量子鍵配送技術に基づくセキュアネットワーク

Secure Network Architecture Based on Quantum Key Distribution Technology

谷澤　佳道　■TANIZAWA Yoshimichi
高橋　莉里香　■TAKAHASHI Ririka

量子力学の基本原理に基づいて通信データの安全性を保証する量子鍵配送（QKD：Quantum Key Distribution）技術は，情報漏えいが許されない将来のセキュアネットワークを支えるキー技術として注目されている。

東芝は，QKD技術の基礎原理の研究開発と並行して，QKDを要素技術として活用し，現実的な通信ネットワークのセキュリティを強化するためのネットワーク・システム技術について，試作開発を進めている。今回，QKD技術を用いることに起因する技術制約を克服するため，複数のQKD装置をネットワーク化して運用するネットワーク技術や，QKD技術によって生成した暗号鍵を安全に中継するための暗号鍵保護・中継技術，複数のアプリケーションを同時に稼働させるためのプロトコル技術，暗号鍵のルーティング技術などを開発した。

Quantum key distribution (QKD), which guarantees communication security based on the principles of quantum physics, is expected to be a vital technology supporting future secure networks.

Toshiba is engaged in the research and development of basic technologies for QKD, as well as network and system technologies using QKD technologies, as elemental technologies to enhance the security of practical network systems. To overcome the technical constraints of current QKD technologies, we have developed a number of technologies including a network in which multiple QKD devices are organized and modern network functionalities are implemented, safer QKD key relaying computer systems, protocols supporting multiple applications, and a routing mechanism for key sharing.

1　まえがき

近年，情報システムや通信ネットワークが社会インフラの一部として用いられるようになり，そのセキュリティはますます重要になってきている。古典暗号と称される多くの既存暗号技術は，現在の技術で解読するには膨大な計算リソースを必要とすることから，現実的には解読できないことを安全性の根拠にしている。しかし，新たな解読アルゴリズムの発見や，量子コンピュータなどのより高性能な計算機の出現をきっかけとして，簡単に解読されてしまうというリスクがある。

量子鍵配送（QKD：Quantum Key Distribution）技術とは，通常，光ファイバで直接接続された2ノード間で乱数を秘密裏に共有する技術である。ここで共有される乱数を盗聴しようとすると，量子力学の基本原理に基づいて攻撃者を検出できる。また，共有した乱数を暗号鍵として用い，一度使用した暗号鍵は捨ててしまうワンタイムパッド暗号通信を行う場合，古典暗号と異なり，攻撃者がどれほどの計算リソースを持っていても，決して解読されないことが情報理論によって証明されている[1]。

東芝は，QKD技術の基礎研究において先進的な成果を挙げている[2]-[6]。これらの成果を踏まえ，QKD技術を具体的な情報システムや社会インフラシステムに組み込み，セキュアなネットワークを構築するための研究開発も進めている[7], [8]。

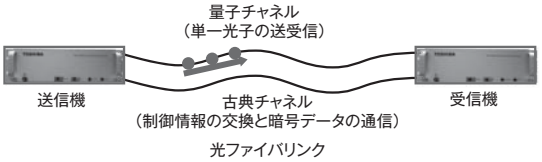

図1．量子鍵配送の基本構成 ― 光ファイバリンクを介して，単一光子の送信機と受信機が接続される。
Basic configuration of QKD

ここでは，QKD技術を2ノード間での暗号鍵共有のための要素技術として活用し，これに基づいたセキュアネットワークを構築するためのアーキテクチャについて述べる。

2　QKD技術の特徴と制約

QKDは，単一光子の送信機と受信機を，量子チャネルと古典チャネルから成る光ファイバリンクで直接接続した構成を基本とする（**図1**）。当社が採用したBB84と呼ばれるQKD方式は，1ビットの情報をエンコードした単一光子を送信機が量子チャネル上に送信し，受信機がこれを検出後，古典チャネル上での制御情報の交換を経て乱数情報として共有するものである。光子にエンコードされた情報をデコードする際，光子の状態が必ず変化してしまうため，第三者による盗聴を確実に検

出できるという不確定性原理に立脚し，盗聴の検出を行う[1]。共有した乱数情報から生成した暗号鍵を用いて暗号化されたデータの通信は，古典チャネル上で行う。

このQKDによる暗号鍵共有技術を一般の情報システムや通信ネットワークに組み込むには，大きく二つの制約がある。

(1) 単一光子の送受信が前提であるため，数十キロメートル以下の光ファイバリンクで直接接続されたノード間でしか暗号鍵を共有できない。長距離で多拠点のネットワークを構築するには，暗号鍵を安全かつ適切に中継する技術が必要

(2) 光子検出素子の物理的制約と通信経路の外乱により，単位時間当たりに共有できる暗号鍵の量（暗号鍵の共有スループット）に上限及び変動がある。実際のネットワークでは，秘匿通話や重要インフラ設備の遠隔監視といった暗号通信アプリケーションが，同時に複数，あるいは複数拠点間で動作しうる。このとき，全てのアプリケーションあるいはノードにおける，暗号データの送信側と受信側で安全に共有された同一の暗号鍵を適切かつ十分に提供できるよう，暗号鍵を管理し，割り当てる仕組みが必要

3 セキュアネットワークのアーキテクチャ

当社は，QKD技術に基づくセキュアネットワークにおいて，前述した制約を克服するためのアーキテクチャを構築した。アーキテクチャは以下に述べる五つの機能要素から構成される。

3.1 ネットワーク構成

セキュアネットワークの構成とその要素を，**図2**及び**表1**に示す。セキュアネットワークは，鍵共有ネットワークと暗号データ通信ネットワークから構成される[9]。

鍵共有ネットワークは，図1に示した光ファイバリンクで接続されたQKDの送信機あるいは受信機によってリンク間で暗号鍵（リンク鍵）を共有するノードで構成される。ノードは更に，QKDとは独立に乱数を生成し，これを複数のリンクの古典チャネルやノードを経由して鍵共有ネットワーク上で接続される別のノードとの間で暗号鍵（アプリケーション鍵）として共有する機能も持つ。ノードは，生成したアプリケーション鍵を隣接ノードに対してリンク鍵でワンタイムパッド暗号化して古典チャネル上で転送し，更にこれを受信したノードは，同一のリンク鍵によって復号する。このような，鍵共有ネットワーク上の複数のノードによるリンク鍵を利用したアプリケーション鍵中継の仕組みにより，多拠点ネットワークにおける暗号鍵（アプリケーション鍵）の安全な共有が可能になる。

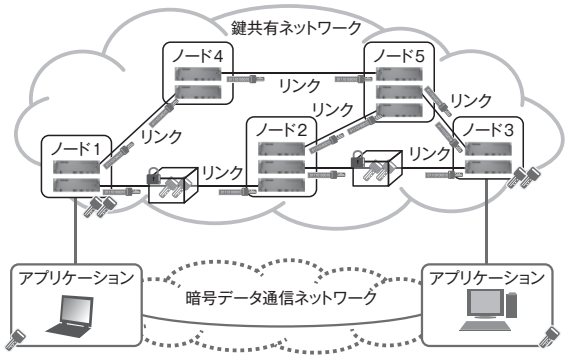

図2．セキュアネットワークの構成 ― 鍵共有ネットワークと暗号データ通信ネットワークから構成される。
Secure network architecture

表1．アーキテクチャの構成要素
Building blocks of secure network architecture

分 類	名 称	説 明
ネットワーク	鍵共有ネットワーク	暗号鍵を共有するためのネットワークで，ノードにより構成される
	暗号データ通信ネットワーク	アプリケーションによる暗号データ通信に利用される
装置	ノード	QKD技術と暗号鍵中継の仕組みにより，リンク鍵とアプリケーション鍵を共有する
	アプリケーション	ノードからアプリケーション鍵を取得し暗号データ通信を行う
暗号鍵	リンク鍵	QKD技術により，隣接するノード間で共有される
	アプリケーション鍵	暗号鍵中継の仕組みにより，リンク鍵で保護され，任意のノード間で共有される

個々のアプリケーションは，ノードに接続してアプリケーション鍵を取得し，一般のインターネット回線などにより実現された暗号データ通信ネットワーク上で，アプリケーション鍵で暗号化したデータの送受信を行う。暗号通信に用いられるアプリケーション鍵は，QKD技術により共有されたリンク鍵によって保護されているため，安全性が保証される。

3.2 セキュア中継ノード

前述のネットワーク構成及び鍵中継メカニズムを採用することで，アプリケーション鍵を任意のノード間で共有できるようになる。しかし，QKD技術が保証するのはリンク鍵を使ったリンク上の通信セキュリティだけであり，アプリケーション鍵を中継するノード（コンピュータ）への侵入や攻撃に対する防御には別の技術が必要になる。そこで当社は，コンピュータセキュリティ技術と物理セキュリティ技術を組み合わせ，アプリケーション鍵を安全に中継するためのセキュア中継ノードを試作した。

コンピュータセキュリティ技術の観点からは，セキュリティチップを利用して，セキュアブート，セキュアOS（基本ソフトウェア），暗号化ファイルシステムへとつながるトラストチェーンを構築し，ハードウェアに立脚した暗号鍵保護機能を搭載することで，ノードへの不正アクセスや暗号鍵データの盗難を防止した。また，物理セキュリティ技術の観点からは，監視カメラや各種センサを備えたサーバラックを作製し，QKD装置や暗号鍵を格納するハードディスクドライブ（HDD）への物理的，

直接的な攻撃や盗難からの保護・検出機能を搭載した。

更に鍵共有ネットワーク上には，セキュア中継ノードへの攻撃を監視する監視機能が稼働する。監視機能は，あるセキュア中継ノード上で異常を検出した場合，そのノードとの暗号鍵共有を禁止させると同時に，攻撃によってノードから漏えいしたリスクのある暗号鍵を特定し，対象の暗号鍵を保持するノードに対してその使用を停止させる。

3.3 暗号鍵共有プロトコル

前述のセキュア中継ノードにより，安全なアプリケーション鍵の中継が可能になった。更に，アプリケーション鍵を中継して送り届ける相手先を選択するため，アプリケーションからの要求情報を反映して，アプリケーション鍵の共有相手を特定するディレクトリ機能と通信プロトコルを導入した[7]。ディレクトリ機能は，ノードに付与された鍵共有ネットワークのIP（Internet Protocol）アドレスと，そのノードに接続しているアプリケーションに付与された暗号データ通信ネットワークのIPアドレスの対応関係を管理する。

一例として，鍵共有ネットワーク上の三つのノードを介して，アプリケーションのペア（クライアントとサーバ）がアプリケーション鍵を共有し，暗号データ通信ネットワークを経由して暗号通信を行う場合の通信手順について述べる（**図3**）。ここで，鍵共有ネットワーク上のノードの各リンクでは常にQKDによるリンク鍵共有処理が動作し，古典チャネルを介したノードのリンク間通信は双方向とも全てリンク鍵により暗号化される。

まず，ノード3に接続したサーバアプリケーションは，自身の暗号データ通信ネットワーク上のIPアドレスと提供サーバ機能（ポート番号）の情報（サーバ情報）をノード3に送信する。ノード3は，事前に設定されたディレクトリ機能を備えるノード（ここではノード2）に対し，サーバアプリケーションとそれが接続されるノードであるノード3のIPアドレス情報を登録する（ディレクトリ登録）。

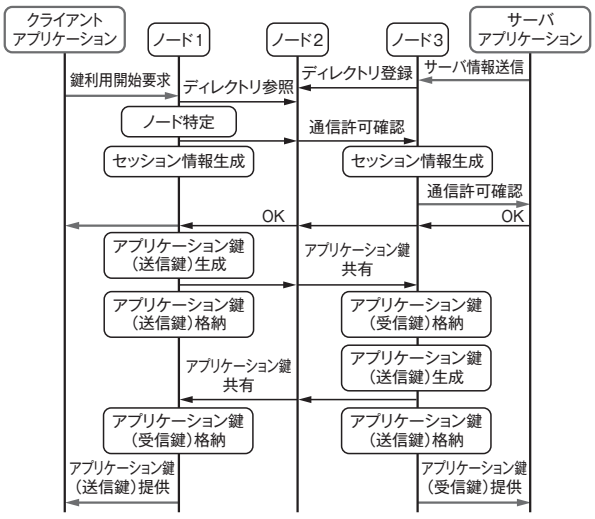

図3．暗号鍵共有プロトコル ― ノードは，アプリケーションからの情報により，アプリケーション鍵を共有するノードを特定する。
Sequence of application key sharing

ここで，ノード1に接続したクライアントアプリケーションは，暗号通信の相手であるサーバアプリケーションの暗号データ通信ネットワーク上のIPアドレスとポート番号及び，要求するアプリケーション鍵の共有スループット情報を含む，鍵利用開始要求をノード1に送信する。ノード1は，前述のノード3と同様にディレクトリ参照し，該当のサーバアプリケーションが接続されているノードがノード3であること，及びノード3の鍵共有ネットワーク上のIPアドレス情報を特定し，ノード3とセッション情報を共有する。セッション情報は，アプリケーションが利用する暗号データ通信ネットワーク上のIPアドレス及びポート番号のペアにより識別され，アプリケーション鍵の共有スループット情報や，後述するアプリケーション鍵割当て情報を含む。

次に，セッション情報を共有したノード1とノード3は，要求された共有スループットに応じて，アプリケーション鍵の共有動作を開始する。ここで，共有スループットが要求を満たせない場合，ノードはアプリケーションに対し提供可能なアプリケーション鍵の共有スループット情報を提供する。アプリケーション鍵には，アプリケーションがデータを暗号化して送信する際に用いる送信鍵と，データを受信して復号する際に用いる受信鍵とがある。暗号通信するアプリケーションのペアに対しては，一方が送信鍵として使う鍵を，他方が受信鍵として使うように制御する必要がある。クライアントアプリケーションに接続されるノード1を例にとれば，クライアントアプリケーション用の送信鍵は自身が生成してノード3に送信し，受信鍵はノード3から受信することで，両アプリケーション鍵をそれぞれ共有し，個別に格納，管理する。また，セッションが継続する限り，ノード1とノード3によるアプリケーション鍵の共有動作は継続する。

そして，ノード1及びノード3で最初のアプリケーション鍵の共有が終わると，両ノードはこれをアプリケーションに提供する。以後，両アプリケーションは，データ送受信の必要に応じて，接続するノードからアプリケーション鍵を取得した後，暗号データ通信を行う。

ここで述べたアプリケーションと接続ノード間の通信が通信開始時，送受信時，及び通信終了時だけのシンプルな通信手順は，一般的な古典暗号用の通信ライブラリと同様であり，そのまま対応付けられることから，既存のアプリケーションをQKD技術に対応させるためのソフトウェア改変は最低限に抑えられる。

3.4 暗号鍵割当て手法

前述のノード1とノード3に複数のアプリケーションのペアが接続される場合，ノードは，複数のアプリケーションから要求された共有スループットを合算した分量のアプリケーション鍵を一括して共有し，その後，ノード間で制御情報を交換する

ことにより，共有済みのアプリケーション鍵をどのアプリケーションに割り当てるかを決定する（**図4**）。このように，ノード間鍵共有機能とアプリケーションへの鍵割当て機能を分離することで，鍵共有処理の効率を高めるとともに，複数アプリケーション動作環境下での暗号鍵の最適分配を図っている。

具体的には，全てのアプリケーションから要求された共有スループットを同時には満たせない場合に，現在の共有スループットで得られるアプリケーション鍵を提供するアプリケーションを優先度や実際のアプリケーション鍵消費量などを考慮して決定したり，アプリケーションの終了で使われずに残った暗号鍵を新たに起動したアプリケーションに即座に割り当てたりすることで，アプリケーションの暗号鍵共有待ち遅延や，むだな暗号鍵の共有削減が可能になる。

3.5　アプリケーション鍵ルーティング手法

一般に，ネットワークの規模が大きくなると，ノード間でデータを転送するための複数の経路から最適な経路を選択するルーティング機能が求められる。特に，ノードがアプリケーション鍵を共有する鍵共有ネットワークにおけるルーティングでは，以下に述べる経路の選択が必要になる。

（1）　3.2節で述べた監視機能により，攻撃にさらされていることが検出されたノードを経由しない経路を選択

（2）　アプリケーション鍵を暗号化して転送するために十分なリンク鍵が蓄積あるいは共有されているリンクを通る経路を選択

（3）　アプリケーション鍵の転送により消費されるリンク鍵の総量を抑制するため，経由するリンクの数ができるだけ少ない経路を選択

そこで，インターネットなどで用いられる一般的なルーティングプロトコルを拡張し，各リンクのリンク鍵残量や共有スループット，経由リンク数，及びノードに対する攻撃状況に基づき最適な経路を選択する手法を開発した。これにより各ノードは，被攻撃ノードと接続されるリンクを停止し，また，接続リンクの状況やリンク鍵残量をノード相互で交換することによって，動的に効率よくアプリケーション鍵を転送できる[8]。

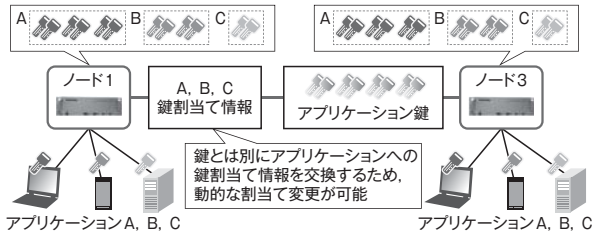

図4．アプリケーション鍵の割当て手法 ― ノードは，アプリケーション鍵の共有とは別に，鍵割当て情報も共有する。
Application key assignment method

（注1）　2011年5月現在，当社調べ。

4　あとがき

QKDを要素技術としたセキュアネットワークの実現を目指し，システム構築に必要な技術を開発した。QKD技術の安全性を備えつつ，現実的な情報システムからも安全かつ簡単に使えるようにするため，セキュア中継ノードやプロトコル技術などを構築した。ネットワーク構成及びプロトコル・ルーティング技術に関しては，QKD装置を模擬したエミュレータ装置を用いて動作を検証した。当社が持つ世界最高性能（注1）のQKD技術と，ここで述べた技術とを組み合わせることで，将来の社会インフラシステムに求められる高いセキュリティ性能を備えたネットワークを構築できる。

今後も当社は，QKDの機能・性能向上のための研究開発や，QKDの原理に基づく新技術の追求とともに，QKDを要素技術とし，これらを実社会に適用できる形に具体化するためのシステム技術や周辺技術を積み上げ，より安全なネットワーク社会の実現に貢献していく。

文　献

（1）　石井　茂．量子暗号 絶対に盗聴されない暗号をつくる．日経BP社．2007，286p.
（2）　Sasaki, M. et al. Field test of quantum key distribution in the Tokyo QKD network. Opt. Express. **19**, 11, 2011, p.10387－10409.
（3）　Dixon, A. R. et al. Continuous operation of a high bit rate quantum key distribution system. Appl. Phys. Lett. **96**, 2010, p161102-1－161102-3.
（4）　ジェイムズ ダインズ 他．高速量子鍵配送プロトタイプによる実証運用．東芝レビュー．**66**，11，2011，p.14－17.
（5）　アンドリュー シールズ 他．世界最高速の無条件に安全な量子暗号鍵配信技術．東芝レビュー．**64**，7，2009，p.7－11.
（6）　Frohlich, B. et al. A quantum access network. Nature. **501**, p.69－72.
（7）　谷澤佳道 他．“量子鍵配送技術をモチーフとしたセキュアネットワークの一提案”．電子情報通信学会 2012ソサイエティ大会．富山，2012-08，電子情報通信学会．2012，p.139.
（8）　高橋莉里香 他．“量子暗号通信のためのセキュア鍵共有ルーティングプロトコルの提案”．第12回情報科学技術フォーラム FIT2013．鳥取，2013-09，情報処理学会 他．2013.
（9）　Dianati, M. et al. Architecture and protocols of the future European quantum key distribution network. Security and Communication Networks. **1**, 1, 2008, p.57－74.

谷澤　佳道　TANIZAWA Yoshimichi
研究開発センター ネットワークシステムラボラトリー研究主務。ネットワークシステム・システムセキュリティ・量子鍵配送技術の研究・開発に従事。IEEE，情報処理学会会員。
Network System Lab.

高橋　莉里香　TAKAHASHI Ririka
研究開発センター ネットワークシステムラボラトリー。ネットワークシステム・量子鍵配送技術の研究・開発に従事。情報処理学会会員。
Network System Lab.