報道関係各位

2022 年 1 月 14 日

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

大容量金融取引データの量子暗号による 高秘匿通信・低遅延伝送の検証実験に成功

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：奥田 健太郎、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：綱川 智、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：森田 隆之、以下 NEC）は、今後の量子暗号技術の社会実装に向けて、高速大容量かつ低遅延なデータ伝送が厳格に求められる株式取引業務をユースケースとした量子暗号技術の有効性と実用性に関する共同検証を 2020 年 12 月に開始し、実際の株式トレーディング業務において標準的に採用されているメッセージ伝送フォーマット（FIX（注 1）フォーマット）に準拠したデータを大量に高秘匿伝送する際の、低遅延性及び大容量データ伝送に対する耐性について国内初の検証を行いました。その結果、今回の想定ユースケースにおいては、①量子暗号通信を適用しても従来のシステムと比較して遜色のない通信速度が維持できること、②大量の株式発注が発生しても暗号鍵を枯渇させることなく高秘匿・高速暗号通信が実現できることの 2 点を確認することができました。この検証の成功により、今後、金融以外の分野も含めた量子暗号技術の社会実装の加速が期待されます。

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 2）「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した。

【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。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などにより、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。

一方、株式取引においては、株価や気配情報、出来高などに応じて、コンピュータシステムが自動的に株式売買注文のタイミングや数量を決めて注文を繰り返すという「アルゴリズム取引」が広く普及しており、日々、膨大な取引処理が行われています。国内証券取引所における 1 日の株式などの取引高は 3 兆円以上にものぼり、こうした株式取引の処理においては、膨大な量の取引データ伝送に耐えられる通信方式が必要とされています。また、株式取引においては、取引処理の遅延が機会損失の発生にも繋がることから、証券取引所では注文応答時間がミリ秒未満の処理性能を持つ通信ネットワーク基盤を提供しています。

社会通信インフラは 5G・Beyond5G にも見られるように、高速・大容量化し、低遅延化が求められていますが、株式取引システムにおいても、大容量データ伝送、低遅延通信が高い水準で求められています。

【今回の共同検証の概要】

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通信方式」である量子暗号通信（注 3）の金融分野への適用可能性について、国内で初めての検証を実施しました。

図 1 に本共同検証のシステムの概要を示します。光の粒である光子に鍵情報をのせ暗号鍵共有を行う量子鍵配送（Quantum Key Distribution：QKD）装置（注 4）からの鍵を使った暗号化装置を用いて、低遅延性と大容量耐性の検証を行いました。

検証には、NICT が 2010 年に QKD 装置を導入し構築した試験用通信ネットワーク環境 「Tokyo QKD Network」（注 5）上に、投資家と証券会社を模した金融取引の模擬環境を整備し、実際の株式注文において標準的に用いられるメッセージング・データのフォーマット（FIX プロトコル）に合わせた模擬データを生成するアプリケーションを野村 HD・野村證券で開発しました。

また NICT では、従来、社会実装を見据え、QKD に組み合わせるデータ暗号化方式の検証を行ってきました。今回、伝送するメッセージの暗号化には、ワンタイムパッド（One Time Pad：OTP）（注 6）方式、Advanced Encryption Standard（AES）方式という 2 種類の暗号化方式を採用しました。

OTP は、いかなる計算力を持った第三者に対しても暗号が解読されないという高い安全性（情報理論的安全性）を持つ暗号方式となりますが、伝送データと同じ量の暗号鍵が必要となることから、暗号鍵消費量が多くなる傾向があり、その結果、鍵が枯渇する危険があるという課題があります。今回は鍵の枯渇に対する備えとして AES を併用しました。なお、実装については Gbps レベルの高スループットを可能とするために、NICT が新たに開発した高速 OTP 装置（注 7）を検証で採用しました。

AES は、OTP と異なり情報理論的安全性は有しておらず、暗号解読を行うために天文学的な計算を必要とするという計算論的な複雑さに依存する安全性（計算量的安全性）を持つ暗号化方式です。今回のユースケースにおいては、QKD により生成した暗号鍵を短時間で更新することにより、AES 方式であっても十分なセキュリティ強度を持つと考え、OTP の代替方式として、256 ビットの鍵長を利用する AES（AES256）を選択しました。AES256 の実装にはソフトウェアベースでの実装方式（SW-AES）（注 8）と、より低遅延性に優れた NEC が開発した回線暗号装置（COMCIPHER-Q）（注 9）を用いた方式の 2 種類を採用しました。上記の高速 OTP、SW-AES、COMCIPHER-Q という計 3 種類の方式による暗号化方式を用いて、それぞれの通信性能の測定・比較検証を行いました。

検証に際しては、東芝が開発した高速 QKD 装置及び NEC が開発した QKD 装置で交換した鍵をもとに実際の株式トレーディング業務に沿ったテストケースを設定し、大容量データ伝送時に複数種類の異なるデータ暗号化方式の応答時間を計測することを通じて、QKD ならびに各暗号化方式の実用性を検証しました。具体的には、証券会社の株式業務で 1 日に伝送される取引メッセージ（FIX メッセージ）のデータ総容量、及びその数十倍のデータ伝送量をそれぞれ想定した場合に計測される応答時間について、上記の高速 OTP、SW-AES、COMCIPHER-Q の計 3 種類の暗号化方式の違いによる影響について検証を行いました。こうした株式取引における具体的なテストケースに沿って大容量データ伝送時の QKD ならびにデータ暗号化方式の実用性を比較検証したことにより、今後、金融以外の分野も含めて量子暗号技術を多方面での社会実装に繋げていく上で、重大な示唆が得られたと考えられます。

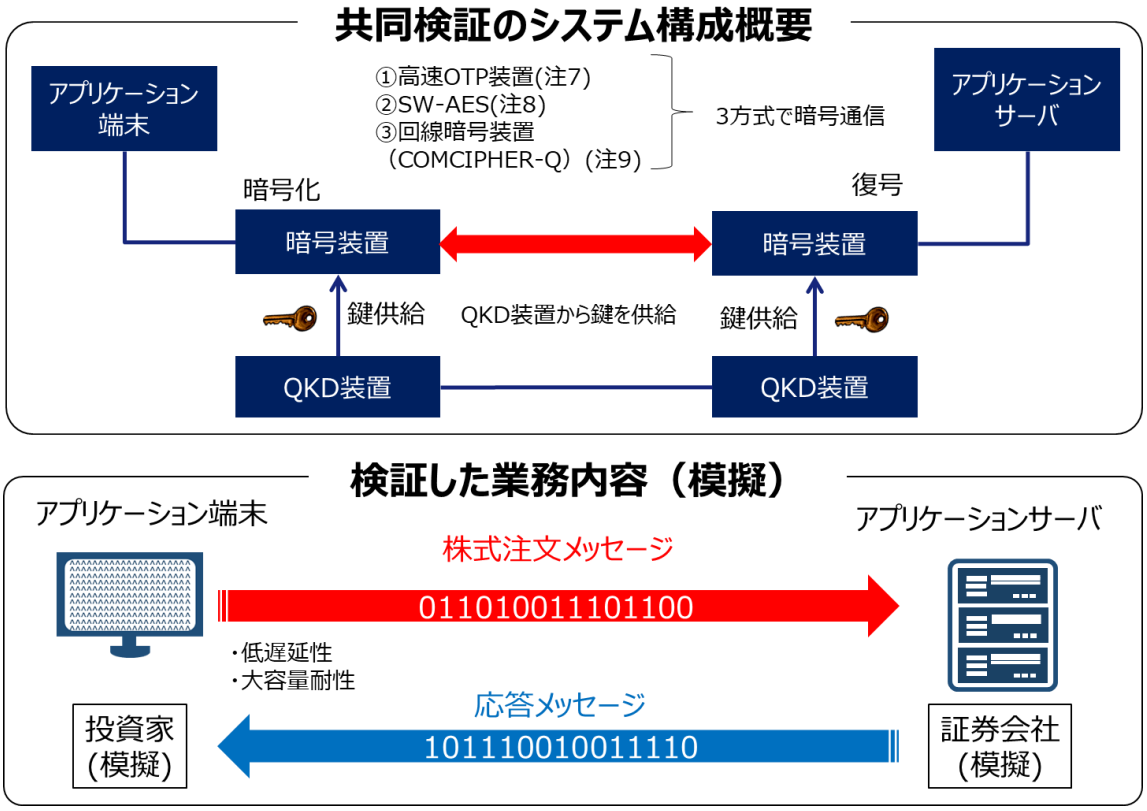


図 1 本共同検証のシステムの概要

【共同検証の結果】

共同検証の実験結果は、図 1 の 3 種類の方式（高速 OTP、SW-AES、COMCIPHER-Q）のいずれかの暗号化方式を用いることで、

① 量子暗号通信を適用しても従来のシステムと比較して遜色のない通信速度が維持できること

② 大量の株式取引が発生しても暗号鍵を枯渇させることなく高秘匿・高速暗号通信が実現できること

を確認できました。

今回の検証では QKD 装置からの鍵の枯渇はありませんでしたが、QKD 装置からの鍵の枯渇が懸念される場合には、鍵消費量の少ない方式に切り替えることで、ビジネスの継続性を維持することが可能です。

これらの結果は、暗号化レベルや暗号通信速度などについて、将来的に様々な顧客ニーズに対応できるシステム構成について、柔軟に提案可能となることを示唆しています。さらに、検証を重ね、再現性及び信頼性のあるデータを蓄積していきます。

【今後の展望】

今回は、①低遅延通信検証及び②大容量データ通信の検証に成功しました。引き続き並行して③連続稼働検証として量子暗号システムを長時間（1 週間程度）連続稼働させてもシステム障害が生じないか（ロングランテスト）、ならびにシステム障害時にシステム切り替えが遅延なく行われるか（ストレステスト）、についても検証中であり、2021 年度末までに検証を行う予定です。

5 者は本共同検証の成果を踏まえ、今後、量子暗号技術の着実な社会実装に向けて、量子暗号技術・量子セキュアクラウドシステムの活用策、ならびに適切な導入プランの策定などに取り組みます。

データの大容量性、通信の低遅延性、システムの連続稼働性について、特に厳しい水準が求められる金融分野において量子暗号システムの実用性を証明することができれば、金融以外の業界にも転用できる可能性が高くなると考えられます。今後は今回の検証を踏まえて量子暗号技術の社会実装に更なる展望を開くべく取り組んでいきます。

以上

＜用語解説＞

（注 1）FIX　：

FIX（Financial Information eXchange：金融情報交換）プロトコルは、財務データや取引に関連するメッセージを電子的にやり取りするための一連のメッセージ仕様である。世界中の銀行やブローカー、取引所、機関投資家、情報技術（IT）プロバイダの協力によって開発され、メッセージ仕様の標準として世界的に認められている。

（fix.pdf　（oanda.jp）より抜粋）

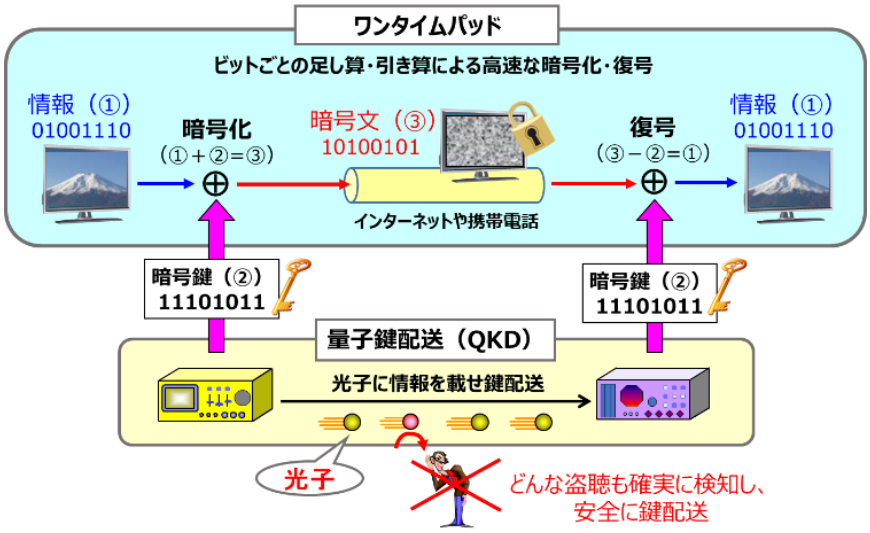
（注 2）戦略的イノベーション創造プログラム（SIP）：

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 3）量子暗号通信：

光子を使って暗号鍵共有を行う量子鍵配送（Quantum Key Distribution：QKD）装置、及びその暗号鍵を使い、ワンタイムパッド（One Time Pad：OTP）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）量子鍵配送装置：

量子鍵配送（QKD）は、通信を行う二者間でのセキュア通信を保証するために、量子力学を用いてランダムな秘密鍵を共有し、それをもとに情報を暗号化・復号するためのものであり、現在、東芝が製品化を行っている。
https://www.toshiba.co.jp/qkd/products.htm

（注 5）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、学習院大学など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。
https://www.nict.go.jp/press/2010/10/14-1.html

（注 6）ワンタイムパッド方式：

ワンタイムパッド（OTP）は、一度使用した暗号鍵を何度も使い回さずに、一度使用したら破棄する方式。

（注 7）高速 OTP 装置：

頻繁な周期的鍵交換をすることなく、ワンタイムパッド（OTP）方式を使用し、高速に動作する安全な暗号装置として開発された試作品。

（注 8）SW-AES：

回線暗号装置（COMCIPHER-Q）がハードウェア上で物理的に鍵交換を行っていた仕組みを、ソフトウェア用に改善し、簡易に鍵交換を行うために開発した試作品。

（注 9）回線暗号装置（COMCIPHER-Q）：

安全保障などの高セキュリティ要求分野で使用されている回線暗号装置（COMCIPHER（AES）シリーズ）に、QKD のための機能を追加したカスタム品（研究試作品）。FPGA（Field Programmable Gate Array）による高速なハードウェア処理を実現した暗号化・復号機能により低遅延・安定した暗号通信を実現。更にソフトウェアで機能追加することにより QKD 向け機能の追加を実現。

（別紙）

【共同検証の前提条件】

図 2 に本共同検証のシステム構成を示します。図中下に示すように、a 系）ネットワークでリファレンス基準値を測定します。次に、b 系）ネットワークで回線暗号装置（COMCIPHER-Q）がもたらす影響を測定します。c 系）ネットワークでは、ハードウェアで物理的に暗号化を行っていた仕組みを、ソフトウェア用に改善した SW-AES を使用した場合の測定をします。最後に d 系）ネットワークでは、QKD 装置から供給された鍵で OTP 暗号化を行い、鍵残量を確認しながら測定を行います。以上の方式で、それぞれの遅延時間、応答時間を測定し、既存システムの通信性能と比較・検討します。本共同検証で測定した遅延時間、応答時間の用語の定義を表 1 に示します。

本共同検証にあたっての前提条件は、以下の通りです。

① 低遅延通信検証（パフォーマンステスト）

実際の証券会社で扱われる注文件数と同程度の量の取引データをアプリケーションによって生成し、遅延時間、応答時間を検証します。

② 大容量データ通信検証（ボリュームテスト）

顧客による取引注文が集中する場合を想定し、上記の取引件数を 80 倍とした上で、遅延時間、応答時間を検証します。

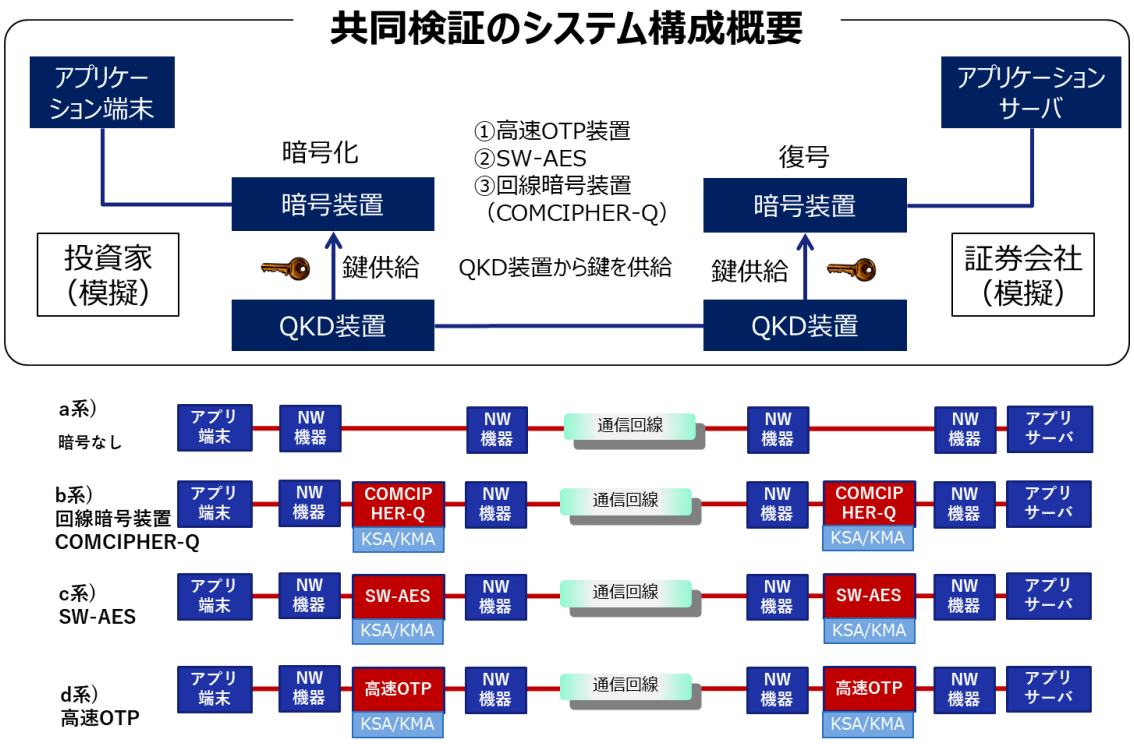


図 2 本共同検証のシステム構成

遅延時間	暗号化なしを基準として、認証局（Certification Authority、CA）などへのドメイン認証の必要ないプロトコル（Transport Layer Security、TLS）を暗号化した場合との差を遅延時間と定義。アプリケーション端末とアプリケーションサーバ間の片道遅延を測定する。
応答時間	アプリケーション端末が問合せメッセージを送信完了した時点（Ts）と、アプリサーバからの応答メッセージがアプリケーション端末で受信され始めた時点（Te）の間隔。（Te-Ts）を応答時間と定義。

表 1 測定のための用語の定義

【共同検証の結果】

検証内容		ネットワーク層の遅延時間測定	低遅延通信検証（パフォーマンステスト10回平均）	大容量データ通信検証（ボリュームテスト80倍）	備考
測定項目		遅延時間	応答時間	応答時間	
回線環境	暗号化なし（a系）	基準（0ms）	1.98 ms	3.60 ms	暗号化なしでリファレンス基準値を求める測定
	COMCIPHER-Q（b系）	0.02 ms	2.04 ms	4.37 ms	ハードウェア系暗号装置がもたらす影響を測定
	SW-AES（c系）	0.22 ms	2.32 ms	4.99 ms	ソフトウェア系暗号装置がもたらす影響を測定
	高速OTP（d系）	0.22 ms	2.34 ms	4.72 ms	OTP暗号化する装置がもたらす影響を測定

表 2　共同検証の結果（パフォーマンステスト及びボリュームテスト）

最初に、メッセージ伝送フォーマット（FIX フォーマット）を模擬したアプリケーションを使用しない状態で、暗号化なし（a 系）を基準として、3 種類の暗号方式（b,c,d 系）とを比較したところ、ミリ秒（0.22ms）以下の範囲の遅延時間に収まり、要求事項の通信性能をネットワーク層以下で有していることを確認しました（表 2）。

①低遅延通信検証（パフォーマンステスト）の結果から、量子暗号通信を適用しても基準となる暗号化なし（a 系）の結果と比較して遜色のない通信速度が維持できることが確認できました。

表 2 から、①低遅延通信検証（パフォーマンステスト）において、3 種類の暗号方式（b,c,d 系）を用いた場合と、暗号なし（a 系）の場合の遅延時間を比較した結果、いずれも 1ms 以下の遅延に収まり、暗号方式の違いを問わず、安定した応答時間でアプリケーションが稼働できていることを確認しました。

②大容量データ通信検証（ボリュームテスト）の結果から、大量の株式取引が発生した場合においても暗号鍵を枯渇させることなく高秘匿・高速暗号通信が実現できることが確認できました。

表 2 から、顧客による取引集中に合せて取引メッセージ件数が増加する場合において、暗号なし（a 系）の場合でパフォーマンステストと比べ応答時間は増加しましたが、同様に暗号化した場合（b,c,d 系）においても、暗号方式にかかわらず、同等程度の増加時間

に収まり、それぞれに差異はみられませんでした。その上で、回線暗号装置（COMCIPHER-Q）による暗号方式（b 系）の場合においては、応答時間が暗号化なし（a 系）と比べても 1ms 以下の遅延で収まりました。

表 2 の測定結果については、今後のロングランテストやストレステストの測定時に再検証を行い、再現性や信頼性を高めていきます。特に、今回のボリュームテストの大容量時の注文殺到時間を増加させ、ストレステストと併せて応答時間、スループットに与える影響を検証していきます。

以上の検証データを基に、上記 3 つの暗号方式を組み合わせることによって、金融アプリケーションを高速暗号化できる条件を導出していきます。さらに次のステップとして、これらに、非常時対応に備えたメインシステム・バックアップシステム間の経路切り替えを可能とするルーティング機能を備えれば、冗長性が向上します。ルーティング機能については、次回以降の応用検証として並行して準備を進めています。