25-121

平成 25 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 26 年 3 月

一般社団法人　日本自動認識システム協会

Auto Race

この事業はオートレースの補助(25-121)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います。

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います。

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、平成 23 年度より 3 年間、取り組んで参りました。この研究開発は、財団法人 JKA 殿より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)そして平成 25 年度はオートレースの補助(25-121)を受けて実施しました。

この「平成 25 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 25 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26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

今後の民間あるいは行政における電子サービスの充実と形態の多様化により、各電子サービス間での認証連携の重要性が増してきていると考えられる。このことはシステムに適用される個人の ID（IDENTIFICATION ; 個体識別符号）を扱う IdM（アイデンティティマネジメント）の中で、複数の電子サービス間の認証連携で必要とされるユーザ認証技術を簡単で安全で安心な形で提供する必要性が増大することを意味する。しかしながら現状を見ると、残念ながらユーザ認証に用いられることの多いパスワードの持つ問題を回避できる簡便なセキュリティ技術が提供されていないと言わざるを得ない状況である。

そのため、今後の社会発展には、IdM システムに適用される本人認証基盤として、バイオメトリック認証技術の持つ特徴を生かしながら電子認証システム等におけるセキュリティの考え方を考慮した複数のバイオメトリック認証技術が組み込み可能な本人認証基盤技術を提供することにより、パスワードの持つ問題が回避され、かつ効率的に管理・運用のできる IdM システムが、全世界的に適用・運用され、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てゆくことが、重要と考えられる。

本事業では、その声にこたえるため、今後の民間あるいは行政での電子サービスの充実と形態の多様化に対応することを目指し、IdM システムに用いることのできる複数のバイオメトリック認証技術を組み込むことを可能とする本人認証基盤の研究と開発を行った。また、電子認証システム等で考慮されるようなったセキュリティの考え方とここで研究開発する共通本人認証基盤との融和あるいはその位置づけの明確化に関する研究と開発に取り組んだ。加えて、実システムへの適用を促進するため、成果を IdM システム開発者、バイオメトリック技術ベンダおよびシステム関係者に周知することも目的とした。

2. 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、活動した。

(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である。

(1) 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。）

(2) 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。）

(3) H25 年度：認証基盤プロトタイプの完成
（複数技術（指紋、静脈、顔、虹彩など）が組み込み可能な認証基盤の完成、
ならびに電子認証システムへの適用（H25 年度追加計画））

平成 25 年度の開発研究は、平成 23 年度および平成 24 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 3 年度として、複数技術（指紋、静脈、顔、虹彩など）が組み込み可能な認証基盤の完成、ならびに電子認証システムへの適用について研究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

(2) プログラム開発とシステム性能評価、検証実験の実施及び評価

3. 開発研究の実施体制

(1) 管理体制および研究体制

本事業の中の全体計画、進行管理、ならびに産官学の有識者により構成した委員会（IdM における共通本人認証基盤検討委員会）の開催、運営を（一社）日本自動認識システム協会が行った。

IdM における共通本人認証基盤検討委員会にて有識者（委員）の知見を持ち寄り、研究開発事項、調査事項の検討ならびに研究成果を取りまとめた。

また、検討委員会で仕様検討時に必要とされる専門的事項の検討にあたって、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。

さらに、検討委員会で提案された海外調査は、具体的な調査項目、調査先および派遣者を委員会にて検討の上、実施した。

なお、検討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。

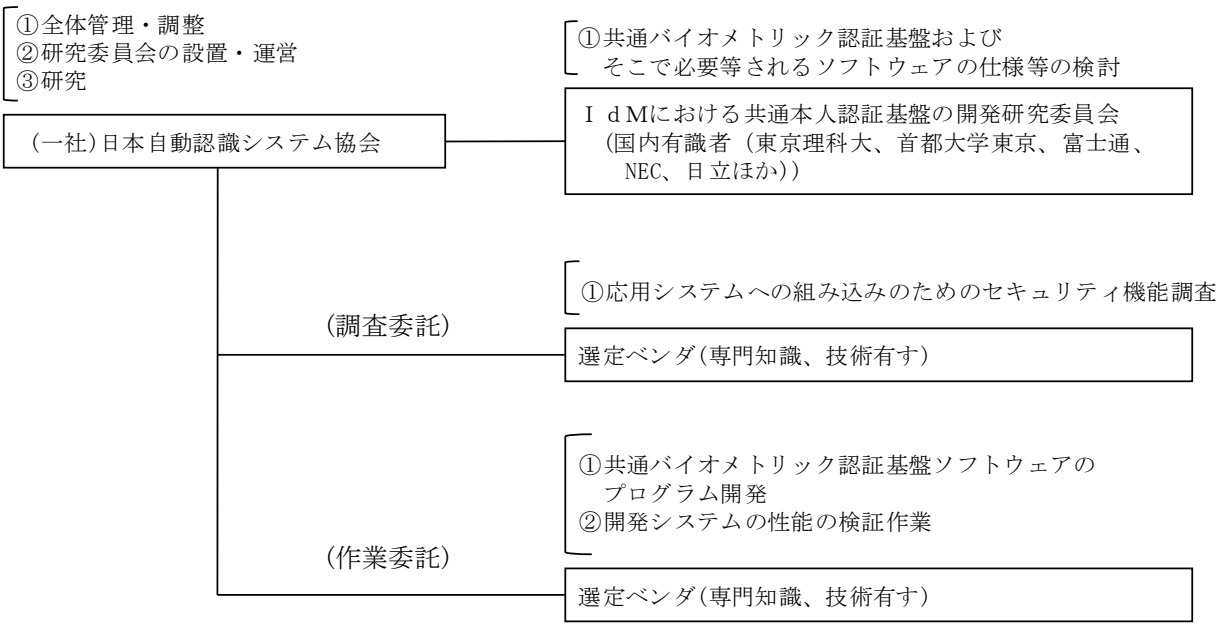


図 3.1　事業実施体制

(2) IdM における共通本人認証基盤の開発研究委員会

表 3.1　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	SC37WG4 委員
委員	中村 敏男	(株)OKI ソフトウェア	SC37WG2 エキスパート
委員	寶木 和夫	独立行政法人　産業技術総合研究所	
委員	山口 利恵	東京大学	
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）	SC37 専門委員会 委員長
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	SC37 専門委員会 幹事
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	岩永 敏明	経済産業省	SC37 専門委員
オブザーバ	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

4. 開発研究の内容概要

4.1 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 4.1)。

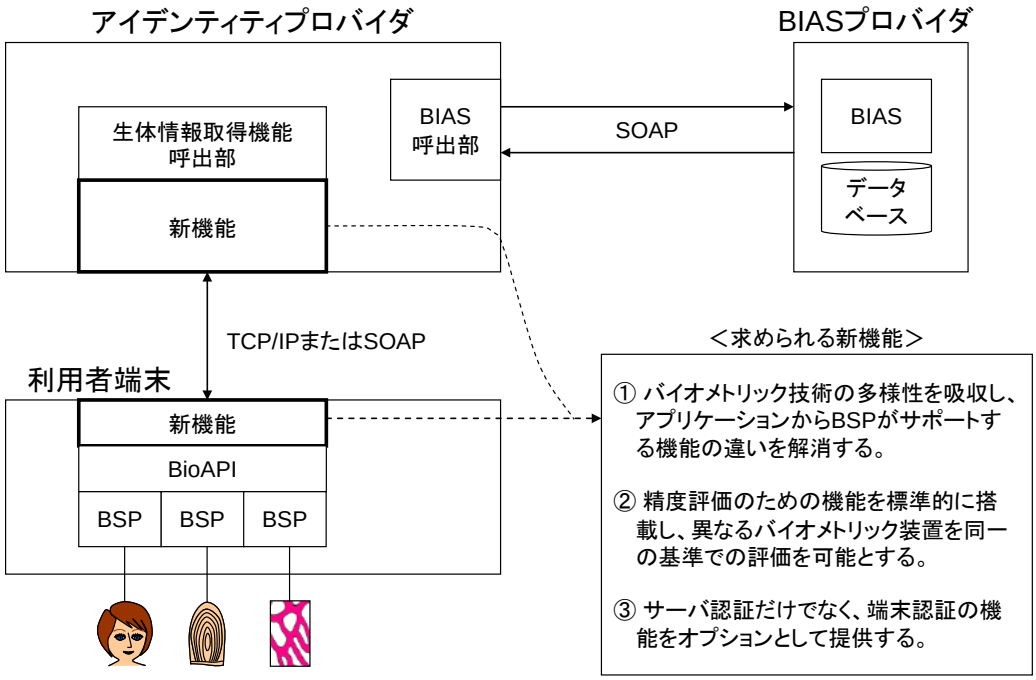


図 4.1　IdM と連携するバイオメトリック認証に求められる新機能

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 4.2 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。

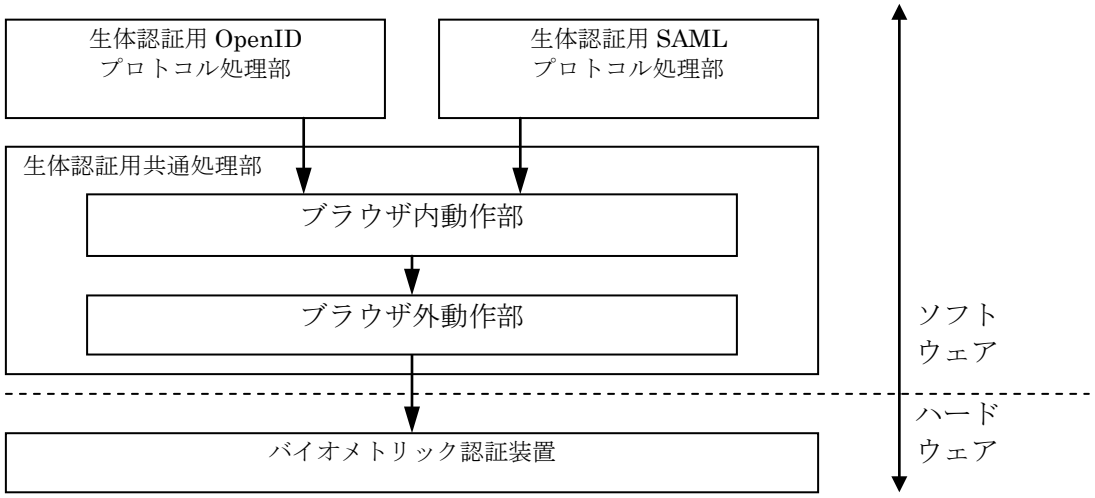


図 4.2　共通バイオメトリック認証基盤の概念

4.2 従来活動成果概要

4.2.1 平成 23 年度活動成果概要

本事業の平成 23 年度活動成果概要を以下に示す。

⑴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。

⑵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。

⑶ 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。

4.2.2　平成 24 年度活動成果概要

本事業の平成 24 年度活動成果概要を以下に示す。

(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

平成 23 年度に引き続き 10 月下旬に開催された英国 Biometrics Exhibition and Conference 2012 の調査を行った。Biometrics Exhibition and Conference 2012 は、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られた。

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るに至った。

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られた。

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

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との結論を得た。

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。

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た。

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た。

4.3 平成 25 年度の実施事項

4.3.1 平成 25 年度の実施事項の概要

平成 25 年度は、平成 23 年度および平成 24 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 3 年度として、複数技術（指紋、静脈、顔、虹彩など）が組み込み可能な認証基盤の完成、ならびに電子認証システムへの適用について研究することを目標として、次の事項を実施した。

(1) IdM における共通本人認証基盤検討委員会

本検討委員会にて有識者（委員）の知見を持ち寄り、研究開発事項、調査事項の検討ならびに研究成果を取りまとめるために、産官学の有識者により構成した IdM における共通本人認証基盤検討委員会を組織し、都合 4 回の委員会を開催した。

(2) 市場動向調査

検討委員会で委員よりの提案を受けて、具体的な調査項目、調査先および派遣者を委員会にて検討の上、海外調査を実施した。

第 1 回委員会の審議により、具体的な海外調査として、定点観測として平成 24 年度に引き続き英国 Biometrics Exhibition and Conference 2013(BC2013)の調査を瀬戸委員にお願いすることとなり、10 月中旬に開催されたコンファレンスに委員を派遣し、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 に関する最新の動向を調査した。

(3) 応用システムへの組み込みのためのセキュリティ機能の調査研究

共通バイオメトリック認証基盤機能に適用可能なセキュリティ技術の調査とともに、本事業成果が適用できるアプリケーションの選定とアプリケーションの機能調査を行った。また、そのアプリケーションで必要となるセキュリティ機能について調査研究した。

なお、この調査研究は、委員会検討内容と関連性が深くまた専門性が高いため、委員各社間から委託先を選定し委託した。

(4) IdM 共通本人認証基盤の機能強化のための開発研究

バイオメトリクスを電子認証システム等に適用する際の共通バイオメトリック認証基盤の機能強化のため、平成 24 年度に開発研究した OpenID に加え、もうひとつの主要な IdM システムである SAML にも適用可能とする研究を行った。

また、前年度組み込んだ指静脈認証技術に加え、複数のバイオメトリック認証技術の組み込みを可能とする基盤部の機能追加の研究を行った。

これらの実施にあたっては、前述のＩｄＭにおける共通本人認証基盤検討委員会にて検討内容を審議し、方向性を確認しながら研究を進めた。

さらに、上記の研究をもとにして、プロトタイププログラムの開発とシステム性能評価および検証実験を行い、検討委員会にて報告し検証した。

なお、プログラム開発とシステム性能評価および検証実験は、委員会検討内容と関連性が深くまた専門性が高いため、委員各社間から委託先を選定し作業委託した。

4.3.2　平成 25 年度の実施日程

本事業は、それぞれを図１に示す日程で実施した。

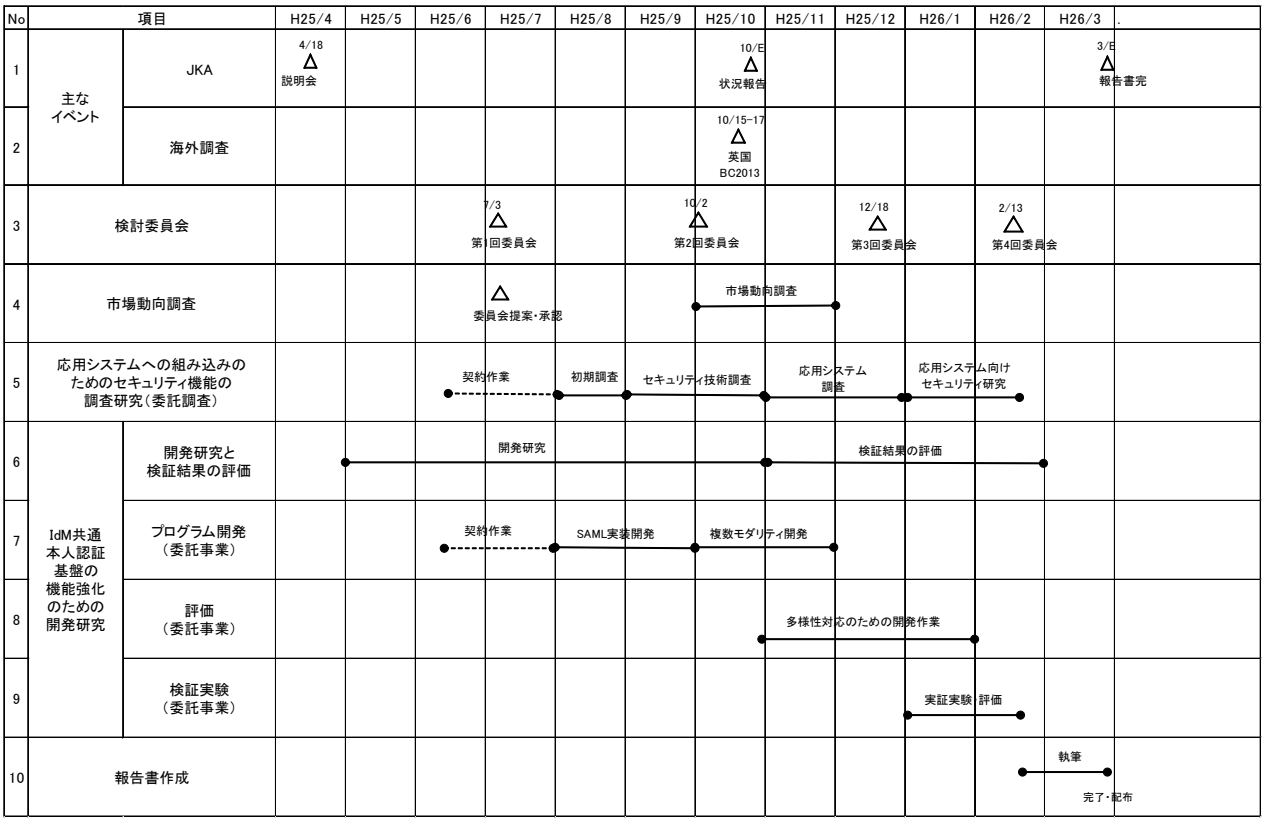


図 4.1　開発研究実施日程

4.4　平成 25 年度成果概要

(1) 検討委員会活動

検討委員会活動は下記である。

①第 1 回検討委員会　平成 25 年 7 月 3 日(水)　　13:00～15:00

1) 趣旨説明及び全体計画紹介

平成 25 年度の「IdM における共通本人認証基盤の開発研究」事業の概要が説明された。3 か年計画の第 3 年度(最終年度)として、認証基盤プロトタイプの完成（複数技術が組み込み可能な認証基盤の完成/電子認証システムへの適用で共通認証基盤全体のプロトタイプの開発を完了することが目標であることが説明された。

2) 本年度の検討事項および開発計画審議

本年度の主な活動内容として下記が提案され、審議の上、承認された。

①共通バイオメトリック認証基盤ソフトウェアの研究では下記を行うこと。

－特定の IdM システムに非依存とし汎用性を持つという目標に対して、本年度は主要な IdM 技術の一つである SAML に対して対応するための検討と開発を行い、有効性を検証すること。

－バイオメトリクスの特性を考慮するため認証技術の多様性に対応するという目標に対して、本年度は手のひら、指紋、顔、虹彩など様々なモダリティのバイオメトリック製品の入手が可能か検討し、入手可能な製品を用いた評価を行い必要な場合は追加開発を行うこと。

－バイオメトリクスの特性を考慮するためプライバシー（セキュリティ）について配慮するという目標に対して、本年度はセキュリティ機能の実現のため、暗号化技術・ACBio・WebSocket の SSL 化の 3 点について調査を行い、実装方法の検討を行い、また、可能な限り実装も行うこと。

②応用システムへの組み込みのためのセキュリティ機能の調査研究内容として、平成 24 年度の研究成果として、OpenID における本人認証の保証レベルと生体認証の組み合わせから、適用が考えられるアプリケーションとして、震災対応システムの可能性が示されたことを踏まえ、震災対応アプリケーションについての調査検討を進めること。

3) 市場調査計画案審議

委員よりご提案のあった英国 BC コンファレンス 2013 にて海外調査を行う計画について審議し、提案委員が出張し調査することが承認された。

4) 作業委託計画提案および見積り依頼

5) 委託調査計画提案および見積り依頼

6) 実験用機器の借用依頼

②第 2 回検討委員会　平成 25 年 10 月 2 日(水)　　10:00～12:00

1) 作業委託/調査委託について状況の口頭報告

作業委託見積り依頼および委託調査見積り依頼の結果として、見積り回答があった会社はそれぞれ 1 社であり、(一社)日本自動認識システム協会内で検討し、当該 1 社に対して委託することに決定し契約をしたことが報告され承認された。

2) IdM における共通本人認証基盤の検討状況報告

「SAML 技術による SSO 機能の実現方法の検討内容」について検討状況のご報告と今後進め方の提案がされた。前年度開発内容、SAML 技術を含んだ OSS、トラストサークルの考え方、WSO2 Identity Server を用いた SAML 技術による SSO システム構成案について説明され承認された。

次に委託調査として実施している「応用システムへの組み込みのためのセキュリティ機能の調査研究内容」について、検討状況の報告と今後進め方の提案がされた。OpenID を用いた処理の流れとして、(案 1) 端末生体認証＋パスワード送信、(案 2) 端末生体認証＋認証結果送信、(案 3) 端末生体認証＋ACBio 送信、(案 4) サーバ生体認証、(案 5) ACBio つきサーバ生体認証の 5 案について説明され、これ以外の構成が考えられる場合は、提案元の委員までご連絡いただくことが各委員に要請された。

3) 委託調査計画について

バイオ IdM 本人共通認証基盤事業における委託調査計画が説明された。審議の結果、提案内容にしたがって進めることが承認された。

①委託調査は次の 4 項目を行う予定であり、被災者支援システムの開発元とコンタクトしながら具体的なシステムを念頭に置いた調査を考えているとの報告がされた。

－初期調査

－セキュリティ技術調査

－応用システム調査

－応用システム向けセキュリティ研究

③第 3 回検討委員会　平成 25 年 12 月 18 日(水)　　10:00～12:00

1) Biometrics exhibition and conference 2013 調査報告

委員会より委託されて出張、調査した英国バイオメトリクス 2013 の報告がされた。

2) IdM における共通本人認証基盤の検討状況報告

バイオ IdM 共通本人認証基盤システムの検討状況として以下の報告と今後進め方が提案され、確認の上、承認された。

①セキュリティ機能の実装方針

以下の 3 つのステップを基本方針として IdM 共通本人認証基盤へのセキュリティ機能の検討をした内容が報告された。

ステップ 1： 「被災者支援システム」を想定アプリケーションする。生体認証機能は、補助的なサービスに限定する

ステップ 2： 補助的なサービスに限定することにより、電子認証システムにおける保証レベルを 2 とする

ステップ 3： 生体認証技術はパスワードのロック解除のために用いる

②セキュリティ機能の実装について

セキュリティ実装対象として、「WSO2 Identity Server を用いた OpenID システム構成」が提示されセキュリティの検討対象となる部分が明示された。

また、セキュリティ機能の実装として、OSS の選択、格納データのセキュリティおよび通信データのセキュリティ部分に対する検討内容が報告された。

③ 応用システムの検討状況

応用システムの機能検討の結果、被災者の個別ニーズと支援物資との引き合わせと引渡しの機能を緊急物資管理システムに追加する機能があると考えている。その内容について被災者支援システムの開発元に訪問して機能について提案しお考えを伺った内容の報告があった。伺ったご意見をもとに機能の検討をさらに加えて、内容の詰めを行う予定であることも報告された。

3) 委託調査状況報告

本事業の検討成果の適用先として「災害支援システムへの適用」という仮説の検証のため、被災者支援システムの開発元と情報交換した内容が報告された。

① 生体認証の活用場所の案として説明した「個々人の生体認証を入手、その方の特定要望を緊急物資管理につなげるシステムの構築」は被災弱者の救済というよりぜいたく品の支給というイメージがある。それよりも優先順位は、避難所での生体認証の活用にあるとのご意見をただいた。

避難所での被災者登録や物資の受け渡しは現状手作業であるが、この部分に生体認証が活用できれば避難所での支援物資の管理の効率化や簡略化など、効果があるのではないかとのご意見もいただいた。

② 生体認証の活用先については、①で述べた避難所の入退所の手続きの簡略化のほかに、同じ入退所の手続きや物資の配布ということを考えると仮設住宅への応用展開も考えられるとのアイディアをいただいた。

4) 成果の共有について

本事業の成果を業界で役立てるため、基本的に被提供者が許諾し、順守することを条件として、成果物提供先の条件を満たす希望者に成果物を提供することにしたいとの事業成果の共有の考え方の案を(一社)日本自動認識システム協会より提示した。委員各社に提示案を持ち帰り、修正等の連絡いただくこととなった。

④第 4 回検討委員会　平成 26 年 2 月 13 日(木)　　13:00～15:00

1) IdM における共通本人認証基盤の検討状況報告

バイオ IdM 共通本人認証基盤システムの検討状況報告として以下の 3 点について検討状況が報告された。

① セキュリティ機能調査研究状況

セキュリティ機能の実装について WebSocket に関して OSS 調査とシステムのサーバおよびクライント内の格納データのセキュリティ実装(暗号化)について確認した。

② 検証実験状況

作業中（40%完了：957 項目中 380 項目を実施済み)。実験項目、システム構成、標準構成試験結果と簡易構成試験結果、ならびに OpenID との比較した結果が報告された。

③ 応用システムの検討

被災者支援システムの開発元が開発している被災者支援システムへの応用について、意見交換を踏まえて実施検被災者支援機能の方向性として考えられる利用シーンとして、次の 3 つと考えられることが報告された。

- 避難所にて、支援物資支給時に被災者が生体認証で本人確認することにより、支援物資の効率的な配布を実現する。
- 避難所にて、支援物資に関する被災者からの個別ニーズに対応する際、要望のあった特定の支援物資の確実な受け渡しのために生体認証を用いる。
- 仮設住宅における入居・退去管理に生体認証を用いる。

また、今後のアクションとして、被災者支援システムの開発元との情報交換を継続し、以下の検討を進めることが提案された。

- 被災地からの情報収集
- 実現すべき機能の選定
- 被災者支援システムへの BioIDM システムの組み込み
- 実証実験などによる有効性の検証

2) 成果の共有について

第 3 回委員会にて提示した「成果の共有について」に関して意見交換後、産業界の振興のために提供するという基本的な方針が承認された。ただし、実際に進める時は、今回の意見を踏まえて、今回の事業の実施者である(一社)日本自動認識システム協会で実際の状況に合わせて契約条件等をより明確化・具体化し、委員であったメンバの意見も聞きながら進めることとなった。

(2) 市場動向調査

英国 Biometrics Exhibition and Conference 2013(BC2013)の参加者は、約 100 名で、展示は約 40 社であった。米国 BCC の内容は、安全保障関係が多いが、本カンファレンスは単品製品、IdM をイメージした展示がされているのが印象的であった。なお、参加人数、展示は、ここ数年減少傾向にあると感じられた。

展示には特記すべき事項はなかった。製品の成熟度があがり、新規製品はないためであると思える。

IdM に関しては、そのものの発表はなかったが、キーワードから類推するに、現状の OpenID などのトラストフレームワークに個人が加わる際にモバイル端末を利用すること、つまり、現状のトラストフレームワークにバイオメトリクスをうまく実装するためには、モバイルへの実装が正解であり、トラストフレームワークをより強化する形での実装が有効との考え方が正しいと思えた。

今回の調査対象である IdM 関係に該当する講演は 4 件あった。

① Online biometric identity assurance (Mobile Biometrics セッション)

発表者:Clive Bourke, Regional Vice President Sales – EMEA and APAC, Daon, Ireland

内容: US National Strategic for Trust Identiy NSTIC や NSTIC で検討している IdP RP AP　Trust framework ATP の概要の紹介。

② Identity Assurance – A vital component of the Information Assurance jigsaw

発表者: Martin George, CEO, Smart Sensors Ltd, UK

内容: モバイル利用のキーは「デバイス認証」「コミュニケーションチャネル認証」「remote sensor 認証」の 3 つである。

③ Smart mobile identity: Smartphone technology's position with biometric identity verification

発表者: huck Yort, VP and General Manager, Identity Solutions, AOptix, USA

内容: Smart mobile 市場は成長している。また、Application /Easy of use などが重要という発表。

④ Mobile biometrics - Empowering people

発表者: John Adye, Chairman, Identity Assurance Systems Ltd, UK

内容: インターネット上での認証の安全性を向上するにはバイオメトリック認証を利用したモバイル端末が必要であるとの発表。

(3) 応用システムへの組み込みのためのセキュリティ機能の調査研究

応用システムに IdM 共通バイオメトリック認証基盤を適用した場合の、共通バイオメトリック認証基盤へのセキュリティ機能の組み込み方法に関して調査研究を行った。研究にあたっては、以下の 3 つの調査・研究を実施した。

①共通バイオメトリック認証基盤におけるセキュリティ対象データの調査

②応用アプリケーションの選定とアプリケーションの機能の調査・検討

③共通バイオメトリック認証基盤への実装が必要になるセキュリティ機能の調査・検討

それぞれの項目における調査・検討結果を以下に示す。

① 共通バイオメトリック認証基盤におけるセキュリティ対象データの調査

OpenID や SAML 技術による SSO システムの本人認証を共通バイオメトリック認証基盤で実現する際の実現方式として以下の 5 つの方式を整理した。

- 実現方式 1：端末から BP へのパスワードの送信（端末でのバイオメトリック認証）
- 実現方式 2：端末から BP への認証結果の送信（端末でのバイオメトリック認証）
- 実現方式 3：端末から BP への認証結果と ACBio 情報の送信（端末でのバイオメトリック認証）
- 実現方式 4：端末から BP への生体情報の送信（サーバでのバイオメトリック認証）
- 実現方式 5：端末から BP への生体情報と ACBio 情報の送信（サーバでのバイオメトリック認証）

続いて、各方式において本人認証のために取り扱う情報を、コンピュータのハードディスクなどの記憶域に保存する格納データと、ネットワーク上を流れる通信データに分類し、実現方式毎にデータ内容を整理した。

② 応用アプリケーションの選定とアプリケーションの機能の調査・検討

応用アプリケーションの候補として、西宮市情報センターが開発・管理を行っている被災者支援システムを取り上げ、調査検討を行った。検討の具体化においては、西宮市情報センターを訪問し、被災者支援の目的で生体認証を用いる可能性について意見交換を行った。

結果として、所持するタイプの ID を失った被災者が避難所で緊急物資の支援を受ける際に、効率よく迅速・的確に物資を供給するための本人確認として用途が考えられるとの結論になった。これとあわせて、仮設住宅における入居・退居管理における本人確認においても有効性がある可能性があることがわかった。

③ 共通バイオメトリック認証基盤への実装が必要になるセキュリティ機能の調査・検討

電子認証システムにおけるセキュリティ機能について述べている NIST SP 800-63 の考え方に沿って検討することとし、上記①でまとめたセキュリティ対象データを上記②でまとめた応用アプリケーションに適用した場合に必要となるセキュリティ技術を適用することとした。

緊急支援物資の支給のための本人確認用途を、NIST SP 800-63 における保証レベル 2 に設定し、レベル 2 を満足するセキュリティ技術を検討した。共通バイオメトリック認証基盤の実現方式として、最も一般的と考えられる実現方式 1（端末から BP へのパスワードの送信）を例に端末、OP および BP において取り扱う暗号化対象データの種類、暗号アルゴリズム、鍵管理方法、鍵ファイルの保護方法を検討した。あわせて、バイオメトリック認証システムのためのセキュリティ技術として東芝ソリューション株式会社が開発および国際規格化を推進した ACBio についても、共通バイオメトリック認証基盤の組み込み方法に関する基本検討を行った。

(4) IdM 共通本人認証基盤の機能強化のための開発研究

共通バイオメトリック認証基盤の機能強化のための開発として、開発内容および各開発項目に対する検証実験の内容について述べた。機能強化のための開発として、まず開発方針の検討を行った。過去 2 年間の開発研究において、追加の開発が必要と思われる項目として以下の 3 つを選択した。

① SAML 技術対応：前年度までに対応した OpenID に加えて SAML 技術での SSO をサポートする。

② 複数モダリティサポート：前年度までに対応した指静脈装置に加え、複数モダリティのサポートとして指紋認証装置をサポートする。

③ セキュリティ機能：応用システムへの組み込みのためのセキュリティ機能の調査研究において検討されたセキュリティ機能を実現する。

本開発方針に基づいて共通バイオメトリック認証基盤の機能強化のための開発を行い、プロトタイプの開発を完了した。

つづいて、開発したプロトタイプの機能の妥当性を検証するための検証実験を行った。実験にあたっては共通バイオメトリック認証基盤の機能を以下の 6 つに分類し、それぞれに実験項目を設けて検証し、妥当性を確認した。

① 登録機能および認証機能

② シングルサインオン機能

③ 複数モダリティサポート機能

④ セキュリティ機能

⑤ システム構成のバリエーション

⑥ 認証性能

4.5　次年度以降に向けての課題

具体的な応用システムとして被災者支援システムを取り上げて検討を行ったが、実際の適用にあたっては東日本大震災や阪神淡路大震災に代表される被災地において実際に被災を受けた方々からのご意見をいただく必要がある。

本事業を継続した場合の活動として、応用システムを被災者支援システムとした場合の次年度以降にすべき活動内容を以下に示す。

① 東日本大震災や阪神淡路大震災など、大規模自然災害の被災者の方々からの情報収集

② 上記①で収集した情報を反映した被災者支援システムへの生体認証機能の組み込みのための開発

③ 上記②で開発したシステムの有効性の検証として被災自治体と連携した実証実験の実施

5. 平成25年度開発研究の詳細

5.1 市場動向調査

バイオメトリック認証技術を用いた本人認証技術について、本事業にて平成 24 年度の Biometrics2012 の調査を行った調査結果を見ると Biometrics2012 のコンテンツが低調であったが、今年度も同様の状況が続く場合、市場傾向が明確になると考えられたため、定点観測の必要性を認め、英国 ロンドンで開催された Biometrics 2013 で技術と市場の動向を調査した。

以下に調査結果を示す。

1. 調査対象：Biometrics exhibition and conference 2012
2. 日程： 平成 25 年 10 月 15 日−17 日
3. 場所： QEII カンファレンスセンター（ロンドン）
4. 概要：

・カンファレンス参加者約 100 名、展示約 40 社（NEC、日立がメインスポンサー、他に crossmatch、Cognitec、CredenceID、展示は富士通も出展)、米国 BCC は安全保障関係が多いが、このカンファレンスは単品製品、IdM をイメージした展示が印象的であった。

・昨年に比べ発表内容に IdM、Mobile、Big data などが含まれるようになり、セッションタイトルは魅力的になったと感じた。

・展示は特記すべき事項はなかった。製品の成熟度があがったが、新規製品はなかった。富士通は自社薄型モバイル PC に手のひら静脈装置を実装した製品を参考出展していた。日立は指静脈＋指紋のマルチモーダル型装置を出展していた。以前の展示物より、小型化された装置であった。

・今回の一番の調査対象である IdM 関係に該当する講演テーマは 4 件であった。

以下、関係する発表に関し概要を示す。

（1）Online biometric identity assurance

①発表者:Clive Bourke, Regional Vice President Sales – EMEA and APAC, Daon, Ireland

②内容: ・US National Strategic for Trust Identiy NSTIC の概要の紹介。

行政サービスやビジネスにおいてネットで個人認証しているが、効率的でない。効率的な Identity システムが必要である。民間分野は Id エコシステムをすでに構築運営しリードしている。

・NSTIC で検討している IdP RP AP Trust framework ATP の紹介

この話自体は特に目新しいものではなかった。

世界の公的な IdM としては、US：NSTIC、UK:Cabinet office GDS Identity Pro

Framework がある。

Daon 社が NSTIC に大きく貢献している。現在 ARPA/Major Bank/Purdue Univ./Paypal などと協力して開発を行っている。

Biometric を IdM に考慮するうえで SP800-63 モデルは重要である。

US NSTIC パイロットプロジェクトは、多要素認証を採用（GPS、PIN、Biometrics）している。

③感想: NSTIC は SP800-63 モデルを参考に多要素認証方式で Id エコシステムを構築しているとの印象を持った。ここで重要なのは、民間分野が進み、官として遅れをとっているという認識が米国政府にあり、民間の Open ID のような trust framework 上に構築することを考えているようであることである。あくまでもバイオメトリクスはモバイル端末認証の位置づけである。したがって、多要素認証のなかでいかにバイオメトリクスモデルを構築するかが今後重要となると考えられる。

（2）Identity Assurance – A vital component of the Information Assurance jigsaw

①発表者:Martin George, CEO, Smart Sensors Ltd, UK

②内容: モバイル利用には次の３つのキーがある。

・デバイス認証

・コミュニケーションチャネル認証

・Remote Sensor 認証

これらを実装する trust framework model Identity Provider Model が必要。またバイオメトリック実施をセキュアにすることも重要である。下記のキーワードが示された。

・Revocable

・Secure

・No release of PII

・Robust

また、バイオ暗号やクレデンシャルなどの方式も重要である。

③感想: Online biometric identity assurance と同様に多要素認証やベースとなる trust framework が重要であり、そして、実装するバイオメトリック自身の信頼性を高めることが重要であることを主張していた。要するに、OpenID のような Trustframework と、モバイル端末による多要素認証＋バイオメトリクスの必要性の明確化と、バイオメトリクス自身をセキュアにする技術、例えば ACbio やバイオ暗号が必要であるということである。これらが、バイオメトリック IdM に必要なものであると再確認できた。

（3）Smart mobile identity: Smartphone technology's position with biometric identity verification

①発表者: Chuck Yort, VP and General Manager, Identity Solutions, AOptix, USA

②内容: Smart mobile 市場は成長している。Application /Easy of use などが重要との発表。

（4）Mobile biometrics - Empowering people

①発表者: ohn Adye, Chairman, Identity Assurance Systems Ltd, UK

②内容: インターネット上での認証の危険性。安全性を向上するにはバイオメトリック認証を利用したモバイル端末が必要であるとの発表。

5. まとめ

・昨年に比べ発表内容に IdM、Mobile、Big data などが含まれるようになり、セッションタイトルは魅力的になったと感じたが、内容として、技術論、実施プロジェクト紹介ではなく、状況紹介的、計画的な発表がほとんどであったのが残念であった。

この意味で欧米と比べ、日本のベンダ技術が劣っているわけではないと実感した。日本がもっと発信力を高めること、ならびに未開拓の社会 ID 的製品で海外市場を狙うことが日本にとっての急務と感じた。

・IdM に関して、具体的な技術に関する発表はなかったが、キーワードから類推するに、以下のことが今後重要であると考える。

－現状の OpenID などのトラストフレームワークに個人が加わる際、モバイル端末を利用する。つまり、現状のトラストフレームワークにバイオメトリクスをうまく適用するためには、モバイルへの実装が正解であり、トラストフレームワークをより強化する形での実装が有効と考える。つまり、デファクトであろうがデジュールであろうが標準準拠が重要であり、バイオメトリクス実装の信頼性を確保するために ACbio の利用が適切と考える。

・米国の政府でのプロジェクトである NSTIC の動きのウオッチは重要であるが、関係者は民間での IdM エコシステムの実装が進んでいるとのことで、どのようにこれを公的システムに取り込むかというような発言が見受けられた。

・新市場に関しては特に大きな話題はなかったが、やはり Data-Centric なビジネスを欧米は意識しているようであり、長崎大学が対応しているアフリカなどでの health 関係の話があった。内容はガーナの病院事例であった。病院内での認証が重要とのこと。新興国市場は重要なターゲットであることを改めて認識した。

・バイオメトリックの市場展開には次の３点が重要であり、また、新興国市場をどのように参入するかがポイントと考えられる。

(1) Big Data の中でのバイオメトリクスの位置づけを明確化

(2) IdM フレームワークでのバイオメトリック技術の位置づけを明確化

(3) アプリを考慮したモバイル実装を行う

5.2 応用システムへの組み込みのためのセキュリティ機能の調査研究

5.2.1 概要

本 5.2 節では、共通バイオメトリック認証基盤プロトタイプへの組み込みが必要と考えられる、バイオメトリックデータの保護を中心としたセキュリティ機能について調査した結果を示す。

5.2.2 調査・検討手順

IdM 共通バイオメトリック認証基盤にセキュリティ機能を組み込むにあたっての調査・検討は、以下の手順で進めることとした。

① 共通バイオメトリック認証基盤におけるセキュリティ対象データの調査
② 応用アプリケーションの選定とアプリケーションの機能の調査・検討
③ 共通バイオメトリック認証基盤への実装が必要になるセキュリティ機能の調査・検討

以下に各手順の内容について説明する。

①共通バイオメトリック認証基盤におけるセキュリティ対象データの調査

BioIDM プロトタイプシステムを構成する各コンポーネントにおいて、本人認証のために用いられる格納データおよび各ネットワークノード間でやり取りされる通信データを抽出する。これらのデータ項目がセキュリティ技術を適用する検討対象となる。

② 応用アプリケーションの選定とアプリケーションの機能の調査・検討

セキュリティ機能を実装するにあたって具体的なアプリケーションを選定する。本事業における前年度の研究により、地震や津波などの天災により所持するタイプの ID を紛失した被災者を、生体認証機能を用いた本人認証機能により支援する応用方法が検討された。これを受けて、本調査では被災者を支援する具体的な応用アプリケーションの有無およびその機能について調査を行う。

③ 共通バイオメトリック認証基盤への実装が必要になるセキュリティ機能の調査・検討

上記②の調査・検討ののち、選定されたアプリケーションにおける共通バイオメトリック認証基盤の用途において必要となるセキュリティ機能を検討する。この際、上記①で示した共通バイオメトリック認証基盤においてセキュリティの対象となるデータ項目に対して、電子認証システムにおける本人認証の保証レベルや必要なセキュリティ技術を示す文書である NIST SP 800-63 の考え方を適用する。あわせて、バイオメトリック認証システムのためのセキュリティ機能である ACBio の組み込みについて基本検討を行う。

5.2.3 調査・検討結果

本節では、5.2.2 節で示した調査・検討手順にしたがって、セキュリティ機能に関する調査・検討を行った結果を示す。

(1) 共通バイオメトリック認証基盤におけるセキュリティ対象データの調査

本項では共通バイオメトリック認証基盤においてセキュリティ技術の適用対象になると考えられるデータ項目について調査した。共通バイオメトリック認証基盤を用いた生体認証方式の一つとして、端末において生体認証を行った結果としてパスワードを有効化する方式を図 5.1 に示す。

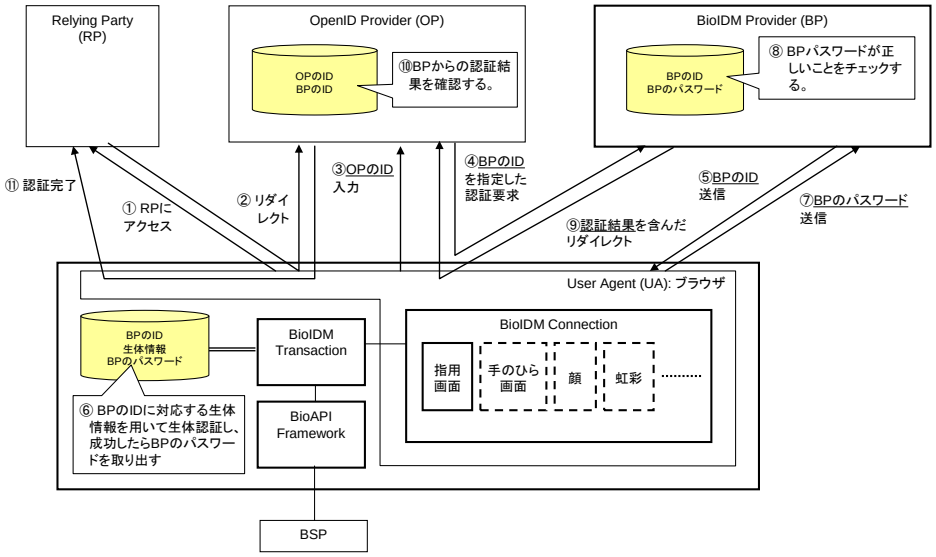


図 5.1　実現方式 1（端末から BP へのパスワードの送信）

本図に示すとおり、共通バイオメトリック認証基盤は 4 つのネットワークノードにより構成される。本図において、Relying Party（RP と略す）、OpenID Provider（OP と略す）、User Agent（UA と略す）の 3 つは OpenID における基本的な構成要素であり、BioIDM Provider（BP と略す）は共通バイオメトリック認証基盤の検討結果により追加された構成要素である。なお、UA は端末内で動作するブラウザのことである。

共通バイオメトリック認証基盤では UA 内に BioIDM Connection と呼ばれるプログラムがブラウザ内で動作する。また、端末内に BioIDM Transaction と呼ばれるプログラムが存在し、BioIDM Connection と連動して生体認証機能を実現する。BioIDM Transaction は下位モジュールとして BioAPI Framework を呼び出し、BioAPI Framework は生体認証ベンダが開発・提供する BSP (Biometric Service Provider)を呼び出す。BioIDM Transaction は、本プロトタイプにおいては生体情報や ID などの各種情報を端末内の記憶域から読み込む（他の実装形態として IC カードなどから読み込む方法も実現可能である）。本図では①から⑪までの番号で、利用者が

RP にアクセスをリクエストしてから RP に本人認証の完了が通知されるまでの一連の処理の流れが示されている。また、セキュリティの対象となるデータとして格納データを黄色のディスクの絵で、通信データをアンダーラインで示している。本図において、バイオメトリクスを用いたシングルサインオンを実現するために追加された情報を取り扱う構成要素である OP、BP、UA、BioIDM Transaction の 4 つにおいて何らかの共通バイオメトリック認証基盤としてのセキュリティ機能の組み込みが必要となる。

次に本図における本人認証処理について説明する。端末内の記憶域に生体情報と BP で用いられるユーザのパスワードを保持し、図中の⑥で示すとおり、端末上で実行される生体認証において認証が成功した場合、BioIDM Transaction が BP のパスワードを取り出す。そして図中の⑦のとおり、取り出された BP のパスワードが BP に送信され、⑧で示されるとおり BP 内でパスワードを用いた本人認証を行う。

共通バイオメトリック認証基盤における認証処理には図 5.1 以外にも様々な方式が考えられる。以降の図 5.2 から図 5.5 までに主な方式を順次示す。

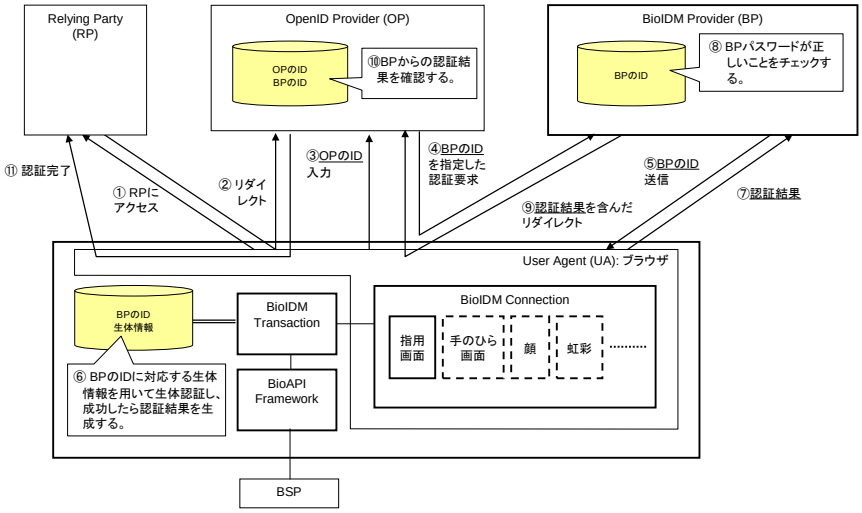


図 5.2　実現方式 2（端末から BP への認証結果の送信）

図 5.2 の図 5.1 との違いは、生体認証を端末内の BioIDM Transaction が実施したあと、生体認証結果である認証成功あるいは認証失敗という認証結果情報を BP に送信する点である。具体的には、図中⑥において生体認証が成功（あるいは失敗）したのち、図 5.1 で示したユーザの BP でのパスワードを取り出す代わりに、認証結果を BP に送信している。この結果 BP は、本人認証結果を認証成功あるいは認証失敗のビット情報で判定する。

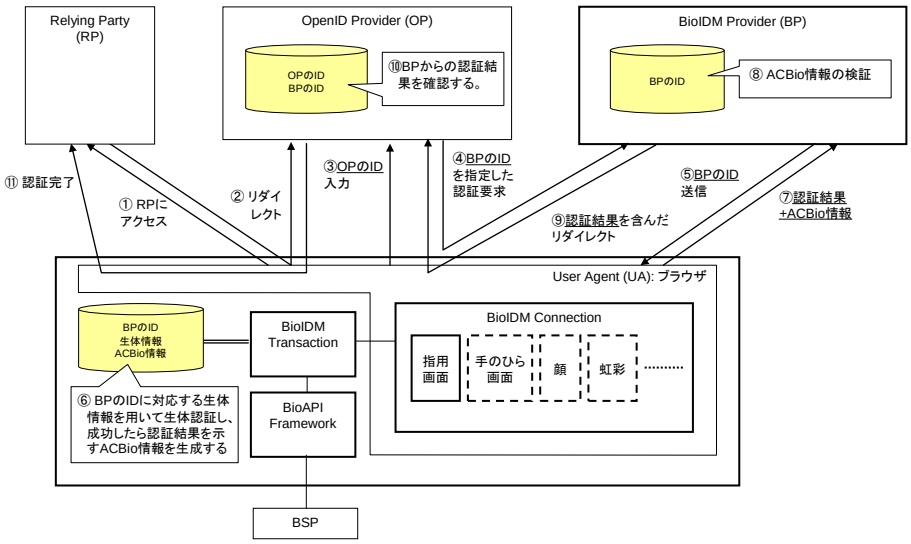


図 5.3　実現方式 3（端末から BP への認証結果と ACBio 情報の送信）

図 5.3 は端末上での生体認証結果を ACBio 情報で検証する機能を付加したものである。本方式では生体認証を端末内で実施したあと、生体認証結果とともにその内容の信頼性を向上させる ACBio 情報を生成し BP に送信する。具体的には、図中⑥において生体認証が成功したのち、図 5.1 で示したユーザの BP でのパスワードを取り出す代わりに、BioIDM Transaction 内で ACBio 情報を生成し、BP に送信する。この結果 BP は、認証結果の信頼性を ACBio 情報に基づいて検証することが可能となる。

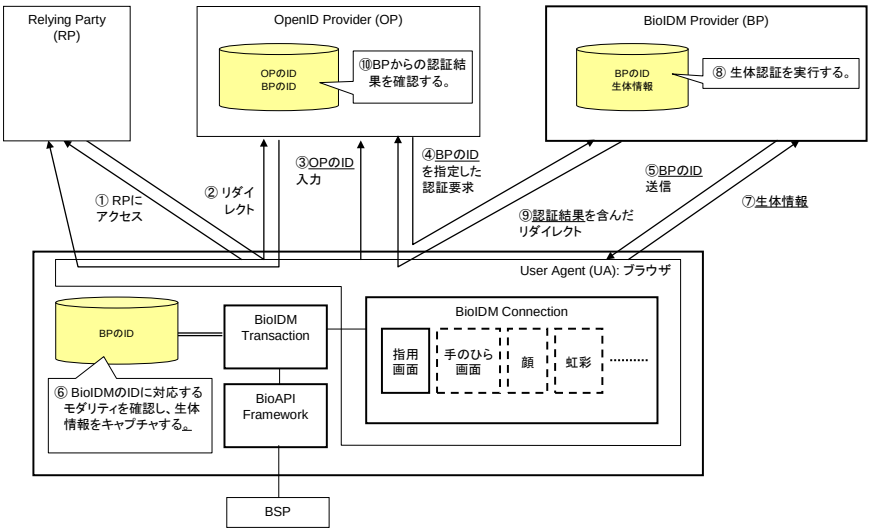


図 5.4　実現方式 4（端末から BP への生体情報の送信（サーバ認証））

図 5.4 は、BioIDM Transaction が取得した生体情報を BP に送信してサーバ認証する方式である。具体的には、図中⑥において生体情報を取得したのち、その生体情報を BP に送信し、BP 内に保存されている生体情報（登録テンプレート）と照合する。

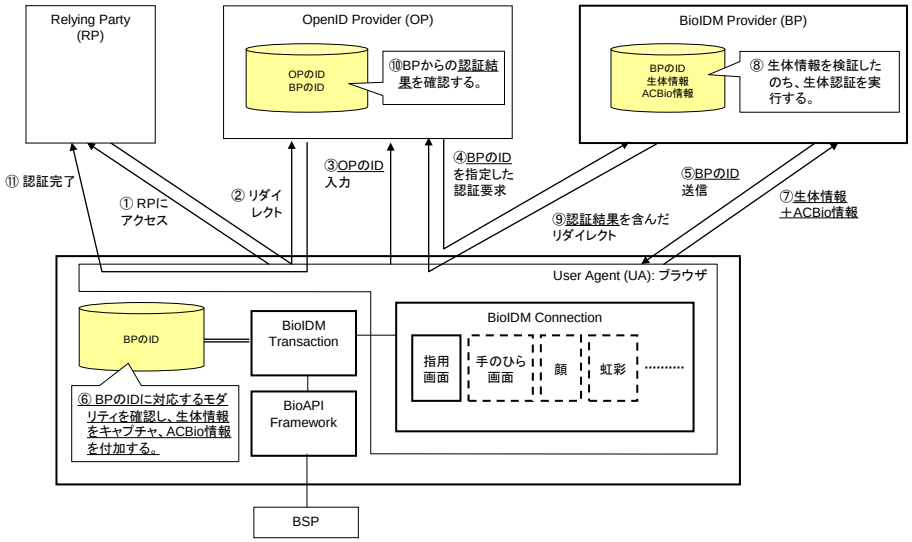


図 5.5　実現方式 5（端末から BP への生体情報と ACBio 情報の送信（サーバ認証））

図 5.5 では、端末内で取得した生体情報を BP に送信してサーバ認証する際に ACBio 情報を付加する方式である。具体的には、図中⑥において生体情報を取得したのち、その生体情報の信頼性を向上する ACBio 情報を生成し、生体情報に ACBio 情報を付加して BP に送信し、BP 内に保存されている登録テンプレートと照合する。この結果 BP は、UA から送信された生体情報を ACBio 情報に基づいて検証することが可能となる。

以上図 5.1 から図 5.5 までで共通バイオメトリック認証基盤における主な本人認証方式を示した。共通バイオメトリック認証基盤におけるセキュリティ対象データをまとめるにあたり、セキュリティの対象となるデータを以下の 2 種類に分類することとする。

① 格納データ： 端末やサーバのディスク内に保存されるデータ

② 通信データ： 端末やサーバ間でやり取りされる通信回線を流れるデータ

次頁において、格納データの項目を表 5.1、通信データの項目を表 5.2 にそれぞれまとめる。

表 5.1　BioIDM システムにおける格納データ項目

No	項目	OP	BP	端末 （BioIDM Transaction）
1	実現方式 1 （端末から BP へのパスワードの送信）	OP の ID BP の ID	BP の ID BP のパスワード	BP の ID 生体情報 BP のパスワード
2	実現方式 2 （認証結果情報の送信）	同上	BP の ID	BP の ID 生体情報
3	実現方式 3 （認証結果情報を ACBio で保証）	同上	同上	BP の ID 生体情報 ACBio 情報
4	実現方式 4 （サーバ認証）	同上	BP の ID 生体情報	BP の ID
5	実現方式 5 （サーバ認証に ACBio 情報を追加）	同上	BP の ID 生体情報 ACBio 情報	同上

表 5.2　BioIDM システムにおける通信データ項目

No	項目	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩	⑪
		UA-RP	RP-UA -OP	OP-UA	OP-UA -BP	BP-UA	UA	UA-BP	BP	BP-UA -OP	OP	OP-UA -RP
1	実現方式 1 （生体認証によるパスワード有効化）	OP の URL	－	OP の ID	BP の URL BP の ID	BP の ID	－	パスワード	－	認証結果	－	認証結果
2	実現方式 2 （認証結果情報の送信）	同上	－	同上	同上	同上	－	認証結果	－	同上	－	同上
3	実現方式 3 （認証結果情報を ACBio で保証）	同上	－	同上	同上	同上	－	認証結果 ＋ACBio	－	同上	－	同上
4	実現方式 4 （サーバ認証）	同上	－	同上	同上	同上	－	生体情報	－	同上	－	同上
5	実現方式 5 （サーバ認証に ACBio 情報を追加）	同上	－	同上	同上	同上	－	生体情報 ＋ACBio	－	同上	－	同上

以上本項では、共通バイオメトリック認証基盤におけるセキュリティ対象データの調査として、共通バイオメトリック認証基盤として考えられる本人認証方式ごとに、格納データと通信データの 2 種類に対象データを分類したうえで、対象データ項目を表として整理した。

(2) 応用アプリケーションの選定とアプリケーションの機能の調査

本項では共通バイオメトリック認証基盤を適用可能な応用アプリケーションについて調査するとともに、共通バイオメトリック認証基盤を応用アプリケーション内で用いた場合に想定される機能についての調査および検討を行った内容について述べる。

なお、前年度（平成 24 年度）の共通バイオメトリック認証基盤事業において、応用アプリケーションの候補として、被災者支援を目的としたシステムが検討されていた。今年度事業における応用システムのより具体的な検討として、被災者支援を目的とした実際のシステムの有無を調査し、該当するシステムへの共通バイオメトリック認証基盤の適用方法を検討した。

①前年度検討内容

前年度に検討された被災者支援を目的とした想定システム構成図を図 5.6 に示す。本図は、被災地において仮に設置された市役所内に OP と BP が立ち上がり、これらのサーバに対して市役所やその他支援を行う組織内の RP からアクセスを行うことにより、生体認証を用いた被災者支援を行える可能性があることを示したものである。

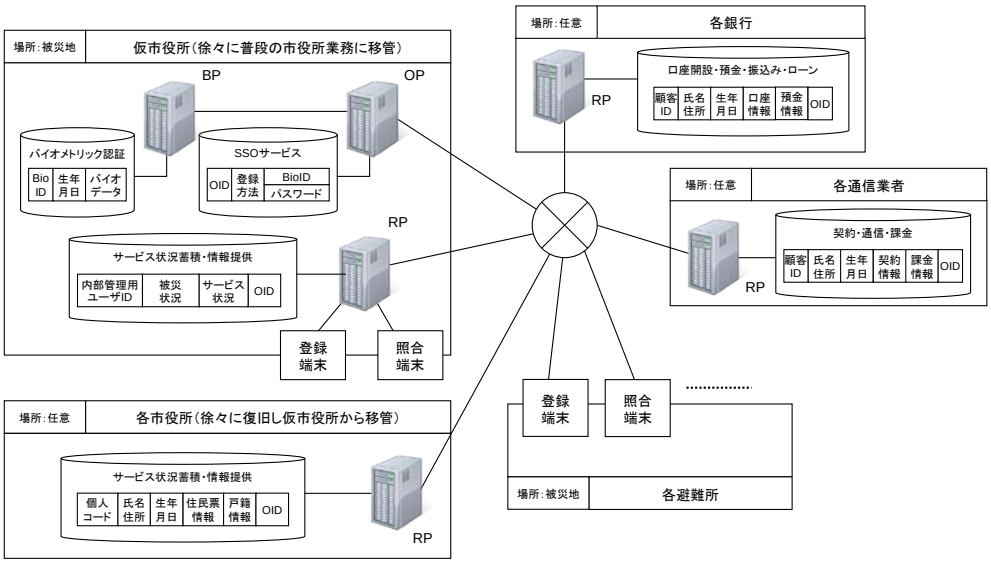


図 5.6　被災者支援を目的とした応用システム想定図（平成 24 年度作成）

②開発実績のある被災者支援システムに関する調査

インターネットを用いて国内で開発実績のある被災者支援システムについて調査を行ったところ、一般財団法人西宮市都市整備公社が運営管理する西宮市情報センターが開発・管理を行っている被災者支援システムが存在することが判明した。以下にシステムの概要を示す。

1) 西宮市情報センターの被災者支援システム概要

①概要

- 1995 年 1 月 17 日の阪神淡路大震災の直後、西宮市電算システムの復旧と同時に被災者支援システムの開発に着手し、市職員自らが開発を行い迅速なシステム立ち上げを果たしたことから始まった。
- 継続的なバージョンアップが続けられ、現在も一部の地方自治体などで運用されている。広く国内の自治体での活用を図るため、オープンソース化し自治体向けだけでなく、自治体以外の組織・企業にも公開している。

②主な機能

- 被災者の属性情報を管理する「被災者台帳」、被害を受けた家屋属性情報を管理する「被災家屋台帳」の２つの台帳管理機能を持ち、被災者の状況や家屋被害状況を記録し、更新する。
- 被災者への「り災証明書」、被災家屋の所有者への「被災家屋証明書」の発行をはじめ、様々な義援金の給付や生活支援金の貸付管理など、各種支援制度の管理機能を持つ。
- 証明書は各自治体の独自様式に対応し、自由設計が可能である。自治体による上乗せ給付など、自治体毎の独自メニューの登録が可能である。
- 被害状況の集計など、基礎的な統計情報の印刷、CSV 形式によるデータ出力機能が可能であり、支援関連データの加工、分析ができる。

2) 西宮市情報センター訪問調査

以上のインターネット上での調査結果を踏まえ、さらなる詳細調査および検討にあたっては、被災者支援システムの開発及びメンテナンスを行っている西宮市情報センターを訪問し、情報収集及び意見交換を行うこととした。以下に西宮市情報センター訪問結果を示す。

① 第 1 回訪問

1) 概要

－訪問日：平成 25 年 9 月 9 日

－目的：

共通バイオメトリック認証基盤の開発研究の検討成果の適用候補として考えられている被災者支援システムの適用可能性について情報交換と協力要請を西宮市情報センターに実施する。具体的な目的は以下のとおりである。

・西宮市災害支援システムの構築の背景や基本理念の理解

・生体認証アイデンティティ管理（BioIDM）システムを用いた大震災被災者救済の可能性についての意見交換

・今後の情報のご提供や打合せ等の協力要請

－場所： 西宮市情報センター（兵庫県西宮市）

－参加者：

「被災者支援システム」全国サポートセンター（運営主体：西宮市情報センター）

センター長　　吉田　稔　殿

(一社)日本自動認識システム協会　　酒井　康夫

(株)OKI ソフトウェア　中村　敏男

(財)ひょうご産学官連携コーディネーター 中嶋 晴久　殿

（西宮市情報センターとの会議の調整をしていただいた。）

2) 打合せ結果

(a) 被災者支援への生体認証の活用を、特定のベンダに依存することなくオープンな形で推進するという共通認証基盤プロジェクトの主旨についてご理解いただき、本プロジェクトとの連携ついて前向きな感触を得ることができた。

(b) 災害支援システムの検討にあたって考慮すべき点について知見が得られた。

・生体認証適用を被災者の視点で捉え、利益を求めないスタンスが重要である。

・生体認証の適用が有効な場所として避難所が考えられること、など

(c) 各種団体やベンダ等から被災者支援システムへのバイオメトリクス連携についてコラボレーションの問い合わせが多数あるとのこと。

② 第 2 回訪問

1) 概要

－訪問日：平成 25 年 11 月 22 日

－目的：

9 月 9 日に実施した第一回訪問での意見交換結果をもとにして検討した生体認証による本人認証の活用の可能性について意見交換を実施する。

－場所： 西宮市情報センター（兵庫県西宮市）

－参加者：

「被災者支援システム」全国サポートセンター（運営主体：西宮市情報センター）

センター長 吉田 稔 殿

(一社)日本自動認識システム協会 酒井 康夫

(株)OKI ソフトウェア 中村 敏男

(財)ひょうご産学官連携コーディネーター 中嶋 晴久 殿

2) 打合せ結果

① 推進者側説明

第 1 回訪問時の意見交換結果を受けて、推進者側から図 5.7 を用いて生体認証を用いた具体的な被災者支援の実現案を説明した。本図は、避難所においてある程度の期間が経過してから発生する被災者による個別ニーズに対応する際に、個別要望の受付と、要望品の受け渡しのために生体認証を適用する可能性を示したものである。

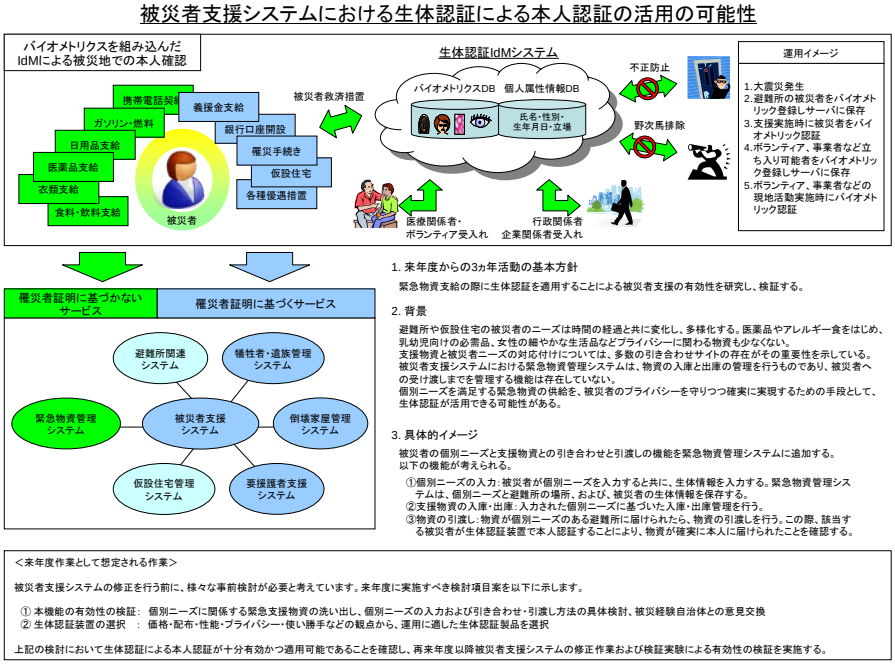


図 5.7 第 1 回訪問時の推進者説明資料

② 意見交換結果

(a) 生体認証の活用場所の優先順位は、案として説明した「生体認証とともに入手する個人個人の特定情報を緊急物資管理システムへ活用するシステムの構築」より、「避難所での活用」が最優先と考えられるとのご意見をただいた。
これは、緊急物資管理は、緊急物資を必要とする場所へ届けるための仕組みであり、避難所の被災者台帳とのリンクも行い、台帳情報をもとに被災弱者対応なども行うようにしているが、一方避難場所での避難者登録や物資の受け渡しは手作業で行っているため、避難所での管理の簡略化が生体認証でできれば、効果があるためとのことである。

(b) 生体認証の活用先については、避難所の入退所の手続きの簡略化もあるが、同じ入退所の手続きや物資の配布ということで考えると「仮設住宅」での応用も考えられるとのアイディアをいただいた。

(c) 義援金の配布は、配布後の管理や混乱回避のために、現金配布は厳禁である。銀行口座経由での配布必須とのこと。したがって、被災後直ぐに銀行口座の開設できるようにすることが大切とのことである。

③ 応用アプリケーションの調査に関する結論

以上述べた西宮市情報センターの被災者支援システムに関する調査および西宮市情報センター訪問による意見交換により、共通バイオメトリック認証基盤の応用アプリケーションとして被災者支援システムへの組み込みについて可能性があることが判明した。理由は以下の 2 点である。

1) 避難所における支援物資支給時の円滑化や効率化に生体認証が貢献できる可能性がある。
2) 具体的なアプリケーションが OSS として存在しており、共通バイオメトリック認証基盤を組み込める可能性がある。

なお、被災者支援システムに共通バイオメトリック認証基盤を適用する場合の具体的な機能として以下の 3 点が考えられることがわかった。

1) 避難所にて、支援物資支給時に被災者が生体認証で本人確認することにより、支援物資の効率的な配布を実現する。
2) 避難所にて、支援物資に関する被災者からの個別ニーズに対応する際、要望のあった特定の支援物資の確実な受け渡しのために生体認証を用いる。
3) 仮設住宅における入居・退去管理に生体認証を用いる。

また、この適用候補のさらなる実現性の検討に向けて、将来的に実施すべき作業項目を以下に示す。

1) 実際に被災に合われた地域の住民の方々からの情報収集・意見交換

2) 情報収集・意見交換の結果を受けた実現機能の選定

3) 被災者支援システムへの BioIDM システムの組み込み

4) 組み込んだ機能に関する実証実験などによる有効性の検証

上記作業の実施にあたっては、西宮市情報センターとの情報交換の継続が重要である。

(3) 共通バイオメトリック認証基盤への実装が必要になるセキュリティ機能の調査・検討

前述の 5.2.3 節(1)および(2)では、それぞれ共通バイオメトリック認証基盤におけるセキュリティ対象データ項目、および、共通バイオメトリック認証基盤の応用システムとして被災者支援システムについての調査・検討結果を示した。本項では、セキュリティ機能の調査として、NIST SP 800-63 の考え方に従った、共通バイオメトリック認証基盤に必要となるセキュリティ機能の調査・検討結果を示す。

① 調査・検討の進め方

本調査・検討は、以下の 3 つの段階で進めることとした。

1) 西宮情報センターの被災者支援システムへの実装機能の特定

応用アプリケーションの候補である西宮市情報センターの被災者支援システムにおける各種機能の中から、共通バイオメトリック認証基盤を用いて本人認証を行う機能を特定する。

2) 電子認証システムにおける保証レベルおよび必要なセキュリティ技術の決定

前述 1)で示した実装機能に基づき、NIST SP 800-63 で示される電子認証システムにおける本人認証の保証レベルを検討し、決定する。これにより、決定した保証レベルに該当する必要なセキュリティ技術が決まる。

3) 実装技術の選択

前述 2)で明らかになった必要なセキュリティ技術より、実際に用いる技術を選択する。

② 調査・検討結果

前述の進め方の手順に沿った調査・検討結果を以下に示す。

1) 西宮情報センターの被災者支援システムへの実装機能の特定

被災者支援システムにおける生体認証機能は、避難所における緊急物資支援の受け渡しや仮設住宅の入居・退去管理など、補助的なサービスとする。被災者の銀行口座アクセスなど金銭管理や、人命に関するサービスは対象外とする。この考え方は、前項の応用アプリケーションの選定とアプリケーションの機能の調査によって得られた結論に基づくものである。

2) 電子認証システムにおける保証レベルおよび必要なセキュリティ技術の決定

NIST SP 800-63 の考え方に基づく保証レベルについては、前述①で示した補助的なサービスに限定することから、レベル 2 を適用することとする。本人認証時の認識エラーが発生した場合の影響や害、および影響度判定について表 5.3 に示す。

表 5.3　保証レベル 2 における認識エラーにより発生する影響や害と影響度判定

認識エラーにより発生する影響や害	影響度判定
不便・苦痛もしくは地位・評判への打撃	中または低
財務上の損失または政府機関の賠償責任	中または低
政府機関の活動計画または公共の利益に対する害	低
機密情報の無許可の公開	低
身の安全	該当なし
民事上または刑事上の法律違反	低

保証レベル 2 において必要となるセキュリティ技術は NIST SP 800-63 に示されている。必要なセキュリティ技術を表 5.4 に示す。

表 5.4　保証レベル 2 に必要なセキュリティ技術

技術項目	必要な技術
トークンの種類	パスワード
必要な保護	オンライン推測、再現、盗聴
パスワード耐性	16384 分の 1
プロトコルの種類	トンネルされたパスワード
その他	検証者または CSP によって第三者に開示されない 共通秘密情報

これは、共通バイオメトリック認証基盤におけるセキュリティ対象データの調査（前述の 5.2.3 節 (1)）で示したセキュリティ対象となるデータ項目（表 5.1 および表 5.2）に対して、表 5.4 で示したセキュリティ技術を適用することを意味する。

3) 実装技術の選択

前述までの検討結果に基づき、共通バイオメトリック認証基盤に組み込むセキュリティ機能についてまとめる。共通バイオメトリック認証基盤には、端末や Web サーバ内にセキュリティが必要な格納データが存在するとともに、端末や Web サーバとの間でやり取りされる通信データに対してもセキュリティが必要である。ここでは、前述の(1)で示した共通バイオメトリック認証基盤におけるセキュリティ対象データ調査で方式案 1 として示された、パスワードを有効化する方式を例にとり説明する。図 5.8 にパスワードを有効化する方式においてセキュリティの対照となる格納データと通信データを示す。また、本図⑦においてパスワードを送信する代わりに、バイオメトリック認証システムのためのセキュリティ機能である ACBio を用いた場合の基本検討として ACBio 情報を送信するケースについても触れる。

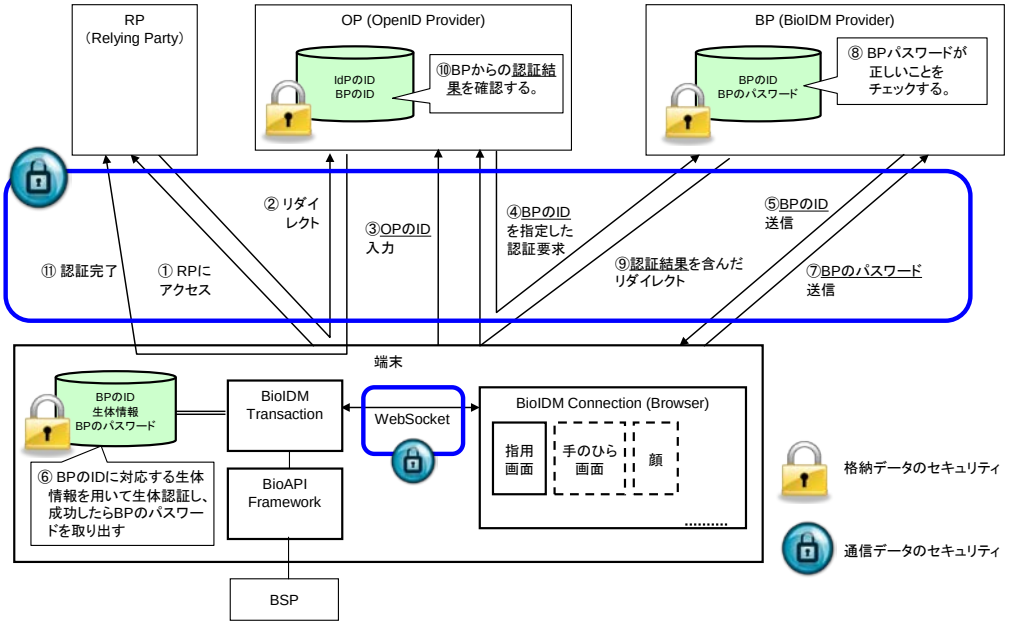


図 5.8　実現方式 1 における格納データと通信データ

本図におけるそれぞれのデータに対するセキュリティ実装案を以下に示す。

- 格納データへのセキュリティ：AES-128 を用いて各データ項目の暗号化を実現する。共通鍵の鍵管理など詳細な実装案について表 5.5 に示す。
- 通信データへのセキュリティ：RP、OP、BP および UA 間の通信については HTTPS を用いる。端末内の BioIDM Connection と BioIDM Transaction の間の通信については、WebSocket SSL を用いることとする。

表 5.5　共通バイオメトリック認証基盤における格納データのセキュリティ技術の実装案詳細

No	項目	端末	OP および BP
1	暗号化対象データ	以下の 3 項目を暗号化する。 ・登録テンプレート ・BP のユーザ ID ・BP のパスワード	サーバプログラムが管理するデータベース全体を暗号化する(1)
2	暗号アルゴリズム	AES-128 を用いる。	同左
3	鍵管理	共通バイオメトリック認証基盤が参照する暗号鍵保存用ファイルに暗号鍵を保存する。	サーバプログラムが参照する暗号鍵保存用ファイル（コンフィグファイル）に暗号鍵を保存する。
4	鍵ファイルの保護	・暗号鍵保存用ファイルに専用ユーザからのアクセス権を設定し、一般ユーザの参照を禁止した。 ・専用ユーザで共通バイオメトリック認証基盤を Windows サービスとして実行する。	・暗号鍵保存用ファイルに特定ユーザからのアクセス権を設定し、他の一般ユーザからの参照を禁止する。 ・サーバプログラム自体を上記特定ユーザで Windows サービスとして実行する。

注）(1) 暗号化対象データに ID が含まれており、クエリ機能の対象になっているため個別に暗号化せず DB 全体を暗号化することとする。

以下に ACBio を用いた場合の基本方式について検討した結果を示す。前述の 5.2.3 節 (1)共通バイオメトリック認証基盤におけるセキュリティ対象データの調査で示した各種実現方式の中で実現方式 3 および 5 では、ACBio が用いられ、認証結果や生体情報の検証機能が実現されている。実現方式 3 において ACBio を組み込む場合、BioIDM Transaction が何らかの ACBio 機能を呼び出す方法が考えられる。また、BioIDM Provider 側では端末から送られた ACBio 情報を検証する機能が必要となる。このような機能を付加したシステム構成のイメージ図を図 5.9 に示す。

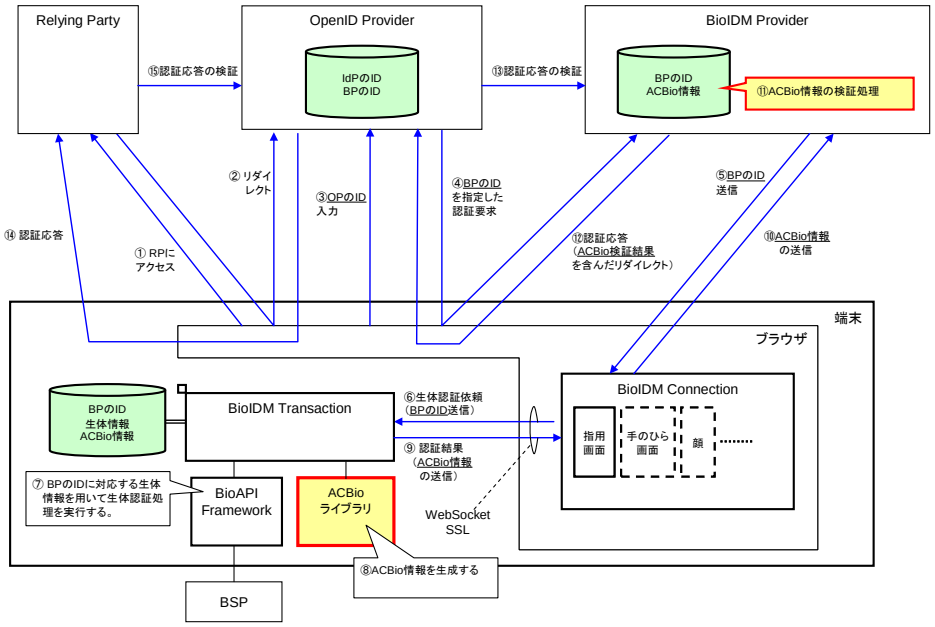


図 5.9　実現方式 3 における ACBio 機能の実装イメージ図

本図において、端末内の ACBio ライブラリは、生体情報の登録時に ACBio 技術における BRT 証明書を生成し、認証時に ACBio 技術における ACBio インスタンスを生成する。BioIDM プロバイダにおける ACBio 情報の検証処理は、認証結果とともに端末から送られた ACBio インスタンスの正しさに関する検証を行う。この際、ACBio 機能の実装可能性については以下の点について留意する必要がある。

・OpenID や SAML など SSO システム、共通バイオメトリック認証基盤システム（BioIDM）、使用する生体認証製品、ACBio といったそれぞれの構成要素がサポートする動作環境について検討する。

・ACBio 呼出部分について必要に応じてインタフェースを定義し実装する。

5.2.4 まとめ

本 5.2 節では、共通バイオメトリック認証基盤のセキュリティに関連する機能の実装方法について調査研究を行った。調査・検討の手順として、共通バイオメトリック認証基盤におけるセキュリティ対象データ項目を明らかにしたのち、共通バイオメトリック認証基盤を適用するアプリケーションの候補を選定するとともに、共通バイオメトリック認証基盤を該当アプリケーション上で用いる際の機能についての調査・検討を行った。その後、共通バイオメトリック認証基盤への実装が必要になるセキュリティ機能として、NIST SP 800-63 の考えに基づいてセキュリティ技術の選択を行った後に、共通バイオメトリック認証基盤における方式を 1 つ選択して具体的なセキュリティ機能の実装案を示した。あわせて、共通バイオメトリック認証基盤における実現方式の中で候補として示されている ACBio を組み込んだ場合の実装について基本的な方式を示した。

今後は、本調査検討結果に基づいた共通バイオメトリック認証基盤へのセキュリティ機能の実装が必要である。また今後は、共通バイオメトリック認証基盤の完成に向け、被災者支援システムを含んだ応用アプリケーションへの共通バイオメトリック認証基盤の組み込みを実施し、本成果を実際のアプリケーションに適用することが重要である。

5.3　IdM 共通本人認証基盤の機能強化のための開発研究

本 5.3 節では共通バイオメトリック認証基盤の機能強化のための開発内容、および開発項目に対する検証実験の内容について示す。

5. 3. 1 開発方針

図 5.10 は前年度以前における共通バイオメトリック認証基盤システムの構成図である。本図において、太枠で示されている部分が、共通バイオメトリック認証基盤システムのプロトタイプとして開発済みの部分である。本図に示すとおり、前年度までは OpenID に基づく SSO システムに生体認証技術による本人認証機能を共通基盤として開発した。

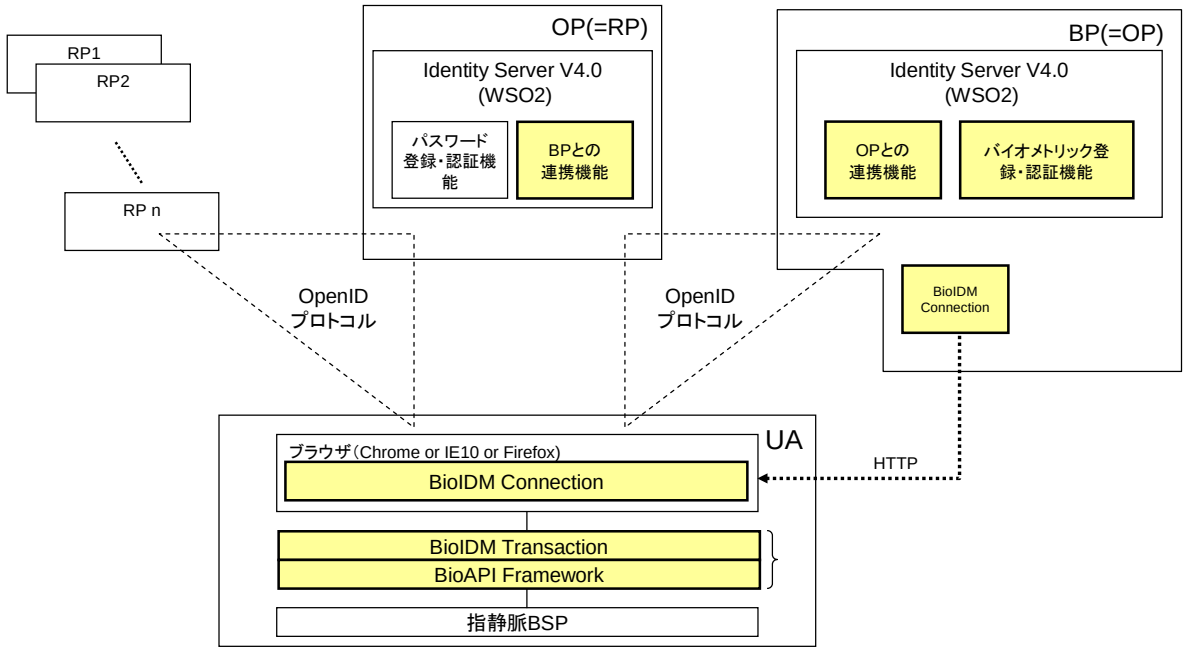


図 5.10　前年度（平成 24 年度）における開発システム

これに対して、共通バイオメトリック認証基盤として当初開発を目指していた目標機能の一覧を表 5.6 に示す。

表 5.6　開発目標項目一覧

No	項目	概要	説明	方針
1	国際標準化の取り込みと貢献	BioAPI、BIP、BIAS などの取り込み	BioAPI V2.2 を実装し、BioAPI 配下に様々な装置が接続できる構造を採用した。実装作業の際に検出された BioAPI 規格の記載上の改善点を国際規格開発作業におけるコントリビューションとして反映させた。	（開発済み）
2	Web 技術との親和性	ブラウザ、サーバサイド Java など Web 技術の適用	生体認証の登録画面や認証画面を HTML で開発した。Web ブラウザと BioAPI 間の情報交換を WebSocket という Web 技術を用いて実現した。	（開発済み）
3	汎用性	特定の IdM システムに非依存	OpenID への対応は完了したが、もう一つの代表的な IdM 技術である SAML には対応できていない。	開発対象とする。
4	バイオメトリクスの特性を考慮	認証技術の多様性	BioAPI ベースで開発したことにより、様々な生体認証技術が組み込みやすい。ただし、実際に接続を確認したのは指静脈認証装置のみである。	開発対象とする
		精度評価	精度評価への応用については本プロジェクトの対象外とする。	開発対象としない
		プライバシー（セキュリティ）	プライバシーの懸念が高いサーバ認証は採用せず、ローカル認証を採用している。暗号化や ACBio、WebSocket の SSL 化などセキュリティ機能への考慮は不十分である。	開発対象とする。

本表で示すとおり、国際標準化の取り込みと貢献、Web 技術との親和性の 2 点については前年度まででプロトタイプとしての開発が完了したが、項番 3 の汎用性と項番 4 のバイオメトリクスの特性を考慮の 2 点については一部対応されていないことがわかる。開発されていない項目の中で、汎用性としての SAML 技術を用いた SSO 機能、認証技術の多様性としての複数モダリティ対応、生体情報を取り扱う際のセキュリティ機能の 3 点について今年度の開発項目とした。

これに対して、バイオメトリクスの特性のひとつとして挙げられている精度評価は、PTS（Performance Test Suite）と呼ばれるバイオメトリック製品用の精度評価ツールの開発が必要と考えられるが、共通バイオメトリック認証基盤単独での対応は困難である。したがって、本プロジェクトとしては開発対象範囲外とした。

前述の方針に従った場合の共通バイオメトリック認証基盤システムのシステム構成図における今年度の開発項目を図 5.11 の破線部として示す。

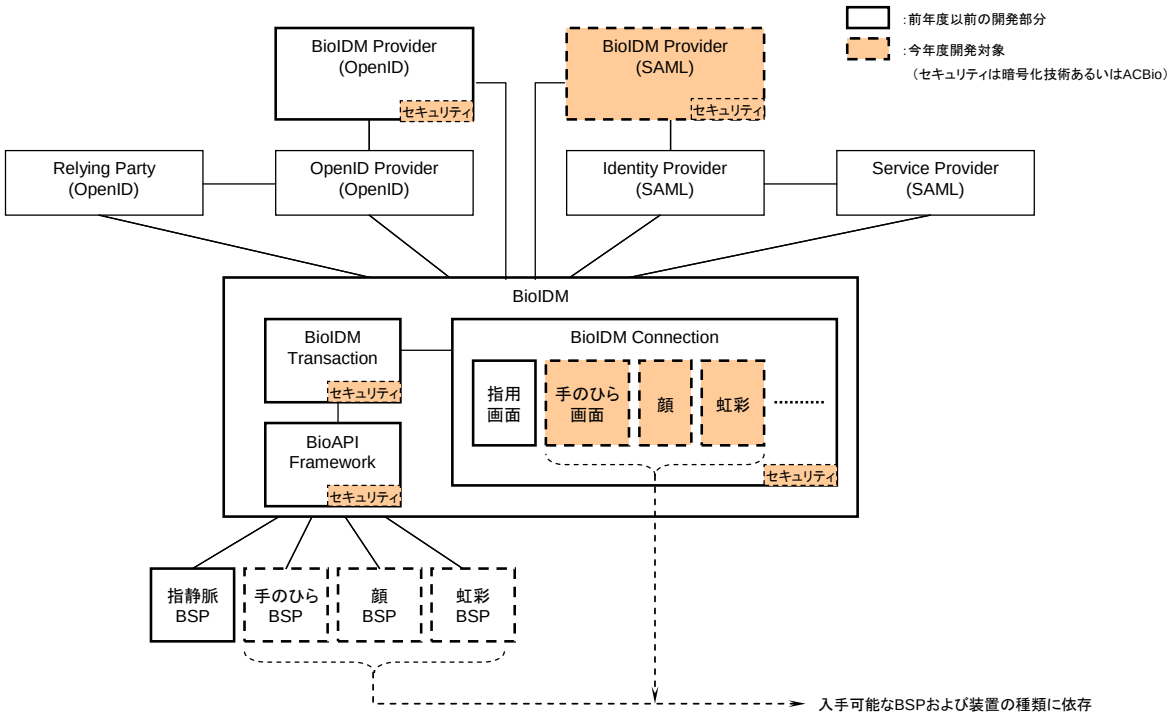


図 5.11　今年度（平成 25 年度）における開発項目

(1) SAML 機能

本項では、前述の開発方針により開発項目のひとつとなった SAML 機能の実装内容について示す。SAML 機能は前年度から使用している WSO2 社の OSS である Identity Server に、OpenID による SSO 機能とともに組み込まれている。本プロジェクトでは、SAML による SSO 機能の実装においても、Identity Server を用いることとした。以下に使用した Identity Server と組み込まれている SAML 機能に関する概要情報を示す。

① OSS 名称： WSO2 Identity Server

② バージョン番号： V4.0.0

③ SAML 関連機能：

・Single Sign-On (SSO) via SAML2

・Federation via SAML2

・Trusted SAML2 Identity Provider per tenant

・Customizable login pages for SAML2

・Extensibility for pluggable authenticators, alternative user stores, XACML/SAML extension points and more

・Comprehensive management & monitoring Web console with enterprise-level security and SAML2 SSO

本 Identity Server を用いて SAML による SSO 機能に生体認証機能を組み込んだプロトタイプシステムを開発した。処理の流れを図 5.12 に示す。

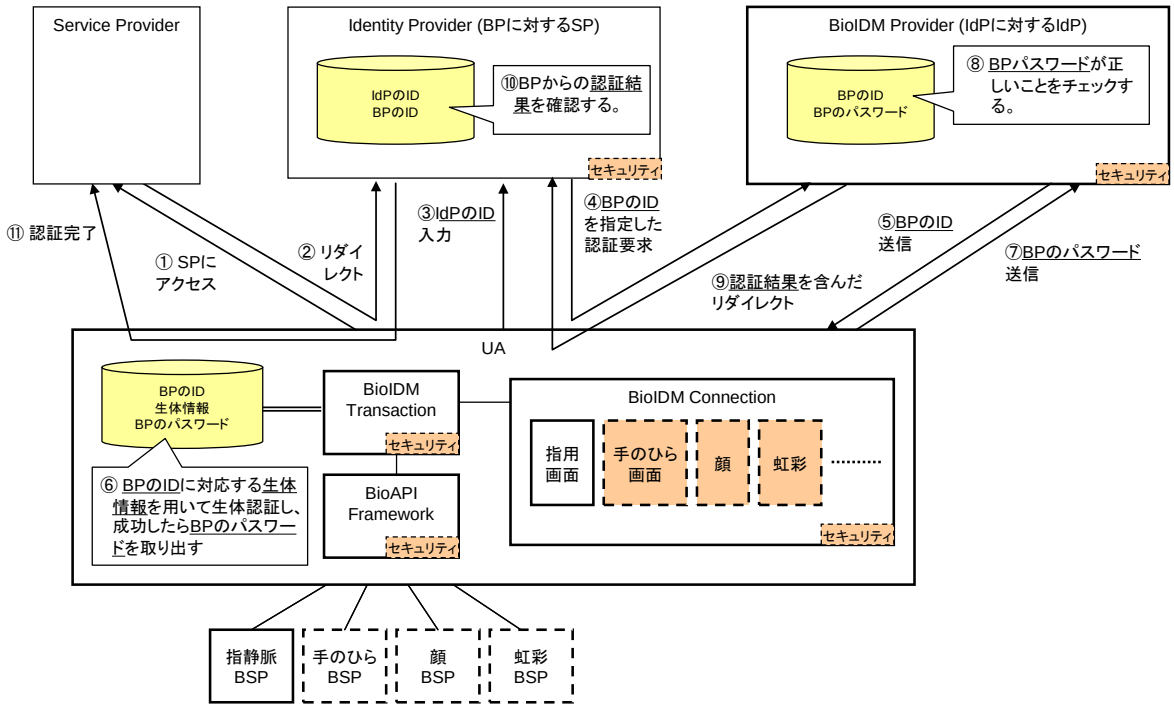


図 5.12　SAML 技術を用いた SSO システム構成図

本開発においては、SAML 技術による SSO 機能の流れの中で、本人認証機能に関わる部分に BioIDM Connection を初めとする生体認証を用いた本人認証機能を組み込んだ。端末内にパスワードを格納しておき、端末内で実行される生体認証結果が成功だった場合にパスワードを取り出して BP における本人認証処理に用いる方法は、前年度の OpenID の場合と同様である。

(2)複数モダリティサポート機能

本項では、前述の開発方針により開発項目のひとつとなった複数モダリティサポート機能の実装内容について示す。複数モダリティサポートにおいては、共通バイオメトリック認証基盤が用いる BioAPI 規格において BSP のサポートが要求される関数を確認した上で、必要な関数をサポートしている BSP を入手する必要がある。共通バイオメトリック認証基盤において、BSP がサポートすべき関数（BioSPI 関数）の一覧を表 5.7 に示す。

表 5.7　BSP がサポートすべき BioSPI 関数一覧

No	BioIDM で用いる関数
1	BioSPI_BSPLoad / BSPUnload / BSPAttach / BSPDetach
2	BioSPI_GetBIRFromHandle
3	BioSPI_SetGUICallbacks
4	BioSPI_Capture
5	BioSPI_CreateTemplate
6	BioSPI_Process
7	BioSPI_VerifyMatch

本表で示した関数をサポートする BSP を調査し、結果的に指紋認証装置用 BSP を入手した。

つづいて本 BSP を用いて指静脈に指紋を加えることによる複数モダリティサポートのための開発を行った。開発後の動作確認結果を表 5.8 に示す。本表に示すとおり、入手した BSP の特性によって共通バイオメトリック認証基盤プログラムの一部に対応が必要になる箇所がみつかった。（これらはベンダの BSP が BioAPI 準拠であれば不要な対応であった。）

しかしながら、本表で示す登録用キャプチャと照合用キャプチャのグラフィックユーザインタフェース（GUI）表示については、ベンダ提供プログラムの表示を抑制することができないため、共通バイオメトリック認証基盤プログラムによる対応は不可と判断した。ベンダが表示する GUI 表示に基づき正常に操作を続けた場合、共通バイオメトリック認証基盤が正常動作することを確認した。

表 5.8　指紋認証装置の実装結果

No	確認項目		確認結果	説明
1	インストール		○	
2	初期化・終了処理		○	入手製品が BioAPI 規格上本来必要でない関数呼び出しを必要としていた。BioIDM 側のプログラム変更で対応した。
3	登録機能	指選択画面	○	
		登録用キャプチャ	×	入手製品が本来表示すべきでない GUI を出力する。
		表示用画像取得	○	BioIDM は BioAPI バージョン 2.1 の関数（BioAPI_SubscribeToGUIEvents）を使用していたが、該当製品はバージョン 2.0 の相当する関数（BioAPI_SetGUICallbacks）をサポートしていた。BioIDM 側で BSP の対応状況に応じてバージョン 2.0 の関数も呼び出すよう修正した。
		テスト照合用キャプチャ	○	
		複数指選択	○	
		終了処理	○	
4	照合機能	照合用キャプチャ	×	上記 3 の登録用キャプチャと同様
		表示用画像取得	○	上記 3 の表示用画像取得と同様。
		マッチング	○	
		終了処理	○	

(3)セキュリティ機能

本項では、前述の開発方針により開発項目のひとつとなったセキュリティ機能の実装内容について示す。セキュリティ機能については 5.2 節において調査結果が示されている。本開発では、5.2 節で示された調査結果に基づいた開発を行った。

表 5.9 は格納データに関するセキュリティ機能の実装結果である。また、図 5.13 は通信データに関するセキュリティ機能の実装結果である。

表 5.9　格納データに関するセキュリティ機能の実装結果

No	項目	端末	OP および BP
1	暗号化対象データ	5.2 節のセキュリティ機能に従い、以下の 3 項目を暗号化対象とした。 ・登録テンプレート ・BP のユーザ ID ・BP のパスワード	Identity Server(1)が管理するデータベース全体を暗号化するように実装した。
2	暗号アルゴリズム	AES-128 用アルゴリズムとして OpenSSL 内のアルゴリズムを採用した。	同左
3	鍵管理	暗号鍵保存用ファイルに暗号鍵を保存する機能を BioIDM Transaction に実装した。	Identity Server が参照する暗号鍵保存用ファイル（コンフィグファイル）に暗号鍵を保存した。（Identity Server の機能を利用した。）
4	鍵ファイルの保護	・暗号鍵保存用ファイルに専用ユーザからのアクセス権を設定し、一般ユーザの参照を禁止した。 ・専用ユーザで BioIDM Transaction を Windows サービスとして実行するように実装した。	・コンフィグファイルに専用ユーザからのアクセス権を設定し、他の一般ユーザからの参照を禁止するように実装した。 ・Identity Server 自体を上記特定ユーザで Windows サービスとして実行するように実装した。

注）(1) WSO2 というオープンソースアプリケーション開発会社が開発し OSS として公開している OpenID や SAML を含んだアイデンティティ管理サーバ

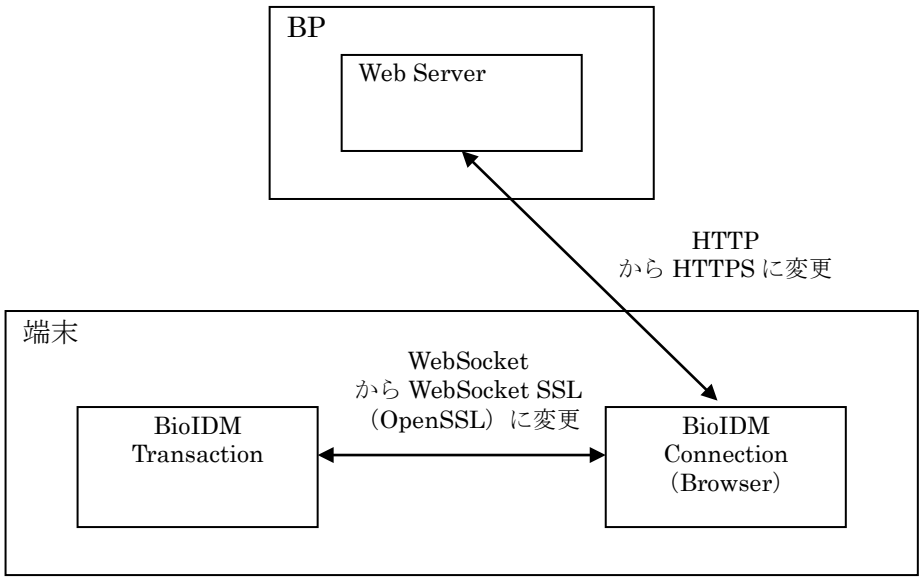


図 5.13　通信データに関するセキュリティ機能実装結果

5.3.2 検証実験

(1) 登録機能および認証機能

本項では共通バイオメトリック認証基盤システムにおける、利用者の登録機能および認証機能に関する検証項目と検証結果を示す。

① 検証環境

検証のための構成は、共通バイオメトリック認証基盤における標準構成とする。

内容は以下の通りである。

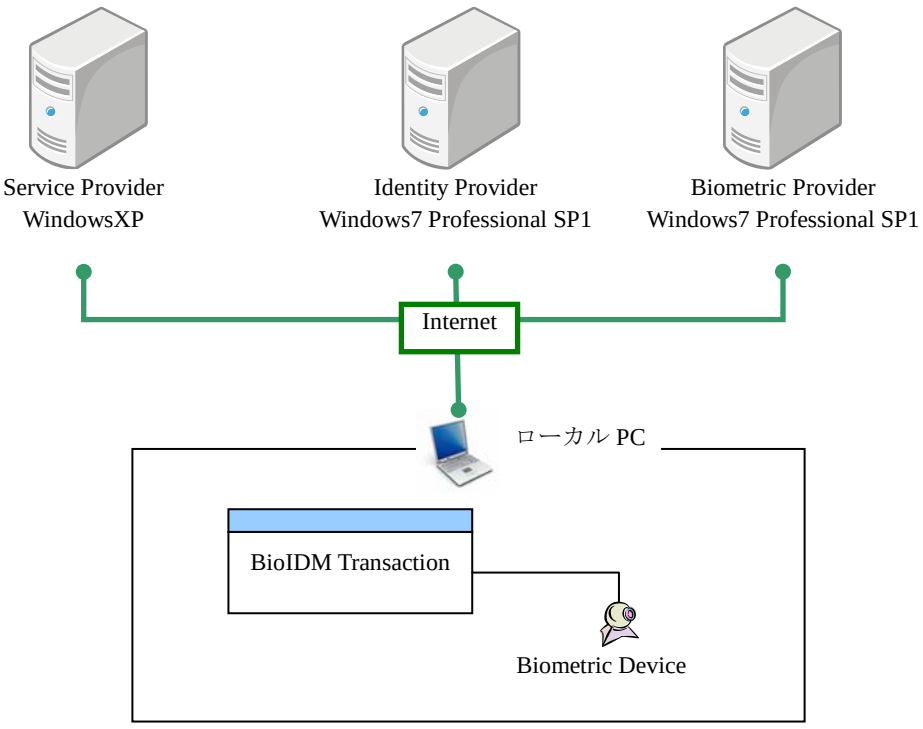
BSP	指静脈認証装置＋BioAPI2.0 対応ドライバ
ブラウザ	Internet Explorer 10 (Windows7)
システム構成	標準（SP、IdP、BP） 
SAML 対応サイト	評価用 SP

図 5.14　検証環境（標準構成）

② バイオメトリック登録機能に関する検証項目と検証結果

以下にバイオメトリック登録機能に関する検証項目および検証結果を示す。

1) BP での ID 登録

表 5.10　BP での ID 登録機能の検証項目と検証結果

No	画面		パターン	操作	検証内容	検証結果	
						結果	備考
1	BP(Identity Server)	初期画面	初期表示	IE10 で BP の URL を開く	BP の初期画面が表示されること ・上フレーム部に「Biometric Provider」が表示されていること ・左フレーム内に「Sign-up」「OpenID Sign-in」リンクが表示されていること ・右フレーム内にログイン用の Username/Password 入力欄、及び「Sign-in」ボタンが表示されていること	○	
2				左フレーム内の「Sign-up」リンクをクリック	右フレームが Sign-up 画面に遷移すること	○	
3		Sign-up 画面	初期表示	-	「Sign-up with User Name / Biometric or Password」の文字列と、その下にリンク用のアイコンが表示されること	○	
4				右フレームの「Sign-up with User Name / Biometric or Password」下のアイコンをクリック	右フレームが登録画面に遷移すること	○	
5		登録画面	初期表示	-	「User Name」「Nick Name」「Gender」「Birth Date」の入力欄が表示されていること 「Enroll with Biometric」「Enroll with Password」「Cancel」ボタンが表示されていること	○	
6				「User Name」を入力せず、「Enroll with Biometric」ボタンをクリック	User Name が必要な旨のエラーが表示されること	○	
7				「User Name」「Nick Name」「Gender」「Birth Date」を全て入力し、「Enroll with Biometric」ボタンをクリック	BioIDM のメイン画面が表示されること	○	

8				「User Name」「Nick Name」「Gender」「Birth Date」を全て入力し、「Enroll with Password」ボタンをクリック	パスワード入力画面が表示されること	○	
9				「User Name」を入力せず、「Cancel」ボタンをクリック	右フレームが Sign-up 画面に遷移すること	○	
10		パスワード入力画面	初期表示	-	パスワード及びパスワード再入力欄が表示されること 「Enroll」「Cancel」ボタンが表示されていること	○	
11				「Cancel」ボタンをクリック	BP の登録画面が表示されること	○	
12				パスワードを入力せず、「Enroll」ボタンをクリック	パスワード入力が必要な旨のエラーダイアログが表示されること	○	
13				パスワード再入力欄を入力せず、「Enroll」ボタンをクリック	パスワード再入力欄に入力が必要な旨のエラーダイアログが表示されること	○	
14				パスワードと再入力欄に 6 文字未満の文字を入力し、「Enroll」ボタンをクリック	パスワードは 6 文字以上の入力が必要な旨のエラーダイアログが表示されること	○	
15				パスワードと再入力欄に 6 文字以上の違う値を入力し、「Enroll」ボタンをクリック	パスワードが一致しない旨のエラーダイアログが表示されること	○	
16				パスワードと再入力欄に同じ値を入力し、「Enroll」ボタンをクリック	ユーザの登録が完了した旨のダイアログが表示されること	○	
17	BioIDM	メイン画面	初期表示	-	BioIDM の初期化中メッセージが表示されること	○	
18			BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない	遷移元画面に戻り、接続失敗のエラーダイアログが表示されること	○	
19			生体認証機器の初期化失敗	生体認証機器を接続しない	遷移元画面に戻り、機器初期化失敗のエラーダイアログが表示されること	○	
20			初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	部位選択（右手）が表示されること 「Capture」「Complete」ボタンが無効となっていること 「Cancel」ボタンが有効となっていること	○	
21				「Cancel」ボタンをクリック	BP の登録画面が表示されること	○	
22				「Left Hand」タブをクリック	部位選択（左手）が表示されること	○	

23				「Right Hand」タブをクリック	部位選択（右手）が表示されること	○	
24				任意の部位をクリック	「Capture」ボタンが有効となること	○	
25				「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
26				部位登録後、再度「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
27				「Complete」ボタンをクリック	BP の登録画面が表示されること BP の登録画面上に登録完了の旨のダイアログが表示されること	○	
28				登録完了ダイアログの「OK」ボタンをクリック	ダイアログが閉じること 右フレームが Sign-up 画面に遷移すること	○	
29		キャプチャ画面	初期表示	-	Enroll イメージ表示欄、TestVerify イメージ表示欄、メッセージ表示欄が表示されること メッセージ表示欄に Enroll ボタンをクリックする旨のメッセージが表示されること 「Enrol」「Cancel」ボタンが有効となっていること 「TestVerify」「OK」ボタンが無効となっていること	○	
30				「Cancel」ボタンをクリック	BioIDM のキャプチャ画面が閉じること	○	
31				「Enroll」ボタンをクリック	キャプチャ待ちとなること ・Enroll イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
32				生体認証装置に指定部位を置く (キャプチャ成功)	・Enroll イメージ表示欄に緑チェックアイコンが表示されること ・Enroll イメージ表示枠が緑になること ・Test Verify ボタンが有効ととなること	○	
33				再度「Enroll」ボタンをクリック	再度 Enroll を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	

34							「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Enroll のキャプチャ待ちとなること	○	
35							「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
36						生体認証装置に指定部位を置く (キャプチャ失敗)		画面に変化が無いこと （引き続きキャプチャ中となる）	○	
37							タイムアウト時	・Enroll イメージ表示欄に赤×アイコンが表示されること ・Enroll イメージ表示枠が赤になること ・タイムアウトのエラーメッセージが表示されること	○	
38						「Cancel」ボタンをクリック		BioIDM のメイン画面が表示されること	○	BioIDM Enrollment 画面
39					「Test Verify」ボタンをクリック			キャプチャ待ちとなること ・Test Verify イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
40						生体認証装置に指定部位を置く (キャプチャ成功)		・Test Verify イメージ表示欄に緑チェックアイコンが表示されること ・Test Verify イメージ表示枠が緑になること ・OK ボタンが有効ととなること	○	
41							再度「Enroll」ボタンをクリック	再度 Enroll を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
42								「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Test Verify のキャプチャ待ちとなること	○	
43								「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
44							再度「Test Verify」ボタンをクリック		再度 Test Verify を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	

45							「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Test Verify のキャプチャ待ちとなること	○	
46							「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
47					生体認証装置に登録していない部位を置く			画面に変化が無いこと （引き続きキャプチャ中となる）	○	
48					生体認証装置に指定部位を置く (キャプチャ失敗)			画面に変化が無いこと （引き続きキャプチャ中となる）	○	
49						タイムアウト時		・Test Verify イメージ表示欄に赤×アイコンが表示されること ・Test Verify イメージ表示枠が赤になること ・タイムアウトのエラーメッセージが表示されること	○	
50					「Cancel」ボタンをクリック			BioIDM のメイン画面が表示されること	○	BioIDM Enrollment 画面
51					「OK」ボタンをクリック			BioIDM のメイン画面が表示されること メイン画面の「Complete」ボタンが有効となること	○	BioIDM Enrollment 画面

2) IdP での ID 登録

表 5.11　IdP での ID 登録機能の検証項目と検証結果

No	画面		パターン	操作	検証内容	検証結果	
						結果	備考
1	IdP(Identity Server)	初期画面	初期表示	IE10 で IdP の URL を開く	IdP の初期画面が表示されること ・上フレーム部に「SAML Identity Provider / OpenID Provider」が表示されていること ・左フレーム内に「Sign-up」「OpenID Sign-in」リンクが表示されていること ・右フレーム内にログイン用の Username/Password 入力欄、及び「Sign-in」ボタンが表示されていること	○	
2				左フレーム内の「Sign-up」リンクをクリック	右フレームが Sign-up 画面に遷移すること	○	
3		Sign-up 画面	初期表示	-	以下の文字列とそのリンクアイコンが横ならびに表示されること ・「Sign-up with User Name / Password」 ・「Sign-up with Biometric Provider」	○	
4				右フレームの「Sign-up with Biometric Provider」下のアイコンをクリック	右フレームが登録画面に遷移すること	○	
5		登録画面（OpenID/SAML 入力）	初期表示	-	「OpenID」が選択されていること 「OpenID on Biometric Provider」の入力欄が表示されていること 「Authenticate」「Cancel」ボタンが表示されていること	○	
6				SAML を選択	「OpenID on Biometric Provider」入力欄が「SAML on Biometric Provider」選択に変化すること。	○	
7				OpenID を選択	「SAML on Biometric Provider」選択が「OpenID on Biometric Provider」入力欄に変化すること。	○	
8				「SAML on Biometric Provider」で BP の URL を選択し、「Authenticate」ボタンをクリック	BP の SAML 認証画面（ユーザ入力）に遷移すること	○	
9				「Cancel」ボタンをクリック	右フレームが Sign-up 画面に遷移すること	○	
10	BP(Identity Server)	SAML 認証画面（ユーザ入力）	初期表示	-	BP の SAML 認証画面が表示されること ・上フレーム部に「Biometric Provider」が表示されていること ・右フレーム内に「User Name」の入力欄、「Nextl」ボタンが表示されていること	○	

11				「User Name」を入力せず、「Next」ボタンをクリック	User Name が必要な旨のエラーダイアログが表示されること	○	
12				エラーダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
13				生体認証で登録した「User Name」を入力し、「Next」ボタンをクリック	BioIDM の認証画面が表示されること	○	
14				パスワードで登録した「User Name」を入力し、「Next」ボタンをクリック	パスワード入力画面が表示されること	○	
15				存在しない「User Name」を入力し、「Next」ボタンをクリック	パスワード入力画面が表示されること	○	
16				パスワードを入力し、「Sign In」ボタンをクリック	ユーザ入力画面に戻り、認証エラーが表示されること	○	
17		パスワード入力画面	初期表示	-	パスワード入力欄が表示されること 「Sign In」ボタンが表示されていること	○	
18				パスワードを入力せず、「Sign In」ボタンをクリック	パスワード入力が必要な旨のエラーダイアログが表示されること	○	
19				エラーダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
20				正しいパスワードを入力し、「Sign In」ボタンをクリック	認証が完了し、IdP のユーザ登録画面（ユーザ情報入力）に遷移すること	○	
21				誤ったパスワードを入力し、「Sign In」ボタンをクリック	SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
22	BioIDM	認証画面	初期表示	-	BioIDM の初期化中メッセージが表示されること	○	
23			BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない	接続失敗の旨のエラーダイアログが表示されること	○	
24				エラーダイアログの「OK」ボタンをクリック	SAML 認証画面（ユーザ入力）が表示されること	○	
25			生体認証機器の初期化失敗	生体認証機器を接続しない	機器初期化失敗のエラーダイアログが表示されること	○	
26				エラーダイアログの「OK」ボタンをクリック	ダイアログの OK クリック後、SAML 認証画面（ユーザ入力）が表示されること	○	
27			初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	キャプチャ待ちとなること ・キャプチャ結果イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること ・「Cancel」ボタンが表示されること	○	
28				「Cancel」ボタンをクリック	SAML 認証画面（ユーザ入力）が表示されること	○	

29				生体認証装置に登録した部位を置く	・メッセージ表示欄に認証成功のメッセージが表示されること ・自動でウィンドウが閉じること ・元画面が IdP の登録画面（ユーザ情報入力）に遷移すること	○	
30				生体認証装置に登録していない部位を置く	画面に変化が無いこと （引き続きキャプチャ中となる）	○	
31				タイムアウト時	・BP のユーザ入力画面に遷移すること ・認証失敗のエラーメッセージが表示されること	○	
32	IdP(Identity Server)	登録画面（ユーザ情報入力）	初期表示	-	「User Name」「Full Name」「Email」「Postal Code」「Country」の入力欄が表示されていること BP に登録した「Nick Name」「Gender」「Date of Birth」の情報が表示されること BP の URL が「SAML on Biometric Provider」欄に表示されていること 「Submit」「Cancel」ボタンが表示されていること	○	
33				「User Name」を入力せず、「Submit」ボタンをクリック	User Name が必要な旨のエラーが表示されること	○	
34				全項目を入力し、「Submit」ボタンをクリック	右フレームが Sign-up 画面に遷移すること 登録完了の旨のダイアログが表示されること	○	
35				登録完了ダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
36				「User Name」を入力せず、「Cancel」ボタンをクリック	右フレームが Sign-up 画面に遷移すること	○	

3) SP での ID 登録

表 5.12　SP での ID 登録機能の検証項目と検証結果

No	画面		パターン	操作	検証内容	検証結果	
						結果	備考
1	SP	初期画面	初期表示	IE10 で SP の URL を開く	SP の初期画面が表示されること ・「Enroll User」「Login」ボタンが表示されていること	○	
2				「Enroll User」リンクをクリック	SP のユーザ登録画面に遷移すること	○	
3		ユーザ登録画面	初期表示	-	「User Name」「Blood Type」の入力欄、「SAML Identity Provider」の選択欄が表示されていること 「Enroll」「Cancel」ボタンが表示されていること	○	
4				「User Name」を入力せず、「Enroll」ボタンをクリック	User Name が必要な旨のエラーが表示されること	○	
5				「Blood Type」を入力せず、「Enroll」ボタンをクリック	エラーが表示されず、処理が続行すること	○	
6				「SAML Identity Provider」で IdP を選択し、「Enroll」ボタンをクリック	選択された IdP の SAML 認証画面（User Name 入力）に遷移すること	○	
7				「Cancel」ボタンをクリック	初期メニューに遷移すること	○	
8	IdP(Identity Server)	SAML 認証画面（ユーザ入力）	初期表示	-	「User Name」入力欄が表示されること 「Next」ボタンが表示されること	○	
9				「User Name」を入力せず、「Next」ボタンをクリック	User Name が必要な旨のエラーダイアログが表示されること	○	
10				エラーダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
11				User Name に登録した IdP の User Name を入力し、「Next」ボタンをクリック	BP の SAML 認証画面に遷移すること	○	
12				User Name に登録していない IdP の User Name を入力し、「Next」ボタンをクリック	パスワード入力画面が表示されること	○	
13				パスワード入力画面	適当なパスワードを入力し、「Sign In」ボタンをクリックすると、認証エラーメッセージが表示されること	○	
14	BP(Identity Server)	SAML 認証画面	初期表示	-	BP の SAML 認証画面が表示されること ・上フレーム部に「Biometric Provider」が表示されていること	○	

15				IdP から認証を要求された User Name に対応する BP ユーザが生体認証登録されている場合	BioIDM の認証画面が表示されること	○	
16				IdP から認証を要求された User Name に対応する BP ユーザがパスワード登録されている場合	BP の SAML 認証（パスワード）画面が表示されること	○	
17		SAML 認証（パスワード）画面	初期表示		パスワード入力欄が表示されること 「Sign In」ボタンが表示されていること	○	
18				パスワードを入力せず、「Sign In」ボタンをクリック	パスワード入力が必要な旨のエラーダイアログが表示されること	○	
19				エラーダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
20				正しいパスワードを入力し、「Sign In」ボタンをクリック	認証が完了し、IdP のユーザ登録画面（ユーザ情報入力）に遷移すること	○	
21				誤ったパスワードを入力し、「Sign In」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
22	BioIDM	認証画面	初期表示	-	BioIDM の初期化中メッセージが表示されること	○	
23			BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない	接続失敗の旨のエラーダイアログが表示されること	○	
24				エラーダイアログの「OK」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
25			生体認証機器の初期化失敗	生体認証機器を接続しない	機器初期化失敗の旨のエラーダイアログが表示されること	○	
26				エラーダイアログの「OK」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
27			初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	キャプチャ待ちとなること ・キャプチャ結果イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること ・「Cancel」ボタンが表示されること	○	
28				「Cancel」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	

29				生体認証装置に登録した部位を置く	・キャプチャ結果イメージ表示欄に緑チェックアイコンが表示されること ・メッセージ表示欄に認証成功のメッセージが表示されること ・自動でウィンドウが閉じること ・元画面が SP の登録完了画面に遷移すること	○	
30				複数部位登録時 （生体認証装置に登録した任意の部位を置く）	登録したどの部位でも認証が行えること	○	
31				生体認証装置に登録していない部位を置く	画面に変化が無いこと （引き続きキャプチャ中となる）	○	
32				タイムアウト時	・IdP のユーザ入力画面に遷移すること ・認証失敗のエラーメッセージが表示されること	○	
33	SP	登録完了画面	初期表示	-	SP の登録画面で入力した「UserID」「Blood Type」「SAML Identity Provider」が表示されていること User Name に対応した IdP の「Full Name」「Email」「Postal Code」「Country」が表示されていること User Name に対応した BP の「Nickname」「Gender」「Date of Birth」の情報が表示されること 「Back」ボタンが表示されていること	○	
34				「Back」ボタンをクリック	SP の初期メニュー画面に遷移すること	○	

③ バイオメトリック認証機能に関する検証項目と検証結果

以下にバイオメトリック認証機能に関する検証項目および検証結果を示す。

表 5.13　バイオメトリック認証機能の検証項目と検証結果

						検証結果	
No	画面		パターン	操作	検証内容	結果	備考
1	SP	初期画面	初期表示	IE10 で SP の URL を開く	SP の初期画面が表示されること ・「Enroll User」「Login」ボタンが表示されていること	○	
2				「Login」リンクをクリック	SP のログイン画面に遷移すること	○	
3		ログイン画面	初期表示	-	「SAML Identity Provider」の選択欄が表示されていること 「Login」「Cancel」ボタンが表示されていること	○	
4				「SAML Identity Provider」で IdP を選択し、「Login」ボタンをクリック	選択された IdP の SAML 認証画面（User Name 入力）に遷移すること	○	
5				「Cancel」ボタンをクリック	初期メニューに遷移すること	○	
6	IdP(Identity Server)	SAML 認証画面(ユーザ入力)	初期表示	-	「User Name」入力欄が表示されること 「Next」ボタンが表示されること	○	
7				「User Name」を入力せず、「Next」ボタンをクリック	User Name が必要な旨のエラーダイアログが表示されること	○	
8				エラーダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
9				User Name に登録した IdP の User Name を入力し、「Next」ボタンをクリック	BP の SAML 認証画面に遷移すること	○	
10				User Name に登録していない IdP の User Name を入力し、「Next」ボタンをクリック	パスワード入力画面が表示されること	○	
11				パスワード入力画面	適当なパスワードを入力し、「Sign In」ボタンをクリックすると、認証エラーメッセージが表示されること	○	
12	BP(Identity Server)	SAML 認証画面	初期表示	-	BP の SAML 認証画面が表示されること ・上フレーム部に「Biometric Provider」が表示されていること	○	
13				IdP から認証を要求された User Name に対応する BP ユーザが生体認証登録されている場合	BioIDM の認証画面が表示されること	○	
14				IdP から認証を要求された User Name に対応する BP ユーザがパスワード登録されている場合	BP の SAML 認証（パスワード）画面が表示されること	○	

15		SAML認証（パスワード）画面	初期表示	-	パスワード入力欄が表示されること 「Sign In」ボタンが表示されていること	○	
16				パスワードを入力せず、「Sign In」ボタンをクリック	パスワード入力が必要な旨のエラーダイアログが表示されること	○	
17				エラーダイアログの「OK」ボタンをクリック	ダイアログが閉じること	○	
18				正しいパスワードを入力し、「Sign In」ボタンをクリック	認証が完了し、SP のログイン完了画面に遷移すること	○	
19				誤ったパスワードを入力し、「Sign In」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
20	BioIDM	認証画面	初期表示	-	BioIDM の初期化中メッセージが表示されること	○	
21			BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない	接続失敗の旨のエラーダイアログが表示されること	○	
22				エラーダイアログの「OK」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
23			生体認証機器の初期化失敗	生体認証機器を接続しない	機器初期化失敗の旨のエラーダイアログが表示されること	○	
24				エラーダイアログの「OK」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
25			初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	キャプチャ待ちとなること ・キャプチャ結果イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること ・「Cancel」ボタンが表示されること	○	
26				「Cancel」ボタンをクリック	IdP の SAML 認証画面（ユーザ入力）に戻り、認証エラーが表示されること	○	
27				生体認証装置に登録した部位を置く	・キャプチャ結果イメージ表示欄に緑チェックアイコンが表示されること ・メッセージ表示欄に認証成功のメッセージが表示されること ・自動でウィンドウが閉じること ・元画面が SP の登録完了画面に遷移すること	○	
28				複数部位登録時 （生体認証装置に登録した任意の部位を置く）	登録したどの部位でも認証が行えること	○	

29				生体認証装置に登録していない部位を置く	画面に変化が無いこと （引き続きキャプチャ中となる）	○	
30	SP	ログイン完了画面	初期表示	-	SP の登録画面で入力した「User Name」「Blood Type」「SAML Identity Provider」が表示されていること User Name に対応した IdP の「Full Name」「Email」「Postal Code」「Country」が表示されていること User Name に対応した BP の「Nickname」「Gender」「Date of Birth」の情報が表示されること 「logout」ボタンが表示されていること	○	
31				「Logout」ボタンをクリック	IdP, BP に対してログアウトが行なわれること （別ウィンドウからログインしても再度ユーザ認証が必要になること） SP の初期メニュー画面に遷移すること	○	

(2) シングルサインオン機能

本項ではバイオメトリック認証機能を用いたIdMでのシングルサインオン機能(SSO機能と略す)に関する検証項目および検証結果を示す。

① 検証環境

前述の(1)で示した標準構成と同様の検証環境とする。但し、IdPが動作するコンピュータ上にもうひとつSPを起動し、これを別のSPとして用いることでSSO機能の動作を検証する。

② 検証項目と検証結果

SSO機能の検証のために、一度認証を行った後で別SPから同一ID(IdP/BP)で認証要求を行い、自動的に認証結果が返却されることを検証する。

表 5.14　SSO機能の検証項目と検証結果

				検証結果	
No	パターン	操作	検証内容	結果	備考
1	ログイン後の自動ログイン	SPにID(IdP)を入力し、認証を行う。（認証結果画面の「ログアウト」はクリックしない）	SPにログイン情報が表示されること。	○	
2		別のSPより認証を行う。	ログインが自動で行なわれること。（IdP側で認証画面が表示されることなく、SPに認証結果が表示されること）	○	IDP上のSPを使用
3		認証結果画面の「ログアウト」をクリック。	SPにメインメニューが表示されること。	○	
4		別のSPより同一のID(IdP)で認証を行う。	ログインが自動で行なわれないこと。（IdP側で認証画面が表示されること）	○	IDP上のSPを使用

(3) 複数モダリティサポート機能

本項では前年度（平成 24 年度）の開発で組み込んだ指静脈技術に対して、複数モダリティとして指紋認証技術を組み込んだことによる複数モダリティのサポート機能に関する検証項目と検証結果を示す。

① 検証環境

標準構成をベースとし、BSP を以下の通り変更する。

BSP	指紋認証装置＋BioAPI2.0 対応ドライバ

※キャプチャ時にベンダ独自の UI（ダイアログ）が表示される場合、共通バイオメトリック認証基盤自身の問題ではないため課題として取り扱わない。

注）BioIDM ユーザで BioIDM Transaction を起動すると、Windows のシステム制限によりダイアログの表示が抑制される。ベンダ提供の BSP がベンダ独自の UI を表示してしまう場合、UI 画面が Windows により抑制されるためキャプチャが行なえない。このような場合は、以下の通りローカルシステムアカウントで実行することにより、回避することができる。

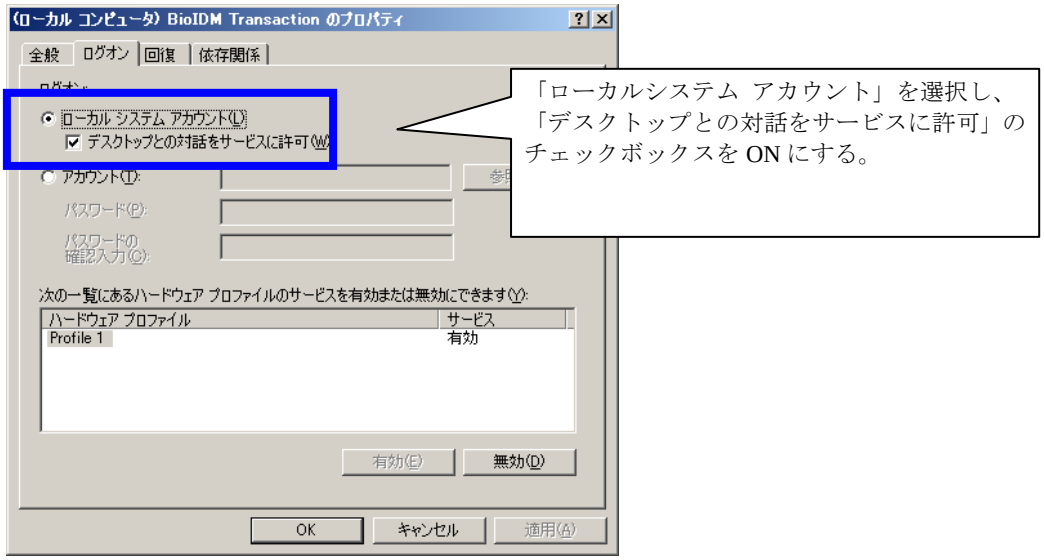


図 5.15　ベンダ独自 UI 表示される場合の対応方法

② 検証項目と検証結果

基本構成とは異なるモダリティの BSP を用いた場合においても、基本構成時の BSP と同様に認証が可能かを検証する。特に、モダリティの変更に直接関連する BioIDM 部分について検証を行う。

表 5.15　複数モダリティに関する検証項目と検証結果

						検証結果	
No	パターン	画面	操作		検証内容	結果	備考
1	登録	BP	BP より、生体認証を用いてユーザ登録を行う。		正しく登録されること。 （BioIDM の動作については、下記の通り詳細な確認を行う）	○	
2		BioIDM - メイン画面	初期表示		BioIDM の初期化中メッセージが表示されること	○	
3			初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	部位選択（右手）が表示されること 「Capture」「Complete」ボタンが無効となっていること 「Cancel」ボタンが有効となっていること	○	
4				「Cancel」ボタンをクリック	BioIDM のウィンドウが閉じること	○	
5				「Left Hand」タブをクリック	部位選択（左手）が表示されること	○	
6				「Right Hand」タブをクリック	部位選択（右手）が表示されること	○	
7				任意の部位をクリック	「Capture」ボタンが有効となること	○	
8				「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
9				「Complete」ボタンをクリック	BioIDM ウィンドウが閉じること BP の登録画面上に登録完了の旨のダイアログが表示されること	○	
10				登録完了ダイアログの「OK」ボタンをクリック	ダイアログが閉じること 右フレームが Sign-up 画面に遷移すること	○	

11			BioIDM - キャプチャ画面	初期表示	-	Enroll イメージ表示、 TestVerify イメージ表示、メッセージ表示欄が表示されること 部位選択（右手）が表示されること 「Enrol」「Cancel」ボタンが有効となっていること 「TestVerify」「OK」ボタンが無効となっていること	○	
12					「Cancel」ボタンをクリック	BioIDM のキャプチャウィンドウが閉じること	○	
13					「Enroll」ボタンをクリック	キャプチャ待ちとなること ・Enroll イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
14					生体認証装置に指定部位を置く (キャプチャ成功)	・Enroll イメージ表示欄に緑チェックアイコンが表示されること ・Enroll イメージ表示枠が緑になること ・Test Verify ボタンが有効となること	○	
15					再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	○	
16					生体認証装置に指定部位を置く (キャプチャ失敗)	・Enroll イメージ表示欄に赤×アイコンが表示されること ・Enroll イメージ表示枠が赤になること	-	独自 UI 表示のため本項目の実施不可
17					再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	-	
18					「Cancel」ボタンをクリック	BioIDM のキャプチャウィンドウが閉じること	○	
19					「Test Verify」ボタンをクリック	キャプチャ待ちとなること ・Test Verify イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること		

20					生体認証装置に指定部位を置く (キャプチャ成功)	・Test Verify イメージ表示欄に緑チェックアイコンが表示されること ・Test Verify イメージ表示枠が緑になること ・OK ボタンが有効ととなること	○	
21					再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	○	
22					再度「Test Verify」ボタンをクリック	再度 Test Verify のキャプチャ待ちとなること	○	
23					生体認証装置に指定部位を置く (キャプチャ失敗)	・Test Verify イメージ表示欄に赤×アイコンが表示されること ・Test Verify イメージ表示枠が赤になること	-	独自 UI 表示のため本項目の実施不可
24					再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	-	
25					再度「Test Verify」ボタンをクリック	再度 Test Verify のキャプチャ待ちとなること	-	
26					「Cancel」ボタンをクリック	BioIDM のキャプチャウィンドウが閉じること	○	
27				「OK」ボタンをクリック		BioIDM のキャプチャウィンドウが閉じること メイン画面の「Complete」ボタンが有効となること	○	
28		IdP		IdP よりユーザ登録を行う。 ・BP に登録した ID を用いる。		BP での生体認証が正しく行われること。 IdP に正しく登録されること。 （BioIDM の認証動作については、下記の通り詳細な確認を行う）	○	
29			BioIDM - 認証画面	初期表示	-		BioIDM の初期化中メッセージが表示されること	○	
30				初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく		キャプチャ待ちとなること ・キャプチャ結果イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること ・「Cancel」ボタンが表示されること	○	

31					「Cancel」ボタンをクリック	BioIDM のウィンドウが閉じること	-	独自 UI 表示のため本項目の実施不可
32					生体認証装置に登録した部位を置く	・キャプチャ結果イメージ表示欄に緑チェックアイコンが表示されること ・メッセージ表示欄に認証成功のメッセージが表示されること ・自動でウィンドウが閉じること ・元画面が IdP の登録画面（ユーザ情報入力）に遷移すること	○	
33					生体認証装置に登録していない部位を置く	画面に変化が無いこと （引き続きキャプチャ中となる）	-	独自 UI 表示のため本項目の実施不可
34		SP（登録）		初期表示	SP よりユーザ登録を行う。 ・IdP に登録した ID を用いる。	IdP から BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく登録されること。	○	
35	認証	SP（認証）			SP より認証を行う。 ・IdP に登録した ID を用いる。	IdP から BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく認証結果が表示されること。	○	

注）検証項目は、登録・認証の確認および基本動作の BioIDM 部分のみとし、BioIDM の初期化失敗については BSP の違いが影響しない為、省略する。

(4) セキュリティ機能

本項では、共通バイオメトリック認証基盤に組み込んだセキュリティ機能に関する検証項目と検証結果を示す。

① 検証環境

標準構成をベースとする。（試験別の差分については、試験項目に記載する。）

② 検証項目と検証結果

1) SSL での通信

BioIDMTransaction、BP、IdP、SP 間の通信が SSL で行われていることを確認する為、それぞれのアクセス URL のスキームが、SSL 用の https 又は wss であることを確認する。

表 5.16　SSL 通信に関する検証項目と検証結果

				検証結果	
No	パターン	画面	検証内容	結果	備考
1	BP	⇔ブラウザ　（画面表示）	BP の画面表示時、ブラウザに表示されている URL が、https://で始まっていることを確認	○	
2		⇔BioIDM Transaction（WebSocket 接続）	-	-	-
3		ユーザ登録時	BP の生体認証時、wss://で始まる URL で BioIDM Transaction へ接続が行われていることを確認 ※Javascript で接続を行っている為、ブラウザのデバッグ機能を用いて確認。	○	
4		IdP からのユーザ認証時	BP の生体認証時、wss://で始まる URL で BioIDM Transaction へ接続が行われていることを確認 ※Javascript で接続を行っている為、ブラウザのデバッグ機能を用いて確認。	○	
5		⇔IdP　（SAML レスポンス）	https://で始まる URL で IdP へ SAML レスポンスが行われていることを確認 ※IdP からの SAML リクエスト処理（org.wso2.carbon.identity.sso.saml.ui.SAMLSSOProvider.handleSAMLRequest()）で、SAML レスポンス先 URL が https://で始まることを確認	○	http_access のログで確認
6	IdP	⇔ブラウザ　（画面表示）	IdP の画面表示時、ブラウザに表示されている URL が、https://で始まっていることを確認	○	

7		⇔SP　（SAML レスポンス）		https://で始まる URL で SP へ SAML レスポンスが行われていることを確認 ※BP からの SAML レスポンス処理（org.wso2.carbon.identity.sso.saml.ui.SAMLSSOProvider.handleSAMLResponse()）で、SP への SAML レスポンス先 URL が https://で始まることを確認	○	
8		⇔BP　（SAML リクエスト）		-	-	-
9			ユーザ登録時	https://で始まる URL で BP に SAML リクエストが行われていることを確認 ※ユーザ登録画面の処理（org.wso2.carbon.identity.sso.saml.ui.SAMLSSOProvider.doPost()のコメント「ユーザ登録処理」部分）で、BP への SAML リクエスト先 URL が https://で始まることを確認	○	
10			SP からのユーザ認証時	https://で始まる URL で SP へ SAML レスポンスが行われていることを確認 ※SP からの SAML リクエスト処理（org.wso2.carbon.identity.sso.saml.ui.SAMLSSOProvider.handleSAMLRequest()）で、BP への SAML リクエスト先 URL が https://で始まることを確認	○	http_access のログで確認
11	SP	⇔ブラウザ　（画面表示）		SP の画面表示時、ブラウザに表示されている URL が、https://で始まっていることを確認	○	
12		⇔IdP　（SAML リクエスト）		-	- -	-
13			ユーザ登録時	https://で始まる URL で IdP に SAML リクエストが行われていることを確認 ※IdP 認証処理（saml.sp.servlet.ConsumerServlet.authRequest()）で、IdP への SAML リクエスト先 URL が https://で始まることを確認	○	
14			SP からのユーザ認証時	https://で始まる URL で IdP に SAML リクエストが行われていることを確認 ※IdP 認証処理（saml.sp.servlet.ConsumerServlet.authRequest()）で、IdP への SAML リクエスト先 URL が https://で始まることを確認	○	http_access のログで確認

注）接続を行う側からの確認。BioIDM Transaction は受信側の為、検証項目はない。（BP から接続できれば問題なし）

2)別ユーザでの実行

BioIDMTransaction、BP、IdP がそれぞれ専用のユーザで実行されることにより、データベースファイル、暗号鍵ファイルに他のユーザがアクセスすることができない為、セキュリティが向上する。試験では実際に別ユーザからアクセスが出来ないかを確認した。

表 5.17　別ユーザによる実行に関する検証項目と検証結果

				検証結果	
No	項目	パターン	検証内容	結果	備考
1	BioIDM	実行ユーザ	BioIDM Transaction が専用のユーザで実行されていることを確認（タスクマネージャからユーザ名を確認）	○	
2		ファイルアクセス	-	-	-
3		暗号鍵ファイル	ファイルのプロパティ→セキュリティタブで、BioIDM Iransaction 実行ユーザ以外にアクセス権がないことを確認	○	
4			BioIDM Iransaction 実行ユーザからはアクセスできることを確認	○	
5			管理者ユーザからはアクセスできることを確認	○	
6			一般ユーザからはアクセスできないことを確認	○	
7		データベースファイル	ファイルのプロパティ→セキュリティタブで、BioIDM Iransaction 実行ユーザ以外にアクセス権がないことを確認	○	
8			BioIDM Iransaction 実行ユーザからはアクセスできることを確認	○	
9			管理者ユーザからはアクセスできることを確認	○	
10			一般ユーザからはアクセスできないことを確認	○	
11	BP	実行ユーザ	BP が専用のユーザで実行されていることを確認（タスクマネージャからユーザ名を確認）	○	
12		ファイルアクセス	-	-	
13		暗号鍵ファイル	ファイルのプロパティ→セキュリティタブで、BP 実行ユーザ以外にアクセス権がないことを確認	○	
14			BP 実行ユーザからはアクセスできることを確認	○	
15			管理者ユーザからはアクセスできることを確認	○	
16			一般ユーザからはアクセスできないことを確認	○	
17		データベースファイル	ファイルのプロパティ→セキュリティタブで、BP 実行ユーザ以外にアクセス権がないことを確認	○	
18			BP 実行ユーザからはアクセスできることを確認	○	
19			管理者ユーザからはアクセスできることを確認	○	
20			一般ユーザからはアクセスできないことを確認	○	
21	IdP	実行ユーザ	IdP が専用のユーザで実行されていることを確認（タスクマネージャからユーザ名を確認）	○	
22		ファイルアクセス	-	-	
23		暗号鍵ファイル	ファイルのプロパティ→セキュリティタブで、IdP 実行ユーザ以外にアクセス権がないことを確認	○	
24			Idp 実行ユーザからはアクセスできることを確認	○	
25			管理者ユーザからはアクセスできることを確認	○	
26			一般ユーザからはアクセスできないことを確認	○	

27			データベースファイル	ファイルのプロパティ→セキュリティタブで、IdP 実行ユーザ以外にアクセス権がないことを確認	○	
28				Idp 実行ユーザからはアクセスできることを確認	○	
29				管理者ユーザからはアクセスできることを確認	○	
30				一般ユーザからはアクセスできないことを確認	○	

3)データ暗号化

BioIDMTransaction、BP、IdP において、DB へのデータ保存時に AES による暗号化が行なわれることを検証する。

表 5.18　データ暗号化に関する検証項目と検証結果

				検証結果	
No	項目	パターン	検証内容	結果	備考
1	BioIDM	データベース	-	-	-
2		BP ユーザ ID	暗号化が行われていること	○	
3		パスワード	暗号化が行われていること	○	
4		生体情報	暗号化が行われていること	○	
5	BP	データベース	-	-	
6		BP ユーザ ID	暗号化が行われていること	○	
7		パスワード	暗号化が行われていること	○	
8		ユーザ属性：nick name	暗号化が行われていること	○	
9		ユーザ属性：gender	暗号化が行われていること	○	
10		ユーザ属性：date of birth	暗号化が行われていること	○	
11	IdP	データベース	-	-	
12		IdP ユーザ ID	暗号化が行われていること	○	
13		BPURL	暗号化が行われていること	○	
14		BP ユーザ ID	暗号化が行われていること	○	
15		ユーザ属性：full name	暗号化が行われていること	○	
16		ユーザ属性：e-mail address	暗号化が行われていること	○	
17		ユーザ属性：postal code	暗号化が行われていること	○	
18		ユーザ属性：country	暗号化が行われていること	○	

(5) システム構成のバリエーション

本項では、その他の検証作業としてブラウザ（Internet Explorer10 に対する Chrome および Firefox）や、システム構成（標準構成に対する簡易構成）などといったシステムが取りえるバリエーションを変更した場合の共通バイオメトリック認証基盤の認証機能に関する検証項目と検証結果を示す。

① 検証環境

標準構成をベースとする。試験別の差分については、検証項目と検証結果の部分に記載する。

② 検証項目と検証結果

1) ブラウザの違い

IE10 以外のブラウザ用いた場合も、基本構成時と同様に認証が可能かを確認する。

特に Websocket を使用する BioIDM について確認を行う。

基本構成の使用ブラウザを以下の通り変更する。

ブラウザ	Chrome 32 (2014.1.27 時点での最新バージョン)
	FireFox 24 (2014.1.27 時点での自己署名証明書エラーを回避可能な最新バージョン)

(注) FireFox では、自己署名証明書をデフォルトで通さないため、初回アクセス時に、例外に追加することが必要である。また、BioIDMTransaction との WebSocket 通信(SSL)用の証明書を以下の手順で登録しておく必要がある。

1. Firefox メニュー「オプション」選択
2. 詳細タブの証明書タブから「証明書を表示」ボタンをクリック
3. サーバ証明書タブの「インポート」ボタンをクリック
4. BioIDMTransaction フォルダの「cacert.der」を選択→　一覧に登録される
5. 一覧から 127.0.0.1 を選択、「信頼性を設定」ボタンをクリック
6. 「この証明書が本物であると信頼する」を選択し、「OK」ボタンをクリック
7. 証明書マネージャウィンドウを「OK」ボタンクリックで閉じる
8. オプションウィンドウを「OK」ボタンクリックで閉じる

表 5.19　ブラウザを変更した場合の検証項目と検証結果

No	ブラウザ	画面	パターン	操作	検証内容	検証結果	
						結果	備考
1	Chrome	BP（登録）		BP より、生体認証を用いてユーザ登録を行う。	正しく登録されること。 （BioIDM の動作については、下記の通り詳細な確認を行う）	○	
2		BioIDM - メイン画面	初期表示	-	BioIDM の初期化中メッセージが表示されること	○	
3			BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない	遷移元画面に戻り、接続失敗のエラーダイアログが表示されること	○	
4			生体認証機器の初期化失敗	生体認証機器を接続しない	遷移元画面に戻り、機器初期化失敗のエラーダイアログが表示されること	○	
5			初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	部位選択（右手）が表示されること 「Capture」「Complete」ボタンが無効となっていること 「Cancel」ボタンが有効となっていること	○	
6				「Cancel」ボタンをクリック	遷移元の画面に戻ること	○	
7				「Left Hand」タブをクリック	部位選択（左手）が表示されること	○	
8				「Right Hand」タブをクリック	部位選択（右手）が表示されること	○	
9				任意の部位をクリック	「Capture」ボタンが有効となること	○	
10				「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
11				部位登録後、再度「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
12				「Complete」ボタンをクリック	BP の登録画面に戻ること その画面上に登録完了の旨のダイアログが表示されること	○	
13				登録完了ダイアログの「OK」ボタンをクリック	ダイアログが閉じること 右フレームが Sign-up 画面に遷移すること	○	

14			BioIDM - キャプチャ画面	初期表示	-		Enroll イメージ表示欄、TestVerify イメージ表示欄、メッセージ表示欄が表示されることメッセージ表示欄に Enroll ボタンをクリックする旨のメッセージが表示されること「Enrol」「Cancel」ボタンが有効となっていること 「TestVerify」「OK」ボタンが無効となっていること	○	
15					「Cancel」ボタンをクリック		BP の登録画面が表示されること	○	
16					「Enroll」ボタンをクリック		キャプチャ待ちとなること ・Enroll イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
17						生体認証装置に指定部位を置く(キャプチャ成功)	・Enroll イメージ表示欄に緑チェックアイコンが表示されること ・Enroll イメージ表示枠が緑になること ・Test Verify ボタンが有効ととなること	○	
18						再度「Enroll」ボタンをクリック	再度 Enroll を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
19						「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Enroll のキャプチャ待ちとなること	○	
20						「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
21						生体認証装置に指定部位を置く(キャプチャ失敗)	画面に変化が無いこと （引き続きキャプチャ中となる） ※QualityError の場合はメッセージが表示され、引き続きキャプチャ中となること。	○	
22						タイムアウト時	・Enroll イメージ表示欄に赤×アイコンが表示されること ・Enroll イメージ表示枠が赤になること	○	
23						再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	○	
24						「Cancel」ボタンをクリック	BioIDM のメイン画面に戻ること	○	

25					「Test Verify」ボタンをクリック			キャプチャ待ちとなること ・Test Verify イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
26						生体認証装置に指定部位を置く(キャプチャ成功)		・Test Verify イメージ表示欄に緑チェックアイコンが表示されること ・Test Verify イメージ表示枠が緑になること ・OK ボタンが有効ととなること	○	
27							再度「Enroll」ボタンをクリック	再度 Enroll を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
28								「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Enroll のキャプチャ待ちとなること	○	
29								「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
30							再度「Test Verify」ボタンをクリック		再度 Test Verify を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
31								「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Test Verify のキャプチャ待ちとなること	○	
32								「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
33						生体認証装置に指定部位を置く(キャプチャ失敗)			画面に変化が無いこと （引き続きキャプチャ中となる）	○	
34							タイムアウト時		・Test Verify イメージ表示欄に赤×アイコンが表示されること ・Test Verify イメージ表示枠が赤になること	○	
35								再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	○	

36							再度「Test Verify」ボタンをクリック	再度 Test Verify のキャプチャ待ちとなること	○	
37						「Cancel」ボタンをクリック		BioIDM のキャプチャウィンドウが閉じること	○	
38					「OK」ボタンをクリック			BioIDM のキャプチャウィンドウが閉じること メイン画面の「Complete」ボタンが有効となること	○	
39		IdP（登録）			IdP よりユーザ登録を行う。 ・BP に登録した ID を用いる。			BP での生体認証が正しく行われること。 IdP に正しく登録されること。 （BioIDM の認証動作については、下記の通り詳細な確認を行う）	○	
40			BioIDM - 認証画面	初期表示	-			BioIDM の初期化中メッセージが表示されること	○	
41				BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない			接続失敗の旨のエラーダイアログが表示されること	○	
42				生体認証機器の初期化失敗	生体認証機器を接続しない			機器初期化失敗の旨のエラーダイアログが表示されること	○	
43				初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく			キャプチャ待ちとなること ・キャプチャ結果イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること ・「Cancel」ボタンが表示されること	○	
44					「Cancel」ボタンをクリック			SAML 認証画面（ユーザ入力）に戻ること	○	
45					生体認証装置に登録した部位を置く			・メッセージ表示欄に認証成功のメッセージが表示されること・自動でウィンドウが閉じること・元画面が IdP の登録画面（ユーザ情報入力）に遷移すること	○	
46					生体認証装置に登録していない部位を置く			画面に変化が無いこと （引き続きキャプチャ中となる）	○	
47						タイムアウト時		・BP のユーザ入力画面に遷移すること ・認証失敗のエラーメッセージが表示されること	○	

48		SP（登録）		初期表示	SP よりユーザ登録を行う。 ・IdP に登録した ID を用いる。	IdP から BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく登録されること。	○	
49		SP（認証）			SP より認証を行う。 ・IdP に登録した ID を用いる。	IdP から BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく認証結果が表示されること。	○	
50	FireFox	BP（登録）			BP より、生体認証を用いてユーザ登録を行う。	正しく登録されること。 （BioIDM の動作については、下記の通り詳細な確認を行う）	○	
51			BioIDM - メイン画面	初期表示	-	BioIDM の初期化中メッセージが表示されること	○	
52				BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない	遷移元画面に戻り、接続失敗のエラーダイアログが表示されること	○	
53				生体認証機器の初期化失敗	生体認証機器を接続しない	遷移元画面に戻り、機器初期化失敗のエラーダイアログが表示されること	○	
54				初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく	部位選択（右手）が表示されること 「Capture」「Complete」ボタンが無効となっていること 「Cancel」ボタンが有効となっていること	○	
55					「Cancel」ボタンをクリック	遷移元の画面に戻ること	○	
56					「Left Hand」タブをクリック	部位選択（左手）が表示されること	○	
57					「Right Hand」タブをクリック	部位選択（右手）が表示されること	○	
58					任意の部位をクリック	「Capture」ボタンが有効となること	○	
59					「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
60					部位登録後、再度「Capture」ボタンをクリック	BioIDM のキャプチャ画面が表示されること	○	
61					「Complete」ボタンをクリック	BP の登録画面に戻ること その画面上に登録完了の旨のダイアログが表示されること	○	

62						登録完了ダイアログの「OK」ボタンをクリック	ダイアログが閉じること 右フレームがSign-up画面に遷移すること	○	
63			BioIDM - キャプチャ画面	初期表示	-		Enrollイメージ表示欄、TestVerifyイメージ表示欄、メッセージ表示欄が表示されること メッセージ表示欄にEnrollボタンをクリックする旨のメッセージが表示されること 「Enrol」「Cancel」ボタンが有効となっていること 「TestVerify」「OK」ボタンが無効となっていること	○	
64					「Cancel」ボタンをクリック		BioIDMのメイン画面に戻ること	○	
65					「Enroll」ボタンをクリック		キャプチャ待ちとなること ・Enrollイメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
66						生体認証装置に指定部位を置く(キャプチャ成功)	・Enrollイメージ表示欄に緑チェックアイコンが表示されること ・Enrollイメージ表示枠が緑になること ・Test Verifyボタンが有効ととなること	○	
67							再度「Enroll」ボタンをクリック	再度Enrollを行なうと､以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
68							「OK」ボタンをクリック	警告ダイアログが閉じ、再度Enrollのキャプチャ待ちとなること	○	
69							「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
70						生体認証装置に指定部位を置く(キャプチャ失敗)		画面に変化が無いこと （引き続きキャプチャ中となる） ※QualityErrorの場合はメッセージが表示され、引き続きキャプチャ中となること。	○	
71							タイムアウト時	・Enrollイメージ表示欄に赤×アイコンが表示されること ・Enrollイメージ表示枠が赤になること	○	

72							再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	○	
73						「Cancel」ボタンをクリック		BioIDM のメイン画面に戻ること	○	
74					「Test Verify」ボタンをクリック			キャプチャ待ちとなること ・Test Verify イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること	○	
75						生体認証装置に指定部位を置く(キャプチャ成功)		・Test Verify イメージ表示欄に緑チェックアイコンが表示されること・Test Verify イメージ表示枠が緑になること・OK ボタンが有効ととなること	○	
76							再度「Enroll」ボタンをクリック	再度 Enroll を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
77								「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Enroll のキャプチャ待ちとなること	○	
78								「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
79							再度「Test Verify」ボタンをクリック		再度 Test Verify を行なうと、以前のデータが無効になる旨の警告ダイアログが表示されること ダイアログには「OK」「Cancel」ボタンが表示されること	○	
80								「OK」ボタンをクリック	警告ダイアログが閉じ、再度 Enroll のキャプチャ待ちとなること	○	
81								「Cancel」ボタンをクリック	警告ダイアログが閉じること	○	
82						生体認証装置に指定部位を置く(キャプチャ失敗)			画面に変化が無いこと （引き続きキャプチャ中となる）	○	
83							タイムアウト時		・Test Verify イメージ表示欄に赤×アイコンが表示されること ・Test Verify イメージ表示枠が赤になること	○	

84							再度「Enroll」ボタンをクリック	再度 Enroll のキャプチャ待ちとなること	○	
85							再度「Test Verify」ボタンをクリック	再度 Test Verify のキャプチャ待ちとなること	○	
86						「Cancel」ボタンをクリック		BioIDM のキャプチャウィンドウが閉じること	○	
87					「OK」ボタンをクリック			BioIDM のキャプチャウィンドウが閉じること メイン画面の「Complete」ボタンが有効となること	○	
88		IdP（登録）			IdP よりユーザ登録を行う。 ・BP に登録した ID を用いる。			BP での生体認証が正しく行われること。 IdP に正しく登録されること。 （BioIDM の認証動作については、下記の通り詳細な確認を行う）	○	
89			BioIDM - 認証画面	初期表示	-			BioIDM の初期化中メッセージが表示されること	○	
90				BioIDM Transaction との接続失敗	BioIDM Transaction を起動しない			接続失敗の旨のエラーダイアログが表示されること	○	
91				生体認証機器の初期化失敗	生体認証機器を接続しない			機器初期化失敗の旨のエラーダイアログが表示されること	○	
92				初期化成功	BioIDM Transaction を起動しておく 生体認証機器を接続しておく			キャプチャ待ちとなること ・キャプチャ結果イメージ表示欄にキャプチャ待ちアイコンが表示されること ・メッセージ表示欄にキャプチャ待ちメッセージが表示されること ・「Cancel」ボタンが表示されること	○	
93					「Cancel」ボタンをクリック			SAML 認証画面（ユーザ入力）に戻ること	○	
94					生体認証装置に登録した部位を置く			・メッセージ表示欄に認証成功のメッセージが表示されること ・自動でウィンドウが閉じること ・元画面が IdP の登録画面（ユーザ情報入力）に遷移すること	○	
95					生体認証装置に登録していない部位を置く			画面に変化が無いこと （引き続きキャプチャ中となる）	○	

96					タイムアウト時	・BP のユーザ入力画面に遷移すること ・認証失敗のエラーメッセージが表示されること	○	。
97		SP（登録）	初期表示	SP よりユーザ登録を行う。 ･IdP に登録した ID を用いる。		・IdP から BP に認証の為のリダイレクトが行われること ・BP での生体認証が正しく行われること ・SP に正しく登録されること	○	
98		SP（認証）		SP より認証を行う。 ･IdP に登録した ID を用いる。		IdP から BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく認証結果が表示されること。	○	

2) システム構成の違い

標準構成時の IdP⇔BP 間についても SAML 準拠のプロトコルを用いて認証を行っている。理論上、SP から直接 SAML 認証を BP に発行しても正しく認証されるべきである為、簡易構成における検証を行った。

（標準構成との違い）

標準構成に対して簡易構成では SP から BP に直接通信を行う。

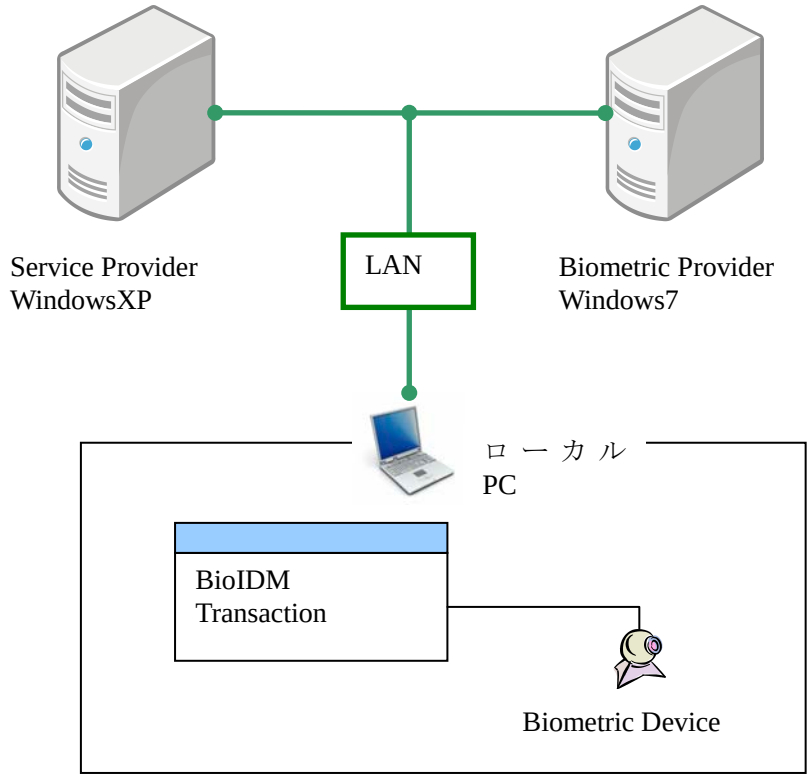
システム構成	簡易（SP、BP のみ） 

図 5.16 検証環境（簡易構成）

表 5.20　システム構成を簡易構成に変更した場合の検証項目と検証結果

					検証結果	
No	パターン	画面	操作	検証内容	結果	備考
1	登録	BP	BP より、生体認証を用いてユーザ登録を行う。	正しく登録されること。	○	性能測定（後述）と合わせて確認した
2		SP	SP よりユーザ登録を行う。 ・BP に登録した ID を用いる。	BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく登録されること。	○	同上
3	認証	SP	SP より認証を行う。 ・BP に登録した ID を用いる。	BP に認証の為のリダイレクトが行われること。 BP での生体認証が正しく行われること。 SP に正しく認証結果が表示されること。	○	同上

(6) 認証性能

本項では、共通バイオメトリック認証基盤のバイオメトリック認証性能に関する検証項目と検証結果を示す。

① 検証環境

前述の 5.3.2 節(1)①で述べた標準構成をベースとし、検証項目ごとに環境を変更する。

（検証項目別の環境の差分については、検証項目の説明を参照のこと。）

注） 性能測定は検証項目のパターン毎にそれぞれ 3 回行い平均をとる。

各検証のたびにブラウザのキャッシュをクリアすることとする。

時刻は全てブラウザの Javascript コンソールに出力する。

② 検証項目と検証結果

1) 標準構成での性能検証

① 概要

・インターネットを用いた標準（3 台）構成でのバイオメトリック認証性能の検証を行う。

・OpenID での認証性能との比較を行う。

・RP/SP⇒IdP⇒BP での認証時、UA にて各リクエストからレスポンスまでの時間を計測する。

注） OpenID 使用時は RP、SAML 使用時は SP

② 性能測定点

以下の箇所で計測する（すべて Chrome 内）

(a)UA より「①認証リクエスト」を RP/SP に向けて送信した時刻
(a1)IdP より「③ユーザ名入力画面」が送信され、UA が受信した時刻
(a2)UA より「④ユーザ名」を IdP に向けて送信した時刻
(b)BP より「⑥BioIDM へ認証要求」が送信され、UA が受信した時刻
→ 緑線ルートの時間を計測（UA からの認証リクエスト～レスポンス）

(c)BioIDMConnection から Transaction へ「⑦認証要求」を送信した時刻
(d)BioIDMTransaction からの「⑧認証応答」を Conenction が受信した時刻
→ 青線ルートの時間を計測（生体認証にかかる時間） ※パスワード認証の場合は無し

(e)UA より「⑨BioIDM からの結果応答」を RP/SP に向けて送信した時刻
(f)RP/SP より「⑫認証結果」が送信され、UA が受信した時刻
→ 赤線ルートの時間を計測（BioIDM からの結果応答～SP からの認証結果応答）

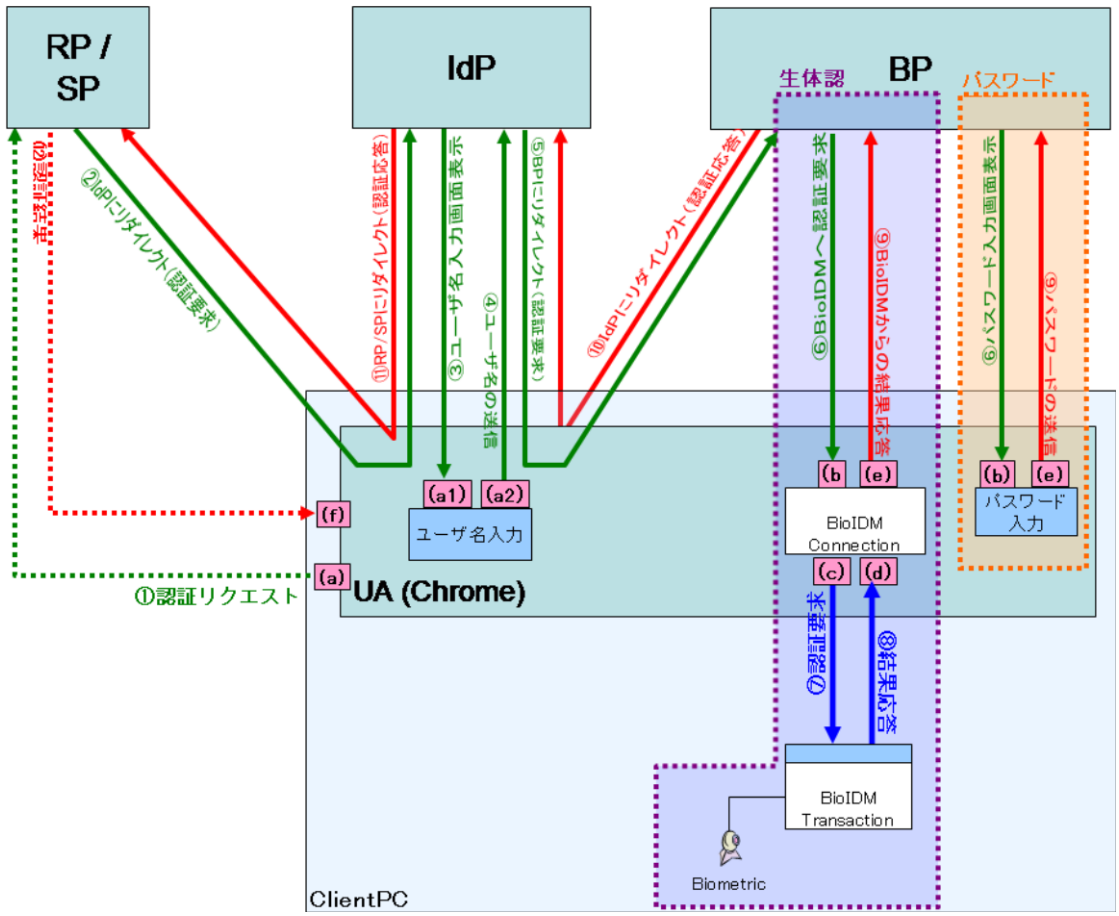


図 5.17　標準構成での性能検証の測定点

注) IE10 ではリダイレクトが行われるとデバッグウィンドウが閉じてしまう（設定を変更しても）場合があり計測結果の確認が困難な為、ブラウザとして Chrome を用いる。

表 5.21　性能検証におけるコンピュータ仕様

クライアント PC	WindowsXP Professional SP3 32bit Core2 6300(1.86Ghz) 2GB RAM
RP/SP	WindowsXP Professional SP3 32bit Core2 Duo E6850(3.00Ghz) 4GB RAM (3.25G 使用可)
OP/IdP	Windows7 Professional SP1 32bit Core i5-2500S (2.70Ghz) 4GB RAM (3.17G 使用可)
BP	Windows7 Professional SP1 32bit Core i5-2500S (2.70Ghz) 4GB RAM (3.17G 使用可)

表 5.22　標準構成における性能検証詳細条件

No	パターン				手順		計測地点
	暗号化	ブラウザキャッシュ	プロトコル	認証方式	画面	操作	
1	有	有	OpenID（ID 付与）※ユーザ名入力画面を通らないまたは SAML	生体認証	RP	RP メニューから「Login」ボタンをクリックし、ログイン画面を開く。 OpenID にパスワード認証ユーザの OpenID(IdP)を入力し、「Login」ボタンをクリック。 ※OpenID は IdP の URL のみ。ID は含まない。	(a)
2					BP - BioIDM 初期画面	-	(b)
3						-	(c)
4						生体認証機器で認証を行う。	(d)
5					BP	-	(e)
6					RP	-	(f)

③ 性能検証結果

本項の前述で示した性能検証環境における性能検証結果を、OpenID の場合と SAML の場合のそれぞれについて以下に示す。

表 5.23　OpenID での標準構成における性能検証結果（単位：秒）

No	性能測定箇所	区間	1 回目	2 回目	3 回目	4 回目	平均値（1～3 回目）	平均値（2～4 回目）
(1)	認証開始から終了までの総時間	(f) - (a)	09.916	07.453	06.341	07.355	07.903	07.050
(2)	UA 内認証時間	(e) - (b)	02.254	01.928	01.875	01.666	02.019	01.823
(3)	バイオメトリック処理時間	(d) - (c)	01.587	01.814	01.773	01.560	01.725	01.716
(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)	08.329	05.639	04.568	05.795	06.179	05.334
(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)	00.667	00.114	00.102	00.106	00.294	00.107
(6)	総時間から UA 内認証時間を引いた時間	(1) - (2)	07.662	05.525	04.466	05.689	05.884	05.227

表 5.24　SAML での標準構成における性能検証結果（単位：秒）

No	性能測定箇所	区間	1回目	2回目	3回目	4回目	平均値（1～3回目）	平均値（2～4回目）
(1)	認証開始から終了までの総時間	(f) - (a)	17.306	08.022	08.964	08.164	11.431	08.383
(x)	ユーザ名入力時間	(a2) - (a1)	07.311	02.911	03.063	02.578	04.428	02.851
(2)	UA 内認証時間	(e) - (b)	02.142	01.714	01.763	01.741	01.873	01.739
(3)	バイオメトリック処理時間	(d) - (c)	01.589	01.592	01.639	01.590	01.607	01.607
(4)	総時間からユーザ名入力時間とバイオメトリック処理時間を引いた時間	(1) - (3) - (x)	08.406	03.519	04.262	03.996	05.396	03.926
(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)	00.553	00.122	00.124	00.151	00.266	00.132
(6)	総時間からユーザ名入力時間とUA 内認証時間を引いた時間	(1) - (2) - (x)	07.853	03.397	04.138	03.845	05.129	03.793

注）　ユーザ名入力画面は存在しない。

2) 簡易構成での性能検証

① 概要

・インターネットを用いた簡易（２台）構成でのバイオメトリック認証性能の検証を行う。

・OpenID での認証性能との比較を行う。

・RP/SP⇒BP での認証時、UA にて各リクエストからレスポンスまでの時間を計測する。

注） OpenID 使用時は RP、SAML 使用時は SP

② 性能測定点

以下の箇所で計測する（すべて Chrome 内）

(a)UA より「①認証リクエスト」を RP/SP に向けて送信した時刻
(a1)BP より「③ユーザ名入力画面」が送信され、UA が受信した時刻
(a2)UA より「④ユーザ名」を BP に向けて送信した時刻
(b)BP より「⑥BioIDM へ認証要求」が送信され、UA が受信した時刻

} 緑線ルートの時間を計測
（UA からの認証リクエスト～レスポンス）

(c)BioIDMConnection から Transaction へ「⑦認証要求」を送信した時刻
(d)BioIDMTransaction からの「⑧認証応答」を Conenction が受信した時刻

} 青線ルートの時間を計測（生体認証にかかる時間） ※パスワード認証の場合は無し

(e)UA より「⑨BioIDM からの結果応答」を SP に向けて送信した時刻
(f)RP/SP より「⑫認証結果」が送信され、UA が受信した時刻

} 赤線ルートの時間を計測
（BioIDM からの結果応答～SP からの認証結果応答）

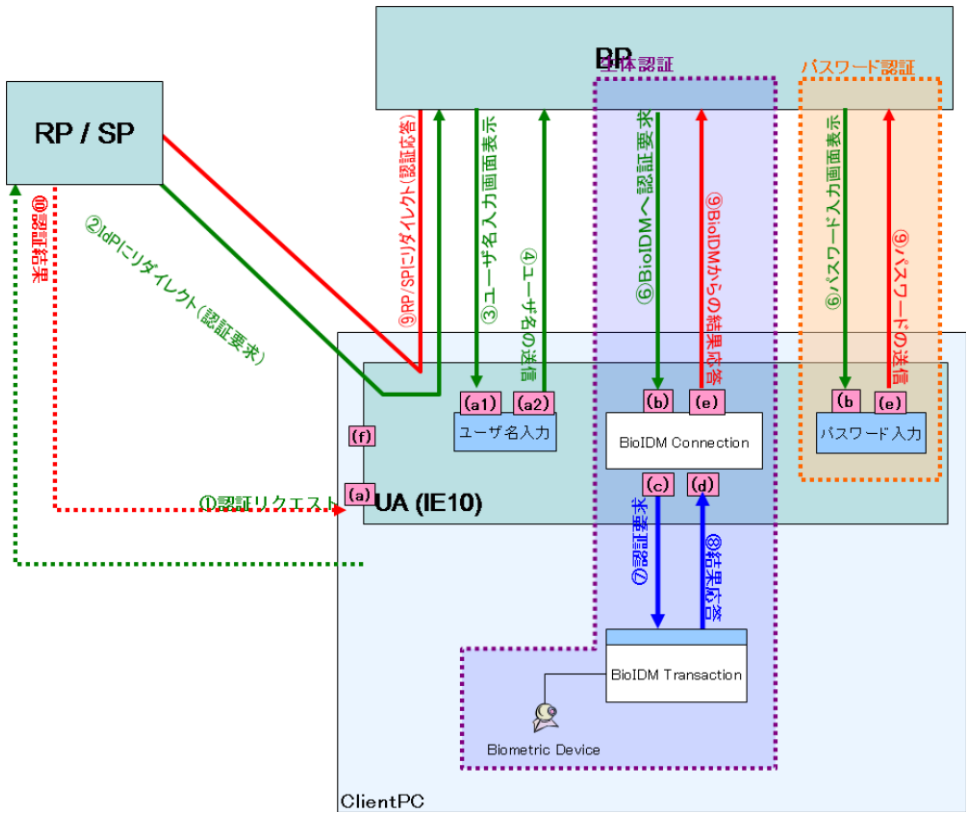


図 5.18　簡易構成での性能検証の測定点

表 5.25　簡易構成における性能検証詳細条件

	パターン				手順		計測地点
No	暗号化	ブラウザキャッシュ	プロトコル	認証方式	画面	操作	
1	有	有	OpenID（ID 付与） ※ユーザ名入力画面を通らない または SAML	生体認証	RP	RP メニューから「Login」ボタンをクリックし、ログイン画面を開く。 OpenID にパスワード認証ユーザの OpenID(BP)を入力し、「Login」ボタンをクリック。 ※OpenID は BP の URL のみ。ID は含まない。	(a)
2					BP - BioIDM 初期画面	-	(b)
3						-	(c)
4						生体認証機器で認証を行う。	(d)
5					BP	-	(e)
6					RP	-	(f)

表 5.26　OpenID での簡易構成における性能検証結果（単位：秒）

No	性能測定箇所	区間	1 回目	2 回目	3 回目	4 回目	平均値（1～3 回目）	平均値（2～4 回目）
(1)	認証開始から終了までの総時間	(f) - (a)	07.023	08.269	06.105	05.743	07.132	06.706
(2)	UA 内認証時間	(e) - (b)	02.284	01.789	01.770	01.766	01.948	01.775
(3)	バイオメトリック処理時間	(d) - (c)	01.633	01.637	01.615	01.614	01.628	01.622
(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)	05.390	06.632	04.490	04.129	05.504	05.084
(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)	00.651	00.152	00.155	00.152	00.319	00.153
(6)	総時間から UA 内認証時間を引いた時間	(1) - (2)	04.739	06.480	04.335	03.977	05.185	04.931

表 5.27　SAML での簡易構成における性能検証結果（単位：秒）

No	性能測定箇所	区間	1 回目	2 回目	3 回目	4 回目	平均値（1～3 回目）	平均値（2～4 回目）
(1)	認証開始から終了までの総時間	(f) - (a)	11.414	07.990	06.938	07.433	08.781	07.454
(x)	ユーザ名入力時間	(a2) - (a1)	05.874	03.247	02.454	02.694	03.858	02.798
(2)	UA 内認証時間	(e) - (b)	02.080	01.788	01.704	01.737	01.857	01.743
(3)	バイオメトリック処理時間	(d) - (c)	01.640	01.613	01.578	01.616	01.610	01.602
(4)	総時間からユーザ名入力時間とバイオメトリック処理時間を引いた時間	(1) - (3) - (x)	03.900	03.130	02.906	03.123	03.312	03.053
(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)	00.440	00.175	00.126	00.121	00.247	00.141
(6)	総時間からユーザ名入力時間と UA 内認証時間を引いた時間	(1) - (2) - (x)	03.460	02.955	02.780	03.002	03.065	02.912

(7) 性能検証結果考察

① 性能値の取り扱いについて

計測された数値はプロトタイプ環境を用いたものであり、サーバ用コンピュータの性能や使用したネットワーク性能にも依存する。また、測定方法としては、同じ操作を 4 回繰り返す方法とした。性能測定としては限定された環境および方法であるため、評価結果は目安として用いるべきものである。なお、OpenID および SAML の標準構成および簡易構成において測定された性能検証結果の各表の項目の中では、(4)として示される時間（各表においてアンダーラインで示す）に着目することとする。本時間は、認証開始から終了までの総時間の中から、端末上で ID 入力や生体認証のためにかかった時間を除いたものである。（ID 入力や生体認証は、人間よる操作時間であり、可変要素とみなす。）

② ブラウザのキャッシュ有無についての違いについて

性能測定は 3 回繰り返した平均値を算出しているが、1 から 3 回の平均値においては 1 回目の測定時点でブラウザ内のキャッシュがクリアされている。これに対して 2 から 4 回目の平均値においてはすべての測定においてブラウザ内のキャッシュにコンテンツがダウンロード済みである。このブラウザキャッシュの有無による性能差を考察する。SAML 技術を用いた場合、標準構成において、ブラウザのキャッシュ有無により約 37%の性能差が生じた。表中の(6)はネットワーク処理時間を表しているが、1 回目と 2 回目以降で約 2 倍の時間差があることがわかる。ブラウザにダウンロードされるコンテンツには、評価に使用した OSS である Identity Server のコンテンツと BioIDM Connection のコンテンツの 2 種類が存在する。これらのコンテンツのブラウザダウンロード時間がネットワーク性能に影響したものと推測される。このことから、1 回目の利用時の速度アップにおいてはブラウザコンテンツの簡略化が有効と思われる。

OpenID における性能差は約 16%であり SAML ほどの違いは見られなかった。これは測定 3 回目のネットワーク処理時間が他の時間に比べて短くなっていることから、ネットワーク性能の時間帯によるばらつきが可能性として考えられる。

③ 標準構成と簡易構成の違いについて

SAML 技術を用いた場合、簡易構成は標準構成に比べてブラウザキャッシュ無しの場合約 63%性能が高く、ブラウザキャッシュ有りの場合約 28%性能が高い。性能内訳を確認すると、1 回目の測定結果におけるネットワーク処理時間を表す(6)の差異が最も大きい。このことから、標準構成では 2 台のサーバ(IdP と BP)からブラウザにコンテンツをダウンロードする時間が、ブラウザキャッシュ無しの場合の大きな性能差を生んだ原因と推測できる。

OpenID の場合、SAML 技術を用いた場合ほどの差異は今回の検証では認められなかった。これはネットワーク処理時間の差異が今回の測定では大きくなかったためである。

④ OpenID と SAML の違いについて

標準構成において、ブラウザキャッシュ無しの場合（1 から 3 回の平均値)、SAML の方が OpenID よりも約 15%性能が高い。ブラウザキャッシュ有の場合、SAML の方が OpenID よりも約 36%程度性能が高い。各表の(6)の部分の時間が異なっていることから、性能差異の要因はネットワーク時間の違いによると言える。SAML においては特に 2 回目以降の時間が短縮される傾向があることがわかる。

5.3.3 まとめ

本 5.3 節では、共通バイオメトリック認証基盤のセキュリティに関連する機能の開発内容と検証実験の内容と結果について述べた。

(1) 開発内容

開発方針として本事業が当初目標としていた開発項目に対して前年度以前までに開発済みの機能を確認することにより、今年度の開発必要項目の洗い出しを行った。その結果以下の 3 つの機能の開発を行った。

① SAML 技術による SSO 機能への共通バイオメトリック認証基盤の組み込み

② 複数モダリティサポート機能としての指紋認証技術の組み込み

③ セキュリティ機能として格納データの AES アルゴリズムによる暗号化および Windows のアクセス権設定による暗号鍵保存ファイルの保護、および、SSL を用いた通信データのセキュリティの組み込み

(2) 検証実験

共通バイオメトリック認証基盤として開発した機能を確認するための検証実験を実施し、実装された機能が正常動作することを検証した。検証内容は以下のとおりである。

①登録機能：SAML 技術を用いた SSO システムにおける BP での ID 登録機能・IdP での ID 登録機能・SP での ID 登録機能

②認証機能：SAML 技術を用いた SSO システムにおけるバイオメトリック認証機能

③シングルサインオン機能：SAML 技術を用いた SSO システムにおける SSO 機能

④複数モダリティサポート機能：指紋認証技術による生体認証機能

⑤セキュリティ機能：5.2 節で示した格納データおよび通信データに関するセキュリティ機能

⑥システム構成のバリエーション：ブラウザを変更した場合、および標準構成から簡易構成に変更した場合のバイオメトリック認証機能

⑦認証性能：バイオメトリック認証を行った場合の処理時間を測定し、システム構成の違い（標準構成・簡易構成）、OpenID と SAML 技術の違いによる性能差の比較を行った。

25-121

平成 25 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 26 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