2002-8-1

H．P．Report

第53号

発行責任者 稲崎義明

セキュリティと暗号（１０）

暗号化について、いいかげんな内容で書こうと思っていたのですが、具体的なものが見つかったので説明してみます。暗号としては「換字暗号」というもので、元の文字を一定の規則に従って別の記号に置き換える暗号で、例えば「ＨＡＬ」という会社があったり、映画に出てくるコンピュータの名前であったりしますが、この「ＨＡＬ」は「ＩＢＭ」を一字だけずらして（Ｉ→Ｈ、Ｂ→Ａ、Ｍ→Ｌ）作られています。もっと具体的な例として、次のような暗号があったとします。

53++!305))6*;4826)4+.)4+);806*;48!8'60))85;]8*:+*8!83(88)5*!;
46(;88*96*?;8)*+(;485);5*!2:*+(;4956*2(5*-4)8'8*;4069285);)6
!8)4++;1(+9;48081;8:8+1;48!85;4)485!528806*81(+9;48;(88;4(+?3
4;48)4+;161;:188;+?;

まるで記号の羅列ですが、記号ごとの個数を見てみると、「８」が33個、「；」が26個あります。前提としてこの文章が英語であるとすれば、統計的に最も出現頻度が高いのが「ｅ」であるらしいので、「８」を「ｅ」としてみます。次に８の出るパターンを調べてみると、「；４８」というのが何回かありますが、これをよく出てくる「ｔｈｅ」と仮定すると「；」が「ｔ」、「４」が「ｈ」ということになります。このように手間隙をかけ、繰り返し検討することによって、解読することができますが、暗号化の方法が最後まで同じであるため、文章が長くなることによって解読することも容易になってきます。そこで、何文字づつずらす（ＩをＨにずらすように）などといった規則を文字ごとに変化させる方法が考えられ、この何文字ずらすかと要ったことを数字にしたものを鍵といいます。またこれが乱数にもなります。乱数はランダムな数字の列ですから、それが知られなければ解読されることもありませんが、送り側と受け側だけでも同じ乱数を持っている必要があります。また、コンピュータの作る乱数は完全な(循環しないランダムな数字列)ではなく、擬似乱数で、その長さ(鍵の長さで、暗号の強度と大体正の相関関係がある)を通常ビット数で表します。では、実際にどのような風になるか暗号を作ってみます。

まずもとの文章、これを平文といいますが、これを″ｔｈｉｓ　ｉｓ　ａ　ｐｅｎ″とします。鍵として４桁の数字を用いることとして”１９８２”とします。これを平文に合わせてみると、″ｔ１ｈ９ｉ５ｓ６　１ｉ９ｓ５　６ａ１　９ｐ５ｅ６ｎ１″となり、数字どおりに文字をずらしてみると″ｕｑｎｙａｒｘｆｂｉｕｋｏ″となり、これで暗号化されたことになります。

このような暗号化するようなプログラムは、プログラムがある程度できれば簡単につくることができます。逆に解読しようとすれば、鍵の長さが分かっていて、今回のように４桁の数字(１０進の４桁なので２進で言えば１４ビットになりますが)であることが分かっていれば、鍵のデータを０から順に、先の暗号化するプログラムを逆にして当てはめてみて、出てきた文章がおかしくないかどうかをみてみる、総当りでおこなったとしてもすぐに解読できてしまいます。なんだ簡単だと思われがちですが、通常の暗号は１２８ビットぐらいを使っています。１４ビット程度であればすぐ終わるのですが、１２８ビットだと２の128乗回試すことになり、１秒間に１０億個の鍵が試すことのできる計算機が１０億台あったとしても、すべての鍵を試すには１０兆年かかってしまいます。これでは大変ということで、いろいろな解読方法のアルゴリズムが考えられています。

（次回へ続く）

(情報誌トピックス)

○日経エレクトロニクス　７月２９日号
特集　ハード設計の危機をソフト技術者が救う
→ソフトウェアを設計するのがソフト技術者、ＬＳＩを設計するのがハード技術者であったが、プログラムがそのままチップになるハードウェアコンパイラの登場によって、ハードの設計をソフトウェア技術者ができるようになってきた。ＬＳＩの設計にＣ言語が積極的に導入されてきている。
解説　「グリッド」の真実
→グリッドコンピューティングとは、ネットワークでつながった無数のコンピュータが、1つのアプリケーションを並列処理するもので、地球規模で処理を実行する巨大なコンピュータがネットワークの高速化に伴って登場する。

○日経パソコン　７月２２日号
特集　ＥＸＣＥＬ必修テクニック
→ＥＸＣＥＬはもっと便利に効率よく使えるソフト。かといってすべての機能を知っている必要はない。データ入力と表計算を効率的に行うには、数値/日時/文字を自在に計算させるには、条件を使って作業を楽にするにはなど、つぼを押えたテクニックを紹介。
解説　ＵＰｎP&サーバ対応の最新ルータガイド
→インターネットに複数台のパソコンを使う場合によく使うダイヤルアップルータにもいろいろある。ビデオチャットで会話しようとすれば、ＵＰｎＰ機能がないとつながらない。常時接続でＷｅｂサーバを立ち上げようとするときには、セキュリティ機能が充実したものを選びたい。安くなったといってもせっかくなら使い方にあったものを。

○日経バイト　８月号
特集　ＵＭＬの真実を探る
→システム開発でＵＭＬが注目されている。ＵＭＬはオブジェクト指向に基づく開発に用いられるもので、ＵＭＬ自体は単なる絵を書くもであるが、対象となるシステムを図で設計する場合に有用なもので、システム開発工程において分析や設計などのモデリングを行うために利用される。
特集　ＩＰｓｅｃの理想と現実
→インターネットにはセキュリティの保証がない。ＩＰｓｅｃはそういった問題を解決するために、ＩＰの欠点を補うために考慮されたプロトコルで、鍵交換、通信時の制御ヘッダ、暗号化方式など複数の仕様で規定されているもので、将来の拡張性も持っている。
解説　ＦＴＴＨは本当に広まるのか
→高速通信の最終形であるＦＴＴＨ。いろいろな会社の参入など話題は多いがなかなか広がっていない。現状のままでどこまで広がっていくのか。

○日経ネットビジネス　７月２５日号
特集　ネット戦略失敗が残した果実

→ネットビジネスに参入し、苦汁を舐めた企業が増えてきている。しかし、ネットビジネスに失敗してもその経験が次へのステップとなっている。

○N＋I　NETWORK Guide　8月号
特集　基本から分かる最新無線ＬＡＮ
→５４Mの高速性を持つ８０２．１１Ａの登場、セキュリティを解決する８０２．１１Ｘなど無線ＬＡＳＮが注目されている。現状の技術内容から、最新システムの構築方、実際の構築事例まで紹介。
特集　そのバックアップとリカバリは無駄だらけ
→何気なくやっているようなバックアップを再検証。正しいバックアップと、何かあったときのリカバリの方法は。その効果的な運用のポイントを探る。

○ＡＳＣＩＩ　8月号
特集　パソコン超ディフェンスガイド
→ウィルスやクラッキングを対岸の火事と思っていては間違い。欧米に比べて日本の個人ユーザのセキュリティ意識は非常に低い。セキュリティの怖さと現状、対策を紹介。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　8月１５日号
特集　最速プラットフォーム決戦
→メモリがＰＣの性能を左右する。現在メモリにはＤＤＲとＲＤＲＡＭがしのぎを削っているが、チップセットベンダーの思惑とＤＲＡＭベンダーの間がどうなっているか、現状のレポート。
特集　書き換え型ＤＶＤ完璧ナビゲータ
→複数の規格が乱立する書き換え型ＤＶＤ。現在ＤＶＤ Ｍｕｌｔｉ とＤＶＤ+ＶＲが火花を散らしている。現在の商品紹介と、とことん使い切るにはどうすればよいか。