

第3問 ネットワークセキュリティに関する次の記述を読んで、設問1，2に答えよ。

A社では、社内のパソコン利用の増加によりネットワーク構成を見直すことにした。また、ネットワークの再構成にともないファイアウォールの設定も見直すことになった。ファイアウォールは、A社と社外を結ぶコンピュータ、LAN及びアクセス制御を設定できる。

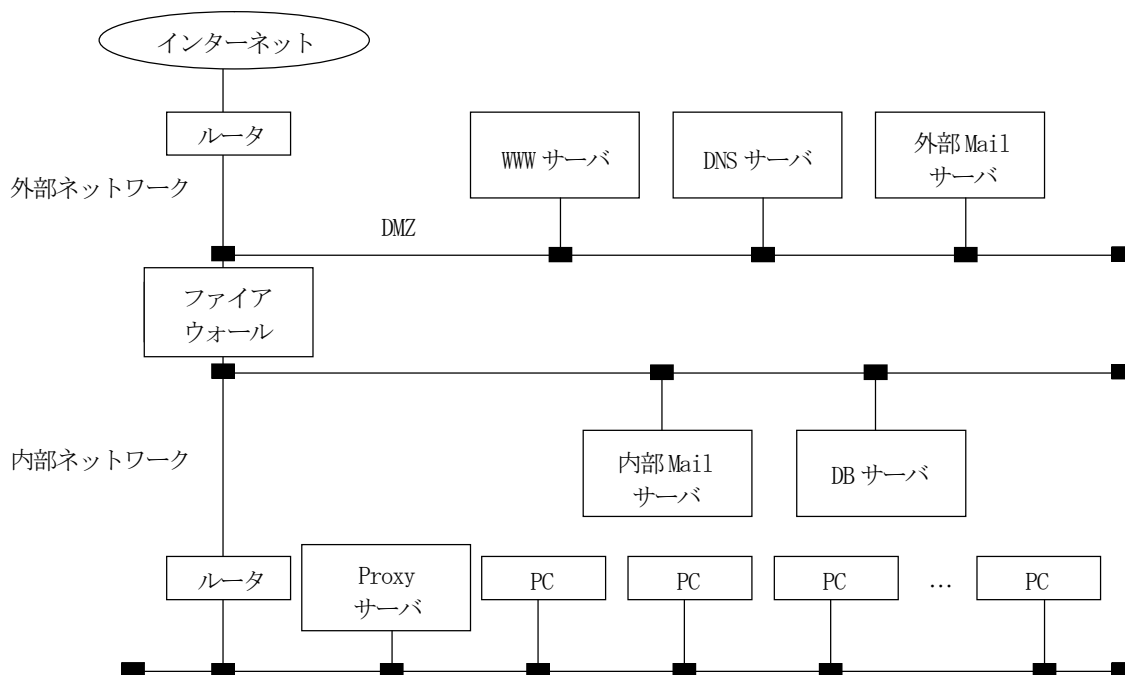


図 A社のネットワーク構成（見直し後）

A社の導入したファイアウォールに設定可能な機能は次のとおりである。

- (1) 内部ネットワーク上にあるPCがインターネット上にあるサーバと通信を行う際に、TCP/IPプロトコルの上層位のサービス（http, https, ftp, smtpなどのプロトコルや利用者が作成したアプリケーションサービス）に対してセキュリティ方針を定義することができる。
- (2) ネットワーク上に存在するコンピュータ（ホスト名）やLAN（LAN名）などの情報を利用し、サービスの許可及び禁止を設定することができる。そこでは、ネットワーク上のすべてのコンピュータやすべてのサービスを指す場合、特別な名称として“すべて”を使用できる。
- (3) ファイアウォールの動作を定義したものの集合をルールベースと呼ぶ。このファイアウォールは、到着したIPデータグラムに対して、定義されたルールベースを上から順に適用し、最初に適合したルールによって、そのIPデータグラムに対する動作を決定する。

設問1 次のファイアウォールの設定方針によって定義される表の“ルールベース”中の空欄(a)～(d)に入れるべき適切な字句を解答群の中から選び、記入せよ。

[ファイアウォールの設定方針]

- ① インターネットから送信されてくる電子メールは、必ず外部Mailサーバで受信し、外部Mailサーバから内部Mailサーバへ中継する。
- ② PCからインターネットへのメール送信は、直接外部Mailサーバを使用せず、一度内部Mailサーバに送信し、外部Mailサーバを経由してからインターネットへ送信する。
- ③ WWWサーバから内部ネットワークへのアクセスは、DB-access及びsmtpの各サービスだけ許可する。

- ④ WWW サーバへのアクセスは、インターネットからのアクセス (http, https) 及び、PC からの直接アクセスも認める。  
 ⑤ PC からインターネットへのアクセスは、http, https, ftp のプロトコルを許可し、必ずProxy サーバを経由する。  
 ⑥ 利用者 (インターネットを含む) からファイアウォールへの直接アクセスをすべて禁止する。  
 ⑦ 上記以外のアクセスはすべて禁止する。

表 ルールベース

送信元	あて先	サービス名称	動作
すべて	ファイアウォール	すべて	(a)
外部 Mail サーバ	内部 Mail サーバ	smtp	許可
内部 Mail サーバ	外部 Mail サーバ	(b)	許可
WWW サーバ	内部ネットワーク	DB-access, smtp	許可
Proxy サーバ	(c)	http, https, ftp	許可
すべて	(d)	http, https	許可
すべて	すべて	すべて	禁止

解答群

- |            |             |               |               |
|------------|-------------|---------------|---------------|
| ア WWW サーバ  | イ Proxy サーバ | ウ ファイアウォール    | エ 外部ネットワーク    |
| オ 内部ネットワーク | カ http      | キ smtp        | ク DB-access   |
| ケ https    | コ インターネット   | サ 外部 Mail サーバ | シ 内部 Mail サーバ |
| ス PC       | セ DMZ       | ソ 許可          | タ 禁止          |

設問2 設問1 で設定したルールベースに追加をすることで、制限可能なアクセスとして適切なものを解答群の中から選び、解答欄(e)に答えよ。

解答群

- ア 社内PCからDMZ上に接続されているサーバの設定を専用アプリケーションサービスによって行うこと。  
 イ 社内PCから内部ネットワーク上に接続されているサーバの設定を専用アプリケーションサービスによって行うこと。  
 ウ インターネットからDNSサーバのdnsサービスを利用すること。  
 エ 特定のユーザIDにのみインターネット上のhttp, https, ftpのサービスの利用を許可すること。