第2章 RSAやTLSでも利用されている！その暗号が破られないことを数学的に考える

暗号技術の安全性を証明する方法

米山 一樹

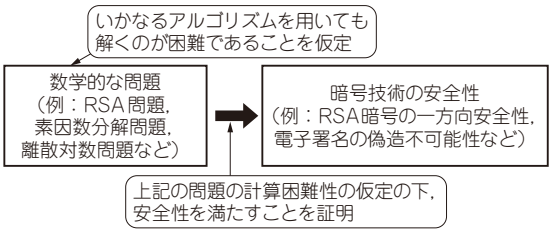

図1　計算困難仮定に対する帰着による安全性証明

本稿では数学的問題を解くのが困難であることを仮定することで暗号技術の安全性を証明する手法について説明します．また，公開鍵暗号であるRSA暗号を例として，安全性概念の数学的な定式化と帰着による安全性証明を示します．

多くの暗号技術は無条件に安全ではありません．利用環境に応じた適切な暗号技術を導入する際に，その環境下においてどのような安全性が要求されるかを考慮する必要があります．設計の際に想定していない攻撃戦略などが存在すると，脆弱性につながる恐れがあります．

従って，利用できるリソースや計算能力（攻撃環境）を持つ攻撃者（確率的多項式時間攻撃者）が，いかなるアルゴリズムを用いても解けないような数学的な問題の難しさを仮定した上で，暗号技術の安全性をその問題の計算困難性にひも付けることでその暗号技術の安全性の証明を行います（**図1**）．このことを計算困難仮定に対する帰着による安全性証明と言います．安全性証明が付けられた暗号技術を利用することで想定外の戦略による攻撃を防ぐことができるというメリットがあります．

定番のRSAやTLSは安全性証明が行われている

代表的な公開鍵暗号であるRSA暗号[2]はRSA問題と呼ばれる数学的な問題の計算困難性に帰着することで，秘密鍵の情報なしでいかなる攻撃者も暗号文から平文を得ることができないこと（一方向安全性）が証明されています（**図1**）．

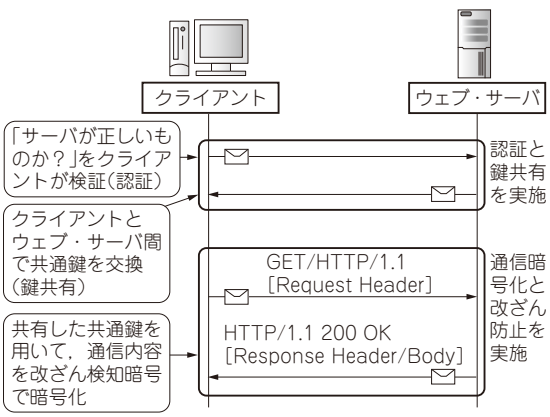

図2　TLSの概要

もう1つ身近な具体例として，ウェブ・ブラウザ-ウェブ・サーバ間通信の改ざん検知や通信内容の秘匿を目的としたセキュリティ・プロトコルであるTLS（Transport Layer Security，**図2**）[1]があります．TLSは，認証，鍵共有，改ざん検知暗号などの複数の暗号技術を部品として組み合わせて構成されており，我々が日常的にウェブ・ブラウザでウェブ・ページを訪問する際の安全性の根幹を担っているため，プロトコル仕様に起因するような攻撃が見つかってしまうと社会的に大きな影響が出てしまいます．しかし，安全性証明が付けられた暗号技術を部品として仮定することで，TLS全体のプロトコルに対して設計段階から利用環境における攻撃環境を考慮した安全性証明が行われていることで，そのような攻撃がないことを保証しています．よって，安心して利用することができています．

安全性をどうやって証明するか

● 証明したい暗号の仕組みの確認

公開鍵暗号を例に解説します．公開鍵暗号の目的は，平文を秘匿して送信する，すなわち，平文から暗