コンピュータセキュリティ　4－10
（1999．3．5）

本人認証ICカードによる高セキュリティシステムの構築

磯部義明，三村昌弘，瀬戸洋一，菊地良知＊
（株）日立製作所　システム開発研究所，＊システム開発本部

オープンネットワークを介したエレクトロニックコマースなどの非対面の商取引では利用者の認証が重要である。一般に，利用者の認証はＰＩＮ（Personal Identification Number）およびパスワード照合より行われているが，盗用などの脅威がある。この脅威に対し，生体情報の照合を用いたＩＣカードの持ち主認証が有効である。本論文では指紋照合および公開暗号技術を用いた本人認証システムの構築について述べる。

A Proposal for Authentication System using a Smart card with Fingerprints

Yoshiaki Isobe, Masahiro Mimura, Yoichi Seto and Kikuchi Yoshinori*
Hitachi,Ltd. Systems Development Laboratory,
*Business & Information Systems Development Division

Abstract

Personal authentication is required for transactions through the open network like electronic commerce. Usually authentication by PIN and password is easy to break. An authentication by biometrics takes an immediate effect on prevention of frauds. This paper describes another system to authenticate the owner of smart card by using fingerprint matching and an asymmetric cryptography.

はじめに

情報システム技術の急速な進展により，オープンネットワークを介した非対面の商取引が急速に立ち上がりつつある。非対面取引においては本人の証明（認証）が必要となるが，現在，広く用いられている所有物や秘密情報による認証は盗用される危険が大きく，生体情報（バイオメトリクス）を利用した本人認証が有効といわれている。

バイオメトリクスは指紋や虹彩など人体の情報を利用して個人を識別する技術である。従来，重要施設の制限区域への入退管理などに単独で利用されてきたが，今後は，ICカードや暗号技術などとの連携による本人認証（Authentication）技術をPCやデータベースのアクセスコントロールや電子商取引，ワンストップ行政サービス，インターネットバンキングなどへの展開が期待されている。

本論文では，指紋照合技術と電子署名技術により高いセキュリティを確保した本人認証システムについて述べる。

バイオメトリクス技術

表１に代表的なバイオメトリックスとその特徴を示す[4][5]。バイオメトリックスには身体的な特徴と行動的な特徴の２種類がある。前者は，指紋，掌形，顔，虹彩などであり，後者は，声紋，署名などである。発声や筆記は随意的な要素があるために声紋，署名は上記の身体的特徴の生体計測的なバイオメトリックスと異なり行動計測的な特徴と呼ばれる。

バイオメトリクス技術を本人認証システムへ導入する場合，以下の項目の検討が必要である。

（１）安全性：

照合精度が高く認証が確実，偽造，盗難などによる悪用が困難，人体に無害，長期にわたり特性が変化しない

（２）経済性：

投資コストに見合う性能が達成できる

（3）簡便性：

操作が簡単，認証時間が早い，携帯性がある

（4）社会的受容性：

違和感，抵抗感なく利用できる

バイオメトリクス技術の性能は安全性だけで決めることはできず，アプリケーションのニーズによって適用するバイオメトリクス技術を選択する必要がある。

指紋は利用者の受容性に心理的抵抗があるといわれているが，小型で安価な入力装置により中程度の照合精度を実現できる特長から適用分野が広く，オフィスや家庭での利用に適している。この理由から，今回の本人認証システムではバイオメトリクス技術として指紋を採用した。

表1 バイオメトリクス技術の比較

バイオメトリクス	特徴量	コスト	ユーザ受容性	安全性	精度[%] 本人拒否	精度[%] 他人受入	データ量[バイト]	適用分野	ベンダ例
指紋	手の指の指紋の特徴点(マニューシャ)を利用	低	登録に心理的抵抗	中	0.5	0.001	<1000	全般	Identix Indicator
掌形	手の大きさ、長さ、厚さあるいは比率	中	容易	低	0.15	0.15	10	低セキュリティ施設管理	Recognition Systems Computer Data System
顔	顔の輪郭、目や鼻の形および配置	中	容易	低	1	1	1000	低セキュリティ施設管理	Miros Visionics
虹彩	目の虹彩(アイリス)の放射上の紋様	高	登録に手間	高	2.8	0	256	高セキュリティ施設管理	IriScan Sensar
声紋	話者の音声特徴	中	容易	低	1	0.1	1000	電話サービス	Nuance Veritel
署名	署名の字体や署名時の書き順、筆圧	低	容易	低	0.2	0.6	1000	セキュアPC	Cadix PenOp
その他	耳形状、キーストローク、手の甲の血管パターン、におい、DNAなど	製品化された技術もあるが多くは研究中							

指紋照合アルゴリズム概要

本論文では，あらかじめ登録した特徴点を含む画像片（チップ）と入力した指紋画像の相関を用いて指紋照合を行うチップマッチング方式を採用している[6]。この方式は登録データ量が多いが，処理時間が早いのが長所である。指紋照合処理は，入力指紋の平行移動量推定，チップマッチング，合否判定処理の順に行われる。図1は照合処理を模式的に示している。左の画像は特徴量として記録されたチップ画像であり，右の画像は位置ずれを補正した後の入力指紋の画像である。この例では，指が登録されている特徴量に対して右下に入力されているので，入力指紋の位置は左上方向に補正され，照合が実行されている。

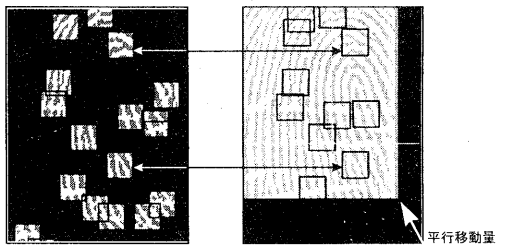

図1 指紋の照合例

本人認証システム

インターネットバンキングやインターネットショッピング，ワンストップ行政サービス，テレワークなど，オープンネットワークを介して複数の利用者が非対面にサービスを要求するアプリケーションにおいて，広く本人認証 IC カードが流布される場合の運用システムを想定する。

本システムの運用シナリオは次の通りである。

- 本人認証 IC カード利用者の新規登録を受け付ける登録端末は，銀行や郵便局，コンビニなど公共的なスペースに多数設置し，広く利用者から個人情報と指紋画像を収集する。
- 登録端末が収集した個人情報と指紋画像は，本人認証 IC カードを発行する発行センターに転送される。
- 発行センターでは，オペレータにより利用者の予信照会を行われ，IC カードの発行を行う。

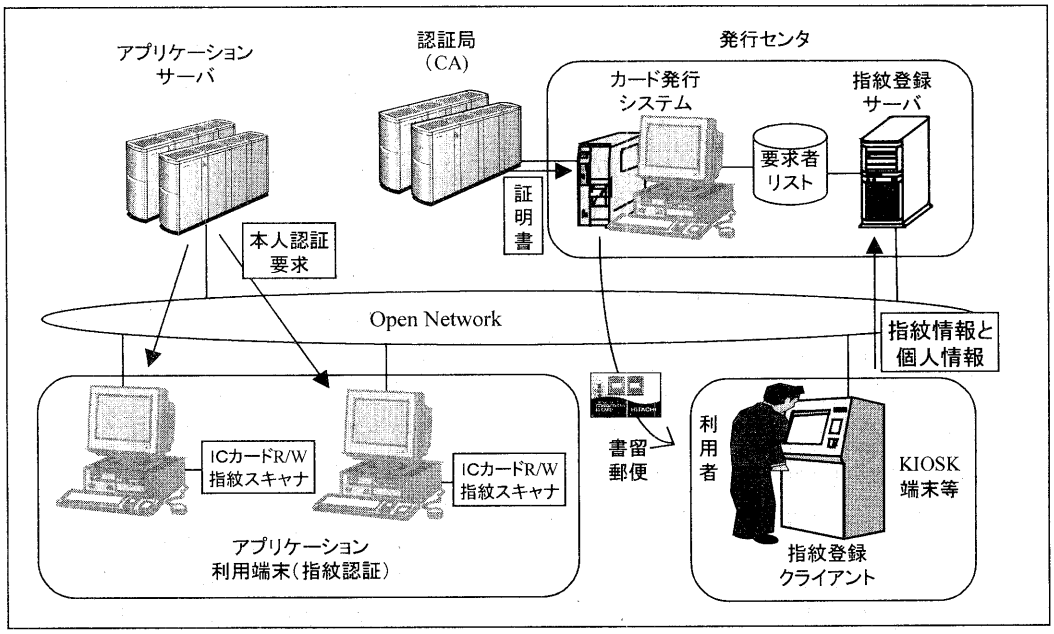

図2 本人認証システムの構成

・本人認証は，IC カード R/W と指紋入力装置を追加した家庭用 PC や公共的なスペースに設置された KIOSK 端末などで実行する。

以上のような要件を想定して，次のようなシステム構成の本人認証システムの開発を進めている（図２）。

（１）指紋登録サブシステム

・KIOSK 端末などを想定した，指紋画像と個人情報の収集を目的とした指紋ライブスキャナを持った指紋登録クライアント

・発行センタにおいて，指紋画像と個人情報を集積する指紋登録サーバ

（２）カード発行サブシステム

・発行オペレータにより予信照会を行い，IC カードの発行を行うカード発行サブシステム

・ＩＣカードに添付する電子証明書を発行する認証局（ＣＡ）

（３）カード認証サブシステム

・家庭やオフィス，KIOSK 端末などからの利用を想定した，指紋ライブスキャナと IC カードリーダを持った指紋認証端末 PC

本論文では，これらのサブシステムのセキュリティ脅威およびその対策，機能，処理フローについて検討した結果について述べる。

指紋登録サブシステム

指紋登録サブシステムにおいて，次のようなセキュリティ脅威が考えられる。

(a)KIOSK 端末に入力した個人情報を他者に盗み見られ，プライバシーが侵害される。

(b)不正な KIOSK 端末に置き換えることで，個人情報および指紋画像が詐取される。

(c)KIOSK 端末と指紋登録サーバとの通信において，個人情報および指紋画像が盗聴される。

(d)KIOSK 端末に入力した情報を KIOSK 端末管理者や係員，店員などに盗聴・改ざんされる。

これらの脅威に対し，次のような対策が考えられる。

(A)ディスプレイを他者から遮蔽する。

(B)KIOSK 端末の偽造・変造を防止するシールを貼るなどの対策を取る。

(C)公開鍵方式による相互認証および暗号化

により，セキュア通信を行う。

(D)個人情報および指紋情報の登録時に係員を介在させず，案件ごとにその場で転送し，KIOSK 端末に情報を残さない。

これらの対策のうち，(C)(D)について機能化を図った。機能ブロック図を図３に示す。

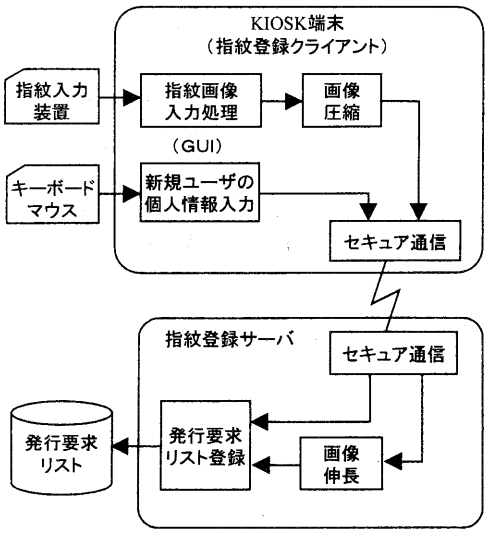

図3 指紋登録サブシステム

指紋登録サブシステムは，複数のクライアントと，IC カード発行サブシステムと同一マシン上にあるサーバプログラムからなる。

指紋登録サブシステムのクライアントは，指紋スキャナおよびキーボードやマウスなどのインプットメソッドを持ち，ＧＵＩによりＩＣカード発行要求者の指紋画像および個人情報を入力する。画像については圧縮処理を行い，入力収集したすべての情報について暗号化しサーバに転送する。

指紋登録サブシステムのサーバは，クライアントから転送されたデータを復号化し，画像については伸長処理を行い，発行要求リスト（データベース）に登録する。

カード発行サブシステム

カード発行サブシステムにおいて，次のようなセキュリティ脅威が考えられる。

(a)発行された IC カードを解析されることにより，不正な IC カードが発行される。

(b)発行された IC カードを解析されることにより，他人の IC カードの情報を盗用し他人に成りすます。

(c)発行オペレータにより，不正な IC カードが発行される。

これらの脅威に対し，次のような対策が考えられる。

(A)発行する IC カードに IC カードの正当性を証明するため認証局（CA)の電子証明書を添付する。

(B)IC カードに持ち主認証のためのバイオメトリクス（本報では，指紋情報）を追加し，さらに，(A)の電子証明書のシリアル番号を含んだ電子署名を作成し添付することで，バイオメトリクスの正当性を保証する。

(C)IC カード発行業務のログを取り，不正発行を監視する。

これらの対策を施したカード発行システムの機能化を図った。機能ブロック図を図４に示す。

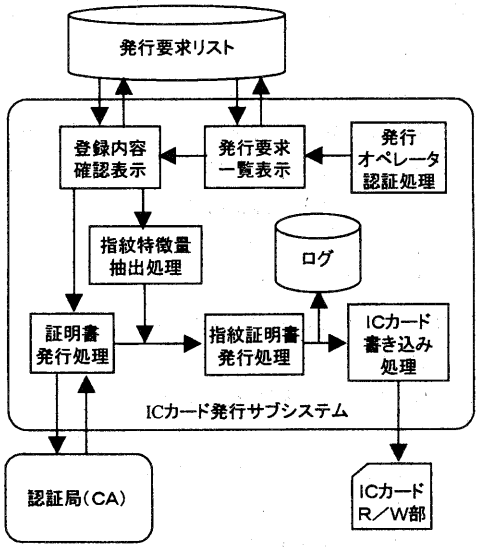

図4 カード発行サブシステム

IC カード発行サブシステムを実行するオペレータにより不正が行われるとシステム全体の

破綻につながるため,厳重な管理が必要である。ここでは，IC カード発行サブシステムの設置場所などへの入退室などを管理した上で，IC カード発行サブシステム実行時に発行オペレータを認証することで発行処理のログを取り，発行オペレータの不正を抑止する。

IC カード発行処理は，まず，複数の登録サブシステムにより登録された発行要求リスト（データベース)より任意の発行要求一覧を GUI に読み出し，一覧より選択することで，発行要求者の登録内容を表示し，ここで表示された情報に基づき予信照会を行う。予信照会で問題がなければ，発行要求者の個人情報について，必要な情報を認証局（CA)に転送し，電子認証用の証明書を得る。指紋画像については，指紋特徴量を抽出し指紋証明書を生成する。この際，電子認証用の証明書のシリアル番号を指紋証明書に含み，ＩＣカードの改ざんなどの脅威に対抗する。電子認証用の証明書および指紋証明書，ユーザー情報を IC カードに書き込み，IC カードを発行する。

ここで，発行した IC カードは，郵便書留めなどを利用して発行要求者に送付される。

カード認証サブシステム

カード認証サブシステムにおいて，次のようなセキュリティ脅威が考えられる。

(a)カード認証サブシステムをなりすます不正なプログラムにより，不正なアクセスが行われる。

この脅威に対し，次のような対策が考えられる。

(A)サーバアプリケーションと IC カードが，直接，相互認証する。このため，サーバアプリケーションの認証要求に対し，IC カードの持ち主認証処理も IC カード内で行う必要がある。

本報告では，IC カード内の処理を PC でシミュレートした図５で示す機能の開発を図った。

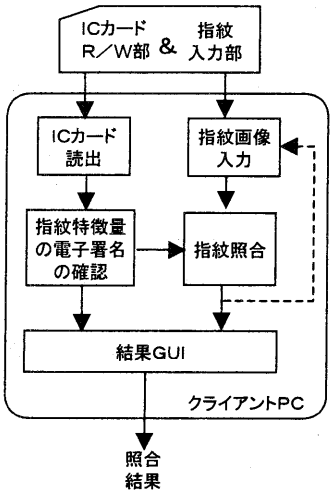

図5 カード認証サブシステム

認証サブシステムは，アプリケーションにより起動されるライブラリ形式となる。起動された認証サブシステムは，IC カードおよび指紋画像を要求する GUI を表示する。指紋証明書の電子署名を確認し，入力した指紋画像と指紋証明書の特徴量により本人照合し，結果を表示し，結果をアプリケーションに返す。アプリケーションはこの結果に従って，高セキュリティの情報などを提供する。

おわりに

ＩＣカード技術と公開鍵暗号方式による電子認証技術と指紋による持ち主認証技術とを組み合わせ，偽造・改ざん等の脅威に対処した，本人認証ＩＣカードシステムについて述べた。今後は，ＩＣカードの偽造脅威に対処するＩＣカード技術の開発を進める。

謝辞

本研究は，「マルチメディアネットワーク共通化技術の研究開発」の一環として，平成 10 年度補正予算にて，通信・放送機構（TAO)から委託をうけて，研究開発中である。

参考文献

[1]佐々木ほか，インターネットセキュリティ

基礎と対策技術，オーム社 (1996).
[2]瀬戸，バイオメトリックスを用いた本人認証技術， 計測と制御 第37巻 第6号 1998年6月
[3]本人認証技術検討WG，本人認証技術検討WG中間報告書-参照モデルと評価基準V0.5-，電子商取引実証推進協議会，平成9年5月.
[4]The World Premier Card and Security Technology Conference, Conference Proceedings CardTech/SecurTech'97, May 19-22 ,Vol.1-2 (1997) .
[5]Special Issue on Automated Biometric Systems, Proc. of The IEEE ,Vol.85, No.9(1997).
[6] 三村，磯部，瀬戸， 指紋によるＩＣカード持ち主認証システムの開発，情報処理学会 CSS'98 論文集 IPSJ Symposium Series Vol.98, No.12
[7] 織茂，瀬戸ほか，セキュリティシステムにおける IC カードの活用 日立評論，Vol.80, No.4, pp.45-50 (1998).