

システム技術開発調査研究

22-R-6

アイデンティティ・マネジメントへの  
バイオメトリクス組み込み時の課題と  
海外動向、標準化動向に関する調査研究

報 告 書

— 要 旨 —

平成23年3月

財団法人機械システム振興協会  
委託先 社団法人日本自動認識システム協会



この事業は、競輪の補助金を受けて実施したものです。

<http://ringring-keirin.jp>

## 序

わが国経済の安定成長への推進にあたり、機械情報産業をめぐる経済的、社会的諸条件は急速な変化を見せており、社会生活における環境、防災、都市、住宅、福祉、教育等、直面する問題の解決を図るためには、技術開発力の強化に加えて、ますます多様化、高度化する社会的ニーズに適応する機械情報システムの研究開発が必要であります。

このような社会情勢に対応し、各方面の要請に応えるため、財団法人機械システム振興協会では、財団法人JKAから機械工業振興資金の交付を受けて、機械システムに関する調査研究等補助事業を実施しております。

これらを効果的に実施するために、当協会に総合システム調査開発委員会（委員長：東京大学名誉教授 藤正 巖氏）を設置し、同委員会のご指導のもとに推進しております。

この「アイデンティティ・マネジメントへのバイオメトリクス組み込み時の課題と海外動向、標準化動向に関する調査研究報告書」は、上記事業の一環として、当協会が社団法人日本自動認識システム協会に委託して実施した成果であります。関係諸分野に関する施策が展開されていく上で、本調査研究の成果が一つの礎石として皆様方のお役に立てれば幸いです。

平成23年3月

財団法人機械システム振興協会

## はじめに

1980年代までの一般的なコンピュータの利用においては、コンピュータの利用自体がシステム管理者から権限を与えられたユーザに限定されていた。またユーザはホストコンピュータに接続された端末の利用者であった。つまり、ITリソースへのアクセスはそのコンピュータのシステム管理者により物理的に制御されていたとあって良いと考えられる。

しかし、オープンシステム、クライアント・サーバといったコンピュータ・パラダイムの変遷、メインフレームの他、UNIX、Windows、更にはLinuxというプラットフォームの多様化、業務分野ごとのシステム構築、インターネットなどによるネットワーク社会の普及、またインターネット上の商用サービスの普及により、現在、例えば、企業においては、業務従事者一人に1台以上のパソコン、複数のサービスの使用が一般的となっており、ユーザに付与されるアクセス権限を管理すべき対象が増加しており、従来のシステム管理の一環としてユーザのアクセスの制御を行うことが事実上不可能となっている。

また、近年の電子行政サービスの充実に伴い、サービス形態が多様化し、各サービス間での認証連携も必要となることが予想される中で、サービスを安全で安心な形で提供するために、システムを利用するユーザのアクセス権限の管理の重要性が増してくるものと予想している。

また、これら社会生活の環境が大きく変わる一方で、IDやパスワードの盗用、なりすましなどのセキュリティに関する問題も発生している。従来から公共、あるいは民間のサービスの本人確認手段として、本人以外が知り得ない情報（IDやパスワードなど）や、本人以外が持ち得ない身分証明書（IDカード、健康保険証、運転免許証など）が用いられているが、なりすましなどを防止するには、生体情報（バイオメトリクス）を利用した個人認証技術が有効であるともいわれている。

本事業では、バイオメトリック認証の高いセキュリティ機能とIdM技術をとともに提供することを可能にすることを目指して、IdMアーキテクチャについて調査するとともに、IdM技術とバイオメトリック認証を標準的に組み合わせるためのアーキテクチャの基本方式について検討した。

本報告書では、IdMアーキテクチャについて調査した結果、また、IdM技術とバイオメトリック認証を標準的に組み合わせるためのアーキテクチャの基本方式と、それを実現するあたりの課題や、それに伴うプライバシー保護の課題の明確化とその対策について取りまとめた。

今後、関係諸分野に関する施策が展開されていく上で、本調査研究の成果がお役に立てば幸いです。

最後になりますが、本調査研究の実施にあたり、総合システム調査開発委員会の藤正委員長(東京大学)、委員各位、また、バイオメトリクスIdM研究委員会の半谷委員長(東京理科大学)、委員各位をはじめとし、ご指導を賜った関係者各位に対し、心より深く感謝を申し上げます。

平成23年3月

社団法人日本自動認識システム協会

## 目 次

序

はじめに

目 次

1. 調査研究の目的 .....	1
2. 調査研究の実施体制 .....	1
3. 調査研究の内容 .....	4
4 調査研究成果の要約 .....	5
4-1 IdMアーキテクチャの分析調査 .....	5
4-2 国内・海外の研究開発動向調査 .....	12
4-3 バイオメトリック技術を実装したIdMアーキテクチャの基本方式の検討 .....	19
4-4 プライバシー保護の課題の明確化とその対策について .....	33
4-5 調査研究の成果（まとめ） .....	45
5. 調査研究の課題及び今後の展開 .....	48

## 1. 調査研究の目的

2001.9.11の世界同時多発テロ以降、個人認証の重要性が年々増加し、個人認証に利用するアイデンティティの管理や運用が複雑になり、その構築運用コストが増大し、運用管理のリスクも増大している。このため、効率的に、かつ確実にアイデンティティを管理することが求められている。

これを解決するための中心技術がバイオメトリクスであり、アイデンティティ管理(Identity Management: IdM)への導入が期待されている。

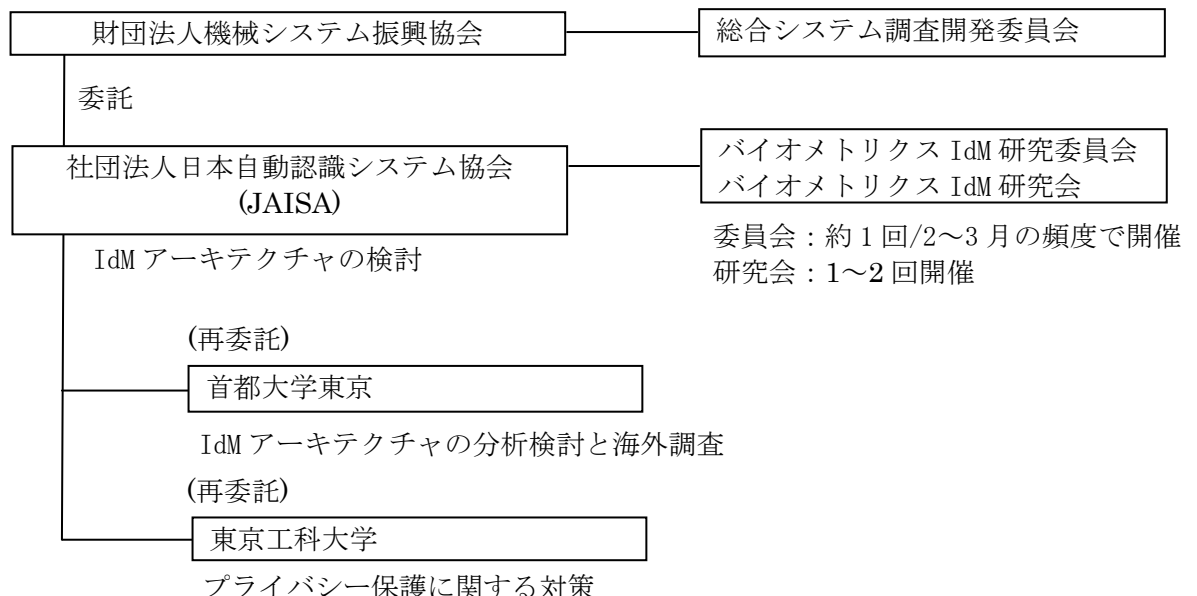
バイオメトリック技術を IdM に導入するには、IdM に関する最新の技術や標準化の動向を調査し、IdM アーキテクチャを明確にすることが必要である。また、バイオメトリック技術を実装するためのアーキテクチャを明確にし、個人の究極の情報であるバイオメトリクスを利用することにより新たに生じるプライバシー問題を明確にし、その対策について検討する必要がある。

本調査研究では、IdM アーキテクチャに関し、先行する欧米各国の技術開発及び国際標準の動向調査、バイオメトリック技術を IdM アーキテクチャに実装する場合の基本方式の検討、及びバイオメトリック技術を導入することによるプライバシー問題の明確化をとおり、システム及び製品を開発・運用するための方向性を示すことを目的とした。

## 2. 調査研究の実施体制

財団法人機械システム振興協会内に総合システム調査開発委員会を設置し、社団法人日本自動認識システム協会(以下 JAISA という。)が調査研究を受託し、海外の状況調査については首都大学東京に、プライバシー保護への対応として東京工科大学に、それぞれ再委託し、IdM へのバイオメトリクスの最適なアーキテクチャの検討については(株) OKI ソフトウェアから役務提供を受け JAISA にて対応した。

またプロジェクトの内容の確認と進捗管理のため3回の委員会を設け、内容の更なる深化を目指し研究会を1~2回設けることとした。



(3) 委員名簿

①総合システム調査開発委員会 (順不同・敬称略)

	氏名	所属	役職
委員長	藤正 巖	東京大学	名誉教授
委員	太田 公廣	埼玉大学 総合研究機構	教授
委員	金丸 正剛	独立行政法人産業技術総合研究所 エレクトロニクス研究部門	研究部門長
委員	志村 洋文	独立行政法人産業技術総合研究所 先進製造プロセス研究部門	招聘研究員
委員	中島 一郎	早稲田大学 研究戦略センター	教授
委員	廣田 薫	東京工業大学大学院 総合理工学研究科	教授
委員	藤岡 健彦	東京大学大学院 工学系研究科	准教授

②バイオメトリクス IdM 研究委員会 (順不同・敬称略)

	氏名	所属	役職
委員長	半谷精一郎	東京理科大学 工学部電気工学科	教授 SC37 WG3 委員
委員	寶木 和夫	(株)日立製作所 システム開発研究所	SC27 委員長
委員	倉内 喜孝	ソニー(株) B2B ソリューション事業本部	SC37 WG2 主査
委員	新崎 卓	(株)富士通研究所 画像・バイオメトリクス研究センター	SC37 WG3 主査
委員	緒方日佐男	日立オムロンターミナルソリューションズ(株) アドバンスト・テクノロジー事業部	SC37 WG3 幹事
委員	平野 誠治	凸版印刷(株) 事業開発・研究本部 総合研究所 情報技術研究室	SC37 WG3 エキスパート
委員	濱中 雅彦	日本電気(株) 第二官公ソリューション事業部	SC37 WG3 幹事
オブザーバ	川内 拓行	経済産業省 製造産業局 産業機械課	係長
推進委員	中村 敏男	(株)OKI ソフトウェア 企画室	SC37 WG2 委員
推進委員	瀬戸 洋一	公立大学法人首都大学東京 産業技術大学院大学 産業技術研究科専門	教授 SC37 専門委員会 委員長
推進委員	村上康二郎	東京工科大学 メディア学部	准教授 SC37 WG6 委員
事務局	高田 敏雄	社団法人日本自動認識システム協会	JAISA 専務理事
事務局	酒井 康夫	社団法人日本自動認識システム協会	
事務局	森本 恭弘	社団法人日本自動認識システム協会	

③バイオメトリクス IdM 研究会（順不同・敬称略）

	氏名	所属	役職
委員長	半谷精一郎	東京理科大学 工学部電気工学科	教授 SC37 WG3 委員
委員	寶木 和夫	(株)日立製作所 システム開発研究所	SC27 委員長
委員	倉内 喜孝	ソニー(株) B2B ソリューション事業本部	SC37 WG2 主査
委員	新崎 卓	(株)富士通研究所 画像・バイオメトリクス研究センター	SC37 WG3 主査
委員	緒方日佐男	日立オムロンターミナルソリューションズ(株) アドバンスト・テクノロジー事業部	SC37 WG3 幹事
委員	平野 誠治	凸版印刷(株) 事業開発・研究本部 総合研究所 情報技術研究室	SC37 WG3 エキスパート
委員	濱中 雅彦	日本電気(株) 第二官公ソリューション事業部	SC37 WG3 幹事
講師	井上 春樹	静岡大学 情報基盤センター	教授
講師	石井夏生利	筑波大学大学院 図書館情報メディア研究科	准教授
講師	津国 剛	(株)三菱総合研究所 社会システム研究本部	主任研究員
オブザーバ	川内 拓行	経済産業省 製造産業局 産業機械課	係長
推進委員	中村 敏男	(株) OKI ソフトウェア 企画室	SC37 WG2 委員
推進委員	瀬戸 洋一	公立大学法人首都大学東京 産業技術大学院大学 産業技術研究科専門	教授 SC37 専門委員会 委員長
推進委員	村上康二郎	東京工科大学 メディア学部	准教授 SC37 WG6 委員
事務局	高田 敏雄	社団法人日本自動認識システム協会	JAISA 専務理事
事務局	酒井 康夫	社団法人日本自動認識システム協会	
事務局	森本 恭弘	社団法人日本自動認識システム協会	

### 3. 調査研究の内容

本調査研究では、アイデンティティ・マネジメント(IdM)の技術並びにバイオメトリクス認証技術の導入が先導的に進められている欧米諸国の IdM アーキテクチャに関する最新の技術動向や標準化の動向を調査し、バイオメトリック技術を IdM アーキテクチャに実装する場合の基本方式の検討、及びバイオメトリック技術を導入することによるプライバシー問題の明確化を通し、システム及び製品を開発・運用するための方向性を示すために、次の 4 項目について調査研究を行うこととした。

#### (1) IdM アーキテクチャの分析調査

- ・代表的なアプローチである **OpenID**、**Liberty Alliance**などを例にアイデンティティ・マネジメントの技術の詳細現状を把握する。

#### (2) 国内・海外の研究開発動向調査

- ・カンファレンス調査

米国におけるカンファレンスでの講演を調査し最先端の動向を調査する。

- ・ウェブ調査(米国、EU)

特に米国大統領府 **National Science Technology Council** に設置された IdM とバイオメトリクス委員会の状況を中心に米国の情報を調査する。

- ・国際標準化委員会での標準化動向を調査する。

SC37 他で開発が進む IdM 標準化動向を調査する。

#### (3) バイオメトリック技術を実装した IdM アーキテクチャの基本方式の検討

- ・アイデンティティ・マネジメントシステムは現状パスワードでの運用が中心となっており、バイオメトリクスを組み込んだ本格的な運用には至っていない。本調査研究では **OpenID** や **Liberty Alliance** などのアイデンティティ管理システムを中心に、バイオメトリクス機能を組み込むためのアーキテクチャの検討及び提案を行う。

#### (4) プライバシー保護の課題の明確化とその対策について

- ・バイオメトリック技術を IdM に実装する場合、バイオメトリクスが究極の個人情報のため、セキュリティの確保が大きな課題となる。つまりプライバシー保護は極めて重要である。課題と対策のフレームワークを明確にする。

## 4 調査研究成果の要約

### 4-1 IdMアーキテクチャの分析調査

日経データボード、日本国内のアイデンティティ管理市場(藤巻信之 2009年9月)によると、日本のアイデンティティ管理市場は近年拡大しており、図 4.1.1 に示すように、2008年度(2008年4月～2009年3月)に出荷金額ベースで対前年度比 20.0%増成長し、約 109 億円となった[1][2]。

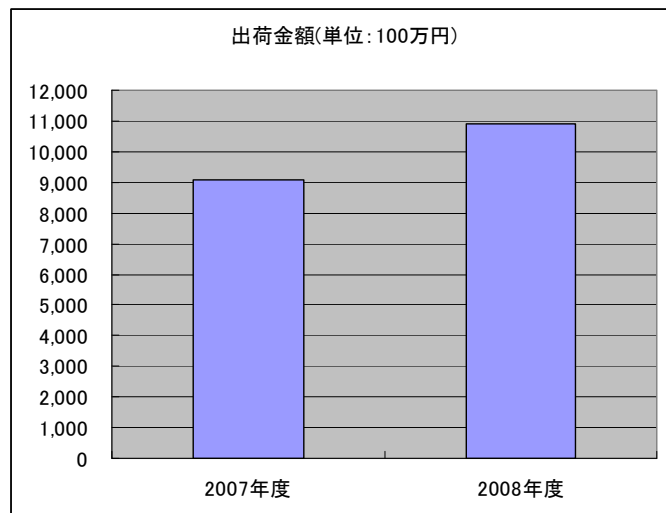


図 4.1.1 日本国内のアイデンティティ管理市場規模の予測推移

また、世界のアイデンティティ管理市場は、図 4.1.2 に示すように、2006年で 31 億米ドル、2010年には 50 億米ドルを超えた。2014年には 123 億米ドルに達すると予想する報告がある[3][4]。ここで成長率は年約 20%であり、今後市場を牽引する重要なアプリケーション分野であるといっている。技術分野ごとの割合を 図 4.1.3 に示す[4]。

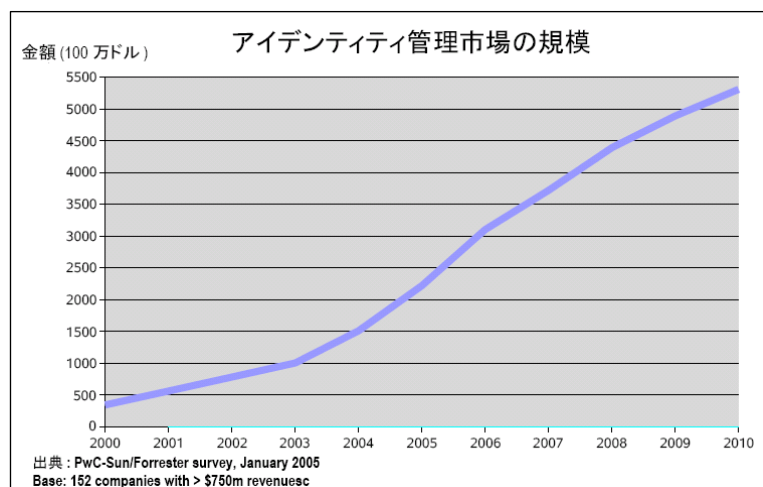


図 4.1.2 世界のアイデンティティ管理市場規模の予測推移

- プロビジョニング 55.2%
- Web上のシングルサインオン 21.0%
- エンタープライズシングルサインオン 14.4%
- フェデレーション 4.4%

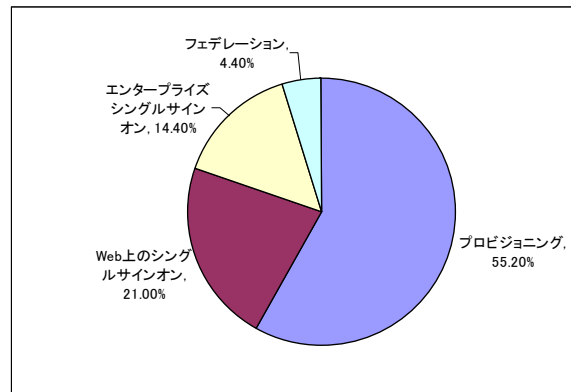


図 4.1.3 技術分野ごとの市場シェア

一方、バイオメトリクス市場であるが、2009年時点では、図 1.1.4 に示すように、日本国内のバイオメトリック市場は、2009年以降市場が拡大する予想されていた。しかしながら、企業にヒアリングしたところでは、現実には、金融分野のバイオメトリック市場が本格的に立ち上がった2004年以前の水準、つまり100億円程度に落ち込んでいる可能性が高く、2009年以降、予想に反し低迷している。

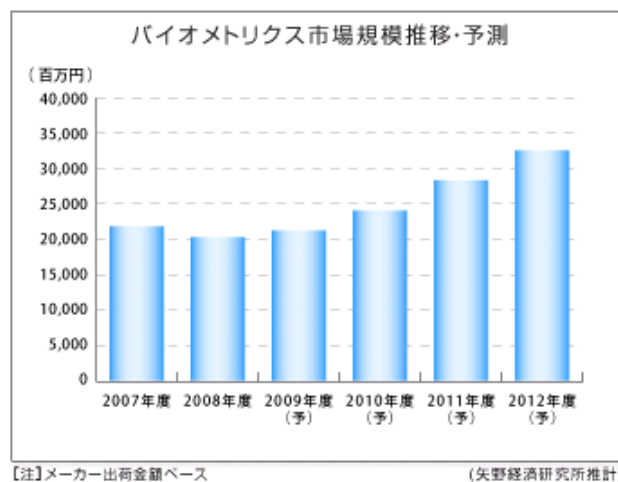


図 4.1.4 日本のバイオメトリック市場

この原因は、金融市場がリプレース市場になったこと、e-passportなどの国内整備が終了した後、輸出に転換できなかったこと、また、政府主導の安全保障や社会インフラの整備が進まなかったことにある。このため、技術や製品の整備が行われず、海外展開が活性化できなかったと考えられる。

日本企業の発展のためには、新たな市場へ展開することが必要になっていると思われ、認証技術の一つであるバイオメトリック認証の高いセキュリティ機能をアイデンティティ管理市場に提供することで、今後、認証・アクセス制御分野で新たな成長が見込めると思われる。そのためには、アイデンティティ管理などの新たな製品体系を整える必要がある [5]。

アイデンティティ管理を定義するにあたり、日本の「政府機関の情報セキュリティ対策のための統一基準（第4版）（平成21年度修正）」[6]、FIPS201-1（Federal Information Processing Standardization）[7]、NSTC レポート[8]などを調査し、次を IdM の定義とした。

アイデンティティ管理とは、「情報システムやネットワークにおいて、利用者のアイデンティティ情報（一例としてユーザ ID、ユーザ権限、ユーザプロファイルなど）の設定をライフサイクル全体に渡り、継続的に追加・変更・削除すること、又はそのための技術の総称」とするのが妥当と考えている。

ここでいうライフサイクルとは、アイデンティティ情報の生成から削除までの各種プロセスのことであり[9][10]、図 4.1.5 と表 4.1.1 にライフサイクルモデルとプロセスの詳細を示す。

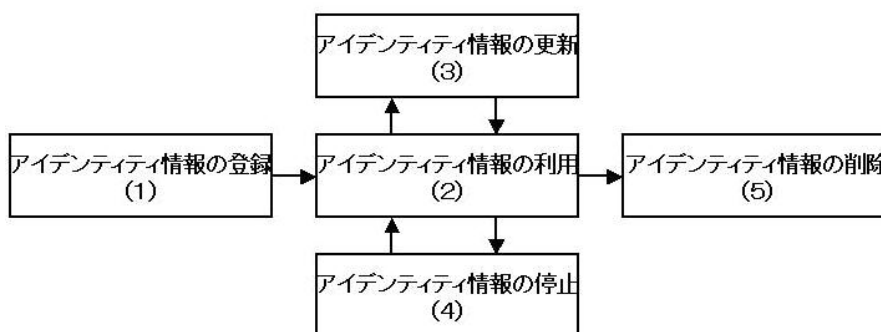


図 4.1.5 ライフサイクルモデル

表 4.1.1 プロセスの詳細

番号	ID 情報のプロセス	定義
1	登録	ID の発行を希望するユーザに対し、ユーザの身元確認、本人確認、サービス提供に関わる審査などを実施した上で、ID を新規に払い出すプロセスを指す。ユーザに対しアカウントを発行するプロセス。
2	利用	ユーザが当該 ID を正常に利用するプロセスを指す。ユーザが ID を提示して ID の認証を受けた上でサービスを利用するプロセス。サービス提供者側が ID の正当性確認や、ID とユーザとの結びつき確認、サービス提供のためのアクセス制御などを実施するプロセス。ID に紐付くサービスの利用をユーザが中止する場合には、削除プロセスへ以降する。
3	更新	ID を保有するユーザに紐付く情報（属性）を更新するプロセス、また ID 自体を新たな ID に引き継ぐプロセスを指す。
4	停止	ユーザ側の状況やサービス提供者側の状況に応じて、払い出している ID を一時的に利用不可状態にするプロセスを指す。利用を再開する場合は ID 利用プロセスへ、そのまま ID を削除する場合は ID 削除プロセスへ移行する。
5	削除	ID そのものを利用不可にし、ID に紐付く情報（属性）も含めて削除するプロセスを指す。

アイデンティティ情報は、表 4.1.2 に示すように、(1) 識別子、(2) クレデンシャル、(3) 属性の 3 種類に分類できる[5]。

表 4.1.2 アイデンティティ情報の詳細

種類	説明	例
識別子	アイデンティティを識別するための情報	<ul style="list-style-type: none"> <li>・アカウント名</li> <li>・メールアドレス</li> <li>・保険証番号、運転免許証番号</li> <li>・社員番号、学生番号</li> <li>・電話番号</li> </ul>
クレデンシャル	ある情報内容の正当性を示すための情報	<ul style="list-style-type: none"> <li>・正当なユーザであることを証明するワンタイムパスワード</li> <li>・国籍を示す電子パスポート</li> </ul>
属性	アイデンティティを特徴付ける情報	<ul style="list-style-type: none"> <li>・氏名</li> <li>・住所</li> <li>・生年月日</li> <li>・所属、役職</li> <li>・信用情報</li> <li>・人間関係 など</li> </ul>

次に、認証の実現方式と特徴を整理した。アイデンティティ管理は、個人の認証であり、認証技術の実現方式をシステム構成の観点から分類すると四つに分類できる[11]。つまり、アクセス元（ユーザ）、認証メカニズム、情報リソースがどこにあるかに着目することで、図 4.1.6 に示すように、ローカル認証、直接認証、間接認証、オフライン認証の 4 パターンに分けることができる。

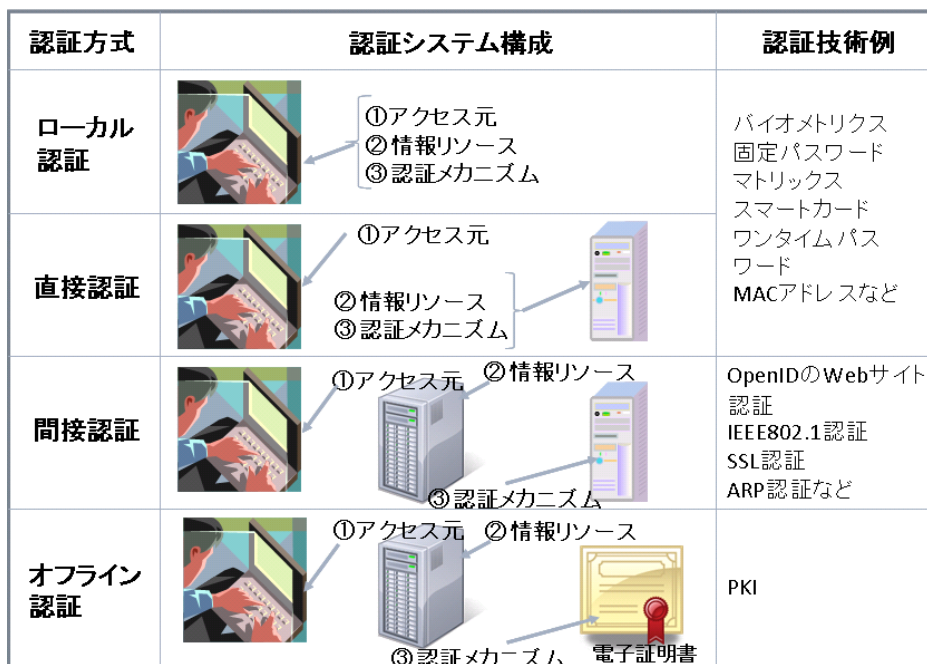


図 4.1.6 認証の実現方式

近年はネットビジネスが拡大し、サービスシステムの増加と個人が管理すべき Identifier が非常に多くなり、管理が適正でないとセキュリティ的な問題が発生する恐れが増大するようになってきている。また、個人の属性が、複数のシステムに分散して登録され、管理の手間の増大が発生した。これをアイデンティティの観点から解決を図るものが、図 4.1.7 に示す SSO (Single Sign On) である。

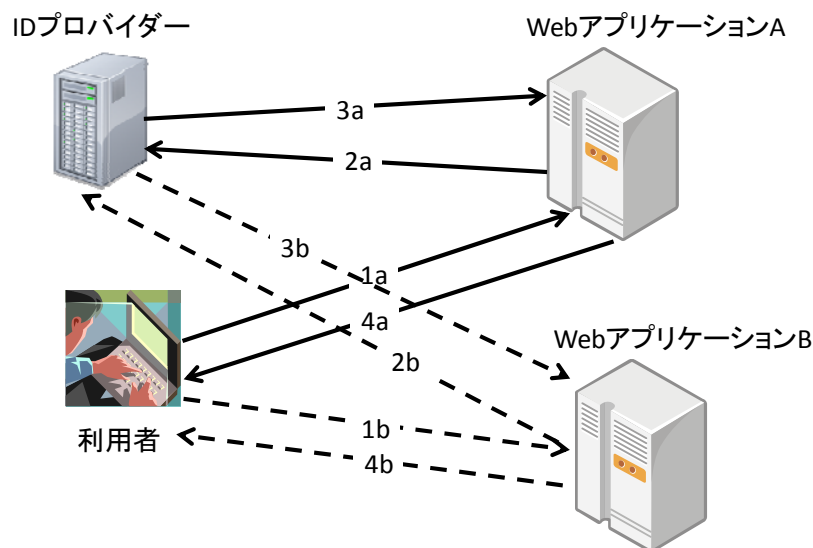


図 4.1.7 SSO の基本的な間接認証アーキテクチャ

これらのことを考慮すると、今後の主流と考える認証つまりアイデンティティ管理の実現技術は、互いに独立した機能から構成される間接認証が重要となると考えられる。

アイデンティティ管理技術を分類すると、組織におけるユーザアクセス管理に用いられ、プロビジョニング機能が中心となり、一種のクローズシステムにおけるアイデンティティ管理応用といえる「IT 内部統制応用」と、間接認証のアーキテクチャであり、SSO をオープンシステム環境で実現するための「Web アプリケーション認証におけるアイデンティティ管理」がある。

Web アプリケーション認証におけるアイデンティティ管理は、異なる組織の IT システムを連携させる場合に、一方のシステムで認証された ID 情報を、安全に他方のシステムと交換・共有することを目的としている ID 連携技術であり、特徴を表 4.1.3 に示す[3][12]。

ID 情報の流通・開示制御の観点から、「プロバイダ（組織）中心モデル」と「ユーザ中心モデル」の 2 種に大別され[3][12][13]、複数の業界団体や標準化団体が、様々なアプローチで管理方式や技術仕様の策定に取り組んでいる。

プロバイダ中心モデルは、組織間の信頼（契約など）に基づき、ID 情報の提供側となる組織（ID プロバイダ；IdP）が ID 情報の流通・開示を制御するモデルであり、複数のアイデンティティを連携して管理する方式である。アイデンティティ連携方式がこれに相当する。代表的な技術仕様は

SAML2.0 (Security Assertion Mark Language2.0) である。

表 4.1.3 アイデンティティ管理方式の特徴

アイデンティティ管理方式	特徴	技術仕様	標準化コンソーシアムなど
連携方式	<p>プロバイダ中心モデル 複数のアイデンティティを連携して管理する。事前に各プロバイダ間の信頼関係を構築して置く必要がある。機能は豊富だが、実装が難しい。IdP が ID 情報の開示・流通を制御するため、エンタープライズ領域との親和性が高いとされている。</p>	SAML2.0	OASIS (Organization for the Advancement of Structured Information Standards) Security Services (SAML) TC
統一方式	<p>ユーザ中心モデル ユーザが一つの識別子で様々なサービスにアクセスする利用形態である。各プロバイダ間の信頼関係はアドホックに構築される。既存技術を多用しているため実装は容易だが、プライバシー保護に課題がある。ユーザ ID はユーザが持つ Web ページの URL であり、その Web ページを提供する ISP (OpenID Provider; OP) がユーザ ID の正当性を保証する。一般向けの web サービスでは主流。</p>	OpenID2.0	<ul style="list-style-type: none"> <li>• OpenID Foundation</li> <li>• OASIS XRI Data Interchange (XDI) TC (基本技術の実装)</li> </ul>
選択方式	<p>ユーザ中心モデル ユーザがアイデンティティを複数持っており、それらをサービスごとに選択して用いる。ID 情報の選択・送信機能がクライアント端末に格納されている。シングルサインオンの機能無し。Microsoft 社の影響が強い。</p>	Information Card	<ul style="list-style-type: none"> <li>• Information Card Foundation</li> <li>• OASIS Identity Metasystem Interoperability (IMI) TC (基本技術の実装)</li> <li>• Microsoft (OS に ID 情報の選択・送信機能を標準搭載)</li> </ul>

ユーザ中心モデルは、ID 情報を持つエンドユーザが、どの組織（サービスプロバイダ）に ID 情報を開示するかを制御するモデルであり、アイデンティティ統一方式、アイデンティティ選択方式がこれに相当する。代表的な技術仕様はそれぞれ OpenID2.0 と Information Card である。

アイデンティティ統一方式とは、あるユーザが、一つの識別子で様々なサービスにアクセスする利用形態を前提にしたアイデンティティ管理方式である。この方式に対応した代表的な技術仕様として OpenID2.0 がある。アイデンティティ選択方式とは、ユーザがアイデンティティを複数持っており、それらをサービスごとに選択して用いるアイデンティティ管理方式である。

広く利用されている SAML2.0 と OpenID2.0 はどちらもインターネット上でのシングルサインオンをサポートし、同じような構成であるが、表 4.1.4 のような相違がある[14]。

表 4.1.4 SAML と OpenID の違い

	SAML	OpenID
開発経緯	エンタープライズ・システムを超えたシングルサインオンの実現のため、標準化した技術として開発	個人が管理する ID 数の削減を目的に開発
対象領域	利用者（ID 所有者）の確認（Authentication）、権限確認（Authorization）双方を対象	利用者（ID 所有者）の確認（Authentication）が対象 アクセス制御などの権限確認（Authorization）は対象外
ID 連携	相互に信頼関係を結んだ Web サイト上でのみ ID 連携を実現	Web サイト同士の信頼関係に関係なく ID 連携を実現

以上のように、アイデンティティ管理は広範な領域を含んでいるが、ユーザアクセス管理とシングルサインオン技術を中心とする Web 上における技術仕様の大きく二つの観点で議論されている。しかしながら、現状の IdM ではバイオメトリクスが考慮されていない。

## 4-2 国内・海外の研究開発動向調査

国際標準化動向として国際標準 SC37 の状況を、また、欧米及び日本国内の研究開発動向として、米国 NSTC(National Science Technology Council)、Biometric Consortium Conference 及び、EU 及び日本国内の学会・企業の開発状況を調査し、動向をまとめた。

国際標準においてアイデンティティ管理そのものの標準化はまだ策定の途中であるが、アイデンティティ管理自体が広範な領域を含んでいるために関連する国際標準は、表 4.2.1 のように多岐にわたっている[1]-[5]。

ISO/IEC JTC1/SC27 と SC37 で、アイデンティティ管理関係する標準が 4 件開発中であり、バイオメトリクスと IdM に関し二つの規格 (BIAS と ACBio) が重要と思われる。

ACBio は日本発の国際規格である。ISO/IEC 24761 Authentication Context for Biometrics として 2009 年 5 月に国際規格として発行され[5]、オープンネットワーク環境におけるバイオメトリクスによるユーザ認証 (以下、生体認証) をセキュリティ的に補完することが ACBio の目的である。

ACBio のデータ構造を図 4.2.1 に示す。

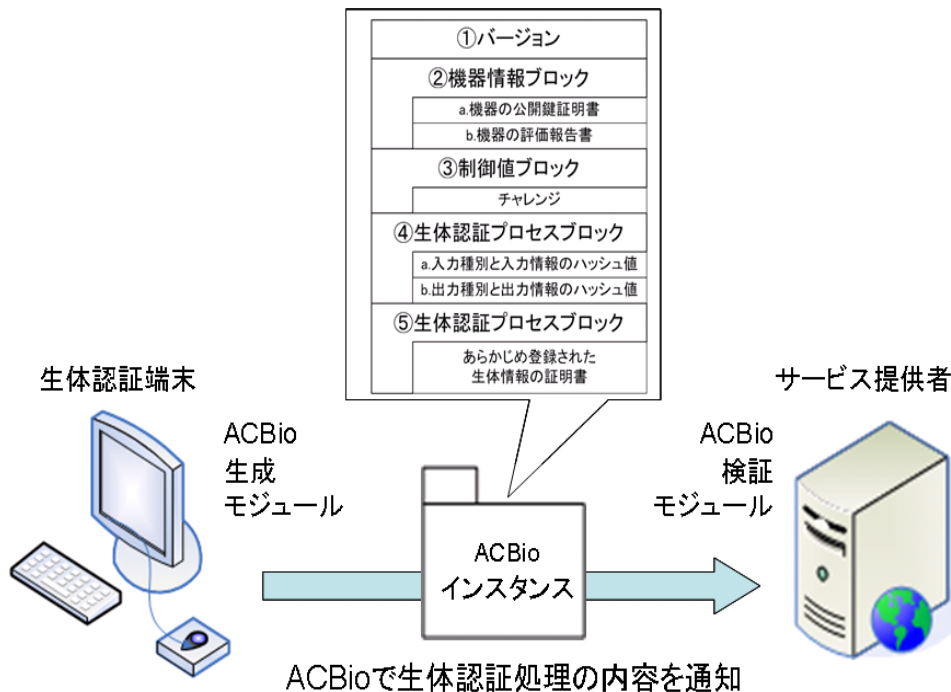


図 4.2.1 ACBio のデータ構造

表 4.2.1 国際標準化活動におけるアイデンティティ管理

(2010年10月時点)

タイトル	国際標準化委員会	内容
WD 29144 The use of biometric technology in commercial identity management applications and processes	SC37 WG6	アイデンティティ管理にバイオメトリクスを利活用する上での考慮点を纏めるもの、英国からの新規提案であり、Base Document を開発中である。
NWIP BIAS Biometric Identity Assurance Services (BIAS)	SC37 WG2	Identity assurance に使用されるサービスベースのフレームワークから呼び出されるバイオメトリックサービスを定義する米国規格 ANSI/INCTIS442-2010 と、標準化団体 OASIS による XML ベースの Web サービスや SOA から利用するための実装である。
WD 29115 Security techniques -- Entity authentication assurance	SC27 WG5	認証において、認証対象が真にそのエンティティであるという信頼性に関する標準である。
WD 24760 Information technology – Security techniques – A framework for identity management	SC27 WG5	アイデンティティ管理のフレームワークと、ある文脈内での実体の識別情報の管理を定義、規定している。情報セキュリティの文脈内で提案されたフレームワークの利用に集中している。
ISO/IEC24761 Authentication Context for Biometrics (ACBio)	SC27 WG5	オープンネットワーク環境におけるバイオメトリクスによるユーザ認証をセキュリティ的に補完する。生体認証が正しく実行されたことをオンラインで判断できる付加情報を提供することによって、生体認証結果の真正性を保証する。規格は付加情報のデータ構造定義である。

BIAS (Biometric Identity Assurance Services、ANSI/INCTIS442-2008) は、米国より 2010 年に ISO/IEC JTC/SC37WG2 に提案され開発が認められた規格 (Biometric Identity Assurance Services (BIAS) : N3946) である[6]。

このなかで、Web サービスを想定したバイオメトリック認証のための規格案であり、サーバ/クライアントモデルのようなネットワーク環境下においてバイオメトリクス利用の個人特定 (Identity) 機能を提供するサーバ側 (サービス) のアーキテクチャを定めている。

また、複数種のバイオメトリクスによる個人特定の統合や、バイオメトリクス以外の情報による個人特定との組み合わせによる個人特定を実行することも組み込まれている。

図 4.2.2 に示すように、SOA (サービスオリエンティドアーキテクチャ) 指向で、OpenID や SAML などの既存の IdM 認証系に容易に接続可能な使用である。したがって、今後、バイオメトリック技術を IdM 市場へ展開するために重要な標準となる可能性がある。

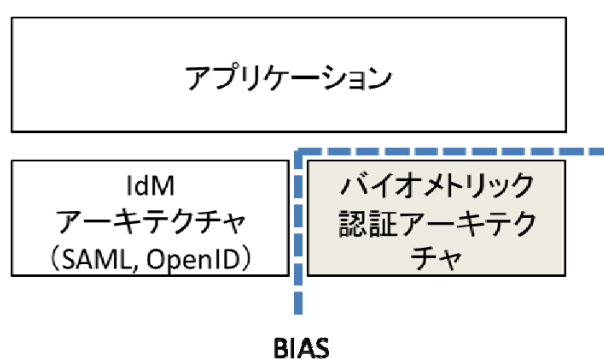


図 4.2.2 BIAS の概要

調査研究活動に関しては、欧州(EU)においては、欧州委員会主導で複数のアイデンティティ管理を対象とする調査研究プロジェクトが、表 4.2.2 に示すように設立されている。学際的アプローチでありアイデンティティ管理を含む、幅広い隣接領域を調査研究の対象としている。

表 4.2.2 欧州におけるアイデンティティ管理関連プロジェクト

番号	プロジェクト名称	内 容
(1)	Primelife [7]	プロジェクト実施期間：2008年3月～2011年2月の3年間。 PRIMEプロジェクトの成果を引き継ぎ、インターネットアプリケーションにおけるプライバシー保護と、プライバシー保護のライフサイクルについて研究する。
(2)	PICOS [8] (Privacy and Identity Management for Community Services)	プロジェクト実施期間：2008年2月～2011年1月の3年間。 プライバシーを保護する信頼性の高い ID 管理ツールを作成するためのプラットフォームを開発する。
(3)	SWIFT [9] (Secure Widespread Identities for Federated Telecommunications)	プロジェクト実施期間：2008年1月～2010年6月の2年6ヶ月間。 ネットワーク上のレイヤを横断するアイデンティティ・フレームワークの構築とユビキタス環境でのユーザセントリックなシングルサインオンの研究。
(4)	FIDIS [10] (Future of Identity in the Information Society)	プロジェクト実施期間：2004年4月～2009年6月の5年3ヶ月間。 アイデンティティ管理システム、アイデンティティに関する法規及びアイデンティティの使用に関する情報の収集。
(5)	PRIME [11] (Privacy and Identity Management for Europe)	プロジェクト実施期間：2004年3月～2008年2月の4年間。 プライバシーを強化したアイデンティティ管理システムのプロトタイプを開発する。
(6)	GUIDE [12] (Government User IDentity for Europe)	プロジェクト実施期間：継続中（実施期間不明）。 欧州向けの安全で相互運用可能な電子政府電子身元サービス及び取引のアーキテクチャを作成するための研究と技術開発。
(7)	TURBINE [13][14]	プロジェクト実施期間：2008年2月～2011年1月の3年間。 電子 ID 管理アプリケーションを実ビジネスレベルで使用するバイオメトリック技術の開発を行う。

この他、欧州では EU 全域において eID の認証を可能とすることを目的とするパイロットプロジェクト STORK (Secure idenTity acrOss boRders linKed) が 2008 年から 3 年間の予定で実施されている。STORK プロジェクトでは、各国の eID システムを連携させるための共通仕様の作成、試験及び確認が実施される。

米国では、2008 年 1 月に NSTC (National Science and Technology Council) が、アイデンティティ管理について、ビジョンを構築するために、国土安全保障省 DHS (Department of Homeland

Security)、国防総省 DOD (Department of Defense)、調達庁 GSA (General Services Administration)、司法省 DOJ (Department of Justice) 及び国立科学財団 NSF (National Science Foundation) など複数の機関の人員で構成されている調査特別委員会を 6 ヶ月の期限で設置した[15][16]。

委員会は、国土安全保障省 DHS (Department of Homeland Security)、国防総省 DOD (Department of Defense)、調達庁 GSA (General Services Administration)、司法省 DOJ (Department of Justice)、国立科学財団 NSF (National Science Foundation) など複数の機関の人員で構成されており Drafting team、Data Collection and Analysis、Digital Identity、Grid、Privacy and Legal の 五つのワーキンググループが設置されている。

さらに、2010 年 6 月にオバマ政権は「サイバー空間での信頼できる ID 導入の国家戦略」(NSTIC: National Strategy for Trusted Identities in Cyberspace) として、「Identity Ecosystem」の導入を促すとする発表を行った[17] [18] [19]。発表内容から類推すると、OpenID のようなシングルサインオン可能なシステムを念頭において戦略が策定されていると考えられる。BIAS とともにアイデンティティエコシステムはバイオメトリクスの利用面を拡大するための重要な事案であり、今後も継続して調査すべき対象と考えている。

このように、米国と欧州でアイデンティティ管理システムの開発をめぐり、競争が激化する可能性は大きい。

また、米国、欧州では、民間企業が主体となってカンファレンス活動が行われている。

表 4.2.3 カンファレンス一覧

番号	カンファレンス名称	開催年	開催地
(1)	European Identity Conference [20]	2007 年より毎年	ドイツ ミュンヘン
(2)	IDM [21]	開始年未確認 2010 年が第 4 回	英国 ロンドン
(3)	Identity management 2010 [22]	2010 年 開始年未確認 毎年開催の様様	米国 Washington DC
(4)	Gartner Identity & Access Management Summit [23] [24] [25]	2010 年 2006 年まで確認 毎年開催の様様	米国 サンディエゴ
(5)	Identity Management for National Defense [26]	2009 年 単発の様様	米国 ワシントン DC
(6)	Biometric Consortium Conference 2010 [27]	2010 年 毎年開催	米国 フロリダ・タンパ
(7)	Biometrics 2010 [28]	2010 年 毎年開催	英国 ロンドン

最も規模が大きいと考えられるのは参加スピーカーが 100 名を超え、4 日間に渡って開催される kuppinger cole 社主催の European Identity Conference である。

主なカンファレンスとして、表 4.2.3 に示すように、(1) European Identity Conference 2010、(2) IDM2010、(3) Identity management 2010、(4) Gartner Identity & Access Management Summit、(5) Identity Management for National Defense、(6) Biometric Consortium Conference 20XX、(7) Biometrics 20XX などがあり、欧米では、定期的にアイデンティティ管理に関するカンファレンスが開催されている。

一方、日本のプロジェクトは、開発ベースにはなく、調査ベースであり、以下のものがある。

(1) 日本ネットワークセキュリティ協会(JNSA)

政策部会アイデンティティ管理ワーキンググループ

「内部統制におけるアイデンティティ管理解説書」を開発した[29]。同解説書は 2008 年 6 月に第 1 版、2009 年 6 月に第 2 版が発行されているが、現在、公開されていない。内部統制、特に IT 全般統制とアイデンティティ管理について取り上げている。また健全なシステムの導入と期待効果の創出を意図して、「アイデンティティ管理システム」の導入における標準的な上流工程作業についてのガイドラインを収めている。

(2) 独立行政法人 情報処理推進機構セキュリティセンタ(IPA)

情報セキュリティ技術動向調査 TG (タスクグループ)

情報セキュリティ技術動向調査報告書(2008 年上期)をまとめている。11 章構成のうち 9 章で、OpenID や SAML などの技術動向に関してまとめている[30]。

(3) 財団法人日本規格協会(JSA) アイデンティティ管理技術の標準化調査研究委員会

Web 資源有効活用を推進する情報基盤の標準化調査研究補助事業として JSA がアイデンティティ管理技術の標準化調査研究委員会を設置し、「アイデンティティ管理技術の標準化調査研究成果報告書」を作成している[31]。

日本国内のアイデンティティ管理に関する学会研究会活動を表 4.2.4 に示す。このように、

(1) カンターラ・イニシアティブ・技術セミナー2010 [32]

(2) OpenID Tech Night Vol.6 [33] [34]

(3) 平成 22 年度情報処理技術セミナー Shibboleth 環境の構築 [35] [36]

(4) CSS (コンピュータセキュリティシンポジウム) 2010 [37]

(5) SCIS (暗号と情報セキュリティシンポジウム) 2011 [38]

(6) 共通番号制度と国民 ID 時代に向けたプライバシー・個人情報保護法制のあり方 [17] [39][40]

などがある。

他にも企業や研究機関などにより多くの研究会、セミナーが行われている。

表 4.2.4 日本国内の学会、研究会、講演活動一覧

番号	名称	開催日	主催者・開催頻度
(1)	カンターラ・イニシアティブ・技術セミナー2010	2010年12月14日	カンターラ・イニシアティブ ジャパン・ワークグループ 2009年に2回、2010年に3 回のセミナー、講演会を開催 している。
(2)	OpenID Tech Night Vol.6	2010年5月28日	OpenID ファウンデーション・ ジャパン 年1回開催
(3)	平成22年度情報処理技術セミナー Shibboleth 環境の構築	2010年7月8日～7 月9日(第1回) 2010年11月15日～ 11月16日 (第2回) 2011年1月11日～1 月12日(第3回)	国立情報学研究所 平成22年度事業
(4)	CSS2010(コンピュータセキュ リティシンポジウム)	2010年10月19日～ 10月21日	情報処理学会コンピュータ セキュリティ研究会 毎年開催
(5)	共通番号制度と国民ID時代 に向けたプライバシー・個人 情報保護法制のあり方 <課題と提言> 第3回 シンポジウム	2010年12月19日	堀部政男情報法研究会 不定期開催 2011年3月26日に第4回を 開催予定

日本の企業、大学における開発事項として、株式会社日立製作所のソリューションでは、キャンセラブルバイオメトリック技術を利用したソリューションを開発し公開している[48]。これは、同社がクラウド環境下で生体認証サーバの運用・管理を行い、ユーザは Web 経由で認証サービスをうけるソリューションである[41]。

また、静岡大学のソリューション BIDM は、既設の LDAP システムを中心とした IT 統合認証システムに、指静脈データ登録と入退室管理を統合したものとして、プライベートクラウド内に LDAP システムを置き、プライベートとパブリックを問わず、全てのクラウド認証は LDAP サーバを通過させて管理するシステムを開発している[42][43]。

アイデンティティ管理システムに関するカンファレンスなどの件数、開催規模を考えると、日本、米国、欧州では電子政府システムの導入に向け、安全で使い易く、標準的な技術を利用したアイデンティティ管理システムの開発に必死になっている状況であると考えられる。また、電子政府システムの導入が現実化しつつある今、技術的な課題だけでなく、アイデンティティ管理についての法的、社会的な課題も併せて検討する時期になっている。

### 4-3 バイOMETリック技術を実装したIdMアーキテクチャの基本方式の検討

最初に検討の基本方針をまとめた。それを図 4.3.1 に示す。

基本方式を検討するにあたって、検討のための方針として、バイオMETリック技術を実装した IdM アーキテクチャが以下の三つの機能を持つこととした。

#### (1) 高い汎用性

本プロジェクトで検討するアーキテクチャは、様々な IdM システムにおいて特定の方式に依存したものであってはならない。どの IdM システムにも適用することが可能であり、かつ、どの IdM システムにおいても同等の性能を発揮することとした。

#### (2) バイOMETリックの特性の考慮

バイオMETリックは本人認証技術の一つとして、これ以外の本人認証技術であるパスワードや IC カードなどと比べていくつかの特性を有している。そのため、本プロジェクトで検討するアーキテクチャは、次に示すバイオMETリックの多岐に渡る特性を考慮したものでなければならない。

- ①技術の多様性
- ②認証精度
- ③プライバシー

#### (3) Web 技術との親和性

近年、インターネットの普及はめざましく、新しく開発・運用されるネットワーク型システムのほとんどがインターネットへの接続を前提とするようになってきているため、Web 技術と高い親和性を有することが必要となる。

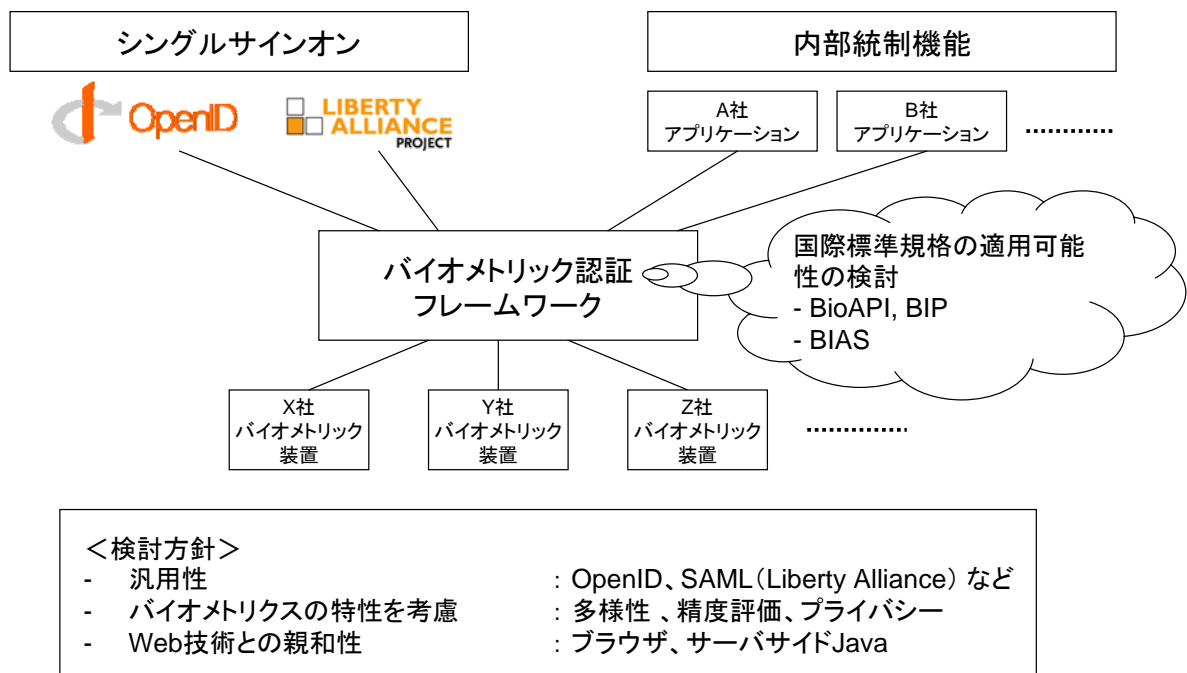


図 4.3.1 検討方針

次に、世の中に存在する IdM システムのアーキテクチャを以下の 2 種類に大別して調査した。

### (1) Web アプリ応用型

インターネット（あるいはイントラネット）の複数の Web サーバに対して、シングルサインオンを行うことを主な目的とした IdM システムである。

主要な規格として以下の二つが存在している。

- ・ OpenID : OpenID ファウンデーションにより策定された規格。
- ・ SAML : OASIS と Liberty Alliance により策定された規格。

### (2) 内部統制応用型

主に企業の組織内でコンピュータリソースにアクセスするためのアカウント情報のライフサイクル管理に用いられるものである。

OpenID は、Web ベースのシングルサインオンのためのインタフェース規格であり、次の技術的特徴を持つ。

- ①特定の中央集権的なサーバを置かない（誰でも OpenID プロバイダになれる）。
- ②Web 技術との親和性が高くブラウザ側に手を加えずに実現できる。
- ③個人を識別する ID 情報として URL を用いる。

OpenID には中核的な規格である”OpenID Authentication 2.0”に加えて拡張規格と呼ばれる周辺規格がいくつか存在している。

OpenID におけるシングルサインオンの概略処理シーケンスを図 4.3.2 に示す。

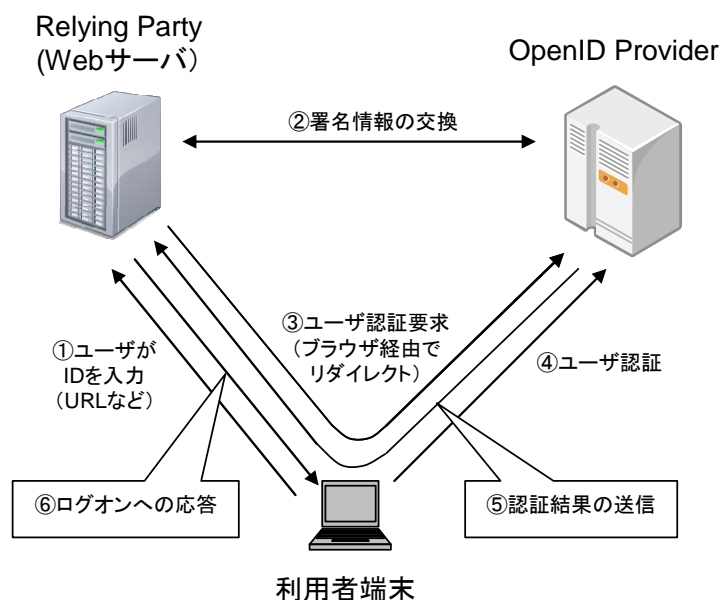


図 4.3.2 OpenID の概略処理シーケンス

OpenID へのバイオメトリクスを組み込みの検討にあたっては、OpenID 関連規格においてバイオメトリック認証がどこまで考慮されているか調査した。結果的に OpenID では認証方式を具体的には規定しておらず、結果的にバイオメトリクスに関する直接的な言及は存在していないことが判明

した。

OpenID における認証シーケンスの詳細を図 4.3.3 に示す。ここで、番号 1 と 7 を除いた部分は OpenID で規格化されているが、番号 1 と 7 の部分は規格外となっている。7 は認証方法に依存する部分であるが、この部分が規格外であるためバイオメトリック認証も規格の対象となっていない。

このことは、OpenID 規格そのものには手を加えることなくバイオメトリック認証を組み込める可能性を示唆するものである。

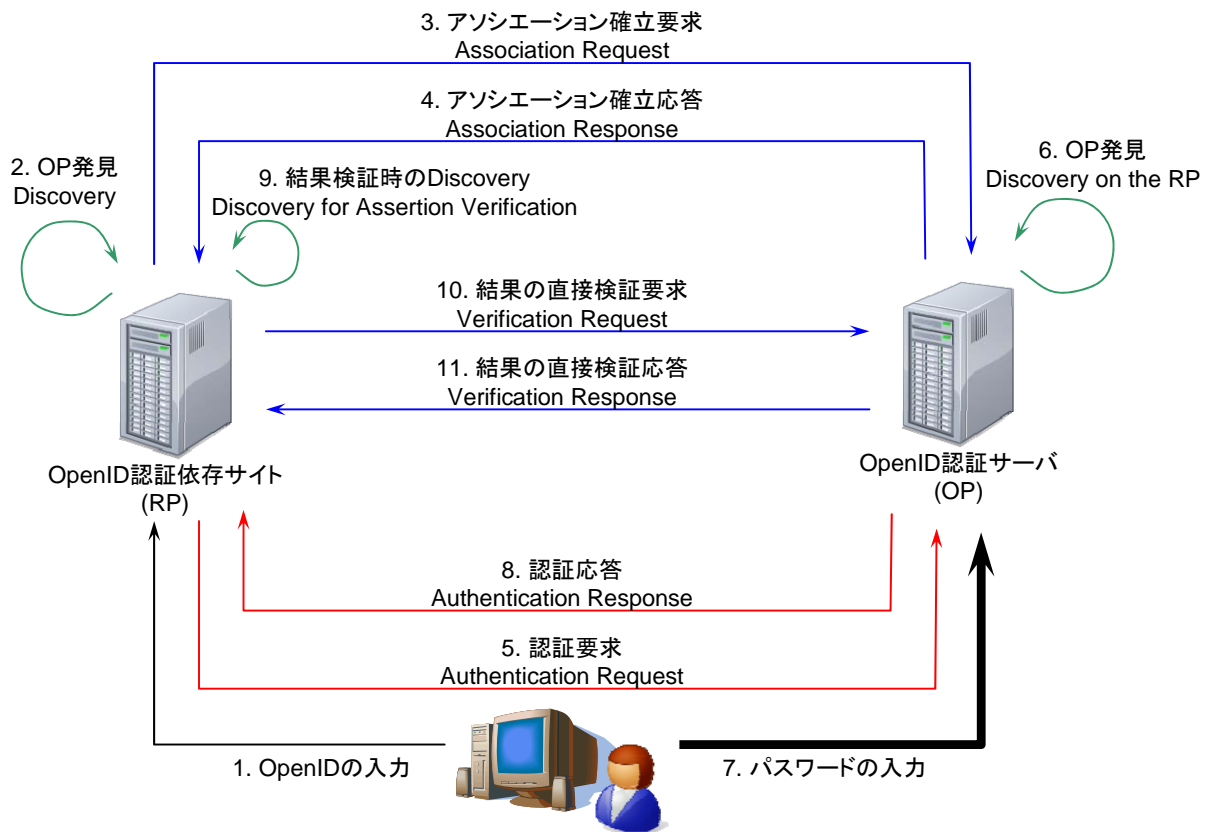


図 4.3.3 OpenID の詳細処理シーケンス

SAML (Liberty Alliance)の技術的特徴は、以下のとおりである。

- ① SAML を利用 (Security Assertion Markup Language : OASIS が策定)。
- ② サイト間で事前の信頼関係を構築するトラストサークル。
- ③ SAML のサービスは三つのオーソリティによって構成される。  
(認証オーソリティ、属性オーソリティ、認可決定オーソリティ)。
- ④ Web サーバが SAML リクエストを発行し、オーソリティは SAML レスポンスを返す。

また、OpenID と同様に中核的な規格である” Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML)”に加えて様々な周辺規格が存在している。

図 4.3.4 に SAML の概略処理シーケンスを示す。

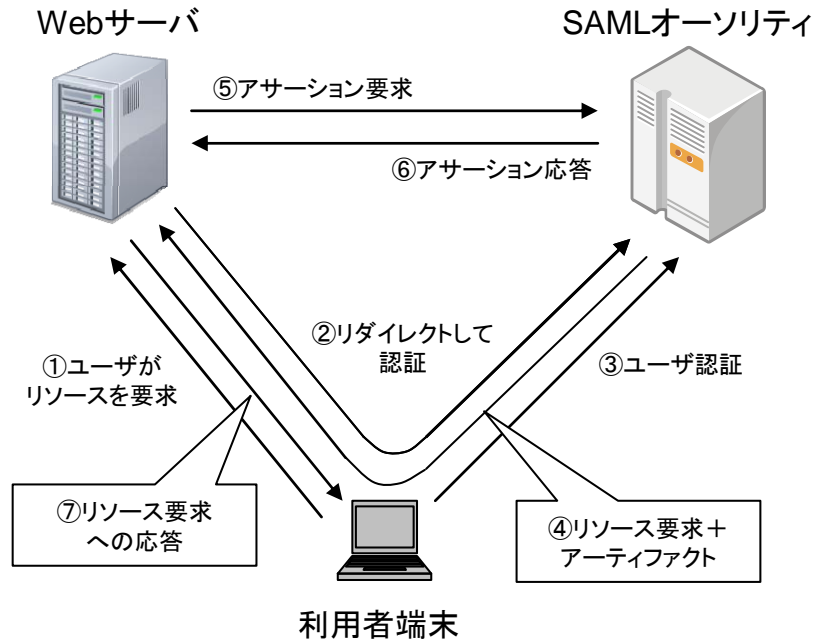


図 4.3.4 SAML の概略処理シーケンス

図 4.3.5 に SAML の詳細処理シーケンスを示す。

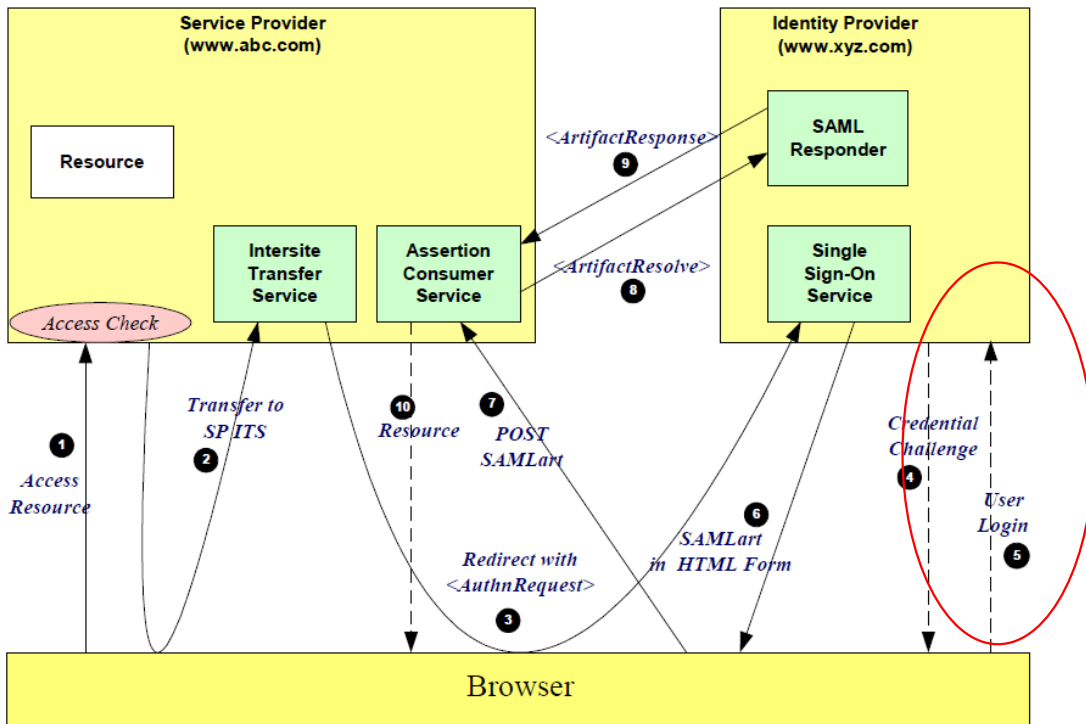


図 4.3.5 SAML の詳細処理シーケンス

SAML (Liberty Alliance)へのバイOMETRICSの組み込みの検討にあたって、規格書の内容を調査したが SAML 規格においてバイOMETRICSについて具体的に言及している場所は見当たらなかった。

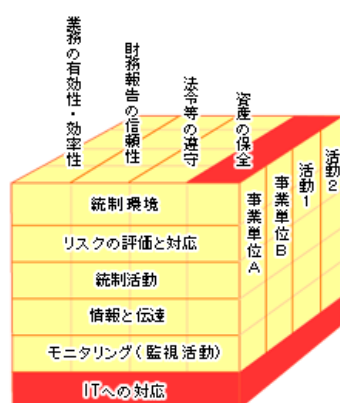
内部統制応用型の IdM システムは、目手として、業務の有効性と効率性、統制環境の構築、SOX 法（日本版 SOX 法）への対応という特徴を有するものである。表 4.3.3 に特徴を示す。

内部統制を共通的に表すフレームワークの機能ブロックを図 4.3.6 に示す。

内部統制応用型にバイオメトリクスを組み込む場合、共通規格が存在しない現時点においては個々の IdM システムにおいて個別にバイオメトリクス機能を組み込む対応が必要となる。各システム・各ベンダの共通解を得ることが困難であり、本調査研究においては検討の対象外とした。

表 4.3.1 内部統制 IdM システムの特徴

No	項目	説明
1	目的	<ul style="list-style-type: none"> <li>• 業務の有効性と効率性</li> <li>• 財務報告の信頼性</li> <li>• 関連法規の遵守</li> <li>• 資産の保全</li> </ul>
2	構成要素	<ul style="list-style-type: none"> <li>• 統制環境</li> <li>• リスクの評価と対応</li> <li>• 統制活動</li> <li>• 情報と伝達</li> <li>• モニタリング</li> <li>• IT への対応</li> </ul>
3	関連する法律・法令	<ul style="list-style-type: none"> <li>• SOX 法（日本版 SOX 法）</li> <li>• 会社法</li> <li>• 金融取引法</li> </ul>



＜日本版 COSO フレームワーク＞  
 企業の内部統制（財務会計の不正を防ぐしくみ）のためのフレームワークの一つ。  
 COSO とは、作成した米国トレッドウェイ委員会組織委員会（Committee of Sponsoring Organizations of Treadway Commission）の略称。日本では、金融庁が 2005 年に公表した「財務報告に係る内部統制の評価及び監査の基準（公開草案）」が日本版 COSO フレームワークともいわれている。

図 4.3.6 内部統制機能ブロック

以上、OpenID、Liberty Alliance の技術的詳細を調査した結果、両者の認証部分にバイオメトリック認証を多要素認証の一つとして追加することで他への体系的な影響を最小限として組み込みが可能との見込みを得た。

並行して国際規格についての技術調査したところ、関連する規格として次のものがあることが分かった。

- ① BioAPI 規格 : ISO/IEC 19784-1:2006
- ② BIP 規格 (BioAPI Interworking Protocol) : ISO/IEC 24708:2008
- ③ BIAS 規格 (Biometric Identity Assurance Services) :  
ISO/IEC 30108 (2010 年米国から NP 提案)

BioAPI 規格は、バイオメトリクスのための共通インタフェース規格であり、図 4.3.7 に示すように、アプリケーション、BioAPI フレームワーク、BSP (Biometric Service Provider) の 3 階層で構成される。

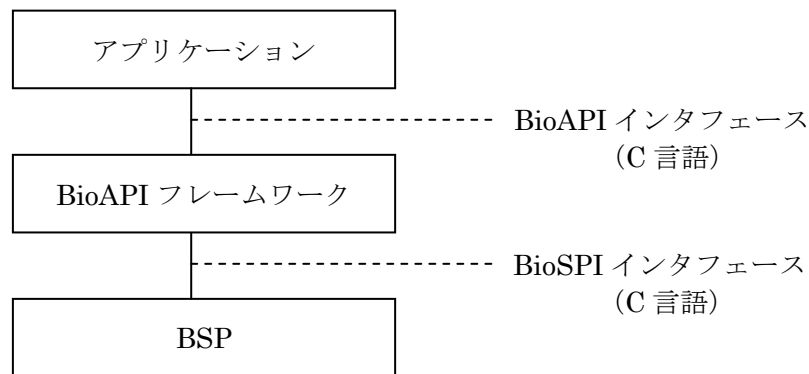


図 4.3.7 BioAPI のソフトウェア構成

BioAPI フレームワークはバイオメトリック用共通関数が定義された API の本体部分である。また、BSP は個々のバイオメトリック技術の依存部分である。これらは、通常バイオメトリック装置やアルゴリズムのベンダが開発し、提供する。

BioAPI フレームワークがアプリケーションに提供しているインタフェースは BioAPI インタフェースと呼ばれる。また、BioAPI フレームワークが BSP を呼び出すインタフェースは BioSPI インタフェースと呼ばれる。これら二つのインタフェースにより、BioAPI では BSP を変更することなくアプリケーションを入れ替えたり、アプリケーションを変更することなく BSP を入れ替えたりすることを可能としている。

BioAPI 仕様はバイオメトリック情報の登録、1:1 照合、1:N 照合などの代表的な機能に加えて、初期化・終了処理、装置制御、データベース制御など様々な機能を定義した関数群である。

BIP 規格は、図 4.3.8 に示すように、BioAPI 規格で定義される関数及びパラメータを、ネットワーク上を流れるメッセージとして規格化したものである。

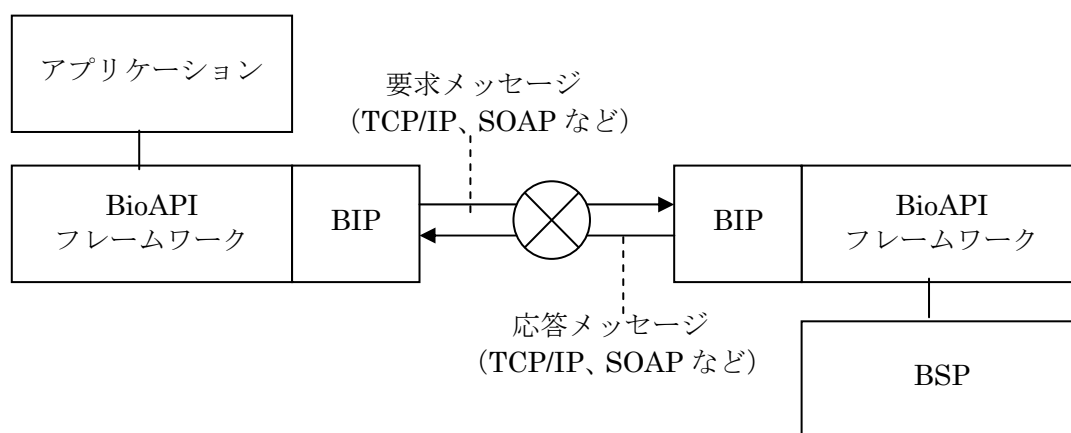


図 4.3.8 BIP のシステム構成

BioAPI のインタフェースをそのまま 1 対 1 に通信メッセージに置き換えることで、アプリケーションや BSP はともに手を加えずにネットワークシステムに拡張することが可能となる。

機能として、BioAPI がサポートする関数と同様の機能を有しているため、BioAPI で定義されている関数と同様の機能が通信メッセージ仕様として定義されている。

特定のプロトコルに依存していない一般的な規定となっているが、BIP の実装プロトコル (binding と呼ぶ) として TCP/IP を用いた仕様 (TCP/IP binding) と SOAP を用いた仕様 (SOAP binding) の二つについて具体的な定義が記述されている。

BIAS 規格は、ISO/IEC JTC1/SC37 に 2010 年に米国から新規提案され、承認されたプロジェクトである（プロジェクト番号は ISO/IEC 30108）。BIAS は Web サービスを想定したバイオメトリック認証のための規格案である。

BIAS の主な特徴は、以下のとおりである。

- ①近年注目されている SOA (Service Oriented Architecture) に基づくインタフェースを採用する。
- ②特定のバイオメトリック技術、装置、ベンダに依存しない。
- ③既存の規格を活用する (CBEFF など)。
- ④特定の転送方式に依存しない。
- ⑤オープンなマルチプラットフォームであること。
- ⑥遠隔呼び出しを主な利用ケースとする。

BIAS はクライアントからの依頼を受け付けて動作するサービスプロバイダの内部で動作するサービスである。BIAS の内部には BioAPI アダプタやベンダアダプタなどといった個々のバイオメトリック技術が実装された階層を持つ。

BIAS システムの構成図を図 4.3.9 に示す。

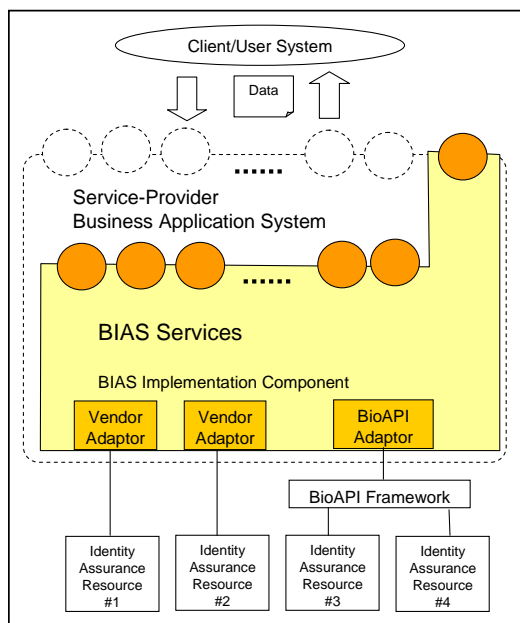


図 4.3.9 BIAS のシステム構成

BIAS は Web サービスなど SOA に基づくバイオメトリック用の各種サービスを定義した規格であり、本調査研究で取り扱う IdM システムへの高い接続性を持つことが予想されたため、詳細な調査を実施した。BIAS の主な特徴は、以下のとおりである。

(1) 2種類のサービスが存在する。

BIAS は内部に、Primitive サービスと Aggregate サービスの 2 種類のサービスを持つことが可能な構造を持っている。

(2) XML ベースの規格である。

(3) サーバ認証のみを考慮している。

(4) バイオグラフィック情報管理機能を持つ。

BIAS の規格書から作成した BIAS の内部構成についての予想図を図 4.3.10 に示す。

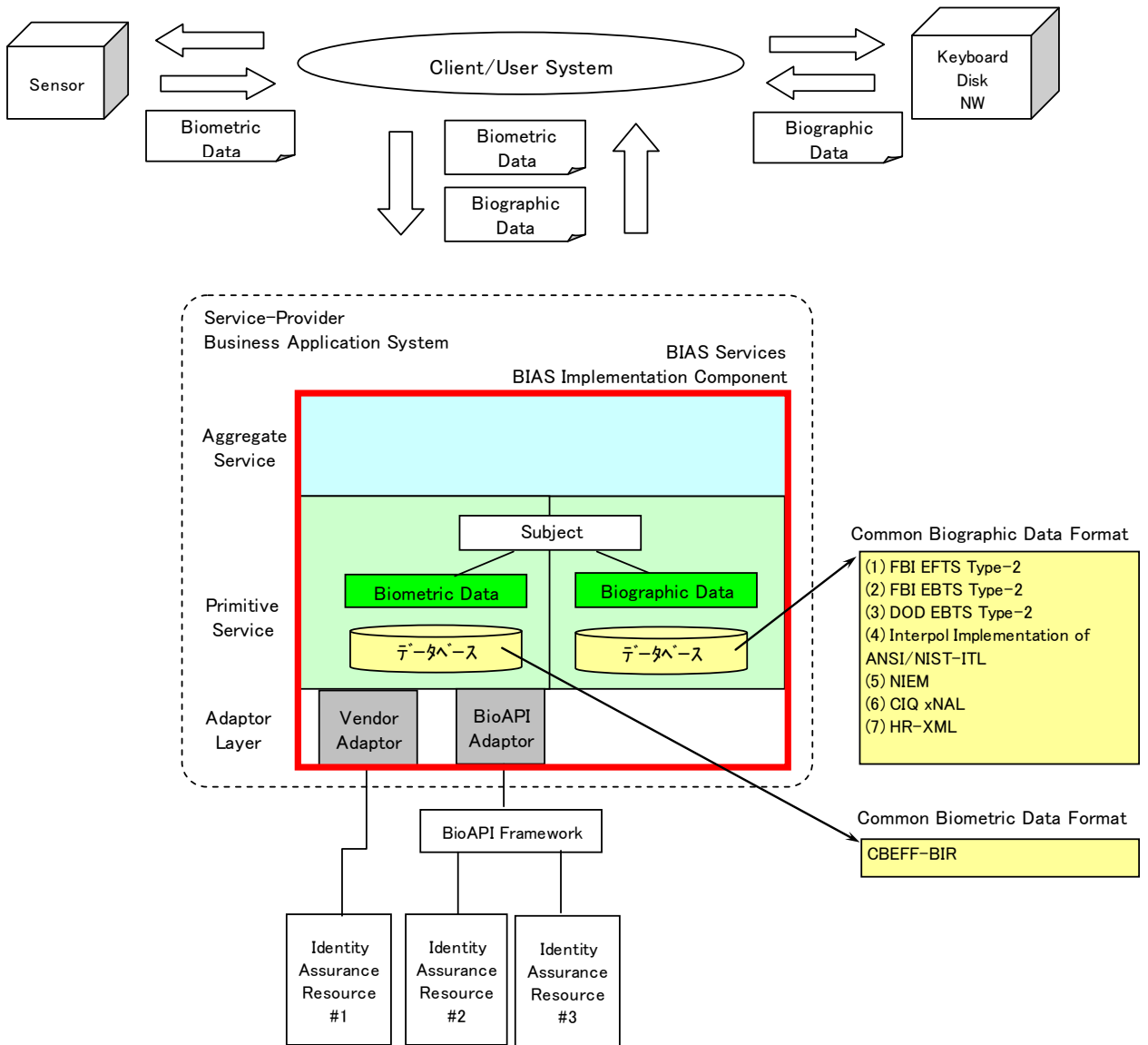


図 4.3.10 BIAS のシステム構成

本図に示すとおり、BIAS は上下に Aggregate サービスと Primitive サービスを配置し、左右に Biometric 用サービスと Biographic 用サービスを配置した構造を持つことが可能である。また、

BIASはXMLに基づいており、同じくXMLに基づくIdM仕様であるSAMLと親和性が高いと考えられるため、SAMLの認証のためのRequest/ResponseにBIASを加えられるかを検討した。

サービスプロバイダがアイデンティティプロバイダに認証要求をSAMLで発行する場合、<AuthnRequest>というXML要素を使用する。この要求に対してアイデンティティプロバイダが認証応答する場合は、認証結果としてSAMLアサーション及び認証ステートメントを返却するが、この認証ステートメントの中に、図4.3.11に示すように、認証結果の詳細情報としてBIASの認証結果が格納される。

このように認証応答の中にBIASの実行結果をそのまま埋め込むことができ、上位アプリケーション（この場合はサービスプロバイダ）もXMLをそのまま受け取り解釈することができる。このことから、BIASはSAMLと親和性の高い方式ということが確認できる。

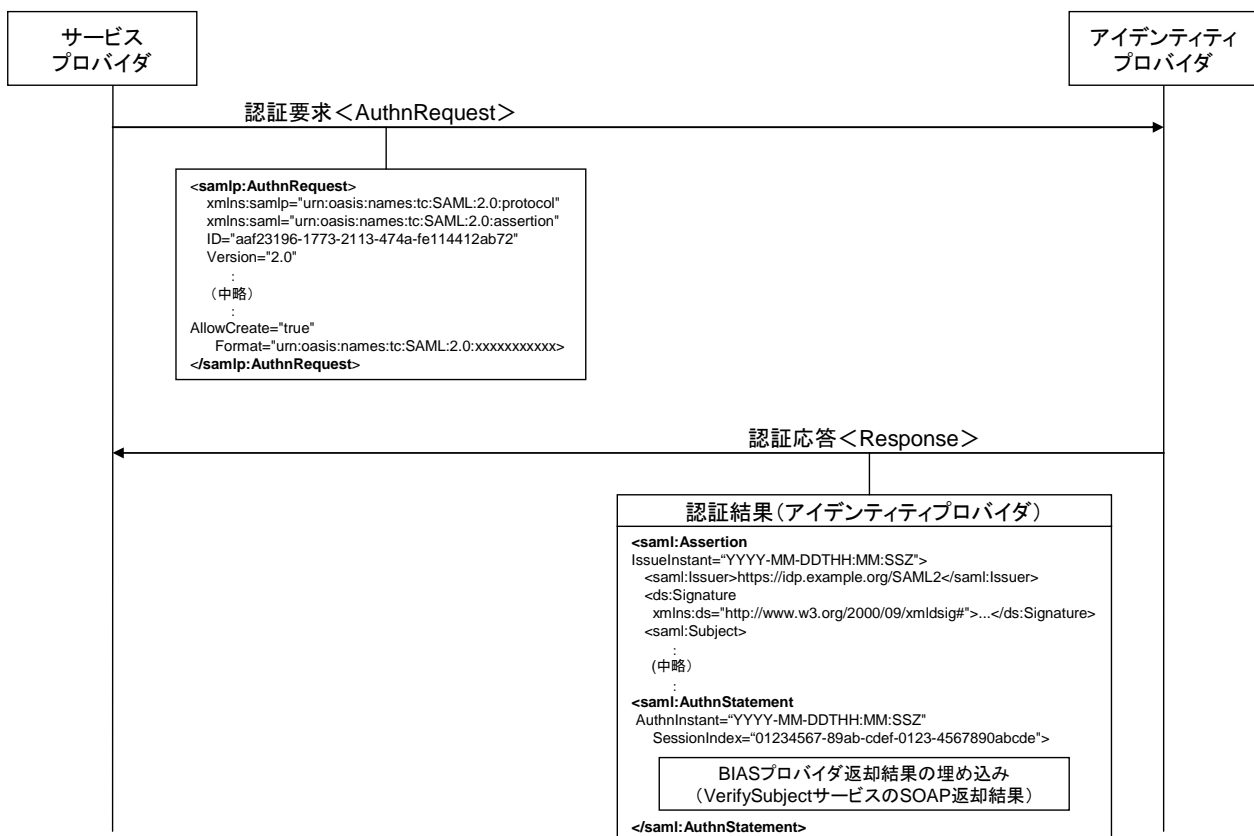


図 4.3.11 SAML メッセージへの BIAS メッセージの組み込み

次に、前述した三つの国際標準規格を用いて IdM システムにバイOMETリック認証を組み込む方式について検討した結果を示す。

説明にあたってはパスワード認証のシーケンスを示した上で、これにバイOMETリック認証を追加するための方式を示すこととする。

BIAS の IdM システムへの組み込みを確認するにあたり、SAML におけるパスワードを用いた認証手順を示す。

図 4.3.12 にパスワード認証手順、図 4.3.13 にパスワード認証時の詳細処理フローを示す。

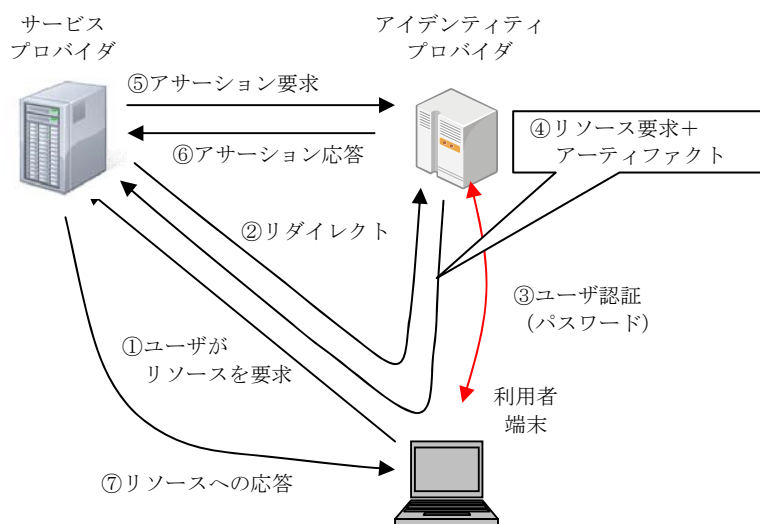


図 4.3.12 SAML でのパスワード認証手順

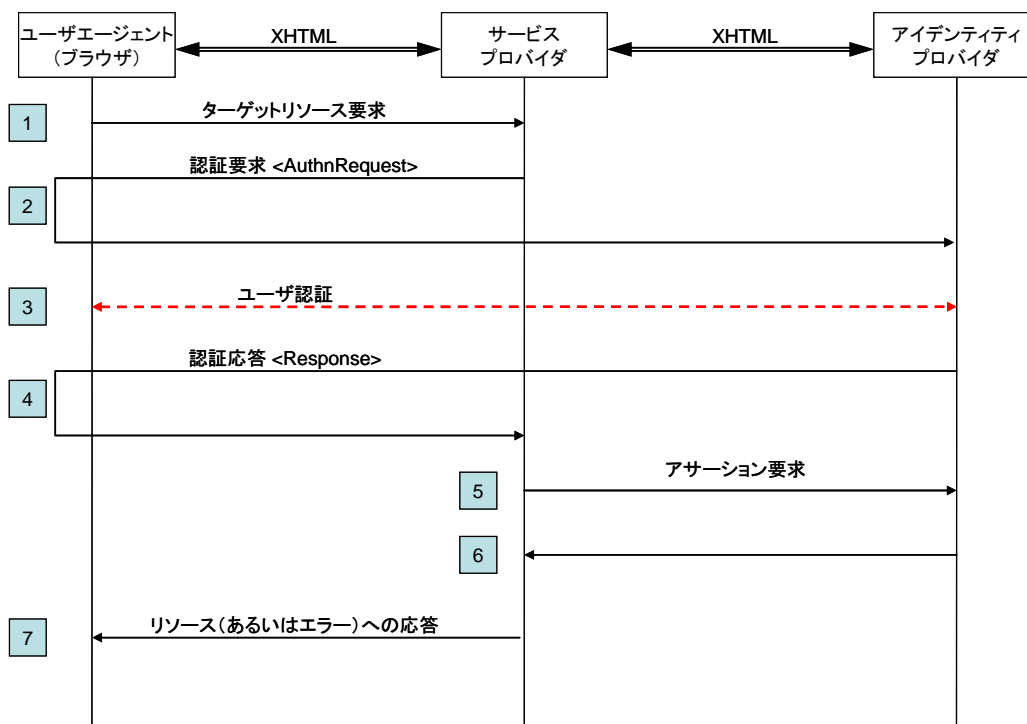


図 4.3.13 パスワード認証時の詳細処理フロー

パスワード認証にバイOMETリック認証を加える場合のシステム構成は、図 4.3.14 に示すように、バイOMETリック認証を行うためのバイOMETリック認証サービス用サーバをシステム構成に追加し、アイデンティティプロバイダがバイOMETリック認証依頼を受け付けると、利用者端末を呼び出して生体情報を取得し、取得した情報をバイOMETリック認証サービスを提供するサーバに送付してバイOMETリック認証依頼を行うことが考えられる。

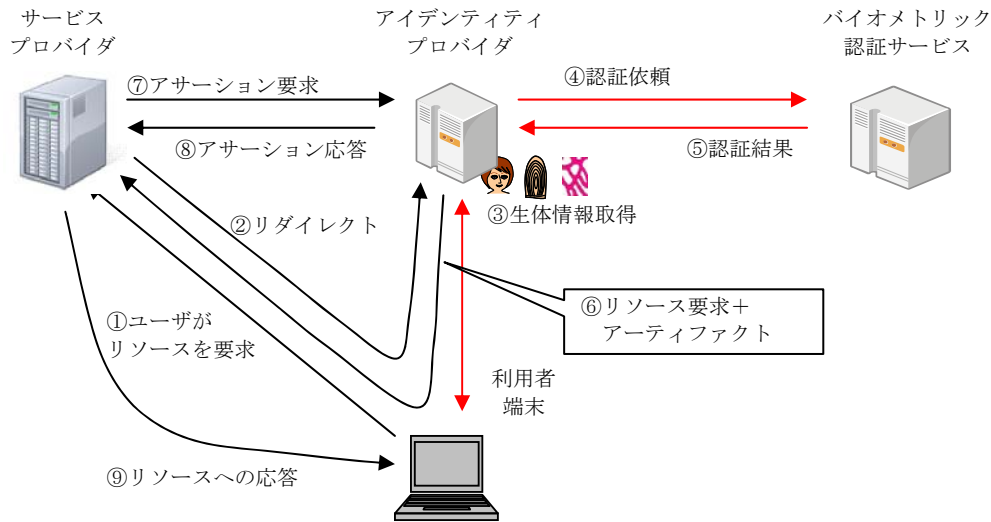


図 4.3.14 SAML でのバイOMETリック認証手順 (案)

また、その時の認証手順として、図 4.3.15 にパスワード認証時の詳細処理フローを示す。

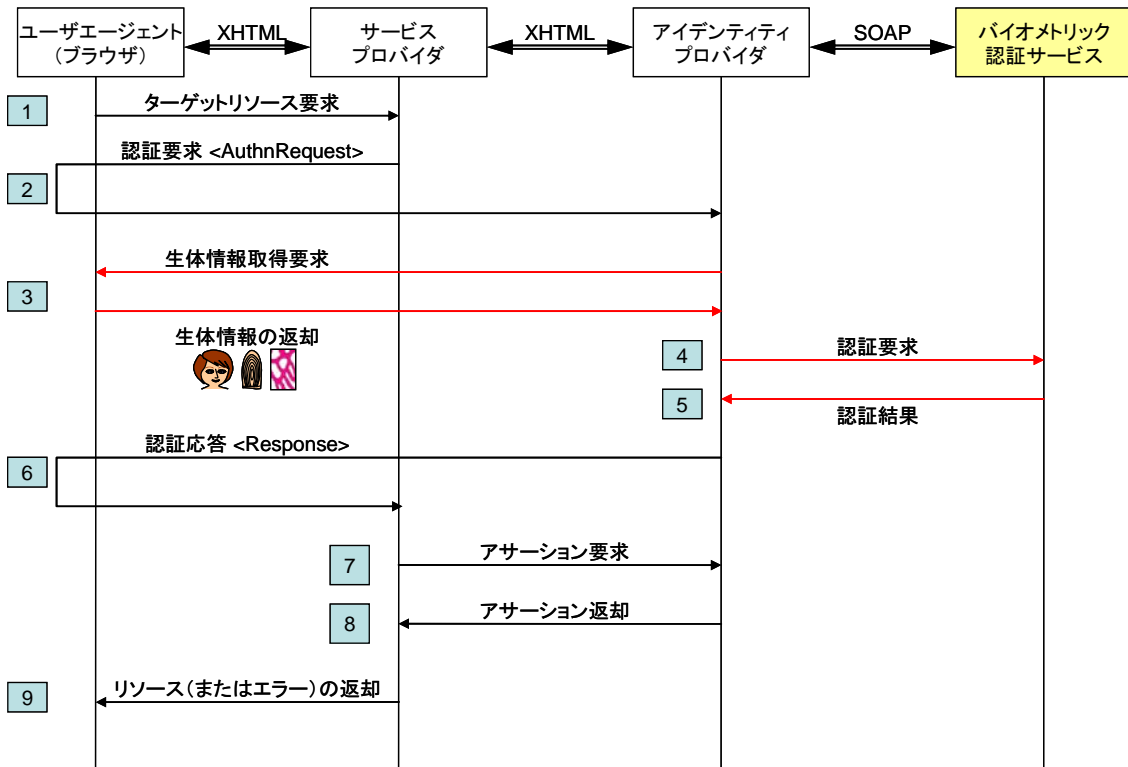


図 4.3.15 SAML でのバイOMETリック認証詳細フロー

以上検討してきたように、既存の国際標準規格である BIAS、BIP 及び BioAPI を適切に組み合わせることで IdM にバイOMETリック認証を組み込むことが可能であるとの見込みを得た。方式案を 図 4.3.16 に示す。

本図に示すとおり、バイOMETリック認証部分はインターネット上に SOA に基づいて構築可能な BIAS を配置することでアイデンティティプロバイダとバイOMETリック認証サービス間の接続を確立する。また、アイデンティティプロバイダと利用者端末の間はバイOMETリック装置の制御や生体情報の取得機能を有する BioAPI と BIP の組合せで実現する案である。

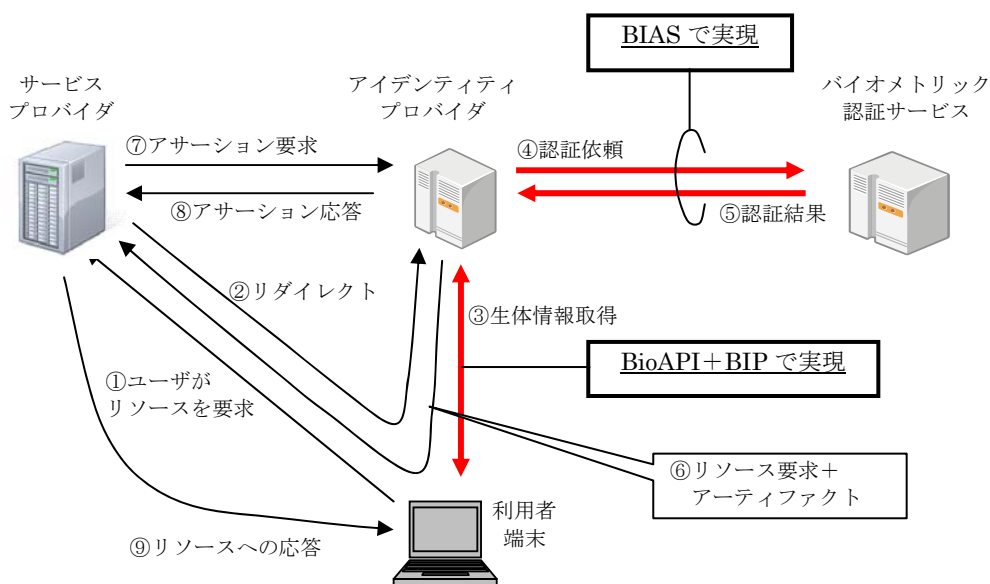


図 4.3.16 実現方式案

しかしながら、基本方針で示したバイOMETリックの特性を考慮すると、上記のバイOMETリック認証を組み込む方式案には以下の課題が存在する。

- (1) 利用者端末上で動作するアプリケーションが、バイOMETリック製品ごとのサポート機能の違いに対応しなければならない。このため、サポートするバイOMETリック装置を追加するたびにアプリケーションのロジックの変更や試験が必要となる。
- (2) 本システムに組み込まれるバイOMETリック製品の性能はアプリケーションの生体情報取得や認証のための処理内容に依存してしまう。したがって、同一のバイOMETリック製品を用いた場合でもアプリケーションが異なると、性能が異なる可能性がある。
- (3) プライバシー情報の漏洩リスクを軽減するためにはサーバ認証のみではなく端末認証も考慮に入れることが望ましい。

図 4.3.18 にバイOMETRICSを組み込んだ IdM アーキテクチャとして望ましいシステム構成図を示す。本図において新機能と記述されている部分が、既存あるいは現在審議中の国際標準に対して新規に検討する必要があると考えられる部分である。

今後この部分についての具体的な検討を推進する必要があると考えている。

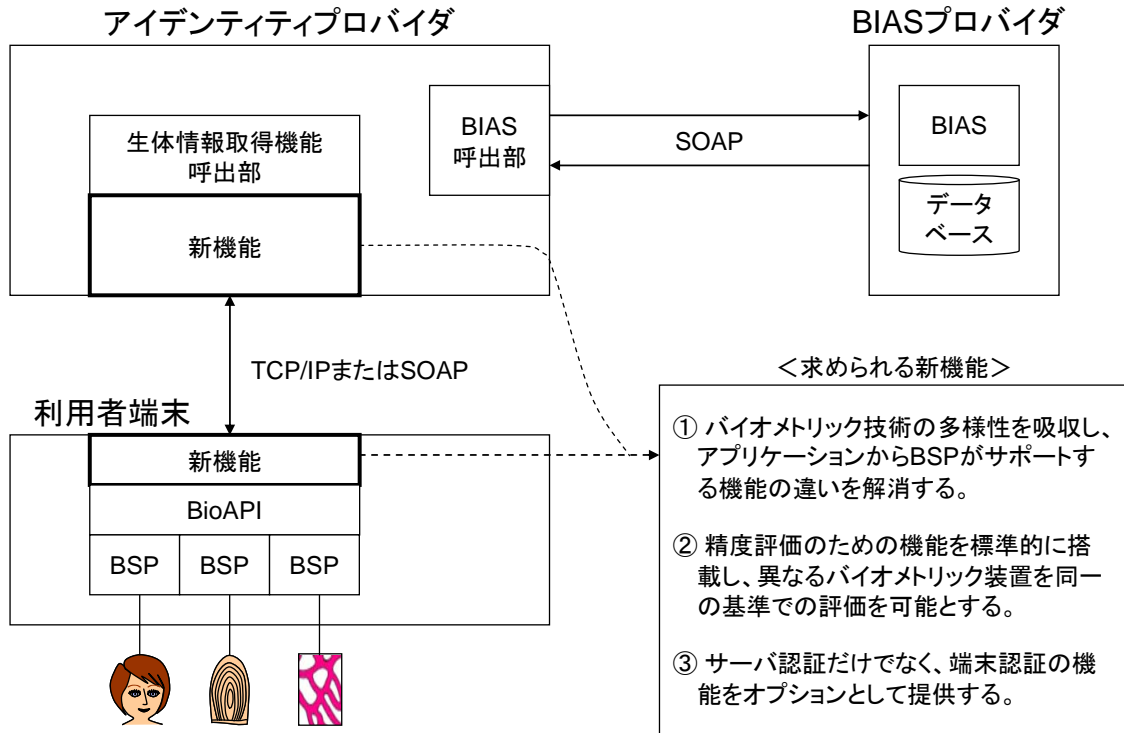


図 4.3.18 バイOMETRICS認証のために求められる新機能

#### 4-4 プライバシー保護の課題の明確化とその対策について

アイデンティティ・マネジメント（以下「IdM」と表記する。）へバイオメトリクスを組み込む際には、プライバシーや個人情報保護に関する問題が発生する。

まず、IdM 自体について、プライバシー・個人情報保護の課題が存在する。公的部門ないし公的サービスにおける IdM の問題としては、近年、納税者番号と社会保障番号の共通化の是非や国民 ID の導入の是非という形で議論されているが、本調査研究では、民間部門における IdM に焦点が当てられている。このように、民間部門で IdM を用いる場合、特に、SAML や OpenID のようにシングルサインオン（SSO）を中心とするシステムを導入する場合には、アイデンティティ提供者（認証事業者）と各サービス提供者の間における個人情報の取扱いなどが問題となる。

次に、バイオメトリクスについても、従来から、プライバシー及び個人情報保護の課題が存在することが指摘されている[1]。バイオメトリクスでは、指紋、顔、静脈、虹彩など人間の生体情報という重要な情報が利用されるため、プライバシー保護については、慎重な対応が必要になるところである。

これらを踏まえ、IdM にバイオメトリクスを組み込む際には、IdM 自体のプライバシー・個人情報保護の問題と、バイオメトリクスのプライバシー・個人情報保護の問題の両方が発生することになるため、この二つの問題を踏まえた上で、検討を行った。

基本的な前提問題として、まず、プライバシー権や個人情報保護法制に関する一般論を整理し、我が国においても、比較的検討が進んでいるバイオメトリクスに関するプライバシー問題を取り上げた。その上で、まだあまり議論がなされていない IdM に関するプライバシー問題を検討し、最後に、IdM にバイオメトリクスを組み込む際のプライバシー問題について検討を行った。

##### (1) プライバシー権

プライバシー権については[2]、学説上は、プライバシー権を、私生活を公開されない権利というような消極的権利として捉える見解よりも、自己情報コントロール権という積極的権利として捉える見解が有力になってきている[3] [4]。

これに対して、判例上は、プライバシーに係る情報の範囲が拡大してきているものの[5]、なお判例によって自己情報コントロール権説が正面から採用されるところには至っていないという状況にある。

##### (2) 個人情報保護法制

プライバシー権と密接に係る法制度として、個人情報保護法制が存在する。我が国でも、2003年5月に個人情報保護関連5法が制定されているが、欧米では我が国よりも早くからこのような法制度が整備されている。

国際的な動向としては、以下の二つが重要である。

(i) OECDプライバシー・ガイドライン (1980年) [6] [7] [8]

(ii) EU個人データ保護指令[9]

米国の個人情報保護制度に関して、米国には、今のところ、公的部門と民間部門の両方を包括的に規制する連邦レベルの個人情報保護法は存在しない。公的部門については、1974年にプライバシー法が成立しているが、民間部門については、包括法は存在せず、基本的には自主規制に委ねられている[10]。もっとも、民間部門については、特定の分野ごとに個別法が制定されており、いわゆるセクトラル方式が採用されている。代表的なものとしては、金融プライバシー権法 (1978年)、電子通信プライバシー法 (1986年)、ビデオ・プライバシー保護法 (1988年)、児童オンラインプライバシー保護法 (1998年) などがある。このように、米国の個人情報保護制度は、EUほど個人情報を厳格に保護しておらず、むしろ、情報の自由な流通や経済の発展を重視している。基本的には、プライバシー権の侵害があった場合に事後的に民事法上の救済を与えれば良いという発想があり、緩やかな事後規制型ということができる。

諸外国におけるのと同様に、我が国でも上述した1980年のOECDガイドラインを受けて、個人情報保護法制の必要性が強調されたが、公的部門の扱うデータについては、特に量的ウェイトが高いことから、まずは公的部門を対象とする法制度の整備が進められた[11]。その結果、1988年に「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律」が制定された。それに対して、民間部門を構成する法律は、制定されず、基本的には自主規制に委ねられたままになった。

しかし、その後、民間部門についても、個人情報を保護するための法整備が必要であると認識されるようになり[12]、2003年5月に、個人情報保護関連5法が制定された。

個人情報保護法は、基本理念などを定めた基本法部分と、民間部門に関する一般法部分とから構成される。まず、基本法部分では、基本理念、政府による個人情報の保護に関する施策の基本となる事項、国及び地方公共団体の責務が定められている。

民間部門に関する一般法部分においては、個人情報取扱事業者の義務が定められている。

### (3) バイオメトリクスに関するプライバシー問題

バイオメトリクスについては、それが人間の生体情報を用いるものであるところから、プライバシーないし個人情報の保護に関わる問題を生じさせるものと認識されている。個人情報には様々な種類のものがあるが、その中でも生体認証情報は、特に重要な情報であり、そのため慎重な取扱いが要請される[13]。

バイオメトリクスの認証モデルは、バイオメトリックデータをユーザが所持するICカードなどのトークンに保管するユーザ管理型 (ローカルシステム) と、サーバにデータベースとして保管するサーバ管理型 (センターシステム) の二つが存在する。前者のユーザ管理型の場合にもプライバシー問題は発生するが、サーバ管理型は、より深刻な問題を発生させると考えられる。

サーバ管理型の場合、まず登録処理が行われる。すなわち、本人から生体情報を取得し、これから特徴抽出を行い、テンプレート化を行う。そして、これを蓄積していくことによってデータベースを作成する。また、認証処理の際には、データベースの情報と本人の生体情報を照合することによって、本人か否かの判定を行うということになる。これらの全ての段階において、プライバシーに対する脅威が存在する。まず、本人から生体情報を取得する時点で、不正な取得がなされる恐れがあり、テンプレートやデータベースの情報が、不正に漏洩したり、売買されたりする恐れがある。また、照合・判定の際にも、データが不正に取得される恐れがある。このようにして、バイオメトリクスにおいては、プライバシー・個人情報保護に関わる問題が生じることになる。

#### (4) バイオメトリクスと個人情報保護法制

バイオメトリクスの対象となる生体情報は、個人情報になる可能性があるため、個人情報保護法制に関わる問題も発生する。

この問題については、EUにおける議論が先行的になされてきた。

EUにおいては、前述したようにEU個人データ保護指令が重要な意味を持っている。そのため、バイオメトリクスについても、EU個人データ保護指令をバイオメトリクスに適用していく際の解釈論という形で議論されることが多い。EUの中では、ドイツにおける取り組みが先行した。1997年には、TeleTrust/WG6が設立され、また、1998年から2002年にかけては、BioTrustというプロジェクトが行われた。このプロジェクトは、「バイオメトリックデータの悪用・誤用防止に関する勧告」を出している。これらを受けて、更にEU諸国を巻き込んで大規模に行われたのが、次のBIOVISIONプロジェクトである。

このプロジェクトは、欧州委員会（EC）が統括する第5期研究開発プロジェクトの一環として行われたものであり、かなり大規模なプロジェクトである。BIOVISIONは、2003年に“Privacy Best Practice in Deployment of Biometric Systems” [14][15]（以下「ベストプラクティス」と称する）という報告書を公開している。

更に、EUでは、BIOVISIONのベストプラクティスを受けて、EU個人データ保護指令29条に基づいて設置された作業部会が、2003年に、“Working Document on Biometrics” [16]を公開している。これは、EU指令の作業部会が策定したものであり、ベストプラクティスよりも重要度が高いということができる。

EUにおいて、EU個人データ保護指令におけるバイオメトリクスの取り扱いが検討されているように、我が国においても個人情報保護法制をバイオメトリクスに適用していく際の解釈論を行っていくことによって、法律上のバイオメトリクスの取り扱いを明確化していくことが重要である。

バイオメトリック認証システムが一定規模以上の民間事業者、正確には個人情報保護法2条3項にいう個人情報取扱事業者によって運用される場合は、個人情報保護法が関係してくることになる。

### ① バイオメトリックデータの個人情報該当性

対象となるバイオメトリックデータに個人情報保護法が適用されるためには、当該バイオメトリックデータが、個人情報保護法 2 条 1 項の個人情報に該当することが必要である。そこで、バイオメトリックデータがいかなる場合に個人情報にあたるのかが問題となる。

この点については、我が国では、様々な見解が存在するところである。顔画像については、それが特定個人を識別可能なものである限り、基本的に個人情報に該当することに争いが無いが、それ以外の指紋、虹彩、静脈などについては、どのような場合に、個人情報に該当するのかについて争いが存在する[17]。もっとも、バイオメトリックスの認証システムを用いて認証を行う事業者が、バイオメトリックデータと氏名などの個人情報を容易に照合できる状態にある場合もありうる所であり、そのような場合には、当該バイオメトリックデータは、その個人情報取扱事業者との関係で個人情報に該当することになる。この点は、テンプレートデータについても、同様であり、一般的には、テンプレートデータ単体では、原則として、個人情報に該当しないものと理解されているが、認証事業者がテンプレートと氏名などの個人情報を容易に照合できる状態にある場合には、当該テンプレートもその認証事業者との関係において、個人情報に該当することになる。

### ② バイオメトリックデータの取得

EU 個人データ保護指令 7 条は、個人データの取得などの処理をするには、原則として本人の同意が必要だとしている。これに対して、我が国の個人情報保護法 17 条は、「偽りその他不正な手段により個人情報を取得してはならない」としているだけで、必ずしも明確には本人同意を要求していない。

この点については、実務運用上は、バイオメトリックデータの重要性からいって、原則として本人の同意を得るようにすることを推奨するというところも考えられるところである。

### ③ センシティブデータ（機微情報）の取扱いについて

EU との比較法的観点から問題となるのは、センシティブデータの取扱いである。EU 個人データ保護指令 8 条 1 項は、センシティブデータの処理を原則として禁止している。

バイオメトリックデータの場合、例えば、顔画像からは、人種、民族、健康状態などのセンシティブデータが抽出される恐れがある。また、静脈、掌形、虹彩などからもその人の健康状態を明らかにすることができるという指摘もなされてところである。

このような場合、EU 指令ではセンシティブデータの取扱いについて規定があるためその規律が明確であるが、我が国の個人情報保護法では、センシティブデータに関する規定が存在しないため問題になる。我が国では、現在のところ、各省庁から出される個人情報保護法に関するガイドラインにおいて、センシティブデータの取り扱いが定められるようになっている。例えば、金融庁から 2004 年 12 月 6 日に出された「金融分野における個人情報保護に関するガイドライン」[18]の 6 条がある。

更に、金融庁は、2005年1月6日に、上記の「金融分野における個人情報保護に関するガイドライン」における安全管理措置の実効性を担保するものとして、「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」[19]を出している。

従来、バイオメトリクスプライバシー問題については、欧米の方が先行しているところもあったが、以上見てきたように、我が国でも活発な議論が行われるようになり、ガイドラインなどの整備もなされるようになってきている。IdMにバイオメトリクスを組み込む際にも、以上のような議論状況を踏まえた上で、検討する必要があるものと考えられる。

## (5) アイデンティティ・マネジメント (IdM) に関するプライバシー

～シングルサインオンを中心として～

IdMに関するプライバシー問題としては、現在、活発に議論されている国民IDないし共通番号制度のような公的部門における問題もあるが、本研究では、民間部門においてIdMが利用される場合を中心に見ていくことにする。また、民間部門においてIdMを利用する場合も、様々なシステムが存在する。

シングルサインオンとは、ユーザがいったん認証されると、その後は、認証を受けずに複数のサービスを利用することが可能になるものをいう。シングルサインオンを用いたIdMとして、代表的なものとしては、OASISによって策定されたSAML2.0や、OpenID Foundationによって策定されたOpenID2.0などがある[20]。このシングルサインオンについては、ユーザとしては、一度認証を受ければ、その後は、いちいち認証を行わなくても、様々なサービスを利用することができるため、一定の利便性を有するものであるといえる。しかし、その一方で、プライバシーや個人情報保護に関わる問題を生じさせるものと考えられる。

シングルサインオンが有するプライバシーの脅威については、2002年の時点で、以下の三つの点が指摘されている[21]。

- ① 同一サイト内でのユーザ行動の関連付け
- ② 複数サイト間でのユーザ行動の関連付け
- ③ 送信元情報の流出

また、上記の三つでは、十分に指摘されていないが、シングルサインオンには、もう一つプライバシーに関する問題が存在する。シングルサインオンを用いたIdMにおいては、氏名、住所などの属性情報の共有（属性共有）が行われることが多い。属性情報としては、氏名、住所の他、生年月日、所属、役職、信用情報、人間関係などが挙げられている[22]。これらの属性情報は、プライバシー情報や、個人情報に該当する場合が多いため、これらの属性情報が、認証を行うアイデンティティ提供者や、複数のサービス提供者間において共有されると、プライバシーや個人情報保護に関する問題を生じさせることになる。

シングルサインオンを用いた最も代表的な IdM の方式として、業界団体 OASIS によって策定され、Liberty Alliance によって相互運用テストが実施されている SAML2.0 がある。

この SAML2.0 については、プライバシー問題に対して、ある程度の対応がなされているものと考えられる。第一に、SAML2.0 は、統一的な識別子を用いるアイデンティティ統一方式ではなく、アイデンティティ連携方式を採用しているということである[23]。複数のサービスで統一の識別子を用いれば、その識別子を通じて、様々な個人情報が名寄せされる恐れが高くなり、プライバシーのリスクが大きくなるが、アイデンティティ連携方式では、各サービスで異なるアイデンティティを用いるため、プライバシーに関するリスクは相対的には低くなるといえる。

第二に、SAML2.0 は、サービス提供者間において、属性情報を共有する際に、本人から同意を取得することを基本的に想定しているということである。例えば、ユーザがあるサービス提供者 (SP1) からオンラインショッピングで商品を購入する場合に、SP1 が、当該ユーザの住所などの属性情報を他のサービス提供者 (SP2) から取得するには、SP2 が本人から同意を得る必要があるとされている[24]。SP2 から SP1 に住所などの属性情報を提供することは、プライバシー情報あるいは個人情報を第三者に提供することになるが、本人の同意が適正に取得されていれば、基本的には、プライバシー権侵害や個人情報保護法違反の問題は生じないものと考えられる。

もっとも、アイデンティティ連携方式も、あるサービス内においては、同一のアイデンティティを用いることになるため、上述した①同一サイト内でのユーザ行動の関連付けの問題は、残されているように思われる。

OpenID2.0 は、OpenID Foundation によって策定されたものであり、シングルサインオンを用いた代表的な IdM の方式の一つである。特徴としては、ユーザが URL などで表現されたグローバルにユニークな識別子を持つということが挙げられる。

この OpenID2.0 に対しては、これをアイデンティティ統一方式に位置付けた上で[25]、プライバシー上のリスクが高いとする指摘がなされている。すなわち、「何らかの手段で事前に信頼関係が構築されていなければ、信頼レベルが確認できない相手とアイデンティティ情報をやりとりすることになり、セキュリティ上のリスクは高まる」とし、また、「グローバルでユニークな識別子を複数のサービスで用いる場合は、前述の『名寄せ』によるプライバシー侵害のリスクも高まる」とするのである[26]。

もっとも、これに対しては、OpenID においても、プライバシー保護が可能であるという指摘もなされている。OpenID Foundation の崎村夏彦氏は、OpenID におけるプライバシー保護のためのソリューションとして、いくつかの点を指摘しているが、その中で、「名寄せ防止」についてもふれている[27]。すなわち、「分野ないしサービスごとに異なる『番号』を振り出す仕組みによって『名寄せ防止』が可能」とするのである。

いずれにせよ、OpenID の場合、アイデンティティ提供者 (OpenID Provider) からユーザに関する個人情報が漏洩するリスクが存在する可能性があるように思われる。OpenID では、アイデンティティ提供者になれる者に特に制限がなく、誰でもアイデンティティ提供者になることが可能になってい

る。そのため、プライバシー保護やセキュリティ対策が十分ではない事業者であっても、アイデンティティ提供者になることが可能であり、そのような場合には漏洩のリスクが発生することになる。なお、この点に関連して、[openid.ne.jp](http://openid.ne.jp) のホームページには、以下のような Q&A が記載されている [28]。すなわち、「Q11. もし OpenID の認証サーバがハッキングされたら、登録している全てのユーザの情報が漏洩してしまうのではないですか？」という問いに対して、「はい、確かにその可能性はあります。しかしそれはあなたが良く利用しているポータルサイトの ID が漏洩したらそのポータルサイトの全てのサービスを見られてしまうことと同じことです。つまり情報漏洩は OpenID のシステムに問題があるというより、OpenID の認証サービスを提供する会社をあなたがどこまで信頼できるかという問題だと思います」という解答を掲載しているのである。これは、一定の漏洩リスクが存在することを自認していることの現われのように思われる。

以上見てきたように、シングルサインオンを用いた IdM のプライバシー問題については、少なくとも代表的な方式である SAML2.0 及び OpenId2.0 においては、一定の対応がなされているか、もしくは対応がなされようとしている。しかし、なおプライバシー保護に関する課題は残されているものと考えられる。

この点については、次のような指摘が注目される場所である。すなわち、「(特別な保護メカニズムが入っていない限り) 認証提供者が利用者の利用サービスを知り得るという問題がある」とするのである [29]。これは、基本的には、SAML2.0 及び OpenId2.0 に共通する問題であると考えられる。いずれの方式においても、アイデンティティ提供者は、各サービス提供者からの認証要求に対して、認証結果を通知している以上、ある特定のユーザがどのようなサービスを利用しているのかという利用履歴に関する情報を把握することが可能になっている。様々なサービス利用履歴が蓄積し、これが大量に漏洩することになれば、プライバシーに関する問題を生じさせることになる。特に、OpenID の場合は、どのような事業者であっても、すなわちセキュリティやプライバシー保護の対策が十分でない事業者であってもアイデンティティ提供者 (OP) になることが可能なため、このようなリスクを十分考慮する必要があるように思われる。

## (6) IdM へバイオメトリクスを組み込む際のプライバシー

ここまで、基礎的な前提として、プライバシー権及び個人情報保護法制について整理し、その上で、バイオメトリクスと IdM のプライバシー問題について検討を加えてきた。これらを踏まえて、IdM にバイオメトリクスを組み込む際のプライバシーの課題とそれに対する対応について、見ていくことにする。

IdM も様々な場面において用いられるが、バイオメトリクスとの併用を前提とした場合、各企業における内部統制に用いられる場合 (内部統制型) よりも、インターネットを用いた Web アプリケーションにおいて用いられる場合 (Web アプリ型) の方が、多くの課題が発生するものと考えられる。ここでは、主として、後者の Web アプリ型にバイオメトリクスを組み込む場合を念頭において検討を進めることにした。

これまで述べてきたように、シングルサインオンを用いた代表的な IdM の規格としては、SAML2.0 と OpenID2.0 がある。シングルサインオンを用いた IdM に、バイオメトリクスを組み込む際には、様々な課題が生じるものと考えられる。その多くは、シングルサインオンが、オープンネットワーク環境を利用したリモート認証であるところから生じる。このようなりモート環境においてバイオメトリクスを利用した場合の課題については、次のような点が指摘されている[30]。

例えば、オープンネットワーク環境における一般的な認証方法として、パスワード認証がある。これを、そのままバイオメトリクスに置き換えると、機微な情報と考えられている生体情報を事前にオンラインショッピングの店舗に登録することになるため、ユーザには抵抗感が生じるし、オンライン店舗側としても厳重な管理が必要になるという課題が発生する。そこで、このような課題に対応するため、IC カードなどの媒体に事前に生体情報を登録しておき、生体認証の結果だけをオンライン店舗に送信するという方式が考えられることになる。もっとも、このような方式を用いる場合、オンライン店舗としては、認証結果だけを送られても、その結果をどの程度信用して良いのかが分からない。この生体認証の結果の真正性を保証するような枠組みがあれば、オープンネットワーク環境におけるリモート認証においても、安全にバイオメトリクスを利用することが可能になる。このようなりモート認証においてバイオメトリクスを用いる場合の真正性を確保すること目的とした国際標準規格として、ACBio (ISO/IEC 24761 Authentication Context for biometrics) が存在する[31]。

また、オープンネットワーク環境におけるリモート認証においてバイオメトリクスを用いる場合には、上記の真正性の保証以外にも、プライバシーに関する問題も発生する。上述の ACBio のように、バイオメトリックデータをユーザが保有する IC カードなどに入れてユーザ側が管理する場合には問題は発生しにくい、常にこのようなシステムが用いられるとは限らない。バイオメトリックデータをテンプレート化し、テンプレートをオンライン店舗のサーバ側で管理する場合には、プライバシーや個人情報保護に関する問題が発生することになるのである。なお、オープンネットワーク環境では、データの送信中に、不正な第三者にハッキングされ、バイオメトリックデータないしテンプレートデータや、認証結果が途中で改変されるリスクも存在する。

なお、IdM へのバイオメトリクスの組み込みに関連する標準規格としては、上述の ACBio の他に、BIAS(Biometric Identity Assurance Services)という規格が策定途上にある。これは、ISO/IEC JTC1 SC37/WG2 に米国から提案されているものである。この BIAS も Web サービスにバイオメトリクスを用いる場合を想定したものである[32]。

このように、Web アプリ型のシングルサインオンにバイオメトリクスを組み込む場合には、オープンネットワーク環境においてバイオメトリクスを用いることになるため、様々な課題が発生するが、以下では、これらの課題のうちプライバシーの問題に焦点を当てて検討していくことにしたい。

上述したように、シングルサインオンを用いた IdM にバイオメトリクスを組み込む際には、プライバシーないし個人情報保護に関する問題が生じることになる。現在、ISO/IEC JTC1 SC37/WG6 で検討されている ISO/IEC 29144(The Use of Biometric Technology in Commercial Identity

Management Applications and Processes)においても、プライバシーへの言及が見られるところである[33]。

IdM にバイオメトリクスを組み込む場合のシステム構成としては、様々なものが考えられるところである。一つは、シングルサインオンを用いた IdM において認証を行うアイデンティティ提供者が、バイオメトリック認証も行うというシステム構成である。もう一つは、バイオメトリクスを用いた認証は、アイデンティティ提供者とは別のバイオメトリック認証プロバイダで行うというものである。この両者のいずれのシステム構成によるのかによって、プライバシー・個人情報保護に関する問題の発生も異なってくる部分があるが、以下では、この両者の場合を念頭に置きつつ検討を行うことにする。

なお、いずれにせよ、IdM にバイオメトリクスを組み込んだ際に、アイデンティティ提供者や、各サービス提供者間において、属性共有が行われるということはあまり発生しないものと考えられる。というのは、シングルサインオンにバイオメトリクスを用いる場合であっても、バイオメトリクスを使用するのは認証を行うアイデンティティ提供者やバイオメトリック認証プロバイダだけなので、それ以外のサービス提供者がバイオメトリックデータやテンプレートを必要とする事態はあまり考えられないからである。

したがって、バイオメトリックデータやテンプレートが、アイデンティティ提供者及び各サービス提供者の間で共有されるということ自体があまり発生しないものと考えられる。以下では、ユーザ、アイデンティティ提供者、バイオメトリック認証プロバイダの間で発生するプライバシー問題について見ていくことにする。

#### (a) 生のバイオメトリックデータとテンプレート

生のバイオメトリックデータは、取替えが困難であること、副次的な情報が抽出される恐れがあることなどの理由から、個人に関する情報の中でも重要度が高いものであると考えられる。バイオメトリクスを利用する場合、一般論として、できるだけ生データは速やかに廃棄し、テンプレートのみを取得、管理するのが妥当であるということが、BIOVISION のベストプラクティスにおいて指摘されている。すなわち、「バイオメトリックデータのエンコーディング（符号化）は可及的速やかに行われることが望ましい。可能な限り生データではなくテンプレートのみを利用して可及的速やかに生データは無効化処理しなければならない。もし生のイメージファイルがシステム操作に必須である場合は、それらは適切に保護されなければならない」。特に、Web アプリ型のシングルサインオンにおいて、バイオメトリクスを利用する場合には、オープンネットワーク環境を利用することになるものと想定される。したがって、ユーザがアイデンティティ提供者にデータを送信する途中で不正な第三者にハッキングされ、データを読み取られる恐れがあるため、できるだけ生データよりもテンプレートを利用するのが望ましいものと考えられる。もっとも、モダリティやアプリケーションの種類によっては、生データが必要になる場合もあると考えられる。その場合は、BIOVISION のベストプラクティスにあるように、生データを適切に保護することが重要であると考えられる。

## (b) テンプレートの管理

IdMにおいて、アイデンティティ提供者などの認証事業者が、生のバイOMETリックデータではなく、テンプレートを利用する場合、テンプレートは、ユーザ側で管理するのか、それともアイデンティティ提供者やバイOMETリック認証プロバイダのサーバ側で管理するのかが問題となる。この点、現在、開発が進められているBIASの規格では、明確に定められているわけではないが、テンプレートをサーバ側で管理することが想定されているようである[34]。しかし、プライバシー及び個人情報保護の観点からは、テンプレートなどをサーバ側で管理する集中データベース型（サーバ管理型）よりも、ユーザ側で管理する分散ストレージ型（ユーザ管理型）が望ましいとされることがある。

例えば、BIOVISIONのベストプラクティスには、次のような記述がなされている。「アプリケーションに適しているときは常に集中データベースよりも、分散ストレージを使用することが望ましい。なぜならば、集中データベース内の適切な保護手段には、他者の下で厳しいアクセス権に基づく徹底したコントロールや、暗号化される場合における適切な暗号鍵の管理が常に要求されるからである。多くの場合、これを実際に実現することは困難である。なぜならば、その結果、誤用という潜在的なリスクや、機能脆弱性が、データ主体の直コントロール下にあるストレージよりも、更に容易に発生し得るからである。更にいうと、ユーザに対し、本人のバイOMETリックデータのコントロール権を提供することがより高い透明性の提供を実現可能とするのである。」もともと、このことは、常に分散ストレージ型（ユーザ管理型）でなければならないということまで意味するものではないと考えられる。ベストプラクティスにも次のように書かれている。「ただし、このことは集中データベース利用を絶対的に回避せよという意味」ではないということである。したがって、プライバシー保護の観点からは、サーバ管理型よりも、ユーザ管理型が望ましいところがあるとしても、利用局面やアプリケーションなどに応じて、どちらのタイプを利用するのかを判断することになるものと考えられる。

仮に、BIASにおいて、分散ストレージ型（ユーザ管理型）ではなく、集中データベース型（サーバ管理型）が採用されているとした場合、プライバシー・個人情報保護の観点から、テンプレートなどのデータを厳格に管理する必要があるものと考えられる。

## (c) テンプレートと個人情報の照合可能性

テンプレートは、生のバイOMETリックデータから、特徴点を抽出し、それを一定のアルゴリズムにしたがって、数値化したものであるため、テンプレート単体では、特定の個人を識別することができない場合がほとんどである。したがって、原則として、テンプレートそれ自体は、個人情報保護法上の個人情報には該当しないものと考えられる[35]。しかし、テンプレートが認証事業者の内部において、氏名、住所などの個人情報と容易に照合できる状態にある場合には、それは容易照合可能性があることになり、テンプレートも個人情報保護法上の個人情報に該当することになる。

IdM にバイオメトリクスを組み込む際に、テンプレートをユーザ側で管理するのではなく、アイデンティティ提供者側又はバイオメトリック認証プロバイダ側で管理する場合には、テンプレートと氏名、住所などの個人情報容易に照合可能な状態にある場合が多いのではないかと推測される。その場合には、テンプレートも個人情報に該当するため、アイデンティティ提供者やバイオメトリック認証プロバイダには、個人情報保護法上の義務規定が適用されることになる。また、それらのテンプレート及び氏名、住所などの個人情報がデータベース化されている場合には、「特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの」に該当することになり、それらのデータは、個人情報保護法上の個人データに該当することになる。その場合、アイデンティティ提供者やバイオメトリック認証プロバイダには、個人情報保護法の 19 条から 23 条の義務規定が適用されることになる。

(d) バイオメトリックデータ又はテンプレートの第三者提供

IdM にバイオメトリクスを組み込む場合に、アイデンティティ提供者とバイオメトリック認証プロバイダが別々になるシステム構成も考えられる。このような場合には、生のバイオメトリックデータ又はテンプレートが、アイデンティティ提供者から、バイオメトリック認証プロバイダに対して、提供されるということが想定されるが、これによってプライバシー・個人情報保護に関する問題が発生する。

まず、生のバイオメトリックデータが提供される場合、生のバイオメトリックデータは、個人情報保護法上の個人情報に該当する場合があるため、これをアイデンティティ提供者からバイオメトリック認証プロバイダに提供することは、第三者提供にあたり、個人情報保護法 23 条に基づいて、原則として本人の同意を取得することが必要になる。次に、テンプレートが提供される場合であるが、前述したように、テンプレート単体では、個人情報保護法上の個人情報に該当しないのが原則であるが、テンプレートと氏名、住所などの個人情報が容易に照合できる状態にある場合、それらは個人情報に該当することになるため、そのような場合には、原則として本人の同意を取得することが必要になる。

(e) 個人情報が国境を越えて移転する場合

シングルサインオンを用いた Web アプリ型の IdM にバイオメトリクスを組み込む場合、ユーザに関する様々な情報が国境を越えて移転する場合も考えられるところである。例えば、ユーザとアイデンティティ提供者が異なる国に存在する場合、アイデンティティ提供者とバイオメトリック認証プロバイダが異なる国に存在する場合などである。このような場合には、個人情報ないし個人データの越境流通の問題が生じることになる。

個人データの越境流通は、古くから議論されてきた問題である。1970 年代に、世界の様々な国々で個人データを保護する法制度が制定されるようになったが、それらの内容が大きく異なっていることが問題となった。そこで、国際的な法制度の調和を図ることを目的として、先に紹介した OECD プライバシー・ガイドラインが 1980 年に発行された。しかし、その後も、世

界の国々における個人データ保護法制に相違が存在する状況は続いており、特に、厳格に個人データを保護する EU 諸国と、情報の自由な流通を重視する米国の対立が問題となっている。

個人データの越境流通で具体的に問題となるのは、EU 個人データ保護指令 25 条が十分な保護のレベルにない国に対しては、EU 加盟国から個人データを出してはいけないという規制を行っていることである。この点については、米国は、EU とセーフハーバー協定を締結することによって解決を図ったが、日本は、EU 個人データ保護指令 25 条に対する明確な対応策を打ち出していない状況にある。したがって、IdM にバイオメトリクスを組み込む場合にも、バイオメトリックデータや、テンプレートが EU 加盟国から、日本に移転するような場合には、EU 個人データ保護指令 25 条に対する何らかの対応が必要になる場合がある。例えば、同指令 26 条の例外規定、標準契約条項、拘束的企業準則 (BCR: Binding Corporate Rules) などを用いることが考えられる[36]。

なお、現在のところ、日本の個人情報保護法には、個人情報の国外移転を規制する条文は存在しないため、日本国内から、海外のアイデンティティ提供者や、バイオメトリック認証プロバイダに対して、個人情報やバイオメトリックデータを移転する場合には、特に法律上の規制はかからないという状況になっている。

ここでの検討の視点を改めて整理すると以下の 2 点になる。一つは、個人情報保護法がどのように適用されるのかということであり、もう一つは、プライバシー保護の観点から、どのようなシステムが望ましいのかということである。まず、個人情報保護法が適用される場合には、確実に法律上の要請を遵守する必要があることはいうまでもない。これに対して、プライバシー保護の観点からどのような対策が望ましいのかについては、微妙な判断が必要とされる。本項においては、主としてプライバシー保護の観点に重点を置いて検討してきたが、実際に IdM にバイオメトリクスを組み込んだシステムを開発し、普及させる際には、プライバシー保護の要請だけではなく、ユーザの利便性や、セキュリティ対策の程度など、様々な要素を総合的に考慮する必要があるであろう。その上で、どのようなシステム構成を採用するのかをケースバイケースで判断することが重要であると考えられる。

なお、シングルサインオンを用いた IdM にバイオメトリクスを組み込む場合、アイデンティティ提供者 (あるいはバイオメトリック認証プロバイダ) に、ユーザに関する氏名、住所などの属性情報、テンプレート、ID/PW などの認証情報が集中しやすいところがある。したがって、アイデンティティ提供者は、これらの情報を漏洩させないように、安全な管理を行うことが要請される。特に、OpenID の場合には、規格上誰でもアイデンティティ提供者 (OP) になれるため、漏洩リスクがどの程度あるのか、ユーザ側でアイデンティティ提供者を慎重に見極めて選択する必要があるように思われる。

#### 4-5 調査研究の成果（まとめ）

2001.9.11の世界同時多発テロ以降、個人認証の重要性が年々増加し、個人認証に利用するアイデンティティの管理や運用が複雑になり、構築運用コストが増大し、運用管理のリスクも増大しており、効率的に、かつ確実にアイデンティティを管理することが求められている。

また、近年の電子行政サービスの充実に伴い、サービス形態が多様化し、各サービス間での認証連携も必要となることが予想される中で、サービスを安全で安心な形で提供するために、システムを利用するユーザのアクセス権限の管理の重要性が増してくるものと予想している。

また、これら社会生活の環境が大きく変わる一方で、IDやパスワードの盗用、なりすましなどのセキュリティに関する問題も発生している。従来から公共、あるいは民間のサービスの本人確認手段として、本人以外が知り得ない情報（IDやパスワードなど）や、本人以外が持ち得ない身分証明書（IDカード、健康保険証、運転免許証など）が用いられているが、なりすましなどを防止するには、生体情報（バイオメトリクス）を利用した個人認証技術が有効であるともいわれている。

一方、2009年以降の日本国内のバイオメトリック市場は、企業にヒアリングしたところでは、2004年以前の水準つまり100億円程度に落ち込んでいる可能性がある。日本国内のバイオメトリック製品の大きな市場は、警察関係などのフォレンジック用途と銀行ATM用途に限られ、これらはリプレースなどに限定され伸びが期待できない。

このため、日本企業の発展のために市場をけん引する新規の分野が必要であり、アイデンティティ管理にバイオメトリック技術を適用することにより提供できる「バイオメトリック認証の高いセキュリティ機能を持つアイデンティティ管理」による新たな市場は、今後が期待できる有力な候補であると考えられる。

アイデンティティ管理は広範な領域を含んでいるが、ユーザアクセス管理とシングルサインオン技術を中心とするWeb上における技術仕様の大きく二つの観点で議論されている。

ユーザアクセス管理は、個々の企業システムを対象に製品ベンダがアイデンティティ管理ソリューションを提供するというプロダクトベースでの議論、一方シングルサインオン技術を中心とするWeb上における技術仕様では、様々な企業が連携して標準化団体を作り普及を図っておりプロジェクトベースでの議論となっている。しかしながら、現状のIdMではバイオメトリクスが考慮されていない。

国際標準においてもアイデンティティ管理そのものの標準化はまだ策定の途中であるが、アイデンティティ管理自体が広範な領域を含んでいるために関連する国際標準は多岐にわたっている。

海外においてはEUが主導するプロジェクトベースでの調査研究活動が活発に行われている。

また米国では、アイデンティティ管理そのものへの取り組みはそれほど行われていないが、すでに明文化された個人識別情報の検証PIV（Personal Identity Verification）の技術仕様であるSP800シリーズとの関連の中で検討が行われている。

今回の調査研究において、アイデンティティ管理に関する現状の技術を包括的に明らかにすること

ができた。また、アイデンティティ管理にバイオメトリック技術を適用するためのアーキテクチャの基本方法式案を得ることができた。

本調査研究報告での見解は以下のとおりである。

(1) 市場性

世界におけるアイデンティティ管理市場は、2008年時点で約45億米国ドル、日本国内は約109億円市場である。一方、2009年以降のバイオメトリック市場は、企業にヒアリングしたところでは、2004年以前の水準つまり100億円程度に落ち込んでいる可能性がある。日本国内のバイオメトリック製品の大きな市場は、警察関係などのフォレンジック用途と銀行ATM用途に限られ、これらはリプレースなどに限定され伸びが期待できない。

このため、日本企業の発展のために市場をけん引する新規の分野が必要であり、アイデンティティ管理にバイオメトリック技術を適用することにより提供できる「バイオメトリック認証の高いセキュリティ機能を持つアイデンティティ管理」による新たな市場は、今後が期待できる有力な候補であると考えられる。

(2) 間接認証タイプにバイオメトリック技術を適用する開発が重要

現状のアイデンティティ管理市場における製品はローカル認証、直接認証型が多いため、成長が望めない。オフライン認証は標準化が進むが社会インフラ整備負担が大きく、市場で広く受け入れられていないと考える。

アイデンティティ管理市場で、間接認証は、SAMLやOpenIDなどのIdMアーキテクチャの主流となりつつあり、アイデンティティ管理におけるバイオメトリック技術の適用に向けては、間接認証をベースとしたウェブアプリ型のIdM技術開発が有効と考える。

米国及び標準化では、アイデンティティエコシステムやBIASなどのアーキテクチャが開発されているため、これらの動向を良く見極め、標準にのるような技術開発が必要である。

(3) SOA（サービスオリエンティドアーキテクチャ）の採用が重要

欧米のIdM、バイオメトリック技術は、オープンシステムの傾向にある。したがって、IdM分野を指向するバイオメトリック技術は、既存のIdMアーキテクチャとの親和性のあるSOA型の技術開発が有効である。

(4) バイオメトリック技術を実装したIdMアーキテクチャの基本方式

IdMの仕様調査の対象をシングルサインオン(SSO)に適用可能な規格案であるOpenID、Liberty Allianceの技術的調査結果から考えると、両者の認証部分にバイオメトリック認証を追加することで、他へのシステム的な影響を最小限として組込みが可能との見込みを得た。

並行して国際標準SC37の関連規格を調査したところ、BioAPI、BIPと提案されている

BIAS 規格案を修正するとともに、端末側に新しい機能を追加することで、IdM システムにバイOMETリック認証を組み込むアーキテクチャの基本方式に適用できる可能性が高いと考えている。ただし、バイOMETリクス技術の多様性や精度評価の仕組み、端末認証などを含んだ新しい機能を追加するなどの課題もあるため、今後の取り組みが重要であると考えている。

#### (5) IdM へバイOMETリクスを組み込む際のプライバシー問題

IdM にバイOMETリクスを組み込む場合には、以下の点を考える必要がある。

- ①生のバイOMETリックデータとテンプレートのどちらを管理するのか。
- ②テンプレートをアイデンティティ提供者やバイOMETリック認証プロバイダなどのサーバ側で管理するのか、それともユーザ側で管理するのか。
- ③テンプレートをサーバ側で管理する場合に個人情報保護法が適用されるのか。
- ④バイOMETリックデータやテンプレートがアイデンティティ提供者からバイOMETリック認証プロバイダに移転する場合にどのような問題が生じるのか。
- ⑤個人データが国境を越えて流通する場合にどのような問題が生じるのか。

これらの問題を検討する際には、以下の二つの視点が重要になる。一つは、個人情報保護法がどのように適用されるのかということであり、もう一つは、プライバシー保護の観点から、どのようなシステムが望ましいのかということである。

まず、個人情報保護法が適用される場合には、確実に法律上の要請を遵守する必要があることはいうまでもない。これに対して、プライバシー保護の観点からどのような対策が望ましいのかについては、微妙な判断が必要とされる。本検討では、主としてプライバシー保護の観点に重点を置いて検討してきたが、実際に IdM にバイOMETリクスを組み込んだシステムを開発し、普及させる際には、プライバシー保護の要請だけではなく、ユーザの利便性や、セキュリティ対策の程度など、様々な要素を総合的に考慮する必要があるであろう。その上で、どのようなシステム構成を採用するのかをケースバイケースで判断することが重要であると考えられる。

なお、シングルサインオンを用いた IdM にバイOMETリクスを組み込む場合、アイデンティティ提供者（あるいはバイOMETリック認証プロバイダ）に、ユーザに関する氏名、住所などの属性情報、テンプレート、ID/PW などの認証情報が集中しやすいところがある。したがって、アイデンティティ提供者は、これらの情報を漏洩させないように、安全な管理を行うことが要請される。特に、OpenID の場合には、規格上誰でもアイデンティティ提供者（OP）になれるため、漏洩リスクがどの程度あるのか、ユーザ側でアイデンティティ提供者を慎重に見極めて選択する必要があるように思われる。

## 5. 調査研究の課題及び今後の展開

アイデンティティ管理の応用分野は広く、色々な視点で市場が開拓されている。このため海外では、技術を効率良く開発するためのプロジェクトや統合する組織が再編成されている。一方日本では、プロジェクト及び組織編制とも動きがない。今後、国の方針として示されている国民サービスを安全安心に行うためにも国民 ID 関係の動きと連携した先行するプロジェクトの実施が必要であると考えます。

また、バイオメトリック技術を実装した IdM アーキテクチャの基本方式とした方式案の実現のためには、以下の技術的な課題が存在する。

- ①利用者端末上で動作するアプリケーションが、バイオメトリック製品ごとのサポート機能の違いに対応しなければならない。このため、サポートするバイオメトリック装置を追加するたびにアプリケーションのロジックの変更や試験が必要となる。
- ②本システムに組み込まれるバイオメトリック製品の性能はアプリケーションの生体情報取得や認証のための処理内容に依存してしまう。したがって、同一のバイオメトリック製品を用いた場合でもアプリケーションが異なると、性能が異なる可能性がある。
- ③プライバシー情報の漏洩リスクを軽減するためにはサーバ認証のみではなく端末認証も考慮に入れることが望ましい。

今後この部分についての具体的な検討を進める必要があるため、本調査研究の課題及び今後の展開として、次の事があると考えている。

- ①バイオメトリクスを組み込んだ IdM アーキテクチャとして、望ましいシステム構成を実現するために必要な技術開発プロジェクトの実施。
- ②本成果を基とした、既存あるいは現在審議中の国際標準に対する修正と新規標準の開発プロジェクトの実施。
- ③国民サービスの一つである国民 ID 関係の動きに本成果を適用することで安全安心な IdM システムとなることを示すための実証実験プロジェクトの実施。

## [参 考 文 献]

4 - 1

- [1] 吉澤亨史：アイデンティティ管理市場が急拡大、HP と CA が高いシェア、  
C-NET Japan、2008 年 6 月 <http://japan.cnet.com/news/sec/20375006/>
- [2] 藤巻信之：国内のアイデンティティ管理市場、 日経データボード、2009 年 9 月  
<http://databoard.nikkeibp.co.jp/article/databd/20100617/104190/>
- [3] 高橋健司： アイデンティティ管理の現状と今後、 電子情報通信学会誌 2009
- [4] Identity and Access Management Market Forecast to 2012  
RNCOSE-services Pvt. Ltd., 2009 年
- [5] 榎並利植：共通番号（国民 I D）のすべて、東洋経済新報社、2010 年 12 月
- [6] 情報セキュリティ政策会議  
政府機関の情報セキュリティ対策のための統一基準（第 4 版）（平成 21 年度修正）、2010 年  
<http://www.nisc.go.jp/active/general/pdf/K303-091.pdf>
- [7] National Institute of Standards and Technology  
FIPS PUB 201-1 Personal Identity Verification（PIV） of Federal Employees and  
Contractors 2006 年  
<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>
- [8] National Science and Technology Council  
Identity Management Task Force Report 2008 2008 年  
<http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf>
- [9] @IT 情報マネジメント用語辞典 アイデンティティ管理  
<http://www.atmarkit.co.jp/aig/04biz/idm.html>
- [10] 財団法人日本規格協会 情報技術標準化研究センター アイデンティティ管理技術の標準化調査  
研究成果報告書 2009 年  
[http://www.jsa.or.jp/stdz/instac/syokukai/H20\\_houkoku/H20annual-report/02\\_02.pdf](http://www.jsa.or.jp/stdz/instac/syokukai/H20_houkoku/H20annual-report/02_02.pdf)
- [11] 特集 最新&定番の認証技術、pp.23-27、日経ネットワーク、2009.10
- [12] 社団法人 電子情報技術産業協会 セキュア・プラットフォーム推進コンソーシアム  
平成 21 年度「セキュア・プラットフォームに関する技術動向」調査報告書（統合アクセス制御  
編） 2010 年  
[http://spf.jeita.or.jp/library\\_files/22-100331/22-100331-3.pdf](http://spf.jeita.or.jp/library_files/22-100331/22-100331-3.pdf)
- [13] 日本 HP HP IceWall Identity Manager とは  
<http://h50146.www5.hp.com/products/software/security/icewall/im/feature.html>
- [14] Liberty Alliance  
<http://www.projectliberty.org/>

- [1] ISO/IEC JTC 1/SC 37 Biometrics ISO/IEC PDTR TR29144 2009 年
- [2] ISO/IEC JTC 1/SC 37 ISO/IEC WD 24760 2009 年
- [3] 社団法人情報処理学会 報規格調査会 広報委員会 2008 年度専門委員会関係活動報告  
<http://www.itscj.ipsj.or.jp/newsletter/82-2.pdf>
- [4] 社団法人日本自動認識システム協会 BSC 会  
 ISO/IEC JTC 1/SC 37 (バイオメトリクス) シンガポール会議報告 2010 年  
<http://www.bsc-japan.com/pdf/20100118-22/01.pdf>
- [5] ISO/IEC 24761:2009  
[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=41531](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41531)
- [31] 財団法人日本規格協会 情報技術標準化研究センター アイデンティティ管理技術の標準化調査  
 研究成果報告書 2009 年  
[http://www.jsa.or.jp/stdz/instac/syokukai/H20\\_houkoku/H20annual-report/02\\_02.pdf](http://www.jsa.or.jp/stdz/instac/syokukai/H20_houkoku/H20annual-report/02_02.pdf)
- [6] ISO/IEC JTC 1/SC 37 N 3946  
 Proposal for a New Work Item on Biometric identity assurance services (BIAS)  
 本文書は ISO の N-Documents 検索ページ (<http://isotc.iso.org/livelink/livelink>) で検索し、入手することができる。
- [15] Duane Blackburn NSTC Activities in Biometrics and Identity Management 2008 年  
<http://www.biometrics.gov/Documents/Blackburn%20-%20IdM%20and%20Biometrics%20for%20ITAA.pdf>
- [16] Duane Blackburn National Science and Technology Council Task Force on Identity Management 2008 年  
<http://www.biometrics.gov/Documents/Blackburn%20-%20ITAA%20Oct%202008.pdf>
- [17] National Strategy for Trusted Identities in Cyberspace Draft 2010 年 6 月  
[http://www.dhs.gov/xlibrary/assets/ns\\_tic.pdf](http://www.dhs.gov/xlibrary/assets/ns_tic.pdf)
- [18] Fact Sheet for National Strategy for Trusted Identities in Cyberspace  
<http://www.whitehouse.gov/the-press-office/fact-sheet-national-strategy-trusted-identities-cyberspace>
- [19] Jean Camp : Identity Management's Misaligned Incentives  
 IEEE security & privacy, PP.90-95, Vol8, No6, 2010
- [7] Primelife <http://www.primelife.eu/>
- [8] PICOS <http://www.picos-project.eu/>
- [9] SWIFT <http://www.ist-swift.org/>
- [10] FIDIS <http://www.fidis.net/>
- [11] PRIME <https://www.prime-project.eu/>

- [12] GUIDE <http://www.guide-project.org/>
- [13] The TURBINE Project <http://www.turbine-project.org/>
- [14] TURBINE: Trusted revocable biometric identities  
Biometric Technology Today , February 2009, p.8-p.10
- [20] European Identity Conference 2009 <http://www.kuppingercole.com/events/eic2009>
- [21] IDM2010 <http://www.idm2010.co.uk/>
- [22] Identity Management 2010 <http://events.oasis-open.org/home/IDM/2010>
- [23] Gartner Identity & Access Management Summit A Post-Event Snapshot  
[http://www.gartner.com/it/content/502200/502298/2006iam\\_final.pdf](http://www.gartner.com/it/content/502200/502298/2006iam_final.pdf)
- [24] Gartner Identity & Access Management Summit (2010 年)  
<http://www.gartner.com/technology/summits/na/identity-access/index.jsp>
- [25] Gartner Identity & Access Management Summit (2011 年)  
<http://www.gartner.com/technology/summits/emea/identity-access/index.jsp>
- [26] Identity Management for National Defense  
<http://www.iqpc.com/ShowEvent.aspx?id=189628&langtype=1033>
- [27] 2010 Biometric Consortium Conference & Technology Expo  
<http://www.biometrics.org/bc2010/>
- [28] Biometrics2011 <http://www.biometrics.elsevier.com/index.htm>
- [29] 特定非営利活動法人日本ネットワークセキュリティ協会  
内部統制におけるアイデンティティ管理解説書 (第2版) 2009年6月  
<http://www.jnsa.org/result/2008/pol/idm/index.html>
- [30] 独立行政法人 情報処理推進機構  
情報セキュリティ技術動向調査 (2008 年上期) 2008 年 10 月  
<http://www.ipa.go.jp/security/fy20/reports/tech1-tg/index1.html> (HTML 版)  
<http://www.ipa.go.jp/security/fy20/reports/tech1-tg/documents/tech-1-2008a042.pdf>
- [32] カンタラー・イニシアティブ・技術セミナー2010  
<http://kantarainitiative.org/confluence/display/WGJ/Kantara+Initiative+Tech+Seminar+2010>
- [33] OpenID Tech Night Vol.6  
<http://www.openid.or.jp/modules/news/details.php?bid=30>

- [34] インターネット勉強会：オープンガバメント時代の国民 ID 制度を考える vol.1  
<http://www.openid.or.jp/modules/news/details.php?bid=31>  
インターネット勉強会：オープンガバメント時代の国民 ID 制度を考える vol.2  
<http://www.openid.or.jp/modules/news/details.php?bid=32>  
インターネット勉強会：オープンガバメント時代の国民 ID 制度を考える vol.3  
<http://www.openid.or.jp/modules/news/details.php?bid=33>  
インターネット勉強会：オープンガバメント時代の国民 ID 制度を考える vol.4  
<http://www.openid.or.jp/modules/news/details.php?bid=36>
- [35] 情報処理技術セミナー（旧称：情報処理軽井沢セミナー）  
<http://www.nii.ac.jp/hrd/ja/joho-karuizawa/index.html>
- [36] 学術認証フェデレーションシンポジウムの開催（3月7日（月））  
<https://www.gakunin.jp/docs/node/431>
- [37] コンピュータセキュリティシンポジウム 2010  
<http://www.iwsec.org/css/2010/>
- [38] SCIS2011（暗号と情報セキュリティシンポジウム） <http://www.scis2011.jp/>  
2011 予稿集、2011
- [39] 共通番号制度と国民 ID 時代に向けたプライバシー・個人情報保護法制のあり方 <課題と提言  
>第3回 シンポジウム  
<http://www.horibemasao.org/>
- [40] 株式会社 NTT データ  
NTT DATA DIGITAL GOVERNMENT メールマガジン 2010年7月9日号  
[http://e-public.nttdata.co.jp/f/repo/710\\_m100709/m100709.aspx](http://e-public.nttdata.co.jp/f/repo/710_m100709/m100709.aspx)
- [41] Kenta Takahashi : Cancelable Finger Vein Authentication as a Cloud Service、ABC  
Malaysia Conference、2010. 12
- [42] 日本自動認識システム協会 IdM 研究会における井上春樹氏の資料、2010年9月3日
- [43] @IT ネットワーク用語辞典 LDAP  
<http://www.atmarkit.co.jp/aig/06network/ldap.html>

- [1] バイオメトリクスに関するプライバシー・個人情報保護の問題については、社団法人日本自動認識システム協会『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年度経済産業省基準認証研究開発事業報告書（2005）、新保史生「個人情報保護法に基づくバイオメトリクスの利用」情報メディア研究第4巻第1号（2006）55頁、村上康二郎「バイオメトリクスに関する法的諸問題」情報ネットワーク・ローレビュー第4巻第2号（2005）74頁、同「生体認証技術とプライバシー・個人情報の保護」『プライバシー影響評価PIAと個人情報保護』（中央経済社、2010）103頁以下など参照。
- [2] プライバシー権については、多数の書籍が存在するが、代表的なものとして以下を参照。戒能通孝＝伊藤正巳編『プライバシー研究』（日本評論社、1962）、伊藤正巳『プライバシーの権利』（岩波書店、1963）、堀部政男『現代のプライバシー』（岩波書店、1980）、同『プライバシーと高度情報化社会』（岩波書店、1988）、榎原猛編『プライバシー権の総合的研究』（法律文化社、1991）、堀部政男編『情報公開・プライバシーの比較法』（日本評論社、1996）、竹田稔『[増補改訂版] プライバシー侵害と民事責任』（判例時報社、1998）、新保史生『プライバシーの権利の生成と展開』（成文堂、2000）、船越一幸『情報とプライバシーの権利』（北樹出版、2001）、竹田稔＝堀部政男編『名誉・プライバシー保護関係訴訟法』（青林書院、2001）、田島泰彦＝山野目章夫＝右崎正博編著『表現の自由とプライバシー』（日本評論社、2006）、石井夏生利『個人情報保護法の理念と現代的課題』（勁草書房、2008）、升田純『現代社会におけるプライバシーの判例と法理』（青林書院、2009）堀部政男編『プライバシー・個人情報保護の新課題』（商事法務、2010）、佃克彦『プライバシー権・肖像権の法律実務（第2版）』（弘文堂、2011）など。
- [3] 佐藤幸治『憲法（第三版）』（青林書院、1995）453頁、樋口陽一ほか『注釈日本国憲法上巻』（青林書院、1984）290頁以下〔佐藤幸治執筆〕、佐藤幸治「プライバシーの権利（その公法的側面）の憲法論的考察（一）」法学論叢86巻5号（1970）1頁。
- [4] 芦部信喜『憲法学Ⅱ人権総論』（有斐閣、1994）378頁以下。
- [5] 前田陽一「大学主催の講演会に参加を申し込んだ学生のプライバシーの侵害」平成15年度重要判例解説(2004)90頁、飯塚和之「取引法判例研究260」NBL806号(2005)52頁など。
- [6] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- [7] 訳文は、岡村久道『個人情報保護法（新訂版）』（商事法務、2009）22頁を参照。
- [8] OECD: The 30th Anniversary of the OECD Privacy Guidelines,  
(<http://www.oecd.org/sti/privacyanniversary>) .
- [9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.



- [29] 財団法人日本規格協会情報技術標準化研究センター『平成 21 年度アイデンティティ管理技術標準化調査研究成果報告書』（2010） 47 頁  
〈[http://www.jsa.or.jp/stdz/instac/syukai/H21\\_houkoku/h21annual-report/02\\_02.pdf](http://www.jsa.or.jp/stdz/instac/syukai/H21_houkoku/h21annual-report/02_02.pdf)〉。
- [30] 財団法人日本規格協会情報技術標準化研究センター『平成 20 年度アイデンティティ管理技術標準化調査研究成果報告書』（2009） 26 頁以下  
〈[http://www.jsa.or.jp/stdz/instac/syukai/H20\\_houkoku/H20annual-report/02\\_02.pdf](http://www.jsa.or.jp/stdz/instac/syukai/H20_houkoku/H20annual-report/02_02.pdf)〉。
- [31] ACBio については、財団法人日本規格協会情報技術標準化研究センター・前掲注(30)26 頁以下参照。
- [32] BIAS については、4－3 を参照。
- [33] もっとも、この ISO/IEC 29144 は、まだ 5th WD ということもあり、不十分な点が多い。
- [34] 4－3 を参照。
- [35] 村上・前掲注(1)「生体認証技術とプライバシー・個人情報の保護」116 頁以下など参照。
- [36] EU 個人データ保護指令 25 条への対応については、『国際移転における企業の個人データ保護措置調査報告書』（2010）〈<http://www.caa.go.jp/seikatsu/kojin/H21report1a.pdf>〉などを参照。

システム技術開発調査研究 22-R-6

アイデンティティ・マネジメントへの  
バイオメトリクス組み込み時の課題と  
海外動向、標準化動向に関する調査研究

(要旨)

平成 23 年 3 月

作 成 財団法人機械システム振興協会  
東京都港区三田一丁目 4 番 2 8 号  
TEL 03-3454-1311

委託先名 社団法人日本自動認識システム協会  
東京都千代田区岩本町 1-9-5  
FK ビル 7 階  
TEL 03-5825-6651