量子コンピュータ時代でも安全な情報基盤への移行に向けて

耐量子計算機暗号 (PQC) への移行に関するホワイトペーパー

株式会社NTTデータグループ
技術革新統括本部
システム技術本部
サイバーセキュリティ技術部
E-mail: security-contact@kits.nttdata.co.jp

発行日：2023年10月3日

本資料は、NTT社会情報研究所による支援を基に、株式会社NTTデータグループが作成しました。

目次

1. はじめに

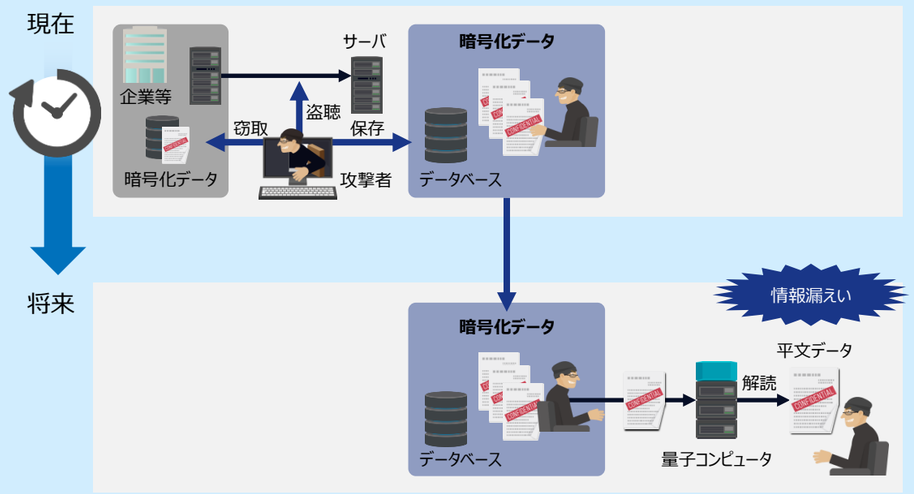
ITシステムと暗号技術

近年のITシステムでは、基礎技術として暗号技術が広く利用されています。例えば、通信路上を流れるデータや、ストレージに保存されたデータが攻撃者に盗聴や窃取をされても、意味のないデータにしか見えないようにして情報を保護するために、**暗号化**が利用されています。さらに、あるデータの作成者が確かにその本人であることを保証し、かつそのデータが改ざんされていないことを保証するために、**デジタル署名**が利用されています。暗号化やデジタル署名は、現在の社会を支える暗号技術の代表的なものです。

一方で、近年、**量子コンピュータ**の実装技術が著しく進展しています。量子コンピュータにより、従来では現実的な時間内では完了しないような計算が短時間でできるようになる可能性があり、AIや創薬などの研究への応用が期待されています。しかし、一般的に、新しい技術が登場するときには、その技術を悪用する攻撃による脅威も同時に登場します。すなわち、将来、量子コンピュータにより、暗号技術が破られることが心配されています。

攻撃者は長期的な視点から暗号の解読を成功させようとします。現在は量子コンピュータの性能が十分でないため暗号を破ることができなくても、将来量子コンピュータの性能が向上した時点で解読を試みる**「Store now, decrypt later 攻撃」**が脅威と捉えられ始めています（図1）。この攻撃は「Capture now, decrypt later 攻撃」または「Harvest now, decrypt later 攻撃」とも呼ばれています。

図1: Store now, decrypt later 攻撃



従来の脅威はスーパーコンピュータ

従来の脅威： スーパーコンピュータの性能向上

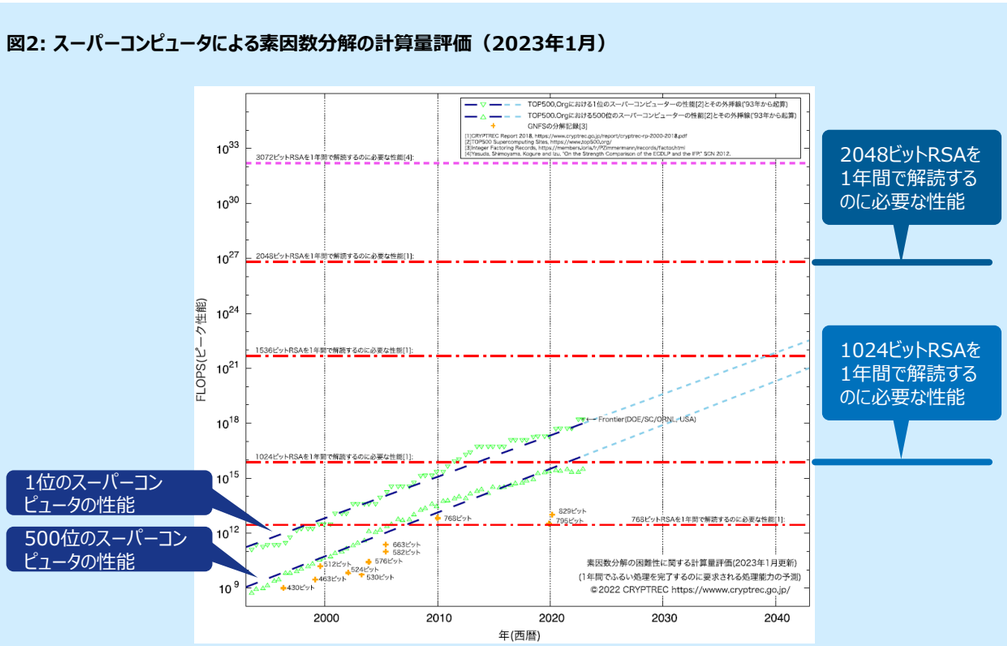
量子コンピュータによる脅威を解説する前に、従来から存在する脅威を解説します。この従来の脅威は量子コンピュータによる脅威に取って代わられる訳ではなく、依然として存在することには注意が必要です。

暗号技術にとって、従来から存在する脅威は**スーパーコンピュータ**でした。その性能が向上する速度を考慮して、暗号化やデジタル署名に使用される鍵の長さの推奨値が見積もられてきました。

例えば、暗号化やデジタル署名の機能を持つ公開鍵暗号の一つに、**RSA暗号**があります。RSA暗号は、大きな桁数の**素因数分解**が困難であることをその安全性の根拠として設計されています。すなわち、大きな桁数の素因数分解が容易に解ければ、RSA暗号は破られることになります。

図2は、スーパーコンピュータによる素因数分解の計算量を評価したグラフであり、横軸は年を、縦軸はFLOPSという単位で表される処理能力（1秒間に処理可能な浮動小数点演算の回数）をそれぞれ表します。図2より、鍵長が1024ビットのRSA暗号を1年間で解読するのに必要な性能は、現在1位の性能を持つスーパーコンピュータにより2012年ごろには達成されていたことがわかります。このグラフ上の直線を右方向に伸ばして考察することにより、スーパーコンピュータの性能向上を考慮した適切な鍵長を検討することができます。

図2: スーパーコンピュータによる素因数分解の計算量評価（2023年1月）



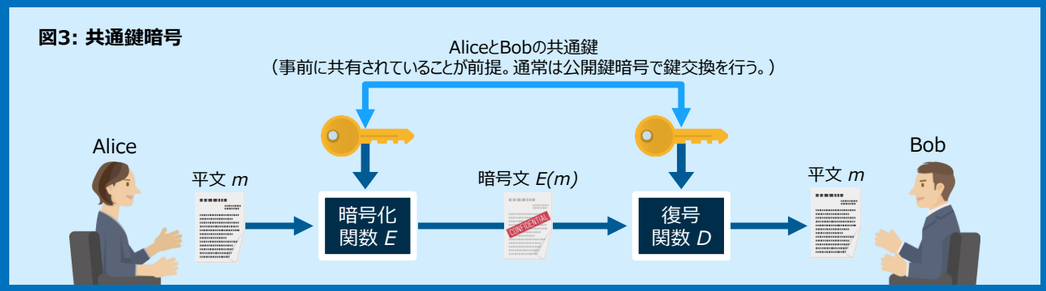
「CRYPTREC Report 2022 暗号技術評価委員会報告書」（CRYPTREC）（ https://www.cryptrec.go.jp/report/cryptrec-rp-2000-2022.pdf ），p.33の図をもとに株式会社NTTデータグループ作成

（参考）暗号技術

■ 共通鍵暗号って何？

共通鍵暗号は、暗号化用の鍵と復号用の鍵が同じ暗号です。最初に何らかの安全な方法で共通の鍵（**共通鍵；対称鍵**）となるデータを共有します。通信相手ごとに共通鍵を秘密に管理する必要があります。一般に、公開鍵暗号より処理速度が断然速いため、通常の暗号化用途では共通鍵暗号が用いられ、その共通鍵を2者間で共有するために公開鍵暗号の技術（暗号化または鍵カプセル化メカニズム（Key Encapsulation Mechanism; KEM））が用いられます。

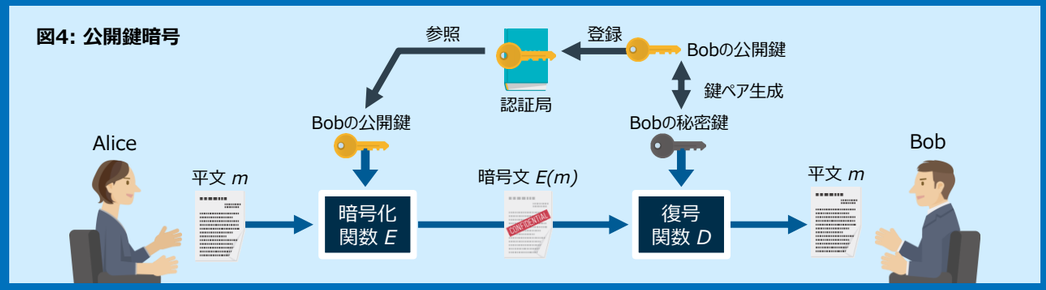
図3: 共通鍵暗号



■ 公開鍵暗号って何？

公開鍵暗号は、暗号化するための鍵と復号するための鍵が異なる暗号です。暗号化用の鍵**（公開鍵）**を公開し、復号用の鍵**（秘密鍵；私有鍵）**を秘密に保持します。通信相手ごとに秘密鍵を秘密に管理する必要がありません。計算量的に解くことが困難な数学的問題に安全性を依拠しています。

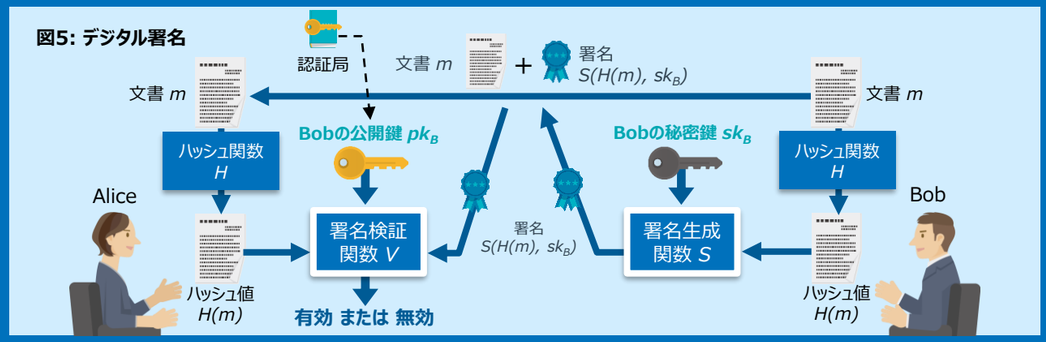
図4: 公開鍵暗号



■ デジタル署名って何？

デジタル署名は、公開鍵暗号の暗号化のアイディアを逆方向に利用したものです。送信者が自分の秘密鍵を用いて文書に対する署名を作成し、受信者が送信者の公開鍵を用いて署名の妥当性を検証します。署名検証の結果が有効なら、文書は改ざんされていないことが保証されます**（完全性）**。さらに、正しい署名を生成できる者は秘密鍵を保持している者のみとなる性質が備わるため、署名が実在すれば「署名していない」ことの主張は認められなくなります**（否認防止）**。

図5: デジタル署名



従来の対策は「鍵長の伸長」で十分であった

従来の対策： 鍵長の伸長

スーパーコンピュータによる脅威に対する従来の対策は、暗号化やデジタル署名に使用される鍵の長さ（ビット数）を大きくすることでした。実際に、RSA暗号の一般的な鍵長は、時代の流れとともに512ビット、1024ビット、2048ビット、のように延伸されながら使用されてきています。最初から長い鍵にしておけばよいと思われがちですが、そうすると正当な利用者による暗号化・復号の処理にも時間がかかるようになってしまい、安全性が過剰に満たされる一方で利便性が損なわれることになります。よって、その時代のコンピュータの性能、およびその時点から20～30年くらい先を予測したコンピュータの性能などを考慮して、適切な鍵長が導かれています。

米国NIST（国立標準技術研究所）は共通鍵暗号・公開鍵暗号の各鍵長に対するセキュリティ強度を**「ビットセキュリティ」**と呼ばれる共通尺度で公開しています（表1，2）。現在は、80ビットセキュリティ以下の強度（公開鍵暗号の一つであるRSA暗号では1024ビットの鍵の安全性に相当する）は使用不可とされています。

表1: ビットセキュリティで表されるセキュリティ強度

セキュリティ強度	共通鍵アルゴリズム	FFC (DSA, DH, MQV)	IFC* (RSA)	ECC* (ECDSA, EdDSA, DH, MQV)
現在は使用不可 ≤ 80	2TDEA	L = 1024 N = 160	k = 1024	f = 160-223
112	3TDEA	L = 2048 N = 224	k = 2048	f = 224-255
128	AES-128	L = 3072 N = 256	k = 3072	f = 256-383
192	AES-192	L = 7680 N = 384	k = 7680	f = 384-511
256	AES-256	L = 15360 N = 512	k = 15360	f = 512+

＊ 量子コンピューティングが実用化された場合、セキュリティ強度の評価値は大きく影響を受ける。

表2: セキュリティ強度のタイムフレーム

セキュリティ強度		2030年まで	2031年以降
< 112	保護の適用（例：暗号化）	不許可	
	処理（例：復号）	レガシーユース*	
112	保護の適用	受け入れ可能	不許可
	処理		レガシーユース*
128	保護の適用、及び保護されている情報の処理	受け入れ可能	受け入れ可能
192		受け入れ可能	受け入れ可能
256		受け入れ可能	受け入れ可能

＊「レガシーユース」とは、アルゴリズム又は鍵長が、レガシーのアプリケーションでの使用のために、使われる可能性があることを意味する（すなわち、アルゴリズム又は鍵長が暗号保護されたデータを処理するために使用される可能性がある）。

出典： National Institute of Standards and Technology, “SP800-57 Recommendation for Key Management Part 1:General (Revision 5),” 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf
（日本語訳）鍵管理における推奨事項 第一部：一般事項. https://www.ipa.go.jp/files/000090943.pdf

（参考）CRYPTREC

日本では、CRYPTREC（Cryptography Research and Evaluation Committees; 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト）が、2070年までの暗号技術のセキュリティ強度要件を示しています（表3）。

表3: CRYPTRECが示すセキュリティ強度要件の基本設定方針概要

必要なセキュリティ強度要件は以下の表をベースとして、
システムの想定運用終了・廃棄年又は利用期間の終了年を基準に設定する。

想定運用終了・廃棄年/利用期間		2022～2030	2031～2040	2041～2050	2051～2060	2061～2070
112ビットセキュリティ	新規生成*1)	移行完遂期間*4)	利用不可	利用不可	利用不可	利用不可
	処理*2)		許容*3)			
128ビットセキュリティ	新規生成*1)	利用可	利用可	移行完遂期間*4)	利用不可	利用不可
	処理*2)				許容*3)	
192ビットセキュリティ	新規生成*1)	利用可	利用可	利用可	利用可	利用可
	処理*2)					
256ビットセキュリティ	新規生成*1)	利用可	利用可	利用可	利用可	利用可
	処理*2)					

*1) 新規に暗号処理を実行する場合（例：暗号化、署名生成）
*2) 処理済みのデータに対して処理を実行する場合（例：復号、署名検証）
*3) 処理済みのデータに対する正当性を担保又は確認するための何らかの技術的又は運用的な対策やルール等（暗号技術によるものとは限らない）を併用している場合
*4) よりセキュリティ強度の高い暗号技術又は鍵長への移行を完遂させなければならない期間。利用する暗号処理が短期間で解決する場合（例：エンティティ認証）、又は既存の電子政府システムの継続利用やそれらとの互換性・相互接続性維持のための利用に限定

注) 2021年末時点での暗号技術の安全性評価の現状等を踏まえたうえで、2070年までの予測可能なセキュリティマージンを持った基準として定めたものである。したがって、精度の高い実現時期の予測が困難な、画期的な暗号解読手法の発明や大規模量子コンピュータの実現によるアルゴリズムの危殆化等については考慮していない。

出典：「CRYPTREC暗号リスト改定に向けた動向及び暗号強度要件設定基準の紹介」（CRYPTREC）
（ https://www.cryptrec.go.jp/symposium/2022_cryptrec-list.pdf ），CRYPTRECシンポジウム2022，2022年7月5日.

新たな脅威は量子コンピュータ

2. 耐量子計算機暗号 (PQC) への移行の必要性

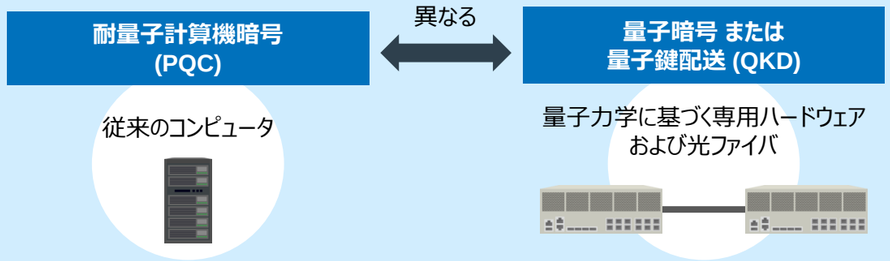
耐量子計算機暗号とは何であり、何と違うか

耐量子計算機暗号 (Post-Quantum Cryptography; PQC) とは、量子コンピュータでも解読や改ざんが難しい暗号技術の総称です。一般的には、後述する米国NISTにより標準化が進められている、複数の公開鍵暗号アルゴリズム群を指します。

PQCとは異なる技術として、**量子鍵配送 (Quantum Key Distribution; QKD)** があります（図6）。QKDは、量子力学に基づく専用ハードウェアと光ファイバを用いた鍵配送技術の一つです。その鍵配送の結果、2者間で共有されるビット列を**ワンタイムパッド**[*1]という共通鍵暗号の鍵として活用する暗号化通信の方式を、**量子暗号 (Quantum Cryptography)** と呼びます。文脈上の混同がなければ、単にQKDのことを「量子暗号」と呼ぶこともあり、その逆の場合もあり、意味としては曖昧に運用される傾向があります。また、歴史的には、QKDおよび量子暗号の概念はPQCよりも古く、1984年に発表されました。

また、PQCもQKDも、それらの用語の中に「量子（quantum)」という語が含まれるため、「量子コンピュータを用いて何かの処理をするものか？」と想像されがちですが、いずれも量子コンピュータ上で何かの処理を行うことはありません。量子コンピュータに対して従来のコンピュータのことを「古典コンピュータ」と呼びますが、PQCは古典コンピュータ上で動作するアルゴリズムとして実現されます。QKDは、量子力学に基づく専用ハードウェア（送信機と受信機）および光ファイバで構成され、その外観はネットワークスイッチやルータのような、サーバラックに収まるハードウェア機器になります。

図6: PQCとQKDの違い



*1 ワンタイムパッド（One Time Pad; OTP)とは、共通鍵暗号におけるストリーム暗号の一種であり、1ビットごとに平文と鍵の排他的論理和をとり、その結果を暗号文とし、鍵を使い捨てにする方式です。コンピュータの性能がいくら向上しても解読には無関係（そもそも解読に有益な情報が何も得られない）という特性を備える**「情報理論的安全性」**を有していますが、事前に十分な量の秘密のビット列を安全に共有することが課題であり、現在は一般的な産業用途ではほぼ利用されていません。しかし、量子鍵配送(QKD) はその課題を解決する手段の一つであり、今後、高い機密性が求められる社会領域から量子暗号（QKDとワンタイムパッドのセット）の活用が進むと考えられます。

脅威の真因「量子アルゴリズム」は既に存在する

素因数分解・離散対数問題を解く「ショアのアルゴリズム」

量子コンピュータによりすべての暗号技術が破られる訳ではありません。ここでは、量子アルゴリズムの存在を意識してその理解を試みます。

まず、古典コンピュータ上で何かを処理するにはプログラムを与える必要があります。そのプログラムの中である目的のために本質的な計算を行う部分は、「○○のアルゴリズム」と呼ばれることがあります。例えば、「平均値を計算するアルゴリズム」、「数値を小さい順に並べるアルゴリズム」などです。

同様に、量子コンピュータ上で量子特有の性質を利用して古典コンピュータよりもはるかに効率的に計算を行う部分は、**量子アルゴリズム**と呼ばれます。実は、素因数分解および離散対数問題を効率よく解く量子アルゴリズムとして、**「ショアのアルゴリズム」**が既に提案されています。この存在が、RSA暗号や楕円曲線暗号などの公開鍵暗号に対する脅威の直接的な要因となります。「ショアのアルゴリズム」が提案された1994年当時は、学術界では大きなインパクトがあったものの、量子コンピュータのハードウェア技術は未成熟な時代であり、産業界では将来の脅威として見なされました。それが近年、量子コンピュータの実装技術が進展してきたのに伴い、脅威が少しずつ大きくなってきていると見なすことができます。

表4は、現在主流の共通鍵暗号であるAES、および公開鍵暗号であるRSA暗号、楕円曲線暗号が、どのような量子アルゴリズムにより脅威を受けるか、その影響の度合い、および望ましい対策を示しています。

共通鍵暗号AESは、データ探索問題および周期探索問題を効率よく解く量子アルゴリズムにより大きな影響を受けます。しかし、その程度は限定的であり、nビットセキュリティの強度が、その半分の n/2 ビットセキュリティの強度に下がると評価されています。よって、AESの鍵長を伸長することにより、量子コンピュータに対する耐性を一定的には向上させることができます。ここで、AESの鍵長は、その仕様により128、192、256ビットの3つのみから選択することとなるため、最長である256ビットの鍵長を採用すれば、128ビットセキュリティの強度が得られ、当面の最良の選択となり得ます。

公開鍵暗号であるRSA暗号および楕円曲線暗号は、ショアのアルゴリズムにより破壊的な影響を受けるため、鍵長の伸長を採択するより、PQCへの移行が本質的な対策となります。

以上よりPQCを捉えると、PQCは公開鍵暗号の種類に属し、「暗号解読のための量子アルゴリズムが現在発見されていないもの」と見なすことができます。現在は発見されていなくても、将来は発見される可能性（古典アルゴリズムとして発見される場合と、量子アルゴリズムとして発見される場合の両方の可能性）がある点は、他の暗号アルゴリズムと同じであることに注意が必要です。

表4: 現在主流の暗号方式への影響

暗号の種類	現在主流の暗号方式	暗号解読のための量子アルゴリズム	量子アルゴリズムが解こうとする問題	暗号への脅威	望ましい対策
共通鍵暗号	AES	グローバーのアルゴリズム	データ探索問題	大きいが限定的	「鍵長の伸長」および「安全な暗号利用モードへの変更」
		サイモンのアルゴリズム	周期探索問題	大きいが限定的	
公開鍵暗号	RSA暗号	ショアのアルゴリズム	素因数分解	非常に大きい	PQCへの移行
	楕円曲線暗号	ショアのアルゴリズム	離散対数問題	非常に大きい	PQCへの移行
	耐量子計算機暗号(PQC)	**現在、発見されていない**	-	現在無し	-

米国はPQCの標準化を先導

量子コンピュータの脅威に対する各国の対応

量子コンピュータの脅威に対し、各国が暗号技術の移行に関する取組を開始しています（表5）。特に、米国は先導的立場にあり、2016年からPQCの標準化活動を進めています。

表5: 各国の対応

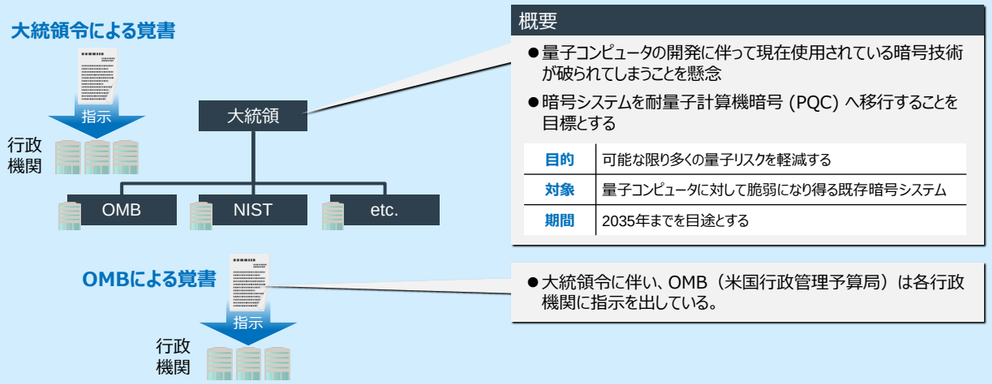
国/地域	対応
米国	• 2030年までに鍵長2048ビットのRSA暗号を破る量子コンピュータが出現することを想定*1) • 2035年までに連邦政府の暗号システムをPQCに移行することを計画*2) • 2016年からPQCの標準化活動を開始*3)
欧州	• ETSI において、NISTのPQC標準化を補足説明する技術レポートを公開*4) • SOG-IS において、将来、合意された量子耐性アルゴリズムの仕様を定義する予定*5)
日本	• CRYPTRECにおいて、暗号技術ガイドライン（耐量子計算機暗号）を公開*6) • CRYPTRECにおいて、耐量子計算機暗号の研究動向調査報告書を公開*7)

*1) NIST, “NISTIR 8105: Report on Post-Quantum Cryptography,” 2016.
*2) The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”, May 4, 2022.
*3) NIST, “Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process,” 2016.
*4) ETSI TR 103 616 V1.1.1 (2021-09) ”Quantum-Safe Signatures”, and ETSI TR 103 823 V1.1.1 (2021-09) ”Quantum-Safe Public Key Encryption and Key Encapsulation”.
*5) SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.3, February 2023.
*6) CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf
*7) CRYPTREC 耐量子計算機暗号の研究動向調査報告書 https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf

米国大統領令

2022年5月4日、米国のジョー・バイデン大統領は、量子コンピュータに耐性のある強固な新暗号技術の確立と普及を図るための大統領令に署名し、その覚書*1が公開されました（図7）。その覚書に示される暗号技術関連の指示内容のうち、主要なものを時系列で整理すると図8のようになります。さらに、大統領令に伴い、OMB（米国行政管理予算局）は各行政機関に具体的な指示を出しており、その覚書*2が公開されています（表6）。

図7: 米国の対応



*1 The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”, May 4, 2022.
https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
*2 Office of Management and Budget, “Memorandum for the Heads of Executive Departments and Agencies”, November 18, 2022.
https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf

図8: 大統領令よる覚書で示されたタイムライン

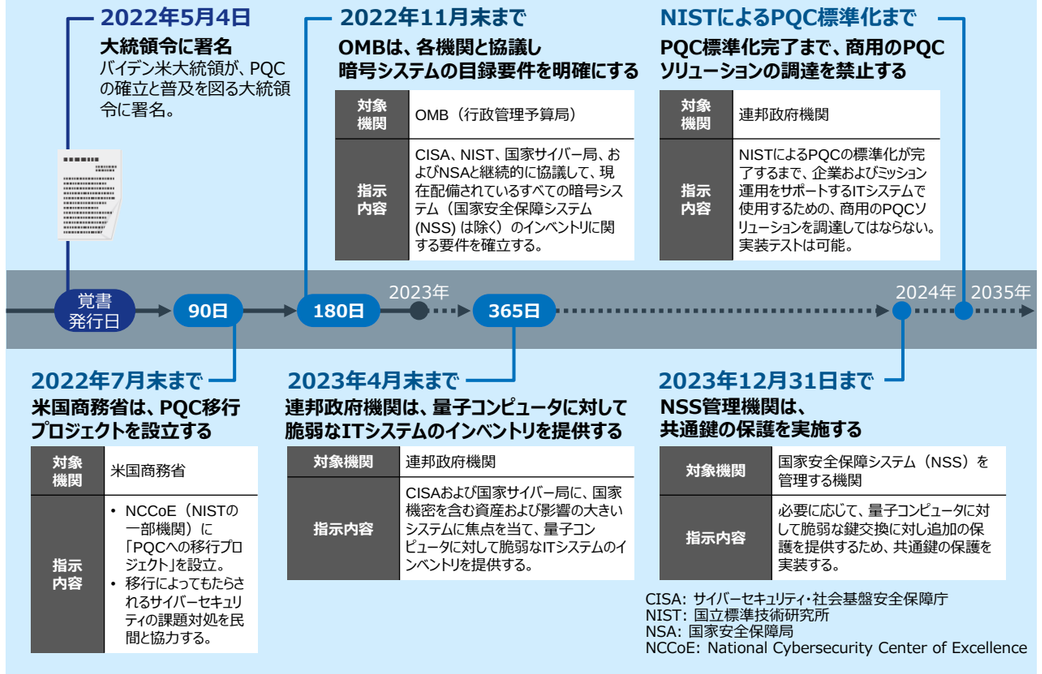


表6: OMBによる覚書で示された暫定の基準

指示内容	期間*1	対象機関
暗号の目録 (cryptographic inventory) を作成し、移行対象を示す。	30日以内（2022年12月18日まで）	全機関
目録の収集と伝達における指示書を発行する。	90日以内（2023年2月16日まで）	ONCD
資金調達における評価の指示書を発行する。	90日以内（2023年2月16日まで）	ONCD
PQCへの移行において、効率よく進めるための情報や実装テストの方法を確立する。	180日以内（2023年5月17日まで）	NIST
自動ツールに関する戦略をリリースし、各機関のPQC採用の進捗状況の評価をサポートする。	365日以内（2023年11月18日まで）	CISA
暗号システムの目録を提出する。	2023年5月4日まで、およびその後毎年	国防省とインテリジェンス・コミュニティ*2に属する機関を除く全機関
資金調達の評価を提出する。	2023年6月3日まで、およびその後毎年	国防省とインテリジェンス・コミュニティ*2に属する機関を除く全機関
事前に標準化されたPQCのテスト結果を報告する。	継続	全機関

*1 括弧内は、参考として、OMBによる覚書が発行された日（2022年11月18日）を起算日とする期限を示す。
*2 インテリジェンス・コミュニティとは、各国の政府が設置している情報機関によって組織されている機関。情報コミュニティ、情報活動コミュニティとも呼ばれる。

ONCD: 国家サイバー局
NIST: 国立標準技術研究所
CISA: サイバーセキュリティ・社会基盤安全保障庁

PQC標準として4方式が決定し、さらに評価を継続

NISTによるPQC標準化の状況

NISTは2016年からPQCの標準化を開始し、現在も継続しています[*1~6]。PQCの標準化は、「公開鍵暗号」、「鍵カプセル化メカニズム (Key Encapsulation Mechanisms; KEM)」、および「デジタル署名」の3カテゴリーでの公募により始まりました。その後、3～4段階のスクリーニング評価を経て徐々に提案方式を絞り込み、最終的に一つの方式ではなく複数の方式を選出する方針により行われています。「鍵カプセル化メカニズム（KEM)」という用語は学術文献で広く使用されてきた用語であり一般的ではないため、本書では「鍵交換 (KEM)」と記述します。

2017年12月に69方式が受理され、2019年1月の第1ラウンド評価結果で26方式が第2ラウンド評価に進み、2020年7月の第2ラウンド評価結果で15方式が第3ラウンド評価に進みました（図9）。そして2022年7月5日、第3ラウンド評価の結果が発表され、「公開鍵暗号」および「鍵交換（KEM)」のカテゴリーにおいて「CRYSTALS-KYBER」の1方式、デジタル署名のカテゴリーにおいて「CRYSTALS-Dilithium」、「FALCON」、および「SPHINCS+」の3方式の計4方式がPQC標準方式に決定されました（表7）。

同時に、第3ラウンド評価では標準となることを保留された、「公開鍵暗号」および「鍵交換（KEM)」のカテゴリーにおける「BIKE」、「Classic McEliece」、「HQC」、および「SIKE」の4方式に対し、第4ラウンド評価が行われることが示され、それら4方式のうち少なくとも1方式は標準に追加される方針であることが示されました。

しかし、その発表から間もない2022年7月、SIKEに対し攻撃が発見されたという論文が発表されました。既に、NISTのPQC標準化Webサイト上でも、SIKEの提案者が自らその攻撃の有効性を認めており、SIKEは今後のPQC標準候補から外れる可能性が高くなりました。

*1 NIST, NIST IR 8105, Report on Post-Quantum Cryptography, April 2016.
https://csrc.nist.gov/publications/detail/nistir/8105/final
*2 NIST, Post-Quantum Cryptography, Workshops and Timeline.
https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline
*3 NIST, Post-Quantum Cryptography, Round 3 Submissions
https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
*4 NIST, Post-Quantum Cryptography, Selected Algorithms 2022.
https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022
*5 NIST, Post-Quantum Cryptography, Round 4 Submissions
https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions
*6 NIST, Post-Quantum Cryptography: Digital Signature Schemes, Round 1 Additional Signatures
https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

図9: NISTによるPQC標準化のスケジュール

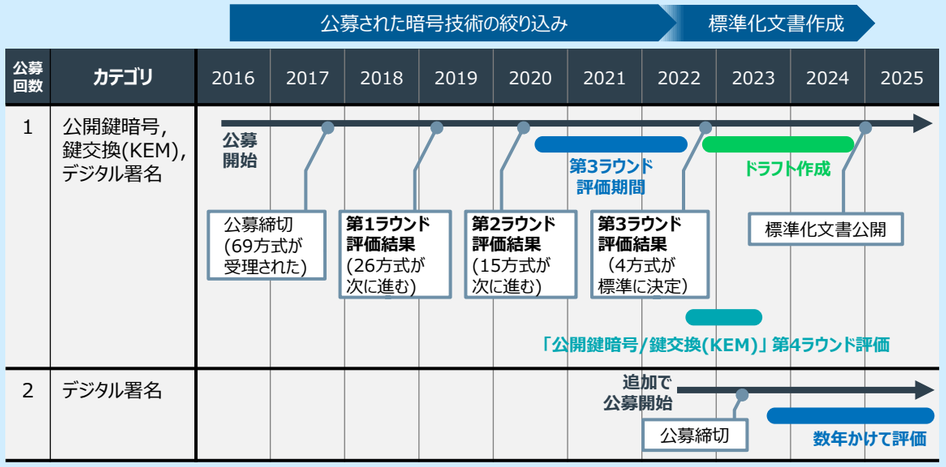


表7: NISTによるPQC標準化の状況

	公開鍵暗号および鍵交換(KEM)	デジタル署名
標準方式として決定	**CRYSTALS-KYBER**	**CRYSTALS-Dilithium** **FALCON** **SPHINCS+**
第4ラウンド評価中	BIKE Classic McEliece HQC	-
追加公募による第1ラウンド評価中	-	**（符号ベース署名）** CROSS, Enhanced pqsigRM, FuLeeca, LESS, MEDS, Wave **（同種写像署名）** SQIsign **（格子ベース署名）** EagleSign, EHTv3 and EHTv4, HAETAE, HAWK, HuFu, Raccoon, SQUIRRELS **（MPC-in-the-Head署名）** Biscuit, MIRA, MiRitH, MQOM, PERK, RYDE, SDitH **（多変数署名）** 3WISE, DME-Sign, HPPC, MAYO, PROV, QR-UOV, SNOVA, TUOV, UOV, VOX **（対称ベース署名）** AIMer, Ascon-Sign, FAEST, SPHINCS-alpha **（その他の署名）** ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Preon, Xifrat1-Sign.I

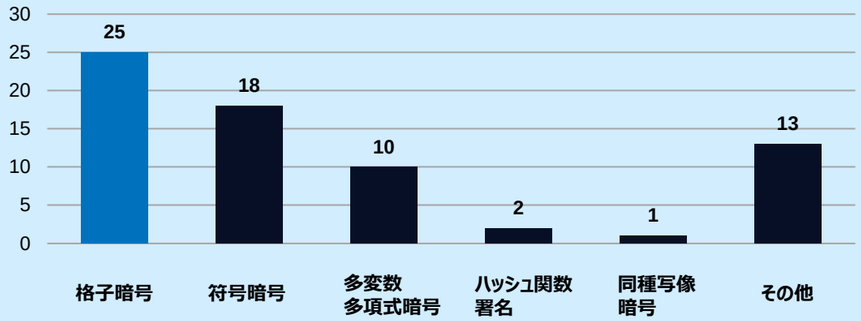
PQC標準の候補では格子暗号が多数

PQC公募暗号で多数を占める格子暗号

PQC標準化公募に受理された69個の暗号方式の分布を分析すると、数学における「格子（lattice)」に関連する様々な困難な問題（本書ではそれらを総称して「格子問題」と呼びます）を安全性の根拠とする方式が25個あり、最も多数でした（図10）。実際に、PQC標準方式に決定された4方式の内、「CRYSTALS-KYBER」、「CRYSTALS-Dilithium」、および「FALCON」の3方式は、格子問題を安全性の根拠とする**格子暗号**に属します。

図10: PQC標準化の第1ラウンド評価に進んだ69方式

● 応募された暗号方式



第2、第3ラウンドの各評価に進んだ方式においても、格子暗号が多い傾向は変わりませんでした（図11）。

この事象から、世界における格子暗号の研究者が多数存在することを読み取ることができます。ある特定の領域の研究者が多いことは、その領域から様々な暗号技術が考案されると同時に、それらの安全性を評価する研究者も多数存在することを期待できるため、その安全性に一定の安心感があると言えます。実際に、素因数分解・離散対数問題は多くの研究者により長年研究され、解くことが困難であることが証明されてきたため、それらを安全性の根拠とするRSA暗号・楕円曲線暗号などの安全性が信頼されてきたと言えます。

したがって、今後PQCに移行する際に暗号アルゴリズムを決定する場面では、安全性の側面から、格子暗号に属する暗号アルゴリズムを選択肢の一つに挙げておくことは望ましいと考えることができます。

図11: NIST PQC標準化第2ラウンド評価の結果（第3ラウンド評価に進んだ15方式）

括弧内は個数を表す

		格子暗号（7件）	符号暗号（3件）	多変数多項式暗号（2件）	ハッシュ関数署名（1件）	同種写像暗号（1件）	その他（1件）
公開鍵暗号および鍵交換（KEM）	最終候補	(3): CRYSTALS-KYBER, NTRU (NTRU-HRSS-KEM + NTRUEncrypt), SABER	(1): Classic McEliece	-	-	-	-
	代替候補	(2): Frodo-KEM, NTRU Prime	(2): BIKE, HQC	-	-	(1): SIKE	-
デジタル署名	最終候補	(2): CRYSTALS-Dilithium, FALCON	-	(1): Rainbow	-	-	-
	代替候補	-	-	(1): GeMSS	(1): SPHINCS+	-	(1): Picnic

PQCへの移行時に気を付けるべきことは？

3. PQCへの移行時の留意点

耐量子計算機暗号（PQC）への移行計画を策定する際に意識しておくべき留意点を以下に示します。

- **留意点①：データのサイズが大きくなる可能性**

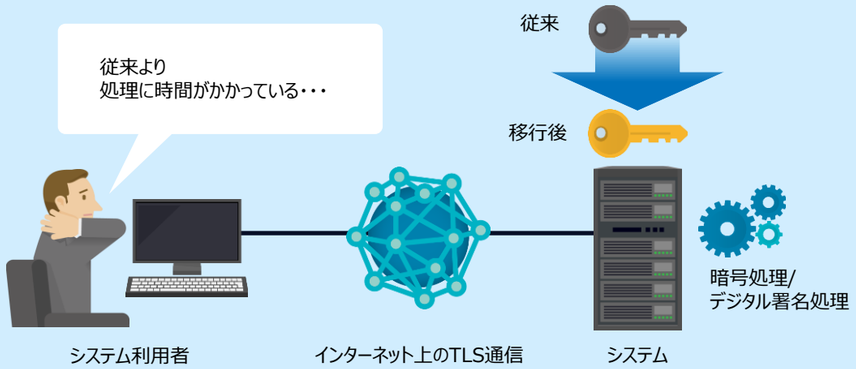
PQCの各アルゴリズムにおいては、従来の暗号方式に比べ、鍵データ、暗号化データ、署名データのサイズが大きくなるものがあります。それらのサイズを意識してプログラムを製造しなければ、メモリやICカードなどにデータを正しく格納できず、システムが異常終了する可能性があります（図12）。

図12: 留意点①：データのサイズが大きくなる可能性

● 留意点②：処理速度が遅くなる可能性

PQCの各アルゴリズムにおいては、鍵生成速度、暗号化速度、復号速度などが従来より速くなるもの、または遅くなるものがあります。遅くなる場合、システム利用者が感じる待ち時間が増大し、利便性が低下する可能性があります。TLSのセッション構築を何度も繰り返すような場合や、IoT機器などの省リソース環境では特に注意が必要になります（図13）。

図13: 留意点②：処理速度が遅くなる可能性



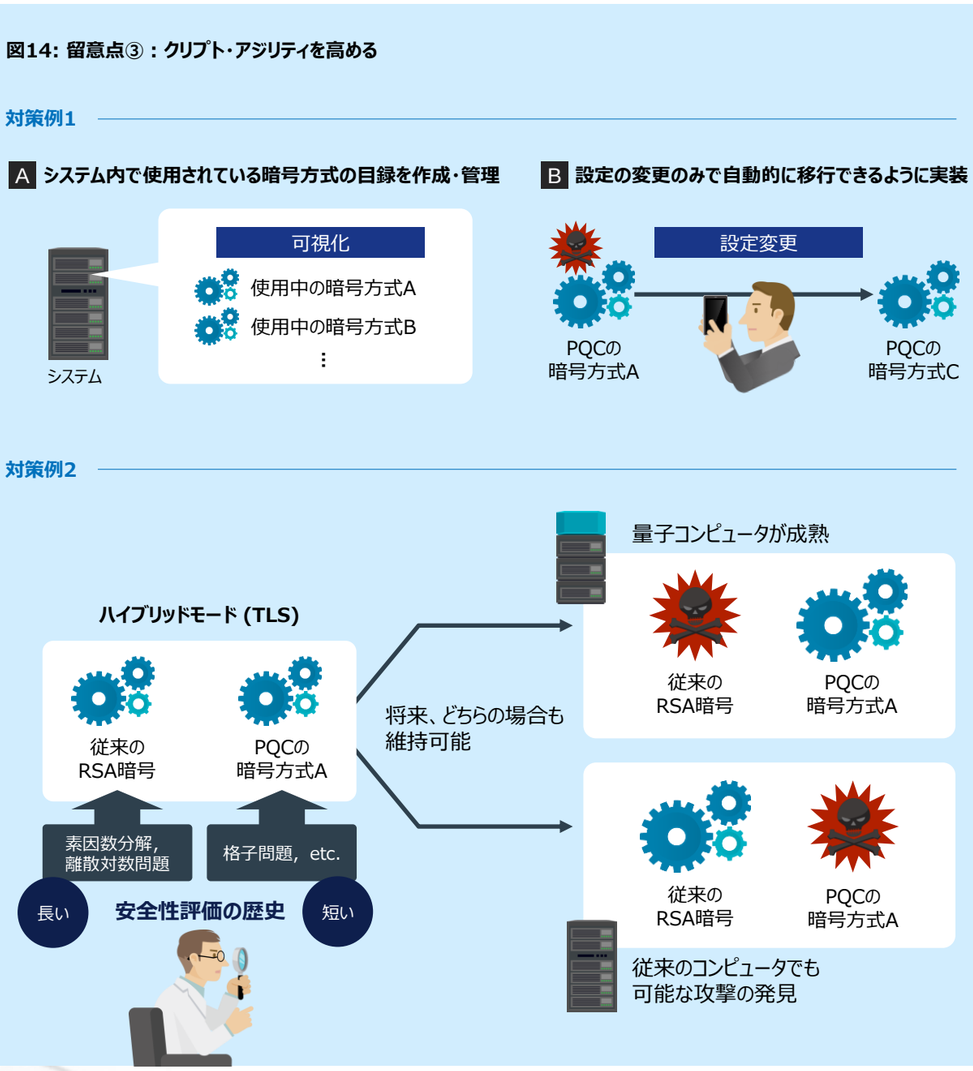
● 留意点③：クリプト・アジリティを高める

PQCの各アルゴリズムの安全性はNISTにより十分に検証されているものの、従来のRSA暗号などに比べればその歴史は浅いため、将来、攻撃が発見される可能性がゼロとは言えません。それを想定した対策例として、以下の2つが挙げられます。

1つ目は、システムで使用されている暗号方式を可視化するとともに、別の暗号方式に容易に移行できるように設計・実装しておくことです。この考え方は、**クリプト・アジリティ（暗号の俊敏性）**と呼ばれます。

2つ目もクリプト・アジリティの一つの実現例ですが、TLSにおいて**ハイブリッドモード**の採用を検討することです。ハイブリッドモードとは、二つの異なる暗号方式を並行化するように組み合わせ、どちらか一方の方式が危殆化により使用不可な状態になっても、安全なもう片方の方式のみでシステムを維持できるようにする概念です。例えば、従来のRSA暗号とPQCのある暗号方式Aをハイブリッドモードで設計・実装すれば、将来RSA暗号が危殆化した場合、および将来PQCの暗号方式Aが危殆化した場合のどちらの場合でも、システムの安全性を維持することができます（図14）。

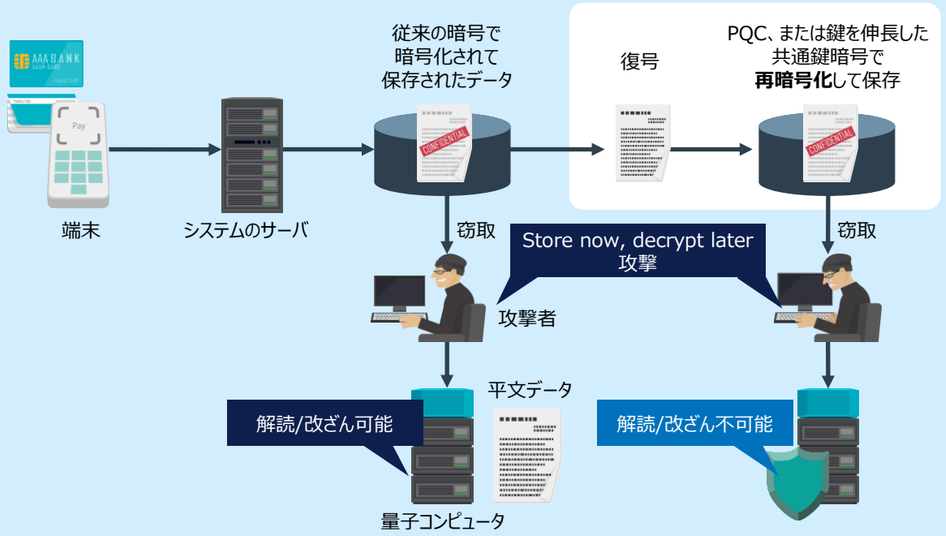
図14: 留意点③：クリプト・アジリティを高める



● 留意点④：暗号化データをシステムに保存している場合、再暗号化の検討が必要

システム内に機密情報などを暗号化して保存している場合（共通鍵暗号の鍵を公開鍵暗号で暗号化して保存している場合を含む）、「Store now, decrypt later攻撃」への対策として、PQC、または鍵を伸長した共通鍵暗号による再暗号化を検討する必要があります（図15）。

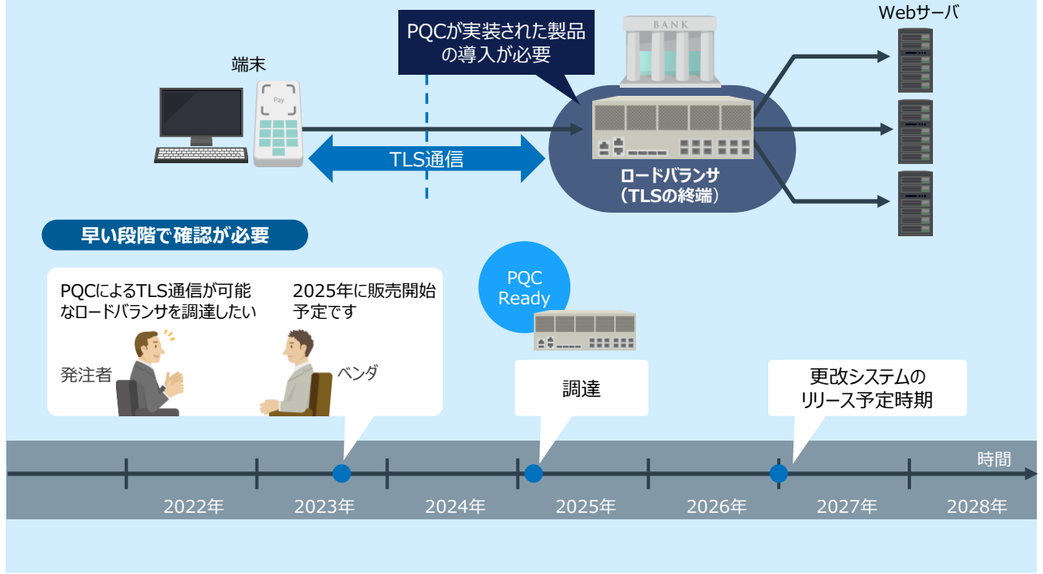
図15: 留意点④：暗号化データをシステムに保存している場合、再暗号化の検討が必要



● 留意点⑤：TLSのハードウェアを使用している場合、その調達は間に合うか？

TLS通信をロードバランサで終端させている場合、暗号ライブラリはロードバランサのハードウェア上に存在するため、PQCに対応するためには、ロードバランサの更新が必要になります。その調達時期を把握し、システム更改に間に合うかを見極めなければなりません。そのためには、早い段階でロードバランサベンダーに販売時期、対応するPQCの暗号方式、鍵長、などを確認する必要があります（図16）。

図16: 留意点⑤：TLSのハードウェアを使用している場合、その調達は間に合うか？

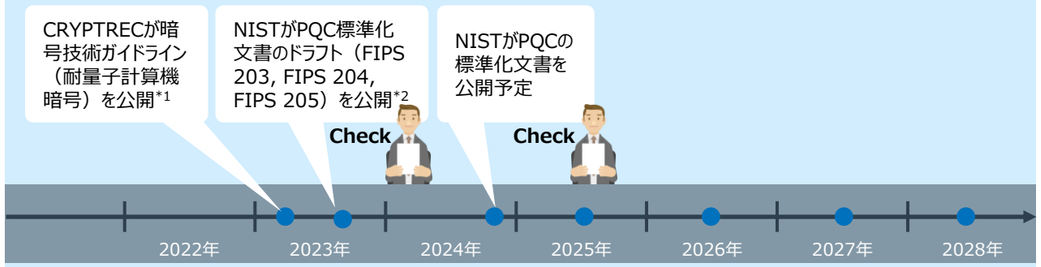


● 留意点⑥：NIST, SOG-IS, CRYPTREC等が公開する情報の継続的な収集

PQCへの移行計画を一度検討した後でも、PQCの安全性評価の更新状況を踏まえ、NIST，SOG-IS，CRYPTRECなどにより公開される情報に注意を払う必要があります。

現時点では、NISTが2024年までにPQCの標準化文書をFIPSとして公開する予定であり、そのドラフトが既に公開されていることから、引き続き最新情報を把握していく必要があります（図17）。

図17: 留意点⑥：NIST, SOG-IS, CRYPTREC等が公開する情報の継続的な収集



*1 CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号），2023年3月.
https://www.cryptrec.go.jp/report/cryptrec-gl-2004-2022.pdf

*2 NIST, Comments Requested on Three Draft FIPS for Post-Quantum Cryptography
https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography

● 留意点⑦：クラウドサービスプロバイダが提供するPQCの機能を把握する

次期システム更改において、システムの全体または一部をクラウドに移行する計画がある場合、そのクラウドサービスプロバイダ(CSP)がサービスとして提供するPQCの機能を活用することも選択肢となり得ます。したがって、CSPが提供する予定のPQC関連サービスの開発計画を把握し、それらを利用するかどうかを決定する必要があります（表8）。

CSPが提供する可能性のあるPQC関連サービスには、鍵管理サービス（KMS）、証明書発行サービス、HSMサービス、暗号化通信サービス、などがあります。それらを利用するのか、サードパーティのPQC暗号ライブラリを利用するのか、またはその両方を組み合わせるのかを検討する必要があります。

表8: 主なクラウドサービスプロバイダが発信するPQCに関する情報

AWS	• AWS Key Management Service (AWS KMS) と AWS Certificate Manager (ACM) が、PQCの暗号アルゴリズムであるCRYSTALS-KYBER, BIKE, SIKEのサポートを開始*1 • AWS Secrets Manager への接続において、従来の鍵共有と、PQCの暗号アルゴリズムであるCRYSTALS-KYBERを組み合わせたハイブリッドモードでのTLS確立のサポートを開始*2 • PQCをさらに推進するために設計されたライブラリ「liboqs」の開発を支援する「Open Quantum Safe Project*3」に参加*4
Google	• GoogleがNISTのPQC標準化に応募したSPHINCS+が標準に選定された。さらに、2つの応募Classic McElieceおよびbikeは、第4ラウンド評価に進んだ。*5
Microsoft	• PQCをさらに推進するために設計されたライブラリ「liboqs」の開発を支援する「Open Quantum Safe Project」に参加*6

*1 AWS,「AWS KMS と ACM が最新のハイブリッドポスト量子 TLS 暗号のサポートを開始」，2022年3月16日.
https://aws.amazon.com/jp/about-aws/whats-new/2022/03/aws-kms-acm-support-latest-hybrid-post-quantum-tls-ciphers/
*2 AWS,「AWS Secrets Manager 接続で Kyber による最新のハイブリッドポスト量子 TLS のサポートを開始」，2022年8月2日.
https://aws.amazon.com/jp/about-aws/whats-new/2022/08/aws-secrets-manager-connections-support-hybrid-post-quantum-tls-kyber/
*3 The Open Quantum Safe (OQS) project
https://openquantumsafe.org/
*4 AWS, Post-Quantum Cryptography, Bringing quantum-resistance to AWS services and customers
https://aws.amazon.com/jp/security/post-quantum-cryptography/
*5 Google,「Google によるポスト量子世界に向けた準備」，2022年7月12日.
https://cloud.google.com/blog/ja/products/identity-security/how-google-is-preparing-for-a-post-quantum-world
*6 Microsoft Research, Post-quantum Cryptography
https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/

4. いつ、どうやって移行するか

Moscaの定理

米国NISTは、PQCへの移行の緊急性を直観的に理解するための**Moscaの定理**を紹介しています。Moscaの定理は、カナダ Waterloo大学の Michele Mosca 教授により提唱されました。

Moscaの定理では、*x*, *y*, *z* を以下の年数と定義します。

- *x*: その時点の暗号技術により、データが秘匿されていてほしい年数
- *y*: 量子コンピュータの攻撃に対し、安全な暗号インフラの構築に必要な年数
- *z*：既存の暗号を破る量子コンピュータの出現にかかる年数

このとき、「$x + y > z$」であるならば問題であり、PQCへの移行を検討する必要があると考えます（図18）。

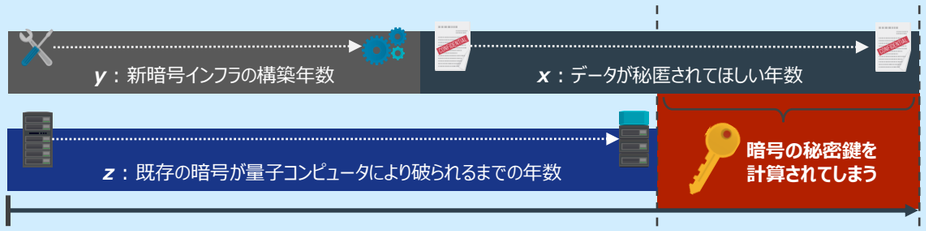
なぜなら、今から *y* 年後に「安全保存期間：*x* 年」として暗号化されるデータが、今から *z* 年以降に、その安全保存期間 *x* 年を満たさずに量子コンピュータにより解読されることが起き得ることになるためです。

図18: Moscaの定理

Moscaの定理：

x	その時点の暗号技術により、データが秘匿されていてほしい年数
y	量子コンピュータの攻撃に対し、安全な暗号インフラの構築に必要な年数
z	既存の暗号を破る量子コンピュータの出現にかかる年数

のとき、$x + y > z$ ならば、問題である。



出典：NIST, The Beginning of the End: The First NIST PQC Standards
https://csrc.nist.gov/csrc/media/Presentations/2022/the-beginning-of-the-end-the-first-nist-pqc-standa/images-media/pkc2022-march2022-moody.pdf

例）

- 電子データの定められた保存期間により、データが秘匿されていてほしい年数を25年とした。（*x*=25）
- これまでのインフラ開発の経験を基に、PQC暗号対応インフラの構築に必要な年数を20年と予測した。（*y*=20）
- RSA暗号を破る量子コンピュータは現在から30年後に出現し普及すると予測した。（*z*=30）

***x* + *y* = 25 + 20 > 30(=*z*)であるため、耐量子計算機暗号への移行検討が至急必要である。**

Migration to Post-Quantum Cryptography

既存の暗号技術から耐量子計算機暗号へ円滑に移行する方法として、
NTTデータグループは「PQCへの移行プロセス」を定義しました。

PQCへの移行プロセス

1 現状把握

- ITシステム上で暗号化された情報に何があるか、およびその情報の所在を特定します。
- 現状の暗号アルゴリズム、鍵長、共通鍵暗号の場合はその「暗号利用モード」、などの暗号仕様を把握します。
- 移行に伴う影響を評価します。**（留意点①、②）**

2 優先順位付け

- ITシステム上で保持する情報の機密性・重要性、および安全に保存すべき期間を評価し、移行すべき対象の優先順位付けを行います。
- Moscaの定理により、「Store now, decrypt later攻撃」の影響、および移行の要否も考察します。

3 移行時期の検討

- ITシステム上で暗号化され保存されているデータの再暗号化が必要かを検討します。**（留意点④）**
- TLS通信をロードバランサーで終端する場合、PQCに対応するロードバランサーの調達可能時期を把握します。**（留意点⑤）**
- お客様および開発プロジェクトにおいて、ガントチャートにより計画を可視化し、移行イメージのすり合わせを行います。

4 移行方法の検討

- クリプト・アジリティを開発プロセスに導入します。また、TLS通信に、従来の暗号方式とPQCの暗号方式とのハイブリッドモードを適用するかを検討します。**（留意点③）**
- NIST, SOG-IS, CRYPTRECなどの最新のガイドラインを参考に、採択すべきPQCの暗号アルゴリズム・鍵長を決定します。**（留意点⑥）**
- クラウドサービスプロバイダが提供するPQCの機能を活用するか、サードパーティまたはOSSのPQC暗号ライブラリを活用するか、またはその両方を活用するかを検討します。**（留意点⑦）**

NTTデータグループは

お客様のPQCへの移行を支援します

情報技術の急速な発展により、私たちの生活やビジネスはますますデジタル化され、データの重要性が増しています。企業は多くの機密情報を取り扱うようになり、それらの情報を守ることは必要不可欠です。サイバーセキュリティに対するリスクマネジメントは重要な経営課題の一つとなっています。

現在のITシステムに使用されている暗号技術は、量子コンピュータの発展に伴い、将来的に解読される可能性があります。よって、耐量子計算機暗号（PQC）への移行は、機密情報を取り扱う企業にとって重要な課題となります。企業は量子コンピュータの発展を見据え、PQCへの移行に対して適切な計画を持つ必要があります。

NTTデータグループは、先進のテクノロジーで、先見の事業変革をお客さまとともに実現します。さらに、ビジネスイノベーションや社会的課題の解決をともに実現していくことで、お客さまから長期的に信頼されるパートナーとなることを目指します。お客様の情報を守るため、PQCを含む暗号技術全般に関する豊富な知識と経験を持つエキスパートを揃え、これまで培った経験を活かし、お客様のPQCへの移行を支援いたします。