Chapter13 セキュリティ

13-1 ネットワークに潜む脅威

問１　ＪＩＳ Ｑ ２７００１では，情報セキュリティは三つの特性を維持するものとして特徴付けられている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。

ア　安全性　　イ　可用性　　ウ　効率性　　エ　保守性

問２　ＩＳＭＳ適合性評価制度の説明はどれか。

ア　ＩＳＯ/ＩＥＣ １５４０８に基づき，ＩＴ関連製品のセキュリティ機能の適切性・確実性を評価する。
イ　ＪＩＳ Ｑ １５００１に基づき，個人情報について適切な保護措置を講じる体制を整備している事業者などを認定する。
ウ　ＪＩＳ Ｑ ２７００１に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する。
エ　電子政府推奨暗号リストに基づき，暗号モジュールが適切に保護されていることを認証する。

問３　ＩＳＭＳにおいて定義することが求められている情報セキュリティ基本方針に関する記述のうち，適切なものはどれか。

ア　重要な基本方針を定めた機密文書であり，社内の関係者以外の目に触れないようにする。
イ　情報セキュリティの基本方針を述べたものであり，ビジネス環境や技術が変化しても変更してはならない。
ウ　情報セキュリティのための経営陣の方向性及び支持を規定する。
エ　特定のシステムについてリスク分析を行い，そのセキュリティ対策とシステム運用の詳細を記述する。

問４　リスクアセスメントに関する記述のうち，適切なものはどれか。

ア　以前に洗い出された全てのリスクへの対応が完了する前に，リスクアセスメントを実施することは避ける。
イ　将来の損失を防ぐことがリスクアセスメントの目的なので，過去のリスクアセスメントで利用されたデータを参照することは避ける。
ウ　損失額と発生確率の予測に基づくリスクの大きさに従うなどの方法で，対応の優先順位を付ける。
エ　リスクアセスメントはリスクが顕在化してから実施し，損失額に応じて対応の予算を決定する。

問５　リスクが顕在化しても，その影響が小さいと想定されるので，損害の負担を受容するリスク対応はどれか。

ア　リスク移転　　イ　リスク回避　　ウ　リスク低減　　エ　リスク保有

問 6　リスク共有（リスク移転）に該当するものはどれか。

ア　損失の発生率を低下させること　　イ　保険への加入などで，他者との間でリスクを分散すること
ウ　リスクの原因を除去すること　　エ　リスクを扱いやすい単位に分解するか集約すること

問 7　リスク対策の手法のうち，リスクファイナンシングに該当するものはどれか。

ア　システム被害につながるリスクの発生を抑える対策に資金を投入する。
イ　リスクが大きいと評価されたシステムを廃止し，新たなセキュアなシステムの構築に資金を投入する。
ウ　リスクが顕在化した場合のシステム被害を小さくする設備に資金を投入する。
エ　リスクによってシステムが被害を受けた場合を想定して保険を掛ける。

問 8　ＪＩＳ Ｑ ２７００１：２００６におけるＩＳＭＳの確立に必要な事項①～③の順序関係のうち，適切なものはどれか。
① 適用宣言書の作成
② リスク対応のための管理目的及び管理策の選択
③ リスクの分析と評価

ア　①→②→③　　イ　①→③→②　　ウ　②→③→①　　エ　③→②→①

問 9　ＪＩＳ Ｑ ２７０００:２０１４(情報セキュリティマネジメントシステム－用語)における真正性及び信頼性に対する定義 a ～ d の組みのうち，適切なものはどれか。

〔定義〕
a：意図する行動と結果とが一貫しているという特性
b：エンティティは，それが主張するとおりのものであるという特性
c：認可されたエンティティが要求したときに，アクセス及び使用が可能であるという特性
d：認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しないという特性

	真正性	信頼性
ア	a	c
イ	b	a
ウ	b	d
エ	d	a

問 10　リスクアセスメントを構成するプロセスの組合せはどれか。

ア　リスク特定，リスク評価，リスク受容
イ　リスク特定，リスク分析，リスク評価
ウ　リスク分析，リスク対応，リスク受容
エ　リスク分析，リスク評価，リスク対応

問11　ＡＥＳ-２５６で暗号化されていることが分かっている暗号文が与えられているとき，ブルートフォース攻撃で鍵と解読した平文を得るまでに必要な試行回数の最大値はどれか。

ア　２５６　　イ　2^{128}　　ウ　2^{255}　　エ　2^{256}

問12　ボットネットにおいてC&Cサーバが担う役割はどれか。

ア　遠隔操作が可能なマルウェアに，情報収集及び攻撃活動を指示する。
イ　攻撃の踏み台となった複数のサーバからの通信を制御して遮断する。
ウ　電子商取引事業者などに，偽のディジタル証明書の発行を命令する。
エ　不正なWebコンテンツのテキスト，画像及びレイアウト情報を一元的に管理する。

問13　組織的なインシデント対応体制の構築や運用を支援する目的でＪＰＣＥＲＴ/ＣＣが作成したものはどれか。

ア　ＣＳＩＲＴマテリアル　　イ　ＩＳＭＳユーザーズガイド
ウ　証拠保全ガイドライン　　エ　組織における内部不正防止ガイドライン

問14　ＪＩＳ Ｑ ２７０００:２０１４(情報セキュリティマネジメントシステム－用語)において，"エンティティは，それが主張するとおりのものであるという特性"と定義されているものはどれか。

ア　真正性　　イ　信頼性　　ウ　責任追跡性　　エ　否認防止

13-2 ユーザ認証とアクセス管理

問 1　人間には読み取ることが可能でも，プログラムでは読み取ることが難しいという差異を利用して，ゆがめたり一部を隠したりした画像から文字を判読して入力させることによって，プログラムによる自動入力を排除するための技術はどれか。

ア　CAPTCHA　　イ　QRコード
ウ　短縮URL　　エ　トラックバックping

問 2　利用者ＩＤとパスワードの適切な運用管理方法はどれか。

ア　管理作業を簡素化するために，現在使用されていない利用者ＩＤとパスワードを再利用する。
イ　トラブル処理を迅速化するために，利用者ＩＤとパスワードの一覧表を作成し，管理者が保管する。
ウ　パスワードを他人に悪用されるのを防止するために，利用者が自分のパスワードをいつでも自由に変更できるようにする。
エ　利便性を向上させるために，利用者登録申請書が届く前に，人事異動速報を見て新任者の利用者ＩＤと仮のパスワードを登録する。

問 3　パスワードリスト攻撃の手口に該当するものはどれか。

ア　辞書にある単語をパスワードに設定している利用者がいる状況に着目して，攻撃対象とする利用者ＩＤを定め，英語の辞書にある単語をパスワードとして，ログインを試行する。
イ　数字4桁のパスワードだけしか設定できないＷｅｂサイトに対して，パスワードを定め，文字を組み合わせた利用者ＩＤを総当たりに，ログインを試行する。
ウ　パスワードの総文字数の上限が小さいＷｅｂサイトに対して，攻撃対象とする利用者ＩＤを一つ定め，文字を組み合わせたパスワードを総当たりに，ログインを試行する。
エ　複数サイトで同一の利用者ＩＤとパスワードを使っている利用者がいる状況に着目して，不正に取得した他サイトの利用者ＩＤとパスワードの一覧表を用いて，ログインを試行する。

問 4　ブルートフォース攻撃に該当するものはどれか。

ア　可能性のある文字のあらゆる組合せのパスワードでログインを試みる。
イ　コンピュータへのキー入力を全て記録して外部に送信する。
ウ　盗聴者が正当な利用者のログインシーケンスをそのまま記録してサーバに送信する。
エ　認証が終了してセッションを開始している，ブラウザとＷｅｂサーバの間の通信で，Ｃｏｏｋｉｅなどのセッション情報を盗む。

問 5　リスクベース認証の特徴はどれか。

ア　いかなる環境からの認証の要求においても認証方法を変更せずに，同一の手順によって普段どおりにシステムが利用できる。
イ　ハードウェアトークンとパスワードを併用させるなど，認証要求元の環境によらず常に二つの認証方式を併用することによって，安全性を高める。
ウ　普段と異なる環境からのアクセスと判断した場合，追加の本人認証をすることによって，不正アクセスに対抗し安全性を高める。
エ　利用者が認証情報を忘れ，かつ，Web ブラウザに保存しているパスワード情報も使用できない場合でも，救済することによって，利用者は普段どおりにシステムを利用できる。

問 6　パスワードを用いて利用者を認証する方法のうち，適切なものはどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
イ　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。
ウ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。

問 7　情報セキュリティの脅威であるキーロガーの説明として，適切なものはどれか。

ア　ＰＣ利用者の背後からキーボード入力とディスプレイを見ることで情報を盗み出す。
イ　キーボード入力を記録する仕組みを利用者のＰＣで動作させ，この記録を入手する。
ウ　パスワードとして利用されそうな単語を網羅した辞書データを用いて，パスワードを解析する。
エ　無線ＬＡＮの電波を検知できるＰＣを持って街中を移動し，不正に利用が可能なアクセスポイントを見つけ出す。

問 8　アクセス制御に用いる認証デバイスの特徴に関する記述のうち、適切なものはどれか。

ア　ＵＳＢメモリにディジタル証明書を組み込み、認証デバイスとする場合は、利用するＰＣのＭＡＣアドレスを組み込む必要がある。
イ　成人には虹彩の経年変化がなく、虹彩認証では、認証デバイスでのパターン更新がほとんど不要である。
ウ　静電容量方式の指紋認証デバイスでは、ＬＥＤ照明を設置した室内において正常に認証できなくなる可能性がある。
エ　認証に利用する接触型ＩＣカードは、カード内のコイルの誘導起電力を利用している。

問 9　シングルサインオンの説明のうち，適切なものはどれか。

ア　クッキーを使ったシングルサインオンの場合，サーバごとの認証情報を含んだクッキーをクライアントで生成し，各サーバ上で保存，管理する。
イ　クッキーを使ったシングルサインオンの場合，認証対象のサーバを，異なるインターネット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シングルサインオンの場合，認証対象の Web サーバを，異なるインターネットドメインに配置する必要がある。
エ　リバースプロキシを使ったシングルサインオンの場合，利用者認証においてパスワードの代わりにディジタル証明書を用いることができる。

問 10　生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　システムを誤作動させるデータを無害化する機能をもつライブラリを使用する。
イ　パターンファイルの頻繁な更新だけでなく，ヒューリスティックなど別の手段を組み合わせる。
ウ　本人のディジタル証明書を信頼できる第三者機関に発行してもらう。
エ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

問 11　認証デバイスに関する記述のうち，適切なものはどれか。

ア　ＩＥＥＥ８０２.１Ｘでは，ディジタル証明書や利用者ＩＤ，パスワードを格納するＵＳＢキーは，２００ｋバイト以上のメモリを内蔵することを規定している。
イ　安定した大容量の電力を必要とする高度な処理には，接触型ＩＣカードよりも非接触型ＩＣカードの方が適している。
ウ　虹彩認証では，成人には虹彩の経年変化がないので，認証デバイスでのパターン更新がほとんど不要である。
エ　静電容量方式の指紋認証デバイスでは，ＬＥＤ照明を設置した室内において正常に認証できなくなる可能性がある。

問12 情報システムに対するアクセスのうち，ＪＩＳ Ｑ ２７００２でいう特権的アクセス権を利用した行為はどれか。

ア　許可を受けた営業担当者が，社外から社内の営業システムにアクセスし，業務を行う。
イ　経営者が，機密性の高い経営情報にアクセスし，経営の意思決定に生かす。
ウ　システム管理者が業務システムのプログラムのバージョンアップを行う。
エ　来訪者が，デモシステムにアクセスし，システム機能の確認を行う。

問13 ＩＰＡ"組織における内部不正防止ガイドライン"にも記載されている，組織の適切な情報セキュリティ対策はどれか。

ア　インターネット上のＷｅｂサイトへのアクセスに関しては，コンテンツフィルタ(ＵＲＬフィルタ)を導入して，ＳＮＳ，オンラインストレージ，掲示板などへのアクセスを制限する。
イ　業務の電子メールを，システム障害に備えて，私用のメールアドレスに転送するよう設定させる。
ウ　従業員がファイル共有ソフトを利用する際は，ウイルス対策ソフトの誤検知によってファイル共有ソフトの利用が妨げられないよう，ウイルス対策ソフトの機能を一時的に無効にする。
エ　組織が使用を許可していないソフトウェアに関しては，業務効率が向上するものに限定して，従業員の判断でインストールさせる。

問14 利用者アクセスログの取扱いのうち，ＩＰＡ"組織における内部不正防止ガイドライン"にも記載されており，内部不正の早期発見及び事後対策の観点で適切なものはどれか。

ア　コストにかかわらずログを永久保存する。
イ　利用者にログの管理権限を付与する。
ウ　利用者にログの保存期間を周知する。
エ　ログを定期的に確認する。

問15 インターネットＶＰＮのセキュリティに関する記述のうち，適切なものはどれか。

ア　ＩＰアドレスを悪用した不正アクセスや侵入の危険性はないので，ＩＰアドレスも含めたパケット全体の暗号化は必要ない。
イ　インターネットＶＰＮの仮想的なトンネルは特定ＬＡＮ間の専用通路であるから，通過するデータに対する盗聴防止の機能はない。
ウ　仮想的なネットワークを形成するものであり，ネットワークに参加する資格のない第三者による盗聴や改ざんを防御できない。
エ　ネットワークに参加する資格のある個々人を識別する能力はない。

問16 無線ＬＡＮやＶＰＮ接続などで利用され，利用者を認証するためのシステムはどれか。

ア　ＤＥＳ　　イ　ＤＮＳ　　ウ　ＩＤＳ　　エ　ＲＡＤＩＵＳ

問 17　セキュリティ対策に関連する標準又は規格に関する記述のうち，適切なものはどれか。

ア　ＪＩＳ Ｑ ２７００２は，製品やシステムのセキュリティ機能及び実装のレベルを技術面から評価する基準である。
イ　ＪＩＳ Ｘ ５０７０は，セキュリティ組織から設備管理に及ぶ運用管理全体の規約を定めた実践規範であり，アクセス制御も評価対象とする。
ウ　ＪＩＳ Ｘ ５７３１-8(ＩＴU-T　X.５０９)は，ＸＭＬ文書の暗号化とディジタル署名関連の規格であり，Ｗｅｂ関連技術におけるＨＴＴＰやＨＴＭＬの標準化を行う任意団体Ｗ３Ｃが任意団体ＩＥＴＦと協力して定めたものである。
エ　インターネットの各種技術の標準化を進めている任意団体ＩＥＴＦは技術仕様をＲＦＣとして発行しており，セキュリティ分野にはＲＡＤＩＵＳやＬＤＡＰの仕様がある。

問 18　ソーシャルエンジニアリング手法を利用した標的型攻撃メールの特徴はどれか。

ア　件名に“未承諾広告※”と記述されている。
イ　件名や本文に，受信者の業務に関係がありそうな内容が記述されている。
ウ　支払う必要がない料金を振り込ませるために，債権回収会社などを装い無差別に送信される。
エ　偽のホームページにアクセスさせるために，金融機関などを装い無差別に送信される。

問 19　セキュアブートの説明はどれか。

ア　ＢＩＯＳにパスワードを設定し，ＰＣ起動時にＢＩＯＳのパスワード入力を要求することによって，ＯＳの不正な起動を防ぐ技術
イ　ＨＤＤにパスワードを設定し，ＰＣ起動時にＨＤＤのパスワード入力を要求することによって，ＯＳの不正な起動を防ぐ技術
ウ　ＰＣの起動時にＯＳやドライバのディジタル署名を検証し，許可されていないものを実行しないようにすることによって，ＯＳ起動前のマルウェアの実行を防ぐ技術
エ　マルウェア対策ソフトをスタートアッププログラムに登録し，ＯＳ起動時に自動的にマルウェアスキャンを行うことによって，マルウェアの被害を防ぐ技術

問 20　ＢＹＯＤの説明，及びその情報セキュリティリスクに関する記述のうち，適切なものはどれか。

ア　従業員が企業から貸与された情報端末を，客先などへの移動中に業務に利用することであり，ショルダハッキングなどのセキュリティリスクが増大する。
イ　従業員が企業から貸与された情報端末を，自宅に持ち帰って私的に利用することであり，機密情報の漏えいなどのセキュリティリスクが増大する。
ウ　従業員が私的に保有する情報端末を，職場での休憩時間などに私的に利用することであり，社内でのセキュリティ意識の低下などのセキュリティリスクが増大する。
エ　従業員が私的に保有する情報端末を業務に利用することであり，セキュリティ設定の不備に起因するウイルス感染などのセキュリティリスクが増大する。

問 21　キーロガーの悪用例はどれか。

ア　通信を行う 2 者間の経路上に割り込み，両者が交換する情報を収集し，改ざんする。
イ　ネットバンキング利用時に，利用者が入力したパスワードを収集する。
ウ　ブラウザでの動画閲覧時に，利用者の意図しない広告を勝手に表示する。
エ　ブラウザの起動時に，利用者がインストールしていないツールバーを勝手に表示する。

問 22　公衆無線ＬＡＮのアクセスポイントを設置するときのセキュリティ対策と効果の組みのうち，適切なものはどれか。

	セキュリティ対策	効果
ア	MAC アドレスフィルタリングを設定する。	正規の端末の MAC アドレスに偽装した攻撃者の端末からの接続を遮断し，利用者のなりすましを防止する。
イ	SSID を暗号化する。	SSID を秘匿して，SSID の盗聴を防止する。
ウ	自社がレジストラに登録したドメインを，アクセスポイントの SSID に設定する。	正規のアクセスポイントと同一の SSID を設定した，悪意のあるアクセスポイントの設置を防止する。
エ	同一のアクセスポイントに無線で接続している端末同士の通信を，アクセスポイントで遮断する。	同一のアクセスポイントに無線で接続している他の端末に，公衆無線 LAN の利用者がアクセスポイントを経由して無断でアクセスすることを防止する。

問 23　別のサービスやシステムから流出したアカウント認証情報を用いて，アカウント認証情報を使い回している利用者のアカウントを乗っ取る攻撃はどれか。

ア　パスワードリスト攻撃　　イ　ブルートフォース攻撃
ウ　リバースブルートフォース攻撃　　エ　レインボー攻撃

問 24　マルウェア対策ソフトでのフォールスネガティブに該当するものはどれか。

ア　マルウェアに感染していないファイルを，マルウェアに感染していないと判断する。
イ　マルウェアに感染していないファイルを，マルウェアに感染していると判断する。
ウ　マルウェアに感染しているファイルを，マルウェアに感染していないと判断する。
エ　マルウェアに感染しているファイルを，マルウェアに感染していると判断する。

問 25　攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

ア　事前調査の段階で，攻撃できそうなサービスがあるかどうかを調査する。
イ　権限取得の段階で，権限を奪取できそうなアカウントがあるかどうかを調査する。
ウ　不正実行の段階で，攻撃者にとって有益な利用者情報があるかどうかを調査する。
エ　後処理の段階で，システムログに攻撃の痕跡が残っていないかどうかを調査する。

問 26　ＳＰＦ(Sender Policy Framework)の仕組みはどれか。

ア　電子メールを受信するサーバが，電子メールに付与されているディジタル署名を使って，送信元ドメインの詐称がないことを確認する。
イ　電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバのＩＰアドレスから，ドメインの詐称がないことを確認する。
ウ　電子メールを送信するサーバが，送信する電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。
エ　電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。

問 27　バイオメトリクス認証システムの判定しきい値を変化させるとき，ＦＲＲ(本人拒否率)と ＦＡＲ(他人受入率)との関係はどれか。

ア　ＦＲＲとＦＡＲは独立している。
イ　ＦＲＲを減少させると，ＦＡＲは減少する。
ウ　ＦＲＲを減少させると，ＦＡＲは増大する。
エ　ＦＲＲを増大させると，ＦＡＲは増大する。

問 28 サーバにバックドアを作り，サーバ内で侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージはどれか。

ア　ＲＦＩＤ　　イ　ｒｏｏｔｋｉｔ　　ウ　ＴＫＩＰ　　エ　ｗｅｂ ｂｅａｃｏｎ

問 29　情報セキュリティにおいてバックドアに該当するものはどれか。

ア　アクセスする際にパスワード認証などの正規の手続が必要な Web サイトに，当該手続を経ないでアクセス可能な URL
イ　インターネットに公開されているサーバの TCP ポートの中からアクティブになっているポートを探して，稼働中のサービスを特定するためのツール
ウ　ネットワーク上の通信パケットを取得して通信内容を見るために設けられたスイッチの LAN ポート
エ　プログラムが確保するメモリ領域に，領域の大きさを超える長さの文字列を入力してあふれさせ，ダウンさせる攻撃

13-3 コンピュータウイルスの脅威

問 1　データの破壊，改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールさせ，実行させるものはどれか。

ア　ＤｏＳ攻撃　　イ　辞書攻撃　　ウ　トロイの木馬　　エ　バッファオーバフロー攻撃

問 2　ウイルスの調査手法に関する記述のうち，適切なものはどれか。

ア　逆アセンブルはバイナリコードの新種ウイルスの動作を解明するのに有効な手法である。
イ　パターンマッチングでウイルスを検知する方式は，暗号化された文書中のマクロウイルスの動作を解明するのに有効な手法である。
ウ　ファイルのハッシュ値を基にウイルスを検知する方式は，未知のウイルスがどのウイルスの亜種かを特定するのに確実な手法である。
エ　不正な動作からウイルスを検知する方式は，ウイルス名を特定するのに確実な手法である。

問 3　ビヘイビア法のウイルス検出手法に当たるものはどれか。

ア　あらかじめ検査対象に付加された，ウイルスに感染していないことを保証する情報と，検査対象から算出した情報とを比較する。
イ　検査対象と安全な場所に保管してあるその原本とを比較する。
ウ　検査対象のハッシュ値と既知のウイルスファイルのハッシュ値とを比較する。
エ　検査対象をメモリ上の仮想環境下で実行して，その挙動を監視する。

問 4　ウイルス検知手法の一つであるビヘイビア法を説明したものはどれか。

ア　ウイルスの特徴的なコード列が検査対象プログラム内に存在するかどうかを調べて，もし存在していればウイルスとして検知する。
イ　各ファイルに，チェックサム値などウイルスではないことを保証する情報を付加しておき，もし保証する情報が検査対象ファイルに付加されていないか無効ならば，ウイルスとして検知する。
ウ　検査対象ファイルのハッシュ値と，安全な場所に保管してあるその対象の原本のハッシュ値を比較して，もし異なっていればウイルスとして検知する。
エ　検査対象プログラムを動作させてその挙動を監視し，もしウイルスによく見られる行動を起こせばウイルスとして検知する。

問 5　クライアントＰＣで行うマルウェア対策のうち，適切なものはどれか。

ア　ＰＣにおけるウイルスの定期的な手動検査では，ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
イ　ウイルスがＰＣの脆弱性を突いて感染しないように，ＯＳ及びアプリケーションの修正パッチを適切に適用する。
ウ　電子メールに添付されたウイルスに感染しないように，使用しないＴＣＰポート宛ての通信を禁止する。
エ　ワームが侵入しないように，クライアントＰＣに動的グローバルＩＰアドレスを付与する。

問 6　コンピュータウイルスの検出，機能の解明，又は種類の特定をする方法について，適切な記述はどれか。

ア　暗号化された文書中のマクロウイルスを検出するにはパターンマッチング方式が有効である。
イ　逆アセンブルは，バイナリタイプの新種ウイルスの機能を解明するのに有効な手法である。
ウ　不正な動作を識別してウイルスを検知する方式は，ウイルス名を特定するのに最も有効である。
エ　ワームは既存のファイルに感染するタイプのウイルスであり，その感染の有無の検出にはファイルの大きさの変化を調べるのが有効である。

問 7　手順に示すセキュリティ攻撃はどれか。

〔手順〕
（1）攻撃者が金融機関の偽のＷｅｂサイトを用意する。
（2）金融機関の社員を装って，偽のＷｅｂサイトへ誘導するＵＲＬを本文中に含めた電子メールを送信する。
（3）電子メールの受信者が，その電子メールを信用して本文中のＵＲＬをクリックすると，偽のＷｅｂサイトに誘導される。
（4）偽のＷｅｂサイトと気付かずに認証情報を入力すると，その情報が攻撃者に渡る。

ア　ＤＤｏＳ攻撃　　イ　フィッシング　　ウ　ボット　　エ　メールヘッダインジェクション

問 8　企業のＤＭＺ上で1台のＤＮＳサーバをインターネット公開用と社内用で共用している。このＤＮＳサーバが，ＤＮＳキャッシュポイズニングの被害を受けた結果，引き起こされ得る現象はどれか。

ア　ＤＮＳサーバのハードディスク上のファイルに定義されているＤＮＳサーバ名が書き換わり，外部からの参照者が，ＤＮＳサーバに接続できなくなる。
イ　ＤＮＳサーバのメモリ上にワームが常駐し，ＤＮＳ参照元に対して不正プログラムを送り込む。
ウ　社内の利用者が，インターネット上の特定のＷｅｂサーバを参照しようとすると，本来とは異なるＷｅｂサーバに誘導される。
エ　社内の利用者間の電子メールについて，宛先メールアドレスが書き換えられ，送受信ができなくなる。

問 9　ＤＮＳキャッシュポイズニングに分類される攻撃内容はどれか。

ア　ＤＮＳサーバのソフトウェアのバージョン情報を入手して，ＤＮＳサーバのセキュリティホールを特定する。
イ　ＰＣが参照するＤＮＳサーバに偽のドメイン情報を注入して，利用者を偽装されたサーバに誘導する。
ウ　攻撃対象のサービスを妨害するために，攻撃者がＤＮＳサーバを踏み台に利用して再帰的な問合せを大量に行う。
エ　内部情報を入手するために，ＤＮＳサーバが保存するゾーン情報をまとめて転送させる。

問 10　ＳＱＬインジェクションの説明はどれか。

ア　Ｗｅｂアプリケーションに悪意のある入力データを与えてデータベースの問合せや操作を行う命令文を組み立てて，データを改ざんしたり不正に情報取得したりする攻撃
イ　悪意のあるスクリプトが埋め込まれたＷｅｂページを訪問者に閲覧させて，別のＷｅｂサイトで，その訪問者が意図しない操作を行わせる攻撃
ウ　市販されているデータベース管理システムの脆(ぜい)弱性を利用して，宿主となるデータベースサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃
エ　訪問者の入力データをそのまま画面に表示するＷｅｂサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送り，訪問者のブラウザで実行させる攻撃

問11　クロスサイトスクリプティングの手口はどれか。

ア　Ｗｅｂアプリケーションに用意された入力フィールドに，悪意のあるＪａｖａＳｃｒｉｐｔコードを含んだデータを入力する。
イ　インターネットなどのネットワークを通じてサーバに不正にアクセスしたり，データの改ざん・破壊を行ったりする。
ウ　大量のデータをＷｅｂアプリケーションに送ることによって，用意されたバッファ領域をあふれさせる。
エ　パス名を推定することによって，本来は認証された後にしかアクセスが許可されていないページに直接ジャンプする。

問12　クロスサイトスクリプティングによる攻撃を防止する対策はどれか。

ア　ＯＳのセキュリティパッチを適用する。
イ　ＷｅｂサーバにＳＮＭＰエージェントを常駐稼働させる。
ウ　Ｗｅｂサイトへの入力データを表示するときに特殊文字のエスケープ処理を行う。
エ　許容範囲を超えた大きさのデータの書込みを禁止する。

問13　ＳＱＬインジェクション攻撃を防ぐ方法はどれか。

ア　入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。
イ　入力にＨＴＭＬタグが含まれていたら，ＨＴＭＬタグとして解釈されない他の文字列に置き換える。
ウ　入力に，上位ディレクトリを指定する文字(../)を含むときは受け付けない。
エ　入力の全体の長さが制限を超えているときは受け付けない。

問14　ＩＴサービスマネジメントにおけるインシデント管理の主な活動はどれか。

ア　インシデントから発生する問題の解決策の評価
イ　インシデントの解決とサービスの復旧
ウ　インシデントの根本原因の究明
エ　インシデントのトレンド分析と予防措置

問15　マルウェアについて，トロイの木馬とワームを比較したとき，ワームの特徴はどれか。

ア　勝手にファイルを暗号化して正常に読めなくする。
イ　単独のプログラムとして不正な動作を行う。
ウ　特定の条件になるまで活動をせずに待機する。
エ　ネットワークやリムーバブルメディアを媒介として自ら感染を広げる。

問16　ＳＱＬインジェクション攻撃の説明はどれか。

ア　Ｗｅｂアプリケーションに問題があるとき，悪意のある問合せや操作を行う命令文を入力して，データベースのデータを不正に取得したり改ざんしたりする攻撃
イ　悪意のあるスクリプトを埋め込んだＷｅｂページを訪問者に閲覧させて，別のＷｅｂサイトで，その訪問者が意図しない操作を行わせる攻撃
ウ　市販されているＤＢＭＳの脆弱性を利用することによって，宿主となるデータベーサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃
エ　訪問者の入力データをそのまま画面に表示するＷｅｂサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃

問17　ＶＢＳｃｒｉｐｔ(Ｖｉｓｕａｌ　Ｂａｓｉｃ　Ｓｃｒｉｐｔ)で作られたコンピュータウイルスの特徴はどれか。

ア　ＨＴＭＬ形式の電子メール本文などに埋め込まれたスクリプトによって動作する。
イ　感染対象が実行形式ファイルであるか文書ファイルであるかにかかわらず，すべてのＯＳで動作する。
ウ　実行ファイルはなくワープロの文書ファイルなどに感染し，関連するアプリケーションソフトを利用して動作する。
エ　ブートセクタに感染して，通常のプロセス起動前にウイルスが呼び出されて動作する。

問18　スパイウェアに該当するものはどれか。

ア　Ｗｅｂサイトへの不正な入力を排除するために，Ｗｅｂサイトの入力フォームの入力データから，ＨＴＭＬタグ，ＪａｖａＳｃｒｉｐｔ，ＳＱＬ文などを検出し，それらを他の文字列に置き換えるプログラム
イ　サーバへの侵入口となり得る脆弱なポートを探すために，攻撃者のＰＣからサーバのＴＣＰポートに順番にアクセスするプログラム
ウ　利用者の意図に反してＰＣにインストールされ，利用者の個人情報やアクセス履歴などの情報を収集するプログラム
エ　利用者のパスワードを調べるために，サーバにアクセスし，辞書に載っている単語を総当たりで試すプログラム

問19　ブルートフォース攻撃に該当するものはどれか。

ア　Web ブラウザと Web サーバの間の通信で，認証が成功してセッションが開始されているときに，Cookie などのセッション情報を盗む。
イ　可能性がある文字のあらゆる組合せのパスワードでログインを試みる。
ウ　コンピュータへのキー入力を全て記録して外部に送信する。
エ　盗聴者が正当な利用者のログインシーケンスをそのまま記録してサーバに送信する。

問 20　ディレクトリトラバーサル攻撃はどれか。

ア　ＯＳコマンドを受け付けるアプリケーションに対して，攻撃者が，ディレクトリを作成するＯＳコマンドの文字列を入力して実行させる。
イ　ＳＱＬ文のリテラル部分の生成処理に問題があるアプリケーションに対して，攻撃者が，任意のＳＱＬ文を渡して実行させる。
ウ　シングルサインオンを提供するディレクトリサービスに対して，攻撃者が，不正に入手した認証情報を用いてログインし，複数のアプリケーションを不正使用する。
エ　入力文字列からアクセスするファイル名を組み立てるアプリケーションに対して，攻撃者が，上位のディレクトリを意味する文字列を入力して，非公開のファイルにアクセスする。

問 21　オープンリダイレクトを悪用した攻撃に該当するものはどれか。

ア　HTML メールのリンクを悪用し，HTML メールに，正規の Web サイトとは異なる偽の Web サイトの URL をリンク先に指定し，利用者がリンクをクリックすることによって，偽の Web サイトに誘導する。
イ　Web サイトにアクセスすると自動的に他の Web サイトに遷移する機能を悪用し，攻撃者が指定した偽の Web サイトに誘導する。
ウ　インターネット上の不特定多数のホストから DNS リクエストを受け付けて応答する DNS キャッシュサーバを悪用し，攻撃対象の Web サーバに大量の DNS のレスポンスを送り付け，リソースを枯渇させる。
エ　設定の不備によって，正規の利用者以外からの電子メールや Web サイトへのアクセス要求を受け付けるプロキシを悪用し，送信元を偽った迷惑メールの送信を行う。

13-4　ネットワークのセキュリティ対策

問 1　ＷＡＦの説明として，適切なものはどれか。

ア　ＤＭＺに設置されているＷｅｂサーバへ外部から実際に侵入を試みる。
イ　ＷｅｂサーバのＣＰＵ負荷を軽減するために，ＳＳＬによる暗号化と復号の処理をＷｅｂサーバではなく専用のハードウェア上で行う。
ウ　システム管理者が質問に答える形式で，自組織の情報セキュリティ対策のレベルを診断する。
エ　特徴的なパターンが含まれるかなどＷｅｂアプリケーションへの通信内容を検査して，不正な操作を遮断する。

問 2　ＷＡＦ（Web Application Firewall）を利用する目的はどれか。

ア　Ｗｅｂサーバ及びＷｅｂアプリケーションに起因する脆弱性への攻撃を遮断する。
イ　Ｗｅｂサーバ内でワームの侵入を検知し，ワームの自動駆除を行う。
ウ　Ｗｅｂサーバのコンテンツ開発の結合テスト時にＷｅｂアプリケーションの脆弱性や不整合を検知する。
エ　Ｗｅｂサーバのセキュリティホールを発見し，ＯＳのセキュリティパッチを適用する。

問 3　ＷＡＦの説明はどれか。

ア　Ｗｅｂサイトに対するアクセス内容を監視し，攻撃とみなされるパターンを検知したときに当該アクセスを遮断する。
イ　Ｗｉ－Ｆｉアライアンスが認定した無線ＬＡＮの暗号化方式の規格であり，ＡＥＳ暗号に対応している。
ウ　様々なシステムの動作ログを一元的に蓄積，管理し，セキュリティ上の脅威となる事象をいち早く検知，分析する。
エ　ファイアウォール機能を有し，ウイルス対策，侵入検知などを連携させ，複数のセキュリティ機能を統合的に管理する。

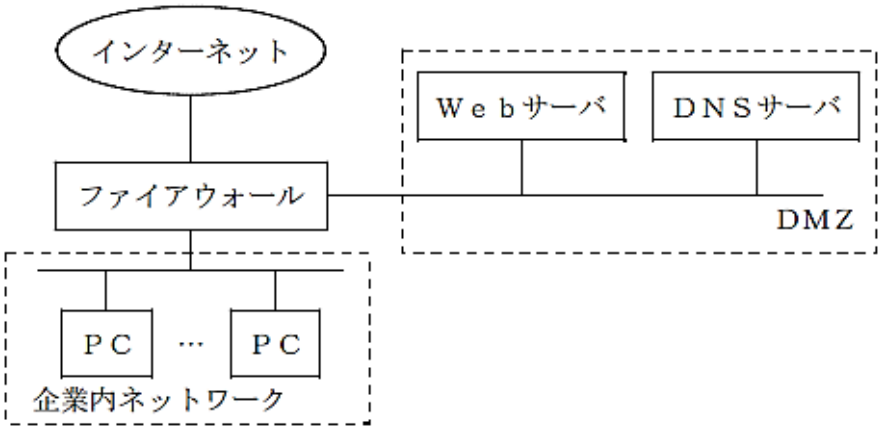
問 4　ファイアウォールのパケットフィルタリング機能を利用して実現できるものはどれか。

ア　インターネットから受け取ったパケットに改ざんがある場合は修正し，改ざんが修正できない場合には，ログを取って内部ネットワークへの通過を阻止する。
イ　インターネットから受け取ったパケットのヘッダ部分及びデータ部分に，改ざんがあるかどうかをチェックし，改ざんがあった場合にはそのパケットを除去する。
ウ　動的に割り振られたＴＣＰポート番号をもったパケットを，受信側で固定値のＴＣＰポート番号をもったパケットに変更して，内部ネットワークへの通過を許可する。
エ　特定のＴＣＰポート番号をもったパケットだけに，インターネットから内部ネットワークへの通過を許可する。

問 5　パケットフィルタリング型ファイアウォールのフィルタリングルールを用いて，本来必要なサービスに影響を及ぼすことなく防げるものはどれか。

ア　外部に公開しないサービスへのアクセス
イ　サーバで動作するソフトウェアの脆弱性を突く攻撃
ウ　電子メールに添付されたファイルに含まれるマクロウイルスの侵入
エ　電子メール爆弾などのＤｏＳ攻撃

問 6　図に示すネットワーク構成で，Ｗｅｂページの閲覧だけを社外に提供する。攻撃を防止するためにファイアウォールのＩＰパケットフィルタリングを設定する場合，フィルタリングルールでインターネットからＤＭＺへのパケットの通過を禁止できないプロトコルはどれか。



ア　ＦＴＰ　　イ　ＨＴＴＰ　　ウ　ＳＭＴＰ　　エ　ＳＮＭＰ

問 7　ペネトレーションテストの目的はどれか

ア　暗号化で使用している暗号方式と鍵長が，設計仕様と一致することを確認する。
イ　対象プログラムの入力に対する出力結果が，出力仕様と一致することを確認する。
ウ　ファイアウォールが単位時間当たりに処理できるセッション数を確認する。
エ　ファイアウォールや公開サーバに対して侵入できないかどうかを確認する。

問 8　パケットフィルタリング型ファイアウォールがルール一覧に基づいてパケットを制御する場合，パケットAに適用されるルールとそのときの動作はどれか。ここで，ファイアウォールでは，ルール一覧に示す番号の1から順にルールを適用し，一つのルールが適合したときには残りのルールは適用しない。

〔ルール一覧〕

番号	送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号	動作
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注記　*は任意のパターンを表す。

〔パケットA〕

送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号
10.1.2.3	10.2.3.4	TCP	2100	25

ア　番号1によって，通過を禁止する。
イ　番号2によって，通過を許可する。
ウ　番号3によって，通過を許可する。
エ　番号4によって，通過を禁止する。

問 9　ポリモーフィック型マルウェアの説明として，適切なものはどれか。

ア　インターネットを介して，攻撃者がＰＣを遠隔操作する。
イ　感染ごとにマルウェアのコードを異なる鍵で暗号化することによって，同一のパターンでは検知されないようにする。
ウ　複数のＯＳ上で利用できるプログラム言語でマルウェアを作成することによって，複数のＯＳ上でマルウェアが動作する。
エ　ルートキットを利用して，マルウェアに感染していないように見せかけることによって，マルウェアを隠蔽する。

問10 Ｗｅｂで利用されるプロキシサーバの機能に関する記述として，適切なものはどれか。

ア　イントラネットで使っているプライベートＩＰアドレスとグローバルＩＰアドレスとを相互変換する。
イ　クライアントがネットワークに接続する際に，クライアントに対してＩＰアドレスを動的に割り当てる。
ウ　内部ネットワークのクライアントが外部のサーバと通信する場合，中継役となりクライアントの代わりにサーバへ接続する。
エ　ホスト名とＩＰアドレスの対応表をもち，クライアントからの問合せに対しホスト名に対応するＩＰアドレスを通知する。

問11 Ｗｅｂアクセスで利用されるプロキシサーバの機能として，適切なものはどれか。

ア　外部サーバのホスト名とＩＰアドレスの対応表をもち，クライアントからの問合せに対してホスト名に対応するＩＰアドレスを通知する。
イ　クライアントが内部ネットワークに接続するときに，クライアントに対してＩＰアドレスを動的に割り当てる。
ウ　内部ネットワークで使っているプライベートＩＰアドレスとグローバルＩＰアドレスとを相互変換し，外部サーバとの直接通信を実現する。
エ　内部ネットワークのクライアントが外部サーバと通信する場合，中継役となりクライアントの代わりに外部サーバに接続する。

問12 ダウンローダ型マルウェアが内部ネットワークのＰＣに感染したとき，そのマルウェアによってインターネット経由で他のマルウェアがダウンロードされることを防ぐ対策として，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危険な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　スパム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 電子メール送信時に送信者に対して宛先アドレスの確認を求めるのが有効であるセキュリティ対策はどれか。

ア　ＯＰ２５Ｂによるスパム対策　　イ　ＳＰＦによるスパム対策
ウ　電子メールの誤送信対策　　エ　電子メールの不正中継対策

問14 電子メールのコンテンツフィルタリングによる情報漏えい対策を説明したものはどれか。

ア　外部に公開されている電子メールアドレスから発信される電子メールは，情報漏えいを検知する必要がない。
イ　電子メールの発信記録からスパムメールを選別し，スパムメール発信者のすべての電子メールの発信を停止する。
ウ　添付ファイルのない電子メールは情報漏えいの疑いがないので，検知する必要がない。
エ　登録したキーワードと自動照合することによって，情報漏えいの疑いのある電子メールを検知して発信を停止する。

問15 毎回参加者が変わる１００名程度の公開セミナにおいて，参加者が持参する端末に対して無線ＬＡＮ接続環境を提供する。参加者の端末以外からのアクセスポイントへの接続を防止するために効果があるセキュリティ対策はどれか。

ア　アクセスポイントがもつＤＨＣＰサーバ機能において，参加者の端末に対して動的に割り当てるＩＰアドレスの範囲をセミナごとに変更する。
イ　アクセスポイントがもつＵＲＬフィルタリング機能において，参加者の端末に対する条件をセミナごとに変更する。
ウ　アクセスポイントがもつ暗号化機能において，参加者の端末とアクセスポイントとの間で事前に共有する鍵をセミナごとに変更する。
エ　アクセスポイントがもつプライバシセパレータ機能において，参加者の端末へのアクセス制限をセミナごとに変更する。

問16 ディジタルフォレンジックスを説明したものはどれか。

ア　画像や音楽などのディジタルコンテンツに著作権者などの情報を埋め込む。
イ　コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり，システムを実際に攻撃して侵入を試みる。
ウ　ネットワーク管理者や利用者などから，巧みな話術や盗み聞き，盗み見などの手段によって，パスワードなどのセキュリティ上重要な情報を入手する。
エ　犯罪に対する証拠となり得るデータを保全し，その後の訴訟などに備える。

問17　JIS Q 27000:2019(情報セキュリティマネジメントシステム－用語)において定義されている情報セキュリティの特性に関する記述のうち，否認防止の特性に関する記述はどれか。

ア　ある利用者があるシステムを利用したという事実が証明可能である。
イ　認可された利用者が要求したときにアクセスが可能である。
ウ　認可された利用者に対してだけ，情報を使用させる又は開示する。
エ　利用者の行動と意図した結果とが一貫性をもつ。

問18　クライアントＡがポート番号８０８０のＨＴＴＰプロキシサーバＢを経由してポート番号８０のＷｅｂサーバＣにアクセスしているとき，宛先ポート番号が常に８０８０になるＴＣＰパケットはどれか。

ア　ＡからＢへのＨＴＴＰ要求及びＣからＢへのＨＴＴＰ応答
イ　ＡからＢへのＨＴＴＰ要求だけ
ウ　ＢからＡへのＨＴＴＰ応答だけ
エ　ＢからＣへのＨＴＴＰ要求及びＣからＢへのＨＴＴＰ応答

問19　ファイアウォールの方式に関する記述のうち，適切なものはどれか。

ア　アプリケーションゲートウェイ方式では，アプリケーションのプロトコルごとにゲートウェイ機能の設定が必要である。
イ　サーキットゲートウェイ方式では，コマンドの通過可否を制御する。
ウ　トランスポートゲートウェイ方式では，アプリケーションのプロトコルに依存するゲートウェイ機能を提供する。
エ　パケットフィルタリング方式では，電子メールの中に含まれている単語によるフィルタリングが可能である。

問20　ディジタルフォレンジックスの手順を収集，検査，分析，報告に分けたとき，そのいずれかに該当するものはどれか。

ア　サーバとネットワーク機器のログをログ管理サーバに集約し，リアルタイムに相関分析することによって，不正アクセスを検出する。
イ　ディスクを解析し，削除されたログファイルを復元することによって，不正アクセスの痕跡を発見する。
ウ　電子メールを外部に送る際に，本文及び添付ファイルを暗号化することによって，情報漏えいを防ぐ。
エ　プログラムを実行する際に，プログラムファイルのハッシュ値と脅威情報を突き合わせることによって，マルウェアを発見する。

問21　ＩＣカードの耐タンパ性を高める対策はどれか。

ア　ＩＣカードとＩＣカードリーダとが非接触の状態で利用者を認証して，利用者の利便性を高めるようにする。
イ　故障に備えてあらかじめ作成した予備のＩＣカードを保管し，故障時に直ちに予備カードに交換して利用者がＩＣカードを使い続けられるようにする。
ウ　信号の読み出し用プローブの取付けを検出するとＩＣチップ内の保存情報を消去する回路を設けて，ＩＣチップ内の情報を容易に解析できないようにする。
エ　利用者認証にＩＣカードを利用している業務システムにおいて，退職者のＩＣカードは業務システム側で利用を停止して，ほかの利用者が使用できないようにする。

問22　経済産業省とＩＰＡが策定した"サイバーセキュリティ経営ガイドライン(Ｖｅｒ１.１)"が，自社のセキュリティ対策に加えて，実施状況を確認すべきとしている対策はどれか。

ア　自社が提供する商品及びサービスの個人利用者が行うセキュリティ対策
イ　自社に出資している株主が行うセキュリティ対策
ウ　自社のサプライチェーンのビジネスパートナが行うセキュリティ対策
エ　自社の事業所近隣の地域社会が行うセキュリティ対策

問23　ファイルの提供者は，ファイルの作成者が作成したファイルＡを受け取り，ファイルＡと，ファイルＡにＳＨＡ－２５６を適用して算出した値Ｂとを利用者に送信する。そのとき，利用者が情報セキュリティ上実現できることはどれか。ここで，利用者が受信した値Ｂはファイルの提供者から事前に電話で直接伝えられた値と同じであり，改ざんされていないことが確認できているものとする。

ア　値ＢにＳＨＡ－２５６を適用して値Ｂからディジタル署名を算出し，そのディジタル署名を検証することによって，ファイルＡの作成者を確認できる。

イ　値ＢにＳＨＡ－２５６を適用して値Ｂからディジタル署名を算出し，そのディジタル署名を検証することによって，ファイルＡの提供者がファイルＡの作成者であるかどうかを確認できる。

ウ　ファイルＡにＳＨＡ－２５６を適用して値を算出し，その値と値Ｂを比較することによって，ファイルＡの内容が改ざんされていないかどうかを検証できる。

エ　ファイルＡの内容が改ざんされていても，ファイルＡにＳＨＡ－２５６を適用して値を算出し，その値と値Ｂの差分を確認することによって，ファイルＡの内容のうち改ざんされている部分を修復できる。

問24　社内ネットワークとインターネットの接続点にパケットフィルタリング型ファイアウォールを設置して，社内ネットワーク上のＰＣからインターネット上のＷｅｂサーバ(ポート番号８０）にアクセスできるようにするとき，フィルタリングで許可するルールの適切な組合せはどれか。

ア

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	80	1024 以上

イ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	1024 以上	80

ウ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	80	1024 以上

エ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	1024 以上	80

問25　ＣＳＩＲＴの説明として，適切なものはどれか。

ア　ＩＰアドレスの割当て方針の決定，ＤＮＳルートサーバの運用監視，ＤＮＳ管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業内・組織内や政府機関に設置され，情報セキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもつ者や組織の総称である。

問26　ボットネットにおいてＣ＆Ｃサーバが果たす役割はどれか。

ア　遠隔操作が可能なマルウェアに，情報収集及び攻撃活動を指示する。
イ　電子商取引事業者などに，偽のディジタル証明書の発行を命令する。
ウ　不正なＷｅｂコンテンツのテキスト，画像及びレイアウト情報を一元的に管理する。
エ　踏み台となる複数のサーバからの通信を制御し遮断する。

問27　手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。

〔手順〕
（1）：送信者は，電子メールの本文を共通鍵暗号方式で暗号化し(暗号文)，その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する(共通鍵の暗号化データ)。
（2）：送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。
（3）：受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号方式で復号し，得た共通鍵で暗号文を復号する。

ア　送信者による電子メールの送達確認
イ　送信者のなりすましの検出
ウ　電子メールの本文の改ざん箇所の修正
エ　電子メールの本文の内容の漏えいの防止

問28　利用者情報を格納しているデータベースから利用者情報を検索して表示する機能だけをもつアプリケーションがある。このアプリケーションがデータベースにアクセスするときに用いるアカウントに与えるデータベースへのアクセス権限として，情報セキュリティ管理上，適切なものはどれか。ここで，権限の名称と権限の範囲は次のとおりとする。

〔権限の名称と権限の範囲〕
参照権限：　レコードの参照が可能
更新権限：　レコードの登録，変更，削除が可能
管理者権限：テーブルの参照，登録，変更，削除が可能

ア　管理者権限
イ　更新権限
ウ　更新権限と参照権限
エ　参照権限

問29　社内ネットワークとインターネットの接続点に，ステートフルインスペクション機能をもたない，静的なパケットフィルタリング型のファイアウォールを設置している。このネットワーク構成において，社内のＰＣからインターネット上のＳＭＴＰサーバに電子メールを送信できるようにするとき，ファイアウォールで通過を許可するＴＣＰパケットのポート番号の組合せはどれか。ここで，ＳＭＴＰ通信には，デフォルトのポート番号を使うものとする。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	ＰＣ	ＳＭＴＰサーバ	２５	１０２４以上
	ＳＭＴＰサーバ	ＰＣ	１０２４以上	２５
イ	ＰＣ	ＳＭＴＰサーバ	１１０	１０２４以上
	ＳＭＴＰサーバ	ＰＣ	１０２４以上	１１０
ウ	ＰＣ	ＳＭＴＰサーバ	１０２４以上	２５
	ＳＭＴＰサーバ	ＰＣ	２５	１０２４以上
エ	ＰＣ	ＳＭＴＰサーバ	１０２４以上	１１０
	ＳＭＴＰサーバ	ＰＣ	１１０	１０２４以上

問30　整数１～1,０００を有効とする入力値が，１～１００の場合は処理Ａを，１０１～1,０００の場合は処理Ｂを実行する入力処理モジュールを，同値分割法と境界値分析によってテストする。次の条件でテストするとき，テストデータの最小個数は幾つか。

〔条件〕
① 有効同値クラスの１クラスにつき，一つの値をテストデータとする。ただし，テストする値は境界値でないものとする。
② 有効同値クラス，無効同値クラスの全ての境界値をテストデータとする。

ア　5　　イ　6　　ウ　7　　エ　8

問31　インターネットに接続された利用者のＰＣから，ＤＭＺ上の公開Ｗｅｂサイトにアクセスし，利用者の個人情報を入力すると，その個人情報が内部ネットワークのデータベース(ＤＢ)サーバに蓄積されるシステムがある。このシステムにおいて，利用者個人のディジタル証明書を用いたＴＬＳ通信を行うことによって期待できるセキュリティ上の効果はどれか。

ア　ＰＣとＤＢサーバ間の通信データを暗号化するとともに，正当なＤＢサーバであるかを検証することができるようになる。
イ　ＰＣとＤＢサーバ間の通信データを暗号化するとともに，利用者を認証することができるようになる。
ウ　ＰＣとＷｅｂサーバ間の通信データを暗号化するとともに，正当なＤＢサーバであるかを検証することができるようになる。
エ　ＰＣとＷｅｂサーバ間の通信データを暗号化するとともに，利用者を認証することができるようになる。

問 32　SIEM(Security Information and Event Management)の特徴はどれか。

ア　DMZ を通過する全ての通信データを監視し，不正な通信を遮断する。
イ　サーバやネットワーク機器の MIB(Management Information Base)情報を分析し，中間者攻撃を遮断する。
ウ　ネットワーク機器の IPFIX(IP Flow Information Export)情報を監視し，攻撃者が他者の PC を不正に利用したときの通信を検知する。
エ　複数のサーバやネットワーク機器のログを収集分析し，不審なアクセスを検知する。

13-5　暗号化技術とディジタル署名

問 1　暗号方式のうち，共通鍵暗号方式はどれか。

ア　ＡＥＳ　　イ　ＥｌＧａｍａｌ暗号　　ウ　ＲＳＡ　　エ　楕円曲線暗号

問 2　暗号方式に関する説明のうち,適切なものはどれか。

ア　共通鍵暗号方式で相手ごとに秘密の通信をする場合，通信相手が多くなるに従って，鍵管理の手間が増える。
イ　共通鍵暗号方式では，送信側と受信側で異なった鍵を用いるので，鍵の機密性が高い。
ウ　公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには，復号鍵を公開することによって，鍵管理の手間を減らす。
エ　公開鍵暗号方式では，署名に用いる鍵を公開しておく必要がある。

問 3　暗号方式に関する記述のうち，適切なものはどれか。

ア　AES は公開鍵暗号方式，RSA は共通鍵暗号方式の一種である。
イ　共通鍵暗号方式では，暗号化及び復号に同一の鍵を使用する。
ウ　公開鍵暗号方式を通信内容の秘匿に使用する場合は，暗号化に使用する鍵を秘密にして，復号に使用する鍵を公開する。
エ　ディジタル署名に公開鍵暗号方式が使用されることはなく，共通鍵暗号方式が使用される。

問 4　非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。

ア　ＡＥＳ　　イ　ＤＳＡ　　ウ　ＩＤＥＡ　　エ　ＲＳＡ

問 5　公開鍵暗号方式に関する記述として，適切なものはどれか。

ア　ＡＥＳなどの暗号方式がある。
イ　ＲＳＡや楕円曲線暗号などの暗号方式がある。
ウ　暗号化鍵と復号鍵が同一である。
エ　共通鍵の配送が必要である。

問 6　文書の内容を秘匿して送受信する場合の公開鍵暗号方式における鍵と暗号化アルゴリズムの取扱いのうち，適切なものはどれか。

ア　暗号化鍵と復号鍵は公開するが，暗号化アルゴリズムは秘密にしなければならない。
イ　暗号化鍵は公開するが，復号鍵と暗号化アルゴリズムは秘密にしなければならない。
ウ　暗号化鍵と暗号化アルゴリズムは公開するが，復号鍵は秘密にしなければならない。
エ　復号鍵と暗号化アルゴリズムは公開するが，暗号化鍵は秘密にしなければならない。

問 7　Xさんは，Yさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容を秘密にする必要があるので，公開鍵暗号方式を用いて暗号化して送信したい。電子メールの内容を暗号化するのに使用する鍵はどれか。

ア　Xさんの公開鍵　　イ　Xさんの秘密鍵
ウ　Yさんの公開鍵　　エ　Yさんの秘密鍵

問 8　ある商店が，顧客からネットワークを通じて注文（メッセージ）を受信するとき，公開鍵暗号方式を利用して，注文の内容が第三者に分からないようにしたい。商店，顧客それぞれが利用する，商店の公開鍵，秘密鍵の適切な組合せはどれか。

	商店が利用する	顧客が利用する
ア	公開鍵	公開鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	公開鍵
エ	秘密鍵	秘密鍵

問 9　社内のセキュリティポリシで，利用者の事故に備えて秘密鍵を復元できること，及びセキュリティ管理者の不正防止のための仕組みを確立することが決められている。電子メールで公開鍵暗号方式を使用し，鍵の生成はセキュリティ部門が一括して行っている場合，秘密鍵の適切な保管方法はどれか。

ア　1人のセキュリティ管理者が，秘密鍵を暗号化して保管する。
イ　暗号化された秘密鍵の一つ一つを分割し，複数のセキュリティ管理者が分担して保管する。
ウ　セキュリティ部門には，秘密鍵を一切残さず，利用者本人だけが保管する。
エ　秘密鍵の一覧表を作成し，セキュリティ部門内に限り参照できるように保管する。

問 10　通信販売の電子商取引では，受発注における改ざん，なりすまし，否認によって販売業者又は利用者に被害が及ぶ危険性がある。この三つの防止に適用できるセキュリティ技術はどれか。

ア　ウイルスチェック　　イ　ジャンクメールフィルタ
ウ　ディジタル署名　　エ　ファイアウォール

問 11　ディジタル署名に用いる鍵の組合せのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問 12　ディジタル署名付きのメッセージをメールで受信した。受信したメッセージのディジタル署名を検証することによって，確認できることはどれか。

ア　メールが，不正中継されていないこと
イ　メールが，漏えいしていないこと
ウ　メッセージが，改ざんされていないこと
エ　メッセージが，特定の日時に再送信されていないこと

問 13　ディジタル署名を通信に利用する主な目的は二つある。一つは，メッセージの発信者を受信者が確認することである。もう一つの目的はどれか。

ア　署名が行われた後でメッセージに変更が加えられていないかどうかを，受信者が確認すること
イ　送信の途中でメッセージが不当に解読されていないことを，受信者が確認すること
ウ　発信者のＩＤを受信者が確認すること
エ　秘密鍵を返送してよいかどうかを受信者が確認すること

問 14　ディジタル署名を生成するときに，発信者がメッセージのハッシュ値をディジタル署名に変換するのに使う鍵はどれか。

ア　受信者の公開鍵
イ　受信者の秘密鍵
ウ　発信者の公開鍵
エ　発信者の秘密鍵

問15 手順に示す処理を実施することによって，メッセージの改ざんの検知の他に，受信者Bができることはどれか。

〔手順〕

送信者Aの処理

(1)：メッセージから，ハッシュ関数を使ってダイジェストを生成する。

(2)：秘密に保持していた自分の署名生成鍵を用いて，(1)で生成したダイジェストからメッセージの署名を生成する。

(3)：メッセージと，(2)で生成したデータを受信者Bに送信する。

受信者Bの処理

(4)：受信したメッセージから，ハッシュ関数を使ってダイジェストを生成する。

(5)：(4)で生成したダイジェスト及び送信者Aの署名検証鍵を用いて，受信した署名を検証する。

ア　メッセージが送信者Aからのものであることの確認
イ　メッセージの改ざん部位の特定
ウ　メッセージの盗聴の検知
エ　メッセージの漏えいの防止

問16 社員が利用するスマートフォンにディジタル証明書を導入しておくことによって，当該スマートフォンから社内システムへアクセスがあったときに，社内システム側で確認できるようになることはどれか。

ア　当該スマートフォンがウイルスに感染していないこと
イ　当該スマートフォンが社内システムへのアクセスを許可されたデバイスであること
ウ　当該スマートフォンのＯＳに最新のセキュリティパッチが適用済みであること
エ　当該スマートフォンのアプリケーションが最新であること

問17 送信者からメール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者がメール本文から求めたハッシュ値とを比較することで実現できることはどれか。ここで，受信者が送信者から受け取るハッシュ値は正しいものとする。

ア　電子メールの送達の確認
イ　電子メール本文の改ざんの有無の検出
ウ　電子メール本文の盗聴の防止
エ　なりすましの防止

問18 ステガノグラフィの機能はどれか。

ア　画像データなどにメッセージを埋め込み，メッセージの存在そのものを隠す。
イ　メッセージの改ざんやなりすましを検出し，否認の防止を行う。
ウ　メッセージの認証を行って改ざんの有無を検出する。
エ　メッセージを決まった手順で変換し，通信途中での盗聴を防ぐ。

問 19 公開鍵暗号方式を採用した電子商取引において，取引当事者から独立した第三者機関である認証局（ＣＡ）が作成するものはどれか。

ア　取引当事者の公開鍵に対する電子証明書　　イ　取引当事者のディジタル署名
ウ　取引当事者のパスワード　　エ　取引当事者の秘密鍵に対する電子証明書

問 20 ＰＫＩ（公開鍵基盤）の認証局が果たす役割はどれか。

ア　共通鍵を生成する。　　イ　公開鍵を利用しデータの暗号化を行う。
ウ　失効したディジタル証明書の一覧を発行する。　　エ　データが改ざんされていないことを検証する。

問 21 ＨＴＴＰＳを用いて実現できるものはどれか。

ア　Ｗｅｂサーバ上のファイルの改ざん検知　　イ　クライアント上のウイルス検査
ウ　クライアントに対する侵入検知　　エ　電子証明書によるサーバ認証

問 22 ＩＰｖ６において，拡張ヘッダを利用することによって実現できるセキュリティ機能はどれか。

ア　ＵＲＬフィルタリング機能　　イ　暗号化機能
ウ　ウイルス検疫機能　　エ　情報漏えい検知機能

問 23 送信者Ａからの文書ファイルと，その文書ファイルのディジタル署名を受信者Ｂが受信したとき，受信者Ｂができることはどれか。ここで，受信者Ｂは送信者Ａの署名検証鍵Ｘを保有しており，受信者Ｂと第三者は送信者Ａの署名生成鍵Ｙを知らないものとする。

ア　ディジタル署名，文書ファイル及び署名検証鍵Ｘを比較することによって，文書ファイルに改ざんがあった場合，その部分を判別できる。
イ　文書ファイルが改ざんされていないこと，及びディジタル署名が署名生成鍵Ｙによって生成されたことを確認できる。
ウ　文書ファイルがマルウェアに感染していないことを認証局に問い合わせて確認できる。
エ　文書ファイルとディジタル署名のどちらかが改ざんされた場合，どちらが改ざんされたかを判別できる。

問 24 電子メールに用いられるＳ／ＭＩＭＥの機能はどれか。

ア　内容の圧縮　　イ　内容の暗号化と署名　　ウ　内容の開封通知　　エ　内容の再送

問 25 電子メールシステムにおいて、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り、選択したメールだけを利用者端末へ転送する機能、サーバ上のメールを検索する機能、メールのヘッダだけを取り出す機能などをもつものはどれか。

ア　ＩＭＡＰ４　　イ　ＭＩＭＥ　　ウ　ＰＯＰ３　　エ　ＳＭＴＰ

問 26　インターネットにおける電子メールの機密性に関する記述のうち，適切なものはどれか。

ア　電子メールの機密性を確保するためには，Ｓ／ＭＩＭＥなどを利用して暗号化の対策を講じる必要がある。
イ　電子メールの機密性を確保するためには，送信者が接続するプロバイダに受信者ＩＤの登録を依頼する必要がある。
ウ　電子メールを発信する場合，メーリングリスト内のやり取りに限定すれば，機密性は確保される。
エ　ワープロソフトなどで作成した文書ファイルを添付して送るとき，ユーザ認証用プロトコルであるＣＨＡＰを利用すれば，通信経路の途中でその内容が読まれるおそれはない。

問 27　通信の暗号化に関する記述のうち，適切なものはどれか。

ア　ＩＰｓｅｃのトランスポートモードでは，ゲートウェイ間の通信経路上だけではなく，発信ホストと受信ホストの間の全経路上でメッセージが暗号化される。
イ　ＬＤＡＰクライアントがＬＤＡＰサーバに接続するとき，その通信内容は暗号化することができない。
ウ　Ｓ／ＭＩＭＥで暗号化した電子メールは，受信側のメールサーバ内に格納されている間は，メール管理者が平文として見ることができる。
エ　ＳＳＬを使用すると，暗号化されたＨＴＭＬ文書はブラウザのキャッシュの有無が設定できず，ディスク内に必ず保存される。

問 28　ディジタルフォレンジックスの活動に含まれるものはどれか。

ア　インシデントの原因究明に必要となるデータの収集と保全
イ　自社システムを攻撃して不正侵入を試みるテストの実施
ウ　定期的なウイルスチェック
エ　パスワード認証方式からバイオメトリクス認証方式への切替え

問 29　画像などのディジタルコンテンツが，不正にコピーされて転売されたものであるかを判別できる対策はどれか。

ア　タイムスタンプ　　イ　電子透かし　　ウ　電子保存　　エ　配達証明

問 30　ディジタル署名における署名鍵の使い方と，ディジタル署名を行う目的のうち，適切なものはどれか。

ア　受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。
イ　送信者が固定文字列を付加したメッセージを，署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。
ウ　送信者が署名鍵を使って署名を作成し，それをメッセージに付加することによって，受信者が送信者を確認できるようにする。
エ　送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。

問 31　公開鍵暗号方式によって，暗号を使って n 人が相互に通信する場合，異なる鍵は全体で幾つ必要になるか。ここで，公開鍵，秘密鍵をそれぞれ一つと数える。

ア　n＋1　　イ　2n　　ウ　n(n－1)／2　　エ　$\log_2 n$

問 32　虹彩認証に関する記述のうち，最も適切なものはどれか。

ア　経年変化による認証精度の低下を防止するために，利用者の虹彩情報を定期的に登録し直さなければならない。
イ　赤外線カメラを用いると，照度を高くするほど，目に負担を掛けることなく認証精度を向上させることができる。
ウ　他人受入率を顔認証と比べて低くすることが可能である。
エ　本人が装置に接触したあとに残された遺留物を採取し，それを加工することによって認証データを偽造し，本人になりすますことが可能である。

問 33　公開鍵暗号方式を採用した電子商取引において，認証局(ＣＡ)の役割はどれか。

ア　取引当事者間で共有する秘密鍵を管理する。
イ　取引当事者の公開鍵に対するディジタル証明書を発行する。
ウ　取引当事者のディジタル署名を管理する。
エ　取引当事者のパスワードを管理する。

問 34　ディジタルフォレンジックスでハッシュ値を利用する目的として，適切なものはどれか。

ア　一方向性関数によってパスワードを復元できないように変換して保存する。
イ　改変されたデータを，証拠となり得るように復元する。
ウ　証拠となり得るデータについて，原本と複製の同一性を証明する。
エ　パスワードの盗聴の有無を検証する。

問 35　A さんが B さんの公開鍵で暗号化した電子メールを，B さんと C さんに送信した結果のうち，適切なものはどれか。ここで，A さん，B さん，C さんのそれぞれの公開鍵は 3 人全員がもち，それぞれの秘密鍵は本人だけがもっているものとする。

ア　暗号化された電子メールを，B さんだけが，A さんの公開鍵で復号できる。
イ　暗号化された電子メールを，B さんだけが，自身の秘密鍵で復号できる。
ウ　暗号化された電子メールを，B さんも，C さんも，B さんの公開鍵で復号できる。
エ　暗号化された電子メールを，B さんも，C さんも，自身の秘密鍵で復号できる。

問 36　ＰＫＩにおける認証局が，信頼できる第三者機関として果たす役割はどれか。

ア　利用者からの要求に対して正確な時刻を返答し，時刻合わせを可能にする。
イ　利用者から要求された電子メールの本文に対して，ディジタル署名を付与する。
ウ　利用者やサーバの公開鍵を証明するディジタル証明書を発行する。
エ　利用者やサーバの秘密鍵を証明するディジタル証明書を発行する。

問 37　情報セキュリティにおけるタイムスタンプサービスの説明はどれか。

ア　公式の記録において使われる全世界共通の日時情報を，暗号化通信を用いて安全に表示するＷｅｂサービス
イ　指紋，声紋，静脈パターン，網膜，虹彩などの生体情報を，認証システムに登録した日時を用いて認証するサービス
ウ　電子データが，ある日時に確かに存在していたこと，及びその日時以降に改ざんされていないことを証明するサービス
エ　ネットワーク上のＰＣやサーバの時計を合わせるための日時情報を途中で改ざんされないように通知するサービス

問 38　電子メールの送信時に，送信者を送信側のメールサーバで認証するためのものはどれか。

ア　ＡＰＯＰ　　イ　ＰＯＰ３Ｓ　　ウ　Ｓ/ＭＩＭＥ　　エ　ＳＭＴＰ-ＡＵＴＨ

問 39　IoT デバイスの耐タンパ性の実装技術とその効果に関する記述として，適切なものはどれか。

ア　CPU 処理の負荷が小さい暗号化方式を実装することによって，IoT デバイスとサーバとの間の通信経路での情報の漏えいを防止できる。
イ　IoT デバイスに GPS を組み込むことによって，紛失時に IoT デバイスの位置を検知して捜索できる。
ウ　IoT デバイスに光を検知する回路を組み込むことによって，ケースが開けられたときに内蔵メモリに記録されている秘密情報を消去できる。
エ　IoT デバイスにメモリカードリーダを実装して，IoT デバイスの故障時にはメモリカードを IoT デバイスの予備機に差し替えることによって，IoT デバイスを復旧できる。