2020 年 12 月 21 日

報道関係各位

野村ホールディングス株式会社
野村證券株式会社
国立研究開発法人情報通信研究機構
株式会社東芝
日本電気株式会社

金融分野のサイバーセキュリティ強化に向けた量子暗号技術活用の共同検証を開始
～株式取引に代表される大容量・低遅延通信への耐性を検証～

野村ホールディングス株式会社（代表執行役社長 グループ CEO 奥田 健太郎、以下 野村 HD）、野村證券株式会社（代表取締役社長 森田 敏夫、以下 野村證券）、国立研究開発法人情報通信研究機構（理事長 徳田 英幸、以下 NICT）、株式会社東芝（代表執行役社長 CEO 車谷 暢昭、以下 東芝）、日本電気株式会社（代表取締役 執行役員社長 兼 CEO 新野 隆、以下 NEC）は、金融分野におけるデータ通信・保管のセキュリティ強化に向けて、量子暗号技術の有効性と実用性に関する国内初の共同検証を 12 月より開始します。

なお、本共同検証は、内閣府が主導する戦略的イノベーション創造プログラム（SIP、注 1）「光・量子を活用した Society 5.0 実現化技術」（管理法人：国立研究開発法人量子科学技術研究開発機構）の一環として実施します。

【背景】

金融機関に対するサイバー攻撃の脅威が増え、金融システムへの影響が懸念されています。こうした中、金融庁により「金融分野におけるサイバーセキュリティ強化に向けた取組方針」が示され、各金融機関がその強化に取り組んでいるところです。特に近年、金融分野においては、デジタライゼーションの加速的な進展や API 連携（注 2）を始めとする企業間の連携強化等、システムを取り巻く環境が大きく変わってきており、そのセキュリティ対策についてもより一層の強化が求められています。

システム内外におけるデータ通信の安全を確保する暗号技術は、既に社会に広く普及しています。現在の暗号は、第三者が解読するには非常に複雑な計算が必要であり、解読までに天文学的な計算時間を要することから、現実的に通信内容が解読・傍受される懸念は無いと考えられてきました。一方、最近では、現在の暗号を高速に解読できることが知られている量子コンピュータ技術の研究開発が急速に進展するなど、潜在的な脅威も高まっています。

金融分野において、顧客情報の保護は遵守すべき最優先事項であり、将来的な脅威に備えた新たな安全性対策が急務となっています。

【今回の共同検証について】

今回、野村 HD、野村證券、NICT、東芝、NEC の 5 者は共同で、「理論上いかなる計算能力を持つ第三者（盗聴者）でも解読できないことが保証されている唯一の暗号方式」である量子暗号（注 3）の金融分野への適用可能性について検証していきます。

なお、金融機関において稼働しているシステム環境の中に、量子暗号に必要となる装置を実際に設置し、検証するという今回の 5 者の取り組みは、国内で初めての試みとなります。

【共同検証の概要】

今回 5 者は、野村證券が保有する顧客情報や株式取引情報等の疑似データ（架空データ）を量子暗号により秘匿伝送する実験や、遠隔地の複数のデータサーバまで秘密分散（注 4）を用いてバックアップ保管や安全な計算処理を行う量子セキュアクラウドシステム（注 5）の動作検証等を実施します。

具体的には、東芝が開発した量子暗号装置を野村證券の拠点に導入し、NICT が 2010 年から運用を続けている量子暗号ネットワーク 「Tokyo QKD Network（注 6）」を野村證券の拠点まで伸長し、図 1 に示すような環境を構築して共同検証を進めます。

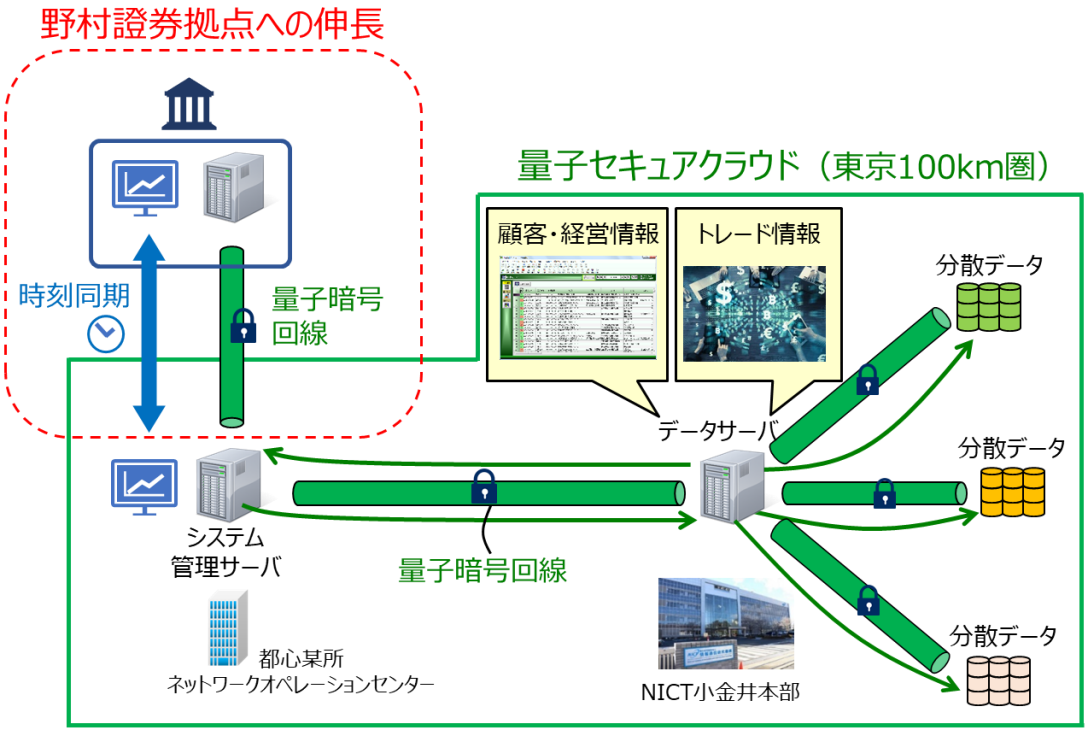


図 1 量子暗号及び量子セキュアクラウドシステムの検証環境のイメージ図

量子暗号における暗号化/復号の処理は、伝送情報/暗号文と暗号鍵の単純な論理和であるため（注 3 の図を参照）、従来の暗号方式よりも低遅延で実行できます。このため、極めて低遅延の通信が求められる取引処理の暗号通信に適しています。

こうした低遅延性の検証のために、今回は、ミリ秒未満での取引処理が求められ、大容量・高速通信が必要となる株式トレーディング業務において、量子暗号を用いた場合に処理遅延が発生しないかを検証していきます。

また、量子セキュアクラウドシステムにおいては、仮に自社システムに外部からの侵入があったとしても、影響を最小限に抑えるための内部対策についても高度化を図る予定です。今回は、安全で利便性の高いアクセス管理技術の高度化、（機密性の高い）顧客データの秘匿性を保ったまま統計情報等を抽出・処理する秘匿計算機能の実装法の検討などに取り組む予定です。

今後、5 者は本検証の成果を踏まえ、金融分野のサイバーセキュリティ強化に向けた量子暗号技術・量子セキュアクラウドシステムの活用策、適切な

導入プランの策定などに取り組んでいく予定です。

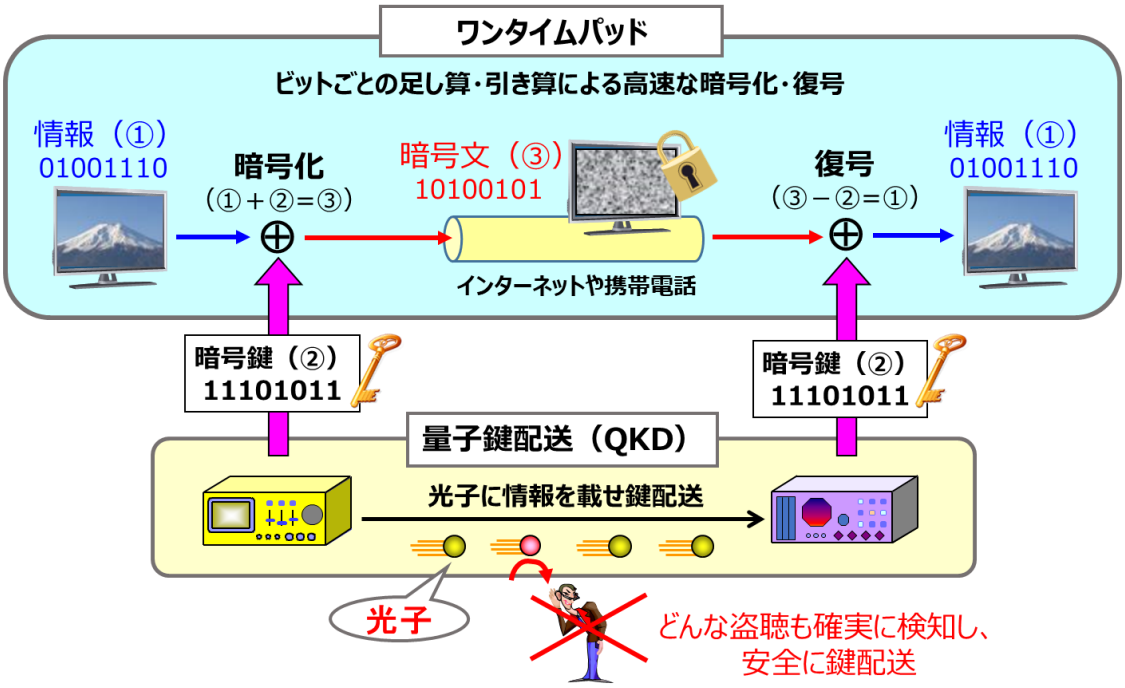
【実施体制】
今回の共同検証は、以下の体制で実施する予定です。

・野村 HD・野村證券：自社システムの提供・金融実務に見合った疑似データ（架空データ）の生成・金融実務への適用可能性検証等
・NICT：Tokyo QKD Network の運用・管理、量子セキュアクラウドシステムの提供および金融環境における機能検証
・東芝：量子暗号装置の導入と運用支援や、他のフィールド実証経験から得た知見に基づく、量子暗号と暗号通信アプリケーションとの連携システムの検討および構築
・NEC：量子暗号装置の開発と運用支援・フィールド実証経験から得た知見に基づく、量子暗号装置とアクセス管理のための認証技術との連携システムの検討および構築

（注 1） 戦略的イノベーション創造プログラム（SIP）：
内閣府総合科学技術・イノベーション会議が司令塔機能を発揮して、府省の枠や旧来の分野を超えたマネジメントにより、科学技術イノベーション実現のために創設した国家プロジェクト。https://www8.cao.go.jp/cstp/gaiyo/sip/

（注 2）API 連携：
API（Application Programming Interface）とは、異なるソフトウェアと相互に情報をやり取りするために定められた手続きを指し、API に従って他のシステムから一部機能を呼び出す、システム間の連携方式を API 連携と呼ぶ。

（注 3） 量子暗号：
光子を使って暗号鍵共有を行う量子鍵配送（QKD）装置、及びその暗号鍵を使い、ワンタイムパッド方式により情報の暗号化・復号を行う暗号技術のこと。量子コンピュータを含むあらゆる計算機で原理的に解読できない極めて安全な通信を実現できる。



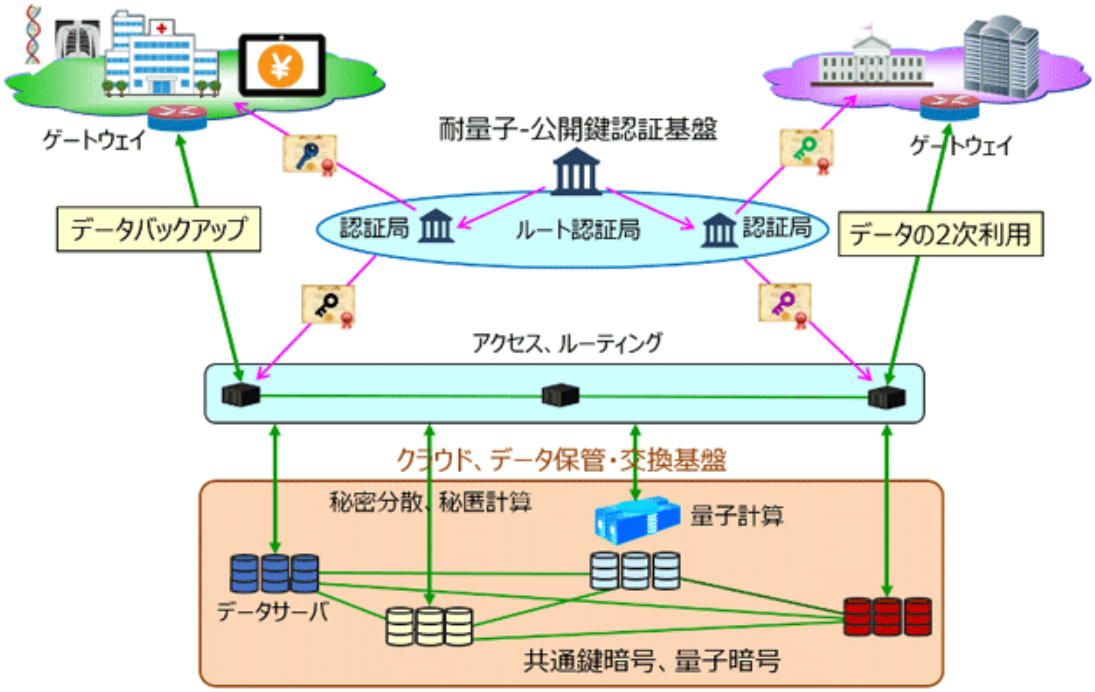
量子暗号回線の構成

（注 4） 秘密分散：

原本データを無意味化した複数（n 個）の分散データに分割し、ある閾値（k 個）以上の分散データがそろわないと原本データを復元できなくする技術。k 個未満の分散データからは、たとえ量子コンピュータでも原本データを復元できない機密性を実現できる。

（注 5） 量子セキュアクラウドシステム：

量子セキュアクラウドシステムは量子暗号技術と秘密分散技術を融合し、データの安全な流通/保管/利活用を可能とするクラウドシステムのこと。本技術の確立により、改ざん・解読が不可能な高いセキュリティ性を担保するだけでなく、例えば、医療、新素材、製造、金融分野で蓄積された個人情報や企業情報など秘匿性の高いデータの収集/分析/処理/利用を可能とする。



量子セキュアクラウドシステムの実装イメージ

（注 6） Tokyo QKD Network：

NICT が 2010 年から東京圏に構築・運用を続けている量子鍵配送（QKD）ネットワークのテストベッド。NEC、東芝、NTT-NICT、学習院大学等の様々な産学機関で開発された QKD 装置が導入され、装置改良の研究開発、長期運用試験、相互接続やネットワーク運用試験など、QKD ネットワーク技術の実用化に向けた研究開発のほか、QKD ネットワークを現代セキュリティ技術と融合した新しいセキュリティアプリケーションの研究開発などを進めている。http://www.tokyoqkd.jp/