今からできるPQC移行の準備

量子コンピュータの脅威が現実味を帯びる中、耐量子計算機暗号（Post-Quantum Cryptography：PQC）移行は多くの組織にとって避けられない課題である。現場でよく聞かれる課題意識を踏まえつつ、標準的なPQC移行プロセスを整理し、今の段階でも着手できる実務的な取り組みから実施することが望ましい。

現場で共通する認識

筆者はこれまで、官公庁や金融機関をはじめとする民間企業を対象に、PQCをテーマとした勉強会や意見交換を実施してきた。そうした場で「PQC移行に関して課題に感じていることは何か」と尋ねると、多くの組織で共通して挙がるのが「どこから着手すべきかわからない」「量子コンピュータの脅威がいつ現実化するのか不透明で、対応期限をどう設定すべきかが判断できない」といった声である。

加えて、「規制や技術、市場の動向が明確になってから移行を検討すればよいのではないか」という意見も少なくない。こうした意見は確かに一見、合理的に思えるが、大きなリスクを内包している。その代表例が「Harvest Now, Decrypt Later（HNDL）」攻撃である。これは攻撃者が現時点で暗号化されたデータを様々な手法で収集し、将来、量子コンピュータが実用化された時点で解読を試みる手法である。敢えて具体例を示さないが、長期保護が必要な情報ほど標的となる。

また、これまで暗号アルゴリズムの置き換えは繰り返されてきたが、その対応が長期化し決して容易ではなかったことも想起すべきだろう。規制や技術動向が固まるまで「待つ」という姿勢は、一見合理的でも実際にはリスクを放置し、将来の対応をより困難にする可能性が高い。したがって、今できることから備えることが、現実的なアプローチである。

PQC移行の進め方は各国の公的機関が公表した文献や専門機関の報告書で整理されており、細部は異なるが大枠は共通している。典型的な流れは以下の通りである。

1. **準備**：移行の必要性を認識し、PQCに関する規制・技術・市場動向の最新情報を収集するとともに、推進体制を構築する。
2. **現状の把握**：情報資産やシステムの棚卸を行い、移行優先度を整理する。また暗号利用状況を、設計書の確認や担当者ヒアリングといった人的調査に加え、ツールも併用して把握し、クリプトインベントリ（暗号アルゴリズムの使用状況の管理と情報の一覧化）を作成する。
3. **計画と実行**：優先度を踏まえて移行計画を策定し、PQC移行を推進する。同時に、進捗に応じてクリプトインベントリを更新し、移行が間に合わないシステムには暫定的なリスク低減策を検討する。
4. **監視と評価**：進捗を監視し、最新のPQC動向や新たな脅威、規制の変化に応じて計画を改善する。

今から着手できる実務領域

以上の大枠の進め方を理解したうえで重要なのは、「現時点でも取り組めること」を見極めることである。規制や市場動向に左右されない取り組みを今から進めることが、将来の円滑な移行に直結する。

筆者が様々な組織と意見交換をしてきた中では、依然として「1. 準備」にとどまるケースが大半であり、「2. 現状の把握」に本格的に着手している例はまだ限られる。しかし、この現状把握こそが規制や市場の方向性が未確定のなかでも取り組むことができるテーマといえる。現状把握は、PQC移行に直結するだけでなく、資産管理や暗号利用状況の可視化といった基本的なセキュリティ強化策としても有効であることを見逃してはなら

ない。

システム重要度の優先付け

組織の規模によってはシステム数が数百に及ぶことがあり、すべてを一律に移行していくことは現実的ではない。そのため、優先度をつけて段階的に進めていくことになる。優先度を判断する観点としては、システムの業務上の重要度、外部公開の有無、データ保護期間などの確認に加え、システムの更改タイミングやセキュリティ対策状況といった要素も考えられる。これらを総合的に整理し、どの観点を重視するかの重みづけを決定するだけでも相応の時間を要する。

システムの棚卸自体が不十分であれば、その見直しから着手する必要があり、全体の期間は一層長期化する。特に、資産管理が申告ベースの場合、漏れや誤認によって実態と乖離が生じるリスクがある。この補完策として有効なのがASM（Attack Surface Management）である。ASMは本来、組織の外部からアクセス可能なIT資産を継続的に発見・監視し、脆弱性やリスクを攻撃者視点で検出・評価する仕組みである。その機能を応用することで外部公開資産の洗い出しに役立ち、棚卸を精緻化するための補完手段となる。こうした活用は、PQC移行の前提となる基盤整備を進めるうえでも有効な選択肢の一つであると筆者は考える。

クリプトインベントリの作成

クリプトインベントリの作成は、暗号技術の利用状況を一覧化し、使用アルゴリズムや暗号鍵長、暗号実装箇所などを把握する作業である。現時点では標準化された方法論やデファクトスタンダードは存在しないため、まずは設計書の確認や現場担当者・ベンダーへのヒアリングを通じて全体像を把握することが最初の一歩となる。特に、レガシーシステムやベンダー依存のブラックボックス的なアーキテクチャ、属人的に管理された証明書や暗号鍵はツールだけでは検出が難しく、人的作業による確認が不可欠である。

そのうえで、コードスキャンによる旧式暗号の自動検知や、エンドポイントを対象とした暗号ライブラリ・バージョン情報の収集など、補完的にツールを活用することを検討することが有効である。ただし、ひとつのツールですべての暗号利用箇所を把握することは現実的には難しいため、人的作業と複数ツールを組み合わせたアプローチが将来における現実的な進め方といえる。

クリプトインベントリは一度作成して終わりではなく、システム更改やサービス追加のたびに更新を続ける必要がある。また、標準化動向やツールの成熟度を継続的にモニタリングし、自社のPQC成熟度に応じて組織・プロセス・ツールを段階的に整えていくことが望ましい。将来的には暗号設定や鍵情報を中央で一元化し、変更を効率的に複数システムへ反映できる仕組みを整えることが、将来の暗号技術の切替えを柔軟かつ迅速に進めるうえで重要である。ただしシステム全体への影響が大きいため、段階的な計画が不可欠である。

Writer's Profile

高木 裕紀 Hironori Takagi
NRIセキュアテクノロジーズ
エキスパート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