金融機関が量子コンピュータからの攻撃に対して安全な暗号(QSC)で自らを守るべき理由

本ホワイトペーパは SSH Communications 社発行、著作権を持つ「Why financial institutions should protect themselves with Quantum-safe cryptography (QSC)」の日本語訳です。

技術の飛躍的な進歩は、新たなリスクの景観をもたらす

量子コンピューティングの脅威とリスクの軽減

量子コンピュータの時代が到来して久しいが、大規模な商業利用が可能になるまでには、まだ何年もかかると思われます。しかし、量子コンピュータへの移行は徐々に進むと思われます。

1960 年代、パーソナルコンピュータはまだ存在しませんでしたが、コンピュータはすでに軍事やビジネスで重要な役割を担っていました。それと同じように、量子コンピュータもまずは軍事や、金融業界などの大企業で採用されるでしょう。バイデン政権はつい最近、オーストラリアとイギリスとの新しい戦略的パートナーシップを発表し、次のように強調しています。

「AUKUS は、我々の軍、科学者、産業を結集し、サイバー、人工知能、量子技術などの軍事能力と重要技術における優位性を維持・拡大する」と。

量子へのシフトは始まっている。

本ホワイトペーパでは、この緩やかな移行が金融業界のサイバーセキュリティにどのような影響を及ぼすのか、特に暗号化、安全なファイル転送、量子コンピュータに対して安全なアルゴリズムに重点を置いて解説しています。また、金融機関が今日からすぐに量子コンピュータに対して安全な暗号(QSC)への移行を計画すべき理由と、この移行によって組織が現在と将来の両方でどのようなメリットを得ることができるかを明らかにします。

サイバー犯罪者の格好のターゲットである金融データ

サイバー犯罪は増加の一途をたどっています。2020 年における世界の被害額は 1 兆ドルを超えています。これは世界の GDP の 1%以上です。サイバーセキュリティ・ベンチャーズ社の専門家によると、2025 年までの世界の年間被害額は 10 兆 5 千億ドルに達する可能性があり、主だった麻薬の違法取引をすべて合わせた額よりも多く、最も収益性の高い犯罪分野になっています。また、将来的には、実質的に無限のリソースを持つ国家に支援された行為者による攻撃である「ハイブリッド戦争」が益々増えていくでしょう。

彼らは政府組織を直接狙うだけでなく、金融セクターのように社会や経済に不可欠な企業にもダメージを与えようとするでしょう。金融セクターの情報漏えいの平均コストは 571 万ドルで、全産業の平均より 35%も高くなっています。

金融セクターは、顧客の個人データを日常的に取り扱い、保管しています。2019 年に広く公表された事例では、米国の大手銀行である Capital One が 1 億人分の顧客データを流出させました。問題のデータは与信申請に関するもので、実際の支払いデータは含まれていませんでした。当該銀

行は、この情報漏洩の管理にかかる総費用を 1 億~1 億 5,000 万ドルと考えていました。それに加えて、同行は米国規制当局からの制裁金 8000 万ドルを負担しました。個々の顧客レコード漏洩に対するコストは、1.80 ドルから 2.30 ドルでした。

信用報告会社の Equifax は 2017 年の調停では、漏洩した顧客記録 1 件につき 4.75 ドルの罰金を科せられました。ヨーロッパで活動する企業にとって、GDPR は巨額の懲罰的賠償になります。

Capital One の場合、支払いデータ、カード番号、ログイン情報の漏洩がなかったのは幸運だったと言えるでしょう。プライマリーアカウント番号(PAN)が悪用された場合、カード所有者はクレジットカードの請求書に不正な請求がなされることが予想されます。発行会社にとっては、チャージバックの処理、代替カードの発行、信用の低下を意味します。PAN の漏洩を防ぐために、Payment Card Industry Data Security Standard (PCI-DSS)という一連の規制が存在し、違反した場合の罰金は一か月あたり 10 万ドルにものぼります。

量子コンピュータは暗号をどう破るのか？

暗号化は、転送中および保存中のデータを保護するために必要な要素です。どのような暗号であっても、利便性(暗号化／復号化に必要な時間と計算資源)とセキュリティ(暗号を破るのに必要な時間と計算資源)の間にはトレードオフがあります。処理能力が向上し、やがて一般的になれば、これまで十分安全だと思われていたレベルの暗号も、解読が容易かつ安価になり、いずれはより安全な暗号に置き換える必要が出てきます。

これまでのところ、暗号の強度を向上させるには、データ暗号化に使用する秘密鍵の長さを調整することがほとんどでした。長い鍵は通常、解読が著しく困難になるからです。例えば、以前は広く使われていた 512 ビットの RSA はもはや使われておらず、2048 ビットに置き換わっています。NIST によれば、2030 年まではこの 2048 ビットが有効です。それ以降については、ビット数を増やせばよいのでしょうか。

残念ながら、ここで量子コンピューティングが実証済みの方法を破ってしまうのです。現在広く使われている暗号アルゴリズムはすべて、量子コンピュータが得意とする素因数分解という攻撃に弱いのです。現在の量子コンピュータはこの攻撃をうまく処理することができませんが、これは急速に変わっていくことでしょう。Google の CEO である Sundar Pichai によると、量子システムは私たちが知っている暗号を破壊するでしょう。それは今から 5~10 年後(2021 年)のことです。それはシステムをアップグレードするまで 5 年から 10 年の期間があたえられているという意味になるのでしょうか。

財務データが危険にさらされる

1. 後で悪用するためにセッションを記録する。

どの金融機関でも、長期間にわたって秘密にし、保護しておかなければならないデータがあります。例えば、パーマネント アカウント番号(PAN)等 5～10 年先も通用する重要な秘密があれば、それを考慮する必要があります。クレジットカードの寿命は通常 5 年以上で、新しいカードは一般的に同じ PAN で発行され、有効期限だけが将来に延長されるだけです。

2021 年の暗号通信を記録して保存することで、仮に 今、その解読技術がなくても、量子コンピュータによる処理が可能になったときにそのこのメッセージを解読することが可能となります。

この例の場合、攻撃者は 2021 年に保存した暗号化ファイルを開き、暗号を解読して平文で PAN にアクセスできることを意味します。カード所有者にとっては不正請求の可能性があり、銀行にとっては膨大な数の PAN を変更しなければならず、しかも怒れる顧客や関係者に対応しなければなりません。

通常、この一連の過程は一般的な悪質な犯罪者にとっては回収に時間がかかりすぎるものですが、潜在的な報酬が十分に大きい場合、豊富な資金や資源を持つブラックハットグループにとっては充分魅力的です。言うまでもなく、金融機関の情報は常に貴重なターゲットです。

このように、量子コンピュータの脅威は、それ自体がまだ深刻な脅威要因として存在していなくても、実際に今ビジネスに影響を及ぼしているのです。

あなたの組織には、5 年後、10 年後でも重要で有効なデータはないのでしょうか。

2. 企業が一般的に考えているよりも早く準備を始める必要がある

量子コンピュータが遠い未来の脅威のように思えても、新しい技術の本格的な導入には、企業が考えている以上に時間がかかることが多いのです。現在の公開鍵暗号のインフラについて考えてみましょう。そのキーテクノロジーの 1 つである Secure Shell プロトコルは、すでに 26 年前に発明されたものです。当初は小規模なものでしたが、ひとたび普及が始まると、インタラクティブな自動ファイル転送を暗号化するためのデファクトスタンダードとなり、現在に至っています。

しかし、歴史的に見れば、現代の公開鍵暗号のインフラが整備されるまでに 20 年近くかかっています。量子コンピュータが深刻な脅威となるのに 15～20 年かかるとしても、その到来に向けた準備は今すぐ始める必要があるのです。

技術が実用化されるまで待ったり、実用化されてから対応したりするのでは、すでに遅すぎるのです。

3. 量子コンピュータからの攻撃に対して安全な暗号は古典暗号と並存できる

量子リスクを軽減する技術は既に存在しています。量子コンピュータからの攻撃に対して安全な暗号(QSC: Quantum-safe cryptography)は、ポスト量子暗号(PQC: Post-Quantum Cryptography)とも呼ばれ、現在の暗号で使われている量子コンピュータに対して脆弱な既存のアルゴリズムを、従来のコンピュータと量子コンピュータの両方がもたらす脅威に対抗できるバージョンに置き換えることができます。鍵認証とデジタル署名の両方を量子コンピュータからの攻撃に対して安全化することがでます。QSC はソフトウェア、ハードウェア双方に実装することが可能です。例えば、NCSC(National Cybersecurity Center)は QSC の採用が量子コンピュータの脅威を最も効果的に緩和することになると確信しています。

4. 移行の準備

大規模な組織では、長期的なロードマップに「量子コンピュータの脅威」を織り込み、どのシステムを優先的に移行させるかを明確にする必要があります。優先すべきシステムとデータには、機密性の高い個人データやビジネス上極めて重要なデータがあり、それを処理するシステムで、一般的に最も置き換えが困難なものが含まれるはずです。QSC/PQC プロトコルの標準化は急速に進んでおり、NIST が推奨するアルゴリズムの初期セットも実質的には既に利用可能な状態です。今こそ、重要な情報を扱う企業が移行プロセスを開始する時なのです。

Tectia Quantum - 将来性を見据えた暗号

幸いなことに、量子コンピュータでは全ての暗号化アルゴリズムを陳腐化させることはできません。PQC(ポスト量子暗号)アルゴリズムは何年も前から開発されており、2021 年時点では標準化が進行中です。量子コンピュータは、PQC アルゴリズムに対しては大きなアドバンテージを得ることはできません。

最大限のセキュリティを確保するためには、従来のコンポーネントとポスト量子コンポーネント双方を持つハイブリッドアルゴリズムが推奨されます。両者を組み合わせることで、どちらのタイプの攻撃にも耐えることができます。

SSH.COM は量子コンピュータが出現した後でも、その通信が未来永劫利用可能であるように、新しい量子対応 Secure shell クライアント/サーバアプリケーション、Tectia Quantum を発表しました。Tectia Quantum は、リモートアクセス(SSH プロトコル)、ファイル転送(SFTP プロトコル)、またはトンネルした TCP 接続を保護することができます。

結論

量子対応の導入を遅らせる必要はありません。大企業や国家が競って量子コンピュータの開発に取り組んでおり、その本格的な導入は日に日に現実味を帯びてきています。

同時に、経験豊富なサイバーセキュリティの専門家である SSH.COM は様々な企業やフィンランド政府と長年にわたって協力し、量子コンピュータの脅威を軽減するための世界クラスのポスト量子暗号を作り上げてきました。

SSH.COM Tectia Quantum は、従来の攻撃に対する従来の暗号アルゴリズムの安全性と、量子攻撃に対する PQC アルゴリズムの安全性を、製品の効率性を損なうことなく組み合わせた、ハイブリッドなアプローチを採用しています。また、このソリューションは、以前の Tectia やサードパーティの SSH クライアントやサーバーとの完全な上位互換性を持っています。Tectia Quantum を選択することで、転送中のデータ、すなわち 組織の秘密は、量子コンピュータの時代でも安全であり続けるのです。