

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23年8月26日(金) 14:40~17:00

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 | 14:40 ~ |
| 2. 配布資料の確認 | 事務局 | 14:41 ~ |
| 3. 議事 | 半谷委員長 | 14:45 ~16:50 |
| 1) 前回議事録確認 | 事務局 | 14:45 ~14:50 |
| 2) ACBioについて | 山田委員 | 14:50 ~15:30 |
| 3) OpenIDについて | 岡オブザーバ | 15:30 ~16:00 |
| 4) アーキテクチャ案について | 中村委員 | 16:00 ~16:40 |
| 5) まとめ | 半谷委員長 | 16:40 ~16:50 |
| 4. 事務連絡 | 事務局 | 16:50 ~17:00 |
| 1) 今後の日程 | | |
| 2) 見積もり依頼の件 | | |
| 3) 写真撮影など | | |

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 | 中村 敏男 | (株)OKI ソフトウェア 企画室 |
| ・委員 | 寶木 和夫 | (株)日立製作所 横浜研究所 |
| ・委員 | 菊地 健史 | (株)日立ソリューションズ プラットフォーム部 外本部 |
| ・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 | 諫田 尚哉 | (株)日立製作所 セキュリティ・トレーサビリティ事業部 |
| ・オブザーバ | 熊谷 隆 | (株)日立ソリューションズ プラットフォーム部 外本部 |
| ・オブザーバ | 岡 敏生 | 凸版印刷(株) 事業開発・研究本部 |
| ・オブザーバ | 山中 豊 | 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 |
| ・事務局 | 森本恭弘 | (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: BioIDM アーキテクチャの詳細について
- 資料4: プロジェクト調査計画案について
- 資料4-1: アイデンティティエコシステム
- 資料5: OpenIDに関する動向
- 参考資料: 見積もり依頼書

6. 議事内容

1) 前回議事録確認

資料2を用いて、第1回IdMにおける共通本人認証基盤の開発研究委員会の議事録を確認した。特に問題なく承認された。

2) ACBioについて概要紹介

資料をプロジェクトに投影ながら、山田委員より、ACBioについて概要とバイオメトリック機器にACBioを使うための配慮点について紹介があった。

主なポイントは下記である。

- ①ACBioは、ISO/IEC 24761 Authentication Context for Biometricsという国際標準
 - オンラインで生体認証処理を行うときに安全にバイオメトリック認証データを扱うための規格
- ②オープンネットワークでバイオメトリック認証データを扱うときの懸念は下記で、その懸念を解決するためのものがACBioである。
 - 生体情報をネットワークに流すことによる漏えいの
 - サーバ認証時のサーバ上のバイオメトリックデータの漏えい
 - 相互運用性が確保できるのか
- ③ACBioのポイントは、バイオメトリック認証自体には手を加えず、バイオメトリック認証が正しく行われたことを示す証拠の情報やセキュリティ評価や精度情報を含む情報(ACBio データ)を別に作り、それをネットワーク上の機器間でセキュアに交換することにより、バイオメトリック認証結果をオープンネットワークの上の機器間で取り扱えるようにしたもの。
 - ネットワーク上の機器はすべてACBio データを取り扱うことができることが必要
 - バイオメトリック情報その物をネットワークに流さず、ACBio データを流す
 - ACBio データの正当性を検証することにより、バイオメトリック認証機器でのバイオメトリック認証結果の正当性を担保する
 - ・要求に対するACBio データの応答であることはチャレンジ・レスポンスで担保する
 - ・ACBio データ全体の正当性は電子署名で担保する
 - ・認証に用いられたテンプレートの正当性はテンプレート認証局が発行するテンプレート証明書を確認することで担保する
 - ・認証に用いられた機器の正当性は、ACBio データの中の機器情報の正当性を確認することにより担保する
 - ・基本的な考え方はPKI

以上により、下記が言える。

- バイオメトリック認証機器でのバイオメトリック認証の正当性を確認する処理がネットワーク上で相互に行われる処理で、バイオメトリック認証の方式やモダリティに依存していないので、バイオメトリック認証機器が変わっても相互運用性が確保できる
- サービス提供者側から見るとユーザ選択したバイオメトリック認証機器の認証結果を用いてサービスを接続できる
- バイオメトリック認証機器の精度に応じて、サーバ側のサービスを切り替えることができる

④ACBioに関わる国際標準

- ACBio データ構造は、ISO/IEC 24761 で規定
- ACBio データをネットワーク上に流す方法に関しては、CBEFF Part4 のセキュリティブロックに含めて送るよう規定
- PCなどとのACBio データの授受についてはBioAPI Amend. 3にて規定

⑤OpenID や SAML への適用

OpenID や SAML の認証サーバがACBioを扱うことができるようにし、ACBio データをOpenID や SAML の認証サーバと端末機器の間でやり取りするようにすることで、OpenID や SAML にACBioを整合性良く組み込むことが可能と考えられる。

主な質疑およびコメントは下記の内容。(Q:質問、A:応答、C:コメント)

- ① Q: OpenID や SAML の認証サーバの結果を使用するサービスプロバイダが、初期認証を行う認証サーバと異なるドメイン、たとえば、日本に初期認証サーバ、米国にサービスプロバイダと従の認証サーバがあるとき、日本にある端末が米国にあるサービスを使うときに、日本にある ACBio 対応初期認証サーバを使ってバイオメトリック認証することで問題ないのか。
- A: 初期認証サーバが ACBio 対応をしていれば、その初期認証サーバの認証結果を用いて行う処理は、OpenID や SAML の処理そのもので済むので問題なくできると考える。日本と米国の間では特に ACBio に絡むデータのやり取りはなく、OpenID や SAML での認証結果の処理のやり取りでよいと考えている。
- ② Q: テンプレート再登録の時にテンプレート証明書の再発行が必要と思うがその処理はどの程度か。
- A: テンプレートハッシュ値の登録であるので、非常に簡単で、処理時間もほとんどかからないと考えている。
- ③ Q: 認証端末は個人のものである必要があるのか。
- A: 認証する人のテンプレートとテンプレート証明書が端末の中に入っていればよいので、特に端末が個人のものである必要性はない。
- ④ C: ACBio の処理は軽そうだ。
- A: サーバ側の処理が結構正当性の確認のための処理であり結構重いと思っている。また、サーバ側で ACBio データから認証に関わっている処理プロセスの一つ一つの正当性まで確認することになっているので、たとえば On Card Matching だけでなく PC での認証やその他の認証方式の機器などをカバーするためにサーバ側で複数の認証方式をサポートしようとする、結構大変との認識である。
- ⑤ Q: PC とその外付け機器で ACBio を実現しようとするときに、現状の市場にある外付け機器をそのまま使えるのか、あるいは改造が必要なのか。
- A: セキュリティの考え方による。現状の機器を使い PC 中での対応でセキュリティが守られるとの考え方であれば、現状機器はそのまま使えるし、守られないとの考えであれば、機器の改造が必要になる。
- C: セキュリティの担保をどこで、どう行うかにより、機器の構成も含めて変わる。

3) OpenID について概要紹介

岡オブザーバより、資料5を用いて、OpenID の動向について紹介があった。

主なポイントは下記である。

- ① OpenID は OpenID foundation が作成した Web 上の SSO に関する規格。
- SAML に比べると柔軟かい用途に使われている
 - アカウント提供サイト (OpenID プロバイダ, OP) のアカウントを利用して、OpenID 対応サイト (ライティング・パーティ, RP) のウェブサイトログイン可能とするもの
- ② OpenID の用途およびメリットは次の二つ
- アカウント統合 (1 組織の複数サイト)
 - アカウント連携 (複数組織のサイト)
- ③ 現行規格
- OpenID 2.0 (現行規格) . . . 認証連携用の規格
 - OAuth 1.0a (現行規格) . . . サービス・情報連携用の規格
- 現在、OAuth を認証に使っているところもあるが、本来認可情報のやり取りで、認可の範囲を限定してないので、合鍵を渡すようなものでデータのアクセスまで許すのでリスクが高い
- ④ 規格の動向
- OpenID ⇒ OpenID Connect
 - OAuth 1.0a ⇒ OAuth 2.0

- ⑤OpenID Connect 何が変わるか
 - OAuth と一元化されることにより、サービス連携・情報連携が容易になる
 - スマートフォン、携帯端末のサポートが強化される
 - OpenID Connect では広範囲なセキュリティ要件に応えられるようになる(LoA 1~4)
- ⑥OpenID Connect 規格の状況
 - OpenID Connect は OAuth2.0 に依存しているが、OAuth2.0 が依然策定中(IETF internet-draft, draft version 20)
- ⑦米国 NSTIC との関連性
 - オバマ政権はサイバー空間のセキュリティ強化の一環として、National Strategy for Trusted Identities in Cyberspace (NSTIC)を打ち出している
 - Open Identity Exchange(OIX)と Kantara Initiative が Identity, Credential and Access Management (ICAM)に対して各種規格の採用を働きかけている模様
- ⑧まとめ
 - OpenID Connect/OAuth2.0 は今年(度)中に策定見込み
 - OAuth は確定直前、OpenID は数カ月後の見込み
 - OpenID/OAuth は複数サービスを連携するための重要技術

主な質疑およびコメントは下記の内容。(Q:質問、A:応答、C:コメント)

- ① Q: SSO になるとセキュリティ上の弱さが出てくることはないのか。
A: SSO は良い面と悪い面が両方あると考える。
OP が破られるとすべて破られるというリスクがある。
しかしながら、現在のユーザの多くはパスワードの使いまわしをしているので、その中で弱いところがあると同じようにすべて破られる。しかしながら、OP 自体のセキュリティさえ高ければ、全体の認証が保護できるのでその点はメリットともなる。
- ② Q: OpenID Connect になった場合の処理の流れは OpenID 2.0 と変わるのか。
A: RP、OP、ユーザエージェント間のデータのやり取りが少し変わる。

4) BioIDM アーキテクチャ案の提案と討議

中村委員より、資料3を用いて、BioIDM アーキテクチャ案について、提案があり、検討した。
具体的な提案内容は下記。

- ①今回の提案は、ACBio 等の対応についてではなく、OpenID や SAML などの IdM で使うときにコンポーネント性が高められて、各コンポーネントが自由に入れ替えられるようになっていることにより、自由度が広がることで、IdM 市場での活用や普及が広まると考え、コンポーネント性を高めることを狙い検討した内容の提案である。
- ②Web 技術を使うことになるので、Web ブラウザの下で動く実態を持つ構成とし、仮称として BioIDM とした。
- ③今回は端末認証ということで、端末側の認証に集中している。
- ④BioIDM は以下の2つのコンポーネントに分離する。
 - BioIDM Connection: ID Provider インターフェイスおよびマンマシンインタフェースを実現
OpenID や SAML とのインターフェイス部分を担当するとともに、バイオメトリックスのユーザインタフェース(Biometric GUI)を実現する。
HTML や JavaScript などで記述。
 - BioIDM Transaction:バイオメトリック登録や照合のためのトランザクション処理を実現する。
内部には Biometric Transaction および下位処理である Biometric Attempt がある。Biometric Attempt は、マルチ制御のための Capture Thread と Matching Thread を呼び出す。C++で記述。
- ⑤全体の処理は、登録や照合の処理として整理した。「システム全体の流れ」図を参照のこと。
- ⑥「システム全体の流れ」図のなかの Connection は、バイメトリックスの場合、登録や照合時この

部位を選ぶということや、成功がうまくいったとか、やりなおしてほしいとかのインタラクションが必要になるので、それへのインターフェイスを司るものと考えている。

BioIDM Connectionの一機能であるBiometric GUIは、BioGUI規格(BioAPI Amd.1)のコンセプトを採用することで考えている。

- ⑦ 「システム全体の流れ」図のなかのConnectionを使うことにより、「BioIDM Connectionによって生成される画面例」に示すような画面が、BioAPIより上位のアプリケーション側で、BioAPIの下側のBSPを意識することなしに簡単に開発することができるように考えている。
- ⑧ また、Biometric GUIを活用することで、標準化の際に国際的な合意も得られるものと考えている。提案結果を受け、基本的には妥当性があるとの方向となった。

主な質疑およびコメントは下記の内容。(Q:質問、A:応答、C:コメント)

- ① Q: このアーキテクチャの実現の用途はどの程度あるのか。
A: これからの検討である。
C: 以前の例でセキュリティポリシーファイルのダウンロードと設定しなくてはならない例があった。そのようなことあると普及は難しかったという経験がある。そのポイントも参考にされて検討を進めてもらいたい。
- ② Q: 前回の提案ではBIAS等を考えた提案であったが、今回の提案はそのようではないが。
A: 今回は第1回委員会でのご指摘と検討結果を踏まえ、サーバ認証を前提としたBIASから、直近として応用が広いと思われる端末認証を前提とした構成を考えることに方向性を変更している。
- ③ C: モジュールの構成としてBioAPIフレームワークとブラウザの間に1つモジュールがある構成は、妥当性があると思う。
- ④ Q: IDを管理する部分については、今回のご提案のフレームワークとは別個にあって、ユーザインタフェースの実現のためにフォーカスしたご提案か。
A: そうである。本プロジェクトのスコープに、IDを管理する部分についても入っているが、今回の提案では触れていない。
- ⑤ C: IDを管理する部分については、今後の検討が必要であるが、今回ご紹介いただいたACBioを適用してゆくことで、比較的簡単に実現できるように思える。
- ⑥ C: 本フレームワークは認証を主務としているベンダの製品の機能と機能的にはオーバーラップしているように思える。そのプレーヤとの対応や協調をどのように進めるかについても考えてゆく必要がありそうと考える。
- ⑦ C: 携帯電話の世界を考えると、現在は携帯電話のPC化が進んでおり、部品の共通化が進んでいる。今回のプロジェクトのスコープの一つであるここでいう部品の共通化というコンセプトが受け入れられる余地は十分にあると思う。どこを本プロジェクトの出口を考えるかは、各委員の事業戦略を踏まえながら、今後検討してゆく必要があると考える。
- ⑧ C: 本フレームワークは認証を主務としているベンダの製品の機能と機能的にはオーバーラップしているように思える。そのプレーヤとの対応や協調をどのように進めるかについても考えてゆく必要がありそうと考える。

5) プロジェクト調査計画について

所用により欠席された瀬戸委員より、資料4「プロジェクト調査計画案」と資料4-1「アイデンティティエコシステム」の資料がご提供された。

事務局より提示し、次回の委員会にて瀬戸委員より簡単にご説明いただくこととなった。

6) まとめ

オープン化の方向を目指すのが適切ではないかと思うので、本日の議論を踏まえて検討を進めていただきたいというご発言をいただきまとめとした。

7. 事務連絡

1) 次回予定等

1-1) 委員会開催について

①場所： 一般社団法人 日本自動認識システム協会

②日程： 第3回 10月14日(金) 15時から

第4回 11月16日(水) 15時から

第5回 2012年1月27日(金) 15時から

第6回 2月22日(水) 15時から

1-2) 第2回委員会

日時：2011年10月14日(金) 15:00～17:00

場所：JAISA 会議室B

2) 見積もり依頼の確認

第1回委員会にて事務局より作業計画として提示されていた「本年度に実施する「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」と「開発システムの検証実験の実施及び評価」開発研究に関わる「プログラム開発」と「実証実験の実施と評価」の委託に関する見積もり依頼」が、すでに委員会の構成メンバーのベンダ各社に発行されていること、ならびに見積もり依頼書が参考として配布され、内容が説明された。

その上で、各社への見積もり検討と見積もり回答が依頼された。

以上