光が導く次世代の暗号技術「量子暗号」

伊東 洋一郎　遠山 裕之

要 旨

量子暗号は、将来にわたり解読されるリスクがなく超長期的に情報を保護できる暗号方式で、国家レベルの重要な基幹システムなどに適用が期待されています。

量子暗号は、量子鍵配送によって事前に暗号鍵を伝送共有し、ワンタイムパッドと呼ばれる暗号方式で通信を暗号化することを指します。量子鍵配送では、光の粒である光子に鍵情報を載せ、その量子力学的な性質で鍵を守ります。

NECでは、BB84と呼ばれる方式に加えて、次世代技術のCV-QKD方式の研究を進めています。

KeyWords
安全・安心なサイバー空間／セキュリティ／量子鍵配送／量子暗号

1. なぜ今、量子暗号か

私たちの現代社会は、インターネットをはじめとした高度に情報化したインフラの多大な恩恵によって成立しています。今後、情報がより一層私たちの社会に不可欠なものになっていくなかで、悪意のある第三者に情報が盗まれてしまうと、社会生活が危機に瀕することも予想されます。

NECでは、豊かな社会を実現するための社会価値として、「安全」「安心」「公平」「効率」を掲げています。本稿は、それらを実現する究極の技術としての量子暗号を紹介します。

1.1 現代暗号の安全性

現在の情報化社会において交換される情報のほとんどは、AESやRSA暗号などの「現代暗号」によって守られています。現代暗号を簡単に言うと、暗号化の方法（アルゴリズム）は皆知っているが、鍵を秘密にすることで情報を秘匿するというものです。

そして、現代暗号の安全性は、解読するための計算に非常に時間が掛かるということにより、担保されています。

1.2 現代暗号の危殆化

しかし、この現代暗号の安全性は、量子コンピューターの登場によって脅かされようとしています。例えばRSA暗号は、非常に大きな数の素因数分解の計算に莫大な時間が掛かることを応用したものですが、量子コンピューターを用いることで、短時間に計算できるようになることが分かっています。もちろん、更に大きな数の素因数分解にすることで、現在開発されている量子コンピューターではまだ解読に時間が掛かることにはなります。

しかし、それは、同じ応酬の繰り返しでしかありません。世界中が量子コンピューターの研究に取り組み、近年急速に進展している現状を鑑みると、現代暗号は早晩危殆化してしまうことが危惧されます。

1.3 量子暗号の意義

量子暗号によって、この応酬の繰り返しを終わらせることができます。たとえ最高性能の量子コンピューターを使おうと、桁外れの能力の未来の計算機を持ってきたとしても、絶対に解読できないことが保証されています。それが「絶対安全」という、量子暗号の最大の意義になります。

なお、量子暗号は、共通鍵暗号に位置付けられるものですが、従来の暗号とは大きく異なる特徴があります。それは、古来暗号を使うときに常に悩みの種であった、送り手と受け手で、鍵を絶対安全でありかつ自動で共有できる仕

組みを持っていることです。

2. 量子暗号とは

量子暗号がなぜ絶対安全なのかについて、第２章では概略を紹介します。

量子暗号は、「ワンタイムパッド」と「量子鍵配送」と呼ばれる２つの部分からなります（**図1**）。ワンタイムパッドとは、実際に通信するときに、暗号化/復号を行う方式になります。量子鍵配送とは、事前に暗号鍵を伝送/共有する仕組みになります。

2.1 ワンタイムパッドとは

ワンタイムパッドとは、送受信するメッセージと同じ長さの乱数を、事前に送信者と受信者で共有しておき、その乱数を暗号鍵として使用することで、メッセージを暗号化/復号するものです。ただし、１回使用するごとに、その暗号鍵は破棄します。暗号化/復号に使用される演算は、排他的論理和と呼ばれる非常に単純で軽量なものです。

このようなワンタイムパッドと呼ばれる暗号化/復号の方式は、絶対に解読できないことが1940年代に数学的に証明されています。簡単でしかも絶対安全なこの方式がなぜ使われていないのか、それは平文と同じ長さの鍵を安全に共有するのは現実的ではなかったからです。ところが、量子力学を応用した量子鍵配送によってこの欠点を補うことができるようになりました。

2.2 量子鍵配送とは

量子鍵配送とは、メッセージを送受信したい送信者と受信者で暗号鍵（乱数）を事前に共有する仕組みです。

ここでは、分かりやすさのために単純化して説明します。まず、１ビットの鍵の情報を光子１粒ごとに与えて、送信者から受信者に送るようにします。もしも途中で盗聴者がいて、光子を盗み取ってしまうと、その光子は受信者に届きません（量子論的に光子はそれ以上分割できない）。一方で、盗聴者が光子を盗み見てまた戻したとしても、量子力学的に光子の状態が変化するため、盗聴の判別ができます。したがって、１粒の光子に鍵情報を載せて伝送/共有することで、盗聴の検知と防止ができるため、盗聴の可能性がある鍵は使わず、安全な暗号鍵だけを共有できます。

量子鍵配送を実現するプロトコル（方式）として、複数考案されており、方式ごとに厳密な安全性の議論がなされています。安全性の証明には、盗聴者が物理的にあらゆる攻撃が可能という前提で議論がなされ、安全性が理論的に証明されているため、量子暗号が将来的にも「絶対安全」といえます。

2.3 BB84方式の量子鍵配送

ここではBB84方式と呼ばれる、量子鍵配送の代表的なプロトコルを簡略化して説明します。

送信者は、１粒の光子ごとに１ビットの鍵の情報を載せて送ります（**図2**）。具体的には、送信機において、光子源からの光子１粒に対して、乱数から生成された1ビットの情報を載せて送ります。受信機では、光子検出器で光子1

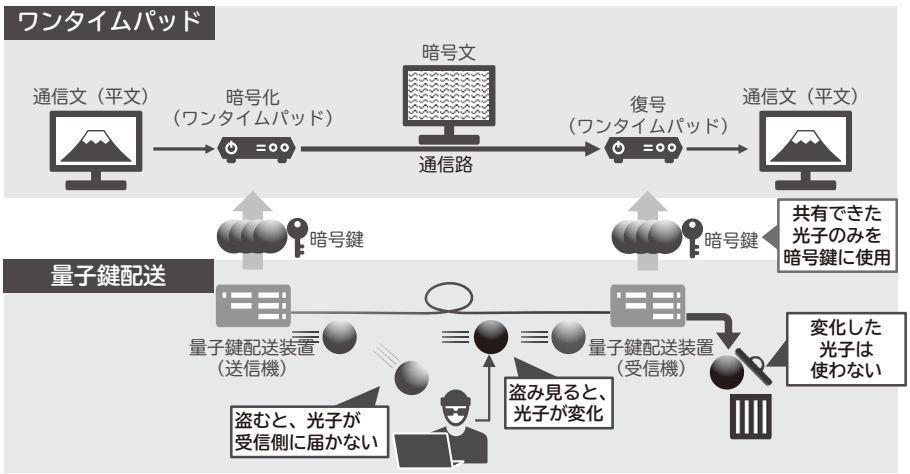


図１　量子暗号の仕組みの概略

粒を検出して、ビットの情報を読み取ります。盗聴があった場合は、第２章２節で説明したとおり、盗聴の検知と防止ができます。実際は、盗聴の判断とその結果、鍵を抽出する処理が理論的に厳密に考えられてプログラムされています（図2）。

現在は、前述した内容を少し複雑にしたデコイBB84方式と呼ばれるプロトコルが、絶対安全であることが証明されており、世界中で開発が行われている方式になります。NECも、国立研究開発法人情報通信研究機構（以下、NICT）とともに研究開発を行っています。

2.4 CV-QKD方式の量子鍵配送

次に、CV-QKD方式と呼ばれる量子鍵配送のプロトコルです（**図3**）。BB84での光子の検出は、光子検出器として高い性能を有するものが求められます。また、光ファイバーを占有する必要があるなどの制約もあります。

本方式は、送信機では、微弱な光波と通常光との位相差に、1ビットの鍵の情報を載せて受信機に伝送します。受信機の光波検出器は、特別な性能は必要ありません。これにより、同じ光ファイバー上で通常の光通信との共存が可能になり、より安価に実現できます。

現在、NECでは、学習院大学とともに、本方式の研究開発を行っています。

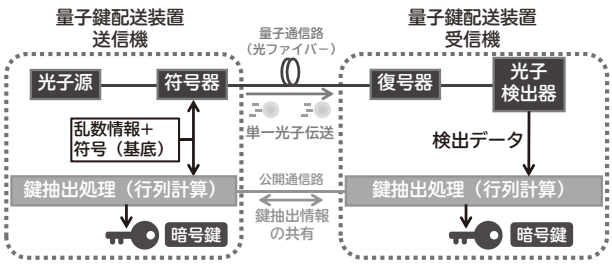


図２　BB84方式の量子鍵配送の概要

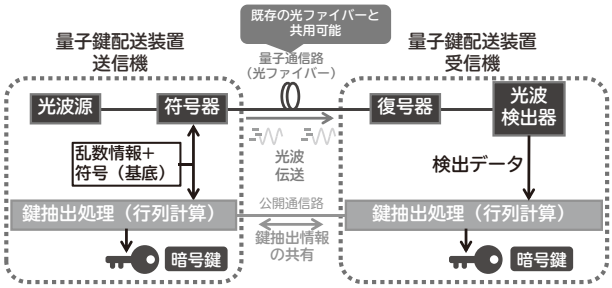


図３　CV-QKD方式の量子鍵配送の概要

2.5 量子鍵配送の課題と対策

量子鍵配送は、課題（というより物理的な制約）もあります。光子1粒を光ファイバーで伝送すると、大きな伝送ロスが発生します。このため、距離と鍵生成速度（1秒当たり何ビット暗号鍵を生成できるか）に、制約を与えてしまいます。NECで開発した装置では、伝送距離は50kmにおいては、50～100kbps程度になります。

距離制約には、量子鍵配送装置をつなぎ、鍵リレーすることで対策します。実際に、Tokyo QKD Network（NICTが運用中）として、鍵リレーを行い実証しています。

鍵生成速度制約には、波長多重という仕掛けを行って鍵生成量を増やすことや、AESなどの現代暗号と併用することで鍵の共有バランスを取るなどの方法があり、NECでも実証しています。

3. NECの研究開発状況

NECでは、量子鍵配送の製品化に向けて、さまざまな研究開発に取り組んでいます。量子鍵配送を実世界に適用するうえでは、実際の厳しいフィールド条件で、長期安定的に鍵供給できることが必要になると考えています。

特にNECのBB84装置は、外的な環境変動の大きい光ファイバーでも、強い耐性を備えた仕組み（PLC干渉計を含む回路）を有しています。NECでは、そういった厳しい環境での長期安定動作を実証しています（**図4**）。

4. 社会実装の状況

量子暗号の社会実装に向けて、さまざまな実証実験を実施しています。第４章では、その取り組みについて紹介します。

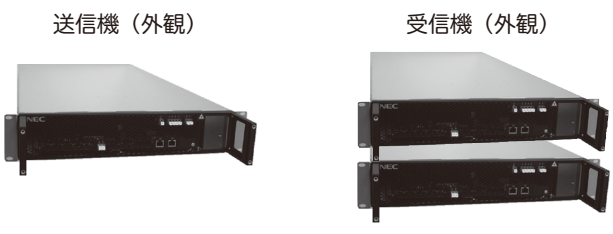


図４　NECのBB84装置の試作品

4.1 生体認証領域における実証実験*

生体認証は、人間の身体的特徴を抽出し、認証を行うもので、利用方法が簡単で紛失もしない優れた特性を持ちます。

一方、その情報が盗まれると、更新できないという課題もあります。また、生体認証用参照データは、個人情報であり、極めて高い安全性で保護することが要求されます。

NECはNICTと協力して量子暗号と生体認証技術を統合して、顔認証時の特徴データ伝送を量子暗号で秘匿化するシステムを開発し、Tokyo QKD Network上で実証しています（**図5**）。

4.2 医療分野における実証実験*

近年、自然災害により甚大な被害が発生していますが、災害時であっても医療サービスを維持する必要があります。このため、災害時に備えて患者の電子カルテデータを遠隔地に保管し、復元して取り出せる仕組みが求められています。

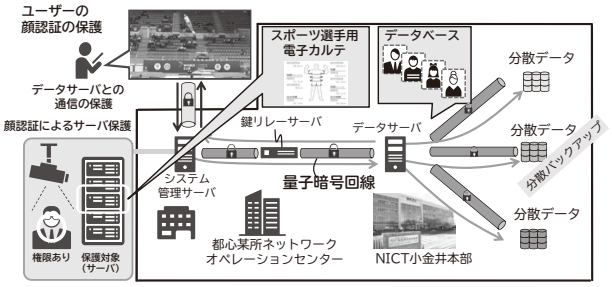


図5　顔認証による実証実験概要

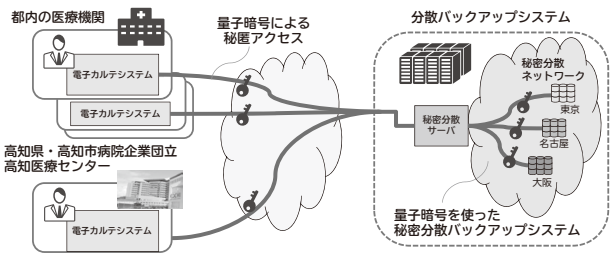


図6　医療分野における実証実験概要

NECはこの課題を解決するため、NICT及び株式会社ZenmuTechと協力し、電子カルテのデータの伝送を量子暗号で秘匿化し、ネットワーク経由で安全な伝送を行うシステムを開発しました（**図6**）。

4.3 金融分野における実証実験の計画*

金融機関に対するサイバー攻撃の脅威が増え、金融システムへの影響が懸念されています。こうしたなか、金融庁の取り組みの強化指針もあり、将来的な脅威に備えた新たな安全対策が急務となっています。

NECは、野村ホールディングス株式会社、野村證券株式会社、NICT、株式会社東芝と共同で、量子暗号の金融分野への適用可能性の検証を予定しています。

5. 将来の展望

今後、私たちの社会は、データの活用によるデジタルトランスフォーメーションが加速していくと考えられます。データからさまざまな社会価値が生み出されていく世界では、そのデータや生み出された価値を確実に守る仕組みも不可欠です。そうした次世代の安全・安心に支えられた豊かな社会に向けて、量子暗号を含めたトータルソリューションを提供していくことを目指しています。

なお、NECの量子暗号の研究活動は、革新的研究開発推進プログラム、第2期戦略的イノベーション創造プログラムなどのナショナルプロジェクト（NP）の活動成果によっております。

執筆者プロフィール

伊東 洋一郎
ナショナルセキュリティ・ソリューション事業部
マネージャー

遠山 裕之
ナショナルセキュリティ・ソリューション事業部

* 第4章1節から第4章3節の実証実験は、内閣府が主導する戦略的イノベーション創造プログラム（SIP）「光・量子を活用したSociety 5.0実現化技術」（管理法人：国立研究開発法人量子科学技術研究開発機構）の一環として実施しました。

関連URL

Communication Theory of Secrecy Systems
http://pages.cs.wisc.edu/~rist/642-spring-2014/shannon-secrecy.pdf

The Tokyo QKD Network
http://www.tokyoqkd.jp/

生体認証データの高秘匿・高可用性な伝送・保管を量子暗号を用いて実現
https://jpn.nec.com/press/201910/20191029_02.html

量子暗号を用いて電子カルテを秘匿し、伝送・秘密分散バックアップを行う実証実験に成功
https://jpn.nec.com/press/202010/20201022_01.html

金融分野のサイバーセキュリティ強化に向けた量子暗号技術活用の共同検証を開始
https://jpn.nec.com/press/202012/20201221_01.html

「金融分野におけるサイバーセキュリティ強化に向けた取組方針」のアップデートについて
https://www.fsa.go.jp/news/30/20181019-cyber.html

NEC 技報のご案内

NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報（日本語）　NEC Technical Journal（英語）

Vol.74 No.1　安全・安心・公平・効率を提供する社会インフラ特集

安全・安心・公平・効率を提供する社会インフラ特集によせて
社会インフラを通じて、すべての人が豊かさを享受できる社会の実現を目指すNECの取り組みについて

◇ 特集論文

社会システムのDXを実現する技術 ～ 政府・行政サービスのDX

デジタル・ガバメントを推進する、これからのクラウド活用
自治体DXに向けた取り組み
音声の可視化による学びの改革 協働学習支援ソリューション

社会システムのDXを実現する技術 ～ 放送システムのDX

映像流通DXが目指す新たな社会インフラ「映像プラットフォームサービス」
未来の放送業界のDXを支える映像符号化技術

社会システムのDXを実現する技術 ～ 空港のDX

空港の税関検査場の混雑緩和とスムーズな手続きを実現する税関検査場電子申告ゲート
顔認証を活用した新しい搭乗手続き「Face Express」（成田国際空港「One ID」）
GPSを利用した航空機進入着陸システム（GBAS）の開発
次世代に向けた航空交通管理への取り組み

社会システムを支えるセンシング技術 ～ 見えないところで活躍するセンシング技術

気候変動観測衛星（しきさい）を支えた光学センサ技術と成果
宇宙から見守るまちの安全・安心 ～衛星搭載合成開口レーダ活用サービス～
ミュオグラフィを活用した内部構造の観測
海中の音波をあやつる可変深度ソーナー
マスト中段配置型艦船用TACAN（電波灯台）アンテナの開発
画像解析を活用して鉄道の沿線検査業務を支援する「列車巡視支援システム」

社会システムを支えるセンシング技術 ～ 検知と認識のセンシング技術

電波識別技術の現状と将来
ディープラーニング技術を用いた指紋照合技術の現状と将来
顔の三次元情報の計測と顔画像照合への応用
インビジブルセンシング技術によるウォークスルーセキュリティ検査

未来の社会を支える最先端技術 ～ 社会に浸透してゆく先端技術

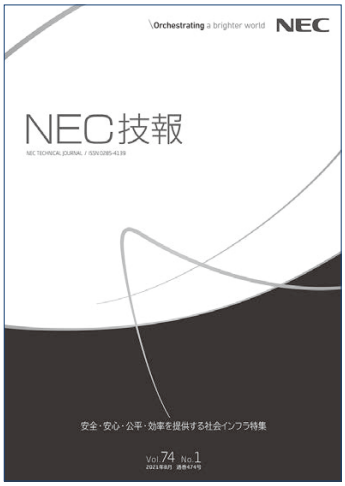
ソフトウェア無線技術のその発展と取り組み
人工衛星運用における自動化・省力化技術
光が導く次世代の暗号技術「量子暗号」
重作業の省人化・無人化を実現するロボティクス技術
海中の無人機に効率良く大電力を伝送できるワイヤレス給電アンテナの開発

未来の社会を支える最先端技術 ～ 宇宙で活躍する先端技術

はやぶさ2 イオンエンジンと今後の展望
はやぶさ2 リュウグウへの高精度タッチダウンを実現した自律航法誘導制御
はやぶさ2の快挙をセンシング技術で支えた「衛星搭載ライダー」
はやぶさ2 システム設計と運用結果
高速・大容量のデータ通信を実現する光衛星間通信技術
美笹深宇宙探査用地上局向け30kW級X帯固体電力増幅装置の開発
世界最高性能の薄膜太陽電池パドルの開発

◇ NEC Information

2020年度C&C賞表彰式典開催



Vol.74 No.1
（2021年8月）

特集TOP