

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

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
第1章 IdMアーキテクチャの分析調査	5
1.1 アイデンティティ管理とは何か	5
1.1.1 アイデンティティ管理の市場規模	5
1.1.2 アイデンティティ管理の定義	8
1.1.3 位置付けと分類	10
1.1.4 アイデンティティ管理をどこで行うか	14
1.2 アイデンティティ管理技術の分類	16
1.2.1 IT内部統制応用	16
1.2.2 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	20
1.3 まとめ	29
第2章 国内外の標準化及び学会活動状況	31
2.1 国際標準の状況	31
2.2 欧米の状況	35
2.2.1 米国	35
2.2.2 欧州	41
2.2.3 欧米におけるアイデンティティ管理に関するカンファレンス	46
2.3 日本国内の状況	51
2.3.1 プロジェクト	51
2.3.2 学会研究会など	52
2.3.3 企業、大学における開発	56
2.4 まとめ	58
第3章 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	62
3.1 検討の進め方	62
3.1.1 基本方針	62
3.1.2 関連する国際標準規格	64
3.1.3 検討方針	65
3.2 IdMアーキテクチャの技術調査	66

3.2.1	Webアプリ応用型.....	66
3.2.2	内部統制応用型.....	74
3.3	国際規格技術調査.....	75
3.3.1	BioAPI規格.....	76
3.3.2	BIP規格.....	79
3.3.3	BIAS規格.....	81
3.4	方式検討結果.....	90
3.5	方式案の考察.....	92
3.6	今後の課題.....	93
第4章	プライバシー保護の課題の明確化とその対策について.....	94
4.1	問題の所在.....	94
4.2	プライバシー権と個人情報保護法制.....	94
4.2.1	プライバシー権.....	94
4.2.2	個人情報保護法制.....	97
4.3	バイオメトリクスに関するプライバシー.....	102
4.3.1	バイオメトリクスに関するプライバシー問題の発生.....	102
4.3.2	バイオメトリクスとプライバシー権.....	103
4.3.3	バイオメトリクスと個人情報保護法制.....	105
4.4	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.....	113
4.4.1	シングルサインオンを用いたIdMのプライバシー問題.....	113
4.4.2	SAMLとプライバシー.....	114
4.4.3	OpenIDとプライバシー.....	115
4.4.4	プライバシー保護に関する残された課題.....	116
4.5	IdMへバイオメトリクスを組み込む際のプライバシー.....	117
4.5.1	IdMへバイオメトリクスを組み込む際の課題.....	117
4.5.2	IdMへバイオメトリクスを組み込む際のプライバシー問題.....	118
4.	調査研究の成果 (まとめ).....	123
5.	調査研究の課題及び今後の展開.....	126

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。

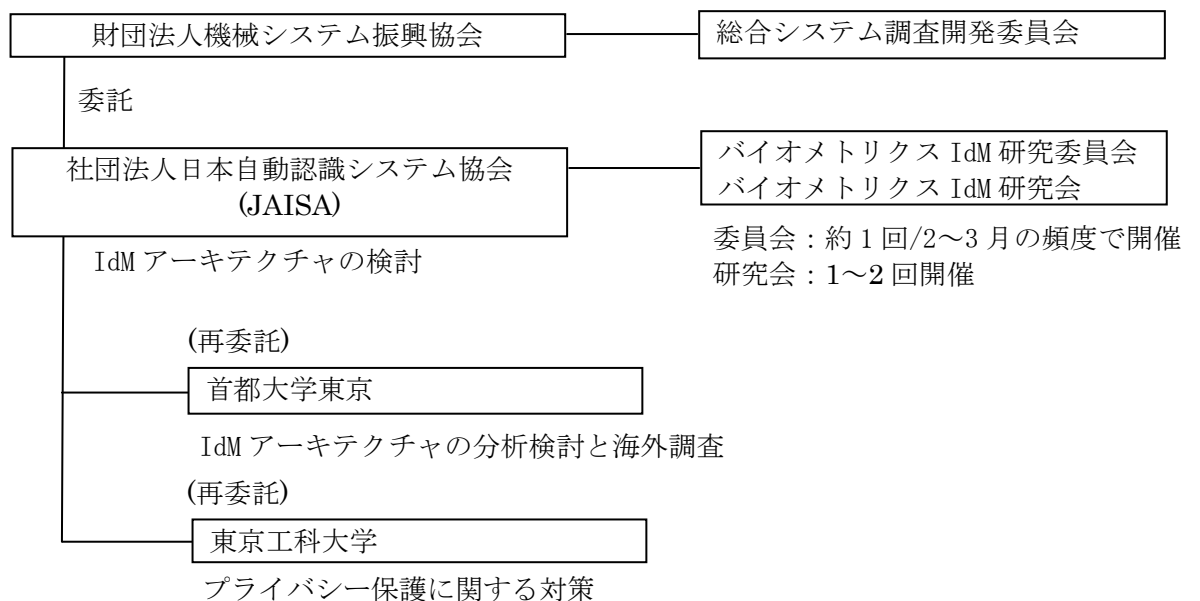
バイオメトリック技術を IdM に導入するには、IdM に関する最新の技術や標準化の動向を調査し、IdM アーキテクチャを明確にすることが必要である。また、バイオメトリック技術を実装するためのアーキテクチャを明確にし、個人の究極の情報であるバイオメトリクスを利用することにより新たに生じるプライバシー問題を明確にし、その対策について検討する必要がある。

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	JALISA 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。

S C 3 7 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。

第1章 IdMアーキテクチャの分析調査

1.1 アイデンティティ管理とは何か

1.1.1 アイデンティティ管理の市場規模

日経データボード「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、日本国内のアイデンティティ管理市場は近年拡大しており、図 1.1.1 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]。

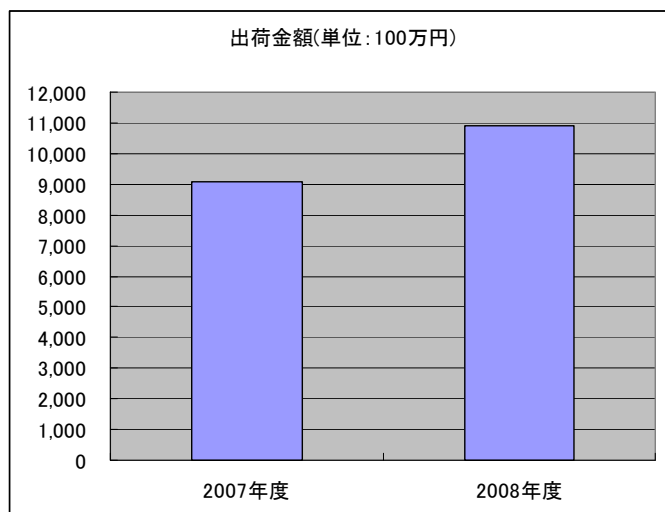


図 1.1.1 日本国内のアイデンティティ管理市場規模の予測推移

また、世界のアイデンティティ管理市場は、図 1.1.2 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]。

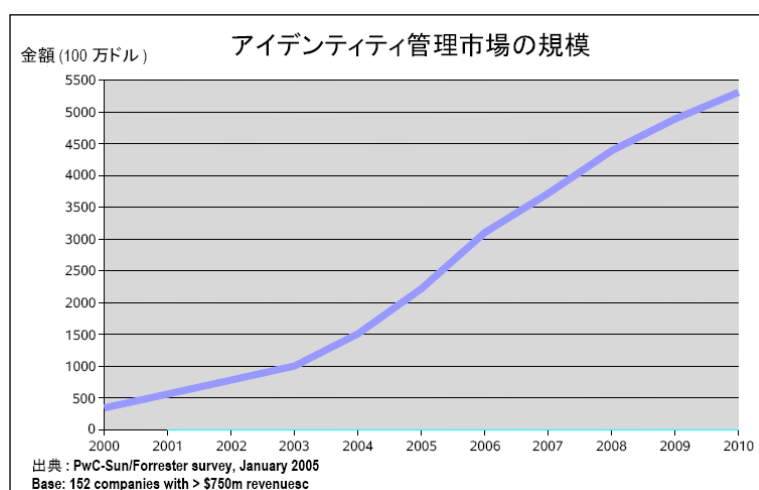


図 1.1.2 世界のアイデンティティ管理市場規模の予測推移

また、2008年の市場における各技術分野のシェアを図1.1.3に示す[4]。

- 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%

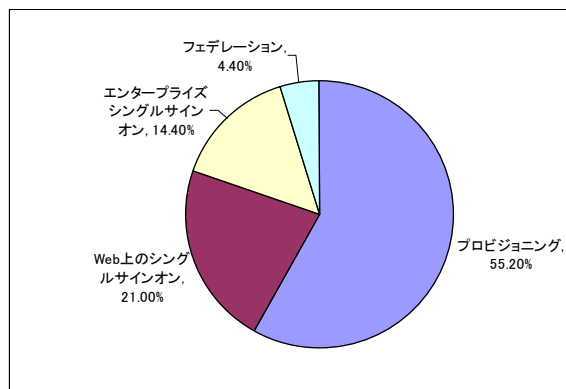


図 1.1.3 技術分野ごとの市場シェア

プロビジョニングとは、「ルールに基づき、ユーザ管理、ロールアサイン、認可管理を実施した結果を関連する全システムに反映し、適正なアイデンティティ管理環境を維持する技術」である。

例えば、ユーザのアクセス権限を変更する場合、アクセス要求承認を行うことが考えられる。

組織のビジネスポリシー及びアクセス要求の承認プロセスをワークフローとして定義して、アイデンティティ管理システムに実装することにより正確で迅速な処理を実現できる。ワークフローは、何らかの要求を正しい承認者に送付して、承認がなされると直ちにプロビジョニングが実行されるという手法である。実行者の役割（ロール）や責任に基づくことからロールベースのワークフローと呼ばれる場合がある。

この技術は情報の不正利用防止に不可欠な技術であるため、特に会計情報や個人情報を取り扱う業務分野でのニーズが高い。エンタープライズシングルサインオンは主に企業内の複数システムに単一のID、パスワードでログインするための製品群を指す。

フェデレーションとは、「イントラネットを超えて他社のシステムやアプリケーション、サービスとの間でSSOやWebサービスの処理結果を他のサービスに受け渡す技術、もしくはそれを実現する考えのこと」である。例えば、異なる企業の社内部署、外部ビジネスパートナー、他のサードパーティにまたがって、あたかも全てが同じセキュリティドメインに属しているかのようにユーザやアプリが作業を行えるようにするのがフェデレーションである。

上述したように、アイデンティティ管理製品市場は、現在、世界では50億米ドル、年20%の成長率であり、IT業界では有望な市場である。

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。

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ことにあると考えられる。

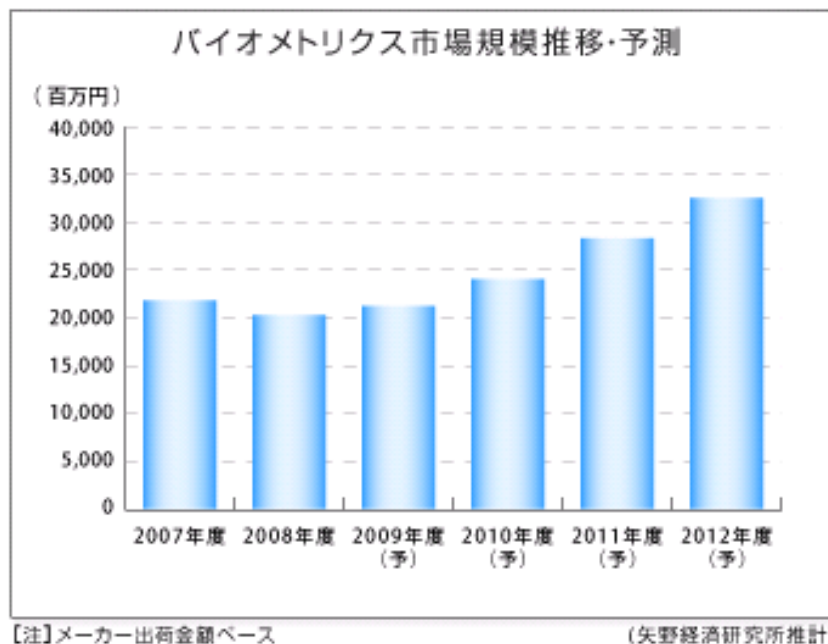


図 1.1.4 日本国内のバイオメトリック市場予測(2009年時点)

以上のように、アイデンティティ管理の市場は、日本国内、海外ともに、順調な伸びを示しているが、日本国内のバイオメトリクス市場は低迷している。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られると思われる。そのためには、アイデンティティ管理などの分野で新たな製品体系を整える必要がある [5]。

1.1.2 アイデンティティ管理の定義

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）」（以下、「政府統一基準」という。）の用語定義では「アイデンティティ」あるいは「アイデンティティ管理」についての記述は存在しない[6]。

しかし、「識別」、「識別コード」について次のように記述されている。

- ・「識別」とは、情報システムにアクセスする主体を特定することをいう。
- ・「識別コード」とは、主体を識別するために、情報システムが認識するコード（符号）をいう。
代表的な識別コードとして、ユーザ ID が挙げられる。

上記で言及されている「主体」については次のように記述されている。

「主体」とは、情報システムにアクセスする者や、他の情報システム及び装置などをいう。主体は、主として、人である場合を想定しているが、複数の情報システムや装置が連動して動作する場合には、情報システムにアクセスする主体として、他の情報システムや装置も含めるものとする。

FIPS201-1（Federal Information Processing Standardization）では、Identity Management System（IdMS）を次のように説明している[7]。

“Identity management system comprised of one or more systems or applications that manages the identity verification, validation and issuance process.”（IdMSは、アイデンティティ証明、検証、保証プロセスを管理する一つ以上のシステムあるいはアプリケーションから構成される。）

NSTC レポートでの説明は以下のとおりである[8]。

“The combination of technical systems, rules and procedures that define the ownership, utilization, and safeguard of personal identity information. The primary goal of the Identity Management process is to assign attributes to a digital identity, and to connect that identity to an individual.”（個人のアイデンティティ情報の所有、使用を規定し、保護する技術システム、規則、手続きの組み合わせ。アイデンティティ管理プロセスの主要な目的はデジタルアイデンティティに属性を付与し、特定の個人に結びつけることである。）

以上より、アイデンティティ管理の定義としては、

「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

とである[9] [10]。

図 1.1.5 にライフサイクルのモデルをまとめ、表 1.1.1 に各プロセスの詳細をまとめる。

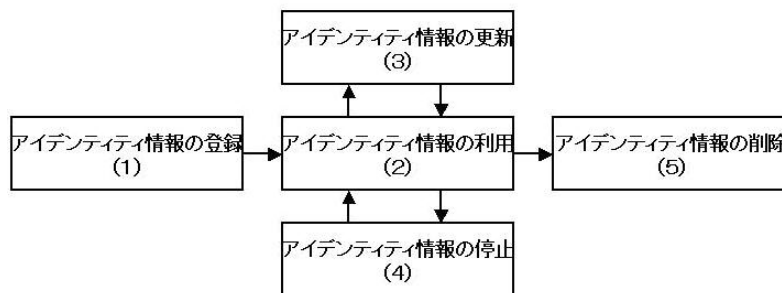


図 1.1.5 ライフサイクルモデル

表 1.1.1 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 に紐づ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づく情報（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 に紐づく情報（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 1.1.2 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 1.1.2 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"> ・アカウント名 ・メールアドレス ・保険証番号、運転免許証番号 ・社員番号、学生番号 ・電話番号
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"> ・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 ・国籍を示す電子パスポート
属性	アイデンティティを特徴付ける情報	<ul style="list-style-type: none"> ・氏名 ・住所 ・生年月日 ・所属、役職 ・信用情報 ・人間関係 など

1.1.3 位置付けと分類

(1) 内部統制における位置付け

内部統制から考慮したアイデンティティ管理の効果は、以下の二つが考えられる[11][12]。

- ・ 予防的統制： アイデンティティ情報を追加・変更・削除すること（ユーザに対しては職務内容に応じてアクセス権限を付与・はく奪すること＝ユーザプロビジョニング）の統制が有効に働き、内部統制に役立つことが期待される。
- ・ 発見的統制： 各システムに格納されているアイデンティティ情報を確認・修正を行うことにより、セキュリティ・内部統制上の脆弱性やリスクを軽減することが期待される。

(2) 認証技術からの分類

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図 1.1.6 に示すように四つに分類できる[13]。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。

・ ローカル認証

アクセス元、情報リソース、認証メカニズムが一つにまとまったスタンドアロン環境で使用、ネットワークは介在しない。

- ・直接認証

アクセス元とそれ以外が LAN 経由で接続する。認証メカニズムと情報リソースは同じ筐体に収納されている。

- ・間接認証

三つの要素は分散しており、ネットワークで接続している。認証メカニズムと情報リソースの提供者は別々の可能性がある。現在の認証システムの主流である。Web 上の認証は主に間接認証で行われる。

- ・オフライン認証

電子証明書使用のサーバ認証で多く採用されている。配布された電子証明書を使用することにより、オフライン状態でもアクセス元だけで自律して認証可能である。

認証方式	認証システム構成	認証技術例
ローカル認証	<p>①アクセス元 ②情報リソース ③認証メカニズム</p>	バイオメトリクス 固定パスワード マトリックス スマートカード ワンタイムパスワード MACアドレスなど
直接認証	<p>①アクセス元 ②情報リソース ③認証メカニズム</p>	OpenIDのWebサイト 認証 IEEE802.1認証 SSL認証 ARP認証など
間接認証	<p>①アクセス元 ②情報リソース ③認証メカニズム</p>	OpenIDのWebサイト 認証 IEEE802.1認証 SSL認証 ARP認証など
オフライン認証	<p>①アクセス元 ②情報リソース ③認証メカニズム 電子証明書</p>	PKI

図 1.1.6 認証の実現方式

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。

(3) 間接認証のアーキテクチャ

内部統制対応の ID 管理は、主に管理面からのセキュリティと経済性を求めるものであった。しかし、近年ネットビジネスが拡大すると、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、管理が適正でないセキュリティ的な問題が発生するようになった。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。アイデンティティの観点から解決を図るものが SSO (Single Sign On) である。従来の SSO はローカルなシステムでの利用が目的であったが、間接認証のアーキテクチャからなるオープンシステムでのサービスが実現された。

具体的な実現方法は以下のとおりである。図 1.1.7 により説明する。

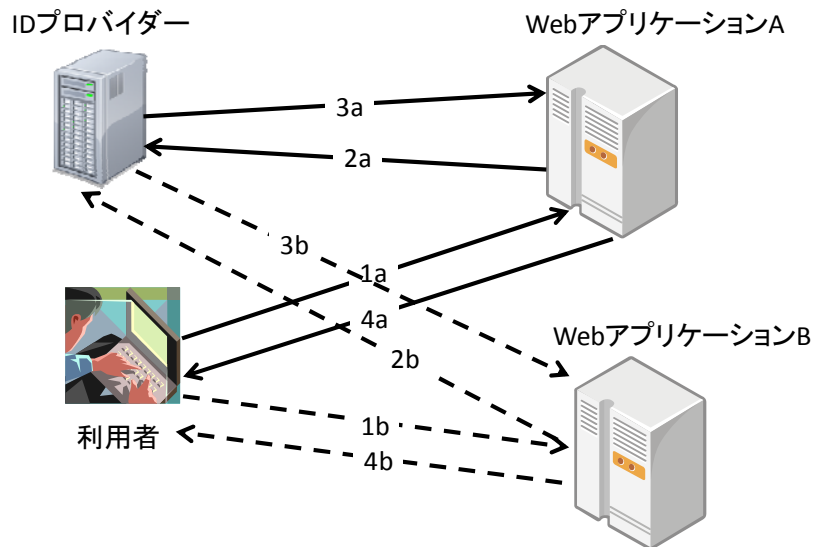


図 1.1.7 SSO の基本的な間接認証アーキテクチャ

ステークホルダーは、Web アプリケーションの利用者、Web アプリケーション、つまりサービスを提供するサービス提供者（サービスプロバイダー）、利用者のアイデンティティ情報（認証情報）と基本的な属性情報を保管する ID 提供者（ID プロバイダー）である。なお、間接認証に関しては、いくつかのコミュニティで標準的なアーキテクチャが開発されている。後述する SAML（Security Assertion Markup Language）と OpenID である。サービス提供者を SAML では Service Provider、OpenID では Relying Party、また、ID 提供者をそれぞれ ID Provider、OpenID Provider と呼んでいる。

処理の流れは以下のとおりである。

- 1a：利用者は、サービス提供者（Web アプリケーション）にサービス提供要求する。
- 2a：利用者をリダイレクトし、ID 提供者に認証を要求する。
- 3a：利用者をリダイレクトし、Web アプリケーションに認証アサーション（認証情報）を応答する。
- 4a：認証アサーションを判断して、問題なければサービスを開始する。
- 1b：別のアプリケーションにサービスを要求する。
- 2b：利用者をリダイレクトし、ID 提供者に認証を要求する。認証は 1a-4a の手続きで済んでいる。
- 3b：利用者をリダイレクトし、認証アサーションを応答する。
- 4b：認証アサーションを判断して、問題なければサービスを開始する。

認証アサーションには、基本的な属性情報を含んでいる。サービス提供者は、認証情報とともに属性情報の提供を受けて、権限の制御を行う。

(4) 応用面からの分類

アイデンティティ管理を応用面から考慮すると、大きく二つの応用に整理できる。

一つはユーザアクセス（ワークフロー）管理応用である。アイデンティティ管理をユーザアクセス（ワークフロー）管理の観点で見ると、組織の持つ IT リソースへのアクセスをユーザに提供し、それを制御することを可能にするビジネスプロセスやポリシーや技術が統合されたシステムといえる。個人やビジネス上の秘密情報を不正アクセスから守る技術と密接な関連がある。

もう一つはシングルサインオン技術（ローカルでなくオープンなシステムでの実現技術としての SSO）を中心とする Web アプリケーションである。アイデンティティ管理は適用分野が多岐にわたるため、数多くの業界団体や標準化団体が様々な目的に対し異なるアプローチで、アイデンティティ管理方式や技術仕様の策定に取り組んでいる。詳細は第 2 章で述べる。

ユーザアクセス管理は、その特性から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となっている。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、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。

前者は組織内に限定したクローズシステム、後者はインターネット上で利用されるオープンシステムといえる。

1.2 節ではアイデンティティ管理の詳細について述べる。1.2.1 項ではユーザアクセス管理の側面から、内部統制におけるアイデンティティ管理、1.2.2 項では Web 上の認証技術の側面から、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の各詳細を分析する。1.2.3 項ではクラウドコンピューティングにおけるアイデンティティ管理の例を述べる。

1.1.4 アイデンティティ管理をどこで行うか

クラウドコンピューティングの利用では、シングルサインオン(SSO)が一般的である。

これは、図 1.1.8 に示すように、サービス利用時の不安があり、個々のサービスプロバイダの認証強度にセキュリティを依存することが事実上、困難だからである。

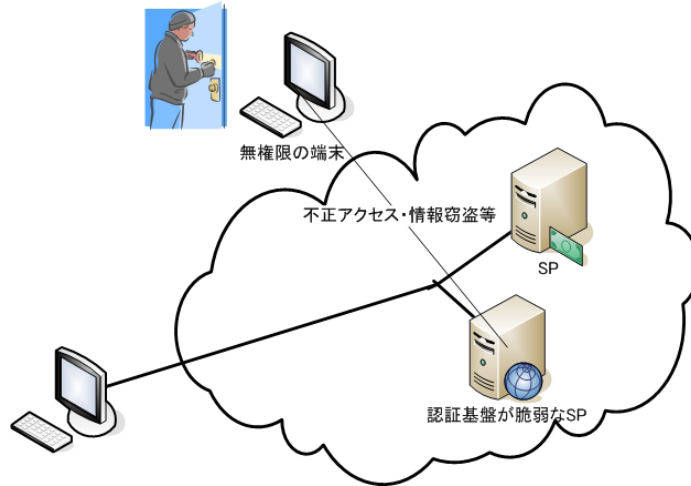


図 1.1.8 クラウドサービス利用時の不安

安全な認証の実現には、例えば、図 1.1.9 に示すように、SAML2.0 仕様のシングルサインオン(SSO)では SP からの認証要求は IdP に対して行われる。IdP を組織内部に置き、認証要求は内部 IdP に送られるように設定すれば、認証情報をクラウド上に置かずにクラウドサービスを利用することができる。

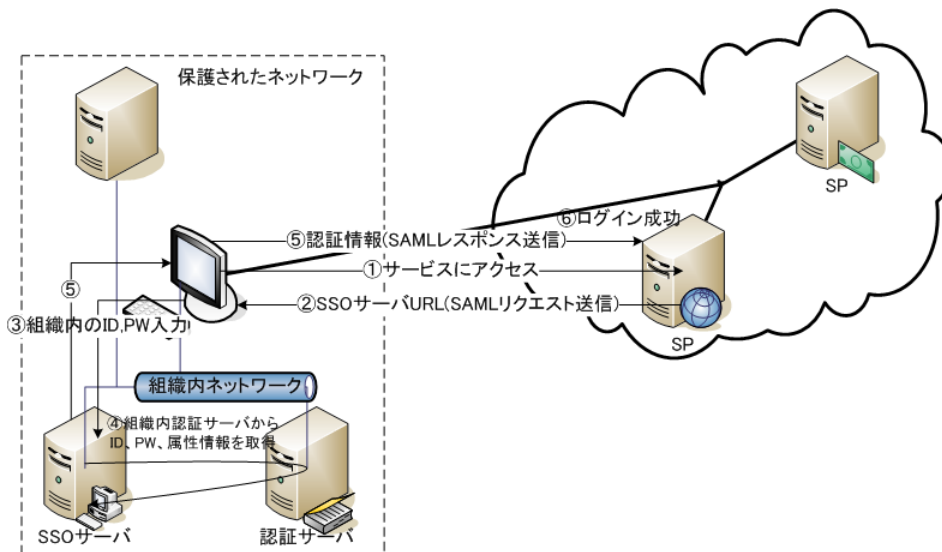


図 1.1.9 組織内認証によるクラウドサービスの利用

クラウドコンピューティングのセキュリティのためのベストプラクティスの普及を目的とする団体である CSA (Cloud Security Alliance) は、アイデンティティ及びアクセス管理のガイダンス文書でクラウド上のサービスとしてのアイデンティティ (IDaaS、 Identity as a Service) という概念を提示している[14]。アイデンティティ管理、アクセス管理をサービスとして提供することを表現する語であると考えられる。機能としてはアイデンティティ連携方式の SSO における IdP と AP の役割を兼ねたものというのがもっともイメージとしては近いと考える。

CSA ではサービスが提供する機能を次のように記述している[14]。

“The service is provided as third party management of identity and access control functions, including user life cycle management and single sign-on.” 「このサービスはユーザのライフサイクル管理と SSO を含むアイデンティティとアクセスコントロール機能の (ユーザとベンダ以外の) 第三者的な管理として提供される。」

前述のように、組織はセキュリティを重視する場合、アイデンティティ管理をできるだけ内部に囲い込もうとする。IDaaS が普及するかどうかは提供側のセキュリティ向上と、ユーザ側の取捨選択、つまり、どの程度の情報であればコストとリスクの兼ね合いで管理を外注しても良いと考えるか、に左右されると考える。

組織内で運用される内部統制応用もアイデンティティ管理は、SAML や OpenID などを実現可能である。これらのアーキテクチャは SOA (Service Oriented Architecture) にも親和性がある。したがって、SAML、OpenID などの間接認証タイプのアイデンティティ管理技術の重要性が増すと考える。

これらのアイデンティティ管理技術の認証アサーション (認証情報) は、ID、パスワードを利用している。したがって、なりすましが生じる可能性がある。ID プロバイダにおいて、バイオメトリクスを用いた認証を行えるアーキテクチャを検討する必要があると考える。

しかし、バイオメトリクスを ID プロバイダで管理する場合、バイオメトリクスは個人固有の特性であり、取り替えることのできない属性である。また、一人の人間を認証するデータ (テンプレートデータ) は、500-2,000 バイトとデータ量は大きい。このため、間接認証タイプのアイデンティティ管理にバイオメトリクスを適用することは、本人認証の安全性を高めるが、単に認証アサーションにバイオメトリック情報を管理し、認証すれば安全な認証方式を実現可能というわけではなく、十分な検討が必要であると考えられる。

1.2 アイデンティティ管理技術の分類

1.2.1 IT内部統制応用

組織におけるユーザアクセス管理は、主にワークフローなど内部統制との関連で検討しシステムが構築されている。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。

内部統制の法的背景とアイデンティティ管理の実施にあたり組織に求められる要件の詳細、アイデンティティ管理製品について、以下にまとめる。

(1) IT技術による内部統制の必要性

2006年4月から会社法の改正により全ての企業において内部統制の構築が義務付けられた。また、2006年6月に成立した金融商品取引法により、上場企業に対しては財務諸表とともに内部統制報告書の提出が、2008年4月1日以降に始まる会計年度より義務付けられている[15][16]。

内部統制応用は、法令遵守の面から進められている。現在業務のほとんどで情報システムが利用されている。情報システムなしでは業務が成り立たないだけでなく、会社活動自身が成り立たない。例えば、組織員の異動や昇進などでワークフローのアクセス管理を適正に行う必要がある。このような状況から情報システムの目的に沿った稼動を保証するための取り組みとして、IT内部統制が重要視されている。

内部統制に関する国際的な標準としてControl Objectives for Information and related Technology (COBIT) とInformation Security Management System (ISMS) がある。COBITとは、情報システムコントロール協会とITガバナンス協会が1992年に作成を開始した情報技術管理についてのベストプラクティス集(フレームワーク)である。COBITはマネージャ、監査人、ITユーザに一般に通じる尺度や判断基準、ビジネスプロセスやベストプラクティスを提供して情報技術を利用して得られる利益を最大化するための補助とし、企業内の適切なITガバナンスや内部統制の開発の補助となる。一方ISMSは、組織(企業、部、課など)における情報セキュリティを管理するための仕組み。情報セキュリティ管理システムともいう。組織の情報資産について、機密性、完全性、可用性をバランス良く維持し改善することが、情報セキュリティマネジメントシステムの基本コンセプトである。

COBITとISMSにおけるアイデンティティ管理のポイントを整理すると以下ようになる。

- ・全てのアイデンティティ管理プロセス(一般ユーザ、管理者、平常時・緊急時全てを含む)の明確化
- ・アイデンティティ管理プロセスにおける職務分離、職務の分割
- ・業務上の必要性に基づくアクセス権限の明文化とIdentifierの付与
- ・アイデンティティの作成・更新・削除のタイムリーな実施
- ・アイデンティティとアクセス権についての定期的レビュー

(2) IT内部統制におけるアイデンティティ管理システムの構成要素

ここではIT内部統制に必要となる六つの要素—①ユーザ管理、②ロールアサイン、③認可管理、④識別・認証管理、⑤プロビジョニング、⑥モニタリング—について概要を述べる[17]。

図1.2.1に組織に属するメンバーのIDの登録から削除・破棄までのライフサイクルを示す。

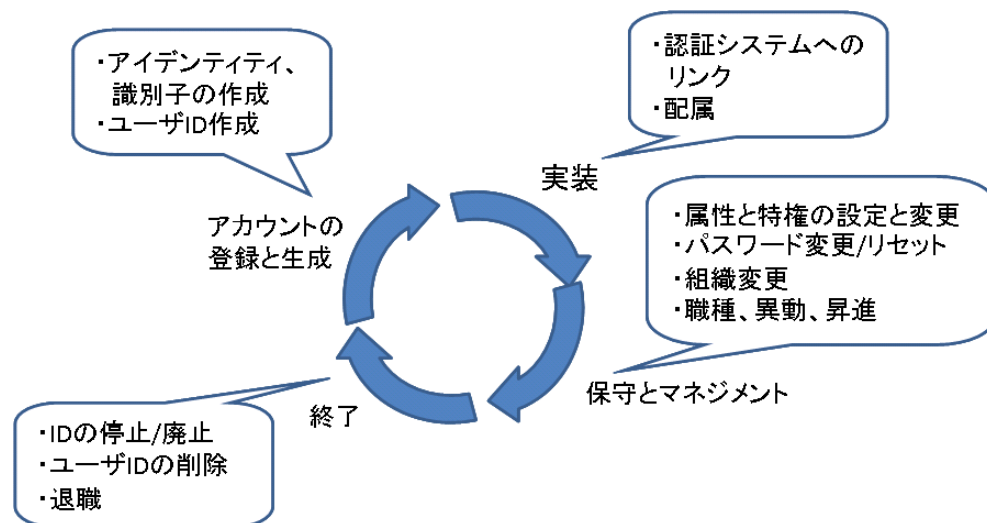


図 1.2.1 ID のライフサイクル

ユーザの新規登録から始まり、登録されたユーザへのアクセス権限の付与、変更、削除／破棄に至るまでの全ての過程が統制の対象となる。

① ユーザ管理

関係する全システムにおけるユーザ情報の正確性と完全性を保証、つまりアクセス権限が与えられるユーザの正確性を確保し、ユーザのライフサイクルを管理する。

ユーザ情報をアイデンティティ管理システムの情報源となるシステムに正確に反映するためには管理アカウントを必要最小限にするなどの管理面による統制が必要である。システムの更新内容はリアルタイムでアイデンティティ管理システムに反映し、一方で、アイデンティティ管理システムではユーザ情報を変更できないようにすることが信頼性確保の面からは望ましい。

② ロールアサイン

ユーザに対して「Need To Know」、「Least Privilege (最小権限)」、「Separation of Duties (職務権限の分離)」の原則に基づく適切なロール (役割) を割り当て (ロールアサイン)、ユーザ属性の変更をロールに正しく反映させる (上記三つの考え方の詳細は付記として記載)。

ロールアサイン・変更・削除などは規定された運用手順などにしたが、アイデンティティ管理システムで自動的に行われること、また、ロールアサインはアイデンティティ管理システムを通じてのみ実施可能とすることが信頼性確保の面からは望ましい。

③ 認可管理

業務に応じた適正なロール定義と、関係する全システムへの正確な反映を行う。またロールアサイン方針を決定する。

ロール定義権限を持つ管理者と、ロール実装権限を持つ管理者を分離すること、ロール定義の変更などに際してはロールアサイン方針を見直すことが信頼性確保の面からは望ましい。

④ 識別・認証管理

関係する全システムに対し適切な手段（ユーザ ID とパスワード、生体認証など）を用いて識別・認証を行う。またユーザの識別・認証の記録を取得しトレーサビリティを確保する。

システムの重要度に応じた識別・認証基準を適用すること、識別・認証手段に対応する適正なセキュリティ対策の採用、アクセス記録管理を行うことが信頼性確保の面からは望ましい。

⑤ プロビジョニング

プロビジョニングとは、IT リソースへのアクセス権をユーザに提供するプロセスである。具体的には、アイデンティティのライフサイクルに合わせ、図 1.2.1 のようにアカウントを実際に作成/変更/削除することを指す。

プロビジョニング・ルールはシステムで自動的に適用されることが信頼性確保の面からは望ましい。

⑥ モニタリング

システムログなどに基づき不正や異常の有無を確認する。

ID と権限の設定状況の定期的な確認、アイデンティティ管理システムによる変更やアクセス状況の定期的な監視が信頼性確保の面からは望ましい。

[付 記]

- **Need To Know** : 所属部署や職位に関係なく、自身の業務に必要なシステム資源にのみアクセスできるようにするという情報セキュリティの原則。この原則を実施するには、誰が何について、何ができなくてはいけないかをルールとして定める必要がある。このルールの規定に際しては「職務分掌の明確化」と「職務権限の分離」を前提として慎重に検討する必要がある。
- **Least Privilege (最小権限)** : データやアプリケーション処理などのシステム資源に対するユーザのアクセス権限を最小限にまで絞り込むための情報セキュリティの原則。最小限のアクセス権限は、「許可されるアクセス権限そのものを最小限に限定する」だけではなく「アクセス権限の使用時間を最小限にする」、「アクセス権限の有効期間を最小限にする」、「アクセス権限を認めるプログラムモジュールを最小限にする」、「利用できるファイルやデータを最小限にする」、「利用できる機器を最小限にする」、「利用する場所を最小限にする」など様々な意味を持つ。
- **Separation of Duties (職務権限の分離)** : **Separation of Duties** は、トランザクションや操作の一連の流れにおいて不正行為が完結しないよう、原則として「実施」、「承認」、「記録管理」、「モニタリング」といった職務を兼務させないことを念頭に置く。職務を分離することによって不正行為の実施には複数の担当者や組織が関与することになり、その実現が格段に難しくなることで、不正を減らすことができるという考え方。

(3) アイデンティティ管理製品の具体例

アイデンティティ管理製品は、国内、海外各社から出ている。これらの製品がアイデンティティ管理として提供する機能は、認証データベース上のユーザ情報へのロールベースのアクセス制御である。人事異動などによるアクセス権限変更の自動化のためのプロビジョニング機能が業務の正確さ、迅速さに寄与する。また証跡の確保により内部統制など、コンプライアンスの向上にも寄与している。しかし、シングルサインオンの実現には、複数製品の組み合わせを必要としている。

製品例として日本HPのHP IceWall Identity Managerを説明する[18]。HP IceWall Identity Managerを利用することによって複数のアプリケーションにおけるユーザが利用できる範囲をロールとして一つの認証データベースに固定することができる。図1.2.2はその例である。

図1.2.3にあるように、HP IceWall Identity Managerが担うのは認証データベース上のユーザ情報へのアクセス制御のみである。シングルサインオンを実現するには日本HPの場合には、HP IceWall SSOという製品を組み合わせている。

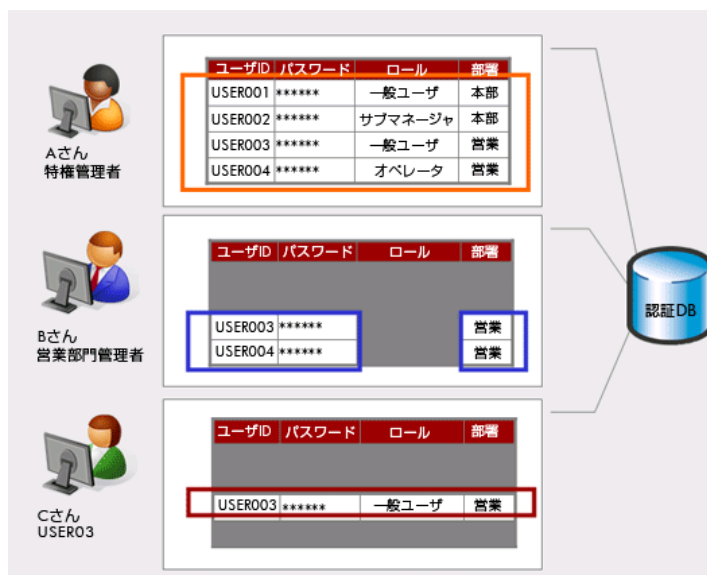


図 1.2.2 ユーザ情報の管理

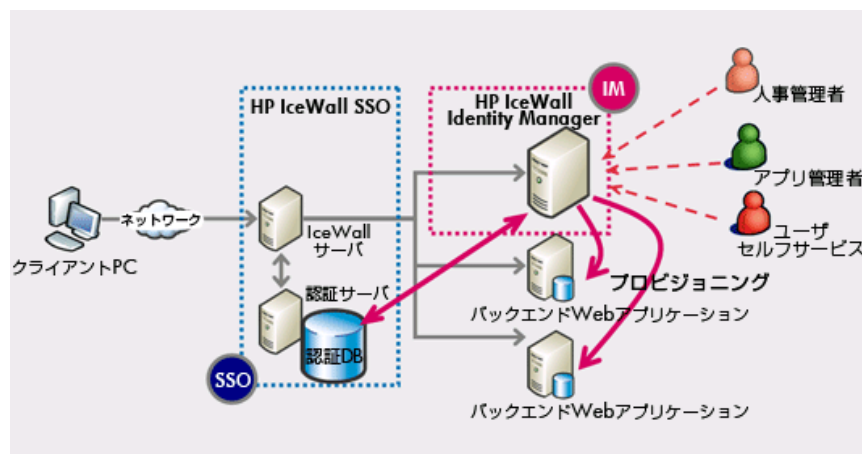


図 1.2.3 HP IceWall Identity Manager 構成

1.2.2 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

Web 上におけるアイデンティティ管理は、1.1 節で述べたように間接認証のアーキテクチャである。SSO をオープンシステム環境で実現するのが目的である。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。

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 連携技術である。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 種に大別される [3][18][19]。

・プロバイダ中心モデル

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。サポートされる主な機能はシングルサインオン、シングルサインアウト、NameID（仮 ID）、アカウント連携、属性情報交換。機能が豊富な反面、実装が課題となる。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。

・ユーザ中心モデル

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。サポートされる主な機能はシングルサインオン、属性情報交換。機能は限定されているが、実装は比較的容易とされている。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。

上記三つの方式を整理すると以下のとおりである。

(1) アイデンティティ連携方式

アイデンティティ連携方式は、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では、アイデンティティの連携状況に応じて各 SP（Service Provider）間で認証結果を共有することにより、シングルサインオンを行う。このようなシングルサインオンの仕組みを規定する代表的な技術仕様が SAML2.0 である。SAML2.0 は XML 言語で、認証、認可、属性に関する情報の表現形式及び送受信手順が定義されている。現在、国際標準化コンソーシアム OASIS（Organization for the Advancement of Structured Information Standards）の OASIS Security Services（SAML）TC が SAML2.0 の仕様を維持管理している。

また、業界団体（Liberty Alliance、現在は Kantara Initiative が活動を承継）では SAML2.0

の相互運用テストを実施している。

SAML2.0 では以下の事項を規定している。

①アサーション

ユーザ情報を記述した ID 発行事業者による証明書であるアサーションの構造と内容

②プロトコル

アサーションの要求方法と、プロトコルメッセージの XML スキーマ（構造定義）

③バインディング

SAML プロトコルメッセージを HTTP や SOAP などの通信路に載せる方法

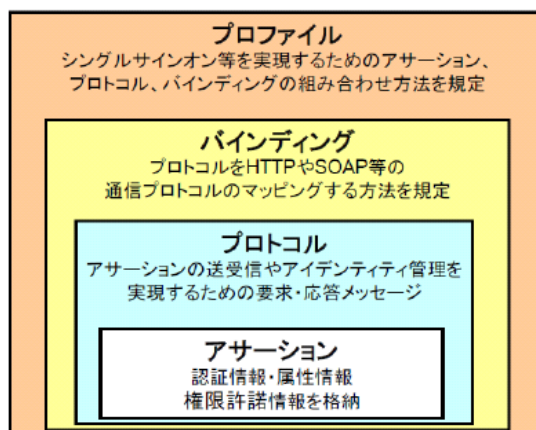
④プロファイル

SAML プロトコル、バインディング、アサーションの組み合わせ方法と Web ブラウザを利用したシングルサインオンなどのプロファイル

⑤メタデータ

シングルサインオン、ログアウトの実行方法、サービスのエンドポイント

メタデータ以外の規定事項は図 1.2.4 の構造をとっている。



出典：第一回 Liberty Alliance 技術セミナー資料

図 1.2.4 SAML 規定事項の構造[20]

アイデンティティ連携方式は一般的に、ユーザ(端末)、アイデンティティ提供者 (IdP: Identity Provider)、サービス提供者 (SP: Service Provider) から構成される[21]。フェデレーション (federation) はもともと連携を意味する英単語であるが、複数の ID 管理システムが連携して ID 管理を行うことを指して特にフェデレーションということが多い。また、連携する複数の ID 管理システムのまとまりもフェデレーションと呼ばれる。アイデンティティ連携方式を用いてユーザへのサービスを安全かつシームレスに行う IdP と SP のフェデレーションを Circle of Trust (CoT) 又は Trust Circle と呼ばれている[22]。

アイデンティティを連携する際に、仮名を用いることにより、プライバシー保護を強化することができる。

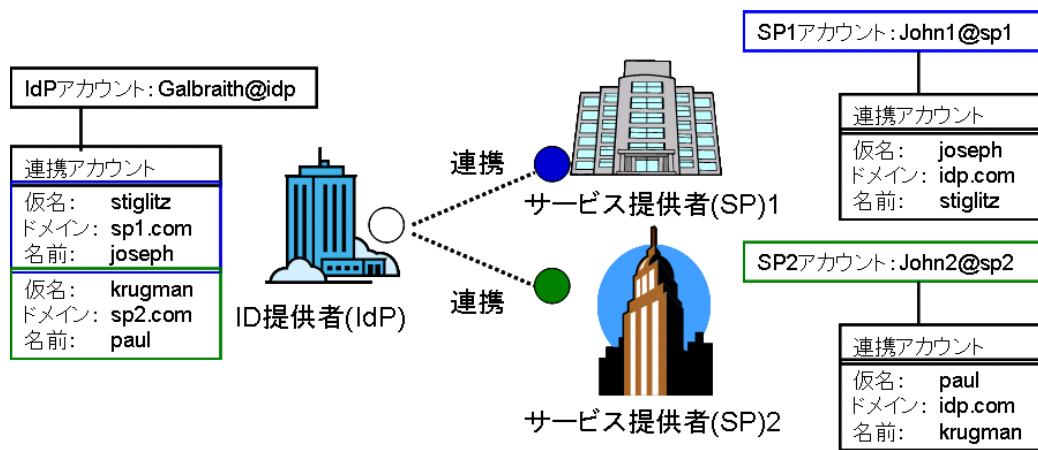


図 1.2.5 アイデンティティ連携方式のプライバシー保護

図 1.2.5 に示すように、IdP-SP の組ごとに異なる仮名を用いることにより、あるユーザが各 SP でどのようなサービスを利用したかなどの情報を収集する「名寄せ」によるプライバシー侵害や、実アカウント名の不正な流出を防止する。アイデンティティ連携方式の導入は、テレコム、企業向けシステム、電子政府などの分野で進んでいる。

アイデンティティ連携方式は、以下の手順でアイデンティティを管理する。

①複数の IdP 及び SP が、図 1.1.6 に示すトラストサークルを形成。

(ビジネスや技術面での情報交換及び合意形成。)

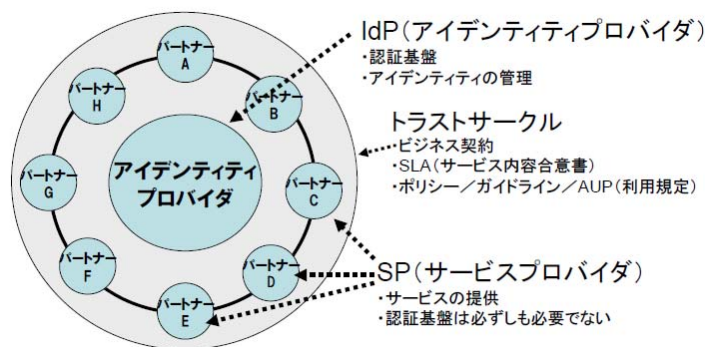


図 1.2.6 トラストサークル[19]

②ユーザがある IdP のアカウントと複数の SP (例 SP1、SP2) のアカウントとのリンクを確立。(一度確立したら (4) でリンクを解消するまでユーザ作業は不要。)

③ユーザが複数の SP にシングルサインオンや属性共有を実施する。

④ユーザがシングルサインオンした SP から一度にログアウトする。

(シングルログアウトと呼ぶ。)

⑤ユーザが確立したリンクのいくつか (もしくは全て) を削除する。

(注：ユーザの同意による自動的な各アカウントの一括リンクや、アカウントのない

サイトも一時的に利用できる仕組みなども、SAML2.0では定義されている。
参考に、図 1.2.7 に SAML プロトコルの概要を示す。)

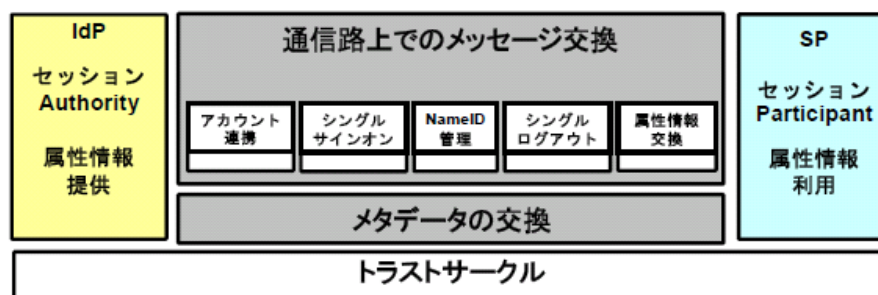


図 1.2.7 SAML プロトコルの概要[19]

日本でのフェデレーションの例としては、学術分野のフェデレーションである学術認証フェデレーションがある[23]。学術認証フェデレーションとは、学術 e-リソースを利用する大学、学術 e-リソースを提供する機関・出版社などから構成された連合体である。各機関はフェデレーションが定めた指針(ポリシー)を信頼しあうことで、相互に認証連携を実現することが可能となる。

認証連携を実現すれば、学内でのシングルサインオンを実現することが可能になるとともに、他大学や商用のサービスにおいても、一つのパスワードを利用し、かつ ID・パスワードの再入力を行わずに利用できる環境を実現可能である。例えば、他大学の無線 LAN をいつも大学で使用している ID とパスワードで利用することができ、かつ自大学が契約している電子ジャーナルヘシームレスにアクセスすることも可能となる。

学術認証フェデレーションで使用されている Shibboleth は SAML をベースとして開発されたシングルサインオンとフェデレーションを実現するシステムである[24]。

最新版の Shibboleth2.0 は SAML2.0 に対応している。

アイデンティティ連携方式と後述のアイデンティティ統一方式、アイデンティティ選択方式との大きな違いはアイデンティティ開示のイニシアティブをアイデンティティ提供者 (IdP) が握っているということである。開示ポリシーを統一し、厳守したいエンタープライズ領域、行政システムなどに向けた方式であると考えられる。

(2) アイデンティティ統一方式

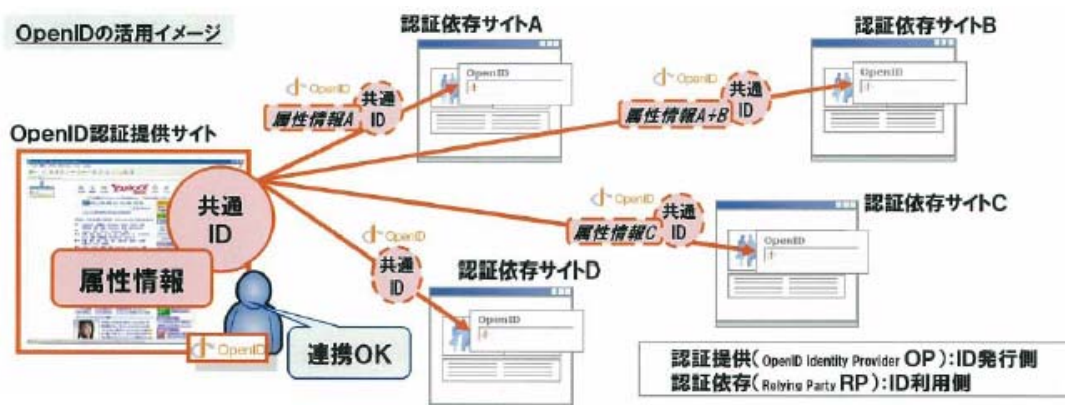
アイデンティティ統一方式とは、あるユーザが、一つの識別子で様々なサービスにアクセスする利用形態を前提にしたアイデンティティ管理方式である。この方式に対応した代表的な技術仕様として OpenID2.0 がある。

現在 OpenID2.0 仕様は米国の非営利団体 OpenID Foundation で維持管理されている。OpenID Foundation は知財管理、追加仕様の策定、技術の普及・啓発活動を連携団体の OpenID Foundation Europe などを通じてグローバルに行っている。日本国内にも OpenID 技術の普及を図る団体として一般社団法人 OpenID ファウンデーション・ジャパンが存在する。

2009年現在、世界で14億4,000万IDが発行され、50,000以上のサイトでOpenIDが利用可能となっている。

図1.2.8にOpenIDの利用イメージを示し、OpenID2.0を例にアイデンティティ統一方式の概要を解説する。

OpenID2.0に基づく方式は、一般的にユーザ（ユーザ端末）及び、アイデンティティ提供者（OP：OpenID Provider）、サービス提供者（RP：Relying Party）から構成される[25]。ユーザは、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ち、複数のRPで利用する。



出典：OpenID ファウンデーション・ジャパン資料

図 1.2.8 OpenID の利用イメージ[20]

OpenIDの識別子はユーザを識別するという本来の役割以外に、それが代表するユーザのアイデンティティ情報へのアクセス方法も示す役割を果たしている。このように役割を重複させると、ユーザ識別子（アカウント）のOP間におけるポータビリティの低下やアイデンティティ情報の分散的な配置の阻害、即ち、情報流出時の被害を大きくするなどのリスクがあるので、システムやサービス設計時にこのようなリスクを考慮する必要があると考える。

図1.2.9に、OpenID2.0のSSO処理の流れの概要を示し、合わせて処理手順を示す。

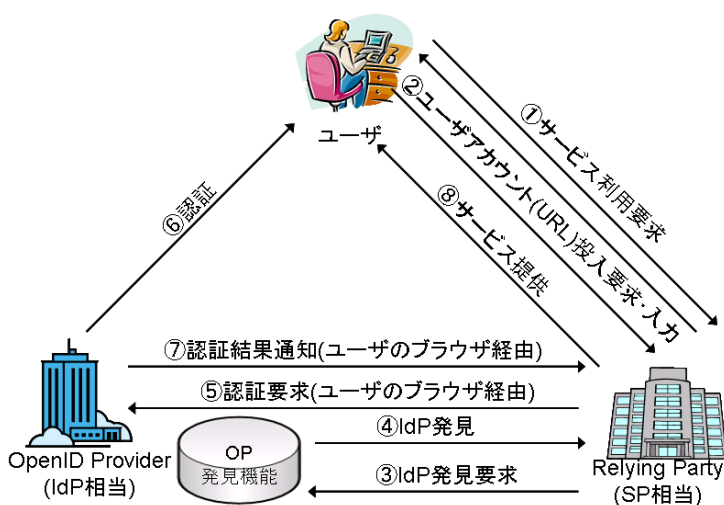


図 1.2.9 アイデンティティ統一方式におけるシングルサインオンの処理の流れ

- ①ユーザが RP にサービス利用を要求する。
- ②RP は、まだユーザの認証をしていないので、ユーザにアカウント名 (URL) の投入を要求し、ユーザがアカウント名を投入する。
- ③RP は、投入された URL を用いて IdP 発見要求を出す。
- ④発見要求に合致する OP が返答する。
- ⑤RP は、ユーザのブラウザを介して、認証要求を OP に送る。
- ⑥OP はユーザを何らかの手段で認証する。ここで、どのような認証手段を用いるかは OpenID2.0 では規定しておらず、ユーザ、OP、RP 間の合意に基づき決定される。
- ⑦認証結果が OP から、ユーザのブラウザ経由で、RP に返送される。
- ⑧RP は認証結果に基づき、サービスを提供する。

ユーザが他のサービスを用いる場合は、ユーザが直接認証作業を行うステップ②を除いて、同様の処理が繰り返される。このようにして、シングルサインオンが実現されている。

OpenID2.0 では、属性情報を交換する方式も仕様化されている[26]。その処理手順は、認証結果を交換する場合とほぼ同じである。OpenID2.0 仕様の手順は、SAML2.0 仕様体系の処理の流れに類似している。SAML2.0 における IdP が OP に、SP が RP に対応している。ただし、事前にトラストサークルを構成して置く SAML2.0 とは異なり、RP は OP を URL などで実現された識別子から動的に発見しアクセスする。

OpenID 認証プロトコルは HTTP リダイレクションやクッキーなどの十分に普及している既存技術で実装することができる[19]。OpenID2.0 は、SAML2.0 のような様々な端末や送信手段に対応した仕様体系を持たない。例えば、仕様には通信の暗号化や送受信証跡の保存を前提としておらず、また送信手段は HTTP リダイレクションを利用する手順だけを規定している。

実運用面では、仕様上は事前に OP や RP 間の信頼関係を構築する必要がなく、各アカウントをリンクする必要もない。しかし、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。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には、「名寄せ」によるプライバシー侵害のリスクも高まると考える。

現在 OpenID2.0 は、セキュリティ要件が比較的軽微なサービス (SNS、ブログなど) を中心に広まっている。将来の発展に向けて、対象サービスや利用目的に応じて、セキュリティやプライバシーなどに関して、ユーザ、OP、RP 間で合意が必要な事項を明確にしていく必要があると考える。

(3) アイデンティティ選択方式

アイデンティティ選択方式は、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[3]。代表的な技術仕様として Information Card があり、業界団体 (Information Card Foundation、OASIS) が仕様化、及

び普及を進めている。また、実装例として、Microsoft 社の Windows CardSpace があり、同社の OS に標準装備されている。

Information Card では、「カード」のメタファでアイデンティティを使い分ける。例えば、このカードは、電子的な身分証明書、クレジットカードや会員証などである。アイデンティティ選択方式では、認証と属性交換の明確な区別はなく、ユーザがサービスの利用認可に必要なアイデンティティ情報（例：「20 歳以上である」）を選択して提示する。Information Card 仕様は、シングルサインオンの手順を規定していない。

アイデンティティ選択方式では、ユーザ端末には、ユーザがアイデンティティ（カード）を選択し送受信するための Identity Selector 機能が組み込まれている。また、アイデンティティ提供者として Security Token Server (STS)、サービス提供者として Relying Party (RP) が配置される。Information Card は、Microsoft 社のサービスなどを中心に普及が進んでいる。

図 1.2.10 は、Information Card の処理手順を示す。

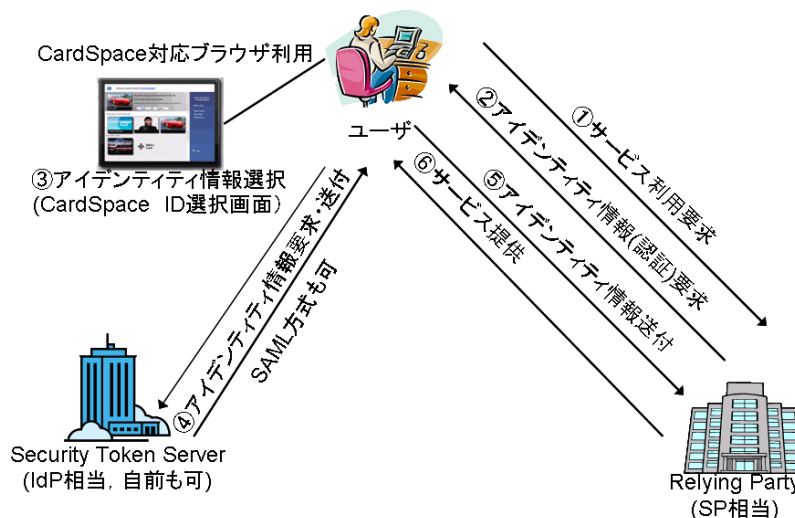


図 1.2.10 アイデンティティ選択方式の処理手順

- ① ユーザが RP にサービスの利用を要求する。
 - ② RP は、まだユーザの認証をしていないので、ユーザにアイデンティティ情報を要求する。
 - ③ ユーザは Identity Selector を用いて、必要なアイデンティティ情報を選択する。
 - ④ ユーザは STS から必要なアイデンティティ情報を取得する。④と⑤では WS-Trust、WS-Policy、WS-Metadata Exchange プロトコルを利用する。アイデンティティ情報取得は SAML 方式でも良い。
 - ⑤ ユーザがアイデンティティ情報を RP に送付する。
 - ⑥ RP は、送付されたアイデンティティ情報に基づき、サービス提供の可否を決定する。
- アイデンティティ選択方式は他の二つの方式と違い、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。サービスごとにアイデンティティを選択するため、シングルサインオンの機能はない。

Microsoft 社が Cardspace の名称で OS に ID 情報の選択・送信機能を組み込んでいる。

表 1.2.1 に代表的なアイデンティティ管理方式をまとめた[3][19]。

表 1.2.1 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</p> <p>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	<p>OASIS (Organization for the Advancement of Structured Information Standards)</p> <p>Security Services (SAML) TC</p>
統一方式	<p>ユーザ中心モデル</p> <p>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"> • OpenID Foundation • OASIS XRI Data Interchange (XDI) TC (基本技術の実装)
選択方式	<p>ユーザ中心モデル</p> <p>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なし。Microsoft 社の影響が強い。</p>	Information Card	<ul style="list-style-type: none"> • Information Card Foundation • OASIS Identity Metasystem Interoperability (IMI) TC (基本技術の実装) • Microsoft (OS に ID 情報の選択・送信機能を標準搭載)

なお 2010 年現在、上記 3 方式間の相互運用を推進する動きが加速している[27]-[29]。

中心となっているのは Kantara Initiative[30]である。Kantara Initiative は Liberty Alliance[31]の活動を継承し、発展させている。OpenID Foundation の支部である OpenID Society、Information Card の標準化団体である Information Card Foundation が有料会員として参加している。

Kantara Initiative に参加している日本の企業、組織は、理事会員として野村総研と NTT、有料会員として NHK である。理事会員は代表者 1 名が理事会への参加／投票権を持ち、有料会員は、それが組織である場合には所属するものが、個人であれば本人が分科会（ワークグループ、ディスカッショングループ）の議長となる場合、当該議長は議長会における投票権を持っている。

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 1.2.2 のような相違がある[32]。

表 1.2.2 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

1.3 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、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。

このような中で、日本国内のアイデンティティ管理市場は近年拡大しており、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。

また、世界のアイデンティティ管理市場は、2006年で31億米ドル、2014年には123億米ドルに達すると予想する報告がある。

一方、企業にヒアリングしたところでは、日本国内のバイオメトリクス市場は、約100億円市場と低迷している。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、これらがリプレース市場になったことにある。また、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も一因である。これらにより、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ためと考えられる。

バイオメトリクス市場の拡大のためは、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る新たな市場は、今後に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)」、FIPS201-1(Federal Information Processing Standardization)、NSTCレポートなどを調査した。

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、ユーザプロフィールなど）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る。

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。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。

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た。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SSO(Single Sign On)である。

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、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・共有を目的としている ID 連携技術である。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、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。

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。

このように、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。

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。

第2章 国内外の標準化及び学会活動状況

2.1 国際標準の状況

表 2.1 に国際標準化活動におけるアイデンティティ管理の活動をまとめる[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 件開発中である。SC37WG6 で扱う WD 29144 The use of biometric technology in commercial identity management applications and processes は、バイオメトリクスを扱うアイデンティティ管理に関するものであるが、目次のみ作成された状況であり、その後のドキュメント開発が遅れており、現時点では目的が不明確である。

SC37WG2 で扱う新規開発案件 BIAS Biometric Identity Assurance Services (BIAS) は、米国内のコンソーシアムで開発が進む規格である。SAML や OpenID などのアイデンティティ管理への接続を容易にするバイオメトリックインタフェースを規格化する。

SC27 で開発中の案件は、アイデンティティ管理のフレームワークと認証対象の信頼性を確保するための規格である。標準規格として成立したものでは ISO/IEC24761 Authentication Context for Biometrics (ACBio) がある。

バイオメトリクスと IdM に関し重要と思われる二つの規格 (BIAS と ACBio) に関し、以下に詳述する。

(1) ACBio

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た[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。以下、オープンネットワーク環境における生体認証の課題について述べる[6]。

文献[6]では、オンラインショッピングの際のパスワード認証の図を利用して説明している。このパスワードをそのまま生体情報に置き換えたのが IdM とバイオメトリクスのアーキテクチャとしている。しかし、機微な情報と考えられる生体情報を予めオンライン店舗などに登録する必要があるため、ユーザには抵抗があり、オンライン店舗としても厳重な管理にコストを要する。

この改良として、IC カードなどの媒体に予め生体情報を登録し、ローカルな生体認証結果だけをオンライン店舗に送る方式が考えられる。しかしこの場合、オンライン店舗は結果だけを受け取ってもその結果を信じて良いか判断することができない。しかし、この生体認証結果の真正性を保証する何らかの仕組みがあれば、オープンネットワークを介した安全な生体認証が実現することができると思われる。

生体認証が正しく実行されたことをオンライン店舗が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ことが ACBio の目的であり、この付加情報のデータ構造が国際規格として発行された。ACBio のデータ構造を図 2.1.1 に示す。

表 2.1.1 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スペ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。

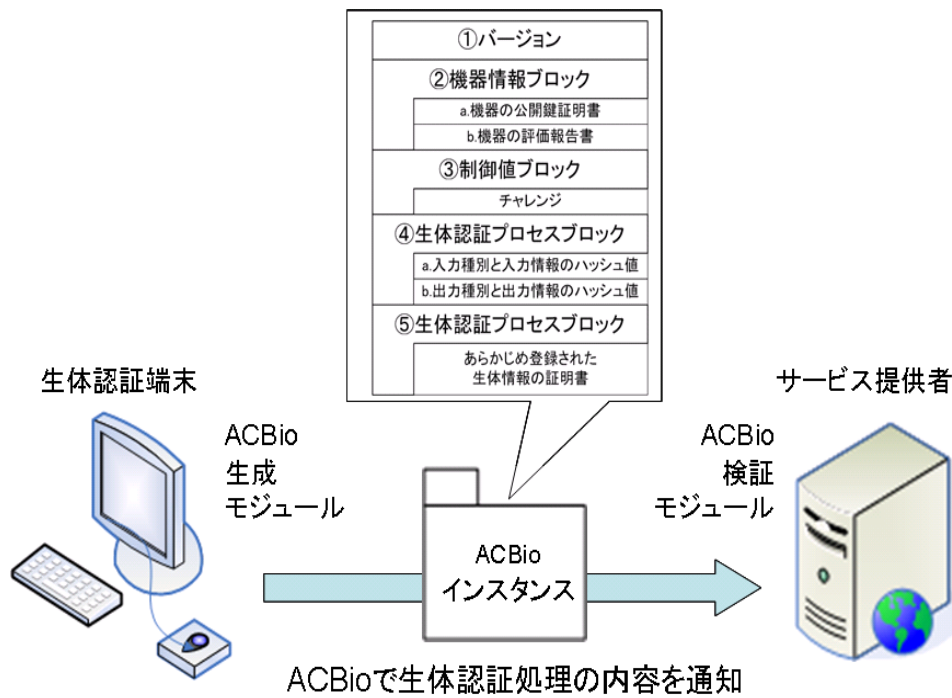


図 2.1.1 ACBio のデータ構造

ACBio を用いた生体認証は、次のようなプロセスをとる。図 2.1.1 の生体認証端末が実行した生体認証処理プロセスの内容や結果を ACBio で規定された共通データ構造（ACBio インスタンス）で出力し、サービス提供者側へ送る。ACBio では均質なセキュリティ強度を持ち、連続した生体認証処理のプロセスからなるハードウェア又はソフトウェアを BPU（Biometric Process Unit）と呼称している。ACBio では、ACBio インスタンスはこの BPU ごとに出力される仕様となっている。サービス提供者側は全ての機器から得られた ACBio インスタンスを検証することで、生体認証処理全体の内容と結果を検証する。

ACBio のデータ構造で「信頼できる生体認証機器で正しく実行されたこと」を検証するための内容は以下のとおりである。

① 生体認証機器の精度と安全性

ACBio インスタンスの「機器情報ブロック」には、ACBio インスタンスを出力した機器の生体認証処理の精度や、機器が安全に実装されているかを評価する機器評価報告書（図 2.1.1 の②）が記述される。この報告書は第三者評価機関が製品を評価して発行することを想定している。この報告書を検証することで処理精度や機器の安全性を確認できる。

② 生体認証機器の認証処理の正当性

ACBio はチャレンジレスポンス認証に対応している。サービス提供者側から送られてきたチャレンジ（乱数）が ACBio インスタンスの「制御値ブロック」（図 2.1.1 の③）に記述される。ACBio インスタンスには機器が保持する秘密鍵を用いて生成された ACBio インスタンス全体に対する電子署名又は認証子が付与される。これにより ACBio インスタンスのリプレイ（再送攻撃）を防止し、正しい機器で処理が実行されたことを検証できる。

③ 複数生体認証機器間のデータ授受の正当性

ACBio インスタンスの「生体認証プロセスブロック」(図 2.1.1 の④)には機器で実行された生体認証処理プロセスの種別と機器の入出力のハッシュ値が記述される。これにより複数の機器間で正しくデータが授受されたかを検証可能である。また (2) の制御値ブロックの値の同一性確認で生体認証処理の一貫性も検証可能である。

④ テンプレートの正当性

採取生体情報との比較に使用したテンプレートの正当性を検証するために、テンプレートを保管する機器が出力する ACBio インスタンスの「テンプレート証明書ブロック」(図 2.1.1 の⑤)にはテンプレート証明書が記述される。この証明書は、予め採取した生体情報が本人のものであることを信頼できる第三者機関が確認し、保証するために発行することを想定している。サービス提供者側はテンプレート証明書の検証により、テンプレートの正当性を確認可能である。

(2) BIAS

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) であり[7]、Web サービスを想定したバイOMETリック認証のための規格案である。

これは、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OMET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た規格であり、複数種のバイOMETリクスによる個人特定の統合や、バイOMET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。

BIAS で定義される機能は Primitive Service と Aggregate Service に大別されている。詳細は不明であるが、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を想定した Biometric を使った個人特定 (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た規格である。もともと米国の標準化団体の OASIS (Organization for the Advancement of Structured Information Standards) が策定したものである。

図 2.1.2 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OMET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。

本規格は、バイOMETリック認証技術における個人の基準となるデータ (テンプレート) をどのように管理するか、つまり、データベースで一括管理するのか、あるいは、IC カードで個人管理するか、プライバシーに関する仕様はどうなるかなどがポイントになる。

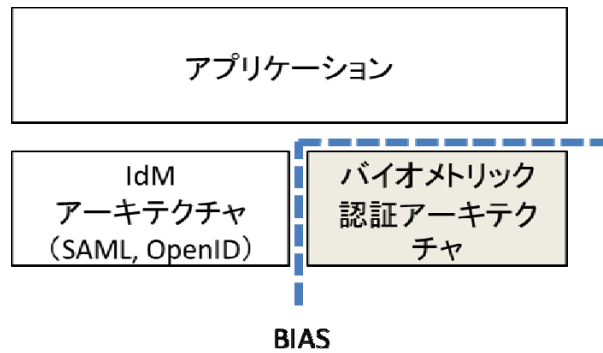


図 2.1.2 BIAS の概要

2.2 欧米の状況

2.2.1 米国

(1) NSTC Identity Management Task Force

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の調査特別委員会を6ヶ月の期限で設置した[8][9]。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。

図 2.2.1 に委員会の構成を示す。

また、調査結果をまとめたレポートが NSTC のウェブサイト公開されている。以下にレポートの要点をまとめる[10]。

- ・アイデンティティ管理は、ID アプリケーション、グローバルテレコミュニケーショングリッド、あらゆる種類のデジタル ID リポジトリの3種類の要因から成り立っている。
- ・スクリーニングとアクセスコントロールのプロセスは米国政府内で共存している。
- ・パブリックメッセージングと社会的受容は、米国政府のアイデンティティ管理へのアプローチでは、ネガティブな結論とともに側面的な問題だと見られている。
- ・個人識別情報 (Personally Identifiable Information) は、アプリケーション固有データとデジタル ID の認証成立に使用されるデータに分割される可能性がある。

上記のようにレポートの内容は概念的であり、具体的な主張を理解分析するには、更に詳細な資料が必要であると考えられる。

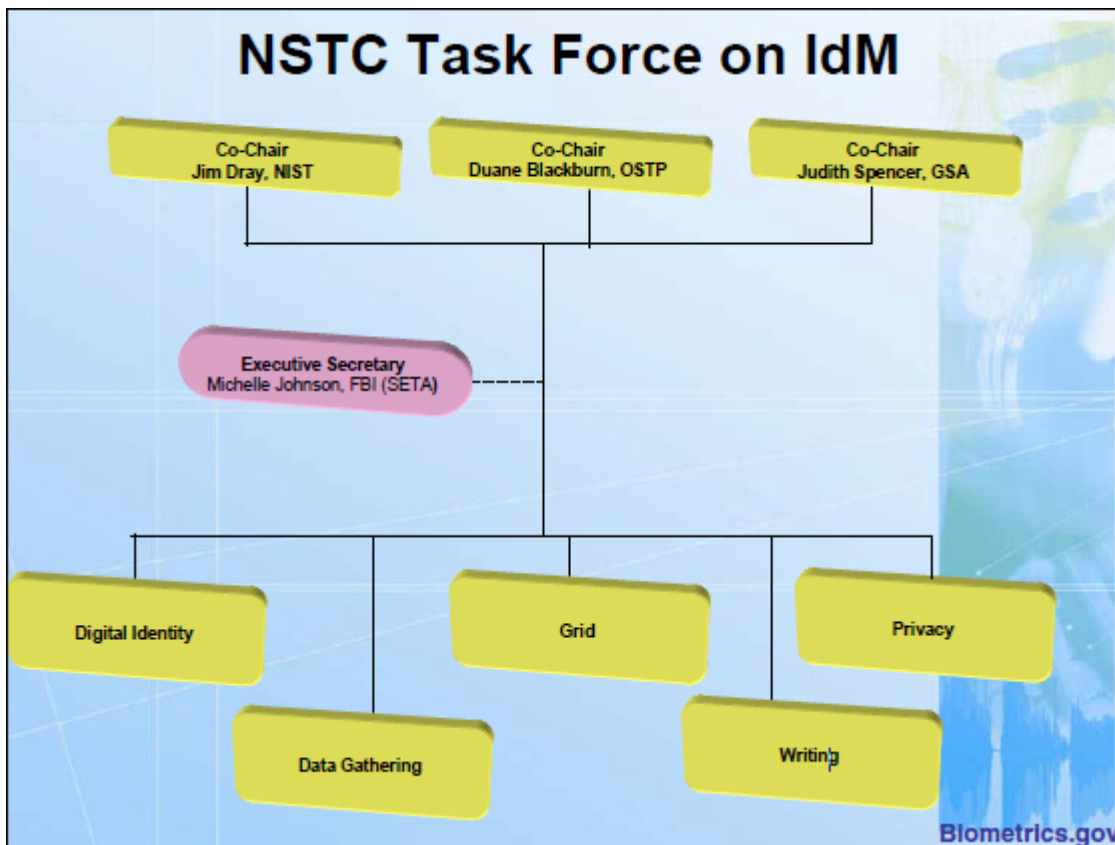


図 2.2.1 NSTC アイデンティティ管理調査特別委員会の構成

(2) The Biometrics Identity Management Agency

前項記載の特別調査委員会の構成組織に DOD が入っていることから分かるように、バイオメトリクスを応用したアイデンティティ管理には防衛関係者が強い関心を示している。米国では従来 DOD 内にバイオメトリクスについて調査・研究するタスクフォースを設置していたが、2010年3月、恒久的な組織として The Biometrics Identity Management Agency (BIMA) を設置した[11]。

BIMA は国立標準技術研究所 NIST (National Institute of Standards and Technology) とともに各種標準化団体のメンバーとして活動している。メンバーとなっている標準化団体は以下のとおりである[12]。

- ・ Technical Committee on Biometrics (M1) of the International Committee for Information Technology Standards (INCITS)
- ・ Subcommittee 37 (SC 37) of the Joint Technical Committee 1 (JTC 1) of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- ・ BIMA serves as the SC 37 Liaison to SC 27 on Security Techniques
- ・ Biometric Identity Assurance Services (BIAS) Technical Committee of the Organization

for the Advancement of Structured Information Standards (OASIS)

- Workshop for developing the ANSI/NIST ITL 1-200x standards、 sponsored by the National Institute of Standards and Technology (NIST)
- BIMA serves as editor of the DoD Electronic Biometric Transmission Specification (EBTS) and is responsible for the DoD EBTS change control.

アイデンティティ管理は、複数の組織で、異なる視点で開発、運用されているため、BIMA のような組織で情報を共有・調整することは意義があると考えられる。

(3) Identity Ecosystem

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[13] [14] [15]。

ポイントは以下のとおりであり、バイオメトリクスとの関係は不明であるが、今後の調査が必要な事案である。

- アイデンティティエコシステム (Identity Ecosystem) とは「信頼できる組織が作り認証するデジタル ID を介し、個人や組織、サービス、デバイスが情報をやりとりできる仕組み」となっており、ユーザネームやパスワードを使わずに ID 証明をする仕組みである。
- 例えば、銀行や携帯電話会社などが信頼できる ID 証明を発行し、電子メールプロバイダやソーシャルネットワーキングサイトがこれを ID 証明として受け入れれば、ユーザネームやパスワードを入力せずに自動的にログインできるようになる。
- Identity Ecosystem を実現する具体的なデバイスは特定していないが、スマートカード、携帯電話、USB ドライブ、信頼できるコンピューティングモジュールなどが例として挙げられている。

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。NSTIC は国土安全保障省 DHS で公開されており、政権がサイバーセキュリティを物理的なセキュリティと同等、あるいはそれ以上に重視している。

公開されている NSTIC ドラフトの用語集では Identity Ecosystem を次のように表現している[14]。

「権限のあるソースを確立して、デジタル ID を認証するため、個人、組織、サービス、及びデバイス相互の信頼を保護するオンライン環境である。自然の生態系と同様、異なる組織及び個人がともに機能し、包括的な標準及び規則のセットによる固有の役割と責任が要求される。」

NSTIC ドラフトでは Identity Ecosystem はアイデンティティを秘匿し取引を実現するために必要な情報のみを共有することにより匿名の参加者を保護する一方、より身元確認が必要な取引や医療情報の照会などにも対応するとしている。

NSTIC の目標は以下 4 項目である。

- Goal1: 包括的な Identity Ecosystem フレームワークを構築する。
- Goal2: Identity Ecosystem フレームワークに基づき相互連携可能なアイデンティティインフラストラクチャを構築・実装する。
- Goal3: 信頼を高め Identity Ecosystem に参加しようという意欲を喚起する。
- Goal4: Identity Ecosystem の長期的な成功を確かなものとする。

この目標を実現するために、以下 9 項目が重要とされている。

- Action1: ゴールや戦略を実現するためのパブリック/プライベートセクターの取り組みを連邦政府がリードすることを示す。
- Action2: 共有され包括的なパブリック/プライベートセクターの実施計画を作成する。
- Action3: Identity Ecosystem に関連する政府サービス、実験、政策を拡大する。
- Action4: 強化されたプライバシー保護の実現のためにパブリック/プライベートセクターで協働する。
- Action5: リスクモデルと相互連携のための標準の開発と改善。
- Action6: サービス提供者や個人間の責任の所在を明確にする。
- Action7: 全てのステークホルダーに対する広報や啓蒙を行う。
- Action8: 国際的なコラボレーションを継続する。
- Action9: 米国内における Identity Ecosystem の採用を促進する他の方法を特定する。

NSTIC では、実行、管理、統制の各レイヤを規定しアイデンティティエコシステムを構築運用する。

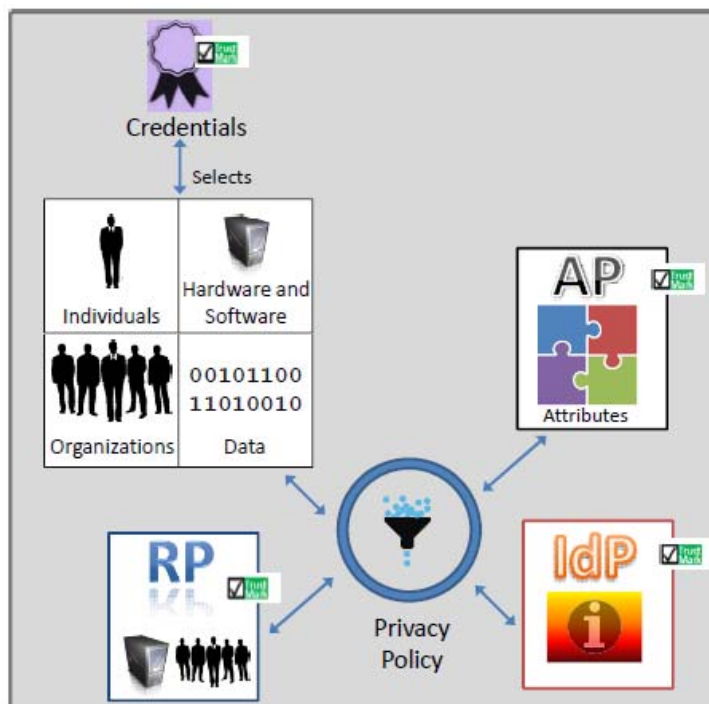


図 2.2.2 実行レイヤ

図 2.2.2 に示す実行レイヤは、人間、組織、ハードウェアやシステムなどの人間以外の主体が相互に関与しつつオンライントランザクション上で活動する層である。

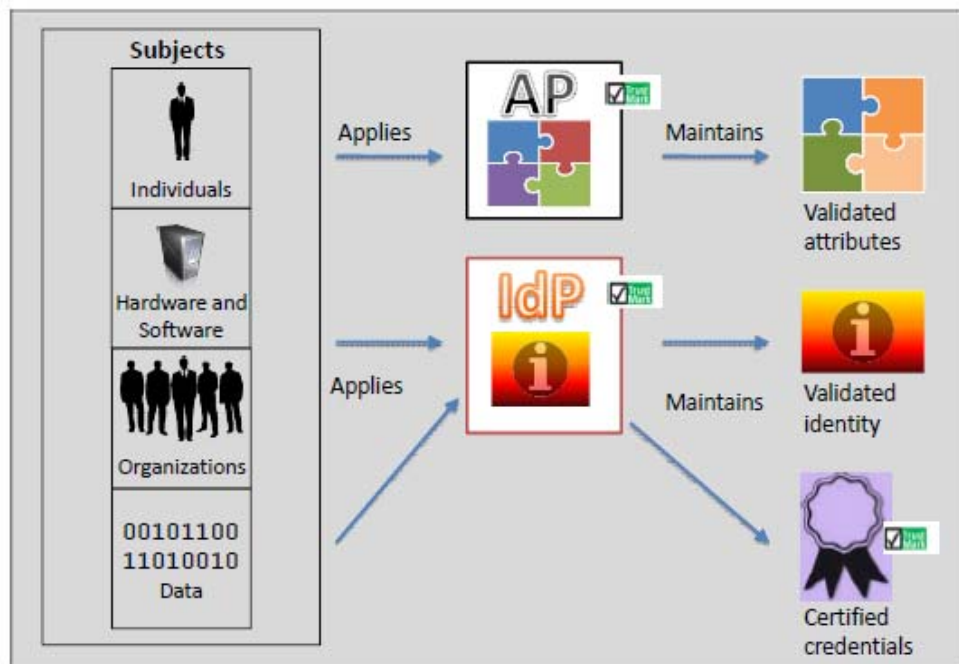


図 2.2.3 管理レイヤ

図 2.2.3 に示す管理レイヤは、人間とそれ以外の主体が同じ IdP のもとで活動する層である。

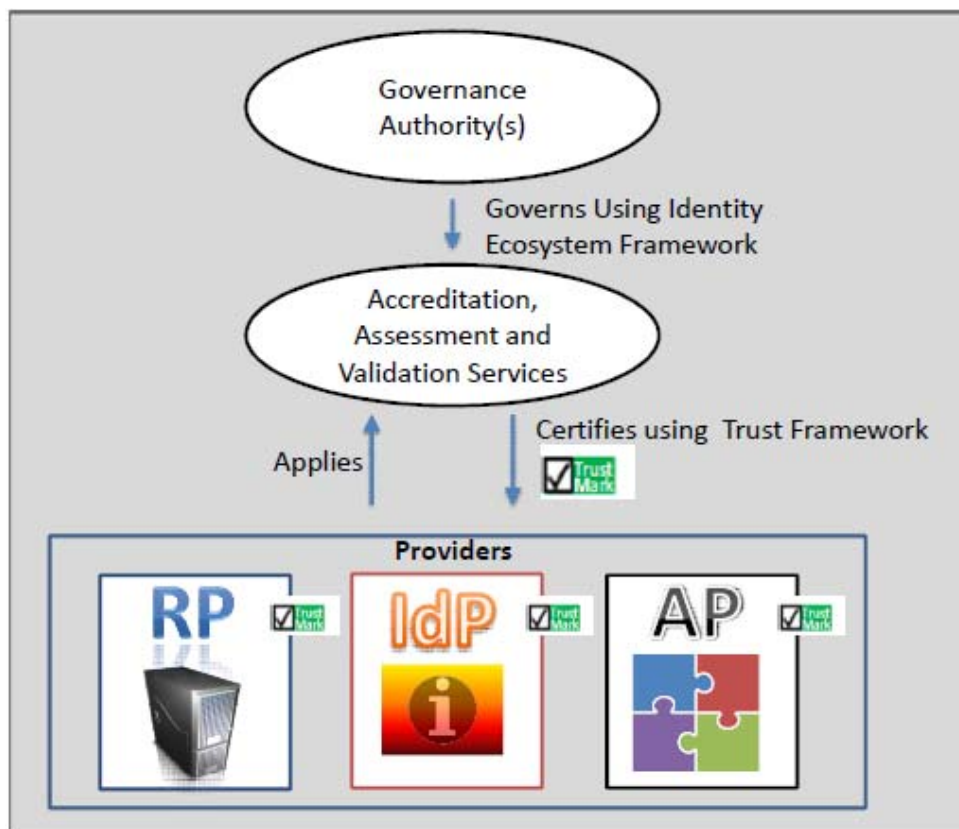


図 2.2.4 統制レイヤ

図 2.2.4 に示す統制レイヤは、提携関係にない主体が、互いのデジタルアイデンティティを信頼できるようにするレイヤである。

デジタル ID の管理の仕方が不明であるが、デジタル ID は端末などで管理する可能性もあり、端末の所有者認証などにバイオメトリクスは重要な機能となる可能性がある。

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る。

2.2.2 欧州

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含む、幅広い隣接領域を調査研究の対象としている。以下に最近の代表的なプロジェクトの概要をまとめる。

(1) primelife

primelife は EU 第 7 次フレームワーク計画によって設立された。第 6 次フレームワーク計画において実施された PRIME プロジェクトの成果を基盤に、これを拡張するものと位置付けられている。バーチャルコミュニティなどの新しいインターネットアプリケーションにおいて、プライバシーをどう保護するか、プライバシーのライフサイクル保護はどのように可能かを検討した。primelife では、この二つの課題の中心にあるプライバシーと信頼の問題に取り組んでいる。また、コミュニティ全般が確実にプライバシー技術を取り入れることを目的とし、オープンソース方式を採用し、標準化団体及びパートナープロジェクトと積極的に協力する方針となっている[16]。

(2) PICOS

PICOS (Privacy and Identity Management for Community Services) は、モバイルコミュニティにフォーカスした国際的なリサーチプロジェクトである。EU 第 7 次フレームワーク計画のサポートを受けている。7 カ国からなる 11 のパートナーで構成されており、科学、リサーチ、産業界の専門家が多数参加している。

近年、ソーシャルネットワークなどのオンラインコミュニティサービス娯楽として、またビジネスを支援するサービスとして利用されることが多くなったが、ユーザは意識せずに個人情報をコミュニティに残しており、プライバシーの管理はこのサービスにとって常に重要な課題である。その上、また段々とメッセージなどのサポートサービスが事業者の間で相互に運営されるものとなりつつあり、サービスプロバイダ間でのサポートサービスのインターオペラビリティも必要となって、ユーザ ID の管理形態が複雑になる。その上、これらの問題は不透明な仕方では解決されてはならず、コミュニティメンバーによる個人情報の管理が必要であるため、PICOS は信用、プライバシーを尊重する 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している。開発されるツールは相互接続性が確保され、オープンなアーキテクチャである[17]。

(3) SWIFT

SWIFT (Secure Widespread Identities for Federated Telecommunications) は EU 第 7 次フレームワーク計画によって設立された。このプロジェクトは、利用者にとっても提供者にとっても利便性のある、サービスと輸送インフラの統合の鍵としてのアイデンティティ技術の目標達成のための力となる。このプロジェクトは、ユーザビリティとプライバシー関係のアイデンティティ機能とネットワーク連携の拡大にフォーカスしている[18]。

(4) FIDIS

EU の第 6 次フレームワーク計画のプロジェクトである FIDIS (Future of Identity in the Information Society) は、EIS (European Information Society) 及び構築中の技術や基盤における将来のアイデンティティ管理の要件をまとめている[19]。

FIDIS の目標は以下のとおりである。

- ・ アイデンティティにおける専門機関となる。
- ・ アイデンティティ管理システム、アイデンティティ法規及び使われ方に関する情報の収集
- ・ 成果物の開示。
- ・ 調査機関、科学的コミュニティ、標準化団体及び先駆けに対しての影響を与える。

(5) PRIME

EU 第 6 次フレームワーク計画のプロジェクトである PRIME (Privacy and Identity Management for Europe) は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ことを目的としている。市場の導入を育成するため、アイデンティティ・マネジメントの斬新な解決策が、興味深いシナリオ、例えばインターネットコミュニケーションや航空機の搭乗プロセスや位置情報サービスや e ラーニングとして実演された[20]。

(6) GUIDE

EU 第 6 次フレームワーク計画のプロジェクトであり 13 か国の 23 の構成から成る GUIDE (Government User IDentity for Europe) はヨーロッパ向けに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を行っている。プロジェクトのアプローチは学際的で、ヨーロッパ横断的な技術、手続及びポリシー開発を含んでいる。GUIDE は、身元認証のオープン・アーキテクチャの生成によってヨーロッパが電子政府サービスのグローバルリーダーになることを目標にしている[21]。

(7) TURBINE

EU では多くの調査研究プロジェクトが実行されているが、この中で特に IdM とバイオメトリクスに関係が深いと思われるのが EU 第 7 次フレームワーク計画の TURBINE プロジェクトである。プロジェクト名称が TrUsted Revocable Biometric IdeNtitiEs の省略名であることから分かるように、取り消し可能なバイオメトリックアイデンティティについての研究と技術開発を行っている[22][23]。

プロジェクトの目的は以下のとおりである。

- ・ 電子 ID 認証のための指紋バイオメトリックによる革新的なプライバシー保護技術ソリューションの開発。
- ・ 上記ソリューションのパフォーマンスとセキュリティを実証する。十分な市民のプライ

プライバシー保護と指紋による電子アイデンティティ管理に対するユーザの信頼をもって商業ベースの電子 ID 管理アプリケーションで使用できるレベルを目指す。

本プロジェクトの実施期間は 2008 年 2 月～2011 年 1 月の 3 年間である。2011 年 1 月にはベルギーのブリュッセルで"CryptoBiometrics for Enhanced Trusted Identity Management: Dreams and Reality" と銘打った最終のワークショップが開催された。

TURBINE は暗号化と指紋認証を併用した多分野にまたがるプライバシー保護技術である。バイオメトリクスを利用した 1 対 1 照合は、バイオメトリクスを利用したアイデンティティ管理についてプライバシー上の懸念がもたれているにも拘らず、異なるシステム間での相互接続やシステムのセキュリティに威力を発揮することも確かである。本プロジェクトの主目的は商業上の利用に十分見合う大規模なアイデンティティ管理に要求されるソリューションとして、十分成熟した技術を提供することである。

本目的達成のため、取り消し可能な保護されたバイオメトリックテンプレートと指紋データを用いる擬似アイデンティティに関する基盤技術と応用技術の開発と評価が行われている。また、バイオメトリックデータの不可逆な暗号化保護と、バイオメトリック照合によるプライバシーなどに対する種々の影響を最小限にすることが必要であるとされている。TURBINE によるデータの不可逆変換の考え方を図 2.2.5 に示す。

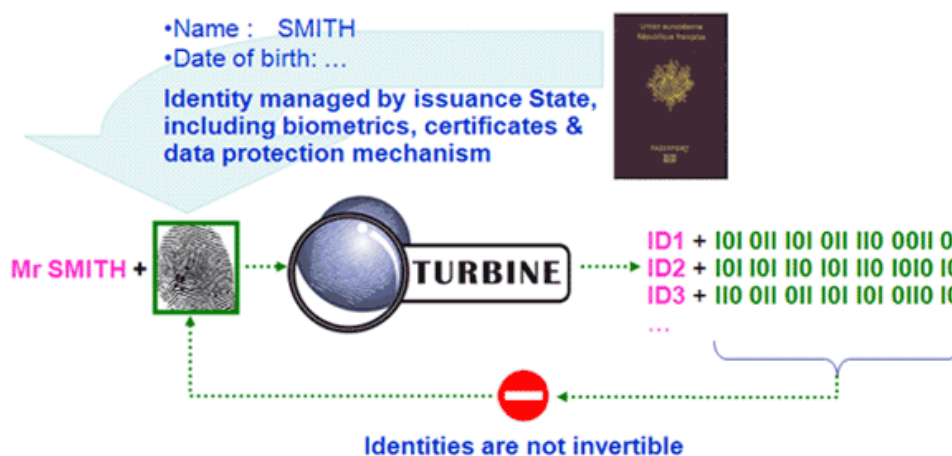


図 2.2.5 TURBINE によるデータの不可逆変換[22]

プロジェクトの成果は暗号化による保護ありとなしとで巨大な指紋データベースを用いて評価される。

実証のための実演はテサロニケ国際空港のセキュリティエリアで、エンドユーザ管理下のスマートカードトークン関与下で行われる予定である。

TURBINE プロジェクトで利用される指紋照合アルゴリズムは 2 種類ある。一つはオランダ・University of Twente と Philips Research Europe によるスペクトラム特徴点を二次元フーリエ

変換して利用するアルゴリズムと、ノルウェー・Gjøvik University College による特徴点のハッシュ値による幾何学的補正アルゴリズムである。

TURBINE プロジェクトは国際標準も視野に入れている。ISO/IEC 24745 “Biometric Template Protection”である。この規格（案）は 2010 年 9 月 21 日現在、FCD（Final Committee Draft）から次の段階に進むための投票が終了した段階である [24]。

2011 年 1 月 17 日 - 18 日にベルギーのブリュッセルで最終ワークショップ CryptoBiometrics for Enhanced Trusted Identity Management: Dreams and Reality が開催された。概要は以下のとおりである。TURBINE は Morpho 社が実質的な推進主体であり、参加者は約 100 名、日本及び米国など欧州以外からも参加があった。欧州では多くの国で、法律によりバイオメトリクス情報のデータベース管理が禁止されている。TURBINE はバイオメトリクスのプライバシー保護が中心となる研究プロジェクトである。

主な発表は、以下のとおり。

- Improve biometric adaptation for cryptographic technique (Anil Jain, Michigan State Univ, 米国)

キャンセラブルバイオメトリクスには"fuzzy vault"と"fuzzy commitment"の二通りのやり方があり、前者は元の特徴量にノイズを追加して復元できなくするもの、後者は元の特徴量に暗号コードを追加して、それをテンプレートとのマッチングを通じて復元することである。いずれの方法も 40 ビット程度の暗号強度しか持たない。

- Spectral minutiae representation (Raymond Veldhuis, University of twente, オランダ)

キャンセラブル化でテンプレート容量が増加することの対策（圧縮技術）の発表。

- Fingerprint feature vector representations (Vincent Despiegel, Morpho, フランス)

指紋のマニューシャをキャンセラブル化に対する発表する。

- TURBINE architecture and protocols for Trusted ID management (Herve Chabanner/Julien Bringer, Morpho, フランス)

ノイズを含む対象に有効なキャンセラブルバイオメトリクスの発表。

- TURBINE Performance evaluation from benchmarks to Airport deployment (Christoph Busch, Gjøvik University College, NORWAY)

ドイツの空港で行ったキャンセラブルバイオメトリクス評価結果の紹介。

表 2.2.1 に欧州におけるアイデンティティ管理関連プロジェクトを示す。

表 2.2.1 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	<ul style="list-style-type: none"> 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 (Privacy and Identity Management for Community Services)	<ul style="list-style-type: none"> 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 (Secure Widespread Identities for Federated Telecommunications)	<ul style="list-style-type: none"> 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 (Future of Identity in the Information Society)	<ul style="list-style-type: none"> 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 (Privacy and Identity Management for Europe)	<ul style="list-style-type: none"> 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 (Government User IDentity for Europe)	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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OMET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[25][26][27]。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。当プロジェクトにより作成される共通仕様は、プロジェクトに参加しない国も含めた全 EU 加盟国に照会されるため、EU 全域に影響力を持つものになることが期待されている。また、作成された共通仕様は、将来において eID を活用したサービスを開発しようとする全ての業界に対して公開される。参考資料、ガイドライン、マニュアル及び教育用マニュアルも作成される予定である。

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。

2.2.3 欧米におけるアイデンティティ管理に関するカンファレンス

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。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の一覧を表 2.2.2 に示し、以下、概要をまとめる。

表 2.2.2 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	2007 年より毎年	ドイツ ミュンヘン
(2)	IDM	開始年未確認 2010 年が第 4 回	英国 ロンドン
(3)	Identity management 2010	2010 年 開始年未確認 毎年開催の模様	米国 Washington DC
(4)	Gartner Identity & Access Management Summit	2010 年 2006 年まで確認 毎年開催の模様	米国 サンディエゴ
(5)	Identity Management for National Defense	2009 年 単発の模様	米国 ワシントン DC
(6)	Biometric Consortium Conference 2010	2010 年 毎年開催	米国 フロリダ・タンパ
(7)	Biometrics 2010	2010 年 毎年開催	英国 ロンドン

(1) European Identity Conference 2010

European Identity Conference 2010 は、2010年5月4日から7日にかけてドイツミュンヘンで4日間に渡って開催された欧州内の企業を対象とした大規模なカンファレンスである。第1回のカンファレンスが2007年に開催されて以来、毎年ミュンヘンで開催されている。アイデンティティ管理に関する最先端の技術的、応用的なテーマを扱っている。

kuppinger cole 社がモデレータを務めており様々な分野から142名の講演者が参加した。また2009年から European Identity Award という賞を設けている[28]。

カンファレンスでの話題となったキーワードは、以下のとおりである。

- ・Lean IT: Creating more Value for less through Identity Management & GRC
- ・Business / IT Alignment
- ・Rising Maturity: Expansion & Replacement Best Practices
- ・Finding the Best Possible Response to Top Information Security Risks
- ・Extending Identity based Information Security into the Cloud
- ・Solving the Identity Issues of Virtualization
- ・Safely Managing Privileged Identities
- ・Access Governance – Controlling access and ensuring information and system security
- ・Role Based & Attribute Based Access Control (RBAC vs. ABAC)
- ・Integrating Identity, Roles and Data Loss Prevention
- ・Privacy & Regulation
- ・Consistent Approaches for Authentication and Authorization

(2) IDM2010

IDM2010 は、2010年11月3日に英国ロンドンで開催された英国内のパブリックセクター・銀行や保険などの金融分野・その他の企業を対象としたカンファレンスである[29]。毎年定期的で開催されている。欧州連合のネットワークセキュリティ及び情報セキュリティに関する機関である ENISA (European Network and Information Security Agency)、Bank of England、英国財務省、英国の行政関係で IT 業務に従事するメンバーを主として構成される Soctim (Society of Information Technology Management)、金融グループの Barclays が後援している。運営はカンファレンス運営会社の Whitehall Media Ltd.が行っている。

以下にセッションと講演などのタイトルをまとめる。

Session 1 - What will a Comprehensive, Customer-Focussed Identity Management Infrastructure look like in the 21st Century - Cross-Sectoral Case Studies and Industry Perspectives?

- ・ Pursuit for Sign-On Simplicity
- ・ Banking and Finance Case Study from Intragen: SNS Reaal/Zwitsersleven

- Implementing trust, security and compliance controls in public and private Cloud environments
- Identity, Governance and Security: The real role of Identity and Access Management for the Enterprise
- AD as an Identity Store: Are you mad?...

Session 2 - Identity and Access Management Innovations, new technologies and case studies driving both the business and the security agendas in the UK.

- Higher Education Case Study - University of Nottingham IDM – from disillusion to reality
- Security Perspectives and Identity Management in the Cloud
- Health Sector Case Study: Mid-Yorkshire Hospitals NHS Trust Identity Management - its all in the name. An NHS journey.

Session 3 - Thought Leadership

- Successful Identity & Access Management strategies
- Identity Management - Foundation to a integrated security framework

(3) Identity management 2010

Identity management 2010 は 2010 年 9 月 27 日、28 日に米国で開催された OASIS と IBM がスポンサー、世界銀行がホストのカンファレンスである[30]。本カンファレンスは OASIS のイベントサイトに記載された情報から推察すると、毎年開催されているようである。カンファレンスのスポンサー、運営協力者は毎回代わっているようであるが、2009 では NIST、オープンソースのアイデンティティ・フレームワーク構築を目指す Higgins Project の運営主体である Identity Commons (<http://www.idcommons.net/>)、Information Card Foundation が運営に携った。

(4) Gartner Identity & Access Management Summit

Gartner Identity & Access Management Summit は、Gartner 社主催のカンファレンスである。開催は 2006 年まで遡って確認された[31]。昨年 2010 年は 11 月 15 日から 17 日にかけて米国サンディエゴで開催された[32]。本年は 2011 年 3 月 9 日、10 日に英国ロンドンでの開催が予定された[33]。2010 年のテーマ “Transforming IAM: The New Business Intelligence Connection”、2011 年のテーマ “Prepare for the Best: The IAM-Enabled Business” から、統制に力点を置いたカンファレンスである。

(5) Identity Management for National Defense

Identity Management for National Defense は、2009 年 7 月 27 日から 29 日にかけて IDGA (Institute for Defense & Government Advancement) 主催によってワシントン DC で開催されたカンファレンスである[34]。

(6) Biometric Consortium Conference 20XX

毎年9月に米国タンパ（フロリダ）で開催されている NIST など米国政府主催のバイオメトリック技術・プロジェクト・標準に関するカンファレンスである。内容は米国政府の活動が中心となっている[35]。

2010年は9月21日 - 23日に開催された。100件ほどの発表があった。三つのセッション（政府関係、技術関係、標準化関係）に分かれている。概要は以下のとおりである。

米国国防総省に今年4月 BIMA(Biometric Identity Management Agency)が設置された。これに伴い、米国の IdM に関するプロジェクトが新たに生じるのかと期待したが、政府関係の動きは、例年と同様であった。つまり、FBI は Forensic 関係、DHS は US-VISIT 関係、DoD は個人情報収集と分析システムの構築関係を粛々と進めている。新しい動きは、DNA のセッションが、一日も受けられたことである。DNA に関しては20件ほどの研究成果が発表されていた。主催が NSA、DoD などであり仕方ないが、民需の動きが把握できなかった。展示会場も DoD や FBI 対応の製品がほとんどであった。

米国の IdM のプロジェクトは、現状の LDAP などの認証プロトコルにバイオメトリクスを実装しようというのではなく、あくまでもバイオメトリクスの情報共有を効率的に行うというものであった。

IdM に関連するセッションとしては、Federal Identity Research Needs (DHS)をはじめとし9件の講演があった。また、サイドセッションとして USNORTHCOM Biometric & Identity Management Interagency & International challenges のパネルセッションがあった。USNORTHCOM とは北米司令部の意味である。

アルゼンチン、オーストラリア、中国、ロシア、インド、EU、日本のバイオメトリクス市場動向などの発表があった。このように、各国で社会 ID などのプロジェクトが確実に進んでいる。

EU はドイツの Bush 氏が Turbine プロジェクトを発表した。プロジェクトも完了時期にあり、2011年に成果発表会がある模様である。EU はプライバシーに関し厳しい制約があり、プライバシープロテクションの活動が Sagem 社、Philip 社を中心に行われた。本プロジェクトの成果に関しては精査が必要であると考えられる。

(7) Biometrics 20XX

毎年10月に英国ロンドンで開催されている学術情報大手のオランダ Elsevier 社主催のバイオメトリック・プロジェクトに関するカンファレンスである。内容は欧州及びアフリカなどの近隣の国々の活動が中心となっている[36]。

2010年は The Queen Elizabeth II Conference Center, London) で10月18日 - 20日開催された。約30件の発表があった。3分の1は自動化ゲート（入国管理システム）に関する各国のとりくみである。あとはセキュリティ関係の発表があり、インドなど新興国における社会 ID の適用に関する発表があったが、アイデンティティ管理の発表は見当たらなかった。

Biometrics2009は、The Queen Elizabeth II Conference Center, London) で、2009年10月

20日 - 22日開催された。参加者は、政府関係政策者、企業研究者、大学研究者などカンファレンス約200名ある。

カンファレンスの内容は、以下のとおりである。カンファレンス（約50件）と展示（IEEE他世界のバイオメトリックセキュリティ主要ベンダ）。3日間開催された。

2008年の金融危機により、バイオメトリック製品を扱う企業は次の十年を見越した方向転換を求められている。技術の進歩は、精度、使い勝手などの改善をもたらし、個人利用、商用利用、政府関係のアプリケーションなどが進んだ。しかしいくつかの大きなプロジェクトで問題も生じた。例えば、US-VISIT Exit プログラムの失敗、TWICの縮小（1200万人空港従事者から100万人海港の従事者への縮小）、UK National ID cardの変容（選択枝となった）などである。

J.Wayman教授らは、バイオメトリック企業に対し金融危機は打撃にはなったが、壊滅的な状況ではないとの見解を示した。政府関係プロジェクトは、スローダウンしたが、一方では、経済を活性化するために投資も考慮されている。商業利用も経済の好調さに合わせて良くなる方向にあると関係者は考えており、バイオメトリック世界市場は2017年までに110億ドル（1兆1000億円）に達する（2009年は25億ドル（2500億円）と見積もられている。しかしながら、過去の経験からこの数値は楽観値と思われる。

EUでは、EU政府アプリとして、The biometric matching systemのSOAソリューションを検討している。

A Directorate C migration and border（移民と国境に関する欧州理事会勧告）

B Immigration（入国管理に関する欧州理事会勧告）

の二つのEU理事会勧告により、EUのセンターシステムEURODACを開発している。

具体的には、

① Schengen Information system II 開発中

② Visa information system 開発中

である。

この二つのシステムを仲介するのがBMS（biometrics matching system）であり、10指を扱うシステムである。これらはプライバシーも考慮したシステムということである。

つまり、BMSを介し二つのアプリシステムが統合化（SIS2-BMS-VISという関係）され、その共通的なプラットフォーム的な位置付けとして、BMS providing biometric matching serviceを設ける構成である。また、Entry/Exit systemは、2010年稼働目的に法的手続き中とのことであった。

BMSに関しては、要調査事項である考える。

上記のように欧米では、定期的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。

2.3 日本国内の状況

2.3.1 プロジェクト

日本国内のプロジェクトは、開発ベースではなく、調査ベースである。

(1) JNSA政策部会アイデンティティ管理ワーキンググループ

日本ネットワークセキュリティ協会（JNSA）の内部統制におけるアイデンティティ管理ワーキンググループは、「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[37]。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) IPA情報セキュリティ技術動向調査TG（タスクグループ）

独立行政法人 情報処理推進機構セキュリティセンター内の「情報セキュリティ技術動向調査TG（タスクグループ）」で、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[38]。この報告書は年2回発行されており、2008年下期、2009年上期、同下期の報告書でもアイデンティティ管理について取り上げている。

(3) 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、財団法人日本規格協会(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[6]。

2.3.2 学会研究会など

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 2.3.1 に示す。

表 2.3.1 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)	SCIS (暗号と情報セキュリティシンポジウム) 2011 [45]	2011年は1月25～ 28日	毎年1月に開催
(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

(1) カンターラ・イニシアティブ・技術セミナー2010

2.2 節でアイデンティティ管理方式の相互運用促進に努めている団体として紹介した Kantara Initiative 主催のセミナーである[39]。下記の講演と事例研究で構成されている。

特別講演

「SAML 準拠の Shibboleth を活用した学術認証連携基盤の構築」

国立情報学研究所 学術ネットワーク研究開発センター 教授 中村 素典

事例研究

「バックオフィス連携実験における ID 連携技術の適用」

株式会社NTTデータ リージョナルビジネス事業本部

2010年に同団体が主催して開催された他の講演会などは以下のとおりである。

- ・カンターラ・イニシアティブ 発足記念セミナー（2009年7月14日）
- ・カンターラ・イニシアティブ・シンポジウム 2009（2009年11月6日）
- ・カンターラ・イニシアティブ・セミナー2010（2010年4月16日）
- ・カンターラ・イニシアティブ・シンポジウム 2010（2010年9月1日）

(2) OpenID Tech Night Vol.6

3.2節で紹介するID管理方式のうち、OpenIDを日本で普及・推進する団体によるOpenIDファウンデーション・ジャパン主催の技術セミナーである[40]。事例紹介が主であるが、OpenID Foundation 理事（開催当時）の野村総研・崎村夏彦氏によるOpenIDとOAuth（APIアクセス委譲についてのオープンプロトコル）の次期仕様紹介など、先端の話題も取り上げている。なお、崎村氏は2011年のOpenID Foundation 理事長に選出されている。

OpenIDファウンデーション・ジャパンでは技術的なセミナー、講演会の他に、インターネットでの中継という形で「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」を4回開催している[41]。この勉強会は電子政府・行政におけるこれまでのID/認証の仕組みを振り返り、オープンガバメント時代の新しい国民IDのあり方を議論・共有することを目的としている。

(3) 平成22年度情報処理技術セミナー Shibboleth環境の構築

3.2節で紹介する学術認証フェデレーションの参加に必要なShibboleth環境の構築・運用について必要となる知識を大学・研究機関などの情報処理関連部署に勤務し、機関内のシステム運用管理に係る業務を担当している教職員が修得するためのセミナーである[42]。このセミナーは大学などの関係者のみが受講対象となっているが、学術認証フェデレーションでは2011年3月7日にシンポジウムを開催した[43]。

(4) CSS（コンピュータセキュリティシンポジウム）2010

2010年10月19日・21日、岡山コンベンションセンター（岡山市）で開催された[44]。

アイデンティティ管理に関係する二つのセッションを徴候した。(1)クラウドコンピューティング、(2)認証とID管理である。新たにこの二つのテーマが話題になるのが最近の学会研究会の傾向である。

オープン環境でのコンピュータシステムの構築とサービス提供時における本人認証は、オープンな環境でのセキュリティ確保という従来にない認証アーキテクチャが必要とされている。各セッションの状況については、以下のとおりである。

① クラウドコンピューティング

・ Cryptographic Cloud Storage with Fine-grained and Flexible Access Control (九大)

クラウドストレージに関し、二つの暗号技術を効果的に利用し融合することで、安全に共有するためのアクセス制御方法を提案した。

・ クラウドにおけるデータ秘匿・追跡技術とその応用 (富士通研究所)

パブリッククラウドにおいてセキュリティレベルを確保したセキュリティウェアネスクラウドの提案である。特にアイデンティティ管理・アクセス管理 (IAM) と鍵管理が重要である。提案としては、認証における保証レベルを自組織で行う。また、鍵管理はパブリッククラウドでの保証レベルを鍵の保証レベルで置き換えるために本質的であることを明らかにした。

・ セキュリティウェアクラウド：概念とモデル (東大)

クラウドでのソーシャルセキュリティに関し、複数のステークホルダーにおけるアクセス制御とオープン環境にデータを保管する問題とみなし、鍵管理と IAM を内部統制下で行う ISMS の観点から解析した。

② 認証と ID 管理

・ 公的 IC カードを利用した医療機関からの保険資格確認方法の検討 (東工大)

今後実装予定の公的 IC カードの電子認証 PKI を利用し、保険資格確認要求が、利用者本人か、医療機関などにより代行要求なのかを判別するシステムに関する手法の検討を行なった。

・ Felica の利用履歴を用いた個人認証 (電通大)

交通機関などで利用される Felica を用いて、本人しか知らないであろう所持者の利用履歴情報を用いて、カード所有者の認証を行う方式。

・ OpenID における属性情報の登録と活用に関する提案 (理科大)

OpenID は、URI (Uniform Resource Identifier) 又は XRI (extension Resource Identifier) を識別子とするユーザ中心の分散認証サービスであり、SSO (シングルサインオン) の対応が可能となる。OpenID は OP、RP、User の 3 者モデルで表され、OP (OpenID Provider) はユーザが主張する Identifier を認証する主体であり、RP (Relying Party) はユーザを認証するために OP に認証を依頼する主体である。User は自身の ID である Identifier を主張し OP から認証される主体である。OpenID にはいくつかの拡張使用があり、OpenID Attribute Exchange AX は属性交換のための拡張方針である。本発表では AX を利用し、OAuth を効率良く組み込む方式を開発した。ちなみに OAuth とは、トークンを利用することで認証を必要とせず、ユーザの同意のもとに API へのアクセス権を得るものである。

・ OpenID における ID 継続の提案 (理科大)

ユーザ認証を一元管理して行うシングルサインオンにおいて、認証サーバが停止した場合、ID やサービスを継続して利用できなくなる問題がある。本発表では、認証サーバ A から予備とする認証サーバ B に ID と検証のための情報を渡し、認証サーバ A 停止後に認証サーバ B

- からサービスにそれらの情報を提示することで、ID とサービスの継続利用を可能としている。
- ・ 端末プラットフォーム技術における認証手法（KDDI 研究所）
端末プラットフォーム技術における端末プラットフォームサーバ群での認証として、既存の Web ベースのシングルサインオン技術で運用可能な認証手法の構成についての発表である。

(5) SCIS（暗号と情報セキュリティシンポジウム）2011

暗号と情報セキュリティシンポジウム SCIS は毎年 1 月に開催されている。2011 年は 1 月 25 日 - 28 日に小倉で開催された。IdM に関する発表は以下の 3 件があった[45]。今回の調査研究に直接合致する研究発表はなかった。

- ・ クロスドメインロールベースアクセス制御におけるユーザロール関係記述（奈良先端大）
- ・ 認証サーバ選択方針による OpenID フィッシング対策の検証（早稲田大学）
- ・ Multi-trapdoor commitment に基づくデジタル置換から ID ベース認証へ（東京電機大学）

(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

＜課題と提言＞第 3 回 シンポジウム

情報法の専門家、堀部政男一橋大学名誉教授の名を冠した研究会が主催するシンポジウムである。第 1 回、第 2 回は法的、制度的な課題について講演があった。第 3 回は技術についての講演が OpenID Foundation 理事長で野村総合研究所の崎村夏彦氏、独立行政法人産業技術総合研究所の高木浩光氏により行われた[46]。

崎村氏の講演で「アイデンティティ・エコシステム」について触れた。アイデンティティエコシステムは、2010 年 6 月にドラフトが公開され、パブリックコメントに附された米国の”National Strategy for Trusted Identities in Cyberspace”で使われている[13][47]。

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。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と考える。

2.3.3 企業、大学における開発

(1) 指静脈認証クラウドサービス

株式会社日立製作所のソリューションでは、キャンセル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。

従来のサーバ管理下での生体認証では、クライアントから送信されるバイオメトリック情報は暗号化されており、サーバに保管されているバイオメトリック情報も暗号化されている。しかし、照合には復号を必要とし、再度の暗号化とともにセキュリティ上のボトルネックとなっていた。

本ソリューションでは、図 2.3.1 に示すように、サーバ格納の暗号化生体情報をクライアント側が不可逆に暗号化した生体情報とそのまま照合することが可能である。

また、もし情報が漏洩しても、図 2.3.2 に示すように、変換パラメータを更新することで対応可能である。更新は、新しい変換パラメータと古い変換パラメータの差分パラメータを用いて、サーバに格納した暗号化生体情報を再暗号化する。以降は新パラメータで暗号化した生体情報をクライアントからサーバに送信して照合を行う。

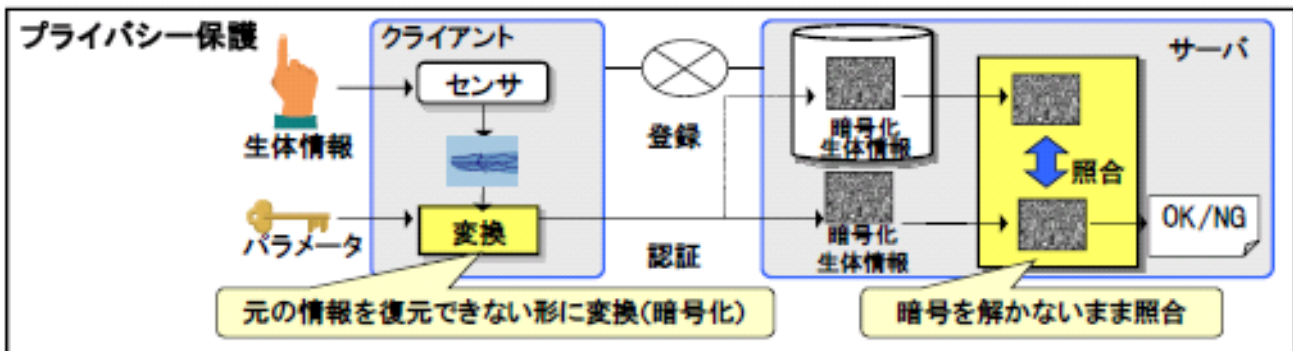


図 2.3.1 暗号化生体情報の照合

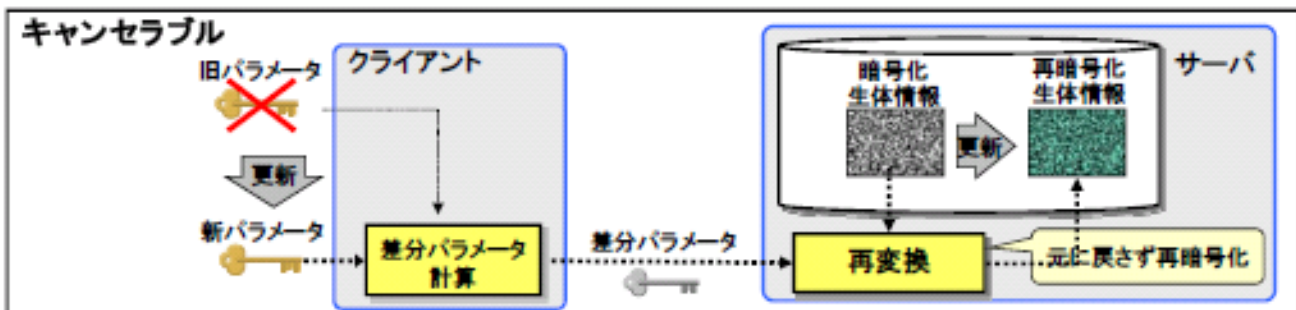


図 2.3.2 変換パラメータの更新

キャンセルラブルバイオメトリック技術を工夫し展開したソリューションであるが、利用できるモダリティが限定されること、性能の評価などが困難であること、他の方式、例えば、標準化さ

れた暗号技術、OpenID などのアーキテクチャとの比較が不明確であり、競合する技術との優位性を明確にするのが今後の課題である。

(2) クラウドと指静脈による統合認証システム

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である。図 2.3.3 に示すように、同大学では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いる[49]。

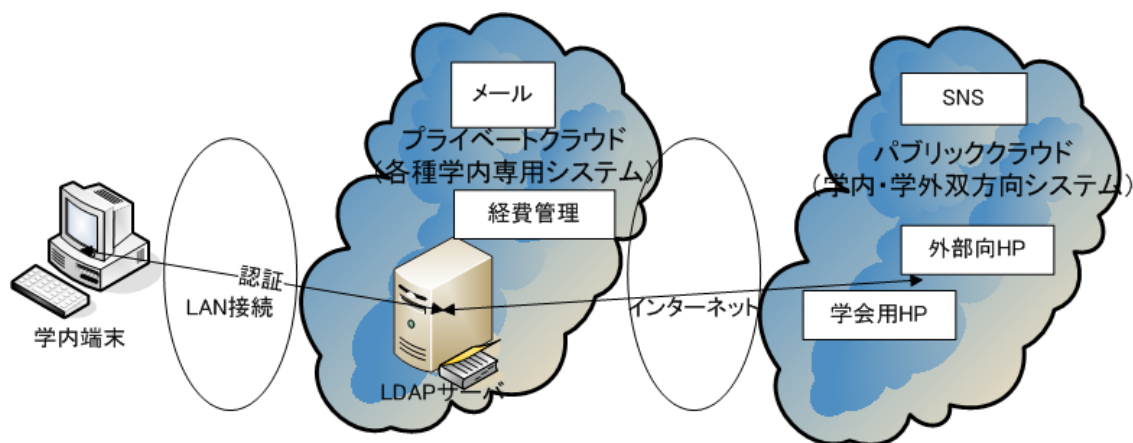


図 2.3.3 静岡大学のクラウド認証

LDAP (Lightweight Directory Access Protocol) は ITU-T 勧告の X.500 ディレクトリサービスをベースに開発された、ネットワーク機器やユーザなどの情報を管理するディレクトリサービスへ接続するためのプロトコルである[50]。ディレクトリサービスは、ネットワークに存在する様々な情報を一元的に管理し、検索などの機能を提供するプログラムである。

クライアントは、LDAP サーバに接続し、属性で構成されるエントリ（関連する属性のまとまり）の検索、追加、削除、修正といった操作を行う。複数サービスのユーザ ID とパスワードを、1人のユーザ ID の属性としてまとめると各サービス（プログラム）は LDAP サーバのみを参照して認証作業ができるようになる。管理者も一元的に情報を管理できることから、サービスそれぞれのディレクトリでユーザ情報を変更するといった手間を削減できる。

情報システムへのログイン管理と入退室管理システムが LDAP サーバを参照して指静脈認証を利用できるようにしたものが静岡大学の BIDM である。

2.4 まとめ

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多岐にわたっている。

ISO/IEC JTC1/SC27 と SC37 で、アイデンティティ管理に関係する標準が 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) が重要と考える。

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、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。

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) であり、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おり、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。

調査研究活動に関しては、海外では 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ことがわかった。

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)、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。

調査結果をまとめたレポートが NSTC のウェブサイト公開されているが、レポートの内容は概念的であり、具体的な主張を理解分析するには、更に詳細な資料が必要であると考えられる。

また、従来 DOD 内にバイオメトリクスについて調査・研究するタスクフォースを設置されていたが、2010 年 3 月、恒久的な組織として The Biometrics Identity Management Agency (BIMA) が設置された。アイデンティティ管理は、複数の組織で、異なる視点で開発、運用されているため、BIMA のような組織で情報を共有・調整することは意義あると考える。

更に、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。

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。NSTIC は国土安全保障省 DHS で公開されており、政権がサイバーセキュリティを物理的なセキュリティと同等、あるいはそれ以上に重視し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る。

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含む、幅広い隣接領域を調査研究の対象としている。最近の代表的なプロジェクトは、以下のとおりである。

(1) primelife

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 (Privacy and Identity Management for Community Services)

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 (Secure Widespread Identities for Federated Telecommunications)

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 (Future of Identity in the Information Society)

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 (Privacy and Identity Management for Europe)

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 (Government User IDentity for Europe)

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

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。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、(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、日本国内のプロジェクトは、開発ベースではなく、調査ベースであり、以下のとおりである。

(1) 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。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) 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。

(3) JSAアイデンティティ管理技術の標準化調査研究委員会

「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。

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として、(1) カンターラ・イニシアティブ・技術セミナー2010、(2) OpenID Tech Night Vol.6、(3) 平成22年度情報処理技術セミナー Shibboleth 環境の構築、(4) CSS（コンピュータセキュリティシンポジウム）2010、(5) SCIS（暗号と情報セキュリティシンポジウム）2011、(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。

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OMETリック技術を利用し、同社がクラウド環境下で生体認証サーバの運用・管理を行いユーザに認証サービスを提供するソリューションを開発し、公開している。

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。

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

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と考える。

第3章 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

3.1 検討の進め方

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を進めるにあたり、方式検討の基本方針について整理することとした。以後の具体的な検討は、ここで整理する基本方針にしたがって行うこととした。

3.1.1 基本方針

IdM アーキテクチャにバイオメトリック認証を組み込む場合、重要と考えられるポイントを以下に示す。

(1) 高い汎用性

本プロジェクトで検討するバイオメトリック認証用アーキテクチャは、特定の IdM の方式に依存したものであってはならない。IdM として考えられている様々な IdM システムのどれ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を基本方針の一つとした。

例えば Web アプリ応用型の IdM システムとして OpenID や SAML (Liberty Alliance) といった異なる仕様が存在するが、今回検討するアーキテクチャはどちらの仕様にも適用可能であり、バイオメトリックシステムとしての性能は同等相当であることが重要である。

(2) バイオメトリックスの特性の考慮

本人認証技術の一種であるパスワードや IC カードなどと比べて、バイオメトリック認証にはいくつかの固有の特性がある。本プロジェクトで検討するアーキテクチャは、バイオメトリックスの特性を考慮し、それを設計に反映させたものでなければならない。バイオメトリックスの主な特性を以下に示す。

①技術の多様性

バイオメトリックスでは人間の体の部位の身体的特徴や行動的特徴を用いて本人認証を行う。認証において必要となる要素は以下のとおり多岐に渡る。

人体の部位の多様性：指紋の特徴、顔の形状、虹彩パターン、指や手のひらの静脈が作り出す影の模様、声の特徴、署名の形状など、様々な人体の部位の形状あるいは部位の振る舞いが作り出すパターンを用いた認証方式が存在している。

- ・装置の多様性：各部位ごとに生体情報を取得する装置にも様々な方式が存在しており、方式やセンサーの特性によって同じ部位の情報取得でもデータの一部（あるいは全体）が方式によって異なる場合が存在する。

- ・アルゴリズムの多様性：生体情報は取得された後アルゴリズムによって処理される（このことを本章ではコード化と呼ぶこととする）。登録処理や認証処理では取得された生体情報をアルゴリズムによってコード化することが一般的に行われており、アルゴリズムが生体情報をコード化すると、認証に有効な情報だけが抽出されコンパクトなデータ形式に変換される。このコード化の方法はアルゴリズムごとに異なるため、二つのアルゴリズムにデータの互換性がない場合、一つのアルゴリズムでコード化した情報を他のアルゴリズムで用いることはできない。また、認証性能もアルゴリズムによって異なるのが一般的である。

②認証精度

認証精度とはバイOMETリックシステムの性能を表す尺度である。この認証精度には代表的なものに本人拒否率（FRR：False Rejection Rate）や他人受け入れ率（FAR：False Accept Rate）などがあり、これらの認証精度によってシステムの利便性やセキュリティの高さが左右されることから、バイOMETリックシステムにおける最も重要な性能尺度といえる。

この認証精度は確率で表現されるのが一般的である。これは、バイOMETリクスが生身の人体を取り扱うことから同じ人が同じセンサーを用いて生体情報の取得を行ったとしても、取得される情報にはばらつきが生じることによるものである。本人拒否や他人受け入れは確率的に発生することから、その数値化においては統計的な手法がとられることが一般的である。

この認証精度は以下の理由からそれを決定する因子が更に多数存在しており、精度評価の方法や評価結果は慎重に取り扱う必要がある。

- ・環境の影響：環境光、温度、湿度、背景音など装置周辺の環境によって精度が変化する。
- ・利用者の違い：利用者の年齢層、性別、体質、職業、文化的な違い、協力的か否かなど様々な要因で精度が変化する。
- ・脆弱性対策の影響：生体検知（偽造防止技術）、テンプレート保護技術、暗号化などバイOMETリック認証における様々な脆弱性対策の影響により認証精度が変化する可能性がある。
- ・ヒューマンインタフェースの影響：利用者に対して画面や光、音などを用いたガイダンスを出すことが一般的に行われている。ヒューマンインタフェースの方法によって認証精度が変化する可能性がある。
- ・センサーやアルゴリズムの改良・変更の影響：同一の製品であってもセンサーを構成する部品の変更や改良、また、認証用アルゴリズムの変更や改良が精度の変動要因となる。

バイOMETリック技術を実装した IdM アーキテクチャの検討にあたっては、この精度評価の取り扱いについての考慮が不可欠であると考ええる。

③ プライバシー

バイOMETリック情報は究極の個人情報ともいわれるものであり、漏洩や偽造などが発生した場合のプライバシー問題が懸念される。

IdM アーキテクチャの検討にあたりプライバシーへの考慮が不可欠であると考える。

(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た。この結果、個々のシステムコンポーネントも Web 技術を用いて構築されるように変化してきている。OpenID や SAML (Liberty Alliance) などといった IdM システムも Web 技術を前提として設計されている。このような状況を踏まえて、本調査研究で検討する IdM へのバイオメトリクスを組み込みにおいても、Web 技術と高い親和性を有することが重要な条件となる。

3.1.2 関連する国際標準規格

バイオメトリクスのインタフェースに関わる国際標準規格は ISO/IEC JTC1/SC37 で 2002 年から審議されており、現在様々なインタフェース規格が国際標準化を完了している。また、新しい規格提案も登場しつつある。

バイオメトリック技術を実装した IdM アーキテクチャの検討の推進にあたっては、ISO/IEC JTC1/SC37 の国際標準規格（現在審議中のものも含む）を IdM システムに取り込むこととし、その中で前述の 3.1.1 項で示した検討方針で示した要求事項を満たしているかどうか評価・検討することとした。検討対象とした国際規格として以下のとおり三つの仕様を挙げる。

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

3.1.3 検討方針

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を進めた際の検討方針を図 3.1.1 にまとめる。

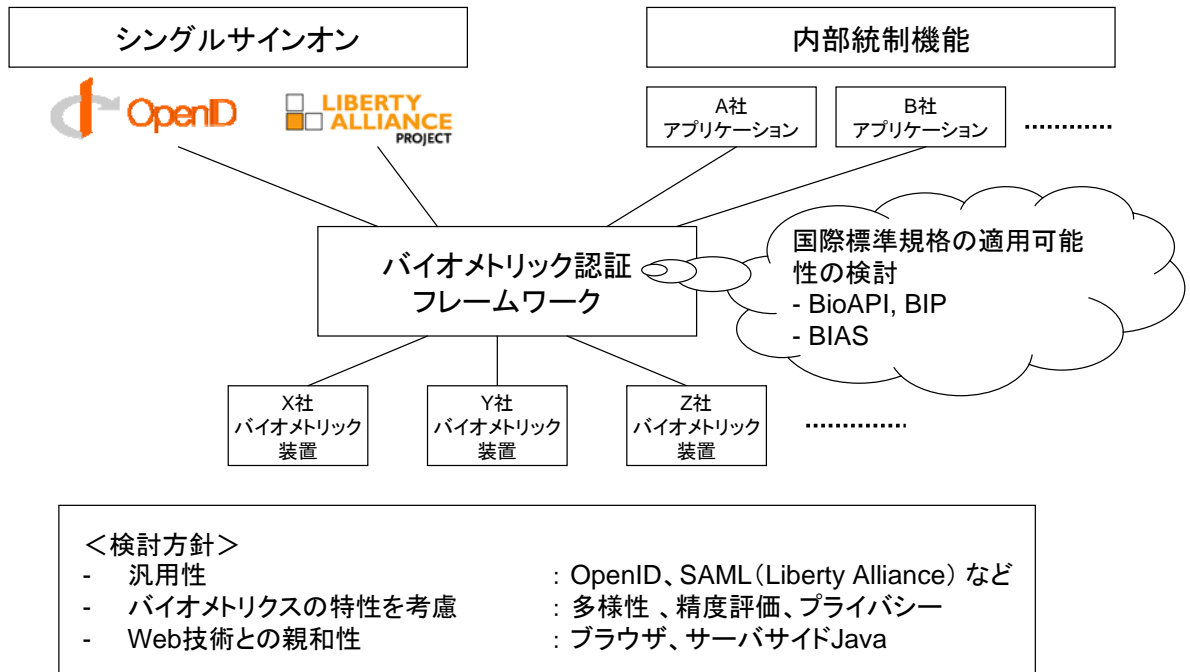


図 3.1.1 検討方針の説明

本図に示すとおり、今回検討するアーキテクチャは上位に Web アプリ応用型アプリケーションである OpenID や SAML (Liberty Alliance)、あるいは IT 内部統制型アプリケーションを配置し、下位に様々なバイオメトリック装置を配置する。

これらのアプリケーションやバイオメトリック装置の中央にバイオメトリック認証フレームワークとして上位及び下位のコンポーネントを接続する役割を果たすものとする。

このバイオメトリック認証フレームワークを実現するためのインタフェースの候補として、国際標準規格である BIAS、BioAPI 及び BIP の採用を検討した。

これらの検討にあたってはその検討方針として、汎用性・バイオメトリクスの特性そして Web との親和性を考慮することとした。

3.2 IdMアーキテクチャの技術調査

本節では、市場において広く用いられている IdM システムを以下の 2 種類に大別して調査を実施した。

(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 2 種類が存在している。

- OpenID: OpenID ファウンデーションにより策定された規格。(主な参加企業は、Facebook、Google、IBM、Microsoft、PayPal、VeriSign、Yahoo!、野村総研など。)
- SAML: OASIS と Liberty Alliance により策定された規格。(主な参加企業は、AOL、BT、CA、Fidelity、Intel、Novell、NTT、Oracle など。)

これら主要な二つの規格の技術調査を実施し、バイオメトリクス組み込みについての検討を行うこととした。

(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。内部統制応用型システムについて機能とともに共通的に用いられる規格の存在の有無について調査を行い、バイオメトリクスの組み込みに関して考察する。

3.2.1 Webアプリ応用型

Web アプリ応用型として OpenID 及び SAML(Liberty Alliance)の 2 種類について調査した結果を示す。

3.2.1.1 OpenID

(1) 主な特徴

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る。

技術的特徴は以下に示すとおりである。

- 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。

(2) 関連規格

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 に関する規格案の一覧を表 3.2.1 に示す。

表 3.2.1 OpenID の主要規格文書一覧

No	規格書
1	OpenID Authentication 2.0
2	OpenID Attribute Exchange 1.0
3	OpenID Provider Authentication Policy Extension 1.0
4	OpenID Simple Registration 1.0 (SREG)
5	OpenID OAuth Extension
6	Yadis Discovery Protocol (OpenID 内部で使用)

(3) 処理シーケンス

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 3.2.1 に示す。

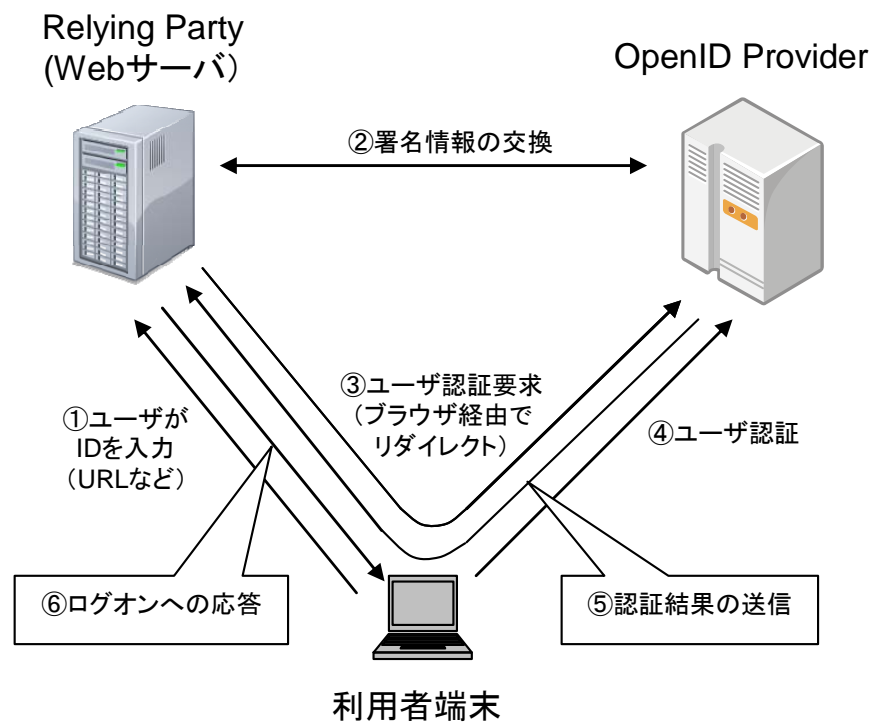


図 3.2.1 OpenID の概略処理シーケンス

- ① ユーザが Web ブラウザから利用者自身の ID 情報を入力する。この際、OpenID プロバイダでのシングルサインオンを要求する場合は、OpenID プロバイダの URL を入力することができる。(この URL に加えて、OpenID プロバイダ上に存在する利用者の ID を URL の一部として入力することもできる。)
- ② Relying Party (一般的には Web サーバ) と OpenID プロバイダの間で署名情報の交換が行われ、セキュアな通信のための事前処理を完了する。
- ③ Relying Party は、ブラウザを介したりダイレクトを用いて認証要求を OpenID プロバイダに発行する。
- ④ OpenID プロバイダが利用者に対してユーザ認証を行う。この際の認証方法としては現状パスワードが一般的である。
- ⑤ OpenID プロバイダは、ブラウザを介したりダイレクトを用いて認証結果を Relying Party に送信する。
- ⑥ Replaying Party は利用者に対して①で行われたログインへの応答を実行する。

(4) バイオメトリクスの組み込みについて

OpenID 規格へのバイオメトリクスの組み込みの検討にあたっては、上記に示した OpenID 関連規格においてバイオメトリクス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、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。

唯一、PAPE (OpenID Provider Authentication Policy Extension) と呼ばれる OpenID の拡張規格の一つの中で、OpenID プロバイダが実行する認証のポリシーを Relying Party 側が事前に要求できるようになっており、その認証ポリシーの一部にバイオメトリクスが含まれているのが現状である。

以下に現 PAPE 規格 (PAPE1.0) において、Relying Party が指定できる 三つの認証ポリシーを示す。

- ① フィッシング耐性認証
- ② 複数要素認証
- ③ 物理複数要素認証

上記の③において、認証手段として以下の記述が存在する。

“at least one of the factors is a physical factor such as a hardware device or biometric”

このように物理複数要素認証における認証方法の一つとしてバイオメトリクスが言及されているが、ハードウェアトークンとの区別が付かない記述となっており、Relying Party からバイオメトリクス認証のみを指定して要求することはできない。

図 3.2.2 に OpenID における認証シーケンスの詳細を示す。

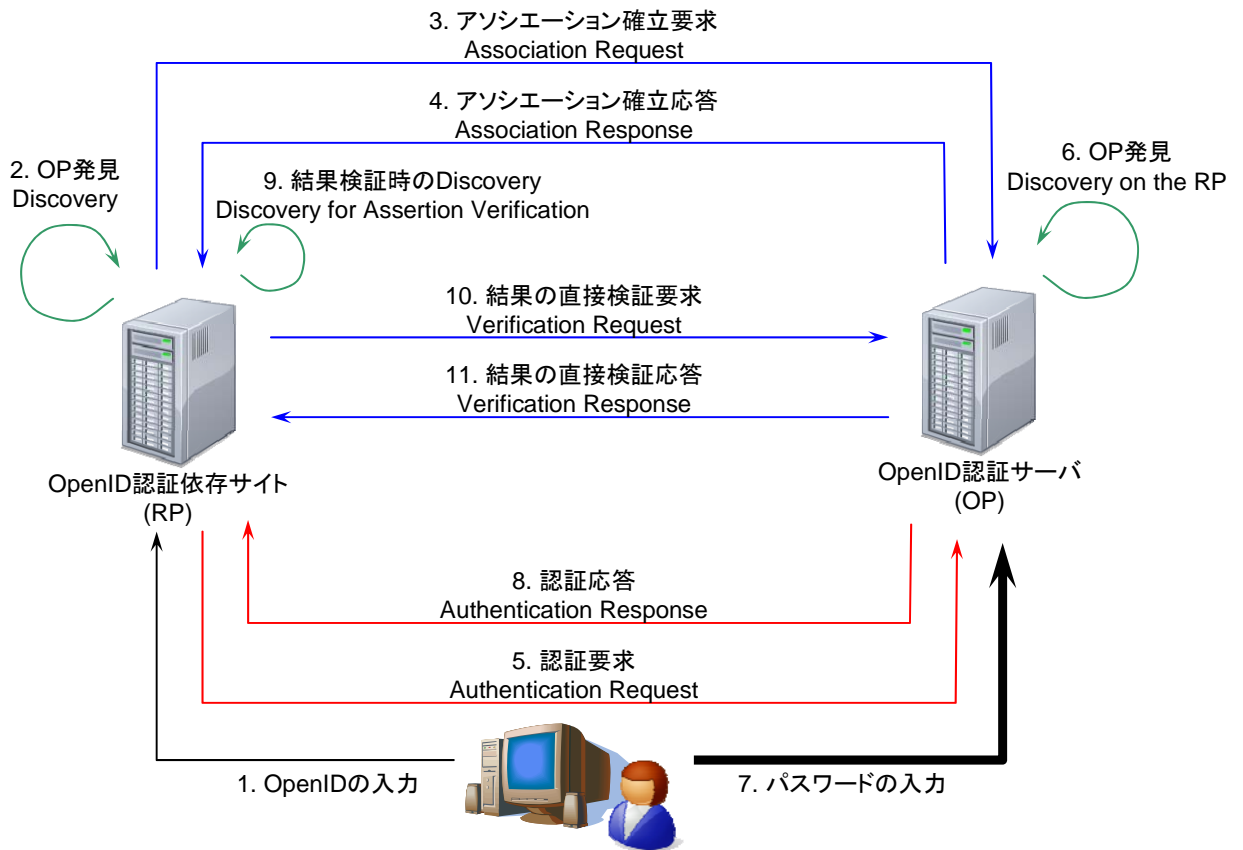


図 3.2.2 OpenID の詳細処理シーケンス

図 3.2.2 において、番号 1 と 7 を除いた部分は OpenID で規格化されており、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OMETRICS 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OMETRICS 認証を組み込める可能性を示唆するものであると考える。

3.2.1.2 SAML (Liberty Alliance)

(1) 主な特徴

OpenID と同様、Web ベースのシングルサインオンなどの本人認証を可能とするための規格である。

- ① SAML と呼ばれる XML 言語による記述方法を採用している (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 (トラストサークルとも呼ばれる)。
- 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。

(2) 関連規格

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。

SAML に関係する規格案の一覧を表 3.2.2 に示す。

表 3.2.2 SAML の主要規格文書一覧

No	規格書
1	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1, V2.0
2	Liberty Alliance ID-FF 1.2 Specifications
3	Liberty Alliance ID-WSF 1.1 Specifications
4	Liberty Alliance ID-WSF Data Services Template v2.0 Specifications
5	Liberty Alliance ID-SIS 1.0 Specifications
6	Identity Assurance Framework Document Repository
7	Liberty Alliance ID-WSF Advanced Client 1.0 Specifications
8	Liberty Alliance Identity Governance Framework (IGF) 1.0 Specifications
9	Liberty Identity Assurance Framework – Service Assessment Criteria v2.0

(3) 概略処理シーケンス

図 3.2.3 に SAML の概略処理シーケンスを示す。

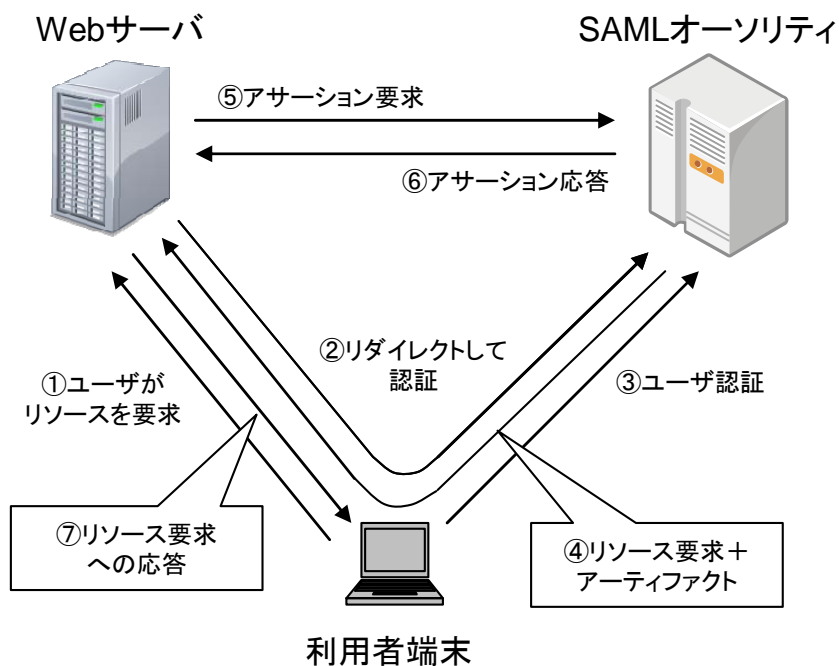


図 3.2.3 SAML の概略処理シーケンス

- ① ユーザが利用者端末のブラウザから利用者自身の ID 情報を入力する。
- ② サービスプロバイダ（一般的には Web サーバ）は HTTP のリダイレクトを使ってブラウザ経由でアイデンティティプロバイダ（SAML オーソリティ）に認証依頼を発行する。
- ③ アイデンティティプロバイダが利用者に対してユーザ認証を行う。この際の認証方法としては現状パスワードが一般的である。認証結果は SAML アサーションとしてアイデンティティプロバイダ内に保持される。
- ④ アイデンティティプロバイダは、ブラウザを介したリダイレクトを用いて認証結果をアーティファクトとしてサービスプロバイダに送信する（アーティファクトは、SAML アサーションを一意に識別するデータ量の少ない一種のトークンである）。
- ⑤ サービスプロバイダはアイデンティティプロバイダに対して SAML アサーションを要求する。この際、④で取得したアーティファクトを指定する。
- ⑥ アイデンティティプロバイダは、要求された SAML アサーションをサービスプロバイダに送信する。
- ⑦ サービスプロバイダは取得した SAML アサーションを確認し、利用者に対して①で行われたリソースへの応答を実行する。

(4) 詳細処理シーケンス

図 3.2.4 に SAML の詳細処理シーケンスを示す。

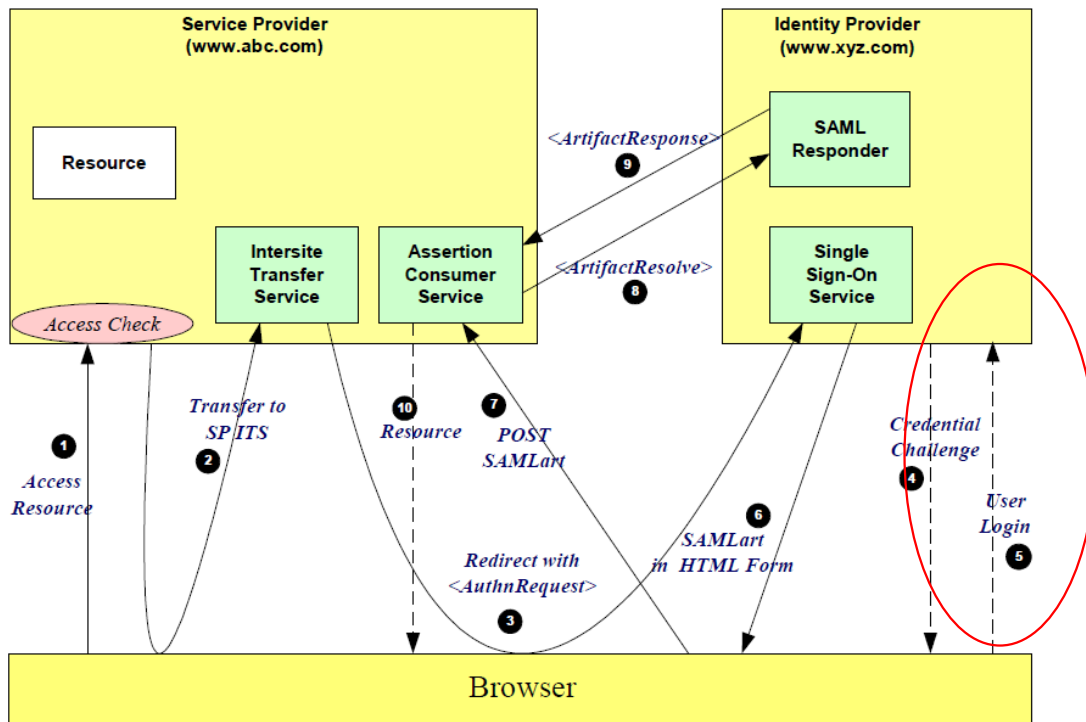


図 3.2.4 SAML の詳細処理シーケンス

- ① 利用者がサービスプロバイダ（www.abc.com）のリソースへのアクセスを試みる。その時点でユーザはまだログオンしていない。
- ② アプリケーションはサイト間の転送サービスに要求を発行する。この要求の中ではアイデンティティプロバイダの URL も含める（www.xyz.com）。
- ③ サイト間転送サービスは、ブラウザに HTTP リダイレクトメッセージを送信する。HTTP ヘッダにはアイデンティティプロバイダが提供するシングルサインオンサービスを示す URI が含まれる。これと合わせて、SAMLRequest と一般的に称されるクエリ変数として <AuthnRequest> というエレメントも送られる。
- ④ シングルサインオンサービスは、アイデンティティプロバイダにおいて現在ユーザがログイン中か、あるいはそのユーザに対して認証が必要かをチェックする。そのユーザへの認証が必要な場合は、実際の認証情報の提示が利用者に対して要求される。
- ⑤ 利用者は認証情報を提示し、ログイン状態となる。
- ⑥ シングルサインオンサービスは利用者のためのアサーションを生成し、合わせてアーティファクトを生成する。そしてブラウザに対して SAML アーティファクトを含んだメッセージを HTTP メッセージとして送信する。

- ⑦ アサーション消費サービス (Assertion Consumer Service) はこのHTTPメッセージを受け取ると、SAMLアーティファクトに含まれるソースIDと呼ばれる情報を取り出す。このソースIDにはアイデンティティプロバイダのURL情報 (www.xyz.com) に結びついており、アサーション消費サービスは、www.xyz.comにアクセスする必要があることを認識する。
- ⑧ www.abc.comのアサーション消費サービスは<ArtifactResolve>というSAMLメッセージをアイデンティティプロバイダに送信する。このメッセージにはアイデンティティプロバイダが生成したSAMLアーティファクトが含まれる。
- ⑨ SAML 応答者は<ArtifactResponse>メッセージを返却する。このメッセージにはすでに生成されているアサーションが含まれる。
- ⑩ アサーション消費サービスはブラウザに対して要求されたリソースを提供する。

本シーケンスの破線部分は SAML の規格外でありこれには④や⑤で示される認証部分が含まれる。したがって、バイオメトリクス認証も規格外であり SAML の規格そのものに直接影響を与えずに実装が可能と考える。

(5) バイオメトリクスの組み込みについて

規格書の内容を調査したが SAML 規格においてバイオメトリクス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。表 3.2.3 に現状 SAML で定義されている認証方法の一覧を示す。

(Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0 の 7.1 Authentication Method Identifiers より)

表 3.2.3 SAML で定義されている認証方法の一覧

No	認証方法
1	パスワード
2	Kerberos
3	セキュアレポートパスワード (SRP)
4	ハードウェアトークン
5	SSL/TSL に基づくクライアント認証
6	X.509 公開鍵
7	PGP 公開鍵
8	SPK 公開鍵
9	XKMS 公開鍵
10	XML デジタル署名
11	指定なし

3.2.2 内部統制応用型

(1) 主な特徴

内部統制応用型の IdM システムは、主に表 3.2.4 の特徴を有するものである。

表 3.2.4 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"> ・業務の有効性と効率性 ・財務報告の信頼性 ・関連法規の遵守 ・資産の保全
2	構成要素	<ul style="list-style-type: none"> ・統制環境 ・リスクの評価と対応 ・統制活動 ・情報と伝達 ・モニタリング ・IT への対応
3	関連する法律・法令	<ul style="list-style-type: none"> ・SOX 法（日本版 SOX 法） ・会社法 ・金融取引法

また、内部統制を共通的に表すフレームワークとして図 3.2.5 に示す機能ブロックでの表現が行われている。

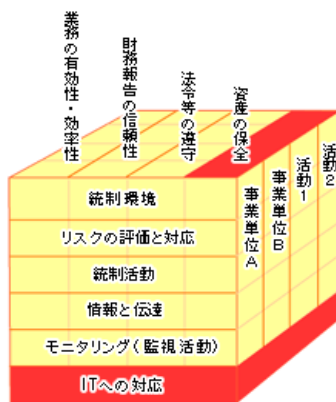


図 3.2.5 内部統制機能ブロック

＜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。

(2) 関連規格

前述 3.2.1 項で示した Web アプリ応用型とは異なり、内部統制応用型の IdM システムには OpenID や SAML に相当する共通規格が現時点で存在していない。

このため、Web アプリ応用型で示したような共通の処理シーケンスも存在しない。

(3) バイオメトリクスの組み込みについて

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する。

3.3 国際規格技術調査

本節では関連する国際規格についての技術調査結果をまとめる。

以下の三つの国際標準規格を調査対象とする。

① BioAPI 規格 (Biometric Application Programming Interface) :

ISO/IEC 19784-1:

2006 (2006 年国際規格化完了)

② BIP 規格 (BioAPI Interworking Protocol) :

ISO/IEC 24708:2008 (2008 年国際規格化完了)

③ BIAS 規格 (Biometric Identity Assurance Services) :

ISO/IEC 30108 (2011 年に新規プロジェクトとして発足。米国提案。)

3.3.1 BioAPI規格

(1) 主な特徴

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 3.3.1 のとおりアプリケーション、BioAPI フレームワーク、BSP (Biometric Service Provider) の 3 階層で構成される。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 の本体部分であり、BSP は個々のバイオメトリック技術の依存部分であり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。

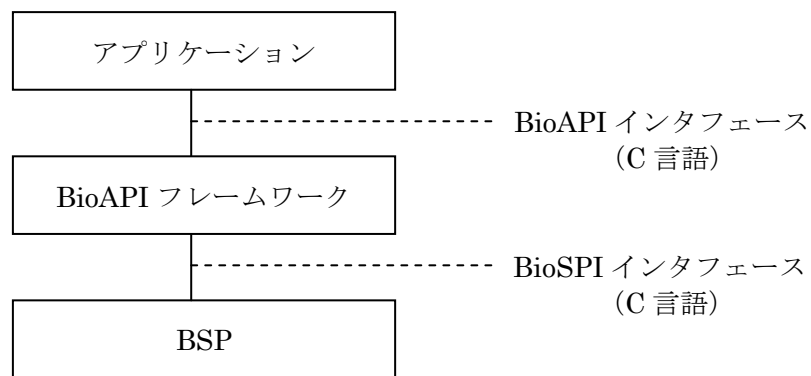


図 3.3.1 BioAPI のソフトウェア構成

(2) 機能

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。BioAPI が提供する関数には大別して以下の 2 種類が存在している。

① 単純関数

生体情報の取得、1:1 照合、1:N 照合などといった単純なバイオメトリック機能を定義したものである。アプリケーションはこれらの単純な関数を一つずつ組み合わせて呼び出すことにより、バイオメトリック認証システムを実現することができる。

以下に主な単純関数を示す。

- BioAPI_Capture : 生体情報の取得
- BioAPI_CreateTemplate : 登録用生体情報 (テンプレート) の生成
- BioAPI_Process : 照合用生体情報の生成
- BioAPI_VerifyMatch : 1:1 照合の実行
- BioAPI_IdentifyMatch : 1:N 照合の実行

② 組合せ関数

上記①の単純関数を組み合わせた関数であり、アプリケーションの開発負荷を軽減するものである。これらの関数群は一般的にスタンドアロン環境での利用が想定されており、クライアントサーバシステムなどのネットワーク環境での適用はできない。以下の三つの組合せ関数が定義されている。

- BioAPI_Enroll : 生体情報の取得 (BioAPI_Capture) と登録用生体情報の生成 (BioAPI_CreateTemplate) の組合せ
- BioAPI_Verify : 生体情報の取得 (BioAPI_Capture) と照合用生体情報の生成 (BioAPI_Process) と 1:1 照合の実行 (BioAPI_VerifyMatch) の組合せ
- BioAPI_Identify : 生体情報の取得 (BioAPI_Capture) と照合用生体情報の生成 (BioAPI_Process) と 1:N 照合の実行 (BioAPI_IdentifyMatch) の組合せ

(3) 関数一覧

BioAPI で定義されている主な関数を表 3.3.1 に示す。

表 3.3.1 BioAPI の主な関数と機能概要

分類	関数名	機能概要
コンポーネント 管理関数	BioAPI_Init	BioAPI 本体を初期化する。
	BioAPI_Terminate	BioAPI 本体を終了する。
	BioAPI_EnumBSPs	BSP スキーマと呼ばれる BSP の属性情報を問い合わせる。
	BioAPI_BSPLoad	BSP をメモリにロードし初期化する。
	BioAPI_BSPAttach	BSP とアプリケーションの関係を確立する。 戻り値として BSP ハンドルを返却する。
ハンドル関数	BioAPI_GetBIRFromHandle	BIR を返却する。
	BioAPI_FreeBIRHandle	BIR を解放する。
コールバック・ イベント関数	BioAPI_EnableEvents	バイオメトリクス装置の挿入・削除・生体情報有無などイベント通知の設定を行う。
	BioAPI_SetGUICallbacks	登録・照合中に BSP が表示する画面の代わりにアプリケーションが画面表示を行うためのコールバックを登録する。
バイオメトリック関数	BioAPI_Enroll	生体情報を取得し、登録コードを生成する。
	BioAPI_Verify	生体情報を取得し、登録コードとの 1:1 照合を実行する。
	BioAPI_Identify	生体情報を取得し、登録コードとの 1:N 照合を実行する。
	BioAPI_Capture	生体情報を取得する。生体情報の取得方法として登録データ用か照合データ用かのいずれかを指定する。
	BioAPI_CreateTemplate	登録コード用 BIR を生成する。
	BioAPI_Process	照合コード用 BIR を生成する。
	BioAPI_VerifyMatch	1:1 照合を実行する。
	BioAPI_IdentifyMatch	1:N 照合を実行する。
データベース 関数	BioAPI_DbOpen	データベースをオープンする。
	BioAPI_DbClose	データベースをクローズする。
	BioAPI_DbStoreBIR	データベースに BIR を保存する。
	BioAPI_DbGetBIR	データベースから BIR を取り出す。

3.3.2 BIP規格

(1) 主な特徴

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 3.3.2 に BIP のシステム構成図を示す。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。

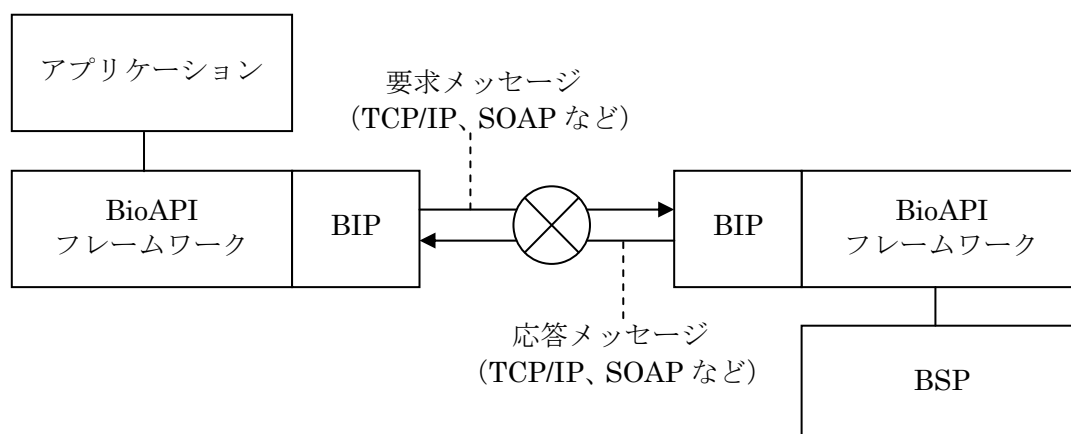


図 3.3.2 BIP のシステム構成

(2) 機能

BioAPI がサポートする関数と同様の機能を有しており、前述 3.3.1 で述べた 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。

(3) メッセージ一覧

BIP で定義されている主なメッセージの一覧を表 3.3.2 に示す。

表 3.3.2 主な BIP メッセージと機能概要

分類	BioAPI 関数名	対応する BIP メッセージ
コンポーネント 管理関数	BioAPI_Init	なし
	BioAPI_Terminate	masterDeleteEvent 通知メッセージ
	BioAPI_EnumBSPs	なし
	BioAPI_BSPLoad	bspLoad 要求及び応答メッセージ
	BioAPI_BSPAttach	bspAttach 要求及び応答メッセージ
ハンドル関数	BioAPI_GetBIRFromHandle	getBIRFromHandle 要求及び応答メッセージ
	BioAPI_FreeBIRHandle	freeBIRHandle 要求及び応答メッセージ
コールバック・イ ベント関数	BioAPI_EnableEvents	
	BioAPI_SetGUICallbacks	GUI 専用の要求及び応答メッセージ群
バイオメトリック 関数	BioAPI_Enroll	enroll 要求及び応答メッセージ
	BioAPI_Verify	verify 要求及び応答メッセージ
	BioAPI_Identify	identify 要求及び応答メッセージ
	BioAPI_Capture	capture 要求及び応答メッセージ
	BioAPI_CreateTemplate	createTemplate 要求及び応答メッセージ
	BioAPI_Process	process 要求及び応答メッセージ
	BioAPI_VerifyMatch	verifyMatch 要求及び応答メッセージ
	BioAPI_IdentifyMatch	identifyMatch 要求及び応答メッセージ
データベース関 数	BioAPI_DbOpen	dbOpen 要求及び応答メッセージ
	BioAPI_DbClose	dbClose 要求及び応答メッセージ
	BioAPI_DbStoreBIR	dbStoreBIR 要求及び応答メッセージ
	BioAPI_DbGetBIR	dbGetBIR 要求及び応答メッセージ

3.3.3 BIAS規格

ISO/IEC JTC1/SC37 に 2010 年に米国から新規提案され、発足したプロジェクトである（プロジェクト番号：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。以下に調査結果を示す。

3.3.3.1 概要

バイオメトリックシステムのためのインタフェースとして米国の OASIS（XML の共通規格を策定）と INCITS M.1（バイオメトリックスの共通規格を策定）の二つの組織が共同で策定した規格案である。以下に BIAS の主な特徴を示す。

- 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（別の規格として Web サービスへの適用ケースを示す）。
- 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 システムの構成図を図 3.3.3 に示す。

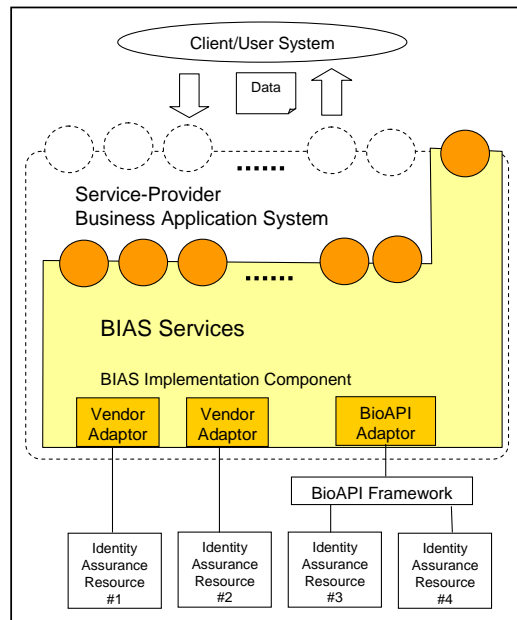


図 3.3.3 BIAS のシステム構成

図 3.9 に示すとおり、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。

3.3.3.2 詳細調査結果

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る。このことから、BIAS 規格について詳細な調査を実施した。以下に BIAS の主な特徴を示す。

(1) 2 種類のサービスが存在する

BIAS は内部に以下の 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。

- ・ Primitive サービス : BIAS としてサポートすべき基本的なサービスを集めたものである。
- ・ Aggregate サービス : Primitive サービスに比べて集約的で複合的なサービスである。BIAS の実装においては、Aggregate サービスを複数の Primitive サービスから実現することもできる。

(2) XML に基づく規格

BIAS は XML の標準化を推進する OASIS が INCITS と共同で策定した規格であり、具体的なサービスの提供形態として XML を用いた SOAP が想定されている。Web アプリ応用型の IdM の一つである SAML も XML で記述されることから、BIAS は SAML との親和性が高いことが予想される。

(3) サーバ認証のみ

BIAS で提供する機能は全て遠隔地からの操作に限定されており、バイオメトリック認証は必然的にサーバ認証のみとなる（端末側での認証は BIAS 規格の規定対象外。）

(4) バイオグラフィック情報管理機能を持つ

BIAS はデータベース内にバイオメトリック情報（利用者の体の部位のデジタルデータをバイオメトリック装置を用いて取得したもの）と合わせて、バイオグラフィック情報を管理する。バイオグラフィック情報とは、氏名・性別・生年月日などの個人の属性情報に相当するものである。BIAS では表 3.3.3 に示すとおり七つのデータフォーマットがバイオグラフィック NP 提案時に発行された WD 文書に掲載されている。

表 3.3.3 Biographic データフォーマット一覧

データフォーマット	略名	参照 URL	情報の種類
FBI EFTS Type-2 (versions 7.x or earlier)	FBI-EFTS	http://www.fbibiospecs.org/	ASCII
FBI EBTS Type-2 (version 8.x or later)	FBI-EBTS	http://www.fbibiospecs.org/	ASCII
DOD EBTS Type-2	DOD-EBTS	http://www.biometrics.dod.mil/	ASCII
Interpol Implementation of ANSI/NIST-ITL	INT-I	http://www.interpol.int/	ASCII
NIEM	NIEM	http://www.niem.gov/	XML
CIQ xNAL	xNAL	http://www.oasis-open.org/	XML
HR-XML	HR-XML	http://www.hr-xml.org/	XML

BIAS ではこれらのバイオグラフィックデータを読み書きしたり削除したりするためのサービスが提供されている。

前述の SAML との親和性において、SAML における属性オーソリティを BIAS が兼ねる場合、このバイオグラフィック情報を属性オーソリティからの返却値として呼び出し側に提供する。

(5) 内部構成予想図

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 3.3.4 に示す。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と考えられる。

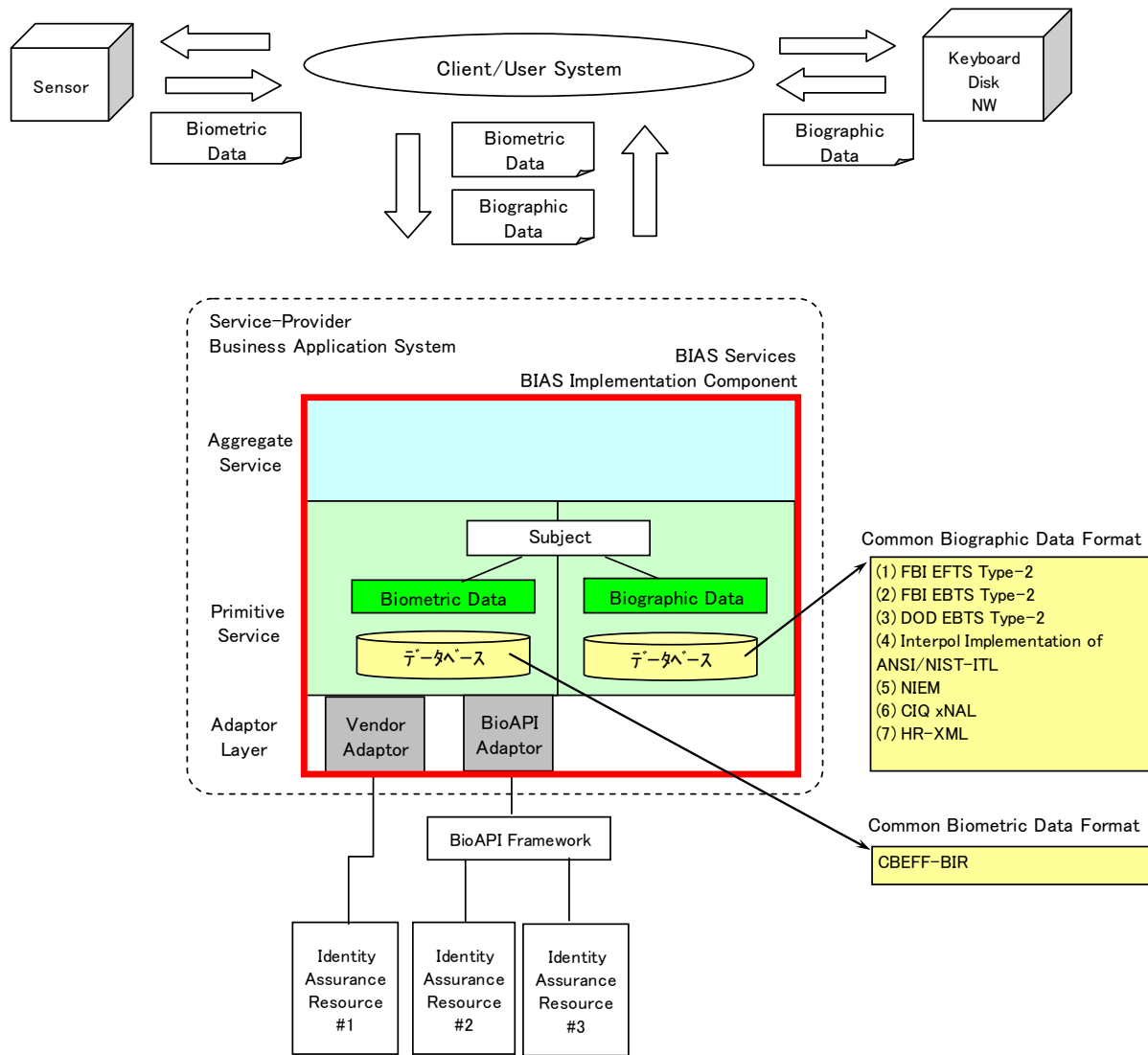


図 3.3.4 BIAS のシステム構成

(6) BIASの機能一覧

以下に BIAS の規格書で定義されている Primitive サービスと Aggregate サービスの機能一覧をそれぞれ表 3.3.4 及び表 3.3.5 に示す。

表 3.3.4 Primitive サービス一覧

No	サービス名	概要
1	Add Subject To Gallery	ギャラリーへのサブジェクトの追加
2	Check Quality	CBEFF-BIR の品質スコアの返却
3	Classify Biometric Data	CBEFF-BIR の分類分け
4	Create Subject	サブジェクトの生成 (Subject ID が返却される)
5	Delete Biographic Data	サブジェクトの個人データを削除
6	Delete Biometric Data	サブジェクトのバイオメトリックデータを削除
7	Delete Subject	サブジェクトの削除
8	Delete Subject From Gallery	サブジェクトをギャラリーから削除
9	Get Identify Subject Results	1:N 照合が非同期だった場合に、照合結果を取得
10	Identify Subject	1:N 照合の実行
11	List Biographic Data	個人データリストの取得
12	List Biometric Data	バイオメトリックデータリストの取得
13	Perform Fusion	マッチスコアを受け付けてフュージョン後の照合結果を返却
14	Query Capabilities	BIAS システムの能力値問合せ
15	Retrieve Biographic Information	個人データの取得
16	Retrieve Biometric Information	バイオメトリックデータの取得
17	Set Biographic Data	サブジェクトへの個人データの設定
18	Set Biometric Data	サブジェクトへのバイオメトリックデータの設定
19	Transform Biometric Data	バイオメトリックデータの変換
20	Update Biographic Data	個人データの更新
21	Update Biometric Data	バイオメトリックデータの更新
22	Verify Subject	1:1 照合の実行

表 3.3.5 Aggregate サービス一覧

No	サービス名	概要
1	Enroll	新しいサブジェクト、あるいは新しい Encounter を追加
2	Get Enroll Results	Enroll サービスの登録結果を取得
3	Get Identify Results	1:N 照合結果の取得
4	Get Verify Results	1:1 照合結果の取得
5	Identify	1:N 照合の実行
6	Retrieve Information	個人情報及び/又はバイオメトリック情報の取得
7	Verify	1:1 照合の実行

(7) SAMLのRequest/Response例

BIAS と同様 XML に基づく IdM 仕様である SAML を例にとって認証のための Request/Response に BIAS を加えた例を図 3.3.5 に示す。

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。

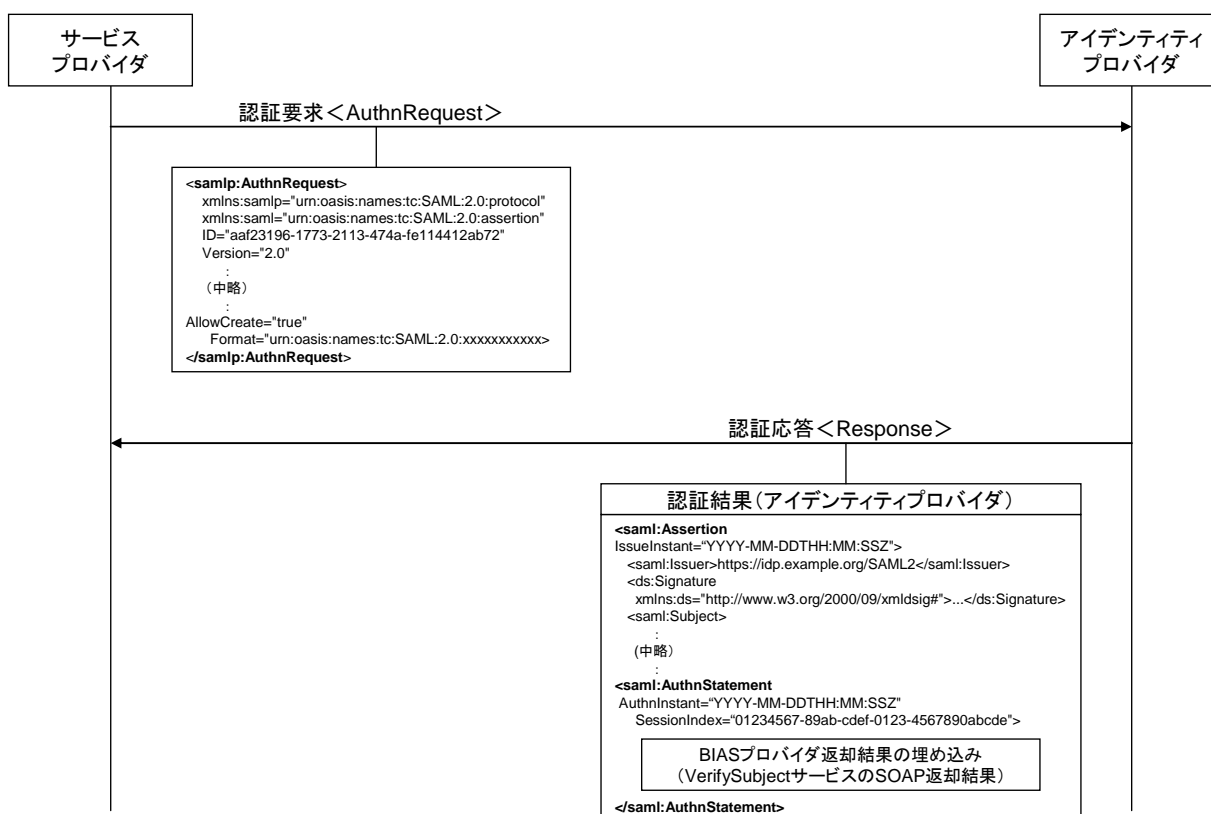


図 3.3.5 SAML メッセージへの BIAS メッセージの組み込み

3.3.3.3 IdMシステムへの組み込みについて

本節では前述までで述べ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。

3.3.3.3.1 パスワード認証シーケンス

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。

<認証手順>

- ① エンドユーザが利用者端末からサービスプロバイダのリソース (URL など) を要求する。
- ② サービスプロバイダは HTTP リダイレクトを用いてアイデンティティプロバイダに自動的に切り替える。
- ③ アイデンティティプロバイダは利用者端末を呼び出してパスワードを取得し、ユーザ認証を行う。
- ④ 認証に成功したらアイデンティティプロバイダは HTTP リダイレクトを用いてサービスプロバイダに自動的に切り替える。この際、リソース要求情報とともにアーティファクトと呼ばれる認証アサーションを間接的に示す情報を渡すことができる。
- ⑤ サービスプロバイダはアイデンティティプロバイダにアーティファクトを渡して認証アサーションを要求する。
- ⑥ アイデンティティプロバイダは、サービスプロバイダに認証アサーションを返却する。
- ⑦ サービスプロバイダは認証アサーションを受け取ったら、利用者端末からのリソース要求に応答する。

図 3.3.6 にパスワード認証手順、図 3.3.7 にパスワード認証時の詳細処理フローを示す。

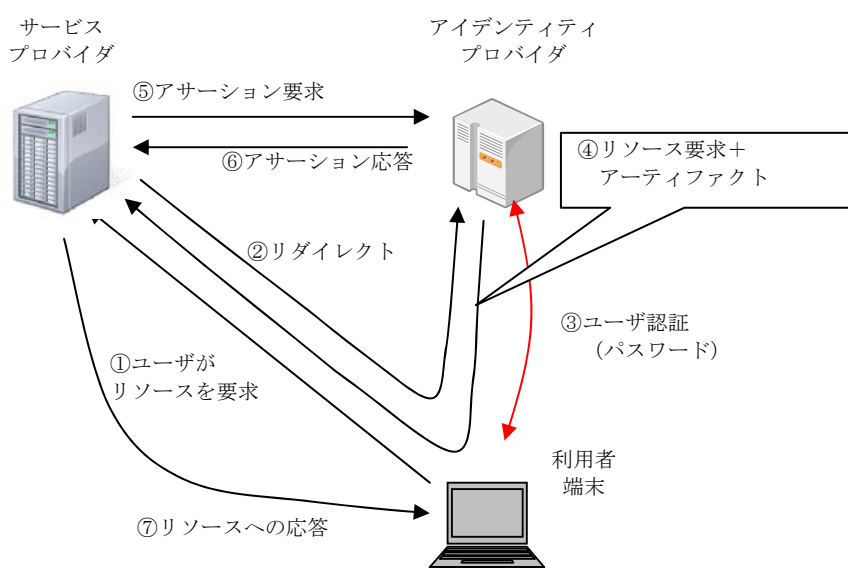


図 3.3.6 SAML でのパスワード認証手順

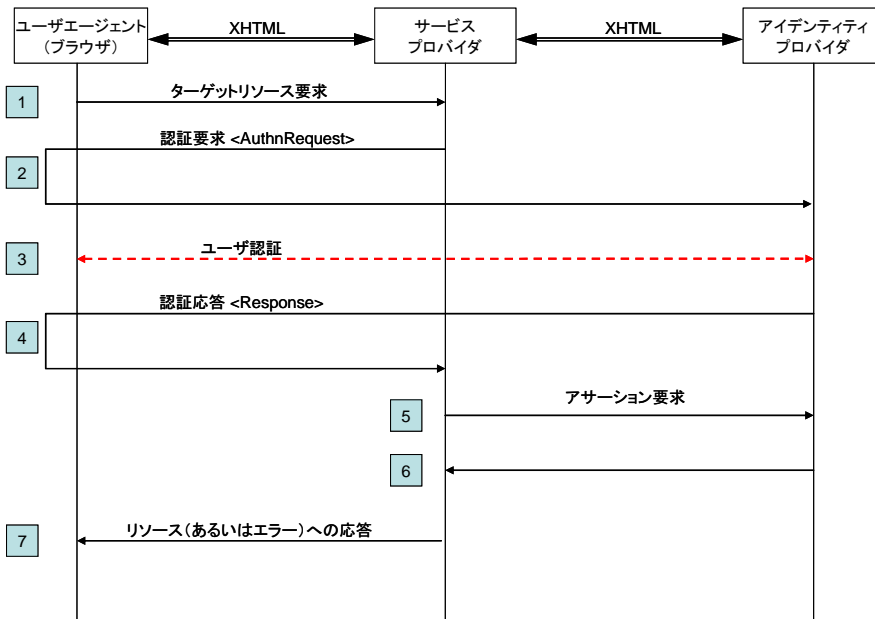


図 3.3.7 パスワード認証時の詳細処理フロー

3.3.3.3.2 バイオメトリック認証シーケンス

パスワード認証にバイオメトリック認証を加える場合の認証手順を示す。

(1) システム構成

バイオメトリック認証を行うためのバイオメト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オメト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オメトリック認証サービスを提供するサーバに送付してバイオメトリック認証依頼を行う。

図 3.3.8 に SAML でのバイオメトリック認証手順（案）を示す。

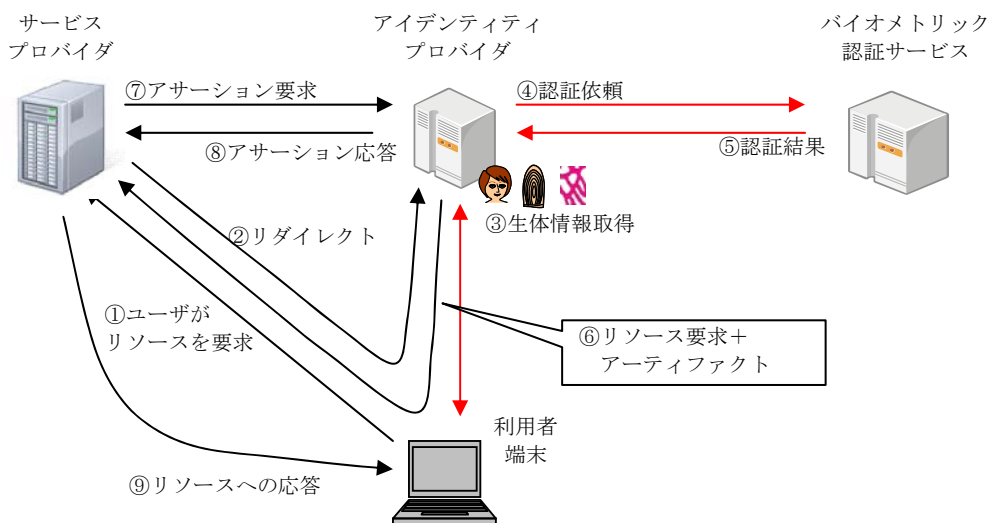


図 3.3.8 SAML でのバイオメトリック認証手順（案）

(2) 認証手順

- ① エンドユーザが利用者端末からサービスプロバイダのリソース（URL など）を要求する。
- ② サービスプロバイダは HTTP リダイレクトを用いてアイデンティティプロバイダに自動的に切り替える。
- ③ アイデンティティプロバイダは利用者端末を呼び出して生体情報の取得を行う。
- ④ アイデンティティプロバイダは取得した生体情報を指定して、BIAS プロバイダに認証依頼（Verify Subject など）を行う。
- ⑤ BIAS プロバイダはバイオメトリック認証を行い、認証結果をアイデンティティプロバイダに返却する（Verify Subject Response）。
- ⑥ 認証に成功したら、アイデンティティプロバイダは HTTP リダイレクトを用いてサービスプロバイダに自動的に切り替える。この際、リソース要求情報とともにアーティファクトと呼ばれる認証アサーションを間接的に示す情報を渡すことができる。
- ⑦ サービスプロバイダはアイデンティティプロバイダにアーティファクトを渡して認証アサーションを要求する。
- ⑧ アイデンティティプロバイダは、サービスプロバイダに認証アサーションを返却する。
- ⑨ サービスプロバイダは認証アサーションを受け取ったら、利用者端末からのリソース要求に応答する。

図 3.3.9 にパスワード認証時の詳細処理フローを示す。

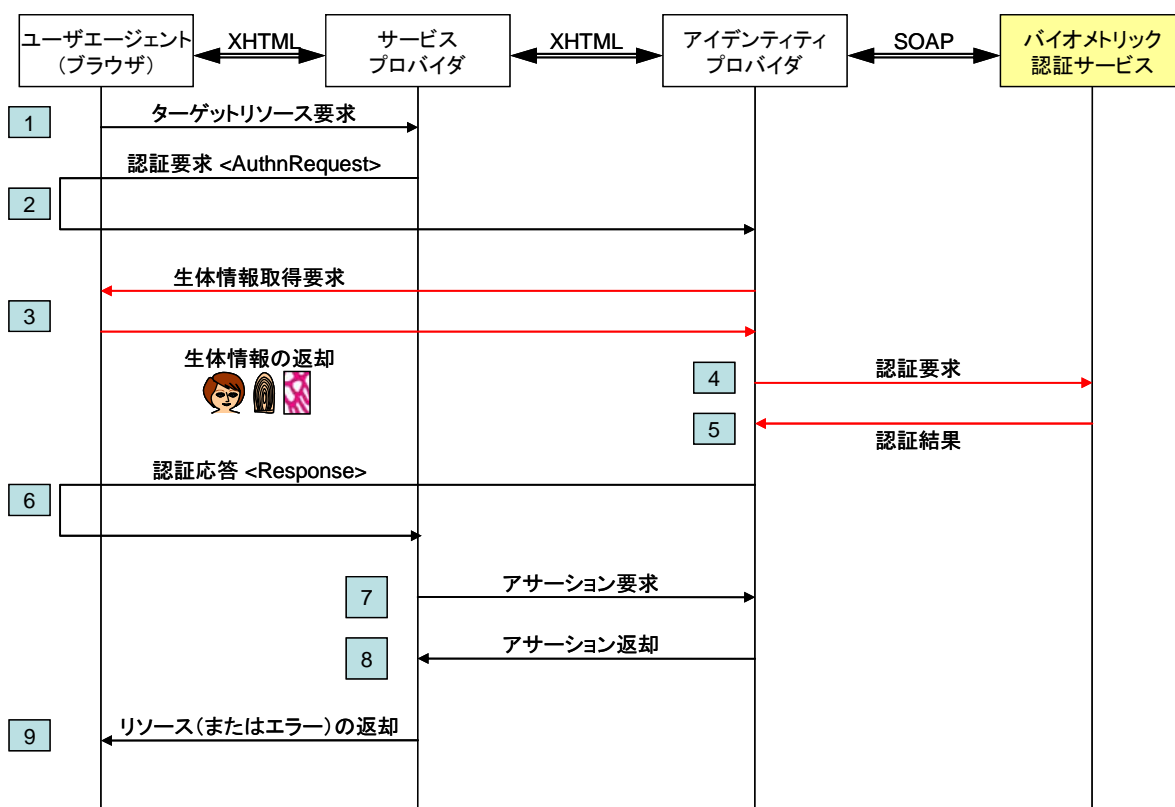


図 3.3.9 SAML でのバイオメトリック認証詳細フロー

3.4 方式検討結果

本節では IdM システムにバイOMETリック認証を組み込む具体的な方式として、既存の国際標準規格である BIAS、BIP 及び BioAPI を組み込んだ場合のアーキテクチャについて検討する。検討対象となる方式案を図 3.4.1 に示す。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。

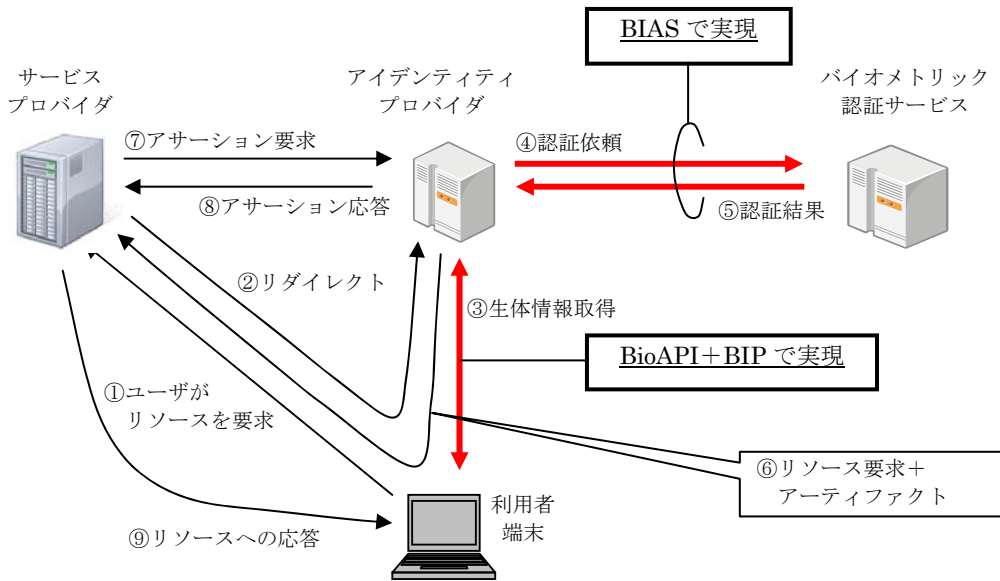


図 3.4.1 実現方式案

上記、図 3.4.1 で示したシステム構成において、バイOMETリック認証に関する部分の詳細について記述したシステム構成を図 3.4.2 に示す。

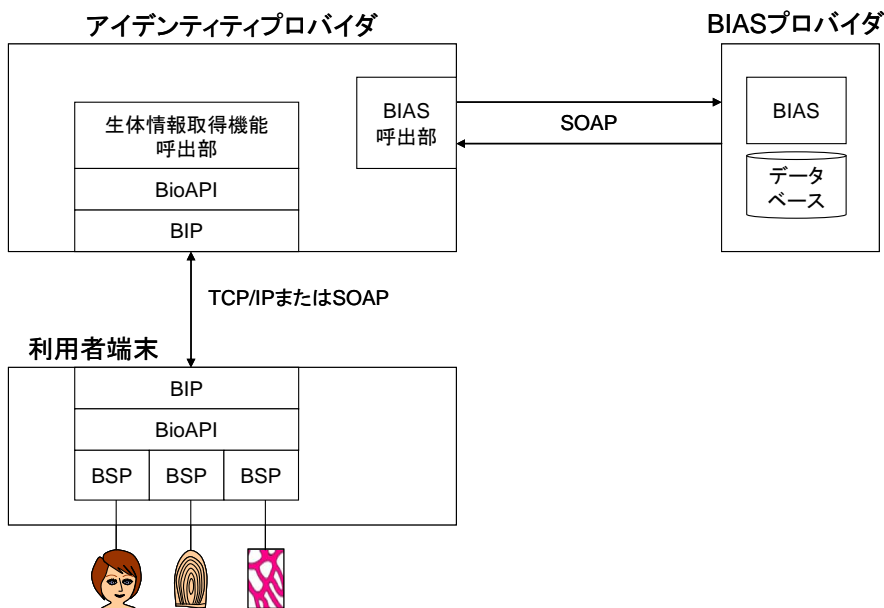


図 3.4.2 バイOMETリック認証部分の詳細構成図

以下に処理手順を示す。

<処理手順>

- ① アイデンティティプロバイダはサービスプロバイダからの認証依頼を受け付ける。
- ② アイデンティティプロバイダは **BioAPI** 関数を呼び出して利用者端末のバイオメトリック装置を遠隔で制御し、生体情報を取得する。この際に用いる代表的な関数は以下のとおりである。
 - ・ **BioAPI_BSPLoad** : 利用者端末の **BSP** モジュールのメモリへのローディング（初期化処理の一部として実行）。
 - ・ **BioAPI_BSPAttach** : 利用者端末の **BSP** のアプリケーションとの接続（初期化処理の一部として実行）。
 - ・ **BioAPI_Capture** : 利用者端末で利用者の生体情報を取得する。
 - ・ **BioAPI__Process** : 利用者端末で利用者の生体情報から、認証アルゴリズムがマッチングに用いるコード化情報を生成する。
 - ・ **BioAPI_GetBIRFromHandle** : 利用者端末で生成したマッチングに用いるコード化情報を呼び出し元であるアイデンティティプロバイダ側で取得する。
- ③ アイデンティティプロバイダ側でコード化情報が取得できたら、これを入力パラメータの一つとして **BIAS** プロバイダのバイオメトリック認証サービス（**Verify Subject** サービス又は **Identify Subject** サービスなど）を呼び出し、バイオメトリック認証を行う。
- ④ アイデンティティプロバイダは **BIAS** サービスからの認証結果を受け取ると、サービスプロバイダにリソース要求とアーティファクトを返却する。

3.5 方式案の考察

本検討における基本方針として 3.1.1 項に示したとおり、検討した実現方式について、汎用性・バイオメトリクスの特性の考慮・Web 技術との親和性の 3 点について考察した結果を表 3.5.1 に示す。

表 3.5.1 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検討結果の考察

No	項目		考察結果	評価
1	汎用性		OpenID、SAML (LibertyAlliance) とともに特定の認証技術に依存していない。このため、バイオメトリック認証の実装は IdM システムの方式に無関係であり、本質的に汎用的であるといえる。 今回の検討で取り上げた BIAS は XML を用いており、同様に XML を用いる SAML との親和性が高いものの、OpenID に対しても適用可能な方式である。	○
2	バイオメトリクスの特性の考慮	技術の多様性	<ul style="list-style-type: none"> ・バイオメトリック認証サービス (BIAS プロバイダ) バイオメトリック認証のために用いる BIAS サービスは特定のバイオメトリック技術を意識せず中立的である。使用する主なサービスは登録、1:1 照合、1:N 照合であり、バイオメトリック技術ごとの差異が存在しない抽象的な定義となっている。 ・利用者端末 (BioAPI+BIP) バイオメトリック端末を制御するための BioAPI 関数は、特定のバイオメトリック技術を意識せず中立的ではある。しかしながら、BioAPI 仕様は多様なバイオメトリック技術に対応するために多数のオプション関数やオプションパラメータが定義されており、異なる BSP を取り扱う場合には、それぞれの BSP が提供する機能に対してアプリケーション側で厳密な使い分けが必要である。 	○
		精度評価	BioAPI や BIAS で定義されている関数は、生体情報の取得、照合用バイオメトリックデータの生成、1:1 照合の実行、1:N 照合の実行など単純な機能をアプリケーション側で組み立てる必要がある。この結果、バイオメトリックシステムの性能はアプリケーションの作りに依存してしまう。	×
		プライバシー	BIAS が提供する認証方式はサーバ認証が前提のため、サーバがアタックされた場合の登録データに対する潜在的なリスクが存在する。 実装方法として BIAS プロバイダ内にバイオメトリックデータベースを持つ方式とともに、端末側からバイオメトリック登録テンプレートを送信し、BIAS プロバイダ内でバイオメトリック認証する実装も可能である。この方法であればサーバ内にデータベースは不要であり、プライバシーのリスクは軽減される。	△
3	Web 技術との親和性		BIAS は SOAP に基づく実装が可能となっておりアイデンティティプロバイダは Web サービスとして BIAS を呼び出すことが可能である。BioAPI は従来 C 言語のインタフェースのみであったが、2010 年度米国からオブジェクト指向 BioAPI 規格の新規提案が行われ Java 言語が加えられることになった。BioAPI は今後、Web 技術との親和性を確保する見込みである。	○

3.6 今後の課題

前述 3.5 の考察結果より、国際標準規格である BIAS、BIP 及び BioAPI 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案には以下のとおり課題が存在する。

- (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 3.6.1 にバイOMET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。

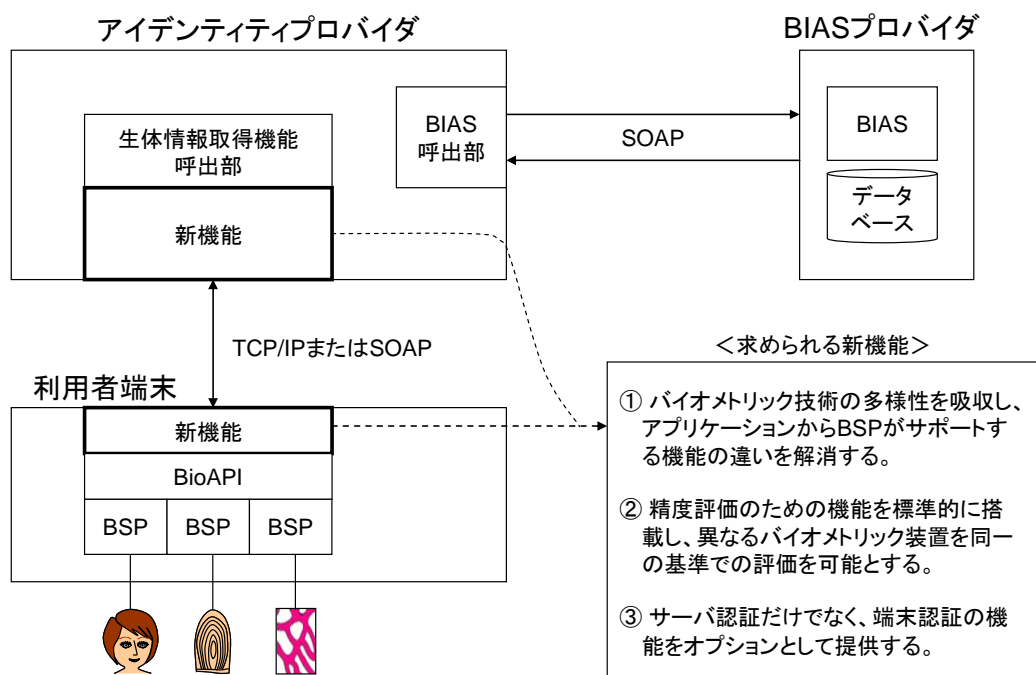


図 3.6.1 バイOMETリック認証のために求められる新機能

第4章 プライバシー保護の課題の明確化とその対策について

4.1 問題の所在

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。

これらを踏まえると、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、検討する必要がある。以下では、4.2 節で、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する。次に、4.3 節で、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る。その上で、4.4 節で、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、4.5 節で、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うことにする。

4.2 プライバシー権と個人情報保護法制

バイオメトリクスや IdM に関するプライバシー問題を検討する前提として、そもそも、プライバシー権はどのような権利なのか、また個人情報保護法制はどのようなものなのかという総論的な課題を整理する。

4.2.1 プライバシー権

まず、プライバシー権がどのような権利なのかという問題であるが、この点については、我が国の判例、学説において様々な見解が主張されてきている[2]。

(1) 私生活をみだりに公開されない権利

我が国におけるプライバシー権に関する最初期の裁判例として、宴のあと事件に関する東京地判 1964 (昭和 39) 年 9 月 28 日下民集 15 卷 9 号 2317 頁がある。この事件において東京地裁は、プライバシー権は「私生活をみだりに公開されないという法的保障ないし権利として理解される」と判示した。そして、プライバシーを侵害する行為が民法 709 条の不法行為となる要件については、以下の三つを挙げている。すなわち、①「私生活上の事実又は私生活上の事実らしく受け取られるおそれのあることがらであること」、②「一般人の感受性を基準として当該私人の立場に立った場合公開を欲しないであろうと認められることがらであること」、③「一般の人々に未だ知られていないことがらであること」である。このようにプライバシー権は、はじめは「私生活をみだりに公開されない権利」という消極的な権利として捉えられた。

(2) 自己情報コントロール権

その後、コンピュータやデータベースなどが発展・普及するようになって、従来の消極的な権利では不十分であると認識されるようになった。そこで、プライバシー権を自己に関する情報をコントロールする権利というように、積極的な権利として捉える見解（自己情報コントロール権説）が憲法学説において主張され、有力化するようになった。もっとも、この自己情報コントロール権説についても、内容は論者によって異なっている。

代表的な学説としては、まず、佐藤幸治教授の見解がある[3]。佐藤幸治教授は、プライバシー情報を個人の道徳的自律の存在に直接かかわる情報である「プライバシー固有情報」と、個人の道徳的自律の存在に直接かかわらない外的事項に関する個別の情報である「プライバシー外延情報」の二つに分けられる。そして、前者の固有情報については、公権力がその人の意思に反して接触を強要し、それを取得し、利用ないし開示することが原則的に禁止されるとする。それに対して、後者の外延情報については、正当な政府目的のために、正当な方法を通じて、取得・保有・利用しても、プライバシー侵害にはならないとする。ただし、外延情報であっても、悪用され、集積されるとき、個人の道徳的自律の存在に影響を及ぼすものとして、プライバシー侵害の問題が生じるとされている。

また、芦部信喜教授は、対象となる情報を更に細かく四つに分類される[4]。すなわち、①だれが考えてもプライバシーであると思われる情報、②一般的にプライバシーと考えられる情報、③プライバシーに該当するかどうか判然としない情報、④法令の規定によって何人でも閲覧できる情報に分けられるのである。そして、その収集、保有、利用ないし開示についてプライバシー権の侵害の有無が争われた場合、①のだれが考えてもプライバシー情報と思われるものが侵害されたときは「やむにやまれぬ利益」基準、②の一般にプライバシーに属すると思われる情報の侵害が争われたときは「厳格な合理性」基準を用いるのが妥当であるとされる。

このようにプライバシー権については、自己情報コントロール権説が有力になってきているが、コントロールの対象となる自己情報はどこまでの情報を含むのか、どのような場合に自己

情報コントロール権が侵害されたことになるのか、このような強力な権利を対公権力の場合だけでなく、対私人の場合にも無制限に認めて良いのかなど、多くの課題が残されている。

(3) 最近の注目すべき最高裁判決

また、比較的最近、プライバシー権に関する注目すべき最高裁判決が出されているので、この点について見ていくことにする。

従来、プライバシー権侵害になるための要件として、宴のあと事件における東京地裁判決のように、「一般の人々に未だ知られていないことがらであること」が挙げられてきた。これは、非公知の情報だけがプライバシー権の対象になり、公知の情報はプライバシー権の対象にならないという立場に立っているものと考えられる。しかし、最近の最高裁判決では、プライバシー情報の範囲が広がってきているように思われる。

その例として挙げられるのは、早稲田大学講演会名簿提出事件に関する最判 2003（平成 15）年 9 月 12 日民集 57 卷 8 号 973 頁である。この事件において、最高裁は次のように判示している。すなわち、「学籍番号、氏名、住所及び電話番号は、早稲田大学が個人識別などを行うための単純な情報であって、その限りにおいては、秘匿されるべき必要性が必ずしも高いものではない。……しかし、このような個人情報についても、本人が、自己が欲しない他者にはみだりにこれを開示されたくないと思えることは自然なことであり、そのことへの期待は保護されるべきものであるから、本件個人情報、上告人らのプライバシーに係る情報として法的保護の対象となるべきである」というものである。ここで問題となっている情報のうち、学籍番号は別として、氏名、住所、電話番号などは電話帳に記載されることもあって、公知性を有するとされてきたものであり、従来、プライバシー情報にはならないという立場が有力であった。このような公知性を有する情報であっても、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと思えることは自然」なので、「プライバシーに係る情報として法的保護の対象となるべきである」としたところに本判決の特徴がある。このように最高裁の判例は、プライバシー情報となるかどうかの判断にあたって、非公知性をあまり重視しなくなっている。

また、住民基本台帳ネットワークの合憲性について判断を下した最判 2008（平成 20）年 3 月 6 日民集 62 卷 3 号 665 頁も注目される。この事件において、最高裁は次のように判示している。すなわち、「住基ネットによって管理、利用などされる本人確認情報は、氏名、生年月日、性別及び住所から成る 4 情報に、住民票コード及び変更情報を加えたものにすぎない。このうち 4 情報は、人が社会生活を営む上で一定の範囲の他者には当然開示されることが予定されている個人識別情報であり、変更情報も、転入、転出などの異動事由、異動年月日及び異動前の本人確認情報にとどまるもので、これらはいずれも、個人の内面に關わるような秘匿性の高い情報とはいえない。……住基ネットによる本人確認情報の管理、利用などは、法令などの根拠に基づき、住民サービスの向上及び行政事務の効率化という正当な行政目的の範囲内で行われているものということができる。」本判決は、結果的に住基ネットはプライバシー権を侵害するものではないという判断をしているが、氏名、住所などの基本的な情報であってもプライバシ

一に係る情報になり得るという立場を前提にしているものと考えられ、その点では前記の最高裁判決と同様の立場に立っているといえる。

なお、学説の中には、これらの判決を持って、最高裁が自己情報コントロール権説を採用したと評価するものもあるが[5]、これらの判決では「自己情報コントロール」という表現は用いられていないこともあり、そのように断定することは適切ではないように思われる。

以上のように、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。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、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までは至っていないという状況にある。

4.2.2 個人情報保護法制

プライバシー権と密接に関係する法制度として、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。そこで、まず欧米などの国際的な議論動向を整理した上で、我が国の個人情報保護法制について見ていくことにする。

(1) OECDプライバシー・ガイドライン (1980年)

個人データ保護に関するガイドラインとしては、国際的に強い影響力を持つものとして、1980年にOECDから出された「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」がある[6]。現在、ほとんどの先進諸国において個人情報保護法制が整備されるようになってきているが、いずれも多かれ少なかれ、このOECDプライバシー・ガイドラインから影響を受けているということができる。OECDプライバシー・ガイドラインには、以下の八つの原則が定められている[7]。

① 収集制限の原則

個人データの収集には制限を設けなければならない、データの収集は、適法かつ公正な手段によって、かつ適当な場合には、データ主体に通知又は同意を得て行わなければならない。

② データ内容の原則

個人データは、その利用目的に沿ったものでなければならない、かつ利用目的に必要な範囲内で正確、完全であり、最新の状態に保たなければならない。

③ 目的明確化の原則

収集目的は収集時より遅くない時期において明確化されなければならない、その後における利用は当初の収集目的と矛盾することなく、かつ明確化されたものに制限すべきである。

④ 利用制限の原則

個人データは、目的明確化の原則にしたがって明確化された目的以外の目的のために、開示され、利用可能な状態に置かれ、又はその他の形での使用に供されてはならない。但し、
(a) 本人の同意がある場合又は (b) 法律によって認められる場合はこの限りでない。

⑤ 安全保護の原則

個人データは、紛失又は無権限アクセス、破壊、使用、修正もしくは開示その他のリスクに対し、合理的な安全保護措置により保護されなければならない。

⑥ 公開の原則

個人データに係る開発、実施、方針は一般に公開しなければならない。また個人データの存在、種類及びその主要な利用目的とともにデータ管理者のアイデンティティ及び住所を明らかにするための手段が容易に利用できなければならない。

⑦ 個人参加の原則

個人は以下の権利を有する。

(a) データ管理者が本人に関するデータを保有しているか否かについて、データの管理者から又はその他の方法により確認を得ること。

(b) 本人に関するデータについて、(i) 合理的期間内に、(ii) 仮に必要とする場合でも過度にならない手数料で、(iii) 合理的な方法により、かつ、(iv) 本人が容易に理解できる様式で、本人が通報を受けること。(c) 上記 (a) 及び (b) の権利に基づく要求が拒否されたときは、その理由がしめされること及びそのような拒否に対して異議申立ができること。(d) 本人に関するデータに対して異議を申立てること、及び、その異議が認められた場合には、そのデータを削除、訂正、完全化又は補正すること。

⑧ 責任の原則

データ管理者は上記諸原則を実施するための措置にしたがう責任を有する。

なお、この OECD プライバシー・ガイドラインについては、30 周年を迎えたのを機に改定に向けた検討が行われるようになっている[8]。このガイドラインの改定については、OECD の WPISP(Working Party on Information Security and Privacy)において議論が進められている。

(2) EU個人データ保護指令

諸外国の個人情報保護法制は、OECD ガイドラインから影響を受けているが、その中でも、EU 諸国は高いレベルで個人データを保護している。EU では、「個人データの処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令」(以下、「EU 個人データ保護指令」と表記する) [9]が重要な意味を持っている。この EU 個人データ保護指令は、公的部門と民間部門を特に区別しておらず、いわゆるオムニバス方式を採用している。特徴としては、個人データの収集、記録、蓄積、利用、頒布、削除

などの処理を行うことについて、原則としてデータ主体の同意を要求していること（7条）、センシティブデータについては、特に厳格な保護を与えており、原則として処理を禁止していること（8条）、管理者は自動処理作業又は一連の作業を実施する場合には、事前に監督機関に通知しなければならないとしていること（18条）、などを挙げることができる。つまり、EU 個人データ保護指令は、オムニバス方式、事前規制型を採用し、厳格に個人データを保護するものということができる。

また、EU 域外の諸外国にとって問題となるが、EU 個人データ保護指令 25 条である。同条は、次のように規定している。すなわち、「加盟国は、処理過程にある個人データ又は移転後処理することを目的とする個人データの第三国への移転は、この指令の他の規定にしたがって採択されたその国の規定の遵守を損なうことなく、当該第三国が十分なレベルの保護を確保している場合に限って行うことができるということを規定しなければならない」というものである。つまり、個人情報について十分なレベルの保護を行っていない第三国に対しては、EU 加盟国からは個人データを出してはいけないということである。そのため、EU 域外の多くの国が、十分なレベルの保護に達しているという認定を受けるために、個人情報保護法制を整備せざるを得ないという状況になっている。

(3) 米国の個人情報保護制度

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[10]。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。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、いわゆるセクター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。

問題となるのは、EU 個人データ保護指令 25 条との関係である。米国では民間部門を包括的に規制する法律が存在していないため、指令 25 条の十分なレベルの保護に達していないということになり、EU 加盟国からの個人データの移転について障害が生じてしまうことになる。そこで、米国は、EU と協議を行い、セーフハーバー協定を締結するにいたった。これは、一定の要件を満たしている企業、組織については、セーフハーバーという安全な港の中にあるものとして EU 加盟国から個人データの移転を受けられることにしたものである。

(4) 我が国の個人情報保護法制の概要

以上の欧米の個人情報保護法制に関する動向を踏まえた上で、我が国の個人情報保護法制について見ていくことにする。

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とのことから、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。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[11]。

しかし、その後、主として以下の四つの理由から、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った[12]。

- ① 1980 年 OECD プライバシー・ガイドラインへの対応。
- ② 1995 年 EU 個人データ保護指令への対応。同指令 25 条は、加盟国から第三国への個人データの移転は、当該第三国が適切なレベルの保護を提供している場合に限定しているため、日本もこれへの対応が必要になった。
- ③ 情報化社会の進展により個人情報の大量漏洩事件が頻発するようになった。
- ④ 住民基本台帳ネットワークシステムの導入によって、個人情報漏洩の危機が生じる恐れがある。

このような認識を背景として、2003 年 5 月に、個人情報保護関連 5 法が制定された。これは以下の五つの法律からなる。

- ① 「個人情報の保護に関する法律」(個人情報保護法)
- ② 「行政機関の保有する個人情報の保護に関する法律」(行政機関個人情報保護法)
- ③ 「独立行政法人等の保有する個人情報の保護に関する法律」(独立行政法人等個人情報保護法)
- ④ 「情報公開・個人情報保護審査会設置法」(設置法)
- ⑤ 「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律」(整備法)

これらのうち、①の個人情報保護法は、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。

次に、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。すなわち、この法律は、個人情報取扱事業者を「個人情報データベース等を事業の用に供

している者」(2条3号)と定義し、この個人情報取扱事業者は、その取り扱う情報の種類により、以下のような義務を負うとしている。

- ・ 利用目的の特定 (15条)
- ・ 利用目的による制限 (16条)
- ・ 適正な取得 (17条)
- ・ 取得に際しての利用目的の通知 (18条)
- ・ データ内容の適切性の確保 (19条)
- ・ 安全管理措置 (20条)
- ・ 従業員の監督 (21条)、委託先の監督 (22条)
- ・ 第三者提供の制限 (23条)
- ・ 保有個人データに関する事項の公表 (24条)
- ・ 開示 (25条)、訂正 (26条)、利用停止 (27条)
- ・ 理由の説明 (28条)
- ・ 開示の求めに応じる手続 (29条)

これらのうち、15条から18条は「個人情報」(「生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日、その他の記述により特定の個人を識別できるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む)」)について適用される義務である。

また、19条から23条は「個人データ」(「個人情報データベース等を構成する個人情報」)にのみ適用される義務である。

そして、24条から27条は「保有個人データ」(「個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであつて、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は一年以内の政令で定める期間以内に消去することとなるもの以外のもの」)にのみ適用される義務である。

4.3 バイオメトリクスに関するプライバシー

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。

4.3.1 バイオメトリクスに関するプライバシー問題の発生

(1) バイオメトリックデータの重要性

バイオメトリックデータが特に重要であると考えられる理由は、それが以下のような特徴を有しているからである[13]。

第一に、取り替えが不能な情報であるということである。ID やパスワードなどは、それが漏洩してしまった場合には変更するということが可能である。しかし、顔や指紋などの生体情報は、漏洩してしまったとしても、容易に変更することはできない。この点は、初めから変更可能なように変形したデータを用いる技術（Cancelable Biometrics）なども開発されているが、技術によって完全に問題を解決することは困難であると考えられる。第二に、本人認証と関係のない副次的な情報が抽出される恐れがあるということである。例えば、顔画像からは、人種、健康状態、精神状態など本人認証とは関係のない情報が抽出され、利用される恐れがある。第三に、無意識のうちに情報が取得されやすいという側面を有しているということである。特に、顔画像は、本人の気がつかないうちに、遠隔システムによって取得されてしまう恐れがある。

(2) バイオメトリクスの認証モデルとプライバシー問題

上記のようなバイオメトリックデータは、一般的に指摘されているように、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。この点については、認証モデルごとの検討が必要である。

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、ここでは、より深刻な問題を発生させるサーバ管理型を例に見ていくことにする。

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。

4.3.2 バイオメトリクスとプライバシー権

(1) プライバシー情報の範囲

プライバシー権をどのような権利として捉えるのかについては、前述したように様々な見解が主張されているが、生体認証のプライバシー問題を考える上で重要になるのは、プライバシー権の対象となる情報の範囲に関する問題である。とりわけ、プライバシー情報に、公知の情報が含まれるのかということが重要な問題となる。

上述したように、プライバシー権の対象となる情報の範囲については、判例、実務において変遷が存在する。従来、プライバシー権侵害になるための要件として、宴のあと事件における東京地裁判決のように、「一般の人々に未だ知られていないことがらであること」が挙げられてきた。これは、非公知の情報だけがプライバシー権の対象になり、公知の情報はプライバシー権の対象にならないという立場に立っているものと考えられる。しかし、早稲田大学講演会名簿提出事件など、最近の最高裁判決では、プライバシー情報の範囲が広がってきており、公知の情報かどうかはあまり重視されなくなっている。

生体認証の対象となる生体情報は非公知のものが多いが、特に顔画像を用いる場合には、顔は公知のものなので、プライバシー権の対象にならないのではないかということが問題となる。そもそも、どのような場合に公知性が認められるのかという問題もあるが、通常、人間は顔をさらしながら生活をしており、少なくとも自己の周囲にいる人々には知られてしまうものであるから、一定の範囲で公知性を有しているといえる。しかし、自己が欲しない他者にはみだりに顔画像を開示されたくないと思えることは自然であると考えられるので、前記最高裁判決の立場からは、顔画像もプライバシー情報になり得るものと考えられる。もっとも、後述するように、顔や容姿については、我が国では肖像権の問題として議論されることが多かったので、肖像権との関係に注意する必要がある。

(2) 顔認証システムと肖像権

バイオメトリクスの対象となる生体情報の中でも、指紋、虹彩、静脈などの生体情報ではなく、顔画像が用いられる場合には、プライバシー権だけでなく、肖像権が関係してくることになる。

肖像権とは、自己の顔や容姿などの肖像を勝手に撮影されたり、公表されたりするのを禁止することができる権利である[14]。肖像権に関する判例としては、リーディングケースになるものとして、京都府学連事件に関する最判 1969（昭和 44）年 12 月 24 日刑集 23 卷 12 号 1625

頁がある。この判決は、「個人の私生活上の自由の一つとして、何人も、その承諾なしに、みだりにその容貌・姿態（以下「容ぼう等」という。）を撮影されない自由を有するものというべきである。これを肖像権と称するかどうかは別として、少なくとも、警察官が、正当な理由もないのに、個人の容ぼうなどを撮影することは、憲法 13 条の趣旨に反し、許されない」と判示しており、この判決によって、実質的に肖像権が承認されたことになる。

バイオメトリクスとの関係で特に注目されるのは、顔認証システムと監視カメラを組み合わせた監視システムが開発されるようになってきているということである[15]。すなわち、ゲートなどに監視カメラを設置し、通過する人物の顔画像をカメラで取得して、事前に用意したリストに登録されている顔画像との照合をリアルタイムで行うものである[16]。このようなシステムについては、警察が設置した防犯カメラの適法性に関する下級審裁判所の裁判例が関係してくることになる[17]。代表的なものとしては、山谷地区防犯カメラ事件に関する東京高判 1988（昭和 63）年 4 月 1 日判時 1278 号 152 頁や、釜ヶ崎あいりん地区防犯カメラ事件に関する大阪地判 1994（平成 6）年 4 月 27 日判時 1515 号 116 頁などがある。防犯カメラが許容される要件として、前者は、①「当該現場において犯罪が発生する相当高度の蓋然性が認められる場合」、②「予め証拠保全の手段、方法をとって置く必要性及び緊急性」がある、③「その撮影、録画が社会通念に照らして相当と認められる方法でもって行なわれるとき」を挙げており、後者では、①「目的が正当であること」、②「客観的かつ具体的な必要があること」、③「設置状況が妥当であること」、④「設置及び利用による効果があること」、⑤「使用方法が相当であること」が挙げられている。バイオメトリクスを用いた顔認証システムについても、それが警察など公的機関が設置したものである場合には、これらの要件を満たしているかどうかが問題になるものと考えられる。

(3) 個人の生体情報とプライバシー権

顔画像以外の指紋、虹彩、静脈などその他の生体情報については、肖像権は問題とならず、プライバシー権との関係が問題となる。バイオメトリクスにおいて人の生体情報を用いる際に、どのような場合に、プライバシー権の侵害になるのかということについては、プライバシー権についてどのような立場に立つのかによって左右される。

まず、宴のあと事件判決のように、プライバシー権を「私生活をみだりに公開されない権利」と解する場合には、他人の生体情報をみだりに公開した場合だけがプライバシー権侵害ということになる。これに対して、自己情報コントロール権説には様々な見解が存在するため厳密には各見解ごとに検討していく必要があるが、基本的には、生体情報は重要なプライバシー情報なので、これを本人の同意を得ずに取得したり、第三者へ開示したり、改ざんしたりする行為は原則としてプライバシー権侵害ということになるものと考えられる。ただし、憲法上の人権としてのプライバシー権については、公共の福祉による制約によってプライバシー権の制約が正当化される場合があるし、民法 709 条のプライバシー権についても、違法阻却事由が存在する場合には、違法性が阻却され、結果的に法的責任が発生しない場合があり得ることになる。

また、プライバシー権について、どのような立場に立つにせよ、バイオメトリクスのように、生体情報を用いる場合には、プライバシー権の保護の対象となるために、当該情報が特定の個人と結びついたものであることが必要とされるのかということが問題となる。生体情報の中でも、顔画像については、特定の個人と結びつきやすいので問題は少ないが、例えば、指紋、静脈、虹彩などの画像があっても、それを見て直ちに誰のものであるかを判別することができるのかという疑問があり、そうだとすると、プライバシー情報に当たらないのではないかということが問題となり得る。

この点、個人情報保護法では、個人情報に該当するためには、「特定の個人を識別することができる」ものであること、すなわち個人識別性が要求されている。そして、どのような場合に個人識別性が認められるのかについて、様々な議論がなされている。これに対して、プライバシー情報については、個人識別性のようなものが要求されるのかについて、これまで必ずしも十分な議論がなされてこなかったように思われる。

プライバシー権の保護の対象となる情報となるには、特定個人との同定可能性ないし個人識別性が必要であるとする、バイオメトリクスの対象となる生体情報がこのような要件を満たすのかということが問題となる。この問題については、個人情報保護法における個人情報の個人識別性の問題と類似しているが、この問題については、後に見ていくことにする。

4.3.3 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ところがあるので、まず、EUにおける議論状況を整理することにしたい。

(1) EUにおける議論状況

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。

① BIOVISION プロジェクト

EUにおける取り組みにおいて注目されるのは、2002年から2003年にかけて行われたBIOVISIONの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” [18]

(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。このベストプラクティスは、注目すべき報告書であるので、以下、詳細に見ていくことにする。

ベストプラクティスは、EU 個人データ保護指令にしたがって法的に要求される事項と実務運用上配慮されるべき事項の双方について、両者の区別に配慮しながらまとめている。ベストプラクティスは、EU 個人データ保護指令の条文ごとに検討を行っているが、以下では、そのうち重要な部分のみを取り上げる。

第一に、バイオメトリックデータがどのような場合に「個人データ」になるのかという点である。EU 個人データ保護指令 2 条は、個人データを特定された、又は特定し得る自然人に関する全ての情報と定義している。バイオメトリックデータが、指令 2 条に定める個人データにあたるかどうかは、当該バイオメトリックデータに指令が適用されるかどうかを左右するものであるため、重要な分水嶺となるものである。この点について、ベストプラクティスには、以下のように書かれている[19]。

「EU 個人データ保護指令は、自然人に関係し得る全ての情報を包含することができるように、個人データを非常に包括的な意味を有するものとして、定義している。このように、EU 個人データ保護指令は、写真、声、指紋、遺伝的特徴のようなバイオメトリックデータをも包含し得るように、開かれたものになっている。あるアプリケーションにおいて、正確にどのようなデータが記録されているのかということに厳重に依拠する場合には、バイオメトリックデータは、この広範な個人データの定義に当てはまらない場合があり得る」。

つまり、EU 個人データ保護指令の定義は、包括的になされているため、バイオメトリックデータも包含される可能性がある。しかし、個別的に厳密に検討していった場合には、特定し得る自然人に関する情報にあたらぬ場合があるため、データの種別に応じた検討が必要である、ということが示唆されている。続けて、ベストプラクティスは、生データとテンプレートデータの違いについて検討している。

「テンプレートが、個人との照合がもはや不可能であり、排除されるような方法によって記録されている場合には、テンプレートは個人データではなくなる。しかしながら、ほとんどの場合には、システムが適切に機能していること、及び誤った排除や誤った受け入れがなされる場合を最終的にチェックするために、少なくともデータ管理者にとっては、特定されたものと想定される個人との照合が可能になっている。したがって、ほとんどの場合には、取得され、処理され、記録されたデータは、個人データ保護指令の意味における個人データとして扱われることになるであろう」。

第二に、センシティブデータに関する問題である。EU 個人データ保護指令の特徴として、センシティブデータを特に厳格に保護しているという点を挙げることができる。指令 8 条 1 項は、センシティブデータに関する定義を置いており、人種、民族、政治的思想、信教又は信条、労

働組合への加入事実、及び健康及び性生活に関するデータの処理と定義している。そして、指令 8 条 2 項によれば、センシティブデータは、本人の明示的同意がある場合など一定の例外的な場合を除いて、原則としてその処理が禁止されている。

そこで、バイOMETリックデータがどのような場合にセンシティブデータに該当するのかが問題となる。この点について、ベストプラクティスには、次のように書かれている。

「バイOMETリクスを用いることによって、一般的にバイOMETリクスで用いるデータ以外の情報も明らかになってしまうことがある。しかし、これは本人確認目的で用いられる特定のバイOMETリクスの性質によるところが大きい（例えば、自動顔画像認識システムで顔を利用する場合、虹彩認証又は掌紋認証を用いる場合よりも、民族や人種に関する情報が明らかになってしまう傾向がある）。また、そのように本人確認目的で使用する情報以外の情報が明らかになる可能性については、生のデータを用いているのか、それともテンプレートが処理されているのかによっても異なる。」

「バイOMETリクスとの関係におけるセンシティブデータとしては、医療（虹彩学、ただし、学問的には必ずしも確立はしていない）、民族又は人種、特定の行動に関する情報（例えば、労働組合への加入事実）、又は性生活に関する情報などが挙げられる。」

第三に、処理の安全性に関する問題である。EU 個人データ保護指令 17 条は、偶発的な又は違法な破壊、偶発的な損失、変更、無権限の開示又はアクセスから個人データを保護するために、管理者が適切な技術的及び組織的措置を実施しなければならないと規定している。バイOMETリクスについて、どのような安全管理措置が要求されるのかについて、ベストプラクティスには、次のように書かれている。

「ベストプラクティスの意義やプライバシー意識高揚の観点の範疇においては、バイOMET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。」

「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。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く、プライバシーに関する法制でも一般的に禁止されてはいない。」

ここでは、バイOMETリックデータを中央のデータベースに集中して蓄積させる集中データベース型（サーバ管理型）よりも、ユーザが所持しているストレージに保管する分散ストレージ型（ユーザ管理型）が望ましいものとされている。確かに、個人データ保護のためには、分散ストレージ型が望ましいものといえるであろうが、両システムにはそれぞれ長所と短所が存在するので、常に集中データベース型でなければならないと強要することは適切ではないものと考えられる。

② 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

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” [20] 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えることができる。この報告書では、概ね以下のようなことが書かれている。

・ EU 個人データ保護指令のバイOMETリクスへの適用

バイOMETリックデータは、ほとんどの場合、EU 個人データ保護指令 2 条の個人データにあたる。

・ 目的原則

バイOMETリックデータがアクセスコントロールのために取得された場合、それを精神状態の評価や仕事場の監視に用いてはならない。

・ 適正な収集

データを取得する際に、目的及び管理者に関する情報を与えなければならない。遠隔でバイOMETリックデータを取得する場合には、特に注意が必要である。

・ 処理の適法性

バイOMETリックデータを処理する場合、原則として本人の同意が必要である。

・ 事前検査

データの処理が、データ主体の権利に特別な危険をもたらす恐れがある場合には、監督機関による事前の検査がなされるべきである。

・ セキュリティ対策

データ管理者は、技術的及び組織的なセキュリティ対策を講じなければならない。テンプレートの暗号化、暗号鍵の保護、アクセスコントロールなど。

・ センシティブデータ

バイOMETリックデータが、人種、民族、健康状態などのセンシティブデータに当たるものとみなされる場合、特別な保護が必要である。

(2) 我が国における議論

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。以下では、中心的に問題になると考えられる個人情報保護法との関係を見ていくことにする。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。

2 条 1 項は、個人情報を「生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日、その他の記述により特定個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）」と定義している。バイオメトリックデータの個人情報該当性については、EU においても必ずしも十分な検討がなされていない。先に紹介した EU 指令 29 条作業部会の“Working Document on Biometrics”においても、ほとんど場合に、個人データに該当するというような抽象的な記述しかなされていない。

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[21]。もっとも、バイオメトリ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得るところであり、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。前述したように、EU 個人データ保護指令 8 条 1 項は、「加盟国は、人種又は民族、政治的意見、宗教又は思想信条、労働組合への加入を明らかにする個人データの処理、及び健康又は性生活に関するデータの処理を禁止しなければならない」として、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」[22]の 6 条は、次のように定めている。この中で、バイオメトリクスとの関係で重要になるのは、1 項 8 号である。

第 6 条 機微（センシティブ）情報について

1 金融分野における個人情報取扱事業者は、政治的意見、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（以下「機微（センシティブ）情報」という。）については、次に掲げる場合を除く他、取得、利用又は第三者提供を行わないこととする。

- ① 法令等に基づく場合
- ② 人の生命、身体又は財産の保護のために必要がある場合
- ③ 公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合
- ④ 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合
- ⑤ 源泉徴収事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属若しくは加盟に関する従業員等の機微（センシティブ）情報を取得、利用又は第三者提供する場合

- ⑥ 相続手続による権利義務の移転等の遂行に必要な限りにおいて、機微（センシティブ）情報を取得、利用又は第三者提供する場合
- ⑦ 保険業その他金融分野の事業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供する場合
- ⑧ 機微（センシティブ）情報に該当する生体認証情報を本人の同意に基づき、本人確認に用いる場合

2 金融分野における個人情報取扱事業者は、機微（センシティブ）情報を、前項各号に定める事由により取得、利用又は第三者提供する場合には、各号の事由を逸脱した取得、利用又は第三者提供を行うことのないよう、特に慎重に取扱うこととする。

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」[23]を出している。この実務指針は、7-1以下において、機微（センシティブ）情報の安全管理措置について定めているが、特に機微（センシティブ）情報に該当する生体認証情報（機械による自動認証に用いられる身体的特徴のうち、非公知の情報。以下同じ）の取り扱いについては、以下の措置を定めている。

7-1-1-1 機微（センシティブ）情報に該当する生体認証情報の取り扱いは、取得、入力段階における取扱規程において、7-1-1に規定する事項に加えて、次に掲げる事項を含まなければならない。

- ① なりすましによる登録の防止策
- ② 本人確認に必要な最小限の生体認証情報のみの取得
- ③ 生体認証情報の取得後、基となった生体情報の速やかな消去

7-1-2-1 機微（センシティブ）情報に該当する生体認証情報の取り扱いは、利用段階における取扱規程において、7-1-2に規定する事項に加えて、次に掲げる事項を含まなければならない。

- ① 偽造された生体認証情報による不正認証の防止措置
- ② 登録された生体認証情報の不正利用の防止措置
- ③ 残存する生体認証情報の消去
- ④ 認証精度設定等の適切性の確認

- 7-1-3-1 機微（センシティブ）情報に該当する生体認証情報の取り扱いは、保存段階における取扱規程において、7-1-3に規定する事項に加えて、保存時における生体認証情報の暗号化を含まなければならない他、サーバなどにおける氏名などの個人情報との分別管理を含むこととする。
- 7-1-5-1 機微（センシティブ）情報に該当する生体認証情報の取り扱いは、消去段階における取扱規程において、7-1-5に規定する事項に加えて、生体認証情報を本人確認に用いる必要性がなくなった場合は、速やかに保有する生体認証情報を消去することを含まなければならない。
- 7-2 金融分野における個人情報取扱事業者は、2-5-2に規定する監査の実施にあたっては、機微（センシティブ）情報に該当する生体認証情報の取り扱いに関し、外部監査を行うとともに、必要に応じて、その他の機微（センシティブ）情報の取り扱いについても外部監査を行うこととする。

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。

4.4 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が、ここでは、SAMLや、OpenIDといったシングルサインオンを用いたシステムのプライバシー問題を検討していくことにする。

4.4.1 シングルサインオンを用いたIdMのプライバシー問題

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[24]。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[25]。

① 同一サイト内でのユーザ行動の関連付け

「同一のユーザが同一のサイトにおいて実際に行った全ての行動が、そのサイトにおいて同一ユーザのものであることを認識される」というプライバシー問題である。

② 複数サイト間でのユーザ行動の関連付け

「同一のユーザIDを複数のサイトで共有する場合、それらのサイトが結託することにより、ユーザが意図したよりも多くの情報が流出する可能性がある」というものである。同一のIDを複数のサイトで利用すると、そのIDを用いることによって、様々なサイトにおけるユーザの行動や氏名、住所などの情報が紐付けられることになってしまう。つまり、統一的なIDを用いることによって、いわゆる「名寄せ」がなされ得ることになり、それによってプライバシー問題が生じるということである。

③ 送信元情報の流出

シングルサインオンを使用するかどうかに関わらず、「ユーザから送信されたパケットの送信元アドレスなどから、ユーザの所属組織名や、ユーザ同一性などのプライバシー情報が流出する可能性がある」という問題である。

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[26]。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。

例えば、ユーザの氏名、住所などの属性情報が個人データを構成する場合に、それが、アイデンティティ提供者から、サービス提供者に対して提供されると、それは個人情報保護法上の第三者提供に当たることになる。この第三者提供については、個人情報保護法は、いくつかの例外を除いて、原則として本人の同意を要求しているところである（個人情報保護法 23 条）。

以下では、SAML2.0 や OpenID2.0 といった代表的な IdM の方式が、これらのプライバシー問題にどのように対応しているのか、また十分に対応できているのかを見ていくことにしたい。

4.4.2 SAMLとプライバシー

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。IdM の方式は、大きく、アイデンティティ連携方式、アイデンティティ統一方式、アイデンティティ選択方式の三つに分けられることがある[27]。アイデンティティ連携方式とは、「複数のアイデンティティを連携して管理する方式」であり、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」方式であり、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」方式である。この三つの方式の中では、SAML2.0 は、アイデンティティ連携方式に該当することになる。

この SAML2.0 については、上述したような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。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[28]。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

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。

4.4.3 OpenIDとプライバシー

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。前述した三つの IdM の分類の中では、アイデンティティ統一方式に位置付けられている[29]。特徴としては、ユーザが URL などによって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。また、OpenID2.0においては、アイデンティティ提供者は、OP(OpenId Provider)と表現され、サービス提供者は、RP(Relying Party)と表現される。

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、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、信頼レベルを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[30]。

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[31]。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 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[32]。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。

4.4.4 プライバシー保護に関する残された課題

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えるという問題がある」とするものである[33]。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。

4.5 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。

4.5.1 IdMへバイオメトリクスを組み込む際の課題

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い。

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。そして、本報告書の第 1 章及び第 3 章において記述されているように、これらの規格においては、アイデンティティ提供者がどのような認証方法を用いて認証を行うのかは規定されていない。例えば、SAML2.0 であれば、「どのような認証手段を用いるかは SAML2.0 では規定しておらず、ユーザ、IdP、SP 間の合意に基づき決定される」[34]とされている。したがって、アイデンティティ提供者がユーザの認証を行う際に、バイオメトリクスを使用することは、規格上は可能になっているといえる。

もっとも、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。このようなリ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[35]。

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置き、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[36]。

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[37]。

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。

4.5.2 IdMへバイオメトリクスを組み込む際のプライバシー問題

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[38]。

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。

(1) 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」。この点は、4.3.3 項において述べたとおりである。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。

(2) 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、生のバイオメト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オメトリック認証プロバイダのサーバ側で管理するのが問題となる。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[39]。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、本人のバイオメト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。」もっとも、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。

(3) テンプレートと個人情報の照合可能性

テンプレートは、生のバイオメトリックデータから、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[40]。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が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。

(4) 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可能性があるため、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。

(5) 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 4.2.2 項において紹介した 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[41]。

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。

ここまで、①生のバイオメト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オメト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からバイオメト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について、考察を加えてきた。

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。本章においては、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. 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ためであると思われる。

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、標準とな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み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

にバイオメト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、バイオメト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 へバイオメトリクスを組み込む際のプライバシー問題

IdM にバイオメト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生のバイオメト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オメト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からバイオメト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。

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、次のこと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]

第 1 章

- [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/syoukai/H20_houkoku/H20annual-report/02_02.pdf
- [11] Phillip J. Windley : Digital Identity, O'Reilly & Associates Inc 2005 年 8 月
- [12] 佐藤 周行、笠松 隆幸、田村 拓也、小林 勇範
情報セキュリティ基盤論、共立出版 2010 年 11 月
- [13] 特集 最新&定番の認証技術、pp.23-27、日経ネットワーク、2009.10
- [14] Cloud Security Alliance Domain 12: Guidance for Identity & Access Management V2.1
2010
<http://www.cloudsecurityalliance.org/guidance/csaguide-dom12.pdf>

- [15] 会社法（平成十七年七月二十六日法律第八十六号）
http://law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=2&H_NAME=&H_NAME_YOMI=%82%a9&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=H17HO086&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1
- [16] 金融商品取引法（昭和二十三年四月十三日法律第二十五号）
http://law.e-gov.go.jp/cgi-bin/idxselect.cgi?IDX_OPT=2&H_NAME=&H_NAME_YOMI=%82%ab&H_NO_GENGO=H&H_NO_YEAR=&H_NO_TYPE=2&H_NO_NO=&H_FILE_NAME=S23HO025&H_RYAKU=1&H_CTG=1&H_YOMI_GUN=1&H_CTG_GUN=1
- [17] IDM 研究会 井上春樹監修 IDM アイデンティティ・マネジメント入門 静岡学術出版 2008
- [18] 日本 HP HP IceWall Identity Manager とは
<http://h50146.www5.hp.com/products/software/security/icewall/im/feature.html>
- [19] 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
- [20] 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>
- [21] SAML V2.0 Executive Overview Committee Draft 01, 12 April 2005
<http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf>
- [22] Liberty Technical Glossary Version: v2.0-05
<http://www.projectliberty.org/liberty/content/download/315/2355/file/draft-liberty-glossary-v2.0-05.pdf>
- [23] 学術認証フェデレーション <https://upki-portal.nii.ac.jp/docs/fed/>
- [24] Shibboleth Information Sheet Overview
<http://www.internet2.edu/pubs/shibboleth-infosheet.pdf>
- [25] OpenID Authentication 2.0 – Final
http://openid.net/specs/openid-authentication-2_0.html
邦訳：OpenID Authentication 2.0 - 最終版
<http://openid-foundation-japan.github.com/openid-authentication.html>
- [26] OpenID Attribute Exchange 1.0 – Final
http://openid.net/specs/openid-attribute-exchange-1_0.html
邦訳：OpenID Attribute Exchange 1.0 - 最終版
<http://openid-foundation-japan.github.com/openid-attribute-exchange.html>
- [27] カンターラ・イニシアティブ、複数のアイデンティティ管理プロトコルに対応した相互運用性試験に関する認定プログラムを開始
<http://kantarainitiative.org/confluence/display/WGJ/2010-04-26+Interoperability+Program>

- [28] カンタラ・イニシアティブ、Open Identity Exchange、OpenID Foundation などと共同でマルチプロトコルの連携型相互運用性デモを実施
<http://kantarainitiative.org/confluence/display/WGJ/2010-07-19+Multi-Protocol+Demonstration>
- [29] カンタラ・イニシアティブと Open Identity Exchange、トラスト・フレームワークの普及に向けて協業
<http://kantarainitiative.org/confluence/display/WGJ/2010-07-27+KI+and+OIX+Collaboration>
- [30] Kantara Initiative <http://kantarainitiative.org/>
- [31] Liberty Alliance <http://www.projectliberty.org/>
- [32] 総務省 情報通信政策研究所
ID ビジネスの現状と課題に関する調査研究 報告書 2010 年 4 月
http://www.soumu.go.jp/main_content/000061624.pdf
- [33] 解雇者によるサイバー犯罪が増加、ベライゾンが 2009 年のデータ侵害事件を分析
<http://itpro.nikkeibp.co.jp/article/Research/20100917/352144/>
- [34] 2010 Data Breach Investigations Report
http://www.verizonbusiness.com/resources/reports/rp_2010-DBIR-combined-reports_en_xg.pdf
- [35] 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
- [36] @IT ネットワーク用語辞典 LDAP
<http://www.atmarkit.co.jp/aig/06network/ldap.html>
- [37] Michael E. Schuckers :
Computational Methods in Biometric Authentication: Statistical Methods for Performance Evaluation, Springer-Verlag 2010 年 6 月

第 2 章

- [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
- [6] 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
- [7] 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。
- [8] Duane Blackburn NSTC Activities in Biometrics and Identity Management 2008 年
<http://www.biometrics.gov/Documents/Blackburn%20-%20IdM%20and%20Biometrics%20for%20ITAA.pdf>
- [9] 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>
- [10] National Science and Technology Council
Identity Management Task Force Report 2008 2008 年
<http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf>
- [11] BIMA FAQs <http://www.biometrics.dod.mil/About/faqs.aspx>
- [12] Standards Development
<http://www.biometrics.dod.mil/CurrentInitiatives/Standards/development.aspx>
- [13] National Strategy for Trusted Identities in Cyberspace Draft 2010 年 6 月
http://www.dhs.gov/xlibrary/assets/ns_tic.pdf
- [14] Fact Sheet for National Strategy for Trusted Identities in Cyberspace
<http://www.whitehouse.gov/the-press-office/fact-sheet-national-strategy-trusted-identities-cyberspace>

- [15] Jean Camp : Identity Management's Misaligned Incentives
IEEE security & privacy, PP.90-95, Vol8, No6, 2010
- [16] Primelife <http://www.primelife.eu/>
- [17] PICOS <http://www.picos-project.eu/>
- [18] SWIFT <http://www.ist-swift.org/>
- [19] FIDIS <http://www.fidis.net/>
- [20] PRIME <https://www.prime-project.eu/>
- [21] GUIDE <http://www.guide-project.org/>
- [22] The TURBINE Project <http://www.turbine-project.org/>
- [23] TURBINE: Trusted revocable biometric identities
Biometric Technology Today , February 2009, p.8-p.10
- [24] ISO/IEC FCD 24745
http://www.iso.org/iso/catalogue_detail.htm?csnumber=52946
- [25] 総務省 情報通信政策研究所
ID ビジネスの現状と課題に関する調査研究 報告書 2010年4月
http://www.soumu.go.jp/main_content/000061624.pdf
- [26] STORK https://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1
- [27] 首相官邸 高度情報通信ネットワーク社会推進戦略本部 (IT戦略本部)
電子政府ガイドライン作成検討会 セキュリティ分科会報告書 2010年2月
http://www.kantei.go.jp/jp/singi/it2/guide/security_guide_line/siryou2.pdf
- [28] European Identity Conference 2009 <http://www.kuppingercole.com/events/eic2009>
- [29] IDM2010 <http://www.idm2010.co.uk/>
- [30] Identity Management 2010 <http://events.oasis-open.org/home/IDM/2010>
- [31] Gartner Identity & Access Management Summit A Post-Event Snapshot
http://www.gartner.com/it/content/502200/502298/2006iam_final.pdf
- [32] Gartner Identity & Access Management Summit (2010年)
<http://www.gartner.com/technology/summits/na/identity-access/index.jsp>
- [33] Gartner Identity & Access Management Summit (2011年)
<http://www.gartner.com/technology/summits/emea/identity-access/index.jsp>
- [34] Identity Management for National Defense
<http://www.iqpc.com/ShowEvent.aspx?id=189628&langtype=1033>
- [35] 2010 Biometric Consortium Conference & Technology Expo
<http://www.biometrics.org/bc2010/>
- [36] Biometrics2011 <http://www.biometrics.elsevier.com/index.htm>
- [37] 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>

- [38] 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>
- [39] カンターラ・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>
- [40] OpenID Tech Night Vol.6
<http://www.openid.or.jp/modules/news/details.php?bid=30>
- [41] 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>
- [42] 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>
- [43] 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>
- [44] 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/>
- [45] 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
- [46] 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/>
- [47] 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
- [48] Kenta Takahashi : Cancelable Finger Vein Authentication as a Cloud Service、ABC
Malaysia Conference、2010. 12
- [49] 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
- [50] @IT ネットワーク用語辞典 LDAP
<http://www.atmarkit.co.jp/aig/06network/ldap.html>

第 4 章

- [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 頁による。
- [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.

- [10] 米国の個人情報保護制度については、新保・前掲注(2)308頁以下、岡村久道＝新保史生『電子ネットワークと個人情報保護』（経済産業調査会、2002）121頁以下、石井・前掲注(2)419頁以下など参照。
- [11] 我が国における個人情報保護法制定にいたる経緯については、園部逸夫編『個人情報保護法の解説（改訂版）』（ぎょうせい、2005）5頁以下、岡村・前掲注(7)10頁以下、宇賀克也『個人情報保護法の逐条解説（第3版）』（有斐閣、2009）1頁以下、三宅弘＝小町谷育子『個人情報保護法』（青林書院、2003）54頁以下など参照。
- [12] 岡村・前掲注(7)10頁以下。
- [13] See, e.g. John D Woodward Jr., *Biometrics: Identifying Law and Policy concerns*, *BIOMETRICS Personal Identification in Networked Society*, 385-405 (1999). 村上・前掲注(1)「バイオメトリクスに関する法的諸問題」76頁。
- [14] 肖像権一般については、大家重夫『肖像権（新版）』（太田出版、2007）、佃・前掲注(2)239頁以下、五十嵐清『人格権法概説』（有斐閣、2003）163頁以下など参照。
- [15] 簡単な紹介としては、例えば、<http://www.nhk.or.jp/zero/dsp32.html>;
<http://www.jaisa.or.jp/topics/pdfs/01-2.pdf> などがある。
- [16] このようなシステムについては、すでに実証実験が行われている。例えば、2006年5月に東京メトロ霞ヶ関駅において、顔認証システムを用いた地下鉄セキュリティ実証実験が行われている。これは、改札などを通行する人物を複数のカメラで撮影し、立体画像データ処理により、事前に登録されているデータベースの画像データ一覧と照合し、画像の人物を特定するものである。この実証実験については、http://www.mlit.go.jp/tetudo/kiki/pdf/2_3_2jissyoujikken.pdf を参照。
- [17] 防犯カメラの適法性については、さしあたり、前田雅英「防犯カメラの役割と設置の要件」『河上和雄先生古稀祝賀論分集』（青林書院、2003）501頁、亀井源太郎「防犯カメラ設置・使用の法律問題—刑事法の視点から」都法43巻2号（2003）111頁など参照。
- [18] *BIOVISION, Privacy Best Practice in Deployment of Biometric Systems*, (<http://www.eubiometricsforum.com/dmdocuments/D7.4%20Best%20Practices1.pdf>) .
- [19] ベストプラクティスの訳文については、BSC リーガル WG における翻訳を参考にした。
- [20] *ARTICLE 29 - Data Protection Working Party, Working Document on Biometrics*, (http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf) .
- [21] 学説の詳細については、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」114頁以下参照。
- [22] 金融庁「金融分野における個人情報保護に関するガイドライン」
(<http://www.fsa.go.jp/siryousiryousiryou/kj-hogo/01.pdf>) .
- [23] 金融庁「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」(<http://www.fsa.go.jp/siryousiryousiryou/kj-hogo/04.pdf>) .

- [24] IdM の最近の動向については、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 92 巻 4 号（2009）287 頁など参照。
- [25] 岡田浩一＝大西真樹＝富士仁「シングルサインオンにおけるプライバシー保護について」情報技術レターズ 1 号（2002）229 頁。
- [26] 高橋・前掲注(24)288 頁。
- [27] 高橋・前掲注(24)288 頁以下。
- [28] 高橋・前掲注(24)290 頁。
- [29] 高橋・前掲注(24)290 頁以下。
- [30] 高橋・前掲注(24)291 頁。
- [31] 崎村夏彦「OpenID 利用者中心のインターネット社会の実現に向けて」（2010）9 頁
〈http://www.soumu.go.jp/main_content/000066402.pdf〉。
- [32] <http://www.openid.ne.jp/>。
- [33] 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/syokukai/H21_houkoku/h21annual-report/02_02.pdf〉。
- [34] 高橋・前掲注(24)289 頁。
- [35] 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/syokukai/H20_houkoku/H20annual-report/02_02.pdf〉。
- [36] 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(35)26 頁以下参照。
- [37] BIAS については、本報告書の第 3 章を参照。
- [38] 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。
- [39] 本報告書の第 3 章を参照。
- [40] 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。
- [41] 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。

—禁無断転載—

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

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