量子ICTフォーラム・セミナー

# 量子コンピュータに耐性をもつ暗号への移行：金融分野における検討動向

2023年12月20日

宇根　正志
日本銀行金融研究所


本資料は2023年11月16日の時点での情報に基づいています。
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　　システム開発・管理に従事（～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）

日本ソフトウェア科学会（正会員）

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. 量子コンピュータへの対応に関する
   海外のセキュリティ当局のスタンス
2. 金融分野での検討事例

# 1. 量子コンピュータへの対応に関する海外のセキュリティ当局のスタンス

2. 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

〈アイウエオ順〉

# アメリカ

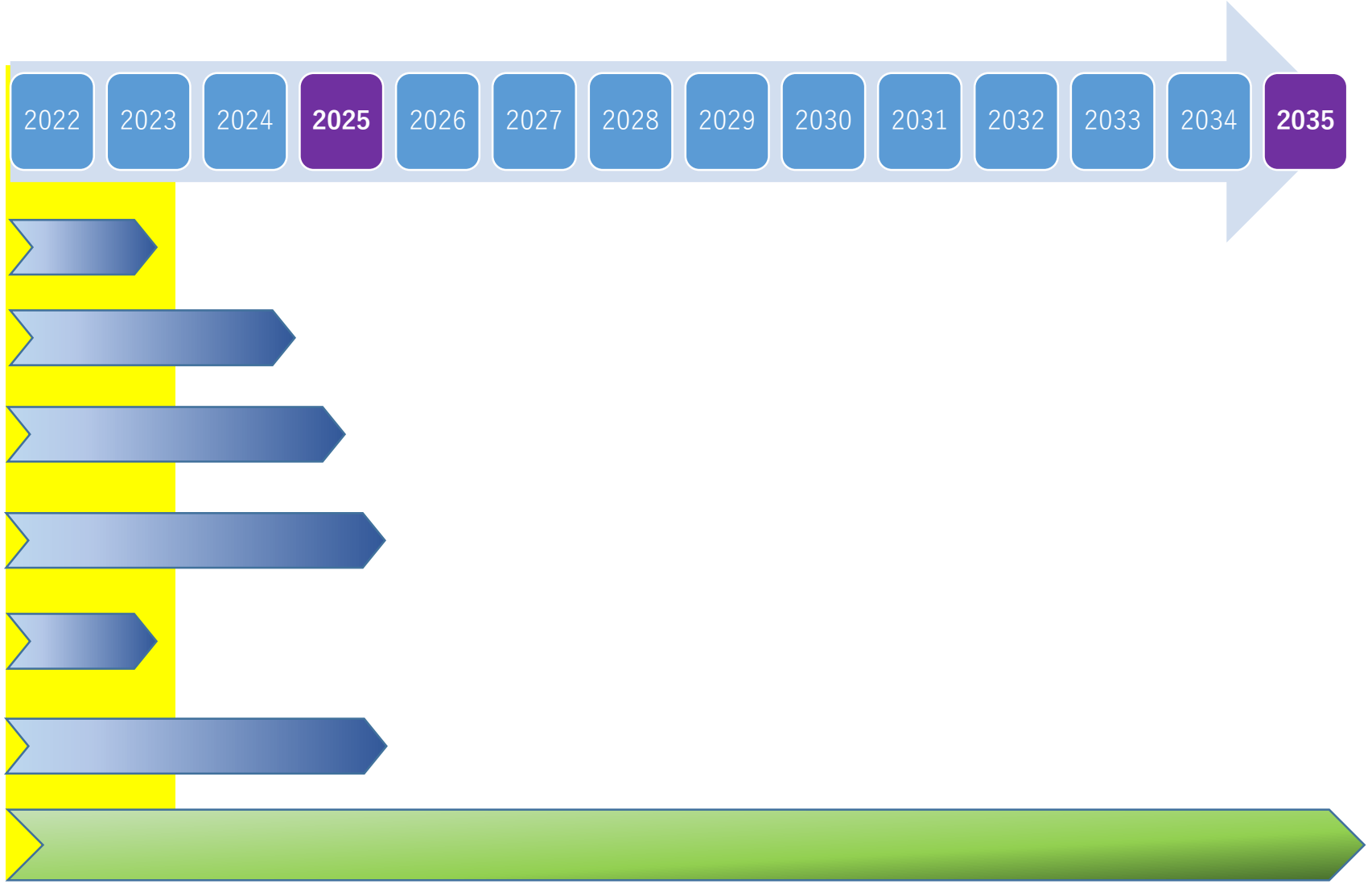
- **量子コンピュータによる産業競争力向上の可能性とそれによる暗号解読リスクとをバランスさせる**ために、量子コンピュータ（CRQC：cryptanalytically relevant quantum computer）でも解読困難な次世代暗号を標準化し、連邦政府機関の情報システムに導入する方針[1]

- 2016年～：PQC（post-quantum cryptography）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[2]

- 2022年～：暗号を用いるシステムのインベントリ作成などを推進[3, 4]
  - （M-23-02）Migrating to Post-Quantum Cryptography
  - （M-23-18）Administration Cybersecurity Priorities for the FY 2025 Budget

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
[2] https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography
[3] https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf
[4] https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf

# National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (May 2022)



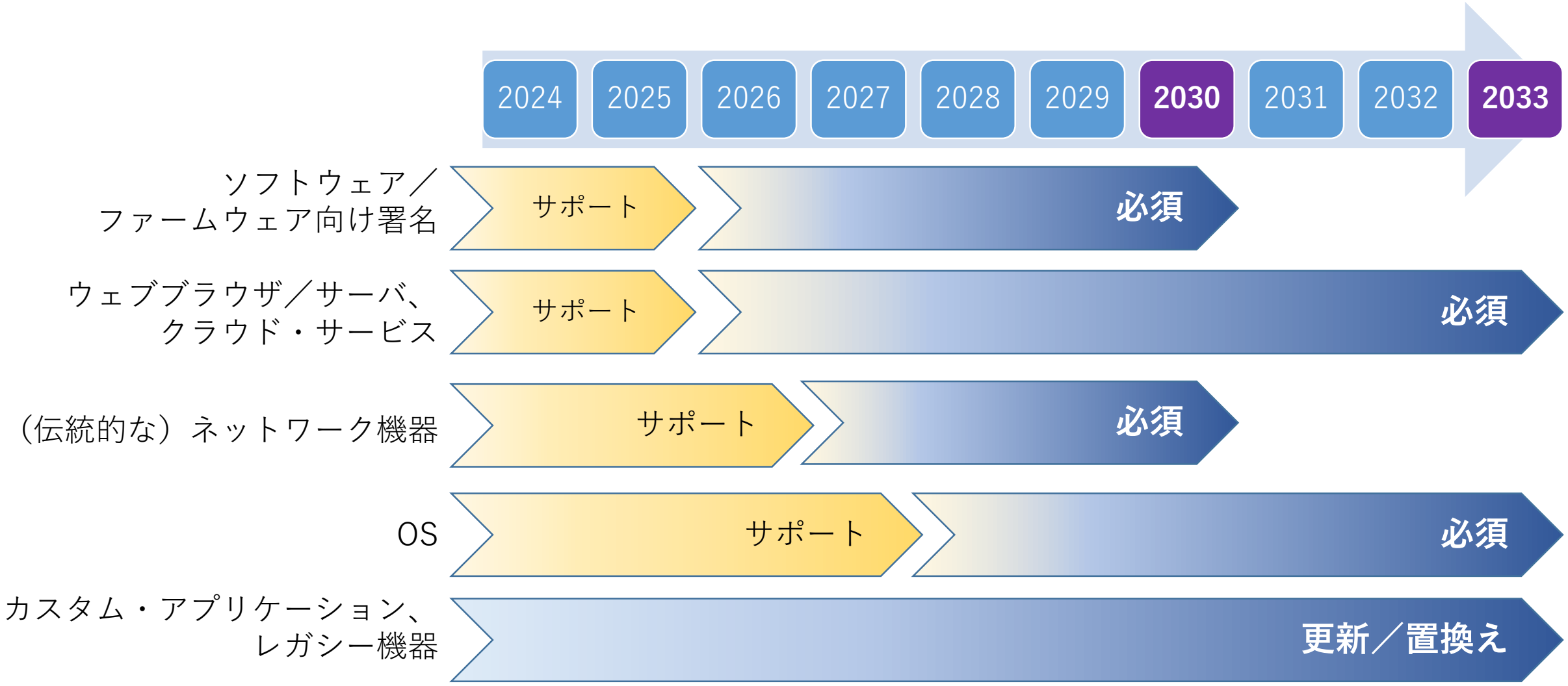

https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

# 国家安全保障関連システム向け機器における暗号スイート（CNSA）2.0 (NSA, Sept. 2022, version 1.0)

| | CNSA 1.0 | CNSA 2.0 |
|---|---|---|
| ブロック暗号 | AES-256 | AES-256 |
| ハッシュ関数 | SHA-384 | SHA-384 or **SHA-512** |
| 鍵共有 | RSA-3096 or ECDH P-384 | **CRYSTALS-Kyber (level V)** |
| デジタル署名 | RSA-3096 or ECDSA P-384 | **CRYSTALS-Dilithium (level V)** |
| ソフトウェア／ファームウェア向けの署名 | | **LMS or XMSS (LMS: SHA-256/192 recommended)** |

https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf

# NSAによるタイムライン：CNSA 2.0の採用




https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf

# イギリス

- NCSCが2023年にガイダンス（アップデート版）を公表[1]
  - 「Next Steps in Preparing for Post-Quantum Cryptography」
- 「非常に価値の高いデータを公開鍵暗号によって長期間保護する必要がある組織においては、**CRQCはまだ実現していないものの、ハーベスト攻撃が将来可能になりうるという意味で、現時点で大きな脅威になっているといえる**」
  - 「対処方法としてPQCへの移行が最も望ましい」
  - 「**NISTが標準化するPQCを推奨（右図参照）**」
- PQCへの移行に関する推奨事項
  - **ハイブリッド方式の採用（PQ/T hybrid scheme）**
    - **長期的にはPQCのみの使用に移行することを展望**
  - PQCの実装はNISTの標準化が完了してから開始

| 用途 | PQC |
|---|---|
| 鍵共有 | CRYSTALS-Kyber |
| デジタル署名（汎用） | CRYSTALS-Dilithium |
| デジタル署名（コード署名用） | SPHINCS+<br>LMS, XMSS |

NCSC: National Cyber Security Centre

[1] https://www.ncsc.gov.uk/pdfs/whitepaper/next-steps-preparing-for-post-quantum-cryptography.pdf

# 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の場合、**ハーベスト攻撃による解読のリスクを評価**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
- 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**
  - **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」
  - 「標準化されたPQC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（インベントリの活用）**
  - 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更新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（KEM）
  - （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2023年にポジション・ペーパー（アップデート版）を公表[1]
  - 「ANSSI views on the Post-Quantum Cryptography Transition (2023 follow up)」
- 「すべての企業・組織に対して、**量子コンピュータによる脅威をリスク分析に含める**とともに、**リスク軽減策の暗号製品への適用について検討する**ことを推奨する」
  - 「2030年以降も情報を保護するためのセキュリティ製品にはハイブリッド方式を推奨」
  - 「共通鍵暗号は少なくともAES-256以上のセキュリティを確保すべき」
- PQCへの移行に関する推奨事項
  - **NISTが選定したPQCに加えてFrodoKEMも推奨（右図）**
  - **ハイブリッド方式は標準化されたものや安全性証明付きのものの使用を推奨**
  - **ハイブリッド方式を実現する製品の認証を2024～2025年に実施予定**

| 用途 | PQC |
|---|---|
| 鍵共有 | CRYSTALS-Kyber<br>FrodoKEM |
| デジタル署名 | CRYSTALS-Dilithium<br>Falcon, SPHINCS+<br>LMS, XMSS |

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

[1] https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography

# スタンスや推奨事項

- 複数の先が指摘・推奨している点
  - ハーベスト攻撃によるリスクの認識と評価の必要性
    - 特にカナダ（CSE）やフランス（ANSSI）は緊要性を強調
  - クリプト・インベントリの整備
  - PQCとのハイブリッド方式の採用
  - クリプト・アジリティの付与
  - ベンダーとの連携や対応

# QKDに関する見方

| 国 | 公開資料での記述 |
|---|---|
| アメリカ<br>（NSA [1], 2021） | • 通信相手の認証手段を別途準備する必要。専用のQKD機器・通信路も必要<br>• 中継設備のセキュリティ管理が別途必要であるほか、内部犯罪対策も必要<br>• QKD装置の安全な実装方法が確立していない<br>• 課題が解決しない限り、QKDの使用をサポートしない |
| ドイツ<br>（BSI [2], 2023） | • 通信距離の制約、専用装置の必要性といった実用上の制約がある<br>• 安全性証明可能な標準化されたプロトコルが存在しない<br>• 特別なユースケースにおいてのみ適用可能 |
| フランス<br>（ANSSI [3], 2022） | • 専用の通信インフラが必要であり、限定された用途にのみ適用可能 |
| イギリス<br>（NCSC [4], 2020） | • 専用のハードウェアが必要であるほか、デジタル署名の機能を提供しない |
| オランダ<br>（NBV [5], 2021） | • 通信相手の認証手段を別途準備する必要<br>• 適切な安全性証明が付与されたQKD実装が存在しない<br>• 通信距離の制約があり、長距離の場合には中継設備を安全に管理する必要 |
| カナダ<br>（CSE [6], 2021） | • セキュアかつスケーラブルなQKDの開発はまだ途上にある<br>• 現時点では公開鍵暗号の代替となるとはいえないが、将来可能になるかもしれない |

[1] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
[2] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf
[3] https://cyber.gouv.fr/en/publications/anssi-views-post-quantum-cryptography-transition
[4] https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography
[5] 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
[6] https://www.cyber.gc.ca/sites/default/files/cyber/publications/itsap00017-e.pdf

1. 海外のセキュリティ当局のスタンス

# 2. 金融分野での検討事例

- FS-ISAC
- ASC X9


# FS-ISACの活動

- Post-Quantum Cryptography Working Groupを設置
- CRQC（cryptographically relevant quantum computer）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
- 技術報告書（technical paper）を2023年に公表[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

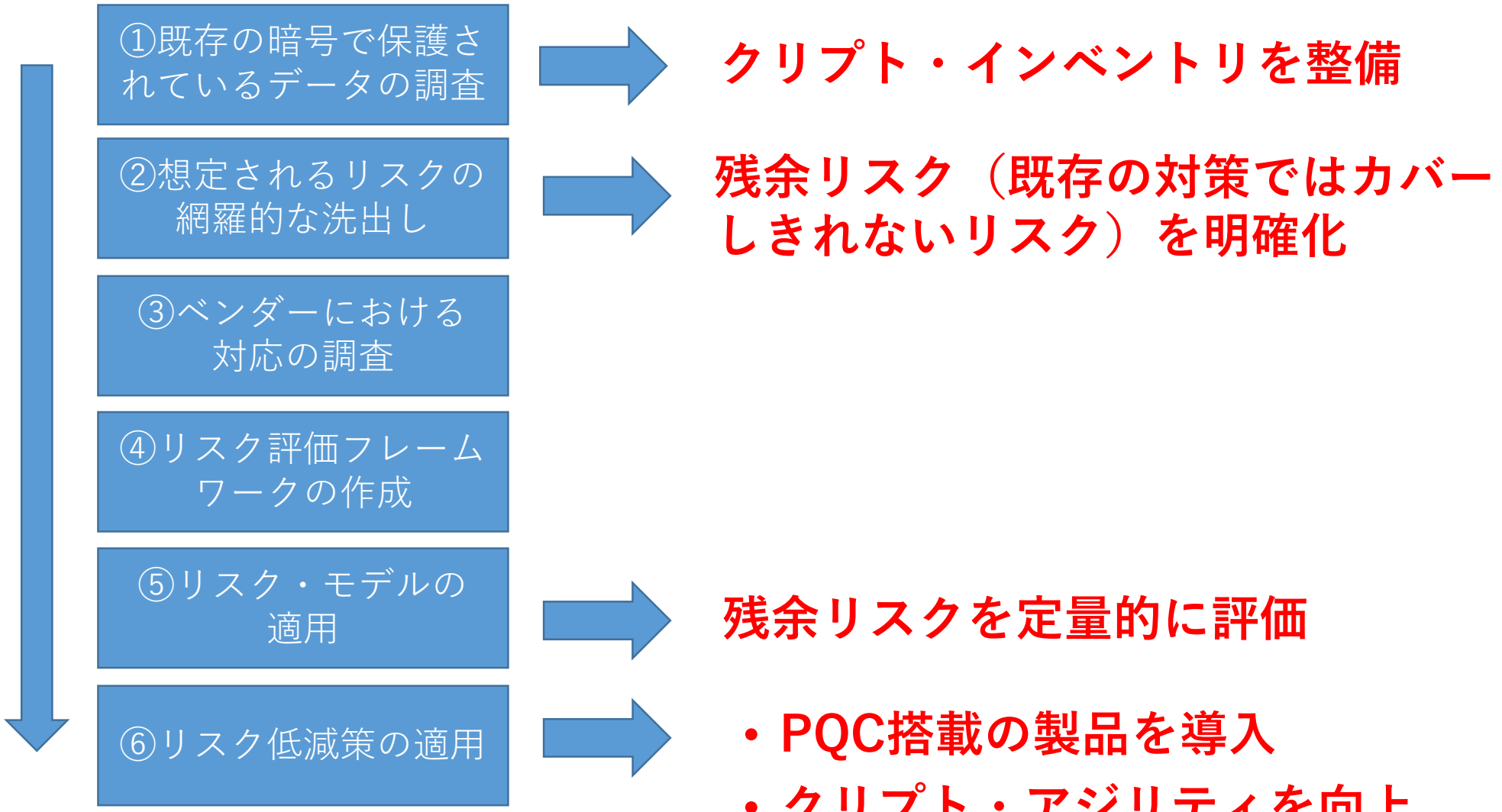
# 技術報告書のサマリー・ペーパー

- 「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ため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する必要」
  - 「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**しつつ、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によっ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



# ASC X9の活動

- X9F Quantum Computing Risk Study Groupを設置
- Informative Reportを2022年に公表
  - 「Quantum Computing Risks to the Financial Services Industry」[1]
- レポート：以下の情報を提供
  - CRQCによる脅威やリスク
  - 量子コンピュータの動作や構成
  - PQCとその標準化の動向
  - **脅威やリスクを評価・軽減するための対応**

ASC X9: Accredited Standards Committee X9 Inc.
X9F: Data & Information Security Subcommittee
[1] https://x9.org/download-qc-ir

# エグゼクティブ・サマリー（レポート 1節）

- 近年、**CRQCに対する見方が変化している**
  - 従来：CRQCの開発の障害となっている課題や技術的障壁を**解決できるか**？
  - 最近：課題や技術的障壁は**いつ解決されるか**？
- **CRQCの影響を検討し対応に向けた計画を立案すべき**
  - CRQCの影響を受ける資産を特定し、それらを保護する方策を決定
- CRQCの実現が見込まれる時期は5～30年後
  - 研究開発投資の金額、技術的課題の解決能力などに依存
- 時間が経過すれば、CRQC実現のタイミングを予測しやすくなる反面、準備や計画立案の時間が減少

# 暗号移行のための示唆（レポート 13節）

- 暗号移行戦略（quantum-safe migration strategy）のポイント

A）CRQCとそのインパクトの概要を理解

B）CRQCを用いた攻撃に対処するためのツール、技術、標準規格の概要を理解し、これらの動向をフォロー

**C）脆弱な暗号の使用箇所と形態を特定（クリプト・インベントリの整備）。自社の業務やサービスへの影響を評価**

**D）対処用ツール等の適用箇所を特定。自社のサプライチェーンに含まれるサプライヤーに暗号移行戦略の立案を要請**

**E）Proof-of-conceptを実施し対処方法の効果を検証**

F）有効性を確認した対処方法の実施計画を立案

# QKDに関する見方

- FS-ISAC
  - ― Future State Technical Paper[1]の記述
    - QKDの商用製品が発売され一部使用されているものの、通信距離の制約など、技術的な課題が残されている
    - 今後の技術開発により通信距離が実用的なレベルに達する可能性がある
- ASC X9
  - ― Quantum Computing Risks to the Financial Service Industry[2]の記述
    - 実用上の課題がいくつか残されている
    - ノード間の通信距離に制約がある
    - 中継ノードやエンドポイントにおけるセキュリティ管理にはコストがかかる
    - Denial-of-Service攻撃への対策が必要。設備の冗長化にはコストがかかる

[1] https://www.fsisac.com/hubfs/Knowledge/PQC/FutureState.pdf?hsLang=en
[2] https://x9.org/download-qc-ir

# おわりに

- 調査対象のセキュリティ当局は、CRQCによる暗号解読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
- 金融分野でもFS-ISACやASC X9が検討を推進
  - スタンスや課題認識、アプローチは外国セキュリティ当局と類似の方向性
- 技術的な課題として以下が挙げられる
  - クリプト・インベントリ
  - ハイブリッド方式
  - クリプト・アジリティ

# ご清聴ありがとうございました

関連する内容はこちら（↓）をご参照ください

宇根正志、「量子コンピュータが暗号に及ぼす影響にどう対処するか：海外における取組み」、金融研究所ディスカッションペーパー No. 2023-J-13、日本銀行金融研究所、2023年9月

https://www.imes.boj.or.jp/research/abstracts/japanese/23-J-13.html