情報セキュリティ工学研究室

http://www.iselab.jp/


（写真左から）
教授：林　優一 yu-ichi@is.naist.jp
助教：藤本　大介 fujimoto@is.naist.jp

社会基盤を支えるセキュリティ技術を開発しよう

研究を始めるのに必要な知識・能力

研究室に入ってから必要となる知識は輪講などを通じて身に付けるので、研究を始めるのに必要となる具体的な知識や能力は特にありません。代わりに「○○なシステムのセキュリティを確保したい！」という強い思いとやる気のある学生さんは大歓迎です。

研究室の指導方針

学生のテーマ決めは学生と教員が適宜相談しながら行います。基本的には学生が希望する内容取り組める様にテーマを設定します。また、研究室では主にハードウェアセキュリティに関する研究を行いますが、研究室の教員が参画する実践セキュリティ人材育成コース(SecCap：https://www.seccap.jp)などを通じて、物理層からアプリケーション、法制度など幅広いセキュリティ知識を習得し、システム全体および利用形態を俯瞰することで、レイヤを縦断した最適なセキュリティ対策を実施できる人材を育成することを目指しています。

この研究で身につく能力

プログラミング輪講、暗号アルゴリズムのハードウェア実装演習、サイドチャネル情報計測・解析演習などを研究室に入った学生全員に実施しており、こうした輪講・演習を通じて、ソフトウェア及びハードウェアのプログラミングスキルや実装を行うアルゴリズムに関する知識を身に付けることができます。さらに、ハードウェア計測及び計測情報を処理するために、さまざまな計測器の使用法とその原理及び計測信号を処理するための統計学に関する知識を身に付けることもできます。

修了生の活躍の場

研究室で身に付けた実践手的なセキュリティスキルを生かす場としては、通信インフラやセキュリティ関連企業、シンクタンクを含む情報通信業、電機メーカーや自動車メーカーなどを含む製造業に主に活躍の場があると思います。また、セキュリティの確保は多くの業種で求められていますので、上述の業種に限らず活躍の場があると思います。

研究内容

【研究概要】
情報セキュリティ工学研究室では、情報セキュリティをシステムに実現する際、セキュリティアンカーとなるハードウェアの安全性確保に関する研究に取り組んでいます。また、ハードウェアを基礎として構成される上位レイヤを含めたシステム全体のセキュリティを確保するための研究も行っています。

【研究内容】
・漏えい電磁情報によるセキュリティ低下に関する評価・対策技術に関する研究
情報端末から生ずる電磁信号を通じた情報漏えいによるセキュリティ低下のリスク評価(図1)及び対策技術に関する研究(図2)を行っています。
・電磁的な外乱によるセキュリティ低下に関する評価・対策技術に関する研究
ハードウェアへの電磁的な外乱によるセキュリティ低下のリスク評価及び対策技術に関する研究を行っています。
・内部回路の意図的な改変によるセキュリティ低下に対する評価・対策技術に関する研究
情報機器の内部回路を意図的に変更することで実装されるマルハードウェアによるセキュリティ低下のリスク評価及び対策技術に関する研究を行っています。
・情報理論的に安全な秘密鍵共有の枠組みやプロトコルの開発
RSA公開鍵暗号やAESブロック暗号などのように計算の難しさに安全性の根拠を置こうとする暗号方式とは一線を画く研究ストリームである情報理論的に安全な暗号プロトコルの研究を行っています。
・大規模電磁界シミュレーションに関する研究
漏えい及び妨害電磁波による情報セキュリティ低下のメカニズム解明及び機器の設計段階でのリスク評価を行うために必要となる大規模電磁界シミュレーションに関する研究を行っています（図3)。
・情報通信システムの信頼性に関する研究
環境電磁工学(EMC)及び機構デバイス工学の観点から電磁信号の漏えいが少なく、電磁気的な外乱にも耐性のある情報通信システムを構成する機器の設計手法に関する研究を行っています。

図1　モバイル端末に対する電磁波を介した情報漏えいのリスク評価

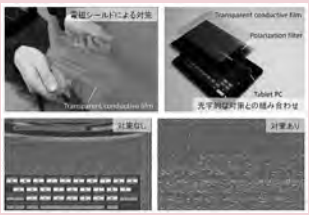

図2　漏えい電磁波を通じた情報漏えいの対策技術の開発

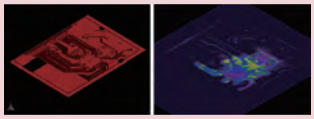

図3　大規模シミュレーションを用いた情報漏えい経路の可視化

研究設備

ハードウェアセキュリティ評価用プラットフォーム、オシロスコープ、スペクトラムアナライザ、任意及びパルス信号発生器、各種高周波プローブ、ソフトウェア無線、漏えい電磁界シミュレーションソフトウェアなどを用いてハードウェアセキュリティ評価・対策技術の研究開発を行っています。

研究業績・共同研究・社会活動・外部資金など

【共同研究】
・国内共同研究先：東北大学、電気通信大学、神戸大学、横浜国立大学など
・国外共同研究先：KU Leuven(ベルギー)、Telecom ParisTech(フランス)、Missouri University of Science and Technology(アメリカ)など

【外部資金】
・文部科学省・卓越研究員事業
・日本学術振興会・二国間交流事業(交流先：KU Leuven(ベルギー))
・日本学術振興会・科学研究費助成事業：基盤研究(A)(分担)、基盤研究(B)(代表)、基盤研究(B)(分担)、挑戦的萌芽研究(代表)
・NEDO・IoT推進のための横断技術開発プロジェクト
・NEDO・戦略的イノベーション創造プログラム(SIP)／重要インフラ等におけるサイバーセキュリティの確保
・セコム科学技術振興財団・挑戦的研究助成