ネットワークセキュリティ

問５ Check □ □ □ 【20011年春期 応用情報 問9】

サーバへのサイバー攻撃対策に関する次の記述を読んで，設問１～３に答えよ。

Ｄ社はおもちゃを扱う中堅商社であり，取扱商品を紹介するためにWebサーバやデータベースサーバ（DBサーバ）などを自社で運用している。Ｄ社のネットワーク構成を図１に，各サーバの役割を表１に示す。

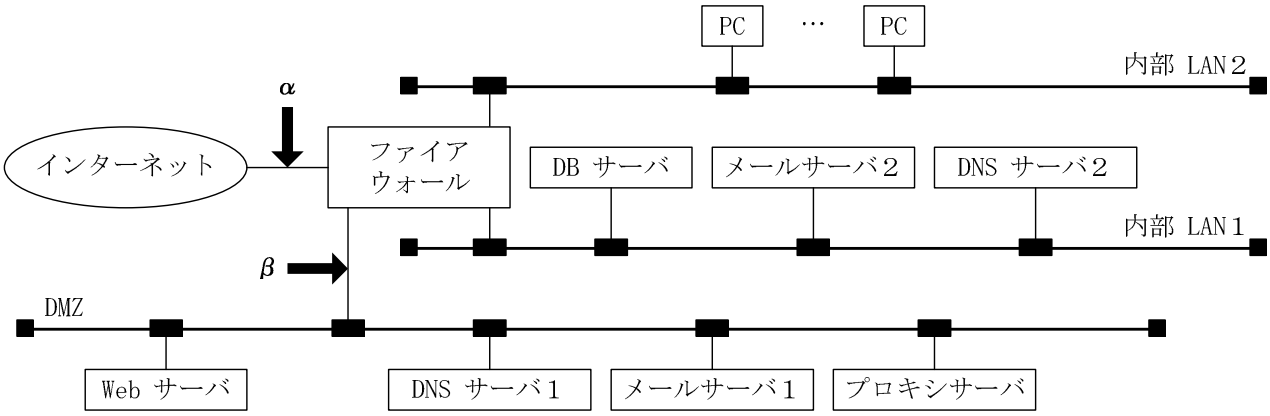

図１　Ｄ社のネットワーク構成

表１　各サーバの役割

サーバ名（ホスト名）	役割
DBサーバ	取扱商品の情報を格納し，Webサーバからのリクエストに応じて必要な情報を渡す。
DNSサーバ１	自社ドメインを管理し，インターネットからの問合せに応答する。
DNSサーバ２	自社内のホスト情報を管理し，社内からの問合せに応答する。
Webサーバ	DBサーバにアクセスすることによって，取扱商品をインターネット向けに紹介する。
メールサーバ１	自社あてのメールをインターネットから受け取り，メールサーバ２に転送する。社外あてのメールをメールサーバ２から受け取り，インターネットに転送する。
メールサーバ２	自社あてのメールをメールサーバ１から受け取る。社外あてのメールをメールサーバ１に転送する。PCからのメール送受信要求を受け付ける。
プロキシサーバ	PCからの社外へのWebアクセスを中継する。

あるとき，Ｄ社の顧客から“Webサイトが表示されない”と問合せがあった。原因を調査したところ，Webサーバが反応しない状態であったので，Webサイトの運営を一時中止して原因を探った。その結果，各サーバに対して，次のサイバー攻撃が行われていたことが判明した。

【サイバー攻撃１】Web サーバに対して，Web ページを表示するためのリクエストが大量に送られ，CPU とメモリの使用率が許容限度を超えてしまっていた。

【サイバー攻撃２】DB サーバにアクセスするプログラムの不備を利用して，データベース上の情報に不正にアクセスしようとした形跡が，Web サーバにあった。

【サイバー攻撃３】DNS プログラムが確保したメモリサイズを超えた入力を与えて，管理者権限を奪おうとした形跡が，DNS サーバ１にあった。

【サイバー攻撃４】使用可能なサービスを探した形跡が，DMZ 内の各サーバにあった。

Ｄ社では判明したサイバー攻撃に対応するために，ファイアウォールの設定を変更するとともに，ネットワーク型 IDS（Intrusion Detection System，侵入検知システム）を導入することにした。

〔ファイアウォールの設定変更〕

ファイアウォールの新しいフィルタリングルールを表２に示す。フィルタリングルールの設定は，次の方針で行うことにした。

・インターネット以外のあて先は，ホスト名で指定する。
・必要なサービスだけを通過させる。

なお，表２で用いるフィルタリングルールの記述方法は，次のとおりである。

・通信パケットの送信元，あて先及びサービスの組合せによって，許可又は拒否の動作を指定することができる。
・送信元，あて先には個別のホスト名又は“インターネット”，“DMZ”，“内部 LAN１”，“内部 LAN２”のネットワーク名又は“すべて”が指定できる。
・サービスにはポート番号（複数指定可）又は“すべて”が指定できる。ポート番号は，SMTP は 25，DNS は 53，HTTP は 80，POP3 は 110，DB サーバへのアクセスは 1521，プロキシサーバへのアクセスは 8080 とする。
・項番が小さいものから順に調べて，最初に一致したルールが適用される。

表２　ファイアウォールの新しいフィルタリングルール

項番	送信元	あて先	サービス	動作
1	内部 LAN２	メールサーバ２	25，110	許可
2	内部 LAN２	DNS サーバ２	53	許可
3	内部 LAN２	a	b	許可
4	メールサーバ２	メールサーバ１	25	許可
5	メールサーバ１	メールサーバ２	25	許可
6	Web サーバ	c	d	許可
7	メールサーバ１	インターネット	25	許可
8	プロキシサーバ	インターネット	すべて	許可
9	インターネット	Web サーバ	80	許可
10	インターネット	e	f	許可
11	インターネット	DNS サーバ１	53	許可
12	すべて	すべて	すべて	拒否

〔ネットワーク型 IDS の導入〕

Ｄ社では，早期にサイバー攻撃を検知するために，ネットワーク型 IDS を図１のαの位置に設置した。設置した IDS の概要は，次のとおりである。

・不正侵入の特徴的なパターンをシグネチャとして事前に登録し，検知した脅威の種類を示すシグネチャの識別子，脅威の名称，詳細な通信内容などをログに記録するとともに，管理者あてに警告メールで通知する機能をもつ。
・検知されるサイバー攻撃には，４段階の優先度（優先して対応する必要性の度合い）が付与されている。優先度は，優先度１が最も高く，優先度４が最も低い。

Ｄ社で判明したサイバー攻撃１～４に対応する優先度の初期値は，表３のとおりである。

表３　Ｄ社で判明したサイバー攻撃１～４に対応する優先度の初期値

サイバー攻撃の種類	優先度の初期値
サイバー攻撃１	2
サイバー攻撃２	1
サイバー攻撃３	1
サイバー攻撃４	2

Ｄ社では，IDS の優先度の設定は初期値のままとし，優先度が１，２のものを管理者に警告メールで通知する設定で，IDS の試験運用を開始した。

試験運用を開始してすぐに，IDS から管理者あてに警告メールが大量に送られるようになった。警告メールが多いと，管理者が重要な警告を見落とすおそれがあることから，Ｄ社では IDS の導入効果を維持したまま警告メールの件数を少なくするために，①IDS の設置位置を図１のβの位置に変更した。

6　情報セキュリティ

設問１　サイバー攻撃１～４について，その名称を解答群の中から選び，記号で答えよ。

解答群

ア　DoS 攻撃　　イ　SQL インジェクション
ウ　ソーシャルエンジニアリング　　エ　トロイの木馬
オ　バッファオーバフロー攻撃　　カ　ポートスキャン

設問２　Ｄ社で実施したファイアウォールの設定変更について，表２中の［ a ］～［ f ］に入れる適切な字句を答えよ。

設問３　IDS から管理者あてに送られる警告メールの大量発生後に，Ｄ社が実施した対策について，(1)，(2)に答えよ。

(1) 本文中の下線①の対策について，警告メールが減少する理由を 35 字以内で述べよ。

(2) 本文中の下線①の対策の結果，警告メールが最も効果的に減少すると考えられるサイバー攻撃の種類をサイバー攻撃１～４から選び，番号で答えよ。

設問１	サイバー攻撃１		サイバー攻撃２	
	サイバー攻撃３		サイバー攻撃４	
設問２	a		b	
	c		d	
	e		f	
設問３	(1)			
	(2)			