2002-6-1

H．P．Report

第49号

発行責任者 稲崎義明

セキュリティと暗号（6）

今回から暗号についてです。暗号はずいぶん昔から利用されていたもので、戦争やスパイ映画なんかでは必ずといってでてくるものです。初めは、内容だけを伝えるもので、ある一定の法則でアルファベットを文字ごとに置き換えることによって全く意味のない文章にするものや、単語ごとに別の言葉に置き換えるものなどが使われたようで、よく乱数表などがスパイの持ち物に出てきたものです。第二次世界大戦になると暗号用の機械などで自動化されていたようです。これから説明する通信の暗号はこれらの発展形で、コンピュータが利用するためにより複雑になっているものです。

前に書いた無線ＬＡＮのＷＥＰという暗号を再度説明すると、この暗号には「ＲＣ４」というアメリカのメーカが開発した関数が登場します。送る際に送るメッセージデータのほかに初期化ベクトルと鍵データが必要となります。ここであとで説明しますが、暗号化には鍵データが出てきます。初期化ベクトルは24ビットの数字で、鍵データは40または104ビットの長さがあります(初期化ベクトルと合わせて64または128ビットになります)。このデータを「ＲＣ4」の関数に入れることによってランダムなデータが出力されます。このデータと送るメッセージデータの排他的論理和を取ることによって暗号化されます。送るときには、この暗号化されたデータに「ＲＣ4」に代入した初期化ベクトルを合わせて送信することになります。暗号を元にもどすときは、送信側と同じ鍵データを受信側は持っていますから、同じ様に初期化ベクトルと「ＲＣ4」に入れて出力されたランダムなデータを、受信データと排他的論理和をとることによってもとのデータに復号することができます。この際に排他的論理和を利用することがこの暗号方式の特徴で、排他的論理和は、ご存知の通り同じ値なら「0」、異なる値なら「1」にするというもので、複号化する場合も簡単なのですが、同じ初期化ベクトルのデータを数多く集めたり、相手に対して内容のわかっているメールを送信することによって、鍵データを解析することができることになります。この暗号の解読の仕方は以前書いたとおりです。

一般的な暗号についてですが、暗号には大きく2つの方法があります。ＷＥＰのところでもでてきましたが、暗号には鍵を使用します。いくらコンピュータが発達したといっても、何も情報がなければ受け取ったほうで復号化することができません。この暗号鍵には、ＷＥＰのように利用するものがすべて同じ鍵を持つ共通鍵暗号方式と、公開鍵と秘密鍵の2つを使用する公開鍵暗号方式があります。共通鍵方式は、送信側と受信側が同じ鍵を持つ必要があるため、鍵を盗まれてしまったり、鍵をずっと変えないため、解析により導き出されたりします。そこで考えられたのが公開鍵方式といって、暗号化と復号を別の鍵を使ってやろうとするもので、暗号化する鍵は一般に広く公開された鍵で、送信側はこの鍵を入手することによってデータを暗号化して受信側に送ります。受信側では復号するための秘密鍵を持ち、送られてきたデータを復号化します。公開暗号方式では秘密鍵は外部に出さないためデータを盗まれる危険性が、公開鍵方式に比べて少なくなります。最近はこれらの方式を組み合わせ、まず共通鍵方式でデータを暗号化し、共通鍵を公開鍵方式で暗号化して受信側に送る方式がよくとられています。受け取ったほうは、まず公開鍵方式で送られてきたデータを複合化することによって共通鍵を作り、その共通鍵でデータ本体を復号化します。この方式ではデータを送るたびに共通鍵をあらためて送るため、安全性と処理速度の両方を兼ね備えた方式となります。

（次回へ続く）

（情報誌トピックス）

○日経エレクトロニクス　５月２０日号
　特集　貴方のすき間にケータイ動画
　　→ケータイ動画は携帯電話の画面に表示される動画だけではなく、ＰＤＡでも、携帯用ビデオプレーヤでもいい。ちょっとしたときに5分から10分程度見れればいいものがケータイ動画。これまでの映像配信の考え方が変わる。
　解説　ケータイ電波の人体影響低減処理に待ったなし
　　→無線が氾濫している中で、携帯電話機に新たな規制が加わる。それが携帯電話から放射する電磁波がどれだけ人体頭部に吸収されるかの計測。対岸の火事ではない。

○日経パソコン　５月２７日号
　特集　Ｗｉｎｄｏｗｓデスクトップ操作の心得
　　→デスクトップはＷｉｎｄｏｗｓの画面のこと。使いやすいデスクトップ環境を作るにはどうすればよいか。アイコンの配置からタスクバーへのアプリの登録、壁紙、スクリーンセーバーまで自分なりにするには。
　特集　ｅ都市ランキング２００２
　　→2002年度版の全国自治体のｅ都市ランキング。トップから岡山、三鷹、可児など。ちなみに金沢は第6位、富山、福井はアンケートに未回答でランク外。

○日経バイト　６月号
　特集　携帯電話の未来
　　→6500万台が利用され、通話だけでなく8割はデータのやり取りや情報処理に使われている携帯電話。約10年ごとに変わる規格も3世代目のＩＭＴ－2000のサービスが始まってきている。今後の使われ方はどうなっていくのか。カメラか、テレビか、ナビゲーションか、コミュニケーションか。未来に対応する要素技術は。
　特集　目の前にあるネットの罠
　　→インターネットの危険性は、そんなサイトに触っていなくても陥る罠はある。勝手に国際電話の請求が着てみたり、見に覚えのないサービス料の請求がきたり。その手口を公開。対岸の火事ではない。

○日経ネットビジネス　５月２５日号
　特集　だめなＣＲＭはもう要らない！
　　→ＣＲＭ(カスタマー・リレーションシップ・マネージメント)とは、顧客一人一人と長く付き合うことによって、顧客が生涯にわたって企業にもたらす利益を増やそうとする経営手法で、顧客開拓をすると共にその顧客を大事にし、企業にとって利益のある顧客に育てようとするもの。ＣＲＭを成功させるには、社内をまとめる「キーマン」が必要。ＣＲＭ成功への7か条。

○Ｎ＋Ｉ　ＭＡＧＡＺＩＮＥ　６月号
　特集　社内ＬＡＮを限界まで使い切る
　　→社内ネットワークには、近年ＩＰ－ＶＰＮや広域イーとネットを導入

し、全体をＩＰネットワークに統合する動きがある。こうした場合、勘定系や情報系、音声系の情報が同じネットワークに統合されることが多い。こうした場合、他の影響が他のシステムに及ぼすことも考えられる。ネットワークを調査し、限界までネットワークを使い切るには。

特集　認証システム導入の最適解

→認証システムは会社のセキュリティを保つために書くことはできない。いかに最適な認証システムを構築するにはどうすればよいか。その基盤となる考え方を解説。

○ＡＳＣＩＩ　６月号

特集　プロバイダ選び最強鉄則はこれだ！

→現在プロバイダは淘汰され、大手の数十社が生き残っている。そのサービスも似たり寄ったりで、あまり選択の余地がなかったが、ブロードバンド時代になって、ブロードバンド専業か総合プロバイダかの選択が出てきた。今どのプロバイダを選べばいいのか。使い方を知友真にその選択肢を考える。

特集　記録型ＤＶＤの賢い買い方･使い方

→ＤＶＤ＋Ｒの登場で、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷの各機器がそろった。今買うべき記録型ＤＶＤはどれか。そのときＤＶＤによるビデオ作りとデータバックアップへの利用について。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　６月１５日号

特集　脱常識の自作ＰＣ

→現在自作に使用するマザーボードは以前に比べて高機能になっている。5.1ｃｈオーディオやＢｌｕｅｔｏｏｔｈ機能など。これら個性的なマザーボードを使って個性的な自分だけのＰＣを自作するには。