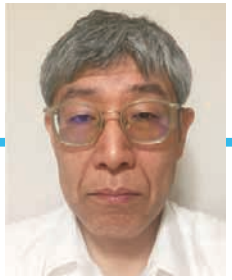
耐量子計算機暗号への移行に向けて何をすべきか？



日本銀行金融研究所　宇根（うね）　正志（まさし）

量子コンピュータに対しても安全な暗号アルゴリズムとして、耐量子計算機暗号（PQC：Post-Quantum Cryptography）のアルゴリズムの研究開発が活発化している。同時に、米国連邦政府は耐量子計算機暗号の標準化を進めている。本稿では、暗号アルゴリズムの安全性評価の現状、現在普及している暗号アルゴリズムに対して量子コンピュータが及ぼし得る影響を概観し、暗号アルゴリズムを使用するITシステムの運営者が今後の耐量子計算機暗号への移行に向けて何をすべきかを説明する。耐量子計算機暗号と米国連邦政府による標準化の動向については、本号収録の草川恵太氏の記事を参照されたい。本稿は、2022年4月28日時点の情報に基づいて執筆されたものであるほか、本稿で示されている意見は筆者個人に属し、日本銀行の公式見解を示すものではないことを予め断っておく。

1. 情報通信インフラを担う暗号アルゴリズムとその安全性評価

暗号アルゴリズムは、インターネットなどのオープンなネットワーク上でデータを安全に通信するために欠かせない存在となっている。これを実装するハードウェア（パソコン、スマートフォン、ICカード）も、「安全性が高い」と専門家が評価した暗号アルゴリズムを動作させることができるよう発展してきた。オンラインでの会議やショッピング、インターネット・バンキングやスマートフォン決済などでは、パソコンなどの暗号の機能を用いて、通信相手を認証したり、個人の属性データや金融取引に関するデータなどを秘匿して送信することが一般化している。インターネット上で重要なデータを安心して通信できるのは暗号アルゴリズムのおかげといっても過言ではない。

もっとも、暗号アルゴリズムの安全性は不変ではなく、経年劣化する点に注意が必要である。暗号アルゴリズムの安全性は、暗号化されたデータを解読するのに要する時間や費用の見積りに基づいて評価される[1]。暗号解析技術や計算技術は時間とともに進化し、コンピュータの性能は向上する。それに伴って暗号解読に要する時間や費用が低下するため、暗号アルゴリズムの安全性も低下していく。

こうした特性ゆえに、ITシステムの運営者は、暗号アルゴリズムの脆弱性や解読手法、コンピュータの性能向上など、安全性の低下につながり得る事象を絶えずウォッチし、現在使用している暗号アルゴリズムに及ぼす影響を評価しなければならない。評価の結果、安全性が低下した、または、近い将来低下するおそれがあると判明した場合、ITシステムやサービスへの影響を評価し対策を講じることになる。

暗号アルゴリズムの脆弱性や解読手法による影響の分析には、高度なスキルが要求され、専門家でないと難しい。我が国では、政府向けの暗号アルゴリズムの評価・選定を、暗号アルゴリズムの専門家によって構成されているCRYPTRECが担っている。CRYPTRECは、安全性や実装性能が優れた暗号アルゴリズムを評価・選定し「CRYPTREC暗号リスト」として公表しているほか、安全性が低下したものについても随時情報を公開している。金融機関をはじめとする民間部門も、自社のITシステムで使用する暗号アルゴリズムを選定したり安全性を評価したりする際に、CRYPTRECからの情報を活用することができる。

2. 量子コンピュータによる暗号アルゴリズムの安全性低下とその影響

暗号アルゴリズムの安全性の先行きに関して近年注目を集めているのが、量子コンピュータによる暗号解読の可能性である。量子コンピュータは、量子力学の原理を用いて実現されるコンピュータの総称である。スーパー・コンピュータでも解くことが難しい問題の解の候補を高速に求めることができるなど、産業界の様々な課題への応用が期待されている。もっとも、暗号アルゴリズムへの影響という点では、現在普及している主要な暗号アルゴリズムが量子コンピュータによって解読される可能性が懸念されている[2]。

量子コンピュータによる安全性低下の影響が大きいとみられているのは、RSA暗号や楕円曲線暗号である。これらは、通信相手の認証（なりすまし対策）、通信データの一貫性の確認（データの改ざん対策）、大きなデータを暗号化するための暗号鍵の共有（データの盗聴対策）の機能を果たす手段として極めて広範に普及している。代表的な暗

号通信プロトコルであるTLS（Transport Layer Security）をはじめ、数多くの国際標準や技術仕様に採用されているほか、CRYPTREC暗号リストにも含まれている。

一方で、RSA暗号や楕円曲線暗号の安全性のベースとなっている数学の問題を、量子コンピュータによって高速に解くためのアルゴリズムが既に提案されている[3]。こうしたアルゴリズムを理論どおり動作させることができれば、RSA暗号や楕円曲線暗号はもはや安全とはいえなくなる。ITシステムの運営者は、量子コンピュータに対しても安全な暗号アルゴリズム、すなわち、耐量子計算機暗号に移行せざるを得なくなるであろう。では、暗号アルゴリズムの移行にあたって、何を、いつ、行えばよいのであろうか？

3. 暗号アルゴリズムの移行にあたって何を実施するか

ITシステムの運営者は、まず、現在使用している暗号アルゴリズム（以下、現行アルゴリズム）の状況を把握する必要がある。把握すべき情報としては、例えば、以下が含まれる。

① 現行アルゴリズムを特定する情報（名称、用途、パラメータ〈例：鍵のサイズ、平文・暗号文のサイズ〉、暗号処理を実行するソフトウェア／ハードウェア〈暗号ライブラリなど〉）
② 暗号化対象データに関する情報（当該データの内容、用途、保存期間〈データが暗号化されてから破棄されるまでの期間〉など）
③ セキュリティ要件（想定する攻撃方法〈適応的選択暗号文攻撃など〉、達成すべき安全性レベル〈識別不可能性など〉）
④ 性能要件（暗号処理速度、通信速度、通信データ・サイズ、準拠する技術仕様など）
⑤ 動作環境（現行アルゴリズムと連動して動作するソフトウェア、OSなど）

次に、現行アルゴリズムが解読されたときにどのような影響がITシステムやそれを用いたサービスに及ぶかを評価する。例えば、暗号化されたデータの解読、データの改ざんやなりすましが発生すると、それに伴ってITシステムの稼働やサービスの提供が阻害される可能性がある。このようにITシステムの稼働が阻害されるなどの問題が実際に発生するか否かを各アルゴリズムに関して評価し、「問題が発生する」との結果が得られたアルゴリズムを移行対象とする。

移行対象と判断された現行アルゴリズムについては、移行先となる耐量子計算機暗号のアルゴリズムと、それを動作させるソフトウェア（暗号ライブラリなど）やハードウェア（専用プロセッサなど）を選定する。アルゴリズムの選定では、米国の国立標準技術研究所（NIST：National Institute of Standards and Technology）が進めている標準化の候補アルゴリズムが有力である。標準化は2022～2024年に完了する予定であるが、候補アルゴリズムを前提とした技術仕様の策定[4]や暗号ライブラリの開発・テスト[5]が民間技術者らによって既に開始されており、候補アルゴリズムを実装する環境の整備も並行して進められている。

耐量子計算機暗号のアルゴリズムやソフトウェアなどを選定し終えたら、ITシステムに組み込む際に必要となる改修の範囲と内容を検討し、システム改修の計画を立案して実行することとなる。

4. 暗号アルゴリズムの移行にいつ着手するか

暗号アルゴリズムの移行にかかる作業は、「暗号解読に使用できる量子コンピュータが実現し得る時期」（暗号解読時期）より前に完了させる必要がある。したがって、暗号解読時期を見積もると同時に、「現行アルゴリズムの使用状況の把握に着手してから、現行アルゴリズムによって暗号化されたデータすべての保存期間（暗号による秘匿が必要とされる期間）が終了するまでの期間」（暗号化データ保護期間）を見積もることが求められる。例えば、暗号解読時期を2040年頃、暗号化データ保護期間を12年と見積もった場合、遅くとも「2028年（＝2040年－12年）」には移行に着手する必要があることが分かる。

暗号解読時期については、専門家の間で様々な意見がある。NISTは、2016年4月にレポート[6]を発表し、「2030年までに、（2000ビット程度の鍵サイズの）RSA暗号を数時間で解読する性能を持つ量子コンピュータを約10億ドルで構築できるようになる可能性を指摘する専門家もいる」として、今後10年足らずで暗号解読時期の到来を指摘する見方を紹介している。他方、CRYPTRECは、2020年2月に、「現在の量子コンピュータの開発状況を踏まえると、暗号解読には規模の拡大だけでなく量子誤り訂正などの実現が必要であるため、CRYPTRECとしては、CRYPTREC暗号リスト記載の暗号技術が近い将来に危殆化する可能性は低い」としている[7]。もっとも、「革新的な技術の発展などにより、量子コンピュータで暗号解読を実現する可能性は否定できません」としており、暗号解読時期が早まる可能性

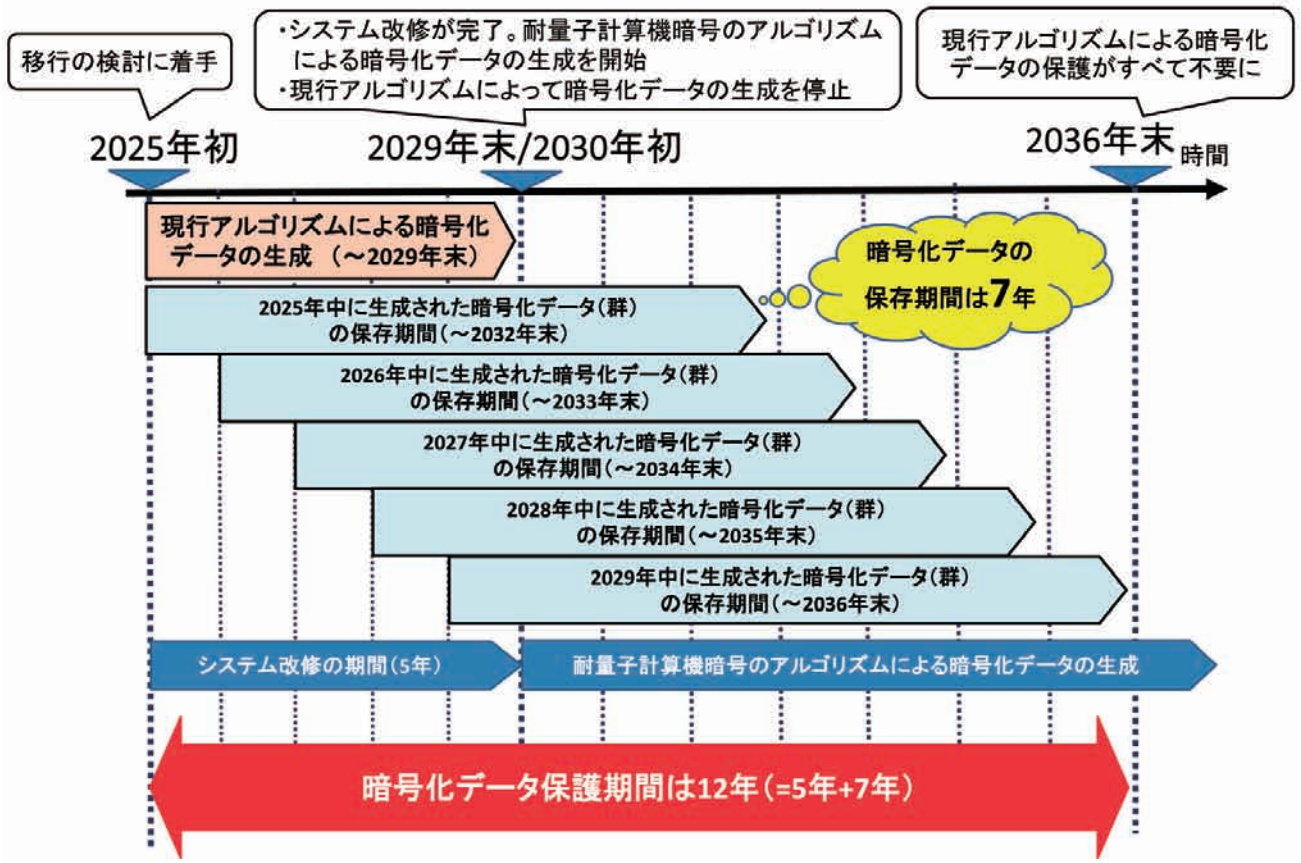
も示唆している。ITシステムの安全性を重視するという方針であれば、NISTのように、比較的早期に量子コンピュータによる暗号解読が実現するシナリオに焦点を当てて暗号解読時期を見積もるという方法もある。

もう一つの論点である暗号化データ保護期間は、現行アルゴリズムによって暗号化されたデータの解読を防ぐ必要がある期間全体を指す[8]。例えば、あるITシステムにおいて移行の検討に2025年初に着手し、5年間のシステム改修を経て、2030年初に耐量子計算機暗号のアルゴリズムによる暗号化データの生成を開始したとする(図を参照)。また、現行アルゴリズムによる暗号化データの生成は、システム改修完了の直前まで続き、2029年末に終了したとする。暗号化データの保存期間が7年であったとすると、現行アルゴリズムによる最後の暗号化データは2036年末（=2029年末+7年）まで保護することになる。この例の場合、暗号化データ保護期間は2025年初から2036年末までの期間であり、おおむね12年（=5年〈システム改修の期間〉+7年〈暗号化データの保存期間〉）となる。

システム改修の期間や暗号化データの保存期間は個々のITシステムによってまちまちである。ITシステムの運営者は、システム改修の計画を立案する過程でシステム改修の期間や暗号化データの保存期間を検討し、暗号化データ保護期間を見積もることとなる。そして、暗号解読時期の見積りの結果を考慮して、実際のシステム改修にいつ着手するかを決定することになろう。

5. おわりに

本稿執筆時点では、NISTによる耐量子計算機暗号の標準化は進行中であり、そうしたアルゴリズムを実装したソフトウェアやハードウェアはまだ入手可能にはなっていない。もっとも、将来の移行に向けた準備として、ITシステムにおける現行アルゴリズムの使用状況を調査したり、現行アルゴリズムが解読された場合の影響を評価したりすることは可能である。量子コンピュータによって現行アルゴリズムが解読されるという事象は、現時点ではテールリスクであるといえよう。しかし、量子コンピュータの研究開発



■図．暗号移行着手から暗号化データの保護が終了するまでの流れ（イメージ）

が今後急速に進展する可能性は否定できない。現行アルゴリズムの解読による影響が大きく、テールリスクを考慮する必要があるようなITシステムにおいては、量子コンピュータの研究開発動向、NISTによる耐量子計算機暗号の標準化動向などを、NISTやCRYPTRECの情報を参考にしながらフォローしつつ、現行アルゴリズムの安全性を巡る情勢が急激に変化したとしても迅速に対応できるよう、現行アルゴリズムの使用状況の調査など、着手できる準備作業に早めに着手しておくことが重要である。

参考文献

［1］宇根他：「暗号ユーザーが暗号アルゴリズムの安全性評価結果をどう活用するか」，金融研究，第29巻，第2号，pp.201-228（2010）

［2］宇根・菅：「量子コンピュータ開発の進展と次世代暗号」，金融研究，第40巻，第4号，pp.55-96（2021）

［3］四方：「量子コンピュータの脅威を考慮した高機能暗号：格子問題に基づく準同型暗号とその応用」，金融研究，第38巻，第1号，pp.73-96（2019）

［4］Stebila, D. et al.：“Hybrid Key Exchange in TLS 1.3, Draft-Ietf-Tls-Hybrid-Design-02”, Internet-Draft, IETF（2021）

［5］Paquin, C. et al.：“Benchmarking Post-Quantum Cryptography in TLS”, Proc. of Conference on Post-Quantum Cryptography 2020, LNCS 12100, Springer, pp.72-91（2020）

［6］Chen, L. et al.：“Report on Post-Quantum Cryptography”, NISTIR 8105, NIST（2016）

［7］CRYPTREC暗号技術評価委員会：「現在の量子コンピュータによる暗号技術の安全性への影響」，CRYPTREC ER-0001-2019（2020）

［8］伊藤：「量子コンピュータが公開鍵暗号基盤に与える影響」，2018年暗号と情報セキュリティシンポジウム発表論文，3A3-6（2018）