大和総研
Daiwa Institute of Research

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　ホワイトペーパーの概要

2026年3月31日
株式会社大和総研

目次

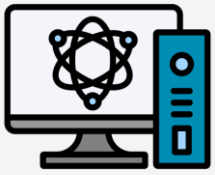
1. 耐量子計算機暗号概念実証の目的と背景
2. 概念実証の概要と体制
3. 概念実証を通じて得られた知見（総括）

1. 耐量子計算機暗号概念実証の目的と背景

- 量子コンピュータの進展により、RSA暗号や楕円曲線暗号等、従来の公開鍵暗号方式の安全性低下が懸念されている。
- 暗号化されたままデータを現在収集し、将来の量子コンピュータで解読する「Harvest Now, Decrypt Later(今収集し、後で解読)」というリスクは、金融機関が扱う顧客情報や取引情報に重大な影響を及ぼす恐れがある。
- 米国では、国家安全保障システムを対象に、2030年までのPQC移行完了を目標としたロードマップが示されている。
- 日本でも、内閣官房・国家サイバー統括室を中心に、PQC移行に関する検討が進められている。
- こうした背景のもと、大和証券グループでは、オンラインサービスを対象に、耐量子計算機暗号(PQC)の技術的・運用的な実現可能性を検証する実証実験を行った。

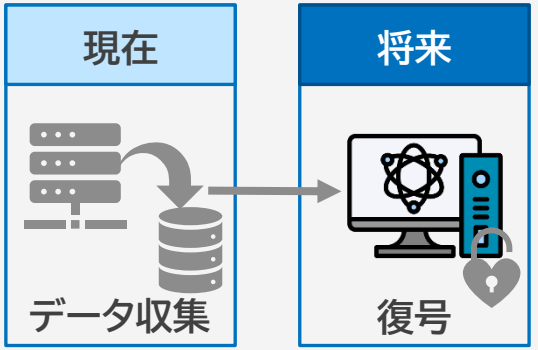
量子コンピュータ出現による従来暗号の危殆化

- インターネットで広く利用されている公開鍵暗号は量子コンピュータによって、効率的に解読されてしまう(Shorのアルゴリズム)



「Harvest Now, Decrypt Later」の脅威

- 暗号化されたままデータを収集し、量子コンピュータの出現後に解読する脅威



金融分野のPQCに対する注目

- 2025年5月、金融庁は銀行等に対してPQCに関する対応に着手する要請を行った
- 日銀やメガバンクを中心にPQC対応に関する議論が行われている

2. 概念実証の概要と体制

- 概念実証は、大和証券の証券業務システムの開発環境を用いて実施
- 大和証券グループ本社、大和証券、大和総研、NEC、F5ネットワークスジャパン合同会社、デジサート・ジャパン合同会社の6社による共同検証
- 2025年9月から2026年3月で検証を実施し、ホワイトペーパーを執筆。

検証概要

インターネット通信における暗号化方式のPQC対応に伴う影響検証

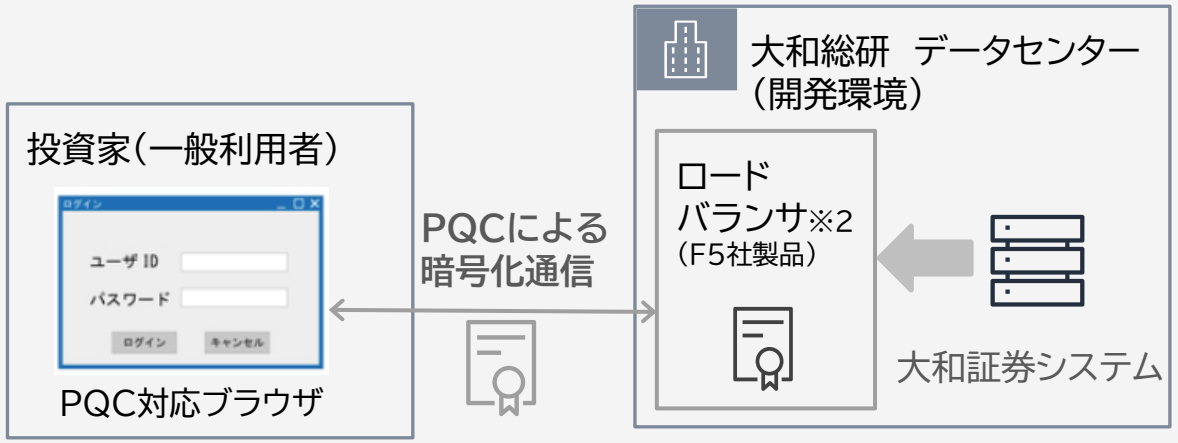
（検証方法）

① PQCの暗号方式に対応したロードバランサを導入

② 証券業務システム（開発環境）での負荷テストを実施。
サーバ負荷、性能、安定性等を検証

（検証期間）

2025年9月～2026年3月



※2：負荷分散装置。処理の負荷分散とインターネット接続時の暗号化を行う

各社の役割

会社名	各社の役割
大和証券 グループ本社 大和証券	• PQC導入の方針策定 • オンラインサービスへの適用検討 • 検証活動案件の組成 • ユーザーの立場での全体企画支援
大和総研	• 検証環境の整備 • 検証シナリオの作成 • 検証及び評価の実施 • ホワイトペーパーの執筆
NEC	• シナリオのレビュー • ホワイトペーパーのレビュー、及び同社見解を記載
F5 ネットワーク ス	• ロードバランサの提供 • PQC対応版のファームウェアの提供
デジサート	• デジタル署名に関する標準化動向の情報を提供

3. 概念実証を通じて得られた知見（総括）

- 本実証実験では、PQC移行の技術的影響（処理・通信）を評価した。その結果、PQCの鍵交換（KEM）は処理時間の増加が小さく、検証を行った**大和証券システムでは通信影響は軽微であり、移行・実運用における影響はない**ことが分かった。
- ただし、デジタル署名・認証など一部標準化途上の技術があり、**システム更改時期を踏まえた移行計画の策定が必要。**
- 必要に応じて、暗号移行チームを組成し、**大和証券グループ全体として計画的な移行推進を検討するべき。**

①実証結果

鍵交換のPQC移行は大和証券システムでは影響なし

■鍵交換（KEM）
暗号に関する処理時間の増加はごくわずかである。
大和証券システムにおいては影響なし。

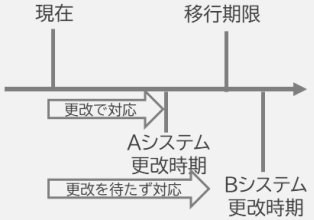
■デジタル署名（DSA）
まだ標準化がされておらず、システム面での評価は難しい。
基礎検証でKEMと同様に鍵サイズ増加の影響を確認しているため、DSAでも署名サイズ増加自体や通信への影響は確認すべき。

②標準化の動向

標準化動向とシステム更改時期を見定める必要あり

署名や認証等のまだ標準化されていない領域に関しては標準化を待つ必要がある。

標準化動向や移行期限のガイダンスを確認し、システムの更改のタイミングに合わせるか、更改を待たずに移行するか見定める必要あり。



③PQC移行の進め方

暗号移行のチーム組成と暗号台帳作成の推進

実証実験では、1つのシステムで検証を行ったが、1つのシステムでもTLS以外にも様々な箇所で暗号が利用されていることや、各箇所ごとに標準化の状況が異なるなど、考慮すべき観点が複数あることが分かった。

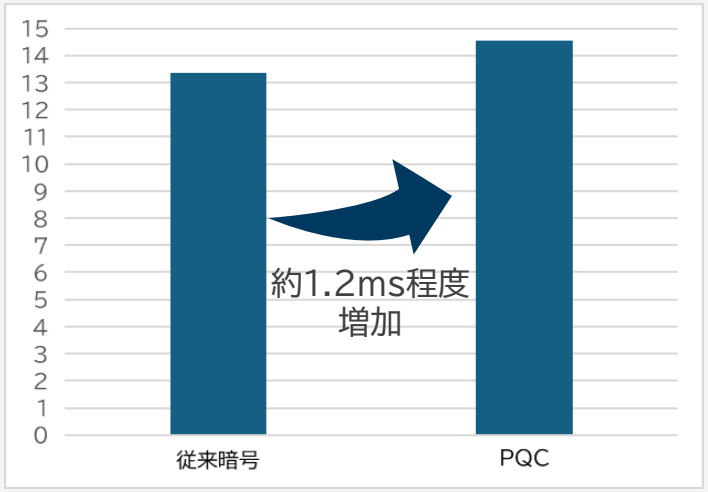
システム全体を俯瞰して暗号台帳の整理を行う必要があり、グループ横断し、暗号移行に関するチームを作り、システムの調査と暗号台帳（インベントリ）の作成を行い、移行準備を行うべき。

①実証結果

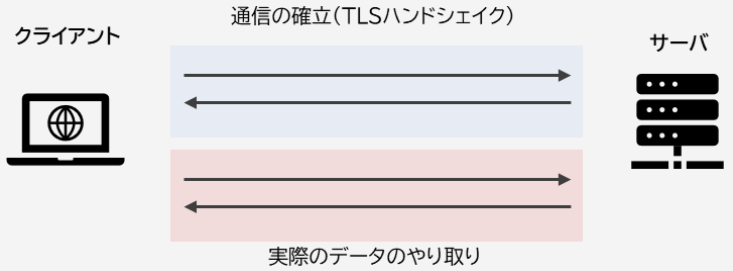
- 概念実証の結果、インターネットの暗号化通信において、PQC（ML-KEM）を用いた鍵交換は、暗号計算時間の増加は極めて短く、通信の確立（TLSハンドシェイク）全体に与える処理性能への影響は軽微であることが確認された。
- 一方、PQCの鍵サイズの大きさによってクライアント、サーバ共に通信量が増え、パケット数が増加する。そのため、無線通信・回線帯域が限られる環境では通信に関する影響は、生じ得る可能性があり、導入にあたっては事前の評価が必要。**回線帯域が確保されている大和証券システムにおいては影響なしと判断。**

従来暗号とPQC　処理時間の比較

- 従来暗号とPQCを使った通信の確立の時間を比較したところ、平均1.2ミリ秒程度通信時間が増加することが分かった。
- システム全体の処理時間と比べると増加幅は軽微であり、影響はほぼ無いと考えられる。



鍵サイズの増加による通信量、パケット数増加



- PQCでは通信確立の通信量が増加する。結果としてパケット数も増加する。

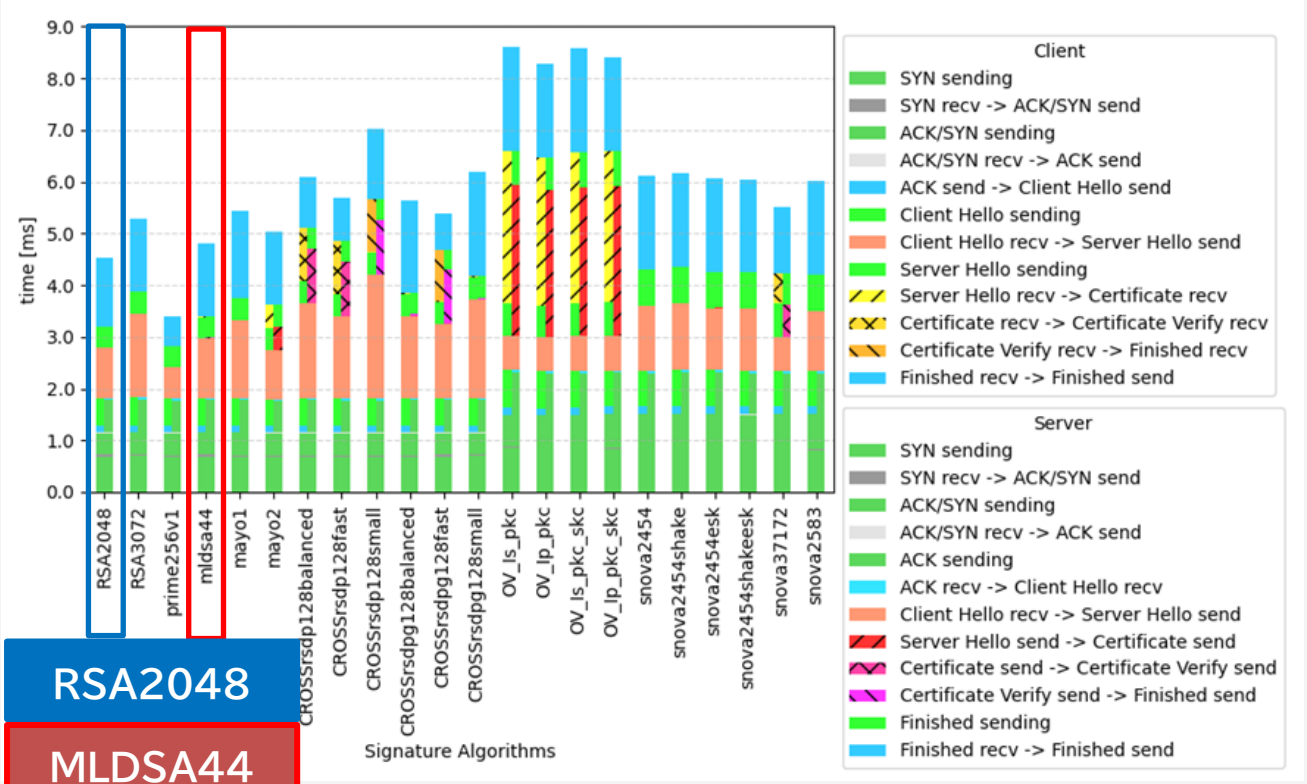
※単位はバイト

	従来暗号	PQC
クライアント	455	1631
サーバ	3661	4749
パケット数	4	6

<参考情報>デジタル署名に関するAWS環境における検証

- デジタル署名については、ロードバランサが未対応のため、大和証券システムを使った実証実験が出来なかった。
  そのため、AWS環境で検証機を利用して基礎検証を実施した。
- 検証の結果、デジタル署名に関しても、NISTが選定しているアルゴリズムML-DSAについては、**従来の暗号アルゴリズムと比較して性能に遜色がない**ことが分かった。

通信速度に関する暗号別グラフ



- 現在主流のRSA暗号である
  RSA2048（2048ビットRSA暗号）
  と比べ、PQCであるML-DSAの通
  信速度はほとんど変わらない

※NISTは、選定した暗号が解読された場合に備え、複数の暗号アルゴリズムを標準化選定している。そのため、本検証においても複数のアルゴリズムの検証を行った。

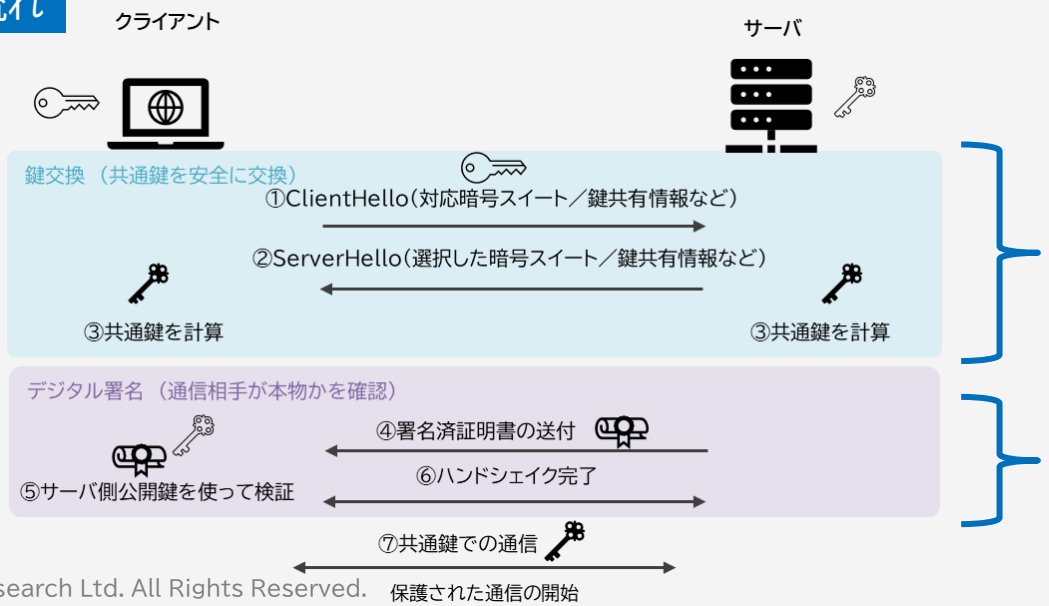
（環境前提）

鍵交換アルゴリズム ： X25519
ルート認証局署名アルゴリズム ： P256

②標準化の動向

- インターネットの暗号通信であるTLSでは、「鍵交換」と「デジタル署名」の2か所で公開鍵暗号が利用されており、PQCの移行においては両者を対象に検討が必要。
- 「鍵交換」については、NIST（米国国立標準技術研究所）による標準化が完了しており、PQCの利用が始まりつつある
- 一方、「デジタル署名」については、インターネット技術の標準化団体（IETF）で標準化が未完了であり、各ベンダーが提供するハードウェアにおいても対応が進んでいない。
- そのため、2026年時点でTLSのPQC移行を行う場合は、標準化済みの「鍵交換」を先行し、「デジタル署名」は標準化動向を注視しつつ、段階的に対応していく必要がある。
- **大和証券グループシステムにおいても、標準化動向や移行期限のガイダンスを確認し、システムの更改のタイミングに合わせるか、先行移行するか見定める必要がある。**

TLS通信の流れ



NISTにより標準化完了
社会実装も開始されている

NISTにより標準化完了
IETFによる標準化が行われていないため、社会実装が開始されていない

③PQC移行の進め方（1/2）

- PQC移行は長期の対応になることが想定されるため、グループ横断で対応する体制（専門チーム）の構築が有効。
- 多数のシステムで暗号移行が必要になることから、**システムの重要度を考慮し、重要度の高いシステムは他のシステムとしては分けて管理するデュアルトラックアプローチ**が考えられる。
- PQCは量子コンピュータで効率的に解読できないことを前提とする一方、将来的に効率的に解読される手法が発見される可能性がある。そのため別の暗号への移行を行いやすい設計にするクリプト・アジリティの考え方も重要になる。

Step1 体制構築
グループ横断の推進チームの設置し、全体計画の策定、推進を行う

Step2 暗号台帳の作成
どこでどの暗号が使われているか、暗号台帳を作成する

Step3 リスク評価と優先順位付け
影響度、蓋然性、移行困難性、秘密保持期間から移行するべきシステムを評価する

Step4 ロードマップ策定
システムの重要度も考慮したデュアルトラックで移行のロードマップを作成する

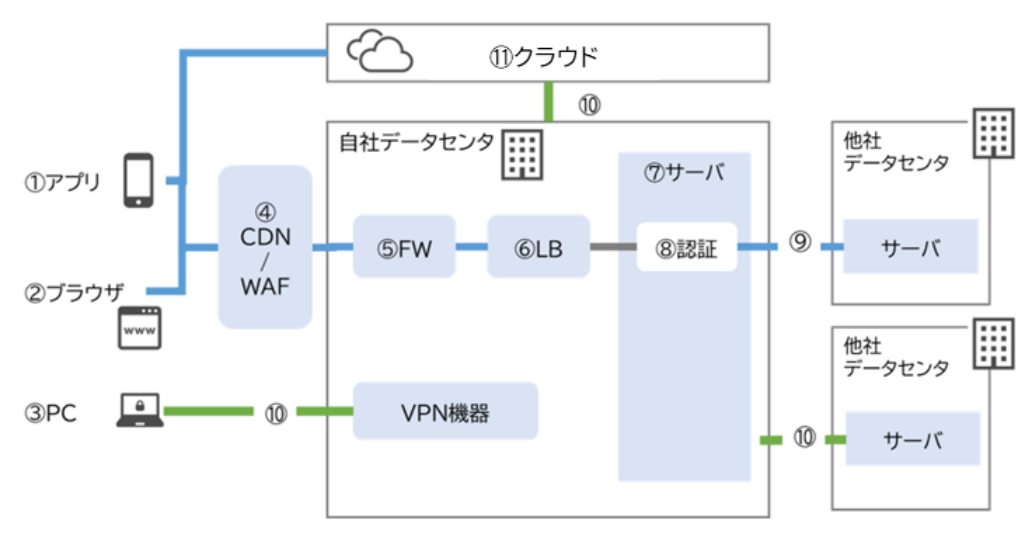
Step5 移行方法の検討
将来の暗号変更も考慮し、クリプト・アジリティを確保した移行方法を検討する

Step6 影響評価
移行前に影響を及ぼす可能性を認識し、移行後に影響確認とチューニングを行う

③PQC移行の進め方（2/2）

- 暗号台帳の作成の際に、以下のようなシステム概念図を利用して調査する方法が考えられる。
- スマホアプリ、サーバサイドアプリで利用している**認証（パスキー、SAML、OIDC、OAuth等）でも対応が必要**となる
  ※現在インターネット技術の標準化団体であるIETF等で規格を策定中のため状況の確認が必要となる

暗号利用箇所の整理



凡例
- 外部インターネット通信
- 内部通信（非暗号化）
- VPN通信

暗号利用箇所	対応要否
①アプリ	スマホアプリでパスキーを利用している場合、PQC対応要
②ブラウザ	主要ブラウザは対応済のため、原則対応不要
③PC	VPN接続を利用するPCがある場合、PQC対応要
④CDN/WAF	TLS終端場所に応じて、PQC対応を要する箇所が変わる。 ※左図はLBでTLS終端している場合。
⑤FW	
⑥LB	
⑦サーバ	
⑧認証	SAML、OpenIDConnect、OAuth、クライアント認証等について、PQC対応要
⑨API接続	サーバ間のAPI接続について、⑧と併せてPQC対応が必要
⑩VPN接続	接続箇所がある場合PQC対応要
⑪クラウド	クラウド内のCDN、FW、LBなど、TLS通信を行う箇所の洗い出し、対応要。マネージドサービスの場合クラウドベンダーのサービス提供待ち。