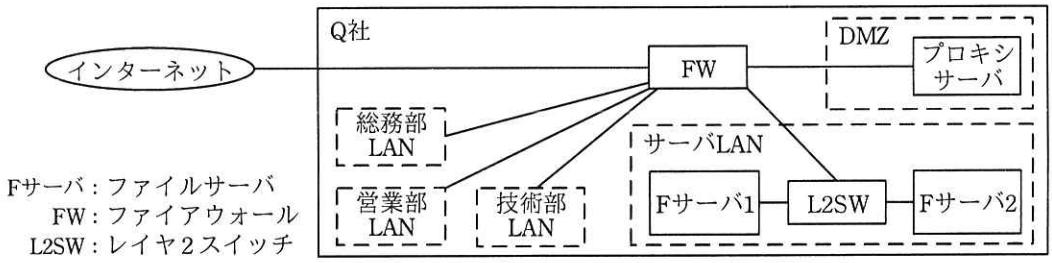
問３　PC のマルウェア対策に関する次の記述を読んで，設問 1～3 に答えよ。

Q 社は，従業員 100 名の金属加工会社である。Q 社には，総務部，営業部及び技術部がある。

Q 社では，全従業員に PC を貸与している。総務部員の PC は総務部 LAN に，営業部員の PC は営業部 LAN に，技術部員の PC は技術部 LAN に接続されている。業務に必要なソフトウェアを自らインストールして使用したいという各部からの要求に対応するために，貸与している PC の従業員の利用者 ID に管理者権限を付与している。

〔Q 社のネットワーク構成〕

Q 社の情報システムの管理は，総務部情報システム係の D 主任と E さんが行っている。Q 社のネットワーク構成を図 1 に示す。



注記 1　PC の記載は省略している。
注記 2　プロキシサーバには，グローバル IP アドレスを固定で割り当てている。
注記 3　総務部 LAN，営業部 LAN 及び技術部 LAN 内の各 PC，並びに F サーバ 1 及び F サーバ 2 には，プライベート IP アドレスを固定で割り当てている。

図 1　Q 社のネットワーク構成（抜粋）

F サーバ 1 及び F サーバ 2 には，PC 上の Web ブラウザを使ってアクセスする。利用者 ID 及びパスワードでログインした後，ファイルの格納及び取り出しが行える。F サーバ 1，F サーバ 2 及び PC のそれぞれの hosts ファイルには，プロキシサーバ，F サーバ 1 及び F サーバ 2 のホスト名と IP アドレスが登録されている。

プロキシサーバの機能概要を表 1 に示す。

表1　プロキシサーバの機能概要（抜粋）

機能名	機能概要
URL フィルタリング機能	・V 社の URL フィルタリングソフトが組み込まれており，URL フィルタリングルール（以下，UF ルールという）を用いて，指定した URL へのアクセスを許可又は拒否することができる。 ・UF ルールは，アクセス元の IP アドレス範囲ごとにそれぞれ別のルールを設定することができる。 ・一つの UF ルールは，次の三つのリストから成り，上から順に適用される。 －管理者許可リスト：管理者が設定できる，アクセスを許可する URL のリスト －管理者拒否リスト：管理者が設定できる，アクセスを拒否する URL のリスト －V 社拒否リスト：V 社が提供する，アクセスを拒否する URL のリスト ・管理者許可リストに，“全て”と記載すると，全ての URL へのアクセスが許可される。管理者拒否リストに，“全て”と記載すると，管理者許可リストで許可した URL 以外の URL へのアクセスが拒否される。管理者許可リストに何も設定しないと，そのリストはスキップされる。管理者拒否リストも同様である。 ・どの UF ルールにも該当しない場合は，アクセスは許可される。
ログ機能	・アクセスの日時，アクセス元 IP アドレス，URL 並びに，許可又は拒否の結果をアクセスログとして保存する。

注記1　V 社拒否リストは，V 社サイトから適時ダウンロードされる。
注記2　Q 社では，管理者許可リスト及び管理者拒否リストに何も設定していない。

Q 社では，PC 及びサーバに，V 社のマルウェア対策ソフトを導入し，リアルタイムスキャンを有効にしている。マルウェア定義ファイルは，PC では起動時及び毎朝 9 時に，サーバでは毎朝 9 時に，自動で V 社のマルウェア定義ファイル配布サイト（以下，V 社配布サイトという）に HTTPS で接続し，更新している。PC の利用者及びサーバの管理者は，マルウェア対策ソフトの画面の操作によってマルウェア定義ファイルを手動で更新することもできる。さらに，別の PC を用いてマルウェア定義ファイルを V 社配布サイトから手動でダウンロードし，そのファイルを保存した DVD-R を用いて更新することもできる。F サーバ 1 及び F サーバ 2 がインターネットと通信するのは，マルウェア定義ファイルの更新時だけである。

F サーバ 1 及び F サーバ 2 に，OS 及びアプリケーションソフトウェアの脆弱性修正プログラムを適用する場合，E さんが，各ベンダのサイトから脆弱性修正プログラムを PC にダウンロードして DVD-R に保存し，サーバに適用している。

E さんは，週次アクセスログ調査として，毎週月曜日の 10 時に，前週の月曜日から日曜日までの F サーバ 1 及び F サーバ 2 へのアクセスログを調査している。

FW は，ステートフルパケットインスペクション型である。FW では，アドレス変換機能を使用していない。FW のフィルタリングルールを表 2 に示す。

表2　FWのフィルタリングルール

項番	送信元	宛先	サービス	動作
1	プロキシサーバ	インターネット	HTTP，HTTPS	許可
2	サーバLAN，総務部LAN， 営業部LAN，技術部LAN	プロキシサーバ	代替HTTP[1]	許可
3	総務部LAN，営業部LAN，技術部LAN	Fサーバ1	HTTPS	許可
4	総務部LAN，営業部LAN，技術部LAN	Fサーバ2	HTTPS	許可
⋮	⋮	⋮	⋮	⋮
9	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5～8には，HTTP及びHTTPSに関するルールはない。
注[1]　代替HTTPのポート番号は，8080である。

〔不審なログインの発見と対応〕

Eさんが，12月9日月曜日に週次アクセスログ調査をしたところ，12月6日の11時から13時にFサーバ1及びFサーバ2にログインを試みて失敗した記録が多数見つかった。アクセス元は，営業部のGさんのPC（以下，PC-Gという）であった。Eさんが，10時40分にGさんに電話で問い合わせたところ，12月6日は，Fサーバ1及びFサーバ2にはログインを試みていないとのことであった。Eさんは，PC-Gがマルウェアに感染したおそれがあると考え，①マルウェア感染拡大防止のためのPC-Gの初動対応をGさんに指示した。また，Gさんへの代替PCの貸出しとPC-Gの回収を行い，PC-Gについてはマルウェア感染への対応として，ディジタルフォレンジックスによる調査を行うことにして②必要な情報を取得した。

Eさんからマルウェア感染のおそれがあるという報告を受けたD主任は，PC-Gで［　a　］という方法を使って［　b　］をした後に，フルスキャンを実施するようEさんに指示した。さらに，図2に示すマルウェアへの対処をQ社全体に指示することにした。

(1) マルウェア対策ソフトによる対処について
貸与しているPCで，［　c　］という方法を使って［　b　］をした後，フルスキャンを実施する。
(2) 報告について
上記(1)の結果を情報システム係に報告する。

図2　マルウェアへの対処

Eさんは，PC-Gのフルスキャンで検出されたマルウェア（以下，マルウェアXという）の駆除を16時に完了した。Eさんは，マルウェアXへの感染の経緯を確認するために，GさんにPC-Gの使用状況をヒアリングした。

Eさんは，図3に示す調査結果を，12月10日の13時にD主任に報告した。

(1) GさんのPC-Gの使用状況
- 12月6日9時にPC-Gを起動した。
- 10時に，インターネットの検索サイトでファイル比較ツールを検索した。検索して見つかったサイト（以下，サイトPという）にあったツールPをダウンロードした。その後，管理者権限を用いてツールPをインストールした。
- 11時にツールPを起動した。
- 17時にPC-Gをシャットダウンした。
- 12月6日は，Fサーバ1及びFサーバ2にはログインしていない。
- 12月9日9時に，PC-Gを起動した。

(2) マルウェアXに関する情報
- V社のサイトに，マルウェアXに関する次の情報が掲載されていた。
  - マルウェアXは，ツールPを装っている。
  - C&CサーバのURLのリスト（以下，Cリストという）がマルウェア中に保持されている。
  - マルウェア中のパスワードリストを使って，hostsファイルに登録されている機器へのログインを試行する。ログインが成功すると，その機器からファイルをダウンロードし，C&Cサーバにアップロードする。
- V社は，マルウェアXに対応したマルウェア定義ファイルを12月9日10時にリリースした。

(3) V社拒否リストに関する情報
- CリストにURLは，11月25日にV社拒否リストに追加されていた。

(4) プロキシサーバのアクセスログの調査
- アクセス元IPアドレスがPC-Gであるアクセスを，プロキシサーバのアクセスログで，12月9日17時から3か月遡って調査した。調査の結果，CリストのURLへのアクセスは，12月6日に1件だけであり，そのアクセスはURLフィルタリング機能で拒否されていた。

（省略）

(7) その他
- 12月9日17時に，Q社全体でのフルスキャンでマルウェアは検出されなかったことを確認した。
- 12月9日0時から17時までのFサーバ1及びFサーバ2のアクセスログに，ログインの失敗の記録はなかった。

図3　調査結果

報告を受けたD主任は，プロキシサーバに関して次の2点を指示した。

- Q社内からサイトPに接続できないようにするための管理者拒否リストの設定変更
- <u>③プロキシサーバのアクセスログに関して調査すべき範囲の漏れをカバーするための追加調査</u>

Eさんは，設定変更したこと，及び追加調査の結果，問題がなかったことをD主任に報告した。D主任とEさんは，図3，設定変更の実施及び追加調査の結果を総務部長に報告した。総務部長は，今回のマルウェアXの感染を踏まえ，追加のマルウェア対策の検討を指示した。D主任とEさんは，次の項目を検討することにした。

項目1：万が一マルウェアに感染した場合の被害拡大を防ぐ対策

項目2：マルウェア感染のリスクを低減する対策

〔項目1の検討〕

D主任とEさんは，PCがマルウェアに感染した場合，Fサーバ1及びFサーバ2にも影響があり得ると考えた。そこで，従業員が，所属している部以外のLANにPCを接続することを禁止した上で，FW及びプロキシサーバの設定変更の案を次のとおりまとめた。

・Fサーバ1の利用者を総務部員及び営業部員に，Fサーバ2の利用者を技術部員にそれぞれ振り分けて，④FWのフィルタリングルールのうちの二つのルールについて，送信元を変更する。

・サーバLANとインターネットとの間の通信を運用に必要なものだけにするために，アクセス元がサーバLANのUFルールを表3のとおりに設定する。

表3　アクセス元がサーバLANのUFルール

リスト	URL
管理者許可リスト	d
管理者拒否リスト	e
V社拒否リスト	（省略）

D主任とEさんは，設定の変更は直ちに実施できると考え，変更内容を総務部長に報告し，許可を得て設定を変更した。

〔項目2の検討〕

D主任とEさんは，マルウェア感染のリスクを低減するために，管理者権限の付与は，情報システム係の利用者IDに限定するのがよいと考えた。さらに，あらかじめ

登録した実行ファイルだけの実行を，ファイルのハッシュ値を比較することによって許可するソフトウェア（以下，Y ソフトという）の導入を検討することにした。E さんは，Y ソフトを利用する上で注意点はないのかと，D 主任に質問した。D 主任は，次のように答えた。

・⑤ハッシュ値の登録変更が必要になる場合がある。

・⑥ある種のマルウェアでは実行を禁止できない。

D 主任と E さんは，Y ソフトのメリットとデメリットの確認，及び導入案の作成を進めた。

設問 1　〔不審なログインの発見と対応〕について，(1)～(4)に答えよ。

(1)　本文中の下線①について，初動対応の内容を 15 字以内で述べよ。

(2)　本文中の下線②について，どのような情報か。10 字以内で答えよ。

(3)　本文中の［　a　］に入れる適切な方法を 35 字以内で，本文及び図 2 中の［　b　］に入れる適切な対応を 20 字以内で，図 2 中の［　c　］に入れる適切な方法を 25 字以内でそれぞれ述べよ。

(4)　本文中の下線③について，追加調査の範囲を 25 字以内で具体的に述べよ。

設問 2　〔項目 1 の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線④について，変更する二つのルールの項番と，それぞれの変更後のルールにおける送信元の内容を答えよ。

(2)　表 3 中の［　d　］，［　e　］に入れる適切な設定内容を答えよ。

設問 3　〔項目 2 の検討〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑤について，どのような場合か。30 字以内で具体的に述べよ。

(2)　本文中の下線⑥について，どのようなマルウェアか。35 字以内で具体的に述べよ。