URL https://journal.ntt.co.jp/article/38465
DOI https://doi.org/10.60249/26031301

NTT社会情報研究所
特別研究員
西巻　陵 Ryo Nishimaki

未来の安心・安全な情報通信を実現する「耐量子暗号」と「消去証明」技術

量子コンピュータの実用化は，現在使用されている暗号の多くが解読されてしまうという危険性がある半面，量子コンピュータの能力を用いることで初めて可能になる暗号技術の実現という恩恵ももたらします．今回，量子コンピュータ時代の情報セキュリティシステムにおいて中核となり得る「暗号技術」のトップランナー，西巻陵特別研究員にお話を伺いました．

◆PROFILE：2007年京都大学 情報学研究科 社会情報学専攻 修士課程修了．同年，日本電信電話株式会社入社．暗号理論の研究に従事．2010年東京工業大学（現　東京科学大学）大学院 情報理工学研究科 数理・計算科学専攻 博士後期課程修了 博士（理学）取得．東京科学大学特定教授．2008年電子情報通信学会SCIS論文賞．2013年電子情報通信学会SCISイノベーション論文賞．2023年The ACM Conference on Computer and Communication Security トップレビューアー賞受賞．

クラウド上の個人情報を保護する最新暗号技術とは

■まず「暗号技術」の要となる「暗号化鍵と復号鍵」について教えてください．

「暗号化鍵」と「復号鍵」というのは，それぞれデジタルデータの暗号化と復号に用いられるデータのことで，情報セキュリティにおいて重要な役割を果たします．物理的な鍵のようにデータを暗号化して施錠し，正しい鍵を持つ人だけが復号できるようにするため，データの保護や機密性を保つために使用されます．オンライン・ショッピングやネットバンキングで口座番号やパスワードなどの個人情報を取り扱う際，第三者による悪用を防ぐためのものです．ところが現在，量子技術の発展が著しく2030年には実用的な量子コンピュータが実現するといわれています．この量子コンピュータが登場すると，情報処理能力は飛躍的に上昇し，従来使用されてきた「RSA（Rivest-Shamir-Adleman）」や「楕円曲線」などと呼ばれる暗号は，容易に解読されてしまうことが判明しています．そのため，こうした量子技術による情報処理能力の向上に対応可能な新しい暗号技術の研究・開発が，私の研究グループを含めて世界各国で盛んに行われています（**図1**）．

ところで，現在の暗号技術でできることについても，1例を挙げておきましょう．現在は従来の「1対1」の通信ではなく，クラウド環境でみられるような「1対多」，あるいは「多対多」の通信が頻繁に行われるようになっています．複数人で行われるオ

量子コンピュータの実用化とともに急上昇する量子時代の危険性（イメージ）

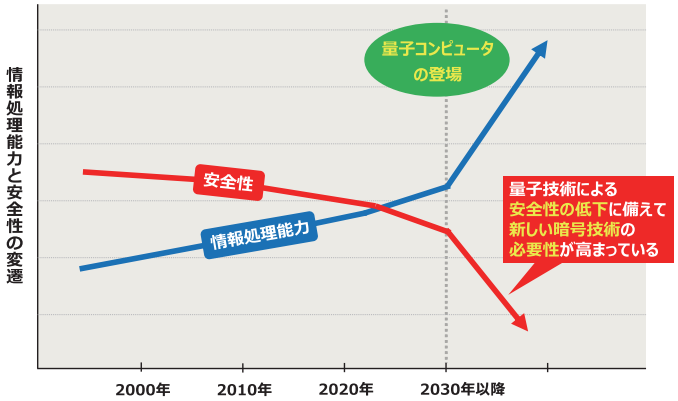

図1　コンピュータの情報処理能力と安全性

ンライン会議などがその例といえますが，こうした「1対多」「多対多」の通信の際，各参加者に渡す情報を同じものにできない場合があり，「1対1」の通信に対応した通常の暗号では不十分なケースが起こり得ます．例えば，ある企業内で重役から一般社員まで，立場や役職の異なる参加者による“企業秘密を含む”重要な社内会議がオンラインで行われたとします．すべての参加者に“暗号化された同じ会議用資料データ”を配布し，役職に応じて異なる復号鍵を渡すことで，情報開示を細かく制御できます．具体的には，部長以上の管理職にはすべて内容を復号できる鍵を，それ以外の社員には機密情報が復号されない制限付きの鍵を付与することで，秘匿したい情報を隠すことが可能になります（**図2**）．

このように各参加者が持つ復号鍵に応じて，1つのデータから得られる情報を細かく制御できるものを「関数型暗号」といい，「1対多」「多対多」の通信に適した暗号になります．

また，現在コンピュータやスマートフォンなどを活用する際のほとんどは，写真などを含めた個人情報をクラウドに保存されていると思います．こうしたクラウド内に保存された情報やデータについて，セキュリティ対策の必要性が現在非常に高まっています．

■クラウド内でのデータセキュリティについて教えてください．

サブスクリプションのアプリケーションなどを申し込むと，IDやパスワードなどの長い文字列を支給され，その文字列を入力し認証することでサービスの使用を許可されますが，すでにクラウド（外部ストレージ）を使用していれば，こうした煩雑な情報はクラウド内に保存して自動入力のかたちで使用していることがほとんどだと思います．しかし，こうした外部ストレージ上に保存されたデータが悪用される危険性は常に存在します．具体的には，ネットショッピングで使用するためにクラウドに保存していたクレジットカード番号をハッキングされるなどといった危険性は否定できません．契約期間が切れて削除したと思っていても，どこかにコピーが残っている可能性は排除できないのが現実です．

従来の古典コンピュータでは，データや情報を完全に消去することは不可能です．前述のクラウド内に保存していた“消去済みデータ”であっても，企業サイドは定期的に全データのバックアップを保存していますから，何かシステム全体に問題が起きて，予告なしにバックアップデータ（消去以前のデータ）と置き換えられた場合に，消去したはずのデータが復活してしまうなどということも可能性としてはゼロではありません．現在の古典コンピュータでのデジタル情報は，コピーをいくらでもつくることが可能ですから，どこにもコピーが残っていないことを証明することは，俗にいう「悪魔の証明」となります．

しかし，量子情報技術を利用すると，この状況は一変します．あくまで量子コンピュータの存在が前提となりますが，量子状態の暗号文や秘密鍵（復号鍵）を生成することで，量子の特性を利用した完全な「消去証明」の可能な復号鍵や暗号文が実現できるようになります（**図3**）．

量子コンピュータの実用化が徐々に近づいてきている現在，量子コンピュータの能力を活用することで初めて実現できる暗号技術が今後は非常に重要になってくると考えられます．

■量子情報技術を使用した「消去証明」について教えてください．

基本的に現在利用されている暗号というのは，計算能力がものすごく高ければ破れてしまうものです．現在の暗号技術は，計算をすることが非常に難解でその計算に膨大な時間がかかる，という理由で成立している技術になります．ところが，元の暗号文を「完全に消去」できれば，将来無限大の計算能力を持つコンピュータができたとしても，その暗号文の内容は，消去した後では全く分からないようになります．

私は情報の「消去証明」や「情報の安全な貸し出し」というアプローチで，量子コンピュータ時代の暗号技術を研究していますが，古典コンピュータを用いている限り，情報を消去したことを証明することや情報（復号鍵など）を返却したことを証明する手段は前述のとおり存在しません．しかし，量子物理の不確定性原理を応用した技術では，ある情報量を観測すると，対となる別の情報量を同時に十分な精度では観測できなくなるという特性を利用することができます．この特性を応用して，量子状態の暗号文

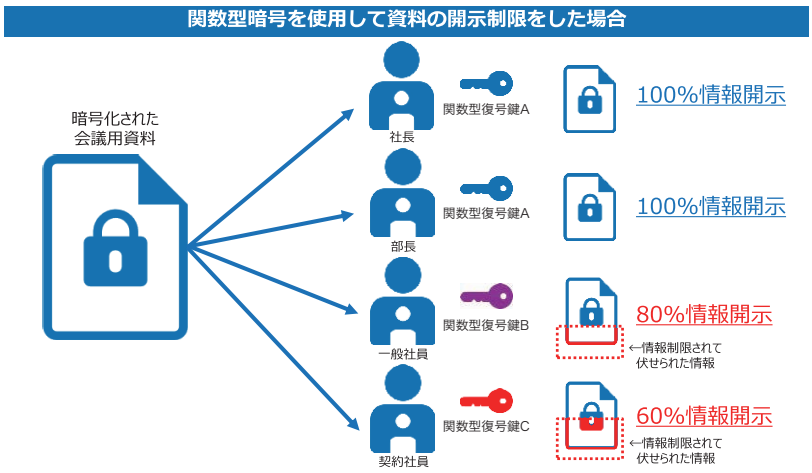

図2　関数型暗号の使用例

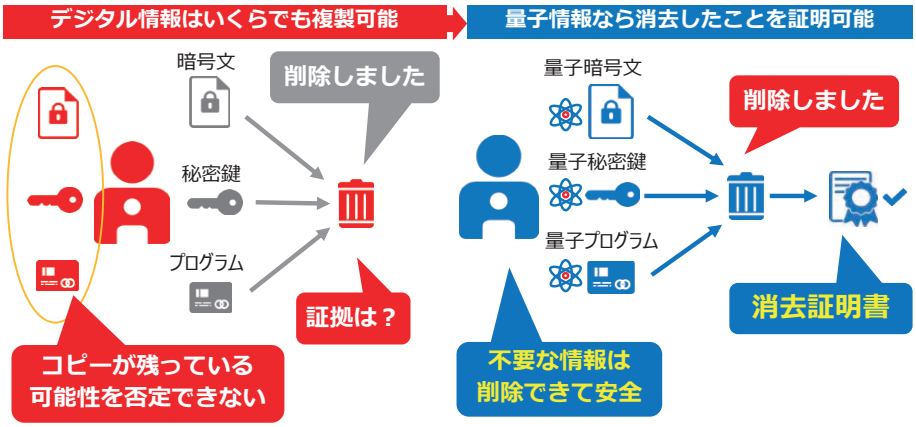

図 3 量子情報技術＋暗号技術で可能となる消去証明

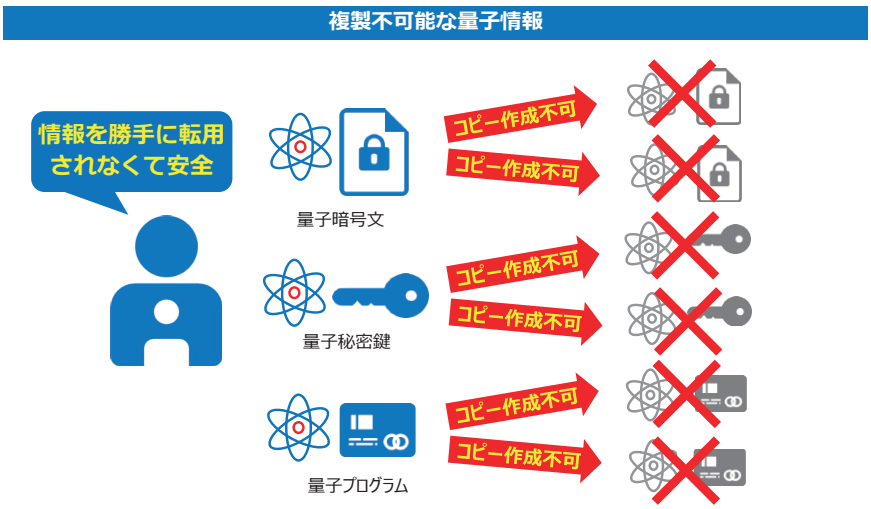

図 4　量子物理の特性でコピー不可能

を生成した後にその暗号文を消去すると，そのデータが確実に消去されたことを証明する「消去の証明書」を得ることが可能になります．この証明書が正しいことを確認できた場合は，元のメッセージに関する情報を一切得られないことが保証できます．また，量子状態の復号鍵を生成することでユーザに貸し出し，ユーザは返却するときに消去した証明書を送り，確かに返却したことを証明可能にもなります．このような量子コンピュータの存在を前提として，初めて実現できる暗号機能という観点から研究を進めています（**図 4**）．

■研究で苦労された点や今後のご研究に向けた課題点を教えてください．

昨今，暗号技術の分野では，さまざまな研究論文が急速に増えて発表されています．私自身，STOC（Symposium on Theory of Computing: 理論計算機科学の国際会議）やCRYPTO（クリプト），EUROCRYPT（ユーロクリプト）などの暗号理論のトップ会議で多数の研究論文を発表しています．具体的にはCRYPTOでは「公開鍵暗号」などを 8 件，EUROCRYPTでは「量子暗号」をはじめ 9 件，STOCでも「プログラム電子透かし」を含む 2 件，Journal of Cryptology（暗号理論のトップジャーナル）では「プログラム難読化」など 8 件（その他，多数の特許も含む）という数多くの論文が採録されていますが，当初はこうした最先端の研究スピードにどうついていくか，最先端の研究の進め方のサイクルを身につけるまで少し戸惑いました．また，以前は研究が思うように進まないときなど，気持ちを切り替えるのに時間が必要でした．しかし今では，学生時代から続けている水泳などで体を動かし，気持ちを切り替える方法を見つけることで，この課題を克服しています．

技術的な問題としては，私の研究はあくまで理論研究であり，2030年に実用化されるといわれている量子コンピュータに対応した耐量子暗号なども，まだ実証実験できる実機が存在しない状況です．私の「消去証明」も理論的に可能であることは分かっていますが，実証実験が可能になった段階でより完璧な方式にするために，どのように修正し実用化していくかということが今後の課題になります．

情報にかかわるすべての業界のイノベーションに貢献するために

■この研究によって実現されることや将来の応用先を教えてください．

具体的にはまず，動画配信サービスや音楽配信，ソフトウェア配信のほか公共サービスなどといった，各種のサブスクリプション・サービスで利用が見込めると考えています．現在，各社で運用しているサブスクリプション・サービスのほとんどは，システムでユーザの利用を制御しています．そこで例えば，有料動画自体を暗号化してユーザサイドに秘密鍵（復号鍵）を渡すことで視聴を可能にするかたちにすれば，違法ダウンロードや違法のデータ頒布が減少し，より健全なユーザ視聴が可能になりますし，契約期間が切れた場合でも，秘密鍵の返却や消去証明によって配信側の利益も保証される可能性が高まります．また消去の証明を応用してプログラム（アプリ）を安全に貸与することも可能になり得ます．例えばアプリをお試しで利用してもらい，お試し期間後に返却してもらえればユーザの手元にアプリの情報は残らず，アプリの海賊版が流通する可能性が減り，アプリ提供元の利益を保護しつつアプリの柔軟な提供が可能になり得ます．これが実現すれば，著作権保護はもとより，世界中のあらゆるコンテンツ業界への貢献につながる可能性があります．

また，NTTの提案している「IOWN（Innovative Optical and Wireless Network）」構想によって，拡大の一途をたどる通信の世界はもちろん，ソフトウェアの開発やアプリケーションやゲーム開発の分野など，「暗号技術」は情報のやり取りをする環境ではどこであっても必要とされる技術です．暗号技術はネットワーク環境の発展に応じて，これからもかたちを変えて進歩していくはずです．私はこれからも進歩していくこのネットワーク環境に対応した，新しいインパクトのある暗号技術を研究・開発し続けていきたいと考えています．

■研究に対する想いや大事にされていることを教えてください．

私は大学時代からNTT入社後も，すでに20年近く暗号理論について研究を続けてきました．私が研究テーマを選ぶ観点は2つあります．1つは基本的に自分がワクワクする内容であること．「これは絶対面白い」と心で感じるのが一番です．そしてもう1つが将来「役に立つ」と自分で信じることができる技術であることです．そして，もし選択肢があって迷うようなら，より困難なこと，難しいほうに挑戦することです．この考え方は私の研究グループの中でも共有し，実践しています．

■所属されているNTT社会情報研究所について，どのような研究所かをご自身の印象を交えてお願いします．

NTT社会情報研究所を端的に表現すると，主にセキュリティ全般に関しての研究をしている研究所になります．研究内容は多岐にわたるもので，非常に多様な観点からセキュリティに取り組んでいます．ネットワークセキュリティやOSセキュリティといったシステム的なセキュリティの研究者はもちろん，中には人間の「安心」や「安心感」という観点からセキュリティを扱うような研究を行っている部署もありますし，法律的な観点から声優や俳優などの「声」の権利に関するセキュリティを扱う部署もあります．そのため，各研究員たちの専門分野も，通信はもとより，法律学，心理学などと多彩なバックグランドを持った研究者たちの集まりです．

実際の勤務や就業環境については，非常に柔軟な働き方ができる環境の研究所です．基本的に勤務はリモート業務が主体ですが，私の研究グループでは週1回，全員で出社して会議や打ち合わせなどをしています．私は研究関連の「雑談」をすることも大事だと考えているので，この週1回の出勤は，皆で顔を合わせてあえて行う雑談時間ともなっています．実際にこの雑談の中から，新しい発想や研究テーマが見つかったり，抱えている問題の解決の糸口が掴めたりしているので，大変実効性のある試みです．

■読者の方や研究者・学生・ビジネスパートナーへのメッセージをお願いいたします．

NTTの暗号研究は，世界的にトップクラスです．そのため，毎年のように海外から私の研究グループへのインターン希望がありますし，実際に一定期間滞在する海外の学生も多くいます．また，海外の第一線で活躍する研究者が，ゲストとして来訪することも珍しくはありません．そうしたゲストの方々には，必ず参加自由の講義をしていただいています．私自身も東京科学大学（旧東京工業大学）で特定教授をしていて，年に数回，学生たちに講義させていただくこともあり，そのときに知り合った学生たちやさまざまな大学の研究室に声がけして，この海外研究者が開いてくれる講義に招いたりもしています．実は現在，私の研究グループに所属している研究者は，私がこのようにして知り合った人たちがほとんどです．こうして海外の著名な研究者たちと直接コミュニケーションを取ることで，視野を広げて，世界的にインパクトのある研究がしたいと思う学生や研究者の方は，ぜひNTTにいらしてください．前述の海外研究者による講義は，どのような方でも参加自由ですので，そのきっかけになっていただけたら嬉しく思います．最後に，ご協力いただいているビジネスパートナーの方たちとは，今後も良い関係で研究を進めていければ幸甚です．これからもよろしくお願いいたします．

（今回はリモートにてインタビューを実施しました）