**※今回の実習は、apache、bind、postfix、dovecotが前提（4章5章）**

**●実習１０－１．UFWの状態管理**

**UFW(ファイアウォール)の状態を管理する。**

（１）UFWの状態を確認して、有効化する。

①　UFWの状態を確認する。

sudo ufw status

**コマンド→**

ステータスの状態：[ inactive ]

② UFWを有効化する。

**コマンド→**

sudo ufw enable

③ UFWを再読み込みする。

**コマンド→**

**Sudo ufw reload**

④ UFWの状態を確認する。

**コマンド→**

**Sudo ufw status**

（２）接続を確認する。

　　UFWはデフォルトのincomingポリシーはdenyのため、接続ができないことを確認する。

　　＊ただし、例外で許可されているものあるので注意する。

　　①　Apacheが動作しているか確認する。

**コマンド→**

**Sudo systemctl status apache2**

②　Apacheが起動していなければ、起動する。

**コマンド→**

**Sudo systemctl start apache**

③　ブラウザでサーバーのIPアドレスを指定して接続できないことを確認する。

　　　　[　接続できない　]

④ PCのコマンドプロンプトからpingコマンドでサーバーへの接続を確認する。

**コマンド→　ping IPアドレス**[　接続できる　]

⑤ いったん、SSH接続を切断し、SSHの接続が可能か確認する。

　＊接続はTera Termなどで行う。

[　接続できない　]

**●実習１０－２．必要なサービスの許可１（SSH）**

デフォルトのUFWのポリシーdenyのため、動作させているサービスを許可する。

SSHも許可されていないため、最初の確認は仮想マシンの「端末」で行う。

**※ここは仮想マシン上の「端末」で実施してください**

1. 現在のポリシーを確認する。

　 ① 設定されているポリシーを確認する。

sudo ufw status verbose

**コマンド→**

表示結果を記載する。

|  |
| --- |
| Status: active  Logging: on (low)  Default: deny(incoming), allow (outgoing), disabled(routed)  New profiles: skip |

② ①の結果からincomingのポリシーが[　　deny　　　]とわかる

（２） SSHを許可するポリシーを追加し、リモート接続できるようにする。

　 ① PCのネットワークアドレスを調べる。

**Ifconfig**

**コマンド→**

　ネットワークアドレス/プレフィックス：[ 10.21.10.0 /24]

② PCの所属するネットワークからSSHを許可する設定を追加する。

sudo ufw allow from 10.21.10.0/24 to any port 22

**コマンド→**

③ ②で設定したポリシーを確認する。

sudo ufw status verbose

**コマンド→**

④ SSHの接続が可能か確認する。　＊接続はTera Termなどで行う。

[　接続できる　]

**※これ以降は再びTeraTermなどから実施してください。**

**●実習１０－３．必要なサービスの許可１（Web・DNS・メール）**

**動作させているサービスを許可する。**

（１）現在のサービスの状態を確認する

　①　bindが動作しているか確認する。

**コマンド→**

**Sudo systemctl status bind9**

②　bindが起動していなければ、起動する。

**コマンド→**

**Sudo systemctl start bind9**

③　postfixが動作しているか確認する。

**コマンド→**

sudo systemctl status postfix

④　postfixが起動していなければ、起動する。

**コマンド→**

sudo systemctl start postfix

⑤　dovecotが動作しているか確認する。

**コマンド→**

sudo systemctl status dovecot

⑥　dovecotが起動していなければ、起動する。

**コマンド→**

sudo systemctl start dovecot

（２）Webの許可をポリシーに追加する。

　①　Webで使用すると思われるプロトコルは[　HTTP ]、[　　HTTPS ]

②　Webのアクセスを許可するポリシーを追加する。Webのサービスは送信元の指定は不要。

　　＊今回は2つ追加する。

**コマンド→**

Sudo ufw allow http

**コマンド→**

Sudo ufw allow https

③ ②で設定したポリシーを確認する。

sudo ufw status verbose

**コマンド→**

④　ブラウザでサーバーのIPアドレスを指定して接続できることを確認する。

　　　　[　接続できる　]

（３）DNSの許可をポリシーに追加する。

　①　DNSで使用するポート番号は[　53　]、トランスポート層のプロトコルは[　UDP　]

②　DNSのアクセスを許可するポリシーを追加する。サービスは送信元の指定は不要。

　　＊今回は2つ追加する。

**コマンド→**

Sudo ufw allow 53/udp

**コマンド→**

Sudo ufw allow 53/tcp

③ ②で設定したポリシーを確認する。

sudo ufw status verbose

**コマンド→**

**＊DNSの設定については、bind9でも設定はできる。**

（４）メールの許可をポリシーに追加する。**（第5章時点のもの。SSL等は考慮しない。）**

　①　メールで使用しているサービスは[　pop3 ]、[ smtp　]

②　メールへのアクセスを許可するポリシーを追加する。サービスは送信元の指定は不要。

　　＊今回は2つ追加する。POPサーバーのサービスはポート番号/プロトコルで設定

**コマンド→**

**sudo ufw allow SMTP**

**コマンド→**

**sudo ufw allow 110/tcp**

③ ②で設定したポリシーを確認する。

**Sudo ufw status verbose**

**コマンド→**

（５）設定したポリシーを確認し、ufw.kad10.txtにリダイレクトする。

　①　ポリシーを確認し、ufw.kad10.txtにリダイレクトする。

**コマンド→**

sudo ufw status verbose > ufw.kad10.txt

**●実習１０－４．ログなどの確認**

**UFWのログを確認する。**

（１）ログを確認する。

　①　UFWログを出力する。

**コマンド→**

sudo cat /var/log/ufw.log

②　サーバー宛てのUTWログをリアルタイムで出力する。

**コマンド→**

sudo tail -f /var/log/ufw.log

③　TeraTermなどからサーバーへtelnet接続をし、ログが表示されることを確認する。

[　確認できない　]

④　UFWのログ（①の出力）をufwlog.kad10.logファイルにリダイレクトする。

**コマンド→**

Sudo cp /var/log/ufw.log ufwlog.kad10.log

**●チェック項目**

* **最終的なファイアウォールポリシーの表示（IPv4は7つ、IPv6は6つあるはず）**

**sudo ufw status verbose　または sudo cat ufw.kad10.txt**

* **UFWログにtelnet接続拒否が記録されていること**

**sudo cat /var/log/ufw.log | grep DPT=23**

**または**

**sudo cat ufwlog.kad10.log | grep DPT=23**

**●実習１０－５．提出用ファイルの作成と提出**

①ufw.kad10.txt、ufwlog.kad10.logをコピー＆ペーストしてクラス番号ufw.kad10.txt、クラス番号.ufwlog.kad10.logで保存する。

**●課題提出**

**３つのファイル（クラス名番号ufw.kad10.txt、クラス名番号ufwlog.kad10.log、クラス名番号日付.log）をsv23の指定された場所へ課題を提出しなさい。**

**未チェックの場合は、このWordファイルも提出してください。チェックの代わりにします。**