平成１５年度経済産業省委託事業成果

平成１５年度基準認証研究開発事業
生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化

平成１６年3月

社団法人日本自動認識システム協会

まえがき

本報告書は、平成15年度・基準認証研究開発事業として、経済産業省の委託により、社団法人日本自動認識システム協会が実施した「生体情報による個人識別技術（バイオメトリクス）を利用した社会基盤構築に関する標準化」の初年度事業に関する研究開発の成果を取りまとめたものである。

目　次

1.　総論（要約）・・・4

2.　委託業務実施計画・・7
2.1　事業の目的・・7
2.2　事業内容・・・8
2.3　実施体制・・・8
2.4　研究開発スケジュール・・10
2.5　本年度実施事項・・10
2.5.1　バイオメトリクスのリスク評価基準の研究開発・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・10
2.5.2　バイオメトリクス認証結果保証基盤の研究開発・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・11
2.5.3　バイオメトリクス精度評価環境の標準化・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・11
2.5.4　バイオメトリクスの可搬型メディアに応用するための技術調査・・・・・・・・・・・・・・・・・・・12

3.　バイオメトリクスセキュリティ評価基準の研究開発・・・・・・・・・・・・・・・・・・・・・・・・分冊　A
日立分室分として別途掲載。
4.　バイオメトリクス認証結果保証基盤の研究開発・・・・・・・・・・・・・・・・・・・・・・・・・・・分冊　B
東芝ソリューション分室分として別途掲載
5.　バイオメトリクス精度評価環境の標準化・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・分冊　C
日立エンジニアリング分室として別途掲載
6.　バイオメトリクスを可搬型メディア（近接型非接触ICカード）に応用するための技術調査
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・分冊　D
ニューメディア開発協会分室として別途掲載

（註　原本600ページに及もの、Web 掲載上、ご覧いただける方が扱いやすいように3章～6章まで分冊とした）

1. 総論

[研究目的]

身体的特徴あるいは行動パターンなどを利用して本人の識別を行うバイオメトリクス要素技術の発展に伴い、これらの技術を応用したシステム構築の試みが活発化している。

生体情報による個人識別技術（バイオメトリクス）は他人へのなりすましや、偽造を防ぐ有効な手段として期待されており、安全な社会基盤の実現には不可欠な技術であり、また、バイオメトリクスを情報セキュリティ分野に適用するには、バイオメトリクスの安全性評価が重要となって来る。しかし現状では、情報セキュリティの観点に基づいたバイオメトリクスの安全性に関する検討が充分になされていない。

また、生体情報を記録したパスポートや、社会 ID として、ICカードが現実のものになろうとしており、バイオメトリクス情報を近接型ICカード（PICC）に記録し、所持者認証に応用するには、電子カメラから得られた顔画像を、圧縮技術（JPEG－2000）で記録したデータとスキャナーで取り込んだ電子データとを照合し、所定の性能と精度が要求されている。しかしながら、これまでにPICCに応用した標準化報告はなく、国際民間航空機関（ICAO）の最新技術レポートにおいても高機能なパーソナルコンピュータ（PC）による机上データでの検証に留まっている。

更には、バイオメトリクス情報をテンプレートデータ、或いは、データベースとして管理し、運用していくためには、個人情報を収集する際の課題や、プライバシー、法的、文化的な諸問題を整理、分析し、課題を明確化する必要がある。

そこで実用化に向けた各種の課題を明確にするために、下記の4項目を研究開発テーマとして本事業を推進した。

本研究開発における成果は、基盤技術である評価基準、評価環境等に関する国際標準案を策定して、国際標準化機構（ISO）と国際電気標準会議（IEC）の合同専門委員会（JTC 1）の分科委員会SC37、SC17等へ提案することを目指す。

1）バイオメトリクスセキュリティ評価基準の研究開発
2）バイオメトリクス認証結果保証基盤の研究開発
3）バイオメトリクス精度評価環境の標準化
4）バイオメトリクスの可搬型メディアに応用するための技術調査

[研究内容]

①バイオメトリクスセキュリティ評価基準の研究開発

今年度は、バイオメトリクスセキュリティに関する現状の技術、制度及び標準に関する調査

を行った。また、次年度以降の具体的な作業項目を明確にするため、課題の抽出を行った。具体的には、以下の研究開発を実施した。

a) バイオメトリクスのリスク評価基準の調査研究

バイオメトリクスの脅威及び脆弱性に関する現在の研究状況を調査及び分析し、今後の課題を明確にした。

b) バイオメトリクスのセキュリティ要件と評価方法の調査研究

欧米で策定されたバイオメトリクス向けのプロテクションプロファイル（PP）及び共通評価方法論（CEM）を調査及び分析し、今後の課題を明確にした。

c) バイオメトリクスの脅威及び脆弱性公開におけるガイドラインの調査研究

コンピュータウィルス等バイオメトリクス以外の情報セキュリティにおける脅威及び脆弱性公開の基準に関する調査及び分析を行い、バイオメトリクスに適用する際の課題を明確化した。

②バイオメトリクス認証結果保証基盤の研究開発

バイオメトリクスをネットワーク等のオープン環境に適用するには、認証者（認証する組織、人等）に対して安全な環境と認証結果が改竄されていないことを保証する必要がある。このため、今年度具体的には、以下の研究開発を実施した。

a) バイオメトリクス保証基盤の調査研究

バイオメトリクスをオープン環境で利用する際の現状の問題点を整理し、今後の課題を明確にするとともに、本技術の仕様について整理を行った。

b) バイオメトリクス認証プロトコルの調査研究

バイオメトリクス保証基盤を実現するために必要となる、公開鍵基盤（PKI）を用いたバイオメトリクス認証プロトコルに関する調査を行い、その有効性や付随する課題について明確にした。

c) バイオメトリクス・デバイス証明書のプロファイルに関する調査研究

SC37WG5、バイオメトリクステストセンター（米国）のバイオメトリクスWG、国立物理学研究所（ナショナル　フィジカル　ラボラトリー、英国）、電子通信セキュリティグループ（コミュニケーション　エレクトロニクス　セキュリティ　グループ、英国）、財団法人日本規格協会（JSA）の情報技術標準化研究センター（INSTAC）等で検討されているデバイスの精度評価基準や、ANSI規格等との連携を取るための調査を行い、その結果の整理を行った。

③バイオメトリクス精度評価環境の標準化

日本工業規格（JIS）の標準情報（TR）「指紋、顔、虹彩等認証システムの精度評価方法」に定めたバイオメトリクス精度評価を実施するため、評価環境、評価に用いるデータベース及び運用におけるテンプレートファイルを構築する場合を想定して、国内外における現状技術に関する調査を行い、分析、整理すると共に課題を明確にした。

具体的には、最も早期の実現が求められるパスポートへのバイオメトリクス情報の搭載に関して「顔」を題材に作業を実施し、今後の検討課題を明確にした。

具体的には、以下の調査等を実施した。

a) バイオメトリクス個人情報収集に関する課題抽出

国内外におけるバイオメトリクス装置の評価実験及び評価方法の標準化に関する文献を調査し、システム評価段階及び運用段階において必要となるバイオメトリクスデータ、付随する個人情報、被験者の分布と数、登録方法、登録から照合までのエージング、照合試行回数、適用不可の判断基準等を定量的に見積もり、課題を分析した。

b) バイオメトリクス運用における個人保護並びに法的、文化的及び医学的な諸問題の調査

これまでに構築された国内外の標準データベースの製作機関に対して聞き取り調査を行い、プライバシー問題及び法的側面の取り扱いを調査した。

また、バイオメトリクス個人認証に対する国民感情（寛容あるいは忌避の度合い等）や、バイオメトリクスデータに対する取扱いの文化的側面を調査した。

さらに、バイオメトリクスデータが公的機関によって管理される場合、その取り扱い方法や管理方法について調査し、問題点や解決するべき課題を明らかにした。

なお、本項b）は、京都大学大学院に、再委託して実施した。

④バイオメトリクスの可搬型メディアに応用するための技術調査

今年度は、PICCにバイオメトリクスを応用するために必要な以下の3点の調査等を行った。

a) 米国連邦標準技術局（NIST）政府系カード国際統一仕様書、ICAO技術レポート（2003年4月版）及び国内ベンダー技術の調査

国内のベンダー各社は個別に開発を行っているため、標準化推進に当たって必要な技術調査（国際互換性のための最新の技術レポート等）を行った。

b) 顔画像の実用化に必要なファイル、コマンド等統一仕様書（案）の作成

顔画像記録データは、既存のICカード用チップが一度に処理を行えるRAM容量を超えるため、データを分割しながら照合処理を繰り返すことになる。この分割処理に対応したデータ構造（ロジカル・データ・ストラクチャー）を定める統一仕様書（案）を作成した。

c) ISO／IEC14443タイプBによる机上実データの作成と国際提案書の作成

NIST政府系カード国際統一仕様書及びICAO技術レポートにおける顔画像データの記述は、全てPC上での机上データで作成されている。本事業では、わが国で既に実用し、PCに比べ処理能力が限られているPICCタイプBカードによるデータを作成し、国際提案にもって行く。

なお、本テーマは、財団法人ニューメディア開発協会に、再委託して実施した。

2. 委託業務実施計画

2.1 事業の目的

生体情報による個人識別技術（バイオメトリクス）は他人へのなりすましや、偽造を防ぐ有効な手段として期待されており、安全な社会の実現には不可欠な技術である。バイオメトリクスを情報セキュリティ分野に適用するには、バイオメトリクスの安全性評価が重要である。しかし、情報セキュリティの観点に基づいたバイオメトリクスの安全性に関する検討が充分になされていないのが現状である。そこで本事業では、バオイメトリクスの実用化を推進するために、

①基盤技術である評価基準、評価環境等に関する国際標準案を策定して、国際標準化機構（ISO）と国際電気標準会議（IEC）の合同専門委員会（JTC1）の分科委員会（SC37）等へ提案することを目指す。

また、バイオメトリクスをオープンなネットワーク環境等に適用するには、認証者（認証する組織、人等）に対して安全な環境と認証結果が改竄されていないことを保証する必要があることから、

②バイオメトリクス認証結果保証基盤の研究開発

更に、ネットワーク環境下にバイオメトリクスデータベースを生成したり、ICカード等の媒体上にバイオメトリクステンプレートデータを生成する場合など、様々な使用形態を考慮して、精度評価環境を検討する必要がある。それぞれのバイオメトリクスについて技術的な精度評価環境を調査分析する必要があるが、各々の技術課題と並行して、共通する課題、即ち

③バイオメトリクス運用における個人保護並びに法的、文化的及び医学的な諸問題の調査とバイオメトリクス個人情報を収集する場合の課題等を検討し、ISO／IEC JTC1 SC37 WG5及びWG6へ日本案として提案を目指す。

バイオメトリクスを近接型ICカード（PICC）に記録し、所持者認証に応用するには、電子カメラから得られた顔画像を、圧縮技術（JPEG－2000）で記録したデータとスキャナーで取り込んだ電子データとを照合する必要がある。しかしながら、これまでにPICCに応用した標準化報告はなく、国際民間航空機関（ICAO）の最新技術レポートにおいても高機能なパーソナルコンピュータ（PC）による机上データでの検証に留まっている。そこ

で、

④バイオメトリクスを可搬型メディアに応用するための技術調査を行い、SC17 WG3及びSC37へ技術レポートとして報告する。

2.2 事業内容

本研究開発事業において、下記4点を推進する。

(1) バイオメトリクスセキュリティ評価基準の研究開発

(2) バイオメトリクス認証結果保証基盤の研究開発

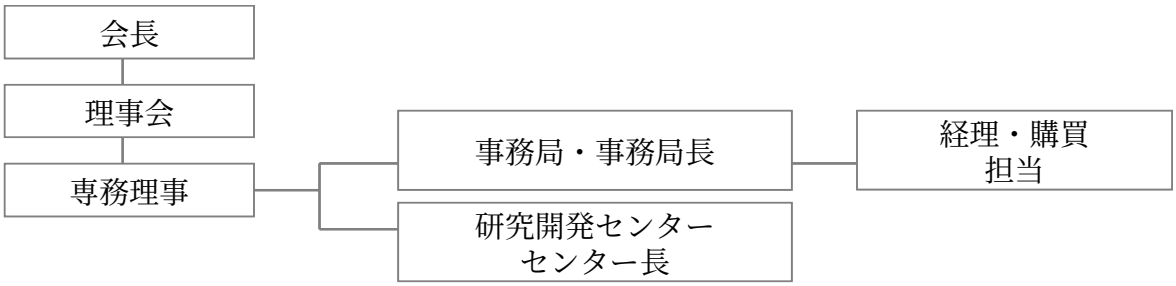
(3) バイオメトリクス精度評価環境の標準化

(4) バイオメトリクスを可搬型メディアに応用するための技術調査

2.3 実施体制

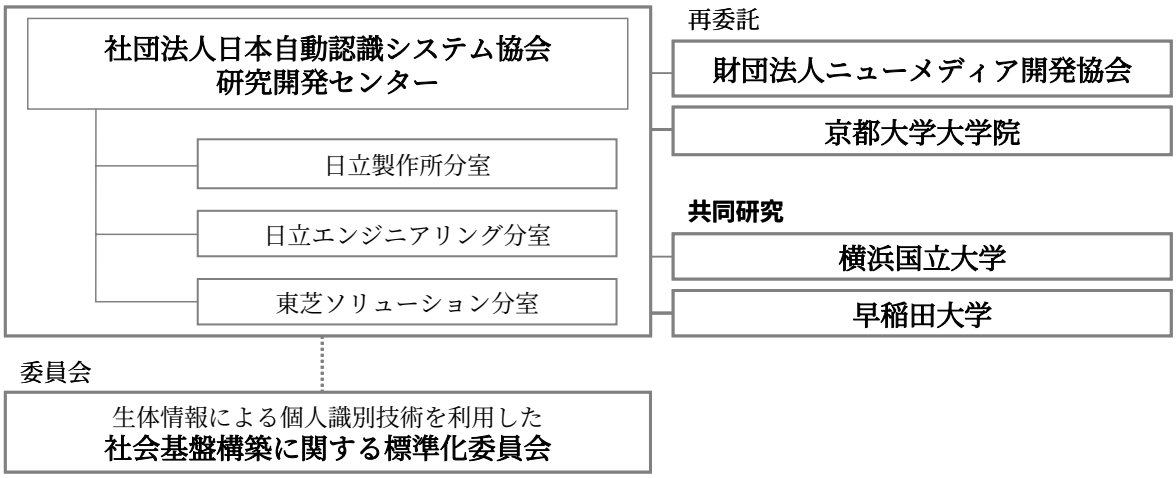
(1) 研究管理体制

本委託事業は、社団法人日本自動認識システム協会が受託し、研究開発の管理、取りまとめを実施した。下記は、同協会による管理体制である。



(2) 研究開発体制

本委託事業は、下記の通りの開発体制をとり、産業界の主たる企業と大学の研究機関による共同の研究開発を実施した。



(3) 共同研究者

本研究開発に協力いただいた大学の研究機関は、下記の通りである。

研究機関名	所属	役職	氏名
京都大学大学院	情報学研究科	ＣＯＥ研究員	鷲見　和彦
横浜国立大学	環境情報研究院	教授	松本　　勉
早稲田大学	理工学部	教授	小松　尚久

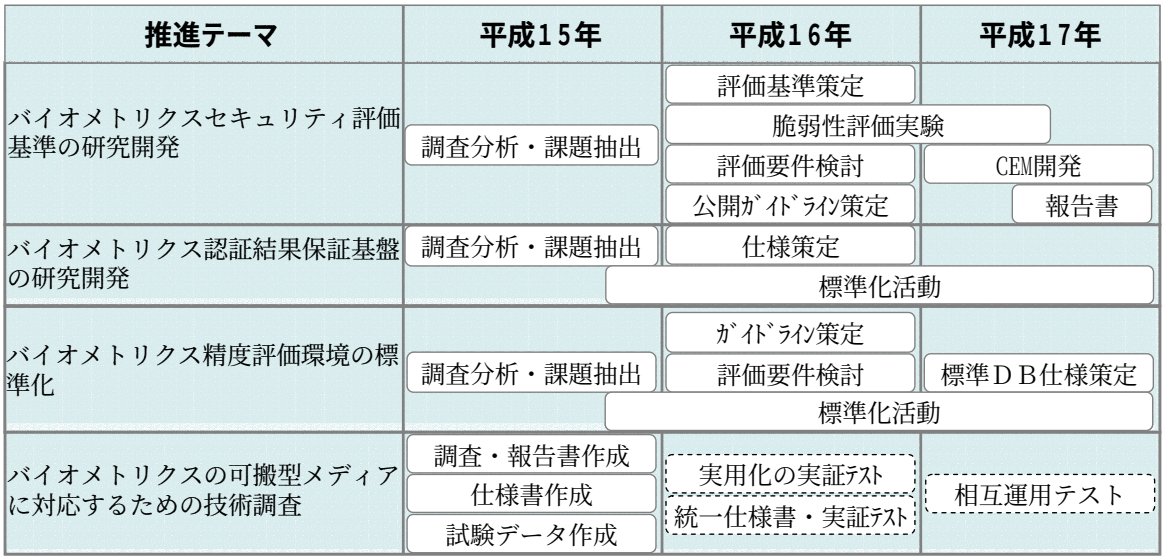
(4) 委員会構成メンバー

委員	研究機関名	所属	役職	氏名
委員長	東京理科大学	工学部・電気工学科	教授	半谷　精一郎
幹事	ＳＣ３７国内委員会		委員長	瀬戸　洋一
委員	経済産業省	産業技術環境局標準課	室長	坂井　喜毅
委員	経済産業省	製造産業局産業機械課	課長補佐	上山　辰美
委員	(財）日本規格協会	標準部	部長	八田　　勲
委員	名古屋工業大学	大学院・工学研究科	教授	梅崎　太造
委員	東京工科大学	メディア学部	専任講師	村上　康二郎
委員	ＢＳＣ	基盤技術部会	部会長	池野　修一
委員	ＢＳＣ	基盤技術部会	WG1主査	笹川　耕一
委員	ＢＳＣ	基盤技術部会	WG3主査	宇都宮　康夫
委員	ＢＳＣ	運用仕様策定部会	部会長	尼子　大介
委員	ＢＳＣ	運用仕様策定部会	幹事	赤津　昌幸
委員	ＳＣ１７国内委員会		委員長	大山　永昭
委員	ＳＣ２７国内委員会		委員長	宝木　和夫
オブザーバー	経済産業省	産業環境局標準課	課長補佐	勝亦　眞人
オブザーバー	経済産業省	産業環境局標準課	専門職	小谷　光弘
オブザーバー	情報処理振興事業協会	セキュリティーセンター		宮川　寧夫
オブザーバー	電子商取引推進協議会		主席研究員	浅沼　省吾
事務局	(社）日本自動認識ｼｽﾃﾑ協会		主任研究員	赤沼　　泰
事務局	(社）日本自動認識ｼｽﾃﾑ協会		主任研究員	中嶋　晴久

2．4　研究開発スケジュール

本研究開発事業は、平成15年を初年度として、3ヵ年の実施計画を策定した。本項では、その3ヵ

年の開発スケジュールを示す。



2．5　本年度実施事項

以下に、事業内容別の本年度実施事項を述べる。

2．5．1　バイオメトリクスセキュリティ評価基準の研究開発

本年度は、バイオメトリクスセキュリティに関する現状の技術、制度及び標準に関する調査を行った。また、次年度以降の具体的な作業項目を明確にするため、課題の抽出を行った。

具体的には、以下の研究開発を実施した。

(1) バイオメトリクスのリスク評価基準の調査研究

バイオメトリクスの脅威及び脆弱性に関する現在の研究状況を調査･分析し、今後の課題を明確化した。

(2) バイオメトリクスのセキュリティ要件と評価方法の調査研究

欧米で策定されたバイオメトリクス向けのプロテクションプロファイル（ＰＰ）及び共通評価方法論（ＣＥＭ）を調査･分析し、今後の課題を明確化した。

(3) バイオメトリクスの脅威及び脆弱性公開におけるガイドラインの調査研究

コンピュータウィルス等バイオメトリクス以外の情報セキュリティにおける脅威及び脆弱性公開の基準に関する調査･分析を行い、バイオメトリクスに適用する際の課題を明確にした。

2．5．2　バイオメトリクス認証結果保証基盤の研究開発

バイオメトリクスをネットワーク等のオープン環境に適用するには、認証者（認証する組織、人等）に対して安全な環境と認証結果が改竄されていないことを保証する必要がある。具体的には本年度、以下の研究を実施した。

(1) バイオメトリクス保証基盤の調査研究

バイオメトリクスをオープン環境で利用する際の現状の問題点を整理し、今後の課題を明確にし、本技術の仕様について整理した。

(2) バイオメトリクス認証プロトコルの調査研究

バイオメトリクス保証基盤を実現するために必要となる、公開鍵基盤(PKI)を用いたバイオメトリクス認証プロトコルに関する調査を行い、その有効性や付随する課題について明確にした。

(3) バイオメトリクス・デバイス証明書のプロファイルに関する調査研究

海外や、国内で検討されているデバイスの精度評価基準や、ANSI規格等との連携をとるための調査を行い、その結果を整理した。

2.5.3 バイオメトリクス精度評価環境の標準化

指紋、顔、虹彩等認証システムの精度評価方法(JIS－TR)に定めたバイオメトリクス精度評価を実施するため、評価環境、評価に用いるデータベース及び運用におけるテンプレートファイルを作成する場合を想定して、国内外における現状技術に関する調査を行い、課題を明確にした。 具体的には、本年度、以下の調査を実施した。

(1) バイオメトリクス個人情報収集に関する課題の抽出

国内外におけるバイオメトリクス装置の評価実験及び評価方法の標準化に関する文献を調査し、システム評価段階及び運用段階において必要となるバイオメトリクスデータや、付随する個人情報、被験者の分布と数、登録方法、登録から照合までのエージング、照合試行回数、適用不可の判断基準等を定量的に見積もり、課題を分析した。

(2) 個人保護及び法的、文化的、医学的な諸問題の調査

これまでに構築された国内外の標準データベースの製作機関に対して聞き取り調査を行い、プライバシー問題及び法的側面や、バイオメトリクス個人認証に対する国民感情(寛容あるいは忌避の度合い等)や、バイオメトリクスデータに対する取扱いの文化的側面を調査した。

また、バイオメトリクスデータが公的機関によって管理される場合、その取り扱い方法や管理方法について調査し、問題点や解決するべき課題を明らかにした。

2.5.4 バイオメトリクスの可搬型メディアに応用するための技術調査

本年度は、PICC(近接型ICカード)にバイオメトリクスを応用するために必要な以下の3点の技術調査を行った。

(1) 米国連邦標準技術局(NIST)政府系カード国際統一仕様書、ICAO技術レポート(200

3年4月版）及び国内ベンダー技術の調査

国内のベンダー各社は個別に開発を行っているため、標準化推進に当たって必要な技術調査（国際互換性のための最新の技術レポート等）を行った。

（2）顔画像の実用化に必要なファイル、コマンド等統一仕様書（案）の作成

顔画像記録データは、既存のICカード用チップが一度に処理を行えるRAM容量を超えるため、データを分割しながら照合処理を繰り返すことになる。この分割処理に対応したデータ構造（ロジカル・データ・ストラクチャー）を定める統一仕様書（案）を作成した。

（3）ISO／IEC14443タイプBによる机上実データの作成と国際提案書の作成

NIST政府系カード国際統一仕様書及びICAO技術レポートにおける顔画像データの記述は、全てPC上の机上データで作成されている。そこで、わが国で既に実用化され、PCに比べ処理能力が限られているPICCタイプBカードによるデータを作成し、評価を行った。

3. バイオメトリクスセキュリティ評価基準の研究開発

日立分室分として別途掲載。

4. バイオメトリクス認証結果保証基盤の研究開発

東芝ソリューション分室分として別途掲載

5. バイオメトリクス精度評価環境の標準化

日立エンジニアリング分室として別途掲載

6. バイオメトリクスを可搬型メディア（近接型非接触ICカード）に応用するための技術調査

ニューメディア開発協会分室として別途掲載