セキュリティ演習問題

問１

企業の情報セキュリティポリシの基本方針策定に関する記述のうち，適切なものはどれか。

ア　業種ごとに共通であり，各企業で独自のものを策定する必要性は低い。
イ　システム管理者が策定し，システム管理者以外に知られないよう注意を払う.
ウ　情報セキュリティに対する企業の考え方や取り組みを明文化する.
エ　ファイアウォールの設定内容を決定し．文書化する.

問２

データの破壊やシステムの可用性が損なわれることで発生する損失に含まれる費用はどれか。

ア　業務形態の変更によるシステム再開発費用とデータベースの移行費用
イ　システム開発の実行可能性の検討にかかる費用
ウ　システムが復旧するまでの間，代替の手段にかかる費用
エ　新システムへの移行費用

問３

情報セキュリティにおける“完全性”を脅かす攻撃はどれか。

ア　Ｗｅｂページの改ざん
イ　システム内に保管されているデータの不正コピー
ウ　システムを過負荷状態にするＤｏＳ攻撃
エ　通信内容の盗聴

問４

コンピュータ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　一時記憶領域に残っている機密データは，ジョブ終了時に確実に消去する。
イ　金利計算処理などで，端数を特定口座に振り込む，いわゆるサラミ技術に対しては，データにチェックディジットを付加する。
ウ　端末から入力された数値データの改ざんに対しては，仮想記憶額域のページ又はセグメント単位に割り付けられた記憶保護キーによって，保護のレベルを変える。
エ　ユーティリティプログラムを使用したデータ改ざんに対しては，そのユーティリティプログラムのバックアップをとっておき，元のプログラムと比較する。

問５

インターネットＶＰＮのセキュリティに関する記述のうち，適切なものはどれか。

ア　ＩＰアドレスを悪用した不正アクセスや侵入の危険性はないので，ＩＰアドレスも含めたパケット全体の暗号化は必要ない。
イ　インターネットＶＰＮの仮想的なトンネルは特定ＬＡＮ間の専用通路であるから，通過するデータに対する盗聴防止の機能はない。
ウ　仮想的なネットワークを形成するものであり，ネットワークに参加する資格のない第三者による盗聴や改ざんを防御できない。
エ　ネットワークに参加する資格のある個々人を識別する能力はない。

問６

ある会社の資材担当者が電子メールを取引先へインターネットで送信したところ，取引先から不明なファイルが添付されているとの連絡が入った。資材担当者はファイルを添付した覚えがなく，電子メールソフトのマニュアルを見ても，添付されるとは記載されていないファイルであった。この場合，資材担当者の取るべき行動のうち，適切なものはどれか。

ア　送信履歴の添付ファイルを開き，確認する。画面上に見覚えのない画面が表示された場合，送信履歴から送信メールを削除する。
イ　どのような内容が送信されたのか，添付ファイルを開いて確認してくれるように送信先に依頼する。
ウ　パソコンにデータ破壊などの異常が発生していなければ，問題なしと判断し，そのままにする。
エ　連絡を受けた時点で，取引先には，添付ファイルを開かないように依頼し，すぐに自社のセキュリティ対策担当部署に調査を依頼する。

問７

通商産業省の“コンピュータウイルス対策基準”によるコンピュータウイルスの対策として，適切なものはどれか。

ア　ウイルスに感染した直後の対応として，一般利用者が最初にすべきことは，ウイルスの種類を解明し，特定することである。
イ　ウイルスに感染した媒体は，原則として廃棄する。どうしても廃棄できない重要なファイルがある場合だけ，ワクチンによるウイルスの駆除を試みる。
ウ　常に最新バージョンのワクチンプログラムを導入し，定期的にウイルスをチェックすることによって，ウイルスの感染を完全に防ぐことができる。
エ　バックアップファイルへのウイルス感染を防ぐには，バックアップ用の媒体として，ライトプロテクトを施せるものでは不十分であり，ライトワンスのものを用いる必要がある。

問８

電子メール送信時に送信者に対して宛先アドレスの確認を求めるのが有効であるセキュリティ対策はどれか。

ア　ＯＰ２５Ｂによるスパム対策
イ　ＳＰＦによるスパム対策
ウ　電子メールの誤送信対策
エ　電子メールの不正中継対策

問９

“コンピュータウイルス対策基準”において，コンピュータウイルスは三つの機能のうち少なくとも一つを有するものと定義されている。この機能の組合せとして，正しいものはどれか。

ア　自己伝染機能，潜伏機能，増殖機龍
イ　自己伝染機能，潜伏機能，発病機能
ウ　自己伝染機能，増殖機能，マクロ機能
エ　自己伝染機能，発病機能，マクロ機能

問10

コンピュータウィルスに関する記述のうち、適切なものはどれか。

ア　ウィルスの潜伏しているプログラムファイルがコンピュータ内に存在している場合であっても、コンピュータ利用者が意図的にファイルを起動しない限り感染しない。
イ　ウィルスは、主記憶装置を物理的に破壊したり、コンピュータ利用者の意図しない動作を引き起こしたりする。
ウ　ウィルスを検出・駆除するためのエンジンや定義ファイルなどが、最新のものに更新されているコンピュータでは感染しない。
エ　駆除作業では、ウィルスに感染していないＯＳ起動ディスクを使用することによって、ブートセクタからの感染を回避することができる。

問11

不正プログラムのワームに関する記述として、適切なものはどれか。

ア　アプリケーションソフト専用のマクロ言語で記述されている。
イ　ある指定の期日や条件を満たしたときに機能が働き、データファイルなどを破壊する。
ウ　ネットワーク経由でコンピュータ間を自己複製しながら移動する。
エ　他のプログラムに感染し、ネットワークを利用せずに単独で増殖する。

問12

コンピュータウイルス対策に関する記述のうち，適切なものはどれか。

ア　ウイルスに感染したディスクは論理フォーマッティングを行い，感染ファイルごとにウイルスを消去すべきである。
イ　書換え可能媒体からソフトウエアをインストールするときには，書込み禁止処置をせずにインストールすべきである。
ウ　ソフトウェアをインストールするときには，コンピュータ自体がウイルスに感染していないことを確認してからインストールすべきである。
エ　マルチユーザシステムでもウイルス対策は個人の問題なので，責任者を置かなくてもよい。

問13

コンピュータウィルス対策で用いられるウイルス定義ファイルに関する記述のうち，適切なものはどれか。

ア　ウイルス対策ソフトに含まれているファイルであり，ウイルスに感染したファイルを修復するために使用する。
イ　既知ウイルスのシグネチャコードを記録したファイルであり，ウイルス対策ソフトがウイルス検出時に使用する。
ウ　既知ウイルスのプログラムコードを記録したファイルであり，ウイルスを再現し，動作を監視するために使用する。
エ　復旧のためのファイルであり，ウイルスによってデータファイルが破壊されたときに使用する。

問14

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，未知のウイルスが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15

プログラムの一部をひそかに入れ替えて、本来の仕様どおりに機能させながら、データの不正コピー、悪用、改ざんなどの不正を意図的に実行させる方法はどれか。

ア　サラミ法　　イ　スーパザップ法
ウ　タッピング　　エ　トロイの木馬

問16

コンピュータウィルスを発見したときの適切な対処はどれか。

ア　ウイルス感染時の動作特性からウイルス名を特定するために，動作の再現性を確認する。
イ　短時間のうちに広範囲に感染するワームが発見されても，オンライン業務システムとして稼働中の場合は，そのままの状態でウイルス対策を進める。
ウ　ネットワークを経由してほかのコンピュータに感染する可能性があるので，まず感染したコンピュータをネットワークから切り離す。
エ　メモリ上にウイルスプログラムが展開されている可能性があるので，まずコンピュータの電源を切る。

問17

データの破壊，改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールさせ，実行させるものはどれか。

ア　ＤｏＳ攻撃　　イ　辞書攻撃
ウ　トロイの木馬　　エ　バッファオーバフロー攻撃

問18

手順に示すセキュリティ攻撃はどれか。

〔手順〕
（１）　攻撃者が金融機関の偽のＷｅｂサイトを用意する。
（２）　金融機関の社員を装って，偽のＷｅｂサイトへ誘導するＵＲＬを本文中に含めた電子メールを送信する。
（３）　電子メールの受信者が，その電子メールを信用して本文中のＵＲＬをクリックすると，偽のＷｅｂサイトに誘導される。
（４）　偽のＷｅｂサイトと気付かずに認証情報を入力すると，その情報が攻撃者に渡る。

ア　ＤＤｏＳ攻撃　　イ　フィッシング
ウ　ポット　　エ　メールヘッダインジェクション

問19

ソーシャルエンジエアリングに分類される手口はどれか。

ア　ウイルス感染で自動作成されたバックドアからシステムに侵入する。
イ　システム管理者などを装い，利用者に問い合わせてパスワードを取得する。
ウ　総当たり攻撃ツールを用いてパスワードを解析する。
エ　バッファオーバフローなどのソフトウエアの脆弱性を利用してシステムに侵入する。

問20

フィッシングの手口に該当するものはどれか。

ア　Ｗｅｂページに入力した内容をそのまま表示する部分がある場合，ページ内に悪意のスクリプトを埋め込み，ユーザとサーバに被害を与える。
イ　ウイルスに感染したコンピュータを，インターネットなどのネットワークを通じて外部から操る。
ウ　コンピュータ利用者のＩＰアドレスやＷｅｂの閲覧履歴などの個人情報を，ひそかに収集して外部へ送信する。
エ　電子メールを発信して受信者を誘導し，実在する会社などを装った偽のＷｅｂサイトにアクセスさせ，個人情報をだまし取る。

問21

コンピュータシステムを利用する上でウィルスという新しい災害が出現し、これに対する予防や検知、事後対策等が講じられている。対策に利用されているものは次のうちのどれか。

ア　クリッパー　　イ　カスケード
ウ　ミケランジェロ　　エ　ワクチン

問22

コンピュータ犯罪の代表的な手口に関する記述のうち,適切なものはどれか。

ア　サラミ法とは、多数の資産から、全体への影響が無視できる程度にわずかずつ詐取する方法である。
イ　スキャビンジング(ごみ箱あさり)とは、電話機や端末を使用してコンピュータネットワークからデータを盗用する方法である。
ウ　盗聴とは、音声の伝送を行っている電話回線への不正アクセスに用いられる犯罪手口のことであり、コンピュータデータを対象としない。
エ　トロイの木馬とは、プログラム実行後のコンピュータ内部、又はその周囲に残っている情報をひそかに入手する方法である。

問23

コンピュータ犯罪の手口の一つであるサラミ法はどれか。

ア　回線の一部に秘密にアクセスして他人のパスワードやＩＤを盗み出してデータを盗用する方法である。
イ　ネットワークを介して送受信されている音声やデータを不正に傍受する方法である。
ウ　不正行為が表面化しない程度に，多数の資産から少しずつ詐取する方法である。
エ　プログラム実行後のコンピュータ内部又はその周囲に残っている情報をひそかに探索して，必要情報を入手する方法である。

問24

最近、増加しているマクロウィルスに関する記述として、正しいものはどれか。

ア　感染したアプリケーションを実行すると、マクロウィルスは主記憶にロードされ、その間に実行したほかのアプリケーションのプログラムファイルに感染する。
イ　感染したフロッピーディスクからシステムを起動するとマクロウィルスは主記憶にロードされ、ほかのフロッピーディスクのブートセクタに感染する。
ウ　感染した文書ファイルを開いた後に、別に開いたり新規作成した文書ファイルに感染する。
エ　マクロがウィルスに感染しているかどうかが容易に判断できるので、文書ファイルを開く時点で感染を防止できる。

問25

コンピュータやネットワークのセキュリティ上の脆弱性を発見するために，システムを実際に攻撃して侵入を試みる手法はどれか。

ア　ウォークスルー
イ　ソフトウェアインスペクション
ウ　ペネトレーションテスト
エ　リグレッションテスト

問26

コンピュータウィルス対策ソフトのパターンマッチング方式を説明したものはどれか。

ア　感染前のファイルと感染後のファイルを比較し，ファイルに変更が加わったかどうかを調べてウイルスを検出する。
イ　既知ウイルスのシグネチャコードと比較して，ウイルスを検出する。
ウ　システム内でのウイルスに起因する異常現象を監視することによって，ウイルスを検出する。
エ　フアイルのチェックサムと照合して，ウイルスを検出する。

問27

ＳＱＬインジェクションの説明はどれか。

ア　Ｗｅｂアプリケーションに問題があるとき，データベースに悪意のある問合せや操作を行う命令文を入力して，データベースのデータを改ざんしたり不正に取得したりする攻撃
イ　悪意のあるスクリプトを埋め込んだＷｅｂページを訪問者に閲覧させて，別のＷｅｂサイトで，その訪問者が意図しない操作を行わせる攻撃
ウ　市販されているＤＢＭＳの脆弱性を利用することによって，宿主となるデータベースサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃
エ　訪問者の入力データをそのまま画面に表示するＷｅｂサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃

問28

ＳＱＬインジェクション攻撃を防ぐ方法はどれか。

ア　入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。
イ　入力にＨＴＭＬタグが含まれていたら，ＨＴＭＬタグとして解釈されない他の文字列に置き換える。
ウ　入力に，上位ディレクトリを指定する文字列(‥／)を含むときは受け付けない。
エ　入力の全体の長さが制限を超えているときは受け付けない。

問29

緊急事態を装う不正な手段によって組織内部の人間からパスワードや機密情報を入手する行為は，どれに分類されるか。

ア　ソーシャルエンジニアリング　　イ　トロイの木馬
ウ　パスワードクラック　　エ　踏み台攻撃

問30

ディレクトリトラバーサル攻撃に該当するものはどれか。

ア　攻撃者が，Ｗｅｂアプリケーションの入力データとしてデータベースへの命令文を構成するデータを入力し，管理者の意図していないＳＱＬ文を実行させる。
イ　攻撃者が，パス名を使ってファイルを指定し，管理者の意図していないファイルを不正に閲覧する。
ウ　攻撃者が，利用者をＷｅｂサイトに誘導した上で，Ｗｅｂアプリケーションによるｈｔｍｌ出力のエスケープ処理の欠陥を悪用し，利用者のＷｅｂブラウザで悪意のあるスクリプトを実行させる。
エ　セッションＩＤによってセッションが管理されるとき，攻撃者がログイン中の利用者のセッションＩＤを不正に取得し，その利用者になりすましてサーバにアクセスする。

問31

ＤＮＳキャッシュポイズニングに分類される攻撃内容はどれか。

ア　ＤＮＳサーバのソフトウェアのバージョン情報を入手して，ＤＮＳサーバのセキュリティホールを特定する。
イ　ＰＣが参照するＤＮＳサーバに誤ったドメイン情報を注入して，偽装されたＷｅｂサーバにＰＣの利用者を誘導する。
ウ　攻撃対象のサービスを妨害するために，攻撃者がＤＮＳサーバを踏み台に利用して再帰的な問合せを大量に行う。
エ　内部情報を入手するために，ＤＮＳサーバが保存するゾーン情報をまとめて転送させる。

問32

情報漏えい対策に該当するものはどれか。

ア　送信するデータにチェックサムを付加する。
イ　データが保存されるハードディスクをミラーリングする。
ウ　データのバックアップ媒体のコピーを遠隔地に保管する。
エ　ノート型ＰＣのハードディスクの内容を暗号化する。

問33

虚偽のデータや不正プログラム等を入力して、自分の預金口座に振り込み、入金させたり、偽造や変造したりプリペイドカードを使って不正な利益を得る行為に適用される犯罪はどれか。

ア　詐欺罪　　イ　電磁的記録不正作出罪
ウ　電子計算機損壊等業務妨害罪　　エ　電子計算機使用詐欺罪

問34

リスクアセスメントに関する記述のうち，適切なものはどれか。

ア　以前に洗い出された全てのリスクへの対応が完了する前に，リスクアセスメントを実施することは避ける。
イ　将来の損失を防ぐことがリスクアセスメントの目的なので，過去のリスクアセスメントで利用されたデータを参照することは避ける。
ウ　損失額と発生確率の予測に基づくリスクの大きさに従うなどの方法で，対応の優先順位を付ける。
エ　リスクアセスメントはリスクが顕在化してから実施し，損失額に応じて対応の予算を決定する。

問35

リスク分析に関する記述のうち，適切なものはどれか。

ア　考えられるすべてのリスクに対処することは時間と費用がかかりすぎるので，損失額と発生確率を予測し，リスクの大きさに従って優先順位を付けるべきである。
イ　リスク分析によって評価されたリスクに対し，すべての対策が完了しないうちに，繰り返しリスク分析を実施することは避けるべきである。
ウ　リスク分析は，将来の損失を防ぐことが目的であるから，過去の類似プロジェクトで蓄積されたデータを参照することは避けるべきである。
エ　リスク分析は，リスクの発生による損失額を知ることが目的であり，その損失額に応じて対策の費用を決定すべきである。

問36

リスク移転を説明したものはどれか。

ア　損失の発生率を低下させること
イ　保険に加入するなど資金面での対策を講じること
ウ　リスクの原因を除去すること
エ　リスクを扱いやすい単位に分解するか集約すること

問37

リスクが顕在化しても，その影響が小さいと想定されるので，損害の負担を受容するリスク対応はどれか。

ア　リスク移転　　イ　リスク回避
ウ　リスク低減　　エ　リスク保有

問38

ネットワーク障害の原因を調べるために使用するＬＡＮアナライザの運用上の注意点はどれか。

ア　ＬＡＮアナライザにはネットワークを通過するパケットを表示できるものがあるので，盗聴などに悪用されないように注意する必要がある。
イ　障害発生に備えて，ネットワーク利用者にＬＡＮアナライザの保管場所と使用方法を周知しておく必要がある。
ウ　測定中は，本来通信すべきあて先のパケットを破棄してしまうので，測定対象外のコンピュータ利用を制限しておく必要がある。
エ　測定に当たって，ＬＡＮケーブルを一時的に切断する必要があるので，利用者に対して測定日を事前に知らせておく必要がある。

問39

情報システムのセキュリティコントロールを予防，検知，復旧の三つに分けた場合，復旧に該当するものはどれか。

ア　オペレータとプログラマの職務分離
イ　コンティンジェンシープラン
ウ　パスワードの利用
エ　メッセージ認証

問40

企業内ネットワークやサーバにおいて，侵入者が通常のアクセス経路以外で侵入するために組み込むものはどれか。

ア　シンクライアントエージェント　　イ　ストリクトルーティング
ウ　バックドア　　エ　フォレンジック

問41

ネットワークシステム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　ＩＳＤＮ回線やパケット交換回線では，接続時に通知される相手の加入者番号によって相手確認を行うことができる。これをコールバックと呼ぶ。
イ　回線暗号化装置をＤＴＥ(通信制御装置や端末装置など)とＤＣＥ(モデムやＤＳＵなど)の間に設置して，伝送区間ごとに暗号化を行う方法では，既設のハードウェアやソフトウェアの一部に変更が必要になる。
ウ　閉域接続機能をもつ回線交換網を利用して，回線接続の範囲を特定の利用者グループに限定することは，外部からの不正アクセスの防止に有効である。
エ　無線ＬＡＮの使用は，ケーブルを介在させないので伝送途中の盗聴防止に有効である。

問42

Ｗｅｂサーバが外部から侵入され、コンテンツが改ざんされた。その後の対応の順序のうち，適切なものはどれか。

①	サーバ，IDS（Intrusion Detection System），ファイアウォールの各ログを解析し，不正アクセス手法，影響範囲，侵入経路を特定する。
②	システムを再構築し，最新のパッチやセキュリティ設定情報を適用する。
③	サーバをネットワークから切り離す。
④	ネットワークに接続後，しばらく監視する。

ア　①→②→③→④　　イ　①→③→②→④
ウ　②→③→①→④　　エ　③→①→②→④

問43

ＷＡＦ(Web Application Firewall)を利用する目的はどれか。

ア　Ｗｅｂサーバ及びアプリケーションに起因する脆弱性への攻撃を遮断する。
イ　Ｗｅｂサーバ内でワームの侵入を検知し，ワームの自動駆除を行う。
ウ　Ｗｅｂサーバのコンテンツ開発の結合テスト時にアプリケーションの脆弱性や不整合を検知する。
エ　Ｗｅｂサーバのセキュリティホールを発見し，ＯＳのセキュリティパッチを適用する。

問44

クライアントとＷｅｂサーバの間において，クライアントからＷｅｂサーバに送信されたデータを検査して，ＳＱＬインジェクションなどの攻撃を遮断するためのものはどれか。

ア　ＳＳＬＶＰＮ機能　　イ　ＷＡＦ
ウ　クラスタ構成　　エ　ロードバランシング機能

問45

ＩＳＭＳプロセスのＰＤＣＡモデルにおいて，ＰＬＡＮで実施するものはどれか。

ア　運用状況の管理
イ　改善策の実施
ウ　実施状況に対するレビュー
エ　情報資産のリスクアセスメント

問46

ＪＩＳＱ27001:2006におけるＩＳＭＳの確立に必要な事項①～③の順序関係のうち，適切なものはどれか。

① 適用宣言書の作成
② リスク対応のための管理目的及び管理策の選択
③ リスクの分析と評価

ア　①→②→③　　イ　①→③→②
ウ　②→③→①　　エ　③→②→①

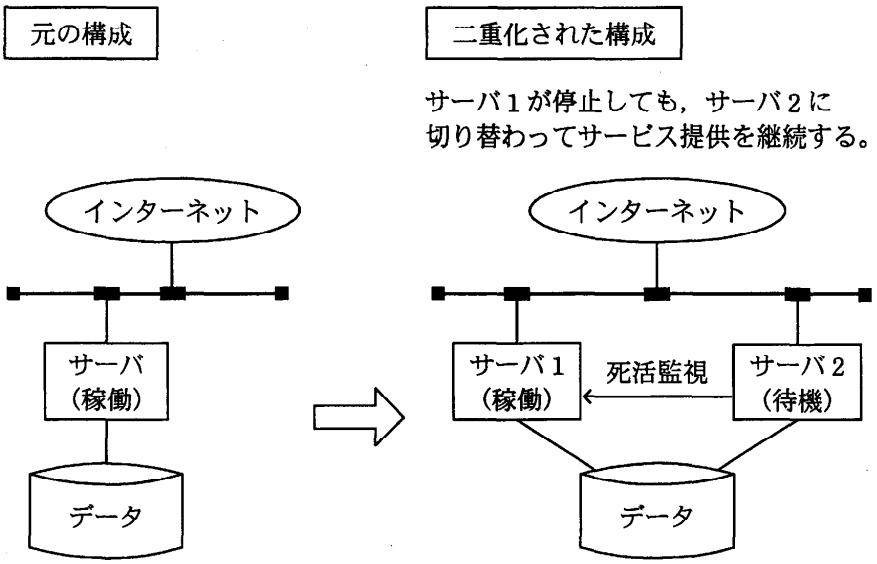
問47

情報システムへの脅威とセキュリティ対策の組合せのうち，適切なものはどれか。

	脅威	セキュリティ対策
ア	誤操作によるデータの論理的な破壊	ディスクアレイ
イ	地震と火災	コンピュータ内で複数の仮想化OSを利用したデータの二重化
ウ	伝送中のデータへの不正アクセス	HDLC手順のCRC
エ	メッセージの改ざん	公開鍵暗号方式を応用したディジタル署名

問48

図のようなサーバ構成の二重化によって期待する効果はどれか。



ア　可用性の向上　　イ　完全性の向上
ウ　機密性の向上　　エ　責任追跡性の向上

問49

システム障害を想定した事業継続計画（ＢＣＰ）を策定する場合，ビジネスインパクト分析での実施事項はどれか。

ア　ＢＣＰの有効性を検証するためのテストを実施する。
イ　情報システム障害時の代替手順と復旧手順について関係者を集めて教育する。
ウ　情報システムに関する内外の環境の変化を踏まえてＢＣＰの内容を見直す。
エ　情報システムに許容される最大停止時間を決定する。

問50

ＢＣＰの説明はどれか。

ア　企業の戦略を実現するために，財務，顧客，内部ビジネスプロセス，学習と成長の視点から戦略を検討したもの
イ　企業の目標を達成するために業務内容や業務の流れを可視化し，一定のサイクルをもって継続的に業務プロセスを改善するもの
ウ　業務効率の向上，業務コストの削減を目的に，業務プロセスを対象としてアウトソースを実施するもの
エ　事業中断の原因とリスクを想定し，未然に回避又は被害を受けても速やかに回復できるように方針や行動手順を規定したもの

問51

会社や団体が，自組織の従業員に貸与するスマートフォンに対して，セキュリティポリシに従った一元的な設定をしたり，業務アプリケーションを配信したりして，スマートフォンの利用状況などを一元管理する仕組みはどれか。

ア　ＢＹＯＤ (Bring Your Own Device)
イ　ＥＣＭ (Enterprise Contents Management)
ウ　ＬＴＥ (Long Term Evolution)
エ　ＭＤＭ (Mobile Device Management)

問52

ＢＹＯＤ(Bring Your Own Device)の説明はどれか。

ア　従業員が企業から貸与された情報端末を,客先などへの移動中に業務に利用することであり，ショルダハッキングなどのセキュリティリスクが増大する。
イ　従業員が企業から貸与された情報端末を，自宅に持ち帰って私的に利用することであり，機密情報の漏えいなどのセキュリティリスクが増大する。
ウ　従業員が私的に保有する情報端末を，職場での休憩時間などに私的に利用することであり，社内でのセキュリティ意識の低下などのセキュリティリスクが増大する。
エ　従業員が私的に保有する情報端末を業務に利用することであり，セキュリティ設定の不備に起因するウイルス感染などのセキュリティリスクが増大する。

問53

クライアントＰＣで行うマルウェア対策のうち，適切なものはどれか。

ア　ＰＣにおけるウイルスの定期的な手動検査では，ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
イ　ウイルスがＰＣの脆弱性を突いて感染しないように，ＯＳ及びアプリケーションの修正パッチを適切に適用する。
ウ　電子メールに添付されたウイルスに感染しないように，使用しないＴＣＰポート宛ての通信を禁止する。
エ　ワームが侵入しないように，クライアントＰＣに動的グローバルＩＰアドレスを付与する。

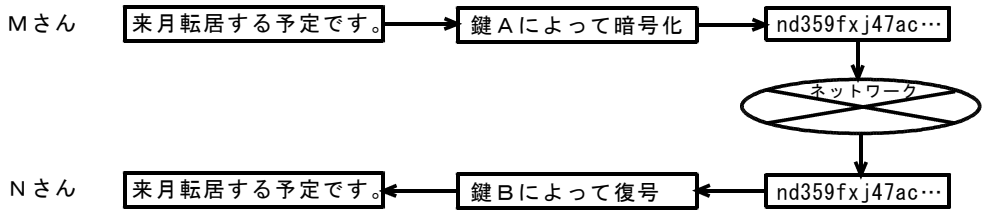
問54

通信の“傍受や盗聴”の被害を避ける対策として，正しいものはどれか。

ア　暗号化　　イ　デジタル署名
ウ　ファイアウオール　　エ　メッセージ認証

問55

公開鍵暗号方式を用いて、図のようにＭさんからＮさんに他人に秘密にしておきたい文章を送るとき、暗号化と復号に用いる鍵として、適切な組合せはどれか。



	鍵Ａ	鍵Ｂ
ア	Ｍさんの秘密鍵	Ｍさんの公開鍵
イ	Ｎさんの公開鍵	Ｎさんの秘密鍵
ウ	共通の公開鍵	Ｎさんの秘密鍵
エ	共通の秘密鍵	共通の公開鍵

問56

公開かぎ暗号方式で，送信者が受信者に暗号文を送る場合の手順はどれか。

ア　送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
イ　送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する。
ウ　送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
エ　送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する。

問57

公開かぎ暗号方式の暗号化かぎと復号かぎの関係として，適切なものはどれか。

	暗号化鍵と復号鍵の関係	暗号化鍵	復号鍵
ア	暗号化鍵≠復号鍵	公開	公開
イ	暗号化鍵≠復号鍵	公開	秘密
ウ	暗号化鍵＝復号鍵	秘密	公開
エ	暗号化鍵＝復号鍵	秘密	秘密

問58

Ｘさんは，Ｙさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容は秘密にする必要があるので，公開かぎ暗号方式を使って暗号化して，送信したい。電子メールの内容を暗号化するのに使用するかぎとして，適切なものはどれか。

ア　Ｘさんの公開かぎ　　イ　Ｘさんの秘密かぎ
ウ　Ｙさんの公開かぎ　　エ　Ｙさんの秘密かぎ

問59

ある商店が、顧客からネットワークを通じて注文を受けるために、公開鍵暗号方式を利用して、注文の内容が第三者に分からないようにした。商店、顧客それぞれが利用する鍵の適切な組合せはどれか。

	商店	顧客
ア	公開鍵	秘密鍵
イ	公開鍵	公開鍵と秘密鍵
ウ	秘密鍵	公開鍵
エ	秘密鍵	公開鍵と秘密鍵

問60

暗号方式に関する記述のうち、正しいものはどれか。

ア　公開かぎ暗号方式では、暗号かぎを通信相手へ秘密裡に配信する必要がある。
イ　公開かぎ暗号方式では、秘密かぎ暗号方式よりも後で考案され、数学的に巧みな理論を応用しているので、秘密かぎ暗号方式に比べ復号処理が単純で高速なものとなっている。
ウ　秘密かぎ暗号方式のかぎを通信の開始時に公開かぎ暗号方式を使って送り、データの暗号化をそのかぎで行うという方法が実用化されている。
エ　秘密かぎ暗号方式は、多数の相手との通信の際、同一の暗号かぎを用いても安全である。

問61

文書の内容を秘匿して送受信する場合の公開鍵暗号方式における鍵の取扱いのうち，適切なものはどれか。

ア　暗号化鍵と復号鍵は公開してもよいが，暗号化のアルゴリズムは秘密にしなければならない。
イ　暗号化鍵は公開してもよいが，暗号化のアルゴリズムは秘密にしなければならない。
ウ　暗号化鍵は秘密にしなければならないが，復号鍵は公開する。
エ　復号鍵は秘密にしなければならないが，暗号化鍵は公開する。

問62

暗号化に関する記述のうち，正しいものはどれか。

ア　ＤＥＳは公開かぎ暗号方式，ＲＳＡは秘密かぎ暗号方式の代表例である。
イ　公開かぎ暗号方式では，必ず暗号化かぎを秘密にして，復号かぎを公開する。
ウ　デジタル署名に利用するには，公開かぎ暗号方式よりも秘密かぎ暗号方式の方がよい。
エ　秘密かぎ暗号方式では，暗号化かぎと復号かぎは同じである。

問63

暗号に関する記述のうち,適切なものはどれか。.

ア　ＤＥＳは,公開かぎ暗号方式の一種である。
イ　ＲＳＡは,素因数分解の計算の複雑さを利用した公開かぎ暗号方式の一種である。
ウ　公開かぎ暗号方式の難点は,かぎの管理が煩雑になることである。
エ　公開かぎ暗号方式は,暗号化と復号とに異なるかぎを用い,受信者の復号かぎを公開する方式である。

問64

代表的な暗号方式の一つであるＤＥＳについて、正しいものはどれか。

ア　アルゴリズムが公開されている共通鍵方式である。
イ　暗号化鍵だけを公開し、復号鍵を秘密にする方式である。
ウ　処理に時間がかかるが、認証機能に優れインターネットでの利用に適した方式である。
エ　米国政府の標準方式で、盗聴者はもちろん、作成者も暗号文を平文に戻すことはできない安全性の高い方式である。

問65

平文を公開かぎ暗号方式を用いて暗号化するときの“かぎ”に関する記述として，正しいものはどれか。

ア　暗号文を受信した時に，暗号化かぎから計算によって復号かぎを算出する。
イ　事前に，暗号化かぎから計算によって復号かぎを算出しておく。
ウ　受信側は，暗号化かぎを知っている。
エ　送信側は，暗号化かぎから算出した復号かぎを，暗号化されたメッセージ本文とは別に受信側へ渡す。

問66

暗号化方式の名称に関する記述のうち，共通かぎ方式に分類されるものはどれか。

ア　ＤＥＳ　　イ　ＲＳＡ　　ウ　エルガマル暗号　　エ　だ円曲線暗号

問67

公開鍵暗号方式に関する記述として，適切なものはどれか。

ア　ＡＥＳなどの暗号方式がある。
イ　ＲＳＡや楕円曲線暗号などの暗号方式がある。
ウ　暗号化鍵と復号鍵が同一である。
エ　共通鍵の配送が必要である。

問68

公開かぎ暗号方式の用法に関する記述のうち，送信者が間違いなく本人であることを受信者が確認できるのはどれか。

ア　送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
イ　送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する。
ウ　送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
エ　送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する。

問69

平文を４文字ずつのブロックに分け、それぞれのブロック内の文字の位置を、１番目を３番目に、２番目を１番目に、３番目を４番目に、４番目を２番目に置き換える転置式暗号がある。このとき、平文“ＤＥＥＲＤＩＤＤＲＥＡＭＤＥＥＰ”の暗号文として、正しいものはどれか。

ア　ＤＩＤＤＤＥＥＰＤＥＥＲＲＥＡＭ
イ　ＥＤＲＥＤＤＤＩＡＲＭＥＥＤＰＥ
ウ　ＥＲＤＥＩＤＤＤＥＭＲＡＥＰＤＥ
エ　ＩＤＤＤＥＰＤＥＥＲＤＥＥＭＲＡ

問70

共通かぎ方式の暗号として，ビット列のデータにかぎとの排他的論理和(Å)を適用する方式がある。排他的論理和とは，次のとおりの結果になる演算である。

０Å０＝０　０Å１＝１　１Å０＝１　１Å１＝０

例えば，１１００というデータに対して，１０１０というかぎを使って暗号化すると，暗号データは０１１０となり，同じかぎとの排他的論理和をとることによって復号もできる。

データ	1	1	0	0
かぎ	1	0	1	0
暗号データ	0	1	1	0

↓暗号化　↑復号

１０１０というかぎを使って００１０という暗号データを得た。元のデータはどれか。

ア　００１０　　イ　１０００　　ウ　１０１０　　エ　１１００

問71

シーザ暗号はアルファベットをＮ文字分ずらす暗号方式である。例えば、ａｂｃｄをＮ＝２で暗号化するとｃｄｅｆとなる。シーザ暗号で暗号化された結果得られた文ｇｅｗｌを復号したところｃａｓｈであることが分かった。Ｎの値で正しいものはどれか。

ア　２　　イ　３　　ウ　４　　エ　５

問72

電子メールの送信者が正当な相手かどうかを確認するために，公開かぎ暗号方式を用いたディジタル署名を利用する場合，必要となるかぎの組合せはどれか。

ア　受信者の公開かぎと受信者の秘密かぎ
イ　受信者の公開かぎと送信者の秘密かぎ
ウ　送信者の公開かぎと受倍者の秘密かぎ
エ　送信者の公開かぎと送信者の秘密かぎ

問73

公開鍵暗号方式に関する記述のうち，適切なものはどれか。

ア　ＡＥＳは，ＮＩＳＴが公募した公開鍵暗号方式である。
イ　ＲＳＡは，素因数分解の計算の困難さを利用した公開鍵暗号方式である。
ウ　公開鍵暗号方式に参加する利用者の数が増えると鍵の配送が煩雑になる。
エ　通信文の内容の秘匿に公開鍵暗号方式を使用する場合は，受信者の復号鍵を公開する。

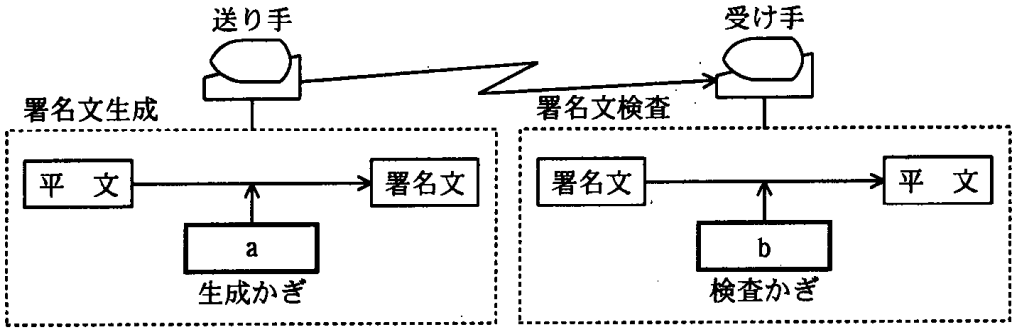
問74

非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。

ア　ＡＥＳ　　イ　ＤＳＡ　　ウ　ＩＤＥＡ　　エ　ＲＳＡ

問75

図は，公開かぎ暗号方式による電子署名の構成を示している。ａ，ｂに該当する適切な組合せはどれか。



	a	b
ア	受け手の公開鍵	受け手の秘密鍵
イ	送り手の公開鍵	送り手の秘密鍵
ウ	送り手の秘密鍵	受け手の公開鍵
エ	送り手の秘密鍵	送り手の公開鍵

問76

ディジタル署名に用いる鍵の種別に関する組合せのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

問77

デジタル署名の説明として、最も適切なものはどれか。

ア　受信者が署名鍵を使って暗号文を元の平文に戻す。
イ　送信者が、送信する平文の意味を関係者以外に分からないようにする。
ウ　送信者は平文に冗長性を付加し、暗号化する。受信者は復号したとき、予め定められた冗長性が入っていれば正しいメッセージと判断する。
エ　送信者は平文に署名鍵を使って署名することによって、受信者が送信者を確認できるようにする。

問78

デジタル署名に関する記述のうち，適切なものはどれか。

ア　発信者は相手の公開かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。
イ　発信者は相手の秘密かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。
ウ　発信者は自分の公開かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。
エ　発信者は自分の秘密かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。

問79

ディジタル署名などに用いるハッシュ関数の特徴はどれか。

ア　同じメッセージダイジェストを出力する二つの異なるメッセージは容易に求められる。
イ　メッセージが異なっていても，メッセージダイジェストは全て同じである。
ウ　メッセージダイジェストからメッセージを復元することは困難である。
エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

問80

ディジタル署名を利用する主な目的は二つある。一つは，受信者がメッセージの発信者を確認することである。もう一つの目的はどれか。

ア　受信者が，発信者のＩＤを確認すること
イ　受信者が，秘密かぎを返送してよいかどうかを確認すること
ウ　署名が行われた後で，メッセージに変更が加えられていないかどうかを確認すること
エ　送信の途中で，メッセージが不当に解読されていないことを確認すること

問81

インターネットで公開されているソフトウェアにディジタル署名を添付する目的はどれか。

ア　ソフトウェアの作成者が保守責任者であることを告知する。
イ　ソフトウェアの使用を特定の利用者に制限する。
ウ　ソフトウェアの著作権者が署名者であることを明示する。
エ　ソフトウェアの内容が改ざんされていないことを保証する。

問82

暗号を利用したデジタル署名に関する記述のうち、正しいものはどれか。

ア　発信者は自分の公開鍵でメッセージを暗号化することによってデジタル署名を行い、受信者は自分の公開鍵で復号し確認する。
イ　発信者は自分の公開鍵でメッセージを暗号化することによってデジタル署名を行い、受信者は自分の秘密鍵で復号し確認する。
ウ　発信者は相手の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、自分の公開鍵でさらに暗号化する。
エ　発信者は自分の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、相手の公開鍵でさらに暗号化する。

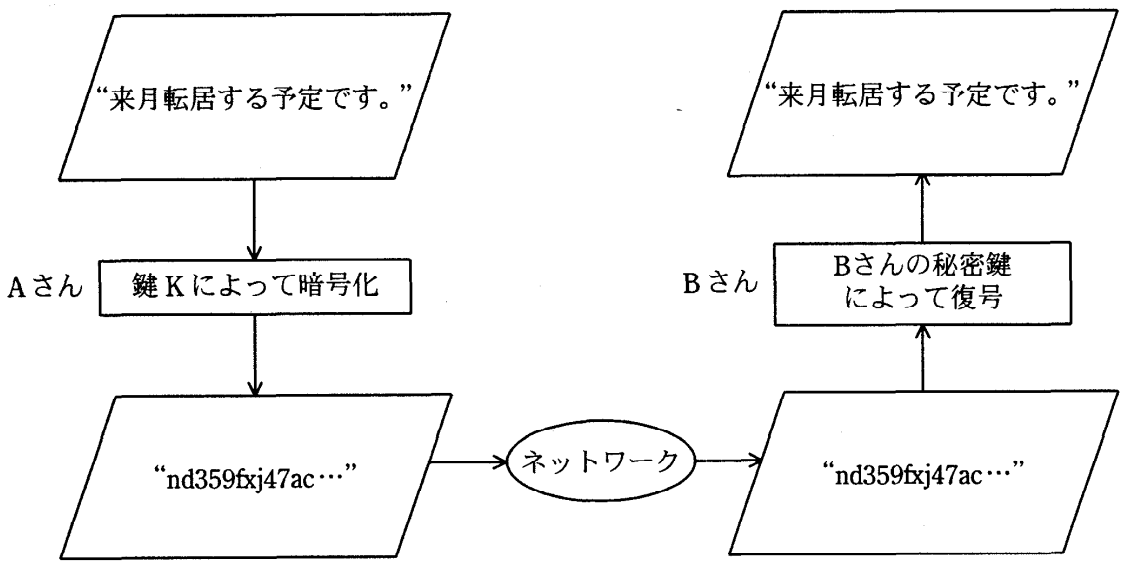
問83

ディジタル証明書をもつＡ氏が，Ｂ商店に対して電子メールを使って商品の注文を行うときに，Ａ氏は自分の秘密鍵を用いてディジタル署名を行い，Ｂ商店はＡ氏の公開鍵を用いて署名を確認する。この事法によって確認できることはどれか。ここで，Ａ氏の秘密鍵はＡ氏だけが使用できるものとする。

ア　Ａ氏からＢ商店に送られた注文の内容は，第三者に漏れない。
イ　Ａ氏から発信された注文は，Ｂ商店に届く。
ウ　Ｂ商店に届いたものは，Ａ氏からの注文である。
エ　Ｂ商店は，Ａ氏に商品を売ることの許可が得られる。

問84

公開鍵暗号方式を用いて，図のようにＡさんからＢさんへ，他人に秘密にしておきたい文章を送るとき，暗号化に用いる鍵Ｋとして，適切なものはどれか。



ア　Ａさんの公開鍵　　イ　Ａさんの秘密鍵
ウ　Ｂさんの公開鍵　　エ　共通の秘密鍵

問85

ディジタル署名付きのメッセージをメールで受信した。受信したメッセージのディジタル署名を検証することによって，確認できることはどれか。

ア　メールが，不正中継されていないこと
イ　メールが，漏えいしていないこと
ウ　メッセージが，改ざんされていないこと
エ　メッセージが，特定の日時に再送信されていないこと

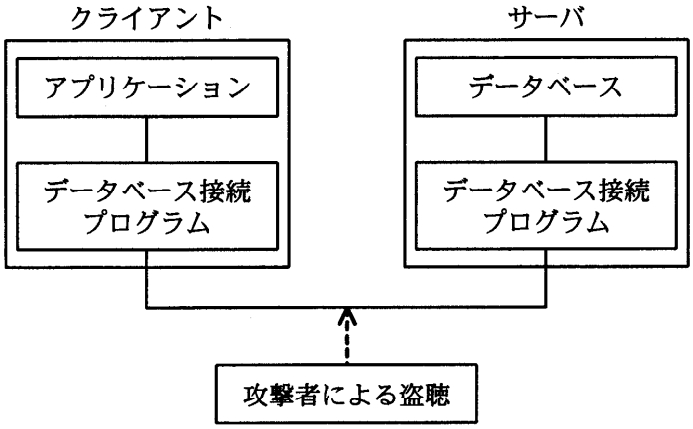
問86

ネットワークを使用するシステムで，暗号化技術を利用しても実現できないものはどれか。

ア　いったん受信したメッセージを，後で送信元から送信した覚えはないといって否定されることを防止する。
イ　受信メッセージが，正当な送出者からのものであることを確認する。
ウ　データの第三者への漏えいを防止する。
エ　メッセージが途中で失われることを防止する。

問87

図のように，クライアント上のアプリケーションがデータベース接続プログラム経由でサーバ上のデータベースのデータにアクセスする。データベース接続プログラム間で送受信されるデータが，通信経路上で盗聴されることに対する対策はどれか。



ア　クライアント側及びサーバ側にあるデータベース接続プログラム間の通信を暗号化する。

イ　サーバ側のデータベース接続プログラムにアクセスできるクライアントのＩＰアドレスを必要なものだけに制限する。

ウ　サーバ側のデータベース接続プログラムを起動・停止するときに必要なパスワードを設定する。

エ　データベース接続プログラムが通信に使用するポート番号をデータベース管理システムによって提供される初期値から変更する。

問88

手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。

〔手順〕

（１）送信者は，電子メールの本文を共通鍵暗号方式で暗号化し(暗号文)，その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する(共通鍵の暗号化データ)。

（２）送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。

（３）受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号方式で復号し，得た共通鍵で暗号文を復号する。

ア　送信者による電子メールの送達確認

イ　送信者のなりすましの検出

ウ　電子メールの本文の改ざんの有無の検出

エ　電子メールの本文の内容の漏えいの防止

問89

通信販売の電子商取引では，受発注における改ざん，なりすまし，否認によって販売業者又は利用者に被害が及ぶ危険性がある。この三つの防止に適用できるセキュリティ技術はどれか。

ア　ウィルスチェック　　イ　ジャンクメールフィルタ
ウ　ディジタル署名　　エ　ファイアウォール

問90

電子メールを暗号化するために使用される方式はどれか。

ア　ＢＡＳＥ６４　　イ　ＧＺＩＰ
ウ　ＰＮＧ　　エ　Ｓ／ＭＩＭＥ

問91

電子メールに用いられるＳ／ＭＩＭＥの機能はどれか。

ア　内容の圧縮　　イ　内容の暗号化と署名
ウ　内容の開封通知　　エ　内容の再送

問92

ＰＣからサーバに対し，ＩＰｖ６を利用した通信を行う場合，ネットワーク層で暗号化を行うのに利用するものはどれか。

ア　ＩＰsec　　イ　ＰＰＰ　　ウ　ＳＳＨ　　エ　ＳＳＬ

問93

“コンピュータ不正アクセス対策基準”に適合しているものはどれか。

ア　監視効率を向上させるためにすべてのネットワークを相互接続する。
イ　業務上必要な場合は，利用者ＩＤを個人間で共有して使用できる。
ウ　システム管理者が，すべての権限をもつ利用者ＩＤを常に使用できる。
エ　組織のセキュリティ方針を文書化し，定期的に研修を開催する。

問94

コンピュータシステムに対する利用者の利用資格の正当性チェックと利用状況の把握を行う目的で，利用者に付与される情報を表す用語として，適切なものはどれか。

ア　ＩＰアドレス　　イ　アクセス権
ウ　パスワード　　エ　ユーザＩＤ

問95

インターネット利用時のセキュリティ確保に関する記述のうち，適切なものはどれか。

ア　インターネットを経由してデータベースサーバを利用する場合，データベースへの不正アクセスやデータの改ざんを防止する対策も必要となる。
イ　インターネットを利用して電子メールを送る場合，暗号化を行えば，電子メールの到達確認ができる。
ウ　インターネットを利用するには，利用者認証システムに登録する必要がある。
エ　社内電子メールシステムをインターネットで社外と接続しても，ファイアウォールを導入すれば，社内からの重要情報の流出は自動的に防止できる。

問96

セキュリティ技術に関する記述のうち、適切なものはどれか。

ア　地震や火災に対しては、フォールトトレラント方式のコンピュータによるシステムの二重化が有効である。
イ　データの物理的な盗聴や破壊に対しては、ディスクアレイシステムやファイアフォールが有効である。
ウ　伝送中のデータへの不正アクセスに対して、ＨＤＬＣプロトコルのＣＲＣ方式が有効である。
エ　メッセージの改ざんやなりすましによる不正アクセスに対しては、公開鍵暗号方式を応用したディジタル署名が有効である。

問97

公衆回線を利用しているコンピュータシステムで、セキュリティの面から適切な運用方法はどれか。

ア　あらかじめ定められたパスワードの変更を禁止する。
イ　接続要求があった場合、特定の電話番号にコールバックして接続する。
ウ　パスワードはユーザが確認できるように、ログイン時に端末に表示する。
エ　パスワードをあらかじめ定めた回数間違えて入力した場合、パスワードを通知する。

問98

ユーティリティプログラムの不正な実行によるデータの改ざんや破壊を防止する上で，効果的な管理手段として，最も適切なものはどれか。

ア　システムログの採取
イ　ソースプログラムと実行プログラムの比較
ウ　データのバックアップ
エ　ファイルへのアクセス権限の設定

問99

ユーザＩＤの管理について、最も適切なものはどれか。

ア　同じプロジェクトに参加している利用者は、みな同じユーザＩＤを用いる。
イ　複数のユーザＩＤをもつ利用者は、すべてのＩＤに対して同じパスワードを設定する。
ウ　ユーザＩＤに権限を設定する場合は、必要最小限なものにする。
エ　ユーザＩＤの抹消は、廃止の届出後、十分な期間をおいてから行う。

問100

あるコンピュータのログイン時に入力するパスワードの文字数は５文字である。英字の大文字２６字と数字が使えるものとする。一つのパスワードが使用できるかどうかを試みるのに０．５秒かかるとした場合、すべてのパスワードの組合せを試すためにはどの程度の期間を必要とするか。

ア　１０日　　イ　１０週間　　ウ　６か月　　エ　１年

問101

データベースの不正利用を防止する方法として有効なものはどれか。

ア　アクセス権の設定　　イ　一貫性維持の制御
ウ　データのカプセル化　　エ　ファイルの二重化

問102

利用者認証に用いられるＩＣカードの適切な運用はどれか。

ア　ＩＣカードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通なＰＩＮを設定する。
イ　ＩＣカードの表面に刻印してある数字情報を組み合わせて，ＰＩＮを設定する。
ウ　ＩＣカード紛失時には，新たなＩＣカードを発行し，ＰＩＮを設定した後で，紛失したＩＣカードの失効処理を行う。
エ　ＩＣカードを配送する場合には，ＰＩＮを同封せず，別経路で利用者に知らせる。

問103

パスワードに使用する文字の種類をＭ，パスワードのけた数をｎとするとき，設定できるパスワードの個数Ｐを求める数式はどれか。

ア　$P=M^n$　　イ　$P=\dfrac{M!}{(M-n)!}$

ウ　$P=\{\dfrac{M!}{(M-n)!}\}\times\dfrac{1}{n!}$　　エ　$P=\{\dfrac{(M+n-1)!}{(M-1)!}\}\times\dfrac{1}{n!}$

問104

ＩＣカードとＰＩＮを用いた利用者認証における適切な運用はどれか。

ア　ＩＣカードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通のＰＩＮを設定する。
イ　ＩＣカードの表面に刻印してある数字情報を組み合わせて，ＰＩＮを設定する。
ウ　ＩＣカード紛失時には，新たなＩＣカードを発行し，ＰＩＮを再設定した後で，紛失したＩＣカードの失効処理を行う。
エ　ＩＣカードを配送する場合には，ＰＩＮを同封せず，別経路で利用者に知らせる。

問105

コンピュータシステムにおけるパスワード運用管理方法として、適切なものはどれか。

ア　トラブル処理を迅速化するために、ユーザＩＤとパスワードの一覧表を作成し、管理者しか分からないように隠す。
イ　利用者が自分のパスワードをいつでも自由に変更できるようにする。
ウ　利用者管理作業を簡素化するために、現在使用されていないユーザＩＤとパスワードを再利用する。
エ　利用者登録申請書が届く前に、新任者の人事異動速報を見てユーザＩＤと仮のパスワードを登録する。

問106

認証局（ＣＡ）の役割に関する記述のうち、適切なものはどれか。

ア　相手の担保能力を確認する。
イ　公開鍵暗号方式を用いて、データの暗号化を行う。
ウ　転送すべきデータのダイジェスト版を作成し、電子署名として提供する。
エ　ユーザの公開鍵の正当性を保証する証明書を発行する。

問107

パスワードを用いて利用者を認証する方法のうち，適切なものはどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
イ　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。
ウ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。

問108

ＰＫＩ（公開鍵基盤）の認証局が果たす役割はどれか。

ア　共通鍵を生成する。
イ　公開鍵を利用しデータの暗号化を行う。
ウ　失効したディジタル証明書の一覧を発行する。
エ　データが改ざんされていないことを検証する。

問109

入力パスワードと登録パスワードを用いて利用者を認証する方法において，パスワードファイルへの不正アクセスによる登録パスワードの盗用防止策はどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して参照した登録パスワードと入力パスワードを比較する。
イ　パスワードをそのまま登録したファイルを圧縮しておき，認証時に復元して，入力されたパスワードと比較する。
ウ　パスワードをそのまま登録しておき，認証時に入力されたパスワードと登録内容をともにハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

問110

送信者からメール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者がメール本文から求めたハッシュ値とを比較して実現できることはどれか。ここで，送信者からのハッシュ値は保護されているものとする。

ア　改ざんの有無の検出
イ　盗聴の防止
ウ　なりすましの防止
エ　メールの送達の確認

問111

公開かぎ暗号方式を採用した電子商取引において，取引当事者から独立した第三者機関である認証局（ＣＡ）が作成するものはどれか。

ア　取引当事者の公開かぎに対する電子証明書
イ　取引当事者のディジタル署名
ウ　取引当事者のパスワード
エ　取引当事者の秘密かぎに対する電子証明書

問112

二つの通信主体X，Y間で，次の手順で情報をやり取りしたときの認証に関する記述のうち，正しいものはどれか。

手順１：Yは任意の情報を織り込んだ文字列(チャレンジコード)をXへ送信する。

手順２：Xは，あらかじめX，Y間で定めたルールに基づき，受け取った文字列から新たな文字列(レスポンスコード)を生成しYへ返送する。

手順３：Yは返送されてきたレスポンスコードが正しいことを確認する。

ア　XがYを認証し，YがXを認証する。

イ　XがYを認証する。

ウ　Xがチャレンジコードを認証する。

エ　YがXを認証する。

問113

ＥＣ(電子商取引)における認証の役割に関する記述のうち、最も適切なものはどれか。

ア　受信側で、送信者の正当性を証明することである。

イ　送信側及び受信側で、トランザクションの内容が正しいことを証明することである。

ウ　第三者機関によって、トランザクションの内容が正しいことを証明することである。

エ　第三者機関によって、取引相手の正当性を証明することである。

問114

手順に示す処理を実施したとき，メッセージの改ざんの検知の他に，受信者Bがセキュリティ上できることはどれか。

〔手順〕

送信者Aの処理

（１）　メッセージから，ハッシュ関数を使ってダイジェストを生成する。

（２）　秘密に保持していた自分の署名生成鍵を用いて，（１）で生成したダイジェストからメッセージの署名を生成する。

（３）　メッセージと，（２）で生成したデータを受信者Bに送信する。

受信者Bの処理

（４）　受信したメッセージから，ハッシュ関数を使ってダイジェストを生成する。

（５）　受信したデータ，（４）で生成したダイジェスト及び送信者Aの署名検証鍵を用いて，署名を検証する。

ア　メッセージが送信者Aからのものであることの確認

イ　メッセージの改ざん部位の特定

ウ　メッセージの盗聴の検知

エ　メッセージの漏えいの防止

問115

メッセージ認証符号におけるメッセージダイジェストの利用目的はどれか。

ア　メッセージが改ざんされていないことを確認する。
イ　メッセージの暗号化方式を確認する。
ウ　メッセージの概要を確認する。
エ　メッセージの秘匿性を確保する。

問116

セキュリティプロトコルＳＳＬの特徴はどれか。

ア　ＳＳＬはＷｅｂサーバだけで使用されるセキュリティ対策用のプロトコルで，ネットワーク層に位置するものである。
イ　ＳＳＬを利用するＷｅｂサーバでは，そのＦＱＤＮをディジタル証明書に組み込む。
ウ　個人認証用のディジタル証明書は，ＰＣごとに固有のものを作成する必要がある。
エ　日本国内では，政府機関に限り１２８ビットの共通鍵長のディジタル証明書を取得申請できる。

問117

インターネット経由で、WWWサーバにアクセスして商取引をしたい。このWWWサーバの提供者が、商取引上、信頼できる相手であるかどうかを判断するのに有効な情報を与えてくれる仕組みはどれか。

ア　ＩＰパケットフィルタリング　　イ　ＩＰポート番号
ウ　ＳＳＬ　　エ　クッキーヘッダ

問118

ＳＳＬ／ＴＬＳを利用することによって実現できるものはどれか。

ア　クライアントサーバ間の通信の処理時間を短縮する。
イ　クライアントサーバ間の通信を暗号化する。
ウ　ブラウザとＷｅｂサーバの通信の証跡を確保する。
エ　メールソフトからＷｅｂサーバへのＳＭＴＰ接続を可能にする。

問119

無線ＬＡＮやＶＰＮ接続などで利用され，利用者を認証するためのシステムはどれか。

ア　ＤＥＳ　　イ　ＤＮＳ　　ウ　ＩＤＳ　　エ　RADIUS

問120

バイオメトリクス認証システムの判定しきい値を変化させるとき，ＦＲＲ(本人拒否率)とＦＡＲ(他人受入率)との関係はどれか。

ア　ＦＲＲとＦＡＲは独立している。
イ　ＦＲＲを減少させると，ＦＡＲは減少する。
ウ　ＦＲＲを減少させると，ＦＡＲは増大する。
エ　ＦＲＲを増大させると，ＦＡＲは増大する。

問121

生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　システムを誤作動させるデータを無害化する機能をもつライブラリを使用する。
イ　パターンファイルの頻繁な更新だけでなく，ヒューリスティックなど別の手段を組み合わせる。
ウ　本人のディジタル証明書を信頼できる第三者機関に発行してもらう。
エ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

問122

バイオメトリクス認証には身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

ア　血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。
イ　署名するときの速度や筆圧から特徴を抽出して認証する。
ウ　どう孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。
エ　隆線によって形作られる紋様からマニューシヤと呼ばれる特徴点を抽出して認証する。

問123

ＨＴＴＰＳを用いて実現できるものはどれか。

ア　Ｗｅｂサーバ上のファイルの改ざん検知
イ　クライアント上のウイルス検査
ウ　クライアントに対する侵入検知
エ　電子証明書によるサーバ認証

問124

画像などのディジタルコンテンツが，不正にコピーされて転売されたものであるかを判別できる対策はどれか。

ア　タイムスタンプ　　イ　電子透かし　　ウ　電子保存　　エ　配達証明

問125

ＨＴＴＰＳ(HTTP over SSL/TLS)の機能を用いて実現できるものはどれか。

ア　ＳＱＬインジエクションによるＷｅｂサーバへの攻撃を防ぐ。
イ　ＴＣＰポート８０番と４４３番以外の通信を遮断する。
ウ　Ｗｅｂサーバとブラウザの間の通信を暗号化する。
エ　Ｗｅｂサーバへの不正なアクセスをネットワーク層でのパケットフィルタリングによって制限する。

問126

ネットワークを通してデータ交換を行う場合，ユーザを認証する方法として，適切なものはどれか。

ア　受信データが改ざんされていないかどうかを調べる。
イ　送信データを暗号化する。
ウ　データを発信しているコンピュータを特定する。
エ　パスワードの一致を調べる。

問127

Ｗｅｂサーバのコンテンツの改ざんを検知する方法のうち，最も有効なものはどれか。

ア　Ｗｅｂサーバのコンテンツの各ファイルの更新日を保管しておき，定期的に各ファイルの更新日と比較する。
イ　Ｗｅｂサーバのコンテンツの各ファイルのハッシュ値を保管しておき，定期的に各ファイルから生成したハッシュ値と比較する。
ウ　Ｗｅｂサーバのメモリ使用率を定期的に確認し，バッファオーバフローが発生していないことを確認する。
エ　Ｗｅｂサーバへの通信を監視し，ＨＴＴＰ，ＨＴＴＰＳ以外の通信がないことを確認する。

問128

ファイアウォールのパケットフィルタリング機能に関する記述のうち，適切なものはどれか。

ア　インターネットから受け取ったパケットに改ざんがある場合は修正し，改ざんが修正できない場合には，ログを取って内部ネットワークへの通過を阻止する。
イ　インターネットから受け取ったパケットのヘッダ部分及びデータ部分に，改ざんがあるかどうかをチェックし，改ざんがあった場合にはそのパケットを除去する。
ウ　動的に割り振られたＴＣＰポート番号をもったパケットを，受信側で固定値のＴＣＰポート番号をもったパケットに変更して，内部ネットワークへの通過を許可する。
エ　特定のＴＣＰポート番号をもったパケットだけに，インターネットから内部ネットワークへの通過を許可する。

問129

ディレクトリに，読取り，更新，配下のファイル作成のアクセス権を設定できるＯＳがある。この３種類のアクセス権は，それぞれに１ピットを使って許可，不許可を設定する。この３ピットを８進数表現０～７の数字で設定するとき，次の試行結果から考えて，適切な記述はどれか。

〔試行結果〕

① ０を設定したら，一切のアクセスができなくなってしまった。

② ３を設定したら，読取りと更新はできたが，作成ができなかった。

③ ７を設定したら，すべてのアクセスができるようになった。

ア ２を設定すると，読取りと作成ができる。

イ ４を設定すると，作成だけができる。

ウ ５を設定すると，更新だけができる。

エ ６を設定すると，読取りと更新ができる。

問130

利用者情報を管理するデータベース(利用者データベース)がある。利用者データベースを検索し，検索結果を表示するアプリケーションに与えるデータベースのアクセス権限として，セキュリティ管理上適切なものはどれか。ここで，権限の範囲は次のとおりとする。

〔権限の範囲〕

参照権限： 利用者データベースのレコードの参照が可能

更新権限： 利用者データベースへのレコードの登録，変更，削除が可能

管理者権限：利用者データベースのテーブルの参照，登録，変更，削除が可能

ア 管理者権限　　イ 更新権限

ウ 参照権限　　エ 参照権限と更新権限

問131

１台のファイアウォールによって，外部セグメント，ＤＭＺ，内部ネットワークの三つのセグメントに分割されたネットワークがある。このネットワークにおいて，Ｗｅｂサーバと，重要なデータをもつＤＢサーバから成るシステムを使って，利用者向けのサービスをインターネットに公開する場合，インターネットからの不正アクセスから重要なデータを保護するためのサーバの設置方法のうち，最も適切なものはどれか。ここで，ファイアウォールでは，外部セグメントとＤＭＺ間及びＤＭＺと内部ネットワーク間の通信は特定のプロトコルだけを許可し，外部セグメントと内部ネットワーク間の通信は許可しないものとする。

ア ＷｅｂサーバとＤＢサーバをＤＭＺに設置する。

イ ＷｅｂサーバとＤＢサーバを内部ネットワークに設置する。

ウ ＷｅｂサーバをＤＭＺに，ＤＢサーバを内部ネットワークに設置する。

エ Ｗｅｂサーバを外部セグメントに，ＤＢサーバをＤＭＺに設置する。

問132

パケットフィルタリング型ファイアウォールがルール一覧に基づいてパケットを制御する場合，パケットＡに対する制御はどれか。ここで，ファイアウォールでは，ルール一覧に示す番号の１から順にルールの適用判断を行い，一つのルールが適用されたときには残りのルールは適用しない。

〔ルール一覧〕

番号	送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号	動作
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注記　＊は任意のパターンを表す。

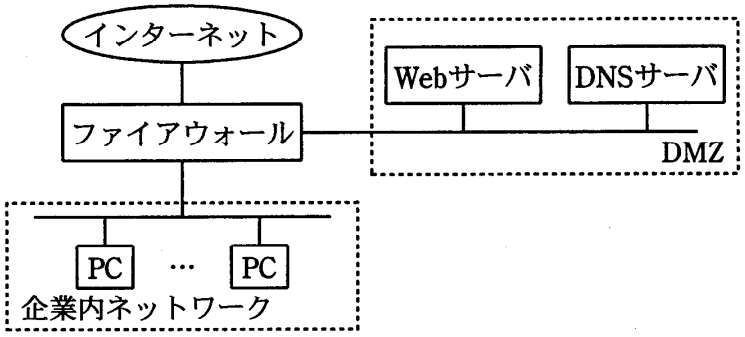
〔パケットA〕

送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号
10.1.2.3	10.2.3.4	TCP	2100	25

ア　番号１によって，通過を禁止する。
イ　番号２によって，通過を許可する。
ウ　番号３によって，通過を許可する。
エ　番号４によって，通過を禁止する。

問133

図に示すネットワーク構成で，Ｗｅｂページの閲覧だけを社外に提供する。攻撃を防止するためにファイアウォールのＩＰパケットフィルタリングを設定する場合，フィルタリングルールでインターネットからＤＭＺへのパケットの通過を禁止できないプロトコルはどれか。



ア　ＦＴＰ　　イ　ＨＴＴＰ
ウ　ＳＭＴＰ　　エ　ＳＮＭＰ

問134

複数の業務システムがある場合のアクセス管理の方法として，最も適切なものはどれか。

ア　業務の担当変更に迅速に対応するために，業務グループごとに共通の利用者ＩＤを使用する。
イ　人事異動が頻繁に発生する場合には，年初にまとめてアクセス権限の変更を行う。
ウ　新入社員の名簿に基づいて，あらかじめ全業務システムに全員の利用者登録を実施しておく。
エ　利用者の職位権限にかかわらず，業務システムごとに適切なアクセス権限の設定を行う。

問135

ＰＣへの侵入に成功したマルウェアがインターネット上の指令サーバと通信を行う場合に，宛先ポートとしてＴＣＰポート番号８０が多く使用される理由はどれか。

ア　ＤＮＳのゾーン転送に使用されるので，通信がファイアウォールで許可されている可能性が高い。
イ　ＷｅｂサイトのＨＴＴＰＳ通信での閲覧に使用されることから，侵入検知システムで検知される可能性が低い。
ウ　Ｗｅｂサイトの閲覧に使用されることから，通信がファイアウォールで許可されている可能性が高い。
エ　ドメイン名の名前解決に使用されるので，侵入検知システムで検知される可能性が低い。

問136

Ｗｅｂビーコンに該当するものはどれか。

ア　ＰＣとＷｅｂサーバ自体の両方に被害を及ぼす悪意のあるスクリプトによる不正な手口
イ　Ｗｅｂサイトからダウンロードされ ＰＣ上で画像ファイルを消去するウイルス
ウ　Ｗｅｂサイトで用いるアプリケーションプログラムに潜在する誤り
エ　Ｗｅｂページなどに小さい画像を埋め込み，利用者のアクセス動向などの情報を収集する仕組み

問137

認証デバイスに関する記述のうち，適切なものはどれか。

ア　ＩＥＥＥ８０２．１Ｘでは，ディジタル証明書や利用者ＩＤ，パスワードを格納するＵＳＢキーは，２００ｋバイト以上のメモリを内蔵することを規定している。
イ　安定した大容量の電力を必要とする高度な処理には，接触型ＩＣカードよりも非接触型ＩＣカードの方が適している。
ウ　虹彩認証では，成人には虹彩の経年変化がないので，認証デバイスでのパターン更新がほとんど不要である。
エ　静電容量方式の指紋認証デバイスでは，ＬＥＤ照明を設置した室内において正常に認証できなくなる可能性がある。

問138

暗号解読の手法のうち，ブルートフォース攻撃はどれか。

ア　与えられた１組の平文と暗号文に対し，総当たりで鍵を割り出す。
イ　暗号化関数の統計的な偏りを線形関数によって近似して解読する。
ウ　暗号化装置の動作を電磁波から解析することによって解読する。
エ　異なる二つの平文とそれぞれの暗号文の差分を観測して鍵を割り出す。

問139

標的型攻撃メールで利用されるソーシャルエンジニアリング手法に該当するものはどれか。

ア　件名に“未承諾広告＊”と記述する。
イ　件名や本文に，受信者の業務に関係がありそうな内容を記述する。
ウ　支払う必要がない料金を振り込ませるために，債権回収会社などを装い無差別に送信する。
エ　偽のホームページにアクセスさせるために，金融機関などを装い無差別に送信する。

問140

ＩＳＭＳ適合性評価制度の説明はどれか。

ア　ISO/IEC 15408 に基づき，ＩＴ関連製品のセキュリティ機能の適切性・確実性を評価する。
イ　JIS Q 15001に基づき，個人情報について適切な保護措置を講じる体制を整備している事業者などを認定する。
ウ　JIS Q 27001に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する。
エ　電子政府推奨暗号リストに基づき,暗号モジュールが適切に保護されていることを認証する。

問141

ネットワーク障害の原因を調べるために，ミラーポートを用意して，ＬＡＮアナライザを使用できるようにしておくときに留意することはどれか。

ア　ＬＡＮアナライザがパケットを破棄してしまうので，測定中は測定対象外のコンピュータの利用を制限しておく必要がある。
イ　ＬＡＮアナライザはネットワークを通過するパケットを表示できるので，盗聴などに悪用されないように注意する必要がある。
ウ　障害発生に備えて，ネットワーク利用者に対してＬＡＮアナライザの保管場所と使用方法を周知しておく必要がある。
エ　測定に当たって，ＬＡＮケーブルを一時的に切断する必要があるので，ネットワーク利用者に対して測定日を事前に知らせておく必要がある。

問142

ワームの検知方式の一つとして，検査対象のファイルからSHA-256を使ってハッシュ値を求め，既知のワーム検体ファイルのハッシュ値のデータベースと照合することによって，検知できるものはどれか。

ア　ワーム検体と同一のワーム
イ　ワーム検体と特徴あるコード列が同じワーム
ウ　ワーム検体とファイルサイズが同じワーム
エ　ワーム検体の亜種に当たるワーム

問143

２要素認証に該当するものはどれか。

ア　２本の指の指紋で認証する。
イ　虹彩とパスワードで認証する。
ウ　異なる２種類の特殊文字を混ぜたパスワードで認証する。
エ　異なる二つのパスワードで認証する。

問144

キーロガーの悪用例はどれか。

ア　通信を行う２者間の経路上に割り込み，両者が交換する情報を収集し，改ざんする。
イ　ネットバンキング利用時に，利用者が入力したパスワードを収集する。
ウ　プラウザでの動画閲覧時に，利用者の意図しない広告を勝手に表示する。
エ　プラウザの起動時に，利用者がインストールしていないツールバーを勝手に表示する。

問145

ディジタル署名における署名鍵の用い方と，ディジタル署名を行う目的のうち，適切なものはどれか。

ア　受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。
イ　送信者が固定文字列を付加したメッセージを署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。
ウ　送信者が署名鍵を使って署名を作成し，それをメッセージに付加することによって，受信者が送信者を確認できるようにする。
エ　送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。

問146

データベースで管理されるデータの暗号化に用いることができ，かつ，暗号化と復号とで同じ鍵を使用する暗号化方式はどれか。

ア　ＡＥＳ　　イ　ＰＫＩ　　ウ　ＲＳＡ　　エ　ＳＨＡ−２５６

問147

社員が利用するスマートフォンにディジタル証明書を導入しておくことによって，当該スマートフォンから社内システムへアクセスがあったときに，社内システム側で確認できるようになることはどれか。

ア　当該スマートフォンがウイルスに感染していないこと
イ　当該スマートフォンが社内システムへのアクセスを許可されたデバイスであること
ウ　当該スマートフォンのＯＳに最新のセキュリティパッチが適用済みであること
エ　当該スマートフォンのアプリケーションが最新であること

問148

Ｗｅｂサーバの検査におけるポートスキャナの利用目的はどれか。

ア　Ｗｅｂサーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する。
イ　Ｗｅｂサーバの利用者ＩＤの管理状況を運用者に確認して，情報セキュリティポリシとの相違を調べる。
ウ　Ｗｅｂサーバへのアクセス履歴を解析して，不正利用を検出する。
エ　正規の利用者ＩＤでログインし，Ｗｅｂサーバのコンテンツを直接確認して，コンテンツの脆弱性を検出する。

問149

ディジタルフォレンジックスでハッシュ値を利用する目的として，適切なものはどれか。

ア　一方向性関数によってパスワードを復元できないように変換して保存する。
イ　改変されたデータを，証拠となり得るように復元する。
ウ　証拠となり得るデータについて，原本と複製の同一性を証明する。
エ　パスワードの盗聴の有無を検証する。

問150

企業内ネットワークやサーバに侵入するために攻撃者が組み込むものはどれか。

ア　シンクライアントエージェント　　イ　ストリクトルーテイング
ウ　ディジタルフォレンジックス　　エ　バックドア

問151

社内ネットワークとインターネットの接続点にパケットフィルタリング型ファイアウォールを設置して，社内ネットワーク上のＰＣからインターネット上のＷｅｂサーバの８０番ポートにアクセスできるようにするとき，フィルタリングで許可するルールの適切な組合せはどれか。

ア

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	80	1024 以上

イ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	1024 以上	80

ウ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	80	1024 以上

エ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	1024 以上	80

問152

機密ファイルが格納されていて，正常に動作するＰＣの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策のうち，適切なものはどれか。

ア　異なる圧縮方式で，機密ファイルを複数回圧縮する。
イ　専用の消去ツールで，磁気ディスクのマスタブートレコードを複数回消去する。
ウ　特定のビット列で，磁気ディスクの全領域を複数回上書きする。
エ　ランダムな文字列で，機密ファイルのファイル名を複数回変更する。

問153

検索サイトの検索結果の上位に悪意のあるサイトが並ぶように細工する攻撃の名称はどれか。

ア　ＤＮＳキャツシュポイズニング　　イ　ＳＥＯポイズニング
ウ　クロスサイトスクリプティング　　エ　ソーシャルエンジニアリング

問154

ＳＱＬインジェクション攻撃の説明として，適切なものはどれか。

ア　Ｗｅｂアプリケーションのデータ操作言語の呼出し方に不備がある場合に，攻撃者が悪意をもって構成した文字列を入力することによって，データベースのデータの不正な取得，改ざん及び削除をする攻撃
イ　Ｗｅｂサイトに対して，他のサイトを介して大量のパケットを送り付け，そのネットワークトラフィックを異常に高めてサービスを提供不能にする攻撃
ウ　確保されているメモリ空間の下限又は上限を超えてデータの書込みと読出しを行うことによって，プログラムを異常終了させたリデータエリアに挿入された不正なコードを実行させたりする攻撃
エ　攻撃者が罠を仕掛けたＷｅｂページを利用者が閲覧し，当該ページ内のリンクをクリックしたときに，不正スクリプトを含む文字列が脆弱なＷｅｂサーバに送り込まれ，レスポンスに埋め込まれた不正スクリプトの実行によって，情報漏えいをもたらす攻撃

問155

Ｗｅｂシステムのパスワードを忘れたときの利用者認証において合い言葉を使用する場合，合い言葉が一致した後の処理のうち，セキュリティ上最も適切なものはどれか。

ア　あらかじめ登録された利用者のメールアドレス宛てに，現パスワードを送信する。
イ　あらかじめ登録された利用者のメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難なＵＲＬを送信する。
ウ　新たにメールアドレスを入力させ，そのメールアドレス宛てに，現パスワードを送信する。
エ　新たにメールアドレスを入力させ，そのメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難なＵＲＬを送信する。

問156

公開鍵暗号を利用した電子商取引において，認証局（ＣＡ）の役割はどれか。

ア　取引当事者間で共有する秘密鍵を管理する。
イ　取引当事者の公開鍵に対するディジタル証明書を発行する。
ウ　取引当事者のディジタル署名を管理する。
エ　取引当事者のパスワードを管理する。

問157

スパイウェアに該当するものはどれか。

ア　Ｗｅｂサイトへの不正な入力を排除するために，Ｗｅｂサイトの入力フォームの入力データから，ＨＴＭＬタグ，JavaScript，ＳＱＬ文などを検出し，それらを他の文字列に置き換えるプログラム
イ　サーバへの侵入口となり得る脆弱なポートを探すために，攻撃者のＰＣからサーバのＴＣＰポートに順番にアクセスするプログラム
ウ　利用者の意図に反してＰＣにインストールされ，利用者の個人情報やアクセス履歴などの情報を収集するプログラム
エ　利用者のパスワードを調べるために，サーバにアクセスし，辞書に載っている単語を総当たりで試すプログラム

問158

SaaS(Software as a Service)を利用するときの企業のセキュリティ管理についての記述のうち，適切なものはどれか。

ア　システム運用を行わずに済み，障害時の業務手順やバックアップについての検討が不要である。
イ　システムのアクセス管理を行わずに済み，パスワードの初期化の手続や複雑性の要件を満たすパスワードポリシの検討が不要である。
ウ　システムの構築を行わずに済み，アプリケーションソフトウェア開発に必要なセキュリティ要件の定義やシステムログの保存容量の設計が不要である。
エ　システムのセキュリティ管理を行わずに済み，情報セキュリティ管理規定の策定や管理担当者の設置が不要である。

問159

人間には読み取ることが可能でも，プログラムでは読み取ることが難しいという差異を利用して，ゆがめたり一部を隠したりした画像から文字を判読して入力させることによって，プログラムによる自動入力を排除するための技術はどれか。

ア　CAPTCHA　　イ　ＱＲコード
ウ　短縮ＵＲＬ　　エ　トラックバックping

問160

サーバにバックドアを作り，サーバ内での侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージはどれか。

ア　ＲＦＩＤ　　イ　rootkit
ウ　ＴＲＩＰ　　エ　webbeacon

問161

ＰＫＩにおける認証局が，信頼できる第三者機関として果たす役割はどれか。

ア　利用者からの要求に対して正確な時刻を返答し，時刻合わせを可能にする。
イ　利用者から要求された電子メールの本文に対して，ディジタル署名を付与する。
ウ　利用者やサーバの公開鍵を証明するディジタル証明書を発行する。
エ　利用者やサーバの秘密鍵を証明するディジタル証明書を発行する。

問162

ＷＡＦの説明はどれか。

ア　Ｗｅｂサイトに対するアクセス内容を監視し，攻撃とみなされるパターンを検知したときに当該アクセスを遮断する。
イ　Ｗｉ－Ｆｉアライアンスが認定した無線ＬＡＮの暗号化方式の規格であり，ＡＥＳ暗号に対応している。
ウ　様々なシステムの動作ログを一元的に蓄積，管理し，セキュリティ上の脅威となる事象をいち早く検知，分析する。
エ　ファイアウォール機能を有し，ウイルス対策，侵入検知などを連携させ，複数のセキュリティ機能を統合的に管理する。

問163

ウイルス検出におけるビヘイビア法に分類されるものはどれか。

ア　あらかじめ検査対象に付加された，ウイルスに感染していないことを保証する情報と，検査対象から算出した情報とを比較する。
イ　検査対象と安全な場所に保管してあるその原本とを比較する。
ウ　検査対象のハッシュ値と既知のウイルスファイルのハッシュ値とを比較する。
エ　検査対象をメモリ上の仮想環境下で実行して，その挙動を監視する。

問164

攻撃者が用意したサーバXのＩＰアドレスが，Ａ社ＷｅｂサーバのＦＱＤＮに対応するＩＰアドレスとして，Ｂ社ＤＮＳキャッシュサーバに記憶された。この攻撃によって，意図せずサーバXに誘導されてしまう利用者はどれか。ここで，Ａ社，Ｂ社の各従業員は自社のＤＮＳキャッシュサーバを利用して名前解決を行う。

ア　Ａ社ＷｅｂサーバにアクセスしようとするＡ社従業員
イ　Ａ社ＷｅｂサーバにアクセスしようとするＢ社従業員
ウ　Ｂ社ＷｅｂサーバにアクセスしようとするＡ社従業員
エ　Ｂ社ＷｅｂサーバにアクセスしようとするＢ社従業員

問165

別のサービスやシステムから流出したアカウント認証情報を用いて，アカウント認証情報を使い回している利用者のアカウントを乗っ取る攻撃はどれか。

ア　パスワードリスト攻撃　　イ　ブルートフォース攻撃
ウ　リバースブルートフォース攻撃　　エ　レインボー攻撃

問166

共通鍵暗号の鍵を見つけ出そうとする，ブルートフォース攻撃に該当するものはどれか。

ア　一組みの平文と暗号文が与えられたとき，全ての鍵候補を一つずつ試して鍵を見つけ出す。
イ　平文と暗号文と鍵の関係を表す代数式を手掛かりにして鍵を見つけ出す。
ウ　平文の一部分の情報と，暗号文の一部分の情報との間の統計的相関を手掛かりにして鍵を見つけ出す。
エ　平文を一定量変化させたときの暗号文の変化から鍵を見つけ出す。

問167

経済産業省とＩＰＡが策定した”サイバーセキュリティ経営ガイドライン（Ｖｅｒ１．１）”が，自社のセキュリティ対策に加えて，実施状況を確認すべきとしている対策はどれか。

ア　自社が提供する商品及びサービスの個人利用者が行うセキュリティ対策
イ　自社に出資している株主が行うセキュリティ対策
ウ　自社のサプライチェーンのビジネスパートナが行うセキュリティ対策
エ　自社の事業所近隣の地域社会が行うセキュリティ対策

問168

情報セキュリティにおけるタイムスタンプサービスの説明はどれか。

ア　公式の記録において使われる全世界共通の日時情報を，暗号化通信を用いて安全に表示するＷｅｂサービス
イ　指紋，声紋，静脈パターン，網膜，虹彩などの生体情報を，認証システムに登録した日時を用いて認証するサービス
ウ　電子データが，ある日時に確かに存在していたこと，及びその日時以降に改ざんされていないことを証明するサービス
エ　ネットワーク上のＰＣやサーバの時計を合わせるための日時情報を途中で改ざんされないように通知するサービス

問169

公開鍵暗号方式の暗号アルゴリズムはどれか。

ア　ＡＥＳ　　イ　KCipher-2　　ウ　ＲＳＡ　　エ　ＳＨＡ－２５６

問170

ポットネットにおいてＣ＆Ｃサーバが果たす役割はどれか。

ア　遠隔操作が可能なマルウェアに，情報収集及び攻撃活動を指示する。
イ　電子商取引事業者などに，偽のディジタル証明書の発行を命令する。
ウ　不正なＷｅｂコンテンツのテキスト，画像及びレイアウト情報を一元的に管理する。
エ　踏み台となる複数のサーバからの通信を制御し遮断する。

問171

マルウェアについて，トロイの木馬とワームを比較したとき，ワームの特徴はどれか。

ア　勝手にファイルを暗号化して正常に読めなくする。
イ　単独のプログラムとして不正な動作を行う。
ウ　特定の条件になるまで活動をせずに待機する。
エ　ネットワークやリムーバブルメディアを媒介として自ら感染を広げる。

問172

リスクアセスメントを構成するプロセスの組合せはどれか。

ア　リスク特定，リスク評価，リスク受容
イ　リスク特定，リスク分析，リスク評価
ウ　リスク分析，リスク対応，リスク受容
エ　リスク分析，リスク評価，リスク対応

問173

ＣＳＩＲＴの説明として，適切なものはどれか。

ア　ＩＰアドレスの割当て方針の決定，ＤＮＳルートサーバの運用監視，ＤＮＳ管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業内・組織内や政府機関に設置され，情報セキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもつ者や組織の総称である。

問174

電子メールの送信時に，送信者を送信側のメールサーバで認証するためのものはどれか。

ア　ＡＰＯＰ　　イ　ＰＯＰ３Ｓ　　ウ　Ｓ／ＭＩＭＥ　　エ　SMTP-AUTH

問175

ドライブバイダウンロード攻撃に該当するものはどれか。

ア　ＰＣ内のマルウェアを遠隔操作して，ＰＣのハードディスクドライブを丸ごと暗号化する。
イ　外部ネットワークからファイアウォールの設定の誤りを突いて侵入し，内部ネットワークにあるサーバのシステムドライブにルートキットを仕掛ける。
ウ　公開Ｗｅｂサイトにおいて，スクリプトをＷｅｂページ中の入力フィールドに入力し，Ｗｅｂサーバがアクセスするデータベース内のデータを不正にダウンロードする。
エ　利用者が公開Ｗｅｂサイトを閲覧したときに，その利用者の意図にかかわらず，ＰＣにマルウェアをダウンロードさせて感染させる。

問176

Ａさんがｂさんの公開鍵で暗号化した電子メールを，ＢさんとＣさんに送信した結果のうち，適切なものはどれか。ここで，Ａさん，Ｂさん，Ｃさんのそれぞれの公開鍵は３人全員がもち，それぞれの秘密鍵は本人だけがもっているものとする。

ア　暗号化された電子メールを，Ｂさんだけが，Ａさんの公開鍵で復号できる。
イ　暗号化された電子メールを，Ｂさんだけが，自身の秘密鍵で復号できる。
ウ　暗号化された電子メールを，Ｂさんも，Ｃさんも，Ｂさんの公開鍵で復号できる。
エ　暗号化された電子メールを，Ｂさんも，Ｃさんも，自身の秘密鍵で復号できる。

問177

JISQ27000:2014（情報セキュリティマネジメントシステム―用語）において，“エンティティは，それが主張するとおりのものであるという特性”と定義されているものはどれか。

ア　真正性　　イ　信頼性　　ウ　責任追跡性　　エ　否認防止

問178

攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

ア　後処理の段階において，システムログに攻撃の痕跡が残っていないかどうかを調査する。
イ　権限取得の段階において，権限を奪取できそうなアカウントがあるかどうかを調査する。
ウ　事前調査の段階において，攻撃できそうなサービスがあるかどうかを調査する。
エ　不正実行の段階において，攻撃者にとって有益な利用者情報があるかどうかを調査する。

問179

社内ネットワークとインターネットの接続点に，ステートフルインスペクション機能をもたない，静的なパケットフィルタリング型のファイアウォールを設置している。このネットワーク構成において，社内のＰＣからインターネット上のＳＭＴＰサーバに電子メールを送信できるようにするとき，ファイアウォールで通過を許可するＴＣＰパケットのポート番号の組合せはどれか。ここで，ＳＭＴＰ通信には，デフォルトのポート番号を使うものとする。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	PC	SMTP サーバ	25	1024 以上
	SMTP サーバ	PC	1024 以上	25
イ	PC	SMTP サーバ	110	1024 以上
	SMTP サーバ	PC	1024 以上	110
ウ	PC	SMTP サーバ	1024 以上	25
	SMTP サーバ	PC	25	1024 以上
エ	PC	SMTP サーバ	1024 以上	110
	SMTP サーバ	PC	110	1024 以上

問180

セキュリティバイデザインの説明はどれか。

ア　開発済みのシステムに対して，第三者の情報セキュリティ専門家が，脆弱性診断を行い，システムの品質及びセキュリティを高めることである。

イ　開発済みのシステムに対して，リスクアセスメントを行い，リスクアセスメント結果に基づいてシステムを改修することである。

ウ　システムの運用において，第三者による監査結果を基にシステムを改修することである。

エ　システムの企画・設計段階からセキュリティを確保する方策のことである。

問181

生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　本人のディジタル証明書を，信頼できる第三者機関に発行してもらう。

イ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

ウ　マルウェア定義ファイルの更新が頻繁な製品を利用することによって，本人を誤って拒否する確率の低下を防ぐ。

エ　容易に推測できないような知識量と本人が覚えられる知識量とのバランスが，認証に必要な知識量の設定として重要となる。

問182

ＳＰＦ(Sender Policy Framework)の仕組みはどれか。

ア　電子メールを受信するサーバが，電子メールに付与されているディジタル署名を使って，送信元ドメインの詐称がないことを確認する。

イ　電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバのＩＰアドレスから，ドメインの詐称がないことを確認する。

ウ　電子メールを送信するサーバが，送信する電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。

エ　電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。