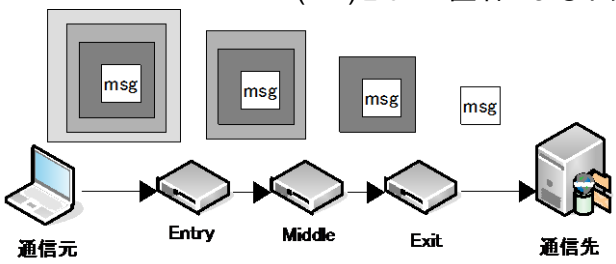
# パケット解析を用いたTor通信の特徴分析の検討

# Discovering Features for Tor Deanonymization Using Packet Analysis

早川宏志・ネットワーク分科会・情報セキュリティ大学院大学

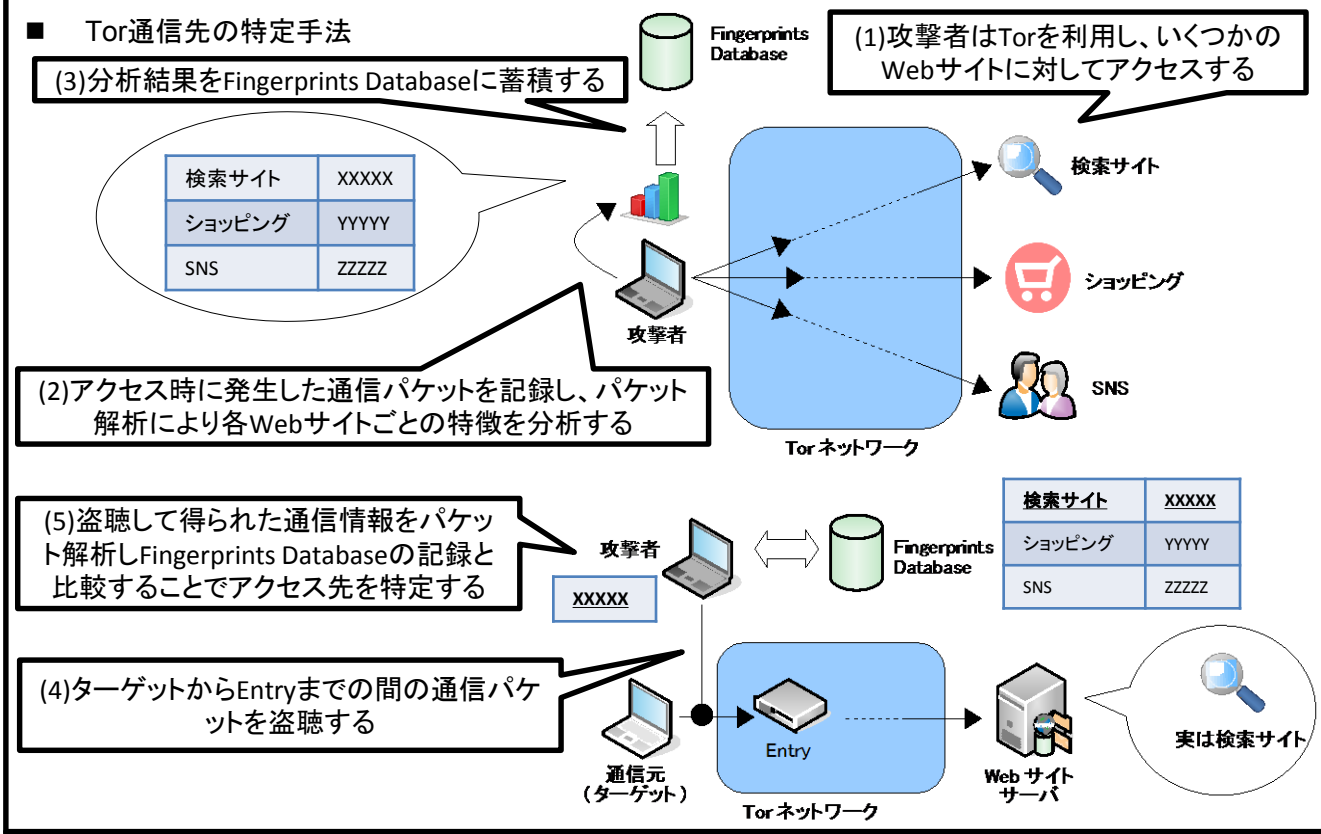
The Onion Router (Tor) is an anonymization network system. In this research, we propose one of techniques how to distinguish the destination of Tor communication using several features.

■ The Onion Router(Tor)とは・・・匿名によるネットワーク通信を実現するシステムの一つ




- ✓ Torでは3つの中継ノードを経由する。データは通信元で多重に暗号化され、その後各中継ノードで順に復号が行われる。
- ✓ 多重暗号化により中継ノードでは前後のノードのIPアドレスしか把握できず、第三者から見た場合ではTor通信先がどこであるのかわからない

■ Tor通信先の特定手法




■ Tor通信におけるWebサイトごとの特徴の例

Google(左)とAmazon(右)の送信パケットサイズを10(bytes)ごとに区切り、20回分の平均値を求めた図を示す。縦軸はパケット数の平均、横軸はパケットサイズ(bytes)である。特定のパケットサイズにおけるパケット数に違いがあらわれている。