SC

平成28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　組込み機器を利用したシステム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。

C社は，製造事業者向けの機械及び制御用コンピュータを製作・販売している従業員数1,200名の会社である。保守サービスの事業拡大を目的として，顧客の工場に設置されたC社製品の稼働状況を遠隔で監視するシステム（以下，工場遠隔監視システムという）を開発することになった。

工場遠隔監視システムは，機械に取り付けられているセンサの情報を制御用コンピュータ経由でリアルタイムにクラウドサービス上の監視サーバへ送信し，それをC社保守員が遠隔で監視する。センサ情報には，異常や故障を知らせる“障害情報”及び部品交換時期の目安となる使用回数などの“統計情報”が含まれる。

携帯電話網を通じてインターネットにアクセスするために，C社は自社が保有する組込み機器の開発技術を生かしてLinuxで動作するLTE（Long Term Evolution）対応ルータ（以下，LTEルータという）を開発することにした。制御用コンピュータは，LTEルータを使用することによって，機械から収集したセンサの情報をクラウドサービス上の監視サーバに送信できるようになる。監視サーバでは，通信プログラムが制御用コンピュータからセンサの情報を受信して，データベースに格納する。格納したデータは，保守員が使用する監視端末に表示される。また，顧客はWebブラウザで監視サーバにアクセスし，稼働状況を確認できる。監視端末からLTEルータの設定変更ができるように，LTEルータではSSHサービスを稼働させる。

〔試験環境の構築〕

開発担当のE君は，工場遠隔監視システムの試験環境（以下，試験環境という）を構築した。試験環境の構成を図1に示す。

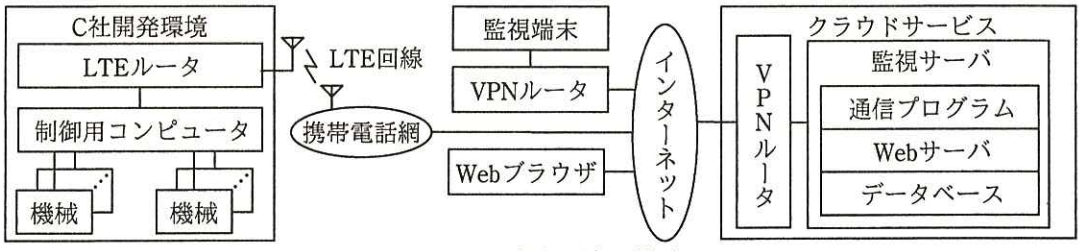


図1　試験環境の構成

インターネットを流れる通信は，Web ブラウザから監視サーバへの通信を除き，全て IPsec を使って暗号化する。IPsec では，通信モードに［ a ］モードを使用し，ルータ間の通信を全て暗号化する。鍵交換には，IKEv2 を使用し，認証方式には，事前共有鍵方式を選択する。片側のルータの IP アドレスが動的に変わる環境においては，IKEv1 の場合，［ b ］モードを使用する必要があるが，IKEv2 の場合は標準で対応している。

〔試験環境における情報セキュリティインシデントの発生〕

試験を開始してから 7 日後，E 君が監視端末から LTE ルータに SSH でログインしたところ，見覚えのない IP アドレスからログインされていることに気付いた。E 君は，不正アクセスを受けている可能性があることをプロジェクト責任者の W 主任に報告し，調査を開始した。

LTE ルータにおいて，netstat コマンドを実行したところ，表 1 に示すとおり，試験環境と無関係のグローバル IP アドレスとの接続が複数あること，及び［ c ］を送信元として SSH サービスにログインされていることが分かった。

表 1　netstat コマンドの実行結果（抜粋）

プロトコル	ローカルアドレス	外部アドレス	状態	プロセス ID
TCP	0.0.0.0:22	0.0.0.0:*	LISTEN	1543
UDP	0.0.0.0:53	0.0.0.0:*	LISTEN	1145
UDP	0.0.0.0:123	0.0.0.0:*	LISTEN	1380
UDP	0.0.0.0:500	0.0.0.0:*	LISTEN	1417
TCP	192.168.10.1:22	192.168.20.123:54433	ESTABLISHED	1545
TCP	z1.z2.z3.z4:22	x1.x2.x3.x4:32489	ESTABLISHED	1547
TCP	z1.z2.z3.z4:45532	y1.y2.y3.y4:25	ESTABLISHED	1689
TCP	z1.z2.z3.z4:45533	y1.y2.y3.y4:25	SYN_SENT	1689

注記　x1.x2.x3.x4，y1.y2.y3.y4 及び z1.z2.z3.z4 は，グローバル IP アドレスである。

更に調査したところ，攻撃者が SSH のポートフォワード機能を使って，［ d ］を宛先として SMTP で電子メールを転送していることが分かった。LTE ルータのログには，SSH サービスがパスワードの辞書攻撃を受けた痕跡が残っていた。

E 君は，IPsec を経由しなくても，インターネットから LTE ルータの SSH サービスにアクセスできる状態になっていることに気付いた。不正にログインされないた

めの暫定対策として，①SSH のログイン認証をパスワード強度に依存しない方式に設定変更した。

〔セキュリティ対策の検討〕

情報セキュリティインシデントの発生を受けて，C 社は，LTE ルータのセキュリティ対策について，セキュリティ専門業者 N 社の S 氏に相談した。

次は，セキュリティ対策に関する E 君と S 氏との会話である。

E 君 ：SSH サービスについて暫定対策を行いましたが，工場遠隔監視システムのリリースに向けてどのような対策を行う必要がありますか。

S 氏 ：LTE ルータでは，監視端末を利用した場合にだけ，SSH サービスにアクセスできる仕様にすべきです。

E 君 ：そのようにします。具体的には，どのように実現すればよいでしょうか。

S 氏 ：TCP Wrapper を使って，［ e ］することで実現できます。

E 君 ：SSH サービスに関して，他に気を付ける点はありますか。

S 氏 ：市販の幾つかの組込み機器について，②SSH のホスト鍵が同一モデルで全て同じになっているという脆弱性（ぜい）が，セキュリティ機関から注意喚起されています。C 社でも，SSH のホスト鍵は，機器 1 台ごとに異なるものを使用するように設定してください。

E 君 ：出荷する前に，いろいろとセキュリティ設定を行う必要があるのですね。

S 氏 ：さらに，新たな脆弱性が発見された場合の対応として，LTE ルータのファームウェアを更新する仕組みを実装しておく必要があります。

E 君 ：インターネット又は外部記憶媒体経由で，ファームウェアの更新用イメージファイル（以下，イメージファイルという）を LTE ルータに読み込んで保存し，コマンドを使って更新するという機能を実装したいと考えています。どのようなことに注意が必要ですか。

S 氏 ：ファームウェアの更新機能において，イメージファイルが③改ざんされていないか検証できるようにする必要があります。

E 君 ：イメージファイルを暗号化しておく必要はありますか。

S 氏 ：イメージファイルの解析ツールを使うことで，パスワードなどの重要な情報

がファームウェアにハードコードされているという脆弱性が見つかった事例が報告されており，解析されないように暗号化することも対策の一つです。④しかし，イメージファイルを暗号化しても，攻撃者が復号のための鍵を入手して，イメージファイルを復号するという可能性を排除できません。解析されても問題がないように設計することが重要です。

E君　：セキュリティに関する仕様を明確化し，基本仕様書に反映します。また，顧客に引き渡す前に，チェックリストを基にセキュリティに関する設定項目についてレビューするようにしたいと思います。

E君は，LTEルータのセキュリティ対策を実施し，W主任の承認を得ることができた。E君は，工場遠隔監視システムのリリースに向けて作業を開始した。

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　アグレッシブ　　イ　アドホック　　ウ　トランスポート

エ　トンネル　　オ　パッシブ　　カ　ブロック

設問2　〔試験環境における情報セキュリティインシデントの発生〕について，(1)，(2)に答えよ。

(1)　本文中の［　c　］，［　d　］に入れるIPアドレスを答えよ。

(2)　本文中の下線①について，実施したSSHの設定変更を30字以内で述べよ。

設問3　〔セキュリティ対策の検討〕について，(1)～(4)に答えよ。

(1)　本文中の［　e　］に入れる適切な設定内容を30字以内で述べよ。

(2)　本文中の下線②の脆弱性を悪用する攻撃手法にはどのようなものが考えられるか。20字以内で述べよ。

(3)　本文中の下線③について，どのようにして実現するか。イメージファイルの作成時と更新時に行うディジタル署名に関連した処理を，使用する鍵の種類を明示した上で，それぞれ35字以内で述べよ。

(4)　本文中の下線④について，攻撃者はどのような方法で復号のための鍵を入手するか。35字以内で具体的に述べよ。

問2　ソフトウェア開発における脆弱性対策に関する次の記述を読んで，設問 1～4 に答えよ。

V 社は，ディジタル機器の開発及びソフトウェアの受託開発を行う，従業員数 400 名の企業である。昨今，ソフトウェアの重大な脆弱性が相次いで報告されているので，V 社開発部の L 氏は，セキュリティ専門業者 S 社の情報セキュリティスペシャリストの K 氏から，ソフトウェア開発についてのアドバイスを受けることとした。

〔脆弱性及びその悪用〕

ソフトウェアの脆弱性の情報を組織間で一意に特定し共有できる仕組みが運用されている。例えば，脆弱性が報告されると，［　a　］識別子が付番され，日本国内では JPCERT/CC などが公表し注意喚起している。ただし，公表前に悪用されるものもあり，［　b　］脆弱性と呼ばれる。［　b　］脆弱性は，特定の組織を狙う攻撃，つまり［　c　］型攻撃でしばしば悪用される。

脆弱性の中でも，バッファオーバフロー脆弱性（以下，BOF 脆弱性という）は，最近開発されたソフトウェアにおいても数多く報告されている。BOF 脆弱性は，主に，スタックベース BOF 脆弱性とヒープベース BOF 脆弱性に分類される。ソフトウェアに BOF 脆弱性がある場合，当該ソフトウェアへの入力によって，①開発者が想定しないメモリ領域に書き込まれ，開発者の意図しない命令が実行されることがある。

今，Linux において実行可能ファイルが四つあるとする。図 1 は，それらが存在するディレクトリでの ls コマンドの出力である。実行権限の属性に“s”が表示されているファイルは，ファイルの所有者権限で実行されることを示している。四つのファイルのうち［　ア　］は，一般利用者 suzuki によって起動された場合でも root 権限で動作する。［　ア　］に BOF 脆弱性があると，外部の攻撃者やマルウェアによって，開発者の意図しない命令が root 権限で実行されてしまう。

```
suzuki@linux:~/temp$ ls -al
合計 40
drwxrwxr-x  2 suzuki  suzuki  4096  1月 18日 16:19 .
drwxr-xr-x 22 suzuki  suzuki  4096  1月 18日 15:54 ..
-rwxrwxr-x  1 root    root    7205  1月 18日 16:08 sample1
-rwsrwxr-x  1 root    root    7205  1月 18日 16:10 sample2
-rwxrwxr-x  1 suzuki  suzuki  7205  1月 18日 16:10 sample3
-rwsrwxr-x  1 suzuki  suzuki  7205  1月 18日 16:10 sample4
suzuki@linux:~/temp$
```

図1　ls コマンドの出力

〔ヒープベース BOF 脆弱性〕

K 氏によると，最近，ヒープベース BOF 脆弱性を悪用する攻撃の報告が増えてきているという。L 氏は，出荷前の V 社製品のソフトウェアについてヒープベース BOF 脆弱性がないか，K 氏のレビューを受けることにした。

図2のプログラム Y は，起動時に，第1引数は利用者 ID を，第2引数はパスワードを受け取る。このプログラム用にあらかじめ登録された“利用者 ID とパスワード”の組と引数で与えられた組を比較し，利用者認証する。“利用者 ID とパスワード”は，いずれも半角英数字，最小 6 文字最大 8 文字の文字列と仕様で定められている。

```
 1: #include <iostream>
 2: #include <cstring>
 3: (省略)
 4: #define UID_SIZE 8     // 利用者 ID の文字列の上限値
 5: #define PASS_SIZE 8    // パスワードの文字列の上限値
 6: (省略)
 7: using namespace std;
 8:
 9: void getPass(char *pass, char *uid)
10: {
11: (省略, uid で指定された利用者 ID を基に登録済パスワードを取得し pass に格納, 利用者
    ID が存在しない場合は長さ 0 の文字列を pass に格納)
12: }
13: (省略)
14:
15: int main(int argc, char **argv)
16: {
17:     static char *uid;
18:     static char *pass;
19:     (省略, 引数の個数をチェック)
20:     uid = new char[UID_SIZE+1];
21:     pass = new char[PASS_SIZE+1];
22:     getPass(pass, argv[1]);
23:     strcpy(uid, argv[1]);
24:
25:     if (strlen(pass) == 0 || strcmp(argv[2], pass) != 0) {
26:       cout << "認証失敗" << endl;
27:       (省略, uid を出力, 認証失敗時の処理)
28:     } else {
29:       cout << "認証成功" << endl;
30:       (省略, uid を出力)
31:     }
32: }
```

図 2　ヒープベース BOF 脆弱性のあるプログラム Y

プログラム Y にはヒープベース BOF 脆弱性があり，②引数によっては，利用者認証を回避される可能性があると，L 氏は K 氏に指摘された。ただし，K 氏によると，③このプログラム Y は引数が同じでも，実行環境によっては利用者認証を回避されないとのことだった。L 氏は，V 社の開発した他のプログラムについても確認することとした。

〔V 社の脆弱性対策〕

BOF 脆弱性は，メモリを直接操作することが可能なプログラム言語 C や C++などで発生する。その対策として，例えば，Windows ではハードウェア DEP（Data Execution Prevention）のようなデータ実行防止機能を適用することで，一部の BOF

脆弱性を悪用する攻撃を抑制できる。しかし，④プログラム Y での利用者認証を回避する攻撃に対しては有効に機能しない。そこで，V 社では，C や C++の利用が避けられない場合を除き，BOF 脆弱性が起きにくい他のプログラム言語を利用することとした。一般的には，開発時に，静的解析ツールを利用したり，通常の利用では想定しないデータを入力し，その応答から脆弱性を探す［ d ］検査を行うツールを利用したりして，脆弱性を洗い出すことも効果的である。また，V 社では，ソフトウェアのリリース後，脆弱性が発見された場合に備え，V 社製品の利用者に更新プログラムを提供するサイトを準備することとした。

設問 1　本文中の［ a ］～［ d ］に入れる最も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　CVE　　イ　ゼロデイ　　ウ　標的　　エ　ファジング

設問 2　脆弱性を悪用する攻撃について，(1)，(2)に答えよ。

(1)　本文中の下線①について，スタックベース BOF 脆弱性を悪用する攻撃の場合，関数呼出し時にスタックに必ず積まれるはずの，何の値を書き換えることによって攻撃が開始されるか。20 字以内で答えよ。

(2)　本文中の［ ア ］に入れるファイル名を全て答えよ。

設問 3　図 2 のプログラムの脆弱性について，(1)～(3)に答えよ。

(1)　本文中の下線②はどのような引数で利用者認証を回避されるか。引数の組を解答群の中から選び，記号で答えよ。

解答群

記号	第 1 引数	第 2 引数
ア	001（繰返し）0111111111	11111110
イ	001（繰返し）1111111111	11111110
ウ	011（繰返し）1111111101	11111101
エ	111（繰返し）1111111111	67891231
オ	123（繰返し）1231231231	67891231

(2) 利用者認証を回避される原因となるヒープベース BOF 脆弱性の存在箇所を，実際にバッファがオーバフローするコードの行番号で答えよ。

(3) (2)で示した行番号の行を差し替えて行う改修案として適切なものを解答群の中から全て選び，記号で答えよ。

解答群

ア `memcpy(uid, argv[1], strlen(argv[1])+1);`

イ `memcpy(uid, argv[1], UID_SIZE+1);`

ウ `pass = new char[PASS_SIZE+8];`

エ `strncpy(uid, argv[1], strlen(argv[1])+1);`

オ `strncpy(uid, argv[1], UID_SIZE+1);`

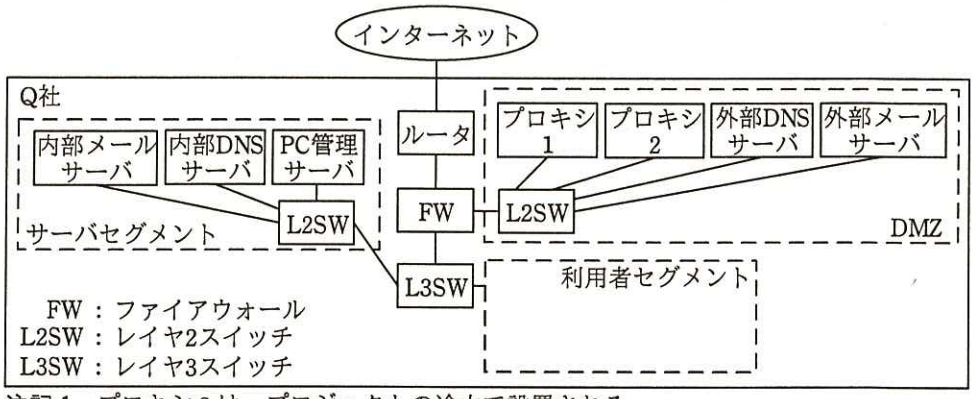
設問4 利用者認証の回避について，(1)，(2)に答えよ。

(1) 本文中の下線③について，利用者認証が回避されない理由を，攻撃のタイミングではなく実行環境の観点で，40 字以内で述べよ。

(2) 本文中の下線④について，有効に機能しない理由を，30 字以内で述べよ。

問３　プロキシサーバによるマルウェア対策に関する次の記述を読んで，設問 1～4 に答えよ。

Q 社は従業員数 1,000 名の医薬品製造会社である。Q 社では，セキュリティ対策を強化するために，ブラックリスト指定の URL フィルタリング機能だけを有しているプロキシサーバ（以下，プロキシ 1 という）を，セキュリティ機能が豊富な新しいプロキシサーバ（以下，プロキシ 2 という）に更新するプロジェクトを開始した。Q 社のネットワーク構成を図 1 に示す。



注記 1　プロキシ 2 は，プロジェクトの途中で設置される。
注記 2　Q 社の管理 PC 及び社員 PC は，利用者セグメントに接続されている。

図 1　Q 社のネットワーク構成

情報システム部（以下，情シ部という）は，情報システムの管理及び情報セキュリティインシデントの対応を行っている。サーバ管理業務は，情シ部のサーバ管理者が行う。情シ部にはサーバ管理者が複数人いる。サーバ管理者は各種設定などのサーバ管理業務を行う場合だけ，1 台の管理 PC に自分の管理者 ID でログオンし，OS の管理用のコマンドなどを使用する。OS の管理用のコマンドは，一般利用者でも起動可能なものもある。管理 PC はサーバ管理業務だけに用い，Web ブラウザによるインターネット接続及び電子メール（以下，メールという）の送受信はできないように設定されている。管理 PC での作業後には，開始日時，終了日時及び作業者名を記録する運用が徹底されている。

Q 社の従業員は，一人 1 台貸与された社員 PC を使用している。管理 PC 及び社員 PC には，全て，固定 IP アドレスが割り振られている。社員 PC からインターネット

への通信は，外部メールサーバ経由のメールの送受信と，プロキシ 1 経由の HTTP 及び HTTP over TLS での Web アクセスだけが利用できるようになっている。社員 PC の Web ブラウザは，インターネット接続時に，プロキシ 1 を経由するよう設定されている。社員 PC には OS の管理用のコマンドはインストールされていない。

PC のプログラム起動禁止設定は，PC 管理サーバによって，全て一括管理されている。プログラム起動禁止設定には，プログラム名が一致した場合にプログラムの起動を禁止にする方式と，プログラムの実行ファイルのハッシュ値が一致した場合に禁止する方式があり，両方の方式を組み合わせた設定もできる。Q 社は，複数の P2P プログラムのプログラム名を指定して起動を禁止している。

サーバ及び PC では，ログオン，ログオフ及び操作のログを，ネットワーク機器では通信ログをそれぞれ取得している。プロキシ 1 では，日時，接続先 URL，送信元 IP アドレス，ステータスコード，応答のサイズなどのログを取得している。

プロキシ 2 の機能を表 1 に示す。

表 1　プロキシ 2 の機能

機能		説明
フィルタリング機能	URL フィルタリング機能	・ホワイトリストに設定した URL を許可する。 ・ブラックリストに設定した URL を遮断する。
	カテゴリ単位フィルタリング機能	・カテゴリ単位に次のいずれかを指定する。 “許可”：カテゴリごとに定義された URL を許可し，ログに記録しない。 “検知”：カテゴリごとに定義された URL を許可し，ログに記録する。 “遮断”：カテゴリごとに定義された URL を遮断し，ログに記録する。
プロキシ認証機能		・PC からインターネットの Web サイトへの接続時に利用者 ID とパスワードによる利用者認証を行い，認証結果をログに記録する。
a 機能 [1)]		・インターネットから Web サーバへの通信を中継する。

注 1)　Q 社では本機能は使用しない。

プロキシ 2 のカテゴリ単位フィルタリング機能のために，ニュース，ゲーム，外部ストレージサービスなどのカテゴリが用意されており，これらについては，カテゴリごとに分類された URL リストが随時更新され，プロキシベンダの Web サイトを通じて提供される。サーバ管理者がカテゴリを選んで，通常は“遮断”を指定する。URL フィルタリングとカテゴリ単位フィルタリングで同じ URL が設定された場合は，URL フィルタリングによる設定が優先される。URL フィルタリングのホワイトリス

ト，ブラックリストで同じ URL が設定された場合は，ホワイトリストの設定が優先される。

Q社では，フィルタリング機能の設定は，情シ部のサーバ管理者が行う。

〔プロキシ更新〕

情シ部ではプロキシ1からプロキシ2への更新を，次に述べるフェーズ1～3の3段階で行うことにした。

フェーズ1では，プロキシ1と社員PCとの通信方法を変えずに，DMZにプロキシ2を導入し，プロキシ1とインターネット間の通信を，全てプロキシ2経由とする。プロキシ1のURLフィルタリング機能を無効にして，プロキシ2のフィルタリング機能の一部だけを有効にする。ログについては，プロキシ2で，プロキシ1と同じ項目のログを取得するよう設定する。

フェーズ2では，プロキシ2のフィルタリング機能及びプロキシ認証機能を強化する。

フェーズ3では，社員PCのWebブラウザのプロキシ設定をプロキシ1からプロキシ2に変更し，プロキシ1を撤去する。

このようにフェーズ分けを行うのは，情シ部の次の二つの判断による。

・社員 PC の導入時期が異なるので，複数種類，複数バージョンの Web ブラウザが使用されており，プロキシ2に切り替えると不具合が発生する可能性が高い。
・何らかの不具合が発生した場合に，迅速に旧環境への切り戻しができる。

〔情報セキュリティインシデントの発生と対応〕

フェーズ1開始後まもなく，海外のセキュリティ専門業者から，C&C（Command & Control）サーバにQ社からの通信の記録があるとの連絡があった。情シ部のJ部長が経営陣に報告し，情報セキュリティスペシャリストのTさんとともに調査したところ，次のことが分かった。

・文書ファイルが添付されたメールが複数の従業員宛てに届いた。
・そのうち，営業部のUさんが添付ファイルを開いたので，Uさんの社員PCがマルウェア（以下，マルウェアZという）に感染した。
・マルウェアZは，文書ファイルのマクロとして実装されていた。マルウェアZは，

Uさんの社員PC上で動作し，文書閲覧ソフトの脆弱性を悪用してC&Cサーバと通信し，攻撃用プログラムを当該PC上にダウンロードして起動させた。

・攻撃用プログラムは，OSの管理用のコマンドをUさんの社員PC上に複数ダウンロードして起動させ，サーバ情報を窃取した。

・マルウェアZには，ネットワークで接続された他のPCやサーバに感染を広げる機能がある。

・Uさんの社員PC以外には感染したPCやサーバはなかった。

J部長は，不審なメールを受信した場合，添付ファイルや，メール内に記載されているURLをクリックしないよう全従業員に注意喚起を行った。次に，J部長は次の二つを指示した。

・社員PCで，［ b ］のプログラム起動禁止設定を行う。

・管理PCで，［ c ］のプログラム起動禁止設定を行う。

〔プロキシサーバにおける追加設定〕

情シ部は，C&CサーバのURLをプロキシ2のブラックリストに設定した。また，マルウェアの感染の拡大に備えて，今後はプロキシ2によってC&Cサーバへの接続が遮断されたPCをプロキシサーバのログから特定し，直ちにLANから切り離すことにした。ところが，Tさんは，次の問題があることに気付いた。

・プロキシ1のログだけでは，プロキシ2で遮断したことが確認できない。

・①プロキシ2のログだけでは送信元PCが特定できない。

そこで，プロキシ1では，HTTPヘッダとして［ d ］ヘッダフィールドを追加するように設定し，プロキシ2では，［ d ］ヘッダフィールドをログに出力するように設定した。

情シ部は，インシデント対応を完了し，プロジェクトをフェーズ2に進めた。

〔フェーズ2の開始〕

フェーズ 2 において，情シ部は，まず，②プロキシ認証に対応したマルウェアも多いとの調査報告を踏まえ，効果が完全ではないことを認識しながらも，プロキシ 2 のプロキシ認証機能を有効にした。

次に，計画どおりプロキシ 2 のカテゴリ単位フィルタリング機能を用いて，業務に不要と思われるカテゴリを“遮断”に設定した。すると，一部の部門から，業務で使用している Web サイトが使用できなくなったとの連絡があった。そこで，業務に不要と思われるカテゴリを“検知”に設定し，1 か月間運用した後，③業務に必要かつ安全であることを確認した URL は許可し，それ以外の URL は遮断することにした。

情シ部は，問題がないことを確認後，プロジェクトをフェーズ3に進めた。

設問1　表 1 中の［ a ］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　DMZ　　イ　フォワードプロキシ

ウ　プロキシ ARP　　エ　リバースプロキシ

設問2　〔情報セキュリティインシデントの発生と対応〕について，(1)，(2)に答えよ。

(1)　本文中の［ b ］，［ c ］に入れる次の(i)～(iii)の適切な組合せを，それぞれ解答群の中から選び，記号で答えよ。

(i)　OS の管理用のコマンド

(ii)　攻撃用プログラム

(iii)　マルウェア Z

解答群

ア　(i)　　イ　(i)，(ii)　　ウ　(i)，(ii)，(iii)　　エ　(i)，(iii)

オ　(ii)　　カ　(ii)，(iii)　　キ　(iii)

(2)　プログラム名を指定する方法とハッシュ値を指定する方法の両方でプログラム起動禁止設定を行ったとしても，攻撃用プログラムの起動を防ぎきれない場合がある。それは，どのような攻撃用プログラムの場合か。30 字以内で具体的に述べよ。

設問3　〔プロキシサーバにおける追加設定〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，プロキシ2のログだけでは送信元PCが特定できない理由を，30字以内で述べよ。

(2)　本文中の［　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　Max-Forwards　　イ　Proxy-Authorization　　ウ　Referer

エ　User-Agent　　オ　X-Forwarded-For

設問4　〔フェーズ2の開始〕について，(1)，(2)に答えよ。

(1)　本文中の下線②について，マルウェアは，どのようにして，認証を成功させるか。50字以内で具体的に述べよ。

(2)　本文中の下線③について，プロキシ2でどのように設定すべきか。URLフィルタリング機能及びカテゴリ単位フィルタリング機能について，それぞれ40字以内で具体的に述べよ。

〔 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。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。