コンピュータセキュリティ　10－21
（2000．　7．25）

ＩＣカード実装型指紋照合装置の開発

石田　修一，　三村　昌弘，　瀬戸　洋一
（株）日立製作所　システム開発研究所
244-0817　神奈川県横浜市戸塚区吉田町 292 番地
shuichi@sdl.hitachi.co.jp, mmimura@sdl.hitachi.co.jp, seto@sdl.hitachi.co.jp

あらまし

インターネットなどを介した個人認証にはＩＣカードと生体情報を組み合わせた認証が効果的である．認証はデジタル署名技術を用いたＩＣカードの認証と，カードに格納した生体情報を用いたカード利用者の認証の2段階で行われる．生体情報によるカード利用者の認証は，安全性等の面からＩＣカード内部で行われるのが望ましい．本報告では，ＩＣカード実装型の指紋照合技術について述べ，そのプロトタイプシステムを開発した結果を報告する．

キーワード　生体認証，　ＩＣカード，　認証，　デジタル署名

Development of Personal Authentication System Embedded in Smartcard

Shuichi Ishida, Masahiro Mimura, and Yoichi Seto
Systems Development Laboratory, Hitachi, Ltd.
292 Yoshida-cho, Totsuka-ku, Yokohama,244-0817 Japan
shuichi@sdl.hitachi.co.jp, mmimura@sdl.hitachi.co.jp, seto@sdl.hitachi.co.jp

Abstract

The combination of Smart card and biometrics is effective for personal authentication through the open network. The combination is realized as two steps authentication that the smart card is authenticated by PKI and the card holder is verified to the template stored in the card by biometrics technique. The biometric verification has to be executed in the card on purposed of security. This paper presents a fingerprint verification method that can be embedded in a smart card.

key words　Biometrics, Smartcard, Authentication, Digital Signature

1. はじめに

インターネットに代表されるネットワーク基盤の整備により，エレクトロニックコマース（EC），電子的情報交換（EDI），WWW による情報流通などのオープンネットワーク上で行われる電子取引が立ち上がりつつある．電子取引には一般的に認証，守秘，データ完全性などの情報セキュリティが必要とされており，これらは暗号化とデジタル署名などの暗号技術を用いて実現されている．さらに電子取引はその非対面性から利用者の本人確認（認証）を必要とする場合がある．本人認証は，IC カードなどの記憶装置に保存した利用者の秘密鍵を用いるデジタル認証と，パスワードなどの秘密情報や指紋などのバイオメトリクス（生体情報）を用いた本人確認を組み合わせて実現する．デジタル認証における本人認証には秘密鍵が必要であり，鍵の保管には IC カードを用いる．本人確認には，万人不動な個人の体の特徴を利用するバイオメトリクスが有効といわれている[1][2][3]．

バイオメトリクスによる本人認証はパスワードなどの秘密情報に比べ利便性と安全性の面で利点がある．具体的には，所持あるいは記憶の必要はないという利点がある．その反面，画像処理などの方法で生体の特徴を計測するため，精度（安全性）が十分でないという問題がある．利便性を重視した本人認証システムの場合，現状の ID およびパスワードをバイオメトリクスに置き換えることが可能である．一方，安全性を重視する本人認証システム場合，オープンネットワーク環境やプロテクティッドエリア外での運用を想定し，暗号技術を用いたデジタル認証との組み合わせが不可欠となる．デジタル認証では利用者の秘密鍵を安全に保持・運用する必要があるため，秘密鍵は通常 IC カードに保管される．従って安全性を重視した本人認証システムとでは，IC カードとバイオメトリクスの連携が有効となる．

指紋照合を用いてICカードの持ち主（利用者）を認証する場合，あらかじめ指紋から抽出した特徴量（テンプレート）をICカードに登録しておき，特徴量と新たに入力した指紋を照合することで，利用者の本人確認を行う．コンピュータ（PC）を安全に運用することのできる管理領域（プロテクテッドエリア）などでは，指紋を照合する装置を管理下に置くことで，特徴量や本人認証処理を安全に管理・運用することが可能である．しかし消費者ECのように利用環境が限定されない場合には，指紋照合装置への攻撃がたやすく行えるため，テンプレートの盗用，照合結果の偽造，入力指紋の盗用を防止する強固なセキュリティ対策が必要となる．

本報告では，利用環境が限定されない場合にも安全に運用可能なICカード実装型指紋照合装置を提案する．またその開発に最も重要である指紋照合アルゴリズムの接触型ICカードへの実装に関して述べる．

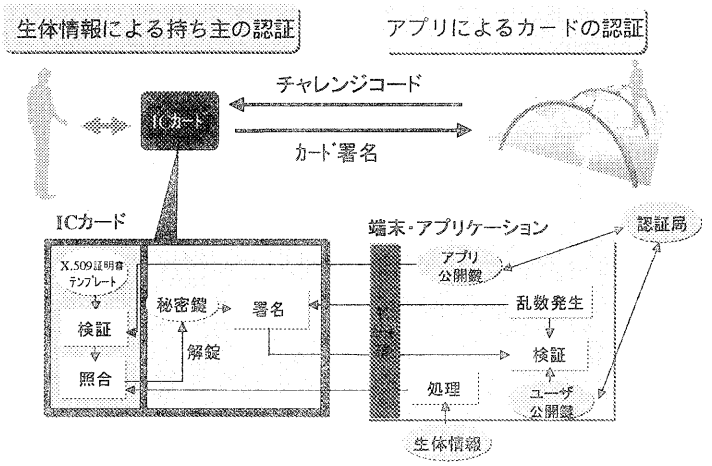

図 1． IC カード持ち主認証システム

2．IC カード持ち主認証システム

ネットワークでの認証技術として一般的にはデジタル署名を用いる．暗号技術を用いるデジタル認証では、ユーザが認証用の鍵を安全に管理する必要がある。このとき鍵の格納媒体，署

名作成媒体として,ICカードを利用することは，秘密鍵の安全な管理を実現する上で有効である．しかし，IC カードには紛失・盗難時に第三者に悪用される恐れがあるため，PIN などを用いてカード利用者の確認を行う必要がある．本研究では，利用者の確認技術として指紋照合を用い，デジタル署名技術と，指紋照合技術を連携したシステムを開発した．

図1に IC カード持ち主認証システムを示す．ディジタル証明書による認証を，IC カード内のバイオメトリクス情報のデータ完全性の確保と IC カードの利用権の認証の2つに利用している[4]．

バイオメトリクスを用いた IC カード持ち主認証技術の実現方法としては，以下の2つがある．

Stored Template 型　：　テンプレートを IC カードに保管しておき，テンプレートと新たに入力した指紋を IC カードの外部処理装置（例えば PC）で照合する．(図 2)

Embedded Process 型　：　テンプレートの保管および照合処理を IC カード内で行う．(図 3)

さらに IC カードに電子的指紋入力装置（ライブスキャナ）を一体化し，入力から一貫処理するタイプの開発計画が海外のメーカである．

Embedded Process 型の照合方式はカード内で照合を行うため，テンプレートや照合結果がカード外に出力されないという利点がある．これは，端末におけるテンプレートの漏洩や照合結果の改ざんを防ぐことができるため，端末の安全性が完全に保証できない PC での認証を行うシステム（オンラインショッピング等）に有効である．

Stored Template 型に関しては，テンプレートデータに X.509 証明書を添付し改ざん防止を強化した方式を開発済みである[4][5]．本発表では照合処理も IC カード内で実現する Embedded Process 型の本人認証技術について述べる．認証処理の概要は以下のとおりである．

① IC カードに保管したバイオメトリクス情報（テンプレート）が不正に発行されたものでないか確認を行う．これはテンプレートに X.509 形式の証明書を添付し，利用に際して，アプリケーション側から対応する公開鍵を送信し IC カード内で検証する．

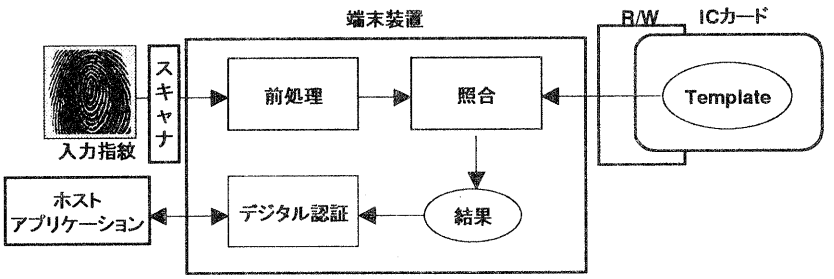

図 2．Stored Template 型

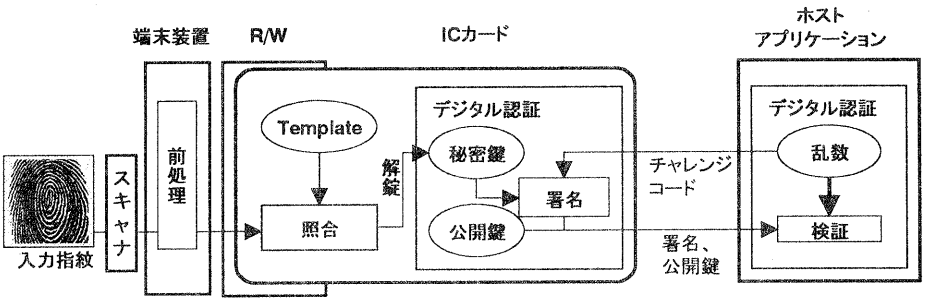

図 3．Embedded Process 型

② 認証の結果，正当なテンプレートであることが判明したら，そのデータを用い，入力したバイオメトリクスと照合することで，ICカードの正しい持ち主か否かを判定する．

③ 正しい持ち主であることが判明した場合，秘密鍵を使える状態にし，アプリケーション側から送られたチャレンジコードに署名し送信する．

④ アプリケーション側では署名データを検証することにより，アプリケーションの正当な利用者か否かの判定を行う．

3．指紋照合アルゴリズムの概要

日立の指紋照合アルゴリズムの概要を示す．指紋照合アルゴリズムは，登録処理と認証処理の2つの処理より構成される．

登録処理はライブスキャナで取得された指紋に前処理（コア探索，2値化，細線化，位置補正）を行い，その指紋画像より山画像と谷画像を生成し特徴点を抽出する．次に抽出した特徴点の周りの小領域画像を切り出し，チップ画像の集まりをテンプレートとして保存する．

認証処理はライブスキャナで取得した提示指紋に前処理を行い，テンプレートと照合し類似度を算出（チップマッチング処理）する．類似度により提示指紋が登録指紋と同一人物のものか判定する．

以下に認証処理アルゴリズムの IC カードへの実装について述べる．

4．ICカードへの実装

4．1照合処理フロー

本報告では，3節で説明した指紋照合アルゴリズムのうち，照合処理部分を IC カードを利用したモデルで検討し開発を行なった．図 3 の Embedded process 型の図を用いて、照合処理の説明を行う。IC カード内照合システムは端末装置（PC：アプリケーション），電子指紋入力装置（ライブスキャナ），IC カードリーダライタ（R/W），IC カードにより構成される．ライブスキャナは入力指紋を取得し，PC に対して取得したデータを送る．PC では入力指紋に対して前処理を行う．前処理をした入力指紋を IC カード R/W を介して IC カードに送信し，入力指紋と IC カードに保存してある登録指紋（テンプレート）を照合する．照合の結果，利用者の確認に成功した場合は，秘密鍵を UNLOCK し，アプリケーションとの認証処理での利用を可能にする．IC カードは，IC カード R/W を介して PC に照合成功を送信する．PC は照合結果を取得し，その結果に応じてホストアプリケーションとの認証処理を開始する．

照合処理は以下に示す理由により PC 内で行う処理と IC カード内で行う処理に分離する方式を採用した．

(1)秘密情報であるテンプレートを IC カード外へ露出しない．

(2)IC カードの処理負荷の軽減．

(3)入力指紋をすべて転送する必要がなく PC と IC カード間の通信負荷の軽減．

(4)高次の補正処理を PC で行うことによる精度の向上．

(5)IC カードあるいは端末が盗難にあった場合のリスク分散．

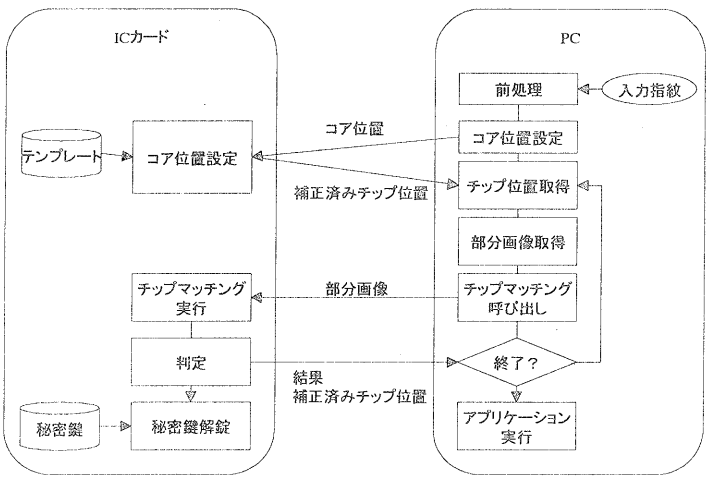

図 4．分離型指紋照合処理フロー

図 4 に IC カードと PC に分離した照合処理のフローを示す．IC カードと端末間との連携は以下に述べるように実現される．

(1) PC→IC カード

入力指紋画像よりコア位置情報を算出し，IC カードへ送信する．

(2) IC カード→PC

入力指紋画像のコア位置情報と IC カードに登録されているテンプレートのコア情報を用いてチップ位置補正量を求め，PC へ送信する．

(3) PC→IC カード

入力指紋画像よりチップ画像を切り出し，IC カードへ送信する．送信されたチップ画像とテンプレートを用い照合処理を行う．照合処理は次節で述べるスパイラルマッチング方式とエラービットカウント方式を提案し処理効率の改善を図った．

(4) IC カード→PC

照合が成功すると秘密鍵を解錠し，アプリケーションへアクセス可能とする．

(2)から(3)の処理を，テンプレートとして登録した参照用データ数だけ処理を行う．

次に図 4 のフローにおけるそれぞれの処理の内容を述べる．

(1) ずれ補正処理

図 5 にずれ補正処理の内容を示す．本処理では，PC 側で入力指紋画像のコア（指紋の渦の中心点）位置を導出し，IC カード側に送信する．IC カード側では，受信したコア位置とテンプレート登録指紋のコア位置から，登録指紋と入力指紋の位置のずれを導出し，これを補正値として設定する．

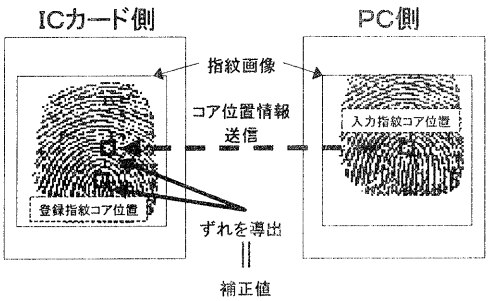

図 5．コア位置設定コマンド

(2) チップ位置送信処理

図 6 にチップ位置送信処理の内容を示す．IC カード側では，ずれ補正処理で算出した補正値を用いて，IC カードにあるテンプレートに格納されている登録指紋のチップ位置のずれを補正し，導出した補正チップ位置（チップがあると想定される座標）を端末に送信する．

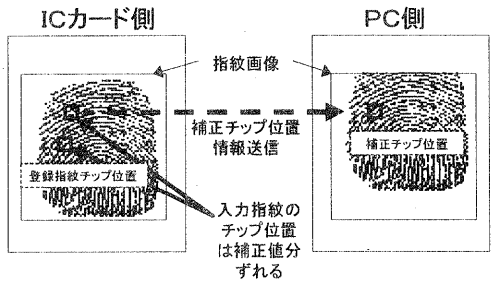

図 6．チップ位置送信コマンド処理

(3) チップマッチング実行処理

図 7 にチップマッチング実行処理を示す．PC 側では受け取った補正チップ位置の周辺にあたる画像を入力指紋画像から抽出し，抽出した部分画像を IC カードに送信する．IC カード側では受信した部分画像と IC カードのテンプレートに格納された登録指紋のチップ画像とをチップマッチング処理を用いて照合する．

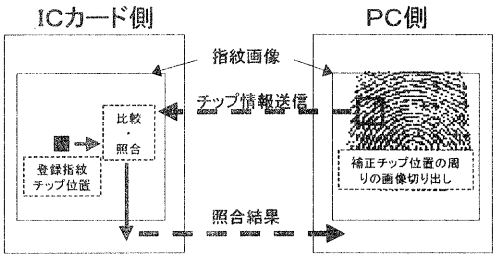

図 7．チップマッチング実行処理

次に，チップマッチング処理の詳細について述べる．チップマッチング処理は，チップ画像が入力された部分画像内に存在するかを判定する．本処理では，以下の方式を採用している．

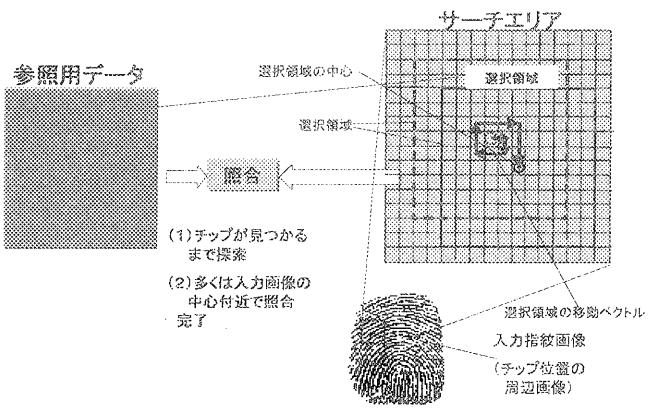

図 8. スパイラルマッチング方式

(1) スパイラルマッチング方式
(2) エラービットカウント方式

次にそれぞれの方式の処理内容を述べる。

(1) スパイラルマッチング方式

スパイラルマッチング方式を図8に示す．この処理は，入力部分画像内にチップ画像が存在するかを判定するために，入力部分画像内からチップと同じサイズの領域を選択してチップ画像と比較する．チップ画像と類似する領域が見つかるまで順番に領域を選択していく．このときチップ画像と比較する領域を，図10の入力部分画像上の矢印で示すように，中心から螺旋状（スパイラル）に移動させるように順番に選択していく．チップ画像と選択領域を比較した結果，類似誤差が事前に設定したしきい値以上であれば，照合不一致とし処理を終了する．類似誤差は，チップ画像と選択領域の画像をピクセル毎に比較して値が一致しないピクセルの数（エラービット数）で表す．

エラービット数がしきい値以下であれば，対象チップ画像は照合一致とする．エラービット数がしきい値以上であれば，次の領域を選択し照合を継続する．入力部分画像中のすべての領域を探索して，チップと類似した領域が見つからなければ，照合は失敗となる．

(2) エラービットカウント方式

図 9 にエラービットカウント方式を示す．この処理では，チップ画像とスパイラルマッチング処理で選択した領域とを比較し，エラービット数が設定されたしきい値以上かどうか判定する．このとき，チップ画像と入力部分画像との比較は 1 ライン単位で行い，画像の類似誤差が大きい場合は処理を途中で終了することで，照合処理の高速化を図っている．

1ライン分の処理手順を以下に示す．

(1) サーチエリア画像内の選択領域のデータを抽出するためにシフト演算およびマスク処理を行い計算用データ（バイト単位）を生成する．
(2) 参照用データと計算用データの排他的論理和（バイト単位）をとる．
(3) エラービット数の計算は高速化のためエラービットテーブルを用い算出する．

(1)から(3)の処理を画像の各ラインについて行う．算出したエラービット数を累積し，合計が

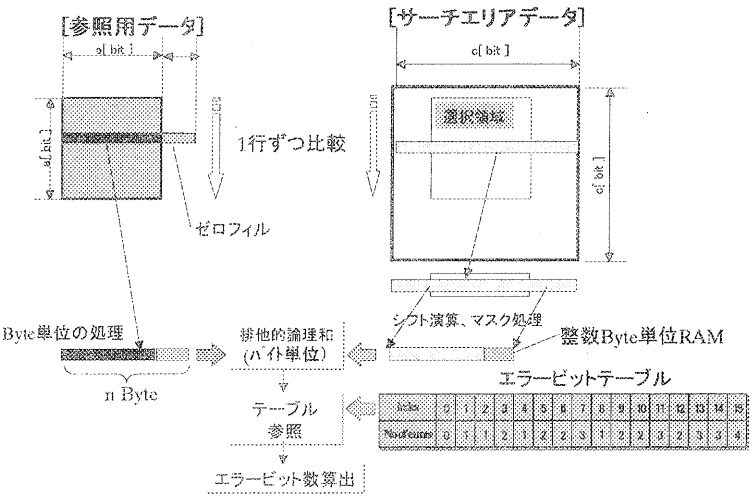

図 9. エラービットカウント方式

しきい値以上になった場合には照合は不一致（失敗）として，エラービットカウントを終了し，スパイラルマッチング処理において次の選択領域へ移動し，同様の処理を繰り返す．

サーチエリア画像のすべてのラインを処理した時点で累積エラービット数がしきい値以下なら照合は一致（成功）とする．

ここで，エラービットテーブルとは，チップ画像と選択領域の 1 バイト分のデータの排他的論理和をとって導出した 2 進数データの“1”の数（エラービット数）をテーブルに格納したものである．例えば，排他的論理和演算の結果が“18”だった場合，“(18) D= (00010010) B”からエラービット数（“1”の数）は 2 つである．テーブルよりエラービット数を得る方法は，テーブルの 0 番目のアドレスに 18 を加えたアドレスを参照することで，インデックス値【18】の“2”を得ることができる．

4．評価実験

上記のアルゴリズムを IC カードと端末に対して実装した．また，開発したプログラムの基本性能を評価した．

(1) 実験環境

表1．ハードウェア一覧

No.		
1	PC	Pentium 166MHz 64MB RAM
2	ライブスキャナ	Veridicom VFS-I
3	ICカードR/W	Maxell MR-162E
4	ICカード	Maxell製

図10は開発環境のハードウェア構成を示す．本システムはPCとライブスキャナ，ICカードリーダライタ（R/W），とICカードから構成される．

ライブスキャナは，300×300ピクセルのグレースケールの画像を取得する．この時の解像度は500dpiで色の階調8bitである．取得された画像に対して，まずフィルタリングにより，スキャン時のノイズを除去する．次に画像の解像度を310dpiに変更し，176×176ピクセルの画像に

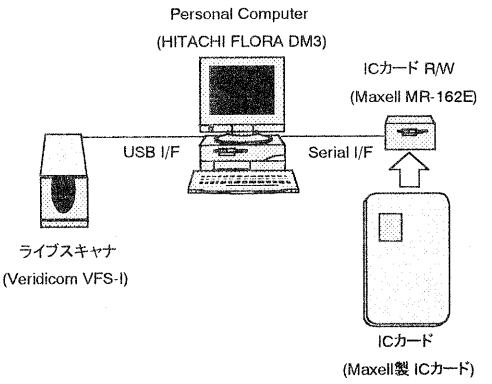

図 10．ハードウェア構成

変換する．次に、特徴点の検出を行うために，検出の前にまず，画像を白黒の2値画像に変換する．次に画像から，すべての特徴点を検出し，特徴点の周辺画像をチップ画像として抽出する．

ライブスキャナ（指紋取得用スキャナ）にはVeridicom社のVFS-Iを採用した．VFS-Iはsolid-state capacitance sensor を用いて指紋画像のキャプチャを行う．ライブスキャナはUSBインタフェースを介してPCに接続され，スキャンした500dpiの指紋画像をPCに出力する．指紋画像は300×300ピクセルの256階調グレースケールの画像である．スキャナからPCへの通信は，USBインタフェースにより，0.1秒以内で行われる．

ICカードには日立マクセル製ICカードを用いた。本ICカードはICカードリーダライタ（MR-162E）を介して，PCに接続される．ICカードの内部クロックは3.58MHzである．ICカードはシングルチップマイクロプロセッサH8/3113を搭載しており，16KBのEEPROMと，32KBのROM，2.5KBのRAMなどを搭載しており，ROMやEEPROMに格納したプログラムを実行することが出来る．本ICカードはユーザアプリケーション開発用のカードであり，開発したICカード用アプリケーションをEEPROMにダウンロードして実行することが出来る．

本開発では，開発した指紋照合アプリケーションと，指紋の特徴点のデータをEEPROMにダウンロードし，ライブスキャナからスキャンした指紋画像と照合を行った．

また，開発言語はアセンブラ言語（IC カード内照合部分）とC言語（PC処理部分）を用いた．

(2) 評価結果

ICカードは，メモリ容量が小さく，またCPUの処理能力もPCなどに比べて十分ではないため，本開発では，プログラムの速度性能とコードサイズが重要な問題になる．このことから，ICカード内のプログラム開発にはアセンブラ言語を用いた．本プログラムのICカード実装部分のコードは1.3Kバイトであった．実行時間は図11に示す通りであった．

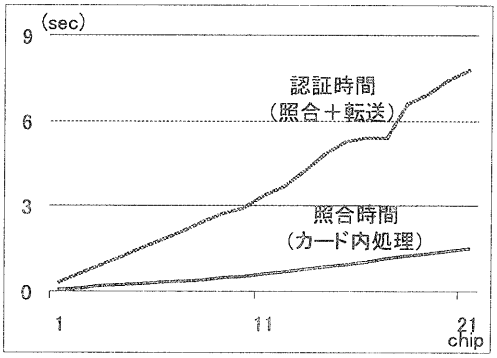

図11．照合時間

今回の評価実験ではデータ転送処理の最適化は行わなかったので，処理時間の約70%以上はデータ転送に費やされた．転送時間の改善は今後の課題である．

5．まとめ

ICカード利用者の本人認証技術などで指紋の照合技術を用いるシステムの開発が進められている．本研究では，ICカードでの利用を想定した，デジタル署名と指紋情報を用いた本人認証技術の連携を提案し，ICカード内で指紋照合を行うシステムの研究開発を行った．具体的には，ICカードと端末との連携により指紋照合を実現するプログラムを開発した．本システムの特徴としては，

(1) 秘密情報であるテンプレートがICカード外へ露出しない．

(2) ICカードの処理負荷が軽減する．

(3) 入力指紋をすべて転送する必要がなくPCとICカード間の通信負荷が軽減する．

(4) 高次の補正処理をPCで行うことによる精度の向上が実現できる．

(5) ICカードあるいは端末が盗難にあった場合のリスクが分散する．

等があげられる．

また，本指紋照合システムに関して，性能評価を行った．その結果，ICカード内での照合処理の速度が十分高速であることが確認でき，実利用が可能な性能の見通しを得ることができた．

参考文献

[1]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-ver0.5-，電子商取引実証推進協議会（1998）

[2]瀬戸：バイオメトリクスを用いた本人認証技術，計測と制御，Vol.37,No.6（1998）

[3]特集ここまできたバイオメトリクスによる本人認証システム，情報処理学会誌，Vol.40, No.12（1999）

[4]磯部，瀬戸，三村：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，情報処理学会，CSEC-4, Vol.9, No.24, pp.55-60(1999)

[5]三村，瀬戸：指紋によるICカード持ち主認証システムの開発，情報処理学会シンポジウム，Vol.98, No.12, pp. 185-188（1998）

[6]The Biometric Consortium Fall'99, Conference（1999）

[7]瀬戸，三村，石田：ICカード実装型指紋照合による本人認証技術の開発，暗号と情報セキュリティ・シンポジウム，SCIS2000-D01, (2000)