問題

問 1

正解 完璧 直前CHECK

チャレンジレスポンス方式として，適切なものはどれか．

ア　SSLによって，クライアント側で固定パスワードを暗号化して送信する．
イ　トークンという装置が表示する毎回異なったデータをパスワードとして送信する．
ウ　任意長のデータを入力として固定長のハッシュ値を出力する．
エ　利用者が入力したパスワードと，サーバから送られたランダムなデータとをクライアント側で演算し，その結果を認証用データに用いる．

問 2

正解 完璧 直前CHECK

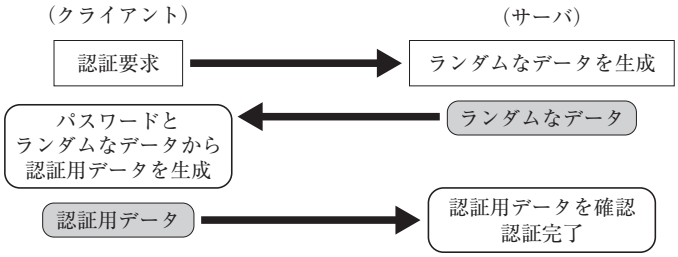
ブラウザがWebサーバとの間でSSLで通信する際，ディジタル証明書に関する警告メッセージが表示される原因となり得るものはどれか．

ア　Webサーバが，SSL通信の暗号化方式として，ハンドシェイク終了後に共通鍵暗号化方式でSSLセッションを開始した．
イ　ブラウザがCRLの妥当性をVAに問い合わせる際に，OCSPやSCVPが用いられた．
ウ　ブラウザがWebサーバのディジタル証明書の検証に成功した後に，WebサーバからSSLセッションを確立した．
エ　ルートCAのディジタル証明書について，Webサーバのディジタル証明書のものがブラウザで保持しているどのものとも一致しなかった．

問1　エ

ア：SSLで保護した**ベーシック認証**の説明である．
イ：**ワンタイムパスワード**の説明である．
ウ：**ハッシュ関数**の説明である．
エ：**チャレンジレスポンス方式**の説明である．

チャレンジレスポンスの図：



問2　エ

ブラウザにはSSL通信に用いる**ルートCA証明書**が登録されている．このルートCA証明書は，信頼できるルートCAから発行されたものとして登録されている．そのため，SSL通信のサーバ証明書検証時に，検証に用いるルートCA証明書が登録されていない場合，ユーザに対してそのサーバ証明書を受け入れるかどうかの警告が表示される．

問3

正解 完璧 直前CHECK

SMTP-AUTH認証はどれか.

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CAの公開鍵証明書をもち，クライアントから送信されたCAの署名付きクライアント証明書の妥当性を確認する.

エ　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4

正解 完璧 直前CHECK

コンティンジェンシープランにおける留意点はどれか.

ア　企業のすべてのシステムを対象とするのではなく，システムの復旧の重要性と緊急性を勘案して対象を決定する.

イ　災害などへの対応のために，すぐに使用できるよう，バックアップデータをコンピュータ室内又はセンタ内に保存しておく.

ウ　バックアップの対象は，機密情報の中から秘密度を勘案して選択する.

エ　被害状況のシナリオを作成し，これに基づく“予防策策定手順”と“バックアップ対策とその手順”を策定する.

問5

正解 完璧 直前CHECK

企業のDMZ上で1台のDNSサーバをインターネット公開用と社内用で共用している．このDNSサーバが，DNSキャッシュポイズニングの被害を受けた結果，引き起こされ得る現象はどれか.

ア　DNSサーバで設定された自社の公開WebサーバのFQDN情報が書き換えられ，外部からの参照者が，本来とは異なるWebサーバに誘導される.

イ　DNSサーバのメモリ上にワームが常駐し，DNS参照元に対して不正プログラムを送り込む.

ウ　社内の利用者が，インターネット上の特定のWebサーバを参照する場合に，本来とは異なるWebサーバに誘導される.

エ　電子メールの不正中継対策をした自社のメールサーバが，不正中継の踏み台にされる.

問3　イ

SMTP-AUTH認証は，クライアントがメールを送信する際，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電子メール送信を許可する認証方式である．

ウ：SMTPにおける**SSLクライアント認証**の説明である．

エ：**APOP**の説明である．

問4　ア

ア：**コンティンジェンシープラン**（緊急時対応計画，非常事態対応計画）では，企業内の全システムを考える必要はない．重要度（緊急事態発生時予想損害額）および対応コストを考慮して対策対策を選択し，有効性の高い対策を検討する．

イ：リスク分散の観点から，バックアップはコンピュータ室やセンタと別の場所に保管することが望ましい．

ウ：**重要情報**（消失したら困る情報）と**機密情報**（漏れらたら困る情報）は，必ずしも一致しない．

エ：予防策策定手順，バックアップ対策手順の立案は，緊急事態発生前の平常時運用手順である．コンティンジェンシープランではない．

問5　ウ

DNSキャッシュポイズニングは，DNSサーバに偽ドメイン情報をキャッシュさせる攻撃手法である．DNSサーバに偽ドメイン情報がキャッシュされてしまうと，DNSサーバはクライアントに偽ドメインのアドレスを返してしまい，クライアントは偽装されたWebサーバに誘導されてしまう．

ア：**FQDN情報**とは，完全修飾ドメイン名（Fully Qualified Domain Name）と呼ばれる．これはDNSサーバにIPアドレスを問い合わせる際に問合せ側が使用する．したがってこれが書き換えられると，自社の公開サーバにアクセスできなくなる可能性がある．

エ：**踏み台攻撃**と呼ばれる手法である．

問題

問 6

正解 □ 完璧 □ 直前CHECK □

NIDS（ネットワーク型IDS）を導入する目的はどれか．

ア　管理下のネットワーク内への不正侵入の試みを検知し，管理者に通知する．
イ　サーバ上のファイルが改ざんされたかどうかを判定する．
ウ　実際にネットワークを介してサイトを攻撃し，不正に侵入できるかどうかを検査する．
エ　ネットワークからの攻撃が防御できないときの損害の大きさを判定する．

問 7

正解 □ 完璧 □ 直前CHECK □

クロスサイトスクリプティングによる攻撃へのセキュリティ対策に該当するものはどれか．

ア　OSのセキュリティパッチを適用することによって，Webサーバへの侵入を防止する．
イ　Webアプリケーションがクライアントに入力データを表示する場合，データ内の特殊文字を無効にする処理を行う．
ウ　WebサーバにSNMPエージェントを常駐稼働させることによって，攻撃を検知する．
エ　許容範囲を超えた大きさのデータの書込みを禁止し，Webサーバへの侵入を防止する．

問 8

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付加しておき，検査対象の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6　ア

NIDS（ネットワーク型IDS：Intrusion Detection System）は，保護する機器へのネットワーク経路上に設置して，ネットワーク上流れる通信内容で不正アクセス等の可能性があると判断されたものをネットワーク管理者に通知するシステムである．

イ：**ホスト型IDS**の説明である．

ウ：**ペネトレーションテスト**の説明である．

エ：**リスク分析**の説明である．

問7　イ

クロスサイトスクリプティングは，動的にWebページを生成するアプリケーションの脆弱性を利用した攻撃である．例えば，攻撃者によって掲示板に悪意のスクリプトコードが書きこまれた場合に，スクリプトコードをチェックせずに掲示板に載せることで，その掲示版にアクセスしたブラウザが悪意のスクリプトを実行させられてしまう．

対策としては，入力されたデータをチェックして，スクリプトの文字列を置き換えて無効化する**サニタイジング**が有効である．

問8　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（システム領域へ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．

問題

問 9

正解 完璧 直前CHECK

コンピュータフォレンジクスの説明として，適切なものはどれか．

ア　あらかじめ設定した運用基準に従って，メールサーバを通過する送受信メールをフィルタリングすること
イ　磁気ディスクなどの書換え可能な記憶媒体を単に初期化するだけではデータを復元される可能性があるので，覆い隠すように上書きすること
ウ　不正アクセスなどコンピュータに関する犯罪の法的な証拠性を確保できるように，原因究明に必要な情報を保全，収集して分析すること
エ　ホストに対する外部からの攻撃や不正なアクセスを防御すること

問 10

正解 完璧 直前CHECK

ステガノグラフィの機能はどれか．

ア　画像データなどにメッセージを埋め込み，メッセージの存在そのものを隠す．
イ　メッセージの改ざんやなりすましを検出し，否認の防止を行う．
ウ　メッセージの認証を行って改ざんの有無を検出する．
エ　メッセージを決まった手順で変換し，通信途中での盗聴を防ぐ．

問 11

正解 完璧 直前CHECK

パケットフィルタリング型ファイアウォールのフィルタリングルールを用いて，本来必要なサービスに影響を及ぼすことなく防げるものはどれか．

ア　外部に公開していないサービスへのアクセス
イ　サーバで動作するソフトウェアのセキュリティの脆弱(ぜいじゃく)性を突く攻撃
ウ　電子メールに添付されたファイルのマクロウイルスの侵入
エ　電子メール爆弾などのDoS攻撃

問9　ウ

コンピュータフォレンジクスとは，コンピュータ犯罪に対する科学的調査のことである．コンピュータの状態や記録の証拠性を確保し，法的問題を解決するための手法である．

たとえばシステムのファイルやログの収集・分析，ハードディスクの解析・復旧・復元などを行うとき，データの証拠性が失われないように，改ざん防止や改ざん検出の手段が講じられていることが必要である．このような，コンピュータ犯罪の調査・分析して証拠を検出するための取り組みのことである．

問10　ア

ステガノグラフィとは**電子透かし**のことを意味する．透かしで代表されるものは紙幣であるが，この紙の透かしの仕組みを画像に応用したものがステガノグラフィである．著作権の保護，不正コピー防止に役立つ技術である．

ステガノグラフィは，映像，画像，映像等のデータに見た目にはわからないように符号や文字列等を埋め込み，専用の閲覧ソフトによって埋め込んだ符号や文字列等を確認する．埋め込んだ符号や文字列等によりそのデータが不正にコピーされたり流通していたかどうかを知ることができる．

問11　ア

イ，ウ：**パケットフィルタリング**ではIPパケット内のデータをチェックしないため，ソフトウェアの脆弱性を突く攻撃を防止できない．同様に，電子メールに添付されたファイルをチェックしないため，**マクロウィルス**の侵入を許してしまう．

エ：電子メールによる**DoS攻撃**は，送信元のメールサーバからのパケットを通さないことで対応可能であるが，送信元から送られてくる正規のメールまで受け取れなくなってしまう．そのため，本来必要なサービスに影響を及ぼしてしまう．

問題

問 12

正解 完璧 直前CHECK

ブルートフォース攻撃に該当するものはどれか.

ア　可能性のある文字のあらゆる組合せのパスワードでログインを試みる.
イ　コンピュータへのキー入力をすべて記憶して外部に送信する.
ウ　盗聴者が正当な利用者のログインシーケンスをそのまま記録してサーバに送信する.
エ　認証が終了し，セッションを開始しているブラウザとWebサーバの間の通信で，クッキーなどのセッション情報を盗む.

問 13

正解 完璧 直前CHECK

レイヤ2スイッチや無線LANアクセスポイントで接続を許可する仕組みはどれか.

ア　DHCP　　イ　Webシングルサインオン
ウ　認証VLAN　　エ　パーソナルファイアウォール

問 14

正解 完璧 直前CHECK

SQLインジェクション対策について，Webアプリケーションの実装における対策とWebアプリケーションの実装以外の対策の組合せとして，適切なものはどれか.

	Webアプリケーションの実装における対策	Webアプリケーションの実装以外の対策
ア	Webアプリケーション中でシェルを起動しない.	chroot環境でWebサーバを実行する.
イ	セッションIDを複雑なものにする.	SSLによって通信内容を秘匿する.
ウ	バインド機構を利用する.	データベースのアカウントのもつデータベースアクセス権限を必要最小限にする.
エ	パス名やファイル名をパラメタとして受け取らないようにする.	重要なファイルを公開領域に置かない.

問12　ア

ブルートフォース攻撃とは，あらゆる文字列を組み合わせたパスワードを用いて総当たりでログインを試みる手法である．効率の悪い攻撃手法であるが，時間をかけることでパスワードを見つけることができる．ブルートフォース攻撃の対策としては，一定回数ログインに失敗するとアカウントをロックすることが有効である．

イ：**キーロガー**に関する説明である．

ウ：**リプレイ攻撃**に関する説明である．

エ：**セッションハイジャック**に関する説明である．

問13　ウ

認証VLAN：LANに接続する際に機器（レイヤ2スイッチや無線LANアクセスポイント）が認証サーバを用いてPCのユーザを認証し，そのユーザに対応するVLANにPCを接続する．

DHCP（Dynamic Host Configuration Protocol）：IPアドレスやサブネットマスクなど，TCP/IP接続に必要な設定を動的に行うプロトコル．

Webシングルサインオン：ユーザが認証サーバで一度認証操作を行えば，許可されたWebサーバで再度認証操作せずに接続可能となる．

パーソナルファイアウォール：機器のネットワーク接続の通信を制御するアプリケーションであり，PCへの不正アクセスを防止する個人向けのファイアウォールである．

問14　ウ

SQLインジェクションは，アプリケーションの想定しないSQL文を実行することでデータベースシステムを不正に操作し，データの取得や書き換え等を可能とする脆弱性のことである．対策としては，**バインド機構**や**エスケープ処理**を用いる．

バインド機構はSQL文のひな型を用意し，後から可変値の部分に入力値を割り当ててSQL文を生成する．

エスケープ処理は，特殊な意味を持つ文字列をチェックして特殊文字を置き換える．

また，データベースのアカウントのもつアクセス権を必要最小限にして，最低限な機能のみ実行可能としておくことも必要である．

問題

問 15

正解 完璧 直前CHECK

SLCP（共通フレーム）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達成すべき保証の程度を決定する．
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に実施する．

問 16

正解 完璧 直前CHECK

ネットワークのQoSで使用されるトラフィック制御方式に関する説明のうち，適切なものはどれか．

ア　通信を開始する前にネットワークに対して帯域などのリソースを要求し，確保の状況に応じて通信を制御することを，アドミッション制御という．
イ　入力されたトラフィックが規定された最大速度を超過しないか監視し，超過分のパケットを破棄するか優先度を下げる制御を，シェーピングという．
ウ　パケットの送出間隔を調整することによって，規定された最大速度を超過しないようにトラフィックを平準化する制御を，ポリシングという．
エ　フレームの種類やあて先に応じて優先度を変えて中継することを，ベストエフォートという．

問 17

正解 完璧 直前CHECK

電源オフ時にIPアドレスを保持することができない装置が，電源オン時に自装置のMACアドレスから自装置に割り当てられているIPアドレスを知るために用いるデータリンク層のプロトコルで，ブロードキャストを利用するものはどれか．

ア　ARP　　イ　DHCP　　ウ　DNS　　エ　RARP

問15　ア

SLCP（Software Life Cycle Processes）は，ソフトウェア開発に関する作業を明確に定義したものである．ソフトウェアの開発者と購入者の取引のための国際規格適合フレームワークとして，システム開発での作業工程を「プロセス」「アクティビティ」「タスク」などに分割して明確に定義し，開発者と購入者の取引の明確化・円滑化をはかる．

ソフトウェアの開発では，要件定義，システム設計，プログラミング，テスト，ソフトウェア受入れ，ソフトウェア保守のプロセスがある．要件定義では，ソフトウェアに求められる機能や性能等が明確に定義される．

ア：ソフトウェアの機能や性能を明確にしているので，正しい．

問16　ア

アドミッション制御は，**QoS保証**の枠組み（IntServ/RSVP，DiffServ）に基づいて，通信を開始する前にネットワークに対してリソース確保要求を行い，リソースの確保状況に応じて通信を制御する．例としては，音声通話や映像配信などの遅延が問題となるアプリケーションや，緊急通話のような高負荷状況のネットワークでも通話可能であるアプリケーションに用いる．

イ：**ポリシング**の説明である．

ウ：**シェーピング**の説明である．

エ：**ベストエフォート**とは，状況等によってネットワークのパフォーマンスは上下するが，それぞれの状況に応じて最善の努力を行い，サービスを提供することを意味する．

問17　エ

ARP（Address Resolution Protocol）：IPアドレスからMACアドレスを取得するプロトコル．

DHCP（Dynamic Host Configuration Protocol）：IPアドレスやサブネットマスクなど，TCP/IP接続に必要な設定を動的に行うプロトコル．

DNS（Domain Name System）：機器名とIPアドレスの変換を相互に行うシステム．

RARP（Reverse Address Resolution Protocol）：MACアドレスからIPアドレスを取得するプロトコル．

問題

問 18

正解 完璧 直前CHECK

ネットワークに接続されているホストのIPアドレスが212.62.31.90で，サブネットマスクが255.255.255.224のとき，ホストアドレスはどれか.

ア 10　　イ 26　　ウ 90　　エ 212

問 19

正解 完璧 直前CHECK

イーサネットのレイヤ2で使用されるプロトコルで，ネットワークを冗長化させる際にループの発生を防ぐものはどれか.

ア IGMP　　イ RIP
ウ SIP　　エ スパニングツリープロトコル

問 20

正解 完璧 直前CHECK

暗号化や認証機能をもち，リモートからの遠隔操作の機能をもったプロトコルはどれか.

ア IPsec　　イ L2TP　　ウ RADIUS　　エ SSH

問18　イ

サブネットマスクから，ホストアドレスを求める．問題文からサブネットマスクとホストのIPアドレスを2進数表記すると，下の表のようになる．

サブネットマスク	255.	255.	255.	224
（2進数表記）	11111111.	11111111.	11111111.	11100000
ホストのIPアドレス	212.	62.	31.	90
（2進数表記）	11010100.	00111110.	00001111.	01011010

サブネットマスクの2進数表記では，下位5ビットが0となっている．ホストアドレスはこの下位5ビットで示されるところであるため，これをホストのIPアドレスの2進数表記から読み取ると，11010となる．これを10進数に変換すると，11010＝26となる．

問19　エ

IGMP（Internet Group Management Protocol）：IPマルチキャストの機能を持つルータ間でグループ管理の情報を交換するためのプロトコル．

RIP（Routing Information Protocol）：ルータ間で経路情報を交換するためのプロトコル．

SIP（Session Initiation Protocol）：VoIPを用いたIP電話等で用いられる，機器間でセッションを確立するためのプロトコル．

スパニングツリープロトコル：LANにおいてループ状の構成がある場合，データがネットワーク上にとどまり続けることがあり，これを**ループ**と呼ぶ．このループを回避するためのプロトコルである．

問20　エ

IPsec（IP Security Protocol）：IPパケットのデータの暗号化と改ざん検出を行うプロトコルである．

L2TP（Layer 2 Tunneling Protocol）：仮想的にデータリンク層のトンネルを構築するプロトコルである．ダイヤルアップ接続よるインターネットを介したリモートアクセスにおいて，VPN構築に用いられる．

RADIUS（Remote Authentication Dial In User Service）：認証サーバがネットワーク上のサーバに認証とアカウントのサービスを提供するプロトコル．

SSH（Secure Shell）：リモートからホストのシェルを操作する通信で，その通信を暗号技術で保護している．

問題

問 21

正解 完璧 直前CHECK

Webサーバを使ったシステムにおいて，インターネットから受け取ったリクエストをWebサーバに中継する仕組みはどれか．

ア　DMZ　　イ　フォワードプロキシ
ウ　プロキシARP　　エ　リバースプロキシ

問 22

正解 完璧 直前CHECK

ブラックボックステストのテストデータの作成方法のうち，最も適切なものはどれか．

ア　稼働中のシステムから実データを無作為に抽出し，テストデータを作成する．
イ　機能仕様から同値クラスや限界値を識別し，テストデータを作成する．
ウ　業務で発生するデータの発生頻度を分析し，テストデータを作成する．
エ　プログラムの流れ図から，分岐条件に基づいたテストデータを作成する．

問 23

正解 完璧 直前CHECK

開発した製品で利用している新規技術に関して特許の出願を行った．日本において特許権の取得が可能なものはどれか．

ア　学会で技術内容を発表した日から11か月目に出願した．
イ　顧客と守秘義務の確認を取った上で技術内容を説明した後，製品発表前に出願した．
ウ　製品に使用した暗号の生成式を出願した．
エ　製品を販売した後に出願した．

問21 エ

DMZ（DeMilitarized Zone）：外部ネットワークと内部ネットワークの間にある，ファイアウォールによって隔離された区域である．外部ネットワークからの不正アクセスを防止しながら，内部ネットワークを保護している．

フォワードプロキシ：内部ネットワークのクライアントから外部ネットワークのサーバへのアクセスを中継するプロキシ．

プロキシARP：ホストへのARP要求に対して，代理としてARP応答する機能である．

リバースプロキシ：外部ネットワークのクライアントから内部ネットワークのサーバへの要求を中継するプロキシ．

問22 イ

ブラックボックステストは，入力に対して仕様書通りの出力が得られるかどうかを確認することで，外部から見た機能の検証を行う．入力と出力だけに着目し，内部的な処理構造は問題としない．テストデータは，**限界値分析**や**同値クラス**を用いて作成する．

エ：ホワイトボックスにおけるテストデータ作成の説明である．

問23 イ

ア，エ：特許取得では，次の条件の発明は受け付けられない．

・特許出願前に日本国内又は外国において公然知られた発明

・特許出願前に日本国内又は外国において公然実施をされた発明

・特許出願前に日本国内又は外国において頒布された刊行物に掲載された発明

ウ：特許権取得では，自然法則を利用した技術的思想の創作のうち高度なものを保護の対象とするため，計算方法や暗号等の自然法則の利用がないものは対象とならない．

問題

問 24

正解 完璧 直前CHECK

雷サージによって通信回線に誘起された異常電圧から通信機器を防護するための装置はどれか.

ア　IDF（Intermediate Distributing Frame）
イ　MCCB（Molded Case Circuit Breaker）
ウ　アレスタ
エ　避雷針

問 25

正解 完璧 直前CHECK

ITに係る内部統制を評価し検証するシステム監査の対象となるものはどれか.

ア　経営企画部が行っている中期経営計画の策定の経緯
イ　人事部が行っている従業員の人事考課の結果
ウ　製造部が行っている不良品削減のための生産設備の見直しの状況
エ　販売部が行っているデータベースの入力・更新における正確性確保の方法

問24　ウ

IDF（Intermediate Distributing Frame）：**中間配線盤**とも呼ばれ，通信経路の集線盤である主配線盤（DMF）と，モジュラージャック等のアウトレットを中継する配電盤である．

MCCB（Molded Care Circuit Breaker）：配線用遮断機とも呼ばれ，異常な電流が流れると，電源供給を遮断して回路や電線を破損から守る．

アレスタ：避雷器とも呼ばれ，通信機器などを雷の影響による異常な高電圧から保護する．

避雷針：建物の屋上等に設置し，落雷時に電流を避雷針から直接地面に流して建物の損害を防ぐ．また周辺への落雷を防止する．

問25　エ

システム監査は情報システムの信頼性，安全性，効率性について監査を行う．選択肢のうち，情報システムに関する監査に対応するものはエである．

信頼性：データ，処理正確性，監査証跡書確保，品質確保，障害対策（処理継続性），規則・手続準拠性等がある．

安全性：災害・障害・不正アクセス，破壊からの資源保護対策（リスク明確化・対策組込，システム内部，運用手続・規則，設備・保全等）がある．

効率性：レスポンスタイム，処理時間見積もり，資源使用量予測，運用・処理効率性，開発・保守容易性等がある．