

暗号分野におけるセンターオブエクセレントを目指して研究活動を展開

情報セキュリティ技術の中核となる暗号技術。要素技術から、電子マネー、電子投票、電子入札をはじめとする応用技術にいたるまで、暗号技術の世界的権威である岡本龍明NTT R&Dフェロー・NTT情報流通プラットフォーム研究所情報セキュリティプロジェクト主席研究員に、暗号研究に取り組まれた経緯から今後の抱負までお話をうかがった。

理論と実用が密接に関係している 暗号の面白さに填ってしまった

岡本フェローは、セキュリティがご専門で、特に暗号分野では多くの成果をあげていらっしゃいます。はじめに、岡本フェローと暗号との出会い、興味を覚えたきっかけなどを教えてください。

岡本 私は、1978年に横須賀通信研究所に入社しました。入社前は、武蔵野の研究所でトラフィック理論

を研究していた大学の研究室の先輩の話聞き、そこに入ることを考えていました。しかし研修期間中に、現在のインターネットのような、コンピュータネットワークにより異種コンピュータ間の資源の相互利用を可能とするDCNA(Data Communication Network Architecture)の話聞いて、こちらのほうが面白そうだということで、急遽横須賀の研究所を希望しました。入社して数年間は、横須賀通信研究

所のデータ通信研究部でネットワークアーキテクチャーの研究開発に従事していました。しかし、コンピュータの普及拡大やネットワーク化の進展に伴い、データの盗用やコンピュータの不正使用、通信回線の盗聴などの犯罪が発生し始めました。1982～83年頃に当時の電電公社でも、暗号やセキュリティの研究に本格的に取り組むことになり、数名からなる暗号技術の研究チームが発足。私は、コンピュータネットワークに関連した研究を行っていたこともあり、このチームにアサインされました。自分から研究したいといったわけではありませんが、一度やり始めたらその面白さに完全に填ってしまい、暗号の虜になってしまいました。

どのような点が面白いと思われたのですか…。

岡本 もともと数学は好きでしたので、数学的な理論を使うという点と、アプリケーションというか実際に使われる現場が見えるという点です。私は入社以来、一貫して応用研究色の強い研究所(横須賀通研データ通信研究部、情報通信研究所など)に属して研究業務に携わってききましたが、その中では理論色の強い研究



NTT R&Dフェロー
NTT情報流通プラットフォーム研究所
情報セキュリティプロジェクト
主席研究員
岡本龍明氏
おかもと たつあき

1978年電電公社電気通信研究所入社。暗号・認証理論を中心とした情報セキュリティ理論の研究・開発などに従事。1989～1990年カナダWaterloo大学客員助教授、1994～1995年AT&Tベル研究所客員研究員。1998年科学技術庁長官賞、1998年電気通信普及財団賞を受賞。1999年NTT R&Dフェロー、2003年電子情報通信学会フェロー。現在、NTT R&Dフェロー、情報流通プラットフォーム研究所情報セキュリティプロジェクト主席研究員。京都大学大学院情報学研究所客員教授。工学博士(東京大学)。

に従事してきました。このような環境のため、応用と理論の狭間の中で、応用サイドの話を知ると、それをどのように理論化しようかと考え、理論サイドの話を知ると、その実用性を考えるというようなスタイルで研究を進めてきました。このような形で仕事ができただけでなく、私が主に従事してきた暗号という研究分野が、理論と実用が密接に関係しているという特長を持っていたことによるところが大きいと思います。

基本3要素の研究から、より広範な応用技術にチューンした研究へと拡大

NTTが本格的に暗号技術の研究開発に取り組み始めた1980年代初頭と比べ、基本的な仕組みに変化はありませんか。

岡本 1970年代後半は、現在の公開鍵暗号や、共通鍵暗号による米国のDES (Data Encryption Standard) ができた時代で、まさに暗号が学会レベルで研究されるようになった時代でした。私が暗号技術の研究開発に取り組み始めた1980年代初頭と比べ、暗号技術の基本的な仕組みに大

きな変化はありませんが、当時と比べ大きく変わったのは、周囲の環境です。当時、私たちは暗号の大切さを一生懸命啓蒙しましたが、世の中の反応はよくありませんでした。しかし、1990年代半ばにインターネットが急激に普及拡大するのに伴い、暗号に対する世の中の見方が一変し、現在では誰もが暗号は必要不可欠なツール・基盤技術であると認識するようになりました。それから、当初は暗号の基本3要素である、大量のデータを暗号化する際に用いる「共通鍵暗号」と、共通鍵暗号で使う秘密鍵を配送する「公開鍵暗号」、正当性を保証する「電子署名(デジタル署名)」の研究が中心でしたが、いろんな用途に暗号を使うように、より広範なアプリケーションにチューンした暗号の研究が広がっているという点です。

暗号開発で世界でも先駆的な役割を果たしているNTT研究所

世界的にも競争の激しい暗号分野で、NTTの技術はどのあたりのレベルにあるのでしょうか。

岡本 暗号技術は、秘匿や認証のための暗号アルゴリズムのような要素的技術

から応用技術まで、階層化されています。要素的な暗号技術については、ISO/IECやIEEEで国際標準化活動が進められていますが、加えて各国の政府機関においても暗号アルゴリズムの評価プロジェクトが進行しています。2000年より欧州連合はNESSIE (New European Schemes for Signature, Integrity and Encryption) プロジェクトを発足させていますし、日本でも電子政府推奨暗号選定プロジェクトとしてCRYPTREC (Cryptography Research & Evaluation Committees) が評価活動を行っています。また、IETF (Internet Engineering Task Force) やTV-Anytime Forumなどの団体も認定作業を行っています。このような場にNTTは自社で開発した各種暗号方式を提案して高い評価を得てきており、暗号の要素技術については、世界でもトップレベルにあるといえます(表1参照)。特に三菱電機との共同開発による共通鍵暗号「Camellia」は米国のAES (Advanced Encryption Standard) と並んでNESSIEの第一推薦暗号アルゴリズムに認定された他、日本の電子政府推奨暗号にも公式認定されていますし、IETFのRFCにも採録されています。また公開鍵暗号「PSEC-KEM (Provably

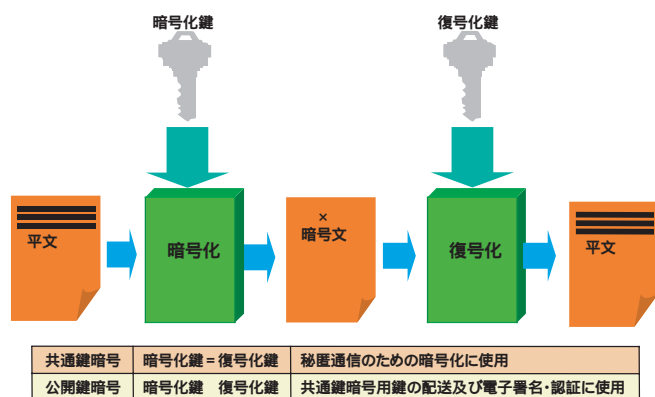


図1 共通鍵暗号と公開鍵暗号

表1 NTT暗号技術の標準化状況

暗号の種類	NTT暗号	主な標準化先
共通鍵暗号	Camellia	NESSIE, CRYPTREC, TV-Anytime Forum, IETF, ISO/IEC (標準化作業中)
公開鍵暗号	PSEC-KEM	NESSIE, CRYPTREC, IETF, ISO/IEC
デジタル署名	ESIGN	ISO/IEC, IEEE

SecureElliptic Curve encryption with Key Encapsulation Mechanism)」も、RSA社の提案を抑えNESSIEで公開鍵暗号の第一推薦アルゴリズムに認定された他、日本の電子政府推奨暗号に公式認定されています。さらにデジタル署名「ESIGN (Efficient digital Signature scheme)」は、国産のデジタル署名として初めてISO/IECの国際標準デジタル署名方式に選定された他、IEEEの標準規格にも採用されています。

一方、電子マネーや電子投票等、暗号技術の応用についても、NTTは1980年代後半から先駆的に取り組んできており、間違いなく世界の先陣を切って走っていると思います。現在、企業において暗号分野でセンターオブエクセレント的な研究活動を行っているのは、NTTとIBMくらいで、その意味でもかなりのポジションにあるといえます。

NTTは、暗号の基本特許を公開していますね。

岡本 NTTでは、Camellia、PSEC-KEM、ESIGN、さらには素因数分解問題ベースの公開鍵暗号EPOC (Efficient Probabilistic public-key encryption) の基本特許を2001年より無償公開しています。

RSA法に比べ、数十倍高速な署名速度を実現したESIGN

岡本フェローは、ESIGNという世界的に優れたデジタル署名方式を発明されていますが、思いついたきっかけなどを教えてください。

岡本 私が暗号の研究を始めたとき、最初に取り組んだテーマの一つが高速なデジタル署名を開発することでした。きっかけは、当時のPCの性能では、代表的なデジタル署名方式であるRSA法を実装した場合、署名作成に1分程度の時間がかかりとても実用に耐えるように思われなかったからです。そこで、当時のPCでも1秒以内で署名の作成と検証が行えるアルゴリズムの開発を目標にしました。

RSA方式の数十倍以上高速な署名方式を、どのようにして実現しようと考えたのですか。

岡本 整数論的な手法から組み合わせ論的な手法まで使える原理を試行していった結果、一番有力そうに思えた手法が数学分野における未解決問題の一つである素因数分解の困難性を使う方法でした。またRSA法は、暗号にも署名にも使えますが、署名に特化すればRSA法よりも高速な方式ができるに違いないという思い込みに基づいて、研究を進めました。いろいろと失敗を繰り返した末に、1985年の国際会議で発表しました。ESIGNの特長は、何とんでもその高速性にあります。当初の目標どおり、RSA法に比べて署名速度で数十倍程度高速で、当時のPCでもソフトウェア実装で1秒以内の署名作成に成功しました。もちろん署名検証も同様に高速です。したがって、PCの性能が格段に向上した現在でも、ICカードや携帯端末といった非常に性能の限られたプラットフォームでも

ESIGNを使うことにより、高速な署名生成が可能です。2002年には、ESIGNをベースに安全性をより高めたESIGN-TSH (Trisection Size Hash)を開発しています。

NTTの電子マネーに関する基本特許が、日本の銀行界を救った

暗号の応用技術として、1980年代後半から電子マネーの研究を行われたということですが...

岡本 電子マネーは、暗号の応用の中でも最も重要な分野の一つです。電子マネーには、オフラインで、つまり店舗がセンターに問い合わせなくても支払い処理が出来るオフライン電子マネーと、オンラインで(店舗がセンターに問い合わせで)支払い処理をするオンライン電子マネーがあります。センターの管理負担や応答速度の観点で、オフライン電子マネーが優れています。一方、電子マネーに要求される条件として、分割利用可能性(利用金額の合計が、額面の金額になるまでどのような額でも利用できる)があります。そこで、分割利用を可能にしたオフライン電子マネーの実現が望まれていましたが、このタイプの電子マネーは困難とされていました。しかし、私たちは、Crypto '91で世界初の分割利用可能オフライン電子マネーを提案し、さらにCrypto '95で効率を向上させた方式を提案しました。さらに、通常の利用環境では匿名性を持っているが、マネーロンダリングなどの不正が行えないように、運用条件により電子マネーの匿名性を剥

奪するような機能を持ったエスクロー電子マネーを開発しました。この方式を基本として、日本銀行金融研修所との共同研究に基づいて複数銀行（電子マネー発行機関）間の決済が可能な実用性の高い電子マネー方式を1996年に開発し、実証実験を行いました。

実は、1980年代後半にNTTは電子マネーに関する特許を出願し、ある意味で日本における電子マネーの基本特許的な位置づけになっていました。1996年に、電子マネーに関する米国の銀行の特許出願を巡って日本の銀行界が異議を申し立てる騒ぎが起きましたが、結果的にはNTT特許の存在もあり、その銀行は中核的な部分を除いたところしか押さえることができませんでした。いわば、NTT特許が米国銀行による電子マネー特許という黒船の日本上陸を水際で食い止めることに大きく貢献したといえるかもしれません。

電子投票への応用についてはいかがですか。

岡本 電子投票は電子マネーと並んで暗号の最も重要な応用の一つであると考えています。私たちは、1992年のAuscrypt '92で、大規模な投票に適し実用性の高い電子投票方式を発表しました。この方式は、MITやワシントン大学など世界各地で実装が行われており、現在最も代表的な電子投票方式となっています。

将来を見据えた量子公開鍵暗号、Universal Composabilityの研究に注力

コンピュータの性能が飛躍的に向

上していく中、今後の暗号技術がどのようになっていくのが展望をお聞かせください。

岡本 将来、量子力学の原理を用いた量子コンピュータが実現できれば、現在使われている公開鍵暗号や電子署名のほとんどは、素因数分解と楕円曲線上の離散対数問題に基づいているため、ほとんどが解読されてしまいます。このような危機に対し、量子原理を暗号に利用した量子暗号の利用が有望視されています。しかし、量子暗号は送信者と受信者との間に、量子通信路という特別な通信設備を必要とし、インターネットのような通常のネットワークには適用できません。また、デジタル署名のような機能も提供しないので、適切な解決策とは思えません。そこで私たちは、通常のネットワークに適用でき、デジタル署名のような機能も提供し、さらに将来的に量子コンピュータが実現されても安全性が保証されるような暗号の概念として、量子公開鍵暗号という新しい概念を提案しています（図2参照）。この概念に基づき、ナップザック問題と代数的整数論を用いた量子公開鍵暗号の具体的実現例をCrypto2000において提案しました。

岡本フェローが特に興味を持たれて注力されている研究分野についてお聞かせください。

岡本 やはり、量子的なデバイスの研究が急速に進んでいますので、

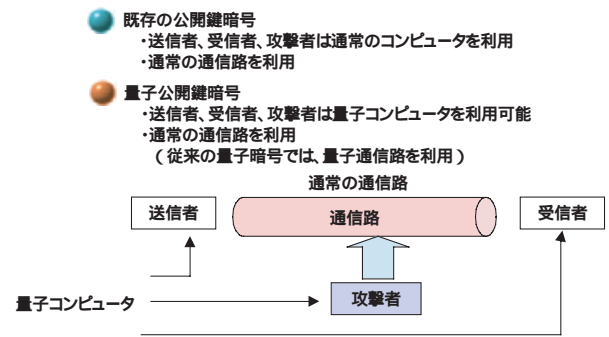


図2 量子公開鍵暗号の概念

量子公開鍵暗号や量子情報を使った量子マネー、量子効果を応用した量子投票などの研究を行っていきたいと思います。

さらに、新しい暗号理論の取組みとして、Universal Composability（汎用的結合可能性）というものがあります。これは、従来の暗号理論を集大成し、リニューアルするもので、21世紀の暗号理論の中核となるものです。これまでの理論では、安全な暗号技術と安全な電子署名技術を組み合わせる際に、相互干渉によって安全ではなくなることがあるのでその点を考慮する必要がありました。しかしUCの理論では、安全な暗号技術と安全な電子署名技術は、どんな組み合わせ方をしても安全であることを保証するというものです。実的にも、UCのコンセプトに基づく安全なモジュールを組み合わせることで、インターネット上でより高いセキュリティを保障するアプリケーションを容易に実現可能になります。

本日は有り難うございました。

（聞き手・構成：編集長 河西義人）