SC

平成27年度　春期
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〕

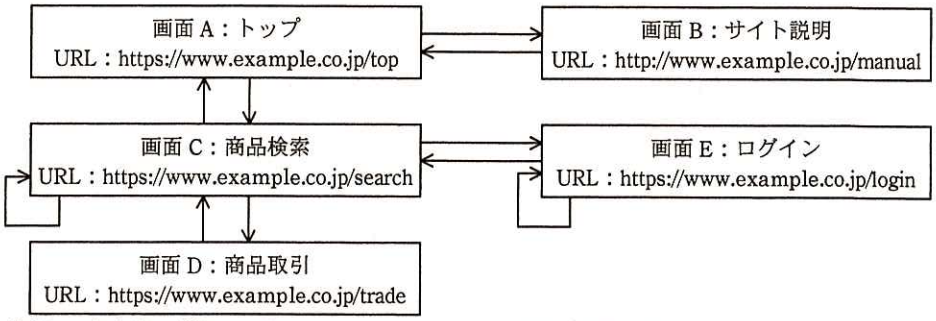
選択欄	
2問選択	○問1
	問2
	○問3

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。

問1　Webサイトの脆弱性と対策に関する次の記述を読んで，設問1～3に答えよ。

S社は，情報システムの構築，運用，コンサルティングなどのサービスを顧客に提供する従業員数5,000名の企業である。S社にはセキュリティプロフェッショナルグループ（以下，SPGという）という組織があり，Webアプリケーションソフトウェア（以下，Webアプリという）の脆弱性を検査するサービス（以下，脆弱性検査という）を提供している。

SPGでは，脆弱性検査に従事できる者を認定するために，技能試験を実施している。技能試験は，Webアプリに脆弱性が作り込まれた，技能試験用のWebサイト（以下，試験用サイトという）を用いて実施される。試験用サイトは，個人間で取引するオークションシステムを想定しており，“http://...”及び“https://...”の画面がある。図1に試験用サイトの画面構成と画面の遷移を，図2に画面Cの概要をそれぞれ示す。また，試験用サイトの機能のうち，セッション管理機能の仕組みを図3に，検索文字列の引継機能の仕組みを図4に示す。



注記1　矢印は，ボタン又はリンクのクリックによる画面の遷移を表す。
注記2　技能試験に関係しない画面は，省略している。

図1　試験用サイトの画面構成と画面の遷移

- 最上部に，画面Eへのリンク，検索フィールド及び検索ボタンがある。
- 検索フィールドに検索文字列を入力した後，検索ボタンをクリックすると，画面Cを再表示し，検索フィールドには入力された検索文字列が，画面の下部には検索された商品一覧が表示される。
- 画面Eへのリンクは，未ログインの状態では“ログイン”と表示されており，クリックすると画面Eに遷移する。画面Eでログインに成功すると遷移前の画面Cが再表示されるが，“ログイン”の表示が“ログイン中”という表示に変わり，クリックはできなくなる。
- ログイン中であって画面下部に商品一覧が表示された状態では，商品一覧中のいずれかの商品をクリックすることによって，画面Dに遷移して商品取引に進むことができる。

図2　画面Cの概要

・Web ブラウザ起動後，試験用サイトの画面の中で最初にアクセスできるのは，画面 A，B だけであり，画面 C～E の URL を指定してアクセスしても，あらかじめ画面 A にアクセスしていないと，画面 A にリダイレクトされる。
・画面 A にアクセスがあると，セッション ID を格納する Cookie（名前を SESSIONID とする）の有無を調べ，ない場合には，試験用サイトが動作するサーバで，セッション ID の値をキーとしたログイン状態を保持するセッションオブジェクトを新規に生成する。その後，サーバは，名前を SESSIONID とする Set-Cookie ヘッダを Web ブラウザに返信する。以後，同一のセッション ID によるアクセスには，同一のセッションオブジェクトが利用され，サーバでセッションが管理される。
・画面 B へのアクセスによってセッション ID が更新されることはない。

図３　セッション管理機能の仕組み

・画面 C において，利用者が検索フィールドに文字列を入力した後，又は検索フィールド中の文字列を書き換えた後，検索ボタンをクリックすることによって，検索フィールドの文字列が，クエリ文字列のパラメタとして URL エンコードされた状態でサーバに送信され，サーバで商品検索が実行される。
・商品検索が実行されると，サーバは応答時に，名前が KENSAKU であり，値を検索文字列とする Set-Cookie ヘッダを返す。
・Web ブラウザは，名前が KENSAKU である Set-Cookie ヘッダを受け取ると，当該 Cookie を更新するとともに，以後のリクエストヘッダに含めて毎回当該 Cookie を送信する。
・他の画面から画面 C に戻ったときに，既に商品検索が実行されていた場合には，リクエストヘッダ中の当該 Cookie の値に基づいて，商品検索の最新の実行結果及び検索フィールドが表示される。

図４　検索文字列の引継機能の仕組み

〔技能試験〕

SPG に新たに配属された従業員は研修検査員と呼ばれ，2 か月間の研修を終えると，技能試験を受ける。技能試験に合格した者だけが脆弱性検査を実施できる規則になっている。技能試験では，脆弱性検査専用の Web ブラウザを使用する。検査専用の Web ブラウザには，一般的な Web ブラウザの機能に加えて，送信する HTTP リクエストやパラメタの値を意図的に変更する機能がある。

技能試験では，試験官とのディスカッション，検査手順や報告書の作成を通して，力量が判断され，合否が決定される。このたび，研修検査員の T 君が，技能試験を受けることになった。試験官は U 主任である。最初に，U 主任は，技能試験の前提として図１及び図２の内容を T 君に伝えた。

なお，図３及び図４の内容は T 君には伏せられている。

〔検査シナリオと HTTP ヘッダ〕

技能試験の開始に当たって，U 主任は，図５に示す検査シナリオの順番で画面にアクセスするよう T 君に指示した。T 君が検査シナリオを実行した際の HTTP リクエ

ストヘッダ及びHTTP レスポンスヘッダを，図6に示す。

検査専用の Web ブラウザを起動→画面 A→画面 B→画面 A→画面 C→画面 C→画面 E→画面 C→画面 D

図5　検査シナリオ

リクエストX

```
01 GET /top HTTP/1.1
02 Accept: text/html,
   application/xhtml+xml, */*
03 Accept-Language: ja-JP
04 Accept-Encoding: gzip, deflate
05 Host: www.example.co.jp
06 Connection: Keep-Alive
```

→

レスポンスX

```
07 HTTP/1.1 200 OK
08 Date: Tue, 10 Jun 2014 05:30:31 GMT
09 Set-Cookie: SESSIONID=134D96E470da240421svr5B019;
   Expires= Wed, 11-Jun-2014 05:30:31 GMT;
   domain=example.co.jp;
10 Expires: Thu, 19 Nov 1981 08:52:00 GMT
11 Cache-Control: no-store, no-cache
```

リクエストY

```
12 GET /manual HTTP/1.1
13 Accept: text/html, application/xhtml+xml, */*
14 Accept-Language: ja-JP
15 Accept-Encoding: gzip, deflate
16 Host: www.example.co.jp
17 Cookie: SESSIONID=134D96E470da240421svr5B019
```

→

レスポンスY

```
18 HTTP/1.1 200 OK
19 Date: Tue, 10 Jun 2014 05:32:16 GMT
20 Expires: Thu, 19 Nov 1981 08:52:00 GMT
21 Cache-Control: no-store, no-cache
```

リクエストZ

```
22 GET /trade?itemid=10 HTTP/1.1
23 Accept: text/html, application/xhtml+xml, */*
24 Accept-Language: ja-JP
25 Accept-Encoding: gzip, deflate
26 Host: www.example.co.jp
27 Cookie: SESSIONID=134D96E470da240421svr5B019
28 Cookie: KENSAKU=jewelry
```

→

レスポンスZ

```
29 HTTP/1.1 200 OK
30 Date: Tue, 10 Jun 2014 05:45:58 GMT
31 Expires: Thu, 19 Nov 1981 08:52:00 GMT
32 Cache-Control: no-store, no-cache
```

注記1　リクエストXとレスポンスXは，最初に画面Aを表示した際のHTTP ヘッダである。
注記2　リクエストYとレスポンスYは，画面Aから画面Bに遷移した際のHTTP ヘッダである。
注記3　リクエストZとレスポンスZは，画面Cから画面Dに遷移した際のHTTP ヘッダである。
注記4　リクエスト及びレスポンス中の行番号は，本図中における通し番号である。

図6　検査シナリオを実行した際のHTTP ヘッダ（抜粋）

〔脆弱性に関するディスカッション〕

次は，図6に関するU主任とT君のディスカッションである。

U 主任：図 6 中のレスポンス X について，セキュリティ上，気になる点があれば指摘してください。

T 君　：Set-Cookie ヘッダに，①secure 属性が設定されていません。secure 属性を設定しないと，セッション ID を第三者に盗聴されるリスクがあり，セッションハイジャックなどにつながると思います。

U 主任：他に，図 6 全体を通して，気になる点はありますか。

T 君　：HTTP ヘッダインジェクションの脆弱性が存在する可能性があります。図 7 の検査コードをリクエストのクエリ文字列のパラメタの値にセットし，スクリプトの実行ができるかどうか，確認してみます。

```
a  %3chtml%3e%3cbody%3e%3cscript%3ealert%28%221%22%29%3c%2fscript%3e%3c%2fbody%3e%3c
%2fhtml%3e
```

注記 1　図中の文字列は URL エンコード済みの形式である。
注記 2　ASCII 文字コード一覧を図 8 に示す。

図 7　クエリ文字列のパラメタの値にセットする検査コード

文字	文字コード
NUL	00
SOH	01
STX	02
ETX	03
EOT	04
ENQ	05
ACK	06
BEL	07
BS	08
HT	09
LF	0a
VT	0b
FF	0c
CR	0d
SO	0e
SI	0f

文字	文字コード
DLE	10
DC1	11
DC2	12
DC3	13
DC4	14
NAK	15
SYN	16
ETB	17
CAN	18
EM	19
SUB	1a
ESC	1b
IS4	1c
IS3	1d
IS2	1e
IS1	1f

文字	文字コード
SP	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2a
+	2b
,	2c
-	2d
.	2e
/	2f

文字	文字コード
0	30
1	31
2	32
3	33
4	34
5	35
6	36
7	37
8	38
9	39
:	3a
;	3b
<	3c
=	3d
>	3e
?	3f

注記　文字コード 00～1f は制御文字である。文字コード 20 は空白文字である。

図 8　ASCII 文字コード一覧（抜粋）

T 君が，図 7 の検査コードを用いて確認したところ，予想どおり，警告ダイアログが表示された。T 君は，HTTP ヘッダインジェクションの脆弱性が存在することを指摘した。

T 君　：サーバ側での HTTP レスポンスヘッダの出力処理に問題があり，HTTP ヘッダインジェクションの脆弱性が存在すると思います。具体的には，入力された検索文字列を適切に処理せずに Set-Cookie ヘッダの値にセットしているものと思われます。この脆弱性を突いた攻撃では，［ b ］攻撃と同様に，攻撃者が指定した任意のスクリプトをクライアント側で実行できます。

U 主任：仮に問題があるとした場合，Set-Cookie ヘッダの値をセットするサーバ側の処理において，どのような対策が考えられますか。

T 君　：幾つかの対策があります。例えば，HTTP レスポンスヘッダを適切に出力するために，Web アプリの実行環境やプログラム言語が用意している，ヘッダ出力用の関数や API を使用する方法が考えられます。それが使用できない場合は，［ c ］するといった処理を開発者が自身で実装する方法も考えられます。

U 主任：その他に気になる点はありますか。

T 君　：はい。図 6 の一連の HTTP ヘッダのうち，例えば，行番号［ d ］と行番号［ e ］を見比べると，サーバ側のセッション管理に問題があり，セッションフィクセーションの脆弱性が存在する可能性があります。攻撃者が Cookie Monster Bug を突く攻撃や，前述した HTTP ヘッダインジェクション攻撃を組み合わせることによって，セッションフィクセーションを成功させる可能性があります。図 9 に攻撃手順の一例を示します。

1. 攻撃者 J が，試験用サイトの画面 A にアクセスし，セッション ID を取得する。このときの，セッション ID を“01234”とする。
2. 攻撃者 J が，攻撃対象の利用者 K に HTML メールを送信する。この HTML メールには URL リンクがあり，攻撃用のクエリ文字列を含む画面 C の URL が記載されている。
3. 利用者 K が，試験用サイトの画面 A にアクセスし，セッション ID を取得する。このときの，セッション ID を“56789”とする。その後，HTML メールの URL リンクをクリックする。その際に送信される HTTP リクエストには，攻撃者 J が用意した攻撃用クエリ文字列が含まれており，検索文字列の値は次のとおりである。

   `%0d%0aSet%2dCookie%3a%20SESSIONID%3d` ［ f ］ `%3b%20Expires%3d（省略）domain%3dexam ple%2eco%2ejp%3b（省略）`
4. 利用者 K がログインする。
5. 攻撃者 J は，利用者 K になりすまし，本来はアクセス権限がない画面にアクセスできるようになる。

図 9　攻撃手順の一例

U 主任：セッションフィクセーションの脆弱性について，どのような対策が考えられますか。

T 君　：例えば，サーバ側の処理を変更する方法があります。検査シナリオの画面遷移でいえば，ログイン後の，画面 E から画面 C に遷移する際の，サーバ側の処理において，［ g ］といった対策を行うことによって，この脆弱性を確実に防ぐことができます。

U 主任は，その後も T 君に対してディスカッションや報告書の審査などを行い，技能試験は終了した。

T 君は見事，技能試験に合格し，SPG の検査員として業務を始めた。

設問 1　本文中の下線①について，(1)，(2)に答えよ。

(1) secure 属性が設定されていないと，どの画面に遷移するときにセッション ID を盗聴されるリスクがあるか。遷移直後の画面を，画面 A～E の中から一つ選び，答えよ。

(2) secure 属性が設定されていないと，セッション ID を盗聴されるリスクがある理由を，40 字以内で述べよ。

設問 2　HTTP ヘッダインジェクションの脆弱性について，(1)～(3)に答えよ。

(1) 図 7 中の［ a ］に入れる適切な文字列を URL エンコード済の形式で答えよ。

(2) 本文中の［ 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　SQL インジェクション　　イ　TCP SYN Flood

ウ　クロスサイトスクリプティング　　エ　ディレクトリトラバーサル

(3) 本文中の［ c ］に入れる適切な処理を，30 字以内で具体的に述べよ。

設問 3　セッション管理の脆弱性について，(1)～(4)に答えよ。

(1) 本文中の［ d ］，［ e ］に入れる適切な行番号を答えよ。

(2) 図 9 中の［ f ］に入れる適切な字句を答えよ。

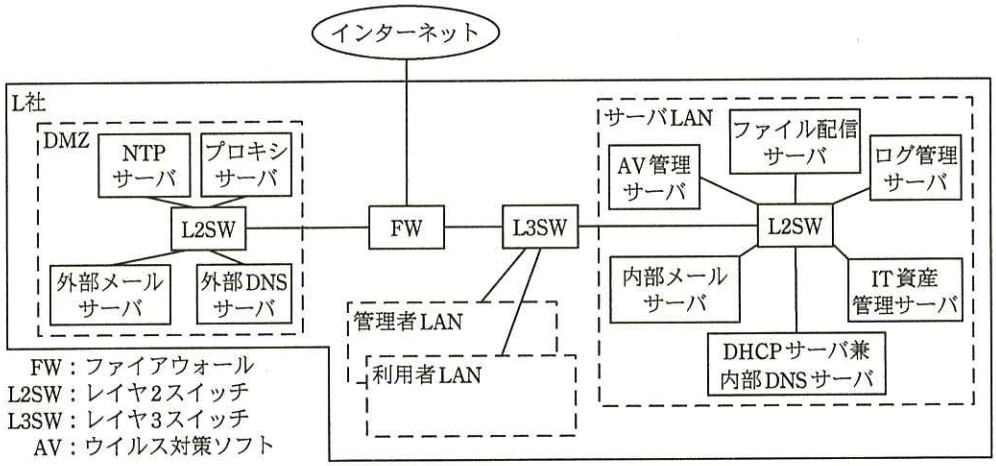
(3) 図 9 中の手順 4 及び 5 について，利用者 K がログインした後，攻撃者 J が

利用者 K になりすますことができるのはなぜか。“セッション ID”という字句を含めて 40 字以内で述べよ。

(4) 本文中の [g] に入れる適切な対策を，30 字以内で述べよ。

問2　情報漏えいインシデントの調査に関する次の記述を読んで，設問1～3に答えよ。

L社は，従業員数700名のシステムインテグレータである。L社のネットワーク構成を図1に，主なサーバとその概要を表1に示す。



注記1　L3SWのデフォルトゲートウェイは，FWに設定されている。
注記2　L社のPCは，利用者LAN又は管理者LANに接続されている。

図1　L社のネットワーク構成（概要）

表1　主なサーバとその概要

サーバ名称	概要
プロキシサーバ	・プロキシ認証機能を使用し，利用者IDとパスワードで認証する。 ・ブラックリスト型のURLフィルタリング機能をもつ。
AV管理サーバ	・各PC及び各サーバ上で稼働しているAVは，ウイルス定義ファイルをAV管理サーバから自動的に取得するよう設定されている。
ファイル配信サーバ	・パッチの自動配信及びパッチの強制適用に利用されている。
ログ管理サーバ	・図1中のネットワーク機器及びサーバのログをsyslogで受信し，直近3か月分を保存する。 ・syslog受信に必要なポート以外は全て閉じ，リモートからアクセスできないようにしている。
IT資産管理サーバ	・各PC及び各サーバの次の情報を保管する。 - 管理番号 - 管理者従業員番号 - 型式及びシリアル番号 - MACアドレス - OS名とそのバージョン
内部DNSサーバ	・L社ネットワーク上にある機器の名前解決を行う。
外部DNSサーバ	・L社外部メールサーバのMXレコードに関する名前解決，及びL社ネットワーク外の機器の名前解決を行う。

各サーバは，アクセスログ，操作ログ，ミドルウェアのログ及びアプリケーションプログラムのログをログ管理サーバに送信するとともに，各サーバ上でも直近 3 か月分のログを保存している。

FW はステートフルパケットインスペクション型であり，NAPT 機能を使用している。また，許可した通信，拒否した通信ともにログを取得するように設定し，取得したログは全てログ管理サーバに送信している。FW のフィルタリングルールを表 2 に示す。

表 2　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
1	インターネット	外部メールサーバ	SMTP	許可
2	インターネット	外部 DNS サーバ	DNS	許可
3	外部メールサーバ	インターネット	SMTP	許可
4	プロキシサーバ	インターネット	HTTP，HTTPS	許可
5	NTP サーバ	インターネット	NTP	許可
6	外部 DNS サーバ	インターネット	DNS	許可
7	サーバ LAN	プロキシサーバ	代替 HTTP	許可
8	利用者 LAN	プロキシサーバ	代替 HTTP	許可
9	管理者 LAN	プロキシサーバ	代替 HTTP	許可
10	管理者 LAN	DMZ	SSH	許可
11	DMZ	ログ管理サーバ	syslog	許可
⋮	⋮	⋮	⋮	⋮
25	全て	全て	全て	拒否

注記 1　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。
注記 2　項番 12～24 は，送信元及び宛先のどちらもインターネットではないルールである。
注記 3　L 社では，代替 HTTP は TCP ポート 8080 を使用している。

L 社ネットワーク上の全てのサーバ，ネットワーク機器及び PC は，NTP サーバと時刻同期を行っている。

L 社での PC に関する環境を図 2 に示す。

- PC は，従業員 1 人につき 1 台貸与されている。
- USB は使用できない設定となっている。
- 光学メディア用のドライブ及びメモリカード用のリーダは，搭載していない。
- DHCP で IP アドレスが動的に付与されるとともに，デフォルトゲートウェイが L3SW に，DNS サーバが内部 DNS サーバに設定される。
- Web ブラウザでのインターネットアクセスは，プロキシサーバを使用するよう設定されている。

図 2　PC に関する環境（抜粋）

L 社のサーバ，ネットワーク及び PC は，IT 部が，M 部長の下，リーダの N さんを中心に 10 名で設計，構築，保守・運用を行っている。

L 社では，サーバごとに個別の利用者 ID を IT 部の各従業員に付与しており，サーバの保守・運用時には，その利用者 ID を用いて SSH でサーバに接続し，管理者権限に昇格して作業を行う規則になっている。また，IT 部ではサーバの保守・運用に使用する利用者 ID 及びパスワードの情報を PC に保管してはならない規則となっている。

〔情報漏えいインシデント〕

4 月 23 日に，L 社が加盟しているセキュリティ情報共有団体から L 社に連絡が入った。海外のセキュリティ団体が入手した C&C（Command & Control）サーバの通信履歴の中に，L 社に割り当てられている IP アドレスからの通信が含まれていたとのことであった。セキュリティ情報共有団体からは，C&C サーバの IP アドレス及びポート番号，送信元 IP アドレス並びに C&C サーバ側の受信日時の情報が提供された。受信日時は協定世界時（UTC）で 4 月 16 日 7 時 13 分であった。

〔初期対応〕

M 部長から指示を受け，N さんが確認したところ，送信元 IP アドレスは間違いなく L 社のものであった。また，①この IP アドレスから当該 C&C サーバへの通信が発生していたことも確認できた。送信日時は日本時間で 4 月 16 日 16 時 13 分であった。これらの確認結果を基に，セキュリティ情報共有団体に更なる情報提供を依頼したところ，当該 C&C サーバに送信された情報が提供された。その中には，L 社のファイル配信サーバのホスト名，IT 部の V さんに付与された当該サーバの利用者 ID 及びパスワードが含まれていた。

N さんは，調査結果を M 部長に報告し，次の緊急対応を実施した。

・ファイル配信サーバ上での当該利用者 ID の無効化
・FW による，当該 C&C サーバへの通信の遮断

N さんは M 部長の指示で，漏えい元を特定するために，C&C サーバへの通信の送信元を調査した。その結果を図 3 に示す。

1. 提供された送信元 IP アドレスは，L 社のネットワーク構成から分かるように，［ a ］のものであった。
2. ［ a ］のログから，当該 C&C サーバと［ a ］経由で通信を行っていた機器の IP アドレスを特定したところ，［ b ］のものであった。
3. ［ b ］のログから，当該 C&C サーバに［ b ］経由で HTTP 接続を行っていた機器の IP アドレス，及び［ b ］接続時の認証に使用した利用者 ID が特定できた。
4. 認証に使用された利用者 ID は，V さんに付与されたものであった。
5. DHCP サーバのログから，上記 3 で特定した IP アドレスが割り当てられていた機器の［ c ］が特定できた。
6. IT 資産管理サーバに保管されている情報によると，当該［ c ］をもつ機器は，V さんに貸与されている管理番号 0019 の PC であった。
7. V さんは，管理者 LAN に接続した当該 PC から，ファイル配信サーバを含む複数のサーバの保守・運用を行っている。
8. V さんは，これら保守・運用対象のサーバにアクセスするための利用者 ID 及びパスワードを，当該 PC に保管していなかった。

図 3　C&C サーバへの通信の送信元の調査結果

N さんは当該 PC をネットワークから切り離した上で，M 部長に図 3 の調査結果を報告した。

〔詳細調査と暫定対応〕

N さんは M 部長の指示で，当該 PC に対するディジタルフォレンジックスによる調査を，セキュリティ専門会社に依頼した。セキュリティ専門会社による調査報告を図 4 に示す。

・当該 PC には，次の 3 種類のマルウェアに感染している痕跡が残っていた。
  - ダウンローダ
  - キーロガー
  - リモートから制御できるトロイの木馬
・これらのマルウェアは，いずれも自ら感染を広げるタイプではない。
・マルウェア内に C&C サーバの FQDN が記述され，C&C サーバへの接続に使用されていた。五つの異なる FQDN が確認できた。
・各マルウェアの C&C サーバとの通信は，次の手順で行われていた。
  1. ②プロキシサーバを利用せずに C&C サーバへの接続を試みる。
  2. 上記 1 が失敗した場合，Web ブラウザのプロキシ設定を基に，プロキシサーバを利用して接続を試みる。
  3. 上記 2 が失敗した場合，PC に保管されている利用者 ID 及びパスワードを窃取して認証突破を試みる。
  4. 上記 3 が失敗した場合，ランダムな時間間隔で上記 2 だけを繰り返す。
・最初の感染は 3 月 28 日 13 時 7 分であると考えられる。
・この時刻よりも前にエクスプロイトやマルウェアをダウンロードした痕跡は残っていなかった。
・この時刻よりも後に複数のマルウェアをダウンロードした痕跡が残っていた。
・マルウェアが C&C サーバにアップロードした情報の痕跡は残っていなかった。
・これらのマルウェアは 5 月 14 日時点で L 社が使用していた AV では検知されなかった。

図 4　セキュリティ専門会社による調査報告（抜粋）

N さんは，M 部長に図 4 の調査報告を説明した。M 部長は，この調査によって明らかになったマルウェアの特徴から，IP アドレスを基にした FW による通信の遮断では，C&C サーバへの通信を完全には遮断できない可能性があることを指摘した。N さんは，M 部長の指摘に基づき，③この調査で明らかになった C&C サーバへの通信方法を考慮した，新たな遮断方法を検討し，M 部長の承認を得た上で実施した。

〔追加調査〕

N さんは，影響範囲及びマルウェア感染経路を特定するための追加調査を立案し，M 部長から実行承認を得た。追加調査の内容を図 5 に示す。

追加調査 1.　V さんの PC 以外の PC 及びサーバに対する，図 4 で報告されたマルウェアの感染状況調査
追加調査 2.　④最初のマルウェア感染後にファイル配信サーバから配信されたファイルの調査
追加調査 3.　最初のマルウェア感染後に V さんの利用者 ID でアクセスしたサーバの特定と，アクセス内容の調査
追加調査 4.　最初のマルウェア感染前に V さんが受け取った電子メールの調査

図 5　影響範囲及びマルウェア感染経路を特定するための追加調査

L 社では，AV ベンダとの間で，マルウェアの調査及び対応するウイルス定義ファイルの作成を依頼できる契約を結んでいる。N さんは，図 4 で報告された 3 種類のマルウェアについて，対応するウイルス定義ファイルの作成を AV ベンダに依頼し，そ

のウイルス定義ファイルを用いて追加調査 1 を実施した。その結果，L 社内の他の PC 及びサーバでは，これらのマルウェアの感染は確認されなかった。

N さんは，追加調査 2 として，ファイル配信サーバ上に保存されている操作ログ，アプリケーションプログラムのログ及び配信ファイルのアーカイブを調査した。ファイル配信サーバから 3 月 28 日以降に配信されたファイルは，全て N さんが V さんに指示して配信したものであることが確認できた。

N さんは，追加調査 3 として，L 社内のサーバのうち，V さんの利用者 ID でアクセス可能な全てのサーバ上のアクセスログを調査し，最初のマルウェア感染後に V さんの利用者 ID で当該 PC からアクセスされたサーバを特定した。当該サーバとして，ファイル配信サーバ以外に，NTP サーバ，DHCP サーバ兼内部 DNS サーバ及びプロキシサーバの 3 台が確認できた。これら 3 台のサーバ上の操作ログを更に詳細に確認したところ，各サーバに対する V さんの利用者 ID での操作は，全て N さんの指示に基づく保守・運用作業であり，不正な操作が行われた形跡はなかった。これら 3 台のサーバは，L 社ネットワーク構成において重要であり，サービス停止ができないものであった。N さんは，これらのサーバ上で不正な操作が行われた形跡がなかったこと及びサービス停止ができないことから，⑤これらのサーバ上で実行可能で効果の見込まれる対策を実施した。

N さんは，追加調査 4 として，3 月 1 日から 28 日までに V さんが受け取った電子メールを調査するとともに，V さんへの聞き取りを実施した。その結果，V さんが，3 月 28 日に，インターネットファックスサービスを装った電子メールを受け取り，添付ファイルを開いていたことが判明した。AV ベンダに調査を依頼した結果，このファイルはダウンローダをインストールすることが分かった。

N さんは，これらの結果を M 部長に報告した。

M 部長は，追加調査 3 について，⑥これら 3 台のサーバ上のログに対する改ざんの痕跡が残っていないことを確認したか，N さんに尋ねた。N さんは，ログの改ざんを想定した調査は行っていなかったことを報告し，ログの再調査を実施した。再調査の結果，これら 3 台のサーバ上のログに対する改ざんの痕跡は残っていなかった。N さんは，M 部長に再調査の結果を報告した。

M 部長は，調査結果を了承し，恒久対応としての再発防止策の立案を N さんに指示した。

設問 1　〔初期対応〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，確認の具体的な方法を，30 字以内で述べよ。

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

設問 2　〔詳細調査と暫定対応〕について，(1)，(2)に答えよ。

(1)　図 4 中の下線②の試みは，L 社の PC からでは必ず失敗するが，FW のログには記録されない。その理由を 35 字以内で述べよ。

(2)　本文中の下線③について，遮断の具体的な方法を 40 字以内で述べよ。

設問 3　〔追加調査〕について，(1)～(3)に答えよ。

(1)　図 5 中の下線④の調査は，どのような攻撃を想定したものか。想定した攻撃を 30 字以内で述べよ。

(2)　本文中の下線⑤について，これら 3 台のサーバ上で実施すべき対策を 20 字以内で述べよ。

(3)　本文中の下線⑥について，ログの改ざんの痕跡を確認する方法を 30 字以内で述べよ。

問 3　パスワードへの攻撃に関する次の記述を読んで，設問 1～4 に答えよ。

Z 社は，従業員数 300 名の衣料品販売企業であり，インターネット上で衣料品を購入できるショッピングサイト（以下，Z サイトという）を 7 年前から運営している。Z サイトは，携帯電話，スマートフォン及び PC を対象としたサイトであり，オンライン決済にはクレジットカードを採用している。クレジットカード情報は会員情報として保存せずに，決済の都度入力してもらう方式にしている。利用者は，会員登録をすれば，購入金額に応じたポイントをためて，購入代金への充当や，他社のギフト券への交換ができる。Z サイトの現在の会員数は約 400 万人である。

Z サイトの会員の利用者 ID は，会員のメールアドレスであり，パスワードは，携帯電話での利便性を考慮し，数字 6 桁の固定長となっている。同じ日の 0 時から 24 時の間に連続 5 回認証に失敗した利用者 ID は，アカウントロック状態となり，翌日にその状態が解除される仕組みとなっている。

〔不正アクセスの発生〕

ある日，Z サイトの問合せ窓口の担当者から，Z サイトの運用を担当しているシステム運用部の A 主任に連絡があり，ポイントが勝手にギフト券に交換されたという被害の連絡を，会員 11 名から受けたことが報告された。報告を受けた A 主任がログサーバを調査したところ，特定の IP アドレスから，Z サイトの会員ページへのログイン試行が，短時間のうちに大量に発生していたことが分かった。A 主任は，上司である B 部長の指示の下，全会員に事象を告知するとともに，経営陣の承認を経て Z サイトを緊急閉鎖し，以前にセキュリティ診断を依頼したことがある Y 社に，この不正アクセスの調査を依頼した。大量のログイン試行のログを表 1 に示す。

表 1　大量のログイン試行のログ（抜粋）

日時	接続元 IP アドレス	利用者 ID	パスワード
2014/9/18 19:21:10	x.y.1.12	abcde@aaaaa.ne.jp	123456
2014/9/18 19:21:10	x.y.1.12	agikaen@bbbbb.com	123456
2014/9/18 19:21:11	x.y.1.12	12ko3k3@bbbbb.com	123456
2014/9/18 19:21:12	x.y.1.12	k323t4t34@ccccc.ne.jp	123456
2014/9/18 19:21:13	x.y.1.12	93adfasga@ddddd.ne.jp	123456
2014/9/18 19:21:13	x.y.1.12	192slsoso@aaaaa.ne.jp	123456

〔不正アクセスの調査結果〕

3日後，Y社による，不正アクセスの詳細な調査が終了した。次は，A主任がB部長に調査結果を報告した際の会話である。

A主任：Y社の調査によると，パスワードを固定した上で，約70万個の文字列を次々に利用者IDとして入力し，ログインを試行するという攻撃があったとのことでした。試行された利用者IDのうち，7万個については，利用者IDとして実在していました。また，実際に560件の利用者IDについては，不正ログインまで成功しており，さらに，130件については，ポイントが不正に交換されていました。

B部長：ポイントが不正交換された会員への連絡は済んでいるのかね。

A主任：はい，不正交換された会員を含め，不正ログインされた会員への個別連絡と，全会員への注意喚起は完了しています。

B部長：分かった。経営陣には私から報告しておく。

A主任：不正ログインされた会員に対して，パスワードリセットを実施したいのですが，よろしいでしょうか。

B部長：Zサイトの再開までにはパスワードリセットも必須だが，それよりも，今回のような攻撃は今後も繰り返される可能性があるので，Y社に依頼して，現在のZサイトのアカウント管理の問題点を調査してもらってくれ。パスワードリセットとZサイトの再開時期については，問題点の調査結果を見た上で考えることにする。

A主任：分かりました。それでは再度Y社に調査を依頼します。

A主任は，早速Y社に調査を依頼し，当日中にY社による調査が開始された。

〔問題点の調査結果と改善案〕

調査開始から4日後，Zサイトのアカウント管理における問題点の調査結果の報告がY社からあり，複数の問題点が存在することが分かった。Y社が報告したZサイトのアカウント管理の主要な問題点を図1に示す。

問題点(ア)　パスワード強度が不十分である
　パスワードに使用できる文字種が数字だけであり，かつ，パスワード長が短い。
問題点(イ)　パスワード保存方法が不適切
　パスワードをハッシュ化しただけで保存しているので，パスワードファイルが窃取された際に，パスワードを推測されるおそれがある。

図1　アカウント管理の主要な問題点

また，Y社は，これらの問題点についてそれぞれ図2の改善案を提示した。

改善案(ア)　パスワード強度の変更
・パスワードに使用できる文字種を，英大文字，英小文字，数字及び記号の80種とする。
・パスワードの最小文字数を8文字，最大文字数を64文字とする。
改善案(イ)　パスワード保存方法の変更
・①アカウントごとにソルトを設定し，ソルトとパスワードを結合したものをSHA-256ハッシュ関数でハッシュ化して保存する。

図2　改善案

A主任は，これらの改善案を実施するためのシステム改修の見積作業に取り掛かった。

〔暫定再開の検討〕

見積りの結果，ハッシュ値の保存に必要な領域が，1アカウント当たり16バイトから［　a　］バイトに変更されるのに加え，ソルトの保存領域の追加などの改修やディスクの増設が必要となり，再開まで3か月掛かることが分かった。A主任は，そのことをB部長に相談したところ，3か月間のZサイト閉鎖は，経営上の影響が非常に大きいので，何らかの対応を行った上で暫定再開する方法をY社と検討するよう指示を受けた。次はその時の，A主任とY社のC氏との会話である。

A主任：システム改修の3か月間，Zサイトを閉鎖することは，当社にとって影響が非常に大きいことから，何らかの対応を行った上で暫定再開させたいのですが，良い方法はないでしょうか。

C氏　：経営上の影響を考えると暫定再開はやむを得ないですね。図3のようなパスワードに対する攻撃（以下，パスワード攻撃という）を検知し対応する仕組みを導入し，攻撃を検知した場合は都度対応する運用とした上で，暫定再開

する方法はいかがでしょうか。ただし，暫定再開に当たっては，不正ログインされた会員のパスワードリセットを忘れずに実施してください。また，ポイントの交換については，システム改修が完了するまで停止した方が良いと思います。

方法(ア)
単位時間当たりのアカウントロックされた会員の数のしきい値を設定し，そのしきい値を超えた場合には，システム運用部に通知する。
方法(イ)
方法(ア)で検知されない場合に対処するために，［ b ］のしきい値を設定し，そのしきい値を超えた場合には，システム運用部に通知する。システム運用部は，当該 IP アドレスからの接続をファイアウォールのルール設定で遮断する。
方法(ウ)
方法(ア)でも方法(イ)でも検知されない場合に対処するために，単位時間当たりのログイン失敗数のしきい値を設定し，そのしきい値を超えた場合には，システム運用部に通知する。システム運用部は，Z サイトを緊急に閉鎖する必要があるかどうかを検討し，必要がある場合，経営陣の承認を経て閉鎖する。

図３　パスワード攻撃を検知し対応する方法

A 主任：分かりました。ところで，三つの方法は，それぞれどのようなパスワード攻撃を検知することができるのですか。

C 氏　：方法(ア)では，パスワード総当たり攻撃や辞書攻撃を検知します。方法(イ)では，今回の攻撃のように，同一 IP アドレスからのリバースブルートフォース攻撃を検知します。方法(ウ)では，［ c ］から行われるパスワード攻撃を検知します。ただし，どの方法も，攻撃を 100％検知できるというわけではありません。

A 主任：分かりました。それらの対応であれば１週間でできそうです。

A 主任は，暫定再開に向けた作業を行い，１週間後，Z サイトを暫定再開した。

〔本格再開の検討〕

A 主任は，本格再開に向けた作業を確認するために，再び C 氏に相談した。次はその時の A 主任と C 氏との会話である。

A 主任：パスワード攻撃の監視と対応を継続すれば，システム改修にもう少し時間を掛けてもよいのではないかと考えているのですが。

C 氏　：それは危険です。実は問題が幾つかあります。例えば，パスワード攻撃には，方法(ア)～(ウ)を組み合わせても検知できないものがあります。現行のパスワード強度と改善後のパスワード強度を比較評価するため，その攻撃が行われた場合に，どのくらいの時間で攻撃が成功するかを計算してみましょう。

C 氏は，方法(ア)～(ウ)を組み合わせても検知されずに行われるパスワード攻撃が成功するまでの所要時間を，図 4 のように説明した。

【前提条件】
(A)　会員によるログイン失敗が，1 日当たり 7,000 件あるとする。
(B)　方法(ウ)中の単位時間当たりのログイン失敗数のしきい値を(A)の 2 倍，つまり，1 日当たり 14,000 件とする。
(C)　攻撃方法の前提条件
（i）何らかの方法で n 人分の利用者 ID（会員メールアドレス）のリストを取得済み
なお，n > 5,000 とする。
（ii）方法(ア)で検知されないよう，利用者 ID ごとに 1 日 4 回を上限に攻撃
（iii）方法(イ)で検知されないよう，［ c ］から攻撃
（iv）方法(ウ)で検知されないよう，パスワード攻撃の試行回数の上限は，(A)と合わせても(B)より少ない 1 日当たり 5,000 件

【攻撃成功時間の計算】
(あ)　数字 6 桁のパスワードの場合，パスワードの全組合せは，［ d ］通りである。上記の前提条件に沿って，試行の都度パスワードと利用者 ID を変えながらパスワードの全組合せを試行すると，少なくとも［ e ］日掛かる。また，一つのパスワードで，取得済みの全ての利用者 ID に対して試行した後，別のパスワードで，取得済みの全ての利用者 ID に対して試行する。これをパスワードを変えながら繰り返すと，どれか一つの利用者 ID のログインに成功するために要する平均日数は，n によって異なるが，［ e ］日の半分よりも大きく，［ e ］日以下である。
(い)　文字種が 80 種で 8 桁のパスワードの場合，パスワードの全組合せは，［ f ］通りである。全てのパスワードを試行するためには，3,355 億 4,432 万日掛かる。また，(あ)と同様に試行した場合，どれか一つの利用者 ID のログインに成功するために要する平均日数は，n によって異なり，3,355 億 4,432 万日の半分よりも大きく，3,355 億 4,432 万日以下である。

図 4　パスワード攻撃が成功するまでの所要時間の計算

A 主任：なるほど，暫定期間を延ばすと，検知を擦り抜けて不正ログインされる可能性が十分に現実的になるということですね。それでは，パスワード強度の変更とパスワード保存方法の変更が完了したことを条件として本格再開の時期

を設定します。他に気をつけることはありますか。

C氏　：会員には②他のサイトで使っていないパスワードを設定してもらうよう注意喚起した方がいいですね。

A主任：分かりました。

A主任は，Zサイトの本格再開に向けたシステム改修計画をまとめ，B部長とともに経営陣の承認を取り，3か月後に本格再開を果たした。

設問1　図2中の下線①は，ハッシュ値が保存されているファイルが漏えいした場合に，そのファイルに保存されたハッシュ値からパスワードが推測されることを防ぐための方法である。ソルトを用いることによって防ぐことができる攻撃方法を，60字以内で具体的に述べよ。

設問2　〔暫定再開の検討〕について，(1)～(3)に答えよ。

(1)　本文中の［　a　］に入れる適切な数値を答えよ。

(2)　図3中の［　b　］に入れる適切な字句を，30字以内で述べよ。

(3)　本文中及び図4中の［　c　］に入れる適切な字句を，15字以内で答えよ。

設問3　図4中の［　d　］～［　f　］に入れる適切な数式又は実際の値を答えよ。

設問4　本文中の下線②は，どのような攻撃による被害を避けるための注意喚起か。攻撃方法を45字以内で具体的に述べよ。

〔 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。
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。

午