2026年は量子セキュリティ元年

アスピレイション代表取締役
石塚宏一
いしづか　ひろかず

迫り来るQ-Dayの現実と脅威

2026年は、世界のサイバーセキュリティ史において「量子セキュリティ元年」として記憶されることになるであろう。量子コンピューターが現在の公開鍵暗号を打破する「Q-Day」へのカウントダウンが加速する中、われわれは認識を根本から改める必要がある。Q-Dayはしばしば将来の出来事として扱われるが、リスクの観点からはすでに「今ここにある危機」である。

量子技術の進展により、2026年にも限定的脅威が顕在化するとの予測が出る中、米予測市場Kalshiでは、2027年以前に「有用な量子コンピューター(RSA-2048解読可能)」が登場する確率を8%と算出している。

また、Q-Dayの到来時期にかかわらず、注視すべきは「Harvest Now, Decrypt Later(HNDL:今盗み、後で解読する)」という攻撃手法の存在である。攻撃者は、現時点では解読不能な暗号化データを組織的に窃取・蓄積し、高性能な量子コンピューターが登場した瞬間にそれらを一斉に解読しようともくろんでいる。健康記録、国家機密、知的財産といった長期保存を要するデータにとって、脅威は現在進行形で存在しているのである。

さらに、現行の暗号で署名された正規データを収集し、Q-Day後に秘密鍵を特定、署名偽造によりアイデンティティとサプライチェーンを破壊する「Trust Now, Forge Later(今信頼させ、後で偽造する)」といった攻撃も現実味を帯びている。

量子計算技術の飛躍的進展と暗号解読のリアリティ

なぜ量子コンピューターはこれほどまでに脅威なのか。その核心は「ショアのアルゴリズム」にある。従来のコンピューターが数千年以上を要する巨大な整数の素因数分解を、量子コンピューターはこのアルゴリズムによって劇的に短縮し、わずか数時間で完了させる。現代のサイバーセキュリティを支えるRSA暗号などが「量子耐性を持たない」とされるゆえんである。

量子コンピューティングの進化速度は、いまや予測を超えて加速している。ハードウエア面では、米国IonQが20万量子ビット級プロセッサのテスト時期を2028年に開始するというロードマップを公開した。

さらに注目すべきなのは、アルゴリズムの効率化による解読コストの激減である。最新の研究によれば、新たなコードを活用した新アーキテクチャにより、従来は100万物理量子ビットが必要とされたRSA-2048暗号の解読が、わずか10万物理量子ビットで実現する可能性も示された。これは、既存の暗号体系の寿命が、近々に迫っている可能性があることを意味する。

次世代の盾:耐量子計算機暗号(PQC)への移行

この脅威に対抗する決定打がPQCである。PQCは数学的なアルゴリズムに基づいており、既存のインフラで利用可能である点が、専用設備を要する量子鍵配送に対する大きな利点である。米国立標準技術研究所(NIST)による標準化も完了し、すでに実装フェーズに入っている。

米国では、国家安全保障覚書第10号(NSM-10)および大統領令14144に基づき、PQC移行を国家安全保障の最優先事項と位置付けている。これにより、政府機関のみならず、防衛・重要インフラを支えるサプライヤーに対しても、NIST標準に準拠した移行プロセスの即時開始と、期限を定めた実装が事実上義務付けられた。

欧州のNIS2指令やデジタル・オペレーショナル・レジリエンス法のもとでは、PQCへの移行は経営責任を伴う「法的義務」へと変貌している。シンガポールでは金融機関に対し、2026年までのPQC移行計画策定を義務付けた。日本においても、金融庁が「将来のPQC移行を前提とした、暗号インベントリ把握などの即時準備」を怠らないよう、強く求めている。日本企業にとっても、既存の暗号資産や通信経路をPQCへとアップデートする「切り替え可能性」の確保が、経営上の最優先課題となっている。

しかし、極めて重要な視点がある。ソフトウエアとしてのPQCだけでは不十分だという点である。アルゴリズムが堅牢でも、電力変動から秘密鍵を盗む「サイドチャネル攻撃」をソフトのみで防ぐことは困難である。そのため、電力を物理的に遮断する「ガルバニック絶縁」のハードウエアとの融合が、米国の防衛領域を中心に不可欠な認識として広がっている。この二段構えの防御こそが、真の量子耐性を実現する唯一の道である。

実践的ソリューションによる即時防御

課題は「解決策の欠如」ではなく「適切なソリューションをいかに大規模に実装するか」にある。われわれが提供するソリューション「Isidore Quantum®」は、この実装の壁を打ち破る。米国防総省・ミサイル防衛局にも選定された本ソリューションは、以下の特性を持つ。

・Drop-In型実装　既存インフラやソフトウエアの大規模改修を伴わず、量子安全な暗号層を迅速にオーバーレイすることが可能

・ハードとソフトの融合　量子乱数生成器とNIST承認のアルゴリズム(ML-KEM,AES-256 GCM)を統合し、数学的に証明可能な安全性を実現

・物理的防御　ガルバニック絶縁等により、電力解析などのサイドチャネル攻撃にも耐える強固な設計

プロアクティブ・サイバー防御としてのPQC

企業価値を担保するためには、サイバーリスクを経営リスクと捉え、予測・定量化に基づき先回りして低減する「プロアクティブ・サイバー防御」の継続的プロセスが不可欠である。

リスク管理は個別の「点」からサプライチェーンという「面」へと広がりを見せている。技術革新により新興スタートアップの誕生が加速する中、AIエージェントを用いたコンプライアンス・ギャップ分析を含むサプライチェーン・リスク管理(SCRM)は、いまや世界的な潮流である。また、公知の脅威のみならず、未知の脅威をいかに迅速に捉え、リスク管理に活用できるかが鍵となる。

そして、将来のリスクを先取りして耐性を確保するPQCは、この統合的防御の重要な一翼を担う。Q-Dayへの備え、そして現在進行中のHNDL攻撃への対策準備を本格化させる2026年は、まさに「量子セキュリティ元年」となるであろう。