

問040004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。

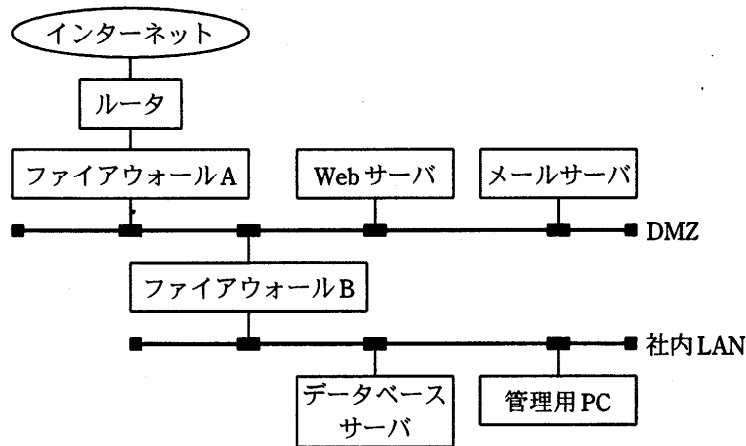


図 X社のネットワーク構成

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
<input type="text" value="a"/>	任意	<input type="text" value="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