宮地充子先生の文部科学大臣表彰
科学技術賞受賞（研究部門）に寄せて

筑波技術大学保健科学部
岡本　健

北陸先端科学技術大学院大学・情報科学研究科の宮地充子先生が平成 26 年度科学技術分野の文部科学大臣表彰科学技術賞（研究部門）を受賞されました．心より敬意を表するとともにお祝いを申し上げます．これまでの成果について，受賞された業績を中心に私が知っている範囲のことを述べます．

先生がこれまで取り組んでこられた主要な研究の一つに楕円曲線暗号があります．楕円曲線の研究は，数論において重要な位置を占めますが，これを暗号に応用したものが，楕円曲線暗号です．この暗号は公開鍵暗号系に分類され，小さい鍵サイズで高い安全性を実現できることから，安全な ICT 社会を構築するのに不可欠な要素技術となっています．楕円曲線暗号は，1980 年中頃に発見されましたが，先生は黎明期から，この分野の研究に従事されました．

楕円曲線暗号系の一つとして，ペアリングを用いた暗号方式があります．ペアリングとは双線形写像 $e:G_1\times G_2\rightarrow G_T$ を満たす非退化な一方向写像であり，$e(aP,Q) = e(P,aQ) = e(P,Q)^a$ という性質をもちます．ここで，G_1, G_2, G_T は同じ位数を持つ群，a は整数，$P\in G_1$, $Q\in G_2$ です．現代暗号で用いられるペアリングは楕円曲線を用いて定義されています．ペアリングを用いた暗号は，従来の公開鍵暗号では実現が困難であった新たなセキュリティパラダイムを構成できることが知られており，現在，世界中の技術者，研究者によって精力的に研究が進められています．

楕円曲線がある特定の条件を満たすとき，その曲線を「ペアリングに適した（paring-friendly）楕円曲線」と呼びます．先生の研究グループでは，埋め込み次数と呼ばれるパラメータ k=3, 4, 6 の場合において，曲線のパラメータがもつ特徴を明確にしました．また，k=3 において，素数位数をもつ paring-friendly 楕円曲線の構成アルゴリズムを示しました．この手法によって選ばれた曲線は，研究提案者の名前から MNT（Miyaji-Nakabayashi-Takano）曲線と呼ばれています．この成果は，楕円曲線暗号に対し，数学的な厳密性をもって暗号の安全性を証明することが可能であることを示唆しています．楕円曲線暗号に対して，このような安全性を示したのは，著者の知る限り初めての試みです．

また，ペアリングは対称と非対称のタイプに分けられます．ペアリング暗号が出現した当初，使用されるペアリングは主に対称タイプに限定されていましたが，MNT 曲線が提案されて以後，この曲線がもつ優位性から非対称タイプにも目が向けられ，多くの

有益な方式が提案されました．このことからも，この曲線が発見されたインパクトが，いかに大きかったかがわかると思います．

2010 年 12 月には，石川県山中温泉にてペアリングに関する国際会議 Pairing 2010 が開催されました．この会議で先生は，プログラム委員長など，運営に関する主要な役割を担いました．これにより国内外の学生，技術者，研究者が親交を深め，ペアリングが暗号の主要な研究の一つとして成長するための場が提供されました．私自身もこの会議の運営に従事しましたが，先生の発案により，エクスカーションに狂言の鑑賞や俳句のレクチャーを行いました．参加者は日本文化に触れ，大変好評のうちに終えることができました．この他にも先生は，多くの研究会や国際会議を運営されており，後進を育てています．

楕円曲線暗号の実装に関しても多くの業績を残しています．暗号解読手法の一つにサイドチャネル攻撃と呼ばれるものがあり，これは暗号装置の物理的な特性を観測することにより秘密鍵などの情報を読み取る攻撃です．先生は全サイドの攻撃に対し，安全な楕円曲線暗号の実装手法を提案しました．この手法は高い安全性に加え，暗号処理におけるメモリ量や計算量を削減すること可能です．この成果は暗号実装において著名な国際会議である CHES 2010 にて発表されています．

さらに国際規格の標準化にも多大な功績があります．暗号は主に通信を用いて利用されます．このため，提案する暗号技術を普及させるには，その技術の標準化・規格化が大変重要になります．ISO/IEC 15946 は，国際標準化機構（International Organization for Standardization: ISO）と国際電気標準会議（International Electrotechnical Commission: IEC）が共同で策定した楕円曲線に基づく暗号技術の規格です．ISO/IEC 15946-1（総論）では，前回の規格においてペアリング暗号に必要な技術が組み込まれていなかったのに対して，先生は既存の楕円曲線暗号の規格と互換性を保ちつつ，規格化することに尽力されました．その他，ISO/IEC JTC1/SC27（セキュリティ技術）ではプロジェクトエディタなどを歴任されています．これらの功績により，2007 年に経済産業省産業技術環境局長賞（国際標準化奨励者賞）など，多くの組織・団体から称えられ，数々の賞を受賞するとともに，日本の情報セキュリティ技術の国際化推進や国際的地位の向上に貢献しました．

先生の功績は，教育研究をはじめ，研究会運営や標準化推進などの社会貢献にまでおよび，いずれも大変素晴らしい成果をあげています．女性の社会進出が求められる今日において，先生の目覚ましい活躍を見て勇気をいただいた方も多いのではないでしょうか．これからもさらに活躍を続けられていくことを心から願っております．