電子情報科学専攻	研究分野	情報セキュリティ	Lab. ID EC28
研究室Webサイト	http://iseclab.ec.t.kanazawa-u.ac.jp/ja/index.html		

研究課題の概要

情報社会の基盤技術として、情報セキュリティ技術の重要性が高まっています。情報セキュリティを確立する要素技術として、暗号技術があり、守秘を目的とする暗号、メッセージの内容と作成者を保障するディジタル署名、更にはシステムにアクセスしようとする利用者の正当性を保障する認証技術などが含まれます。安全な認証技術を構成し、更に電子商取引・電子選挙・電子オークションなどの暗号プロトコル(暗号技術を利用した処理手続き)を構成することにより、社会でのこれらの営みを、情報ネットワークを活用しながら、より確実に実行できるようになり、安全な情報社会を構築することが可能となります。
・暗号基礎技術:　暗号方式、ディジタル署名方式、ユーザ認証方式、擬似乱数生成など
・セキュアプロトコル/暗号プロトコル:　仮想通貨、ブロックチェーン技術、スマートコントラクトのプライバシー保護、電子決済、電子オークションなど
・その他の保護・認証技術:　プライバシー保護、ディジタルコンテンツ保護、ソフトウェア保護、行動認証など
・新分野でのセキュリティ対策:　クラウドやエッジコンピューティング、IoTとセキュリティ、AIセキュリティ・プライバシー、耐量子計算機など

博士前期課程/後期課程院生の指導方針、具体的なカリキュラム、研究室での活動等

基礎的もしくは最先端な内容を記載した専門書を用いた輪講や、学術論文の内容紹介もしくは研究状況の報告を行うゼミなどを通して、博士前期課程もしくは博士後期課程での研究を遂行する上で必要となる知識や技術を身に付けます。
これらの知識や技術の修得に加えて、各学生は、担当教員からの指導を受けながら、博士前期課程もしくは博士後期課程での研究課題に取り組みます。
研究成果は、国内のセキュリティ関係の主要研究会やシンポジウム更には国際会議において発表を行っていきます。そして、発表で得られたフィードバックを元に修正を行い、学術雑誌へ投稿して、掲載を目指します。

研究室生活の紹介等

一人1台のPCを使用することができます。
過去にソフトボール大会への参加やフットサル、卓球、ランニング、サイクリングなどの企画あり。
研究の疲れを癒すジュースやお菓子もあります。

教員からのメッセージ

研究室では技術的な側面からアプローチしますが、情報セキュリティは、暗号理論もしくはITセキュリティやその基盤となる計算機科学、計算機工学、情報通信工学の知識や技術だけでなく、管理運営手法、法律・社会制度、モラルや心理などにも関連します。広い視点で課題を捉えながら、解決方法を探ってください。
学外からの進学状況は、国内の他大学からの進学実績があります。留学生も受け入れています。
修士号取得後に博士後期課程に進学し、産学連携イノベーション人材養成コースに参加して、大手の企業でのインターンシップを経験してきた学生もいます。
修了生は通信系、ソフトウェア系などの一般企業、もしくは、大学職員などの幅広い分野で活躍しています。

最近(過去3年間＋必要に応じて)の修士論文題目

修了年月	タイトル
2021.3	機械学習における敵対的エグザンプル対策について
2021.3	検証可能関数とその応用について
2021.3	暗号のホワイトボックス化に関する研究
2021.3	編集可能ブロックチェーンに関する研究
2021.3	ウェブアクセス履歴に係わるプライバシーリスクについて
2020.3	IoTシステムセキュリティ技術に関する研究
2020.3	サイバーセキュリティ向けデータバックアップ手法に関する解析
2020.3	Webアクセス履歴データにおける位置情報を考慮したプライバシーリスク分析
2019.3	クラウド・エッジコンピューティング環境下のセキュリティ・プライバシー技術の検討
2019.3	ブロックチェーンにおける公平性のためのインセンティブ設計に関する研究
2019.3	暗号技術における確率分布の近似に関する研究
2019.3	IoT向け暗号実装に関する研究
2019.3	パーソナルデータのプライバシリスク評価に関する考察
2019.3	A Study on the Effective Detection Method against Adversarial Examples (敵対的エグザンプルに対する効果的検出手法に関する研究)
2017.3	合理的な証明と合意プロトコルの構成法に関する研究

2017.3	プライバシーとユーザビリティを向上させるシステムの構成と評価
2017.3	無線LAN情報を用いた認証に関する研究
2017.3	ARM Cortex-M0マイクロコントローラ向け暗号ライブラリの実装と評価
2016.3	簡易で安全なWebシングルサインオン方式の構成と実装
2016.3	ユーザビリティとインセンティブを考慮した暗号技術に関する研究
2015.3	パターンロックにおける覗き見耐性の改善
2015.3	クッキー漏洩に起因する成りすまし被害の低減手法
2015.3	完全準同型暗号の構成に関する研究
2015.3	位置情報に基づくユーザ識別手法の検討
最近（過去3年間＋必要に応じて）の博士論文題目	
修了年月	タイトル
2021.9	Design and Implementation of the Efficient and Secure Content Distribution Scheme in Named Data Networking （名前に基づくネットワーキングにおける効率的で安全なコンテンツ配信方式の設計と実装）
2020.9	A Study on the Preservation of Name Privacy in Named Data Networking （名前付きデータネットワーキングにおける名前プライバシーの保護に関する研究）
2019.9	A Study on the Personal Privacy Preservation in Set-Valued Database Publishing （集合値データベースでの個人プライバシーの保護に関する研究）
2019.9	Trust Establishment for Fog Computing Service in Vehicular Network （車両ネットワークにおけるフォッグコンピューティングサービス向け信頼確立）
2016.9	A Study on the Secure Online Examination System（安全なオンライン試験に関する研究）
研究室連絡先メールアドレス	満保雅浩 <mambo *at* ec.t.****> ****: kanazawa-u.ac.jp