

アイリス認証セキュリティシステム

羽鹿 健 江原 和明
中村 敏男

近年、インターネットの普及とともに、ネットワークの利用の範囲が急速に拡大し、流通する情報の価値や情報量も年々増加している。それに伴い、さまざまな電子情報にかかわる不正や犯罪の増加が社会問題になっており、またその影響も大きくなる傾向にある。このような不正行為は、コンピュータ施設への物理的な侵入や機器の不正使用、あるいはネットワークからの不正アクセスによる侵入によって行われている。

これらの不正や犯罪を防止する対策として、第一に施設への不正侵入を防止するための物理セキュリティの充実、第二にネットワークへの不正侵入や情報への不正アクセスを防止するための情報セキュリティの充実が挙げられる。いずれの対策においても、利用者の本人確認を確実に行うことが有効な手段の一つであり、利用者の身体的特長を用いるバイオメトリクス認証が、究極の本人確認手段として注目を集めている。その中でも、人の目の虹彩（アイリス）の模様が個人によって異なることを利用するアイリス認証技術は、高精度での認証が可能なることから、今後の普及が期待されている。

当社は、このアイリス認証技術にいち早く着目し、まず、業界に先駆けて物理セキュリティ向け「アイリスパス[®]*1)-Sゲート管理システム」を商品化した。そして、今回、情報セキュリティ向け「アイリス認証セキュリティシステム」（以下、本システムと略す）を商品化した。

本稿では、本システムの概要およびその適用例について述べる。

システム概要

本システムは、既存のコンピュータシステムにインストールして、オペレーティングシステムやネットワークシステムへのログイン、あるいは各種業務の承認機能を、アイリス認証で実行可能にするものである。従来のパスワードや、カード等による本人確認に比較して、確実な本人認証が可能なので、システムのセキュリティを高めることができる。また、パスワードを忘れたり、カードを紛失するといった従来システムの問題も解決でき運用

面の大幅な効率化が期待できる。

本システムでは、パーソナルコンピュータ（以下、PCと略す）単体で動作可能なスタンドアロン・システムと、ネットワークシステムで動作可能なクライアント／サーバ・システムの2種類の形態で使用できる。以下に、これらのシステムを構築するための、アイリス撮影用カメラ、アイリス認証制御ソフトウェア、およびアイリス認証サーバ・ソフトウェアについて説明する。

(1) アイリス撮影用カメラ「アイリスパス[®]-h」

アイリスパス[®]-hは、PCのUSBインタフェースに接続して使用するアイリス撮影専用カメラユニットである。外観を図1に、諸元を表1に示す。

本カメラで撮影したアイリスの画像をPCに取り込んで後述のアイリス認証制御ソフトウェアで処理することにより、アイリス認証機能を実現する。

本カメラの開発にあたっては、利用者が自身のアイリスを撮影するための使い易さを最優先課題とした。

①撮影距離

最初に、アイリスの画像を撮影するための撮影距離を決定した。目から遠く離して撮影する方法は、距離の調整が難しくなり、また、手ぶれも起こりやすくなるので、目に近づけて撮影する方法にして、誰にでも簡単に距離合わせできるようにした。また、この距離は眼鏡着用者でも、眼鏡レンズに当たることなく撮影できることも考慮



図1 アイリスパス[®]-hの外観

*1) アイリスパス[®]は、沖電気工業(株)の登録商標。

表1 アイリスパス[®]-hの諸元

項 目		仕 様
認識性能	認識率	99.9%以上
	誤認識率	0.000083%以下
認識時間		1秒以下 ^(*)
インタフェース		USB
消費電流		300mA以下
外形寸法		59(W)×121(H)×52(D)mm
重量		160g (ケーブル含む)

(*) Pentium[®]*2 III600MHz使用時。
システム側でのロス時間を除く。

して決定した。

②サイズ、形状

手に持って使用するので、手になじむサイズ、形状とした。また、右利きと左利きのどちらの人でも自然に持ったときに、親指で押せる位置に認証開始スイッチを配置して、操作を容易にするとともに親指で覗き窓や照明を隠すことのないようにした。

③操作ガイダンス

操作ガイダンスには、覗き窓の奥に見えるLEDの表示と、内蔵ブザーの音による方法を採用した。

LEDの表示は四角形表示とし、4辺がすべて欠けることなく見える位置がカメラ正面になるようにして、利用者の目の位置をカメラ画角内に誘導する方式を採った。また、LEDの点灯のしかた（点滅、点灯等の組み合わせ）で、距離合わせの確認ができるようにした。

ブザー音は距離合わせの操作を補助するために用意したが、利用者の好みや使用環境によってオフにすることもできる。

④眼鏡レンズ上照明反射の対策

アイリスの撮影には照明を使用するため、眼鏡着用者の場合、照明が眼鏡レンズ上で反射して白く光り、アイリス模様を隠してしまうという問題があった。この問題を解決するために、覗き窓の周囲に複数の照明を配置し、これらの点灯を切り替えて撮影することで、反射による影響のないアイリス画像を撮影できるようにした。

アイリス認証操作は、カメラを手に持って、認証開始スイッチを押下し、覗き窓の中の表示LEDを見ながら位置と距離合わせを行う。実験の結果、経験のない人でも3回程度の学習で操作できた。

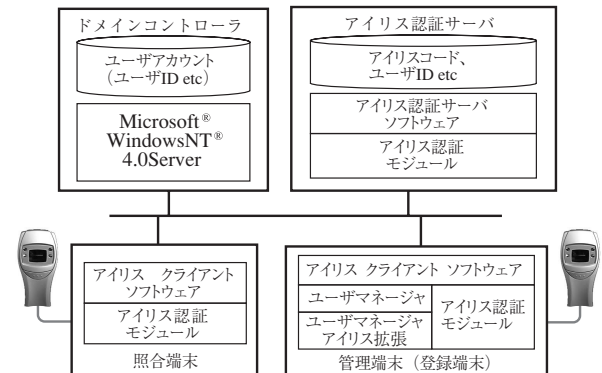


図2 アイリス認証ソフトウェアシステム構成図
(クライアント/サーバ・システムの場合)

(2) アイリス認証制御ソフトウェア

アイリス認証制御ソフトウェアは、PCやネットワークシステムへのログインや各種業務における承認機能を実現する。

本ソフトウェアを用いてPCにログインする場合、パスワードを用いてログインする場合のパスワード入力画面がアイリス撮影画面に置き換わる。アイリス撮影画面が表示されているときに、前述したアイリスパス[®]-hを用いてアイリスを撮影することにより、アイリス認証によるログインを行うことができる。

本システムの形態には、スタンドアロン・システムとクライアント/サーバ・システムの2種類が存在する。

スタンドアロン・システムの主な目的は、デスクトップやノートPCのスタンドアロン環境でのローカルログインである。これに対してクライアント/サーバ・システムは、ネットワーク上のドメインやWebシステムに対するログインを主な目的としている。

クライアント/サーバ・システムのシステム構成は図2に示すとおりアイリス認証サーバ・管理端末、および照合端末の3つから構成される。

アイリス認証サーバでは、ユーザIDとともにアイリスを登録する際に生成されるアイリスコードなどの情報がデータベースに格納される。また、本サーバのアイリス認証モジュールは、クライアントからの照合依頼を受け付け、アイリス照合を高速に実行する。アイリス認証サーバの詳細については、(3) で述べる。

管理端末は、アイリス登録を行うための端末であり、登録権限を持った利用者が使用する。ユーザアカウント作成用ツールであるユーザマネージャにアイリス登録機能を組み込むことにより、登録管理者がユーザアカウントを作成する際に、操作の流れの中で違和感なくアイリス登録に移行できるように工夫した。アイリス登録操作に

*2) Pentiumは、米国 Intel Corporationの登録商標。 *3) Microsoft、Windows NT、SQL Server は米国Microsoft Corporationの米国およびその他の国における商標または、登録商標。

移行したのちは、管理者にとってわかりやすいように対話型で直感的な画面表示を実現し、管理者の負担を軽減させた。

照合端末では、パスワードログインの代わりにアイリス照合を行うことでシステムのセキュリティが向上する。操作は画面上の撮影ボタンを押すか、アイリスパス[®]-hカメラの撮影開始スイッチを押すだけであり、誰でも簡単にアイリス照合することができる。

また、アイリス認証サーバに格納されるアイリスコードなどのデータや、管理端末・照合端末とアイリス認証サーバ間の通信データは暗号化されるため、情報漏洩に対するセキュリティ対策も十分である。

さらに、端末側から照合依頼を行うためのAPI (Application Programming Interface) を提供しており、各種のアプリケーションから本システムを利用することも可能である。

(3) アイリス認証サーバ・ソフトウェア

アイリス認証サーバ・ソフトウェアは、管理端末からのアイリス登録要求を受け付け、データベースにアイリスコードを格納したり、照合端末からのアイリス照合要求を受け付け、照合処理、結果の通知を行う。

アイリス認証サーバ・ソフトウェアの構成を図3に示す。

本システムでは数万件規模のアイリスコード登録が可能で、照合要求はすべて本サーバ内で処理される。登録されているアイリスコードを端末側に送信することはないのでセキュリティ面での信頼が高い。

また、本サーバには端末側からの登録操作、照合操作、権限変更などの各種履歴情報が格納されるため、履歴が格納されたデータベースを管理者が閲覧することにより過去の事象を追跡することができる。

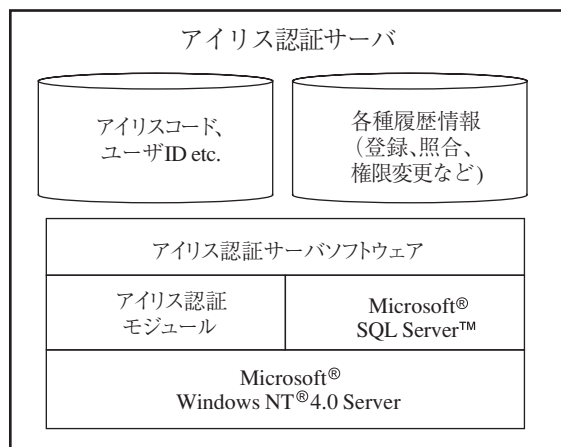


図3 アイリス認証サーバのウェアシステム構成図

さらに、本サーバはアイリス以外のバイオメトリクス、たとえば指紋や音声などにも対応したマルチバイオメトリクス方式を採用しており、アイリス単独のバイオメトリクスのみならず視覚障害者などにも対応できるように複数のバイオメトリクスが混在したシステム構築が機構上可能となっている。

適用例

本システムの適用例を以下に示す。

(1) イン트라ネットセキュリティシステム

イントラネットに本システムを適用する例について説明する。イントラネットにアイリスセキュリティを組み込む場合、社内システムの一部としてWebサーバとともにアイリス認証サーバを配置する。イントラネットセキュリティシステムの構成例を図4に示す。

この例においては、イントラネット内の利用者が、社内向けに提供しているWebサイトへのアクセスをパスワードの代わりにアイリス照合を用いて行う。

各Webサイトごとにアクセス権限を設定し、権限を持つ人を確実に認証することで、セキュリティを高くし、不正や情報流出などを防止することが可能である。

また、利用者ごとに、アイリス照合とパスワード照合の混在が可能であるため、本システムの導入にあたり、徐々に適用範囲を拡大する方法も選択できる。また、マルチバイオメトリクスに対応しているため、他のバイオメトリクスとの混在も可能である。

さらに、端末側からの照合依頼を行うためのAPIを用いて、アプリケーションにアイリス認証機能を組み込むこ

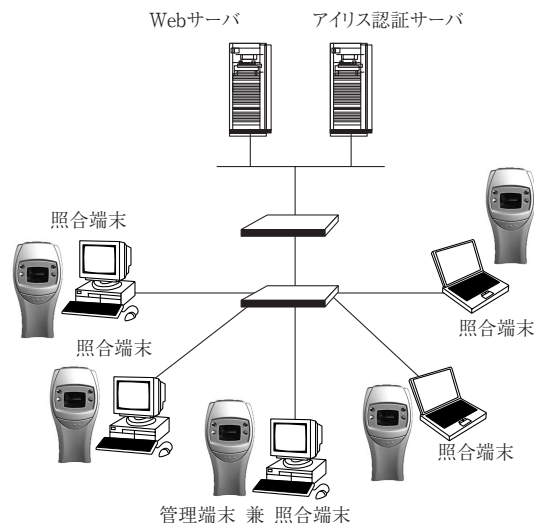


図4 イン트라ネットセキュリティシステム構成例

とにより、社内システムの中でも高いセキュリティを要求する部分や、本人確認の要求度が高い部分への適用も容易である。

(2) 電子決済システム

インターネットを利用した電子商取引では、取引相手を確認する手段、あるいはこちら側の利用者の正当性を相手に伝える手段が課題である。

通常、これらの確認手段としては、パスワード、あるいは公開鍵方式を用いた暗号化を用いるのが一般的である。しかし、パスワードは盗まれたり、推測し易いという問題があり、暗号化は鍵を端末内に記憶して管理することが多いので、実質は人の認証ではなく端末の認証になっているという問題がある。そのため、安心して電子商取引を行うためには、より確実な本人認証が必要である。

このような電子商取引に、本システムを適用することにより、確実な本人認証ができ、なりすましによる不正を防止することができる。

図5にアイリス電子決済システムの構成例を示す。

アイリス認証機能はアイリス認証局、あるいは決済システムの中に置かれたアイリス認証サーバで行い、サービス提供者や銀行システムと連携して、安全な決済処理を行うことが可能になる。利用者は、取引の開始、あるいは決済承認の際にアイリス認証を行うことにより本人であることを証明する。決済サービスを提供する側では、本人認証ができた段階でサービスの提供を行う。

この例で示すようなシステムでは、アイリス認証局を、異なるサービス提供者や、複数の異なるサービスで共通に利用することができるため、利用者だけでなくサービス提供者にとってもメリットのある方法である。

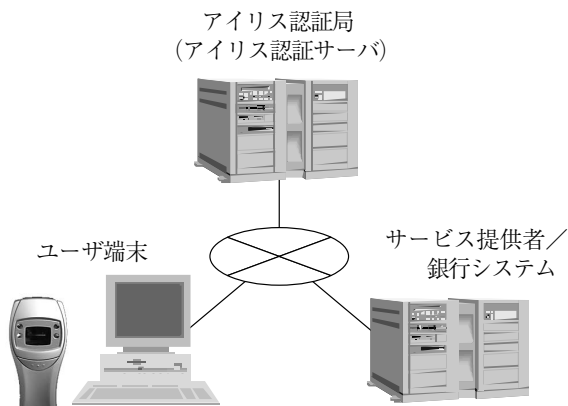


図5 アイリス電子決済システム構成例

まとめ（今後）

以上、今回開発したアイリス認証セキュリティシステムの概要とその適用例を紹介した。

今回の商品化により、物理セキュリティ市場向けにはアイリスゲート管理システム、情報セキュリティ市場向けにはアイリス認証セキュリティシステムという商品の品揃えができた。市場においてもバイオメトリクスの導入気運が高まっており、徐々にではあるが実績も上がってきた。

今回のシステムは、アイリスゲート管理システムに比較して、大幅な低価格化、小型化を実現するとともに、誰もが簡単に使用できる操作性を実現した。また、PCに接続するアイリス撮影用のカメラとアイリス認証制御ソフトウェアの構成にすることにより、柔軟なシステム構築を可能としている。そのため、今回紹介した適用例だけでなく個人認証を利用したさまざまなアプリケーションへの適用が考えられる。

今後は、官公庁、自治体、金融機関や一般企業への本システムの展開を積極的に図っていく。さらに、現状の製品に満足することなく、より使い易く、低価格で、小型の商品開発も推進していく予定である。 ◆◆

参考文献

- 1) 松下満次, 他: アイリス個人認識システム, 沖電気研究開発第175号, Vol.64, No.3, pp.107-110, 1997年
- 2) 塚田光芳: アイリス認識システムの金融機関への適用, 日本実務出版(株), 安全と管理, pp.26-29, 5月号, 1999年
- 3) 羽鹿健, 他: アイリス認識システムの金融機関への適用, 沖電気研究開発第181号, Vol.66, No.2, pp.47-50, 10月号, 1999年
- 4) 藤高敦子, 他: アイリス認証を用いたインターネットペイメントシステム, 沖電気研究開発第182号, Vol.67, No.1, pp.41-44, 2000年

筆者紹介

羽鹿健: Takeshi Hajika.システムソリューションカンパニー システム機器事業部 マーケティング部
 江原和明: Kazuaki Ebara.システムソリューションカンパニー システム機器事業部 C17プロジェクト
 中村敏男: Toshio Nakamura.システムソリューションカンパニー システム機器事業部 セルフチャネルソリューション 第三部