2008年度 大川賞受賞者

受賞理由

符号理論と暗号理論ならびにその応用に関する研究への多大な貢献

今井　秀樹　博士

現　　職　中央大学　理工学部　教授
東京大学　名誉教授
産業技術総合研究所　情報セキュリティ研究センター長

学　　位　工学博士　（東京大学　1971年）

生年月日　1943年5月31日（65才）

略　　歴
1966年　東京大学　工学部　卒業
1968年　同　大学院　工学研究科　修士課程修了
1971年　同　博士課程修了
1971年　横浜国立大学　工学部　講師
1972年　同　助教授
1984年　同　教授
1992年　東京大学　生産技術研究所　教授
2005年　産業技術総合研究所
情報セキュリティ研究センター長兼務（現在に至る）
2005年　日本学術会議会員兼務（現在に至る）
2006年　中央大学　理工学部　教授（現在に至る）
2006年　東京大学　名誉教授

主な受賞等
1976年・1991年・1992年・2003年・2004年・2008年
電子情報通信学会著述賞、論文賞
1992年　IEEEフェロー
1992年・2003年
電子情報通信学会　年間最優秀論文賞
（米澤賞,猪瀬賞）
1998年　米国電気電子学会（IEEE）
情報理論ソサイエティ・ゴールデン・ジュビリー・ペーパー・アワード
2002年　総務大臣表彰,経済産業大臣表彰
2007年　国際暗号研究学会（IACR）フェロー
2007年　The Wilkes Award（British Computer Society）

主な業績

今井博士は、通信の効率化と情報の保護に関して数多くの課題に取り組み、斬新かつ独創的な視点を持ってその分野における新たな基礎理論を生み出した。また、それらの理論を基礎とする応用技術のいくつかは実用化され、様々な分野において通信品質の向上や情報の安全性の向上に欠かせない技術となっている。さらに、国内外の暗号分野の研究者を束ね、暗号技術の評価を多面的に行い、我が国の電子政府において安全に使える推奨暗号のリストを作成するなど、暗号・情報セキュリティ政策にも大きく貢献した。

博士は、1966年東京大学 工学部 電子工学科を卒業し、1971年同大学院 工学研究科 博士課程 電気工学専攻を修了後、直ちに横浜国立大学講師として採用され、1972年同助教授、1984年同教授に昇任した。1992年東京大学教授に就任し、2005年からは産業技術総合研究所 情報セキュリティ研究センター長を兼務している。2006年に東京大学名誉教授の称号を与えられ、同年、中央大学教授に就任した。この間、情報通信分野において研究・教育活動を推し進め、優れた研究成果を挙げるとともに研究者・技術者を数多く学界・産業界に送り出している。

研究面では、1971年より符号理論の研究に携わり、2次元系列・2次元巡回符号の先駆的研究を行い、この分野の開拓に多大な貢献を行った。1970年代の中頃には、符号化変調の先駆的業績であるマルチステージ復号法とマルチレベル符号化法を提案し、学界および産業界に大きなインパクトを与えた。この符号化変調の研究分野は、符号理論と変調理論の境界に位置する分野として、大きな分野に成長すると共に、極超短波通信や衛星放送などにおいて実用化され、また、光通信などの分野への応用も期待されている。1970年代から1980年代には、符号分割多元接続（CDMA）の干渉波除去方式に関する先駆的研究を行い、世界に先駆けて論文を発表し、新たな研究分野の開拓に大きく貢献した。干渉波除去技術は、第3世代携帯電話のW-CDMA方式や地上デジタル放送等においても利用されており、通信の品質を上げる際の欠かせない要素技術の1つとなっている。

1970年代の後半からは、暗号理論の研究を開始し、多次多変数多項式や線形符号に基づく公開鍵暗号方式、情報量的に安全な電子署名方式、量子鍵共有方式など既存の計算量的な安全性に頼らない暗号技術に関する先駆的研究を行い、長期間の安全性を確保するために必要となる新たな暗号理論を構築した。これらの理論は、世界中の暗号分野の研究者に大きな影響を与え、情報理論的に安全な暗号や量子計算機出現後にも安全に使える暗号など、新たな研究分野の形成に大きく貢献している。また、人間の視覚を使ったのぞき見に強い認証方式や、短いパスワードを安全に使える認証鍵共有プロトコル、プライバシ保護など、人的要素を暗号技術に取り入れるヒューマンクリプトという独創的な研究分野を提唱し、ユニークな視点をもって暗号研究に取り組んできた。さらに、相手のIDを使って予備通信を行うことなく安全に秘密鍵を共有するKPS（Key Pre-distribution System）やIDベース暗号、電子透かしや著作権保護方式などの一連の研究を通して、情報の安全性を高めるための基礎技術の確立に大きく貢献した。これらの一部は、情報家電などに採用され、映像や音楽などのコンテンツを、著作権管理ポリシーを遵守する機器間でやり取りする方式の一部として利用されている。

以上のように、符号理論、暗号理論の幅広い見地から世界に先駆けて取り組んできた一連の研究成果は、それぞれ情報通信研究分野の進展に大きく寄与しており、これらの業績に対し、電子情報通信学会（IEICE）から米澤ファウンダーズ・メダル、業績賞、猪瀬賞、功績賞及びフェロー会員の称号などを授与され、米国電気電子学会（IEEE）からフェロー会員の称号、同情報理論ソサイエティからGolden Jubilee Award、国際暗号研究学会（IACR）からフェロー会員の称号、英国コンピュータ学会からWilkes賞を授与されるなど多くの賞を授与されている。

これらの学術活動に加え、内閣情報通信技術戦略本部情報セキュリティ部会委員、総務省・経済産業省暗号技術検討会座長、暗号技術評価委員会（CRYPTREC）委員長など多数の要職を歴任し、我が国の情報通信技術に関わる学術行政と科学技術の推進に貢献している。特に、CRYPTRECでは委員長として国内外の暗号研究者を束ね、多面的に暗号技術の評価を行い、電子政府において安全に使える推奨暗号のリストを作成するなど、我が国の情報セキュリティ政策にも大きく貢献した。これらの業績に対して、総務大臣表彰および経済産業大臣表彰を受けている。

以上のような今井博士の符号理論と暗号理論ならびにその応用に関する研究と、暗号・情報セキュリティ政策を通じた社会への多大な貢献に対し、ここに大川賞を贈呈しその功績をたたえるものである。