

## 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

1. 日時:平成25年7月3日(水) 13:00~15:00

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   |
| 2. 配布資料の確認          | 事務局   |
| 3. 委員紹介             | 事務局   |
| 4. 議事               | 半谷委員長 |
| 1) 委員長挨拶            | 半谷委員長 |
| 2) 委員紹介             | 事務局   |
| 3) 本年度の計画概要         | 事務局   |
| 4) 本年度の検討事項および開発計画  | 中村委員  |
| 5) 調査計画案について        | 事務局代読 |
| 6) 作業委託および見積り依頼について | 事務局   |
| 7) 委託調査および見積り依頼について | 事務局   |
| 8) 実験用機器の借用について     | 事務局   |
| 5. 事務連絡             | 事務局   |
| 1) 今後の日程            |       |
| 2) 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     | 山口 利恵 | 東京大学 ソーシャルICT 研究センター         |
| ・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 外部本部  |
| ・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     | 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 研究開発センター     |
| ・委員(代理) | 大木 哲史 | 産業技術総合研究所 セキュアシステム研究部門       |
| ・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  | 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) 海外事業部 |
| ・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1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: | 平成25年度 IdMにおける共通本人認証基盤の開発研究委員会名簿       |
| 資料3: | 平成25年度 IdMにおける共通本人認証基盤の開発研究補助事業 事業の計画  |
| 資料4: | 平成25年度 IdMにおける共通本人認証基盤の開発研究補助事業 スケジュール |
| 資料5: | 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        |
| 資料6: | Biometrics 2013 (ロンドン) における技術と市場の動向調査  |
| 資料7: | 平成25年度 作業委託見積り依頼書                      |
| 資料8: | 平成25年度 委託調査見積り依頼書                      |
| 資料9: | 弊協会実施事業へのご協力をお願い                       |

## 6. 議事内容

### 1) 委員紹介

事務局より、資料2を用いて、本年度委員の方も基本的に昨年度のメンバの継続でお願いしたとの状況の紹介があり、その後、今年度委員の紹介とともにご挨拶をいただいた。

また、委員の事情により、下記の方が変更および新任である旨、紹介された。

①委員変更：山口委員 → 寶木委員 (産総研)

②新任：山口委員 (東大)

### 2) 本年度の計画概要

事務局より、資料3を用いて、平成25年度の「IdMにおける共通本人認証基盤の開発研究」事業の概要の説明があった。平成23年度および24年度に引き続き 公財)JKA 殿より補助金を受けて実施するもので、平成23年度に申請した三か年計画の第三年度(最終年度)であることが説明された。

平成25年度の事業は、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。(詳細は資料3を参照のこと。)

現時点での計画は下記。

#### (1) 共通バイオメトリック認証基盤ソフトウェアの研究

- ・市場調査して英国 BC2013 での IdM 関連状況調査 (定点調査、委員派遣)
- ・もうひとつの主要な IdM 技術である SAML にも適用可能とする開発研究
- ・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
- ・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 (委託調査)

#### (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検証実験

- ・共通認証基盤全体のプロトタイプの開発 (委託作業)
- ・システム性能評価 (委託作業)
- ・検証実験 (委託作業)
- ・結果まとめ

このうち、「英国 BC2013 における市場調査」を、委員を派遣して実施する計画であること。

また、「共通認証基盤全体のプロトタイプの開発」と「システム性能評価」ならびに「検証実験」を委員企業から選定し、作業委託して実施する計画であること。さらに、「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」を委員企業から選定し、委託調査として実施する計画であることが説明された。

なお、事業スケジュールについては資料4を用いて説明された。

質疑応答のなかで、SAMLはマークアップランゲージであるので IdMシステムではなく IdM 技術であるのご指摘があった。計画書はすでに提出済みなので、提出済みの計画書の中の「主要な IdMシステムの一つである SAML」は「主要な IdM技術の一つである SAML」と解釈することとし、今後の検討資料や報告書の中での同様の意味の語句の使用時には「主要な IdM技術の一つである SAML」と訂正する対応をすることとなった。

また、SAMLに対する対応を今年度進めることが本プロジェクトの範囲に一致しているかに

ついで問題提起と審議が行われ、本プロジェクトとして複数の IdM に対する対応ができること、また SSO (Single Sign On) に本プロジェクトの開発技術を適用してゆくことが「共通本人認証基盤の開発」という本プロジェクトのスキームの一つであるので、本事業の目的として「IdMの中でもSSOが重要であり、その注目技術としてSAMLを対象として本年度の開発を行う」ことが確認された。ただし、計画書の現記載だけでは分かりにくいところもあるので、今後の検討資料や報告書の中での同様の意味を持つ説明の際には「IdMの中でもSSOが重要であり、その注目技術としてSAMLを対象として本年度の開発を行う」というように説明を追加する対応をすることとなった。

審議により、提案計画に対して上記の訂正をして今年度の活動を進めることが承認された。

### 3) 本年度の検討事項および開発計画について

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として本年度実施したいと考えている事項についてご提案があった。(詳細は資料5を参照のこと。)

本年度の主な活動内容の提案は下記である。

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を提案する。

- (1) 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、昨年度までの活動で、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ため、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。
- (2) 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、昨年度までの活動で、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環境は開発できたが、実際に接続を確認したのは日立社製指静脈認証装置のみであり、他の機器を使つての確認ができていないため、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。
- (3) 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、昨年度までの活動で、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たが、暗号化や ACBio、WebSocket の SSL 化などセキュリティの考慮は不十分であるため、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う。また、可能な限り実装も行う。

また、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が提案され、具体的には「西宮市被災者支援システム」や「ひょうご震災記念21世紀研究機構」の調査を行い、その結果をもとにして検討することが提案された。

#### [質疑応答の内容]

Q1: 生体認証の登録テンプレートの場所について、質問したい。

震災対応の場合、カード等ないのでサーバに一元管理の必要があると思う。

昨年度の構造ではローカル認証なので、クライアント側にテンプレートがあることが前提になっている構造と思われる。

今年度はテンプレートがサーバに集約管理されている前提なのか、それともクライアント側にテンプレートがあることが前提になっているのか、どちらでお考えになっているのか。

A1: 被災者については、持ち物の管理ができない避難所などでの適用になるので、サーバ認証にならざるを得ないと思っている。

一方、持ち物管理ができる人たち(医療関係者やボランティア)への応用シーンもある。

そのため、現実的には、両方を合わせ持つ構成が考えられる。

Q2: サーバ認証のためには、何かが起こってから IC カードから抜きだしてサーバに登録ができるかと言ったらできないと思うので、震災前の事前登録が必要と思う。

A2: 考え方がいろいろあると思う。

現状では、震災前の事前登録はプライバシーの課題などで難しさがある。

震災が起きた直後に被災者が散らばらない時に避難所などで近所の知り合いがお互いの顔を見て相互確認できる環境が一時的にあるので、その時に役所の人などを介して登録することができるという考え方があると思う。

C1: お互いの顔を見て相互確認という考え方がセキュリティという観点からどの程度受け入れられるかについても考える必要があると思う。

C2: 日頃いる場所と被災した場所が離れていた場合の確認について考慮が必要と思う。

C3: 被災者システムの際は、認証の起点というものの考え方が必要ではないのではないかというぐらい自由に考えていいのではないかと思っている。連続性がほしいだけ、つまり、朝ご飯を食べに来た人に昼ごはんを与える時に二重配布を防ぐために使うというようなことでいいのではないかと考えている。

役所のサービスのような厳格な信頼性が必要なものには適さないと考えている。

C4: サービスのレベルによると思う。例えば一時金を払うというような場合に、被災者ではない人が被災者に成りすますことは防がなくてはならないのではないかと。

C5: それはそうだが、今の日本の社会で震災前の事前登録をする/させるということは考えにくい。

C6: そうかもしれないが、システム的には事前登録ができることを排除する必要はない。

事前登録された方とそうではない方で、受けられるサービスのプライオリティ付けをするという考え方もあると思う。

C6: システム的にはローカルでもネットワーク環境でも作り方次第であるが、災害時のどの時点で使うものかということも考えてシステムを考えておくことも必要である。

Q3: 震災対応アプリケーションについての調査検討の目的は何か。

バイOMETリック認証が使えるシステム、ある程度具体的なユースケースを決めてみるのか。

いま議論があったことを踏まえ、検討して行って、妥当性のあるものを考えていると捉えてよいか。

A3: 最終的なアウトプットの一つはそうなると思っている。また進め方もそうかなと考えている。

Q4: 今年度の開発対象の中の「セキュリティ」とはどういうことを考えているのか。

SAMLの技術を使うのか、それとも何か新たなセキュリティ機能を考えているのか。

A4: まだ、ぼやっとしている。バイOMETリクスに関わる所について新しいセキュリティ機能が必要と思っているので、データベースの暗号化やほかの手段を組み込んでゆくことを検討することになると思う。

Q5: 本プロジェクトの成果はどう考えればよいか。また、どのように周知、共有するかについても考

えていただきたい。

Q5: 進め方について今後の検討が必要であるが、後半のSWGの中で、適用場面やアーキテクチャ等も含めて議論、検討することも考えたいと思っている。

質疑応答を経て、提案内容に今回の審議内容を追加、検討、修正し、委員会にて検討を進めることが承認された。

#### 4) 調査計画案について

事務局より、資料6を用いて、瀬戸委員よりご提案の英国BCコンファレンス2013にて海外調査を行いたいのご提案内容をご説明し、提案者の瀬戸委員にご出張いただき、調査いただくことが提案され、審議の結果、承認された。(提案詳細は資料6を参照のこと。)

なお、質疑の中で、海外調査の定点観測として英国ロンドンで開催されるBiometricsカンファレンスを選択している理由がたずねられた。情報収集に良い会議として、①米国のBiometricsカンファレンスと②英国Biometricsカンファレンスの二つがある。米国のカンファレンスは米国政府の動きにかかわるものであり、資料等が公開されており情報収集ができるが、英国のカンファレンスは、全体の動きと標準化等もふくまれ、また会費制で情報及び資料が参加者のみに限定されているため、英国のカンファレンスを選択しているとの説明がされ、了承された。

#### 5) 作業委託および見積り依頼について

事務局より、資料7を用いて、日本自動認識システム協会より、本事業の一部として承認された「共通認証基盤全体のプロトタイプの開発」と「システム性能評価」ならびに「検証実験」に関する作業委託の見積り依頼が見積り依頼先に対してお送りしたこと。またその内容について説明があり、見積りへの協力依頼があった。(依頼内容の詳細は資料7別紙3を参照のこと。)

#### 6) 委託調査および見積り依頼について

事務局より、資料8を用いて、日本自動認識システム協会より、本事業の一部として承認された「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」に関する調査委託の見積り依頼が見積り依頼先に対してお送りしたこと。またその内容について説明があり、見積りへの協力依頼があった。(依頼内容の詳細は資料8別紙3を参照のこと。)

#### 7) 実験用機器の借用について

事務局より、資料9を用いて、本年度も各委員のご所属の会社様に今年度の検討に向けたバイオメトリック認証装置、BSP、SDKのご提供の依頼があった。

委員各社にてご検討いただき、事務局にご連絡いただくこととなった。

### 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、後程事務局にて調整することとなった。また、第3回目以降については、順次委員会にて確認をすることとなった。

以上