平成２２年度戦略的基盤技術高度化支援事業

（平成２２年度補正予算事業）

# 「高度化指紋認証セキュリティデバイスの開発」

# 成果報告書

平成２４年　３月

委託者　内閣府沖縄総合事務局

委託先　株式会社トロピカルテクノセンター

本報告書の取扱について

この報告書には、委託業務の成果として、産業財産権等の対象となる技術情報（未出願又は未公開の産業財産権等又は未公開論文）、ノウハウ等の秘匿情報が含まれているので、通例の取扱いにおいて非公開とする。ただし、行政機関の保有する情報の公開に関する法律（平成１１年法律第４２号）に基づく情報開示請求の対象の文書となります。

目　次

# 第1章　研究開発の概要

## 1-1　研究開発の背景・研究目的及び目標

### 1-1-1　背景

近年、企業や大学、各省庁・自治体などの機関において、入退出や情報の管理等のセキュリティ強化のための、より有効な認証システムが求められており、その解決法として、従来のICカード認証システムの流用が可能で、紛失・なりすましのリスクを回避でき、認証精度が高いエリア型指紋センサによる指紋認証ICカードのニーズは高い。

指紋認証ICカードシステムの開発については、カード外にあるライン型センサからの指紋情報とカード内に登録した指紋情報の照合をカード上で行うICカードは2010年9月に発表されているが、本技術開発の課題となる、センサによる指紋情報の取り込みから登録情報との照合までを非接触型ICカード上で行うAuthentification On Cardに関する内外の技術特許並びに規格は無い。

一方、これまでの取り組みとしてアクシオヘリックスは、ICカードに導入可能なサイズ・消費電力の指紋センサの世界初の開発に成功した。また同様にICカードに導入可能なCPUを設計し、プロトタイプ開発にも成功した。

そこで、本研究では、開発したセンサ・CPUを活用し、カード上で指紋情報の取得、認証が可能であり、デバイスと組込技術による安全性・利便性を高めた新たなシステムの開発を目指す。具体的には、認証プロセス、データの保管、非接続による情報の通信、暗号化、電力制御、エラーコントロール等のモジュールの制御設計および開発を行う。

### 1-1-2　本研究の目的

・非接触型ICカード上で動作する指紋認証システムの開発

ICカード上に搭載したエリア型指紋センサとCPUで動作する指紋照合アルゴリズムにより、カード自体に正当なカード使用者であるかどうかの認証機能を持った、従来よりセキュリティを向上させ、かつ、従来の非接触型カードシステムと互換性を持ったICカードを開発する。

また、指紋認証の精度向上のための新規アルゴリズムを組み合わせた認証ソフトウェアを開発する。

目標：

従来ICカードとの互換性の確保

指紋照合精度：FRR<0.1%、FAR＜0.001%

指紋照合時間：1秒以内

・非接触型 IC カード上の電子回路への高効率電力供給システムの開発

従来の非接触型カードリーダで供給される電力ではカード上で生体認証機能を動作させるには十分でないため、光発電素子とキャパシタを付加した蓄電池をソフトによって充放電制御する電力供給システムを開発する。

目標:

ソフトウェアによる蓄電池の高効率な充放電制御

耐久性:トータルで数十万回のカード使用を可能にする

・モジュール間暗号通信の開発

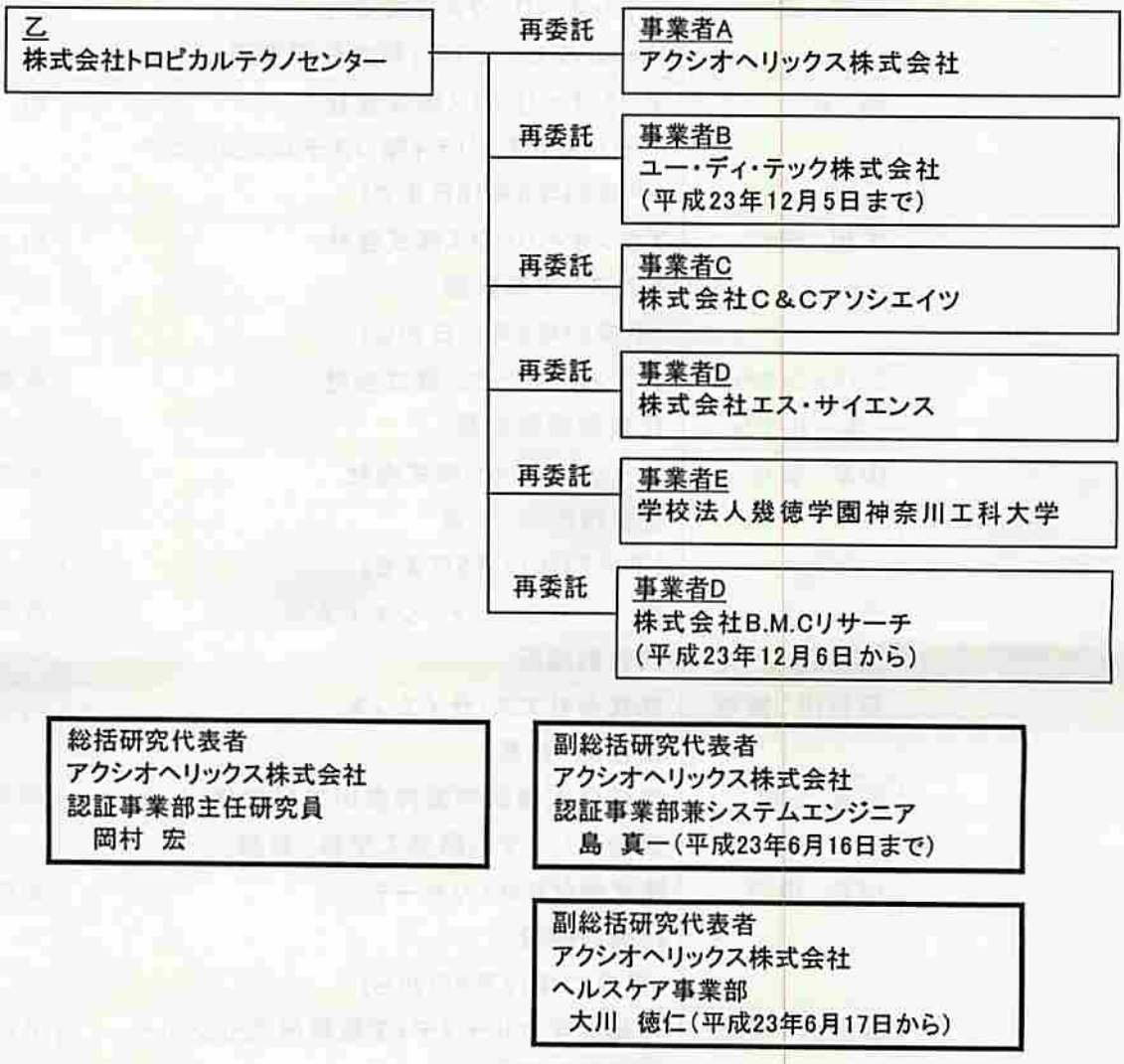
非接触型生体認証 IC カードシステムの各モジュール間のデータ転送に動的鍵暗号(ストリーム型暗号)方式で通信を行うための暗号通信システムを開発する。

目標:

暗号演算時間1ビット時間

## 1-2 研究体制

### 1-2-1 研究組織及び管理体制



1-2-2研究開発委員会

| 氏名 | 所属・役職 | 備考 |
|---|---|---|
| 岡村　宏 | アクシオヘリックス株式会社<br>ホーム＆セキュリティ部主任研究員 | PL |
| 島　真一 | アクシオヘリックス株式会社<br>ホーム＆セキュリティ部システムエンジニア<br>（平成23年6月16日まで） | SL |
| 大川　徳仁 | アクシオヘリックス株式会社<br>ヘルスケア事業部<br>（平成23年6月17日から） | SL |
| シバスンタラン<br>スハルナン | アクシオヘリックス株式会社<br>代表取締役社長 | 再委託先 |
| 山本　智也 | ユー・ディ・テック株式会社<br>営業技術部　部長<br>（平成23年12月5日まで） | 再委託先 |
| 赤嶺　学 | 株式会社C＆Cアソシエイツ<br>代表取締役 | 再委託先 |
| 長谷川　裕克 | 株式会社エス・サイエンス<br>業務部　部長 | 再委託先 |
| 石濱　正男 | 学校法人幾徳学園神奈川工科大学<br>自動車システム開発工学科　教授 | 再委託先 |
| 川合　信明 | 株式会社B.M.Cリサーチ<br>代表取締役<br>（平成23年12月6日から） | 再委託先 |
| 喜屋武　盛基 | 沖縄大学マルチメディア教育研究センター<br>非常勤研究員 | アドバイザー |

1-2-3 事業化担当企業

アクシオヘリックス株式会社

## 1-3 成果概要

### 1-3-1 本研究の目標

・非接触型 IC カード上で動作する指紋認証システムの開発

従来のICカードに生体認証(以後指紋認証)システムを搭載し、指紋認証により、従来通りの使用を可能とする。指紋の登録データもカード上に搭載され、カード単独で指紋認証が完結する。これによって、指紋認証の操作を除き、オリジナルのカード大きさと使用法を踏襲することができる。

システムを指紋認証モジュール、給電モジュール及びメーンCPUモジュールの3モジュール群に分割して、開発効率の向上を図り、モジュール毎にバージョンアップ等が可能な機能向上の容易性を実現する。また、小型エリア方式の指紋認証システムソフトを採用し、新しい認証ロジックを追加することで、現在普及している大容量メモリ・大型 CPU・高消費電力(12V 等)による装置と同等以上なセキュリティの機能を達成する。

・非接触型 IC カード上の電子回路への高効率電力供給システムの開発

光発電素子とキャパシタ付蓄電池の充放電バランスの制御ソフトにより、省電力化を達成すること。

・モジュール間暗号通信の開発

動的暗号キーシステム(ストリーム型暗号システム)により各モジュール間やICカード認証システムとの通信の暗号化を行い、セキュリティを向上させること。

### 1-3-2 本研究のサブテーマ

①オリジナルICカードとの互換性を確保する指紋認証システムの開発
②指紋認証システムの各モジュール間通信の暗号化組み込みソフト開発
③指紋等認証モジュールソフト開発とその高度化
④給電モジュールの組込みソフトの開発とその高度化

### 1-3-3 実施内容

①オリジナルICカードとの互換性を確保する指紋認証システムの開発

研究実施機関:アクシオヘリックス

具体的内容:

従来の非指紋認証ICカードのバージョンアップの基本設計を変更せず、指紋認証機能を追加した IC カードシステムを開発する事で、従来カードの管理システムに影響が無く、そのまま使用できる互換性を確保する。追加指紋認証機能は従来のIC認証システムとは

分割独立させた形で、ICカード内に組み込み、指紋認証部からの認証結果の信号により、従来のICカード制御部のアクティブ化のオンオフ制御を行うようにする。

また、指紋認証機能の分割により従来のICカードへの指紋認証ソフトの組込みに関するメーカへのOEM供給の容易化を図る。

②指紋認証システムの各モジュール間通信の暗号化組み込みソフト開発

研究実施機関:アクシオヘリックス

具体的内容:

疑似乱数ビット列生成暗号を応用した暗号化技術特許(特願平8-245158)(喜屋武、翁長、名嘉村)を応用して、システムの各モジュール間のデータの暗号通信を行うためのハードウェアにマッチした制御のためのソフトウェアを開発する

当暗号方式は素数ビット長を持つ複数のシフトレジスタと各シフトレジスタの出力の非線形フィードバック回路より構成される数ふるい回路の出力する疑似ランダムビット列により暗号化対象データ(平文)と排他的論理和を取る事により暗号化および復号を行うものである。他の暗号方式に比べ小規模回路で演算時間が1ビット時間以内で済むという特長を生かしてカード上に組み込めるソフトウェアの開発を行う。

③指紋等認証モジュールソフト開発とその高度化

研究実施機関:アクシオヘリックス、神奈川工科大学

具体的内容:

指紋認証のセンサ部は既開発の電荷方式薄型エリアセンサを利用する。

認証ソフトウェアに狭小測定エリア方式(8×8点)での認証のロバスト性向上ロジックを開発し組込む。従来のロジックに指紋稜線垂直方向のピッチデータのフーリエ解析による周波数特性を抽出するアルゴリズムを組合せる。

また、新規に、低電圧、小電力消費型(50mW以下を目標)を達成するための小電力化制御ソフトを開発しその高度化を行う。

これらのソフト組込みカードの厚さは、目標:0.7mmとし、フェリカ対応ソフトの組込みカードのソフトを開発する。

④給電モジュールの組込みソフトの開発とその高度化

研究実施機関:ユー・ディ・テック

具体的内容:

薄型光発電素子+キャパシタ+蓄電池をICカード内に組込み機能させるものとする。

フィルム積層型キャパシタと積層型蓄電池との充放電バランス制御ソフトを構築し、機能と信頼性を評価する。制御レスに対して、20%の効率向上を目標とし、耐久性は50万回をクリアすることを目標とする。

⑤統合テスト、フィードバック

研究実施機関：C&C アソシエイツ、エス・サイエンス

具体的内容：

指紋認証 IC カードシステムに対し、認証反応、シミュレーションと実指紋による認証精度の確認、温度・湿度・硬さ等の耐久性のテスト、あらゆる状況に置けるカードの反応分析等統合テストを実施すると共に、各サブテーマ担当へのフィードバックを行う。

⑥プロジェクトの管理・運営

研究実施機関：(株)トロピカルテクノセンター

具体的内容：

本研究を円滑に推進するため、研究開発推進委員会を設置し、その運営により各研究開発項目における課題の抽出、検討及び成果の統括・報告書の作成を行う。

### 1-3-4 成果概要

(1) 接触型(タッチ方式)ICカードをベースに、従来のカード入れに収納可能な厚さ1．5mmで、予定する機能をすべて搭載し、目標を達成した。

(2) ICカードの安定した充電バランスを達成した。当初の光発電ディバイスは目標達成が難しく、実現にもコストがかかるため、将来性の高いコイル式によるワイヤレス給受電システムにて、目標を達成した。

(3) 応用事例として、カーセキュリティシステムへ適用し、ICカードの非接触通信として、Bluetooth を採用し、車載制御装置の秘匿性を高め、多重ロック機構と組み合わせた従来品と差別化されたセキュリティを達成した。また、作動の信頼性にも十分な配慮を加えた。

## 1-4 当該研究開発の連絡窓口

| | |
|---|---|
| 所属 | アクシオヘリックス株式会社 |
| 役職 | 代表取締役 社長 |
| 氏名 | シバスンタラン スハルナン |
| 電話 | 098-988-4235 |
| FAX | 098-988-4238 |
| E-mail | ssivasundaram@axiohelix.com |

## 第2章　本論

### 2-1　委託事業の内容

#### 2-1-1　目的

カード外に指紋情報を出すことなく、カード上で指紋認証を行い、IC カード機能をオン・オフできる IC カード、およびシステムを提供する。従来の IC カード読み取り装置をそのまま使用して、IC カードをより安全性の高い本人確認を可能とすることが本ディバイスにより可能とすることを目的とする。

#### 2-1-2　事業概要、課題、高度化目標及び技術目標値

詳細は、別紙 6 に示した。

### 2-2　開発結果報告

#### 2-2-1　技術開発の背景

IC カードは、半導体集積回路（IC）で作られた小型コンピュータを搭載しており、その演算力と大きな記憶容量により、ICカード自身が利用者の正当性を確認し、記憶内容への読み書きを許可するアクセス制御機能を有する。磁気ストライプカードに対して、カードへのサイバー攻撃に対する耐タンパー性・信頼性が高い。しかし、近年各種のサイドチャンネル攻撃の手法が出現し、比較的低コストでカードとの送受信による暗号秘密鍵を解読する事例が出現している。生体認証を取り入れたシステムが導入されているが、カード読み取り装置自身を改造する必要があり、まだ普及には至っていない。この状況をクリアーし、生体認証によるセキュリティの向上を実現する方策として、IC カードの内部に生体認証照合データを搭載し、ICカードでの送受信機能のONOFF制御を行うことで、飛躍的にそのセキュリティを向上させるディバイスの開発を行う。この製品を使用することで、現存のカード読み取り装置をそのまま利用することで、高いセキュリティ性を獲得することができる。ICカードの利用は、最近はその利便性からますます多方面に拡大しており、それに伴うセキュリティ性の確保が強く求められている。

## 2-2-2 目標課題

| 課題 | 特徴 | 成果 |
|---|---|---|
| 現在の普及しているICカードシステムと互換性の高いセキュリティ向上システムの構築 | オリジナルのICカードに生体認証システムを搭載しており、生体認証により、従来通りの使用が可能である | 今回は、カードの厚さが 1.5mmで、最近普及が著しい非接触型に限定ではあるが、カード内に指紋認証機能を搭載し、実現した。 |
| 入退室管理等のセキュリティディバイスを基本的に変更し、投資することなく、ICカードシステムのセキュリティ機能を大幅に向上さ<br>ること | 生体認証の登録データもカード上に搭載され、カード単独で生体認証が完結する。カードとPW盗まれてもカードの使用は阻止できる。 | 既存の導入システムを変更せず、直ちにセキュリティ向上が試作品で確認できた。 |
| ICカードの利用者にとって、いままでとほぼ同じような大きさで手になじみ、生体認証の操作性に違和感が無く、カードを利用することが出来ること | 生体認証の操作を除き、オリジナルのカード大きさと使用法を踏襲することができる | 上記の通り、カード厚さが2倍になったが、一般的なカード入れであれば収納が可能であり、使用感も従来品と同じである。 |
| カード会社がいままでのICカード記載システムを変えること無く、ICカードの認証のアクティビティのみON，OFF機能追加のみでバーションアップができること | 生体認証付ICカードに切り替えても、従来の窓口でのカード操作盤を変更すること無く利用できる | 非接触型カードであれば、(エディ等)であれば使用可能である。 |
| 生認証ソフトを各機能に分けて、開発効率の向上、機能向上の容易性を達成できること | ここでは、生体認証モジュール、給電モジュール及びメーンCPUモジュールの3モジュール群に分割して、開発効率向上ができ、バージョンアップにも当該モジュールのみの変更で済む | 3モジュールが独立して開発され、モジュール間の通信を解読されないように暗号化技術が用いられ、カードから情報採取の攻撃に対し、高いバリアを構築した。 |
| 小型コンパクト化する指紋認証のためのロバスト性、信頼性を向上させる生体認証ソフトであること | 小型エリア方式の指紋認証システムソフトを採用し、新しいロジックを追加<br>することで、現在の普通型の大きな装置と同等以上なセキュリティの機能を達成している | エリア型、スライド型でも可能で、消費電力のミニマム化も視野に入れて、認証ソフトを組込、従来装置と同等な性能を得た。 |
| 光発電素子キャパタ付蓄電池の充放電バランスの制御ソフトにより、省電力化を達成すること | 制御レスよりは20%の効率向上の小電力化を達成している | 効率のよい素子が入手できず、その代替えとして、最近注目され将来性の高いコイル式ワイヤレス給受電モジュールを導入した。 |

| | | |
|---|---|---|
| 各モジュール間やICカード認証システムとの通信の暗号化を行い、セキュリティを向上させること | 動的暗号キーシステムを採用し、現在普及しているセキュリティシステムの最高水準を達成している | ICカード機能のONOFF制御信号に適合させた。 |
| 提案の生体認証付ICカードのオリジナルの機能、耐久性をそのまま踏襲できること | 十分にICカードの基本機能や耐久性を保持している。 | ICカードの基本設計を各モジュールごとに分離しており、オリジナルの機能は保持されている。 |
| 提案の生体認証付ICカードの更なる操作性や認証率の向上の求が絶え間なく出てくる傾向を念頭に置き、その商品力向のため、更なるシステムソフトのバージョンアップを検討すること | 更に上位の生体認証モジュールや現在急速な発展を続けている給電モジュールは、そのコストと機能のバランスで、バージョンアップを用意し、将来への更なるセキュリティの要求に応じる生体認証システムソフトの向上を用意する | 一番のネックは、各モジュールの最大厚さを規定に入れてその機能を満足する必要がある。各専門メーカーとの連携を強め、対応する。 |

### 2-2-3 研究開発の高度化目標及び技術的目標値

**目標1：オリジナルICカードとの互換性を確保する指紋認証組み込みソフトシステムの開発**

従来の非指紋認証ICカードのバージョンアップの基本設計を変更せず、指紋認証機能を追加したICカードシステムを開発する事で、従来カードの管理システムに影響が無く、そのまま使用できる互換性を確保する。追加指紋認証機能は従来のIC認証システムとは分割独立させた形で、ICカード内に組み込み、指紋認証部からの認証結果の信号により、従来のICカード制御部のアクティブ化のオンオフ制御を行うようにした。

ここでは、従来ICカード機能を有するチップ部、指紋認証モジュール（含、指紋センサー部）、ワイヤレス給受電モジュール（含、二次電池部）、生体認証データ通信部（Felica, Bluetooth 等）から構成されている。

また、指紋認証機能の分割により従来のICカードへの指紋認証ソフトの組込みに関するメーカーへのOEM供給の容易化を図る。

結果：本課題100%実施した。

詳細は別紙1、7に示した。

**目標2：指紋認証システムの各モジュール間通信の暗号化組み込みソフト開発**

疑似乱数ビット列生成暗号を応用した暗号化技術特許（特願平8-245158）（喜屋武、翁長、名嘉村）を応用して、システムの各モジュール間のデータの暗号通信を行うためのハードウェアにマッチした制御のためのソフトウェアを開発する

当暗号方式は素数ビット長を持つ複数のシフトレジスタと各シフトレジスタの出力の非線形フィードバック回路より構成される数ふるい回路の出力する疑似ランダムビット列により暗号化対象データ(平文)と排他的論理和を取る事により暗号化および復号を行うものである。他の暗号方式に比べ小規模回路で演算時間が1ビット時間以内で済むという特長を生かしてカード上に組み込めるソフトウェアの開発を行う。

結果:100%実施した。

詳細は別紙4に示した。

技術目標値

1)演算時間が1ビット時間以内で済むという特長を持つ

⇒本ソフトを指紋認証モジュール部とカード機能を有するチップ間に適用し、起動信号をチップ部に送信する情報の暗号化に適合した。

**目標3指紋等認証モジュールソフト開発とその高度化**

指紋認証のセンサ部は既開発の電荷方式薄型エリアセンサを利用する。

認証ソフトウェアに狭小測定エリア方式(8×8点)での認証のロバスト性向上ロジックを開発し組込む。従来のロジックに指紋稜線垂直方向のピッチデータのフーリエ解析による周波数特性を抽出するアルゴリズムを組合せる。

また、新規に、低電圧、小電力消費型(50mW以下を目標)を達成するための小電力化制御ソフトを開発しその高度化を行う。

これらのソフト組込みカードの厚さは、目標:0.7mmとし、フェリカ対応ソフトの組込みカードのソフトを開発する。

結果:100%達成した。応用で、車セキュリティ、入退出セキュリティー、PC のセキュリティーに導入した。

詳細は別紙2に示した。

技術目標値

1)指紋の照合精度:FRR<0.1%, FAR<0.001%

2)指紋の照合時間≦1秒

⇒いずれも達成している。今回はモニター試験でのデータであり、(約100回のトライ)更に数増しや意地悪試験を実施してゆく。

**目標4:給電モジュールの組込みソフトの開発とその高度化**

薄型光発電素子+キャパシタ+蓄電池をICカード内に組込み機能させるものとする。

フィルム積層型キャパシタと積層型蓄電池との充放電バランス制御ソフトを構築し、機能と信頼性を評価する。制御レスに対して、20%の効率向上を目標とし、耐久性は50万回をクリアすることを目標とする。

結果：100%実施した。ただし、当初、薄型光発電素子＋キャパシタ＋蓄電池で駆動させる方式を想定したが、IC カードを安定的に駆動できるだけの電力量を確保することが難しいことが実験の結果判明したため、電磁誘導によるワイヤレス給電＋薄型のリチウムイオン二次電池というシンプルな構成とし、動作確認を行った。ただし、充放電バランスを配慮し、600mWh の二次電池容量を満足する薄型電池が実用レベルに達しようとしている段階であり、今回は、ICカード標準の厚さ 0.76mm ではなく、カード2枚分（カード入れに収納可能な厚さ）1.5mm の厚さとし、最近急速需要が伸びている非接触型ICカード対応とした。

詳細は別紙3に示した。

技術目標値

1） 耐久性は50万回をクリアすることを目標とする

⇒今回は、単体テストにて、達成した。

### 2-2-4 生体認証付ICカード（第3世代）の開発実施内容

実施項目を図1に示す。また、それらの詳細は、別紙1，3，5に示した。

生体認証付 IC カード(第 3 世代)

[1] IC カードの厚さ

挿入型・・現用厚さ：0.76mm　　大きさ 54mm×85.7mm

接近型・・カードケース対応型：1.5mm 以下⇒1.5mm 採用

多機能型・・厚さ：1.5～6mm 程度 2

[2] 指紋認証モジュール

スライド型／エリア型・・厚さ 0.3mm

照合精度：

本人拒否率 FRR<0.1%・・OK

他人誤認率 FAR<0.001%・・OK

照合時間≦1 秒・・OK

[3] 給電モジュール

ワイヤレス給電

給電側・・5W、受電側・・1W、5V

給電テープル設定

ワイヤレス受電

厚さ・・0.55mm(Max.)、　大きさ・・50mm×42mm　　コイル外形・・Φ40mm

マルチ電源・・1.8V3.3V　　100mA 以下

充電側制御実施

単体で効率向上確認

耐久性

50 万回クリア

薄型リチウムイオン式ポリマー二次電池・・0.76mm 厚さに入るもの入手難しい

容量・・600mWh

厚さ・・1.35mm

光発電素子キャパシタ

充放電バランス制御ソフト・・20%効率向上目標

・・採用せず、コイル式ワイヤレス給受電で代替え

[4]　モジュール間通信

動的暗号キーシステム

疑似乱数ビット列生成暗号化

[5]　メーン CPU モジュール

消費電力

50mW 以下　・・OK

[6]　システム認証通信

NFC

接近型、タッチ型

Felica

カーセキュリティ向け

○Bluetooth

[7]　既存読取装置での互換性

生体認証照合機能内蔵・・OK

接近型・タッチ型への互換性・・厚さ 1.5mm

[8]　製品と価格

ライセンス料

1000 円／枚

販売先

カーセキュリティ(車両盗難防止)

応用事例として、Bluetooth 通信付でシステム構築、

高齢者支援システム会員証

巡回医療システム受診証

入退室管理システム
クレジットカード
金融関連 IC カード
企業社員証

### 2-2-5 応用事例:カーセキュリティシステムでの開発実施内容

実施項目を図2に示す。また、それらの詳細は、別紙2，5に示した。

応用課題:カーセキュリティシステム

[1] 車両盗難防止

[1-1]エンジン始動ロック方式

① リレー回路挿入
スタータ回路 ON-OFF
点火装置回路 ON-OFF
燃料ポンプ回路 ON-OFF

② リレー回路作動電圧変更
24V 化←12V

③ 信頼性 ‥誤作動防止
ドア開閉検知
運転席接近センサ検知
ロック回路ハーネス切断 ‥警報装置作動

④ 一定時間離席
認証解除

[1-2]従来エンジンキーシステムと独立
追加ロックが解除で本来キーが稼働する方式
適用車種への設定が容易

[2] 生体認証 IC カード
指紋認証登録
アンドロイド OS 携帯
通信方式‥Bluetooth
登録作業携帯
車両搭載制御システム

[3] 車両搭載制御システム
ワイヤレス化‥搭載位置秘匿
Bluetooth
認証プロセス ‥プールプルーフ化

認証状況インジケータ設置

[4] 車両盗難システムのニーズ

車両盗難プロ集団

東南アジア多い　　日本にも存在

高級車がターゲット

イモビライザー （電子キー）

イモビカッターで破られる

[5] 販売と価格

本開発品価格 ‥生体認証付

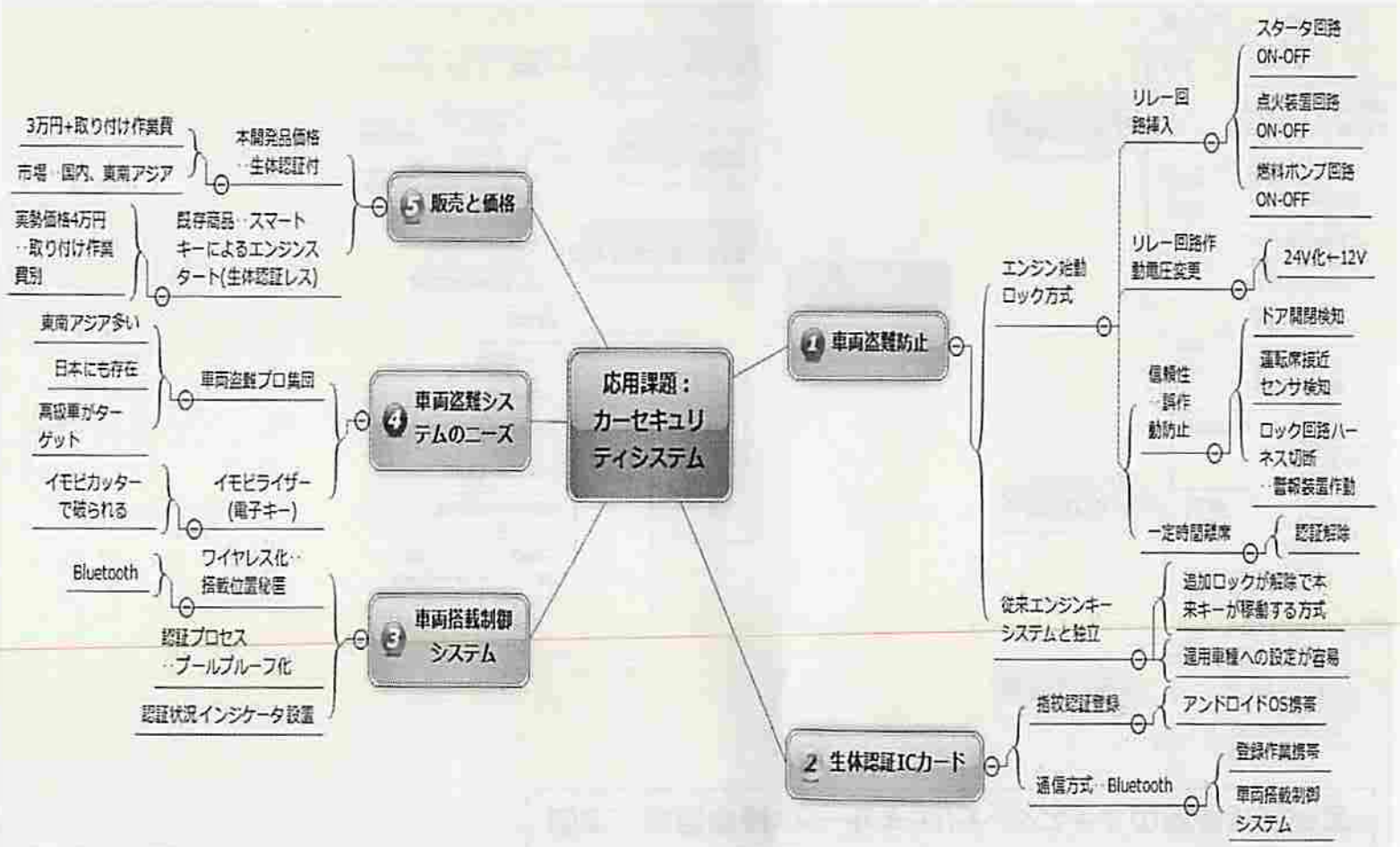
3 万円+取り付け作業費

市場‥国内、東南アジア

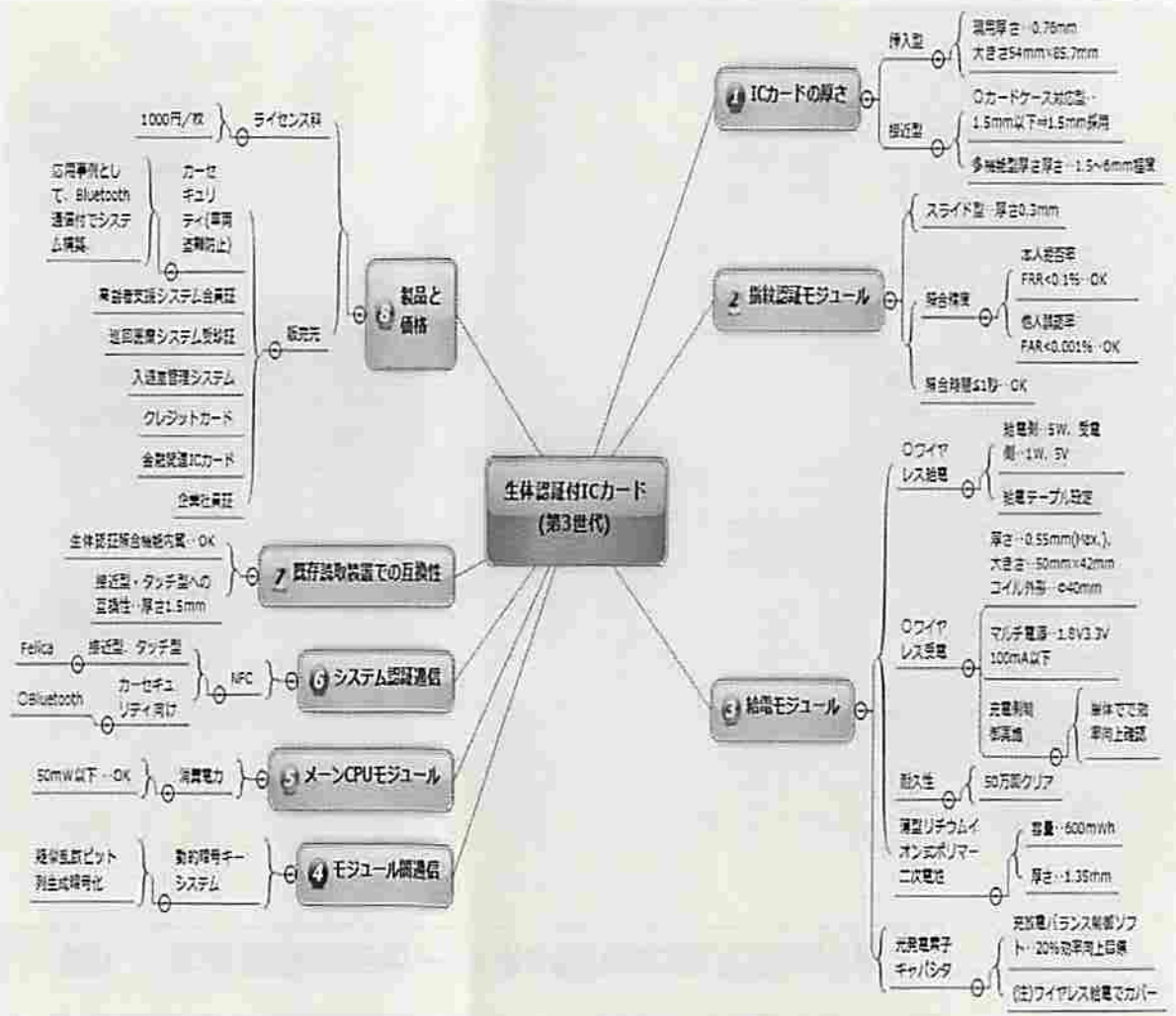
既存商品‥スマートキーによるエンジンスタート(生体認証レス)

実勢価格 4 万円 ‥取り付け作業費別

## 図1　生体認証付ICカード（第3世代）の開発実施内容



## 図2　応用事例：カーセキュリティシステムの開発実施内容



## 2-3まとめ

### 2-3-1 結言

(4) 接触型(タッチ方式)ICカードをベースに、従来のカード入れに収納可能な厚さ1．5mmで、予定する機能をすべて搭載し、目標を達成した。

(5) ICカードの安定した充電バランスを達成した。当初の光発電ディバイスは目標達成が難しく、実現にもコストがかかるため、将来性の高いコイル式によるワイヤレス給受電システムにて、目標を達成した。

(6) 応用事例として、カーセキュリティシステムへ適用し、ICカードの非接触通信として、Bluetooth を採用し、車載制御装置の秘匿性を高め、多重ロック機構と組み合わせた従来品と差別化されたセキュリティを達成した。また、作動の信頼性にも十分な配慮を加えた。

### 2-3-2今後の方針

(1) ICカードの厚さを挿入型(0.76mm)とするための各機能モジュールはほぼ目途がついているので、総合性能が確保できること目指す。指紋認証エリア型のコストと性能の両立、薄型二次電池(0.76mm以下)の電気容量増大が課題となる。

(2) 更に、作動信頼性と充放電バランスの確保が普及には必要となる。ライセンス料1000円／枚でのビジネスを検討する。

(3) 現在想定されているいくつかのニーズ先へのカードの提供だけでなく、自らその付加価値を増大させる応用事例システムの構築も手がける。バイタルデータの個人情報秘匿等への適用は将来有望である。

### 2-3-3 謝意

必要性が高く且つ技術的難度が高いAOCの開発に当たり、平成 22-23 年度の戦略的基盤技術高度化支援事業費助成の実施に深く感謝致します。この助成により、最大課題の1つであるカードセキュリティーのリーダーになるための第一歩が踏み出せました。今後はこの実績を生かし、AOCの市場導入、普及、大量生産にがんばんばりたいと考えています。

2-3-4 添付資料:

別紙1　高度化指紋認証まとめ概要
別紙2　カーセキュリティシステム報告書
別紙3　ワイヤレス給電システム報告書
別紙4　暗号化組込ソフト
別紙5　応用事例:カーセキュリティまとめ
別紙6　高度化提案書概要
別紙7　指紋認証付カード開発報告書

## 2-4 追記資料

### ア. ネットワークサービスの多様化(情報家電間のネットワーク化を含む)

#### A. 企業における入退室管理ネットワークのセキュリティ強化

企業等は研究部門の一部等に入退の厳しい部屋を持っている場合が多いが、一時的に入退を許可する人が生じる場合もありあいまいとなり易い。また、これからは、一般の業務にもセキュリティを導入するニーズが高まってきた。企業のグローバル化が進む企業ほどそのニーズは強い。従って、従業員全体へのトータルとしてのセキュリティシステムの導入のニーズがあり、セキュリティの高い生体認証への期待は大きい。しかし、最近導入が進んでいる社員証のICカード化が進んでおり、更に重複する高価な生体認証システムの導入はコスト的に厳しい状態である。盗難、紛失、置き忘れ等に対して高いセキュリティを確保できる生体認証付社員証ICカードであれば、ICカードのカード認証のアクティビティをカードに組み込まれている生体認証(指紋認証等)で行うことで、普及しているICカードを用いている認証システムを流用できるメリットがある。

#### B. 大学、研究所、各省庁・自治体での入退室・各種情報家電等の操作のセキュリティ・ネットワークの強化

大学での授業出欠管理への他人成りすまし防止や各期間での研究室や情報機器室等の入退室に関しても学生、業者、部外者等を含め多くの人の出入りがあり、企業と同様に、できるだけ現在のICカードシステムを活用し、廉価でセキュリティ強化が可能な生体認証付ICカード導入のニーズが強い。

#### C. 店舗、会員クラブでのICカード利用時のセキュリティ強化

買い物や利用料金の支払に関するセキュリティの強化は、客側も店舗側からも強いニーズがあり、支払機やクレジットカードとしてのカード会社との情報通信の際の本人確認機能の強化は求められている。

### イ. 信頼性の確保(機能安全確保を含む)

すでに広く普及している従来からのICカード認証装置への投資を無駄にしないで、ICカードの本人認証に関するセキュリティを強化することが求められている。現在は、銀行系等でカード認証窓口の装置側に生体認証の機能付きの新型の設置が始まっているが、その普及は進んでおらず、従来のシステムの方が多数派である。従って、普及の進まない窓口に設置してあるカード認証装置側ではなく、ICカード側での生体認証機能の付与のニーズがある。

**ウ。誰もが安心して使える**

指紋認証は、PC、携帯電話等のディバイス側に設置が始まっているが、その認証方式はコストの課題もあり、スリット型がほとんどである。その認証操作が指のスライドが必要であり、認証率は決して高くは無いため、普及にはいたっていない。だれでも安心して使える操作性のよい生体認証システムが望まれている。

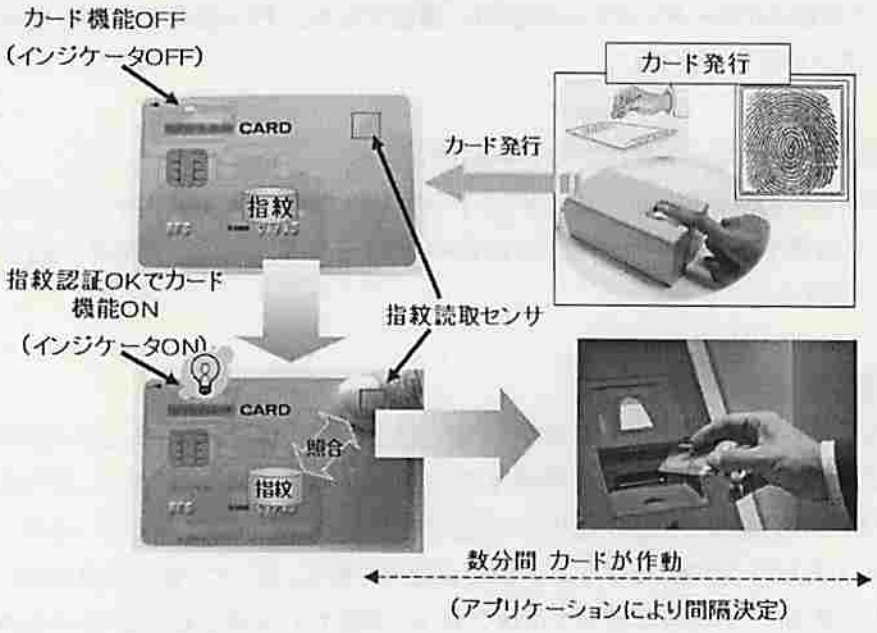
**エ. 利用者の理解、利用度の促進**

ICカード自身は、すでに普及が進んでおり、我々の生活の中に深く浸透している。生体認証付ICカードは、今までとほぼ同じ大きさで外見はほぼ同じであり違和感が無い。と同時に、カードの紛失時の不便さ、リスクの高さは多くの人が経験しているため、追加となる認証の操作への理解度は確保される。但し、課題として、生体認証への成功率を現在のICカード仕様時のものと遜色無いものにする必要がある。

**オ. 使い勝手の良さ**

認証できないため、機器が利用できなくなってしまうリスクや操作のめんどくさが寄与して、先行するディバイスに付属している生体認証システムは普及していない。従って、指紋認証においては。エリア式で、添えるだけでよく、認証率の高い認証システムの導入が必要である。

**Authenticate On Card(AOC) 概念**

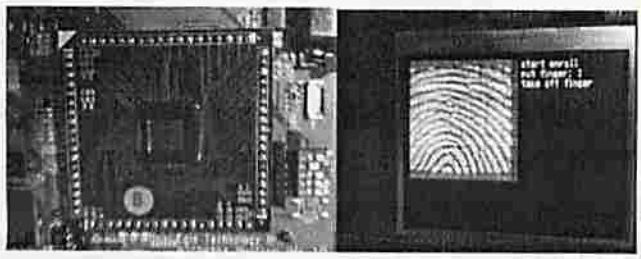


## 1) 研究開発の背景やこれまでの取り組みの概要

### ①センタ開発に成功(NEDOの開発)

弊社はカードの導入可能な指紋センサーの開発に成功した。カードに導入可能はセンサーは世界発である。その仕様は以下の通りである。

1) 指紋読取センサの厚み≦0.3㎜(ICカードの厚みは0.76㎜)
2) 指紋の読取面積＝8㎜角(ICカードの曲げ、捩れ強度を考慮)
3) 指紋読取センサの解像度≧508dpi
4) 指紋読取センサの読取寿命≧50万回
5) ESD:クラス4(カード上)
6) 指紋読取センサの消費電力≦50mW
7) 指の検知機能と生体検知機能の実現

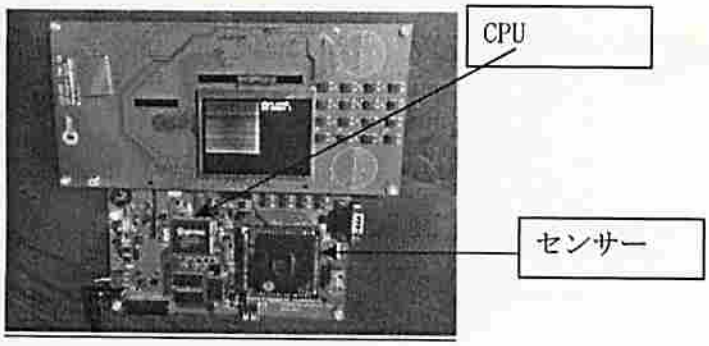


### ②CPU開発に成功(自社開発)

また同様にカードに導入可能か CPU を設計し、プロトタイプ開発を行った。

おもな仕様

1) 200MHz frequency, 32bits CPU
2) Input clk 12Mhz
3) Supply voltage 3.0~3.6V
4) 3.3V I/O, 1.2V core



2)当該分野の研究開発動向

・最新の技術水準や今後のトレンド、国内外の研究開発動向と応募テーマとの関係

ICカードの所有者の本人確認を生体認証(指紋認証)により実施する試みは、以下のような経緯を経て行われてきている。

【第一世代】

ICカードの内部メモリーに所有者の登録指紋情報を記録する。

本人確認は、PC等の外部装置にICカード内の登録指紋情報を一度読出し、その装置に接続された指紋読取手段により採取されたライブ指紋との照合をPC上で実施する。この方式の場合、登録された指紋をICカードの外部に読み出さねばならないと共に、PC上での照合実施がセキュリティーホールとなる。

【第二世代】

ICカードの中に登録指紋データと指紋の照合アルゴリズムを格納し、指紋のデータ抽出は外部装置に委ね、認証時にカード外部から照会用の指紋データを送りこむ。ICカードの外部からカードに渡される照合用指紋データの正当性にセキュリティー上の脆弱性が指摘される。 OKI 電気は先月発表したラインセンサー指紋カードは第2世代にある。またサンプル出荷価額は3000円と聞いている。

【第三世代】

本技術開発の課題となるAuthentification On Card(=以降AOC)にあたる。関連する内外の技術特許並びに規格は無い。

## 用語集

（1）ICカード

IC カード（アイシーカード、integrated circuit card; ICC）とは、情報（データ）の記録や演算をするために集積回路(IC)を組み込んだカードの事である。国際的にはスマートカード(smart card)やチップカード（chip card）とも呼ばれ、日本では特に演算処理機能を持つものをスマートカードと呼ぶ。

カード内に RAM や ROM、EEPROM といった半導体メモリを組み込む事により、情報量が従来の磁気ストライプカードと比べて数十倍から数千倍になる。さらに、CPU やコプロセッサなどを内蔵する事で、カード内部で情報処理が可能になるという特徴がある。

（2）FRR

本人拒否率（False Rejection Rate）。登録されたユーザ本人であるのに認証システムが誤って拒否してしまう率。

（3）FAR

他人受入率（False Acceptance Rate）。登録ユーザ以外の人であるのに認証システムが誤って登録ユーザとして受け入れてしまう率。