# 情報理工学科 2015年度研究室配属説明会資料

# ① 研究室名(場所)

森 達哉 研究室 (55号館 N棟 608室)

e-mail: tmori@waseda.jp URL: http://nsl.cs.waseda.ac.jp/

研究室決定後の集合場所・日時:3/28(土) 14時~(研究室配属終了後)・場所:研究室

#### ② 研究分野

**セキュリティ & プライバシー** (スマートフォンセキュリティ,マルウェア解析,ウェブセキュリティ,パスワード解析,インフラハッキング,ソーシャルエンジニアリング,侵入検知技術,等々)

# ③ 研究テーマ

当研究室のミッションは、現代社会において必要不可欠なインフラである様々なネットワーク 化されたシステム (Networked Systems) を (1) 攻撃や障害から守ること、および (2) それらシステムの発展や社会への応用に貢献することです。基礎的な研究からすぐに具体的な貢献が見込めるテーマまで幅広く取り組みます。現時点では特にサイバーセキュリティの研究に力点をおいています。 研究室に配属されたみなさんには、(1)、(2) のいずれかの研究テーマに取り組んで頂きます。サイバーセキュリティの研究対象はスマートフォン、スマートグラス、スマートウォッチ、Web、無線LAN、マルウェア、ボットネット、スパム、Twitter、広告サイト、インフラ系制御システム、パスワード、医療機器、ロボット、人間(ソーシャルエンジニアリング)等、非常に多岐に渡りますので、学際的で面白い研究テーマが考えられると思います。

当研究室に特徴的な研究アプローチは、いずれの研究テーマにおいても対象のデータ収集と分析を基軸とし、リアリティを追求することにあります。計測・分析を行うツールとして様々な技術や知識を活用します。例えばデータの収集に必要となるサーバ構築・運用やソフトウェアの開発、および分析に必要となる各種プログラミング技術、数理統計、機械学習・パターン認識、各種アルゴリズム等です。我々が使うツールは多岐に渡りますが、それらのすべてを一度に習得しようとする必要はありません。研究室に配属された後、各自の卒論テーマを進める上で必要な知識・技術を実地で習得していきます。特にプログラミング技術やUNIX系OSの経験があると研究を進める上で有利ですが、経験がなかったとしても好奇心と良いモチベーションを持っていることが知識や技術を習得するために非常に有効です。

計測・分析は研究のミッションを進めるための強力なツール(手段)ですが、それ自体が最終的な目的というわけではありません。最終的な目的はドメイン知識とデータ計測・分析結果の両方にもとづいて対象を深く理解・洞察し、対象が抱える課題の根源的な対策方法(すなわちバリュー)を提示することにあります。我々にとってのドメイン知識とはサイバーセキュリティが対象とする特定の領域に関する高度な専門知識です。研究においてはこれらの複数の技術や知識を深く理解することに加え、これらを統合していかにバリューを生み出すかをとことん考えぬくことが本質です。本研究室での研究活動を通じて、時間をかけて知識を統合し、深く考え抜く経験を積むことができるでしょう。そのような経験を積むことは社会に出てから大変有用です。

#### ④ 人員構成

准教授1名, D1学生2名, M1学生5名, B4学生8名(内1名国際コース, 4名が大学院進学予定)

## ⑤ ゼミ 研究ゼミ (毎週火曜日13:00-16:30)

正書の輪読および各自の研究進捗報告や論文紹介をします。その他個別のミーティングを希望に応じて随時実施します。

#### ⑥ 研究室の行事

歓迎会(春・秋2回), 暑気払い, 夏季合宿, 忘年会, 送別会等 その他個別の飲み会は随時

⑦ オープンハウスの日程 3/24: 説明会終了後~18:00 3/26, 27: 14:00-18:00.

# ⑧ その他

当研究室は2013年4月にスタートした新しい研究室です。主宰者の理念として学生の**主体性** を最も尊重しています。なぜなら主体的に行動することで人は成長するからです。日頃のゼミに 加えてさらに研究に深く打ち込む希望を主体的に申し出た学生には懇切丁寧な個別指導を実施 しています。その結果、2013 年度は B4 の藤野君が国内学会での最優秀論文賞受賞、B4 の笹 生君, 竹越君, 藤野君が参加した MWS CUP (セキュリティ技術の競技コンペ)での**総合優勝** (後 藤研究室と連携), 2014 年度は M1 の渡邉君が国際学会でのペストポスター賞および国内学 会学生論文賞等、自らチャレンジしてみた学生は全員が公的に認められる業績を残しています。 さらにこの2年間で延べ9名の学生が学会発表等のために国内および海外出張を経験しました. 彼ら全員は自ら希望してこうした経験をしたわけですが、主宰者から見ても彼らは成長したと思 いますし、自身としての充実度も非常に高いようです。彼らは国内での活躍に飽きたらず、世界 に通用する研究成果を上げるべく日々燃えています。先輩・後輩で互いに日々切磋琢磨しつつも とても仲が良いようです。**セキュリティ技術が着目されている今、深い知識と技術を身に** つけて一緒に世界に挑戦しませんか?きっと生涯有用な実力が身につくはずです。

# 研究リソース

- ・ 個人用 PC: 一人 1 台支給 、データ解析用ハイエンドサーバ多数
- ・ フレッツ光ネクスト+ISP 4 社、AWS、Google Apps
- · Google Glass 他 Android 端末多数,ZTE OPEN C,IDA PRO,
- ・ マルウェア検体、Android アプリ、スパムデータ、動的解析ログ、パケットデータ等を大量 に収集・保管しています。これらのデータを収集するための環境も整備されています。
- ・ この他、MWS データセット、Android Genome データセット、CAIDA データセット、 MALICIA データセット等、外部組織から提供されたデータを多数保有しています。

## 学外組織との連携・コラボレーション

研究に必要となる専門知識や実際の現場における課題を深く理解するために本研究室では民 間企業や他組織との連携を積極的に進めています。企業の社員との対話を通じて技術的な内容だ けではなく、会社の概要や普段の仕事の様子などを知ることが出来ます。

• 共同研究パートナー: NTT 研究所 (x2), NTT コミュニケーションズ, FFRI, JPRS, NICT アクティビティ

- トップカンファレンス勉強会:都内近郊の主要なセキュリティ関連研究者による定期的な勉 強会に参画しています。これまでに早稲田のキャンパスで3回開催しました
- ・ CTF サークル: 森研・後藤研の学生有志が中心となって CTF サークル m1z0re (みぞれ)を結 成しました。m1z0r3 は日本最高峰の CTF 大会である SECCON CTF に 2 年連続でファイナ ルに食い込んでいます。研究室としてmlzOr3の活動を全面的にサポートしています。



