問1　脆弱性検査の結果とその後の対策に関する次の記述を読んで，設問1～3に答えよ。

A社は，衣料品を取り扱う会員制インターネット通販会社である。A社では，セキュリテイ専門会社のB社に依頼して，Webアプリケーションの脆弱性検査を，年に4回定期的に実施している。検査を実施した結果，会員の属性情報の登録，変更などを行う会員情報管理システム（以下，Pシステムという）において，指摘事項が2件報告された。

A社情報システム部のX部長は，指摘事項の確認と対策の検討を，Y主任に指示した。

〔脆弱性検査の結果〕

Y主任は，早速，B社の検査担当者から，指摘事項2件についての詳細な説明を受けた。

指摘事項A：画面の遷移の中で，暗号化通信と非暗号化通信が混在しているが，暗号化通信でだけ使用されるべきクッキーに，［　a　］属性が設定されていないページが存在する。

指摘事項B：任意のスクリプトが実行可能であるページが存在する。

説明に当たってB社からは，指摘事項Aを検出したときのログイン操作直後のHTTPレスポンス（図1），指摘事項Bを検出したときに使用されたHTTPリクエスト（図2）と，図2のHTTPリクエストに対するHTTPレスポンス（図3）が示された。検査においてフォーム認証に使用した会員H）とパスワードは，検査のために用意されたものである。

```
HTTP/1.1 200 OK
Date: Sun, 01 Apr 2012 12:00:00 GMT
Set-Cookie: JSESSIONID=0C3FE1B62D5B5A5DE5A06E5D5C23F6F9
（以下，省略）
```

図1　指摘事項Aを検出したときのログイン操作直後のHTTPレスポンス

```
GET /mypage/progA?PID=xx&QTY=yy"><script>alert("script")</script> HTTP/1.1
Host: www.a-sha.co.jp
Cookie: JSESSIONID=0C3FE1B62D5B5A5DE5A06E5D5C23F6F9
Referer: http://www.a-sha.co.jp/prog0
（以下，省略）
```

図2　指摘事項Bを検出したときに使用されたHTTPリクエスト

```
HTTP/1.1 200 OK
（中略）
<form name="form" method="post" action="/mypage/progB">
    <table>
    <tr>
      <th>商品 ID</th>
      <td><input type="text" name="PID" value="xx" ></td>
      <th>個数</th>
      <td>
        <input type="text" name="QTY" value="yy"><script>alert("script")</script>">
      </td>
    </tr>
    </table>
（以下，省略）
```

図３　図２の HTTP リクエストに対する HTTP レスポンス

Y 主任は，提示された図 1～3 の内容を手掛かりに，対象のプログラムのソースコードを調査し，指摘事項 A と指摘事項 B が P システムにおいて，脆弱性といえるものであることを確認した。

〔脆弱性の影響の検討〕

続いて Y 主任は，脆弱性の影響について検討を行った。まず，今回の指摘事項 A と指摘事項 B に対して，どのような攻撃があり得るか，また，その攻撃を受けた場合，どのような被害が予想されるかについて検討を行った。検討結果の抜粋は，表 1 のとおりである。

表１　予想される攻撃と被害（抜粋）

指摘事項	予想される攻撃	予想される被害
A	クッキーに含まれるセッション ID が，非暗号化通信時に盗聴される。	盗聴されたセッション ID が使用され，セッションが乗っ取られる。
B	HTTP リクエストに挿入されたスクリプトが，ブラウザ上で実行されることで，クッキー内のセッション ID が窃取される。	窃取されたセッション ID が使用され，セッションが乗っ取られる。

さらに，Y 主任は，これまでに表 1 の攻撃及び被害が実際に起きているかどうかを，ログから確認することにした。

指摘事項 A で予想される攻撃である，セッション ID の盗聴については，ログから検出することは困難である。次善の策として，盗聴されたセッション ID が不正に使用されたことを検出するために，同一のセッション ID が，複数の送信元 IP アドレスから送信されているリクエストをログから抽出することにした。この方法では，①正当なアクセスを誤って検出してしまう場合と，②不正なアクセスを捻出できない場合があるが，それらの場合については容認することにした。

指摘事項 B に対する攻撃は，③HTTP アクセスログから検出することにした。ただし，この方法では［　b　］メソッドが使用された場合にしか検出できない。

以上の方法で過去のログを確認したところ，不正使用や攻撃は検出されなかった。

〔改修方法の検討〕

Y 主任は，脆弱性への対応を行うために，まず，指摘事項 B に該当する複数のプログラムのソースコードを再度確認した。該当するプログラムの一つを図 4 に示す。

```
01: import java.io.*;
02: import java.util.*;
03: import javax.servlet.*;
04: import javax.servlet.http.*;
05:
06: public class SearchWord extends HttpServlet {
07:    public void doGet(HttpServletRequest request, HttpServletResponse response)
08:    throws IOException, ServletException {
09:
10:       response.setContentType("text/html;charset=UTF-8");
11:       PrintWriter out = response.getWriter();
12:
13:       String word = request.getParameter("word");
14:       String category = request.getParameter("category");
```

図 4　指摘事項 B に該当するプログラム

```
15:
16:       out.println("<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML4.01 Transitional//EN\">");
17:       out.println("<html>");
18:       out.println("<head>");
19:       out.println("<meta http-equiv=\"Content-Type\" content=\"text/html; charset= utf
   -8\">");
20:       out.println("<title>Search</title>");
21:       out.println("</head>");
22:       out.println("<body>");
23:       out.println("<h3>Search</h3>");
24:       out.println("<form action=\"searchWord\" method=\"GET\">");
25:       out.println("word<br>");
26:       out.println("<input type=\"text\" size=\"10\" name=\"word\">");
27:       out.println("<br>");
28:       out.println("category(option)<br>");
29:       out.println("<input type=\"text\" size=\"10\" name=\"category\">");
30:       out.println("<br>");
31:       out.println("<input type=\"submit\">");
32:       out.println("</form>");
33:
34:       out.println("<br>");
35:       out.println("- - results - - category: " + escape(category) + "<br>");
36:
37:       out.println("<a name=\"#\" onclick= \"alert('" + escape(word) + "')\">");
38:       out.println("Previous search word" );
39:       out.println("</a>");
40:
41:       if (word != null) {
42:         searchResult(out, word, category);
43:       }
44:       out.println("</body>");
45:       out.println("</html>");
46:    }
47:
48:    public void doPost(HttpServletRequest request, HttpServletResponse response)
49:    throws IOException, ServletException {
50:       doGet(request, response);
51:    }
52:
53:    private static String escape(String message) {
54:       //  この関数は，message に含まれる文字を次のように置換した String 型の文字列を返す。
55:       //  「&」→「&amp;」  「<」→「&lt;」  「>」→「&gt;」  「"」→「&quot;」
56:       (省略)
57:    }
58:
59:    private void searchResult(PrintWriter out, String word, String category) {
60:       //  検索を実行し，結果を表示する。
61:       (省略)
62:    }
63: }
```

図４　指摘事項Ｂに該当するプログラム（続き）

このプログラムは，利用者が入力した文字列をダイアログに表示するために，受け取ったパラメタの値をスクリプトに埋め込み，動的にスクリプトを生成する。図４の［ c ］行目では，通常の HTML にパラメタの値を埋め込むときと同じ方法で，

エスケープ処理を行っていたことから，生成されるスクリプトに問題が生じてしまうことが分かった。

Y 主任は，以上の検討結果から，指摘事項 A と指摘事項 B に対する改修方針を，表 2 のとおりにまとめた。

表 2　指摘事項に対する改修方針

指摘事項	改修方針
A	暗号化通信でだけ使用するクッキーに［ a ］属性を設定する。
B	出力するときの文脈に合わせたエスケープ処理を行う。

特に，表 2 中の指摘事項 B の改修方針を実現するために，図 4 の［ c ］行目の escape 関数呼出しを，新たに作成する escape2 関数（図 5）呼出しに変更することにした。escape2 関数では，意図したスクリプトが生成されるように，まず，スクリプト言語の文法上必要なエスケープ処理を行った後，更に escape 関数でエスケープ処理を行う。

```
private static String escape2(String message) {
  //  この関数は，message に含まれる文字を次のように置換した String 型の文字列を生成し，
  //  その文字列を escape 関数に渡し，その結果の String 型の文字列を返す。
  //  「［ d ］」→「［ e ］」  「［ f ］」→「［ g ］」
  (省略)
}
```

図 5　新たに作成する escape2 関数

その後，Y 主任は，X 部長の承認を得た上で，改修作業を行い，脆弱性検査結果についての対策を完了した。

設問 1　本文中と表 2 中の［ a ］と，本文中の［ b ］に入れる適切な字句を，それぞれ 8 字以内で答えよ。

設問 2　〔脆弱性の影響の検討〕について，(1)～(3)に答えよ。

(1)本文中の下線①について，正当なアクセスを誤って検出してしまう場合とはどのような場合か。40 字以内で具体的に述べよ。

(2)本文中の下線②について，不正なアクセスを検出できない場合とはどのような場合か。40 字以内で具体的に述べよ。

(3)本文中の下線③について，どのような条件のログを検出すればよいか。35 字以内で具体的に述べよ。

設問 3　〔改修方法の検討〕について，(1)，(2)に答えよ。

(1)本文中の［ c ］に入れる適切な行番号を一つ数字で答えよ。

(2)図 5 中の［ d ］～［ g ］について，［ d ］，［ f ］には置換の対象文字を，［ e ］，［ g ］には置換後の文字列を，それぞれ答えよ。

問2　Webアプリケーション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。

O社は従業員数20名のインターネット通販会社であり，通販サイト（以下，Xサイトという）で会員向けに化粧品を販売している。Xサイトは O社が開発し，運用している。

ある日，会員からの問合せがあり，Xサイトで管理している会員の個人情報が流出していることが判明した。O社は，被害拡大防止のためにXサイトを一旦停止した上で，流出件数，原因などを明らかにするために，情報システム担当者であるVさんから，セキュリティ専門会社D社のS氏に調査を依頼した。

S氏は，Vさんから Xサイトのシステム構成を聞いた後，関係するログを調査した。

Xサイトでは，会員ID及びパスワードを，データベースの m_user テーブルの cust_id 及び pwd という列にそれぞれ格納しており，ログイン機能（1ogin.cgi プログラム）では cid，pw という引数とデータベースに格納されている値を照合している。表1は，Webサーバの HTTP アクセスログのうち不正アクセスに関連する部分の抜粋であり，左から順に，便宜上付けた番号，クライアントの IP アドレス，HTTP のアクセスメソッド，cgi プログラム名，クエリ文字列である。

〔調査結果〕

S氏が表1の HTTP アクセスログを調査した結果，次の攻撃が判明した。

・攻撃1:IP アドレスが［　a　］の攻撃者が，［　b　］.cgi に対し SQL インジェクションによって全会員分に当たる約8,000件の会員ID及びパスワードを窃取していた。

・攻撃2 : SQL インジェクションによって Xサイトのデータが改ざんされ，その後アクセスした会員の PC にマルウェアを強制的にダウンロードさせられていた。（表1中の20番）

・攻撃3 : SQL インジェクションによってデータが改ざんされ，会員ID及びパスワードを詐取されていた。（表1中の22番）

・攻撃4 : 不正ログインを試行されていた。

S氏は，調査結果をVさんに説明した。次は，そのときの会話の一部である。

Vさん：攻撃2ですが，IP アドレスが ipJ の攻撃者（以下，攻撃者 ipJ という）によって，画面の一部であるバナーとして表示されるデータ（ban_url）が改ざんされていたということですね。Xサイトにアクセスした一部の会員から“ウイルス対策ソフトが警告を表示する”という問合せがあったのは，それが原因ですね。

S氏　：はい。会員が，改ざんされたデータを含む画面に表示されだ重要なお知らぜをクリックすると，攻撃者 ipJ が用意した外部サイトに誘導されて，ブラウザが誘導先ページのコンテンツと一緒に，不正な動作を引き起こすファイルをダウンロードします。それから，そのファイルが，ブラウザの［　c　］で処理される過程で，ブラウザの［　c　］の脆弱性を突くコードを実行することで，PC が感染し，その後，別のファイルがダウンロードされます。もし途中で PC のウイルス対策ソフトが検知，駆除しなければ，最終的にはキーロガーとして存在していました。

表 1　Web サーバの HTTP アクセスログ（不正アクセスに関連する部分の抜粋）

番号	IP	メソッド	cgi	クエリ文字列 1)
1	ipA	GET	login.cgi	cid=yamada&pw=fajsl334
2	ipB	GET	login.cgi	cid=cust51&pw=password
3	ipC	GET	login.cgi	cid=tanaka&pw=p7g3dfb0
4	ipB	GET	login.cgi	cid=cust51&pw=pass
5	ipB	GET	login.cgi	cid=cust51&pw=cust51
6	ipB	GET	login.cgi	cid=cust51&pw=
7	ipC	GET	search.cgi	item=gf34' and select cust_id, pwd, null, null from m_user where '1' = '1&kind=09
8	ipB	GET	login.cgi	cid=cust51&pw=15tsuc
9	ipB	GET	login.cgi	cid=cust51&pw=a
10	ipB	GET	login.cgi	cid=cust51&pw=b
11	ipB	GET	login.cgi	cid=cust51&pw=c
12	ipD	GET	search.cgi	item=gf44' union select pwd, null, null, null from m_user where '1' = '1&kind=09
13	ipB	GET	login.cgi	cid=cust51&pw=d
14	ipE	GET	login.cgi	cid=cust01&pw=password
15	ipG	GET	confirm.cgi	cat=0217&iname=../ls |
16	ipE	GET	login.cgi	cid=cust12&pw=password
17	ipF	GET	search.cgi	item=gf36' union select cust_id, null, null, null from m_user where '1' = '1&kind=9
18	ipC	GET	confirm.cgi	cat=1127&iname=tanaka><script>alert("test");</script>
19	ipE	GET	login.cgi	cid=cust33&pw=password
20	ipJ	GET	search.cgi	item=0b24';update m_contents set ban_url = ban_url || '">重要なお知らせ
21	ipH	GET	search.cgi	item=gf12' union select cust_id, pwd, null, null from m_user where '1' = '1&kind=09
22	ipI	GET	search.cgi	item=0b24';update m_contents set ban_url = ban_url || '"><script type="text/javascript" language="javascript">document.write("<html>（省略）</html>");</script>

注 1)　クエリ文字列は，URL デコード済である。

V さん：なるほど。では，攻撃 3 についても説明をお願いします。
S 氏　：攻撃 3 も同じくデータ改ざんによるものですが，攻撃 2 の後しばらくしてから攻盤を受けており、①攻撃 1 とは異なる手口で会員 ID とパスワードの詐取が試みられていました。

続いて S 氏は V さんに，攻撃 3 の具体的な手口や攻撃 4 のログの特徴についても説明した。

〔パスワード格納方法の検討〕

S 氏は V さんに，HTTP アクセスログの調査結果から判明した不正アクセスについて説明した後，SQL インジェクションに関係していた m_ user テーブルを調査して気付いたことを指摘した。次は，そのときの会話である。

S 氏：m_user テーブルを見ていて気付いたのですが，パスワードは暗号化されていますよね。どのような暗号アルゴリズムで暗号化しているのですか。
V さん：暗号アルゴリズムは自作しました。例えば，元の文字列が password の場合，まず，［　d　］式暗号で drowssap に変換し，次に，［　e　］式暗号で espxttbq に変換します。
S 氏　：そのアルゴリズムは変更すべきです。CRYPTREC(暗号技術評価プロジェク

ト)が電子政府推奨暗号リストに公開している暗号アルゴリズムと異なり，自作アルゴリズムは，［ f ］について公的な機関の評価を受けていないので推奨できません。

V さん：なるほど。それでは，修正を検討します。

S 氏　：それから，攻撃者が何度も会員登録した上で，攻撃者の指定したパスワードとそれに対する暗号文から解読する［ g ］攻撃によって会員のパスワードを解読された可能性が高いので，サイトの再開前に全会員のパスワードを初期化し，初期化する前のパスワードへの変更を禁止すべきです。

V さん：承知しました。会員にはパスワードを初期化したことを通知します。

S 氏　:それだけではなく，②初期化する前のパスワードが解読されている可能性が高いことも通知してください。

その他，S 氏は V さんに，改ざんされたデータの復旧方法や攻撃に対するプログラムの修正方法などを説明した。

O 社は，S 氏の指摘に従って，被害の状況や再発防止策などの情報を自社の Web サイトで公表した。その後，プログラム修正，パスワードの格納方法の改善などの対策を完了させ，全会員のパスワードを初期化して会員に連絡した上で，X サイトを再開させた。

設問 1　〔調査結果〕について，(1)～(3)に答えよ。

(1)本文中の［ a ］に入れる IP アドレスを一つ答えよ。

(2)本文中の［ b ］に入れる cgi プログラム名を 7 字以内で答えよ。

(3)表 1 に示されている IP アドレス ipB による攻撃は，ログを調査した結果，ある特徴から不正ログインの試行と判明した。その特徴について 35 字以内で述べよ。また，その不正ログイン試行対策を 35 字以内で述べよ。

設問 2　〔パスワード格納方法の検討〕について，(1)，(2)に答えよ。

(1)本文中の［ d ］～［ g ］に入れる字句をそれぞれ解答群の中から選び，記号で答えよ。

解答群

ア　DoS	イ　Exploit	ウ　安全性	エ　換字
オ　サイドチャネル	カ　辞書	キ　市場性	ク　選択平文
ケ　誕生日	コ　転置	サ　分散性	

(2)本文中の下線②について，初期化する前のパスワードへの変更を禁止する以外に，会員に通知する理由は何か。その理由を 50 字以内で述べよ。

設問 3　SQL インジェクションによるデータ改ざんについて，(1)，(2)に答えよ。

(1)本文中の［ c ］に入れる字句を 10 字以内で答えよ。

なお，会員の PC の OS 及びブラウザ本体への攻撃は実施されなかったものとする。

(2)本文中の下線①について，会員 ID 及びパスワードを詐取する方法を 50 字以内で具体的に述べよ。

問 3　保守作業の証跡確保のための対策検討に関する次の記述を読んで，設問 1～4 に答えよ。

M 社は，従業員数 900 名の保険会社である。M 社は損害保険業務を支援する保険システムを稼働させている。保険システムの利用者は，M 社の従業員である。M 社は，保険システムの開発をソフトウェア開発会社の Z 社に委託している。また，保険システムは M 社のグループ会社が運営するデータセンタ（以下，DC という）に設置し，主に M 社が運用と保守を行っているが，一部の保守作業については Z 社に委託している。保険システムは，20 台のサーバ（以下，保険サーバという）から構成されており，保険システムのサービス（以下，保険サービスという）を提供するための様々なソフトウェアが稼働している。保険システムの構成を図 1 に示す。

Z 社が請け負っている保守作業は，機能追加などに基づく保険システムのプログラムモジュールの更新，保険システムに障害が発生した場合の原因調査，本番システムへの設定変更などの作業が主である。Z 社は M 社から作業依頼書を受け取ると，保険システムを担当する 5 名の保守チームの中から当該作業担当者を 1 名選び，作業担当者氏名や作業期間などを記載した作業計画書を M 社に提出する。作業計画が承認されると，作業で使用するために，OS の特権 ID が使用可能な状態に有効化され，通知される。特権 ID とは，OS に対する全てのシステム管理特権を付与された利用者 ID のことである。作業担当者は通知された特権 ID を使い，Z 社 PC から保険サーバにリモートアクセスを行って作業を実施する。Z 社内の M 社保険システム保守用 LAN，M 社 LAN 及び DC 内の DCLAN は IP-VPN で接続されている。

なお，DC 内の保険サーバのコンソールからの操作や電源の操作は，M 社が実施している。また，保険サーバやネットワーク機器の時刻は全て同期している。

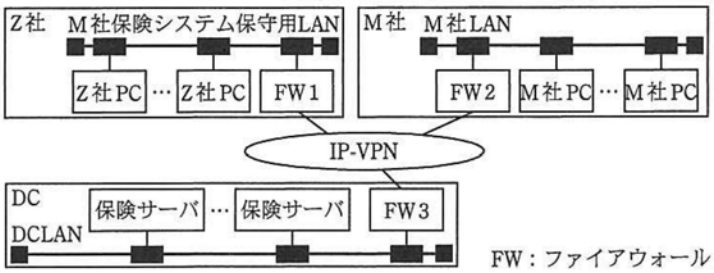

図 1　保険システムの構成

〔対策の検討と対策方針の策定〕

M 社の同業の C 社で情報漏えい事件が起きた。C 社の保守作業委託先の従業員が，保険加入者のデータを不正に持ち出して名簿業者に売却したと報じられた。事件は，C 社が事態をすぐに把握できなかった管理上の不備に対する指摘とともに，連日報道された。M 社の経営幹部は，C 社の事件をきっかけに，自社の保険システムにおいても同様の問題が起きる可能性はないか早急に調査するよう，情報システム部長に指示を出した。調査の結果，保険システムについても，Z 社の保守作業において，保険加入者の情報が保存されたファイル（以下，機密ファイルという）が，作業依頼書に指定した範囲を超えてアクセスされるおそれがあることが指摘された。そこで，情報システム部の L 主任がリーダとなり，対策を検討することになった。

検討を開始した当初は，Z 社の保守作業において機密ファイルへのアクセス制御を実施する案も出たが，M 社保守担当者から，特権 ID の運用が複雑になる上，保守作業には緊急性が求められる場合もあり，現実的な対策ではないといった意見があった。

そこで，①L 主任は Z 社の作業担当者の保守作業の作業証跡を取得し，作業内容とは無関係な機密ファイルの操作（以下，機密ファイル操作違反という）を検知する仕組みを備えるという対策方針を立てた。本対策方針は経営幹部に報告された後，M 社役員会議で承認された。

L 主任は，Z 社が行う作業の操作ログを取得し，操作ログから Z 社の機密ファイル操作違反の可能性を自動検知する対策がよいと考えた。検知後に，作業者の機密ファイル操作違反前後の一連の操作を追跡することを想定した対策である。

〔対策実現に向けた要件と実現方式の検討〕

L 主任は部下の N 君に次の三つの要件を示した上で，実現方式の検討を指示した。

要件 1：保険サーバで Z 社の作業担当者が行うファイル操作を，ログサーバに記録できること

要件 2：特定のファイルのアクセスや，特定のプロセスの起動と停止などの検知ルールをあらかじめ定義でき，操作ログ上で検知ルールに一致したファイル操作ログが見つかったときに，管理者に通知できること

要件 3：操作ログの取得を実現する上で，保険サービスの可用性に影響を与えないこと

N 君は，操作ログが取得可能な製品の中でシェアの高い二つの市販ソフトウェアパッケージ製品 PP1，PP2 を候補とし，それぞれのパッケージ製品を利用した対策実現方式案（以下，それぞれ案 1，案 2 という）を表 1 のとおり取りまとめて，L 主任に報告した。

〔実現方式案の要件の確認〕

L 主任は最初に，案 1，案 2 が要件を満たしているかどうかを確認した。L 主任は，案 1 は，ログサーバがダウンしている場合，及び②作業担当者が保険サーバのネットワーク設定を不正に変更して操作ログの転送を妨害した場合において，③その後，作業担当者がある操作を実行すると，その前後のファイル操作について要件 1 及び要件 2 が満たされなくなると指摘した。

要件 3 については，L 主任は，特に案 1 について，保険サーバ内の [a] と既存ソフトウェアとの間で相互に悪影響を及ぼさないか，十分なテストを実施する必要があると考えた。

表1　案1及び案2の実現方式概要

案1	案2
・PP1を採用する。 ・操作ログを取得する各保険サーバにPP1のエージェントモジュールをインストールする。 ・ログサーバをDCLANに設置し，PP1のメインモジュールをインストールする。 ・Z社の保守作業におけるリモートアクセス手順に変更はない。 ・エージェントモジュールが取得するログ項目は，利用者ID，時刻（保険サーバの時刻）及び次のいずれかである。 (a) 実行されたコマンド (b) 操作対象ファイル名と操作（参照，コピー，更新，削除） (c) アプリケーションの起動と終了（エージェントモジュールの起動と停止も含む） ・PP1（メインモジュールとエージェントモジュール）の起動と停止には，インストールされているサーバの特権IDが必要である。 ・ログサーバはM社が管理する。 ・操作ログは，Z社の作業担当者が保険サーバにログインしてからログアウトするまでの間，取得する。	・PP2を採用する。 ・DCLANに中継サーバを設置し，中継サーバにPP2をインストールする。 ・操作ログは中継サーバで取得する。 ・ログサーバをDCLANに設置する。 ・Z社の保守チームには，担当者ごとに中継サーバの利用者IDを付与する。 ・Z社の保守作業におけるリモートアクセス手順は，リモートデスクトップ接続を行い中継サーバに一旦ログインして，さらにリモートアクセスを行い，各保険サーバにログインするように変更する。 ・取得するログ項目は，保険サーバの利用者ID，時刻（中継サーバの時刻）及び次のいずれかである。 (a) 保険サーバで実行されたコマンド (b) 保険サーバでの操作対象ファイル名と操作（参照，コピー，更新，削除） (c) 保険サーバでのアプリケーションの起動と終了 (d) Z社PCに表示されるリモートデスクトップ先（中継サーバ）のウィンドウ画面のスナップショット画像 ・中継サーバの利用者IDごとに，保険サーバへのリモートアクセスの許可と拒否の制御ができる。 ・PP2の起動と停止には，中継サーバの特権IDが必要である。 ・中継サーバ及びログサーバはM社が管理する。 ・操作ログは，Z社の作業担当者が中継サーバにログインしてからログアウトするまでの間，取得する。
・操作ログは，保険サーバ又は中継サーバで暗号化してログサーバに転送する。ただし，何らかの理由でログサーバに転送できない場合は，暗号化して，保険サーバ又は中継サーバのローカルディスクに一時保管し，定期的にログサーバへの転送をリトライする。 ・PP1，エージェントモジュール，PP2を停止させた場合，停止操作の操作ログがログサーバに転送された後に停止動作が実行される。 ・ログサーバ上の操作ログは付属する専用ビューアで閲覧する。 ・ログサーバ上の操作ログについては，機密ファイル操作違反の隠蔽防止のために，④メッセージダイジェストを使用した［　b　］機能をもつ。 ・保守作業を幾つかのパターンに分類し，パターンごとに作業内容に関係のある機密ファイルを決定し，検知ルールを定義しておく。そうすると，Z社の作業担当者が保守作業中に作業依頼書に指定した範囲を超えて機密ファイルにアクセスした場合，ログサーバでは転送された操作ログの記録内容を基に，あらかじめ指定されたメールアドレス宛てに電子メールを送信する。	

〔要件以外の比較検討〕

次に，L主任は要件以外の点についても検討を進めた。案1は導入に特に大きな支障はないと考えられた。

一方で案2は，中継サーバが導入されることから，Z社の作業担当者の作業手順や，

保険サーバなどのアクセス制御を見直す必要がある。例えば，案2を実現するには，［ c ］から保険サーバへのアクセスは禁止するが，［ d ］やM社PCからのアクセスは許可する必要がある。

また，案2の場合は，中継サーバを利用するための利用者IDの付与と，保守作業ごとの各保険サーバの特権IDの通知の2点の実施方法を考慮する必要がある。

しかし，L主任は，案2の場合，中継サーバの利用者IDをZ社の保守チームの担当者ごとに作成するので，保守作業を作業計画書に記載された作業担当者だけに限定するという，より安全な仕組みが実現できると考えた。

〔対策の実施〕

L主任は，以上の確認と比較検討の結果，Z社の作業担当者の作業手順が変わる点などの不都合があるものの，要件を実現する上で案2の方が優れていると判断し，案2を選択することにした。その上で，保守作業の証跡を取得するためのシステム化計画を取りまとめ，経営幹部に報告し，M社役員会議で承認を受けた。その後，システム化作業を行い，対策を実施した。

設問1　ログサーバ上の操作ログの安全な保管について，(1)，(2)に答えよ。

(1)表1中の［ b ］に入れる適切な字句を答えよ。

(2)表1中の下線④について，最も適切と考えられるアルゴリズムはどれか。解答群の中から選び，記号で答えよ。

解答群

ア　AES　　イ　SHA-1　　ウ　SHA-256　　エ　Triple DES

設問2　案1及び案2の実現方式について，(1)，(2)に答えよ。

(1)本文中の［ a ］に入れる適切な字句を，表1中の用語を用いて答えよ。

(2)本文中の［ c ］，［ d ］に入れる適切な機器名を，それぞれ図1中又は表1中の用語で答えよ。

設問3　操作ログのセキュリティについて，(1)～(3)に答えよ。

(1)本文中の下線③のある操作とは，どのような操作か。30字以内で述べよ。

(2)案1について，本文中の下線②のような操作ログの転送を妨害した上で行う方法以外に，z社の作業担当者が保険サーバで，どのような操作を行うことによって，要件1の実現を妨害できるか。25字以内で述べよ。

(3)上記(2)の操作をM社が検知するための，案1の機能を用いた有効な手段を35字以内で述べよ。

設問4　M社のセキュリティについて，(1)，(2)に答えよ。

(1)本文中の下線①の対策方針を実現することによって，Z社の作業担当者の機密ファイル操作違反を検知することができる。さらに機密ファイル操作違反を抑止することを効果的に行うためには，M社は何を実施すべきか。40字以内で述べよ。

(2)案2について，作業計画書に記載された作業担当者だけが特権IDを利用できるようにするために作業計画ごとに設定する制御を，60字以内で述べよ。

問4　情報セキュリティ技術者の育成に関する次の記述を読んで，設問1～4に答えよ。

K 社は，従業員数 9,000 名の機械製造会社であり，本社の他，全国に工場が 8 か所，営業所が 10 か所ある。図 1 に示すとおり，K 社には本社，工場及び営業所を接続した社内ネットワークが構築されており，全社でサーバが 200 台，PC が 5,000 台接続されている。社内ネットワーク，サーバ及び PC の運用管理は，主として本社に勤務する情報システム部員が担当しているが，各工場にも情報システム部員を配置して，現地でなければ実施できない運用管理を行っている。

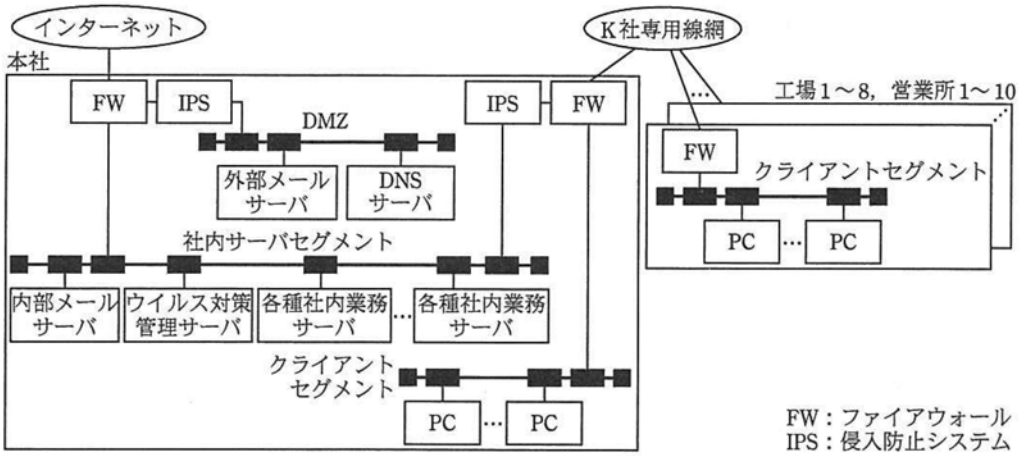

図 1　K 社ネットワーク全体構成図

全ての PC にはウイルス対策ソフトが導入されており，図 1 中のウイルス対策管理サーバは，このウイルス対策ソフトの管理とウイルス定義ファイルの配信を行っている。ウイルス対策ソフトはウイルス定義ファイルに基づきパターンマッチングによってウイルスを検出するものであり，ウイルス定義ファイルは最低でも 1 日に 1 回は更新されている。

〔K 社の情報セキュリティ対策の現状〕

K 社では過去に多くの情報セキュリティインシデントが発生しており，そのうちの幾つかは K 社の製品に関する機密情報の窃取を狙ったものと推測されている。K 社ではこの事態を重くみて，2 年前，総務部内に総員 10 名の情報漏えい対策チーム（以下，P チームという）を常設組織として設置し，文書，口頭，ネットワークなど，全ての経路での情報漏えいの予防及び情報漏えい発生時の緊急対応を実施してきた。この P チームは，幾つかの班に分かれており，そのうちの技術班のリーグが T 主任である。

〔標的型攻撃への対策の検討〕

T 主任は，K 社を取り巻く最近の状況から，悪意あるプログラムを電子メール（以下，メールという）の添付ファイルとして送付してくる攻撃に注意が必要であると考えていた。特に，①メール本文やタイトルに K 社に関連した内容が含まれるなど高度な偽装が施されており，かつ，②新たに作成された悪意あるプログラムを含んだファイルが添付されている，いわゆる標的型攻撃メールに対して危機感を持っており，その対策について検討を始めていた。

検討を進める中で T 主任は，セキュリティコンサルティング会社から，標的型攻撃に対応する演習のための教材一式を入手することができた。その教材には，実際に標的型攻撃に使用されたメール及び攻撃用プログラムを基にした，メール本文例及び疑

似攻撃プログラムであるプログラムSが含まれていた。教材は，演習用環境で不正な通信が発見されてから，その通信が発生した原因を突き止めるまでの演習を対象範囲にしている。T主任は，この教材を利用してPチーム内で標的型攻撃に対応する演習を行い，その結果に基づいてインシデント対応方法の改善を目指すことにした。

〔標的型攻撃に対応する演習の準備〕

T主任は演習の対象者として，Pチーム内で1年間ほどインシデント対応を担当しているU君を選抜した。この演習に当たって，T主任は図2に示す演習用環境を構築した。

なお，この演習用環境は他の全てのネットワークから切り離されている。

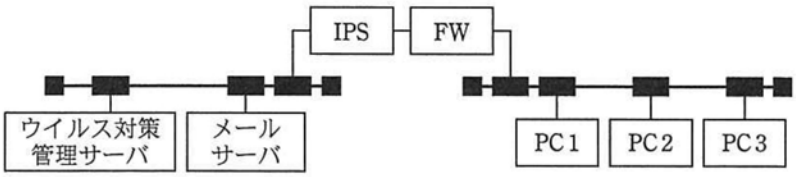

図2　演習用環境

また，インシデント対応において必要になる可能性が高いと考えて，図2の環境とは別にパケットキャプチャ装置を用意して解析用の隔離環境を整えた。

T主任は，演習用環境内のPC1が標的型攻撃に遭遇した状況を作るために，図3に示す準備を行った。演習に使用したプログラムSの動作は図4のとおりであった。ただし，図3及び図4の内容はU君には知らせなかった。

(1)　教材のメール本文例を参考に，K社に関連した内容を含んだ標的型攻撃用メールを作成した。
(2)　標的型攻撃用メールには，プログラムSを添付した。プログラムSは実行形式であるが，受信者のメールソフト上では文書形式ファイルのアイコンが表示されるように偽装している。
(3)　標的型攻撃用メールを，PC2 からメールサーバ経由で PC1 の利用者のメールアドレス宛てに送信した。送信に当たっては社内の実在するメールアドレスからの送信であるように偽装した。
　なお，他のメールも100通ほど送信し，標的型攻撃用メールが他のメールに紛れるようにした。
(4)　各 PC にはウイルス対策ソフトを導入した。さらに，演習で用いるウイルス定義ファイルを使用した場合でも，プログラムSがウイルスとして検出されないことを確認した。
(5)　プログラムSが動作する際の通信が，IPSによって不正な通信として検出されることを確認した。
(6)　演習の開始直前に PC1 にログインしてメールを受信し，メールの添付ファイルであったプログラム Sを実行した。

図3　演習の準備

(1) 実行すると，利用者に気づかれないようにPCに常駐する。
(2) 自セグメント及び近隣のセグメントに接続されたコンピュータにアクセスを試みる。その際に，相手のコンピュータのセキュリティホールを利用する。
(3) (2)でアクセスに成功したらファイルの取得を試みる。ファイルが取得できたら，そのファイルを攻撃者のメールアドレスに送信する。
(4) 他のコンピュータに自身をコピーして，常駐させる。ただし，演習用なので，コピーする台数，世代数には制限を設けている。また，指定された期日を過ぎると動作を停止する。
(5) リムーバブルメディアが接続されたことを検知して，利用者に気づかれないように他のコンピュータへの感染経路として利用する。

図4　プログラムSの動作

〔標的型攻撃に対応する演習〕

演習用環境の準備を整えた後，T主任はU君に演習の開始を告げた。次は，その時の会話である。

T主任：それでは演習を開始します。この後IPSが不正な通信を検出するので，その検出をきっかけにインシデント対応を実行してみてください。
U君　：はい。本番だと思ってやってみます。
T主任：早速IPSで不正な通信が検出されたようですよ。

対応を開始したU君は，まずIPSによる不正な通信の検出結果を確認した後，ウイルス対策管理サーバ，FW及びIPSのログ分析を開始した。

FW及びIPSのログ分析の結果，U君はPC1からメールサーバに対して不審なアクセスが行われていると思われるログを発見した。次は，その時の会話である。

T主任：ここまでの演習で，標的型攻撃への理解は深まりましたか。
U君　：はい。ウイルスとしては検知されないんですね。こうなると，PC1に原因があるとは即座に絞り込むことができないので，IPSでの誤検知や送信元IPアドレスのIPスプーフィングの可能性も調べないといけませんね。
T主任：そうですね。ただ，PC1から不審なアクセスが行われている可能性があると分かった時点で，PC1を早めに切り離した方がよかったのではないでしょうか。

その後，U君はPC1を演習用環境から切り離す措置をとった。切り離したPC1は，解析用の隔離環境に接続し，PC1の解析を行った。2時間ほどしたところでU君が行き詰まっているのに気が付いたT主任は，U君に声を掛けた。

T主任：どうやら苦戦しているようですね。
U君　：解析用の隔離環境で行ったパケットキャプチャの結果全体と，パケットの送信元IPアドレスを見て，PC1から不正なTCP通信が行われていることは確認できたのですが，PC1でどのような悪意あるプログラムが動いているかが分かりません。起動中の常駐プログラム名の一覧を確認したのですが，正常なPCとの差異はありませんでした。
T主任：常駐プログラムに目を付けたのはいいけれど，プログラム名を見ただけでは十分とは言えませんね。プログラム名ぐらいは簡単に偽装できますよ。

U 君　：そうなんてすか。では，悪意あるプログラムを特定するには，何を糸口にすればよいのでしょうか。
T 主任：パケットキャプチヤの結果を分析すれば，不正な通信の詳細情報が分かります。その情報の中には，当然 TCP セッション情報が含まれていますよね。それが糸口になりませんか。
U 君　：なるほど。今の話で③悪意あるプログラムを特定する方法を思い付いたので解析作業に戻ります。
T 主任：ところで，本番のインシデントでは証拠保全の必要があります。 PC1 は重要な証拠であり保全の対象となるので，本来であれば PC1 の複製を使用して解析を行うことになります。今回は演習なので証拠保全の措置は省略しましたが，インシデント対応手順を考える上で証拠保全は必要な措置となるので覚えておいてください。
U 君　：はい，分かりました。

この後 U 君は，下線③の方法を使って悪意あるプログラムを特定し，さらに PC1 の利用者のメールアドレス宛てに到着したメールの中から不審な添付ファイルを見つけ出した。利用者がこの添付ファイルを実行したことによって悪意あるプログラムが常駐してしまい，他のコンピュータへの不正な通信を行っていたことを突き止めた。

〔演習の振返り〕
U 君　：今回は何とか不審な添付ファイルを見つけることができましたが，メール本文は総務部からの社内連絡を装っている上，送信元のメールアドレスも実在するものであり，添付ファイルのアイコン偽装以外は不審な点は一切見当たりませんでした。実際の状況を想定してみると，標的型攻撃は，発見が難しいものなんですね。
T 主任：そうなんです。この演習は他社で過去に起きた事例を参考にしたものです。だから，当社にもこの程度の攻撃があると想定しなければいけません。このような標的型攻撃による被害を未然に防ぐためには，全従業員への指導も併せて行っていく必要があるのです。

演習の後，U 君は従業員が社内ネットワーク上の PC で今回のような標的型攻撃メールを受信して添付ファイルを実行してしまった場合，どのような被害が発生するか，その被害への対応をどうすべきかを検討して，インシデント対応手順にまとめた。また，インシデント対応のため，PC を LAN から切り離して解析作業を行っている間に，その PC の利用者から内蔵ハードディスク内のファイルが欲しいと言われる可能性が高いと考えた。そこで，証拠保全が可能な方法によって PC を複製した後に，④複製した PC からファイルを取り出す手順をインシデント対応手順に記載した。さらに，インシデントを未然に防ぐための標的型攻撃対策を作成した。

その後，T 主任はインシデント対応手順及び標的型攻撃対策を承認し，P チーム内の正式ドキュメントとして発行した。標的型攻撃対策に基づき，P チームは全従業員に対して標的型攻撃に関する指導を行った。K 社では，このような対策の効果もあり，標的型攻撃による被害を未然に防ぐことに成功している。

設問 1　攻撃者が本文中の下線①及び下線②のような細工をする目的を，下線①につい

て 40 字以内，下線②について 30 字以内で述べよ。

設問 2　本文中の下線③の悪意あるプログラムを特定する方法とは何か。その方法を 50 字以内で述べよ。

設問 3　本文中の下線④について，ウイルス感染を広めることのないように，利用者が必要とするファイルを PC から取り出すにはどのような方法をとればよいか。その方法を 50 字以内で具体的に述べよ。ただし，取り出すべきファイルはウイルスに感染していないものとする。

設問 4　本文中の下線①及び下線②の特徴を持った標的型攻撃メールを受信した場合の被害を回避するためには，従業員にどのような指導を行えばよいか。添付ファイル付きメールの取扱いについて指導すべき内容を 40 字以内で述べよ。

解答例

問 1

《出題主旨》

Web アプリケーションの脆弱性検査の指摘事項に対する正しい対応策を問う。エスケープ処理では，出力する文脈に合わせた処理を行う必要がある。

本問では，特に，スクリプトを動的に生成する場合のセキュアプログラミングに関する知識を問う。

設問 l　a　secure
　　b　GET

設問 2　(1) 端末の IP アドレスがセッションの途中で変わるようなアクセスの場合
(2) 攻撃者と被害者が同一のプロキシサーバや NAT を経由してアクセスした場合
(3) クェリ文字列にスクリプトが含まれているログを検出する。

設問 3　(1) c　37
(2) ①　d　＼（バックスラッシュ）
　　e　＼＼（バックスラッシュ＋バックスラッシュ）　　①と②は順不同
②　f　’（シングルクォート）
　　g　＼’（バックスラッシュ＋シングルクォート）

問 2

《出題主旨》

Web システムに対する攻撃は非常に多いにもかかわらず，インシデントが発生した後のサーバ管理者又は運用者の対応は必ずしも万全とはいえない。

本問では，Web サーバのアクセスログを見て何か起きたのかを理解し，そのインシデントに関する適切な対応とセキュリティ対策を問題として取り上げた。

設問 1 (1) a　ipH
(2) b　search
(3) **特徴**　**同一 IP アドレスから**，　一つの会員 ID に対して様々なパスワードでログインを試みている。
　　対策　連続してログインに失敗した時は，その会員 ID をロックする。

設問 2 (1)　d　コ
　　e　エ
　　f　ウ
　　g　ク
(2) 他のサイトで同じ会員 ID，パスワードを使用している会員に対し，その変更を促す必要があるから

設問 3　(1) c　プラグイン
(2) 偽の入力画面を表示させ，そこに入力させた情報を攻撃者が用意したサイトに送信する。

問 3

《出題主旨》

近年，機密情報の漏えい時の調査や外部監査対応時の証跡提示などの目的から，IT システムの利用者のアクセスログだけでなく，操作内容を記録する企業が増えてきている。操作内容を記録する場合，その目的や対象利用者のアクセス権などを考慮しなければ，記録した内容の真正性に疑義が生じる可能性がある。

本問では，業務委託先作業担当者の操作内容の証跡確保を題材として，セキュリティ上の考慮点を問う。

設問 1　(1)　b　改ざん検知
(2)　ウ

設問 2　(1)　a　エージェントモジュつレ
(2)　c　Z 社 PC
d　中継サーバ

設問 3　(1)　保険サーバに一時保管された操作ログを削除する操作
(2)　エージェントモジュールを停止させる操作
(3) エージェントモジュールを停止させる操作を検知ルールに設定する。

設問 4　(1)　Z 社の保守チームに，操作ログを取得し，監視していることを伝える。
(2)　作業計画書に記載された作業担当者と一致する利用者 ID にだけ，中継サーバから保険サーバへのアクセスを許可する。

問 4

《出題主旨》

セキュリティ技術者が不足していると言われているものの，その育成については個々の現場に委ねられている状況が見受けられる。しかし，セキュリティ技術者の育成に当たっては演習などを通じた実践的な育成が重要である。

本問では，標的型攻撃という題材を取り上げつつ，現実に近いネットワーク環境での演習による技術者の育成について問う。

設問 1　**下線**①　メール受信者に正常なメールと誤認識させて添付ファイルを開かせるため
下線②　ウイルス対策ソフトで検出されることを防ぐため

設問 2　不正な通信の送信元 TCP ポート番号を基に，そのポートを使用しているプログラムを特定する。

設問 3　正常な OS で起動した他の PC に, 複製した PC のハードディスクを接続してファイルを取り出す。

設問 4　添付ファイルの安全が確信できない場合，電話などで送信者に送信の事実を確認する。

採点講評

問 1

問 1 では, Web アプリケーションの脆弱性検査の指摘事項への対応策について出題した。全体として正答率は低かった。

設問 2(1)(2)では，攻撃状況をログから解析する場合に，正当なアクセスと不正なアクセスを判別することが困難である具体的な状況を解答してほしかったが，正答率は低かった。特に(2)では，“IP アドレスを詐称しだとする解答が多かったが，本問での状況では IP アドレスの詐称は起き得ないことに気づいてほしかった。

設問 3(2)は，正答率が低かった。エスケープ処理はいつも同じようにすればよいものではなく，プログラムが満たすべき要件や，出力が渡される処理系によって，適切に処理しなければならない。エスケープ処理の本質をよく理解しておいてほしい。

問 2

問 2 では，Web アプリケーションに対する SQL インジェクション攻撃を受けた際のログ分析と，DB に格納されているパスワード情報を題材に，Web アプリケーションにおけるインシデント対応とセキュリティ対策について出題した。全体として正答率は低かった。

設問 1(1)は，正答率が低かった。表 1 のログを注意深く確認することで，窃取されていた会員 ID (cust_id)とパスワード(pwd)を select している ipH を選択できたはずである。(2)(3)は正答率が高く，不正ログイン試行とその対策であるアカウントロツクに対する理解は進んでいると思われる。

設問 2(1)の中で g(選択平文)については正答率が著しく低かった。基本用語については理解を確実にしておいてほしい。(2)も正答率が低かった。利用者は複数のサイトで同じ認証情報の組合せを使い回している場合が多い。二次被害拡大防止のためにも利用者にとって必要なアクションが取れるような通知を心がけてほしい。

設問 3(1)は, 外部サイトに誘導される場合にブラウザやそのプラグインの脆弱性を突かれるケースを題材にした。企業や組織内で頻発している事象であるので，誘導からマルウェアの感染とその後の活動までの仕組みを理解しておいてほしい。

問 3

問 3 では，委託先作業担当者の操作内容の証跡確保を題材として，操作ログを取得するパッケージソフトのセキュリティ上の考慮点について出題した。

設問 3（3）は，正答率が低かった。Z 社の作業担当者が保険サーバで行う不正な行為に関して，案 1 の機能を用いた検知手段を問う問題であったが，“M 社の従業員が操作ログをリアルタイムに監視する”といった，案 1 の機能とは全く関係のない検知手段を述べる解答が多かった。一般的な知見での解答ではなく，本文の記載内容に基づいて解答してほしかった。

設問 4（2）は，作業計画書に記載された作業担当者だけが特権 ID を利用できるようにするための制御を問う問題であったが，“適切な特権管理を行う”といった曖昧な内容の解答が散見された。案 2 を採用した後のシステム構成や保守作業時の運用を理解した上で，操作ログの取得と同様に中継サーバで制御する機能として，表 1 に示される PP2 の機能“利用者ごとのリモートアクセスの許可と拒否の制御”に気がついてほしかった。

問 4

問 4 では，標的型攻撃に関して出題した。この問で取り上げている標的型攻撃に遭遇した場合，設問 1 から 4 の全てにおいて，ウイルス対策ソフトが本来の機能を発揮できない場合があることを理解した上での解答を期待したが，その点の理解が不足している解答が目立った。

設問 2 は，TCP セッションのパケットキヤプチヤを出発点として未知のウイルスの解析を行う場合を例にとり，常駐してしまったウイルスの検出方法について出題した。この場合は，TCP ポート番号が大きな手がかりになるという点を理解してほしかったが，正答率は低かった。

設問 3 は，未知のウイルスに感染しているかもしれないという状況下で必要なデータファイルを確保する作業の方法について出題した。既知であれ未知であれウイルスの感染が疑われる OS 環境では，その OS を起動してはいけないことを踏まえた解答を期待したが，正答率は低かった。