第 19 回
情報セキュリティ・シンポジウム「量子コンピュータが金融サービスのセキュリティに与える影響」の模様

1. はじめに

日本銀行金融研究所情報技術研究センター（Center for Information Technology Studies: CITECS）は、2018 年 3 月 1 日、「量子コンピュータが金融サービスのセキュリティに与える影響」をテーマとして第 19 回情報セキュリティ・シンポジウムを開催した。

近年、量子コンピュータの研究開発が活発化している。量子コンピュータの処理性能が一定以上のレベルに達すると、現在主流の公開鍵暗号（RSA 暗号等）を現実的な時間で解読できることが知られているほか、共通鍵暗号についてもそのセキュリティが低下しうることが指摘されている。米国連邦政府は、2030 年頃までにそのような量子コンピュータが実現されうるとの見解を示し、2026 年頃までに対策する計画を発表している。

こうした動向を踏まえると、金融業界においても 2030 年以降も使用するシステムに関して、量子コンピュータの脅威への対応の検討を始めることが望ましい。今回のシンポジウムでは、量子コンピュータの最新動向と金融サービスのセキュリティへの影響について、講演とパネル・ディスカッションを行った。情報セキュリティ技術にかかわる金融機関の実務者や官公庁関係者、暗号学者、システム開発・運用に携わる実務者や技術者等、約 120 名が参加した。本稿では、下記プログラムに沿って、シンポジウムの講演等の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

本稿に示されている意見はすべて発言者たち個人に属し、その所属する組織の公式見解を示すものではない。

1 文中における各参加者の所属ならびに肩書きはシンポジウム開催時点のものである。各講演の資料については、CITECS のウェブサイト（https://www.imes.boj.or.jp/citecs/）に掲載しているので参照されたい。

【第 19 回情報セキュリティ・シンポジウムのプログラム】

- キーノート・スピーチ「量子コンピュータが金融サービスのセキュリティに与える影響」
  横浜国立大学大学院　教授　松本勉
- 講演 1「超伝導量子コンピュータの仕組みと研究開発をめぐる最新動向」
  東京大学先端科学技術研究センター　教授　中村泰信
- 講演 2「量子コンピュータの商用化動向」
  日本アイ・ビー・エム東京基礎研究所　副所長　技術理事　小野寺民也
- 講演 3「量子ゲート型コンピュータが暗号に与える影響と対策」
  日本銀行金融研究所　清藤武暢
- 講演 4「耐量子計算機暗号の標準化動向」
  東京大学大学院　教授　高木剛
- パネル・ディスカッション「量子コンピュータの脅威に対して金融機関が検討すべき対策とは」
  モデレータ：横浜国立大学大学院　教授　松本勉
  パネリスト：横浜国立大学大学院　教授　四方順司
  金融 ISAC　専務理事／ CTO　鎌田敬介
  三井住友銀行システム統括部システムリスク統括室
  室長代理　中山広樹
  NTT データ金融事業推進部技術戦略推進部技術戦略企画担当
  部長　山本英生

2. キーノート・スピーチ「量子コンピュータが金融サービスのセキュリティに与える影響」

松本は、量子コンピュータの最新動向や、量子コンピュータが金融サービスに与える影響について、以下のとおり発表した。

(1) 金融サービスと暗号

金融サービスにおいては、各種取引の安全性を確保するための基礎技術として暗

号（公開鍵暗号、共通鍵暗号）が利用されている[2]。現在主流の公開鍵暗号として RSA 暗号や楕円曲線暗号が挙げられ、共通鍵暗号については AES が挙げられる。暗号に対する従来の脅威としては、スーパー・コンピュータによって秘密の鍵を効率的に探索し、それを用いて暗号文を解読することや署名を改ざんすることが知られている。対策としては、スーパー・コンピュータの処理性能を評価したうえで、現実的な時間で探索できないように暗号鍵のサイズ（鍵長）等を設定して利用するという方法が採用されている。米国の国立標準技術研究所（National Institute of Standards and Technology: NIST）は、スーパー・コンピュータの処理性能に基づいて定めたセキュリティ・レベル（ビット・セキュリティ）を達成するための鍵長と推奨される利用期間を示している[3]。また、クレジットカードおよびデビットカードの業界標準である EMV 仕様においても、推奨する RSA 暗号等の鍵長とその利用期間を公表している[4]。

(2) 量子情報技術の発展と量子コンピュータの脅威

近年、量子力学の性質を利用した情報処理技術（量子情報技術）として、量子力学の性質を演算処理に応用する量子コンピュータ（量子計算機）と、その性質をデータ通信に応用する量子通信の研究開発が活発化している。量子コンピュータは、従来のスーパー・コンピュータ（古典コンピュータ）よりも高速な演算処理が可能であり、量子通信は、高速な通信速度やセキュアな鍵の配送を実現できる技術である[5]。これらの技術については、世界各国において実用化に向けた研究開発が進展している。

量子コンピュータは、量子ゲート型コンピュータと量子アニーリング型コンピュータの 2 種類に大別される[6]。これらのうち、量子ゲート型コンピュータにつ

2 公開鍵暗号は、暗号化に用いる鍵（暗号鍵）と復号に用いる鍵（復号鍵）が異なる暗号方式であり、暗号鍵を公開できるため、当事者間で事前に鍵の共有を行う必要がない。共通鍵暗号は、暗号鍵と復号鍵が同一（共通鍵と呼ばれる）となり、当事者間で事前に鍵の共有を行う必要がある一方、公開鍵暗号と比較して暗号処理を高速に行うことができる。

3 ビット・セキュリティは、暗号のセキュリティを評価する際の指標の 1 つである。この指標では、スーパー・コンピュータを用いて暗号鍵を探索するために必要な処理量を基準として、異なる暗号の方式間のセキュリティを相対的に評価できる。

4 EMV 仕様（EMV specifications）とは、IC クレジットカード・IC デビットカードのビジネスリスク管理を高度化するため、IC カード内での暗号処理などを含めた仕様を定めたもの。

5 量子コンピュータ以外のコンピュータを総称して、本稿では古典コンピュータと呼ぶ。

6 量子アニーリング型コンピュータは、対象とする問題をある種の物理問題に変換し、量子効果が働く装置を用いて行った実験結果から、当初の問題の解を求めるという仕組みに基づくものである。量子ゲート型コンピュータの仕組みについては、3 節（1）を参照されたい。

いては、その処理性能が一定のレベルに達すると公開鍵暗号や共通鍵暗号のセキュリティに影響を及ぼすことが知られており、新たな脅威として注目されている。

(3) 各国における対応

量子ゲート型コンピュータが暗号に及ぼす脅威への対応について、各国で検討が進められている。米国では、暗号鍵の鍵長が 2,048 ビットの RSA 暗号を数時間で解読可能な量子ゲート型コンピュータが 2030 年頃までに実現しうるとして、米国連邦政府が利用する公開鍵暗号について、量子ゲート型コンピュータでも容易に解読を行うことができない耐量子計算機暗号に移行する計画の策定が進められている。欧州では、耐量子計算機暗号を標準化するためのロードマップの検討が 2017 年 9 月に開始されている。わが国でも、暗号技術評価プロジェクトである CRYPTREC において、耐量子計算機暗号の調査が開始されている。金融サービスにおいても、今後、量子ゲート型コンピュータによる暗号のセキュリティ低下に対応していくことが求められるようになると考えられる。

今次シンポジウムのテーマは「量子コンピュータが金融サービスのセキュリティに与える影響」である。量子ゲート型コンピュータとその脅威に関する正しい理解を促進するために、量子ゲート型コンピュータの研究開発状況や、耐量子計算機暗号の現状について、第一線で活躍されている専門家の方々に講演していただく。さらに、パネル・ディスカッションでは、専門家の方々と金融サービスへの影響について議論したい。

3. 講演 1「超伝導量子コンピュータの仕組みと研究開発をめぐる最新動向」

中村 は、超伝導を用いた量子ゲート型コンピュータの仕組みについて解説し、その開発状況を紹介した。

(1) 量子ゲート型コンピュータの概要

量子ゲート型コンピュータの研究は、1980 年以降に発展した量子情報科学の理論を基に、素因数分解問題を解くアルゴリズム（ショアのアルゴリズム）や誤りを

量子的に訂正する技術等の提案を起爆剤として急速に発展した[7]。古典コンピュータで処理される情報の単位であるビットは、1 つのビットで 0 か 1 のどちらかの情報のみ表現することができる。一方、量子ゲート型コンピュータに用いる量子ビットは、量子力学の重ね合わせ状態を応用することにより、1 つの量子ビットで 0 と 1 を同時に表現することができる[8]。量子コンピュータでは、この量子ビットを用いた一種の並列処理が可能であり、これをうまく利用すると、古典コンピュータと比べて極めて高速な演算処理を実現することが可能となる。

ただし、現実の状況下では、量子ビットを用いた演算処理にはノイズ等の影響により誤りが発生することが知られており、この誤りを訂正しないと演算処理が正しく実行されないおそれがある。現時点において、理論的に誤り訂正処理を行うことが可能である量子コンピュータは量子ゲート型コンピュータのみである。一部の量子ゲート型コンピュータ実験では基本的な誤り訂正処理が既に実証されている。なお、量子アニーリング型コンピュータについては、現時点では誤り訂正処理の手法が見つかっていない。

このほか、量子コンピュータにおける演算処理と誤り訂正処理の実現に向けた研究を加速させるため、量子ビット数（量子ビット集積数とも呼ばれる）や量子ビットのコヒーレンス時間（量子ビットが誤りを起こさずに状態を保持することのできる平均的な時間）を向上させるための研究も世界規模で行われている。

(2) 世界の開発動向

主な企業における量子コンピュータの開発状況について紹介する。まず、量子ゲート型コンピュータについては、グーグル社が、9 量子ビットの量子コンピュータを実現しており、誤り訂正処理実験を行っている。さらに集積度を 49 量子ビットまで拡張させる研究に取り組んでいる[9]。また、アイ・ビー・エム社は、20 量子ビットの量子コンピュータを実現している。

これらの大企業だけでなく、スタートアップ企業による取組みも盛んである。例えば、最近 6,400 万ドルの投資を集め、19 量子ビットの量子ゲート型コンピュータを実現しているリゲッティ・コンピューティング（Rigetti Computing）社等が当て

7 ここでの誤りとは、量子ゲート型コンピュータにおいて演算処理を行う際に、ノイズ等によって量子ビットの状態に影響が生じる現象である。この誤りを訂正しつつ状態を制御することが量子ゲート型コンピュータの実用化における大きな課題となっている。

8 重ね合わせ状態は、複数の状態が同時に存在するという、量子力学における性質の 1 つである。

9 なお、2018 年 3 月 5 日の米国物理学会において、グーグル社は、72 量子ビットまでの拡張に成功し、回路を作製して実験を行っていると発表した。

はまる。そのほか、量子ゲート型コンピュータを動作させるためのソフトウェア（プログラム）を開発している企業も多数存在する。

量子アニーリング型コンピュータについては、ディー・ウェーブ（D-Wave）社が2,000量子ビットの規模を実現している。量子アニーリング型コンピュータで実装されている量子ビット数は、量子ゲート型コンピュータと比較して大きな値となっている。量子アニーリング型コンピュータは、量子ビット集積回路の最もエネルギーの低い状態を利用して、最適化問題の解を探索するものであり、量子ゲート型コンピュータとは計算原理や対象とする問題が異なる。量子アニーリング型コンピュータが古典コンピュータよりも優れた処理性能を発揮できるような問題と応用を見出すことを目的とした研究が盛んに行われている。

21世紀は、量子ゲート型コンピュータ等、量子力学の原理に基づく新技術体系へ向けた世界的潮流が生まれ、それを活かした新しいインフラやサービスが提供されていく時代になると考えられる。

4. 講演２「量子コンピュータの商用化動向」

小野寺は、アイ・ビー・エム社が開発を進めている量子ゲート型コンピュータを概説するとともに、その商用化の動向を説明した。

(1) アイ・ビー・エム社における量子ゲート型コンピュータの提供動向

アイ・ビー・エム社は、量子ゲート型コンピュータの開発を行っている。2016年5月に、5量子ビットの量子ゲート型コンピュータをクラウド（IBM Cloud）を介して誰でも利用できるようにした。これまでに世界中から6万ユーザがこの環境を利用しているほか、1,500の大学等や35の研究機関で使われており、利用実績が積み上がっている。さらに、2017年11月に、商用化を目的とした20量子ビットの量子ゲート型コンピュータを開発したほか、今後50量子ビットまで拡張する計画を立てている。

量子ゲート型コンピュータを活用する際は、（古典コンピュータのプログラムとは異なる）量子コンピュータ用のプログラムを用いる必要がある。当社では、このプログラムの製作を支援するソフトウェア開発キット（Software Development Kit）を、QISKitという名称で既に提供している。QISKitはGUI（Graphical User

Interface）を利用してプログラムを作成することも可能であり、量子ゲート型コンピュータのプログラムを容易に作成することができる。

(2) 量子ゲート型コンピュータの応用例

量子ゲート型コンピュータが応用可能と考えられる分野として、現時点においては、化学、人工知能（機械学習）、最適化問題の 3 分野が挙げられる。例えば、JP モルガン・チェース社は、QISKit を活用するなどして、量子コンピュータを活用したエコシステムの育成を行うネットワーク（IBM Q Network）に参加しており、トレーディング戦略、ポートフォリオ最適化、リスク分析等に活用したいと考えている。ダイムラー・アーゲー（Daimler AG）社は、自動車用新素材、製造プロセスの最適化、機械学習等に活用したいと考えている。日本企業も、JSR 社、日立金属社、本田技研工業社、長瀬産業社が IBM Q Network への参加を表明している。例えば、JSR 社は、電子部品（ディスプレイ等）用新素材の開発等に活用したいと考えている。

このように、取り扱うことが可能な量子ビット数が少ないにもかかわらず、少なからぬ企業が量子ゲート型コンピュータの本格利用に乗り出しているのは、今後、量子ビット数が急速に増加し、古典コンピュータを上回る演算処理が可能となった際に、速やかに量子ゲート型コンピュータを活用したサービスを提供できる環境を予め準備しておきたいとの考え方に基づいているとみられる。量子ゲート型コンピュータで動作するプログラムは、古典コンピュータでのプログラムとは全く異なっており、新規に設計・構築する必要がある。また、そうしたプログラムが適切に動作することを保証するために、プログラムの企画、実装、検証等に相応の時間を要することになる。

暗号鍵の鍵長が 2,048 ビットの RSA 暗号を量子ゲート型コンピュータで解読を行うためには、誤り訂正処理を実装したうえで、およそ 800 万量子ビットが必要とされている。現時点においては、その量子ビット数まで拡張できる量子コンピュータの実現は数十年先だと考えられている。

今後、量子ゲート型コンピュータを軸として、さまざまな企業と連携し、新しいサービスの提供に貢献していきたいと考えている。

5. 講演３「量子ゲート型コンピュータが暗号に与える影響と対策」

清藤は、量子ゲート型コンピュータを利用した暗号に対する攻撃手法や金融サービスに利用されている標準規格に及ぼす影響について、次のとおり発表した。

(1) 量子ゲート型コンピュータを利用した攻撃手法と対策

量子ゲート型コンピュータを実現する際には、量子アルゴリズムが必要である。量子アルゴリズムとは、量子ビットの重ね合わせ状態を維持したまま演算処理を行うとともに、処理結果の量子ビットを観測した際に、最適な解が得られるように量子ビットに設定されている確率を操作する手順である[10]。一部の量子アルゴリズムは、公開鍵暗号や共通鍵暗号に対する攻撃手法に利用することが可能であり、一部の暗号については現実的な時間で解読を行うことができる。例えば、①素因数分解問題を解くショアのアルゴリズム、②検索条件に合致するデータの探索を行うグローバーのアルゴリズム、③関数の周期を探索するサイモンのアルゴリズムが該当する[11]。

代表的な公開鍵暗号である RSA 暗号と楕円曲線暗号は、素因数分解問題と楕円曲線離散対数問題の困難性をそれぞれ安全性の根拠としている[12]。ショアのアルゴリズムを実現できれば、これらの問題を現実的な時間で解くことが可能であり、RSA 暗号や楕円曲線暗号のセキュリティは失われることとなる。対策としては、耐量子計算機暗号への移行が考えられる。

共通鍵暗号では、ブロック暗号である AES（Advanced Encryption Standard）に暗号利用モードを組み合わせる方式が主流である。これに対する攻撃手法として、グローバーのアルゴリズムを利用して共通鍵を全数探索する方法が知られており、鍵長を 2〜3 倍程度伸長するという対策が考えられる[13]。もっとも、最近では、鍵長を

10 量子ビットは、外部から何らかの手段によって観測されると、重ね合わせ状態が失われ、古典コンピュータのビットと同様に、同時に表現されていたものがいずれかのデータに変換される。どのデータに変化するかは、量子ビットに設定されている確率に依存する。

11 関数の周期とは、関数において、出力値が同一となる（異なる複数の）入力値の間に存在する関係性のことである。

12 ここでの素因数分解問題は、自然数 N が与えられたとき、$N = P \times Q$ を満たす 2 つの素数 P と Q を求める問題を指す。楕円曲線離散対数問題は、特殊な曲線（楕円曲線）上の 2 点 T と G について、T と G の間の関係性を求める問題である。

13 探索する鍵候補の個数を 2^{100} としたとき、古典コンピュータを用いて正しい共通鍵を探索する場合

伸長したとしても、一部の共通鍵暗号については、サイモンのアルゴリズムを活用することにより、現実的な時間で共通鍵等を探索できることが報告されている[14]。対策としては、サイモンのアルゴリズムに耐性のある方式への移行が考えられる。

(2) 金融サービスで利用されている標準規格への影響

公開鍵暗号と共通鍵暗号は、金融サービスで利用されている標準規格において規定され、広く利用されている。

こうした標準規格としては、金融取引における本人確認に利用される暗証番号の安全性を確保する仕組みを規定する ISO 9564-1, 2 や、金融サービスでの利用を推奨する暗号を取り纏めた ISO/TR 14742 等が挙げられる。また、インターネット上で利用される技術の標準化を推進する IETF（Internet Engineering Task Force）の暗号通信プロトコル TLS（Transport Layer Security）は、金融機関がオンライン・バンキングの安全性を確保するために利用されている。EMV 仕様等も、公開鍵暗号や共通鍵暗号を規定している。これらの規格においては、今後、耐量子計算機暗号への移行や共通鍵暗号の鍵長の伸長等の対策を踏まえた改訂が必要になると考えられる。

6. 講演 4「耐量子計算機暗号の標準化動向」

高木 は、耐量子計算機暗号の標準化をめぐる最近の動向について、以下のとおり説明した。

(1) 耐量子計算機暗号の標準化

米国の国家安全保障局（National Security Agency）が RSA 暗号や楕円曲線暗号を耐量子計算機暗号に移行する計画を 2015 年に公表したことを機に、欧米を中心に耐量子計算機暗号に関連する国際会議やワークショップが数多く開催され、理論や

には最大で 2^{100} 回程度の処理が必要となるのに対し、グローバーのアルゴリズムを用いる場合には 2^{50} 回程度の処理で探索することができる。

14 探索する総数を 2^{100} 個としたとき、古典コンピュータを用いて周期を求める場合には最大で 2^{100} 回程度の処理が必要となるのに対し、サイモンのアルゴリズムを用いる場合には 100 回程度の処理で探索することができる。

実装面の研究が活発化した。わが国においても、科学技術推進機構による助成を受けた耐量子計算機暗号に関する大規模な研究プロジェクトが、九州大学・東京大学・東京工業大学の研究チームにより進められている。

NIST は、暗号鍵の鍵長が 2,048 ビットの RSA 暗号を数時間で解読可能な量子ゲート型コンピュータが 2030 年頃までに実現する可能性があるとの見解を示したうえで、2026 年頃までに米国連邦政府で使用する公開鍵暗号を耐量子計算機暗号に移行する計画を示している[15]。この計画の一環として、NIST では耐量子計算機暗号の標準化に向けた作業を進めている。2017 年 11 月末まで標準化候補の耐量子計算機暗号を募集し、その後 3〜5 年かけて、応募された方式の安全性や効率性を評価したうえで標準化する方式を決定するというものである。応募された方式（69 件）については、格子問題に基づく耐量子計算機暗号（格子暗号）が最も多く（24 件）、符号暗号（16 件）、多変数多項式暗号（10 件）と続く[16]。各方式については、暗号鍵の鍵長や処理速度の観点において一長一短があり、すべての観点において優れた方式は現時点では存在していない。

汎業界的な暗号の国際標準を規定する ISO/IEC JTC 1/SC 27 においては、耐量子計算機暗号の研究動向のサーベイを進めており、今後、報告書を作成する予定である。また、IETF においては、耐量子計算機暗号の標準規格のドラフト版を公表しコメントを募集している。わが国の電子政府で利用可能な暗号のリスト（CRYPTREC 暗号リスト）の策定および管理を行っている CRYPTREC においても、耐量子計算機暗号の調査を行っており、調査結果を 2019 年末までに公表する予定である。

(2) 暗号の安全性評価と標準化プロセスの関係性

新しい暗号が提案された後、実用化されるまでのフェーズは、大きく分けて提案、安全性検証、実用化の 3 つである。提案フェーズでは、新しい暗号が提案され、安全性検証フェーズでは、国際会議等、公開された環境下で安全性に関する議論や検証等が行われる。安全な鍵長等についてコンセンサスが得られると、暗号に

15 NIST は、現在広く利用されている暗号の利用にかかるガイドライン（SP 800-57 Part 1）を 2030 年まで利用可能としているが、その後の利用期限については明らかにしていない。

16 格子とは、空間上に規則正しく並んでいる点の集合である。格子問題とは、この格子上で定義される数学的問題であり、ある条件を満たす格子上の点を探索する問題の総称である。これらの数学的問題を安全性の根拠として利用する公開鍵暗号は格子暗号と呼ばれる。
　符号暗号は、データに誤りが生じた際にそれを訂正する誤り訂正符号について、一定レベル以上の誤りが生じたデータから、元のデータを復号する問題を解くのが困難であることを安全性の根拠とする公開鍵暗号である。多変数多項式暗号は、多変数非線形方程式が与えられたとき、その解を求める問題を解くのが困難であることを安全性の根拠とする公開鍵暗号である。

関する標準規格の策定が行われる。最後に、実用化フェーズでは、企業による情報システム等への実装が行われる。

暗号の安全性は経年劣化するため、標準規格の暗号については、定期的に安全性評価を行い、対策（鍵長の伸長等）を新たに規定する必要がある。RSA 暗号についても、学界等で定期的に安全性評価が行われており、安全な鍵長が NIST や CRYPTREC 等により順次公表されている。

代表的な耐量子計算機暗号である格子暗号については、現在、その安全性評価が行われている。数学的な安全性評価に加えて、コンピュータを用いた格子暗号の解読を行うコンテストも行われており、安全な鍵長等の見積りが行われている。今後、格子暗号等の耐量子計算機暗号の安全性評価が進展すると、RSA 暗号と同様に、コンセンサスが得られた安全な鍵長等が公表され、企業の情報システムに実装されていくようになると考えられる。

7. パネル・ディスカッション「量子コンピュータの脅威に対して金融機関が検討すべき対策とは」

パネル・ディスカッションでは、耐量子計算機暗号への移行に際して金融機関が検討すべき事項等について、以下のとおり議論を行った。

(1) 量子コンピュータによるメリットとデメリット

モデレータの 松本 は、まず、金融機関が量子コンピュータに対して期待していることや想定されるユースケースについて、パネリストに意見を求めた。

中山 は、人工知能を利用した業務や与信審査、マーケット分析にかかる演算処理等に適用することができるのではないかとの見方を示した。

山本 は、量子アニーリング型コンピュータが金融のマーケット分析に有用であろうと述べた。さらに、資産管理に関連する業務にも活用できるのではないかとの見解を示した。

鎌田 は、仮想通貨のマイニング処理や人工知能（深層学習）における学習処理等に適用し、それらの高速化が期待されるとの意見を述べた。また、金融機関において膨大な処理時間を有する業務がある場合には、その業務に量子コンピュータを活用することが有用であるとした。

次に、松本は、量子コンピュータの性能向上によって危惧されることについて、パネリストに意見を求めた。

中山は、本シンポジウムのテーマでもある現在主流の暗号が危殆化することを懸念しているとしたうえで、金融機関はさまざまなアプリケーションを提供しており、その多くがセキュリティ低下という影響を受けるのではないかと述べた。特に、顧客向けのアプリケーション（例えば、インターネット・バンキング）のセキュリティ低下を回避することは、安心・安全を使命としている金融機関として必須であることから、そうしたアプリケーションへの対応を実施することになるであろうとの見解を示した。また、働き方改革の一環で、在宅勤務を行うために行内システムへのアクセスを遠隔から可能とするリモート・アクセス・システムにも影響が及ぶ可能性があり、その場合は、業務継続上の課題も生じうると付言した。

鎌田は、仮想通貨が暗号のセキュリティに依存している部分があり、万一、システム側の対策が後手に回ってしまうと、多くの利用者が仮想通貨を失いかねないとの見解を示した。

これを受けて、山本は、仮想通貨が改ざん防止にハッシュ関数を利用している場合、量子コンピュータによりハッシュ関数のセキュリティが低下すると、取引内容が改ざんされるおそれがあると説明した。特に、パブリック型のブロックチェーンを利用する仮想通貨等では、不特定多数の利用者による合意形成が前提となることから、そのインパクトは大きいと付言した。

四方は、仮想通貨やブロックチェーン等のプロトコルを量子コンピュータ出現時にも安全に利用するためには、プロトコル内で利用されている暗号アルゴリズムを洗い出したうえで、それらが量子コンピュータに耐性を有することを確認する必要があると説明した。

(2) 誰が量子コンピュータを悪用しうるか

松本は、暗号の脅威となる量子ゲート型コンピュータを、当初、誰が保有し、利用することが想定されるかについて、パネリストに意見を求めた。

山本は、量子ゲート型コンピュータには莫大な開発コストや維持管理コストが必要となることから、まずは国家や（現在開発している）大手 IT 企業、国から援助を得ている研究機関において利用可能となると考えられ、当初は国家レベルの攻撃に使われるであろうとの見解を示した。

これに対して、フロアから、中村（講演 1 の講演者）は、量子ゲート型コンピュータは世界各国で開発されており、実機を保有しているのはごく一部の企業や研究機関に限定されているとみられるものの、開発している事実を公表し

ていない企業や研究機関がその他に存在する可能性もあると補足した。また、小野寺（講演 2 の講演者）も、アイ・ビー・エム社の場合、商用化に当たっては、量子ゲート型コンピュータの設備を企業に提供するという形態ではなく、量子ゲート型コンピュータの利用環境をクラウド経由で提供するという形態になるであろうとの見方を示した。

中山は、金融機関の最も重要な勘定系システムにおいては、量子コンピュータを活用するニーズはないと考えられると説明した。一方、人工知能を利用した業務や与信審査、マーケット分析、リスク計算等のシステムにおいては、高速化が求められる場面がありうる。その場合は、自前で量子コンピュータを保有することは考えにくく、クラウド経由での利用形態になるであろうと述べた。

松本は、従来の暗号に対する攻撃手法について、複数のゲーム機や GPU（Graphical Processing Unit）を用いた並列処理により効率化する研究成果が報告されているが、量子ゲート型コンピュータを用いても同様のことが可能であるかについてパネリストや講演者にコメントを求めた[17]。

これに対して、フロアから、高木（講演 4 の講演者）は、複数の量子ゲート型コンピュータによる並列処理は、量子ビットの制御（量子重ね合わせ状態の維持等）に高度な技術が要求されるため、攻撃手法の高速化は難しいとの見解を示した。

次に、松本は、量子コンピュータのエネルギー効率について意見を求めた。

小野寺（講演 2 の講演者）は、アイ・ビー・エム社の量子ゲート型コンピュータでは、絶対零度近くまで冷却する必要があるが、いったん冷却すれば、古典コンピュータに比べ遥かに少ない電力で稼働維持できると説明した。

(3) 推奨される暗号の移行パターン

松本は、RSA 暗号等から耐量子計算機暗号への移行パターンとして、従来の暗号の暗号鍵を伸長した後、耐量子計算機暗号に移行するパターン（パターン 1）と、暗号鍵の伸長を行わずに耐量子計算機暗号に移行するパターン（パターン 2）を示し、セキュリティや可用性等の観点からどちらが望ましいかについてパネリストに意見を求めた。

中山は、一般に、金融機関ではシステムの更改時期に合わせて暗号の移行を行うが、その時点で最適な暗号が選択可能な状態になっていることが求められるとしたうえで、更改時期に耐量子計算機暗号が選択可能となっている場合にはパターン

17 GPU は、画像処理に特化したプロセッサであり、3 次元画像のリアルタイム処理等で必要となる単純かつ大量の演算処理を、並列処理により効率よく処理できるという特長を有する。そのため、画像処理以外でも大量のデータを並列処理する際には、GPU が利用される場合が多い。

2 も採用しうるが、そうでない場合にはパターン 1 とせざるを得ないとの考えを示した。

山本 は、中山の意見に賛意を示したうえで、システムの実装において暗号処理のモジュール化を行っている場合には、パターン 2 の方がより効率的に実施できると付言した。

鎌田 も、中山、山本と同様に、量子ゲート型コンピュータの開発スピードがパターン選択に際しての重要なポイントになると補足した。さらに、金融機関がシステム更改に合わせて耐量子計算機暗号を導入するか否かを判断するための情報を入手可能な環境の整備や、耐量子計算機暗号への移行が困難な端末を利用している顧客への対応（レガシー対応）もパターンの選択において重要となるとの考えを示した。

四方 は、パターン 1 の場合、（古典コンピュータの攻撃アルゴリズムに加えて）量子ゲート型コンピュータの実用化動向も考慮に入れて、鍵長の伸長度合いを決めるべきであるが、過去のケースに比べて大幅に伸長しなくてはならない可能性もあると指摘した。さらに、米国政府が耐量子計算機暗号の標準化を推進していることから、2030 年頃には、耐量子計算機暗号が主流となっている可能性があるとの見方を示した。

ここで、フロア参加者 から、公開鍵証明書の発行や管理業務を行う認証局の一部においては、既にパターン 1 による移行（鍵長を 3,072 ビットに伸長）が進められていることが紹介された。また、これまでの経験上、新しい暗号が標準化されたとしても、普及するまでには 20 年から 30 年の時間を要することから、暗号の移行にかかる長期的な計画をまず立案することが望ましいとの意見が示された。

次に、松本 は、システムに暗号を実装する方法として、暗号処理を行う部分をモジュール化する方法（一般的構成法）と、特定の暗号に特化して処理を最適化する方法（直接的構成法）があると説明した。そのうえで、量子ゲート型コンピュータへの対策を進める際に、どちらの実装方法が望ましいかについてパネリストに意見を求めた。

中山 は、一般的構成法に基づいて実装することが理想的であるものの、システム全体の信頼性や可用性に関するテストを行う必要性も考慮して実装方法を決定する必要があるとの考えを示した。

ここで、フロア参加者 より、金融機関のシステムにおいて、暗号を利用している部分は主に顧客との通信を行う処理であるとしたうえで、暗号の移行に際しては、顧客の OS やブラウザが耐量子計算機暗号に対応していることが前提となるとの意見が寄せられた。さらに、顧客の OS 側での対応が進めば、金融機関側でも対策を進めざるを得なくなる可能性があるとの発言があった。

これを受けて、山本 は、耐量子計算機暗号に移行するためには、顧客の OS やブ

ラウザでの対応に加えて、セキュリティ・ベンダーが耐量子計算機暗号のソリューションを提供しなければならないと説明した。そのうえで、システム構築・運用に関連するすべての部分において移行の準備が整うことが重要であると補足した。

さらに、フロア参加者 より、耐量子計算機暗号の安全性評価が研究途上であり、古典コンピュータでも解読や改ざんが行われるリスクがあるのではないかとの質問が寄せられた。これに対して、四方 は、耐量子計算機暗号は、古典コンピュータでも、量子ゲート型コンピュータでも効率的には解かれないという数学的問題（NP 困難問題）がセキュリティの根拠になっていると述べた。ただし、具体的に用いられるパラメータ選択が適切でなければ、解読や改ざんが行われる可能性はあるため、今後、耐量子計算機暗号に対するパラメータの評価が行われることになろうと述べた。

また、小野寺（講演 2 の講演者）は、金融分野だけでなく、社会全体において暗号を移行しやすいシステムを構築する、すなわち、利用している暗号が危殆化した際には、システム全体ではなく、暗号を制御している箇所のみを移行できるように構築するという考え方について、パネリストやフロア参加者に意見を求めた。これに対して、フロア参加者 より、現時点では移行に時間を要するシステム構成が主流となっているが、今後、暗号を移行しやすいシステム構築を行うとともに、ソフトウェア等に有効期限を設けるという考え方もありうるとの意見が示された。

(4) 耐量子計算機暗号への移行を検討する際の留意点

松本 は、暗号の移行には相応の期間（10 年程度）が必要となるが、金融機関はどのような点に留意して移行の検討を進めていくべきかについて、パネリストに意見を求めた。

鎌田 は、金融機関では、暗号の移行以外にもシステム面で解決すべき課題が山積しており、それらの課題と耐量子計算機暗号への移行のバランスを考慮することが重要であると説明した。

中山 は、耐量子計算機暗号への移行について予め検討しておくことが重要であるとしたうえで、量子ゲート型コンピュータが RSA 暗号等に対して現実の脅威となりうる時期が明確になると、逆算して対応スケジュールが定まるとした。その際、量子ゲート型コンピュータの開発動向をフォローすることはもとより、システム面での具体的な検討の開始時期に直結することから、セキュリティ・ベンダーによる耐量子計算機暗号のソリューションの提供動向についてもフォローすることが必要であると付言した。暗号の移行に際しては、まずは重要度の低いシステムで試行し、信頼性や可用性に関する検証を行った後に、信頼性・可用性の要求度合いが

高いシステムへと順に対応していくことになる可能性や、システムのライフサイクルの期間と更改時期に合わせて対応する可能性等を考慮すると、現時点において耐量子計算機暗号のソリューションが提供されていないのであれば、2030年までの対応が困難であるかもしれないとの考えも示した。さらに、その場合は、現在主流の暗号の危殆化がどの程度の脅威かということを踏まえて、リスクを許容できるかどうかを検討し、許容できない場合には、代替としてどのようなリスク対策が可能かを検討しなければならないであろうと述べた。

山本は、暗号のセキュリティが低下することによる損失と量子ゲート型コンピュータの利用にかかるコストのバランスについて、研究動向等を踏まえて見極めることが、移行の検討を開始する時期を決定するうえで重要なポイントとなるとの考えを示した。

松本は、全体の議論を総括し、量子ゲート型コンピュータの研究開発が進展することにより、金融分野では、新しいサービスの提供や業務の効率化等のメリットがある一方、暗号の解読という脅威への対応について、金融機関は予め検討しておくことが重要であると説明した。耐量子計算機暗号の標準化や製品化等、移行に際して必要な環境がまだ整備されておらず、具体的な検討開始時期を現時点で明確にすることは難しいものの、NISTによる標準化動向等をフォローしておくことが必要であると述べた。最後に、金融分野での検討が進展し、ひいては社会全体での対応を後押しする動きにつながることを期待したいとして、パネル・ディスカッションを締め括った。