

えいせいくんがご案内!

取材協力/スカパーJSAT
マンガ/うえたに夫婦
取材・文/戸村悦子

スカパーJSATの

ゆかいななかまたち

Vol.13 衛星量子鍵配送で大事な情報を守ろう!

えいせい先輩にいわれ、情報通信研究機構※1 (NICT) にやってきたえいせいくん

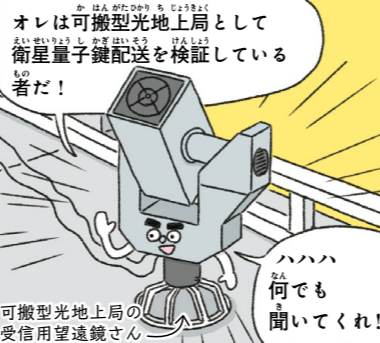
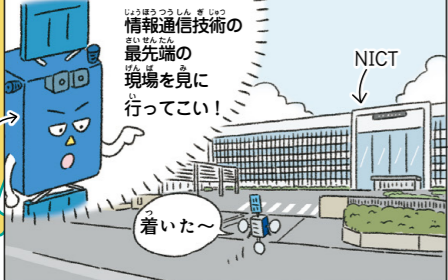
その敷地の一角にて……

オレは可搬型光地上局として衛星量子鍵配送を検証している者だ!

えーっとこの車……かな?

おー! 君がえいせいくんか! 話は聞いてるよ

ハハハ何でも聞いてくれ!



※1 情報通信分野を専門とする日本唯一の公的研究機関

……実はあまりよくわからず来ちゃいました

ハハハ、オッケー! 簡単にいうと、オレはインターネット通信の安全性向上に関わっている

インターネットでは重要な情報が暗号化されているのは知っている? 例えばクレジットカードの暗証番号や病院のカルテ情報など、他にも多くの情報が暗号化されている。

ただ、実は現在の暗号化技術は近い将来、すべて解読されてしまう可能性がある……

え!? それはまずい!

そう、そこで新たに「量子暗号通信」というのが開発されつつある。さっきいった「衛星量子鍵配送」はそのうちの1つなんだ



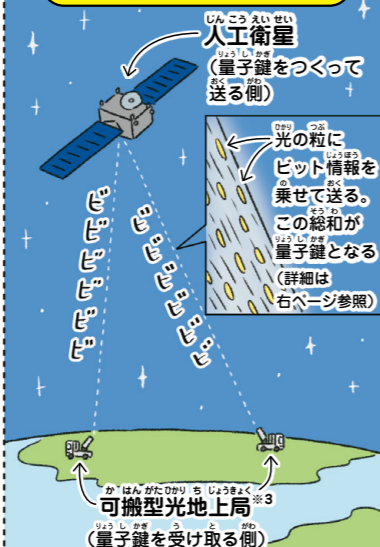
量子暗号通信とは…

量子力学の原理を利用した暗号化技術で、「絶対に解読されない次世代の暗号技術」といわれている。光の最小単位である光子(光の粒)に情報を乗せて通信を行う。

衛星量子鍵配送とは…

量子暗号通信に必要な暗号鍵※2(量子鍵ともいう)を衛星でやり取りする技術で、セキュリティ性や耐災害性が高く、地球上の広い範囲に送れるなど、メリットが多い。スカパーJSATとNICTが共同で開発中で、2030年に実現予定。

衛星量子鍵配送のイメージ



うーん、なんだか難しいけど、要は衛星が安全性の高い通信技術に役立つってこと?

ハハハ、その通り! ちなみにその衛星はまだどれになるか決まっていなくて……

え、ボクやりたい! 2030年ごろだけだよね?

全然オッケー! 宇宙に行けるなら!

※2 暗号化されたデータを元に戻して読めるようにするもの。

※3 現在は試作機

えいせいくん、2030年には宇宙に行ける!?

宇宙から「鍵」を届ける、衛星量子鍵配送って何?

インターネット取引などに使われる暗号方式は、2030年ごろには最新の量子コンピューターによって解読されちゃうかも!? そこで今注目なのが、スカパーJSATが実証プロジェクトを進める「衛星量子鍵配送」だ。衛星を使ったサイバーセキュリティのしくみを知ろう!

教えてくれたのは

スカパーJSAT
宇宙・防衛事業部宇宙チーム
田中賢太郎さん 横手紗織さん

スカパーJSATでは、国立研究開発法人情報通信研究機構(NICT)と協力しながら衛星量子鍵配送の実用化に向けてお手伝いをしている。事業がスタートしたら、通信衛星技術のノウハウを活かして鍵配送に使う衛星の打ち上げ・運用も担当する予定だ。まずは大事な国家機密や医療・金融情報などを守るために、日本をはじめ各国で実証テストが進行中。将来はキミの大切な個人情報も、衛星から届いた鍵がガッチリ守ってくれるかもしれないゾ!

※公開鍵方式…受け手が暗号化する公開鍵と復元する秘密鍵を別々につくり、公開鍵を送り手に送る。送り手はそれでデータを暗号化し、受け手が秘密鍵で復元する。この方式はネットショッピングなどでも使われている。

! 今の暗号は大ピンチ!?

重要なデータを送信するとき、送り手は他人に盗み見されないようにデータを暗号にして送り、受け手はそれを復元して中身が読めるようにする。その際に使われるのが「暗号鍵」で、みんなもよく知るパスワードにあたるものだ。

今ある暗号方式は主に2種類。1つは送り手がある鍵でデータを暗号化し、受け手は送られてきた同じ鍵を使って復元する共通鍵方式。高速で大容量のデータ送信ができるけど、受け手へ鍵を送るとき他人に盗まれるリスクがある。もう1つの公開鍵方式※は、送り手と受け手の鍵が別々で、受け手は自分だけの秘密の鍵で復元する。これなら鍵を盗まれるリスクは低いが、この方式もいずれ量子コンピューターで解読されるかもしれない。こうしたセキュリティの問題を解決する切り札が、絶対に解読されない方法で鍵を届ける「量子鍵配送」なんだ。

衛星から「鍵」を届ける!

量子鍵配送は、鍵の情報をこれ以上分けられない小さな光の粒(光子)に乗せて届けるしくみ。地上の光ファイバー回線でも、人工衛星を使って届けることもできる。衛星量子鍵配送では、まず衛星の中で鍵の材料をつくり、それを光子に乗せて地上へ降らせ、地上局で受け取れたものだけを使って鍵をつくる(図)。衛星は宇宙空間にあるので侵入できないし、災害で断線することもない。低軌道衛星なら地球上の広いエリアに配送できるのがメリットだ。

衛星量子鍵配送のしくみ

- 1 人工衛星** 衛星の中で鍵の材料(ビット情報)をたくさんつくる。
- 2 光子(フォトン)** 鍵の情報を光の1粒1粒に乗せて地上局(送り手と受け手の2か所)に降らせる。送り手と受け手には別々の鍵の情報が届く。
- 3 地上局(鍵蒸留)** 光子は自然現象によって地上に届くものと届かないものがある。光子を受信・検知する地上局では、受け取れた光子だけを並べて文字の配列をつくり、それが共通鍵になる(下のコラムを参照)。

もっと知りたい!! 深ボリ情報

衛星量子鍵配送は どうして絶対に安全なの?

データの復元(パスワード)は普通数字やアルファベットで、すべて0と1で表すことができる。衛星量子鍵配送は、0または1と書かれた小さなボールを衛星からランダムに投げ続けるイメージ。でも地上では的を外れたり、盗聴者がキャッチしたりして届かないボールがあり、地上側は「何番目が抜けた」と衛星側に伝えてその情報が省かれる。だから盗聴されてもすぐわかるし、それが0か1かは誰にもわからないので絶対に安全といえる。送り手と受け手はそれぞれ違う鍵の情報を受け取り、最後に答え合わせをして共通している部分を鍵として使うんだよ。