資料3

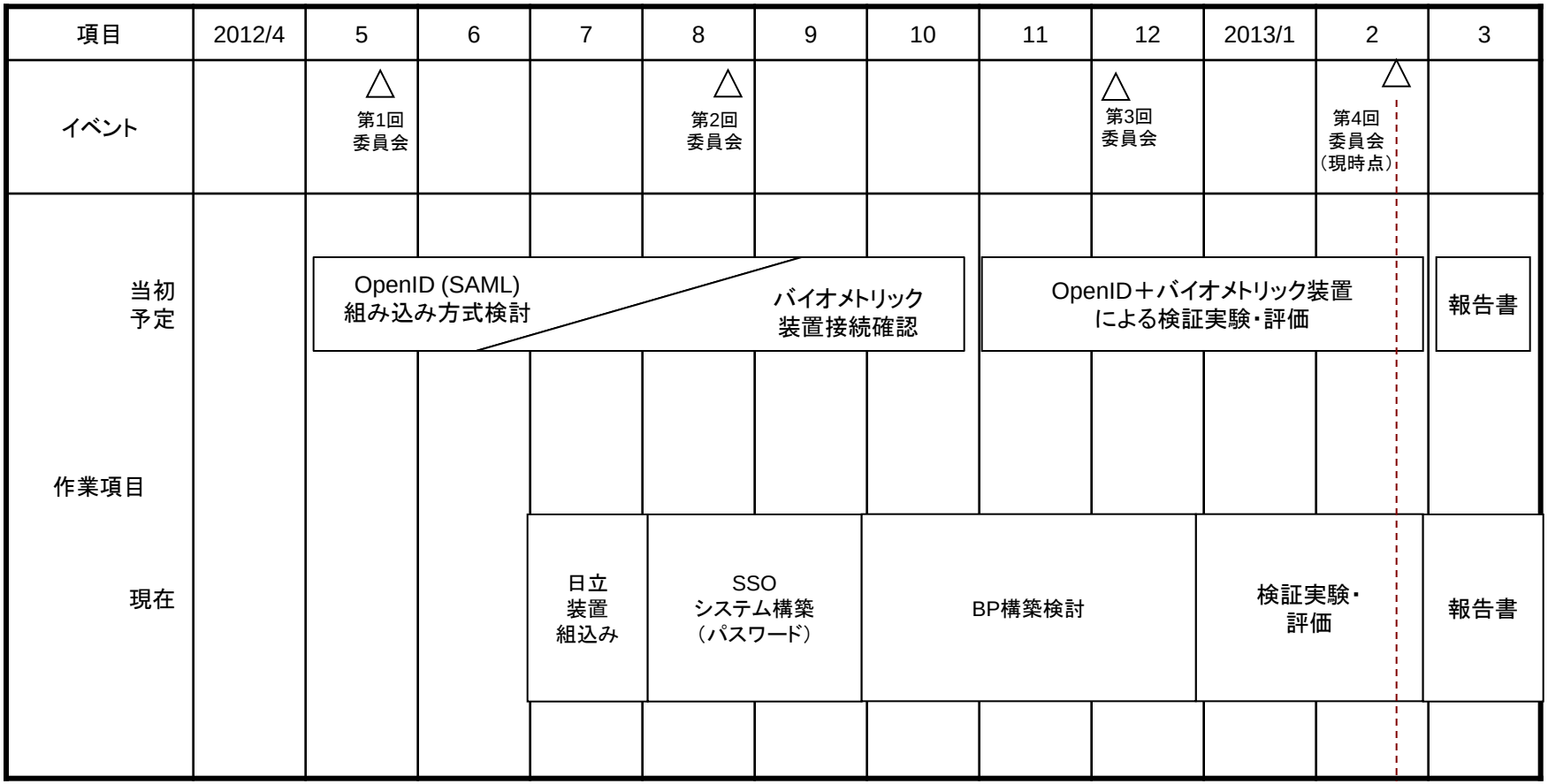
第4回　平成24年度 バイオ共通本人認証基盤検討委員会

バイオIdM
共通本人認証基盤システムの検討状況

2013年2月22日
OKIソフトウェア
中村敏男

1. 今年度の予定

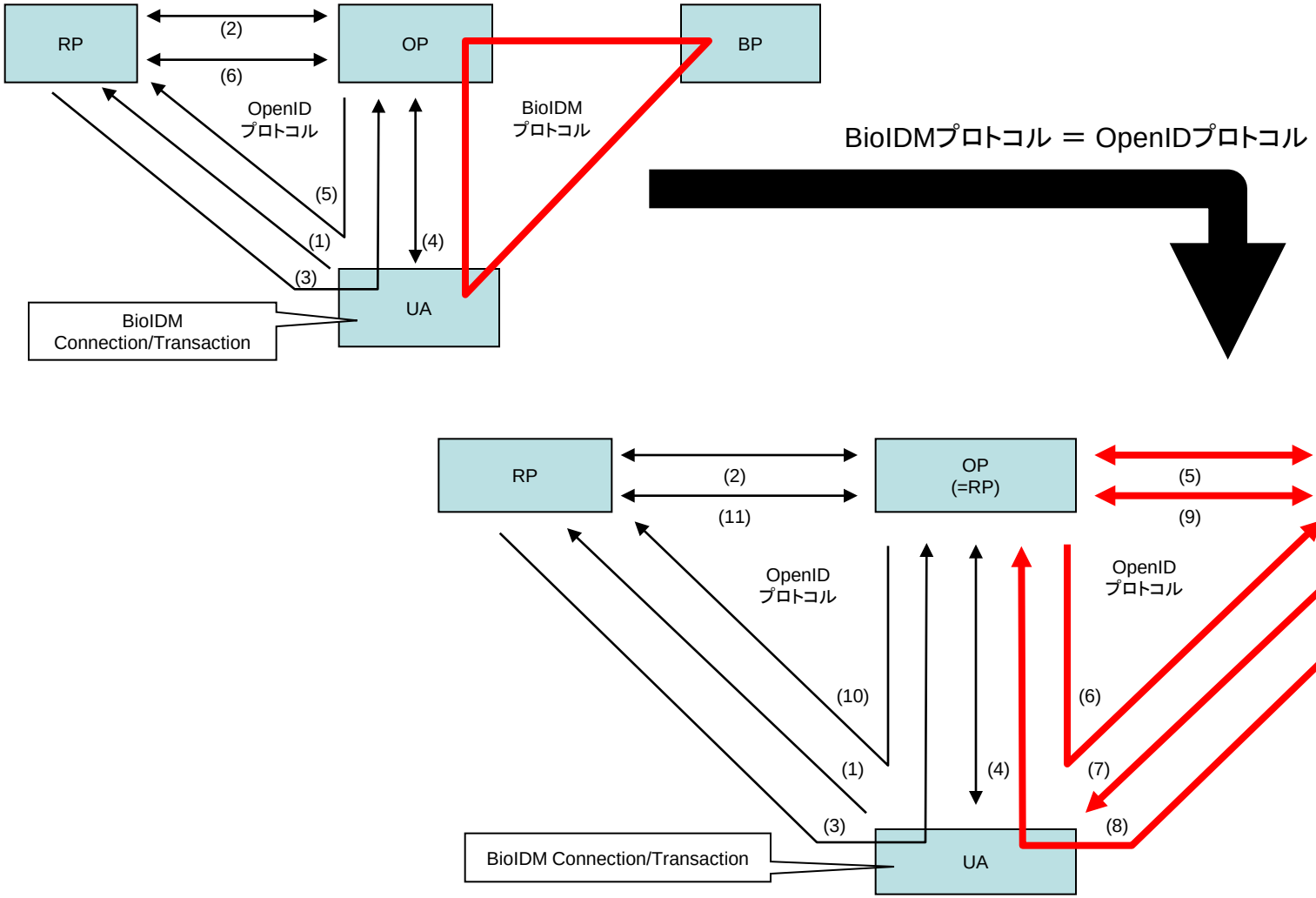
No	項目	状況
1	BioIDMとOpenIDとの接続	作業完了
2	バイオメトリック装置を用いた検証実験	作業完了
3	ACBioとの接続可能性検討	（2013年2月以降）



2. 前回報告内容

2.1 システム構成

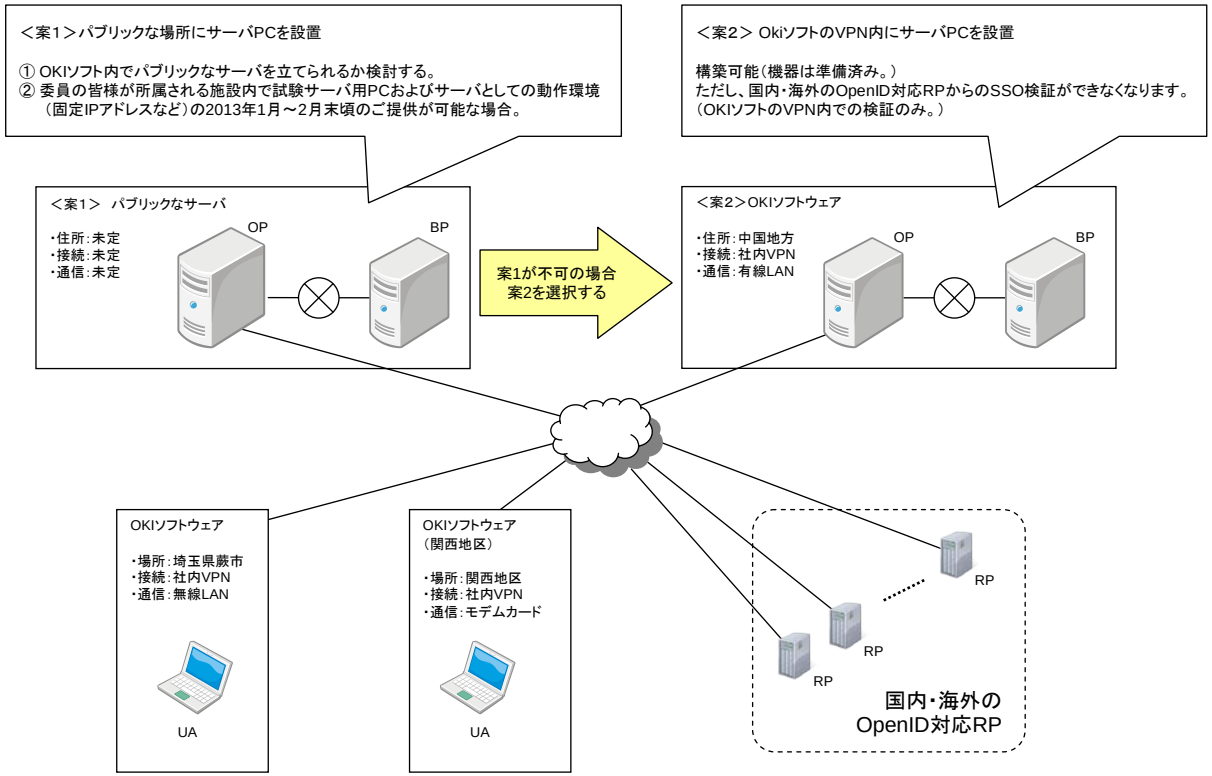
BioIDMプロトコル（OP-BP-UA間のプロトコル）は、OpenIDプロトコルを流用することとする。



2.2 検証実験のイメージ

本方式を採用した場合の検証実験は、下表の観点に着目してそれぞれの条件におけるシングルサインオンの機能検証および性能評価（速度評価）を行うこととする。

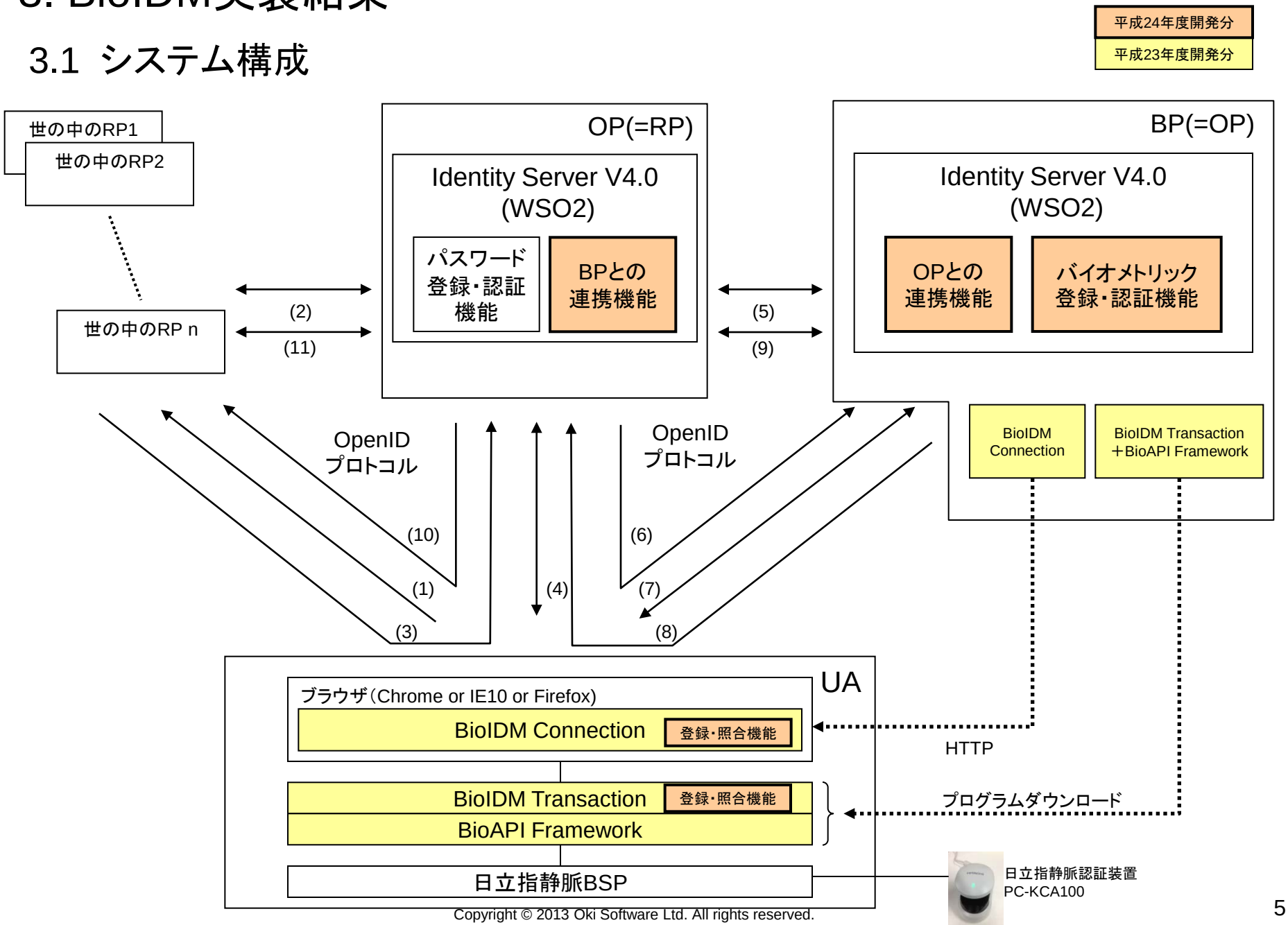
No	観点	内容	分類	検証対象
1	BSPの違い	指静脈・指紋(1)	UA	BioIDM Connection/Transaction
2	ブラウザの違い	Chrome・IE10・Firefox		
3	システム構成の違い	標準構成・簡易構成	BP	BioIDM Protocol
4	OpenID対応サイトの違い	評価用RP、国内・海外のOpenID対応サイト(2)	OP	システム全体（WSO2含む）



注：(1) 指紋装置を用いた実験可否については検討中
(2) 実験システムのOP,BPがパブリックな場所に設置できた場合のみ実施可能

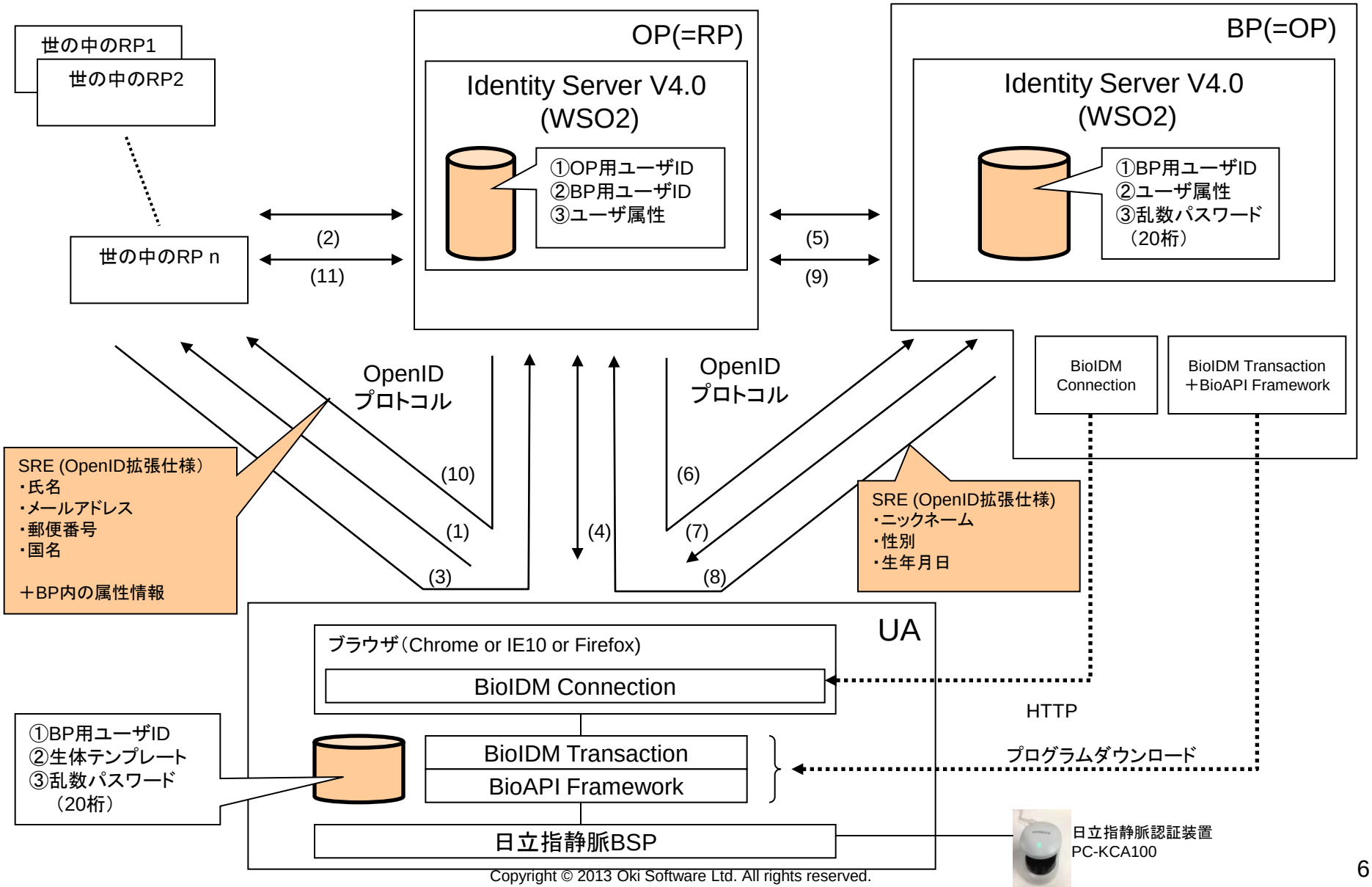
3. BioIDM実装結果

3.1 システム構成



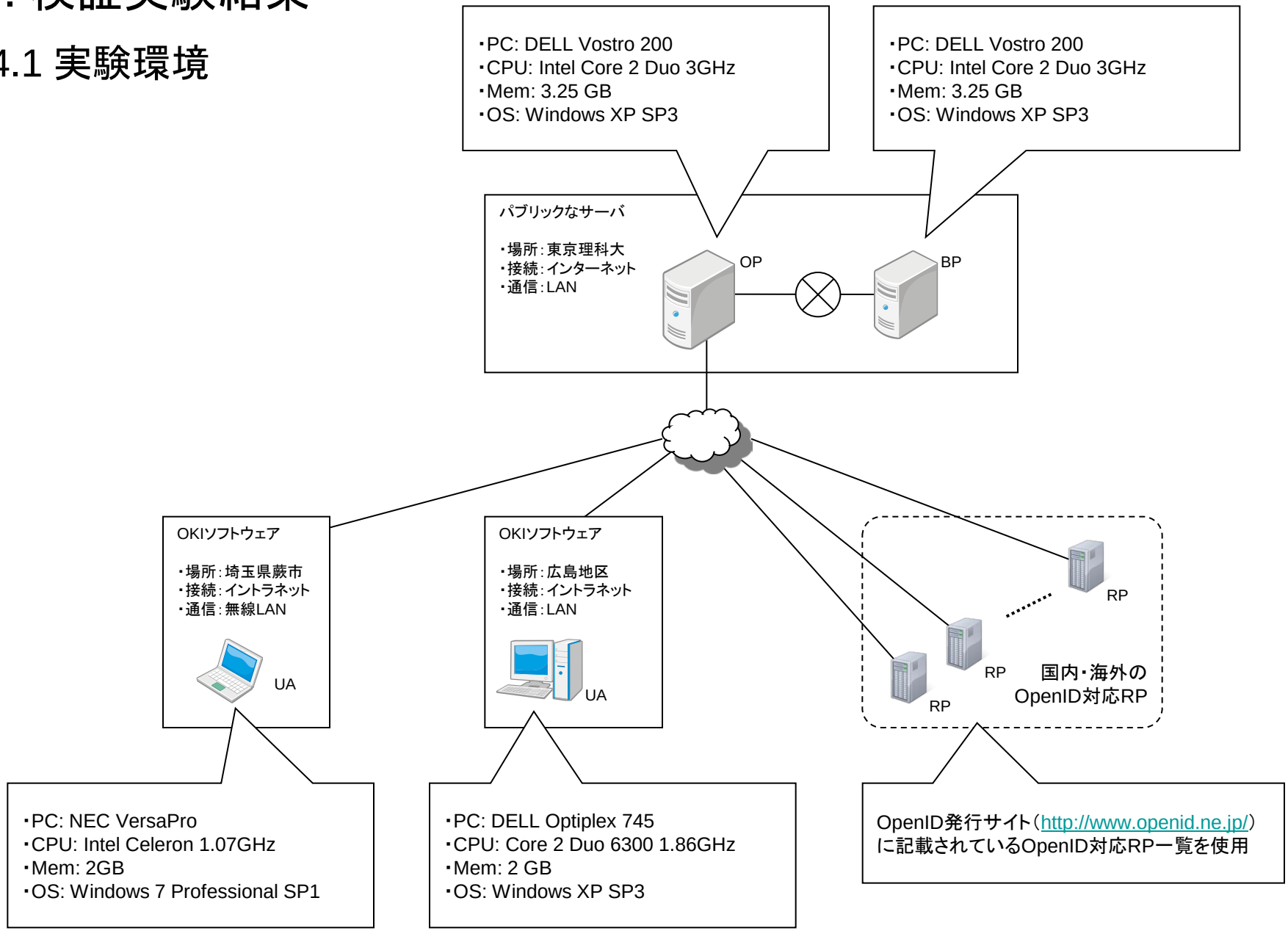
3. BioIDM実装結果

3.2 取り扱うデータ



4. 検証実験結果

4.1 実験環境



4.2 実験結果

(1) 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	標準構成試験	標準構成 (RP-OP-BP-UA)	Chrome	試験用RP	① 操作試験:167項目 ② SSO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。
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) 標準構成試験結果

① 操作試験: 一般的な操作周りの試験(ボタンの動作)、画面表示結果

② SSO試験1: 複数RP
- 2つのRPから同一のIDで認証依頼する
- 2つのRPから異なるIDで認証依頼する
＜結果＞ 正常: 同一IDの場合のみ、2回目は生体認証要求が行われない。

③ SSO試験2: 認証成功後OPが表示する認証許可画面
- ”Approve”ボタンを押した後の動作
- ”Approve Always”ボタンを押した後の動作
＜結果＞ 正常: Approve Alwaysの場合のみ、2回目は認証許可画面が表示されなくなる。

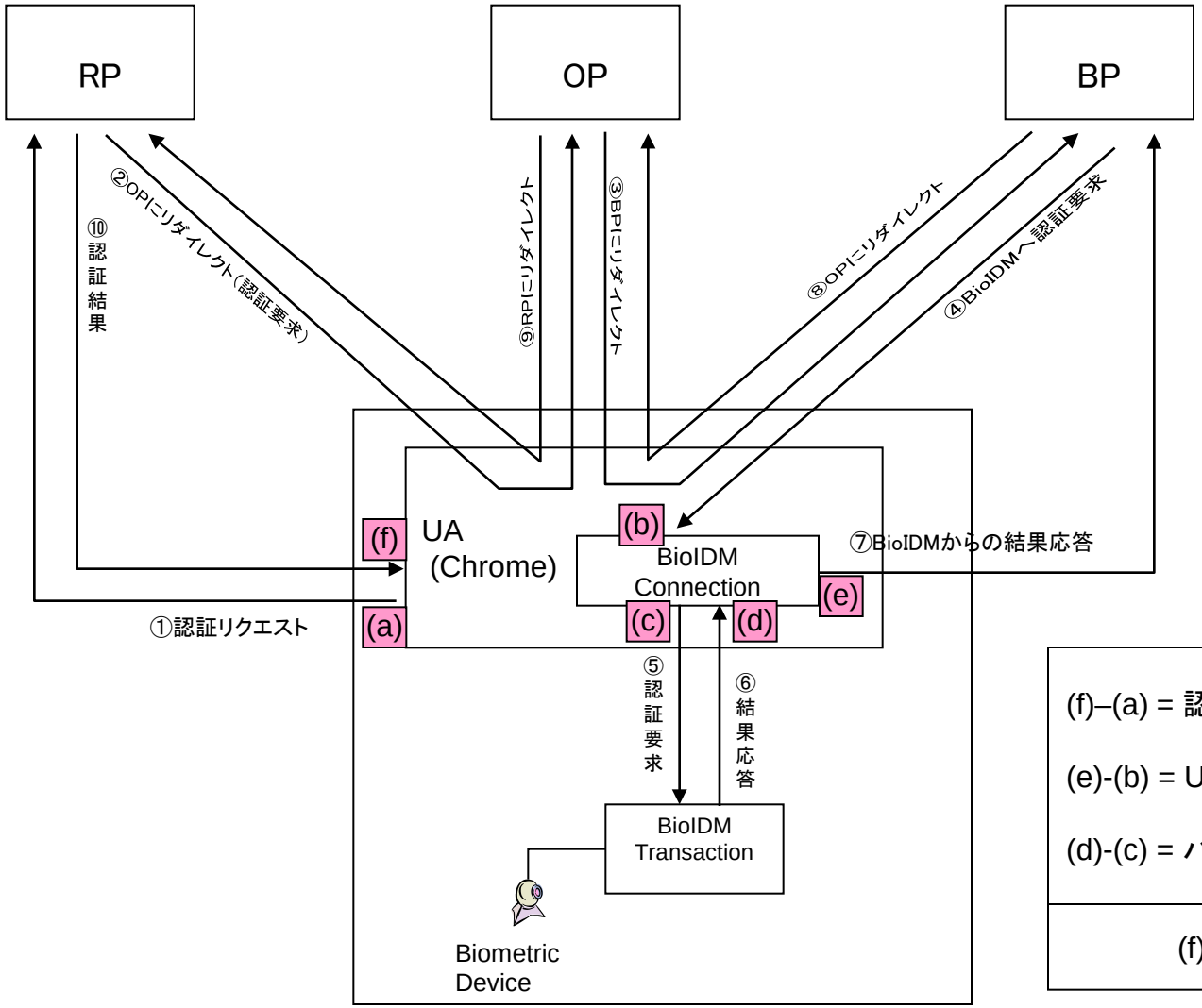
ただし、以下の制約がある。

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、次回以降の同一タイミングで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。

(2) 標準構成試験結果

④ 性能測定



(f)–(a) = 認証開始から終了までの総時間

(e)-(b) = UA内認証時間

(d)-(c) = バイオメトリック処理時間

(f)-(a) ＞ (e)-(b) ＞ (d)-(c)

※上記を3回計測

(2) 標準構成試験結果

＜性能測定結果＞

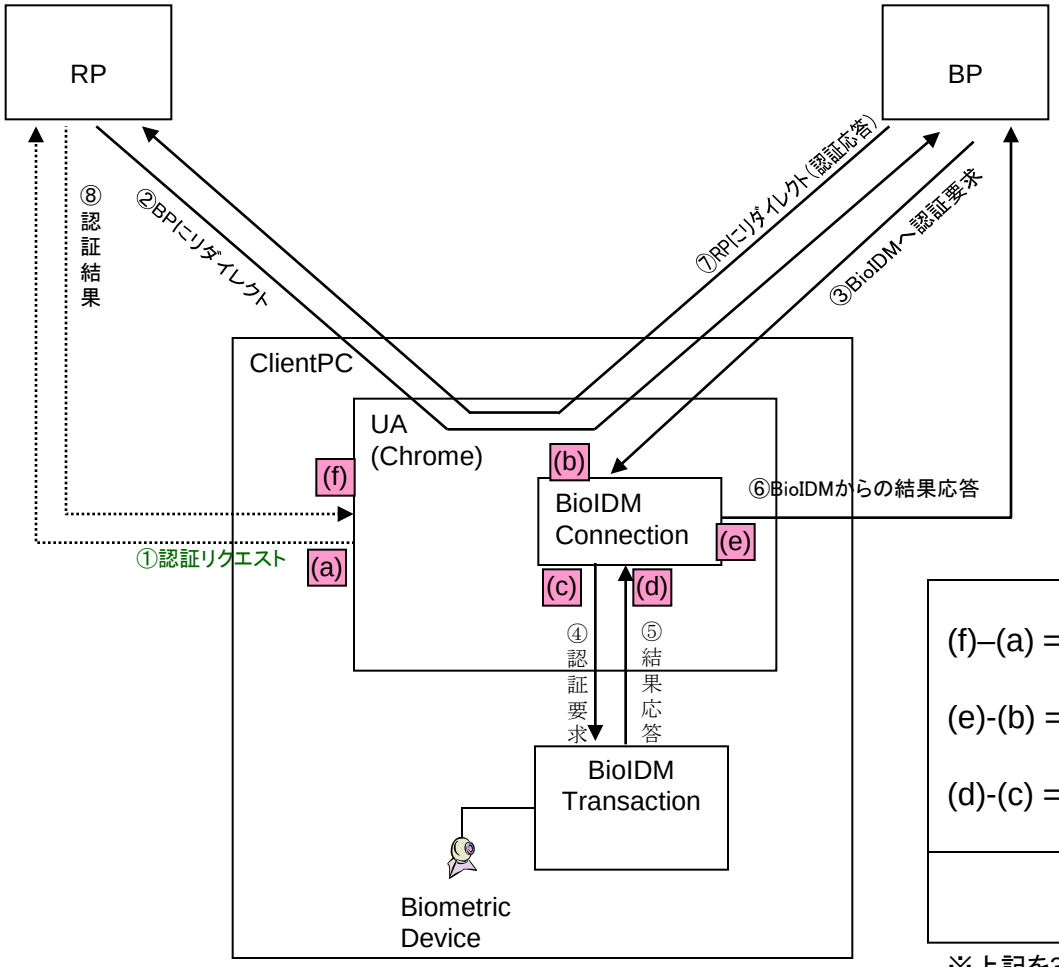
※ 計測時間は3回測定した平均値

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**	生体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BioIDM 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**	

(3) 簡易構成試験結果

① 操作試験：基本操作として、OPやBPへの登録および、RPを用いた認証操作試験を実施。

② 性能測定



(f)–(a) = 認証開始から終了までの総時間 (e)-(b) = UA内認証時間 (d)-(c) = バイオメトリック処理時間
(f)-(a) ＞ (e)-(b) ＞ (d)-(c)

※上記を3回計測

(3) 簡易構成試験結果

＜性能測定結果＞

※ 計測時間は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**	生体認証を除いたシステム処理時間
(4)	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BioIDM 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**	

(3) 簡易構成試験結果

③ 標準構成と簡易構成の性能測定比較

※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**

(4) ブラウザ試験結果

① ブラウザ試験用ブラウザ
Internet Explorer 10： Windows 7 Prerelease版
Firefox：バージョン18.0

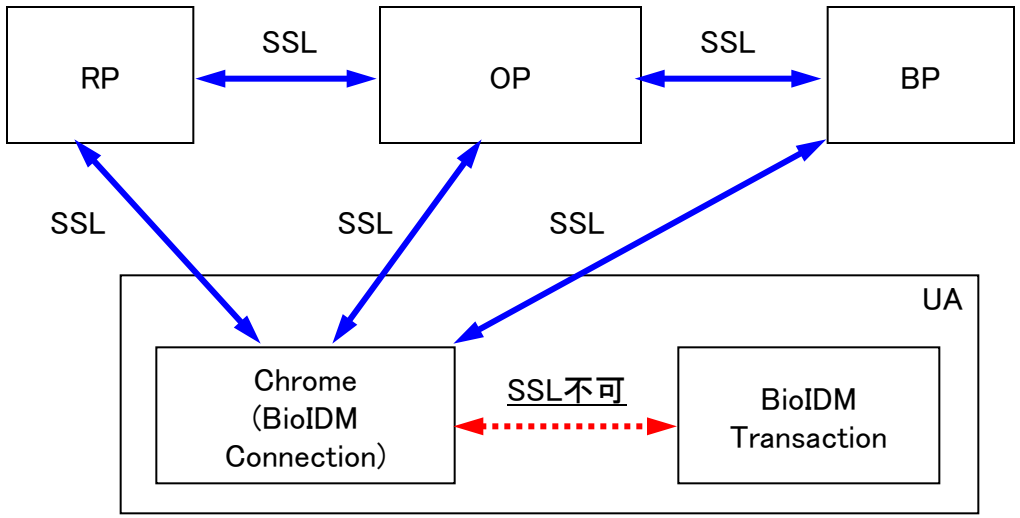
② 実施試験内容
・バイオメトリック登録処理および認証機能の試験：BioIDM Connection / Transaction間のWebSocket通信
・OpenIDプロトコルに関する試験：RP – OP – BP – UA 間のOpenIDプロトコルに関わる動作試験

結果

試験項目はすべて合格となったが、SSL対応に関して実装上の差異があることが判明した。
・BioIDMのWebSocketは現状SSL未対応（OSSがWebSocketに対応していないため）(1)
・ブラウザの種類によりSSLの扱いが異なっており、これがシステムの動作に影響を与える。

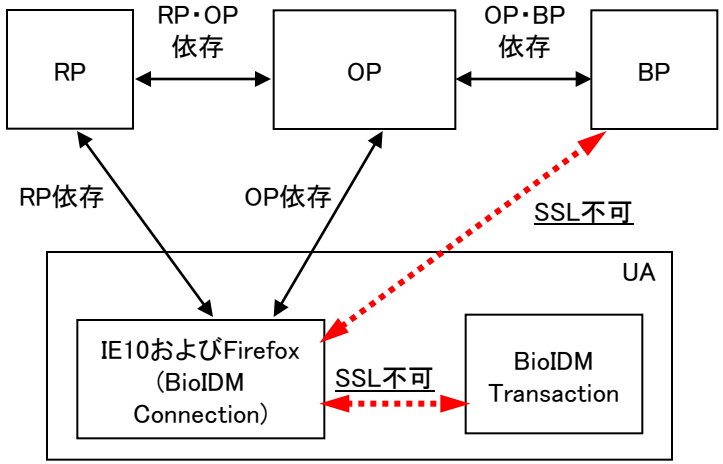
注) (1) WebSocketライブラリとしてwebsocket++ (http://www.zaphoyd.com/websocketpp)を使用

① Chromeの場合



(4) ブラウザ試験結果

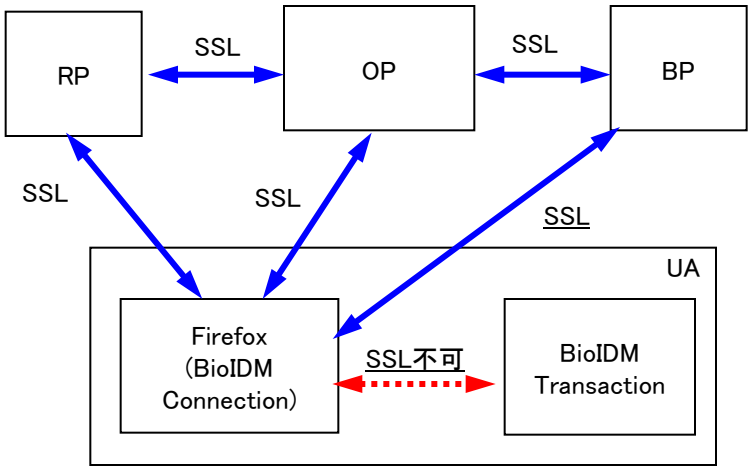
② IE10およびFirefoxの場合



Webサーバとブラウザがhttpsで通信している場合、SSLを用いないWebSocketは禁止される。

左記、実線矢印のプロトコルをSSL対応するためには各サーバの考慮が必要。
市販のWebサーバがSSLの有効無効を単一の設定でしか行えない場合、そのサーバを使用する限りSSLが無効になる。

注）使用したブラウザは以下のとおり
Internet Explorer 10： Windows 7 Prerelease版
Firefox：バージョン18.0



ただし、Firefox場合、ブラウザの設定値である、network.websocket.allowInsecureFromHTTPSを有効にすることにより本制限を回避できる。

(5) 国内外RP試験

OpenID発行サイト（http://www.openid.ne.jp/）

対象RP：18サイト

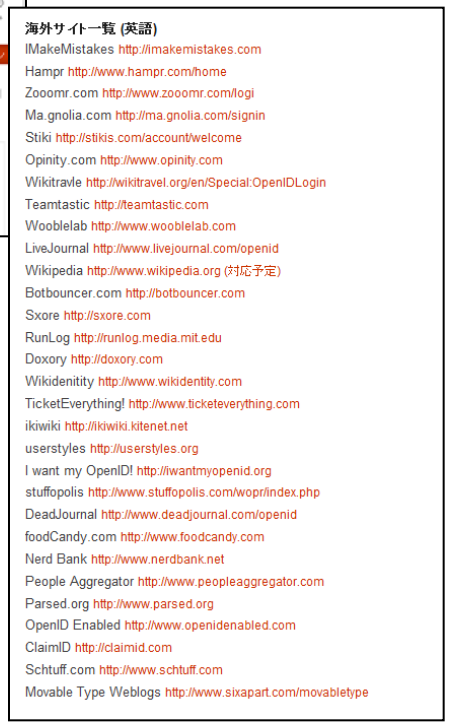
内訳：
・使用可能：5サイト(1)
・使用不可：3サイト
・リンク切れ：10サイト

注）(1) 5サイトのうち、条件付成功が2サイト

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のみ）
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
Haru.fm	http://www.haru.fm	対象外?	OPにリクエストが来ないため、使用可能なOPを限定している可能性あり。
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）
UPD.JP	http://upd.jp/	対象外?	OPにリクエストが来ないため、使用可能なOPを限定している可能性あり。
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。

(5) 国内外RP試験

OpenID発行サイト（http://www.openid.ne.jp/）



対象RP：30サイト

内訳：
・使用可能：2サイト
・使用不可：3サイト
・リンク切れ：25サイト

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	対象外?	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

5. まとめ

(1) 基本機能
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、生体認証を用いたOpenIDのSSOシステムを構築することができた。

(2) 性能測定
認証処理においてUAとOPおよびUAとBPの間のリダイレクト処理時間が大きいことがわかった。性能改善の可能性について今後検討する必要がある。

(3) ブラウザとSSL
BioIDM ConnectionとBioIDM Transactionの間のWebSocketにおいて、現状SSLが実現されていない。セキュリティ上およびシステム構築上の問題となるため、今後対応する必要がある。
※WebSocketのSSL対応版がOSSとして最近提供されたためBioIDMへの組み込みが可能となった。

(4) 国内・海外RP
一部のRPについて、本システムとの接続時にエラーが発生した。RPがOPを限定していると思われるケースが多かったが、原因の特定されていないものもあるため、確認が必要である。

平成25年度 作業	① 性能改善検討 ② WebSocketのSSL対応 ③ 国内外RPとの接続確認・検証 ④ ACBioの実装研究 ⑤ 震災時の本人確認システムの開発（サブワーキング検討結果）