キーワード②

ハッカーとクラッカー
暗号と認証
SSL（Webブラウザのセキュリティ対策）

大阪府立工業高等専門学校教授　高橋 参吉

クラッカーとハッカー

インターネット上でWebサーバやメールサーバ等のコンピュータシステムは，常に不正アクセスや攻撃にさらされている。サーバ内のファイルを削除や改ざんしたり，機能を停止させたり，意図的にインターネットに接続されたコンピュータ環境を破壊する行為をクラッキングという。このようにコンピュータ環境を破壊する人達をクラッカーと呼んでいる。

一方，ネットワークやソフトウェアの技術的な問題を発見したり，広く利用者に有効な技術情報を提供する人達にはハッカー（コンピュータに精通した人達を尊敬した呼び方）という言葉が使われてきた。また，ハッカーの行為をハッキングという。しかし，最近日本では，ハッカーやハッキングという言葉は，クラッカーやクラッキングと同じ意味として使われることも多い。

暗号と認証

暗号は，通信データを暗号文に変換することにより，暗号文が仮に盗聴されても，盗聴者に元の情報がわからないようにする技術である。すなわち，暗号化は，元の情報（平文という）に，ある数学的な変換をして，容易に元の文章に推測あるいは特定できないような暗号文にすることである。

暗号技術には，送信者及び受信者が共通の鍵で暗号化・復号化をする共通鍵（秘密鍵）方式，暗号化の鍵と復号化の鍵が異なり，暗号化鍵を公開し復号化鍵を秘密に保持する公開鍵方式の二つがある。

共通鍵方式では，送信者及び受信者が同じ秘密鍵を持つ必要があるので，鍵の送信が必要である。一方，公開鍵方式では，暗号化鍵が公開されているので，鍵の送信が不要であり，不特定多数間での暗号通信が容易となる。

＊鍵は暗号を復号するデータのことである。共通鍵方式の鍵は，普通の鍵のように閉めるとき（暗号化）と開けるとき（複号化）は同じ鍵であるが，公開鍵方式の場合は，閉める時と開ける時は，鍵が異なる。「閉める鍵」で閉めたあとは，専用の「開ける鍵」でしか開かないことになる。したがって，「閉める鍵」は，不特定多数の人に公開しても問題はない。

認証は，不法アクセス，データの改ざん，否認（情報を送信したのに送信者が送信してないということ）などの不正行為に対する対策技術である。相手認証は，ネットワークを通じて通信している相手が真の相手かどうか確認する技術で，認証技術の一つである。相手認証の方法には，パスワード，使い捨てパスワード，電子署名（デジタル署名）などを用いた認証方式が使われる。指紋・声紋・網膜の虹彩パターンなど本人の固有の特徴を利用して本人かどうかを確認する生体認証の技術の研究も行われている。

SSL（Webブラウザのセキリティ対策）

WebブラウザとWebサーバとの送受信についても，インターネット上での盗聴などに留意する必要がある。盗聴などの危険性からWebでの通信を守る方法として，SSL（Secure Sockets Layer）と呼ばれる暗号化通信技術が利用されている。WebサーバとWebブラウザがSSLに対応していることが必要であるが，Webブラウザの設定は，例えば，Internet Explorerの場合は，「インターネットのプロパティ（詳細設定）」によって行うことができる。

また，SSLに対応したWebサーバは，URLが「https://」で始まる。Webブラウザで，そのURLを指定すると，セキュリティで保護された旨のメッセージが表示される。Webブラウザの下部に，図1のようなロックマークが現れ，WebサーバとWebブラウザとの通信は暗号化されて行われる。

図1　SSLに対応したページにリンクした場合（Internet Explorerの場合）

SSLを利用するWebサイトは，あらかじめWebブラウザに登録されている認証局と呼ばれる会社から電子証明書の発行を受ける必要がある。ロックマークをダブルクリックすると電子証明書の内容を参照できる。