とい1。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、要求事項において、リスクを受容するプロセスに求められるものはどれか？。。

ア。受容するリスクについては、リスク所有者が承認すること。。

イ。受容するリスクを監視やレビューの対象外とすること。。

ウ。リスクの受容は、リスク分析まえにおこなうこと。。

エ。リスクを受容するかどうかは、リスク対応後に決定すること。

せいかいわ。ア。受容するリスクについては、リスク所有者が承認することです。。。

なお、いわ、受容するリスクを監視やレビュー対象にしなければならないため不適切です。。

うわ、リスクの受容は、リスク分析後におこなうことが正しいため不適切です。。

えわ、リスクを受容するかどうかは、りすく対応まえにおこなう必要があるため不適切です。

とい2。退職する従業員による不正を防ぐための対策のうち、IPA、組織における内部不正防止ガイドライン、だいごはんにてらして、適切なものはどれか？。。

ア。在職中に知り得た重要情報を退職後に公開しないように、退職予定者に提出させる秘密保持誓約書には、秘密の保持の対象を明示せず、重要情報を客観的に特定できないようにしておく。。

イ。退職後、同業他社に転職して重要情報をもらすということがないように、職業選択の自由を行使しないことを明記したうえで、具体的な範囲を特定しない包括的な競業避止義務契約を入社時に締結する。。

ウ。退職者による重要情報の持ち出しなどの不正行為を調査できるように、従業員に付与した利用者IDや権限は退職後も有効にしておく。。

エ。退職間際に重要情報の不正な持ち出しがおこなわれやすいので、退職予定者に対する重要情報へのアクセスや媒体のもちだしの監視を強化する。

せいかいわ。エ。退職間際に重要情報の不正な持ち出しがおこなわれやすいので、退職予定者に対する重要情報へのアクセスや媒体のもちだしの監視を強化するです。。

なお、あわ、秘密保持の対象を明示し、重要情報を客観的に特定する必要があるため不適切です。。

いわ、具体的な範囲を設定する必要があるため不適切です。。

うわ、はっきりいって論外ですね。。不正アクセスの要因としてよく問題にもされるので覚えておきましょう。

とい3。じすきゅー27000、2019、情報セキュリティマネジメントシステム、用語において、不適合が発生した場合にその原因を除去し、再発を防止するためのものとして定義されているものはどれか？。。

ア。継続的改善。。イ。修正。。ウ。是正処置。。エ。リスクアセスメント

せいかいわ。ウ。是正処置です

ほかの選択肢につては、じすきゅー27000、2019にて以下のようにていぎされています。。

参考までにご紹介いたします。。

継続的改善。コンティにゅあるインプルーブメント。。

パフォーマンスを向上するために繰り返しおこなわれるかつどう。。

修正。コレクション。。

検出された不適合を除去するためのしょち。。

リスクアセスメント。。

リスク特定、リスク分析およびリスク評価のプロセスぜんたい。。

とい4。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のサポートユーティリティに関する例示に基づいて、サポートユーティリティと判断されるものはどれか？。。

ア。サーバの空調。。イ。サーバの保守契約。。

ウ。特権管理プログラム。。エ。ネットワーク管理者

せいかいわ。ア。サーバの空調です。。。詳しくは、個別の解説動画をご覧ください。

とい5。じすきゅー27000、2019、情報セキュリティマネジメントシステム、用語におけるリスクレベルの定義はどれか？。。

ア。脅威によってつけこまれる可能性のある、資産または管理策の弱点。。

イ。結果とその起こりやすさの組み合わせとして表現される、リスクの大きさ。。

ウ。対応すべきリスクに付与する優先順位。。

エ。リスクの重大性を評価するために目安とする条件。

せいかいわ。イ。結果とその起こりやすさの組み合わせとして表現される、リスクの大きさです

とい6。サイバーセキュリティ基本法にもとづき、内閣にサイバーセキュリティ戦略本部が設置されたのと同時に、内閣官房に設置された組織はどれか？。。

ア。IPA。。イ。ジプデック。。ウ。ジェイぴーさーとしーしー。。エ。にすく

せいかいわ。エ。ニスクです。。。聞き流し動画でもご紹介しております、内閣が得意なニスクくんで覚えましょう

とい7。クリプトレックの役割として、適切なものはどれか？。。

ア。外国為替および外国貿易ほうで規制されている暗号装置の輸出許可申請を審査、承認する。。

イ。政府調達においてIT関連製品のセキュリティ機能の適切性を評価、認証する。。

ウ。電子政府での利用を推奨する暗号技術の安全性を評価、監視する。。

エ。民間企業のサーバに対するセキュリティ攻撃を監視、検知する。

せいかいわ。ウ。電子政府での利用を推奨する暗号技術の安全性を評価、監視するです

※語呂合わせ

とい8。緊急事態を装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不正なこういは、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。踏み台こうげき。。エ。ブルートフォース攻撃

せいかいわ。ア。ソーシャルエンジニアリングです。。。

これはサービス問題ですね。即答できましたか？。。

とい9。エーしゃでは現在、インターネットじょうのwebサイトを内部ネットワークのPCじょうのwebブラウザから参照している。あらたなシステムを導入し、DMZじょうによういしたVDI、バーチャルデスクトップインフラストラクチャーサーバにPCからログインし、インターネットじょうのwebサイトをVDIさーばじょうの仮想デスクトップのwebブラウザからから参照するように変更する。この変更によって期待できるセキュリティじょうの効果はどれか？。。

ア。インターネットじょうのwebサイトから、内部ネットワークのPCへのマルウェアのダウンロードを防ぐ。。

イ。インターネットじょうのwebサイト利用時に、MITB攻撃による送信データの改ざんを防ぐ。。

ウ。内部ネットワークのPCおよび仮想デスクトップのOSがボットに感染しなくなり、シーアンドシーサーバにコントロールされることを防ぐ。。

エ。内部ネットワークのPCにマルウェアが侵入したとしても、ほかのPCに感染するのを防ぐ

せいかいわ。ア。インターネットじょうのwebサイトから、内部ネットワークのPCへのマルウェアのダウンロードを防ぐです

とい10。デジタルフォレンジックでハッシュちを利用する目的として、適切なものはどれか？。。

ア。いちほうこうせい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、証拠となりうるように復元する。。

ウ。証拠となりうるデータについて、げんぽんと複製の同一性を証明する。。

エ。パスワードの盗聴のうむを検証する

せいかいわ。ウ。証拠となりうるデータについて、げんぽんと複製の同一性を証明するです。。。詳しくは、個別の解説動画をご覧ください。

とい11。利用者PCの内蔵ストレージが暗号化されていないとき、攻撃者が利用者PCから内蔵ストレージを抜きとり、攻撃者が用意したPCに接続して内蔵ストレージないの情報を盗む攻撃の対策に該当するものはどれか？。。

ア。内蔵ストレージにインストールしたOSの利用者アカウントに対して、ログインパスワードを設定する。。

イ。内蔵ストレージに保存したファイルの読み取り情報を、ファイルの所有者だけに付与する。。

ウ。利用者PCじょうでHDDパスワードを設定する。。

エ。利用者PCじょうでバイオスパスワードを設定する。

せいかいわ。ウ。利用者PCじょうでHDDパスワードを設定する。。。

これはサービス問題でしたね。。即答できましたか？

とい12。ルートキットの特徴はどれか？。。

ア。OSなどに不正に組み込んだツールの存在を隠す。。

イ。OSの中核であるカーネル部分の脆弱性を分析する。。

ウ。コンピュータがマルウェアに感染していないことをチェックする。。

エ。コンピュータやルータのアクセス可能な通信ポートを外部から調査する。

せいかいわ。ア。OSなどに不正に組み込んだツールの存在を隠すです。。。

これもサービス問題でしたね。。即答できましたか？

とい13。ビーイーシー、ビジネスイーメールコンプロマイズに該当するものはどれか？。。

ア。巧妙なだましの手口を駆使し、取引先になりすましてにせの電子メールを送り、金銭をだまし取る。。

イ。送信もとを攻撃対象の組織のメールアドレスに詐称し、多数の実在しないメールアドレスに一度に大量の電子メールを送り、攻撃対象の組織のメールアドレスを故意にブラックリストに登録させて、利用を阻害する。。

ウ。第三者からの電子メールが中継できるように設定されたメールサーバを、スパムメールの中継に悪用する。。

エ。誹謗中傷メールのそうしんもとを攻撃対象のメールアドレスに詐称し、組織の社会的な信用を大きく損なわせる。

せいかいわ。ア。巧妙なだましの手口を駆使し、取引先になりすましてにせの電子メールを送り、金銭をだまし取る。。。とてもよく見る問題なので必ず覚えておきましょう

とい14。ボットネットにおけるシーアンドシーサーバの役割として、適切なものはどれか？。。

ア。Webサイトのコンテンツをキャッシュし、本来のサーバに代わってコンテンツ利用者に配信することによって、ネットワークやサーバの負荷を軽減する。。

イ。外部からのインターネットを経由して社内ネットワークにアクセスするさいに、チャップなどのプロトコルを中継することによって、利用者認証時のパスワードの盗聴を防止する。。

ウ。外部からインターネットを経由して社内ネットワークにアクセスするさいに、時刻同期方式を採用したワンタイムパスワードを発行することによって、利用者認証時のパスワードの盗聴を防止する。。

エ。侵入して乗っ取ったコンピュータに対して、ほかのコンピュータへの攻撃などの不正な操作をするよう、外部から命令をだしたり応答を受け取ったりする。

せいかいわ。エ。侵入して乗っ取ったコンピュータに対して、ほかのコンピュータへの攻撃などの不正な操作をするよう、外部から命令をだしたり応答を受け取ったりする。。。

これもよく見かける問題なので必ず覚えておきましょう

とい15。PCへの侵入に成功したマルウェアがインターネットじょうの指令サーバと通信をおこなう場合に、宛先ポートとして使用されるTCPポート番号80に関する記述のうち、適切なものはどれか？。。

ア。DNSのゾーン転送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。。

イ。WebサイトのHTTPS通信での閲覧に使用されることから、マルウェアと指令サーバとのあいだの通信が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。ドメインめいの名前解決に使用されることから、マルウェアと指令サーバとのあいだの通信が侵入検知システムで検知される可能性が低い。

せいかいわ。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です。。。

なお、あの、DNSのゾーン転送にもちいられるのはTCPポート番号53です。。

いの、HTTPS通信にもちいられるのはTCPポート番号443です。。

えの、ドメイン名の名前解決にもちいられるのはUDPポート番号53となります。

とい16。特定のサービスやシステムから流出した認証情報を攻撃者がもちいて、認証情報を複数のサービスやシステムで使い回している利用者のアカウントへのログインを試みる攻撃はどれか？。。

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

せいかいわ。ア。パスワードリスト攻撃です。。。

詳しくは、個別の解説動画をご覧ください

とい17。攻撃者が用意したサーバエックスのIPアドレスが、エーしゃwebサーバのFQDNに対応するIPアドレスとして、びーしゃDNSキャッシュサーバに記憶された。これによって、意図せずサーバエックスに誘導されてしまう利用者はどれか？。ここで、えーしゃ、びーしゃのかく従業員は自社のDNSキャッシュサーバを利用して名前解決をおこなう。。

ア。えーしゃwebサーバにアクセスしようとするえーしゃ従業員。。

イ。えーしゃwebサーバにアクセスしようとするびーしゃ従業員。。

ウ。びーしゃwebサーバにアクセスしようとするえーしゃ従業員。。

エ。びーしゃwebサーバにアクセスしようとするびーしゃ従業員

せいかいわ。イ。えーしゃwebサーバにアクセスしようとするびーしゃ従業員です。。。

えーしゃのwebサーバのFQDNに対応するIPアドレスとして、びーしゃのDNSキャッシュサーバに記憶されたとあります。よって、使用するのはびーしゃ従業員となり、アクセス先はえーしゃのwebサーバとなります。

とい18。攻撃者が、多数のオープンリゾルバに対して、あるドメインの実在しないランダムなサブドメインを多数問い合わせる攻撃、ランダムサブドメイン攻撃を仕掛け、多数のオープンリゾルバが応答した。この時に発生する事象はどれか？。。

ア。あるドメインを管理する権威DNSサーバに対して負荷がかかる。。

イ。あるドメインを管理する権威DNSサーバに登録されているDNS情報が改ざんされる。。

ウ。オープンリゾルバが保持するDNSキャッシュに不正なあたいを注入される。。

エ。オープンリゾルバが保持するゾーン情報を不正に入手される。。

せいかいわ。ア。あるドメインを管理する権威DNSサーバに対して負荷がかかるです。。。

ランダムサブドメイン攻撃は、ディードス攻撃の一種です。

とい19。SEOポイズニングの説明はどれか？。。

ア。web検索サイトの順位づけアルゴリズムを悪用して、検索結果のじょういに、悪意のあるwebサイトを意図的に表示させる。。

イ。車などで移動しながら、無線ランのアクセスポイントを探し出して、ネットワークに侵入する。。

ウ。ネットワークを流れるパケットから、侵入のパターンに合致するものを検出して、管理者への通知や、検出した内容の記録をおこなう。。

エ。マルウェア対策ソフトのセキュリティじょうの脆弱性を悪用して、システム権限で不正なしょりを実行させる。

せいかいわ。ア。web検索サイトの順位づけアルゴリズムを悪用して、検索結果のじょういに、悪意のあるwebサイトを意図的に表示させるです。。。

ちなみにSEOは、サーチエンジンオプティマイゼーションの略で、検索エンジンの最適化のことです。検索結果で自社のサイトをじょういに表示させるための仕組みです。

とい20。データベースで管理されるデータの暗号化にもちいることができ、かつ、暗号化と復号とで同じ鍵を使用する暗号方式はどれか？。。

ア。AES。。イ。PKI。。ウ。RSA。。エ。しゃーにーごーろく

せいかいわ。ア。AESです。。。これもサービス問題ですね

とい21。オープンPGPやエスマイムにおいてもちいられるハイブリッド暗号方式の特徴はどれか？。。

ア。暗号通信方式としてIPセックとTLSを選択可能にすることによって利用者の利便性を高める。。

イ。公開鍵暗号方式と共通鍵暗号方式を組み合わせることによって鍵管理コストと処理性能の両立をはかる。。

ウ。複数の異なる共通鍵暗号方式を組み合わせることによって処理性能を高める。。

エ。複数の異なる公開鍵暗号方式を組み合わせることによって安全性を高める。

せいかいわ。イ。公開鍵暗号方式と共通鍵暗号方式を組み合わせることによって鍵管理コストと処理性能の両立をはかるです。。。詳しくは、個別の解説動画をご覧ください

とい22。デジタル署名にもちいる鍵のくみのうち、適切なものはどれか？。。

ア。デジタル署名の作成にもちいる鍵、共通鍵。デジタル署名の検証にもちいる鍵、秘密鍵。。

イ。デジタル署名の作成にもちいる鍵、公開鍵。デジタル署名の検証にもちいる鍵、秘密鍵。。

ウ。デジタル署名の作成にもちいる鍵、秘密鍵。デジタル署名の検証にもちいる鍵、共通鍵。。

エ。デジタル署名の作成にもちいる鍵、秘密鍵。デジタル署名の検証にもちいる鍵、公開鍵。。

せいかいわ。エ。デジタル署名の作成にもちいる鍵、秘密鍵。デジタル署名の検証にもちいる鍵、公開鍵です。。。デジタル署名は公開鍵暗号方式ですよね

とい23。メッセージが改ざんされていないかどうかを確認するために、そのメッセージから、ブロック暗号をもちいて生成することができるものはどれか？。。

ア。PKI。。イ。パリティビット。。ウ。メッセージ認証符号。。エ。ルート証明書

せいかいわ。ウ。メッセージ認証符号です。。。これもよく見かける問題なので必ず覚えておきましょう

とい24。リスクベース認証に該当するものはどれか？。。

ア。インターネットバンキングでの取引において、取引の都度、乱数ひょうの指定したますめにある英数字を入力させて認証する。。

イ。全てのアクセスに対し、トークンで生成されたワンタイムパスワードを入力させて認証する。。

ウ。利用者のIPアドレスなどの環境を分析し、いつもと異なるネットワークからのアクセスに対して追加の認証をおこなう。。

エ。利用者の記憶、持ち物、からの特徴のうち、必ずふたつ以上の方式を組み合わせて認証する。

せいかいわ。ウ。利用者のIPアドレスなどの環境を分析し、いつもと異なるネットワークからのアクセスに対して追加の認証をおこなうです。。。2025年4月現在では、楽天証券口座ののっとりなどの対策として、このリスクベース認証がいっきに有名になりましたね。

とい25。webサイトで利用されるキャプチャに該当するものはどれか？。。

ア。ひとからのアクセスであることを確認できるよう、アクセスしたものに応答を求め、その応答を分析する仕組み。。

イ。不正なSQLぶんをデータベースに送信しないよう、webサーバに入力された文字列をプレースホルダに割り当ててSQLぶんを組み立てる仕組み。。

ウ。利用者が本人であることを確認できるよう、webサイトから一定時間ごとに異なるパスワードを要求する仕組み。。

エ。利用者が本人であることを確認できるよう、乱数をwebサイトがわで生成して利用者に送り、利用者がわでその乱数を鍵としてパスワードを暗号化し、webサイトに送り返す仕組み。

せいかいわ。ア。ひとからのアクセスであることを確認できるよう、アクセスしたものに応答を求め、その応答を分析する仕組みです。。。

なお、いわ、バインド機構の説明です。。

うわ、ワンタイムパスワードの説明です。。

えわ。チャレンジレスポンス認証の説明です

とい26。HTTPオーバーTLS、HTTPSをもちいて実現できるものはどれか？。。

ア。webサーバじょうのファイルの改ざん検知。。

イ。Webブラウザが動作するPCじょうのマルウェア検査。。

ウ。Webブラウザが動作するPCに対する侵入検知。。

エ。デジタル証明書によるサーバ認証

せいかいわ。エ。デジタル証明書によるサーバ認証です。。。これもサービス問題ですね

とい27。SPF、センダーポリシーフレームワークを利用する目的はどれか？。。

ア。HTTP通信の経路じょうでの中間者攻撃を検知する。。

イ。ランへのPCの不正接続を検知する。。

ウ。内部ネットワークへの侵入を検知する。。

エ。メール送信者のドメインのなりすましを検知する。

せいかいわ。エ。メール送信者のドメインのなりすましを検知するです。。。詳しくは、個別の解説動画をご覧ください

とい28。電子メールをドメインエーの送信者がドメインビーの宛先に送信するとき、送信者をドメインエーのメールサーバで認証するためのものはどれか？。。

ア。エーポップ。。イ。ポップスリー。。ウ。エスマイム。。エ。SMTPオース

せいかいわ。エ。SMTPオースです。。。これもサービス問題ですね

とい29。マルウェアの動的解析に該当するものはどれか？。。

ア。検体のハッシュちを計算し、オンラインデータベースに登録されたきちのマルウェアのハッシュちのリストと照合してマルウェアを特定する。。

イ。検体をサンドボックスじょうで実行し、その動作や外部との通信を観測する。。

ウ。検体をネットワークじょうの通信データから抽出し、さらに、逆コンパイルして取得したデータから検体の機能を調べる。。

エ。ハードディスクないのファイルの拡張子とファイルヘッダの内容をもとに、拡張子が偽装された不正なプログラムファイルを検出する。

せいかいわ。イ。検体をサンドボックスじょうで実行し、その動作や外部との通信を観測するです。。。

なお、あわ、コンペアほうの説明です。。

うわ、せいてき解析、ホワイトボックス解析とも呼ばれるものの説明です。。

えわ、マルウェアの検出法にかんする記述です。

とい30。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からの逸脱が無いことを調べる。。

ウ。webサーバへのアクセスの履歴を解析して、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。

せいかいわ。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です。。。詳しくは、個別の解説動画をご覧ください。

とい31。個人情報保護委員会、特定個人情報の適正な取り扱いに関するガイドライン、事業者編、令和よねんさんがつ一部改正およびそのキューアンドエーによれば、事業者によるファイル作成が禁止されている場合はどれか？。。

なお、キューアンドエーとは、特定個人情報の適正な取り扱いに関するガイドライン、事業者編および別冊金融業務における特定個人情報の適正な取り扱いに関するガイドラインにかんするキューアンドエーれいわよねんしがつついたち更新のことである。。

ア。システム障害に備えた特定個人情報ファイルのバックアップファイルを作成する場合。。

イ。従業員の個人番号を利用して業務成績を管理するファイルを作成する場合。。

ウ。税務署に提出する資料かんの整合性を確認するために個人番号を記載した明細ひょうなどチェックようファイルを作成する場合。。

エ。保険契約者の死亡保険金支払いにともなう支払調書ファイルを作成する場合。

せいかいわ。イ。従業員の個人番号を利用して業務成績を管理するファイルを作成する場合です。。。

個人番号、いわゆるマイナンバーは、社会保障、税、災害対策の範囲のみで利用可能とされていますのでご注意ください。

とい32。企業が業務で使用しているコンピュータに、記憶媒体をかいしてマルウェアを侵入させ、そのコンピュータのデータを消去したものを処罰の対象とする法律はどれか？。。

ア。刑法。。イ。製造物責任法。。ウ。不正アクセス禁止法。。エ。プロバイダ責任制限法

せいかいわ。ア。刑法です。。。とてもよく見る問題なので、反射的にこたえられるようにしましょう

とい33。企業が、特定電子メールの送信の適正化などに関する法律に定められた特定電子メールに該当する広告宣伝メールを送信する場合に関する記述のうち、適切なものはどれか？。。

ア。SMSで送信する場合はオプトアウト方式を利用する。。

イ。オプトイン方式、オプトアウト方式のいずれかを企業が自ら選択する。。

ウ。原則としてオプトアウト方式を利用する。。

エ。原則としてオプトイン方式を利用する。

せいかいわ。エ。原則としてオプトイン方式を利用するです。。。詳しくは、個別の解説動画をご覧ください。

とい34。えーしゃは、びーしゃと著作物の権利に関する特段の取り決めをせず、えーしゃの要求仕様にもとづいて、販売管理システムのプログラム作成をびーしゃに委託した。この場合のプログラム著作権の原始的帰属にかんする記述のうち、適切なものはどれか？。。

ア。えーしゃとびーしゃが話し合って帰属先を決定する。。

イ。えーしゃとびーしゃの共有帰属となる。。

ウ。えーしゃに帰属する。。

エ。びーしゃに帰属する。

せいかいわ。エ。びーしゃに帰属するです。。。著作物の権利に関する取り決めをしていない場合、著作権は作成者になってしまいます。。

実務のさい、契約書にはかならず書いておきましょう。。

まぁ普通は法務部などのチェックで追記されると思いますが。。。

とい35。システムテストの監査におけるチェックポイントのうち、最も適切なものはどれか？。。

ア。テストケースが網羅的に想定されていること。。

イ。テスト計画は利用者がわの責任者だけで承認されていること。。

ウ。テストは実際に業務がおこなわれている環境で実施されていること。。

エ。テストは利用者がわの担当者だけでおこなわれていること。

せいかいわ。ア。テストケースが網羅的に想定されていることです。。。

この選択肢いがいはありえないものばかりですね

とい36。アクセス制御を監査するシステム監査にんの行為のうち、適切なものはどれか？。。

ア。ソフトウェアに関するアクセス制御の管理台帳を作成し、保管した。。

イ。データに関するアクセス制御の管理規定を閲覧した。。

ウ。ネットワークに関するアクセス制御の管理方針を制定した。。

エ。ハードウェアに関するアクセス制御の運用手続きを実施した。

せいかいわ。イ。データに関するアクセス制御の管理規定を閲覧したです。。。

システム監査にんは主体的に改善活動をおこわないため、ほん選択肢以外は全てあやまりとなります。

とい37。我が国の証券取引所に上場している企業において、内部統制の整備および運用に最終的な責任をおっているものは誰か？。。

ア。株主。。イ。監査役。。ウ。業務担当者。。エ。経営者

せいかいわ。エ。経営者です。。。これは一般常識レベルの問題ですね

とい38。ヒューマンエラーに起因する障害を発生しにくくする方法に、エラープルーフかがある。運用作業におけるエラープルーフかの例として、最も適切なものはどれか？。。

ア。画面じょうの複数のウィンドウを同時に使用する作業では、ウィンドウを間違えないようにウィンドウの背景色をそれぞれ異なる色にする。。

イ。長時間におよびシステム監視作業では、疲労がちくせきしないように、二時間おきに交代で休憩を取得する体制にする。。

ウ。ミスが発生しやすい作業について、過去に発生したヒヤリハット情報を共有して同じミスを起こさないようにする。。

エ。臨時の作業をおこなうさいにも落ち着いて作業ができるように、臨時の作業の教育や訓練を定期的におこなう。

せいかいわ。ア。画面じょうの複数のウィンドウを同時に使用する作業では、ウィンドウを間違えないようにウィンドウの背景色をそれぞれ異なる色にするです。。。詳しくは、個別の解説動画をご覧ください。

とい39。あるデータセンタでは、受発注管理システムの運用サービスを提供している。つぎの受発注管理システムの運用中の事象において、インシデントに該当するものはどれか？。。

受発注管理システムの運用ちゅうの事象。。

夜間バッチ処理において、注文トランザクションデータから注文書を出力するプログラムが異常終了した。異常終了を検知した運用担当者から連絡を受けた保守担当者は、緊急出社してサービスを回復し、後日、異常終了の原因となったプログラムの誤りを修正した。。

ア。異常終了の検知。。イ。プログラムの誤り。。

ウ。プログラムの異常終了。。エ。保守担当者の緊急出社

せいかいわ。ウ。プログラムの異常終了です。。。

IT分野におけるインシデントは、システム障害、情報漏えいなどが該当いたしますので覚えておきましょう

とい40。ソフトウェア開発プロジェクトにおいてWBSを作成する目的として、最も適切なものはどれか？。。

ア。開発の期間と費用とがトレードオフの関係にある場合に、総費用の最適化をはかる。。

イ。作業の順序関係を明確にして、重点管理すべきクリティカルパスを把握する。。

ウ。作業の日程を横棒、バーであらわして、作業の開始時点や終了時点、現時点の進捗を明確にする。。

エ。作業を、階層的に詳細化して、管理可能な大きさに細分化する。

せいかいわ。作業を、階層的に詳細化して、管理可能な大きさに細分化するです。。。

ちなみにWBSは、ワークブレークダウンストラクチャーのりゃくです。

とい41。プロジェクトの日程計画を作成するのに適した技法はどれか？。。

ア。パート。。イ。回帰分析。。ウ。時系列分析。。エ。線形計画法

せいかいわ。ア。パートです。。。

なお、パートはプログラムエバルエーションアンドレビューテクニークの略で、別名アローダイアグラムといいます。

とい42。いっぽうのコンピュータが正常に機能しているときには、たほうのコンピュータが待機状態にあるシステムはどれか？。。

ア。デュアルシステム。。イ。デュプレックスシステム。。

ウ。マルチプロセッシングシステム。。エ。ロードシェアシステム

せいかいわ。イ。デュプレックスシステムです。。。

情報セキュリティマネジメントでは最近でてないですが、ITパスポートや基本情報では見かける問題ですね

とい43。データベースの監査ログを取得する目的として、適切なものはどれか？。。

ア。権限のない利用者のアクセスを拒否する。。

イ。チェックポイントからのデータ復旧に使用する。。

ウ。データの不正な書き換えや削除を事前に検知する。。

エ。問題のあるデータベース操作を事後に調査する。

せいかいわ。エ。問題のあるデータベース操作を事後に調査するです。。。ログの調査なので、事後しか分からないですよね

とい44。社内ネットワークのPCから、中継装置を経由してインターネットじょうのwebサーバにアクセスする。中継装置は宛先のwebサーバのドメインめいからDNSを利用してグローバルIPアドレスをもとめ、そのグローバルIPアドレスあてにアクセス要求の転送をおこなう機能をゆうする。この中継装置として、適切なものはどれか？。。

ア。プロキシサーバ。。イ。リピータ。。

ウ。ルータ。。エ。レイヤツースイッチ

せいかいわ。ア。プロキシサーバです。。。この問題も典型的な問題ですね

とい45。BPOの説明はどれか？。。

ア。災害や事故で被害を受けても、重要事業を中断させない、または可能な限り中断期間を短くする仕組みを構築すること。。

イ。社内業務のうちコアビジネスでない事業に関わる業務の一部または全部を、外部の専門的な企業に委託すること。。

ウ。製品の基準生産計画、部品ひょうおよび在庫情報をもとに、資材の所要量と必要な時期をもとめ、これを基準に資材の手配、納入の管理を支援する生産管理手法のこと。。

エ。プロジェクトを、戦略との適合性や費用対効果、リスクといった観点から評価をおこない、情報化投資のバランスを管理し、最適化を図ること。

せいかいわ。イ。社内業務のうちコアビジネスでない事業に関わる業務の一部または全部を、外部の専門的な企業に委託することです。。。詳しくは、個別の解説動画をご覧ください。

とい46。製造業の企業が社会的責任をはたす活動の一環として、雇用創出や生産設備の環境対策に投資することによって、べんえきをきょうじゅするステークホルダは、株主、役員、従業員に加えて、どれか？。。

ア。近隣地域社会の住民。。イ。原材料の輸入もと企業。。

ウ。製品を購入している消費者。。エ。取引をしている下請け企業

せいかいわ。ア。近隣地域社会の住民です。。。

ステークホルダは利害関係者ともいい、株主、従業員、地域社会などが例としてあげられます

とい47。ひょうから、期末在庫ひんを先入れ先出し法で評価した場合の期末の在庫評価額はなんぜんえんか？。。

期首在庫。10こ。10せんえん。。

仕入しがつ。1個。11せんえん。。

しいれろくがつ。2個。12せんえん。。

しいれしちがつ。3こ。13せんえん。。

しいれくがつ。4こ。14せんえん。。

期末在庫。12こ。。

選択肢。。

ア。132。。イ。138。。ウ。150。。エ。168

せいかいわ。う。150です。。。

計算方法を解説いたします。。

しがつから九月のしいれは、全部で10こです。。

期首在庫10ことあわせると、20こであるとわかります。。

期末在庫は12こなので、期首在庫が8こ販売されたことがわかります。。

先入先出法なので、期首在庫2個、あとはかくつきのしいれりょうと単価をかけて、すべて足すと答えが150とわかります。。

分からなかったひとは、一時停止をしてて計算をしてみてください。

とい48。製造原価明細書から損益計算書を作成したとき、売上総利益はなんぜんえんか？。。

たんいせんえん。。

製造原価明細書。。

材料費。400。。

労務費。300。。

経費。200。。

とうき製造費用。ほにゃらら。。

期首仕掛品棚卸高。150。。

期末仕掛品棚卸高。250。。

当期製品製造原価。ほにゃらら。。

損益計算書。。

売上高。1000。。

売上原価。。

期首製品棚卸高。120。。

当期製品製造原価。ほにゃらら。。

期末製品棚卸高。70。。

売上原価。ほにゃらら。。

売上総利益。ほにゃらら。。

ア。150。。イ。200。。ウ。310。。エ。450

せいかいわ。ア。150です。。。

計算方法をご説明いたします。。

製造原価明細書の当期製造費用は、材料費と労務費と経費を足せばよいので900とすぐにわかります。。

当期製品製造原価は、当期製造費用に期首仕掛品棚卸高をたして、期末仕掛品棚卸高をひけばよいので、800とわかります。。

損益計算書にいきましては、まずは当期製品製造原価にさきほどの800をあてはめます。。

売上原価は、期首製品棚卸高に当期製品製造原価を加え、期末製品棚卸高を引けばよいので、850とわかります。。

最後に売上総利益は、売上高から売上原価を引けばよいので、答えは150と求めることができます。。

分からなかったひとは、一時停止をして手計算をしてみてください。

とい49。えーしゃは、放送会社や運輸会社むけに広告制作ビジネスを展開している。えーしゃは、人事業務の効率化を図るべく、人事業務の委託を検討することにした。えーしゃが委託する業務、以下、びー業務というを図1に示す。。

図1。びー業務。。

採用予定者から郵送されてくる入社時の誓約書、前職の源泉徴収票などのしょるいをPDFファイルに変換し、ファイルサーバに格納する。省略。。

委託先候補のしーしゃは、びー業務について、つぎのようにえーしゃに提案した。。

びー業務だけに従事する専任の従業員を割り当てる。。

びー業務では、図2の複合機のスキャン機能を使用する。。

図2。複合機のスキャン機能、抜粋。。

スキャン機能を使用する際は、従業員ごとに付与した利用者IDとパスワードをパネルに入力する。。

スキャンしたデータをPDFファイルに変換する。。

PDFファイルを従業員ごとに異なる鍵で暗号化して、電子メールに添付する。。

スキャンを実行した本人あてに電子メールを送信する。。

PDFファイルが大きい場合は、PDFファイルを添付するかわりに、自社の社内ネットワークじょうに設置したサーバ、以下、ビーサーバという、に自動的に保存し、保存先のURLを電子メールの本文に記載して送信する。

えーしゃは、シーシャと業務委託契約を締結する前に、秘密保持契約を締結して、しーしゃを訪問し、業務委託での情報セキュリティリスクの評価を実施した。その結果、図3の発見があった。。

図3。発見事項。。

複合機のスキャン機能では、電子メールの差出人アドレス、件名、本文および添付ファイルめいを初期設定、かっこ1の状態で使用しており、誰がスキャンを実行しても同じ名前である。。

複合機のスキャン機能の初期設定情報はベンダーのwebサイトで公開されており、誰でも閲覧できる。。

注意かっこ1。シーシャの情報システム部だけが複合機の初期設定を変更可能である。

そこで、えーしゃでは、初期設定の状態のままではえーしゃにとって情報セキュリティリスクがあり、対策が必要であると評価した。

設問。対策が必要であるとえーしゃが評価した情報セキュリティリスクはどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。びー業務に従事する従業員が、びー業務に従事するほかの従業員になりますまして複合機のスキャン機能を使用し、PDFファイルを取得して不正に持ち出す。その結果、エーしゃに採用予定者の個人情報が漏えいする。。

イ。びー業務に従事する従業員が、攻撃者からの電子メールを複合機からのものと信じて本文中にあるURLをクリックし、攻撃者が用意したwebサイトにアクセスしてマルウェア感染する。その結果、えーしゃ採用予定者の個人情報が漏えいする。。

ウ。攻撃者が、複合機から送信される電子メールを盗聴し、添付ファイルを暗号化して身代金を要求する。その結果、えーしゃが復号鍵を受け取るために多額の身代金を支払うことになる。。

エ。攻撃者が、複合機から送信される電子メールを盗聴し、本文に記載されているURLをSNSに公開する。その結果、エーしゃの採用予定者の個人情報が漏えいする。

せいかいわ。イ。びー業務に従事する従業員が、攻撃者からの電子メールを複合機からのものと信じて本文中にあるURLをクリックし、攻撃者が用意したwebサイトにアクセスしてマルウェア感染する。その結果、えーしゃ採用予定者の個人情報が漏えいするです。

それではもう一度、図3。発見事項を見てみましょう。。

複合機のスキャン機能では、電子メールの差出人アドレス、件名、本文および添付ファイルめいを初期設定、かっこ1の状態で使用しており、誰がスキャンを実行しても同じ名前である。。

複合機のスキャン機能の初期設定情報はベンダーのwebサイトで公開されており、誰でも閲覧できる。。

注意かっこ1。シーシャの情報システム部だけが複合機の初期設定を変更可能である。

と記載されています。。

つまり、悪意のある攻撃者がスキャンを実行しても、電子メールの情報は初期設定のままであり、その初期設定情報はベンダーのwebサイトで公開しているため悪用は可能ということですね。

ということで、せいかいわ。イ。びー業務に従事する従業員が、攻撃者からの電子メールを複合機からのものと信じて本文中にあるURLをクリックし、攻撃者が用意したwebサイトにアクセスしてマルウェア感染する。その結果、えーしゃ採用予定者の個人情報が漏えいするとなります。。。

なお、あわ、スキャンを使用するときは個人に割り振られたIDとパスワードが必要となるため、適切ではないです。。

ウとエは、電子メールの盗聴にかんするもので今回の情報セキュリティリスクには該当しません。よって不適切です。。

とい50。えーしゃは、分析、計測機器などの販売および機器を利用した試料の分析受託業務をおこなう分析機器メーカーである。えーしゃでは、図1の情報セキュリティリスクアセスメント手順にしたがい、年に一度、情報セキュリティリスクアセスメントの結果をまとめている。。

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、可用性の評価ちは、それぞれぜろから2の三段階とし、ひょう1のとおりとする。。

情報資産の機密性、完全性、可用性の評価ちの最大ちを、その情報資産の重要度とする。。

脅威および脆弱性のひょうかちは、それぞれぜろから2の三段階とする。。

情報資産ごとに、様々な脅威に対するリスクちを算出し、その最大ちを当該情報資産のリスクち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ちは、つぎの式によって算出する。。

リスクちいこーる情報資産の重要度かける驚異の評価ちかける脆弱性のひょうかち。。

情報資産のリスクちのしきいちを5とする。。

情報資産ごとのリスクちがしきいち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ちがしきいちを超えた場合は、保有以外のリスク対応をおこなうことを基本とする

ひょう1。情報資産の機密性、完全性、可用性の評価基準。。

機密性。評価ち2。評価基準。法律で安全管理措置が義務付けられている。該当する情報の例。健康診断の結果、保健指導の記録。給与所得の源泉徴収票。。

評価ち2。取引先から守秘義務の対象として指定されている。取引先から秘密と指定されて受領した資料。取引先の公開前の新製品情報。。

評価ち2。自社の営業秘密であり、漏えいすると自社に深刻な影響がある。自社の独自技術、ノウハウ。取引先リスト。特許出願前の発明情報。。

評価ち1。関係者外秘情報または社外秘情報である。見積書、仕入れ価格など取引先や顧客との商取引に関する情報。社内規定、事務処理要領。。

評価ちぜろ。公開情報である。自社製品カタログ、自社webサイト掲載情報。。

完全性。評価ち2。法律で安全管理措置が義務付けられている。健康診断の結果、保健指導の記録。給与所得の源泉徴収票。。

評価ち2。改ざんされると自社に深刻な影響、または取引先や顧客に大きな影響がある。

社内規定、事務処理要領。自社の独自技術。ノウハウ。設計データ。原本。。

評価ち1。改ざんされると事業に影響がある。受発注情報、決済情報、契約情報。設計データ、印刷物。。

改ざんされても事業に影響は無い。廃盤製品カタログデータ。。

可用性。省略。

えーしゃは、自社のwebサイトをインターネットじょうに公開している。えーしゃのwebサイトは、自社が取り扱う分析機器の情報を画像付きで一覧表示する機能をゆうしており、おもにえーしゃで販売する分析機器に関する機能の説明や操作マニュアルを掲載している。えーしゃで分析機器を購入した顧客は、えーしゃのwebサイトからマニュアルをダウンロードして利用することが多い。えーしゃのwebサイトは、製品を販売する機能を有していない。えーしゃは、年次の情報セキュリティリスクアセスメントの結果を、ひょう2にまとめた。

ひょう2。えーしゃの情報セキュリティリスクアセスメント結果、抜粋。。

情報資産名称。社内規定。説明。行動規範や判断基準を含めた社内ルール。機密性の評価ち。1。完全性の評価ち。2。可用性の評価ち。1。情報資産の重要度。2。驚異の評価ち。1。脆弱性の評価ち。1。リスクち。2。

設計データ、印刷物。えーしゃにおける主力製品の設計図。省略。

自社webサイトにあるコンテンツ。分析機器の情報。ひょうかちの読み上げは省略いたします。

せつもん。ひょう2ちゅうのえーわんからえーふぉーにいれる数字の組み合わせを、エーに関する解答群から選べ。。

エーに関する解答群。。

解答群についての読み上げはあまり意味がないため省略いたします。

せいかいわ。エ。エーワン、ゼロ。エーツー。2。エースリー。2。エーフォー。4です。。

それではまず。ひょう2の自社webサイトにあるコンテンツの、機密性のひょうかちから考えてみましょう。。

ひょう1。情報資産の機密性、完全性、可用性の評価基準を見てみましょう。。

公開情報である自社webサイトの掲載情報の機密性は、ゼロ、となっていますね。。

よって、ひょう2のエーワンは、ゼロ、とわかります

つぎは、完全性の評価ち、えーつーを確認してみましょう

問題文の戻ってみると、えーしゃで分析機器を購入した顧客は、えーしゃのwebサイトからマニュアルをダウンロードしてりようする。とありますね

ではひょう1にもどりましょう。えーしゃのwebサイトからマニュアルをダウンロードできる状態のため、マニュアルが改ざんされると顧客におおきな影響がでると考えられます。

よって、完全性のひょうかちは、2、であると考えられます。

それではつぎに、情報資産の重要度について考えてみましょう。

ず1。情報セキュリティリスクアセスメント手順を見てみましょう。

情報資産の重要度は、情報資産の機密性、完全性、可用性の評価ちの最大ちとすると書いていますね

ひょう2にもどりましょう。機密性、完全性、可用性のひょうかちの最大ちは、2なので、情報資産の重要度は2となりますね。最後にリスクちについて考えてみましょう。

図1によると、リスクちは、情報資産の重要度かける驚異の評価ちかける脆弱性の評価ちとありますね。

ということで、リスクちを求めると、2かける2かける2で、8とわかります。

えーにかんする解答群としては、エ。が正解となります。。意外と簡単だったでしょう？

とい51。えーしゃは、金属加工をおこなっている従業員50めいの企業である。同業他社がサイバー攻撃を受けたというニュースがふえ、えーしゃの社長は情報セキュリティに対する取組が必要であると考え、新たに情報セキュリティリーダーをおくことにした。。

社長は、どのような取り組みが良いかを検討するよう、情報セキュリティリーダーに任命されたびー主任に指示した。ビー主任は、調査の結果、IPAが実施しているセキュリティーアクションへの取り組みを社長に提案した。。

セキュリティ－アクションとは、中小企業みずからが、情報セキュリティ対策に取り組むことを自己宣言する制度であるとの説明を受けた社長は、セキュリティーアクションのひとつぼしを宣言するために情報セキュリティごかじょうに取り組むことをきめ、ビー主任に、情報セキュリティごかじょうへの自社での取り組み状況を評価するように指示した。

ビー主任の評価結果はひょう1のとおりであった。

ひょう1。ビー主任の評価結果。

情報セキュリティごかじょう。

1。OSやソフトウェアは常に最新の状態にしよう。

評価結果。

一部のPCについて実施している。

2。省略。

3。パスワードを強化しよう。

4。共有設定を見直そう。

5。脅威や攻撃の手口を知ろう

ひょう１ちゅうの1の評価結果についてビー主任は、つぎのとおり説明した。

Aしゃが従業員にPCを貸与するときに導入したOSとえーしゃの業務で利用しているソフトウェア、以下、標準ソフトという、わ、自動更新機能を使用して最新の状態に更新している。

それ以外のソフトウェア、以下、非標準ソフトという、わ、どの程度利用されているか分からないので、試しに数台のPCを確認したところ、大半のPCで利用されていた。最新の状態に更新されていないPCも存在した。

えーしゃでは、ひょう1ちゅうの1について評価結果を実施しているにするために新たに追加すべき対策として2あんを考え、どちらかを採用することにした。

せつもん。ひょう1ちゅうの1の評価結果を実施しているにするためにえーしゃで新たに追加すべき対策として考えられるものはつぎのうちどれか？。考えられる対策だけを全てあげた組み合わせを、解答群のなかから選べ。。

1。PCじょうのプロセスの起動、終了をきろくするエンドポイントディテクションアンドレスポンス、EDRの導入。。

2。PCのOSおよび標準ソフトを最新の状態に更新するという設定ルールの導入。。

3。全てのPCへの脆弱性修正プログラムの自動適用をおこなうIT資産管理ツールの導入。。

4。非標準ソフトのインストール禁止および強制アンインストール。。

5。ログデータを一括管理、分析して、セキュリティじょうの脅威を発見するためのセキュリティーインフォメーションアンドイベントマネージメント、しーむの導入

なお、解答群はこのようになっております。。読み上げても意味はないので読み上げはおこないません。。

せいかいわ。ク。3、4です。。

対策としては、3。全てのPCへの脆弱性修正プログラムの自動適用をおこなうIT資産管理ツールの導入と。4。非標準ソフトのインストール禁止および強制アンインストールになります。

ひょう1の1を見てみましょう。OSやソフトウェアは常に最新の状態にしよう。というものについて対応したいというものでしたね。

設問にもどりましょう。少なくとも、1と5は関係ないことが直ぐにわかります。。

2については、既に実装されているので追加の必要はありませんね。。

よって答えは、3と4になります。。簡単ですよね？

とい52。えーしゃは、複数の子会社を持つ食品メーカーであり、在宅勤務に適用するPCセキュリティ規定、以下、えーしゃPC規定という、を定めている。

エーしゃは、にせんえっくすねんしがつついたちに同業のびーしゃを買収して子会社にした。びーしゃは、在宅勤務できる日数の上限をしゅうふつかとした在宅勤務制度を導入しており、全ての従業員が利用している。

びーしゃは、えーしゃPC規定と同様の規定を作成して順守することにした。びーしゃは、じしゃの規定の作成にあたり、ひょう1のとおりえーしゃPC規定への対応状況の評価結果をとりまとめた。

ひょう1。えーしゃPC規定へのびーしゃの対応状況の評価結果、抜粋。。

こうばん1。えーしゃPCきてい。省略。評価結果。オーケー。。

2。省略。オーケー。。

3。会社が許可したアプリケーションソフトウェアだけを導入できるように技術的に制限すること。エヌジー。。

4。外部記憶媒体へのアクセスを技術的に禁止すること。エヌジー。かっこ1。。

5。ブルートゥースの利用を技術的に禁止すること。エヌジー。。

ちゅうき。評価結果がオーケーとは、えーしゃPC規定をみたすばあい、エヌジーとはみたさないばあいをいう。。

ちゅう1。びーしゃは、外部記憶媒体へのアクセスのうち、外部記憶媒体に保存してあるアプリケーションソフトウェアおよびファイルのNPCへのコピーだけは許可している。。

評価結果のうち、えーしゃPC規定をみたさないこうばんについては、必要な追加対策を実施することによって、情報セキュリティリスクを低減することにした。

せつもん。ひょう1ちゅうのこうばん4について、びーしゃがひつような追加対策を実施することによって低減できる情報セキュリティリスクはつぎのうちどれか？。低減できるものだけを全てあげた組み合わせを、解答群のなかから選べ。ここで、こうばん3、5への追加対策は実施しないものとする。。

1。びーしゃで許可していないアプリケーションソフトウェアが保存されている外部記憶媒体がNPCに接続された場合に、当該NPCがマルウェア感染する。。

2。外部記憶媒体がNPCに接続された場合に、当該外部記憶媒体に当該NPCないのでーたを保存して持ち出される。。

3。マルウェアつきのファイルが保存されている外部記憶媒体がNPCに接続された場合、当該NPCがマルウェア感染する。。

4。マルウェアに感染しているNPCに外部記憶媒体が接続された場合に、当該外部記憶媒体がマルウェア感染する。

なお、解答群はこのようになっております。。読み上げても意味はないので読み上げはおこないません。。

せいかいわ。エ。1、3です。。

選択肢としては、1。びーしゃで許可していないアプリケーションソフトウェアが保存されている外部記憶媒体がNPCに接続された場合に、当該NPCがマルウェア感染すると、3。マルウェアつきのファイルが保存されている外部記憶媒体がNPCに接続された場合、当該NPCがマルウェア感染するが正解となります。

ひょう1のこうばん4を見てみましょう。外部記憶媒体へのアクセスを技術的に禁止することについて、評価結果はエヌジーとなっていますね。。

しかし、ちゅう1には、びーしゃは、外部記憶媒体へのアクセスのうち、外部記憶媒体に保存してあるアプリケーションソフトウェアおよびファイルのNPCへのコピーだけは許可しているとあります。。

つまり、外部記憶媒体に保存されたものの読み込みだけはできてしまうということです。。怖いですねえ

せんたくしを見てみましょう。2については外部記憶媒体への保存となっているため不適切だとわかります。。4についてもおなじような内容ですね。。

よって、せいかいわ。1と3になります。。これも簡単でしたね

とい53。えーしゃは、高級家具を販売する企業である。えーしゃは2年前に消費者に直接通信販売する新規事業を開始した。それまでえーしゃは、個人情報はほとんど取り扱っていなかったが、通信販売事業を開始したことによって、複合機で印刷した送り状など、顧客の個人情報を大量にあつかうようになってきた。そのため、オフィスないに通販事業部エリアをもうけ、個人情報がろうえいしないよう対策した。具体的には、通通販事業部エリアの出入り口に、ICカード認証でドアを解錠するシステムを設置し、通販事業部の従業員だけが通販事業部エリアに入退室できるようにした。ほかのエリアはえーしゃの全従業員が自由に利用できるようにしている。ず1は、えーしゃのオフィスのレイアウトである。

ず1。えーしゃのオフィスのレイアウト。。

このレイアウトでの業務を観察したところ、通販事業部エリアへの入室時に、えーしゃの従業員同士による智連れがおこなわれているという問題点が発見され、改善案を考えることになった。

せつもん。改善案として適切なものだけを全てあげた組み合わせを、解答群のなかから選べ。。

1。ICカードドアに監視カメラを設置し、1年に一回監視カメラの映像をチェックする。。

2。ICカードドアのわきに、ともづれのもたらすリスクを知らせる標語を掲示する。。

3。ICカードドアを、エーイーエスの暗号方式をもちいたものに変更する。。

4。ICカードの認証にくわえてゆび静脈認証もおこなうようにする。。

5。せいもん内側の自動ドアにともづれ防止用のアンチパスバックを導入する。。

6。通販事業部エリアないでは、従業員しょうをつねに見えるところに携帯する。。

7。ともづれを発見した場合は従業員どうしで個別に注意する。

なお、解答群はこのようになっております。。読み上げても意味はないので読み上げはおこないません。。

せいかいわ。オ。2、7です。

選択肢としては、2。ICカードドアのわきに、ともづれのもたらすリスクを知らせる標語を掲示すると、7。ともづれを発見した場合は従業員どうしで個別に注意するです。。

この設問は、ともづれ防止に関する対策についてとわれたものです。。

1は、監視カメラを設置するのは良いですが、1年に一回程度のチェックでは効果が期待できないため不適切です。。

3と4は、ICカードのセキュリティを強固にしたとしても、ともづれじたいは防止できないため不適切です。。

5わ、通販事業部エリアへの対策であるため、せいもんうちがわの自動ドアにアンチパスバックを設置しても意味がないため不適切です。。

6わ、従業員しょうをみたところでともづれで入ったかどうかまでは判断できないため不適切です。。

とい54。えーしゃは旅行商品を販売しており、業務のなかで顧客情報を取り扱っている。えーしゃが保有する顧客情報は、えーしゃのファイルサーバ一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すべてのファイルを磁気テープに毎週土曜日にバックアップするように設定されている。バックアップは、にせだいぶんが保存され、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。

えーしゃではねんにいちど、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イー主任は、えーしゃ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。えーしゃのデータ保管に関するリスク、抜粋。。

1。ランサムウェアによってデータが暗号化され、最新のデータが利用できなくなることによって、最大一週間ぶんの更新情報が失われる。。

以下省略。。

イー主任は、図1の1に関するリスクを現在の対策よりも、より低減するための対策を検討した。

設問。イー主任が検討した対策はどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。しゅういっかいのバックアップを取得するかわりに、毎日一回バックアップを取得してななせだいぶん保存する。。

イ。バックアップ後に磁気テープのなか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ォルダちゅうのファイルのリストを比較し、さぶんがないことをかくにんする。。

ウ。バックアップに利用する磁気テープ装置を、より高速な製品に交換する。。

エ。バックアップようの媒体を磁気テープからハードディスクに変更する。。

オ。バックアップをふたくみ取得し、うちひとくみを遠隔地に保管する。。

カ。ファイルサーバにマルウェア対策ソフトを導入する。

せいかいわ。ア。しゅういっかいのバックアップを取得するかわりに、毎日一回バックアップを取得してななせだいぶん保存するです。。。

問題となっているのは、ランサムウェア被害にあった場合最大いっしゅうかんぶんの更新情報が失われることです。よって、さぶんを少なくする対策をすれば良いです。というかふつうしますよね？。。。

ほかのかいとうぐんは、どれもリスク低減対策にはなりません。。。

このもんだいは簡単でしたね

とい55。えーしゃは、サース形式の給与計算サービス。以下、エーサービスという、を法人向けに提供する、従業員100めいのIT会社である。えーしゃは、自社でもエーサービスを利用している。えーしゃの従業員は、webブラウザでエーサービスのログイン画面にアクセスし、エーサービスのアカウント。以下、エーアカウントというの利用者IDおよびパスワードを入力する。ログインに成功すると、自分の給与および賞与の確認、パスワードの変更などができる。利用者IDは、個人ごとに付与した不規則なはちけたの番号である。ログインじにパスワードを連続してごかい間違えるとエーアカウントはロックされる。ロックを解除するためには、エーサービスの解除画面で申請する。

えーしゃは、半年にいっかい、標的型攻撃メールへの対応訓練、以下、エイチ訓練というを実施しており、ひょう1にしめすにせんえっくすねんしもきのエイチ訓練計画案が経営会議に提出された。

ひょう1。にせんえっくすねんしもきのエイチ訓練計画案、抜粋。。

項目。電子メールの送信日時。内容。つぎのにちじに、エイチ訓練の電子メールを全従業員あてに送信する。にせんえっくすねん10がつついたちじゅうじゼロゼロふん。。

送信者メールアドレス。エーサービスをよそおったドメインのメールアドレス。。

電子メールのほんぶん。つぎをふくめる。エーアカウントはロックされていること。ロックを解除するには、つぎのURLにアクセスすること。にせ解除サイトのURL。。

にせ解除サイト。氏名、所属部門めいならびにエーアカウントの利用者IDおよびパスワードを入力させる。

全ての項目の入力が完了すると、エイチ訓練であることをひょうじする。。

結果の報告。経営会議への報告予定日。にせんえっくすねん10月31日。。

ちゅうき。にせ解除サイトで入力された情報は、保存しない。えーしゃは、従業員の氏名、所属部門めいおよびエーアカウントの情報を個人情報としている。。

経営会議では、ひょう1の計画あんはどのような標的型攻撃メールを想定しているのかという質問があった。

せつもん。ひょう1の計画案が想定している標的型攻撃メールはどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。従業員をエーサービスに誘導し、エーアカウントのロックが解除されるかをしこうする標的型攻撃メール。。

イ。従業員を攻撃者が用意したwebサイトに誘導し、エーアカウントがロックされない連続失敗回数の上限を発見する標的型攻撃メール。。

ウ。従業員を攻撃者が用意したwebサイトに誘導し、従業員の個人情報を不正に取得する標的型攻撃メール。。

エ。複数の従業員をエーサービスに同時に誘導し、アクセスを集中させることによって、一定期間、エーサービスを利用不可にする標的型攻撃メール。

せいかいわ。ウ。従業員を攻撃者が用意したwebサイトに誘導し、従業員の個人情報を不正に取得する標的型攻撃メールです。。。これは即答できますよね？。。

なお、あわ、エーアカウントのロックが解除されるかをしこうするのではなく、にせサイトへの誘導となっているため不適切です。。

いについてもどうようです。。

えもどうようです。。また100めいていどの規模の会社でサーバへの負荷テストって時点でもへんな選択肢だと思いますよね。。。ぜいじゃくぅぅぜいじゃくぅぅ

とい56。えーしゃは学習塾を経営している会社であり、全国に50の校舎を展開している。えーしゃには、教務部、情報システム部、監査部などがある。学習塾にかようまたはかよっていた生徒、以下、塾生という、の個人データは、学習塾向けの管理システム、以下、塾生管理システムという、に格納している。塾生管理システムのシステム管理は情報システム部がおこなっている。塾生の個人データ管理業務と塾生管理システムの概要を図1にしめす。

図1。塾生の個人データ管理業務と塾生管理システムの概要。。

教務部員は、入塾した塾生および退塾する塾生の登録、塾生プロフィールの編集、模試結果の登録、進学先の登録など、塾生の個人データの入力、参照および更新をおこなう。。

教務部員が使用する端末は教務部の共用端末である。。

塾生管理システムへのログインには利用者IDとパスワードを利用する。。

利用者IDは個人別に発行されており、利用者IDの共用はしていない。。

塾生管理システムの利用者のアクセス権限には参照権限および更新権限の二種類がある。

参照権限があると塾生の個人データを参照できる。更新権限があると塾生の個人データの参照、入力および更新ができる。アクセス権限は塾生の個人データごとに設定できる。。

教務部員は、担当する塾生の個人データの更新権限をもっている。担当しない塾生の個人データの参照権限および更新権限はもっていない。。

共用端末のOSへのログインには、共用端末の識別し、以下、端末IDという、とパスワードを利用する。。

共用端末のパスワードおよび塾生管理システムの利用者のアクセス権限は情報システム部が設定、変更できる。。

教務部は、今年実施の監査部による内部監査の結果、webブラウザに塾生管理システムの利用者IDとパスワードを保存しており、情報セキュリティリスクが存在するとの指摘を受けた。

せつもん。監査部から指摘された情報セキュリティリスクはどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。共用端末と塾生管理システムかんの通信が盗聴される。。

イ。共用端末が不正に持ち出される。。

ウ。情報システム部員によって塾生管理システムの利用者のアクセス権限が不正に変更される。。

エ。教務部員によって共用端末のパスワードが不正に変更される。。

オ。塾生の個人データがアクセス権限を持たない教務部員によって不正にアクセスされる。

せいかいわ。オ。塾生の個人データがアクセス権限を持たない教務部員によって不正にアクセスされるです。。。監査部からの指摘は、webブラウザに塾生管理システムの利用者IDとパスワードを保存しているとありますね。。つまり、webブラウザに記憶されていたほかの人の認証情報が利用できてしまうということになります。よって、答えは、オ、いったくとなります。。

とい57。えーしゃは従業員600めいの投資コンサルティングがいしゃである。東京の本社には、情報システム部、監査部などの管理部門があり、関西にビー支店がある。ビー支店の従業員は10めいである。

ビー支店では、情報システム部が運用管理しているファイルサーバを使用しており、顧客情報を含むファイルを一時的に保存する場合がある。その場合、ファイルのアクセス権は、当該ファイルを保存した従業員が最小権限の原則にもとづいて設定する。今年、ビー支店では、従業員にヒアリングをおこない、ファイルのアクセス権がそのとおりに設定されていることを確認した。

自己評価の実施。。

えーしゃでは、一年に一回、監査部が各部門に、評価項目を記載したシート、以下、自己評価シートという、を配布し、自己評価の実施と結果の提出を依頼している。

ビー支店で情報セキュリティリーダーをつとめるシーシは、監査部から送付されてきた自己評価シートに従って、職場の状況を観察したり、従業員にヒアリングしたりして評価した。自己評価シートの評価結果は図1の判定ルールに従って記入する。シーシが作成したビー支店の評価結果をひょう1にしめす。。

図1。評価結果の判定ルール。。

評価項目通りに実施している場合、オーケー。。

評価項目どおりに実施していないが、だいたいコントロールによってオーケーの場合と同程度にリスクが低減されていると考えられる場合、オーケー、かっこだいたいコントロールを具体的に評価根拠ランに記入する。。

評価項目どおりに実施しておらず、かつ、だいたいコントロールによって評価項目にかんするリスクがおさえられていないと考えられる場合、エヌジー。。

評価項目に関するリスクがそもそも存在しない場合、えぬえー。

ひょう1。ビー支店の評価結果、ばっすい。。

10ばん。評価項目。省略。評価結果。オーケー。評価根拠。省略。。

19ばん。ファイルサーバじょうの顧客情報のアクセス権は最小権限の原則にもとづいて設定される。えー。。

25番。省略。オーケー。省略。

せつもん。ひょう1ちゅうのえーにいれる字句はどれか？。解答群のうち、最も適切なものを選べ。。

えーに関する解答群。。

ア。評価結果。オーケー。評価根拠。アクセス権の設定状況が適切であることを確認した。。

イ。オーケー。アクセス権を適切に設定するルールが存在することを確認した。。

ウ。オーケー。ファイルサーバは情報システム部が運用管理している。。

エ。えぬえー。顧客情報をファイルサーバに保存することは禁止されている。

せいかいわ。ア。評価結果。オーケー。評価根拠。アクセス権の設定状況が適切であることを確認したです。

該当箇所を見てみましょう。ビー支店のファイルのアクセス権は、当該ファイルを保存した従業員が最小権限の原則にもとづいて設定するとあり、今年のヒアリングでそのとおりにせっていされていることを確認したとあります。

ということで、正解は、あ、となります。。。これも簡単でしたね

とい58。国内外に複数の子会社をもつえーしゃでは、インターネットに公開するwebサイトについて、えーしゃグループの脆弱性診断基準、以下、えーしゃグループ基準という、をもうけている。えーしゃの子会社であるびーしゃは、会員向けに製品を販売するwebサイト、以下、ビーしゃサイトという、を運営している。びーしゃサイトは、会員だけがびーしゃの製品やサービスを検索できる。会員の氏名、メールアドレスなどの会員情報も管理している。びーしゃでは、11がつに情報セキュリティ活動の一環として、えーしゃグループ基準をもとに自己点検を実施し、その結果をひょう1のとおりまとめた。

ひょう1。びーしゃ自己点検結果、抜粋。。

こうばん1。点検項目。Webアプリケーションプログラム、以下、webアプリという、に対する脆弱性診断の実施。えーしゃグループ基準。インターネットに公開しているwebサイトについて、webアプリの新規開発時、および機能追加時におこなう。

機能塚などの変更がない場合でも、ねんいっかい以上おこなう。

点検結果。3年前にびーしゃさいとをリリースするいっかげつ前に、webアプリに対する脆弱性診断をおこなった。リリース移行は実施していない。

3年前の脆弱性診断では、軽微な脆弱性がにけん検出された。。

こうばん2。OSおよびミドルウェアに対する脆弱性診断の実施。インターネットに公開しているwebサイトについて、ねんいっかい以上おこなう。

昨年しがつおよび10月に、びーしゃサイトに対しておこなっている。今年しがつの脆弱性診断では、脆弱性が3件検出された。

こうばん3。脆弱性診断結果の報告。webアプリ、OSおよびミドルウェアに対する脆弱性診断をおこなった場合、その結果を、診断後にかげつ以内に各社の情報セキュリティ委員会に報告する。三年前にwebアプリに対する脆弱性診断をおこなった二週間後に、結果を情報セキュリティ委員会に報告した。OSおよびミドルウェアに対する脆弱性診断の結果は、しがつと10がつそれぞれの月末の情報セキュリティ委員会に報告した。。

こうばん4。脆弱性診断結果の対応。webアプリ、OSおよびミドルウェアに対する脆弱性診断で、脆弱性が発見された場合、緊急をようする脆弱性については、診断後、いっかげついないに対応する。指定された期限までの対応が困難な場合、対応の時期を明確にし、最高情報セキュリティ責任者、シーアイエスオーのしょうにんを得る。

３年前に検出したwebアプリの脆弱性にけんについて、びーしゃサイトのリリースいっしゅうかんまえに対応した。

ことししがつに検出したOSおよびミドルウェアに対する脆弱性のうち、にけんは翌日に対応した。のこりいっけんは、恒久的な対策は来年いちがつのびーしゃサイトのこうかいじに対応するものとし、それまでは、設定変更による暫定対策をとるという対応計画について、脆弱性診断のとおかごにシーアイエスオーの承認をえた。

せつもん。ひょう1ちゅうの自己点検の結果のうち、えーしゃグループ基準をみたすこうばんだけを全て挙げた組み合わせを解答群のなかから選べ。。

なお、解答群の読み上げは今回も省略いたします。。

せいかいわ。ク。に、さん、よんです

それではそれぞれを見ていきましょう。。

こうばん1は、機能追加などの変更がない場合でも脆弱性診断をいちねんに一回以上おこなうとありますが、残念ながら3年前のリリースいこうはおこなっていないとあります。

よってこうばん1は不適合となります。。

こうばん2は、グループ基準にしたがって年ににかい脆弱性診断をおこなっているのでてきごうですね。

こうばん3も、グループ基準にしたがい、脆弱性診断ごにかげついないにじっしされていますね。。

こうばん4も、脆弱性診断ごいっかげついないに対応し、期限までにたいおうができないものについても適切にたいおうしていますね。

よってせいかいわ。ク。に、さん、よんとなります。。。これも簡単でしたね～

とい59。えーしゃは従業員200めいの通信販売業者である。一般消費者向けに生活雑貨、ギフト商品などの販売を手掛けている。取り扱い商品の一つである商品ゼットは、ゼット販売課が担当している。

ゼット販売課の業務。

現在、ゼット販売課の要因は、商品ゼットについての受注管理業務および問い合わせ対応業務をおこなっている。商品ゼットについての受注管理業務の手順を図1にしめす。

商品ゼットの顧客からの注文は電子メールで届く。

1。入力。

販売担当者は、届いた注文、変更、キャンセル含むの内容を受注管理システム、かっこいち、以下、ジェイシステムという、に入力し、販売責任者、かっこ2に承認を依頼する。。

2。承認。

販売責任者は、注文の内容とジェイシステムへの入力結果を突き合わせて確認し、問題が無ければ承認する。問題があれば差し戻す。。

ちゅういち。えーしゃ情報システム部が運用している。利用者は、販売責任者、販売担当者などである。。

ちゅうに。ゼット販売課の課長いちめいだけである。

ジェイシステムの操作権限。。

ゼット販売課では、ジェイシステムについて、つぎの利用方針を定めている。。

方針1。ある利用者が入力した情報は、別の利用者が承認する。。

方針2。販売責任者は、ゼット販売課の全業務の情報を閲覧できる。。

ジェイシステムでは、業務上必要な操作権限を利用者に与える機能が実装されている。このたび、商品ゼットの受注管理業務が受注増によって増えていることから、びーしゃに一部を委託することにした。以下、商品ゼットの受注管理業務の入力作業をおこなうびーしゃ従業員を商品ゼットのびーしゃ販売担当者といい、商品ゼットのびーしゃ販売担当者の入力結果をチェックするびーしゃ従業員を商品ゼットのびーしゃ販売責任者という

委託にあたって、ゼット販売課は情報システム部にジェイシステムに関する次の要求事項を伝えた。。

要求1。びーしゃが入力した場合は、えーしゃが承認する。。

要求2。えーしゃの販売担当者が入力した場合は、現状どおりにえーしゃの販売責任者が承認する。。

じょうきをふまえ、情報システム部は今後のかく利用者に付与される操作権限をひょう1にまとめた。

ひょう1。操作権限案。。

ひょうのよみあげが省略いたします。。

ちゅうき。まるは操作権限がふよされることをしめす。。

せつもん。ひょう1ちゅうのえーにいれる適切なじくを解答群のなかから選べ。。

解答群。。

ア。ゼット販売課の販売責任者。。

イ。ゼット販売課の販売担当者。。

ウ。ゼット販売課のよういん。。

エ。商品ゼットのびーしゃ販売責任者。。

オ。商品ゼットのびーしゃ販売担当者。

せいかいわ。ア。ゼット販売課の販売責任者です。。。

閲覧と承認に権限があるところがポイントですね。

それでは該当箇所を見てみましょう。

要求事項をみてみると、承認権限があるのはどちらもえーしゃであり、えーしゃのなかでも販売責任者であることがわかります。

ということで、解答群から選ぶべきせいかいわ。ア。ゼット販売課の販売責任者になります。。

これも即答できますね

とい60。えーしゃは輸入食材をあつかう商社である。ある日、経理課のビー課長は、えーしゃの海外子会社であるしーしゃのでぃーさんからの不審な点がある電子メール、以下、メールという、を受信した。ビー課長は、えーしゃの情報システム部に調査を依頼した。えーしゃの情報システム部がしーしゃの情報システム部と協力して調査した結果を図1に示す。

1。ビー課長へのヒアリングならびに受信したメールおよび添付されていた請求書からは、つぎが確認された。。

こうばん1。でぃーさんが早急な対応を求めたことは今まで一回もなかったが、メール本文では送金先の口座を早急に変更するよう求めていた。。

こうばん2。添付されていた請求書は、えーしゃがしーしゃに支払う予定で進めている請求書であり、しーしゃがさんかげつまえから利用を開始したテンプレートを利用したものだった。。

こうばん3。添付されていた請求書は、振込先が、しーしゃが所在するくにではないくににある銀行のこうざだった。。

こうばん4。添付されていた請求書が作成されたPCのタイムゾーンは、しーしゃのタイムゾーンと異なっていた。。

こうばん5。メールの送信者、フロムのメールアドレスには、しーしゃのドメインめいとは別の類似するドメインめいが利用されていた。。

こうばん6。メールの返信先、リプライ、トゥはでぃーさんのメールアドレスではなく、フリーメールのものであった。。

こうばん7。メール本文では、ビー課長とディーさんの間でろっかげつまえから何度かやり取りしたメールの内容を引用していた。。

2。不正ログインしたものが、以降のメール不正閲覧の発覚を避けるために実施したと推察される設定変更がディーさんのメールアカウントに確認された。

せつもん。ビー課長に疑いをもたれないようにするためにメールの送信者が使った手口として考えられるものはどれか？。図1に示すかくこうばんのうち、該当するものだけをすべて挙げた組み合わせを、解答群のなかからえらべ。。

解答群の読み上げはいみがないため省略いたします。

せいかいわ。カ。こうばん2。こうばん5。こうばん7です

それではず1をみてみましょう。。

ビー課長に疑いをもたれないようにするための手口という観点でみてみると、

こうばん1は、急がせているだけなので不適切ですね。。

こうばん2は、請求書のテンプレートがさんかげつまえから使用されていたあたらしいものを使用していますね。よってこれは適切です。。

こうばん3と4は違うくにからおこなわれたということをしめしているので不適切です。。

こうばん5は、よくあるドメインさしょうなので適切です。。

こうばん6は、メールの返信先がフリーメールであるというだけなので不適切です。。

こうばん7は、ビー課長とディーさんとのあいだでろっかげつまえからやりとりをしていたメールの内容を引用しているということで、だましに来ています。よって適切です。

ということで、せいかいわ。カ。こうばん2。こうばん5。こうばん7です