平成24年9月13日

第２回　IdMにおける共通本人認証基盤の開発研究委員会 議事録

1. 日　時：平成24年8月24日(金)　　１５：００～１７：００

2. 場　所：一般社団法人 日本自動認識システム協会　B会議室

3. 次　第：

１．開会の挨拶		事務局	15:00 ～
２．配布資料の確認		事務局	15:01 ～
３．新任委員紹介		事務局	15:03 ～
４．議事		半谷委員長	15:05 ～16:55
1)	委員長挨拶	半谷委員長	15:05 ～15:08
2)	前回議事録確認	事務局	15:08 ～15:20
3)	バイオIdMシステムの検討および開発について	中村委員	15:20 ～16:20
4)	Biometrics 2012の調査について	瀬戸委員	16:20 ～16:30
5)	ドイツ・フランス状況報告	事務局	16:30 ～16:40
6)	作業委託について	事務局	16:40 ～16:45
7)	機器借用状況　(口頭)	事務局	16:45 ～16:46
8)	プロトタイプの提供について	事務局	16:46 ～16:50
５．事務連絡		事務局	16:50 ～17:00
1)	今後の日程		
2)	写真撮影など　(適宜)		

4. 出席者：(敬称略)

・委員長	半谷精一郎	東京理科大　工学部電気工学科
・委員	瀬戸 洋一	首都大学東京産業技術大学院大学
・委員	中村 敏男	(株)OKIソフトウェア　企画室
・委員	山口 利恵	産業技術総合研究所　セキュアシステム研究部門
・委員	菊地 健史	(株)日立ソリューションズ ﾌﾟﾗｯﾄﾌｫｰﾑﾌﾟﾛﾀﾞｸﾄ本部
・委員	坂本 静生	日本電気(株) 第二官公ソリューション事業部
・委員	福田 充昭	(株)富士通研究所 ソフトウェアシステム研究所
・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)
・委員	平野 誠治	凸版印刷(株) 事業開発・研究本部
・委員	山田 朝彦	東芝ソリューション(株) IT技術研究所
・オブザーバ	鎌倉　健	(株)富士通研究所 ソフトウェアシステム研究所
・オブザーバ	岩永 敏明	経済産業省　産業技術環境局　情報電子標準化推進室
・事務局	酒井 康夫	(一社)日本自動認識システム協会

5. 配布資料

資料1:　第２回ＩｄＭにおける共通本人認証基盤の開発研究委員会アジェンダ
資料2:　第１回ＩｄＭにおける共通本人認証基盤の開発研究委員会議事録(案)
資料3:　英国BC2012の調査について
資料4:　2012年7月ドイツ・フランス出張報告
資料5:　バイオIdMシステムの検討および開発について
資料6:　作業委託見積依頼書
資料7:　プロトタイプの提供について

6. 議事内容

1) 新任委員紹介

事務局より、経済産業省　産業技術環境局　情報電子標準化推進室　山中オブザーバの退省に伴い、同室より新任オブザーバとして岩永 敏明氏が就任された旨、報告があった。

2) 前回議事録確認

事務局より、資料２を用いて、ＩｄＭにおける共通本人認証基盤の開発研究委員会議事録を確認し、承認された。

3) バイオ IdM システムの検討および開発について

中村委員より、資料５を用いて、「バイオ IdM 共通本人認証基盤システムの検討および開発について」ご報告とご提案があった。

質疑応答と検討を行い、次の方針にしたがって今後開発研究を進めることが承認された。

(1) 今年度の具体的作業項目

(i) 開発研究

①電子認証システム関連規格調査

セキュリティ関連調査と検討のための SWG を立ち上げて検討する。

現在の委員からセキュリティおよび電子認証システムとの連携の検討に関係の深い委員に参加いただいたサブワーキンググループを立ち上げて検討を進める。

サブワーキンググループは、山口委員に中心になっていただき、坂本委員、平野委員、山田委員、中村委員、酒井で構成し、ボランティアとして開催(２回程度)する。

ただし、山口委員には、推進可能か持ち帰り検討していただき、結果をご連絡いただく。

②OpenID への BioIDM の組込み

提案と討議内容を参考にして、ローカルに保存したパスワードを生体認証で有効化するなどの方法にて OpenID システムへ BioIDM を組み込むことで検討と開発を進める。

ただし言葉、定義等の一般化を検討する。

これは中村委員に推進をお願いする。

③電子認証システム関連規格調査に基づいた基本設計

プロジェクトの成果を市場、業界に役立つものにするため、どのように展開してゆくのが良いのかなどの検討が継続して必要であり、また並行して電子認証システムの世界でのセキュリティの側面を考慮した検討も必要であるので、上記①の「電子認証システム関連規格調査」を踏まえながら、①で触れたＳＷＧにて、電子認証システムの世界のセキュリティ面を考慮した検討、また ACBio 的なものを適用して組み込めば十分であるかなどの検討も踏まえながら、電子認証システムとの連携のための基本設計として必要な事項を検討する。

この結果と今年度の「OpenID への BioIDM の組込み」における検討結果を突合せ、来年度以降の課題を見出すように進める。

(ii) 検証実験

上記「②OpenID への BioIDM の組込み」システムを検証するため、提案にしたがって進める。

[報告概要]

(1) 今年度の作業予定

下記と考えているとの説明があった。

(i)開発研究

① 電子認証システム関連規格調査

② OpenID へのBioIDMの組込み

（ローカルに保存したパスワードを生体認証で有効化する）

③ 電子認証システムに関わる規格調査に基づいた基本設計

(ii)検証実験

上記②のシステムに基づいた検証実験の実施

このうち、現在、「日立殿より借用の指静脈装置組込み」と「OpenID システムの構築（パスワードSSO)」の仕様検討が進んでいる。また今後「関連規格調査とセキュリティ方針の決定」に取り組みたいと考えているとのご報告があった。

(2) 電子認証システムとしての設計について

考えを整理するための要素として、「競輪補助事業として平成19年～21年の3ヵ年で調査したプロジェクトの成果の活用」、「米国政府系機関や国際標準化機関からすでに発行済みないし策定中の電子認証システムにおける本人認証に関するガイドラインの参照・活用」および「本プロジェクトで取り組む方向性(OpenID＋生体認証だけで考えるか、あるいは想定アプリケーション＋OpenID＋生体認証として考えるかなど)」を考えていることが説明された。その後、特に米国政府系機関や国際標準化機関からすでに発行済みないし策定中の電子認証システムにおける本人認証に関するガイドラインの内容について説明があった。

(3) プロジェクトの推進方針について

開発研究で取り上げた③電子認証システムに関わる規格調査に基づいた基本設計についての推進方針について、下記を検討対象として考えていることが説明された。

①想定アプリケーションを選択して、OMB M 04-04が定めるStep 1～Step 5を実行してみる

②SP 800-63で生体認証が用いられるレベル3ないしレベル4を想定してBioIDMを実装する

③生体認証をトークンとして用いるという考えを導入してSP 800-63を考え直す

(1) 生体情報をサーバに格納してサーバ認証する

(2) ACBioを採用する

(3) その他のアプローチ

また、その開発研究に向けた具体的作業項目として、下記の案が提案された。

① 電子認証システム関連規格調査

② OpenID へのBioIDMの組込み

ローカルに保存したパスワードを生体認証で有効化する

SP 800-63のレベル2あるいは1を想定してBioIDMを実装する

③ 電子認証システムに関わる規格調査に基づいた基本設計

有識者によるサブワーキングを立ち上げて検討を進める

[質疑概要]

[OpenIDへのBioIDMの組込みについて]

C1: 生体認証を間接認証的なフレームワークに乗せましょうというのが一番初めの目的であったと考えている。その間接認証というのが広く使われているのがSAMLとかOpenIDである。したがって、SAMLとかOpenIDにバイオメトリクスがどうやって接続できるかということに対応しましょうということで進めたという認識である。

早く形を作って強いところにくっついて実装していく方がより重要だと思う。

もっとスピード感をもってやらないといけないからもっと早めに開発を進めましょうということを言いたい。

Q1：C1コメントは、具体的に3ページに提示した線表だとこれは遅いということか。今年の末には

OpenIDとパスワードでつなぎましょうということになっているが、今年では遅いということか。

A1: 現計画で良いと思う。

Q2: 今年度の開発内容部で「パスワードをバイオメトリクスで活性化」する部分は、生体認証なしにパスワードを手でOpenIDプロバイダに入力したら、認証されるものなのか。
OpenID プロバイダのシステムに対して、保存されたパスワードを入力されたら認証されてしまうのか。

A2: プロトコル上でパスワードを流すということであれば、何か介入出来て、パスワードを流すことができれば、認証してしまう。

Q3: 今年度の開発内容部で「パスワードをバイオメトリクスで活性化」する部分は、生体認証でOpenID側に流すパスワードの流し込みを制御するものと思える。今年の開発部分にはセキュリティ的な検討が入っていないと思う。

Q4: 今の質問は、その流し込み部分に、IDとパスワードを知っているものが、流し込んだら認証されてしまうということか。

A4: 今年度の開発内容部で「パスワードをバイオメトリクスで活性化」する部分は、「IDとパスワード自動入力」する機能を持つソフトがすでにあるので、それと何が違うかを示すことができるかということを心配して聞いたものだ。

C2: 生体認証で「IDとパスワード自動入力」するものはないことはない。当社にもそのようなアプリケーションはある。決められた場所に記憶している「IDとパスワード」を入力するものである。
今年度開発するものについても、今あるものとの差を言うことが必要であろう。

C3: 来年度のACBioの組み込みを想定して、検討、設計しているということであれば、それはそれでいいのではないか。
この次のステップで作りこんだものがみんなに最終的に見せるものだろう。

C4: 次のステップに作りこむ段階で、どういうレベルに合わせてゆくのかということの表現方法をどれに合わせてゆくのかという話だと思う。そこを表現するのにひとの作ったものを活用するのは話が早い。また人にも説明しやすい。「IDとパスワード自動入力」と今の検討との違いを出すということについては、現状の標準のこのレベルに合わせていますという以外はあり得ないのではないかと思う。

C5: 今年度はパスワードと生体認証の組み合わせで開発するが、その中でもなにがしかの定義があったほうが良いと思う。そういた意味でもSWGの内容と意見交換しながら進めるのが良いと思う。

C6: 今年度はパスワードに限定しなくてはならないのか。ハードウェアトークンのアクティベートなどは考えられないのか。

C7: 今年度は実装のしやすさ、速やかに動くものを見せられるということから、対応できるハードウェアトークンが入手しやすいのであれば考えられるが・・・・。

C8: バリエーションがつけられることを示すことができると良いと思う。今のままではパスワードだけでは、今ある「IDとパスワード自動入力」のとの違いがない、所詮パスワードレベルということで受け入れられがたいのではないか。
銀行系では強い方、民生用途であれば使い勝手を優先して自動パスワード機能が選択できるというバリエーションがあることが魅力になるとと思う。

C9: 少なくともパスワードということは避けたほうが良い。もっとジェネラルな言葉にしないと誤解を招く。あとは実際に違うもので見せられるということがポイント。

C10: 身分を証明するものとして、パスワードを使ってはどうか。

C11:定義されている言葉をつかってはどうか。トークンとか、アサーションとか。より一般性が上がる。

［電子認証システム関連規格調査と基本設計について］

C1：SP800-63のような他人が作った、使われてもいないものを検討し、採用して意味ないと思う。

C2：開発のスケジュール自体は当初計画のそのまま続けているので、「関連規格調査セキュリティ方針決定の実施」検討をしたから開発のペースが遅くなるということはない。

C3：OpenIDで、SP800-63のようなものは使わないのではないか。

C4：OpenID独自でやっていたら米国政府と接続ができないので、OpenIDの人たちもSP800-63のレベル2、レベル3ベースで作成をするという認識でおり、そこをSP 800-63ベースで考えている。決してOpenIDはSP800-63をみてないとか、SAMLはみてないとか、そういうことはない。SAMLもこのベースで作っている。

OpenIDのほうは独自のことを進めすぎていて、SP800-63とのつながりがなくなりすぎているので、戻しているという感じがある。

OpenIDの進め方にあわせるのかどうか。ただ、厳格なやり方をする必要まではないと考えていて、軽くこういう考え方のレベル分けを理解しておいて、例えばレベル４と生体認証は接続が良さそうだということを理解してそのやり方を考えるというのが筋としてはいいと思う。考える途中でSP800-63を一度見るのはしかたないが細かく理解する必要はないだろう。

C5:その通りだろう

Q1：SP800-63自体は実際に参照されているものではあるのか。電子認証システム向けで実際に参照されているのか

A1：米国政府によって採用されている。かつ日本政府によってSP800-63に合わせた政府認証ガイドラインというのがあって日本政府なりにオリジナルから変えたものが存在している。

C6：OpenIDは2と3で使おうとしているのに、生体認証はレベル４でもともとレベルが合っていないので、OpenIDとつなげるのはそこまで筋がよいものなのか、それよりもSAMLの方が筋がいいかというのをもう一度考えた方がよいと思う。

Q2：生体認証はレベルを上げるために用いられているのか。生体認証単独ということは考えられていないのか。

A2：SP800-63では生体認証単独ということは、現在カバーしていない。生体認証を電子認証で用いるための評価をNISTが計画しているとは記載してある。

SP800-63には、ただバイオメトリクスだけを使えばレベルが上がると書かれているだけで、精度や信頼性についての記述は存在していない。

C7：SP800-63の世界では生体認証はパスワードの代替にはなりえない、レベルを上げるために使うというのは我々の常識なのではないか。

C8：ハードウェアトークン、パスワードトークン、ワンタイムパスワードデバイスは既存のものがあって、それに生体認証をどういう形で転用することによってレベルをあげられるというストーリーを考えられているのか、いまひとつピンと来ない。

生体認証を付け加えることによって鍵長が例えば長くなるからよりレベルが上がるというような話であれば素人的にはわかりやすくなる。

リモート認証プロトコルには生体認証は適さないということであれば、サーバに送るような形では生体認証は使わないということとなり、ローカルなトークンまたはデバイスに対して何かしら付け加えるという使い方となる。

しかし、まだその方法自体は具体的には示されていない。

元に戻ると、今はローカルで認証してOpenID用のパスワードをアクティベートすると考えているけれど、そのこと自体は問題にはならない。

C9：そもそも現状使われている認証アーキテクチャの中にバイオメトリクスをどうやって組み込むかというのはローカル認証だとか直接認証とかそういうやり方しかない。

それはもうさっきのNISTの資料に載っていた様にバイオメトリクスというものはパスワードとか暗号鍵と同等に扱われるべきものではないということである。

セキュリティレベルを上げるためのものではあるけれど。

C10: トークンとかデバイスやパスワード認証はあるがこれらはレベル2や3に割当てられている。生体認証を実際に適用することでレベルが上がっていることを示すときに、レベル２や３のものがちゃんとレベル４に上がっていることを具体的にどのように示すかが一番重要で、それができればいろんなIDシステムに適用してもよい、ということになると思う。
逆に言うとレベルがあがるということを定量的になり、定性的になり示さないとこの委員会ではいけないのではないかと思う。
その定量的、定性的に示すというのは例えば生体認証そのものの精度であったり、確かに生体認証が正しく行われたということを示すACBioであったり、他のものもあるかもしれないが、そういうものでちゃんとレベルが上がることを示すことではないか。
ここでは、生体認証そのものをトークンとして使うことまでは言っていない。そもそもトークンと併用するという使い方でよいのかというのも疑問が残るが、シナリオに基づくとトークンとして生体認証を用いるというのはないので、ある意味前提条件としてそれはそれでよく、プラスアルファでちゃんとレベルが上がるというのを示すのが現在のシナリオに合致すると考える。これはバイオメトリクス業界の方向にも大まかに合致するかもしれないと思う。

C11: SP800-63には、ただバイオメトリクスだけを使えばレベルが上がると書かれている。精度や信頼性についての記述は存在していない。

C12: 認証のレベルというか、そのレベルがどの程度にあるかということを評価するという側面がある。OpenID全体としてはレベル２とかレベル３を考えており、今回のシナリオで初期認証の部分はパスワードを発行するのにバイオメトリクスで活性化するということになると、SP800-63により、初期認証に用いるものはレベルいくつであるということが言えて、バイオメトリクスとしての組み合わせると、その結果として全体としてはどのレベルなのかというのが結論できてしまうのではないかと思う。
現在のシナリオではパスワードそのものを最終的には評価として用いるとなっており、ワンタイムパスワードとかではない、それらをどう考えるかというのが今後あると思う。

C13:それはSP800-63あり得ない組み合わせになってしまっている。

C14: 多分リスクが違うところにあるものを補完するということになるのではないかと思う。

C15: パスワードについては乱雑さだとかそういうものからリスクの確率が表現できます。もしこのパスワードをバイオメトリクスで有効化してしまうとパスワードの信頼性がバイオメトリクスに依存してしまうことになり、いくらパスワードの桁数をあげても意味が無くなる。
したがって生体認証の信頼性を定量的に表現するにはどうするかという問題が起きてくる。

C16: となると、SP800-63ではただレベルが上がるとさらっと書いていて中味がない。でそれはぜんぜん良くなくて、また精度が良いものと悪いものを一緒くたにすることはナンセンスなので、リスク・要件に対してちゃんと分析し、生体認証はここのところがあがるからレベルが上がるということをちゃんと書くようにしていくことが必要ではないか。

C17:それはSP800-63に次の課題としてこの文書では示されている。

C18: 積極的に表現すると、NISTに提案できるようなリスク・要件分析をやりましょうということになります。

Q3: プロジェクトの狙いは、「NISTに提案できるSP800-63ダッシュ的なもののバイオメトリクスの部分を検討する。そこにはバイオメトリック認証という部分を追加しており、レベルいくつまでいくと記載することを狙う」ということになるのでしょうか。

C19: OpenIDファウンデーションに提案するのはないのか。NISTに提案したってなんの役にも立たない。我々はビジネスをやろうとしている。そういうものは結果論でつければいい話であって、ビジネスや市場を作りたい。

C20: OpenIDがレベル２やレベル３までしかターゲットにしていなら、生体認証を入れることによってレベル４までカバーできると言ってあげた方が、生体認証としては存在意義がでると思う。

[今後のプロジェクトの方向について]

C1: そもそも現状使われている認証アーキテクチャの中にバイオメトリクスをどうやって組み込むかというのはローカル認証だとか直接認証とかそういうやり方しかない。
それはもうさっきの NIST の資料に載っていた様にバイオメトリクスというものはパスワードとか暗号鍵と同等に扱われるべきものではないということ。セキュリティレベルを上げるためのものではあるけれど。
だから現状の広く使われている認証というのは間接認証タイプだから、間接認証にバイオメトリクスをどう組み込むかというのが出だしだった。
SAML でやるか OpenID でやるかはいろいろ問題があるが、とりあえず一番開発しやすい方法でやったほうがよいと思う。
OpenID＋バイオメトリクスが最良の形態ではないかわからないが、間接認証にバイオメトリクスを組み込むとこんな形になるというのを見せる、というのが目的ではないか。
OpenID が SP800-63 とコネクションをもっているとか、SAML がもっているとかいうことは、それは SAML とか OpenID の世界でやってもらえばいい話であって、現状は間接認証の中にバイオメトリクスをどうやって組み込むかというのが最初の出だしだったのではないかと思う。

C2: そういう意味では OpenID も紹介いただいた OSS を用いて構築中である。バイオメトリクスを組み込むということでは作業を進めている。

C3: OpenID にバイオメトリクスを組み込んでパスワードを活性化させようというのはいいが、そのバイオメトリクス自体の信頼性をもうちょっと向上するために ACBio 的なところも組み込めば新しいプロトタイプの姿を示せるのではないか、という話で進んでいたのではないか。
ここでは製品開発をしているのではなくてフィージビリティスタディをしているのであって、最初に OpenID が最適なのか SAML が最適なのかそれはわからない。それは各企業が製品開発のときに考えてもらえばよい。
今年度行う鍵の活性化という形でバイオメトリクスを実装し、次にテンプレートの信頼性を確保するために ACBio みたいなものをくっつけるということが本当にできることを示すことがスタートラインだったと思う。

C4: BioAPI とか国際標準にこだわりすぎているのも問題かと思っている。それも結果論的にもっていければいいのであって、私が最初に言ったのはまずプロトタイプを作ってそのあと細かなところはあとから作っていくというのがよいということ。BioAPI 関数ありきではなくて、新しい BioAPI を提案するように、まずはまっさらな状態ではじめたほうがよいのではないか。

C5:その部分に関しては前年度においてそういった枠組みをすでに作ってある。

C6: バイオメトリクスを運用するシチュエーションというのはどういうものかを考える必要がある。
私の理解では、バイオメトリクスはすごく厳格なサービス、厳格に認証を行わなければならないサービスにおいて利用するものであるという前提があるので、パスワードであるとか他の方法はある意味レベルの低いものであって、バイオメトリクスというものはレベルの高いものであるとの理解がある。レベルの高いものであるとするならば、OpenID の目的はわりとレベルの低いところをいかに手軽に使っていくかというところに彼らの目的があるので、バイオメトリクスとの相性は決していいものではない。そのため、逆に OpenID に対してこちらが提案するという選択肢はあると思う。レベルの高いところまでターゲットを広げませんかというシナリオで提案していくという考え方である。今の OpenID の規格にそのまま乗っかってしまうとレベルの低いところにしかターゲットがないので、バイオメトリクスのせっかくのよさがまともに生きないことになってしまうと思う。

C7: バイオメトリクス業界拡大のために今一番必要なのは市場の創出だと考えている。

C8: 市場を拡大するにあたってバイオメトリクスのキラーアプリケーションというのはレベルの高い認証が実現できるということをアピールすることではないのか。

C9:生体認証にはそれ以外に利便性という特徴がある。

Q1:レベルが低くても利便性が高ければ今のパスワードの代替になりうるということか。

A1: 生体認証というのは暗号やパスワードと同列で扱えないと思っている。セキュリティというか、元々バイオメトリクスはパスワードが露出したものだから、露出しているものなんてパスワードにはなりえず、普通に考えると利便性という軸で見なければならないと考えている。
認証という大きなフィールドがあって、パスワードは覚えるのが大変だとか、トークンは持っていないといけないから大変だとか。バイオメトリクスという利便性の高いものを入れたらもっと使い勝手のいいものになるとか。その認証のビジネスっていうのはかなり大きいので、そのバックボーンにバイオメトリクスが乗るかどうかというのが一つの最初のモチベーションだった。
バイオメトリクスというのは技術が孤立している。技術だけが幅をきかせていて市場がない。市場を見つけたい。それは利便性という面にあると考えている。私もパスワードを使っているが覚えきれない。パスワードなんて崩壊している。紙に書かないといけない、しょっちゅう変えないといけないから、生体認証みたいなのをくっつけて利便性みたいなのをくっつけたら、パスワードというのはより信頼性の高いものになるんじゃないかと考えている。

C10: より信頼性を上げるのであれば、やはり先ほどの話「レベルの高い認証が実現できるということをアピールする」に戻ることになる。

C11: 今言っている信頼性というのはパスワードの信頼性がほとんどないことから来ている。覚えられないから紙に書くとかしょっちゅう変えなければならないとか。パスワード自体には信頼性はあるかもわからないけれど、運営自体には信頼性がない。運営自体のところに生体認証を使って利便性・信頼性を向上させることができないか。でその相手というのは市場のあるところ、市場のあるところと付き合いたい。

C12: OpenID 系の方と話をすると同じような話になって、バイオメトリクスは信頼性が高いので厳格な本人確認だから違う、ということになる。そこが実はかみ合っていない。例えばバイオメトリクスにおいて、フォールスアクセプタンスが 0.1%だ、0.01%だとか言っても千回に 1 回は間違ってしまうことになる。そのセキュリティレベルだと全然セキュリティが高いという話ではない。

C13: 暗号と同じ空間でいくと 6 ビットとか9 ビットでしかない。

C14: 多分先ほどセキュリティが高い低いといっているのは違うリスクに対して高い低いといっていて、それが先ほど「C11」のように運用の話しであったり利便性の話しであったりすると思う。そこの整理が必要だと思う。

C15: 生体認証を間接認証的なフレームワークに乗せましょうというのが一番初めの目的であったと考えている。その間接認証というのが広く使われているのが SAML とか OpenID である。したがって、SAML とか OpenID にバイオメトリクスがどうやって接続できるかということに対応しましょうということで進めたという認識である。
早く形を作って強いところにくっついて実装していく方がより重要だと思う。
開発を進め、そして見せる。見せてオープンソースにする。厳密なところは各企業がそれをベースにしてセキュリティレベルを改善したりセキュリティを考慮して作ったり。コアのところ、完全にこういう方向性で良いというところを見せるためのプロトタイプを作って欲しい、というのが私の一番やってほしいこと。
フェーズ 1 としてまずは進めて、そのつぎは生体認証自体のセキュリティレベルを向上させることを考えて ACBio を組み込むということか、あるいは ACBio じゃないライトを組み込むか、その辺のところが研究テーマになってくると思っている。
それが SP800-63 とどういうマッチングがあるかというのは後付けで考えていけばよいと思っている。誰も使っていないということで、SP800-63 ベースで作った SC37 の国際標準は廃案になった。

C16: OpenID の世界で言うと今使われている OpenID は、ほぼセキュリティのない使い勝手のいい形でウェブのサイト連携とかアプリケーション統合のレベルで使われているものでおそらくセキュリティレベルの低いものである。

今作っているOpenID Connectという規格はOAuthを使ってパスワードと証明書を使う、いわゆるPKIも含めた非常に複雑な仕様になっていて、まだ仕様も確定していないと聞いており、まさにそこが利便性とセキュリティのトレードオフになっていると思う。

C17：OpenIDファウンデーションみたいなところとくっついていけば良いのではないか。OpenIDファウンデーションに行ったら彼が、「クレデンシャルはRPまで行くのか?」とか、まったくこちらの考え方と向こうの考え方が食い違っていた。向こうは生体認証を非常に誤解してとらえていると思えた。こちらの方ではあるべき姿を早めに示してあげて彼らに素材を与えてあげるというのも必要じゃないかと考えている。生体認証はここまで使える、こういう使い方ができるということを。

C18：OpenIDってその人の属性を渡すためのプロトコルと聞いているので、そこに生体情報の何かが入るのか、それとも先ほど言ったOAuthのパスワード＋生体認証の使い方になるのか、その辺のところが勉強不足で私もわかっていない。

C19：そこのところを明確にするのがこのプロジェクトの目標のひとつだと思っている。どういう形で組みこめられるのがベストなのか、ということ。

C20：OAuthが先ほどなぜ出てきた訳は、実はOpenIDがさっきSP800-63を見るようになった過程においてそうなったからである。OpenIDが軽すぎて、改変しないといけないということでOAuthの方に話が行ったわけです。SP800-63ベースにしていくために変えていった。
その中で、あとづけのセキュリティであってまだそこに脆弱性があるということで、「すったものだ」していると考えられる。

C21：そちらの「すったものだ」に巻き込まれるよりも最初からここをターゲットにしたほうがよい、という考え方もある。それは考え方の問題で、どっちの考え方も理解できる。

C22：強いやつと組まないといけないと思う。

C23：OpenIDは少なくともSP800-63にすりよりはじめているわけで、であれば最初からそちらを向いてSP800-63と仲良くするという道もないわけではない。

C24：SP800-63と付き合うということはNISTと付き合うということか。

C25：NISTと付き合わないということであれば、こちらのベースで作ってしまうというのもあると思う。私はどっちの筋がいいかというのはわからない。

C26：前提とする市場は、民需対応で市場があって、市場が大きいところと思う。

C27：ベンダ各社殿はどう進めるのが一番バイオメトリクス市場が広がると考えるのか。

C28：それはやっぱり大きなところに擦り寄るのがいいんじゃないでしょうか。

C29：いい旦那、金を持ったいい旦那がいい。少なくともメーカとかドアにつく鍵メーカではない。パソコンでもない。携帯モバイル関係の旦那か、認証ビジネスで儲かっているところがいい。

C30：IdMの世界に擦り寄ろうとするのは無理か。

C31：社会IDとか国のシステムはまた違って、それはあるベンダさんのところでまだ私見がいろいろある。

C32：アメリカの国という中では、アメリカ政府は政府でIdシステムを彼らは作れる、企業単位の中でもIdシステムを作れるけれど間をつなぐものがない、という話が問題にはなって、その仮定でOpenIDが取り上げられて、政府の規格にOpenIDが擦り寄ったというシナリオではあるので、別に最初に提案されているような8SP800-63を基準にして話をしても、OpenIDの方に擦り寄っていっても、アメリカ政府が考えたシナリオにはどちらにせよ乗っていると思う。
だから全然間違ってはいない。あとはどちらの方が早いかとか、お付き合いしやすいとか、そういうレベルの話なのではないかというのが個人的な印象である。

C32：スピード感をある程度持って、産業界に早めに示すような進め方がよいと思う。ここでちゃんとしたものを作る必要はまったくない。方向性を示すことが大切

C33：今年度の検討により、来年度はこういう方向で進めるのか一番良いということを示すのではないかと考えている。

C34：物を作るということは進めつつ、ただいろいろな可能性がありそうなのでそれを検討することも並行して進めることが大切と考えている。

C32: 開発と方向性の検討をやる人を分けてはどうか。理論づけのほうは山口委員にしていただくことはできないのか。
C32:できることはお手伝いさせてもらいたい。基本的には前向きだ。
C33:皆さんのバイオメトリクスはセキュリティの高いものとしてといものがキラーアプリケーションなのか、セキュリティが弱いところに使い勝手を良くするとして売り込む方向なのか。どうお考えなのか。
C34: 両方あるのではないか。市場によって違う。金融系はセキュリティで、コンシューマ系は利便性ではないか。
C35: 利便性。高信頼ではないのではないか。
C36: 利便性が主張されて、市場に理解され、受け入れられていれば、今でもエンタープライズのIdMやSSO用途などにバイオメトリクスが使われてもよいはず。それがそのようになっていないのには何らかの理由があるはず。
C37: ソリューションが足りなくて、広がっていない。オフィスのアクセスコントロール、情報システムへのログイン管理、その他管理などを統合的に取り扱うところに適用されるソリューションが提示できていないためだと思う。そのため、そのような用途の入り口であるIdMやSSOと連携することが突破口となるのではないかと考えている。
プロトタイプを開発と、市場性があるところに生体認証を適用するというための理論づけの検討を分けて考えてはどうか。
C38: 生体認証で照合できただけで終わるというアプリケーションはない。なにかと付かないと売れない。
C39: 先日の崎村さんを訪問した結果では、OpenID の中のレベルにマッピングできないと OpenID 側と話が進まないと思える。
C40: それは、OpenID+BioIDMにつながるサービスアプリケーションがあるかどうかという問題ではないか。
レベル２であろうが売れればいい。

4) Biometrics 2012の調査について

瀬戸委員より、資料３を用いて「Biometrics 2012の調査について」ついて説明いただき、第１回委員会で承認済みの「英国BC コンファレンス 2012 調査への瀬戸委員の派遣」の内容について、再確認した。

5) ドイツ・フランス状況報告

事務局より、資料４を用いて JAISA 酒井が７月にドイツ・フランス出張したときの情報につい情報共有のため報告があった。

［報告概要］
(1) ドイツフランクフルト空港におけるBioAPI システムの見学
ドイツは国際標準規格であるBioAPIの採用を国内の公共システムに義務付けしている国である。ドイツにおけるBioAPIの採用は、以下の２つを目的としていると考えられる。
① アプリケーションの開発容易性
② コンポーネント化による再利用性の実現
ドイツは国内標準であるBSI Technical Guideline TR-03121 とともに、BioAPIを用いた実装をVISシステムの成功例としてEU各国に紹介している。EU諸国においては、オーストリアとチェコ共和国がドイツのシステムを採用することを決定している。
ドイツは第三者適合性試験のための仕組みも国内に構築済みであり、適合性試験を合格した製品のみを公共システムに展開するという制度上の整備もすでに終えている。
今後ドイツを中心としてBioAPI 規格を用いたシステム構築がEU諸国全体に広まる可能性があるため、ドイツの動きは継続的に注視する必要がある。

(2) SC37/WG2パリ会議におけるBioAPI規格およびBioAPI適合性試験規格に関する審議

SC37/WG2パリ会議で最も重要な審議はBioAPI規格(ISO/IEC 19784-1)の審議だった。ここではドイツから 100 件を超えるコメントが寄せられ、その中には 26 件もの重要な技術コメント（Technical Major）が含まれていた。これらのコメントの多くにはコントリビューションとして具体的な仕様が示されていた。ドイツはBioAPIに基づく公共システムの構築を推進しており、ここで得られた経験からBioAPI規格に対して様々な修正を加えてきたと考えられる。

WG2 におけるドイツの標準化活動は、BioAPI 本体への貢献に加えてファンクションプロバイダインタフェースの規格化がある。4つあると考えられているファンクションプロバイダのうち、ドイツはアーカイブファンクションおよびセンサーファンクションのIS化を終えていたが、今回のパリ会議ではプロセシングファンクションおよびマッチングファンクションという残りの2つのファンクションプロバイダに関するNP提案も行った。

これらの活動から、ドイツがBioAPIに基づく公共システムの構築をさらに推進する意向があることが推測される。過去のBioAPIシステム構築実績に基づいた経験から、BioAPIそのものに手を加えて、さらにシステム構築がしやすい仕様に変えようとしている。また、ファンクションプロバイダの国際規格化を推進することで、システムのさらなるコンポーネント化を図り、部品の交換性を高めシステムの効率化を実現することを意図していると考えられる。

アジア生体認証技術評価基盤で扱うBioAPIはV2.2でありひとつ前のバージョンであるため、今回のドイツの動きが現在推進中のプロジェクトに直接的な影響を与えるものではない。今回の動きを受けて、先行的なBioAPI V3.0 仕様の取り込みの可能性の検討など、将来的に検討していく必要がある。今後ともドイツの動きに注目しながら、情報収集を行っていく必要がある。

また、BioAPI適合性試験(24709-1および2)については、規格文書の効率的な記述方法に関して過去の基準認証プロジェクトでの実績を持つ日本に対して、直接コントリビューションが求められている。EUを中心としたBioAPIの普及の可能性を前に、このような貢献には日本の現在のポジションをさらに高める価値があると考える。

6)　作業委託について

事務局より、資料６を用いて第１回委員会以降にJAISAより本プロジェクトに関係者に対して依頼した本事業の一部である「共通バイオメトリック認証基盤ソフトウェアのプログラム開発と「開発システムの評価等の検証作業の見積もり依頼内容と見積もり回答結果について報告があり、報告内容を承認した。

［報告概要］

(1) 見積り依頼先:　８社

(2) 見積もり回答:　１社

(3) 今後の対応:

現時点で見積もり期限がきているので、回答のあった１社を選定して委託することで進めたいと考えている。

また、当初計画の委託予定金額を超えているので、財)JKAとの相談予定である。

7)　機器借用状況　（口頭）

事務局より口頭にて、第１回会議以降に各ベンダ殿に依頼した本プロジェクトに適用する機器の借用依頼状況について、㈱日立製作所殿より指静脈認証装置が借用がさせていただけた旨、報告があった。

8)　プロトタイプの提供について

事務局より、資料７を用いて平成２４年度第１回ＩｄＭにおける共通本人認証基盤の開発研究委員会委員会で提起された「ＩｄＭにおける共通本人認証基盤の開発研究」における成果物の一つである「プロトタイプ・プログラム」の委員への提供について、取り扱い方法の提案があり、承認された。

なお、事務局より希望者は事務局に連絡することとなり、それを受けて詳細の検討することとなった。

［提案内容］

⑴提供の取り扱い

・希望者に対して提供可能とする

⑵提供条件

・目的外使用の禁止を含む借用書の取り交わし　(JAISA　⇔　借用者)

・現在は開発途中のためオブジェクト提供とする

7. 事務連絡

1) 次回以降の予定等

事務局より今年度の委員会の予定について提案があり、審議の結果、下記となった。

ただし、第４回目については、順次委員会にて確認をすることとなった。

①場所：　一般社団法人 日本自動認識システム協会にて

②日程：　第３回　11 月 21 日（水）　15 時から

第４回　平成 25 年 2 月 13 日（水）　15 時から　(次回再確認)

2) 第３回委員会予定

日時：平成 24 年 11 月 21 日（水）　15:00～17:00

場所：JAISA　会議室Ｂ

以上