平成 19 年度
「多種類のバイオメトリクス簡易認証システムの調査・開発」
調査開発報告書

平成 20 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。

URL : http://keirin.jp/

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おります。

認証のための装置の一つである 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。近年、その IC カードの正規の利用者であることを証明するために、本人の指紋を使ったバイオメトリクス技術を IC カードに適用する技術が向上し、普及が進みつつあります。

また、バイオメトリクス情報には、指紋のほかに、静脈や顔、虹彩、掌形といった身体的特徴を扱うものや、声紋、署名といった行動的特徴から取得するものもあります。この中でも、とりわけ、指静脈による本人認証技術については、銀行 ATM やマンションやオフィスの入退管理、PC のログインなどの用途で使われ、普及しつつあります。

今後、指静脈による本人認証技術が指紋と並んで普及すると、利用シーンに応じて適切な方式を選択して本人認証が行えるようになり、システム利用者の利便性を高めることが可能となります。そのためには、指紋認証だけではなく、指静脈による本人認証どちらの方式でも可能とするようなシステムが必要となってきます。

そこで、本事業では、前年度開発した簡易認証システムをもとに、指紋、指静脈のどちらでも本人認証を可能とするデモシステムを開発し、達成された成果及び抽出された課題を整理しました。

あわせて、指静脈認証技術の標準化状況や、実際に指静脈を用いた本人認証技術の適用モデルの調査を行い、指静脈を用いた本人認証技術に関する技術動向、実態などを把握しました。

この報告書は、以上に挙げた結果についてとりまとめたものであり、今後のバイオメトリクスによる認証システム発展の一助になれば幸いです。

平成 20 年 3 月

財団法人ニューメディア開発協会

目　次

＜他社所有商標に対する表示＞

- 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。
- 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。
- Microsoft Excel は、米国 Microsoft Corp.の商品名称です。
- MULTOS は、MAOSCO Ltd.の登録商標です。
- 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。
- 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. 本事業の背景、目的

バイオメトリクス（生体情報）を利用して簡易に本人であることを認証するシステムの認証方式の一つに、指紋データを IC カード内に格納し（テンプレート）、指紋読取装置から読み取った本人の指紋情報を照合させて認証する方式がある。

指紋による本人認証は、利用者が指に傷を負ったり、環境条件等によって、指紋を用いた本人認証ができない場合が想定される。また、乾燥指などにより、採取した指紋画像データが薄く、本人認証ができない場合もある。さらに、「指紋を採取する」ことに対して心理的な抵抗感を感じる利用者も存在する。

一方、銀行 ATM やマンションの入退室などの一部サービスでは、指静脈による本人認証が採用されつつあり、指紋以外のバイオメトリクスを利用した本人認証技術も普及しつつある。

平成 17 年度事業では暗証番号（または、ID / パスワード）の代わりに、指紋データをテンプレートとして登録し IC カードで本人認証を行う簡易認証システムの開発を行った。翌平成 18 年度は、平成 17 年度に開発した簡易認証システムに対し、一枚の IC カードから他システムの本人認証を可能とする開発を行い、複数の指紋認証システムの互換性を確保した互換性検証システムへの拡張を行った。

これらを踏まえ、本事業では、平成 17 及び 18 年度に開発した、指紋認証による IC カードの互換性を持たせた簡易認証システムをベースとして、これまでの「指紋」認証方式に加え、「指静脈」認証方式を新たに採用し、両方の本人認証方式を共存させた簡易認証システムの開発を行うことを目的とする。

これにより、利用者は好みのバイオメトリクス情報を選択して、本人認証方式を選択することが可能となり、簡易認証システムの柔軟性、利便性を高めることが期待される。加えて、単独での本人認証が困難な場合でも、もう一方の方法によって認証を行うことにより、安定した本人認証が可能になる。また、指紋に加えて指静脈認証方式を採用することにより、簡易認証システムの認証レベルの強化を可能にすることができると考えられる。例えば、指紋と指静脈をともに認証できた場合のみ認証を可能にするなど、セキュリティレベルを考慮したシステム構築の検討が可能になる。

上記開発に対して、指紋及び指静脈認証の双方の認証方式を共存させた簡易認証システムの評価を行う。この評価結果に基づき、課題を抽出することで、複数のバイオメトリクスを利用した簡易認証システムの「あるべき姿」を提示することを目的とする。

2. 調査・開発計画

本事業で実施する調査・開発の計画概要を示す。

2.1 調査

2.1.1 指静脈認証による本人認証方式の標準化状況調査

指静脈を用いた本人認証方式の標準化状況について、国際標準規格の検討状況の現状を調査する。

2.1.2 指静脈認証を用いた本人認証の適用モデルの調査

身近な現実社会において指静脈による本人認証システムがどのように利用・運用されているかなどの現状把握や、製品の市場動向調査などを行う。

2.2 開発

2.2.1 互換性検証システムの仕様

指紋による本人認証方式と、指静脈による本人認証方式を共存させた簡易認証システム（以下「互換性検証システム」と言う。）を開発するにあたり、その実現性に向けた仕様の検討を行う。

2.2.2 互換性検証システムの評価

上記 2.2.1 で検討・策定した仕様に基づいて開発した互換性検証システムに対して、指紋及び指静脈のどちらの認証方式でも IC カードへの指紋 / 指静脈データ（以下「テンプレート」と言う。）の登録と本人認証が可能であることの確認や、開発の過程で発生した課題などを整理する。

3. 調査・開発結果

本章では、第 2 章で定めた調査・開発計画に対する実施結果を述べる。

3.1 調査

3.1.1 指静脈認証による本人認証方式の標準化状況調査

2008 年 3 月時点での指静脈による本人認証方式の標準化状況を示す。

（1）ISO/IEC JTC1 SC37 におけるバイオメトリクス技術に関する標準化動向

国際規格（ISO/IEC JTC1）の SC37 では、汎用的なバイオメトリック技術に関する標準化を担当しており、６つのワーキンググループ体制がある。

WG3（Biometric Data Interchange Formats / バイオメトリックデータ交換フォーマット）では、バイオメトリックデータの交換形式を策定するグループであり、バイオメトリックシステム間で認証の相互運用性（Interoperability）確保を目的として、交換用データフォーマットの策定を行っている[1]。

具体的には、認証技術ごとにパートを分けた ISO/IEC 19794（交換用データフォーマット）、29794（バイオメトリックサンプル品質）及び 29109（準拠性、Conformance）の審議を進めており、14 種のフォーマットを審議中である。（表 3.1.1-1）

表 3.1.1-1　SC7/WG3 標準化活動の動き（2007 年 2 月 15 日時点）[2]

種類（Modality）		フォーマット（19794）	データ品質（29794）	準拠性（29109）	性能
指紋	画像	19794-4：IS	29794-4（TR）：WD	Part4：NP	WG5 検討
	特徴点	19794-2：IS	19794-2A1：NP	Part2：NP	
	図形	19794-3/8：IS		Part3/8：NP	
顔	画像	19794-5：IS 19794-5A2：PDAM	29794-5（TR）：NP 19794-5A1：FDAM	Part5：NP	
	特徴量	19794-12：予定			
虹彩	画像	19794-6：IS		Part6：NP	
署名 /	時系列	19794-7：FDIS		Part7：NP	

[1] IPSJ/ITSCJ ウェブページ、2006 年度 専門委員会関係活動報告－SC37 専門委員会（バイオメトリクス）、http://www.itscj.ipsj.or.jp/senmon/06sen/sc37.html

[2] バイオメトリクス セキュリティ コンソーシアム（BSC）ウェブページ、SC37 最新動向セミナー「SC37 Biometrics 標準化報告 WG3 Biometric Data Interchange Formats」、http://www.bsc-japan.com/pdf/20070803_WG3.pdf

種類（Modality）		フォーマット（19794）	データ品質（29794）	準拠性（29109）	性能
サイン	特徴量	19794-11：WD		Part11：NP	
血管（静脈）	画像	19794-9：IS		Part9：NP	
手外形	図形	19794-10：FDIS		Part10：NP	
声	波形特徴量	19794-13：NP		Part13：NP	

＜審議状況＞

NP：New Work Item Proposal → WD：Working Draft → CD：Committee Draft → FCD：Final Committee Draft → FDIS：Final Draft Int. Std →IS：International Standard

（2）血管（静脈）画像データ交換フォーマットの標準化動向

SC37/WG3 で扱っているバイオメトリックデータの交換フォーマット策定のうち、パート 9（19794-9）では、Vascular (Vein) Image Data、血管（静脈）の画像データのフォーマット標準化を検討している。2007 年 3 月に、IS（International Standard：国際標準）規格として発行された。

19794-9 では、血管・静脈による認証用の画像交換データを規定し、手の両面（手のひらおよび手の甲）及び指の静脈状況を用いたバイオメトリクス認証のデータ交換に使うもので、認証アルゴリズムに左右されない原画像レベル（原則は近赤外画像）での交換形式を規定している。

29109（Conformance Testing Methodology）のパート 9 にて、19794-9 で定めたデータフォーマットへの準拠性（conformance）をテストする方法について米国から提案され、現在進行中である。

3.1.2　指静脈認証を用いた本人認証の適用モデルの調査

指静脈による本人認証システム事例や適応モデルの調査結果を示す。

（1）指静脈入退管理システム SecuaVeinAttestor[3]

指静脈入退管理システム SecuaVeinAttestor は、指静脈による本人認証を行うことでビルやオフィスの安全を確保するシステムである。

指静脈入退管理システムは、「指静脈スキャナー」を用いて指静脈による本人認証を行う。「指静脈スキャナー」は、①IC カード内に指静脈データを格納しその IC カードを用いて本人認証を行う IC カード連携タイプ、②利用者の ID 番号を入力し、指静脈による本人認証と ID 番号の入力の双方あるいはいずれかの認証が可能なテンキータイプ、③無線認識 IC を利用したミューチップ対応タイプ、④フラッパーゲートへの指静脈スキャナーの組み込みによる連携、の 4 タイプがある。

上記「指静脈スキャナー」は、ビルやオフィスのセキュリティレベルに応じて、例えば表 3.1.2-1 に示すようなタイプの選択が可能である。

表 3.1.2-1　ビルやオフィスのセキュリティレベルと適用例、指静脈スキャナーの設置タイプ例

低 ↓ 高

レベル	説明	適用例	指静脈スキャナーの設置タイプ
レベル 1	不特定多数の人が来場する準パブリックスペースで、外来者の入場を制限する。入口に設置し、指静脈で本人認証が確認された関係者以外の入館を制限し、不審者侵入防止を支援する。	オフィスエントランス、マンションエントランス、エレベーターホール、空港、港など	③ミューチップ対応タイプの指静脈スキャナー ④フラッパーゲート連携
レベル 2	業務スペースへの関係者以外の入室を防止する。入室を厳格にし、関係者以外の入室を制限する。秘密情報保護や個人情報保護の厳格化を図ることができる。	オフィス（人事課、研究開発室など）、金融、保険、証券会社、クレジット会社、情報処理会社、データセンター、病院（院長室、薬品室、病原菌培養室、研究室など）	②テンキー付属の指静脈スキャナー
レベル 3	特定の人だけが出入りする場所に活用できる。	サーバ室、金庫室、研究室・実験室、薬品・危険物管理室など	①IC カード対応タイプの指静脈スキャナー

[3] セキュリティソリューション《セキュアオフィス®》シリーズ　指静脈認証システム、株式会社日立情報制御ソリューションズ

システム構成は、以下に示す通り、スタンドアロンからネットワークに対応した構成をとることが可能である。また、指静脈スキャナーのみで登録/認証するケースと、テンプレートを IC カードに登録し入退室の際に認証するケースにも分類される。

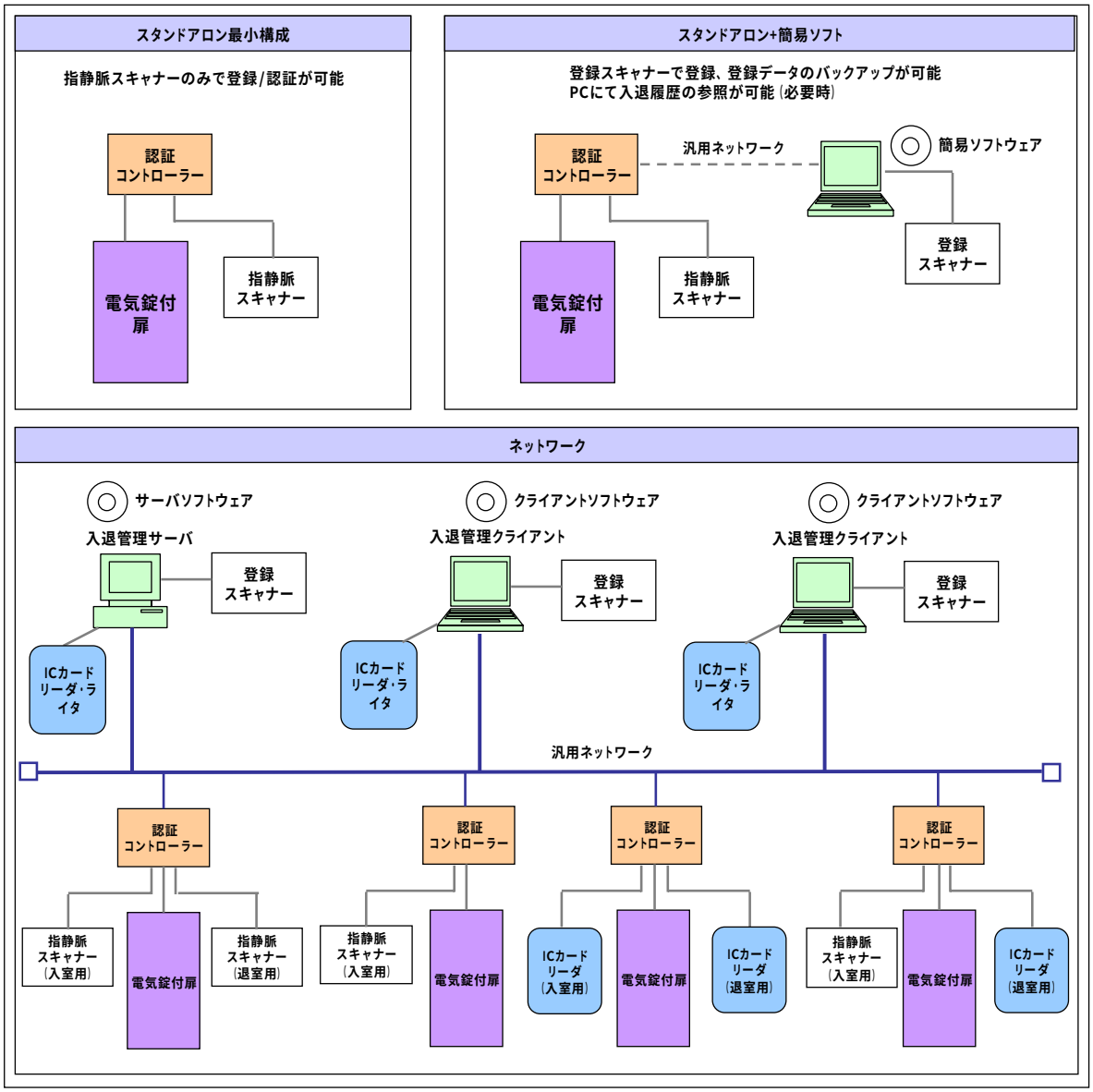


図 3.1.2-1　SecuaVeinAttestor **のシステム構成例**

（2）卓上型指静脈認証装置[4]

卓上型指静脈認証装置は、PC のログインやスクリーンセーバ解除時などにおいて指静脈による本人認証を行うことで、PC の利用者を特定することを可能にする装置である。また、PC 以外にも、タイムレコーダやプリンタなどの機器にも接続が可能である。

卓上型指静脈認証装置を用いたシステム構成は、PC に接続して PC 内の専用ソフトで本人認証する「PC 認証タイプ」と、タイムレコーダ、プリンタ、PC などの機器に接続して、指静脈認証装置内で本人認証する「自己認証タイプ」がある。（表 3.1.2-2）

表 3.1.2-2　卓上型指静脈認証装置を用いたシステム構成

システム構成タイプ	本人確認の方法（例）
PC 認証タイプ	指をかざし、PC に登録してある指静脈パターンと照合して本人確認を行う
自己認証タイプ	1.タイムレコーダ/プリンタなどの機器で ID ナンバを入力する。 2.指をかざし、機器から読み込んだ指静脈パターンと照合して本人認証する。 ※認証ロジックが卓上装置内にあるため、CPU の弱い機器でも導入が可能。

卓上型指静脈認証装置を用いた適用例を以下に示す。

（ア）PC ログイン・各種業務アプリケーションの使用管理

特定の利用者のみ、PC の利用を許可したり、各業務システムへのアクセスを許可したりするなどが可能である。指静脈認証により個人の特定も可能なため、ID とパスワードのログインと比べアクセスログ管理も確実となる。

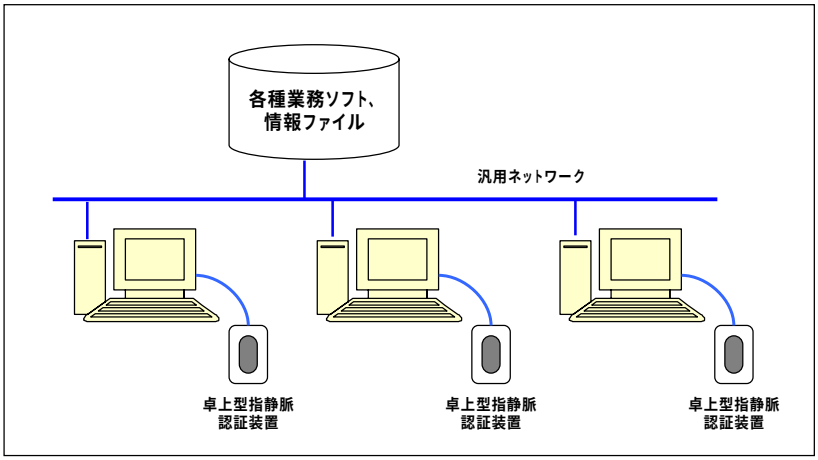


図 3.1.2-2　卓上型指静脈装置を用いた適用イメージ 1

[4] セキュリティソリューション《セキュアオフィス®》シリーズ　卓上型指静脈認証装置、株式会社日立情報制御ソリューションズ

（イ）出退勤の管理

作業者（従業員やアルバイト）など、多様化する雇用形態に対応した確実な勤怠管理が可能となる。情報の漏洩や不審者の侵入を未然に防ぐこともできる。

（ウ）機密情報の出力管理

プリンタ出力の際、指静脈による本人認証を行わなければならないことにより、機密情報の漏洩を防ぐことが可能となる。また、出力した個人の履歴管理も可能である。

なお、図 3.1.2-3 は、PC 画面で出力指示を行った人物と、プリンタ側で出力した紙を受け取る人物が同一であることを指静脈による本人認証により確認してからプリンタから紙が出力される構成を示している。

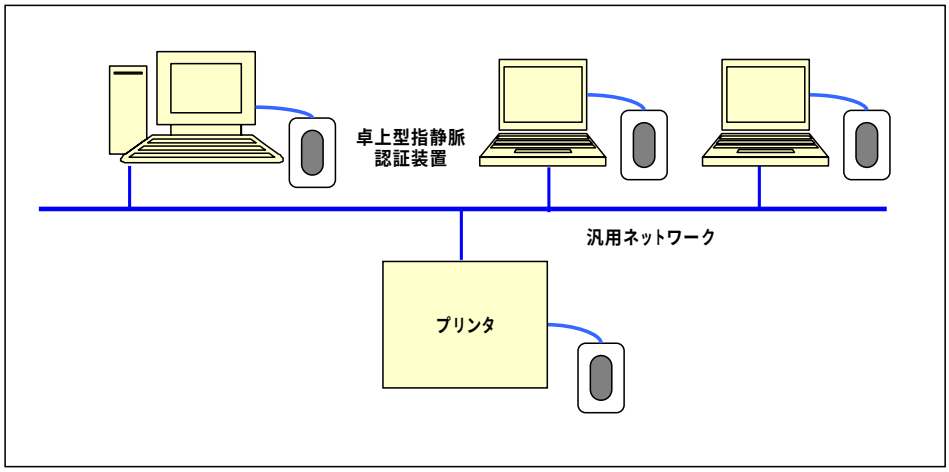


図 3.1.2-3　卓上型指静脈装置を用いた適用イメージ 2

（3）日立指静脈認証装置[5]

日立指静脈認証装置　PC-KCA100 は、前述の「（2）卓上型指静脈認証装置」と同様に、ユーザ ID とパスワード、またはパスワードの代わりに指静脈認証を行うことで、PC へのログインやスクリーンセーバの解除、アプリケーションへのログインを可能とする認証装置である。

図 3.1.2-4　**日立指静脈認証装置**　PC-KCA100

認証装置上部のフードにより外光の影響を低減するとともに、近赤外線を指の上から透過させ、下からカメラで読み取る方式を採用したことにより、高い認証精度を実現していることが特徴の一つであるといえる。

また、国際標準規格 BioAPI(Biometric Application Program Interface) 2.0 に対応していることから、同規格に対応した認証サーバに、指静脈による認証システムを付加するこが可能である。

[5] 日立製作所ウェブページ、指静脈ソリューション＞IT セキュリティ、
http://www.hitachi.co.jp/Prod/vims/solutions/fvu/index.html

（4）指静脈認証管理システムによる導入事例[6]

ここでは、株式会社日立製作所が提供する「指静脈認証管理システム」を用いて、指静脈による本人認証がどのように使われているかの事例を紹介する。

大塚製薬株式会社では、医療品の品質や安全確保のまたの国際基準「GMP（Good Manufacturing Practice：製造管理と品質管理の基準)」に基づく電子文書管理システムの認証に、「指静脈認証管理システム」を導入した。

（ア）指静脈認証管理システム導入前の課題

指静脈認証管理システム導入前の課題を以下の通り示す。

（a）電子署名を付与するたびに発生するユーザ ID、Password の入力の負担

e-文書法の施行によって､GMP 文書の作成や保管が完全に電子化されるようになり、これまで責任者のサインによって行っていた文書の受付・承認方法が、本人認証による電子署名を付与する方法に変わることとなった。

しかし､電子署名の付与にあたっては､その都度ユーザ ID と Password の入力が必要とされることとなり、担当者によっては、一日に数十回、電子署名を行う必要があり、そのたびにユーザ ID と Password の入力を行わなければならず､負担が生じるようになった。

（b）複雑化するパスワード管理

GMP に基づいた文書管理業務以外の業務システムでも、それぞれのシステムで異なる Password が付与され、それが数ヶ月おきに変更される状況が発生し、パスワード管理など、システム管理者に対する負担が生じている。

（イ）指静脈認証管理システムの導入による解決策

上記（1）に示す課題に対し、既存の文書管理システムに対して指静脈認証管理システムを連携させる認証システムを構築した。図 3.1.2-5 は、指静脈認証で GMP に基づいた文書を作成するときに電子署名を付与する仕組みを示したものである。

[6] 日立製作所ウェブページ、指静脈認証ソリューション＞導入事例：IT セキュリティ、http://www.hitachi.co.jp/Prod/comp/app/yubi/casestudy/otsuka/

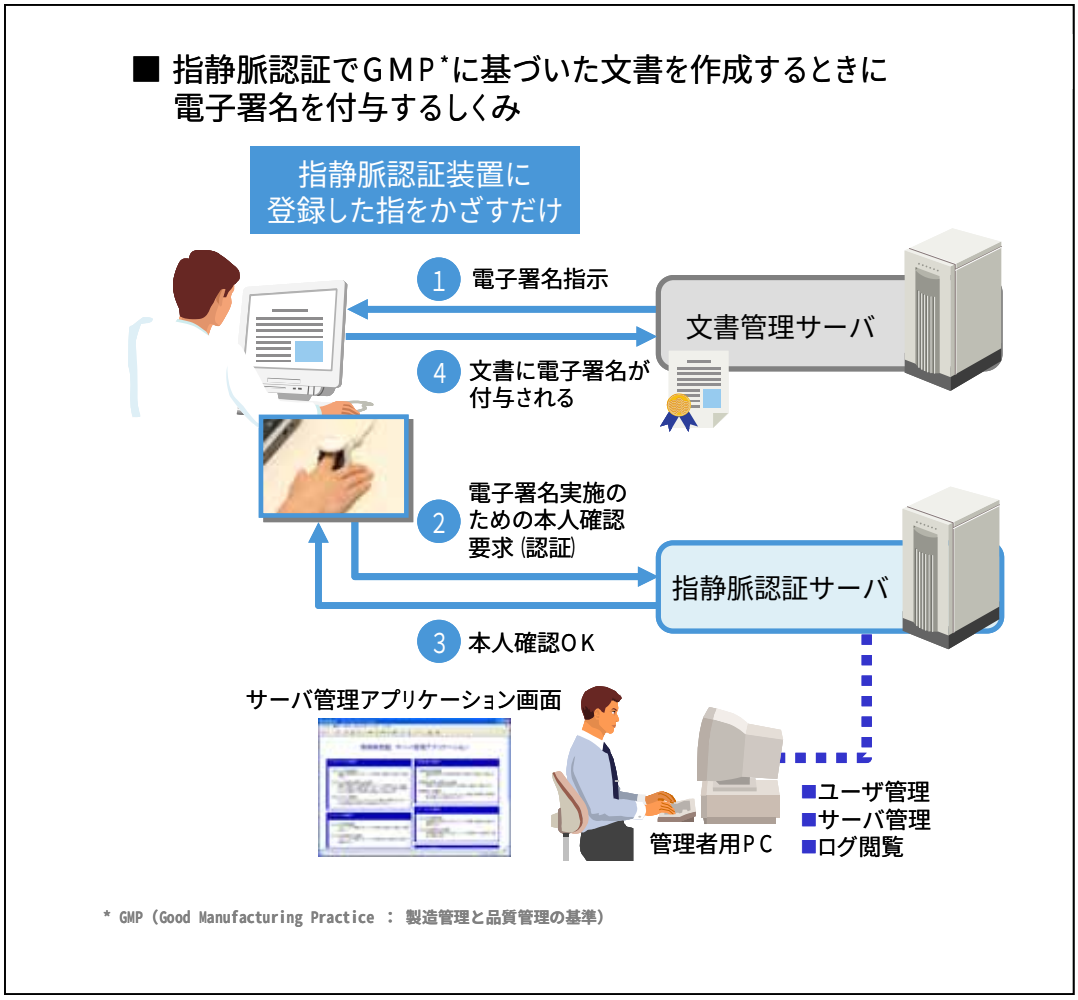


図 3.1.2-5　指静脈認証で GMP に基づいた文書を作成するときに電子署名を付与する仕組み

（ウ）システム導入後の効果

指静脈による本人認証システムを導入したことによる効果を以下に示す。

（a）セキュリティ強化と業務効率の向上を同時に実現

指静脈による本人認証を導入したことにより、GMP に基づいた文書作成と保存を行う際に、これまで 1 回ごとにユーザ ID と Password を入力することで付与されていた電子署名を、指静脈認証で代替する仕組みに変更した。

これにより、これまで電子署名の付与 1 回ごとにユーザ ID と Password を手で入力していた本人確認が、指静脈読取装置に指をかざすだけで瞬時に完了し、利用者の負担を軽減し、業務を効率化させることができた。

同時に、指静脈という生体認証での本人確認を行うことによりユーザ ID / Password に比べてセキュリティが強化され、より信頼性の高い文書管理システムとなった。

（b）タイムスタンプ効果

誰がいつ、どの PC からログインしたか等の履歴の管理が可能となった。また、常に記録をとられていることへの牽制効果も働いたと考えられ、セキュリティ強化に役立った。

（c）認証情報の一括管理で今後の運用負担軽減にも期待

これまで業務システムごとに異なり、かつ、それぞれが数カ月おきに更新される複数のパスワードの管理から、指静脈認証のみを一括管理することができるため、管理者の負担を軽減する効果も期待ができる。

3.2 開発

3.2.1 互換性検証システムの成果

指紋による本人認証方式と指静脈による本人認証方式の双方での認証を可能とする互換性検証システムを開発するにあたっての仕様の検討を行った。

その結果決定した互換性検証システムのシステムイメージを以下に示す。

（1）ハードウェアイメージ

互換性検証システムのハードウェアイメージを図 3.2.1-1 の通り示す。

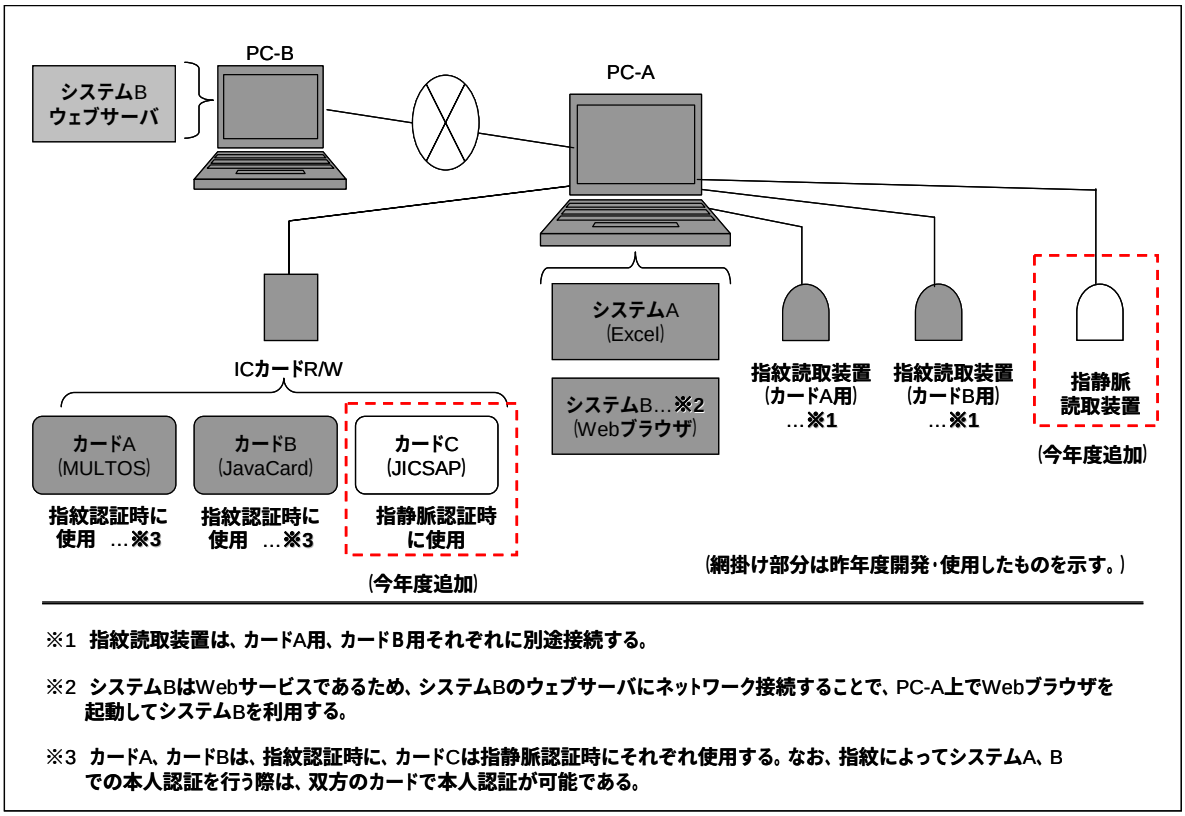


図 3.2.1-1 互換性検証システムのハードウェアイメージ

PC-A（FLORA270WC、日立製作所製）に対して、指紋認証用のカード A、カード B にそれぞれ対応した指紋読取装置と IC カード R/W 及び指静脈読取装置をそれぞれ取り付ける。また、PC-B（Let's Note、松下電器製）にはシステム B[7]の Web サーバが搭載されていることから、PC-B と PC-A とのネットワーク接続を行う。これにより、PC-A 上

[7] システム B：Web ブラウザを用いて出張申請書の申請及び承認を行う際に、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システム。指紋登録データ（テンプレート）と Web アプリケーションにログインするためのアカウント情報及び暗証番号を IC カード内に搭載し、認証時に 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する。

で、システム A[8]及びシステム B の双方を利用可能とし、それぞれのシステムで指紋認証及び指静脈認証双方を可能とする構成とする。

[8] システム A：Excel で作成された帳票への承認・押印を行う際に、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システム。指紋登録データ（テンプレート）を IC カード内に搭載し、認証時に 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する。

(2) ソフトウェアイメージ

互換性検証システムのソフトウェアイメージを図 3.2.1-2 の通り示す。

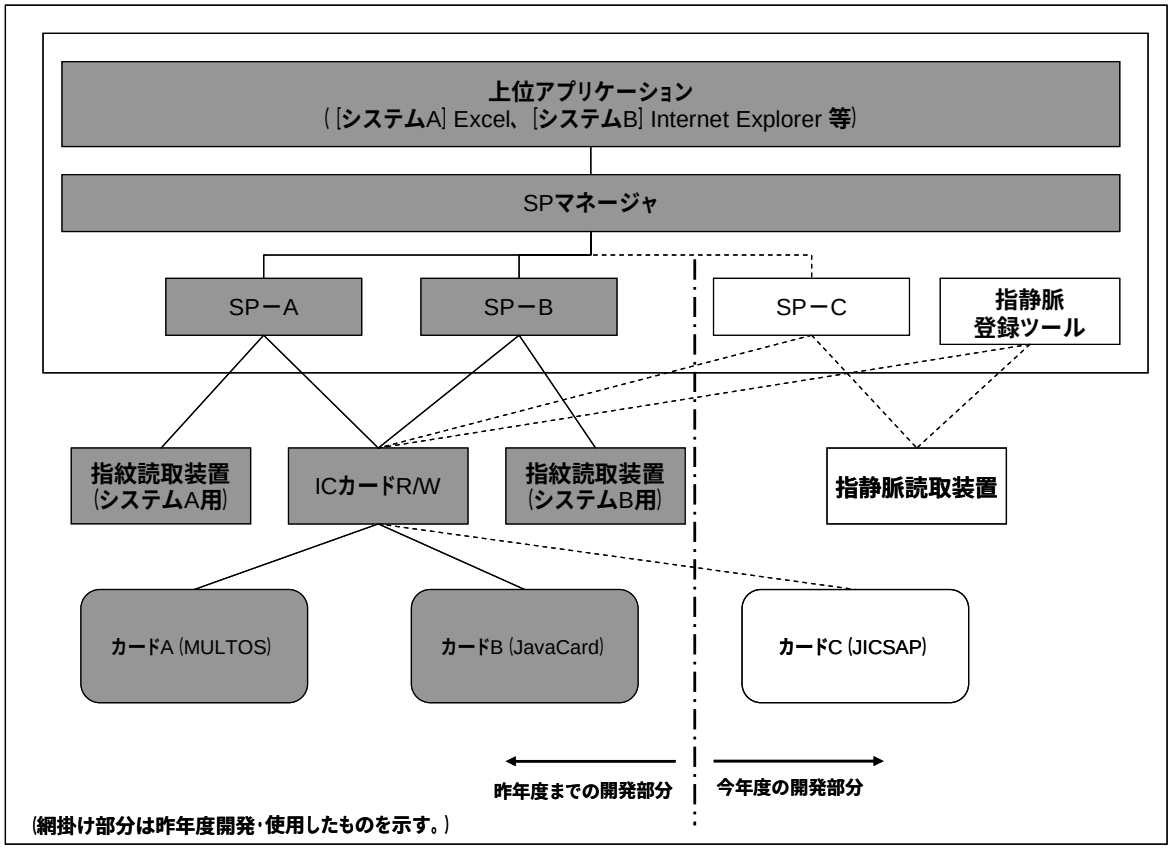


図 3.2.1-2　互換性検証システムのソフトウェアイメージ

指紋と指静脈による認証方式を共存させた簡易認証システムの前提条件を以下に示す。

1) 指紋認証システムの差異を吸収している SP マネージャの仕様、機能はそのままに、指静脈認証用に新たに SP を開発する（SP-C)。
2) 新たに開発する SP のインタフェースは平成 18 年度で開発した SP の仕様と同一とし、上位側への影響を出さない方針とする。
3) 上図のカード A、カード B（指紋認証）はカード内で認証を行うが、カード C については PC 内で認証を行う。

図中にある各項目の詳細を以下に示す。

(A) 上位アプリケーション

生体情報（バイオメトリクス情報）を利用して本人認証を行うアプリケーション。平成 18 年度では、システム A（Excel)、システム B（Web）ともに、SP マネージャとの

インタフェースを取込む改造を行った。

（B）SP マネージャ（サービスプロバイダマネージャ）

下記（C）～（E）の SP（サービスプロバイダ）から受け取った本人認証結果を、上位のアプリケーションに渡すための共通的な API を持ったプログラム。また、SP の切り分けを自動判別する機能を有する。

（C）指紋認証用 SP ＜SP-A＞

指紋読取装置より読み込まれた指紋データを下記（F）のカード A に渡すと同時に、カード A 内のカードアプリケーションで行ったマッチング結果を SP マネージャに渡すプログラム。

（D）指紋認証用 SP ＜SP-B＞

指紋読取装置より読み込まれた指紋データを下記（G）のカード B に渡すと同時に、カード B 内のカードアプリケーションで行ったマッチング結果を SP マネージャに渡すプログラム。

（E）指静脈認証用 SP ＜SP-C＞

下記（H）のカード C に格納された指静脈テンプレートと、指静脈読取装置より読み取った指静脈データとの比較によりマッチングを行い、本人認証結果を SP マネージャに渡すプログラム。

（F）カード A

カード所有者の指紋テンプレートと、専用のアプリケーションを搭載した MULTOS カード。専用のアプリケーションでは、テンプレートと SP-A より送付される指紋データとの照合を行い、SP マネージャを通じてアプリケーションに対し本人認証結果を返す。

（G）カード B

カード所有者の指紋テンプレートと、専用のアプリケーションを搭載した Java カード。専用のアプリケーションでは、テンプレートと SP-B より送付される指紋データとの照合を行い、SP マネージャを通じてアプリケーションに対し本人認証結果を返す。

（H）カード C

専用のフォーマットで、カード所有者の指静脈テンプレートを登録した JICSAP カード。

（I）指静脈登録ツール

指静脈読取装置で読み込まれた指静脈データをカード C にテンプレートとして登録するツール。

3.2.2　互換性検証システムの評価

「3.1.1　互換性検証システムの仕様検討結果」に基づき開発した指紋及び指静脈の双方の認証方式で本人認証を可能とする、互換性検証システムに対しての評価結果を示す。

（1）互換性検証システムの実施日時・目的

互換性検証システムの評価実施の概況を、表 3.2.2-1 に示す。

表 3.2.2-1　互換性検証システムの評価実施概況

日時	平成 20（2008）年 2 月 1 日（金）15：30～16：15
場所	イデア コラボレーションズ株式会社　会議室
目的 （主な評価項目）	（1）互換性検証システムの動作確認 ・指紋のテンプレート登録（カード A、カード B）及び指静脈のテンプレート登録（カード C）をそれぞれ正常に行えること。 ・カード A～カード C による指紋 / 指静脈認証が、システム A、システム B それぞれに対して正常に行えること。 ・指静脈認証対応 SP（SP-C）を追加で拡張したことによって、上位側アプリケーションとの連携に問題がないかどうかを確認する。 （2）指紋 / 指静脈認証方式の違いによる有意差の確認（参考） 同一人物で、指紋 / 指静脈テンプレートの登録（本人認証）を行ったとき、指紋と指静脈のどちらも可能かどうか、あるいは片方のみ可能であったかを確認し、指紋、指静脈の違いによって本人認証に差が出るかどうかの確認を行う。

互換性検証システムの評価で使用した機器一式を図 3.2.2-1 に示す。

図 3.2.2-1 に示すハードウェアイメージの通り、PC-A に対して、カード A、カード B を用いた指紋認証用の指紋読取装置をそれぞれ取り付け、新たに指静脈読取装置を取り付けた。また、PC-A と PC-B をクロスケーブルでつなぐことで、PC-A 上でシステム A（Excel）及びシステム B（Web）の両方のシステムを利用可能とした。

これにより、PC-A 上で、システム A 及びシステム B のどちらも利用可能となり、かつ、どちらのシステムでもカード A～C を用いて指紋 / 指静脈認証が可能となるような構成とした。

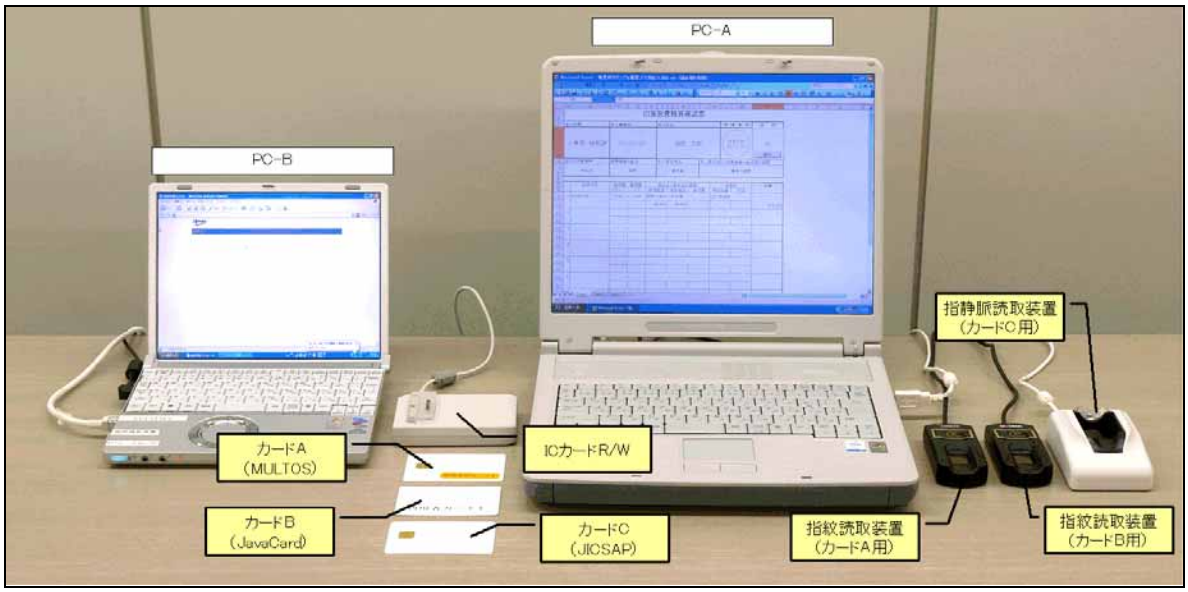


図 3.2.2-1　互換性検証システムの評価で使用した機器一式

(2) 評価項目

互換性検証システムの評価は、大きく「互換性検証システムの動作確認」と、「指紋 / 指静脈認証方式の違いによる登録・認証の有意差の確認」の 2 つの観点で行われた。

「互換性検証システムの動作確認」では、(a) 指紋 / 指静脈データのカード内への登録 (テンプレート登録) が正しく行われること、(b) 本人認証が正しく動作すること、(c) 新規に開発・実装した SP-C によって上位アプリケーションとの連携に問題はないこと、という 3 つの観点を設定した。

「指紋 / 指静脈認証方式の違いによる登録・認証の有意差の確認」とは、同一人物で、指紋 / 指静脈のテンプレート登録及び本人認証をそれぞれ行い、どちらの認証方式でもテンプレート登録・認証が可能かどうか、片方のみ可能であったかどうか、あるいはどちらの認証方式でも不可能であったかどうかのデータをとり、同一人物でも、バイオメトリクスデータの違いによってテンプレート登録や本人認証に差が出るのかどうかの傾向把握を行った。

以下、評価観点ごとに評価項目や確認ポイント等を示す。

（ア）互換性検証システムの動作確認

（a）登録

カード A～C について、それぞれ指紋 / 指静脈データのテンプレート登録が正しく行われることを確認する。

表 3.2.2-2　互換性検証システムの評価項目表（テンプレート登録）

評価項目	結果
指紋テンプレートの登録（カード A）	1-1
指紋テンプレートの登録（カード B）	1-2
指静脈テンプレートの登録（カード C）	1-3

（b）認証

カード A～C それぞれについて、システム A 及びシステム B 双方での本人認証が正しく行われることを確認する。

確認項目は、カードとシステムの組合せにより表 3.2.2-3 に示す通りとなる。

なお、平成 17 年度事業では、表中の 2-1 及び 2-4 のみのパターン（システム A（システム B）の本人認証に対してはカード A（カード B）のみを用いる）であったが、平成 18 年度でカード A（カード B）からシステム B（システム A）の指紋認証を可能とするシステムを開発した（表中の 2-2 及び 2-3)。さらに今年度では、両システムについて指紋に加え指静脈による本人認証を可能とするシステムを開発した(表中の 2-5 及び 2-6)。

表 3.2.2-3　互換性検証システムの評価項目表（本人認証）

		システム A	システム B
カード	カード A（MULTOS）［指紋認証］	2-1	2-2
	カード B（JavaCard）［指紋認証］	2-3	2-4
	カード C（JICSAP）［指静脈認証］	2-5	2-6

（c）上位アプリケーションとの連携

SP-C を新たに開発・実装したことによって上位アプリケーションへの影響がないことを確認する。

具体的には、システム A では Excel 帳票ファイルの OPEN / CLOSE、書き込み、保存などが正しく行えること、システム B では入力フォームによる申請書の登録や申請状

況の確認、管理者機能によるユーザ登録・更新などが正しく行えることを確認する。

表 3.2.2-4　互換性検証システムの評価項目表
（上位アプリケーションとの連携）

評価項目	結果
［システム A］ Excel 帳票が正しく動作すること。	3-1
［システム B］ Web アプリケーションが正しく動作すること。	3-2

（イ）指紋 / 指静脈認証方式の違いによる登録・認証の有意差の確認

表 3.2.2-5 に示す通り、指紋、指静脈それぞれについて、テンプレート登録及び本人認証を同一人物（被験者）で行い、どちらの認証方式でも可能かどうか、あるいは片方のみ可能であったか、両方とも不可能であったかどうかの確認を行う。これにより、同一人物でも認証に使用するバイオメトリクス情報の種類によって、テンプレート登録や本人認証の成否に差が出るのかどうかの傾向把握を行う。

表 3.2.2-5　指紋 / 指静脈による登録・認証確認表

被験者 ID.	指紋（カード A）		指静脈（カード C）	
	登録	認証	登録	認証
1				
2				
3				
4				
5				
6				
7				
8				

（3）評価結果

互換性検証システムの評価結果を示す。

（ア）互換性検証システムの動作確認

（a）登録

カード A～C における指紋 / 指静脈データのテンプレート登録結果を表 3.2.2-6 に示す。

表 3.2.2-6 の通り、カード A～C に対するそれぞれのテンプレートは正常に登録された。

表 3.2.2-6　互換性検証システムの評価結果（テンプレート登録）

評価項目	結果
指紋テンプレートの登録（カード A）	1-1　OK
指紋テンプレートの登録（カード B）	1-2　OK
指静脈テンプレートの登録（カード C）	1-3　OK

なお、カード A～C の指紋 / 指静脈テンプレートが正常に行われた様子の画面を以下に示す。

（i）カード A における指紋テンプレートの登録（1-1）

カード A における指紋登録及び登録完了画面を図 3.2.2-2～図 3.2.2-4 に示す。指紋の読み取りを 5 回行い、テンプレート登録が完了すると登録を完了した旨のウインドウが表示される。

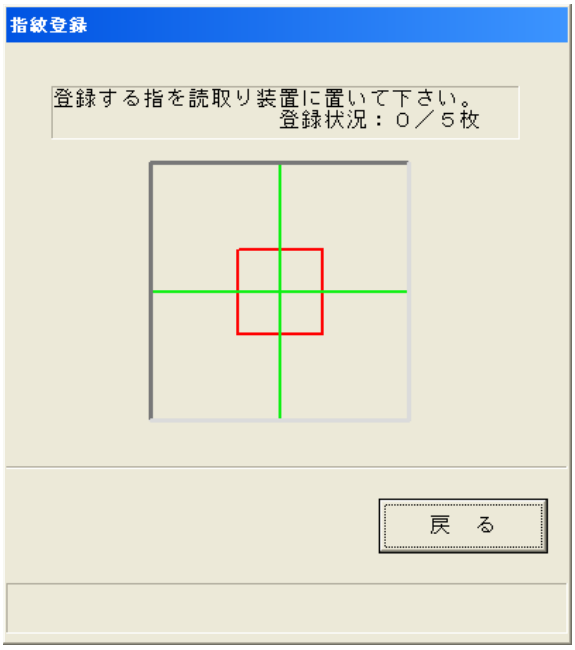


図 3.2.2-2　カード A における指紋テンプレートの登録画面（1/3）

図 3.2.2-3　カード A における指紋テンプレートの登録画面（2/3）

図 3.2.3-4　**カード** A **における指紋テンプレートの登録画面**（3/3）

（ii）カード B における指紋テンプレートの登録（1-2）

カード B における指紋登録及び完了画面を図 3.2.2-5 及び図 3.2.2-6 に示す。指紋の読み取りを 2 回行い、テンプレート登録を完了すると「認証情報を IC カードに登録しました」のメッセージが表示される。

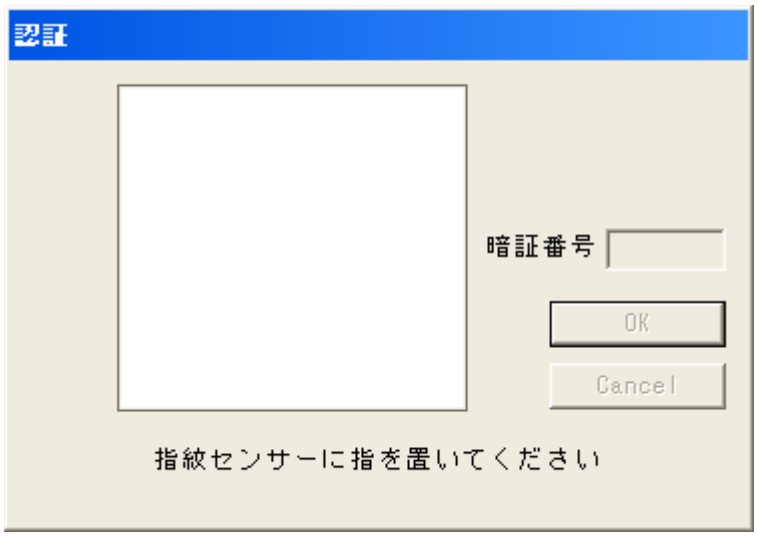


図 3.2.2-5　カード B における指紋テンプレート登録画面（1/2）

図 3.2.2-6　カード B における指紋テンプレート登録画面（2/2）

（iii）カード C における指静脈テンプレートの登録（1-3）

カード C における指静脈テンプレート登録画面を以下に示す。指静脈登録ツールで［指静脈読み取り］ボタンをクリックすると、指静脈テンプレートの登録画面が表示される。

図 3.2.2-7　カード C における指静脈テンプレートの登録（1/5）

指静脈の登録画面を図 3.2.2-8～図 3.2.2-11 に示す。

図 3.2.2-8　カード C における指静脈テンプレートの登録（2/5）

登録が成功指静脈の登録は 3 回[9]行われる。1 回目の登録が成功すると、図 3.2.2-9 に示す画面が表示され、2 回目の指静脈読み取りが行われる。

図 3.2.2-9　カード C における指静脈テンプレートの登録（3/5）

図 3.2.2-10 は、2 回目の読み取りが完了し、3 回目の読み取りを促す画面を示したものである。

図 3.2.2-10　カード C における指静脈テンプレートの登録（4/5）

[9] 指静脈登録ツールの設定による。今回の互換性検証システムにおける指静脈ツールの設定では、3 回と設定している。

指静脈の読み取りを 3 回行い、指静脈登録ツールの［登録］ボタンをクリックすると、図 3.2.2-11 に示す通り、登録を完了する画面が表示されることを確認した。

図 3.2.2-11　**カード C における指静脈テンプレートの登録**（5/5）

（b）認証

カード A～C それぞれにおける、システム A 及びシステム B 双方での本人認証結果を表 3.2.2-7 に示す。

表 3.2.2-7 の通り、カード C によるシステム A、システム B の指静脈認証（表中の 2-5 及び 2-6）をはじめとし、カード A とカード B の指紋認証における IC カードの互換性が確保されたこと（表中の 2-2 及び 2-3）の確認を行い、カードとシステムの組合せで行った本人認証結果については、すべてのケースで正常に行われたことを確認した。

表 3.2.2-7　互換性検証システムの評価結果（本人認証）

		システム A	システム B
カード	カード A（MULTOS） ［指紋認証］	2-1　OK	2-2　OK
	カード B（JavaCard） ［指紋認証］	2-3　OK	2-4　OK
	カード C（JICSAP） ［指静脈認証］	2-5　OK	2-6　OK

なお、カードとシステムの組合せで行った指紋 / 指静脈による本人認証（表中の 2-1～2-6）の画面をそれぞれ以下に示す。

（i）カード A によるシステム A の指紋認証（2-1）

カード A によるシステム A の指紋認証結果画面を図 3.2.2-12 に示す。指紋による本人認証が正常に行われたことを確認した。なお、本ケースは平成 17 年度の開発範囲である。

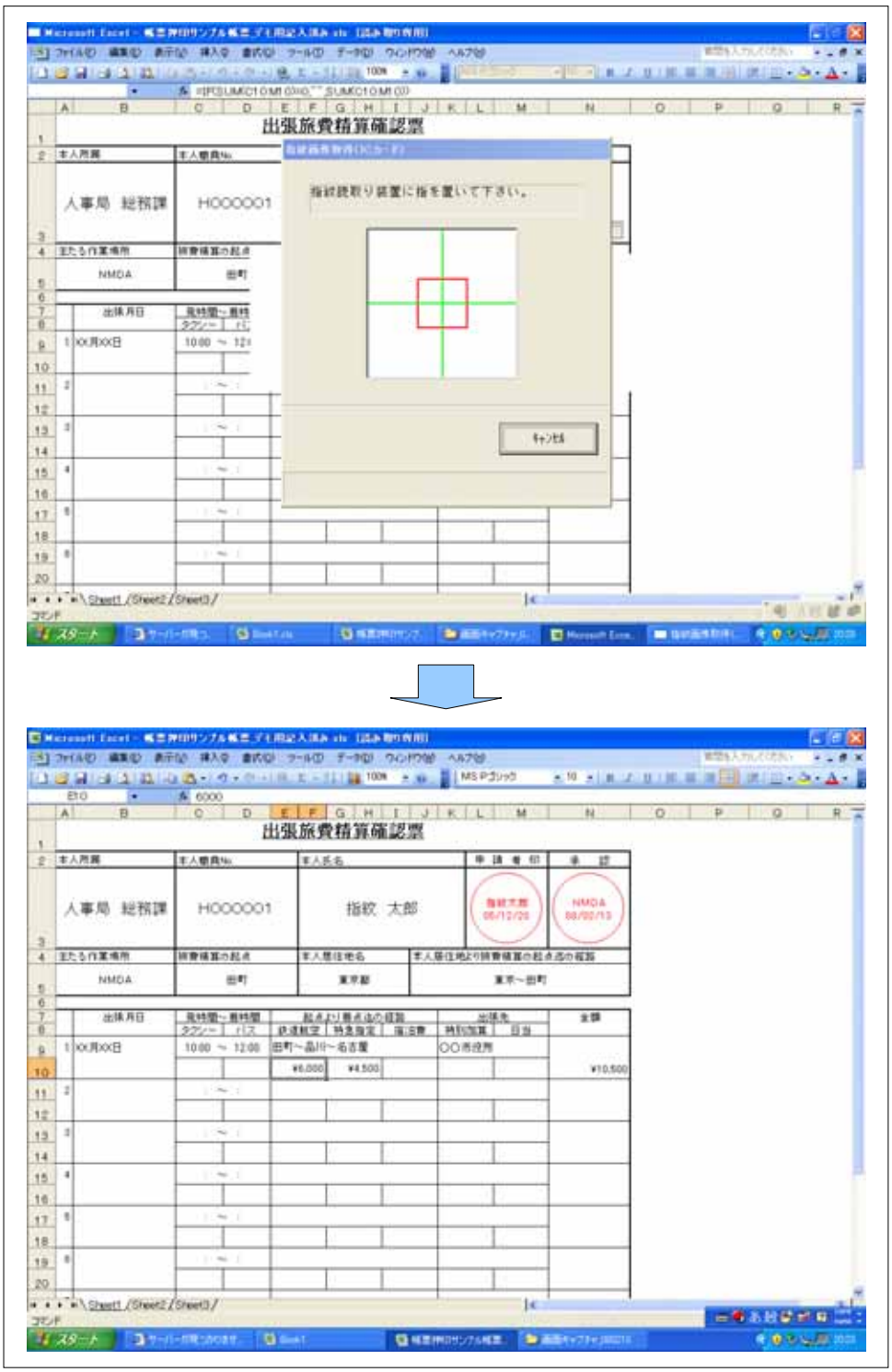


図 3.2.2-12　カード A によるシステム A の本人認証結果画面（指紋認証）

（ii）カード A によるシステム B の指紋認証（2-2）

カード A によるシステム B の指紋認証結果画面を図 3.2.2-13 に示す。指紋による本人認証が正常に行われたことを確認した。なお、本ケースは、平成 18 年度の開発範囲である。

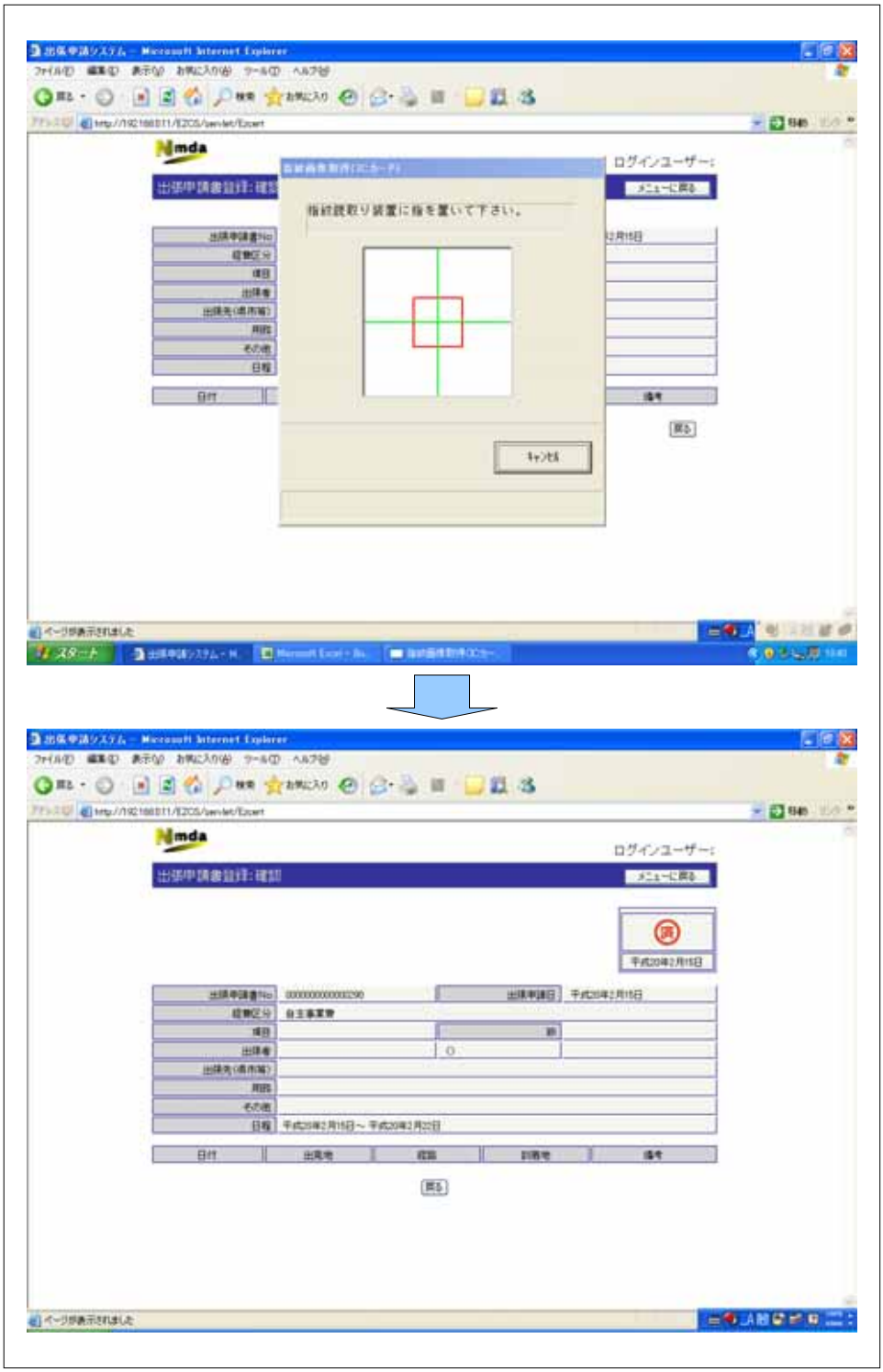


図 3.2.2-13　カード A によるシステム B の本人認証結果画面（指紋認証）

（iii）カード B によるシステム A の指紋認証（2-3）

カード B によるシステム A の指紋認証結果画面を図 3.2.2-14 及び図 3.2.2-15 に示す。指紋による本人認証が正常に行われたことを確認した。なお、本ケースは平成 18 年度の開発範囲である。

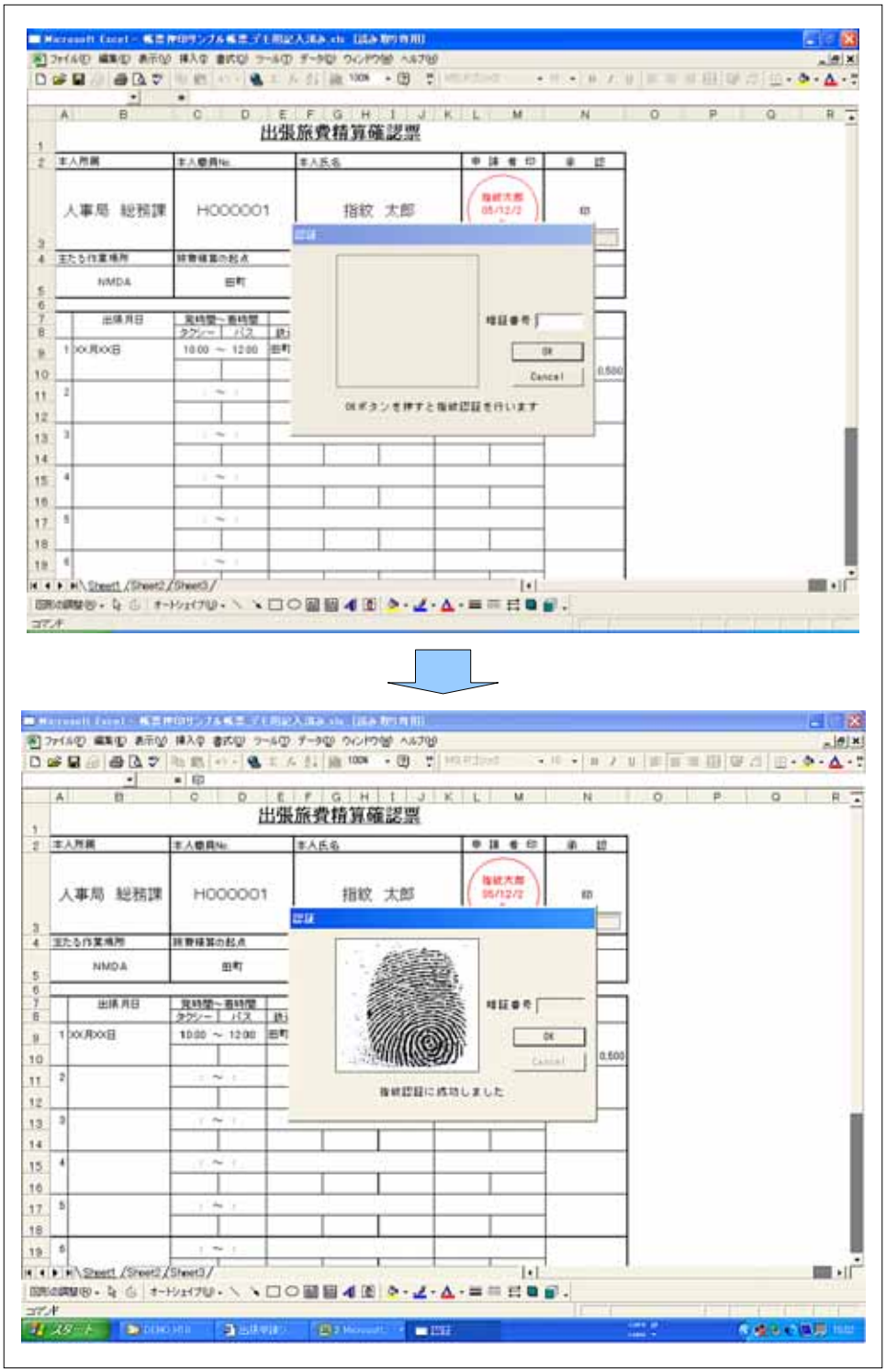


図 3.2.2-14　カード B によるシステム A の本人認証結果画面（指紋認証）（1/2）

図 3.2.2-15　**カード** B **によるシステム** A **の本人認証結果画面（指紋認証）**（2/2）

（iv）カード B によるシステム B の指紋認証（2-4）

カード B によるシステム B の指紋認証結果画面を図 3.2.2-16 及び図 3.2.2-17 に示す。指紋による本人認証が正常に行われたことを確認した。なお、本ケースは平成 17 年度の開発範囲である。

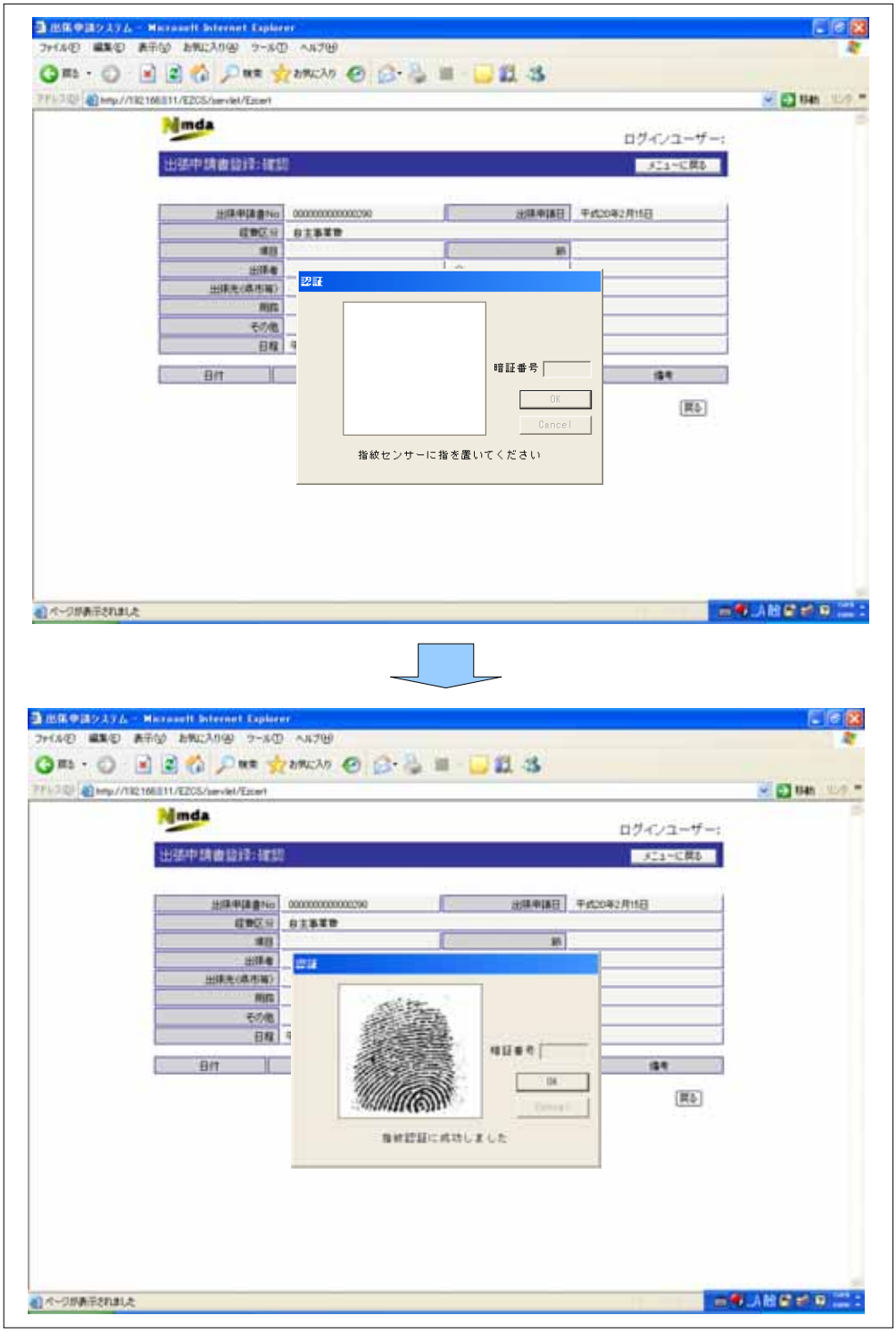


図 3.2.2-16　カード B によるシステム B の本人認証結果画面（指紋認証）（1/2）

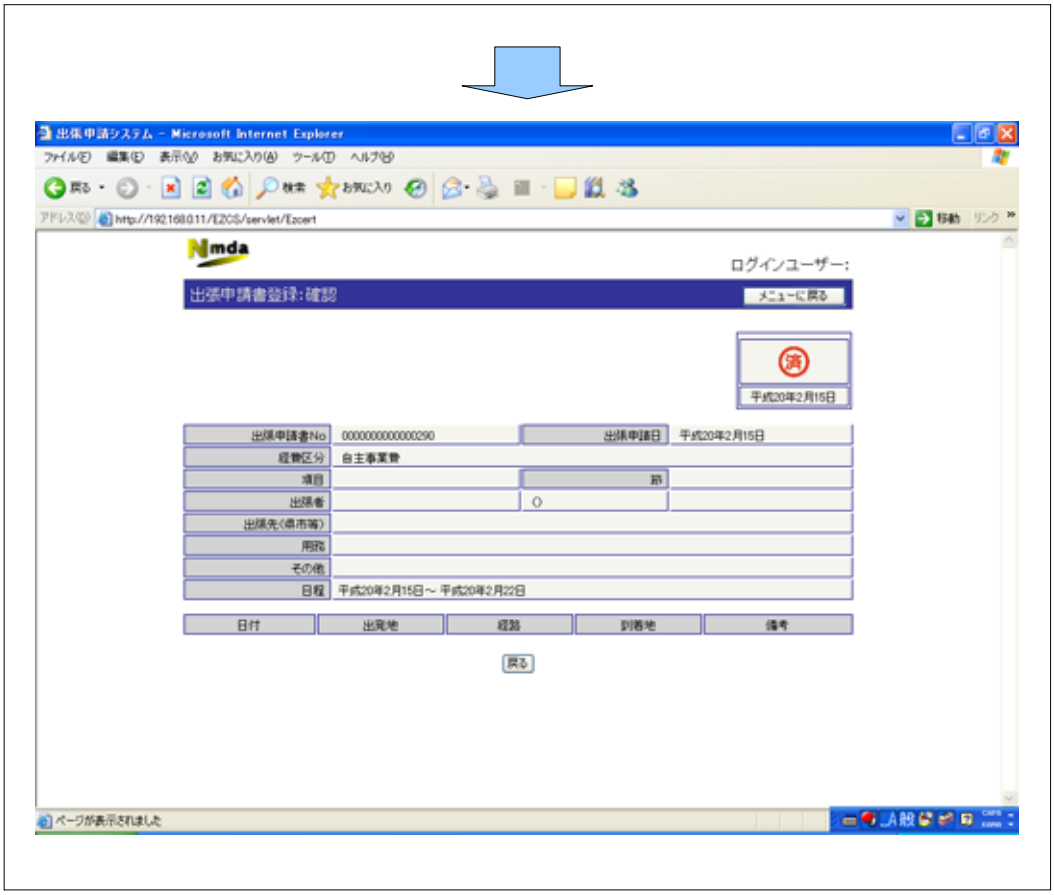


図 3.2.2-17　**カード** B **によるシステム** B **の本人認証結果画面（指紋認証）**（2/2）

（v）カード C によるシステム A の指静脈認証（2-5）

カード C によるシステム A の指紋認証結果画面を図 3.2.2-18 に示す。指静脈による本人認証が正常に行われたことを確認した。なお、本ケースは本年度の開発範囲であり、計画通りの結果となることが確認できた。

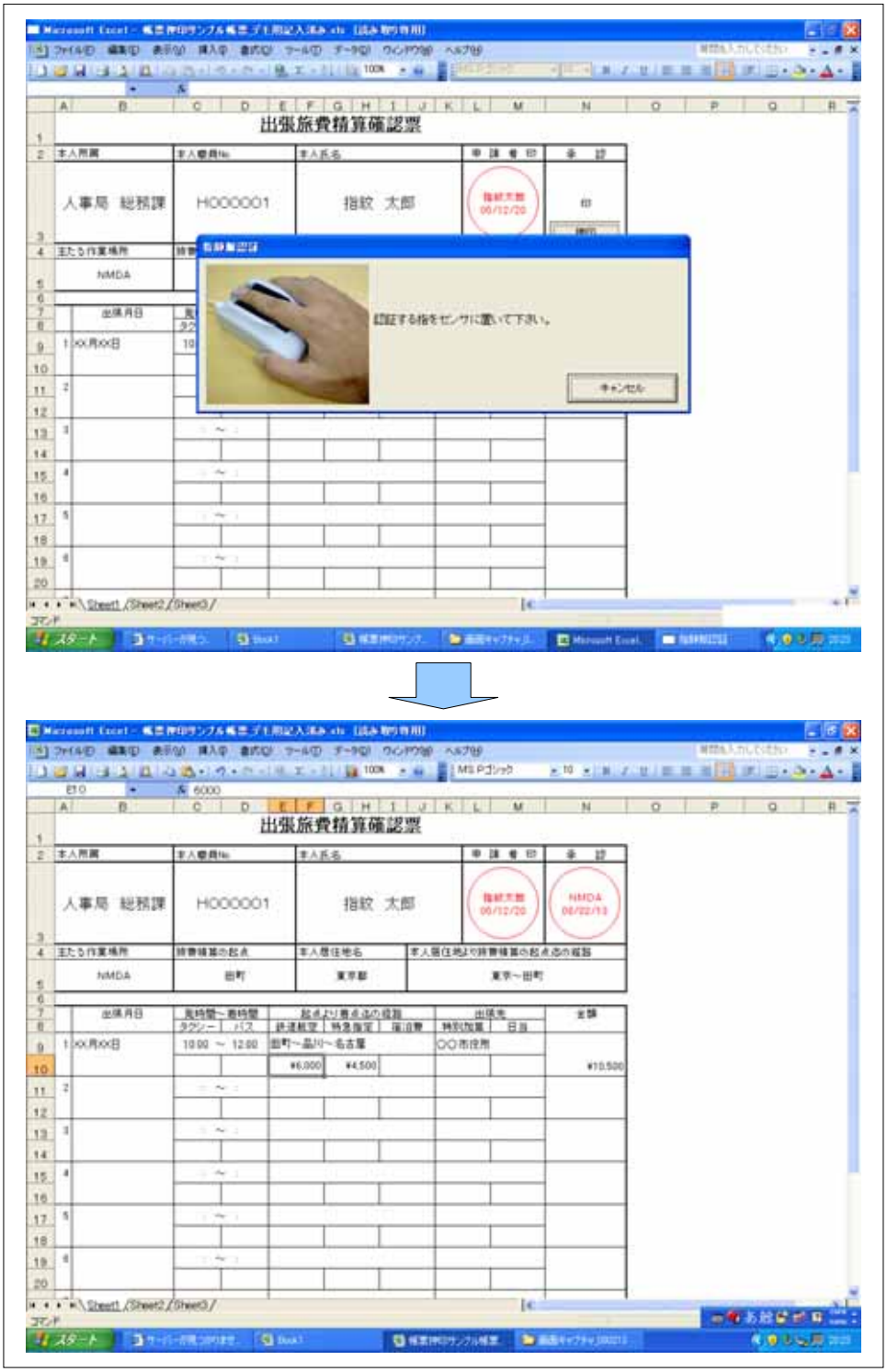


図 3.2.2-18　カード C によるシステム A の本人認証結果画面（指静脈認証）

（vi）カード C によるシステム B の指静脈認証（2-6）

カード C によるシステム B の指紋認証結果画面を図 3.2.2-19 に示す。指静脈による本人認証が正常に行われたことを確認した。なお、本ケースは本年度の開発範囲であり、計画通りの結果となることが確認できた。

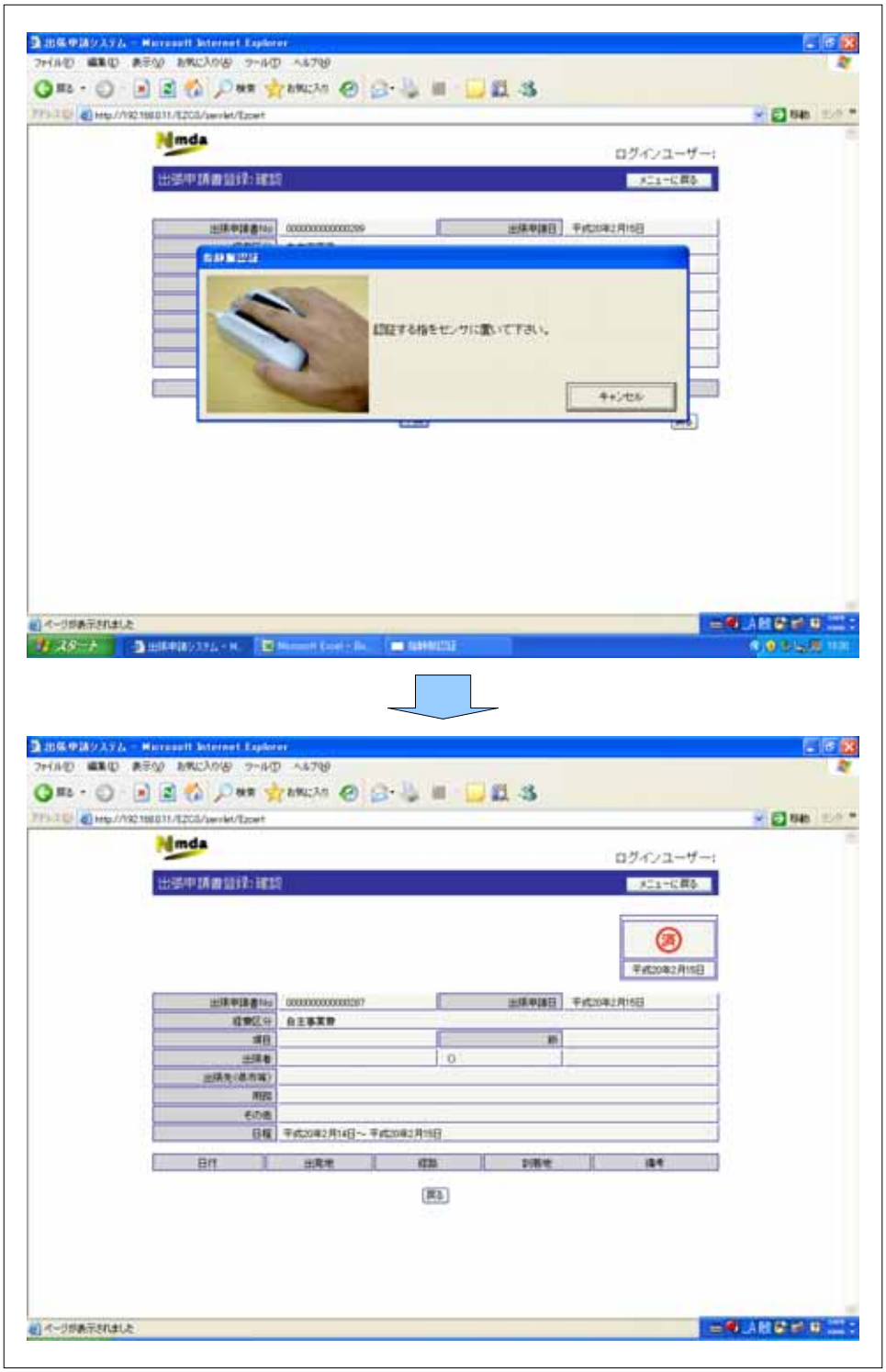


図 3.2.2-19　カード C によるシステム B の本人認証結果画面（指静脈認証）

（c）上位アプリケーションとの連携

SP-C を新たに開発・実装したことによる上位アプリケーションへの影響結果を表 3.2.2-8 の通り示す。

表 3.2.2-8　互換性検証システムの評価項目表
（上位アプリケーションとの連携）

評価項目	結果
［システム A］ Excel 帳票が正しく動作すること。	3-1　OK
［システム B］ Web アプリケーションが正しく動作すること。	3-2　OK

評価項目 3-1 については、Excel の帳票の入力や、指紋 / 指静脈認証による決裁が行われ押印がされたファイルの保存、一端保存したファイルの再 OPEN を行ったが、いずれも動作上の問題点などは特に発見されず、正常にシステム A が動作することを確認した。

評価項目 3-2 については、Web ブラウザからの出張申請書の登録や承認、指紋 / 指静脈認証による決裁が行われた後の出張申請承認状況画面でステータスが適切に変わっているかどうか、出張申請書 No.がシーケンスで自動付与されているかなどの確認、管理者機能によるユーザ情報の入力、更新を行ったが、いずれも動作上の問題点などは特に発見されず、正常にシステム B が動作することを確認した。

（イ）指紋 / 指静脈認証方式の違いによる登録・認証の有意差の確認

参考として、指紋 / 指静脈それぞれについて、テンプレート登録及び本人認証を同一人物（被験者）で行った。結果を表 3.2.2-9 に示す

表 3.2.2-9　指紋 / 指静脈による登録・認証確認表

被験者 ID.	指紋（カード A）		指静脈（カード C）	
	登録	認証	登録	認証
1	OK	OK	OK	OK
2	OK	OK	OK	OK
3	OK ※1	OK ※2	OK	OK ※5
4	OK ※3	OK ※4	OK	OK
5	OK	OK	OK	OK
6	OK	OK	OK	OK
7	OK	OK	OK	OK

［備考］

※1［指紋テンプレート登録］
2 回目の登録で正常に登録を完了した。

※2［指紋認証］
5 回本人認証を行ったがいずれも失敗に終わった。6 回目の認証で成功した。

※3［指紋テンプレート登録］
右手人差し指で登録を 2 回行ったがいずれも失敗に終わった。指を変え、右手中指で登録を行うと正常に完了した（3 回目）。

※4［指紋認証］
2 回本人認証を行ったが、いずれも失敗に終わった。3 回目の認証で成功した。

※5［指静脈認証］
2 回目の認証で成功した。

表 3.2.2-9 に示す通り、被験者が少ないため得られた結果から全体の傾向を類推することはできないが、同一人物で、指紋テンプレートの登録と本人認証、指静脈テンプレートの登録と本人認証のどちらも正常に行われたことを確認した。

ただし、一部では、テンプレートの登録あるいは認証を、何度か繰り返して行うことにより成功するケースがあった。例えば、指紋テンプレートの登録では 7 名中 2 名が、指紋による本人認証では 7 名中 2 名が何回かエラーとなり、再試行を余儀なくされることがあった。一方、指静脈の認証では、7 名中 1 名が再試行を行った。

4.　今後の課題、まとめ

本章では、本事業で得られた課題と成果について述べる。

4.1　課題

（1）指静脈認証、指紋認証以外の機能を持った IC カードと上位アプリケーションの連携

指静脈認証、指紋認証双方の認証方式の互換性の確保により、システムの利便性、柔軟性が高まったことが挙げられると同時に、今後は、「指紋認証（指静脈認証）以外の機能を持った IC カード」と、「指紋認証（指静脈認証）双方の認証方式の利用が可能なアプリケーション、システム」との互換性に関する組合せも想定される。

このとき、指紋認証（指静脈認証）以外の機能を持つ IC カードを利用するための方策を検討する必要がある。

（2）認証デバイス（指紋 / 指静脈読取装置、IC カード R/W）が物理的に必要

指静脈認証と指紋認証方式のどちらも利用可能とする簡易認証システムにおいて、本事業で開発した互換性検証システムのハードウェア構成は、指静脈読取装置と指紋認証読取装置をそれぞれ 1 台必要とする構成であった。なお、昨年度同様、IC カード R/W は共通で使えることが分かった。（図 4.1-1）

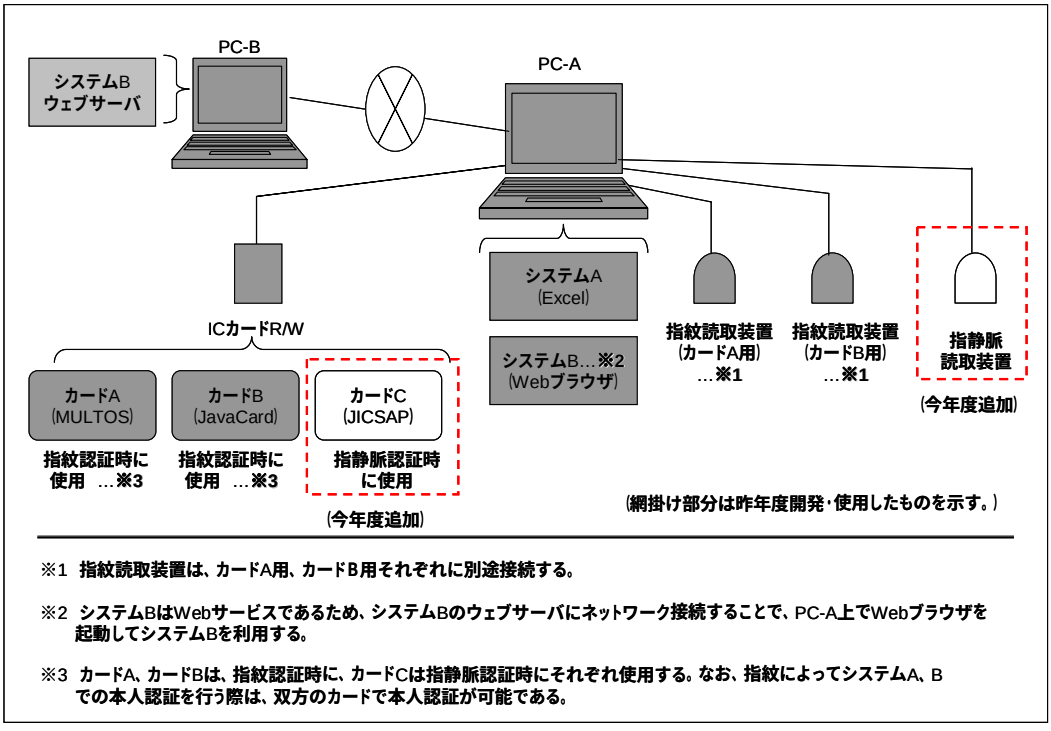


図 4.1-1　互換性検証システムのハードウェアイメージ（図 3.2.1-1 の再掲）

このように、一つのシステムやアプリケーションにおいて、本人認証方式を拡張するごとに、それぞれの認証方式に対応した認証デバイス（読取装置、IC カード R/W）が物理的に必要となる構成となることが課題の一つといえる。加えて、昨年度でも挙げられた課題ではあるが、同じ認証方式（指紋認証）でも、それぞれのシステムで使用している指紋読取装置のデバイスドライバに互換性がないことにより、それぞれのシステムに対応した指紋読取装置を物理的に必要とする結果となった。

図 4.1-2 は、互換性検証システムの汎用的なイメージを示したものである。

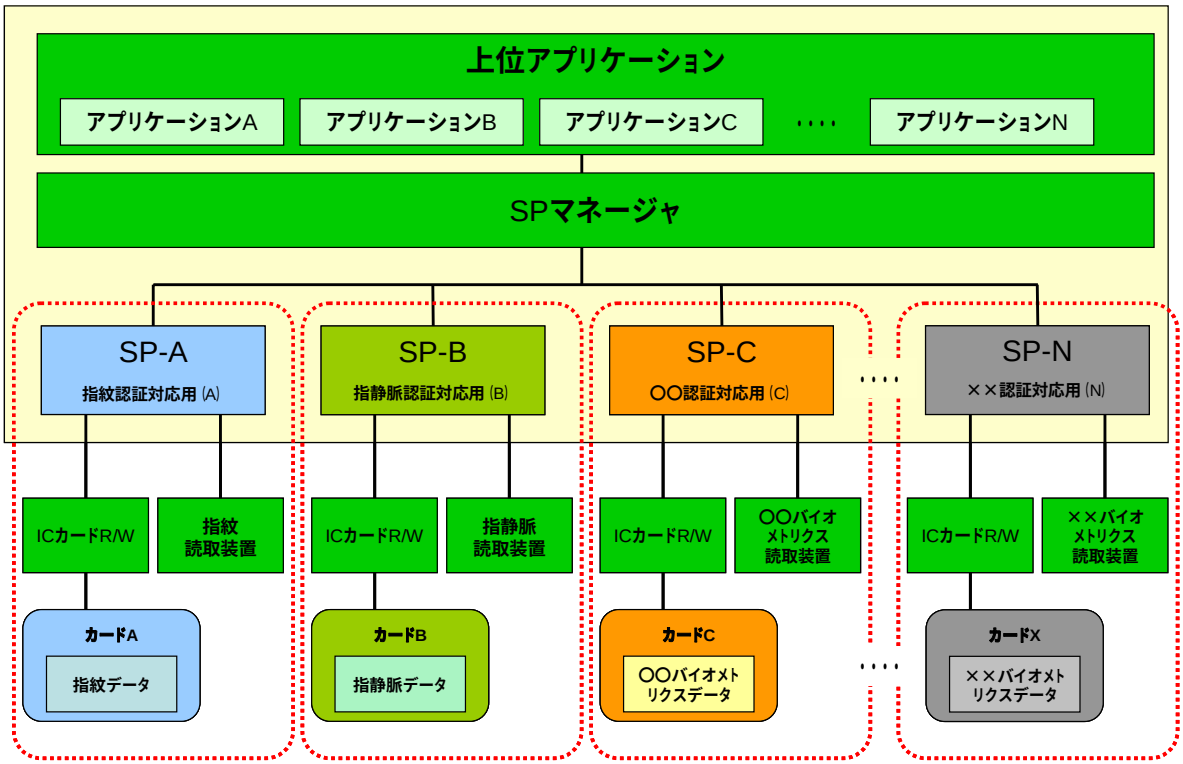


図 4.1-2　互換性検証システムの汎用イメージ

今後、一つのシステムやアプリケーションで、異なる認証方式や同じ認証方式でも IC カードの互換性の確保を実現させたシステムを構築するにあたっては、認証デバイスをいかに共通的に使うことができるかが課題となる。

（3）SP の技術的な課題

今回開発したシステム構成では、本人認証方式の違いに応じて SP の数が増えることに対応する仕組みとなっている。このとき、現状では、SP が IC カードの AID を順次参照し、その SP が利用できる IC カードである場合、新たなセッションを確立する仕組みとなっている。（図 4.1-3）

このとき、今後、SP が増えると、順次 IC カード内の AID を参照することにより処理に時間を要する可能性があるため、システムの利便性を確保しつつ認証方式の拡張を行う上では、別の仕組みを考慮する必要がある。

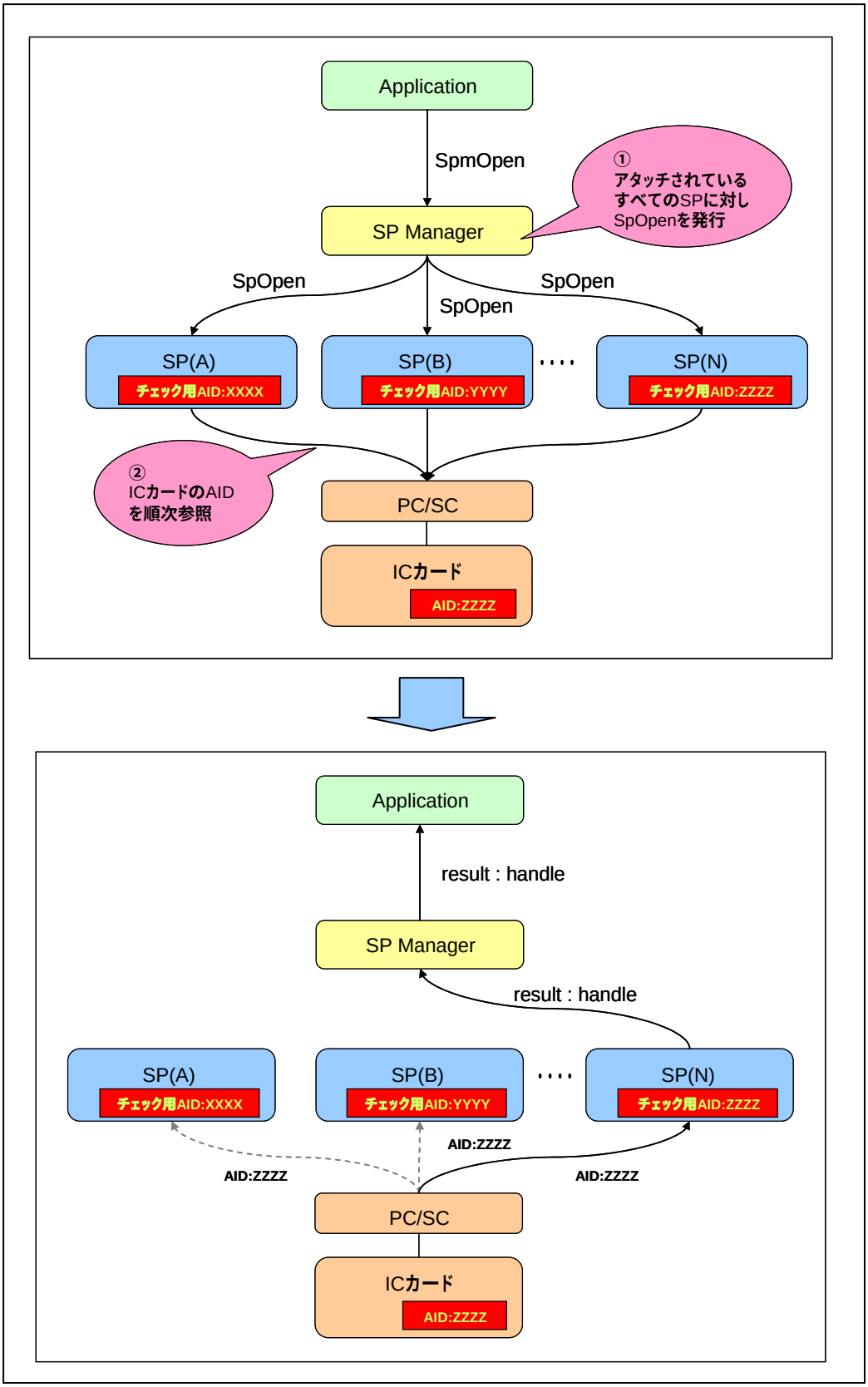


図 4.1-3　SP の AID 参照イメージ図

4.2 成果

バイオメトリクス認証技術は、従来、施設における物理的なアクセス制御の分野に限定し展開されてきた。入退室管理など物理的アクセス制御では、データの機密性、正当性などのセキュリティ要件の確保は、装置単体で考慮すればよかった。しかし、近年、情報システムへのバイオメトリクス認証装置の利用の拡大により、ネットワーク上でのセキュリティ装置、多数の利用者へのサービスなどの観点での展開が期待できると考えられる。また、施設管理から個人情報管理への利用（市場）がシフトしている。例えば、医療福祉介護カードなどの社会コミュニティ、ガス・電気・生命保険などの分野におけるフィールドサービスコミュニティなどにおいて多数の利用者が、広域にわたり IC カードやモバイル端末などを利用するシステムにバイオメトリクス認証が適用される。

本事業で実施した指静脈による本人認証の適用モデル調査（「3.1.2 指静脈認証を用いた本人認証の適用モデルの調査」参照）では、オフィスの入退室管理での適用に限らず、PC ログインやオフィス内プリンタの印刷等の認証で指静脈認証方式を採用した製品やシステム、あるいは、指静脈認証システムを企業の基幹システムに取り入れたりするなどの事例を取り上げ、従来の ID/Password 方式に比べてよりセキュリティが強化されるとともに、指にかざすだけでより容易に認証ができることによって業務効率化を図れるなど、ニーズの高さが確認された。また、指静脈認証による標準化状況調査（「3.1.1　指静脈認証による本人認証方式の標準化状況調査」参照）では、2007 年 3 月に血管（静脈）の画像データのフォーマットの国際標準規格が発行され、指紋に続いて指静脈による本人認証技術の重要性も確認された。

このような背景のなか、本事業を通じて得られた開発モデル、開発事例は先進事例として扱われる可能性を秘めたものといえる。

つまり、一つのシステム、アプリケーションで、利用者の生体情報である「指紋」と「指静脈」をそれぞれ対応する IC カードに登録し、その双方のカードのどちらを使っても本人認証が可能となるデモシステム（互換性検証システム）の開発を実現したことにより、異なる認証方式の互換性を確保した開発モデル、開発事例の一つを本事業で示すことができた。これに加えて、昨年度（平成 18 年度）に開発した指紋認証の機能を持った IC カードの互換性の確保とあわせると、IC カードの互換性と、認証方式の互換性のどちらも確保した簡易認証システムを実現させたことになる。

今後企業部門内において、ある会計システムの決裁では指紋をテンプレートとして搭載した IC カードを用いて本人認証を行う指紋認証方式を採用し、入退室管理では指静脈テンプレートとして搭載した IC カードを用いて指静脈認証方式を採用したシステムの双方があり、一枚の IC カードでどちらのシステムも利用可能としたい、あるいはどちらのカードでも双方のシステムを使いたいといったニーズや、IC カードの統合化、拡張化に対応したビジネスモデルなどが考えられた場合、本事業を通じて得られた成果が先進事例の一つとなることも想定される。

また、本事業の成果は、マルチモーダルバイオメトリクス認証技術分野での足がかりの一つとなったのではないかと考えられる。マルチモーダルバイオメトリクス認証技術

とは、指紋、静脈、署名、顔、声紋などのバイオメトリクスを 2 つ以上用い、各バイオメトリクスの照合結果を用いて、融合判定により総合的に個人の識別を行う。例えば、セキュリティレベルに応じて、指紋と指静脈のどちらの認証も通さないとシステムやアプリケーションの操作や権限がおりない、といった利用モデルも考えられ、より強固なセキュリティを確保したシステム、アプリケーションなどが考えられると、本事業で得られた成果を適用することが可能である。また、指紋認証、指静脈認証の双方の認証技術を共存させたシステムの実現により、利用者はシステムによって一つの認証方式の制約を受けずに、自身の好みの認証方式を選択する権利が与えられることにもなり、システムやアプリケーションの利便性や柔軟性を高めることができると考えられる。

以上

5. 参考文献

［1］ 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、財団法人ニューメディア開発協会、2005 年
［2］ 平成 18 年度　バイオメトリクスによる簡易認証システムの互換性に関する調査・開発　調査開発報告書、財団法人ニューメディア開発協会、2006 年
［3］ 瀬戸洋一：ユビキタス時代のバイオメトリクスセキュリティ、日本工業出版（2003）

6. 添付資料

添付資料の一覧を、表 6-1 に示す。

表 6-1　調査開発報告書　別紙添付資料

No.	添付資料名
資料 1	互換性検証システム　インタフェース仕様書
資料 2	互換性検証システム 指静脈認証用 SP　取扱説明書

添付資料１

互換性検証システム　インタフェース仕様書

平成 19 年度

「多種類のバイオメトリクス簡易認証

システムの調査・開発」

互換性検証システム　インタフェース仕様書

平成 20 年 3 月

イデア コラボレーションズ株式会社

目　次

1. 概要

指紋や指静脈などのバイオメトリクス情報をテンプレートとして登録したICカードを用いて本人認証を行うにあたり、一枚のICカードで異なるシステムへの本人認証を可能としたり、一つのシステム内で、異なるバイオメトリクス情報でも本人認証を可能とする「互換性検証システム」を開発します。

互換性検証システムは、「SP（サービスプロバイダ）」及び「SPマネージャ」と呼ばれるプログラムを開発・実装して行うことで実現します。

図1-1は、互換性検証システムのシステムイメージを示したものです。

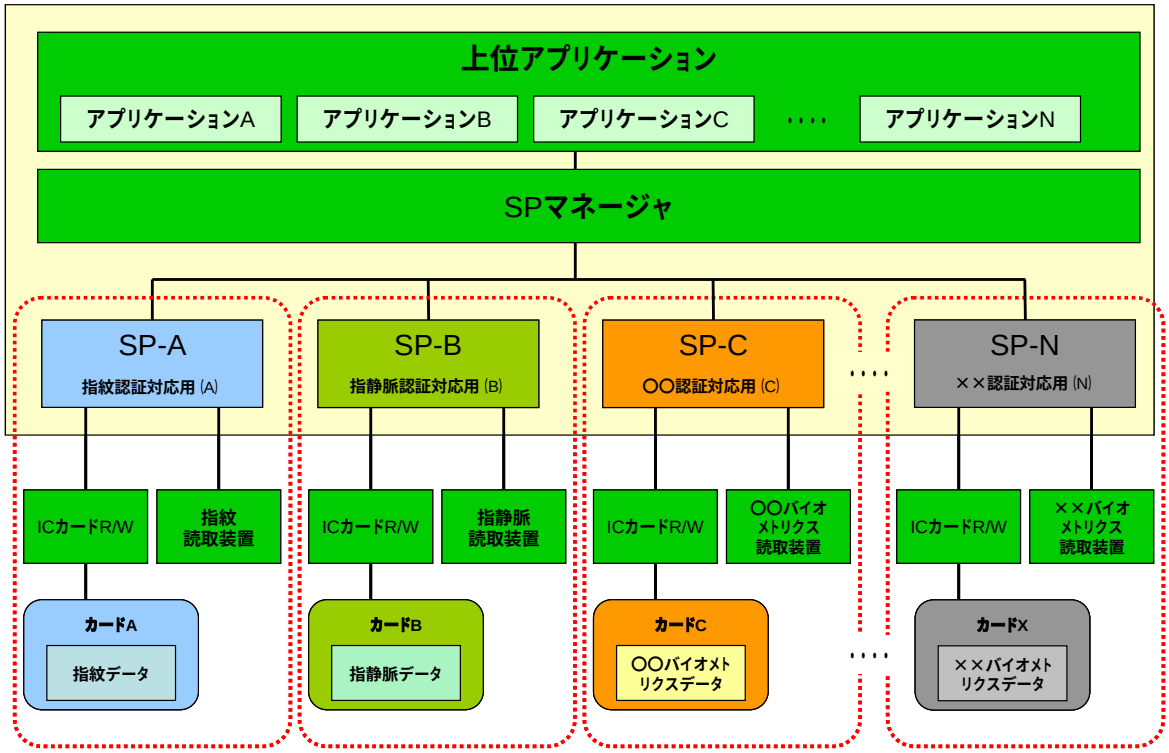


図1-1　互換性検証システムイメージ

この互換性検証システムの具体的な動きは以下の通りです。詳細は、「2.　動作モデル」の図2-1　互換性検証システムのシーケンス図を参照願います。

（1）カードアプリケーション内でマッチング（照合）を行う場合

① ICカードをICカードR/Wにかざした時に、SPマネージャで対象カードの利用可能なSPを選択する。

② （指紋、指静脈等の）読取装置から読み込まれた情報を、SPにてカードアプリケーションに渡す。

③ SPより受け取った情報とテンプレートのマッチング（照合）をカードアプリケー

ション内で行い、SP マネージャに本人認証結果を返す。

④ SP マネージャで受け取った本人認証結果をアプリケーションに返す。

(2) SP 内でマッチング（照合）を行う場合

① IC カードを IC カード R/W にかざした時に、SP マネージャで対象カードの利用可能な SP を選択する。

② （指紋、指静脈等の）読取装置から読み込まれた情報と、テンプレートのマッチング（照合）を SP 内で行う。

③ SP マネージャで受け取った本人認証結果をアプリケーションに返す。

なお、この仕組みを取り入れることにより、例えば以下のようなシステムの実現が可能となります。[1]

- 自システムとは異なるシステムで使用している IC カード(指紋認証方式)を使って、自システムの本人認証が可能となる。他システムにも同様の仕組みが実装されていると、一枚の IC カードで双方のシステムの認証が可能となる。また、例えば、同一の PC 内で、アプリケーションの違いによって IC カードを使い分けているケースなどでも、双方の IC カードで双方のアプリケーションの本人認証が可能となる。(IC カードの互換性確保)
- 指紋認証方式による本人認証、指静脈認証方式による本人認証、どちらの認証も使うことができ、利用者は好みに応じたバイオメトリクス認証の選択が可能となる。(バイオメトリクス認証の互換性確保)

本仕様書は、上記に示した「互換性検証システム」を開発するにあたり、アプリケーションと SP マネージャ及び SP マネージャと SP のインタフェース仕様を定めたものです。

[1] 平成 18 年度では、一枚の IC カードで自システムの指紋認証及び他システムの指紋認証を可能とする互換性検証システムを開発しました。平成 19 年度では、指紋情報をテンプレートとして登録した IC カードと、指静脈情報をテンプレートとして登録した IC カードのどちらのカードを用いても本人認証を可能とする互換性検証システムを開発します。

2. 動作モデル

「互換性検証システム」のシーケンス図を以下の通り示します。

なお、SP－PC/SC、及び、SP－指紋 Driver 間は SP 依存となります。

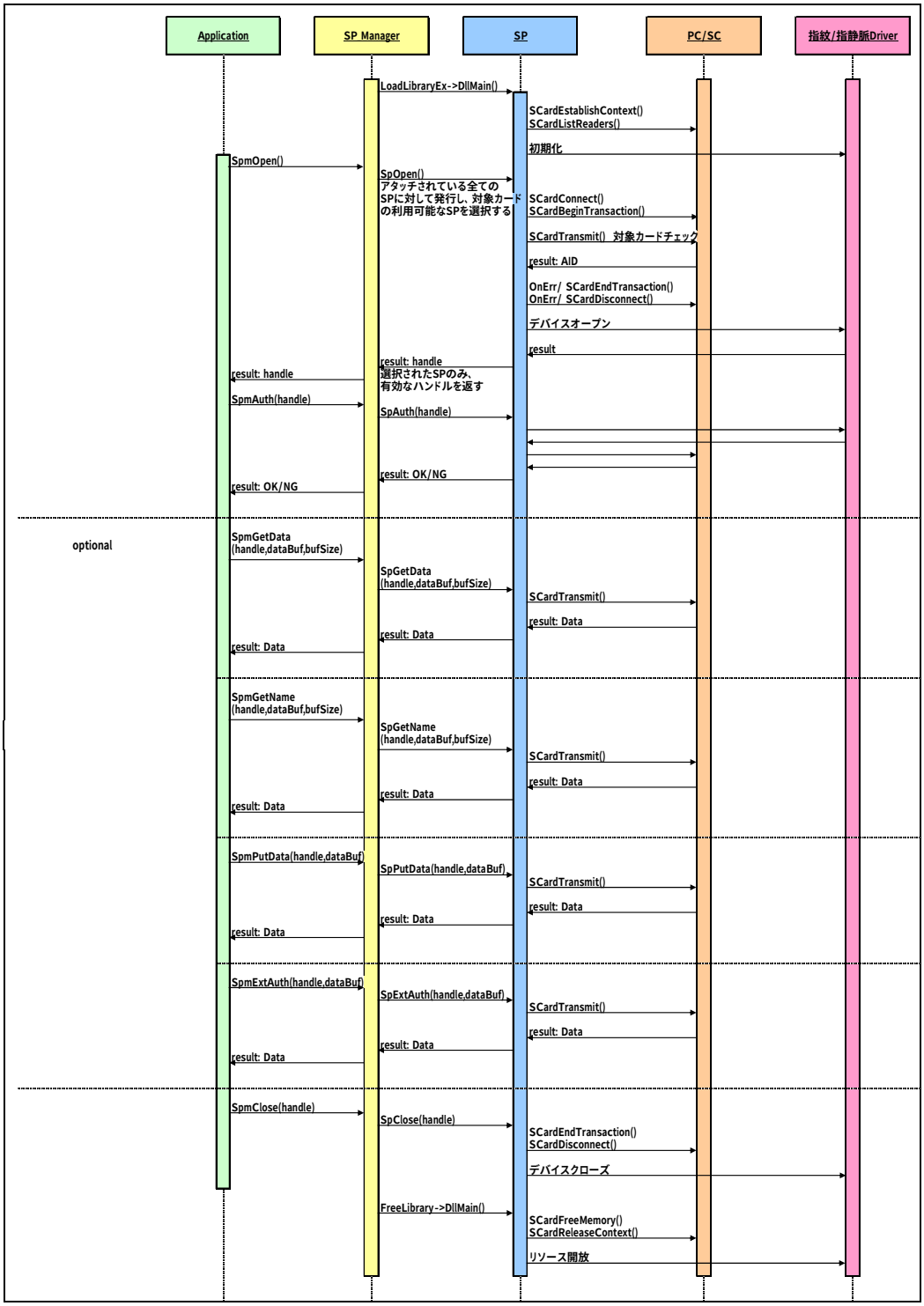


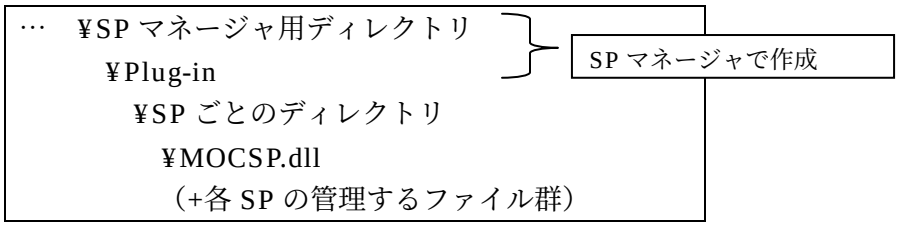
図　2-1　互換性検証システムのシーケンス図

3. インタフェース仕様

本章では、アプリケーション－SP マネージャ、及び、SP マネージャ－SP 間のインタフェース仕様を示します。前者を 3.1 節で、後者を 3.2 節でそれぞれ説明します。

まず、SP マネージャ、SP の詳細を以下の通り示します。

- ✓ SP を開発する際、以下のようなディレクトリ構成で用意する必要がある。



3.1 アプリケーション － SP マネージャ間のインタフェース仕様

アプリケーションと SP マネージャのインタフェースには、以下の 2 種類の方法を提供します。

- ✓ DLL の関数を用いた方法（MOCSPM.dll）
- ✓ TCP/IP による通信を用いた方法

3.1.1 DLL によるアプリケーション － SP マネージャのインタフェース

DLL の関数を用いたアプリケーションと SP マネージャ間のインタフェース仕様を、以下の通り示します。

なお、DLL によるアプリケーション－SP マネージャのインタフェース仕様は、システム A で適用されます。システム B は、Web システムのため、TCP/IP による通信を用いた手法でインタフェース仕様を策定します。

関数の呼び出し規約は StdCall 形式とします。

(1) SpmOpen

サービスマネージャに接続し、認証手続きのセッションを作成することで、そのハンドルを取得します。

```
int   SpmOpen   (
            long   timeout
);
```

パラメータ

timeout(IN)
IC カードアクセスに対するタイムアウト時間（ミリセカンド）

戻り値

関数が成功すると、正の値のハンドルが返ります。
関数が失敗すると、負の値のエラーが返ります。
SPManager の返すエラーは以下の表に示す通りです。また、SP 固有のエラーは-10000～の負の値とし、SP のエラーはそのまま上位に返されます。

名前	値	説明
SPM_NOERROR	0	正常終了
SPM_ILLEGALREQUEST	-1	呼び出し時に不正なパラメータを渡した
SPM_NOMEMORY	-2	処理に必要なメモリーが確保できなかった
SPM_NOTREADY	-3	SPManager 呼び出しの準備が出来ていない
SPM_SOCKETERROR	-4	SPManager 内部で利用するソケットでエラーが発生した
SPM_UNKNOWNERROR	-5	上記以外のエラーが発生した
SP_CANTOPEN	-1001	インストールされた全ての SP のオープンに失敗した
SP_NOTOPEN	-1002	SP がオープンされていない
SP_INVALIDHANDLE	-1003	不正なハンドルが指定された
SP_NOFUNCTION	-1004	オープンされている SP に呼び出された関数が実装されていない
SP_TIMEOUT	-1005	最後のアクセスから一定時間経過すると、指定されたハンドルのセッションはクローズされこの値が返される
SP_INUSE	-1006	別のプロセスが SPManager を利用している

SPManager の返すエラーコード

(2) SpmAuth

SP マネージャに対して認証の実行を要求します。

```
int   SpmAuth(
          int   handle
);
```

パラメータ

handle(IN)
　SpmOpen で取得したハンドル

戻り値

認証に成功した場合、AUTH_OK（値：1）が返ります。

名前	値	説明
AUTH_OK	1	認証に成功

認証に失敗した場合、AUTH_NG（値：0）が返ります。

名前	値	説明
AUTH_NG	0	認証に失敗

関数が失敗すると、負の値のエラーが返ります。エラーの値・種別については SpmOpen を参照してください。

(3) SpmGetData

Optional として本関数を用い、SP から認証したユーザのデータを取得することができます。取得されるデータはヌルターミネイトされた文字列となります。取得データの内容はオープンされている SP に依存します。

```
int   SpmGetData   (
        int          handle,
        LPBYTE       dataBuf,
        int          bufSize
 );
```

パラメータ

handle(IN)
SpmOpen で取得したハンドル

dataBuf(IN/OUT)
データ取得のためのデータバッファへのポインタ（SP 呼び出し時に渡すパラメータを格納することもできます)。

bufSize(IN)
dataBuf のサイズ

戻り値

データ取得に成功した場合、0 以上のデータサイズを返します。
データがない場合には 0 を返します。
取得されるデータサイズはヌルターミネイトされた文字列長となります。
データ取得に失敗した場合、エラーコードとして負の値を返します。エラーの値・種別については SpmOpen を参照してください。

(4) SpmClose

SpmOpen で確立したセッションをクローズする。

```
void   SpmClose   (
        int      handle
);
```

パラメータ

handle(IN)
SpmOpen で取得したハンドル

戻り値

なし

(5) SpmGetName

Optional として本関数を用い、現在オープンされている SP を識別するための文字列を返します。

```
int     SpmGetName   (
        int             handle,
        LPBYTE      dataBuf,
        int             bufSize
);
```

パラメータ

handle(IN)
SpmOpen で取得したハンドル。

dataBuf(OUT)

SP 識別文字列取得のためのデータバッファへのポインタ。

bufSize(IN)
dataBuf のサイズ

戻り値

関数が成功すると、文字列の長さを返します。
関数が失敗すると、負の値のエラーを返します。エラーの値・種別については、SpmOpen を参照して下さい。

(6) SpmExtAuth

Optional として本関数を用い、オープンされている SP に対して外部認証の実行を要求します（SP 依存）。

```
int   SpmExtAuth   (
      int          handle,
      LPBYTE       dataBuf
);
```

パラメータ

handle(IN)

SpmOpen で取得したハンドル

dataBuf(IN)

外部認証用データ（ヌルターミネイトされた文字列）

戻り値

認証に成功した場合、AUTH_OK（値：1）が返ります。

名前	値	説明
AUTH_OK	1	認証に成功

認証に失敗した場合、負のエラーコードが返ります。エラーの値・種別については SpmOpen を参照して下さい。

(7) SpmPutData

Optional として本関数を用い、外部認証に成功した SP へユーザのデータを渡すことができます（SP 依存)。

```
int   SpmPutData   (
      int          handle,
      LPBYTE       dataBuf
);
```

パラメータ

handle(IN)

SpmOpen で取得したハンドル

dataBuf(IN)

SP に渡すユーザーデータ（ヌルターミネイトされた文字列）

戻り値

成功した場合、1 を返します。
失敗した場合、0 を返します。

3.1.2 TCP/IP によるアプリケーション － SP マネージャのインタフェース

TCP/IP を用いたアプリケーションと SP マネージャ間のインタフェース仕様を、以下の通り示します。

TCP/IP を用いて SP マネージャにアクセスするためのプロトコルは HTTP/1.0、メソッドは GET とします。

レスポンスは、JSONP 形式の文字列です。

SP マネージャ内でエラーが発生した場合、以下の形式のレスポンスが返されます。

SpmError({ret: '戻り値', msg: 'メッセージ'});

(1) SpmOpen

サービスマネージャに接続し、認証手続きのセッションを作成することで、そのハンドルを取得します。

● リクエストパラメータ

FUNC = SpmOpen
TIMEOUT = IC カードアクセスに対するタイムアウト時間（ミリセカンド）

● SP からのレスポンス（リクエストパラメータ）

SpmOpen({ret: '戻り値'});

戻り値は、オープンに成功した場合、正の値のハンドル、SP 内でエラーが発生した場合は SP の返すエラーコードが返ります。

(2) SpmAuth

SP マネージャに対して認証の実行を要求します。

● リクエストパラメータ

FUNC = SpmAuth
HANDLE = SpmOpen で取得したハンドル

● SP からのレスポンス（リクエストパラメータ）

SpmAuth({ret: ‘リターン値’});

認証に成功した場合、AUTH_OK（値：1）が返ります。

名前	値	説明
AUTH_OK	1	認証に成功

認証に失敗した場合、AUTH_NG（値：0）が返ります。

名前	値	説明
AUTH_NG	0	認証に失敗

関数が失敗すると、負の値のエラーが返ります。エラーの値・種別については SpmOpen を参照して下さい。

(3) SpmGetData

Optional として本関数を用い、SP から認証したユーザのデータを取得することができます。取得されるデータはヌルターミネイトされた文字列となります。取得データの内容はオープンされている SP に依存します。

● リクエストパラメータ

FUNC = SpmGetData
HANDLE = SpmOpen で取得したハンドル
LENGTH = 受信可能な最大文字列長
DATA = SP に渡す文字列（SP 依存）

● SP からのレスポンス（リクエストパラメータ）

SpmGetData({ret: ‘リターン値’ , data: ‘文字列’});

データ取得に成功した場合、0 以上のデータサイズを返します。
データがない場合には 0 を返します。
取得されるデータサイズはヌルターミネイトされた文字列長となります。
データ取得に失敗した場合、エラーコードとして負の値を返します。エラーの値・種別については SpmOpen を参照してください。

(4) SpmClose

SpmOpen で確立したセッションをクローズします。

● リクエストパラメータ

FUNC = SpmClose
HANDLE = SpmOpen で取得したハンドル

● SP からのレスポンス（リクエストパラメータ）

SpmClose({ret: ‘リターン値’});

戻り値に意味はありません。

(5) SpmGetName

Optional として本関数を用い、現在オープンされている SP を識別するための文字列を返します。

● リクエストパラメータ

FUNC = SpmGetName
HANDLE = SpmOpen で取得したハンドル
LENGTH = 受信可能な最大文字列長

● SP からのレスポンス（リクエストパラメータ）

SpmGetName({ret: ‘リターン値’ , data: ‘文字列’});

関数が成功すると、文字列の長さを返します。
関数が失敗すると、負の値のエラーを返します。エラーの値・種別については、SpmOpen を参照して下さい。

(6) SpmExtAuth

Optional として本関数を用い、オープンされている SP に対して外部認証の実行を要求します（SP 依存）。

● リクエストパラメータ

FUNC = SpmExtAuth
HANDLE = SpmOpen で取得したハンドル
DATA = SP に渡す文字列（SP 依存）

● SP からのレスポンス（リクエストパラメータ）

SpmExtAuth({ret: ‘リターン値’ });

認証に成功した場合、AUTH_OK（値：1）が返ります。

名前	値	説明
AUTH_OK	1	認証に成功

認証に失敗した場合、負のエラーコードが返ります。エラーの値・種別については SpmOpen を参照して下さい。

(7) SpmPutData

Optional として本関数を用い、外部認証に成功した SP へユーザのデータを渡すことができます（SP 依存)。

● リクエストパラメータ

FUNC = SpmPutData
HANDLE = SpmOpen で取得したハンドル
DATA = SP に渡す文字列（SP 依存）

● SP からのレスポンス（リクエストパラメータ）

SpmPutData({ret: ‘リターン値’});

成功した場合、1 を返します。
失敗した場合、0 を返します。

3.2 SP マネージャ － SP 間のインタフェース仕様

SP マネージャは、SP マネージャの管理するプラグインディレクトリ以下に用意された SP ごとのサブディレクトリを検索して、SP ごとのサブディレクトリ以下の MOCSP.dll をダイナミックにロードします。

SP は DLL エントリポイント関数をもった形とします。

DLL エントリポイントは、ダイナミックロード時とリソースの解放時にコールされます。DLL エントリポイントでは、ダイナミックロード時（第 2 引数が DLL_PROCESS_ATTACH）に DLL の管理するリソースを確保します。DLL エントリポイントでリソースの解放を要求された場合（第 2 引数が DLL_PROCESS_DETACH）、管理しているリソースを解放します。

(1) SpOpen

サービスマネージャに接続し、認証手続きのセッションを作成することで、そのハンドルを取得します。

```
int   SpOpen   (
          long   timeout
 );
```

パラメータ

timeout(IN)

IC カードアクセスに対するタイムアウト時間（ミリセカンド）

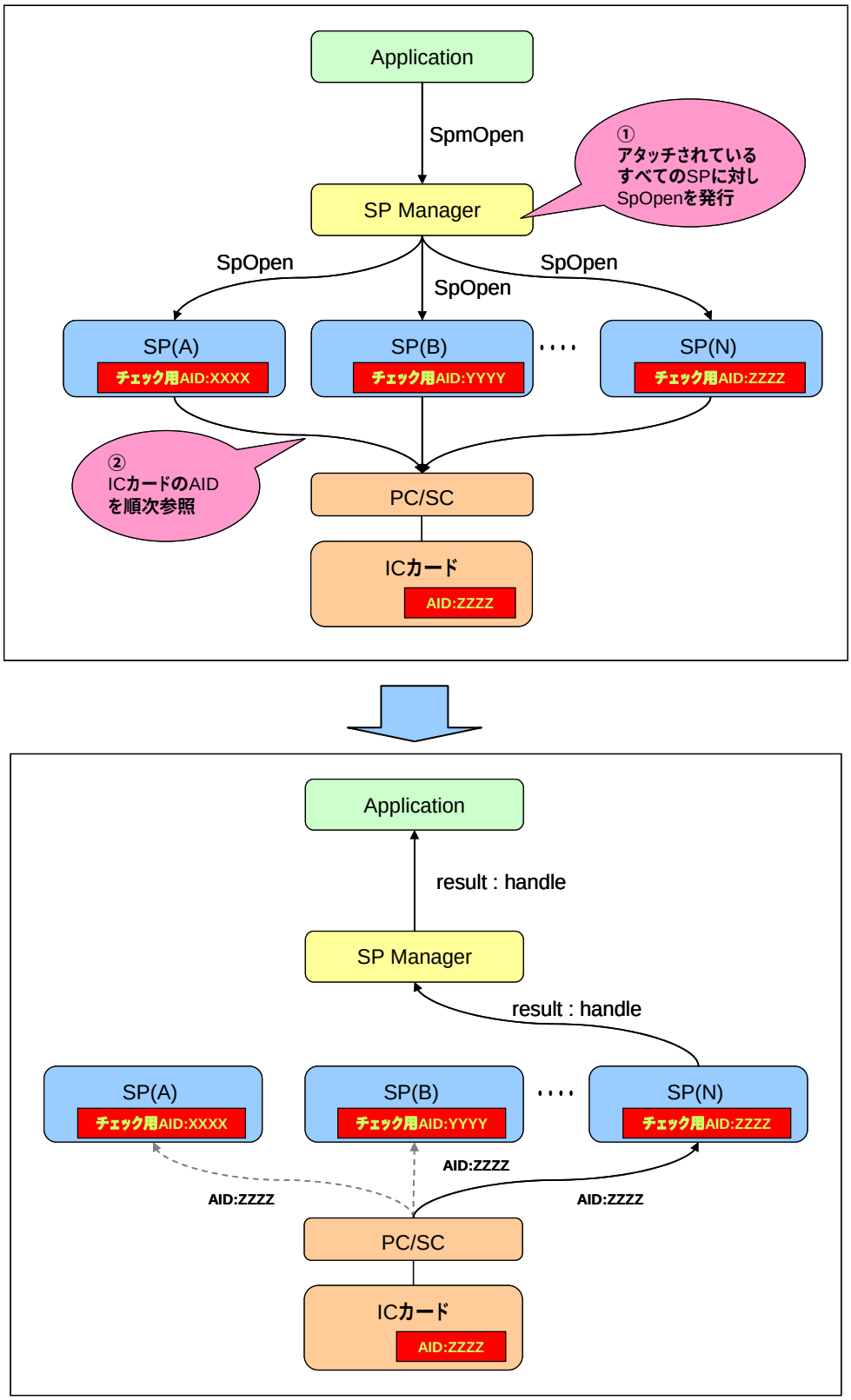
戻り値

関数が成功すると、正の値のハンドルが返ります

関数が失敗した場合、-10000 以下の SP 固有の負の値をエラーとして返します。

補足

以下の図に示す通り、接続されている IC カード R/W に挿入されている IC カードの AID を確認し、その SP が利用できるカードの場合、新たなセッションを確立し、そのハンドルを返します。IC カードが挿入されていなかったり、AID がその SP の対応する AID でない場合は、SpOpen は失敗し、エラーとなります。


Application
SpmOpen
SP Manager
①
アタッチされている
すべてのSPに対し
SpOpenを発行
SpOpen
SpOpen
SpOpen
SP(A)
チェック用AID:XXXX
SP(B)
チェック用AID:YYYY
SP(N)
チェック用AID:ZZZZ
②
ICカードのAID
を順次参照
PC/SC
ICカード
AID:ZZZZ
Application
result : handle
SP Manager
result : handle
SP(A)
チェック用AID:XXXX
SP(B)
チェック用AID:YYYY
SP(N)
チェック用AID:ZZZZ
AID:ZZZZ
AID:ZZZZ
AID:ZZZZ
PC/SC
ICカード
AID:ZZZZ

(2) SpAuth

SP に対して認証の実行を要求します。

```
int   SpAuth(
          int   handle
);
```

パラメータ

handle(IN)
　SpOpen で取得したハンドル

戻り値

認証に成功した場合、AUTH_OK（値：1）が返ります。

名前	値	説明
AUTH_OK	1	認証に成功

認証に失敗した場合、AUTH_NG（値：0）が返ります。

名前	値	説明
AUTH_NG	0	認証に失敗

関数が失敗した場合、-10000 以下の SP 固有の負の値をエラーとして返します。

(3) SpGetData

Optional として本関数を用い、SP からユーザのデータを取得することができます。取得されるデータはヌルターミネイトされた文字列となります。

```
int   SpGetData   (
        int             handle,
        LPBYTE          dataBuf,
        int             bufSize
 );
```

パラメータ

handle(IN)
SpOpen で取得したハンドル

dataBuf(IN/OUT)
データ取得のためのデータバッファへのポインタ（SP 呼び出し時に渡すパラメータを格納することもできます)。

bufSize(IN)
dataBuf のサイズ

戻り値

データ取得に成功した場合、0 以上のデータサイズを返します。
データがない場合には 0 を返します。
取得されるデータサイズはヌルターミネイトされた文字列長となります。
データ取得に失敗した場合、エラーコードとして負の値を返します。関数が失敗した場合、-10000 以下の SP 固有の負の値をエラーとして返します。

(4) SpClose

SpOpen で確立したセッションをクローズする。

```
void   SpClose   (
        int      handle
);
```

パラメータ

handle(IN)

SpmOpen で取得したハンドル

戻り値

なし

(5) SpGetName

SP を識別するための文字列を返します。

```
char *    SpGetName   (
        void
);
```

パラメータ

なし

戻り値

文字列を返します。

(6) SpExtAuth

Optional として本関数を用い、オープンされている SP に対して外部認証の実行を要求します（SP 依存）。

```
int   SpmExtAuth   (
        int             handle,
        LPBYTE     dataBuf
);
```

パラメータ

handle(IN)

SpmOpen で取得したハンドル

dataBuf(IN)

外部認証用データ（ヌルターミネイトされた文字列）

戻り値

認証に成功した場合、AUTH_OK（値：1）が返ります。

名前	値	説明
AUTH_OK	1	認証に成功

認証に失敗した場合、AUTH_NG（値：0）が返ります。
関数が失敗した場合、-10000 以下の SP 固有の負の値をエラーとして返します。

(7) SpPutData

Optional として本関数を用い、外部認証に成功した SP へユーザのデータを渡すことができます（SP 依存)。

```
int   SpmPutData   (
        int             handle,
        LPBYTE     dataBuf
);
```

パラメータ

handle(IN)

SpmOpen で取得したハンドル

dataBuf(IN)

SP に渡すユーザーデータ（ヌルターミネイトされた文字列）

戻り値

データ取得に成功した場合、0 以上のデータサイズを返します。
データがない場合には 0 を返します。
取得されるデータサイズはヌルターミネイトされた文字列長となります。
データ取得に失敗した場合、エラーコードとして負の値を返します。関数が失敗した場合、-10000 以下の SP 固有の負の値をエラーとして返します。

添付資料 2

互換性検証システム　指静脈認証用 SP

取扱説明書

互換性検証システム
指静脈認証用 SP

取扱説明書

２００８年２月

株式会社日立製作所

＜はじめに＞

本マニュアルは、指静脈対応 SP(サービスプロバイダ)のセットアップ方法や機能を説明するものです。

＜御注意＞

1．本資料の内容については、改良のため予告なしに変更することがあります。

＜他社所有商標に対する表示＞

1．Microsoft®は、米国およびその他の国における米国 Microsoft Corp.の登録商標です。
2．Windows®は、米国およびその他の国における米国 Microsoft Corp.の登録商標です。
3．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 に略称いたします。

－ 目 次 －

１．概要

1.1. 機能概要

本プログラムは、互換性検証システムの SP マネージャの要求に従い、IC カードに記録された指静脈情報を使用して本人確認を行うものです。本プログラムは SP マネージャの Plug-in として動作しますので、単体で動作させることはできません。

1.2. 関連ドキュメント

・互換性検証システム　インタフェース仕様書

1.3. 適用ＯＳ

・Windows XP Professional (ServicePack2)

1.4. 前提ハードウェア

1.4.1. 前提 IC カード

本プログラムはコンビ型 IC カードを使用します。以下に本プログラムでサポートしている IC カードを示します。

表 1-1 本プログラムがサポートしている IC カード一覧

項番	品名	メーカ	備考
1	JICSAP V3 カード	日立製作所	本システム専用にフォーマットしたもの

1.4.2. 前提 IC カードリーダライタ

本プログラムは、USB 接続の非接触型 IC カードリーダライタを使用します。以下に本プログラムでサポートしている IC カードリーダライタを示します。

表 1-2 本プログラムがサポートしている IC カードリーダライタ一覧

項番	品名	メーカ	形名
1	非接触型リーダライタ	日立情報制御ソリューションズ	HICRW-US0101-SHP
2	非接触型リーダライタ	シャープセミコンダクタ	PK40PR010(PD2002P)

1.4.3. 前提静脈読取装置

本プログラムは、指紋読取装置を使用します。以下に本プログラムでサポートしている指紋読取装置を示します。

表 1-3 本プログラムがサポートしている指紋読取装置一覧

項番	品名	メーカ	形名
1	指静脈認証装置	日立情報制御ソリューションズ	OFV30-U

1.5. 前提プログラム

本プログラムは、互換性検証システムの SP マネージャの一部として動作します。

表 1-4 本プログラムが前提とするプログラム一覧

項番	品名	備考
1	互換性検証システム SP マネージャ	―

２．インストール

2.1. 注意事項

本プログラムをインストールする前に、以下の項目について確認してください。

(1) Administrator 権限をもつユーザでログオンしているか確認してください。

(2) ディスクの空き容量が十分にあるか確認してください。

2.2. IC カードリーダライタドライバのインストール

IC カードリーダライタを利用するためには、IC カードリーダライタのメーカが提供するドライバをインストールする必要があります。ドライバのインストール方法は、各メーカが提供するマニュアルを参照してください。

2.3. 指静脈認証装置ドライバのインストール

指静脈認証装置を利用するためには、指静脈認証装置メーカが提供するドライバをインストールする必要があります。ドライバのインストール方法は、メーカが提供するマニュアルを参照してください。

2.4. 指静脈認証用 SP のインストール

インストール媒体に格納されているファイル一式を、SP マネージャの指定するフォルダにコピーし、”ICFVEnroll.exe”のショートカットを”指静脈登録ツール”の名称でデスクトップに作成してください。また、格納先フォルダのパスを環境変数の Path に登録してください。

３．環境設定

3.1. 指静脈登録環境の準備

3.1.1. IC カードリーダライタの設定

“CardReader.ini”に、使用する IC カードリーダライタの名称(PC/SC 上で認識される名称)を Card_ReadName に設定してください。

設定例）[Proc_Connect]

```
Card_ReadName =SHARP PD2002USB 0
```

3.1.2. 指静脈登録ツールの設定

“ICFVEnroll.ini”に、指静脈登録ツールで使用するパラメータを設定してください。ログファイルの出力先や登録時に読み取る回数、しきい値などが設定できます。

設定例）[LOG]

```
; ログ出力ディレクトリ
OUT_PATH=.¥¥LOG
[ATTESTORE]
; しきい値
THRESHOLD=0
; 登録時の読み取り回数(1,3,5)
NUMBEROFSCAN=3
```

3.2. SP マネージャの準備

3.2.1. SP マネージャの設定変更

本プログラムは指静脈認証時にダイアログを表示します。サービスの設定で”デスクトップとの対話をサービスに許可(W)”にチェックを入れてください。この設定を有効にしないと、正しく動作しません。設定を変更させた後、サービスを再起動してください。

図 3.1 サービス画面

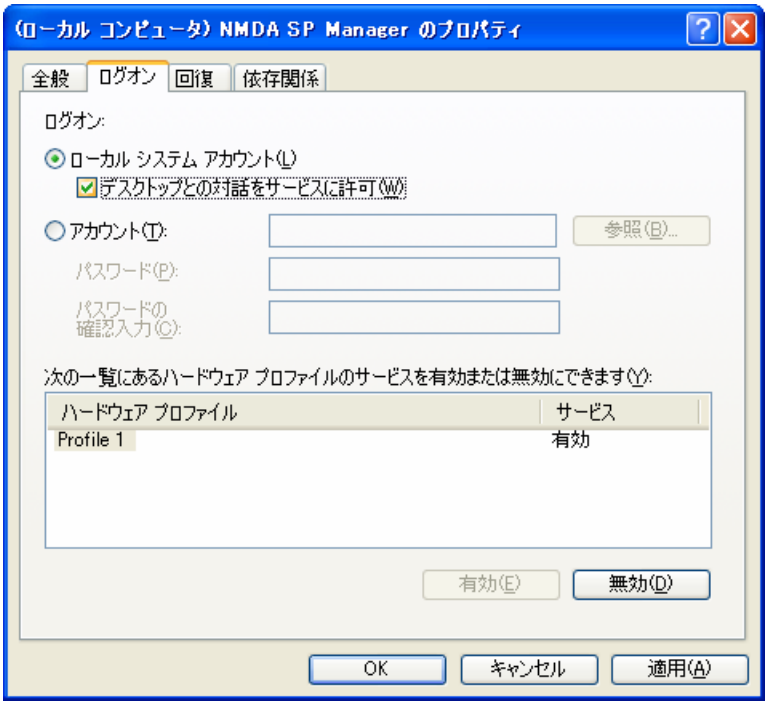


図 3.1 NMDA SP Manager のプロパティ画面

4．アンインストール

4.1. SP のアンインストール

コピーしたファイルをフォルダごと削除し、デスクトップに作成した”指静脈登録ツール”のショートカットを削除してください。また、環境変数に登録した Path を削除してください。

５．指静脈情報の登録

5.1. 登録処理の概要

指静脈登録ツールを使用して IC カードに指静脈を登録します。

5.2. 指静脈登録

(1) 登録ツールの起動

IC カードリーダライタに IC カードをセットし、デスクトップにある指静脈登録ツールを起動してください。

(2) 個人情報の設定

個人情報の欄に氏名等を設定してください。

図 5.1 指静脈登録ツール

(3) 指静脈の読み取り

登録する指と登録先を選択して、[指静脈読み取り]ボタンをクリックしてください。指静脈の登録画面が表示されますので、画面の指示に合わせて登録する指をセンサに置いてください。

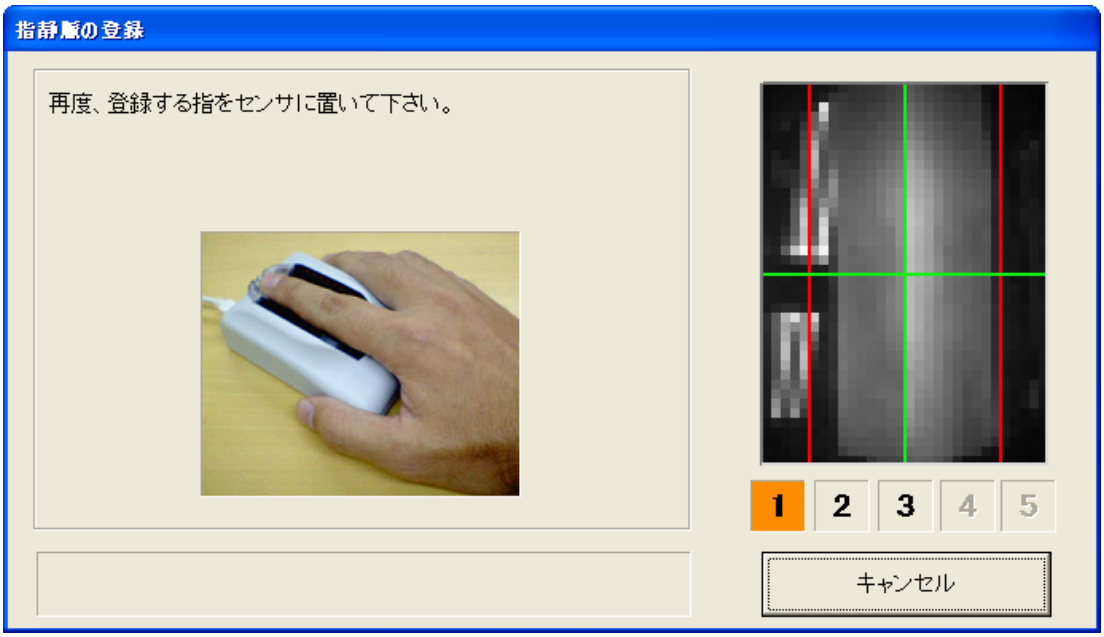


図 5.2 指静脈の登録

(4) 認証テスト

確認する登録データを選択して、[認証テスト]ボタンをクリックしてください。指静脈認証の画面が表示されますので、画面の指示に合わせて指をセンサに置いてください。

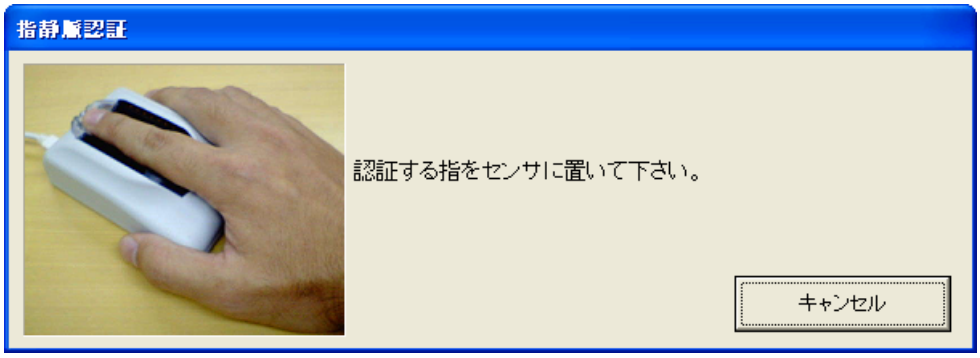


図 5.3 指静脈認証

(5) IC カードへの登録

IC カードリーダライタに IC カードがセットされていることを確認して、[登録]ボタンをクリックすると、「指静脈認証データを登録しますか？」と確認されます。[はい(Y)]ボタンをクリックすると IC カードに登録されます。IC カードへの登録が完了すると「カードへの書き込みが終了しました。」と表示されます。この表示が出るまでは、IC カードを取り外さないでください。

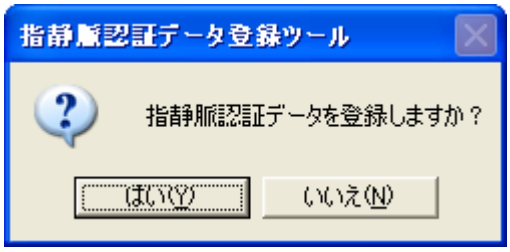


図 5.4 登録確認

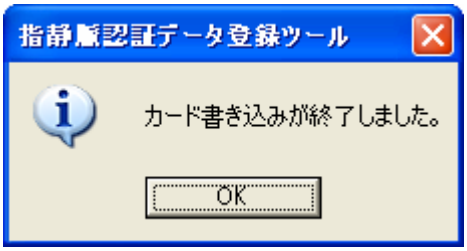


図 5.5 登録完了

(6) 指静脈データの消去

[カードデータ消去]ボタンをクリックすると、IC カードに登録された情報を全て削除し、初期状態に戻します。

※削除したデータは元に戻すことはできません。ご注意ください。

(7) 指静脈登録ツールの終了

[終了]ボタンをクリックすると、指静脈登録ツールを終了します。

６．指静脈認証

6.1. 認証処理の概要

SP マネージャから認証を要求されると指静脈認証の画面を表示します。画面の指示に合わせて指をセンサに置いてください。

6.2. 指静脈認証

(1) 認証画面

指静脈認証の画面が表示されたら、IC カードに登録されている指をセンサに置いてください。

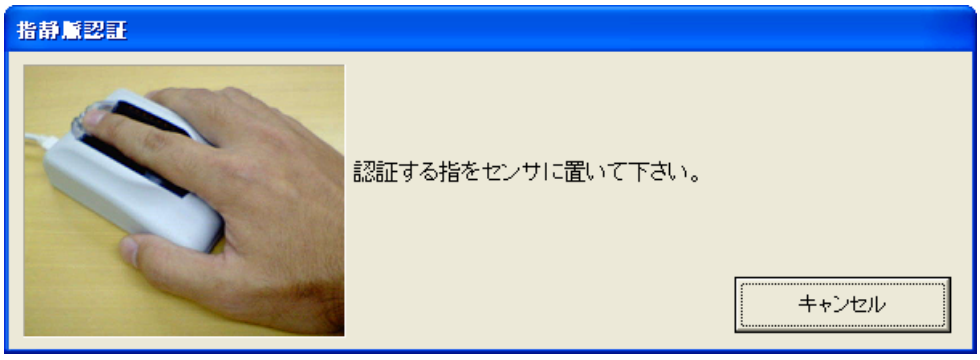


図 6.1 指静脈認証画面

(2) 認証に成功した場合

認証に成功すると「認証しました。」と表示した後、画面を閉じます。

図 6.2 認証成功

(3) 認証に失敗した場合

認証に失敗すると、「指の置き方が違います。指を置き直して下さい。」と表示されますので、再度指を置きなおしてください。

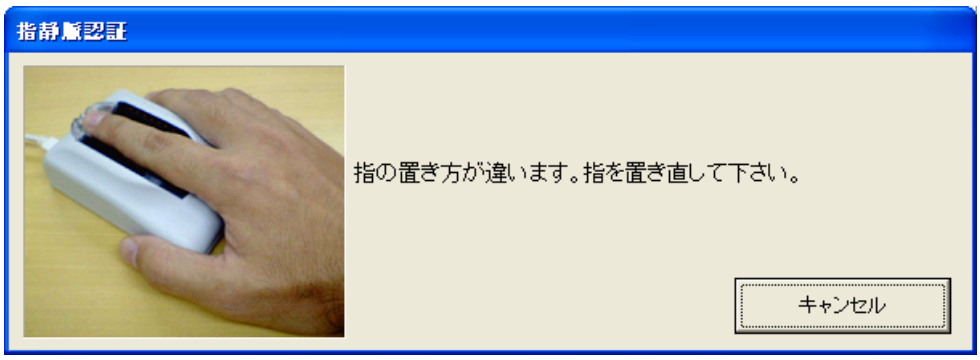


図 6.3 認証失敗

発行日　平成 20 年 3 月
作　成　財団法人ニューメディア開発協会
住　所　〒112-0014　東京都文京区関口 1 丁目 43 番 5 号　新目白ビル 6 階
電　話　03-5287-5032　ＦＡＸ　03-5287-5029

調査･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　Net2.三田ビル 4F

調査･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

――

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
「多種類のバイオメトリクス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