教員名	松浦幹太教授	研究場所	生研	研究分野	情報セキュリティ

情報セキュリティの研究

―暗号、ネットワーク、そしてマネジメント―

【概要】 松浦研究室では、情報セキュリティの立場から、誰もが快く生活できる社会へ貢献することを研究目標としている。暗号、ネットワークセキュリティ、セキュリティマネジメントの三大分野をカバーし、目標にアプローチしている。卒業生は、技術分野だけでなくコンサルティング分野でも活躍している。

【主要な研究】

暗号学とその考え方（評価のあり方）に基礎を置き、それら基礎研究を行うほか、以下の分野で開拓者的な研究に挑戦している。一見、対象が分散しているようではあるが、本質的にはいずれも数学などの理論基盤と実データによる検証を重視している。近年は、暗号（基礎理論）とセキュリティマネジメント（経済理論と実践の双方）が伸びている。

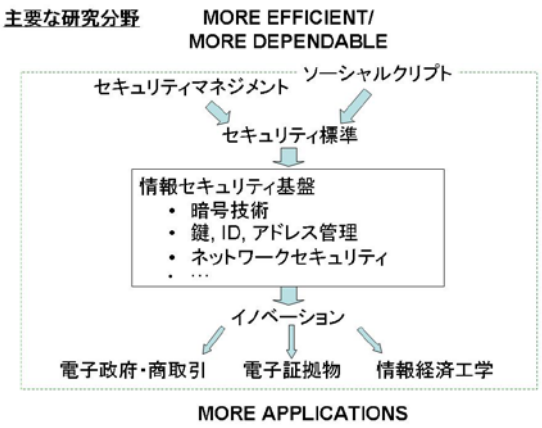
１．暗号とネットワークセキュリティ

誤った安全性評価は不幸を招く。我々は、メンバー全員が暗号理論から安全性評価の考え方を学び、研究を進めている。したがって、幾つかの安全性定義の間の関係（例えば、「前提 A のもとで B という攻撃に対して C という耐性を持つ」という安全性が「前提 D のもとで E という攻撃に対して F という耐性を持つ」という安全性と等価である、などの関係）を厳密に証明する研究のように証明可能安全性と呼ばれるアプローチの研究をしているメンバーがいるが、来訪者があれば他のメンバーもその内容を説明する。このアプローチは、職人芸的なアルゴリズムをブラックボックスとしてシステムを組みパスワード認証の限界を克服する認証技術など、身近な応用へと発展している。**深い理論が応用の拡大に貢献する喜びを体験できる分野である。**

ネットワークにおいては、不正ソフトウェアによる攻撃やサービス妨害(Denial-of-Service: DOS)攻撃、遠隔操作ウィルス事件で話題になった匿名通信システムを悪用した犯罪など、実際に様々な問題が起きている。我々は、それらへの対策とその評価手法を研究している。例えば、匿名通信システムの順探知技術では、世界のトップパフォーマンスを達成した。**厳しいがやり甲斐のある競争を数字で実感できる分野である。**

２．セキュリティマネジメント

株式の誤発注事件では、損失分担の分岐点が争点となった。セキュリティインシデントで被害が出ても、最後は保険でカバーしようという考えもある。電子社会において「お金」は紛争解決や補償の重要な要素であり、情報セキュリティは経済学と深い関係がある。経済主体の行動は、心理的側面を知らなければ理解できない。我々は、情報セキュリティ経済学や心理学の先駆的研究に取り組んでいる。例えば、2001 年に我々が発表したリスク管理理論は、最近問題となっているビットコインのような仮想通貨とそのリスク管理に役立つ金融商品を一般化したものである。また、広義の仮想通貨に関する研究では、交換可能なポイントやマイルに関するセキュリティの実証研究に世界で初めて成功した。**開拓者としての冒険ができる分野である。**



研究室連絡先(生研 E 棟 4 階 Ew-401 号室)：
（内線 56286）
教員連絡先(生研 E 棟 4 階 Ee-403 号室)：
kanta@iis.u-tokyo.ac.jp （内線 56284）