SC

平成24年度　秋期
情報セキュリティスペシャリスト試験
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　インターネット Web サイトの刷新に関する次の記述を読んで，設問 1～4 に答えよ。

A 社は，従業員数 700 名の外食サービス会社であり，地方都市で事業を展開している。A 社グループ傘下には，レストラン，ピザ店及びハンバーガー店がある。A 社では，これまで，様々な業務のシステム化を行ってきたが，今年末の宅配すし事業の立上げを契機に，販売促進システムの一部であるインターネット Web サイトにおけるサービス向上を検討することになった。

〔A 社のインターネット Web サイトの概要〕

A 社のインターネット Web サイトには，一般公開用のもの（以下，一般サイトという。ドメインは a-sha.co.jp）と，事前に登録した会員向けのもの（以下，会員サイトという。ドメインは a-sha-kaiin.com）がある。

一般サイトでは，会社情報及び商品情報を提供しており，誰でも閲覧できる。一般サイトは，コンテンツの更新も含めて B 社に運用管理を委託している。会員サイトは，一般サイトにあるリンクで示された Web ページでログインでき，登録した届け先住所を用いた手軽な注文が可能で，注文履歴に基づいてお勧め商品に関する情報を表示するといったサービスを提供している。会員の誕生日には割引券も発行しており，評判が良い。

会員サイトは個人情報を扱うことから，①サーバ認証による HTTPS を採用し，その上でのフォームを用いた利用者認証を行っている。例えば，ある会員がブラウザで会員サイトにアクセスしようとすると，利用者 ID とパスワードによる利用者認証が求められ，認証に成功すると，会員サイトにアクセスできるようになる。クッキーの有効期限が切れるか，利用者がログアウトした後は，当該ブラウザから会員サイトにアクセスできなくなり，再び利用者認証を求められる。

会員サイトは，D 社に運用管理を委託しており，A 社情報セキュリティポリシ上，個人情報を扱う会員サイトから一般サイトへのデータの転送といった機密データの連携は一切行わないことになっている。

〔インターネット Web サイトのサービス向上策の検討〕

会員が一般サイトにアクセスした際に，当該会員の獲得ポイント状況，最近の注文

状況のほか，近隣のグループ店からのお知らせなどの情報を表示するサービス（以下，ターゲット型広告サービスという）を検討することにした。そこで，最近話題になっているマッシュアップ技術を有効活用したサービス（以下，マッシュアップサービスという）が実現可能かどうかを調査することになった。

マッシュアップサービスの実現に関しては，まず，Ajax（Asynchronous JavaScript + XML）という技術を用いることを検討した。

Ajax を用いると，Web ページ全体を再描画することなく，現在表示されている Web ページの表示の一部だけを更新することができる。例えば，［ a ］を利用する HTML ファイル群をブラウザがダウンロードして実行すると，非同期的又は同期的に Web サーバにアクセスし，そのレスポンスデータを用いて Web ページを更新することができる。

しかし，通常，ブラウザではセキュリティ確保のための［ b ］ポリシが採用されているので，［ a ］を利用する HTML ファイル群をダウンロードして実行する際，FQDN，プロトコル又はポート番号のいずれかが，ダウンロードしたものと異なる URI にはアクセスできず，A 社が想定するターゲット型広告サービスを実現できない。そこで，次に，JSONP（JavaScript Object Notation with Padding）という技術を用いて，マッシュアップサービスを実現することを検討した。JSONP を用いて上記の 3 要素のいずれかが異なる URI からでもデータを取得することが可能な JavaScript（以下，JSONP 呼出しスクリプトという）を記述できる。

A 社では JSONP を用いてターゲット型広告サービスを実現する仕組みを検討した。図 1 はその案である。この案では，会員のポイントの獲得状況を表示するサービス（以下，ポイント表示サービスという）用の JSONP 呼出しスクリプト（図 2）を呼び出すページを，一般サイトのトップページに用意しておく。例えば，利用者 ID を user1 としてログインした会員が，一般サイトのトップページを閲覧した際，会員サイトから送られてくる図 3 に例示したような JSONP 型データを用いて，その月の獲得ポイントとトータルの獲得ポイントを表示する。

A 社ではポイント表示サービスのほかにも，会員の誕生月にポイントを 2 倍付与するサービスと，会員が住む地域のグループ店からのお得情報を提供するサービスを検討している。

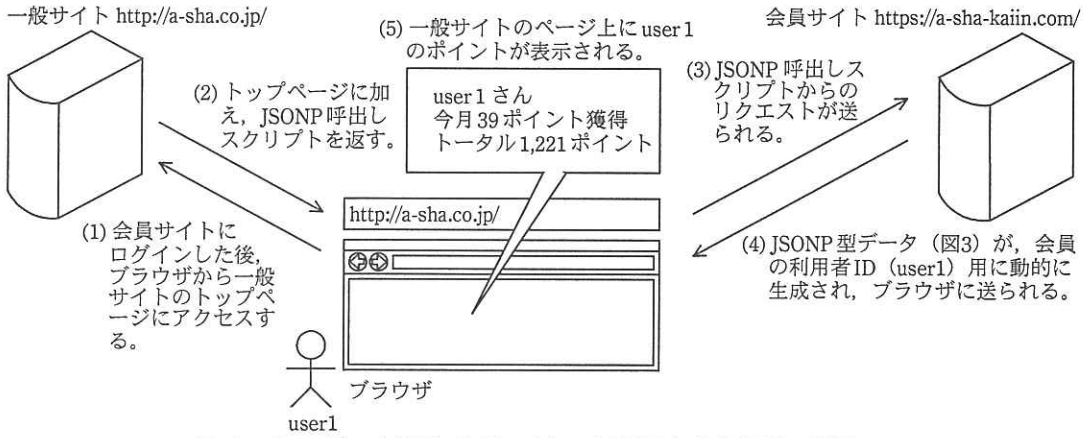


図１　ターゲット型広告サービスを実現する仕組み（案）

```
function putUserData(data) {
    dispUserPoint(data.name, data.thisMonthPoint, data.totalPoint);
}
// データ提供用に用意された会員サイトのURL
var url = "https://a-sha-kaiin.com/callback.json";
// 動的にSCRIPTタグを生成
var script = document.createElement("script");
script.setAttribute("src", url);
```

注記　dispUserPointは，ブラウザに表示をするために別途用意された関数である。

図２　ポイント表示サービス用のJSONP呼出しスクリプト（抜粋）

```
putUserData({name:"user1", thisMonthPoint:39, totalPoint:1221,
birth:"1978/3/15", address:"user1の住所", telephone:"029-xxx-yyyy"});
```

図３　会員サイトから送られてくるJSONP型データの例

〔セキュリティに関する検討〕

A社では，マッシュアップサービスを初めて導入することもあり，ターゲット型広告サービスの仕組みについて，セキュリティ専門家のZ氏にレビューを受けた。すると，ポイント表示サービスの仕組みには，次に示すようにJSONP呼出しスクリプトを悪用する攻撃で会員の個人情報が漏えいする可能性があるとの指摘を受けた。

A社のポイント表示サービスの仕組みの場合，［c］から送られる［d］が，会員の個人情報を含む。しかし，②ある条件が成立しているとき，悪意あるWebサイトにアクセスし，図4のように動作するJSONP呼出しスクリプトを［e］が実行すると，［d］に含まれる会員の個人情報を奪われる可能性がある。

ステップ1)　[c] にアクセスし，目的とする [d] を取得する。
ステップ2)　取得した [d] から会員の個人情報を抽出して，悪意あるWebサイトに転送する。

図4　悪意あるJSONP呼出しスクリプトの動作概要

Z氏からは，このような攻撃に対する一般的な対策として図5が示され，対応をA社関係者で検討した。

JSONP型データをブラウザに送信する前に，そのリクエストが正規のものであることを確認し，確認できた場合にだけJSONP型データをレスポンスで返す。この確認の実現方法には次の二つがある。
(1)　認証情報を用いた確認
　リクエストのHTTPヘッダに埋め込んである認証情報を確認する。認証情報とは，そのリクエストが [f] からのアクセスであることを確認できるものである。(以下，省略)
(2)　Refererヘッダによる参照元の確認
　JSONP型データをリクエストする直前に特定のページにアクセスしていたことをRefererヘッダで確認する。(以下，省略)

図5　JSONP呼出しスクリプトを悪用しようとする攻撃への一般的な対策

ポイント表示サービスの実現においては，会員が一般サイトのトップページにアクセスした際，JSONP呼出しスクリプトが会員サイトにアクセスする。そのため，図5の(1)の対策をとるには，一般サイトで“トップページへのアクセスのリクエストが [f] からのアクセス”という情報が必要になる。しかし，一般サイトと会員サイトの運用管理会社が違うこともあり実現方法の検討に期間を要してしまうので，この対策方法は見送ることにした。

図5の(2)の対策については，A社のWebサイトは様々な環境の利用者を想定していることから，Refererヘッダの情報がサーバに [g] というケースもあり得るので，Refererヘッダの情報の利用を前提としてポイント表示サービスを実現すると，正規のリクエストか否かを区別できないケースがある。そのため，この対策方法も見送ることにした。

Z氏との検討の結果，ポイント表示サービスを含むターゲット型広告サービスは，将来普及が見込まれる [a] の新規格を用いることも含めて検討課題とし，最終的には，ターゲット型広告サービスを除いてA社のWebサイトを刷新することとした。

設問 1　本文中の［　a　］，［　b　］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　APT　　イ　ATM　　ウ　Same-Origin

エ　XMLHttpRequest　　オ　アノニマス　　カ　プライバシ

設問 2　本文中の下線①について，SSL のクライアント認証と比較した場合の，サーバ認証による HTTPS 通信上でフォームを用いた利用者認証を行う利点を，25 字以内で述べよ。

設問 3　悪意ある JSONP 呼出しスクリプトについて，(1)～(3)に答えよ。

(1)　本文及び図 4 中の［　c　］並びに本文中の［　e　］に入れる適切な字句を答えよ。

(2)　本文中の下線②における条件を，本文に即して，50 字以内で述べよ。

(3)　本文及び図 4 中の［　d　］に入れる適切な字句を，10 字以内で具体的に答えよ。

設問 4　JSONP を用いて，個人情報を扱う際の対策の検討について，(1)，(2) に答えよ。

(1)　本文及び図 5 中の［　f　］に入れる適切な字句を，10 字以内で答えよ。

(2)　本文中の［　g　］に入れる適切な字句を，10 字以内で答えよ。

問2　ログの管理に関する次の記述を読んで，設問1～3に答えよ。

H 社は，200 名が勤務する高級化粧品の訪問販売会社である。H 社では，顧客の連絡先，訪問記録，購買履歴などの個人情報を管理する顧客管理システム（以下，B システムという）を利用している。B システムを利用しているのは，営業部の 1 課～5 課に所属する 140 名である。そのうち，営業を行っている 120 名は個人情報にアクセスする権限をもち（以下，有権限者という），担当顧客の情報を記録，参照している。残りの 20 名は，売上状況などを集計するためだけに B システムを利用しているので，個人情報にアクセスする権限をもたない（以下，無権限者という）。各営業部員は貸与された端末を社内で利用している。

最近，H 社の同業他社である C 社において，顧客の個人情報がシステムから漏えいするという事件があった。そこで H 社では，情報システム部の D 部長が中心となって個人情報漏えい対策を強化することになった。D 部長は，対策の検討に当たって部下の E 課長に対し，H 社のシステムの中で最も多くの個人情報を保有している B システムのアクセス管理の状況を確認するように指示した。

E 課長は，B システムの利用者 ID の管理状況を調査した。その結果，次の点を確認することができた。

- 利用者 ID の登録，変更及び削除は，申請に基づいて実施している。
- 3 か月ごとに利用者 ID と利用者名の一覧を営業部の各課長に提示の上，業務上の必要性について確認している。なお，利用者 ID と利用者は 1 対 1 に対応している。
- B システムのログを取得し，3 年間保存している。

E 課長がこれらの調査結果を D 部長に報告したところ，D 部長から，“利用者 ID の管理状況は分かったが，それだけでは B システムの利用が適切に行われているという保証にはならない。個人情報漏えいにつながるような不審な利用がないか，その予兆も含めて，ログを分析して確認するプロセス（以下，そのプロセスをモニタリングという）が必要である”と指摘された。

〔モニタリングの検討〕

指摘を受けた E 課長は，まず，B システムで取得しているログの種類を確認し，表 1 にまとめた。

表1　取得しているログ

ログを取得するイベント	取得する情報
ログイン成功	日付，時刻，機能番号(0001)，端末 ID，利用者 ID，成功(1)
ログイン失敗	日付，時刻，機能番号(0001)，端末 ID，ログインしようとした利用者 ID，失敗(0)
ログアウト	日付，時刻，機能番号(0099)，端末 ID，利用者 ID
ログインとログアウト以外の機能の利用成功	日付，時刻，機能番号(1000～9999)，端末 ID，利用者 ID，成功(1)
ログインとログアウト以外の機能の利用失敗 [1)]	日付，時刻，機能番号(1000～9999)，端末 ID，利用者 ID，失敗(0)

注 [1)]　利用権限のない機能もメニューに表示される。選択しても利用できず，ログが取得される。
注記 1　個人情報にアクセスする機能の機能番号は，8000 番台である。
注記 2　機能を使って読み出せる個人情報は 1 回当たり 1 人分である。
注記 3　集計機能では個人情報を読み出すことはできない。機能番号は 7000 番台である。

次に，E 課長は，B システムへのアクセスのうち，不審な利用及びその予兆とするものを表 2 にまとめた。

表2　不審な利用及びその予兆

記号	不審な利用及びその予兆
ア	他人の利用者 ID を使おうとして，推測した利用者 ID 又は推測したパスワードでログインを試みる。
イ	有権限者が，自分の利用者 ID を用いて，業務目的外で大量の個人情報にアクセスする。
ウ	普段，深夜・早朝に B システムを利用することがない有権限者が，オフィスに人がいない深夜・早朝に，業務目的外で個人情報にアクセスする。
エ	無権限者が，自分の利用者 ID を用いて，個人情報へのアクセスを試みる。

続いて，E 課長は，①営業部の F 部長にヒアリングを行い，ログから不審な利用者 ID を抽出するための条件（以下，モニタリング条件という）を検討し，表 3 にまとめた。

表3　モニタリング条件

条件名	抽出する利用者 ID	表 2 中の対応する記号
条件 1	1 週間で，ログイン失敗が 3 回以上の利用者 ID	ア
条件 2	1 週間で，8000 番台の機能の利用成功回数が 50 回を超えた利用者 ID	イ
条件 3	1 週間で，22 時～翌日 6 時に 8000 番台の機能の利用成功回数が 1 回以上の利用者 ID	ウ
条件 4	1 週間で，［ a ］の利用者 ID	エ

保存されているログを表 3 のモニタリング条件で分析したところ，どの条件に合致する利用者 ID も見つからなかった。E 課長は，F 部長へのヒアリング結果とログの分析結果を D 部長に報告した。

報告を受けた D 部長は，今後も表 3 の条件でモニタリングを行うように指示した。E 課長は，継続的にモニタリングを行うには，機械処理が必要と考え，ツールの開発を始めた。ツールの開発では，まず，モニタリング条件が，具体的かつ機械処理が可能なものになっていることを確認した。さらに，B システムのモニタリング手順を図 1 にまとめた。

手順 1. 毎週月曜日の朝 8 時に，過去 2 週間分（前週分と前々週分）のログを B システムから抽出し，モニタリング条件に合致する利用者 ID がログ中に存在するか確認する。
手順 2. モニタリング条件に合致する利用者 ID がログ中に存在した場合は，その利用者 ID を保有している従業員を調査の対象とする。②利用者 ID が B システムに登録されていない場合は，関係するログに記録されている端末 ID をもつ端末を貸与されている従業員を，調査の対象とする。
手順 3. 調査の対象になった従業員の上司に対してヒアリングを行う。個人情報漏えいにつながる可能性があると判断された場合は，更に詳細な調査を行う。

図 1　B システムのモニタリング手順

〔モニタリングの実施〕

B システムのモニタリング手順をまとめてから 2 週間後にツールが完成し，ツールによるモニタリングを開始した。D 部長は，③モニタリングの実施を社内に通達するよう指示した。ただし，④モニタリング条件はセキュリティ上の懸念から開示しないよう指示した。

モニタリングを開始してから 3 か月後に，化粧品の専門知識をもった従業員 4 名が，商品部から営業部 1 課に異動になった。4 名は，全ての顧客を対象として，顧客の購買履歴を基に，電話又は電子メールでアフターケアをする新サービスを担当することになった。4 名は，新サービスを行うために，1 人当たり毎週 200 回近く個人情報にアクセスすることになった。その結果，4 名は表 3 のモニタリング条件 2 に該当し，業務目的のアクセスであるにもかかわらず，営業部 1 課の課長が毎週ヒアリングを受けることになってしまった。そこで E 課長は，条件 2 の利用成功回数のしきい値を 50 回から 200 回に引き上げることを D 部長に提案した。

提案を受けた D 部長は，⑤条件 2 の利用成功回数のしきい値を引き上げると，適切

なモニタリングができなくなるので，再度検討するようにE課長に指示した。E課長は再検討の結果，改善案として，表3に示すモニタリング条件2を，表4に示す新たなモニタリング条件2′で置き換えることを提案した。

表4　新たなモニタリング条件2′

条件名	抽出する利用者ID	表2中の対応する記号
条件2′	[b]，かつ，8000番台の機能の利用成功回数が前の週に比べて2倍以上の利用者ID	イ

D部長は，当分はこの改良を加えたモニタリングを実施することを了承した。さらに，D部長は，“営業部の業務は今後も変化していくと考えられる。今回は，ヒアリングの実施件数が急増したことでモニタリング条件を見直すことになったが，モニタリング条件の見直しをせずにいると，モニタリングが有効に機能しなくなったり，非効率になったりすることがある”として，E課長に対し，⑥モニタリングの有効性と効率性を維持するための施策を検討するように指示した。

その後，H社ではその施策を踏まえたモニタリングを継続して実施している。

設問1　〔モニタリングの検討〕について，(1)～(3)に答えよ。

(1)　本文中の下線①を行わなかった場合に，表3を作る上でどのような情報が不足すると考えられるか。25字以内で具体的に述べよ。

(2)　表3中の [a] に入れる条件とは何か。具体例を一つ挙げ，25字以内で述べよ。

(3)　図1中の下線②について，調査の対象とする従業員を端末IDで特定しようとするのはどのイベントの場合か。表1中のイベントから選べ。

設問2　〔モニタリングの実施〕について，(1)～(4)に答えよ。

(1)　本文中の下線③について，どのような効果があると考えられるか。20字以内で述べよ。

(2)　本文中の下線④について，モニタリング条件の開示によるセキュリティ上の懸念とは何か。40字以内で述べよ。

(3)　本文中の下線⑤について，適切なモニタリングができなくなるのは，どのよ

うな従業員が，どのようなアクセスを行った場合か。本文中の字句を用いて 60 字以内で具体的に述べよ。

(4) 表 4 中の [b] に入れる条件とは何か。具体例を一つ挙げ，30 字以内で述べよ。

設問 3 本文中の下線⑥について，モニタリングの有効性と効率性を維持するための施策とは何か。50 字以内で具体的に述べよ。

問3　標的型攻撃メールへの対応に関する次の記述を読んで，設問1～3に答えよ。

Z社は，従業員数300名の家具卸売会社であり，メーカ10社から商品を仕入れ，小売店20社に販売している。Z社のインターネット接続環境は図1及び図2に示すとおりであり，その環境を使って従業員はインターネット上のWebサイトにアクセスしたり，電子メール（以下，メールという）を送受信したりしている。メールの送受信のために，インターネットドメイン名 z-sha.co.jp を取得している。z-sha.co.jp のゾーン情報は，外部業者の保有するDNSサーバに登録し，管理を委託している。

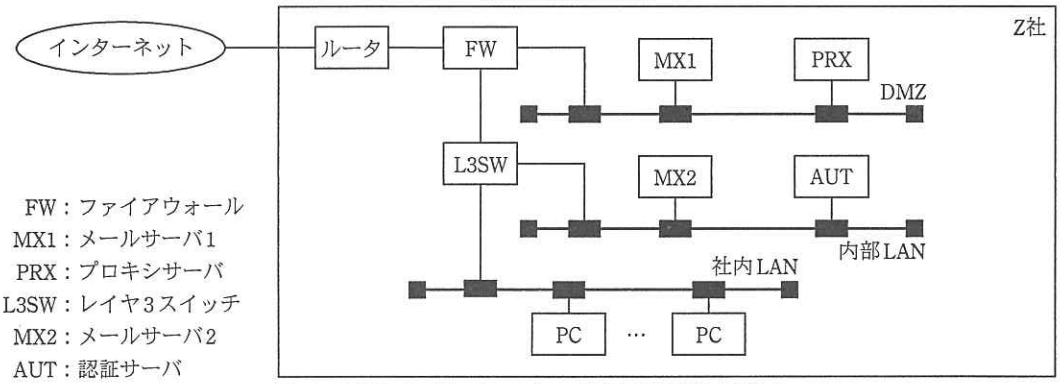


図1　Z社のインターネット接続環境の構成

・PC
　PCからのインターネット利用は，ブラウザによるWebアクセスと，メールクライアントによるメール送受信に限定する。
・AUT
　従業員のアカウント管理用ディレクトリを保有する。DNSサーバとして，社内で利用するイントラネットドメインのゾーン管理を行い，社内のPCに対して，社内サーバのFQDNの名前解決を提供する。
・PRX
　PCからインターネットへのWebアクセスを中継する。Webサイトから PCにダウンロードされるファイルのうち，暗号化されていないものに対してウイルススキャンを行う。
・MX2
　社内向けメールサービスを提供する。従業員は，メールクライアントからメールの送受信を行う。MX2は各従業員のメールボックスを管理する。
・MX1
　社外のメールサーバと MX2 間のメール転送を行う。暗号化された添付ファイルを除くメールのウイルススキャン，及びウイルスを検知したメールの隔離を行う。
・FW
　社内とインターネットとの間の通信制限を行う。具体的には，社内とインターネットとの間の通信は次の3種類だけを許可する。
　・PCからPRX経由のインターネット上のWebサイトへのアクセス
　・MX1とインターネットとの間のメール転送
　・PRX及びMX1からインターネットへのDNS通信
　社内とインターネットとの間の通信には，グローバルIPアドレス z.y.x.1 をNATアドレスとして使用する。

注記　上記のサーバ及びPCにはウイルス対策ソフトが導入されている。

図2　Z社のインターネット接続環境の概略

〔不審なメールへの対応〕

Z 社では，セキュリティ強化のために，従業員教育に力を入れており，次の点について繰返し研修を行っている。

・不審な添付ファイルは開かないなどのメールの閲覧に関する注意事項
・不審なメールが届いた場合の，社内のセキュリティデスクへの通報手段
・PC 環境の適切なアップデート方法

ある日，営業部の A 君からセキュリティデスクに対して，次のような通報があった。

“メーカ Y 社の B 氏のメールアドレス（b-shi@y-sha.co.jp）からメールが届いたが，直前まで Y 社内で B 氏と打合せをしており，疑問を抱いた。そのメールは，記載されている社名，部署名，氏名及びメールアドレスが全て正しかったが，念のため B 氏に確認したところ，やはり送信していないとのことだったので，不審なメールであると判断した。”

なお，Y 社は，メールサーバを含む情報システムを国内で運用している。

メールには文書ファイルが添付されていたが，A 君は，日頃の研修を思い出し，添付ファイルを開かずに，セキュリティデスクに通報していた。さらに，この添付ファイルを開くためのパスワードだと記入されたメールを直後に受信したので，それもセキュリティデスクに報告した。1 通目の不審なメールのヘッダを図 3 に示す。

```
Return-Path: <b-shi@y-sha.co.jp>
Delivered-To: a-kun@z-sha.co.jp
Received: from mx1.z-sha.co.jp (mx1.z-sha.co.jp [□□.△△.○○.▽▽])
          by mx2.z-sha.co.jp (smtp) with ESMTP id ■■
          for <a-kun@z-sha.co.jp>; Fri, 27 Jan 2012 17:38:12 +0900 (JST)
Received: from smtp.y-sha.co.jp  (unknown [80.◎◎.◇◇.☆☆])
          by mx1.z-sha.co.jp (smtp) with ESMTP id ▲▲
          for <a-kun@z-sha.co.jp>; Fri, 27 Jan 2012 17:38:10 +0900 (JST)
Received: from mail.y-sha.co.jp (localhost [127.0.0.1])
          by smtp.y-sha.co.jp (smtp) with SMTP id ●●
          for <a-kun@z-sha.co.jp>; Fri, 27 Jan 2012 9:37:58 +0100 (CET)
Date: Fri, 27 Jan 2012 9:37:58 +0100
Message-ID: <▼▼>
From: b-shi@y-sha.co.jp
To: a-kun@z-sha.co.jp
Subject: ◆◆
```

注記 1　Y 社のインターネットドメイン名は y-sha.co.jp である。

注記 2　図中の□□，△△，○○，▽▽，◎◎，◇◇，☆☆は，特定の数字を表し，■■，▲▲，●●，▼▼，◆◆は，特定の英数字と記号を含む ASCII 文字列を表す。

図 3　1 通目の不審なメールのヘッダ

セキュリティデスクで図 3 のヘッダを調べ，不審な点として，［ a ］と［ b ］から，偽メールと判断した。ただし，ヘッダは，途中で書き換えられた可能性を否定できないことと，［ b ］については，経由するサーバの設定が必ずしも正しいとは限らないことの 2 点から，悪意のある攻撃メールの疑いはあったが，そうだとは断定できなかった。

セキュリティデスクは，支援契約を結んでいるセキュリティ専門会社に，添付ファイルとパスワードを提示し，調査を依頼した。後日，添付ファイルは，マクロ機能を使ったスパイウェアであることが判明した。

〔メールアドレスの偽装と対策〕

しばらくたったある日，今度は Y 社情報システム部から A 君に対して，“あなたが差出人の不審なメールが届いた。そのメールを添付したので，確認してほしい”という問合せメールが届いた。添付されていたメールは，A 君が開いて確認すると，確かに A 君が差出人になっていたが，心当たりのないものだった。そのメールには添付ファイルはなかったが，本文に社外サイトへのリンクが記入されていた。A 君がリンクをたどったところ，やはり心当たりのない社外サイトであった。A 君はこの事態をセキュリティデスクに通報した。

セキュリティデスクで調査した結果，何者かが A 君を装った偽メールを Y 社に送信し，不審サイトに誘導しようとしたと判断した。Y 社に調査結果を連絡するとともに，セキュリティ専門会社などにも連絡した。

Z 社では，相次ぐ偽メールに危機感が高まり，情報システム部が中心になって，メールアドレスの偽装について対策を強化することになった。情報システム部の P 部長は，まず，送信ドメイン認証技術についての検討を S 主任に指示した。

S 主任は検討した結果を P 部長に報告した。次は，そのときの P 部長と S 主任の会話である。

P 部長 ：メールアドレスの偽装はどのように阻止すればよいのだろうか。

S 主任 ：当社のメールアドレスを偽装したメールの発信を，技術的対策で阻止することは難しいと思います。しかし，送信ドメイン認証技術を使えば，当社から

正規に送信されたメールかどうかを，受信側で検証できます。ただし，当社が採用した送信ドメイン認証技術に，受信側のメールサーバが対応している必要があります。送信ドメイン認証技術の候補としては，普及率を考慮して，SPF（Sender Policy Framework）がよいと思います。Y 社をはじめとする主要取引先と，導入について協議してみてはどうでしょうか。

P 部長：なるほど。SPF の導入に際して，どんな作業が必要になるのかね。

S 主任：z-sha.co.jp のゾーン情報を管理している DNS サーバに，図 4 に示す TXT レコードを登録します。当社のメールサーバの設定変更は不要です。

P 部長：偽装したメールかどうかはどのように判定するのかね。

S 主任：受信側のメールサーバが，［ c ］中の SMTP の［ d ］コマンドの引数で指定されたアイデンティティのうちドメイン名の部分を基に，DNS サーバに問合せを行い，SMTP 接続元の IP アドレスと比較します。

P 部長：分かった。メールを頻繁に送受信する取引先と協議を始めることにしよう。

```
z-sha.co.jp. IN TXT "v=spf1 +ip4:[ e ] -all"
```

図 4　登録する TXT レコード

〔標的型攻撃への対策〕

P 部長と S 主任は，送信ドメイン認証技術の導入を進める一方，標的型攻撃への対策についても検討を行った。

P 部長：今回の A 君の対応はどうだったかな。

S 主任：A 君は研修を熱心に受け，この前の不審なメールへの対応は万全でした。しかし，今回の Y 社情報システム部からの問合せメールについては，①A 君の対応は不適切でした。今回は幸運でしたが，被害が出る可能性がありました。Y 社からの問合せなので油断したのかもしれません。

P 部長：標的型攻撃の恐ろしいところだな。しかも，攻撃が巧妙化していけば，阻止しようとする対策だけでは限界がある。もし攻撃が成功したとしても被害を最小限にとどめるための対策も必要になる。

S主任 ：典型的な標的型攻撃では，(A)ウイルスが，様々な方法で社内に侵入し，(B)社内で感染を拡大させ，(C)感染したPC及びサーバのアクセス権を入手して情報収集を行います。このとき，ウイルスの活動によって異常なトラフィックが発生したり，PC又はサーバが異常な振る舞いをしたりすることもあります。その後，(D)収集した情報をネットワーク経由で攻撃者に報告します。

P部長 ：そうだな。このような被害の拡大をどこかで断ち切れるように対策を強化していこう。

S主任：はい。(A)については，MX1及びPRXにウイルス対策ソフトを導入しており，(B)についてはPC及びサーバにウイルス対策ソフトを導入しています。(C)については②PC又はサーバの監視強化を検討します。(D)は，バックドア通信と呼ばれるものですが，対策は簡単ではありません。

P部長 ：つまりどういうことかね。

S主任 ：バックドア通信については，③当社のネットワーク設定で既に遮断できる通信もあります。しかし，例えば，ウイルスがWebアクセスの通信パターンを模倣して行う通信については，現在のところ防げません。これに関しては，④更なる対策を検討していきます。

P部長 ：そうか。引き続き，バックドア通信について対策を検討してくれ。

Z社では，こうした議論を踏まえ標的型攻撃への対策の強化を進めた。

設問1　〔不審なメールへの対応〕について，本文中の［　a　］，［　b　］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　Y 社が国内で運用しているはずのメールサーバのタイムゾーンが，日本ではなく，海外になっている点

イ　Y 社と Z 社間で中継サーバを経由した記録がなく，中間経路を隠蔽する改ざんが行われている点

ウ　Y 社のメールサーバのアドレスが，Y 社のアドレスではなく，かつ，DNS 参照が“unknown”になっている点

エ　Z 社のメールサーバのローカルアドレスではなく，Z 社のグローバルアドレスが参照されており，NAT 変換が無視されている点

設問2　〔メールアドレスの偽装と対策〕について，(1)，(2)に答えよ。

(1)　本文中の［　c　］，［　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　EXPN	イ　MAIL FROM	ウ　RCPT TO
エ　VRFY	オ　メールエンベロープ	カ　メールボディ

(2)　図 4 中の［　e　］に入れる適切な字句を図 1～3 中から選び答えよ。

設問3　〔標的型攻撃への対策〕について，(1)～(4) に答えよ。

(1)　本文中の下線①について，A 君の対応のうち，添付されていたメールを不用意に開いた点以外の不適切だった点を 20 字以内で述べよ。

(2)　本文中の下線②に示した PC 又はサーバの監視強化には幾つかの方法が考えられる。監視強化のためのシステムを導入する場合，導入するシステムの名称及び設置場所を 10 字以内で答えよ。また，そのシステムで監視すべき事象を 15 字以内で答えよ。

(3)　本文中の下線③で示したネットワーク設定を，図 1 中の機器名を二つ以上用いて，40 字以内で具体的に述べよ。

(4)　本文中の下線④で示した更なる対策として考えられる具体的な手段を，40 字以内で述べよ。

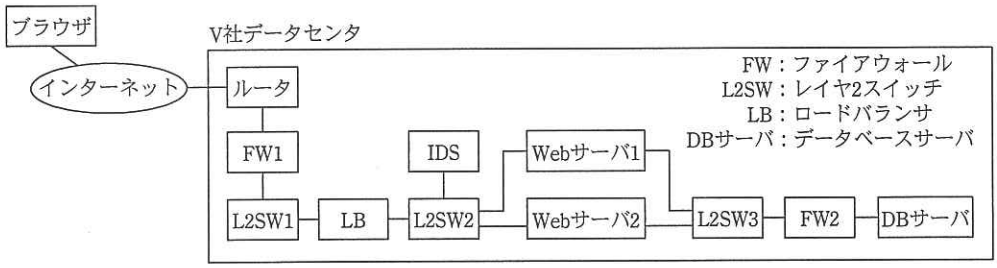
問4　情報セキュリティインシデント対応に関する次の記述を読んで，設問1～3に答えよ。

W社は，地方都市を拠点とする人材派遣会社で，従業員数は60名である。W社では，インターネット上のWebサイト（以下，人材情報サイトという）で，派遣社員登録希望者に対して，W社への登録，求人情報の閲覧などができるサービスを，3年前から提供している。

派遣社員登録希望者は，まず，人材情報サイトから個人プロフィールをW社に送信する。次に，面接を受けて合格すれば，W社に正式登録され，非公開求人情報の閲覧，W社の担当者への相談が可能になる。

〔人材情報サイトの概要〕

人材情報サイトは，V社のデータセンタに設置されている。人材情報サイトのネットワーク構成を図1に，人材情報サイトの機器のFQDN及びIPアドレスを表1に，人材情報サイトの概略を図2に示す。



注記　図中の管理用セグメントは省略

図1　人材情報サイトのネットワーク構成

表1　人材情報サイトの機器のFQDN及びIPアドレス（抜粋）

機器名称	FQDN	IPアドレス	説明
FW1	－	□□.2.2.1	FW1のインターネット側IPアドレス
	www.w-sha.co.jp	□□.2.2.2	Webサーバの仮想IPアドレス
	－	192.168.0.1	FW1のLB側IPアドレス
LB	－	192.168.0.3	LBのインターネット側IPアドレス
	－	192.168.0.10	Webサーバの仮想IPアドレス
	－	192.168.1.254	LBのWebサーバ側IPアドレス
Webサーバ1	－	192.168.1.11	Webサーバ1のインターネット側IPアドレス
Webサーバ2	－	192.168.1.12	Webサーバ2のインターネット側IPアドレス

注記　表中の□□は，特定の数字を表す。

(1) 利用者は，ブラウザからインターネットを経由して人材情報サイトを利用する。ブラウザからのアクセスは，LB によって 2 台の Web サーバ（2 台を合わせて Web サーバ群という）に負荷分散される。

(2) Web サーバ上では，次の四つが稼働している。

・OS

・HTTP による送受信を処理する Web サーバプログラム

・Web アプリケーションを動作させるためのミドルウェア

・Web アプリケーション

Web アプリケーションは，ミドルウェア経由で DB サーバにアクセスする。ブラウザからのアクセスについて，Web サーバプログラムが処理する最大同時セッション数は，Web サーバプログラムで 50 に制限している。LB では，任意の HTTP ヘッダフィールドを追加可能であるが，現在は何も追加していない。追加した HTTP ヘッダフィールドは，全て Web サーバのアクセスログに出力可能である。

(3) Web アプリケーションの開発は，W 社の情報システム部で行っている。

(4) 機器のハードウェア保守は，V 社に業務委託している。OS を含むソフトウェアのバージョン管理及びバージョンアップは，W 社の情報システム部で行っている。全ての機器の時刻は，V 社の NTP サーバを利用して同期させている。

(5) FW は，パケットフィルタリング型である。

(6) IDS は，L2SW2 のミラーポートを監視対象とし，トラフィックに対してシグネチャとのパターンマッチングを行い，攻撃を検知する。アラートレベルは，High，Medium 及び Low に分けられており，High の場合だけアラートが IDS から管理用セグメントを経由して W 社情報システム部の運用チーム（以下，運用チームという）に電子メールで通知される。シグネチャは，製品の標準設定で自動更新されるようになっている。

(7) LB は，SSL アクセラレータ機能と負荷分散機能を提供しており，Web サーバの仮想 IP アドレスをもち，2 台の Web サーバにアクセスを負荷分散する。また，Web サーバ群の死活監視機能をもち，負荷分散対象である Web サーバの TCP8443 番ポートに，1 分間に一度アクセスしてサービスの稼働チェックを行う。アクセスしてから 30 秒以内に死活監視用コンテンツを取得できない場合は，サービスダウンとみなして警告（以下，サービスダウンとみなした警告をイベント通知という）を発し，運用チームに電子メールで通知する。サービスダウンの Web サーバにはリクエストを送らない。また，HTTP ヘッダフィールドとして X-Forwarded-For ヘッダフィールドを追加可能であるが，現在は利用していない。

図 2　人材情報サイトの概略

〔インシデントの発生〕

ある月曜日の朝，LB のイベント通知が発生した。運用チームの G 主任が，原因を調査することになった。G 主任が，運用チームの Web サーバ管理担当者 H さんに確認したところ，Web サーバプログラムで制限している最大同時セッション数が不足してイベント通知が発生したとの報告を受けた。人材情報サイトは，リリース後にアクセス数が増加しているので，最大同時セッション数の設定の見直しを運用チーム内で検討していた。特に月曜日は，求人情報の定期更新があり，16 時まではアクセスが集中する。そこで，たとえイベント通知が発生しても，次のサービス稼働チェックで復旧した場合は無視することにした。ところが，16 時を過ぎてもイベント通知が発生した

ので，G 主任は改めてイベント通知の原因の調査を開始した。

G 主任は，①各機器の当日のログを調査した結果，人材情報サイトが攻撃を受けていた可能性が高いと判断した。LB のサービス稼働チェックログを表 2 に，IDS がシグネチャ A に該当するとして検知した事象のログを表 3 に，表 3 の各事象に関する FW1 のログを表 4 に，同じく表 3 の各事象に関する Web サーバ 1，2 のアクセスログを表 5，表 6 に，Web サーバ群のリソースグラフを図 3 に示す。

なお，各ログは，調査で確認した当日の各機器の大量のログから抜粋したものである。

表 2　LB のサービス稼働チェックログ（抜粋）

検知時刻	監視対象 IP アドレス	ステータス
10:05:00	192.168.1.11	down
10:06:00	192.168.1.11	up
11:01:00	192.168.1.11	down
11:02:00	192.168.1.11	up
12:15:00	192.168.1.12	down
12:16:00	192.168.1.12	up
13:02:00	192.168.1.12	down
13:03:00	192.168.1.12	up
14:00:00	192.168.1.12	down
14:01:00	192.168.1.12	up
15:05:00	192.168.1.11	down
15:06:00	192.168.1.11	up
18:51:00	192.168.1.12	down
18:52:00	192.168.1.12	up
19:23:00	192.168.1.11	down
19:24:00	192.168.1.11	up

注記 1　ステータスが down のもの及びその 1 分後のものの抜粋
注記 2　表中の検知時刻は，稼働チェック用のリクエストを送信した時刻を表す。

表 3　IDS の検知ログ（シグネチャ A 検知に関連するログの抜粋）

項番	検知時刻	アラートレベル	送信元 IP アドレス	宛先 IP アドレス	送信元ポート番号	宛先ポート番号
(1)	11:00:12	Low	192.168.1.254	192.168.1.11	19212	8443
(2)	13:21:06	Low	192.168.1.254	192.168.1.12	14506	8443
(3)	15:04:54	Low	192.168.1.254	192.168.1.11	39871	8443
(4)	16:59:23	Low	192.168.1.254	192.168.1.11	40192	8443
(5)	18:50:20	Low	192.168.1.254	192.168.1.12	10211	8443
(6)	19:22:43	Low	192.168.1.254	192.168.1.11	50983	8443

表4　FW1 のログ（シグネチャ A 検知に関連するログの抜粋）

項番	処理時刻	処理	プロトコル	送信元 IP アドレス	宛先ポート番号	送信バイト数
(1)	11:00:12	許可	TCP	△△.123.123.123	443	6,401,200
(2)	13:21:06	許可	TCP	○○.1.1.1	443	301,201
(3)	15:04:54	許可	TCP	△△.123.123.123	443	6,401,121
(4)	16:59:23	許可	TCP	○○.1.1.2	443	305,121
(5)	18:50:20	許可	TCP	△△.123.123.123	443	6,401,220
(6)	19:22:43	許可	TCP	△△.123.123.123	443	6,401,198

注記　表中の△△，○○は，特定の数字を表す。

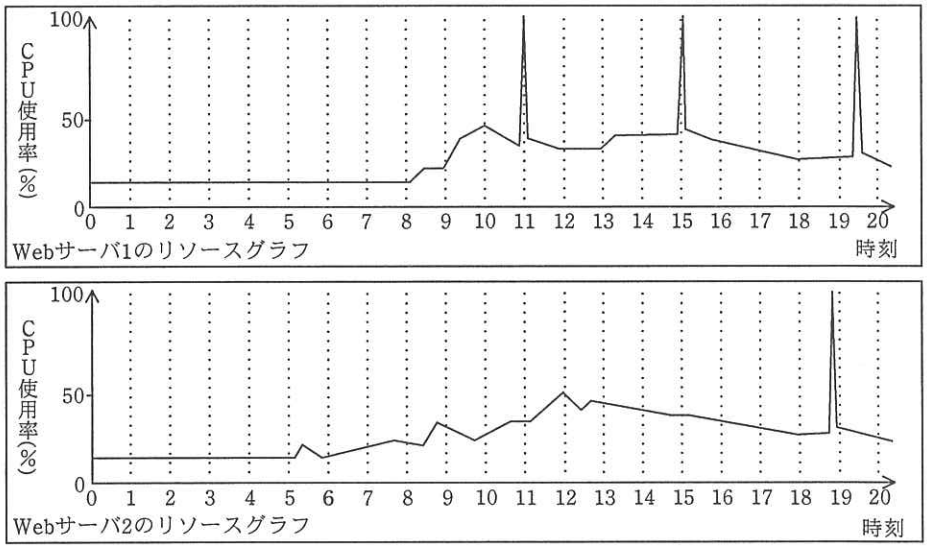


図3　Web サーバ群のリソースグラフ

表5　Web サーバ 1 のアクセスログ（シグネチャ A 検知に関連するログの抜粋）

項番	送信元 IP アドレス	アクセス時刻	リクエスト内容	ステータスコード	受信バイト数
(1)	192.168.1.254	11:00:12	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,124
(2)	192.168.1.254	15:04:54	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,011
(3)	192.168.1.254	16:59:23	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	200	305,071
(4)	192.168.1.254	19:22:43	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,162

表6　Webサーバ2のアクセスログ（シグネチャA検知に関連するログの抜粋）

項番	送信元IPアドレス	アクセス時刻	リクエスト内容	ステータスコード	受信バイト数
(1)	192.168.1.254	13:21:06	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	200	301,143
(2)	192.168.1.254	18:50:20	POST www.w-sha.co.jp/entry/touroku.php HTTP/1.1	500	6,401,181

〔暫定対策の実施〕

IDSが通知したアラートと，その際にIDSが内部に保存したパケットデータをIDS販売元のセキュリティベンダX社に提供して問い合わせた結果，数日前に情報が公開されたばかりの脆弱性を狙った攻撃であることが判明した。その脆弱性は，特定のデータを受信するとWebサーバのCPUリソースが一時的に枯渇するというものであった。X社からは，ミドルウェアをバージョンアップすることによって，脆弱性を除去できるという回答があった。しかし，Hさんが帰宅してしまっていたので，すぐにはバージョンアップができなかった。そこで，攻撃元だと特定したIPアドレス［　a　］からの通信をFW1で遮断することにした。

また，IDSでは，シグネチャAの検知基準が，標準設定の“HTTP POSTリクエストが300,000バイト以上”だった。したがって，②誤検知が発生する可能性が高く，それを考慮して，アラートレベルはLowにしていた。しかし，アラートレベルがLowではメール通知がされないので，Highに変更すべきかX社に相談したところ，もしアラートレベルをHighにするのであれば，誤検知を減らすために検知基準を変更した方がよいという助言を受けた。そこで，今回の脆弱性を狙った攻撃を検知可能で，かつ，誤検知が減るように検知基準を変更した上で，アラートレベルをHighに変更した。

〔恒久対策の検討と運用強化〕

その後W社では，シグネチャAのアラートは通知されなかった。Hさんはミドルウェアのバージョンアップの影響を調査した後，バージョンアップを実施し，今回の脆弱性への対策を完了した。さらに，セキュリティ運用について情報システム部内で課題を洗い出し，次のような対策案を作成した。

(A) 脆弱性情報の把握と対策の早期実施

IPA及びJPCERT/CCから公開される脆弱性情報を確認し，人材情報サイトに影響を及ぼす脆弱性があれば，速やかに対策を講じる。また，その脆弱性を狙った攻撃

を IDS が検知できる場合は，その脆弱性を検知するシグネチャのアラートレベルを，人材情報サイトへの影響度に見合ったレベルに設定する。

(B) Web サーバのサービス稼働チェックの最適化

Web サーバのサービス稼働チェックでは，対処する必要がない場合でもイベント通知している。対処が必要な場合にだけイベント通知するように，③Web サーバの設定を変更の上，イベント通知すべき条件を変更する。

(C) 相関分析を目的としたログ調査環境・手順の整備

今回は同時に大量のアクセスが発生したので，大量のログから攻撃元を特定するまでに時間が掛かった。今後は，④攻撃元を特定しやすくするために，FW1 と Web サーバ群のログを関連付けられるようにログの出力内容と分析手順を見直す。また，IDS については，L2SW2 のトラフィックの代わりに L2SW1 のトラフィックを監視対象にすることによって，ネットワークアドレス変換前の［ b ］を確認できるので，攻撃元の特定が容易になる。ただし，LB への［ c ］通信については監視できないので，IDS は LB が保有している［ d ］を利用して［ c ］通信についても監視できるものにする。

これらの対策案を基に，W 社ではセキュリティ運用を強化することにした。

設問 1　本文中の下線①について，G 主任は，表 2 によって事象の発生時間帯をある程度絞り込んだ後，更に絞り込むため図 3 に着目した。G 主任が，図 3 に着目した理由は何か。50 字以内で述べよ。

設問 2　〔暫定対策の実施〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］に入れる IP アドレスを，表 4 の中から選んで答えよ。

(2) 本文中の下線②について，表 3 の IDS の検知ログには幾つかの誤検知が含まれている。それらが誤検知であるということは，表 5，表 6 のどのアクセスログから判断できるか。表 5，表 6 から全て選び，例えば，表 5 の項番(1)の場合は，“表 5(1)”のように，表番号と項番の組合せで答えよ。

(3) 上記(2)で誤検知であると判断した理由を，35 字以内で述べよ。

設問3　〔恒久対策の検討と運用強化〕について，(1)～(3)に答えよ。

(1) 本文中の［ b ］～［ d ］に入れる適切な字句を，［ b ］は10字以内，［ c ］，［ d ］はそれぞれ5字以内で答えよ。

(2) 本文中の下線③について，Web サーバの設定変更を実施することによって改善される，不要なイベント通知の原因になっていた Web サーバ内の事象を，35字以内で述べよ。

(3) 本文中の下線④について，FW1 と Web サーバ群のログを関連付けられるようにするために設定変更が必要な機器はどれか。解答群の中から二つ選び，記号で答えよ。また，それぞれの設定内容を40字以内で述べよ。

解答群

ア　ルータ　　イ　FW1　　ウ　LB　　エ　IDS

オ　Web サーバ群

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

〔 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。
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（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。