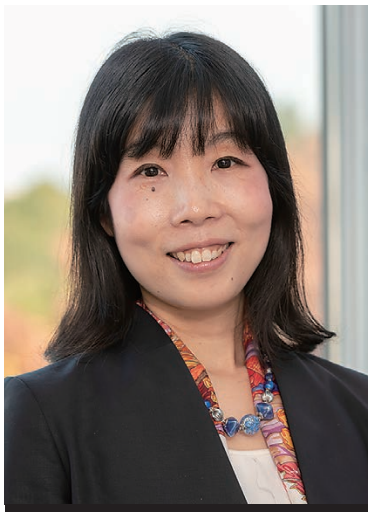
INTERVIEW

安心・安全なデータ利活用を目指して

暗号研究の最前線を探る



盛合 志帆（もりあい しほ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
大学卒業後、日本電信電話（株）、ソニー（株）を経て、2012年から現職。
暗号、情報セキュリティ、プライバシーに関する研究に従事。博士（工学）。

暗号技術は、インターネットが普及した現代社会に欠かせない重要な技術だ。この暗号が今、ある意味「危機」を迎えている。このところ急速に研究が進んでいる量子コンピュータが実現すると、現在広く使われている公開鍵暗号が簡単に破られてしまうためだ。

米国立標準技術研究所（NIST＊1）は、量子コンピュータに耐性のある「耐量子計算機暗号」（PQC＊2）の標準化に向けて準備を進めている。

これからの情報通信技術の激動の時代に、暗号技術はどのように変わり、社会に実装されていくのか。

暗号技術によるICTのセキュリティ基盤の研究をしているサイバーセキュリティ研究所セキュリティ基盤研究室室長の盛合志帆に話を聞いた。

■IoT時代にますます重要となる暗号技術

――暗号の歴史は古いですが、ネット社会になった今、暗号は不可欠な技術になっていると実感しています。暗号技術の変遷など基本的なところを教えてください。

盛合　暗号の歴史は古く、紀元前1世紀の古代ローマ時代にシーザーが使ったシーザー暗号がよく知られています。これは、アルファベットの文字を数文字ずらして伝達する素朴なものでした。暗号が大きく変わったのは、インターネットなどのネットが発達してからです。

ネットによる通信が盛んになるとともに、企業間の商取引に関わる通信、政府の調達や外交情報など、第三者に見られては困る情報がたくさん出てきました。そこで、ネットワークで安全に情報を送るため、暗号技術が急速に発達していきました。

最初は暗号のアルゴリズムを他者に隠すことでメッセージの内容を秘匿していたのですが、それでは不特定多数の人たちの間で利用することができません。そこで、アルゴリズムを公開しても、暗号を解く鍵さえ秘匿していれば安全性が保たれるような暗号が開発され、1977年にNISTの前身であるNBS＊3によって米国政府標準暗号DES＊4として制定され、これが世界標準となっていきました。

この頃から本格的にネットワークが普及し始め、暗号技術の研究が進んでいきました。このあと、DESはAES＊5というものに変わりましたが、どちらも共通鍵暗号です。また、DESが開発された頃、暗号技術に大革命をもたらした公開鍵暗号も登場してきました。

――公開鍵暗号とはどういうものですか。

盛合　暗号は、鍵（数字の列）を使って暗号化と復号を行います。共通鍵暗号は、暗号化も復号も同じ鍵を用います。特定の相手方と通信する場合は処理が早くて便利なのですが、事前に鍵を相手に渡して共有しておかなければなりません。この事前共有のコストが高いことと、第三者に漏れるリスクがあることが課題です。

これに対して、公開鍵暗号は、公開鍵と秘密鍵をペアで生成して、公開鍵を公開しておきます。通信したい人は相手の公開鍵でメッセージを暗号化して情報を送ると、相手方は自分の秘密鍵で復号できます。公開鍵暗号を用いて、共通鍵暗号で使う鍵を事前に共有することができるようになり、安全性が高まりました（次頁図参照）。

公開鍵暗号の代表的なものがRSA＊6暗号で、私たちがインターネットで使っているTLS＊7というセキュア通信プロトコル標準にも使われています。

――インターネットで暗号はどう変わってきたのでしょうか。

盛合　インターネットで様々な情報がやり

＊1 NIST: National Institute of Standards and Technology
＊2 PQC: Post-Quantum Cryptography
＊3 NBS: National Bureau of Standards
＊4 DES: Data Encryption Standard
＊5 AES: Advanced Encryption Standard
＊6 RSA: Rivest, Shamir, Adleman
＊7 TLS: Transport Layer Security

INTERVIEW

安心・安全なデータ利活用を目指して

暗号研究の最前線を探る

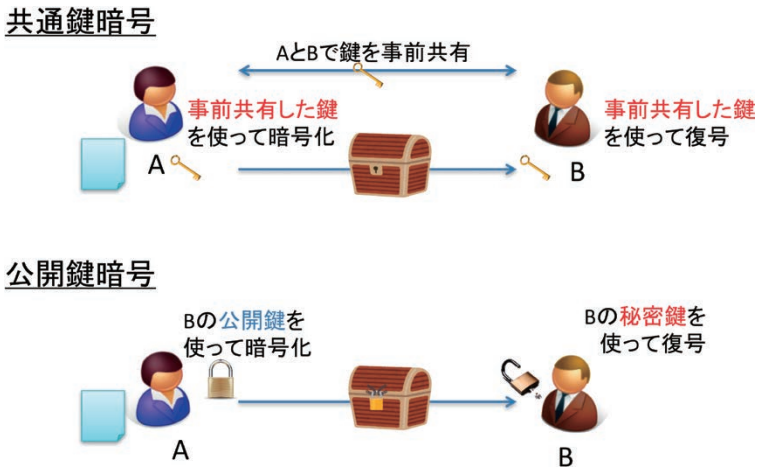


図　暗号技術の基本となる共通鍵暗号と公開鍵暗号

とりされるため、これを守るための暗号化技術も高度化してきています。電子メールでやりとりされるプライバシー情報や、電子マネーやクレジットカード情報などお金に関わる重要な情報もあります。これらの大切な情報を守るために暗号技術は欠かせないものとなっているのです。

今後は、IoTが普及していき、あらゆるものがインターネットにつながります。すなわち、あらゆるものがサイバー攻撃のターゲットになる可能性があるということです。このような中、暗号技術がますます重要になっていきます。

■ 3つの重点研究開発項目

―― NICTの暗号技術に関する取組を説明していただけますか。

盛合　NICTでは5年ごとに中長期計画を立てていまして、今年度は第4期中長期計画（2016～2020年）の3年目となっています。我々の研究室では、この中長期計画の課題として、機能性暗号技術、暗号技術の安全性評価、プライバシー保護技術の3つの研究開発に取り組んでいます。

――では、まず機能性暗号技術について聞かせてください。

盛合　これからはIoTの普及によって新しいニーズが生まれてきます。これにこたえることができるような新しい機能をもつ暗号技術を作ろうというのが本研究の目的です。例えば、IoTデバイスは小型で省電力、メモリサイズも小さいという特徴があり、従来よりも軽量な暗号が必要となります。

また、暗号化したままビッグデータ解析を行う技術も研究しています。ユーザがビッグデータ解析をしたい場合、しばしばデータをクラウドに保存したり、外部の機関に委託したりするケースが出てきます。このとき、個人情報が漏洩しては困ります。そこでデータを暗号化するのですが、暗号化してしまうと普通はそのままでは解析できません。現在、暗号化したままデータを解析できる「準同型暗号」の研究が世界的に進展しています。しかしながら、暗号化されているがゆえに、正しいデータに対して解析を行っているのか分からないという課題がありました。この課題に対して、誤データの混入を検知する機能をもった「まぜるな危険準同型暗号」という技術を提案しました（詳細はP4-5参照）。この技術によって、プライバシーを保護したまま安全にビッグデータ解析が行えるようになりました。昨年、筑波大学と共同で、個人の遺伝子情報と病気の罹患情報との統計的な関連性を、暗号化したまま安全に解析することに成功し、プレスリリース（プライバシーを保護したまま医療データを解析する暗号方式を実証（2018年7月18日） https://www.nict.go.jp/press/2018/07/18-1.html）を行っています。

――2つめの暗号技術の安全性評価についてもお願いします。

盛合　暗号技術の安全性評価に関する研究は、安心・安全なICTシステムの維持・構築に貢献することと、新たな暗号技術の普及・標準化に貢献することを目的としています。その一つの活動が、電子政府推奨暗号等の安全性を評価し、安全なICT社会の実現を目指すCRYPTREC（クリプトレック）*8というプロジェクトの運営です。本プロジェクトは、総務省、経済産業省及び独立行政法人情報処理推進機構と共同運営しています。例えば、量子コンピュータの実現のような大きな技術革新があると、実社会へのインパクトが計り知れません。実現すると、現在のインターネット上でのセキュア通信を支えている公開鍵暗号が破られてしまうため、今から対策を準備しておく必要があります。

――量子コンピュータはいつ頃実現するでしょうか。

盛合　予想は難しいですが、今使われている公開鍵暗号が量子コンピュータによって破られることは数学的に証明されているので、何もしないわけにはいきません。

公開鍵暗号の安全性に直接的なインパクトを与えるとされているのが、量子ゲート方式の量子コンピュータですが、現在使われている強度のRSA暗号を解読できる規模のものが実現するのはまだ先だと思います。一方、量子アニーリング方式のものは商用化が進んでいますが、これは最適化問題を解くのが得意なコンピュータで、RSA暗号の数学的根拠となっている素因数分解を解く手法の検討と評価を富士通研究所や東京大学と共に行っていますが、大きなパラメータの問題を解くのは難しいと考えています。

――3つめのプライバシー保護技術とはどういうものでしょうか。

盛合　パーソナルデータの利活用に貢献するための研究開発を様々な観点から進めており、P8-9で紹介する「プライバシー保護データ解析技術」のほか、匿名加工技術の評価技術についても取り組んでいます。2017年5月に、改正個人情報保護法が施行され、匿名加工情報というものが導入されました。特定の個人を識別することができないように個人情報を加工し、元の個人情報を復元することができないようにした「匿名加工情報」であれば、本人の同意を得ることなく、個人情報を第三者に提供できるというものです。

2019年から個人データを預かって管理する「情報銀行」等の事業が本格化したり、匿名加工医療情報を利活用したいと考えている企業もあります。社会実装に向けて、いかに再識別のリスクを低減して安全性を保ち、データの有用性を保ったまま加工するか。当研究室では、この匿名加工情報の安全性や有用性の評価も行っています。

このような取組は、NICTのみならず、2015年から情報処理学会コンピュータセキュリティシンポジウムにて、PWS CUP匿名加工・再識別コンテストを実施するなど、安全で有用性の高い匿名加工技術の開発を促進するために、業界全体で取り組んでいます。

――中長期計画最終年度である2020年の目標は何でしょうか。

盛合　耐量子計算機暗号の標準化を進めていかなくてはなりません。これまで新しい暗号技術の本格普及までには20年近い時間がかかってきたので、量子コンピュータがいつ完成したとしても間に合うよう、安全性を保つことができる耐量子計算機暗号の安全性評価と標準化が急務です。これを巡っては現在、国内外でいろいろな動きがありますが、特に米国のNISTが進めている標準化の影響は大きいです。

これまで多くの暗号技術について、NISTが主導して国際的デファクトスタンダードを作ってきた経緯があり、この標準化動向を世界各国や関係団体が注視しています。NISTは耐量子計算機暗号標準のドラフトを2022～23年頃を目標に発表することを表明しており、NICTとしても、耐量子計算機暗号の安全性評価や、国内のCRYPTRECにおける各府省の情報システム調達に参照される暗号技術に関する検討に貢献したいと考えています。

■目指す目標

――国立の研究開発機関としての役割は

国立研究開発法人として私たちが心掛けていることは、暗号技術の安全性評価について、公的な立場で中立公正で信頼性の高い情報を継続的に発信していくことです。

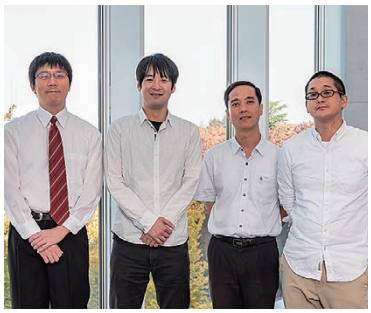
また、セキュリティだけでなく昨今関心の高まっているプライバシーをいかに守るかという課題にも取り組んでいきます。両者とも、今後ますます重要になっていますので、その研究拠点としての役割を果たせるよう尽力したいと考えています。

さらに、社会で実際に活用される研究成果を出し、世の中の役に立つ技術を目指すという気持ちで研究室一同頑張っていきたいと思います。

＊8 CRYPTREC: Cryptography Research and Evaluation Committees

耐量子計算機暗号の開発及び標準化

量子計算機によって暗号が高速に解読されてしまう脅威への対策



左から、青野良範、篠原直行、レ チュウ フォン、林卓也

所属はすべて
サイバーセキュリティ研究所
セキュリティ基盤研究室

篠原 直行（しのはら なおゆき）
主任研究員
2009年NICT入所。公開鍵暗号の安全性評価の研究に従事。博士（数理学）。

青野 良範（あおの よしのり）
主任研究員
2011年NICT入所。暗号の解読アルゴリズムの研究および安全性評価の仕事に従事。博士（理学）。

金森 祥子（かなもり さちこ）
研究技術員
2010年NICT入所。プライバシーに関する研究開発に従事。

黒川 貴司（くろかわ たかし）
研究技術員
2010年NICT入所。暗号技術の安全性評価に関する研究開発に従事。

林 卓也（はやし たくや）
主任研究員
2018年NICT入所。暗号工学、暗号解析、プライバシー保護データマイニングに従事。博士（機能数理学）。

レ チュウ フォン
主任研究員
2015年NICT入所。暗号アルゴリズムの設計、プライバシー保護データマイニングに従事。博士（学術）。

暗号技術は安全な通信や情報の保護のために欠かせない技術であり、携帯電話、電子パスポート、無線LAN、ネットショッピングやネットバンキングなど、身近なところで広く使用されています。近年、量子計算機の開発が進み、そのことによって現在利用されているいくつかの暗号技術の安全性が近い将来に大きく低下することが懸念されています。その対策として、量子計算機を用いた解読に対しても安全性を保つことが期待される暗号技術（耐量子計算機暗号：Post-quantum cryptography（PQC））の開発及び標準化が世界的に活発に進められています。本稿ではセキュリティ基盤研究室の成果を紹介します。

■耐量子計算機暗号が必要とされる理由

量子計算機による解読が懸念される暗号としてRSA暗号と楕円曲線暗号が挙げられます。これらは広く使用されている代表的な公開鍵暗号です。また、その懸念の理由は、これらの暗号で利用される数学的な構造及びShorのアルゴリズムと呼ばれる量子計算アルゴリズムに関係があります。

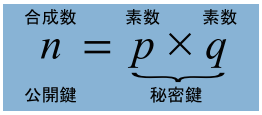
RSA暗号では、図1のように2つの素数が秘密鍵と呼ばれる秘匿すべき情報として利用され、それらの素数の積が公開鍵と呼ばれる誰でも取得可能な公開情報として利用されます。したがって、公開鍵である合成数を素因数分解することができれば秘密鍵を取得されてしまいます。そこで、現在使用されているRSA暗号では、現時点で素因数分解を最も効率よく計算するアルゴリズムである数体ふるい法を用いて、世界最速のスーパーコンピュータで十分な時間（1年など）計算しても解読できないように、公開鍵の大きさ（鍵長）を2048 bit（617桁）に設定しています。もし、数体ふるい法より計算効率が良いアルゴリズムが発見されても、またスーパーコンピュータの性能が向上しても、鍵長を十分大きくすることでRSA暗号の安全性を保つことができます。しかし、鍵長を大きくしすぎると、暗号処理にかかる時間も膨大になり、実用的ではなくなってしまいます。Shorのアルゴリズムは量子計算機を用いて整数の素因数分解を計算するアルゴリズムであり、数体ふるい法よりずっと計算効率が良いことが知られています。したがって、十分大きな素数の積に対してShorのアルゴリズムを適用できる大規模な量子計算機が開発されると、RSA暗号の実用性が大きく低下してしまいます。

同様のことが楕円曲線暗号についても生じることが知られています。楕円曲線暗号は楕円曲線上の離散対数問題を解く計算の困難性をその安全性の根拠としています。Shorのアルゴリズムは離散対数問題を解く計算にも適用でき、整数の素因数分解の場合と同様に、この場合の計算効率も良いことが知られています。

■耐量子計算機暗号の開発

素因数分解や離散対数問題とは異なる、量子計算機でも効率良く解くことができないと考えられている問題を安全性の根拠とした暗号は、耐量子計算機暗号と呼ばれています。現在、この暗号の研究開発及び標

整数を素数の積の形で表す
$23449 = 131 \times 179$
RSAにおける公開鍵と秘密鍵の関係



巨大な合成数の素因数分解は難しい ⇒ 素因数分解問題

図1　RSA暗号の安全性と素因数分解

準化が世界的に進められています。代表的な耐量子計算機暗号の一つとして、格子問題（図2）を利用した格子暗号が挙げられ、セキュリティ基盤研究室では新たな暗号方式であるLOTUS（ロータス）を開発しました。

近年の量子計算機の進化に伴い、米国NIST（国立標準技術研究所）は2016年に耐量子計算機暗号の標準化プロジェクトを開始し、2017年には方式の公募が行われました。NICTもそれに合わせて開発した格子暗号方式LOTUSを提案し、書類審査を通過した69件の中に含まれました（図3）。公募に提案された方式はNISTのWebページに全て掲載され、それに関する議論も専用のメーリングリストで公開されています。2018年12月までに、軽微なものも含めると約30件の方式に対して安全性の欠陥が指摘され、そのうち5件が既に取り下げられています。今のところLOTUSに対する重大な欠陥は発見されていません。しかし、NISTは提案されたPQCの候補を絞り込んだ結果を2019年1月30日に発表し、LOTUSはその候補として残りませんでした。LWE問題（図2）に基づく他の候補に比べてLOTUSの公開鍵のサイズは大きく、暗号文のサイズは小さいという特徴があります。この特徴は、公開鍵を頻繁に更新しない場合に適しています。

暗号方式の提案とは別に、実際に暗号を使うときにどの程度のパラメータを設定したらよいかという問題を議論するため、企業・大学及び公的機関が様々な暗号の安全性に関わる問題を公開し、問題のサイズと解読時間が評価されてきました。LOTUSの安全性の根拠となる格子問題では、ドイツのダルムシュタット工科大学が主催するLattice Challengeが有名であり、世界中の研究者が実験報告を行っています。セキュリティ基盤研究室では、このコンテストにおいて何度も世界記録を更新しており、格子暗号の安全性評価に長年貢献しています。

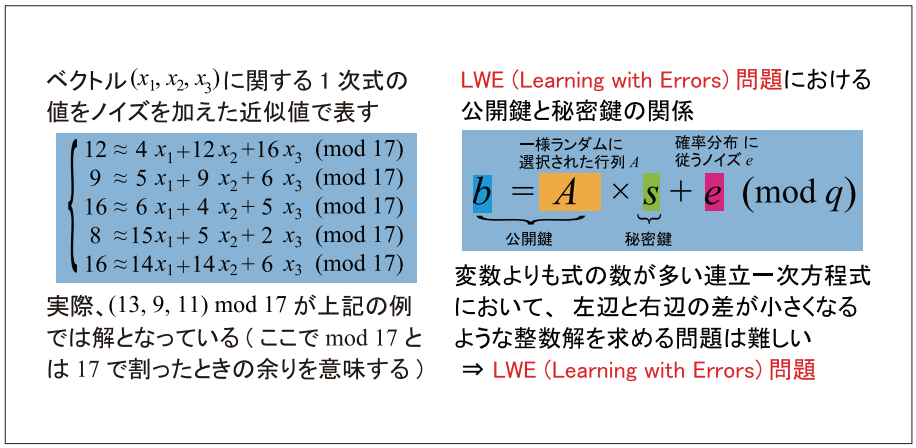


図2　格子問題の例（LWE 問題）

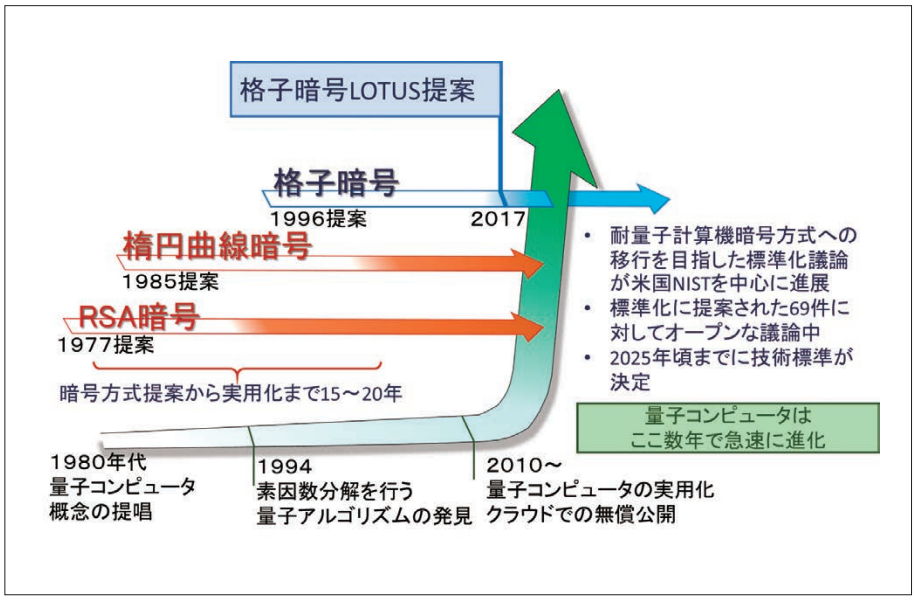


図3　格子暗号 LOTUS の開発

■日本国内における耐量子計算機暗号の標準化の準備

NICTは電子政府で使用する暗号技術の安全性評価等を行うプロジェクトであるCRYPTREC（クリプトレック）を総務省、経済産業省及び独立行政法人情報処理推進機構（IPA）と共同で運営しており、NICTではセキュリティ基盤研究室が実務を担当しています。このプロジェクトにおいて耐量子計算機暗号の有力な候補である格子暗号に関する調査を2014年に実施しています。さらに、他の有力な候補（符号暗号、多変数暗号、同種写像暗号等）についても2017年から調査を開始し、その技術報告書を2019年に公開する予定です。

■今後の展望

近年、NISTによる耐量子計算機暗号の公募等の実施により、多くの耐量子計算機暗号が提案されており、今後はそれらを含む新たな耐量子計算機暗号の安全性評価の研究が活発に進められることが予想されます。セキュリティ基盤研究室は研究開発及びCRYPTRECでの活動によって、格子暗号だけではなく他の耐量子計算機暗号の安全性評価及び開発にも貢献していきます。