2026 年 1 月 21 日
TOPPAN デジタル株式会社

TOPPAN デジタル、IoT 機器の認証から通信まで一貫した耐量子計算機暗号（PQC）への対応を実現

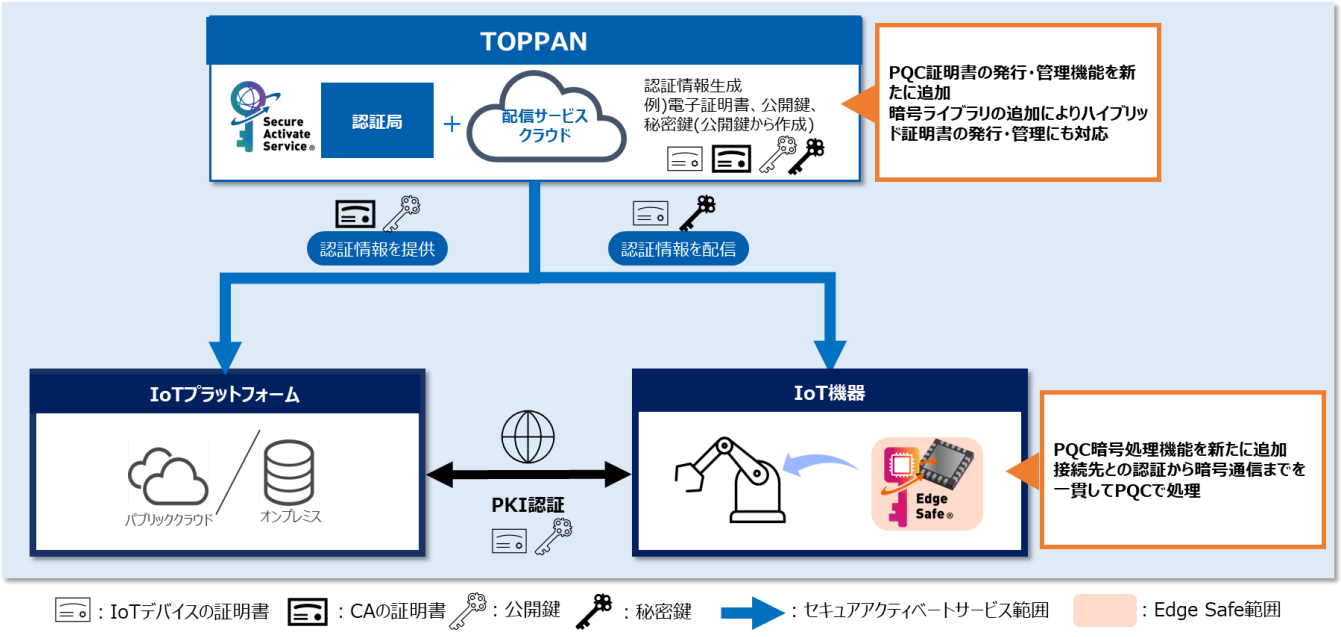
IoT 機器向けセキュアソリューション「Edge Safe®」と「セキュアアクティベートサービス®」へ機能追加、IoT 機器における現行暗号から耐量子計算機暗号への円滑な移行を実現

TOPPAN ホールディングスのグループ会社である TOPPAN デジタル株式会社（本社：東京都文京区、代表取締役社長：坂井 和則、以下 TOPPAN デジタル）は、IoT 機器向けセキュアソリューションとして、セキュアエレメント「Edge Safe®」(※1)と IoT 機器とクラウドの安全な通信を実現する「セキュアアクティベートサービス®」(※2)を提供しています。

このたび、「Edge Safe®」と「セキュアアクティベートサービス®」に、量子コンピューターでも解読が困難とされる耐量子計算機暗号（Post-Quantum Cryptography、以下 PQC）への対応機能を搭載しました。2026 年 1 月 21 日より、スマート家電、製造機器、インフラ設備、医療機器などの長期間利用される IoT 機器を扱うメーカーや業界に向けて、量子コンピューター時代でもセキュアに利用できる IoT ソリューションとして提供開始します。

今回、IoT 機器に組み込むセキュアエレメント「Edge Safe®」では、現行暗号の認証に加え、PQC 処理機能を追加し、IoT 機器と接続先との認証から暗号通信までを全て PQC で扱うことができるようになります。また、IoT 機器と接続するクラウドへの安全な通信を実現する「セキュアアクティベートサービス®」に現行暗号と PQC の両方に対応できるハイブリッド証明書を搭載し、既存の暗号資産を活かしながら PQC への安全かつ段階的な移行を可能にします。

TOPPAN デジタルが提供する 2 つのソリューションの PQC 対応を実現することで、IoT 機器の認証から通信まで一貫して現行暗号および PQC へのハイブリッド対応が可能となり、量子コンピューター時代を見据えた IoT 機器の長期的なセキュリティの確保と、移行リスクを抑えた PQC への早期対応を実現します。



「Edge Safe®」と「セキュアアクティベートサービス®」の PQC 対応機能の概要

■ 開発の背景

近年、膨大な計算能力を持つ量子コンピューターが実用化されることで、インターネット上のサービスの暗号技術である公開鍵暗号（※3)が容易に解読される可能性が指摘されています。このような将来的

TOPPANホールディングス株式会社 広報本部
E-mail:kouhou@toppan.co.jp

な脅威に備え、米国政府機関の国立標準技術研究所（以下 NIST）が PQC の標準化を推進するなど、セキュリティ対策が世界的に加速しています。特に、長期間利用されるIoT機器においては、暗号鍵や証明書の盗聴・改ざん、さらに将来的に行われるハーベスト攻撃(※4)といった潜在的な脅威から、長期間のセキュリティを確保することが急務となっています。セキュリティを確保しながら、PQC への移行を成功させるには、新旧の暗号を並行して安全に利用できる暗号の俊敏性(クリプト・アジリティ)の確保が不可欠です。TOPPAN デジタルは、こうしたセキュリティ環境の変化に対応するため、これまで PQC に対応した IC カードシステムの開発や通信環境の実証を進めてきました。これらの取り組みのノウハウ・知見を活かして、今回、自社で提供する 2 つのソリューションに IoT 機器の認証から通信を保護する PQC 対応を実装しました。IoT サービスを量子コンピューター時代においても継続利用できる基盤の提供により、PQC への早期移行を支援します。

■ 「Edge Safe®」「セキュアアクティベートサービス®」の PQC 対応機能の特長

TOPPAN デジタルは、NIST で選定された PQC アルゴリズムの処理機能を「Edge Safe®」に組み込み、ハイブリッド証明書の発行・管理機能を「セキュアアクティベートサービス®」と一体で開発しました。これにより、IoT 機器の認証から通信までを一貫して PQC に対応させるソリューション提供を行います。

・現行の暗号方式と PQC 方式を一貫処理「Edge Safe®」

暗号鍵を物理的に守るセキュリティチップである「Edge Safe®」は、工場ロボットやインフラ設備などの IoT 機器に組み込むことで、不正操作を防止するソリューションです。今回の機能追加では、現行の暗号処理機能に加え、PQC 処理機能を「Edge Safe®」に組み込みました。実装したアルゴリズムは、PQC アルゴリズムの標準化を進める NIST が長期的な安全性が確保された暗号技術として選定した ML-DSA(電子署名)と ML-KEM(鍵交換)です。これにより、IoT 機器の接続先との認証から暗号通信までにおいて、現行の暗号方式と PQC 方式の両方を同じ「Edge Safe®」上で一貫して処理することが可能になります。

・現行の電子証明書と PQC 証明書、ハイブリッド証明書、それぞれの発行・管理に対応「セキュアアクティベートサービス®」

「セキュアアクティベートサービス®」は、スマート家電や医療機器がメーカーのクラウドサーバーに接続する際、偽物の機器によるなりすましを防ぐための「デジタル身分証」を発行します。今回、認証に必要な現行の電子証明書に加えて PQC 証明書を発行できる機能を追加しました。これにより、導入先は現行の証明書を利用しながら、PQC 証明書への段階的な移行が可能になります。また、1 つの証明書で現行暗号と PQC の両方に対応できるハイブリッド証明書の発行・管理にも対応しました。これにより、PQC への安全かつスムーズな移行を支援します。

■ 参考価格

・「Edge Safe®」：数百円～/個
　※ロット数など各種条件により異なります。
・「セキュアアクティベートサービス®」：年間数十万円～
　※管理機器の台数など各種条件により異なります。

■ 今後の目標

TOPPAN デジタルは、今回の PQC 対応機能を搭載した「Edge Safe®」および「セキュアアクティベートサービス®」について、IoT 機器を扱う幅広い業界に対して本ソリューションの提供を推進していきます。今後も、日本国内における IoT セキュリティ基盤の耐量子計算機暗号（PQC）への早期移行を支援し、量子コンピューター時代にも安全・安心なデジタル社会の実現に貢献してまいります。

※1「Edge Safe®」

IoT 機器内に組み込み、暗号鍵を物理的に守るセキュリティチップ（セキュアエレメント）です 。一般的なメモリと異なり、分解や解析による不正なデータ読み取りを阻止する「強固な金庫」の役割を果たします。工場ロボットやインフラ設備が盗難・分解された際も、内部の重要な鍵情報を守り抜き、不正操作を防止します 。

※2 「セキュアアクティベートサービス®」

IoT 機器がクラウドへ接続する際に、機器の正当性を証明する「デジタル身分証（電子証明書）」を発行・管理する基盤です。スマート家電や医療機器がメーカーのクラウドサーバーに接続する際、偽物の機器によるなりすましを防ぐための「デジタル身分証」を発行します。

※3 公開鍵暗号

データの暗号化やデジタル署名に使用される、ペアになる 2 つの鍵（公開鍵と秘密鍵）を用いた暗号方式。現行のアルゴリズムは RSA 方式や ECDSA 方式などがある。

※4 ハーベスト攻撃

「今、暗号化された通信データを盗聴・蓄積（収集）しておき、将来的に高性能な量子コンピューターが登場した際に解読を行う」攻撃手法 。

＊ 本ニュースリリースに記載された商品・サービス名は各社の商標または登録商標です。

＊ 本ニュースリリースに記載された内容は発表日現在のものです。その後予告なしに変更されることがあります。

以　上

TOPPANホールディングス株式会社　広報本部
E-mail:kouhou@toppan.co.jp