セキュアードディスプレイと IC カードを用いた入退室管理システム
（マルチセキュリティシステム）のご紹介

SKR テクノロジー

偽造カードを使った預金引き出し被害の実態が明らかになったのを受け、対策を検討していた金融機関では、磁気カードから偽造されにくいＩＣカードへの変更、手のひら・指先の静脈パターン情報を予めＩＣカード内に格納しておき、利用者の手のひら・指先の静脈パターンと照合して本人かどうかを確認する認証手段の採用が広がりつつあります。入退室管理の分野のおいても、バイオメトリクス認証、IC カード認証が主流になり、携帯電話の普及・進化を反映して、ＩＣチップの格納された携帯を利用した入退室という手段も出はじめました。

弊社の推奨する入退室管理システムは、ＩＣカードリーダーにカードをかざすだけの認証と誤解されやすいのですが、ＩＣカードは該当する利用者の情報を呼び出すために使用されているに過ぎず、ＩＣカードによって呼び出された認証画面の中から利用者が予め登録した画像の組み合わせを正確に押せるかどうかで本人か否かを見極めるという、高精度のシステムで、どの画像をどのように選んで押しているのかを周囲から覗き見させない特殊液晶ディスプレイを使用しているため、盗難カード・複製カードでのアクセスは不可能になり、安全かつ確実に本人確認を行えるシステムです。

写真を参考に具体的なシステムについて解説致します。
セキュアードディスプレイと IC カードを用いた入退室管理システム（マルチセキュリティシステム）の構成要素は、①可視化フィルム無しでは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、②ＩＣチップ内蔵専用アクセスカード、③視覚長期記憶型認証ソフト（ニーモニックガード）です。
セキュアードディスプレイとは、現在では高精細・高視野角が主流になっている液晶ディスプレイの視野角を本来の用途とは逆に狭め、対になるフィルムを使用しないと画面表示が見えない仕組みとした特殊液晶です。この液晶を利用することにより、周囲からの覗き見が防止され、パスワード等を入力している際の情報流出を防ぎます。フィルムを目の前にかざした利用者だけがディスプレイ上に表示された内容を見る事が出来る、よりセキュリティ性の高い方法と、フィルムをディスプレイ部に設置されたスリットに挿入することで表示内容を見る事の出来る方法の２種類から、ご利用用途にあった方法をお選び頂けます。
ＩＣカードは、I-CODE 対応のチップを使用しており、上記のディスプレイタイプに応じた対フィルムが埋め込まれています。カード内の各ＩＣチップに、リーダーに反応するための番号、カード固有の画像情報を呼び出すための識別番号がアスキーコード（英数字の組み合わせ）を利用して登録しておきます。利用時、リーダーにカードをかざすと、カード

番号に応じた登録情報が呼び出され、ディスプレイ上にはカードごとに異なる認証画面が表示される仕組みです。
視覚長期記憶型認証ソフト（ニーモニックガード SKR バーション）は、本人認証とは何かを原点に立ち返って考えた製品です。従来の英数字を組み合わせたパスワードの場合、忘れないように誕生日やイニシャル・電話番号・地番等を組み合わせた、他人からも容易に類推可能なものにせざるを得なかったり、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かったりするなど、セキュリティという観点からするときわめて低いレベルの安全性しか実現出来ないという欠点があります。セキュリティ性が高く、しかも利用者本人が苦痛を覚えずに利用出来るものは何かと考えた結果生まれたのがこの視覚長期記憶型認証ソフトで、『昔飼っていた猫・犬』『子供の頃の初恋の先生』『新婚旅行先の思い出』など、個々人の記憶の中に眠っている、思い出や好きな事・物・人物の画像をパスシンボル（図絵写真パスワード）として組み合わせるパスシンボル設定技術です。言葉で説明するとわかりにくいので、画像を使ってご説明します。

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す。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します。
認証時の判定の方法は、①本人認証、②他人判定、③異常事態の 3 種類です。本人認証とは言うまでもなく、カード保持者が予め登録したとおりにパスシンボルを選択した場合、他人判定は、予め登録したのと異なる選択を繰り返した場合の判定です。本人といえども、数ある画像の中から登録画像を選ぶ際にうっかりすぐ隣にある画像を押してしまう、あるいは一度押したつもりが、二回押したとカウントされてしまった、その逆に押したつもりがカウントされていない、ということもあり得うるため、本人がやりそうな間違いは許容して何度でもやり直しが可能ですが、本人ならやりそうもない間違い、つまり、登録と異なる画像ばかりを選ぶ、選択の枚数が本人の指定した枚数と異なる、を犯した場合にはすぐに不正アクセスと判断し他人判定を下すわけです。さらに、ドアが閉まらないうちに後からついて入ってしまうような共連れ、不正侵入者にパスシンボル入力を強要されるといったケースに威力を発揮するのが異常事態判定で、自分の本意では無くパスシンボルを入力している、あるいは周囲に異常事態が発生しているということを通報するための『異常事態シンボル』を設定しておき、正しいパスシンボルの後に異常事態シンボルを押すことによって、警備室・管理部門等にアクセス時の状態について通報するシステムです。
ログ履歴ソフトも備わっているので、入退室時の判定状況を管理するとともに、出退勤管理にも併用可能です

ターゲット顧客
個人情報・機密データを管理するデータセンター
空港・原子力関連施設など防衛上または治安上高度なセキュリティを要求される施設
金融機関、行政機関、研究所、ハイセキュリティーマンション等に最適です
都内で情報漏洩を嫌うソフトメーカー様で運用を開始いたしました。
現在はコントローラ、RFID リーダを組み込んで無電圧 a 接点出力付きの情報端末の
販売も始めました。設置工事をせずに配線さえすればすぐにでも使用が可能です。
応用製品の金融機関・自治体向け本人認証システム、ゲートシステムの引き合いを
増えてきております。ネット対応での複数施設での検討を始まりました