

Firewall (FW) 超重要！

ファイアウォール機能は現在リリースされているどの OS でも標準で搭載されているといえます。
Linux にも当然、ファイアウォール機能が搭載されています。

[1] ファイアウォールサービスの現在の状態確認。(デフォルトは有効)

```
[hal@motobe ~]$ systemctl status firewalld.service
```

```
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: active (running) since Sun 2023-05-14 21:31:51 JST; 9min ago
     Docs: man:firewalld(1)
  Main PID: 4440 (firewalld)
    Tasks: 2 (limit: 4364)
   Memory: 29.8M
      CPU: 1.942s
   CGroup: /system.slice/firewalld.service
           └─4440 /usr/bin/python3 -s /usr/sbin/firewalld --nofork --nopid
```

```
5 月 14 21:31:50 motobe.com systemd[1]: Starting firewalld - dynamic firewall daemon...
```

```
5 月 14 21:31:51 motobe.com systemd[1]: Started firewalld - dynamic firewall daemon. [hal@motobe ~]$
```

(注意 1) active: active (running) ~の状態は稼働中。停止の場合は「inactive (dead)」と表示されます。

(注意 2)Firewalld を利用するには、サービスを起動しておく必要があります。ただし、デフォルトでは起動していますので以下のコマンドは必要ありません。

※停止

```
[hal@motobe ~]$ sudo systemctl stop firewalld.service
```

```
[hal@motobe ~]$ systemctl status firewalld.service
```

```
○ firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset: enabled)
   Active: inactive (dead) since Sun 2023-05-14 21:43:17 JST; 6s ago
 Duration: 11min 26.592s
     Docs: man:firewalld(1)
  Process: 4440 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/S>)
 Main PID: 4440 (code=exited, status=0/SUCCESS)
      CPU: 2.117s
```

```
5 月 14 21:31:50 motobe.com systemd[1]: Starting firewalld - dynamic firewall daemon...
```

```
5 月 14 21:31:51 motobe.com systemd[1]: Started firewalld - dynamic firewall daemon.
```

```
5 月 14 21:43:17 motobe.com systemd[1]: Stopping firewalld - dynamic firewall daemon...
5 月 14 21:43:17 motobe.com systemd[1]: firewalld.service: Deactivated successfully.
5 月 14 21:43:17 motobe.com systemd[1]: Stopped firewalld - dynamic firewall daemon.
5 月 14 21:43:17 motobe.com systemd[1]: firewalld.service: Consumed 2.117s CPU time.
(注意) 「 q 」 で端末に戻ります
```

※起動

```
[hal@motobe ~]$ sudo systemctl start firewalld.service
[hal@motobe ~]$ systemctl status firewalld.service
```

※再起動

```
[hal@motobe ~]$ sudo systemctl restart firewalld.service
```

[2] 通信を許可しているかの確認

ファイアウォールサービスを利用する場合、デフォルトではインバウンド通信はほぼ許可されていないため、サーバーに設定/公開するサービス/アプリケーションに応じて、**許可/不許可の設定が必要**になります。

firewalld では、ゾーンという単位で設定が定義されます。
このゾーンと **NIC** が紐づくことで、設定が有効になります。

(1)すべてのゾーンの情報を見る

```
[hal@motobe ~]$ sudo firewall-cmd --list-all-zones
```

block

```
target: %%REJECT%%
icmp-block-inversion: no
interfaces:
```

(略)

public (active) ←この設定が **Linux** に反映されています

```
target: default
icmp-block-inversion: no
interfaces: ens160
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
```

forward-ports:
source-ports:
icmp-blocks:
rich rules:

```
trusted
target: ACCEPT
icmp-block-inversion: no
```

(略)

それぞれのゾーンによって情報が表示されているのがわかるかと思います。

(2)デフォルトのゾーンを確認するコマンドは以下になります。

```
[hal@motobe ~]$ firewall-cmd --get-default-zone
public
```

※public がデフォルトの設定になっています

(3)それぞれのゾーンに設定されているサービスを確認するコマンドは以下になります。

```
[hal@motobe ~]$ sudo firewall-cmd --zone=public --list-services --permanent
cockpit dhcpv6-client ssh
```

※public ゾーンでは表示されたサービス名のポートが空いているということですね。

ゾーンの種類

ゾーン名	対応
drop	外部からのすべてのパケットを破壊
block	内部から送信して外部から返信されたパケットのみ通過、その他のパケットを受信拒否
dmz	DMZ(DeMilitarized Zone : 非武装地帯)向け設定、デフォルトで ssh のみを許可
external	IP マスカレードを有効にしたゲートウェイ向け設定、デフォルトで ssh のみを許可
public	コンピュータを信頼できないパブリックエリア向け設定、ssh と dhcpv6-client のみ許可
work	職場向け設定、デフォルトで ssh と dhcpv6-client のみ許可
home	自宅向け設定、デフォルトで ssh と mdns と samba-client と dhcpv6-client のみ許可
internal	ほぼ信頼できる内部ネットワーク向け、ssh と mdns と samba-client と dhcpv6-client のみ許可
trusted	すべてのパケットを受信許可

(4)定義されているサービスの一覧を表示する。

```
[hal@motobe ~]$ firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd
( 以下略～ )
```

定義されているサービスの定義ファイルは以下の場所に保管されている

独自に定義を追加する場合はここに XML ファイルを追加する

```
[hal@motobe ~]$ ls /usr/lib/firewalld/services
RH-Satellite-6-capsule.xml  isns.xml                proxy-dhcp.xml
RH-Satellite-6.xml         jellyfin.xml             ps3netsrv.xml
afp.xml                    jenkins.xml              ptp.xml
( 以下略～ )
```

[3] Firewalld：基本操作ゾーンにサービスを追加する

恒久的に変更する場合は「--permanent」オプションを指定します。「--permanent」を指定しない場合、システムを再起動すると設定は元に戻ります。

(1)例として http を追加する（設定は即時有効になる）

```
[hal@motobe ~]$ sudo firewall-cmd --add-service=http --zone=public
success
[hal@motobe ~]$ sudo firewall-cmd --zone=public --list-services
cockpit dhcpv6-client http ssh
※http が FW に追加(許可)されました
```

(2)例として http を削除する

```
[hal@motobe ~]$ sudo firewall-cmd --remove-service=http --zone=public
success
[hal@motobe ~]$ sudo firewall-cmd --zone=public --list-services
cockpit dhcpv6-client ssh
※http が削除されました
```

(3)例として http を恒久的に追加する（設定を反映させるためにリロードが必要）

```
[hal@motobe ~]$ sudo firewall-cmd --add-service=http --zone=public --permanent
success
[hal@motobe ~]$ sudo firewall-cmd --reload
success
[hal@motobe ~]$ sudo firewall-cmd --zone=public --list-services --permanent
cockpit dhcpv6-client http ssh
※http が FW に追加(許可)されました
```

[4] Firewallld : 基本操作ゾーンにポートを追加/削除する

(1)例として TCP 465 を追加する

```
[hal@motobe ~]$ sudo firewall-cmd --list-port --zone=public
```

```
[hal@motobe ~]$ sudo firewall-cmd --add-port=465/tcp --zone=public
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --list-port --zone=public
465/tcp
```

(2)例として TCP 465 を削除する

```
[hal@motobe ~]$ sudo firewall-cmd --remove-port=465/tcp --zone=public
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --list-port --zone=public --permanent
```

(3)例として TCP 465 を恒久的に追加する (設定を反映させるためにリロードが必要)

```
[hal@motobe ~]$ sudo firewall-cmd --add-port=465/tcp --zone=public --permanent
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --reload
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --list-port --zone=public --permanent
465/tcp
```

(4) TCP 465 を削除 (設定を反映させるためにリロードが必要)

```
[hal@motobe ~]$ sudo firewall-cmd --remove-port=465/tcp --zone=public --permanent
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --reload
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --list-port --zone=public --permanent
```

[5] Firewallld : 基本操作ゾーンに ICMP のタイプを追加/削除する。

(1)現状確認

```
[hal@motobe ~]$ sudo firewall-cmd --list-icmp-blocks --zone=public
```

※何も設定されていない

```
[hal@motobe ~]$ ping -c 3 192.168.42.161      ←宛先は Windows や MAC のアドレス
PING 192.168.42.161 (192.168.42.161) 56(84) bytes of data.
```

```
64 bytes from 192.168.42.161: icmp_seq=1 ttl=128 time=0.814 ms
64 bytes from 192.168.42.161: icmp_seq=2 ttl=128 time=0.786 ms
64 bytes from 192.168.42.161: icmp_seq=3 ttl=128 time=0.845 ms
```

```
--- 192.168.42.161 ping statistics ---
```

```
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.786/0.815/0.845/0.024 ms
```

```
C:\Users¥moto>ping 192.168.42.2

192.168.42.2 に ping を送信しています 32 バイトのデータ:
192.168.42.2 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.42.2 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.42.2 からの応答: バイト数 =32 時間 =1ms TTL=64
192.168.42.2 からの応答: バイト数 =32 時間 =1ms TTL=64

192.168.42.2 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
    ラウンド トリップの概算時間 (ミリ秒):
        最小 = 0ms、最大 = 1ms、平均 = 0ms
```

※Windows(192.168.42.161)から Linux(192.168.42.2)への疎通確認。アドレスは自分の環境に合わせて下さい。

(2)例として echo-request を追加する

```
[hal@motobe ~]$ sudo firewall-cmd --add-icmp-block=echo-request --zone=public
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --list-icmp-blocks --zone=public
echo-request
```

※echo-request が追加された

(3)確認

```
[hal@motobe ~]$ping -c 3 192.168.42.161      ←宛先は Windows や MAC のアドレス
PING 192.168.42.161 (192.168.42.161) 56(84) bytes of data.
```

```
64 bytes from 192.168.42.161: icmp_seq=1 ttl=128 time=1.11 ms
64 bytes from 192.168.42.161: icmp_seq=2 ttl=128 time=0.879 ms
64 bytes from 192.168.42.161: icmp_seq=3 ttl=128 time=0.793 ms
```

```
C:\Users¥moto>ping 192.168.42.2

192.168.42.2 に ping を送信しています 32 バイトのデータ:
192.168.42.2 からの応答: 宛先ホストに到達できません。
192.168.42.2 からの応答: 宛先ホストに到達できません。
192.168.42.2 からの応答: 宛先ホストに到達できません。
192.168.42.2 からの応答: 宛先ホストに到達できません。

192.168.42.2 の ping 統計:
    パケット数: 送信 = 4、受信 = 0、損失 = 4 (100% の損失)、
```

※echo-request を拒否したから Windows や MAC からの通信は通らない

(4)例として echo-request を削除する

```
[hal@motobe ~]$ sudo firewall-cmd --remove-icmp-block=echo-request --zone=public
success
```

```
[hal@motobe ~]$ sudo firewall-cmd --list-icmp-blocks --zone=public
```

※設定が削除された

(5)確認

```
[hal@motobe ~]$ ping -c 3 192.168.42.161 ←宛先は Windows や MAC のアドレス
```

```
PING 192.168.42.161 (192.168.42.161) 56(84) bytes of data.
```

```
64 bytes from 192.168.42.161: icmp_seq=1 ttl=128 time=0.930 ms
```

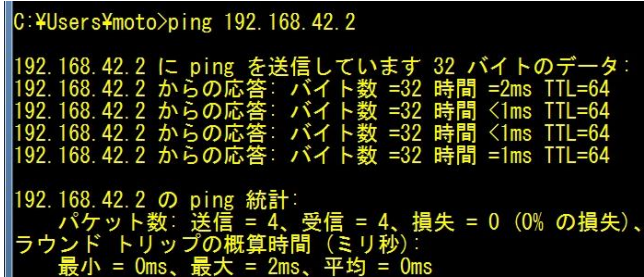
```
64 bytes from 192.168.42.161: icmp_seq=2 ttl=128 time=0.801 ms
```

```
64 bytes from 192.168.42.161: icmp_seq=3 ttl=128 time=0.789 ms
```

```
--- 192.168.42.161 ping statistics ---
```

```
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
```

```
rtt min/avg/max/mdev = 0.789/0.840/0.930/0.063 ms
```



```
C:\Users\moto>ping 192.168.42.2

192.168.42.2 に ping を送信しています 32 バイトのデータ:
192.168.42.2 からの応答: バイト数 =32 時間 =2ms TTL=64
192.168.42.2 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.42.2 からの応答: バイト数 =32 時間 <1ms TTL=64
192.168.42.2 からの応答: バイト数 =32 時間 =1ms TTL=64

192.168.42.2 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
    ラウンドトリップの概算時間 (ミリ秒):
        最小 = 0ms、最大 = 2ms、平均 = 0ms
```

※通信が可能！

(6)指定可能な ICMP タイプの一覧を表示する

```
[hal@motobe ~]$ sudo firewall-cmd --get-icmptypes
```

```
address-unreachable bad-header communication-prohibited destination-unreachable echo-reply
```

```
echo-request fragmentation-needed host-precedence-violation host-prohibited host-redirect host-unknown
```

(以下略～)

[6] ファイアウォールの停止 ←授業では停止しないで下さい

もし、自身のネットワーク内で設定対象とするサーバーの上位にファイアウォール機器が設置されており、サーバー側ではファイアウォールサービスは必要ないといった場合は以下のようにして停止することも可能です。

(1)サービス停止

```
[hal@motobe ~]$ sudo systemctl stop firewalld.service
```

```
[hal@motobe ~]$ sudo systemctl status firewalld.service
```

(2)自動起動設定を無効にする

```
[hal@motobe ~]$ sudo systemctl disable firewalld
```

以上！

FW は非常に重要ですのでしっかり押さえて下さい！