とい1。ECサイトの情報セキュリティの改善に関する次の記述を読んで、せつもん1から5に答えよ。。

ジェイしゃは、従業員数90めいの生活雑貨販売会社であり、店舗とECサイト、いか、ジェイしゃのECサイトをジェイサイトというで生活雑貨を販売している。ジェイサイトでの販売は5年前に開始され、現在はジェイしゃの売り上げのななわりをしめている。ジェイサイトに登録されたアカウントすうは現在100万をこえている。ジェイサイトの顧客は幅広い年齢層に渡ることから、ECサイトに不慣れな顧客でも容易に利用できるように、顧客からの問い合わせへの対応に力をいれており、問合せをジェイサイトの問い合わせフォームおよび電話で受け付けている。ジェイサイトに投稿された問い合わせは、カスタマサポート部に電子メール、以下、電子メールをメールというで送信される。問い合わせには、通常、いちにち以内に対応している。

ジェイしゃには、総務部、商品企画部、店舗営業部、EC営業部、情報システム部、カスタマサポート部のむっつのぶがあり、EC営業部はジェイサイトの利用者の管理および商品登録、以下、サイト運営という、ならびにジェイサイトの情報セキュリティ対策を担当している。

ジェイしゃでは、3年前に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た。ジェイしゃのシーアイエスオーは副社長である。情報セキュリティ委員会の事務局は、情報システム部が担当している。また、各部の部長は、情報セキュリティ委員会の委員、およびじぶにおける情報セキュリティ責任者をつとめ、じぶの情報セキュリティを確保し、維持、改善する役割をになっている。各情報セキュリティ責任者は、じぶの情報セキュリティにかか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。EC営業部のシーさんは、どうぶの情報セキュリティリーダに任命されている。

ジェイサイトの情報セキュリティ対策。。

ジェイサイトはインターネットからの通信を監視、制御するためにファイアウォール、以下、FWという、IPSおよびワフを導入している。ジェイサイトには、次のにしゅるいのアカウントがある。

管理者がハードウェア、OS、ミドルウェアおよびアプリケーションソフトウェアの運用管理、ならびにサイト運営をおこなうさいにもちいる管理用アカウント。。

顧客がジェイサイトで商品を購入するさいにもちいる顧客用アカウント

管理用アカウントでのログインにはにようそ認証を実装しており、パスワードおよび携帯用トークンを使った時刻同期式ワンタイムパスワードを採用している。一方、顧客用アカウントとその認証の仕様は顧客の利便性を考慮し、次のようになっている。。

利用者IDとパスワードの組み、以下、利用者IDとパスワードの組みを認証情報という、を採用。。

パスワードははちもじ以上で英数字混在が必要。。

顧客が登録している情報を確認または変更する際には認証情報の再入力が必要。。

新規にアカウントを登録するさいに、既に使われている利用者IDを指定すると、使用されているむねを画面に表示。。

顧客用アカウントをもっていないものでも問い合わせを投稿できるようにするために、問い合わせを投稿するさいに利用者認証が不要

ジェイサイトの顧客情報。。

ジェイしゃの情報セキュリティリスクアセスメントの結果では、ジェイサイトの顧客の個人情報が、情報セキュリティじょう、じぇいしゃで最も重要な情報となっている。この個人情報には、顧客の氏名、配送先住所、連絡先電話番号、認証情報、メールアドレスが含まれており、それらは、ジェイサイトないのデータベースに保存されている。なお、クレジットカード番号およびクレジットカード会員めいは、外部の決済サービスをもちいて非保持かを実現しており、ジェイサイトでは取り扱っていない。

情報セキュリティインシデントの発生。。

2018年11月なのか、カスタマサポート部からシーさんに連絡があった。にせブランド品の販売サイトと思われるサイトに誘導するメッセージ、以下、誘導メッセージという、が書かれた問い合わせがすう万件投稿されたので、通常の問い合わせへの対応が遅延しているとのことだった。シーさんが情報システム部にジェイサイトの調査を依頼したところ、誘導メッセージ以外にも、不正アクセスと思われるログインしこうがあり、既に調査を開始しているとのことだった。この一連の情報セキュリティ事象をうけて臨時の情報セキュリティ委員会が開催され、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、が宣言された。不正ログインが成功した顧客アカウントについて更に詳細に調査したところ、購入していないものが届いたとか、購入していないのに請求がきたといった被害は無かった。顧客への影響は顧客用アカウントの認証情報を攻撃者に知られてしまったことだけであることが確認できたので、顧客への連絡とパスワードのリセットを実施した。不正ログインへの対応が完了したあとに開催された情報セキュリティ委員会で、今回のインシデントについて、情報システム部のユー部長及びカスタマサポート部のエム部長から調査結果がひょういちのとおり報告された。

ひょういち、調査結果。。

攻撃いち。。

ジェイサイトの2018年10月からのログインログを確認したところ、2018年11月5日のさんじからよじに海外のあるIPアドレスから、不正ログインの試みと思われる攻撃が980件の顧客用アカウントに対して一件ずつあり、そのすべてがジェイサイトに実在する顧客用アカウントに対するものであった。980件の不正ログインの試みのうち、90件が成功していた。。

攻撃に。。

ジェイサイトのアクセスログの中からアカウント新規登録画面へのアクセスのログを確認したところ、攻撃いちとどういつのIPアドレスから合計10万件のアカウントの登録が2018年10月からこころみられており、こうげきいちの不正ログインで利用された980件が登録済みのアカウントとしてエラーとなっていた。。

攻撃さん。。

2018年11月ついたちに、ジェイサイトのログインログに、国内の複数のIPアドレスからそれぞれひとつの顧客用アカウントへのログインしこうが、IPアドレスごとに平均千件程度きろくされ、全てログイン失敗になっていた。。

攻撃よん。。

2018年11月むいかに、誘導メッセージが書かれた問い合わせをジェイサイトに五万件投稿するという攻撃があった。カスタマサポート部は問い合わせの中から誘導メッセージ以外のメッセージを抽出するために多くの工数をとられ、顧客の問い合わせの対応が遅延した。問い合わせ内容に書かれた電話番号すうけんに電話で確認したところ、投稿はしていないとのことであった。誘導メッセージは、攻撃いち、攻撃にとは別の海外のあるIPアドレスから投稿された。一件目と二件目は問い合わせフォームを閲覧してから問い合わせが投稿されていたが、三件目以降は閲覧せずに問い合わせが投稿されていた。

情報セキュリティ委員会は、EC営業部のイー部長に対し、ひょういちの攻撃について、対策を検討するよう指示した。イー部長はシーさんと協力し、対策を検討した。

攻撃いちへの対応。。次は、攻撃いちについてイー部長とシーさんの会話である。。

イー部長。攻撃いちには、ジェイサイトから漏えいした顧客用アカウントの認証情報が利用されているとは考えられませんか？。。

シーさん。考えられません。もし、漏えいした顧客用アカウントの認証情報が利用されているとしたら、ログインが全て成功しているはずです。しかし、ログインのきゅうわりは失敗しています。。

イー部長。攻撃いちでは、どのような方法が使われたと考えられますが？。。

シーさん。攻撃いちでは、最近よく聞くエーという方法が使われたと考えています。その方法を使った攻撃は、一般的にビーの場合に成功しやすいといわれています。。

イー部長。攻撃いちを防ぐにはどのような対策が考えられますか？。。

シーさん。攻撃いちの対策には複数ありますが、利用者本人かどうかを確認するために、認証情報による利用者認証に加え、シーワンを導入する方法が一般的だと考えます。この方法は、攻撃いちの被害を未然に防ぐことができるというメリットがあり、かつ、ほかの多数のECサイトでも利用されています。。

イー部長。その対策には、シーツーという特有の課題があるのではないでしょうか？。。

シーさん。可能性はありますが、多くの実績があるので問題は無いでしょう。。

シーさんは、攻撃いちが成功したのは、顧客側にも問題があるので、その問題も解決する必要があると考え、顧客に自衛のための対策を促すこととした。

こうげきにへの対応。。

次は、攻撃にについてのイー部長とシーさんの会話である。。

イー部長。攻撃にではなにがおこなわれたのでしょうか？。。

シーさん。アカウント新規登録画面へのアクセスログを確認した範囲では、ジェイサイトに対してディーがおこなわれたと考えています。同様の事例が最近、たさいとでもあったという情報がありました。。

イー部長。攻撃にを防ぐにはどのような対策が考えられますか？。。

シーさんは対策を説明した。

こうげきさんへの対応。。

シーさんは、今回、攻撃さんを防ぐことができたものの、イー場合には成功しやすいと考え、連続ログイン失敗回数の上限をこえたアカウントをロックする、以下、アカウントロックという、という対策をイー部長に提案した。イー部長は、対策としてはよいが、顧客に影響があるのでエム部長に意見を求めるようにと指示した。次は、シーさんとエム部長の会話である。。

シーさん。アカウントロックは広く使われている技術です。。

エム部長。ジェイサイトの顧客は幅広い年齢層にわたるので、エフ状況が多数発生し、顧客がカスタマサポート部に電話をして対応を依頼するでしょう。問い合わせが大幅に増えるのは困ります。。

シーさん。問い合わせがなるべく増えないよう、適切に対応します。

こうげきよんへの対応。。

シーさんは、攻撃よんは、問い合わせフォームに自動で大量の投稿をこころみる攻撃であり、大量の投稿が成功してしまった原因はジーことであると考え、対策について、ユー部長およびエム部長に相談した。次はユー部長、エム部長およびシーさんの会話である。。

ユー部長。問い合わせを投稿する際に、利用者認証をしてはどうでしょうか？。。

エム部長。問い合わせフォームは既存の顧客以外からも広く意見を集める重要な手段なので、誰でも投稿できるようにする必要があり、利用者認証をするのはよい方法とは言えません。。

ユー部長。それでは、利用者本人かどうかを確認する代わりに、エイチワンのはどうでしょうか？。。

シーさん。エイチワンのは、利用者によってエイチツーという問題が起こる可能性があるので実装には十分注意する必要がありますね。

攻撃いちから攻撃よんへの対応について検討した結果、以下、検討済み対策という、をイー部長は情報セキュリティ委員会にはかり、実施について承認をえた。ただし、検討済み対策を実施したとしても、攻撃いちから攻撃よんを防ぐことができないこともありえるので、追加の対策として、今回と同様のインシデントが発生したらすばやく対応できるようにするための対策を検討するよう指示があった。

追加の対策の検討。。

シーさんは、追加の対策として、ひょういちの攻撃をけんちするために監視することにし、監視すべきあたいをひょうににまとめた。これらのあたいが単位時間あたり一定数以上となった場合、EC営業部の情報セキュリティ責任者と情報セキュリティリーダにメールで通知する。。

ジェイしゃは、検討済み対策および追加の対策を全て完了させた。その後、ジェイサイトはひょういちと同様の攻撃を受けたが、検討済み対策が有効に機能していたので、攻撃が成功することは少なかった。また、攻撃が成功した場合でも、追加の対策が有効に機能したので、被害を最小限に抑えることができた。ジェイサイトの情報セキュリティは大きく向上した。

せつもんいち。攻撃いちへの対応について、かっこいちからよんに答えよ。。

かっこイチ。本文中のエーにいれるじくはどれか？。解答群のうち、最も適切なものを選べ。。

エーに関する解答群。。

ア。ジェイサイトの顧客の個人情報が保存されているデータベースの管理用アカウントの認証情報を利用して不正アクセスする。。

イ。ジェイサイトの顧客の個人情報が保存されているデータベースの脆弱性を利用して不正アクセスする。。

ウ。ジェイサイトのパスワード入力時のパスワード判定ロジックの脆弱性を利用する。。

エ。認証情報のリストに不正にアクセスし、改ざんする。。

オ。認証情報のリストを入手して利用する

せいかいわ。オ。認証情報のリストを入手して利用するです。。。

それでは該当箇所を見てみましょう。。

エーのところは、最近よく聞く攻撃手法を入れれば良いことがわかります。。

こうげきいちを見てみましょう。。

980件の顧客用アカウントに対して一件ずつ不正ログインの試みがあり、そのすべてがジェイサイトに実在する顧客用アカウントで、90件が成功していたとありますね。

それでは設問に戻りましょう。。

実在する顧客用アカウントが利用されていたということで、認証情報のリストが漏えいし、攻撃に利用されていることが分かります。

よって、回答としては。オ。認証情報のリストを入手して利用するが適切であることが分かります。。。ほかの選択肢は関係ないワードがちりばめられていますね。

かっこに。本文中のビ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。。

ビーに関する解答群。。

ア。攻撃対象のサイトにSQLインジェクションの脆弱性がある。。

イ。攻撃対象のサイトのワフのシグネチャやIPSのシグネチャの定期的な更新がされていない。。

ウ。攻撃対象のサイトの顧客が複数のオンラインサービスで認証情報を使い回している。。

エ。攻撃対象のサイトの顧客用のアカウントの認証情報に単純で短いパスワードを設定できる。。

オ。攻撃対象のサイトの問い合わせフォームの処理に脆弱性がある。。

カ。攻撃対象のサイトのログイン処理に送信元IPアドバイスによるアクセス制御機能がない

せいかいわ。ウ。攻撃対象のサイトの顧客が複数のオンラインサービスで認証情報を使い回しているです

それでは該当箇所を見てましょう。先ほどの設問で、認証情報のリストを入手して利用する方法であることが分かっています。今回の設問は、この手法で不正ログインが成功しやすい条件を問われていることが分かります。

こうげきいちをもう一度見てみましょう。980件の不正ログインの試みのうち、90件が成功していたとあります。つまり、90件はIDとパスワードが他のサービスでも同じものを使用しているということが分かります。

それでは設問に戻りましょう。。

980件のうち、90件は少なくとも認証情報を使い回していることが分かっています。

よって、ウ。攻撃対象のサイトの顧客が複数のオンラインサービスで認証情報を使い回しているが正解であるとわかります。。。SQLインジェクションとかワフの話なんかは出てきてませんよ？

かっこさん。本文中のシーワン、シーツーにいれる技術と課題を、次のかっこイチからじゅうの中から一つずつあげた組み合わせはどれか？。シーに関する解答群のうち、最も適切なものを選べ。。

技術。。

かっこイチ。ジェイサイトの顧客用アカウントの認証情報の複製を保存して利用するディレクトリシステム。。

かっこに。指紋、虹彩、静脈などを利用した生体認証。。

かっこさん。ディジタル証明書を利用したクライアント認証。。

かっこよん。ボットからの入力と人からの入力を判別するきゃぷちゃ。。

かっこご。ログインごとにメールで通知される認証用キーによる利用者認証。。

課題。。

かっころく。顧客が意図せず利用者IDを複数回間違った場合にジェイサイトにログインできなくなる。。

かっこなな。顧客がメールアドレスを変更した際にジェイサイトにログインできなくなる。。

かっこはち。顧客の端末がかわったさいに端末の設定に関する問い合わせがカスタマサポート部にはいる。。

かっこきゅう。ボットの使い方についてカスタマサポート部に問い合わせはいる。。

かっこじゅう。連続ログイン失敗回数が上限をこえてアカウントがロックされ、ジェイサイトにログインできなくなる。。

シーに関する解答群につきましては、読み上げはおこないませんのであしからず

せいかいわ。キ。かっこご。ログインごとにメールで通知される認証用キーによる利用者認証とかっこなな。顧客がメールアドレスを変更した際にジェイサイトにログインできなくなるです

それでは該当箇所を見てましょう。。シーワンについては、利用者本人かどうかを確認するための認証情報による利用者認証に追加するものになります。シーツーについては、追加する認証方法に関する特有の課題について問われています。

それでは設問に戻りましょう。。

利用者本人かどうかを確認する必要があり、かつ一般的な方法として有効な方法は、

かっこご。ログインごとにメールで通知される認証用キーによる利用者認証が適切だと考えられます。。

一般的という意味ではキャプチャも考えられますが、この方法では人かボットかの違いを判別することしかできないため、不適切であると考えられます。

次に特有の課題については、メール通知での認証となることから、かっこなな。顧客がメールアドレスを変更した際にジェイサイトにログインできなくなるが適切であると考えられます。

アカウントロックは関係ないですし、端末が変わったとしてもメールアドレスは変わらないので不適切だと考えられます。。

ボットの使い方については回答として意味不明です。

よって、せいかいわ。キ。かっこごとかっこななだと分かります。

かっこよん。本文中のかせんいちについて、どのような対策が考えられるか？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。各サイトで異なるパスワードを利用する。。

イ。公衆無線ランからはジェイサイトを利用しない。。

ウ。顧客のPCのOSに脆弱性修正プログラムを適用し、OSにログインするためのパスワードを定期的に更新する。。

エ。顧客の自宅や職場の無線ランアクセスポイントのパスワードを推測されにくいものにする。。

オ。顧客の端末にマルウェア対策ソフトを導入し、マルウェア定義ファイルの自動更新を有効にする。。

カ。顧客の端末の内蔵ストレージを暗号化する。。

キ。送信するメールの添付ファイルにパスワードをつける。。

ク。定期的に教育を受け、標的型メール攻撃に注意する

せいかいわ。ア。各サイトで異なるパスワードを利用するです。。。

認証情報の使い回しが原因でしたよね？

もう少し詳しく見ていきましょう。。

該当箇所を確認すると、顧客に自衛のための対策を促すことを考えたとあります。

自衛のための対策を答えれば良いということですね。

繰り返しになりますが、今回の問題は、攻撃対象のサイトの顧客が複数のオンラインサービスで認証情報を使い回していることです。。

よって、答えはア。各サイトで異なるパスワードを利用するとなります。。。

ほかの選択肢は関係ないものばかりなのですぐに分かりますね

せつもんに。本文中のディーにいれるじくはどれか？。解答群のうち、最も適切なものを選べ。。

ディーに関する解答群。。

ア。顧客用アカウントのパスワードのリストの作成。。

イ。実際の利用者が使っているパスワードの複雑性の確認。。

ウ。従業員の認証情報のリストの登録。。

エ。特定の利用者IDが存在するかどうかの確認。。

オ。入力フォームに特定の脆弱性があるかどうかの確認。。

カ。認証方式の確認

せいかいわ。エ。特定の利用者IDが存在するかどうかの確認です

該当箇所を見てみましょう。。

アカウントの新規登録画面へのアクセスログを確認した結果、ジェイサイトに対して攻撃者がおこなった何かが推定されたことがわかります。そのなにかが問われている問題ですね。

攻撃にを見返してみましょう。。

同一のIPアドレスから10万件ものアカウント登録がこころみられており、そのうち980件のアカウントが登録済みとしてエラーとなっていたとあります。このことから、攻撃者は特定のアカウントが存在しているかどうかを確認しているとわかります。

設問にもどります。。

今回の問題は、認証情報、つまりアカウント情報も漏えいしているてんです。

よって、答えはエ。特定の利用者IDが存在するかどうかの確認であることがわかります。。

ほかの選択肢は関係ないものばかりなのですぐに分かりますね。。

例えば、パスワードリストの作成は今回のケースではできないですし、認証方式の確認は10万件も新規登録する必要ないですよね。。

せつもんさん。攻撃さんへの対応について、かっこいちからさんに答えよ。。

かっこいち。本文中のイーにいれるじくはどれか？。解答群のうち、最も適切なものを選べ。。

イーに関する解答群。。

ア。にようそ認証が実装されている。。

イ。ECサイトで要求しているパスワードの強度が低い。。

ウ。ECサイトで利用していないポートが開いている。。

エ。ファイアウォールのルールの末尾に全て拒否のルールが設定されている。。

オ。OSの脆弱性修正プログラムが適用されていない。。

カ。問い合わせフォーム処理時のアクセスが攻撃かどうかの判別に不備がある。。

キ。ファイルへのアクセス制御に不備がある。。

ク。複数のサイトで認証情報を使い回している顧客がいる

せいかいわ。イ。ECサイトで要求しているパスワードの強度が低いです。

それでは該当箇所を見てみましょう。。

攻撃者がログイン成功してしまう場合に関するといですね。。

攻撃さんは、国内の複数のIPアドレスからそれぞれ一つの顧客用アカウントへのログインしこうがされていることから、パスワードの強度に関して問われていることがわかります。

設問にもどります。。

解答群のなかで、パスワードに関するものは、イ。ECサイトで要求しているパスワードの強度が低いだけなので、これが正解だと分かります。。。

他の選択肢は関係ないものばかりですね。。

かっこに。本文中のエフにいれるじくはどれか？。解答群のうち、最も適切なものを選べ。。

エフに関する解答群。。

ア。攻撃者の入力したパスワードが誤っていることを攻撃者に知られてしまう。。

イ。顧客が何回もパスワードを間違えてジェイサイトにログインできなくなる。。

ウ。顧客が利用者IDを変更した際に、ジェイサイトにログインできなくなる。。

エ。導入のさい、顧客自身での生体情報の登録が必要になる。。

オ。ボットと顧客を判別できなくなる

せいかいわ。イ。顧客が何回もパスワードを間違えてジェイサイトにログインできなくなるです

それでは該当箇所を見てみましょう。。

パスワードの入力を何回も失敗したらアカウントロックになるという設定に変更するという流れでしたよね。。

ここでエム部長は、ジェイサイトの顧客は幅広い年齢層にわたるとあることから、パスワードの入力ミスによるアカウントロックが多発することを危惧しています。

せつもんにもどります。。

この解答群の中で、パスワードを間違えるということが記載されているのは、イ。顧客が何回もパスワードを間違えてジェイサイトにログインできなくなるとなるのためこちらが正解となります。

かっこさん。本文中のかせんにについて、どのような対応が必要か？。解答群のうち、最も適切なものを選べ。。

解答群。。

ア。アカウントロックされた顧客からの問い合わせへの対応マニュアルを作成する。。

イ。顧客の連続ログイン失敗回数をログインログから算出し、そのあたいに基づいて、連続ログイン失敗回数の上限を全顧客で一つ決定する。。

ウ。今回の不正ログインしこうの回数をログインログから抽出して、連続ログイン失敗回数の上限を決定する。。

エ。生体認証導入前に、Webページにカスタマサポート部の問い合わせ先を掲載しておく。。

オ。パスワードを連続5回間違えたらアカウントロックする。。

カ。ボットからのアクセスを検知したらアカウントロックする。

せいかいわ。イ。顧客の連続ログイン失敗回数をログインログから算出し、そのあたいに基づいて、連続ログイン失敗回数の上限を全顧客で一つ決定するです

該当箇所を見てみましょう。。

パスワード入力ミスによるアカウントロックの問い合わせが増えないような対応方法について問われていることが分かります。つまり、アカウントロックが起きにくい連続ログイン失敗回数のしきいちに関する問であることが推測できます。

設問にもどります。。

解答群を見てみると、連続ログイン失敗回数のしきいちの決定方法に関するものは、イとウであることが分かります。。

攻撃者の不正ログイン試行回数は、IPアドレスごとに平均千回だったので参考になりません。よって、せいかいわ。イ。顧客の連続ログイン失敗回数をログインログから算出し、そのあたいに基づいて、連続ログイン失敗回数の上限を全顧客で一つ決定するであることが分かります。。簡単でしたよね？

せつもんよん。攻撃よんへの対応について、かっこいち、にに答えよ。。

かっこいち。本文中のジ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。。

ジーに関する解答群。。

ア。問い合わせフォームに入力できる文字数に制限はあるが、文字しゅの制限がない。。

イ。問い合わせフォームへのアクセスを、顧客用アカウントを持っているものだけに許可している。。

ウ。問い合わせを投稿するさいに投稿者を認証する機能がある。。

エ。問い合わせを投稿するさいにボットかどうかを判別する仕組みがない。。

せいかいわ。エ。問い合わせを投稿するさいにボットかどうかを判別する仕組みがないです

それでは該当箇所を見てみましょう。。

攻撃よんの問い合わせフォームに自動で大量の投稿ができてしまった原因について問われていることが分かります。

攻撃よんを見てみましょう。。

問い合わせフォームに五千件の投稿があり、顧客への対応が遅延してしまったというものですね。

よくみると、攻撃いちとにとは別のIPアドレスから投稿されていて、かつ3件目以降は閲覧せずに問い合わせが投稿されていたとあります。このことから、攻撃者はボットを使ったと推測できます。

設問にもどります。。

解答群の中で、ボットに関する記述があるのは、エ、ノミであることが分かります。

よって答えは、エ。問い合わせを投稿するさいにボットかどうかを判別する仕組みがないになります。

かっこに。本文中のエイチワン、エイチツ―にいれる対策と課題を、次のかっこいちからじゅうのなかからひとつずつ挙げた組み合わせはどれか？。エイチに関する解答群のうち、最も適切なものを選べ。。

対策。。

かっこいち。問い合わせの通信パケットをキャプチャし、解析する。。

かっこに。問い合わせは顧客用アカウントをもっているものだけに許可し、問い合わせ投稿時に認証情報を暗号化する。。

かっこさん。問い合わせは顧客用アカウントをもっているものだけに許可し、問い合わせフォームへの入力後に認証情報をハッシュかする。。

かっこよん。問い合わせフォームへの入力後にキャプチャへの対応を求める。。

かっこご。問い合わせフォームへの入力の許容上限時間を設定する。。

課題。。

かっころく。パスワード誤りが続いてアカウントロックされる。。

かっこなな。パスワードを間違えて問い合わせが投稿できない。。

かっこはち。パスワードを間違えてメールが送信できない。。

かっこきゅう。ボットと認識されて問い合わせが投稿できない。。

かっこじゅう。ボットと認識されてメールが送信できない。

せいかいわ。カ。かっこよん。問い合わせフォームへの入力後にキャプチャへの対応を求めると。かっこきゅう。ボットと認識されて問い合わせが投稿できない。です

該当箇所を見てみましょう。。

問い合わせフォームに関する問題ですね。既存の顧客以外からも広く意見を集めるための重要な手段なので、利用者認証はしない方が良いと述べられています。。

利用者認証ではなく、人間であるかどうか判別できれば良いということになるため、キャプチャに関するものが答えであることが推測されます。

設問にもどります。。

対策であるエイチワンについては、キャプチャの記述があるのがかっこよんしかないのですぐに選ぶことができます。。

課題については、キャプチャは人間かどうかを判別するために使用するため、ボットに関する記述、かっこきゅうとかっこじゅうに絞ることができます。。

かっこじゅうは、問い合わせの投稿ではなく、メール送信に関する記述となっているため誤りだと分かります。よって答えはかっこきゅうであるとわかります。

以上より、解答群。カ。が答えであることが分かります。

せつもんご。ひょうにちゅうのあいからけーにいれるじくはどれか？。解答群のうち、最も適切なものをそれぞれ選べ。。

あいからケーに関する解答群。。

ア。ワフが検知した攻撃のうち、ジェイサイトの脆弱性を悪用した攻撃のかず。。

イ。カスタマサポート部にはいった電話でのといあわせすう。。

ウ。同一IPアドレスからの問い合わせフォームへのアクセスすう。。

エ。同一の顧客用アカウントについて一定数以上のIPアドレスからしこうしたログインすう。。

オ。同一の顧客用アカウントについて失敗したログインすう。。

カ。複数の顧客用アカウントについて同一のIPアドレスからしこうしたログインすう

せいかいわ。あいが、カ。複数の顧客用アカウントについて同一のIPアドレスからしこうしたログインすう。。

じぇいが、オ。同一の顧客用アカウントについて失敗したログインすう。。

けーが、ウ。同一IPアドレスからの問い合わせフォームへのアクセスすうです

それでは該当箇所を見てみましょう。。

ひょういちの攻撃を検知するための監視方法に関する問題ですね。。

これだと思い出すのが大変なのでもう少し詳しく見てみましょう。。

簡単にまとめてみました。。

攻撃いちは、同一のIPからの複数のアカウントへの不正ログイン試行でした。。

攻撃さんは、複数のIPからの同一のアカウントへの不正ログイン試行でした。。

攻撃よんは、同一のIPからの問合せフォームへの攻撃でしたよね？。。

これらの攻撃に対する対策を、解答群から選んでみましょう。。

攻撃いちに対する対策あいは、カ。複数の顧客用アカウントについて同一のIPアドレスからしこうしたログインすうが適切であることがわかります。。

攻撃さんに対するたいさくじぇいは、オ。同一の顧客用アカウントについて失敗したログインすうが適切であることがわかります。。

攻撃よんに対する対策けーは、ウ。同一IPアドレスからの問い合わせフォームへのアクセスすうであることがわかります。。

以上が答えとなります。。

情報をまとめると意外とすんなり答えることができますよね