情報セキュリティ歳時記 17

大衆化した暗号技術

前川　徹
早稲田大学 国際情報通信研究センター

➲ 軍事利用からコードレス電話へ

かつて暗号は，主に軍事や外交といった世界で用いられる特殊な技術であった．たとえば，昨年10月末にNHKがBS-1で放映した番組「ステーションX～イギリス・暗号解読作戦～」で取り上げられたEnigmaは，第二次世界大戦中にドイツ軍が用いていた暗号であるし，米国がPurple（紫暗号）と名付けた暗号は，日本が1930年代終わりから1945年まで利用していた外交用暗号である．ちなみに連合軍は，かなり早い時期にこの2つの暗号の解読機を開発し，日独の軍事上の機密情報を分析しており，これが第二次世界大戦の行方を大きく左右したといわれている．しかし，情報技術の発達とインターネットの普及によって，暗号は特殊な世界の技術ではなく，きわめて身近な技術になっている．我々の暮らしに不可欠な技術になっているといっても過言ではないだろう．ただ，多くの人は，自分が暗号を利用しているとは思っていないだけである．

たとえば，多くの家庭に普及しているコードレス電話にも暗号技術が使われている．子機と親機の間は電波で通信が行われているが，この通信は第三者に盗聴されても，その内容が分からないように暗号化されているのである．同様に，ディジタル携帯電話やPHSにも，盗聴防止のために暗号技術が使われている．もしこれが暗号化されていなければ，電話の盗聴はきわめて容易になり，盗聴マニアが増えて大変な社会問題になっているに違いない．

また，通信衛星を利用したディジタル有料放送が徐々に普及しつつあるが，ここにも暗号技術が利用されている．契約者だけが番組を見られるようにするために使われているスクランブル技術は，一種の暗号技術である．さらにディジタルコンテンツの著作権保護にも暗号技術は役立っている．たとえば不正コピーを防止するためにDVDビデオのコンテンツはある種の暗号によってスクランブルがかけられている．

もちろんいうまでもなく，企業にとっても暗号技術はきわめて重要なものになっている．ネットワークによってさまざまな情報を交換する際に重要な情報は暗号化して送ることは常識になっているし，相手を確認する際に利用されている認証技術の1つであるディジタル署名は暗号技術の応用である．個人の場合でも，インターネット・ショッピングでクレジットカード決済を選ぶと，しっかりしたサイトなら，クレジットカード情報の盗聴を防ぐためにWebサーバとパソコンの間の通信は暗号化される仕組みになっている．

かくして歴史の陰に隠れていた暗号技術は，我々のプライバシーやディジタルコンテンツの著作権，企業のさまざまな活動を守るために必要不可欠なものとなっているのである．

➲ 用語の定義と基礎知識

最初に多少の用語の定義が必要である．暗号化する前の文（普通に読める文）を「平文」と呼び，これを暗号に変換することを「暗号化」という．暗号を平文に戻す作業は，正規の受信者が正規の手続きとして行う場合と，本来暗号を読む権利を持たない第三者が行う場合があるが，ここでは前者を「復号」と呼び，後者を「解読」と呼ぶことにする．

歴史が古くかつ一般的な暗号の1つに「シーザー暗号」がある．これは文字をアルファベット順とかアイウエオ順，イロハ順に並べておいて一定の数だけずらした文字に変換するものである．たとえば，映画「2001年宇宙の旅」に出てくるコンピュータのHALはIBMを1字前にずらしたシーザー暗号だといわれているし，Windows NT，つまり，WNTはVMSのシーザー暗号だという説もある（DEC社でVMSを開発したプログラマたちがマイクロソフト社に引き抜かれ，そこで開発したOSがWindows NTだからだろう）．シーザー暗号は単純な暗号ではあるが，現在でも他の仕組みと組み合わせて使われている．

小説の中に登場する暗号もある．エドガー・アラン・ポーの「黄金虫」は暗号小説の傑作であるし，コナン・ドイルの（「シャーロック・ホームズの登場する」といった方が分かりやすいかもしれない）「踊る人形」も有名な暗号小説である．この2つの小説に登場する暗号は「単文字換字暗号」と呼ばれる．こ

れは文字の1つ1つを別の文字や記号に置き換える方法である．シーザー暗号も単文字換字暗号の一種と考えることができる．

こうした古典的な暗号は，現在では容易に解読することができる．たとえば，「黄金虫」に記述されたような文字の出現頻度から推測していく方法が，一般的であり，コンピュータを用いる場合には，2文字以上の連続した文字列の出現頻度も解読の重要な鍵になる．ちなみに英語の1文字出現頻度は高い方から（統計の取り方に依存するが），E, T, A, O, I, N, S, H, R, D, L, Uの順だとされている．

そこで，次に登場したのが「多表式暗号」である．これは平文を一定の長さで区切り，順次文字をずらす数を変えていく方法である．たとえば，平文を3文字単位で区切り，最初の文字は4つ，2文字目は7つ，3文字目は2つずらす，これを繰り返す方法である．分割する長さを長くすれば，解読はかなり難しくなるし，平文と同じ長さの鍵字列（順次ずらす量を並べたもの，前述の例では「4, 7 ,2」が鍵字列になる）を1度しか使わないようにすれば，理論的には解読不可能になる（1文字ずつずらす量が自由にできるということは，どんな平文でも長さが同じであれば同じ暗号文になる鍵字列が考えられるからである）．第二次世界大戦中および戦後しばらくの間，各国で使われた暗号の大半はこの多表式暗号であった．　この多表式暗号の最大の問題は，鍵字列の配布にある．鍵字列が短い場合や，同じ鍵字列を繰り返し使った場合には，解読される可能性が高くなる．したがって機密を要する情報を送るためには，十分な長さの鍵字列を安全に送る必要がある．もちろん，暗号化して送る情報と違って，時間をかけて安全に鍵字列を送っておけばよいのだが，これは容易なことではない．この欠点を克服したのが，「公開鍵暗号」である．公開鍵暗号については次回以降に説明しよう．

➲ DVDの暗号解読事件

暗号は価値のある情報を保護するために用いられる．したがって簡単に解読されては何の意味もない．しかし，Enigmaや紫暗号の歴史が物語るように，暗号は常に解読の危険にさらされている．

1999年11月初めに，DVDビデオの暗号が破られて大騒ぎになった．新聞でも大きく報道されたので，ご記憶の方も少なくないだろう．DVDビデオのコンテンツは，不正な複製を防止するためにContent Scramble Systemという方式で暗号化されている．使用されている暗号鍵の長さは40ビットである．これは暗号研究者からみると信じられないほど短い鍵長である．

しかし，この解読事件の本質は鍵の長さにあるのではない．鍵の管理の問題なのである．

DVDビデオのスクランブルを解除する方法を発見したのは，ノルウェーの技術者たちだといわれている．彼らは，Linux用のDVDプレーヤソフトがないことを理由に，米国のXing社が開発したDVDプレーヤソフトを解析し，その結果としてDVDビデオの暗号を解読する方法を発見したのである．彼らは，復号に必要な鍵を手に入れ，これを組み込んだ「DeCSS」と呼ばれるソフト（DVDビデオのコンテンツを解読してハードディスクにコピーするソフト）を10月にネット上で公開した．11月中頃，映画業界の警告によってDeCSSは，オリジナルのサーバから削除された．しかし，このソフトはすでに無数のサーバに転載されており，その多くは現在も残っているという．考えてみればパソコンでDVDビデオの暗号を復号化してディスプレイに表示するのだから，復号化のために鍵もその中にあることは容易に想像がつく．優秀な技術者であれば，どこを捜せば鍵が見つかるかが分かるに違いない．ハードウェアの場合なら，鍵を無理に取り出そうとすれば装置（あるいはその部品）が壊れるように細工することが可能である．不正な操作を受け付けないICカードやチップの中に重要な鍵を入れておけば，優秀なクラッカーでも鍵を盗むのは不可能だろう．しかし，ソフトウェアのリバースエンジニアリング技術の進歩を考えれば，ソフトウェアの中に重要な鍵を隠すのは賢明とはいえない．おそらく今回の事件の教訓はここにあるように思える．どんな強力な暗号を使おうと，システム全体として鍵管理の仕組みが不十分だと暗号は簡単に破られてしまうのである．

このDVDビデオ暗号解読事件のために，12月1日発売予定だったDVDオーディオ再生機の発売が延期されることになった．一部の報道では，DVDオーディオはDVDビデオより強力な暗号技術が用いられているので問題はないのではないかといわれている．しかし，映画の場合，1つのコンテンツが数ギガバイトもあるためインターネット上で不正コピーが流通する可能性が小さいのに対して，オーディオの場合は音声データであることと1曲単位で流通が可能という点で危険性は高くなる．米国のレコード業界は，これを懸念してより強力な不正コピー防止策を要求してきたのだと報道されている．

今月の参考文献等
1) 吉田一彦著: 暗号戦争, 小学館.
2) DVD ENCRYPTION CRACKED (2600.com) : http://www.2600.com/news/1999/1112.html

(平成11年12月13日受付)