G7 サイバー・エキスパート・グループによる「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」の仮訳

目的

G7 サイバー・エキスパート・グループ（CEG）は、金融システムの安全性とレジリエンスにとって重要性を有するサイバーセキュリティ上の事項について、G7 の財務大臣及び中央銀行総裁に助言する。量子コンピュータが金融システムに及ぼし得る暗号のリスクを踏まえ、CEG は、量子耐性[1]のある（quantum-resistant）暗号及びクリプト・アジリティ（cryptographic agility）への移行に向けた協調的なアプローチを後押しするために本ロードマップを策定した。このステートメントは、指針や規制に関する期待を示すものではない。むしろ、この目的は、移行活動を支援するための情報と背景を提供し、主要な検討事項の整理、金融セクター全体で耐量子計算機暗号（post-quantum cryptography）への適時、安全、そして協調した移行を可能にするためのアプローチを提案することにある。

量子コンピュータがもたらす機会とリスク

2024 年 9 月に G7 CEG は量子コンピューティングに関する利点とリスクについてステートメントを公表した。このステートメントでは、量子コンピュータが金融サービスに重要な新機能をもたらす一方で、十分に高度な量子コンピュータはシステムやデータを保護するために広く利用される暗号プロトコルを破る能力を持つと指摘した。このリスクに対処する主な方法は、いわゆる耐量子計算機暗号及び量子耐性のある暗号アルゴリズムへの移行である。過去 1 年間で、多くの国家当局がガイダンスを公表し、金融エコシステムの一部の参加者は移行計画の策定及び量子耐性のある暗号アルゴリズムの実装を開始した。

金融システムにおける量子コンピューティングのリスクへの対応支援

2024 年のステートメントを踏まえ、G7 CEG は、将来的なリスクに先んじて、組織が耐量子計算機暗号への移行を協調的に、適時かつ目的に沿って進める上で役立ち得る各種活動について、上級管理職に情報提供するためのハイレベルのロードマップを策定した。このロードマップ及び付随するタイムラインは、あるべき規範を示すものではなく、リスクが顕在化する前に検討できる様々な活動について情報提供し、業務継続を支援することを目的とする。

---

[1] 本仮訳では、量子コンピュータを用いた暗号解読にも耐えられるような暗号にかかる安全性を「量子耐性」と訳す。

このロードマップは、G7 各法域の金融当局や産業界における専門家で構成される専任の CEG タスクフォースによって策定され、関連するフォーラムの広範なステークホルダーの意見を反映した。このロードマップは、各法域が柔軟性を保ちながら、法域間の協調と協力を推進するための考慮事項を示しており、暗号移行の計画策定及びガバナンスのための道標となり得る。

さらに、規模に依らず金融機関は、IT 製品、IT ベンダー、及びその他サードパーティの提供者に強く依存し、相互に接続されている。このロードマップは、これらの組織が金融セクターにおける量子耐性のある暗号の重要性及び暗号移行に際して想定される時間的制約を理解する一助となり得る。

耐量子計算機暗号への移行における考慮すべき事項

このロードマップは、暗号移行を円滑に行う上で重要であると G7 が考える幾つかの検討事項に基づいている。

柔軟性 ― このロードマップは、各組織の個別の事情を反映するための柔軟性を向上させることを意図している。変化するリスクを考慮して計画を修正するための継続的なモニタリングと再調整のためのメカニズムを備えている。

リスクベース・アプローチ ― すべての組織、システム、または機能が同じレベルのリスクに曝され、システム上の重要性を有するわけではない[2]。各組織は、最重要の領域に対して短期的なタイムラインを適用し、リスクの低い領域に対しては長期的なタイムラインを適用し得る。状況によっては、重要性の低いユースケースが、より重要なシステムの移行に先立ち経験を蓄積するための試行となり得る。

標準ベースのアプローチ ― 組織は、既存のロードマップや IT セキュリティ関連標準（例：ISO 27001、ITIL）を活用すること、及び、進捗管理、説明責任の履行、再調整を可能にするための定量的な評価指標を設定し得る。これらの評価指標は、組織的及びシステム横断的なレベルでの準備状況の評価に役立ち、金融エ

[2] 原文の脚注 5: これらの枠組みは、金融安定理事会（FSB）が定める重要機能（critical functions）の概念に基づいており、各組織によって実施される業務影響度分析（BIA）によって情報が補完される。民間部門の組織における「重要システム（critical systems）」の指定の責任は、主に各組織自身にある。他方、クリアリングや決済のプラットフォーム等の業界インフラを運営する公的機関は、特定のシステムを重要システムに指定し得る。

コシステム全体にわたる協調的なモニタリングを可能にする。

協力と連携 ― 各法域及びあらゆる規模・形態の金融機関の協力により、相互に学び合い、アプローチが断片化するリスクを軽減し、相互運用性（interoperability）を向上させることができる。さらに、サードパーティとの協力は、サードパーティに依存している点の能動的な管理を可能にするほか、提案されている暗号移行のタイムラインより早くサードパーティのソリューションを利用できる可能性を高める。とりわけ、ベンダー依存が高い中小規模の金融機関にとって、この効果は顕著である。

暗号移行にかかる各種取組と成果

以下の表は、金融機関及び金融当局による移行計画の策定のために、各フェーズにおける主要な取組とその成果に関する検討事項の概要を示している。金融機関としての機能も有する金融当局にとっては、これらのフェーズと取組は重複し得る。表は、順序的な移行フェーズの形式で整理されているが、暗号移行の取組が画一的又は段階的に進捗することを意味するものではない。また、多くの取組は並行して進み、繰り返し実施され得る。各組織は、リスクプロファイル及びシステムの複雑性と重要性に基づいて、各取組の実施時期と順序を調整し得る。この段階的アプローチは、移行計画の策定と協調のための共通の指針を提供するものであり、規範となる道筋を示すものではない。

主要な取組とその成果	想定される金融機関の取組	想定される公的機関の取組
1. 認識と準備	経営陣のリスク認識の醸成、量子耐性の確保に向けた初期戦略の策定及び主要な役割の明確化	量子耐性に関するサイバーリスクとその影響に係る経営陣の認識の醸成
	重要システム、機能、機密情報及び通信プロトコルの列挙	リスク、期待、またはガイダンスについてのステークホルダーとの明確なコミュニケーション
2. 検出とインベントリ	暗号に関する技術的・情報的資産（cryptographic assets）、通信プロトコル、関連するサードパーティ依存関係の包括的なインベントリの作成	金融機関及び公的セクターにわたるシステム全体を対象とした量子耐性の成熟度の評価
	人材、プロセス、組織及び技術的能力におけるギャップの洗い出し	リスク、効果的なプラクティス、またはステークホルダー向けガイダンスについての明確なコミュニケーション
3. リスク評価と計画	ツール、標準及び相互運用性を含めた、重要機能及び非重要機能についての移行計画の策定	金融機関に対して横断的に暗号移行を支援するための明確なコミュニケーション
	能力開発、ガバナンス及びリスク管理のための内部プロセスの適応	国内外のステークホルダー間においてコミュニケーションを強化し、整合性のとれた規制アプローチを支援
4. 移行実施	優先度の高い機能から段階的に量子耐性ソリューションを導入	暗号移行の進捗についてのモニタリング及び監督
	進化する量子技術の脅威動向に適応した暗号移行ペースの調整	想定される障壁の洗い出しと除去、及び能力開発の支援
5. 移行検証	暗号移行が完了した機能の検証	量子耐性について考慮すべき観点の規制アプローチへの織り込み
	エコシステムを指向した量子耐性の検証	量子耐性について考慮すべき観点の検証及び危機対応演習への組み込み
6. 検証とモニタリング	継続的な検証と改良	進化する量子技術の脅威動向に適応する政策枠組みの策定
	新しい暗号技術の標準の導入	業界の能力向上および知識普及のための継続的な支援

現状、多くの組織が、既に暗号移行のための実装の試行や量子耐性のある暗号コンポーネントの統合に着手している。例えば、ウェブ・インフラにおけるハイブリッド・モードの鍵交換が挙げられる。このロードマップは、上記のような積極的な取組を遅らせ、阻むものではない。むしろ、関連する製品や標準規格が利用可能になり、特定のユースケースで有効性が検証された時点で、移行を開始することは、組織にとって有益となり得る。また、クリプト・アジリティを移行計画の目標に組み込むことで、新たな脅威や脆弱性に対応するために暗号技術を適応させることも有益となり得る。

上記の取組と並行して、以下のような現在進行中の継続的な取組も、効果的な暗号移行を支援するために検討する余地がある。これらの一連の取組は、暗号移行のプロセス全体にわたって並行して実施され得る。

(1) **ガバナンスとリスク管理**：量子耐性のある暗号を、既存の組織ガバナンス及び公的な監督の枠組みに組み込み、必要に応じて、実装を支援する金融監督上の仕組みや業界横断的なメカニズムを含めること。
(2) **外部依存性の管理**：量子技術、標準、ツール、及び脅威の高度化の程度をモニタリングすること。
(3) **ステークホルダーとの対話**：課題の特定、知見の共有、そして、共通の解決策の推進に向けた、体系的な対話を促進すること。

量子耐性のある暗号への移行において想定されるタイムラインの考察

量子コンピューティングの技術発展の道筋には不確実性があるものの、暗号解読に利用できる量子コンピュータ（cryptographically relevant quantum computer: CRQC）が登場する前に目標を確実に達成できるよう、整合的な暗号移行のタイムラインを設定することは有益である。実施目標を設定するにあたり、当局と各組織は、標準化団体（standard-setting bodies）、各国のサイバーセキュリティ当局、業界団体等が主導するベンチマーク策定の取組を参考にできる。

G7 CEG は、様々な情報を評価し、金融セクター全体が量子耐性のある暗号に移行するため、困難だが堅実な目標となる移行期間を割り出した。こうした移行時期は公式のものではなく、リスク環境の変化に応じて見直しが必要である一方で、各法域間で移行計画について議論する際の共通目標として役立ち得る。複数の法域や標準化団体、国際機関による現行のガイダンスでは、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。この移行時期の目標は、専門家の意見を勘案した CEG の見解、及び、量子技術の開発者が CRQC の開発を見込む時期と一致する。また、HNDL（harvest-now-decrypt-later）攻撃を想定するシナリオのもとでは、CRQC の登場よりもはるか前の時点でデータが危険にさらされ得ることも考慮されている。さらに、G7 CEG が収集した情報に基づけば、システムの安全かつ健全な暗号移行には、長期間のリードタイムが必要であるという現実を反映している。加えて、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[3]。

移行時期の目標は、リスク環境の変化に応じて変更され得る。これらのタイムラインは、変化する脅威の情勢、データとシステムの重要性、移行作業の複雑性といった要因に基づいて、各組織によって調整され得る。また、量子耐性のある暗号の標準化の進展、及び、適用される規制上の期待などによっても調整され得る。

以下の図は、金融機関における想定上の非重要システムについて、量子耐性への移行工程の概要を視覚的に例示したものである。金融機関は、保有するシステムの重要性と特有の事情に応じて、本書に類似する別のロードマップを作成し、適用することも検討し得る。

[3] 原文の脚注 9: デュアルトラック・アプローチは、スケジュールを固定化する趣旨ではなく、金融機関がリスクに基づいてシステムやデータ資産の優先順位を検討することを促すもの。2030 年～2032 年の期間は、重要システムの移行において G7 各法域で想定される様々なアプローチを反映している。

G7 CEG は、金融当局及び金融機関に以下を推奨する：

- 既存のガバナンス、リスク管理枠組み及び技術戦略に、これらのアプローチを組込み、継続した経営陣の関与を検討する。
- 集団的なレジリエンスを高めるため、影響を受けるリスク及びシステム上の重要性に基づいて移行計画の優先順位を検討する。
- 本ロードマップで示した成功要因を各組織の移行計画に組み込むことにより、実施の道筋をつけることを検討する。

G7 CEG は、金融当局と連携し、以下を行うことを表明する：

- 耐量子計算機暗号への移行状況のモニタリング、法域間の情報共有、移行取組への支援、法域間における整合性向上に取り組む。技術進歩及びその理解の深化に伴い、必要に応じてタイムラインを見直し得る。
- 標準化団体及びその他の主要なステークホルダーと協調することにより、国際的な協力を推進する。
- 重要インフラセクター、技術提供者との対話及び知見共有を促進することにより、移行に向けた準備を加速させる。
- 進化し続ける脅威、技術、暗号移行に関して得られる教訓の動向を継続的に確認し、組織を支援するためのリソースの見直しを検討する。