gzn030401 「セキュリティとリスク管理」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

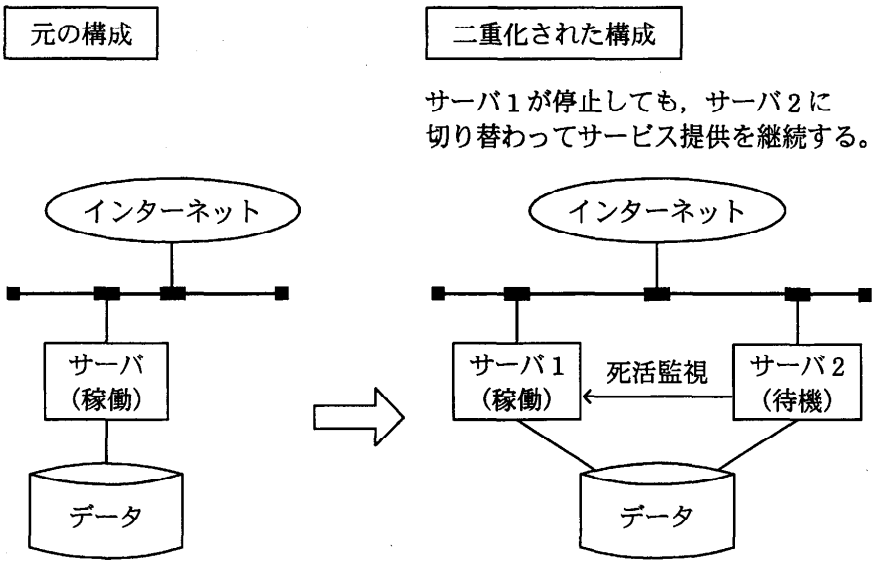
問48

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49

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

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55

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56

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57

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58

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59

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60

ディジタルフォレンジックスでハッジ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61

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62

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63

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64

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キャッシュポイズニング　　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65

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66

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67

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68

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　検査対象のハッジュ値と既知のウイルスファイルのハッジュ値とを比較する。
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69

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70

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71

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72

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73

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74

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75

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76

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77

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78

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79

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80

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81

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。