問 1 正解 完璧 直前チェック

特定の認証局が発行した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，失効したディジタル証明書に対応する秘密鍵が登録される。
イ　CRLには，有効期限内のディジタル証明書のうち破棄されているディジタル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　有効期限切れで失効したディジタル証明書は，所有者が新たなディジタル証明書を取得するまでの間，CRLに登録される。

問 2 正解 完璧 直前チェック

XML署名において署名対象であるオブジェクトの参照を指定する表記形式はどれか。

ア　OIDの形式
イ　SSIDの形式
ウ　URIの形式
エ　ディジタル証明書のシリアル番号の形式

問 3 正解 完璧 直前チェック

クラウドサービスにおける，従量課金を利用したEDoS（Economic Denial of Service，Economic Denial of Sustainability）攻撃の説明はどれか。

ア　カード情報の取得を目的に，金融機関が利用しているクラウドサービスに侵入する攻撃
イ　課金回避を目的に，同じハードウェア上に構築された別の仮想マシンに侵入し，課金機能を利用不可にする攻撃
ウ　クラウド利用企業の経済的な損失を目的に，リソースを大量消費させる攻撃
エ　パスワード解析を目的に，クラウド環境のリソースを悪用する攻撃

春

問1　イ

解説　**CRL**（Certificate Revocation List）は，有効期間中に失効した公開かぎ証明書を記載したリストで，認証局から発行される。公開かぎ証明書の検証時に，公開かぎ証明書の失効確認に使用するため常に参照される。

公開かぎ証明書の有効期間中に秘密かぎの紛失や漏えいが発生した場合には該当する証明書の廃棄手続きが行われ，公開かぎ証明書のシリアル番号がCRLに記載される。

ア：秘密鍵ではなく，公開鍵が登録される。
ウ：CRLは定期的に更新されるがリアルタイムに更新されない。
エ：失効したディジタル証明書は，所有者が新たなディジタル証明書を取得してもCRLに登録された状態を継続する。

問2　ウ

解説　XML署名は，XML文書に付加する署名である。署名のアルゴリズムや証明書あるいは署名のタグを定め，任意のデータに署名を付けられるだけでなく，XML文書の指定したエレメントやコンテントに対して署名を付けることもできる。署名の表示形式はURI（Uniform Resource Identifier）が使用される。

OID（Object IDentifier）：オブジェクト識別子である。通信において識別されるべきオブジェクトを，全世界で一意に識別できるよう管理するために割り当てられた値である。

SSID（Service Set ID）：無線LANのアクセスポイントを識別するためのIDである。

問3　ウ

解説　**EDoS**（Economic Denial of Service）は，クラウドサービスで従量課金となっているネットワーク利用料金を利用して，利用企業のサーバに対する従量課金金額を増やすことを目的とした攻撃である。攻撃された企業のサーバは課金額が膨大となり支払による経済的な損失が発生する。

問 4 正解 完璧 直前チェック

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IP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 5 正解 完璧 直前チェック

PCなどに内蔵されるセキュリティチップ（TPM：Trusted Platform Module）がもつ機能はどれか。

ア　TPM間での共通鍵の交換
イ　鍵ペアの生成
ウ　ディジタル証明書の発行
エ　ネットワーク経由の乱数送信

問 6 正解 完璧 直前チェック

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　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。
エ　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付けられるものだけを通過させることができる。

春

問4　イ

解説 **OP25B**（Outbound Port 25 Blocking）は，内部ネットワークから外部ネットワークへのポート25番の通信（SMTP）を遮断する手法である。例えば，ISPがOP25Bを用いることで，会員がISPの外部ネットワークに存在するメールサーバを使用してスパムメールを送信しようとすることを防止することが可能となる。

問5　イ

解説 **TPM**（Trusted Platform Module）とは，PCに内蔵する暗号化の鍵を格納するセキュリティチップである。一般的に，企業向けPCのハードディスクを暗号化してセキュリティを高めるために，このチップの搭載が進んでいる。

仕組みとしては，ハードディスクを暗号化する鍵をセキュリティチップに記録する。ハードディスクが盗難にあってもセキュリティチップに格納された鍵がなければ複合できない。

セキュリティチップには，ハードディスクに格納するデータを暗号化するための鍵を生成する機能がある。

ア：TPM間の共通鍵ではなく，TPMとハードディスク間の共通鍵交換となる。
ウ：証明書の発行は，TPMでは行えない。
エ：TPMはPC内のみで利用できる。PCからはずすとPCが起動できなくなる。したがって，取り外しやネットワーク経由等では利用できない。

問6　エ

解説 **ダイナミックパケットフィルタリング**は，ファイアウォールのパケット通過時のパケット開放の方式である。内部から外部への通信を実行した際に，外部からの戻りパケットもファイアウォールで開放する必要がある。ダイナミックパケットフィルタリングでは，戻りパケットを必要な状況に応じて動的に開放し，要求がない場合はポートを閉じておく方式である。

ア：IPアドレスの変換とは関係がない。
イ：パケットの暗号化とは関係がない。
ウ：パケットのデータ部分のチェックは行っていない。

問 7 正解 完璧 直前チェック

ポリモーフィック型の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　感染するごとにウイルスのコードを異なる鍵で暗号化し，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 正解 完璧 直前チェック

ICMP Flood攻撃に該当するものはどれか。

ア　HTTP GETコマンドを繰返し送ることによって，攻撃対象のサーバにコンテンツ送信の負荷を掛ける。
イ　pingコマンドを用いて大量の要求パケットを発信することによって，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。
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てリソースを枯渇させる。

問 9 正解 完璧 直前チェック

自ネットワークのホストへの侵入を，ファイアウォールにおいて防止する対策のうち，IPスプーフィング（spoofing）攻撃の対策について述べたものはどれか。

ア　外部から入るTCPコネクション確立要求パケットのうち，外部へのインターネットサービスの提供に必要なもの以外を破壊する。
イ　外部から入るUDPパケットのうち，外部へのインターネットサービスの提供や利用したいインターネットサービスに必要なもの以外を破棄する。
ウ　外部から入るパケットの宛先IPアドレスが，インターネットとの直接の通信をすべきでない自ネットワークのホストのものであれば，そのパケットを破棄する。

エ　外部から入るパケットの送信元IPアドレスが自ネットワークのものであれば，そのパケットを破棄する。

春

問7　イ

解説　**ポリモーフィック型ウイルス**は，感染するたびにウイルス自体を暗号化することにより，ウイルス対策ソフトから検知されないように振る舞うウイルスである。暗号化されたコードは変化するが，ウイルスが発動するときの復号ロジックは変換しないという特徴がある。ウイルス対策ソフト側では，この特徴を利用してウイルス感染を検出する。
ア：ハッキングまたはクラッキングの説明である。

問8　イ

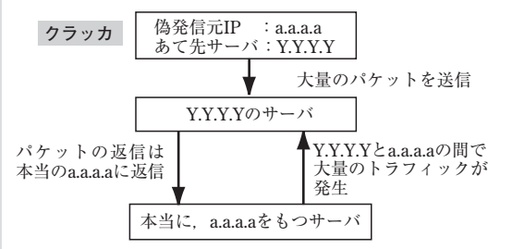
解説　**ICMP Flood**攻撃は，pingを用いてサーバに対して行われる代表的なDoS（Denial of Service:：サービス不能）攻撃の一つである。選択肢イ，ウ，エの攻撃との違いは，ICMPを利用している点である。利用するプロトコルにより攻撃名称が異なる。
ICMP（Internet Control Message Protocol）：pingやtraceroute（経路情報を得るコマンド）に用いられる送信エラーや，制御メッセージの通知に利用される。
ア：**HTTP GET Flood**の説明である。
ウ：**TCP SYN Flood**の説明である。
エ：**TCP Connection Flood**の説明である。

問9　エ

解説　**IPスプーフィング**とは，攻撃者が送信元を隠ぺいするために，送信元IPアドレスを偽装したパケットを相手に送りつけることである。外部からのパケットは，通常であれば発信元は「外部」，あて先は「自ネットワーク」となる。しかし選択肢エでは，発信元が自ネットワークであり，自ネットワークを発信元としたパケットが外部から送られてくることは不自然である。

選択肢ア，イ，ウは，IPスプーフィングではなく，不正アクセスに対する防止策である。

IPスプーフィングで発信元を偽装したDoS攻撃のときのパケットの流れは，右図のようになる。



問 10 正解 完璧 直前チェック

Webサーバが HTTPS 通信の応答で cookie に Secure 属性を設定したときのブラウザの処理はどれか。

ア　ブラウザは，cookie の “Secure=” に続いて指定された時間を参照し，指定された時間を過ぎている場合にその cookie を削除する。
イ　ブラウザは，cookie の “Secure=” に続いて指定されたホスト名を参照し，指定されたホストにその cookie を送信する。
ウ　ブラウザは，cookie の “Secure” を参照し，HTTPS 通信時だけその cookie を送信する。
エ　ブラウザは，cookie の “Secure” を参照し，ブラウザの終了時にその cookie を削除する。

問 11 正解 完璧 直前チェック

テンペスト（TEMPEST）攻撃を説明したものはどれか。

ア　故意に暗号化演算を誤動作させて正しい処理結果との差異を解析する。
イ　処理時間の差異を計測し解析する。
ウ　処理中に機器から放射される電磁波を観測し解析する。
エ　チップ内の信号線などに探針を直接当て，処理中のデータを観測し解析する。

問 12 正解 完璧 直前チェック

脆弱性検査で，対象ホストに対してポートスキャンを行った。対象ポートの状態を判定する方法のうち，適切なものはどれか。

ア　対象ポートに SYN パケットを送信し，対象ホストから “RST/ACK” パケットを受信するとき，対象ポートが開いていると判定する。
イ　対象ポートに SYN パケットを送信し，対象ホストから “SYN/ACK” パケットを受信するとき，対象ポートが閉じていると判定する。
ウ　対象ポートに UDP パケットを送信し，対象ホストからメッセージ “port unreachable” を受信するとき，対象ポートが閉じていると判定する。
エ　対象ポートに UDP パケットを送信し，対象ホストからメッセージ “port unreachable” を受信するとき，対象ポートが開いていると判定する。

春

問10　ウ

解説　WebサーバがHTTPS通信を利用している場合，セッションIDが第三者に漏えいすることを防止するために，cookie発行時にSecure属性を付ける対策がある。これは，Webへのアクセスの際に同一ホスト内で，HTTPのページとHTTPSのページがあり相互に行き来する場合にHTTP通信時にHTTPSで使うべきcookieの値が流出する可能性があるためである。対処方法としては，HTTPS通信時だけcookieを送信する。

問11　ウ

解説　**テンペスト**（TEMPEST）**攻撃**とは，コンピュータやディスプレイ，ケーブル等から放射される電磁波を受信・解析することで，キー入力情報の収集や表示画面の復元などを行う攻撃（盗聴）手法である。

テンペスト攻撃の対策としては，周辺機器やケーブル等をシールドして電波の放射を防ぐ方法が有効である。具体的には，回線設計の段階で信号の漏えいを防ぎつつ，ケーブル等を被覆して電磁波をシールドすることが基本的な対策である。また，コンピュータの設置された部屋全体をシールドする手段もある。

問12　ウ

解説　ポートスキャンの結果から状態を判定する場合，TCP，UDP両方のポートが開いている場合と閉じている場合の動作を理解する必要がある。

ア：**RST/ACK（リセット）**が返信された場合は，ポートは閉じていると判断する。RST/ACKは，通信を拒否されたときに返信されるパケットとなる。

イ：**SYN/ACK（応答）**が返信された場合は，ポートは開いていると判断する。SYN/ACKは，通信を許可されたパケットである。

ウ：**port unreachable（ポート到達不可）**は，ポートが閉じている場合に受信するパケットである。

問 13 正解 完璧 直前チェック

無線LANのセキュリティ対策に関する記述のうち，適切なものはどれか。

ア　EAPは，クライアントPCとアクセスポイントとの間で，あらかじめ登録した共通鍵による暗号化通信を実現できる。

イ　RADIUSでは，クライアントPCとアクセスポイントとの間で公開鍵暗号方式による暗号化通信を実現できる。

ウ　SSIDは，クライアントPCごとの秘密鍵を定めたものであり，公開鍵暗号方式による暗号化通信を実現できる。

エ　WPA2では，IEEE 802.1Xの規格に沿った利用者認証及び動的に更新される暗号化鍵を用いた暗号化通信を実現できる。

問 14 正解 完璧 直前チェック

JVN（Japan Vulnerability Notes）などの脆弱性対策ポータルサイトで採用されているCWE（Common Weakness Enumeration）はどれか。

ア　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製品の脆弱性を評価する手法

イ　製品を識別するためのプラットフォーム名の一覧

ウ　セキュリティに関連する設定項目を識別するための識別子

エ　ソフトウェアの脆弱性の種類の一覧

春

問13　エ

解説

EAP（Extensible Authentication Protocol）：PPP（Point to Point Protocol）を拡張した認証プロトコル。ユーザID/パスワード以外にも，スマートカード（ICカード）やディジタル証明書など様々な認証方式をサポートしている。EAP-TLS,EAP-TTLSなどがある。

RADIUS（Remote Authentication Dial In User Service）：アクセスサーバと認証サーバ間でやり取りする認証プロトコル。クライアントが認証を求める際に，認証を必要とするサーバ（アクセスサーバ）と認証機能を分離し，利用者の一元管理，アクセスログの記録が可能となる。

SSID（Service Set ID）：無線LANのアクセスポイントを識別するためのIDである。

WPA2（Wi-Fi Protected Access 2）：WPAの改良版で，AES（Advanced Encryption Standard）を採用したCCMP（Counter-mode with CBC-MAC Protocol）暗号化方式である。無線の暗号化は，WEPがセキュリティ的に脆弱だということでWPAが作られ，さらに強力なWPA2が作られた。日々の技術進歩により，暗号を解読できる速度が速くなるためより強力な暗号技術が必要となっている。

問14　エ

解説

JVN（Japan Vulnerability Notes）：日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し，情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト。JPCERT コーディネーションセンターと独立行政法人情報処理推進機構（IPA）が共同で運営している。

CWE（Common Weakness Enumeration）：ソフトウェアにおけるセキュリティ上の弱点（脆弱性）の種類を識別するための共通の基準としての識別子である。脆弱性タイプは，ビュー（View），カテゴリー（Category），脆弱性（Weakness），複合要因（Compound Element）の4種類に分類される。

問 15 正解 完璧 直前チェック

Webアプリケーションの脆弱性を悪用する攻撃手法のうち，Perlのsystem関数やPHPのexec関数など外部プログラムの呼出しを可能にするための関数を利用し，不正にシェルスクリプトや実行形式のファイルを実行させるものは，どれに分類されるか。

ア　HTTPヘッダインジェクション
イ　OSコマンドインジェクション
ウ　クロスサイトリクエストフォージェリ
エ　セッションハイジャック

問 16 正解 完璧 直前チェック

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 17 正解 完璧 直前チェック

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の旧バージョンのライブラリを，攻撃者が外部から破壊する。

春

問15　イ

解説

HTTPヘッダインジェクション：動的にHTTPヘッダが生成されるHTTP通信の機能を利用した攻撃手法。HTTPヘッダに改行コードを生成させることで不正な動作を実行させる。

OSコマンドインジェクション：サーバ内のOSコマンドを外部から実行させることでサーバに不正な動作を実行させる攻撃手法。

クロスサイトリクエストフォージェリ：Webサイトに埋め込まれているスクリプトや命令が，利用者がそのWebサイトにアクセスすることによって自動的に実行させられてしまう攻撃手法。掲示板への書き込みやオンラインショップでの買い物などが，意図せずに行われてしまう。

セッションハイジャック：セッションIDを盗み出すことでセッションを乗っ取り，あたかもそのセッションの参加者であることを装う攻撃手法。セッションの参加者でなければ見ることのできない情報を盗み出すことができる。

問16　イ

解説 **WAF**（Web Application Firewall）：Webアプリケーションのやり取りを把握・管理することによって不正侵入を防御するファイアウォール。プログラムに渡される入力内容などを直接に検査することによって，不正と見なされたアクセス要求を遮断する仕組みが採用されている。クライアントの操作するWebブラウザとWebサーバ間に介在し，ブラウザとの直接的なやり取りをWAFが受け持つ。**SQLインジェクション**や**クロスサイトスクリプティング**，**強制ブラウジング**といった要求はWAFが遮断する。

ブラックリストには問題のある通信データパターンが定義され，**ホワイトリスト**には問題のない正規の通信データパターンが定義されている。それ以外の通信はいわばグレーゾーンであり，ホワイトリストで許可してそれ以外のグレーゾーンを含む通信を拒否するか，ブラックリストのみ拒否してそれ以外のグレーゾーンを含む通信を許可するのかを考えなければならない。

日々新しいWebアプリケーションは増えており，新しい攻撃もあるため，運用まで考慮すると，ブラックリストとホワイトリストの優劣はつけ難い。

問17　ア

解説 **SSLのバージョンロールバック攻撃**は，SSL通信経路上の攻撃者により脆弱なバージョンを利用する事を強制させられ，情報を盗み取られることである。一般的には，脆弱制のあるバージョンの利用を無効にするなどの対策を取ることで回避可能である。

ウ：**サイドチャネル攻撃**の説明である。

問 18 正解 完璧 直前チェック

10 Mビット/秒のLANで接続された4台のノード（A，B，C，D）のうち，2組（AとB，CとD）のノード間でそれぞれ次のファイル転送を行った場合，LANの利用率はおよそ何％か。ここで，転送時にはファイルの大きさの30％に当たる各種制御情報が付加されるものとする。また，LANではリピータハブが使用されており，更に衝突は考えないものとする。

ファイルの大きさ：平均1,000バイト
ファイルの転送頻度：平均60回/秒（1組当たり）

ア 2　　イ 6　　ウ 10　　エ 12

問 19 正解 完璧 直前チェック

VoIPにおいて，ユーザエージェント間のセッションの確立，変更，切断を行うプロトコルはどれか。

ア RTCP　　イ RTP　　ウ SDP　　エ SIP

問 20 正解 完璧 直前チェック

インターネットVPNを実現するために用いられる技術であり，ESP（Encapsulating Security Payload）やAH（Authentication Header）などのプロトコルを含むものはどれか。

ア IPsec　　イ MPLS　　ウ PPP　　エ SSL

春

問18 エ

解説 このLANでは**リピータハブ**を用いているので，二つのファイル転送は回線を共有している。衝突は考えなくて良いので，2組の転送のそれぞれの転送時間を単純に合計したものが答えとなる。

転送されるファイルには30％の制御情報が付加され，1秒当たり平均60回転送される。これが2組あるので，1秒当たりの転送データ量は1,248kビットとなる。ここで，1バイト＝8ビットの変換を忘れないこと。

1,000 × 1.3 × 60 × 2 = 156kバイト/秒 = 1,248kビット/秒

この値で10Mビット/秒のLANを用いて転送するときの利用率は12.48％となる。

1,248kビット/秒 ÷ 10Mビット/秒 = 0.1248 ≒ 12％

問19 エ

解説

RTCP（Real Time Control Protocol）：通話参加者に管理パケットを送信するプロトコル。RTPとセットで利用される。

RTP（Real Time Transport Protocol）：音声データを送信するためのプロトコル。RTCPとセットで利用される。

SDP（Session Description Protocol）：マルチメディアセッションの記述に利用される。SDPは，SIPによるセッション確立の中で利用される。

SIP（Session Initiation Protocol）：セッションの確立，変更，切断を行うプロトコル。

問20 ア

解説

IPSec（IP Security Architecture）：データの完全性検証に用いる**AH**（Authentication Header）と，データの暗号化に用いる**ESP**（Encapsulated Security Payload）の二つのセキュリティプロトコルから構成されている。

MPLS（Multi Protocol Label Switching）：主にWANで使用されるL3スイッチングである。ルーティング情報にラベルを付けることで，ルーティングを高速化する技術である。

PPP（Point to Point Protocol）：ダイヤルアップによるISPへの接続などに用いられるデータリンク層プロトコル。認証機能やデータ圧縮機能等を備えている。

SSL（Secure Socket Layer）：OSI参照モデルのトランスポート層（第4層）の情報を暗号化して送受信するプロトコルである。HTTPなどのプロトコルのデータを暗号化し，プライバシーに関わる情報やクレジットカード番号，企業秘密等を安全に送受信することができる。

問 21 正解 完璧 直前チェック

関係モデルにおける外部キーに関する記述のうち，適切なものはどれか。

ア　外部キーの値は，その関係の中で一意でなければならない。
イ　外部キーは，それが参照する候補キーと比較可能でなくてもよい。
ウ　参照先の関係に，参照元の外部キーの値と一致する候補キーが存在しなくてもよい。
エ　一つの関係に外部キーが複数存在してもよい。

問 22 正解 完璧 直前チェック

UML2.0において，オブジェクト間の相互作用を時間の経過に注目して記述するものはどれか。

ア　アクティビティ図　　イ　コミュニケーション図
ウ　シーケンス図　　エ　ユースケース図

問 23 正解 完璧 直前チェック

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。

春

問21　エ

解説　**外部キー**とは，テーブルのカラムに，別テーブルの特定カラムに含まれる項目のみに限定することである。例えば，商品コードの列に，商品テーブルの商品コードを外部キーとして設定することで，商品テーブルに含まれる商品コード以外の内容を入力できなくすることや，商品コードを選択して入力する操作を可能とする。

問22　ウ

解説　オブジェクト間の相互作用を表す図には，**シーケンス図**と**コミュニケーション図**がある。シーケンス図は相互作用を時間の経過に注目して記述し，コミュニケーション図はオブジェクト間の関係に注目して記述する。

アクティビティ図は，処理の流れを表現する図で，ビジネスプロセスやワークフローのモデリングに利用される。

ユースケース図は，システムが外部に提供する機能（ユースケース）を表現する図である。

問23　ウ

解説　**SOA**：サービス指向アーキテクチャは，サービスの集まりとしてシステムを構築する手法である。サービスとは外部から標準化された手順で呼び出すことができるひとまとまりのソフトウェアの集合であり，各サービスがXMLで記述されたメッセージをSOAPでやり取りし，連携して動作する。

ア：**SOAP**（Simple Object Access Protocol）の説明である。
イ：**UDDI**（Universal Description，Discovery，and Integration）の説明である。
エ：**SLA**（Service Level Agreement）の説明である。

問 24 正解 完璧 直前チェック

システムの改善に向けて提出された4案について，評価項目を設定して採点した結果を，採点結果表に示す。効果及びリスクについては5段階評価とし，それぞれの評価項目の重要度に応じて，重み付け表に示すとおりの重み付けを行った上で次の式で総合評価点を算出したとき，総合評価点が最も高い改善案はどれか。

〔総合評価点の算出式〕

総合評価点＝効果の総評価点－リスクの総評価点

採点結果表

	評価項目＼案	案1	案2	案3	案4
効果	セキュリティ強化	3	4	5	2
効果	システム運用品質向上	2	4	2	5
効果	作業コスト削減	5	4	2	4
リスク	スケジュールリスク	2	4	1	5
リスク	技術リスク	4	1	5	1

重み付け表

	評価項目	重み
効果	セキュリティ強化	4
効果	システム運用品質向上	2
効果	作業コスト削減	3
リスク	スケジュールリスク	8
リスク	技術リスク	3

ア　案1　　イ　案2　　ウ　案3　　エ　案4

問 25 正解 完璧 直前チェック

システム監査報告書に記載された改善勧告に対して，被監査部門から提出された改善計画を経営者がITガバナンスの観点から評価する際の方針のうち，適切なものはどれか。

ア　1年以内に実現できる改善を実施する。
イ　経営資源の状況を踏まえて改善を実施する。
ウ　情報システムの機能面の改善に絞って実施する。
エ　被監査部門の予算の範囲内で改善を実施する。

春

問24　ウ

解説　問題文に指定された重み付けを利用して総合評価点を計算する。計算式は次のとおり。

各システムの改善案の採点結果×各評価項目の重み付け＝各項目の評価点

案1：(3×4+2×2+5×3)－(2×8+4×3)=3
案2：(4×4+4×2+4×3)－(4×8+1×3)=1
案3：(5×4+2×2+2×3)－(1×8+5×3)=7
案4：(2×4+5×2+4×3)－(5×8+1×3)=−13
総合評価点が最も高い改善策は，案3の7となる。

問25　イ

解説　**システム監査報告書**に記載された改善勧告は，実施されることが必要であるが，経営資源の状況によっては，必ずしも直ちに実施できるわけではない。
ア：1年以上かかる改善勧告であっても実施されなければならない。
ウ：システムの機能面だけでなく，セキュリティ面なども考慮し実施されなければならない。
エ：必要な改善は，予算措置を行ってでも実施されなければならない。