本リリースは、株式会社インテックとキヤノン IT ソリューションズ株式会社と Quantinuum の 3 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。

2024 年 8 月 2 日
株式会社インテック
キヤノン IT ソリューションズ株式会社
Quantinuum

インテック、キヤノン IT ソリューションズ、クオンティニュアム、耐量子暗号証明書を利用したインターネット EDI 接続検証を完了

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）とキヤノンITソリューションズ株式会社（本社：東京都港区、代表取締役社長：金澤 明、以下キヤノンITS)、Quantinuum（本社：米国コロラド州ブルームフィールド市、CEO: Rajeeb Hazra、以下クオンティニュアム）は、共同で、量子コンピュータ由来の乱数を利用して強化された、耐量子計算機暗号証明書（以下、PQC証明書）を利用したインターネットEDIにおける、接続検証を完了したことを発表します。

■背景

1. NIST による耐量子暗号技術の標準化について

NIST（米国商務省標準化技術研究所：National Institute Standards and Technology）は、量子コンピュータ※1 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計算機暗号（PQC：Post-Quantum Cryptography）の標準化を進めています。

2016 年に選定及び公募活動を開始し、2023 年に 4 つの暗号アルゴリズムを標準化候補として選定しています。2024 年には標準化作業が完了し、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になっています。

※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。

2. インターネット EDI における暗号証明書について

インターネット EDI における電子証明書も、認証・署名・暗号化に利用されており、量子コンピュータの出現はセキュリティ上の脅威となります。そこで、かねてより EDI ソリューション分野で協業しているインテックとキヤノン ITS は、インターネット EDI における PQC 証明書の実用化に向け、インテックの EDI アウトソーシングサービス（EINS/EDI-Hub Nex）と、キヤノン ITS の EDI パッケージソフトウェア「EDI-Master B2B for JX-Client」間で、耐量子暗号証明書を利用した接続検証を行いました。

3. インテックのインターネット EDI 対応電子証明書発行サービスの強化について

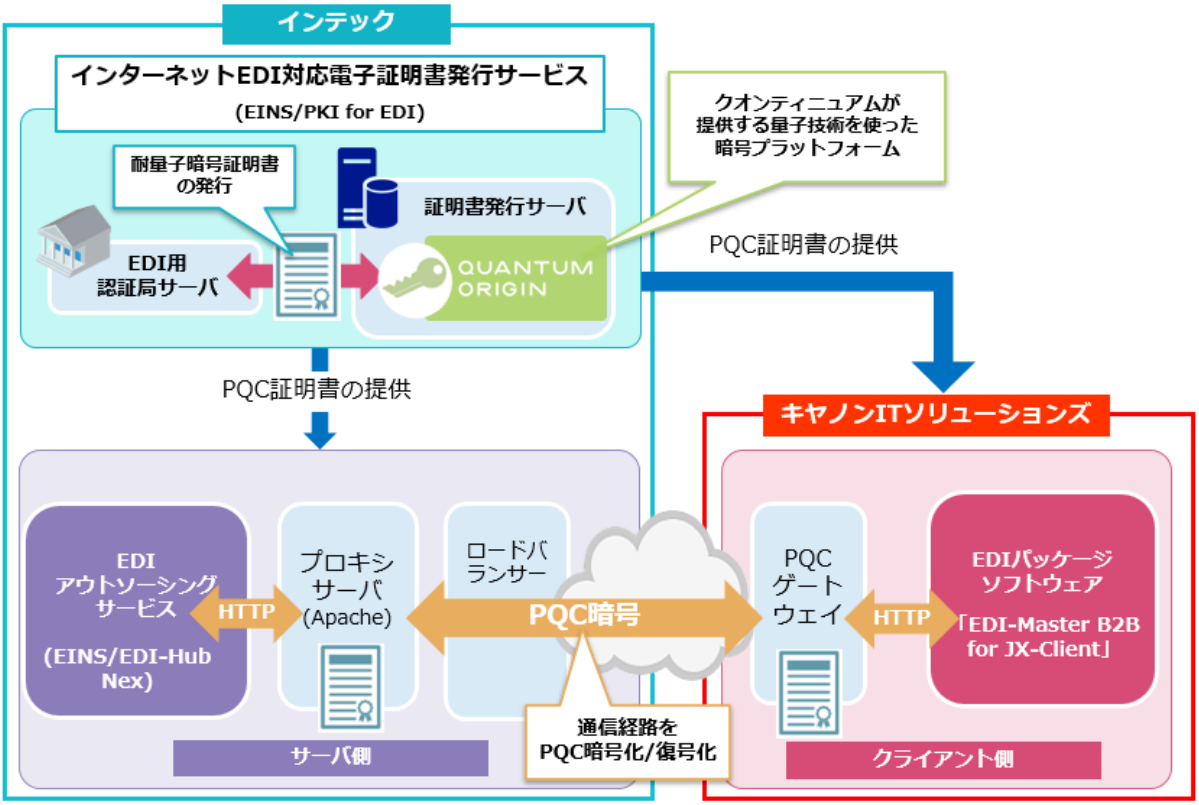
インテックはインターネット EDI 対応電子証明書発行サービス（EINS/PKI for EDI）※2 を提供しており、インターネット EDI における認証・署名・暗号化を行うための電子証明書を発行しています。

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エントロピーの質が証明される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。

※2 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）はインターネット EDI 普及推進協議会（Japan internet EDI Association：略称 JiEDIA/ジェディア）の認証局認定制度の認定を受けています。
URL：https://www.jisa.or.jp/jiedia/tabid/2822/Default.aspx

■PQC 証明書を利用したインターネット EDI 接続検証の概要
＜インターネット EDI 接続検証のイメージ＞



1. インターネット EDI 対応電子証明書発行サービスへの PQC 証明書発行機能の実装

インテックのインターネット EDI 対応電子証明書発行サービス（EINS/PKI for EDI）の基盤に「Quantum Origin」を組み込み、証明可能で予測不可能な量子乱数を生成し、NIST での標準化候補として挙げられている署名アルゴリズム「dilithium2」で署名した電子証明書を発行。

2. EDI 通信内容に対して PQC 暗号化処理を行う PQC ゲートウェイサーバの開発

キヤノン ITS の R&D 部門にて PQC の暗号化処理を行うツール「PQC ゲートウェイサーバ」を新規開発。EDI 通信ソフトのプロキシとして動作し、通信内容を PQC 暗号化して送信することで耐量子暗号技術を活用したセキュアな通信を実現。

3. インターネット EDI における接続検証

キヤノン ITS のインターネット EDI パッケージソフトウェア「EDI-Master B2B for JX -Client」をクライアント、インテックの EDI アウトソーシングサービス（EINS/EDI-Hub Nex）をサーバとして接続を検証。

「EDI-Master B2B for JX-Client」の前段に PQC ゲートウェイサーバ、「EINS/EDI-Hub Nex」の前段にプロキシサーバソフトウェア「Apache」※3 を配置。クライアント側とサーバ側に「EINS/PKI

for EDI」から発行したPQC証明書を組み込み、インターネットEDIプロトコルでの暗号化通信に成功。

■今後の展開

2024年中に、NISTから暗号化アルゴリズム標準化候補のドキュメント公開が予定されています。インテックは、NISTの標準化動向を鑑みてPQC証明書の商用販売の準備を進めてまいります。また、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）だけではなく、お客様専用の認証局を構築して組織内での利用に限定した電子証明書を発行する「端末認証用証明書発行サービス（EINS/PKI for Smart Device)」にもPQC証明書の発行基盤を組み込み、電子証明書発行サービス（EINS/PKI）全体を通してお客様の安全なネットワーク利用を引き続きサポートしてまいります。

キヤノンITSは、来たる量子コンピュータによるセキュリティの脅威に備え、今回の実証実験・実績を生かしながら、EDI-Masterシリーズへの PQC暗号処理機能の実装準備を進めてまいります。今後もR&D部門にて先進技術の研究開発に取り組むと共に、これまで40年以上にわたりEDIシステムを提供してきた知見と実績をもとに、EDIのリーディングカンパニーとして、新しいインターネットEDI時代を築くEDIのベストパートナーをめざします。

※3 Apache：世界的に最も普及しているWebサーバ（HTTPサーバ）ソフトウェアの一つ。

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います。お客様の用途別に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/）

EDI-Masterシリーズについて

さまざまな業界・業種で利用されている標準プロトコルにクラウドも含めたマルチプラットフォームで対応し、小規模～大規模EDIシステムまで構築可能なトータルEDIソリューションです。通信機能はもちろん、EDIシステムに必要な変換、運用管理機能もご用意。経験豊富な専任スタッフが、EDIシステムの導入から構築、運用までをご支援します。
製品紹介ページ：https://www.canon-its.co.jp/solution/edi/

Quantum Originについて

クオンティニュアムが開発したユニークな量子コンピュータ由来の量子乱数を提供するソリューション。量子シードを使用して、ターゲットシステム内の既存のランダムネスを強化し、予測不可能な乱数を生成し、使用することが可能で、非常に強固な暗号鍵を生成することが可能となる。既存の暗号アルゴリズムだけでなく耐量子計算機暗号(PQC)にも対応。
サービス紹介ページ：https://quantinuum.co.jp/business/origin/

株式会社インテックについて（https://www.intec.co.jp/）

お客様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」企業としてお客様に新しい価値を提供してまいります。

キヤノン IT ソリューションズ株式会社について（https://www.canon-its.co.jp/）

キヤノン IT ソリューションズは、キヤノンマーケティングジャパングループの IT ソリューション事業の中核企業として、長期ビジョン『先進 ICT と元気な社員で未来を拓く“共想共創カンパニー”』のもと、システムインテグレーションやコンサルティング、各種ソフトウェアの開発・販売、データセンターサービスやネットワークインフラ構築・運用・保守など幅広く事業を展開しています。

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、350 名以上の科学者を含む 480 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

キヤノン IT ソリューションズ株式会社
企画本部 コーポレートマーケティング部 コミュニケーション推進課
TEL：03-6701-3603（直通）

◆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
情報流通プラットフォームサービス事業本部　営業部　竹内
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

キヤノン IT ソリューションズ株式会社
ビジネスソリューション営業本部 営業部
TEL：03-6701-3456（直通）