つじい しげお　　第２２回　２００６年度　高柳記念賞

辻井 重男　氏

「通信に於ける情報セキュリティ技術及び暗号理論に対する貢献」

辻井重男氏は、早くから研究対象として情報セキュリテイ技術、特に暗号理論に着目しており、これらの分野で先駆的な研究活動を行い、また、本分野の指導者として多くの研究者を育成するだけでなく、産業界・国際的にも多くの業績を挙げられている。

(1) 公開鍵暗号方式の研究

1980 年代、多変数多項式の求解困難性に基づく公開鍵暗号、「順序解法を利用した公開鍵暗号方式」を世界に先駆けて考案している。現在、公開鍵暗号としては、素因数分解の困難性に依拠する RSA 暗号、或いは離散対数問題の困難性に基づく楕円暗号が多く利用されているが、これらは量子コンピュータが出現した場合、理論的には解読可能であることが示されたことなどを受けて、1990 年代から現在まで、内外から様々な多変数多項式型公開鍵暗号が提案されている。同氏は、2003 年、殆どの多変数多項式公開鍵暗号の安全性を強化することの出来る汎用的手法として、「持ち駒を利用した公開鍵暗号方式」を考案しており、量子計算機が実現した際の暗号技術を対象とする世界初の国際会議 PQCrypto に採録されている。同氏が先駆的に研究を行なった多変数方程式の求解困難性に基づく公開鍵暗号方式は、現在でも、次世代の暗号方式の候補として、世界各国で活発な研究開発が進められている。

また、世界で最初となる ID based 暗号方式を離散対数問題の困難性に基づいて創案するとともに、各種暗号方式の安全性検証にも精力的に取り組み、ナップザック問題に基づく暗号方式としては唯一解読法が示されていなかった乗算型ナップザック暗号の解読手法を見出すなど顕著な成果を得ている。

(2) 暗号プロトコルの研究

同氏は、早くからゼロ知識証明の理論的側面を研究し、能力のゼロ知識証明に関する考察や通信ラウンドの最適化に関する数多くの結果を得ている。また、同氏は暗号プロトコルに関する研究にも取り組み、ID 情報に基づく認証方式における安全性向上のための鍵更新方式を提案している。これは、後に Forward Security と命名され、学会において重要な概念として再発見されている。更には、剰余暗号を用いた Mental Poker の提案や秘密分散共有法の組合せデザインによる考察などの理論的な成果とともに短いメッセージを用いた同報通信のような具体的な手法についても成果を得ている。

(3) (超)精円暗号の研究

安全でかつ実用的な楕円暗号・超楕円暗号方式を構成するために重要な曲線の構成法、その安全性評価、高速計算法の考案などについて、CM テストやリフテイングといった手法を用いて安全な曲線を構成する数多くの方式やそれらの曲線上で構成されるヤコビ多様体における離散対数問題の困難性検証、加法演算の高速計算法などの成果を得ている。

(4) 情報セキュリティの研究

ネットワークセキユリテイの分野で、プライバシー保護を考慮した電子資金移動方式の提案やデータベースネットワークの情報セキュリテイに関する考察、送受信者追跡の不可能な通信プロトコルに関する研究、実用的な電子投票方式の考案などの成果を得ている。また、バイオ情報に基づくセキュリテイの分野では、DNA - ID を用いた DNA 個人情報管理システムの提案、DNA バイメトリックス本人認証方式の提案などをするだけでなく、IC カードと本人との一体的連結性強化のため、人間が有する唯一のデジタル情報である DNA 情報を、プライバシー問題を回避しつつ、数理的構造として暗号鍵への埋め込みといった画期的な提案を行なっている。

(5) 学会・政府関連活動

同氏は、電子情報通信学会において、情報セキュリテイ研究専門委員会、情報通信倫理研究会各委員長、総務理事、副会長、などを歴任の後、平成 8 年度には会長として学会の運営に貢献されました。また、現在、日本セキェリテイマネッジメント学会会長として、情報セキュリテイ総合科学の発展に尽力され、さらに、Asiacypt'90(亜州暗号学国際会議)をはじめ多くの国際会議の組織委員会委員長等を務められました。

郵政省電子決済、電子現金とその利用環境整備に関する調査研究会座長、郵政省電波監理審議会委員、内閣官房電子政府評価・助言会議委員、総務省電波監理審議会会長、文部省学術審議会専門委員、日本学術会議会員などを歴任され、学術・技術行政にも貢献され、その功績に対し、多くの賞を受賞されております。また、世界的研究拠点を育成するため、文部科学省が実施している 21 世紀 COE プログラムに対し、同氏が中央大学の情報セキュリテイグループを結成して応募した「電子社会の信頼性向上と情報セキュリテイ」が、国立・公立・私立大学の中で、唯一、情報セキュリテイ分野の研究拠点として採択され、現在も研究活動を続けられております。

経　歴　1933 年生まれ

学　歴　1958.3　東京工業大学 電気工学課程卒業

1970.1　工学博士の学位取得(東京工業大学)

職　歴　1958,4　日本電気株式会社 入社

1965.3　山梨大学 工学部助教授

1971.4　東京工業大学 助教授

1978.7　東京工業大学 教授

1994.4　東京工業大学 名誉教授

1994.4　中央大学 理工学部教授

1999.7　中央大学 研究開発機構長

2004.4　中央大学 研究開発機構教授

2004.4　情報セキュリテイ大学院大学 学長

受賞歴

社団法人発明協会 関東地方発明表彰(1978)

電子情報通信学会　論文賞（1980 年度、1988 年度、1990 年度）

著述賞（1984 年度)、業積賞（1984 年度）、功績賞（1995 年度）

財団法人大川情報通信基金 大川出版賞（1996）

日本エリクソン株式会社 日本エリクソンコミュニケ ―ションアワード（1999）

米国電気電子学会（IEEE）　第三千年紀記念賞（2000）

総務省 「電波の日」総務大臣表彰(2003)

日本放送協会 第 55 回放送文化賞(2004)