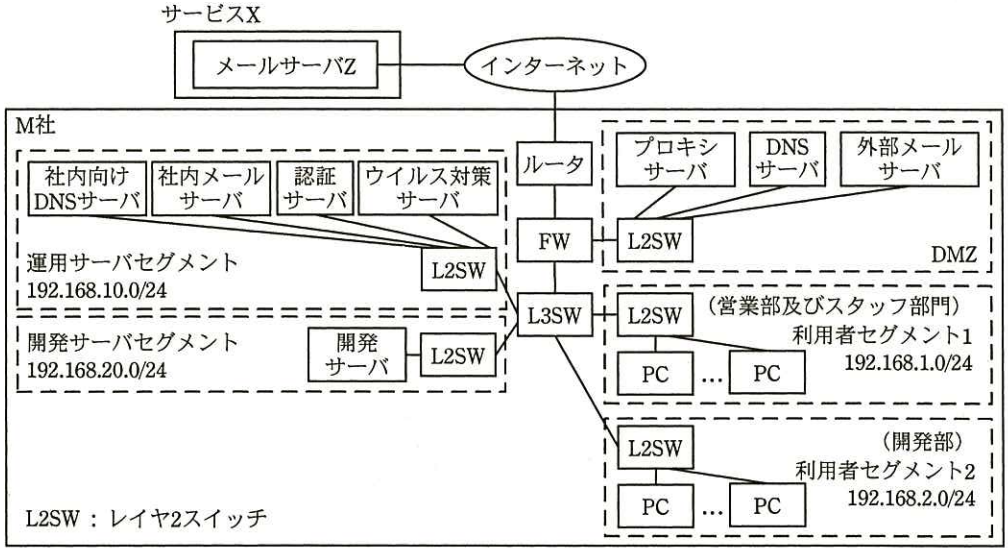
問 3　マルウェア感染への対応に関する次の記述を読んで，設問 1～4 に答えよ。

M 社は，従業員数 200 名のソフトウェアパッケージ開発会社であり，開発部，営業部及びスタッフ部門がある。

開発部は，ソフトウェアパッケージの開発・保守を行っている。営業部は，顧客を訪問し，製品紹介，製品販売及び顧客管理を行っている。スタッフ部門は，M 社のスタッフ業務全般を担当しており，総務部，経理部，情報システム部（以下，情シ部という）などから成っている。情シ部では，M 社の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への対応を行っている。M 社のネットワーク構成を図 1 に，M 社のサーバの機能一覧を表 1 に示す。

M 社のネットワークでは，ファイアウォール（以下，FW という）とレイヤ 3 スイッチ（以下，L3SW という）でネットワークのアクセス制御を行っている。FW のフィルタリングルールを表 2 に，L3SW のフィルタリングルールを表 3 に示す。



注記 1　192.168.1.0/24，192.168.2.0/24，192.168.10.0/24 及び 192.168.20.0/24 は，ネットワークアドレスを示す。

注記 2　PC のブラウザは，ポート番号 8080 でプロキシサーバを経由してインターネットアクセスするように設定されている。

注記 3　PC のデフォルトゲートウェイには，L3SW を設定している。

注記 4　L3SW においては，DMZ 及びインターネット宛てのパケットは，FW に転送されるようにルーティング設定が行われている。

図 1　M 社のネットワーク構成

表１　M 社のサーバの機能一覧（抜粋）

サーバ名	機能
外部メールサーバ	・電子メール（以下，メールという）の中継機能 ・外部からのメールフィルタリング機能（現状は無効） －フィルタリングのルールとして，ホワイトリストに許可，ブラックリストに拒否の指定が可能である。 －ホワイトリスト及びブラックリストには，送信元メールサーバの IP アドレスのリスト及び送信ドメイン名のリストがある。 －ホワイトリスト及びブラックリストの両方にマッチした場合は，ホワイトリストを優先する。
認証サーバ	・利用者の氏名，所属及びメールアドレスの管理機能 ・利用者認証機能
ウイルス対策サーバ	・ウイルス定義ファイル配信機能 －半日ごとに最新のウイルス定義ファイルをプロキシサーバ経由でベンダからダウンロードし，他のサーバと PC に配信する。

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（ポート番号）	動作
1	プロキシサーバ	インターネット	全て	許可
2～7	⋮	⋮	⋮	⋮
8	ウイルス対策サーバ	プロキシサーバ	代替 HTTP（8080）	許可
9	PC [1]	プロキシサーバ	代替 HTTP（8080）	許可
10	全て	全て	全て	拒否

注記１　項番の小さいものから順に，最初に一致したルールが適用される。
注記２　項番 2～7 は，SMTP 又は DNS に関するルールである。
注 [1]　192.168.1.0/24 及び 192.168.2.0/24 の全ての IP アドレス

表３　L3SW 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	利用者セグメント 2	開発サーバセグメント	全て	許可
2	開発サーバセグメント	利用者セグメント 2	全て	許可
3	運用サーバセグメント	開発サーバセグメント	全て	許可
4	開発サーバセグメント	運用サーバセグメント	全て	許可
5	開発サーバセグメント	全セグメント [1]	全て	拒否
6	全セグメント [1]	開発サーバセグメント	全て	拒否
7	全セグメント [1]	全セグメント [1]	全て	許可

注記　項番の小さいものから順に，最初に一致したルールが適用される。
注 [1]　全てのセグメントを示し，FW，DMZ 及びインターネットを含む。

情シ部員は，運用サーバセグメントの管理を，自席の PC のブラウザから行っている。開発サーバには，M 社の機密情報であるソフトウェアパッケージのソースコード

を保管している。

営業部では，SaaS 型クラウドサービスであるサービス X を利用して顧客管理を行っている。サービス X には，営業部の PC から，HTTP の CONNECT メソッドを使用してプロキシサーバ経由でアクセスしており，プロキシサーバからサービス X へのアクセスにはポート番号 2560 を使用している。また，サービス X 内のメールサーバ Z は，M 社専用であり，製品紹介のメールを M 社の顧客に対して自動送信すると同時に，メールの写しを M 社営業部員全員に送信している。送信の際には，送信者メールアドレスとして M 社のメールアドレスを使っている。

〔情報セキュリティインシデントの発生〕

営業部の D さんから情シ部の S さんに，D さんの PC でマルウェア Y が検出されたとの報告があった。S さんが確認したところ，マルウェア Y は，既に正常に駆除されていた。S さんは，マルウェア Y について調査した。マルウェア Y の特徴は図 2 に示すとおりであった。

1. マルウェア Y の動作
   - ブラウザ又は PDF 閲覧ソフトの脆(ぜい)弱性を悪用して感染し，PC の起動時に自身が起動されるようにシステム設定を変更する。
   - 攻撃者が用意した C&C（Command & Control）サーバと通信する。
   - リモートシェルの実行，キー入力操作情報の収集などを行う。
   - ネットワークで接続された，他の PC，サーバに感染を広げる。
2. マルウェア Y と C&C サーバとのバックドア通信
   次の 2 通りがある。
   - プロキシサーバを経由せずに，TCP ポート番号 8050 を使用して，アクセスする。
   - プロキシサーバに対して，HTTP の CONNECT メソッドを使用してアクセスし，プロキシサーバから C&C サーバへは，任意のポート番号でアクセスする。

図 2　マルウェア Y の特徴

〔情報セキュリティインシデントの調査〕

情シ部で，他の全ての PC とサーバを調査したが，マルウェア Y に感染したものはなかった。

次に D さんに確認したところ，送信者メールアドレスが総務部の F さんであるメールを受信した際に，マルウェア Y が検出されたことが分かった。ところが，F さんにはそのようなメールを送信した覚えはないとのことであった。そこで，当該メールのメールヘッダを調査したところ，当該メールは，送信者メールアドレスを F さんのメールアドレスに偽装した上，外部のメールサーバから送られてきたことが分かった。添付ファイルは，PDF ファイルに偽装したものであった。

今回のインシデントでは情報漏えいの被害はなかったものの，同様なマルウェアによって情報漏えいが発生した他社の事例もあり，マルウェア対策を見直すことになった。受信メールの制限，バックドア通信の遮断，及びマルウェアから社内のサーバへの不正アクセスリスクの軽減策をそれぞれ検討するとともに，サーバの脆弱性検査を実施した。

〔受信メールの制限〕

次は，受信メールの制限についての，情シ部の K 部長と部下でセキュリティ担当の S さんの会話である。

K 部長：送信者メールアドレスのドメイン名が当社のものに偽装されていた場合は，受信者は開いてしまう可能性が高い。良い対策はないだろうか。

S さん：外部メールサーバにある，外部からのメールのフィルタリング機能を使用しましょう。具体的には，フィルタリングルールとして，送信ドメイン名のブラックリストに当社のドメイン名を指定します。

K 部長：それだと，①正規のメールも一部届かなくなるね。

S さん：そうですね。②フィルタリングルールを追加します。

〔バックドア通信の遮断〕

続いて，K 部長と S さんは，マルウェア Y と C&C サーバとのバックドア通信の遮断について検討した。次は，そのときの会話である。

S さん：マルウェア Y は，2 通りの方法で C&C サーバとの通信を試みます。一つ目は，プロキシサーバを経由しない方法であり，既に③防ぐことができています。二つ目は，マルウェア Y が，HTTP の CONNECT メソッドで任意のポート番号を用いる方法です。これについては，表 4 に示すアクセス制御ルールをプロキシサーバに設定すれば，許可するポート番号以外の通信を防ぐことができます。

表 4　プロキシサーバのアクセス制御ルール

項番	メソッド	ポート番号	動作
1	CONNECT	443	許可
2	CONNECT	全て	拒否
3	全て	全て	許可

注記　項番の小さいものから順に，最初に一致したルールが適用される。

K 部長：表 4 でアクセスを許可する通信をマルウェアが使用する場合の対策については，別途検討しよう。ところで，表 4 の設定では④業務に支障が出るので，⑤項番 1 と項番 2 の間に設定を 1 行追加する必要があるな。

〔マルウェアからサーバへの不正アクセスリスクの軽減策〕

次に，情シ部では，マルウェアから社内のサーバへの不正アクセスリスクの軽減策を検討した。開発サーバについては，現状，開発部の PC がマルウェアに感染してしまうと，そのマルウェアからアクセスされるリスクが高い。そのため，開発専用 PC を数十台，開発サーバセグメント内に置き，ソフトウェアパッケージの開発を開発専用 PC 及び開発サーバだけで行うようにし，かつ，⑥L3SW のフィルタリングルールを変更することによって，開発サーバがマルウェアからアクセスされるリスクを軽減することにした。さらに，開発専用 PC 自身がマルウェアに感染するリスクを軽減する対策も行うことにした。

一方，運用サーバセグメントのサーバについては，運用管理を行う PC がマルウェアに感染してしまうというリスクに絞って軽減することにした。具体的には，運用管理専用 PC を運用サーバセグメントに 1 台設置し，従来，情シ部の PC で行っていた運用サーバセグメントの管理を，そこで行うことにした。さらに，その運用管理専用 PC では，［ a ］を禁止することにした。

〔サーバの脆弱性検査〕

次に，情シ部で全サーバの脆弱性検査を行ったところ，OS のパスワード格納方法について，幾つかのサーバに脆弱性があることが分かった。これらのサーバでは，パスワードは，表 5 に示す二つのハッシュ値が格納される。OS の設定によって L2 ハッシュだけを格納することもできる。

表 5　L1 ハッシュと L2 ハッシュ

項目	L1 ハッシュ	L2 ハッシュ
パスワード文字種	英数字及び記号（合計 69 種）	英数字及び記号（合計 95 種）
パスワード長	1 字から 14 字まで	1 字から 127 字まで
文字列分割	8 字以上の場合は，前半 7 字と残りに分割 [1]	なし
ハッシュ値のバイト数	16 バイト（生成された二つのハッシュ値を結合）	16 バイト
ソルトの使用の有無	なし	なし

注 [1]　例えば，“1234567AB”というパスワードの場合，前半“1234567”と後半“AB”からそれぞれのハッシュ値を計算し，その 2 個の結果を結合して格納する。

次は，OS のパスワードの格納方法についての S さんと K 部長の会話である。

S さん：OS のパスワードのハッシュ値が入手できた場合に，14 字までのパスワードを総当たり攻撃で解析することを考えてみましょう。L1 ハッシュでは，前半 [b] 字までについて，最大で（$\sum_{i=1}^{[b]}$ [c]）個のハッシュ値を求めれば，同じものを後半 [b] 字までについても使うことができます。一方，L2 ハッシュでは，最大で（$\sum_{i=1}^{[d]}$ [e]）個となり，同一のパスワード長であっても，L1 ハッシュに比べ格段に増加します。

K 部長：なるほど。L1 ハッシュを格納しないように設定を変更しよう。ところで，表 5 にあるソルトを使用するとどのような効果が得られるのか。

S さん：ソルトを使用するとハッシュ値からパスワードを特定しにくくなります。

K 部長は，検討した対策案についての実施計画と，別途検討する項目についての検討時期を経営陣に報告し，対策を進めた。

設問 1　〔受信メールの制限〕について，(1)，(2)に答えよ。

(1)　本文中の下線①について，届かなくなるメールを 30 字以内で述べよ。

(2)　本文中の下線②について，追加するフィルタリングルールを 50 字以内で述べよ。

設問 2　〔バックドア通信の遮断〕について，(1)～(3)に答えよ。

(1)　本文中の下線③について，その理由を 30 字以内で述べよ。

(2)　本文中の下線④について，支障が出る業務を，本文中の用語を用いて 5 字以内で答えよ。

(3)　本文中の下線⑤について，追加すべき設定内容を表 4 に倣って答えよ。

設問 3　〔マルウェアからサーバへの不正アクセスリスクの軽減策〕について，(1)，(2)に答えよ。

(1)　本文中の下線⑥について，L3SW でのフィルタリングルールの変更内容を 35 字以内で述べよ。

(2)　本文中の [a] に入れる適切な禁止事項を 35 字以内で具体的に述べよ。

設問 4　〔サーバの脆弱性検査〕について，(1)，(2)に答えよ。

(1)　本文中の［　b　］～［　e　］に入れる適切な数式又は数値を答えよ。

(2)　ソルトを使用するとハッシュ値からパスワードを特定しにくくなるのはなぜか。その理由を 35 字以内で述べよ。