N-017

コンテンツ流通おける認証機関を介さない権利譲渡方式の実現手法

Rights Transfer Method without Centric Certification for Digital Contents Distribution

諸井　太郎†　　亀山　渉†
Taro Moroi　　Wataru Kameyama

1．まえがき

ネットワーク等を媒体としたディジタルコンテンツの流通においては、一般的に無断複製等の問題があり普及が進んでいるとは言えない。また、コンテンツの「使用量に応じた課金方式」や一度購入したコンテンツ視聴の権利を他人に譲渡するような「個人間の視聴権利譲渡方式」においては、使用記録や権利情報の安全な取り扱いが課題となっている。

著者はこの課題の解決策として既にコンテンツ視聴管理システムを提案している。[1]

本稿では、コンテンツ視聴管理システムにおいて重要な２つの機能「LOG の正当性保証機能」「視聴権利譲渡機能」の実装について報告する。

2．コンテンツ視聴管理システムの概要

提案システムでは、LOG（ユーザーLOG：使用記録や視聴権利等の情報）をユーザー端末に保存した場合でも、LOG の正当性を端末単独で保証する。[1]　これにより、認証機関とオフラインの状態で、①権利者が認めた期間内でのコンテンツの継続使用、②個人間での視聴権利譲渡、を実現する。

LOG の正当性保証機能の概要を図１に示す。

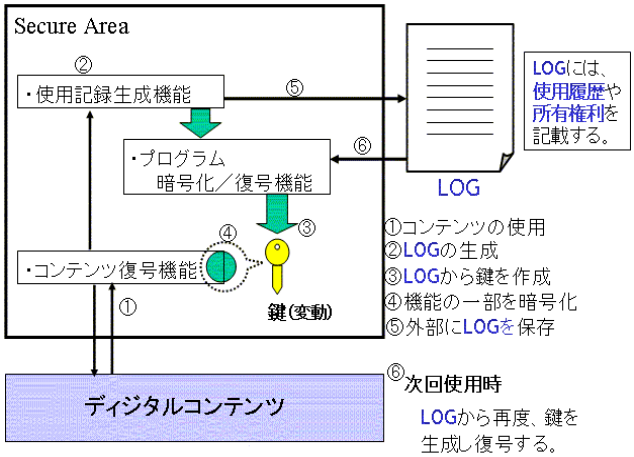

図１　LOG の正当性保証

視聴権利譲渡機能は、ユーザー間で Peer to Peer にてセキュア通信を実現し視聴権利情報の伝達を行う。

Web サービスを利用して視聴権利譲渡を実現する方法を図２に示す。ここでは、Web サービスのセキュリティ標準を利用することで端末間でのセキュア通信を実現し、User-A の視聴権利を User-B に譲渡する。まず譲渡内容に従い User-B の LOG ファイルの書換えを行い、完了後 User-A の LOG ファイルの書換えを行う。

†　早稲田大学大学院国際情報通信研究科, GITS, Waseda University

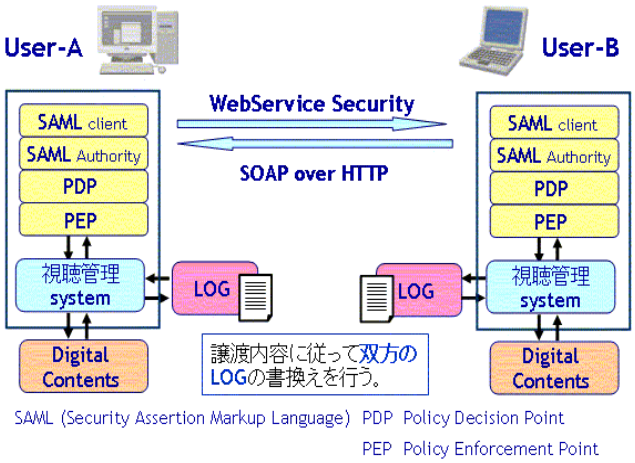

図２　視聴権利の譲渡

3．コンテンツ視聴管理システムの実装

3.1　LOG ファイルの記載内容

コンテンツ視聴管理システムの実装に先立ち、ユーザー情報を記載する LOG ファイルの記載内容について述べる。

本システム使用にあたって、事前に存在していると推定されるデータおよび LOG ファイルの記載内容は以下のとおり。

事前に存在していると推定されるデータ
- 暗号化されたコンテンツ
- コンテンツ・メタデータ
- RMPI（Rights Management and Protection Information）[2]
  （著作権保持者とその権利、利用条件、課金、セキュリティ技術情報等）

提案システムにおける LOG ファイルの記載内容
- デバイスＩＤ (deviceID)
- ユーザー情報 (UserInfo)
- 視聴履歴 (UsageHistory)
- 所有している視聴権利 (license)

3.2　LOG ファイルの構造

LOG ファイルの構造を図３に示す。

基本的な方針としては、各標準化団体(MPEG-7, TV-Anytime Forum)等で提案されている記載方法を最大限利用して、不足しているものについてのみ拡張を行う。

具体的には、Root 要素である「userlogMain」，ユーザー情報を表す「UserInfo」，視聴履歴の報告期限を表す「ReportingLimit」，コンテンツ参照ＩＤの「CRID」，視聴回数・時間を表す「validityFruquency」「validityTime」を拡張する。（独自拡張機能を下線付き斜字で示す。）

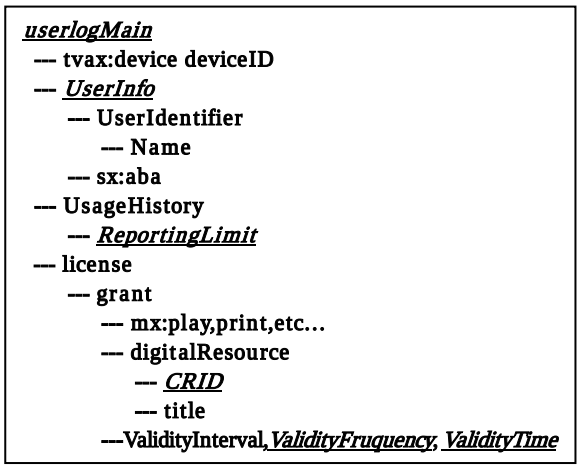

図３　LOG ファイルの構造

3.3　実装箇所

実装箇所は以下のとおりである。

（１）端末単独で LOG 情報の正当性を保証する機能

指定した LOG ファイルから秘密鍵を取り出し、その鍵を使ってプログラムを暗号化／復号する処理

（２）個人間での視聴権利譲渡機能

視聴権利情報を記載した LOG ファイルから各視聴権利情報を読み出し、User-A が選択した譲渡内容に従い、User-B の LOG ファイルを更新し、更新完了通知を得た後、User-A の LOG ファイルを更新する処理

3.4　実装環境

実装環境は以下のとおり。

JAVA：J2SDK 1.4.0

XML Parser：ELECTLIC XML 6.0.3

Web Service Platform：GLUE 1.2

3.5　LOG の正当性保証

暗号化処理の流れは以下のとおり。（図４）

①LOG の読み込み，②LOG からハッシュ値（160bit）の生成，③秘密鍵（生成したハッシュ値）を使用してプログラムファイルを暗号化

暗号化処理によりプログラムは正常に動作しないことを確認した。

復号の場合も同様に、①LOG の読み込み，②LOG からハッシュ値（160bit）の生成，③秘密鍵（生成したハッシュ値）を使用してプログラムファイルを復号，という手順で処理を行い復号したプログラムが正常に動作することを確認した。（図４）

また、LOG ファイルに少しでも変更を加えた場合には正常に復号されないことを確認した。

3.6　個人間での視聴権利譲渡

（１）譲渡する視聴権利の選択と実行

処理の流れは以下のとおり。

①LOG ファイルの読み込み，②GUI 画面に所有するコンテンツの情報を表示，③ユーザーは、譲渡するコンテンツと譲渡分量の選択し実行ボタンを押す。④指定した視聴権利譲渡内容に従い、User-B の LOG ファイルを書換え、処理「成功」通知を得た後、User-A の LOG ファイルの書換えを行う。

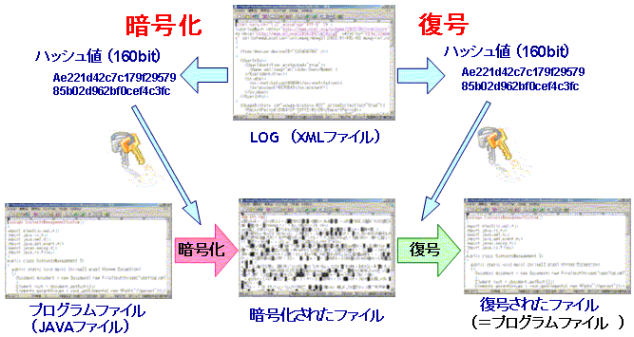

図４　プログラムファイルの暗号化／復号

（２）LOG ファイル記載内容の書換え

一連の視聴権利譲渡処理によって、User-B のログファイルには譲渡された視聴権利が追加された。（図５）

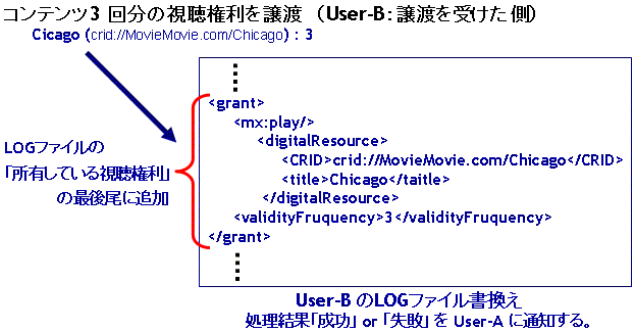

図５　User-B のログファイル

同様に、User-A のログファイルからは譲渡分の視聴権利が減少した。（図６）

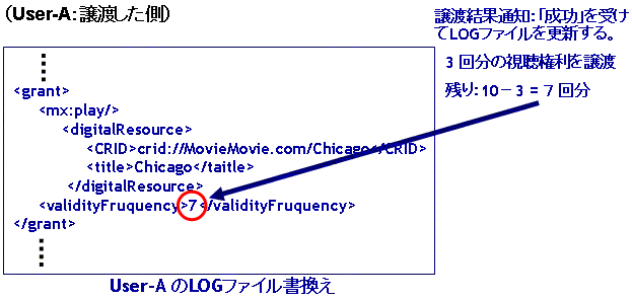

図６　User-A のログファイル

4　まとめと今後の課題

本稿では、コンテンツ視聴管理システムの実装について報告を行った。

今後は、LOG 情報に基づく課金管理や権利者への分配等に関する具体的モデルの検討が課題である。

参考文献

[1] 諸井 太郎，亀山 渉：“ コンテンツ流通システムにおける使用記録の保護と認証機関を介さない権利譲渡方式の提案 ” 情報処理学会第 65 回全国大会 5x-6 (2003.3)

[2] TV-Anytime Forum：“ RMP Specification Drafting Process Specification Workbook ”，WD550 (2002.3)