Ｃｈａｐｔｅｒ１３　セキュリティ

１３－１　ネットワークに潜む脅威〔解答・解説〕

問１　イ
〔解説〕情報セキュリティの３つの特性とは，機密性（Confidentiality），完全性（Integrity），可用性（Availability）であり，ＣＩＡと呼ばれる。

問２　ウ
〔解説〕ア　ＩＴセキュリティ評価及び認証制度(ＪＩＳＥＣ)の説明
イ　プライバシーマーク制度の説明
エ　暗号モジュール試験及び認証制度（ＪＣＭＶＰ)の説明

問３　ウ
〔解説〕ア　社内全体に広めることでセキュリティに対する意識の向上を図る
イ　ビジネス環境や技術の変化に伴い，常に改良するべきである
エ　ＩＳＭＳの適用範囲のすべてのシステムに対してリスクアセスメントを行う

問４　ウ
〔解説〕リスクアセスメントとは，リスク分析によって得られたリスクが顕在化した場合の損失額と発生確率の予測から対応の優先順位を付けることである。

問５　エ
〔解説〕ア　「リスク移転」とは，保険に加入するなどリスクを第三者に肩代わりさせることである
イ　「リスク回避」とは，個人情報を保有しないなどリスクの原因を除去することである
ウ　「リスク低減」とは，機密情報の暗号化をしないなど損失の発生率を低下させることである

問６　イ
〔解説〕リスク移転とは，保険に加入するなどしてリスクを第三者へ移転させることをいう。

問７　エ
〔解説〕リスクファイナンシングとは，リスクが顕在化した場合に備えて，保険に加入するなどして損失の補てんや対応費用などを確保しておくことである。

問８　エ
〔解説〕情報セキュリティマネジメントシステム（ＩＳＭＳ）とは，情報に関するセキュリティを管理するための制度であり，その確立のための要求事項として
１．リスク対策のために選択肢を識別し，評価すること。
２．リスク対応のための，管理目的及び管理策を選択すること。
３．適用宣言書を作成すること。
の３つがＩＳＯにより定義されている。

問 9　イ
〔解説〕真正性：
　利用者、プロセス、システム、情報などが、主張どおりであることを確実する特性のこと
信頼性：
　情報システムによる処理に欠陥や不具合がなく、期待した処理が確実に行われている特性のこと

a：信頼性(Reliability)の定義
b：真正性(Authenticity)の定義
c：可用性(Availability)の定義
d：機密性(Confidentiality)の定義

適切な対応は真正性＝b、信頼性＝a なので、正解は「イ」。

問 10　イ
〔解説〕リスクアセスメントは、リスクを見つけ、発見されたリスクの大きさを評価し、そのリスクが許容できるか否かを決定する一連の活動。

問 11　エ
〔解説〕ＡＥＳ-２５６は、共通鍵暗号方式であるＡＥＳのうち、鍵長２５６ビットの暗号鍵を用いて暗号化／復号を行う方式のこと。鍵長２５６ビットということは、2^{256}種類の鍵の中でいずれか１つが使用されているということなので、正しい平文に戻すためには最大で2^{256}回の試行が必要。

問 12　ア
〔解説〕C&C サーバは、攻撃者がマルウェアに対して指令コマンドを送信し、マルウェアに感染した支配下のコンピュータ群(ボットネット)の動作を制御するために用いられる外部の指令サーバ(C&C＝コマンド&コントロール)。

問 13　ア
〔解説〕ＣＳＩＲＴマテリアルは、組織的なインシデント対応体制である「組織内ＣＳＩＲＴ」の構築を支援する目的で作成されたガイドライン。ＩＴセキュリティに対応する為の情報およびノウハウが提示されている。
イ　ＩＳＭＳユーザーズガイドは、ＩＳＭＳ認証基準(JIS Q 27001:2014)の要求事項について一定の範囲でその意味するところを説明しているガイド
ウ　証拠保全ガイドラインは、電磁的証拠の保全手続きの参考として、様々な事案について広く利用できるように策定された指針
エ　組織における内部不正防止ガイドラインは、組織が管理する情報と情報システムに対する内部不正の防止、および不正行為発生時の早期発見と拡大防止のための体制の整備を推進する為の指針

問 14　ア
〔解説〕イ　信頼性は、「意図する行動と結果が一貫しているという特性」と定義されている
ウ　責任追跡性は、情報資産に行われたある操作についてユーザと動作を一意に特定でき、過去に遡って追跡できる特性のこと
エ　否認防止は、「主張された事象又は処理の発生，及びそれを引き起こしたエンティティを証明する能力」と定義されている

13-2 ユーザ認証とアクセス管理〔解答・解説〕

問 1　ア
〔解説〕イ　QR コードは、携帯電話での URL の読取りや、販売店や工場における在庫管理などにも利用される二次元コードの規格
ウ　短縮 URL は、長くなりがちな URL を20文字程度に短縮する仕組みです。リダイレクトを利用することで本来の URL に接続できるようになっている
エ　トラックバック ping は、ブログシステムに組み込まれている機能の1つで、他のブログページへのハイパリンクを設置した際に、そのハイパリンクを設置した事実やその設置ページの情報をリンク先ブログに通知する仕組み

問 2　ウ
〔解説〕ア　１度使用された利用者ＩＤやパスワードを再利用することは望ましくない
イ　一覧表を作成すると情報が漏洩する可能性がある
エ　利用者登録申請書がきてから利用者ＩＤとパスワードを登録すべきである

問 3　エ
〔解説〕ア　辞書攻撃の説明
イ　リバースブルートフォースアタック攻撃(逆総当たり攻撃)の説明
ウ　ブルートフォース攻撃(総当たり攻撃)

問 4　ア
〔解説〕ブルートフォース攻撃とは，パスワードの解読のため，あらゆる文字の組合せを総当たりで入力する方法である。

問 5　ウ
〔解説〕ア　RADIUS認証の説明。
イ　二要素認証の説明。
エ　パスワードリマインダの説明。

問 6　ウ
〔解説〕ア、エ　ＩＤのハッシュ値とパスワードのハッシュ値は一致しないので意味のない比較である
イ　認証にパスワードが使用されていないので不適切である

問 7　イ
〔解説〕キーロガーとは，キーボードからの入力を監視して記録するハードウェア及びソフトウェアの総称であり，不特定多数のユーザが利用するＰＣ上でパスワードが盗まれるなどの被害が発生している。
アはソーシャルエンジニアリング行為、ウは辞書攻撃、エはウォードライビングの説明。

問 8　イ
〔解説〕虹彩の模様は妊娠期間中にランダムに決まるため、双子や親子などでもパターンが違い、経年による変化もないため、バイオメトリクス認証として使用されます。

問 9　エ

〔解説〕シングルサインオン(Single Sign-On, SSO)は、ユーザ認証を一度受けるだけで許可された複数のサーバへのアクセスについても認証する技術。

ア　クッキーはサーバで生成され、クライアントのコンピュータに保存される。

イ　クッキーの有効範囲は同一ドメイン内のページに限られている。異なるドメインに配置されたシステムは他のドメインで生成されたクッキーにアクセスすることができないので認証を行うことはできないん。

ウ　Webサーバには認証を行わないとアクセスできないようにしたいので、リバースプロキシと同一ドメインに配置しなくてはならない。

問 10　エ

〔解説〕生体認証（バイオメトリクス）システムでは，ＦＲＲ（本人拒否率）とＦＡＲ（他人受入率）は反比例関係にあるため，双方を勘案して装置を調整する必要がある。

問 11　ウ

〔解説〕ア　メモリに関する規定はない

イ　接触型ＩＣカードの方が適している

エ　ＬＥＤ照明でも正常に認証できる

問 12　ウ

〔解説〕特権的アクセス権とは、システム上のあらゆる作業を可能にする強力な操作権限のことで、システムを管理する役割を持つ管理者ＩＤ／特権ユーザなどに与えられます。

問13　ア

〔解説〕イ　情報が外部に意図せずに漏えいすることを防ぐために業務のメールを個人のメールアドレスに転送する設定になっていないかを確認する

ウ　組織内で許可されたソフトウェア以外のもの（例えば、ファイル共有ソフト※等）をインストールして利用することを禁止する

エ　従業員の判断ではなく組織で判断することが求められる

問 14　エ

〔解説〕ア　ログの保存期間は、リスクとコストのバランスによって決定する

イ　ログの確認には、特定のシステム管理者からのみアクセス可能等の措置が取られていることが望まれる

ウ　ログ保存期間は、内部不正の抑止の観点から内部者に知らせないことが望まれる

問 15　エ

〔解説〕ＶＰＮ（Virtua Private Network）とは，暗号化やトンネリング（各ネットワークのプロトコルをＩＰプロトコルでカプセル化すること）を利用し，インターネット上にプライベートネットワークを構築することである。

ア　暗号化は必要である

イ，ウ　暗号化により盗聴・改ざんを防止することができる

問 16　エ

〔解説〕ＲＡＤＩＵＳ(Remote Authentication Dial In User Service）は，電話回線などを通じてサーバにダイヤルアップしたユーザを認証するシステムで，無線ＬＡＮやＶＰＮなどにも利用されている。

問17　エ
〔解説〕ア　組織の情報セキュリティマネジメントシステムの仕様を定めた規格
イ　情報技術の製品及びシステムのセキュリティ特性を評価するためのＪＩＳ規格
ウ　公開鍵証明書の標準形式や証明書パス検証アルゴリズムなどを定めたもの

問 18　イ
〔解説〕標的型攻撃メールとは，特定の企業や組織，個人に対して，取引先や知人などになりすましてウイルスに感染させるメールを送信するものである。

問 19　ウ
〔解説〕セキュアブートとは、コンピュータの起動時にＯＳ起動ファイルやドライバのディジタル署名を検証し、起動プロセスを認証することで、不正なプログラムの実行を未然に防止する仕組み。
ア　ＢＩＯＳパスワードの説明
イ　ＨＤＤパスワードの説明
エ　セキュアブートは OS 起動前のマルウェア実行を防ぐ技術

問 20　エ
〔解説〕ＢＹＯＤ（Bring Your Own Device）とは，従業員が個人所有のＰＣやスマートフォンなどの情報端末を職場に持ち込み，それを業務に使用することである。

問 21　イ
〔解説〕キーロガー(Keylogger)は、ＰＣへのキーボードやマウス入力を逐一監視し、それを記録するソフトウェアまたはハードウェアのこと
ア　プロキシサーバを悪用した中間者攻撃
ウ　アドウェアを悪用した例
エ　ブラウザのアドオンを悪用した例

問 22　エ
〔解説〕ア　ＭＡＣアドレスフィルタリングは、無線ＬＡＮのアクセスポイントに正当な機器のＭＡＣアドレスを登録しておくことで、正当な機器以外からのアクセスを拒否する機能。しかし、ＭＡＣアドレスが偽装された場合には接続を拒否できない。
イ　ＳＳＩＤを秘匿にするためにはアクセスポイントにＳＳＩＤステルスの設定を行う。これにより、アクセスポイントから発せられるビーコンにＳＳＩＤの情報が含まれなくなるため、第三者にアクセスポイントのＳＳＩＤを知られてしまう危険性を小さくできる。
ウ　不正アクセスポイントの設置は、ＳＳＩＤや暗号化キーを類推できないものにすることがある程度の対策になる。問題では、公開情報であるドメイン名をＳＳＩＤとして設定するとしており不適切。

問 23　ア
〔解説〕イ　特定の文字数および文字種で設定される可能性のある組合せのすべてを試すことで不正ログインを試みるパスワードクラック手法
ウ　ブルートフォースとは逆に、パスワードを固定し、利用者ＩＤを総当りで試していくことで不正ログインを試みるパスワードクラック手法
エ　想定され得るパスワードとそのハッシュ値との対のリストを用いて、入手したハッシュ値からパスワードを効率的に解析する攻撃

問 24　ウ
〔解説〕フォールスネガティブ（False Negative）：
　本来は検知すべき悪意のある活動を、誤って害のないものとして分類すること。検知漏れ。

フォールスポジティブ（False Positive）：
　本来は通過させるべき害のない活動を、誤って悪意のあるものとして分類すること。過剰検知。
ア　適切な処理であり、誤検知とは関係ない。
イ　フォールスポジティブに該当する。
エ　適切な処理であり、誤検知とは関係ない。

問 25　ア
〔解説〕ポートスキャナは、検査対象のコンピュータやルータの全て(または特定範囲)の通信ポートに信号を送ることで、サービスの稼働状態を外部から調査するツール。

問 26　イ
〔解説〕ＳＰＦ(Sender Policy Framework)は、ＳＭＴＰ接続してきたメールサーバのＩＰアドレスをもとに、正規のサーバから送られた電子メールかどうかを検証する技術
ア　ＳＰＦではディジタル署名を使用しない。記述はＤＫＩＭの仕組み
ウ　メールの誤送信を防止するのための仕組み
エ　メールアーカイブシステムの仕組み

問 27　ウ
〔解説〕ア　ＦＲＲとＦＡＲの関係はトレードオフ(何かを得れば何かを失う)
イ　ＦＲＲを減少させると，ＦＡＲは増大する
エ　ＦＲＲを増大させると，ＦＡＲは減少する

問28　イ
〔解説〕ルートキット(ｒｏｏｔｋｉｔ)は、攻撃者がシステムへ不正侵入した後に侵入した痕跡を隠蔽したり、再び侵入するためのバックドアを設置するための機能をまとめたソフトウェア群。

問 29　ア
〔解説〕コンピュータセキュリティ用語としての「バックドア」は、一度不正侵入に成功したコンピュータやネットワークにいつでも再侵入できるように攻撃者によって設けられた仕掛けのことを指す。
イ　ポートスキャナの説明。
ウ　ミラーポートの説明。
エ　バッファオーバフロー攻撃の説明。

13-3　コンピュータウイルスの脅威〔解答・解説〕

問 1　ウ
〔解説〕ア　特定のサーバに過大な負荷をかけてサービスを停止させる攻撃
イ　辞書に登録されている単語を片っ端から入力し，パスワードや暗号の解読を行う攻撃
エ　バッファを超えるような入力を行ない，オーバフローさせてシステムをダウンさせる攻撃

問 2　ア
〔解説〕イ　既知のウイルスやその亜種の検出に有効な手法である
ウ　ウイルスに感染しているかどうかを確認するのに有効な手法である
エ　ウイルスの動作から，未知のウイルスを検出するのに有効な手法である

問 3　エ
〔解説〕ビヘイビア法とは，検査対象プログラムを安全な環境で動作させ，その挙動を監視することにより，そのプログラムが実際に行なう行為を検知するウイルス検出手法である。

問 4　エ
〔解説〕ア　パターンマッチング法の説明
イ　チェックサム法の説明
ウ　コンペア法の説明

問 5　イ
〔解説〕ア　定義ファイルの更新前にウイルス感染している可能性があるので，すべてのファイルをスキャンするべきである
ウ　使用しないＴＣＰポート宛の通信を禁止しても，電子メールの添付ファイルを介したウイルス感染には効果がない
エ　クライアントＰＣにグローバルＩＰアドレスを付与すると，インターネットから直接アクセスすることが可能になるので，ワームに感染する危険性が高まる

問 6　イ
〔解説〕実行ファイルをアセンブリ言語に逆変換することを逆アセンブルという。
ソースコードを入手することができないソフトウェアでも、機械語ではなくプログラマが理解しやすいアセンブリ言語に変換することで内部の動作を解析することができるようになる。

問 7　イ
〔解説〕フィッシングとは，偽のサイトへ誘導し，個人情報などを詐取する攻撃である。

問 8　ウ
〔解説〕ＤＮＳサーバには問合せにより検索したドメインのＩＰアドレスを一時的にキャッシュする機能があり，ＤＮＳキャッシュポイズニングはこのキャッシュ情報を不正に書き換え，偽の情報を返すことで，利用者を偽のＷｅｂサーバに誘導する攻撃手法である。

問 9　イ
〔解説〕ア　ポートスキャンの説明
ウ　ＤＮＳリフレクション攻撃の説明
エ　ゾーン転送を悪用した登録情報の収集

問 10　ア
〔解説〕イ　ＸＳＲＦ(クロスサイトリクエストフォージェリ)の説明
ウ　ワームの一種 ＳＱＬ Ｓｌａｍｍｅｒの説明
エ　ＸＳＳ(クロスサイトスプリクティング)の説明

問 11　ア
〔解説〕イはクラッキング，ウはバッファオーバフロー，エはディレクトリトラバーサルの説明である。

問 12　ウ
〔解説〕クロスサイトスクリプティングとは，Ｗｅｂサイトに攻撃用のスクリプトを混入させ，被害者のブラウザ上で実行させる攻撃であり，危険な文字を検出し，置換・除去を行うことで防ぐことができる。

問 13　ア
〔解説〕ＳＱＬインジェクション攻撃は、データベースを扱うアプリケーションのセキュリティ上の不備を悪用して、データベースシステムを不正に操作するＳＱＬ文を発行させる攻撃手法

イ　クロスサイトスクリプティング(ＸＳＳ)を防ぐ方法
ウ　ディレクトリトラバーサル攻撃を防ぐ方法
エ　バッファオーバフロー攻撃を防ぐ方法

問 14　イ
〔解説〕ア　変更管理の活動
ウ　問題管理の活動
エ　問題管理の活動

問 15　エ
〔解説〕ア　ランサムウェアの特徴
イ　どちらのマルウェアも単独で動作可能
ウ　トロイの木馬の特徴

問 16　ア
〔解説〕イ　クロスサイトリクエストフォージェリの説明
ウ　ＳＱＬ　Ｓｌａｍｍｅｒなどのセキュリティホールを付いて感染を広げるタイプのワームの説明
エ　クロスサイトスクリプティングの説明

問 17　ア
〔解説〕VBScript で作られたコンピュータウィルスは、メール本文や Web ページなどの HTML 形式の文書に埋め込まれ、閲覧したと同時に実行されるスクリプトによってコンピュータを感染させるという特徴を持つ。
イ　感染対象は Microsoft Windows がインストールされたコンピュータのみです。
ウ　マクロウィルスの特徴です。
エ　ブートセクタウィルスの特徴です。

問 18　ウ
〔解説〕ア　サニタイジングの説明
イ　ポートスキャンツールの説明
エ　辞書攻撃を行うパスワードクラックツール

問 19　イ
〔解説〕ブルートフォース攻撃：パスワードクラックや暗号鍵の解読に用いられる手法の 1 つで、特定の文字数および文字種で設定される可能性のあるすべての組合せを試すことで不正ログインを試みる攻撃手法
ア　セッションハイジャックの説明
ウ　キーロガーの説明
エ　リプレイアタックの説明

問 20　エ
〔解説〕ア　ＯＳコマンドインジェクション攻撃の説明
イ　ＳＱＬインジェクション攻撃の説明
ウ　不正アクセスの事例

問 21　イ
〔解説〕オープンリダイレクト：URL パラメタやフォームデータなどの外部パラメタによって指定された Web ページに遷移するようにしている Web アプリケーションが、実装不備により、無制限に URL を受け入れてしまう状態
ア　標的型攻撃メールやフィッシングの例
ウ　DNS アンプ攻撃（DNS リフレクタ攻撃）の説明
エ　踏み台攻撃の説明

13-4　ネットワークのセキュリティ対策〔解答・解説〕

問 1　エ
〔解説〕ＷＡＦ（Web Application Firewall）とは，Ｗｅｂアプリケーションへの通信内容を検査して攻撃を防ぐファイアウォールであり，ＳＱＬインジェクション攻撃やクロスサイトスクリプティング攻撃などを遮断できる。アはペネトレーションテスト、イはＳＳＬアクセラレータ、ウはインタビュー法の説明である。

問 2　ア
〔解説〕ＷＡＦ（Web Application Firewall）とは，Ｗｅｂアプリケーションの脆弱性を悪用した攻撃などからＷｅｂアプリケーションを保護するソフトウェアまたはハードウェアのことである。

問 3　ア
〔解説〕イ　ＷＰＡ２(Wi-Fi Protected Access 2)の説明
ウ　ＳＩＥＭ(Security Information and Event Management)の説明
エ　ＵＴＭ(Unified Threat Management)の説明

問 4　エ
〔解説〕パケットフィルタリングとは，条件に合ったポート番号をもったパケットだけを内部ネットワークに通す機能をいう。
ア，イ　パケットに改ざんがあるかどうかをチェックすることはできない
ウ　ＮＡＰＴ（Network Address Port Translation）の説明である

問 5　ア
〔解説〕パケットフィルタリングとは，パケットのＩＰアドレスやポート番号，通信の方向などから中継の可否を判断する機能である。ネットワークサービスにはポート番号が振られているので，外部に公開していないサービスのポート番号があて先になっていれば，パケットを破棄すればよい。

問 6　イ
〔解説〕ＨＴＴＰはＷｅｂサーバへのアクセスに必要なので禁止できない。

問 7　エ
〔解説〕ア　暗号モジュール試験の目的
イ　ブラックボックステストの目的
ウ　負荷テストの目的

問 8　ア
〔解説〕「ルール一覧に示す番号の１から順にルールを適用」と記述されているので,最初に番号の１を見る。ルール一覧の番号の１は,送信元アドレスが１０.１.２.３のパケットならば,宛先アドレス,プロトコル,送信元ポート番号,宛先ポート番号は任意（何でもかまわない）となっている。パケットＡの送信元アドレスは１０.１.２.３なので,このルールが適用されて通過禁止になる。

問 9　イ
〔解説〕ア　ボットの説明
ウ　マルチプラットホーム型マルウェアの説明
エ　ステルス型マルウェアの説明

問 10　ウ
〔解説〕アはＮＡＰＴ，イはＤＨＣＰ，エはＤＮＳの説明である。

問 11　エ
〔解説〕アはＤＮＳ，イはＤＨＣＰ，ウはＮＡＰＴの説明である。

問 12　ア
〔解説〕ダウンロード型マルウェアは、感染したコンピュータのユーザに気付かれないようにインターネット上の悪意のあるＷｅｂサイトに接続し、他のマルウェアをダウンロードして感染を拡散させるタイプのウイルス(またはマルウェア)です。

問 13　ウ
〔解説〕電子メールの誤送信の多くは，送信者が宛先メールアドレスを間違えることで発生するため，送信時にシステムが宛先アドレスを確認することで，誤送信を減らすことができる。
※ＯＰ２５Ｂ（Outbound Port 25 Blocking）
ＩＳＰ管理外ネットワークへのＳＭＴＰ（ポート番号２５）送信の送信を遮断することで，スパムメールの拡散を防止する方法。
※ＳＰＦ（Sender Policy Framework）
送信元メールアドレスの送信ドメインを検証することでメールアドレスの偽装を検出し，フィッシング詐欺などを防止する方法。

問 14　エ
〔解説〕コンテンツフィルタリングとは，送信する電子メールに情報漏えい対象となるキーワードが含まれていないかチェックし，含まれているものの送信を遮断する手法である。

問 15　ウ
〔解説〕ア　ＩＰアドレスの割当て範囲を変更しても，参加者の端末以外からの接続を防止することはできない
イ　ＵＲＬフィルタリングは特定のＷｅｂサイトへのアクセスを遮断する機能であり，参加者の端末以外からの接続を防止することはできない
エ　プライバシセパレータは同じアクセスポイントに接続している子機同士のアクセスを禁止する機能であり，参加者の端末以外からの接続を防止することはできない

問 16　エ
〔解説〕ア　ステガノグラフィの説明
イ　ペネトレーションテストの説明
ウ　ソーシャルエンジニアリングの説明

問 17　ア
〔解説〕否認防止(Non-Repudiation)：情報セキュリティマネジメントの付加的な要素で、行った操作や発生した事象を後になって否認されないように証明できる能力
イ　可用性の説明
ウ　機密性の説明
エ　信頼性の説明

問 18　イ
〔解説〕クライアントがサーバに対してサービスを要求するパケットを送信する際には、ポート番号にサービスを意味する番号を指定する。通常、HTTP ではポート 80 番(HTTPS は 443 番)を使用して通信を行いますが、ポート 8080 番は代替 HTTP ポートと呼ばれ、大抵のプロキシサーバは 8080 番でサービスを待ち受けている。

問 19　ア
〔解説〕ア　アプリケーションゲートウェイ方式では、アプリケーション層レベルでコネクションを中継するため、HTTP，FTP，SMTP などアプリケーションプログラムごとに別々の中継プログラムを用意する必要がある。
イ　サーキットゲートウェイ方式は、ペイロード部をチェックしないためアプリケーション層レベルの情報である"コマンド"によるフィルタリングには対応していない。
ウ　トランスポートゲートウェイ方式は、トランスポート層レベルでコネクションを中継するため、アプリケーションプログラムの形式に依存することはない。
エ　パケットフィルタリング方式は、パケットのヘッダ部の内容に基づいてフィルタリングを行う方式。電子メールの内容はパケットのペイロード部に格納されているためパケットフィルタリングではその内容をチェックすることができない。

問 20　イ
〔解説〕ディジタルフォレンジックス：
不正アクセスや情報漏えいなどのセキュリティインシデントの発生時に、原因究明や法的証拠を明らかにするために対象となる電子的記録を収集・解析すること
フォレンジックプロセスは、収集・検査・分析・報告の 4 つのフェーズから成る。
収集：
データの潜在的なソースを識別し、それらのソースからデータを取得する
検査：
収集したデータから関連する情報を評価して抽出する
分析：
複数のソースのデータを相互に関連付けるなどして、結論を導き出すためにデータの調査と分析を行う
報告：
分析フェーズによって得られた情報を準備して提示する

「イ」の作業は、収集フェーズに該当する。

問 21　ウ
〔解説〕ア、イ　可用性は向上しますが耐タンパ性は高まらない
エ　システムのセキュリティ向上には寄与するが、ＩＣカード自体の耐性が高まる訳ではないため誤り

問 22　ウ
〔解説〕サイバーセキュリティ経営ガイドラインは、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（ＣＩＳＯ等）に指示すべき「重要１０項目」をまとめたもの。
[3 原則]
•セキュリティ投資にリターンは望めないので、経営者がリーダシップをとって対策を推進すべきである。
•系列企業やサプライチェーンのビジネスパートナ等を含めたセキュリティ対策が必要である。
•平時からのセキュリティ対策に関する情報開示など、ステークホルダとの適切なコミュニケーションが必要である。

問 23　ウ
〔解説〕SHA-256：は入力値から 256 ビットの文字列を生成するハッシュ関数
ア　メッセージダイジェスト(値 B)からディジタル署名を生成するには、ハッシュ関数ではなく公開鍵暗号を使用しなければならない。ハッシュ関数だと利用者側で復号することができないからである。又、正しくディジタル署名を生成したとしてもファイル作成者を確認することはできない。
イ　「ア」と同じ理由で誤り。
エ　改ざん部位の特定はできない。

問 24　ウ
〔解説〕インターネット通信に使われるプロトコルは HTTP(HyperText Transfer Protocol)で、ポート番号は 80。このため、インターネット上の Web サーバにアクセスできるようにするには、内部から Web サーバの 80 番ポートに向けた発信パケット(HTTP リクエスト)、および逆向きの、Web サーバのポート 80 からクライアント PC の 1024 番以上に向けた応答パケット(HTTP レスポンス)の通過を許可する必要がある。

問 25　ウ
〔解説〕ＣＳＩＲＴ(Computer Security Incident Response Team，シーサート)は、対象とする範囲でセキュリティ上の問題が起きていないかどうかを監視するとともに、セキュリティインシデントの発生時に対応にあたるチームや組織の総称。
ア　ＩＣＡＮＮ(The Internet Corporation for Assigned Names and Numbers，アイキャン)の説明
イ　ＩＥＴＦ(Internet Engineering Task Force)の説明
エ　ハクティビスト(Hacktivist)の説明

問 26　ア
〔解説〕ボットネットとは，ボット(感染したコンピュータを，インターネット経由で外部から操ることを目的とした不正プログラム)に感染した，複数のコンピュータで構成されたネットワーク。

問 27　エ
〔解説〕ア　送達確認がとれるような仕組みはない
イ　第三者が同じ手順によって送信元を偽装したメールを送信しても、なりすましを検出できる仕組みはない
ウ　暗号文や共通鍵の暗号化データが改ざんされた場合、正しく復号できないので改ざんに気付くことはできるが、改ざん箇所の修正はできない

問 28　エ
〔解説〕アクセス権限は必要最低限の権限を設定するべきである。
「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」は,データベースの情報を変更する必要がないので,参照権限だけがあればよい。

問 29　ウ
〔解説〕ＳＭＴＰ(Simple Mail Transfer Protocol)は、電子メールを転送するプロトコルで通信に
ＴＣＰ/２５ポートを使用する。
ＰＣ(クライアント)はｗｅｌｌ－ｋｎｏｗｎポートでない１０２４番以降のポートを通信に使用する。

問30　エ
〔解説〕①の条件により２～９９の範囲,１０２～９９９のそれぞれから１個ずつ計２個。
②の条件により０,１,１００,１０１,１０００,１００１の６個。
したがって２個＋６個＝８個

問 31　エ
〔解説〕設問の事例は DMZ を介した通信になっているので、コネクションを確立するのは利用者 PC と Web サーバ、Web サーバと DB サーバの組みになる。そして、ディジタル証明書は利用者個人のものですので利用者認証のために使用する。
ア　利用者 PC と通信を行うのは Web サーバ。また、利用者個人のディジタル証明書は利用者の認証に使用する。
イ　DMZ を介した通信なので利用者 PC と DB サーバは通信を行わない。利用者 PC と通信を行うのは Web サーバ。
ウ　利用者個人のディジタル証明書は利用者の認証に使用する。

問 32　エ
〔解説〕SIEM(シーム)は、OS、データベース、アプリケーション、ネットワーク機器など多様なソフトウェアや機器が出力する大量のログデータを分析し、異常があった場合に管理者に通知したり対策を知らせたりする仕組み。
ア　ファイアウォールや IPS などの特徴。
イ　SNMP(Simple Network Management Protocol)の特徴。
ウ　Cisco 社の NetFlow の特徴。

13-5　暗号化技術とディジタル署名〔解答・解説〕

問 1　ア
〔解説〕イ　非常に大きな数の離散対数問題を解くことが困難であることを利用した公開鍵暗号方式
ウ　けた数の大きな数の素因数分解に膨大な時間がかかることを利用した公開鍵暗号方式
エ　楕円曲線上の離散対数問題を解くことが困難であることを利用した公開鍵暗号方式

問 2　ア
〔解説〕共通鍵暗号方式では，通信相手ごとに使用する鍵が異なるため，通信相手が多くなると鍵の管理が煩雑になる。例えば、A，B，Cの３人で共通鍵暗号方式を用いて通信を行うと、A－B間，A－C間，B－C間用の鍵３種類，A，B，C，Dの４人で共通鍵暗号方式を用いて通信を行うと、A－B間，A－C間，A－D間，B－C間，B－D間，C－D間用の鍵６種類が必要になる。

問 3　イ
〔解説〕ア　記述とは逆で、AESは共通鍵暗号方式、RSAは公開鍵暗号方式
ウ　公開鍵暗号方式では、暗号化鍵を公開し復号鍵は厳重に管理する。誰でも暗号化できますが、復号できるのは正当な受信者だけという考え方
エ　ディジタル署名は、共通鍵暗号方式ではなく公開鍵暗号方式を応用した技術

問 4　エ
〔解説〕ＲＳＡ暗号を解読するには巨大な整数を素因数分解する必要があり，事実上解読不可能とされている。

問 5　イ
〔解説〕ア，ウ，エは共通鍵暗号方式の説明である。

問 6　ウ
〔解説〕公開鍵暗号方式では，暗号化鍵を公開し復号鍵を秘密にすることで，暗号化は誰にでもできるが，復号化ができるのは正当な受信者だけとなる。暗号化アルゴリズムは秘密にしなくてもよい。

問 7　ウ
〔解説〕暗号化されたメールは受信者のみが復号できるようにしなければならないため,受信者の秘密鍵で復号することになる。秘密鍵と公開鍵はペアで作成するため,受信者の秘密鍵で復号できるデータを暗号化した鍵は「受信者の公開鍵」となる。

問 8　ウ
〔解説〕顧客が公開鍵を用いて注文内容を暗号化すれば，商店の秘密鍵を用いないと復号できない。

問 9　イ
〔解説〕ア　鍵の生成はセキュリティ部門が一括して行っているので、セキュリティ管理者による不正の可能性がある
ウ　事故が起こった場合の復元方法が考慮されていないので不適切
エ　セキュリティ管理者による不正の可能性がある

問 10　ウ

問 11　エ
〔解説〕ディジタル署名の作成に用いるのは"秘密鍵"、検証に用いるのは"公開鍵"である。

問 12　ウ
〔解説〕ディジタル署名によって，送信者本人の正当性及びメッセージの改ざんの有無を検証できる。

問 13　ア
〔解説〕メッセージを元に署名を作成するので，メッセージに変更が加えられていれば受信側で復元したときに検知することができる
イ　盗聴されたかどうかの検知はできない
ウ　発信者のＩＤを確認することはできない
エ　秘密鍵の送信は行われない

問 14　エ
〔解説〕ディジタル署名の手順は、
1.送信者は、平文をハッシュ関数で圧縮したメッセージダイジェストを”送信者の秘密鍵”で暗号化し、平文と一緒に送信する
2.受信者は、受信したメッセージダイジェストを”送信者の公開鍵”で復号し、受信した平文をハッシュ関数で圧縮したものと比較する
3.一つの平文からハッシュ関数によって生成されるメッセージダイジェストは常に同じになるため、送信者から送られてきたメッセージダイジェストと、受信側でハッシュ化したメッセージダイジェストが同じなら、通信内容が改ざんされていないことが証明される

問 15　ア
〔解説〕イ　改ざん部位を特定する機能は持たない
ウ　通信経路上での盗聴を検知する仕組みはない
エ　メッセージ本文は暗号化しないので情報漏えいの防止はできない

問 16　イ
〔解説〕ディジタル証明書とは，認証局（ＣＡ）によって署名された，サーバやデバイスの正当性を証明するための証明書である。

問17　イ
〔解説〕ディジタル署名の説明であり，実現できるのはなりすましの検知及びメール本文の改ざんの検知である。

問 18　ア
〔解説〕ステガノグラフィ(Steganography)とは、音声や画像などのデータの中に、別のデータ(多くの場合文字列)を秘密裏に埋め込む技術や考え方のこと。イはディジタル署名、ウはＭＡＣ、エは暗号化通信の機能。

問 19　ア
〔解説〕認証局（ＣＡ：Certificate Authority）とは，公開鍵を登録しておき，その鍵が正当であることを保証する機関である。

問 20　ウ
〔解説〕認証局では，ＣＲＬ（秘密鍵の漏えいや被発行者の規則違反などにより有効期間中に失効したディジタル証明書のリスト）を発行する。

問 21　エ
〔解説〕ＨＴＴＰＳ（HTTP over SSL/TLS）とは，Ｗｅｂサーバとブラウザ間のＨＴＴＰ通信を暗号化して送受信するプロトコルであり，サーバはクライアントに電子証明書を送信し，クライアントがサーバ認証を行う。

問 22　イ
〔解説〕ＩＰｖ６の拡張ヘッダは、ＩＰｖ６ヘッダとＴＣＰ/ＵＤＰヘッダの間に挿入される、フラグやオプション情報を追加するための可変長のフィールド。拡張フィールド内に入る情報は多々あり、その中でも認証と暗号化がセキュリティ機能に該当する。

問 23　イ
〔解説〕ディジタル署名は、公開鍵暗号の技術を応用してディジタル文書の正当性を保証する仕組み
ア　改ざん部位を特定することはできない
ウ　ディジタル署名はマルウェアに感染しているか否かを確認する仕組みではない
エ　この場合、ディジタル署名の検証が失敗に終わりますが、どちらが改ざんされたかを判別することはできない

問24　イ

問 25　ア
〔解説〕イ　マルチメディアデータの送信など電子メールを多目的用途に利用できるようにした拡張形式
ウ　電子メールを受信するためのプロトコルですが、サーバ上のメッセージを検索したり、メールのヘッダだけを取り出す機能はない
エ　電子メールを送信するためのプロトコル

問 26　ア
〔解説〕イ　ＩＤを登録しても成り済ましの可能性があるので機密性は確保されない
ウ　メーリングリストはメールをリスト内のメンバ全員に送る機能をもつだけで，メールの機密性には関係ない
エ　ＣＨＡＰでは認証時のデータは暗号化されるが，通信データは暗号化されないので機密性を確保することはできない

問 27　ア

〔解説〕イ　ＬＤＡＰ(Lightweight Directory Access Protocol)は、ユーザＩＤやパスワードなどのユーザ情報やネットワーク資源情報を一元管理するとともに、それらの情報を提供する「ディレクトリサービス」にアクセスするためのプロトコル。ＬＤＡＰ自体は暗号化機能を持たない

ウ　Ｓ／ＭＩＭＥでは、送信元の端末から送信先の端末までＥｎｄ－ｔｏ－Ｅｎｄで暗号化が行われるため、メールサーバ内でも暗号化された状態になっている

エ　ＨＴＴＰヘッダに「Ｃａｃｈｅ－Ｃｏｎｔｒｏｌ：ｎｏ－ｃａｃｈｅ」を加えることでキャッシュしないように設定することができます

問 28　ア

〔解説〕ディジタルフォレンジックスは、収集・解析を行う対象によってコンピュータフォレンジックスや、ネットワークフォレンジックスなどに分類される。

問 29　イ

〔解説〕電子透かしとは，画像や動画などのディジタルコンテンツに，画質などにほとんど影響を与えずに特定の情報を埋め込む技術である。

問 30　ウ

〔解説〕ア　署名鍵は、メッセージダイジェストを暗号化してディジタル署名を生成するために使用される

イ　メッセージダイジェストの復号に使われるのは送信者の公開鍵です。またディジタル署名には改ざん部位を特定する機能はない

エ　ディジタル署名はメッセージ本文の暗号化を目的としていない

問 31　イ

〔解説〕公開鍵暗号方式において通信関係が 1 対多の場合、通信相手がそれだけ多くなろうとも必要な鍵数は秘密鍵と公開鍵の 2 つだけ。つまり各人が秘密鍵を所持し公開鍵を公開しているなら、誰から誰に通信を行っても秘匿性が守れることになる。

したがって必要な鍵の数は、

人数(n)×(公開鍵＋秘密鍵)＝2n 個

の式で表すことができるというわけです。

ちなみに共通鍵暗号方式で n 人が相互に通信を行う場合に必要な鍵数は、n(n-1)／2 の式で表すことができる。

問 32　ウ

〔解説〕ア　虹彩は、満 2 歳以降は経年変化しないので虹彩情報を更新する必要ない

イ　虹彩情報を得るためには、一般的に赤外線カメラを用いて静脈内を流れる血液中のヘモグロビンに近赤外線を照射するが、照度を高くすると精度の高い像が得られる反面、目に負担が掛かる

エ　センサ部に触れずに認証できるので指紋認証のように遺留物が残ることはない。また衛生面も優れている

問 33　イ
〔解説〕認証局(ＣＡ)は、公開鍵暗号方式を用いたデータ通信において、利用者(主にサーバ)の公開鍵の正当性を保証するためのディジタル証明書を発行する第三者機関。

問 34　ウ
〔解説〕ア　ハッシュ値に変換して保存するのは、盗聴や漏えいなどにより第三者に知られても解読できないようにするため
イ　ハッシュ関数は一方向性のため、ハッシュ値から元のデータを復元することはできない
エ　ハッシュ値には盗聴の有無を検知する仕組みはない

問 35　イ
〔解説〕公開鍵暗号方式は、暗号化と復号に異なる鍵を使用する暗号方式。暗号化鍵は誰もが使用できるように公開しておき(公開鍵)、復号鍵は受信者が厳重に管理する(秘密鍵)。
電子メールは、Ｂさんの公開鍵で暗号化されているため、それを復号できるのは公開鍵に対応する秘密鍵を所持するＢさんのみ。よって「イ」が適切な記述である。

問 36　ウ
〔解説〕ア　ＮＴＰ(Network Time Protocol)サーバの役割
イ　Ｓ/ＭＩＭＥやＯｐｅｎＰＧＰの役割
エ　認証局が正当性を証明するのは利用者の公開鍵

問 37　ウ
〔解説〕ア　標準時配信サービスの説明
イ　バイオメトリクス認証の説明
エ　ＮＴＰ(Network Time Protocol)の説明

問 38　エ
〔解説〕ア　メール受信の際に、チャレンジレスポンス方式の認証を行うことで平文の認証情報がネットワークに流れるのを防止するプロトコル
イ　ＴＬＳのセキュアな通信路上でメールソフトからメールサーバ間のＰＯＰ通信を行うプロトコル
ウ　公開鍵暗号技術を使用して認証、改ざん検出、暗号化等の機能を電子メールソフトに提供するもの

問 39　ウ
〔解説〕耐タンパ性：ハードウェアやソフトウェアのセキュリティレベルを表す指標で、外部から重要データを取り出したり盗み出そうとする行為に対する耐性度合いのことを指す。
・専用認証デバイスを接続しないと内部にアクセスできない設計(ハード)
・ソフトウェアの難読化、暗号化(ソフト)
・・・etc