松浦研究室

[インターネット上におけるプライバシー保護技術の現状と課題]

生産技術研究所　情報・エレクトロニクス系部門
Department of Informatics and Electronics, IIS
http://kmlab.iis.u-tokyo.ac.jp/

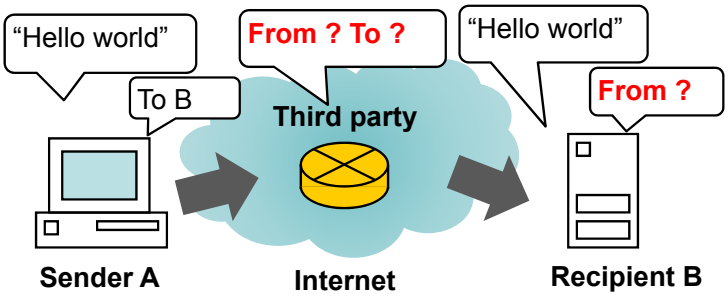
情報理工学系研究科
電子情報学専攻

情報セキュリティ

インターネット上におけるプライバシー保護

Internet Privacy Protection

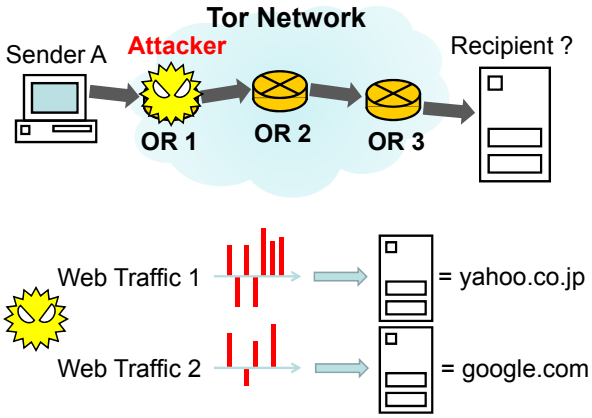
近年インターネットは急速に普及し様々な用途で利用されるようになりました。しかし，手紙や電話の様な他の通信手段と異なり，インターネットはプライバシーに関する安全性が十分でありません．例えば，IT に精通していない者でも一般配布されているツールを用いることで容易に他者の行動を監視できてしまいます。暗号化通信を用いることで通信の内容を秘匿することはできますが、通信の経路情報まで秘匿することはできません。そこで，通信経路を秘匿する目的で多くの匿名通信技術が考案され、それらを実装した匿名通信システムが世の中で普及しています。



- ✓ **匿名通信システムの概念図。通信内容ではなく、通信者のつながり（誰が誰と通信しているか）を秘匿する。**
- **用途**
  - **Webブラウジング中のプライバシー保護**
  - **匿名投票サービス、匿名掲示板　等**

匿名通信システムの脆弱性評価

Vulnerability Assessment of Anonymous Communication Systems



現在最も普及している匿名通信システムであっても、その匿名性は完璧ではありません。

既に、匿名性を低下させる攻撃手段がいくつか発見されています。中でも入りロノードのトラフィックのみに着目する指紋攻撃は，実現のために必要な資源が少なく，現実的な脅威になりうるものとして注目されています．

左は、指紋攻撃の概念図です。
本研究室の実験環境では、指紋攻撃によって 70～80%の確率で通信者のつながりが特定できることを確認しました。