問4　ウイルスの駆除及び感染防止に関する次の記述を読んで，設問1～4に答えよ。

K社は，従業員数1,000名の事務機器販売会社である。K社には，人事総務部，営業部，商品管理部，情報システム部がある。K社のネットワークは図1に示すとおり，DMZと社内ネットワークで構成されている。社内ネットワークは，内部サーバネットワークと部ごとの部門ネットワークに分割されている。社内ネットワーク上のPCから，インターネット上のWebサーバへのアクセスは，DMZのプロキシサーバを経由して行うように，各PCのブラウザが設定されている。

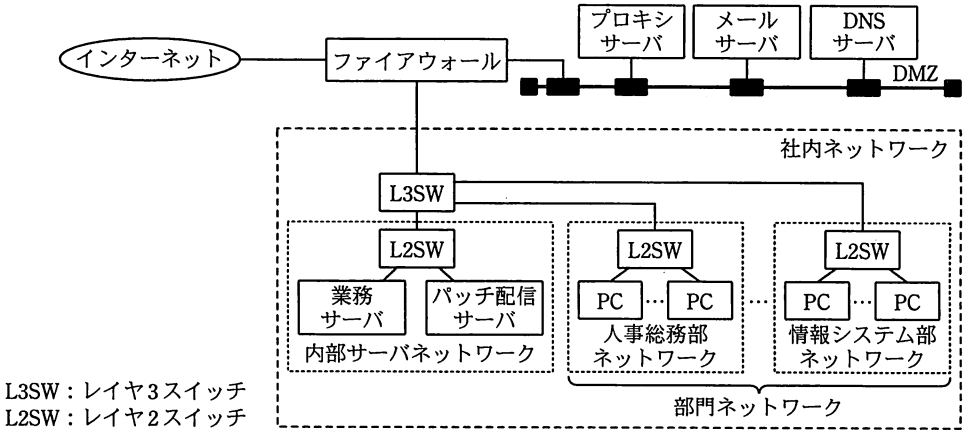

図1　K社のネットワーク（抜粋）

〔新種ウイルスの感染と駆除〕

ある日，情報システム部のA主任は，営業部のC課長から，PCの動作がおかしいので調べてほしいとの依頼を受けた。A主任は，早速，C課長の席を訪れ，PCの状態を確認したところ，全般的に動作が非常に遅く，業務に支障を来す状態となっていた。ハードウェアやソフトウェアの障害についてログを確認したが，障害発生を示す記録は見当たらなかった。そこで，A主任は，ウイルス感染を疑い，その検査を行うことにした。K社では，図2に示すウイルス駆除手順が決められており，A主任はその手順に従って作業を進めた。

(1) 感染が疑われるPCを社内ネットワークから切断する。
(2) 情報システム部では，最新のウイルス定義ファイルを入れたCD-ROMを作成し，そのCD-ROMを用いて，PCのウイルス対策ソフトのウイルス定義ファイルを最新に更新する。
(3) すべてのハードディスクドライブに対してウイルス検査を行い，検知されたウイルスの駆除を行う。
(4) すべてのウイルスの駆除を行った後，社内ネットワークに接続する。
(5) OSとアプリケーションのセキュリティパッチの適用状態を確認して，もし未適用のものがある場合は，最新のセキュリティパッチまですべてを適用する。

図2　K社のウイルス駆除手順

しかし，手順(3)まで行ったが，ウイルスは検知されなかった。セキュリティパッチの適用状態を確認したところ，前月にリリースされたOSのセキュリティパッチが適用されていないことが判明した。そこで，A主任は，PCを社内ネットワークに接続した上で，OSに対して最新のセキュリティパッチまでをすべて適用した。この時点で，PCの状態を確認したが，最初に確認したときと同様な状態であった。

A主任は，情報システム部のB課長に状況を説明して，指示を仰いだところ，現在導入されているI社製ウイルス対策ソフトとは異なるベンダのウイルス対策ソフトで，ウイルス検査を試みるよう指示があった。そこで，PCを社内ネットワークから再び切断して，I社製ウイルス対策ソフトをいったん削除した後，J社製ウイルス対策ソフトを導入し，再度，検査を行ったところ，Xウイルスを検知したという警告が表示された。A主任は，Xウイルスの駆除を行い，駆除が成功したと表示されたことを確認した。その後，J社のWebサイトで，Xウイルスについて情報収集を行った。その結果，Xウイルスは新種のウイルスであることと，図3に示す感染方法と特徴が報告されていることが分かった。

X ウイルスは，次の二つの感染方法をそれぞれ，同一サブネット内の，自らの IP アドレスを除くすべての IP アドレスに対して，IP アドレスの昇順に試みる。

感染方法 1　OS の脆弱性(1)を攻撃することによる感染

OS の脆弱性を攻撃して，感染しようとする。この動作を 10 分間隔で行う。

感染方法 2　OS の管理者 ID に対するパスワード辞書攻撃による感染

OS の管理者 ID としてよく使用される識別名のアカウントに対して，よく使われる約 1,000 個のパスワードを使用した攻撃を試みて，管理者権限を取得した上で，X ウイルス自身をコピーし実行することで感染しようとする。この動作を 30 分間隔で行う。

また，三つ目の感染方法として，PC に接続されたすべての USB メモリに対し，次の方法を試みる。

感染方法 3　USB メモリを媒介する感染

USB メモリに X ウイルス自身のコピーと，自動実行ファイルを作成して，別の PC にその USB メモリが接続されたときに感染しようとする。

感染した PC の動作の特徴として，次のことが確認されている。

特徴 1　X ウイルス自身は動的リンクライブラリであり，OS のシステムプログラムの一部として起動されるので，そのプロセスの停止を行うことはできない。

特徴 2　X ウイルスはインターネット上の特定の Web サーバに接続し，決められた名前のファイルをダウンロードした後，そのファイルを実行しようとする。今のところ，その Web サーバに決められた名前のファイルが存在しないので，ダウンロードは失敗する。Web サーバへの接続には，ブラウザのプロキシ設定情報を利用する。この動作を 60 分間隔で行う。

注(1)　この脆弱性に対するセキュリティパッチは前月にリリースされている。

図 3　X ウイルスの感染方法と特徴

〔X ウイルス駆除手順の作成〕

A 主任は，J 社製ウイルス対策ソフトをすべての PC とサーバに導入することは，費用的な問題ですぐにはできないことや，I 社製ウイルス対策ソフトでも近々検知できるようになると思われることから，C 課長以外の PC については，J 社製ウイルス対策ソフトの導入は，ひとまず行わないことにした。そこで，X ウイルスの感染方法と特徴から，X ウイルスに特化した駆除手順を作成することにした。駆除手順を作成するに当たっては，感染 PC の特定方法，X ウイルスの駆除作業，感染防止策の三つを検討した。まず，X ウイルスの感染方法と特徴を基にして，感染 PC の特定方法を検討した。X ウイルスに感染した PC の特定方法を図 4 に示す。

特定方法 1

感染方法 1 から，部門の L2SW の空きポートに接続したパケットモニタで，［ a ］パケットを監視し，連続した［ b ］に対して昇順に問い合わせ，［ c ］を要求している PC を，感染 PC として特定する。（部門の L2SW には，モニタポートは付いていない。）

特定方法 2

特徴 2 から，［ d ］サーバのログ解析を行い，［ e ］に接続を試みている PC を，感染 PC として特定する。

図 4　X ウイルスに感染した PC の特定方法

X ウイルスの駆除作業については，J 社から無償で提供されている，X ウイルス専用駆除ツールを利用することにした。

感染防止策については，感染方法 1～3 に対応して，それぞれ，図 5 の感染防止策 1～3 を行うこととした。

なお，X ウイルスに感染していない PC だけではなく，①X ウイルスの駆除に成功した PC にも，図 5 の感染防止策を行うことにした。

感染防止策 1

OS とアプリケーションの脆弱性を解消するために，一時的に②特別な接続方法で社内ネットワークに接続し，内部サーバネットワーク上にあるパッチ配信サーバから，セキュリティパッチのダウンロードを行い，最新のセキュリティパッチまでを適用する。

感染防止策 2

［ f ］

感染防止策 3

USB メモリの使用を規則で禁止するとともに，USB メモリ接続時の自動実行機能を，PC の設定で無効化する。

図 5　X ウイルスの感染防止策

以上の検討結果を踏まえ，図 6 の駆除手順を決めた。

(1)　感染 PC を特定する。（具体的な方法は図 4 参照）
(2)　感染 PC を社内ネットワークから切断する。
(3)　感染 PC に，X ウイルス専用駆除ツールを利用する。
(4)　駆除が成功したと表示された場合は，(5) へ進む。そうでない場合は，その PC の使用を禁止し，X ウイルス専用駆除ツールの更新を待って再度駆除を試みるか，ハードディスクドライブを初期化して，OS とアプリケーションの再インストールを行う。
(5)　感染防止策 1～3 を実施する。（具体的な方法は図 5 参照）
(6)　社内ネットワークに接続する。

図 6　X ウイルスの駆除手順

〔X ウイルス駆除の実行〕

A 主任は，情報システム部員とともに，まず，図 6 の (1) を実施した。その結果，営業部で使用している 180 台の PC のうち，30 台が感染 PC であることが分かった。その他の部門ネットワークで，感染 PC は発見されなかった。これら 30 台の感染 PC のうち 23 台については，前月のセキュリティパッチが適用されていなかった。残り 7 台については，OS の管理者 ID のパスワードが，感染方法 2 で使用されるパスワード辞書のものと一致していた。

また，営業部員へのヒアリング調査の結果，この X ウイルス感染は，ある営業部員が，自宅で仕事をしようとファイルを持ち帰るときに使用した，個人所有の USB メモリからの感染が発端であることが判明した。

これら 30 台の感染 PC に対して，X ウイルスの駆除手順に従って，情報システム部員が駆除作業を行い，無事，X ウイルスの駆除を完了した。また，X ウイルスに感染していない PC に対しても，感染防止策を実施し，X ウイルスへの対応を完了した。

その後，B 課長は，セキュリティパッチ適用の時期を，PC の利用者の判断にゆだねていたことが，X ウイルスの感染を広げた原因の一つと考え，K 社が保有するすべての PC への強制的なセキュリティパッチ適用と，サーバへの速やかなセキュリティパッチ適用の方法を検討するよう，A 主任に指示した。

設問 1　図 3 中の特徴 2 について，感染 PC 上のファイルを攻撃者のサーバにアップロードするようなプログラムのファイルがダウンロードされた場合，どのような被害が発生する可能性があるか。30 字以内で具体的に述べよ。

設問 2　感染 PC の特定方法について，図 4 中の［ a ］～［ e ］に入れる適切な字句を答えよ。［ a ］についてはプロトコル名を 5 字以内で，［ b ］，［ c ］についてはそれぞれ 10 字以内で，［ d ］については 5 字以内で，［ e ］については 20 字以内で答えよ。

設問 3　本文中の下線①について，駆除に成功した PC に対して，感染防止策をとらなかった場合には，どのようなことが起こり得るか。15 字以内で述べよ。

設問 4　図 5 の感染防止策について，(1)，(2)に答えよ。

(1)　感染防止策 1 を実行するに当たって，下線②のように接続する必要がある。特別な接続方法を 50 字以内で具体的に述べよ。

(2)　感染防止策 2 として，［ f ］に入れる適切な字句を，30 字以内で述べよ。