すべての金融機関が直ちに着手すべき耐量子計算機暗号への移行

サイバー攻撃の標的とならないようシステム更改時期も見据えた対応を

金融庁
総合政策局長
屋敷 利紀

量子コンピューターの実用化は早ければ２０３０年代半ばと想定される。これによって現在の暗号技術が破られることになれば、インターネットバンキングをはじめとする金融情報システムの安全性が根底から覆される。すべての金融機関は顧客や自身の情報・財産を守るため、規模・特性にかかわらず、直ちに耐量子計算機暗号への移行に着手しなければならない。金融庁では検査・モニタリングなどを通じて、金融機関に早期かつ着実な移行を促していく方針だ。

耐量子計算機暗号への移行の緊要性

量子コンピューターの実用化と普及は社会を革新する可能性を秘める一方で、現在の公開鍵認証基盤で広く用いられる暗号技術（注1）が短時間で解読されてしまう危険をもたらす。暗号技術は、社会生活を支える重要インフラである金融機関の情報システムを情報漏洩や改竄などから防ぐ手段として重要な役割を果たしている（注2）。これらが破られることになれば、インターネットバンキングをはじめとする金融サービスに用いられる情報システムの安全性が根底から覆される。

量子コンピューターの実用化が２０３０年代半ばと聞くと「10年も先のことだ」と思うかもしれない。しかし特定の暗号

技術に的を絞れば、量子コンピューターの実用化前でも短時間で現在の暗号が解読可能になるとの指摘もある。

足元では、すでに「ＨＮＤＬ」（Harvest Now Decrypt Later）と呼ばれるサイバー攻撃が潜行しているともいわれる。これは現在の暗号技術で保護されたデータを収集し、量子コンピューターの実用化後にそのデータを解読して本格的な攻撃を仕掛けるものだ。

量子コンピューターに耐え得る「耐量子計算機暗号」（Post-Quantum Cryptography＝ＰＱＣ）への移行は、５～10年サイクルで取り組む大規模システム更改などに合わせて実施することが現実的だろう。しかも多数のステークホルダーが関与するシステムであれば、調整にも時間を要する。以上を踏まえると、金融機関は直ちにＰＱＣへの移行に着手しなければならない。

ＰＱＣへの移行は、人材の確保も含めて一朝一夕にできるものではない。長期間を要し、その間に多大な経営資源を投入する必要がある。金融機関の経営陣においては、量子コンピューターの実用化がもたらすリスクと、ＰＱＣへの移行期限などを正しく認識することが求められる。その上で強いコミットメントを示しつつ、中長期的な視野に立って必要な経営資源を投入する必要がある。

ＰＱＣへの移行に関しては「取り扱っている業務が単純だから」「小規模で人手が十分でないから」という言い訳は一切通用しない。犯罪者はむしろ防御が脆弱に見える金融機関を狙ってくる。これはフィッシング詐欺などの金融犯罪と同様だ。ＰＱＣへの移行は、顧客情報や資産を守るため、そして金融機関自身を守るため、規模の大小や業務の特性にかかわらず、すべての金融機関が対応しなければならない。

移行への課題を議論した金融庁検討会と報告書

金融庁では昨年７月から10月にかけて、３回にわたって「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」（以下、検討会）を開催した。預金取扱金融機関がＰＱＣへの移行を検討する際の推奨事項、課題および留意事項について議論を深めることが目的である。

検討会は11月に「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報告書」（以下、報告書）を公表した。報告書は、預金取扱金融機関以外の金融機関にとっても参考になるはずだ。

検討会には３メガバンクや農林中央金庫のほか、全国銀行協会をはじめとする業界団体、外部専門家（日本銀行、日本ネットワークセキュリティ協会）に参加してもらった。わずか３回の開催とはいえ、内容の濃い議論が展開された。

報告書では主に、次のような内容を論じている。

①金融機関はまず、自らの情報資産を網羅的に把握した上で、それぞれの情報資産の重要性を評価し、どのような暗号が用いられているかをリスト化したインベントリー（台帳・目録）を作成すること

②その際、自らが運用するシステムだけではなく、サードパーティーに運用を委託している重要システムの情報資産と暗号に関するインベントリーも作成すること

③インベントリーの作成作業にはかなりの労力を要するので、早い段階からＩＴベンダーの協力を得ること

④インベントリーに基づき、量子コンピューターが実用化されると脆弱性にさらされる情報資産のうち、影響が大きいシステ

ムから順にＰＱＣへの移行を進めること
⑤検討の開始から移行までの一連の作業に関して、ロードマップを作成すること
⑥実務的には大規模システム更改などに合わせてＰＱＣへの移行を進める必要があること
⑦ＰＱＣ自体も脆弱性が明らかとなる恐れがあるため、特定の暗号に固定することを前提とするのではなく、それが脆弱になった場合に暗号を差し替えやすいシステムにしておく、いわゆる「クリプト・アジリティー」を確保しておくこと
⑧移行には長い期間と多くの経営資源の投入が必要であるため、経営陣の強いコミットメントが求められること

ＰＱＣへの移行を進める各国の動向

米国では国家安全保障に関するシステム（注3）について、連邦政府が35年までに量子コンピューターによるサイバーセキュリティー脅威に対応するとの方針を表明している。金融セクターはここでいう安全保障に関するシステムに含まれないが、別途、国土安全保障省がＰＱＣへの移行を加速する対象としている「重要インフラ事業者」となっている。

また欧州委員会は24年４月に、ＰＱＣへの移行の検討を促す勧告を公表した。加盟国に対して、２年以内にＰＱＣへの移行に向けたロードマップを策定することを求めている。英国（注4）、カナダ、シンガポール、韓国では政府がＰＱＣに関するガイダンス等を発表するなど、各国の危機意識は高い。

Ｇ７（主要国首脳会議）でも昨年９月、財務大臣・中央銀行総裁に対して助言するサイバー・エキスパート・グループが「量子コンピューター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」を公表した。メンバー法域に対して、量子コンピューターによるサイバーセキュリティーリスクを理解・評価し、移行計画を立てて実行することを推奨している。

この間わが国では、政府横断的な計画（注5）などに基づき、関係省庁・機関がＰＱＣに関するガイドライン整備（注6）や研究開発（注7）を進めている。

対応が遅れればサイバー攻撃の標的に

わが国金融機関が他国に遅れを取ってはならない。ＰＱＣへの移行が他国や他社対比で遅れることになれば、サイバー攻撃の標的になる蓋然性が高まる。最悪の場合には、預金の不正引き出しや不正決済、情報漏洩が生じる。そうなれば顧客の情報や財産が著しく損なわれるばかりか、金融機関の信頼が失墜し、存廃の瀬戸際に立たされることにもなるだろう。また決済サービスを含め、国際的に業務を展開している金融機関では、国際的な信頼と競争力を失うことになりかねない。

現在、金融ＩＳＡＣにおいて、金融機関がＰＱＣへの移行に際して活用可能なロードマップのひな型の検討が進められている。だが、ひな型の完成を待っている時間の余裕はない。金融機関においては、報告書も参考に、自社でできることには直ちに着手しなければならない。ＩＴベンダーと協力しながら、自社運用のシステムだけでなく、運用を委託している重要システムに関するインベントリーの作成などに取り組む必要がある。

ＰＱＣへの移行は、対象となる範囲が広く活動が長期にわたるため、効率的に対応していくことも重要になる。金融機関間で対応にバラつきがあると手

戻りが発生し、PQCへの移行が業界全体として遅延する恐れもある。わが国においては、金融機関と金融ISACなどの共助機関、業界団体、ベンダー、金融庁をはじめとする政府機関がそれぞれ密にコミュニケーションを取りながら、国を挙げて犯罪者からの攻撃に備える必要がある。

＊　＊　＊

「金融機関に対してPQCへの早期かつ着実な移行を促すためには規制が必要だ」との意見があることは承知している。しかし金融庁は現時点において、規制整備に時間をかけるよりも、むしろ検査・モニタリングやさまざまな活動を通じて金融機関にPQCへの移行を促す方が効率的であり、実効性も高いと考えている。

金融機関の経営陣においては、PQCへの移行を「量子コンピューターの実用化は10年も先のことだから、私の責任ではない。次の世代で検討すればよい」などと先送りしては断じてならない。金融情報システムの安全性、ひいては金融システムの安定性が根底から覆される危機は迫ってきている。

金融庁では検査・モニタリングを通じて、金融機関に対し、PQCへの早期かつ着実な移行を促していく方針だ。併せて、金融ISACにおけるロードマップひな型の検討作業に協力し、それを金融業界全体へ着実に共有・普及させていくとともに、業界団体やベンダーに早期移行への理解を深めてもらう取り組みを進めていきたい。

（本稿において意見に係る部分は筆者の個人的見解であり、所属組織の見解を示すものではない）

（注）1　例えば、素因数分解が困難な巨大な素数の積を利用したRSA暗号や、容易に逆算できない楕円曲線上の離散対数問題を利用した楕円曲線暗号といったもの。

2　インターネットバンキングをはじめとする利用者を認証する情報、ファームウエア、デジタルコンテンツ、デジタルコンテンツを暗号化するための鍵、デジタルコンテンツにデジタル署名を付与するための鍵、各種暗号鍵を計算するための情報、電子証明書などに利用されている。

3　諜報活動、国家安全保障に係る暗号解読、軍隊の指揮統制に関するもの、兵器／兵器システムの不可欠な部分に関するもの、軍事・諜報活動の遂行に必要なもの（給与支払い、財務、物流、人事管理を含む日常的な管理業務、ビジネスアプリケーションは含まない）などについて、政府機関やその委託先などが使用するシステム。

4　28年までにPQCへの移行計画を策定、31年までに最も優先度の高いシステムの移行を完了、35年までにすべてのシステムの移行を完了するとしている（The National Cyber Security Centre "Timelines for migration to post-quantum cryptography" 25年3月）。

5　「サイバーセキュリティ2024」（24年7月サイバーセキュリティ戦略本部決定）

6　日本の暗号技術の検討・評価・活用を行う委員会であるCRYPTREC（デジタル庁、総務省および経済産業省が共同で運営する「暗号技術検討会」と、国立研究開発法人情報通信研究機構および独立行政法人情報処理推進機構が共同で運営する「暗号技術評価委員会」や「暗号技術活用委員会」で構成）のプロジェクトを通じてガイドラインの整備を検討中。

7　例えば、国立研究開発法人情報通信研究機構や同新エネルギー・産業技術総合開発機構によるものがある。

やしき　としのり
89年京都大学文学部卒。95年米イェール大学経営大学院修了、米国公認会計士登録。89年日本銀行入行。98年大蔵省金融企画局、00年金融庁総務企画部、08年検査局企画・情報分析室長、15年総務企画局マクロプルーデンス総括参事官、18年総合政策局参事官、審議官を経て24年から現職。