記憶がカギになる本人認証

記憶による入退室管理システム

私たちが生活するうえで，セキュリティが欠かせない時代となっている．家や会社，情報，キャッシュカードやクレジットカードの暗証番号などさまざまだ．

家に入るには鍵が必要なのはいうまでもない．金融機関で預金を下ろすにしてもカードを使って暗証番号という鍵が必要になる．しかも，他人がこの鍵を利用した事件も発生している．

最近は，セキュリティへの関心が高まりを見せ，指紋や声紋，静脈といった本人しか持っていない特徴を生かしたものや思い出の記憶を利用したものが出現している．そんな記憶を鍵とした使った本人認証システムとは一体どんなものなのだろうか．

本人認証とは

本人認証（Authentication）とは、あらかじめ本人であることを登録しておき、その証拠を示すことによって、本人であることを確認することをいう．では，現在使われている代表的な本人認証システム技術にはどんなものがあるのか．本人認証システムはパスワード，所持物認証，生体認証の3つに分けることができる．その特徴を見てみよう．

1つ目のパスワードは，生年月日や自宅の電話番号など簡単に見破られてしまうようなものは不向きである．しかし，なんだかよく分からないアルファベットと数字がランダムに並んでいるパスワードを覚えるのはむずかしい．すべての人が，いつでもそのパスワードを使いこなせることができるわけではない．

パソコンを例にとると，覚えられないパスワードを付箋紙などにメモをして画面に貼り付けるといったことは問題外である．

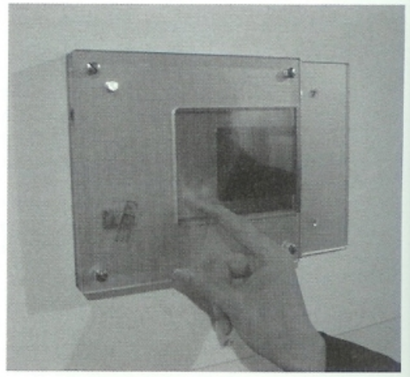
2つ目の所持物認証は，カード（クレジットカード，キャッシュカードなど）やパスポート，印鑑などで，所持物の置き忘れといった問題が必ずつきまとう．

3つ目は，人体の特徴点を計測する生体識別技術を本人認証に応用したものである．これは，最近よく見たり聞いたりすることが多いのではないかと思うが，指紋や静脈などである．この生体識別技術と聞くと，かなりハイテクなうえにセキュリティ度が高く，ちょっとかっこいいといったイメージがある．

この生体識別技術は非常に高い技術であることは間違いないのだが，それを使った本人認証技術が完璧であるとは言い切れない．人間の体は，病気やけが，環境の変化によって絶えず変化している．このことから，本人であるにもかかわらず“本人でない”と判断されてしまう問題がある．

そこで，本人拒否率をなくすためには，閾値（しきい）レベルを下げることになり，逆に他人を本人と誤認してしまう可能性が高くなってしまう．また，本人でないと判断された場合に，パスワードによる認証を追加したものもあるが，これはセキュリティが2重になったのではなく，ドアが2つになっただけのことなのである．

これらの問題を解決したのが，記憶による本人認証システムだ．



IDカードをかざして電源が入る

かざすと見える

この記憶による本人認証システムにはセキュアードディスプレイ，セキュアードディスプレイアクセス用IDカード（透過タイプ），記憶（長期記憶型認証ソフト）で構成されている．

まず，この聞きなれないセキュアードという言葉であるが，セキュアードとは“Secure（安全にする）”と“Display（表示体）”という発想に基づく造語であり，ディスプレイとIDカードにこの言葉が使われている．

ディスプレイにはIDカードの情報を読み取るリーダーが内蔵されていて，IDカードを近づけ本人であることを確認すると，ディスプレイの電源が入る．同時に，液晶画面にはその人の認証画面が映し出されるが，この時点では映し出された認証画面を見ることができない．IDカードをディスプレイに差し込むと認証画面を見ることができるのである．

セキュアードディスプレイは，可視化フィルムを介さないと表示された画面を見ることができない特殊な液晶ディスプレイである．電源が入った状態でも肉眼では画面表示を見えず，IDカードに組み込まれた可視化フィルムを通して見ることができる．

IDカードを液晶からはずすと表示されていた認証画面は見えなくなるため，認証画面を見るためにはIDカードを挿入する必要がある．このほかに画面を見る方法として，専用の可視化フィルムが組み込まれたメガネやカードをかざしたりすることで見ることができる．

パスワードは記憶

表示された認証画面には，従来の英数字の組み合わせによるパスワードではなく，利用者自身の記憶に基づいて登録しておいた画像を認証用パスシンボルとして使われ，16の画像が表示される．そして，表示された16の画像を順番通りに押さないと，本人であると認証されない．パスワードに記憶（思い出）による画像を使うため英数字のように記憶しておく必要がないうえ，忘れることもないのである．

画面に表示された画像は，電源を入れるたびにシャッフルされるので，盗み見されてもテンキーのように配列が決まっていないので心配ない．

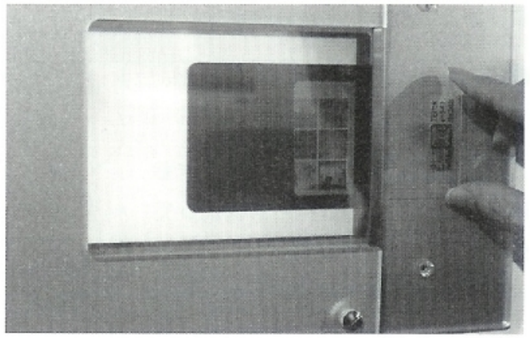
16すべての画像を押す必要はなく，利用者自身が登録した画像だけを押せばよい．別に1つの画像だけでもよいが，セキュリティを考えると最低3つは必要としている．

他人がカードを何らかの形で入手して認証画面を見ることができても，適当な入力や規定回数以上入力をすると他人と判定され，ディスプレイの電源が切れる仕組みだ．また，不審者にパスワードの入力を共用された場合でも，正規の入力を行なった後にあらかじめ登録しておいた“おとり画像”を押すことで不審がられることなく通報が可能なのだ

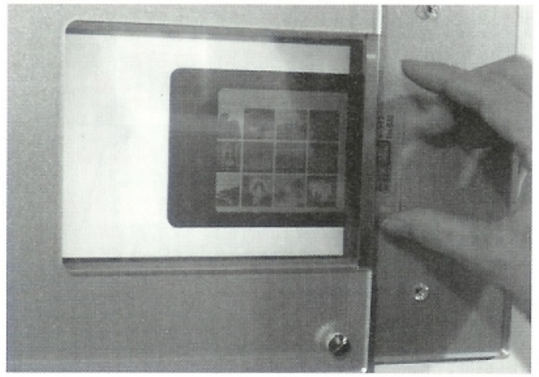
あなたのカギはどんな思い出ですか。

＜資料提供：SKRテクノロジー，www.skr-tech.co.jp＞

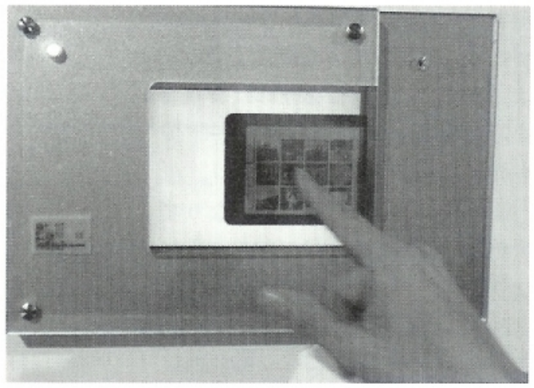
編集部　古川満之



IDカードがないところは見えない



IDカードを挿入すると画面が見える



タッチパネルによる入力