平成１７年度

バイオメトリクスによる簡易認証システムの調査・開発

報　告　書

平成１８年３月

財団法人ニューメディア開発協会

この事業は、競輪の補助金を受けて実施したものです。

まえがき

ＩＴ（情報技術）を利用するシステムにおいては、利用者が本人であることをシステムが認証してはじめて、本人がシステムを利用することができるようになっているものが多数存在します。認証は、通常暗証番号やパスワードを用いたり、認証のための装置をシステムに接続して行ったりする認証方法が用いられています。

認証のための装置のひとつであるＩＣカードは、セキュリティが高いので偽造することが難しい反面、利用するのが比較的簡単で、携帯も手軽なため普及が急速に進んでいます。

通常ＩＣカードを利用する際には、ＩＣカードの正規の利用者であることを証明するための暗証番号の入力が必要になります。しかしながら暗証番号は、それ自体を忘れてしまってＩＣカードが利用できなくなってしまったり、忘れないように暗証番号を記載しておいた紙を紛失したり、暗証番号の入力を盗み見され、ＩＣカードを第三者に不正利用されてしまう等の可能性も皆無ではありません。

そこで、本テーマの調査・開発では、本人確認のための指紋を使ったバイオメトリクス技術を利用して暗証番号の入力の代りとするＩＣカード認証システムを開発し評価を行いました。本開発に係わるバイオメトリクス認証技術については、ＩＣカードに指紋データを登録し、ＩＣカード内で指紋データの照合を行うマッチオンカード方式を採用し、その運用性、認証の所要時間等について評価し、課題の抽出を行いました。

この報告書は、その結果についてとりまとめたものであり、今後のＩＴ社会発展の一助になれば幸いです。

平成１８年３月

財団法人ニューメディア開発協会

目　次

1．バイオメトリクスによる簡易認証システムの調査・開発の目的 1
2．　調査・開発の概要 2
　2．1．開発する簡易認証システムの基本要件 2
3．調査用簡易認証システムの開発 3
　3．1．開発内容 3
　3．2．システム構成の概要 3
　　3．2．1．システムＡ 3
　　3．2．2．システムＢ 6
　3．3．簡易認証システムの動作説明 10
　　3．3．1．システムＡ 10
　　3．3．2．システムＢ 10
4．簡易認証システムの評価 12
　4．1．仕様 12
　4．2．テンプレートの登録 12
　　4．2．1．テンプレート登録の仕様 12
　　4．2．2．テンプレートの登録手順 13
　4．2．3．テンプレート登録時の所要時間 25
　4．3．指紋の認証 29
　　4．3．1．認証の方式 29
　　4．3．2．認証の手順 29
　　4．3．3．認証時の所要時間 42
　4．4．認証の失効 46
　　4．4．1．失効の方式 46
5．互換性・標準化及びその他の課題 48
　5．1．ＩＣカード及びカードＯＳの国際標準化動向 48
　5．2．マッチオンカードの国際標準化動向 48
　5．3．マッチオンカードのセキュリティ 50
　　5．3．1．登録時のセキュリティ 50
　　5．3．2．ＩＣカードに登録されたテンプレートのセキュリティ 50
　5．4．暗証番号 50
まとめ 51
添付資料一覧 52

＜他社所有商標に対する表示＞

1. Microsoft®は、米国及びその他の国における米国 Microsoft Corp.の登録商標です。
2. Windows®は、米国及びその他の国における米国 Microsoft Corp.の登録商標です。
3. Microsoft Excel は、米国 Microsoft Corp.の商品名称です。
4. MULTOS は、MAOSCO Ltd.の登録商標です。
5. Java 及びその他の Java を含む商標は、米国及びその他の国における米国 Sun Microsystems, Inc. の米国及びその他の国における商標または、登録商標です。
6. その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

＜略称説明＞

本資料では、Microsoft® Windows®を Windows に、Microsoft Excel を Excel に、それぞれ略称いたします。

1. バイオメトリクスによる簡易認証システムの調査･開発の目的

本調査・開発事業は、バイオメトリクス認証技術を利用して本人認証を簡易的に行うことについて調査・開発する事業であり、本人の指紋登録データ（以下「テンプレート」という。）をＩＣカードに搭載し、本人が持参したＩＣカード内のテンプレートと本人の指紋読取情報を照合して本人確認を行う認証システムに関するものである。

システムへのログオン等に関しても、ＩＤ・パスワードを入力する代りに本人のバイオメトリクス情報（指紋）をＩＣカードの中で照合し、本人確認を行った後、システムに自動的にログオンできる簡易認証システムや、システムアプリケーションの中で、暗証番号を入力する代りにバイオメトリクス情報を利用して本人確認を行うことができる簡易認証システムについて調査・開発する。

バイオメトリクスの認証については、一般的に、顔の輪郭や指紋等のバイオメトリクス情報を採取し、特徴点を抽出してテンプレートと称する「データ列」を発生させる。このデータを個人本人のデータとして保管しておき、認証時にセンサから抽出したデータと照合して、本人確認を行う。このテンプレートをＰＣ等に保管する場合には、セキュリティ上堅固な対策を施して実施する必要があるが、ＩＣカードを用いたマッチオンカード方式の場合には、本人一人分のテンプレートをＩＣカードの中に搭載しておけば、ＩＣカード本来の強固なセキュリティ機能を利用することにより、ＰＣ等のデータベースに多くの人数分のテンプレートを保管することなく簡単に利用することができる。

2. 調査･開発の概要

本調査・開発では、簡易認証システムを開発し、そのシステムについて評価を行った上で、様々な要件に関する課題を抽出する。

本章では、開発する簡易認証ステムの基本要件について述べる。

2. 1. 開発する簡易認証システムの基本要件

（1）暗証番号（またはＩＤ、パスワード）の代りに、指紋を用いて本人認証をすることができる。

（2）バイオメトリクス認証は、マッチオンカード方式とする。

（3）使用するＩＣカードは、ISO/IEC 14443-TypeB（接触部はオプション）を使用する。また、使用するカードは、ニューメディア開発協会の実装規約書「非接触型ＩＣカードの実装規約（第 2.0 版）」に準拠する。

（4）バイオメトリクスシステムの準拠規格としては、バイオメトリクス関連の最新の国際標準化動向（ISO/IEC JTC1 SC17、SC27、SC37 に関連するもの）を参照するものとする。

3. 調査用簡易認証システムの開発

本調査・開発を行うにあたり、調査用簡易認証システムとしてアプリケーションモデルの異なる二つのシステムを開発した。

本章では、各システムの概要と動作について述べる。

3. 1. 開発内容

株式会社日立製作所（以下「日立製作所」という。）が開発した帳票押印簡易システム（以下「システムＡ」という。）は、Microsoft Excel（以下「Excel」という。）の帳票に押印する際に指紋認証を利用するものである。

サイレックス・テクノロジー株式会社（以下「サイレックス・テクノロジー」という。）及びイデアコラボレーションズ株式会社（以下「IDEAC」という。）が開発した申請決裁簡易システム（以下「システムＢ」という。）は、クライアントサーバ型のアプリケーションであり、ＷＥＢブラウザを用いた申請書作成及び承認に指紋認証を用いるものである。

3. 2. システム構成の概要

システムＡ及びシステムＢの構成の概要は、以下のとおりである。

3. 2. 1. システムA

（1）ハードウェア構成

コンピュータ

- ノート型パソコン

ＩＣカード

- MULTOS カードのマッチオンカード方式ＩＣカード（利用者用）
- MULTOS カードの指紋登録時認証用ＩＣカード（管理者用）

ＩＣカードリーダライタ

- ISO/IEC 14443-TypeB 準拠ＩＣカードリーダライタ 2 台（認証用と登録用）

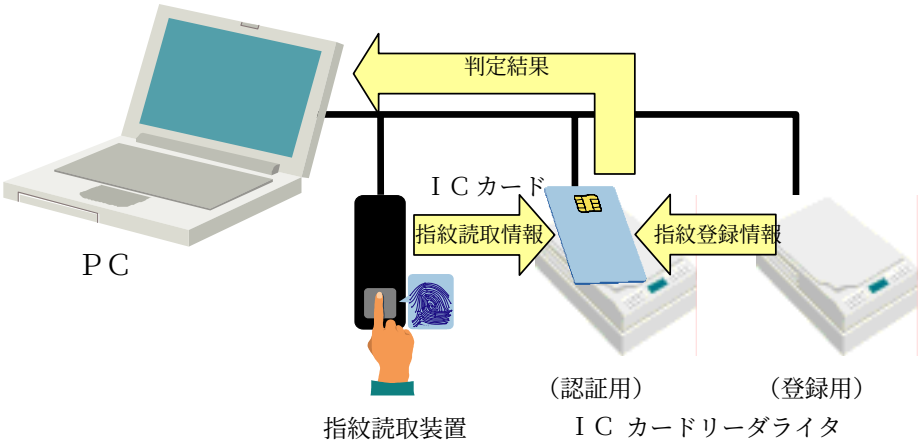
指紋読取装置

- ＵＳＢ接続型指紋読取装置

図表 3-1　ISO/IEC 14443-TypeB 準拠ＩＣカードリーダライタ（日立製作所製）

図表 3-2　ＵＳＢ接続型指紋読取装置（日立製作所製）

図表 3-3　システム A　ハードウェア構成



図表 3-4　システム A　ハードウェア構成図

（2）ソフトウェア構成

オペレーティングシステム

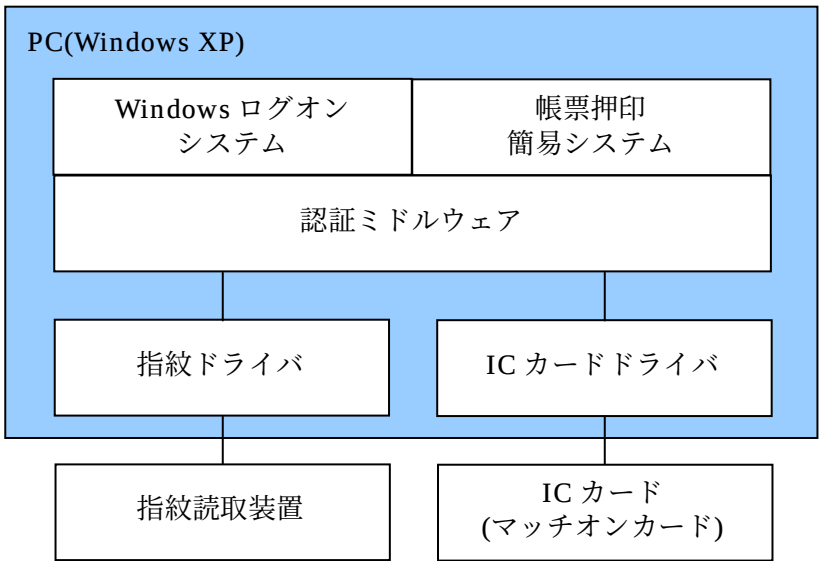
- Windows XP

指紋照合システム

- マッチオンカードシステム

その他前提ソフトウェア

- Microsoft Excel



図表 3-5　システム A　ソフトウェア構成図

3. 2. 2. システムB

（1）ハードウェア構成

コンピュータ

- ノート型パソコン

ＩＣカード

- Precise BioMatch ™ J、Precise BioManager ™ J、Precise IDStore ™ J を搭載した JavaCard のマッチオンカード方式ＩＣカード

ＩＣカードリーダライタ

- ISO/IEC 14443-TypeB 準拠のマッチオンカードリーダライタ

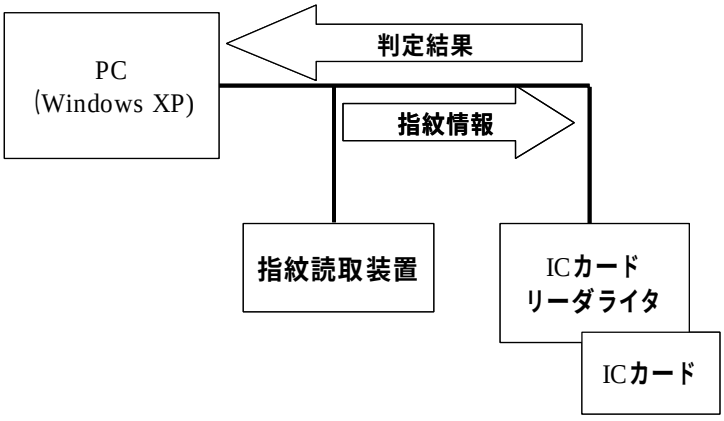
指紋読取装置

- Precise Match-on-Card ™ に対応するＵＳＢ接続型指紋読取装置

図表 3-6　ISO/IEC 14443-TypeB 準拠のマッチオンカードリーダライタ（シャープ製）

図表 3-7　Precise Match-on-Card ™に対応するＵＳＢ接続型指紋読取装置
（サイレックス・テクノロジー製）

図表 3-8　システム B　ハードウェア構成



図表 3-9　システム B　ハードウェア構成図

(2) ソフトウェア構成

オペレーティングシステム

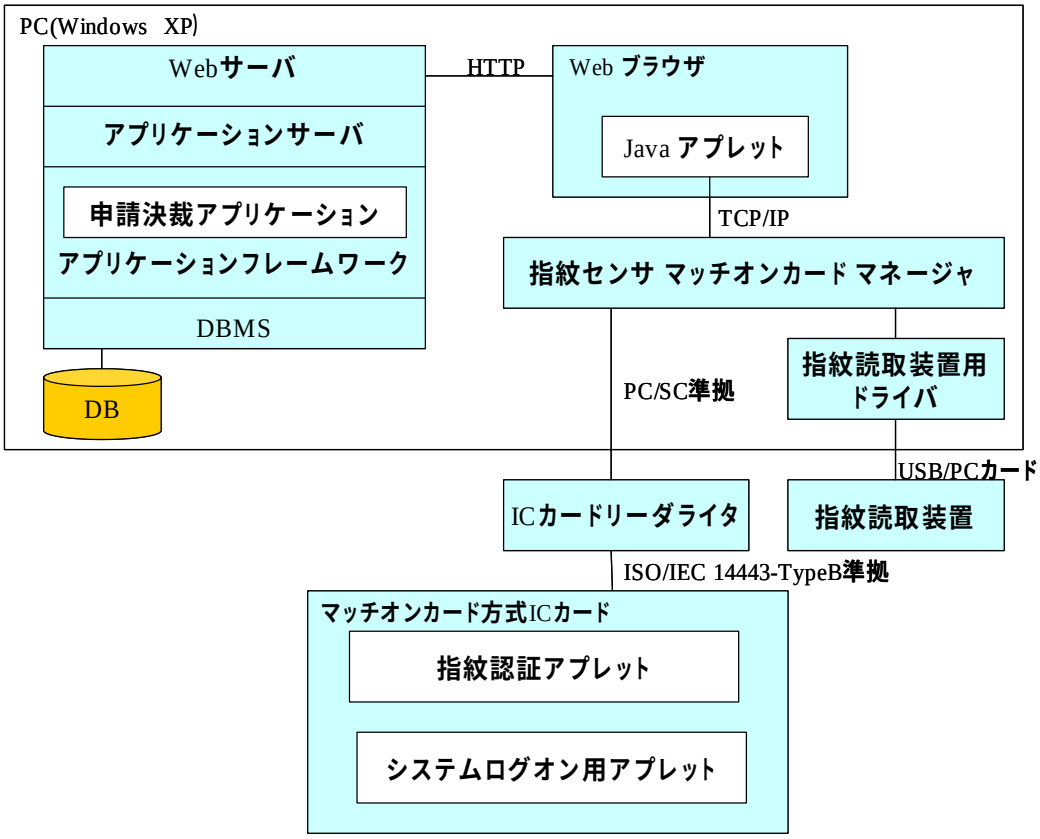
- Windows XP

指紋照合システム

- ドライバ: 指紋センサ用ドライバ
- ミドルウェア: Apache、Tomcat、IFW、PostgreSQL
- 指紋センサ　マッチオンカード　マネージャ

その他前提ソフトウェア

- システムプログラム: Java Plug-in
- ＷＥＢブラウザ: Internet Explorer
- 申請決裁アプリケーション



図表 3-10　システム B　ソフトウェア構成図

3. 3. 簡易認証システムの動作説明

システムＡ及びシステムＢの動作の概要は、以下のとおりである。

3. 3. 1. システムA

システムＡは、マッチオンカード方式の指紋照合により個人を特定し認証することで、Windows へのログオンや Excel で作成された帳票への承認・押印を行うシステムである。

本システムは、ＰＣに接続した指紋読取装置、ＩＣカードリーダライタ及び指紋データ等を登録したＩＣカードから構成される。本システムで用いるＰＣには Excel をインストールし、Excel で作成した帳票を利用する。

本人の指紋登録データは、テンプレートとして事前にＩＣカード内に登録する。認証時は、本人が持参したＩＣカードの中のテンプレートと、指紋読取装置から得た本人の指紋読取情報とを照合し、本人認証を行う。

Windows にログオンする際には、ＩＣカードリーダライタにＩＣカードを載せ、指紋照合することで認証を行う。指紋照合に失敗した場合は、Windows へのログオンは失敗する。

帳票への決済は、Excel で開いた帳票の押印欄に設置されたボタンをクリックすることで行う。ボタンをクリックすると、指紋照合のダイアログが表示され、指紋の読取りを促す。指紋照合に成功した場合は、帳票に押印され、通常の入力状態に戻る。指紋照合に失敗した場合は、暗証番号の入力ダイアログが表示され、暗証番号で認証されれば、指紋照合の認証成功時と同様に押印され、入力状態に戻る。

3. 3. 2. システムB

システムＢは、マッチオンカード方式の指紋照合により個人を特定し認証することで、ＷＥＢブラウザを用いて申請書の作成・承認を行うクライアントサーバ型のシステムである。

本人の指紋登録データはテンプレートとして事前にＩＣカードに搭載する。認証時は、本人が持参したＩＣカードの中のテンプレートと、指紋読取装置から得た本人の指紋読取情報とを照合し本人認証を行う。

本システムは、ＰＣに接続した指紋読取装置、ＩＣカードリーダライタ及び指紋データ等を登録したＩＣカードから構成される。また、本システムで用いるＰＣにはスタンドアロンで動作するＷＥＢサーバシステムをインストールし、調査用のＷＥＢアプリケーションである申請決裁アプリケーションが動作するようにする。申請決裁アプリケーションはＷＥＢブラウザを用いてＷＥＢサーバにアクセスして利用する。

申請決裁簡易アプリケーションは、ログオン、申請登録及び申請承認の各処理について、それぞれＩＣカード所持による認証、指紋もしくは暗証番号による認証、指紋

のみの認証、という3種類の異なるセキュリティレベルを持つ。

システムＢにログオンする際の認証は、ＩＣカードからシステムログオン用のＩＤとパスワードを読出し、そのＩＤとパスワードをサーバに送信してログオン認証を行い、ログオンしたユーザーの権限に応じて、申請登録、承認申請のそれぞれの機能を使用可能とする。

申請登録を行う際は、指紋もしくは暗証番号により認証を行う。指紋認証は、指紋読取装置から読み込まれた照合用の指紋データとＩＣカードに登録されたテンプレートとの照合により認証を行う。暗証番号による認証は、入力された暗証番号とICカードに登録された暗証番号との照合により認証を行う。認証が正しく行われた場合、画面から入力された申請データをデータベースに記録する。

申請の承認を行う際は、データベースに記録された申請データを選択表示し、指紋による認証を行った結果、認証が正しく行われた場合、データベース上にある申請データに承認データを付加して更新する。

4. 簡易認証システムの評価

本章では、システムＡ及びシステムＢの二つの調査用簡易認証システムを用いて行った評価について述べる。評価は、それぞれのシステムの仕様を確認し、課題の抽出、実運用時の所要時間の測定をテンプレートの登録、認証それぞれについて行った。

4. 1. 仕様

各調査用簡易認証システムの基本的な仕様を、図表 4-1 にまとめる。

図表 4-1　調査用簡易認証システム基本仕様

	システム A	システム B
カード OS	MULTOS	JavaCard
指紋登録数	2	2
認証方式	特徴点方式 (チップマッチング)	特徴点方式 （マニューシャ）
登録データ	Window ログオン ID / パスワード他	アプリケーション ID / パスワード、暗証番号他
インターフェイス	ISO/IEC 14443-TypeB	ISO/IEC 14443-TypeB
動作環境	Windows XP	Windows XP
アプリケーション	Microsoft Excel	Internet Explorer、 Web サーバ

4. 2. テンプレートの登録

以下に、システムＡ及びシステムＢの登録の仕様及び手順を示す。

4. 2. 1. テンプレート登録の仕様

マッチオンカードに登録するテンプレートの形式にはいくつかの方式があるが、代表的なテンプレートの方式に特徴点方式が挙げられる。特徴点方式は指紋の画像から指紋の端点や分岐点といった特徴点を抽出してテンプレートを作成するという方式であり、指紋画像に比べデータ量が少なく、特徴点から元の指紋画像を生成する可逆性がないという特徴を備えている。

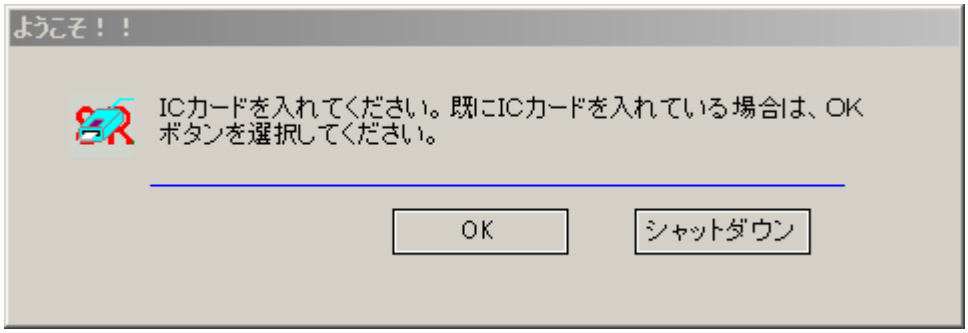
マッチオンカードに登録するテンプレートは、利用者が登録した指に怪我を負ったり体調等の理由から認証に失敗したりする可能性を考慮し、通常 2 指以上のテンプレートを登録可能としている。2 指以上のテンプレートを登録した場合には、各テンプレートとの認証を順番に試みるようにすることができる。

4. 2. 2. テンプレートの登録手順

＜システムA＞

(1) ＩＣカードのセット

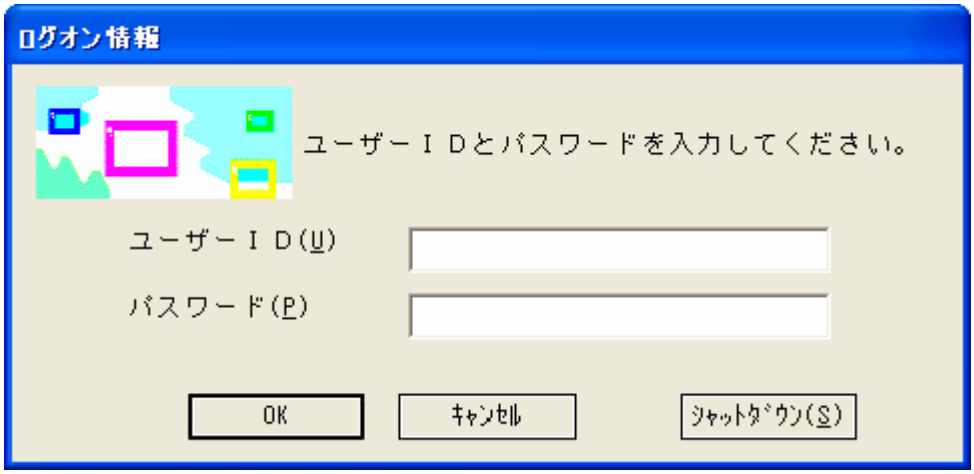
パソコンを起動し、ようこそ画面（図表 4-2）が表示されたら、ログオン用に設定したＩＣカードリーダライタに管理者用カードをセットする。カードをセットしてもようこそ画面が表示され続けている場合は、画面の[OK]ボタンをクリックする。



図表 4-2　ようこそ画面

(2) ユーザーＩＤ、パスワードの入力

ログオン情報画面のユーザーＩＤ、パスワード入力欄に入力し、[OK]ボタンをクリックする。入力された情報が正しければ Windows のデスクトップが表示される。



図表 4-3　ログオン情報画面

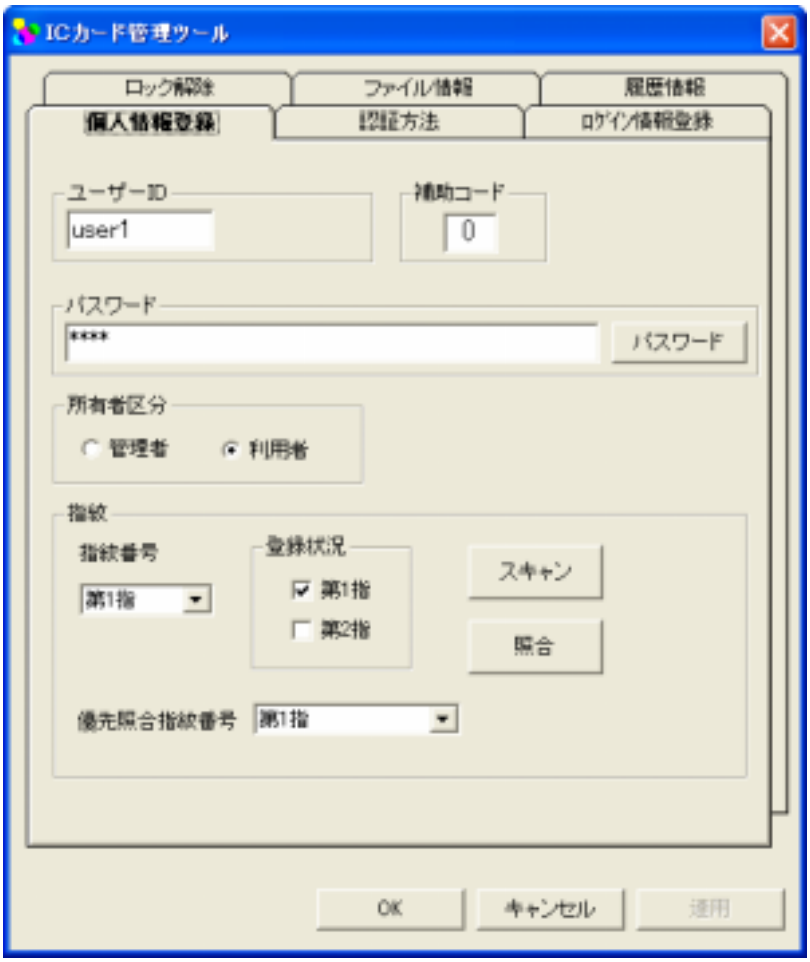
(3) セキュアバイオロック管理ツールの起動

セキュアバイオロック管理ツールを起動してカード要求画面（図表 4-4）が表示されたら、管理ツール用に設定されているＩＣカードリーダライタに指紋登録を行う利用者用カードをセットする。カードをセットしても画面が切り替わらない場合は、[OK]ボタンをクリックする。

図表 4-4　カード要求画面

（4）個人情報の設定

[個人情報登録]タブを選択し、個人情報登録画面（図表 4-5）を表示させる。ＩＣカードで固有となるようにユーザーＩＤ／パスワード／補助コードを入力する。所有者区分は利用者を選択する。

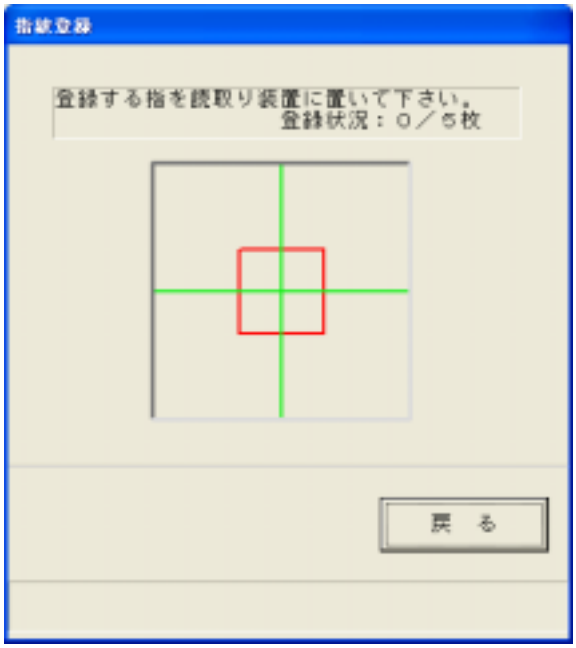


図表 4-5　個人情報登録画面

（5）指紋登録

個人情報登録画面（図表 4-5）左下の指紋番号から第 1 指または第 2 指を選択して、[スキャン]ボタンをクリックすると指紋読取画面（図表 4-6）が表示される。画面の指示に従って、指紋読取装置に指を置く（図表 4-7）。その後、画面の指示に従い、いったん指を離して、指紋読取装置に指を置き直す。指紋読取りは 5 回行なわれ、指紋登録に成功すると、個人情報登録画面の登録状況にチェックが付く。

同様に[照合]ボタンをクリックすると、登録済みの指紋情報で正しく指紋認証できるかを確認することができる。



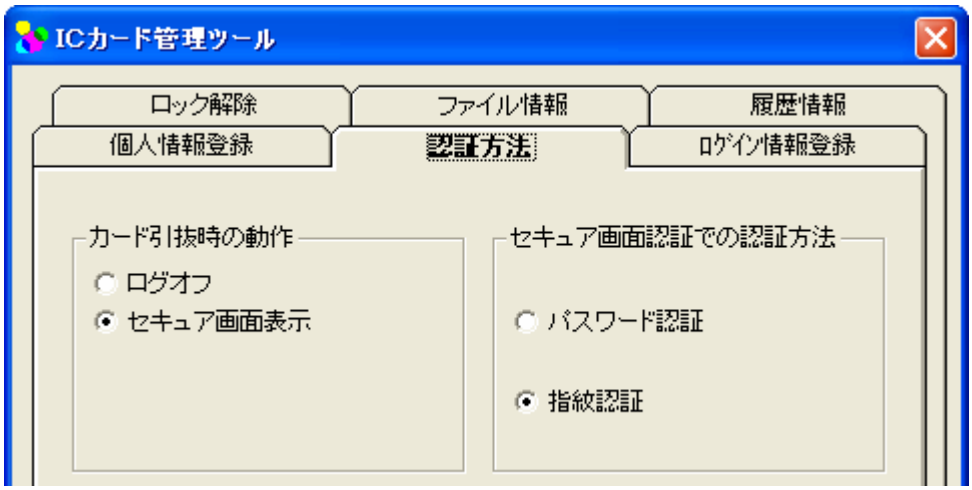
図表 4-6　指紋読取画面

図表 4-7　指紋読取装置に指を置く

（6）認証方法の設定

[認証方法]タブを選択し、認証方法設定画面（図表 4-8）を表示させる。帳票押印機能を使用する場合はカード引抜時の動作に「セキュア画面表示」を、セキュア画面認証での認証方法に「指紋認証」を、それぞれ選択する。これ以外の組み合わせでは、帳票押印機能が正しく動作しない。

上記以外の組み合わせにしてしまった場合、本機能で正しい組み合わせに設定し直す。



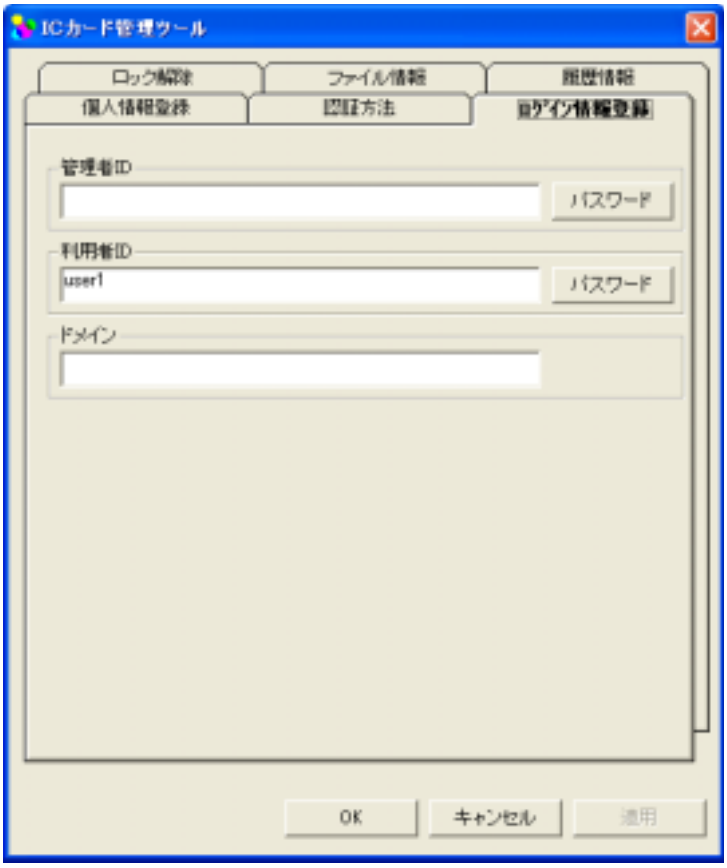
図表 4-8　認証方法設定画面

(7) ログオン情報の登録

[ログオン情報登録]タブを選択し、ログオン情報登録画面（図表 4-9）を表示させる。画面中段の利用者ＩＤに Windows に設定されたユーザーＩＤを入力し、その右側にある[パスワード]ボタンをクリックして Windows に設定されたパスワードを入力する。

本機能では、Windows にログオンするためのアカウント情報を設定する。ここで誤った情報を登録してしまうと指紋認証が成功しても Windows へログオンすることができなくなる。

Windows でアカウント情報（ユーザーＩＤやパスワード）を変更した場合、本機能を使用して新しい情報に更新する。新しい情報に更新しないと、指紋認証が成功しても Windows へログオンすることができなくなる。



図表 4-9　ログオン情報登録画面

(8) 入力情報の確定

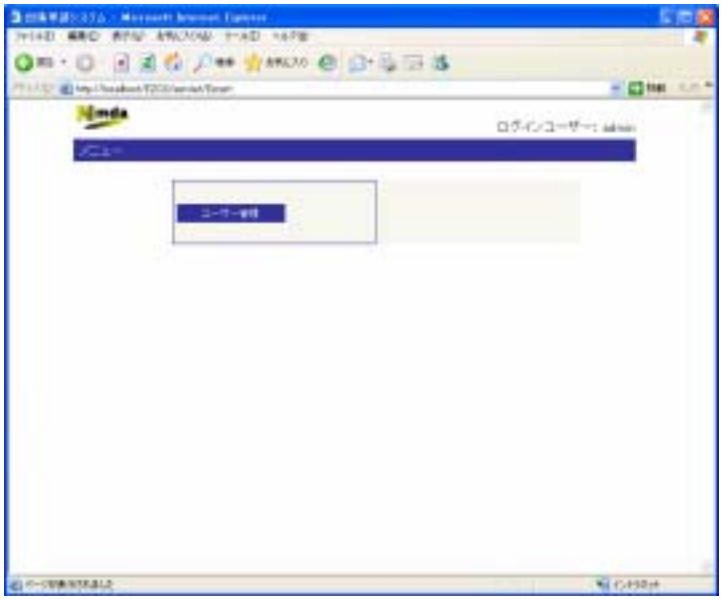
画面下の[OK]ボタンをクリックすると、入力された情報をＩＣカードに書き込む。

指紋情報は、この操作に関わらず、登録処理が完了した時点で利用者カードに格納される。

＜システムB＞

（1）管理者メニューへのログオン

ＩＣカードリーダに管理者カードを置く。カードを置くと、自動的に申請決裁簡易システムに管理者メニュー画面が表示される（図表 4-10）。



図表 4-10　管理者メニュー画面

（2）ユーザー管理画面の選択

管理者メニュー画面の［ユーザー管理］ボタン（図表 4-11）をクリックする。

図表 4-11　［ユーザー管理］ボタン

(3) ユーザーの新規登録

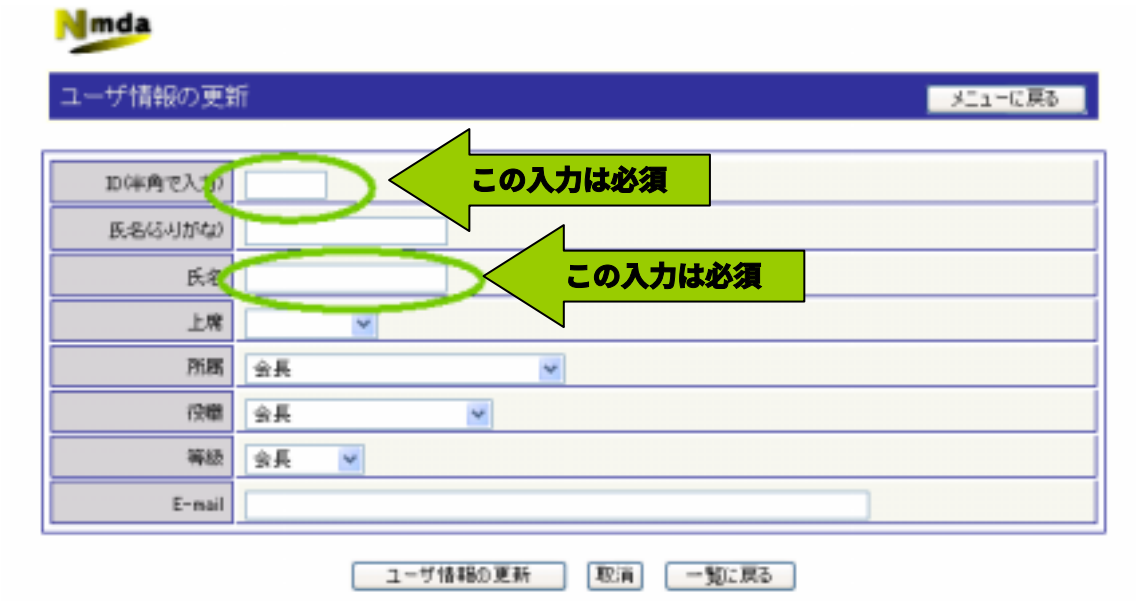
［新規登録］ボタンをクリックする（図表 4-12）。

図表 4-12　［新規登録］ボタン

(4) ユーザー情報の登録

ユーザー情報を入力する。

※「ＩＤ」と「氏名」を入力すると、その他の欄が空欄でも次画面へ進むことができる（図表 4-13）。



図表 4-13　ユーザー情報の入力画面

ＩＤ：半角数字 8 桁を入力する。

氏名（ふりがな）：氏名のふりがなを入力する。

氏名：氏名を入力する。

上席：事前に登録されている上席の中から、直属の上席を選択する。（プルダウン式）
※上席が空欄の場合は、上席がいないことになる。
所属：所属を選択する。（プルダウン式）
役職：役職を選択する。（プルダウン式）
等級：等級を選択する。（プルダウン式）
Email：Email アドレスを入力する。

(5) ユーザー情報の更新完了

画面左方の［ユーザー情報の更新］ボタンをクリックし、ユーザー情報を登録する。

(6) 指紋情報及び暗証番号を更新するＩＣカードの決定

ＩＣカードリーダに、指紋情報及び暗証番号を更新するＩＣカード（申請者カードまたは承認者カード）を置く。

※申請者カードとは、「申請を承認する権限を持たないユーザー情報を登録したカード」を指す。他のユーザーがユーザー情報を新規登録・更新する際に、「上席」として選択しなかったユーザーのカードは、申請者カードとなる。

※承認者カードとは、「申請を承認する権限を持つユーザー情報を登録したカード」を指す。他のユーザーがユーザー情報を新規登録・更新する際に、「上席」として選択したユーザーのカードは、承認者カードとなる。

(7) 指紋情報及び暗証番号の更新画面へのログオン

［ユーザー管理］ボタンをクリックする。

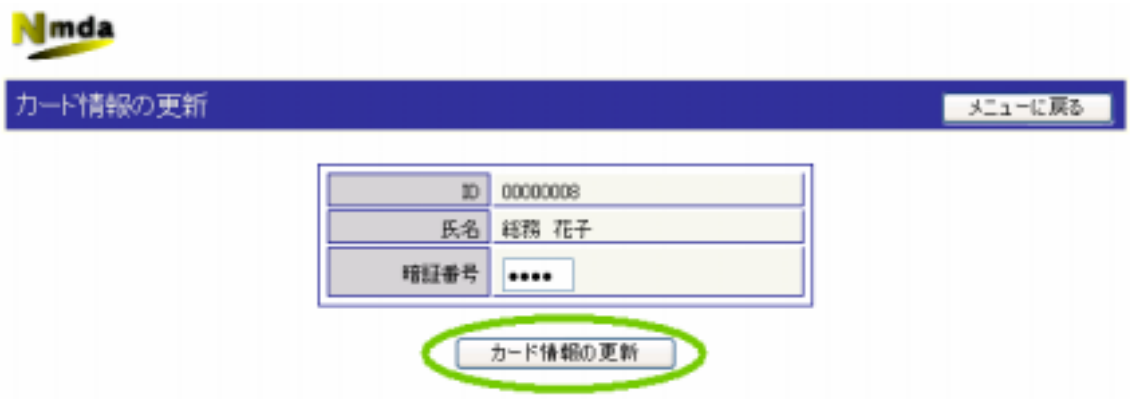
（8）指紋情報及び暗証番号を更新するユーザーの選択

指紋情報及び暗証番号を更新するユーザーを選択し、[カード情報] ボタンをクリックする（図表 4-14)。

図表 4-14　［カード情報］ボタン

（9）暗証番号の更新

半角数字で 4 桁の暗証番号を入力し、[カード情報の更新] ボタンをクリックする（図表 4-15)。

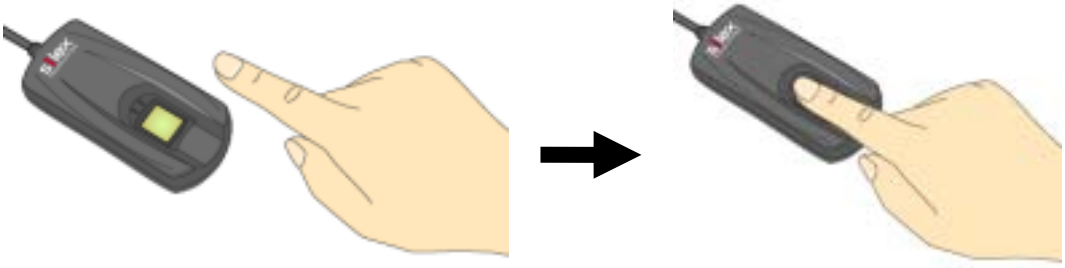


図表 4-15　［カード情報の更新］ボタン

（10）指紋情報の更新

画面下方に表示される案内に従い、指紋読取装置に指を置く（図表 4-16）。「指紋リーダから指を離してください」という案内に従い、いったん指を離し、指紋読取装置に指を置き直す。

※指紋の読取は、2 回行う。



図表 4-16　指紋情報の読取

画面下方に、読取った指紋情報の品質が表示される。品質が 50 以上（最大 100）であれば、テンプレートが作成されＩＣカード（申請者カードまたは承認者カード）の指紋情報及び暗証番号が更新される（図表 4-17）。

品質が 50 以下の場合は、画面下方に表示される案内に従い、もう一度指紋読取装置に指を置く。

図表 4-17　指紋情報の品質が 50 以上の場合

（11）指紋情報の更新の成功

指定したＩＣカード（申請者カードまたは承認者カード）の指紋情報及び暗証番号が更新されると、「カード情報を更新しました」というダイアログボックスが表示される（図表 4-18）。

図表 4-18　カード情報の更新の完了

（12）指紋情報の更新の失敗

指紋情報の更新に失敗すると、「カード情報は更新されませんでした」というダイアログボックスが表示される（図表 4-19）。［OK］ボタンをクリックしてユーザー一覧画面へ戻る。

［カード情報の更新］ボタンをクリックし、もう一度、上記（9）からの操作を行う。

図 4-19　カード情報の更新の失敗

4. 2. 3. テンプレート登録時の所要時間

マッチオンカード方式の指紋認証では、あらかじめＩＣカードにカード利用者の指紋をテンプレートとして登録しておく。

テンプレートの登録は通常一度行うだけである。しかし、登録は認証とは異なった条件のもとで行われるため、利用者にとってある程度の負担を伴うことになる。利用者は、登録にどの程度の時間がかかるかをあらかじめ知っておくと心理的な負担を軽減できる。またシステム管理者は、一人一人にかかる登録時間の目安が分かることで、多数の利用者に登録してもらう際に要する時間を把握することができ、計画をたてやすくなる。

そこで、以下に本調査・開発で開発したシステムＡ、システムＢのそれぞれの指紋登録に要する時間を計測しまとめる。ただし、システムＡ、システムＢはそれぞれの登録の仕様が異なるため、各システムの登録に要する時間の比較は行わないものとする。登録仕様の違いは以下のとおりである。

- 指紋のスキャン回数　：システムＡ　5 回、システムＢ　2 回
- 登録アプリケーション：システムＡ　専用管理ツール、システムＢ　ＷＥＢアプリケーション

ここでは、それぞれのシステムにおける登録に要する時間を利用者がどのように感じるか、また客観的にどの程度の時間を要するのかを計ることが目的である。

所要時間の計測方式を以下に説明する。計測は被験者毎に登録、認証の順に行うため、ここでは、登録時だけでなく認証時の所要時間の計測方法もまとめて記載する。

＜計測方法＞

(1) 計測員は、計測を始めるにあたり、被験者に計測の手順を記載したメモ（添付資料 8「簡易認証システムの調査にご協力ください」）を渡し、所要時間を計測する趣旨を説明する。

(2) 被験者は、システムＡの指紋登録を何度か行って慣れた後、システムＡの認証を練習する。

(3) 被験者は、システムＢの指紋登録を何度か行って慣れた後、システムＢの認証を練習する。

(4) 計測員は、被験者一人毎にシステムＡ、システムＢの順番を変え、下記の（5）以降の手順で所要時間を計測する。

登録時の所要時間計測

（5）登録時の所要時間を計測員 2 名がストップウォッチを用いて計測する。なお、図表 4-20 には、計測員 1 及び計測員 2 としてそれぞれ示した。

（6）計測員は、被験者が指紋読取装置に指を置くと同時に声で合図した時から計測を開始し、画面に認証終了ダイアログが出た瞬間までを計測する。

（7）エラーが出た場合には、その回の登録に要した時間を計測しない。ただし、10 回の正常なテンプレート登録が終了するまでの間に発生したエラーの回数をカウントする。

認証時の所要時間計測

（8）認証時の所要時間を計測員 2 名がストップウォッチを用いて計測する。なお、図表 4-45 には、計測員 1 及び計測員 2 としてそれぞれ示した。

（9）計測員は、被験者が指紋読取装置に指を置くと同時に声で合図した時から計測を開始し、画面に認証終了ダイアログが出た瞬間までを計測する。

（10）エラーが出た場合には、その回の認証に要した時間を計測しない。ただし、10 回の正常な認証が終了するまでの間に発生したエラーの回数をカウントする。

（11）システムＡ、システムＢの登録、認証の所要時間を計測し終わった後、図表 4-46 のアンケートを実施する。

図表 4-20　テンプレート登録時の所要時間測定結果

被験者1

単位:秒

	システムA（計測員1）	システムA（計測員2）	平均
1回目	17.93	18.03	17.98
2回目	18.94	18.97	18.96
3回目	16.93	16.63	16.78
4回目	16.39	16.69	16.54
5回目	16.77	17.41	17.09
6回目	17.22	16.59	16.91
7回目	17.71	17.83	17.77
8回目	16.91	16.68	16.80
9回目	18.89	16.00	17.45
10回目	16.08	16.06	16.07
平均	17.38	17.09	17.23

失敗回数　無計測

	システムB（計測員1）	システムB（計測員2）	平均
1回目	6.68	6.94	6.81
2回目	6.81	6.63	6.72
3回目	6.29	6.10	6.20
4回目	6.26	5.98	6.12
5回目	5.91	5.76	5.84
6回目	6.04	6.12	6.08
7回目	6.13	6.10	6.12
8回目	6.04	6.22	6.13
9回目	5.96	5.84	5.90
10回目	6.33	6.19	6.26
平均	6.25	6.19	6.22

失敗回数　無計測

被験者2

	システムB（計測員1）	システムB（計測員2）	平均
1回目	18.37	18.38	18.38
2回目	17.29	17.16	17.23
3回目	14.80	14.81	14.81
4回目	12.35	12.31	12.33
5回目	12.86	12.89	12.88
6回目	15.98	15.82	15.90
7回目	15.36	15.38	15.37
8回目	11.69	11.60	11.65
9回目	14.73	14.80	14.77
10回目	16.87	16.89	16.88
平均	15.03	15.00	15.02

失敗回数　0回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	8.55	8.59	8.57
2回目	6.37	6.41	6.39
3回目	5.74	5.61	5.68
4回目	5.85	5.70	5.78
5回目	8.48	8.38	8.43
6回目	6.40	6.35	6.38
7回目	6.45	6.36	6.41
8回目	5.86	5.88	5.87
9回目	5.85	5.86	5.86
10回目	7.06	6.87	6.97
平均	6.66	6.60	6.63

失敗回数　0回

被験者3

	システムA（計測員1）	システムA（計測員2）	平均
1回目	16.25	16.14	16.20
2回目	15.49	15.40	15.45
3回目	15.31	15.16	15.24
4回目	13.15	12.93	13.04
5回目	12.90	12.79	12.85
6回目	12.62	12.65	12.64
7回目	11.90	11.80	11.85
8回目	10.80	10.67	10.74
9回目	11.21	11.09	11.15
10回目	10.12	10.29	10.21
平均	12.98	12.89	12.93

失敗回数　0回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	5.41	5.48	5.45
2回目	9.57	9.57	9.57
3回目	6.95	6.99	6.97
4回目	8.89	9.01	8.95
5回目	6.35	6.30	6.33
6回目	7.50	7.38	7.44
7回目	6.61	6.60	6.61
8回目	6.65	6.33	6.49
9回目	7.68	7.67	7.68
10回目	7.68	7.52	7.60
平均	7.33	7.29	7.31

失敗回数　0回

被験者4

	システムB（計測員1）	システムB（計測員2）	平均
1回目	11.97	11.82	11.90
2回目	11.77	11.57	11.67
3回目	11.41	11.45	11.43
4回目	12.20	12.02	12.11
5回目	10.85	10.90	10.88
6回目	11.66	11.48	11.57
7回目	11.40	11.53	11.47
8回目	11.71	11.49	11.60
9回目	11.86	12.06	11.96
10回目	11.50	11.38	11.44
平均	11.63	11.57	11.60

失敗回数　0回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	6.16	6.18	6.17
2回目	5.58	5.46	5.52
3回目	6.11	5.96	6.04
4回目	5.47	5.51	5.49
5回目	6.89	6.70	6.80
6回目	5.72	5.62	5.67
7回目	5.17	4.89	5.03
8回目	5.95	5.88	5.92
9回目	5.72	5.71	5.72
10回目	5.50	5.57	5.54
平均	5.83	5.75	5.79

失敗回数　0回

被験者5

	システムA（計測員1）	システムA（計測員2）	平均
1回目	25.28	25.32	25.30
2回目	25.51	25.53	25.52
3回目	24.15	23.97	24.06
4回目	25.24	24.96	25.10
5回目	23.77	23.81	23.79
6回目	23.92	23.91	23.92
7回目	24.61	24.52	24.57
8回目	25.36	25.24	25.30
9回目	23.26	23.22	23.24
10回目	23.36	23.28	23.32
平均	24.45	24.38	24.41

失敗回数　1回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	6.68	7.04	6.86
2回目	7.65	7.62	7.64
3回目	7.46	7.46	7.46
4回目	8.37	8.41	8.39
5回目	7.28	7.43	7.36
6回目	7.62	7.69	7.66
7回目	7.20	7.26	7.23
8回目	6.54	6.54	6.54
9回目	7.17	6.93	7.05
10回目	6.98	6.75	6.87
平均	7.30	7.31	7.30

失敗回数　0回

被験者6

	システムB（計測員1）	システムB（計測員2）	平均
1回目	17.98	18.08	18.03
2回目	17.75	17.55	17.65
3回目	19.11	19.14	19.13
4回目	18.51	18.06	18.29
5回目	18.50	18.61	18.56
6回目	18.56	19.00	18.78
7回目	18.91	18.85	18.88
8回目	18.66	18.65	18.66
9回目	17.56	17.48	17.52
10回目	18.45	18.86	18.66
平均	18.40	18.43	18.41

失敗回数　0回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	6.38	6.36	6.37
2回目	6.08	6.08	6.08
3回目	5.60	6.06	5.83
4回目	7.07	7.00	7.04
5回目	6.46	6.42	6.44
6回目	5.91	5.97	5.94
7回目	6.21	6.18	6.20
8回目	6.25	6.27	6.26
9回目	5.71	5.66	5.69
10回目	5.60	5.71	5.66
平均	6.13	6.17	6.15

失敗回数　0回

被験者7

	システムA（計測員1）	システムA（計測員2）	平均
1回目	16.22	16.35	16.29
2回目	15.69	15.72	15.71
3回目	16.48	16.14	16.31
4回目	14.08	14.32	14.20
5回目	13.55	13.80	13.68
6回目	12.89	12.93	12.91
7回目	14.42	14.50	14.46
8回目	13.28	13.62	13.45
9回目	12.79	12.93	12.86
10回目	13.09	13.00	13.05
平均	14.25	14.33	14.29

失敗回数　5回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	8.70	8.76	8.73
2回目	5.28	5.37	5.33
3回目	6.87	7.10	6.99
4回目	4.97	5.06	5.02
5回目	5.20	5.10	5.15
6回目	5.11	5.20	5.16
7回目	5.19	5.20	5.20
8回目	5.35	5.22	5.29
9回目	6.71	6.65	6.68
10回目	5.31	5.24	5.28
平均	5.87	5.89	5.88

失敗回数　0回

被験者8

	システムB（計測員1）	システムB（計測員2）	平均
1回目	12.97	13.20	13.09
2回目	16.48	16.76	16.62
3回目	13.15	13.26	13.21
4回目	14.11	14.30	14.21
5回目	14.17	14.38	14.28
6回目	13.57	13.86	13.72
7回目	12.55	12.35	12.45
8回目	14.88	14.80	14.84
9回目	16.69	16.81	16.75
10回目	14.32	14.43	14.38
平均	14.29	14.42	14.35

失敗回数　4回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	6.26	6.36	6.31
2回目	12.86	12.89	12.88
3回目	10.55	10.74	10.65
4回目	7.22	7.14	7.18
5回目	8.15	8.12	8.14
6回目	6.88	6.87	6.88
7回目	6.22	6.43	6.33
8回目	7.33	7.42	7.38
9回目	8.57	8.62	8.60
10回目	7.10	7.30	7.20
平均	8.11	8.19	8.15

失敗回数　0回

4. 3. 指紋の認証

以下に、システムＡ及びシステムＢの指紋認証の方式及び手順を示す。

4. 3. 1. 認証の方式

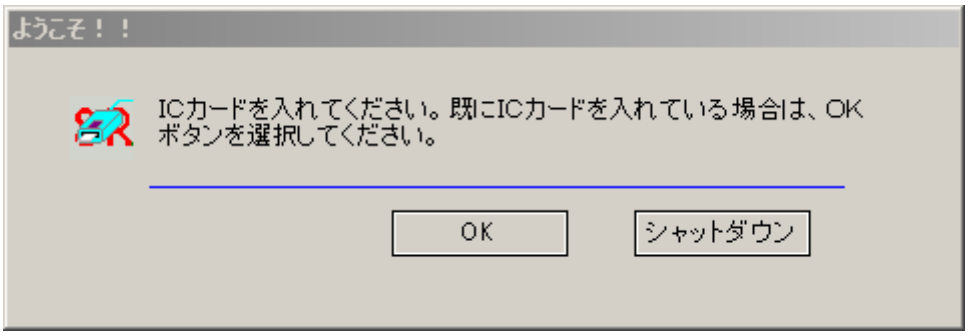
マッチオンカードによる指紋の認証は、指紋読取装置で読取った指紋情報から特徴点を抽出して参照データを作成し、この参照データをマッチオンカードにあらかじめ登録しておいたテンプレートとカード内で照合することにより行われる。

4. 3. 2. 認証の手順

＜システム A＞

（1）ＩＣカードのセット

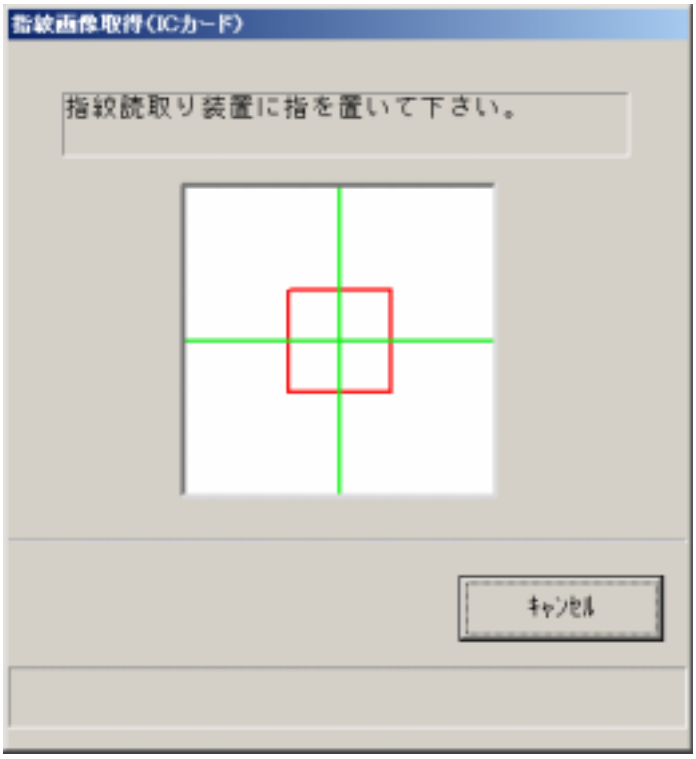
パソコンを起動し、ようこそ画面（図表 4-21）が表示されたら、ログオン用に設定したＩＣカードリーダライタに利用者用カードをセットする。カードをセットしてもようこそ画面が表示され続けている場合は、画面の[OK]ボタンをクリックする。



図表 4-21　ようこそ画面

(2) 指紋スキャン

指紋認証画面（図 4-22）が表示されるので、画面の指示に従い指紋読取装置に指を置く。正常にスキャンできると画面上に指紋が表示される。指紋認証に成功すると Windows のデスクトップ画面が表示される。



図表 4-22　指紋認証画面

(3) サンプル帳票の起動

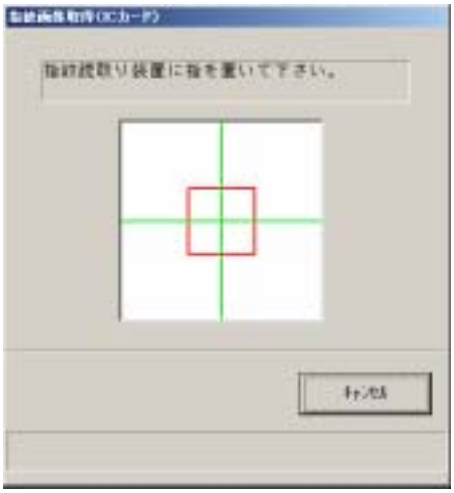
サンプル帳票(帳票押印サンプル帳票_デモ用記入済み)をダブルクリックして開く。

図表 4-23　サンプル帳票の起動

（4）承認処理の開始

記載内容を確認して、承認欄にある[押印]ボタンをクリックする（図表 4-24)。クリックすると指紋承認画面（図表 4-25）が表示される。

図表 4-24　サンプル帳票(押印前)



図表 4-25　指紋認証画面

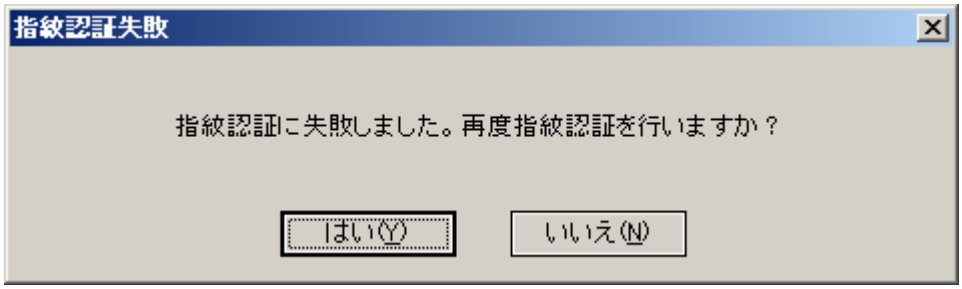
(5) 指紋による承認

ＰＣログオンと同様の手順で指紋スキャンし、指紋認証に成功すると承認欄に押印される（図表 4-26)。

図表 4-26　サンプル帳票(押印後)

(6) 指紋認証の失敗

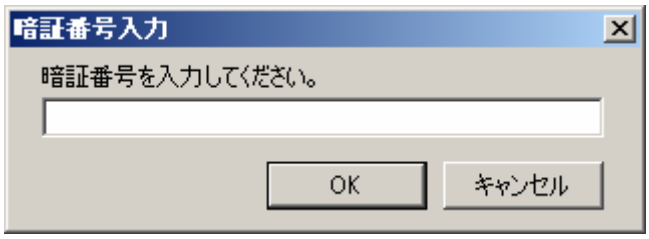
指紋照合に失敗すると、指紋認証失敗ダイアログ（図表 4-27）が表示される。ここで[はい（Y）]ボタンをクリックすると再度指紋認証を行うことができ、[いいえ（N）]ボタンをクリックすると暗証番号による承認処理へ移行する。



図表 4-27　指紋認証失敗ダイアログ

（7）暗証番号による承認

指紋照合に 3 回失敗するか、または指紋照合画面（図表 4-25）で[キャンセル]ボタンをクリックするか、指紋認証失敗ダイアログ（図表 4-27）で[いいえ（N）]ボタンをクリックした場合、暗証番号入力ダイアログ（図表 4-28）が表示される。暗証番号が一致すると承認欄に押印される。



図表 4-28 暗証番号入力ダイアログ

＜システムB＞

システムＢは、申請者が申請書を提出する場合、そして承認者が出張申請書を承認する場合の二通りの認証手順がある。ここでは、まず申請者が申請書を提出する場合について述べ、次いで承認者が出張申請書を承認する場合の手順を述べる。

申請者が申請書を提出する場合

（1）申請者メニューへのログオン

ＩＣカードリーダに申請者カードを置く。カードを置くと、自動的に申請者メニュー画面が表示される（図表 4-29）。

図表 4-29　申請者メニュー画面

(2) 出張申請書の作成

［出張申請書登録］ボタンをクリックする（図表 4-30）。

図表 4-30　［出張申請書登録］ボタン

(3) 出張内容の入力

出張内容を入力し、［確認］ボタンをクリックする（図表 4-31）。

※日程のみを入力すると、その他の欄が空欄でも次画面に進むことができる。

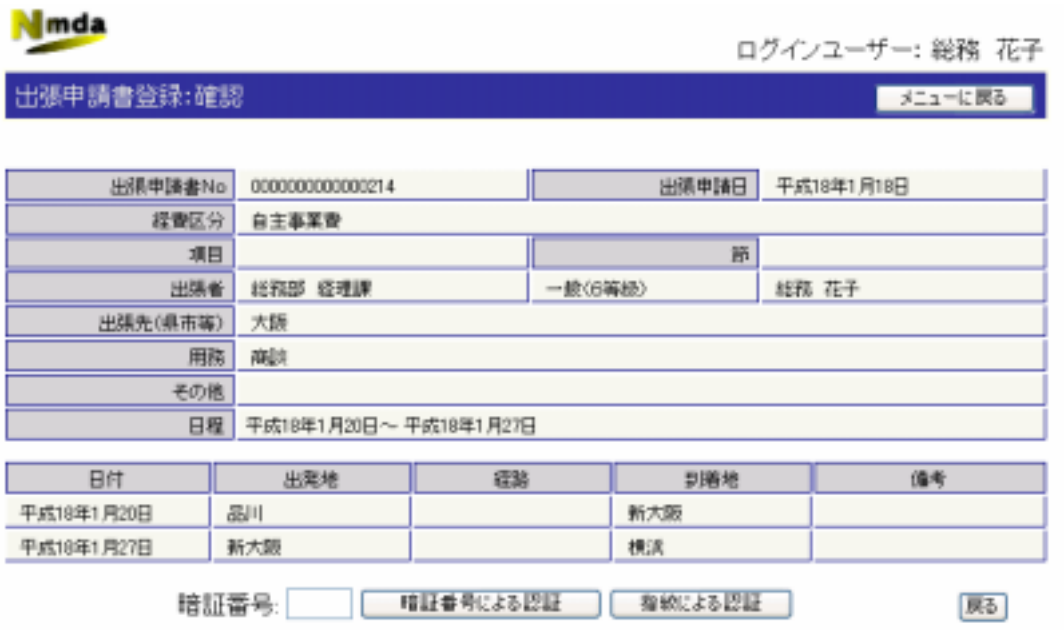
図表 4-31　出張内容の入力画面

（4）記入内容の確認

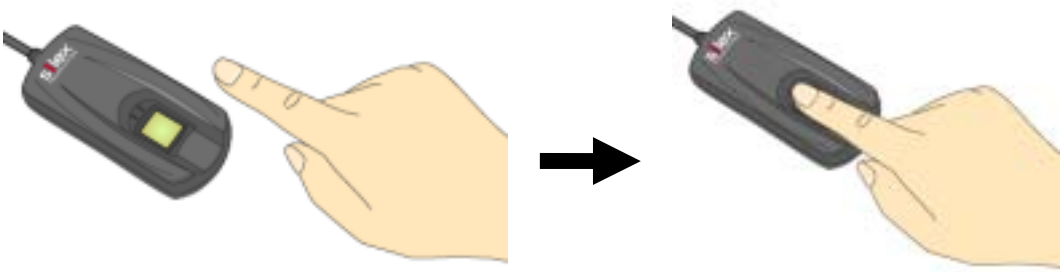
記入内容を確認し、申請を行う（図表 4-32）。

指紋で申請する場合は、[指紋による認証] ボタンをクリックして指紋読取装置に指を置く（図表 4-33）。

暗証番号で申請する場合は、暗証番号を入力してから［暗証番号による認証］ボタンをクリックする。



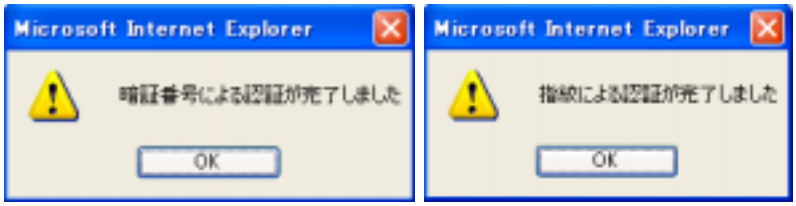
図表 4-32　申請登録画面（例）



図表 4-33　指紋の認証

（5）認証の成功

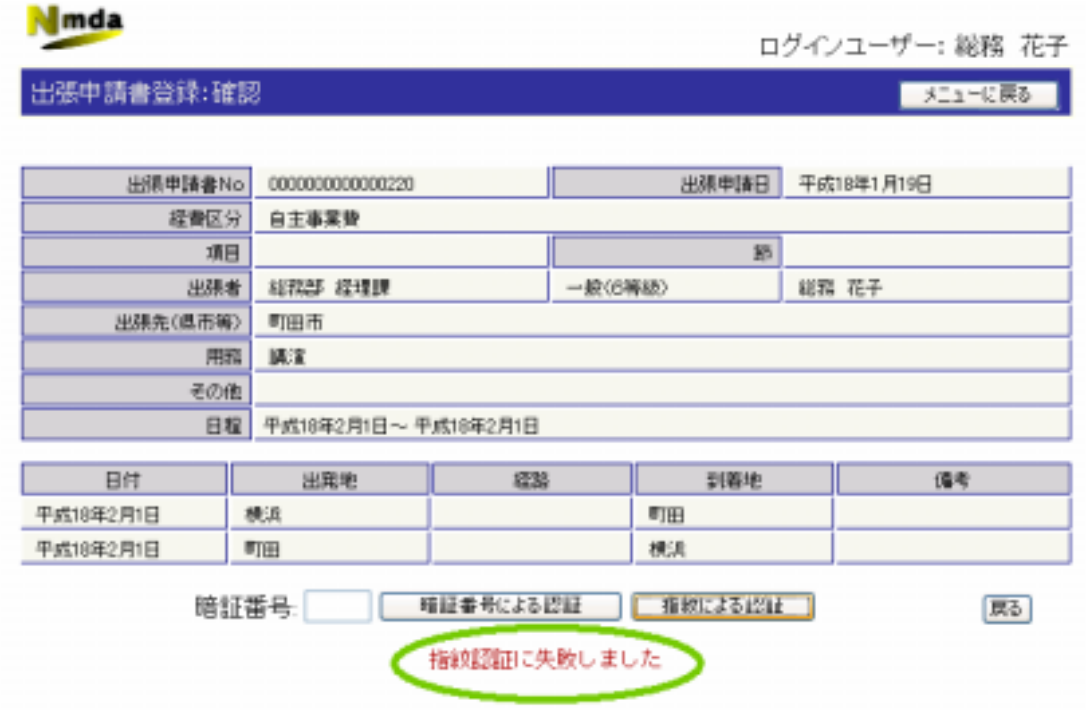
指紋の認証または暗証番号の認証に成功すると、認証が成功し申請が完了したことを示すダイアログボックスが表示される（図表 4-34）。



図表 4-34　出張申請の完了

（6）認証の失敗

指紋の認証に失敗した場合は、画面下方に「指紋認証に失敗しました」と表示される（図表 4-35）。いったん指を離し、指紋読取装置に指を置き直す。



図表 4-35　指紋の認証の失敗画面（例）

（7）認証の失敗

暗証番号の認証に失敗した場合は、「暗証番号が、間違っています」と表示される。もう一度暗証番号を入力し、[暗証番号による認証]ボタンをクリックする（図表 4-36）。

図表 4-36　暗証番号の認証の失敗画面（例）

（8）連続して認証に失敗した場合の注意事項

4 回連続して指紋の認証に失敗すると、「指紋認証に失敗しました」というダイアログボックスが表示される（図表 4-37）。

引き続き申請をする場合は、[OK] ボタンをクリックし、[暗証番号による認証] ボタンまたは [指紋による認証] ボタンをクリックする。

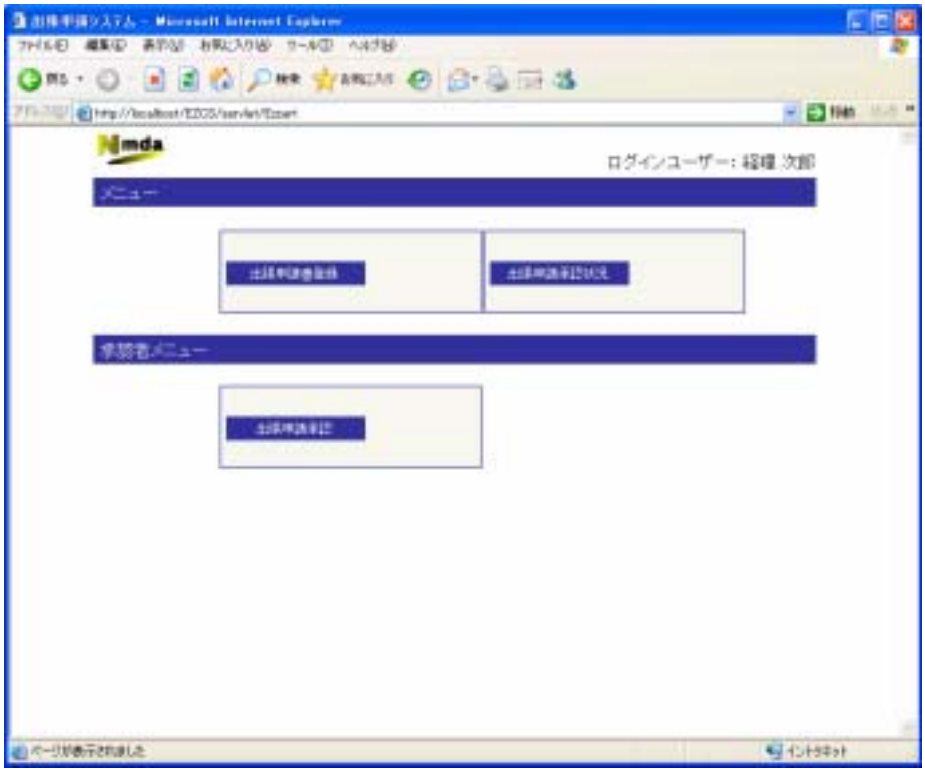
※10 回連続して失敗すると、ＩＣカードがロックされる。

図表 4-37　指紋認証の失敗

承認者が出張申請書を承認する場合

（1）承認者メニューへのログオン

ＩＣカードリーダに承認者カードを置く。カードを置くと、自動的に承認者メニュー画面が表示される（図表 4-38)。



図表 4-38　承認者メニュー画面

(2) 承認画面の表示

［出張申請承認］ボタンをクリックする（図表 4-39)。

図表 4-39　［出張申請承認］ボタン

(3) 承認する出張申請書の選択

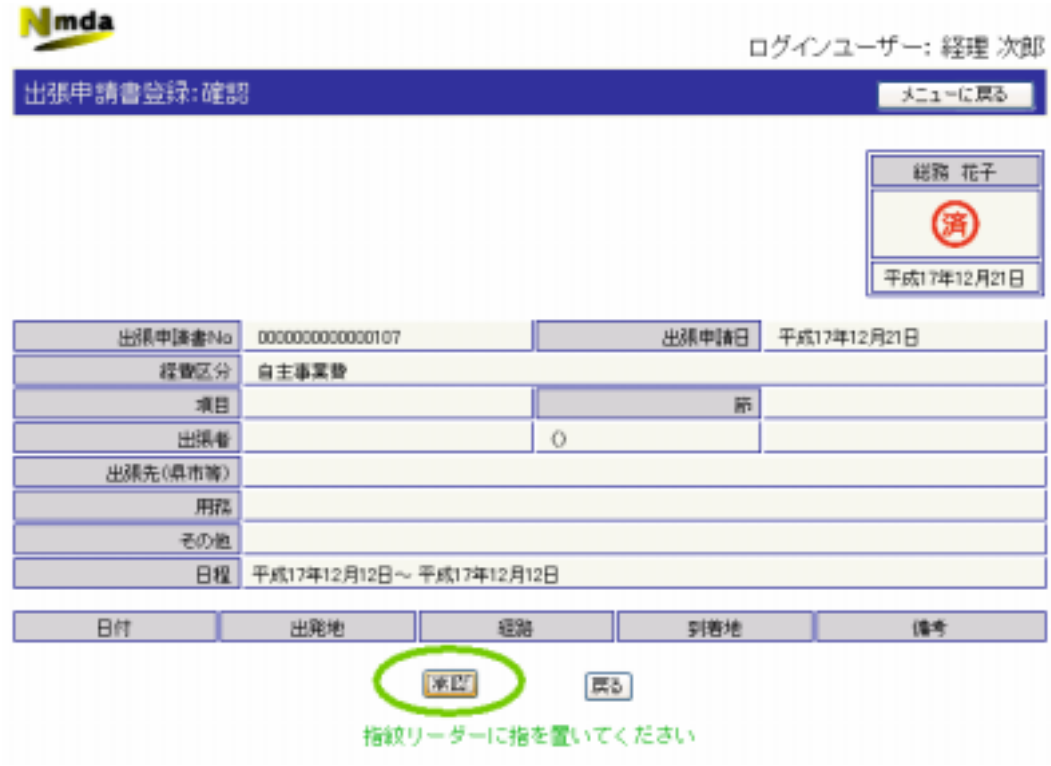
承認する出張申請書を選び、［出張申請書 No］をクリックする（図表 4-40)。

「未／済」欄に「済」と表示されている申請書は、すでに承認済のものである。改めて承認することはできない。

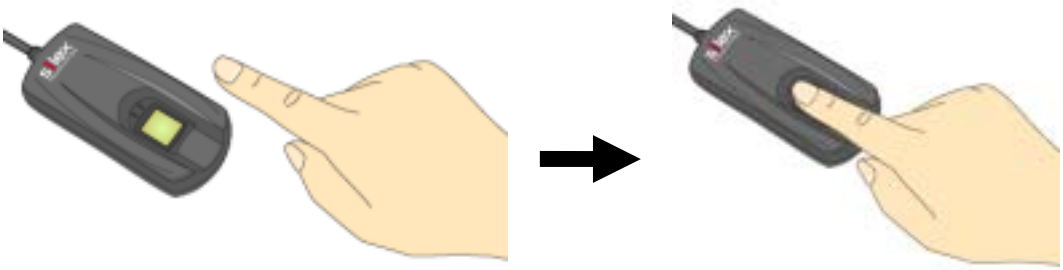
図表 4-40　［出張申請書 No］

（4）出張申請の承認のための指紋認証

［承認］ボタンをクリックし、指紋読取装置に指を置く（図表 4-41、図表 4-42）。



図表 4-41　［承認］ボタン



図表 4-42　指紋の認証

（5）認証の成功

指紋の認証に成功すると、承認完了画面に、承認者の氏名、承認日、及び承認印が表示される（図表 4-43）。

図表 4-43　承認の完了画面

（6）認証の失敗

4 回連続して指紋の認証に失敗すると、「指紋認証に失敗しました」というダイアログボックスが表示される（図表 4-44）。

引き続き承認をする場合は、［OK］ボタンをクリックし、［承認］ボタンをクリックしてから指紋読取装置に指を置く。

※10 回連続して失敗すると、ＩＣカードがロックされる。

図表 4-44　指紋認証の失敗

4. 3. 3. 認証時の所要時間

本節では、簡易認証を利用する際に、利用者の視点からどの程度の時間で利用できるのか、またどのような体感を得られるかを計測する。

計測は「4. 2. 3. テンプレート登録時の所要時間」で記述した手順により実施した。

今回の計測では被験者 2 のように認証時にエラーが多く見られるケースがあった。これは、認証に用いたテンプレート(10 回の登録所要時間計測の 10 回目の計測にて登録されたもの)の品質が良くなかったためと考えられる。

上記からわかるように、実際の登録業務では、登録後に、登録したテンプレートの品質で認証が問題なく行えるかを確認するという手順を含めておくことが望ましい。

図表 4-45　指紋認証時の所要時間計測結果

被験者1

単位:秒

	システムA（計測員1）	システムA（計測員2）	平均
1回目	2.84	2.53	2.69
2回目	1.98	2.28	2.13
3回目	2.20	2.25	2.23
4回目	2.67	2.69	2.68
5回目	2.46	2.59	2.53
6回目	3.18	3.45	3.32
7回目	2.43	2.28	2.36
8回目	2.26	2.16	2.21
9回目	2.53	2.61	2.57
10回目	2.72	2.62	2.67
平均	2.53	2.55	2.54

失敗回数 22回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	4.27	4.35	4.31
2回目	4.00	4.04	4.02
3回目	3.48	3.81	3.65
4回目	5.37	5.42	5.40
5回目	2.76	2.96	2.86
6回目	3.18	3.08	3.13
7回目	2.93	2.92	2.93
8回目	2.96	2.64	2.80
9回目	2.75	2.74	2.75
10回目	2.65	2.65	2.65
平均	3.44	3.46	3.45

失敗回数 0回

被験者2

	システムB（計測員1）	システムB（計測員2）	平均
1回目	2.62	2.65	2.64
2回目	2.82	2.81	2.82
3回目	2.90	2.75	2.83
4回目	2.60	2.47	2.54
5回目	2.68	2.60	2.64
6回目	2.60	2.40	2.50
7回目	2.58	2.63	2.61
8回目	2.19	2.19	2.19
9回目	2.16	2.07	2.12
10回目	2.58	2.68	2.63
平均	2.57	2.53	2.55

失敗回数 0回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	5.16	5.42	5.29
2回目	2.75	2.81	2.78
3回目	3.06	3.11	3.09
4回目	2.55	2.85	2.70
5回目	2.55	2.46	2.51
6回目	1.82	1.75	1.79
7回目	5.65	2.66	4.16
8回目	2.35	2.14	2.25
9回目	2.22	2.21	2.22
10回目	2.48	2.48	2.48
平均	3.06	2.79	2.92

失敗回数 29回

被験者3

	システムA（計測員1）	システムA（計測員2）	平均
1回目	1.85	1.80	1.83
2回目	1.80	1.91	1.86
3回目	1.97	1.90	1.94
4回目	2.06	1.88	1.97
5回目	1.78	1.98	1.88
6回目	2.03	1.99	2.01
7回目	1.77	1.73	1.75
8回目	2.33	2.39	2.36
9回目	2.01	1.79	1.90
10回目	1.60	1.76	1.68
平均	1.92	1.91	1.92

失敗回数 2回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	2.25	2.44	2.35
2回目	2.18	1.94	2.06
3回目	2.85	2.70	2.78
4回目	2.18	2.26	2.22
5回目	2.58	2.63	2.61
6回目	2.42	2.34	2.38
7回目	2.48	2.46	2.47
8回目	2.06	2.24	2.15
9回目	2.31	2.28	2.30
10回目	2.37	2.34	2.36
平均	2.37	2.36	2.37

失敗回数 1回

被験者4

	システムB（計測員1）	システムB（計測員2）	平均
1回目	1.87	1.88	1.88
2回目	1.73	1.76	1.75
3回目	1.58	1.56	1.57
4回目	1.71	1.86	1.79
5回目	2.07	2.06	2.07
6回目	1.86	2.05	1.96
7回目	2.16	1.98	2.07
8回目	2.80	2.71	2.76
9回目	1.88	1.80	1.84
10回目	1.56	1.55	1.56
平均	1.92	1.92	1.92

失敗回数 7回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	2.51	2.36	2.44
2回目	1.86	1.94	1.90
3回目	2.09	1.96	2.03
4回目	2.01	1.81	1.91
5回目	2.01	1.89	1.95
6回目	2.35	2.30	2.33
7回目	2.17	2.08	2.13
8回目	1.86	1.88	1.87
9回目	1.95	2.04	2.00
10回目	1.82	1.93	1.88
平均	2.06	2.02	2.04

失敗回数 0回

被験者5

	システムA（計測員1）	システムA（計測員2）	平均
1回目	2.38	2.34	2.36
2回目	2.29	2.27	2.28
3回目	2.45	2.63	2.54
4回目	2.37	2.45	2.41
5回目	2.85	2.73	2.79
6回目	2.77	2.82	2.80
7回目	2.56	2.89	2.73
8回目	2.36	2.55	2.46
9回目	2.68	2.66	2.67
10回目	3.02	2.81	2.92
平均	2.57	2.62	2.59

失敗回数 7回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	2.48	2.20	2.34
2回目	2.56	2.47	2.52
3回目	2.65	2.70	2.68
4回目	2.71	2.54	2.63
5回目	2.27	2.07	2.17
6回目	2.47	2.48	2.48
7回目	2.72	2.76	2.74
8回目	2.95	2.95	2.95
9回目	2.48	2.49	2.49
10回目	2.25	2.30	2.28
平均	2.55	2.50	2.53

失敗回数 0回

被験者6

	システムB（計測員1）	システムB（計測員2）	平均
1回目	3.65	2.91	3.28
2回目	2.38	2.37	2.38
3回目	2.35	2.36	2.36
4回目	2.46	2.25	2.36
5回目	2.53	2.56	2.55
6回目	2.76	2.74	2.75
7回目	3.44	3.27	3.36
8回目	2.55	2.42	2.49
9回目	3.89	3.80	3.85
10回目	4.42	4.37	4.40
平均	3.04	2.91	2.97

失敗回数 1回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	2.48	2.56	2.52
2回目	2.25	2.36	2.31
3回目	2.45	2.36	2.41
4回目	2.45	2.45	2.45
5回目	2.47	2.62	2.55
6回目	2.46	2.49	2.48
7回目	1.90	1.94	1.92
8回目	1.95	2.16	2.06
9回目	2.05	2.36	2.21
10回目	1.95	2.26	2.11
平均	2.24	2.36	2.30

失敗回数 0回

被験者7

	システムA（計測員1）	システムA（計測員2）	平均
1回目	2.10	2.30	2.20
2回目	1.68	1.96	1.82
3回目	2.10	2.26	2.18
4回目	2.65	2.79	2.72
5回目	2.10	2.27	2.19
6回目	2.25	2.25	2.25
7回目	1.79	1.90	1.85
8回目	2.11	2.12	2.12
9回目	1.90	2.04	1.97
10回目	2.29	2.28	2.29
平均	2.10	2.22	2.16

失敗回数 2回

	システムB（計測員1）	システムB（計測員2）	平均
1回目	2.34	2.50	2.42
2回目	1.99	2.08	2.04
3回目	1.95	2.35	2.15
4回目	2.31	2.40	2.36
5回目	2.18	2.44	2.31
6回目	2.15	2.38	2.27
7回目	2.08	2.09	2.09
8回目	2.06	2.16	2.11
9回目	2.35	2.44	2.40
10回目	2.44	2.41	2.43
平均	2.19	2.33	2.26

失敗回数 0回

被験者8

	システムB（計測員1）	システムB（計測員2）	平均
1回目	1.91	2.06	1.99
2回目	1.79	2.06	1.93
3回目	1.98	1.95	1.97
4回目	2.41	2.28	2.35
5回目	2.00	2.07	2.04
6回目	2.60	2.55	2.58
7回目	2.79	2.98	2.89
8回目	2.17	2.51	2.34
9回目	2.51	2.65	2.58
10回目	2.47	2.50	2.49
平均	2.26	2.36	2.31

失敗回数 0回

	システムA（計測員1）	システムA（計測員2）	平均
1回目	2.17	2.21	2.19
2回目	3.31	3.61	3.46
3回目	2.76	2.74	2.75
4回目	2.14	2.12	2.13
5回目	2.15	2.16	2.16
6回目	2.28	2.38	2.33
7回目	2.39	2.40	2.40
8回目	2.22	2.31	2.27
9回目	2.22	2.47	2.35
10回目	2.22	2.36	2.29
平均	2.39	2.48	2.43

失敗回数 3回

図表 4-46　所要時間測定後に行ったアンケート結果

	指紋登録の所要時間		指紋認証の所要時間		感想
	システムA	システムB	システムA	システムB	
被験者1	5	4	5	5	・コツ（感覚）をつかむのが大変。 ・少し時間がたってから、また認証を行う時に不安。
被験者3	3	2	5	4	・PIN入力に比較すると、指紋認証は明らかに速いので良い。 ・Aシステムは、1・2回失敗しても1回あたりの認証速度が速いので実用的だと思う。 ・指紋認証は、PINの入力や署名の記入より速いため、実用的だと思う。 ・指紋に対する抵抗感は、特にない。 ・Bシステムは、指を指紋読取装置に置いたり離したりするガイダンスがわかりにくい。Bシステムのように文章でガイドされるより、Aシステムのように図で示される方がわかりやすい。Bシステムは、ガイダンスの文字が点滅するため、それもわかりにくい原因だったと思う。 ・Aシステムは、画面に絵が表示されるため、認証成功・失敗のダイアログボックスメッセージが表示される前に、成否を予測することが可能である。
被験者4	2	3	2	3	・A・B両システム共に、指紋の登録・認証の際に指を上げ下げするため疲れる。高齢者にとっては、より疲れる動作でないだろうか。 ・たとえ見えないよう工夫がなされていても、人前でPINを入力することに不安を感じる。指紋を使うのであれば、そのような不安がなくなるだろう。
被験者5	2	4	4	4	・Bシステムは、比較的速く指紋の登録が可能である。一般に、普及させる場合は年齢を問わず簡易認証システムな登録手続きである必要があるだろう。使用の第一段階である「登録」に手間と時間をかけると、利用者がしり込みする。 ・PINより指紋のほうが良いだろう。 ・Aシステムは、登録に手間をかけた割りに、認証時にエラーが出やすい。 ・エラーの回数は、予想以上に多い。
被験者8	3	4	3	4	・指紋認証の導入には反対である。体調により指紋のコンディションが異なるため、書類を開いたり行政手続をする等の行動を体調に左右されることに不安を感じる。自分の身体を束縛されているように感じる。

凡例：　1：とても遅い　2：遅い　3：普通　4：早い　5：とても早い

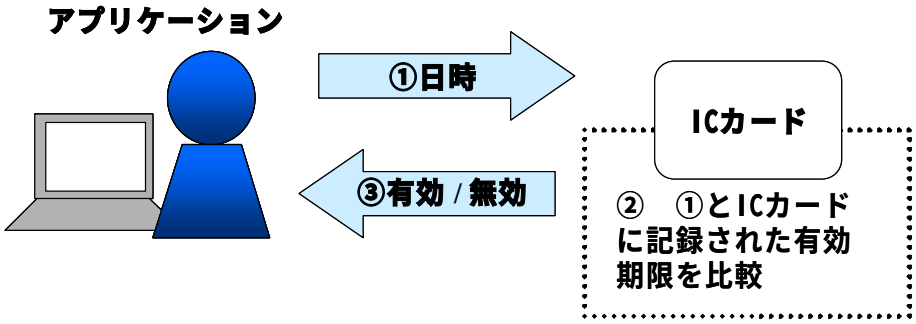
4. 4. 認証の失効

4. 4. 1. 失効の方式

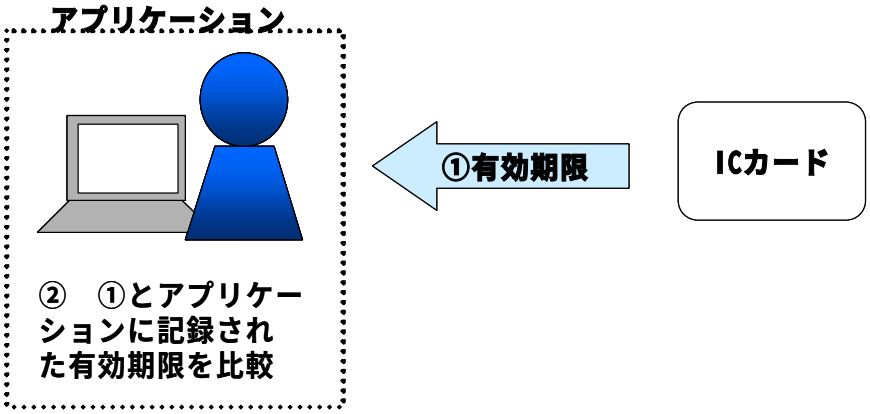
クレジットカードや運転免許証等、証明する内容に対する有効期限を設定しなければならないケースが存在する。またそれらは紛失した場合に第三者に不正に利用されないよう証明書を失効させなければならない。

ＩＣカードを利用した認証でも、その用途によっては有効期限を設定したり、証明書を失効させたりすることができなければならないケースが同様に存在する。

ＩＣカードに有効期限を持たせるためには、ＩＣカードの内部で有効期限、失効を判断して利用不可とする方法とＩＣカードを利用するアプリケーション側で判断する方法が考えられる。



図表 4-47　ＩＣカードで判断する方法



図表 4-48　アプリケーションで判断する方法

マッチオンカードの有効期限、失効の設定も上記と同様に考える事ができるが、さらにマッチオンカードに登録したテンプレートの失効についても考慮する必要がある。

マッチオンカードに登録したテンプレートは、一旦登録するとマッチオンカードの外

部に読み出す手段を提供しないのが一般的な実装となるため、カード自体が第三者の手に渡ってもテンプレートが流出したり、コピーが作られたりすることはない。したがってマッチオンカード内に登録されたテンプレート自体を失効する必要は無いと考えられる。しかし、新しいテンプレートをカードに登録する機能があるため、不正利用者によってテンプレートを書き換えられ、書き換えられたテンプレートをもちいて認証が行われてしまう可能性も考えられる。

テンプレートの書き換えによる不正利用を防ぐ手段としては以下のような方法が考えられる。

(1) 指紋登録を 1 回だけに制限する。

(2) 指紋登録をするための認証を別途行わなければ指紋登録ができないようにする。

(3) テンプレートを登録する際にテンプレートと対になるユニークなデータ生成し、カードとアプリケーションで記録しておき認証時に比較する。

(1) の方法では、一度指紋を登録したカードは、事故等によって正規ユーザーが指紋登録をやり直す必要が発生しても、テンプレートを登録しなおすことができなくなるため現実的ではない。

(2) の方法は、テンプレートを登録する際の認証のための仕組みが別途必要になり、指紋登録時の運用が複雑になる。

(3) の方法は、マッチオンカードとアプリケーションでカードの有効性を確認するためのデータとその照合のためのプログラムが別途必要となる。

(2)のテンプレートの登録を第三者が簡単にできないように専用のシステムを用意するのが一般的だが、(3) の方法と組み合わせることによって、仮にテンプレートを書き換えられてもアプリケーションでテンプレートの失効が判断できるようにすると、より高い安全性を確保することができる。

5. 互換性･標準化及びその他の課題

本章では、互換性、標準化及びその他簡易認証の分野でＩＣカードを活用する際の課題について述べる。

5. 1. ICカード及びカードＯＳの国際標準化動向

ＩＣカードに関連する国際標準規格として、以下の規格がある。

(1) ＩＣカード関連

ISO/IEC 7816-1～4: Identification cards - Integrated circuit(s) cards with contacts (接触型ＩＣカードの規格)

ISO/IEC 14443-1～4: Identification cards - Contactless Integrated circuit(s) cards Proximity cards) (非接触型ＩＣカードの規格)

またＩＣカードの代表的なマルチアプリケーションカードＯＳとしては、以下の規格がある。

(2) カードＯＳ関連

MULTOS: MAOSCO コンソーシアムが仕様設定、開発

JavaCard: Sun Microsystems, Inc.が仕様設定、開発

5. 2. マッチオンカードの国際標準化動向

マッチオンカードに関連する国際標準規格として、ＩＣカード関連、バイオメトリクス関連について以下のような規格がある。

(1) バイオメトリックス関連

ISO/IEC 19794-2:2005: Information technology - Biometric data interchange formats - Part 2:Finger minutiae data (指紋の特徴点抽出データフォーマットに関する規格)

ISO/IEC 19794-4:2005: Information technology - Biometric data interchange formats - Part 4:Finger image data (指紋画像データフォーマットに関する規格)

また審議中の規格としては以下のようなものがある。

ISO/IEC 19785-1: Information technology - Common biometric exchange formats framework - Part 1:Data element specification (バイオメトリックス情報のデータ構造に関する規格)

ISO/IEC 19784-1:2005: Information technology - Biometric application

programming interface- Part 1:BioAPI specification（バイオメトリクスシステムにおけるアプリケーションプログラム及びサービスプロバイダーとの間の標準インターフェイス仕様に関する規格）

ISO/IEC 19792: Framework for Security Evaluation and Testing of Biometric Technology（バイオ情報のセキュリティに関する評価方法、テスト方法を規定した規格）

ISO/IEC 19702: Biometric Information Management and Security for Financial Applications（金融分野でのバイオ情報の取扱に関する規格）

マッチオンカードに関連する国際標準については以下のような活動がある。

(2) マッチオンカード関連

ISO/IEC JTC1 SC17

※シンガポール提案がNWIとして承認されている。今後、WG11とWG4との合同会議により、両WGの作業内容をつめることになっている。

ISO/IEC JTC1 SC27

※バイオメトリクス関連の評価基準及びテンプレートセキュリティがWDとして検討されている段階。また、マッチオンカードのカード処理負荷についても検討が継続されている。

ISO/IEC JTC1 SC37/WG2

※京都会議（2006年1月18日開催）でBioAPI及びCBEFF（Common Biometrics Exchange Format Frameworks）が、ほぼ標準化された。

ISO/IEC JTC1 SC37/WG3

※ISO19794-2(Finger Minutia Data:指紋特徴点)、ISO19794-4(Finger Image Data:指紋画像）については、国際標準（IS）して発行済みである。

※ISO 19794-3（Finger Pattern Spectral Data:指紋パターン）については、2006年に国際標準化の見込みである。

※指紋データ品質について、ISO/IEC 29794（Biometric Sample Quality）でWDとして検討されている。

5. 3. マッチオンカードのセキュリティ

5. 3. 1. 登録時のセキュリティ

マッチオンカードを用いた認証では、マッチオンカードに登録されたテンプレートに対するセキュリティが重要となる。テンプレートの登録時には登録するテンプレートが外部に流出しないように、また登録されたテンプレートに関しては不正なユーザーによって登録されたテンプレートを改ざんされることがないようにする必要がある。

テンプレートが外部に流出しないようにするためには、テンプレート登録システムを外部からアクセスすることの出来ない専用のシステムとすることが望ましい。さらにテンプレート登録システムはテンプレートの流出、改ざんを防ぐためにも、登録のための権限を持つユーザー以外が利用できないように、物理的、ソフトウェア的な防衛措置を施すことが望ましい。

5. 3. 2. ICカードに登録されたテンプレートのセキュリティ

マッチオンカードは登録したテンプレートを外部から読み出すことはできず、指紋読取装置で読取った照合用指紋情報と登録されたテンプレートをカード内で比較する方式となっている。このため登録したテンプレートが第三者に渡ることはない。脅威として唯一考えられることは登録されたテンプレートを改ざんされることだが、「5. 3. 1. 登録時のセキュリティ」で記述したように、登録システムのセキュリティを強化することで対処することができる。

5. 4. 暗証番号

簡易認証では、ＩＣカードを利用する際に入力する暗証番号の代りに指紋認証を行う。しかし、指紋認証は、認証を行うユーザーが指に怪我を負ったり、体調等の理由によりうまく指紋認証できなかったりする場合が考えられる。そこで「4. 2. 1. テンプレート登録の仕様」で記述したように、登録できるテンプレートの数を複数にすることで、認証に失敗した場合に別の指を使うという方法により認証させることが可能である。それでもうまく認証できない場合には、暗証番号でＩＣカードを利用可能とする従来の方法を併せて実装しておくことで、指紋認証によるトラブルにも対処可能となる。

しかし、暗証番号でＩＣカードが利用できる場合には、暗証番号を記憶しなければいけないという理由から暗証番号の桁数をそれほど大きくすることはできず、指紋認証で得られる安全性には及ばなくなり、それが認証の安全性を若干下げる要因にもなるため、安全性と簡易性を考慮してアプリケーション毎に暗証番号との併用を検討する必要がある。

まとめ

「バイオメトリクスによる簡易認証システムの調査・開発」として行った今回の調査開発においては、次の成果が確認された。

従来、ＩＣカードのＣＰＵの処理能力によりＩＣカード内で行う処理に限界があるため、指紋認証等の複雑な処理はＰＣ側で行われてきたが、近年ＩＣカードの処理能力が向上したり指紋認証アルゴリズムが改善されたりしたことにより、指紋認証の処理をＩＣカード側で行っても十分に実用的な処理時間で運用できることが明らかとなった。

本調査・開発では、前述のとおりいくつかの課題が判明したが、一方で実際の運用時の所要時間に関しては、現状のソフトウェア・ハードウェアでも十分に利用可能なレベルにあり、暗証番号の代わりに指紋情報を用いて本人認証を行うことにより、忘れやすい暗証番号を覚えていなくてもＩＣカードを利用することができる簡易認証システムを構築できることが確認された。

また、マッチオンカードの登録指紋情報の互換性が無いことにより、異なるシステム間で同一のマッチオンカードを利用する事ができないという課題が明らかになった。しかし、これらは、国際標準規格の策定及び登録指紋情報に関する標準化等を踏まえて、それに準拠するマッチオンカードシステムの開発等により改善されるものと考えられる。

以上

添付資料一覧

No.	添付資料名
資料1	帳票押印簡易システム仕様書
資料2	申請決裁簡易システム仕様書
資料3	帳票押印簡易システム取扱説明書（導入・環境設定編）
資料4	帳票押印簡易システム取扱説明書（指紋登録編）
資料5	帳票押印簡易システム取扱説明書（利用編）
資料6	申請決裁簡易システム取扱説明書（環境設定編）
資料7	申請決裁簡易システム取扱説明書（利用編）
資料8	「簡易認証システムの調査にご協力ください」
資料9	マッチオンカードの国際標準化動向関連資料（1）： バイオメトリクス セキュリティー コンソーシアム　国際標準化セミナー （2006年2月15日開催）資料
資料10	マッチオンカード対応ICカードデバイス及びアプレット仕様書　（Java Cardベース）
資料11	マッチオンカードの国際標準化動向関連資料（2）： Precise社White Paper（抜粋）

発行日　平成 18 年 3 月
作　成　財団法人ニューメディア開発協会
住　所　〒108-0073　東京都港区三田 1-4-28　三田国際ビル 23 階
電　話　03-3457-0674　ＦＡＸ　03-3451-9604

開発事業者　イデア　コラボレーションズ株式会社
住　所　〒108-0073　東京都港区三田 3-2-8
開発事業者　株式会社日立製作所
住　所　〒136-8632　東京都江東区新砂 1-6-27
開発事業者　サイレックス･テクノロジー株式会社
住　所　〒577-0802　大阪府東大阪市小坂本町 1-6-20

この報告書は、当協会が日本自転車振興会の補助を受けて実施した
「バイオメトリクスによる簡易認証システムの調査･開発」の成果として
とりまとめたものです。

ＵＲＬ：www.nmda.or.jp