問 1

正解 □ 完璧 □ 直前チェック □

AESの特徴はどれか。

ア　鍵長によって，段数が決まる。
イ　段数は，6段以内の範囲で選択できる。
ウ　データの暗号化，復号，暗号化の順に3回繰り返す。
エ　同一の公開鍵を用いて暗号化を3回繰り返す。

問 2

正解 □ 完璧 □ 直前チェック □

SSL/TLSのダウングレード攻撃に該当するものはどれか。

ア　暗号化通信中にクライアントPCからサーバに送信するデータを操作して，強制的にサーバのディジタル証明書を失効させる。
イ　暗号化通信中にサーバからクライアントPCに送信するデータを操作して，クライアントPCのWebブラウザを古いバージョンのものにする。
ウ　暗号化通信を確立するとき，弱い暗号スイートの使用を強制することによって，解読しやすい暗号化通信を行わせる。
エ　暗号化通信を盗聴する攻撃者が，暗号鍵候補を総当たりで試すことによって解読する。

問 3

正解 □ 完璧 □ 直前チェック □

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，不用意に捨てられた機密情報の印刷物をオフィスの紙ごみの中から探し出す。
ウ　通信を行う2者間に割り込んで，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。

春
秋

問1　ア

解説　**AES**（Advanced Encryption Standard）は，米国政府標準の共通鍵暗号方式である。
共通鍵暗号方式は，暗号化鍵と復号鍵に同じ鍵を使用するため，鍵を共有する手続きが必要である。
鍵長は128ビット，192ビット，256ビットの選択が可能なSPN型ブロック暗号である。ブロック長は128ビットとなっている。SPN型ブロック暗号とは，換字と転置を繰り返す暗号方式で，これを「段」と呼ぶ複数回の繰り返しによって暗号化の強度を上げる方式である。

問2　ウ

解説　**SSL**（Secure Sockets Layer）**/TLS**（Transport Layer Security）**のダウングレード攻撃**は，サーバとクライアントの通信がTLSの高い強度バージョンを利用して通信できるにもかかわらず，低いバージョンで通信するよう攻撃されることである。低いバージョンで通信するよう攻撃された場合，通信データの盗聴によって内容を読み取られてしまう。
ア：ディジタル証明書を失効させられることではない。
イ：Webブラウザを古いバージョンにするものではない。
エ：暗号鍵候補を総当たりで試すことではない。総当たり攻撃の説明である。

問3　ア

解説　**サイドチャネル攻撃**は，暗号を解読するための攻撃手法の一つである。暗号化や復号をする際に発生する電磁波，熱，演算処理時間など暗号化を直接解読するのではなく，外部からの観測といった二次的要素から解読を行う手法である。
イ：**スキャベンジング**の説明である。
ウ：**中間者攻撃**（man in the middle attack）の説明である。
エ：**SQLインジェクション攻撃**の説明である。

問 4 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 5 正解 □ 完璧 □ 直前チェック □

セッションIDの固定化（Session Fixation）攻撃の手口はどれか。

ア　HTTPS通信でSecure属性がないCookieにセッションIDを格納するWebサイトにおいて，HTTP通信で送信されるセッションIDを悪意のある者が盗聴する。
イ　URLパラメタにセッションIDを格納するWebサイトにおいて，Refererによってリンク先のWebサイトに送信されるセッションIDが含まれたURLを，悪意のある者が盗用する。
ウ　悪意のある者が正規のWebサイトから取得したセッションIDを，利用者のWebブラウザに送り込み，利用者がそのセッションIDでログインして，セッションがログイン状態に変わった後，利用者になりすます。
エ　推測が容易なセッションIDを生成するWebサイトにおいて，悪意のある者がセッションIDを推測し，ログインを試みる。

問4　イ

解説 **TPM**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5　ウ

解説 **セッションIDの固定化**は，悪意のある者が正規のWebサイトから取得したセッションIDを，利用者のWebブラウザに送り込み，利用者がそのセッションIDでログインして，セッションがログイン状態に変わった後，利用者になりすます攻撃である。

ア：HTTPS通信でSecure属性がないCookieの盗聴は可能であるが，セッションIDの固定化攻撃ではない。
イ，エ：方式は違うがどちらも，セッションハイジャックの説明である。

問 6 正解 □ 完璧 □ 直前チェック □

DNS水責め攻撃（ランダムサブドメイン攻撃）の手口と目的に関する記述のうち，適切なものはどれか。

ア　ISPが管理するDNSキャッシュサーバに対して，送信元を攻撃対象のサーバのIPアドレスに詐称してランダムかつ大量に生成したサブドメイン名の問合せを送り，その応答が攻撃対象のサーバに送信されるようにする。

イ　オープンリゾルバとなっているDNSキャッシュサーバに対して，攻撃対象のドメインのサブドメイン名をランダムかつ大量に生成して問い合わせ，攻撃対象の権威DNSサーバを過負荷にさせる。

ウ　攻撃対象のDNSサーバに対して，攻撃者が管理するドメインのサブドメイン名をランダムかつ大量に生成してキャッシュさせ，正規のDNSリソースレコードを強制的に上書きする。

エ　攻撃対象のWebサイトに対して，当該ドメインのサブドメイン名をランダムかつ大量に生成してアクセスし，非公開のWebページの参照を試みる。

問 7 正解 □ 完璧 □ 直前チェック □

FIPS PUB 140-2の記述内容はどれか。

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技術仕様

エ　無線LANセキュリティの技術仕様

問6　イ

解説 **DNS水責め攻撃**（ランダムサブドメイン攻撃）は，オープンリゾルバとなっているDNSキャッシュサーバに対して，攻撃対象のドメインのサブドメイン名をランダムかつ大量に生成して問い合わせ，攻撃対象の権威DNSサーバを過負荷にさせる攻撃である。

ア：DNSリフレクター攻撃の説明である。

ウ：DNSキャッシュポイズニング攻撃の説明である。

エ：ディレクトリトラバーサル攻撃の説明である。

問7　ア

解説 **FIPS PUB 140-2**：暗号モジュールに関するセキュリティ要件仕様を規定する米国連邦標準規格。

イ：BS7799-2や国内規格のISMS認証基準Ver.2.0の後継として開発された国際規格および国内規格として，JIS Q 27001がある。

ウ：インターネットのためのX.509 公開鍵基盤（PKI）に対する標準がある。

エ：IEEE 802.11 無線LANの国際規格の中では，セキュリティ技術としてSSID（Service Set Identifier），MACアドレスフィルタリング，WEP（Wired Equivalent Privacy），WPA2（Wi-Fi Protected Access 2）などがある。

問 8 正解 完璧 直前チェック

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ビ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に対するセキュリティパッチの管理と適用を実施可か実施不可かの組合せのうち，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 9 正解 完璧 直前チェック

個人情報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　個人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。
イ　個人情報の保管場所に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。
ウ　個人情報を含む情報資産を外部のデータセンタに預託する。
エ　収集済みの個人情報を消去し，新たな収集を禁止する。

問 10 正解 完璧 直前チェック

JVNなどの脆弱性対策ポータルサイトで採用されているCVE（Common Vulnerabilities and Exposures）識別子の説明はどれか。

ア　コンピュータで必要なセキュリティ設定項目を識別するための識別子である。
イ　脆弱性が悪用されて改ざんされたWebサイトのスクリーンショットを識別するための識別子である。
ウ　製品に含まれる脆弱性を識別するための識別子である。
エ　セキュリティ製品を識別するための識別子である。

問8　イ

解説　**NIST**（National Institute of Standards and Technology：米国国立標準研究所）は，連邦政府機関の標準およびガイドラインを作成する機関である。

NISTによるパブリッククラウドのサービスモデル定義では，次のように説明されている。

SaaS（Cloud Software as a Service）：利用者に提供される機能は，クラウドのインフラ上で稼動しているプロバイダ由来のアプリケーション。例外はユーザ固有のアプリケーション設定である。

PaaS（Cloud Platform as a Service）：利用者に提供される機能は，クラウドのインフラ上にユーザが開発したまたは購入したアプリケーションを実装することである。サーバ，OS，ストレージの管理権限は利用者に提供されない。

IaaS（Cloud Infrastructure as a Service）：利用者に提供される機能は，演算機能，ストレージ，ネットワークその他の基本的コンピューティングリソースである。利用者は任意のソフトゥエアを実装し走らせることができる。

本問では，OSに係る設定作業とセキュリティパッチ管理作業を利用者企業の管理であるか，サービス提供側であるかとなるため，イの範囲が正しい。

問9　エ

解説　リスク対応には，**リスク回避**，**リスク受容**，**リスク移転**，**リスク低減**がある。

リスク回避：リスクが発生しないように事前に対策を行うこと。

リスク受容：リスクがあることがわかっていても，対策を行わないこと。被害の影響がきわめて小さい場合や，リスクの発生頻度がきわめて低い場合の対応方法である。

リスク移転：保険や，他への委託により，第三者へリスクを移すことである。

リスク低減：リスク対策を行い，リスクが発生を低減することである。

ア：リスク受容に該当する。
イ：リスク低減に該当する。
ウ：リスク移転に該当する。
エ：リスク回避に該当する。

問10　ウ

解説　**JVN**は，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である。JPCERTコーディネーションセンター（JPCERT/CC）と，独立行政法人情報処理推進機構（IPA）が共同運営している。CVEは，脆弱性を識別するための識別子である。

問 11 正解 完璧 直前チェック

インターネットバンキングの利用時に被害をもたらすMITB（Man-in-the-Browser）攻撃に有効な対策はどれか。

ア　インターネットバンキングでの送金時にWebブラウザで利用者が入力した情報と，金融機関が受信した情報とに差異がないことを検証できるよう，トランザクション署名を利用する。
イ　インターネットバンキングでの送金時に接続するWebサイトの正当性を確認できるよう，EV SSLサーバ証明書を採用する。
ウ　インターネットバンキングでのログイン認証において，一定時間ごとに自動的に新しいパスワードに変更されるワンタイムパスワードを用意する。
エ　インターネットバンキング利用時の通信をSSLではなくTLSを利用して暗号化する。

問 12 正解 完璧 直前チェック

Webアプリケーションの脆弱(ぜい)性を悪用する攻撃手法のうち，Webページ上で入力した文字列がPerlのsystem関数やPHPのexec関数などに渡されることを利用し，不正にシェルスクリプト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 13 正解 完璧 直前チェック

ウイルス対策ソフトでの，フォールスネガティブに該当するものはどれか。

ア　ウイルスに感染していないファイルを，ウイルスに感染していないと判断する。
イ　ウイルスに感染していないファイルを，ウイルスに感染していると判断する。
ウ　ウイルスに感染しているファイルを，ウイルスに感染していないと判断する。
エ　ウイルスに感染しているファイルを，ウイルスに感染していると判断する。

問11　ア

解説　**MITB攻撃**は，ネットバンキングユーザーの端末上のWebブラウザを乗っ取り，アカウント情報を盗み見ることや，ブラウザ上の画面を書き換えることで送金情報を変更することである。，ネットバンキングサイトに正規の認証プロセスを経てログインした後に，Webブラウザを不正に操る攻撃のため，Webブラウザでの入力情報と，金融機関が受信した情報に差異がないことを確認する必要がある。
イ，ウ，エ：インターネットバンキングへの接続に対してのセキュリティを強化してもMITBの場合，正規の認証を利用するため有効な対策とはいえない。

問12　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13　ウ

解説　**フォールスネガティブ**と合わせて，**フォールスポジティブ**がある。
フォールスネガティブ：検出漏れ，異常なものを検知できなかったこと。
フォールスポジティブ：誤検知，正常なものを異常と検知する。
ア，エ：正常な動作である。
イ：フォールスポジティブである。
ウ：フォールスネガティブである。

問 14 正解 完璧 直前チェック

特定の利用者が所有するリソースが，WebサービスA上にある。OAuth 2.0において，その利用者の認可の下，WebサービスBからそのリソースへの限定されたアクセスを可能にするときのプロトコルの動作はどれか。

ア　WebサービスAが，アクセストークンを発行する。
イ　WebサービスAが，利用者のディジタル証明書をWebサービスBに送信する。
ウ　WebサービスBが，アクセストークンを発行する。
エ　WebサービスBが，利用者のディジタル証明書をWebサービスAに送信する。

問 15 正解 完璧 直前チェック

インターネットサービスプロバイダ（ISP）が，OP25Bを導入する目的はどれか。

ア　ISP管理外のネットワークに対するISP管理下のネットワークからのICMPパケットによるDDoS攻撃を遮断する。
イ　ISP管理外のネットワークに向けてISP管理下のネットワークから送信されるスパムメールを制限する。
ウ　ISP管理下のネットワークに対するISP管理外のネットワークからのICMPパケットによるDDoS攻撃を遮断する。
エ　ISP管理下のネットワークに向けてISP管理外のネットワークから送信されるスパムメールを制限する。

問 16 正解 完璧 直前チェック

サンドボックスの仕組みに関する記述のうち，適切なものはどれか。

ア　Webアプリケーションの脆弱性を悪用する攻撃に含まれる可能性が高い文字列を定義し，攻撃であると判定した場合には，その通信を遮断する。
イ　クラウド上で動作する複数の仮想マシン（ゲストOS）間で，お互いの操作ができるように制御する。
ウ　プログラムの影響がシステム全体に及ばないように，プログラムが実行できる機能やアクセスできるリソースを制限して動作させる。
エ　プログラムのソースコードでSQL文の雛形の中に変数の場所を示す記号を置いた後，実際の値を割り当てる。

問14　ア

解説 **OAuth2.0**とは，利用者へのWebサービスアクセス権を，利用者の代理で許可するための認証用プロトコルである。OAuthを利用すると，利用者は認証の際にユーザ名やパスワードをコンテンツ提供者に知らせることなくアクセス許可認証を行うことができる。

WebサービスBが認証を取得する場合は，リソースを所有しているWebサービスAがアクセストークンを発行する。

問15　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。

ア，ウ：OP25Bはメール送信のブロックに利用されるため，ICMPによるDDoS攻撃は遮断できない。
エ：ISP管理外のネットワークから，ISP管理下のネットワーク内部に向けて送信されたスパムメールは，制限できない。

問16　ウ

解説 **サンドボックス**（砂場）は，機能制限されている領域内でプログラムを動作させるセキュリティ対策である。通常，サンドボックス内から，外部のファイルや他のプロセスへのアクセスは禁止されている。

ア：WAF（Web Application Firewall）についての説明である。
イ：遠隔操作の技術は複数あるが，サンドボックスではない。
エ：SQLインジェクション対策などに用いられるプレースホルダのことである。

問 17

正解 □ 完璧 □ 直前チェック □

利用者認証情報を管理するサーバ1台と複数のアクセスポイントで構成された無線LAN環境を実現したい。PCが無線LAN環境に接続するときの利用者認証とアクセス制御に，IEEE 802.1XとRADIUSを利用する場合の標準的な方法はどれか。

ア　PCにはIEEE 802.1Xのサプリカントを実装し，かつ，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，かつ，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，かつ，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，かつ，RADIUSサーバの機能をもたせる。

問 18

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コマンドを繰り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17　イ

解説 **RADIUS**（Remote Authentication Dial In User Service）は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である。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。無線LANだけでなく，優先LANでも利用できる。

IEEE802.1Xでは，認証のためのデータのやりとりを，PCとアクセスポイントで行う。また，アクセスポイントとRADIUSサーバの間ではRADIUSプロトコルによって中継する。

サプリカントとは，IEEE802.1X通信を可能とするためのPC用のソフトウェアである。

ア：PCでは認証自体を行わないため，RADIUSクライアントの機能をもたせない。
イ：正しい。アクセスポイントではRADIUSクライアントの機能をもたせ認証を行う。
ウ：アクセスポイントにはサプリカントを実装しない。
エ：オーセンティケータは，認証を中継するアクセスポイントにもたせる。

問18　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。ア，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 19 正解 完璧 直前チェック

PCやスイッチングハブがもつイーサネットインタフェース（物理ポート）の，Automatic MDI/MDI-Xの機能はどれか。

ア　コネクタの送信端子と受信端子が正しい組合せとなるように，自動で判別して切り替える機能
イ　接続した機器のアドレスを学習し，イーサネットフレームを該当するインタフェースにだけ転送する機能
ウ　通信経路のループを自動的に検出する機能
エ　通信速度や，全二重と半二重のデータ通信モードを自動的に設定する機能

問 20 正解 完璧 直前チェック

IEEE 802.11a/b/g/n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 21 正解 完璧 直前チェック

次のSQL文をA表の所有者が発行した場合を説明したものはどれか。

```
GRANT ALL PRIVILEGES ON A TO B WITH GRANT OPTION
```

ア　利用者Bに対して，A表に関するSELECT権限，UPDATE権限，INSERT権限，DELETE権限などの全ての権限，及びそれらの付与権を付与する。
イ　利用者Bに対して，A表に関するSELECT権限，UPDATE権限，INSERT権限，DELETE権限などの全ての権限を付与するが，それらの付与権は付与しない。
ウ　利用者Bに対して，A表に関するSELECT権限，UPDATE権限，INSERT権限，DELETE権限は付与しないが，それらの全ての付与権だけを付与する。
エ　利用者Bに対して，A表に関するSELECT権限，及びSELECT権限の付与権を付与するが，UPDATE権限，INSERT権限，DELETE権限，及びそれらの付与権は付与しない。

春
秋

問19　ア

解説　**Automatic MDI/MDI-X**とは，スイッチングハブや，ハブがもつ機能で，通信ポートがMDIかMDI-Xかを自動的に判別し接続する機能である。具体的は，PC（MDI）と，スイッチングハブ（MDI-X）を，LANケーブルで接続する場合は，LANケーブルの種類はストレートケーブルを使用する必要がある。このとき，クロスケーブルを使用しても，接続の間違いをスイッチングハブに実装されている，Automatic MDI/MDI-Xによって通信可能となる。
イ，ウ，エ：スイッチングハブの機能で実装されている内容である。

問20　ア

解説
CSMA方式：CSMA（Carrier Sense Multiple Access）は，搬送波感知多重アクセスを意味する。データの送信を開始する際，伝送路にほかの通信が行われていないかを確認してからデータ送信を行う。
CSMA/CD（CSMA/Collision Detection）：CDは衝突検出を意味する。データ送信中にほかの通信と衝突した場合はただちに通信を止め，時間をおいてから再度送信を開始する。
CSMA/CA（CSMA/Collision Avoidance）：CAは衝突回避を意味する。データ送信を開始する際に伝送路をほかの通信が使っている場合，その通信が終了してから少し時間をおいて，データの通信を開始する。
LAPB（Link Access Procedure Balanced）：平衡型リンクアクセス手順。X.25やISDNのBチャネル用データリンク層プロトコルである。パケット交換網などで利用される。
トークンパッシング方式：パケットを送信する際にトークンと呼ばれる送信権のデータがつながっている端末を巡回し，トークンが届いた場合のみ端末はデータを伝送できる。

問21　ア

解説　設問のSQL文のポイントは，GRANTとALL PRIVILEGESである。
GRANT：アクセス権限を与えるコマンド
ALL PRIVILEGES：全権限，全操作が可能
ON A TO B：A表に関してBに付与
WITH GRANT OPTION：オプション権限
したがって，A表に関する全ての権限とオプション権限を利用者Bに付与することとなるので，選択肢アが正しい。

問 22 正解 □ 完璧 □ 直前チェック □

システム及びソフトウェア品質モデルの規格であるJIS X 25010:2013で定義されたシステム及び/又はソフトウェア製品の品質特性に関する説明のうち，適切なものはどれか。

ア　機能適合性とは，明示された状況下で使用するとき，明示的ニーズ及び暗黙のニーズを満足させる機能を，製品又はシステムが提供する度合いのことである。
イ　信頼性とは，明記された状態（条件）で使用する資源の量に関係する性能の度合いのことである。
ウ　性能効率性とは，明示された利用状況において，有効性，効率性及び満足性をもって明示された目標を達成するために，明示された利用者が製品又はシステムを利用することができる度合いのことである。
エ　保守性とは，明示された時間帯で，明示された条件下に，システム，製品又は構成要素が明示された機能を実行する度合いのことである。

問 23 正解 □ 完璧 □ 直前チェック □

コンテンツの不正な複製を防止する方式の一つであるDTCP-IPの説明として，適切なものはどれか。

ア　BSデジタル放送や地上デジタル放送に採用され，コピーワンスの番組を録画するときに使われる方式
イ　DLNAとともに用いられ，接続する機器間で相互認証し，コンテンツ保護が行えると認識して初めて録画再生を可能にする方式
ウ　DVDに採用され，映像コンテンツを暗号化して，複製できないエリアにその暗号化鍵を記録する方式
エ　HDMI端子が搭載されたディジタルAV機器に採用され，HDMI端子から表示機器にディジタル信号を送るときに受信する経路を暗号化する方式

問22 ア

解説 JIS X 25010:2013は，定された特定の条件で利用する場合の，システムの品質，システムが様々な利害関係者の明示的ニーズ及び暗黙のニーズを満足している度合を表すための規格要求事項である。

機能適合性（functional suitability）：明示された状況下で使用するとき，明示的ニーズ及び暗黙のニーズを満足させる機能を，製品又はシステムが提供する度合い。
信頼性（reliability）：明示された時間帯で，明示された条件下に，システム，製品又は構成要素が明示された機能を実行する度合い。
性能効率性（performance efficiency）：明記された状態（条件）で使用する資源の量に関係する性能の度合い。
保守性（maintainability）：意図した保守者によって，製品又はシステムを修正することができる有効性及び効率性の度合い。
使用性（usability）：明示された利用状況において，有効性，効率性及び満足性をもって明示された目標を達成するために，明示された利用者が製品又はシステムを利用することができる度合い。

ア：正しい。機能適合性の説明である。
イ：性能効率性の説明である。
ウ：使用性の説明である。
エ：信頼性の説明である。

問23 イ

解説 **DTCP-IP**（Digital Transmission Content Protection over Internet Protocol）は，著作権保護されたディジタル映像を家庭内LANなどのIPネットワークで送信するためのプロトコルである。

DLNA（Digital Living Network Alliance）は，DVDレコーダといったAV家電や，パソコン，モバイル機器を各種メーカが販売する機器の相互接続性を確立するためのガイドラインとなる。

ア：**CPRM**（Content Protection for Recordable Media）の説明である。
ウ：**CPPM**（Content Protection for Prerecorded Media）の説明である。
エ：**HDCP**（High-bandwidth Digital Content Protection system）の説明である。

問 24 正解 完璧 直前チェック

データの追加・変更・削除が，少ないながらも一定の頻度で行われるデータベースがある。このデータベースのフルバックアップを磁気テープに取得する時間間隔を今までの2倍にした。このとき，データベースのバックアップ又は復旧に関する記述のうち，適切なものはどれか。

ア　フルバックアップ1回当たりの磁気テープ使用量が約2倍になる。
イ　フルバックアップ1回当たりの磁気テープ使用量が約半分になる。
ウ　フルバックアップ取得の平均処理時間が約2倍になる。
エ　ログ情報を用いて復旧するときの平均処理時間が約2倍になる。

問 25 正解 完璧 直前チェック

ある企業が，自社が提供するWebサービスの信頼性について，外部監査人による保証を受ける場合において，次の表のA～Dのうち，“ITに係る保証業務の三当事者”のそれぞれに該当する者の適切な組合せはどれか。

	ITに係る保証業務の三当事者		
	保証業務の実施者	Webサービスの信頼性に責任を負う者	保証報告書の想定利用者
A	Webサービス利用者	外部監査人	当該企業の経営者
B	外部監査人	Webサービス利用者	当該企業の経営者
C	外部監査人	当該企業の経営者	Webサービス利用者
D	当該企業の経営者	外部監査人	Webサービス利用者

ア　A　　イ　B　　ウ　C　　エ　D

問24　エ

解説　設問から，データの追加・削除が一定の頻度で行われた場合，フルバックアップの時間間隔を2倍にしてもデータの総量はあまり変化しない。そのため，フルバックアップ1回当たりの磁気テープ使用量も，約2倍や約半分にはならない。またフルバックアップの取得時間にも大きな差はない。

ジャーナル情報は，日々の処理データの蓄積であるため，データの追加・変更・削除の件数に応じて比例するため，フルバックアップ時間が間隔を2倍にすれば，ジャーナルのデータ量もほぼ2倍となる。したがって，ジャーナル情報からの復旧時間も平均して約2倍となる。

問25　ウ

解説　保証業務の当事者には，保証業務の実施者，責任を負う者，想定利用者が存在する。

保証業務の実施者：ITに関する専門的な知識，技能等を保持していなければならない。職業的専門家としての倫理の遵守など保証業務の実施の前提となる要件を満たす必要がある。外部監査員が該当する。

責任を負う者：本問の場合，Webサービスの信頼性に責任を負う者となっている。そのため企業の責任者が該当する。

想定利用者：本問の場合，Webサービスの利用者が該当する。保証業務の業務実施者，責任を負う者とは別の者となる。