L-035

放送を起点とした個人向け通信サービス利用におけるユーザ-機器認証連携フレームワーク

User-Device Authentication Federation Framework
for Receiving Personalized Telecommunication Services based on Data Broadcasting Service

山村 千草† 藤井 亜里砂† 石川 清彦† 本間 祐次‡ 小尾 高史§ 谷内田 益義‡ 李 中淳¶
Chigusa Yamamura† Arisa Fujii† Kiyohiko Ishikawa† Yuji Homma‡ Takashi Obi§ Masuyoshi Yachida‡ Joong Sun Lee¶

1. はじめに

2011 年の地デジ完全移行を目前に控え，通信機能を搭載したデジタル放送受信機（以下，テレビ受信機）の普及が急速に進んでいる．テレビ受信機は従来，放送が持つ同報性や公共性を特長としてきたが，今後は通信機能を活かすことで，個人の嗜好や意向に即した個人向けサービスを実現できる双方向メディアとして，新しい価値を提供できると期待される．

一方で近年，民間サービスから電子行政に至るまで，様々な分野で情報の電子化が進んでいる．政府の IT 戦略本部で決定された「新たな情報通信技術戦略」では，国民 ID 制度導入にあわせた国民本位の電子行政の実現や，医療分野における自己医療・健康情報活用サービスの枠組み検討などが，重点施策として明記されている[1]．このような個人向け通信サービスが広く国民に利用されるためには，アクセス手段の多様化が不可欠である．特にテレビ受信機は，家庭への普及率が高く，デジタルデバイドを解消し得る身近な端末としても注目され，情報取得手段としての環境整備を要求する声が高まっている．

このような状況を背景に，我々は，放送事業者サービスに他の事業者のサービスを取り込むことで，より充実した放送通信融合型サービスを実現することを目指している．特に，認証を必要とする複数の個人向け通信サービス間でアイデンティティ連携を実現し，ユーザが利便性を損なうことなく，より高度な連携サービスを安全に享受できる環境を構築することを目的に研究を進めてきた．本稿では，放送事業者－外部事業者間の認証連携および属性連携フレームワークを検討し，プロトタイプシステムを開発したので報告する．

2. 想定するサービス形態と要求条件

2.1 融合型個人向け通信サービス

近年，インターネット対応型テレビ受信機が普及してきているが，そこで実現されるインターネットサービスは，放送とは完全に切り離されたものとなっている．

我々が目指す融合型個人向け通信サービスとは，個別に構築されている放送事業者サービスと外部事業者サービスとを連携させることで，双方から提供されるコンテンツやデータを組み合わせた高度なマッシュアップコンテンツを，ユーザに提供できる状態を指す．これによって，例えば，健康番組を視聴中のユーザに，個人の健康情報を扱う外部サービスへのアクセスを誘導したり，ユーザが閲覧している情報にあわせて関連番組をお薦めするなど，放送を起点とした新たな付加サービスを実現し得る．このような放送起点のサービスを実現するためには，画面レイアウトや遷移，番組との関連などのサービス基盤を放送事業者が提供し，そのサービス上で，外部事業者が有する個人向け情報を，他に漏洩することなくユーザに直接提供することが有効である．融合型個人向け通信サービスイメージを図１に示す．

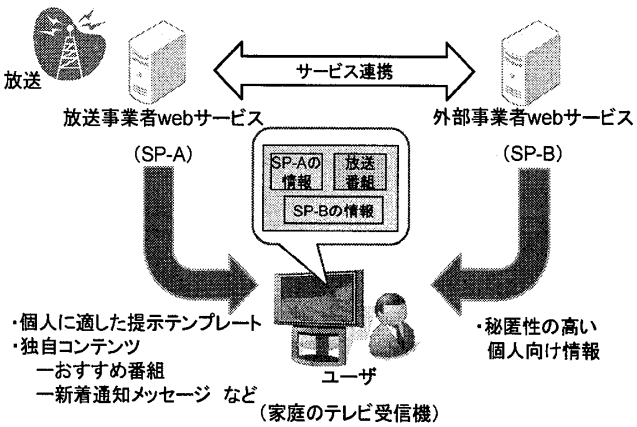

図１　融合型個人向け通信サービスイメージ

本稿では，連携する外部事業者サービスとして，特にテレビ受信機での利用が期待される公共的なサービスを想定する．個人の健康情報や社会保障情報といった秘匿性の高い情報は，放送事業者を経由することなく，放送事業者が提供するサービス上で安全に提示されることを条件とする．

2.2 認証レベルに応じたサービス認可

サービス事業者がポリシーにあわせた適切なアクセス制御を実施するには，ユーザの認証レベルに応じた柔軟なサービス認可を実現する必要がある．特に，秘匿性の高い情報を扱うサービスでは，ID/パスワード（PW）などのユーザ認証だけでなく，そのユーザが利用している端末が正当な機器か否か，あるいは本人が事前に登録している機器か否かなど，機器を特定したアクセス制御が必要となるケースがある．

そこで本稿では，外部事業者サービスの利用に必要な認証レベルとして，ユーザ認証と利用端末の機器認証による

† NHK 放送技術研究所 Science & Technology Research Laboratories, Japan Broadcasting Corporation
‡ 東京工業大学 統合研究院社会情報流通基盤研究センター Advanced research center for Social Information Science and Technology(ASIST), Integrated Research Institute, Tokyo Institute of Technology
§ 東京工業大学 総合理工学研究科 Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology
¶ 東京工業大学 像情報工学研究所 Imaging Science and Engineering Laboratory, Tokyo Institute of Technology

二要素認証を設定することで，ID/PW 方式での認証レベルを強化することとした．これにより，秘匿性の高い情報を含むような個人向けサービスは，世帯内の登録機器での利用に制限するなど，サービス事業者が柔軟なアクセス制御を行うことを可能とする．

2.3 要求条件

上記で想定するサービスを，ユーザが安全かつ簡便に利用可能とするための要求条件を以下に整理する．

(a) SSO（Single Sign On）を実現し，ユーザの煩雑な認証手続きを軽減すること
(b) 各サービス事業者が，認証レベルに応じた柔軟なアクセス制御を行えること
(c) 秘匿性の高い情報は，情報を保有する事業者から直接ユーザに提供されること
(d) 放送事業者が，パーソナライズ化されたサービスをユーザに提供できること

これらの要求条件を満たし，外部事業者サービスを取り込んだ融合型個人向け通信サービスを実現するための，適切なアイデンティティ管理を検討する．

3. アイデンティティ管理技術

アイデンティティ管理技術は，情報システムやネットワーク上において，ユーザの識別情報や属性情報などを適切に管理する技術である．複数の事業者間で連携したアイデンティティ管理を行い，効率的なサービスを実現する仕組みとしては，認証連携（SSO），認可取得，属性情報交換などの技術が知られている．SSO を実現する認証連携技術としては，SAML や OpenID が代表的な方法である．

3.1 SAML

SAML（Security Assertion Markup Language）は，認証，認可，属性などのセキュリティ情報をウェブアプリケーション間で交換するために，標準化団体 OASIS により策定された XML 形式の標準仕様である[2].

SAML モデルは，ユーザ，アイデンティティ提供者（以下，IdP : Identity Provider），サービス提供者（以下，SP : Service Provider）の３つのエンティティから構成される．IdP と SP 間では，事前に信頼関係（トラストサークル）を構築し，認証情報などのやり取りは，アサーションと呼ばれる証明書の形で行う．IdP と SP の間で，事前にローカル ID とは異なる仮名でアカウント連携を行っていれば，IdP が保持するユーザ ID の流出や，名寄せによるプライバシー漏洩の危険性を回避することができる．

3.2 OpenID

OpenID は， URL または XRI（eXtensible Resource Identifier）形式で記述されるユニークな識別子をもとに，複数サービス事業者への SSO を実現する方式として，OpenID Foundation が策定した仕様である[3]．事前の信頼関係や連携付けを必要としない非中央集権型のモデルであり，その簡素さから利用は広まっている．

3.3 ID-WSF

ID-WSF（ID-Web Service Framework）は，Web サービス間で属性情報を交換するために，Liberty Alliance Project が仕様策定したフレームワークであり，属性提供者（以下，WSP : Web Service Provider），属性利用者（以下，WSC : Web Service Consumer），SP 情報管理者（以下，DS : Discovery Service）のエンティティから構成される[4].

4. 方式検討

4.1 認証連携

本研究では，秘匿性の高い情報を扱う外部事業者サービスとの連携を想定したため，限定的なトラストサークル内での連携によって高セキュリティ性を確保する SAML をベースとした認証連携を行い，SSO を実現することとした（要求条件(a)）．XML ベースの仕様であるため，拡張性が高いことも利点である．

本研究では，２章で述べた要求条件(b)を実現するため，SAML プロトコルを拡張した．詳細は５章に記述する．

4.2 属性情報交換

要求条件(d)を満たすには，放送事業者が，外部事業者サービスにおけるユーザ毎の利用可能メニュー情報や，提示スタイルに関連する情報など，秘匿性の低い属性情報のみを取得しておくことが有効である．また，放送事業者が，外部事業者サービスにおけるユーザ単位の新着情報を取得しておくことで，ユーザ単位の新着情報を世帯単位の新着情報に変換し，機器単位での新着通知を行うことができる．

本研究では，放送事業者を WSC，外部事業者を WSP とし，一部の属性情報を ID-WSF に従って交換させることで，ユーザに適したテンプレートを提示することを可能とした．図２に，ID-WSF に基づく属性情報交換の流れを示す．

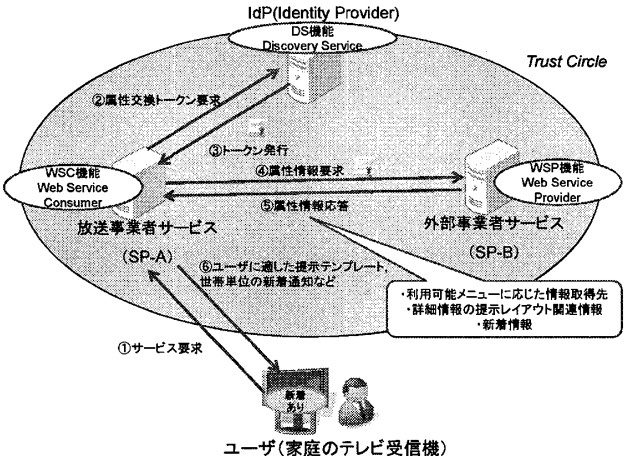

図２　ID-WSF に基づく属性情報交換

4.3 テレビ受信機でのマッシュアップ

要求条件(c)を満たすため，テレビ受信機では，放送事業者から取得した提示テンプレート（XSLT : XML Stylesheet Language Transformation）と，外部事業者から画面遷移とは非同期に取得した詳細情報（XML）をもとに，テレビ

受信機内で BML を生成し，BML ブラウザ上で融合型個人向け通信サービスに遷移を行うこととした[5].

5. 機器認証における課題と解決方式

２章で述べたとおり，本稿では，秘匿性の高い情報を扱う外部事業者サービスとの連携を前提とし，サービス利用に必要な認証レベルを二要素認証（ユーザ認証＋利用端末の機器認証）とした.

しかしユーザ認証とは異なり，機器の認証には，機器やそのプラットフォームに応じた独自の認証方式が存在し，また，機器の識別情報なども公開されていない場合が多い．機器認証を行う事業者自身がサービスを展開する場合には問題ないが，他のサービス事業者すべてに機器の管理体系や認証手段を実装することはコスト面やセキュリティ面でリスクを生じる．今後，特定のプラットフォームや端末上に様々なサービス事業者がサービスを展開する状況を考慮すると，独自の機器認証手段を持つ特定のプラットフォーム事業者やベンダ，キャリアなどが行う機器認証結果を他のサービス事業者が参照できるように整備することで，サービス事業者が柔軟なサービス認可を行えるようになると考えられる.

そこで本稿では，SAML プロトコルを拡張し，独自の機器認証手段を持つ特定事業者が，自身が行った機器認証結果をトラストサークル内で共有できる方式を検討した.

5.1 ユーザ認証と機器認証のバインド

機器認証を行う事業者では，会員登録などの手続きによって機器とユーザの紐付けが実現されており，IdP との間ではトラストサークルを構築しているものとする.

IdP でユーザ認証を実施した結果，共有されるユーザ認証アサーションをもとに，プラットフォーム（機器管理）事業者はそのユーザの登録機器を特定し，ユーザの利用端末との間で機器認証を行う．機器認証後，連携用のユーザ識別子とあわせて機器認証トークンを IdP に引渡し，認証情報の更新を要求する．IdP は機器認証トークンでプラットフォーム（機器管理）事業者に更新内容を問い合わせ，ユーザに紐づく認証結果を更新する．これによって IdP は，図３に示すように，トラストサークル内のサービス事業者に対して，機器認証結果がバインドされた認証情報を連携させることができる.

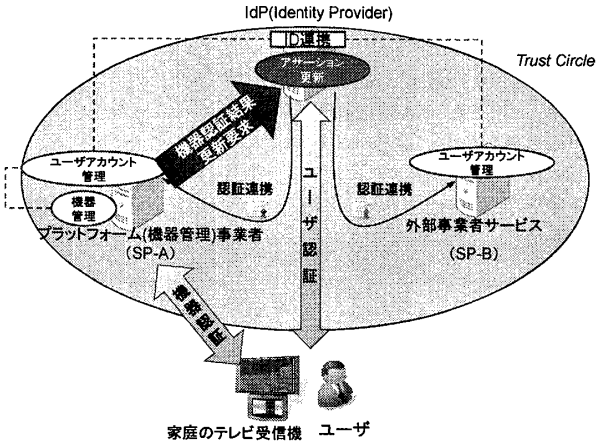

図３　ユーザと利用端末をバインドさせた認証連携手法

5.2 SAML プロトコルの拡張

機器認証を行ったプラットフォーム（機器管理）事業者が IdP に対して認証情報更新を要求するメッセージとして，<samlp:UpdateAuthnQuery>要素を新たに定義した．本メッセージには，機器認証トークンと連携用のユーザ識別子を含む.

6. プロトタイプシステムの構築

ここまで述べてきた認証連携および属性連携のフレームワークをもとに，放送事業者－外部事業者融合型の個人向け通信サービスプロトタイプシステムを構築し，図４のサービス遷移にあわせた動作を，データ放送記述言語である BML（Broadcast Markup Language）対応ブラウザ上で確認した.

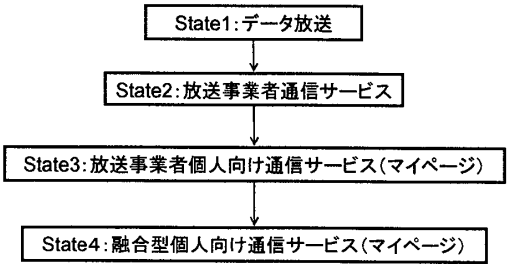

図４　サービス遷移シナリオ

実装したシステムブロック図を図５に示す．IdP および SP には，CPU：Intel Xeon（2GHz），メモリ：4GByte, OS：CentOS release 5.2 の PC を使用した．また，テレビ受信機には，CPU：Intel Xeon（2.83GHz），メモリ：3GByte, OS：WindowsXP の PC を使用した．テレビ受信機を想定した PC には BML ブラウザを動作させ，テレビ受信機における機器認証手段として接触型の IC カードリーダーを接続した.

本稿では，機器認証手段を放送事業者に持たせ，56 ビット鍵を格納した IC カードとの間で，DES によるチャレンジ＆レスポンス方式の機器認証を行った.

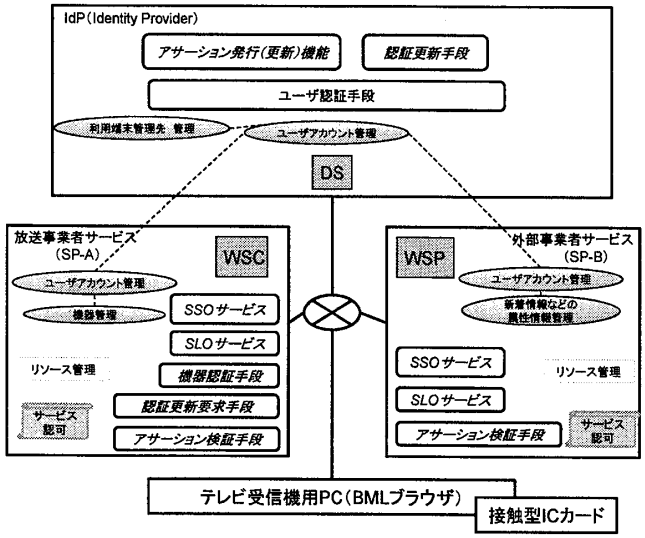

図５　実装システムブロック図

6.1 認証手順

手順 1：
State3（図 4）への遷移時に，ユーザは IdP との間で ID/PW 方式の認証を行う（ユーザ認証フェーズ）
手順 2：
IdP サーバはユーザの認証アサーションを放送事業者に発行する
手順 3：
放送事業者は認証アサーションに含まれる連携用ユーザ識別子から紐づく登録機器を特定し，DES によるチャレンジ＆レスポンスをユーザ利用端末との間で実施し，機器認証トークンを発行する（機器認証フェーズ）
手順 4：
放送事業者は IdP に，連携用ユーザ識別子とあわせた機器認証トークンを引き渡す（認証更新要求フェーズ）
手順 5：
IdP は放送事業者に機器認証トークンを用いて更新内容を問い合せる
手順 6：
IdP は受け取った更新内容をユーザ認証情報にバインドし，更新済みアサーションを発行する（認証バインドフェーズ）
手順 7：
State4（図 4）へ遷移時には，ユーザ認証結果と機器認証結果がバインドされたアサーションで認証連携が行われ，二要素認証を要する外部事業者サービスへの SSO が実現される

6.2 更新済みアサーション

ユーザ認証結果とそのユーザの利用端末の機器認証結果がバインドされたアサーションを図 6 に示す．アサーションを受信したサービス事業者は，アサーション全体の署名を検証してユーザの認証報告を得るとともに，二要素認証を必要とする場合には，さらに機器認証報告の署名を検証し，サービスポリシーにあわせたサービス認可を行うことができることを確認した．

```
<?xml version="1.0" encoding="EUC-JP"?>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0"
ID="s2303bbf0f0eac030d6e8d5f5949850e3bb7d1361b" IssueInstant="2010-03-03T08:27:21Z">
…
<!-- 主体の情報 -->
<saml:Subject>
<saml:NameID>co_n_user01</saml:NameID>
</saml:Subject>
…
<!-- 条件-->
…
<!-- ユーザ認証報告 -->
<saml:AuthnStatement AuthnInstant="2010-02-25T02:47:57Z"          （ユーザ認証結果）
SessionIndex="sff00a13626f37fb7a016ac0c77699bfae4f1d06a">
…
</saml:AuthnStatement>
<!-- 機器認証報告 -->
<saml:AttributeStatement>
<saml:Attribute Name="DeviceAuth">
<AttributeValue xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
<UpdateData xmlns="" ID="s2d258571927adf8918bab0be5a7c768620aad9952">
<Status>SUCCESS</Status>                （機器認証結果）
<Date>2010-02-25T02:50:00Z</Date>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
…
</Signature>                （機器認証実施事業者の署名）
</UpdateData>
</AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
                                                （全体の署名）
```

図 6　認証結果がバインドされたアサーション

6.3 融合型個人向け通信サービス例

プロトタイプシステムで確認した融合型個人向け通信サービス（図 4 State4）の一例を図 7 に示す．放送事業者のテンプレート上で，健康番組の視聴を継続しながら，外部事業者から直接取得したプライバシー情報を閲覧できることを確認した．

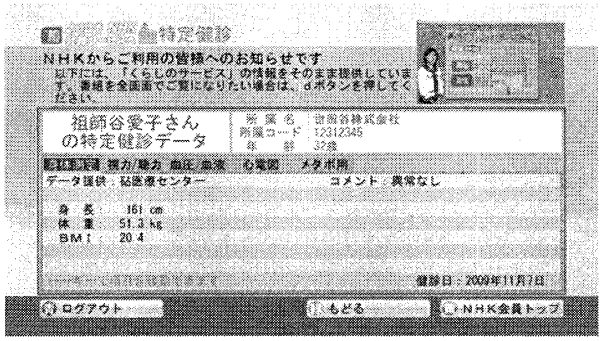

図 7　融合型個人向け通信サービス例

7. まとめ

本稿では，テレビ受信機上で簡便かつ安全な融合型個人向け通信サービスを実現するための認証連携および属性連携フレームワークを検討し，開発したプロトタイプシステムでの動作を確認した．また，機器認証結果とユーザ認証結果をバインドさせた認証情報を，複数事業者が共有することによって，機器管理手段を有しないサービス事業者であっても，ユーザのアクセス環境に応じた柔軟なサービス認可を実現できることを示した．放送事業者と外部事業者とでサービス連携を行うことによって，放送事業者が提供するサービスに閉じることなく，よりオープンな個人向け通信サービス提供基盤を確立できる．

今後は，テレビ受信機における秘匿情報格納方式や不正コンテンツ排除方式の検討に取り組むとともに，既存の認証システムとの整合をとりながら，よりオープンで安全なサービス連携フレームワークを検討していく．

参考文献

[1] 高度情報通信ネットワーク社会推進戦略本部(IT 戦略本部),"新たな情報通信技術戦略",http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf(May. 2010)
[2]SAML v2.0, http://saml.xml.org/saml-specifications#samlv20
[3]OpenID, http://openid.net/foundation/
[4]ID-WSF,http:/www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates/
[5]山村千草,藤井亜里砂,石川清彦："データ放送を用いた外部保有の個人向け情報提示手段の検討" ,2009 映情学年大, 3-7(2009)