セキュア光トランスポートネットワーク

奥田 哲矢[†1]　千田 浩司[†1]
白井 大介[†2]　知加良 盛[†1]
齋藤 恆和[†1]　中林 美郷[†1]
山村 和輝[†1]　田中 友里[†1]
夏川 勝行[†1]　高杉 耕一[†2]

NTT社会情報研究所[†1]
NTT未来ねっと研究所[†2]

近年，データセンタ間通信を中心に，光トランスポートネットワークの実用が進んでいます．光トランスポートネットワークの通信は，インターネットと同様に，公開鍵暗号と共通鍵暗号で保護されますが，特に公開鍵暗号・鍵交換については，量子コンピュータの研究開発の進展により，一部危殆化するリスクが懸念されています．そこで，NTT社会情報研究所とNTT未来ねっと研究所では，量子コンピュータによる暗号危殆化に対して安全な鍵交換の研究開発と，それら鍵交換を光トランスポートネットワークへ適用するためのアーキテクチャ設計や実機検証を進めています．

背　景

■トランスポートとは何か

まず，トランスポートとは何か，辞書的には「(物流の) 運送」や「(通信の) 伝送」を指します．一般的には，法人向けの物流・運送サービスや通信・伝送サービスを指すことが多いと思います．トランスポートと名前の付いた技術であるセキュア光トランスポートネットワークについて，その特徴をイメージしやすいように，物流・運送サービスの例えで話を始めようと思います（**図1**）．

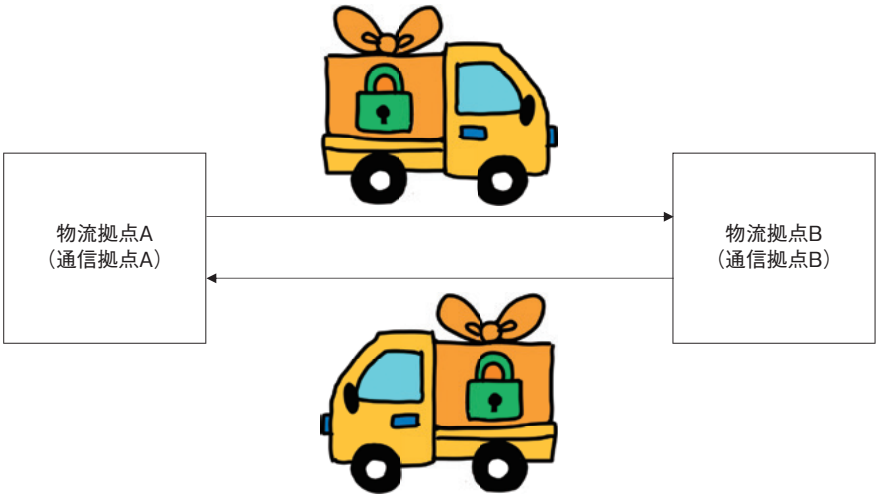


図1　トランスポートとは何か

トラックによる物流・運送サービスの場合，どういった特徴が求められるでしょうか．一度にたくさんの荷物を運べること，注文後にすぐに荷物が届くこと，等々が思いつきます．ここでは，**表**に示す5つの観点を取り上げてみます．

表　物流・運送サービスと通信・伝送サービスの比較

サービスの特徴	物流・運送サービス	通信・伝送サービス
大容量	トラック台数	スループット
低遅延	トラック待ち時間	レイテンシ
経済性	物流最適化	通信ネットワーク最適化
環境負荷	排ガス/CO_2	消費電力
安全性	荷物が正しく届くこと 交通事故が少ないこと	通信の故障が少ないこと セキュリティが高いこと

物流・運送サービスにおいて，大容量であること，低遅延であることは顧客にとってもっとも重要な特徴，サービスの価値であると思います．大容量＝トラック台数が多いこと，低遅延＝トラック待ち時間が少ないことと表現できます．また，事業として物流・運送サービスを営むうえでは，経済性も

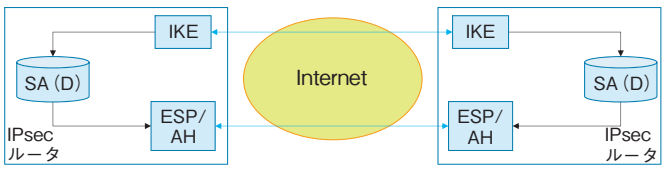
欠かせない特徴です．経済性は，物流が最適化されて経済的に運営されていることと表現できます．また，近年はサービスの社会的影響が問われることも多く，環境負荷や安全性も考慮すべき特徴です．環境負荷＝排ガス/CO_2が少ないこと，安全性＝荷物が正しく届くことや交通事故が少ないことと表現できます．

通信・伝送サービスではどうでしょうか．やはり，大容量であること，低遅延であることは顧客にとってもっとも重要な特徴，サービスの価値であると思います．通信分野の用語では，大容量＝スループットが高いこと，低遅延＝レイテンシが小さいことと表現できます．また，事業として通信・伝送サービスを営むうえでは，経済性も欠かせない特徴です．経済性は，通信・伝送サービスを提供するネットワークの効率性と表現できます．また，通信の業界においても，近年はサービスの社会的影響が重視されており，環境負荷や安全性も考慮すべき特徴です．通信分野では，環境負荷＝低消費電力であること，安全性＝ネットワークの故障が少ないこと，セキュリティが高いことと表現できるでしょうか．

NTTが研究開発を進めるIOWN（Innovative Optical and Wireless Network）/APN（All-Photonics Network）は，表に示した5つの観点のうち，大容量，低遅延，環境負荷の3点を顧客に訴求するサービスをめざしています[(1)]．そして，IOWN/APNに安全性＝セキュリティの観点をプラスする取り組みの1つが，本稿で提唱するセキュア光トランスポートネットワークです．

■光トランスポートネットワークの必要性

携帯電話・スマートフォンの普及，さらに大容量・低遅延の5G（第5世代移動通信システム）の普及で，世の中が便利になることに多くの方が賛同されると思います．法人向けの通信・伝送サービスにおいても，大容量・低遅延は顧客にとって望ましい特徴といえます．特に近年の顧客ニーズとしては，データセンタの災害対策（Disaster Recovery）を想定したデータセンタ間通信（Data Center Inter-connect）や，映像制作の現場における撮影拠点と編集拠点の間で同時並行に作業するリモートプロダクション（Remote Production）向けの非圧縮映像伝送が，注目されているように見受けます．これら大容量のデータを，なるべくリアルタイムに低遅延で，伝送するためには，光トランスポートが適しています[(2)]．この光トランスポートにセキュリティを付加する取り組みを，本稿で紹介します．



通常のIPsecの機器構成

図2　IPsecのアーキテクチャ

既存技術

■インターネット標準

通信・伝送サービスにセキュリティを付加するために，インターネットで利用されている既存技術を活用することは有効で，それら技術が長く使われているほどに，安全性評価の面で成熟していることが期待されます．

インターネットにおいて安全な通信路（セキュアチャネル）を構成するプロトコルの代表例として，SSL/TLSとIPsecが存在します．SSL/TLSは，Webサーバとクライアントの間のセキュアチャネルを構成する標準プロトコルです．IPsecは，企業の本社と支社など拠点間のセキュアチャネルを構成する標準プロトコルで，VPN（Virtual Private Network）サービスに使われる技術として知られています．本稿で紹介するセキュア光トランスポートネットワークは，拠点間の通信・伝送サービスです．

■IPsec

IPsecは，インターネットの事実上標準を定めるIETF（Internet Engineering Task Force）で仕様化されている拠点間のセキュアチャネルを構成するプロトコルで，仕様書の構成としては，アーキテクチャ，暗号化，認証，鍵交換，で構成されています[(3)〜(6)]．

全体像を表すアーキテクチャの中に，鍵交換を行うIKE（Internet Key Exchange），暗号化と認証を行うESP（Encapsulated Security Payload），認証を行うAH（Authentication Header），IKEで合意された鍵をESPまたはAHに伝えるSAD（Security Association Database）が存在します（**図2**）．なお，「認証」には，メッ

セージ認証とエンティティ認証が含意されます．それぞれ，通信先から届いたメッセージが正しいか検証すること，通信先が正しいか検証することに相当します．

次に，IPsecの構成がセキュア光トランスポートネットワークではどう変更されるか紹介します．

課題および提案（I）：量子コンピュータの進展の可能性

■量子コンピュータの進展の可能性

現在，インターネット等の通信では公開鍵暗号に基づく鍵交換が使われています．公開鍵暗号は数学的に解くことが困難な問題を安全性の根拠として構築されており，例えばRSA暗号は大きな2つの素数の積を素因数分解するには非常に多くの時間がかかることを安全性の根拠としています．しかし，誤り耐性を有する本格的な量子コンピュータが実現すると，2つの素数の積を短い時間で素因数分解できてしまい，RSA暗号が安全とはいえないことが知られています．そこで，対策として，量子コンピュータでも破ることのできない鍵交換の研究開発を進めています．

■量子鍵配送（QKD）

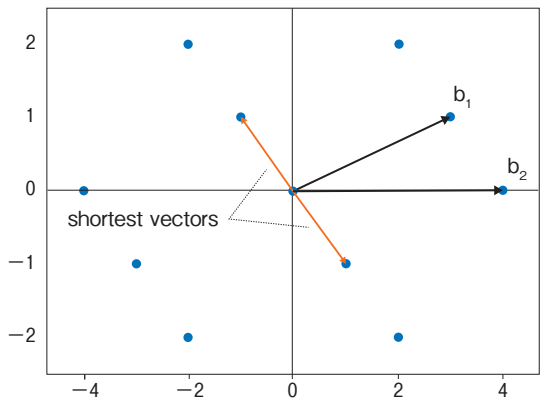
量子鍵配送（QKD：Quantum Key Distribution）は，量子物理による鍵配送の仕組みです．量子状態を伝送することができる量子通信路で，秘密鍵の情報を量子状態に載せて共有します．QKDの最大の特徴は，秘密鍵の共有時，第三者による盗聴を検知できることです．これは「量子状態は測定すると状態が変化する」という量子特有の性質に由来します．二者間で量子状態を送受信している途中で第三者が盗聴，すなわち測定をしたとすると，送信した量子状態と受信した量子状態が異なる場合があります．二者間で，それぞれ送受信した量子状態を公開された通信路で「答え合わせ」し，それが異なっている場合，第三者による盗聴を検知することが可能になります．これらの量子状態の送受信と，盗聴の検知を，繰り返し行って精度を高めることで，最終的に二者間で秘密鍵を共有することが可能になります．

■耐量子計算機暗号による鍵配送（PQCまたはPQKD）

耐量子計算機暗号（PQC：Post-Quantum Cryptography）は，数学的に解くことが困難な問題を安全の根拠とする公開鍵暗号・鍵配送の仕組みで，特に，量子計算機でも難しいと予想される問題を安全性の根拠とします．例えば，格子暗号は，格子点の集合が与えられたときに，原点からもっとも近い格子点を求めることが量子計算機を用いても難しいと予想されていることを安全性の根拠としています．

NTTは，耐量子計算機暗号である格子暗号の1つである，NTTを含むチームの技術が組み込まれたNTRU暗号を中心に研究開発を進めています（**図3**）．

以降では，QKDとPQKD（Post-Quantum cryptography-based Key Distribution）を総称してxKDと呼ぶこととします．



青い点が基底 {b_1, b_2} = {(3, 1), (4, 0)} で生成される2次元格子のベクトル．
この格子の最短ベクトルは（1, −1）と（−1, 1）．
主な格子問題である最短ベクトル問題（Shortest Vector Problem, SVP）は基底 {b_1, b_2} が与えられたときに最短ベクトルを見つけるという問題．

図3　量子計算機でも難しい格子問題の例

課題および提案（II）：アーキテクチャ設計における新たな攻撃者への対策

■ゼロトラストネットワークにおける攻撃者への対策

近年は，閉域ネットワークに絶対の信頼を置かない，ゼロトラストネットワークの攻撃者を想定した設計が普及しており[7]，今回のアーキテクチャ設計においては，通信キャリア網，拠点内ネットワークを含めて，あらゆるネットワーク上の攻撃者を想定する必要が

あります．通信キャリア網については，光ファイバに物理的に接続して通信内容を傍受する攻撃者を，拠点内ネットワークについては，拠点内ネットワークに権限を有して通信内容を傍受する攻撃者を想定します．

通信キャリア網において，光ファイバに物理的に接続して通信内容を傍受する攻撃者については，レイヤ1（物理層）を保護するプロトコルであるOTNsecおよびレイヤ2（データリンク層）を保護するプロトコルであるMACsecなどの，“ホップバイホップ”の暗号化による対策が可能であり，より低レイヤで暗号化の機能を実装することで，IOWN/APNの低遅延性を阻害することなくセキュリティを付加できることが期待されます．

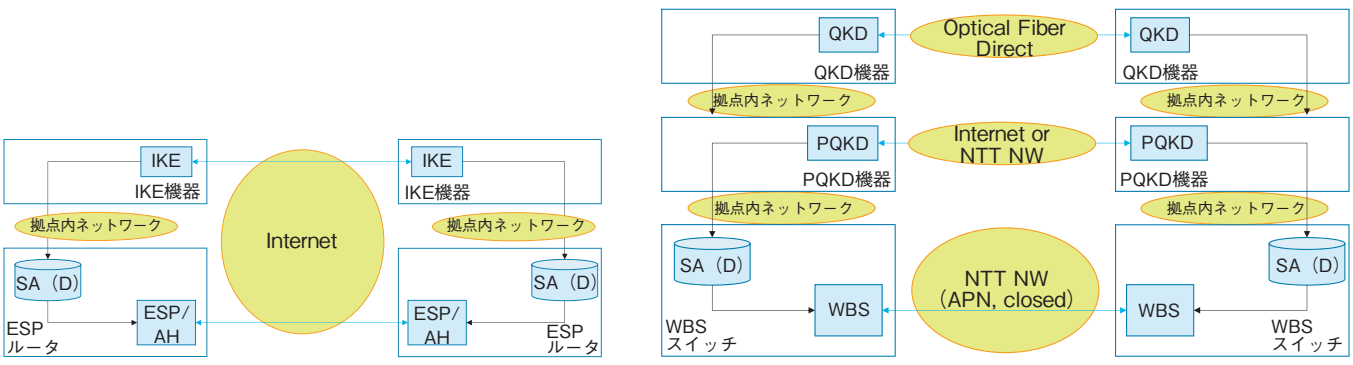
拠点内ネットワークに権限を有して通信内容を傍受する攻撃者については，IPsecに代表される拠点間通信のアーキテクチャ設計は一から見直す必要があります．セキュア光トランスポートネットワークでは，前述したIPsec/IKEに相当する鍵交換の部分がQKD装置あるいはPQKD装置に，IPsecのESP/AHに相当する暗号化の部分が光トランスポンダ・ホワイトボックススイッチに，それぞれ対応します．後述する「ディスアグリゲーション構成」の方向性で，鍵交換と伝送が別機器となることが想定され，IPsecでは一体であった鍵交換と暗号化の機能が分離した構成を想定する必要があります（**図4**）．その結果，IPsecのSA(D)に相当する鍵情報が機器外部のネットワークを流通し，ゼロトラストネットワークの仮定では，あらゆるネットワーク上の通信は保護が必要なため，IKEとESP/AHの間の通信を保護する対策を新たに検討する必要があります．具体的には，xKD装置から光トランスポンダへの安全な鍵配送方法，xKD装置と光トランスポンダの間の機器認証方法，を安全に設計する必要があります．これら検討詳細は公開予定論文[8]をご参照いただければと思います．

■外部から検証可能なアーキテクチャおよび機器の必要性

ゼロトラストネットワークでは，アーキテクチャ，プロトコル，機器等の信頼性を外部から検証可能であることが要求されます．さらに，セキュリティ対策の原則として，何らかの危殆化を見据えて，アーキテクチャ，プロトコル，機器等が個別に更新可能であることを要求します．本稿のアーキテクチャ設計，プロトコル設計，機器選定においては，信頼性を外部から検証可能かつ個別に更新可能とするための技術として，形式検証とホワイトボックススイッチを採用しました．

■形式検証

暗号技術を含むプロトコルの設計時には，プロトコル内の秘密情報の機密性やメッセージの完全性などの安全性を数学的に保証する安全性検証が必要です．特に，トランスポートを担うレイヤであるSSL/TLSやIPsec，ほかには携帯通信の規格である5G認証プロトコルの安全性検証に，形式検証技術が用いられています．形式検証とは，システムとシステムが満たすべき性質を形式言語で記述し，論理的な推論に基づきシステムが性質を満たしているか・いないかを検証する技術です．形式検証ではコンピュータによって自動化されている部分が多いため，再現性確認を含めて結果を外部から検証可能であること，プロトコルの更新に対して適応的に再検証可能であることが優れています．今回のセキュア光トランスポートネットワークにおいて



(a) IPsecの機器が分離した構成　　(b) セキュア光トランスポートネットワークの機器が分離した構成

図4　IPsecとセキュア光トランスポートネットワークの構成の差異

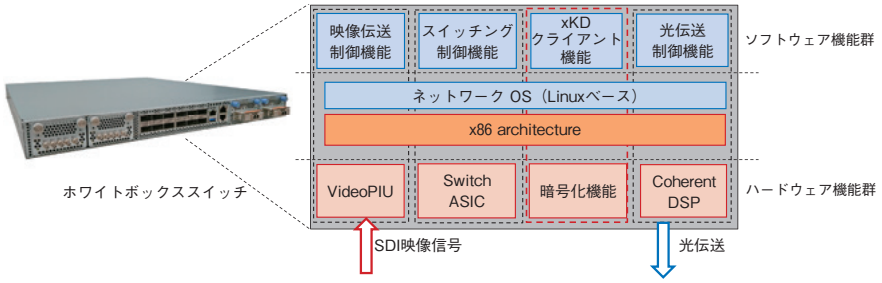


図5　ホワイトボックススイッチのディスアグリゲーション構成

は，xKD装置を光トランスポンダと組み合わせたIPsecベースのプロトコルを設計するに際して，安全性検証を形式検証ツールであるProVerifを用いて行いました[9]．

■ホワイトボックススイッチ

従来，光トランスポートを担う伝送装置は，光モジュールや各種機能などが一体型で提供されていました．これに対し，ディスアグリゲーション構成と呼ばれる，伝送装置の各種機能を分離し，標準化されたインタフェースで制御することで，柔軟な構成変更，付加機能の実現，コストの低減等が可能になる技術を採用した装置を，ホワイトボックススイッチまたはホワイトボックストランスポンダと呼びます．今回，ホワイトボックススイッチ装置のハードウェア機能群における，光伝送データの暗号化機能に対し，xKD装置から暗号鍵を取得して，設定・利用するxKDクライアント機能を新たにソフトウェア実装しました（**図5**）．さらに追加実装したSDI信号（映像信号）の直収機能を用い，40 Gbit/sを超える8K60Pの非圧縮映像を，超低遅延でセキュアに伝送できることを実証しました．これにより，xKD装置と光トランスポンダを連携した，セキュア光トランスポートの実現可能性について一定の検証ができたといえます．

今後に向けて

本稿では，NTTが研究開発を進めるIOWN/APNにセキュリティ機能を付加するための取り組みとしてセキュア光トランスポートネットワークについて紹介しました．また，本取り組みに際してフォーカスした課題と提案について紹介しました．本取り組みをステップに，NTTグループとして，安心・安全な技術およびサービスを提供することに引き続き貢献していきたいと思います．

■参考文献

(1) https://www.rd.ntt/iown/0002.html
(2) 富澤・金子・木村："Beyond 100G光トランスポートネットワークに向けたデバイス技術開発，" NTT技術ジャーナル，Vol.28, No.7, 2016.
(3) Security Architecture for the Internet Protocol https://datatracker.ietf.org/doc/rfc4301/
(4) Internet Key Exchange Protocol Version 2 (IKEv2) https://datatracker.ietf.org/doc/rfc7296/
(5) IP Encapsulating Security Payload (ESP) https://datatracker.ietf.org/doc/rfc4303/
(6) IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap https://datatracker.ietf.org/doc/rfc6071/
(7) S. Rose, O. Borchert, S. Mitchell, and S. Connelly："Zero Trust Architecture，" NIST SP 800-207, August 2020.
(8) 前田・中林・奥田："セキュア光トランスポートNWの実現に向けたアーキテクチャ設計および形式検証による安全性評価，" 第95回CSEC研究会，2021.
(9) B. Blanchet："Automatic Verification of Security Protocols in the Symbolic Model: The Verifier ProVerif，" Foundations of security analysis and design VII, Springer, pp. 54 -87，2013.

（1段目左から）奥田 哲矢/ 中林 美郷/ 齋藤 恆和
（2段目左から）千田 浩司/ 山村 和輝/ 田中 友里
（3段目左から）白井 大介/ 知加良 盛/ 夏川 勝行
（4　段　目）高杉 耕一

大手IT事業者や通信キャリアが，増大するデータセンタ間通信に対応するため，光トランスポートネットワークに注目しています．NTT研究所では，量子コンピュータ時代に適応可能で安心・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