

問 1 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 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 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 デジタル証明書の発行
- エ ネットワーク経由の乱数送信

問 4 暗号アルゴリズムの危殆^{たい}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

問 5 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ジタル証明書を持ち、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 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ジタル証明書の有効期限を CRL に登録する。

問 7 認証局が送信者に発行したデ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 メッセージにデジタル署名を添付して、盗聴を防止する。

問 8 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ффイング	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 9 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 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 11 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 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 13 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 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性評価ツールを用いて定期的実施する。

問 15 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 カードリーダーとが非接触の状態を利用者を認証して、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 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 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 18 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 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処理する。

問 20 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 21 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 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 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 24 (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 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ク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

午前Ⅱ試験

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

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

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