6K-4

P2P ネットワークにおける情報の流通監視方式の提案

仁野裕一　加藤大志　福岡秀幸　谷幹也
ＮＥＣ　インターネットシステム研究所

1. はじめに

近年、ブロードバンド環境の普及に伴い、P2P ネットワーク(NW)によるコンテンツ配信サービスが急速に立ち上がりつつある[1][2][3]。このようなサービスでは、各ピアのコンテンツ保有/転送状況からユーザの興味/ユーザ間の情報交換頻度などのマーケティング情報を得るために、情報の流通状況を監視すること(トレーシング)は有効である。

ところが、現存する P2P コンテンツ配信方式の多くは、(1)自らの P2P NW 以外でコンテンツが流通することを完全には抑止できない、もしくは(2)ユーザがコンテンツを再生しないかぎりコンテンツ流通経路が捕捉されない、などの問題があるため、流通捕捉漏れのない正確なトレーシングが困難であった。

筆者らは、特定の P2P NW 内で情報の流通状況を監視するトレーシングサーバに DRM(著作権管理)機能を付加することにより、その NW 外での流通を抑止しつつ、コンテンツを再生せず単にダウンロードしただけでも流通を捕捉できる流通監視方式を提案する。

本稿ではまず現状の流通監視方式の問題点、提案する流通監視方式の概要/有効性について述べ、弊社で研究開発中の P2PWeb プラットホームへの適用、及び応用例について説明する。

2. 現在の流通監視方式の問題点

現在の P2P NW によるコンテンツ配信サービスでは、流通監視方式として電子透かし[3]を利用した方式、DRM[4][5]を利用した方式の２つが多く検討されている。電子透かしを利用する場合、コンテンツを特定するための ID や著作権情報を透かしとして埋め込み、P2P NW を起動するソフトが流通を管理する DB にトレース情報を登録する。また、DRM を利用する場合、コンテンツを流通前に暗号化し、ライセンスサーバへライセンスを要求する際に、流通先 ID を登録していくことによってトレーシングを実現する。しかし、これらは以下のような問題があった。

まず、電子透かしを利用した方式は、コンテンツの移動/コピーを特定の P2P NW 内に制限することはできないため、その NW 外に一度情報が流出してしまうと、その後流通情報を捕捉することはできない。また、DRM を利用した方式は、あらかじめ P2P NW 上に存在するピアをライセンスサーバに登録しておくことによって、コンテンツが特定の P2P NW 外に流通してもその再生を防止することによって流通を抑止できるが、ユーザがコンテンツを再生するためにライセンスサーバにアクセスに行かないとトレースできない。例えば、図１のようにコンテンツが流通された場合、実際の流通経路は Peer A→Peer B→Peer C であるにもかかわらず、Peer B はコンテンツを再生するためのライセンス購入を行っていないため、ライセンスサーバには Peer A→Peer C に流通したようにログが残ってしまう。

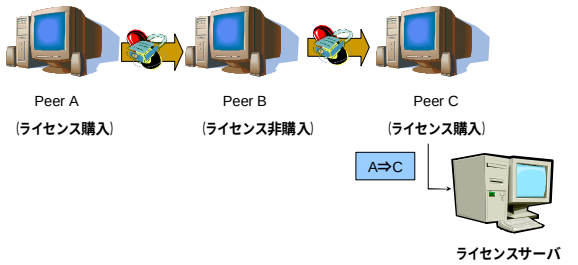

図 1 DRM を利用した従来の流通監視方式

3．提案する流通監視方式

筆者らはこのような問題を解決するため、P2P NW 上でのコンテンツ共有機能に、コンテンツ送信履歴を管理するトレーシングサーバとの通信機能と DRM 機能を付加した流通監視方式を提案する。図２に本方式の全体構成図を示す。

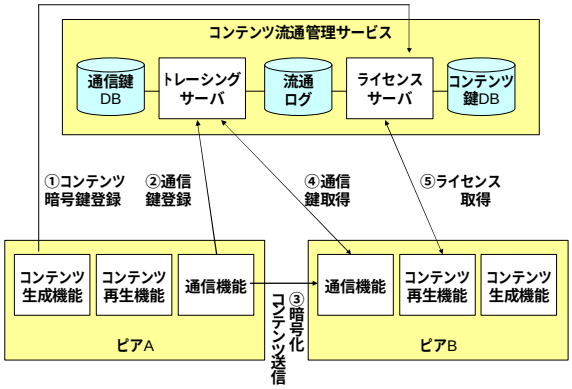

図 2　提案方式の全体構成図

本方式では、以下の方法により流通監視を実現する。

①コンテンツを生成したピア（ピア A）が、そのコンテンツを暗号化し、その暗号鍵（コンテンツ鍵）と再生制御情報をライセンスサーバに登録する。

②ピア A が当該コンテンツを別のピア（ピア B）から送信要求を受けた際には、One Time で生成した鍵を利用してコンテンツを二重暗号化し、その鍵(通信鍵)とコンテンツ ID、ピア A/ピア B の ID をトレーシングサーバに SSL などの秘匿通信を利用して登録する。

③ピア A からピア B に二重暗号化されたコンテンツを送信する。

④ピア B がコンテンツを受信すると、トレーシングサーバに秘匿通信を行い、コンテンツ ID、ピア A/ピア B の

A proposal of an information tracing method in the P2P network
Yuichi NINO, Dasihi KATO,　Hideyuki FUKUOKA and Mikiya TANI, Internet Systems Research Laboratories, NEC Corporation

ID を登録する。トレーシングサーバは②で登録されたものと一致した場合に該当する通信鍵をピア B に送信する。それから、ピア B は二重暗号化されたコンテンツを一回復号する。それと同時に、トレーシングサーバは、コンテンツがピア A からピア B に送信されたログ（流通ログ）を DB に保存する。
⑤ピア B がコンテンツを再生する際には、ライセンスサーバにコンテンツ鍵を要求する。ライセンスサーバは、流通ログを解析して、コンテンツがピア B に流通されたことを確認すると、コンテンツ鍵と再生制御情報を含むライセンスを発行する。ピア B はライセンスを受信すると、再生制御情報に応じてコンテンツを再生する。

4．本方式の有効性

本方式では、(a)コンテンツが特定の P2P NW 外に転送され利用されること、(b)ピア ID の改ざん・なりすまし、(c)コンテンツ送信先(図 2 ではピア B)が fake され、トレーシングサーバに正しい情報を送信しないことの３つの脅威を想定した。コンテンツ送信元の fake を想定しなかったのは、コンテンツ作成者が自分のコンテンツの流通状況を監視できなくすることは考えにくいことと、流通監視を利用したサービスがコンテンツ流通元を優遇するものであるため、送信元がトレーサビリティを阻害するモチベーションがないという理由による。

以下、それぞれの脅威について以下のように対抗した。
(a)ライセンスサーバが流通ログを参照し、P2P NW 上で流通を確認できないものにはライセンスを発行しない。
(b)事前にサーバからピア ID を記載した証明書(ピア証明書)を発行することによって ID の改ざんを防止し、ピア証明書を端末個別に暗号化し格納することによってピア証明書の転送を防止する。
(c)送信元ピア/送信先ピアからのトレーシングサーバへの登録情報が一致しなかった場合、トレーシングサーバが通信鍵を送信先ピアに発行しない。

さらに、本方式では、図１のようにコンテンツが流通しても、Peer A からライセンスを購入していない Peer B への流通ログもトレーシングサーバに残るため（図３）、従来方式[4][5]に比べてより正確なトレース情報を取得できるようになっている。

また、本方式は、サーバを利用しているが、通信鍵・コンテンツ鍵のみの通信のため、サーバ＝クライアント型のコンテンツ配信に比べてサーバのボトルネックは発生せず、ある程度のスケーラビリティは確保できるものと考えられる。

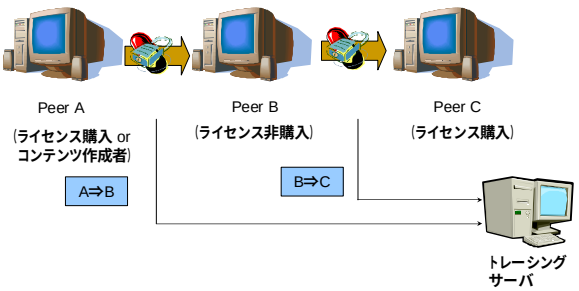

図 3　本方式による流通経路の捕捉

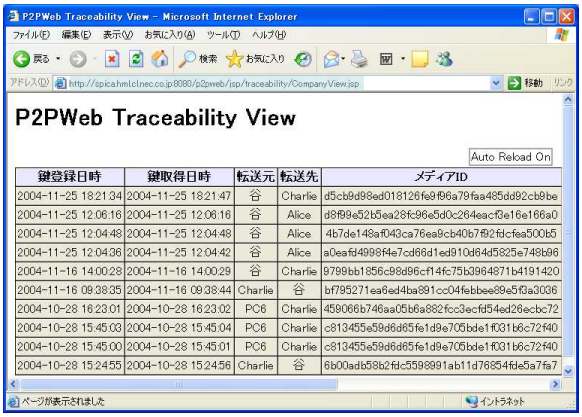

図 4　流通ログ

5．P2PWeb プラットホームへの適用と応用例

本流通監視方式を筆者らが開発中の P2PWeb[5]上で実装を行った。初期の実装として、DRM は Windows Media Rights Management[7]を利用し、Windows Media Format のコンテンツに対して流通監視を行った。図４に Web サービスで流通ログを表示した画面を示す。なお、本方式を実装した P2PWeb プラットホームで作成した Windows Media Format のコンテンツをメモリカードで他のピアに転送して再生を試みたが、再生することはできなかった。

本流通監視方式の応用としては、以下のようなものが考えられる。
・e -learning のような応用において、教材の配布と学習状況の確認に利用する。
・P2PWeb によるコンテンツ配信サービスを安定化させるため、コンテンツ配布に貢献するユーザにインセンティブを付与することによって、P2PWeb を起動状態にすることをユーザに促す。
・コンテンツに広告を付加し、広告を見たことをライセンスサーバが確認してライセンスを発行することと、流通ログとの照合をとることによって、広告の効果度を測定する。([4]の応用)

6．おわりに

本稿では、特定の P2P NW 内で情報の流通状況を監視するトレーシングサーバに DRM(著作権管理)機能を付加する流通監視方式を提案し、その有効性・P2PWeb を利用した応用例について説明した。今後は、DRM 機能を拡張して P2PWeb 上で対応するコンテンツフォーマットを拡大すると同時に、本方式のビジネスモデルの応用など実用化に向けた研究開発を行う予定である。

参考文献

[1] BitTorrent, http://www.bittorrent.com/
[2] Peer Impact™, http://www.peerimpact.com/
[3] SNOCAP, http://www.snocap.com/
[4] NetLeader, http://netleader.mtf.ntt.ocn.ne.jp/feature/index.html
[5] Open Mobile Alliance, “OMA DRMv2 specification” Dec.2004, http://www.openmobilealliance.org/
[6] 神谷他，“P2P によるセキュア情報流通プラットホーム”,第 67 回情処全大, 2004
[7] Windows Media Rights Management, http://www.microsoft.com/windows/windowsmedia/drm/