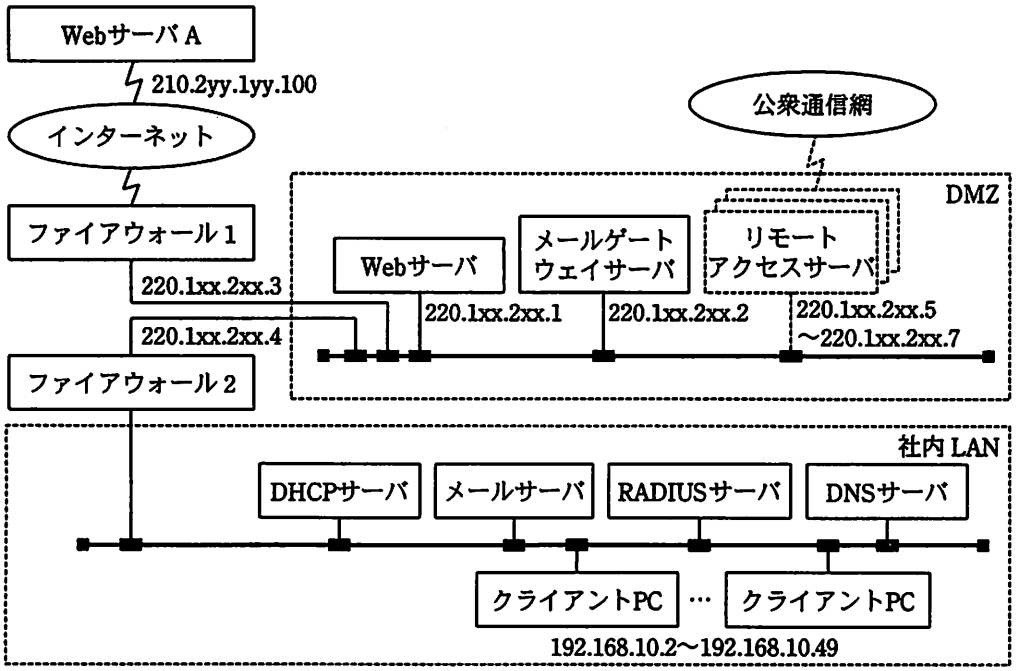
問9　ファイアウォールの設定に関する次の記述を読んで，設問1～4に答えよ。

Q社のネットワーク構成を図1に示す。なお，図中のリモートアクセスサーバは，現在はまだ設置されていない。また，WebサーバAは，外部のサーバである。



注　210.2yy.1yy.100及び220.1xx.2xx.1～220.1xx.2xx.7はIPアドレスである。

図1　Q社のネットワーク構成

Q社では，次の情報セキュリティポリシに基づいて，ファイアウォールの設定などを行っている。

〔情報セキュリティポリシ〕

・インターネットからは，自社のWebサーバ及びメールゲートウェイサーバあての通信のほか，社内LANからインターネット上のWebサーバを参照したときの応答の通信を通過させる。

・社内LANからは，電子メールを送受信するための通信及びインターネット上のWebサイトを参照するための通信だけを許可する。

・インターネットへ送信する電子メールは，メールサーバからメールゲートウェイサーバを経由して送信される。また，インターネットから受信した電子メールはメールゲートウェイサーバを経由し，直ちにメールサーバに転送される。
・ファイアウォール 1 及び 2 のアクセスログを毎日チェックし，異常なアクセスがあれば，その対応策を検討するとともに，ファイアウォールの設定変更などを行う。

ファイアウォール 1 及び 2 における通信制御のための設定は，次のとおりである。

〔ファイアウォール 1 の設定〕

(1) 静的パケットフィルタリング機能

インターネットから［ a ］への通信，及び社内 LAN からインターネットへの通信は，いずれも送信先 IP アドレス，送信先ポート番号及びプロトコルを参照して，アクセスを制御している。また，［ b ］から社内 LAN への通信は，次の動的パケットフィルタリング機能によって通過させるもの以外，すべて遮断する。

(2) 動的パケットフィルタリング機能

社内 LAN 上のクライアント PC から，TCP を使ったインターネット上の Web サイト参照に関しては，フィルタリングテーブルが表のように設定されている。クライアント PC から図 1 の Web サーバ A を参照した際の応答のパケットを通過させるために，例えばクライアント PC（192.168.10.5）からフィルタリングテーブルの行番号 10 によって許可されるパケットを送信すると，動的パケットフィルタリング機能では行番号 10 と行番号 20 の間に行番号 15 の行を挿入する。行番号 15 の行は，TCP セッションの終了パケット受信後に削除する。

表　フィルタリングテーブル（抜粋）

番号	向き	送信元 IPアドレス	送信先 IPアドレス	プロトコル	送信元 ポート番号	送信先 ポート番号	処理
10	OUT	［ c ］	anywhere	TCP	any	80	許可
20	OUT/IN	anywhere	anywhere	TCP	80	any	遮断
15	IN	［ d ］	220.1xx.2xx.4	TCP	80	1024	許可

注　anywhereは任意のIPアドレス，anyは任意のポート番号，“OUT/IN”はOUTとINのいずれかを，それぞれ意味している。

(3) ステートフルインスペクション機能

社内 LAN からインターネット上のサイトを参照したときの応答のパケットを通過させる際に，パケットの順番を管理する TCP ヘッダのシーケンス番号の妥当性を確認して通過させる。これによって，［ e ］の脅威からネットワークを防御する。

〔ファイアウォール 2 の設定〕

(1) 静的パケットフィルタリング機能

メールゲートウェイサーバとメールサーバの間の通信は，双方向とも許可する。それ以外の通信は，［ f ］及び DMZ 上のサーバから［ g ］へは，次の動的パケットフィルタリング機能によって通過させるもの以外，すべて遮断し，［ g ］からは，いずれも送信先 IP アドレス，送信先ポート番号及びプロトコルを参照して許可するか遮断するかを決定する。

(2) 動的パケットフィルタリング機能

ファイアウォール 1 の設定と同様の設定を適用する。

(3) IP アドレスの変換機能

社内 LAN からインターネットへの同時複数通信を可能にするために，NAPT を利用して，プライベート IP アドレスからグローバル IP アドレスへ変換する。これは，グローバル IP アドレス数の不足を解消するとともに，［ h ］という効果も実現している。

〔アクセスログの監視記録〕

アクセスログを基に，ある日にファイアウォール 1 で遮断された通信を送信元 IP アドレス別に分析し，図 2 のようなレポートを作成した。この結果から，［ i ］の危険性が認められるので，ファイアウォールの設定を見直した。

送信元IPアドレス	送信先IPアドレス	プロトコル	送信先ポート番号	受信件数
220.2zz.1zz.40	220.1xx.2xx.1	TCP	1	210
220.2zz.1zz.40	220.1xx.2xx.1	TCP	2	212
220.2zz.1zz.40	220.1xx.2xx.1	TCP	3	211
⋮	⋮	⋮	⋮	⋮
220.2zz.1zz.40	220.1xx.2xx.1	TCP	65534	211
220.2zz.1zz.40	220.1xx.2xx.1	TCP	65535	210

図 2　アクセスログ分析レポート

〔携帯電話を経由したリモートアクセス接続計画〕

Q 社では，営業活動の効率を上げるために，営業員にノート PC を携帯させ，携帯電話を経由して社内 LAN にアクセスできる環境を構築することを計画している。その際のセキュリティ対策は，次のとおりである。

・複数の営業員からの同時接続を可能にするために，ダイヤルアップ接続に利用するリモートアクセスサーバを DMZ に 3 台設置する。同サーバには認証機能をもたせず，社内 LAN に設置されている［ j ］で認証を行う。これによって，認証情報の安全性を確保するとともに，［ k ］を可能にする。

・ファイアウォール 2 では，リモートアクセスサーバと［ j ］及びリモートアクセスを許可された社内 LAN 上のサーバとの通信を許可するように，パケットフィルタリングの設定を追加する。

設問 1　本文中の［ a ］，［ b ］，［ f ］，［ g ］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。解答は重複して選んでもよい。

解答群

ア　DMZ　　イ　インターネット　　ウ　社内 LAN

設問 2　本文中の［ c ］，［ d ］，［ j ］に入れる適切な字句を答えよ。なお，［ j ］には，図 1 中にあるサーバの名前が入る。

設問 3　本文中の［ h ］には，社内 LAN のセキュリティを維持するのに有効な機能に関する字句が，［ k ］には，［ j ］が果たすべき役割に関する字句がそれぞれ入る。［ h ］に入れる適切な字句を 30 字以内で，［ k ］に入れる適切な字句を 20 字以内で答えよ。

設問 4　本文中の［ e ］と［ i ］に入れる攻撃手法を解答群の中から選び，記号で答えよ。

解答群

ア　IP スプーフィング　　イ　SQL インジェクション

ウ　クロスサイトスクリプティング　　エ　パスワードクラッキング

オ　ポートスキャン