迫る耐量子計算機暗号（PQC）への移行とそのポイント

近い将来、量子コンピュータの発展により従来の暗号技術が解読される可能性が示唆されている。各金融機関は、各国の動向に鑑み2030年代半ばまでに、量子コンピュータへの耐性を備えた暗号技術に移行することが求められる。移行の要点を押さえつつ、早期着手が肝要である。

新暗号技術導入をなぜ急ぐのか

金融システムやサービスは、多くの技術によってその安全性が保たれている。とりわけ暗号技術は、口座のIDやパスワードなどの秘密を第三者への漏えいから守る重要な技術となっている。ところが今、この安全性への信頼が揺らぎかねない事態が起ころうとしている。近い将来、早ければ10年後にも量子コンピュータの実用化によって、この暗号技術で担保されていた秘密が解読されてしまう可能性があるからだ。

現在の暗号技術は、たとえば巨大な数の素因数分解を活用し、従来のスーパーコンピュータを利用しても現実的な時間内で解くことが難しい数学的概念・計算困難性をベースとしている。しかし、量子コンピュータには効率的に暗号を解読するアルゴリズムがあるため、その性能が向上した場合、従来の暗号技術を現実的時間内で解いてしまう可能性がある。

暗号解読への対応は、量子コンピュータが実用化されてから、その対策を進めておけばよいと考えがちである。しかし、事態は量子コンピュータの実用化を見越し、かなり前から準備しなければならない段階に来ている。

従来の暗号技術を解読してしまう性能を持った量子コンピュータをCRQC（Cryptographically Relevant Quantum Computer）と専門用語では表現する。このCRQCが悪意ある者に利用されることで特に問題と提起されているのが、HNDL（Harvest Now Decrypt Later）攻撃である。この攻撃は、現在解読できない暗号化された情報を、通信の盗聴や端末の侵害、ダークウェブ等での購入を通して事前に入手し、CRQC登場後に解読してやろうという試みである。

つまり、CRQC登場後に慌てて対策を行っても、この攻撃を防ぐことはできない。この攻撃を防ぐには、CRQCの登場時期を見越し、情報が安全に秘匿されるべき期間を考慮して、CRQCでも解読できない次世代の暗号技術であるPQC（Post-Quantum Cryptography）に事前に移行を進めていく必要がある。

PQC移行の時期は意外に早い

このPQCという暗号技術は、いくつかの候補が示されている。詳細は省略するが、効率的な暗号解読アルゴリズムが発見されていない格子問題を応用した暗号技術が有力視されている。この暗号技術は世界中の有識者によって量子コンピュータに対する安全性の検証が進められており、確認されつつある。

では、実際いつを目途に移行を進めればいいのか。早期と書いたが、実際にはCRQCの登場時期は専門家でも意見が分かれている。従って、CRQC登場時期を予測したリスク評価や正確な費用対効果を計算することは、現時点では非常に難しい。

とはいえ、AIの技術進歩を目の当たりにしている中、量子コンピュータによる脅威は現実化しないだろうと楽観視するのは危険であり、また前述のHNDL攻撃も考えると猶予はあまりない。アメリカ政府では2035年を目途にこの脅威への対応を推進している。また、金融庁および国内有識者によって取りまとめられた報告書[1)]からも、わが国でも重要度の高いシステムについて、同様の対応が2030年代半ばを目安に実施することが望ましいとも報告されている。ひとつの目安となるのではないか。

野村総合研究所　金融イノベーション研究部

NOTE

1）「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」、令和6年11月26日。

PQC移行プロセスの留意点

具体的にPQCへの移行をどのように推進すればよいのか。筆者が特に重要だと考えるプロセスは、①現状把握（クリプト・インベントリの作成、管理）、②リスクアセスメントによる優先順位管理、③クリプト・アジリティの向上・推進である。

従来の暗号技術は数十年にわたって安全であると考えられていたので、システムを構成するソフトウェアやハードウェアの広範に、そして奥深くまでその技術が組み込まれている。その結果大きな組織であればあるほど、①の現状把握に膨大な時間とコストを要する。

例えば、金融機関であれば数十（あるいはそれ以上）を超える多種多様なシステムを保有し、それぞれのシステムがAPI等で内部・外部と複雑に連携している。このような場合、システム間連携・依存関係を考慮し、背後にある数十種にも上る暗号技術のつながり（暗号アーキテクチャ）を紐解いたうえで、どのシステムにどういった用途で、どの暗号技術が利用されているかを把握する（これを「クリプト・インベントリの作成」という）には多くのリソースと専門性を要する。

また、多数の情報システムで一斉にPQC移行対応を進めることは困難であるので、②で挙げた優先順位付けを行い、社会的インパクトが大きいシステムから少しずつ移行を進める必要がある。

そして③だが、PQC対応は移行して終わりというわけにもいかない。なぜなら、将来的に導入した新技術（PQC含む）に脆弱性やシステム実装時の課題が発見される可能性もあるためだ。そういった事態が生じた際に、ビジネスの継続性確保を目的とし、迅速に暗号技術を切り替えられるような柔軟性・敏捷性（これをクリプト・アジリティという）をシステムに組み込んでいく必要がある。具体的には、システムの暗号処理部分をモジュール化し、入れ替え可能なように設計する、オンラインでの変更ができるようソフトウェアで実装するといった手法がある。

このクリプト・アジリティへのシフトは、組織のモダナイゼーション、クラウド移行、DXといった戦略的目標のプロセスと統合して推進することで、より実効性・費用対効果の高い結果となるだろう。

PQC移行は長期戦を覚悟のうえ、多くのリソースを投入する必要がある。その点で、経営トップの関与が移行を推進するうえで重要な要因となることは間違いない。

また、暗号技術はニッチな分野である。それゆえ、暗号に特化した部門・人材は十分に確保されていない企業の方が多いだろう。専門人材の育成、外部パートナーを含めたリソースの確保などの早期着手にも期待したい。

加えて、この作業は自社組織だけでは決して終わらない。システムは多くのステークホルダーによって形作られており、例えば製品調達先・開発先ベンダーのPQC対応がボトルネックになるケースもあるだろう。PQC移行を推進するためには、例に挙げた関連ベンダーをはじめ、業界団体、ときには政府当局といった多岐にわたるステークホルダーと連携し、対応を進めることが望ましい。

Writer's Profile

小泉 光 Hikaru Koizumi
NRIセキュアテクノロジーズ
シニアセキュリティコンサルタント
専門は暗号・鍵管理
focus@nri.co.jp