問題５　次のパケットフィルタリングに関する記述を読み，各設問に答えよ。

Ｊ社では，図のように２つのファイアウォールにより DMZ と社内 LAN の２つのセグメントに分けられたネットワークを構築している。

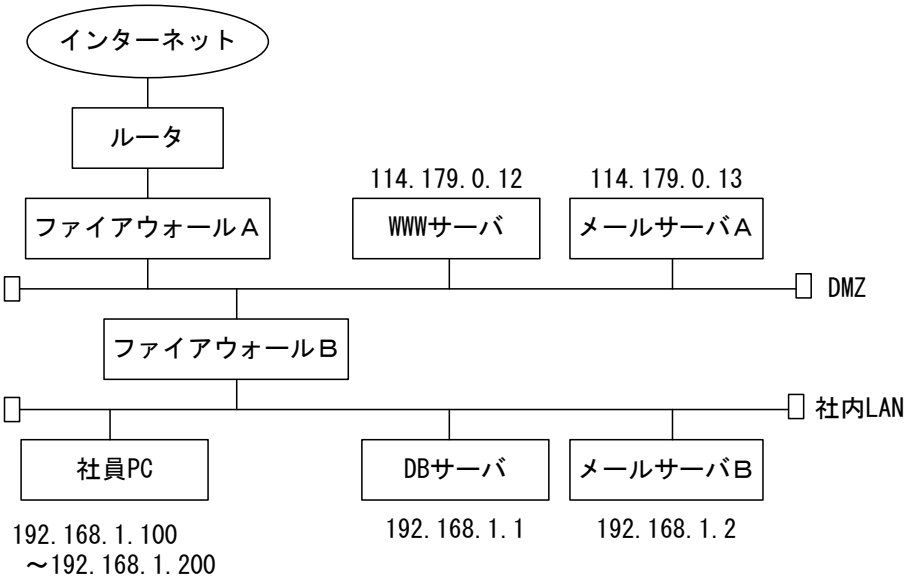

図１　Ｊ社のネットワーク構成

各サーバは次のような役割を持っている。

［WWW サーバ］

Ｊ社の Web ページをインターネットに公開する。Ｊ社の商品を紹介するページもあり，WWW サーバに保存されている CGI プログラムで DB サーバをアクセスして，商品情報を表示している。

［メールサーバＡ］

メールサーバＢおよび社外との電子メールの送受信を行う。

［メールサーバＢ］

社内 LAN の電子メールの送受信とメールサーバＡとの間で電子メールの送受信を行う。

［DB サーバ］

WWW サーバで利用するデータを格納する。

なお，社員 PC から WWW サーバとメールサーバＡへのアクセスは許可されていない。また，社員 PC が社外と電子メールを送受信する場合は，次のような手順で行う。

［社員 PC から社外へ電子メールを送信する場合］

社員 PC からメールサーバＢに転送された後，メールサーバＢからメールサーバＡへ転送して社外に送信される。

［社外からの電子メールを社員 PC で受信する場合］

メールサーバＡに転送された社員あての電子メールは，メールサーバＢへ転送される。社員 PC はメールサーバＢから電子メールを受信する。

ネットワーク上で利用するプロトコルとポート番号の対応は表１のようになっている。

表１　プロトコルとポート番号の対応

サービス	プロトコル	ポート番号
WWW	HTTP	80
電子メール転送	SMTP	25
電子メール受信	POP3	110
DB アクセス	DBMS 専用	3306

＜設問１＞　DMZ の説明として適切なものを解答群から選べ。

(1) の解答群

ア．外部ネットワークからの不正侵入に対処するように設置する機器。

イ．内部ネットワークから外部ネットワークへ情報を流出させないために暗号化する。

ウ．外部ネットワークからの情報に悪意のあるプログラムが含まれているかを判断するための仕組みである。

エ．外部ネットワークと内部ネットワークの間の領域で，外部ネットワークからアクセスさせる機器を設置する。

＜設問２＞　次のファイアウォールのフィルタリングに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ファイアウォールＡのパケットフィルタリング設定を表２に，ファイアウォールＢのパケットフィルタリング設定を表３に示す。

パケットフィルタリングでは，送信元の IP アドレス，あて先の IP アドレス，接続先のポート番号から通信の許可と拒否を制御する。上の行の規則から順番に調べ，最初に条件に一致した動作を行う。

なお，応答パケットは動的フィルタリングにより自動的に許可されるので，設定は不要である。

表２　ファイアウォールＡのフィルタリング設定

送信元 IP アドレス	あて先		動作
	IP アドレス	ポート番号	
任意	114.179.0.12	(2)	許可
任意	114.179.0.13	(3)	許可
114.179.0.13	(4)	25	許可
任意	任意	任意	拒否

表３　ファイアウォールＢのフィルタリング設定

送信元 IP アドレス	あて先		動作
	IP アドレス	ポート番号	
114.179.0.12	(5)	(6)	許可
114.179.0.13	192.168.1.2	25	許可
(7)	(8)	25	許可
任意	任意	任意	拒否

(2)，(3)，(6) の解答群

ア．25　　イ．80　　ウ．110　　エ．3306

(4)，(5)，(7)，(8) の解答群

ア．114.179.0.12　　イ．114.179.0.13

ウ．192.168.1.1　　エ．192.168.1.2

オ．任意

＜設問３＞　次のファイアウォールに関する記述中の［　　］に入れるべき適切な字句を解答群から選べ。

ファイアウォールによる制御は，IP アドレスによるパケットフィルタリング型と，［(9)］型がある。前者は IP アドレスやポート番号で制御をするもので，後者は通信を中継するプロキシサーバを利用し，データの内容まで見て制御しながら社内ネットワークとインターネットの間で直接通信ができないようにするものである。

(9) の解答群

ア．アプリケーションゲートウェイ　　イ．ポートスキャン

ウ．セション　　エ．ドメインネーム