2002-7-15

H．P．Report

第52号

発行責任者　稲崎義明

セキュリティと暗号（9）

今回から暗号の話です。といってもなかなか資料がなくて困っているのですが、暗号といえばスパイが使うものという感じがします。これまでの暗号は、内容を別のものに置き換えて、それだけでも文章になっているが、意味は最初の取り決めどおり別のものになるもの、例えば日本軍の「トラトラトラ」のようなものなどが思い浮かぶと思います。日常使っている文章の中に暗号を混ぜてみたり、前後関係で暗号であったり、なかったり（特別な言葉があれば、そのあとが暗号だったり）などいろいろな方法があったようです。また、現在でも工作員がつかまると、持っているものの名が乱数表があったりしますが、これも暗号をつくったり、解読したりする場合に必要なものです。日本語を含めて、アルファベットなどもご存知の通りコードがつけられています（情報機関の使うコード費用が一般的なコード表と同じとは考えませんが）が、このコードをそのまま送っては意味がありません。そこで、暗号に変換するわけですが、通常のコードを何番に変換するかの変換テーブルが乱数表です。たとえば「２３」と送られてくれば、乱数表の23番目の値が正しいコードとなる様にです(実際はこんな簡単ではないでしょうが)。これは工作員が暗号解読器を持っていないため、手作業で送られてくる暗号に対処しようとすれば、このような変換表に基づくのが簡単であるためです。これもいわば秘密鍵方式で、乱数表を奪われてしまえば相手に暗号を解読されてしまいます。コンピュータのないころや持ち歩くわけに行かない場合はよく使われているようです。その後情報機関の暗号には暗号機が登場し、自動で暗号の作成や解読ができる物でした。この暗号機は器械計算を行うもので、いろいろ有名なものがあったようです。

暗号というわけではないのですが、古代文字の解読も暗号のようなものです。中にはいまだに解読されていないインカ文字などもあるようですが、ここではエジプト文字を取り上げます。エジプト文字の解読にはご存知の通りロゼッタストーンが欠かせません。ロゼッタストーンはナポレオンがエジプト侵略を行った際に、地中海から攻めて来る、イギリス軍に対応するために、海岸防備の強化の一環として要塞の修復工事を行った際に見つかったもので、エジプト文字である「ヒエログリフ」と民衆の言葉「デモティック」、「ギリシャ文字」の3層が書かれたものでした。文章の内容は同じであったため、その比較を行うことにより解読することができたものです。とはいってもその解読には20年を有しました。それは、ギリシャ文字などは音を表現する表音文字であるに対して、ヒエログリフは、あるときは意味を表す表意文字であったり、あるときは表音文字であったりしたためです。解読したシャンポリオンもまず表音文字としての機能から解読し、それでは分からない部分を表意文字の特性から解読していきました。このとき、表音文字の解読の際に、文字に含まれる表音の中で最も多いのが何であるか(確か「ｅ」だったと思うのですが)ということから、最も多く出てくる文字をその音と仮定したりしながら解読していきました。

古代文字は、分からなくしようとなっているわけではないのですが、暗号を解読するという点から、旧式の暗号の場合よく分かる例ではないでしょうか。また、現代の暗号化は、文字をすべて数字として捉えて暗号化していますので、どちらかと言えば完全に数学の世界になっています。例えば、暗号として楕円曲線暗号や、暗号を解く方法も、線形解読法などといった数式による解析がなど行われ、解読する場合には計算機による計算の繰り返しによって行われるようになっています。（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１５日号
特集　センサがネットにつながれば
→センサがネットワークにつながったらどうなるか。これまでセンサをネットにつなぐのは工場だけだったが、センサの小型、低価格化とネットワークの普及によっていろいろなセンサがつながるようになってきている。街角監視カメラのネットワーク化もその1つで、高齢化社会に対しても便利なことは多いのだが。
解説　記録型ＤＶＤの未来 規格争いの先にあるもの
→記録型ＤＶＤには、追記型の「Ｒ」のほかに書き換え型の「－ＲＡＭ」、「－ＲＷ」、「＋ＲＷ」などがあるが、機器としては複数の規格に対応したものが登場する一方、安価な追記型のものの需要が増える。

○日経パソコン　7月８日号
特集　９８&Ｍｅの定番トラブル５０
→既に市場に出なくなった９８とＭｅだが、ここで定番ともいえるトラブル５０を紹介し、再確認を行う。
特集　目的最優先のＷｅｂサイト作成法
→ネットで仕事仲間や友達との情報共有を行うためのＷｅｂサイトを無料でかつ１０分で作るサービスを紹介。できるのは、デジカメの画像閲覧と掲示板、ファイル共有の３つ。

○日経オープンシステム　7月号
特集　必要とされるＳＥ
→必要とされるＳＥの確保が難しくなっている。ＳＥのプロが少ないなど需給バランスが悪いためで、ベテランＳＥが言うＳＥ像は何か。ユーザの目的を達成できることが第一条件で、役割ごとにプロの技術スキルが求められる。
検証　ＭｏｚｉｌｌａやＯｐｅｒａでＩＥを置き換える
→セキュリティの問題からＩＥを別のものに書き換えられるか。ＨＴＭＬやＪａｖａＳｃｒｉｐｔなどの互換性はどうか。ＭｏｚｉｌａやＯｐｅｒａの日本語版の実用性を検証。

○日経ネットビジネス　7月１０日号
特集　ネットビジネス幼年期の終わり
→各企業のネットビジネス部門が収束したり、吸収されたりすることによって変化している。すべてのビジネスがネット対応になる今後をどのように対応していけばよいか。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　8月1日号
特集　最新鋭チップセット完全マスター
→今後新しいチップセットが登場してくる。ＣＰＵもメモリ規格もインターフェース規格もＩＤＥ規格も何から何まで代替わりの時期を迎えている。チップセットの基本から最新テクノキーワードとこれから登場するチップセットのスペックまでを紹介。
特集　ＦＴＴＨ選択の基準
→各家庭へのネットワークの再集計となるＦＴＴＨ。既存の電話線を使え

るＡＤＳＬは爆発的に普及したが、ＦＴＴＨはなかなか価格も高く普及もしていない。現状はどうなっているのか。利用したいのだけれどもどうすればよいかを紹介。