金融高度化センター設立20周年記念ワークショップ
「デジタル化とわが国の金融の未来」
第3部　デジタル技術を活用した金融サービスの安定的な提供について

耐量子計算機暗号(PQC)と金融機関の対応について

みずほフィナンシャルグループ
グループ執行役員　グループCISO
寺井　理

2025年1月31日

ともに挑む。ともに実る。
MIZUHO

自己紹介

寺井　理（テライ　オサム）

みずほフィナンシャルグループ
グループ執行役員　情報セキュリティ担当（グループCISO）

みずほ銀行/みずほ信託銀行/みずほ証券/
みずほリサーチ＆テクノロジーズ
常務執行役員　情報セキュリティ担当（CISO）

＜経歴＞

- 新卒で銀行のシステム子会社に入社
- 銀行のロンドン支店で通貨ユーロ導入、Y2K対応、みずほ統合プロジェクトなどを推進
- 野村総合研究所へ転職。データセンター移転、デリバティブシステムの導入、顧客向けプライベートクラウドサービスの企画構築まで幅広く経験
- みずほ証券に転職。IT基盤の部長をつとめつつ、みずほグループのパブリッククラウド導入・活用を推進
- フィナンシャルグループのサイバーセキュリティ統括部署の部長を経て2022年４月よりグループ共同CISO、2024年４月より現職

アジェンダ

- 〈みずほ〉について
- 耐量子計算機暗号（PQC）について
- まとめ

アジェンダ

- 〈みずほ〉について
- 耐量子計算機暗号（PQC）について
- まとめ

会社概要

商号	株式会社みずほフィナンシャルグループ
上場 （証券コード）	東京証券取引所プライム市場（8411） ニューヨーク証券取引所（MFG）
所在地	東京都千代田区大手町1丁目５番5号
代表者	執行役社長　木原 正裕
従業員数 (連結子会社合計)	52,307人
発行済 普通株式数	25億3,924万株

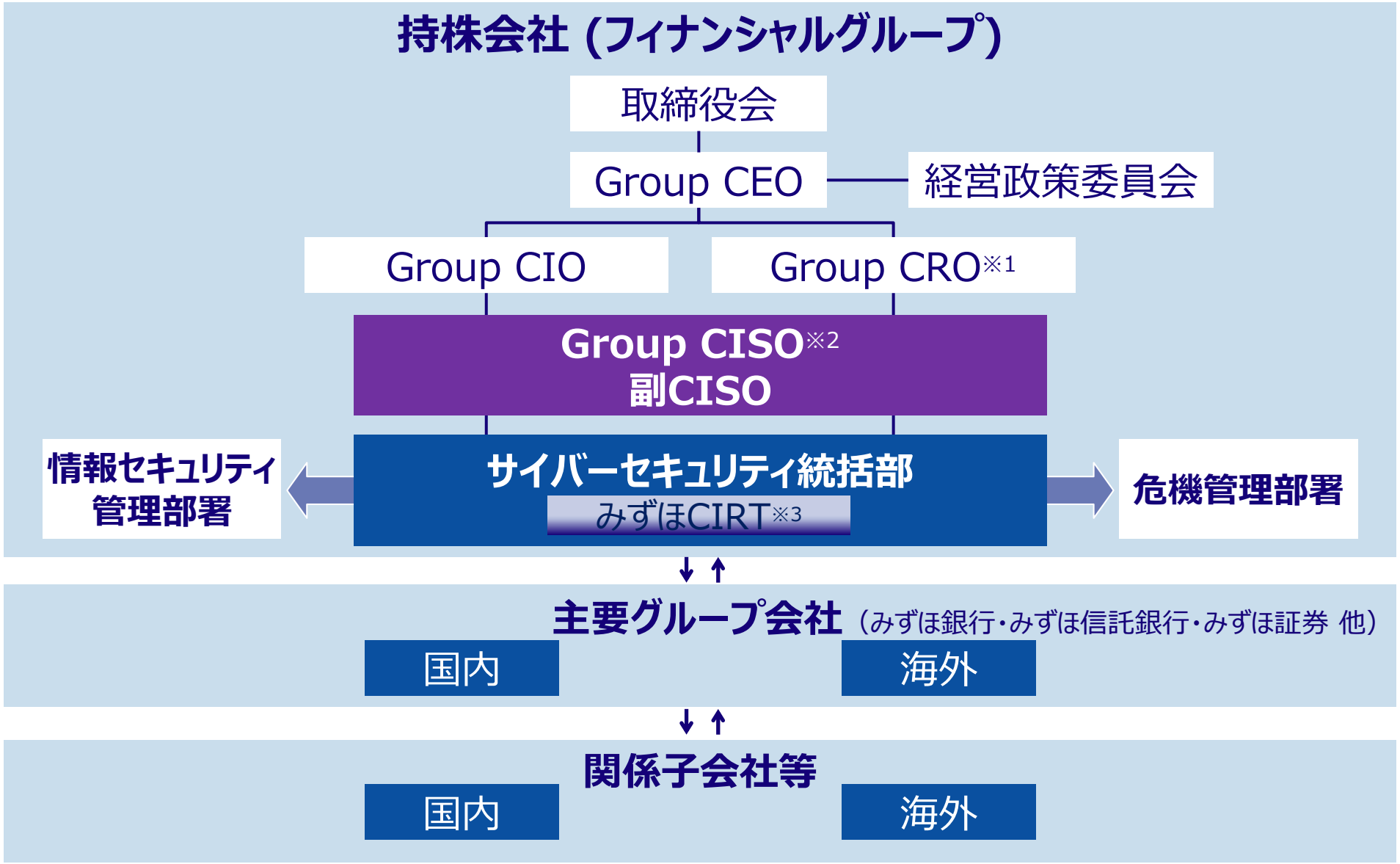
資本金	2兆2,567億円
流通株式数	18億4,351万株

（2024年3月31日現在）

〈みずほ〉グループの組織

- カンパニー制によるエンティティとのマトリックス運営
- CISOはFG、銀行、信託銀行、証券、リサーチ＆テクノロジーズを兼職

〈みずほ〉のサイバーセキュリティ体制



※1 CRO:Chief Risk Officer
※2 CISO:Chief Information Security Officer。〈みずほ〉では情報セキュリティ担当
※3 CIRT:コンピュータセキュリティインシデントに対応する活動を行う組織

アジェンダ

■ 〈みずほ〉について

■ 耐量子計算機暗号（PQC）について

■ まとめ

暗号技術の用途と鍵の種類

暗号技術の主な用途

1. 暗号化：通信の暗号化・鍵交換、データベースなどの暗号化
2. 電子署名：電子文書やソフトウェア、Eメールなどへの署名
3. 認証：サーバ証明書、クライアント証明書などを使った認証

鍵の種類

1. 共通鍵暗号：暗号化と複合で使う鍵が同じ
2. 公開鍵暗号：暗号化と複合で使用する鍵が異なる
   - 「公開鍵」を使って暗号文を作成し「秘密鍵」で平文に複合
   - 現在使用が認められている暗号アルゴリズム・鍵長では、公開鍵から秘密鍵を現実的な時間で算出することはできない

耐量子計算機暗号(Post-Quantum Cryptography: PQC)とは何か

- 一定以上の能力をもつ量子コンピュータ(Cryptographically Relevant Quantum Computer: CRQC)が実用化された際には、既存暗号の一部が解読される脅威があると指摘されている
- CRQCに対して耐性がある「耐量子計算機暗号(PQC)」への移行が各国政府や民間企業の重要なテーマとなってきている

暗号アルゴリズム	タイプ	用途	CRQCの影響
AES	共通鍵	暗号	より大きな鍵長が必要
SHA-2、SHA-3	------	ハッシュ	より大きな出力が必要
RSA	公開鍵	署名、鍵交換	安全ではなくなる
ECDSA、ECDH	公開鍵	署名、鍵交換	安全ではなくなる
DSA	公開鍵	署名、鍵交換	安全ではなくなる

出所：”Impact of Quantum Computing on Common Cryptographic Algorithms (NISTIR8105)”講演者訳

PQC標準化動向

- 米国国立標準技術研究所(National Institute of Standards and Technology: NIST)は2016年からPQCの公募、検証を実施
- 2024年８月に３つのアルゴリズムをPQCの標準アルゴリズムとして発表
- 発表以降、さまざまな標準化団体や業界団体による実装方式の標準化や移行ガイドラインの検討が活発化

暗号アルゴリズム	用途	元になったアルゴリズム
FIPS 203 ML-KEM	鍵交換	CRYSTALS-KYBER
FIPS 204 ML-DSA	署名	CRYSTALS-Dilithium
FIPS 205 SLH-DSA	署名	SPHINCS+

出所：”NIST Releases First 3 Finalized Post-Quantum Encryption Standards (NIST)”をもとに講演者作成

CRQCはいつ実用化されるのか

- IBMの2024年に更新されたロードマップでは、2029年に誤り耐性型量子コンピュータ(Fault Tolerant Quantum Computer: FTQC)の提供開始、2033年以降は特定分野で実用レベル(量子ビット、ゲート数)としたFTQCを提供、としている※1
- Googleは105量子ビット、誤り訂正機能を搭載したチップ「Willow」を開発。現在の最速のスーパーコンピュータで1,000兆年かかる計算を5分未満で実行したと発表※2
- Global Risk InstituteとevolutionQが毎年行っている、32人の量子コンピュータ専門家へのアンケート2024年版では、24時間でRSA-2048を破ることができるCRQCが10年以内に開発される可能性は楽観的解釈で平均34%、悲観的解釈で19%※3
- Nvidia CEOのJensen Huang氏はCES 2025の基調講演で、「有用な量子コンピュータについては15年から30年かかるだろう」と発言※4

※1: https://www.ibm.com/quantum/assets/IBM_Quantum_Developmen_&_Innovation_Roadmap_Explainer_2024-Update.pdf
※2: https://blog.google/technology/research/google-willow-quantum-chip/
※3: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
※4: https://www.msn.com/en-us/news/technology/quantum-computing-stocks-dive-after-nvidia-ceo-says-tech-15-30-years-away/ar-AA1x8Tix

各国・地域の政府機関の対応

米国	• 連邦政府機関の国家安全保障に関わるシステムについては**2035年までに最大限リスクを解消**する方針を発表 (2022年) • 国家安全保障局は、それらのシステムで使用される暗号アルゴリズムの組み合わせを更新 (CNSA 2.0)。調達製品については概ね**2033年までにデフォルトで搭載**するよう要請 (2022年)
欧州	• 欧州委員会が各加盟国へPQC移行検討を促す勧告を発信 (2024年) • EU18か国のサイバー機関がPQC移行検討を促す声明を発表※1 (2024年)
カナダ	• セキュリティ当局がCRQCへのリスク対応ガイダンスを発表 (2021年)
APAC	• オーストラリア信号局が「高い保証が求められる暗号機器 (HACE)」で使用される暗号技術ガイドラインを発表。2030年以降のRSA等CRQC脆弱な暗号アルゴリズムの使用禁止を明記※2 (2024年) • 韓国では独自でPQCアルゴリズムを公募し評価作業中

※1: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.html
※2: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography
その他は「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 報告書」（金融庁）より抜粋、要約

金融当局・金融業界団体の動向

G7サイバー専門家グループ	• HNDL攻撃やCRQCのリスク低減対応への着手を推奨する提言を発表(2024年)
金融庁	• 「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」(PQC検討会)開催(2024年)
日本銀行	• 金融研究所が各種レポートやセミナーを通じてPQC対応の必要性を発信（2018年～）
FS-ISAC	• PQCWGを設置し、金融サービスへのリスクと対処方針を記載した技術報告書やクリプト・アジリティへの移行プロセス解説ペーパを公表(2023年、2024年)
QSFF	• PQC移行支援のための欧州金融機関が中心のフォーラム(2024年)
UK Finance	• 量子コンピュータが金融サービスに及ぼす影響やリスク、対処方法を示す提言ペーパーを公表(2023年)
金融ISAC	• 金融庁PQC検討会の後続をFintechセキュリティWGで引き取り検討（2024年）

「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 報告書」等より抜粋、要約

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

令和６年11月26日
金融庁

「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報告書」の公表について

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（座長：寺井 理 株式会社みずほフィナンシャルグループ グループ執行役員・情報セキュリティ担当（グループ CISO）、金融 ISAC FinTech セキュリティワーキンググループ座長）においては、PQCへの移行を検討する際の推奨事項、課題及び留意事項について、令和６年７月から10月にかけて関係者と幅広く議論を行いました。

今般、同報告書がとりまとまりましたので、「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報告書」（別紙）を公表します。

（別紙） 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報告書（PDF：2.6MB）

関連リンク

- 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

お問い合わせ先

金融庁　Tel　03-3506-6000（代表）
総合政策局リスク分析総括課ITサイバー・経済安全保障監理官室（内線2217、3850）

「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」

メンバー等名簿

（敬称略、五十音順）

座長	寺井　理	株式会社みずほフィナンシャルグループ グループ執行役員・情報セキュリティ担当（グループ CISO） 金融 ISAC FinTech セキュリティワーキンググループ座長
メンバー	安藤　彰英	株式会社名古屋銀行　執行役員　業務部長
	岩崎　三郎	株式会社静岡銀行　リスク統括部長
	宇根　正志	日本銀行　金融研究所　参事役
	大城　徹	株式会社しんきん情報システムセンター　上席執行役員
	菅野　洋平	労働金庫連合会　情報システム部　副部長
	白井　大輔	株式会社三井住友フィナンシャルグループ グループ CISO　サイバーセキュリティ統括部長
	高瀬　徹	農林中央金庫　IT 統括部部長（システムリスク管理担当）
	松本　泰	特定非営利活動法人日本ネットワークセキュリティ協会 フェロー
	峰　匡親	株式会社三菱 UFJ フィナンシャル・グループ グループ CISO　サイバーセキュリティ推進部　部長
	村山　朋彦	信組情報サービス株式会社　常勤取締役
オブザーバー	一般社団法人金融 ISAC、CRYPTREC 事務局、公益財団法人金融情報システムセンター、日本銀行　金融機構局、内閣サイバーセキュリティセンター	
事務局	金融庁	

出所：https://www.fsa.go.jp/news/r6/singi/20241126.html

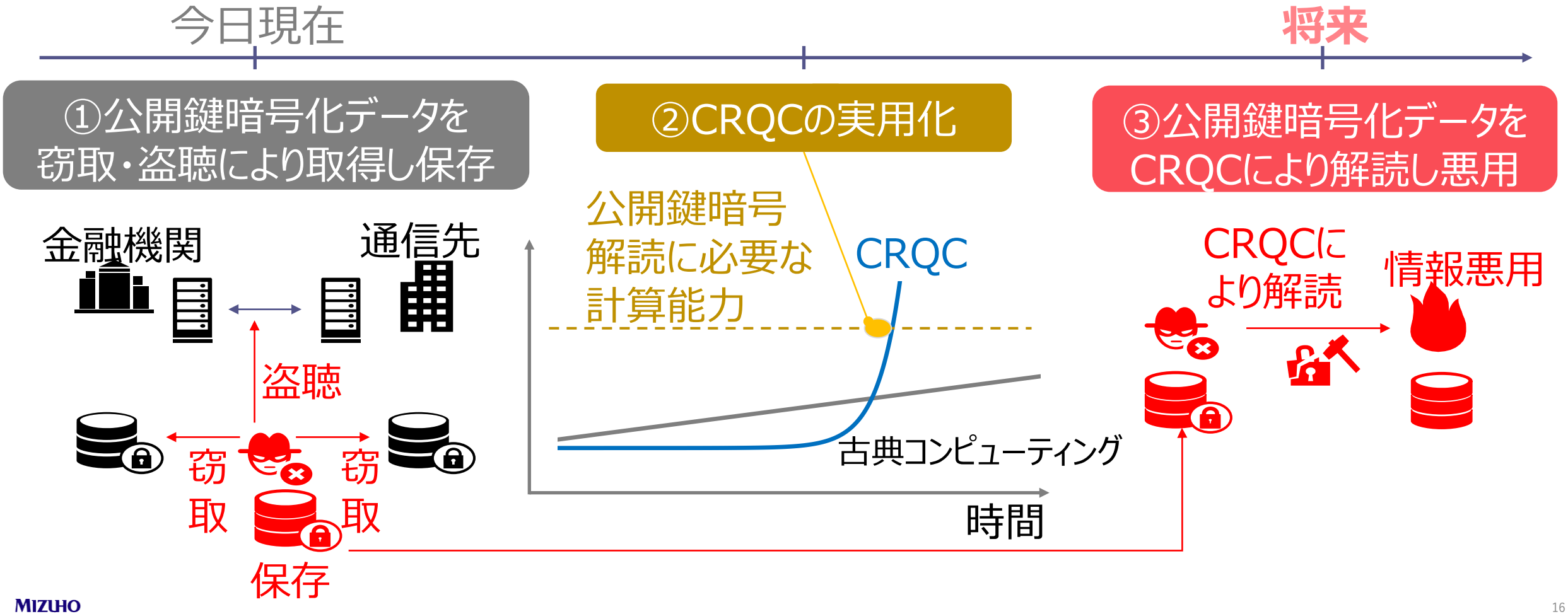
CRQCが悪用された際のリスク

リスクの分類	UK Financeによる例示
機密性の低下	• ホールセール決済システムの認証の脆弱化 (Risk 2) - 合法的な取引を模倣した不正決済の実行 • 銀行間システムのインターフェースの侵害 (Risk 3) - 複数銀行の機密性の高い金融データや顧客情報、取引記録への不正アクセス
完全性の低下	• 分散型台帳技術 (DLT) を基にした金融商品の侵害 (Risk 4) - 初期ブロック内容の変更によるブロックの完全性保証の毀損 • ソフトウェアの完全性における脆弱化 (Risk 7) - 署名改ざんによる不正ソフトウェアのなりすまし • 金融取引記録の改ざん （Risk 8 企業固有の台帳） - デジタル署名付与済の金融取引記録の改ざん

https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/minimising-risks-quantum-technology-and-financial

Harvest Now Decrypt Later (HNDL) について

- Harvest Now Decrypt Later(HNDL)とは、今のうちから暗号化されたデータを収集し、CRQCが登場した後に解読し悪用するという攻撃の手口
- 金融機関として長期に保全すべきデータをHNDL攻撃からの保護対象と優先的に対応



PQC対応の特徴

1. 移行が長期にわたる

- 公開鍵暗号は金融機関のさまざまなところで使用されており、網羅的な把握と対応に時間がかかる
- 移行にあたって関わるステークホルダーが多岐にわたる(開発ベンダー、製品ベンダー、接続先、利用顧客の調整など)
- PQCの実装プロトコルやPQC対応製品の提供にはまだ時間がかかるとみられる

2. CRQC・PQCの不確実性

- CRQCがいつ登場するかが現在のところ未定である
- PQCが比較的新しい技術であり、採用された暗号方式の脆弱性が発見される可能性は否定できない

PQC対応の基本事項

対応事項	概要
優先順位付け	• CRQCにより侵害される蓋然性が高く、侵害の影響が大きいシステムの優先度を高く設定
クリプト・インベントリの作成	• 公開鍵暗号によって保護されている資産を把握 • どのシステム・サービスのどの箇所で、どのような暗号が使用されているか、侵害された場合の影響も含めて一覧化（継続更新する体制も構築）
アジャイルなアーキテクチャの適用	• PQC対応後も暗号の入れ替えを迅速に行えるようなアーキテクチャ(クリプト・アジリティ)を適用
移行計画の策定・実行	• 優先度の高いシステムについては2030年代半ばまでを目安にPQC移行が完了するように計画

対応期限の考え方

- CRQC登場時期は不明ながらも、欧米亜の各国・地域の政府はPQC移行について、時期を提示しつつ推進している状況
- 金融機関が接続する国際的な決済サービスなどが、その動向に同調してPQC対応を進める可能性があり、その流れから外れることはビジネスリスク
- それらを考慮すると、2030年代半ばまでを目安に、優先度の高いシステムのPQC対応を完了させることが推奨される

米国	• 連邦政府機関の国家安全保障に関わるシステムについては**2035年までに最大限リスクを解消** • それらのシステムで使用される製品については概ね**2033年までにデフォルトでPQC対応暗号を搭載**するよう要請
欧州	• EU18か国声明はHNDLへの保護を**遅くとも2030年までに実施**することを推奨

金融機関の経営層が果たすべき役割

1. 移行方針の決定

- 「預金取扱金融機関の経営層が全社（または全組織的）施策としてリーダーシップを発揮し、各システムで利用されている暗号状況や自組織データの重要性及び保存期間等を把握し、適切なリスク評価や優先順位付けした上で、移行方針を決定することが望ましい」（報告書より抜粋）

2. 経営資源の配分と移行体制の立ち上げ

- PQC移行を進めるにあたっての情報収集、ハイレベルな計画策定体制の立ち上げ
- 自社重要システムのITベンダーへの働きかけ
- 活動のための経営資源（予算・人員）の配分

金融ISAC Fintechセキュリティ WGの活動

活動概要
本邦金融機関としてのPQC対応ロードマップひな形の作成
PQC対応に関する各種情報収集と金融ISAC内での共有 • 国内外の標準化団体、海外政府機関・金融当局・金融機関 • SWIFTなどの金融インフラ機関 • ITベンダー／製品ベンダー • 他の重要インフラセクター
移行に向けた論点の具体的な検討 • クリプト・インベントリの作成・管理に関するプラクティス • 対策優先度が高いデータとはどのようなものか　等
金融業界内、関係省庁、他の重要インフラ事業者などへの啓発、情報連携 • 金融ISAC内、金融業界内の勉強会、等 • 重要インフラ専門調査会、他のISAC、重要インフラCISO連絡会、等

アジェンダ

- 〈みずほ〉について
- 耐量子計算機暗号（PQC）について
- まとめ

まとめ

- 公開鍵暗号はITシステムやハードウェアで広範囲に使われている
- CRQCが実用化されると現在の公開鍵暗号アルゴリズムが解読されるリスクがある
- CRQCがいつ実用化されるかは明確ではないものの、世界では2030年代の半ばを重要なシステム移行完了のターゲットとしている
- PQC移行にかかわるステークホルダーは多岐に渡る。ITシステム所管やサイバーセキュリティチームだけではなく、ビジネスオーナーや企画部門も含めた全社的な移行体制を立ち上げる
- CRQCのリスクを理解し、自社で開発・利用するITシステムのPQC対応優先順位を決める。完全性と機密性、特にHNDLのリスクを考慮する
- PQC対応は手法が未確立。情報収集や業界内の連携に積極的に取り組む

ともに挑む。ともに実る。

MIZUHO

ご清聴ありがとうございました

本資料は、掲示したテーマに関するディスカッションを目的として作成されたものであり、本資料に含まれる情報の確実性あるいは完結性を表明するものではありません。
また、本資料における分析および意見は講演者個人に属するものであり、みずほフィナンシャルグループの公式見解を示すものではありません。

今後の関連制度や環境の変化などによっては、その仮定や分析手法などを大幅に変更する必要がある可能性があり、その場合には本資料における分析とは相違する結果となる可能性がありますので、あらかじめご了承ください。

本資料に記載される内容につきましては、上記を十分にご理解のうえ、みなさまご自身の判断でご活用ください。