順天堂大学　健康データサイエンス学部
田辺瑠偉　博士（情報学）

Juntendo University Faculty of Health Data Science
Rui TANABE, Ph.D.

研究概要 / Research overview

不正プログラム（**Malware**）の対策に取り組んでいる。特に、以下の研究を行っている。

- サイバー攻撃の**観測**
- 攻撃インフラやマルウェアの**分析・解析**
- セキュリティ対策技術の**評価・提案**
  新たな脅威への**注意喚起と対策検討**

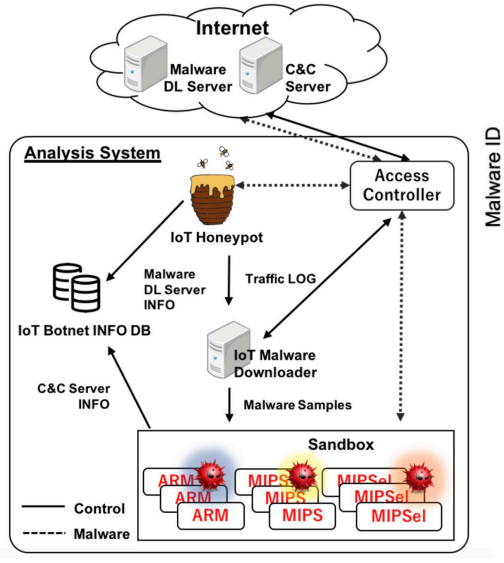
We fight against **Malware**. To achieve our research goal, we conduct four approaches.

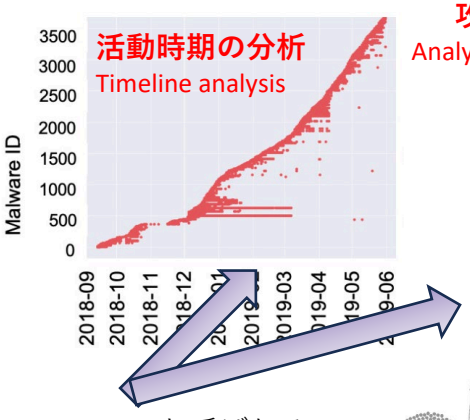
- **Monitor** cyber attacks
- **Analyse** attack infrastructure, malware binaries, and other form of cyber threats
- **Propose** countermeasures
- **Prevent** and notify future threats

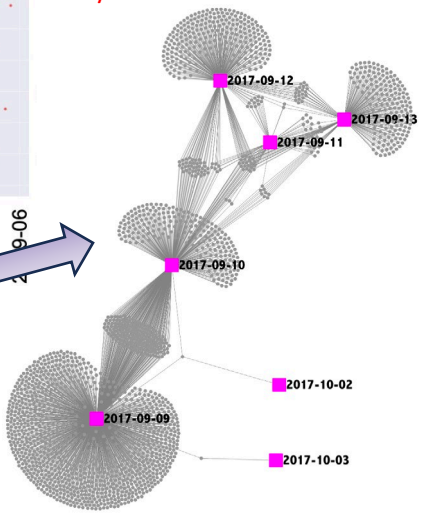
研究成果 / Research outputs

Honeypotと呼ばれる囮のシステムを
インターネット上に公開してマルウェアを捕獲
Reveal **Honeypot** system and capture malware samples

攻撃の分析 / Analysis

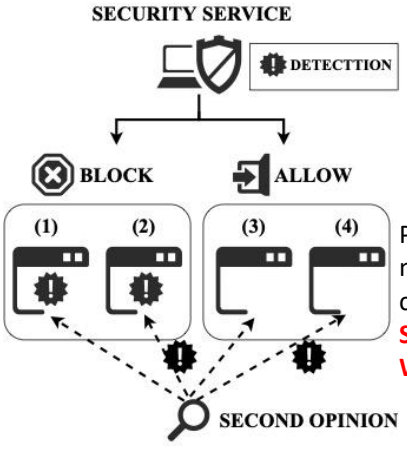






Sandboxと呼ばれる
解析環境内で実行
Execute malware samples
in **Sandboxes**

対策技術の提案 / Proposal



Proposal method to collect **Suspicious Websites**

攻撃の注意喚起 / Prevention

アクセス時に実害をもたらす可能性がある
怪しいWebサイトの収集手法の提案
解析を回避する**高度なマルウェア**の予測
Prevent future attacks of **Advanced malware**