量子コンピュータ時代を見据えたセキュア光トランスポートネットワーク技術

村上 啓造[†1]　谷口 篤[†2]
工藤 史堯[†1]　知加良 盛[†1]
清村 優太郎[†1]　向山 明夫[†1]
飯島 悠介[†1]　持田 康弘[†2]
佐成 晏之[†2]　木村 直宏[†2]

NTT社会情報研究所[†1]
NTT未来ねっと研究所[†2]

NTT技術ジャーナル2021年11月号にて，量子コンピュータ時代でも安全に光トランスポートを行う技術として，セキュア光トランスポートネットワークを紹介しました．本稿では，今後既存の暗号技術から耐量子セキュリティを持った暗号技術へ移行する際に重要であり，量子コンピュータ時代にも考慮する必要がある，クリプトアジリティ，マルチファクタセキュリティといった考え方を解説し，これらの考え方をセキュア光トランスポートネットワークに取り入れるための取り組みについて紹介します．

背　景

ネットワーク上を流れるデータは映像データや音声データなど大容量化しています．また，金融や遠隔医療などではこれまで以上に用いる通信の遅延が少ないことが求められています．また，サービスを持続するうえで消費電力を低減することも重要です．

NTTが研究開発を進めるIOWN（Innovative Optical and Wireless Network）APN（オールフォトニクス・ネットワーク）は，低消費電力，大容量・高品質，低遅延の3点を訴求するサービスをめざしています[(1)]．これに加えて金融や遠隔医療では，システムが攻撃を受けた場合の経済的な損失の大きさや人命への影響から，高度なセキュリティも求められます．これらの特徴はデータ流通の観点からも重要です．

2030年代には実用化されるといわれている量子コンピュータにより，交通渋滞の解消・金融データのリスク分析・新薬開発等への導入が期待される一方で，RSA暗号や楕円曲線暗号などの既存暗号が解読されることが懸念されています．

NTT社会情報研究所とNTT未来ねっと研究所では，IOWN APNに安全性をプラスする取り組みとして，光伝送装置間で耐量子計算機暗号（PQC：Post-Quantum Cryptography）や量子鍵配送（QKD：Quantum Key Distribution）を用いて共通鍵を共有し，その鍵で通信を暗号化することで，量子コンピュータ時代でも安全なセキュア光トランスポートネットワーク技術（セキュア光トランスポート）の研究開発を行ってきました[(2)]（**図1**）．データ流通の観点から，伝送路や蓄積されたデータを暗号化するだけでなくエンド・ツー・エンドのセキュリティが求められますが，本技術は特に伝送路を対象としたものです．

現在は，量子コンピュータ時代のIOWNに求められる耐量子セキュリティ*1のあるべき姿についてIOWN

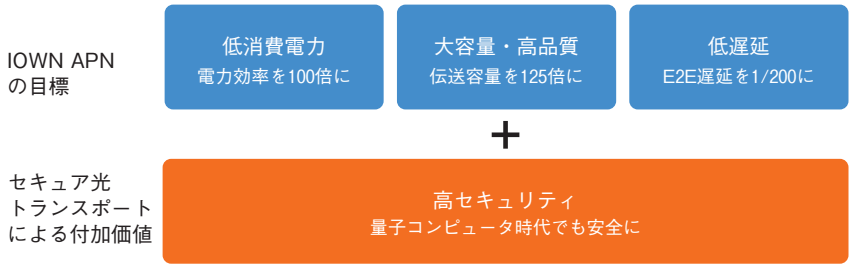


図1　セキュア光トランスポートの特徴

*1　耐量子セキュリティ：量子コンピュータによる攻撃への耐性を備えたセキュリティレベル．

Global Forum（IOWN GF）にて検討を行っており，その実現方法の1つとしてセキュア光トランスポートの新規機能であるElastic Key Control技術および，暗号処理のディスアグリゲーション技術を提案しました．その活動と技術について紹介します．

課　題

従来のセキュア光トランスポートの鍵共有[(2)]は，任意のPQCまたはQKDからいずれか1つを用途に応じて選択することで，量子コンピュータの発展により従来の公開鍵暗号方式が破られても安全な情報通信を保証するものでした．

PQCは量子コンピュータでも効率的に解くことができないとされている問題を安全性の根拠とした暗号方式です．PQCは既存暗号に比べて歴史が浅く，研究段階から実用化に向けて進みつつある段階です．現在，米国国立標準技術研究所（NIST）によりPQCによる鍵交換と署名方式の標準化が開始されており，今後社会実装され普及していくことが見込まれます．一方で，PQCの研究は進展段階であり，新たな攻撃手法が見つかり，ある日突然危殆化*2する可能性もゼロではありません．実際に，NISTのPQCの選定コンペのRound4で標準化が検討されていた鍵共有方式 SIKEは，コンペ中の2022年7月現在のコンピュータでも1時間あまりで解読できる攻撃手法が見つかりました[(3)]．

そのため，量子コンピュータ時代を見据えると以下のようなことに対応する必要があります．

- 1つの暗号アルゴリズムが危殆化しても即座に通信が脅威にさらされないこと
- 危殆化した暗号アルゴリズムから他のアルゴリズムへの切り替え，または，新たな暗号アルゴリズム採用を柔軟に行えること

IOWN GFでは，このような要件への対応をIOWN Securityとして議論を行っています．本稿では，近年概念が提唱され始めている，マルチファクタセキュリティ，クリプトアジリティ，ハイブリッド方式などを対象にしています．

IOWN GFでの活動について

■IOWN security（IOWNsec）

IOWN GFでは，IOWNを実現する新しい通信・計算基盤のアーキテクチャやユースケースの議論を行っています．IOWN GF 設立から2年以上経ち，IOWNを実現する技術や活用ユースケースが徐々に具現化し，最近ではIOWN 時代のセキュリティに関する議論が始まっています．

IOWNsecでは，量子コンピュータ時代を見越して，IOWNユースケースのデータ通信をエンド・ツー・エンドで耐量子セキュリティを保つためのアーキテクチャを規定し，2023年1月に，技術文書として「Technology outlook of Information Security」文書（IOWNsec文書）をIOWN GFより公開しました．

■マルチファクタセキュリティ

IOWNsecでは，エンド・ツー・エンドで耐量子セキュリティを持った通信を実現するため，Multi Factor Security（MFS）というコンセプトを掲げています．MFSとは，単一の技術では獲得できないセキュリティレベルを複数の技術を組み合わせることで実現するコンセプトです．例えば，通信の暗号化のための鍵交換において，耐量子セキュリティを実現する技術としてPQCやQKD，Pre shared key（PSK）などが知られています．しかし，いずれの技術もメリットとデメリットがあり，単一の技術で完全なセキュリティを実現することはできません．例えば，QKDは情報理論的安全性*3を有する鍵交換技術ですが，長距離の鍵配送には鍵リレーを行う第三者ネットワークが必要で，内部攻撃のリスクを回避できないといわれています[(4)]．またPQCを活用した鍵交換方式はソフトウェアで実現可能であるため，厳密にエンドポイント間で鍵交換が可能ですが，その安全性は計算量的安全性*4であり，将来的に危殆化する可能性もあります．そこでIOWNsecではMFSによりPQCとQKDやその他のPSKなど複数のセキュリティ方式を組み合わせることで双方のデメリットを補完し，より広範な脅威に対応可能な選択肢をユーザに提供可能なアーキテクチャを規定しました（**図2，3**）．またMFSをより幅

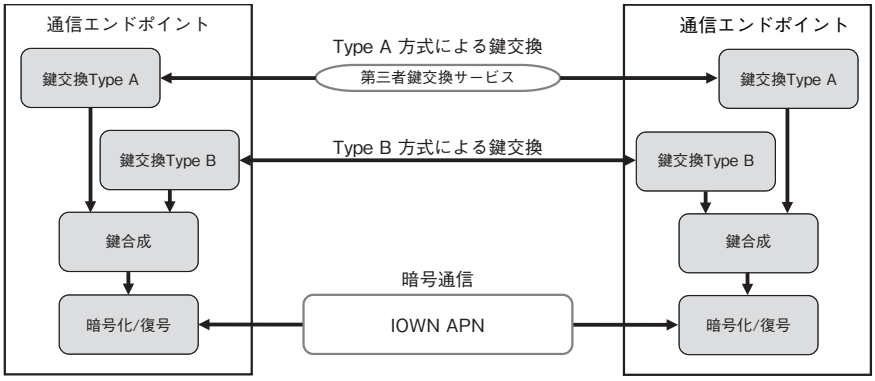
*2　危殆化：特に暗号の危殆化とは，暗号の安全性のレベルが低下した状況．アルゴリズム自体が原因の場合もあれば，実装上の問題が原因の場合もあります．
*3　情報理論的安全性：考え得るもっとも強力な攻撃者，すなわち無限の計算能力を持った攻撃者に対する安全性．
*4　計算量的安全性：暗号解読に必要な計算量が，利用できる計算機の能力に比較して膨大であり，現実的時間では実行不可能であるという仮定に依拠した安全性．

広いユースケースで活用してもらえるよう，実装バリエーションとして，エンド・ツー・エンド通信を行うメインCPU上のアプリケーションとして実装する以外にネットワークインタフェースカードへの実装も検討しています．

関連する外部動向

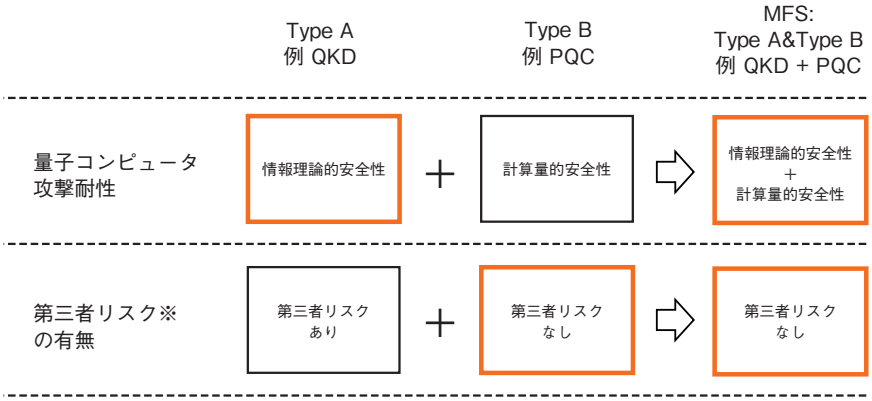
■クリプトアジリティ（Crypto Agility）

NISTにより提唱されている[5],[6]考え方で，直訳すると暗号の機敏性となります．ネットワークやシステムで利用されている暗号方式が危殆化した場合や新たな暗号アルゴリズムが登場した場合などに，利用する暗号方式を素早く切り替えていく概念です．この概念は，既存のネットワークやシステムへの影響を小さく切り替えられること，検証にかかる期間が短く済むことなどをねらいとしており，既存の暗号方式をPQCへ移行する際にも重要となると考えています．



TypeA方式・・・通信エンドポイントから見た第三者サービスを利用した鍵交換方式
TypeB方式・・・通信エンドポイントとなる２者間で実現可能な鍵交換方式

図２　Multi Factor Securityの具体例



※第三者リスク・・・第三者サービスが内包する，内部攻撃などのセキュリティリスク

図３　Multi Factor Securityの鍵交換における効果の例

■ハイブリッド方式

暗号技術の文脈で「ハイブリッド」というと公開鍵暗号と共通鍵暗号を組み合わせて用いる「ハイブリッド暗号方式」のことを指すことが多いですが，本項目での「ハイブリッド方式」とは複数の公開鍵暗号方式で鍵交換や電子署名を実施し，その結果を合成して１つの秘密鍵や署名を生成する方式のことを指します．このハイブリッド方式は，近年，インターネット標準を規定しているフォーラムIETF（Internet Engineering Task Force）等で提案されています[7]．ハイブリッド方式により，「RSA暗号や楕円曲線暗号といった従来の暗号方式（従来暗号）」「PQC」「QKDによる共有鍵をはじめとしたPSK」から複数の方式を選択し，生成結果を合成することで，どれか１つの方式が危殆化したとしても即座にシステム自体が危険にさらされなくなります．ハイブリッド方式を利用することで，PQCへの移行期においては従来暗号の安全性を担保しつつPQCの社会実装を進めることができます．また，PQC移行後も，急激な危殆化を避ける意味で複数PQCをハイブリッド化することは有効です．

提案技術

■Elastic Key Control技術

NTT社会情報研究所はIOWNsecのMFSの考え方の１つの実現方法として，ハイブリッド方式を取り入れたElastic Key Control技術を提案し，開発しました．

従来のセキュア光トランスポート技術は，鍵交換方式として任意のPQC

またはQKDからいずれか1つをシステム要件に応じて選択できる方式でした．それを発展させたものがElastic Key Control技術です．Elastic Key Control技術とは，ユーザニーズ・暗号アルゴリズムの利用状況などに応じて，柔軟に鍵交換に利用する暗号アルゴリズムを切り替えられる方式です（**図4**）．利用できるアルゴリズムは従来暗号，PQC，PSK単独だけでなく，任意の組み合わせのハイブリッド方式も選択可能です．また，鍵交換だけでなく各サーバの認証に用いる署名とその検証についても従来暗号とPQCのハイブリッドで動作することを確認しました．現時点では鍵交換方式としてECDHE，CRYSTALS Kyber，NTRUを，署名方式としてECDSA，CRYSTALS Dilithiumを実装しましたが，ライブラリとして実装されているものであれば選択肢に加えることが可能です．

これにより，例えば，まず従来暗号とPQCを組み合わせて実用化し，PQCの社会的な利用実績を積んだうえで，量子コンピュータ時代を迎えることができます．その後，量子コンピュータ時代には複数のPQCの組み合わせに切り替えることで，双方危殆化しない限り安全な状況を保ちながら，将来登場する暗号アルゴリズムを素早く実装して利用することが可能になります．このようにElastic Key Control技術により，クリプトアジリティを高めることが可能です．

■暗号処理のディスアグリゲーション技術

従来，光伝送装置は，光モジュール等が一体型で提供されていました．近年，光伝送装置の各種機能を分離することで柔軟な構成変更が容易なディスアグリゲーション構成を適用したオープントランスポート光伝送装置が検討されています．しかし，暗号処理モジュール（ハードウェア）はいまだに光伝送装置と一体で提供されており，暗号処理モジュールを制御するライブラリ（ソフトウェア）は光伝送装置のNetwork Operation System（NOS）に依存していました．クリプトアジリティの観点からも新しい暗号アルゴリズムを迅速に適用できる構成が必要になります．また，光伝送の場合，共通鍵を交換する通信が途切れたとしても安定した暗号通信ができることが必要です．

そこで，今回，オープントランスポート光伝送装置上で，受け取った共通鍵の鍵情報共有等下位の暗号処理（MACsec，OTN暗号化等）に依存しない鍵管理を行う鍵管理部，光伝送装置間の通信のセッション鍵を管理するセッション鍵情報共有等下位の暗号

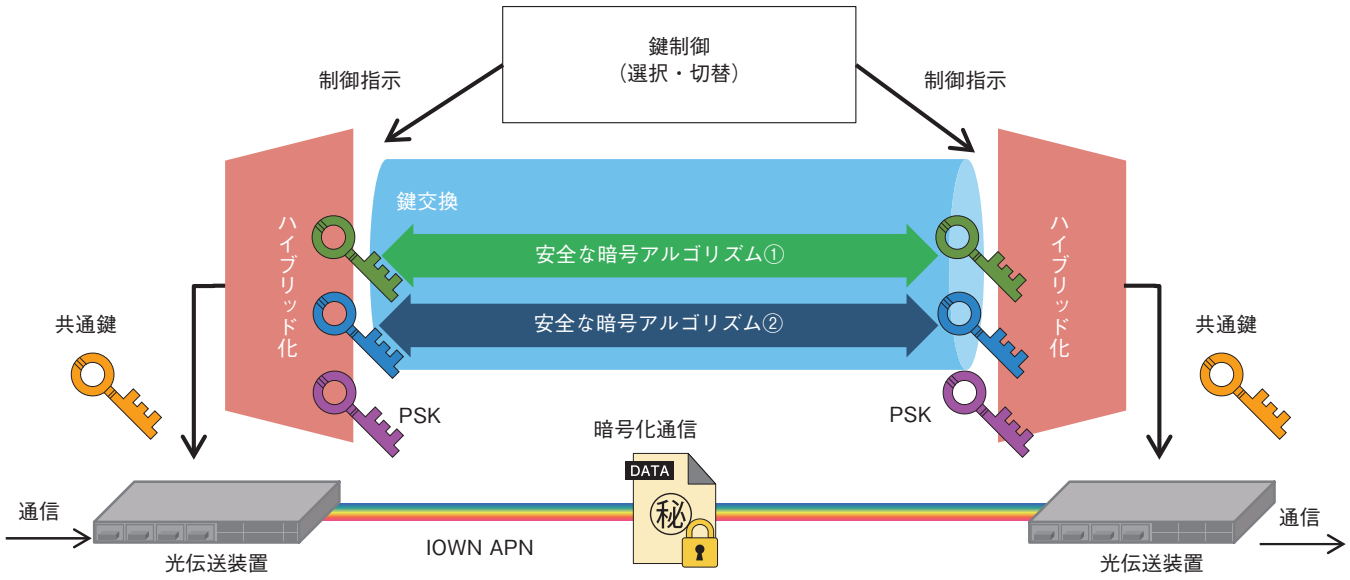


図4　Elastic Key Control 技術

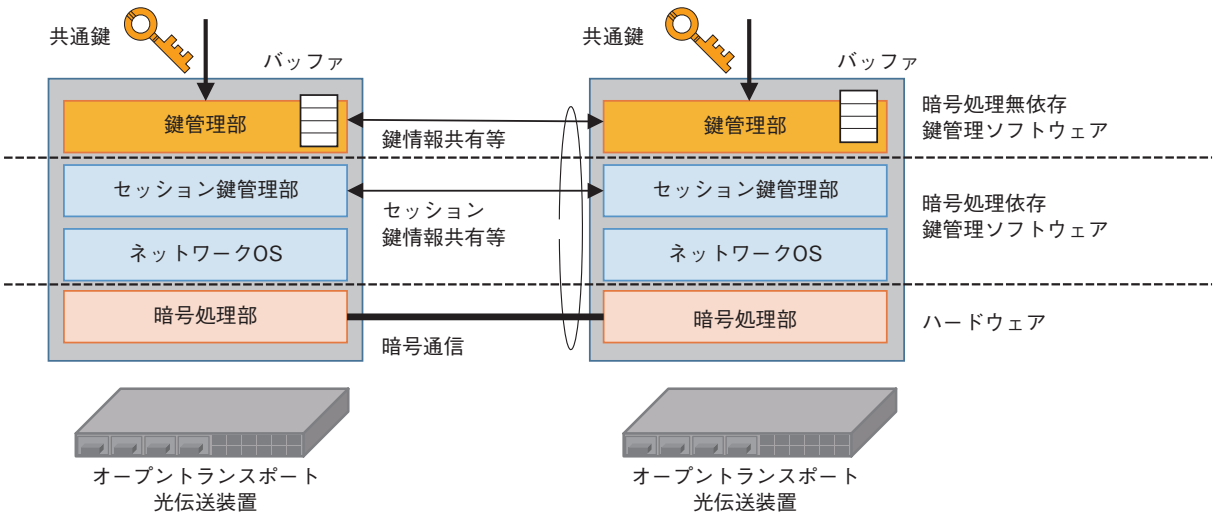


図5　暗号処理のディスアグリゲーション技術

処理に依存する管理を行うセッション鍵管理部，ハードウェアで暗号処理を行う暗号処理部に機能を分離して実装し，鍵管理部とセッション鍵管理部との間を疎結合にすることでNOSに依存しない暗号処理を実現しました（**図5**）．また，暗号処理は従来同様ハードウェアで処理するため高速に処理が可能です．インタフェースを共通化することで上位の暗号交換方式の違いや下位の暗号処理の違いを吸収し，同じ鍵供給方法でさまざまな装置で暗号処理することが期待できます．さらに，鍵交換通信で取得した共通鍵から複数の共通鍵を生成しバッファに保存することで冗長化する機能を開発し，通信障害や鍵枯渇により一部の鍵方式から共通鍵が取得できなくても暗号通信が継続できることを確認できました．

今後に向けて

本稿では，NTTのセキュア光トランスポート技術を発展させる取り組みとしてElastic Key Control技術と暗号処理のディスアグリゲーション技術について紹介しました．今後は本技術をNTT研究所のネットワークの一部で利用するトライアルの準備を進めています．将来的には一般向けサービスとして展開し，遠隔医療や金融といった大容量・低遅延・高セキュリティが求められる分野での活用を見込んでいます．

■参考文献

(1) https://www.rd.ntt/iown/0002.html
(2) https://journal.ntt.co.jp/article/16202
(3) W. Castryck and T. Decru: “An efficient key recovery attack on SIDH (preliminary version),” Cryptography ePrint Archive, 2022.
(4) https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
(5) https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final
(6) https://csrc.nist.gov/publications/detail/white-paper/2021/08/04/migration-to-post-quantum-cryptography/final
(7) https://datatracker.ietf.org/doc/html/draft-ietf-tls-hybrid-design

（1段目左から）村上　啓造/ 谷口　篤
持田　康弘
（2段目左から）工藤　史堯/ 木村　直宏
佐成　晏之
（3段目左から）知加良　盛/ 飯島　悠介
清村　優太郎
（4段目）向山　明夫

NTT研究所では，大容量，低遅延，低消費電力かつ量子コンピュータ時代でも安心・安全な光トランスポートネットワークの実現に向けて研究開発を進めています．

◆問い合わせ先
NTT社会情報研究所
企画担当
E-mail　solab＠hco.ntt.co.jp