第3章 定番のRSAと楕円曲線暗号を例に
鍵の生成から暗号化と復号，署名と検証まで

公開鍵暗号の原理と基礎

宮田 賢一

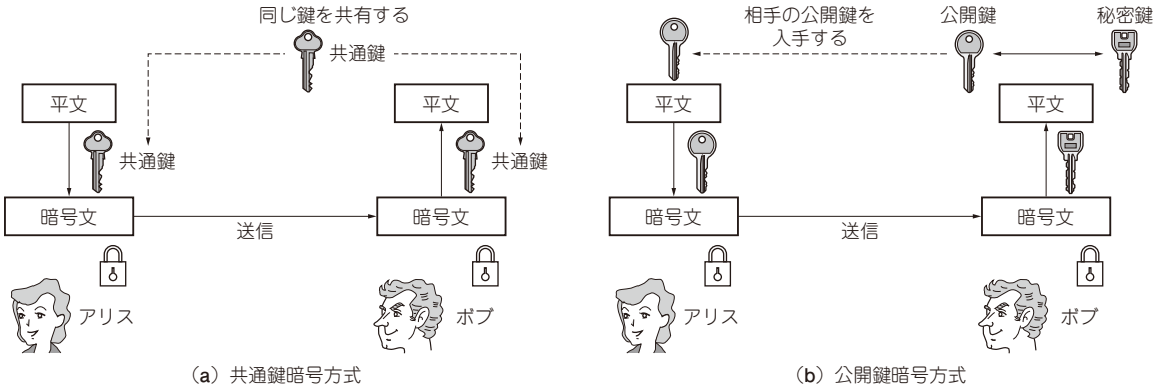

図1　データを暗号化する方式

あらゆるデバイスがネットワークにつながるIoT時代において，セキュリティは最初の設計段階から織り込むべき要素となっています．

特にマイコン・ボードを使ったセンサ・デバイスや制御デバイスにおいては，外部からの不正アクセス，データの改ざん，なりすましによる誤動作など，多様なリスクが存在します．

本稿では，RSAと楕円曲線暗号（Eliptic Curve Cryptography：以下ECC）という2つの代表的な公開鍵暗号方式の仕組みを解説します．

データ暗号化の方式…共通鍵/公開鍵の2種類

データを暗号化する方式には，大きく分けて2つの種類があります．

- 共通鍵暗号方式
- 公開鍵暗号方式

図1にそれぞれの動きを示します．データを送りたい側にアリス，データを受け取りたい側にボブという名前を付けます．また，暗号化前の元のデータを平文（ひらぶん），暗号化されたデータを暗号文と呼びます．つまりアリスは送りたいデータの平文を暗号化してボブに送信し，ボブは受け取った暗号文を復号して元の平文を取得するという言い方ができます．

共通鍵暗号方式［**図1**（**a**）］は，データの暗号化と復号に共通鍵と呼ぶ同じ鍵を使用する方式です．第1部第2章で説明したAESは共通鍵暗号方式の1つです．共通鍵は事前に作成した鍵をアリスとボブが共有する必要があるため，安全に鍵を共有する手段が課題となります．

公開鍵暗号方式［**図1**（**b**）］は，公開鍵と秘密鍵という2つの異なる鍵を用います．公開鍵と秘密鍵は数学的な計算式により結びつけられています．この方式では鍵のペアのうち公開鍵だけを相手に共有します．公開鍵が第三者に傍受されたとしても，簡単には秘密鍵を復元できないような数学的な原理に基づいてセキュリティを確保しています．

公開鍵暗号の原理

公開鍵暗号方式は，一方向性関数という数学的な背景に支えられています．一方向性関数とは，ある値xから関数$f(x)$を計算するのは容易だが，$f(x)$から元のxを逆算するのが非常に困難であるという特性を持つ関数のことを指します．

この原理を利用した実際の暗号方式の代表として，RSA暗号（または単にRSA）とECC暗号（または単にECC）があります．本稿ではこれらの数学的な仕組み