量子コンピュータ時代の暗号技術
量子暗号の限界と今後の対策

＜はじめに＞

近年、量子コンピュータ※1の開発が進む中、既存暗号技術の限界が議論され始めた。きっかけは、1994年、米国ベル研究所のピーター・ショア博士（Peter Williston Shor, 1959－）によって、量子コンピュータを使用する素因数分解を実用的な時間で計算できるアルゴリズムの発表だった。これを用いると、原理的には数回から数千回程度の計算で素因数分解が可能となる。つまり、「量子コンピュータが実現すると、現在の暗号はすべて破られてしまう」というのである。

2030年頃には量子コンピュータが普及すると考えられており、2015年 8月、米国国家安全保障局(NSA)は、過去10年以上にわたって推奨してきたAES、SHA-256を含む暗号技術が、もはや安全ではないと宣言した。また、2016年2月、重要データを扱う企業や、政府各部門に対して、「量子コンピューティングの分野で研究が深まっており、NSAがすぐ行動を起こさなくてはいけないほどの進歩になっている」と、量子コンピューティングの脅威に関する詳細を発表した。

すでにNSAは、米国国立標準技術研究所(NIST)と共同で、量子コンピュータ時代以後にも使える耐量子コンピュータ暗号のいくつかの新しい標準アルゴリズムに取り組んでおり、新たなアルゴリズムの募集を行っている。欧州連合やそのほかの国でも、耐量子コンピュータ暗号や量子暗号についての取り組みが行われはじめている。

わが国でも、国立研究開発法人情報通信研究機構(NICT)が、格子理論に基づく新暗号方式「LOTUS」を開発したと発表した。NICTサイバーセキュリティ研究所セキュリティ基盤研究室が開発したもので、量子コンピュータでも解読が難しい、耐量子コンピュータ暗号として開発された暗号化方式であり、公開鍵方式として現在広く使われているRSA暗号や楕円曲線暗号は、ピーター・ショア博士のアルゴリズムを使うことで、簡単に解読できることが数学的に証明されているが、格子理論ではまだそのような効率的に解くアルゴリズムが見つかっていない。今回のLOTUSは、NISTの耐量子コンピュータ暗号において、2017年12月に書類選考を通過した69件の候補の1つに残っており、今後数年かけて各候補の評価と選定が行なわれる予定である。そのほか、KDDI総研の「線形符号の復号」、東芝の「非線形不定方程式の求解」を利用した提案も候補に残っている。

暗号技術は情報セキュリティにおける最重要技術であり、究極の暗号技術及びその実施によって、外交上、防衛上、産業上の優位を獲得できることは自明であり、各国しのぎを削ってきた。各国とも膨大な予算を注ぎ込むとともに、他国との競争に極めて敏感である。スノーデン事件※2の折には、米国による独国への諜報活動に対してメルケル首相が苦言を呈したことが全世界に知れ渡った。米国は友好国に対してさえ諜報活動を行っていたのである。当の諜報活動を暴露したスノーデン氏は今もロシアの保護下にいる。各国がどのような暗号技術をどこで用いているか。用いている暗号技術に弱点はないのか。暗号技術をめぐる競争は激烈である。世界秩序を重視しないどこか一国だけが、究極の暗号技術を手に入れたら悪夢である。この究極の技術を武器に圧倒的優位な立場を築き上げるであろう。

そんな中、中国の研究チームが、ハッキングや盗聴を不可能にする「量子暗号通信」を飛躍的に向上させた衛星実験に成功、米科学誌「サイエンス」（6月16日付）にその概要を発表した。実験に成功したのは中国

の物理学者、潘建偉氏をトップとするチーム。2016 年 8 月 16 日、中国科学院国家宇宙科学センターによって打ち上げられた世界初の量子科学実験衛星「墨子号」は 4 カ月にわたる軌道上実験の後、2017 年 1 月 18 日「光子のペアを量子もつれの状態で地上に放出」。約 1200 キロ離れた青海省と雲南省の 2 カ所で「それぞれ光子を受信することに成功した」としている。潘建偉チームは今後、7400 キロ離れた中国とオーストラリアの 2 地点での実験を計画しているということである。
米ウォール・ストリート・ジャーナル紙によると、「もし中国が量子通信ネットの確立に成功すれば、米国のコンピューター・ネットワークにおける優位性が減衰する」（6 月 15 日）とされるが、暗号通信ネットワークは、今後中国優位のまま推移していくのであろうか？

＜暗号技術の基礎＞
暗号技術は、暗号アルゴリズムと暗号鍵から構成される。古代ローマのガイウス・ユリウス・カエサル（Gaius Julius Caesar、BC100 – BC44）が使用したとして知られる「シーザー暗号」では、アルファベット順に文字をずらすというアルゴリズムであり、何文字ずらすかが暗号鍵となる。CAT を 1 文字ずらせば DBU、2 文字ずらせば ECV となる。しかしながら、アルファベットの文字数は 26 なので、暗号文に対してたったこれだけの暗号鍵をすべて試せば平文が判明してしまう。例えば、2001 年宇宙の旅で有名な人工知能 HAL は 1 文字ずらすだけで IBM となり、著者が裏に隠した言葉が容易に見つかる。したがって、暗号を強化するためには、①暗号アルゴリズムをもっと複雑にするか、②暗号鍵の場合の数を増やすことが考えられる。シーザー暗号を強化したいなら、文字をずらすだけでなく文字を入れ替えたりノイズ文字を入れたりする。数字やアラビア文字を使えるようにすれば暗号鍵の数は増える。ところが、①、②のどちらの方法を極めても、解読不可能な暗号は作れない。現在の暗号技術のほとんどは、解読困難性を、解読に膨大な計算量が必要であることを拠り所としており、決して解読不可能とは言えない。それゆえ、コンピュータの性能が向上すると、解読される可能性が高まるので、2010 年問題[※3]のように、より難解な暗号アルゴリズムを用いたり、暗号鍵長を長くして場合の数を増やすように変更したりする必要があり、その都度対応してきた。量子コンピュータ時代においては、上記のような耐量子コンピュータ暗号技術が必要となる。しかし、量子コンピュータがさらに発展する近未来においては、やがて理論的に解読不可能な暗号技術が求められる。
この人類史上の難問に答えを出したとされるのが、AT&T に勤務していたギルバート・ヴァーナム（Gilbert Sandford Vernam、1890 – 1960）によって 1918 年に考案された暗号方式であり、1949 年にクロード・シャノン（Claude Elwood Shannon、1916 – 2001）によって、ある条件下において解読不可能であることが証明されたものである。これは、ヴァーナム暗号またはワンタイムパッドと呼ばれ、事前に暗号者と復号者の間で共有する暗号鍵が、ランダムで、かつ、その鍵の長さが送信される平文と同じかそれ以上の長さを持つ場合に、解読不可能となるものだが、これまで、これほどの長さの暗号鍵を共有することは、実用的でないとされてきた。平文と同じ長さの暗号鍵が共有できるのなら、平文自体を共有すればよいからである。
このように、現在、究極の暗号技術を開発する上での最終課題となっているのが、「解読不可能な暗号技術問題」と「暗号鍵の配送問題」の 2 つである。「暗号鍵の配送問題」が解決すれば、ヴァーナム暗号などの「解読不可能な暗号技術問題」を解決した暗号技術を用いることができ完全秘匿通信が可能になる。
この「暗号鍵の配送問題」を解決したとされるのが、「公開鍵方式」である。この方式は大きな欠陥を抱えながらも、現在広く世界中で使われている。さらにその究極のソリューションとされているのが、量子暗号を用いる量子鍵配送（QKD）である。

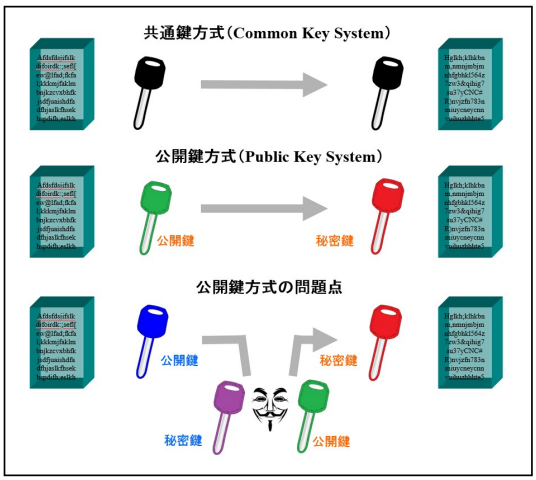
＜公開鍵暗号方式とその欠陥＞

公開鍵暗号は、現在インターネットセキュリティを中心に、最も広く使用されている暗号方式である。暗号者と復号者の間で暗号鍵を事前に共有しなければならない共通鍵方式の最大の問題点である「暗号鍵の配送問題」を克服するため、1970 年代に、英国においてはジェームス・エリス（James Henry Ellis、1924 - 1997）とクリフォード・コックス（Clifford Christopher Cocks、1950 - ）及びマルコム・ウイリアムソン（Malcolm John Williamson、1950 - ）によって、米国においてはスタンフォード大学のホイットフィールド・ディフィー（Bailey Whitfield Diffie、1944 - ）とマーティン・エドワード・ヘルマン（Martin Edward Hellman、1945 - ）によって考案された。公開鍵方式では暗号化する暗号鍵と復号化する暗号鍵が異なるペアによって構成される。公開鍵で暗号化した暗号文はこれと一対をなす秘密鍵によってしか復号化できない。もしこのような一対の鍵が存在する時において、秘密鍵を持つ側に送信される情報はすべて公開鍵によって暗号化されれば、唯一秘密鍵を持つ者だけしか復号化できない。万一ハッカーが公開鍵を手に入れたとしても復号化はできないのである。その結果、公開鍵は誰にでも公開し、いつでも使えるようにしておくことができるので、公開鍵方式（PKS）と呼ばれるようになった。

一般に、公開鍵から秘密鍵を導き出すのに、現実的には不可能なくらいのコンピューティングパワーと時間が必要とされ、よって実質上解読できないとされてきた。RSA 暗号においては、「素因数分解問題」、楕円曲線暗号においては「楕円曲線離散対数問題」と呼ばれる数学的問題を利用している。ところが、共通鍵方式に比べて長大な暗号鍵を用いるため計算時間が膨大に必要で、共通鍵方式の暗号鍵の配送に用いられることが多くなり、現在では「暗号鍵の配送問題」を解決した暗号方式と考えられるようになっている。公開鍵方式では公開鍵を予め公開しておけるので、インターネット時代に最適で、電子入札や SSL、ブロックチェーンなど、広く使われている。そのため、コンピューティングパワーが向上するにつれて解読の可能性が高まったため、その都度脆弱性を克服するために鍵長を長くする試みが行われてきた。しかし、いよいよ量子コンピュータ時代を迎えるにあたり、鍵長を長くするだけでは解決できなくなり、前述の通り、米国 NIST などが、量子コンピュータ時代以後にも使える耐量子コンピュータ暗号の新しい標準アルゴリズムに取り組み始め、新たなアルゴリズムの募集を行っているのである。

しかしながら、より根本的な問題として、公開鍵の真正性の保証が容易ではないという問題が露見し、現在では、信頼できる第三者機関（Trusted Third Party、TTP）が発行する公開鍵証明書※4 を用いる公開鍵基盤（PKI）と呼ばれる方法が考案され広く使われている。ところが、証明書をいくらつけても、さらに証明書の証明書であるルート証明書を用いても、偽造が防げないことが明らかとなっており、当初期待された「暗号鍵の配送問題」さえも、解決されないことが判明している。

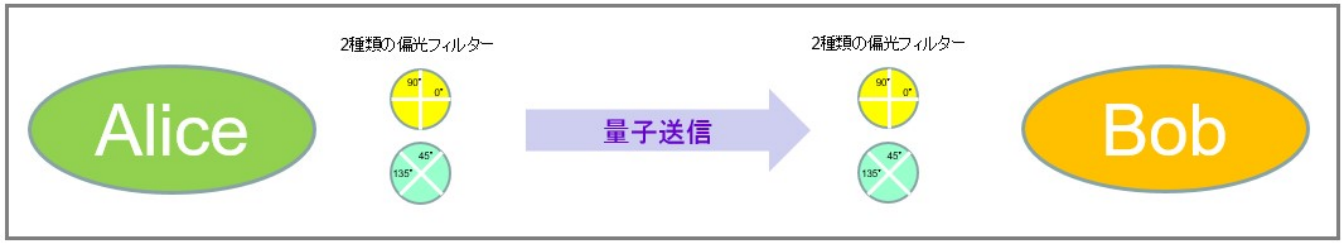
そこで考案されたのが、量子鍵配送（QKD）である。



＜量子暗号とその限界＞

量子の特性を利用して秘匿通信を行う量子暗号と呼ばれる技術が注目されている。量子暗号は、量子力学と情報理論を融合した量子情報科学から生みだされ、「状態の重ね合わせ」や「量子のエンタングルメント」、

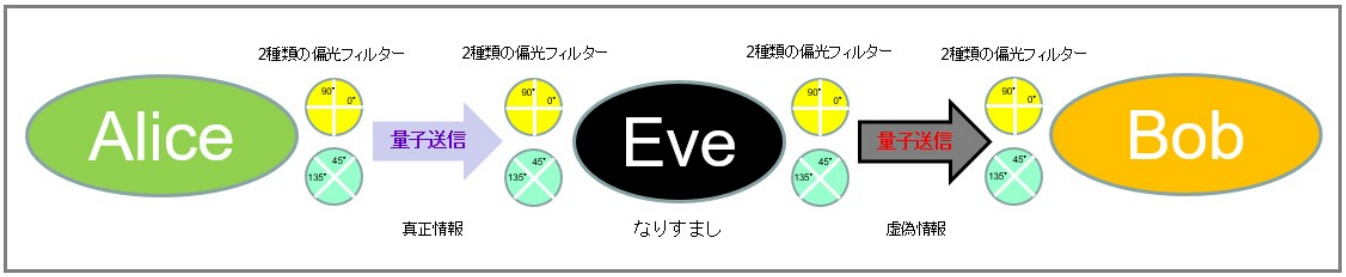
「量子テレポーテーション」を利用する。
当初量子暗号は、量子 1 個の状態の重ね合わせの性質を利用した共通鍵の配送方法として考案された。不確定性原理に支配された量子は、観測によって重ね合わせ状態が解消する。送信者（Alice）が受信者（Bob）に量子を送信する際、盗聴者（Eve）によって量子が観測されると、量子の状態が定まってしまい、観測前の状態が分からなくなってしまう。つまり盗聴していることがばれる。1984 年、IBM ワトソン研究所で量子コンピュータを研究していた物理学者チャールズ・ベネット（Charles Henry Bennett、1943 － ）とモントリオール大学の数学者ジル・ブラサール（Gilles Brassard、1955－ ）によって最初の量子暗号 BB84 が発表された。以下 BB84 の仕組みについて説明する。



BB84 では、「０°　と 90°」と「45°　と 135°」の 2 組の偏光フィルター、4 種類の偏光を用いる。Alice がデータを送る際、1 ならば 0°か 45°、0 ならば 90°か 135°のどちらかにランダムに偏光させる。一方 Bob は、同じ 2 種類の「０°　と 90°」、「45°　と 135°」の偏光フィルターを用いて受信する。Bob がどちらの偏光フィルターを用いるかランダムに決めれば、2 分の 1 の確率で正しく受信することができる。例えば、Alice が 1 を「０°　と 90°」の偏光フィルターを使って送信し、Bob が同じ「０°　と 90°」の偏光フィルターを使って受信すれば正しく受信できるが、「45°　と 135°」の偏光フィルターを使って受信すれば正しく受信できない。一連の送信が終わった後、通常の通信回線を使い Alice と Bob はどの偏光フィルターを使ったか確認し、正しく送受信できたものだけを選んで暗号鍵として用いる。こうして暗号鍵の配送が安全に行われる。
Eve が盗聴する場合を考えると、Eve は観測したあと、観測前と全く同じ状態の量子を複製して Bob に送信するしかない。詳細は省くが、Alice が光量子 1 個を送信した場合に Eve の存在を見破ることのできない確率は 75%となる。しかも、未知の状態の量子は複製できないことが知られているので、盗聴は必ずばれるということになる。
このほか QKD として、量子のエンタングルメントを利用したイギリスの物理学者アルトゥル・エカート（Artur Konrad Ekert、1961－ ）による E91 が知られている。エンタングルメント状態にある 1 対の量子は引き離してもその状態が保たれる。観察されるまでは「UP」と「DOWN」の重ね合わせ状態をとっており、観察されるまでどちらかに決まることはない。ところが、片方が観察され、例えば UP と決まれば、必ずもう一方は DOWN となる。この特性を使えば暗号鍵の配送ができるが、数学的には BB84 と同じと考えてよい。
ところで、鍵配送ではなく、量子の特性は本文そのものを送信するのには使えないだろうか？
暗号鍵を共有しているとの前提であれば、本文そのものの量子暗号通信はいろいろと考案されてきた。ベネットとブラサールは、BB84 を発表する前、前述の 2 つの偏光フィルターをどの順番で使うかという暗号鍵情報を共有したうえであれば、Alice と Bob が量子を 1 つずつ安全に送信できることを発表している。また、量子雑音を用いる方法も数々考案されている。
以上の通り、QKD によって暗号鍵が安全委配送できるので、その暗号鍵を使ってヴァーナム暗号や量子暗号

通信を用いれば完全に安全な秘匿通信が可能と考えられる。現時点で残る問題点として考えられている、伝送距離については、量子テレポーテーションを使えば中継ができ距離を延ばせる。また前述の通り中国は1200 kmの長距離伝送に成功したと発表している。また、単一光子を使用する場合伝送速度に制約が残るが、レーザーなどを使う方法が考案されている。

しかし、量子暗号を使ってさえも、必ずしも真正な相手と通信できないという、送受信者同士の認証問題はまだ解決されていない。Eve が Bob になりすましてしまえば、Alice と直接量子暗号を用いた通信を行い、すべての情報を手に入れたうえで、正しい情報、または虚偽の情報を Bob に再送することができるのである。



＜まとめ＞

膨大な必要計算量に依存してきた従来の暗号技術は、量子コンピュータの実用化が間近に迫った現在、最早十分安全とは言えなくなった。そこで各国とも耐量子コンピュータ暗号の開発に着手した。

人類はすでに、暗号技術の最終課題である「暗号鍵の配送問題」と「解読不可能な暗号技術問題」の 2 点のうちの後者を解決するヴァーナム暗号を手に入れており、前者の共通鍵の配送問題（事前共有）が成功すれば、完全な秘匿通信技術が手に入るはずであった。そのため、公開鍵方式（PKS）、公開鍵基盤（PKI）、量子鍵方式（QKD）が次々に開発されたが、なりすまし攻撃を防御する「送受信者同士の認証問題」はまだ解決できていない。つまり、「暗号鍵の配送問題」は解決していない。

この「暗号鍵の配送問題」を解くには、本学会機関誌 2017 年冬号（vol.42）と 2018 年春号（vol.43）にて、送信者と受信者のお互いだけしか知らない「Shared Secret」が必須であり、これがあれば、「Remote Synchronization」が確立されることを説明させていただいた。

繰り返すが、暗号技術は情報セキュリティにおける最重要技術であり、究極の暗号技術及びその実施によって、外交上、防衛上、産業上の優位を獲得できることは自明である。今すぐ最新の暗号技術を用いたインフラを構築できる国こそが競争優位を得ることは必至だ。

第一段階として、最も困難とされる「暗号鍵の配送問題」を解決するインフラを構築する。その上であれば、現状の AES 暗号を用いても今は十分安全である。量子コンピュータ時代に真っ先に危機に陥るのは長大な暗号鍵が必要な公開鍵方式であり、共通鍵方式である AES 暗号はしばらく安全と考えられるからである。次に第二段階として、量子コンピュータが共通鍵方式に脅威を与えるようになる前に、AES 暗号を、ヴァーナム暗号や量子暗号通信などの論理的または物理的解読不可能を証明された暗号アルゴリズムに変更する。現在すでにヴァーナム暗号や量子暗号通信に比べても、格段にシンプルで効果的な解読不可能なアルゴリズムが開発されており、第三段階ではこの最終的な暗号アルゴリズムを導入することで完成する。

平和を追求する日本がその最初の国となることを期待したい。

※1. 量子コンピュータ

量子コンピュータは、量子力学的な重ね合わせを用いて並列性を実現するとされるコンピュータ。従来のコンピュータの論理ゲートに

代えて、「量子ゲート」を用いて量子計算を行う原理のものについて研究がさかんであるが、他の方式についても研究・開発は行われている。いわゆる電子式など従来の一般的なコンピュータ（以下「古典コンピュータ」）の素子は、情報について、「0 か 1」などなんらかの 2 値をあらわすいずれかの状態しか持ち得ない「ビット」で扱う。量子コンピュータは「量子ビット」（キュービット）により、重ね合わせ状態によって情報を扱う。n 量子ビットがあれば、2^n の状態を同時に計算できる。もし、数千 qubit のハードウェアが実現した場合、この量子ビットを複数利用して、量子コンピュータは古典コンピュータでは実現し得ない規模の並列コンピューティングが実現する。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/量子コンピュータ/）

※2. スノーデン事件

スノーデン事件とは、米国家安全保障局（NSA）がテロ対策として極秘に大量の個人情報を収集していたことを、元 NSA 外部契約社員のエドワード・スノーデン容疑者(30)が暴露した事件。米中央情報局（CIA）の元職員でもあるスノーデン容疑者は、香港滞在中の 2013 年 6 月上旬、英米紙に対して NSA の情報収集活動を相次いで暴露した。米通信会社から市民数百万人の通話記録を入手したり、インターネット企業のデータベースから電子メールや画像などの情報を集めていたりしたという。

(出典：THE PAGE　https://thepage.jp/detail/20130718-00010002-wordleaf /)

※3. 2010 年問題

標準的に利用されている暗号アルゴリズムや鍵長について、米国標準技術研究所(NIST)が 2010 年までに廃止及び移行を打ち出したことに端を発した問題。2010 年に移行対象となっている暗号については、例えば共通鍵暗号では「2-key Triple DES」から「AES」へ、公開鍵暗号では 1024 ビットの鍵長を持つ「RSA」や「DSA」から 2048 ビットの鍵長への移行が望ましいとされた。

(出典：日立ソリューションズ　情報セキュリティブログ　https://securityblog.jp/words/675.html /)

※4. 公開鍵証明書

公開鍵証明書は、公開鍵暗号を広い範囲で使用する場合に用いられる。ユーザー同士で暗号鍵を直接やりとりするのは、よほど小さなネットワークでない限り実用的ではない。公開鍵暗号はこの鍵配送の問題を回避する手段を提供する。

例えばある通信当事者（ここではアリスと呼ぶことにする）に対して他の通信当事者たち（たとえばボブなど）が秘密のメッセージを送りたいとき、アリスは公開鍵を作成してボブらに公開すれば、ボブや公開鍵を入手した誰でもアリス宛てのメッセージを暗号化でき、アリスはそれを復号することができる。だが、盗聴者（ここでは仮にイブと呼ぶことにする）が作成した公開鍵でも、それをアリスの公開鍵であるとして配布できてしまうため、この偽の公開鍵を受け取った人のメッセージはイブに復号されてしまう。これを回避するために、ユーザー同士で直接に公開鍵をやりとりするのでは、鍵配送の問題は解決されない。

そこで、信頼できる第三者機関（Trusted Third Party、TTP）として振る舞う人（ここでは仮にトレントと呼ぶことにする）が、アリスの公開鍵の証明書を作成すると、トレントを信頼する誰もが、「証明書に記載されている公開鍵がアリスの物である」ということを証明書の署名を確認するだけでよくなる。このように、公開鍵とその正当な所持者の関係を証明するために公開鍵証明書が用いられる。

(出典：Wikipedia　https://ja.wikipedia.org/wiki/公開鍵証明書/)