問 1　チャレンジレスポンス方式として，適切なものはどれか。

ア　SSL によって，クライアント側で固定パスワードを暗号化して送信する。

イ　トークンという装置が表示する毎回異なったデータをパスワードとして送信する。

ウ　任意長のデータを入力として固定長のハッシュ値を出力する。

エ　利用者が入力したパスワードと，サーバから送られたランダムなデータとをクライアント側で演算し，その結果を認証用データに用いる。

問 2　ブラウザが Web サーバとの間で SSL で通信する際，ディジタル証明書に関する警告メッセージが表示される原因となり得るものはどれか。

ア　Web サーバが，SSL 通信の暗号化方式として，ハンドシェイク終了後に共通鍵暗号化方式で SSL セッションを開始した。

イ　ブラウザが CRL の妥当性を VA に問い合わせる際に，OCSP や SCVP が用いられた。

ウ　ブラウザが Web サーバのディジタル証明書の検証に成功した後に, Web サーバから SSL セッションを確立した。

エ　ルート CA のディジタル証明書について, Web サーバのディジタル証明書のものがブラウザで保持しているどのものとも一致しなかった。

問 3　SMTP-AUTH 認証はどれか。

ア　SMTP サーバに電子メールを送信する前に，電子メールを受信し，その際にパスワード認証が行われたクライアントの IP アドレスに対して，一定時間だけ電子メールの送信を許可する。

イ　クライアントが SMTP サーバにアクセスしたときに利用者認証を行い，許可された利用者だけから電子メールを受け付ける。

ウ　サーバは CA の公開鍵証明書をもち，クライアントから送信された CA の署名付きクライアント証明書の妥当性を確認する。

エ　電子メールを受信する際の認証情報を秘匿できるように，パスワードからハッシュ値を計算して，その値で利用者認証を行う。

問 4　コンティンジェンシープランにおける留意点はどれか。

ア　企業のすべてのシステムを対象とするのではなく，システムの復旧の重要性と緊急性を勘案して対象を決定する。

イ　災害などへの対応のために，すぐに使用できるよう，バックアップデータをコンピュータ室内又はセンタ内に保存しておく。

ウ　バックアップの対象は，機密情報の中から機密度を勘案して選択する。

エ　被害状況のシナリオを作成し，これに基づく“予防策策定手順”と“バックアップ対策とその手順”を策定する。

問5　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サーバで設定された自社の公開Webサーバの FQDN情報が書き換えられ，外部からの参照者が，本来とは異なるWebサーバに誘導される。

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サーバを参照する場合に，本来とは異なるWebサーバに誘導される。

エ　電子メールの不正中継対策をした自社のメールサーバが，不正中継の踏み台にされる。

問6　NIDS（ネットワーク型IDS）を導入する目的はどれか。

ア　管理下のネットワーク内への不正侵入の試みを検知し，管理者に通知する。

イ　サーバ上のファイルが改ざんされたかどうかを判定する。

ウ　実際にネットワークを介してサイトを攻撃し，不正に侵入できるかどうかを検査する。

エ　ネットワークからの攻撃が防御できないときの損害の大きさを判定する。

問 7　クロスサイトスクリプテイングによる攻撃へのセキュリティ対策に該当するものはどれか。

ア　OSのセキュリティパッチを適用することによって，Webサーバへの侵入を防止する。

イ　Web アプリケーションがクライアントに入力データを表示する場合，データ内の特殊文字を無効にする処理を行う。

ウ　WebサーバにSNMPエージェントを常駐稼働させることによって，攻撃を検知する。

エ　許容範囲を超えた大きさのデータの書込みを禁止しWebサーバへの侵入を防止する。

問8　ウイルスの検出手法であるビヘイビア法を説明したものはどれか。

ア　あらかじめ特徴的なコードをパターンとして登録したウイルス定義ファイルを用いてウイルス検査対象と比較し，同じパターンがあれば感染を検出する。

イ　ウイルスに感染していないことを保証する情報をあらかじめ付加しておき，検査対象の検査時に不整合があれば感染を検出する。

ウ　ウイルスの感染が疑わしい検査対象を，安全な場所に保管する原本と比較し，異なっていれば感染を検出する。

エ　ウイルスの感染や発病によって生じるデータ書込み動作の異常や通信量の異常増加などの変化を監視して，感染を検出する。

問 9　コンピュータフォレンジクスの説明として，適切なものはどれか。

ア　あらかじめ設定した運用基準に従って，メールサーバを通過する送受信メールをフィルタリングすること

イ　磁気ディスクなどの書換え可能な記憶媒体を単に初期化するだけではデータを復元される可能性があるので，覆い隠すように上書きすること

ウ　不正アクセスなどコンピュータに関する犯罪の法的な証拠性を確保できるように，原因究明に必要な情報を保全，収集して分析すること

エ　ホストに対する外部からの攻撃や不正なアクセスを防御すること

問 10　ステガノグラフイの機能はどれか。

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 11　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　外部に公開してい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セキュリティ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のマクロウイルスの侵入

工　電子メール爆弾などの DoS 攻撃

問 12　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すべ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，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，クッキーなどのセッション情報を盗む。

問 13　レイヤ 2 スイッチや無線 LAN アクセスポイントで接続を許可する仕組みはどれか。

ア　DHCP　　イ　Web シングルサインオン

ウ　認証 VLAN　　エ　パーソナルファイアウォール

問 14　SQL インジェクション対策について，Web アプリケーションの実装における対策と Web アプリケーションの実装以外の対策の組合せとして，適切なものはどれか。

	Webアプリケーションの実装における対策	Webアプリケーションの実装以外の対策
ア	Web アプリケーション中でシェルを起動しない。	chroot 環境で Web サーバを実行する。
イ	セッションIDを複雑なものにする。	SSL によって通信内容を秘匿する。
ウ	バインド機構を利用する。	データベースのアカウントのもつデータベースアクセス権限を必要最小限にする。
エ	パス名やファイル名をパラメタとして受け取らないようにする。	重要なファイルを公開領域に置かない。

問15　SLCP（共通フレーム）に従いシステム開発の要件定義の段階で実施することとして，適切なものはどれか。

ア　システムに必要なセキュリティ機能及びその機能が達成すべき保証の程度を決定する。

イ　システムに必要なセキュリティ機能に関連するチェックリストを用いてソースコードをレビューする。

ウ　組織に必要なセキュリティ機能を含むシステム化計画を立案する。

エ　第三者によるシステムのセキュリティ監査を脆弱性評価ツールを用いて定期的に実施する。

問16　ネットワークのQoSで使用されるトラフィック制御方式に関する説明のうち，適切なものはどれか。

ア　通信を開始する前にネットワークに対して帯域などのリソースを要求し，確保の状況に応じて通信を制御することを，アドミッション制御という。

イ　入力されたトラフィックが規定された最大速度を超過しないか監視し，超過分のパケットを破棄するか優先度を下げる制御を，シェーピングという。

ウ　パケットの送出間隔を調整することによって，規定された最大速度を超過しないようにトラフィックを平準化する制御を，ポリシングという。

エ　フレームの種類やあて先に応じて優先度を変えて中継することを，ベストエフォートという。

問17　電源オフ時にIV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IV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18　ネットワークに接続されているホストのIVアドレスが212．62．31．90で，サブネットマスクが255．255．255．224のとき，ホストアドレスはどれか。

ア 10　　イ　26　　ウ　90　　エ　212

問 19　イーサネットのレイヤ 2 で使用されるプロトコルで，ネットワークを冗長化させる際にループの発生を防ぐものはどれか。

ア　IGMP　　イ　RIP
ウ　SIP　　エ　スパニングツリープロトコル

問 20　暗号化や認証機能をもち，リモートからの遠隔操作の機能をもったプロトコルはどれか。

ア IPsec　　イ　L2TP　　ウ　RADIUS　　エ　SSH

問 21　Web サーバを使ったシステムにおいて，インターネットから受け取ったリクエストを Web サーバに中継する仕組みはどれか。

ア　DMZ　　イ　フォワードプロキシ
ウ　プロキシ ARP　　エ　リバースプロキシ

問 22　ブラックボックステストのテストデータの作成方法のうち，最も適切なものはどれか。

ア　稼働中のシステムから実データを無作為に抽出し，テストデータを作成する。
イ　機能仕様から同値クラスや限界値を識別し，テストデータを作成する。
ウ　業務で発生するデータの発生頻度を分析し，テストデータを作成する。
エ　プログラムの流れ図から，分岐条件に基づいたテストデータを作成する。

問 23　開発した製品で利用している新規技術に関して特許の出願を行った。日本において特許権の取得が可能なものはどれか。

ア　学会で技術内容を発表した日から 11 か月目に出願した。
イ　顧客と守秘義務の確認を取った上で技術内容を説明した後，製品発表前に出願した。
ウ　製品に使用した暗号の生成式を出願した。
エ　製品を販売した後に出願した。

問 24　雷サージによって通信回線に誘起された異常電圧から通信機器を防護するための装置はどれか。

ア　IDF（Intermediate Distributing Frame）
イ　MCCB（Molded Case Circuit Breaker）
ウ　アレスタ
エ　避雷針

問 25　IT に係る内部統制を評価し検証するシステム監査の対象となるものはどれか。

ア　経営企画部が行っている中期経営計画の策定の経緯

イ　人事部が行っている従業員の人事考課の結果

ウ　製造部が行っている不良品削減のための生産設備の見直しの状況

エ　販売部が行っているデータベースの入力・更新における正確性確保の方法

午前Ⅱ試験

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

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

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