金融分野における耐量子計算機暗号への移行に向けた動向について

2024年7月18日
事務局提出資料

※本資料は７月18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

背景

- 量子コンピュータの実現と普及は、一方で社会に恩恵をもたらすが、他方で既存の暗号化技術を危殆化させ、金融機関及び金融システムのリスクを増大させる可能性もある
- 攻撃者は、量子コンピュータを暗号の解読のために使用する可能性があり、顧客情報を含む金融機関の情報が脅威に晒されるおそれがある。攻撃者は、現在解読できない暗号でも、量子コンピュータにより、後日解読可能となることを想定し、秘密情報を取得しておく攻撃（所謂「ハーベスト攻撃」）を行っている可能性があり、顧客情報と金融機関に対する信用が将来脅かされるおそれがある
- こうした中、米国の国立標準技術研究所（NIST）において、耐量子計算機暗号（PQC）技術の基準作りが進められており、新暗号化方式の標準が2024年に公表される予定である

金融分野の特性

- 量子コンピュータの技術の発展及び既存の暗号が危殆化する時期については不透明な部分が多く、約10年内に量子コンピュータが実用化され、暗号が危殆化するとの見方があるが、その時期は遅行する可能性もあれば、早期化する可能性もある
- ただ、金融機関が、既存の暗号の危殆化によって脅威に晒され得る情報資産を洗い出し、重要性に応じて優先順位を付け、システム投資を含めた対応を行うには、数年以上の時間と多くのリソースが必要となると考えられる。このため、金融機関はできる限り早期に準備を始めることが期待されている
- 求められる対応として次の取組みが指摘されている*

  i) リスクとリスク低減のための戦略について理解を深める

  ii) リスクを評価する

  iii) リスク低減のための計画を策定する

*例えば、以下を参照のこと。
- FS ISAC (March 2023), “Preparing for a Post-Quantum World by Managing Cryptographic Risk”
- Monetary Authority of Singapore (February 2024), “Advisory on addressing the cybersecurity risks associated with quantum”

1.リスクとリスク低減戦略の理解

- 以下のような取組みにより、量子コンピュータの最新動向の把握に努め、量子コンピュータに伴うサイバーリスクとそのリスクを軽減するための戦略についての理解を深める
  - 経営陣が、量子技術の潜在的な脅威及び早期対応の重要性を理解し、PQCへの移行に関する調査、リスク評価、計画策定などの社内の取組みをサポートする
  - ITベンダーと連携し、ITサプライチェーンのリスクを評価する
  - 情報共有とリスクの低減の促進のため、業界団体、研究機関、ISAC等と連携する

2.リスクの評価

- 量子コンピュータのリスクを評価する
  - 組織内の技術担当の最高責任者や重要なITベンダーと議論する
  - リスク低減を優先すべき領域を特定するため、クリティカルなデータ、現行の暗号技術の使用状況（組織内及び重要なサードパーティにおける下記の情報）などの情報を含むインベントリ作成に着手する
    - ✓ 暗号アルゴリズムと鍵の長さ
    - ✓ 暗号化された資産の所管部署と責任者
    - ✓ 暗号アルゴリズムが埋め込まれていて現在使用中のシステムまたはアプリケーション
  - 資産に優先順位を付けるため、脆弱な暗号手段に依拠したIT及びデータ資産を、機密性、重要性、IT資産・データ資産のリスクエクスポージャ、期間に基づいて分類する
  - 既存のシステムインフラが暗号アジリティを支えるか否かを評価し、仮に耐量子計算機暗号への移行を阻害するような制約（処理能力、インフラのデザイン、ベンダーサポートの終了など）があれば時間をかけてアップグレードすることを検討する

3.リスク低減のための計画の策定

- リスクに対処するための戦略を立て、能力を構築する
  - 計画に戦略を推進するためのガバナンス体制の整備を盛り込むとともに、関係者の役割・責任を明確化する。また、主要なマイルストーンを設定する
  - 関連スタッフの技術的な能力を向上させる
  - 内部規定を見直す
  - 耐量子計算機暗号に移行できない資産のリスク低減戦略を構築し、また、予想されたタイムラインよりも早く量子コンピュータに伴うサイバーセキュリティリスクが発現したコンティンジェンシーのシナリオの下での計画を立てる
  - リソースが許せば、業務への潜在的な影響や実施上の課題を検証するため、量子セキュリティソリューションPOCトライアルを検討する

PQCレポート作成作業部会（案）

●役割

- 論点を事前に抽出し、検討会での議論のたたき台を作成
- 検討会の結果を踏まえ、議論の結果を成果物としてまとめる
  - ✓今年中に公開予定とされている米国国立標準技術局の暗号標準化文書や今年度末に公開予定とされているCRYPTRECにおけるPQCに関するガイドなどに関する情報も考慮する

●構成員

※事務局注：7月18日開催時点から、更新したもの（7月25日時点）

役割	氏名	所属
部会長	福田 健太	三井住友銀行、金融ISAC FinTechセキュリティWG
メンバー	森 雄喜	三井住友銀行、金融ISAC FinTechセキュリティWG
	長田 繁幸	日本総合研究所
	伊藤 彰志	みずほ銀行
	中山 雄司	みずほ銀行
	設楽 佑一郎	三菱UFJ銀行
	岡野 裕樹	三菱UFJ銀行、金融ISAC FinTechセキュリティWG
	唐沢 勇輔	Japan Digital Design株式会社、金融ISAC FinTechセキュリティWG
	宇根 正志	日本銀行金融研究所
	神田 雅透	情報処理推進機構
	伊藤 忠彦	情報処理推進機構
	鷲見 拓哉	情報処理推進機構