安全，安心なサイバー社会をつくる暗号のしくみを学ぼう

コーディネーター　井上克郎

現代の社会生活は，インターネットを始めとするコンピュータネットワークによって支えられています．ネットワークによる通信が安全に正しく機能することによって，我々の生命や財産が保全され，いろいろな社会活動が可能になっています．

この通信の安全性を担保する技術が暗号です．暗号と聞くと何か隠された技術，秘密で後ろ向きの技術というような印象を持つかもしれませんが，現代の暗号技術は，きっちりとした数学的な理論を背景として，その方法や強さ，解読法などが，国際会議やワークショップなどの公の場で議論されています．非常に知的でオープンな，最先端の研究テーマとなっており，たくさんの優れた研究者が日々切磋琢磨して，新しい暗号方式やその応用，その安全性や解読方法を研究しています．

暗号は，古くから軍事を主な目的として，いろいろな方式が考えられ，実際に用いられてきました．また，それとともに，暗号解読の技術も次々に考案され，昔の暗号が安全に用いることができなくなってきています．暗号の歴史をたどることは，人類の英知の変遷を眺めているようで，大変おもしろく，きっとわくわくすることでしょう．

本書の目的は，コンピュータやネットワークの能力が飛躍的に向上した現代社会で，便利に利用できる暗号技術について，その基礎をきちんと紹介するとともに，それが現代社会でどのように応用さ

れているかを，できるだけ分かりやすく平易に解説することです．

現代の暗号は，その構成方法や安全性を，数学の問題の解法の難しさに帰着させており，いろいろな数学の基礎が必要となってきます．本書では，現在，実際に使われている種々の暗号や暗号技術を応用した署名，認証などについて，その方式や安全性の議論を，比較的簡単な数学の知識を用いて，丁寧に解説しています．ここでは，整数論，統計学，論理学，集合論などについて，高校生程度の知識を前提として詳しく解説するとともに，参考図書を示して，深く学習できるようにしています．

まず，第 1 章では，暗号の簡単な概念を紹介し，過去に用いられたいろいろな暗号方式のなかで，スキュタレー暗号という転置式暗号，シーザー暗号という換置式暗号，そして第二次世界大戦時にドイツで用いられたエニグマ暗号が詳しく説明されています．また，現代の暗号や認証技術の概要として，共通鍵暗号や公開鍵暗号の概念が説明されています．これらの暗号方式を理解することで，暗号の初歩に触れるとともに，以降の現代暗号への導入となっています．

第 2 章では，過去から現在までにわたって，いろいろな場面で頻繁に用いられる暗号の形態である共通鍵暗号について説明されています．究極の共通鍵暗号であるワンタイムパッドは，常に新しい鍵を用いるために，統計的な偏りをなくすことができ，攻撃者の解析の手がかりを消すことができます．しかし，暗号鍵が入力テキストに比例して長くなるために，長大な鍵の配送や保管の問題からあまり実用的ではないことが説明されています．このように，暗号技術では，単に暗号の強度が高く解読ができないことばかり目指すのではなく，実際に簡単に利用することができるか，を常に意識する必要があることが述べられています．その他にも，DES や ASE など，

Wi-Fi や SSH 接続などでお世話になるブロック暗号やそのモードについても詳しい説明があり，これらを使う際に，これらのパラメータの設定が何を意味しているのかが，よく分かるようになります．

第 3 章では，現代暗号の中核技術である公開鍵暗号について詳しく説明されています．暗号のための鍵を公開する，という一見不思議な仕組みですが，秘密の鍵との組合せ方で，いろいろな実現方法を取ることができ，また，数多くの応用に用いることができるので，数多くの研究と実用化が精力的に行われている分野です．本書では，その代表的なものである RSA 暗号について，その原理とともに，巨大な整数の素因数分解の困難性に依存する安全性が詳しく説明されています．また，離散対数問題に依存するエルガマル暗号，楕円曲線を用いた楕円曲線暗号が，その数学的な背景とともに丁寧に説明されています．

第 4 章では，まず，ハッシュ関数について説明されています．ハッシュ関数は，テキストやメッセージを短い固有の値に変換するもので，現在，仮想通貨やそれを実現するブロックチェーンなど，いろいろな方面で研究・利用が進んでいる技術です．また，鍵付きハッシュ関数を用いたメッセージ認証技術についても紹介されています．これによって，メッセージが送り主から正しく送られたもので，途中で改ざんが行われていないことを確認することができます．

第 5 章では，ディジタル署名技術が詳しく紹介されています．4 章のメッセージ認証技術では，メッセージの送り主の確認は，秘密鍵を共有する特定の相手のみ確認でき，それ以外の人にその正しさを示すことはできません．ディジタル署名技術では，公開鍵暗号を用いることによって，一般の第三者に，メッセージの正しさを示す

ことができます．ここでは，RSA やエルガマル暗号を用いた署名方法などの説明とともに，ゼロ知識証明と呼ばれる情報秘匿技術を用いたシュノア署名についても詳しく紹介されています．

第 6 章では，実際のインターネットで使われているいろいろな暗号や認証の具体的な技術の説明と，それらの安全性や問題点について議論されています．現在，大きな問題になっているフィッシングなどの Web サーバの偽造を防ぐためのサーバ認証や公開鍵証明書，PKI などが説明されています．また，SSL/TLS などの広く用いられている共通鍵暗号と公開鍵暗号との組合せ技術についても紹介されています．さらに，コンピュータ性能の向上によって暗号の安全性が低下することについて議論されています．

第 7 章では，高機能暗号と呼ばれる現代のコンピュータネットワークの利用方式に合った暗号システムが紹介されています．ここでは，一対多の放送型ネットワーク通信における秘密通信や認証，暗号文上での検索など，現在のいろいろなネットワーク利用の形態で必要とされる技術について紹介されています．

最後の第 8 章では，暗号や認証の将来技術について語られています．量子コンピュータが実現すると現代の暗号は簡単に解読される危険性がありますが，それを防ぐためのポスト量子暗号が研究されていることが紹介されています．また，IoT が実用段階になって，多数の機器の間を安全にかつ手軽につなぐ必要が生じてきています．これらの問題について議論されています．

本書の著者である中西透先生は，一貫して暗号や認証の技術を研究してこられている第一線の研究者であり，本書で書かれている分野に関して，広く精通されているとともに，多くの新しい方式の提案をされてきています．本書の狙いである暗号や認証の基礎，そしてその応用を紹介するには，最も相応しい著者といえるでしょう．

現在，サイバーセキュリティは大きな社会的な関心事になっています．いろいろな事件や事故が日々発生し，多くの社会的な損失を生んでいます．サイバー空間を安心して利用するためには，暗号や認証の技術は不可欠なものになっています．本書が多くの方々の目に触れることによって，暗号や認証の技術の根幹の理解が進み，安全なサイバー社会が実現することを切に望んでいます．