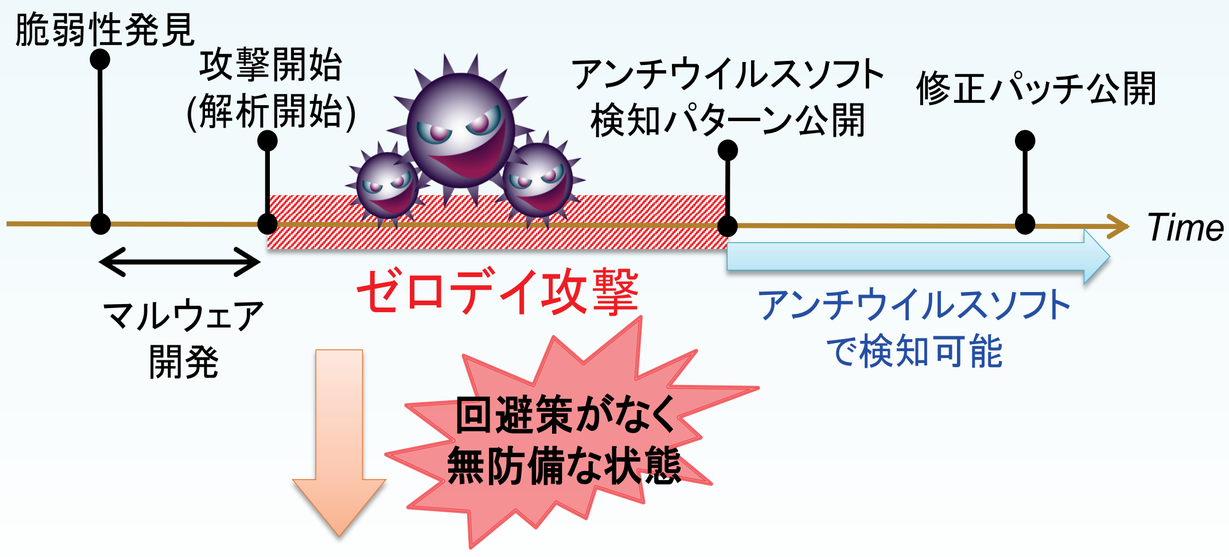
情報ネットワークシステム論講座
情報基盤ネットワーク研究部門

教授：高倉弘喜　　准教授：嶋田創　　助教：山口由紀子

INFORMATION SCIENCE
NAGOYA UNIVERSITY
情報システム学専攻

高精度なゼロデイ攻撃検知手法の開発

- サイバー攻撃のライフサイクル

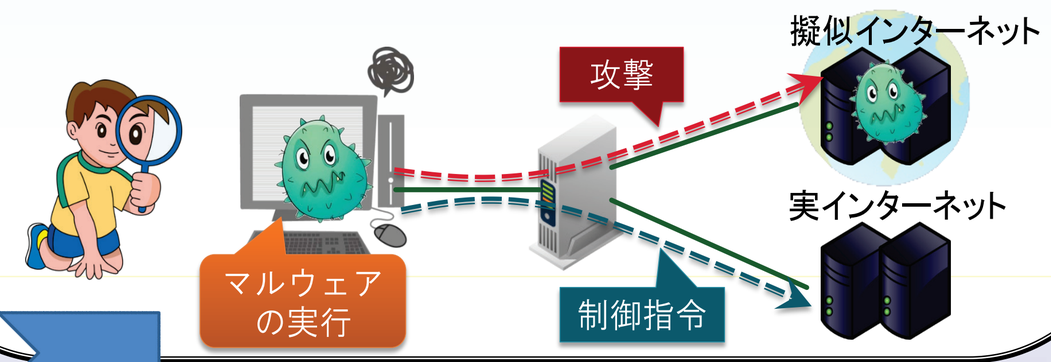


- パターンファイルに依存しない検知（アノマリ検知）
  - 普段頻繁に使用する正常な通信からの挙動の変化を検出

より高精度なアノマリ検知手法の研究

安全なマルウェア動的解析システム

- マルウェア（悪意のあるソフトウェア）をPC上で実行し，動作を解析
  - 問題：詳細な解析のためにはインターネット接続が必要だが，外部サーバへ攻撃を行う危険性がある
- 対策：インターネットを模倣した擬似インターネットを使用し安全性を高める
  - 動作に必要な通信：実インターネットへ転送
  - 悪意ある通信　　：擬似インターネットへ転送



マルウェア分析/標的型攻撃/脆弱性攻撃に対する早期検知/発見

情報基盤センターのサービスと密接した研究/開発

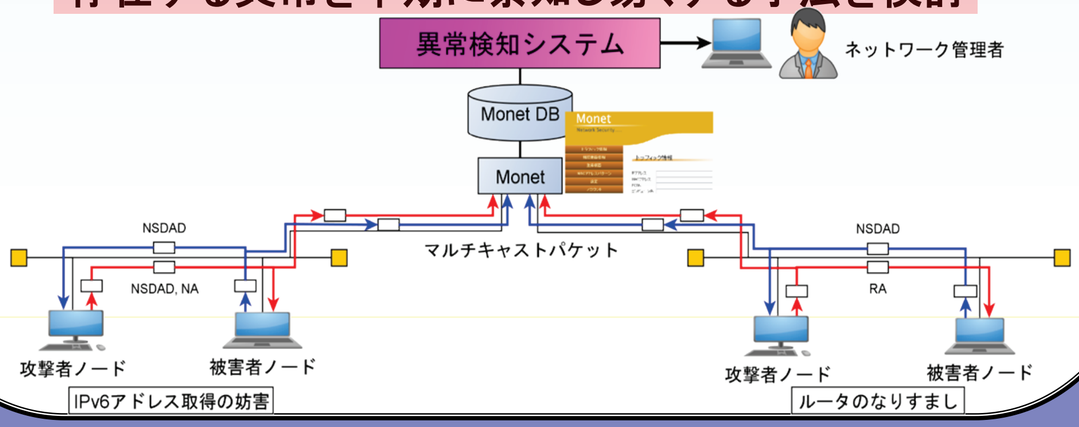
IPv6導入へのシステム整備

グリーンコンピューティングの実現

IPv6監視システムを用いた早期異常検知

- IPv6においてはプロトコルの仕様に起因する様々なセキュリティ問題が存在
  - 名古屋大学が開発したIPv6アドレス監視システム**Monet**
    - インシデントが発生したときにMonetを用いて問題を起こした端末を特定することは可能
    - ネットワークにどのような異常が存在するかは分からない

Monetが収集するデータを統合し、ネットワークに存在する異常を早期に察知し易くする手法を検討



グリーンIT実現のための低消費電力研究

- IT機器の消費電力増加は深刻な問題
  - 日本の全発電力の5%を占め、なお増加中

発電のためのCO2排出 → **地球温暖化**　人間に都合が良い地球環境維持のためには好ましくない

1. ネットワークの運用の工夫で何かできないか?
2. 仮想サーバ運用の工夫で何かできないか?
3. サーバ用計算機のHW構成の工夫で何かできないか?
4. ネットワーク・プロセッサの工夫で何かできないか?