M-005

放送視聴データ利活用に向けた分散型データ管理モデルにおける真正性保証付き放送視聴データの生成方式の一提案

A proposal of a method for generation of signed TV viewing history data in decentralized data management model applicable to various personalized services

関根 大輔† 山村 千草† 田口 周平† 大亦 寿之† 藤沢 寛† 藤井 亜里砂†
Daisuke Sekine Chigusa Yamamura Shuhei Taguchi Hisayuki Ohmata Hiroshi Fujisawa Arisa Fujii

1. はじめに

近年、ユーザの趣味嗜好を表すパーソナルデータは、事業者がマーケティング戦略や個人向けサービスを充実させるうえで欠かせないデータとなっている。既存のパーソナルデータ管理は、個人向けサービスを提供する事業者がユーザのパーソナルデータを集中的に管理するモデルで行われていることが多い。しかし、特定の事業者が大量のパーソナルデータを囲い込むことになり、社会的責任の大きさに伴う管理コストの増加や、ユーザ側からは自らに関するデータの管理状況が見えにくいなどの課題も指摘されている。このような事業者主体の集中型データ管理モデルに対して、ユーザのパーソナルデータの所有権やコントロール権を明確にしてデータの利活用を促進する仕組みとして、ユーザ自身でパーソナルデータを管理する分散データ管理モデルが欧州を中心として検討され、日本でも社会実装が進められている[1]。

我々は、ユーザの趣味嗜好と関連が強い「テレビでいつ、どの番組を見たか」を示す放送視聴データに着目し、ユーザ自身が放送視聴データを管理し、ユーザが主体的に利活用できる仕組みの研究を進めている[2]。

サービスによっては、事業者が放送視聴データの真正性を確認する必要がある。しかし、テレビ番組の情報は公開情報であるため、ユーザから提供された放送視聴データだけから、確かにその番組を視聴したという真正性を検証することは難しい。

そこで今回、ユーザから放送視聴データを提供された事業者がそのデータの真正性を検証可能とするために、放送局が真正性を保証する真正性保証付き放送視聴データの生成方式を提案する。

2. 分散型データ管理モデルにおけるパーソナルデータの利活用

分散型データ管理モデルとは、パーソナルデータを事業者が集中的に管理するのではなく、パーソナルデータの持ち主であるユーザ自身で管理するモデルである。このモデルでは、パーソナルデータストア（PDS: Personal Data Store）と呼ばれるシステムを用いてパーソナルデータを管理する。PDS は、ユーザが自らの意思で 自らのデータを蓄積・管理するためのシステムであり、第三者への提供に係る制御機能を持つ。パーソナルデータを利活用する際には、PDS 内部に蓄積されたデータの中から必要なデータのみをデータ利活用事業者に提供していく（図 1）。放送サービスは不特定多数に向けて送られたコンテンツを受信機側で選択して視聴し、ユーザ側にデータが蓄積される。そのため、放送視聴データの管理は、分散型データ管理モデルの構造を適用しやすい。

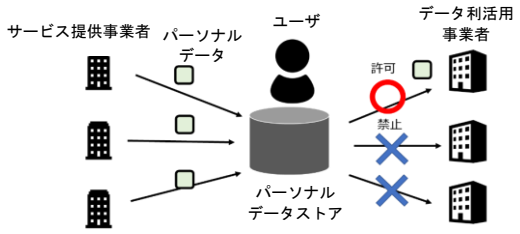

図 1　分散型データモデルでのパーソナルデータ利活用

放送視聴データを利活用する事業者によっては、特定のテレビ番組を視聴したユーザにのみサービスや対価を提供したい場合がある。しかし、いつ、何のテレビ番組が放送されたかという情報は公開情報であるため、ユーザが視聴していないのに、視聴を装うような不正が起こりうる。また、テレビ番組を放送している放送局は、ユーザのテレビ番組の視聴行動を把握していない。そのため、データ利活用事業者が、ユーザから提供された放送視聴データからその真正性を確認することは困難である。したがって、データ利活用事業者が、放送視聴データに対する適切な価値を提供するためには、ユーザから提供された放送視聴データの真正性を検証できる仕組みが必要である。

3. 真正性保証付き放送視聴データの生成方式の提案

今回、特定の事業者に管理されずに、ユーザのコントロールのもと、自身のアイデンティティを実現する仕組みとして、ユーザが Decentralized Identifier（DID）[3]を持つことを前提とした。この前提の下、ユーザが持つ放送視聴データに放送局が真正性を保証する情報を付与することで、第三者が放送視聴データの真正性を検証可能にする方法を検討した。この放送視聴データを真正性保証付き放送視聴データと定義する。真正性保証付き放送視聴データの要求条件を以下の通りに整理した。

A) ユーザは自身で放送から取得したデータを示すことで、放送局に真正性保証付き放送視聴データを生成してもらうこと
B) ユーザは真正性保証付き放送視聴データの所有権が自身に帰属することを示せること
C) ユーザは、真正性保証付き放送視聴データの内容が改ざんされてないことを、放送局以外の事業者にも示せること

† 日本放送協会 放送技術研究所
NHK Science & Technology Research Laboratories

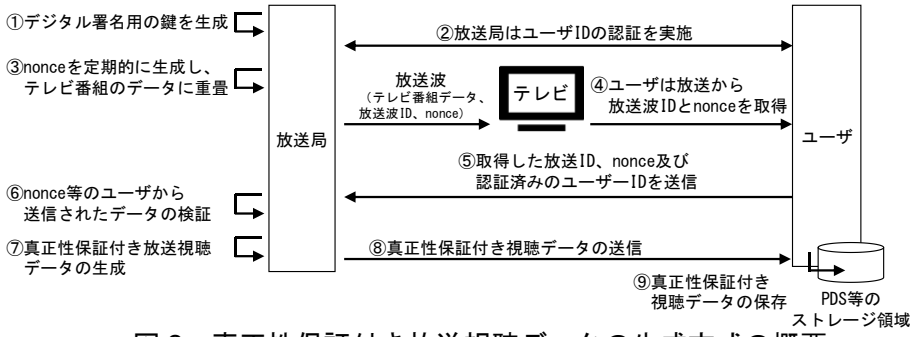

図 2　真正性保証付き放送視聴データの生成方式の概要

次に、上記で整理した要求条件を満たすため実現方法を検討した。A の実現方法として、放送局は放送するテレビ番組のデータに、時間とともに値が変わるデータ（nonce：number used once）を生成し、テレビ番組のデータに重畳する。ユーザはテレビ番組の視聴とともに nonce を取得し、放送局に nonce を送信する。放送局は nonce を確認することで、ユーザがテレビ番組を視聴したと判断し、真正性保証付き視聴データを生成する。B の実現方法として、真正性保証付き放送視聴データにユーザ ID を含めることとした。C の実現方法として、放送局が真正性保証付き放送視聴データにデジタル署名を付与することとした。

真正性保証付き放送視聴データの生成手順を次に示す（図 2）。前提条件として、放送局はユーザのユーザ ID を把握し、認証可能な機能を持つとする。手順として、まず放送局はデジタル署名に必要となる公開鍵と秘密鍵を生成する（①）。放送局はユーザのユーザ ID の認証を行う（②）。nonce を生成し、テレビ番組のデータに重畳する。その後、テレビ番組を放送波で伝送する（③）。ユーザは放送波を受信し、テレビ番組の視聴とともに放送波を識別する ID（放送波 ID）と nonce を取得する（④）。ユーザは放送局に放送波 ID、nonce、②で認証したユーザ ID を送信する（⑤）。放送局は、受信した放送波 ID、nonce が自局で送出した値と一致することと、ユーザ ID が認証済みの値であることを確認し（⑥）、真正性保証付き放送視聴データを作成する（⑦）。真正性保証付き放送視聴データには、ユーザ ID、放送波 ID、視聴時間、デジタル署名データ、署名検証用の公開鍵を取得できる URL が含まれる。放送局はユーザに真正性保証付き放送視聴データを送信し（⑧）、ユーザは受信した真正性保証付き放送視聴データを自身のストレージ領域に保存する（⑨）。

ユーザから真正性保証付き放送視聴データを提供された事業者は、真正性保証付き放送視聴データ内の URL から放送局の公開鍵を取得し、デジタル署名データを検証することでデータの真正性を確認する。

4. 真正性保証付き放送視聴データの作成システムの試作

3 章で提案した真正性保証付き放送視聴データの生成方式の試作装置を構築し、提案方式の動作検証を行った。試作装置は 5 つの部分から成り立つ（図 3）。1 つ目は、放送局側の機能を提供する放送局サーバで、nonce の生成や放送視聴データの生成などを行う。2 つ目は、ユーザが視聴するテレビとそのテレビ上で動作するアプリケーション（テレビアプリ）である。3 つ目は、ユーザ側の操作アプリケーションとなるスマートフォン用アプリケーション（スマホアプリ）である。このスマホアプリは放送局が提供するものとして、ユーザが nonce を抽出して他のユーザに転送することを防ぐ設計とした。4 つ目は、真正性保証付き放送視聴データをユーザから受け取り、データの真正性の検証後に対価となるデータを提供するデータ利活用事業者サーバである。5 つ目は、DID を想定し、放送局サーバとデータ利活用事業者サーバがユーザ ID の認証に用いる共通ユーザ ID 管理サーバである。

これら 5 つが提案した方式に従って動作し、真正性保証付き放送視聴データを生成する。今回、テレビまたはテレビアプリとスマホアプリの連携手段として、ハイブリッドキャストおよび端末連携機能[4]を用いた。生成された真正性保証付き放送視聴データは、PDS を想定したスマホアプリ内のストレージに保存し、そこから利活用事業者サーバに送信する設計とした。試作装置を用いて、3 章で示した A、 B、C の要求条件を満たした放送視聴データを生成できることを確認した。

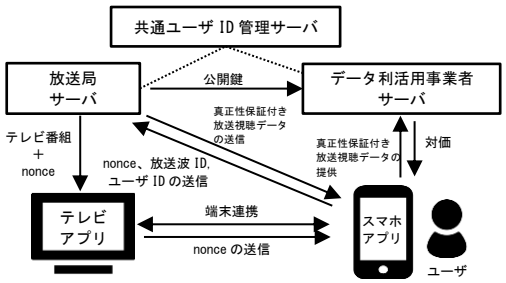

図 3　真正性保証付き放送視聴データの試作装置

5. おわりに

本稿では、分散型データ管理モデルにおいて、データ利活用事業者がユーザの放送視聴データの真正性を検証可能とするために、放送局がデータの真正性を保証する真正性保証付き放送視聴データの要求条件を整理した。その整理に基づき、真正性保証付き放送視聴データの生成方式を提案した。さらに、提案した方式の試作装置を作成し、動作確認を行った。今後、実サービスを想定したユースケースを検討し、本提案方式の適用可能性の検証を行う。

参考文献

[1] 橋田, “分散 PDS と情報銀行：集めないビッグデータによる生活と産業の全体最適化”, 情報管理, No. 60, pp.251-260 (2017).
[2] 田口他, “ユーザセントリックなデータ管理モデルにおける秘匿共通集合計算を用いた視聴データの共通要素抽出アプリの試作”, 映像情報メディア学会技術報告, vol.44, pp.37-40 (2020).
[3] Microsoft, “Decentralized Identity: Own and conrol your identity”, https://www.microsoft.com/ja-jp/security/business/identity/own-your-identity, (参照 2020-06-15).
[4] IPTV フォーラム, “IPTVFJ STD-0013 IPTV 規定 ハイブリッドキャスト運用規定 2.8 版” (2019).