社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2006－DPS－126（38）
2006－CSEC－32（38）
2006／3／17

モバイルエージェントを活用したP2P環境における著作権管理方法の提案

齋藤　武比古、中野　泰奈、中沢　実、服部　進実
金沢工業大学大学院 工学研究科 知的創造システム専攻
E-mail: {takehiko_saito, yasuna_nakano}@acr.kanazawa-it.ac.jp,
{nakazawa, hattori}@infor.kanazawa-it.ac.jp

概 要

P2P ネットワーク上で、コンテンツと共に流通するディジタルコンテンツ情報ファイルに記載された利用条件の違反又はコンテンツの改ざん（ハッシュ値の不一致）を検出した場合、以後のコンテンツの転送を制限する Active Safety 技術と、ディジタルコンテンツ情報ファイルの改ざん又は同時すり替えを検出した場合、転送経路情報をたどりモバイルエージェントが不正行為ピアを追跡する Passive Safety 技術を併用する著作権保護方式を提案する。それを、P2P フレームワーク（JXTA）に実装し、その有効性を検証した。

A Proposal of DRM System over P2P Network using Mobile Agents

Takehiko SAITO, Yasuna NAKANO, Minoru NAKAZAWA and Shimmi HATTORI
Graduate Program in Systems for Intellectual Creation, Kanazawa Institute of Technology

Abstract

In this paper, we propose the Digital Rights Management System which employs Active-Safety technology together with Passive-Safety technology to control distribution of contents over peer-to-peer networks. The former is used for prevention of improper transfer of digital contents in case of the violation of use conditions or tampering with digital contents. The later is used for pursuing illegal peers by mobile agents in case of tampering with digital content information files, tracing the record of its transfer path. We have verified its feasibility over JXTA peer-to-peer network.

１．はじめに

近年、ブロードバンド時代の到来により、インターネット上で流通するディジタルコンテンツの量が爆発的に増加しており、クライアント/サーバモデルに代わるファイル交換方式として期待されているのが、P2P（Peer to Peer）ファイル交換方式である[1][2]。

その一方で、違法コピーされたファイルの不正利用に関する問題がある。ディジタルコンテンツは、従来に比べ複製の容易さや繰り返し複製での劣化がない特徴を有する。そのため、違法に複製された MP3 形式の音楽ファイルを流通させているとして、Napster に始まり、Gnutella、Winny などのファイル交換サービスが責任を追及されてきた。しかし、その理由は、不正にコピーされた MP3 形式フ

ファイルの登録、あるいは、流通した不正ファイルの探索、削除といった管理機能が不十分であったためである。

そこで、本来自由にファイル交換可能というP2Pシステムの特徴を維持しながら、不正コンテンツの流通を制限することを目的として、P2P ネットワーク上で、事前に不正コンテンツの流通を制限するActive Safety型技術と、事後にモバイルエージェントによって不正行為ピアの探索を行う Passive Safety型技術を併用するディジタル著作権管理方法（DRM）を提案する。

２．ディジタル著作権管理方法（DRM）

２．１　従来の著作権管理方法

DRM（Digital Rights Management）とは、ネットワーク上を流通する経済的価値のある情報（ディジタルコンテンツ）の利用について、著作者の持つ権利を保護・管理する技術である。

櫻井ら[3]は､ディジタルコンテンツの著作権保護方式を Active Safety 型技術とPassive Safety型技術に分類している。ここで、Active Safety 型技術とは、事前に不正利用を防止する技術である。一方、Passive Safety 型技術とは、事後に不正利用を検出、立証することで不正を抑止する技術である。前者の例としてはコンテンツカプセル、後者の例としては電子透かし技術がある。

２．２　著作権に関する問題点

P2P ファイル交換システムについては、技術的要請、課題とは別に、違法コピーファイルの問題が無視できない。P2P システムを運営する立場としては、管理責任を果たすことが不可欠である（不正コピーの登録防止、削除機能及び不正行為ピアの特定など)。

任､松下[4]らは､コンテンツとは別に管理情報ファイルを規定し、P2P 上の全てのピアに、ファイル交換履歴をセーブして管理する手法を提案している。しかし、この手法を実現するには、著作権情報処理のために多くのピアの資源を必要とする。また、同手法では流通経路情報を管理情報ファイルに付加する提案をしているが、具体的な不正行為ピアの追跡手段については言及していない。

そこで、本研究ではピア資源やネットワーク負荷の増加を抑えながら、モバイルエージェントにより不正行為ピアを追跡する方法を提案する。

３．著作権管理方法の提案

本研究におけるディジタル著作権管理（DRM）システムの基本コンセプトは、コンテンツとディジタルコンテンツ情報（DCI）ファイルを同時に流通させることである。

本DRMシステムは３個の構成要素から成る。

- ディジタルコンテンツマネージャー（DCM）
- モバイルエージェント（MA）及びモバイルエージェントベース（MAB）
- P2P ネットワーク上のピアにロードされたクライアントソフト

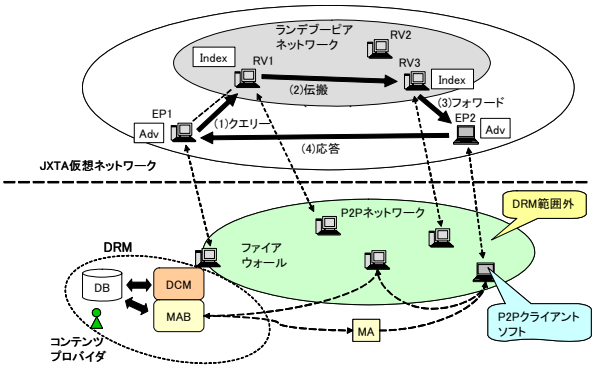

図１　DRMシステムとP2Pネットワーク

３．１　ディジタルコンテンツマネージャー（DCM）

DCM は DRM システムの中核をなし、コンテンツのデータベース（DB）登録や流通を管理するソフトウェアである。セキュリティ上、コンテンツプロバイダ（CP）のみが DCM を利用する。DCM の機能は以下の通りである。

- コンテンツの DB 登録、削除機能（CP がコンテンツ情報を管理するため使用）
- MA の移送先初期値とするため、第一世代ピアの IP アドレスをログに残す機能
- 不正ピア情報を MAB から受け取る機能
- 利用許諾条件を付加したディジタルコンテンツ情報ファイルの作成機能

３．２　モバイルエージェント（MA）及びモバイルエージェントベース（MAB）

一旦 P2P 上に置かれたコンテンツファイルは、DCM の管理から独立して流通する。

コンテンツファイルの不正利用を検出するには、受信側のピアが送信側のピアの不正を検知する機能を各ピアのソフトウェアに組み込むことも可能ではあるが、その処理のために各ピアの資源を余分に使わなければならない。また、P2P ネットワーク上の全ピアがデータベースにアクセスする可能性があることになり、データベースのセキュリティの面から問題となる。そこで、モバイルエージェント[5]の活用を考える。

モバイルエージェント（MA）とは、実行中にネットワーク上のコンピュータ間を移動しながら特定の処理を行うプログラムである。一方、モバイルエージェントベース（MAB）とは、MA の拠点となるプログラムである。

MA/MAB のミッションは、以下の通りである。

(1) 全てのハッシュ計算値とディジタルコンテンツ情報ファイルを DB のオリジナルと比較し、改ざんを検出し、処置すること

(2)ファイル改ざんを検出した場合､経路情報を解析して改ざんを行ったピアを追跡すること

MA の主な機能は、以下の通りである。

- P2P の各ピアが保存している全てのハッシュ値とディジタルコンテンツ情報ファイルを MAB に持ち帰る機能
- 経路情報を解析し、コンテンツが送信されてきたピアへ移動して追跡する機能

一方、MAB の主な機能は以下の通りである。

- MA が持ち帰ったハッシュ値とディジタルコンテンツ情報ファイルを DB にあるオリジナルと照合して、改ざんを検出する機能
- DB へのアクセス機能（移送先初期値のダウンロード、不正ピア情報のアップロード）

ユーザにとって、MA がピアを巡回し、不正検出を行うことは、自己の関知しない不正ファイルを自らのフォルダにダウンロードしてしまい、意図せず権利侵害することを未然に防止できる点でインセンティブとなる。

３．３　P2P クライアントソフト

DRM の立場での P2P クライアントソフトのミッションは、利用条件違反コンテンツの流通を制限することである。その機能は、

- コンテンツファイルに対応するディジタルコンテンツ情報ファイルが揃わない場合、流通を不許可とする機能
- コンテンツファイルのハッシュ値（Ha’）を計算し、ディジタルコンテンツ情報ファイルに記載されたハッシュ値(Ha″)と比較し、不一致の場合は、それ以降の転送を禁止する機能
- 全てのハッシュ値とディジタルコンテン

ツ情報ファイルを MA に渡すために保存する機能

- 経路情報を追加する機能

３．４　ディジタルコンテンツ情報（DCI）ファイル

ディジタルコンテンツ情報は、DCM がコンテンツの管理と保護に用いる情報で、利用許諾条件を含む以下の４つの属性からなる。

- ファイル情報
  コンテンツファイルに関する情報。ファイル名、サイズ、ハッシュ値など
- コンテンツ情報
  コンテンツの概要を示す情報。タイトル、アーティスト名、ジャンルなど。
- 著作権管理情報
  著作権管理を行う上で必要な情報。権利者、利用許諾条件など。
- プロバイダ情報
  コンテンツプロバイダに関する情報。

これらは必要最小限の構成で、カスタマイズ可能である。

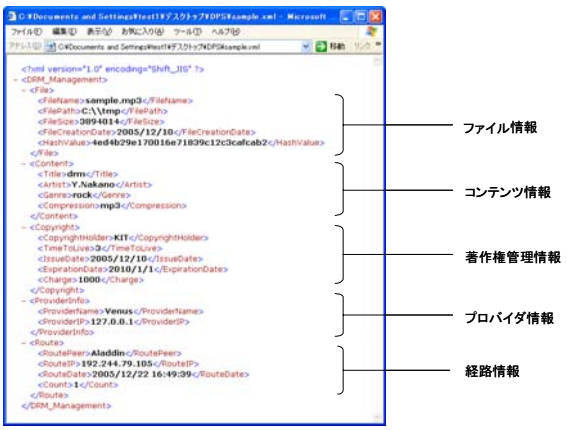

図 2 ディジタルコンテンツ情報ファイル

上図はディジタルコンテンツ情報ファイル（XML 形式）の例である。ここで、経路情報（IP アドレス、日付など）は、Passive Safety 型技術として MA が不正行為を行ったピアを追跡するため、流通経路の各ピアで、次のピアへの転送時に付加されるものである。経路情報には、Active Safety 型技術で使用するピア間累積転送回数(count)も含まれている。

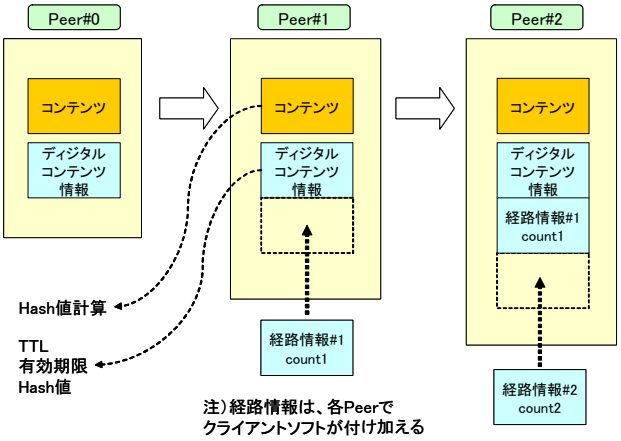

図 3 ディジタルコンテンツ情報の遷移

３．５　不正検出処理

本研究で取り扱う不正と保護方式の対応は、下表の通りである。

表１　不正と保護方式の対応

不正の種類	保護方式
利用条件違反（ピア間転送回数オーバー、コンテンツ有効期限切れ）	Active Safety 型
コンテンツファイルの改ざん（ハッシュ値の不一致）	
ディジタルコンテンツ情報ファイルの改ざん	Passive Safety 型
コンテンツとディジタルコンテンツ情報ファイルの同時すり替え	

次に、不正検出処理について説明する。

(1) コンテンツから計算した MD5 ハッシュ値（Ha’）と、ディジタルコンテンツ情報ファイルに記載されたハッシュ値（Ha″）が不一致の

場合、いずれかが改ざんされているので、それ以降ファイル転送を不許可とする。(クライアントソフトの役割)

(2) ディジタルコンテンツ情報ファイルが改ざんされたか否かは、オリジナルと全文比較することで判別する。(MA、MAB の役割)

(3) ピアで判定可能な条件 (Ha'≠Ha″) だけでは、コンテンツと記載 Hash 値の同時すり替え (Ha'= Ha″≠Ha) が判定できないので、MAB へ持ち帰り、判定する。すり替えが判明した場合は、MA をクライアントソフトに移動し、該当ファイルを転送禁止にする。

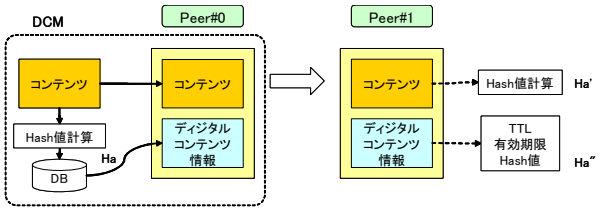

図 4 各ハッシュ値の説明

4. 著作権管理方法の実装

4. 1 実装検討システム

実装検討用に、学内ネットワークに 4 台の Windows PC を配置し、JXTA ネットワーク[6]を形成した。その内 1 台には、DCM 機能もインストールした。

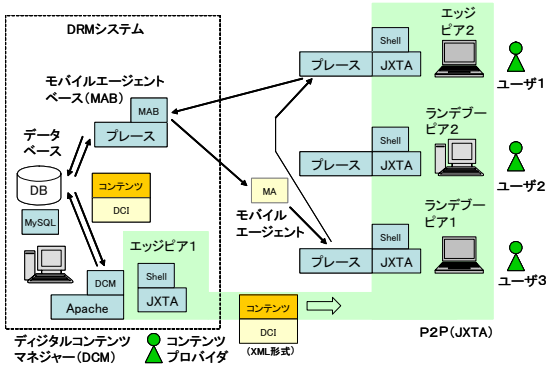

図 5 実装検討システム

(1) P2P

P2P ファイル交換システムの実装には、Java ベースの JXTA[7]を使用した。JXTA は、ピアやピアグループのサービス告知、他のピアからの探索、発見機能、ピア間の通信機能など P2P システム構築に必要なフレームワークを開発者に提供しており、これを利用した。本研究では、JXTA アプリケーションの一つである JXTA Shell に、Java で作成したコマンドを追加することで実装した。

(2) DCM

DB 登録、管理の GUI は、Apache ベースの Web アプリケーションとして実装した。開発言語は MySQL、PHP5 を使用した。

(3) MA 及び MAB

当研究室において Python 言語で開発したエージェント移動型[8]の MA (Pylets) を使用した。移動先ピアの IP アドレスを指定し、プレース (本研究では、Apache ベースの Web アプリケーション) へ移動する。

4. 2 実装結果の確認

コンテンツの登録・管理機能をもつ DCM の起動画面を次図に示す。各処理画面は、起動画面から遷移する。

図 6 DCM 起動画面

次に、JXTA Shell に Java で作成したコマンドを追加し、利用条件違反 (例として、ピア間転送回数オーバー) の場合にファイル転送が不許可になることを確認した結果を次図に示す。

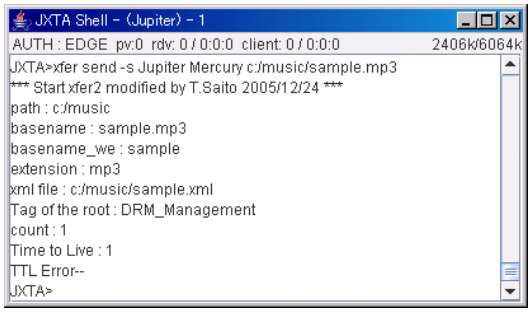

図 7 JXTA Shell 実行例
(転送不許可 count≦TTL)

今回は、検討日程の関係から、モバイルエージェントについては、独立して動作検討を行い、全体での実装検討まで行えなかった。次回の課題としたい。

５．まとめと課題

従来、P2P ファイル交換システムでは、不正なディジタルコンテンツの管理・流通が問題とされてきた。本研究では、Active Safety 型技術と Passive Safety 型技術の併用により、不正コンテンツの流通を防止する著作権管理方式を提案した。

ここで、Active Safety 型技術とは、コンテンツと共に流通するディジタルコンテンツ情報ファイルに記載された利用条件違反（ピア間転送回数オーバーなど）またはコンテンツファイルの改ざん（ハッシュ値の不一致）を検出した場合、それ以後のコンテンツファイルの転送を不許可とするものである。一方、Passive Safety 型技術とは、ディジタルコンテンツ情報ファイルの改ざんまたは同時すり替えが行われた場合に、経路情報をたどりモバイルエージェントが不正行為ピアを追跡するものである。

そして、コンテンツ登録・管理機能を有するディジタルコンテンツマネージャーを作成し、JXTA Shell に追加コマンドを作成して実装を行い、提案した著作権管理方法の有効性を確認した。

今後の課題として、JXTA ネットワークでは、ファイアーウォール越えのファイル転送が可能なため、これを考慮した JXTA アプリケーション版モバイルエージェント[9]の検討も必要である。

参考文献

[1] 「P2P の真実」Aug、2004、日経バイト

[2] 曽根原 登（監修）、画像電子学会（編）、「ディジタル情報流通システム」東京電機大学出版会

[3] 櫻井 紀彦他、「コンテンツ流通における著作権保護技術の動向」情報処理学会論文誌：データベース、vol.42、No.SIG 15(TOD 12)、pp.63-76、Dec、2001

[4] 任 光輝、松下 正彦、「P2P ネットワークにおける著作権管理方法の提案と実装」信学技報、IN2004-153、TM2004-76、OIS2004-74 (2005-01)

[5] 佐藤 一郎、「モバイルエージェント技術と研究動向」NII Journal、no.3、pp.53-66、2001

[6] Bernard Traversat et al.、「Project JXTA 2.0 Super-Peer Virtual Network」http://www.jxta.org/project/www/docs/JXTA2.0protocols1.pdf

[7] JXTA http://www.jxta.org/

[8] 本位田 真一、飯島 正、大須賀 昭彦、「エージェント技術」共立出版

[9] Rita Yu Chen、Bill Yeager、「Java Mobile Agents on Project JXTA Peer-to-Peer Platform」Proc. of the 36th HICSS Conference、2003