2023 年 1 月 18 日

サイバートラスト株式会社
代表取締役社長 眞柄 泰利
東証グロース：4498

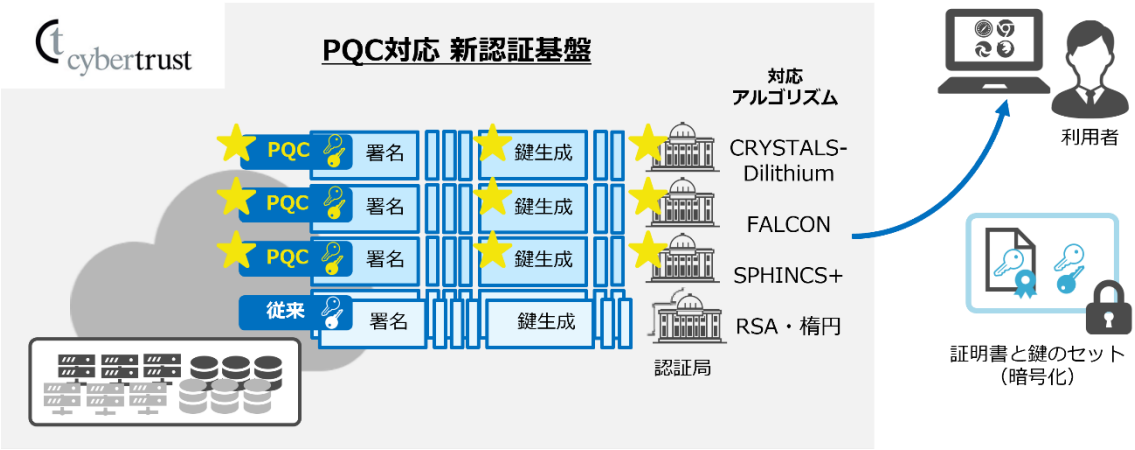
サイバートラスト、証明書の高速・大量発行が可能な新認証基盤における
耐量子計算機暗号(PQC)への対応を実証

～ 簡易な PQC 対応証明書の提供により、既存の暗号方式から PQC への移行検証を支援 ～

サイバートラスト株式会社（本社：東京都港区、代表取締役社長：眞柄 泰利　以下、サイバートラスト）は、証明書の高速・大量発行が可能なサイバートラストの新認証局基盤において、米国国立標準技術研究所（National Institute of Standards and Technology：以下、NIST）が選定した耐量子計算機暗号（Post Quantum Cryptography：以下、PQC）※1 への対応に関わる概念実証（Proof of Concept：PoC）※2 を完了したことを発表します。このたびの概念実証を踏まえて、同基盤で発行する PQC 対応証明書の提供によりお客様の PQC 移行検証の支援を行い、量子コンピュータ時代においても安全な通信や認証の実現を目指します。

＜背景＞
量子コンピュータの進化と普及は、社会に大きなメリットをもたらす一方で、既存の暗号も解読できるようになり、セキュリティ上の脅威をもたらす可能性が懸念されています。これに対し、NIST は、量子コンピュータでも容易に解読できない新しい暗号技術（PQC）の標準化を進めています。 PQC 標準化はカテゴリーごとの公募を 2016 年に開始し、3～4 段階のスクリーニング評価を経て最終的に複数の方式を選出する方針で進められており、2022 年 7 月に第 3 ラウンド評価において PQC デジタル署名としては 3 方式（CRYSTALS-Dilithium、FALCON、SPHINCS+）の選出が発表されました※3。

サイバートラストは、大量の IoT 機器などに高速・大量に証明書を発行・配付可能な商用の新認証基盤を開発・稼働しています。このたび、NIST が選出した PQC デジタル署名 3 方式について、PQC 標準技術を同基盤に実装する PoC 開発を行い、完了しました。



NIST は、既存暗号である RSA 暗号※4 などから PQC への移行準備を推奨しており、既存の各種システム、設備、通信などにおける移行および検証には時間を要すると言及しています※5。

サイバートラストは、既存の自社システムやサービス、アプリケーション等に暗号アルゴリズムとして PQC を追加する開発・検証を進めようとしている企業や組織に向けて、簡易に PQC 対応証明書サンプルの提供を開始し、お客様による PQC 移行の検証を支援します。今後、関連情報や PQC 証明書を用いた接続検証環境などを順次提供予定です。

NIST は、第 4 ラウンドでも追加で標準技術を選定し、2023 年後半から 2024 年に PQC に関わるガイドラインの公開も予定しており、サイバートラストは、引き続きこれらにも対応していく予定です。

※1 耐量子計算機暗号とは：十分な規模の量子コンピュータが実用化されても安全性を保つことができる暗号のこと。

※2 PoC とは：新たなアイデアやコンセプトの実現可能性やそれによって得られる効果などについて試作開発の前段階で実施する検証のこと。

※3 NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, https://csrc.nist.gov/publications/detail/nistir/8413/final

※4 RSA とは：公開鍵暗号アルゴリズムの一種で、複雑な計算によって短時間では解読されない素因数分解の仕組みを応用しています。1977 年に発明されて以降、 SSL/TLS や PKI などの暗号に安定した運用実績があり、高い安全性により中心的な暗号化技術になっています。

※5 The NCCoE Migration to Post-Quantum Cryptography Project (PDF), https://csrc.nist.gov/csrc/media/Presentations/2022/the-nccoe-migration-to-post-quantum-cryptography-p/images-media/session-5-newhouse-nccoe-pqc-migration-pqc2022.pdf

■関連 Web サイト

- 耐量子計算機暗号（PQC）証明書とは／耐量子計算機暗号（PQC）証明書サンプルお

申込みページ

- IoT 機器向け証明書の高速・大量発行とセキュアな識別・管理を実現する商用認証局基盤を構築（2022 年 4 月 27 日発表 サイバートラストプレスリリース）

■サイバートラスト株式会社について

サイバートラストは、日本初の商用電子認証局として長年にわたり提供している認証・セキュリティサービスと、ミラクル・リナックスのカーネル技術やオープンソースソフトウェア（OSS）の知見を応用したオンプレミス、クラウド、組込み領域向けの Linux/OSS サービスを展開しています。

また、これらの技術や実績を組み合わせ、IoT をはじめとする先端分野に向けて、「ヒト・モノ・コト」の正しさを証明し、お客様のサービスの信頼性を支えるサービスを推進しています。

「信頼とともに」。サイバートラストは、IT インフラに関わる専門性・中立性の高い技術で、安心・安全な社会を実現します。

【当リリースに関するお問い合わせ先】

サイバートラスト株式会社

メール：IR 担当(ir@cybertrust.co.jp ）、広報担当（ press@cybertrust.co.jp ）