SE Report

量子暗号通信、その概要と安全性

横浜国立大学 大学院工学研究院 教授
小坂　英男 Hideo Kosaka

1. はじめに

われわれは現在、Society（ソサイエティー）5.0と呼ぶ第4次産業革命を迎えつつあります[1)]。Society 5.0とは、モノのインターネット（IoT：Internet of Things）に代表されるように、ヒト（人間）だけでなくモノ（機械）同士が通信を介して情報をやり取りする（M2M：Machine to Machine）社会と言われています。いわゆるサイバー（情報的）空間とフィジカル（物理的）空間が高度に融合したサイバーフィジカル社会の到来です。人工知能（AI：Artificial Intelligence）が物流だけでなく情報流通をもビッグデータ解析して制御する超スマート社会は、情報の安全性が物理的安全性を脅かし、われわれの生活を豊かにするはずの技術が逆にわれわれの生活を脅かすという両面性をもっており、情報の高度な暗号化技術が喫緊の課題となっています。

暗号といえば、古代ローマ時代のシーザー暗号に始まり第二次世界大戦中のエニグマ暗号に至るまでの非デジタル暗号から、現代のデジタル暗号まで進化してきましたが、Society 5.0を支えるべく更なる進化が望まれています。その本命として世界中が急激に力を注ぎ始めたのが量子暗号技術です。本稿では、現代暗号から量子暗号まで全体を俯瞰し、量子インターネット社会の到来を予見します。

2. 情報セキュリティ

情報セキュリティとは、情報のConfidentiality（機密性）、Integrity（完全性）、Availability（可用性）を維持することと定義され、英語にしたときの頭文字を取り、情報セキュリティのCIAと呼ばれています。（C）機密性とは第三者によって「盗聴されない」ことです。次に（I）完全性とは第三者によって「改竄（かいざん）されない」ことです。これらCとIは、例えば中間者攻撃などの攻撃を受けないよう、通信内容の暗号化だけでなく通信相手の認証が不可欠です。最後に（A）可用性とは「情報を常に使える状態に保つ」ことで、例えば、DoS攻撃※1などを受けないことが重要になります。通常はファイアウォールなどの導入でこの可用性を確保しています。

量子暗号では量子のもつ「測定すると壊れる」性質により、CとIを同時かつ絶対的に暗号化することができます。量子的性質で認証を行う量子認証についても研究が始まっています。

3. 暗号通信方式

現代の暗号通信では2進数のビット列を暗号鍵※2として用い暗号化と復号化を行いますが、この暗号鍵を安全に通信相手と共有するための鍵配布が特に重要です。暗号鍵を直

※1
DoS攻撃（Denial of Service Attack）
サーバなどに意図的に過剰な負荷をかけたりする事でサービスを妨害する攻撃。

※2
暗号鍵
暗号化の手順を制御するためのデータ。暗号文を復号化する際にも、暗号化に対応する鍵が使用される。

接解読して情報を得ることは、一般的なコンピュータでは計算量的に不可能とされています。しかし、暗号鍵がいったん傍受されると、その鍵を使った通信内容が（場合によっては過去にさかのぼって）完全に漏えいしてしまうため、鍵配布の安全性が極めて重要です。

暗号通信には大別して共通鍵暗号と公開鍵暗号の二つの方式があります。

共通鍵暗号方式では、一つの暗号鍵を暗号化にも復号化にも使います。従って、送受信の流れは以下の方式のように至ってシンプルです。

（1）送信側は、データ（平文）を共通の暗号鍵で暗号化し、受信側へ送信する
（2）受信側は、受信したデータを同じ暗号鍵で復号化し、データを取得する

この共通鍵暗号方式では、暗号鍵を安全に配布すること自体が最重要課題となります。この問題を解決するために開発されたのが公開鍵暗号で、以下の方式が取られます。

（1）送信側は、受信側が公開している暗号鍵を取得し、データを暗号化して送信する
（2）受信側は、受信したデータを秘密にしている復号鍵で復号化してデータを取得する

この公開鍵暗号方式では、暗号化する暗号鍵は公開されていて誰でも暗号化できますが、復号化する復号鍵は暗号鍵とは異なり公開されていないため、受信者以外は復号できません。暗号鍵と復号鍵を別にし、暗号鍵を公開鍵とするも、復号鍵は秘密鍵とすることで、鍵配送の秘匿性の問題を回避しているのが公開鍵暗号です。しかしながら、暗号鍵（公開鍵）から復号鍵（秘密鍵）を推測されてしまっては台無しです。一般的な暗号化方式のRSA暗号[※3]では、素因数分解の計算困難性により、復号鍵を暗号鍵から類推することは極めて困難になっています。近年使用されるようになったDH鍵共有方式[※4]でも同様の計算困難性に基づいた安全性を保障しています。

現在の電子メールなどでも一般に使われているSSL（Secure Sockets Layer）やこれをもとにしたTLS（Transport Layer Security）と呼ぶ暗号通信方式、あるいはこれらを用いた最も一般的な通信プロトコルHTTP（Hyper Text Transfer Protocol）では、共通鍵暗号と公開鍵暗号のハイブリッド方式を採用しています。公開鍵暗号方式で受信者から送信者に向けて共通鍵を送付することで共通鍵を配布し、この共通鍵をある程度の期間使いまわしすることで、適度な安全性と高速性の両立を図っています。この際、通信相手認証のための証明書の発行が重要な役割を果たします。そのため最新の通信方式では、認証はRSAで、暗号はDHでと分けて行うことが推奨されています。このようにして、暗号通信に必要な計算負荷は年々急速に高まっており、通信のコストを圧迫しつつあります。

4. IoTとハードウェアセキュリティ

近年急速な需要の増加が見込まれているIoTでは、モノ同士が通信を介して情報をやり取りするM2Mが想定されています。このような状況では、現在一般的な通信プロトコルであるHTTPでは計算負荷が高すぎるとして、MQTT（Message Queueing Telemetry Transport）と呼ぶ、プロトコルヘッダが小さく計算負荷が軽量なため受信側の処理状況を気にせず効率よく送信可能で、双方向で1対多数の通信が可能な通信プロトコルに移行すると言われています。このようなM2M状況下では、そもそもこれまでのSSL/TLSのようにソフトウェア的に安全性を確保するソフトウェアセキュリティに頼ること自体に無

※3
RSA暗号（Rivest-Shamir-Adleman）
桁数が大きい数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つ。

※4
DH鍵共有方式（Diffie-Hellman）
離散対数問題を解くのが困難であることを安全性の根拠とする2種類の公開値と、それを元に生成した秘密値から共通鍵を生成して、以後それを共通鍵暗号の鍵として利用。

理があり、ハードウェア的に安全性を確保するハードウェアセキュリティを併用する必要が出てきます[2)]。例えば、認証にハードウェア自体のもつ固有性を利用するもので、指紋認証、顔認証、虹彩認証などの生体認証もこれに分類されます。しかしながら、近年のスマートフォンの性能向上により、ネット上に流れた高画質の写真からこれらの認証情報を簡単に引き出せる時代となり、更なる進化が要求されています。半導体回路の製造時の微細加工の工程で生じる自然の個体差（レジスト倒壊）を利用し、複製の困難性を高めたハードウェアセキュリティもその試みの一つです。

5. 量子セキュリティ

ソフトウェアセキュリティやハードウェアセキュリティのさらに先にあるのが、量子力学の原理で安全性を絶対的に確保しようとする、いわばカンタム（量子）セキュリティです。ソフトウェアセキュリティでは、公開鍵の解読を防ぐためにセッション毎に異なる暗号鍵を共有するDHE鍵交換方式※5や、成りすまし攻撃を防ぐためにパスワードを一度しか使わないSAS（Simple And Secure Password Authentication Protocol）などワンタイムパスワード認証方式が提案されています。

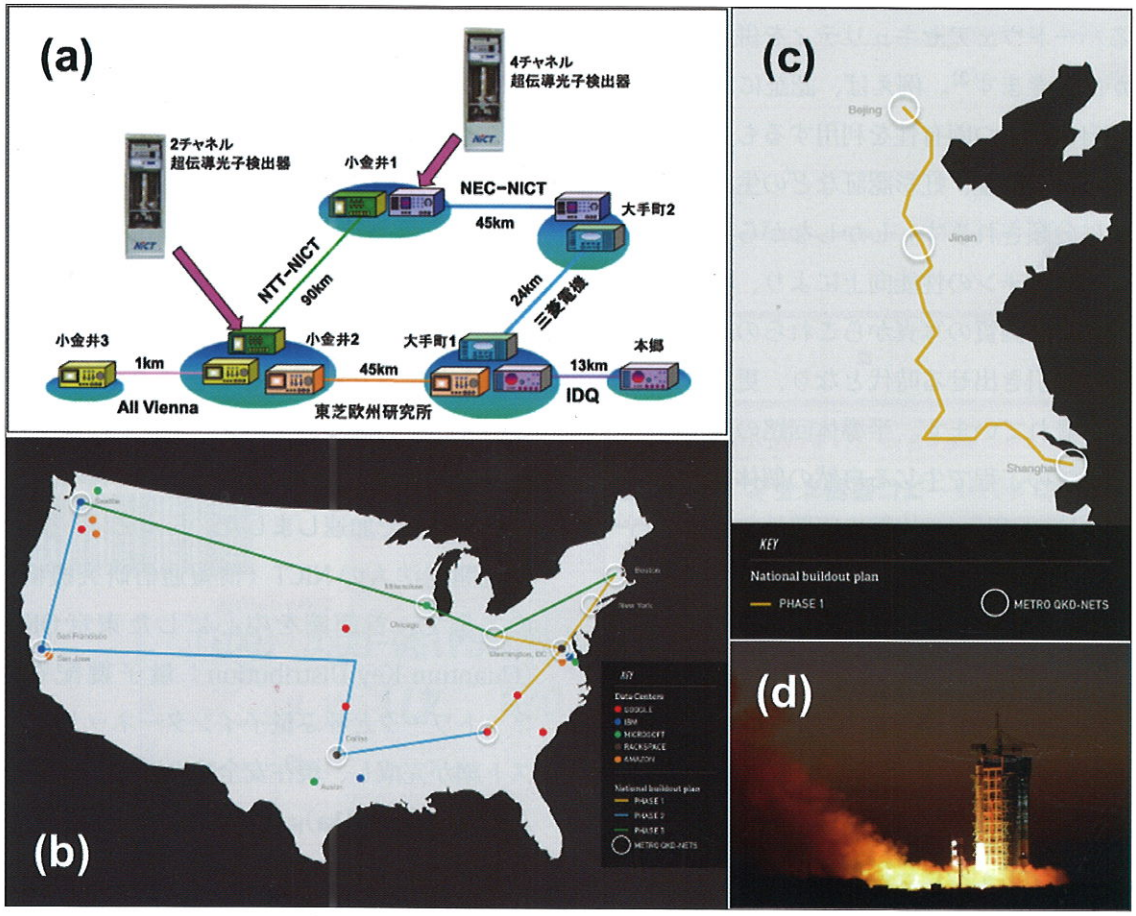
ハードウェアセキュリティでは、先に説明したような個体差を活かした計算負荷の低い認証を目指しています。一方、カンタムセキュリティでは乱数鍵をたった1回しか使わないワンタイムパッド方式となっているため、計算負荷がほぼなく絶対的なセキュリティが確保できます。一般的に量子暗号とは、通信路の暗号化により情報の安全性を保障する技術ですが、われわれの目指すカンタムセキュリティとは、暗号だけでなく認証も同時に量子化して絶対的に安全性を保障する、サイバーフィジカル空間の包括的な量子安全技術を意味しています。

6. 量子インターネット

2013年に米国のFBI（連邦捜査局）やNSA（国家安全保障局）がGoogleやYahooのデータセンター間を結ぶ専用回線で送受信されるデータを傍受していたことが発覚し、この問題を契機に、インターネットの安全性を絶対的に守る量子インターネットの開発が、世界中で加速しました。日本では、国立研究開発法人のNICT（情報通信研究機構）の主導で、首都圏を中心にした東京QKD（Quantum Key Distribution：量子鍵配布）ネットワークと呼ぶ量子インターネットのテスト網が完成し、現在安全性の運用試験が進んでいます（**図1a**）。また米国では、独立研究機関のバテル記念研究所により、東海岸のボストンから西海岸のカリフォルニアに至る米国を横断する量子インターネットの構築を進めており、まずはボストンから東南部のジョージア州までの1800 kmの構築を進めています（**図1b**）[3)]。さらに中国では、国家主導で上海から北京に至る全長2000 kmの量子インターネットを既に構築したと言われています（**図1c**）[3)]。中国は2016年8月に世界初の量子通信衛星「墨子」（Micius）を打ち上げ、本格的な量子暗号通信の利用を目指しています（**図1d**）[4)]。この他、イギリス、ドイツ、オランダ、シンガポールなどでも、量子インターネットを目指した国家規模の取り組みが次々と始まり、主導権争いが激化しています。量子コンピュータの開発で主導権を握ろうとするアメリカ、カナダ、オーストラリアの勢いと呼応し、量子通信の開発競争も激化しています。

※5
DHE鍵交換方式
（DH Ephemeral）
一時的で短命な公開値をサーバ側で動的に生成してそれを利用する方式。

図１　各国の量子インターネット構想（a）日本、（b）米国、（c,d）中国



7. 量子暗号通信

量子暗号通信は先に説明した2種類の方式のうち共通鍵暗号方式に分類できます。しかしながら、HTTP のようにソフトウェア的に公開鍵暗号方式で共通鍵を配布するのではなく、光子[※6]を送受信者でやり取りすることにより物理的に暗号鍵を配布します。この意味でハードウェアセキュリティに類似しています。量子暗号通信の特徴は、量子力学の応用で全くランダムな暗号鍵を送受信者間で自然発生的に共有することです。量子で平文(データ）を送るのではなく、暗号通信に用いる暗号鍵を得るだけなので、誤解を避けるために業界では量子暗号通信ではなく量子鍵配布（QKD）と呼んでいます。量子インターネットでは、量子鍵配布で得られた暗号鍵で平文を暗号化し、通常のインターネット回線で暗号通信を行います。

量子鍵配布には光の基本単位である光子という量子を用います。経路の途中で情報を傍受しようとする盗聴者が存在して光子の状態を測定して複製しようとすると、受信者が受け取る光子は元の状態から変化してしまう性質（量子複製不可能定理）があるため、盗聴が行われたことを知ることができます。その場合は暗号鍵を破棄あるいは量子暗号通信の経路を交換し、再度通信をやり直すことで安全な情報の伝達を可能にします。従って、量子暗号通信の利点は、不可能な盗聴者の介在の検知が極めて単純な仕組みで確実に行えることです。

一方で量子暗号通信の欠点は、通信距離と通信速度の向上が難しいことです。中継することなく量子鍵配布が可能な距離は、原理上

※6
光子
光子は光の基本単位となる粒子である。電子と共に典型的な素粒子であり、量子でもある。電子は量子メモリーに適し、光子は量子伝送に適する。光子はエネルギーや力を媒介する素粒子として知られるが、ここでは量子状態を媒介する量子として光子を用いる。

100 km 程度に過ぎません。通常の光通信では多数の光子を送受信しますが、量子暗号通信では単一（あるいは極少数）の光子を用います。このため、一度に量子鍵配布を行える距離は光子が光ファイバー中で散乱や吸収されることなく伝送できる100 km 程度に限られます。仮に1000 km の量子鍵配布を中継なく行うと、宇宙年齢（約140億年）かかっても1ビットの鍵生成もできません。

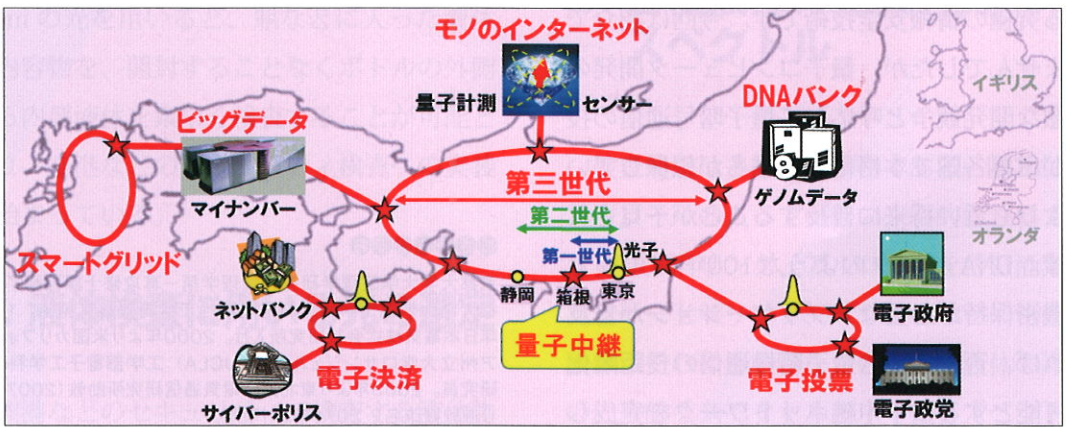
8. 量子中継

量子暗号通信の距離を現状の光ファイバーによる光子の伝送限界である100 km 程度から飛躍的に延ばすためには、量子中継[※7]と呼ぶ特殊な中継器の開発が不可欠です。量子中継では、光子数ではなく光子の量子力学的性質の中継を必要とします。通常の中継器（古典暗号通信の中継を行うので古典中継器と呼ぶことがある）では光子数を増幅して中継しますが、量子中継器では先の量子複製不可能定理のために光子数を増幅しても量子を複製できず、鍵配布の距離を延ばすことができません。そのため量子中継器では、光子を複製するのではなく量子の状態を伝言ゲームのように伝達していくことでより遠くまで暗号鍵を確実に配布します。

量子中継器の開発に向けて、以下の段階的な開発が進められています（**図2**）。第一世代暗号通信では、中継をしないので100 km 程度に留まります。第二世代暗号通信では、一度だけ中継を行うことで距離を2倍にします。このためには量子もつれ[※8]と呼ぶ量子的に相関した二つの量子を必要とします。この生成方法にもいくつかの方法があります。最初に提案されたのは「量子もつれ発光」と呼ぶ特殊な光源を用いた方法です。もう一つの方法はビームスプリッタと呼ぶ通常の光学素子を用い、離れた2点の量子メモリ間に量子もつれを測定により生成する方法です。一方、われわれの提案する方式は、「量子もつれ発光」と「量子もつれ吸収」と呼ぶ物質に内在する量子もつれを利用した方式です。第三世代暗号通信では、何度も量子中継を行うことで、量子暗号通信の距離を飛躍的に延ばすものです。このためには、量子テレポーテーション[※9]と呼ぶ原理で、量子の状態を順次転送する技術が必要です。一定間隔で配置された量子メモリ間に上記のいずれかの方法で量子もつれを生成し、各量子ノード内で二つの量子メモリの量子もつれを検出します。

われわれは、研究開始から第三世代暗号通信の実現を目指してデバイス材料と量子テレポーテーション方式の考案、実証までを進めてきました[5)-8)]。上述の「量子もつれ発光」と「量子もつれ吸収」[5)]に合わせ、「完全ベル

図2　量子インターネットの世代による距離の延長



※7
量子中継
光子が届かない遠方に量子を送るための手段。通常の通信で行われる光子数を増やす中継とは本質的に異なり、一光子を多段に用いて量子を次々と転送していく。いわゆる量子テレポーテーションを動作原理とする。

※8
量子もつれ
2つの量子の間に量子的な相関がある状態。量子的な相関とは、片方を測定したとき、その測定の種類に関わらず他方も同じ測定をしたとき一対一に対応する結果を得るもの。

※9
量子テレポーテーション
量子中継の基本原理。量子もつれにある二つの量子を用意し、この片方と別の量子との間の量子もつれを測定することで、直接は相互作用していない他方の量子に量子状態を再生するもの。

測定」と呼ぶ量子測定技術でこれを可能とします。ダイヤモンド中の単一の窒素空孔中心（NV中心）を量子メモリデバイスとして用い、単一光子から単一窒素核子への量子テレポーテーション転写と10秒間の量子メモリ時間を実証しています[6]。このような量子中継器を多段に接続することで、中継なしでは宇宙年齢で1ビットも生成できない1000 kmの量子暗号鍵の生成レートを、1 Gbps以上と飛躍的に向上することができます[8]。

9. 量子認証

量子暗号通信はあくまでも暗号鍵生成の方式に関するものです。中継部で量子中継を行わない量子リレーと呼ぶ方式の場合には、中間者攻撃を受けるリスクを完全には避けられませんが、量子中継をすれば少なくとも中継部での安全性も絶対的に守られます。しかしながら、末端である送受信者の認証の安全性はこれらの方式では守られません。われわれは、末端の認証をも量子力学的性質で絶対的に守る量子認証を目指し、研究を進めています[9]。

10. おわりに

量子暗号通信は、Society 5.0で迎えるサイバーフィジカル社会の情報セキュリティを、量子力学と呼ぶ物理法則で絶対的に守ろうとする究極の情報安全技術です。今回は紹介できませんでしたが、量子コンピュータ開発の急激な開発競争と呼応して量子暗号通信の技術が世界各国で本格化し、誰もが想像していたよりも近い将来に普及することが予見されます。DNAバンクのような100年間規模での機密保持が必要なアプリケーションが普及すれば、否が応でも量子暗号通信の長距離化を可能とする量子中継ネットワークを完成しなければなりません。それが量子インターネットという形で、われわれの気が付かないところで生活に入り込んでくる日も遠い未来ではないと思われます。本稿では、現代暗号から量子暗号まで全体を安全性の観点から比較し、来るべき量子インターネット社会に向けた量子中継の取り組みを紹介しました。

参考文献

1) 内閣府：科学技術基本計画，2016. http://www8.cao.go.jp/cstp/kihonkeikaku/index5.html
2) 電子情報通信学会：ハードウエアセキュリティ時限研究専門委員会，2017. http://www.ieice.org/~hws/index.html
3) The Verge：Building a globe-spanning quantum internet, 2014. http://www.theverge.com/2014/11/18/7214483/quantum-networks-expand-across-three-continents
4) CNN：中国、「盗聴不可能な量子衛星」を打ち上げ，2016. http://www.cnn.co.jp/fringe/35087613.html
5) Hideo Kosaka, Naeko Niikura：Entangled Absorption of a Single Photon with a Single Spin in Diamond, Phys. Rev. Lett., 114, 053603-1-5, 2015.
6) Sen Yang, Ya Wang, Thai Hien Tran, S. Ali Momenzadeh, M. Markham, D. J.Twitchen, Rainer Stohr, Philipp Neumann, Hideo Kosaka, and Jorg Wrachtrup：High fidelity transfer and storage of photon states in a single nuclear spin, Nature Photonics, 10, 507-511, 2016.
7) Yuhei Sekiguchi, Yusuke Komura, Shota Mishima, Touta Tanaka, Naeko Niikura and Hideo Kosaka：Geometric spin echo under zero field, Nature Communications, 7, 11668, 2016.
8) Yuhei Sekiguchi, Naeko Niikura, Ryota Kuroiwa, Hiroki Kano and Hideo Kosaka：Optical holonomic single quantum gates with a geometric spin under a zero field, Nature Photonics, 11, 309-314, 2017.
9) 倉見谷航洋、須田雄太、後藤優征、関口雄平、佐藤恒司、中村孝秋、石田直輝、長田昂大、小坂英男：ダイヤモンドNV中心の拓く量子認証システムの可能性，第64回応用物理学会春季学術講演会 量子情報シンポジウム，2017.

ごさか●ひでお

京都大学大学院理学研究科物理学第一専攻修士課程修了。京都大学大学院工学研究科電子物性工学専攻論文博士。1989年日本電気株式会社研究所入社。2000年より米国カリフォルニア州立大学ロサンジェルス校（UCLA）工学部電子工学科客員研究員。2003年より東北大学電気通信研究所助教（2007年より准教授改名）。2014年より現職。