また、ニューラルネットワークを中心とした人間の知能の根底には、量子学的な現象があることを示唆する研究成果も報告されており、現在の小規模量子ビットの量子コンピュータ（IBM Q Experience）で動作する、人工ニューラルネットワークに関する AI アルゴリズムの開発も行われている https://iopscience.iop.org/article/10.1088/2058-9565/abb8e4/pdf。

100 万量子ビットを超える実用的な量子コンピュータの実現は、Google や IBM のような有力開発企業のロードマップを考慮すると、2030 年前後になると予想されている。しかし、既存のスーパーコンピュータと量子コンピュータをハイブリッド利用するコンピューティング（ハイブリッドコンピューティング）の研究開発が現在盛んに進められており（図 5-2）、それらは実際に利用しながら進化していくと考えられる。日本においても経済産業省で「量子・古典ハイブリッドコンピューティングの基盤ソフトウェア開発」として 2022 年度補正予算を提案しており、2023 年度には「量子・AI ハイブリッド技術のサイバー・フィジカル開発事業」として量子・AI 融合型コンピューティングシステムによるアプリケーション開発を実施するとともに、ユースケースの創出を推進していく予定である https://www8.cao.go.jp/cstp/ryoshigijutsu/13kai/siryo2-4.pdf。

この様な流れからハイブリッドコンピューティングの活用は数年以内に始まり、今後は、量子機械学習の PoC が盛んに行われるだろうと考えられる。AI 業界をリードする Google は、量子技術を AI に応用するフレームワークとしてハイブリッドコンピュータを応用した TensorFlow Quantum（TFQ）を提供している。TFQ は、量子と古典のハイブリッド 機械学習 モデルのラピッド プロトタイピングのための量子機械学習ライブラリである。量子アルゴリズムとアプリケーションの研究では、すべて TensorFlow 内から Google のフレームワークを活用されている。 https://www.tensorflow.org/quantum。

これらハイブリッドコンピュータの進化は、量子コンピュータ単体より早期に実現でき、それぞれの利点を生かした計算処理の分担を行えるため、非常に有効な計算手段となる。これは、同時にサイバーセキュリティを考える上でも、重要な要因であるため早急に検討が必要となる。

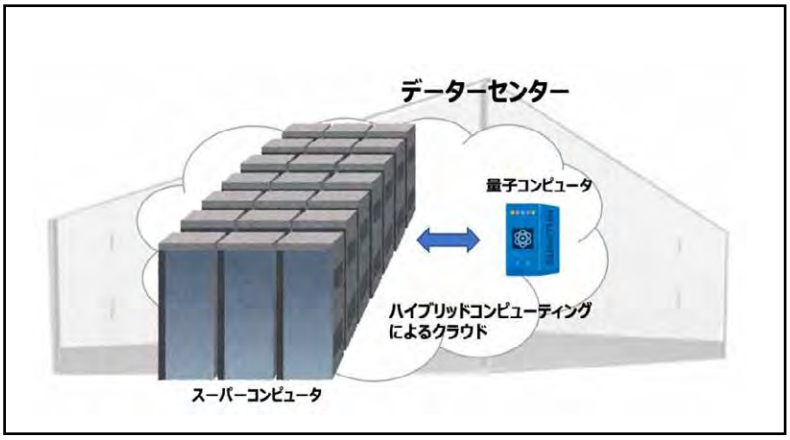



図 5-2　ハイブリッドコンピューティングのイメージ

## 第４節 暗号と量子コンピュータ

■PQC（Post-Quantum Cryptography）

表 5-2 は、2009 年から 2018 年まで 10 年間の各国の量子コンピュータの研究費推計を纏めたものである。前項（図 5-1）の 2021 年の投資額と比較すると、特に中国の変化が著しく大きい。これは、2020 年前後に急激な進化を遂げだす量子コンピュータの進化の変曲点が大きく影響しているものと思われる。

量子コンピュータは、ビットの「量子の重ね合わせ」と「量子もつれ」を利用し、量子コンピュータ用のアルゴリズムを利用することにより処理が大幅に高速化するため、暗号を直接解読することや、暗号鍵の発見に必要な時間を短縮することが可能になる。現在の量子コンピュータは、まだ量子ビットの少ない開発の初期段階であるが、2030 年以前には、RSA 等の公開鍵暗号は瞬時に解読可能になると予測されている。現在、AES に対しては、指数的に高速に鍵を発見できる量子アルゴリズムである Grover のアルゴリズムが開発されているが、鍵の解読に対して更なる脅威を与えるほどの強力で持続的な処理を実行できるアルゴリズムは、現在まだ発表されていない。しかし、現在進行中の量子コンピュータの研究は、そのような解読処理を実現できるよう進化する可能性がある。（既に水面下での開発で実現されているかもしれないという考え方もある。仮に暗号解読が可能になった量子コンピュータを実現できたとしても、自国の優位性を保つためには、絶対に公開することはない

米国の NIST（米国国立標準技術研究所）や各国のサイバーセキュリティ関連組織は、盗聴者が現在、暗号化されたデータを盗聴（ダウンロード）し、量子コンピュータ等の解読可能なコンピュータを実用化できた途端に復号化する「steal-now and decrypt-later 攻撃」を想定しており、既に、現時点での通信インフラの安全性に対して懸念を抱いている。そのため現在利用している標準暗号を今後も使用し続けるシステムは、セキュリティが侵害される危険性があると考えている。米国の National Security Memorandum 10（NSM10：国家安全保障覚書）は、この予測を見越して、その対策について要件を示しており、NIST は、量子耐性暗号（QRC：Quantum Resistant Cryptography）標準に関する新たなプロジェクトを開始している。（後述で詳細説明）

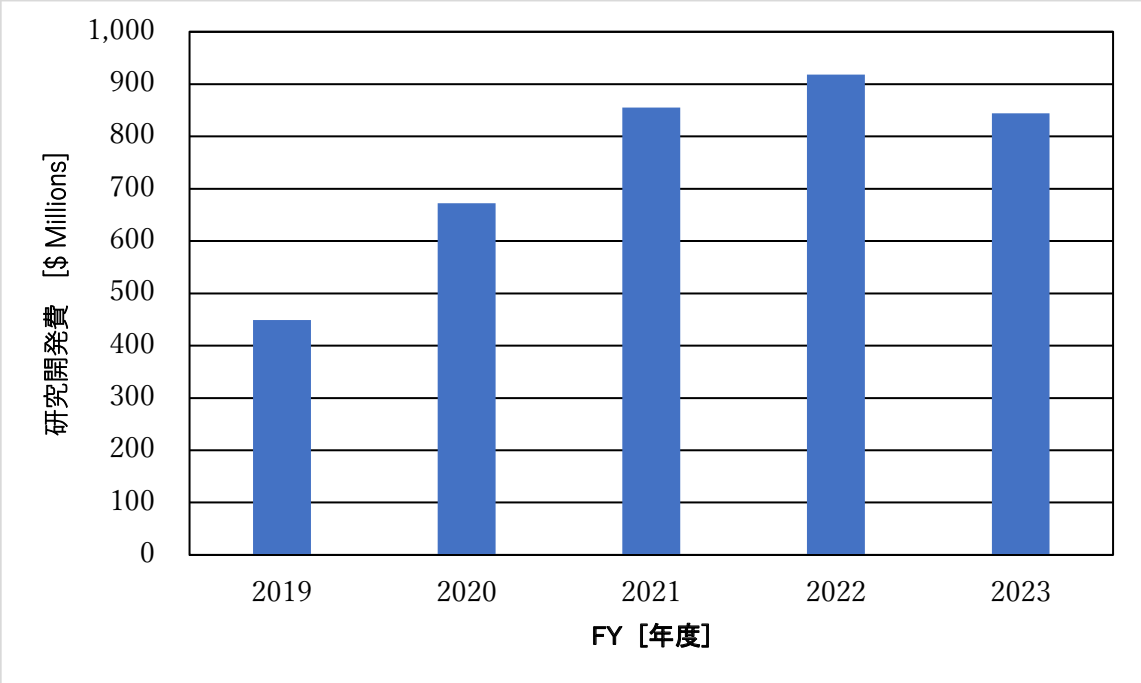
https://crsreports.congress.gov/product/pdf/IN/IN11921/1

表 5-2　主要各国が 10 年間に注いだ量子コンピュータ関連技術の研究費推計（2009 年～2018 年）

| 国 名 | 量子コンピュータ<br>関連技術全体 | 量子ビット<br>集積化・システム化 | 量子コンピュータ<br>クラウドサービス | 量子コンピュータ<br>製造技術 |
|---|---|---|---|---|
| 米 国 | 1060 | 520 | 320 | 640 |
| 英 国 | 830 | 640 | 430 | 760 |
| 中 国 | 630 | 340 | 110 | 280 |
| 豪 州 | 300 | 160 | 140 | 150 |
| 日 本 | 230 | 80 | 50 | 120 |

US＄　Millions

表 5-2 は、2009 年から 2018 年まで 10 年間の各国の量子関連技術研究投資総額である。また、図 5-3 に示すように米国においては、量子情報科学の予算は、2019 年に 400M$強であり、2022 年の要求額は、900M$弱と倍増している。




https://quantumcomputingreport.com/u-s-qis-budget-proposed-to-grow-10-6-to-877-million-in-fy2022/

図 5-3　米国の量子情報科学の研究開発予算

量子技術の中でも、特に情報通信におけるセキュリティに大きく関与する量子コンピュータ開発は、加速しており、開発投資も長期的に増大していくと考えられる。そのため情報通信の安全性を維持するための対策の緊急性と早期実現（実装）が重要である。現在、米国の NIST で行われている耐量子計算機暗号（PQC：Post Quantum Cryptography）の標準化も、その一連の危機感の流れである。

日本においても、量子コンピュータと現代暗号の安全性の関係を理解し、量子コンピュータの技術課題に対する考え方を多角的に調査し俯瞰的な視点で開発ロードマップを予測し、最悪のケースを考えた対応策の推進が重要である。数理的なソフトウェア暗号においても、物理的な暗号においても実装し整備するには時間がかかるため先行した早期対策が必要である。

■量子コンピュータの開発をリードする IBM の状況（図 5-3）

現在、一般的に入手可能な情報の中で、最も進んでいると思われる量子コンピュータ開発グループは、IBM である。既に 2021 年に実用化している 53 ビットクラスの量子コンピュータは、日本を始め、世界中で稼働し、量子コンピュータアルゴリズムやソフトウェア開発に利用され出している。量子コンピュータの性能を表す量子ビット数も今年（2022 年）に 128 ビットを達成し、更に 400 ビットクラスのデバイスの集積化も実現（IBM Osprey プロセッサー）しており、2023 年には、400 ビットクラスの量子コンピュータが、リリースされる予定になっている。このデバイスは、IBM の量子プロセッサの中でも最大の量子ビット数（433 ビット）であり、古典的なビットの数に単純換算すると $2^{433}$ ビット相当となるため（量子コンピュータの量子ビット数は、古典コンピュータと違い、1 ビット増えるごとに、指数的に計算能力が向上する）、利用シーンによっては、古典コンピュータの計算能力をはるかに超えるポテンシャルを持つ。更に、従来、プロセッサとの信号の接続は同軸ケーブルを利用していたが、極低温下でも動作するフラットケーブルに変更している。また、量子回路の状態を途中で観測して、マルチレベル配線を利用した信号ルーティングとデバイスレイアウトを柔軟に対応できるよう回路の変更が可能な「動的回路」も搭載する。更に、ノイズを低減して安定性を向上させるための統合フィルタリングも追加されている。

2023 年には 1121 量子ビットの「Condor」を発表する予定であり、同時期に、周辺の高周波部品の高密度化も実行される。更に新たにモジュール化の概念を導入した量子プロセッサ、「Heron」も公表する。また、量子と従来のワークフローをシームレスに統合するハイブリッドクラウドミドルウェアを採用しながら、スケーリングを可能にし、「量子通信」と「計算」を組み合わせて計算能力を向上させるモジュラーコンピューティングアーキテクチャである量子中心のスーパーコンピュータの実現を開始すると宣言している。2024 年には 1,386 量子ビット以上となる見通しの「Flamingo」を公開する計画である。これらは、モジュール化の概念を導入しており、複数のチップ間を 1m 以上の電気配線で結んだ製品となる見通しだ。同年には複数のプロセッサ同士を短い配線で接続した「Crossbill」も公開する予定である。2025 年には、4,158 量子ビットの「Kookaburra」を公開し、それ以降も量子ビット数の向上に取り組む方針である。

一方、課題である誤り訂正技術においては、ハードウェアとソフトウェアの技術を組み合わせることで、実用的なアルゴリズムが動作するようになる。古典コンピュータのリソースを量子コンピュータと協調動作させることで、複数のタスクを実行しても誤りを抑制できる技術の実装などが進む。また IBM で

は、長時間かけて量子回路の計算を実行する際にエラーの発生頻度を抑えるため、実行単位を小さく分けつつ古典コンピュータのリソースで相互につなげる、「回路編み（サーキットニッティング）」の技術についても研究を進めている。

<table>
<tr><th></th><th>2019</th><th>2020</th><th>2021</th><th>2022</th><th>2023</th><th>2024</th><th>3025</th><th>2026+</th></tr>
<tr><td></td><td>IBMクラウドで<br>量子回路を実行</td><td>量子アルゴリズムと<br>アプリケーションを<br>実証および<br>プロトタイプ</td><td>Oiskitランタイムで<br>Quantumプログラム<br>を100倍速く実行</td><td>Qiskitランタイムに<br>ダイナミックサー<br>キットを持ち込んで、<br>より多くの計算の<br>ロックを解除</td><td>柔軟なコンピュー<br>ティングとOiskitラ<br>ンタイムの並列化に<br>よるアプリケーショ<br>ンの強化</td><td>スケーラブルなエ<br>ラー軽減により、<br>Oiskitランタイムの<br>精度を向上</td><td>oiskitランタイムを<br>制御する回路編み<br>ツールボックスを使<br>用したスケール量子<br>適用</td><td>エラー補正のOiskitラ<br>ンタイムへの統合によ<br>り、量子ワークフロー<br>の精度と速度を向上</td></tr>
<tr><td rowspan="2">カーネル開発</td><td colspan="2" rowspan="2">回路</td><td rowspan="2">Oiskit ランタイム</td><td colspan="5"></td></tr>
<tr><td>動的回路</td><td>スレッドプリミティブ</td><td colspan="2">エラーの抑制と軽減</td><td>エラー訂正</td></tr>
<tr><td>システム<br>モジュール化</td><td>ファルコン<br>27量子ビット</td><td>ハミングバード 65<br>量子ビット</td><td>イーグル<br>127量子ビット</td><td>オスプレイ<br>433量子ビット</td><td>コンドル<br>1,121量子ビット</td><td>フラミンゴ<br>1,386+量子ビット</td><td>クッカブラ<br>4,158+量子ビット</td><td>古典的および量子的な<br>1万-10万 量子ビット<br>へのスケーリング<br>コミュニケーション</td></tr>
<tr><td colspan="5"></td><td>ヘロン<br>133量子ビット x p</td><td>クロスビル<br>408 量子ビット x p</td><td colspan="2"></td></tr>
</table>

https://jp.newsroom.ibm.com/2022-11-10-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

図 5-3　IBM の開発ロードマップ

このような量子コンピュータの進化が、今日のデータ通信の暗号を解読する能力を持つため、新しい暗号システムへの移行が必要である。但しこれには前述の様に時間がかかるため、今から準備を開始することが重要である。2016 年以降、IBM は NIST と協力して、量子コンピュータの脅威に備えるため PQC の標準化にも協力してきている。

2022 年 7 月に NIST は、PQC の 4 つのアルゴリズムを標準化した。これらのアルゴリズムのうちの 3 つ IBM がサポートし開発された。現在 IBM では、この専門知識を業界にもたらし、PQC への移行に向け、ユーザーに IBM Quantum Safe オファリングを提供しており、IBM とボーダフォンは、ボーダフォンと通信業界が量子耐性のある暗号に移行する準備を整えている。

上記の内容を踏まえて、改めて量子コンピュータの性能予測を纏めると、図 5-3 で示したようなロードマップの実現性は高いと考えられる。

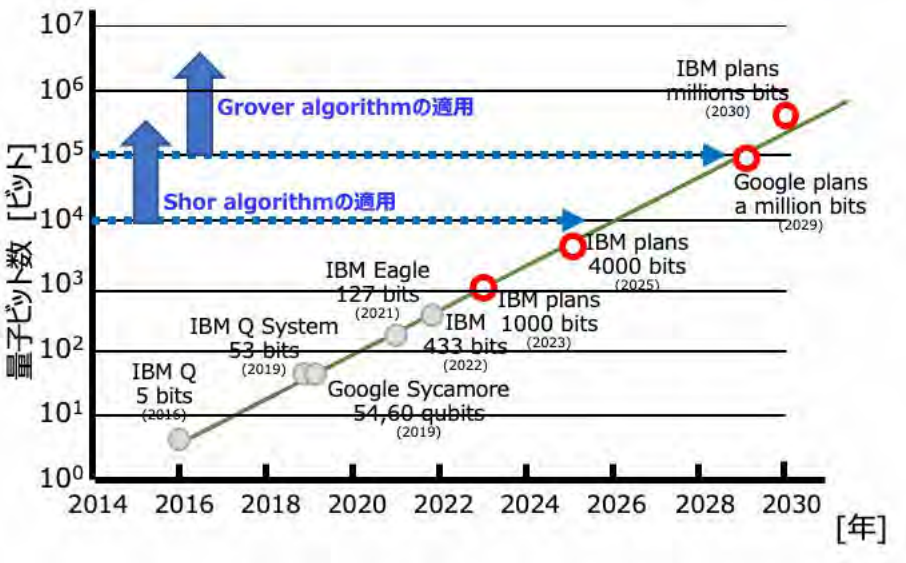



図 5-4　コンピュータの性能予測

現在、既に研究開発されている量子コンピュータ用の代表的なアルゴリズムである Shor のアルゴリズムと Grover のアルゴリズムを使うと、IBM、Google のロードマップ上でも、2030 年前後には、現在主流の公開鍵暗号の RSA や共通鍵暗号の AES は解読されてしまう可能性が非常に高くなる。Shor のアルゴリズは、1994 年、Grover のアルゴリズムは 1996 年に発明されており、まだ量子コンピュータが実現される以前に開発されたものである。現在の利用可能な量子コンピュータは、小規模ではあるが実際に操作させ、クラウド上で利用できる様に運用されているため、実機を利用した更に高度なアルゴリズムの開発も進んでいくと考えられる。(図 5-4)

光ファイバの盗聴においては、前回（2021 年度）報告した様に、光ファイバケーブルから簡単に盗聴することが可能である。工事などを装い、ターゲット拠点近くの通信用マンホールからとう道などへ侵入し、目的の光ファイバケーブルにアクセスしタッピングすることや、架線においては、架線工事を装いユーザー拠点に引き込まれている目的の光ファイバをタッピングすることで信号を確実に抜き取ることが可能である（図 5-4)。

盗聴で得られる信号は、非常に小さく、利用者には気付かれることなく抜き取り続けることも可能であり、この小さな信号は、光ファイバアンプを利用し元の信号を復元することが容易にできる。抜き取った信号が暗号化されている信号であったとしてもそのまま保存することができる。これらの情報は、大規模計算が可能な量子コンピュータが実現できると解読することが可能になる。これが前述の「steal-now and decrypt-later 攻撃」である。

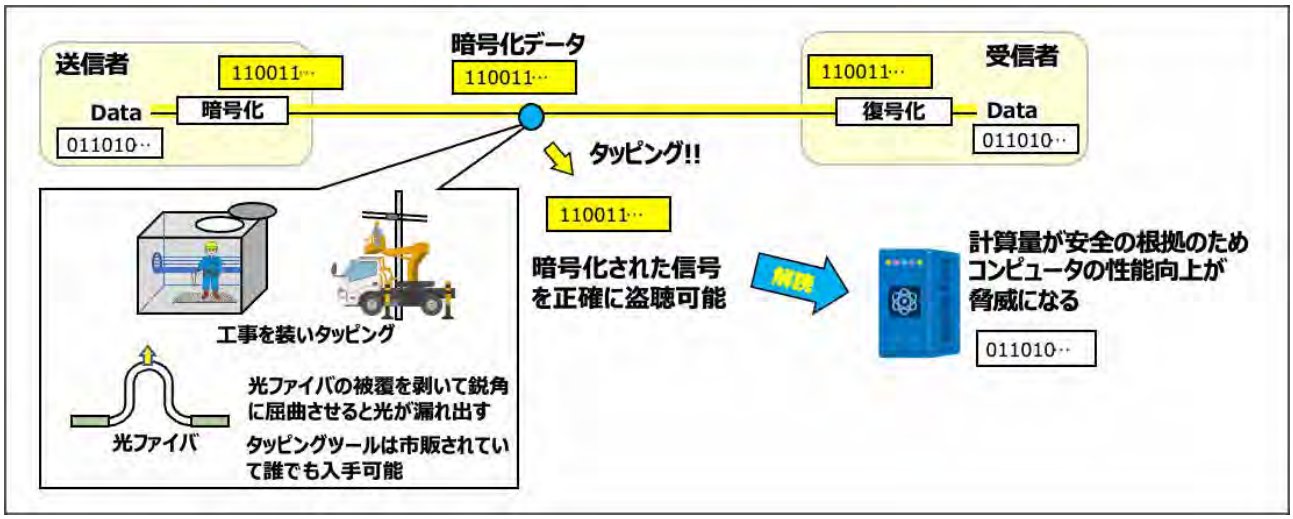



図 5-5　光ファイバの盗聴

前述の様に、IBM を筆頭に、量子コンピュータの開発は、激化しており、また様々な課題に対する隘路事項も同時に解決できる道筋が着実に示されてきており、大規模計算が可能な量子コンピュータの開発において IBM や Google のロードマップを無視する訳にはいかない。

大規模な量子コンピュータが実現できると今日の公開鍵暗号の標準である RSA と楕円曲線暗号は shor のアルゴリズムで破ることができ、ハッカーが次のことが可能になるためデジタル化された経済は機能しなくなる。

・人々の銀行口座や仮想通貨のウォレットを空にする
・機密性の高い通信の傍受と復号化か可能になる
・電力網や通信ネットワークなどの重要なインフラを無効にする
・秘密にしておきたい事実上すべての秘密を暴露する

https://www.insidequantumtechnology.com/news-archive/quantum-news-briefs-september-26-cheng-the-path-to-pqc-migration-biden-administrations-newest-sanctions-on-russia-and-belarus-include-a-ban-on-quantum-computing-pritzker-molecular-engineering-pr/

現在、大規模な量子コンピュータの実用化タイミングは多くの議論があり、多くの予測は 20 年以上先であるとの意見が多い。しかし、脅威は商用量子コンピュータの実用化ではない。クローズドされた実験室等の条件下で進められている暗号解読を可能にするような技術開発の可能性である。それは商用ベースよりもはるかに早くに実現できると考えられる。また、このようなコンピュータが実現できているとしても自国の優位性を保つためには決して公開されることは無い。

以上の様に、我々の情報は、現在既に「盗聴と蓄積」の脅威に曝されているかもしれない。収拾された情報には、政府の秘密、R&D イノベーション、金融サービスの取引データ、および戦略計画等が含まれる可能性がある。いくつかのファイブアイズ・エージェンシーもこの現象がより頻繁になっているとコメントして

いる（特に米国政府は、この脅威に対しては重要視している）

耐量子コンピュータ対策として既存の暗号を利用しているインフラを新たな暗号（PQC など）へ移行するには、ソフトウェアベースでもインターネットに接続する殆どの電子機器の変換が必要になるため、少なくとも 10 年以上かかると推定されている。

2021 年度の光ファイバケーブルの普及率は、58.2%であり、日本政府は、「デジタル田園都市国家構想」の基本方針案では、2027 年度末までに光ファイバ回線を 99.9%の世帯へ普及させるとしている。更に、ファイバケーブルの国内カバー率は、2023 年度までに 99.9%以上を目標にしている。

https://www.cas.go.jp/jp/seisaku/digital_denen/dai8/shiryou2.pdf

https://www.soumu.go.jp/main_content/000803507.pdf

また、島国である日本の国間は、主に光海底ケーブルを利用して世界中に接続されている。光海底ケーブルの盗聴事例は、いくつか報告されている。

光ファイバケーブルは、現代の情報化社会活動において欠かすことができない通信インフラの中心的な役割を担っている。このように一般社会活動においても通信インフラに対する安全保障は重要であり早急に対策する必要がある。

## 第５節 各国の耐量子コンピュータへの取り組み

【米国の PQC の取り組み】

米国の NIST では、2016 年から量子コンピュータの暗号解読を想定した、量子コンピュータの計算能力に耐性のある耐量子計算機暗号（PQC：Post Quantum Cryptography）の公募を開始している。ここで提案されている暗号は公開鍵暗号に置き換わるものであり、認証や鍵共有（鍵配送）に適用するものである。

現在、第３ステージを終了し４つの暗号が標準化に採択された。また、更に、鍵配共有を主とする公開鍵暗号（KEMs）においては４つの暗号が最終候補として残っている。

表 5-3　第３ラウンドで標準化が決定した暗号アルゴリズム（2022 年 7 月 5 日）

| 目的 | 暗号 |
|---|---|
| 公開鍵暗号/KEMs<br>（Public-Key Encryption/KEMs） | CRYSTALS-KYBER：クリスタル：ケイバー |
| デジタル署名<br>（Digital Signatures） | CRYSTALS-Dilithium：クリスタル-ダイリチウム<br>FALCON：ファルコン<br>SPHINCS$^+$：スフィンクス$^+$ |

採択された候補は、SPHINCS＋以外は格子暗号系であり、CRYSTALS-KYBER、CRYSTALS-Dilithium が本命である。ただし CRYSTALS-Dilithium は処理が重たいので軽量な FALCON も標準化に残された。また、SPHINCS＋ は、格子方式暗号だけの依存を回避する目的で残された。ただし、格子方式暗号の暗号化、復

号化は、鍵長が長く、処理が複雑で時間が掛かるため、更により軽い暗号化の検討が求められている。このため検討を更に継続し、４つの検討候補として第４ステージで下記の暗号が最終候補として残っている。

表 5-4　（ファイナル）ラウンドで候補として残った暗号アルゴリズム（2022 年 7 月 5 日）

| 目的 | 暗号 |
|---|---|
| Key-Establishment Mechanisms （KEMs） | BIKE<br>Classic McEliece<br>HQC<br>SIKE |

**BIKE** と **HQC** はどちらも構造化された暗号に基づいており、どちらも格子方式に基づかない汎用 KEM として適している。NIST は、第 4 ラウンドの終了時に、標準化のために、この 2 つの候補のうち多くても 1 つを選択する予定している。

**SIKE** は、鍵と暗号文のサイズが小さいため、標準化に対して魅力的な候補であり、更に第 4 ラウンドで安全性の研究し続ける方針であったが、最近（2022 年 8 月）、安全性に重大な欠陥があり、解読可能であるとの論文が報告されたため、今後 NIST で検討継続をするためには、その欠陥を回避する対策が必須である。

https://eprint.iacr.org/2022/975.pdf

”AN EFFICIENT KEY RECOVERY ATTACK ON SIDH （PRELIMINARY VERSION）” WOUTER CASTRYCK AND THOMAS DECRU imec-COSIC, KU Leuven）

**Classic McEliece** はファイナリストであったが、現時点では、まだ標準化されていない。Classic McEliece は、既に安全であると広く見なされているが、公開鍵のサイズが大きいため、使用するソリューションは、限定的と考える。しかし第 4 ラウンドでは、標準化に採択される可能性がある。

NIST は、PQC を現在の暗号のように、様々なソリューションやシステムで利用したいと考えており、そのためには、更なる軽量化が必要であり、2022 年８月に新しいアルゴリズムの公募を開始している。同時に NIST は、格子アルゴリズムに基づかない新たな追加の汎用署名スキームを公募している。これは、証明書の透明性などの特定のアプリケーションでは、短い署名と迅速な検証を備えた署名スキームが必要なためである。

NIST は、格子アルゴリズムベース以外の暗号の追加公募も実施しており、ポスト量子署名標準（post-quantum signature standards）を多様化することを目指している。これらの公募条件を考えると、現在採択されている格子アルゴリズムの暗号だけでは不十分であり、また、実用的に軽量（処理速度の速い）暗号が必要と考えているようである。更に、SIK のように、採択後に安全性に対する弱点や新たな解読手法が確認されるなど、標準された PQC の安全性が保障されていると考えるのは、まだまだ危険である。

https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

https://csrc.nist.gov/projects/pqc-dig-sig

更に、米国 CRS (Congressional Research Service)の INSIGHT Reports によると、米国政府として、2022

年 5 月 4 日にバイデン大統領は、国家安全保障覚書 10 (NSM 10)に署名した。付随する大統領令（Executive Orde：EO）とともに、覚書では、量子情報科学（quantum information science：QIS）における米国のリーダーシップを促進することを目指している。 NSM 10 は、量子コンピュータが「暗号化」されたデータやシステムに与える可能性のある潜在的な脅威にも対処している。

https://crsreports.congress.gov/product/pdf/IN/IN11921

【中国、ロシアの PQC の取り組み】

中国とロシアは、米国を中心に標準化を進めている PQC とは異なる独自のスキームの PQC を検討している。しかし基盤となる考えは、NIST と同様に格子ベースやハッシュベースの暗号スキームである。中国暗号研究協会 (CACR：Center for Advanced China Research) は PQC の公募を開始し、2020 年初頭にその採択結果を発表した。上位の採択結果は、格子ベースの“Aigi-sig”、”LAC.PKE”、および、誤りのある非対称学習 (LWE：Learning with Errors) 問題に基づいている“Aigis-enc”である。

米国 NIST は 2016 年に PQC の公募を開始し、2022 年の 7 月に最初の採択グループを発表し、2024 年までに PQC 標準を公開することを目指している。一方、中国 CACR は、 2018 年に公募を開始し、2020 年に採択を公開した。その報告では、中国は 2022 年中に 独自の PQC 標準化プロセスを開始する予定であり、2025 年頃に商用移行を開始する予定としている。

【標準化について】

一方で、どの様な国でも、国際標準化機構 (ISO) またはインターネット エンジニアリング タスク フォース(IETF)によって設定された国際基準に従うだろうという意見もある。ISO や IETF 以外で独自の規格を開発した場合、世界の他の地域とシームレスにやり取りすることはできなくなるからである。NIST は、既に、これらの国際機関と協力している。これらの標準化団体は、NIST で行っている標準化に対して非常に期待しており、NIST の結果を待ちたいと考えている。まずは、NIST の暗号を国際標準化機関で採用し、その後で NIST 以外の他のアルゴリズムを追加する考えである。しかし、これらの考えは、注意が必要である。標準化暗号は、どこの国でも一般的な商用利用等はあるが、政府や軍、および国内の重要情報は独自暗号を利用すると考えるのが一般的である。そのため、公開する暗号スキームとクローズドする暗号スキームを個別に開発し使い分けて利用すると考えられる。

https://www.sdxcentral.com/articles/analysis/china-russia-to-adopt-slightly-different-pqc-standards-from-us/2022/10/

【中国の PQC】

中国での PQC の取り組みについて、中国科学院の Jiwu Jing から「Research of Post-Quantum Cryptography in China」というタイトルで講演があった。講演内容の抜粋した考え方は以下の通りである。

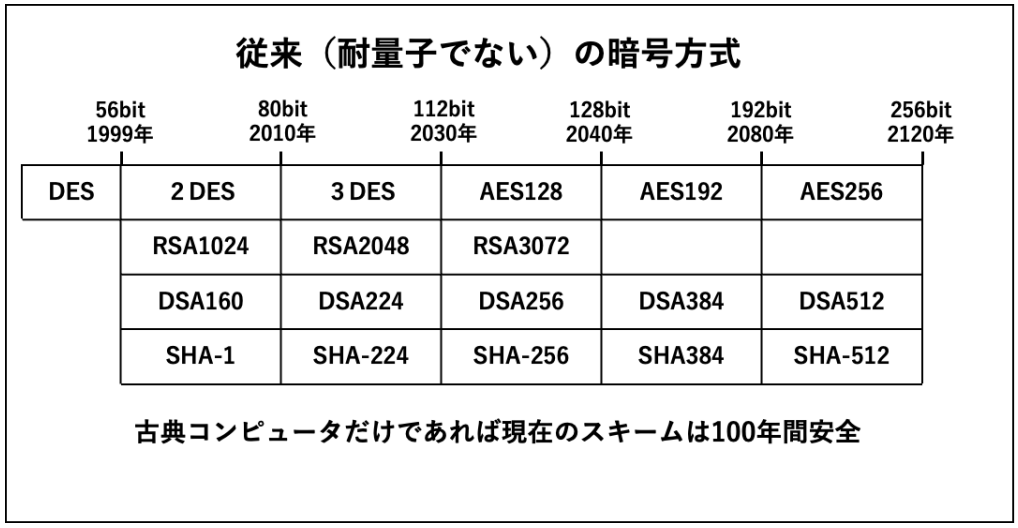



図 5-6　中国の講演資料 1

量子コンピュータが存在しなければ、既存の現代暗号は 100 年間安全である。