第1章 ショアのアルゴリズムでRSAが解かれる？耐量子計算機暗号の考え方とは

なぜ量子コンピュータが現代暗号の脅威なのか

西出 隆志

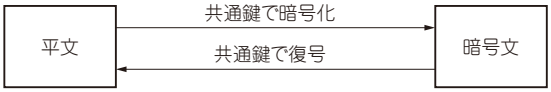

図1 共通鍵暗号の仕組み

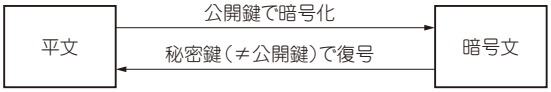

図2 公開鍵暗号の仕組み

本稿では，現在広く利用されている代表的な公開鍵暗号であるRSAと，それに対する量子コンピュータ（以下，量子計算機）の脅威について解説します．続いて，量子計算機が既存の暗号に与える影響を踏まえて登場した耐量子計算機暗号や，その設計に用いられる計算困難性の考え方について説明します．

RSA暗号を含む公開鍵暗号，共通鍵暗号については特集内で既に何度か説明がでていますが，RSA暗号の弱点や耐量子計算機暗号の説明に関係するので，本稿でも解説しています．

現代暗号の仕組み①…共通鍵暗号と公開鍵暗号

暗号技術の主な利用用途としてネットワークにおける通信データの秘匿が挙げられます．ネットワーク上のデータは，送り手のコンピュータから受け手のコンピュータへ直接届くわけではなく，ルータなどの中継ノードを経由して転送されます．そのため，途中のノードを管理する第3者にデータを盗み見られないよう，暗号技術が必要となります．例えば，現代では多くの人々がインターネットを利用する際に，HTTPS通信などを通じて暗号技術を意識せずに利用しています．

● 共通鍵方式

暗号という言葉を聞いて，初めて学ぶ人がおそらく思い描くものは**図1**のようなものだと思います．つまりデータの送り手と受け手が秘密の鍵K（これを共通鍵と呼ぶ）を共有し，その鍵Kを用いてデータの暗号化，復号を行うというものです．このような暗号方式を共通鍵暗号と呼びます．現在，広く使用されている共通鍵暗号の代表例として，AES（Advanced Encryption Standard）があります．

ただし，インターネット上で安全に暗号通信を行うために，共通鍵暗号だけでは十分ではありません．共通鍵暗号を利用するためには，事前に秘密鍵を安全に共有する必要がありますが，常に盗聴が可能なネットワークを介して安全に鍵を共有することは容易ではありません（これは鍵配送問題などと呼ばれる）．

● 公開鍵方式

▶鍵だけど公開

先述のような問題を解決する暗号技術として公開鍵暗号が提案されました（**図2**）．公開鍵暗号ではデータの暗号化に使う鍵（公開鍵）と復号に使う鍵（秘密鍵）を分け，さらに暗号化に使う公開鍵はその名の通り世の中に公開しても安全性が損なわれない，という共通鍵暗号とは大きく異なる特性を持っています[注1]．

公開鍵暗号では，公開鍵と秘密鍵が異なるにも関わらず，暗号化したデータを復号すると元の平文に戻るという不思議な特性を持っています．

例えば，ボブ（送信者）がアリス（受信者）に暗号文を送りたい場合を考えます．このときまずアリスは自身の公開鍵をボブに送信します．この通信は盗聴されている可能性があるネットワークを介していても，公開鍵を秘匿する必要はないため問題はありません．ボブは受け取ったアリスの公開鍵を使ってメッセージを暗号化し，暗号文をアリスに送ります．アリスは自分の秘密鍵を使って復号し，ボブからのメッセージを取得できます．このときアリスが自分の秘密鍵を厳重に

注1：一方で，共通鍵暗号は公開鍵暗号に比べて高速であり，大量のデータを効率的に暗号化できるため，共通鍵暗号と公開鍵暗号は互いに補完し合う関係になっている．