

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

Card-less Internet Payment System with IRIS

藤 高 敦 子
Atsuko Fujitaka

福 田 厚 司
Atsushi Fukuda

安 倍 紀 美
Noriyoshi Anbai

要 旨

人間の虹彩（アイリス）認識技術を個人認証に用い、カードレスでも利用可能なインターネットペイメントシステムを開発した。

1. ま え が き

インターネットの普及がネットワーク社会におけるデジタル経済を個々人にとって身近なものにしていた。ネットワークにおける取引の特徴は、行為者の特定が困難な匿名性、物理的痕跡がない無痕跡性、24時間どこでも利用可能な超時空間性、そして超高速性である。しかし、非常に便利なこのネットワーク社会の進展に「待った」をかけるものがある。それは、なりすまし、偽造、変造、盗聴、侵入といった新たな犯罪の脅威である。米国におけるVISAカードの全トランザクションのうち、インターネット取引はその2%に相当するまでに至った。そのうちの50%、すなわち全トランザクションの1%は不正が明らかになっている。

また、ノルウェーではインターネットでの決済を禁止する条例が成立している。しかし、いくら法律で規制しても市場の要求はとどまることがない。安全性の確保が可能となって初めて消費者は安心してネットワーク社会を享受できるといえよう。

2. セキュリティ提案

そこで公開鍵や暗号の電子署名を用いた認証技術が注視されるのである、

技術発展と共に忘れてはならないのが認証局の設置である。公開鍵自体の正しさを証明するための中立的な信頼のにおける第三者機関の存在である。認証局設置に向けて各国とも法整備を進めつつあるが、認証の方法に公開鍵や電子署名のみならず、新たな「ツール」を用いようという試みが見られる。一つはICカードを使用するというものである。ドイツでは、ICカードを本人確認のためのツールとして使い、認証局データと整合を取るという方式がマルチメディア法で制定された。

ICカードは、2002年には世界中で本人確認のインフラになるといわれており、各国ともこの方向に向かうと思われる。また一方ではこのICカードと併用してバイオメトリクス技術で本人確認を行おうとする動きも活発である。日本でも郵政省を初めとした省庁で本格的に検討することが表明されている。



藤高敦子
システムソリューション
ビジネスグループ
カスタマコンタクトシ
ステム事業部
ソリューション企画部
担当課長



福田厚司
システムソリューション
ビジネスグループ
カスタマコンタクトシ
ステム事業部
ソリューション企画部
SE開発第四チーム係長



安倍紀美
システムソリューション
ビジネスグループ
カスタマコンタクトシ
ステム事業部
セルフチャネルソリュー
ション部
SE第五チームリーダー

当社は、バイオメトリクスの技術の中でも最も精度の高いとされるアイリス認証の技術およびアプリケーション開発に取り組んできた。図1に、他のバイオメトリクス技術との比較を示す。当社は、この分野においては世界のリーディング会社であると自負している。アイリス認識には様々なアプリケーションが考えられるが、ネットワークにおける本人認証に関してはICカー

*通過エラー：本人を確定できない確率
*阻止エラー：他人を誤って通過させる確率

	押し付け がましさ	経年変化	偽造可能性	通過 エラー	阻止 エラー
サイン	中	中	高	高	高
指紋	高	小	中	高	中
掌紋	高	高	中	中	中
顔貌	小	高	中	極高	極高
声紋	高	高	極高	極高	高
網膜	極高	小	極小	小	極小
アイリス	極小	極小	極小	小	極小

*カメラ部を見ただけです。 *2歳以降変化しません。 *目の生体確率を行います。 *通過エラー率は0.1%以下です。 *阻止エラー率は0.001%以下。

図1 バイオメトリクス技術の比較
Fig. 1 Comparison of biometrics technologies

ドのチップ内にそのデータを組み込み、ATM (Automated Teller Machine) 等における照合に使用するというのも有望な一例であろう。また、災害が発生しカードも通帳も紛失した場合でもアイリス登録で間違いなく預金が保証されるというようなアプリケーションも、リスクマネジメントとして金融機関側にも消費者にも有益な事と言える。

そのICカードもマルチアプリケーション化されてきており、ICカードの一つの付加価値としてチップ内にマネーが存在する、電子財布も併せて注目されている。ネットワーク社会においてセキュリティが鍵であると先述したが、もう一つ重要なのはネットワークコストの低減である。インターネットの普及はデジタル情報を売しようとする市場の要求に拍車をかけている。少額決済、価格を自由に設定できるというインターネットペイメントのアプローチとしてはプリペイド型が最も適する。認証に時間がかからず、Valueが移動するだけなので手数料コストが低く抑えられる。この基本となる技術が「End-to-End セキュリティ」、すなわちチップ間でValueを移動させるというものである。当社はChip-to-Chip Value Transferのグローバル特許を有している。

ネットワーク社会におけるキーワードは、セキュ

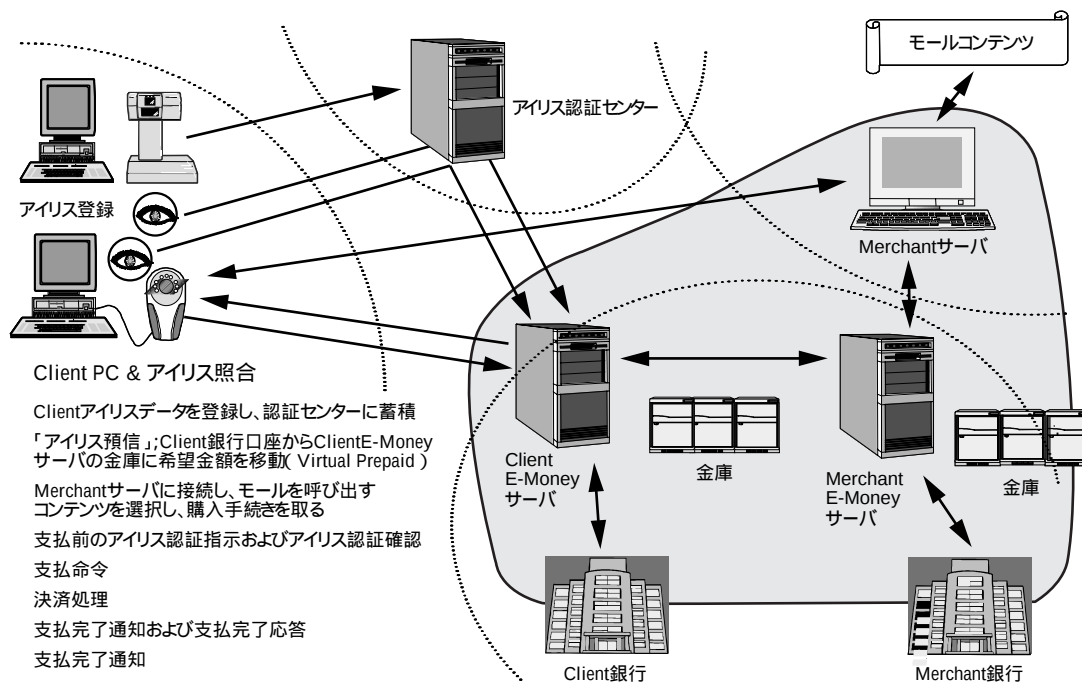


図2 コーナー全体概要
Fig. 2 Outline of corner "Card-less Internet Payment System with IRIS"

リティとネットワーク利用コストの低減であるが、その要求を満足すべく、前述の二つの技術を組み合わせ、インターネットペイメントシステムを開発した。以下では本システム全体のスキームとアイリス認識技術の概要を説明する。

3. インターネットペイメントの処理方式

アイリス認識技術を個人認証に用いたプリペイド型のインターネットペイメントシステムを、カードレスシステムとして構築した。このシステムは、電子マネーサーバ (E-Money Server : EMS) とそれをサポートする、ICカード内蔵の電子金庫 (E-safe) を1セットとし、EMS間でValueを転送する、ペイメントシステム技術と、本人確認のためのアイリス認識技術、2つの要素技術から構成されている。

DataおよびValueのフローを以下に説明する。

ショッピングを実行する時の処理の流れは図2に示す順番で行われる。

インターネットショッピングのクライアントは、アイリス登録機を使って、アイリス認証センタに利用者のアイリスデータを登録する。登録時点では、本人を証明する書類などとともに銀行の支店等で登録することを想定している。また、登録する本人が銀行に口座を開設しておく必要もある。

実際にインターネットのショッピングを行う前に、クライアントの銀行口座から、E-Moneyサーバに現金を電子マネーとして移動させておく。この時に、アイリス認証を使って本人確認を行い、本人の銀行口座から、指定した額の貨幣価値を電子マネーとして、E-Moneyサーバへ転送しておく。たとえば1万円を事前に電子マネーとしておく場合には、1万円が口座から引き落とされ、1万円の電子マネーがE-Moneyサーバに蓄積される。

ショッピングを行うマーチャントにアクセスし、購入する商品を選択して、購入手続を実行する。支払を実行する時点で、アイリス認証を行い、登録された本人であることを確認する。

クライアントのPCからE-Moneyサーバにマーチャントの銀行のE-Moneyサーバへの支払指示を送信する。

クライアントの銀行のE-Moneyサーバからマーチャントの銀行のE-Moneyサーバへ購入代金が転送され

る。

マーチャントの銀行のE-Moneyサーバからマーチャントサーバへ支払が完了した通知が送信される。

クライアントの銀行のE-MoneyサーバからクライアントのPCへ支払が完了した通知が送信される。

インターネットで用いられている決済手段としては、現在は、クレジットカードを利用したものが主流になっている。クレジットカード決済の場合には、マーチャントはクレジットカード会社に手数料を支払う必要がある。インターネットで100円程度の小口の商品を扱いたい場合に、クレジットカード決済を利用すると、手数料の負担が重くなり、また実際の入金もすぐに実行されないため、マーチャントにメリットが少ない。

本システムの場合、実際の貨幣価値の移動は、2つのE-Moneyサーバの間で実行されるため、即時決済が可能である。また、クレジットカードのように手数料が必ずしも必要ではないので、インターネットで少額の即時決済が必要な分野に適していると思われる。

また、ICカード型の電子マネーは、ICカード自体のコストの問題で普及が遅れている。電子マネーの蓄積される場所をサーバ側にしたことで、クライアントにICカードを配布せずに電子マネーの利用を可能にしている。

電子マネーのプロトコルとして、本システムではMONDEXを採用している。E-MoneyサーバにはMONDEXマネーを蓄積するICチップを最大64枚搭載可能な電子金庫をI/O装置として接続している。ICチップの枚数は電子金庫を増設することで拡張可能である。MONDEXの電子マネーでは、価値転送のプロトコルがすべてICチップの中に搭載されており、転送時には送信側と受信側の2つのチップ間の暗号化された価値転送プロトコルにより転送が行われる。E-Moneyサーバは価値転送のためのプロトコルを処理せず、単純な受け渡し役のみのため、ソフトウェアの改ざん等による電子マネーの偽造等が発生しない。

4. アイリス認識システム

4.1 アイリス認識

ネットワークにおける個人認証として、当社はアイリス技術を有望なアプローチとして提案している。ここでは、このアイリス認識の仕組みとそのアプリケーション例について説明する。

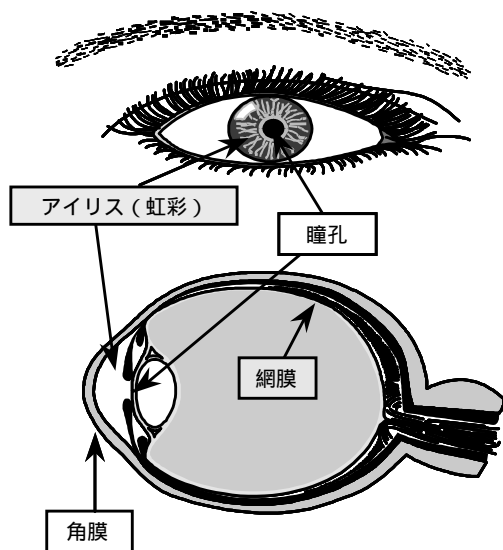


図3 眼の構造図
Fig. 3 Iris structure

図3に、眼の構造を示す。アイリスとは、人の眼の瞳孔を取り巻く黒目の部分であり、瞳孔の大きさの調整を行う筋肉から構成されている。このアイリスに存在する皺のパターンは発育時のランダム性から生じ、各人に固有であり、生後約2年目までに確定し、その後一生変換することはない。

アイリスによる個人認証とは、これらの特徴に着目し、カメラで撮像したアイリスの特徴パターンを、イメージ処理技術を用いてコード化し、このアイリスコードとあらかじめ登録してある本人のアイリスコードを照合することにより個人認証を実現するものである。

アイリスには、経年変化がない、偽造できない、誤認識が稀である、等の特徴があり、アイリス認識は高レベルのセキュリティを実現することができる。

4.2 アイリス認識を用いたシステム

アイリス認識を用いたシステムは、これまでのIDカード、パスワードなどを用いたシステムとは異なり、個人固有のアイリスコードによる照合を行うため、極めて高いセキュリティを確保することができる。また基本的に非接触での個人識別が可能のため、指紋照合型のように接触する不快感を伴わないという特徴を有する。システムの構成例を図4に示す。

システムを構成する装置としては、照合を行うゲー

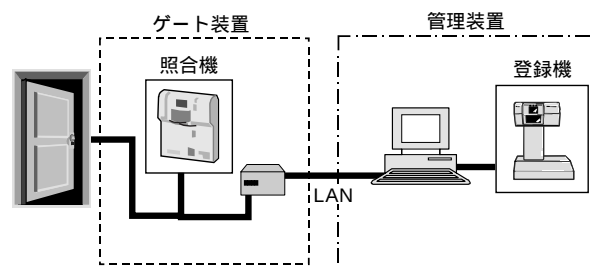


図4 アイリス認識を用いたシステム例
Fig. 4 Example of iris recognition system

ト装置、および登録を行う管理装置から構成される。

管理装置は、接続されるアイリス登録機で取得したアイリス画像をコード化し、個人情報（名前、所属名称等）とともにデータベースに登録し管理する機能を有する。

ゲート装置は、アイリス照合機で取得したアイリス画像をコード化し、データベースに登録されたアイリスコードと照合を行うものである。

本システムの利用者は、あらかじめ管理装置においてアイリス登録を行う。登録所要時間は、オペレータによる登録作業を含めて約3分ほどである。利用者は、アイリス照合機の前に立ち、アイリス照合機のLCD画面を覗き込み、LCD画面に表示される自分の眼の画像を見ながら照合を行う。ゲート装置によりアイリスパターンが取得され、本人が認識される。アイリス照合時に利用者がLCD画面に表示される自分の眼画像を確認しながら照合できるため、良好なアイリスパターンの取得が可能となり、照合時間1秒以下、誤認識率0.001%以下の高精度を確保することが可能である。

5. あ と が き

今後の課題としては、こういった有望アプリケーションにミートした技術開発、それと同時にビジネススキーム開発が急務である。ネットワーク社会においては一地域でクローズされない。従って、Globalな状況を何時も視野に入れながら開発に取り組む必要がある。今後具体的なスケジュールを含めて真剣に検討を進めていきたい。