全問が必須問題です。必ず解答してください。

問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，設問 1～5 に答えよ。

J 社は，従業員数 90 名の生活雑貨販売会社であり，店舗と EC サイト（以下，J 社の EC サイトを J サイトという）で生活雑貨を販売している。J サイトでの販売は 5 年前に開始され，現在は J 社の売上の 7 割を占めている。J サイトに登録されたアカウント数は現在 100 万を超えている。J サイトの顧客は幅広い年齢層にわたることから，EC サイトに不慣れな顧客でも容易に利用できるように，顧客からの問合せへの対応に力を入れており，問合せを J サイトの問合せフォーム及び電話で受け付けている。J サイトに投稿された問合せは，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。問合せには，通常，1 日以内に対応している。

J 社には，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六つの部があり，EC 営業部は J サイトの利用者の管理及び商品登録（以下，サイト運営という）並びに J サイトの情報セキュリティ対策を担当している。

J 社では，3 年前に最高情報セキュリティ責任者（CISO）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及び情報セキュリティ関連規程を整備した。J 社の CISO 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，及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を確保し，維持，改善する役割を担っている。各情報セキュリティ責任者は，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。EC 営業部の C さんは，同部の情報セキュリティリーダに任命されている。

〔J サイトの情報セキュリティ対策〕

J 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 及び WAF を導入している。J サイトには，次の 2 種類のアカウントがある。

・管理者がハードウェア，OS，ミドルウェア及びアプリケーションソフトウェアの運用管理，並びにサイト運営を行う際に用いる管理用アカウント

・顧客がJサイトで商品を購入する際に用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 2 要素認証を実装しており，パスワード及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 8 文字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又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際に，既に使われている利用者 ID を指定すると，使用されている旨を画面に表示
・顧客用アカウントをもっていない者でも問合せを投稿できるようにするために，問合せを投稿する際には利用者認証が不要

〔Jサイトの顧客情報〕

J 社の情報セキュリティリスクアセスメントの結果では，J サイトの顧客の個人情報が，情報セキュリティ上，J 社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，Jサイト内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及びクレジットカード会員名は，外部の決済サービスを用いて非保持化を実現しており，J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 7 日，カスタマサポート部から C さんに連絡があった。偽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）が書かれた問合せが数万件投稿されたので，通常の問合せへの対応が遅延しているとのことだった。C さんが情報システム部に J 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試行があり，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受けて臨時の

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用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来たといった被害はなかった。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後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U部長及びカスタマサポート部のM部長から調査結果が表1のとおり報告された。

表1　調査結果

攻撃	調査結果
攻撃1	J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3:00～4:00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1件ずつあり，その全てがJ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2	J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1と同一のIPアドレスから合計100,000件のアカウントの登録が2018年10月から試みられており，攻撃1の不正ログインで利用された980件が登録済みアカウントとしてエラーとなっていた。
攻撃3	2018年11月1日に，J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一つの顧客用アカウントへのログイン試行が，IPアドレスごとに平均1,000件程度記録され，全てログイン失敗になっていた。
攻撃4	2018年11月6日に，誘導メッセージが書かれた問合せをJサイトに50,000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合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のに多くの工数を取られ，顧客の問合せ対応が遅延した。問合せ内容に書かれた電話番号数件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1，攻撃2とは別の海外のあるIPアドレスから投稿された。1件目と2件目は問合せフォームを閲覧してから問合せが投稿されていたが，3件目以降は閲覧せずに問合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E部長に対し，表1の攻撃について，対策を検討するよう指示した。E部長はCさんと協力し，対策を検討した。

〔攻撃１への対応〕

次は，攻撃１についてのＥ部長とＣさんの会話である。

Ｅ部長：攻撃１には，Ｊ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。

Ｃ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９割は失敗しています。

Ｅ部長：攻撃１では，どのような方法が使われたと考えられますか。

Ｃさん：攻撃１では，最近よく聞く，［ a ］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［ b ］場合に成功しやすいといわれています。

Ｅ部長：攻撃１を防ぐにはどのような対策が考えられますか。

Ｃさん：攻撃１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，［ c1 ］を導入する方法が一般的だと考えます。この方法は，攻撃１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，他の多数のＥＣサイトでも利用されています。

Ｅ部長：その対策には，［ c2 ］という特有の課題があるのではないでしょうか。

Ｃさん：可能性はありますが，多くの実績があるので問題はないでしょう。

Ｃさんは，攻撃１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①自衛のための対策を促すことを考えた。

〔攻撃２への対応〕

次は，攻撃２についてのＥ部長とＣさんの会話である。

Ｅ部長：攻撃２では何が行われたのでしょうか。

Ｃさん：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範囲では，Ｊサイトに対して［ d ］が行われたと考えています。同様の事例が最近，他サイトでもあったという情報がありました。

E 部長：攻撃 2 を防ぐにはどのような対策が考えられますか。

C さんは対策を説明した。

〔攻撃 3 への対応〕

C さんは，今回，攻撃 3 は防ぐことができたものの，[e] 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超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 E 部長に提案した。E 部長は，対策としてはよいが，顧客に影響があるので M 部長に意見を求めるようにと指示した。次は C さんと M 部長の会話である。

C さん ：アカウントロックは広く使われている技術です。

M 部長 ：J サイトの顧客は幅広い年齢層にわたるので，[f] 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。問合せが大幅に増えるのは困ります。

C さん ：②問合せがなるべく増えないよう，適切に対応します。

〔攻撃 4 への対応〕

C さんは，攻撃 4 は，問合せフォームに自動で大量の投稿を試みる攻撃であり，大量の投稿が成功してしまった原因は [g] ことであると考え，対策について，U 部長及び M 部長に相談した。次は U 部長，M 部長及び C さんの会話である。

U 部長 ：問合せを投稿する際に，利用者認証をしてはどうでしょうか。

M 部長 ：問合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。

U 部長 ：それでは，利用者本人かどうかを確認する代わりに，[h1] のはどうでしょうか。

C さん ：[h1] のは，利用者によっては [h2] 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1から攻撃4への対応について検討した対策（以下，検討済対策という）をE部長は情報セキュリティ委員会に諮り，実施について承認を得た。ただし，検討済対策を実施したとしても，攻撃1から攻撃4を防ぐことができないこともあり得るので，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〕

Cさんは，追加の対策として，表1の攻撃を検知するために監視することにし，監視すべき値を表2にまとめた。これらの値が単位時間当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。

表2　監視すべき値

攻撃	監視すべき値
攻撃1	i
攻撃2	（省略）
攻撃3	j
攻撃4	k

J社は，検討済対策及び追加の対策を全て完了させた。その後，Jサイトは表1と同様の攻撃を受けたが，検討済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。Jサイトの情報セキュリティは大きく向上した。

設問1　〔攻撃1への対応〕について，(1)～(4)に答えよ。

(1)　本文中の［　a　］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。

aに関する解答群

ア　J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　J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(ぜい)弱性を利用して不正アクセスする

ウ　J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

(2)　本文中の［　b　］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。

b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WAF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合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アドレスによるアクセス制限機能がない

(3) 本文中の [c1] , [c2] に入れる技術と課題を，次の (i) ～ (x) の中から一つずつ挙げた組合せはどれか。c に関する解答群のうち，最も適切なものを選べ。

［技術］

(i) J 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

(ii) 指紋，虹(こう)彩，静脈などを利用した生体認証

(iii) ディジタル証明書を利用したクライアント認証

(iv) ボットからの入力と人からの入力を判別する CAPTCHA

(v) 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］

(vi) 顧客が意図せず利用者 ID を複数回間違った場合に J サイトにログインできなくなる

(vii) 顧客がメールアドレスを変更した際に J サイトにログインできなくなる

(viii) 顧客の端末が変わった際に端末の設定に関する問合せがカスタマサポート部に入る

(ix) ボットの使い方についてカスタマサポート部に問合せが入る

(x) 連続ログイン失敗回数が上限を超えてアカウントがロックされ，J サイトにログインできなくなる

c に関する解答群

	c1	c2
ア	(i)	(x)
イ	(ii)	(vii)
ウ	(ii)	(viii)
エ	(iii)	(x)
オ	(iv)	(vi)
カ	(iv)	(ix)
キ	(v)	(vii)
ク	(v)	(ix)

(4) 本文中の下線①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 LAN からは J 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 LAN 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付ける。

ク　定期的に教育を受け，標的型メール攻撃に注意する。

設問２　本文中の [d] 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。

d 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

設問３　〔攻撃３への対応〕について，(1) ～ (3) に答えよ。

(1)　本文中の [e] 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。

e に関する解答群

ア　2 要素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　FW 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　問合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

(2)　本文中の [f] 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。

f 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 J 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 J サイトにログインできなくなる

エ　導入の際，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

(3) 本文中の下線②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合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，その値に基づいて，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試行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合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。

設問4　〔攻撃 4 への対応〕について，(1)，(2) に答えよ。

(1) 本文中の [g] 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。

g に関する解答群

ア　問合せフォームに入力できる文字数の制限はあるが，文字種の制限がない

イ　問合せフォームへのアクセスを顧客用アカウントをもっている者だけに許可している

ウ　問合せを投稿する際に投稿者を認証する機能がある

エ　問合せを投稿する際にボットかどうかを判別する仕組みがない

(2) 本文中の [h1] , [h2] に入れる対策と課題を，次の (i) ～ (x) の中から一つずつ挙げた組合せはどれか。h に関する解答群のうち，最も適切なものを選べ。

［対策］

(i) 問合せの通信パケットをキャプチャし，解析する

(ii) 問合せは顧客用アカウントをもっている者だけに許可し，問合せ投稿時に認証情報を暗号化する

(iii) 問合せは顧客用アカウントをもっている者だけに許可し，問合せフォームへの入力後に認証情報をハッシュ化する

(iv) 問合せフォームへの入力後に CAPTCHA への対応を求める

(v) 問合せフォームへの入力の許容上限時間を設定する

［課題］

(vi) パスワード誤りが続いてアカウントロックされる

(vii) パスワードを間違えて問合せが投稿できない

(viii) パスワードを間違えてメールが送信できない

(ix) ボットと認識されて問合せが投稿できない

(x) ボットと認識されてメールが送信できない

h に関する解答群

	h1	h2
ア	(i)	(vii)
イ	(i)	(x)
ウ	(ii)	(vi)
エ	(ii)	(viii)
オ	(iii)	(vii)
カ	(iv)	(ix)
キ	(iv)	(x)
ク	(v)	(ix)

設問5　表 2 中の [i] ～ [k] に入れる字句はどれか。解答群のうち，最も適切なものをそれぞれ選べ。

i ～ k に関する解答群

ア　WAF が検知した攻撃のうち J サイトの脆弱性を悪用した攻撃の数

イ　カスタマサポート部に入った電話での問合せ数

ウ　同一 IP アドレスからの問合せフォームへのアクセス数

エ　同一の顧客用アカウントについて一定数以上の IP アドレスから試行したログイン数

オ　同一の顧客用アカウントについて失敗したログイン数

カ　複数の顧客用アカウントについて同一の IP アドレスから試行したログイン数