2002-8-15

H. P. Report

第54号

発行責任者　稲崎義明

セキュリティと暗号（１１）

暗号の解読にはどういった方法があるのでしょうか。共通鍵や公開鍵などによって違うのかもしれませんが、今回は有名な話に基づいています。

暗号の標準方式で有名なＤＥＳというものがあります。この方法は、米国国家標準規格局(ＮＢＳ、現在の米国連邦標準･技術局（ＮＩＳＴ）)が連邦政府調達システム用の標準暗号として1973年に公募し1977年に標準暗号として規格化されたもので、不特定多数のユーザが利用することを前提とした共通鍵暗号で、アルゴリズムの処理手順は公開されているものです。この暗号は、発表後多くの研究者がＤＥＳの安全性に興味をもち、解読しようとしましたが、20年解読されなかったものです。この方式は、アルゴリズムが公開され、鍵データ以外の情報(暗号化する前の平文と暗号化後の文章)が分かっていると仮定しても、それらの情報から鍵データが推定できなかったわけです。

では、暗号解読にはどのような方法があるのでしょうか。一番簡単なのが｢全数探索法｣です。これは、考えられるすべての鍵の組み合わせを試して、正しい鍵を求める方法で、考え方年は簡単なのですが、計算量が膨大で、必ずしもすべての暗号を解読できるというものではありません。これば、例えば鍵の長さを56ビットとすると、鍵は2^{56}組、つまり約７京個の鍵を用意して計算する必要があります。これは、ＤＥＳが発表された当時のスーパーコンピュータを使っても２０００年かかる計算量となり、事実上解読不可能となっていました。そこに登場したのが１９９０年に発表された、後で言う｢差分解読法｣です。その当時、現ＮＴＴの開発した暗号｢ＦＥＡＬ｣が解読されたということで話題になったものです。この方法はブロック暗号(平文データを一定の長さに分割して暗号化する暗号)に適用されるもので、基本的な発想は、暗号化処理に潜む｢偏り｣を利用しようとするもので、このどの暗号にも潜んでいるわずかな相関を利用して、暗号解析に必要な計算量を劇的に減らそうとするものです。但しそのためには、解読者自身が解読しやすい平文を作って、それを解読者自身が暗号化した暗号文データを用意する必要があります。つまり、少しずつ内容を変えた平文を大量に用意することにより、それらの暗号文の内容を見比べることによって、暗号アルゴリズムの「偏り」を求める手法であるためです。この方法で５６ビットの鍵を使うＤＥＳの鍵データを解読するには、2^{48}組の平文と暗号文を調べればよくなります。これでも現実的な時間で処理できるといえるものではありません。

そこで登場したのが、三菱電機の暗号アルゴリズム｢ＭＩＳＴＹ｣の生みの親である松井氏の考案した「線形解読法」です。差分解読法が、あらかじめ偏りのでき易い平文データを利用する必要がある、解読者に非常に都合の良いものであるのに対して、線形解読法は、任意の平文と暗号文データのペアであれば解読でき、さらに条件によっては、暗号文データだけで解読できる特徴があります。この方法で、松井氏は、１９９４年に、ＣＰＵがＰＡ－ＲＩＳＣ（９９ＭＨｚ）のワークステーション１２台を使って、2^{43}組の平文データと暗号文データを用意することによって長年解読者の夢であったＤＥＳの暗号鍵を５０日かけて解読することに成功しました。解読はされましたが、これでこの暗号が使い物にならなくなったというものではありません。2^{43}組の平文、暗号文データが必要で、さらに５０日もかかったわけですから。しかし、それでもこれまでの解読法に比べて強力で、画期的であったことは間違いありません。（次回へ続く）

(情報誌トピックス)

○日経エレクトロニクス　８月１２日号

特集　知財力で勝つ

→日本の生き残る道はどこにあるか。「モノ作り」でひたひたと日本を追う中国。「知恵作り」でさらにと先へ進むアメリカ。これからの日本は「知」にかける。知的財産を最大限に活用し、国をあげて知的財産立国を目指す。

解説　動画圧縮の進歩が止まらない 一足飛びでＨＤＴＶを身近に

→ＨＤＴＶ画質の映画を６Ｍビット/秒で実現。高効率の画像圧縮技術が登場している。これによって２時間のＨＤＴＶ画像を現在のＤＶＤディスク１枚に入れることも、現在のＡＤＳＬ回線で高画質の放送サービスが可能になる。まだ先と思われていたサービスが身近になるかもしれない。

○日経パソコン　８月１９日号

特集　２４時間電源ＯＮ

→Ｗｉｎｄｏｗｓ ＸＰの省電力設定によって、２４時間電源ＯＮのパソコンが使えるようになる。思い立ったらすぐに使える。２４時間パソコンの実現方法から、何がどう変わるかを解説。

特集　Ｏｕｔｌｏｏｋ２０００/２００２活用大全

→ＯｕｔｌｏｏｋとＯｕｔｌｏｏｋＥｘｐｒｅｓｓはどこが違うか。ＯｕｔｌｏｏｋＥｘｐｒｅｓｓｆ伝メールのソフトであるに対して、Ｏｕｔｌｏｏｋは個人情報管理ソフト。なかなか使いでのあるＯｕｔｌｏｏｋを紹介。

特集　最新ＰＣで９８/２０００を使う

→新しいパソコンのＯＳはＷｉｎｄｏｗｓＸＰ。これは、マイクロソフトのソフト出荷が終了したためだが、いろいろ事情によって、９８を使いたいこともある。メーカごとに使えるかをチェック

○日経ネットビジネス　８月１０日号

特集　ネットで壊す流通の方式

→インターネットは、これまでの流通の仕組みを変えていく。大手小売は、弱体化した中小の店舗を系列として抱え、卸は非効率な流通手段として危機的状態にある。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　９月１日号

特集　大容量･激安最新ＨＤＤ３６０°徹底検証

→次世代のＨＤＤインターフェースはＳｅｒｉａｌＡＴＡとなる。パラレルのフラットケーブルからシリアルのケーブルになり、高いＡＴＡとの互換から、現在のＩＤＥのＨＤＤも使用できる。この新しいインターフェースの紹介。

特集　リモコンソフト遠隔操作三昧

→常時接続環境が一般化している。自宅のパソコンも外出先から使いたい。そんなＰＣのリモコンソフトの使いこなし方と、セキュリティの問題点を紹介。