O-021

テレビ視聴環境での個人向けサービス実現に向けたユーザ認証認可基盤
An Authentication/Authorization Infrastructure for Personalized Services in Hybridcast System

山村 千草† 西本 友成† 藤井 亜里砂†
Chigusa Yamamura Yusei Nishimoto Arisa Fujii

１．はじめに

現在我々は，放送通信連携システム Hybridcast の研究開発を進めている[1]．Hybridcast では，通信の特徴を生かすことで，番組視聴者の個別の要求に応じた多様なサービスを提供することが可能になる．これにより，放送番組と連動したソーシャルサービスや会員制の映像配信サービスなど，Web サービスのアカウントに紐付いた各種個人向けサービスをテレビでも提供できるようになる．

このような個人向けサービスを活性化させるためには，Web サービス間の連携を促進して手軽なサービス参入を実現するとともに，テレビ視聴環境でも簡便に個人向けサービスを享受できる仕組みを構築する必要がある．そこで我々は，これらの要件を満たすユーザ認証認可基盤の検討と開発を進めてきた．本稿では，OAuth2.0[2]をベースに構築したユーザ認証認可基盤のプロトタイプシステム概要と，Hybridcast への適用例について報告する．

２．ユーザ認証認可基盤

ネットワーク上には，ユーザに応じたアクセス制御が必要なデータや機能(以下，保護リソースとする)が複数のサービスで分散して管理されている．“ユーザ認証認可基盤”とは，これらの保護リソースを，ユーザの認証結果やユーザの同意に応じて，サービス間で安全に参照させ，各種個人向けサービスを適切なアクセス制御のもと実現するための仕組みを指す．

我々は，このユーザ認証認可基盤を構築するにあたり，サービス間で保護リソースへのアクセス権限を安全に委譲するためのプロトコル OAuth を用いることとした． OAuth は，シンプルなプロトコルで実装が容易であり，権限範囲を柔軟に設定可能であることから，SNS を中心に利用が広まっている．

さらに我々は，このようなアクセス権限委譲の仕組みが，テレビ視聴環境における個人向けサービス利用に有効であると考えた．家庭のテレビは複数人が頻繁に入れ替わり利用する端末であり，パソコンと同様のユーザ管理機能を備えていないことから，ユーザ ID およびパスワードを必要とする個人向けサービスを，いかに安全で簡便に提供できるかが課題となっている．そこで，ユーザ ID およびパスワードによる認証操作は個人が所有する携帯端末上で行い，テレビの個人向けサービスで必要とする保護リソースへの一時的なアクセス権限のみを，テレビへと委譲させるようにする．これにより，家庭の共有端末であるテレビ上でも，情報漏洩リスクを低減させながら，個人向けサービスを簡便に提供できる基盤の構築を目指す．

† NHK 放送技術研究所, Science & Technology Research Laboratories, Japan Broadcasting Corporation

３．プロトタイプシステム概要

3.1 OAuth

OAuth は，本来ユーザのクレデンシャル(ユーザ ID/パスワードなど)を必要とするような保護リソースへのアクセスを，ユーザ同意のもと，一部の権限に限って他サービスに委譲することを可能にするプロトコルである．図１に，IETF(Internet Engineering Task Force)で現在標準化作業が進められている OAuth2.0 の処理フローを示す．保護リソースを提供する OAuth サービス提供者 (以下，OAuth-SP とする)は，保護リソース要求者であるクライアントからの認可要求に対して(①)，正規の保護リソース保有者(ユーザ)の同意を確認し (①’)，認可された権限を引き渡す(②)．さらにクライアントの認証を行い (③)，信頼性が確認されたクライアントに対しては，有効期限付きのアクセストークンを発行する(④)．クライアントからアクセストークンを伴った保護リソース要求があった場合には(⑤)，アクセストークンに紐付くアクセス権限範囲と有効期限を確認し，適切なアクセス制御を実行する (⑥).

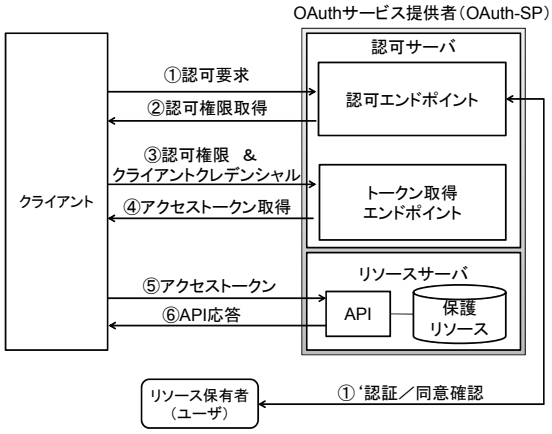

図１ OAuth2.0 の処理フロー

3.2 認証認可情報の統合管理

OAuth2.0 では，認可を扱う認可サーバと，保護リソースを管理するリソースサーバの役割は区別されているものの，その間のインタフェースについては規定のスコープ外となっている．そのため，OAuth-SP を構築する場合，リソースサーバごとに認可サーバを配置するのが一般的である．しかし，複数の認可サーバが存在した場合，ユーザはそれぞれに対して，正規のリソース保有者であることを示すため認証が必要となり，利便性が損なわれる恐れがある．

そこで，保護リソースを管理する複数のリソースサーバ間で共通の認証認可サーバを設け，ユーザ認証およびアクセス権限認可の情報を統合的に管理可能なユーザ認証認可基盤の設計を行い，プロトタイプシステムを試作した．その概要を図２に示す．これにより，ユーザのインタフェースが一元化されて利便性が向上するとともに，各リソース

サーバが共通のインタフェースでユーザの認証結果や認可情報を参照可能となり，容易にサービス連携が拡張可能となる．なお，アクセストークンの取得は，OAuth2.0 プロトコルに準拠して行う．

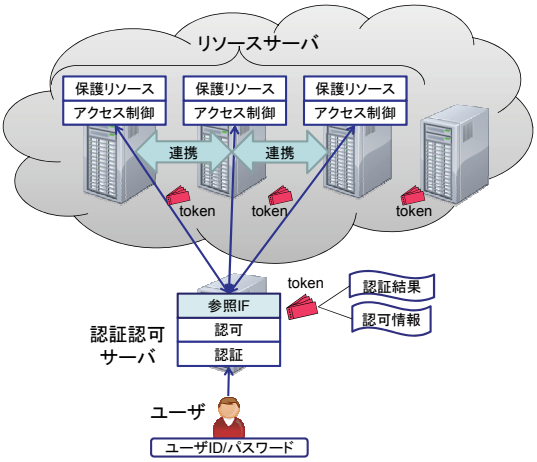

図２　プロトタイプシステム概要

リソースサーバと認証認可サーバとの間では，新たに以下のアクセストークン情報参照 IF を定義し，リソースサーバがアクセストークンに紐付く認証結果や認可情報を統一的なインタフェースで参照できるようにした．参照結果は，JSON Web Token[3]を暗号化した形式で応答し，各リソースサーバは検証した参照結果に応じて，保護リソースへのアクセス制御を実現する．

◆アクセストークン情報参照 IF

・要求パラメータ
　－アクセストークン
　－種別(認証結果 / 認可情報)
・応答パラメータ
　－トークンの有効性（OK/NG）
　－ユーザの連携用 ID
　－トークンの更新日時
　－トークンの有効期限
　－認証方法(※認証結果要求の場合)
　－認証時間(※認証結果要求の場合)
　－アクセス権限の範囲(※認可情報要求の場合)
　－クライアントの情報(※認可情報要求の場合)
　－署名

3.3　複数端末間サービスでのアクセス権限委譲

２章で述べたテレビ特有の課題に対し，本システムでは，ユーザ認証認可基盤で発行されたユーザ同意にもとづくアクセス権限を，テレビ上の個人向けサービスに利用できるようにした．個人が所有するタブレット端末やスマートフォンなどの携帯端末を認証に用いて，携帯端末上で個人向けサービスを実現するとともに，「家族と一緒に大画面で見たい」「放送番組とあわせて閲覧したい」などの利用シーンにあわせ，テレビ上のサービスに必要な一部保護リソースへのアクセス権限を端末間で引き渡すこととした．これにより，テレビ上でのクレデンシャル入力を必要とせず，一部の範囲に制限された短い有効期限のアクセス権限のもと，テレビ上での個人向けサービスを簡便に実現できる．端末間でのアクセス権限委譲処理シーケンスを図３に示す．

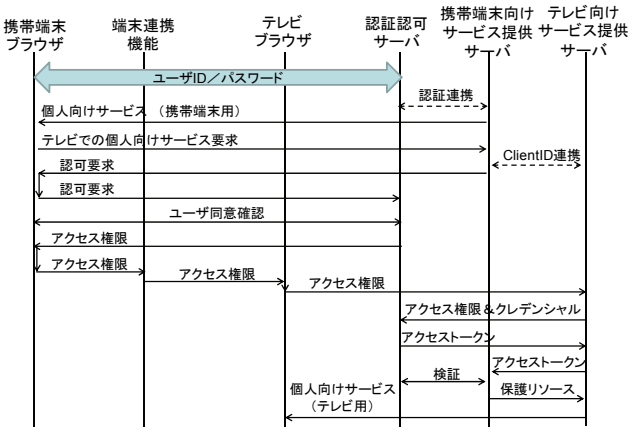

図３　端末間での権限委譲処理シーケンス

4．Hybridcast への適用

Hybridcast で導入が検討されているテレビと携帯端末間の端末連携機能を活用し，ユーザ認証認可基盤のプロトタイプシステムが正常に動作することを確認した．端末連携を活用した個人向けサービス提供図を図４に示す．

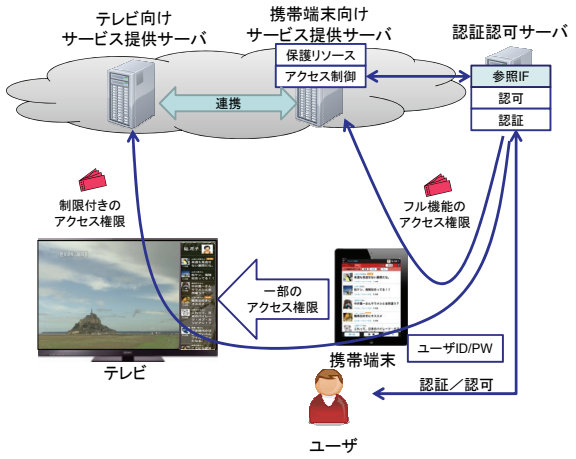

図４　テレビ視聴環境での個人向けサービス提供図

5．まとめ

放送通信融合時代のテレビ視聴環境において，個人向けサービスを活性化させるためのユーザ認証認可基盤を検討し，認証認可情報を統合管理可能なプロトタイプシステムを，OAuth2.0 をベースに構築した．さらに個人が所有する携帯端末から一部のアクセス権限のみをテレビに委譲することで，複数人が利用するテレビ視聴環境においても簡便に個人向けサービスを実現できることを確認した．今後は，効果的な権限範囲記述のための標準フォーマットなどの検討を進め，検証を進めていく．

参考文献

[1]金次ほか: ”放送通信連携システム Hybridcast の提案－放送通信融合時代の新しい放送システムをめざして－,” 映像情報メディア学会技術報告, Vol.35, No.7 (Feb.2011)
[2]OAuth2.0: http://tools.ietf.org/html/draft-ietf-oauth-v2-28 (Jun.2012)
[3]JSON Web Token(JWT): http://tools.ietf.org/html/draft-jones-json-web-token (Jun. 2012)