とい1。びーいーしー、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偽の電子メールを送り、金銭をだまし取る。。

イ。送信元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。誹謗中傷メールの送信元を攻撃対象の組織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偽の電子メールを送り、金銭をだまし取るです

とい2。参加組織及びそのグループ企業において検知されたサイバー攻撃などの情報を、IPAが情報ハブになって集約し、参加組織間で共有するとりくみはどれか？。。

ア．くりぷとれっく。。

イ．しーさーと。。

ウ．じぇいしっぷ。。

エ．じぇいあいせっく

せいかいわ。ウ．じぇいしっぷです

それぞれの選択肢についてもご紹介いたします。。

くりぷとれっく。。

電子政府推奨暗号の安全性を評価、監視し、暗号技術の適切な実装法、運用法を調査、検討するプロジェクトのことです。。。

しーさーと。。

対象とする範囲でセキュリティ上の問題が起きていないかどうかを監視するとともに、発生したセキュリティインシデントについて対応するチームや組織の総称のことです。。。

じぇいあいせっく。。

IT関連製品のセキュリティ機能の適切性、確実性を、セキュリティ評価基準の国際標準であるあいえすおーあいいーしー15408に基づいて第三者、評価機関が評価し、その評価結果を認証機関が認証する制度のことです。

とい3。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、りすく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、リスク分析前に行うこと。。

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、対象外ではなく、すべて対象にすることが正しいです。。

うわ、リスク分析前に行うのではなく、リスク分析後に行うことが正しいです。。

えわ、リスク対応後に決定するのではなく、リスク対応プロセスで行うことが正しいです。

とい4。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。第4版に照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漏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上で、具体的な範囲を設定しない包括的な競業ひし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等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行われやすいので、退職予定者に対する重要情報へのアクセスや媒体の持ち出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行われやすいので、退職予定者に対する重要情報へのアクセスや媒体の持ち出しの監視を強化するです。。

なお、あわ、対象の明示、重要情報を客観的に特定できるようにする必要があるため不適切です。。

いわ、職業選択の自由の制限は憲法違反なので不適切です。。

うわ、退職後は速やかに無効化する必要があるため不適切です。

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？。。

あ。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

他の選択肢についてもご紹介いたします。。

継続的改善は、パフォーマンスを向上するために繰り返し行われる活動のことです。。。

修正は、検出された不適合を除去するための処置のことです。。。

リスクアセスメントは、リスク特定，リスク分析及びリスク評価のプロセス全体のことです。

とい6。ネットワークカメラなどのアイオーティー機器ではTCP23番ポートへの攻撃が多い理由はどれか？。。

ア．TCP23番ポートは、アイオーティー機器の操作用プロトコルで使用されており、そのプロトコルを用いると、初期パスワードを使って不正ログインが容易に成功し、不正にアイオーティー機器を操作できることが多いから。。

イ．TCP23番ポートは、アイオーティー機器の操作用プロトコルで使用されており、そのプロトコルを用いると、マルウェアを添付した電子メールをアイオーティー機器に送信するという攻撃ができることが多いから。。

ウ．TCP23番ポートは、アイオーティー機器へのメール送信用プロトコルで使用されており、そのプロトコルを用いると、初期パスワードを使って不正ログインが容易に成功し、不正にアイオーティー機器を操作できることが多いから。。

エ．TCP23番ポートは、アイオーティー機器へのメール送信プロトコルで使用されており、そのプロトコルを用いると、マルウェアを添付した電子メールをアイオーティー機器に送信するという攻撃ができることが多いから。

せいかいわ。ア．TCP23番ポートは、アイオーティー機器の操作用プロトコルで使用されており、そのプロトコルを用いると、初期パスワードを使って不正ログインが容易に成功し、不正にアイオーティー機器を操作できることが多いからです。。

TCP23番ポートはテルネットです。テルネットは、遠隔地からネットワークを通じて別のコンピュータをリモート操作するためのプロトコルになります。。

よって、他の選択肢はメールに関連するものになるので不適切となります。

とい７。SPF、せんだーぽりしーふれーむわーくの仕組みはどれか？。。

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、送信元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、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。。

エ．電子メールを送信するサーバが、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

せいかいわ。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、送信元ドメインの詐称がないことを確認するです。。

なお、あわ、でぃーきむ、ドメインキーズアイデンティファイドメールの仕組みなので不適切です。。

うわ、メールアーカイブの仕組みなので不適切です。。

えわ、上長承認機能や第三社承認機能のことなので不適切です。

とい8。A社では現在、インターネット上のWebサイトを内部ネットワークのPC上のWebブラウザから参照している。新たなシステムを導入し、DMZ上に用意した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、インターネット上のWebサイトをVDIサーバ上の仮想デスクトップのWebブラウザ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上の効果はどれか？。。

ア。インターネット上の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。インターネット上の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及び仮想デスクトップのOSがボットに感染しなくなり、しーあんどし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、他のPCに感染するのを防ぐ。

せいかいわ。ア。インターネット上の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。。

なお、いの、MITB攻撃にはトランザクション署名が有効です。。

うわ、仮想デスクトップはボット感染の可能性があるため不適切です。。

えわ、VDIはマルウェアに感染したPCからの感染拡大を防ぐ技術ではないので不適切です

とい9。じすきゅー27001、2014には記載されていないが、じすきゅー27017、2016において記載されている管理策はどれか？。。

ア。クラウドサービス固有の情報セキュリティ管理策。。

イ。事業継続マネジメントシステムにおける管理策。。

ウ。情報セキュリティガバナンスにおける管理策。。

エ。制御システム固有のサイバーセキュリティ管理策

せいかいわ。ア。クラウドサービス固有の情報セキュリティ管理策です。。

なお、いわ、じすきゅー22301の管理策。。

うわ、じすきゅー27014の管理策。。

えわ、CSMS、サイバーセキュリティマネージメントシステムの管理策です

とい10。シャドーITに該当するものはどれか？。。

ア。IT製品やITを活用して地球環境への負荷を低減する取組。。。

イ。IT部門の許可を得ずに、従業員又は部門が業務に利用しているデバイスやクラウドサービス。。。

ウ。攻撃対象者のディスプレイやキータイプを物陰から盗み見て,情報を盗み出す行為。。。

エ。ネットワーク上のコンピュータに侵入する準備として、侵入対象の弱点を探るために組織や所属する従業員の情報を収集すること

せいかいわ。イ。IT部門の許可を得ずに、従業員又は部門が業務に利用しているデバイスやクラウドサービスです。。。

なお、あわ、グリーンITのことです。。

うわ、盗み見、ショルダーハッキングことです。。

えわ、フットプリンティングのことです

とい11。ステガノグラフィはどれか？。。

ア。画像などのデータの中に、秘密にしたい情報を他者に気付かれることなく埋め込む。。

イ。検索エンジンの巡回ロボットにWebページの閲覧者とは異なる内容を応答し、該当Webページの検索順位が上位に来るようにする。。

ウ。検査対象の製品に、問題を引き起こしそうなジェイペグ画像などのテストデータを送信し読み込ませて、製品の応答や挙動から脆弱性を検出する。。

エ。コンピュータには認識できないほどゆがんだ文字を画像として表示し、利用者に文字を認識させて入力させることによって、利用者が人であることを確認する。

せいかいわ。ア。画像などのデータの中に、秘密にしたい情報を他者に気付かれることなく埋め込むです。。。

なお、いわ、クローキングのこと。。

うわ、ファジングのこと。。

えわ、きゃぷちゃのことです。

とい12。セキュアハッシュ関数しゃーにーごーろくを用いて、ファイルA及びファイルBのハッシュちを算出すると、どちらも全く同じ次に示すハッシュちえぬ、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ちを算出すると、ファイルAとファイルBのハッシュちが異なる。。

イ。ファイルAとファイルBのハッシュちえぬのデータ量は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のハッシュちの桁数は、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。。。

なお、あわ、ハッシュちが異なるというてんが不適切です。。。

いわ、256ビットをバイトにするには8ビットで割ればよいので、32バイトとわかり、64バイトは不適切であることが分かります。

うわ、入力値の長さに関係なく同じ長さのハッシュちを生成するため、64桁が適切です

とい13。インターネットバンキングでのMITB攻撃による不正送金について、対策として用いられるトランザクション署名の説明はどれか？。。

ア。携帯端末からの送金取引の場合、金融機関から携帯端末の登録メールアドレスに送金用のワンタイムパスワードを送信する。。

イ。特定認証業務の認定を受けた認証局が署名したディジタル証明書をインターネットバンキングでの利用者認証に用いることによって、ログインパスワードが漏えいした際の不正ログインを防止する。。

ウ。利用者が送金取引時に、送金処理を行うPCとは別のデバイスに振込先口座番号などの取引情報を入力して表示されたあたいをインターネットバンキングに送信する。。

エ。ログイン時に、送金処理を行うPCとは別のデバイスによって、一定時間だけ有効なログイン用のワンタイムパスワードを算出し、インターネットバンキングに送信する。

せいかいわ。ウ。利用者が送金取引時に、送金処理を行うPCとは別のデバイスに振込先口座番号などの取引情報を入力して表示されたあたいをインターネットバンキングに送信するです。。。

なお、あわ、要素認証の説明です。。

いわ、クライアント認証の説明です。。

えわ、一定時間だけ有効なログイン用のワンタイムパスワードを使用することは、「不正ログイン」対策ではありません。

とい14。わふにおけるフォールスポジティブに該当するものはどれか？。。

ア。HTMLの特殊文字、しょうなりを検出したときに通信を遮断するようにわふを設定した場合、しょうなりなどの数式を含んだ正当なHTTPリクエストが送信されたとき、わふ が攻撃として検知し、遮断する。。

イ。HTTPリクエストのうち、RFCなどに仕様が明確に定義されておらず、Webアプリケーションソフトウェアの開発者が独自の仕様で追加したフィールドについてはわふが検査しないという仕様を悪用して、攻撃の命令を埋め込んだHTTPリクエストが送信されたとき、わふが遮断しない。。

ウ。HTTPリクエストのパラメタとして許可する文字列以外を検出したときに通信を遮断するようにわふを設定した場合、許可しない文字列を含んだ不正なHTTPリクエストが送信されたとき、わふが攻撃として検知し、遮断する。。

エ。悪意のある通信を正常な通信と見せかけ、HTTPリクエストを分割して送信されたとき、わふが遮断しない。

せいかいわ。ア。HTMLの特殊文字、しょうなりを検出したときに通信を遮断するようにわふを設定した場合、しょうなりなどの数式を含んだ正当なHTTPリクエストが送信されたとき、わふが攻撃として検知し、遮断するです。。。

なお、いわ、わふが検査しないという仕様を悪用するという点から、フォールすネガティブであることが分かるため該当しません。。

うわ。正常な動作であることから該当しません。。

えわ、悪意のある通信を正常な通信と見せかけという点から、フォールスネガティブであることが分かるため該当しません

とい15。ボットネットにおいて、しーあんどしーサーバが担う役割はどれか？。。

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。攻撃の踏み台となった複数のサーバからの通信を制御して遮断する。。

ウ。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。。

エ。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。

せいかいわ。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です。。。

なお、しーあんどしーは、コマンドアンドコントロールの略です。

とい16。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。これによって、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

せいかいわ。イ。A社WebサーバにアクセスしようとするB社従業員です。。。

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と記載されていることから、A社ドメインに対する名前解決要求をB社キャッシュサーバに行うと、サーバXのIPアドレスが返され、攻撃者の用意したサーバXにアクセスさせられてしまうということがわかります。

とい17。PCとサーバとの間でIPせっくによる暗号化通信を行う。通信データの暗号化アルゴリズムとしてAESを使うとき、用いるべき鍵はどれか？。。

ア。PCだけが所有する秘密鍵。。

イ。PCとサーバで共有された共通鍵。。

ウ。PCの公開鍵。。

エ。サーバの公開鍵

せいかいわ。イ。PCとサーバで共有された共通鍵です。。。AESは共通鍵暗号方式の暗号化アルゴリズムです。。。詳しくは個別動画をご覧ください。

とい18。WPAスリーはどれか？。。

ア。HTTP通信の暗号化規格。。

イ。TCP、IP通信の暗号化規格。。

ウ。Webサーバで使用するディジタル証明書の規格。。

エ。無線ランのセキュリティ規格

せいかいわ。エ。無線ランのセキュリティ規格です。。。なお、あわ、TLSまたはHTTPSです。。。いわ、IPせっくです。。。うわ、ITUTX509証明書です。

とい19。リバースブルートフォース攻撃に該当するものはどれか？。。

ア。攻撃者が何らかの方法で事前に入手した利用者IDとパスワードの組みのリストを使用して、ログインを試行する。。

イ。パスワードをひとつ選び、利用者IDとして次々に文字列を用意して総当たりにログインを試行する。。

ウ。利用者ID、及びその利用者IDと同一の文字列であるパスワードの組みを次々に生成してログインを試行する。。

エ。利用者IDをひとつ選び、パスワードとして次々に文字列を用意して総当たりにログインを試行する。

せいかいわ。イ。パスワードをひとつ選び、利用者IDとして次々に文字列を用意して総当たりにログインを試行するです。。。なお、あわ、パスワードリスト攻撃。。。うわ、ジョーアカウント攻撃。。。えわ、ブルートフォース攻撃、総当たり攻撃に該当します。

とい20。ディジタル署名に用いる鍵の組のうち、適切なものはどれか？。。

あ。ディジタル署名の作成に用いる鍵、共通鍵。。ディジタル署名の検証に用いる鍵。秘密鍵。。。

い。ディジタル署名の作成に用いる鍵、公開鍵。。ディジタル署名の検証に用いる鍵。秘密鍵。。。

う。ディジタル署名の作成に用いる鍵、秘密鍵。。ディジタル署名の検証に用いる鍵。公開鍵。。。

え。ディジタル署名の作成に用いる鍵、秘密鍵。。ディジタル署名の検証に用いる鍵。公開鍵。。。

せいかいわ。う。ディジタル署名の作成に用いる鍵、秘密鍵。。ディジタル署名の検証に用いる鍵。公開鍵です。。。

ディジタル署名は公開鍵暗号方式を用いるため、いとえは不適切です。。あわ、作成と検証に用いる鍵が逆になっているため不適切です。

とい21。情報セキュリティにおいてバックドアに該当するものはどれか？。。

ア。アクセスする際にパスワード認証などの正規の手続が必要なWebサイトに、当該手続を経ないでアクセス可能なURL。。

イ。インターネットに公開されているサーバのTCPポートの中からアクティブになっているポートを探して、稼働中のサービスを特定するためのツール。。

ウ。ネットワーク上の通信パケットを取得して通信内容を見るために設けられたスイッチのLANポート。。

エ。プログラムが確保するメモリ領域に、領域の大きさを超える長さの文字列を入力してあふれさせ、ダウンさせる攻撃

せいかいわ。ア。アクセスする際にパスワード認証などの正規の手続が必要なWebサイトに、当該手続を経ないでアクセス可能なURLです。。

なお、いわ、ポートスキャナの説明です。。うわ、ミラーポートの説明です。。えわ、バッファオーバーフローの説明です。

とい22。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既知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上で実行し、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上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コードから検体の機能を調べる。。

エ。ハードディスク内のファイルの拡張子とファイルヘッダの内容を基に、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上で実行し、その動作や外部との通信を観測するです。。マルウェアの動的解析はブラックボックス解析とも呼ばれます。。

なお、あわ、コンペア法のこと。。うわ、ホワイトボックス解析のこと。。えわ、マルウェア検出手法のことです

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、ブロック暗号を用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。う。メッセージ認証符号です。。これは、マック、メッセージオーセンティケーションコードとも呼ばれます。。

なお、あわ、公開鍵基盤のこと。。いわ、伝送時のデータ誤りを検出するために付加される検査用ビットのこと。。えわ、ルートCAが発行した証明書のことです

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、乱数表の指定したマス目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行う。。

エ。利用者の記憶、持ち物、身体の特徴のうち、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行うです。。。

なお、あわ、マトリクスコード認証のことなので非該当。。いわ、全てのアクセスに対しては、リスクベース認証は行わないため非該当。。えわ、多要素認証のことなので非該当です。

とい25。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。このとき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掛かる。。

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掛かるです。。

なお、いわ、DNS情報は改ざんされないため不適切です。。

うわ、不正なあたいをちゅうにゅうされないため不適切です。。

えわ、ゾーン情報を不正に入手されるものではないため不適切です

とい26。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。。

選択肢。。

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箇所の修正。。

エ。電子メールの本文の内容の漏えいの防止

せいかいわ。エ。電子メールの本文の内容の漏えいの防止です。。。

なお、あわ、電子メールの送達確認。。いわ。なりすましの検出。。うわ。改ざん箇所の修正というところが誤りとなります

とい27。クレジットカードなどのカード会員データのセキュリティ強化を目的として制定され、技術面及び運用面の要件を定めたものはどれか？。。

ア。ISMS適合性評価制度。。

イ。PCI DSS。。

ウ。特定個人情報保護評価。。

エ。プライバシーマーク制度。。

せいかいわ。イ。PCI DSSです。。。聞き流し動画でも紹介しておりますが、ぺいぺい、クレカ、いいですという語呂合わせで覚えましょう

とい28。電子メールをドメインAの送信者がドメインBの宛先に送信するとき、送信者をドメインA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。ぽっぷすりーえす。。ウ。えすまいむ。。エ。SMTPおーす

せいかいわ。エ。SMTPおーすです。。。

なお。あ。エーポップは、メール受信の際に、チャレンジレスポンス方式の認証を行うことでひらぶんの認証情報がネットワークに流れるのを防止するプロトコルのことです。。

い。ぽっぷすりーえすは、TLSのセキュアな通信路上でメールソフトからメールサーバ間のぽっぷ通信を行うプロトコルのことです。。

う。えすまいむは、公開鍵暗号技術を使用して認証、改ざん検出、暗号化などの機能を電子メールソフトに提供するものです。

とい19。ハニーポットの説明はどれか？。。

ア。サーバやネットワークを実際の攻撃に近い手法で検査することによって、もし実際に攻撃があった場合の被害の範囲を予測する。。

イ。社内ネットワークに接続しようとするPCを、事前に検査専用のネットワークに接続させ、セキュリティ状態を検査することによって、安全ではないPCの接続を防ぐ。。

ウ。保護された領域で、検査対象のプログラムを動作させることによって、その挙動からマルウェアを検出して、隔離及び駆除を行う。。

エ。わざと侵入しやすいように設定した機器やシステムをインターネット上に配置することによって、攻撃手法やマルウェアの振る舞いなどの調査と研究に利用する。

せいかいわ。エ。わざと侵入しやすいように設定した機器やシステムをインターネット上に配置することによって、攻撃手法やマルウェアの振る舞いなどの調査と研究に利用するです。。。

なお、あわ、ペネトレーションテストの説明。。いわ、検疫ネットワークの説明。。うわ、サンドボックスの説明となります。

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ないことを調べる。。

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。。。

くわしくは個別動画をご覧ください。

とい31。企業において業務で使用されているコンピュータに、記憶媒体を介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者がいたとき、その者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。。。よく出る問題なので今回で覚えておきましょう

＊法改正により没問

問32。技術者の活動に関係する法律のうち、罰則規定のないものはどれか？。。

ア。公益通報者保護法。。。イ 個人情報保護法 。。。ウ。特許法。。。エ。不正競争防止法

とい33。シュリンクラップ契約において、ソフトウェアの使用許諾契約が成立するのはどの時点か？。。

ア。購入したソフトウェアの代金を支払った時点。。

イ。ソフトウェアの入ったDVDろむを受け取った時点。。

ウ。ソフトウェアの入ったDVDろむの包装を解いた時点。。

エ。ソフトウェアをPCにインストールした時点

せいかいわ。ウ。ソフトウェアの入ったDVDろむの包装を解いた時点です。。。

シュリンクラップ契約とは、ソフトウェアのパッケージを開封することで使用許諾契約に同意したとみなす契約方式です。

とい34。A社は、B社と著作物の権利に関する特段の取決めをせず、A社の要求仕様に基づいて、販売管理システムのプログラム作成をB社に委託した。この場合のプログラム著作権の原始的帰属に関する記述のうち、適切なものはどれか？。。

ア。A社とB社が話し合って帰属先を決定する。。

イ。A社とB社の共有帰属となる。。

ウ。A社に帰属する。。

エ。B社に帰属する。

せいかいわ。エ。B社に帰属するです。。。

A社とB社は著作物の権利に関する特段の取り決めをせず、販売管理システムのプログラムさくせいをB社に委託した。というところがポイントとなります

とい35。A社は、A社で使うソフトウェアの開発作業をB社に実施させる契約を、B社と締結した。締結した契約が労働者派遣であるものはどれか？。。

ア。A社監督者が、B社の雇用する労働者に、業務遂行に関する指示を行い、A社の開発作業を行わせる。。

イ。B社監督者が、B社の雇用する労働者に指示を行って成果物を完成させ、A社の監督者が成果物の検収作業を行う。。

ウ。B社の雇用する労働者が、A社の依頼に基づいて、B社指示の下でB社所有の機材、設備を使用し、開発作業を行う。。

エ。B社の雇用する労働者が、B社監督者の業務遂行に関する指示の下、A社施設内で開発作業を行う。

せいかいわ。ア。A社監督者が、B社の雇用する労働者に、業務遂行に関する指示を行い、A社の開発作業を行わせるです。。。

ほかの選択肢は、全て請負契約になり、えにかんしてわ、いわゆる客先常駐のことを指します

とい36。常時10名以上の従業員を有するソフトウェア開発会社が、社内の情報セキュリティ管理を強化するために、秘密情報を扱う担当従業員の扱いを見直すこととした。労働法に照らし、適切な行為はどれか？。。

ア。就業規則に業務上知り得た秘密の漏えい禁止の一般的な規定があるときに、担当従業員の職務に即して秘密の内容を特定する個別合意を行う。。

イ。就業規則には業務上知り得た秘密の漏えい禁止の規定がないときに、漏えい禁止と処分の規定を従業員の意見を聴かずに就業規則に追加する。。

ウ。情報セキュリティ事故を起こした場合の処分について、担当従業員との間で、就業規則よりも処分の内容を重くした個別合意を行う。。

エ。情報セキュリティに関連する規定は就業規則に記載してはいけないので、就業規則に規定を設けずに、各従業員と個別合意を行う。

せいかいわ。ア。就業規則に業務上知り得た秘密の漏えい禁止の一般的な規定があるときに、担当従業員の職務に即して秘密の内容を特定する個別合意を行うです。。。

いわ、従業員の意見を聞く必要があるため不適切です。。

うわ、就業規則よりも処分の内容を重くすることはできないため不適切です。。

えわ、情報セキュリティに関連する規定は就業規則に記載しなければならないため不適切です。

とい37。入出金管理システムから出力された入金データファイルを、売掛金管理システムが読み込んでマスタファイルを更新する。入出金管理システムから売掛金管理システムに受け渡されたデータの正確性及び網羅性を確保するコントロールはどれか？。。

ア。売掛金管理システムにおける入力データと出力結果とのランツーランコントロール。。

イ。売掛金管理システムのマスタファイル更新におけるタイムスタンプ機能。。

ウ。入金額及び入金データ件数のコントロールトータルのチェック。。

エ。入出金管理システムへの入力のエディットバリデーションチェック

せいかいわ。ウ。入金額及び入金データ件数のコントロールトータルのチェックです。。。

コントロールトータルのチェックとは、コンピューターで入力されたデータの項目について、処理する前に別の方法で合計したあたいと、処理後の合計ちを比較して入力ミスなどを確認する手法です。

とい38。金融庁、財務報告に係る内部統制の評価及び監査の基準、平成23年に基づいて、内部統制の基本的要素を、統制環境、リスクの評価と対応、統制活動、情報と伝達、モニタリング、ITへの対応のむっつに分類したときに、統制活動に該当するものはどれか？。。

ア。経営者が自らの意思としての経営方針を全社的に明示していること。。

イ。情報システムの故障、不具合に備えて保険契約に加入しておくこと。。

ウ。内部監査部門が定期的に業務監査を実施すること。。

エ。発注業務と検収業務をそれぞれ別の者に担当させること

せいかいわ。エ。発注業務と検収業務をそれぞれ別の者に担当させることです。。。

なお、あわ、統制環境に該当します。。いわ、リスクの評価と対応に該当します。。。

うわ、モニタリングに該当します

とい39。データの生成から入力、処理、出力、活用までのプロセス、及び組み込まれているコントロールを、システム監査にんが書面上で又は実際に追跡する技法はどれか？。。

ア。インタビュー法。。イ。ウォークスルー法。。ウ。監査モジュール法。。

エ。ペネトレーションテスト法

せいかいわ。イ。ウォークスルー法です。。。

他の選択肢についてもご紹介いたします。。

インタビュー法は、システム監査にんが、監査対象へ直接口頭で問い合わせる手法です。。

監査モジュール法は、システム内に組み込まれた監査モジュールを使ってリアルタイムの監査を行う手法です。。

ペネトレーションテスト法は、外部攻撃者になりすましてシステムの脆弱性を発見するための攻撃シミュレーション法です。

とい40。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程を閲覧した。。

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程を閲覧したです。。。

システム監査人は主体的に改善活動を行いません。

とい41。ITサービスマネジメントにおいて、サービスに対する計画外の中断、サービスの品質の低下、又は顧客へのサービスにまだ影響していない事象を何というか？。。

ア。インシデント。。イ。既知の誤り。。ウ。変更要求。。エ。問題

せいかいわ。ア。インシデントです。

とい42。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、エラープルーフ化がある。運用作業におけるエラープルーフ化の例として、最も適切なものはどれか？。。

ア。画面上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。長時間に及ぶシステム監視作業では、疲労が蓄積しないように、2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。臨時の作業を行う際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行う。

せいかいわ。ア。画面上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。。。

詳しくは個別動画をご覧ください。

とい43。プロジェクトライフサイクルの一般的な特性はどれか？。。

ア。開発要員数は、プロジェクト開始時が最多であり、プロジェクトが進むにつれて減少し、 完了に近づくと再度増加する。。

イ。ステークホルダがコストを変えずにプロジェクトの成果物に対して及ぼすことができる影響の度合いは、プロジェクト完了直前が最も大きくなる。。

ウ。プロジェクトが完了に近づくほど、変更やエラーの修正がプロジェクトに影響する度合いは小さくなる。。

エ。リスクは、プロジェクトが完了に近づくにつれて減少する。

せいかいわ。エ。リスクは、プロジェクトが完了に近づくにつれて減少するです。。。

なお、あわ、完了に近づくと開発要員は減少するため不適切です。。

いわ、成果物への影響度合いはプロジェクトが完了に近づくと減少するため不適切です。。

うわ、修正の影響はプロジェクトが完了に近づくと減少するため不適切です。

とい44。あるプロジェクトの日程計画をアローダイアグラムで示す。クリティカルパスはどれか？。。

ア。えー、しー、いー、えふ。。イ。えー、でぃー、じー。。ウ。びー、いー、えふ。。

エ。びー、いー、じー

せいかいわ。ウ。びー、いー、えふです。。。

クリティカルパスとは、プロジェクト管理において、プロジェクトの全工程で最も所要時間が長く、スケジュールに影響が出る作業経路のことです。。

それぞれの選択肢を計算すると、

あが13日。いが8日。うが14日。えが13日となるため、うが正解と分かります。

とい45。Webシステムの性能指標のうち、応答時間の説明はどれか？。。

ア。Webブラウザに表示された問合せボタンが押されてから、Webブラウザが結果を表示し始めるまでの時間。。

イ。Web ブラウザを起動してから、最初に表示するようにあらかじめ設定したWebページの全てのデータ表示が完了するまでの時間。。

ウ。サーバ側のトランザクション処理が完了してから、Webブラウザが結果を表示し始めるまでの時間。。

エ。ダウンロードを要求してから、ダウンロードが完了するまでの時間

せいかいわ。ア。Webブラウザに表示された問合せボタンが押されてから、Webブラウザが結果を表示し始めるまでの時間です。。。

レスポンスタイムとは、システムや装置などに処理の実行指示を与えてから最初の応答を得るまでの時間を指し、日本語では応答時間とも呼ばれます。システムのパフォーマンスを測る上で基本となる指標で、システムの評価指標に属する用語です。

とい46。データベースのトランザクションに関する記述のうち、適切なものはどれか？。。

ア。他のトランザクションにデータを更新されないようにするために、テーブルに対するロックをアプリケーションプログラムが解放した。。

イ。トランザクション障害が発生したので、異常終了したトランザクションをDBMSがロールフォワードした。。

ウ。トランザクションの更新結果を確定するために、トランザクションをアプリケーションプログラムがロールバックした。。

エ。複数のトランザクション間でデッドロックが発生したので、トランザクションをDBMSがロールバックした。

せいかいわ。エ。複数のトランザクション間でデッドロックが発生したので、トランザクションをDBMSがロールバックしたです。。。

なお、あわ、ロックを開放するのではなく、ロックするのが正しいので不適切です。。

いわ、ロールフォワードではなく、ロールバックが正しいので不適切です。。

うわ、ロールバックではなく、コミットが正しいので不適切です。

とい47。PCが、Webサーバ、メールサーバ、他のPCなどと通信を始める際に、通信相手のIPアドレスを問い合わせる仕組みはどれか？。。

ア。あーぷ。アドレスレゾリューションプロトコール。。

イ。DHCP。ダイナミックホストコンフィグレーションプロトコール。。

ウ。DNS。ドメインネームシステム。。

エ。なっと。ネットワークアドレストランスレーション

せいかいわ。ウ。DNS。ドメインネームシステムです。。。簡単でしたよね？

とい48。RPAを活用することによって業務の改善を図ったものはどれか？。。

ア。くだものの出荷検査のために、画像解析によって大きさや形が規格外のくだものをふるい落とす装置を導入し、検査速度を向上させた。。

イ。事務職員が人手で行っていた定型的かつ大量のコピーあんどペースト作業をソフトウェアによって自動化し、作業時間の短縮と作業精度の向上を実現させた。。

ウ。倉庫での作業従事者にパワーアシストスーツを着用させ、身体の不調で病欠する従業員の割合を低減させた。。

エ。ビッグデータを用いてあらかじめ解析した結果から、タクシーの需要が多いと見込まれる地域を日ごとに特定し、タクシーの空車の割合を低減させた。

せいかいわ。イ。事務職員が人手で行っていた定型的かつ大量のコピーあんどペースト作業をソフトウェアによって自動化し、作業時間の短縮と作業精度の向上を実現させたです。。。

RPA。ロボティックプロセスオートメーションとわ、パソコンで行われる事務作業を自動化できるソフトウェアロボット技術のことです。事務作業というところがポイントですね

とい49。情報システムを取得するための提案依頼書、RFPの作成と提案依頼に当たって取得者であるユーザ企業側の対応のうち、適切なものはどれか？。。

ア。RFP作成の手間を省くために、要求事項の記述は最小限にとどめる。曖昧な点や不完全な点があれば、供給者であるベンダ企業から取得者に都度確認させる。。

イ。取得者であるユーザ企業側では、事前に実現性の確認を行わずに、要求事項が実現可能かどうかの調査や検討は供給者であるベンダ企業側に任せる。。

ウ。複数の要求事項がある場合、重要な要求とそうでない要求の区別がつくようにRFP作成時点で重要度を設定しておく。。

エ。要求事項は機能を記述するのではなく、極力、具体的な製品名や実現手段を細かく指定する。

せいかいわ。ウ。複数の要求事項がある場合、重要な要求とそうでない要求の区別がつくようにRFP作成時点で重要度を設定しておくです。。。

実務でほかの選択肢を行ってしまうと、大変なトラブルが起きてしまうので注意してください

とい50。アンケートの自由記述欄に記入された文章における単語の出現頻度などを分析する手法はどれか？。。

ア。アクセスログ分析。。イ。シックスシグマ。。

ウ。テキストマイニング。。エ。マーケットバスケット分析

せいかいわ。ウ。テキストマイニングです。。。ニュースでもみかけるものなので必ず覚えておきましょう