# まえがき

本書では，現代の暗号・認証技術のしくみについて紹介していきます．

暗号は，紀元前から存在し，主に戦争における秘密通信を実現するために使用されてきました．暗号は暗号解読との戦いであり，暗号解読により暗号が破られ，暗号が改良されていくという歴史でした．第二次世界大戦においても主要な役割を果たしており，暗号作成と暗号解読の攻防が繰り広げられました．

一方，今日では，インターネットを代表とするコンピュータネットワークでの安全性を確保するためのセキュリティ技術として，暗号技術とそれを応用した認証技術は盛んに利用されています．インターネットによって世界中の人々が通信できるようになり，Web，SNS，ネットショッピング，インターネット電話，動画配信など様々なサービスが展開されてきています．また，PC，スマートフォンに留まらず，家電，自動車，センサーなど様々な機器がインターネットに接続されようとしています．しかし，インターネットの普及とその利用の多様化に伴なって，インターネット上での不正・犯罪も多発してきています．無線通信など通信の途中で盗聴される恐れがあります．パスワードを盗聴されてしまうと不正アクセスされてしまいます．通信しているサーバが，想定しているサーバと違っているかもしれません．これらの脅威は，現代の暗号・認証技術によって守られています．

現代の暗号は，第二次世界大戦後，1970 年代から発展してきま

した．従来の秘密鍵を共有する共通鍵暗号に加えて，公開鍵暗号と呼ばれる新しい概念が考案されました．公開鍵暗号では，暗号化と復号で異なる鍵を利用する暗号です．これにより，鍵の配送が容易になり，インターネットのようなオープンな環境での暗号利用が容易になりました．また，公開鍵暗号はディジタル署名に応用されています．ディジタル署名は，署名や印鑑の電子版であり，電子文書の改ざん防止と作成者の確認（認証）が行えます．インターネットでのサーバの認証でも利用されています．

本書では，このような現代の暗号・認証技術のしくみを，予備知識なしで理解できるように紹介しています．また，暗号・認証技術がインターネットでの安全な通信をどのように実現しているかについても解説しています．

クラウドなどネットワーク環境の多様化に伴ない，暗号・認証技術の研究は，公開鍵暗号・ディジタル署名からさらに進んでいます．本書では，最新の研究の一つである高機能暗号についても平易に解説しています．

暗号・認証技術は研究者や開発者だけでなく，一般の方々も知っておく必要のある技術になってきました．本書がその入門として役立つことを期待します．

2016 年 12 月

中西　透