（1） 暗号について

情報セキュリティ技術の代表が、やはり暗号技術です。暗号というと、戦争の最前線と参謀本部の間の通信内容が敵に傍受されないようにする技術というイメージが強く、今のような平和な世の中では、そこまで必要ないのではないかと思う方もおられるかもしれません。しかし残念ながら世の中にはネット社会になったことを利用して、悪事を働く人が後を絶ちません。そのためいろいろな情報セキュリティの脅威が存在しています。暗号技術はそれらの脅威のうち、盗聴、成りすまし、不正アクセス、改ざんに対処することができます。

「盗聴を防ぐ」というと暗号のイメージにはぴったり合いますが、「成りすまし」や「不正アクセス」、「改ざん」を暗号技術を使って防ぐことができるのかどうかは、疑問に思われる方を多いと思います。それらを実現するために、暗号技術にもいろいろな種類があります。それらをご紹介したいと思います。

（2） 盗聴を防ぐ暗号

例えば、企業秘密の文書をメールで送るとき、通信経路上で傍受されて盗聴される恐れがあります。そのため、通信経路上は暗号をかけて送り、盗聴から機密情報を守ります。その時に使用する暗号を共通鍵暗号といいます。「共通鍵」などといきなりわからない言葉が出てきましたが、そもそも「鍵」とは何なのか？

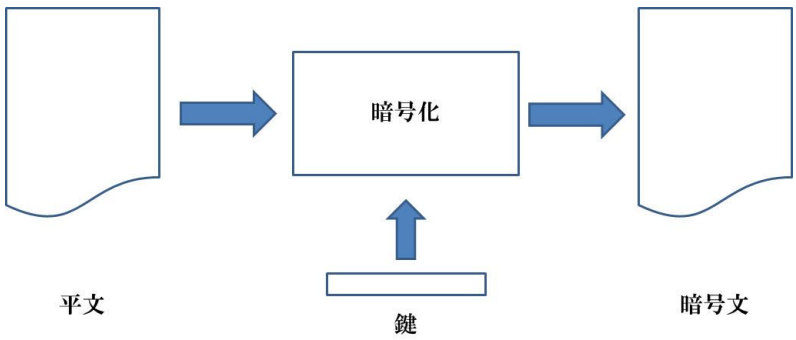
子供のころ、暗号表（例えば下の表のような）を最初に決めておいて、D4C2D5B2C1C2E2F4A3 などと秘密の告白を仲のいい友達だけにそっと教えたりしませんでしたか。この表をお互いに持っておけば、他の人にはわからないように情報のやり取りができますが、この暗号表が「鍵」に相当します。

	A	B	C	D	E	F	G
1	ら	わ	あ	か	さ	た	な
2	り	を	い	き	し	ち	に
3	る	ん	う	く	す	つ	ぬ
4	れ		え	け	せ	て	ね
5	ろ		お	こ	そ	と	の

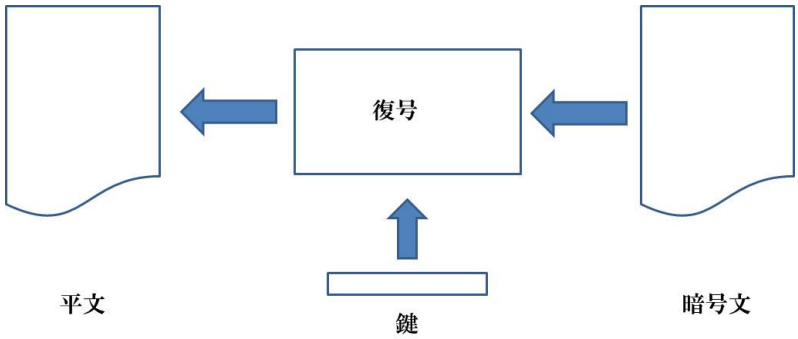
実際にコンピュータではどのように暗号化がされているのでしょうか。暗号処理を簡単に図示しますと、下の図のようになります。暗号をかける前の状態を「平文」と呼びます。それに対して暗号化された情報が暗号文です。暗号化というのは、平文と鍵と呼ばれる情報を入力として、なんらかの演算を情報に施して暗号文という出力を出す処理のことです。先ほどの暗号表を例にすると、「けいこをあいしてる」という平文と暗号表という鍵を入

力として、平文の一文字一文字を暗号表のアルファベットと数字の組み合わせに変換するという演算を施すと、「D4C2D5B2C1C2E2F4A3」という暗号文が出力されるということです。逆に暗号文をもとの平文に戻すことを復号といいます。暗号文と鍵を入力として、平文が出力として出されます。先ほどの例では、「D4C2D5B2C1C2E2F4A3」という暗号文と暗号表を入力として、「けいこをあいしてる」という平文が出力されるわけです。

暗号化



復号



さて、暗号処理では、この「鍵」を用いて暗号化したり、復号したりしますが、共通鍵暗号というのは、暗号化のときと復号のとき同じ鍵を用います。つまり、送信者と受信者が同じ鍵を持って暗号のやり取りをするということで、共通鍵暗号と呼ばれます。

共通鍵とわざわざいうということは、共通ではない鍵の暗号があるのではないかとお思いになるのではないでしょうか？お察しの通りです。共通鍵暗号を別名「対象鍵暗号」と呼びますが、それに対して「非対称鍵暗号」というものがあります。通常は「公開鍵暗号」と呼ばれ、まさに暗号化の時に使う鍵と復号の時に使う鍵が異なるという特徴があります。このような鍵をどのような目的で使うのでしょうか。なぜ公開鍵などと呼ぶのでしょうか。