海外における耐量子計算機暗号（PQC）への移行を見据えた取組み

2023年9月21日

宇根　正志
日本銀行金融研究所

本発表の内容は、発表者個人のものであり、日本銀行の公式見解ではありません。

略歴

- 1994年　日本銀行 入行
- 1996年　金融研究所　情報セキュリティ技術の調査・研究
- 2006年　産業技術総合研究所へ出向（～2007年）
- 2007年　金融研究所へ戻る
- 2010年　システム情報局（～2015年）
- 2015年　金融研究所へ戻る
- 2023年　金融研究所参事役

博士（工学）

情報処理学会 コンピュータセキュリティ研究会（登録会員）

人工知能学会 安全性とセキュリティ研究会（運営委員）、など

アジェンダ

1. 背景
2. 海外のセキュリティ当局のスタンス
3. 金融分野での検討事例

1. 背景

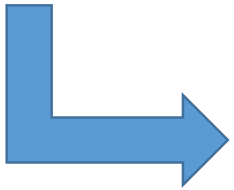
2. 海外のセキュリティ当局のスタンス

3. 金融分野での検討事例

量子コンピュータ：現代暗号への脅威に

- 誤り訂正機能を有する大規模な（量子ゲート型）量子コンピュータ

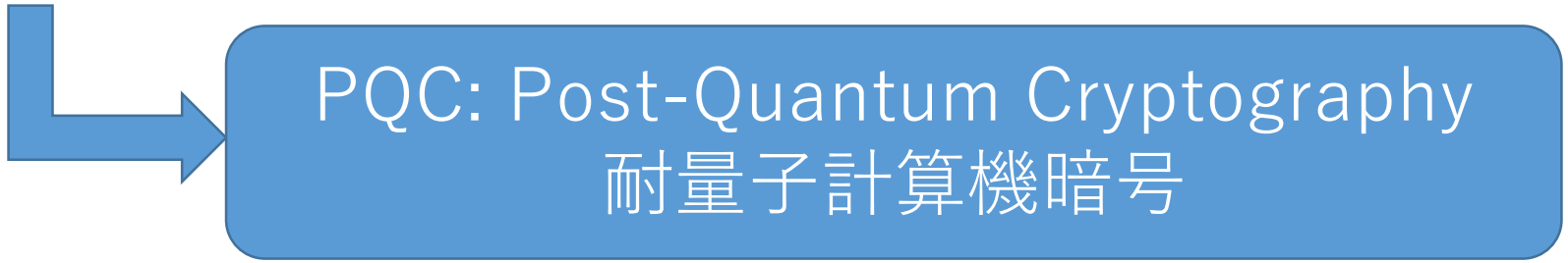
- 主要な現代暗号への影響
  - 共通鍵暗号（AES…）：小さい
  - 公開鍵暗号（RSA、楕円曲線暗号）：大きい



CRQC：Cryptographically Relevant Quantum Computer
暗号解読可能量子コンピュータ

公開鍵暗号におけるリスクとは？

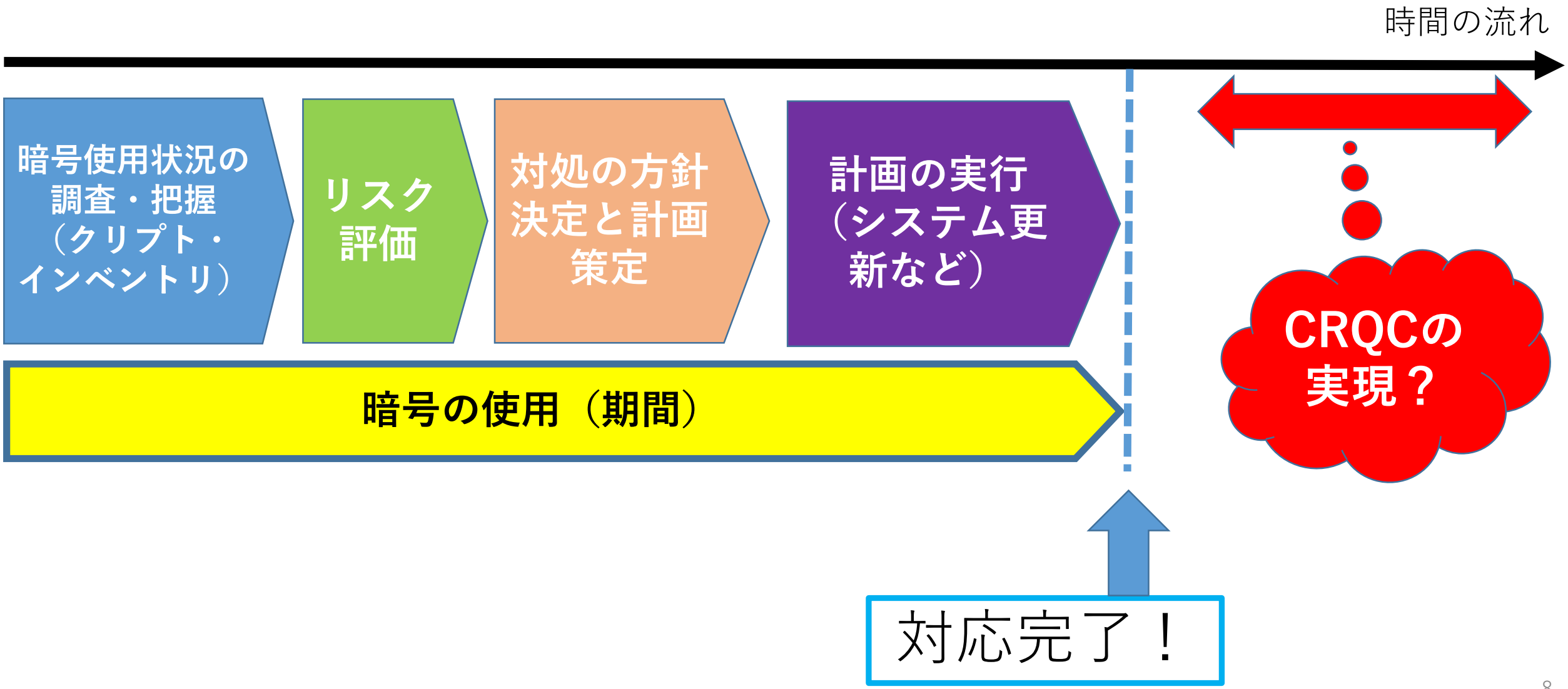
- CRQCが実現すると、過去の暗号化データ（攻撃者が入手しておいたもの）が一気に解読される？
  - ハーベスト攻撃
- 過去のデジタル署名付きデータも改変される？
  - 過去の署名付き文書が信頼を失う可能性
- これらのリスクが許容範囲を超えるのであれば、暗号の更新など、何らかの対処が必要に



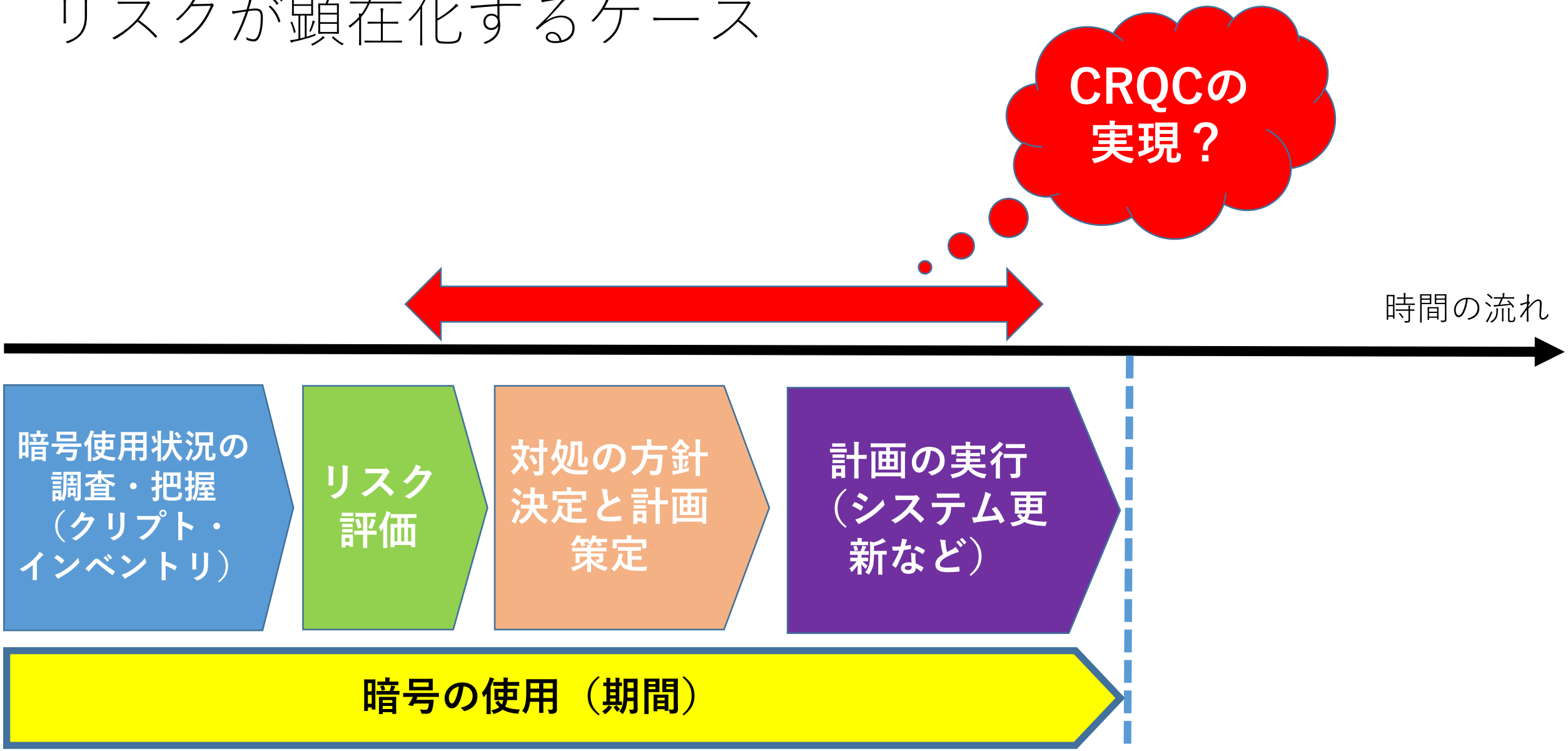
インフラ化した暗号への対処は容易でない？

- 公開鍵暗号を使用している機器やサービスは多種多様
  - パソコン、スマートフォン、ICカード、POS（Point-of-Sales）端末、ATMなど
- 個々の組織が関係するシステムのうち、自らコントロールできる範囲や程度が区々に
  - オンプレミスのシステム
  - アプライアンスやクラウド
  - 個人所有の端末や、ビジネス上関係する他組織のシステム
- ステークホルダーも多様化
- 対処には相応の時間がかかる可能性

CRQCが実現する前に対応を終わらせたい



リスクが顕在化するケース



いつ、着手すればよいのか？

- CRQCの実現可能性や（実現するとすれば）その時期の見通しは、専門家によって区々
- 「実現するかどうかもわからない（あるいは、実現する時期の見通しもあいまいな）のに、リスクを評価する意味はあるのか？」という意見も
  - リスクに向き合う姿勢次第
- CRYPTRECはCRQCやPQCの動向を調査し、ガイドラインや技術報告書を公表
- この問題に関して**海外のセキュリティ当局**はどのようなスタンスなのか？

自分の組織の対応を考えるうえで参考に

CRYPTREC: Cryptography Research and Evaluation Committees

1. 背景

2. 海外のセキュリティ当局のスタンス

3. 金融分野での検討事例

サーベイの対象

① アメリカ
② イギリス
③ オーストラリア
④ オランダ
⑤ カナダ
⑥ ドイツ
⑦ フランス

アメリカ

- 2030年を目途に、連邦政府機関で使用する暗号アルゴリズムをPQCに移行することを企図
- 2016年～：PQCのアルゴリズムを標準化（NIST）
  - 暗号化／鍵カプセル化、デジタル署名のPQC
  - 3つのアルゴリズムの標準規格（FIPS）案を2023年8月に公表[1]
- 2022年～：暗号を使用しているシステムのインベントリ作成などを推進[2, 3]
  - （M-23-2）Migrating to Post-Quantum Cryptography
  - （M-23-18）Administration Cybersecurity Priorities for the FY 2025 Budget

NIST: National Institute of Standards and Technology

[1] https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography
[2] https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
[3] https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf

イギリス

- NCSCが2020年にホワイトペーパーを公表[1]
  - 「Preparing for Quantum-Safe Cryptography」
- 「長期間保護すべきデータを有する組織はハーベスト攻撃に留意すべき」
  - 「対処方法としてPQCへの移行が最も望ましい」
  - 「PQCのアルゴリズムはしかるべき標準化機関などによる評価を経て標準化されたものに限定」
  - 「NISTによる標準化の動向をフォローしつつ各アプリケーションに適したアルゴリズムを今後特定・推奨していく予定」
- PQCへの移行に関する推奨事項
  - インベントリの構築
  - 暗号を使用している部分や製品の依存関係の明確化
  - 対応の優先順位の決定

  ・・・

「Quantum-Safe Cryptography」や「Quantum-Resistant Cryptography」と呼ばれるケースもある

NCSC: National Cyber Security Centre

[1] https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography

オーストラリア

- ASDが2023年にガイダンス（改訂）を公表[1]
  - 「Planning for Post-Quantum Cryptography」
- 「PQCは、CRQCが実現したとしても安全な通信を維持するための実用的な手段」
  - 「NISTの標準化アルゴリズムを参考にしながらPQCのアルゴリズムを評価・選定」
  - 「選定したアルゴリズムを、承認暗号アルゴリズムのリスト（ASD-Approved Cryptographic Algorithms）に追加予定」
- PQCへの移行に関する推奨事項
  - インベントリの整備
  - 公開鍵暗号によって保護されているデータの価値の特定
  - ベンダーやPQCの研究者との連携
  - PQCに関する調査研究・テスト・実証実験の実施

  ・・・

ASD: Australian Signals Directorate

[1] https://www.cyber.gov.au/sites/default/files/2023-05/PROTECT%20-%20Planning%20for%20Post-Quantum%20Cryptography%20%28May%202023%29.pdf

オランダ

- NBVが2021年にガイドラインを公表[1]
  - 「Prepare for the Threat of Quantum Computers」
- 「2030年以降も保護が必要なデータが存在する場合、ハーベスト攻撃による解読のリスクがある。当該リスクを評価し、必要があれば対処方法の検討に着手すべき」
  - 対処方法としてPQCへの移行を検討することを推奨
  - 間に合わなければ、公開鍵暗号による保護などの対応を推奨
- PQCへの移行に関する推奨事項
  - インベントリの整備
  - ハイブリッド方式の採用
  - Classic McElieceまたは FrodoKEMの使用
  - ベンダーのPQC対応状況の問合せ
  - クリプト・アジリティの向上に資する対応

  ・・・

NBV: Nationaal Bureau voor Verbindingsbeveiliging（英語名称：Netherlands National Communications Security Agency）

[1] https://english.aivd.nl/binaries/aivd-en/documenten/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers/Prepare+for+the+threat+of+quantumcomputers.pdf

カナダ

- CSEが2021年にガイダンスを公表[1]
  - 「Preparing Your Organization for the Quantum Threat to Cryptography」
- 「ITシステムにおいて中長期間使用する情報がCRQCによるリスクにさらされるおそれがある」
  - 「CRQCに耐性をもつ暗号への移行計画を検討する」
  - 「標準化されたPQCが利用可能になったタイミングでそれを実装すべき」
- PQCへの移行に関する推奨事項
  - CRQCによるリスクにさらされる情報の特定（リスクアセスメントの一環）
  - ITシステムのライフサイクルの見直し
  - ソフトウェアやハードウェアのアップデータのための予算の確保、研修の実施
  - ベンダーによるPQC実装への対応状況の把握とPQC採用の要請

  ・・・

CSE: Communications Security Establishment

[1] https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsap00017-e.pdf

ドイツ

- BSIが2021年にガイドラインを公表[1]
  - 「Migration to Post Quantum Cryptography, Recommendations for action by the BSI」
- 「長期的にみると、今後PQCが広く採用される」
  - 「適切なリスク管理手法に基づいて暗号の移行の必要性や時期に関する検討に着手すべき」
  - 「NISTの標準化の結果を考慮しつつ、ガイドラインに追加する可能性」
- PQCへの移行に関する推奨事項
  - クリプト・アジリティの付与
  - ハイブリッド方式の採用
  - FrodoKEMやClassic McElieceの採用
  - （PQC移行の時間的余裕がない場合）オフラインによる事前鍵共有

  ・・・

BSI: Bundesamt für Sicherheit in der Informationstechnik（英語名称：Federal Office for Information Security）

[1] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Migration_to_Post_Quantum_Cryptography.pdf

フランス

- ANSSIが2022年にポジション・ペーパーを公表[1]
  - 「ANSSI views on the Post-Quantum Cryptography Transition」
- 「ハーベスト攻撃によるリスクを適切に評価し、それを許容できない場合には、可能な限り早期にPQCへ移行すべき」
  - もっとも、「PQC単独での使用は当面推奨しない」
  - PQCのセキュリティに対する信頼が十分醸成されるまで待つ
- PQCへの移行に関する推奨事項
  - ハイブリッド方式の採用
  - CRYSTALS-Kyber、FrodoKEM、CRYSTALS-Dilithium、Falconを推奨
  - クリプト・アジリティの実現
  - ・・・

ANSSI: Agence Nationale de la Sécurité des Systèmes d'Information（英語名称：French National Cybersecurity Agency）

[1] https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

考察

- 概ね共通している点
  - ハーベスト攻撃によるリスクの認識
  - リスク評価に着手するタイミング
    - 特にカナダ（CSE）やフランス（ANSSI）は緊要性を強調
  - PQCとのハイブリッド方式の採用
- 差がみられる点
  - PQCの推奨アルゴリズムの提示や種類
  - 標準化されたアルゴリズムの推奨
- 論点となりうる事項
  - クリプト・インベントリ
  - クリプト・アジリティ
  - ベンダーへの対応

ハイブリッド方式（セッション鍵のケース）

- 現代暗号とPQCの両方を用いてセッション鍵を生成
- 現代暗号とPQCのどちらかが生き残ればセッション鍵は解読されない

1. 背景説明
2. 海外のセキュリティ当局のスタンス

3. 金融分野での検討事例

FS-ISACの活動

- Post-Quantum Cryptography Working Groupを設置
- CRQCが金融サービスのセキュリティに及ぼしうる影響や対処方法を検討
- 4つの技術報告書（technical paper）を公表[1]
  - Infrastructure Inventory
  - Risk Model
  - Current State (Crypto Agility)
  - Future State

FS-ISAC: Financial Services Information Sharing & Analysis Center
[1] https://www.fsisac.com/knowledge/pqc

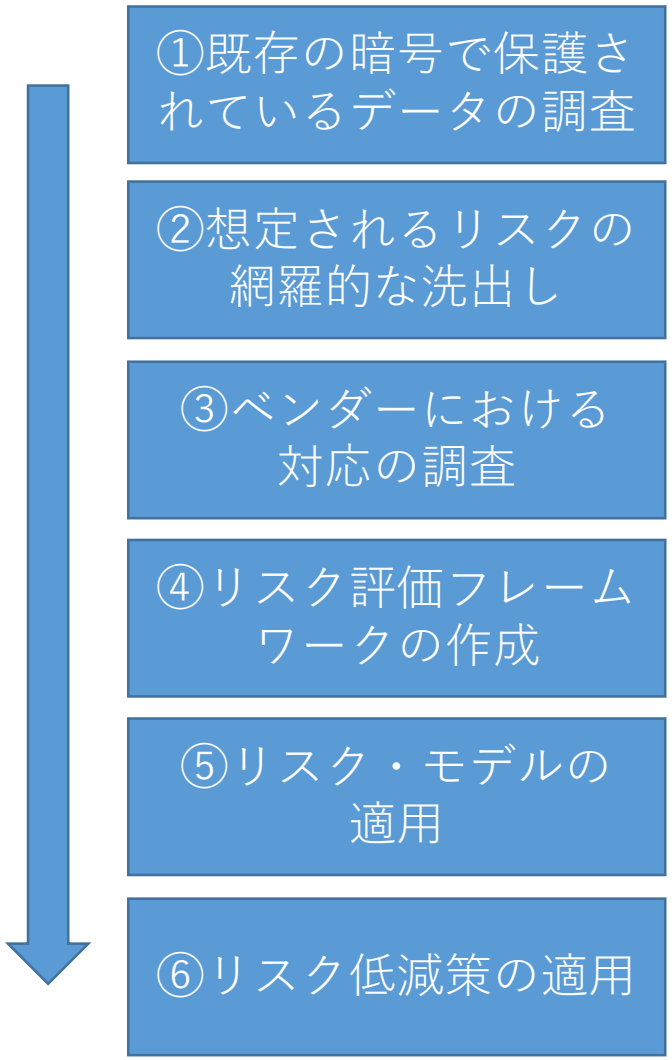
技術報告書のサマリー・ペーパー

- 「Preparing for a Post-Quantum World by Managing Cryptographic Risk」[1]

- CRQCによるリスクと対応のスタンス：
  - 「CRQCの完成時期の予測可能性によらず、そのリスクに対応することができるように情報セキュリティ・システムの準備を直ちに開始しなければならない」
  - 「従来型コンピュータの性能向上によるリスクにも留意の要」
  - 「CRQCと従来型コンピュータの両方に対してセキュリティを確保し、既存のITシステムとの相互運用性が高いセキュリティ・プロトコルを、PQCを用いて開発することが重要」

[1] https://www.fsisac.com/hubfs/Knowledge/PQC/PreparingForAPostQuantumWorldByManagingCryptographicRisk.pdf?hsLang=en

PQC移行準備のロードマップ



①既存の暗号で保護されているデータの調査

①既存の暗号で保護されているデータの調査

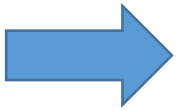
②想定されるリスクの網羅的な洗出し

③ベンダーにおける対応の調査

④リスク評価フレームワークの作成

⑤リスク・モデルの適用

⑥リスク低減策の適用



（クリプト・インベントリの整備）

- 暗号の使用状況の調査
- 保護対象のデータや情報資産の種類・属性の調査
- 収集した情報の適切な管理
- 情報収集時の留意事項も列挙

□　詳細は「Infrastructure Inventory Technical paper」を参照[1]

[1] https://www.fsisac.com/hubfs/Knowledge/PQC/InfrastructureInventory.pdf?hsLang=en

②想定されるリスクの網羅的な洗出し
③ベンダーにおける対応の調査

①既存の暗号で保護されているデータの調査

②想定されるリスクの網羅的な洗出し

③ベンダーにおける対応の調査

④リスク評価フレームワークの作成

⑤リスク・モデルの適用

⑥リスク低減策の適用

- 想定されるリスクの洗出し
- 残余リスク（足許の対策ではカバーしきれないリスク）の明確化

- PQCに関するベンダーへの要求事項の検討
- ベンダーに関するリスク評価プロセスの見直し
- 暗号移行へのベンダーの対応状況の問合せ[1]

[1] https://www.fsisac.com/hubfs/Knowledge/PQC/RiskModel.pdf?hsLang=en

④リスク評価フレームワークの作成ほか

①既存の暗号で保護されているデータの調査

②想定されるリスクの網羅的な洗出し

③ベンダーにおける対応の調査

④リスク評価フレームワークの作成

⑤リスク・モデルの適用

⑥リスク低減策の適用

- 残余リスクを分析するためのツールを作成

【代表例】

  - Quantum Risk Assessment
  - Crypto Agility Risk Assessment

- 残余リスクを定量的に評価

- PQC搭載の製品を導入
- クリプト・アジリティを向上

まとめ

- 海外の主なセキュリティ当局はCRQCによるリスクへの対応に着手することを推奨
  - クリプト・インベントリの整備
  - 中長期間保護するデータに関するリスク評価

- FS-ISACでは、Post-Quantum Cryptography WGにおいて検討が進められている（技術報告書を公表）

- わが国においても、こうした情報を参照しながらCRQCによるリスクへの対処に関して議論・検討を深めていくことが肝要

ご清聴ありがとうございました