特集3 商・材・研・究

認証システム

安全なリモート接続を実現 Iネット VPN需要で注目

相手が見えないネットワーク上において、接続を求めるユーザーが本人であることを証明するために用いられる認証システム。インターネットVPNの利用拡大に伴い、その市場を一挙に広げそうだ。

インターネットを介した社内のシステムリソースへのアクセスに際して、接続を要求するユーザーが正当なユーザーであるかを確認し、第三者からの不正アクセスを防ぐものが「認証システム」だ。この認証システム市場が急速な立ち上がりを見せようとしている。

市場拡大の背景には、ファイアウォールや不正侵入検知・防御装置だけでは防ぎ切れない不正アクセスが多発していることがあげられる。

ブロードバンド・モバイル化の進展は、ビジネスのネットワーク利用を加速させている。イントラネットを活用した社内情報の共有化や関連企業を接続したエクストラネット、さらには顧客との電子商取引はごく一般的なものになりつつある。ここでは従来の固定回線だけでなく公衆無線LANサービスや第3世代携帯電話サービス等、どこからでも社内ネットワークへアクセスできる「ユビキタス環境」も整いつつあり、ビジネスにおけるネットワーク活用はますます進みそうだ。

こうしたインフラの整備によるネットワークアクセスの可用性が向上する反面、外部からの侵入の脅威にさらされる危険性も高くなっている。

中でも最近、注目を集めているのが、他人のユーザーIDやパスワードを盗用することで正規ユーザーを装う「なりすまし」だ。

現実の世界と違い、ネット上ではアクセスしてくる相手の顔を見ることはできない。悪意のある第三者が正規のユーザーになりすまし、社内サーバーに侵入、顧客データや製品開発情報等の機密情報を盗んだり、システムを改ざん、破壊する等の被害が相次いでいるのだ。

特に問題視されているのが個人情報の漏洩で、会員や顧客情報が流出した場合、企業の信頼性を著しく損なうだけでなく、損害賠償等の訴訟問題に発展するケースもある。

こうした悪意のユーザーによる不正アクセスを防ぐために、そのユーザーが本人であることを証明する認証システムが注目を集めているのだ。

不正侵入検知・防御装置
ネットワーク上を流れるトラフィックやパケットを分析し、それが正当なものか、不正なものかを判断、不正アクセスと思われる通信を管理者に警告あるいは遮断するシステム

IDパスワードでは不十分

認証システムと一口にいってもその種別はさまざま。ここでは代表的な認証方式を紹介していこう。

現在、市場に投入されている認証システムの種類には、①「IDパスワード」、②「ワンタイムパスワード(ハードウェアトークン)」、③「ワンタイムパスワード(ソフトウェアトークン)」、④「デジタル証明書」、⑤「認証用メモリーデバイス」、⑥バイオメトリクス(生体認証)」――等がある。

最も一般に認知、普及しているものが①の「IDパスワード」方式。

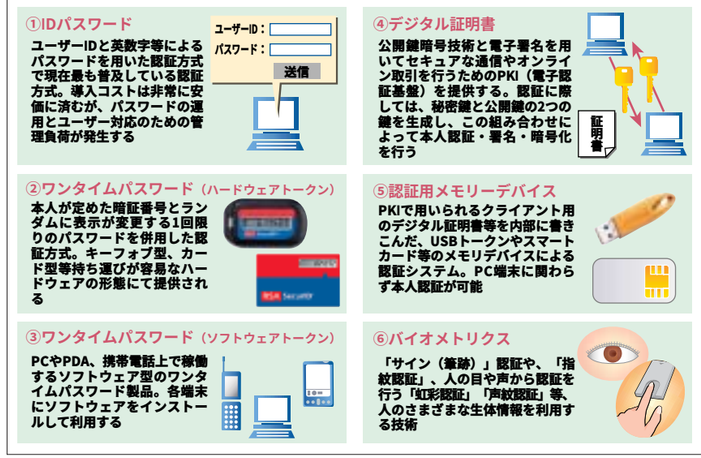
これは英数字や記号の任意の組み合わせによって作成されたユーザーIDとパスワードを用いて本人の認証を行うものだ。

IDパスワードは、固有のハード・ソフトウェアを必要としないため導入時のコストは無料であり、最も安価なシステム構築が行える。しかし、大規模ユーザーを対象とした場合、パスワードの管理やトラブル発生時のユーザー対応等、運用コストが高額になってしまうケースもある。

また、ユーザーが自分の誕生日や電話番号等、覚えやすい英数字を設定した場合、簡単に解析、盗用されてしまう危険性もある。

さらに、複数システムを利用するケースでは、セキュリティ上、それぞれ異なるIDパスワードを設定するのが望ましいが、ユーザー、システム担当者共にその管理が煩雑になってしまうという課題もあげられている。

図1 主な認証方式



盗用困難なワンタイムパスワード

次に②、③の「ワンタイムパスワード」を見ていこう。

ワンタイムパスワードは、認証のために一度限りしか使用できない、いわば「使い捨てのパスワード」で、通常の固定式のIDパスワード方式で危惧されていた「パスワードの盗用」という課題に対処したものだ。

サーバーや、トークンと呼ばれるパスワード生成システムから、「チャレンジ」と呼ばれる認証のための鍵が、ランダムな文字列によってユーザーに提示される。ここでユーザーはパスワードを入力、チャレンジとパスワードを一定のアルゴリズムを元に演算し、サーバーやトークンは生成された結果を検証し、正規のユーザーかどうかを調べる。

チャレンジは、毎回異なる文字列が提示されるようになっているので、同じパスワードが2度と使われることがない。そのため、IDパスワードを盗用されても不正アクセスの用途には利用できなくなる。

ワンタイムパスワードは、カードやキーホルダー型のパスワード生成装置を用いる「ハードウェアトークン」、PCやPDAにソフトウェア型のパスワード生成システムをインストールして利用する「ソフトウェアトークン」が製品として販売されている。

政府主導で広がるPKI

デジタル証明書は、PKI(Public Key Infrastructure：公開鍵暗号方

RSAセキュリティのハードウェアトークン製品「RSA SecurID」。上がカードタイプ、下がキーフォブ型


レインボー・テクノロジーズのUSB型認証デバイス