問 I　APT（Advanced Persistent Threats）の説明はどれか。

ア　攻撃者は DoS 攻撃及び DDoS 攻撃を繰り返し組み合わせて，長期間にわたって特定組織の業務を妨害する。
イ　攻撃者は興味本位で場当たり的に，公開されている攻撃ツールや脆弱性検査ツールを悪用した攻撃を繰り返す。
ウ　攻撃者は特定の目的をもち，特定組織を標的に複数の手法を組み合わせて気付かれないよう執拗に攻撃を繰り返す。
エ　攻撃者は不特定多数への感染を目的として，複数の攻撃方法を組み合わせたマルウェアを継続的にばらまく。

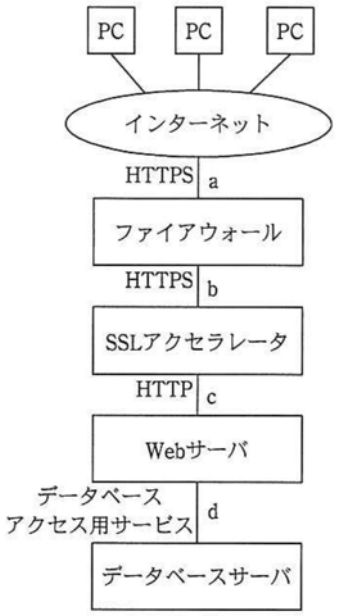
問 2　DNSSEC（DNS Security Extensions）の機能はどれか。

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になるようにする。
イ　DNS サーバから受け取るリソースレコードに対するディ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 3　PKI を構成する OCSP（Online Certificate Status Protoco1）を利用する目的はどれか。

ア　誤って破棄してしまった秘密鍵の再発行処理の進捗状況を問い合わせる。
イ　ディジタル証明書から生成した鍵情報の交換が OCSP クライアントとレスポンダの間で失敗した際，認証状態を確認する。
ウ　ディジタル証明書の失効情報を問い合わせる。
エ　有効期限の切れたディジタル証明書の更新処理の進捗状況を確認する。

問 4　図のような構成と通信サービスのシステムにおいて，Web アプリケーションの脆弱性対策としてネットワークのパケットをキャプチャして WAF による検査を行うとき，WAF の設置場所として最も適切な箇所はどこか。ここで，WAF には通信を暗号化したり，復号したりする機能はないものとする。



ア　a　　イ　b　　ウ　c　　エ　d

問5　サイドチャネル攻撃の説明はどれか。

ア　暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる物理量（処理時間や消費電流など）やエラーメッセージから，攻撃対象の機密情報を得る。
イ　企業などの機密情報を詐取するソーシャルエンジニアリングの手法の一つであり，オフィスの紙ゴミの中から不用意に捨てられた機密情報の印刷物を探し出す。
ウ　通信を行う二者の間に割り込んで，両者が交換する情報を自分のものとすり替えることによって，気付かれることなく盗聴する。
エ　データベースを利用するWebサイトに入力パラメタとしてSQL文の断片を与えることによって，データベースを改ざんする。

問6　SMTP-AUTHにおける認証の動作を説明したものはどれか。

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アドレスは，一定時間だけ電子メールの送信が許可される。
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　サーバは認証局のディジタル証明書をもち，クライアントから送信された認証局の署名付きクライアント証明書の妥当性を確認する。
エ　利用者が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 7　無線 LAN 環境に複数台の PC，複数のアクセスポイント及び利用者認証情報を管理する 1 台のサーバがある。利用者認証とアクセス制御に IEEE 802.1X と RADIUS を利用する場合の実装方法はどれか。

ア　PC には IEEE 802.1X のサプリカントを実装し，RADIUS クライアントの機能をもたせる。
イ　アクセスポイントには IEEE 802.1X のオーセンティケータを実装し，RADIUS クライアントの機能をもたせる。
ウ　アクセスポイントには IEEE 802.1X のサプリカントを実装し，RADIUS サーバの機能をもたせる。
エ　サーバには IEEE 802.1X のオーセンティケータを実装し，RADIUS サーバの機能をもたせる。

問 8　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　国レベルや企業・組織内に設置され，コンピュータ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，信教や政治的な目標を達成するという目的をもった人や組織の総称である。

問 9　NIST の定義によるクラウドコンピューティングのサービスモデルにおいて，パブリッククラウドサーピスの利用企業のシステム管理者が，仮想サーバのゲスト OS に係る設定作業及びセキュリティパッチ管理作業を実施可かどうかの組合せのうち，適切なものはどれか。

	IaaS	PaaS	SaaS
ア	実施可	実施可	実施不可
イ	実施可	実施不可	実施不可
ウ	実施不可	実施可	実施不可
エ	実施不可	実施不可	実施可

問 10　基本評価基準，現状評価基準，環境評価基準の三つの基準で IT 製品のセキュリティ脆弱性の深刻さを評価するものはどれか。

ア　CVSS　　イ　ISMS　　ウ　PCIDSS　　エ　PMS

問 11　CRYPTREC の活動内容はどれか。

ア　客観的な評価によって安全性及び実装性に優れると判断された暗号技術のリストを決定する。
イ　情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ対策の推進に係る企画などを行う。
ウ　組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。
エ　認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。

問 12　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，直接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た DNS サーバが書き換わり，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　社内の利用者間で送信された電子メールの宛先アドレスが書き換えられ，正常な送受信ができなくなる。

問 13　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検査対象に付加しておき，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，安全な場所に保管されている原本と比較し，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 14　DoS 攻撃の一つである 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　サイズが大きい UDP パケットを大量に送信する。
エ　サイズが大きい電子メールや大量の電子メールを送信する。

問 15　ダウンローダ型ウイルスが内部ネットワークの PC に感染した場合に，インターネット経由で他のウイルス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 16　スパム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ィジタル署名を電子メールのヘッダに付加して，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 ポート番号 25 への直接の通信を禁止する。

問 17　IEEE 802.11a や IEEE 802.11b で採用されているアクセス制御方式はどれか。

ア　CSMA/CA　　イ　CSMA/CD
ウ　LAPB　　エ　トークンパッシング方式

問 18　IPv6 グローバルユニキャストアドレスはどれか。

ア　::1　　イ　2001:dc3::35
ウ　fd00::12:fff:fea9:18　　エ　fe80::f:acff:fea9:18

問 19　TCP のフロー制御に関する記述のうち，適切なものはどれか。

ア　OSI 基本参照モデルのネットワーク層の機能である。
イ　ウィンドウ制御の単位は，バイトではなくビットである。
ウ　確認応答がない場合は再送処理によってデータ回復を行う。
エ　データの順序番号をもたないので，データは受信した順番のままで処理する。

問 20　電子メールが配送される途中に経由した MTA の IP アドレスや時刻などの経由情報を，MTA が付加するヘッダフィールドはどれか。

ア　Accept　　イ　Received　　ウ　Return-Path　　エ　Via

問 21　関係データベースのビューを利用する目的はどれか。

ア　DISTINCT 指定，GROUP BY 句及び HAVING 句をもつ演算処理を独立させて，プログラムに単純化したデータ更新手段を提供する。
イ　行や列を特定の条件で絞り込んだビューだけをアクセスさせることによって，基となる表のデータの一部を隠蔽して保護する手段を提供する。
ウ　データベースの物理的記憶構造の変更に影響されないように，アプリケーションプログラムに対して物理的データ独立性を提供する。
エ　複数の表を結合したビューにインデックスを付与することによって，複数の表にまたがった高度な検索手段を提供する。

問 22　既存システムを基に，新システムのモデル化を行う場合の DFD 作成の手順として，適切なものはどれか。

ア　現物理モデル→現論理モデル→新物理モデル→新論理モデル
イ　現物理モデル→現論理モデル→新論理モデル→新物理モデル
ウ　現論理モデル→現物理モデル→新物理モデル→新論理モデル
エ　現論理モデル→現物理モデル→新論理モデル→新物理モデル

問 23　SOA（Service Oriented Architecture）でサービスを設計する際の注意点のうち，適切なものはどれか。

ア　可用性を高めるために，ステートフルなインタフェースとする。
イ　業務からの独立性を確保するために，サービスの命名は役割を表すものとする。
ウ　業務の変化に対応しやすくするために，サービス間の関係は疎結合にする。
エ　セキュリティを高めるために，一度開発したサービスは再利用しない方がよい。

問 24　情報システムの設計のうち，フェールソフトの例はどれか。

ア　UPS を設置することによって，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によって，システムの誤動作を防止できるようにする。

問 25　新システムへの移行に関するシステム監査で確認した状況のうち，指摘事項に該当するものはどれか。

ア　移行作業と併せて，システム運用部門及びシステム利用部門に対する新システムの操作教育を計画し，実施していた。
イ　移行対象，移行方法，移行実施体制及び移行スケジュールを明記した移行計画に従って，移行作業を行っていた。
ウ　移行ツールを利用して，データベースの移行及びその移行結果の検証を行っていた。
エ　システム開発部門内に検証体制を作って移行結果の検証を行い，移行完了としていた。

午前Ⅱ試験

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

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

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