URL https://journal.ntt.co.jp/article/35343
DOI https://doi.org/10.60249/25081301

NTT社会情報研究所
特別研究員
北川冬航 Fuyuki Kitagawa

# 加速度的に増大するデジタル危機を解決する，次世代の安全な「公開鍵暗号技術」

近年，インターネット界隈で横行するサイバー攻撃を防ぐためにはデータや通信内容の「暗号化」が必須です．また，2030年代には量子計算機（量子コンピュータ）が実用化される見込みです．この量子計算機は，特定のタスクにおいて従来のコンピュータの１億倍の性能ともいわれます．この量子計算機が普及すると，社会のデジタル化はさらに進展し，それを支えるセキュリティ技術の必要性も一段と高まります．今回は，量子技術を利用した次世代の「公開鍵暗号技術」研究のトップランナー，北川冬航特別研究員にお話を伺いました．

◆PROFILE：2019年東京工業大学情報理工学院にて暗号理論の博士課程（理学）修了．同年，日本電信電話株式会社に入社．2024年NTT社会情報研究所特別研究員．近年は，暗号理論と量子情報の融合領域の研究に従事．2015年電子情報通信学会SCIS論文賞，2020年東京工業大学手島精一記念研究賞（博士論文賞），2025年電子情報通信学会SCISイノベーション論文賞．

## 新たな量子計算機時代のデジタル環境に際し，安心・安全のために必要不可欠な技術

**■はじめに「安全な公開鍵暗号技術」とはどのような研究でしょうか．**

加速度的に進む現代のデジタル社会では，デジタル化したものやサービスはもはや欠かすことのできない存在です．5G（第５世代移動通信システム），6G（第６世代移動通信システム）など通信環境の高速化に伴う半導体技術の高性能化や，近い将来，想定される量子計算機の登場などによって，さらなる計算機能力の大幅な向上が高い確率で予測されており，社会のデジタル化はより急速に進展していくと考えられます．

例えば，鉄道事業の決済やインターネット間の取引などに代表される電子マネーの登場は，日常生活の利便性を大きく向上させましたが，こうした電子通貨，電子取引はデジタルならではの不正利用や犯罪をも多く生み出しました．社会のデジタル化は，さまざまな面において利便性を飛躍的に向上させる一方で，これまでの社会には存在しなかった危険性も生み出します．これらの危険性をよく知るユーザほどデジタルを利用したサービスの利便性は認識しつつも，利用をためらう傾向もあるようです．デジタル技術はまだまだ課題のある技術であり，誰もがより安心・安全に利用可能に発展させていくために必要となるのがセキュリティです．そしてその情報を守るための代表的な方法の１つが「公開鍵暗号技術」です．

この公開鍵暗号技術の研究は，量子計算機が実用化されるといわれる2030年代を目前に，今まさに変革期にあります．その理由の１つは，量子計算機が実現すると，従来の暗号方式では安全性が確保できない状況が生まれてしまうことです．特に世の中で広く使われている「RSA暗号」や「楕円曲線暗号」と呼ばれる従来の公開鍵暗号方式は，量子計算機を用いると簡単に解読されてしまうことがすでに分かっています．「RSA暗号」や「楕円曲線暗号」は私たちのメールのやり取りから金融機関などで，幅広く普及しているため，この事実は衝撃的ともいえます．そのため，量子計算機の研究開発が加速し，突如実現したとしても混乱が生じぬよう，これら既存の公開鍵暗号に代わる量子計算機でも解読できない公開鍵暗号技術の研究開発が，現在非常に盛んに行われています．この研究は「耐量子暗号」などと呼ばれます．

また量子計算機の実現が迫ってきたことで，量子計算機ならではの性質を活用した新たな暗号技術を開発する試みも盛んに行われています．安全と考えられてきた既存の「RSA暗号」などをも解読してしまう量子計算機の驚異的な能力を使って，逆にこれまでは実現できなかったようなセキュリティ技術を生み出そうというのが私の研究です．この研究は「量子暗号」などと呼ばれます．

私の研究の最終目標は，その専門である暗号理論と量子情報の研究でこの先の将来，量子計算機時代になっても安心・安全を確保して，誰もがデジタル社会の恩恵を享受できるように「新しい暗号方式」，特にこの「量子暗号」を実現することです（**図１**）．

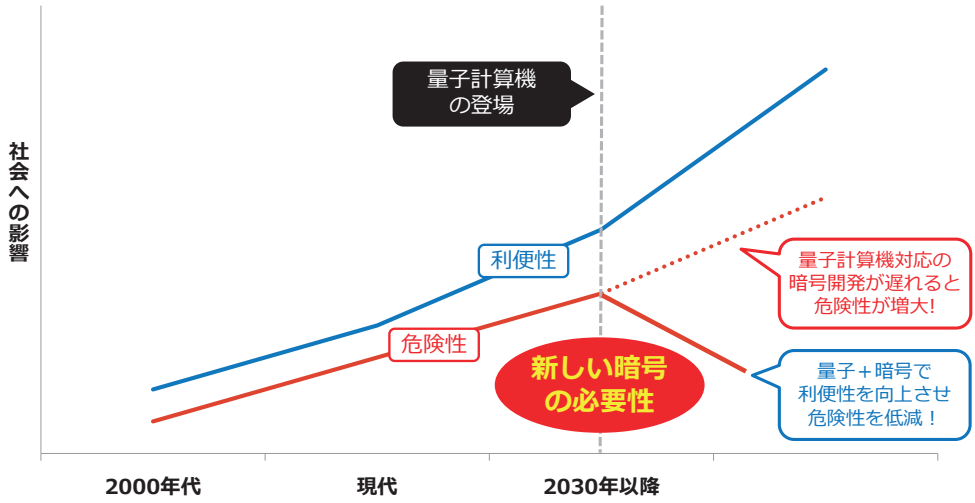



図1　デジタル化の進行に伴う社会的影響の推移イメージ

**■具体的にどのような技術研究に取り組まれていますか.**

将来の安心・安全なデジタル社会に向けて，暗号理論と量子情報を融合することにより，量子計算機が実用化された後も「複製できない電子情報」の実現をめざしています.

現在の情報処理ではすべての電子情報は0と1の組み合わせであるビット列に過ぎず，理論的にすべての電子情報は簡単に「複製」が可能です．私たちは自身のPC上でファイルをコピーしたり，SNSで友だちと写真の共有などを日常的に行っています．このような電子情報の複製が可能な点は大変便利だといえますが，一方でこれが電子情報の危険な点でもあります．デジタルにおける利便性と危険性は表裏一体です．すべての電子情報は一度悪意のあるユーザの手に渡ると，無制限に複製され瞬く間に拡散されてしまう脅威が生じます．産業スパイによる重要な企業秘密の漏洩や特許技術の盗難といった事案もありますし，身近なところでいえば，書籍や音楽の違法ダウンロードといった事例なども頻発しています．また現状では，他者の電子情報の複製をオリジナルの所有者に知らせるという機能も存在しないので，所有者は自身の電子情報が複製され悪用されていることには，情報やデータが拡散されてしまってからしか気付くことができないのです.

しかし，量子情報を使用した処理であれば，この既存の情報処理における問題点を解消した「複製できない電子情報」が実現できます．無断複製や悪用といった事例をも情報解析することができるようになります．この方法では電子情報は，1つひとつの量子ビットがどのような状態にあるのかを表す「量子状態（いわゆるqubit）」を用いてエンコードされます．量子状態はその特性から複製不可能性という性質を持っています．そのため任意の量子状態を完全に複製する技術は存在しません．非常に膨大な数の状態にある量子情報処理へ暗号理論を組み合わせることにより，完全な複製だけでなく断片的な複製すらもできない，暗号理論の観点から見て安全な「複製できない電子情報」が実現できるようになります（**図2**）.

私はこの「複製できない電子情報」の結実に向けて，量子情報処理に暗号理論を組み合わせる研究に取り組んでいます．そしてまた現在，その応用として「複製できない電子通貨（クオンタムマネー）」の研究を注力して進めています（**図3**）．これまでに，この「電子通貨」に関する新方式や関連技術を提案し，その成果は暗号理論および量子情報の主要国際会議において発表し，評価されています.

**■研究で苦労された点や今後の研究に向けた課題点を教えてください.**

課題としてあげるとすれば，量子計算機の実機がまだ存在しないために，私たちの設計している方式や技術を実証することができないという点です．今は理想的な量子計算機が実現されると仮定して方式の設計を行っており，ハードウェアの実現に先んじてアルゴリズムを完成させることを目標に研究しています．この方針においてはかなりの進展を得ていますが，次の段階として量子計算機のハードウェアの開発状況もみながら，実際に実現される環境において実行可能な方式へと改善・改良していく必要があります．また，先行して理論が完成していることでハードウェアの開発にも指針や好影響を与えることができるはずです.

私の研究分野は暗号理論と量子情報の境界領域であり，量子暗号分野などと呼ばれます．この研究は，量子計算機の実現が現実に迫ってきたことで急速に進展しています．近年，非常に多くの

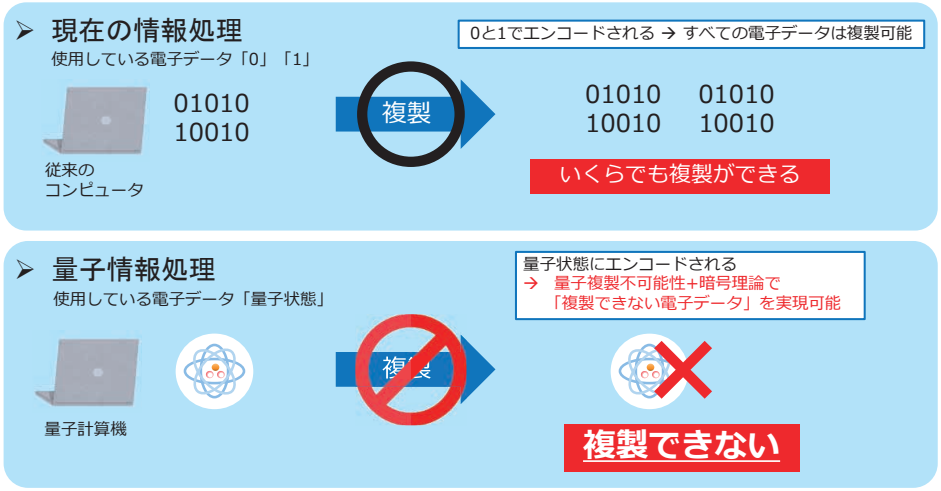



図 2　量子状態の電子データが実現する複製不可能性

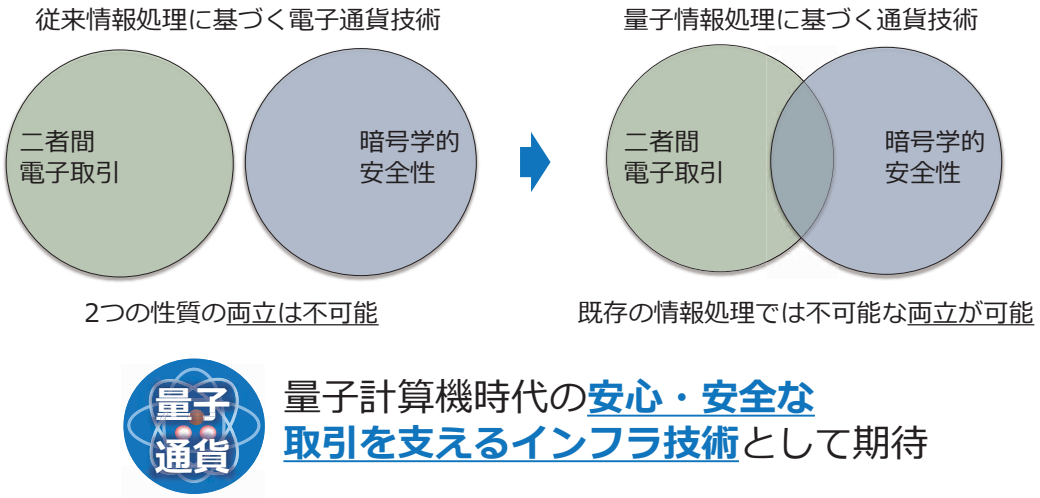



図 3　現在の電子通貨と量子通貨との比較

結果が生まれ，続々と発表されており，その速度はめまぐるしいほどの速さです．私たちのグループでは，これまでに得た成果が他グループと競合することが何度もありました．例えば，暗号理論のトップ会議であるCRYPTOという国際会議に投稿された論文が，2024年は500件程度だったものに対し2025年は650件でした．これは暗号理論のすべての会議の投稿総数ではありませんし，またこの投稿数の増加が量子暗号の進展だけが理由というわけにはいきませんが，この一例をとってもこの分野の研究が急速に進展していることだけは明白です．下手をすると，自分たちが取り組んでいることを矢継ぎ早に他のグループが先に発表してしまうのではという，私たちの懸念も分かっていただけるのではないかと思います．研究を計画的にかつ迅速に進めなければ，この分野で主導権を取って研究していくことは難しいため，その点は気を使わなければならない部分だといえます．

## 安全性の確保された量子通貨で，売買の常識が変化する「完全二者間取引」へ

**■今後の研究の展望を教えてください．**

私の現在の目標は，量子技術を利用して「完全二者間取引」を可能にすることです．私が現在研究している「複製できない電子通貨」は，研究業界では「量子通貨」と呼ばれていて，この技術

は電子通貨の概念を変える革新的技術として期待されています．この「量子通貨」の最大の特徴は，従来の情報処理では実現し得なかった二者間電子取引を非常に高い安全性の下で達成できることです．

従来の暗号理論に基づく電子通貨技術では，安全な方式を設計するためには「第三者による取引の監視」が不可欠でした．暗号学的に安全性を担保しようと思うと，銀行などの決裁権者を間に挟み，この決裁権者に取引内容を伝えて，口座の預金を移動してもらうというのが現状では唯一の方法です．しかしこの方法では，あらゆる取引履歴が第三者（決裁権者）に収集されてしまう可能性があります．この事実に対するユーザの抵抗や恐怖は大きく，こうした点が電子通貨技術の普及に対する障壁になり得ています．

これに対して前述のとおり，「複製できない」量子通貨は暗号学的に安全な完全二者間取引を実現します．量子通貨では，量子状態に価値を付与し，ユーザ間で現金のようにその量子状態を送受信してもらい決済を行います．取引に決裁権者を介する必要はありません．このような暗号学的に安全な完全二者間電子取引は，電子情報が複製不可能な量子情報処理だからこそ実現可能なのであり，従来の情報処理では実現することはできません．量子通貨を使用すれば，あたかも実際の店舗において対面で売買するように，通貨を渡して商品を受け取るという行為が，世界中のどこでもネット上で安全に行えるようになるのです（**図4**）．もちろん，この技術の社会展開には，法律的政治的な対応は別途必要です．

また，今回は「複製できない電子通貨」を例に話をしましたが，同じように量子技術を用いた「複製できないソフトウェア」や「複製できない暗号鍵」という研究も別の応用例として同時に研究しています．こうした量子技術は，その有効活用によって新しい応用や研究に結びつけることができるので，その可能性は無限大だと考えています．

**■現在取り組まれている研究とNTT事業とのかかわりについて教えてください．**

デジタルトランスフォーメーションはNTTの事業において重要な柱の1つです．デジタル社会の拡大を支える堅牢なプラットフォームの構築はNTTにとって重要な課題ともいえます．量子通貨は「ユーザの理想（完全二者間取引）」と「高い安全性（暗号学的に厳密な安全性保証）」を両立する量子計算機時代のデジタルインフラとして非常に訴求力の高い技術です．私の研究している安全な量子通貨を実現し，盤石なデジタルプラットフォーム構築に貢献したいと考えています．

また，量子計算や量子暗号は量子計算機の実現が迫る今，世界が注目している研究領域です．私の研究は量子計算機自体の開発ではなく，それによって起こることが想定される利便性や危険性に対応するためのものですが，これらの研究領域において革新的な研究成果を創出することは，NTTの技術力の高さを世界にアピールするうえで大変効果的であり，グローバル事業の競争力強化の観点からも重要だと考え，日々取り組んでいます．

**■NTTへ入社されたきっかけについて教えてください．**

私は2019年に研究者としてNTTに入社しました．入社したい

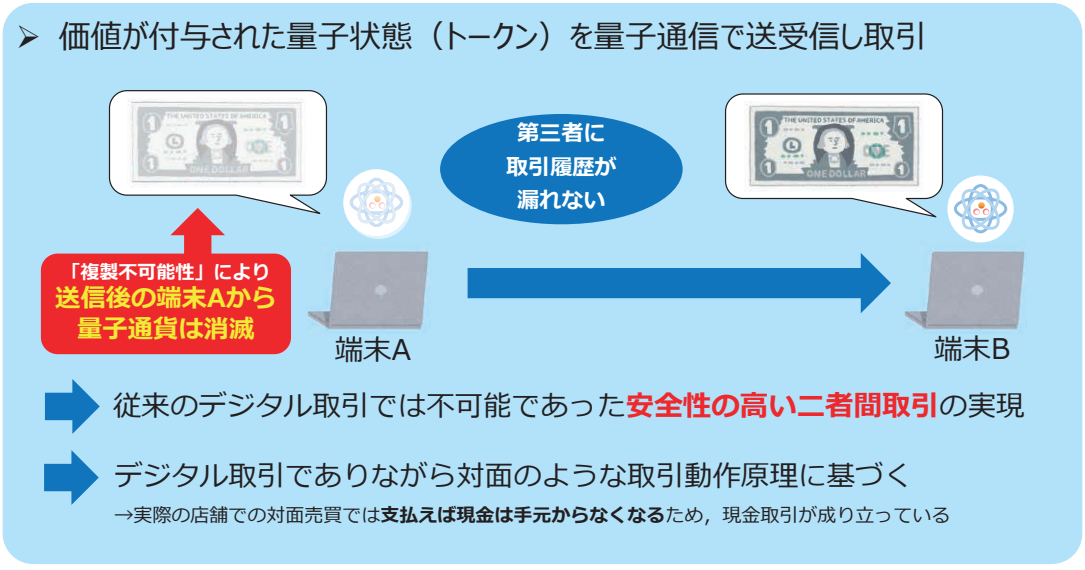



図4　「複製できない電子通貨」を使用した安全な二者間電子取引の実現

と思った１番のきっかけは，博士課程１年のときにNTT研究所でインターンを経験したことです．NTT研究所には，当時から世界的にも著名な暗号理論研究者が数多く在籍しており，通常のインターンの多くは１カ月程度であるのに比べそのときは２カ月の長期インターンだったのです．その２カ月間は非常に刺激的な日々でした．結果，そのときの研究を「ユーロクリプト」という国際学会で発表し，高く評価されるという非常に良い成果も得ることができました．そのインターンの期間中に，世界的にも活躍されているNTT内部の研究者の方に「長期間かかるような研究を一緒にやろう」と声をかけていただいたのが入社の大きなきっかけでした．

おかげで大学に戻った後も，自然に「NTT研究所で働けたらいいな」と考えるようになって，博士課程終了後の進路としてNTT研究所を希望し，運良く入社の運びになりました．今考えれば，インターンで志望がかなえられたことが私の運命だったようにも思えています．

**■所属されているNTT社会情報研究所にはどのような印象をお持ちでしょうか．**

NTT社会情報研究所は，情報通信技術により高度化する社会システムや人間社会の変革と発展に貢献する技術の研究開発を行っている研究所です．今すぐに役に立つような技術の研究開発ばかりではなく，長期的な展望に立って社会生活を豊かにするような新技術創出をめざした地道な基礎研究にも力を入れているのが大きな点です．15年から20年先の社会展開を見据えた研究開発も多数ありますし，私の研究もそのようなものの１つです．

NTTという一企業の研究所でありながら，目先の利益だけにとらわれず，惜しみなく真に価値のある研究を行おうとする姿勢は，この研究所の大きな特徴の１つです．

私が所属しているNTT社会情報研究所もいくつかの分野の研究を行っていますが，その中の１つがセキュリティ，暗号理論の研究です．NTTの暗号理論研究は長い歴史を持ち，国内外からも非常に高く評価されています．毎年，世界中から優秀な教授たちや研究者たち，インターンといった方々が私たちの暗号理論研究グループを来訪してくれているのはその証左です．私としても，こうした世界中の研究者の方々と最先端の研究に取り組み，話し合いができることは，研究者としてこのうえない幸せだと感じています．この研究所は，暗号理論研究に関していえば，国内で他にない唯一無二の環境だと感じています．

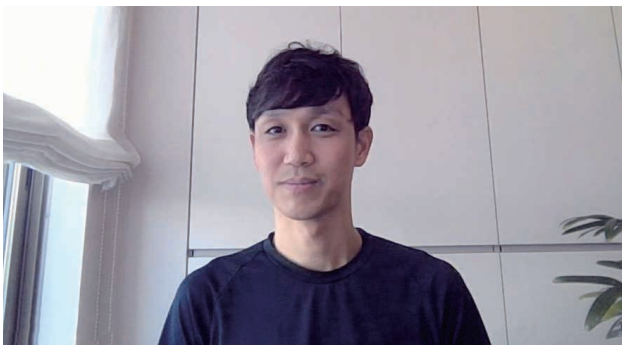
**■研究者・学生・ビジネスパートナーの方々に向けてメッセージをお願いいたします．**

これは学生のころからの持論ですが，私は研究の醍醐味は「議論」だと思っています．１人で黙々と問題を解く時間も楽しいのですが，自分の考えたことをさまざまな人と共有し，議論する中で，良い成果が生まれていく過程は本当に楽しいものです．

例えば，相手が研究者である場合もしかり，学生たち，ましてや基礎的な理論を知らない方たちからでもときには学ぶことがあります．例えば，専門用語を説明したときに出る質問から「ああ，こういう部分が分からないんだな」と，課題を発見でき，次に同じような方々にレクチャーする際の参考になることもあります．また何気ない雑談をきっかけに，非常に優れた成果が生まれることもあり，私は「議論」や「話し合い」の持つ力をこれまで何度も体験し感じてきました．

今後とも議論を重ねて，皆さんと共により良い未来に向けて前進していけたらと考えています．

最後に学生諸君に一言お話しします．NTT研究所は基礎研究の重要性を認識し，地道な基礎研究の積み重ねこそが真の革新的技術の創出につながるという信念を持った研究所です．そのような信念を持っている学生諸君には，NTT研究所は「ぜひに」と心の底からお薦めできる研究環境です．いつか皆さんと一緒に大いに議論し，共に研究できるようになることを楽しみにしています．



（今回はリモートにてインタビューを実施しました）