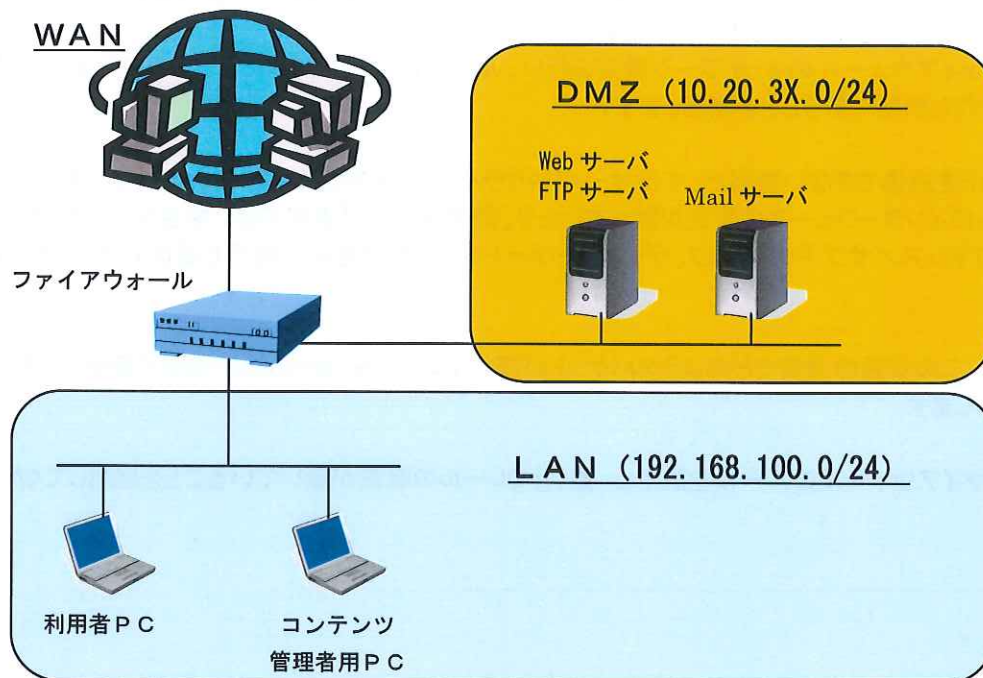


演習 ファイアウォール実機設定

以下に示すネットワークにおいてファイアウォールを設定し、正しく設定できていることを確認しなさい。

ネットワーク構成



ネットワーク環境について

	サーバ	設定機能	サービス
1	Web サーバ FTP サーバ	インターネット利用者と社内の社員へ向けて会社情報案内の発信と、商品情報の発信を行う。 Web コンテンツをアップロードするために社内から FTP 接続を行う。	HTTP、HTTPS、FTP
2	メールサーバ	社員に対してメールサービスを提供する。	SMTP/POP3
3	利用者 PC	業務利用のための PC。	
4	コンテンツ 管理用 PC	コンテンツ管理者が Web コンテンツをアップロードするために使用する	

- (1) 社内の PC からインターネットの Web サーバにアクセスができること
- (2) 社内の PC から DMZ の Web サーバにアクセスできること
- (3) 社内のコンテンツ管理用 PC から FTP サーバに FTP 接続しファイルのアップロードができること
- (4) 社内の利用者 PC から FTP サーバに接続できないこと
- (5) 社内の PC から DMZ のメールサーバを使ったメールの送受信が可能であること
- (6) DMZ のメールサーバからインターネットへメールの送信ができること
- (7) インターネットから Web サーバにアクセスできること
- (8) インターネットから FTP サーバにアクセスできないこと
- (9) インターネットからメールサーバにメールを転送できること
- (10) インターネットからメールサーバに接続しメールの受信ができないこと
- (11) ping は社内から DMZ、インターネットは通ること

- (12) DMZ からインターネットへの ping は通るが、LAN へは通らないこと
- (13) インターネットから DMZ への ping は通るが、LAN へは通らないこと
- (14) 上記の許可したもの以外通らないこと

演習手順

- (1) はじめにクライアントやサーバで検証やサービスのために必要なツールは事前にダウンロードしておいてください。(xampp、WireShark、nmap、ffftpなど)
- (2) ファイアウォールのネットワーク設定を行い、ルールはすべて許可にした状態で、全ての通信が許可された状態にあることを確認します。

このとき通信できない要因としてはサーバやクライアントの設定が誤っている以外にも、ファイアウォールのインターフェースの設定が誤っていたり、許可ルールが適切でない場合や、クライアント PC の IP アドレス／サブネットマスク、デフォルトゲートウェイの設定が不適切で通信できないなどがあります。

また、この状態の通信でどのようなパケットが流れているかを WireShark などで確認しておくことをお勧めします。

- (3) ファイアウォールのルールを設定し、適切にルールの制限が働いていることを確認してください。

演習用ワークシート ファイアウォールのルール設計（解答）

インターフェース From → To	送信元	送信先	サービス	処置
WAN → DMZ	any	WebAP サーバ	HTTP,HTTPS	OK
	any	メールウィルス ゲートウェイ	SMTP	OK
	any	外部 DNS サーバ	DNS	OK
DMZ → WAN	メールウィルス ゲートウェイ	any	SMTP	OK
	外部 DNS	any	DNS	OK
	プロキシサーバ	any	HTTP,HTTPS,FTP	OK
LAN → DMZ	any	メールウィルス ゲートウェイ	SMTP	OK
	any	プロキシサーバ	HTTP プロキシ FTP プロキシ	OK
	any	WebAP サーバ	HTTP,HTTPS	OK
	内部 DNS サーバ	外部 DNS サーバ	DNS	OK
	管理用 PC	WebAP サーバ、 外部 DNS サーバ	SSH	OK
	管理用 PC	メールウィルス ゲートウェイ、 プロキシサーバ	HTTP	OK
DMZ → LAN	WebAP サーバ	DB サーバ	DB-Port	OK
	メールウィルス ゲートウェイ	メールサーバ	SMTP	OK

