NAD Monthly Report.

Market Flash

量子コンピューターの世界　No3
～加速化する新世界～

2022.06

日本アルプス電子株式会社
NIHON ALPS ELECTRONICS CO.,LTD.

～量子コンピューター～

2回にわたり「量子コンピュータ」の仕組みについてみてきたが、その本格的な稼働にはまだ数年或いは数十年かかると言われている。一方で、突然大規模な量子コンピュータの開発技術が発見され数年以内に実用化されるという見方もある。いずれにしても将来的に量子コンピュータが開発され科学・化学・医療などの分野で飛躍的な技術革新が進むものと思われる。
一方で、このような量子コンピュータの開発が進めば、現在のコンピュータでは決して解くことができない暗号（実際には解くのには数年かかるような暗号）が、量子コンピュータの開発により数秒で解読されてしまう危険性（危殆化する）が現実となる。そのため、各国は安全保障上の問題から量子コンピュータでも解読が不可能な「量子暗号」の開発を急いでいる。
そこで今月はこの「量子暗号」についてまとめてみた。

まず基本用語の解説
基本的用語：「暗号化」「復号」「平分」「暗号文」「暗号アルゴリズム」「鍵」
「暗号化」：「意味の分かる情報（そして、知られたくない情報）を「何らかの手段」によって、「意味の分からない情報」に交換すること
「復号化」：「意味の分からない情報」を「意味の分かる情報」に戻すこと
「意味の分かる情報」を「平文」（ひらぶん）、「意味の分からない情報」を「暗号文」という
「何らかの手段」に相当するのが、「暗号アルゴリズム」と「鍵」となる

１．現在の暗号通信
現在の暗号方式には、「共通鍵暗号方式」（暗号化時と復号化時で使用する鍵が共通の暗号）と「公開鍵暗号方式」（暗号化時と復号化時の暗号が異なる鍵を使用する）とがある。
データサイズの小さい鍵情報には公開鍵暗号方式を、データ自体は共通鍵暗号方式でやり取りするのが一般的だ。

（１）公開鍵暗号方式　（PKI：Public－Key　Infrastructure ）
現在の世の中で最も普及している暗号・認証基盤であり、その中でも、「RSA暗号」と「楕円曲線暗号」という方式が一般的となっている。

「RSA暗号」とは、素因数分解を基盤とした暗号で、現在のコンピュータではその暗号を解くのに何年もかかるということから破られることのない暗号と考えられている。

「楕円曲線暗号」は、離散対数問題がその基盤となっている。離散対数問題とは、ある計算の結果から簡単には逆算できないような数学上の問題の一つで、整数のべき乗（2の3乗」、3の4乗などの累乗に限らず、3のマイナス2乗、5の2分の1乗などと言った値も含めた『aのｎ乗』の形で表される数のことを『aのべき乗』という）を素数で割った余りを求める計算で、アルゴリズムの基礎として用いられている。

このように現際は、これらの決して現在のコンピュータではその暗号を解くのに何年もかかる暗号形式として用いている。

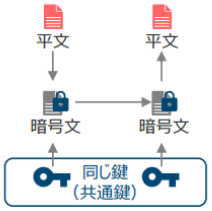
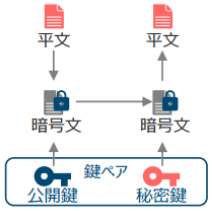
（２）共通鍵暗号方式

共通鍵暗号方式の「代表的な暗号化アルゴリズム」がＡＥＳ（Advanced Encryption Standard）と呼ばれる方式。

共通鍵暗号方式と呼ばれる理由は、まさに暗号化と復号化の鍵が共通しているからで、以下のようなメリットとデメリットがある。

メリット：ファイルやデータの暗号化にかかる処理速度が早い（公開鍵方式の1/1000以下）

デメリット：データを送る人の数だけ管理する鍵が増える。送信した鍵が第三者に盗まれる危険がある

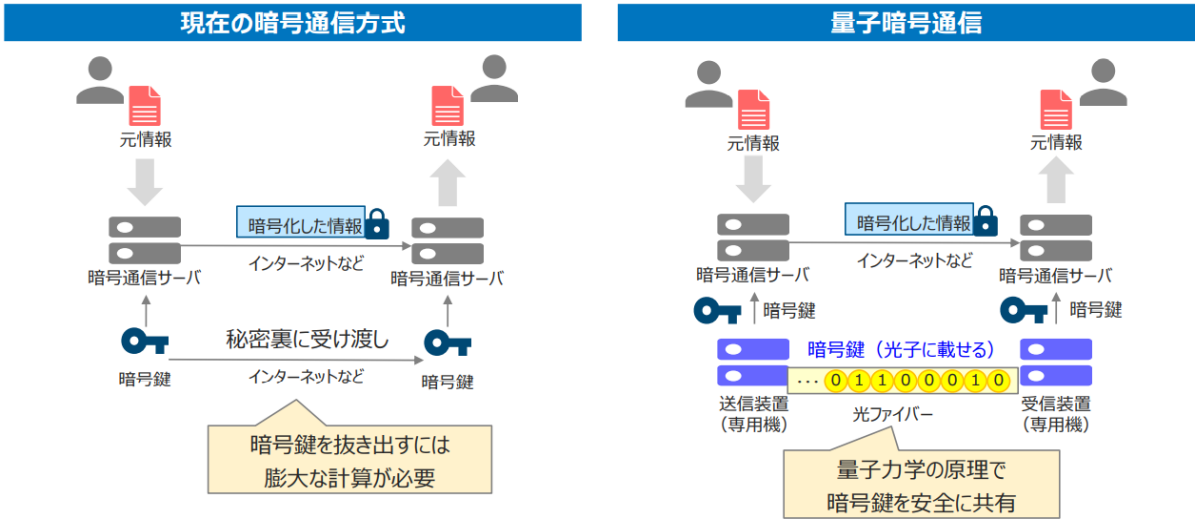
		共通鍵暗号方式	公開鍵暗号方式		
概略図					
概要		• 同じ鍵を用いる（共通鍵） • 暗号化する人と復号する人の間で鍵を事前に共有する	• 公開鍵を用いて暗号化、 秘密鍵を用いて復号する		
メリット		• 暗号化が高速 (公開鍵暗号の1/1000以下)	• 鍵の事前共有が不要 • 公開鍵を知る人は誰でも暗号化できる		
デメリット		• 安全な鍵共有が困難	• 計算速度が遅い		
主な用途		• データ自体の暗号化	• 鍵の共有、デジタル署名		
方式例	暗号名	AES暗号、ワンタイムパッド暗号	**RSA暗号**	**楕円曲線暗号**	準同型暗号
	安全性の根拠	－	素因数分解	離散対数問題	最短格子問題
	耐量子性	有り	無し	無し	有り

２．量子暗号の概要

量子暗号通信とは、暗号鍵を分割して量子の一種である「光子」（光の最小単位）に載せて送ること。

「量子コンピュータ」のレポートで見てきたように、量子暗号は光子が持つ量子力学の性質（観測する状態が変わる性質）を用いて、盗聴などがあった場合には鍵を無効化し再生成することができる。100年以上にもわたって研究されてきた量子力学のこの原理に基づいた暗号であることからその原理に矛盾があるという理論が確認されない限り安全性が担保されていることになる。

もう少し詳しく言うと、量子力学の基本原理とは、「粒子の位置と運動量を同時に確定することはできない」というハイゼンベルグの不確定性原理と、「量子は、観測することにより発生する相互作用でその状態を変える」という量子の観測不可能性により保証される。



～量子暗号～

この原理をもっとわかりやすく説明すると（ＴＤＫのＨＰから抜粋）

「話を分かりやすくするために、2人の人が、粒子を使って情報を送信する例を考えます。暗号業界の決まりごとでは、送信者がアリス、受信者がボブと決まっているそうですので、それに従いましょう。情報を送る時に使う粒子に「色」と「形」という2つの性質があると考えます。使用する粒子の色が赤い時は1、青い時は0を表すものとし、形が立方体の時は1、球の時は0をあらわしているとします。

アリスが「1」という情報をボブに送ろうとする時、「色」を指定して粒子を選ぶか、「形」を指定して粒子を選ぶかをランダムに選択できます。「色」と「形」の両方を選択することはできません。これが、ハイゼンベルグの不確定性原理（どちらか一方を確定するともう一方は確定できない）にあたります。

アリスが「色」を選択した場合、1をあらわす色は「赤」なので、「赤い立方体」か「赤い球」がそれぞれ50%の確率でボブに送られます。どちらが送られたかをアリスは知ることができません。

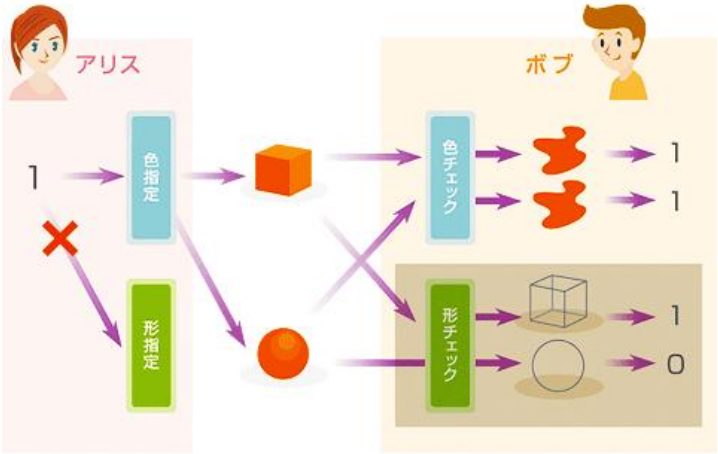
受け取ったボブは、送られてきた粒子の「色」を調べるか「形」を調べるかをランダムに選択できます。どちらを選ぶか、確率は50%です。「色」を調べた場合、送られてきているのは形はどうであれ赤いことは間違いないので、100%の確率で「1」という情報が得られます。一方、「形」を調べた場合、不確定性原理により、立方体である確率は50%、球である確率も50%です。つまり、「1」という情報が得られる確率は50%になります。「色」を調べた場合と「形」を調べた場合を総合すると、75%の確率で正しい情報が伝わり、25%の確率で間違った情報が伝わっていることになります。

ここで、色を調べたのか、形を調べたのかを、ボブはアリスに報告します。アリスは、ボブからの報告で、同じものを調べていれば情報は確実に伝わっているので、その情報を活かします。違うものを調べていた場合は、間違った情報が伝達されている可能性があるので、その情報はお互い破棄してしまいます。

これを繰り返すことで、任意の個数の粒子を、アリスからボブに送信し、秘密鍵を共有することができます。

■ 盗聴は必ずばれてしまう！
さてここで、途中に盗聴者イブがいる場合を考えます（暗号業界では盗聴者の名前はイブということに決まっているそうです）。
途中でイブに盗聴される場合ですが、イブも受信した粒子の色か形、どちらか一方しか調べることができません。つまり、イブは25%の確率で、受け取った粒子の観測結果から、間違った情報を得ることになります。

アリスからボブへの量子による情報伝達



アリスは送信時に色か形のどちらかしか指定できず、ボブは受信時に色か形のどちらかしか調べられない。
2人の指定が一致した粒子だけを有効なデータとして生かすことで、正しい情報が送信される。

一度イブが傍受した粒子は、量子の観測不可能性により、性質が変わってしまっているため、アリスが送ったものとは異なっています。盗聴していることをアリスとボブに気付かれないためには、イブは自分が観測したものと同じ粒子をボブに送信しなおすしかありません。

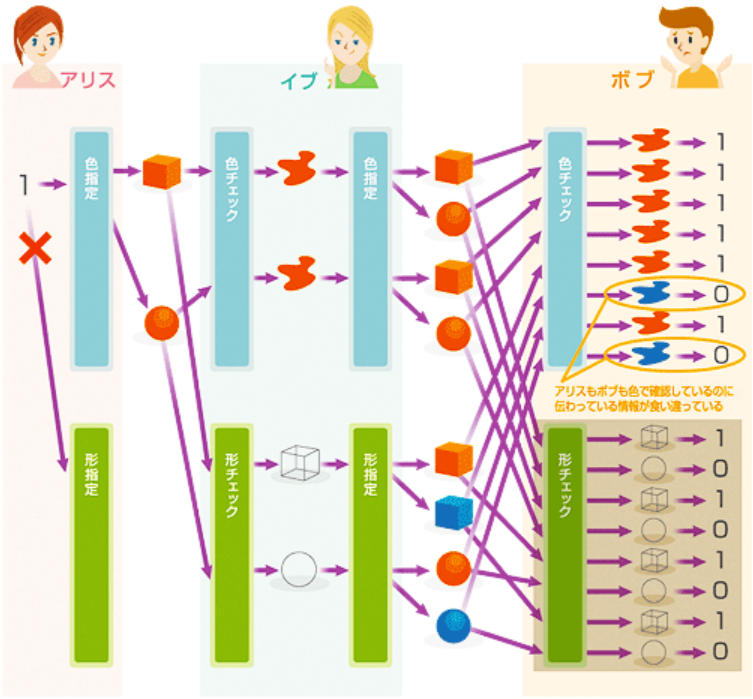
～量子暗号～

しかし、送信時に指定できるのは、「色」か「形」どちらか一方でしかないのです。そして、25%の確率で間違った情報を得ているイブは、一定確率で「青」の粒子を送信してしまう可能性があります。

イブに盗聴されていないかどうかを確認するためには、アリスとボブは、鍵が完成した後、ランダムなビットをいくつか抜き出して、情報が正しいか間違っているかを確認します（チェックビットの確認）。盗聴されていなければ、情報は100%正しいはずですが、イブに盗聴されていれば、一定確率で間違いが見つかるはずです。この間違いを検出できれば、盗聴されていることが確認できるので、この鍵は使うのを中止して新たな鍵を作り直せばよいのです。
チェックビットの確認で間違いがないことが確認できれば、その秘密鍵は、絶対に誰にも盗まれていないことが保証されます。従来の暗号のように、「時間がかかりすぎるから事実上解読不可能」なのではなく、物理学的に盗聴されていないことが保証されているのです。

鍵の共有が完了したら、アリスは、完成した秘密鍵で、文書を暗号化して、光ケーブルなどの通常の通信で送信します。元の平文の長さと同じ長さの秘密鍵で暗号化された文書は、元の秘密鍵を知らなければ復号できないことは数学的に証明されているので、途中で傍受されても第三者に復号されることはありません。暗号化された文書を復号できるのは、秘密鍵を共有しているボブだけです。こうして、理論的に絶対に安全な暗号通信が可能になります。

途中でイブに盗聴された場合の、アリスからボブへの量子による情報伝達



盗聴者イブが介在することで、アリスとボブの指定が一致しても、間違った情報が一定の確率で送信される。
最終的に受信した情報の一部を任意に抜き出して調べることで、食い違いがあれば盗聴者の存在が検知できる。

実際の量子暗号通信に使われるのは光子で、上の説明の「色」や「形」にあたるものとしては偏光（光の波の向き）、位相、スピンなどさまざまな手法があります。

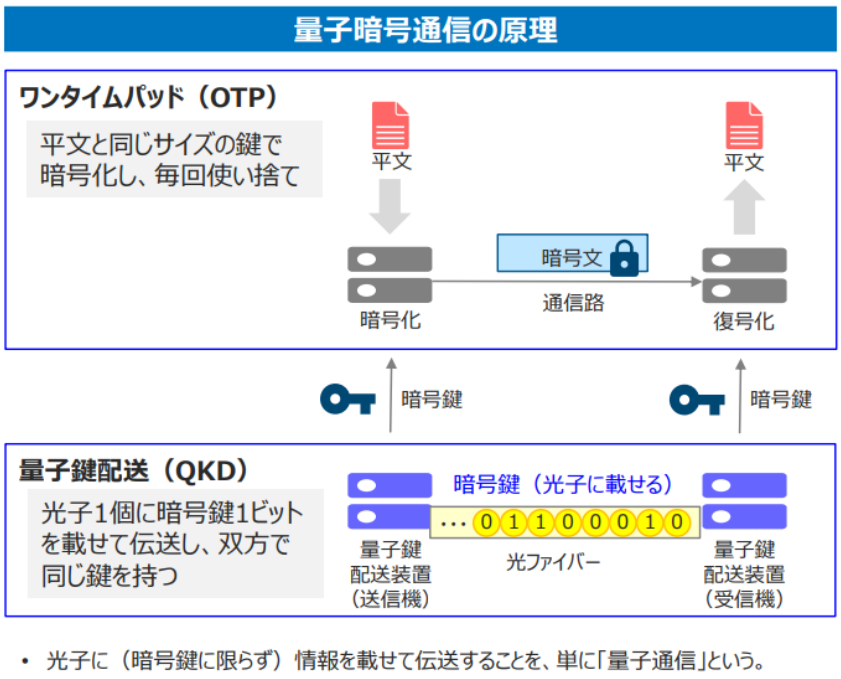
1個の光子に情報を載せて一定間隔で送信する必要がありますが、光子1個ということはとても弱い光なので、安定して遠距離に届ける技術が課題になります。
2007年6月に、NTT物性科学基礎研究所などのチームが、世界最長の送信距離200kmを達成し、「絶対に安全な暗号」の実用化に向けて大きく前進しました。」

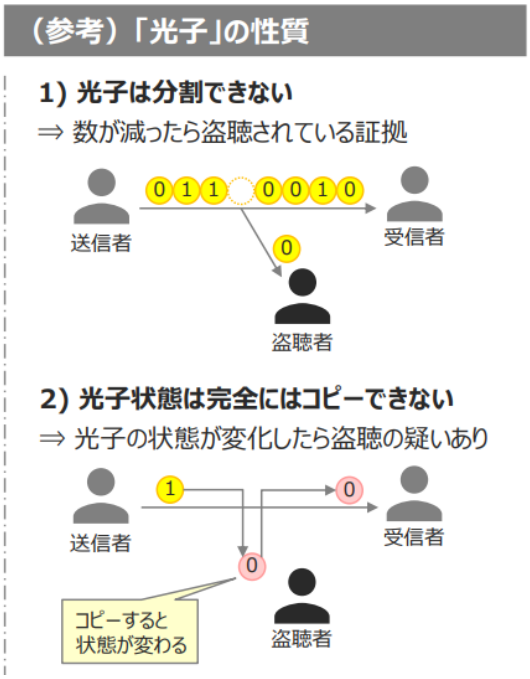
以上が量子暗号の概念である。この光子の量子的振る舞いに基づき、盗聴されていないことが補償された「量子暗号鍵」を光子に乗せて送ることが量子暗号通信ということである。

～量子暗号～

3．量子暗号通信

量子暗号通信とは、暗号鍵を分割して量子の一種である「光子」（光の最小単位）に乗せて送ること。
量子暗号通信の原理は、「ワンタイムパッド」と「量子鍵配送」との2つの部分からなる。





（1）ワンタイムパッド

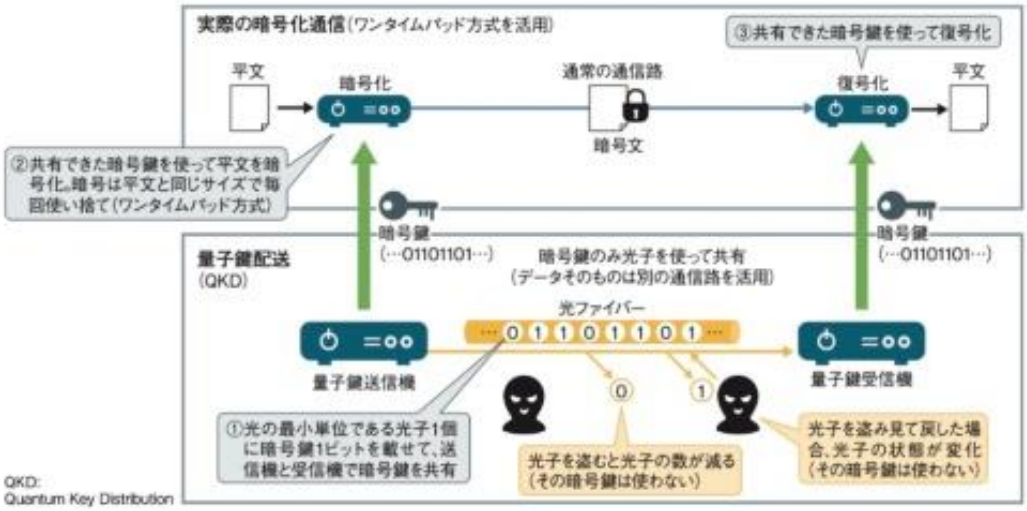
ワンタイムパッドとは、送受信するメッセージと同じ長さの乱数を、事前に送信者と受信者で共有しておき、その乱数を暗号鍵として使用することで、メッセージを暗号化/復号するもの。ただし、1回使用するごとに、その暗号鍵は破棄する。
このようなワンタイムパッドと呼ばれる暗号化/復号の方式は、絶対に解読できないことが1940年代に数学的に証明されている。しかし、簡単でしかも絶対安全なこの方式がなぜ今使われていないのか、それは平文と同じ長さの鍵を安全に共有するのは現実的ではなかったから。ところが、量子力学を応用した量子鍵配送によってこの欠点を補うことができるようになった。

（2）量子鍵配送

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。
その仕組みは、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。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かない（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、盗聴の判別ができる。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る。（これは前述の量子力学の原理である）
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る。

～量子暗号～

量子鍵配送を実現するプロトコル（方式）として複数考案（ＢＢ８４方式、ＣＶ－ＱＫＤ方式）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る。日本ではＮＥＣや東芝が先行している。
世界で実証が進む代表的な量子暗号通信が「BB84」と呼ばれる方式だ。光ファイバーの両端に送信機と受信機を1対1で配置し、暗号鍵を光の最小単位である単一光子に乗せて送る。
光は粒子に加えて波としての性質も持つ。光子の特定の振動方向に対して「1」もしくは「0」の値を割り当て、複数の光子をビット列として扱うことで暗号鍵を作り、送信機と受信機の間で共有する仕組みだ。
なお単一光子を使ってやりとりするのは、あくまでデータを暗号化する暗号鍵だけ。実際のデータの送受信は通常の通信路を使う。



しかし、量子暗号の弱点として、微弱な粒子である光子を利用するため、伝送距離を延ばすのが困難な点があげられる。例えば、2020年1月時点での東芝の技術では、７Ｋｍ、５０Ｋｍ、５００Ｋｍのそれぞれの通信距離に対して、１０Ｍｂｐｓ、１Ｍｂｐｓ、１００ｂｐｓ程度の速度でしか通信できない。この問題を解決するために量子経路に中間地点を設けることや、光子を一旦電子に乗り換えさせるなどの工夫で距離を伸ばそうと研究が進んでいる。

東芝は通信距離などで世界をリードし、関連特許数で世界首位。21年3月までに事業化し、35年度に2兆1千億円と見込む量子暗号市場のうち、約4分の1のシェアを目指す。特許取得数はNECが2位だ。

ただし実用化では中国が先を行く。北京―上海間で約2千キロの量子暗号通信網を構築するなど、環境整備を進める。

（３）中国の量子暗号開発

「中国が作りあげた量子暗号通信網は、“スプートニクショック”のような出来事だ」――。科学イノベーションに関する調査・分析を担うシンクタンクである研究開発戦略センター（CRDS）フェローの眞子隆志氏はこう力を込める。

いわゆる「スプートニクショック」とは、ソビエト社会主義共和国連邦（ソ連）が1957年10月、人類初の人工衛星「スプートニク1号」の打ち上げに成功し、宇宙やミサイル開発のリーダーと自負していた米国が自信を打ち砕かれ、軍事的脅威を受けた状況を示す。中国が作り上げた量子暗号通信網は、「量子時代のスプートニクショック」ともいうべき脅威を、世界各国に与えている。

中国が作り上げた驚異の量子暗号通信網は、2021年1月に科学誌Natureに掲載された中国科学技術大学（USTC）らのグループによる論文で全貌が明らかになった。見えてきたのは「サイバー空間の“万里の長城”」ともいうべき、外敵から完璧に防御する巨大な暗号ネットワークの姿だ。

上海市から北京市までの2000kmのネットワーク、さらに上海市や合肥市、済南市、北京市といった中核都市内には網の目のように量子暗号通信網が張り巡らされている。

地上のみならず、宇宙空間にも量子暗号通信網を築く。中国は2016年、世界初の量子暗号通信衛星「墨子号」の打ち上げに成功。この量子暗号通信衛星を介して、中国・南山区と中国・興隆県を結ぶ2600kmの暗号ネットワークも稼働している。

地上と衛星を含めた全長は実に4600kmだ。この暗号ネットワークを中国国内では既に、中国・新華社通信や中国工商銀行、中国・国家電網などが機密情報を送受信のために活用しているとされる。

（４）米国の対応

こうした状況に危機感を強めたのが米国だ。新米国安全保障研究所は18年に「中国の量子科学の躍進は、将来の軍事的・戦略的バランスに影響を与える可能性がある」と警告を発した。米国家安全保障局（NSA）は20年、量子暗号通信を安全保障上のデータ送信に使うことを支持しない方針を明らかにした。米国は通信の仕組みは大きく変えず、暗号の中身だけを新しいものに置き換えようとNTT方式（後述）などに次世代の暗号通信を委ねる。

量子暗号通信としては、米Quantum　Xchange社が東芝と組んで金融向け耐量子ネットワークの実験をしている。通信距離としとては、ニューヨーク州とニュージャージー州を結ぶ32Km程度と中国とはかなりの差がある。

（５）日本

日本ではNTTが早くから研究に着手し、NEC、東芝、情報通信研究機構（NICT)などで研究開発がし閉められている。

- 2010年から、NICTを中心に量子暗号ネットワークテストベッドの構築に関する研究開発。ImPACT「量子セキュアネットワークプロジェクト」にて、都市圏QKDネットワーク「Tokyo QKD Network」(小金井-大手町間45km)の実証
- 2018年度から、内閣府の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Society5.0実現化技術」にて、量子暗号と秘密分散を統合した社会実装に取組み
- 2020年10月、NEC、NICT、ZenmuTechは、電子カルテのサンプルを量子暗号で伝送そのものを秘匿し、広域網経由で秘密分散技術を用いてバックアップ成功

3．耐量子コンピュータ暗号

これまで見てきた「量子暗号」が、量子力学の原理を応用して文章を暗号化するための秘密鍵を安全委配送できる一連の技術を指す。
これに対して、耐量子コンピュータ暗号は、量子コンピュータの計算性能でも解読に時間がかかるような暗号全般を指す。
量子の世界においては、現在使われているインターネットやコンピュータの暗号が量子コンピュータの開発によって容易に解読されるリスクに対する「耐量子コンピュータ暗号技術」と量子コンピュータの開発を科学などの分野に有効に活用するために量子コンピュータ同士をむずびつけ性能をさらに高めるための「量子暗号通信技術」が必要になってくる。（やや複雑ではあるがこの二つは区別しておく必要がある）
量子暗号が防衛や医療など特に秘匿性の高い情報を扱う分野の利用を想定するのに対し、これからお話しする耐量子コンピュータ暗号はより一般的なネット利用などが対象だ。
電子情報技術産業協会（JEITA）によると30年の世界の通信量は20年比15倍に増える。ネットが社会インフラとしての機能を維持・拡大するため、量子時代に対応して安全性を高める必要に迫られている。

（1）耐量子コンピュータ暗号の必要性

前述のように、公開鍵暗号は数学的問題を用いて安全性の仕組みを実現しており、現在主流の RSA 暗号と楕円曲線暗号は、それぞれ「素因数分解問題」と「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。これらの数学的問題は、現在のコンピュータ環境では現実的な時間で解くのが難しいと期待されており、RSA 暗号や楕円曲線暗号の安全性の根拠となっている。しかし、量子力学の性質を演算処理に応用したコンピュータである量子コンピュータ（特に、量子デジタル型）が実現すると、たとえ鍵長を長くしたとしても、素因数分解問題や楕円曲線離散対数問題を容易に解けることが知られている。（1994 年にピーター・ショアにより発表された「ショアのアルゴリズム」により解読が容易になってきている）そのため、将来、量子コンピュータが実現するとRSA 暗号や楕円曲線暗号はその安全性を確保できないという潜在的な脅威が存在する。
量子コンピュータの実用化を予め見据えたうえで、量子コンピュータによる解読に耐えうる暗号アルゴリズム（耐量子コンピュータ暗号）の準備を進めておくことは重要になっている。

（2）耐量子コンピュータ暗号の概要

インターネット通信の安全を支える暗号方式が初めて大きく変わろうとしているのである。
現在、米国国立標準技術研究所（ＮＩＳＴ）では、耐量子コンピュータ暗号（PQC ：Post-Quantum Cryptography）の暗号技術を標準化するためのコンペティションを2016年から行っている。NISTが対象とする耐量子コンピュータ暗号は、量子コンピュータでも解読を困難とするための鍵交換技術・公開鍵暗号技術、及び改ざん・なりすましを困難とするための電子署名技術である。
現在、ファイナルラウンドに進んダ4つの方式の中で選定が進んでおり、2024年までに規格として固める方針である。その中にNTTが参画しているNTRUという方式がある。

～量子暗号～

米国は新型暗号を標準化してきた	
16年12月	新型暗号を公募
17年12月	50弱の暗号が１次候補に
19年１月	20弱の暗号が2次候補に
20年７月	４つの最終候補を選定。NTTが関わる暗号も残る
早ければ22年１月中	新型暗号を決定
24年まで	新型暗号の規格を策定、実用化
31年以降	新型暗号を本格的に利用

最終候補に残る４方式の暗号	
開発に関わる企業や大学	特徴
NTT、クアルコムなど	25年間、暗号が破られていない
IBMなど	IBMが自社サービスに試験導入
ルーベン・カトリック大	１大学が主体となり開発
イリノイ大など	他の３つと土台の数学の問題が異なる

(出所) 各暗号の公式サイトを基に作成

インターネット関連の標準化団体「IETF」もNISTの決定に合わせる方針を示しており、事実上の世界標準となる。現行の「RSA暗号」に対応した通信規格はインターネットが普及した1990年代後半から世界中で使われている。世界標準の通信規格が初めて大きく変わることになる。
新暗号が決まれば、IT（情報技術）企業などは対応を迫られる。NISTは高度な量子コンピューターの実用化が見込まれる31年以降は既存の暗号を使わないよう呼びかける方針だ。東京大学の高木剛教授は「それまでにソフトの入れ替えなどが必要」と指摘する。

米調査会社インサイド・クオンタム・テクノロジーの予測によると、新暗号を使うソフトや機器の世界市場は28年に39億ドル（約4500億円）に達する。電子メールやネット通販、銀行ATMといった一般ユーザーの利用にとどまらず、企業間の取引や行政サービスなどネット上のあらゆるやり取りに影響が及ぶ。

米マイクロソフトと米アマゾン・ウェブ・サービス（AWS）は通信で新暗号を使うためのソフトを共同開発する。NTTは光技術を使う独自の次世代通信基盤「IOWN（アイオン）」に新暗号を組み込む考えだ。

（３）NTRU方式の概要
NTRUは「格子暗号」と呼ばれ、「格子点探索問題」という数学的問題を安全性の根拠として利用する公開鍵暗号である。格子点探索問題とは、格子（ベクトル空間上に規則正しく並んでいる点の集合）が与えられたときに、ある条件を満たす格子点（格子上の１つの点）を探索する問題の総称である。（この詳細は何回過ぎて理解できていないため省略する。数学に興味のある方は
https://www.imes.boj.or.jp/research/papers/japanese/kk34-4-7.pdfご参照）

NTTはNTRUが米国標準に選ばれた場合も、第三者利用の特許料を受け取らないことを明らかにしている。
NTT方式の利点は専用の装置が不要なことだ。現行方式から移行するのに障壁が少なくて済む。その上で先行者利益で周辺ビジネスで稼ぐことを狙う。

～量子暗号～

新暗号の市場規模は今後、急速に拡大する見込みだ。米調査会社インサイド・クオンタム・テクノロジーの予測では、量子コンピューターでも解読が難しい暗号を使うソフトやデバイスの世界市場は28年に39億ドル（約4400億円）に達すると試算する。
最初に新暗号を導入することが想定されるのは、米テック企業だ。米グーグルやアップル、マイクロソフトなどはブラウザー（ネット閲覧ソフト）上に新暗号を組み込み、通信の安全性を高めることが求められる。実際、グーグルは18年にブラウザー「クローム」にNTRUを組み込んで通信する実験をしている。

NTTはNTRUが米国標準に選ばれた場合も、第三者利用の特許料を受け取らないことを明らかにしている。
NTT方式の利点は専用の装置が不要なことだ。現行方式から移行するのに障壁が少なくて済む。その上で先行者利益で周辺ビジネスで稼ぐことを狙う。

（４）量子コンピュータの金融へのリスク
最後にセキュリティの観点から最も影響を受けるであろう分野の一つである金融分野のリスクについてみてみる。
金融界は、取引の大半がインターネット通信などで広く使われているRSA暗号などの暗号によって守られており、量子コンピューターが暗号を破れるようになれば、その影響は計り知れない。

米金融機関キャンバス・クレジット・ユニオンの最高情報セキュリティー責任者のカルロス・バズケス氏は、21年11月の米下院金融サービス委員会の消費者保護と金融機関に関する小委員会における証言のなかで「サイバーセキュリティーは変化し続けている。脅威は、少し前までマルウエア（悪意のあるプログラム）、ウイルス、悪意を持った会社のネットワークへの侵入だった。目下はランサムウエア、ソシアル・エンジニアリング（電話などでパスワードを聞き出すなど、不正な手段でネットへのアクセス情報を盗む技術）とサプライチェーン（供給網）攻撃だ。今後は（機械学習を活用し偽動画などによって相手をだます）ディープフェイク技術、量子計算などを用いた脅威に直面するだろう」と証言している。

この量子コンピューターの金融への影響について、IMFのリポート「量子コンピューティングの可能性と危険」（Quantum Computing's Possibilities and Perils）で、筆者のホセ・デオドロ氏らは「インターネットを介した通信を保護するために広く使用されている非対称キーのアルゴリズムに対する攻撃が成功すると、モバイルバンキング、電子商取引（EC）、支払いトランザクション（処理）、ATM現金引き出し、VPN（仮想私設網）通信などの金融システムで使用される接続が危険にさらされる」と指摘。ほとんどの金融機関と規制当局は、これらの新たなリスクにまだ注意を払っていないが、手遅れになる前にリスクを認識し、システムを保護する必要があると警鐘を鳴らしている。

通常の銀行業務でシステムトラブルが続くようではとてもこのような流れに乗ることが難しいと思われる。銀行も新しい淘汰の波が将来訪れるのではないだろうか。