2. 耐量子計算機暗号に関わる国内動向

要約

- 耐量子計算機暗号とは、十分な計算能力を持つ量子コンピュータが実現しても安全であると期待されている暗号である。
- 日本では CRYPTREC や日本銀行、金融庁によって耐量子計算機暗号についての調査や対応が進められている。
- インベントリの作成などによって、今からでも耐量子計算機暗号への対応を始めることができる。

耐量子計算機暗号とは何か？

現代の通信はさまざまな暗号技術を組み合わせることで安全を確保しています。その暗号技術の中でも中心的な公開鍵暗号では、RSA 暗号や楕円曲線暗号がよく用いられています。しかし、これらは十分な計算能力を持つ量子コンピュータによって効率よく攻撃できることが Shor によって示されました。

未来の通信の安全性を確保するために、そのような量子コンピュータに対しても安全性が保たれると期待される暗号が求められています。そのような暗号を総称して耐量子計算機暗号（Post-Quantum Cryptography, PQC）と呼びます。

商用の量子コンピュータは既に存在するものの、現在使われている暗号を破れる程度の計算能力を持つ量子コンピュータは現時点では存在していません。しかし、将来的に実現すると想定して通常の通信によって署名や証明書などを、盗聴によって暗号化された通信やデータを集め、実用化されたタイミングで解読を試みるハーベスト攻撃(*1)の存在が指摘されています。

NISTIR 8105 では、現在の公開鍵暗号インフラの構築にほぼ 20 年かかったことを指摘し、これから耐量子計算機暗号への安全な移行を確保するためにも大きな努力が必要となるとしています。そのため、量子コンピュータがいつ実現するかの明確な予測がないながらも、各国政府や大手 IT 企業を中心に既に耐量子計算機暗号への移行が検討されています。特に、米国では米国国立標準技術研究所（NIST）が中心となって耐量子計算機暗号の標準化を推進し、2024 年 8 月 13 日には標準の最終版が公開されました。日本では CRYPTREC や日本銀行、金融庁によって耐量子計算機暗号についての調査や対応が進められています。

本記事では金融庁を中心とした国内動向について解説します。耐量子計算機暗号の詳細については拙著『耐量子計算機暗号とは何か　移行のために知っておきたいこと』をご参照ください。

日本銀行の動向

日本銀行金融研究所は 2015 年 7 月 7 日にディスカッションペーパー『量子コンピュータの解読に耐えうる暗号アルゴリズム「格子暗号」の最新動向』を公開し、それ以降も耐量子計算機暗号についての調査を継続的に行っています。また、2019 年 8 月 30 日には『量子コンピュータによる脅威を見据えた暗号の移行対応』を公開し、クリプトアジリティの重要性を指摘しています。

(*1) Harvest now, decrypt later 攻撃や store now, decrypt later 攻撃などとも呼ばれます。

2023 年 9 月 27 日には『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』を公開しています。このディスカッションペーパーでは、各国のセキュリティ当局の耐量子計算機暗号に関するガイドラインなどをまとめ、各国のスタンスやインベントリの整備、ハイブリッド方式、クリプトアジリティについての考察を述べています。

2024 年 9 月 26 日には、金融庁と共に G7 サイバー・エキスパート・グループ(*1)による『量子コンピュータの登場に伴う機会とリスクに備えた計画に関する G7 サイバー・エキスパート・グループによるステートメント』を公表しました。金融セクターにおける官民の主体として各国の金融当局は量子技術にかかわるリスクの評価や軽減、そのための戦略についての理解の向上や計画の策定を行うように提言を受けています。

金融庁の動向

金融庁は事務年度ごとに金融行政方針を公開しています。2024 事務年度の金融行政方針には、直近では見られなかった「量子」や「PQC」といった単語が登場しました。これらの単語はサイバーセキュリティに関する新たなリスクとして注釈に小さく記載されているにすぎませんが、比較的民間に近い位置にある金融庁も意識し始めているといえます。

記事の冒頭で述べている通り、量子コンピュータによる暗号技術の危殆化やハーベスト攻撃の可能性が指摘されています。そして、それらは金融機関及び金融システムのリスクを増大させ、信用を脅かす可能性があります。そこで、金融庁は、耐量子計算機暗号への移行に関する金融分野における課題や留意事項についての検討の一環として、2024 年 7 月 18 日に「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」の第 1 回を開催しました。その後、同年 9 月 20 日に第 2 回、同年 10 月 18 日に第 3 回を開催し、2024 年 11 月 26 日には『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』を公表しました。以下、検討会報告書の概要を解説します。

まず、冒頭に記載されたエグゼクティブサマリーでは、経営層が量子コンピュータによる暗号の危殆化リスクや耐量子計算機暗号への移行の期限などを正しく認識する必要があることを指摘しています。その上で、経営層がリーダーシップを発揮し、移行方針を決定することが望ましいとしています。続いて、米国政府が 2035 年をめどに耐量子計算機暗号への移行を推進していることから、各種法令や海外規制動向に耐量子計算機暗号への移行対応を盛り込む可能性を指摘しています。そこで、2030 年代半ばを目安に耐量子計算機暗号を利用可能な状態にすることが望ましいとしています。

続く 2 章では量子コンピュータが現代暗号やセキュリティ対策に与える影響についての一般論と移行における課題、3 章では国内外の対応状況についてまとめています。主に以下のような内容となっています：

	概要
2 章	● 公開鍵暗号は十分な計算能力を持つ量子コンピュータによって危殆化するおそれがあり、このことは金融サービスの運営に大きな影響を与える。 ● 暗号の移行に要する期間とデータの保護期間の和が十分な計算能力を持つ量子コンピュータの登場までの期間より長い場合、ハーベスト攻撃への備えを検討する必要がある。 ● 耐量子計算機暗号を使用可能とする時期は、各国の対応動向等を踏まえ、2030 年代半ばとするのが妥当。 ● 耐量子計算機暗号への移行には長期間を要し、そのため他の脆弱性への対応が遅れる可能性がある。 ● 耐量子計算機暗号は従来の暗号と比べて多くのリソースを必要とし、また耐量子計算機暗号自身が危殆化する可能性もある。 ● 上記課題への対応のためには、インベントリの作成やクリプトアジリティの確保、優先順位の設定といった事前の準備が望ましい。
3 章	● NIST によって耐量子計算機暗号のアルゴリズムが標準化され、IETF によって耐量子計算機暗号を取り込んだ通信プロトコルの標準化が進められている。 ● 米国を始めとした各国当局は耐量子計算機暗号アルゴリズムの性能評価や移行に関するガイダンス・ガイドラインの公表を行っている。 ● 金融業界では、FS-ISAC や ASC X9、UK Finance、DTCC、QSFF によって技術報告書やホワイトペーパーが公開されている。 ● ブラウザや IC カードなどで耐量子計算機暗号への対応事例が既に存在している。

出典：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』を基に大和総研作成

(*1) 2015 年の G7 財務大臣・中央銀行総裁会議の承認に基づいて各国の金融当局・財務省・中央銀行の間に設置された G7 の管轄区域におけるサイバーセキュリティについてのポリシーや戦略を調整する作業グループ。

4 章では、金融分野における耐量子計算機暗号への対応の必要性について述べています。基本的な移行対応については業種を問わないため、他業種の対応方針を参考にすることができます。しかし、金融業界では取引記録などを 7 年間保管することが法律(*1)で定められています。また、貸付期間が 7 年間を超える商品もあります。さらに、漏洩がレピュテーションに深刻な影響を与える情報や取引の内容や事実そのものが重要な情報といった優先して保護すべき情報も取り扱っています。そのような金融機関特有のデータに関しては、用途、保存環境、保存期間などが他業界と異なる可能性があるため、金融機関が主体的に検討することが望ましいとしています。

続いて、金融機関に対して起こり得る脅威シナリオとして UK Finance が例示したものを引用しています。具体的には、不正決済や取引記録の改竄、分散型台帳を基にした金融商品の完全性の喪失、インターフェースへの侵害をあげています。これらが実際に現実的なリスクとして表面化するには相当の時間を要するとしつつも、国内外の各種法令または規制に耐量子計算機暗号への対応などが盛り込まれる可能性が否定できないと指摘しています。

5 章では、金融分野における耐量子計算機暗号への対応に向けた推奨事項について述べています。移行スケジュールが不確実性を帯びていることから、移行についての基本的な考え方として、重要度が高く、量子コンピュータに対する脆弱性を持ち、悪用される可能性が比較的高いシステムを優先することをあげています。次に、移行におけるインベントリの構築やクリプトアジリティの確保の具体的な方法を述べています。

そして、移行対応は組織単独で完了するものではなく、IT ベンダーとの連携が必要であることを指摘しています。さらに、業界団体などの民間に対しても海外規制動向にかかわる情報収集や情報提供、監督当局と連携してのロードマップの策定が期待されています。

6 章ではこれまでの内容をまとめ、耐量子計算機暗号への対応に向けた課題や留意事項として以下のように述べています：

	要約
戦略・態勢面	● 経営層が全社施策としてリーダーシップを発揮して企画・推進することが望ましい。 ● ベンダーの対応に完全に依拠する対応には限界があるため、オーナーシップをもって取り組むことが望ましい。 ● 組織内では各部門の役割や責任を明確にすることが肝要である。 ● 共通化できる部分は他社と協力・分担することで効率的な対応が可能となる。 ● 対応の範囲は広く、期間も長期にわたるため、計画的にリソースを確保することが肝要である。 ● 特に、暗号領域の専門人材は不足している。
法令・規制面	● 各国の政府・省庁は既に耐量子計算機暗号への移行計画と指針を整備している。 ● 現時点では法令・規制として制定されているものは少ないが、法令・規制の整備状況を継続的に注視することが重要である。 ● 海外の取引先が耐量子計算機暗号への対応を先行させているために、自社でも対応を余儀なくされる可能性がある。 ● 海外当局との折衝、海外の法令・規制への遵守の必要性があるため、海外の法令・規制も継続的に注視することが重要である。
技術面	● クリプトアジリティの確保が重要で、そのためには暗号処理の疎結合化、証明書や暗号鍵の管理、利用状態の監視といった設計・実装・運用上の課題に留意する必要がある。 ● 耐量子計算機暗号への対応にあたっては標準化動向や技術の成熟度の把握が重要である。 ● 移行の過渡期には耐量子計算機暗号に対応済みのシステムと未対応のシステムが混在することから、互換性を考慮することが望ましい。 ● リソース最適化の観点から、大規模更改・改修に合わせることが望ましい。

出典：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』を基に大和総研作成

民間企業としてできること

検討会報告書の要約からも分かる通り、耐量子計算機暗号への移行にあたって考慮すべきことが多くあります。今から少しずつリスクや課題についての理解を深め、移行への事前準備を行うことが重要でしょう。

（松井　直己）

(*1) 犯罪による収益の移転防止に関する法律(平成 19 年法律第 22 号)