量子計算機による暗号鍵解読にも強い耐量子セキュリティ技術

Cryptographic Technologies to Prevent Deciphering Cryptographic Key Even with Advent of Quantum Computers

米村　智子 YONEMURA Tomoko　　土井　一右 DOI Kazuaki　　村井　信哉 MURAI Shinya

量子計算機の出現により，公開鍵暗号が解読される懸念がある。そこで，量子計算機にも強いPQC（耐量子計算機暗号）について，幾つかの標準方式が決定され，海外ではそれらへの移行勧告が出るなど，量子暗号通信を含めた耐量子セキュリティ技術の普及拡大が世界的に進んでいる。

東芝グループは，量子暗号通信にHSM（ハードウェアセキュリティモジュール）及び総合監視機構を導入して暗号鍵の保護と異常検知を行うQKD（量子鍵配送）用鍵管理システムとリスク分析に基づくPQC認証技術を開発した。量子暗号通信とPQCの組み合わせや使い分けで，量子計算機でも破れないセキュアネットワークが実現できる。

Decryption of public key cryptography has become a critical issue with the advent of quantum computers. The dissemination of cryptographic technologies, including quantum cryptographic communications, has led to growing demand for the development of post-quantum cryptography (PQC) technologies that are secure against quantum computers. Efforts to standardize PQC algorithms are being actively promoted worldwide, leading to recommendations for transitioning to specified PQC standards in a number of countries.

The Toshiba Group has developed the following technologies: (1) a key management system for quantum key distribution (QKD), which can protect cryptographic keys and detect abnormalities through the introduction of a hardware security module (HSM) and a comprehensive monitoring system into quantum cryptographic communications, and (2) a PQC authentication technology based on risk analyses. These technologies make it possible to construct a highly secure network by appropriately using and combining QKD and PQC even with the advent of quantum computers.

1. まえがき

情報通信システムでは，その安全性を守るために公開鍵暗号であるRSA（Rivest-Shamir-Adleman）暗号と楕円（だえん）曲線暗号が広く利用されている。これらの公開鍵暗号は，計算困難な数学的問題（素因数分解問題と離散対数問題）に基づき構成され，現在までに，従来の計算機では効率的な解法が発見されていないが，量子計算機ではショアのアルゴリズムでこれらの問題を効率的に解ける。現在用いられているRSA暗号と楕円曲線暗号の鍵サイズに対応する素因数分解問題と離散対数問題を解くショアのアルゴリズムを実行できる規模の量子計算機（以下，暗号解読量子計算機と呼ぶ）が登場すると，RSA暗号と楕円曲線暗号は解読され情報通信システムの安全性は守られなくなり，量子計算機は，情報通信システムの安全性にとって脅威となり得る。このような危機感から，NIST（米国国立標準技術研究所）はRSA暗号と楕円曲線暗号を2035年以降許可しないとする内部報告書の初期公開草稿を発表している[(1)]。一方で，実現が発表されている量子計算機では，現在，CRYPTREC（Cryptography Research and Evaluation Committees）の暗号強度要件（アルゴリズム及び鍵長選択）に関する設定基準で推奨される鍵サイズのRSA暗号と楕円曲線暗号の解読ができていない。情報通信システムの安全性が直ちに失われる状況ではないが，暗号解読量子計算機の登場に備えて準備に着手することが重要である。

暗号解読量子計算機に対抗して，海外では従来の計算機で動作するPQCへの移行勧告が出ている。NISTは2024年8月にPQC標準方式としてML-KEM（モジュール格子ベース鍵カプセル化メカニズム）やML-DSA（モジュール格子ベースデジタル署名）のFIPS（米国連邦情報処理標準）を発行した[(2), (3)]。NSA（米国国家安全保障局）はPQC移行のために2022年にCNSA 2.0（商用国家安全保障アルゴリズムスイート2.0）を発行した。CNSA 2.0では国家安全保障システムで用いる汎用的な公開鍵暗号としてML-KEMとML-DSAを承認し，ソフトウェア及びファームウェアに対するデジタル署名では2030年に，制約のある機器や大規模な公開鍵基盤システムでも2033年にPQCへ移行完了することを勧告している[(4)]。欧州委員会は，2024年4月に重要インフラなどのPQC移行を加盟国に勧告し，2026年までの移行計画策定を求めた[(5)]。我が国では，金融庁のwebサイトでPQC対応に関する報告書が公開されていて，暗号解読量子計算機の脅威に加え，PQC対応未了の企業などとの

米・欧による取引規制が懸念されている[6]。取引規制の影響を小さくするため，海外におけるPQC移行勧告は我が国にも波及すると予想される。

標準化については，NISTによるPQC標準の発行を受けてIETF（インターネット技術標準化委員会）でML-KEMやML-DSAを用いた応用プロトコル，例えば，TLS（Transport Layer Security），SSH（Secure Shell），ITU-T（国際電気通信連合-電気通信標準化部門）の規格X.509での公開鍵基盤における公開鍵証明書，の標準化に向けた議論が進んでいる。PQC応用プロトコルの議論を受けて，ICカードに関するISO/IEC JTC1/SC17（国際標準化機構／国際電気標準会議 第1合同技術委員会／第17分科委員会）や電力システムに関するIEC TF57（国際電気標準会議 第57技術委員会）でも，PQC移行の議論を開始している。

PQCとは独立して開発され，暗号解読量子計算機に対抗する技術に量子暗号通信がある。量子暗号通信の基盤となる技術は，1984年に二人の物理学者によって発表されたQKDのプロトコルでBB84と呼ばれる。これ以降，プロトコル・理論・実装に関する研究開発が進み，量子計算機を含むあらゆる解読・盗聴が不可能な暗号通信技術となり，実用性の高い量子技術として注目されている。近年，欧州，米国，中国，日本でもそのネットワーク実証が行われており，ETSI（欧州電気通信標準化機構），ITU-T，ISO/IECといった国際標準化団体における標準化を巡る議論も活発である。このような状況の中，東芝グループは，2020年に量子暗号通信システム事業の開始を発表した。2021年には東芝グループを含む民間企業11社で“量子技術による新産業創出協議会”を発足し，量子暗号通信を含む量子技術の産業化を加速・リードしている。

量子暗号通信とPQCを耐量子セキュリティ技術と呼ぶ。ここでは，東芝グループの耐量子セキュリティ技術として，量子暗号通信にHSMを適用したQKD用鍵管理システム，及びQKDネットワーク（QKDN）へのリスク分析に基づくPQC認証の導入例と通信プロトコルのPQC先行対応について述べる。

2. QKD用鍵管理システムの運用コスト削減検討

各鍵管理拠点は，トラステッドノードとして，物理的及び情報セキュリティの観点から保護されており，現状でも安全に運用できるが，拠点内への侵入監視などの運用負荷を削減するため，以下の2点の機能強化が考えられる。

1点目は，別の暗号鍵（以下，アプリ鍵と呼ぶ）の生成・暗号・管理処理の保護（アプリ鍵保護），2点目は，異常検知機能の高度化である。アプリ鍵保護により，攻撃者（侵入者）に対してアプリ鍵を完全に秘匿でき，アプリ鍵保護に対する異常検知の導入により，想定外の事象の発生を即座に把握し，対策を講じられる。

今回，アプリ鍵保護には情報セキュリティ機器の一種であるHSMの導入，異常検知には総合監視機構の導入を実施した。

HSMの導入では，鍵管理システムの各拠点にHSMを導入し，アプリ鍵生成，アプリ鍵共有処理の際の暗号化処理，アプリ鍵DB（データベース）へのアプリ鍵保管前に実施される暗号化処理をHSM内で実施する構成とした（**図1**）。これにより，非暗号化状態のアプリ鍵がKM（鍵管理）装置内（HSM外）に出現しなくなり，HSM内で保護されるため，アプリ鍵を秘匿できる。また，暗号モジュールの連邦情報処理規格（FIPS 140-3 レベル3）に基づくHSMは，HSMへの不正利用などの各種攻撃に対する自動検知・対処機能を持つため，HSMを確認することで，アプリ鍵保護機能への攻撃の存在を確認できる。

HSM付き鍵管理システムの動作検証について述べる。東芝グループは，HSM導入前の2017年には10 Mビット/sを超える鍵生成速度を達成していた[7]。一方，HSMの導入により，セキュリティ強化は達成できるものの，アプリ鍵生成速度の低下が懸念された。そこで，アプリ鍵の各処理に並列化などの各種検討を基にした対応を行い，アプリ鍵のセキュリティ強化を達成しつつ，隣接拠点間で約12 Mビット/s

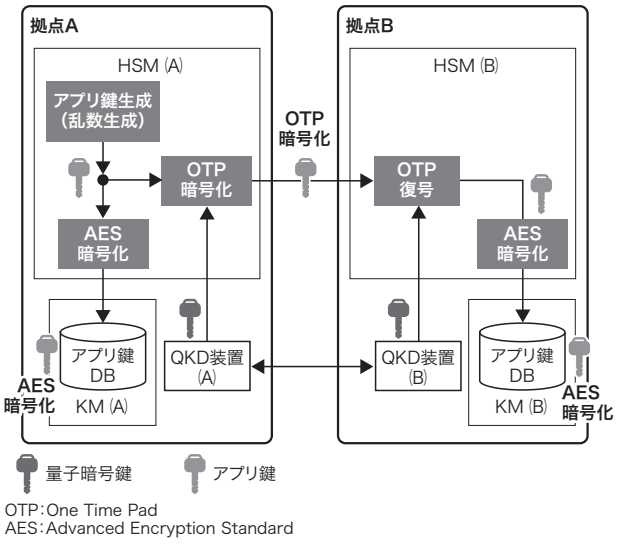

図1. HSM導入によるアプリ鍵の保護

鍵管理システムにHSMを導入することで，非暗号化状態のアプリ鍵をHSM内で保護できるため，アプリ鍵を秘匿できる。

Protection of application keys through introduction of HSM

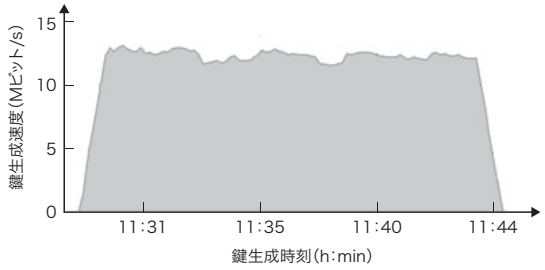

図2. 隣接拠点間でのアプリ鍵の生成速度

HSMの導入に加え，アプリ鍵の各処理の並列化などを行うことで，アプリ鍵のセキュリティ強化を達成しながら，隣接拠点間で約12 Mビット/sの鍵生成速度を達成した。

Application key generation speed between adjacent sites

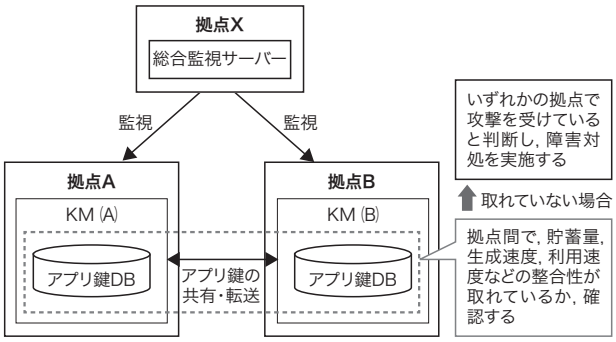

図3. 総合監視機構の構成

拠点内に総合監視サーバーを設け，拠点間でアプリ鍵の統計データの整合性を確認し，整合性が取れていない場合，障害対処を実施する。

Configuration of comprehensive monitoring system

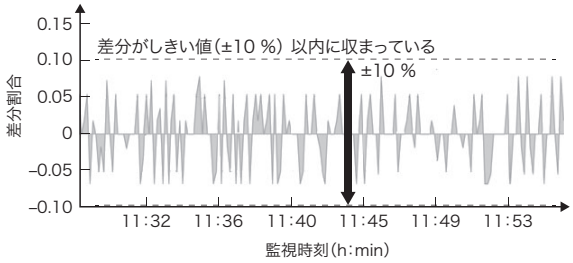

図4. アプリ鍵利用速度の差（正常動作時）

拠点間のアプリ鍵利用速度の差を確認し，正常動作時は，しきい値以内に収まっていることを確認した。

Differences in application key generation speed between adjacent sites during normal operation

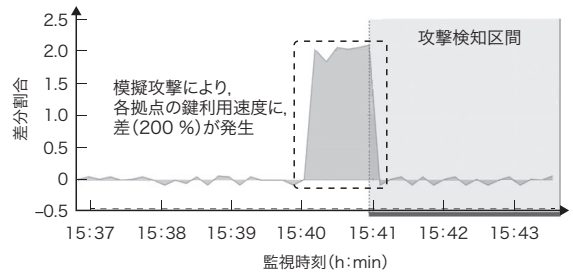

図5. アプリ鍵利用速度の差（攻撃実施時）

模擬攻撃を実施したとき，鍵利用速度の差がしきい値以内に収まらず，攻撃を受けたことを検知できた。

Differences in application key generation speed between adjacent sites at time of cyberattack

の鍵生成速度を達成した（**図2**）。

総合監視機構の導入では，鍵管理拠点とは別に総合監視拠点を設け，拠点内に総合監視サーバーを設けた。

HSMへの監視に関しては，HSMへの不正アクセスなど，HSMに対する不正操作の発生有無を監視し，アプリ鍵DBへの監視に関しては，DB内に保管されているアプリ鍵の窃取など，DBへの攻撃が発生していないかを監視する。

アプリ鍵DBへの監視に関しては，本来，アプリ鍵の共有元拠点と共有先拠点との間で整合しているはずの，アプリ鍵の貯蓄量，生成速度，利用速度などが拠点間で整合性が取れている（同期が取れている）か，鍵共有トラフィック量がアプリ鍵の生成速度と同期が取れているかなど，鍵管理システム内の統計データの整合性を確認する。総合監視サーバーが，統計データの整合性が取れていないと判断した場合，アプリ鍵の消去などの各種対応策を実施する（**図3**）。

総合監視機構の検証について述べる。今回，攻撃される可能性が最も高いと思われるアプリ鍵DBに注目し，アプリ鍵DBへの鍵窃取攻撃が検知でき，同DBへの監視機能が動作するかを検証した。

正常動作時（攻撃未実施時）は，アプリ鍵の利用速度（アプリ鍵のアプリレイヤーへの提供速度）の整合性が取れている（利用速度の差がしきい値未満になっている）ことを確認し（**図4**），鍵窃取攻撃を実施したときは，鍵利用速度の整合性が取れず，攻撃検知できることを確認した（**図5**）。これにより，正常動作時と攻撃検知時の両方の場合において，想定どおりの動作をしていることを確認した。

3. QKDNへのPQC認証の導入例

脅威の重大度と可能性を考慮したリスク分析に基づくPQC認証の，QKDNへの導入例について述べる。QKDN構築に当たっては，量子レイヤーを除く通信には専用線ではない通常ネットワークを用いることが想定される。そこで，この想定におけるリスク分析を実施する。ここでは，リスクが運用の中断につながるような，トラステッドノードと運用拠点の間について，PQC認証の導入例を示す。一般に，リスク

分析は，以下に示す手順で行われる。

・登場人物，情報資産，システム構成を基に脅威を特定
・脅威が起こった際の被害の重大度を特定
・脅威の発生可能性を特定
・被害の重大度と発生可能性に応じた対策の決定

まず，ITU-T X.1710「QKDNのセキュリティフレームワーク」及びITU-T X.1712「QKDNの鍵管理に関するセキュリティ要件と対策」で特定されるセキュリティ脅威について，X.1710の記載をベースに被害の重大度を特定し，X.1710及びX.1712に記載のない発生可能性を特定する。次に，被害の重大度と発生可能性に応じた対策としてPQCの適用箇所を検討し，X.1712に記載される対策との対応を整理する。

情報資産は，鍵データ，メタデータ，制御，及び管理情報である。セキュリティ脅威には，成り済まし，盗聴，削除，又は破損がある。X.1710で特定される被害の重大度を**表1**に示す。

セキュリティ脅威について被害の重大度を特定する。鍵データの盗聴，KM装置の成り済まし，は高レベルである。メタデータの盗聴，メタデータ，制御，及び管理情報の削除又は破損，KM装置に接続するQKDN制御装置及びQKDN管理装置の成り済まし，は中レベルである。制御及び管理情報の盗聴は低レベルである。メタデータに関する脅威は中レベルと判定した。

表1．セキュリティ脅威による被害の重大度

Severity of damages caused by cyberattacks

被害の重大度	説　明
高レベル	脅威は，鍵データの機密性の破壊につながる可能性がある。
中レベル	KM層，QKDN制御層，及びQKDN管理層の制御及び運用情報に対する脅威である。脅威が発生した場合，QKDNの安全で信頼性のある運用は達成できない。
低レベル	QKDNの制御及び管理情報の盗聴であり，認識されない形で行われる可能性がある。鍵データの漏えいや量子鍵配送ネットワークの運用の中断は発生しないが，攻撃者にとって有益である可能性がある。

表2．被害の重大度と発生可能性に応じた対策

Countermeasures according to severity of damages and likelihood of security threats

重大度	可能性		
	高 （拠点間，拠点外）	中 （拠点内）	低 （装置内）
高レベル （鍵データの漏えい）	情報理論的 安全な対策	計算量的 安全な対策	計算量的 安全な対策
中レベル （運用の中断）	計算量的 安全な対策	計算量的 安全な対策	—
低レベル （制御及び管理情報の漏えい）	計算量的 安全な対策	—	—

セキュリティ脅威の発生可能性を特定する。外部攻撃者からの攻撃が可能な，拠点間（KM装置間の接続），拠点外（QKDN制御装置及びQKDN管理装置との接続）における発生可能性は高である。内部攻撃者による攻撃が可能な拠点内（同一拠点におけるKM装置とQKD装置の接続，KM装置とアプリ装置の接続）における発生可能性は中である。内部攻撃者による高度な攻撃となる装置内における発生可能性は低である。

被害の重大度と発生可能性に応じた対策を**表2**に示す。符号「–」は，セキュリティ脅威がX.1710及びX.1712に登場しないことを表す。表2はX.1712に記載される対策の具体化となっており矛盾しない。計算量的安全な対策のうち公開鍵暗号で実現する箇所をPQCに移行する。PQC適用箇所には，拠点内の認証と鍵交換，拠点間と拠点外のメタデータと制御及び管理情報に関する認証と鍵交換，がある。拠点外の制御及び管理情報に関する認証と鍵交換の具体例としては，QKDN管理装置とKM装置の間をSSH接続する場合が考えられる。

SSH接続のPQC先行対応として，楕円曲線暗号とML-KEM・ML-DSAの両方を用いるハイブリッド方式SSHプロトコルのドラフト[8]をSSHクライアントのOSS（オープンソースソフトウェア）であるPuTTYに実装した。高速なネットワークで，ハイブリッド方式の所要時間は楕円曲線暗号に遜色なく，PQC導入は量子暗号通信システムに性能面の影響を与えないことが分かった。

4. あとがき

情報通信システム，特に，量子計算機の脅威に対抗する重要インフラへの対策は，準備期間を考えると今から検討に着手する必要がある。耐量子セキュリティ技術の導入は，高度機密ネットワーク，安全保障システム，重要インフラ，金融分野から始まると考えられる。東芝グループは，高度機密ネットワークにおける量子暗号通信システムの運用コスト削減及びPQC認証導入だけでなく，通常ネットワークのPQC移行についても進めていく。

この研究の一部は，内閣府総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「先進的量子技術基盤の社会課題への応用促進」（管理法人：国立研究開発法人量子科学技術研究開発機構）によって実施された。また，総務省のICT（情報通信技術）重点技術の研究開発プロジェクト「グローバル量子暗号通信網構築のための研究開発（JPMI00316）」によって実施した成果を含んでいる。

文　献

(1) Moody, D. et al. Transition to Post-Quantum Cryptography Standards. NIST, 2024, NIST IR 8547, 26p.
(2) FIPS 203：2024. Module-Lattice-Based Key-Encapsulation Mechanism Standard. NIST.
(3) FIPS 204：2024. Module-Lattice-Based Digital Signature Standard. NIST.
(4) NSA. Commercial National Security Algorithm Suite 2.0. 2022.
(5) European Commission. COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. C(2024) 2393 final, 2024, 5p.
(6) 預金取扱金融機関の耐量子計算機暗号への対応に関する検討会．預金取扱金融機関の耐量子計算機暗号への対応に関する検討会報告書．金融庁，2024，59p．<https://www.fsa.go.jp/singi/pqc/houkokusyo.pdf>,（参照 2025-04-01）.
(7) 東芝．“量子暗号通信で世界初の10Mbpsを超える鍵配信速度を達成”．ニュースリリース．<https://www.global.toshiba/jp/news/corporate/2017/09/pr1501.html>,（参照 2025-04-01）.
(8) Kampanakis, P. et al. "PQ/T Hybrid Key Exchange in SSH". IETF. <https://www.ietf.org/archive/id/draft-kampanakis-curdle-ssh-pq-ke-05.html#>, (accessed 2025-04-01).

米村　智子　YONEMURA Tomoko
総合研究所 AIデジタルR&Dセンター
セキュリティ基盤研究部
IACR（国際暗号学会）会員
Security Research Dept.

土井　一右　DOI Kazuaki
総合研究所 AIデジタルR&Dセンター
コンピュータ＆ネットワークシステム研究部
Computer & Network System R&D Dept.

村井　信哉　MURAI Shinya
東芝デジタルソリューションズ（株）
ICTソリューション事業部 QKD事業推進室
電子情報通信学会・情報処理学会会員
Toshiba Digital Solutions Corp.