次の問1は必須問題です。必ず解答してください。

問1　マルウェア対策に関する次の記述を読んで，設問1～5に答えよ。

T社は，社員60名の電子機器の設計開発会社であり，技術力と実績によって顧客の信頼を得ている。社内のサーバには，設計資料や調査研究資料など，営業秘密情報を含む資料が多数保管されている。

T社の社員は，社内LANのPCからインターネット上のWebサイトにアクセスして，情報収集を日常的に行っている。ファイアウォール（以下，FWという）には，業務上必要となる最少の通信だけを許可するパケットフィルタリングルールが設定されており，社内LANからのインターネットアクセスは，DMZのプロキシサーバ経由だけが許可されている。T社の現在のLAN構成を図1に示す。

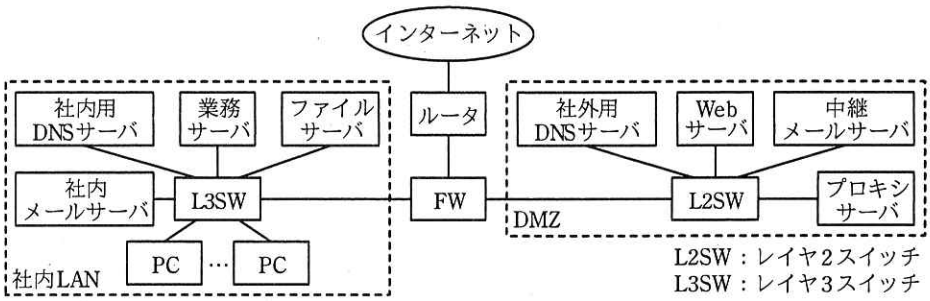

図1　T社の現在のLAN構成

T社では，マルウェアの感染を防ぐために，PCとサーバでウイルス対策ソフトを稼働させ，情報セキュリティ運用規程にのっとり，最新のウイルス定義ファイルとセキュリティパッチを適用している。

〔マルウェア対策の見直し〕

最近，秘密情報の流出など，情報セキュリティを損ねる予期しない事象（以下，インシデントという）による被害に関する報道が多くなっている。この状況に危機感を抱いたシステム課のM課長は，運用担当のS君に，情報セキュリティ関連のコンサルティングを委託しているY氏の支援を受けて，マルウェア対策を見直すよう指示した。

S君から相談を受けたY氏がT社の対策状況を調査したところ，マルウェアの活

動を抑止する対策が十分でないことが分かった。Y氏はS君に，特定の企業や組織内の情報を狙ったサイバー攻撃（以下，標的型攻撃という）の現状と，T社が実施すべき対策について説明した。Y氏が説明した内容を次に示す。

〔標的型攻撃の現状と対策〕

最近，標的型攻撃の一つである［ a ］攻撃が増加している。［ a ］攻撃は，攻撃者が，攻撃対象の企業や組織が日常的に利用するWebサイトの［ b ］を改ざんし，Webサイトにアクセスした PC をマルウェアに感染させるものである。これを回避するには，Webブラウザや OS のセキュリティパッチを更新して，最新の状態に保つことが重要である。しかし，ゼロデイ攻撃が行われた場合は，マルウェアの感染を防止できない。

マルウェアは，PC に侵入すると，攻撃者がマルウェアの遠隔操作に利用するサーバ（以下，攻撃サーバという）との間の通信路を確立した後，企業や組織内のサーバへの侵入を試みることが多い。サーバに侵入したマルウェアは，攻撃サーバから送られる攻撃者の指示を受け，サーバに保管された情報の窃取，破壊などを行うことがある。①マルウェアと攻撃サーバの間の通信（以下，バックドア通信という）は，HTTP で行われることが多いので，マルウェアの活動を発見するのは容易ではない。

Y氏は，このようなマルウェアの活動を抑止するために，次の3点の対応策をS君に提案した。

・DMZ に設置されているプロキシサーバと PC での対策の実施
・ログ検査の実施
・インシデントへの対応体制の構築

〔DMZ に設置されているプロキシサーバと PC での対策の実施〕

S君は，プロキシサーバと PC で，次の3点の対策を行うことにした。

・プロキシサーバで，遮断する Web サイトを T 社が独自に設定できる［ c ］機能を新たに稼働させる。
・プロキシサーバで利用者認証を行い，攻撃サーバとの通信路の確立を困難にする。
・プロキシサーバでの利用者認証時に，②PC の利用者が入力した認証情報がマルウェアによって悪用されるのを防ぐための設定を，Webブラウザに行う。

〔ログ検査の実施〕

S君は，ログ検査について検討し，次の対策と運用を行うことにした。

プロキシサーバは，社内LANのPCとサーバが社外のWebサーバとの間で通信した内容をログに記録している。業務サーバ，ファイルサーバ，FWなどの機器も，ログインや操作履歴をログに記録しているので，プロキシサーバだけでなく他の機器のログも併せて検査する。③ログ検査では，複数の機器のログに記録された事象の関連性も含めて調査することから，DMZにNTP（Network Time Protocol）サーバを新規に導入し，ログ検査を行う機器でNTPクライアントを稼働させる。導入するNTPサーバは，外部の信用できるサーバから時刻を取得する。NTPサーバの導入に伴って，表1に示すパケットフィルタリングルールをFWに追加する。

表1　FWに追加するパケットフィルタリングルール

項番	送信元	宛先	サービス	動作
1	[d] のNTPサーバ	[e] のNTPサーバ	NTP	許可
2	社内LANのサーバ	[d] のNTPサーバ	NTP	許可

注記　FWは，最初に受信して通過させるパケットの設定を行えば，応答パケットの通過を自動的に許可する機能をもつ。

ログ検査では，次の2点を重点的に行う。

・プロキシサーバでの利用者認証の試行が，短時間に大量に繰り返されていないかどうかを調べる。この検査によって，マルウェアによるサーバへの [f] 攻撃が行われた可能性があることを発見できる。

・セキュリティベンダやセキュリティ研究調査機関が公開した，バックドア通信の特徴に関する情報を基に，プロキシサーバのログに記録された通信内容を調べる。この検査によって，バックドア通信の痕跡を発見できることが多い。

〔インシデントへの対応体制の構築〕

S君は，④インシデントによる情報セキュリティ被害の発生，拡大及び再発を最少化するために社内に構築すべき対応体制についてまとめた。

以上の検討を基に，S君は，マルウェア対策の改善案をまとめてM課長に報告し

た。改善案は承認され，実施に移すことになった。

設問1　本文中の［ a ］～［ c ］，［ f ］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　DDoS　　イ　IPアドレス　　ウ　URLフィルタリング

エ　Webページ　　オ　キーワードフィルタリング　　カ　総当たり

キ　フィッシング　　ク　水飲み場型　　ケ　レインボー

設問2　本文中の下線①の理由について，最も適切なものを解答群の中から選び，記号で答えよ。

解答群

ア　バックドア通信の通信相手を特定する情報は，ログに記録されないから

イ　バックドア通信の通信プロトコルは，特殊なので解析できないから

ウ　バックドア通信は大量に行われるので，ログを保存しきれないから

エ　バックドア通信は通常のWebサーバとの通信と区別できないから

設問3　本文中の下線②の設定内容を，25字以内で述べよ。

設問4　〔ログ検査の実施〕について，(1)，(2)に答えよ。

(1)　本文中の下線③について，NTPを稼働させなかったときに発生するおそれがある問題を，35字以内で述べよ。

(2)　表1中の［ d ］，［ e ］に入れる適切な字句を，図1中の名称で答えよ。

設問5　本文中の下線④の対応体制について，適切なものを解答群の中から二つ選び，記号で答えよ。

解答群

ア　インシデント発見者がインシデントの内容を報告する窓口の設置

イ　原因究明から問題解決までを社外に頼らず独自に行う体制の構築

ウ　社員向けの情報セキュリティ教育及び啓発活動を行う体制の構築

エ　情報セキュリティ被害発生後の事後対応に特化した体制の構築

オ　発生したインシデントの情報を社内外に漏らさない管理体制の構築