SC

平成29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

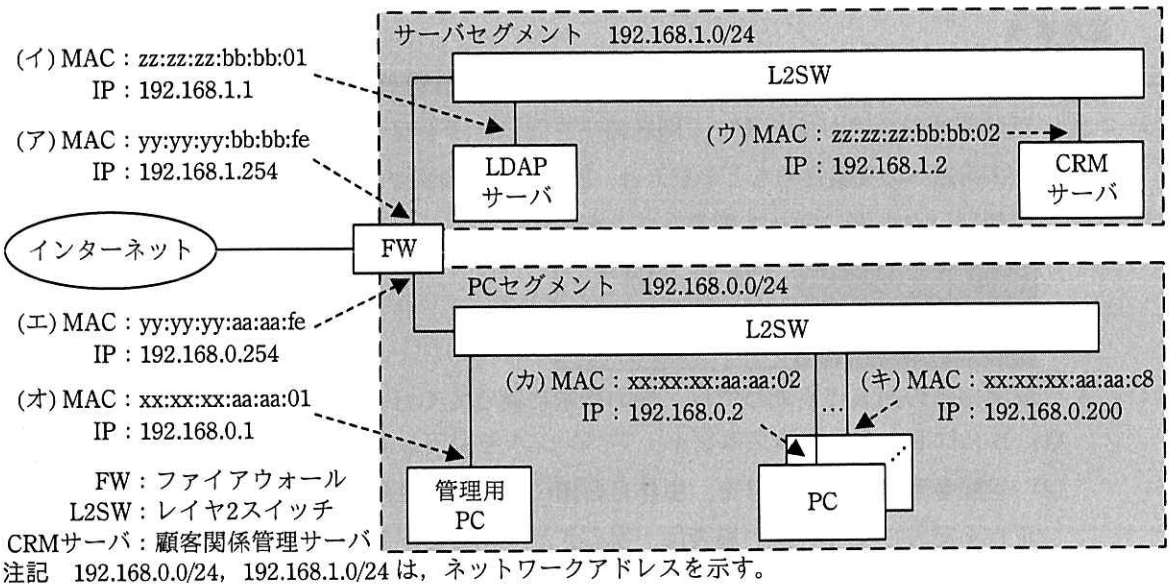
5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。3問とも○印で囲んだ場合は，はじめの2問について採点します。
   (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〕

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　社内で発生した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 1～3 に答えよ。

D 社は，従業員数 100 名のシステム開発会社である。D 社のネットワーク構成を図 1 に示す。



注記　192.168.0.0/24，192.168.1.0/24 は，ネットワークアドレスを示す。

図 1　D 社のネットワーク構成

D 社のネットワークでは静的に IP アドレスが付与され，各セグメント間の通信はステートフルパケットインスペクション型の FW で制限されている。FW のフィルタリングルールを表 1 に示す。

表 1　FW のフィルタリングルール

項番	送信元	宛先	サービス	動作	ログの記録
1	PC セグメント	インターネット	HTTP, HTTP over TLS	許可	する
2	PC セグメント	LDAP サーバ	LDAP	許可	しない
3	PC セグメント	CRM サーバ	HTTP over TLS	許可	する
4	管理用 PC	サーバセグメント	SSH	許可	する
5	PC セグメント	サーバセグメント	全て	拒否	する
⋮	⋮	⋮	⋮	⋮	⋮
20	全て	全て	全て	拒否	しない

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

従業員には，個人ごとに PC と利用者 ID が割り当てられており，自身の PC 上では，自身の利用者 ID に対して管理者権限が付与されている。利用者 ID は，LDAP サーバで一元管理されており，PC にログインする際，LDAP サーバで利用者認証が行われる。D 社の顧客情報は全て CRM サーバに保管されており，営業業務に携わる従業員は，PC から Web ブラウザで CRM サーバにアクセスして，顧客情報の登録・参照を行っている。

サーバ及びFWは，入退室管理されたサーバルーム内に設置されている。利用者ID作成などのサーバの運用は，サーバ管理者が，事前申請をした上で，管理用 PC から SSH でサーバにログインして行っている。SSH でログインする際も PC にログインする際と同様に，LDAP サーバで利用者認証が行われる。

D 社では，事前申請なしで CRM サーバへの SSH によるログインがあった場合，そのことを日次のバッチ処理によって顧客情報管理責任者である N 部長に電子メールで通知する仕組みを導入している。通知にはログイン時刻，SSH の接続元 IP アドレス及び利用者 ID が記載される。

〔セキュリティインシデントの発生〕

ある日，サーバ管理者の Y 主任の利用者 ID で，管理用 PC から CRM サーバにログインしたことを示す通知が N 部長に届いた。N 部長が，Y 主任に確認したところ，その時間帯にはログインしていないとのことであった。

Y 主任が CRM サーバの SSH 認証ログを確認すると，身に覚えがない自分のログイン（以下，不審ログインという）の記録が残っていた。Y 主任の報告を受けて，N 部長は，不正侵入のセキュリティインシデント（以下，インシデントという）が発生したと判断し，インターネット接続を遮断した上で，セキュリティ専門業者 Z 社に調査を依頼した。

Z 社の W 氏が，サーバへの不正侵入の有無，侵入手口及び顧客情報窃取の有無に関する調査を進めることになった。

〔サーバへの侵入手口の調査〕

W 氏は，まずサーバへの不正侵入の有無及び侵入手口の調査を行った。その調査結果を図 2 に示す。調査結果から，W 氏は図 3 に示す手順でサーバへの不正侵入が行

われていたと推測した。

・従業員 A さんの PC が遠隔操作型マルウェアに感染していたが，その他のサーバ及び PC のマルウェア感染は確認されなかった。
・A さんの PC に，ARP ポイズニングに使われるツールが削除された形跡があった。
・不審ログインからログアウトまでの時間帯に，管理用 PC にログイン中の利用者はいなかった。
・不審ログインがあった 5 分前に，LDAP サーバの SSH 認証ログに Y 主任の利用者 ID によるログインの記録があった。
・LDAP サーバ及び CRM サーバの SSH 認証ログに記録された接続元 IP アドレスは，全て管理用 PC の IP アドレスであった。

図 2　W 氏の調査結果

1. マルウェアに感染した A さんの PC を遠隔操作する。
2. A さんの PC 上で ARP ポイズニングを用いて，通信を盗聴する。
3. A さんの PC 上で通信を盗聴して，LDAP サーバ及び CRM サーバの IP アドレスを特定する。
4. A さんの PC 上で LDAP 通信を盗聴して，従業員の利用者 ID とパスワードを収集する。
5. A さんの PC から LDAP サーバ及び CRM サーバの SSH ポートへのアクセスを試みるが，アクセスに失敗する。
6. A さんの PC 上で通信を盗聴して，管理用 PC の IP アドレスを特定する。
7. A さんの PC 上で通信を盗聴して，サーバ管理者である Y 主任の利用者 ID とパスワードを入手する。
8. A さんの PC 上で管理用 PC の IP アドレスを詐称して，LDAP サーバ及び CRM サーバの SSH ポートにアクセスし，Y 主任の利用者 ID とパスワードでログインする。

図 3　W 氏が推測したサーバへの不正侵入手順（抜粋）

図 3 の 2 の通信が盗聴されている時点では，FW，管理用 PC 及び A さんの PC の ARP テーブルが，それぞれ表 2～4 に示すようになっていたと W 氏は推測した。

表 2　盗聴されている時点の FW の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.0.1	xx:xx:xx:aa:aa:02
192.168.0.200	xx:xx:xx:aa:aa:02

表 3　盗聴されている時点の管理用 PC の ARP テーブル（抜粋）

IP アドレス	MAC アドレス
192.168.0.254	a

表4　盗聴されている時点のAさんのPCのARPテーブル（抜粋）

IPアドレス	MACアドレス
192.168.0.1	b
192.168.0.254	c

図3の6の特定方法としては，管理用PCのIPアドレスを総当たりで推測することも考えられるが，そのような方法が採られた場合にFWのフィルタリングルール［ d ］によって記録されるはずのログが残っていなかった。このことから，①通信の盗聴によって管理用PCのIPアドレスが特定されたとW氏は推測した。

〔顧客情報窃取の有無の調査〕

続いて，W氏は顧客情報窃取の有無を調査した。CRMサーバの顧客情報を窃取する手口として三つ考えられたので，それぞれ調査を行った。

一つ目は，不正侵入されたCRMサーバからの直接の情報窃取である。調査した結果，CRMサーバからの直接の情報窃取はなかったと判断した。

二つ目は，AさんのPCからAさんがCRMサーバにアクセスした際の，AさんのPC又は通信からの情報窃取である。調査した結果，AさんはCRMサーバにはアクセスしていないことがFWのログ及び聞き取りから確認できた。

三つ目は，その他のPCからCRMサーバにアクセスした際の通信からの情報窃取である。D社内のWebブラウザの設定は，②サーバ証明書の検証に失敗した場合は接続しない設定にしている。このことから，CRMサーバにアクセスした際の通信からの情報窃取はなかったと判断した。

W氏は更に調査した結果，顧客情報の窃取はなかったとN部長に報告した。

〔セキュリティ対策の実施〕

Y主任は今回のインシデントを受けて，まず，マルウェアの駆除，ARPテーブルの初期化，全利用者IDのパスワード変更などの暫定対応を行った。その後，W氏の助言を受けながら，今回のように社内ネットワークに侵入された場合の被害拡大を防ぐために，社内ネットワークにおいて，二つのセキュリティ対策を実施することにした。

第一に，図3の8を防ぐために，図4のようにネットワーク構成を変更し，表5のようにFWのフィルタリングルールを変更することにした。これらの変更によって，③図3の6が行われることも防ぐことができる。また，④仮に図3の6とは異なる方法で管理用PCのIPアドレスが特定され，図3の8が試みられた場合でも，TCPコネクションの確立を防ぐことができる。

第二に，図3の4を防ぐために，LDAPサーバへの通信ではLDAP over TLSを利用することにした。

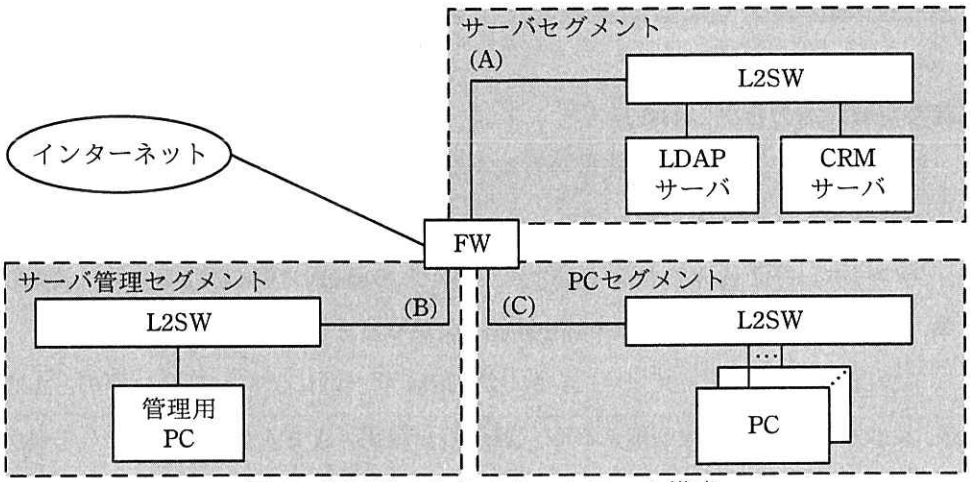


図4　変更後のD社のネットワーク構成

表5　変更後のFWのフィルタリングルール

項番	送信元	宛先	サービス	動作	ログの記録
1	PCセグメント	インターネット	HTTP, HTTP over TLS	許可	する
2	PCセグメント	LDAPサーバ	LDAP over TLS	許可	しない
3	PCセグメント	CRMサーバ	HTTP over TLS	許可	する
4	管理用PC	サーバセグメント	SSH	許可	する
5	PCセグメント	サーバセグメント	全て	拒否	する
6	PCセグメント	サーバ管理セグメント	全て	拒否	する
7	サーバ管理セグメント	脆弱性修正プログラム提供元, ウイルス定義ファイル提供元	HTTP over TLS	許可	する
8	サーバ管理セグメント	LDAPサーバ	LDAP over TLS	許可	する
9	サーバ管理セグメント	PCセグメント	全て	拒否	する
⋮	⋮	⋮	⋮	⋮	⋮
24	全て	全て	全て	拒否	しない

注記　項番が小さいルールから順に，最初に一致したルールが適用される。

これらの対策は N 部長によって承認され，今回と同様のインシデントに対する社内ネットワークのセキュリティ耐性が高まることになった。

設問1　〔サーバへの侵入手口の調査〕について，(1)～(3)に答えよ。

(1) 表 3 中の［ a ］及び表 4 中の［ b ］，［ c ］に入れる適切な字句を，図 1 中の機器の MAC アドレスから選び，(ア)～(キ)の記号で答えよ。

(2) 本文中の［ d ］に入れる適切なフィルタリングルールを，表 1 中の項番 1～5 から選び，数字で答えよ。

(3) 本文中の下線①について，攻撃者が管理用 PC の IP アドレスを特定するために盗聴したのはどのような通信か。送信元，宛先及びサービスを，それぞれ解答群の中から選び，記号で答えよ。

解答群

ア　ARP	イ　A さんの PC	ウ　FW
エ　HTTP over TLS	オ　LDAP	カ　LDAP サーバ
キ　SSH	ク　インターネット	ケ　管理用 PC

設問2　本文中の下線②について，このような設定にすることは，A さんの PC に侵入した攻撃者によって行われるどのような攻撃への対策になるか。攻撃名を 10 字以内で答えよ。また，攻撃に際して詐称される対象の機器名を図 1 中から選び，答えよ。

設問3　〔セキュリティ対策の実施〕について，(1)，(2)に答えよ。

(1) 本文中の下線③について，防ぐことができる理由を 35 字以内で具体的に述べよ。

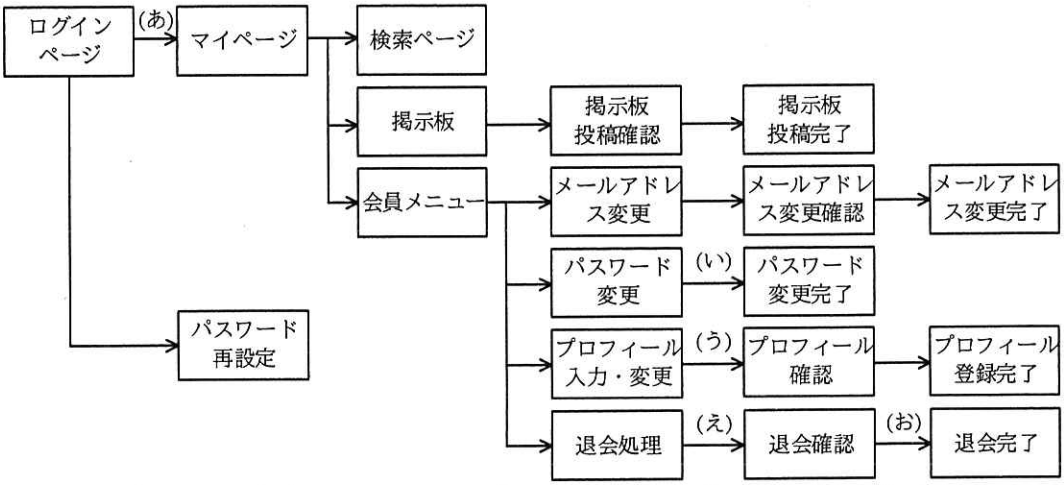
(2) 本文中の下線④について，TCP コネクション確立開始時の SYN パケットと SYN-ACK パケットはそれぞれどのような経路をたどるか。図 4 中の経路を通過する順に選び，(A)～(C)の記号で答えよ。

問2　Webサイトのセキュリティ対策に関する次の記述を読んで，設問1～3に答えよ。

E社は，従業員数200名の情報サービス事業者である。E社は，3年前からWebサイトα（以下，サイトαという）を利用して，次のような機能をもつ会員制の飲食店情報提供サービスを行っている。

・飲食店情報の検索
・飲食店情報に関する掲示板での投稿
・新規登録情報の，会員への電子メール（以下，メールという）による通知

サイトαに対する脆弱(ぜいじゃく)性修正プログラムの適用や，コンテンツ作成などの日々の作業は，情報提供サービス担当チームが行っている。チームはリーダのQさんと5名のメンバで構成されている。サイトαで稼働しているWebアプリケーションソフトウェアは，情報提供サービス担当チームがベンダに開発と保守を委託している。サイトαの画面遷移図を図1に，画面遷移の仕様を表1に示す。



注記1　ログインページ以外からのマイページへの画面遷移，エラー時の画面遷移，画面を戻るための遷移，ログアウトの画面遷移は省略している。
注記2　全画面とも同一ドメイン（www.e-sha.co.jp）で提供されている。

図1　サイトαの画面遷移図（抜粋）

表1　サイトαの画面遷移の仕様（抜粋）

画面遷移	PCでの操作例，URL及びPOSTデータ	操作の結果
(あ)	操作例：利用者ID（例：user0302）とパスワード（例：aBcD1234）を入力し，ログインボタンを押す。 URL：https://www.e-sha.co.jp/login POST データ：action_id=login&user_id=user0302&passwd=aBcD1234	・user_id と，passwd のハッシュ値がサイトαに登録されたものと同じ場合，新しいセッションID（JSESSIONID）とセッションオブジェクトが取得され，マイページが表示される。JSESSIONID は Cookie に格納される。それ以外の場合，セッション ID とセッションオブジェクトは取得されず，ログインページに戻る。 ・ログイン記録（利用者 ID と時刻）が取得される。
(い)	操作例：現在のパスワード（例：aBcD1234）と新しいパスワード（例：aBcD5678）を入力し，変更ボタンを押す。新しいパスワードは確認のために，2回入力する。 URL：https://www.e-sha.co.jp/member/changepasswd POST データ：action_id=submit&old_passwd=aBcD1234&new_passwd1=aBcD5678&new_passwd2=aBcD5678	・次を全て満たす場合はパスワードが new_passwd1 の値に変更され，次画面が表示される。 - old_passwd のハッシュ値が，サイトαに登録された現在のセッションをもつ利用者のパスワードのハッシュ値と同じである。 - old_passwd と new_passwd1 の値が異なる。 - new_passwd1 と new_passwd2 の値が同じで，かつ，定められた複雑さを満たす。 ・それ以外の場合はパスワードが変更されず，エラー画面が表示される。
(う)	操作例：名前（例：Bob）とコメント（例：よろしく）を入力し，確認ボタンを押す。 URL：https://www.e-sha.co.jp/member/profile POST データ：action_id=confirm&nickname=Bob&comment=%E3%82%88%E3%82%8D%E3%81%97%E3%81%8F [1]	・nickname と comment に入力された値がセッションオブジェクトに格納され，次画面が表示される。profile_token が生成されてセッションオブジェクトに格納され，profile_token（例：CACC321A638BBC11DE9352EB8D5E56A3）がプロフィール確認画面の hidden に格納される。 ・プロフィール入力・変更画面では一部の HTML の要素の入力が許可されている。（許可されている要素：b，font，i，s，sub，sup，u） ・コメントに URL を記載するとリンクとして表示される。
(え)	操作例：退会理由（例：特になし）を入力し，退会確認ボタンを押す。 URL：https://www.e-sha.co.jp/member/taikai POST データ：action_id=confirm&taikai_message=%E7%89%B9%E3%81%AB%E3%81%AA%E3%81%97 [2]	・taikai_message に入力された値がセッションオブジェクトに格納され，次画面が表示される。taikai_token（例：B582DF03524FBB9DBCCE0BA0610F2EA1）が生成されてセッションオブジェクトに格納され，退会確認画面の hidden に格納される。[3]

表1　サイトαの画面遷移の仕様（抜粋）（続き）

画面遷移	PCでの操作例，URL及びPOSTデータ	操作の結果
(お)	操作例：退会ボタンを押す。 URL：https://www.e-sha.co.jp/member/taikai POSTデータ：action_id=submit&taikai_token=B582DF03524FBB9DBCCE0BA0610F2EA1	・taikai_tokenの値がセッションオブジェクト内の値と同じ場合，退会処理が行われ，次画面が表示される。違う場合，退会処理が行われず，エラー画面が表示される。 ・退会処理時にセッションIDとセッションオブジェクトが無効にされ，ログアウトされる。

注[1] “よろしく”をURLエンコードした値
注[2] “特になし”をURLエンコードした値
注[3] taikai_tokenの値が0になることはない。

〔利用者からの問合せ〕

ある日，サイトαの利用者L氏から，“今朝9時にログインし，サイトαを利用していたら，10時に急にログアウトさせられ，その後ログインできなくなった。パスワードを再設定しようとしたが，エラーが表示され，再設定できない。”という内容のメールがE社宛てに届き，他にも同様の問合せが数件来た。

情報提供サービス担当チームのXさんがサイトαの会員情報データベースにアクセスし，L氏の情報を確認したところ，退会処理が完了していた。Xさんは，誰かが嫌がらせ目的でL氏のアカウントで不正ログインし，退会処理を行った可能性を疑った。①Xさんは，L氏に詳細な利用状況を確認し，その確認内容とログイン記録を照合した結果から，L氏のアカウントは少なくとも今日は不正ログインされていないとの結論に至った。

Xさんが，ログインできなくなる前にどのような操作をしたかをL氏に聞いたところ，サイトα内の掲示板に投稿していた人のプロフィール画面を見て，そこに記載されていたリンクをクリックしたとのことであった。リンク先は，別サイトのURLであり，かつ，Xさんが確認した時点ではリンク先は既に削除されていた。

Xさんは，今回の事象が起きたのはサイトαに脆弱性があるからかもしれないと考え，セキュリティ専門業者J社にWebアプリケーションソフトウェアの脆弱性検査（以下，WebAP検査という）を依頼することにした。WebAP検査の結果，脆弱性が二つ（以下，脆弱性1，脆弱性2という）検出された。

〔脆弱性1について〕

脆弱性1は［ a ］の脆弱性であった。脆弱性1を確認した手順を表2に示す。

表2　脆弱性1を確認した手順

項番	手順	画面遷移（お）を試みる際のPOSTデータ	表示された画面
1	画面遷移（え）を行った後，画面遷移（お）を試みる	action_id=submit&taikai_token=B582DF03524FBB9DBCCE0BA0610F2EA1 [1)]	退会完了
2	画面遷移（え）を行った後，画面遷移（お）を試みる	action_id=submit&taikai_token=0	エラー画面
3	画面遷移（え）を行った後，画面遷移（お）を試みる	action_id=submit	退会完了
4	画面遷移（え）を経ずに，ログイン後すぐに画面遷移（お）に相当するアクセスを試みる	action_id=submit&taikai_token=0	エラー画面
5	画面遷移（え）を経ずに，ログイン後すぐに画面遷移（お）に相当するアクセスを試みる	action_id=submit	エラー画面

注[1)] 画面遷移（え）で生成されたtaikai_tokenの値とする。

次は，Xさんが J社の情報処理安全確保支援士K氏から，脆弱性1についての報告を受けた時の会話である。

Xさん：開発委託時の要件に［ a ］の脆弱性への対策を含めていたので，脆弱性1の対策はできていると思っていました。

K氏　：対策を試みたけれど，プログラムの実装に不備があったようです。プロフィール確認画面についても脆弱性1が確認されています。

Xさん：そうですか。退会処理が行われてしまった利用者がクリックしたリンク先はどのようなものだったのでしょうか。

K氏　：例えば，図2のようなHTMLです。このHTMLは，表2中の項番［ b ］のような動作をWebブラウザにさせます。

Xさん：変更操作がある画面のうち，パスワード変更画面は，そもそも［ a ］の脆弱性への対策をしていませんが，問題ありませんか。

K氏　：パスワード変更画面では表1にあるように，［ c ］を入力させる仕様

です。［ c ］は攻撃者が［ d ］情報であることを前提としてよいので，問題ありません。画面遷移（お）のような実装の不備もないようでした。

```
 1 <html>
 2 <head>
 3 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
 4 </head>
 5 <body>
 6 <iframe src="ifrm1.html" width="1" height="1" name="ifrm1"></iframe>
 7 <iframe src="ifrm2.html" width="1" height="1" name="ifrm2"></iframe>
 8 <form target="ifrm1" method="POST" action="https://www.e-sha.co.jp/member/taikai">
 9 <input type="text" name="action_id" value="［ e ］">
10 <input type="text" name="taikai_message" value="OK">
11 <input type="submit">
12 </form>
13 <form target="ifrm2" method="POST" action="https://www.e-sha.co.jp/member/taikai">
14 <input type="text" name="action_id" value="［ f ］">
15 <input type="submit">
16 </form>
17 <script>setTimeout('document.forms[0].submit()',0);</script>
18 <script>setTimeout('document.forms[1].submit()',1000);</script>
19 </body>
20 </html>
```

図２　退会処理が行われてしまう HTML

〔脆弱性２について〕

脆弱性 2 は“クロスサイトスクリプティング”であった。脆弱性 2 を確認したのはプロフィール入力・変更画面であった。次はＫ氏とＸさんとの会話である。

Ｋ氏　：プロフィール入力・変更画面は，利用者が入力できる HTML の要素が制限されています。しかし，例えば“<b>”タグ中に，②特定の属性を指定することによってスクリプトの実行が可能です。スクリプト実行の結果，Cookie の属性の設定によっては，Cookie の情報が盗まれます。これを用いて，［ g ］が行われ，勝手にプロフィールを閲覧されたり，変更されたりするおそれがあります。

Ｘさん：そういうことですか。では，利用者が入力できる HTML の要素の制限は変

えずに，［ h ］という仕様に変更したいと思います。

K氏　：それで問題ありません。

X さんは，二つの脆弱性について，対策をベンダに依頼した。対策後，J 社に WebAP 検査を依頼し，問題がないことを確認した。X さんは，リリース前の WebAP 検査の義務化を Q さんに提案し，採用された。

設問1　本文中の下線①について，L 氏のアカウントが不正ログインされていないとの結論に至るには，L 氏に確認した内容から分かる何の値と，ログイン記録から分かる何の値を抽出して，一致していることが確認できればよいか。それぞれ 25 字以内で述べよ。

設問2　〔脆弱性 1 について〕について，(1)～(4)に答えよ。

(1)　本文中の［ a ］に入れる脆弱性の名称を，カタカナ 20 字以内で答えよ。

(2)　本文中の［ b ］に入れる表 2 中の項番を 1～5 から選び，数字で答えよ。

(3)　本文中の［ c ］，［ d ］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

(4)　図 2 中の［ e ］，［ f ］に入れる適切な文字列を，それぞれ 10 字以内で答えよ。

設問3　〔脆弱性 2 について〕について，(1)～(3)に答えよ。

(1)　本文中の下線②に該当する属性を解答群の中から全て選び，記号で答えよ。

解答群

ア	accesskey	イ	class	ウ	hidden	エ	id
オ	lang	カ	onclick	キ	onmouseover	ク	title

(2)　本文中の［ g ］に入れる攻撃の名称を 15 字以内で答えよ。

(3)　本文中の［ h ］に入れる仕様を 25 字以内で具体的に述べよ。

問3　クラウドサービスの認証連携に関する次の記述を読んで，設問1～3に答えよ。

F社は，従業員数300名のソフトウェア開発会社である。F社では，社外のクラウドサービスを試行的に導入し始めており，交通費精算サービス，グループウェアサービス，オンラインストレージサービスの三つを現在利用している。これらのクラウドサービスには，各クラウドサービスの利用者IDとパスワードを用いてログインする。これらのクラウドサービスは，社内からの利用に限定するという社内ルールを定めている。

従業員が利用する端末は，社内ネットワークに設置されており，ウイルス対策ソフトが導入され，最新のウイルス定義ファイルが毎日適用されている。社外から社内ネットワークへの通信はファイアウォールによって禁止されている。端末からクラウドサービスを利用する際には，プロキシサーバを経由する必要がある。

〔クラウドサービスへの不正アクセス〕

ある日，交通費精算サービスで従業員の振込先口座が勝手に変更されたとの相談が，経理部から情報システム部のC主任にあった。Rさんの振込先口座がF社指定の銀行以外の口座に変更されていたので，Rさんに確認したところ，本人による変更ではないことが分かったとのことであった。

C主任は，社外の攻撃者による不正アクセスの可能性を考え，交通費精算サービスに記録されているログイン記録を調査した。F社で利用しているクラウドサービスではログイン記録として，アクセス日時，利用者ID，接続元IPアドレス，接続先URLが記録されている。調査の結果，Rさんの利用者IDによるログイン記録には，接続元IPアドレスとして，F社のIPアドレス以外に，海外のIPアドレスが一つあった。Rさんに話を聞いたところ，このログインには心当たりがないということであった。Rさんに更に詳しく話を聞いたところ，4月9日に交通費精算サービスから登録情報の確認を促す電子メール（以下，メールという）が1通，Rさんの私用メールアドレスに届いており，Rさんが4月10日にそのメールを自宅で読み，記載内容に従って自宅からログイン操作を行ったことが分かった。そのメールをRさんから転送してもらい，C主任がメールに記載されていたURLを確認したところ，交通費精算サービスを模したフィッシングサイトであった。C主任はこのフィッシングサイト

から利用者 ID とパスワードが盗まれた可能性が高いと判断した。そこで，R さんがパスワードを使い回している可能性も考慮して，他のクラウドサービスに対する R さんのログイン記録も調査した。その結果，他のクラウドサービスに対する R さんの利用者 ID を用いたログインは，F 社からのものだけであることを確認した。

今回は金銭的な損害に至らなかったが，情報システム部の B 部長は早急な対策が必要と考え，C 主任に暫定対策の実施と根本的な対策の検討を指示した。

〔暫定対策の実施と根本的な対策の検討〕

C 主任はまず，暫定対策として三つの対策を行うことにした。第一に，フィッシングメールに注意するよう従業員に周知した。第二に，F 社で利用している各クラウドサービスに対するログイン記録を C 主任が調査して，①F 社以外からのログインがあった利用者 ID を特定し，その利用者 ID を利用する者にはパスワードを変更させることにした。第三に，F 社以外からのログインを検知できるよう，ログイン記録の監視を行うことにした。C 主任は暫定対策が完了したことを確認し，根本的な対策の検討を開始した。

C 主任は，今回の不正アクセスの原因の一つが，F 社の IP アドレス以外からクラウドサービスへのログインが可能になっていたことにあると考え，F 社の IP アドレス以外からのログインを制限することが可能か調査した。F 社で利用しているクラウドサービスのうち，グループウェアサービスだけは，接続元 IP アドレスを制限する機能を備えていたので，その機能を有効化し，社内からだけログインできるように設定した。しかし，残りのクラウドサービスは接続元 IP アドレスの制限機能を備えていなかった。

C 主任は，接続元を制限する他の方法を検討した。その結果，クラウドサービスへログインする際，F 社に既に設置してある LDAP サーバでの認証を必要とすることにすれば，接続元を制限できるようになると考えた。そこで，F 社で利用しているクラウドサービスを調べたところ，全て SAML（Security Assertion Markup Language）を用いた認証連携に対応していることが分かった。C 主任は，クラウドサービスと LDAP サーバとの間で，SAML を用いた認証連携による接続元の制限を検討することにした。

〔SAML を用いた認証連携と接続元制限方式の概要〕

SAML は，認証，認可などの情報を安全に交換するためのフレームワークである。SAML を用いることによって，利用者にサービスを提供するサービスプロバイダ（以下，SP という）と，ID プロバイダ（以下，IdP という）との間で利用者の認証結果などの情報を安全に連携することができる。SAML には複数の処理方式が存在する。今回 F 社で導入を検討している方式のシーケンスを図 1 に示す。図 1 中の各通信のプロトコルは，IdP と LDAP サーバ間は LDAP であり，それ以外は HTTP over TLS である。

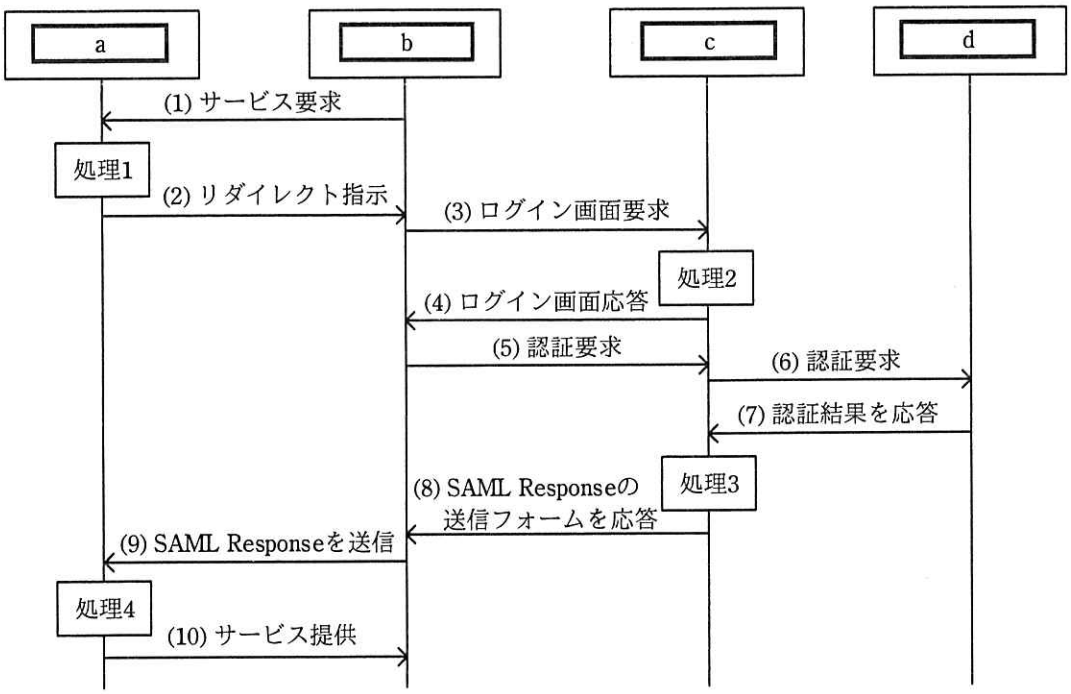


図 1　導入を検討している方式のシーケンス

SAML を用いた認証連携を行うためには，事前に IdP と SP との間で様々な情報を共有することによって，信頼関係を構築しておく必要がある。事前に共有する情報としては，通信の方式や連携する属性情報などが記述されたメタデータ，［　e　］で生成して送出する URL，［　f　］において必要な IdP のディジタル証明書などがある。

図 1 中の処理 1～4 の処理内容を表 1 に示す。

表1　処理内容

処理番号	処理内容
処理1	・IdPに認証を要求するSAML Requestを生成する。 ・SAML Requestをエンコードする。 ・エンコード結果をIdPのログイン画面のURLと組み合わせて，リダイレクト先URLを生成する。
処理2	・URL内の［　g　］からSAML Requestを取得する。 ・信頼関係が構築されたSPからの認証要求であることを検証する。
処理3	・利用者の認証が成功した場合，認証結果やSPとの間で連携する属性情報，有効期間，それらの情報に対するディジタル署名を含めたSAML Responseを生成する。
処理4	・SAML Responseに含まれるディジタル署名を検証することによって，ディジタル署名が［　h　］によって署名されたものであること，及びデータの［　i　］がないことを確認する。 ・SAML Response内の属性情報も検証することによって，サービスを提供すべきか決定する。

C主任は図1のシーケンスから，②IdPを社内ネットワークに設置しても認証情報の連携が成立することを確認した。そこで，IdPは社内ネットワークに設置し，IdPのログイン画面のURLのFQDNには，社内のFQDNを割り当てることにした。

〔SAMLを用いた認証連携と接続元制限の動作検証〕

最後にC主任は，F社で利用しているクラウドサービスを用いて，SAMLによる認証連携の動作を検証することにした。C主任はIdPを社内ネットワークに設置して必要な設定を行い，各クラウドサービス上に，既に利用しているものとは別の検証用アカウントを作成し，社内からのクラウドサービスへのログインが可能であることを確認した。また，③社外からクラウドサービスへのログインを試みると，失敗することも確認した。

C主任は検証結果をB部長に説明し，承認を得て，SAMLを用いた認証連携と接続元制限を開始した。また，シングルサインオンも併せて実現したことによって，クラウドサービスを利用する従業員の利便性も向上させることができた。

設問1　本文中の下線①について，条件を満たす利用者 ID を特定するためには，どのような条件を満たすログイン記録を抽出すればよいか。満たすべき条件を 35 字以内で述べよ。

設問2　〔SAML を用いた認証連携と接続元制限方式の概要〕について，(1)～(5)に答えよ。

(1) 図 1 中の［ a ］～［ d ］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 IdP　　イ LDAP サーバ

ウ SP　　エ 利用者端末の Web ブラウザ

(2) 本文中の［ e ］，［ f ］に入れる適切な処理番号を，表 1 中の処理 1～4 の中から選び，答えよ。

(3) 表 1 中の［ g ］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 Cookie　　イ HTML　　ウ クエリ文字列

エ スキーム　　オ リファラ

(4) 表 1 中の［ h ］，［ i ］に入れる適切な字句を，それぞれ 5 字以内で答えよ。

(5) 本文中の下線②について，SP と IdP が直接通信できないにもかかわらず，認証情報の連携が成立するのはなぜか。その理由を，35 字以内で述べよ。

設問3　本文中の下線③について，社外から交通費精算サービスとグループウェアサービスにアクセスしたとき，それぞれのサービスは，異なる理由でログインに失敗する。それらは，図 1 中のどの通信ができないことによるものか。図 1 中の(1)～(10)から選び，答えよ。また，その理由を，それぞれ 35 字以内で述べよ。

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，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。
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。