問題

問 1

正解 完璧 直前CHECK

AESの暗号化方式を説明したものはどれか.

ア　鍵長によって，段数が決まる.
イ　段数は，6回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CHECK

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　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
イ　チャレンジレスポンスによる利用者認証
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

正解 完璧 直前CHECK

PC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1　ア

AES（Advanced Encryption Standard）は，米国政府標準の**共通鍵暗号方式**である．また，RSAは3名の発案者（R.Rivest，A.Shamir，L.Adleman）の頭文字から名づけられた**公開鍵暗号方式**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

IEEE 802.1xは，クライアントPCと，無線のアクセスポイントやスイッチングハブとの間での**鍵交換**（鍵更新を含む）や**認証**のためのプロトコルである．鍵交換により共有された鍵を用いてクライアントPCと接続先との暗号化通信を行う．IEEE 802.1Xでは認証方式として，EAP-TLSやEAP-PEAPなどが使用される．

EAP-TLS（Extensible Authentication Protocol - Transport Layer Security）：OSI第4層のトランスポート層に基づいてディジタル証明書による相互認証（サービス提供者の詐称をも防止する）を行う認証手順である．

問3　イ

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に内蔵される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内部のみでの利用できる．PCから取りはずすと，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．

問題

問 4

正解 完璧 直前CHECK

暗号アルゴリズムの危殆化を説明したものはどれか.

ア　外国の輸出規制によって十分な強度をもつ暗号アルゴリズムを実装した製品が利用できなくなること
イ　鍵の不適切な管理によって，鍵が漏えいする危険性が増すこと
ウ　計算能力の向上などによって，鍵の推定が可能となり，暗号の安全性が低下すること
エ　最高性能のコンピュータを用い，膨大な時間やコストを掛けて暗号強度をより確実なものとすること

問 5

正解 完璧 直前CHECK

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アドレスに対して，一定時間だけ電子メールの送信を許可する.
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 6

正解 完璧 直前CHECK

X.509におけるCRL（Certificate Revocation List）の運用を説明したものはどれか.

ア　PKIの利用者は，認証局の公開鍵がブラウザに組み込まれていれば，CRLを参照しなくてもよい.
イ　認証局は，X.509によって1年に1回のCRL発行が義務付けられている.
ウ　認証局は，ディジタル証明書を有効期限内にCRLに登録することがある.
エ　認証局は，発行したすべてのディジタル証明書の有効期限をCRLに登録する.

問4　ウ

暗号アルゴリズムの**危殆化**とは，暗号アルゴリズム自体がセキュリティ上危険となることであると，漢字から推測することができる．

アルゴリズム自体が危険な状態とは，容易に解読できてしまう状態であることが考えられる．PCの処理性能を考えても，数十年前の大型コンピュータと現在のPCの処理性能では，現在のPCのほうが高いこともあるため，解読性能の向上やアルゴリズムの解析等の危険が顕在化している状態が危殆化している状態であるといえる．

ア：暗号アルゴリズムが輸出規制となるかどうかは，「外国為替および外国貿易法（外為法）」によって定められている．法規制であるため，アルゴリズムそのものが危険となるわけではない．

イ：鍵管理は運用上の問題であるため，アルゴリズムが危険となる場合とは異なる．

エ：暗号強度をより確実なものとすることは危険度が減少することを意味する．したがって，危殆化とは逆の説明となる．

問5　イ

SMTP-AUTH認証は，クライアントがメールを送信する際のSMTPサーバへのアクセス時にユーザ認証を行い，認証されたクライアントのみに電子メールの送信を許可する認証方式である．

SMTP自体は標準で認証する仕様となっておらず，他の方式をあわせて利用制限を行っている．SMTPサーバではIPアドレスやドメイン名でアクセスを制限することが一般的であったが，スパムメールに利用されることなどを避けるために，SMTP-AUTHを利用して個人単位でメールを送信する機能が作られた．

ア：POP Before SMTPの認証の説明である．

ウ：SMTP over SSLの説明である．

エ：APOP（Authenticated Post Office Protocol）の説明である．

問6　ウ

CRL（Certificate Revocation List）は，有効期間中に失効した公開鍵証明書を記載したリストで，認証局から発行される．公開鍵証明書の検証時の公開鍵証明書失効確認に使用するため，常に参照される．

公開鍵証明書の有効期間中に秘密鍵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，公開鍵証明書のシリアル番号がCRLに記載される．

問題

問 7

正解 □ 完璧 □ 直前CHECK □

認証局が送信者に発行したディジタル証明書を使用して送信者又は受信者が行えることはどれか.

ア　受信した暗号文を復号して，盗聴を検知する.
イ　受信した暗号文を復号して，メッセージが改ざんされていないことと送信者が商取引相手として信頼できることを確認する.
ウ　受信したメッセージのディジタル署名を検証して，メッセージが改ざんされていないこととメッセージの送信者に偽りのないことを確認する.
エ　メッセージにディジタル署名を添付して，盗聴を防止する.

問 8

正解 □ 完璧 □ 直前CHECK □

サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち，適切なものはどれか.

	辞書攻撃	スニッフィング	ブルートフォース攻撃
ア	パスワードを平文で送信しない.	ログインの試行回数に制限を設ける.	ランダムな値でパスワードを設定する.
イ	ランダムな値でパスワードを設定する.	パスワードを平文で送信しない.	ログインの試行回数に制限を設ける.
ウ	ランダムな値でパスワードを設定する.	ログインの試行回数に制限を設ける.	パスワードを平文で送信しない.
エ	ログインの試行回数に制限を設ける.	ランダムな値でパスワードを設定する.	パスワードを平文で送信しない.

問7　ウ

ディジタル証明書を利用することで，本人が送信したことの証明や暗号化，メッセージが改ざんされていないことの証明を行うことができる．

本人が送信したことを証明することで，商品を注文した後に否認されることを防ぐことができる．

ア，エ：盗聴されること自体の検知や防止はできない．

イ：商取引としての信頼性は，ディジタル証明書とは関係ない．

問8　イ

辞書攻撃：辞書にある単語を利用してパスワードを不正に取得する方式．辞書に載らないようなランダムなパスワードをつけることで防ぐことが可能．

スニッフィング：パスワードを盗聴することで不正に取得する方式．パスワードを平文で送らず，暗号化することで防ぐことが可能．

ブルートフォース攻撃：総当り攻撃とも呼ばれる．パスワードとなりえる文字列をすべて試行してパスワードを不正に取得する方式．攻撃の回数が多くなるため，ログイン時の失敗回数でロックをかけるなどの制限で防ぐことが可能．

問題

問 9

正解 □ 完璧 □ 直前CHECK □

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，安全な場所に保管する原本と比較し，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 10

正解 □ 完璧 □ 直前CHECK □

ウイルスの調査手法に関する記述のうち，適切なものはどれか.

ア　逆アセンブルは，バイナリコードの新種ウイルスの動作を解明するのに有効な手法である.

イ　パターンマッチングでウイルスを検知する方式は，暗号化された文書中のマクロウイルスの動作を解明するのに有効な手法である.

ウ　ファイルのハッシュ値を基にウイルスを検知する方式は，ウイルスのハッシュ値からどのウイルスの亜種かを特定するのに確実な手法である.

エ　不正な動作からウイルスを検知する方式は，ウイルス名を特定するのに確実な手法である.

問9　エ

ビヘイビア法は，ウイルスの感染や発病による異常な振る舞い（システム領域の書込み動作や，通信量の増加等）を監視し，ウイルスを検出する手法である．

ビヘイビア法の特徴としては，システム上の異常な振る舞いを監視しているため，既存のウイルスの亜種や未知のウイルスであっても検出できることがある．

ア：パターンマッチング法の説明である．
イ：チェックサム法の説明である．
ウ：コンペア法の説明である．

問10　ア

ア：バイナリを逆アセンブルすることでウイルスの動作を解析する手がかりとなる．
イ：暗号化されたデータはウイルス自体も暗号化されているため，復号されるまでウイルスであるとは判断できない．
ウ：ハッシュ値を用いて一意なウイルスを特定することはできるが，ウイルスの亜種になるとハッシュ値が変わるため，特定することはできない．
エ：不正な動作を識別してもウイルス名は特定できない．例として，メールの添付ファイルを開くとウイルスメールを送信するウイルスには複数の種類が存在するため，その動作のみでは特定できない．

問題

問 11

正解 □ 完璧 □ 直前CHECK □

通信の暗号化に関する記述のうち，適切なものはどれか．

ア　IPsecのトランスポートモードでは，ゲートウェイ間の通信経路上だけではなく，送信ホストと受信ホストとの間の全経路上でメッセージが暗号化される．

イ　LDAPクライアントがLDAPサーバに接続するとき，その通信内容は暗号化することができない．

ウ　S/MIMEで暗号化した電子メールは，受信側のメールサーバ内に格納されている間は，メール管理者が平文として見ることができる．

エ　SSLを使用すると，暗号化されたHTML文書はブラウザでキャッシュの有無が設定できず，ディスク内に必ず保存される．

問 12

正解 □ 完璧 □ 直前CHECK □

自社の中継用メールサーバのログのうち，外部ネットワークからの第三者中継と判断できるものはどれか．ここで，AAA.168.1.5とAAA.168.1.10は自社のグローバルIPアドレスとし，BBB.45.67.89とBBB.45.67.90は社外のグローバルIPアドレスとする．a.b.cは自社のドメイン名とし，a.b.dとa.b.eは他社のドメイン名とする．また，IPアドレスとドメイン名は詐称されていないものとする．

	接続元IPアドレス	送信者のドメイン名	受信者のドメイン名
ア	AAA.168.1.5	a.b.c	a.b.d
イ	AAA.168.1.10	a.b.c	a.b.c
ウ	BBB.45.67.89	a.b.d	a.b.e
エ	BBB.45.67.90	a.b.d	a.b.c

問11 ア

ア： IPSecのトランスポートモードではEnd-to-Endでメッセージを暗号通信するため，ゲートウェイ間の通信経路上だけでなく発信側システムと受信側システムとの間の全経路上でメッセージが暗号化されている．

イ：LDAPでは，TLSやSSLを用いた暗号通信について標準化されている．

ウ：S/MIMEでは送信者が電子メールのメッセージを暗号化し，受信者がメッセージを復号するため，メールサーバ内に格納されている間もメッセージが暗号化されている．

エ：SSLを使用した場合においては，ブラウザでキャッシュの有無が設定できないことや，暗号化されたHTMLデータがディスク内に必ず保存されることについて，何も規定していない．

問12 ウ

第三者中継とは，自社と関係ない利用者からメールサーバを利用されることである．主にスパムメールの発信に利用されていることである．第三者中継による不正利用を防ぐには，自社のドメインやIPアドレスで利用制限を行うことである．

設問の表では，送信元が他社，送信者が他社，受信者が他社となっているものは，自社に関係なく利用されていると判断できる．

問 13

正解 □ 完璧 □ 直前CHECK □

経済産業省“ソフトウェア管理ガイドライン”に定められた，ソフトウェアを使用する法人，団体などが実施すべき基本的事項の記述のうち，適切なものはどれか．

ア　ウイルスからソフトウェアを保護するため，関係法令や使用許諾契約などについて利用者の教育啓発を行う．

イ　セキュリティ対策に責任を負うセキュリティ管理責任者を任命し，適切な管理体制を整備する．

ウ　ソフトウェアの違法複製などの有無を確認するため，すべてのソフトウェアを対象として，その使用状況についての監査を実施する．

エ　ソフトウェアの脆弱(ぜい)性を突いた不正アクセスから保護するため，ソフトウェアの使用手順や管理方法などを定めたソフトウェア管理規則を制定する．

問 14

正解 □ 完璧 □ 直前CHECK □

共通フレーム2007に従いシステム開発の要件定義の段階で実施することとして，適切なものはどれか．

ア　システムに必要なセキュリティ機能及びその機能が対策として達成すべき内容を決定する．

イ　システムに必要なセキュリティ機能に関連するチェックリストを用いてソースコードをレビューする．

ウ　組織に必要なセキュリティ機能を含むシステム化計画を立案する．

エ　第三者によるシステムのセキュリティ監査を脆弱(ぜい)性評価ツールを用いて定期的に実施する．

問13　ウ

ソフトウェア管理ガイドラインには以下のように書かれている．

4．法人等が実施すべき基本的事項
(1) ソフトウェアの使用等を的確に管理し，ソフトウェアの違法複製等の行為を効果的に防止するため，法人等におけるソフトウェアの使用等について責任を負うソフトウェア管理責任者を任命し，ソフトウェアの適切な管理体制を整備すること．
(2) ソフトウェアの適正な使用等を確立するため，ソフトウェアの使用手順や管理方法等を定めたソフトウェア管理規則を策定すること．
(3) ソフトウェアの違法複製等の有無を確認するため，すべてのソフトウェアを対象として，ソフトウェアの使用状況についての監査（以下「ソフトウェア監査」という．）を実施すること．
(4) ソフトウェアの適正な使用等に対するソフトウェアユーザ意識の向上を図るため，関係法令や使用許諾契約等について，ソフトウェアユーザの教育，啓蒙を行うこと．

ア，イ，エは基本的事項に近い内容が書かれているが誤っている．

問14　ア

共通フレーム2007（SLCP-JCF 2007/Software life cycle process － Japan common frame）は，システム開発においてユーザ（発注側）とベンダ（受注側）の双方に共通して利用する用語や作業内容を標準化するためのガイドラインである．**プロセス**とは，システム開発作業を役割の観点でまとめたものである．
ア：要件定義プロセスで行う作業である．
イ：開発プロセスで行う作業である．
ウ：企画プロセスで行う作業である．
エ：監査プロセスで行う作業である．

問 15

正解 完璧 直前CHECK

ICカードの耐タンパ性を高める対策はどれか.

ア　ICカードとICカードリーダとが非接触の状態で利用者を認証して，利用者の利便性を高めるようにする.

イ　故障に備えてあらかじめ作成した予備のICカードを保管し，故障時に直ちに予備カードに交換して利用者がICカードを使い続けられるようにする.

ウ　信号の読出し用プローブの取付けを検出するとICチップ内の保存情報を消去する回路を設けて，ICチップ内の情報を容易に解析できないようにする.

エ　退職者のICカードは業務システム側で利用を停止して，ほかの利用者が使用できないようにする.

問 16

正解 完璧 直前CHECK

ルータで接続された二つのセグメント間でのコリジョンの伝搬とブロードキャストフレームの中継について，適切な組合せはどれか.

	コリジョンの伝搬	ブロードキャストフレームの中継
ア	伝搬する	中継する
イ	伝搬する	中継しない
ウ	伝搬しない	中継する
エ	伝搬しない	中継しない

問 17

正解 完璧 直前CHECK

ある企業の本店で内線通話を調査したところ，通話数が1時間当たり120回，平均通話時間が90秒であった．本店内線の呼量は何アーランか.

ア　0.03　　イ　3　　ウ　180　　エ　10,800

問15　ウ

耐タンパ性とは，内部情報の読み取りに対する物理的あるいは論理的な耐性のことである．設問から，ICカードの物理的・論理的な防御策を選択すればよい．

ア：利便性を高めることは，耐タンパ性を高めることにはならない．

イ：故障時の予備交換は保守性を高めることである．

エ：セキュリティを向上の説明である．

問16　エ

ルータで接続された二つのセグメント間の通信は，OSI参照モデルで考える必要がある．

コリジョンおよびブロードキャストフレームは，いずれも第2層のデータリンク層で中継される．そのため，第3層のルータでは伝搬されない．

注意しなければならないのは，ブロードキャストフレームは第2層だが，ブロードキャストパケットとなると第3層になる．呼び方に注目する必要がある．

OSI基本参照モデル	PDU	機器
第7層　アプリケーション層	メッセージ	ゲートウェイ等
第6層　プレゼンテーション層		
第5層　セション層		
第4層　トランスポート層	セグメント	
第3層　ネットワーク層	パケット	ルータ，L3スイッチ
第2層　データリンク層	フレーム	ブリッジ，L2スイッチ
第1層　物理層	ビット	リピータ，ハブ

コリジョン：フレームの衝突を通知すること．

ブロードキャストフレーム：第2層で接続されている機器全体へ送付するフレーム．

問17　イ

アーランは，通信回線の単位である．1回線を1時間，継続的に占有して利用するときの呼量を指す．アーランは1時間当たりの単位であるため，3,600で割る必要がある．

（120回×90秒）÷ 3,600秒 = 3〔アーラン〕

問題

問 18

正解 完璧 直前CHECK

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

問 19

正解 完璧 直前CHECK

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　ウィンドウ制御はビット単位で行う．
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

正解 完璧 直前CHECK

通信プロトコルで使用するデータ形式を記述するための記法であって，SNMPのパケットの符号化に利用されているものはどれか．

ア　ASN.1　　イ　JSON　　ウ　SGML　　エ　SOAP

問18　ア

IPSecは，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，プライバシー関わる情報やクレジットカード番号，企業秘密などを安全に送受信することができる．

問19　ウ

フロー制御とは，受信側の端末でパケットを受け取りきれなくなる場合に，送信を一時的に停止または送出速度を落とすことを送信側に要請し，受信量を調整する仕組みである．ウィンドウサイズが大きくなると，受信確認をせずに多くのパケットを送信できるため，パフォーマンスが良くなる．

ア：TCPはトランスポート層（4層）の機能である．

イ：ウィンドウ制御はセグメント単位で行う．

エ：シーケンス番号という順序番号を持ち順序制御がある．

問20　ア

SNMP（Simple Network Management Protocol）は，RFC 1157で定義されているネットワーク管理プロトコルである．管理対象機器に常駐するエージェントと，エージェントから情報を受け取るマネージャで構成される．

ASN.1（Abstract Syntax Notation One）：データ構造を定義する言語．SNMPやS/MIME，SSLなどのプロトコルに用いられている．

JSON（JavaScript Object Notation）：RFC 4627で公開されているテキスト形式のデータ交換用フォーマット．JavaScritpで利用される．

SGML：(Standard Generalized Markup Language)：文書の論理構造や意味構造を記述するマークアップ言語．HTMLは SGMLの一種である．

SOAP（Simple Object Access Protocol）：SOAPによる通信では，XML文書にエンベロープと呼ばれる付帯情報がついたメッセージをHTTPなどでやり取りする．

問題

問 21

正解 □ 完璧 □ 直前CHECK □

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　A表に関する，SELECT権限，UPDATE権限，INSERT権限，DELETE権限などのすべての権限，及びそれらの付与権限を利用者Bに対して付与する.

イ　A表に関する，SELECT権限，UPDATE権限，INSERT権限，DELETE権限などのすべての権限を利用者Bに対して付与するが，それらの権限の付与権限は付与しない.

ウ　A表に関する，SELECT権限，UPDATE権限，INSERT権限，DELETE権限は与えないが，それらのすべての権限の付与権限だけを利用者Bに対して付与する.

エ　A表に関する，SELECT権限，及びSELECT権限の付与権限を利用者Bに対して付与し，UPDATE権限，INSERT権限，DELETE権限，及びそれらの付与権限は付与しない.

問 22

正解 □ 完璧 □ 直前CHECK □

操作に不慣れな人も利用するシステムでは，間違ったデータが入力されることが想定される．誤入力が発生しても，プログラムやシステムを異常終了させずに，エラーメッセージを表示して次の操作を促すような設計を何というか.

ア　フールプルーフ　　イ　フェールセーフ

ウ　フェールソフト　　エ　フォールトトレランス

問 23

正解 □ 完璧 □ 直前CHECK □

共通フレーム2007で取り決められているものはどれか.

ア　作成する文書の種類及び書式

イ　信頼性，保守性などのソフトウェアの品質尺度

ウ　適用すべき開発モデル，技法及びツール

エ　プロセスごとの作業の主体者（役割）と責任の所在

問21　ア

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表に関するすべ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　ア

フールプルーフ：ユーザの誤操作や予想できない操作によって障害が起きないようにあらかじめ対策をとることである．

フェールセーフ：故障や誤動作が発生した場合，暴走しないように安全な方向に動作あるいは停止させる技術である．例えば，信号が故障したら赤になるようなシステムである．

フェールソフト：システムの一部が故障しても，システムが停止せずに一部の機能だけで縮退し継続維持していく技術である．

フォールトトレランス：耐故障技術．故障が発生してもシステムに影響しないようにする技術である．

問23　エ

共通フレーム2007は，ソフトウェアを中心としたシステム開発，システム，サービスに関する共通フレーム，つまり供給者と取得者との間で共通に定める取引の枠，物差しのことである．

共通フレーム2007ではプロセスを細分化し，アクティビティ，タスク，リスト，作業項目と役割を定義している．各プロセスで定義されているものは，役割と責任である．

詳細なフォーマットや品質尺度，ツール等は定義されていない．

問題

問 24

正解 完璧 直前CHECK

(1)～(4)はある障害の発生から本格的な対応までの一連の活動である．(1)～(4)の各活動とそれに対応するITILの管理プロセスの組合せのうち，適切なものはどれか．

(1) 利用者からサービスデスクに“特定の入力操作が拒否される”という連絡があったので，別の入力操作による回避方法を利用者に伝えた．
(2) 原因を開発チームで追究した結果，アプリケーションプログラムに不具合があることが分かった．
(3) 障害の原因となったアプリケーションプログラムの不具合を改修する必要があるのかどうか，改修した場合に不具合箇所以外に影響が出る心配はないかどうかについて，関係者を集めて確認し，改修することを決定した．
(4) 改修したアプリケーションプログラムの稼働環境への適用については，利用者への周知，適用手順及び失敗時の切戻し手順の確認など，十分に事前準備を行った．

	(1)	(2)	(3)	(4)
ア	インシデント管理	問題管理	変更管理	リリース管理及び展開管理
イ	インシデント管理	問題管理	リリース管理及び展開管理	変更管理
ウ	問題管理	インシデント管理	変更管理	リリース管理及び展開管理
エ	問題管理	インシデント管理	リリース管理及び展開管理	変更管理

問 25

正解 完璧 直前CHECK

入出金管理システムから出力された入金データファイルを，売掛金管理システムが読み込んでマスタファイルを更新する．入出金管理システムから売掛金管理システムへのデータ受渡しの正確性及び網羅性を確保するコントロールはどれか．

ア　売掛金管理システムにおける入力データと出力結果とのランツーランコントロール
イ　売掛金管理システムのマスタファイル更新におけるタイムスタンプ機能
ウ　入金額及び入金データ件数のコントロールトータルのチェック
エ　入出金管理システムへの入力のエディットバリデーションチェック

問24　ア

ITIL（IT Infrastructure Library）は，システム管理・運用規則に関するガイドラインである．設問の中で展開管理が示されていることから，ITIL v3の設問であるといえる．

インシデント管理：日常的なハードウェア障害やソフトウェア不良による障害から，業務処理が正常にできるまでに復旧させる．

問題管理：未知の問題が発生したときに，その問題を回避するための解析と解決方法を示す．

変更管理：変更を実施することで発生するリスク確認や変更作業そのものを行ってよいかの承認を行う．

リリース管理および**展開管理**：変更管理で承認された変更要求に対する実装を行う．

問25　ウ

入金額と入金データ件数をチェックすることで，データが欠けたり誤っていないことが検証できる．

ア，エ：データの正確性はチェックできるが，受け渡しが正確に行われたかをチェックすることはできない．

イ：マスタファイル更新のタイムスタンプだけでは，データ受渡しがすべて行われたか，正しく行われたかを確認できない．