はじめに

日本を代表する企業からの大量顧客情報流出が連日のように新聞紙面を賑わしたことは記憶に新しく、これを機に情報漏洩防止・セキュリティ向上に対する関心がさらに高まってきている。こうした事件の多くは外部からの侵入というよりはむしろ内部犯行であると推測され、社員・従業員・関係者のモラルという目に見えないものに左右されるだけに一層厄介である。事件発生リスクを回避するためには社員等に情報を盗み出す気をおこさせないシステム、すなわち簡単には他人が成りすまし出来ないような本人認証システムを構築する必要性が出てくる。何となれば機密情報を盗み出そうとする者はすぐに自分に疑いがかかるようなアクセスの仕方はせず、アクセス権のある他人のＩＤを悪用するなどして犯行に及ぶケースが多いと考えられるので、確実な本人認証システムを経ないと機密情報へ到達出来ず、アクセス毎に履歴が管理されるシステムは犯罪抑止効果につながるからである。弊社は起業以来可視化フィルムを使用しないと画面表示を見ることの出来ないセキュアードディスプレイ（写真 1）を活用したセキュリティシステムの開発に従事しており、昨秋にはＩＣチップ内蔵専用アクセスカード（写真 2）・長期記憶型認証ソフト「ニーモニックガード」（写真 3）と組み合わせることにより、確実かつ安全な本人認証を行った上で入室が可能となる、従来にはない画期的な入退室管理システム『マルチセキュリティシステム』1 号機を完成させた。同システムに関しては本誌１２月号においてもご紹介する機会に恵まれたため、ご記憶の方もいらっしゃるかと思うが、次の項で最新の状況と絡めてご紹介することにする。

写真２　ＩＣチップ内蔵アクセスカード

写真３　長期記憶型認証ソフト「ニーモニックガード」

ニーモニックガードは、本人認証とは何かを原点に立ち返って考えた製品で、利用者本人が一生忘れない思い出や好きな事・物や人物などをパスシンボル（図絵写真パスワード）として用いることによって、本人を排除することなく、他人を有効に排除する認証用パスシンボル設定技術である。例えば、『昔飼っていたペット』『子供の頃好きだった事』を画像として登録・選択することによって自分だけのパスシンボル設定が可能になるため、従来の英数字のパスワード採用の場合に起こりうる、忘れない為には誕生日やイニシャルを組み合わせるという他人でも容易に類推可能なパスワードを選択せざるを得ない、あるいは忘れてしまわないようにメモ書きを残さざるを得ないというセキュリティ不在の状況から解放される。なお、選択するパスシンボルの個数は任意で、かつ選択順序（パスシンボルを押す順序）を設定することも可能である。起動するたびにシンボルの表示位置を変えるという選択肢を選べばさらにセキュリティが向上する。

マルチセキュリティシステムとは

ＩＣチップ内蔵専用アクセスカード（写真 2）がセキュアードディスプレイ（写真 1）に組み込まれたリーダー部に接近しリーダーと交信した結果、登録済ユーザと認められるとディスプレイの電源が点灯するとともにユーザ毎に個別に設定された認証画面が起動する。利用者はＩＤカードに組み込まれた可視化フィルムを使用して周囲からの覗き込みを懸念することなくタッチパネル上で認証を行い、入室する仕組みである。なお、認証に使用するのは利用者本人が忘れることのない昔の記憶の中にある画像、あるいは将来の願望を組み合わせた画像によるパスシンボル「ニーモニックガード」（写真 3）であり、従来の英数字の組み合わせによるパスワード利用の場合におこりがちな他人の類推を防ぐ事が可能である。また、正規ユーザだったら選択するはずのないパスシンボルばかりを押す、パスシンボル入力個数が登録と異なるといった場合には、他人と判定し管理部門等へ通報する、悪意の第三者からパスシンボル入力を強要された場合にはあらかじめ設定したＳＯＳシンボルを正規パスシンボルのあとに入力することによって異常事態を管理部門等へ通報するなどの対応を取ることも可能である。認証画面起動のたびに表示位置を変えるという選択肢を適用すれば、指の押し跡からの類推も防止できる。認証フローチャートとシステム構成は下記の通りである。(図 1　認証フローチャート　図 2　システム構成）

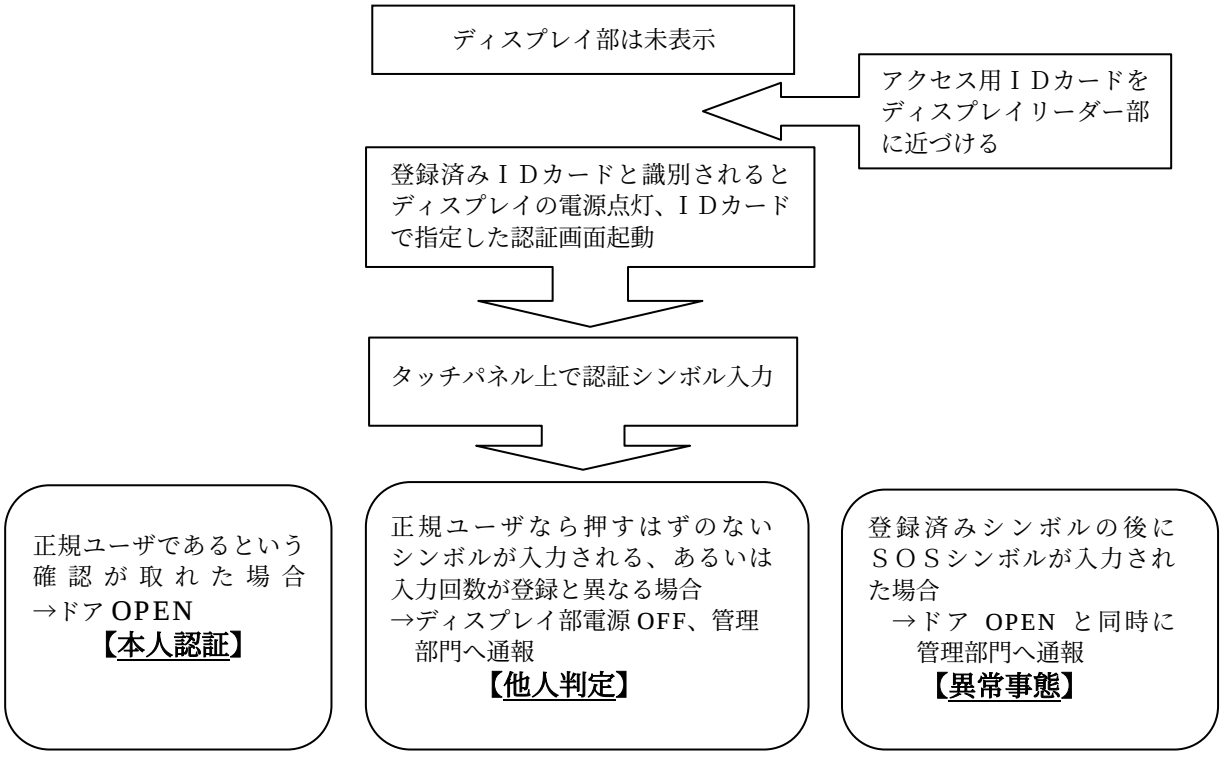

図 1　認証フローチャート

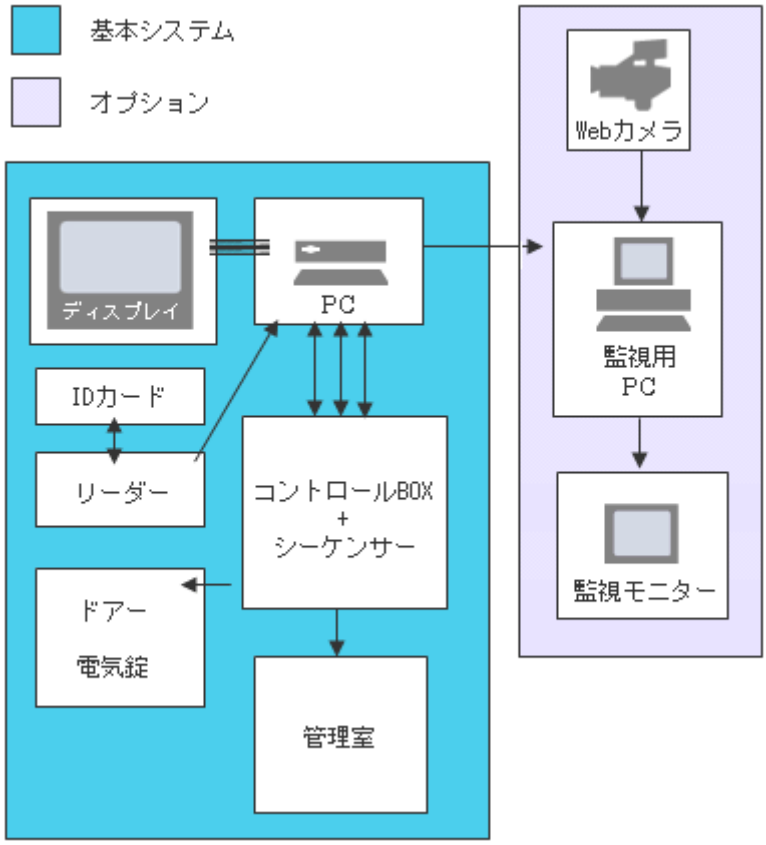

図２　システム構成

写真１の可視化フィルムを目の前にかざして画面表示を見るセキュアードディスプレイは、ディスプレイ自体に改造を加えているためユーザ手持ちのディスプレイに外付けすることはできない、一方の手で可視化フィルムをかざし、他方でタッチパネルを押して認証シンボルを入力するため両手がふさがってしまうなどの短所もあり、これに代わるタイプのディスプレイ研究開発を同時並行で進めていたが、この度偏光板の光学特性を利用し、通常は画面表示が真っ黒であるが、可視化フィルムをディスプレイユニット内に挿入すると透過する新しいタイプのセキュアードディスプレイ（写真４）が完成し、ユーザのニーズにあわせてお選び頂けるようにした。（図 3 製品ラインナップ）なお、可視化フィルムにＩＣチップを埋め込むことにより、ディスプレイの電源 ON が可能であることは言うまでもない。

写真４ セキュアードディスプレイ　（BLACK タイプ）
左　可視化フィルムを半分まで挿入した状態
中　可視化フィルムを挿入し、全画面表示にした状態
右　ＩＣチップ内蔵可視化フィルム

型式	ディスプレイ種類	コンタクト方法
SDW-100	PPT 液晶ディスプレイ使用 	非接触 IC カード（可視化フィルム内蔵）
SDW-110		非接触 IC タグ（可視化フィルム複合）
SDB-100	SKR セキュアードディスプレイ使用 	非接触 IC カード（可視化フィルム内蔵）
SDB-110		非接触 IC タグ

図 3　製品ラインナップ

確実な本人認証システムへの転用

これまで入退室管理システムを中心に書き進めてきたが、ＩＣチップ内蔵専用アクセスカードで本人識別を行った後（ここまでなら他人でも容易に成りすましが可能である）、記憶によるパスシンボル入力で本人確認を行うマルチセキュリティシステムが本人認証手段として最適であることはおわかり頂けたことと思う。登録者本人はストレスを感じることなく予め設定した記憶・願望に基づく認証パスシンボルを選択可能であるが、他人がなりすましを行おうとしても、正解パスシンボルの組み合わせにたどり着く可能性は排除され、さらに、本人が選択していないシンボルばかりを選んだ場合や、選択シンボル数が登録したものと異なる場合には他人判定され管理部門へ通報される機能も備わっているとあれば、不正使用を断念せざるを得ないであろう。

最近は一部の銀行で不正引き出しを防止する手段として指紋・静脈パターンといった生体認証を利用した本人認証システムを導入する動きが出てきている。しかしながら、生体認証には次のような問題点を指摘する声もあり、現実的利用に即しているかどうかは疑問である。本人拒否が起きたときの代替認証方法の脆弱性（代替認証方法として採用されることが多いと考えられるのは英数字パスワードであるが、利用頻度が高くないと想定される代替認証用であるため、「絶対に忘れない」＝「他人にも類推し易い」ものを選択しがちである。そのような状況では、悪意を持つ者は生体認証を突破する代わりに、パスワード破りを狙う可能性が高い。）生体情報といえどもコピーされる可能性は十分にあり、かつ万一コピーされた際には生体情報であるが故に防御策がないこと委任行為が困難であること

これに対してマルチセキュリティシステムは『本人拒否』『他人による成りすまし』を排除し、確実に本人確認を行う手段として金融期間における認証手段としてもご利用可能である。現在簡易型デモ機で検証作業を行っているところである。（写真 5）


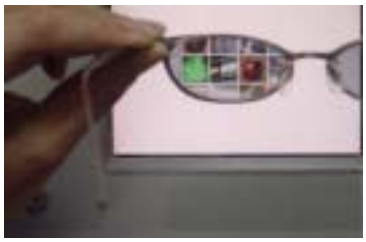


写真５　金融機関向け認証システム
左　全体図（アクセス用ＩＤカードをリーダーに近づけて、認証画面を起動させる）
中　肉眼では認証画面表示は見えないので周囲からの覗き込みを懸念することなく、利用者　だけが専用メガネ、もしくは専用カードを使用して画面表示を確認しながら認証を行う。
右　登録済みパスシンボルが正しく押されたら、【本人認証】ランプが点灯、登録済みパスシンボルと異なる場合には【他人判定】ランプ点灯、パスシンボル入力を強要されていることを知らせるＳＯＳシンボルが押された場合には【異常事態】ランプ点灯により、不正引き出し防止が可能となる。

今後の展開

入退室管理システム、金融機関向け本人認証システムとも製品化の目処が付きつつあり、次に取り組むべき課題としてセキュアードディスプレイ・ＲＦＩＤ技術・ニーモニックガードを組み合わせたセキュリティ私書箱の開発を予定している。宅配ロッカーをはじめ、自宅以外で物の受け渡しをする、銀行口座の開設などの書類手続きもコンビニ付設のロッカーで行うなど、利用者の利便性が高まる製品が普及しつつあるが、その利便性が盗難などの犯罪を行おうとする者にとっても好都合となりかねない危険性をはらんでいる。確実に本人確認の出来るシステムを応用展開する可能性はつきず、まだまだ研究をする甲斐があるというものである。