情報セキュリティ・シンポジウム「ポスト量子時代の暗号技術」

金融ISACにおける移行ガイドと金融業界の取組みについて

みずほフィナンシャルグループ

常務執行役員　グループCISO
寺井　理

2026年2月

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
常務執行役員　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）

一般社団法人金融ISAC　理事、FintechセキュリティWG座長

Fast, Frank, and Friendly
Financials ISAC Japan

＜経歴＞

1993年　興銀情報開発センター（現『みずほリサーチ＆テクノロジーズ』）
1998年　日本興業銀行 ロンドン支店
2002年　野村総合研究所 ネットワーク事業部
2012年　みずほ証券 IT基盤統括部 部長
2020年　みずほフィナンシャルグループ セキュリティ&データマネジメント部 部長
2022年　みずほフィナンシャルグループ グループ共同CISO、金融ISAC FintechセキュリティWG座長
2024年　みずほフィナンシャルグループ グループCISO、上記主要エンティティCISO（現職）
2025年　金融ISAC 理事

アジェンダ

■ 既存の暗号アルゴリズム危殆化リスク

■ PQC対応のタイムライン／ロードマップ

■ PQC対応の進め方

公開鍵暗号が破られると何が起こるか

リスクの分類	UK Financeによる例示
 暗号化された情報の漏えい・解読	●口座情報や金融資産、機微情報を含む**個人特定情報の漏えい**(Risk1) ●銀行間システムのインターフェースやAPIへの侵害による、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**(Risk3)
 電子署名の改ざん	●ソフトウェアやファームウェアへの電子署名の改ざんによる**不正ソフトウェアのなりすまし**(Risk7) ●企業内で保存されている**金融取引記録の改ざんによる不正取引の創出**(Risk8) ●ブロックチェーンなどの分散型台帳技術（DLT）での初期ブロック内容の改ざんによる**金融商品の完全性への侵害**(Risk4)
 認証情報の偽造によるなりすまし	●ホールセール決済システムへの不正ログインによる**不正決済の実行**(Risk2) ●管理者権限の認証への侵害による、**内部システムへの不正侵入**(Risk5) ●**オンライン金融サービスの認証基盤への侵害**(Risk6)

出所：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

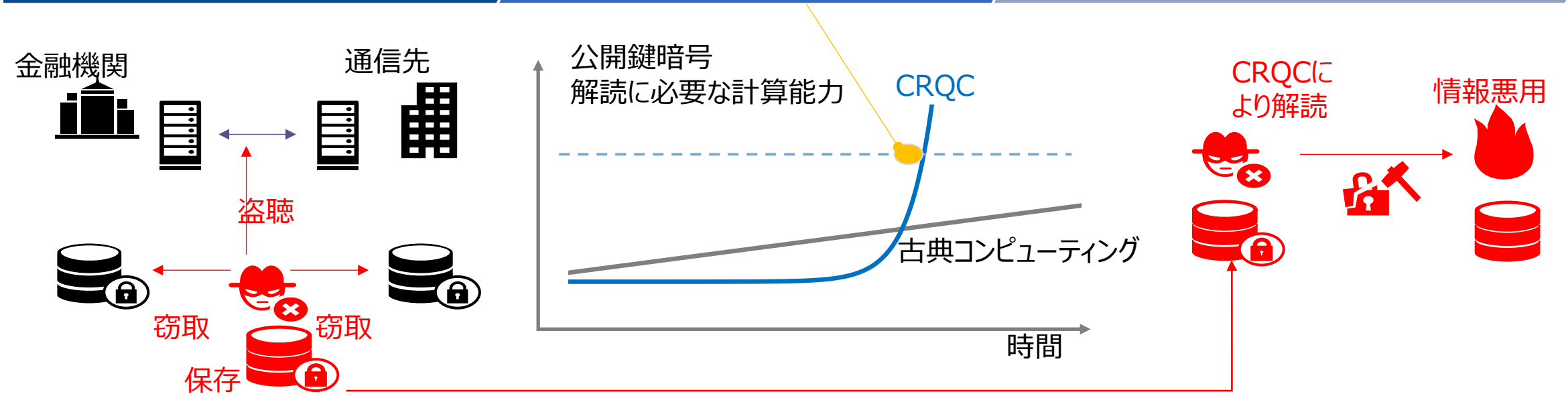
Harvest Now Decrypt Later（HNDL）とは、今のうちから暗号化されたデータを収集し、CRQCが登場した後に解読し悪用するという攻撃の手口。

先行する金融機関においてはHNDLにフォーカスしすぎないようにしている。理由は、①CRQC実現時期がいつかという議論に流れていってしまう、②PQC対応をしなかった場合のリスクが限定的にとらえられてしまうこと。

現在
公開鍵暗号化データを
窃取・盗聴により取得し保存

CRQCの実用化

将来
公開鍵暗号化データを
CRQCにより解読し悪用



Trust Now Forge Later（TNFL）について

Trust Now Forge Later（TNFL）とは、RSAやECDSAなどの現在の暗号アルゴリズムで作成されたデジタル署名を解読し、本物と同じデジタル署名を第三者が作れてしまう攻撃。

デジタル署名は、コンピュータプログラムや金融取引などの真正性を証明するものであるが、デジタル署名の偽造により、悪意のあるコンピュータプログラムの配布や、金融取引の改ざんにつながるリスクがある。

〈正しいアプリ〉

abc.exe
abc_start.dll
abc_calc.dll
・・・

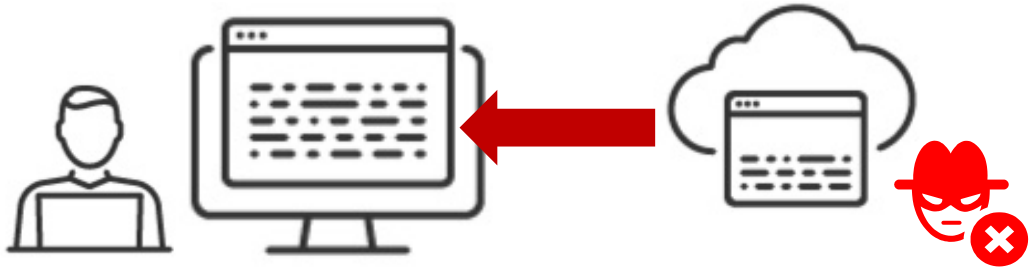
→ abc_start.dll
署名者：abc銀行
・・・

〈同名でバックドアを含むプログラムを仕込む〉

abc.exe
abc_start.dll
abc_calc.dll
・・・

→ abc_start.dll
署名者：abc銀行
・・・

abc銀行の
署名を偽造



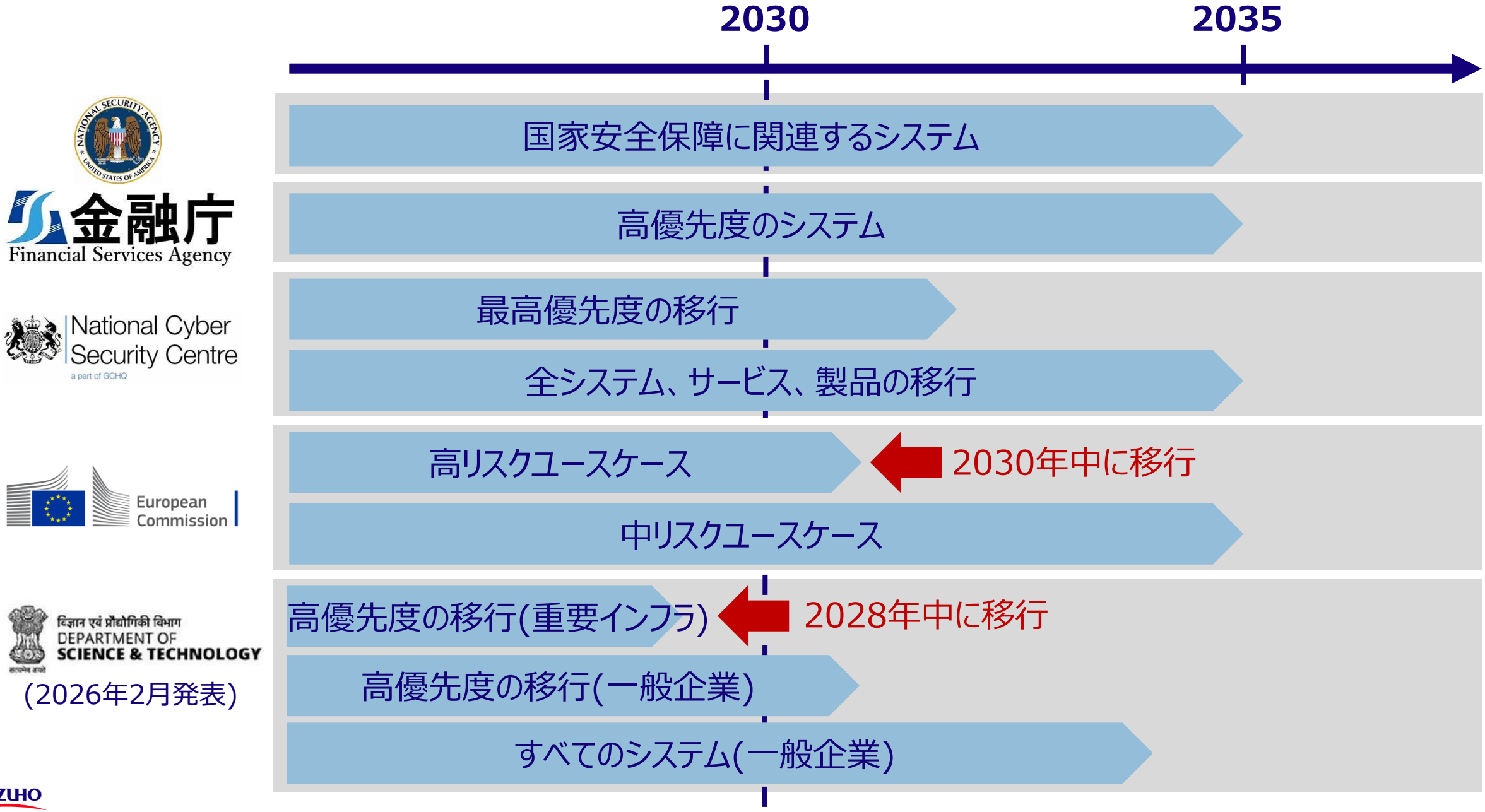
アジェンダ

■ 既存の暗号アルゴリズム危殆化リスク

■ PQC対応のタイムライン／ロードマップ

■ PQC対応の進め方

PQC対応のタイムラインについて

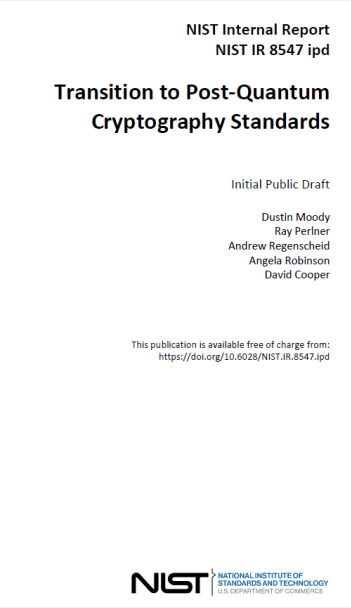


いつまでに対応すべきか（標準化・規制の観点）

NIST IR 8547（ipd）（2024年11月公表）

IR 8547（初版ドラフト）において、以下の暗号アルゴリズムの2035年以降の利用禁止を記載

- 署名：ECDSA、EdDSA、RSA
- 鍵設定：FFDHEとMQV、ECDHとMQC、RSA


NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

Initial Public Draft

Dustin Moody
Ray Perlner
Andrew Regenscheid
Angela Robinson
David Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8547.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

出所：https://csrc.nist.gov/pubs/ir/8547/ipd

PCI DSS V.4.0.1（2025年4月必須化）

- 「オープンな公共ネットワークでカード会員データを伝送する場合、強力な暗号化技術でカード会員データを保護」（主なPCI DSS要件）
- 「脆弱な、安全でない、または不適切な暗号の実装、アルゴリズム、暗号スイート、または操作モードを悪用しようとする試みを含む、暗号の使用に関する攻撃」（安全なシステム及びソフトウェアの開発と維持 6.2.4）


PCI Security Standards Council

Payment Card Industry
データセキュリティ基準

要件とテスト手順
v4.0.1
2024 年 6 月

出所：https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1-JA.pdf

SWIFT FAQ 6000674（2025年8月更新）

- 「2030年までにSwiftコミュニティを耐量子計算機暗号に移行させるという目標を達成するために、2027年にSwiftNetリリース8.0を導入する予定である」
- 「新しいセキュリティパラダイムの採用を容易にするために、我々は、顧客がメッセージングのカウンターパーティの個々の準備レベルを確認する必要がないように、移行の異なる段階にあるカウンターパーティ間の相互運用性を確保する」
- 「移行期間が完了した後、最終的に従来の暗号化のサポートを終了する予定である」

出所：www2.swift.com/knowledgecentre/kb_articles/6000674

G7 Cyber Expert Group（CEG）のステートメント

2026年1月13日、「**Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector**（仮訳：金融セクターにおける耐量子計算機暗号への移行に向けた協調的なロードマップの推進に関するステートメント）」を公表

PQC移行を進めるにあたって考慮すべき事項

- システムや機能のリスクや重要度に応じて、「リスクベース」で移行タイムラインを設定する
- 法域（地域）間、業態や規模の異なる金融機関の間、また、サードパーティと協力・連携することで、先行する金融機関の知見を生かし、対応アプローチがばらばらになることを防ぐことができる

PQC移行の取組

- PQC移行のために必要な取組（タスク）を、金融機関と公的機関のそれぞれの立場で記載している
- 金融機関のPQC移行計画の策定と、各取組での当局との協調事項が示されており、これらも参考にPQC移行計画を策定することが推奨される

PQC移行のタイムライン

- G7として絶対的・確定的な対応期限を提示するものではない
- 「政府または民間部門のシステムあるいはその両方を対象とした量子耐性のある暗号への移行の全体的な目標として2035 年を挙げていることが多い」
- 「最重要（the most critical）と規定されるシステムについて（例えば、移行時期の目標を2030年～2032年に設定し）優先的に対応することにより、リスクの顕現化が早期化するダウンサイド・リスクを減らす」

金融庁（日本語仮訳）https://www.fsa.go.jp/inter/etc/20260115/pqc_kariyaku.pdf

いつまでに対応すべきか（金融ISACの推奨）

金融ISACが2025年9月にリリースしたガイドでは、「日本の金融機関においても、優先度の高いITシステムのPQC移行については、2030年代前半の早い時期を完了目標とすることが推奨される」とした

ステップ ／暦年		2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
FY		2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
【外部マイルストーン】		PQC移行工程表骨子案(内閣官房)※	PQC移行工程表策定(内閣官房)※				112 bit セキュリティの暗号方式の非推奨化				量子脆弱な方式の利用終了	
		標準化・製品化										
							PQC移行完了期間					
							高優先度システムの移行完了推奨期間					
ステップ	担当											
1.体制立上・予算確保	推進	予算・体制立上										
2.スコープ・優先度の設定	推進	検討・決定										
3.移行フレームワーク策定	推進＋システム所管											
3.1. クリプト・インベントリ作成			方法検討・試行									
3.2. リスク評価			評価方法検討・試行									
3.3. 全社ロードマップ作成			移行期限設定・システムの更改情報収集									
4.システムごとのPQC移行実施	システム所管			PQC移行（原則システム更改にあわせて実施）								
高優先度システムの移行				高優先度システムの移行				▲移行完了	▲移行完了	▲移行完了		
その他の優先度のシステム移行							その他の優先度のシステムの移行			▲移行完了	▲移行完了	
5.定常化 (仮)												
5-1.設計・調達標準				設計標準・調達標準の更新								
5-2.継続監視				体制立上	使用中の暗号技術の危殆化予定・状況の調査 (以降継続)							

※「政府機関等における耐量子計算機暗号（PQC）利用に関する関係府省庁連絡会議（第１回）」https://www.cas.go.jp/jp/seisaku/pqc/dai1/gijisidai.html

出所：「日本の金融機関のためのPQC移行ガイド(2025年9月版)」、金融ISAC Fintechセキュリティ WG、2025年9月

アジェンダ

■ 既存の暗号アルゴリズム危殆化リスク

■ PQC対応のタイムライン／ロードマップ

■ PQC対応の進め方

PQC対応ステップ（金融ISACの推奨）

ステップ.作業項目	実施事項	実施時期(FY)
1.推進体制立ち上げ・予算確保	• 社内の移行検討・推進体制の立ち上げ • 活動予算確保 • 社内の役割分担決定	2025～2026年 (FY2025)
2.スコープおよび優先度の設定	• 移行単位の定義 • 移行優先度の定義 • 移行対象システムの決定	2025～2026年 (FY2025～2026)
3.移行フレームワーク策定		
3-1.クリプト・インベントリ作成	• 暗号処理用途を含むクリプト・インベントリ作成対象、作成手順の明確化 • インベントリ作成試行	2026～2027年 (FY2026)
3-2.リスク評価	• 危殆化対象の暗号利用の特定 • リスク分析および優先的な移行箇所の特定	2026～2027年 (FY2026)
3-3.全社ロードマップの作成	• 優先度ごとの移行期限の設定 • 対象システムのPQC更改スケジュールの把握 • 自社・グループの移行ロードマップの作成	2026～2027年 (FY2026)
4.ITシステムごとのPQC移行実施	• システム更改にあわせた移行 • 単独案件としての移行	2027～2035年 (FY2027～2035)
5.継続監視	• 移行後の暗号の安全性についての継続調査 • 危殆化に備えた計画検討	2027年～ (FY2027～)

出所：「日本の金融機関のためのPQC移行ガイド(2025年9月版)」、金融ISAC FintechセキュリティWG、2025年9月

日本の金融機関向けのPQC移行の流れ

アクション	ポイント
 優先順位付け	●CRQC（暗号解読に影響する量子コンピュータ）により侵害される蓋然性と影響がが大きいシステムとデータを特定する
 クリプトインベントリ作成	●どの処理に何の暗号が使われているかをリストアップする ●侵害の影響を可視化しリスクを理解する ●継続的なインベントリ更新のプロセスを構築する
 アジャイルなアーキテクチャの適用	●迅速に暗号の入れ替え（クリプトアジリティ）が可能なアーキテクチャを検討し適用する
 移行計画の策定と実行	●高優先度のシステムの移行は2030年前半の早い時期（2030～2032年）までに完了させるような計画を策定し実行する

PQC移行に向けて速やかに実施すべきこと

経営陣

- PQC移行は情報資産の保護、コンプライアンス対応であり、相互接続する金融機関すべてで必要な対応であることを理解
- IT・サイバー部門だけではなく、ビジネス部門やリスク管理部門も含めた移行推進体制立ち上げを指示
- 長期にわたる取り組みを推進するために十分なリソース（予算・人員）の確保を指示

ビジネス部門

- PQC移行が情報資産の保護だけだけでなく、顧客の安心と安全に直結することを理解
- 担当するビジネスにおけるITシステムのPQC移行に参画し、ビジネス観点のリスクを踏まえたスコープや優先順位を決定

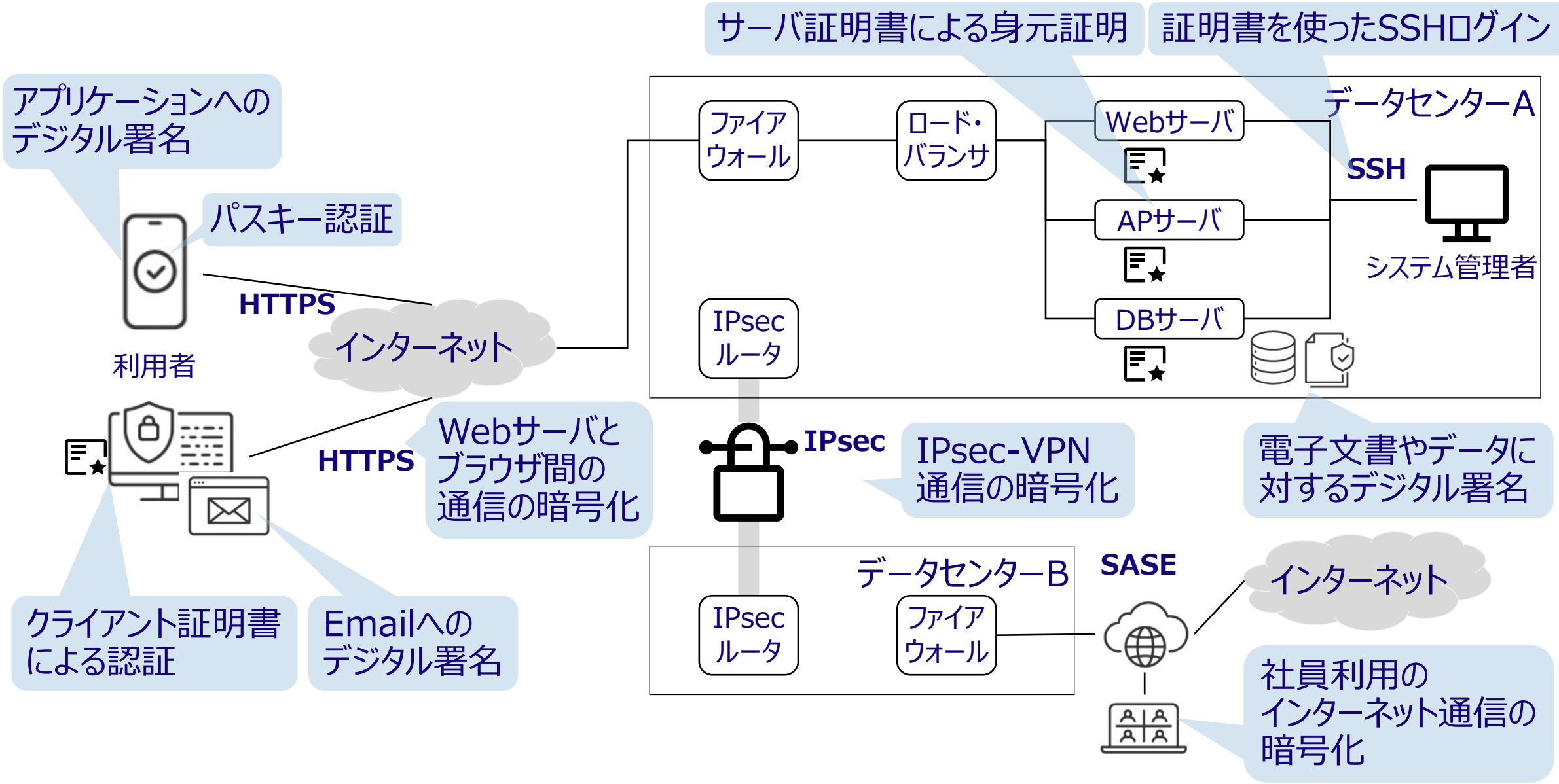
IT/サイバー部門

- 自社が利用するITシステムのPQC移行推進体制を、経営陣や関連する部門と連携して組成
- PQC移行の対象となるITシステムと移行対象の暗号処理を洗い出し、ビジネス部門とともにスコープや優先順位を決定
- 委託先であるITパートナーにPQC移行のために必要な支援を要請

ITパートナー

- 委託元である金融機関のPQC移行をプロジェクト推進や技術的な観点で支援
- 自社のITサービスや製品のPQC移行のロードマップを金融機関にタイムリーに共有

公開鍵暗号はどこで使われているか



システムの移行優先度の考え方（例）

システムの移行優先度をどのようにして決定するか？

Step1: 規制対象？（例：PCI-DSS） → 規制がもとめる期限に対応する計画を策定

Step2: 暗号が破られた場合の「影響」と破られるリスクの「蓋然性」で評価

影響が大きい:

- 機密性の高いデータを扱っている
  例：顧客の健康情報
- 高い完全性が求められる
  例：決済システム

蓋然性が（相対的に）高い:

- インターネット接続システム
- 対策が弱いシステム
  例：WAFが入っていないなど

対象となるシステムのプライオリティを決定

クリプト・インベントリの項目例

#	項目名	収集・管理の目的、内容	記載例
1	暗号用途 （ユースケース）	何の目的のために暗号を使用しているのかを記載する	「Web通信内容保護のための暗号化」 「契約内容を電子的に保護するための署名」
2	暗号実装/利用箇所	暗号の実装箇所・利用箇所を記載する 可能であれば製品名およびバージョンを記載する	社ファイアウォール WebサーバXX
3	通信先セグメント	CRQCリスクの蓋然性が高いインターネット通信の利用か否かを特定するため	インターネット⇔DMZ（自分） DMZ（自分）⇔内部ネットワーク
4	通信相手情報	社外のシステムや顧客、自社内で接続している他のITシステムを把握するため	「○○社 △△サービス」
5	暗号プロトコル、TLS バージョン	主に通信保護の場合の暗号による保護方法を把握するため、利用している暗号プロトコルを記載する	IPsec/IKEv2 HTTPS(TLS1.3) SSH
6	暗号アルゴリズム名および鍵長	量子脆弱な暗号利用を判別するため、利用している暗号アルゴリズム名および鍵長（ハッシュ関数の場合は出力長）を記載する	RSA-OAEP-2048 ECDSA-256 TLS_AES_128_GCM_SHA256
7	重要データ通信有無	機微情報、インサイダー情報など重要情報の通信有無を把握するため。対象システムでデータ保管せず、通信のみが発生するパターンも、この項目により把握する	有：個人顧客の機微情報
8	保護対象データ/ファイル名/ライブラリ名	重要データやファイルを暗号化/署名/ハッシュで保護している場合、危殆化による解読リスクや改ざんリスクを把握するため保護対象のデータを記載する	お客様個人情報 xx.dll
9	ITシステム名	インベントリ作成の対象システム名やシステムIDを管理できるようにする	○○インターネットシステム
10	担当部署/担当者名	連絡のため対象ITシステムの所管部署や担当者を記載する	○○部△△チーム
11	最終更新日	インベントリの最終更新日を管理する	2025年10月1日

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。