# 卒業論文に向けて

学部4年生
島本 大輔

# 概要

- 題材選び
- 進捗報告
- 今後の予定

# 題材選び

- 分野:セキュリティ関係
  - ウィルス対策
  - IDS

# ウィルス対策

**ウィルス**TOP10
(トレンドマイクロ社ホームページより)

| | |
|---|---|
| 1 | WORM_ANTINNY.A |
| 2 | PE_PARITE.A |
| 3 | HTML_NETSKY.A |
| 4 | JAVA_BYTEVER.A |
| 5 | WORM_ANTINNY.G |
| 6 | WORM_NETSKY.P |
| 7 | WORM_NETSKY.Q |
| 8 | WORM_NETSKY.D |
| 9 | HTML_REDIR.A |
| 10 | WORM_ANTINNY.J |

- **特徴**
  - **亜種**
  - **ネットワーク経由**
  - **脆弱性を突く**

# ウィルス対策

- ClamAVの改良
  - 新しい機能を付加
  - 別アルゴリズムを考えて、付加
  - Windowsへの移植
- ウィルス対策ソフト from scratch
  - 根本的に異なる仕組みのものを作成
- シグネチャの自動生成
  - ワームについてはUSENIX Security ‘04の論文にあり

# ClamAV

- 有名なオープンソースウィルス対策ソフト
- シグネチャをマッチング
- 基本的にUNIX系向け
- 導入例
  - Sourceforge、DynDNS、など

➡ これを改良？

# ウィルス対策 from scratch

- PDAなど、別プラットフォーム上で動作するウィルス対策ソフト
- 実行するかもしれないものを予測し、未知のウィルスを発見
  - 呼び出す可能性のあるAPI・ライブラリを検出

➡ 時間的に間に合うのか？

# シグネチャの自動生成

- ウィルスのシグネチャを自動的に生成する
- Autograph
  - USENIX Security '04 より
  - ネットワークのワーム用
  - 詳しくは輪講で (発表者がいれば)
- 完全に生成しないまでも、シグネチャ作成者の支援

# IDS

- Windows**向けの**IDS
- **サンドボックス的な**IDS
  - **ワームを**pot**のようなものに閉じ込めて実行**

# 進捗報告

- ウィルス関係の情報調べ
- 関連論文
- ClamAVのソースコードの読み始め
- Detoursライブラリのソースコードの読み始め

# 今後の予定

- 題材の決定
  - ウィルス対策ソフトになる可能性大
- ソースコードの解読
  - ClamAV、Snortなど
  - Detoursライブラリ (実装に使う可能性あり)
- 関連論文の調査