預金取扱金融機関の耐量子計算機暗号への対応に関する検討会　御中

耐量子計算機暗号に関する概況と取り組み状況

2024年9月20日

日本アイ・ビー・エム株式会社

※本資料は９月20日の検討会資料に編集上の修正を加えている場合があります。

本日のポイント

- 量子コンピューターは将来のコンピューター像の一翼を担うものとして、今後、新たな価値創出が期待される一方、量子技術の登場により新たに顕在化する脅威（既存の情報資産を守っている暗号が解読、重要なデータが流出・改ざん・悪用される脅威）も、サイバーセキュリティーの新たな視点として指摘されています。

- これまでとは大きく異なる考えの下での備えが必要となる中、米国では、政府および国立標準技術研究所（NIST）が耐量子の暗号アルゴリズムの標準仕様の策定を進め、2024年8月、重要な節目としてのマイルストーンを達成したことを正式に発表。重要な安全保障の問題意識の下、海外では取り組みも加速し、政府・業界団体・民間企業が連携して具体的な取り組みを推進し、様々なエコシステムも登場しています。

- 本日は、IBMにおける耐量子計算機暗号に関わる認識概況と取り組み状況をご報告させていただきます。

量子・耐量子暗号推進：西林 泰如　理事 パートナー

IBM先進テクノロジービジネス・戦略コンサルティング・リーダー
兼
IBM Quantum Distinguished Ambassador

理事・パートナー

- 総合電機R&Dおよび戦略企画（半導体、デジタルプロダクツ、社会インフラ）、グローバル戦略コンサルティングファーム戦略グループを経て、IBMへ参画。専門はビジネス戦略と先進テクノロジーに関する、経営企画・経営戦略、事業開発・事業戦略、提携・投資/M&A、海外事業開発（米国ボストン、シリコンバレー、シンガポールにて、6年の駐在）、情報通信・インターネット技術（通信・コンピュータを中心に120 件超の特許*登録発明）。
- IBM では、戦略コンサルティンググループの理事・パートナーとして、先進テクノロジービジネス開発の戦略コンサルティング組織（Advanced Tech Business）のリーダーを務め、量子・耐量子暗号推進（Quantum、Quantum Safe）のリーダーを兼任する。
- 経営層アジェンダのビジネス戦略と先進テクノロジー**を組み合わせたイノベーション創造と実行に強みを有する。
- 先進テクノロジービジネス戦略、グローバル戦略、中期経営戦略/事業戦略、事業構造変革/ビジネスデザイン、クロスボーダーM&A、新規事業開発、DX/GX、などの先進テーマを対象に、製造・流通、銀行・信販、通信・メディア・ハイテク、公共・社会インフラ、ヘルスケア&ライフサイエンス等広範囲の業界への戦略策定・実行のリード多数。
- 工学修士（MEng）、および、経営管理修士（MBA）

- 学歴・資格等
  - 早稲田大学理工学部電子情報通信学科（工学士）、2001年3月
  - 早稲田大学大学院理工学研究科電子情報通信学専攻（工学修士）、2003年3月
  - 早稲田大学大学院商学研究科 専門職学位課程ビジネス専攻（MBA：首席）、2012年3月
  - MIT Sloan School of Management Alumni （Executive MBA）、 2014年4月

*：コンピュータ・サイエンス、コンピュータ・アーキテクチャ、コンピュータ・ネットワーク（含：*Wi-Fi*の規格必須ライセンス特許）
**：*Quantum*、*Quantum Safe*、*AI*、先端半導体 等

量子・耐量子暗号推進：大西克美　技術理事

大西　克美
オオニシ　カツミ
Ohnishi Katsumi

所属部門：
日本アイ・ビー・エム株式会社
IBM コンサルティング事業本部
CyberSecurity Services
プラクティス・リーダー

技術理事
（*Distinguished Engineer*）

セキュリティ*CTO*

＜略歴＞　大学、研究機関担当のお客様エンジニアとして、大規模UNIXシステム、インターネット基盤のプロジェクトを担当。2000年前半より、ITセキュリティーのスペシャリストとして、金融機関等のコンサルティング、アーキテクチャ設計などで活躍。日本アイ・ビー・エムにおけるセキュリティ第一人者として、講演、政府活動、執筆活動など幅広く活躍。現在は自動車・IoTセキュリティ、FinTech・トークンエコノミー領域や新規技術領域（AI、Quantum Safeなど）のメンバーとして活動中。

＜専門領域・得意分野＞

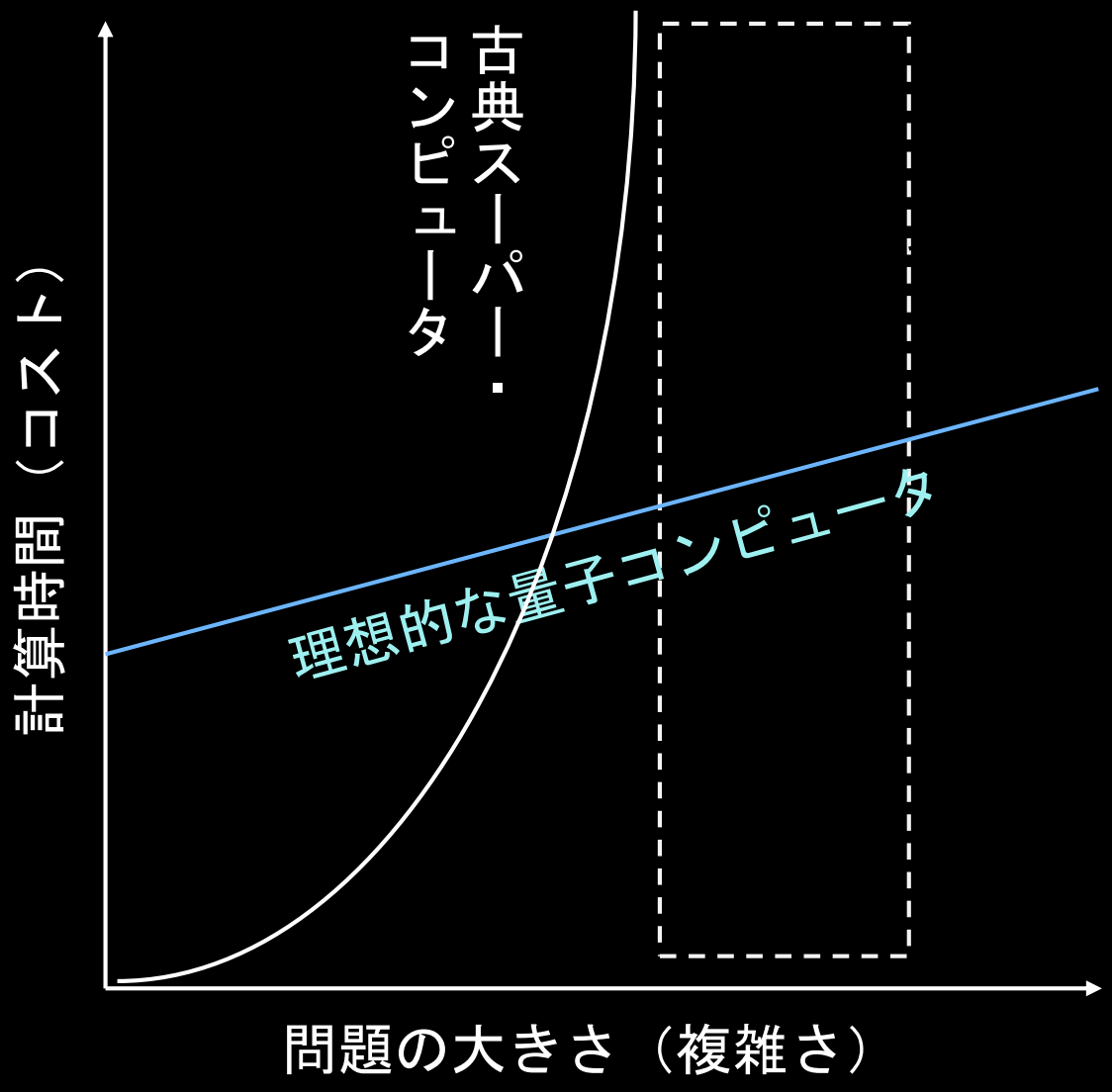
- Security by Design　（Threat Modeling）
- APIバンキング、仮想通貨交換サービス
- IoTセキュリティ（自動車、スマートメーター、複合機）
- WP29 ソリューションニング、ISO21434/ UN-R 155ベースのコンサルティング
- アーキテクチャ設計
- セキュリティ・インシデント対応/対策支援

＜社外活動/ テクニカルエミネンス＞

- 慶應大学、中央大学、東京大学、東北大学、関西学院大学、電気通信大学、立命館大学にて講座
- ソフトウェア・ジャパン講演、情報処理学会全国大会、2014年, 2018年
- “Advanced Security and Privacy in connected vehicles”, IBM Journal of Research and Development 、2014出版
- IBM IBV “生成AIを以って生成AIを制す”
- “IoT セキュリティ”、IBM Provision、2015年出版
- メディアインタビュー（新聞、雑誌寄稿・連載）

耐量子暗号移行に関する概況や現状認識
（最新動向、脅威リスク、時期目安、金融機関様向けの示唆等）

量子コンピューターがもたらす潜在力



問題が極度に大きくなると、最新スーパー・コンピュータでも「事実上解けない」領域があった

理想的な量子コンピュータでは計算の複雑度による計算時間の増大が大きく抑えられるため、問題によっては、この計算不能領域に到達できる可能性がある
将来的に理想とされるゲート型量子コンピュータは Fault Tolerant Quantum Computer （FTQC）、
特に、暗号解読が可能な性能を持つFTQCはCryptographically Relevant Quantum Computer（CRQC）と呼ばれている

<u>量子計算の威力が発揮される例</u>

- 桁数の大きい素数を用いた素因数分解
- 大規模な化学反応のシミュレーション
- 大規模な最適化問題の解決
- 多くの不確定要素を持つリスク解析 等

量子コンピュータのもたらす脅威

暗号鍵が指数関数的速度で解読される。
*米国NISTは「2030年までに暗号鍵長2048*ビットの公開鍵暗号は破られる可能性」を指摘。*

素因数分解を用いた暗号技術とは

公開鍵暗号方式は、桁数の多い合成数の素因数分解を現実的な時間で実施するのが難しいことを利用した暗号方式（計算時間の長さに依存）

25195908475657893494027183240048398571429281262040320277771378360436620207075955562640185258807844069182906412495150821892985591491761845028084891200728449926873928072877767359714183472702618963750149718246911650776133798590957000973304597488084284017974291006424586918171951187461215151726546322822168699875491824224336372590851418654620435767984233871847744479207399342365848238242811981638150106748104516603773060562016196762561338441436038339044149526344321901146575445441784240209246165157233507787077498171257724679629263863563732899121548314381678998850404453640235273819513786365643921201039712282212

2048ビットの公開鍵暗号：現在、広く普及している暗号
合成数：自然数で、1とその数自身以外の約数を持つ数

素因数分解

$= p \times q$

量子計算の威力

今日の最高性能のコンピュータで数10年～100年以上

量子ショア（Shor）のアルゴリズムでは指数関数的高速に解読

暗号 | 認証（鍵交換） | デジタル証明

前提

一般的な暗号技術はコンピューティングの計算能力が向上すると安全性が低下

量子コンピューティングでは
特定の問題を
指数関数的に高速に
解ける可能性

金融機関にもたらされる脅威リスクの例

世界の金融業界団体によって金融業界固有の脅威が特定され、対策の必要性が求められている。

Risk 1：個人を識別できる情報（PII）の漏洩

- APT攻撃（Advanced Persistent Threat）*は、従来の暗号化システムの脆弱性を悪用して、口座詳細や金融資産などの重要な顧客情報に不正アクセスし、データを取得することができる
- 侵害されたデータは、CRQCの実現まで隠されており攻撃の発見が遅れる可能性がある

Risk 2：ホールセール決済システムの認証の脆弱化

- ホールセール決済システムは認証に公開鍵暗号に強く依存。そのため、CRQCの攻撃で合法的な取引を模倣した不正決済を実行される可能性がある
- APT攻撃は中央銀行の決済システムを標的としており対策が必要（例：バングラデシュ銀行やニューヨーク連邦準備銀行への攻撃では、SWIFTネットワークの脆弱性が悪用され不正取引が実行された）

Risk 3：銀行間システムのインターフェースの侵害

- オープンバンキングや相互接続された金融システムの普及により、利便性向上の一方、CRQC攻撃の対象になる可能性も高まっている
- インターフェースの脆弱性に対して攻撃し、複数銀行の機密性の高い金融データや顧客情報、取引記録に不正アクセスされる。相互接続されたシステムを標的としたサイバー攻撃が増加している

Risk 4：分散型台帳技術（DLT）を基にした金融商品の侵害

- DLTの固有のセキュリティも脆弱性をもつ
- CRQCによって、基盤である初期のブロック（ジェネシスブロック）の内容が後から変更されると、その後のブロックの完全性が崩れ、DLTの不変性と透明性を損なう可能性がある。DLTを基にした金融商品は全て脅威にさらされる

Risk 5：金融インフラやシステムへの特権的なアクセス（管理者権限）における認証の脆弱化

- 金融システムの管理者認証は、しばしば公開鍵暗号に依存し脆弱性を持つ
- 一度内部に侵入するとソフトウェアやセキュリティ制御、システム設定を操作することで、従来の検出方法を逃れる詐欺取引の生成が可能となる

Risk 6：消費者決済システムにおける認証の脆弱化

- 消費者の決済システムは、取引の完全性・個人情報の保護を認証プロトコルに依存しており脆弱性をもつ
- 消費者決済への攻撃は、小規模に思われるが、長期的に継続した場合の被害と、消費者からの信頼の構築を踏まえると早期の対策が必要

Risk 7：ソフトウェアの完全性における脆弱化

- デジタル署名はソフトウェアとファームウェアの正当性の検証の基盤となっている。これらの署名は、しばしば公開鍵アルゴリズムに依存しており脆弱性をもつ
- 攻撃者はソフトウェアをコントロールし、重要なシステムに混乱をもたらす（例：SolarWinds事件。IT管理および監視ツールであるソフトウェアを侵害し、政府/民間を含む多数の組織のネットワークに侵入）

Risk 8：金融取引記録の改ざん（企業固有の台帳）

- 企業の内部ITシステムに保存されている金融取引記録は、CRQCによるデータの改ざんなど、信用損失の脅威が存在する
- 資産の所有権を書き換え、不正な取引の実行、取引履歴の変更等、取引記録（台帳）が保証する正確性と透明性を損なう可能性がある

Risk 9：金融取引記録の改ざん（公的な台帳）

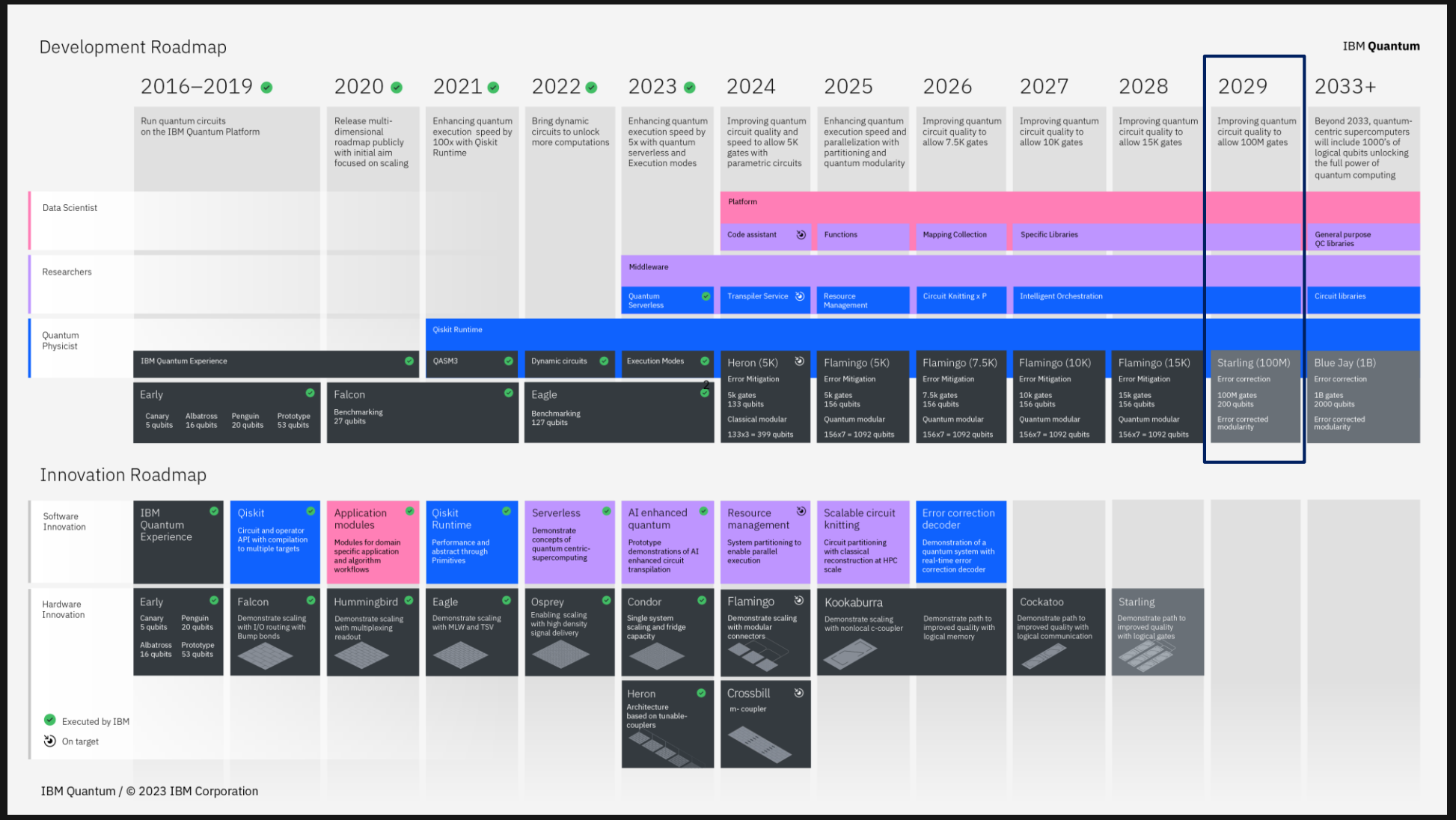
- 土地登記などの台帳に保存される公共資産記録は、不動産の所有権、住宅ローン、および関連する証券の基礎として機能しており改ざんのリスクをもつ
- 所有権や法的権利、公開企業の記録、規制当局への提出書類、およびその他のデータソースも改ざんされる可能性があり、組織がこれらのデータをリスクや融資の意思決定に活用できなくなる

*APT攻撃（Advanced Persistent Threat）：主に国家主導の攻撃で、スパイ行為または妨害工作を遂行するために組織へのセキュリティ侵害を行い、なおかつ長期間検知されないことを目的とした攻撃

出所：UK Finance, "MINIMISING THE RISKS: QUANTUM TECHNOLOGY AND FINANCIAL SERVICES"

（参考）2020年代後半には誤り耐性型量子コンピュータ登場

IBMは2029年までに誤り耐性型量子コンピュータを開発することを計画し、最新のロードマップで発表。

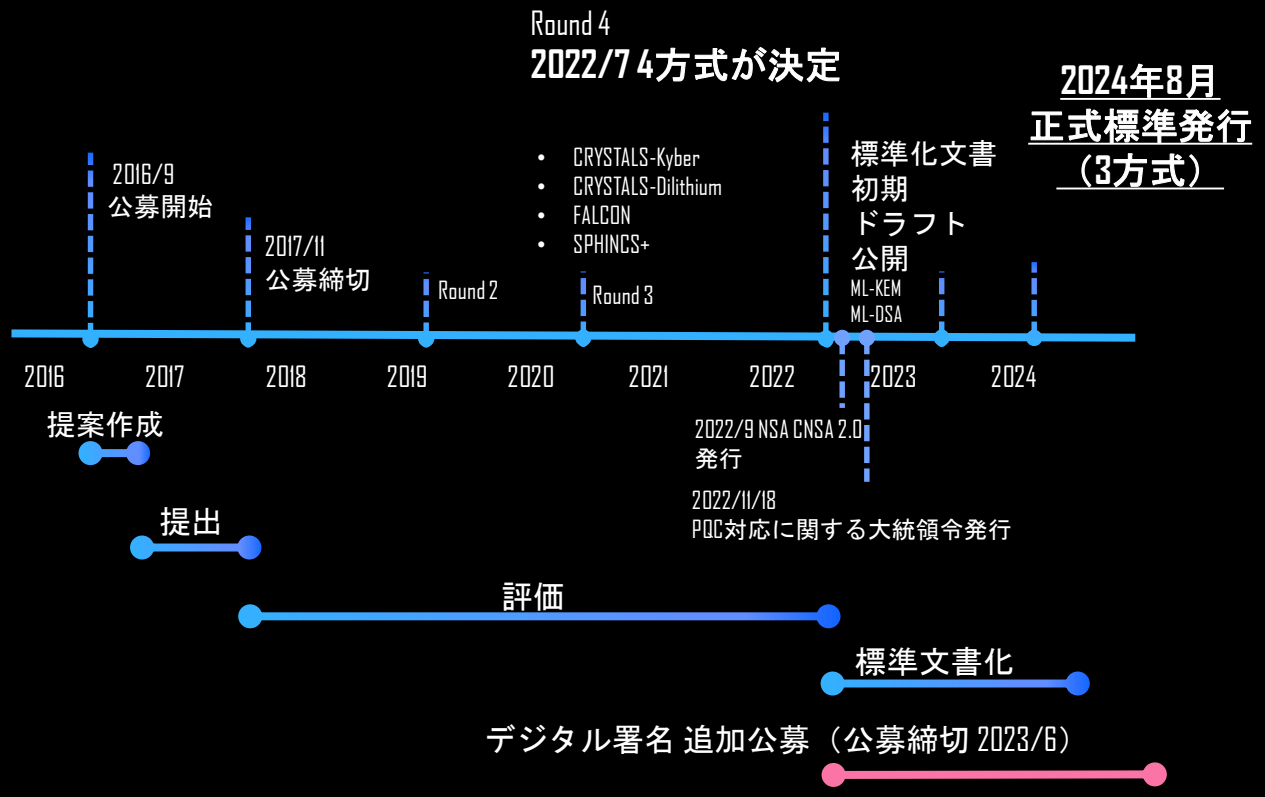


出所：IBM Quantum Summit 2023

脅威に向けた備えとしての耐量子計算機暗号の最新動向

要素技術として、NISTでの耐量子暗号アルゴリズムの標準化活動が進展し、2024年8月13日に正式アナウンス。
また、移行に向けたソリューションの実装を見据えた技術開発・標準化が主要団体・ITベンダーで進行している。

NISTにおける標準化アプローチ



ソリューション実装の技術開発・標準化のための主な共同プロジェクト

- **NCCoE（NIST主導）：**
  耐量子暗号標準化を推進するための専門知識や手法の提供
  NIST National Cybersecurity Center of Excellence (NCCoE)
- **オープンソースプロジェクト：**
  耐量子アルゴリズムとプロトコルのオープンソース開発とプロトタイピング
  Post-Quantum Cryptography Alliance
  OPEN QUANTUM SAFE
- **産業別コンソーシアム：**
  業界全体への移行に向けたガイド提供・情報共有
  - 業界横断：NIST、PQCA、MITRE*
  - 金融：FS-ISAC、NACHA The Electronic Payments Association、EPA EMERGING PAYMENTS ASSOCIATION
  - 通信：GSMA

*MITRE：米国の非営利団体で公共機関に対して幅広い領域にわたり研究開発等の支援を実施。サイバーセキュリティでは、MITRE ATT&CKフレームワークの制定、テクニックの共有促進、カンファレンスの開催等を実施

NIST 耐量子計算機暗号 標準アルゴリズムに関するリリース

2024年8月13日、NISTがPQC標準アルゴリズムの初版として3方式をリリース
補足：3方式のバックアップとして、FALCONベースの暗号化アルゴリズムセット、デジタル署名のアルゴリズムセットの評価を継続

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

#	標準アルゴリズム名	概要
1	ML-KEM （Module-Lattice-Based Key-Encapsulation Mechanism）	一般的な暗号化のための標準アルゴリズム。比較的小さな暗号鍵を2つの当事者が容易に交換できることや、その操作の速さが利点。CRYSTALS-Kyberに基づくアルゴリズム
2	ML-DSA （Module-Lattice-Based Digital Signature Algorithm）	デジタル署名の保護のための標準アルゴリズム。CRYSTALS-Dilithiumに基づくアルゴリズム
3	SLH-DSA （Stateless Hash-Based Digital Signature Algorithm）	デジタル署名の保護のための標準アルゴリズム。ML-DSAが脆弱であることが判明した場合のバックアップ手段。SPHINCS+に基づくアルゴリズム

（参考）IBM 耐量子計算機暗号対応に関するリリース

IBMでも同日（8/13）にプレスリリース。日本でも8/16に発表

以下、プレスリリース内容より抜粋

13 August 2024 – Yorktown Heights, New York – Two IBM-developed algorithms have been officially formalized within the world's first three post-quantum cryptography standards, which were published today by the U.S. Department of Commerce's National Institute of Standards and Technology （NIST）.
【ニューヨーク州ヨークタウン・ハイツ – 2024年8月13日 （現地時間）発】世界初の3つの耐量子計算機暗号標準（Post-Quantum Cryptography Standards）に、IBMが開発した2つのアルゴリズムが正式に採用されたことが、本日、米国商務省の国立標準技術研究所 （NIST） から発表されました。

The standards include three post-quantum cryptographic algorithms: two of them, ML-KEM （originally known as CRYSTALS-Kyber） and ML-DSA （originally CRYSTALS-Dilithium） were developed by IBM researchers in collaboration with several industry and academic partners. The third published algorithm, SLH-DSA （initially submitted as SPHINCS+） was co-developed by a researcher who has since joined IBM. Additionally, a fourth IBM-developed algorithm, FN-DSA （originally called FALCON）, has been selected for future standardization.
耐量子計算機暗号標準には、3つの耐量子計算機暗号アルゴリズムが含まれており、ML-KEM （当初の呼称はCRYSTALS-Kyber） とML-DSA （当初の呼称はCRYSTALS-Dilithium）の２つは、IBMの研究者が業界および学術界のパートナーと協力して開発しました。3番目に公開されたアルゴリズムSLH-DSA （当初はSPHINCS+として提出） は、その後IBMに入社した研究者によって共同開発されたものです。さらに、IBMが開発した4番目のアルゴリズムFN-DSA （当初の呼称はFALCON） は、将来の標準化に向けて選出されています。
（中略）
Toward its mission to make the world quantum-safe, IBM continues to explore how post-quantum cryptography can be integrated into many of its own products, including IBM z16 and IBM Cloud. In 2023, the company unveiled the IBM Quantum Safe roadmap, a three-step blueprint to chart the milestones towards increasingly advanced quantum-safe technology, and defined by phases of discovery, observation, and transformation. Alongside this roadmap, the company also introduced IBM Quantum Safe technology and IBM Quantum Safe Transformation Services to support clients in their journeys to becoming quantum safe. These technologies include the introduction of Cryptography Bill of Materials （CBOM）, a new standard to capture and exchange information about cryptographic assets in software and systems.
世界を耐量子の状態にするというミッションに向け、IBMは耐量子計算機暗号をIBM z16やIBM Cloudといった多くの自社製品に統合する取り組みを進めています。2023年にIBMは、IBM Quantum Safeロードマップを発表しました。これは、ますます進化する耐量子技術に向けたマイルストーンを示す三段階の青写真であり、発見、観測、変革のフェーズで定義されています。このロードマップに加えて、お客様が耐量子を実現できるように支援するために、IBM Quantum SafeテクノロジーとQuantum Safeへの実現に向けた計画策定から移行を含めたIBM Quantum Safe Transformation Servicesを発表しました。これらのテクノロジーには、ソフトウェアやシステム内の暗号資産に関する情報を特定・交換するための新しい標準である暗号部品表 （CBOM） の導入を含めた”クリプト・インベントリー”や”クリプト・アジリティ”への対応が含まれます。

日本国内での耐量子計算機暗号対応に関わる示唆

1 量子コンピューター技術が進展する中、セキュリティーの脅威が顕在化

- 量子コンピューティングの展開が進んでいく中、量子技術の不正利用によるサイバーセキュリティーへの脅威が顕在化。現在の計算機では現実的な時間では解けなかった暗号鍵の復号等が、量子コンピューターによって指数関数的な速度で解読される
- 重要なデジタルインフラにおける、①暗号化された機密データの復号、②不正な認証、③デジタル署名の偽造

2 耐量子暗号対応は、量子コンピューターの実用化前に対応完了が求められる

- 守るべき重要なデータとシステムが特定され、目標のターゲット（重要領域）で移行が実行されていることが必要
  ①デジタルインフラのアップデートには時間を要する
  ②新規構築/更改予定のシステム（含：推進中）は耐量子暗号対応を考慮に入れない場合、二重投資が必要になる
  ③長期保存が必要なデータは今から対応を進める必要がある（HNDLを含めた複数脅威への対応が必要）

3 耐量子暗号移行への対応は海外の動向を参照しつつ適切な対策推進が重要

- NISTにて2024年8月、耐量子計算機暗号（PQC）標準化に関する重要マイルストーンのアナウンスが正式に発信
- 諸外国では取り組みが加速。国内でも耐量子暗号対応は、海外の動向を参照しつつ適切な対策推進することが重要
  ①脅威を把握（可視化）するクリプト・インベントリの作成・整備
  　当該インベントリに基づき、想定されるリスクをアセスメントした上での移行プランの策定
  ②移行の実施（含：クリプトへのガバナンスと継続的かつ柔軟に脅威に対応できるクリプト・アジリティの構築）

耐量子暗号移行に向けたサービス提供に関する状況
（暗号インベントリー作成や移行支援に関するサービス提供状況等）

IBMの取り組み（1/3）耐量子計算機暗号移行にむけたロードマップ

	2022	2023	2024	2025	2026+
Regulatory milestones	NIST selects algorithms for standardization	Federal agencies plan for PQC adoption	NIST publishes PQC standards	CNSA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC
Consortia	● Open Quantum Safe (OQS) ● Post-Quantum Telco Network	● NCCoE ● PQC Coalition (MITRE)	◔ Payments (EPAA, NACHA) ◔ PQC Alliance (Linux Foundation)	○ Critical Infrastructure Protection Coalition	
IBM services		● Quantum-safe preparation & advisory	◔ Application modernization ◔ Platform modernization	○ Security platform modernization	○ Quantum-safe talent transformation
IBM Quantum Safe technology			**IBM Quantum Safe Remediator** — *Transform* ◔ Adaptive proxy ◔ TLS, VPN, SSL ◔ Performance benchmarking	◔ Crypto-agility framework ◔ Encryption ◔ Key/certificate management	○ Automated remediation ○ LLM-based recommendation
			IBM Guardium Quantum Safe Posture Management - *Observe* ◔ Dynamic scan ◔ Cryptographic inventory ◔ Cryptographic posture mgmt	◔ Risk-based prioritization ◔ Enriched metadata	○ AI-driven risk analysis
		IBM Quantum Safe Explorer — *Discover* ● Static scan ● CBOM generation ● CI/CD integration	◔ Custom library support ◔ Remediation recommendation	○ LLM-assisted scanning	
Algorithms, protocols, standards, libraries	● Key encryption: CRYSTALS - Kyber ● Digital signature: CRYSTALS - Dilithium, FALCON	● Cryptography Bill of Materials (CBOM)	◔ MAYO, UOV, SQISign ◔ OpenSSL		
IBM infrastructure		● IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	◔ IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power		

IBM **Quantum** Safe

IBMの取り組み（2/3）耐量子計算機暗号移行に係るソリューション

IBM Quantum Safe Technology

Discover

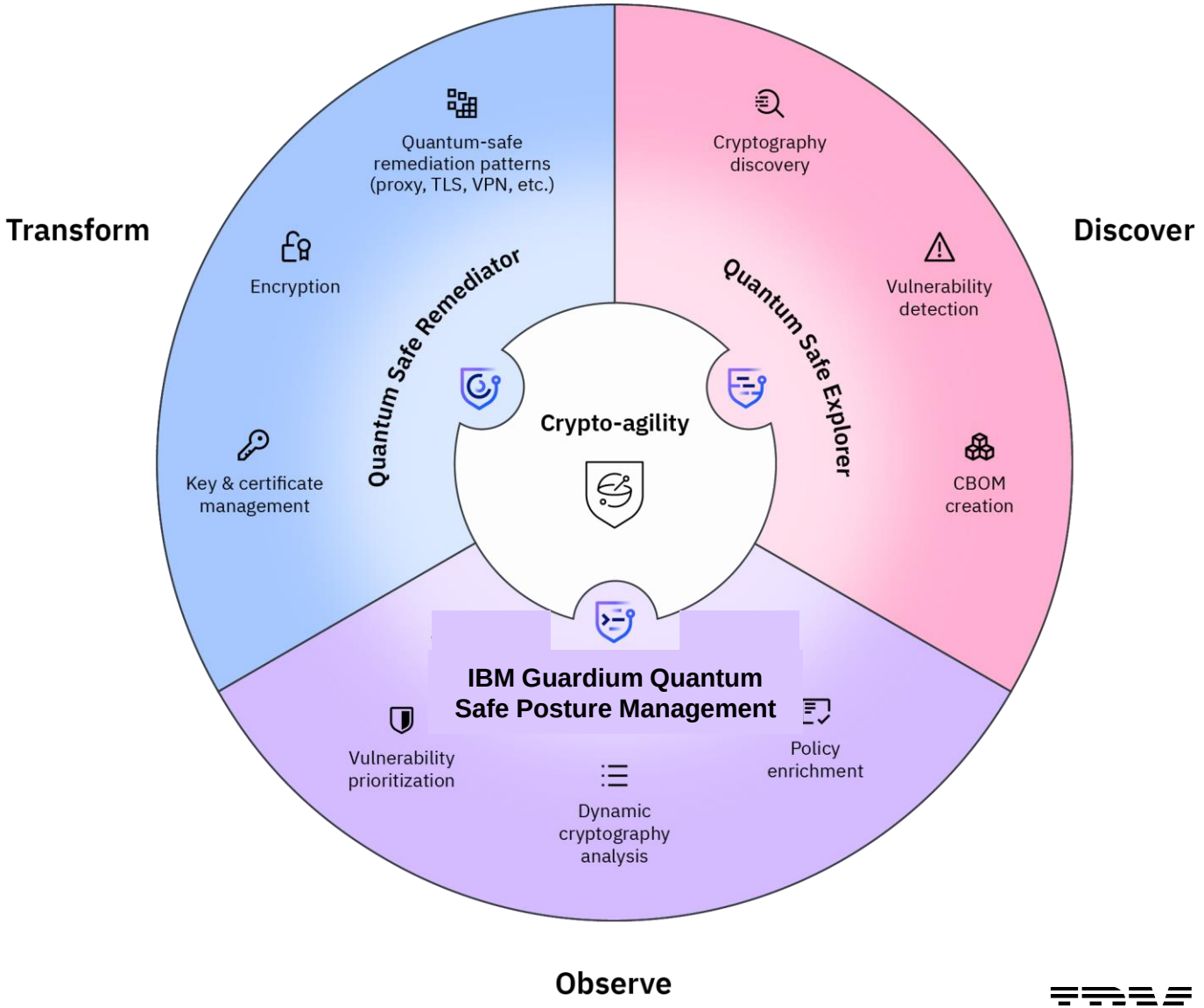
- 情報システムの中で、どこでどのような暗号アルゴリズムが使われているかを把握、リスクにさらされる資産を特定
- 暗号部品表（CBOM：Cryptography Bill of Materials）を含むクリプト・インベントリーを作成

Observe

- 企業の暗号化に関わるポリシーを参照し、セキュリティ・コンプライアンス、脆弱性の遵守状況を分析
- リスクに基づいて、改善に向けた優先順位を設定

Transform

- クリプト・アジリティの実現に向けた技術パターンを適用（例：Adaptive Proxy）
- パフォーマンス評価を通じて、耐量子計算機暗号アルゴリズム（PQC）の適用を最適化



IBM **Quantum** Safe

IBM

IBMの取り組み（3/3）IBMテクノロジーの耐量子計算機暗号対応

IBM Quantum Safe Example – z/OS

Comprehensive support for IBM z/OS Platform. Industry first quantum-safe system protected by quantum-safe technologies through multiple layers of firmware. Helps protect IBM z16 firmware from quantum attacks through a built-in dual signature scheme with no changes required.

Industry first quantum-safe system protected by quantum-safe technologies through multiple layers of firmware

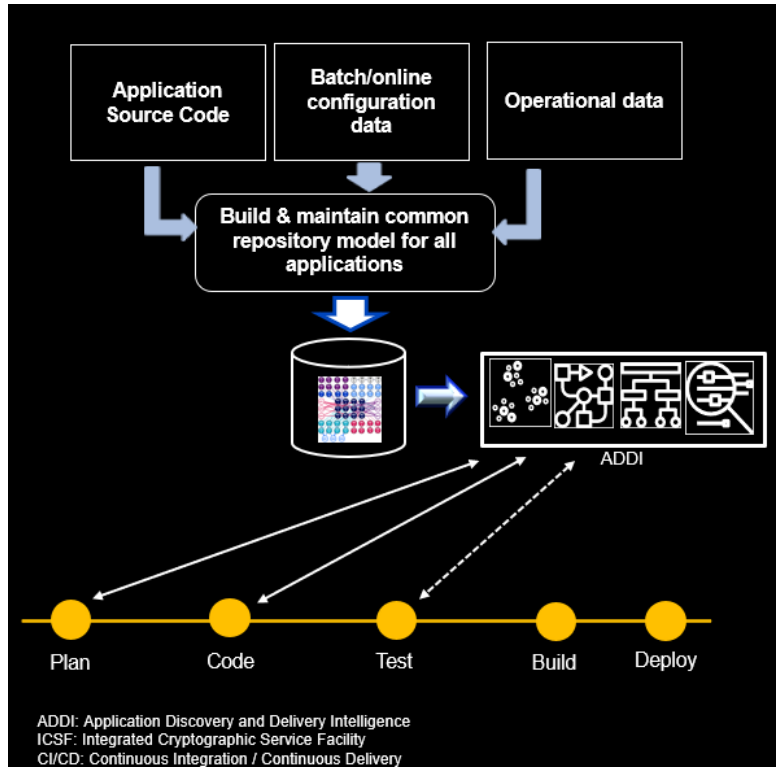
Helps protect IBM z16 firmware from quantum attacks through a built-in dual signature scheme with no changes required

New Crypto Express card with quantum-safe APIs to modernize existing and build new applications leveraging quantum-safe cryptography along with classical cryptography

Discover where and what crypto is used in applications to aid in developing a crypto inventory for migration and modernization planning

New crypto discovery features in IBM Application Discovery and Delivery Intelligence（ADDI）to analyze COBOL source code and discover crypto usage in applications

Aid in migration and modernization planning



EOF