UNIXサーバー構築 Ⅱ

第10章　ファイアウォール(UFW)

UFW(Uncomplicated Firewall)

UFW(Uncomplicated Firewall)

UFWとは、**iptables**、**nftables**を設定するためのツール。

Ubuntuでは**nftables**が現在のバージョンではデフォルトになっている。

iptables、nftablesとは

パケットフィルタリングツール。元々はiptablesが使用されていたが、近年は、nftablesを使用するディストリビューションも増えてきている。

＊inuxカーネル3.13以降で利用可能

UFW確認コマンド

sudo systemctl status ufw

UFWの状態を確認するコマンド。デフォルトでは、UFWはインストール済みではある。ただし、状態は有効にはなっていない。

<例>出力結果

● ufw.service - Uncomplicated firewall

Loaded: loaded (/lib/systemd/system/ufw.service; enabled; vendor preset: e>

Active: active (exited) since Mon 2023-12-18 09:49:32 JST; 3min 40s ago

＊Activeだが状態は**非アクティブ**になっている。

UFW確認コマンド

- **sudo ufw status , sudo ufw status verbose**

  UFWの状態を確認するコマンド。verboseを付けるとポリシーも表示される。ただし、UFWがアクティブになっていないとポリシーは表示されない。

  <例>出力結果

状態: **アクティブ**

ロギング: on (low)

Default: deny (incoming), allow (outgoing), disabled (routed)

新しいプロファイル: skip

UFWの有効・無効・再読み込み

- **sudo ufw enable**

  UFWの有効化。コマンドを入力すると次のようなメッセージが表示。

Command may disrupt existing ssh connections. Proceed with operation (y|n)? y

- **sudo ufw disable**

  UFWの無効化

- **sudo ufw reload**

  UFWの再読み込み

incoming(受信)ポリシー

■受信ポリシー(incoming policy)

incomingポリシーの**デフォルトはdeny(拒否)**されている。

■ポリシーの設定

ポリシーはデフォルト拒否なので、許可するものを設定する。

sudo ufw allow port番号/プロトコル

sudo ufw allow from 送信元to 宛先 port ポート番号 proto プロトコル

＊送信元、宛先、ポート番号を指定したポリシー

incoming(受信)ポリシーの設定例

設定例

ここでは、3つの設定を例にあげる。

sudo ufw allow **http**　　・・・　HTTP(80)を許可

sudo ufw allow **2049/tcp**　　・・・　TCPの2049番ポートを許可

sudo ufw allow **from 192.168.1.0/24 to any port 22**

送信元が192.168.1.0/24ネットワークのポート22番を許可。宛先はany(すべて)が許可される。

incoming(受信)ポリシーの操作コマンド

ポリシーを番号付きで表示

sudo ufw status numbered

```
To                         Action      From
--                         ------      ----
[ 1] 80/tcp                ALLOW IN    Anywhere    番号付きで表示される。
[ 2] 443                   ALLOW IN    Anywhere
```

ポリシーの削除

sudo ufw delete 番号

sudo ufw delete allow ポート番号/プロトコル

<例>sudo ufw delete 1

incoming(受信)ポリシーの操作コマンド

ポリシーをリセット

ポリシーをリセットし、UFWを無効化する。

sudo ufw reset

incoming(受信)ポリシーの操作(その他)

■ポリシーの前の状態を確認

現在設定されているポリシーの前の状態を保存しているため、確認することができる。

cat /etc/ufw/before.rules

/etc/ufwディレクトリ直下にはUFWで設定された情報が保存される。

<例>一部抜粋

ok icmp codes for INPUT　・・・ICMPに関するルールが確認できる。

-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT

-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT

-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT

-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

UFWのログ

■UFWのログ

UFWのログは**/var/log/utw.log**と**/var/log.syslog**に保存される。

sudo cat /var/log/ufw.log

Dec 22 10:20:26 ecc kernel: [3457.000154] [UFW BLOCK] IN=enp0s3 OUT=
MAC=01:00:5e:00:00:fb:ce:3e:b8:fe:9b:c9:08:00 SRC=10.200.0.72 DST=224.0.0.251 LEN=32
TOS=0x00 PREC=0x00 TTL=1 ID=58742 PROTO=2

■宛先が10.200.6.35へのUFWのログの表示例

sudo tail -f /var/log/ufw.log | grep DST=10.200.6.35

Dec 18 11:39:57 ecc kernel: [4936.468735] **[UFW BLOCK]** IN=enp0s3 OUT=
MAC=08:00:27:6f:1b:bf:f0:57:a6:f6:c8:7c:08:00 SRC=10.200.3.172 **DST=10.200.6.35** LEN=40 TOS=0x00
PREC=0x00 TTL=128 ID=1595 DF PROTO=TCP SPT=56974 DPT=80 WINDOW=513 RES=0x00 ACK URGP=0