IMES DISCUSSION PAPER SERIES

量子コンピュータによる脅威を見据えた暗号の移行対応

伊藤忠彦・宇根正志・清藤武暢
（いとうただひこ　うねまさし　せいとうたけのぶ）

Discussion Paper No. 2019-J-15

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

IMES Discussion Paper Series 2019-J-15
2019 年 8 月

量子コンピュータによる脅威を見据えた暗号の移行対応

伊藤忠彦(いとうただひこ)*・宇根正志(うねまさし)**・清藤武暢(せいとうたけのぶ)***

要　旨

近年、量子コンピュータの研究開発が活発化しており、その処理性能が向上し続けている。量子コンピュータの処理性能が一定レベルを超えると、現在広く利用されている暗号（公開鍵暗号や共通鍵暗号）の安全性が低下しうることが知られている。暗号は、金融サービスのセキュリティを支える基盤技術として活用されており、今後、金融機関は、暗号の移行等、安全性低下への対応を検討する必要がある。本稿では、量子コンピュータが暗号の安全性へ与える影響について概説するとともに、金融機関の情報システムで利用される暗号を移行するうえでの留意点等について考察する。

キーワード: 暗号の移行、共通鍵暗号、公開鍵暗号、耐量子計算機暗号、
量子コンピュータ

JEL classification: L86、L96、Z00

*　セコム株式会社 IS 研究所（E-mail: tadahi-ito@secom.co.jp）
**　日本銀行金融研究所企画役（E-mail: masashi.une@boj.or.jp）
***　日本銀行金融研究所主査（E-mail: takenobu.seitou@boj.or.jp）

本稿の作成に当たっては、国立研究開発法人産業技術総合研究所サイバーフィジカルセキュリティ研究センターの時田俊雄氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行あるいはセコム株式会社の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。本稿は 2019 年 8 月 15 日時点までの情報をもとに作成されている。

目 次

１．はじめに

金融分野では、各種取引のセキュリティを確保するための基盤技術として、暗号（公開鍵暗号や共通鍵暗号）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は、顧客の端末と金融機関のホスト・コンピュータの間でやり取りされるデータ（暗証番号や取引内容等）の盗聴や改変の防止に暗号が利用されているほか、ATM や POS 端末を介した金融取引における IC カード（クレジットカード等）の真正性確認等にも暗号が利用されている。

こうしたなか、量子力学の性質を演算処理に利用した量子コンピュータ（特に、量子ゲート型コンピュータ）の研究開発が、近年活発化している。量子ゲート型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だけでなく、一部の暗号については現実的な時間で解読しうることが知られている（Shor [1994, 1997]、Bennett *et al.* [1997]、Brassard, HØyer, and Tapp [1998]等）。現時点では、量子ゲート型コンピュータによる既存の暗号への脅威が顕在化する時期は明確になっていないものの、そうした暗号の安全性が低下すると、多くの金融サービスに大きな影響を及ぼす可能性があると考えられる。

金融機関は、このような暗号の安全性低下が金融サービスに及ぼす影響を把握したうえで、金融サービスのセキュリティを確保するために、暗号の移行等を検討する必要がある。金融機関では、新しい暗号を金融サービスに利用する場合には、重要度の低いものから高いものへ順番に対応することが一般的であり、システムの重要度に応じて段階的に移行を進めることになると予想される。こうした事情を踏まえると、金融機関における情報システムの暗号の移行には、相応の期間を要すると考えられる。そのため、量子ゲート型コンピュータによる暗号への脅威が顕在化する時期を予測できるようになってから対応を開始するのではなく、余裕を持って対応できるように、予め検討を進めておくことが重要である。

このような問題意識に基づき、本稿では、量子ゲート型コンピュータが暗号の安全性へ与える影響について概説するとともに、金融機関の情報システムで利用される暗号を移行するうえでの留意点等について考察する。まず、2 節では、量子ゲート型コンピュータが暗号の安全性へ与える影響を説明する。続いて、3 節では、暗号の移行プロセスにおける問題を説明し、4 節では、3 節で示した問題への対応について検討する。最後に、5 節で金融機関における対応の留意点を示して全体を締め括る。

２．量子コンピュータが暗号の安全性へ与える影響

（１）量子コンピュータ

近年、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の研究開発が活発化している。量子コンピュータは、一般に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大別される[1]。特に、量子ゲート型コンピュータについては、そ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に大きな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[2,3]。

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）を演算処理に利用する。スーパー・コンピュータ（古典コンピュータ）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する。一方、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を「量子ビット」と呼ぶ。量子ビットは、上記の重ね合わせ状態を利用することにより、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できる。そのため、量子ビットに対する 1 回の演算処理により、両方のデータに対して同時（並列的）に処理を実行できる。そして、量子ゲート型コンピュータで取り扱うことができる量子ビットの数が 2 倍や 3 倍に増加すると、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。このように、量子ビットの数が大きくなるにつれて、より大量のデータを同時に処理できるため、古典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。

（２）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用いて演算処理を行う場合には、量子アルゴリズムが必要となる。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、量子ビットに設定する確率を操作する手順である[4]。い

---

[1] 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いている。

[2] ハッシュ関数についても、量子ゲート型コンピュータにより（共通鍵暗号と同程度に）安全性が低下することが知られている。こうした状況を踏まえ、米国連邦政府はハッシュ関数を規定している標準規格の見直しを予定している（Moody [2018]）。

[3] 最近では、量子アニーリング型コンピュータを利用して素因数分解問題を解く研究が報告され始めている（Jiang *et al*. [2018]、清水ほか［2019］等）。もっとも、量子ゲート型コンピュータと比較して相対的に研究成果が少ないため、本稿では量子ゲート型コンピュータに焦点を当てることとする。

[4] 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、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。どのデータに変換されるかは、量子ビットに設定する確率に依存する。

くつか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できることが知られている[5]。

公開鍵暗号については、RSA 暗号と楕円曲線暗号が代表的である。これらは、それぞれ素因数分解問題と楕円曲線上の離散対数問題の困難性を安全性の根拠とするものである[6]。これらの問題は、大規模な量子ゲート型コンピュータが実現した場合、ショアのアルゴリズム（Shor [1994, 1997]）によって現実的な時間で解くことが可能と考えられている。対策としては、量子ゲート型コンピュータを用いた攻撃手法に対しても安全な公開鍵暗号（耐量子計算機暗号）への移行が考えられる。

共通鍵暗号としては、AES（Advanced Encryption Standard）に暗号利用モードを組み合わせて利用されるケースが多い。AES を量子ゲート型コンピュータで攻撃する手法としては、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（Grover [1996]）が知られている。この攻撃への対策としては、鍵長を 2 倍程度伸長することが効果的と考えられている（Bennett *et al*. [1997]、Brassard, HØyer, and Tapp [1998]等）[7]。もっとも、鍵長を伸長しても、一部の暗号利用モードの場合、サイモンのアルゴリズム（Simon [1997]、Kuwakado and Morii [2010, 2012]、 Kaplan *et al*. [2016]、Anand *et al*. [2016]等）によって現実的な時間で探索できることが報告されている[8]。この攻撃への対策としては、サイモンのアルゴリズムに耐性のある暗号利用モードを利用することが考えられる。

このように、公開鍵暗号については、耐量子計算機暗号への移行が必要となり、共通鍵暗号については、鍵長を伸長するとともにサイモンのアルゴリズムに耐性を有する暗号利用モードに移行することが必要となる。

（３）金融サービスで利用されている標準規格への影響

金融サービスで利用されている公開鍵暗号と共通鍵暗号は標準規格等において規定されている。例えば、ISO 9564-1, 2 は、金融取引における本人確認用の暗証番号のセキュリティを確保するための仕組みを規定している（International

---

[5] 詳細については、清藤・青野・四方［2015］や清藤・四方［2019］を参照されたい。

[6] 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 を求める問題である。また、楕円曲線上の離散対数問題は、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。

[7] 探索する鍵候補の総数を 2^{100} としたとき、古典コンピュータを用いて正しい暗号鍵を探索する場合には最大で 2^{100} 回程度の処理が必要となるのに対し、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。

[8] サイモンのアルゴリズムは関数の周期を探索するアルゴリズムである。関数の周期とは、その関数について、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。探索する鍵候補の総数を 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。

Organization for Standardization [2014, 2017]）。ISO 16609 は、金融取引でやり取りされるデータにおける改変を検知するための仕組みを規定しているほか、ISO/TR 14742 は金融サービスでの利用を推奨する暗号を記載している（International Organization for Standardization [2010, 2012]）。RFC（Request for Comments）8446 は、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）によって策定された暗号通信プロトコル TLS（Transport Layer Security）の標準仕様であり、金融機関のオンライン・バンキングで利用されている（Rescorla [2018]）。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 仕様等も、公開鍵暗号や共通鍵暗号を規定している（EMVCo [2011]）。これらの規格は、今後、本節（2）で示した各種対策に沿って改訂されていくとみられる。

（４）移行に要する期間についての検討

量子ゲート型コンピュータへの対応を検討するうえで、それが暗号に対して現実的な脅威となりうる時期をどう予測するかが重要である。既存の公開鍵暗号を解読するためには、演算処理中の誤りを訂正する機能（誤り耐性）を有する量子ゲート型コンピュータを実現することが求められる。量子コンピュータに関する研究の第一人者であるウォータールー大学のミハエル・モスカ（Michel Mosca）は、2015 年の時点で、誤り耐性を有する量子ゲート型コンピュータが 2021 年頃に実現するとの見方を示している（Mosca [2015]）[9]。もっとも、誤り耐性を有する量子ゲート型コンピュータの実現時期については、専門家の間でもさまざまな意見があり、現時点ではコンセンサスが得られていない[10]。

誤り耐性を有する量子ゲート型コンピュータが実現されたタイミングから、当該コンピュータを用いて既存の暗号を現実的な時間で解読可能となる時期まで、最短で 10 年程度ではないかとの見方が示されている（Mosca [2018]）。そのため、誤り耐性を有する量子ゲート型コンピュータが実現されたタイミングを起点として暗号移行の検討を開始した場合、移行が完了する前に既存の暗号が解読されてしまう可能性がある。

これまで、金融分野を含むさまざまな分野では、利用する共通鍵暗号やハッシュ関数について、安全性が低下している方式（Triple DES、SHA-1）から安全性の高い方式（AES、SHA-2）への移行を経験しているが、移行に 10 年以上を

[9] 量子ゲート型コンピュータにおいては、データの入出力や演算処理を行う際に発生するノイズ等によって量子ビットの状態に影響が生じる。こうしたノイズによる演算処理の誤りを訂正しつつ量子ビットの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。

[10] 誤り耐性を有し、既存の暗号に対して現実的な脅威となりうる量子ゲート型コンピュータの実現時期については補論 1 を参照されたい。

要しているのが実情である（伊藤［2018a, b］）。また、米国の国立標準技術研究所（National Institute of Standards and Technology : NIST）や国家安全保障局（National Security Agency：NSA）は、連邦政府機関等で利用している大規模な情報システムにおいて、新しい暗号の実装に 20 年程度、機器の入替えを完了させるまでに 30 年以上を要する場合があるほか、情報システムにより生成されたデータを 30 年以上保護することが求められる場合があるとしている（National Institute of Standards and Technology [2016b]、National Security Agency [2016]）。こうした見方も踏まえると、米国の連邦政府機関等だけでなく、それら以外の大規模な情報システムにおいても、暗号の移行に 20～30 年を要する可能性がある。

（５）足許における暗号移行への対応

イ．各国政府機関等における動き

米国は、2016 年に連邦政府で利用する公開鍵暗号を 2026 年頃までに耐量子計算機暗号へ移行する計画を公表した。その一環として、NIST により耐量子計算機暗号の標準規格の策定が進められている（National Institute of Standards and Technology [2016a, 2019]、Chen [2017]、四方［2019］）。具体的には、2017 年 11 月末を期限に全世界から標準化候補の方式を募集し、最初の選考過程（第 1 ラウンド）を経た後、2019 年 1 月末より次の選考過程（第 2 ラウンド）が行われている。第 2 ラウンドの選考期間は、1 年から 1 年半程度を要することが想定されており、必要に応じて最終選考過程（第 3 ラウンド）を行った後、2022 年から 2024 年頃に標準規格が策定される予定である。

欧州連合においても、欧州電気通信標準化機構（European Telecommunications Standards Institute：ETSI）が耐量子計算機暗号への移行に関するロードマップの検討を進めているほか、耐量子計算機暗号の実装性能（処理性能や実装可能性等）を評価する作業部会の設置等も行っている（Pecen [2018]）[11]。

わが国では、暗号の安全性の評価・監視を行い「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」の策定および管理を行っている CRYPTREC が、耐量子計算機暗号に関する研究動向を 2017～18 年度に調査し、2019 年 4 月に調査報告書を公開した（CRYPTREC 暗号技術調査ワーキング・グループ［2019］）。また、2019 年度より、量子ゲート型コンピュータの動向を踏まえつつ、次期 CRYPTREC 暗号リストの要件や課題等を整理するためのタスクフォースが開催されている（情報通信研究機構・情報処理推進機構［2019］）。

[11] ETSI は、欧州における情報・電気通信・放送にかかる技術の標準化を推進する非営利組織である。

ロ．民間企業における動き

マイクロソフト社では、暗号ソフトウェアのオープンソース・ライブラリである OpenSSL、OpenSSH、OpenVPN への耐量子計算機暗号の採用に取り組んでいる[12]。これらの活動は、Open Quantum Safe （OQS）プロジェクトと呼ばれており、マイクロソフト社は、ベンダー（アマゾン社、エボリューションキュー＜evolutionQ＞社、エスアールアイ・インターナショナル＜SRI International＞社）や大学（ウォータールー大学）と連携して推進している（Open Quantum Safe [2018]、Crockett, Paquin, and Stebila [2019]）。暗号ハードウェアについても、公開鍵認証基盤（Public-Key Infrastructure：PKI）を実現するためのハードウェア・セキュリティ・モジュールの開発を進めている[13]。同社は、耐量子計算機暗号を実装する暗号ソフトウェア／ハードウェアの開発を 2021 年頃までに完了させた後、それらの導入や移行を開始し、2030 年頃までに移行を完了させるという見通しを示している。

フランスの IC チップ・ベンダーのジェムアルト（Gemalto）社では、次世代の IC チップ等に実装する公開鍵暗号として耐量子計算機暗号の採用を検討している（Gouget [2017]）。同社は、量子ゲート型コンピュータが暗号の脅威として顕在化した場合の影響は甚大であることから、予め対応する必要があるとの見解を示している。同社は、具体的な対応方法としてハイブリッド方式と呼ばれる実装に注目している。この方式は、現在広く利用されている既存の公開鍵暗号（RSA 暗号等）と耐量子計算機暗号をともに IC チップ上に実装し、将来、量子ゲート型コンピュータによる脅威が顕在化した場合には、（安全性が低下した）既存の公開鍵暗号の利用を停止して耐量子計算機暗号のみを利用するというアイデアに基づくものである[14]。

暗号の移行に関する検討を推進している関係機関（各国の政府機関、民間企業や標準化団体等）における対応スケジュールの一例を図表 1 にまとめる。金融機関が耐量子計算機暗号への移行を検討する場合には、関係機関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。

３．情報システムの構成とその移行プロセス

本節では、暗号アルゴリズムを実装する情報システムを想定し、暗号の移行プ

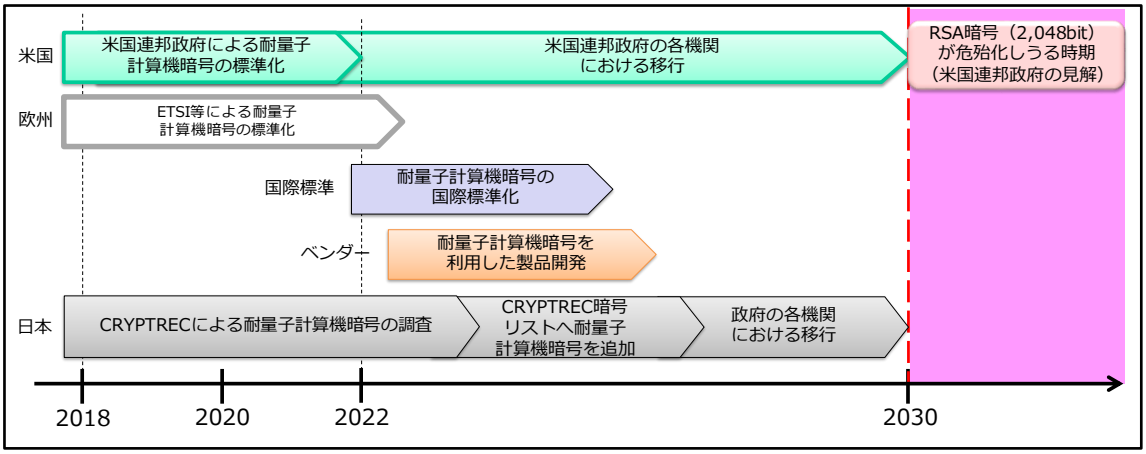
---

[12] OpenSSL は、暗号通信プロトコル SSL や TLS を実装するためのライブラリである。OpenSSH は SSH（Secure Shell）通信を実装するためのライブラリであり、OpenVPN は VPN（Virtual Private Network）を実装するためのライブラリである。

[13] PKI では、信頼される第三者である「認証機関」が、公開鍵とその所有者（の識別子）を紐付けるためのデータ（証明書記載情報）に、これらのデータの完全性を検証するためのデジタル署名を付加した「電子証明書」を生成し発行する。

[14] ハイブリッド方式は学界においても研究されており、例えば、ハイブリッド方式に基づく電子証明書の生成手法が提案されている（詳細は補論 2 を参照）。

図表 1　関係機関における対応スケジュールの一例



資料：清藤［2018］

ロセスの例を示すとともに、移行にかかる問題について検討する。

（１）検討対象とする情報システム

まず、検討対象とする情報システムは、一定の入力に対して予め決められた処理を実行し、その結果を出力するものとする（図表 2 を参照）。

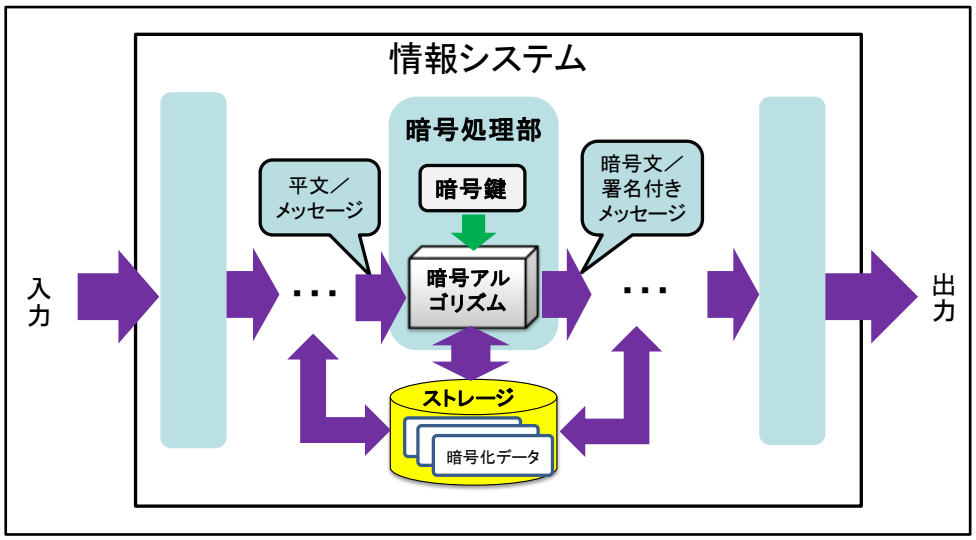
暗号処理を実行する部分（暗号処理部）においては、共通鍵暗号と公開鍵暗号による処理が実行されるとする。一般に、共通鍵暗号はデータの暗号化・復号や改変の検知に用いられるほか、公開鍵暗号はデジタル署名の生成・検証や共通鍵暗号で用いられる暗号鍵（秘密鍵）の配送に用いられることが多い。ここでは、暗号処理部への入力（平文あるいはメッセージ）を共通鍵暗号によって暗号化・復号するほか、公開鍵暗号によって署名を生成・検証するものとする。このようにして生成される暗号文と署名付きメッセージをまとめて「暗号化データ」と呼ぶ。

暗号処理部で生成された暗号化データは、暗号処理部から出力され、情報システム内部の他の処理部に送られるほか、後日の使用のために保管する場合には、ストレージに送られる。暗号文については、後日、平文の内容を参照する際にストレージから抽出され、暗号処理部において復号される。署名付きメッセージの場合には、暗号処理部において署名が検証され、その結果が出力される。

共通鍵暗号と公開鍵暗号は、暗号処理部において、それぞれ仕様通りに実装され、情報システム稼働中に改変されないと仮定する。暗号鍵（公開鍵暗号の場合には署名生成鍵）も、暗号処理部内において秘密に格納され、外部に漏えいすることはないとする[15]。

[15] 暗号アルゴリズムによる処理途中のハードウェアの動作から平文や暗号鍵を推定可能となる

図表２　情報システムの構成（概念図）



（２）暗号の移行プロセス

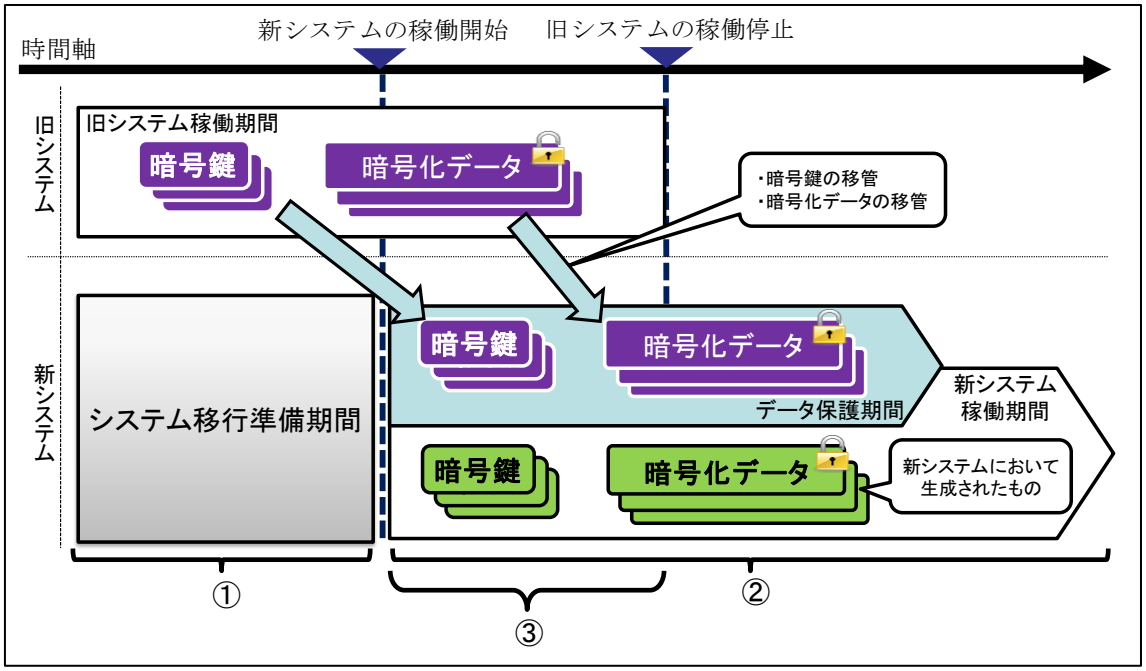
量子ゲート型コンピュータに対しても安全な暗号への移行では、既存の公開鍵暗号（RSA 暗号等）を耐量子計算機暗号に移行するとともに、既存の共通鍵暗号（AES 等）の鍵長を伸長することになる。以下では、既存の暗号が用いられる情報システムを「旧システム」と呼び、耐量子計算機暗号および鍵長伸長後の共通鍵暗号が用いられる新しい情報システムを「新システム」と呼ぶ。ここでは、新システムを旧システムとは別の情報システムとして構築するケースを想定する。こうした移行は、通常、システム移行の準備、新システムへの切替え、旧システムの暗号化データの保護という 3 つのフェーズから構成される（図表 3 を参照）。各フェーズの概要は以下のとおりである。

イ．システム移行の準備

まず、旧システムが稼働している期間（旧システム稼働期間）において、開発にかかる諸作業（企画検討、システム化計画立案、要件定義、設計、実装、テスト）を実施する。これらに要する期間を「システム移行準備期間（図表 3 中の①の期間）」と呼ぶ。また、旧システムのストレージに保管されている暗号化データの重要度や使用期間等を明確にして、新システムの稼働を開始する時点から（旧システムの）暗号化データの保護が終了する時点までの期間（データ保護期間）を設定する。

場合があり、そうした実装環境を保護することも求められるケースがある。ここでは、暗号移行の検討に焦点を当てるために、こうした保護が有効に実施されていると仮定する。

図表 3　情報システムの移行プロセス



ロ．新システムへの切替え

新システムの開発やデータ保護期間の設定が完了した後、旧システムと併用する形で新システムが稼動を開始するとともに、新システムへの切替えが進められる。ここで、新システムと旧システムが稼働する期間を、それぞれ「新システム稼働期間（図表 3 中の②の期間）」および「旧システム稼働期間」と呼ぶ。新システムが稼働を開始した時点から旧システム稼働期間が満了するまでの間（切替期間、図表 3 中の③の期間）、旧システムは、新しい暗号化データの生成とストレージへの保管を継続する。

切替期間において、新システムでは、耐量子計算機暗号や鍵長を伸長した共通鍵暗号が実装され、それらによって暗号化データの生成が行われる。同時に、旧システム内の暗号鍵と暗号化データを新システムに移管する作業が進められる。また、暗号化データを復号したり、署名を検証したりするためのハードウェアやソフトウェアも、新システムに移管されるとする。その際、暗号鍵や暗号化データが外部に漏えいすることはないと仮定する。切替期間が満了すると、旧システムは稼動を停止する[16]。

[16] 新システムへの切替えにおいては、旧システムから移管された暗号鍵を用いて（移管された）暗号化データの復号等を行った後、新システムの暗号アルゴリズムによって再暗号化（あるいは署名の再生成）を行う場合も想定される（詳細は後述）。もっとも、暗号化データが大量に存在する場合には、短期間に再暗号化等を完了させることができない可能性がある。

ハ．旧システムの暗号化データの保護

旧システムの稼働停止後、旧システムの暗号化データ（新システムに移管されたもの）は、新システムの一部として保護され、データ保護期間が満了するまでストレージから抽出されて使用される。データ保護期間が満了すると、暗号鍵、暗号化データ、それらを使用するためのハードウェア等が廃棄される。新システムにおいて新たに生成される平文やメッセージについては、耐量子計算機暗号等によって暗号化データが生成され、ストレージに保管される。

（３）移行プロセスにおいて想定される問題

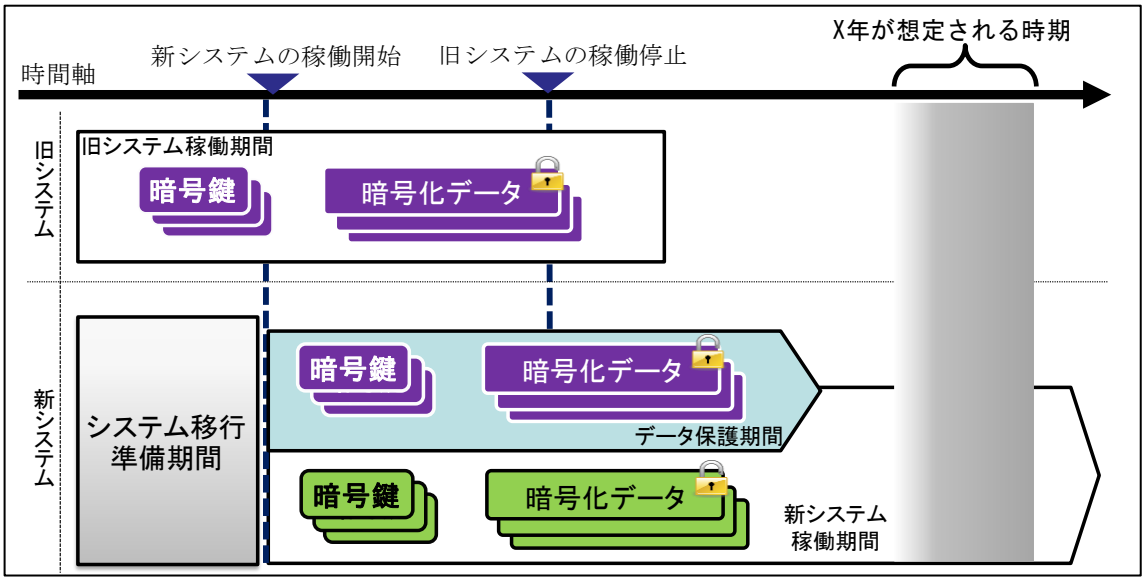
イ．理想的なケース

次に、量子ゲート型コンピュータによって既存の暗号を現実的な時間で解読可能となる時期を「X 年」としたうえで、上記の移行プロセスの各フェーズとの関係を整理する。理想的なケースは、X 年が到来すると想定される時期よりも前にデータ保護期間が満了するというケースである（図表 4 を参照）。もっとも、すべての情報システムにおける移行がこれに該当するとは限らない。例えば、X 年が想定される時期がシステム移行準備期間と重なるケース（ケース A）、切替期間と重なるケース（ケース B）、切替期間満了後のデータ保護期間と重なるケース（ケース C）がそれぞれ想定される。

ロ．ケース A の場合

X 年が想定される時期がシステム移行準備期間と重なるケースでは、X 年が想定される時期において新システムがまだ稼働しておらず、旧システムの暗号

図表 4　理想的な移行プロセス



処理部やストレージに存在する暗号化データが量子ゲート型コンピュータによる攻撃の対象となりうる（図表 5 を参照）。例えば、量子ゲート型コンピュータを使用できる攻撃者が、旧システムへの不正アクセス等によって、暗号処理部において生成された暗号化データやストレージに格納されている暗号化データを盗取・解読したり改変・偽造したりする可能性がある。特に、暗号処理部において生成され、その後、情報システム内部の他の処理部において処理される予定の暗号化データが不正に改変・偽造されてしまうと、情報システムの処理結果を信頼することができなくなるという問題につながる。

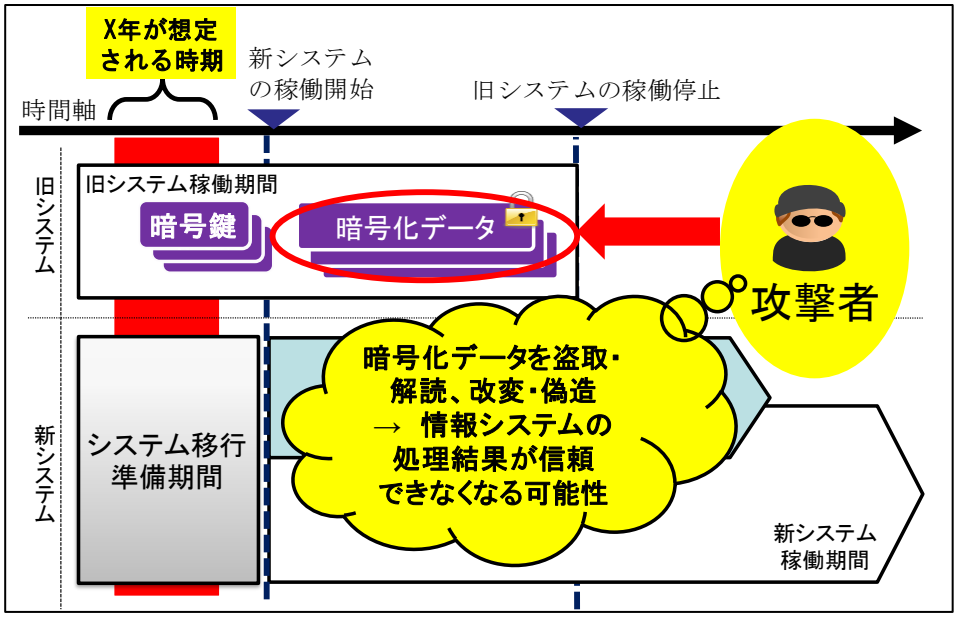
ハ．ケース B の場合

X 年が想定される時期が切替期間と重なるケースでは、ケース A と同様に、旧システムの暗号処理部やストレージに存在する暗号化データが量子ゲート型コンピュータによる攻撃の対象となる可能性がある（図表 6 を参照）。これに加えて、旧システムから新システムに移管された暗号化データの一部も攻撃の対象になりうる。このため、旧システムと新システムの両方で対応が必要となる。

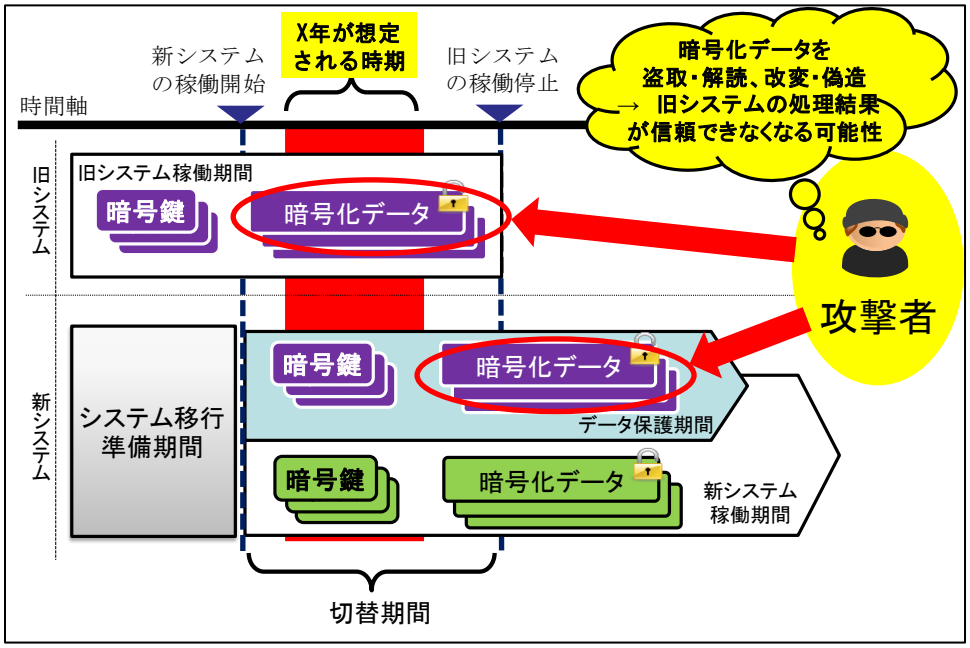
ニ．ケース C の場合

このケースでは、X 年が想定される時期において、旧システムが既に稼働を停止しており、新システムの一部として存在する（ストレージに格納されている旧システムの）暗号化データが攻撃の対象となりうる（図表 7 を参照）。新システムによって生成された暗号化データであれば、鍵長が伸長された共通鍵暗号や

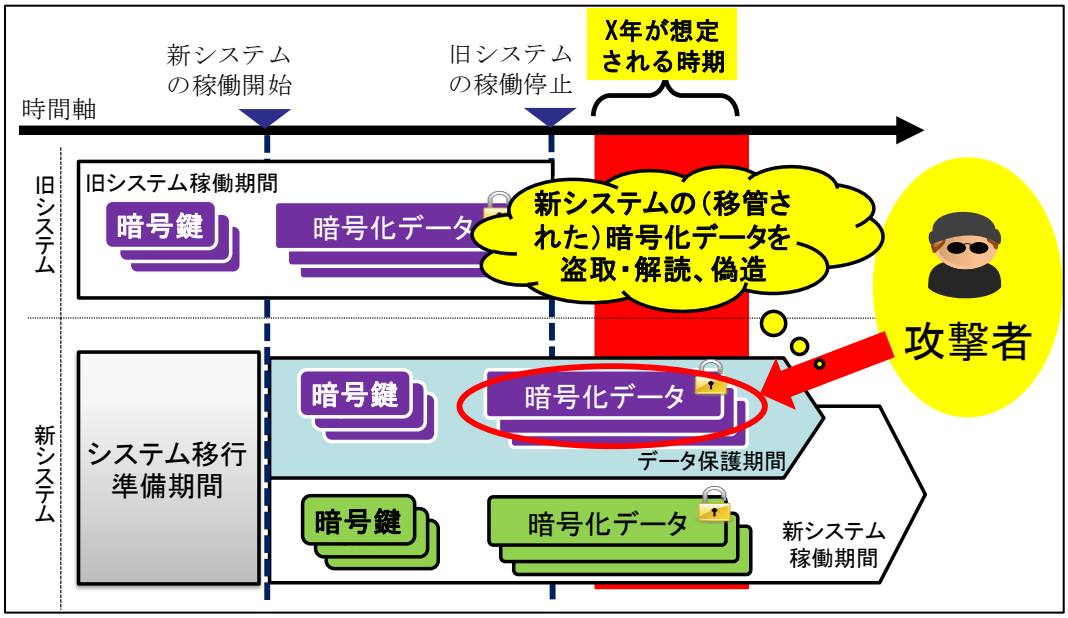
図表 5　ケース A：システム移行準備期間における攻撃



図表６　ケースＢ：切替期間における攻撃



図表７　ケースＣ：データ保護期間（切替期間後）における攻撃



耐量子計算機暗号が適用されていることから、量子ゲート型コンピュータを使用できる攻撃者であってもセキュリティを確保できる。

４．移行プロセスにおける問題への対応

3 節（3）で整理した 3 つのケースにおける問題への基本的な対応は、いずれも、システム移行準備期間、切替期間、データ保護期間を可能な限り短縮し、X

年が到来すると想定される時期をデータ保護期間満了後とすることである。もっとも、大規模な開発を伴う情報システムや他の複数の情報システムと連動して稼動する情報システムの場合では、これらの期間を十分に短縮させることができず、何らかの追加的な対応が必要となる場合が想定される。本節では、各期間の短縮や追加的な対応策の候補について説明する。

（１）システム移行準備期間や切替期間の短縮

問題への対応を検討するうえで、データ保護期間が必要最小限に設定されていることが前提となる。データ保護期間は、通常、暗号化データの使用目的（例えば、署名付きメッセージの有効期間）等によって予め決定されているケースが多く変更の自由度が低いと考えられる。ただし、旧システムにおいて、実際には短期間のみ使用するにもかかわらず長期間のデータ保護期間が設定されている場合があるならば、そのデータ保護期間を必要最小限に設定し直すという対応が求められる。

そのうえで、情報システムの設計時に、暗号移行に伴うシステム移行準備期間や切替期間を短縮する仕掛けを組み込んでおくことが考えられる。こうした設計思想は「クリプト・アジリティ」（crypto agility）と呼ばれている。クリプト・アジリティによる設計上の主な留意事項として、以下が知られている（Housley [2015]、National Institute of Standards and Technology [2016a]、Langley *et al.* [2017]）。

① 情報システムの開発の初期段階（企画検討、システム化計画立案、要件定義）において、暗号処理部を情報システムの他の処理部から物理的に独立させるようにする。

② 暗号処理部における暗号アルゴリズムの実装形態として、無線通信等を用いて更新可能な形態（ソフトウェア等）を採用する。

③ 旧システムと新システムの間で互換性（同じ種類のモジュールを利用可能にするなど）を確保する。

こうした事項を予め考慮して設計することにより、旧システムの（暗号処理部以外の）他の処理部やストレージをそのまま活用しつつ、暗号処理部のみを更新することで新システムを実現するという方法が考えられる。その結果、システム移行準備期間と切替期間の両方が短縮可能になると期待される。

もっとも、既存の情報システムでは、クリプト・アジリティを考慮しておらず、暗号処理部のみを更新することは容易でなく、暗号の移行を新システムへの切換えのタイミングで実施することが多い。そうした情報システムに関しては、将

来の暗号の移行に備えて、ハードウェアやソフトウェアのサポート切れ対応等を契機にシステムの更改を実施する際に、クリプト・アジリティの設計思想を適用することが考えられる。

また、暗号の移行に際して、情報システム自体に加えて、そのユーザーが所持する機器（PC、スマートフォン、IC カード等）で用いられる暗号（特に公開鍵暗号）の移行やソフトウェアの更新を円滑に実施することが求められる場合も想定される。こうした場合には、「セキュリティ・アジリティ」（security agility）の設計思想を適用することが有用である。セキュリティ・アジリティは、クリプト・アジリティを一般化した概念であり、（情報システム内部の）暗号処理部のみならず、情報システムとその周辺環境全体を対象としたセキュリティ確保を目標としている。

（２）期間を十分短縮できない場合の対応

クリプト・アジリティの考え方に基づいて予め情報システムを更改したとしても、情報システムの特性（規模や他の情報システムとの連携等）や移行プロセスにおける作業遅延（システム移行準備に携わる人員の不足等）によって、十分に期間を短縮できない場合がありうる。以下では、署名付きメッセージと暗号文に分けて対応を考察する。3 節（3）で整理した各ケースごとに求められる対応を予め図表 8 にまとめる。

イ．署名付きメッセージの保護にかかる対応

署名付きメッセージを保護する方法としては、タイムスタンプ局を利用して、ストレージに保管されている署名付きメッセージに耐量子計算機暗号ベースの

図表 8　各ケースにおいて求められる対応

<table>
<tr><th rowspan="2">保護対象</th><th rowspan="2">ケース</th><th colspan="2">旧システムにおける対応</th></tr>
<tr><th>ストレージのデータ</th><th>暗号処理部のデータ</th></tr>
<tr><td rowspan="3">署名付き
メッセージ</td><td>A</td><td>タイムスタンプ局の利用</td><td rowspan="2">アクセス制御の強化</td></tr>
<tr><td>B</td><td rowspan="2">タイムスタンプ局の利用、あるいは新システムにおける署名の付与</td></tr>
<tr><td>C</td><td></td></tr>
<tr><td rowspan="3">暗号文</td><td>A</td><td colspan="2">アクセス制御の強化</td></tr>
<tr><td>B</td><td>アクセス制御の強化、あるいは鍵長を伸長した共通鍵暗号により再暗号化</td><td>アクセス制御の強化</td></tr>
<tr><td>C</td><td colspan="2">アクセス制御の強化、あるいは鍵長を伸長した共通鍵暗号により再暗号化</td></tr>
</table>

タイムスタンプ署名等を付与する方法と、処理途中の署名付きメッセージ（ストレージに格納される前のもの）をアクセス制御の強化によって保護する方法が考えられる。

（イ）タイムスタンプ局の利用

ストレージに保管されている署名付きメッセージは、後日、それと電子証明書（公開鍵を含む）を他のユーザー等に示し、メッセージの内容とその完全性を証明するために用いられる。したがって、他のユーザー等が攻撃者となり、（攻撃対象の）署名付きメッセージを入手することを前提とした対応が必要となる。また、コストの観点からは、旧システムや新システムにおける署名付きメッセージの保護には、情報システムへの追加的な対応対応をなるべく行わない手法が望ましい。特に、旧システムは、先行き稼働を停止することから、実務上、新たなシステム対応を回避することが求められる場合が多いと考えられる。

こうした状況で有効と考えられるのは、外部のタイムスタンプ局（正確な時刻を取得可能な信頼できる第三者機関）が提供するタイムスタンプ署名の活用である。タイムスタンプ署名は、メッセージがある特定の時刻に存在していたこと、および、その時刻以降に当該メッセージが変更されていないことを検証するために生成されるデジタル署名であり、メッセージと時刻情報に対して生成される（図表 9 を参照）[17]。タイムスタンプ署名を付与されたメッセージは、一定期間が経過した後（または任意のタイミングで）、新たなタイムスタンプ署名を再度付与することによって、メッセージの完全性を中長期的に確保することも可能となる[18]。

タイムスタンプ局の利用は、情報システム側での追加的なシステム対応がほぼ不要になると考えられることから、特に、旧システムのみが稼働しているケース A における対応を検討する際に参考になる[19]。すなわち、旧システムの署名付きメッセージ（群）をタイムスタンプ局に送信し、耐量子計算機暗号によるタイムスタンプ署名が付与された（署名付き）メッセージをタイムスタンプ局から取

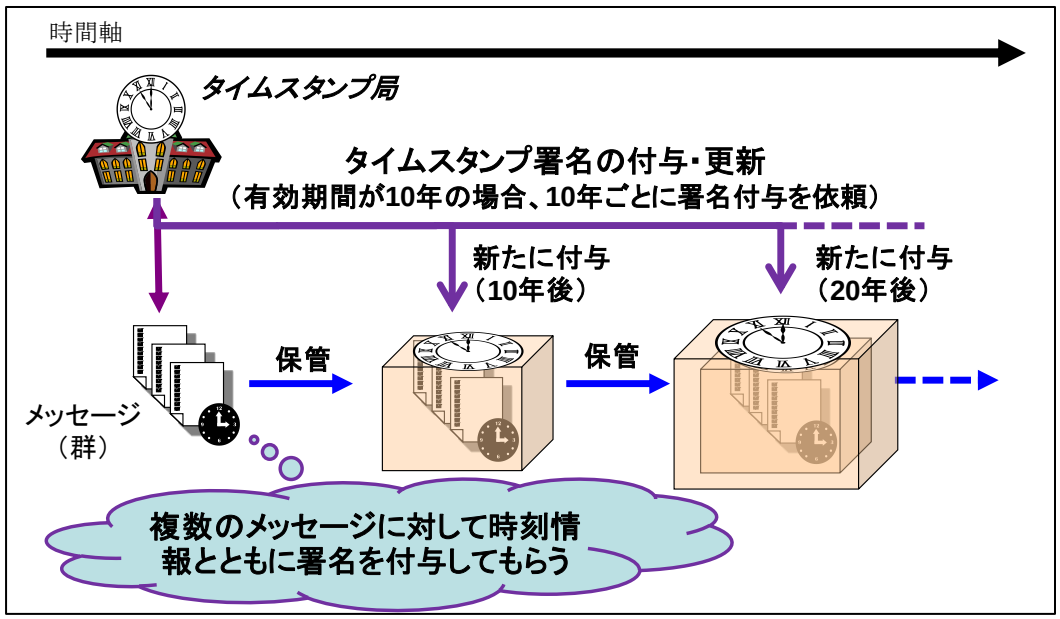
---

[17] タイムスタンプ局には、メッセージのハッシュ値が送信される。このため、メッセージの機密性を確保しつつ、タイムスタンプ署名を得ることができる。

[18] こうした目的を実現するためのデータ形式として、近年、エビデンス・レコード・シンタックス（Evidence Record Syntax : ERS）が提案されており、RFC4998 として標準化されている（Gondrom, Brandner, and Prodesch [2007]）。ERS は、タイムスタンプ署名に設定される有効期間を更新する機能や、（それらの署名を生成・検証するための）公開鍵暗号の鍵ペアを更新する機能を有する仕様となっている。また、大量のメッセージに対してタイムスタンプ署名を効率的に付与するために、ERS では、ハッシュ関数を用いて複数のメッセージを少数のハッシュ値に集約するという方法も規定されている。

[19] ERS に基づくタイムスタンプ署名を得るためには、メッセージの形式を ERS に基づく形式に変換する必要があり、そのためのシステム対応のコストが発生する。

図表 9　タイムスタンプ局によるタイムスタンプ署名の付与と更新（イメージ）



得するというものである。コスト抑制の観点からは、量子ゲート型コンピュータによる脅威が顕在化するタイミングをある程度予測可能となるまでは従来の署名付きメッセージを保管・使用し、顕在化するタイミングを予測可能となった時点で、タイムスタンプ局の利用を開始することが望ましい。

（ロ）新システムにおける署名の付与

新システムが稼働しているケース B とケース C では、タイムスタンプ局の利用だけでなく、新システムにおける（耐量子計算機暗号による）署名生成の機能を活用するという選択肢もある。例えば、旧システムの署名付きメッセージを新システムに入力し、新システム内の暗号処理部において新たに署名を生成・付与するというものである。上記の新システムによる対応と外部のサービス（タイムスタンプ局）の利用のどちらを採用するかについては、必要となるシステム対応の内容、追加的に発生する運用上のコスト、対応にかかる時間等を比較しつつ判断することとなる。

（ハ）アクセス制御の強化

ケース A と B においては、暗号処理部から出力され、旧システム内部での処理の対象となっている署名付きメッセージを保護する必要がある。その方法として、旧システムの暗号処理部へのアクセス制御を一段と強化することが考えられる。強化する対象としては、①情報システムの端末への物理的なアクセス（入室管理等）、②その端末でのユーザー認証（パスワード認証やスマートカー

ド等による所持物認証等)、③情報システムが外部のネットワーク等に接続されている場合には、それらを経由した不正侵入の防止機構（ファイアウォールや不正侵入検知装置＜intrusion prevention system＞等）が想定される。例えば、旧システムにおけるユーザー認証の手段として、PKI による認証が利用されており、そのベースとなっている公開鍵暗号が耐量子計算機暗号でないとすれば、認証が有効でなくなる可能性があるため、それを耐量子計算機暗号を利用したものに切り替えることが対応の候補として挙げられる。

新システムにおいて署名付きメッセージを保護する場合（ケース B と C）においても、上記と同様の方針でアクセス制御の強化を実施することが考えられる。もっとも、新システムは、耐量子計算機暗号の使用を前提として開発されており、例えば、ユーザー認証用のアルゴリズムとして耐量子計算機暗号が採用されている状況が想定される。その場合、上記の対応は不要となる。

ロ．暗号文の保護にかかる対応

暗号文を保護する方法としては、暗号文へのアクセス制御を強化して攻撃者による盗取を防止すること、あるいは、仮に盗取されたとしても解読困難とする仕組みを予め講じておくことが考えられる。

（イ）アクセス制御の強化

旧システムにおいて暗号文を保護する場合（ケース A と B)、本節 (2) イ（ハ）で説明したアクセス制御の強化を暗号処理部やストレージに適用することが考えられる。新システムにおいて暗号文を保護する場合（ケース B と C）についても、アクセス制御の強化という観点では、上記と同様の対応が考えられる。

（ロ）鍵長を伸長した共通鍵暗号による再暗号化

暗号文が盗取されることを前提とする対応としては、暗号文をいったん復号したうえで、2 節（2）で示したように、鍵長を伸長した共通鍵暗号によって平文を再度暗号化するという方法が考えられる[20]。

旧システムにおいて再暗号化を実施する場合には、暗号処理部内に、暗号文を復号するための（既存の）機能を維持しつつ、鍵長を伸長した暗号鍵によって暗号文を生成するための機能を新たに実装することが求められる。ただし、旧システムは稼働停止を予定しており、こうしたシステム対応を追加的に実施することがコスト面等から困難な場合も想定される。旧システムにおいて実施困難となれば、再暗号化は、旧システムのみが動作するケース A の暗号文、および、ケース B における旧システム内部で処理途中の暗号文には適用できないという

[20] この場合、暗号利用モードも適切に選択することが前提となる（2 節（2）を参照)。

ことになる。

ケースBとCにおいて、ストレージに保管されている暗号文については、新システムにおいて再暗号化を実施することが考えらえる。旧システムから移管した暗号文を復号した後、その結果の平文を新システムにおいて再暗号化する。また、旧システムと新システムとの間でデータの受渡しを安全に行うことができるならば、旧システムにおいて暗号文を復号し、その平文を新システムに移管するという方法も想定される。

こうした対応では、新システムの暗号処理部内に格納されている暗号鍵を変更することになる点に留意が必要である。3 節（1）で説明したように、本稿では、暗号鍵が安全に管理されているとの前提を置いて議論してきた。もっとも、実際に再暗号化を行う際には、大規模な暗号鍵の更新（廃棄と生成）を実施することになり、これを安全かつ効率的に行うことが求められる。どのような管理体制のもとで暗号鍵の更新を実施するかについて検討しておく必要がある。

５．結びに代えて：金融機関における対応の留意点

金融分野における暗号の移行について考える際には、個々の金融機関が運営する情報システムの問題として検討するとともに、金融分野全体の問題として検討する必要がある。

（１）個々の金融機関における視点

まず、個々の情報システムの問題として捉える場合には、その情報システムを運営する金融機関が個別に対応を検討することになる。具体的には、情報システムにおけるデータ保護期間を適切に設定したうえで、システム移行準備期間や切替期間をどう短縮するかをまず検討する。その結果、量子ゲート型コンピュータが実現可能とされる X 年の到来時期よりも前に旧システムのデータ保護期間が満了しないとの見通しが濃厚となった場合には、量子ゲート型コンピュータによる暗号文解読や署名付きメッセージ改変のリスクを評価し、対応策を検討することとなる。

現時点では、X 年の到来時期について、確度の高い予測結果は示されていない。したがって、暗号の移行にかかるシステム対応を直ちに着手する必要性は低いといえる。むしろ、既存の情報システムの更改や新たな情報システムの開発の際に、データ保護期間の見直しやクリプト・アジリティの設計思想に基づいた対応を検討しておくことが、将来の暗号移行を効率的に行ううえで有用である。設計段階から、暗号処理のモジュール化、無線通信等を用いたソフトウェアのアップデート、ユーザーが利用する端末との互換性の確保等を実現するよう配慮す

ることが望ましい[21]。

上記の対応について、今後、個々の金融機関では、（暗号を使用している）複数の情報システムに関して個別に検討することになると考えられる。その際、例えば、暗号移行のシステム対応を、優先度を決定したうえで順番に実施していくとすれば、すべての情報システムにおける対応が完了するまでに相応の時間を要する可能性がある点にも留意する必要がある。

（２）金融分野全体での視点

金融分野全体として暗号移行にかかる対応を考える場合、個々の金融機関に閉じた対応（本節（1）に示した対応）に加えて、複数の金融機関の情報システムと連携して稼働する情報システムでの対応が重要な課題となる。

X 年の到来時期が高い確度で予測できるようになれば、そのタイミングから、各金融機関における暗号移行にかかる検討が本格化するであろう。個々の金融機関は、自社の情報システムにおける対応の優先順位だけでなく、複数の金融機関の情報システムが連携して稼動する情報システムに関しても、優先順位をどのように設定するかを、関係する複数の金融機関と調整する必要が生じることになる。

また、そうした際には、各情報システムの運行・維持管理を担当するシステム・ベンダーのサポートを受けることになる可能性が高い。複数の金融機関から暗号移行にかかる検討の依頼がシステム・ベンダーに対してほぼ同じ時期に集中して寄せられた場合、人材確保に時間がかかり、タイムリーな検討を実施できない可能性があるほか、そうした検討にかかる費用も増大すると予想される。

暗号移行にかかる検討は、金融分野にのみ発生するものではなく、政府機関の情報システムのほか、各産業分野における多くの情報システムにおいても発生する。その結果、暗号移行の検討にかかる人材への需要が急速に増大し、「データ保護期間の検討を実施したものの、具体的なシステム移行の検討を開始できない」とか、「システム移行の計画を策定したものの、新システムの開発要員を十分に確保することができず、開発に着手できない」といった状況が発生することも想定される。金融分野において暗号移行をどのように計画的に進めていくかを検討するだけでは十分とはいえず、他の産業分野や政府機関とも連携して検討することが必要となる可能性がある。例えば、X 年の到来が想定される時期が明確になった際に想定される金融分野等への影響、暗号移行の検討着手の優先順位、検討やシステム開発に携わる人員の手当てや配分等が、主な検討項目として含まれると考えられる。

---

[21] こうした設計は、量子ゲート型コンピュータ以外の脅威（古典コンピュータによる脅威や未知の脅威）への対応として暗号の移行を実施する場合にも有効である（詳細は補論 3 を参照）。

こうした検討を分野横断的に実施する体制の整備も必要となる可能性も考慮すると、海外での先行事例を踏まえつつ暗号移行を適切に進めていくうえで、十分な時間的余裕をもった対応が重要である。今後、金融分野における暗号移行対応にかかる議論が深まっていくことを期待したい。

以　上

参考文献

伊藤忠彦、「量子コンピュータの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発表論文、電子情報通信学会、2018 年 a

———、「量子コンピュータによる PKI 危殆化とその対策に関する考察」、日本セキュリティマネジメント学会第 32 回全国大会発表論文、日本セキュリティマネジメント学会、2018 年 b

四方順司、「量子コンピュータに耐性のある暗号技術の標準化動向：米国政府標準暗号について」、金融研究所ディスカッション・ペーパーNo. 2019-J-4、日本銀行金融研究所、2019 年

清水俊弥・伊豆哲也・篠原直行・盛合志帆・國廣昇、「アニーリング計算による素因数分解について」、2019 年暗号と情報セキュリティシンポジウム発表論文、電子情報通信学会、2019 年

情報通信研究機構・情報処理推進機構、「暗号技術検討会 2018 年度報告書」、情報通信研究機構・情報処理推進機構、2019 年

杉山昇太郎・伊藤忠彦・磯部光平、「ハードウェアセキュリティモジュールへの耐量子計算機暗号の実装と評価」、2019 年暗号と情報セキュリティシンポジウム発表論文、電子情報通信学会、2019 年

清藤武暢、「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」、日銀レビュー18-J-4、日本銀行、2018 年

———・青野良範・四方順司、「量子コンピュータの解読に耐えうる『格子暗号』の最新動向」、『金融研究』第 34 巻第 4 号、日本銀行金融研究所、2015 年、135～170 頁

———・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」、『金融研究』第 38 巻第 1 号、日本銀行金融研究所、2019 年、45～72 頁

日本銀行金融研究所、「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」、『金融研究』第 38 巻第 1 号、日本銀行金融研究所、2019 年、29～44 頁

CRYPTREC 暗号技術調査ワーキング・グループ、「耐量子計算機暗号の研究動向調査報告書」、情報通信研究機構・情報処理推進機構、2019 年（https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2018.pdf、2019 年 8 月 15 日）

Anand, Mayuresh Vivekanand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh, “Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation,” *Proceedings of International Workshop on Post-Quantum Cryptography (PQCrypto) 2016*, *Lecture Notes in Computer Sciences*, 9606, Springer-Verlag, 2016, pp. 44-63.

Bennett, Charles Henry, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, "Strengths and Weaknesses of Quantum Computing," *SIAM Journal on Computing*, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1510-1523.

Brassard, Gilles, Peter HØyer, and Alain Tapp, "Quantum Cryptanalysis of Hash and Claw-Free Functions," *Proceedings of Latin American Symposium on Theoretical Informatics (LATIN) 1998*, *Lecture Notes in Computer Science*, 1380, Springer-Verlag, 1998, pp. 163-169.

Crockett, Eric, Christian Paquin, and Douglas Stebila, "Prototyping Post-Quantum and Hybrid Key Exchange and Authentication in TLS and SSH," Cryptology ePrint Archive, 2019/858, International Association for Cryptologic Research, 2019.

Chen, Lidong, "Cryptography Standards in Quantum Time: New Wine in an Old Wineskin?" *IEEE Security & Privacy*, 15(4), IEEE, 2017, pp. 51-57.

EMVCo, "EMV Integrated Circuit Card Specifications for Payment Systems Book2 Security and Key Management Version 4.3," EMVCo, 2011.

Fowler, Austin G., Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland, "Surface Codes: Towards Practical Large-Scale Quantum Computation," *Physical Review A*, 86(3), 032324, American Physical Society, 2012 (https://journals.aps.org/pra/abstract/10.1103/PhysRevA.86.032324、2019 年 8 月 15 日).

Gidney, Craig, and Martin Ekerå, "How to Factor 2048 Bit RSA Integers in 8 Hours Using 20 Million Noisy Qubits", arXiv: 1905.09749v1, Cornell University Library, 2019.

Gondrom, Tobias, Ralf Brandner, and Ulrich Pordesch, "Evidence Record Syntax (ERS)," Request for Comments, 4998, International Engineering Task Force, 2007.

Gouget, Aline, "PQ-Crypto Standardization Preparing Today for the Future of Cryptography," presentation at Quantum-Safe Cryptography for Industry (QsCI), 2017 (https://risq.fr/pres/17_QsCI_Gemalto_AG.pdf、2019 年 8 月 15 日).

Grover, Lov K., "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of Annual ACM Symposium on Theory of Computing (STOC) 1996*, Association for Computing Machinery, 1996, pp. 212-219.

Housley, Russ, "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms," Request for Comments, 7696, International Engineering Task Force, 2015.

International Organization for Standardization, "ISO/TR 14742:2010 Financial Services -- Recommendations on Cryptographic Algorithms and Their Use," International Organization for Standardization , 2010.

———, “ISO 16609:2012 Financial Services -- Requirements for Message Authentication Using Symmetric Techniques,” International Organization for Standardization, 2012.

———, “ISO 9564-2:2014 Financial Services --Personal Identification Number (PIN) Management and Security -- Part 2: Approved Algorithms for PIN Encipherment,” International Organization for Standardization, 2014.

———, “ISO 9564-1:2017 Financial Services -- Personal Identification Number (PIN) Management and Security -- Part 1: Basic Principles and Requirements for PINs in Card-Based Systems,” International Organization for Standardization, 2017.

Jiang, Shuxian, Keith A. Britt, Alexander J. McCaskey, Travis S. Humble, and Sabre Kais, “Quantum Annealing for Prime Factorization,” *Scientific Reports*, 8, Article No. 17664, Springer Nature, 2018 (https://www.nature.com/articles/s41598-018-36058-z.pdf、2019 年 8 月 15 日).

Kaplan, Marc, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia, “Breaking Symmetric Cryptosystems Using Quantum Period Finding,” *Proceedings of CRYPTO 2016 Part 2*, *Lecture Notes in Computer Science*, 9815, Springer-Verlag, 2016, pp. 207-237.

Kuwakado, Hidenori, and Masakatsu Morii, “Quantum Distinguisher between the 3-Round Feistel Cipher and the Random Permutation,” *Proceedings of IEEE International Symposium on Information Theory (ISIT) 2010*, IEEE, 2010, pp. 2682-2685.

———, and ———, “Security on the Quantum-Type Even-Mansour Cipher,” *Proceedings of IEEE International Symposium on Information Theory and its Applications (ISITA) 2012*, IEEE, 2012, pp. 312-316.

Langley, Adam, Alistair Riddoch, Alyssa Wilk, Antonio Vicente, Charles Krasic, Dan Zhang, Fan Yang, Fedor Kouranov, Ian Swett, Janardhan Iyengar, Jeff Bailey, Jeremy Dorfman, Jim Roskind, Joanna Kulik, Patrik Westin, Raman Tenneti, Robbie Shade, Royan Hamilton, Victor Vasiliev, Wan-The Chang, and Zhongyi Shi, “The QUIC Transport Protocol: Design and Internet-Scale Deployment,” *Proceedings of Conference of ACM Special Interest Group on Data Communication (SIGCOMM) 2017*, Association for Computing Machinery, 2017, pp.183-986.

Moody, Dustin, “Let’s Get Ready to Rumble -The NIST PQC Competition,” presentation at International Workshop on Post-Quantum Cryptography (PQCrypto) 2018, Florida Atlantic University, 2018.

Mosca, Michele, “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” Cryptology ePrint Archive, 2015/1075, International Association for

Cryptologic Research, 2015.
———, “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?” *IEEE Security & Privacy*, 16(5), IEEE, 2018, pp. 38-41.
National Institute of Standards and Technology, “Report on Post-Quantum Cryptography,” NIST Internal Report, 8105, National Institute of Standards and Technology, 2016a.
———, “Recommendation for Key Management, Part 1: General,” NIST Special Publication, 800-57 Part 1 Revision 4, National Institute of Standards and Technology, 2016b.
———, “PQC Standardization Process: Second Round Candidate Announcement,” National Institute of Standards and Technology, 2019 (https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates、2019 年 8 月 15 日).
National Security Agency, “Commercial National Security Algorithm Suite and Quantum Computing FAQ,” MFQ-U-OO-815099-15, National Security Agency, 2016.
Open Quantum Safe, “Open Quantum Safe: Software for Prototyping Quantum-Resistant Cryptography,” Open Quantum Safe, 2018 (https://openquantumsafe.org/, 2019 年 8 月 15 日).
Pecen, Mark, “Chairman’s Report for 2018: ETSI Cyber Working Group for Quantum-Safe Cryptography,” presentation at ETSI/IQC Quantum Safe Workshop, European Telecommunications Standards Institute, 2018.
Rescorla, Eric, “The Transport Layer Security (TLS) Protocol Version 1.3,” Request for Comments, 8446, International Engineering Task Force, 2018.
Roetteler, Martin, Michael Naehrig, Krysta M. Svore, and Kristin Lauter, “Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms,” *Proceedings of ASIACRYPT 2017*, *Lecture Notes in Computer Science*, 10625, Springer-Verlag, 2017, pp. 241-270.
Shor, Peter W., “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” *Proceedings of IEEE Annual Symposium on Foundations of Computer Science (FOCS) 1994*, IEEE, 1994, pp. 124-134.
———, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” *SIAM Journal on Computing*, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1484-1509.
Simon, Daniel R., “On the Power of Quantum Computation,” *SIAM Journal of Computing*, 26(5), Society for Industrial and Applied Mathematics, 1997, pp. 1474-

1483.

Truskovsky, Alexander, Philip Lafrance, Daniel Van Geest, Scott Fluhrer, Panos Kampanakis, Mike Ounsworth, and Serge Mister, “Multiple Public-Key Algorithm X.509 Certificates,” Internet Draft, International Engineering Task Force, 2018.

補論 1. 量子ゲート型コンピュータが既存の公開鍵暗号の脅威となる時期

RSA 暗号（鍵長 2,048 ビット）を解読可能な量子ゲート型コンピュータの実現時期について、レットラーとファウラーの研究成果に基づき考察する（Roetteler *et al.* [2017]、Fowler *et al.* [2012]）。

レットラーは、RSA 暗号の解読に必要な量子ビット数の（後述の誤り率を考慮していない）理論値を示しており、ファウラーは誤り率と RSA 暗号の解読に必要な量子ビット数の関係式を示している。これらを組み合わせることにより、RSA 暗号が解読されうる時期を試算する。

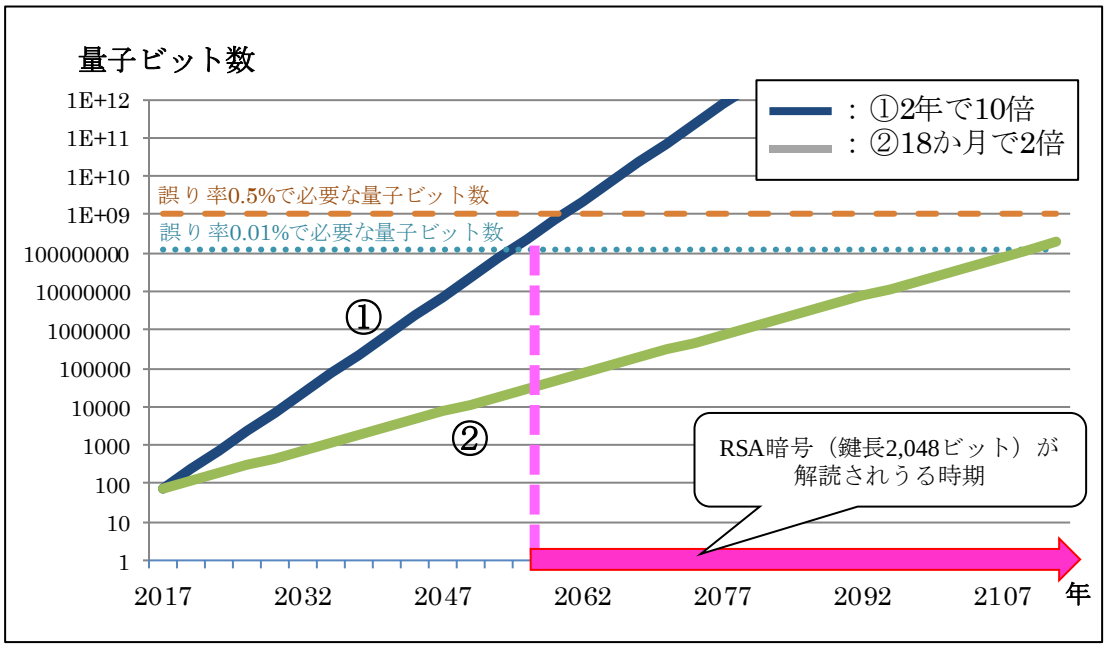
誤り率については、最近の研究動向を踏まえ、既存の量子ゲート型コンピュータで発生している「0.5%」と、今後の目標として設定されている「0.01%」の 2 つを想定する。量子ゲート型コンピュータには、量子ビット数が増えるほど、誤り率が上昇するという特性がある。もっとも、ここでは、ワースト・ケースを考慮するという観点から、量子ビット数の増加に比例して、誤り訂正に関する技術も向上し、その結果として、量子ビット数が増加しても誤り率は一定となると仮定する。量子ゲート型コンピュータにおいて取り扱うことが可能な量子ビット数の増加の度合いについては、最近の量子ゲート型コンピュータの研究において最も顕著であった伸び率（2 年で 10 倍）と、古典コンピュータと同程度の伸び率（18 か月で 2 倍）の 2 つを想定する。

RSA 暗号を解読するためには、10^8 個以上の量子ビットが必要と考えられている（Roetteler *et al.* [2017]、Fowler *et al.* [2012]）。そこで、量子ゲート型コンピュータが取扱い可能な量子ビット数が 10^8 個以上となる時期を「解読されうる時期」とする。

これらを踏まえ、RSA 暗号が解読されうる時期の試算結果をグラフ化した（図表 A-1 を参照）。量子ビット数が 2 年で 10 倍になると仮定すると、RSA 暗号を解読しうる量子ゲート型コンピュータが実現するまでには、本稿執筆時点（2019 年）からさらに 30 年以上の期間が必要と考えられる。

上記の期間に関しては、必要とする量子ビット数を削減する研究（Gidney and Ekerå [2019]等）の進展によっては前倒しされる可能性もある。モスカが主張しているように、誤り耐性を有する量子ゲート型コンピュータが実現された場合（2 節（4）を参照）、必要な量子ビットの数は大きく変化する。誤り耐性を有する量子ゲート型コンピュータ（例えば、誤り率が限りなくゼロに近い理想的なもの）が開発された場合には、量子ビットの実装技術が短期間で進展し、膨大な数（数千個）の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が実現することもありうる。そのため、今後の動向に注目する必要がある。

図表 A-1　RSA 暗号（鍵長 2,048 ビット）が解読されうる時期の試算



補論 2. ハイブリッド方式に基づく電子証明書の生成方法

既存の PKI においては、RSA 暗号や楕円曲線暗号を利用して電子証明書における署名を生成する場合が多い。そこで、既存の署名方式の使用を継続しつつ、耐量子計算機暗号に基づく署名方式を並行して使用し、量子ゲート型コンピュータによる脅威が顕在化した際には、耐量子計算機暗号に基づく署名方式のみを使用するように切り替えるという対応が考えられる。

トルスコフスキーらは、既存の PKI の仕組み（電子証明書のフォーマットや発行スキーム等）を大幅に変更することなく耐量子計算機暗号に移行する方式（ハイブリッド方式）を提案した（Truskovsky *et al.* [2018]）。既存の電子証明書においては、証明書記載情報に対して 1 つの署名方式によって署名が生成される。ハイブリッド方式では、証明書記載情報に対して耐量子計算機暗号による署名と既存の署名方式による署名の両方を生成し、電子証明書に組み込む。これによって、どちらか 1 つの署名を検証可能な機器であれば、同一の電子証明書を利用することができる。そして、（ユーザーが利用する）機器に実装されている暗号を一斉に耐量子計算機暗号へ切り替えるのではなく、時間に余裕を持って徐々に入れ替えることが可能となり、移行にかかるコストの抑制も期待できる。

ただし、既存の電子証明書と比べて電子証明書のサイズや鍵のサイズが増加するほか、2 つの署名の検証結果が異なる場合にどう判断するかなどに関して明確な規則（ポリシー）を検討しておくことが必要である（杉山・伊藤・磯部［2019］）。

補論 3. 古典コンピュータによる脅威を考慮した暗号移行の検討

暗号を利用する情報システムにおいては、量子ゲート型コンピュータによる脅威への対応に加えて、古典コンピュータの性能向上に伴う脅威への対策についても検討する必要がある[22]。

米国連邦政府は、暗号の移行に関するガイドライン（SP800-57）を制定しており、既存の公開鍵暗号（RSA 暗号や楕円曲線暗号）の鍵長について、2030 年までに伸長することを推奨している（National Institute of Standards and Technology [2016b]）[23]。そのため、公開鍵暗号を耐量子計算機暗号へ移行することを検討する際には、古典コンピュータによる脅威への対応についても考慮することが望ましい。仮に、古典コンピュータへの対策（鍵長の伸長）を完了した後、X 年の到来時期が早まるなどの要因により、短期間で耐量子計算機暗号に移行する必要が生じたならば、移行に必要なコストが増大する可能性がある。したがって、耐量子計算機暗号への移行期間は、少なくとも 2030 年を目途とした鍵長の伸長対応の期間と重ならないようにする必要がある。

こうした対応には 2 通りの方法が考えられる（National Security Agency [2016]、日本銀行金融研究所［2019］）。1 つは、既存の公開鍵暗号や共通鍵暗号の鍵長の伸長を優先的に行い、その後、耐量子計算機暗号に移行するという方法である。もう 1 つは、既存の公開鍵暗号の鍵長の伸長を行わず、耐量子計算機暗号への移行を優先する方法である。前者は、X 年の時期が予想以上に早かった場合、耐量子計算機暗号への移行時に要するコストが増加する反面、古典コンピュータによる脅威への対応を確実に実施できる[24]。後者は、移行が 1 回で済み、移行にかかるコストが前者よりも小さくなるものの、耐量子計算機暗号の標準化の状況によっては、移行完了が 2030 年以降となる可能性がある。その場合、2030 年以降も、既存の公開鍵暗号の使用を継続することとなり、古典コンピュータへの脅威への対応が不十分となりうる。

本稿執筆時点（2019 年 8 月 15 日）では、どちらがより適切であるかについて、米国連邦政府は明確な指針を示していない（National Security Agency [2016]）。耐量子計算機暗号の標準化動向と量子ゲート型コンピュータの開発の進捗状況

---

[22] 公開鍵暗号においては、古典コンピュータの処理性能の向上により安全性が徐々に低下することが知られており、鍵長を適宜伸長していくことが必要となる。

[23] SP800-57 の内容は、金融サービスでの利用を推奨する暗号等に関する技術報告書（ISO/TR 14742）においても参照されている（International Organization for Standardization [2010]）。なお、SP800-57 では、（耐量子計算機暗号を含む）他の暗号への移行を行う場合は、古典コンピュータに対して RSA 暗号や楕円曲線暗号と同程度の安全性（古典コンピュータを想定）を有するものを選択することが推奨されている。

[24] 移行にかかるコスト増加を抑えるために、鍵長の伸長を一部の情報システムのみで実施することとしたり、データ保護期間等に応じて対策実施の優先順位を再検討したりすることが考えられる。

を確認しつつ、金融機関が独自に判断していくことが必要となる。

なお、耐量子計算機暗号は、既存の公開鍵暗号よりも、鍵長や暗号化データのサイズ等が増加することが想定される。そのため、暗号化データを保管するためのストレージ、暗号化データを通信するための通信回線、暗号演算を行うサーバ等に必要となるコストが大幅に増加しうる。耐量子計算機暗号への移行を検討する際には、情報システムの運用コストについても十分留意しておくことが望ましい。