セキュリティは私達のライフライン

サイバーセキュリティ領域
宮地研究室

宮地 充子（教授），高野 祐輝（特任准教授），奥村 伸也（助教）

キーワード

セキュリティ，暗号，ネットワーク，数論アルゴリズム，OS，プログラミング言語，ポスト量子

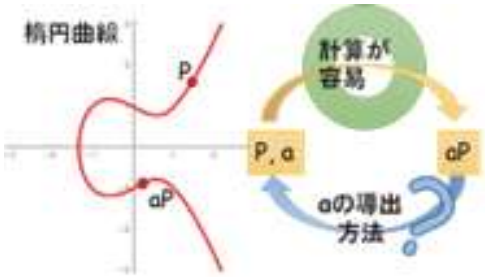
本研究室は安全・安心な社会を実現する情報セキュリティの骨格となる暗号理論，ビッグデータ解析・利活用を促進するセキュリティ技術，IoT機器を用いた各種アプリケーションにおけるプライバシ技術からサイバーセキュリティ技術の最前線までを研究する情報セキュリティ研究拠点である．

セキュアなビックデータ利活用の最前線

近年，車や家電製品などが IoT機器として多様・大量の情報をインターネットへ発信しており，このビッグデータの解析・利活用が次世代産業創生の鍵となるが，その普及・発展のためには，情報の安全を確保すること重要な課題となる．データを利活用する方法として，Private Set Intersection（PSI）に関する研究を行っている．PSIとはデータのプライバシを秘匿し，各機関のデータを解析する技術である．研究室では，PSIを拡張した新たなデータ解析手法や最適化に関する研究を行うとともに，企業や医療機関と連携し，実用化をすすめている．

IoT向け暗号のセキュアな構築

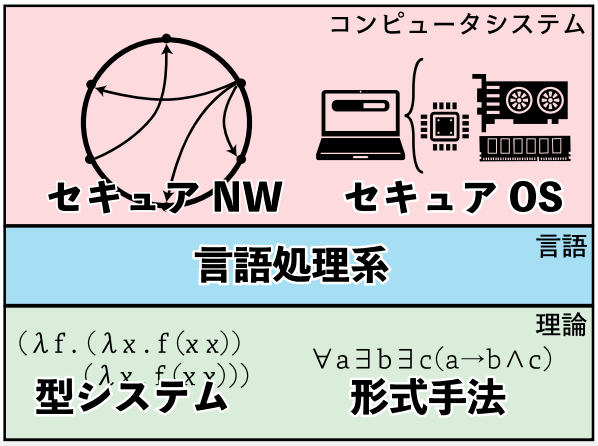
楕円曲線暗号は短い鍵長で実現可能であるため，計算資源やメモリ容量が制限された組込み機器に利用される．研究室では安全性を高める研究や，処理の高速化等の楕円曲線暗号の最適化全般に関する研究を行っている．逆に，楕円曲線暗号の安全性を検証するために，安全性の根拠であるECDLPに対する解読に関する研究も行っている．



信頼のおけるソフトウェアの設計・実装

アルゴリズムがいくら安全であったとしても，その実装が間違っていては安全とは言えない．事実，現状ではほとんどの脆弱性はソフトウェアのバグに起因するものである．

そこで，本研究室では，型システムや形式手法といった技術も活かし，言語処理系，オペレーティングシステム（OS），ネットワークソフトウェアといったシステムソフトウェアを，セキュアで高信頼に設計・実装するための研究をしている．研究を通して，Rust，Haskellといったプログラミング言語や，UNIXなどのOS，TCP/IPなどのネットワークに詳しくなる．



情報セキュリティの基礎理論

情報
セキュリティ

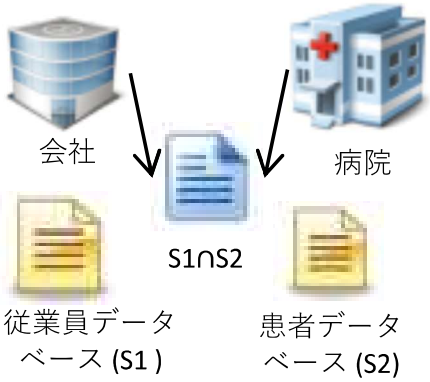
数理・情報科学の基礎理論

情報セキュリティの基礎理論

情報セキュリティは数理・情報科学の強固な理論的基盤によって支えられている. 研究室では, 数学, 計算量理論, 符号理論, 情報理論などを駆使し, ポスト量子暗号などの情報セキュリティ技術の限界に挑む.

共通鍵暗号はデータ及び通信の暗号化に利用され, 情報秘匿と改ざん防止を実現する. 研究室では, 共通鍵暗号に対して様々な攻撃を加え, 共通鍵暗号の解読を行うことで安全な暗号の実現を目指す.

Private Set Intersection



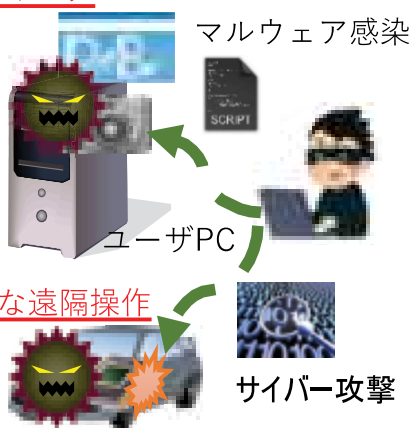
耐量子暗号

現在の計算量理論に基づく暗号は, 量子計算機の出現により, 解読されます. 量子計算機が実現されても安全な暗号, それが耐量子暗号です. 現在, 耐量子暗号の世界標準が進められています.

本研究室では, 提案されている耐量子暗号の解読による安全性解析や, 耐量子暗号を用いた各種プロトコルの構築を行っています. さらに, 高速な準同型暗号を実現できる耐量子暗号も存在します. 準同型暗号とは情報を暗号化したまま様々な演算が可能となる新しい技術であり, ビッグデータ処理でのプライバシ保護を達成する基盤として大きな期待を集めている. 研究室ではこの新しい暗号技術の効率化や多機能化, それらに基づくビッグデータ処理への応用技術に関する研究を行っている.

準同型暗号

ハッキング



欺瞞的防御システム

ファイアウォールや侵入検知システムといった従来型の境界型防御システムでは, 標的型攻撃などの高度化するサイバー攻撃に対して十分に防御することができなくなってきている. 事実, 日本国においても, 国民年金機構や国防関連企業など様々な組織が標的型攻撃の被害にあっており, もはや一企業, 一組織だけの問題ではなくなってきている.

そこで, 本研究室では, 攻撃者に侵入されることを前提として防御を行う欺瞞的防御システムの研究を行っている. 欺瞞的防御システムでは, 通常利用しているネットワーク内に, 囮となるノードやデータを配置し, サイバー攻撃の標的をそれら囮ノードへそらすことで, 攻撃の横展開などを遅らせる, あるいは被害を低減させる.