第3章 量子雑音を利用して安全なデータ通信を行うY-00暗号

数理アルゴリズムに頼らない! 物理現象を利用する暗号通信

二見 史生

表1　数理暗号と物理現象を利用した暗号の比較

	暗号例		安全性の根拠	安全性の特徴	メリット	利用状況
	鍵共有	暗号通信				
数理暗号	RSA/PQC	AES	計算困難性	破られるかもしれない	比較的安価で実用的	日常生活で利用
物理現象を利用した暗号	QKD	Y-00	物理現象（量子雑音など）	安全性を保証できる	コンピュータ処理が高速化しても破られない	研究開発段階（一部は製品化）

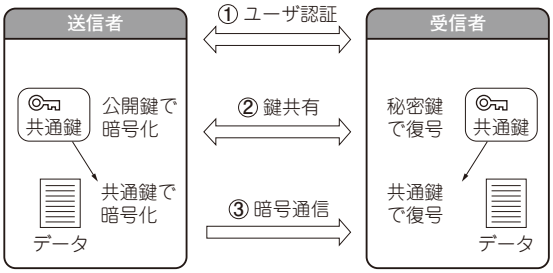

図1　暗号通信システムの基本構成

本稿では，量子雑音（量子力学的な起源で必ず発生する物理量のゆらぎ）という物理現象を利用してデータを安全に通信するための暗号通信方式であるY-00暗号[1]を紹介します．Y-00暗号は，大容量，長距離の暗号通信に利用できます．その上，安全性が保証される特徴があります．

数理暗号と物理現象を利用した暗号の違い

一般に，暗号技術は数理アルゴリズムに基づいています．本稿ではこれを数理暗号と呼ぶことにします（**表1**）．数理暗号は，原理的な安全性の保証はありませんが，計算量が非常に膨大なため，現実的な時間内に解読することが困難であり，実用的には安全とされています（例えばRSA暗号は素因分解の計算困難性に基づく）．このため，数理暗号は日常生活において広く利用されています．

しかし，計算機の性能向上による計算時間の短縮化や新たな解読アルゴリズムの発見により，計算量が大幅に減少するリスクがあります．実際に過去には，米国標準規格として採用された数理暗号（DES）が解読される事例もありました[2]．

暗号は数理暗号だけではありません．物理現象を利用すると，従来の数理暗号ではできない，安全性を保証する暗号方式を実現できる可能性があります．

暗号通信システムの基本

● 暗号通信システムの3要素

はじめに一般的な暗号通信システムの概要を紹介します．**図1**のように次の3つの要素で構成されています．

▶ユーザ認証

通信相手があらかじめ意図した相手であるか識別する機能です．第三者による不正使用やなりすましを防止します．

▶鍵共有

暗号通信を行う当事者間で利用する共通鍵を安全に共有します．

▶暗号通信（データ）

通信を行う当事者間で共有された共通鍵を利用してデータを暗号化して，第三者による盗聴を防ぎます．

暗号を用いた通信を行う際は，まずユーザ認証を行います．次に，暗号通信に使用する共通鍵を通信者間で共有します．その後，共有した共通鍵を用いてデータの暗号通信を行います．

● さまざまな暗号方式がある

鍵共有と暗号通信（データ）に用いられる暗号方式を**表1**に示します．数理暗号では鍵共有にはRSA暗号[3]，暗号通信（データ）にはAES暗号（Advanced Encryption Standard）[4]が広く利用されています．