問2　テレワークのセキュリティに関する次の記述を読んで，設問1～5に答えよ。

Q社は，従業員数700名のシステムインテグレータである。東京，名古屋及び大阪に事業所がある。各事業所では，固定席をもたないフリーアドレスが採用されている。営業員やシステムエンジニアなど，テレワークを行っている社員はモバイラと呼ばれ，モバイルPCとUSBデータ通信端末が貸与されている。モバイラは，休暇や長期出張などの場合を除き，週1時間以上Q社事業所に出社し，モバイルPCを社内LANに接続することが義務付けられている。

Q社では，モバイルPCを含むIT機器全てを情報システム部（以下，IT部という）が管理している。Q社には，IT全般に関する問合せ窓口としてIT部内にITヘルプデスクが設けられており，電話，電子メール（以下，メールという），チャットでサポートを行っている。ITヘルプデスクは情報セキュリティに関する問合せも受け付けている。

〔モバイラのテレワーク環境〕

Q社では，モバイラの顧客先などでのテレワークを支援するために，表1に示すクラウドコンピューティングで実現されたサービス（以下，クラウドサービスという）を利用させている。クラウドサービス利用に関するQ社のセキュリティガイドラインを図1に示す。

表1　Q社が利用させているクラウドサービス

サービス	機能概要
H社Webメール	メール，SPAMフィルタ及びマルウェア対策の機能を提供する。
J社セキュアプロキシ（以下，Jプロキシという）	利用者認証付きのHTTPプロキシ機能，URLフィルタ機能，及びHTTPリクエストヘッダの文字列検査によるフィルタ（以下，RHフィルタという）機能を提供する。RHフィルタ機能では，正規表現を使用することができる。利用者認証の有効期間は24時間である。
N社コラボレーションツール（以下，Nコラボという）	ファイル共有，掲示板，チャットなどの機能を提供する。各利用者に5Gバイトのファイル保管領域が割り当てられている。利用者がきめ細かなアクセス制御を設定可能である。
P社CRMツール	顧客企業情報管理，案件情報管理などの機能を提供する。

1. ユーザインタフェース上で無操作状態が 5 分以上続いた場合は，自動的にログオフされるよう設定する。
2. 利用者認証が連続して 3 回失敗した場合は，アカウントがロックされるよう設定する。
3. Q 社貸与のモバイル PC 及び社内 LAN からの，HTTP 及び HTTP over TLS（以下，HTTPS という）によるアクセスだけを許可するよう設定する。

図 1　クラウドサービス利用に関する Q 社のセキュリティガイドライン（抜粋）

Q 社のモバイル PC には，マルウェア対策ソフト（以下，AM という）やパーソナルファイアウォール（以下，PFW という），オフィスソフトウェアなどの Q 社が利用を認めたソフトウェア（以下，標準ソフトという）がインストールされている。

Q 社内には，AM 管理サーバがあり，社内 LAN だけからアクセス可能である。モバイル PC は，社内 LAN 接続時に，AM のログを AM 管理サーバにアップロードする。

Q 社のモバイル PC の概要を表 2 に，Q 社のモバイル PC に導入されている PFW の概要を図 2 に示す。

表 2　Q 社のモバイル PC の概要

項目	概要
利用者 ID	利用者は，ローカルユーザの利用者 ID 及び 8 桁以上のパスワードを使用する。各利用者 ID には当該モバイル PC の OS の管理者権限が与えられている。
プロキシ	プロキシ自動設定機能によって，インターネット上の Web サイトへのアクセスは自動的に J プロキシを利用するよう設定されている。
可搬記憶媒体	可搬記憶媒体を利用する場合，媒体上のデータが自動的に暗号化される。
ハードディスク暗号化	ハードディスク全体が暗号化されている。パワーオン時には，OS 起動前にパスワードの入力を求めるプログラムが立ち上がり，認証を行う。認証が成功すると，ハードディスクへの書込み時の暗号化と読出し時の復号を透過的に行うようになり，その後 OS を起動する。OS からは，ハードディスク内にデータが平文で格納されているかのようにアクセスできる。
AM	ファイルの書込み時，読出し時及び実行時にパターンマッチングによるマルウェアスキャンを行う。マルウェアの検知時には，ポップアップを表示し，マルウェア名と対処内容（検知だけ，隔離，駆除済み）を表示するとともに，ログに記録する。マルウェア定義ファイルは，インターネット上の専用サイト（以下，AM サイトという）から自動的にダウンロードされ，更新される。
脆弱（ぜい）性修正プログラム（以下，修正パッチという）	OS の修正パッチは，インターネット上のベンダサイトから自動的にダウンロードされ，適用される。

・次の通信だけを許可する。
- J プロキシを介した HTTP 通信及び HTTPS 通信
- PFW 管理サーバ，AM 管理サーバ及び AM サイトへの通信
- インターネット上のベンダサイトへの OS の修正パッチダウンロード用の通信
- DHCP 通信，DNS 通信及び NTP 通信

・次のログを記録し，モバイル PC が社内 LAN に接続されたときに，Q 社内に設置されている PFW 管理サーバにアップロードする。
- モバイル PC 外との許可された通信の場合，通信したプロセスの実行ファイル名，通信先 IP アドレス，通信先ポート番号，自ポート番号及び通信開始時刻
- モバイル PC 外への許可されていない通信の場合，通信を開始したプロセスの実行ファイル名，通信先 IP アドレス，通信先ポート番号，自ポート番号及び通信開始時刻（アラートを PC 画面上にも表示する。）
- モバイル PC 外からの許可されていない通信の場合，通信元 IP アドレス，通信元ポート番号，通信先ポート番号及び通信開始時刻

・上記通信許可及びログの記録に関する設定を含むポリシは，PFW 管理サーバ上にあり，それが更新された後，初めてモバイル PC が社内 LAN に接続されたときに，ダウンロードされ，適用される。

図 2　Q 社のモバイル PC に導入されている PFW の概要

Q 社には，モバイル PC のバックアップを自動的に取得する仕組みはない。そのため，必要なファイルは N コラボに保管しておくことが推奨されている。

〔マルウェアの検知〕

Q 社では，マルウェア検知時の対応手順を，図 3 のとおり定めている。

1. マルウェア定義ファイルを最新にした後，PC をネットワークから切り離す。
2. 当該 PC 上で AM のフルスキャンを実行する。
3. フルスキャンでマルウェアが検知された場合，IT ヘルプデスクに報告し，判断を仰ぐ。検知されなかった場合，継続利用してよい。

図 3　マルウェア検知時の対応手順

2 月 1 日，名古屋事業所の B さんから IT ヘルプデスクに“モバイル PC で繰り返しマルウェアが検知される”との連絡が入り，IT 部の情報セキュリティ担当者である C さんが対応した。次は，その時の B さんと C さんの会話である。

B さん：私のモバイル PC で，先週 1 週間に 3 回も同じマルウェア M が検知されました。毎回“駆除済み”と表示されるのですが，駆除できていないのでし

ようか。

C さん：マルウェア検知時の対応手順に従って AM のフルスキャンをしましたか。

B さん：はい。もちろんです。3 回とも実施しましたが，何も検知されませんでした。

C さん：問題ないと思いますが，念のため IT 部で調査します。モバイル PC のホスト名と最後に社内 LAN に接続した日を教えてください。

B さん：ホスト名は PC01 です。今日も，社内 LAN に接続しています。

〔IT 部による調査〕

C さんが AM 管理サーバのマルウェア検知ログを調べたところ，PC01 ではマルウェア M が 3 回検知され，駆除されていた。他のマルウェアは検知されていなかった。

次に，C さんは PFW 管理サーバで，マルウェア検知と同じ時間帯の，PC01 の PFW のログを確認した。PFW のログには，OS 標準の Web ブラウザ（以下，標準ブラウザという）のプロセスからの通信だけが記録されていた。

C さんが，マルウェア検知と同じ時間帯の J プロキシのログを調査したところ，次のことが分かった。

・マルウェア検知の直前に 3 回とも同じ URL にアクセスし，同じ長さのコンテンツがダウンロードされていた。

・当該 URL への HTTP 通信は，HTTP リクエストヘッダの User-Agent（以下，UA という）が標準ブラウザとは異なっていた。

・HTTP リクエストヘッダには，UA と Host だけが設定されていた。

該当するログは表 3 のとおりである。

表3　Jプロキシの該当ログ

Time	CIP	User	RM	URL	SC	CCL	SCL	UA	Ref
2016-01-25 09:13:29 +0900	xx.xx.13.1	user01	GET	http://yy.yy.yy.yy/?v1 =（省略）	200	-	218783	DL2	-
2016-01-27 09:23:34 +0900	10.10.2.101	user01	GET	http://yy.yy.yy.yy/?v1 =（省略）	200	-	218783	DL2	-
2016-01-28 09:12:27 +0900	xx.xx.13.1	user01	GET	http://yy.yy.yy.yy/?v1 =（省略）	200	-	218783	DL2	-

Time：処理終了時刻，CIP：クライアント IP アドレス，User：認証利用者 ID，RM：HTTP リクエストメソッド
SC：HTTP ステータスコード，CCL：クライアントからのリクエストのコンテンツ長
SCL：サーバからのレスポンスのコンテンツ長，Ref：Referer
注記1　"user01" は B さんの認証利用者 ID を示す。
注記2　"xx.xx.13.1" は USB データ通信端末利用時の IP アドレスを，"10.10.2.101" は Q 社の IP アドレスを，"yy.yy.yy.yy" は C&C サーバの IP アドレスを示す。

C さんは，マルウェア M をダウンロードする未知のマルウェアが，UA を DL2 に設定して C&C サーバと通信していると考えた。J プロキシのログから UA が DL2 の通信を検索したところ，次のことが分かった。

・アクセス先 URL は異なるものの，PC01 は，1 月 25 日以降ほぼ毎日 UA が DL2 の通信を行っていた。
・他に PC02～PC04 の 3 台のモバイル PC が，UA が DL2 の通信を行っていた。
・調査日当日も PC01 から UA が DL2 の通信があり，"200 OK" が返っていた。
・①当該アクセス先 URL に，C さんに貸与されている PC の標準ブラウザからアクセスしたところ，"404 Not Found" が返ってきた。

C さんは，これらのログの調査から，B さんのモバイル PC でマルウェアの検知・駆除が繰り返される事象は，未知のマルウェアが原因だと結論付けた。

C さんは，②当該マルウェアによるモバイル PC から C&C サーバへの通信をブロックする必要があることと，PC01 について専門業者による詳細な調査の必要があることを IT 部 D 部長に説明し，調査依頼の承認を得た。

C さんは，C&C サーバへの通信のブロックを担当者に依頼した。次に，C さんは，PC01～PC04 について，利用者に連絡を取り，IT 部への送付を依頼した。B さんを含む各利用者は，当該モバイル PC を IT 部に送付した。

〔専門業者による調査〕

C さんは，PC01 の調査をセキュリティ専門業者の X 社に依頼した。X 社による調査結果は図 4 のとおりであった。

- PC01 の一時ディレクトリに不審なファイル 5 個と削除済みの不審なファイル 13 個があった。
- 不審なファイル 5 個のうち，2 個はマルウェア本体，他の 3 個はマルウェアが利用する一時ファイルであった。
- 削除済みの不審なファイル 13 個のうち，少なくとも 4 個は実行可能コードを含んでおり，マルウェアの一部であった。また，他の 3 個は先頭部分に圧縮ファイルを示す文字列が含まれていたが，ファイルが不完全であったので展開できなかった。残りの 6 個は詳細が判明しなかった。
- 活動している未知のマルウェアのプロセスを解析した結果，その実行ファイルは標準ブラウザであった。標準ブラウザに対し，[a] インジェクション攻撃が行われ，不正なコードが呼び出されて実行されていた。この不正なコードを含むファイルは，システムディレクトリにあった。
- 当該マルウェアは，改ざんされたバナー広告の表示によって感染が起きるマルウェアの亜種であった。

図 4　X 社による調査結果（抜粋）

〔侵入経路と被害状況の調査〕

X 社の報告を受け，C さんはマルウェアの侵入経路及び外部への情報漏えいの有無を調査した。侵入経路については，Web サイト W からマルウェアをダウンロードしていたことが判明した。Web サイト W で表示していたバナー広告が改ざんされており，当該バナー広告を表示するときに利用するビューア（以下，ビューア V という）の脆弱性を利用して，自動的にダウンローダを導入・実行する攻撃コードが含まれていた。いわゆる [b] ダウンロード攻撃であった。ビューア V は以前に業務上必要があったので標準ソフトとして導入されていたが，現在では必要性はなくなっていた。ビューア V の脆弱性は度々報告されていたが，Q 社では標準ソフトの脆弱性を管理しておらず，修正パッチの適用も強制していなかった。

PC02～PC04 も，B さんと同様に利用者が Web サイト W にアクセスしたことによって感染していた。

外部への情報漏えいの有無については，各種ログやハードディスクに残されていたファイルの痕跡からは，判断できなかった。PC01～PC04 のうち，PC01 だけは，お客様プロジェクト関連情報（以下，PJ 情報という）を含むファイルがハードディ

スク上に複数保管されており，いずれも圧縮状態で 200 k バイト以上であった。一方，J プロキシのログは，PC01 から外部に送信された HTTP 通信の CCL が，全て 2 k バイト未満であることを示していた。これらから，C さんは，外部への PJ 情報の漏えいはないと結論付け，調査結果を D 部長に報告した。

次は，調査結果についての C さんと D 部長の会話である。

D 部長：この分析結果から PJ 情報の漏えいがないと判断するのは無理があります。

C さん：なぜですか。

D 部長：まず，PC01 についてですが，マルウェアが PJ 情報の入ったファイルを [c] して送信した可能性があります。また，PC01 のハードディスクではなく，[d] や [e] に格納されていた PJ 情報が窃取された可能性もあります。

C さん：確かにそうですね。再度調査します。

C さんは，再度調査を行ったが，PJ 情報漏えいの痕跡は発見できなかった。C さんはそのことを D 部長に報告した。D 部長は調査結果を了承した。

C さんはこの調査結果を，B さん及び PC02～PC04 の利用者に伝えた。

〔委託元への報告〕

B さんは，名古屋に本社がある流通業 E 社の業務システム開発プロジェクトに参画している。E 社との契約では，情報漏えいなどのセキュリティインシデント発生時には遅滞なく E 社に報告することが定められている。E 社では，業務システムのプログラム開発及びテストには専用の PC を貸与している。B さんは，設計書を含む文書作成は PC01 で行い，プログラム開発及びテストは E 社から貸与された PC で行っていた。

IT 部での調査結果を基に，今回の件では PJ 情報の漏えいはなかったというのが Q 社の見解であるが，営業部，IT 部，法務部及び名古屋事業所の F 部長が協議した結果，IT 部の調査結果を基に E 社に報告することにした。

3 月 28 日，F 部長が E 社に報告したところ，E 社の G 部長から非常に厳しい叱責を受けた。G 部長の見解は図 5 のとおりである。

・マルウェア感染は報告すべきセキュリティインシデントである。
・業務システムの設計書が外部に漏れると，事業上多大な影響がある。
・発生後すぐにセキュリティインシデント報告をすべきであった。
・Q社内の調査だけで情報漏えいはなかったと結論付けているが信用できない。
・Bさんのモバイル PC から E 社に提出又は送信した文書ファイルによって，E 社のシステムがマルウェアに感染した可能性もある。

図5　E社G部長の見解（抜粋）

F 部長は，営業部，IT 部及び法務部と相談し，図 6 の対応方針をまとめ，早急に対応を進めた。

・次の追加調査をX社に依頼する。
　- 情報漏えいの痕跡
　- BさんからE社宛てに送信したメールの添付ファイル
　- BさんがE社に提出又は送信した文書ファイル
・今回のマルウェア感染に対する再発防止策を策定する。
・上記の調査結果と再発防止策をF部長からE社G部長に説明する。

図6　対応方針（抜粋）

X 社の追加調査の結果は，Q 社内での調査と同様，情報漏えいの痕跡は認められないというものであった。また，B さんから E 社宛てに送信したメールの添付ファイル及び E 社に提出又は送信した文書ファイルには，不審なコードは含まれていなかったとの報告であった。

〔再発防止策の策定〕

今回のマルウェア感染に対する再発防止策を，IT 部が中心に策定することとなった。C さんは，調査で判明した事実を基に，他の IT 部のメンバとともに課題を抽出し，対策を検討した。その結果は表 4 のとおりである。

表4　課題と対策

項番	課題	対策
1	（省略）	標準ソフトの脆弱性管理を行い，必要な修正パッチを適用する。
2	ビューア V を含む標準ソフトの［　f　］が行われていなかった。	定期的に標準ソフトの［　f　］を行う。
3	・マルウェアが検知されても，AM で駆除でき，AM のフルスキャンで他のマルウェアが検知されなければ，当該 PC の継続利用を認めていた。 ・AM の検知状況を監視していなかった。	（省略）
4	（省略）	未知のマルウェアに対する対策（以下，未知マルウェア対策という）を行う。

C さんは，課題と対策を D 部長に報告した。D 部長は，表 4 の項番 1～3 の対策を再発防止策とし，可能な対策から順次実施するとともに，項番 4 の対策を具体化するよう指示した。

〔未知マルウェア対策の検討〕

C さんは，D 部長の指示に従い，未知マルウェア対策の検討を始めた。次は，未知マルウェア対策の検討についての C さんと D 部長の会話である。

C さん：未知マルウェア対策として，図 7 の案を考えました。未知のマルウェアを全て検知するのは無理です。そのため，未知のマルウェアへの感染を前提とした対策も必要です。

【未知のマルウェアの検知を目的とした対策】
・入口対策：Web 閲覧やメールで入ってきたファイルをサンドボックスで実行し，振る舞いを調べることによってマルウェアを検知する対策など
・出口対策：レピュテーションやアノマリ検知によって，C&C 通信を発見する対策など
【未知のマルウェアへの感染を前提とした対策】
・マルウェアに感染しても情報が漏えいしない対策（データの暗号化など）
・マルウェアに感染しても感染前の状態に戻せる対策（ブートイメージからの復元など）

図 7　未知マルウェア対策案（抜粋）

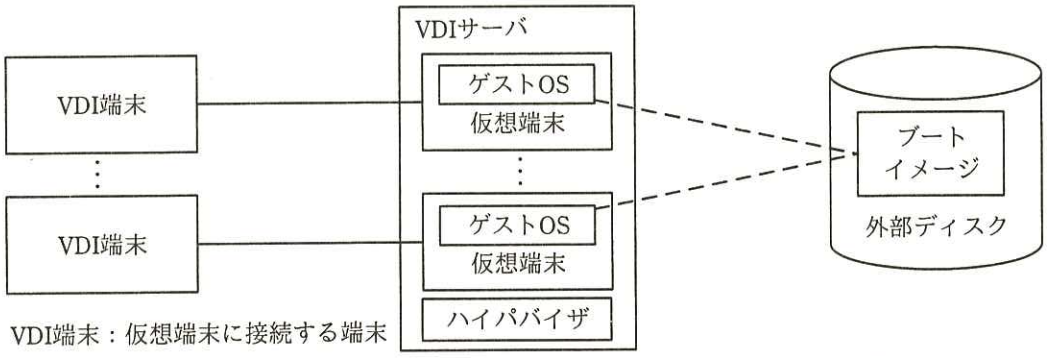
D 部長：我が社のモバイル PC ではハードディスクの暗号化を行っていますが，マル

ウェア感染時の情報漏えいを防げますか。

C さん：残念ながら，③マルウェア感染による情報漏えい対策としては役に立ちません。そうした情報漏えいを防ぐためには DRM のような仕組みが必要になり，取引先にも影響があります。

D 部長：なるほど。ブートイメージからの復元というのはどのようなものですか。

C さん：ブートイメージとは OS の起動に必要なファイルや標準ソフトなどをひとまとめにしたものです。これを読取り専用領域に保存し，起動時に読み込ませることで，動作環境を復元します。実装方法として，モバイル PC 上に読取り専用領域を作成する方法と，図 8 のように，仮想端末上でゲスト OS を動かす，画面転送型の仮想デスクトップ環境（以下，VDI という）の二つがあります。これら二つの対策を我が社が利用した場合，表 5 で示すメリットとデメリットがあります。



VDI端末：仮想端末に接続する端末

注記　破線は，ブートイメージを仮想端末にゲスト OS として読み込むことを示す。

図 8　VDI のシステム構成

表 5　メリットとデメリット（抜粋）

項番	対策	メリット	デメリット
1	モバイル PC 上に読取り専用領域を作成	・実装が容易 ・オフラインでも使える。	・④再起動時に一部のセキュリティ対策が初期化される。 ・利用者ごとの個別の設定が困難 ・運用負荷が高い。
2	VDI	・運用負荷が低い。 ・利用者ごとの個別の設定が容易	・既存の AM 利用時に問題が発生する。 ・設備費用が高い。

D 部長：表 5 によると VDI が良さそうですが，デメリットを解消する方法はありますか。

C さん：AM に関しては，VDI に対応した仮想アプライアンスやゲートウェイ型のものが利用できるクラウドサービスを検討します。

D 部長：VDI 端末としてモバイル PC は使えるのですか。

C さん：はい。モバイル PC を使って USB メモリから VDI 専用 OS を起動する方法があります。

D 部長：VDI 端末には，どのような要件が必要ですか。

C さん：要件は，次の四つです。

要件 1：VDI サーバにログインできる。

要件 2：仮想端末との間では，画面及びキーボード・マウスの操作データだけの送受信を許可する。

要件 3：マルウェア感染を防ぐ仕組みがある。

要件 4：要件 1～要件 3 を満たすのに必要な通信だけを許可する。

D 部長：要件 3 が満たせずに，VDI 端末がマルウェアに感染しても，要件 2 が満たされていれば，仮想端末には影響がないですよね。

C さん：いいえ。⑤要件 2 が満たされても，VDI 端末上のマルウェアによる仮想端末からの情報の窃取は可能です。

D 部長：そうですか。

C さん：そういった情報の窃取を防ぐためには，VDI 端末の徹底的な要塞化が必要です。VDI 端末に汎用 OS を使う場合，VDI 端末の保護のための仕組みが必要になります。一方，VDI 専用 OS を使用する場合，読取り専用の USB メモリに VDI 専用 OS を入れておきます。VDI 端末のハードディスクの中身は全て消去し，USB メモリからだけブートできるようにします。ブートすると VDI に接続するためのソフトウェアが自動的に起動します。

D 部長：なるほど。それでは，その案をベースに，VDI の実装案と移行計画をまとめて提出してください。その際には，既存のガイドラインへの影響なども考慮に入れてください。

C さんは，VDI の実装案，⑥クラウドサービス利用に関する Q 社のセキュリティ

ガイドラインの変更案，及び移行計画を D 部長に提出した。D 部長はこれを承認し，関係各部と調整して年次計画に組み込んだ。

F 部長はこれらの結果を受けて，X 社による追加調査の結果，再発防止策及び未知マルウェア対策の計画を E 社 G 部長に説明し，理解を得た。

設問 1　〔IT 部による調査〕について，(1)，(2)に答えよ。

(1)　本文中の下線①の動作を実現するためには，C&C サーバでどのような仕組みが必要か。表 3 の記載内容を用いて，40 字以内で具体的に述べよ。

(2)　本文中の下線②について，〔モバイラのテレワーク環境〕で述べられている機能を用いて実現する方法が二つある。どの機能でブロックすべきか。それぞれ 20 字以内で答えよ。

設問 2　図 4 中の［　a　］に入れる適切な字句を，5 字以内で答えよ。

設問 3　〔侵入経路と被害状況の調査〕について，(1)，(2)に答えよ。

(1)　本文中の［　b　］，［　c　］に入れる適切な字句を，それぞれ 10 字以内で答えよ。

(2)　本文中の［　d　］，［　e　］に入れる具体的な保管場所を，〔モバイラのテレワーク環境〕を考慮して，それぞれ 10 字以内で答えよ。

設問 4　表 4 中の［　f　］に入れる適切な字句を，5 字以内で答えよ。

設問 5　〔未知マルウェア対策の検討〕について，(1)～(4)に答えよ。

(1)　本文中の下線③について，役に立たない理由を 40 字以内で述べよ。

(2)　表 5 中の下線④について，具体例を二つ，それぞれ 25 字以内で述べよ。

(3)　本文中の下線⑤について，どのような攻撃を想定しているか。20 字以内で述べよ。

(4)　本文中の下線⑥について，VDI 以外のクラウドサービスに関して，セキュリティガイドラインの変更が必要な項目を図 1 中の番号で答えよ。また，変更後の案を 60 字以内で述べよ。