2002-6-15

H. P. Report

第50号

発行責任者　稲崎義明

セキュリティと暗号（7）

公開鍵方式ですが、公開鍵と秘密鍵の２つがあるとしましたが、実際の運用ではどうなるのでしょうか。共通鍵方式の場合、鍵を送信側と受信側で同じ物にする必要があります。そのために鍵をネットワークとは別に人為的にセットできるのであればよいのですが、ネットワークを利用しようとした場合、最悪鍵を暗号化しないで交換することとなってしまいます。そのためこのときに盗聴されてしまうと、そのあとのデータに対する暗号化は全く意味のないものとなってしまいます。公開鍵方式の場合、例えばネットワークで取引をしようとした場合、運用管理側では秘密鍵と公開鍵を用意することになります。この公開鍵を取引先に配信することになります。公開鍵では暗号化することはできますが、復号化することができないので、このときに盗聴されても必要なデータを解読されることにはなりません。ただし、公開鍵を利用してなりすますことはできるため対処の方法が必要となります。取引先では、必要な取引データをこの公開鍵で暗号化して運用管理者側へ送信します。運用管理者側では管理者側だけが持っている秘密鍵で復号化することができます。これが公開鍵方式で、誰でもがすぐに暗号化されたやり取りを行うことができるわけではないのです。

共通鍵方式の暗号方としてはＤＥＳ(Data Encryption Standard)が広く使われていますが、現在既にＤＥＳの暗号強度が充分でないとして、３回鍵を変えて暗号化する３ＤＥＳや、米国立標準技術研究所が定めたＡＥＳ(Advanced Encryption Standard)が使われるようになってきています。また、公開暗号方式としては、ＲＳＡ(Rivest, Shamir, Adleman)がよく使われ、他に楕円曲線暗号（ＥＣＣ:Elliptic Curve Cryptography)やＥ１Ｇａｍａ１暗号などが使われています。

さて、暗号化システムの使い方ですが、大きく2つの方法があります。1つはネットワークに流れるデータをすべて暗号化する方法で、もう1つが特定アプリケーションに暗号化システムを組み込む方法で、組み込むアプリケーションとしては、メールやＷｅｂアクセス、Ｔｅｌｎｅｔ、ＦＴＰなどです。

まずメールの場合ですが、一般にはＰＯＰやＳＭＴＰなどのプロトコルを用いてデータをやり取りするのですが、メール本体はＭＩＭＥという方式で変換して送信することになります。このＭＩＭＥは暗号化まですするものではないため、簡単に元にもどすことができます。そこで暗号化するためにはＰＧＰやＳ／ＭＩＭＥを用いるのが一般的です。この暗号化のソフトはフリーウェアで、暗号化の方法としては、共通鍵方式で暗号化し、その共通鍵を公開鍵方式で暗号化するという併用方法です。メールで公開鍵を利用する場合、その公開鍵が本当にメールを送りたい相手のものであるかを管理する必要があります。つまり、だまされてメールを送りたい相手の公開鍵ではなくて攻撃側の公開鍵を使って暗号化してしまうと、メールを受信した生気の相手が読むことができず、攻撃側だけがメールを読むことができるという状態に陥ってしまいます。そのため、入手した公開鍵が誰のものであるかを第三者が保証する仕組みが必要となります。この仕組みとして一般的なのが認証局(ＣＡ)を利用する方法です。ＣＡは公開鍵の身元を保証する機関で、ＰＧＰやＳ／ＭＩＭＥともにこの方式の鍵を利用することができます。ただ、友人同士のメールのやり取りにここまで大掛かりな方法をとる必要がないので、ＰＤＰでは、信用できる相手から受け取った公開鍵についても同様に使用できるようになっています。ＣＡには米国のVeriSign社など数社が認証局を立ち上げています。

（次回へ続く）

(情報誌トピックス)
○日経エレクトロニクス　６月３日号
　特集　五里霧中のデジタルテレビ不要論と向き合う
　　→本当に始まるのか始まらないのか･もともと２００３年に大都市でスタートし、２００６年には全国でスタート、２０１１年には現行のアナログ放送が終了する予定であったが、BSデジタルの大苦戦などから暗雲がたなびいている。機器メーカの切望のほかに、携帯電話やPDAなどへの利用のために別の方面からの期待が込められている。
　解説　第４世代通信サービス 無線LANショックで目前に
　　→移動体通信サービスで一人勝ちだった携帯も、ここにきて無線ＬＡＮが登場し、多様化が始まってきている。

○日経エレクトロニクス　６月１７日号
　特集　アイデアいっぱい 無線ならではの機器設計
　　→短距離無線通信機能をいろいろな機器が取り込むことによって、設計が変わりつつある。機能を複数の機器に分けて無線で接続したり、ネットワークに無縁だったものを無線で接続することによって、新たな分野ができつつある。
　連載として、暗号アルゴリズム「ＭＩＳＴＹ」の開発スタート

○日経パソコン　６月１０日号
　特集　ネットショッピングの心得
　　→常時接続環境が普及して、より便利になったネットショッピングを見直す。現在のネットショッピングの状況から、買い物するための基礎知識。

○日経オープンシステム　６月号
　特集　WWWシステムの性能を上げる
　　→システムを構築してカットオーバしたら性能が出なくなった。どこに原因があるのか。ボトルネックとなっているところは。使い方、アクセス数の想定から、事例を元にそのチューニング方法を探る。

○日経ネットビジネス　６月１０日号
　特集　ｅ－Ｊａｐａｎの「お値段」
　　→２００５年までにネットなどのインフラ構築に５兆円を投じ、１１１兆円の巨大なＥＣ市場を誕生させるというｅ－Ｊａｐａｎ戦略を徹底解剖。無限のチャンスがそこにあるが、一方問題点も多い。

○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　７月１日号
　特集　ＷｉｎｄｏｗｓＸＰツイーカーへの道
　　→ＷｉｎｄｏｗｓもＸＰになって使いやすくなってきている(実際はあまり使ってないので分からないが、らしい)。バージョンが上がるたびに、ＯＳ側で初心者にも使いやすいよう機能アップしているが、そのために重たいＯＳになっていることも事実。自分でカスタマイズすることによって、軽く、自分なりに使いやすくすることもできる。カスタマイズには、ＯＳ標準のプロパティの変更の段階や、カスタマイズ用ユーティリティの使用の段階、そしてレジストリの直接的変更の各段階がある。「ツ

イーク」とは標準カスタマイズツール「Ｔｗｅａｋ　ＵＩ」を使った、ユーザインターフェースをいじりまわすというところからきている。

特集　いまどきホームクライアントＰＣはこれだ

→予算18万で購入するホームクライアントＰＣ。家庭で必要な機能は、使いやすいＰＣは、各機種でどこが違うのか。購入を検討する前に。