本リリースは、株式会社インテックとQuantinuumの2社から配信しております。重複して受信される場合がございますが、予めご了承ください。

2025年2月4日
株式会社インテック
Quantinuum

インテックとクオンティニュアム、インテックの電子証明書発行サービス（EINS/PKI）で耐量子コンピューター暗号証明書の提供を開始

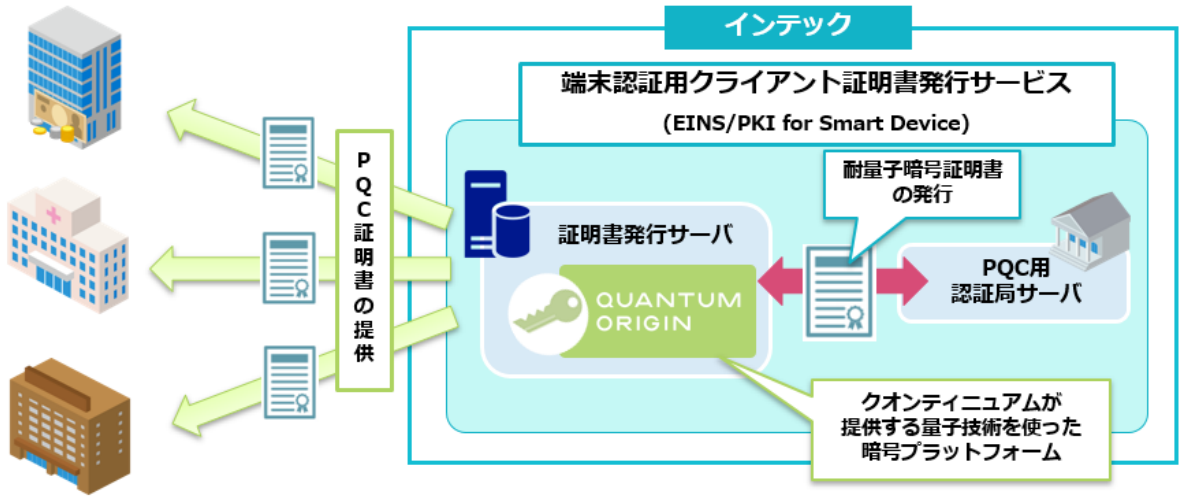
～量子コンピューター時代を見据えた暗号アルゴリズム対応を強化～

TISインテックグループの株式会社インテック（本社：富山県富山市、代表取締役社長：疋田　秀三、以下：インテック）とQuantinuum（本社：米国コロラド州ブルームフィールド、CEO：Rajeeb Hazra、以下：クオンティニュアム）は共同で、お客さまの検証に利用可能な耐量子コンピューター暗号証明書（以下：PQC証明書）の発行機能を、インテックが提供する「端末認証用クライアント証明書発行サービス（EINS/PKI for Smart Device）」に実装し、2025年2月から提供を開始します。

インテックの「端末認証用クライアント証明書発行サービス（EINS/PKI for Smart Device）」に、クオンティニュアムが提供する量子技術を使った暗号プラットフォームである「Quantum Origin」を導入することで、より強固な暗号アルゴリズムの標準化への対応をサポートし、きたる量子コンピューター※1時代を見据えた高度なセキュリティを実現します。

※1 量子力学の特性を利用し、特定の問題を、現在の古典的なコンピューターよりも劇的に速く解ける可能性があると期待されるコンピューター。

＜PQC証明書発行機能のイメージ＞



■PQC 証明書発行機能の概要

1.「端末認証用クライアント証明書発行サービス（EINS/PKI for Smart Device)」への PQC 証明書発行機能の実装

「端末認証用クライアント証明書発行サービス（EINS/PKI for Smart Device)」の基盤にクオンティニュアムの「Quantum Origin」を組み込み、連邦情報処理標準（Federal Information Processing Standards：FIPS）※2 として標準化された暗号アルゴリズムの 1 つである「ML-DSA」で署名した PQC 電子証明書を発行。

※2 米国国立標準技術研究所（NIST）が、連邦情報セキュリティマネジメント法（FISMA）に基づいて制定した、コンピューターシステムに関する基準とガイドライン。

2. お客さま検証用 PQC 証明書の提供

量子コンピューターによる既存暗号の解読が現実の脅威となる前に、自社のサービスやアプリケーションへの PQC 証明書の導入を検討しているお客さま向けに、検証用の PQC 証明書を提供し、長期的なデータ保護と自社のサービスやアプリケーションの信頼性向上の実現をサポート。

＜PQC 証明書の利用シーン＞

秘匿性の高いデータを取り扱っている以下の分野での活用を想定

金融業界：金融取引や顧客情報などの機密情報を保護

医療分野：電子カルテやゲノム情報などの機密医療情報を保護

製造業　：IoT デバイスの認証を強化、企業の技術情報や知的財産を保護

行政機関：住民情報や納税情報などの個人情報を保護

■背景

1. 米国国立標準技術研究所（以下：NIST）による耐量子コンピューター暗号技術の標準化

NIST は、量子コンピューターの発展により、将来、RSA などの従来の暗号アルゴリズムが解読されてしまう可能性を見据え、より強固な暗号アルゴリズムである耐量子コンピューター暗号（PQC：Post-Quantum Cryptography）の標準化を進めています。

2016 年に選定および公募活動を開始し、2024 年 8 月に標準化を進めていた 4 つの暗号アルゴリズムのうち 3 つを FIPS として採用しました。

今後、NIST から PQC 証明書のプロファイルや実装ガイドラインが提供され、2035 年までに米国政府調達要件としての PQC が完全に盛り込まれる予定です。

そのため、インテックは、企業やサービス・アプリケーション開発者が、前もって新たな暗号アルゴリズムを検証し、PQC 証明書の導入がスムーズに行えるよう、検証用証明書の提供を開始しました。

2. 高品質な乱数生成の重要性

暗号システムの信頼性は、鍵の生成と安全な通信に使用される乱数の強度と予測不可能性に依存しています。しかし、従来の方法ではランダム性を近似するに留まり、完全な乱数を実現することは困難でした。クオンティニュアムは、「Quantum Origin」を通じて、量子現象を活用した真に予測不可能な乱数生成技術を提供します。この技術は、証明可能な量子乱数を基盤とし、現在および将来の暗号セキュリティのための強固な基盤を実現します。

3. インテックの「端末認証用クライアント証明書発行サービス」の強化

インテックは「端末認証用クライアント証明書発行サービス（EINS/PKI for Smart Device)」を提供し、お客さま専用プライベート認証局を構築し、リモートアクセス時の認証やデータの署

名・暗号化を行うための電子証明書を発行しています。
インテックでは、量子社会に向けたセキュリティ強化と PQC の標準化に対応するため、電子証明書発行サービスのアプリケーションに、クオンティニュアムの質の高いエントロピーを持つ量子乱数を生成することが可能な「Quantum Origin」を組み込み、より安全な PQC 証明書の発行を可能にしました。

＜提供価格＞
個別にご相談の上、都度見積となります。料金の詳細はお問い合わせください。

■今後の展開
インテックとクオンティニュアムは、NIST の標準化動向や今後のネットワーク機器および通信ソフトウェアへの PQC 証明書実装の対応状況を鑑みながら、PQC 証明書の商用提供の準備を進めていきます。お客さまのデータを最新のセキュリティ技術で安全に保護できるよう、引き続きサービス機能のアップデートを行う予定です。

※ 記載されている会社名、製品名は、各社の登録商標または商標です。
※ 記載されている情報は、発表日現在のものです。最新の情報とは異なる場合がありますのでご了承ください。

■インテックの「電子証明書発行サービス（EINS/PKI）」について
サーバやデバイスの本人性証明／メッセージ認証／通信経路の暗号化などを実現する電子証明書を提供しており、用途別に 3 つのサービスを展開しています。

・パブリック Web サーバ証明書発行サービス
https://www.intec.co.jp/service/detail/eins_pki_publicweb/
・端末認証用クライアント証明書発行サービス（EINS/PKI for Smart Device）
https://www.intec.co.jp/service/detail/eins_pki_smartdevice/
・インターネット EDI 対応電子証明書発行サービス（EINS/PKI for EDI）
https://www.intec.co.jp/service/detail/eins_pki_edi/

■クオンティニュアムの「Quantum Origin」について
Quantum Origin は、市場で最高品質とされる乱数を生成し、数学的に完璧に近いことが証明されるランダム性を実現します。 クオンティニュアムの量子コンピューターと高度な数学を活用し、ソフトウェア実装を通じて既存の乱数発生器を飛躍的に強化し暗号鍵の最大限のセキュリティを確保します。この革新的なソリューションは、既存システムにシームレスに統合することができ、現代の暗号化における課題に対応すると同時に、量子時代の到来を見据えた耐量子コンピューター暗号の需要にも備えます。

詳細は、以下をご参照ください。
https://www.quantinuum.com/products-solutions/quantum-origin/

株式会社インテックについて（https://www.intec.co.jp/）
お客さまの経営戦略に沿った情報化戦略の立案からシステムの企画、開発、アウトソーシング、サービス提供、運用保守まで、IT 分野において幅広く事業を展開しています。インテックは、1964 年の創業以来培ってきた技術力をもとに、AI、RPA 等のデジタル技術の活用や、新たな市場の創造にも積極的に挑戦しています。常にオープンな姿勢で、人、企業、社会を技術でつなぎ、自らも変革しながら「豊かなデジタル社会の一翼を担う」企業としてお客さまに新しい価値を提供していきます。

Quantinuumについて（https://quantinuum.com）

Quantinuumは、Honeywell Quantum SolutionsのハードウェアとCambridge Quantumのミドルウェアおよびアプリケーションを併せ持つ量子コンピューティング企業です。科学主導・企業駆動（science led, enterprise driven）で、量子コンピューティングと化学、サイバーセキュリティ、金融、最適化などのアプリケーションの開発を加速しています。エネルギー、物流、気候変動、ヘルスケアなどの分野で、世界で最も差し迫った問題を解決するためのスケーラブルで商業的な量子ソリューションを創造することに重点を置いています。米国、欧州、日本の9つの拠点で、370名以上の科学者を含む500名以上の従業員を擁しています。

【本件に関するお問い合わせ先】

◆報道関係からのお問い合わせ先

株式会社インテック　テクノロジー＆マーケティング本部　広報室　小川、長谷、稲垣
E-Mail：press@intec.co.jp

クオンティニュアム株式会社
広報事務局（株式会社プラップジャパン）　担当: 佐藤・藤井
Tel: 03-4580-9156
E-Mail：quantinuum_pr@prap.co.jp

◆本サービス・技術に関するお問い合わせ先

株式会社インテック
ＩＣＴプラットフォームサービス事業本部　ネットワークサービス事業部
ＴＰＳサービス部　白木
E-Mail：net_info@intec.co.jp

クオンティニュアム株式会社
マーケティング担当　左近（サコン）
E-Mail：japan.marketing@quantinuum.com