2025 年 8 月 27 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

オンラインサービスにおける耐量子計算機暗号（PQC）技術の概念実証を開始
～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」）および、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」）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 : PQC）技術の概念実証（以下「実証」）を開始いたします。

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および運用面での検証を行うものです。

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やデジタル署名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 や F5 ネットワークスと共に、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することとしました。

■ 実証概要

- 対象システム：オンラインサービスの開発環境
- 実施期間：2025 年 9 月～2026 年 3 月（予定）
- 検証内容：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への PQC 技術の適用
- 検証項目：通信時間への影響、既存処理との互換性、安定性の評価　等

本検証の結果についてはホワイトペーパー[2]として公表し、金融業界における PQC 対応を推進するための参考資料として広く活用されることを目指します。また、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

---

[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

[2] 特定の技術や課題に関する調査・検証結果を体系的にまとめた文書のこと

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。

■ 各社が担う役割

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す。
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す。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を図ります。
NEC	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す。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、ホワイトペーパーを大和総研と共同で執筆します。
F5 ネットワークスジャパン	PQC 対応の ADC（Application Delivery Controller）を提供、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。

以　上