基礎講座

情報セキュリティ技術と現代暗号

インターネットに代表される最近のネットワークの発達により、国境といった概念さえ希薄となる社会環境が生まれています。この仮想的な社会での安全性を守る技術として、情報セキュリティ技術や暗号技術が注目を浴びています。今回の解説は、この情報セキュリティ技術と暗号技術の動向を簡単に解説します。

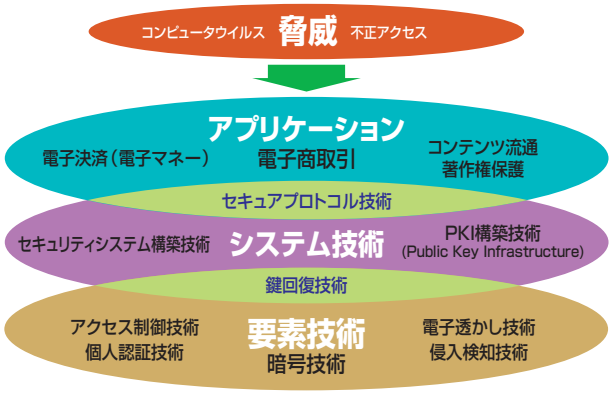
1．はじめに

半導体技術や情報処理技術の進展に伴い、一般家庭や各種機器にコンピュータが浸透し、最近はインターネットの普及と相まって、それぞれのコンピュータがネットワーク化されつつあります。

特に、インターネットは国境という概念を超越したグローバルな広がりを包含しています。そこでは利便性は向上したもののこれまで考えられなかったような危うさをもたらしたともいえます。

2．情報セキュリティ技術と暗号技術

情報セキュリティ技術は、ユーザーが使用するサービスに組み込まれ、通常は意識されないようになっていますが、その目的は、脅威(攻撃)から、システムを保護し、円滑にサービスを提供し続けることです。



図－1　情報セキュリティシステム技術の概要

システムに対する代表的な脅威としては、メールや電磁媒体を介して媒介されシステム破壊や個人情報の流失を招くコンピュータウィルスやコンピュータ、ネットワークに不正侵入し、コンピュータやネットワーク上にある情報の盗聴や改ざん等が考えられます。

情報セキュリティ技術は、安全な通信の手順を定めたセキュアプロトコル技術、ネットワークやコンピュータ間での認証の手続きを定めた公開鍵基盤(PKI)構築技術、安全なコンピュータシステムを構築するためのセキュリティシステム構築技術等の情報セキュリティシステム構築技術から成り立っています。さらに情報セキュリティシステム構築技術における安全性は、個人認証技術、侵入検知技術、アクセス制御技術、暗号技術等の情報セキュリティ要素技術により支えられています。中でも、暗号技術は情報セキュリティシステムを支えるキー技術となっています。

暗号技術自体は、従来は軍事・外交の分野を中心に使用されてきたため、一般ユーザーにはなじみが薄く、小説等を通して目に触れる程度でした。しかし、近年の情報化・ネットワーク化の進展に伴い、急速に身近な技術となってきています。特に、1970年代後半に相次いで発表された公開鍵暗号技術や米国標準暗号DES(Data Encryption Standard)といった技術は、「現代暗号技術」の名にふさわしい新たな技術を生み出すに至っています。

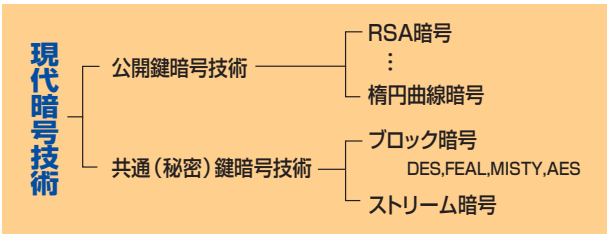
3．現代暗号技術

暗号技術とは、ある情報を特定のグループ内で共有し、第三者に対し漏洩することを防止する技術です。特に、情報セキュリティ技術を支える現代暗号技術は、コンピュータの発達とともに生まれたといっても過言ではありません。この現代暗号技術は、公開鍵暗号技術と共通鍵暗号技術に大別され、この2つの方式が組み合わされて用いられてます(図－2、3)。

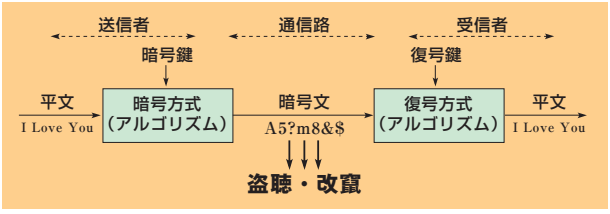
3．1 共通鍵暗号技術

共通鍵暗号とは、情報の送り手(送信者)と受け手(受信者)の間で「(共通)鍵」と呼ばれる情報を共有している場合にのみ正しく情報が伝達できる仕組みです(図－4)。

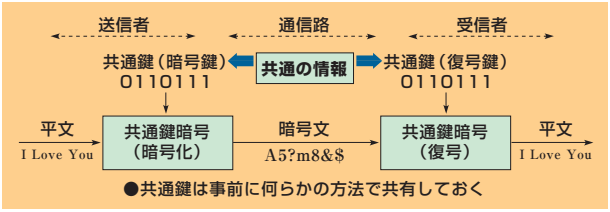
現代暗号としての共通鍵暗号方式は、1976年に米国政府により連



図－２　現代暗号技術の分類



図－３　暗号の原理



図－４　共通鍵暗号の原理

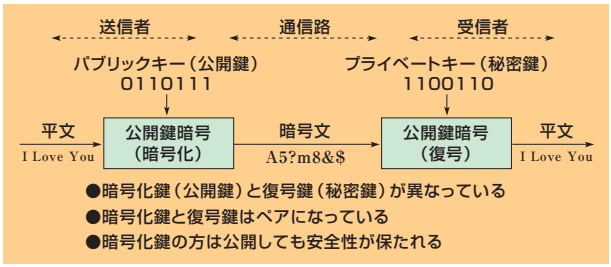
邦情報処理標準(FIPS: Federal Information Processing Standard)として制定されたデータ暗号化標準DES(Data Encryption Standard)に始まります。この暗号方式の特徴は、暗号アルゴリズム(情報を暗号化するための手続き)を公開したことです。それまでの共通鍵暗号方式は、鍵ばかりでなく暗号アルゴリズムも秘匿されているのが当然でした。しかし、インターネットのようなオープンな環境では、暗号アルゴリズムは様々な形態で、不特定多数に配布されるため、暗号アルゴリズムの秘匿は事実上困難となっています。逆に、積極的に公開することにより設計者自身の評価だけでなく、第三者の安全性評価を受、信頼性の向上が期待できるメリットもあります。

３．２共通鍵暗号の安全性評価

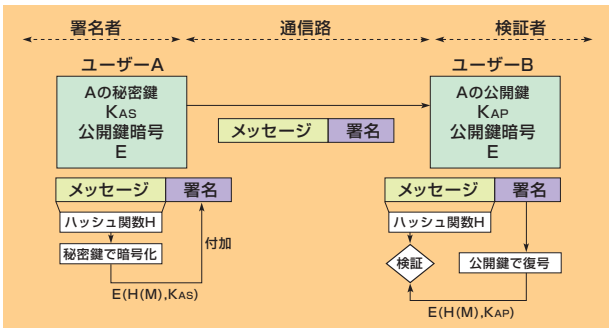
では、現代の共通鍵暗号は、どのように安全性を評価しているかを概観してみましょう。現代暗号の安全性は、暗号解読と密接な関係があります。ここでの暗号解読とは、平文(元の情報)に関する情報と暗号文から鍵を推定することをいい、暗号の強度とは暗号解読に必要な情報量と計算量といい換えることができます。具体的な、解読の方法には全数探索法、差分解読法、線形解読法といった様々な解読法があるため、各々の解読法ごとに評価する必要があります。

３．３ 公開鍵暗号方式

1976年に、DiffieとHellmanによって見いだされた「公開鍵暗号方式」は、現代暗号を代表する暗号方式です(図－５)。公開鍵暗号方式では、暗号アルゴリズムだけでなく暗号化に用いる鍵(暗号化鍵)さえも公開しても安全性が確保できる方式です。暗号化鍵を公開してしまうことから「公開鍵暗号」と呼ばれます。さらに、この「公開鍵暗号方式」のもう一つの特長に「ディジタル署名」という機能があります。この「ディジタル署名」は、ネットワークの中で、「印鑑」や「サイン(署名)」の代役を果たす機能であり、認証書(証)をベースとした「公開鍵暗号基盤(PKI：Public Key Infrastructure)」の基本技術となっています(図－６)。



図－５　公開鍵暗号の原理



図－６　ディジタル署名

公開鍵暗号方式の代表例が、1977年にRivest, Shamir, Adelemanの３人によって発明されたＲＳＡ暗号です。RSA暗号は大きな整数に関する「素因数分解問題の困難性」を安全性の根拠としています。このＲＳＡ暗号も、暗号解読技術(素因数分解能力)の向上に伴い、暗号の鍵の長さが長くなる傾向にあり、使いにくくなりつつあります。

そこで、代数学の成果を利用した「楕円曲線暗号」という新しい公開鍵暗号方式の研究が活発に行われています。

４．まとめ

ネットワークの発達に伴い、身近な技術となりつつある情報セキュリティ技術と暗号技術の最近の動向をご紹介しました。この分野は、現在もっとも研究開発が活発な分野の一つであり、目が離せない技術といえます。