2^n

問 22 バグ埋込み法において、埋め込まれたバグ数を S 、埋め込まれたバグのうち発見されたバグ数を m 、埋め込まれたバグを含まないテスト開始前の潜在バグ数を T 、発見された総バグ数を n としたとき、 S 、 T 、 m 、 n の関係を表す式はどれか。

ア $\frac{m}{S} = \frac{n-m}{T}$

イ $\frac{m}{S} = \frac{T}{n-m}$

ウ $\frac{m}{S} = \frac{n}{T}$

エ $\frac{m}{S} = \frac{T}{n}$

問 23 ソフトウェア開発組織の活動状態のうち、CMMI モデルにおける成熟度レベルが最も高いものはどれか。

ア 作業成果物の状況が、主要なタスクの完了時点で管理層に対して見える状態になっている。

イ 実績が定量的に把握されており、プロセスが組織的に管理されている。

ウ プロセスが明文化されて、組織内の全ての人がそれを利用している。

エ プロセスを継続的に改善していくための仕組みが機能している。

問 24 情報システムの設計において、フェールソフトが講じられているのはどれか。

ア UPS 装置を設置することで、停電時に手順どおりにシステムを停止できるようにし、データを保全する。

イ 制御プログラムの障害時に、システムの暴走を避け、安全に運転を停止できるようにする。

ウ ハードウェアの障害時に、パフォーマンスは低下するが、構成を縮小して運転を続けられるようにする。

エ 利用者の誤操作や誤入力を未然に防ぐことで、システムの誤動作を防止できるようにする。

問 25 ISMS におけるリスク分析手法の一つである“詳細リスク分析”で行う作業はどれか。

- ア 情報セキュリティポリシーの作成
- イ セーフガードの選択
- ウ リスクの評価
- エ リスクの容認

午前Ⅱ試験

問番号	正解
問 1	イ
問 2	ウ
問 3	ウ
問 4	ア
問 5	エ
問 6	イ
問 7	ア
問 8	ウ
問 9	ア
問 10	ア

問番号	正解
問 11	ウ
問 12	ア
問 13	エ
問 14	ア
問 15	エ
問 16	イ
問 17	イ
問 18	エ
問 19	エ
問 20	ア

問番号	正解
問 21	エ
問 22	ア
問 23	エ
問 24	ウ
問 25	ウ