とい2。アカウント乗っ取りによる情報セキュリティインシデントに関する次の記述を読んで、設問1から4に答えよ。。

ピー社は、従業員数300めいの食品メーカーである。東京に本社があり、関東に営業所と工場が点在している。本社には、製造部、流通管理部、営業部、情報システム部などがある。営業所は、営業部の管轄であり、担当地域の取引店への営業、配送管理などを担当している。キュー県を担当するアール営業所には、所長と副所長のほかに、15めいの営業担当者、にめいの流通担当者、にめいの事務担当者が配置されている。

ピーしゃでは、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する情報セキュリティ委員会、以下、ピーしゃ委員会という、を設置し、情報セキュリティポリシおよび情報セキュリティ関連規定を整備している。ピーしゃ委員会の事務局は、情報システム部が担当し、情報システム部のエル課長が情報セキュリティインシデント、以下、インシデントという、発生時のインシデント対応責任者をつとめている。さらに、本社のかくぶの部長、各営業所の所長、および各工場の工場長は、ピーしゃ委員会の委員、およびじぶしょにおける情報セキュリティ責任者をつとめている。各情報セキュリティ責任者は、じぶしょの情報セキュリティを確保、維持および改善する役割を担っており、じぶしょ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。アール営業所の情報セキュリティ責任者はエー所長であり、情報セキュリティリーダはビー副所長である。

ピーしゃでは、全従業員が基盤情報システムを利用して日々の業務をおこなっている。基盤情報システムは、サーバ、ネットワークおよび各従業員に貸与される端末から構成され、設定と運用管理は、情報システム部がおこなっている。貸与される端末にはノートPC、以下、NPCという、デスクトップPC、以下、DPCという、およびスマートフォン、以下、スマホという、がある。図1にサーバの概要を、ひょう1に端末の概要を示す。

図1。基盤情報システムのサーバの概要。抜粋。。

1。VPNサーバおよびプロキシサーバ。。

1.1。セキュリティベンダが提供する、悪意のあるサイトへのアクセスを遮断するURLフィルタリングサービスが導入されている。。

1.2。アクセス成功とアクセス失敗の両方にかんして、アクセス先URL。アクセスもとIPアドレス、アクセスにちじおよびアクセスの成否がアクセスログに記録され、直近さんかげつぶんが保存される。。

1.3。設定の変更およびログの確認は、情報システム部だけがおこなえる。。

2。ファイルサーバ。。

2.1。営業所ごとに、業務で利用するファイルを保存するためのファイルサーバがあり、従業員は所属する営業所のファイルサーバだけを利用できる。

ひょう1。基盤情報システムの端末の概要、抜粋。。

機器を貸与されるもの。。NPC。営業所の所長、副所長および営業担当者。。DPC。NPCを貸与されない従業員。。スマホ。本社の課長以上の管理職、ならびに営業所の所長、副所長および営業担当者。。

Webブラウザでのインターネットの閲覧。。NPC。ぴーしゃの社内ランに直接接続している場合はプロキシサーバを経由し、それ以外の場合はVPNサーバを経由して閲覧する。。DPC。プロキシサーバを経由して閲覧する。。スマホ。携帯通信網を経由して閲覧する。。

ファイルサーバの利用。。NPC。ぴーしゃの社内ランに直接接続している場合は社内ランだけを経由し、それ以外の場合はVPNサーバ及び社内ランを経由して利用する。。DPC。社内ランを経由して利用する。。スマホ。利用できない。。

セキュリティ機能。。NPC。マルウェア対策ソフトの定義ファイルの更新機能、マルウェアスキャンの機能が有効になっている。。DPC。マルウェア対策ソフトの定義ファイルの更新機能、マルウェアスキャンの機能が有効になっている。。スマホ。マルウェア対策ソフトの定義ファイルの更新機能、マルウェアスキャンの機能、URLフィルタリング機能、注意1。が有効になっている。。

注意1。URLフィルタリング機能は、悪意のあるサイトへのアクセスを遮断するブラックリストがたである。アクセスを遮断した場合だけ、アクセス先URLおよび日時がスマホないにログとして記録され、ちょっきんなのかぶんのログだけが保存される。

チャットサービス。。

ピーしゃでは、製造した食品の取引店への配送を、配送業者に委託している。交通事情などによって配送が遅延する場合、配送業者は、各営業所の流通担当者に電子メール、以下、電子メールをメールという、で連絡する。配送業者から連絡を受けた流通担当者は、メールで営業担当者に連絡し、営業担当者が各顧客に連絡している。

アール営業所が担当する地域では、交通事情による遅延の頻度が高いので、流通担当者が営業担当者にメールを見たかどうかを電話で確認することも多く、この問題を解決するために、ブイしゃが提供しているサース形式のチャットサービス、以下、ブイサービスという、を配送の連絡に利用すること、および業務効率化のためにブイサービスをアール営業所におけるそのたの連絡にも利用することをエー所長に提案した。エー所長はこの提案をピーしゃ委員会にはかり、承認をえた。ブイサービスのサービス仕様を図2に示す。

図2。ブイサービスのサービス仕様、抜粋。。

1。基本情報。。

1.1。利用者はPCのWebブラウザ、またはスマホのWebブラウザもしくわブイサービス専用アプリケーションソフトウェア、以下、ブイアプリという、を利用してアクセスする。。

1.2。同一利用者がPCとスマホの両方から同時にログインできる。。

2。ワークスペース、以下、WSという。。

2.1。利用者は、WSを作成することができる。WSを作成した利用者は、作成したWSの管理者権限を持つ。。

2.2。WSの管理者権限をもつ利用者、以下、WS管理者という、わ、ほかの利用者をWSに参加させること、WSに参加している利用者、以下、WS利用者という、に管理者権限を付与すること、およびWSを削除することができる。。

3。グループチャット、以下、GCという。。

3.1。WS管理者は、WSないにGCを作成し、WS参加者をGCに参加させることができる。。

3.2。利用者は、ブイサービスにログインご、自身が参加しているWSおよびGCにアクセスできる。。

3.3。利用者は、GCないで文字列のメッセージ、以下、GCメッセージ、およびファイルを送信できる。GCメッセージおよびファイルは、GCないに保存され、GCに参加している利用者、以下、GC参加者という、だけが閲覧できる。。

3.4。GCメッセージおよびファイルには、送信した利用者のアカウントめいおよび送信日時、以下、GC送信情報という、が記録される。。

3.5。送信されたGCメッセージはGCごとに直近の千件分が、ファイルはGCごとに直近のひゃっけんぶんが保存された。それより前のものは自動的に削除される。削除されたGCメッセージおよびファイルについてのGC送信情報も同時に削除される。。

3.6。WS管理者は、WSないのGCメッセージ、ファイル、およびGC送信情報を削除できる。

図2。ブイサービスのサービス仕様、抜粋、続き。。

4。セキュリティ機能。。

4.1。ブイサービスへの接続には、HTTPオーバーTLSを使用する。。

4.2。かく利用者のアカウントは、メールアドレスを利用者IDとして登録し、ログイン時の利用者認証のためのパスワードを設定する。パスワードはえい大文字、えいこもじ、数字、記号の文字しゅの全てを組み合わせ、はちもじ以上でなければならない。。

4.3。Webブラウザをとじた場合は、一定時間ごに自動的にブイサービスからログアウトされる。ブイアプリをとじた場合は、その時点で自動的にブイサービスからログアウトされる。。

4.4。利用者が自身のパスワードを変更した場合、利用中の全てのセッションでブイサービスからログアウトされ、再度ログインを求められる。。

4.5。利用者は追加の利用者認証機能、以下、ブイ認証機能という、を有効にすることができる。。

・ブイ認証機能を有効にした場合は、ブイサービスへのログイン時に、利用者IDとパスワードによる利用者認証にくわえ、あらかじめ登録しておいた電話番号にSMSで送信されるろっけたの数字、または利用者IDとして設定されたメールアドレスに送信されるごけたの数字を入力することによる追加の利用者認証を実施する。。

・ブイサービスは、スマホの端末識別番号、またはブイサービスへのログイン時に発行されるクッキーの有無をもとに、初めてブイサービスを利用する端末かどうかを判断する。。

・ブイ認証機能を有効にした場合、同じ端末でのにどめ以降のブイサービスへのログインじの追加の利用者認証を30にちかん省略する機能、以下、ブイ省略機能という、を有効にすることができる。

ビー副所長は、エー所長の指示を受け、図3に示すアール営業所でのブイサービスの利用ルール、以下、ブイサービス利用ルールという、を策定した。。

図3。ブイサービスの利用ルール、抜粋。。

1。利用者IDには、自身のぴーしゃのメールアドレスを登録すること。。

2。GCで送信する全てのファイルをパスワードで保護すること。。

3。ブイサービスのパスワードおよびファイルを保護するためのパスワードは、たにんに推測されにくく、ほかのサービスのパスワードとして利用していない文字列とすること。。

4。ブイサービスのパスワードはたにんに知られないように適切に管理すること。。

5。ファイルを保護するためのパスワードは、ブイサービスのパスワードとは別の文字列を利用し、ファイルを送信したGCないで別のGCメッセージとして送信すること。

エー所長は、ブイサービスの利用開始をビー副所長に指示した。ビー副所長は、ブイサービスでアール営業所ようのWSを作成し、アール営業所の全従業員をWSに参加させ、自身のほかの事務担当者だけにWSの管理者権限を付与した。また、ひょう2に示すGCを作成したうえで、アール営業所の全従業員に、ブイサービス利用ルールを周知した。次に、アール営業所の全てのNPC、DPCおよびスマホのWebブラウザのブックマークにブイサービスのURLを登録してもらったうえで、ろくがつついたちに利用を開始した。

ひょう2。アール営業所で利用するGC。。

GC1。GCめい、管理職。GC参加者、アール営業所の所長、副所長および事務担当者。おもなようと、業務連絡。。

GC2。GCめい、アール営業所。GC参加者、アール営業所のぜん従業員。おもなようと、業務連絡。。

GC3。GCめい、えいぎょう。GC参加者、アール営業所の所長、副所長、営業担当者および事務担当者。おもなようと、勤務スケジュール連絡、業務連絡。。

GC4。GCめい、配送。GC参加者、アール営業所の流通担当者、営業担当者および事務担当者。おもなようと、配送スケジュール連絡

インシデント発生。。

7月みっかの15時5分、ビー副所長のもとにケーさんが報告に来た。報告内容は次のとおりであった。。

・営業担当者であるディーさんから、ひょう3に示すGCメッセージが送られてきた。。

・不審に思ったので、ディーさん本人が送信したGCメッセージであるかどうかをどうじつ15時にディーさんに電話で確認したところ、本日は、社外研修を受講しており、当該GCメッセージは送信していないとの回答であった。。

ひょう3。ディーさんのアカウントから送信されたメッセージ。。

番号1。GC4。7月みっか、13時35分。アカウントの確認が必要です。ほにゃららにアクセスしてください。

ビー副所長は、ディーさんに成りすましたなにものか、以下、なりすましものという、がディーさんのアカウントに不正にログインしたおそれがあると考え、エー所長に報告した。。

報告をうけたエー所長は、インシデントの発生を宣言し、ブイサービスのGCを利用しないようアール営業所の全従業員に通知するとともに、このインシデントについてシーアイエスオーおよびエル課長に報告した。ビー副所長はエル課長と協力し、被害拡大の防止策を実施した。

被害状況の把握と影響範囲の調査。。

次は、インシデントの被害状況と被害影響に関するエル課長とビー副所長の会話である。。

エル課長。ひょう3のGCメッセージちゅうのURL、以下、URLPという、わブイサービスのURLではありません。悪意のあるサイトのURLと考えられるので、URLPへのアクセスの成功が記録されている可能性のあるエーのログについて調査しましたが、該当する記録はありませんでした。エーのログだけでは確認できないので、アール営業所の従業員のうち、必要があるものに対してURLPにアクセスしたがどうかをヒアリングしましたが、全員がアクセスしていないという回答でした。ディーさんのアカウントへの不正ログインによる情報漏えいの有無についてはどうでしたか？。

ビー副所長。事務担当者からの報告によると、なりすましものがアクセスした可能性のあるビーのGCメッセージを調査した結果、ぴーしゃの業務に関する情報はありましたが、会社が秘密と規定した情報、以下、秘密情報という、は含まれていませんでした。しかし、現時点で確認可能なGCメッセージの調査だけでは十分な調査とはいえません。。

エル課長。ビーを利用していた利用者にヒアリングが必要ですね。ところで、GCに送信されたファイルはどうでしたか？。。

ビー副所長。10ファイルありましたが、全てブイサービス利用ルールをみたしたパスワードで保護されていました。

エル課長。今回の場合、パスワードで保護されていても、なりすましものが短時間にパスワードを入手または特定して、ファイルの内容を閲覧できたと思われます。ファイルにはどのような情報が含まれていたのでしょうか？。。

ビー副所長。業務に関する情報は含まれていましたが、秘密情報は含まれていませんでした。。

エル課長。分かりました。調査結果をエー所長およびシーアイエスオーに報告しましょう。

原因調査。。

次は、原因に関するビー副所長とエル課長の会話である。。

ビー副所長。ディーさんヒアリングしたところ、ブイサービスにアクセスしてアカウントの確認をするように求めるメールがブイサービスから来たので、すぐにNPCでメールちゅうのURL、以下、URLRという、にアクセスし、メールアドレスとパスワードを入力したとのことでした。調べてみると、メールの時刻は7月みっか11時22分でした。

エル課長。URLRはフィッシングサイトと考えられます。URLPとURLRは、ディーさんがURLRにアクセスした時点では、URLフィルタリングサービスに悪意のあるサイトのURLとして登録されていませんでした。しかし、現在は登録されていますし、フィッシング対策協議会のサイトに緊急情報として掲載されています。ほかの従業員が同様のメールを受信し、URLRにアクセスしていないかも調査します。念のため、ディーさんが利用していたNPC、以下、NPCDという、わ、証拠として保全し、詳細に調査します。詳細調査には一週間かかります。。

ビー副所長。一週間かかると、ディーさんの業務に影響があります。

エル課長。NPCDを初期化し、セキュリティ修正プログラムを適用してから、文書作成ソフトなどのアプリケーションソフトウェアを再インストールするという対応も考えられます。しかし、NPCDを初期化すると詳細調査に影響があります。ディーさんの業務への影響を軽減する策を講じれば大丈夫ですか？。。

ビー副所長。それなら大丈夫です。

対策の検討。。

ビー副所長およびエル課長は、詳細調査の結果をもとに、アール営業所でのブイサービス利用における問題点と対策をひょう4のように整理した。。

ひょう4。アール営業所でのブイサービス利用における問題点と対策。抜粋。。

1。今回の問題点。URLRが悪意のあるサイトのURLとしてURLフィルタリングサービスに登録されるよりも前に、ディーさんがURLRにアクセスしてしまった。。

今後対策。シーことを確実に実施する。フィッシング対策に関する従業員研修を実施する。。

2。今回の問題点。利用者認証に利用者IDとパスワードだけを利用していたので、不正ログインされてしまった。。今後の対策。ブイ認証機能を有効にする。。

次は、ひょう4に関するビー副所長とエル課長の会話である。。

ビー副所長。番号2の対策では、ログインが煩雑になり利便性が低下してしまうことを懸念しています。。

エル課長。それでは、ディーすることにすれば、利便性も保てます。。

ビー副所長とエル課長は、詳細調査の結果と今後の対策をエー所長に報告し、承認を得た。また、エー所長はぴーしゃ委員会に報告し、今回のブイサービス活用による業務効率化は高く評価された。そのご、ブイサービスはぴーしゃ全体に導入され、業務効率向上に貢献した。

設問1。インシデント発生について、かっこ1、2に答えよ。。

かっこ1。本文中の下線まるいちについて、ケーさんが、電話ではなく、ブイサービスでディーさんに連絡した場合に想定される被害はどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。ケーさんが、なりすましものとのやりとりの結果、ひょうさんのGCメッセージがディーさんからのものと信じ、URLPにアクセスすることによって、Kさんのパスワードが窃取される。。

イ。ケーさんが、なりすましものにGCメッセージを送ることによって、ブイサービスで利用しているビー副所長のアカウントが、なりすましものによって不正に利用される。。

ウ。ケーさんがなりすましものへの連絡のために送ったGCメッセージが、なりすましもの以外の第三者に盗聴され、内容が第三者に漏えいする。。

エ。ケーさんが連絡した直後に、なりすましものによって証拠隠滅が図られ、ディーさんのアカウントが利用されてGCメッセージが削除される。

せいかいわ。ア。ケーさんが、なりすましものとのやりとりの結果、ひょうさんのGCメッセージがディーさんからのものと信じ、URLPにアクセスすることによって、Kさんのパスワードが窃取されるです。

それでは改めて該当箇所を見てみましょう。。

設問の通り、ディーさんのメッセージを不審に思ったケーさんが、ディーさんに直接電話で確認したところでしたよね。。

パット見たところ、誰でも怪しむ内容ですね。

それでは解答群に戻りましょう。。

アわ。なりすましものが狙ったストーリーそのものなので適切ですね。。

イわ。KさんがなりすましものにGCメッセージを送ったところで、B副所長のアカウントが窃取できるわけではないので不適切ですね。。

ウわ。なりすましもの以外の第三者へ漏えいは、犯罪組織であればありえるかもしれませんが、問題文では第三者の存在について触れられておらず、なりすましものの狙いからはずれていると考えられるため不適切です。。

エわ。怪しいメッセージを証拠隠滅したとしても、ログには残るだろうし、被害と言えるほどのものでもないので不適切ですね。。

かっこ2。本文中のかせんまるにについて、次のかっこいちからごのうち、実施した防止策として適切なものだけを全てあげた組み合わせを、解答群の中から選べ。。

かっこいち。ディーさんに、ブイサービスのパスワードを変更するよう指示する。。

かっこに。アール営業所の全従業員に、URLPにアクセスした場合はビー副所長に報告するよう指示する。。

かっこさん。アール営業所の全従業員に、URLPにアクセスしないよう指示する。。

かっこよん。ブイアプリをスマホにインストールしているアール営業所の従業員に、ブイアプリを再インストールするよう指示をする。。

かっこご。WS管理者のパスワードを変更する。。

解答群。。

ア。かっこいち、に、さん。。イ。かっこいち、さん。。ウ。かっこいち、よん、ご。。

エ。かっこに、さん、よん。。オ。かっこに、よん、ご。。カ。かっこさん、よん

せいかいわ。ア。かっこいち。ディーさんに、ブイサービスのパスワードを変更するよう指示する。。かっこに。アール営業所の全従業員に、URLPにアクセスした場合はビー副所長に報告するよう指示する。。かっこさん。アール営業所の全従業員に、URLPにアクセスしないよう指示するです

それでは該当箇所を見てみましょう。。

設問のとおり、今回のインシデントに対する被害拡大の防止策に関して問われていますね

それでは設問にもどりましょう。。

かっこいちの、ディーさんに、ブイサービスのパスワードを変更するよう指示する。については確実に実施する必要があるため適切ですね

かっこにの、アール営業所の全従業員に、URLPにアクセスした場合はビー副所長に報告するよう指示する。についても状況把握と歯止めをかけるために必要な策なので適切ですね。

かっこさんの、アール営業所の全従業員に、URLPにアクセスしないよう指示する。についても当然必要な処置になるためてきせつですね。

かっこよんについては、ブイアプリを再インストールしたところでアカウント情報の漏洩対策や被害拡大に対する対策にならないため不適切です。。

かっこごも同様に不適切ですね。。

以上より、こたえわ、あ。になりますね

せつもんに。被害状況のはあくと影響範囲のちょうさについて、かっこいちからごに答えよ。。

かっこいち。本文中のえーに入れる適切な字句はどれか？。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。URLフィルタリング機能。。

イ。VPNサーバ。。

ウ。VPNサーバおよびURLフィルタリング機能。。

エ。VPNサーバおよびプロキシサーバ。。

オ。プロキシサーバ。。

カ。プロキシサーバ、VPNサーバおよびURLフィルタリング機能。。

キ。プロキシサーバおよびURLフィルタリング機能。

せいかいわ。エ。VPNサーバおよびプロキシサーバです

それでは該当箇所を見てみましょう。。

URLPのアクセスログに関する問題ですね。なにのアクセスログを見るべきかを答える必要があることが分かります。

ず1。基盤情報システムのサーバの概要、抜粋の。

1。VPNサーバおよびプロキシサーバをみてみましょう。。

1.2に。アクセス成功とアクセス失敗の両方に関して、アクセス先URL、アクセスもとIPアドレス、アクセスにちじおよびアクセス成否がアクセスログに記録され、直近さんかげつぶんが保存されると記載されています。。

このことから、VPNサーバおよびプロキシサーバのログを調べれば良いことがわかります。

なお、ひょういち。基盤情報システムの端末の概要、抜粋を見てみると。

注意のところにURLフィルタリング機能は、悪意のあるサイトへのアクセスを遮断するブラックリストるいである。と書いてあります。今回のURLはブラックリスト未登録のため、ログを見ても分からないこと判断できますね。

あらためてせつもんにを見てみましょう。。

この解答群の中で、VPNサーバおよびプロキシサーバに関するものは、

エ。VPNサーバおよびプロキシサーバになりますね。。

落ち着いてみてみると簡単ですよね

かっこに。本文中のかせんまるさんについて、最低限、アール営業所のどの従業員にヒアリングをする必要があるか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。営業担当者。。

イ。所長、副所長、営業担当者および事務担当者。。

ウ。所長、副所長および営業担当者。。

エ。所長および副所長。。

オ。流通担当者および事務担当者。

せいかいわ。ア。営業担当者です

それでは該当箇所を見てみましょう。。

先ほどのログ調査以外での調査についてです。URLPにアクセスしうるアール営業所の従業員はだれか？、ということが問われていますね。

まずディーさんについてですが、ディーさんは営業担当者でしたね。。

ひょうさんをみると、そのディーさんのアカウントから送信されたGCメッセージのGC番号は、GCふぉーでした。

ひょうに、アール営業所で利用するGCを見てみましょう。。

GC4は、アール営業所の流通担当者、営業担当者および事務担当者が参加者であることが分かりますね。

ひょういち、基盤情報システムの端末の概要、抜粋を見てみましょう。。

営業担当者はNPCが貸与されていますが、流通担当者と事務担当者はDPCが貸与されており、そのDPCはプロキシサーバを経由してインターネットを閲覧する仕組みとなっております。

つまり、DPCを使用する流通担当者と事務担当者は、ログ調査でURLPへのアクセスの有無が確認できているということになります。

設問にもどりましょう。。

これまでの事実より、営業担当者のみにヒアリングすれば良いということになりますので、

せいかいわ。ア。営業担当者だと分かります。。。

推理ゲームみたいで面白いですね

かっこさん。本文中のビーにいれる適切な字句を、解答群の中から選べ。。

ビーに関する解答群。。

ア。GC1、GC2およびGC3。。

イ。GC1、GC2およびGC4。。

ウ。GC1、GC3およびGC4。。

エ。GC2。。

オ。GC2およびGC3。。

カ。GC2、GC3およびGC4。。

キ。GC2およびGC4。。

ク。GC3。。

ケ。GC3およびGC4。。

コ。GC4

せいかいわ。カ。GC2、GC3およびGC4です

それでは該当箇所を見てみましょう。。

この問題は、なりすましものがアクセスした可能性のあるGCについて問われていますね。。

それではひょうに、アール営業所で利用するGCを見てみましょう。。

さきほどの問題より、営業担当者はURLPにアクセスした可能性があるということが分かっていますね。。

つまり、このひょうのなかのアール営業所のぜん従業員と営業担当者が参加者となっているGCを選べばよいということになります。。

よって、答えはGC2、GC3およびGC4であるとわかります。

ということで、選ぶべき解答群としては、

カ。GC2、GC3およびGC4ということになります。。

すっきりしましたか？

かっこよん。本文中のかせんまるよんについて、十分な調査とはいえない理由はどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。ディーさんのアカウントでは確認できないGCメッセージがあるから。。

イ。URLPにアクセスした結果、マルウェアをダウンロードした従業員がいる可能性があるから。。

ウ。なりすましものがディーさんのアカウントに不正にログインしたあと、GCメッセージのうち秘密情報を含むものを選んで削除した可能性があるから。。

エ。なりすましものがディーさんのアカウントに不正にログインしていたあいだは閲覧可能であったが、そのあとに削除されたGCメッセージがあった可能性があるから。。

オ。ひょうさんに示すGCメッセージを閲覧していない従業員がいるから。

せいかいわ。エ。なりすましものがディーさんのアカウントに不正にログインしていたあいだは閲覧可能であったが、そのあとに削除されたGCメッセージがあった可能性があるからです

それでは該当箇所を見てみましょう。。

さきほどの問題の続きですね。。

GC2、GC3およびGC4のGCメッセージを調査した結果、ぴーしゃの業務に関する情報はあったが、会社が秘密と規定した情報は無かったそうです。しかし、確証がないため、追加の調査が必要であるとかかれていますね。。

設問に戻りましょう。。じゅうぶんな調査と言えない理由とそれぞれ考えてみます。

アわ。ディーさんのアカウントのなりすましものなのに、ディーさんのアカウントでは確認できないGCメッセージがあるからとある点がおかしいですね。よって不適切です。。

いわ。URLPにアクセスした結果とありますが、それはこれまでの調査でわかっていることなので不適切ですね。。

うわ。いっけんこれが正しいそうにみえますが、秘密情報をふくむものを選んで削除するというのは秘密情報であることを知っていないと難しいですし、それらだけ選んで削除したらメッセージの前後関係もちぐはぐになりそうですね。よって不適切です。。

えわ。なりすましものがディーさんのアカウントにログインしていたあいだは閲覧可能であったが、そのあとに削除されたGCメッセージがあった可能性があるとあり、これが一番ありえると考えられます。よって適切です。。

おわ。GCメッセージを閲覧していない従業員がいるからなりすましものが秘密情報を窃取したというりゆうとはならないため不適切です。

かっこご。本文中のかせんまるごについて、パスワードを入手または特定した方法はどれか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。ディーさんのスマホを物理的に入手しフォレンジックすることによって特定する。。

イ。GCメッセージから特定する。。

ウ。辞書攻撃をおこなうことによって特定する。。

エ。ほかのサービスから流出したパスワードのリストから特定する。

せいかいわ。イ。GCメッセージから特定するです。

該当箇所を見てみましょう。。

GCメッセージに送信されたファイルにかけられたパスワードの入手または特定方法についてとわれていますね。

ディーさんへのヒアリング結果を見てみましょう。。

Vサービスにアクセスしてアカウントの確認をするように求めるメールがブイサービスからきたので、すぐにNPCでメール中のURLにアクセスし、メールアドレスとパスワードを入力したとあります。

しかも、このURLはフィッシングサイトであるともかかれております。

設問にもどりましょう。。

先ほどの通り、ブイサービスからきたフィッシングメッセージにひっかかったということ原因ですので、せいかいわ、イ。GCメッセージから特定するになります。。

これは簡単でしたね

せつもんさん。本文中のかせんまるろくからまるはちについて、詳細調査のあいだのディーさんの業務への影響、詳細調査への影響および詳細調査への影響なしにディーさんの業務への影響を軽減する策を、つぎのかっこいちからじゅうのなかからひとつずつあげた組み合わせはどれか？。解答群のうち、もっとも適切なものをえらべ。。

詳細調査の間のディーさんの業務への影響。。

かっこいち。ディーさんがNPCを業務に利用できない。。

かっこにディーさんがURLPにアクセスできない。。

かっこさん。ディーさんが配送業者からの連絡を受けることができない。。

詳細調査への影響。。

かっこよん。ディーさんが参加しているGCのメッセージが消去され、内容を追跡できない。。

かっこご。NPCDないに保存されているデータが消去されてしまい、調査できない。。

かっころく。NPCDのOSの設定変更が発生してしまい。ブイサービスにディーさんのアカウントでログインしても、内容を調査できない。。

詳細調査への影響なしにディーさんの業務への影響を軽減する策。。

かっこなな。ディーさんが業務で利用しているファイルを詳細調査の対象から外す。。

かっこはち。ディーさんに、あらたにNPCを手配し、詳細調査のあいだはついかで貸与する。。

かっこきゅう。ディーさんの業務終了後の時間帯に詳細調査をおこなう。

かっこじゅう。NPCDに保存されているファイルを全てバックアップし、バックアップファイルを詳細調査する。

解答群はこのようになっておりますが、長いので読み上げは割愛いたします。。

せいかいわ。イ。かっこいち、ご、はちです。

該当箇所を見てみましょう。。

設問の通り、詳細調査の間のディーさんの業務への影響。詳細調査への影響。詳細調査への影響なしにディーさんの業務への影響を軽減する策について問われていることがわかります。

それでは設問にもどりましょう。。

詳細調査の間のディーさんの業務への影響について考えてみましょう。

本文を見てみると、詳細調査をおこなうため、ディーさんが利用していたNPCを証拠として保全し、1週間ほどかけて調査をおこなうとあります

ということで一週間もNPCがつかないということから、詳細調査の間のディーさんの業務への影響は、かっこいち。ディーさんがNPCを業務に利用できないが適切ですね。。

つぎに詳細調査への影響と詳細調査への影響なしにディーさんの業務への影響を軽減する策を考えてみましょう。

本文を見てみると、NPC-Dを初期化すると、詳細調査に影響があり、ディーさんの業務への影響を軽減する策についてとわれていることがわかりますね。

ということで、詳細調査への影響としては、かっこご。NPCDないに保存されているデータが消去されてしまい、調査できないが適切ですね。。

そのまんまの回答でしたね。。

つぎにディーさんの業務への影響を軽減する策についてです。。

これも簡単ですね。。

せいかいわ。かっこはち。ディーさんに、あらたにNPCを手配し、詳細調査のあいだはついかで貸与するしかないですね。

ということで、解答群としては、イ。かっこいち、ご、はちが正解となります。

せつもんよん。対策の検討について、かっこいち、かっこにに答えよ。。

かっこいち。ひょうよんちゅうのし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。。

しーにかんする解答群。。

あ。VPNサーバ、プロキシサーバおよびスマホに、悪意のあるサイトのIPアドレスをもとにサイトへの接続を遮断する機能をもつセキュリティ対策ソフトを追加導入する。。

イ。ブイサービスに対して、ぴーしゃが指定する監査法人による監査を毎年実施するよう要求し、実施しない場合は、ブイサービスの利用を停止する。。

ウ。ブイサービスのかわりに、これまでフィッシング対策協議会の緊急情報にフィッシングメールが報告されたことが無いべつのチャットサービスを利用し、緊急情報を毎日確認する。。

エ。従業員がwebブラウザからブイサービスにアクセスするときは、必ずブックマークからアクセスする。。

オ。フィッシングサイトにアクセスしたときに、それが確実に記録されるように、NPCまたはDPCからだけブイサービスを利用する。。

せいかいわ。エ。従業員がwebブラウザからブイサービスにアクセスするときは、必ずブックマークからアクセスするです。。これはよくおこなう対策ですね。

それでは該当箇所を見てみましょう。。

しーわ、URLRが悪意のあるサイトのURLとしてURLフィルタリングサービスに登録されるよりも前に、でぃーさんがURLRにアクセスしないようするするための策についてとわれていますね

設問にもどりましょう。。

この解答ぐんからですと、よくおこなう対策はエ。従業員がwebブラウザからブイサービスにアクセスするときは、必ずブックマークからアクセスするなので即答できると思います。。

ちなみに他の解答群についてもご説明いたします。

あわ。悪意のあるサイトであると判明する前に行われたら意味をなさないため不適切です。。

いわ。監査法人による監査を毎年実施してもフィッシングメールの対策にはならないため不適切です。。

うわ。別のチャットサービスを利用したとしてもフィッシングメール対策にはならないので不適切です。。

おわ。フィッシングサイトにアクセスするなよ。。ということで不適切です。。

突っ込みどころが多い解答群でしたね

かっこに。本文中のでぃーにいれるじくはどれか？。解答群のうち、最も適切なものをえらべ。。

でぃーにかんする解答群。。

ア。ぴーしゃないでフィッシングたいさくについての従業員研修をおこない、研修を終えた従業員は、ぶいにんしょうきのうを無効のままにできるようにブイサービス利用ルールを更新する。。

イ。アール営業所の全従業員についてブイ認証機能およびブイ省略機能を有効にする。。

ウ。アール営業所の全従業員についてブイ認証機能を有効にし、ブイサービスのパスワードのながさを32もじ以上に設定した従業員だけ、ブイ省略機能を有効にする。。

エ。ブイサービスのパスワードを30日ごとに変更するようブイサービス利用ルールにさだめ、ブイ認証機能を有効にしない。。

オ。ブイサービス利用ルールをみたしたパスワードを利用しているか、ツールによって確認し、みたしている従業員は、ブイ認証機能を無効にする。

せいかいわ。イ。アール営業所の全従業員についてブイ認証機能およびブイ省略機能を有効にするです

それでは該当箇所を見てみましょう。。

ばんごうにの対策をすると、ログインが煩雑になり利便性が低下すると書かれており、その対策についてとわれています。

ばんごうにを見てみましょう。。

利用者認証に利用者IDとパスワードだけを利用していたので、不正ログインされてしまったという問題に対し、ブイ認証機能を有効にするとあります。

ずに。ブイサービスのサービス仕様、抜粋、続きを見てみましょう。。

ブイ認証機能を有効にした場合、おなじ端末でにどめ以降のブイサービスへのログインじの追加の利用者認証を30日間省略するきのう、いか、ブイ省略機能を有効にすることができるとありますね。つまり、ブイ認証機能を有効にしても、ブイ省略機能を有効にすれば利便性は低下しないということがわかります。

設問にもどりましょう。。

解答群をみてみると、イ。アール営業所の全従業員についてブイ認証機能およびブイ省略機能を有効にするというのがただしいことがわかりますね。。

なお、あわ、ブイ認証機能を無効にすると不正アクセスのリスクが高まるため不適切です。。

うわ。パスワードの複雑さを高めた従業員だけ、ブイ省略機能を有効にしても全従業員の煩雑さは低減できないため不適切です。。

エわ。ブイ認証機能を有効にしないのはあと同様、不正アクセスのリスクが高まるため不適切です。。。

おも。ブイ認証機能を無効にすることは不正アクセスのリスクが高まるため不適切です。