NOMURA
Connecting Markets East & West

資料2-1

金融システムにおける量子耐性の獲得

野村ホールディングス株式会社　デジタル戦略部
デジタル戦略部長　　林　周仙

Drive Sustainability.

Drive Sustainability.

2022年11月24日（木）

NOMURA

目次

- 金融分野の情報セキュリティ
- 金融領域における秘匿通信、秘密分散の（現在・将来の）ニーズ、将来性
- 野村HDにおける取組み
- 金融領域におけるユースケース
- 金融領域で得られる示唆

1. 金融分野の情報セキュリティ

金融では、近年の激変するインフラ環境から、セキュリティリスクに対して常に不安を抱えている。
量子コンピュータの発展に伴う、さらなる国家規模のインフラ攻撃リスクに対して一社だけで対応しきれるのか。

顧客チャネルのデジタル化

非金融業種との連携

在宅勤務に伴うアクセスポイントの多様化

オープンAPIの法制化

（金融機関）

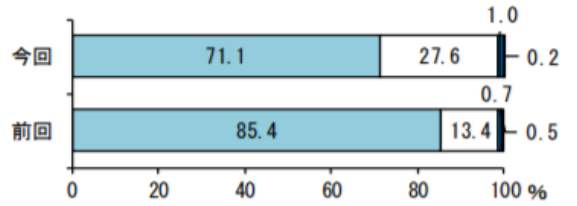
（従来のアプローチ）

金融システムを外部環境から物理的に隔離することによってセキュリティを担保

完全に隔離し切ることがますます困難化になり、セキュリティの重要性が相対的に増大

量子コンピュータによる暗号の危殆化

（ご参考）2017年頃と比較したサイバー攻撃の脅威認識



- 自社に対するサイバー攻撃に脅威を感じており、その脅威はより高まってきている
- 自社に対するサイバー攻撃に脅威を感じているが、その脅威に変化はない
- 自社に対するサイバー攻撃に脅威を感じているが、その脅威は低下してきている
- 自社に対するサイバー攻撃に脅威を然程感じていない

（注）前回は、2015 年頃と比較したサイバー攻撃の脅威認識。

（出所）日本銀行「サイバーセキュリティの確保に向けた金融機関の取り組みと課題－アンケート（2019 年 9 月）調査結果－」

2.金融領域における秘匿通信、秘密分散の現在・将来のニーズ、将来性、課題

金融では守るべき情報・利用シーンに合わせて、現在・将来にわたり業界全体で量子耐性を必要とする。
PQC、QKDのそれぞれの時間軸・特性を踏まえた利用検討が必要か。

既存インフラから見る量子耐性

金融の顧客向けサービスや在宅勤務体制など、通常のインターネット回線やVPNを利用した回線については、NICTによるPQC標準化計画に沿った形での対応に合わせていく。

一方でQKDは、社会実装が近い点また物理回線を用いる点から、現在ある専用線を置き換えるという利用方法が想定しやすい。金融システムにおいては、取引所との通信、税務情報などの情報照会をはじめとして多くの専用線を利用している。金融が攻撃対象になりやすいインフラである点や、ハーベスト攻撃から守るべき情報を踏まえ、QKD導入検討の余地がある。

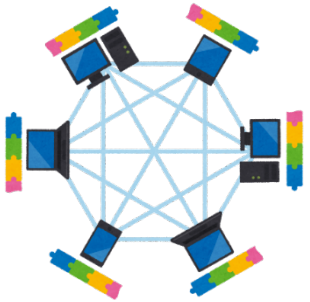
また、マイナンバー制度の活用や金融の相続手続きにおける行政の戸籍情報の活用を、行政コスト負担を減少やデータ管理の在り方について議論する中で、量子耐性のある回線を将来的に必要とする可能性がある。

QKD導入の課題としては、コストとして専用線と比せる競争力が必要か。金融においてはFISCやCRYPTREC等の各種ガイドラインへの導入が必要となるケースもある。またデータ管理の在り方については監督官庁も巻き込んだ議論が必要か。

次世代インフラから見る量子耐性

ブロックチェーン技術などをもちいた次世代の決済インフラにおいては、
量子耐性の検討もされている。

その特性から一度システムをスタートすると止めることが
難しい点や、オープンソース提供といった点も考慮する必要があり、
長期システムを想定したシステム構築も期待される。



3. 野村ホールディングスにおける取組

実際のQKD回線を用いて、低遅延通信・大容量等のテストのため株式取引の通信を実施。実装は容易で実験も成功。

NOMURA　NICT　TOSHIBA　NEC　SIP

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

図1　年初プレスリリース

図2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

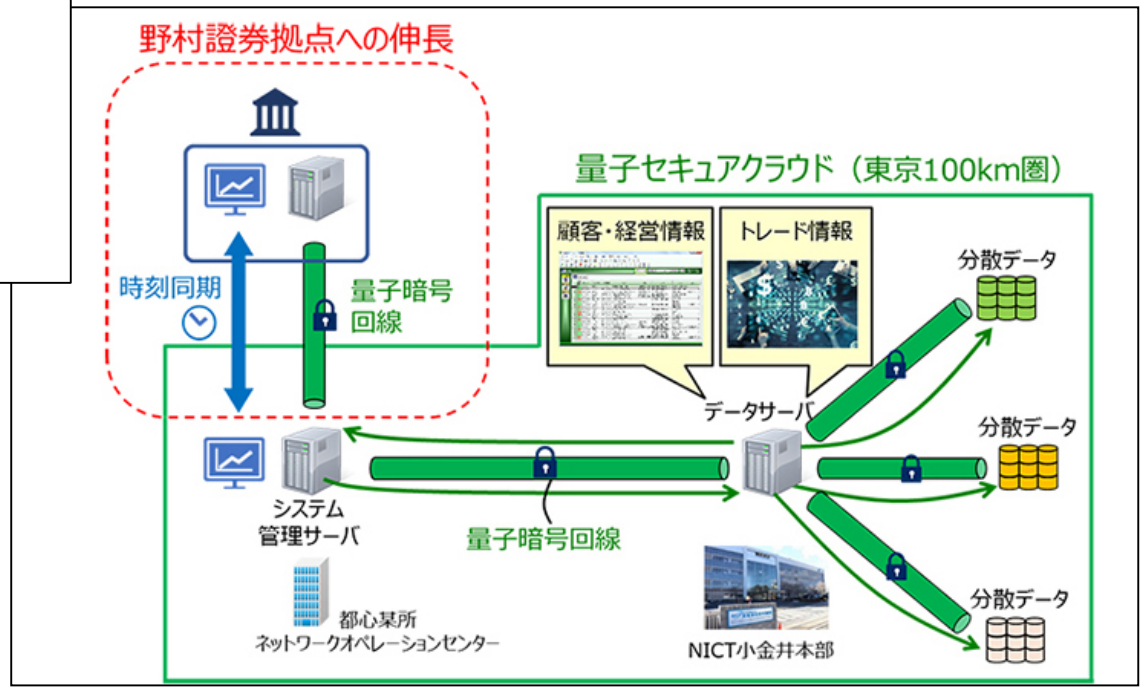


図1　大容量金融取引データの量子暗号による高秘匿通信・低遅延伝送の検証実験に成功 | NOMURA (nomuraholdings.com)
図2　金融分野のサイバーセキュリティ強化に向けた量子暗号技術活用の共同検証を開始 | NOMURA (nomuraholdings.com)

4.金融領域におけるユースケース

他国でも金融領域における実証事例は複数存在、技術検証が進んでいる。
しかし活用領域については各種暗号の特性や情報の性質を踏まえた検討が必要。

既存システムに関わる各種事例

プライバシー保護深層学習技術を活用した不正送金検知の実証実験において金融機関5行との連携を開始

https://www.nict.go.jp/press/2020/05/19-1.html

凸版印刷とNICT、世界初、米国政府機関選定の
耐量子計算機暗号をICカードシステムに実装する技術を確立

https://www.toppan.co.jp/news/2022/10/newsrelease221024_1.html

海外大手金融機関の本社とバックオフィス拠点間の通信セキュリティに応用

https://www.global.toshiba/jp/products-solutions/security-ict/qkd/cases/case2.html

Private asset and wealth management company（スイス）でQKDを利用し、本社と災害復旧センターにて通信した事例

次世代決済インフラにおけるユースケース

海外金融機関では、QKDを利用したブロックチェーンシステムを稼働

https://www.jpmorganchase.com/news-stories/jpmc-toshiba-ciena-build-first-quantum-key-distribution-network

既存の暗号資産では量子耐性獲得を見据えた取り組みが始動

<ヴィタリック氏、イーサリアムのロードマップを更新 (coinpost.jp)>

https://coinpost.jp/?p=404648

量子耐性を持つブロックチェーンの開発プロジェクトも存在

QRL: The Quantum Resistant Ledger (theqrl.org)

5.金融領域で得られる示唆

金融機関においてシステム面で考えるべきリスクは多い

● **背景：技術・環境の変化により社会から求められる変化**
デジタライゼーションの加速、他分野との情報連携、ITガバナンス、クラウド化、在宅勤務によるリモートアクセス、システム更改

● **現状の脅威：既存の金融サービスへの攻撃**
外部からのサイバー攻撃、フィッシングサイト、不正な認証による既存オンラインサービスの悪用

● **今後の脅威：量子コンピュータの登場**
従来の暗号方式の危殆化、ハーベスト型攻撃

事例から得られた示唆

- PQCやQKDの時間軸・特性を理解し、利用者（ユーザー）である
  金融機関、金融業界がどの領域での利用・実装について想定・検討をするべきか
- 業界横断で共有するデータもあり、金融業界全体でのセキュリティレベル向上を目指し、管轄官庁、ベンダーを含めて、データ管理の議論、取組の議論をすべきか
- 上記検討、議論の上で産官学で本格的な量子技術の社会実装に向けた動きを加速
  → 人・モノ・資金の質・量投下による取り組み強化

本資料は、ご参考のために野村ホールディングス株式会社が独自に作成したものです。本資料は、新聞その他の情報メディアによる報道、民間調査機関等による各種刊行物、インターネットホームページ、有価証券報告書及びプレスリリース等の情報に基づいて作成しておりますが、野村ホールディングス株式会社はそれらの情報を、独自の検証を行うことなく、そのまま利用しており、その正確性及び完全性に関して責任を負うものではありません。また、本資料のいかなる部分も一切の権利は野村ホールディングス株式会社に属しており、電子的または機械的な方法を問わず、いかなる目的であれ、無断で複製または転送等を行わないようお願い致します。