令和５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

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。情報セキュリティ管理基準、平成28年に関する記述のうち、適切なものはどれか？。。

ア。ガバナンス基準、管理策基準及びマネジメント基準のみっつの基準で構成されている。。

イ。じすきゅー27001、2014、情報セキュリティマネジメントシステム、要求事項及びじすきゅー27002、2014、情報セキュリティ管理策の実践のための規範との整合性をとっている。。

ウ。情報セキュリティ対策は、管理策基準に挙げられた管理策の中から選択することとしている。。

エ。トップマネジメントは、マネジメント基準”に挙げられている事項の中から、自組織に合致する事項を選択して実施することとしている。。

せいかいわ。イ。じすきゅー27001、2014、情報セキュリティマネジメントシステム、要求事項及びじすきゅー27002、2014、情報セキュリティ管理策の実践のための規範との整合性をとっている、です

問２。入室時と退室時にIDカードを用いて認証をおこない、入退室を管理する。このとき、 入室時の認証に用いられなかったIDカードでの退室を許可しない、又は退室時の認証に用いられなかったIDカードでの再入室を許可しないコントロールをおこなう仕組みはどれか？。。

ア。TPMOR、トゥーパーソンミニマムオキュパンシールール。。

イ。アンチパスバック。。

ウ。インターロックゲート。。

エ。パニックオープン。。

せいかいわ。イ。アンチパスバック、です

問３。デジタルフォレンジックスの説明はどれか？。。

ア。サイバー攻撃に関連する脅威情報を標準化された方法で記述し、その脅威情報をセキュリティ対策機器に提供すること。。

イ。受信メールに添付された実行ファイルを動作させたときに、不正な振る舞いがないかどうかをメールボックスへの保存前に確認すること。。

ウ。情報セキュリティインシデント発生時に、法的な証拠となるデータを収集し、保管し、調査分析すること。。

エ。内部ネットワークにおいて、通信データを盗聴されないように暗号化すること。。

せいかいわ。ウ。情報セキュリティインシデント発生時に、法的な証拠となるデータを収集し、保管し、調査分析すること、です

問４。暗号方式に関する記述のうち、適切なものはどれか？。。

ア。公開鍵暗号方式、共通鍵暗号方式ともに、大きな合成数の素因数分解が困難であることが安全性の根拠である。。

イ。公開鍵暗号方式では原則としてセッションごとに異なる鍵を利用するが、共通鍵暗号方式では一度生成した鍵を複数のセッションに繰り返し利用する。。

ウ。公開鍵暗号方式は仕様が標準化されているが、共通鍵暗号方式はベンダーによる独自の仕様で実装されることが一般的である。。

エ。大量のデータを短い時間で暗号化する場合には、公開鍵暗号方式よりも共通鍵暗号方式が適している。

せいかいわ。エ。大量のデータを短い時間で暗号化する場合には、公開鍵暗号方式よりも共通鍵暗号方式が適している、です

問５。セキュアハッシュ関数しゃーにーこーろくを用いてファイルA及びファイルBのハッシュ値を算出すると、どちらも全く同じ次に示すハッシュ値えぬ、16進数で示すと64桁となった。この結果から考えられることとして、適切なものはどれか？。。

ア。ファイルAとファイルBの各内容を変更せずに再度ハッシュ値を算出すると、ファイルAとファイルBのハッシュ値が異なる。。

イ。ファイルAとファイルBのハッシュ値えぬのデータ量は64バイトである。。

ウ。ファイルAとファイルBを連結させたファイルCのハッシュ値の桁数は16進数で示すと128桁である。。

エ。ファイルAの内容とファイルBの内容は同じである。

せいかいわ。エ。ファイルAの内容とファイルBの内容は同じである、です

問６。迷惑メール対策のSPF、センダーポリシーフレームワークの仕組みはどれか？。。

ア。送信側ドメインの管理者が、正規の送信側メールサーバのIPアドレスをDNSに登録し、受信側メールサーバでそれを参照して、IPアドレスの判定を行う。。

イ。送信側メールサーバでメッセージにデジタル署名を施し、受信側メールサーバでそのデジタル署名を検証する。。

ウ。第三者によって提供されている、スパムメールの送信元IPアドレスのデータベースを参照して、スパムメールの判定を行う。。

エ。ファイアウォールを通過した要求パケットに対する応答パケットかどうかを判断して、動的に迷惑メールの通信を制御する。

せいかいわ。ア。送信側ドメインの管理者が、正規の送信側メールサーバのIPアドレスをDNSに登録し、受信側メールサーバでそれを参照して、IPアドレスの判定を行う、です。。。

なお、い、わ、でぃーきむのこと。う、わ、DNSブラックリストのこと。え、わ、ダイナミックパケットフィルタリングのことです

問７。Webアプリケーションにおけるセキュリティ上の脅威とその対策に関する記述のう ち、適切なものはどれか？。。

ア。OSコマンドインジェクションを防ぐために、Webアプリケーションが発行するセッションIDに推測困難な乱数を使用する。。

イ。SQLインジェクションを防ぐために、Webアプリケーション内でデータベースへの問合せを作成する際にプレースホルダを使用する。。

ウ。クロスサイトスクリプティングを防ぐために、Webサーバ内のファイルを外部から直接参照できないようにする。。

エ。セッションハイジャックを防ぐために、Webアプリケーションからシェルを起動できないようにする。

せいかいわ。イ。SQLインジェクションを防ぐために、Webアプリケーション内でデータベースへの問合せを作成する際にプレースホルダを使用する、です

問８。電子署名法に関する記述のうち、適切なものはどれか？。。

ア。電子署名には、電磁的記録ではなく、かつ、コンピュータで処理できないものも含まれる。。

イ。電子署名には、民事訴訟法における押印と同様の効力が認められる。。

ウ。電子署名の認証業務を行うことができるのは、政府が運営する認証局に限られる。。

エ。電子署名は共通鍵暗号技術によるものに限られる。

せいかいわ。イ。電子署名には、民事訴訟法における押印と同様の効力が認められる、です

問９。情報システムのインシデント管理に対する監査で判明した状況のうち、監査にんが、指摘事項として監査報告書に記載すべきものはどれか？。。

ア。インシデント対応手順が作成され、関係者への周知が図られている。。

イ。インシデントによってデータベースが被害を受けた場合の影響を最小にするために、規程に従ってデータのバックアップをとっている。。

ウ。インシデントの種類や発生箇所、影響度合いに関係なく、連絡、報告ルートが共通になっている。。

エ。全てのインシデントについて、インシデント記録を残し、責任者の承認を得ることが定められている。

せいかいわ。ウ。インシデントの種類や発生箇所、影響度合いに関係なく、連絡、報告ルートが共通になっている、です

問10。HTTPのクッキーに関する記述のうち、適切なものはどれか？。。

ア。クッキーに含まれる情報はHTTPヘッダの一部として送信される。。

イ。クッキーに含まれる情報はWebサーバだけに保存される。。

ウ。クッキーに含まれる情報はWebブラウザが全て暗号化して送信する。

エ。クライアントがクッキーに含まれる情報の有効期限を設定する。

せいかいわ。ア。クッキーに含まれる情報はHTTPヘッダの一部として送信される、です

問11。BPMの説明はどれか?。。

ア。企業活動のしゅとなる生産、物流、販売、財務、人事などの業務の情報を一元管理することによって、経営資源の全体最適を実現する。。

イ。業務プロセスに分析、設計、実行、改善のマネジメントサイクルを取り入れ、業務プロセスの改善見直しや最適なプロセスへの統合を継続的に実施する。。

ウ。顧客データベースを基に、商品の販売から保守サービス、問合せやクレームへの対応など顧客に関する業務プロセスを一貫して管理する。。

エ。部品の供給から製品の販売までの一連の業務プロセスの情報をリアルタイムで交換することによって、在庫の削減とリードタイムの短縮を実現する。

せいかいわ。イ。業務プロセスに分析、設計、実行、改善のマネジメントサイクルを取り入れ、業務プロセスの改善見直しや最適なプロセスへの統合を継続的に実施する、です。。。

なお、BPMはビジネスプロセスマネージメントの略です。。。

また、あ、わ、ERP。う、わ、CRM。え、わ、SCMの説明となります。

問12。品質管理において、結果と原因との関連を整理して、魚の骨のような図にまとめたものはどれか？。。

ア。管理図。。イ。特性要因図。。ウ。パレート図。。エ。ヒストグラム

せいかいわ。イ。特性要因図、です。フィッシュボーンダイアグラムとも呼ばれ、フィッシュボーンは魚の骨という意味です。

問13。A社は、分析、計測機器などの販売及び機器を利用した試料の分析受託業務を行う分析機器メーカーである。A社では、図1の情報セキュリティリスクアセスメント手順に従い、年一度、情報セキュリティリスクアセスメントを行っている。

図1、情報セキュリティリスクアセスメント手順。

・情報資産の機密性、完全性、可用性の評価値は、それぞれぜろからにのさん段階とする。。

・情報資産の機密性、完全性、可用性の評価値の最大値を、その情報資産の重要度とする。。

・脅威及び脆ぜい弱性の評価値は、それぞれぜろからにのさん段階とする。。

・情報資産ごとに、様々な脅威に対するリスク値を算出し、その最大値を当該情報資産のリスク値として情報資産管理台帳に記載する。ここで、情報資産の脅威ごとのリスク値は、次の式によって算出する。。

リスク値イコール情報資産の重要度かける脅威の評価値かける脆弱性の評価値。。

・情報資産のリスク値のしきい値を5とする。。

・情報資産ごとのリスク値がしきい値以下であれば受容可能なリスクとする。

・情報資産ごとのリスク値がしきい値を超えた場合は、保有以外のリスク対応を行う。。

A社の情報セキュリティリーダーであるBさんは、年次の情報セキュリティリスクアセスメントを行い、結果を情報資産管理台帳に表1のとおり記載した。。

表1、A社の情報資産管理台帳、抜粋。。

情報資産。

いち。従業員の健康診断の情報。機密性の評価値、2。完全性の評価値、2。可用性の評価値、2。情報資産の重要度、省略。驚異の評価値、2。脆弱性の評価値、2。リスク値、省略。。

に。行動規範などの社内ルール。機密性の評価値、1。完全性の評価値、2。可用性の評価値、1。情報資産の重要度、省略。驚異の評価値、1。脆弱性の評価値、1。リスク値、省略。。

さん。自社Webサイトに掲載している会社情報。機密性の評価値、0。完全性の評価値、2。可用性の評価値、2。情報資産の重要度、省略。驚異の評価値、2。脆弱性の評価値、2。リスク値、省略。。

よん。分析結果の制度を向上させるために開発した技術。機密性の評価値、2。完全性の評価値、2。可用性の評価値、1。情報資産の重要度、省略。驚異の評価値、2。脆弱性の評価値、1。リスク値、省略。。

設問。表1ちゅうの各情報資産のうち、保有以外のリスク対応を行うべきものはどれか。該当するものだけを全て挙げた組合せを、解答群の中から選べ。

解答群。

ア。いち、に。。イ。いち、に、さん。。

ウ。いち、に、よん。。エ。いち、さん。。

オ。いち、さん、よん。。カ。いち、よん。。

キ。に、さん。。ク。に、さん、よん。。

ケ。に、よん。。コ。さん、よん

せいかいわ。エ。いち、さん、です。。。

情報資産の評価値は、情報資産の機密性、完全性、可用性の評価値の最大値なので、すべて2になります。リスク値わ、リスク値イコール情報資産の重要度かける脅威の評価値かける脆弱性の評価値で求められるので、それぞれこのようになります。情報資産のリスク値のしきい値を5とするとあるので、せいかいわ、え。いち、さん、となります。

問14。A社は旅行商品を販売しており、業務の中で顧客情報を取り扱っている。A社が保有する顧客情報は、A社のファイルサーバ1台に保存されている。ファイルサーバは、顧客情報を含むフォルダにある全てのデータを磁気テープに毎週土曜日にバックアップするよう設定されている。バックアップは2世代分が保存され、ファイルサーバの隣にあるキャビネットに保管されている。

A社では年に一度、情報セキュリティに関するリスクの見直しを実施している。情報セキュリティリーダーであるE主任は、A社のデータ保管に関するリスクを見直して図1にまとめた。

図1。A社のデータ保管に関するリスク、抜粋。

1。省略。。

2。省略。。

3。省略。。

4。バックアップ対象とするフォルダの設定ミスによって、データが復旧できなくなる。。

E主任は、図1の4のリスクを低減するための対策を検討し、効果が期待できるものを選んだ。。

設問。次の対策のうち、効果が期待できるものをふたつ挙げた組合せを、解答群の中から選べ。。

いち。週1回バックアップを取得する代わりに、毎日1回バックアップを取得して7世代分保存する。。

に。バックアップ後に、磁気テープ中のファイルのリストと、ファイルサーバのバックアップ対象ファイルのリストとを比較し、合致しているかを確認する。。

さん。バックアップ対象とするフォルダの設定を、必ずにめいで行うようにする。。

よん。バックアップ用の媒体を磁気テープから外付けハードディスクに変更する。。

ご。バックアップをふたくみ取得し、うち一組みを遠隔地に保管する。

解答群。

ア。いち、に。。イ。いち、さん。。ウ。いち、よん。。エ。いち、ご。。オ。に、さん。。

カ。に、よん。。キ。に、ご。。ク。さん、よん。。ケ。さん、ご。。コ。よん。ご

せいかいわ。オ。に。バックアップ後に、磁気テープ中のファイルのリストと、ファイルサーバのバックアップ対象ファイルのリストとを比較し、合致しているかを確認する。と、さん。バックアップ対象とするフォルダの設定を、必ずにめいで行うようにする。です

問15。消費者向けの化粧品販売を行うA社では、電子メール、以下、メールという、の送 受信にクラウドサービスプロバイダB社が提供するメールサービス、以下、Bサービスという、を利用している。A社が利用するBサービスのアカウントは、A社の情報システム部が管理している。

Bサービスでの認証。

Bサービスでの認証は、利用者IDとパスワードに加え、あらかじめ登録しておいたスマートフォンの認証アプリを利用した2要素認証である。入力された利用者IDとパスワードが正しかったときは、スマートフォンに承認のリクエストが来る。リクエストを一分以内に承認した場合は、Bサービスにログインできる。

社外のネットワークからの利用。

社外のネットワークから社内システム又はファイルサーバを利用する場合、従業員は貸与されたPCから社内ネットワークにVPN接続する。

PCでのマルウェア対策。

従業員に貸与されたPCには、マルウェア対策ソフトが導入されており、マルウェア定義ファイルを毎日16時に更新するように設定されている。マルウェア対策ソフトは、毎日17時に、各PCのマルウェア定義ファイルが更新されたかどうかをチェックし、更新されていない場合は情報システム部のセキュリティ担当者に更新されていないことをメールで知らせる。

メールに関する報告。

ある日の15時頃、販売促進部の情報セキュリティリーダーであるC課長は、在宅で勤務していた部下のDさんから、メールに関する報告を受けた。報告を図1に示す。

図1、Dさんからの報告。

・販売促進キャンペーンを委託しているE社のFさんから9時30分にメールが届いた。。

・Fさんとは直接会ったことがある。この数か月頻繁にやり取りもしていた。。

・そのメールは、これまでのメールに返信する形で作成されており、メールの本文には販売キャンペーンの内容やFさんがよく利用する挨拶文が記載されていた。。

・急ぎの対応を求める旨が記載されていたので、メールに添付されていたファイルを開いた。。

・メールの添付ファイルを開いた際、特に見慣れないエラーなどは発生せず、ファイルの内容も閲覧できた。。

・ファイルの内容を確認した後、返信した。。

・11時頃、Dさんのスマートフォンに、承認のリクエストが来たが、Bサービスにログインしようとしたタイミングではなかったので、リクエストを承認しなかった。。

・12時までと急いでいた割にその後の返信がなく不審に思ったので、14時50分にFさんに電話で確認したところ、今日はメールを送っていないと言われた。。

・現在までのところ、PCの処理速度が遅くなったり、見慣れないウィンドウが表示されたりするなどの不具合や不審な事象は発生していない。。

・現在PCは、インターネットには接続しているが、社内ネットワークへのVPN接続は切断している。。

・Dさんはすぐに会社に向かうことは可能で、Dさんの自宅から会社までは1時間掛かる。。

C課長は、すぐにPCを会社に持参し、オフラインでマルウェア対策ソフトの定義ファイルを最新版に更新した後、フルスキャンを実施するようDさんに指示をした。スキャンを実行した結果、DさんのPCからマルウェアが検出された。このマルウェアは、マルウェア対策ソフトのベンダーが9時に公開した最新の定義ファイルで検出可能であることが判明した。。

A社では、今回のマルウェア感染による情報セキュリティインシデントの問題点を整理し、再発を防止するための対策を講じることにした。。

設問。A社が講じることにした対策はどれか？。解答群のうち、最も適切なものを選べ。。

解答群。

ア。PCが起動したらすぐに自動的にVPN接続するように、PCを構成する。。

イ。これまでメールをやり取りしたことがない差出人からメールを受信した場合は、添付されているファイルを開かず、すぐに削除するよう社内ルールに定める。。

ウ。マルウェア定義ファイルは、10分ごとに更新されるように、マルウェア対策ソフトの設定を変更する。。

エ。マルウェア定義ファイルは、8時にも更新されるように、マルウェア対策ソフトの設定を変更する。。

オ。メールに添付されたファイルを開く場合は、一旦PCに保存し、マルウェア対策ソフトでスキャンを実行してから開くよう社内ルールに定める。

せいかいわ。ウ。マルウェア定義ファイルは、10分ごとに更新されるように、マルウェア対策ソフトの設定を変更する、です