問1　セキュアハッジュ関数 SHA-256 を用いて，32 ピット，256 ビット，2,048 ビットの三つの長さのメッセージからハッジュ値を求めたとき，それぞれのメッセージのハッシュ値の長さはどれか。

単位 ビット

	メッセージの長さ		
	32	256	2,048
ア	32	256	256
イ	32	256	2,048
ウ	256	256	256
エ	256	256	2,048

問2　XML ディジタル署名の特徴はどれか。

ア　XML 文書中の，指定したエレメントに対して署名することができる。
イ　エンベロービング署名（Enveloping Signature）では一つの署名対象に必ず複数の署名を付ける。
ウ　署名形式として，CMS（Cryptographic Message Syntax）を用いる。
エ　署名対象と署名アルゴリズムを ASN.1 によって記述する。

問3　A 社の Web サーバは，認証局で生成した Web サーバ用のディジタル証明書を使って SSL/TLS 通信を行っている。PC が A 社の Web サーバに SSL/TLS を用いてアクセスしたとき，サーバのディジタル証明書を入手した後に，認証局の公開鍵を利用し PC が行う処理はどれか。

ア　暗号化通信に利用する共通鍵を生成し，認証局の公開鍵を使って暗号化する。
イ　暗号化通信に利用する共通鍵を認証局の公開鍵を使って復号する。
ウ　ディジタル証明書の正当性を認証局の公開鍵を使って検証する。
エ　利用者が入力，送付する秘匿データを認証局の公開鍵を使って暗号化する。

問4　S/KEY ワンタイムパスワードに関する記述のうち，適切なものはどれか。

ア　クライアントは認証要求のたびに，サーバへシーケンス番号と種（Seed）からなるチャレンジデータを送信する。
イ　サーバはクライアントから送られた使い捨てパスワードを演算し，サーバで記憶している前回の使い捨てパスワードと比較することによって，クライアントを認証する。
ウ　時刻情報を基にパスワードを生成し，クライアント，サーバ間でパスワードを時刻で同期させる。
エ　利用者が設定したパスフレーズは 1 回ごとに使い捨てる。

問5　100人の送受信者が共通鍵暗号方式で，それぞれ秘密に通信を行うときに必要な共通鍵の総数は幾つか。

ア　200　　イ　4,950　　ウ　9,900　　エ　10,000

問6　情報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　情報の重要性と対策費用を勘案し，あえて対策をとらない。
エ　データの安易な作成を禁止し，不要なデータを消去する。

問7　経済産業省告示の“ソフトウェア等脆弱性関連情報取扱基準”におけるWebアプリケーションに関する脆弱性関連情報の適切な取扱いはどれか。

ア　Webアプリケーションの脆弱性についての情報を受けた受付機関は，発見者の氏名・連絡先をWebサイト運営者に通知する。
イ　Webアプリケーションの脆弱性についての通知を受けたWebサイト運営者は，当該脆弱性に起因する個人情報の漏えいなどが発生した場合，事実関係を公表しない。
ウ　受付機関は，Webサイト運営者からWebアプリケーションの脆弱性が修正されたという通知を受けたら，それを速やかに発見者に通知する。
エ　受付機関は，一般利用者に不安を与えないために，Webアプリケーションの脆弱性関連情報の届出状況は，受付機関の中で管理し，公表しない。

問8　DNSサーバに格納されるネットワーク情報のうち，第三者に公開する必要のない情報が攻撃に利用されることを防止するための,プライマリDNSサーバの設定はどれか。

ア　SOAレコードのシリアル番号を更新する。
イ　外部のDNSサーバにリソースレコードがキャッシュされる時間を短く設定する。
ウ　ゾーン転送を許可するDNSサーバを登録する。
エ　ラウンドロビン設定を行う。

問9　ワームの侵入に関する記述のうち，適切なものはどれか。

ア　公開サーバへのワームの侵入は，IDSでは検知できない。
イ　未知のワームの侵入は，パターンマッチング方式で検知できる。
ウ　ワームは，アプリケーションソフトの脆弱性を突いて侵入できる。
エ　ワームは，仮想OS環境内のゲストOSに侵入できない。

問 10　ステガノグラフィを説明したものはどれか。

ア　データの複写を不可能にする（コピーできないようにする）技術のことをいう。
イ　データを第三者に盗み見られても解読できないようにするため，決まった規則に従ってデータを変換することをいう。
ウ　文書の正当性を保証するために付けられる暗号化された署名情報のことをいう。
エ　メッセージを画像データや音声データなどに埋め込み，その存在を隠す技術のことをいう。

問 11　DMZ 上のコンピュータがインターネットからの ping に応答しないようにファイアウォールのセキュリティルールを定めるとき，“通過禁止”に設定するものはどれか。

ア　ICMP
イ　TCP 及び UDP のポート番号 53
ウ　TCP のポート番号 21
エ　UDP のポート番号 123

問 12　ダウンローダ型ウイルスが PC に侵入した場合に，インターネット経路でほかのウイルスがダウンロードされることを防ぐ有効な対策はどれか。

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 13　ディジタル証明書を使わずに，通信者同士が，通信によって交換する公開鍵を用いて行う暗号化通信において，通信内容を横取りする目的で当事者になりすますものはどれか。

ア　Man-in-the-middle 攻撃
イ　war driving
ウ　トロイの木馬
エ　ブルートフォース攻撃

問 14　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与して，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 25 番への直接の通信を禁止する。

問 15　SMTP-AUTH を使ったメールセキュリティ対策はどれか。

ア　ISP 管理下の動的 IP アドレスからの電子メール送信について，管理外ネットワークのメールサーバへ SMTP 通信を禁止する。
イ　PC からの電子メール送信について，POP 接続で利用者認証済の場合にだけ許可する。
ウ　通常の SMTP とは独立したサブミッションポートを使用して，メールサーバ接続時の認証を行う。
エ　電子メール送信元のサーバについて DNS の逆引きが成功した場合にだけ，電子メール受信を許可する。

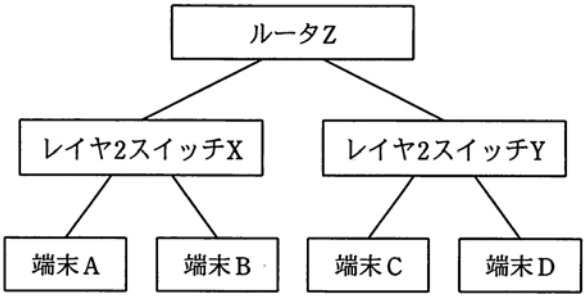
問 16　セキュリティプロトコル SSL/TLS の機能はどれか。

ア　FTP などの様々なアプリケーションに利用されて，アプリケーション層とトランスポート層（TCP）との間で暗号化する。
イ　MIME をベースとして，電子署名とメッセージの暗号化によって電子メールのセキュリティを強化する。
ウ　PPTP と L2F が統合された仕様で，PPP をトンネリングする。
エ　特定のアプリケーションの通信だけではなく，あらゆる IP パケットを IP 層で暗号化する。

問 17　IPsec に関する記述のうち，適切なものはどれか。

ア　IKE は IPsec の鍵交換のためのプロトコルであり，ポート番号 80 が使用される。
イ　鍵交換プロトコルとして，HMAC-MD5 が使用される。
ウ　トンネルモードを使用すると，元のヘッダまで含めて暗号化される。
エ　ホスト A とホスト B との間で IPsec による通信を行う場合，認証や暗号化アルゴリズムを両者で決めるために ESP ヘッダではなく AH ヘッダを使用する。

問 18　図のような 2 台のレイヤ 2 スイッチ，1 台のルータ，4 台の端末からなる IP ネットワークで，端末 A から端末 C に通信を行う際に，送付されるパケットのあて先 IP アドレスである端末 C の IP アドレスと，端末 C の MAC アドレスとを対応付けるのはどの機器か。ここで，ルータ Z においてプロキシ ARP は設定されていないものとする。



ア　端末 A　　イ　ルータ Z
ウ　レイヤ 2 スイッチ X　　エ　レイヤ 2 スイッチ Y

問 19　インターネットで電子メールを送信するとき，メッセージの本文の暗号化に共通鍵暗号方式を用い，共通鍵の受渡しには公開鍵暗号方式を用いるものはどれか。

ア AES　　イ IPsec　　ウ MIME　　エ S/MIME

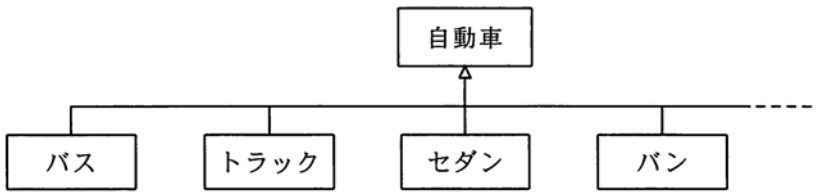
問 20　192.168.1.0/24 のネットワークアドレスを，16 個のサブネットに分割したときのサブネットマスクはどれか。

ア　255.255.255.192　　イ　255.255.255.224
ウ　255.255.255.240　　エ　255.255.255.248

問 21　データマイニングツールに関する記述として，最も適切なものはどれか。

ア　企業内で発生する情報を主題ごとに時系列で蓄積することによって，既存の情報システムだけでは得られない情報を提供する。
イ　集計データを迅速かつ容易に表示するなど，利用者に対して様々な情報分析機能を提供する。
ウ　大量に蓄積されたデータに対して統計処理などを行い，法則性の発見を支援する。
エ　利用者が情報を利用するための目的別データベースであり，あらかじめ集計処理などを施しておくことによって検索時間を短縮する。

問 22　次のクラス図におけるクラス間の関係の説明のうち，適切なものはどれか。



ア　“バス”，“ドラック”などのクラスが“自動車”クラスの定義を引き継ぐことを，インスタンスという。
イ　“バス”，“ドラック”などのクラスの共通部分を抽出じ自動車”クラスとして定義することを，汎化という。
ウ　“バス”，“ドラック”などのクラスは，“自動車”クラスに対するオブジェクトという。
エ　“バス”，“ドラック”などのそれぞれのクラスの違いを“自動車”クラスとして

定義することを，特化という。

問 23　SOA（Service Oriented Architecture）の説明はどれか。

ア　Web サービスを利用するためのインタフェースやプロトコルを規定したものである。
イ　XML を利用して，インターネット上に存在する Web サービスを検索できる仕組みである。
ウ　業務機能を提供するサービスを組み合わせることによって，システムを構築する考え方である。
エ　サービス提供者と委託者との間でサービスの内容，範囲及び品質に対する要求水準を明確にして，あらかじめ合意を得ておくことである。

問 24　情報システムの設計において，フェールソフトが講じられているのはどれか。

ア　UPS 装置を設置することで，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で，システムの誤動作を防止できるようにする。

問 25　“情報セキュリティ監査基準”の位置付けはどれか。

ア　監査人が情報資産の監査を行う際に判断の尺度として用いるべき基準であり，監査人の規範である。
イ　情報資産を保護するためのベストプラクティスをまとめたものであり，監査マニュアル作成の手引書である。
ウ　情報セキュリティ監査業務の品質を確保し，有効かつ効率的に監査を実施することを目的とした監査人の行為規範である。
エ　組織体が効果的な情報セキュリティマネジメント体制を構築し，適切なコントロールを整備，運用するための実践規範である。

午前Ⅱ試験

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

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

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