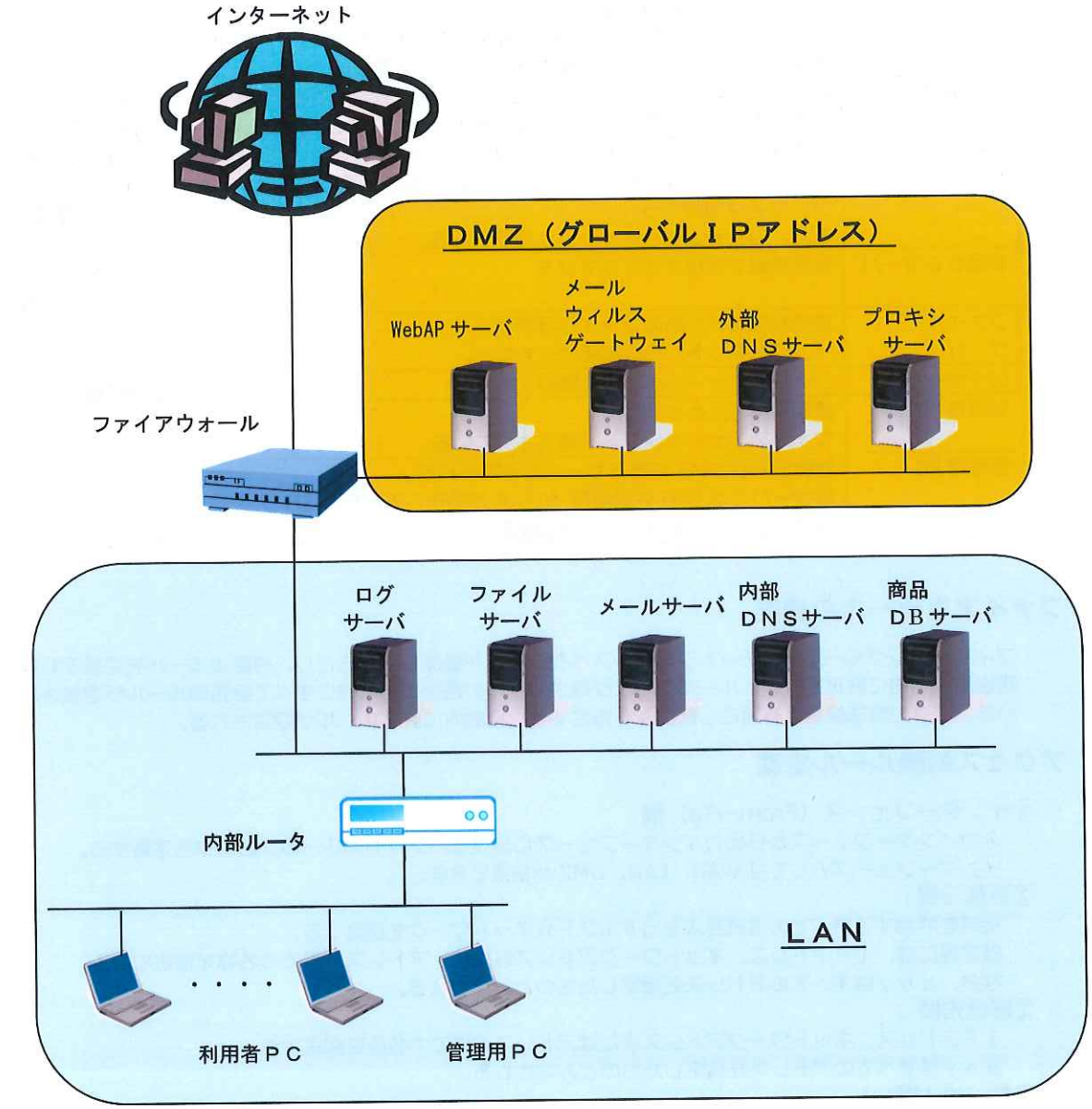
演習ファイアウォールアクセス制限ルールの設計

以下に示すネットワークにおいて「ファイアウォールの仕様」を参考にファイアウォールの提供する機能を設計し、アクセス制限ルールを作成しなさい。

ネットワーク構成



	サーバ	設定機能	サービス
1	WebAP サーバ	インターネット利用者へ向けて会社情報案内の発信と、商品情報の発信、また社内ユーザに対して社員向け情報発信。商品情報は AP サーバにより動的に社内のＤＢサーバから取得する。 社内の利用者 PC からのアクセスとインターネットからの接続の識別は送信元の IP アドレスによって行い、社員向け情報へのインターネットからのアクセスを制限する。	HTTP、HTTPS SSH（管理用）
2	メールウィルスゲートウェイ	ウィルスチェックの機能を有し、メールの宛先が自社宛てのものは社内のメールサーバへ、そうでないメールはインターネット上の他社のメールサーバへ転送する。	SMTP HTTP（管理用）
3	メールサーバ	社員用メールサーバ。メールクライアントからのメール取り込みに対してメールの配信を行う。	SMTP、POP3 SSH（管理用）
4	外部 DNS サーバ	公開用のサーバ（Web サーバ、メールウィルスゲートウェイ、プロキシサーバ）の名前解決を行う。 また、内部 DNS サーバの名前解決問合せに対して、インターネットへの問合せを行い、結果を内部 DNS サーバに応答する。	DNS SSH（管理用）
5	内部 DNS サーバ	社内のサーバ、PC およびネットワーク機器の名前解決を行う。 社外のドメインの解決については外部 DNS サーバに解決を依頼する。	DNS SSH（管理用）
6	プロキシサーバ	社内からインターネットへの HTTP、HTTPS、FTP の接続を代理する。 コンテンツフィルタリングの機能により仕事に関係のないサイトへのアクセスは制限する。 また、コンテンツのキャッシュ機能もある。	HTTP プロキシ FTP プロキシ HTTP（管理用）
7	商品ＤＢサーバ	商品情報を管理するＲＤＢＭＳ	DB-Port SSH（管理用）
8	ファイルサーバ	社内利用者のためのファイル共有サーバ。 インターネットからの利用はできない。	CIFS
9	ログサーバ	ファイアウォールのログを取得する	syslog
10	利用者 PC	業務利用のための PC。 ウィルスチェックソフトが導入されている。	
11	管理用 PC	社内および DMZ にあるサーバの管理を行う。 各サーバでは SSH や管理用 WebUI が動作しており、SSH クライアントやブラウザによりリモート管理を行う。	

ファイアウォールの機能

フィルタリングルールはステートフルインスペクションが機能しているとし、往路のルールを定義すれば、復路は自動的に許可される。ルールブロック毎にルールの最後に暗黙的にすべて拒否のルールが定義されている。ログの転送機能は有効にし転送先を指定すると自動的に許可ルールが設定される。

アクセス制限ルール定義

①インターフェース（From→To）欄
　入力インターフェースから出力インターフェースに抜けるパケットのルールブロックを定義する。
　インターフェースとしては WAN、LAN、DMZ が指定できる。
②送信元欄
　接続を開始する時点での接続要求を出すホストやネットワークを指定する。
　指定欄には、ＩＰアドレス、ネットワークアドレス以外に、アドレス定義での名称を指定できる。
　なお、ａｎｙはすべてのアドレスを指定したものとみなされる。
③送信先欄
　ＩＰアドレス、ネットワークアドレスまたはアドレス定義での名称を指定可能。
　ａｎｙはすべてのアドレスを指定したものとみなされる。
④サービス欄
　下記のサービスはプロトコル名で指定可能。また、ポート番号を直接記入することもできる。
　ａｎｙはすべてのプロトコルを指定したものとみなされる。
⑤処置欄
　ＯＫ・・接続を許可する。　ＮＧ・・接続を拒否する。

演習用ワークシート　ファイアウォールのルール設計

インターフェース From → To	送信元	送信先	サービス	処置