24 - 84

平成２４年度

IdM における共通本人認証基盤の開発研究

報　　告　　書

平成２５年３月

一般社団法人　日本自動認識システム協会

この事業はオートレースの補助(24-84)を受けて実施しました。

http://ringring-keirin.jp

はじめに

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よう自動認識システムの研究開発を続けることが必要です。

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、一般社団法人日本自動認識システム協会では、自動認識システム関する研究開発事業を実施しております。

近年のオープンシステム、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充実･普及などに伴い、サービス形態の多様化と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きております。

このような中、当協会は、なりすましなどの防止に有効である高いセキュリティ機能を持つと言われている生体情報（バイオメトリクス）を利用した個人認証技術と各サービス間の認証連携に有効であるといわれている IdM 技術を組み合わせるための技術の研究開発に､財団法人 JKA の機械工業振興活動として平成 23 年度は競輪の補助(23-7)、平成 24 年度はオートレースの補助(24-84)を受けて取り組んで参りました。

この「平成 24 年度　IdM における共通本人認証基盤の開発研究 報告書」は、上記研究開発事業の平成 24 年度活動の成果です。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一つの礎石として皆様方のお役に立つことが出来れば幸いです。

最後になりますが、本調査研究の実施にあたり、IdM における共通本人認証基盤の開発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、深く感謝を申し上げます。

平成25年3月

一般社団法人 日本自動認識システム協会

目　　次

１．開発研究の目的

近年の電子行政サービスや民間での電子サービスの充実に伴い、サービス形態が多様化している。この中で、ユーザおよび事業者に一層の利便性を提供するため、各サービス間での認証連携が必要とされ始めており、認証を取り巻く環境が大きく変わりつつある。

従来から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、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。このような中、パスワード漏洩時の被害の増大が懸念され、この危険性を回避するため本人認証基盤のセキュリティ強化を望む声がある。

また、電子行政サービスや民間での電子サービスで SAML や OpenID に代表される IdM システム(Identification Management System)が導入され始めているが、これら電子行政サービスや民間での電子サービスのシステムに共通的に適用され得るポテンシャルを持ち、両者のサービスをシームレスに接続する横断的なソリューションに適用可能な共通本人認証基盤が、今後のサービスの展開には必要と考えられている。

これに対応してゆくため、セキュリティリスクの少ない効率的に管理・運用のできる IdM として、本人認証にバイオメトリック技術が導入された IdM システムが全世界的に適用、運用され、その結果として安全で安心できる経済・社会活動が営まれることを目指し、IdM 技術とバイオメトリック認証技術を組み合わせる新しい本人認証基盤（以下「共通バイオメトリック認証基盤」という）を研究、開発することを目的とした。

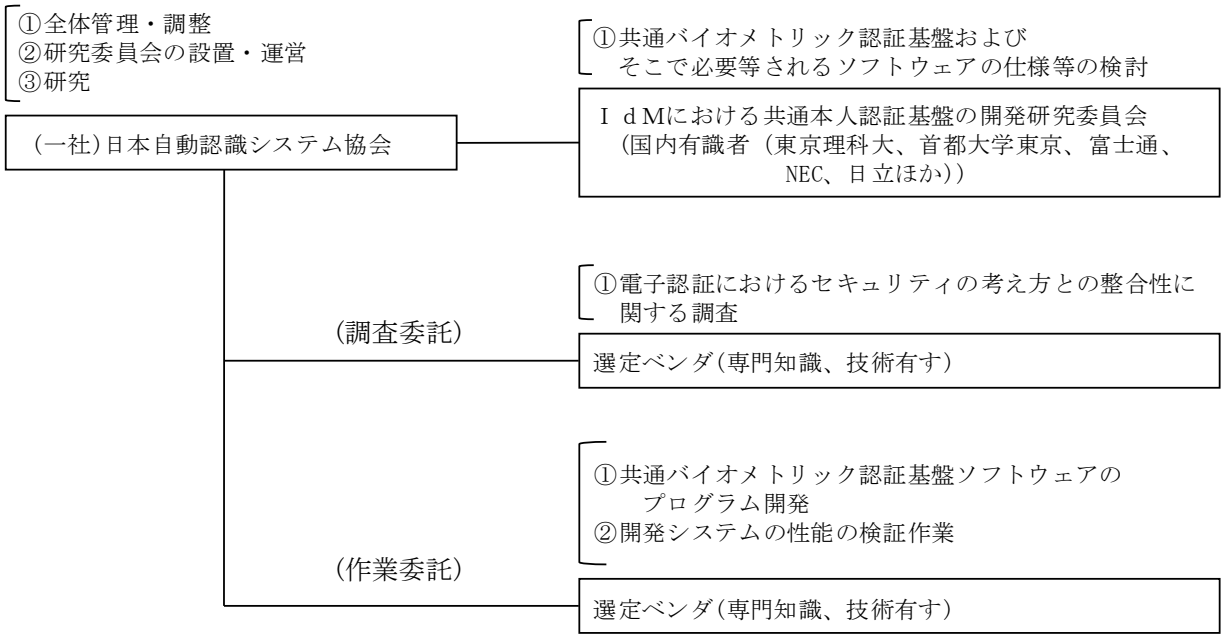
２．開発研究の実施体制

(1) 管理体制および研究体制

一般社団法人日本自動認識システム協会（以下 JAISA という。）にて、産官学の有識者による IdM における共通本人認証基盤の開発研究委員会（以下委員会という。）を構成、運営し、共通バイオメトリック認証基盤の仕様ならびにそこで必要とされるソフトウェアの仕様等の検討を行った。

委員会での仕様検討時に必要とされる海外調査は、具体的な調査先および派遣者を委員会にて検討の上、実施した。また、委員会で仕様検討時に必要とされる専門的事項の調査も行ったが、このうち委託調査が必要なものについては、当該研究分野の専門技術を持つ委員会の構成メンバのベンダ各社より選定の上、委託して調査した。

また、委員会にて検討したソフトウェア仕様の確認のため、プロトタイププログラムの開発や本開発システムの性能評価等の検証等の作業を作業委託して実施し、その内容を委員会にて審議、検証した。これらの開発検証作業は、当該研究分野の専門技術を持つ委員会の構成メンバのベンダ各社より選定の上、作業委託し実施した。



(2) IdM における共通本人認証基盤の開発研究委員会

IdM における共通本人認証基盤の開発研究委員会委員名簿（順不同・敬称略）

役割	氏名	所属	備考
委員長	半谷精一郎	東京理科大	SC37WG3 委員
委員	瀬戸 洋一	首都大学東京　産業技術大学院大学	SC37 国内委員会 委員長
委員	中村 敏男	(株)OKI ソフトウェア	SC37WG2 委員
委員	山口 利恵	独立行政法人産業技術総合研究所	
委員	菊地 健史	(株)日立ソリューションズ	
委員	坂本 静生	日本電気(株)	SC37WG3 委員
委員	福田 充昭	(株)富士通研究所	SC37WG2 委員
委員	吉福 貴史	日立オムロンターミナルソリューションズ(株)	SC37WG2 エキスパート
委員	平野 誠治	凸版印刷(株)	SC37WG3 エキスパート
委員	山田 朝彦	東芝ソリューション（株）	SC37WG2 委員 SC37WG5 委員
オブザーバ	鎌倉　健	(株)富士通研究所	
オブザーバ	諫田 尚哉	(株)日立製作所	SC37WG5 幹事 SC37WG6 委員
オブザーバ	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)	SC37WG3 委員
オブザーバ	熊谷　隆	(株)日立ソリューションズ	SC37WG2 主査
オブザーバ (7 月まで)	山中　豊	経済産業省	SC37 専門委員
オブザーバ (7 月より)	岩永 敏明	経済産業省	SC37 専門委員
オブザーバ (11 月まで)	川内 拓行	経済産業省	
オブザーバ (11 月より)	山中 裕二	経済産業省	
事務局	酒井 康夫	(一社)日本自動認識システム協会	SC37WG2 ﾘｴｿﾞﾝ SC37WG6 主査

３．研究開発の実施計画

本事業は、IdM システム開発者、バイオメトリック技術ベンダに対して、以下の事項を汎用的に提供することを目指し、民間サービスだけでなく、公共性の高い電子行政サービスにも適用可能な IdM システムにバイオメトリクスを組み込むことを可能とする本人認証基盤の研究、開発とその評価を行うことを目指して、3 年間で行うことで計画し、活動している。

(1) 多様化した電子サービスに向けバイオメトリック認証技術を用いた強固で利便性の高いセキュリティの提供

(2) バイオメトリック装置、システムの開発範囲をスリム化することによる開発コストの低減と開発期間の短縮

(3) 開発したインタフェースを国際規格化し世界的な共通プラットフォームとすることによる国際競争力の向上

3 年間全体の開発計画は以下の通りある。

・H23 年度：認証基盤プロトタイプの開発研究 1
（単一技術における認証基盤の重要部分（生体情報取得機能）を開発する。）

・H24 年度：認証基盤プロトタイプの開発研究 2
（単一技術における認証基盤全体の開発として IdM システムへの組み込みを完了する。）

・H25 年度：認証基盤オープンソースの完成
（主要技術（指紋、静脈、顔、虹彩）が組み込み可能な認証基盤の完成）

平成 24 年度の開発研究は、平成 23 年度の活動成果をもとにして、認証基盤プロトタイプの開発研究の第 2 年度として、単一技術における認証基盤全体の開発を完了することを目標とし、次の事項の実施を計画した。

(1) 共通バイオメトリック認証基盤ソフトウェアの研究、開発

(2) 開発システムの検証実験の実施及び評価

４．開発研究の内容概要

4.1　平成 24 年度の実施事項

平成 24 年度の開発研究では、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ック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 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 に実装する共通バイオメトリック認証基盤を開発するため、次の 2 項目を実施した。

なお、本開発研究は、財団法人 JKA の機械工業振興活動としてオートレースの補助(24-84)を受けて活動した。

(1) 共通バイオメトリック認証基盤ソフトウェアの研究、開発

① 関連技術の最新動向調査（委員を派遣して実施）

バイオメトリクスに関する市場形成のシーズの明確化と大きなシナリオのもとでの開発が必要なため、平成 23 年度に引き続き、海外におけるカンファレンス調査として 10 月下旬に開催された英国 Biometrics Exhibition and Conference 2012(BC2012)の調査を行い最先端の動向を調査した。

②電子認証におけるセキュリティの考え方との整合性に関する調査（委託調査として実施）

平成 24 年度の委員会での検討で、「バイオメトリクスの持つセキュリティ性という観点」だけではなく、それと異なる観点が必要である「電子認証システム等で近年考慮されるようになったセキュリティの考え方への対応にまで考慮範囲を拡張した」研究開発の必要性が明らかになった。このため「電子認証におけるセキュリティの考え方との整合性に関する調査」を行った。委託調査は、当該研究分野の専門技術を持つベンダ各社より選定の上、委託し実施した。

③ 共通バイオメトリック認証基盤の仕様検討

共通バイオメトリック認証基盤として共通本人認証基盤（BioIDM システムと称する）に関する仕様検討を行った。今年度は、単一技術における認証基盤全体の開発として IdM システムへの組み込みを完了することに集中して検討した。

④ プロトタイプの開発（委託作業として実施）

委員会で検討したソフトウェアの仕様等の確認のためプロトタイププログラムを開発した。作業は、当該研究分野の専門技術を持つベンダ各社より選定の上、作業委託し実施した。

(2) 開発システムの検証実験と評価（委託作業として実施）

プロトタイププログラムを用い開発システムの性能評価等の検証作業を実施し、その内容を委員会にて審議、検証した。検証作業は、当該研究分野の専門技術を持つベンダ各社より選定の上、作業委託した。

4.2　平成 24 年度の実施日程と概要

平成 24 年度開発研究は、図 1 に示す日程で実施した。

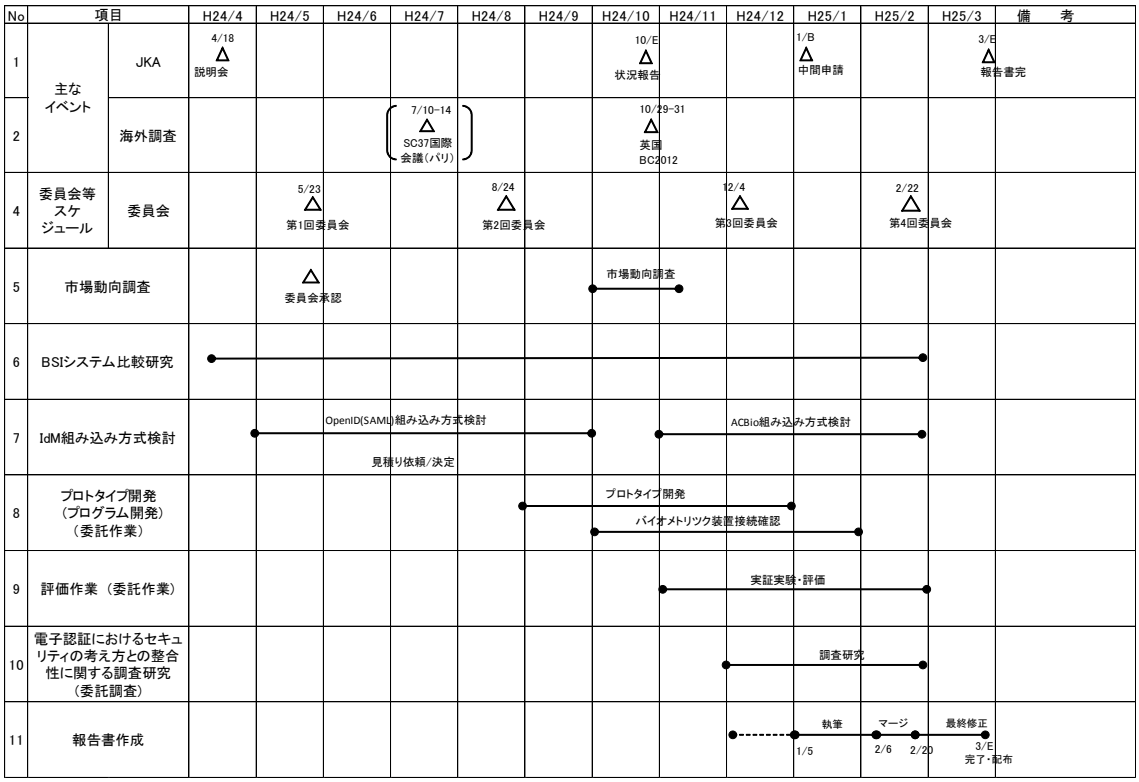


図 1　開発研究実施日程

(1) 共通バイオメトリック認証基盤ソフトウェアの研究、開発

① 関連技術の最新動向調査（委員を派遣して実施）

関連技術の最新動向調査は、第 1 回委員会の審議により、具体的な海外調査として、定点観測として昨年に引き続き英国 Biometrics Exhibition and Conference 2012 の調査を瀬戸委員にお願いすることとなり、10 月下旬にコンファレンスでの講演を調査し最先端の動向を調査した。

② 電子認証におけるセキュリティの考え方との整合性に関する調査（委託調査として実施）

電子認証におけるセキュリティの考え方との整合性に関する調査は、電子認証におけるセキュリティの考え方との整合性に関する以下の調査と整理を行った。

1) 電子認証システム関連規格調査

2) 電子認証システム等のセキュリティの考え方の整理

3) 電子認証システム等のセキュリティの考え方に対応するため要件の整理

OpenID への BioIDM の組込みを踏まえ、電子認証システムにおけるセキュリティの考え方に対応することを考慮した電子認証システムとの連携するために必要な事項、要件についてまとめた。

委託調査は、当該研究分野の専門技術を持つベンダ各社より選定の上、委託し実施した。

③ 共通バイオメトリック認証基盤の仕様検討

IdM に単一のバイオメトリック認証技術が組み込まれた形でバイオメトリック共通認証基盤が動作するバイオ IdM システムを検討するため、下記を実施した。

1) OpenID あるいは SAML のようなインタフェースを持つ IdM システムと平成 23 年度に開発した「BioIDM Connection」の接続方式の検討と仕様の開発

2) ベンダ BSP と平成 23 年度に開発した「BioIDM Transaction」の接続の検討

検討にあたっては、委員会を開催し、その中で仕様提案および検討を進めた。

この委員会活動は、下記にて実施した。

・第 1 回　平成 24 年 5 月 23 日(水)　13:00～15:00　JAISA にて開催
　－趣旨説明及び全体計画紹介
　－調査計画案審議
　－検証実験および参加依頼
・第 2 回　平成 24 年 8 月 24 日(金)　15:00～17:00　JAISA にて開催
　－共通認証基盤システムの仕様審議
　－Biometrics exhibition and conference 2012 の調査案審議
　－ドイツ・フランス状況報告
　－作業委託説明
・第 3 回　平成 24 年 12 月 4 日(火)　10:00～12:00　JAISA にて開催
　－Biometrics exhibition and conference 2012 調査報告
　－バイオメトリクスと ID 体系の整理報告
　－共通認証基盤システム検討状況審議
・第 4 回　平成 25 年 2 月 22 日(金)　15:00～17:00　JAISA にて開催
　－共通認証基盤システム検討状況審議

④ プロトタイププログラムの開発

委員会で検討したソフトウェアの仕様等の確認のためプロトタイププログラムを開発した。OpenID プロバイダとして WSO2 社のオープンソースである Identity Server 4.0 版を使用し、生体認証装置としては日立製作所の指静脈認証装置 PC-KCA100 を用いたプロトタイプシステムを開発した。なお、プログラム開発作業は、当該研究分野の専門技術を持つベンダ各社より選定の上、作業委託し実施した。

(2) 開発システムの検証実験と評価

共通バイオメトリック認証基盤の仕様検討結果に沿って開発した BioIDM システムのプロトタイププログラムについて、その機能や性能の有効性を検証するために検証実験を行った。

なお、その内容を委員会にて審議、検証した。検証作業は、当該研究分野の専門技術を持つベンダ各社より選定の上、作業委託した。

4.3 成果概要

(1) 共通バイオメトリック認証基盤ソフトウェアの研究、開発

① 関連技術の最新動向調査

昨年に引き続き 10 月下旬に開催された英国 Biometrics Exhibition and Conference 2012 の調査を行った。

しかしながら、例年に比べ、内容が充実していない感があった。この原因は、欧州では、公的市場（社会 ID）の開発が一段落したことと、金融問題などにより民間市場が立ち上がっていない、あるいは飽和している状況にあるためではないかと考える。

社会的（ID 関係の実証プロジェクト、脆弱性プライバシーなどのプロジェクト）には、相変わらず欧米は日本よりはるかに進んでいるが、技術開発的には日本の企業の方が遥かに進んでいるとの感想を持った。

また、欧州は、アフリカ、中近東などかつての宗主国のポジションを利用し、これらの国へのバイオメトリクスを市場展開することに重点を置いて取り組んでいるように感じられた。

このことを考えると、日本において、社会的な大型プロジェクトが実施されていないこと、アジアへの市場展開が遅いことが、日本の産業界の問題ではないかと考えられる。

また、本研究で実施したようなアプローチで IdM 技術を開発した事例は、今年度の調査では見当たらなかった。平成 23 年度の研究報告では米国ではエコシステムの開発を進めていると報告したが、今年度、その実体が把握できなかった。現在は、モバイル端末などの利用者サイドの開発から進んでいるようであると感じている。

② 電子認証におけるセキュリティの考え方との整合性に関する調査

電子認証システム関連規格調査およびセキュリティの考え方の整理として、米国の電子認証システムのための本人認証に関するガイドラインである OMB M-04-04 および NIST SP 800-63 について調査を行った。この結果、電子認証システムにおける本人認証の保証レベルが 1 から 4 までの 4 段階で定義される中で、ハードウェアトークン・ソフトウェアトークン・パスワードなどの既存の本人認証技術を用いることで達成される保証レベルに対して、生体認証技術はその保証レベルを引き上げる役割を与えられていることが分った。

次に、電子認証システム等のセキュリティの考え方に対応するための要件の研究として、OpenID と生体認証を組み合わせたシステム要件について検討した。現在広く普及している OpenID システムが比較的低い保証レベルで使われるケースが主流であるのに対して、電子認証システムのための本人認証ガイドラインにおいては生体認証技術の位置づけがより高い保証レベルを実現するものとして捉えられている。保証レベルの不一致を避けることができるシステム要件を検討した結果、震災時の電子認証システムを取り上げた。震災時における利用環境を考えると、ハードウェアトークン・ソフトウェアトークン・パスワードのいずれも、電子認証システムにおける本人認証として被災者に適用するには困難さが存在する。これに対して生体認証は、

簡便さと高セキュリティという 2 つの特長に加えて、紛失・盗難の恐れがなく、また記憶する必要もないため、震災時において広範囲な被災者への適用が可能であると考えられる。

今後は、OpenID と生体認証を組み合わせた具体的な震災対応システムを検討・開発し、その有効性を確認する必要がある。

③ 共通バイオメトリック認証基盤の仕様検討

共通バイオメトリック認証基盤として共通本人認証基盤（BioIDM システムと称する）に関する仕様検討を行った。

BioIDM システムは IdM のプロトコルとして SAML に比べて実装が軽いといわれている OpenID を開発容易性が高いと解釈し、採用することとした。

BioIDM システムのシステム構成として、運用上標準的に用いられることを想定した標準構成と、構造がより単純な簡易構成の 2 種類を検討し、両構成の処理の流れ、長所と短所を明確にした。

標準構成における処理の流れについては開発効率を考慮し、OP・BP・UA 間のプロトコルとして OpenID プロトコルを採用することとした。認証方式としてはサーバ認証に比べてセキュリティ対策の条件が緩やかなローカル認証方式を採用することとした。

サーバ側で動作するプログラムとして OP における BP との連携機能、BP における OP との連携機能およびバイオメトリック登録・認証機能の仕様検討を行い、また、端末側で動作するプログラムとして、前年度開発の BioIDM Connection と BioIDM Transaction における登録・照合機能の仕様検討を行った。

また、以上の仕様検討結果を受けて、OpenID プロバイダを用いるプロトタイプシステムの開発仕様を明確にした。プロトタイプシステムの開発においては、OpenID プロバイダとして WSO2 社のオープンソースである Identity Server 4.0 版を使用し、生体認証装置としては日立製作所の指静脈認証装置 PC-KCA100 を用いたプロトタイプシステムを開発することとした。

(2) 開発システムの検証実験と評価

共通バイオメトリック認証基盤の仕様検討結果に沿って開発した BioIDM システムのプロトタイププログラムについて、その機能や性能の有効性を検証するために検証実験を行った。

実行環境の要素を変化させながら様々な環境で BioIDM システムの検証実験を行うこととし、東京理科大学殿のご協力によりサーバを 2 機借用し、それぞれに OP と BP をインストールしてインターネット上に OP や BP を配置して実験を行った。

端末としては(株)OKI ソフトウェア殿のイントラネット上にある端末を 2 機種用いた。これらは埼玉県と広島県という国内において地理的に離れた場所に設置されているものである。

検証実験の成果を下記に示す。

①基本条件試験および簡易構成試験

WSO2 の Identity Server と BioIDM システム（BioIDM Connection、BioIDM Transaction、BioAPI Framework）および日立指静脈認証装置を組み合わせることにより、バイオメトリック認証を用いた OpenID システムのバイオメトリック情報登録から認証ま

での基本機能および SSO の機能が正常に動作することを確認できた。

②性能測定

標準構成と簡易構成の 2 種類の構成で、バイオメトリック認証に要する時間を計測した。特に標準構成において OP と BP の間の通信処理時間が大きく、簡易構成の約 2 倍の時間がかかっていることがわかった。RP や OP・UA などの各構成要素間の OpenID プロトコルのための通信回数が多く、その分時間を要したことが標準構成において時間がかかる原因と考えられる。標準構成における性能改善について今後検討する必要があることがわかった。

③ブラウザと SSL

WebSocket は主要ブラウザへの搭載が出揃ったばかりの比較的新しい技術であるが、Google Chrome・Internet Explorer 10（Windows7 Prerelease 版）、Firefox ともに BioIDM Transaction との WebSocket 通信が正常に動作することが確認できた。ただし、BioIDM Transaction に組み込んだ WebSocket において現状 SSL が実現されておらず、セキュリティ上の問題となるとともに、Internet Explorer 10 や Firefox では Web サーバが HTTPS で動作している場合、WebSocket が SSL 未サポートだと通信が失敗してしまうことがわかった。WebSocket の SSL 対応版 OSS の提供がはじまったため、今後対応が可能であると考えている。

④国内・海外 RP 接続

国内 RP、海外 RP ともに今回開発した BioIDM システムの標準構成にてバイオメトリック認証による正常なログオンが行えることがわかった。ただし、一部の RP について正常動作しなかった。いくつかのケースにおいて OP に対して OpenID プロトコルが通知されてこないことから、RP が利用可能な OP を限定している可能性が考えられる。それ以外の RP においては原因が特定されていないものもあるため、本事業で開発したシステム側の原因かどうかの切り分けが今後必要であると考えている。

4.4　次年度以降に向けての課題

(1) 共通バイオメトリック認証基盤ソフトウェアの研究、開発に関して

平成 24 年度の活動では、電子認証システム等で近年考慮されるようなったセキュリティの考え方に融和できる形での開発が必要であるとことがわかった。

また、今後、電子行政サービスや民間での電子サービスに広く適用するための基盤を作ることが重要であり、標準化への取り込みも重要であると考えている。

このため、次の事項が今後の課題であると考えている。

①バイオメトリクスの特長を生かしながら、ＩｄＭシステムなどの電子認証システムとして十分なセキュリティ機能を持つ本人認証基盤とすること

②具体的な応用事例として震災対応システムへの応用にむけた検証

③標準化に向けた検討

(2) 開発システムの検証実験と評価に関して

今年度の検証実験から得た課題として今後検討が必要と考えている事項を下記に示す。

①性能面で標準構成における性能改善に向けた検討

②ブラウザと SSL について、WebSocket が SSL 未サポートだと通信が失敗してしまうことに対しては、WebSocket を SSL 対応にすることで解決することの検証

③国内・海外 RP 接続において、一部の RP について正常動作しなかったたいくつかのケースについて、BioIDM システム側の原因かどうかの切り分け

５．開発研究の詳細

第１章　総論

1.1　IdM における共通本人認証基盤の必要性と概念

近年の電子行政サービスや民間での電子サービスの充実に伴い、サービス形態が多様化している。この中で、ユーザおよび事業者に一層の利便性を提供するために、例えば SSO(Single Sign On)に代表されるような各サービス間での認証連携が必要とされ始めている。

従来から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、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。

IdM システム(Identification Management System)側では、複数の電子サービスに跨る利便性を提供するため、SAML や OpenID に代表される IdM システムが導入され始めている。これらは電子行政サービスや民間での電子サービスのシステムを跨って適用されるポテンシャルを持っているため、セキュリティに関しては従来以上に配慮する必要があると考えられる。このため、全世界的に適用､運用される複数の IdM システムに跨って適用でき､かつ従来以上にセキュリティリスクの少ない共通本人認証基盤が、今後必要になると考えられる。

これの実現に向かうフィージビリティスタディとして､平成 22 年度に財団法人機械システム振興協会殿より受託して､「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」を実施した。その結果、適用する IdM システムとして現在の主流となっている SAML や OpenID に的を絞り､また市場にあるバイオメトリック認証装置に広く対応できる形で実現してゆくことが必要であるとの見解を得た(図 1.1)。

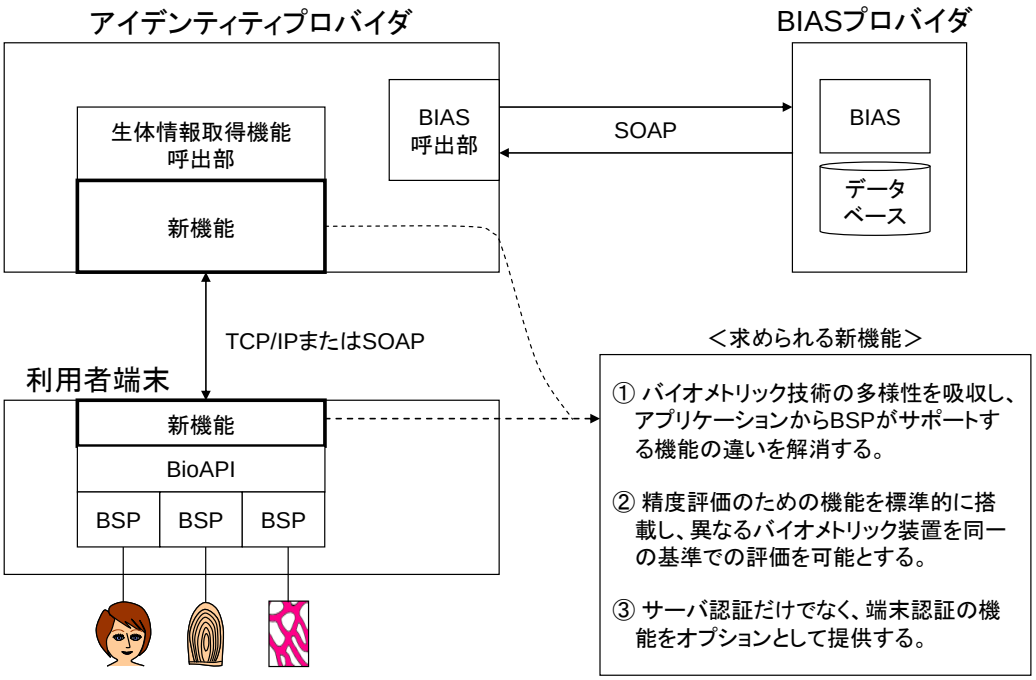


図 1.1　IdM と連携するバイオメトリック認証に求められる新機能

フィージビリティスタディで課題となった新機能の実現に向け、バイオメトリック認証技術に基づいて IdM 技術とバイオメトリック認証技術を組み合わせる新しい本人認証基盤を「共通バイオメトリック認証基盤」と名付け、今年度、研究開発に取り組んだ。

その概念は、図 1.2 に示すように、SAML や OpenID に代表される IdM システムで認証機能を担うアイデンティティプロバイダとのインタフェース機能を実現する「生体認証用 OpenID プロトコル処理部」あるいは「生体認証用 SAML 処理部」を備え、その下位に市場にあるバイオメトリック認証装置に非限定的に対応する機能を実現する「生体認証用共通処理部」を持つものである。この「生体認証用共通処理部」の元にハードウェアとしてのバイオメトリック認証装置を配置し、生体認証を IdM に組み込むことを実現するものである。

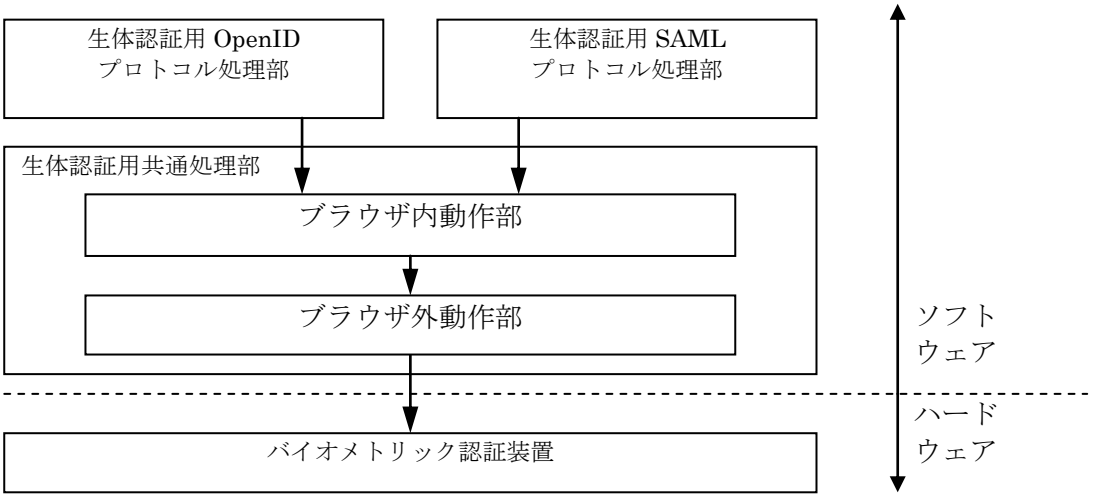


図 1.2　共通バイオメトリック認証基盤の概念

1.2　平成 23 年度活動成果概要

本事業の平成 23 年度活動成果概要は以下である。

(1)関連市場の最新動向調査

平成 23 年 9 月 18 日から 20 日まで、英国ロンドンで開催された Biometrics exhibition and conference 2011 を調査した。その結果、バイオメトリック装置を使った社会 ID や国境管理システムなどの大規模システムの構築が大きな流れとなっていること、および、各国で構築する ID システムは、国民 ID と民間 ID などと連携して行うことにより利用者へ様々なサービスを効率よく提供できるエコシステムの実現を目的にしているようであることが確認できた。また、バイオメトリクスをシステム構築要素の観点でとらえ、バイオメトリック認証と IdM を組み合わせる新しいアーキテクチャの重要性は増してきていると考えられることが確認できた。

(2)生体認証用共通処理部の詳細設計

IdM システムにバイオメトリック認証を組み込むための生体認証用共通処理部のアーキテクチャを検討し、詳細仕様設計を完了した。生体認証用共通処理部にはブラウザでのグラフィックユーザインタフェースや、様々なバイオメトリック装置が接続できる共通的な仕組みが必要であり、BioIDM と名付けた生体認証用共通処理部の仕様を検討した。BioIDM は、ブラウザ上でバイオメトリック登録や照合を実現するためのグラフィックユーザインタフェースを含んだソフトウェアコンポーネント（BioIDM Connection）と、バイオメトリック装置の性能を引き出す共通的な仕組みを持ったソフトウェアコンポーネント（BioIDM Transaction）の 2 つから構成し、これら 2 つのコンポーネント間のインタフェース仕様を検討した。本検討によって、バイオメトリック装置の共通部品化とインターネットへの接続性を達成した。

(3) プロトタイプ開発と妥当性検証

前述の設計に基づいたプロトタイプソフトウェアの開発を完了した。あわせて、検討したアーキテクチャおよびインタフェース仕様の妥当性検証のために速度評価を実施した。

その結果、BioIDM による全体性能へのインパクトが十分小さいことが判明し、設計の妥当性が確認できた。これにより、BioIDM を OpenID や SAML などの IdM システムと接続することにより、IdM システムにバイオメトリック認証機能を組み込むための準備を整えることができた。

第２章　共通バイオメトリック認証基盤ソフトウェアの研究、開発

2.1　関連市場の最新動向調査

バイオメトリック認証技術を用いた本人認証技術の市場および技術動向に関し調査した。

調査の目的は以下の 3 点である。

・IdM 関係の新技術、プロジェクトの調査

・適合性評価の状況調査

・モバイル関係の新技術、プロジェクトの調査

調査対象は、英国 ロンドンで開催された Biometrics exhibition and conference 2012 である。以下に概要を述べる。

1. 調査対象：Biometrics exhibition and conference 2012
2. 日程： 平成 24 年年 10 月 29 日−31 日
3. 場所： QEII カンファレンスセンター（ロンドン）
4. 概要：

・欧州を中心とした商業的なカンファレンス（コーディネータ Elsevier)。メインスポンサーNEC、富士通、展示会社 42 社、セミナー53（14 セッション)、
参加者約 225 名（セミナー登録者数)、
参加者の特徴：アフリカ、中近東の参加者も含まれる（5%）日本からの参加者：6 名
中国系（China 1 名 Hong Kong3 名）が参加登録者名簿以上に多く感じた。

・全般の感想として、展示会社数は、減っていない。Forensic 用途（DNA など）が新規に目につくほかは大きな注目点はない。セミナー参加者数は例年に比べ少なく感じる。一つのセッションの参加者は、30−70 名程度。

・セミナーの内容は、興味あるテーマの講演が中止になるなど、新規情報が少ないという感想である。これは、シェンゲン情報システムなどの開発も一段落し、DNA などの forensic 用途以外の大口の新市場が立ち上がっていない模様。また、モバイルなど新しい市場に関する発表もあったが、発表のレベルが低く、この分野の日本の技術的なリードは一目瞭然。

・欧州は入国管理システムに関し、アフリカ、中近東に対し、市場開拓のため技術的なリーダシップをとって取り囲みを図っているように感じた。

・日本として、(1)アジアの社会 ID 市場、(2)先行するモバイル技術に関する市場を、いかにリードするかのビジネス戦略が各企業に求められると考える。

以下、関係する発表に関し概要を述べる。

(1) Biometrics in EU border controls: The move towards smarter borders Nikos Isaris (Deputy Head of Unit Large-Scale IT Systems and Biometrics European Commission DG Home Affairs)

・シェンゲン情報システムは平成 7 年に第 1 期システム、平成 25 年に第 2 期システムが稼働。EORODAC は平成 15 年 1 月、EU の次世代 e-passport システムは顔、指紋を利用する。

・VIS システム（Smart border Package）は平成 23 年 10 月より稼働。技術的な問題はなく、アフリカ、中近東、湾岸地域に利用を拡張中。認証には過去は指紋であったが、今後は顔の利用を促進。マルチモーダル化を図る。平成 24 年中に Smart border legislation を提出する予定。

(2) Biometrics and borders - An update from Australian immigration

（David Chadwick, Director - Biometrics Projects, Identity Branch, Department of Immigration and Citizenship, Australia）

・Identiy の main components は、

-personal attribute

-Documents

-Social footprint

の 3 つ＋biometrics である。

・Biometrics を利用する理由は「成りすまし対策の最後の手段」と「比較的入手が容易」な点にある。Handheld device の開発が重要であり、将来的に real time identification を実現する。現在シドニー空港でパイロットプロジェクトを実施中。

・Biometrics 利用にあったての留意点は、以下にある。

-単独で用いない（isolation）

-標準ベース

(3) Biometrics in the EU-VIS - First year experiences and state of play（Fares Rahmun, VIS Project Manager, Federal Office of Administration (BVA) UK）

・欧州における国境における状況の紹介。中央の C-V VIS、VIS システムの基盤の BMS が中央で運用され、各国で registraion システムが連携するシステム構成であった。上記の中央システムにドイツで Nat、N-VIS が接続されている構成であった。

・運用は region1（北アフリカ）、Region2（中近東）、Region3（湾岸地域）となっており、平成 25 年に運用開始とのこと。

・エストニアに新しい EU 組織を構築するとのこと。

実践的な課題（Practice problem in the field）として下記をあげている。

-workflow adjustment

-Low level error

-biometric error

-Insufficient biometric quality（指紋の相互運用ができない）

・Usage of ESP(external service provider) from VISA application in EU is increase.

→長所　旅行者に便利、

短所　セキュリティ、データ保護の問題がある。EU の研究機関の Frontex が関与している。TR03121 (BSI) の標準を採用。

(4) What’s different about mobile biometrics?（David Benini, Senior Director of Marketing,Aware, Inc., USA）

・バイオメトリクスはなぜパワフルか？

バイオメトリクスはセキュリティを強化するための IdM である。Digital assets、physical assets を守るため

・Owner base 、permission base、 operator base などのスケールでアプリ開発があるという紹介。

・Mobile の紹介があるが、欧米で使う mobile は広い定義になっている。例えば入国管理における可搬型端末もモバイルという扱い。どちらかというと、こちらの方が多い。Mobile wallet における指紋利用はセキュリティを許可できる。

Mobile biometrics は大きな市場となる。

(5) UNHCR‘s Identity Management needs UnHo Choi (Senior ICT Security Officer Division of Information Systems and Telecoms)

・国連高等弁務官組織による、難民管理へバイオメトリクスの利用の紹介

UNHCR では 76,000 名が働いている。平成 24 年度の予算は 3,159 万ドル。難民の管理のために ID カードを発行している。

・2003 年以降、なりすましを防止するために指紋（crossmath）を利用しポリオ予防注射などを実施している。フェーズ 1 の試用が終了した。RFP を用意した。

バイオメトリクスは UHCR になじむ技術である。

(6) Achieving biometric success in government – The Nigerian National Identity Management System (NIMS)（Chris Onyemenam, Director General/CEO, National Identity Management Commission (NIMC), Nigeria）

・ナイジェリア政府における国民 ID 管理システム NIMS の話。

NIMS は下記を考慮して構築。

-Interoperability

-XML integration

-web サービス

-Authentication/Identification サービス

(7) その他：

・Daon が米国 NSTIC によって提案された trusted identities in Cyberspace における identity ecosystem のパイロットプロジェクトをスタートさせた。

・Intel Labs はラップトップコンピュータなどの認証に対し（パスワードの問題に対し）、バイオメトリクスが有効であることを発表した。また、指紋よりも手のひらスキャンが有効であることを発表した。手のひら静脈は、米国の healthcare 部門で採用された手のひら静脈は、HT

system の PatientSecure system を利用している。

・Apple と Google はモバイル端末の unlocking に顔認証を利用する特許を取得した。

・EC が出資した Biometrics Evaluation And Testing BEAT プロジェクトが開始された。

BEAT プロジェクトは、バイオメトリックシステムの信頼性を評価する 7 つのフレームワークプロジェクトを実施する。特に BEAT は以下の 3 点に焦点を置いている。

(a) 性能評価

(b) 成りすましなどの脅威に対する脆弱性に関するロバスト性

(c) プライバシー保護技術。

・BEAT は、北米、アジアでも同様に進む組織との連携を検討している模様。

BEAT は、システマティックな方法での評価、いくつかの評価尺度による性能評価、あるいは、性能、脆弱性、プライバシーなどの基準のフレームワークを構築することを目的とする。

・米軍において、バイオメトリクスは識別と認証を行う重要な技術であるととらえている。

平成 23 年年から 2015 年で３５００億円（3.5b ドル）の予算を組んでいる。バイオメトリクス技術は BIMA(Biometric Identity Management Agency)を中心に実施利用されてきた。米軍はヘビーユーザであり、技術革新に貢献してきたが、必ずしも民間技術に一致していない。米軍はヘビーユーザでもあるが、COTS の重要性を認識している。優れたコア技術は民間企業にあると認識している。

5. 総括：

(1) 例年に比べ、内容が充実していない感があった。この原因は、欧州では、公的市場（社会 ID）の開発が一段落したことと、金融問題などにより民間市場が立ち上がっていない、あるいは飽和している状況と考える。

(2) 社会的（ID 関係の実証プロジェクト、脆弱性プライバシーなどのプロジェクト）には日本よりはるかに進んでいるが、技術開発的には日本の企業の方が遥かに進んでいるという感想である。

(3) 欧州はアフリカ、中近東などかつての宗主国のポジションを利用し、これらの国への市場展開に重点を置いているようである。

(4) 上記を考えると、日本においては、社会的な大型プロジェクトが実施されていないこと、アジアへの市場展開が遅いことが、日本の産業界の問題と考える。

2.2　関連技術の最新動向調査

本節では、共通バイオメトリック認証基盤の開発および適用に関連する規格として、電子認証システム関連の規格について調査を行う。具体的には米国の電子認証システムのための本人認証に関するガイドラインであるOMB M-04-04およびNIST SP 800-63について調査することにより、両文書で示される電子認証システムにおける生体認証技術の考え方を整理する。OMB M-04-04およびNIST SP 800-63は、日本の電子政府システムに対するセキュリティ確保策として認証方式の導入を検討する際の活用基準を提供することを目的とした「オンライン手続きにおけるリスク評価および電子署名・認証ガイドライン」（URL：http://www.kantei.go.jp/jp/singi/it2/guide/）にて参照されており、国内の電子認証システムにおける本人認証の指針に影響を与えている文書である。このことから、本事業における生体認証技術の位置づけを検討するのに適した文書であると判断した。

次に本事業における生体認証技術の適用方法について検討する。共通バイオメトリック認証基盤で用いるOpenIDなどのアイデンティティ管理システムは電子認証システムの一種である。本システムに生体認証を組み込みにあたり、電子認証システムにおける本人認証として生体認証技術を用いる場合の位置づけを考慮して、適用方針を定めることとする。

2.2.1　関連標準に関する調査結果

本節では、関連する標準として米国で作成されたOMB M-04-04とNIST SP 800-63の2つの文書について調査した結果を示す。

(1) OMB M-04-04

本文書は米国連邦政府機関向けの電子認証にかかわるガイダンスであり、OMB（Office of Management and Budget：大統領府行政管理予算局）が2003年12月に発行したものである。本文書では、運用する電子認証システムについて、政府機関がリスクアセスメントを使用して適切な保証レベルを決定し、その保証レベルを満足する本人認証技術を選択する手順を示している。図2.1に、本人認証技術を選択するための手順を示す。

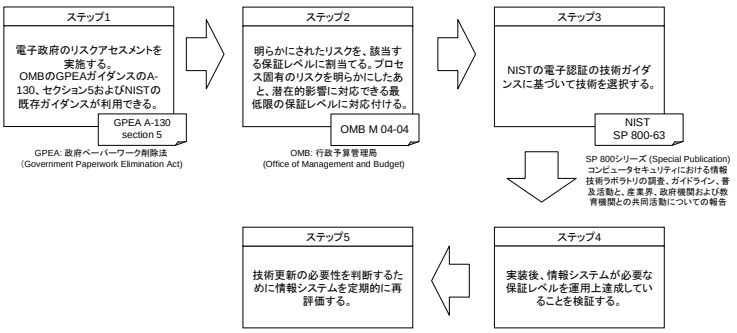


図2.1 OMB M-04-04における認証技術選択の手順

本図に示すとおり、OMB M-04-04では運用する電子認証システムの本人認証技術を5つのステップで実現する流れが示されている。ステップ1ではリスクアセスメントによって運用する電子認証システムのリスクを明確化する。ステップ2とステップ3は、本人認証技術の選択に関わる部分であり、ステップ2において電子認証システムのリスクと保証レベルの関係を確定したのち、ステップ3で該当する保証レベルを満足する本人認証技術を選択する。ステップ3の詳細は外部文書であるNIST SP800-63で示される（後述）。ステップ4では、実装した技術が保証レベルを満足しているかを検証し、ステップ5でこれを定期的な評価で維持する。

OMB M-04-04には、こうした流れに加えてステップ2における詳細手順が述べられている。表2.1から表2.3は本文書で述べられている保証レベル、潜在的な影響や害、影響度の定義を示したものである。なおここに掲載する表は、IPA（独立行政法人情報処理推進機構）の海外情報セキュリティ関連文書の翻訳・調査研究（NIST文書など）のOMB M-04-04のURLからダウンロードした文書から引用したものである。(1)

参照URL：http://www.ipa.go.jp/security/publications/nist/documents/OMBm04-04.pdf

表2.1 保証レベルの定義

保証レベル	内容
レベル1	主張された識別情報の有効性についてほぼ、あるいはまったく信頼性がない。
レベル2	主張された識別情報の有効性についてある程度の信頼性がある。
レベル3	主張された識別情報の有効性について高い信頼性がある。
レベル4	主張された識別情報の有効性についてきわめて高い信頼性がある。

表2.2 潜在的な影響や害の分類

No	分類
1	不便、苦痛もしくは地位または評判に対する打撃
2	財務上の損失または政府機関の賠償責任
3	政府機関の活動計画または公共の利益に対する害
4	機密情報の無許可の公開
5	身の安全
6	民事上または刑事上の法律違反

表2.3 影響度の定義

No	影響度
1	低位の影響
2	中位の影響
3	高位の影響

OMB M-04-04では、表2.2で示した潜在的な影響や害の分類ごとに、表2.3で示した3つの影響度それぞれについて、さらに詳細化した定義を行っている。その上で、電子認証システムの担当者が自分の担当するシステムについて、表2.4で示す影響プロファイルを参照して、最低限の保証レベルを決定する。

表2.4 保証レベルに対する影響プロファイル

No	認証エラーの潜在定期影響の分類	レベル1	レベル2	レベル3	レベル4
1	不便、苦痛もしくは地位または評判に対する打撃	低位	中位	中位	高位
2	財務上の損失または政府機関の賠償責任	低位	中位	中位	高位
3	政府機関の活動計画または公共の利益に対する害	該当なし	低位	中位	高位
4	機密情報の無許可の公開	該当なし	低位	中位	高位
5	身の安全	該当なし	該当なし	低位	中位 高位
6	民事上または刑事上の法律違反	該当なし	低位	中位	高位

本表における6つの分類それぞれに対して該当の有無を確認し、ひとつでも該当すればそれが最低限の保証レベルとなる。OMB M-04-04ではこのような手順で、運用する電子認証システムの保証レベルが決定される。

(2) NIST SP 800-63

① 概要

本文書は米国のNIST（国立標準技術研究所：National Institute of Standards and Technology）が2006年1月に発行した電子認証に関するガイドラインである。本文書は、ネットワークを経由したユーザのリモート認証に関するガイドラインとして、身元識別情報に関して4つの保証レベルに対応付けた技術的要求事項を記述している。この4つの保証レベルとは前述のOMB M-04-04で述べられている保証レベルに対応している。すなわち、OMB M-04-04で運用する電子認証システムの保証レベルを設定したあと、SP 800-63によってその電子認証システムの保証レベルを満足する本人認証に関わる技術を選択することができる。

SP 800-63の記載例として、認証時に必要となる技術をまとめたものを表2.5から表2.9に示す。なおここに掲載する表や文章は、前述のOMB M-04-04と同様、IPA（独立行政法人情報処理推進機構）の海外情報セキュリティ関連文書の翻訳・調査研究（NIST文書など）のSP 800-63のURLからダウンロードした文書から引用したものである。(1)

注）(1) 参照URL：http://www.ipa.go.jp/security/publications/nist/documents/SP800-63-J.pdf

表2.5 各保証レベルで使用することができるトークンの種類

No	項目	レベル1	レベル2	レベル3	レベル4
1	ハード暗号トークン	✓	✓	✓	✓
2	ワンタイムパスワードトークン	✓	✓	✓	
3	ソフト暗号トークン	✓	✓	✓	
4	パスワードおよび暗証番号	✓	✓		

表2.6 各保証レベルで保護の対象となる攻撃

No	項目	レベル1	レベル2	レベル3	レベル4
1	オンライン推測	✓	✓	✓	✓
2	再現	✓	✓	✓	✓
3	盗聴		✓	✓	✓
4	検証者なりすまし			✓	✓
5	中間者			✓	✓
6	セッションハイジャック				✓

表2.7 オンラインパスワード推測に対する最小限の耐性

No	項目	レベル1	レベル2
1	標的を定めた攻撃：ユーザ名以外に「事前に」何も知らない攻撃者が、パスワードの有効期限にわたって、選択したユーザのパスワードを推測する最大の確率	2^{10}分の1 （1/1024）	2^{14}分の1 （1/16384）
2	標的を定めない攻撃：最小エントロピー	-	10ビット

表2.8 認証プロトコルの種類

No	項目	レベル1	レベル2	レベル3	レベル4
1	プライベート鍵 PoP (1)	✓	✓	✓	✓
2	対称鍵 PoP (1)	✓	✓	✓	✓
3	トンネルされたパスワードまたはゼロ知識パスワード	✓	✓		
4	Challenge - response パスワード	✓			

注）(1) PoP: Proof of Possessionの略。

表2.9 そのほかの必要なプロパティ

No	項目	レベル1	レベル2	レベル3	レベル4
1	検証者またはCSPによって第三者に開示されない共有秘密鍵情報		✓	✓	✓
2	複数要素の認証			✓	✓
3	認証される機密データ転送				✓

このようにSP 800-63では電子認証システムの技術として、トークン・保護の対象となる攻撃・オンラインパスワード推測への耐性・認証プロトコル・その他の5つに分けて、OMB M-04-04で定めた保証レベルを満足する技術を選択するようになっている。

② 生体認証に関わる記述部分

SP 800-63には生体認証についての言及が複数個所存在する。SP 800-63における生体認証技術の電子認証システムにおける位置づけを明らかにするため、生体認証に関する主な言及箇所を以下に抜粋する。

・「概要」

本指針では、秘密情報に基づいたリモート認証を行うために従来から広く実装されている手段のみを対象とする。認証対象となる個人はこれらの手段を講じて、自分がなんらかの秘密情報を知っていることまたは所持していることを証明する。NISTでは、ほかのリモート認証手段（生体認証を使用するものや、個人的ではあるが真の意味で秘密ではない個人情報の詳細な知識を使用するものなど）についても調査し、それらのリモート認証手段の使用に関する追加の指針を作成することも検討している。

・「3. はじめに」

生体認証による方法は、建物に立ち入る際など、本人が物理的に認証が行われる場所にいる場合にその個人を認証する方法として広く使用されている。生体認証情報は、本文書で説明している従来型のリモート認証プロトコルにおける使用に適した秘密情報ではない。ローカル認証では、認証要求者が観察され、検証者によって管理されている取り込み装置を認証要求者が使用するため、生体認証情報の秘密は維持される必要がない。本文書では、従来型の認証トークンの「ロックの解除」と登録の否認防止に生体認証情報を使用することについて明示する。

NISTでは知識ベースの認証と生体認証の両方について引き続き調査を行っており、ネットワーク経由での個人のリモート認証にそれらの認証方式を使用することに関して追加の指針を発行する可能性がある。

・「3.2 トークン」

たとえば、暗号鍵を保持するハードウェアデバイスを考える。この場合、パスワードによって鍵を活性化することが考えられる。または、ハードウェアデバイスに生体情報取り込み装置が組み込まれていて、生体認証情報を使用して鍵を活性化することも考えられる。このようなデバイスは実質的に2つの要素による認証を提供するものとみなされるが、検証者と認証要求者間での認証プロトコルでは鍵の所在が証明されるだけである。（中略）生体認証情報はユニークで個人的な属性であり、個人の識別に使用することができる。これには、顔写真、指紋、DNA、虹彩や網膜のスキャン、声紋など多数ある。本文書では、生体認証情報をトークンとして直接使用することはない。

③ SP 800-63における生体認証技術の位置づけ

電子認証システムにおける生体認証技術のセキュリティにおける考え方の整理を行った結果として、図2.2にSP 800-63における生体認証技術の位置づけを示す。本図に示すとおり、SP 800-63では生体認証技術は単独で身分を証明する技術として用いられておらず、他の本人認証技術と組み合わせることで保証レベルを引き上げる方法として用いられている。

具体的には、ハードウェアトークンは単独では保証レベルが2だが、生体認証と組み合わせることで4に引き上げることができる。同様に、ソフトウェアトークンおよびワンタイムパスワードは保証レベルを2から3に引き上げることができるが、生体認証単体として電子認証システムに用いることはSP 800-63では想定されていない。

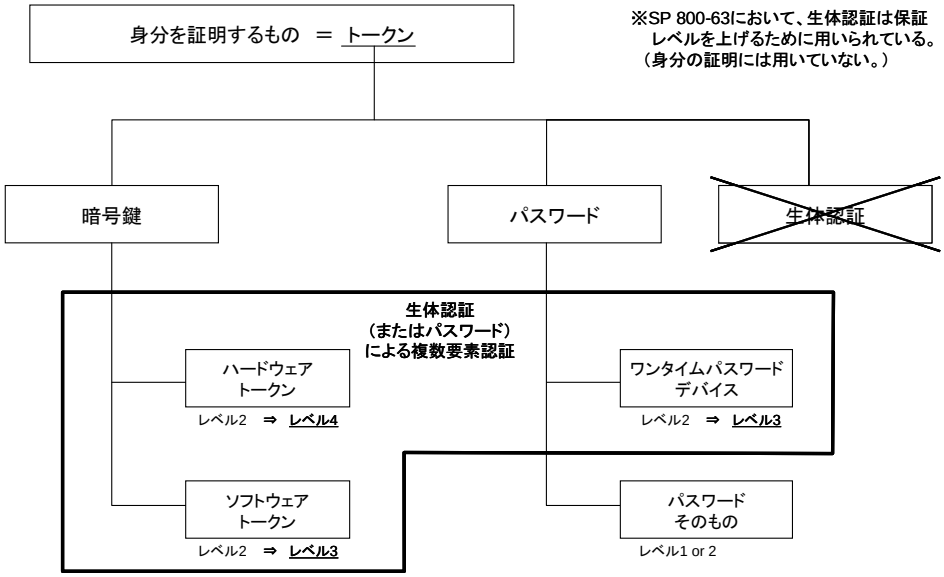


図2.2 SP 600-83における生体認証技術の位置づけ

2.2.2 生体認証技術の適用方法

本節では、電子認証システム等のセキュリティの考え方に対応するための要件の研究として、生体認証技術を本事業において適用するための方法について検討した結果を示す。

(1) 保証レベルの考慮

前節で示したとおり、OMB M-04-04やSP 800-63において電子認証システムにおける生体認証技術は単体では用いられず、他の本人認証技術と組み合わせて保証レベルを引き上げるために用いられることが想定されている。

本事業においてアイデンティティ管理システムとして取り上げたOpenIDは、GoogleやYahooに代表されるグローバルなウェブサイトを含め多くのWebサイトで採用されているが、主要なOPにおいて保証レベルが低い条件下で使われることが多い。このため、保証レベルを引き上げることを可能とする生体認証との組み合わせが必ずしも適しているとは言えない。(1)

したがって、運用するOpenIDが想定する保証レベルと生体認証が提供する保証レベルの間で不一致が起きないよう、本事業で開発研究を行う共通本人認証基盤の適用分野の選択には何らかの考慮が必要である。

注）(1) OpenIDの拡張仕様であるPAPEには、NIST SP 800-63などの保証レベルを含める機能が盛り込まれている。

(2) 適用アプリケーションの検討

保証レベルと生体認証の位置づけを考慮した結果、本事業における適用アプリケーションの候補として、震災時のアイデンティティ管理を取り上げることとする。2011年3月11日に発生した東日本大震災では、免許証や健康保険証、銀行のキャッシュカードなど所持するタイプのIDを市民が紛失することにより、行政や民間によるサービス提供の際に本来されるべき本人確認ができなくなる事例が多数発生した。この事態を受けて、行政や民間では所持するIDを使った身分証明ができなくても、特例的に自己申告でサービスを提供する措置がとられた。このような環境下において、電子認証システムにおけるより安全で安心な本人認証手段として生体認証の適応が考えられる。

震災時における利用環境では、今まで述べてきたOMB M-04-04やSP 800-63で示される保証レベルの考えにおいて、単独で使用可能な本人認証手段として扱われている従来からの本人認証方式が必ずしも適用できない。ハードウェアトークンのような所持するタイプの本人認証手段は、避難所において紛失したり、またセキュリティが高いといえない状況下において盗難にあったりする危険性から逃れることができない。パスワードのような記憶するタイプの本人認証手段の場合、セキュリティを考慮するとある程度長くて複雑な文字列にせざるを得ない。利用者が高齢者や子供だった場合、覚えることが困難である。ソフトウェアトークンはコンピュータ内にハードウェアトークンのアルゴリズムを実装したものだが、これを守るためにパスワードなど別の本人認証手段が必要となる。以上から、ハードウェアトークン・ソフトウェアトークン・パスワードのいずれも、震災時の電子認証システムにおける本人認証としての適用には、通常の運用にはない困難さが存在する。

これに対して生体認証は、所持物のような紛失の心配がなく盗難の恐れもない。また、パスワードのように新しく記憶する必要もないため、震災時においても広範囲の市民に対して適用が可能である。さらに生体認証は簡便さと高セキュリティという2つの特徴が両立した本人認証手段であり、震災時などの深刻な状況において被災者に対して確実な本人認証を行い、必要不可欠なサービスを効率的かつ迅速に提供するために重要な役割を果たすことができると考えられる。

図2.3に、震災時における適用例として、OpenIDと生体認証を組み合わせたシステム構成を示す。本図では左上に仮市役所が設置され、ここにOPやBP（BioIDM Providerの略で、IdMシステムにおいて生体認証を行うためのサービスプロバイダである。）などといったプロバイダが配置される。また、被災者へのサービス利用状況を蓄積するためのRPも設置される。

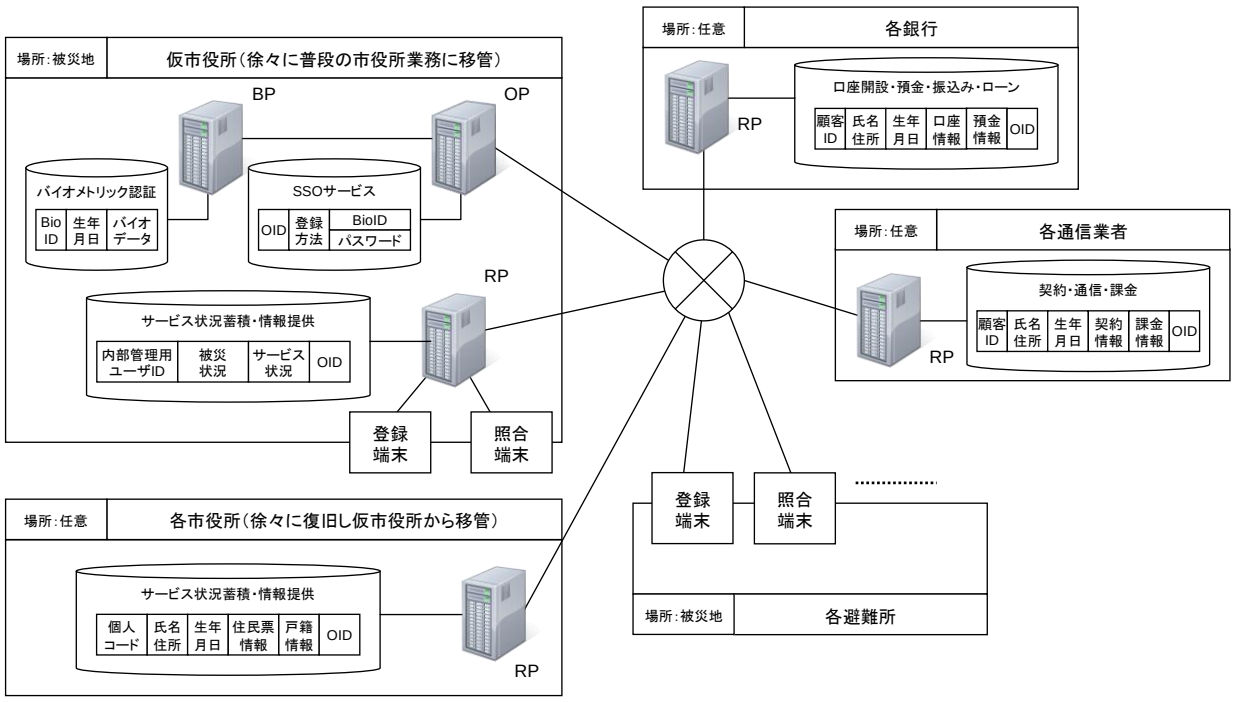


図2.3 震災時のOpenIDと生体認証を組み合わせた適用案

この例ではサービス提供者として銀行や通信業者が挙げられている。これらのサービス提供側では顧客管理において仮市役所で行う本人認証サービスとリンクするためのIDを顧客ごとに保持し、それぞれがRPの一つとして機能する。被災者は、避難所などにおいて生体情報の登録とともに個人属性情報を登録する。この際、氏名や住所、生年月日、電話番号など必要に応じた本人確認を行った後に生体情報を登録する。これらの情報のうち、生体情報と生年月日の情報がBP内のデータベースにID情報（ここではBioIDと呼ぶ）と共に格納される。あわせて、OPに被災者のOpenIDとBioIDが紐付けられて管理される。認証時には、各RPにて被災者の生年月日情報と生体情報の組み合わせを入力することで、OPおよびBPにて本人認証が行われ認証に成功するとRPによるサービスが提供される。

こういった被災者向けの民間サービスを市民が受ける際に、OpenIDによるシングルサインオンなどのアイデンティティ管理機能を用いて仮市役所のRP側でもサービスを提供する。被災者が銀行や通信業者のRPでサービスを受けた後で、仮市役所のRPでもサービスを提供するには、仮市役所側のRPでもログオンが必要になるが、これはOpenIDのシングルサインオンの機能によりOPに自動ログオンすることで、被災者を煩わせることなく複数のRP間を跨いだサービス提供が可能となる。仮市役所のRPでは、被災者の安否確認とあわせて民間のRPで受けたサービスの利用状況の把握が可能となる。仮市役所のデータベースに被災者ごとの状況把握のための情報を蓄積することにより、仮市役所のRPから被災者に対して被災者個人の状況にあわせたきめ細やかな情報やサービスの提供が可能になる。仮市役所の業務は、本来の市役所が復旧するとその業務を本来の市役所に移管する。

2.3　共通バイオメトリック認証基盤の仕様検討

本節では、共通バイオメトリック認証基盤として平成24年度に開発を行った共通本人認証基盤（本節以降これをBioIDMシステムと称する）に関する仕様検討結果について説明する。

本事業においてBioIDMシステムはIdMのプロトコルとしてSAMLに比べて実装が軽いといわれているOpenIDを開発容易性が高いと解釈し、採用することとした。OpenIDのバージョンには1.0, 1.1, 2.0やOpenID Connectなどが存在するが、本事業における開発時にOSSとして入手が容易なバージョンとしてOpenID 2.0を採用することとする。従って、本書におけるシステム内の各コンポーネントの機能やインタフェースを説明する際に使われる用語は原則的にOpenID 2.0で定義されているものを用いることとする。OpenIDの詳細についてはOpenID Foundationなどにより公開されているインターネット上の情報を参照されたい。

（参考URL例：http://openid-foundation-japan.github.com/openid-authentication.html）

2.3.1　システム構成

BioIDMシステムのシステム構成として、運用上標準的に用いられることを想定した標準構成と、構造がより単純な簡易構成の2種類を検討した。それぞれを図2.4および図2.5に示す。

図2.4の標準構成は、Relying Party（以下RPと略す）・OpenID Provider（以下OPと略す）・User Agent（以下UAと略す）に加えてBioIDM Provider（以下BPと略す）の4つのコンポーネントにより構成される。BPは、OpenID仕様には存在しない構成要素であり、バイオメトリック認証専用のサービスを提供することを想定したものである。これに対して図2.5の簡易構成は、RP・BP・UAの3つの要素により構成される。本構成においてBPは、バイオメトリック認証の機能を提供するとともにOpenID仕様におけるOPと同等の役割を果たす。

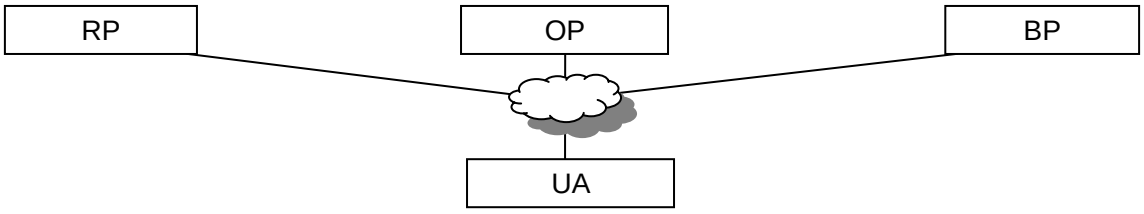


図2.4　標準構成

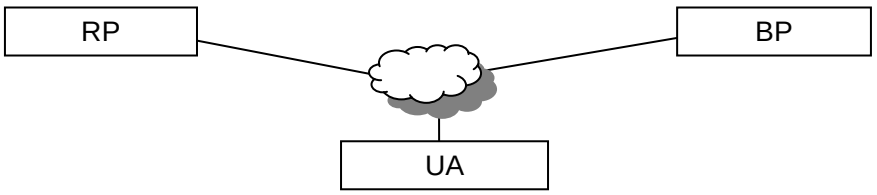


図 2.5　簡易構成

標準構成および簡易構成の各構成要素について、それぞれ表2.10および表2.11を用いて説明する。

表2.10 標準構成における構成要素

No	構成要素	説明
1	RP （Relying Party）	OPによる認証成功後、エンドユーザが求めるサービスを提供する。
2	OP （OpenID Provider）	エンドユーザがパスワード認証を要求した場合、OP内部でパスワード認証方式による本人認証機能を提供する。 エンドユーザがバイオメトリック認証を要求した場合、OpenID仕様における本人認証処理部分がBPに対するRPとして機能し、BPに対して認証要求を発行する。
3	BP （BioIDM Provder）	本人認証処理部としてバイオメトリック認証による本人認証機能を提供する。サーバのWebコンテンツとしてBioIDM Connectionを保持し、バイオメトリック認証の際にはこのコンテンツがUA上で動作する。 標準構成においてBPはOPに対するOpenID Providerとして機能する。
4	UA （User Agent）	エンドユーザが選択した本人認証方法に従って、RP、OPおよびBPとの間でOpenIDプロトコルを実行するブラウザである。

表2.11　簡易構成における構成要素

No	構成要素	説明
1	RP （Relying Party）	BPによる認証成功後、エンドユーザが求めるサービスを提供する。
2	BP （BioIDM Provider）	標準構成におけるOPとBPの役割を兼ねたプロバイダであり、エンドユーザの要求に応じて、バイオメトリック認証あるいはパスワード認証による本人認証機能を提供する。
3	UA （User Agent）	エンドユーザが選択した本人認証方法に従って、RPおよびBPとの間でOpenIDプロトコルを実行するWebブラウザである。

標準構成と簡易構成にはそれぞれ表2.12に示す長所と短所が存在する。これらの長所短所のうち、性能面の特徴については開発を実施した後に行う検証実験によりその内容を検証することとする。

表2.12　基本構成と拡張構成の特徴

No	項目	長所	短所
1	標準構成	OPとBPとに役割を明確に分けることにより、OPがバイオメトリック認証サービスを提供するためにOpenIDプロトコルに従ってBPを呼び出すだけで済む。バイオメトリクスの専門性を有する組織がBPを立ち上げれば、OPとしてバイオメトリクスに関する特別な知識修得や開発を必要としないため、容易にバイオメトリック認証サービスを提供できる。加えて、バイオメトリック認証方式として新しいモダリティ（指紋、虹彩、静脈など）を追加する場合も、OP側に直接的な影響がない。	一度の認証にOPとBP間の通信が発生するため、処理時間が長くなることが予想される。 認証時間の長さがエンドユーザや運用者にとって負担になる場合、本方式の適用は困難になる。(1)
2	簡易構成	システム構成が単純であり、プロトコルの通信回数がOpenIDの標準的通信回数どおりとなる。認証時間が標準構成に比べて短くなることが予想される。(1)	バイオメトリック認証を実現するための機能をOP内に組み込まなければならない。組み込みのために開発者側がバイオメトリック認証技術を習得する必要がある。

注）(1) 検証実験における性能測定で検証した（後述参照）。

本報告書作成時点ですでに数多くのOpenIDプロバイダが存在しており、ほとんどが認証方式としてパスワード認証を採用している。例えばGoogleやYahoo、ミクシィなどの既存のOpenIDプロバイダに、技術的な専門性の高いバイオメトリック認証機能を組み込む努力を求める方法は普及という観点で望ましくないと考えた。このことから本書では、既存のOpenIDプロバイダがバイオメトリック認証を行う際にバイオメトリック認証の高度な専門的知識を要求しない標準構成を前提として研究を進めることとする。

2.3.2　処理の流れ

本節ではBioIDMシステムの標準構成における処理の流れについて説明する。図2.6は、認証時の基本的な処理の流れを示したものである。今年度の開発においては、年度内におけるプロトタイプの確実な実装完了を目標とし、OP・BP・UA間のプロトコルとしてOpenIDプロトコルを用いることとする。これは、OPがRPに対してOpenIDプロバイダの役割を果たすと共にBPに対してRelying Partyの役割を果たし、BPはOPに対してOpenIDプロバイダの役割を果たすことを意味する。この結果、エンドユーザがRPに対して認証依頼を行うと、1回の認証の度に2回のOpenIDプロトコルが実行されることになる。

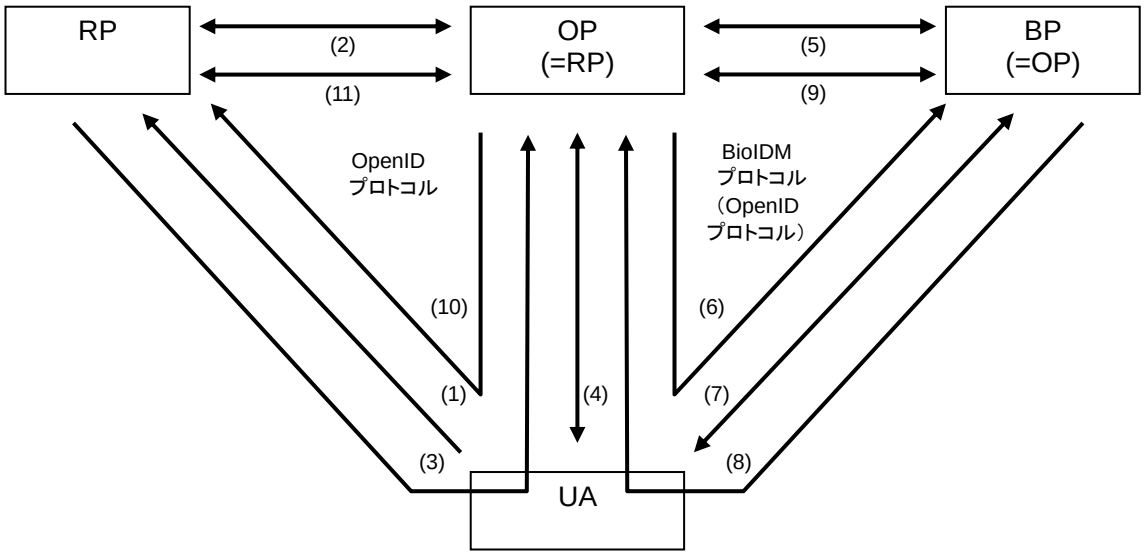


図2.6 BioIDMシステム標準構成における認証処理の流れ

以下に本図における処理の流れを、図中の番号に沿って説明する。

(1) UAがRPに対してサービスを提供するためのアクセスを行う。（RPのウェブサイトを訪問する。）この際、OpenIDによる認証をエンドユーザが希望すると、エンドユーザはOP識別子(OP Identifier) を入力するか、ユーザ入力識別子（User-Supplied Identifier）を入力する。

(2) RPはOPとの間でアソシエーション確立と呼ばれるハンドシェイクを行う。

(3) RPからUA、UAからOPへとリダイレクトが行われ、OP側に制御が移る。

(4) OPはUAとの間で必要に応じてやり取りを行う。OPのコンテンツにより、エンドユーザに認証方式（バイオメトリック認証またはパスワード認証など）を選択させる。OpenID仕様では、ここでエンドユーザがユーザ入力識別子を入力する場合がある。

(5) OPはあらかじめ認識していたBPとの間でアソシエーション確立と呼ばれるハンドシェイクを行う。

(6) エンドユーザがバイオメトリック認証を指定した場合、OPからUA、UAからBPへとリダ

イレクトが行われBPに制御が移る。

(7) BPとUAの間でバイオメトリック認証による本人認証処理が実行される。

(8) バイオメトリック認証結果を受けて、BPからUA、UAからOPへとリダイレクトが行われOPに制御が移る。

(9) OPはBPに対して認証結果の検証（Assertion Verification）を行う。

(10) 認証結果の検証を受けて、OPからUA、UAからRPへとリダイレクトが行われRPに制御が移る。

(11) RPはOPに対して認証結果の検証（Assertion Verification）を行う。

(12) 認証結果の検証を受けて、RPはエンドユーザにサービスを提供する。

以上示したとおり、今回の開発において、標準構成ではRP － OP － UAの間でOpenIDプロトコルが用いられるとともに、OP － BP － UAの間でもOpenIDプロトコルが用いられる。

以降に、登録機能および照合機能それぞれにおける処理の流れの詳細を示す。

2.3.3 登録機能

本節ではBioIDMシステムにおけるエンドユーザの登録機能について説明する。

(1) 概要

本システムにおけるエンドユーザの登録機能の概要ついて説明する。図2.7は、RP・OP・BPにおいてエンドユーザを登録する際に扱われるそれぞれのデータの関係を示したものである。本図において、BPIDはBPがOpenIDプロバイダとして管理するエンドユーザのIDを表し、BPIDはOPがOpenIDプロバイダとして管理するエンドユーザのIDを表す。これに対して、RPIDはRPがエンドユーザを管理するためのIDを表す。

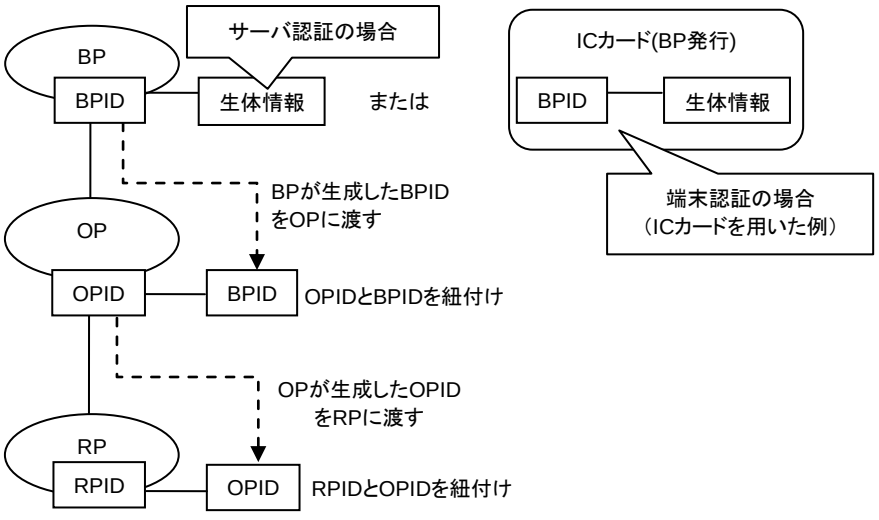


図 2.7 登録データの関係

本図では最上位にあるBPに、BPIDとバイオメトリック情報が存在する。BPはエンドユーザに対して登録時に一意のBPIDを割当てるとともに、そのIDに対応したバイオメトリック情報を生成し、BPIDとバイオメトリック情報の組をBP内に保持する。保持する場所は、BPが認証方式としてサーバ認証をサポートする場合はBP内のデータベースとなり、端末認証をサポートする場合はICカードなどの媒体内に格納するのが一般的である。本事業で採用した認証方式については、後述の2.4節（プロトタイプシステムの開発）で説明する。

OP内ではOPIDとBPIDを紐付けて管理する。OPはエンドユーザに対して登録時にOPIDを割当てるとともに、そのIDに対応したBPIDの組をOP内に保持する。こうすることで、OP内のOPIDとBP内のバイオメトリック情報がBPIDによって関連付けられる。

RP内ではRPIDとOPIDを紐付けて管理する。RPはエンドユーザに対して登録時にRPIDを割当てるとともに、そのIDに対応したOPIDの組をRP内に保持する。こうすることで、RP内のRPIDとBP内のバイオメトリック情報が、RPIDとOPIDの紐付けとOPIDとBPIDの紐付けを用いて関連付けられる。

このようなデータの関係を構築することにより、RP上でエンドユーザがRPIDを指定して認証を依頼すると、以後OpenIDのプロトコルに従うことでBP上でのバイオメトリック認証を行われ、結果的にRPに認証結果を伝えユーザへのサービス提供可否を判断することができるようになる。登録処理の流れの詳細については後述を参照されたい。また、認証処理の詳細については次節を参照されたい。

⑵ 詳細

登録処理の流れをまとめたものを図2.8に示す。

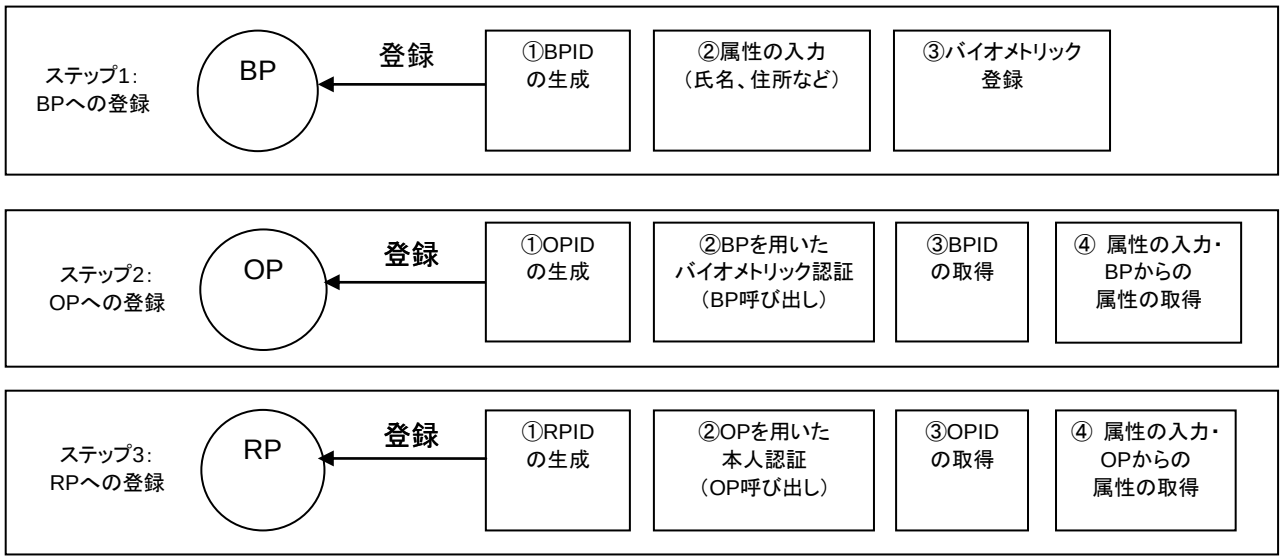


図 2.8 登録処理の流れ

①ステップ1：BPでのエンドユーザ登録

BPでエンドユーザの登録を行う。この処理にはエンドユーザに対してBPIDを生成するとともに、BPとして必要となる属性情報を入力し、あわせてバイオメトリック情報を登録する機能が含まれる。登録データの格納場所は、実装時の認証方式がサーバ認証方式かローカル認証方式かで異なる。

②ステップ2：OPでのエンドユーザ登録

OPでエンドユーザの登録を行う。これには、エンドユーザに対してOPIDを生成する処理とあわせて、BPIDを指定してBPに対する本人認証依頼を行う処理が必要となる（OPは、それ自身がBPに対するRPとして動作する）。この結果BPでバイオメトリック認証が実行される。本人認証結果がOPに届くとともに、OPはBPIDやBP登録時に入力した属性情報をBPから取得することができる。OPはBPから受け取った情報をOPにおけるそのエンドユーザのための登録情報の一部として用いることができる。あわせて、OPとして独自の属性情報を登録する。

③ステップ3：RPでのエンドユーザ登録

RPでエンドユーザ登録を行う。これには、エンドユーザに対してRPIDを生成する処理とあわせて、OPIDを指定してOPに対する本人認証依頼を行う処理が必要となる。認証依頼を受けたOPは、与えられたOPIDから、OP内に格納されているBPIDを参照する。次にOPはBPに対するRPとして動作し、BPIDを指定してBPに対して本人認証依頼を行う。この結果、BPは指定されたBPIDを用いてバイオメトリック認証を実行する。認証に成功した場合、BPは認証成功をOPに通知する。OPはこの結果を受けて、OPIDや属性情報を取得し、RPに提供することができる。RPはOPから受け取った情報をRPにおけるその利用者のための登録情報の一部として用いることができる。あわせて、RPとして独自の属性情報を登録する。

2.3.4 認証機能

本節ではBioIDMシステムにおいて開発したエンドユーザを本人として認証する機能について説明する。本人認証処理は、図2.9に示すとおりの流れで実行される。

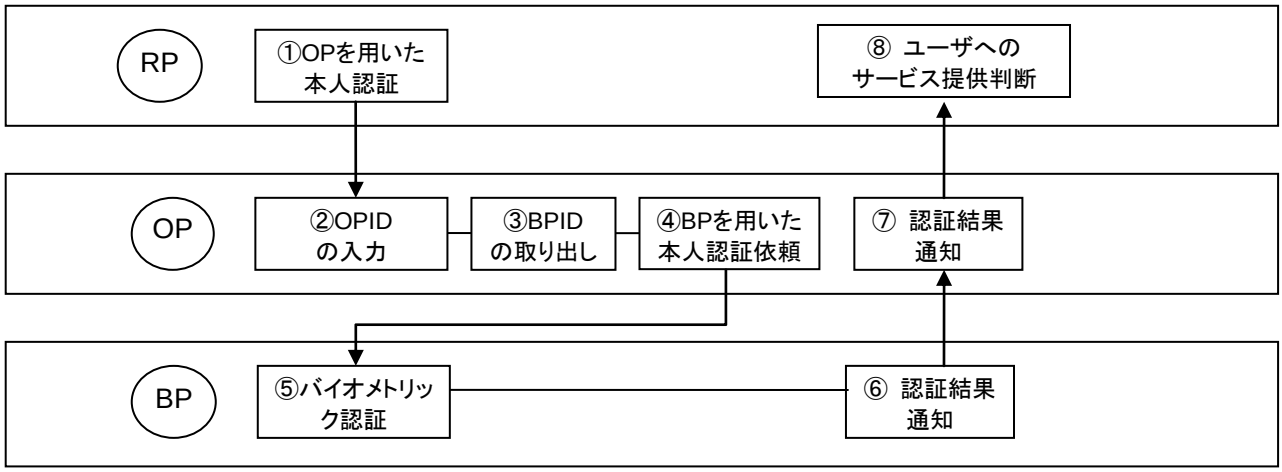


図 2.9 本人認証処理の流れ

本人認証処理は登録処理におけるRPへの登録処理と類似の処理となる。以下に各ステップの処理内容について説明する。

①OPを用いた本人認証（RP内処理）

エンドユーザがRPで本人認証を依頼する際に、OpenIDにおける認証を実行するためにOP識別子(OP Identifier)としてOPのURLを指定する。認証依頼を受けて、OpenIDプロトコルに従いOPに制御が移行する。

② OPIDの入力（OP内処理）

OPで認証するユーザを指定するためにエンドユーザはOPIDを入力する。

③ BPIDの取り出し（OP内処理）

OPはOP内に格納されているOPIDに対応したBPIDを取り出す。

④ BPを用いた本人認証依頼（OP内処理）

このBPIDを指定して、OPはBPに対して本人認証依頼を行う。OpenIDプロトコルにより、BPIDがBPに通知される。

⑤ バイオメトリック認証（BP内処理）

BPは、指定されたBPIDを用いてバイオメトリック認証を実行する。具体的には、指定されたBPIDを用いてBioIDM Connectionを呼出し、エンドユーザが操作する端末上でバイオメトリック認証のためのバイオメトリック情報の取得が行われる。認証方式にはサーバ認証方式とローカル認証方式の2種類が存在するが、いずれの方式においてもBioIDM ConnectionとBioIDM Transactionが動作することでバイオメトリック情報の取得およびバイオメトリック認証が行われる。

⑥ 認証結果通知（BP内処理）

BPはBioIDM Connectionから認証結果を受け取ると、OpenIDプロトコルに従ってOPに認証結果を通知する。

⑦ 認証結果通知（OP内処理）

OPはBPから認証結果を受け取ると、OpenIDプロトコルに従ってRPに認証結果を通知する。

⑧ ユーザへのサービス提供（RP内処理）

RPはOPから認証結果を受け取ると、その結果に応じてRPのサービスを利用者に提供するかどうかを決定する。

2.4　プロトタイプシステムの開発

本節では、前節で説明した共通バイオメトリック認証基盤の検討結果を受けて、実際のOpenIDプロバイダを用いたプロトタイプシステムの開発作業内容を示す。

2.4.1　OpenID プロバイダ

作業の効率を考慮し、本事業で使用するOpenIDプロバイダは新規開発せずに既存のオープンソースを活用することとした。OpenIDプロバイダのオープンソースはインターネットで複数の候補を見つけることができるが、本事業ではWSO2社のIdentity Serverを用いることとした。

WSO2社は米国、英国、スリランカに拠点を持つミドルウェアのオープンソースを開発・提供するソフトウェア会社であり、Identity ServerはOpenIDプロバイダを含んだオープンソースソフトウェアである。本ソフトウェアは過去10回を超える改版が続けられており、本プロジェクト推進中にもアップデートが行われた。継続的な更新が行われていることから、オープンソースとしての安定性が期待できると考えられたため本ソフトウェアを選択することとした。

本プロジェクトで使用するWSO2 Identity Serverのバージョンは事業推進時点における最新版のバージョン4.0であり、OpenIDプロトコルは2.0に対応している。OpenID以外にもアイデンティティ管理に関係するプロトコルとしてXACML 3.0やOAuth 2.0、SAML 2.0など様々なインタフェースに対応している。Identity Serverの詳細については、WSO2社のホームページを参照されたい(1)。

システム構成における標準構成では、RP・OP・BPの3つのWebサーバが存在する。このうちOPとBPにIdentity Serverを採用することとする。Identity Serverがソース公開されていることから、OP、BPともに本プロジェクト用の修正が可能である（修正内容の詳細については後述する）。なお、BioIDM ConnectionおよびBioIDM Transactionは特定のOpenIDプロバイダに依存しないため、Identity Server以外のOpenIDプロバイダにも原理的に組み込むことが可能である。

注）(1) WSO2社 Identity Serverの参照URL：http://wso2.com/products/identity-server/

2.4.2　バイオメトリック認証装置

本事業ではバイオメトリック認証装置として株式会社日立製作所製の指静脈認証装置PC-KCA100を使用する。本装置は上部のフードにより外光の影響を低減するとともに、近赤外線を指の上から透過させ、下からカメラで読み取る方式を採用し、高い認証精度を実現した製品である。

同社から提供されるソフトウェア製品のひとつとしてBioAPI用ソフトウェア開発キットがある。この製品はBioAPI V2.0に準拠しており、BioAPI仕様におけるバイオメトリック装置を制御するソフトウェアコンポーネントであるBSP (Biometric Service Provider) を含んだものである。

本事業においては、日立製作所様のご協力により指静脈認証装置PC-KCA100およびソフトウェア開発キットが無償で貸与されたため、システムの開発および検証実験の実施が可能となった。受託者として日立製作所様のご好意に感謝の意を表したい。

図2.10は指静脈認証装置PC-KCA100をイメージ図である。

本製品の詳細については、日立製作所のホームページを参照されたい。（URL：http://www.hitachi.co.jp/products/it/veinid/index.html）

図 2.10 日立製作所　指静脈認証装置 PC-KCA100

2.4.3　認証方式

前述のとおり、ネットワーク上のシステムにおける本人認証としてバイオメトリック情報を用いる方式には、端末上でバイオメトリック認証処理（マッチング）を行うローカル認証と、サーバ上でバイオメトリック認証処理を行うサーバ認証の2種類の方式が存在する。インターネット環境におけるアイデンティティ管理システムであるOpenIDの運用環境を考慮した場合、IDプロバイダとエンドユーザ間で同一国内だけでなく国を跨いで運用されるケースもあると考えられる。

インターネット上でバイオメトリック情報を取り扱うことについてはプライバシーとの係わりが広く取り上げられており、情報漏えいやプライバシー侵害の懸念が存在する。特にサーバ認証方式の場合、インターネット上に配置されたサーバにバイオメトリック情報を格納することから、バイオメトリック情報が攻撃者からアクセスしやすい環境に置かれる。このため、より強固なセキュリティ上の対策が必要になる。あわせて、認証のたびに端末上で取得したバイオメトリック情報を認証サーバまでインターネットを経由して送信する必要があり、通信系路上のセキュリティについても十分な対策が必要となる。

サーバ認証方式ではこのようなプライバシーおよびセキュリティに関する特別な考慮が必要であり、プロトタイプ開発においても対策の要否に関する何らかの評価が必要と考えられる。これに対してローカル認証方式では、攻撃対象となりやすいWebサーバにバイオメトリック情報を格納する必要もなく、かつ、インターネット上にバイオメトリック情報が流れることもない。

以上より、今年度の本事業においてはバイオメトリック認証を組み込んだOpenID上のプロトタイプシステムにおけるバイオメトリック認証方式としてローカル認証を採用することとした。

2.4.4　実装内容詳細

本節では、OpenIDシステムへのバイオメトリック認証機能の組み込みに関する実装内容の詳細についてまとめる。

(1) 全体構成

図2.11に本システムの全体構成とともに平成24年度事業において開発対象とした部分を示す。本図で示されるBioIDM TransactionおよびBioIDM Connectionは平成23年度事業として開発したプログラムであり、BioIDM Transactionはエンドユーザが使用する端末にダウンロードするソフトウェアとして、またBioIDM Connectionはエンドユーザの端末上で動作するブラウザにHTTPプロトコルで転送されるWebコンテンツとして、それぞれBPサーバ上に配置することを想定している。

平成24年度事業として開発したプログラムは、OP内で動作するBPとの連携機能、BP内で動作するOPとの連携機能およびバイオメトリック登録・認証機能、端末内で動作するBioIDM TransactionとBioIDM Connectionにおいて登録・照合処理を行う部分である。それぞれのプログラムの機能詳細について後述する。

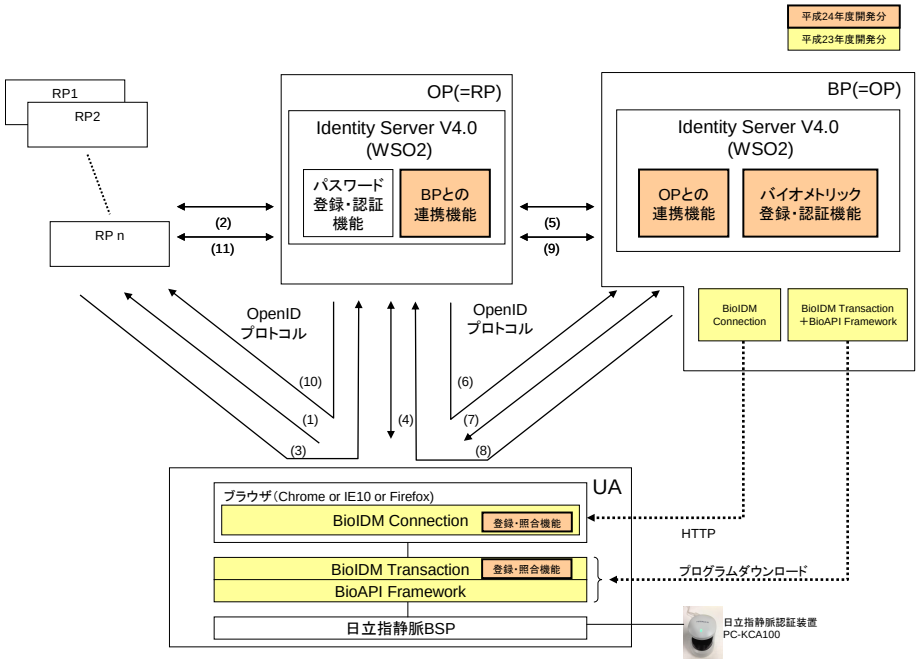


図 2.11 実装箇所の説明

(2) サーバ側動作プログラムの開発内容

以下に図2.11における平成24年度開発分の機能としてサーバ側で動作するプログラムの開発内容について示す。

① BPとの連携機能（OP内）

本開発部分は、OPにおいてエンドユーザが登録操作を行った場合、BPに対するRelying Partyとして機能し、BPに対してOpenID認証を呼び出す。BPから認証成功が返った場合BPから通知されるBPIDを受け取り、エンドユーザが設定したOPIDとともにデータベースに格納する。

あわせて、SRE（Simple Registration Extention）を用いてBPから属性情報を受け取る。RPにおいてエンドユーザがOPへの認証要求を行うと、与えられたOPIDからBPIDを取り出し、BPに対して認証要求を発行する。BPから認証結果を受け取ると、結果をRPに対して通知する。あわせてBPからの属性情報を、OP自身が管理する属性情報とあわせてRPに渡す。

② OPとの連携機能（BP内）

本開発部分は、OPにおいてエンドユーザが登録操作を行った場合、OPに対するOpenIDプロバイダとして機能し、OPからのOpenID認証要求を受け付ける。OPから与えられたBPIDを用いてBP内で認証を行い、認証結果をOPに通知する。あわせて、SREを用いて属性情報をOPに提供する。

OPにおいてエンドユーザが認証操作を行った場合も、OPに対するOpenIDプロバイダとして機能し、OPからのOpenID認証を受け付ける。基本的にBPの処理は前述の登録時のBPの処理と同一である。

③ バイオメトリック登録・認証機能（BP内）

本開発部分は、BPにおいてエンドユーザがバイオメトリック登録を行った場合、BioIDM Connectionを呼び出してバイオメトリック登録を開始する。BioIDM Connectionからの登録結果を受けて、登録処理が成功だった場合はエンドユーザに対して登録作業の完了を知らせる画面を表示するか、失敗だった場合はエンドユーザに再試行あるいは中止を選択させる画面を表示する。

エンドユーザがバイオメトリック認証を行った場合も同様にBioIDM Connectionを呼び出してバイオメトリック認証を開始する。認証結果を受けた動作も、バイオメトリック登録の場合と同様である。

(3) 端末側動作プログラムの開発内容

本開発部分は、BioIDM ConnectionおよびBioIDM Transactionにバイオメトリック登録および照合のための機能を追加したものである。具体的には、図2.12に示すとおりブラウザが動作する端末上でBioIDM TransactionとBioIDM Connectionが動作してバイオメトリック認証が行われるが、BioIDM Transactionがローカルコンピュータのハードディスク中にエンドユーザのBPIDおよびバイオメトリック情報の登録テンプレートおよびパスワードをエンドユーザ毎に管理する。認証の際にはBioIDM Connectionからの認証依頼とともにBPIDがBioIDM Transactionに通知される。これらの情報を受けてBioIDM TransactionはBPIDに対応するバイオメトリック情報テンプレートをハードディスクの所定の場所から取り出すとともに、一連のBioAPI関数を呼び出してバイオメトリック認証を行う。認証に成功するとBPIDに対応するパスワード情報をハードディスクの所定の場所から取り出し、認証結果とともにBioIDM Connectionに渡す。この結果BioIDM Connectionは、通常のパスワード認証と同じ方法でBPと認証処理を行う。この際にブラウザとBPの間でやり取りされるパスワードは、通常人間が扱うパスワードに対して桁数を20桁に増やすと共に乱数などを用いることで高いセキュリティを実現する。

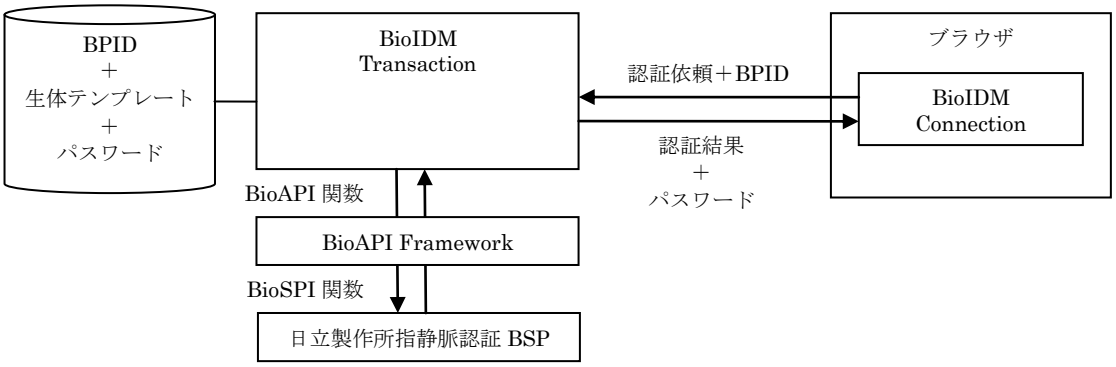


図 2.12 ローカル認証の詳細

以下にBioIDM ConnectionおよびBioIDM Transactionの処理内容詳細を示す。

① BioIDM Connection

・登録機能

今回対象とするバイオメトリック認証技術が指静脈であることから、登録用GUIとして両手の指を表示し、エンドユーザがどの指を登録対象とするか選択できるようにする。過半数のエンドユーザが右利きであることを想定し、右手が初めに選択されている状態とする。本GUIでは、指をマウスクリックによりひとつ選択したあと、登録用のキャプチャおよびテスト照合用のキャプチャと操作を進めることで、ひとつの指の登録が完了するように実装した。最大10指分の登録が可能である。キャプチャ画面においてエンドユーザのフィードバックの為にストリーミング画像と呼ばれるキャプチャ画像がBSPから提供する場合これを表示する機能を持つが、ストリーミング画像が提供されない場合は、BioIDM Connectionが内部で保有するGIFイメージとして点が回転するアニメーションを組み込んだ。

・認証機能

認証機能では操作のスピードを考慮し、指の選択機能を実装しなかった。認証操作においては、エンドユーザは即座に指静脈装置に指を置く動作を求められる。エンドユーザが複数の指を登録している場合、BioIDM Transactionと協調して登録されているすべての指静脈データと認証を行う。どれか1つの登録データとの間で認証に成功したらその時点で認証成功となる。複数の登録データのすべてで認証に失敗した場合、認証失敗として取り扱う。

② BioIDM Transaction

・登録機能

BioIDM Connectionから登録依頼が呼び出されると、登録依頼時に与えられたBPIDに基づきハードディスク上の所定の場所にBPID、バイオメトリックテンプレートおよびパスワードのセットを格納し、管理する。ここでバイオメトリックテンプレートは指静脈認証用BSPがサポートするBioAPIの登録関数からの戻り値に含まれるBIR（Biometric Informaction Record）と呼ばれるバイオメトリック情報を含んだデータブロックである。BioIDM Connectionの操作により複数の指を登録した場合、登録した指の数だけバイオメトリック情報が保存される。最大10指の情報を保存することができる。パスワードは乱数などを用いて生成した20桁の英数字や記号などからなる情報である。

・ 認証機能

BioIDM Connectionから認証依頼が呼び出されると、認証依頼に与えられたBPID情報に基づきハードディスク上の所定の場所に格納されたバイオメトリックテンプレートを取り出し、一連のBioAPI関数を呼び出してバイオメトリック認証を行う。認証に成功した場合、ハードディスク上の所定の場所に格納された対応するパスワードを取り出し、BioIDM Connectionに認証結果とともに返却する。登録時に複数の指を登録した場合は、各登録テンプレートに対して1対1照合が実行され、どれかひとつに対して認証が成功すれば成功と

して取り扱う。複数の登録テンプレートすべてで認証が失敗したときは認証失敗として取り扱う。

(4) データの取り扱い

図2.13は実装システムにおけるデータの取り扱いについて示したものである。以下、本図に示すデータ内容に沿って説明する。

① OP内のデータ

OPにおける登録時にOP用ユーザIDであるOPIDとBP用ユーザIDであるBPID、そしてユーザ属性情報をデータベース上に格納する。これら3つのデータはセットとしてエンドユーザ毎に存在する。

② BP内のデータ

BPにおける登録時にBP用ユーザIDであるBPIDとユーザ属性情報、そしてパスワード情報をデータベース上に格納する。これら3つのデータはセットとしてエンドユーザ毎に存在する。なお、パスワードは乱数で発生された文字列であり20桁固定である。（この桁数はIdentity Serverのパスワード上限である。）ユーザ属性にはそのユーザがバイオメトリック登録ユーザであることを示すフラグ情報が含まれる。

③ 端末内のデータ

エンドユーザが使用する端末では、BPへの登録時にBP用ユーザIDであるBPIDとバイオメトリックテンプレート、そしてパスワードをローカルなハードディスク上に格納する。

④ 属性情報（吹き出し部分）

OPとBP間の認証処理およびRPとOP間の認証処理において、OpenIDプロトコルの拡張仕様であるSREを用いて属性情報が受け渡される。本実装においては、OPとBP間でニックネーム・性別・生年月日が渡され、RPとOP間はOPとBP間の情報に加えて氏名・メールアドレス・郵便番号・国名が受け渡される。

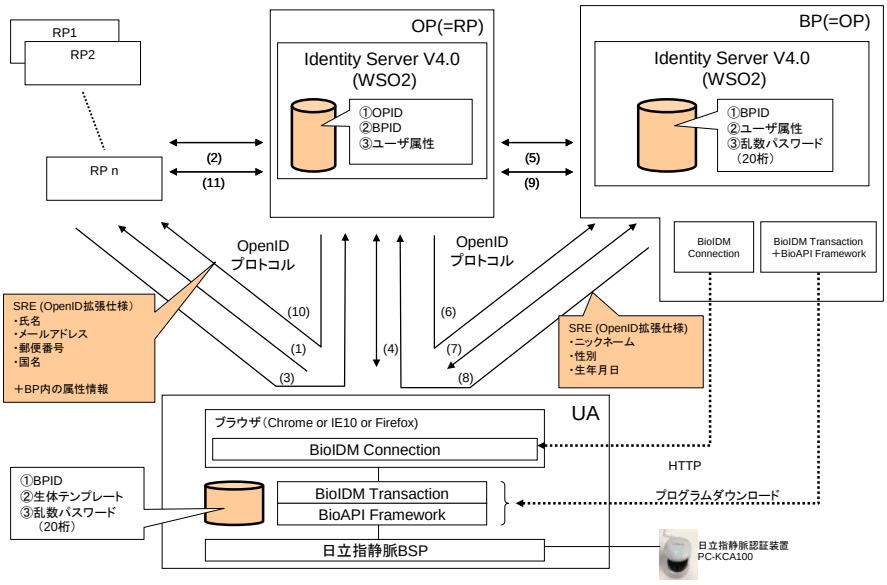


図 2.13 実装システムにおけるデータの扱い

(5) 処理の流れ詳細

標準構成における初回認証時の処理の流れは以下の通りである。

＜初回認証時＞　（処理の流れを図2.14に示す）

① エンドユーザがRPのログイン画面でOPIDを入力する。

② RPはOPIDを指定して、OPに認証要求を行う（OpenIDプロトコルの一部である）。

③ OPは、与えられたOPIDに紐づけられているBPIDをOP内のデータベースから取得する。

④ OPはBPIDを指定して、BPに認証要求を行う（OpenIDプロトコルの一部である）。

⑤ BPは与えられたBPIDからエンドユーザの認証条件がバイオメトリック登録ユーザであることを示すフラグ情報から確認する。BPはUAに対してバイオメトリック認証依頼を発行する。

⑥ エンドユーザは、UA上でバイオメトリック認証画面に応じて自身のバイオメトリック情報を取得し、認証を行う。BPはUAから認証結果を受け取る。

⑦ BPはBPIDを指定して認証結果をOPに提示する（OpenIDプロトコルの一部である）。

⑧ OPは、与えられたBPIDに紐づけられているOPIDを取得する。

⑨ OPはOPIDを指定して認証結果をRPに通知する（OpenIDプロトコルの一部である）。

⑩ RPは認証結果に応じてエンドユーザにサービスを提供する。

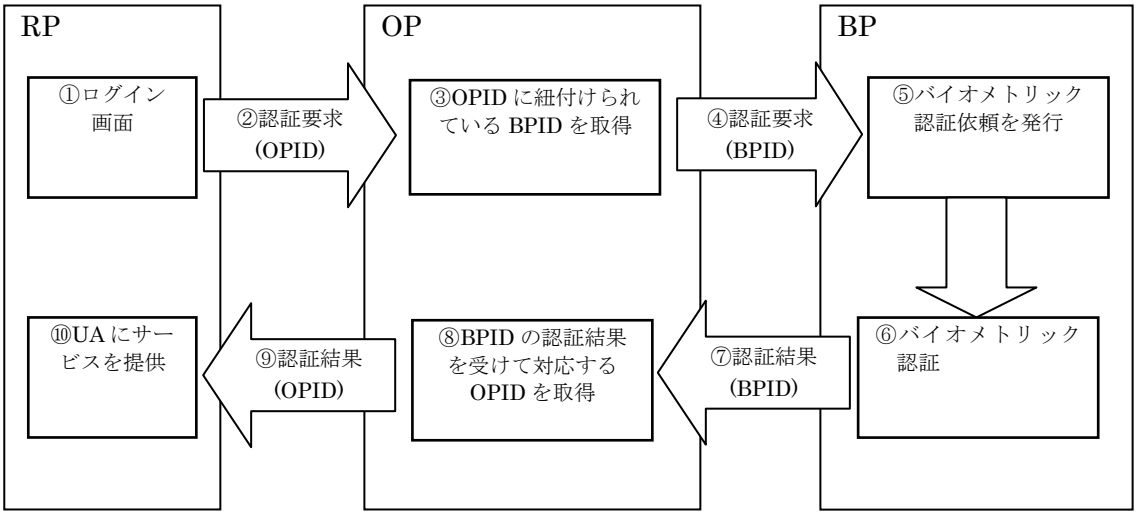


図 2.14 認証処理の流れ

＜2回目認証時の処理の流れ詳細（シングルサインオン動作）＞　（処理の流れを図2.15に示す）

① エンドユーザがRPのログイン画面でOPIDを入力する。

② RPはOPIDを指定してOPに認証要求を行う（OpenIDプロトコルの一部である）。

③ OPは、与えられたOPIDに紐づけられているBPIDをOP内のデータベースから取得する。

④ OPはBPIDを指定して、BPに認証要求を行う（OpenIDプロトコルの一部である）。

⑤ BPは与えられたBPIDからエンドユーザの認証条件を確認する。シングルサインオンとして規定された時間以内に認証済みのエンドユーザが再度認証依頼していると判定すると、BPはUAに対してバイオメトリック認証依頼を発行せず、認証済み扱いとする。

⑥ BPはBPIDを指定して認証結果をOPに提示する（OpenIDプロトコルの一部である）。OPは、与えられたBPIDに紐づけられているOPIDを取得する。

⑧ OPはOPIDを指定して認証結果をRPに通知する（OpenIDプロトコルの一部である）。

⑨ RPは認証結果に応じてエンドユーザにサービスを提供する。

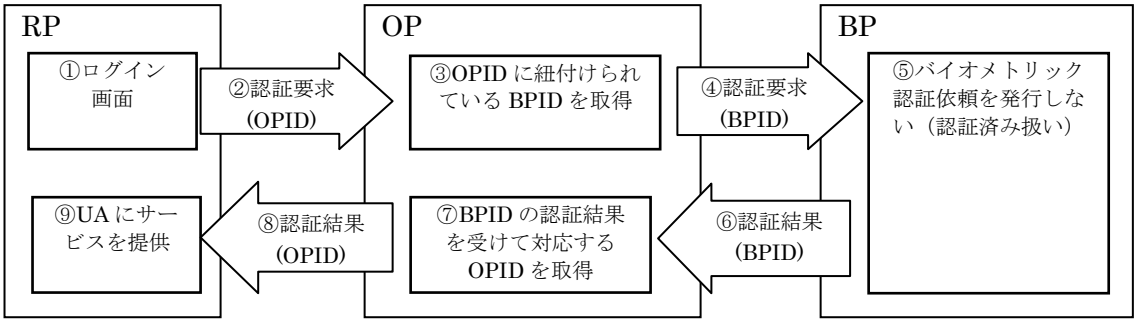


図 2.15 SSO における認証処理の流れ

第３章　開発システムの検証実験と考察

本章では、第2章で説明した共通バイオメトリック認証基盤の仕様検討結果に沿って開発したBioIDMシステムについて、その機能や性能の有効性を検証するために行った検証実験の結果およびその考察について説明する。

3.1　方針

BioIDMシステムを検証する際に用いた実行環境は、以下の条件を基本構成として、要素を変化させながら様々な環境で検証実験を行うこととした。

・システム構成：標準構成
・バイオメトリック認証装置：日立製作所指静脈認証装置
・ブラウザ　　：Google Chrome
・Relying Party：開発時に構築した評価用Relying Party

具体的には上記で示した動作環境に対して、条件を一つだけ変えた環境を用意することで、BioIDMシステムの動作条件を変化させながら機能上・性能上問題がないかどうかを明らかにする。

表3.1に本方針に基づいた検証実験環境を示す。本表で示すとおり、基本条件での実験を行った後に、システム構成、ブラウザ、OpenID対応RPサイトを変えた実験環境で実験を行うこととした。

表3.1　検証実験における動作条件

No	観点	条件	検証対象
1	基本条件試験	システム構成として標準構成、ブラウザとしてChrome、RPとして評価用RPを用いる構成を基本構成とする。	システム全体
2	簡易構成試験	基本条件試験の条件のうち、システム構成を標準構成から簡易構成に変えて試験を行う。	同上
3	ブラウザ試験	基本条件試験の条件のうち、ブラウザをChromeからInternet Explorer 10やFirefoxに変えて試験を行う。	BioIDM ConnectionおよびBioIDM Transactioin
4	国内外RP試験	基本条件試験の条件のうち、RPを評価用RPから国内外のRPに変えて試験を行う。	システム全体

3.2　実験環境の構築

検証実験のシステム構成図を図3.1に示す。

前述の実験方針に従った動作環境として、イントラネット上ではなくインターネット上にOPやBPを配置する必要がある。これは、国内・海外にある既存のRelying PartyからBioIDMシステムに接続するにあたり、OPやBPが開発を担当したOKIソフトウェア社が開発環境として使用した社内イントラネット内に存在したままだと、ファイアウォールなどのセキュリティによってOpenIDプロトコルが正常に動作しないためである。

インターネット上にOPやBPを配置するにあたっては、東京理科大学様のご協力によりサーバを2機借用することができたため、それぞれにOPとBPをインストールして実験を行うこととした。受託者として東京理科大様のご好意に感謝の意を表したい。

端末としてはOKIソフトウェア社のイントラネット上にある端末が2機種用いられた。これらは埼玉県と広島県という国内において地理的に離れた場所に設置されているものである。

これ以外に、国内外のRelying Partyが検証実験に用いられた。実験に用いられたRelying PartyはOpenID発行サイト（http://www.openid.ne.jp/）においてOpenID対応サイトとして紹介されているRelying Partyから抽出したものである。

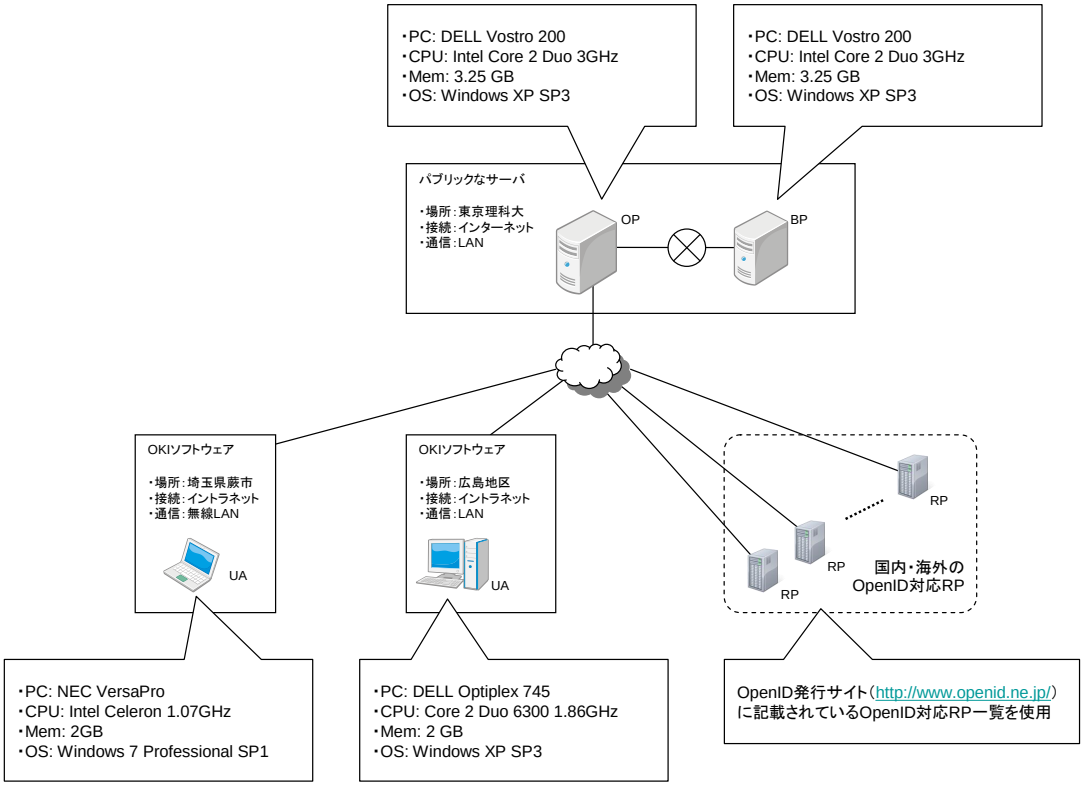


図3.1　検証実験のシステム構成図

3.3 実験結果

本節では検証実験結果についてまとめる。

(1) 結果概要

表3.2に機能実験の結果を示す。本表に示すとおり、機能実験ではまず基本条件試験として図3.1の環境での実験を行った。基本条件試験では、RP-OP-BP-UAの4台のコンピュータが動作する状況で実験を実施した。実施した実験項目は操作試験、SSO（Single Sign On）試験、性能測定の3種類であり、実施項目数は263項目である。

この実験において、Identity Managerと指静脈認証装置を組み合わせたBioIDMシステムにおいて、一通りの機能が正常動作することを確認することができた。これは、当初目標であったOpenIDとバイオメトリック認証を組み合わせたSSOの機能検証ができたことを意味する。

またブラウザ試験では、Internet Explorer 10やFirefoxを用いた機能検証を行った。WebSocketの実装にブラウザ毎の差があることが考えられたが、WebSocketプロトコルとしてはブラウザに違いは見られず、どれも正常に動作した。また、国内外RP試験においては既存のRPとの接続を行い、正常動作するRPが存在することが確かめられた。

ただし本検証実験において、機能面および性能面についていくつかの考慮事項が存在することもわかった。それぞれの実験結果の詳細については(2)以降に示す。

表3.2　機能実験結果概要

No	項目	環境			試験内容	結果概要
		システム構成	ブラウザ	RP		
1	基本条件試験	標準構成（RP-OP-BP-UA)	Chrome	試験用RP	①操作試験：167項目 ②SSO試験：13項目 ③性能測定：40項目	①開発プログラムおよびIdentity Serverにおいて、生体認証およびSSO機能が正常に動作した。 ②性能においてはOpenIDプロトコルによる通信時間の全体時間に占める比率が高い。(1)
2	簡易構成試験	簡易構成(RP-BP-UA)	Chrome	試験用RP	①操作試験：3項目 ②性能測定：40項目	
3	ブラウザ試験	標準構成(RP-OP-BP-UA)	IE10およびFirefox	試験用RP	①操作試験(IE10)：48項目 ②操作試験(Firefox)：48項目	WebSocketの通信機能そのものはブラウザ間に違いはなく正常動作した。 ただし、SSLに関してブラウザによって実装上の違いがあった。
4	国内外RP試験	標準構成(RP-OP-BP-UA)	Chrome	国内外のRP	①操作試験(国内RP)：8サイト ②操作試験(海外RP)：5サイト	RPにより接続できるものとできないものがある。 接続できない主な原因として、RPが使用可能なOPを限定していることが考えられる。

(2) 標準構成試験の詳細

以下に標準構成試験の試験結果詳細を説明する。

① 操作試験

一般的な操作周りの試験（ボタンの動作）や画面表示、画面遷移について目視で動作を確認する試験である。登録機能の開始から終了までの一連の操作、および認証機能の開始から終了までの一連の操作について合計167項目の試験項目を作成し結果を確認した。すべての項目が合格という結果となった。

② SSO試験

OpenIDが持つSSO機能の有効性を検証するための試験である。以下の2つのケースを想定して今回実装で採用したIdentity ServerのSSO機能がバイオメトリック認証と組み合わせて正常に動作するかどうかを検証した。13項目の試験がすべて合格という結果となった。

・複数RPによる試験1: 2つのRPから同一のIDを用いて、ひとつのBioIDMシステムに認証依頼を複数回行う試験である。2回目以降の認証依頼はエンドユーザに対してバイオメトリック認証要求が行われず、Identity Serverによって本人認証が正しくスキップされることを確認した。

・複数RPによる試験2: 2つのRPから異なるIDを用いて、ひとつのBioIDMシステムに認証依頼を行う試験である。BioIDMから見て2回目以降の認証依頼であっても、エンドユーザに対して正しくバイオメトリック認証要求が行われることを確認した。

・許可確認動作試験:認証成功後にIdentity Serverがエンドユーザに対してIdentity Serverによる認証をRPが用いることを許可することを意味する“Approve”ボタンあるいは“Approve Always”ボタンを押した後、再度認証を行った場合のIdentity Serverの動作が想定どおりであることを確認した。

ただし、以下の制約がある。

Identity ServerはApprove Alwaysを押したとき、RPがリクエスト時に指定したopenid.return_to パラメータをサーバ内に記録し、次回以降同一のタイミングで記録した情報を参照し画面表示要否を判断する。RPによっては、このパラメータが同一ユーザでも異なる場合があるため、そのようなRPの場合同一ユーザでも認証許可画面が再度表示されてしまう。この問題は、RPの実装とOPの実装の違いで発生するものと推測される。今回はOPとしてWSO2社がOSSとして公開しているIdentity Serverを用いたが、実際のアプリケーション開発の際にはこのような状況への対応について検討する必要がある。

③ 性能測定の詳細

図3.2に基本条件試験における性能測定ポイントについて示す。

本図において、(a)から(f)が性能測定ポイントであることを示す。各ポイントはそれぞれ以下のとおりである。

(a): UAにおいてRPに対する認証依頼を開始するポイントである。エンドユーザがOpenIDプロバイダにユーザ入力識別子を指定するとともに認証依頼を行うタイミングである。

(b): 認証依頼を受けたRPから2回のリダイレクトを経て、BPがUAに対して本人認証のための処理開始を行うタイミングである。（BP内のサーバプログラムが端末内のBioIDM Connectionに認証依頼を発行したときの、UA内で依頼を受け付けるタイミングである。）

(c): BioIDM ConnectionがBioIDM Transactionに対して認証依頼を発行するタイミングである。

(d): BioIDM Transactionが認証結果をBioIDM Connectionに返却するタイミングである。

(e): BioIDM ConnectionがBP内のサーバプログラムに認証結果を返却するタイミングである。

(f): BPからRPまで2回のリダイレクトを経て、RPがUAに対して認証結果を返却するタイミングである。

これらより、性能の単位として以下の3つを挙げることができる。

(f) - (a) = 認証開始から終了までの総時間

(e) - (b) = UA内認証時間（UA内でバイオメトリック認証にかかった総時間）

(d) - (c) = バイオメトリック処理時間

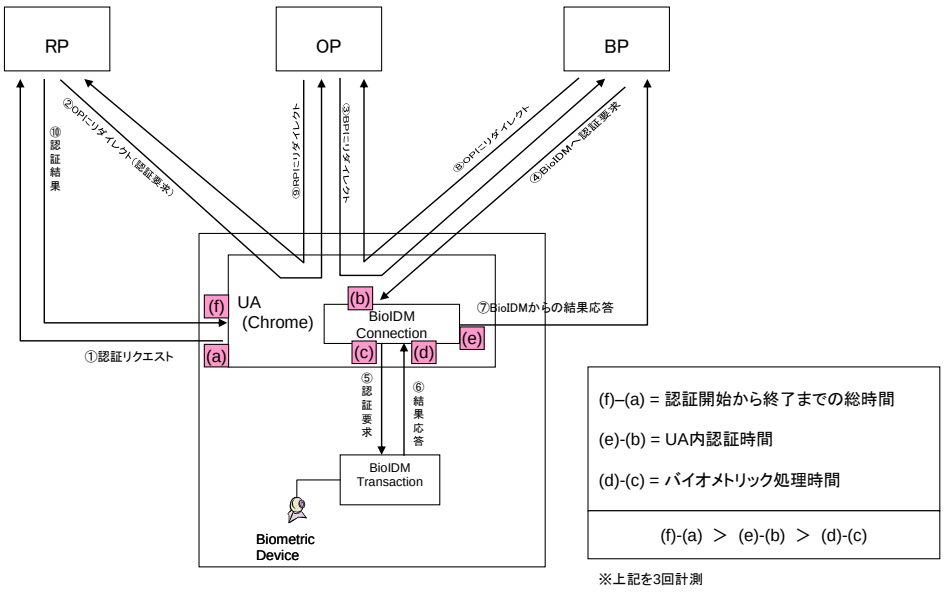


図3.2　標準構成における性能測定ポイント

④ 性能実験結果

表3.3に性能実験結果を示す。本表において、(1)から(3)は前述の性能測定ポイントで測定した時間であり、(4)から(6)は3つの測定時間から算出した時間である。このうち(3)のバイオメトリック処理時間は、バイオメトリック認証装置を用いて被験者がバイオメトリック情報をキャプチャした時間が含まれる。キャプチャ時間には被験者の挙動時間（センサーに人体の部位を移動させ、キャプチャ可能な状況（静止する、向きを合わせる、などのために要する時間）が含まれる。）一般的に挙動時間は、被験者の挙動やバイオメトリック認証装置によって異なるため、本性能実験としては参考情報として取り扱う。また、今回の性能実験は同様の操作を3回繰り替えして平均をとったものだが、3回の測定において毎回ブラウザのキャッシュを削除したものと、削除しなかったものを併記した。両者の測定結果を比較すると、毎回キャッシュを削除した方が時間がかかっているが、これは削除しない場合において1回目より2回目と3回目の方がキャッシュの効果で処理が短時間で終わっているためである。ブラウザのキャッシュを削除しない場合は、測定回数が多ければ平均時間が少なくなる傾向があるため参考値として扱うこととし、3回の測定で安定した結果となった毎回キャッシュを削除する場合について考察する。

本表の(4)は認証開始から終了までの総時間からバイオメトリック処理時間を減じた時間であり、本システムにおける認証のための総時間からバイオメトリック認証処理時間を取り除いた所要時間である。本表の(5)はUA内認証時間からバイオメトリック処理時間を引いた時間であり、本システムにおいてブラウザ内に認証依頼が来てから処理が終わるまでの時間からバイオメトリック処理時間を減じたものである。また、本表の(6)は認証開始から終了までの総時間からUA内認証時間を減じたものであり、RPやOP、BPとUA間でネットワーク通信を含む一連のOpenIDプロトコルを実行するための時間と考えられる。

表3.3　標準構成の性能実験結果

※3 回測定した平均値

No	観点	内容	ブラウザのキャッシュ		備考
			毎回削除	削除しない	
(1)	認証開始から終了までの総時間	(f) – (a)	7.5秒	6.4秒	
(2)	UA内認証時間	(e) - (b)	2.0秒	1.9秒	
(3)	バイオメトリック処理時間（参考情報）	(d) - (c)	(1.5秒)	(1.5秒)	キャプチャのための被験者の挙動時間や初期処理・終了処理時間を含む
(4)	総時間からバイオメトリック処理時間を引いた時間	(1) – (3)	**6.0秒**	**4.9秒**	バイオメトリック認証を除いたシステム処理時間
(5)	UA内認証時間からバイオメトリック処理時間を引いた時間	(2) – (3)	**0.5秒**	**0.4秒**	BSP処理時間を除いたBioIDM ConnectionとTransactionの処理時間
(6)	総時間からUA内認証時間を引いた時間	(1) – (2)	**5.5秒**	**4.5秒**	

本表の結果より、今回の実装を用いたバイオメトリック認証を伴うOpenIDの認証機能では、バイオメトリック認証時間を除いた場合、全体にかかった6.0秒のうち、約92%に相当する時間がOpenIDプロトコルの処理時間であったことがわかる。（5.5秒 ÷ 6.0秒 ＝ 約92%）

(3) 簡易構成試験の詳細

以下に簡易構成試験の試験結果について詳細を説明する。

① 操作試験

一般的な操作周りの試験（ボタンの動作）や画面表示、画面遷移について目視で動作を確認する試験である。登録機能の開始から終了までの操作や照合機能の開始から終了までの操作など、主要な機能について全般的な処理の流れに着目した試験項目3項目分を作成し結果を確認した。すべての項目が合格という結果となった。

② 性能測定試験

図3.3に標準構成における性能測定ポイントについて示す。

前述の標準構成と同様に、(a)から(f)が性能測定ポイントを用いて測定する。各ポイントの意味は標準構成の場合と同様である。

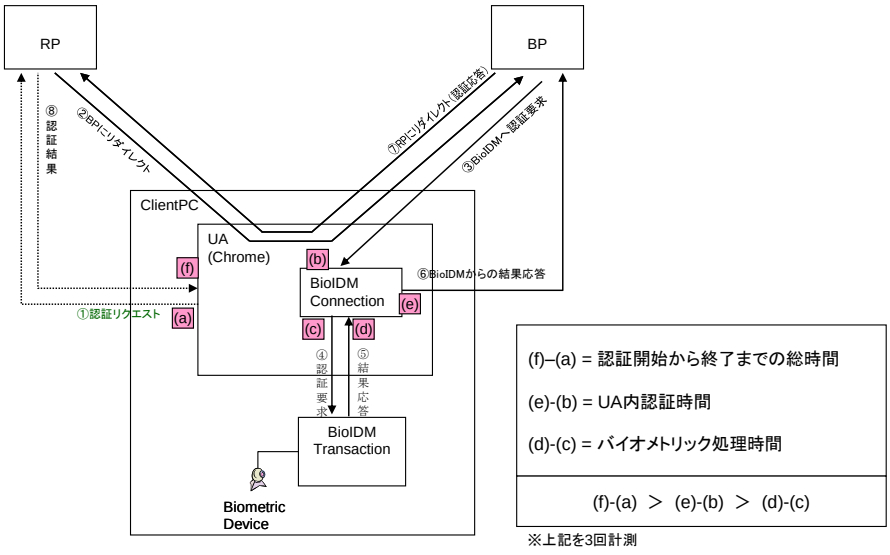


図3.3　簡易構成における性能測定ポイント

③ 性能実験結果

表3.4に性能実験結果を示す。本表の見方は前述の表3.3の場合と同様である。

表3.4　簡易構成の性能実験結果

※3 回測定した平均値

No	観点	内容	ブラウザのキャッシュ		説明
			毎回削除	削除しない	
(1)	認証開始から終了までの総時間	(f) – (a)	4.4秒	4.0秒	
(2)	UA内認証時間	(e) - (b)	2.0秒	2.0秒	
(3)	バイオメトリック処理時間(参考情報)	(d) - (c)	(1.7秒)	(1.5秒)	キャプチャのための被験者の挙動時間や初期処理・終了処理時間を含む
(4)	総時間からバイオメトリック処理時間を引いた時間	(1) – (3)	**2.7秒**	**2.5秒**	バイオメトリック認証を除いたシステム処理時間
(5)	UA内認証時間からバイオメトリック処理時間を引いた時間	(2) – (3)	**0.3秒**	**0.5秒**	BSP処理時間を除いたBioIDM ConnectionとTransactionの処理時間
(6)	総時間からUA内認証時間を引いた時間	(1) – (2)	**2.4秒**	**2.0秒**	

本表の結果を前述の表3.3と同様の方法で考察する。

今回の実装を用いたバイオメトリック認証を伴うOpenIDの認証機能では、バイオメトリック認証時間を除いた場合、全体にかかった2.7秒のうち、約89%に相当する時間がOpenIDプロトコルの処理時間であったことがわかる（2.4秒 ÷ 2.7秒 ＝ 88.9%）。

表3.5に、標準構成での性能結果と簡易構成での性能結果を比較した表を示す。（ブラウザのキャッシュを毎回削除したもの同士を用いて比較する。）

表3.5　標準構成と簡易構成の性能結果比較

※ブラウザのキャッシュを毎回削除した場合

No	観点	内容	標準構成	簡易構成	比率
(1)	認証開始から終了までの総時間	(f) – (a)	7.5秒	4.4秒	1.7
(2)	UA内認証時間	(e) - (b)	2.0秒	2.0秒	1.0
(3)	バイオメトリック処理時間(参考情報)	(d) - (c)	(1.5秒)	(1.7秒)	(0.9)
(4)	総時間からバイオメトリック処理時間を引いた時間	(1) – (3)	6.0秒	2.7秒	**2.2**
(5)	UA内認証時間からバイオメトリック処理時間を引いた時間	(2) – (3)	0.5秒	0.3秒	**1.7**
(6)	総時間からUA内認証時間を引いた時間	(1) – (2)	5.5秒	2.4秒	**2.3**

本表では標準構成での測定結果と簡易構成での測定結果から、それぞれの処理時間の比率を計算している。バイオメトリック処理にかかる時間そのものは、標準構成および簡易構成で性能に影響を与えるシステム上の違いはないため、両構成におけるバイオメトリック処理時間の差異はバイオメトリック情報取得時の被験者の挙動など、人間の動作に要する時間の差異が主であると考えられる。バイオメトリック処理時間を除いたシステムの処理時間に着目すると、本表より総時間からバイオメトリック認証処理時間を引いた時間について、標準構成と簡易構成の比率は2.2となった。また、総時間からUA内認証時間を引いた時間の標準構成と簡易構成の比率もほぼ同様の2.3であった。標準構成は簡易構成に比べて、OpenIDプロトコルを回して通信するための時間が2倍以上を要していることがわかる。標準構成と簡易構成ではOpenIDプロトコルのための通信処理回数の割合が以下のとおりほぼ2倍に近い割合となっている。

・標準構成における通信回数：20回
（8回のリダイレクト関係通信および8回のアソシエーション関係通信を含む）
・簡易構成における通信回数：12回
（4回のリダイレクト関係通信および4回のアソシエーション関係通信を含む）

このことから、標準構成において認証性能を向上させるにあたっては、通信回数の削減が最も寄与する可能性が高いと予想される。性能向上についての検討は今年度事業の対象外とし、来年度以降の検討とした。

(4) ブラウザ試験の詳細

以下にブラウザ試験の試験結果について詳細を説明する。

① 操作試験

WebSocketに対応しているブラウザとしてInternet Explorer 10（Windows 7用プレリリース版）およびFirefox 18を用いた試験を実施した。それぞれのブラウザについて基本操作パターン48項目を実施し、すべての項目が合格となった。

② 課題

本検証実験において、WebSocketのSSL対応に関係して課題が見つかった。以下にその内容について説明する。

本開発においてBioIDM Transaction内で実装したWebSocketはSSLに対応できていない。

（使用したOSSであるwebsocket++が、本事業におけるソフトウェア開発の段階でSSL未対応だったため。）

OpenID仕様ではRPやOPとUA間のすべての通信にSSLを用いることが強く推奨されている。

標準構成において、BioIDM TransactionのWebSocketがSSL対応できていないというこ

とは、BPからUAに対して認証依頼を発行したあとブラウザ内のBioIDM ConnectionとBioIDM Transactionの間で行われるWebSocket通信でSSLが使えないことを意味する。

この状況を図3.4に示す。本図において実線の矢印で示すとおり、RP、OP、BPおよびUA（この場合はChrome）との間ではSSL通信（HTTPS）が行われるが、Chrome内のBioIDM ConnectionとBioIDM Transactionの間のWebSocket通信はSSL化できていない。

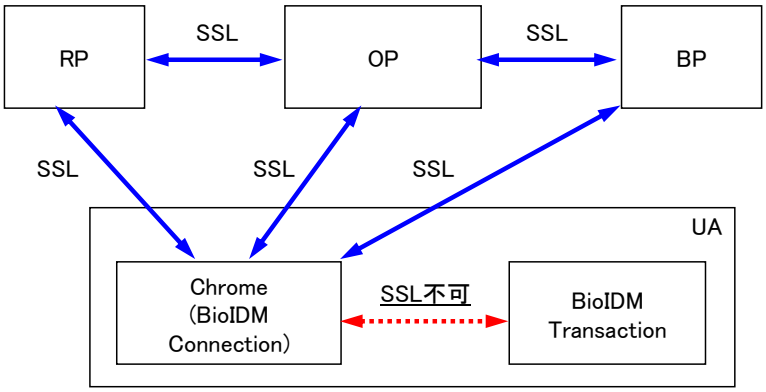


図3.4　本開発におけるOpenIDとWebSocketのセキュア通信の状況

このような実装上の制約下において、Google Chromeは問題なく動作するが、Internet Explorer10およびFirefox 18では、BPからの認証要求でHTTPSが用いられると、その後のBioIDM ConnectionとBioIDM Transaction間のWebSocketがSSLでない場合、WebSocket通信がエラーとなる。Internet Explorer 10およびFirefoxでの動作詳細を図3.5に示す。

これは、BPとUA間ではセキュアな通信が行われていたのに、その後に制御が移ってからブラウザのWebSocket通信でセキュリティが低下したことについてブラウザによるチェック機構が働いたものと考えられる。

Internet Explorer 10　（Windows7用Prerelease版）にはこのエラーに対する対処方法は存在しなかったが、Firefoxについてはブラウザの設定値(network.websocket.allowInsecureFromHTTPS)を有効にすることにより、このチェック機構を無効にすることができる。

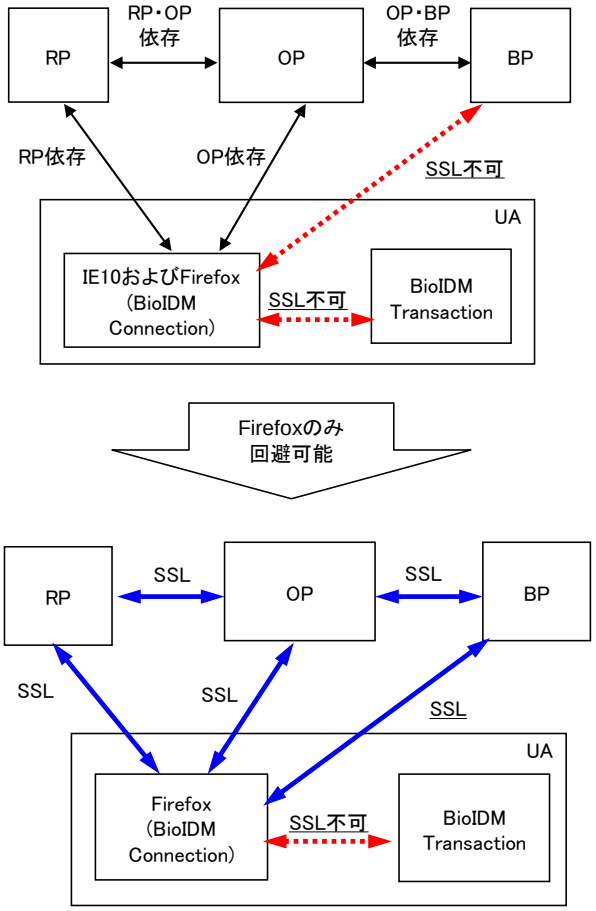


図 3.5　SSL 対応に関する IE10 および Firefox の動作詳細

③ 課題への対策案

本課題に対する対応策としてWebSocketのSSL対応が考えられる。本報告書執筆時点である平成25年3月において、WebSocketのオープンソースのSSL対応版が提供済みのため、今後の開発においてはWebSocketのSSL対応が可能となる。

(5) 国内外RP試験

以下に国内外RP試験結果について詳細を説明する。

国内外のRPとしては、OpenIDに関するWebサイトである http://www.openid.ne.jp/ において平成25年2月時点で、OpenID対応サイト一覧として紹介されていた国内サイト（日本語対応）および海外サイト一覧（英語）として示されているサイト名とURLのリストの中からいくつかのサイトを選んで検証実験を行った。

国内サイト（日本語対応）での実験結果の詳細を表3.6に示す。本表に示すとおり、6サイトで確認したうち、5サイトで成功（ないし条件付成功）となった。1サイトのみOpenIDプロトコルが正常に動作しなかったが、RP側でOPを限定していることが判明したため、検証試験の対象外とした。

表3.6　国内サイト（日本語対応）に掲載されているRPでの動作確認結果

RPサイト名	URL	結果	詳細
Choix	http://www.choix.jp	対象外	限定されたOPしか許していない（対象OP：Yahoo,Hatena,Jugemu,livedoorの
LiveJournal	http://www.livejournal.com/openid	成功	OpenIDで直接ログイン可能（ユーザ登録不要）。URL入力のみでログイン可能。
Place engine	http://www.placeengine.com/auth/login	成功	OpenIDで直接ログイン可能（ユーザ登録不要）。URL入力のみでログイン可能
Stack Stock Books	http://stack.nayutaya.jp/	成功	OpenIDで直接ログイン可能（ユーザ登録不要）。 URLのみでログイン可能（登録時j）
ClipCast	http://clipcast.jp/	条件付成功	OPのサーバ証明書が正式なものでない為、TLSハンドシェイク時にエラーが発生する（48:unknown_ca）。httpで接続したところ使用できた。
埼玉の地域情報 Saitama-e.com	http://www.saitama-e.com/	条件付成功	OPのサーバ証明書が正式なものでない為、TLSハンドシェイク時にエラーが発生する（48:unknown_ca）。httpで接続したところ使用できた。

海外サイト一覧（英語）で示されたRPサイトを用いた試験結果について表3.7に示す。本表に示すとおり、5サイトで確認したうち、2サイトで成功となった。残りの3サイトでOpenIDプロトコルが正常に動作しなかった。現時点で原因は不明であるが、このうちの2件についてはRP側でOPを限定しているか、要求する属性情報が見つからなかったことが原因の可能性がある。

表3.7　海外サイト一覧に掲載されているRPでの動作確認結果

RPサイト名	URL	結果	詳細
Hampr	http://www.hampr.com/home	失敗	OPのURLやOpenID URLをログイン用テキストボックスに入力してSubmitしたが、ログイン画面に進まなかった。原因不明。
Wikitravle	http://wikitravel.org/en/Special:OpenIDLogin	保留	OpenID URLを入力すると以下のエラーが発生してログインできない。 An error occured during verification of the OpenID URL. OpenID の URL を限定している可能性あり。（My OpenID 、Flickr 、LiveJournal、Verisign,Blogger）
LiveJournal	http://www.livejournal.com/openid	成功	RPへの正常登録および認証ができた。
userstyles	http://userstyles.org	成功	RPへの正常登録および認証ができた。
ClaimID	http://claimid.com	失敗	RPへの登録のためにOPで認証成功後、以下のエラーが表示される。 error:Required attributes missing ns:http://specs.openid.net/auth/2.0

3.4　考察およびまとめ

本節では、前述までで示した検証実験の考察およびまとめを示す。

(1) 基本条件試験および簡易構成試験

WSO2のIdentity ServerとBioIDMシステム（BioIDM Connection、BioIDM Transaction、BioAPI Framework）および日立指静脈認証装置を組み合わせることにより、バイオメトリック認証を用いたOpenIDシステムのバイオメトリック情報登録から認証までの基本機能およびSSOの機能が正常に動作することを確認できた。これにより、本事業の当初目標を達成することができた。

(2) 性能測定

標準構成と簡易構成の2種類の構成で、バイオメトリック認証に要する時間を計測した。特に標準構成においてOPとBPの間の通信処理時間が大きく、簡易構成の約2倍の時間がかかっていることがわかった。RPやOP・UAなどの各構成要素間のOpenIDプロトコルのための通信回数が多く、その分時間を要したことが標準構成において時間がかかる原因と考えられる。標準構成における性能改善について今後検討する必要がある。

(3) ブラウザとSSL

WebSocketは主要ブラウザへの搭載が出揃ったばかりの比較的新しい技術であるが、Google Chrome・Internet Explorer 10（Windows7 Prerelease版）、FirefoxともにBioIDM TransactionとのWebSocket通信が正常に動作することが確認できた。ただし、BioIDM Transactionに組み込んだWebSocketにおいて現状SSLが実現されておらず、セキュリティ上の問題となるとともに、Internet Explorer 10やFirefoxではWebサーバがHTTPSで動作している場合、WebSocketがSSL未サポートだとWebSocketが失敗してしまうことがわかった。WebSocketのSSL対応版OSSの提供がはじまったため、今後対応が可能である。

(4) 国内・海外RP

国内RP、海外RPともに今回開発したBioIDMシステムの標準構成にてバイオメトリック認証による正常なログオンが行えることがわかった。ただし、一部のRPについて正常動作しなかった。いくつかのケースにおいてOPに対してOpenIDプロトコルが通知されてこないことから、RPが利用可能なOPを限定している可能性が考えられる。それ以外のRPにおいては原因が特定されていないものもあるため、本事業で開発したシステム側の原因かどうかの切り分けが今後必要である。

24 - 84

平成 24 年度
IdM における共通本人認証基盤の開発研究
報　　告　　書

平成２５年３月

作　　成　一般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