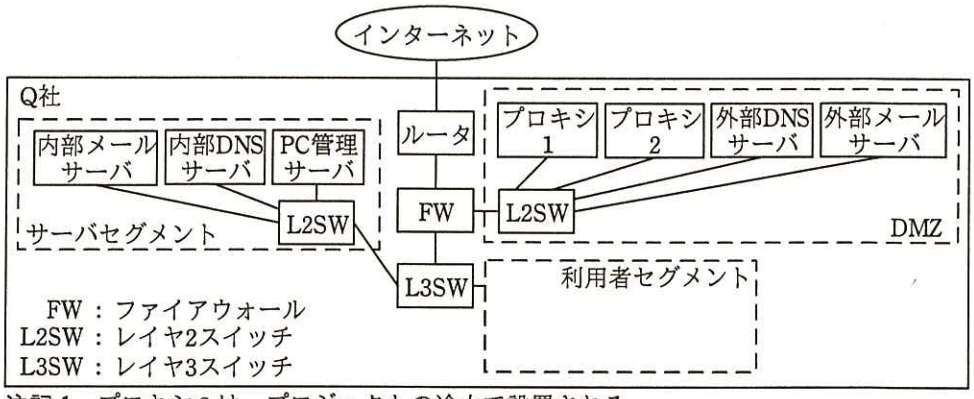
問３　プロキシサーバによるマルウェア対策に関する次の記述を読んで，設問 1～4 に答えよ。

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。