2008年度 大川賞受賞者

受賞理由

RSA暗号の創案ならびに暗号技術の進展に関する多大な貢献

アディ シャミア　博士

現　　職　ワイツマン研究所　Paul and Marlene Borman 応用数学教授（イスラエル）

学　　位　Ph.D（ワイツマン研究所　1977年）

生 年 月 日　1952年7月6日（56才）

略　　歴

1973年	テルアビブ大学（イスラエル）卒業
1975年	ワイツマン研究所（イスラエル）計算機科学　修士
1976年	ワーウィック大学（英）計算機科学科　研究員
1977年	ワイツマン研究所　計算機科学　博士
1977年	MIT（米）数学科　講師
1978年	同　助教授
1980年	ワイツマン研究所　応用数学科　准教授
1984年	同　教授・計算機科学　ボーマン教授

主な受賞等

1975年	ワイツマン研究所フェインバーグ大学院 ジョン・F・ケネディ賞
1978年	米国電気電子学会（IEEE） 情報理論グループ　最優秀論文賞
1982年	イスラエル情報処理学会　特別賞
1983年	ワイツマン研究所　ルーベル賞
1983年	イスラエル数学会　エルデシュ賞
1986年	IEEE　ベイカー賞
1990年	フランス　UAP　UAP科学賞
1992年	バチカン　法王庁アカデミー　ピウス11世 ゴールドメダル
1994年	イスラエル　ロスチャイルド賞
1997年	米国計算機学会　カネラキス賞
1998年	イスラエル科学アカデミー会員に選出
2000年	IEEE　小林賞
2002年	米国計算機学会　チューリング賞
2003年	フランス　高等師範学校　名誉博士
2004年	国際暗号研究学会フェローに選出
2005年	米国国立科学アカデミー会員に選出
2007年	欧州学術院会員に選出
2008年	イスラエル賞（計算機科学部門）

主な業績

シャミア博士は、情報セキュリティ技術の基盤である暗号に関して多くの基本的な研究成果を挙げ、現代暗号理論の創生と発展、ならびに実用化に多大な貢献をした。その中で特筆すべき業績は、リベスト、エーデルマン両博士とRSA暗号を提案したことである(1977)。これは、公開鍵暗号の初めての具体例であり、広く実用に供された。現在、インターネットやICカードなどに使用されている公開鍵暗号のほとんどはRSA暗号である。この功績でリベスト、エーデルマン両博士とチューリング賞を共同受賞している。

これに留まらず、シャミア博士は、暗号技術の基本的手法となっている秘密分散法の提案（1979）、秘密情報を漏らさずに認証、署名を行う零知識認証・署名法(Fiat-Shamir法/Feige-Fiat-Shamir法)の提案（1986、1988）、およびそれらの方法を応用した有料放送方式の開発と実用化への貢献、さらには次世代暗号の有力候補である「ID（識別子）に基づく暗号」の概念の提案(1985)など、暗号技術とその応用に関する多くの業績を上げてきた。近年も、プライバシー保護技術の基盤となり得るリング署名、電子投票等への応用が期待される視覚復号型暗号(1994)などの提案を通じて、現代暗号理論のさらなる展開に大きな影響を与え続けている。また、小額決済のための簡便な電子マネー方式の提案など、実用につながる技術に対する貢献も枚挙に暇がない。

また、一方で、シャミア博士は各種の暗号に対する攻撃法の提案を通じて、暗号の安全性向上に大きく貢献した。具体的には、米国連邦政府標準暗号であったDES暗号をはじめとする実用共通鍵暗号の解読に大きなインパクトを与えた差分攻撃法(1989)のほか、マークル-ヘルマン暗号の解読(1982)、専用ハードウェアTWIRLの考察に基づくRSA暗号の安全性の検討(2003)やヨーロッパの標準暗号SFLASHの実際的攻撃法(2006)などが挙げられる。

さらに、認証、署名方式の理論的基礎をなす「対話証明」に基づく計算モデルと従来の計算量モデルの関係を明らかにして、多項式オーダーの対話回数からなる対話証明をもつ言語クラスIPと多項式オーダーの空間複雑度を有するチューリング機械で受理可能な言語クラスPSPACEとの等価性を示すなど、計算量理論分野へも大きな貢献をした(1992)。

現代暗号理論に基づく情報セキュリティ技術は、現在そして将来の情報化社会において安全・安心を得るために必要不可欠な基盤技術である。この現代暗号理論の創成、発展とその応用展開において、シャミア博士は、多くの画期的発明やそれを実現する技術開発の指導さらには優れた研究者の育成を通して、先導的かつ主導的役割を務め、暗号研究分野において長年にわたり指導的役割を果たしてきた。シャミア博士は情報化社会の安全・安心を実現する技術に対する貢献において、最高の研究者であると言うことができる。

これらの業績により、博士は、欧州学術院、米国国立科学アカデミー（NAS）、イスラエル科学アカデミーなどの様々な学会のメンバーに選出され、チューリング賞（ACM, USA）、イスラエル賞、ピウス11世ゴールドメダル（バチカン法王庁アカデミー）など数多くの賞を受賞した。

このようにアディ シャミア博士のRSA暗号の創案ならびに暗号技術の進展に関する多大な貢献に対し、ここに大川賞を贈呈してその功績をたたえるものである。