第5章 ディフィー・ヘルマン鍵共有から楕円曲線ディジタル署名アルゴリズムまで

アルゴリズムから理解する公開鍵暗号技術

白勢 政明

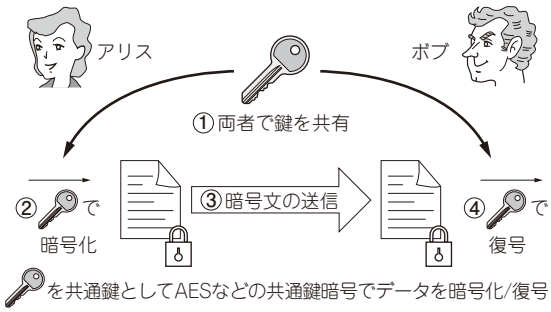

図1 鍵共有方式におけるデータの受け渡し

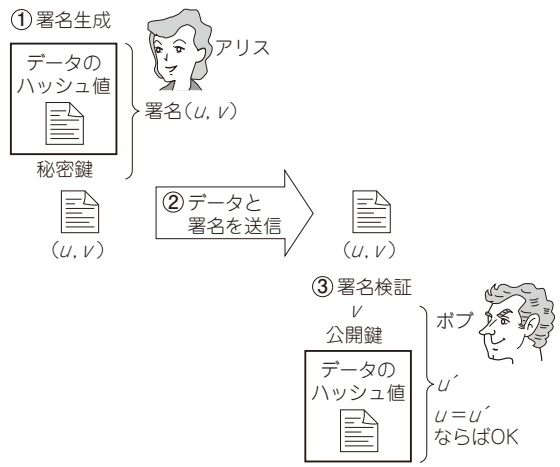

図2 公開鍵暗号技術における電子署名(ECDSA)

安全な通信を実現するためには，秘密情報を直接やり取りすることなく共通鍵を生成する鍵共有方式(**図1**)と，データの改ざんやなりすましを防ぐ電子署名方式(**図2**)が重要な役割を果たしています．これらは公開鍵暗号技術の一種であり，現代のインターネット通信の多くはこの技術の上に成り立っています．

本稿では，特にインターネット通信の基盤となるTLS1.3において使用されている，ディフィー・ヘルマン(Diffie-Hellman)鍵共有(以下，DH鍵共有)，楕円曲線ディフィー・ヘルマン(Diffie-Hellman)鍵共有(以下，ECDH鍵共有)，および楕円曲線ディジタル署名アルゴリズム(ECDSA)の数式からPythonプログラムを作成します．特に，暗号分野で用いられる楕円曲線については，詳しく解説します．

本稿で必要となるimport文を**リスト1**に示します．

世界初の公開鍵暗号技術「ディフィー・ヘルマン鍵共有」

インターネットでのやりとりでは，個人情報やパスワード，クレジットカード番号などの機密にすべきデータが送受信されることがあります．その場合，通信データを暗号化し，データを盗聴されても分からないようにする必要があります．この暗号化にはAESやChaCha20といった共通鍵暗号が用いられます．ここで問題となるのが，共通鍵暗号で用いる鍵を安全に共有する方法です．この目的のために用いられるのがDH鍵共有です．DH鍵共有は，安全な通信路を必要とせずに2者間で共通の秘密鍵を生成する手法であり，1976年に提案された世界初の公開鍵暗号技術です．安全な通信路がなくても2者間で共通の秘密鍵を生成できます．素数の剰余演算を用いて構成され，DH鍵共有の安全性は離散対数問題[注1]の困難性に依存します．

● DH鍵共有の仕組み

盗聴者の存在を前提に，アリス(データを送りたい

リスト1 本稿のプログラムを行うためのimport文

```
1 from sympy import randprime
2 import math
3 import random
4 from sympy import randprime, isprime
5 import hashlib
6 from sympy.ntheory.residue_ntheory import sqrt_mod
```

注1：離散対数問題とは，ある素数pと自然数gおよびyが与えられたときに，$y \equiv g^x \pmod{p}$を満たすxを求める問題です．pが十分大きい(例えば2048ビット)安全素数ならば，離散対数問題を解くことは非常に困難です．安全素数についてはコラム1で解説します．