とい3。業務委託先への情報セキュリティ要求事項に関する次の記述を読んで、設問いちからよんに答えよ。。

エックスしゃは、携帯通信事業者から通信回線設備を借り入れ、データ通信サービスおよび通話サービス、以下、両サービスをあわせてエックスサービスという、を提供している従業員すう70めいの企業である。エックスしゃには、法務部、サービスマーケティング部、情報システム部、利用者サポート部、以下、利用者サポート部をユーエス部という、などがある。エックスしゃでは、最高情報セキュリティ責任者、シーアイエスオーを委員長とした情報セキュリティ委員会、以下、エックスしゃ委員会という、を設置している。エックスしゃいいんかいでは、情報セキュリティ管理規定の整備、情報セキュリティ対策の強化などが審議される。エックスしゃ委員会の事務局長はユーエス部のエス部長である。各部の部長は、エックスしゃ委員会の委員および自部における情報セキュリティ責任者を務め、自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダを選任している。ユーエス部の情報セキュリティリーダはジー課長である。

ユーエス部には、25めいの従業員が所属している。おもな業務は、エックスサービスを利用している顧客、およびエックスサービスへの新規の申し込みを検討している潜在顧客、以下、エックスサービスを利用している顧客および潜在顧客をあわせてエックス顧客という、からの問い合わせへの対応業務、以下、エックス業務という、である。

ユーエス部が利用しているコールセンタ用サービスの概要。。

ユーエス部では、エックス業務を遂行するためにクラウドサービスプロバイダエヌしゃのサースコールセンタようサービス、以下、エヌサービスという、を利用している。エヌサービスには、会社から貸与されたPCのWebブラウザから、暗号化された通信プロトコルであるエーを使ってアクセスする。エヌサービスは、ずいちの基本機能およびセキュリティ機能を提供している。

図いち。エヌサービスの基本機能およびセキュリティ機能。。

1。基本機能。。

1.1。管理画面じょうで手動で実行できる昨日、以下、手動実行きのうという。。

・顧客情報の検索、閲覧。。

・顧客との通話。。

省略。。

2。セキュリティ機能。。

2.1。手動実行機能。。

2.1.1。アクセス制御の設定。。

えぬサービスにアクセスできるIPアドレスの登録、更新、削除。。

2.1.2。アカウント管理。。

エヌサービスのログインようのアカウントの登録、更新、削除。。

2.1.3。顧客情報の操作権限の設定。。

かくアカウントに対する顧客情報の登録、閲覧、削除の権限の設定。。

省略。。

2.2。自動実行機能。。

2.2.1。監査ログの収集。。

エヌサービスへのログインおよび手動実行機能を実行した時刻、アカウント、アクセスもとIPアドレスなどのログの収集。。

省略。。

エヌサービスのデータベース、以下、NDBという、に、氏名、年齢、住所、利用中のサービスプラン、問い合わせ対応記録そのたのエックス顧客に関する情報、以下、エックス情報という、わ暗号化されて、また、検索用キーはひらぶんで保存されている。エックス情報は、ユーエス部の従業員に貸与しているPCにだけ格納した暗号鍵をもちいて、ユーエス部の従業員が復号できる仕組みになっている。PCへのログインには利用者IDとパスワードが必要である。。

エックスしゃでは、エヌサービスのセキュリティ機能のうち、手動実行機能は、管理者アカウントを持つユーエス部の特定の従業員だけが実行できる。えっくすしゃ利用分の監査ログは、えっくすしゃの情報システム部が常時監視している。。

ユーエス部では、業務効率化のいっかんとして、2019年10月にエックス業務のさんわりを外部に委託し、残りの業務は連続してエヌサービスを利用しながらユーエス部ないで遂行することにした。

その委託先の第一候補がワイしゃである。わいしゃを選んだ理由は、つぎのにてんである。。

ほかの候補と比較してサービス内容にそんしょくがなく、しかも低価格であること。。

秘密保持契約を締結したうえで、業務委託にかかわる範囲を対象とした、情報セキュリティ対策の評価に協力してくれること。。

わいしゃの概要。。

わいしゃは、つぎのゴールセンタサービス、以下、ワイサービスという、を提供する従業員200めいのきぎょうである。。

委託元に代わって顧客からの姓日にゃサービスに関するさまざまな問い合わせや苦情を受け付ける。。

委託元の製品やサービスの評判を新聞、雑誌などのメディア、インターネットじょうのSNS、掲示板などをもとに調査し、委託元に報告する。著作物を複製する場合は、著作権者の許諾をえておこなう。

わいしゃはコールセンタシステム、以下、ワイシステムという、を構築、通常はそれを利用してワイサービスを提供している。。

ワイしゃの組織のおもな業務および体制をひょういちに示す。。

ひょういち。わいしゃの組織のおもな業務および体制、抜粋。。

人事総務部、営業部は省略します。。

カスタマサービス部、以下、ワイシーエス部という。主な業務、ワイサービスの企画立案、ワイサービスの提供。体制、ティー部長、課長いちめい、主任よんめい、一般従業員ごめい、パートタイマ50めい。。

システム管理部。主な業務、ワイシステム、わいしゃないに導入している入退管理システムなどのシステムの企画、開発、運用。

情報セキュリティに関わる企画、開発、運用。

ワイシステムのデータベースの管理、障害対応および機能改修。

体制、部長いちめい、エフ課長、主任にめい、一般従業員はちめい、パートタイマぜろめい。。

ちゅうき、一般従業員とは、管理職およびパートタイマをのぞく従業員をいう。主任以上を管理職という。。

ちゅういち。本業務を実施するさいには従業員がデータベースのデータにアクセスすることがある。

ワイしゃわ、従業員を対象に、原則四月および十月のついたちに社内の定期人事異動がある。また、これらの時期以外でも組織再編、業務の見直しなどの理由で人事異動がある。

ワイシーエス部のパートタイマは、一年間でやくにわりが退職する。人事総務部は、欠員補充のために、ほぼ同数を新規に採用している。。

わいしゃの情報セキュリティ対策。。

わいしゃわ、東京都内のななかいだてビルのさんからごかいに入居しており、ほかのかいには別の企業が入居している。ビルの出入りは誰でも可能であり、階段やエレベータを使用して、かくかいに移動できる。わいしゃの入退管理をずにに示す。

ず2。わいしゃの入退管理。。

かくかいには業務エリアがひとつずつある。各業務エリアには出入り口がにかしょあり、入室時にろっけたの暗証番号によってドアを解錠する入退管理システムが設置されている。。

暗証番号は各業務エリアでことなる。。

システム管理部は、しがつおよび十月のついたちに各業務エリアの暗証番号を更新する。暗証番号は、各業務エリアの入室権限を与えた従業員だけに事前に通知する。。

システム管理部の通知後は、人事異動によって配属された従業員への暗証番号の通知はかくぶでおこなう。。

ともづれで入室することおよびたぶの従業員に暗証番号を教えることは禁止している。。

わいしゃの従業員以外が視察や情報セキュリティ調査などの目的で業務エリアに入室する場合、わいしゃの管理職が同行し、入室中は指定のネックストラップを常時着用させる。。

各業務エリアの出入り口付近に監視カメラが設置されており、毎日にじゅうよじかん録画している。。

業務エリアに出入りする際の持ち物検査はおこなっていない。。

3かいわワイシーエス部の、また、4階および5階はたぶの業務エリアである。。

ワイシーエス部の管理職および一般従業員は、五階の会議室で営業部の従業員と会議をすることが多いので、三階および五階への入室権限が与えられている。

3から5階には、複合機が二台ずつ設置されており、コピー、プリント、スキャンの機能が使用できる。ワイシーエス部はスキャンの機能を使用して、新聞、雑誌などに紹介された委託元の製品やサービスに関する記事をPDFかし、委託元に報告している。スキャンしたPDFファイルは電子メール、以下、電子メールをメールという、にパスワードなしで添付されて、スキャンを実行した本人だけに送信される。PDFファイルの容量が大きい場合は、PDFファイルを添付するかわりにプリントサーバないの共有フォルダに自動的に保存され、保存先のURLがメールの本文に記載されて送信される。そのさい、メールの送信者名、件名、本文および添付ファイルめいの命名規則などは、複合機の初期設定のまま使用している。そのため、誰がスキャンを実行しても、メールの送信者めいなどは同じになる。複合機のマニュアルはインターネットに記載されている。

管理職にはデスクトップPCおよびノートPCが、そのたの従業員にはデスクトップPCが貸与されている。ノートPCは、社内会議での資料のプロジェクタによる投影、在宅での資料作成などに利用する。わいしゃが貸与しているPC、以下、わいPCという、の仕様および利用状況をひょう2にしめす。

ひょう2。わいPCの仕様および利用状況、ばっすい。。

デスクトップPC。

１。セキュリティケーブルを使用して机に固定しており、鍵はシステム管理者が保管している。。

2。社内のゆうせんランだけに接続できる。。

3。インターネットには、DMZじょうのプロキシサーバを経由してアクセスする。。

ノートPC。

1。社内外の無線ランに接続できる。有線ランには接続できない。。

2。社外または社内からインターネットにアクセスする場合、まずVPNサーバに接続し、みずからの利用者アカウントをもちいてログインする。そのご、DMZじょうのプロキシサーバを経由してアクセスする。。

3。盗難防止のために、離席時はセキュリティケーブルを併用する。。

共通。

1。つぎのふたつの制御が実装されている。。

USBメモリなどの外部記憶媒体は、データの読み込みだけを許可する。。

アプリケーションソフトウェアは、わいしゃが許可しているものだけを導入できる。。

2。業務上、外部記憶媒体へのデータの書き出しが必要な場合およびアプリケーションソフトウェアの追加導入が必要な場合は、わい社内のルールに従って、システム管理部に申請する。。

3。業務で使用するwebブラウザおよびメールクライアントが導入されている。。

4。マルウェア対策ソフトが導入されえており、いちにちに一回、ベンダのサーバに自動的にアクセスし、マルウェア定義ファイルをダウンロードして更新する。。

5。表示された画面を画像形式のデータとして保存できる。

プロキシサーバにはつぎの機能があるが、現在は使用していない。。

指定されたURLへのアクセスを許可または禁止する機能、以下、プロキシ制御機能という。。

利用者IDおよびパスワードによる認証機能、以下、利用者認証機能という。。

プロキシサーバのログ、以下、プロキシログという、わログサーバに転送され、三カ月間保存される。プロキシログは、ネットワーク障害、不審な通信などの原因を調査する場合に利用する。プロキシログには、アクセス日時およびアクセス先IPアドレスが記録されるが、利用者認証機能を使用すると、Webサイトにアクセスした従業員の利用者IDも記録される。。

VPNサーバにはパケットフィルタリングの機能及びあらかじめせっていしたドメインへの通信を禁止する機能、以下、両機能をあわせてVPN制御機能という、があるが、現在はしようしていない。

わいしゃからの提案。。

わいしゃがエックス業務に利用するシステムまたはサービスは、ひょうさんに示すにあんがある。エックスしゃから特段の要求がなければ、わいしゃはあんいちを採用する。。

ひょう3。わいしゃがえっくす業務に利用するシステムまたはサービス。。

案1。ワイシステム。ワイシーエス部の主任のうちにめい、一般従業員のうちにめい、パートタイマのうちよんめいがワイシステムにアクセスできる。。

案2。エヌサービス。ワイシーエス部の主任のうちにめい、一般従業員のうちにめい、パートタイマのうちよんめいがエヌサービスにアクセスできる。。

主任にめいは、エヌサービスの監査ログからえっくす業務での操作履歴を確認できる。

エックスしゃ委員会における案1および案2の検討。。

えっくすしゃ委員会は、案2では、案1のもつビーできるので、案2の採否について議論した。エックスしゃ委員会では、業務委託後の残留リスクを受容できると判断できた場合は、わいしゃに委託することにした。そこで、シーアイエスオーは、業務委託に関わる範囲を対象としてわいしゃの情報セキュリティ対策を確認し、エックスしゃ委員会に報告するようエス部長に指示した。。

エス部長は、ジー課長にわいしゃの情報セキュリティ対策を確認して報告するように指示した。エス部長は、情報システム部に技術面での協力を依頼し、どうぶのエイチ主任がジー課長に協力することになった。

エックスしゃの情報セキュリティ要求事項と評価。。

ジー課長とエイチ主任は、自社の情報セキュリティ管理規定をもとに、エックス業務の外部への委託における情報セキュリティ要求事項、以下、エックス要求事項という、を取りまとめた。。

エックスしゃとわいしゃかんで秘密保持契約を締結したあと、ジー課長は、わいしゃを訪問した。ジー課長はわいしゃの承諾をえたうえで、エックス要求事項をもとに、ワイシーエス部従業員へのヒアリングおよび設備稼働状況の目視による確認などをおこなった。そのさい、ティー部長およびエフ課長に動向を依頼した。そのご、ひょう4のとおり評価結果と評価根拠をまとめてわいしゃに事実確認を依頼したところ、事実だ、との回答があった。評価結果はつぎのルールに従って記入した。。

要求事項を満たす場合、オーケー。要求事項を満たさない場合、エヌジー

ひょう4。エックス要求事項に対するわいしゃの対策の評価結果と評価根拠、抜粋。。

5。

要求事項。エックス業務でエヌサービスへのアクセスが可能な業務エリアはワイシーエス部の業務エリアだけに限定すること。。

評価結果。エヌジー。。

評価根拠。現状のままでは、わいしゃのエヌサービスにアクセスできるようになったら、シーが、3階以外からエヌサービスにアクセスできてしまう。。

省略。。

8。

要求事項。エックス業務を実施する業務エリアへの入室は、入室権限が与えられている従業員だけにせいげんすること。。

評価結果。エヌジー。。

評価結果。入室権限に次のにてんの不備がある。ディー、イー。。

12。

要求事項。省略。。

評価結果。エヌジー。。

評価根拠。複合機が初期設定のままになっている。。

13。

要求事項。エックス業務には、わいしゃ貸与のPCを使用すること。。

評価結果。オーケー。

評価根拠。省略。。

14。

要求事項。エックス業務で使用するPCでは、外部記憶媒体へのアクセスを禁止すること。。

評価結果。エヌジー。。

評価根拠。ワイPCで実装している技術的な制限では、外部記憶媒体のデータの読み込みが可能となっている。。

18。

要求事項。インターネットじょうのwebサイトへのエックス情報のもちだしをけん制する対策があること。。

評価結果。エヌジー。。

評価根拠。省略

評価結果に対する対応案の検討。。

ごじつ、ジー課長はティー部長とエフ課長に、わいしゃと業務委託契約をしたいと伝え、その前提として、評価結果がエヌジーの要求事項への対応を依頼した。わいしゃはジー課長に対応案を伝えた。ジー課長はエイチ主任と相談のうえ、対応案をエス部長に報告した。。

エス部長がひょう4および対応案をエックスしゃ委員会に報告したところ、わいしゃにエックス業務を委託することが承認され、無事に業務が開始された。えっくすしゃはわいしゃへの業務委託によって業務の効率化を進めることができた。

設問1。ユーエス部が利用しているコールセンタようサービスの概要について、かっこ1、2に答えよ。。

かっこ1。本文中のエーに入れる字句はどれか？。解答群のうち、最も適切なものを選べ。。

エーに関する解答群。。

ア。ディーキム。。イ。ドメインキーズ。。ウ。HTTPオーバーTLS。。

エ。アイマップオーバーTLS。。オ。ポップスリーオーバーTLS。。カ。SMTPオーバーTLS

せいかいわ。ウ。HTTPオーバーTLSです

該当箇所を見てみましょう。。

エヌサービスには、会社から貸与されたPCのWebブラウザから、暗号化された通信プロトコルであるえーを使ってアクセスするとあります。。

この時点でHTTPSが答えであると容易に推測できます。

設問にもどりましょう。。

解答群を見ると、HTTPSにあたるのは、ウ。HTTPオーバーTLSであるとすぐに分かります。。

これは簡単ですね

念のため、他の解答群についてもご紹介いたします。。

ディーキム。ドメインキーズアイデンティファイドメール。。

電子メールにおける送信ドメイン認証技術のひとつであり、メールを送信する際に送信元が電子署名をおこない、受信者がそれを検証することで、送信者のなりすましやメールの改ざんを検知できるようにするものです。。

ドメインキーズ。。

電子メールの認証技術のことです。。

アイマップオーバーTLS。。

電子メールの受信にもちいるプロトコルであるアイマップに、伝送路を暗号化するSSLTLSを組み合わせたものです。。

ポップスリーオーバーTLS。。

電子メールの受信にもちいるプロトコルであるポップスリーに、伝送路を暗号化するSSLTLSを組み合わせたものです。。

SMTPオーバーTLS。。

電子メールの受信にもちいるプロトコルであるSMTPに、伝送路を暗号化するSSLTLSを組み合わせたものです。

かっこ2。本文中の下線1について、情報セキュリティじょうのどのような効果が期待できるか？。次のかっこいちからろくのうち、期待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。。

かっこ1。NDBのDBMSの脆弱性を修正し、インターネットからの不正なアクセスによる情報漏えいのリスクを低減する効果。。

かっこ2。NDBを格納している記憶媒体が不正に持ち出された場合にエックス情報が読まれるリスクを低減する効果。。

かっこ3。えぬしゃの従業員がNDBに不正にアクセスすることによってエックス情報が漏えいするリスクを低減する効果。。

かっこ4。エックス情報へのアクセスが許可されたユーエス部の従業員がNDBを誤って操作することによってエックス情報を変更するリスクを低減する。。

かっこ5。攻撃者によってNDBに仕込まれたマルウェアを駆除する効果。。

かっこ6。攻撃者によってNDBに仕込まれたマルウェアを検知する効果。。

解答群はこのようになっております。読み上げは省かせていただきます。。

せいかいわ。エ。かっこ2、3となります

該当箇所を見てみましょう。。

下線部1は、エックス情報は、ユーエス部の従業員に貸与しているPCにだけ格納した暗号鍵をもちいて、ユーエス部の従業員が復号できる仕組みとなっております。これによって期待される情報セキュリティじょうの効果について選択すればよいということになります。

設問にもどりましょう。。

この中から情報セキュリティじょうの効果が期待できるのは、

かっこ2。NDBを格納している記憶媒体が不正に持ち出された場合にエックス情報が読まれるリスクを低減する効果と。

かっこ3。えぬしゃの従業員がNDBに不正にアクセスすることによってエックス情報が漏えいするリスクを低減する効果になります。。

かっこ1については、NDBのDBMS、データベースマネージメントシステムの脆弱性を修正し、とありますが、そのような機能や効果はないため不適切です。。

かっこ4については、ユーエス部の従業員がNDBを誤って操作することによってエックス情報を変更するリスクを低減する効果はないため不適切です。。

かっこ5、6についてはマルウェアに対する効果を期待して実装したものではないため不適切です。。

よって、解答群から選ぶべき答えは、エ。かっこ2、3となります。。冷静に考えると簡単でしょう？

設問2。本文中のビーに入れる字句はどれか？。解答群のうち、最も適切なものを選べ。。

ビーに関する解答群。。

ア。エックス業務に従事しないワイシーエス部の従業員によるエックス情報の不正な持ち出しリスクを低減。。

イ。エックス業務に従事するワイシーエス部の従業員によるエックス情報の不正な持ち出しリスクをエヌしゃに移転。。

ウ。エックス業務に従事するワイシーエス部の従業員によるエックス情報の不正な持ち出しリスクを回避。。

エ。システム管理部の従業員によるエックス情報の不正な持ち出しリスクを回避。

せいかいわ。エ。システム管理部の従業員によるエックス情報の不正な持ち出しリスクを回避。

該当箇所を見てみましょう。。

エックスしゃ委員会は、案2では、案1のもつビーできるので、案2の採否について議論したとあります。ということで、わいしゃからの提案を見る必要がありますね。

ひょう3。わいしゃがエックス業務に利用するシステムまたはサービスを見てみましょう。。

案2。エヌサービス。ワイシーエス部の主任のうちにめい、一般従業員のうちにめい、パートタイマのうちよんめいがエヌサービスにアクセスできる。。

主任にめいは、エヌサービスの監査ログからえっくす業務での操作履歴を確認できるとあります。

よくある権限設定とは異なり、システム管理部以外でも監査ログが確認できる設定になっていますね。ここがポイントです。

ひょう1、わいしゃの組織のおもな業務および体制、抜粋のシステム管理部のおもな業務を見てみましょう。。

情報セキュリティに関わる企画、開発、運用が確認できますね。

それでは設問にもどりましょう。。

これらの解答群の中で、最も適切だとおもわれるものは

エ。システム管理部の従業員によるエックス情報の不正な持ち出しリスクを回避です。。。

システム管理部とワイシーエス部主任との相互監視ができるということですね。

せつもん3。エックスしゃの情報セキュリティ要求事項と評価について、かっこいちからよんに答えよ。。

かっこ1。ひょう4ちゅうのシーに入れる字句はどれか？。解答群のうち、最も適切なものを選べ。。

シーに関する解答群。。

ア。エフ課長。。

イ。ティー部長。。

ウ。えっくす業務に従事するワイシーエス部のにめいの一般従業員。。

エ。えっくす業務に従事するワイシーエス部のにめいの主任。。

オ。えっくす業務に従事するワイシーエス部のパートタイマ

せいかいわ。エ。えっくす業務に従事するワイシーエス部のにめいの主任です

該当箇所を見てみましょう。。

いわゆるゾーニングに関する問題ですね。評価根拠の現状のままでは、わいしゃでエヌサービスにアクセスできるようになったら、だれかがさんかい以外からエヌサービスにアクセスできてしまうということで、その誰かについてとわれた問題ですね。

図2。わいしゃのにゅうたい管理のしたのところを見てみましょう。。

三階はワイシーエス部の、また、四階および五階はたぶの業務エリアである。

ワイシーエス部の管理職および一般従業員は、三階および五階への入室権限が与えられているとあります。。

この辺りがポイントとなります

もう少し見てみましょう。。

管理職には、デスクトップPCおよびノートPCが貸与されていることが分かります。

また、ここでいう管理職というのは、主任以上となります。

つまり主任以上であればノートPCを持っているということが分かりますね

ひょう3。わいしゃがエックス業務に利用するシステムまたはサービスを見てみると。

案2のエヌサービスには、ワイシーエス部の主任にめいがアクセスできるとあります。

つまり、主任にめいはノートPCを使用し、VPN経由でアクセスすることができることが分かります。

それでは設問にもどりましょう。。

これらの解答群の中で、最も適切だとおもわれるものは

エ。えっくす業務に従事するワイシーエス部のにめいの主任です。。。

先ほどまでの解説でおわかりいただけただろうか？

かっこ2。ひょう4ちゅうのディー、イーに入れる評価根拠として適切なものを、回答群のなかから選べ。。

ディー、イーに関する解答群。。

ア。ワイシーエス部の従業員が三階の業務エリアに入室できる。。

イ。ワイシーエス部のパートタイマが五階の業務エリアに入室できる。。

ウ。営業部の従業員が三階の業務エリアに入室できる。。

エ。システム管理部の従業員が五階の業務エリアに入室できる。。

オ。退職者の一部が三階の業務エリアに入室できる。。

カ。元ワイシーエス部の従業員が、た部門に移動したあとも、三階の業務エリアに入室できる。

せいかいわ。オ。退職者の一部が三階の業務エリアに入室できると、カ。元ワイシーエス部の従業員が、た部門に移動したあとも、三階の業務エリアに入室できるです。。

今回は設問が並列のため、回答は順不同となります。

該当箇所を見てみましょう。。

ひょう4。エックス要求事項に対するわいしゃの対策の評価結果と評価根拠、抜粋のこうばん８。エックス業務を実施する業務エリアへの入室は、入室権限が与えられている従業員だけに制限すること。に対する不備にてんに関する問題です。

ず2。わいしゃの入退管理を見てみましょう。。

システム管理部は、しがつおよび10月のついたちに各業務エリアの暗証番号を更新するとあります。はんとしに一回とは結構長いですね。その期間に移動や辞めた人が暗証番号を知っていれば入室出来ちゃいますね

それでは設問にもどりましょう。。

先ほどの通り、暗証番号の更新がはんとしに一回と長いため、その期間に移動や辞めた人が暗証番号を知っていれば入室できてしまいます。

ということでせいかいわ。。オ。退職者の一部が三階の業務エリアに入室できると、カ。元ワイシーエス部の従業員が、た部門に移動したあとも、三階の業務エリアに入室できるです。。。これは簡単でしたね

かっこ3。ひょう4ちゅうのかせんまる2は、どのような情報セキュリティリスクが残留していると考えたものか。つぎのかっこいちからごのうち、残留している情報セキュリティリスクだけを全てあげた組み合わせを、解答群のなかから選べ。。

かっこいち。エックス業務に従事する従業員が、攻撃者からのメールを複合機からのものと信じてメールの本文中にあるURLをクリックし、フィッシングサイトに誘導される。。

かっこ2。エックス業務に従事する従業員が、攻撃者からのメールを複合機からのものと信じて添付ファイルを開き、マルウェア感染する。。

かっこ3。エックス業務のなかで、複合機から送信されるメールが攻撃者宛に送信される。。

かっこ4。攻撃者が、複合機から送信されるメールの本文および添付ファイルを改ざんする。。

かっこ5。攻撃者が、複合機から送信されるメールを盗聴する。

解答群はこのようになっております。。読み上げはあまり意味がないので省かせていただきます。

せいかいわ。ア。かっこいち。エックス業務に従事する従業員が、攻撃者からのメールを複合機からのものと信じてメールの本文中にあるURLをクリックし、フィッシングサイトに誘導されると。

かっこ2。エックス業務に従事する従業員が、攻撃者からのメールを複合機からのものと信じて添付ファイルを開き、マルウェア感染するです

それでは該当箇所を見てみましょう。。

ひょう4のこうばん12を見ると、評価根拠は複合機が初期設定のままになっているとあります。。

他の箇所を見てみましょう。。

複合機でスキャンしたPDFファイルは、電子メールにパスワードなしで添付され、スキャンを実行した本人にだけ送信される。。

PDFファイルの容量が大きい場合は、保存先のURLがメール本文に記載されて送信される。。

誰がスキャンを実行しても、メールの送信者めいなどは同じになるとあります。。

これはフィッシングを狙う攻撃者としておいしい状況になっていますね。

それでは設問にもどりましょう。。

解答群の中で、適切なものは、

かっこいち。エックス業務に従事する従業員が、攻撃者からのメールを複合機からのものと信じてメールの本文中にあるURLをクリックし、フィッシングサイトに誘導されると。

かっこ2。エックス業務に従事する従業員が、攻撃者からのメールを複合機からのものと信じて添付ファイルを開き、マルウェア感染するになりますね。。。

かっこ3は、複合機から送信されるメールは本人だけなので不適切です。。

かっこ4は、複合機から送信されるメールの本文及び添付ファイルをかいざんするものではないため不適切です。。

かっこ4は。メールを盗聴できるものでもないので不適切です。

ということで、解答群としては、ア。かっこいちとかっこにとなります。。

これも簡単でしたね

かっこ4。ひょう4ちゅうのこうばん14について、わいしゃが追加の対策をとり、要求事項をみたすことによってどのような情報セキュリティリスクが低減できるか？。つぎのかっこいちからよんのうち、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。。

かっこいち。わいPCないのデータを外部記憶媒体に保存して持ち出される。。

かっこ2。わいPCないのデータを複合機でプリントして持ち出される。。

かっこ3。わい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USBメモリをわいPCに接続されて、わいPCに当該ソフトウェアが導入される。。

かっこ4。マルウェアつきのファイルが保存されているUSBメモリをわいPCに接続されて、わいPCがマルウェア感染する。

解答群はこのようになっております。。読み上げはあまり意味がないので省かせていただきます。

せいかいわ。コ。かっこ4。マルウェアつきのファイルが保存されているUSBメモリをわいPCに接続されて、わいPCがマルウェア感染するです

それでは該当箇所を見てみましょう。。

こうばん14。エックス業務で使用するPCでは、外部記憶媒体へのアクセスを禁止することに関し、わいPCで実装している技術的な制限では、外部記憶媒体のデータの読み込みが可能となっているとされています。

ひょう2。わいPCのしようおよび利用状況抜粋の、きょうつうを見てみると。

USBメモリなどの外部記憶媒体は、データの読み込みだけを許可するとあります。。

データなら何でも読み込めるんですね？。。ありえない制御ですね

それでは設問にもどりましょう。。

解答群の中で適切なものは

かっこ4。マルウェアつきのファイルが保存されているUSBメモリをわいPCに接続されて、わいPCがマルウェア感染するだけですね。。。

なお、かっこ1は、保存はできない仕様のため不適切です。。

かっこ2は、外部記憶媒体の話であれば、かっこ1と同じく保存はできない仕様のため不適切です。。

かっこ３は、許可のうむに関わらず、USBめもりないのデータはよみこめてしまうため不適切です。。

解答群としては、コ。かっこ4となります。。これも簡単でしたね

せつもん4。評価結果に対する対応案の検討について、かっこ1、2に答えよ。。

かっこ1。本文中のかせんまる3について、ひょう4ちゅうのこうばん5の要求事項への有効な対応案はどれか？。解答群のうち、最も有効なものを選べ。。

解答群。。

ア。エヌサービスのアクセス制御の設定機能でエックスしゃおよびワイしゃ以外からのアクセスを禁止する。。

イ。エヌサービスの監査ログを監視し、三階の業務エリア以外からのアクセスを検知する。。

ウ。エヌサービスの顧客情報の操作権限の設定機能で、エックス情報の閲覧だけ許可する。。

エ。VPNサーバのVPN制御機能を使用して、ノートPCからエヌサービスへのアクセスを禁止する。。

オ。ワイシーエス部の管理職は、エヌサービスへのアクセスを禁止する。。

カ。プロキシサーバのプロキシ制御機能を使用して、エヌサービスへのアクセスを禁止する

せいかいわ。エ。VPNサーバのVPN制御機能を使用して、ノートPCからエヌサービスへのアクセスを禁止するです

該当箇所を見てみましょう。。

対応案にかんする記述のみですね

こうばん5を改めて見てみましょう。主任いじょうがノートPCからエヌサービスに3階以外からアクセスできてしまうことに対する対応案について答えればよいということですね。

それでは設問にもどりましょう。。

解答群の中で、もっとも有効な対応案は

エ。VPNサーバのVPN制御機能を使用して、ノートPCからエヌサービスへのアクセスを禁止するです。。。

なお、あわ。エックスしゃおよびわいしゃ以外からのアクセスを禁止しても、主任にめいはアクセスできるので不適切です。。

いわ。三階の業務エリア以外からのアクセスを検知するだけでは歯止めにならないため不適切です。。

うわ。閲覧情報を絞ることが問題ではないため不適切です。。

おわ。ワイシーエス部の管理職がエヌサービスにアクセスできなくなったら業務に支障をきたすため不適切です。。というかこんなこと提案したら上司は切れると思います。。

かわ。主任にめいのアクセスを禁止したら業務に支障をきたすため不適切です。。

かっこ2。本文中のかせんまる3について、ひょう4ちゅうのこうばん18の要求事項への有効な対応策としてどのようなものがあるか？。つぎのかっこいちからごのうち、有効なものだけを全てあげた組み合わせを、解答群の中から選べ。。

かっこ1。エヌサービスにログインできる従業員のデスクトップPCからWebブラウザを削除し、導入が必要な場合だけ、システム管理部に申請する。。

かっこ2。エヌサービスにログインできる従業員は、デスクトップPCは使用せずに、ノートPCだけを使用してエックス業務を実施する。。

かっこ3。エヌサービスにログインできる従業員を対象に、プロキシサーバの利用者認証機能を使用し、プロキシログを監視するむねを通知する。。

かっこ4。デスクトップPCからはエヌサービスだけにアクセスすることを社内ルールに明記し、エヌサービスにログインできる従業員を対象に、通知する。。

かっこ5。プロキシサーバのプロキシ制御機能を使用して、エヌサービスいがいへのアクセスを禁止する。

解答群はこのようになっております。。読み上げはあまり意味がないので省かせていただきます。

せいかいわ。カ。かっこ3。エヌサービスにログインできる従業員を対象に、プロキシサーバの利用者認証機能を使用し、プロキシログを監視するむねを通知するです

それではこうばん18の要求事項を見てみましょう。。

インターネットじょうのwebサイトへのエックス情報の持ち出しをけん制する対策があることとあります。この対応策に関する問題ですね。

それでは設問にもどりましょう。。

選択肢の中で、webサイトへのエックス情報の持ち出しをけん制する対策としてもっとも有効な対応案は

かっこ3。エヌサービスにログインできる従業員を対象に、プロキシサーバの利用者認証機能を使用し、プロキシログを監視するむねを通知するだけですね。。。

かっこ1は、webブラウザを削除したらけんせいどころか業務に支障をきたしてしまいます。。

かっこ2は、ノートPCだけを使用したところでけん制にならないのは明白ですね。。。

かっこ4は、デスクトップPCからはNサービスだけにアクセスすることを社内ルールに明記したとしても、従業員が無視したら意味がないですね。。

かっこ5は、Nサービス以外へのアクセスを禁止したら業務効率が下がるため有効な対策とは言えないですよね。。

現実の社会で提案したらボコボコにされそうな選択肢ばかりで面白いですね。

いじょうより、解答群から選ぶ答えとしては、カ。っこ3。エヌサービスにログインできる従業員を対象に、プロキシサーバの利用者認証機能を使用し、プロキシログを監視するむねを通知するとなります