問040006問題

パケットフィルタリングに関する次の記述を読んで、設問１、２に答えよ。

Ｘ社では、図に示すネットワークを構築し、インターネットへのＷｅｂサイトの公開と電子メール(以下、メールという)の送受信を行っている。

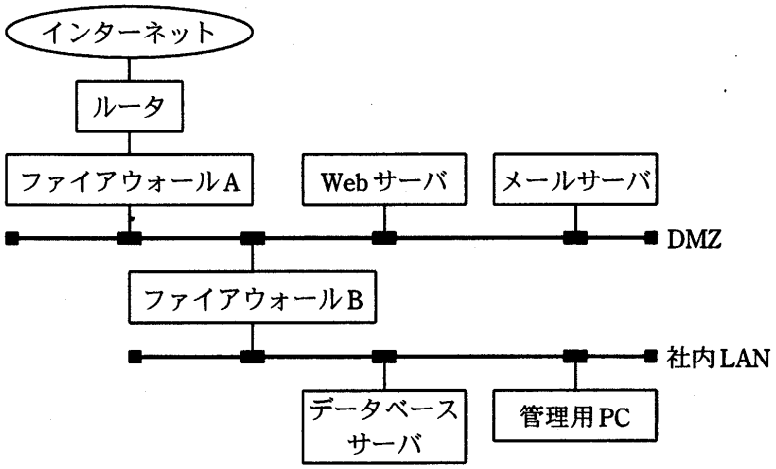

図　Ｘ社のネットワーク構成

Ｘ社のネットワークは二つのファイアウォールによって、ＤＭＺ及び社内ＬＡＮの二つのセグメントに分けられている。Ｗｅｂサーバ、メールサーバ及びデータベースサーバ(以下、ＤＢサーバという)は、それぞれ次の役割を果たしている。

（１）Ｗｅｂサーバ

Ｗｅｂサイトとして、自社の情報をインターネットに公開する。Ｗｅｂサーバ上では、社外との取引情報を処理するプログラムが動作する。このプログラムが利用するデータはＤＢサーバ上に格納される。

（２）メールサーバ

社外とのメールの送受信を行う。また、取引先に対してメールを自動配信するプログラムが動作する。メール配信のためのデータはＤＢサーバ上に格納される。

（３）ＤＢサーバ

Ｗｅｂサーバ及びメールサーバで利用するデータを格納する。

社内ＬＡＮに接続された管理用ＰＣからは、ＳＳＨを使った各サーバへのログイン操作と、メールサーバを介した外部とのメール送受信が可能である。管理用ＰＣから自社Ｗｅｂサーバの参照はできるが、社外Ｗｅｂサイトの利用は許可されていない。

ネットワーク上で使われるプロトコルとポート番号を表１に示す。

表1　プロトコルとポート番号

サービス	プロトコル	ポート番号
Web	HTTP	80
メール転送	SMTP	25
セキュアシェル（遠隔ログイン）	SSH	22
メール受信	POP3	110
DBアクセス	DB専用	1999

設問１　次の記述中の［　　］に入れる正しい答えを、解答群の中から選べ。解答は重複して選んでもよい。

インターネットとＤＭＺをつなぐファイアウォールＡのパケットフィルタリングの設定を表２に示す。また、ＤＭＺと社内ＬＡＮをつなぐファイアウォールＢのパケットフィルタリングの設定を表３に示す。

フィルタリングの設定ルールは、送信元のＩＰアドレス、あて先のＩＰアドレス及び接続先ポート番号を指定して通信の許可／拒否を制御する。設定は上の行のルールから調べて，最初に条件が合致した行の動作を実行する。また、応答パケットについては動的フィルタリング機能によって自動的に許可されるので設定は不要なものとする。

表2　ファイアウォールＡのフィルタリングの設定

条件			動作
送信元	あて先	ポート番号	
任意	Webサーバ	80	許可
任意	メールサーバ	25	許可
a	任意	b	許可
任意	任意	任意	拒否

ａ，ｃに関する解答群

ア　ＤＢサーバ　　イ　Ｗｅｂサーバ　　ウ　管理用ＰＣ

エ　メールサーバ　　オ　任意

ｂ，ｄに関する解答群

ア　２２　　イ　２５　　ウ　８０

エ　１１０　　オ　１９９９

表3　ファイアウォールBのフィルタリングの設定

条件			動作
送信元	あて先	ポート番号	
Webサーバ	DBサーバ	1999	許可
メールサーバ	DBサーバ	1999	許可
管理用PC	c	d	許可
管理用PC	メールサーバ	22	許可
管理用PC	メールサーバ	25	許可
管理用PC	Webサーバ	80	許可
管理用PC	Webサーバ	22	許可
任意	任意	任意	拒否

設問２　X社のネットワークでは、ファイアウォールによるパケットフィルタリングによって、インターネット接続に伴うセキュリティ上のリスクを低減しているが、パケットフィルタリングは、すべての脅威に対する防御とはならない。パケットフィルタリングによって防ぐことができるセキュリティ上のリスクとして、正しい答えを解答群の中から二つ選べ。

解答群

ア　Ｗｅｂサイトとやり取りされるデータの盗聴や改ざん

イ　ＷｅｂサイトへのＳＱＬインジェクション攻撃

ウ　インターネットからＤＭＺ内のサーバへの許可されていないポートでの接続

エ　インターネットから社内ＬＡＮへの不正アクセスによる攻撃

オ　メールによる社内からのファイル流出