日銀レビュー

2018-J-4

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とその対策

金融研究所　清藤武暢

Bank of Japan Review

2018 年 6 月

金融分野では、金融サービスの安全性を確保するための基盤技術として暗号が利用されている。現在、広く利用されている暗号は、既存のコンピュータ（スーパーコンピュータ）を用いても解読が困難なように設計されている。しかし、近年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向上すると、これらの暗号の安全性が低下しうることが知られている。本稿では、量子コンピュータが暗号の安全性低下を通じて金融サービスのセキュリティに与える影響と、金融機関が今後検討すべき事項について整理する。

はじめに

金融分野では、金融サービス等において取り扱われるデータの安全性を確保するために、暗号が広く利用されている。例えば、オンライン・バンキングにおいて、顧客と金融機関のホスト・コンピュータ間でやり取りされるデータ（暗証番号や取引内容等）の盗聴や改ざんの防止、ATM や POS 端末における IC カード（キャッシュカードやクレジットカード等）の真正性確認等のために活用されている。

こうしたなか、近年、量子力学の性質を利用した量子コンピュータの研究開発が活発化している[1]。量子コンピュータの処理性能が一定のレベルに達すると、現在広く利用されている暗号の安全性が低下するとともに、一部の暗号については現実的な時間で解読できることが知られている。このため、量子コンピュータによる暗号の安全性低下は、金融サービス全体にも大きな影響を及ぼすと考えられる。今後、金融機関は、量子コンピュータの脅威の程度を把握したうえで、当該サービスのセキュリティを確保するための対策を検討する必要がある。

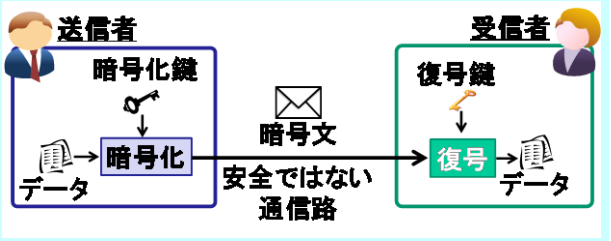
暗号とその仕組み

暗号は、通信路上で第三者（攻撃者等）による盗聴や改ざんを防ぐために、データを変換する技術の総称である。暗号を利用した通信においては、データの送信者は、暗号化鍵を用いてデータを暗号化し、暗号化したデータ（暗号文）を受信者に送信する（図表 1）。受信者は、復号鍵を用いて暗号文から元のデータを復号する。こうした通信を行うためには、暗号化鍵や復号鍵を当事者間で安全に共有しておく必要がある。その仕組みの違いにより、公開鍵暗号と共通鍵暗号の 2 種類に大別される。

公開鍵暗号は、暗号化鍵と復号鍵が異なる方式である。この方式では、暗号化鍵を公開できるため、データのやり取りを行う当事者間で事前に鍵を共有する必要がない。代表的な公開鍵暗号である RSA 暗号は、桁数の大きな 2 つの素数の積（合成数）から元の素数を求める数学的問題の困難性を利用している[2]。

共通鍵暗号は、暗号化鍵と復号鍵が同一（共通鍵と呼ばれる）の方式である。当事者間で事前に共通鍵を共有する必要がある一方、公開鍵暗号と

【図表 1】暗号の処理フロー



比較してデータの暗号化や復号にかかる処理を高速に行うことができる。金融分野で広く利用されている共通鍵暗号として、AES（Advanced Encryption Standard）が挙げられる[3]。

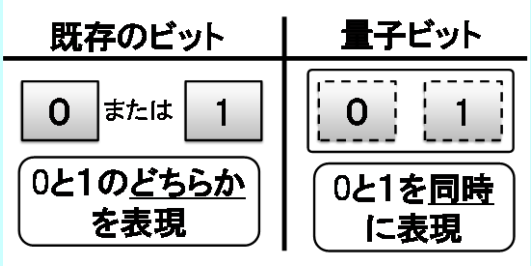
公開鍵暗号と共通鍵暗号は、金融サービスの安全性を確保することを目的とするさまざまな標準規格において規定されている。例えば、金融取引用の暗証番号の安全性を確保するための仕組みを規定する国際規格（ISO 9564-1,2）や、金融サービスでの利用を推奨する暗号を取りまとめた技術報告書（ISO/TR 14742）等が挙げられる。また、オンライン・バンキングの安全性を確保するために広く利用されている暗号通信プロトコル TLS（RFC 5246）でも、公開鍵暗号や共通鍵暗号が規定されている。さらに、クレジットカードやデビットカードの業界標準である EMV 仕様においても、取引における成りすましや取引内容の改ざん等を防ぐために公開鍵暗号や共通鍵暗号の利用が規定されている。

量子コンピュータとその開発動向

量子コンピュータは、実現方式の違いにより、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に分類される。量子ゲート型コンピュータは、既存のコンピュータと同様、さまざまな問題を解くことを目的としている。他方、量子アニーリング型コンピュータは、特定の問題（組合せ最適化問題）を解くことを目的としている[4]。現時点では、暗号の解読と組合せ最適化問題の関係性が明らかになっておらず、量子アニーリング型コンピュータを用いて暗号を効率よく解読することは難しいと考えられている。

量子ゲート型コンピュータは、複数の状態が同時に存在するという量子力学の性質（重ね合わせ状態と呼ばれる）を演算処理に利用する。既存のコンピュータでは、取り扱うデータの最小単位はビットであり、1 つのビット（1 ビット）で 0 か 1 のどちらかのデータのみを表現できる。量子ゲート型コンピュータでは、取り扱うデータの最小単位は量子ビットと呼ばれる。量子ビットは、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（1 量子ビット）で 0 と 1 の 2 つのデータを同時に表現することができる（図表 2）。そのため、量子ビットに対する 1 回の演算処理により、両方

【図表 2】既存のビットと量子ビット



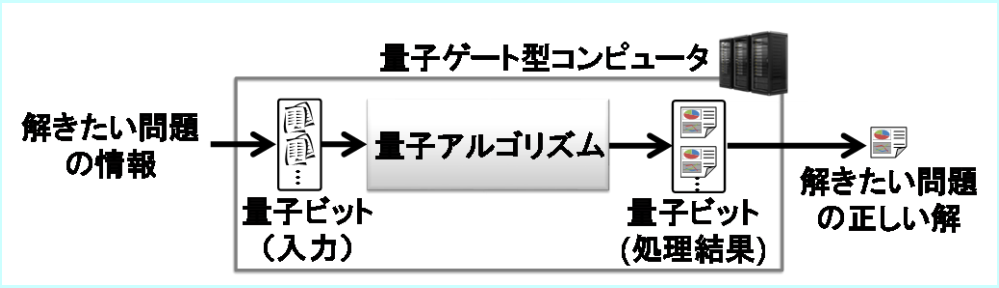
のデータに対して同時に（並列的に）処理を行うことができる。一般に、量子ゲート型コンピュータで取り扱うことが可能な量子ビットの数が 2 倍や 3 倍に増えると、1 回で処理できるデータの個数はそれぞれ 4（= 2^2）倍や 8（= 2^3）倍となる。こうしたことにより、量子ゲート型コンピュータは、既存のコンピュータと比較して、極めて高速な演算処理を実現できるとみられている。

近年、海外の企業を中心に量子ゲート型コンピュータの開発が進められている。グーグル社は、2018 年 3 月に、72 量子ビットを取り扱うことが可能な量子ゲート型コンピュータを実装するための基礎技術（プロセッサ）を開発し、さらに、このプロセッサを利用した演算処理の精度向上に関する研究や実証実験に取り組んでいる[5]。アイ・ビー・エム社は、2017 年 11 月に、20 量子ビットを取り扱うことが可能な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公表している[6]。インテル社は、2018 年 1 月に、49 量子ビットを取り扱うことが可能な量子ゲート型コンピュータを実装するためのプロセッサを開発し、さらに、このプロセッサの小型化に向けた研究に取り組んでいる[7]。マイクロソフト社は、2017 年 12 月に、量子ゲート型コンピュータの演算処理を既存のコンピュータ上でシミュレーションすることが可能な開発環境を公開している[8]。

量子ゲート型コンピュータによる暗号解読

量子ゲート型コンピュータで問題を解く際に重要となるのは、量子ビットの制御である。量子ビットは、外部から何らかの手段により観測すると、重ね合わせ状態が失われ、同時に表現されていたもののいずれかのデータ（1 量子ビットの場

【図表 3】量子コンピュータと量子アルゴリズム



合には 0 か 1）に変化する。どちら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基づいて定まる。量子ゲート型コンピュータを用いて正しい解を得るためには、量子ビットの重ね合わせ状態を維持しつつ、上記の確率を適切に操作する必要がある。こうした操作の手順は量子アルゴリズムと呼ばれる（図表 3）。

公開鍵暗号の解読に利用可能な量子アルゴリズムとして、ショア（Shor）のアルゴリズムが挙げられる。前述のとおり、RSA 暗号は、素因数分解することが難しいことを安全性の根拠としている。ショアのアルゴリズムを利用することにより、素因数分解を現実的な時間で解くことが可能となり、RSA 暗号が安全でなくなることが知られている。

共通鍵暗号の解読に利用可能な量子アルゴリズムとしては、グローバー（Grover）のアルゴリズムとサイモン（Simon）のアルゴリズムが挙げられる。グローバーのアルゴリズムは、検索条件に合致するデータを探索するアルゴリズムであり、これを利用して共通鍵の全数探索を効率的に行う手法が知られている。また、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利用することにより、共通鍵を効率よく推測し、現実的な時間で解読できることが報告されている[9]。

各国の対応動向

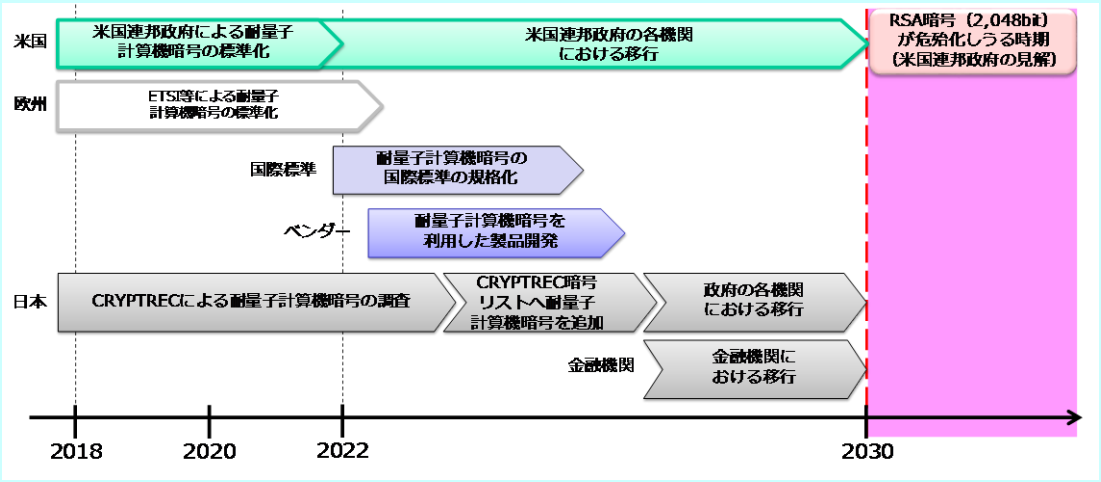
量子ゲート型コンピュータが暗号に及ぼす脅威への対応については、近年、各国で検討が進められている。

米国連邦政府は、RSA 暗号を数時間で解読できる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ている。そのうえで、2022 年頃までに、量子ゲート型コンピュータに耐性を有する公開鍵暗号（耐量子計算機暗号）の政府調達基準を策定し、現在使用している RSA 暗号等を、2026 年頃までに耐量子計算機暗号へ移行する計画を発表している[10]。

欧州では、近年、耐量子計算機暗号の標準化に向けた動きが活発化している。欧州電気通信標準化機構（European Telecommunications Standard Institute: ETSI）は、欧州の情報通信にかかる技術の標準化を進める団体であり、耐量子計算機暗号へ移行する際の留意点等に関する報告書を 2017 年に公表している。また、耐量子計算機暗号への移行スケジュールを検討することを目的とする作業部会を設置している。

わが国では、2017 年より、CRYPTREC 暗号リストの策定および管理を行っている CRYPTREC（総務省と経済産業省が共催しているプロジェクト）が、耐量子計算機暗号に関する学界の研究動向を調査しており、2018 年度末までに調査報告書を公表する予定である[11]。CRYPTREC 暗号リストは、金融機関が情報システムのセキュリティ対策を行う際の指針となる金融機関等コンピュータシステムの安全対策基準・解説書において、当該システムで利用する暗号を選定する際に参照することが推奨されている。今後、当該リストに耐量子計算機暗号を追加することが検討される可能性があり、その動きが注目される。

【図表 4】関係機関における対応スケジュールの一例



金融機関が今後検討すべき事項

量子ゲート型コンピュータの性能が向上すると、暗号の安全性低下を通じて金融サービスのセキュリティが低下することとなる。金融機関がこうした問題に円滑に対応していくためには、以下の 2 点について検討を進める必要があると考えられる。

1 つは、量子ゲート型コンピュータの研究開発や対策技術（耐量子計算機暗号）等の動向について、暗号の移行に関連する外部組織（他の金融機関、政府機関、ベンダー等）と情報交換や議論を行うための連携体制を整備することである。一般に、耐量子計算機暗号等の新しい暗号が金融機関のシステムへ実装されるまでの流れは、以下のようになる（図表 4）。

① 政府機関と学界が連携したうえで、新しい暗号の安全性に関する評価や議論を行い、安全な方式やその利用方法についてのコンセンサスを確立する。
② 上記①で確立したコンセンサスに基づき、政府機関や各種標準化団体は、当該暗号の標準規格を策定する。
③ 上記②で策定された標準規格を参照したうえで、ベンダーは新しい暗号を利用した製品（ソリューション）の開発および提供を行う。
④ 金融機関は、システムの新規導入や更改の時期に合わせて、ベンダーが提供している新しい暗号の製品を当該システムへ実装する。

このように、金融機関が暗号の移行を検討する際には、関連するさまざまな外部組織と連携して対応スケジュール等を検討することが必要不可欠といえる。

もう 1 つは、上記の検討と並行して、自行内のシステムにおける暗号の移行にかかる検討を計画的に進めることである。具体的には、システムにおける暗号の利用個所を把握し、暗号の安全性低下によるリスクを分析したうえで、対策の優先順位を決定することが考えられる。さらに、システムの新規導入や更改を行う際には、当該システムのライフサイクルや用途等を考慮したうえで、必要に応じて暗号の移行等の対応を効率的に実施できるようなシステムの設計・実装を行うことが望ましい。

量子ゲート型コンピュータが暗号の脅威となる時期についてはさまざまな意見があり、その時期を正確に予測することが難しい。しかし、上記の 2 つの対応には相応の時間を要すると考えられる[1][2]。そのため、量子ゲート型コンピュータが暗号の脅威となる時期を正確に予測できるようになってから対応に着手するのではなく、余裕を持って対処できるように、予め検討を進めておくことが重要であろう。

[1] 量子力学とは、物質の構成単位である原子の内部構造のような極めて微細な世界における物理現象を対象とする物理学の研究分野の 1 つである。

[2] この数学的問題（素因数分解問題と呼ばれる）は、桁数の大きな（現時点では、10 進数で 600 桁程度）素数を利用することにより、スーパーコンピュータを用いたとしても効率よく解けないことが知られており、RSA 暗号の安全性の根拠となっている。RSA

暗号の詳細については、例えば、清藤武暢・四方順司、「公開鍵暗号を巡る新しい動き:RSA から楕円曲線暗号へ」(『金融研究』、第 32 巻第 3 号、2013 年、17～50 頁）を参照されたい。

[3] 共通鍵暗号の仕組みや安全性の詳細については、清藤武暢・四方順司、「量子コンピュータが共通鍵暗号の安全性に与える影響」（『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』、No.2018-J-2、日本銀行金融研究所、2018 年）や、金子敏信、「共通鍵暗号の安全性評価」（『Fundamental Review』、Vol.7(1)、電子情報通信学会、2013 年、14～29 頁）を参照されたい。

[4] カナダのディー・ウェーブ（D-Wave）社が商用化し、2011 年から販売を開始している量子コンピュータは、量子アニーリング型コンピュータに分類される。

[5] 詳細については、例えば、Kelly, Julian, "A Preview of Bristlecone, Google's New Quantum Processor,"（Google Research Blog, Google, 2018）を参照されたい。

[6] 詳細については、例えば、Gil, Dario, "The future is quantum,"（IBM Research, 2017)を参照されたい。

[7] 詳細については、Intel Corporation, "2018 CES: Intel Advances Quantum and Neuromorphic Computing Research,"(Newsroom, 2018) を参照されたい。

[8] 詳細については、Linn, Allison,"The future is quantum: Microsoft releases free preview of Quantum Development Kit,"(The AI Blog, Microsoft, 2017)を参照されたい。

[9] サイモンのアルゴリズムは、関数の周期を探索する量子アルゴリズムである。一部の共通鍵暗号は、共通鍵が周期となる関数に変換し、現実的な時間で解読できるため、これらの方式は安全ではなくなることとなる。なお、それ以外のアルゴリズムを含め量子アルゴリズムの詳細については、例えば、清藤武暢・四方順司、「量子コンピュータが共通鍵暗号の安全性に与える影響」(『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』、No.2018-J-2、日本銀行金融研究所、2018 年）を参照されたい。

[10] この計画の一環として、米国内で利用する技術に関する標準化を担当する米国立標準技術研究所では、連邦政府で使用する耐量子計算機暗号の標準化活動を推進している。具体的には、2017 年 11 月末までに標準化候補となる耐量子計算機暗号の募集を行い、その後、3 年から 5 年かけて安全性、効率性や実装性等の観点からの評価を行ったうえで標準化する方式を決定するというプロセスで進めていくことを予定している。

[11] 詳細については、情報通信研究機構・情報処理推進機構、「CRYPTREC シンポジウム配付資料」(2017 年）を参照されたい。

[12] 金融分野等のさまざまな分野では、利用する共通鍵暗号について、安全性が低下している方式（Triple DES）から AES への移行を推進しているが、この移行には 10 年以上を要している。そのため、新しい暗号に完全に移行するためには 20 年から 30 年程度の期間を要するとの見方もある。詳細については、伊藤忠彦、「量子コンピュータが公開鍵基盤に与える影響と対策」(『2018 年暗号と情報セキュリティシンポジウム予稿集』、電子情報通信学会、2018 年）を参照されたい。