SG

令和元年度　秋期
情報セキュリティマネジメント試験
午後　問題

試験時間	12:30 ～ 14:00（1時間30分）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1 ～ 問3
選択方法	全問必須

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) 答案用紙は光学式読取り装置で読み取った上で採点しますので，B 又は HB の黒鉛筆で答案用紙の**マークの記入方法**のとおりマークしてください。マークの濃度がうすいなど，**マークの記入方法**のとおり正しくマークされていない場合は読み取れないことがあります。特にシャープペンシルを使用する際には，マークの濃度に十分注意してください。訂正の場合は，あとが残らないように消しゴムできれいに消し，消しくずを残さないでください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入及びマークしてください。答案用紙の**マークの記入方法**のとおり記入及びマークされていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入及びマークしてください。
   (3) **解答**は，次の例題にならって，**解答欄**にマークしてください。答案用紙の**マークの記入方法**のとおりマークされていない場合は，採点されません。

〔例題〕　次の［　　］に入れる適切な字句を，解答群の中から選べ。

秋の情報処理技術者試験は，［ a ］月に実施される。

解答群　　ア　8　　イ　9　　ウ　10　　エ　11

適切な字句は“ウ　10”ですから，次のようにマークしてください。

例題	a	ア	イ	●	エ	オ	カ	キ	ク	ケ	コ

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

正　誤　表

令和元年 10 月 20 日実施

情報セキュリティマネジメント試験　午後　問題

ページ	問題番号	行	誤	正	訂正の内容
38	3	8 行目	N 社のうちの US 部以外の従業員	N 社の従業員	下線部分を削除する。

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

問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1～4に答えよ。

P社は，従業員数300名の食品メーカである。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。Q県を担当するR営業所には，所長と副所長のほかに，15名の営業担当者，2名の流通担当者，2名の事務担当者が配置されている。

P社では，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（以下，P社委員会という）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ている。P社委員会の事務局は，情報システム部が担当し，情報システム部のL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務めている。さらに，本社の各部の部長，各営業所の所長，及び各工場の工場長は，P社委員会の委員，及び自部署における情報セキュリティ責任者を務めている。各情報セキュリティ責任者は，自部署の情報セキュリティを確保，維持及び改善する役割を担っており，自部署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。R営業所の情報セキュリティ責任者はA所長であり，情報セキュリティリーダはB副所長である。

P社では，全従業員が基盤情報システムを利用して日々の業務を行っている。基盤情報システムは，サーバ，ネットワーク及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，情報システム部が行っている。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），及びスマートフォン（以下，スマホという）がある。図1にサーバの概要を，表1に端末の概要を示す。

1 VPN サーバ及びプロキシサーバ
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関して，アクセス先 URL，アクセス元 IP アドレス，アクセス日時及びアクセス成否がアクセスログに記録され，直近 3 か月分が保存される。
1.3 設定の変更及びログの確認は，情報システム部だけが行える。
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。

図 1　基盤情報システムのサーバの概要（抜粋）

表 1　基盤情報システムの端末の概要（抜粋）

項目	NPC	DPC	スマホ
機器を貸与される者	営業所の所長，副所長及び営業担当者	NPC を貸与されない従業員	本社の課長以上の管理職，並びに営業所の所長，副所長及び営業担当者
Web ブラウザでのインターネット閲覧	P 社の社内 LAN 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。	プロキシサーバを経由して閲覧する。	携帯通信網を経由して閲覧する。
ファイルサーバの利用	P 社の社内 LAN に直接接続している場合は社内 LAN だけを経由し，それ以外の場合は VPN サーバ及び社内 LAN を経由して利用する。	社内 LAN を経由して利用する。	利用できない。
セキュリティ機能	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。	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。	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 [1] が有効になっている。

注 [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型である。アクセスを遮断した場合だけ，アクセス先 URL 及び日時がスマホ内にログとして記録され，直近 7 日分のログだけが保存される。

〔チャットサービス〕

P 社では，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。

R 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，連絡の煩雑さが問題となっている。R 営業所の流通担当者である K さんは，この問題を解決するために，V 社が提供している SaaS 形式のチャットサービス（以下，V サービスという）を配送の連絡に利用すること，及び業務効率化のために V サービスを R 営業所におけるその他の連絡にも利用することを A 所長に提案した。A 所長はこの提案を P 社委員会に諮り，承認を得た。V サービスのサービス仕様を図 2 に示す。

1 基本機能
1.1 利用者は PC の Web ブラウザ，又はスマホの Web ブラウザ若しくは V サービス専用アプリケーションソフトウェア（以下，V 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 の管理者権限をもつ。
2.2 WS の管理者権限をもつ利用者（以下，WS 管理者という）は，他の利用者を WS に参加させること，WS に参加している利用者（以下，WS 参加者という）に管理者権限を付与すること，及び 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 内に 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，V サービスにログイン後，自身が参加している WS 及び GC にアクセスできる。
3.3 利用者は，GC 内で文字列のメッセージ（以下，GC メッセージという）及びファイルを送信できる。GC メッセージ及びファイルは GC 内に保存され，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 メッセージ及びファイルには，送信した利用者のアカウント名及び送信日時（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 1,000 件分が，ファイルは GC ごとに直近の 100 件分が保存され，それより前のものは自動的に削除される。削除された GC メッセージ及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 内の GC メッセージ，ファイル，及び GC 送信情報を削除できる。

図 2　V サービスのサービス仕様（抜粋）

4 セキュリティ機能
4.1 V サービスへの接続には，HTTP over TLS を使用する。
4.2 各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。パスワードは英大文字，英小文字，数字，記号の文字種の全てを組み合わせ，8 文字以上でなければならない。
4.3 Web ブラウザを閉じた場合は，一定時間後に自動的に V サービスからログアウトされる。V アプリを閉じた場合は，その時点で自動的に V 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 V 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，V 認証機能という）を有効にすることができる。
・V 認証機能を有効にした場合は，V 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加え，あらかじめ登録しておいた電話番号に SMS で送信される 6 桁の数字，又は利用者 ID として設定されたメールアドレスに送信される 6 桁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。
・V サービスは，スマホの端末識別番号，又は V サービスへのログイン時に発行される Cookie の有無を基に，初めて V サービスを利用する端末かどうかを判断する。
・V 認証機能を有効にした場合，同じ端末での 2 度目以降の V サービスへのログイン時の追加の利用者認証を 30 日間省略する機能（以下，V 省略機能という）を有効にすることができる。

図 2　V サービスのサービス仕様（抜粋）（続き）

B 副所長は，A 所長の指示を受け，図 3 に示す R 営業所での V サービスの利用ルール（以下，V サービス利用ルールという）を策定した。

1　利用者 ID には，自身の P 社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　V サービスのパスワード及びファイルを保護するためのパスワードは，他人に推測されにくく，他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　V サービスのパスワードは他人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，V 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 内で別の GC メッセージとして送信すること。

図 3　V サービス利用ルール（抜粋）

A 所長は，V サービスの利用開始を B 副所長に指示した。B 副所長は，V サービスで R 営業所用の WS を作成し，R 営業所の全従業員を WS に参加させ，自身のほか事務担当者だけに WS の管理者権限を付与した。また，表 2 に示す GC を作成した上で，R 営業所の全従業員に，V サービス利用ルールを周知した。次に，R 営業所の全ての NPC，DPC 及びスマホの Web ブラウザのブックマークに V サービスの URL を登録してもらった上で，6 月 1 日に利用を開始した。

表2　R営業所で利用するGC

GC番号	GC名	GC参加者	主な用途
GC-1	管理職	R営業所の所長，副所長及び事務担当者	業務連絡
GC-2	R営業所	R営業所の全従業員	業務連絡
GC-3	営業	R営業所の所長，副所長，営業担当者及び事務担当者	勤務スケジュール連絡，業務連絡
GC-4	配送	R営業所の流通担当者，営業担当者及び事務担当者	配送スケジュール連絡

〔インシデント発生〕

7月3日の15時5分，B副所長のもとにK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Dさんから，表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，Dさん本人が送信したGCメッセージであるかどうかを同日15時に①D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。

表3　Dさんのアカウントから送信されたGCメッセージ

番号	GC番号	日時	内容
1	GC-4	7月3日 13時35分	アカウントの確認が必要です。 https://www.v-service.example.com/にアクセスしてください。

B副所長は，Dさんになりすました何者か（以下，なりすまし者という）がD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，A所長に報告した。

報告を受けたA所長は，インシデントの発生を宣言し，VサービスのGCを利用しないようR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CISO及びL課長に報告した。B副所長はL課長と協力し，②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影響範囲に関するL課長とB副所長の会話である。

L 課長　：表 3 の GC メッセージ中の URL（以下，URL-P という）は V 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，URL-P へのアクセスの成功が記録されている可能性のある［　a　］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。［　a　］のログだけでは確認できないので，③R 営業所の従業員のうち，必要がある者に対して URL-P にアクセスしたか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。D 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。

B 副所長：事務担当者からの報告によると，なりすまし者がアクセスした可能性のある［　b　］の GC メッセージを調査した結果，P 社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，④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。

L 課長　：［　b　］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。

B 副所長：10 ファイルありましたが，全て V サービス利用ルールを満たしたパスワードで保護されていました。

L 課長　：今回の場合，パスワードで保護されていても，⑤なりすまし者が短時間にパスワードを入手又は特定して，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。

B 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。

L 課長　：分かりました。調査結果を A 所長及び CISO に報告しましょう。

〔原因調査〕

次は，原因に関する B 副所長と L 課長の会話である。

B 副所長：D さんにヒアリングしたところ，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 V サービスから来たので，すぐに NPC

でメール中の URL（以下，URL-R 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 3 日 11 時 22 分でした。

L 課長　：URL-R はフィッシングサイトと考えられます。URL-P と URL-R は，D さんが URL-R 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。他の従業員が同様のメールを受信し，URL-R にアクセスしていないかも調査します。念のため，D さんが利用していた NPC（以下，NPC-D という）は，証拠として保全し，詳細に調査します。詳細調査には，1 週間掛かります。

B 副所長：1 週間掛かると，⑥D さんの業務に影響があります。

L 課長　：NPC-D 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，NPC-D を初期化すると，⑦詳細調査に影響があります。⑧D 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。

B 副所長：それなら大丈夫です。

〔対策の検討〕

B 副所長及び L 課長は，詳細調査の結果を基に，R 営業所での V サービス利用における問題点と対策を表 4 のように整理した。

表 4　R 営業所での V サービス利用における問題点と対策（抜粋）

番号	今回の問題点	今後の対策
1	URL-R 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，D さんが URL-R にアクセスしてしまった。	・［　c　］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	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。	V 認証機能を有効にする。

次は，表4に関するB副所長とL課長の会話である。

B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。

L課長　：それでは，［ d ］ことにすれば，利便性も保てます。

B 副所長と L 課長は，詳細調査の結果と今後の対策を A 所長に報告し，承認を得た。また，A 所長は P 社委員会に報告し，承認を得た。その後，必要な対策を実施し，V サービスの業務利用を再開した。今回の V サービス活用による業務効率化は，高く評価された。その後，V サービスは P 社全体に導入され，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，(1)，(2)に答えよ。

(1) 本文中の下線①について，K さんが，電話ではなく，V サービスで D 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　K さんが，なりすまし者とのやり取りの結果，表 3 の GC メッセージが D さんからのものと信じ，URL-P 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　K さんが，なりすまし者に GC メッセージを送ることによって，V サービスで利用している B 副所長のアカウントが，なりすまし者によって不正に利用される。

ウ　K さんがなりすまし者への連絡のために送った GC メッセージが，なりすまし者以外の第三者に盗聴され，内容が第三者に漏えいする。

エ　K さんが連絡した直後に，なりすまし者によって証拠隠滅が図られ，D 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。

(2) 本文中の下線②について，次の (i) ～ (v) のうち，実施した防止策として適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) D さんに，V サービスのパスワードを変更するよう指示する。

(ii) R 営業所の全従業員に，URL-P にアクセスした場合は B 副所長に報告するよう指示する。

(iii) R 営業所の全従業員に，URL-P にアクセスしないよう指示する。

(iv) V アプリをスマホにインストールしている R 営業所の従業員に，V アプリを再インストールするよう指示する。

(v) WS 管理者のパスワードを変更する。

解答群

ア (i)，(ii)，(iii)　　イ (i)，(iii)　　ウ (i)，(iv)，(v)

エ (ii)，(iii)，(iv)　　オ (ii)，(iv)，(v)　　カ (iii)，(iv)

設問2 〔被害状況の把握と影響範囲の調査〕について，(1) ～ (5) に答えよ。

(1) 本文中の［ a ］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。

a 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 サーバ及び URL フィルタリング機能

エ VPN サーバ及びプロキシサーバ

オ プロキシサーバ

カ プロキシサーバ，VPN サーバ及び URL フィルタリング機能

キ プロキシサーバ及び URL フィルタリング機能

(2) 本文中の下線③について，最低限，R 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，営業担当者及び事務担当者

ウ 所長，副所長及び営業担当者

エ 所長及び副所長

オ 流通担当者及び事務担当者

(3) 本文中の [b] に入れる適切な字句を，解答群の中から選べ。

b に関する解答群

ア GC-1，GC-2 及び GC-3

イ GC-1，GC-2 及び GC-4

ウ GC-1，GC-3 及び GC-4

エ GC-2

オ GC-2 及び GC-3

カ GC-2，GC-3 及び GC-4

キ GC-2 及び GC-4

ク GC-3

ケ GC-3 及び GC-4

コ GC-4

(4) 本文中の下線④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 D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 URL-P 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 なりすまし者がDさんのアカウントに不正にログインした後，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 なりすまし者が D さんのアカウントに不正にログインしていた間は閲覧可能であったが，その後に削除されたGCメッセージがあった可能性があるから

オ 表3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

(5) 本文中の下線⑤について，パスワードを入手又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 D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 辞書攻撃を行うことによって特定する。

エ 他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。

設問3　本文中の下線⑥～⑧について，“詳細調査の間の D さんの業務への影響”，“詳細調査への影響”及び“詳細調査への影響なしに D さんの業務への影響を軽減する策”を，次の (i) ～ (x) の中から一つずつ挙げた組合せはどれか。解答群のうち，最も適切なものを選べ。

[詳細調査の間の D さんの業務への影響]

(i)　D さんが NPC を業務に利用できない。

(ii)　D さんが URL-P にアクセスできない。

(iii)　D さんが配送業者からの連絡を受け取ることができない。

[詳細調査への影響]

(iv)　D 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。

(v)　NPC-D 内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。

(vi)　NPC-D の OS の設定変更が発生してしまい，V サービスに D 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 D さんの業務への影響を軽減する策]

(vii)　D 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。

(viii)　D さんに，新たに NPC を手配し，詳細調査の間は追加で貸与する。

(ix)　D さんの業務終了後の時間帯に詳細調査を行う。

(x)　NPC-D 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

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

設問4　〔対策の検討〕について，(1)，(2)に答えよ。

(1)　表4中の［　c　］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。

cに関する解答群

ア　VPNサーバ，プロキシサーバ及びスマホに，悪意のあるサイトのIPアドレスを基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　Vサービスに対して，P社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，Vサービスの利用を停止する

ウ　Vサービスの代わりに，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ない別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V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又はDPCからだけVサービスを利用する

(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　P 社内でフィッシング対策についての従業員研修を行い，研修を終えた従業員は，V 認証機能を無効のままにできるよう V サービス利用ルールを更新する

イ　R 営業所の全従業員について V 認証機能及び V 省略機能を有効にする

ウ　R 営業所の全従業員について V 認証機能を有効にし，V サービスのパスワードの長さを 32 文字以上に設定した従業員だけ，V 省略機能を有効にする

エ　V サービスのパスワードを 30 日ごとに変更するよう V サービス利用ルールに定め，V 認証機能を有効にしない

オ　V サービス利用ルールを満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，満たしている従業員は，V 認証機能を無効にする

問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 1 ～ 4 に答えよ。

X 社は，携帯通信事業者から通信回線設備を借り受け，データ通信サービス及び通話サービス（以下，両サービスを併せて X サービスという）を提供している従業員数 70 名の企業である。X 社には，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 US 部という）などがある。X 社では，最高情報セキュリティ責任者（CISO）を委員長とした情報セキュリティ委員会（以下，X 社委員会という）を設置している。X 社委員会では，情報セキュリティ管理規程の整備，情報セキュリティ対策の強化などが審議される。X 社委員会の事務局長は US 部の S 部長である。各部の部長は，X 社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。US 部の情報セキュリティリーダは G 課長である。

US 部には，25 名の従業員が所属している。主な業務は，X サービスを利用している顧客，及び X サービスへの新規の申込みを検討している潜在顧客（以下，X サービスを利用している顧客及び潜在顧客を併せて X 顧客という）からの問合せへの対応業務（以下，X 業務という）である。

〔US 部が利用しているコールセンタ用サービスの概要〕

US 部では，X 業務を遂行するためにクラウドサービスプロバイダ N 社の SaaS のコールセンタ用サービス（以下，N サービスという）を利用している。N サービスは ISMS 認証及び ISMS クラウドセキュリティ認証を取得している。N 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［ a ］を使ってアクセスする。N サービスは，図 1 の基本機能及びセキュリティ機能を提供している。

1 基本機能
 1.1 管理画面上で手動で実行できる機能（以下，手動実行機能という）
  ・顧客情報の検索，閲覧
  ・顧客との通話
  （省略）
 1.2 自動で実行される機能（以下，自動実行機能という）
  ・顧客との通話の録音
  （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
   ・N 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
   ・N サービスのログイン用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
   ・各アカウントに対する顧客情報の登録，更新，閲覧，削除の権限の設定
  （省略）
 2.2 自動実行機能
  2.2.1 監査ログ収集
   ・N サービスへのログイン及び手動実行機能を実行した時刻，アカウント，アクセス元 IP アドレスなどのログの収集
  （省略）

図 1　N サービスの基本機能及びセキュリティ機能

N 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，問合せ対応記録その他の X 顧客に関する情報（以下，X 情報という）は暗号化されて，また，検索用キーは平文で保存されている。①X 情報は，US 部の従業員に貸与している PC にだけ格納した暗号鍵を用いて，US 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。

X 社では，N 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もつ US 部の特定の従業員だけが実行できる。X 社利用分の監査ログは，X 社の情報システム部が常時監視している。

US 部では，業務効率化の一環として，2019 年 10 月に X 業務の 3 割を外部に委託し，残りの業務は継続して N サービスを利用しながら US 部内で遂行することにした。その委託先の第一候補が Y 社である。Y 社を選んだ理由は，次の 2 点である。

・他の候補と比較してサービス内容に遜色がなく，しかも低価格であること

・秘密保持契約を締結した上で，業務委託に関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

〔Y 社の概要〕

Y 社は，次のコールセンタサービス（以下，Y サービスという）を提供する従業員数 200 名の企業である。

・委託元に代わって顧客からの製品やサービスに関する様々な問合せや苦情などを受け付ける。

・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，インターネット上の SNS，掲示板などを基に調査し，委託元に報告する。著作物を複製する場合は，著作権者の許諾を得て行う。

Y 社はコールセンタシステム（以下，Y システムという）を構築し，通常はそれを利用して Y サービスを提供している。

Y 社の組織の主な業務及び体制を表 1 に示す。

表 1　Y 社の組織の主な業務及び体制（抜粋）

組織	主な業務	体制
人事総務部	（省略）	（省略）
営業部	（省略）	（省略）
カスタマサービス部（以下，Y-CS 部という）	・Y サービスの企画立案 ・Y サービスの提供	T 部長 課長：1 名 主任：4 名 一般従業員：5 名 パートタイマ：50 名
システム管理部	・Y システム，Y 社内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 ・Y システムのデータベースの管理，障害対応及び機能改修 [1)]	部長：1 名 F 課長 主任：2 名 一般従業員：8 名 パートタイマ：0 名

注記　一般従業員とは，管理職及びパートタイマを除く従業員をいう。主任以上を管理職という。

注 [1)]　本業務を実施する際に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。

Y 社は，従業員を対象に，原則 4 月及び 10 月の 1 日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。

Y-CS 部のパートタイマは，1 年間で約 2 割が退職する。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。

〔Y 社の情報セキュリティ対策〕

Y 社は，東京都内の 7 階建てビルの 3～5 階に入居しており，他の階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，各階に移動できる。Y 社の入退管理を図 2 に示す。

・各階には業務エリアが一つずつある。各業務エリアには出入口が 2 か所あり，入室時に 6 桁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異なる。
・システム管理部は，4 月及び 10 月の 1 日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各部で行う。
・共連れで入室すること及び他部の従業員に暗証番号を教えることは禁止している。
・Y 社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，Y 社の管理職が同行し，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口付近には監視カメラが設置されており，毎日 24 時間録画している。
・業務エリアに出入りする際の持ち物検査は行っていない。

図 2　Y 社の入退管理

3 階は Y-CS 部の，また，4 階及び 5 階は他部の業務エリアである。

Y-CS 部の管理職及び一般従業員は，5 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，3 階及び 5 階への入室権限が与えられている。

3～5 階には，複合機が 2 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。Y-CS 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 化し，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代わりにプリントサーバ内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。その際，メールの送信者名，件名，本文及び添付ファイル名の命名規則などは，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

ルの送信者名などは同じになる。複合機のマニュアルはインターネットに掲載されている。

管理職にはデスクトップ PC 及びノート PC が，その他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。Y 社が貸与している PC（以下，Y-PC という）の仕様及び利用状況を表 2 に示す。

表 2　Y-PC の仕様及び利用状況（抜粋）

PC の種類	仕様及び利用状況
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，鍵はシステム管理部が保管している。 2　社内の有線 LAN だけに接続できる。 3　インターネットには，DMZ 上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 LAN に接続できる。有線 LAN には接続できない。 2　社外又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，自らの利用者アカウントを用いてログインする。その後，DMZ 上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使用する。
共通	1　次の二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，データの読込みだけを許可する。 ・アプリケーションソフトウェアは，Y 社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出しが必要な場合及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，Y 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 ブラウザ及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ており，1 日に 1 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次の機能があるが，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又は禁止する機能（以下，プロキシ制御機能という）

・利用者 ID 及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）はログサーバに転送され，3 か月間保存される。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，アクセス日時及びアクセス先 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設定したドメインへの通信を禁止する機能（以下，両機能を併せて VPN 制御機能という）があるが，現在は使用していない。

〔Y 社からの提案〕

Y 社が X 業務に利用するシステム又はサービスは表 3 に示す 2 案がある。X 社から特段の要求がなければ，Y 社は案 1 を採用する。

表 3　Y 社が X 業務に利用するシステム又はサービス

案	X 業務に利用するシステム又はサービス	アクセスできる従業員
案 1	Y システム	・Y-CS 部の主任のうち 2 名，一般従業員のうち 2 名，パートタイマのうち 4 名が Y システムにアクセスできる。
案 2	N サービス	・Y-CS 部の主任のうち 2 名，一般従業員のうち 2 名，パートタイマのうち 4 名が N サービスにアクセスできる。 ・主任 2 名は，N サービスの監査ログから X 業務での操作履歴を確認できる。

〔X 社委員会における案 1 及び案 2 の検討〕

X 社委員会は，案 2 では，案 1 のもつ［ b ］できるので，案 2 の採否について議論した。X 社委員会では，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，Y 社に委託することにした。そこで，CISO は，業務委託に関わる範囲を対象として Y 社の情報セキュリティ対策を確認し，X 社委員会に報告するよう S 部長に指示した。

S 部長は，G 課長に Y 社の情報セキュリティ対策を確認して報告するよう指示した。S 部長は，情報システム部に技術面での協力を依頼し，同部の H 主任が G 課長に協力することになった。

〔X社の情報セキュリティ要求事項と評価〕

G 課長と H 主任は，自社の情報セキュリティ管理規程を基に，X 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，X 要求事項という）を取りまとめた。

X社と Y 社間で秘密保持契約を締結した後，G 課長は，Y 社を訪問した。G 課長は Y 社の承諾を得た上で，X 要求事項を基に，Y-CS 部従業員へのヒアリング及び設備状況の目視による確認などを行った。その際，T 部長及び F 課長に同行を依頼した。その後，表 4 のとおり評価結果と評価根拠をまとめて Y 社に事実確認を依頼したところ，“事実だ”との回答があった。評価結果は次のルールに従って記入した。

・要求事項を満たす場合：“OK”

・要求事項を満たさない場合：“NG”

表 4　X 要求事項に対する Y 社の対策の評価結果と評価根拠（抜粋）

項番	要求事項	評価結果	評価根拠
5	X 業務で N サービスへのアクセスが可能な業務エリアは Y-CS 部の業務エリアだけに限定すること	NG	・現状のままでは，Y 社で N サービスにアクセスできるようになったら，［ c ］が，3 階以外から N サービスにアクセスできてしまう。 ・（省略）
8	X 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	NG	入室権限に，次の 2 点の不備がある。 ・［ d ］ ・［ e ］
12	（省略）	NG	・②複合機が初期設定のままになっている。
13	X 業務には，Y 社貸与の PC を使用すること	OK	（省略）
14	X 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	NG	・Y-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込みが可能となっている。
18	インターネット上の Web サイトへの X 情報の持出しをけん制する対策があること	NG	（省略）

〔評価結果に対する対応案の検討〕

後日，G 課長は T 部長と F 課長に，Y 社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“NG”の要求事項への対応を依頼した。Y 社は G 課長に③対応案を伝えた。G 課長は H 主任と相談の上，対応案を S 部長に報告した。

S 部長が表 4 及び対応案を X 社委員会に報告したところ，Y 社に X 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。X 社は Y 社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　〔US 部が利用しているコールセンタ用サービスの概要〕について，(1)，(2)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　DKIM	イ　DomainKeys	ウ　HTTP over TLS
エ　IMAP over TLS	オ　POP3 over TLS	カ　SMTP over TLS

(2) 本文中の下線①について，情報セキュリティ上のどのような効果が期待できるか。次の (i) ～ (vi) のうち，期待できるものだけを全て挙げた組合せを，解答群の中から選べ。

(i) 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

(ii) 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 X 情報が読まれるリスクを低減する効果

(iii) N 社のうちの US 部以外の従業員が NDB に不正にアクセスすることによって X 情報が漏えいするリスクを低減する効果

(iv) X 情報へのアクセスが許可された US 部の従業員が NDB を誤って操作することによって X 情報を変更するリスクを低減する効果

(v) 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

(vi) 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

ア (i)，(ii)	イ (i)，(ii)，(iii)	ウ (i)，(v)
エ (ii)，(iii)	オ (ii)，(v)	カ (iii)，(iv)
キ (iii)，(vi)	ク (iv)，(v)	ケ (iv)，(v)，(vi)

設問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　X業務に従事しないY-CS部の従業員によるX情報の不正な持出しリスクを低減

イ　X業務に従事するY-CS部の従業員によるX情報の不正な持出しリスクをN社に移転

ウ　X業務に従事するY-CS部の従業員によるX情報の不正な持出しリスクを回避

エ　システム管理部の従業員によるX情報の不正な持出しリスクを回避

設問3　〔X社の情報セキュリティ要求事項と評価〕について，(1)～(4)に答えよ。

(1)　表4中の［　c　］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。

cに関する解答群

ア　F課長

イ　T部長

ウ　X業務に従事するY-CS部の2名の一般従業員

エ　X業務に従事するY-CS部の2名の主任

オ　X業務に従事するY-CS部のパートタイマ

(2) 表 4 中の [d], [e] に入れる評価根拠として適切なものを，解答群の中から選べ。

d，e に関する解答群

ア　Y-CS 部の従業員が 3 階の業務エリアに入室できる。

イ　Y-CS 部のパートタイマが 5 階の業務エリアに入室できる。

ウ　営業部の従業員が 3 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 5 階の業務エリアに入室できる。

オ　退職者の一部が 3 階の業務エリアに入室できる。

カ　元 Y-CS 部の従業員が，他部門に異動した後も，3 階の業務エリアに入室できる。

(3) 表 4 中の下線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。次の (i) ～ (v) 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挙げた組合せを，解答群の中から選べ。

(i) X 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。

(ii) X 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。

(iii) X 業務の中で，複合機から送信されるメールが攻撃者宛に送信される。

(iv) 攻撃者が，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改ざんする。

(v) 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

ア (i)，(ii)	イ (i)，(ii)，(iii)	ウ (i)，(iii)，(iv)
エ (ii)，(iii)	オ (ii)，(iii)，(iv)	カ (ii)，(iv)，(v)
キ (iii)，(iv)	ク (iii)，(iv)，(v)	ケ (iv)，(v)

(4) 表 4 中の項番 14 について，Y 社が追加の対策をとり，要求事項を満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。次の (i) ～ (iv) のうち，適切なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) Y-PC 内のデータを外部記憶媒体に保存して持ち出される。

(ii) Y-PC 内のデータを複合機でプリントして持ち出される。

(iii) Y 社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 Y-PC に接続されて，Y-PC に当該ソフトウェアが導入される。

(iv) マルウェア付きのファイルが保存されている USB メモリを Y-PC に接続されて，Y-PC がマルウェア感染する。

解答群

ア (i)	イ (i)，(ii)，(iv)	ウ (i)，(iii)
エ (i)，(iv)	オ (ii)	カ (ii)，(iii)
キ (ii)，(iii)，(iv)	ク (iii)	ケ (iii)，(iv)
コ (iv)		

設問4　〔評価結果に対する対応案の検討〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，表 4 中の項番 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　N サービスのアクセス制御の設定機能で X 社及び Y 社以外からのアクセスを禁止する。

イ　N サービスの監査ログを監視し，3 階の業務エリア以外からのアクセスを検知する。

ウ　N サービスの顧客情報の操作権限の設定機能で，X 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 N サービスへのアクセスを禁止する。

オ　Y-CS 部の管理職は，N 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，N サービスへのアクセスを禁止する。

(2) 本文中の下線③について，表 4 中の項番 18 の要求事項への有効な対応案としてどのようなものがあるか。次の (i) ～ (v) のうち，有効なものだけを全て挙げた組合せを，解答群の中から選べ。

(i) N 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，導入が必要な場合にだけ，システム管理部に申請する。

(ii) N 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 X 業務を実施する。

(iii) N 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旨を通知する。

(iv) 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，N サービスにログインできる従業員を対象に，通知する。

(v) プロキシサーバのプロキシ制御機能を使用して，N サービス以外へのアクセスを禁止する。

解答群

ア (i)	イ (i)，(v)	ウ (ii)
エ (ii)，(iii)	オ (ii)，(v)	カ (iii)
キ (iii)，(iv)	ク (iv)	ケ (iv)，(v)
コ (v)		

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	13:10 ～ 13:50

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。