ルールリスト

TCPのフラグ

- □UDPやICMPはコネクションレスな通信
  - ○ポート番号やIPアドレス，ネットワークインタフェースを用いたフィルタリングのみ
- □TCPはコネクション指向の通信
  - ○通信の様々な段階で異なるフラグがを手掛かりにした
  - ○フィルタリングが可能
- □コネクション確立時のパケット
  - ○SYNフラグ有り
  - ○ACKフラグ無し
  - ○コネクションの確立時に確立しようとする側から最初に送られてくるパケットに付けられるフラグ
- □コネクション確立後のパケット
  - ○ACKフラグまたはRSTフラグ有り
  - ○コネクションの確立後の通信のパケットに付けられるフラグ