令和6年度、情報セキュリティマネジメント試験、科目A、B公開問題聞き流し動画

注意。IPAで公開されているのは、60問のうち15問だけとなります。

問１。じすきゅー31000、2019、リスクマネジメント、指針における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

せいかいわ。イ。リスク特定、リスク分析、リスク評価です

問2。情報の取扱基準の中で、社外秘情報の持出しを禁じ、周知した上で、従業員に情報を不正に持ち出された場合に、社外秘情報とは知らなかった、という言い訳をさせないことが目的のひとつになっている対策はどれか？。。

ア。権限がない従業員が文書にアクセスできないようにするペーパレス化。。。

イ。従業員との信頼関係の維持を目的にした職場環境の整備。。。

ウ。従業員に対する電子メールの外部送信データ量の制限。。。

エ。情報の管理レベルについてのラベル付け

せいかいわ。エ。情報の管理レベルについてのラベル付けです

問３。マルウェアの検出方法のうち、検査対象のプログラムを実行する必要があるものはどれか？。。

ア。コンペア法。。。イ。チェックサム法。。。

ウ。パターンマッチング法。。。エ。ビヘイビア法

せいかいわ。エ。ビヘイビア法です。

ビヘイビア法は、プログラムを実行し、振る舞い（ビヘイビア）から脅威を判断する方法です。この方法が「振る舞い検知」で、「動的ヒューリスティック」とも呼ばれます。

問４。サイバーキルチェーンに関する説明として、適切なものはどれか？。。

ア。委託先の情報セキュリティリスクが委託元にも影響するという考え方を基にしたリスク分析のこと。。。

イ。攻撃者がクライアントとサーバとの間の通信を中継し、あたかもクライアントとサーバが直接通信しているかのように装うことによって情報を盗聴するサイバー攻撃手法のこと。。。

ウ。攻撃者の視点から、攻撃の手口を偵察から目的の実行までの段階に分けたもの。。。

エ。取引データを複数の取引ごとにまとめ、それらを時系列につなげたチェーンに保存することによって取引データの改ざんを検知可能にしたもの

せいかいわ。ウ。攻撃者の視点から、攻撃の手口を偵察から目的の実行までの段階に分けたものです。。。なお、あわ、サプライチェーンの説明です。。。いわ、中間者攻撃、まんいんざみどるあたっくの説明です。。。えわ、ブロックチェーンの説明です

問５。リスクベース認証の説明として、適切なものはどれか？。。

ア。機器の画面に表示された点を正しい順序にひとふでがきでなぞった場合、認証が成功し、機器のロックが解除される。。。

イ。通常とは異なるIPアドレス、Webブラウザなどから認証要求があった場合に、追加の認証を行う。。。

ウ。認証局が、Webサイトへのサーバ証明書発行において、サーバ証明書に記載される組織のドメイン利用権、法的及び物理的実在性を確認する。。。

エ。ゆがんだ文字を含む画像を表示し、その文字が正しく入力された場合に認証が成功する。

せいかいわ。イ。通常とは異なるIPアドレス、Webブラウザなどから認証要求があった場合に、追加の認証を行うです。。。ちなみにあわ、パターン認証の説明です。。。うわ、SSLサーバ証明書の説明です。。。えわ。きゃぷちゃのせつめいです

問６。A社のWebサーバは、サーバ証明書を使ってTLS通信を行っている。PCからA社のWebサーバへのTLSを用いたアクセスにおいて、当該PCがサーバ証明書を入手したあとに、認証局の公開鍵を利用して行う動作はどれか？。。

ア。暗号化通信に利用する共通鍵を、認証局の公開鍵を使って復号する。。。

イ。暗号化通信に利用する共通鍵を生成し、認証局の公開鍵を使って暗号化する。。。

ウ。サーバ証明書の正当性を、認証局の公開鍵を使って検証する。。。

エ。利用者が入力して送付する秘匿データを、認証局の公開鍵を使って暗号化する。

せいかいわ。ウ。サーバ証明書の正当性を、認証局の公開鍵を使って検証するです

問７。個人情報保護法が保護の対象としている個人情報に関する記述のうち、適切なものはどれか？。。

ア。企業が管理している顧客に関する情報に限られる。。。

イ。個人が秘密にしているプライバシーに関する情報に限られる。。。

ウ。生存する個人に関する情報に限られる。。。

エ。日本国籍を有する個人に関する情報に限られる。

せいかいわ。ウ。生存する個人に関する情報に限られるです

問８。内部統制の基本的要素の一つである統制活動に該当するものはどれか？。。

ア。経営目的を達成するための経営方針及び経営戦略。。。

イ。個人情報保護に関する脅威と脆ぜい弱性の分析。。。

ウ。受注から出荷に至る業務プロセスに組み込まれた処理結果の検証。。。

エ。定期的に計画して実施する内部業務監査

せいかいわ。ウ。受注から出荷に至る業務プロセスに組み込まれた処理結果の検証です

問９。システムの信頼性指標としてレイシスがある。そのうちのAは可用性を表し、システムのサービス時間など、ある一定期間でのシステムの機能を維持する度合いを表している。このAを向上させるものはどれか？。。

ア。MTBFとMTTRをともに2倍にする。。。

イ。MTBFは変えず、MTTRを2倍にする。。。

ウ。MTBFを2倍にして、MTTRは変えない。。。

エ。MTBFを半分にして、MTTRは2倍にする。

せいかいわ。ウ。MTBFを2倍にして、MTTRは変えないです。。。

なお、MTBF、ミーンタイムビットウィーンフェイリュアーは平均故障間隔のことです。

故障までに稼働した時間の平均を示します。システムや機器の信頼性を示す指標のひとつです。

一方、MTTR、ミーンタイムトゥーリペアーは、平均修理時間のことです。故障から復旧までにかかった時間の平均を示します。システムや機器の保守性を示す指標の一つです。。。

これらのことから、信頼性の指標であるMTBFを二倍にし、保守性を示す指標であるMTTRを変えないことで、可用性を向上することができます。

問10。社内ネットワークからインターネットへのアクセスを中継し、Webコンテンツをキャッシュすることによってアクセスを高速にする仕組みで、セキュリティ確保にも利用されるものはどれか？。。

ア。DMZ。。。イ。IPマスカレード、なぷと。。。ウ。ファイアウォール。。。

エ。プロキシサーバ

せいかいわ。エ。プロキシサーバです

問11。全社的な推進体制でRPAを導入するときの留意点として、適切なものはどれか？。。

ア。各業務部門が連携して、RPAの対象業務に対して業務プロセス全体の可視化と業務プロセスの見直しを行った上で、RPAの導入を行う。。。

イ。業務フローが固定的で画面の変更が少ない業務よりも、業務フローの変更や画面の変更が多い業務から優先的に導入する。。。

ウ。情報システム部門や他部門との連携は行わずに、個々の業務部門が主導して、RPAツールの選定、ソフトウェアロボットの作成、活用及び運用を推進する。。。

エ。ルール化された処理や繰返し処理が多い業務よりも、例外処理が多い業務や条件が複雑な業務に対して、優先的にRPAの導入を行う。

せいかいわ。ア。各業務部門が連携して、RPAの対象業務に対して業務プロセス全体の可視化と業務プロセスの見直しを行った上で、RPAの導入を行うです

問12。特性要因図を説明したものはどれか？。。

ア。原因と結果の関連を魚の骨のような形態に整理して体系的にまとめ、結果に対してどのような原因が関連しているかを明確にする。。。

イ。時系列的に発生するデータのばらつきを折れ線グラフで表し、管理限界線を利用して客観的に管理する。。。

ウ。収集したデータを幾つかの区間に分類し、各区間に属するデータの個数を棒グラフとして描き、品質のばらつきを捉える。。。

エ。データを幾つかの項目に分類し、出現頻度の大きさの順に棒グラフとして並べ、累積和を折れ線グラフで描き、問題点を絞り込む。

せいかいわ。ア。原因と結果の関連を魚の骨のような形態に整理して体系的にまとめ、結果に対してどのような原因が関連しているかを明確にするです。。。特性要員図は、別名フィッシュボーンダイアグラムといい、魚の骨のような形が特徴です。。。なお、いわ、管理図の説明です。。。うわ、ヒストグラムの説明です。。。えわ、パレート図の説明です

問13。A社は、従業員100名の食品製造、販売会社である。A社では、営業部が取り扱う顧客情報をX社のサースであるX顧客管理サービス、以下、X サービスという、を利用して管理している。また、A社は、Xサービスの不正アクセス対策として、Xサービスへのログインは、A社の社内ネットワークからだけ許可しており、A社の社外からはできないように設定している。。

Xサービスに備わっている不正ログインを防止するための機能と、A社がXサービスに適用している現在の設定をひょう1に示す。。。

ひょう1。不正ログインを防止するための機能と現在の設定、抜粋。。

不正ログインを防止するための機能。

機能1。指定したIPアドレスからアクセスした場合だけ、ログインできるよう制限する。

現在の設定。有効、かっこ1。。

機能2。利用者IDとパスワードによって認証する。有効。。

機能3。英字、数字、記号の3種類全てを含む8文字以上のパスワードを強制する。有効。。

機能4。ワンタイムパスワードによって認証する。無効。。

機能5。ログイン画面にきゃぷちゃを表示し、回答させる。無効。。。

注意1。A社が使用しているグローバルIPアドレスを指定している。。。

A社では、昨今の社会情勢を鑑みて、営業部員を対象にテレワーク制度の導入を検討することにした。社外からもXサービスを利用できるようにしたい。また、社外から不正アクセスされるリスクを低減するために、利用者認証を強化したい。そこで、機能1から5の設定について、必要な変更をふたつ実施することにした。

設問。A社が実施することにした設定変更の組合せはどれか？。。解答群のうち、最も適切なものを選べ。。。

解答群。。

ア。有効から無効に変更する機能、機能1。無効から有効に変更する機能。機能4。。。

イ。有効から無効に変更する機能、機能1。無効から有効に変更する機能。機能5。。。

ウ。有効から無効に変更する機能、機能2。無効から有効に変更する機能。機能4。。。

エ。有効から無効に変更する機能、機能2。無効から有効に変更する機能。機能5。。。

オ。有効から無効に変更する機能、機能3。無効から有効に変更する機能。機能4。。。

せいかいわ。ア。有効から無効に変更する機能、機能1。無効から有効に変更する機能。機能4です。。。

改めて設定内容を見ていきましょう。テレワーク制度を導入したいので、機能1の指定IPからのログイン制限は外さないといけないことは直ぐに分かります。機能2、3については認証方法、パスワードポリシーに関する内容なので、有効のままである必要があります。

機能4については、2段階認証の要素として必要なので有効にする必要があります。

機能5については、利便性が低くなるため適切ではありません。。

よって、正解はア。有効から無効に変更する機能、機能1。無効から有効に変更する機能。機能4となります

問14。A社は医療品の販売を行う従業員100名の企業である。営業部では、オンプレミスのデータベースに顧客情報を格納している。営業部では、図1に示すバックアップポリシーを順守している。。

図1。営業部におけるバックアップポリシー。。

1。データベースは毎週日曜日にフルバックアップを、それ以外の日は毎日の増分バックアップを毎日、別のテープメディアに取得する。。。

2。バックアップは1週間分保存する。。。

3。データベースの目標復旧時点、RPOは24時間とする。。。

4。バックアップからの目標復旧時間、RTOは6時間とする。。。

5。バックアップを保存しているテープメディア、以下、バックアップテープという、は鍵付きのキャビネットに保管する。。。

6。バックアップはシステムを停止せずに取得する。

先日、金曜日に営業部では、アプリケーションの不具合によってデータベースの内部構造の破損、以下、論理破損という、が生じたので、データベースを復旧する必要が生じた。しかし、火曜日のバックアップテープが物理的に破損していたので、データベースをバックアップポリシーどおりには復旧できなかった。。

そのため、営業部の情報セキュリティリーダーであるB課長は、論理破損が起き、かつ、バックアップテープが物理的に破損していたとしてもデータベースを復旧できるようにする再発防止策を検討し、効果の高いものを選んだ。

設問。B課長が選んだ再発防止策はどれか？。。解答群のうち、最も適切なものを選べ。。。

解答群。。

ア。DBMSをイアースじょうに構築したサーバで稼働させ、データベースもイアース上に格納する。。。

イ。データベースのレプリケーションを行って、データベースのコピーを確保する。。。

ウ。データベースを格納しているディスクをレイドファイブ構成にする。。。

エ。テープメディアに加え、NASにもバックアップを1週間分保存する。。。

オ。毎日1回システムを停止させ、フルバックアップを取得する。

せいかいわ。エ。テープメディアに加え、NASにもバックアップを1週間分保存するです

問15。A社は、飲食店へのコンサルティングを行う従業員50名の企業である。A社の全てのPCでは、マルウェア対策ソフト、以下、Xソフトという、が有効にされている。ある日、総務部の情報セキュリティリーダーであるC 課長は、部下のDさんから、次の連絡を受けた。。。

A社のPCのWebブラウザでWebサイトを閲覧していたところ、PCがマルウェアに感染しているとの警告画面、以下、警告画面という、が全画面に表示された。。

警告画面が表示されたあと何もPCの操作をせずに直ちにC課長に連絡をした。

C課長は、情報システム部に報告した。情報システム部はDさんのPCを確認し、数時間後、図1のとおり報告した。。。

図1、情報システム部からの報告。。

1。警告画面には、次が表示されていた。

Xソフトの製品のロゴ。。

マルウェアを削除するためのツールをインストールする指示。。

サポートが必要な場合の電話番号とチャットウィンドウ。。

2。念のため、Xソフトを使ってDさんのPCをスキャンしたが、マルウェアは検出されなかった。また、警告画面の表示は、Xソフトによるものではないことを確認した。。

3。昨今、類似した警告画面の事例の報告が日本国内で増えている。。。

A社では、警告画面が表示された場合の適切な対応について全従業員に周知することにした。

設問。周知すべきことはどれか？。。解答群のうち、最も適切なものを選べ。。。

解答群。

ア。警告画面に、急いで対応する必要があるとの表示がある場合は、直ちに警告画面に表示された指示に従ってツールをインストールすること及びその具体的方法。。。

イ。警告画面に表示された指示には従わずに、直ちにWebブラウザを終了すること及びその具体的方法。。。

ウ。警告画面に表示されたツールと競合しないように、Xソフトをアンインストールし、警告画面に表示された指示に従ってツールをインストールすること及びその具体的方法。。。

エ。警告画面に表示された電話番号に直ちに連絡し、サポートオペレーターの指示に従うこと。。。

オ。警告画面に表示されている、Xソフトの製品のロゴが、製品開発元のWebサイトに掲載されている正規の製品のロゴと同じである場合は、警告画面に表示された指示に従ってツールをインストールすること及びその具体的方法

せいかいわ。イ。警告画面に表示された指示には従わずに、直ちにWebブラウザを終了すること及びその具体的方法です。。。この選択肢以外は、フィッシング詐欺などにあう危険性があるため、実生活でも選ばないようにしてください