SC

平成26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アプリケーションに関する次の記述を読んで，設問1～3に答えよ。

B社は，従業員数50名のインターネットサービス企業であり，インターネット上で各種の情報サービスを提供している。これらのサービスの実現に当たり，必要なアプリケーションを自社開発してきた。このたびB社では，画像ファイルを対象としたオンライン共有ストレージサービス（以下，Sサービスという）を立ち上げることにし，R部長を責任者としてアプリケーション開発に着手した。Sサービスの画面には広告主のサイトへのリンクを含んだバナー広告を掲載し，利用者からの利用料収入に加えて広告料収入の獲得も目指す。

〔Sサービスの要件定義〕

B社では，P主任を中心としてSサービスの要件を検討した。検討の結果，P主任はSサービスの要件案を図1に示すとおりまとめた。

(1) クライアント側はWebブラウザだけとし，専用アプリケーションは使用しない。プロトコルは，HTTPとHTTP over TLS（以下，HTTPSという）のどちらも使用できる。
(2) 利用者は，Sサービスの利用に先立ち，英字4文字に数字4文字を付加した全8文字の利用者IDの割当てを受ける。利用者種別は，契約者と閲覧者の2種類とする。
(3) 契約者になるためには利用料を支払う必要がある。閲覧者になるための料金は不要である。
(4) 利用者がSサービスにアクセスする際は，最初に利用者IDとパスワードによる認証が行われる。
(5) 契約者は，共有フォルダを作成でき，書込・削除・読取権限をもつ。さらに，任意の閲覧者に対して，その共有フォルダへの読取権限を付与することができる。
(6) 契約者が保存できる画像ファイルのサイズの合計は，契約条件で定める最大値を超えないように制限される。
(7) 画像ファイルのアップロード時には，画像ファイルに，注釈文を添付することができる。
(8) 利用者は，読取権限をもつ共有フォルダ内の画像ファイルを，小さな画像として一覧表示（以下，サムネイル表示という）でき，必要に応じてオリジナルの画像ファイルをダウンロードできる。
（以下，省略）

図1　Sサービスの要件案

この要件案は，レビューされた後，R部長によって承認された。

〔システム・ソフトウェア要件定義〕

その後，Q主任を中心としてシステム・ソフトウェア要件定義を実施した。その結果，Sサービスは Java サーブレットを利用した Web アプリケーションで構成するこ

とにした。画像処理プログラムについては C++で記述し，プログラム内では C ベースの画像処理ライブラリである V-lib を利用することにした。Java から C++プログラムを呼び出す際には，JNI（Java Native Interface）を利用することにした。

〔ソフトウェアの基本設計〕

システム・ソフトウェア要件定義が完了し，ソフトウェアの基本設計を開始した。その中で，V 君は Web アプリケーションのセッション管理の方式について検討した。次は，検討に際しての Q 主任と V 君との会話である。

Q 主任：HTTP セッション管理には，どのような方式を採用するつもりかな。

V 君　：セッション管理には，ログオン時にランダム文字列をセッション ID として割り当てた上で，クエリパラメタの中にセッション ID を格納する方式を採用するつもりです。

Q 主任：当社でも実績のある方式だね。ただ，今回は HTTPS だけでなく HTTP も使用できるようにするから，GET メソッドではなく POST メソッドを使用しておかないと，①HTTP ヘッダ内のフィールドが原因で，バナー広告に設定されたリンク先の Web サーバへセッション ID が漏えいすることが考えられるね。

更に基本設計が進む中で，実行形式ファイルがアップロードされるとウイルスの温床になりかねないという指摘があった。議論した結果，この指摘への対策の一つとして，アップロードするファイルの拡張子を画像ファイルのものに制限することとした。制限する方式として，V 君は，Web ブラウザにおいてスクリプトによって判定することを考えた。この方式を実装したスクリプトを含む HTML ファイル例を図 2 に示す。この方式案について相談を受けた Q 主任は，②契約者の操作によっては，拡張子が画像ファイルのものでないファイルがアップロードできてしまうという問題点を指摘し，制限する方式には③スクリプトによらない方式を検討するよう指示した。V 君はその後，異なる方式を提案し，採用に至った。

```
<form action="/sservice/UploadFile" method="POST" id="form_upload"
 enctype="multipart/form-data">
    <input type="file" name="upload" size="128">
    <input type="submit" name="button_submit" value="送信">
</form>
<script type="text/javascript">
    <!--
    var input = document.getElementById("form_upload");
    input.onsubmit = function () {
    （省略）/* アップロードするファイルの拡張子を調べて，画像ファイルかどうか判定し，画像でない
          ファイルの送信を停止する。*/
    }
//   -->
</script>
```

図２　HTML ファイル例（抜粋）

〔画像処理プログラムでの不具合〕

基本設計及び詳細設計が無事完了し，U 主任を中心としたグループでプログラムの作成を開始した。U 主任は，サムネイル表示の際に使用するために，様々なファイル形式の画像ファイルを縦横とも 128 ピクセルに変換する画像処理プログラム（以下，ピクセル数変換プログラムという）の作成を T 君に指示した。T 君は，最初に，複数のファイル形式の中からファイル形式 Z を選択して，ピクセル数変換プログラムの作成に取り掛かった。

このプログラムで取り扱う，ファイル形式 Z を図 3 に示す。ピクセル数変換そのものには，V-lib 内の vlibResize 関数を使用することにした。V-lib 内で定義され，vlibResize 関数の引数として使用する vlibMat 構造体の説明を図 4 に示す。また，vlibResize 関数の外部仕様を図 5 に示す。

ヘッダ部	
	ファイル形式識別子　2 バイト（固定文字列）
	ファイル形式バージョン番号　2 バイト（整数）
	列数　2 バイト（整数）
	行数　2 バイト（整数）
	各ピクセルのバイト数　2 バイト（整数）
ピクセルデータ (1 行目のピクセルデータが RGB の順に並び，続いて 2 行目以降のピクセルデータが並ぶ。行と行の間には区切り記号はない。)	

注記　整数はいずれも符号なしとする。

図３　ファイル形式 Z

```
typedef struct {
    char* data;    /* ピクセルデータへのポインタ，各ピクセルのサイズは 3 バイト(RGB)とする */
    int  cols;     /* 画像の列数 */
    int  rows;     /* 画像の行数 */
} vlibMat;
```

data が指す領域は，1 行目のピクセルデータが RGB の順に並び，続いて 2 行目以降のピクセルデータが並ぶ。
なお，各行の先頭を 256 バイト境界に配置するために，必要に応じてパディングをする。

data 領域のパディング例： 1 行当たり 128 ピクセル，384 バイトの場合

図 4　vlibMat 構造体の説明

```
int vlibResize(const vlibMat* src, vlibMat* dst)
  機能：src を基に，縦横ピクセル数を変換して dst に書き込む。
  引数：src：入力画像
        dst：出力画像
             変換後の横ピクセル数を dst->cols に，
             変換後の縦ピクセル数を dst->rows にセットして，
             dst->data が指す領域は，書込み可能領域として確保してから呼び出す。
  返却値：正常に完了すれば 0，正常に完了しなかった場合は-1 とする。
```

図 5　vlibResize 関数の外部仕様

T 君は，図 6 のピクセル数変換プログラムを作成し，U 主任によるソースコードレビューを受けた。そのソースコードレビューで，U 主任は，入力する画像ファイルの内容によっては 38 行目において［ a ］が発生し，その結果として 50 行目において［ b ］が発生することを指摘した。

なお，この処理系において，int 型は 4 バイト，short int 型は 2 バイト，char 型は 1 バイトである。また，char 型は特に記述がなければ符号なしである。

```
 1: #include <cstdlib>
 2: #include <iostream>
 3: #include <exception>
 4: #include "vlib.h"    /* 画像処理ライブラリ V-lib 用ヘッダファイル */
 5: （省略）/* その他，必要なヘッダファイルを読み込む。 */
 6: using namespace std;
 7:
 8: const int kIndexCols = 128;    /* サムネイル表示用列数 */
 9: const int kIndexRows = 128;    /* サムネイル表示用行数 */
10: const int kMaxMatData = 104857600;    /* 100M バイト */
11: const int kMaxInteger = 0x7fffffff;
12: const int kColors = 3;
13:
14: typedef struct {
15:     char ident0, ident1;
16:     unsigned short int f_version, cols, rows, colors;
17: } zHeader;  /* ファイル形式 Z のヘッダ部 */
18:
19: int resize_fileZ(FILE *fp, vlibMat* matBuf) throw(std::out_of_range, std::bad_alloc)
20: {
21:     /* fp はファイル形式 Z の画像ファイルへのファイルポインタ */
22:     /* matBuf はピクセル数変換後の画像を保存する構造体へのポインタ */
23:     /* matBuf->data が指す領域はこの関数内で確保し，呼出し側で解放する。 */
24:     int       bytesOfRow, bytesOfBuff;
25:     zHeader   fhBuf;
26:     char *    pixBuf;
27:     vlibMat   inBuf;
28:
29:     fseek(fp, 0L, SEEK_SET);    /* ファイル読込位置をファイルの先頭に移動 */
30:     /* ファイル fp から，zHeader のバイト数だけデータを読み込み，fhBuf に書き込む。 */
31:     /* 読込の結果，ファイル読込位置は読込バイト数だけ移動する。 */
32:     fread(&fhBuf, sizeof(zHeader), 1, fp);
33:     （省略）/* ファイル形式識別子とファイル形式バージョン番号をチェックする。 */
34:     if (fhBuf.colors != kColors) throw out_of_range("Illegal header");
35:     if (fhBuf.cols == 0 || fhBuf.rows == 0) throw out_of_range("Illegal header");
36:     bytesOfRow = fhBuf.cols * fhBuf.colors;
37:     bytesOfRow += 255 - ((bytesOfRow + 255) % 256); /* 256 バイト境界に調整 */
38:     bytesOfBuff = bytesOfRow * fhBuf.rows;
39:     if (bytesOfBuff > kMaxMatData) throw out_of_range("Image too large");
40:
41:     pixBuf = (char *)malloc(bytesOfBuff);
42:     if (pixBuf == NULL) throw bad_alloc();
43:     inBuf.data = pixBuf;
44:     inBuf.cols = fhBuf.cols;
45:     inBuf.rows = fhBuf.rows;
46:
```

図6　ピクセル数変換プログラム

```
47:     for (int i = 0; i < fhBuf.rows; i ++) {
48:         /* ファイル fp から，(fhBuf.cols * kColors) バイトだけデータを読み込み，*/
49:         /* pixBuf に書き込む。ファイル読込位置は読込バイト数だけ移動する。 */
50:         fread(pixBuf, kColors, fhBuf.cols, fp);
51:         pixBuf += fhBuf.cols * kColors;
52:         pixBuf += 255 - ((fhBuf.cols * kColors + 255) % 256); /* 256 バイト境界に調整 */
53:     }
54:     matBuf->data = (char *)malloc(((kIndexCols * kColors + 255) / 256) * 256 *
    kIndexRows);
55:     if (matBuf->data == NULL) {
56:         free(inBuf.data);
57:         throw bad_alloc();
58:     }
59:     matBuf->cols = kIndexCols;
60:     matBuf->rows = kIndexRows;
61:     if (vlibResize(&inBuf, matBuf) == -1) {
62:         free(inBuf.data);
63:         throw bad_alloc();
64:     }
65:     free(inBuf.data);
66:     return 0;
67: }
```

図 6　ピクセル数変換プログラム（続き）

T 君はこの指摘を受けて，図 6 の 37 行と 38 行の間に図 7 に示す行を追加し，再度 U 主任のソースコードレビューを受けた。ソースコードレビューの結果，指摘された問題点が修正されていること，他の部分に同種の問題点が存在しないことが確認された。

```
if ( [ c ] < [ d ] ) throw out_of_range("Image too large");
```

図 7　ピクセル数変換プログラムへの追加行

その後，全てのプログラムの作成とテストが完了して，B 社は S サービスの運用を開始することができた。

設問 1　〔ソフトウェアの基本設計〕について，(1)～(3)に答えよ。

(1)　本文中の下線①の HTTP ヘッダ内のフィールド名は何か。英字 10 字以内で答えよ。

(2) 本文中の下線②の契約者の操作とは何か。30 字以内で述べよ。

(3) 本文中の下線③の方式とはどのようなものか。30 字以内で述べよ。

設問 2 〔画像処理プログラムでの不具合〕について，(1)，(2) に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な字句を，それぞれ 15 字以内で答えよ。

(2) U 主任が指摘した［ a ］が発生する入力ファイルに関する条件を，kMaxInteger という字句を用いて 60 字以内で述べよ。

設問 3 図 7 中の［ c ］，［ d ］に入れる適切な式又は変数を答えよ。

なお，［ c ］，［ d ］のどちらか一方は，kMaxInteger を含むこと。

問2　インターネット接続システムにおける迷惑メール対策に関する次の記述を読んで，設問1～4に答えよ。

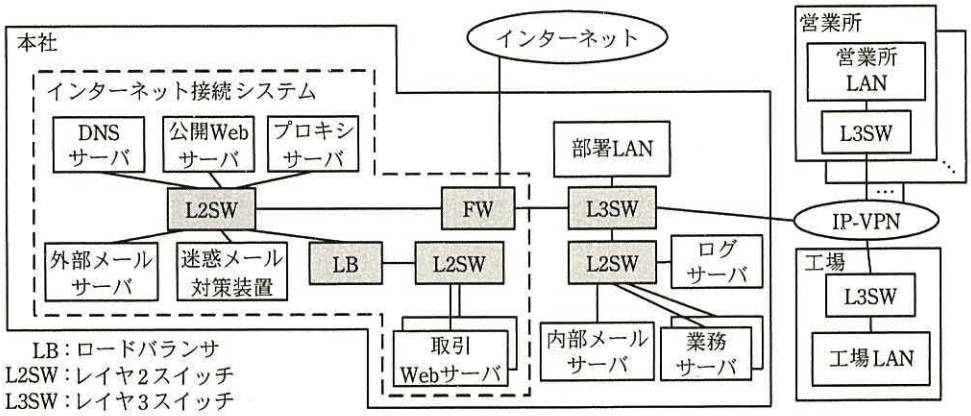
A社は，従業員数2,000名のスポーツ用品製造会社である。東京に本社，国内8か所に営業所，国内1か所に工場がある。A社では，本社にインターネット接続システムを導入し，電子メール（以下，メールという）やWeb閲覧などに利用している。本社，営業所及び工場のLANは，IP-VPNで接続されている。

〔インターネット接続システムの概要〕

インターネット接続システムの運用は，責任者である情報システム部のD部長の下で，E主任とFさんが担当している。インターネット接続システムの各サーバでは，サーバへのアクセス及びサーバ上でのプログラムの動作のログをログサーバに保存している。ログを収集，転送する方式には，UNIXで一般的に使われている［　a　］というプロトコルを利用している。ファイアウォール（以下，FWという）では，拒否した通信のログを保存している。

A社では，ドメイン名a-sha.co.jp（以下，A社ドメイン名という）を取得している。メールアドレスのドメイン名にはA社ドメイン名を使用している。

A社のネットワーク構成を図1に，インターネット接続システムの主な機器と機能概要を表1に示す。



注記1　A社のPCは全て，部署LAN，営業所LAN又は工場LANのいずれかに接続している。
注記2　PCの記載は省略している。
注記3　網掛けの機器は二重化している。

図1　A社のネットワーク構成

表1　インターネット接続システムの主な機器と機能概要

機器名称	機能概要
LB	HTTP，SMTP などのサービスの振分け機能及び IP アドレス変換機能がある。送信元 IP アドレスによって，振分け機能及び IP アドレス変換機能を使用しない設定もできる。
迷惑メール対策装置	インターネットから内部メールサーバへのメール転送機能，迷惑メールフィルタリング機能及びメールに対するウイルススキャン機能がある。迷惑メール対策装置のベンダの Web サーバから 1 時間ごとにウイルス定義ファイルをダウンロードし，更新する。
外部メールサーバ	内部メールサーバからインターネットへのメール転送機能及びメールに対するウイルススキャン機能がある。迷惑メール対策装置の故障に備えて，インターネットから内部メールサーバへのメール転送も行うことができる。ウイルス対策ソフトのベンダの Web サーバから 1 時間ごとにウイルス定義ファイルをダウンロードし，更新する。
プロキシサーバ	プロキシ機能，Web コンテンツキャッシュ機能，URL フィルタリング機能及び Web コンテンツに対するウイルススキャン機能がある。プロキシソフトのベンダの Web サーバから 1 時間ごとに URL フィルタリング定義ファイル及びウイルス定義ファイルをダウンロードし，更新する。サーバ管理者の URL の登録によって URL フィルタリングを行うことができるプロキシブラックリスト（以下，ブラックリストを BL という）がある。
取引 Web サーバ	販売店からの注文受付機能がある。注文情報は業務サーバに保存される。

インターネット接続システムでは，迷惑メール対策装置及び外部メールサーバだけがメールを扱う。

FW はステートフルパケットフィルタリング型である。その FW のルールを表 2 に示す。

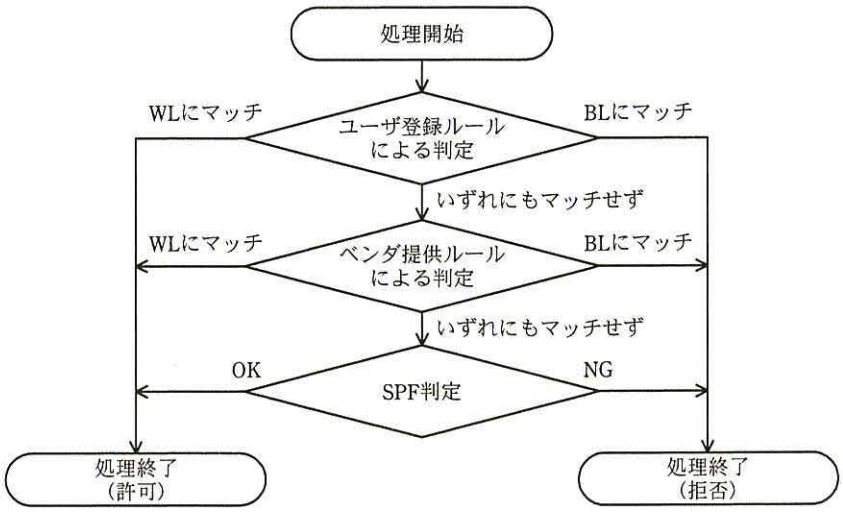
表2　FW のルール

項番	送信元	宛先	サービス	動作
1	インターネット	迷惑メール対策装置	SMTP	許可
2	インターネット	外部メールサーバ	SMTP	許可
3	迷惑メール対策装置	内部メールサーバ	SMTP	許可
4	外部メールサーバ	インターネット	SMTP	許可
5	外部メールサーバ	内部メールサーバ	SMTP	許可
6	内部メールサーバ	外部メールサーバ	SMTP	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，最初に一致したルールが適用される。
注記 2　項番 7～24 は，SMTP に関連しないルールである。

迷惑メール対策装置は，図 2 に示すようにメールの転送に関する情報及びメールの

内容を検査し，転送を許可又は拒否する。転送の許可又は拒否の判定に用いられるルールには，利用者が設定可能な“ユーザ登録ルール”と，迷惑メール対策装置のベンダから提供される“ベンダ提供ルール”があり，これらのルールを利用した判定に加え，SPF（Sender Policy Framework）を利用して判定する“SPF 判定”がある。



WL ： ホワイトリスト

注記 WL と BL の優先度については表 3 を参照

図 2　迷惑メール対策装置における判定処理

ユーザ登録ルールとベンダ提供ルールはそれぞれ表 3 に示す WL 及び BL から構成される。ユーザ登録ルールの各リストへの登録は，社内からの要望を情報システム部が受け付け，サーバ管理者である F さんが行っている。ベンダ提供ルールは，迷惑メール対策装置のベンダの Web サーバから 1 時間ごとにダウンロードして更新される。ベンダ提供ルールの具体的な内容は，開示されていない。

表3　ユーザ登録ルールとベンダ提供ルール

項番	ルール種別	形式	マッチング対象
1	IP アドレス WL	IP アドレスの並び	メールの送信元 IP アドレス
2	IP アドレス BL	IP アドレスの並び	メールの送信元 IP アドレス
3	ドメイン名 WL	ドメイン名の並び	エンベロープの送信者メールアドレスのドメイン名
4	ドメイン名 BL	ドメイン名の並び	エンベロープの送信者メールアドレスのドメイン名
5	URL BL	URL の並び	ヘッダ及びメール本文中に含まれる URL
6	単語 BL	単語の並び	ヘッダ及びメール本文中に含まれる単語

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。

A 社のメールアドレスを使ったなりすましを防ぐために，A 社の DNS サーバで SPF の設定を行っている。A 社のメールアドレスを使ったメールを送信するのは外部メールサーバだけである。メールに関する DNS の設定を図 3 に示す。

```
msv1.a-sha.co.jp.   IN A x1.y1.z1.3
msv2.a-sha.co.jp.   IN A x1.y1.z1.4
a-sha.co.jp.        IN MX 10 msv1.a-sha.co.jp.
a-sha.co.jp.        IN MX 20 msv2.a-sha.co.jp.
a-sha.co.jp.        IN TXT "v=spf1 +ip4:x1.y1.z1.4 [    b    ] "
```

注記 1　x1.y1.z1.3 は迷惑メール対策装置の IP アドレス，x1.y1.z1.4 は外部メールサーバの IP アドレスである。

注記 2　逆引き定義は省略しているが，適切に設定されている。

図3　メールに関する DNS の設定

〔迷惑メールの増加の調査〕

先週，“2 週間前から，社外が送信元とみられる迷惑メールが増加している”と営業部から情報システム部に連絡があった。D 部長は，E 主任と F さんに調査を指示した。調査したところ，全ての機器は設定どおり動作していた。次に，ログサーバに保存されているログを調査したところ，①迷惑メールが外部メールサーバから内部メールサーバに転送されており，2 週間前からその数が増加していた。

報告を受けた D 部長は，E 主任と F さんに迷惑メール対策装置のユーザ登録ルールの見直しを行ってから，今回の迷惑メールの増加への対策を行うよう指示した。

〔迷惑メール対策装置のユーザ登録ルールの見直し〕

E 主任と F さんは，迷惑メール対策装置のユーザ登録ルール全般を見直すことにし

た。

まず，IP アドレス WL と IP アドレス BL への登録の効果の持続性について検討した。たとえ取引先の IP アドレスを IP アドレス WL に登録していたとしても，メールが急に届かなくなる可能性もある。届かなくなった場合は，IP アドレス WL の登録内容を見直す必要がある。そこで，F さんは，IP アドレス WL の登録内容の見直し方法を運用手順に追加した。

次に，ドメイン名 WL とドメイン名 BL への登録について検討した。F さんは，SPF 判定があれば，ドメイン名 WL とドメイン名 BL への登録は不要ではないかと E 主任に質問した。E 主任は，“SPF を使えばドメイン名を詐称する迷惑メールの拒否が可能である。しかし，②迷惑メール送信者の行為によっては，迷惑メール対策装置が SPF を使って正しいと判定したサーバから送信された迷惑メールを防ぐことができないので必要である”と，F さんに説明した。

さらに，URL BL について検討した。F さんは，③［ c ］に登録する設定を URL BL にも登録することを提案し，効果があることを説明した。この提案には，E 主任も同意した。

最後に，単語 BL について検討し，現状のままでも問題がないことを確認した。

〔迷惑メールの増加への対策の検討〕

E 主任と F さんは，迷惑メールの増加への対策について検討した。検討の結果，④図 1 のネットワーク構成と LB の設定を変更することで，インターネット上のメールサーバからの SMTP 通信を制御することにした。さらに，表 2 のルール及び図 3 の設定を LB による制御に対応するように変更することにした。

E 主任と F さんは，検討した対策を D 部長に報告し，了承を得た。D 部長は，この対策で従業員に届く迷惑メールの減少が期待できるものの，迷惑メール対策装置だけでは，防ぐことができない迷惑メールがあるので，次の 2 点を周知するように指示した。

・不審なメールの添付ファイルを開かない。

・不審なメール中の URL をクリックしない。

指示を受けたE主任とFさんは，設定の変更と従業員への周知を行った。

これらの対処によって，従業員に届く迷惑メールが減少するとともに，不審なメールに対する従業員の対処が定着した。

設問1　〔インターネット接続システムの概要〕について，(1)，(2) に答えよ。

(1)　本文中の［　a　］に入れる適切な字句を，英字8字以内で答えよ。

(2)　図3中の［　b　］に入れる適切な字句を，英字及び記号5字以内で答えよ。

設問2　本文中の下線①について，増加した迷惑メールは，外部メールサーバにどのように送られていたか。表2のルール及び図3の設定を考慮して，35字以内で述べよ。

設問3　〔迷惑メール対策装置のユーザ登録ルールの見直し〕について，(1)～(3) に答えよ。

(1)　IPアドレスWLを見直す必要があるのは，取引先でどのような事象が発生した場合か。25字以内で具体的に述べよ。

(2)　本文中の下線②について，迷惑メールを防ぐことができなくなる迷惑メール送信者の行為を，30字以内で述べよ。

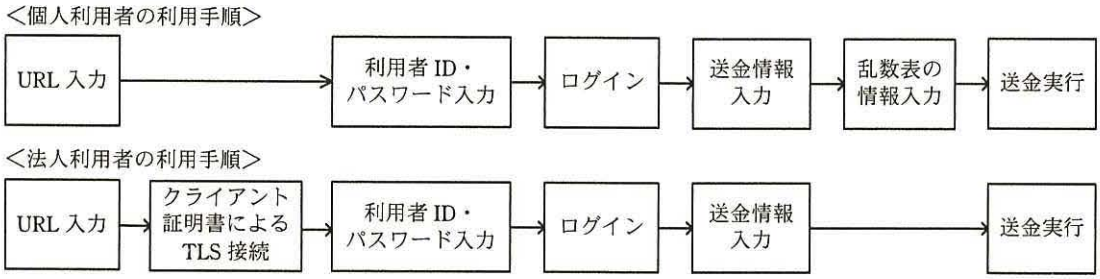
(3)　本文中の［　c　］に入れる適切な機器名を図1中から選び，答えよ。また，本文中の下線③における，登録の効果とは何か。15字以内で述べよ。

設問4　本文中の下線④について，迷惑メール対策装置が正常に稼働している場合，SMTP通信をどのように制御すべきか。30字以内で具体的に述べよ。

問3　インターネットを利用した銀行取引サービスを狙うマルウェアへの対策に関する次の記述を読んで，設問1～3に答えよ。

X銀行は，従業員数2,000名の地方銀行である。X銀行では，PCからインターネットを利用して送金，取引照会などを行える銀行取引サービス（以下，ネットバンキングという）としてXネットサービスを提供している。Xネットサービスのドメイン名はx-bank.jpであり，HTTP over TLS用にEV SSL証明書（以下，サーバ証明書という）を使用している。

Xネットサービスでは，個人利用者の認証と法人利用者の認証に，それぞれ異なる方式を採用している。Xネットサービスの送金時の利用手順を図1に示す。



注記　法人利用者の使用するクライアント証明書に対応する秘密鍵は，エクスポートできない状態でPCにインストールされる。

図1　Xネットサービスの送金時の利用手順

〔マルウェア対策〕

ある日，情報セキュリティ対策機関から，ネットバンキングを悪用するマルウェア（以下，マルウェアJという）への注意喚起が発表された。そこで，Xネットサービス事業部のセキュリティ担当のW主任は，Xネットサービスへの影響について調査した。マルウェアJに感染したPCでXネットサービスを利用した場合の動作を，図2に示す。

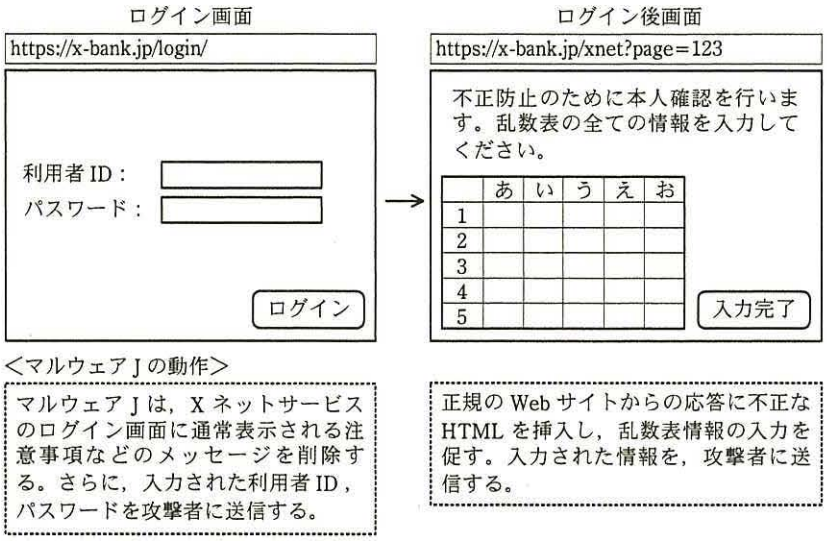


図 2　マルウェア J に感染した PC で X ネットサービスを利用した場合の動作

W 主任は，注意喚起の内容を確認した後，X ネットサービスが狙われた場合のリスクを上司の G 部長に説明した。次は，その時の W 主任と G 部長の会話である。

G 部長：この攻撃は，利用者 ID，パスワード，乱数表の情報（以下，併せて認証情報という）を盗もうとするものだが，利用者を①偽 Web サイトに誘導するものではないね。マルウェア J に感染した PC で，正規の Web サイトにアクセスすると，マルウェア J が，認証情報を盗むために邪魔なメッセージを削除し，偽の乱数表情報入力画面を表示するものだね。

W主任：そのとおりです。利用者は，マルウェア J が不正な画面を表示していることに気付かず，認証情報を入力してしまうようです。

G 部長：②法人利用者については，利用者 ID，パスワードを盗まれたとしても，金銭的な被害が発生する可能性は低いね。

W主任：はい。しかし，個人利用者の場合は，金銭的な被害が発生する可能性が高いと考えられます。

G 部長：それでは，利用者の PC がマルウェア J に感染したとしても，攻撃者に認証情報を盗まれないように，当行の Web サイト，電子メールで注意を促すことにしよう。

〔新たなマルウェア対策の検討〕

X 銀行がマルウェア J に対する注意を促した後，海外のネットバンキングで被害が発生したとされるマルウェア（以下，マルウェア K という）への注意喚起が，海外の情報セキュリティ関連 Web サイトに公開された。この情報を基に，W 主任は，マルウェア K に感染した PC で X ネットサービスを利用した場合の動作をまとめ，G 部長に報告した。この動作を，図 3 に示す。

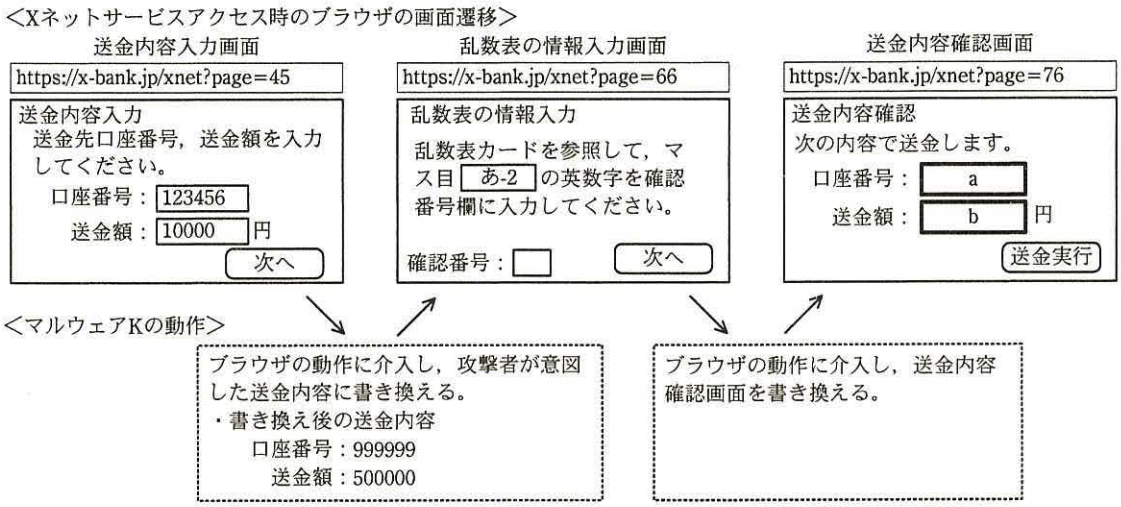


図 3　マルウェア K に感染した PC で X ネットサービスを利用した場合の動作

次は，マルウェア K に関して W 主任が G 部長に報告した際の会話である。

W 主任：海外では，利用者が入力した送金内容をマルウェア K が書き換えて，攻撃者の口座に送金するという被害が発生したそうです。

G 部長：そうか。X ネットサービスでの対策はどうするのだ。

W 主任：動作をまとめたところ，マルウェア K の挙動は，ブラウザとサーバとの通信経路上に攻撃者が割り込んで通信を中継する中間者攻撃と同じようです。X ネットサービスでは中間者攻撃への対策として，サーバ証明書を使用しています。中間者攻撃であれば，新たな対策は不要だと思います。

G 部長：確かに，例えば，利用者が使用している DNS サーバを攻撃することで，x-bank.jp へのアクセスを偽 Web サイトに誘導して行われる中間者攻撃であ

れば，③最新のブラウザを使っている利用者は攻撃に気付くことができる。しかし，マルウェア K は，通信経路上に介在するわけではないな。この攻撃は Man-in-the-Browser と呼ばれている攻撃手法だから，利用者は気付くことができないよ。

W 主任：分かりました。更に調べて，マルウェア K による不正送金を防ぐためのセキュリティ対策について検討します。

〔セキュリティ対策の再検討〕

W 主任は，まず国内外のネットバンキングで採用された実績があるセキュリティ対策を調査した。その上で，現在，X ネットサービスで採用している認証方式と，調査したセキュリティ対策について，マルウェア J，マルウェア K のそれぞれに効果がある対策という観点から評価を行った。X ネットサービスで新たに採用を検討したセキュリティ対策を表 1 に，現在 X ネットサービスで採用している認証方式も含めた評価結果を表 2 に示す。

表 1　採用を検討したセキュリティ対策

名称	方式
ワンタイムパスワード認証	認証のたびに，要求するパスワードが変わる方式。入力すべきパスワードは，専用デバイスに表示される。
リスクベース認証	通常と異なる環境からログインしようとした場合などに，あらかじめ利用者が登録しておいた合言葉を追加で入力させる方式。
送金内容認証	送金内容に対して，メッセージ認証コードを用いる方式。利用者とネットバンキングの Web サイト間で，利用者ごとの鍵（以下，共通鍵という）を設定した HMAC 計算ツールをあらかじめ共有しておく。利用者がネットバンキングで送金するときは，HMAC 計算ツールに送金先口座番号及び送金額を送金内容として入力し，HMAC 計算ツールで計算した結果（以下，HMAC 値という）も Web サイトに送信する。Web サイトでは，利用者側で計算した HMAC 値と，送信された送金内容から Web サイト側で計算した HMAC 値を比較することによって，送金内容が改ざんされていないか検証を行う。

表2　セキュリティ対策の評価結果

項番	セキュリティ対策	マルウェアJの感染に起因する不正送金への対策としての評価	マルウェアKの感染に起因する不正送金への対策としての評価
1	利用者ID・パスワード認証	対策にならない	対策にならない
2	クライアント証明書による認証	対策になる	対策にならない
3	乱数表による認証	対策にならない	対策にならない
4	ワンタイムパスワード認証	c	対策にならない
5	リスクベース認証	対策になる	対策にならない
6	送金内容認証	d	対策になる

注記　利用者は，マルウェアJ，マルウェアKの感染に気付くことができないことを前提とする。

表2の評価結果から，マルウェアKに感染したPCの不正送金対策として有効なのは，項番6であることが分かった。また，項番1と項番4の認証を組み合わせた［ e ］認証といわれる認証方式の評価も行ったが，マルウェアKに感染したPCの不正送金対策にはならなかった。G部長は，マルウェアKが進化し，更に手口が巧妙化することも考えられるので，④HMAC計算ツールをPC用のプログラムではなく，専用デバイスの形態で利用者に提供することを検討するよう，W主任に指示した。

Xネットサービスとしては，利用者に，PCのOSのセキュリティパッチ適用の徹底や，ウイルス対策ソフトの導入とウイルス定義ファイルの更新の徹底を促すとともに，新種のマルウェアの情報を継続して提供していくことにした。あわせて，“送金内容認証”の提供準備を進めることにした。

設問1　〔マルウェア対策〕について，(1)，(2)に答えよ。

(1)　本文中の下線①のようなWebサイトの一般的な総称を，10字以内で答えよ。

(2)　本文中の下線②の理由を，Xネットサービスにおける法人利用者の利用手順に着目し，35字以内で述べよ。

設問2　〔新たなマルウェア対策の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線③について，利用者はどのようにして攻撃に気付くことができるか。35字以内で述べよ。

(2)　図3中の［ a ］，［ b ］に入れる適切な口座番号と送金額をそれぞれ答えよ。また，マルウェアKが，送金内容確認画面を書き換える目的を，

35字以内で述べよ。

設問3 〔セキュリティ対策の再検討〕について，(1)～(3)に答えよ。

(1) 表2中の［ c ］，［ d ］に入れる適切な評価を“対策になる”又は“対策にならない”で答えよ。

(2) 本文中の［ e ］に入れる適切な字句を，5字以内で答えよ。

(3) 本文中の下線④について，HMAC 計算ツールを，PC 用のプログラムの形態で提供したときのセキュリティ上の問題点を，55字以内で述べよ。

〔 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。