URL　https://journal.ntt.co.jp/article/36082
DOI　https://doi.org/10.60249/25095105

量子計算機時代の到来を見据えた暗号研究

NTT社会情報研究所では，量子計算機時代の社会課題解決と社会変革に資する，世界トップレベルの暗号・セキュリティ技術の研究開発に取り組んでいます．本稿では，耐量子計算機暗号理論の研究や標準化，現代暗号から耐量子暗号への移行に資するクリプトアジリティ技術の研究開発に加え，暗号理論と量子情報処理を融合した新たなセキュリティ技術の研究について紹介します．

キーワード：#耐量子計算機暗号，#PQC移行，#量子情報処理技術

髙屋　和幸（たかや　かずゆき）／安田　幹（やすだ　かん）
鷲尾　知暁（わしお　ともあき）／川原　祐人（かわはら　ゆうと）
阿部　正幸（あべ　まさゆき）

NTT社会情報研究所

NTTの暗号研究の実績と動向

NTT社会情報研究所は，40年以上にわたり暗号技術の研究開発に取り組み，世界トップレベルの成果を創出し続けてきました．主な成果としては，デジタル署名方式ESIGN（1990年），鍵カプセル化メカニズムPSEC-KEM（1999年），NTTと三菱電機が共同で開発した共通鍵ブロック暗号Camellia（カメリア，2000年），メッセージ回復型署名方式ECAOS（2008年），などが挙げられます．これら暗号化・署名方式のほかにも，安全性解析や攻撃手法の研究においても数多くの成果を創出してきました．直近の10年ほどは毎年，IACR（The International Association for Cryptologic Research：国際暗号学会）が主催する難関国際会議CRYPTO/Eurocrypt/Asiacryptに私たちの研究成果が採録され，いくつかは世界初の画期的な成果として高い注目を集めています．

また，私たちはそれら研究成果の社会実装にも幅広く取り組んできました．例えば，高機能暗号の1つである属性ベース暗号ABEの研究開発を進めてライブラリ化しました．属性ベース暗号は，ユーザの属性に基づいてデータへのアクセス制御を行うことが可能な暗号技術です．同じく，高機能暗号の1つである準同型暗号を活用した秘密計算技術を開発し，その成果はNTTグループ会社を通じてサービス化されました．秘密計算は，データを暗号化したまま計算できる技術であり，同技術はISO国際標準に採択されました(1)．

暗号分野においては，共通鍵暗号，鍵共有，公開鍵暗号，ハッシュ関数，署名，属性ベース暗号，秘密計算などの基礎技術があります．NTT研究所を含む世界中の研究者たちが長年にわたり，それら基礎技術の高度化や新たな基礎技術の確立に取り組んできました．

これらの基礎技術が確立されていたからこそ，冒頭で述べたESIGNなどの新技術，現在広く利用されている社会インフラが登場してきたといえます．例えば，インターネットの登場により不特定多数との通信が主流になったことを受け，公開鍵暗号と署名を活用してPKI（Public Key Infrastructure：公開鍵）基盤が実現されました．ほかにも，高速無線通信やクラウドの普及に伴ってIoT（Internet of Things）デバイスや組み込み機器が登場したことで，計算量・消費電力・メモリ使用量などを抑えた軽量暗号という新たな技術が誕生しました．新たな技術の中には，基礎技術として位置付けられ，さらに研究が進められるものもあります（**図1**）．

このように，さまざまな環境変化に応じて新技術や社会インフラをタイムリーに具現化し，安心・安全な社会を実現し続けるためには，土台となる暗号基礎技術の継続的な研究開発が非常に重要であると考え，私たちは日々の研究開発に取り組んでいます．

ここまでに述べた研究開発成果は，古典計算機＊1の上で現代暗号＊2を利活用する前提でしたが，私たちは現在，「量子計算機時代の到来」という大きな環境変化を見据えた研究開発を多く進めています．

量子計算機＊3の研究開発はここ数年で加速度的に大きく進展し，2030年代に実用的な量子計算機が登場するといわれています．環境変化の具体例として攻撃者が量子

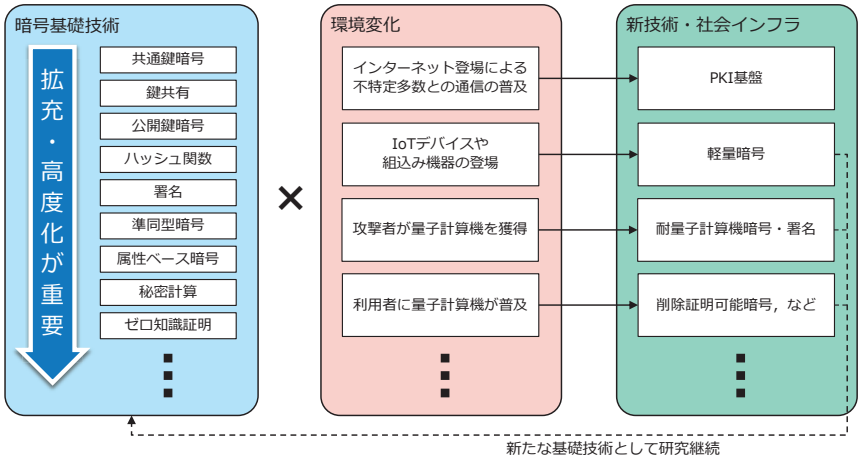

図1　環境変化に応じた新技術・社会インフラ実現の土台となる暗号基礎技術

＊1 古典計算機：私たちが日常的に利用しているコンピュータ（例：PC，スマートフォン，サーバーなど）のこと．情報を0と1の2進数で表現し，それを電気的スイッチのオフ・オンで実現しています．量子計算機と対比する表現として用いられます．

＊2 現代暗号：数学的な問題を安全性の根拠とし，暗号化アルゴリズムが既知であっても，情報を保護できる暗号方式のこと．共通鍵暗号方式のAESや公開鍵暗号方式のRSAなどが広く利用されています．

計算機を獲得することが想定されるため，私たちを含む世界中の研究者が耐量子計算機暗号*4の研究開発を現在も進めています（図1）．

また，量子計算機の実用化が差し迫ってきたことを受け，現代暗号を耐量子計算機暗号に置き換え移行する動きも世界中で活発化してきました．

さらに将来には，利用者が日常的に量子計算機を利用できる世界が訪れると思われます．そのような未来を見据えて，私たちは暗号理論と量子情報処理を融合し，従来では実現不可能だった新たな暗号機能を創出する研究にも取り組んでいます（図1）．

耐量子計算機暗号（PQC：Post-Quantum Cryptography）の研究開発

1994年に米国の数学者ピーター・ショアが，現代暗号の基礎になっている素因数分解問題や離散対数問題を解ける量子アルゴリズムを考案したことにより，公開鍵暗号が量子計算機を用いて現実的な時間内に解読される可能性が示されました．これを受け，量子計算機の計算能力をもってしても解読が困難な耐量子計算機暗号の研究が2010年代から本格的に始まり，私たちも取り組んできました．

その後，米国NIST（National Institute of Standards and Technology：米国国立標準技術研究所）は，国家サイバー戦略の優先実施項目としての指定に基づき，2016年から耐量子計算機暗号の標準化（コンペ）を開始しました．応募数が多いため，標準化は段階的に候補を絞り込むラウンド制で進められ，これまでに暗号化・鍵交換で2方式（ML-KEM，HQC），署名で3方式（ML-DSA，SLH-DSA，FN-DSA）の標準化が決定しています（**図2**）．私たちも格子問題に基づく暗号化・鍵交換方式NTRUを応募しました．NTRUは第3ラウンドまで進出しましたが，残念ながら標準化には至りませんでした．しかし，NTRUは標準化された方式（ML-KEM，旧CRYSTALS-Kyber）に対して処理時間での優位性があったので，IETF（Internet Engineering Task Force）での標準化に現在も取り組んでいます．

また，NISTは2022年9月に耐量子計算機署名の追加公募を開始し，世界から40方式の応募が集まりました．私たちは東京大学・九州大学・長崎県立大学と共同で，多変数多項式問題に基づくQR-UOVを提案しています．2024年10月に第2ラウンドに進出する14方式が発表され，QR-UOVも選出されました[2]（**図3**）．現在は第3ラウンド進出に向け，仕様の改良，安全性証明，ソフトウェア・ハードウェア両面での実装時の処理性能改善などに取り組んでいます．

ほかにも，NTTが長年取り組んできた楕円曲線暗号の知見を活かし，同種写像問題に基づく耐量子計算機暗号の研究にも取り組んでいます．同種写像暗号は，他の方式と比べて公開鍵や暗号文のデータサイズが小さいことから注目を集めている技術です．従来の同種写像暗号SIKEが2022年に破られて以降，複数の代替案が考案されてきましたが，私たちはもっとも計算効率が良い方式QFESTAを開発しました[3]．QFESTAは，ML-KEMと比較した場合に，秘密鍵のデータサイズで5分の1以下，公開鍵のデータサイズで3分の1以下を達成するとともに，暗号文のデータサイズでも下回る結果を出しました．また，私たちは東京大学やベルギーKU Leuvenの研究者と共同で，同種写像を利用した署名方式SQIsign2D-Eastも開発しました[4]．これは，NISTの耐量子計算機署名の追加公募に参加している方式SQIsignの検証コストを大幅に抑えた方式です．この成果が認められた結果，私たちの仲間が標準化の第2ラウンドからSQIsignチームに合流して研究開発を進めています．

以上のとおり，私たちは複数種類の耐量子計算機暗号の研究開発に取り組み，世界的にみても高い成果を創出し続けていると自負しています．引き続き，安心・安全な情報通信や社会の実現に資する耐量子計算

＊3 量子計算機：量子重ね合わせや量子もつれといった量子力学の現象を利用して実現されたコンピュータのこと．古典計算機よりも並列処理能力が高く，特定の問題を高速に解けると期待されています．
＊4 耐量子計算機暗号：量子計算機の計算能力をもってしても解読が困難な暗号方式のこと．

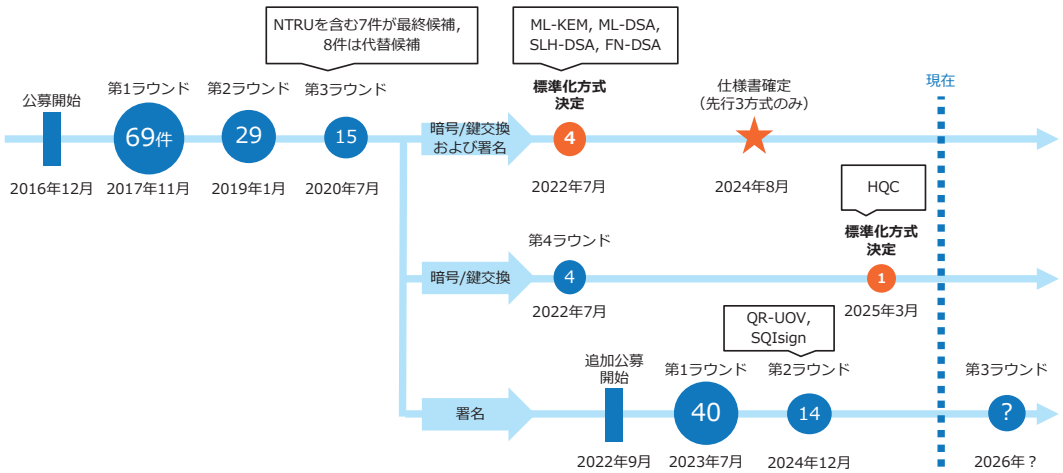

図2　NISTによる耐量子計算機暗号・耐量子計算機署名の標準化プロセス

機暗号の研究開発に取り組みます．

耐量子計算機暗号（PQC）への移行に関する研究開発

量子計算機のアイデアは1981年にさかのぼるといわれています．特にここ数年ではGoogle，IBM，ベンチャー各社による量子計算機の開発競争が激化しており，2030年代には誤り訂正機能を備えた量子計算機FTQC（Fault-Tolerant Quantum Computer）や暗号解読に適した量子コンピュータCRQC（Cryptographically Relevant Quantum Computer）がついに登場するといわれています．前述のショアのアルゴリズムとFTQC/CRQCとの組合せにより，PKI基盤などで幅広く利用されている公開鍵暗号が解読される脅威が現実味を帯びてきました．ほかにも，今のうちから攻撃対象の暗号文を集め，量子計算機の実用化後に解読する「ハーベスト・ナウ・ディクリプト・レイター（HNDL）攻撃」も現実的な脅威となっています．このような状況を受け，現代暗号から耐量子計算機暗号への移行（以降，「PQC移行」と呼びます）を行う必要性は，日に日に高まっている状況です．また，公開鍵暗号RSA-2048の使用期限を2030年末に迎えること（暗号の2030年問題）も，PQC移行を後押しする要因だといわれています．

以上の状況を踏まえ，私たちはPQC移行に資するクリプトアジリティ技術の研究開発にも取り組んでいます．クリプトアジリティとは，暗号方式を迅速かつ柔軟に切り替える能力のことであり，既存の暗号方式が破られたり新しい暗号方式が登場したりした場合に，システムに大きな変更を加えることなく新しい暗号方式に円滑に移行できるようにすることを指します．過去にも暗号の危殆化に伴う移行は行われてきましたが，鍵長の拡大対応を行って同一の暗号方式を継続利用する場合が多かったのが実態です．一方のPQC移行は，現代暗号から耐量子計算機暗号という全く新たな方式への移行であり，主だったものだけでも以下のような難しさがあります．

① 耐量子計算機暗号は，現代暗号に比べると研究開発期間が短いため，移行した耐量子計算機暗号の脆弱性がある日突然発見され，再度の移行を迫られる可能性がある．

② 耐量子計算機暗号は，現代暗号に比べるとデータサイズや鍵サイズが大きいため，通信コストやストレージコストなどの増加を招き，さらにIoT機器などの省リソースな機器では正常に動作しない場合もある．

③ 研究開発の歴史が浅い耐量子計算機暗号は，ポートフォリオ戦略に沿って特徴の異なる複数方式が同時並行で研究開発されており，従来の暗号移行と比べると移行先方式の選択が難しい．

PQC移行は，ほぼすべてのICTシステムが関係するものであり，企業・個人のみならず国家としても対応が必要であるため，各国が対応方針やタイムラインを公表しています．

米国では，バイデン大統領（当時）が2022年5月，量子計算機の開発に伴う既存暗号の危殆化を懸念し，2035年までを目途に耐量子計算機暗号へ移行することを目標とした大統領令に署名しました．これを受け，耐量子計算機暗号への移行に関して，各行政機関が2023年までに実施すべきタスクが示されました（しかし，トランプ大統領の政策変更により，本稿執筆時点でこれらのドキュメントは非公開になっており，活動の最新状況は一般的には分からなくなってしまいました）．

英国政府もPQC移行のタイムラインを公表しています．その概要は，2028年までにアセスメントを終えて移行計画を立てる，2031年までに最優先システムの移行を完了する，2035年までにそれ以外の全システムの移行を完了する，という計画です[5]．

EUも2025年2月にロードマップを公表しました[6]．英国のタイムラインよりも少し早く進める計画になっており，2026年末までにロードマップ策定を行って高リスク・中リスクのパイロットプロジェクトを開始する，2030年末までに高リスクについて移行完了する，2035年末までに中リスク・小リスクについて移行完了する，という内容です．

日本でのPQC移行に関する検討については，金融業界が先行しています．金融庁が「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」を立ち上げ，PQCへの移行を検討する際の推奨事項，課題および留意事項について幅広く議論を行い，2024年11月に報告書を公表しました[7]．金融庁は，メガバンクだけでなく地域銀行に対しても，早急にPQC移行の検討に着手するよう求めています．また，2025年6月30日には，政府機関等におけるPQC利用に関する施策を検討・推進するため，「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議」が開催されました[8]．2025年11月ころに，PQC移行の工程表（ロードマップ）の骨子を取りまとめる予定になっています．

Code-Based	Lattice-Based	MPC-in-the-Head	Multivariate
CROSS	EagleSign	Biscuit	3WISE
Enhanced pqsigRM	EHTv4	**MIRA***	DME-Sign
FuLeeca	HAETAE	**MiRitH***	HPPC
LESS	**HAWK**	**MQOM**	**MAYO**
MEDS	HuFu	**PERK**	PROV
WAVE	Raccoon	**RYDE**	**QR-UOV**
	SQUIRRELS	**SDitH**	**SNOVA**
Other			TUOV
ALTEQ	**Symmetric-Based**	**Isogeny-Based**	**UOV**
eMLE-Sig 2.0	AIMer	**SQIsign**	VOX
KAZ-SIGN	Ascon-Sign		
PREON	**FAEST**		
Xifrat1-Sign.I	SPHINCS-alpha		

青字：第2ラウンド進出
＊印の2方式は Mirath として統合

図3 NISTによる耐量子計算機署名の追加公募への参加方式

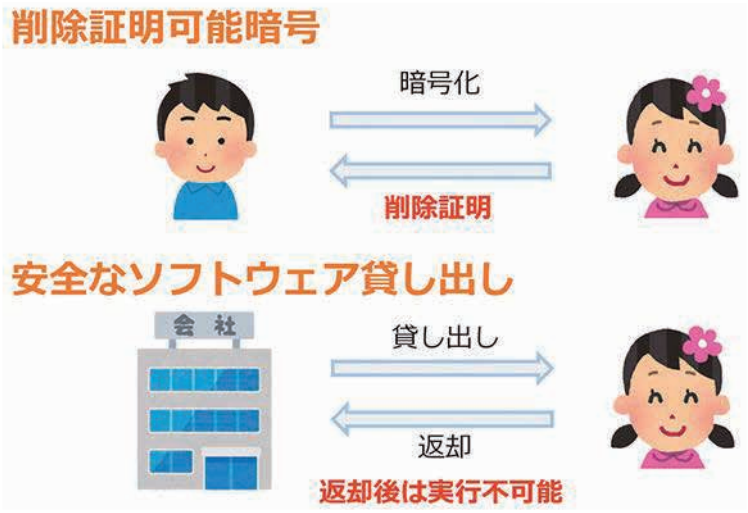

図 4　新たな暗号機能による社会問題の解決

今後ますます，PQC移行に関する動きが各国・各業界で本格化すると考えられます．PQC移行はNTTグループ各社やお客さま環境においても避けて通れない課題であり，私たちは円滑なPQC移行に資するクリプトアジリティ技術の創出および普及展開に引き続き取り組みます．

量子情報処理を活用した新たな暗号機能の研究開発

量子情報処理とは，量子力学の原理を利用して，従来のコンピュータでは不可能な情報処理を行う技術です．具体的には，量子ビットの重ね合わせやエンタングルメント（量子もつれ）といった量子力学的な現象を利用しています．量子計算機は，量子情報処理の代表例といえます．

2030年代に実用的な量子計算機が登場すると，まずは企業ユーザによる利用が進むと考えられますが，将来的には一般ユーザがクラウドサービスのようなかたちで日常的に量子計算機を利用できる世界が訪れると考えられます．そのような未来を見据えて，私たちは量子情報処理と暗号理論を融合させ，新たな暗号機能を創出する研究に取り組んでいます．

現在，私たちは日常的に重要なデータを暗号化してやり取りしています．暗号化されたデータを受け取った受信者は，そのデータをいくらでもコピー可能であり，データを利用し終ったときに受信者の手元から完全に削除されたことを送信者が確認する手段は存在しません．一方で，現実的には，利用し終ったデータが確実に削除されたことを保証する手段が求められています．

私たちはこのような課題の解決に向け，量子力学での「複製不可能定理」という，与えられた量子状態を複製することが不可能であるという定理を上手く活用することで，データ（暗号文）が削除されたことを証明できる暗号方式の研究を進めています[9]．この技術が確立された際には，例えば安全かつ適正なソフトウェアの貸し出し・返却が実現できます．具体的には，あるソフトウェアを借りたとき，レンタル期間中はそのソフトウェアを実行できますが，いったん返却した後は実行できない，というサービスが可能になります（**図 4**）．

これらはまだ基礎研究の段階ですが，このような研究を進めていくことにより，将来はデータ所有者の権利を適切に保護する仕組みを実現し，より信頼性の高い技術に基づいた安心・安全なデータ流通と利活用が広がる社会を実現できると考えています．

おわりに

本稿では，量子計算機時代の到来を見据えたNTT社会情報研究所の暗号技術の研究開発内容を，３つに大別して紹介しました．暗号技術は，安心・安全な社会の実現に資する基礎技術として今後も重要であり続けるものです．私たちは暗号技術のさらなる発展・高度化に向けて引き続き研究開発に取り組んでいきます．

■参考文献

(1) https://group.ntt/jp/newsrelease/2024/03/21/240321b.html
(2) https://group.ntt/jp/newsrelease/2025/01/20/250120a.html
(3) https://group.ntt/jp/newsrelease/2024/09/05/240905a.html
(4) https://group.ntt/jp/topics/2024/12/09/asiacrypt2024.html
(5) https://www.ncsc.gov.uk/pdfs/guidance/pqc-migration-timelines.pdf
(6) https://digital-strategy.ec.europa.eu/en/news/eu-reinforces-its-cybersecurity-post-quantum-cryptography
(7) https://www.fsa.go.jp/news/r6/singi/20241126.html
(8) https://www.cas.go.jp/jp/seisaku/pqc/dai1/gijisidai.html
(9) 山川：“量子コンピュータ時代に安全な通信を創出する暗号プロトコル研究，” NTT技術ジャーナル，Vol.34, No.12, pp.57-59, 2022.

(上段左から)髙屋　和幸／ 安田　幹／ 鷲尾　知暁
(下段左から)川原　祐人／ 阿部　正幸

量子計算機時代の到来を間近に控え，長年研究してきた耐量子計算機暗号をいよいよ社会実装する段階になりました．引き続き，各種の暗号基礎技術，耐量子計算機暗号，PQC移行に資するクリプトアジリティ技術，および社会に新たな価値を提供する暗号技術の研究に取り組んでいきます．

◆問い合わせ先

NTT 社会情報研究所
情報保護技術研究プロジェクト