2026 年 3 月 31 日

各 位

株式会社大和証券グループ本社
大和証券株式会社
株式会社大和総研
日本電気株式会社
F5 ネットワークスジャパン合同会社
デジサート・ジャパン合同会社

オンラインサービスにおける耐量子計算機暗号（PQC）技術の概念実証結果を公表
～量子コンピュータ時代に向けたセキュリティ強化の取り組み～

株式会社大和証券グループ本社（以下「大和証券グループ本社」）傘下の大和証券株式会社（以下「大和証券」）、株式会社大和総研（以下「大和総研」）は、日本電気株式会社（以下「NEC」）、F5 ネットワークスジャパン合同会社（以下「F5 ネットワークス」）およびデジサート・ジャパン合同会社（以下「デジサート」）と協働し、量子コンピュータ時代に備えた耐量子計算機暗号[1]（Post-Quantum Cryptography、以下「PQC」）技術の概念実証（以下「実証」）について、その結果を公表いたします。

本実証は、大和証券のオンラインサービスにおけるインターネット通信のセキュリティ強化を目的とし、PQC の正式導入に向けた技術面の観点から検証を行ったものです。

量子コンピュータ開発の進展により、将来的に従来の公開鍵暗号方式の安全性が失われる可能性が指摘されています。お客様の重要な情報を取り扱う金融機関においては特に PQC の早期導入が必要だと考え、大和証券、大和総研は、PQC に関する専門的な知見を持つ NEC、F5 ネットワークス、デジサートと共に、証券業界における PQC の実用化に向けた取り組みとして、オンラインサービスを用いた実証を実施しました。

本実証の結果と標準化などの動向および移行の進め方の考察を併せてホワイトペーパーとして取りまとめました。主なポイントは以下のとおりです。

① 実証結果
インターネット通信において、PQC の鍵交換処理に伴う処理時間の増加は限定的である一方、鍵サイズ増加による通信量やパケット数が増加することから、十分な帯域が確保されていない通信環境については、事前の確認が必要であることが明らかになりました。

② 標準化の動向
インターネット通信で利用される暗号処理の一部については、業界における標準化が進展途上にあるものも存在しており、今後の標準化動向を踏まえた段階的な移行が必要であることを整理しました。

③ PQC 移行の進め方
今回検証したシステムにおいても複数の暗号方式が利用されていることから、システム全体を俯瞰した対応を行うためには、暗号移行を専門に検討する体制の構築や、暗号の利用箇所と方式を整理した台帳の作成に着手することが有効であるとの示唆が得られました。

検証結果を踏まえ、大和証券グループにおける PQC の正式導入に向けた方針を策定し、量子コンピュータの実用化を見据えたセキュリティ強化と安全なシステム基盤の構築を推進していきます。

---

[1] 耐量子計算機暗号（Post-Quantum Cryptography ： PQC）とは、十分な計算能力を持つ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と考えられている暗号の総称

■ 各社の役割

大和証券グループ本社	グループ内の連携・調整、進捗およびリスク管理を担い、検証結果を基に大和証券グループのオンラインサービスにおける安全性と利便性を両立する PQC 導入の方針を策定しました。
大和証券	本実証活動において、オンラインサービスへの PQC 適用時における互換性、処理性能、運用影響を検証し、その結果を実運用時のシステム設計・運用方針の策定に反映していきます。
大和総研	これまでに行った PQC に関する概念実証の知見を活かし、検証環境の構築からシナリオ作成、技術検証、評価までを一貫して実施しました。さらに、成果をホワイトペーパーとしてまとめ、金融業界に向けて知識の共有と議論の深化に貢献いたします。
NEC	実証に際して PQC に関する専門的見解を提供し、技術的信頼性の向上に貢献しました。量子技術に関するこれまでの研究成果と知見も活かして、ホワイトペーパーのレビューを担当しました。
F5 ネットワークスジャパン合同会社	PQC 対応の ADC（Application Delivery Controller）を提供し、次世代ネットワークインフラの実現に向けた基盤技術を支えています。
デジサート・ジャパン合同会社 DigiCert Inc.	世界有数の認証局としてインターネット標準作成に参画する立場から PQC に関する国際標準化動向と PKI（Public Key Infrastructure：公開鍵暗号を安全に運用するための基盤）の専門知見を提供しました。

詳細なホワイトペーパーは大和総研のウェブサイトからご確認ください。
https://www.dir.co.jp/report/technology/security/20260331_025651.html

以　上