情報数理・融合システム分野

情報セキュリティの基礎理論
暗号・論理・数理で実現するSociety 5.0

岡﨑研究室では暗号の研究をおこなっています。暗号はICT社会をささえるインフラの要素として重要となっています。しかし、暗号は情報理論、計算理論、あるいは数学など情報工学のさまざまな技術分野の上に成り立つ総合的な学問分野であり専門家の数は限られています。数理的技法を用いてコンピュータを使って暗号システムの安全性を検証する仕組みを作り、暗号の専門家でなくてもセキュリティバイデザインを実現するために暗号技術を正しく使い、安全な情報システムの設計・開発が行えるようにします。

准教授 **岡﨑 裕之**

博士（工学）
（京都工芸繊維大学）
2021年より現職。暗号理論の研究に従事。数論アルゴリズム応用による暗号方式、形式的安全性証明等に取り組む。

≫ 私の学問へのきっかけ

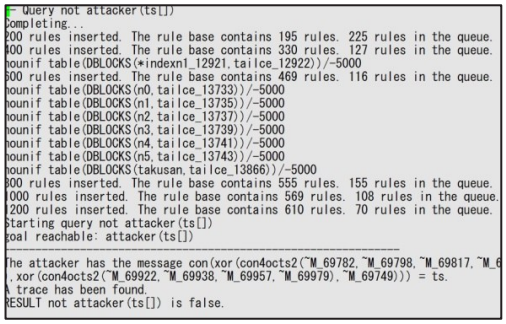
もともと理論物理学をやりたかったのですが、数学が苦手だったので工学系の大学の実験物理学、特に電子顕微鏡の研究をやっていた電子情報工学科に入りました。電気、通信、情報など幅広く勉強しましたが、符号理論の先生が教鞭をとられていた情報数学の講義で苦手であった微分・積分をやらなくてもよい数学があると知りました。セキュリティは情報通信分野全般にわたる応用分野であり、必要とされる課題が尽きません。

≫ 研究から広がる未来

IoT,フィンテックをはじめとするSociety 5.0を実現する様々なテクノロジーは暗号技術なくして成り立ちません。電子情報システムのすべてを支え、ブレイクスルーをもたらす根幹技術を開発しましょう。

≫ 卒業後の未来像

情報セキュリティ人材が不足しています。暗号に限らず情報セキュリティに関する理論、技術、法律やマネージメント等幅広い知識を習得し、情報セキュリティの専門家として活躍することを期待しています。



形式的安全性検証ツールProVerifによる
CBCのパディングオラクル攻撃導出（抜粋）

エプソンアヴァシス株式会社共同研究
IoTセキュリティ（TMP2.0へのサイドチャネルアタック実験）

RISS:018816®

LinuC-3

教員本人の資格試験及び学生への指導に取り組んでいる

情報処理安全確保支援士
（登録番号018816）
LinuCレベル3 303 Security認定

先鋭融合　知能機械　情報サイエンス　情報デザイン

研究キーワード　暗号理論・形式的手法・定理証明・計算理論・数理論理・数理構造

研究シーズ

- 形式的手法による暗号方式の安全性証明
  - 確率的関数の識別不能性の形式化
  - アルゴリズムの形式化
  - 暗号方式の形式化
  - 計算量の形式化
- 暗号プロトコルの安全性自動検証
  - 暗号プリミティブの形式化
  - 暗号プロトコルの安全性検証（SSL/TLS等）
  - **IoTの通信プロトコル等も安全性検証できます**

共同研究・外部資金獲得実績

- 科研費（代表）基盤（C）令和7年-令和10年
  ブロックチェーン関連技術の形式的安全性検証に関する研究
- 科研費（分担）基盤（C）令和4年-令和7年
  ネットワークシステムのセキュリティで等価な仮想評価環境の構築
- 科研費（代表）基盤（C）平成29年-令和2年
  形式手法による暗号の安全性証明自動検証システムの開発
- 科研費（分担）基盤（C）平成30年-令和3年
  情報セキュリティ人材育成のための暗号技術学習支援eラーニングシステムの開発
- 共同研究（エプソンアヴァシス株式会社）　令和元年度より
  IoTデバイス間相互認証方法の研究
  （共同研究成果）
  PatentNo.：US11,757,856B2
  Mienoetal.（45)DateofPatent：Sep. 12, 2023
  CRYPTOGRAPHICCOMMUNICATION SYSTEM,CRYPTOGRAPHIC COMMUNICATIONMETHOD,AND CRYPTOGRAPHICCOMMUNICATION APPARATUS

最近の研究トピックス

無線LANセキュリティ
情報処理学会
第61回インターネットと運用技術研究会　学生奨励賞を受賞
WPA2-Enterpriseに対する
RaspberryPiを用いた2段階
EvilTwin攻撃の提案

表彰状

優秀教育実践賞

2019年1月23日に愛媛大学で開催された日本ソフトウェア科学会 第5回実践的IT教育シンポジウムにおいて発表されたあなたの論文

形式的安全性検証ツールを用いた暗号教育の実践と eProvingeasing教材化の課題について

日本プログラム委員会において優秀教育実践賞の受賞にふさわしい優秀な論文と認められました。
よってここに表彰いたします

2019年1月23日

一般社団法人 日本ソフトウェア科学会
実践的IT教育研究会
主査 田原 康之

第5回実践的IT教育シンポジウムrePiT2019 in 愛媛において電子情報システム工学科3年次科目デザインプロジェクトＩで行った暗号プロトコル設計演習の取り組みが優秀教育実践賞として表彰されました