問 1　特定の CA が発行した CRL（Certificate Revocation List）に関する記述のうち，適切なものはどれか。

ア　CRL には，失効された公開鍵証明書に対応する秘密鍵が登録される。
イ　CRL には，有効期限内の公開鍵証明書のうち破棄されている公開鍵証明書と破棄された日時の対応が提示される。
ウ　CRL は, 鍵の漏えい, 破棄申請の状況をリアルタイムに反映するプロトコルである。
エ　有効期限切れで無効になった公開鍵証明書は，所有者が新たな公開鍵証明書を取得するまでの間，CRL に登録される。

問 2　IEEE 802.1X で使われる EAP-TLS によって実現される認証はどれか。

ア　CHAP を用いたチャレンジレスポンスによる利用者認証
イ　あらかじめ登録した共通鍵によるサーバ認証と，時刻同期のワンタイムパスワードによる利用者認証
ウ　ディジタル証明書による認証サーバとクライアントの相互認証
エ　利用者 ID とパスワードによる利用者認証

問 3　SEO（Search Engine Optimization）ポイズニングの説明はどれか。

ア　Web 検索サイトの順位付けアルゴリズムを悪用して，キーワードで検索した結果の上位に，悪意のあるサイトを意図的に表示させる。
イ　ウイルス検索エンジンのセキュリティ上の脆弱性を悪用して，システム権限で不正な処理を実行させる。
ウ　車などで移動しながら，無線 LAN のアクセスポイントを探し出して，ネットワークに不正侵入する。
エ　ネットワークを流れるパケットから，不正侵入のパターンに合致するものを検出して，管理者への通知や，検出した内容の記録を行う。

問 4　2011 年に経済産業省が公表しだクラウドサービス利用のための情報セキュリティマネジメントガイドライン”が策定された目的について述べたものはどれか。

ア　JIS Q 27002 の管理策を拡張し，クラウドサービス利用者が情報セキュリティ対策を円滑に行えるようにする。
イ　クラウドサービス提供事業者に対して情報セキュリティ監査を実施する方法を利用者に提示する。
ウ　クラウドサービスの利用がもたらすセキュリティリスクをサービス提供事業者の視点で提示する。
エ　セキュリティリスクの懸念の少ないクラウドサービス提供事業者を利用者が選択できるような格付け基準を提供する。

問 5　スパムメールの対策として，宛先ポート番号 25 番の通信に対して ISP が実施する OP25B の説明はどれか。

ア　ISP 管理外のネットワークからの通信のうち，スパムメールのシグネチャに該当するものを遮断する。
イ　動的 H) アドレスを割り当てたネットワークから ISP 管理外のネットワークへの直接の通信を遮断する。
ウ　メール送信元のメールサーバについて DNS の逆引きができない場合，そのメールサーバからの通信を遮断する。
エ　メール不正中継の脆弱性をもつメールサーバからの通信を遮断する。

問 6　ファイアウォールにおけるダイナミックパケットフィルタリングの特徴はどれか。

ア　IP アドレスの変換が行われるので，ファイアウォール内部のネットワーク構成を外部から隠蔽できる。
イ　暗号化されたパケットのデータ部を復号して，許可された通信かどうかを判断できる。
ウ　戻りのパケットに関しては，過去に通過したリクエストパケットに対応したものだけを通過させることができる。
エ　パケットのデータ部をチェックして，アプリケーション層での不正なアクセスを防止できる。

問 7　ポリモーフィック型ウイルスの説明として，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　感染するごとに鍵を変えてウイルスのコードを暗号化することによってウイルス自身を変化させて，同一のパターンで検知されないようにする。
ウ　複数の OS で利用できるプログラム言語でウイルスを作成することによって，複数の OS 上でウイルスが動作する。
エ　ルートキットを利用してウイルスに感染していないように見せかけることによって，ウイルスを隠蔽する。

問 8　FIPS 140-2 を説明したものはどれか。

ア　暗号モジュールのセキュリティ要求事項
イ　情報セキュリティマネジメントシステムに関する認証基準
ウ　ディジタル証明書や証明書失効リストの標準仕様
エ　無線 LAN セキュリティ技術

問 9　特定の情報資産の漏えいに関するリスク対応のうち，リスク回避に該当するものはどれか。

ア　外部の者が侵入できないように，入退室をより厳重に管理する。
イ　情報資産を外部のデータセンタに預託する。
ウ　情報の新たな収集を禁止し，収集済みの情報を消去する。
エ　情報の重要性と対策費用を勘案し，あえて対策をとらない。

問 10　ICMP Flood 攻撃に該当するものはどれか。

ア　ping コマンドを用いて同時に発信した大量の要求パケットによって，攻撃対象のサーバに至るまでの回線を過負荷にしてアクセスを妨害する。
イ　繰り返し HTTP GET コマンドを送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける。
ウ　コネクション開始要求に当たる SYN パケットを大量に送ることによって，攻撃対象のサーバに，接続要求ごとに応答を返すための過大な負荷を掛ける。
エ　大量の TCP コネクションを確立することによって，攻撃対象のサーバに接続を維持させ続けリソースを枯渇させる。

問 11　標準化団体 OASIS が，Web サイト間で認証，属性及び認可の情報を安全に交換するために策定したフレームワークはどれか。

ア　SAML　　イ　SOAP　　ウ　XKMS　　エ　XML Signature

問 12　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　ネットワークの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 13　ゼロデイ攻撃の特徴はどれか。

ア　セキュリティパッチが提供される前にパッチが対象とする脆弱性を攻撃する。
イ　特定のサイトに対し，日時を決めて，複数台の PC から同時に攻撃する。
ウ　特定のターゲットに対し，フィッシングメールを送信して不正サイトへ誘導する。
エ　不正中継が可能なメールサーバを見つけた後，それを踏み台にチェーンメールを大量に送信する。

問 14　SSL に関する記述のうち，適切なものはどれか。

ア　SSL で使用する Web サーバのディジタル証明書には IP アドレスの組込みが必須なので，Web サーバの IP アドレスを変更する場合は，ディジタル証明書を再度取得する必要がある。
イ　SSL で使用する個人認証用のディジタル証明書は，IC カードなどに格納できるので，格納場所を特定の PC に限定する必要はない。
ウ　SSL は Web サーバを経由した特定の利用者間の通信のために開発されたプロトコルであり，Web サーバ提供者への事前の利用者登録が不可欠である。
エ　日本国内では，SSL で使用する共通鍵の長さは，128 ビット未満に制限されている。

問 15　WAF（Web Application Firewall）のブラックリスト又はホワイトリストの説明のうち，適切なものはどれか。

ア　ブラックリストは，脆弱性があるサイトの IP アドレスを登録したものであり，該当する通信を遮断する。
イ　ブラックリストは，問題がある通信データパターンを定義したものであり，該当する通信を遮断するか又は無害化する。
ウ　ホワイトリストは，暗号化された受信データをどのように復号するかを定義したものであり，復号鍵が登録されていないデータを遮断する。
エ　ホワイトリストは，脆弱性がないサイトの FQDN を登録したものであり，登録がないサイトへの通信を遮断する。

問 16　SSL に対するバージョンロールバック攻撃の説明はどれか。

ア　SSL の実装の脆弱性を用いて，通信経路に介在する攻撃者が弱い暗号化通信方式を強制することによって，暗号化通信の内容を解読して情報を得る。
イ　SSL のハンドシェイクプロトコルの終了前で，使用暗号化アルゴリズムの変更メッセージを，通信経路に介在する攻撃者が削除することによって，通信者が暗号化なしでセッションを開始し，攻撃者がセッションの全通信を盗聴したり改ざんしたりする。
ウ　SSL を実装した環境において，攻撃者が物理デバイスから得られた消費電流の情報などを利用して秘密情報を得る。
エ　保守作業のミスや誤操作のときに回復できるようにバックアップした SSL の旧バーションのライブラリを，攻撃者が外部から破壊する。

問 17　ネットワークを構成する装置の用途や機能に関する記述のうち，適切なものはどれか。

ア　ゲートウェイは，主にトランスポート層以上での中継を行う装置であり，異なったプロトコル体系のネットワーク間の接続などに用いられる。
イ　ブリッジは，物理層での中継を行う装置であり，フレームのフィルタリング機能をもつ。

ウ　リピータは，ネットワーク層での中継を行う装置であり，伝送途中で減衰した信号レベルの補正と再生増幅を行う。
エ　ルータは，データリンク層のプロトコルに基づいてフレームの中継と交換を行う装置であり，フロー制御や最適経路選択などの機能をもつ。

問 18　DNSSEC に関する記述として，適切なものはどれか。

ア　DNS サーバへの DoS 攻撃を防止できる。
イ　IPsec による暗号化通信が前提となっている。
ウ　代表的な DNS サーバの実装である BIND の代替として使用する。
エ　ディジタル署名によって DNS 応答の正当性を確認できる。

問 19　2 台の PC を IPv6 ネットワークに接続するとき，2 台ともプレフィックスが 2001:db8:100:1000::/56 の IPv6 サブネットに入るようになる IP アドレスの組合せはどれか。

	1 台目の PC	2 台目の PC
ア	2001:db8:100::aa:bb	2001:db8:100::cc:dd
イ	2001:db8:100:1000::aa:bb	2001:db8:100:2000::cc:dd
ウ	2001:db8:100:1010::aa:bb	2001:db8:100:1020::cc:dd
エ	2001:db8:100:1100::aa:bb	2001:db8:100:1200::cc:dd

問 20　HTTP の認証機能を利用するクライアント側の処理として，適切なものはどれか。

ア　ダイジェスト認証では，利用者 ID とパスワードを“:”で連結したものを，MD5 を使ってエンコードし Authorization ヘッダで指定する。
イ　ダイジェスト認証では，利用者 ID とパスワードを“:”で連結したものを，SHA を使ってエンコードし Authorization ヘッダで指定する。
ウ　ベーシック認証では，利用者 ID とパスワードを“:”で連結したものを，BASE64 でエンコードし Authorization ヘッダで指定する。
エ　ベーシック認証では，利用者 ID とパスワードを“:”で連結したものを，エンコードせずに Authorization ヘッダで指定する。

問 21　データベースのデータを更新するトランザクションが，実行途中で異常終了したとき，更新中のデータに対して行われる処理はどれか。

ア　異常終了時点までの更新ログ情報を破棄することによって，データをトランザクション開始前の状態に回復する。
イ　チェックポイント時点からコミットが完了しているトランザクションの更新をロ

ールフォワードすることによって，データを回復する。
ウ　トランザクションの更新ログ情報を使って異常終了時点までロールフォワードすることによって，データを回復する。
エ　ロールバックすることによって，データをトランザクション開始前の状態に回復する。

問 22　オブジェクト指向における情報隠蔽に関する記述として，適切なものはどれか。

ア　オブジェクトの特性（属性，関連，操作）をまとめて抽象化する。
イ　オブジェクトは，メッセージによってだけアクセス可能となる。
ウ　親クラスに定義されたメソッドを，実行時に子クラスに引き継ぐ。
エ　同一メッセージでも，実行時の受信クラスに基づいて適用されるメソッドが決まる。

問 23　特許権に関する記述のうち，適切なものはどれか。

ア　A 社が特許を出願するよりも前に独自に開発して発売した製品は，A 社の特許権の侵害にならない。
イ　組込み機器におけるハードウェアは特許権で保護されるが，ソフトウェアは保護されない。
ウ　審査を受けて特許権を取得した後に，特許権が無効となることはない。
エ　先行特許と同一の技術であっても，独自に開発した技術であれば特許権の侵害にならない。

問 24　ソフトウェア開発・保守の工程において，リポジトリを構築する理由として，最も適切なものはどれか。

ア　各工程で検出した不良を管理することが可能になり，ソフトウェアの品質分析が容易になる。
イ　各工程での作業手順を定義することが容易になり，開発・保守時の作業ミスを防止することができる。
ウ　各工程での作業予定と実績を関連付けて管理することが可能になり，作業の進捗管理が容易になる。
エ　各工程での成果物を一元管理することによって，開発・保守作業の効率が良くなり，用語の統一もできる。

問 25　システム監査で用いる統計的サンプリングに関する記述のうち，適切なものはどれか。

ア　開発プロセスにおけるコントロールを評価する際には，開発規模及び影響度の大

きい案件を選定することによって，母集団全体への評価を導き出すことができる。

イ　コントロールが有効であると判断するために必要なサンプル件数を事前に決めることができる。

ウ　正しいサンプリング手順を踏むことによって，母集団全件に対して検証を行う場合と同じ結果を常に導き出すことができる。

エ　母集団からエラー対応が行われたデータを選定することによって，母集団全体に対してコントロールが適切に行われていることを確認できる。

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

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

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