電脳博士Mr.HIROSEの ITこぼれ話

第12回 「認証のお話」

ITプランナー　廣瀬隆夫

先日、米国のカード会社の決済部門から4,000万件にも及ぶカード情報が漏洩したという事件が報じられました。すでに、その情報は詐欺師の手に渡って68,000件に上る不正行為が確認されたということです（2005年6月末現在）。漏洩したのは、厳重に管理されているはずのキャッシュカードで使われている氏名やパスワードです。便利なカード社会の脆弱性が露呈した事件でした。暴漢に会ったわけでもない、泥棒に入られた訳でもない、物は何も取られていないのに、銀行に預けたお金が他人に無断で使われる、こんな恐ろしいことが現実に起こっているのです。

何でこんなことが起きるのか？

皆さん、時代劇で忍者が「山」「川」と言って仲間を確認する場面を見たことがあると思いますが、コンピュータで使われているパスワードによる本人確認の方法も基本的には同じです。この方式は何十年も前のメインフレームの時代から使われています。メインフレームは、国勢調査や軍事という機密情報を扱うことを目的に開発されましたので、使用環境については安全が考慮されていました。本体は、エアコンの効いた電算室に置かれており、誰にも触られないように厳重に管理されていました。一般の人は端末機にさえ触れることができませんでした。悪意を持った人が触れない仕組みになっていましたので、IDとパスワードという簡単な認証の方式でも十分にシステムを守ることが出来たのです。メインフレームで基幹システムが動いている限りシステムは安全だったのです。

しかし、パンドラの箱は、開けられてしまいました。1970年代にパソコンが発明され、より小さく、より速く、より高性能なパソコンが普及しました。パソコンは、サーバと言う名で基幹業務にも導入され始め、あっという間に、メインフレームの市場を奪いました。このパソコンの普及と同時に、高速でオープンなインターネットが普及し、サーバへのアクセスが誰からでも可能になりました。パソコンやインターネットの開発の目的は、情報を共有したいということでした。今までメインフレームで厳重に管理されていた金融や販売管理などの重要なデータが、安全性より利便性を優先するパソコンの世界に委ねられたのです。

コンピュータシステムに精通したハッカーの目からみると、機密情報の入った封筒が無防備な駅のホームに置かれたようなものです。今回の米国のカード会社のハッキング事件では、通帳と印鑑の役割をするパスワードがインターネットからアクセスできる管理の甘いサーバに格納されていて、ここが狙われたのです。使用環境が劇的に変化し、これほど危険な状態になったにも関わらず、未だにメインフレームと同じIDとパスワードによる認証方式が使われていることに今のシステムの問題点があります。

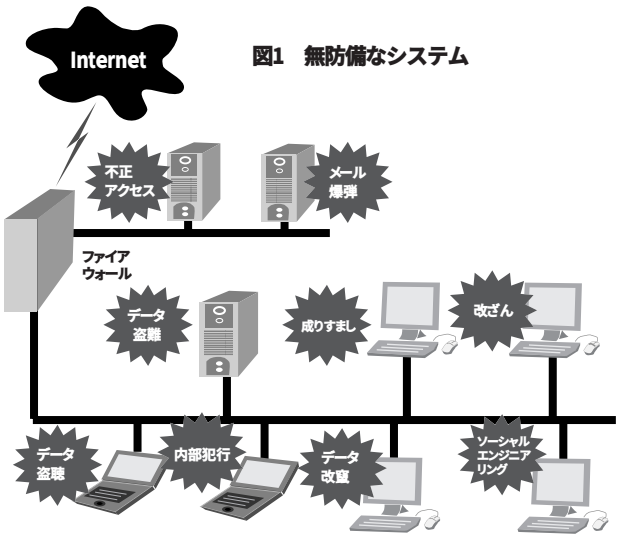


図1　無防備なシステム

ネットとデジタルの危険性

電話をグラハム・ベルが発明してから100年以上経ち

ますが、盗聴は別にして電話のシステムで大きな問題は起きていません。それは、電話というシステムが会話という情報の中身とダイヤルという制御の部分を明確に分けているからです。電話番号が盗まれたからと言って会話の中身まで盗まれるわけではありません。会話の内容は電話局に蓄積されていませんので、会話の内容が盗まれる危険性は極めて少ないのです。テレビも、基本的には同じで、テレビの画像は何処にも蓄積されません。だから盗もうと思っても簡単に盗めないのです。

一方、インターネットは電話線や光ケーブルの上をパケットいう名前のデジタル信号が流れています。パケットの中身は、TCP/IPという規格で仕様が公開されており、誰でも読むことができます。この信号の中にはアドレスなどの制御情報と会社の決算資料のような機密情報が、一緒に格納されています。パケットが目的地に到達するまで、様々なプロバイダーを経由して送られ、ルーターやサーバに機密情報が満載されたパケットをコピーしながら送っているのです。インターネットを使って情報を送るということは、世界中にコピーをばらまいていることと同じなのです。しかも、中身は0と1からなるデジタル信号ですから、原本とコピーの区別がつきません。盗んだIDとパスワードで成りすました犯罪者が、こっそり情報をコピーして持ちだしても、中身を改ざんしても全く証拠が残りません。

認証とは何か？

そこで、認証という難しい問題がクローズアップされてきます。認証とは「本人であることを公的な第三者が証明すること」と言われています。ITの世界では「情報の漏洩や改ざんを防ぐために、成りすましを防ぐ仕組み」のことです。実は、私たちの日常生活では、至るところでこの認証行為が行われています。例えば、会社のIDカードは社員を認証するためのものです。海外旅行をするときには、パスポートが重要な本人確認のための証明書になります。家に入るときの鍵も一種の認証のツールです。鍵も免許証もパスポートもなく、自分も含めた家族全員が記憶をなくしてしまったら、「私が私であること」をどのようにして証明するのでしょうか。この認証をコンピュータ上で実現することは非常に難しいのです。

どんな認証方式があるのか？

日常生活では当たり前のように行われている認証の手続きをシステムで実現するために様々な方式が提供されています。認証には、次の三つの方式が一般的に使われています。

図2　様々な認証方式

1. 記憶による認証

本人しか知り得ない情報に基づき認証を行うための方式で、通常パスワード認証と呼ばれています。パスワード認証には、固定パスワードと利用するたびにパスワードが毎回変わるワンタイムパスワードの2つがあります。 固定パスワードは非常にシンプルな確認方式で、堅牢性より利便性に重きを置いて開発されたものです。パスワードが漏れていたり、類推されたりしまう危険性があり、一度パスワードが知られてしまうと簡単に成りすましが出来てしまいます。

ワンタイムパスワードは、パスワードを一度しか使わせない方式で、認証のたびにパスワードが変わります。変わったパスワードは、電子メールや携帯電話で使用者に知らせます。携帯電話が盗まれたり、電子メールが盗聴されたりしたら効果はありませんが、現時点でかなり普及している認証方式です。

2. 所有物による認証

所有物による認証は、本人が持っているICカードやデバイスで認証を行うための方式です。実社会での社員証やクレジットカード、パスポートなどがこれに該当します。所有物による認証は、紛失の危険性があり、拾った人が使っても分らないという欠点があります。これを回避するために、クレジットカードでは、自筆のサインを付加したり、パスワードによる認証を組み合わせたりすることでセキュリティの強度を上げています。携帯電話を、ICカードの代わりに認証のデバイスに

利用しようと言う動きも出ています。携帯電話のGPS（地理情報システム）を使うことで自分以外の誰かが何処かで不正使用をすることを防ぐことができます。

3. 生体の特徴による認証

記憶や所有物による認証は、忘れたり、盗まれたり、落としたりと言うリスクがありました。生体認証は本人の身体的な特徴に基づいて認証を行う方式です。私たちは、自然に顔かたちや声、しぐさ、体格などで相手を確認しながら社会生活を送っています。五感を使って総合的に判断して個人を認識しています。この人間の目や耳の代わりをする認証方式が生体認証です。

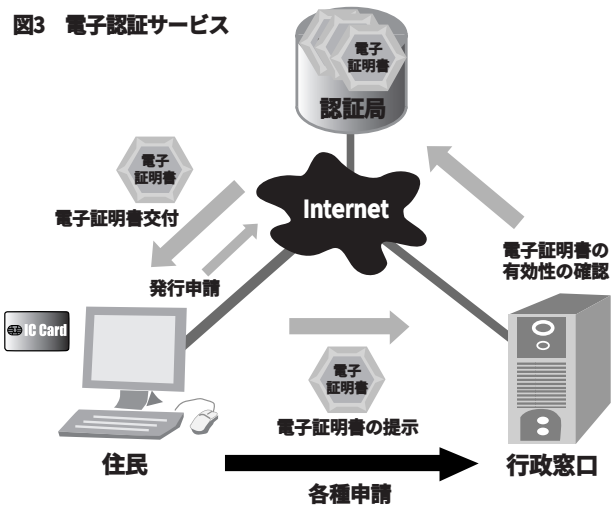
現在実用化されている生体認証には、指紋認証、顔認証、網膜認証、虹彩認証、掌形認証、静脈認証、筆跡認証、ボイス認証などがあります。最近は、銀行のカードの認証にも静脈認証という生体認証が使われはじめました。また、ニューヨークの9.11テロ以降、空港で指紋認証による本人確認も行われています。海外では街角で顔認証による犯罪者の摘発なども行われているようです。何種類かの生体認証を組み合わせた、より精度の高い複合生体認証が研究されています。今後、普及が期待される認証方式の一つです。

国が推進する認証基盤 電子認証サービス

不特定多数に対して本人であること証明するためには電子認証という技術が必要になります。電子認証は、本人であるということを認証局という公的な第三者機関が証明する技術です。何年か前に、住基ネットの是非が議論されましたが、住基ネットは、この電子認証を実現するために必要な仕組みです。住基ネットで使われる住基カードには、本人であること証明する電子証明書というものが格納できるようになっています。住基カードと電子証明書は、印鑑と印鑑登録証明書をネット上で実現したものです。住基カードは公的個人認証サービスで使われます。

このサービスは、インターネットを利用した電子申請などの行政手続を利用するときの本人確認に利用できます。市町村と都道府県が協力して全国一律に安い費用で提供しています。住基カードが一枚500円というのは格安の値段です。この認証基盤がしっかりしていないと申請者の成りすましや、情報の改ざんを許すことになり、行政のシステムの根本を揺るがすことになります。電子自治体の要のサービスとして国をあげて普及を推進しています。

図3　電子認証サービス



認証技術がもたらす夢の社会

最後に、認証技術を使った未来社会の寓話をご紹介いたします。犯罪防止というネガティブな使い方でなく、このような夢のある社会を実現するために認証技術を使っていきたいものです。

「朝、指紋認証センサーに指を当てて目覚ましのアラームを止めると目覚まし時計があなたの名前を呼んで朝の挨拶をします。家を出るときには携帯電話をドアのセンサーにかざすと全ての鍵が閉まり、テレビやエアコンは自動的に電源が切れます。

あなたが車に乗るときには指紋センサーに指を置くとドアが開きます。車の座席は自動的にあなたにあわせて調整され、優しい声であなたに呼びかけます。虹彩センサーをのぞき込むと、あなたのお気に入りのCDが自動的に演奏されます。

オフィスに着いたら入り口に設置された顔認証センサーが作動し、あなたが来たことを自動的に同僚や上司に伝えます。コンピュータを立ち上げるとログオン画面が表示され、「おはよう」と声をかけるとボイス認証で、すぐにコンピュータが使えるようになります。」