# ネットワーク開発演習　10...ファイアーウォールによる防御

# １.侵入した者のログをとる方法

ターゲットはSSHサーバとする

2. 出力ファイルの設定

$sudo emacs /etc/rsyslog.d/iptables.conf

:msg,contains,"DROP" /var/log/iptables/DROP.log

"DROP" という文字列を含むメッセージを /var/log/iptables/DROP.logに出力する

3. iptables の追加

SSH のための静的NATをログする

sudo iptables -t nat -A PREROUTING -d $IP --dport 22 -j LOG --log-prefix "DROP: "

4. 出力ログファイルの作成

$sudo mkdir /var/log/iptables

$sudo touch /var/log/iptables/DROP.log

$sudo chown syslog /var/log/iptables/DROP.log

$sudo chgrp adm /var/log/iptables/DROP.log

5. rsyslog の再起動

$ sudo service rsyslog restart

6. ログの確認方法

$ tail -f /var/log/iptables/DROP.log