

コンテンツ、メタデータの改ざん防止及び両者の一致性を

6G-7

保証する方式の提案*

西谷 智広†

高橋 健司‡

日本電信電話株式会社

NTT 情報流通プラットフォーム研究所¹

1 はじめに

現在、広く普及している Naspter 型の P2P (Peer to Peer) コンテンツ配信においてコンテンツ毎に課金をすることは困難を伴う。なぜならばコンテンツ仲介者が課金等をしようとするコンテンツの特徴を記述したメタデータを利用するが、そのメタデータは利用者によって簡単に改造でき、またメタデータと対応しないコンテンツを他の利用者へ送信する事が可能なためである。本方式ではメタデータを利用者が改ざんできないようにすることに加え、コンテンツとそのコンテンツメタデータの対応を保証する手法を提案する。

2 セキュリティ対策

著作権を守るためにコンテンツを暗号化すると、特定のソフトウェア、端末でしかコンテンツを利用できないという点が指摘されている。本検討ではコンテンツ自体には暗号化を施さず、付随するメタデータの管理を厳重にすることにより利便性を向上する事に成功した。

2.1 コンテンツ

コンテンツには信頼できる第三者機関によりコンテンツ ID が割り当てられる。また著作権者は十分に長い乱数文を作成する。これをバインド数と呼ぶ。著作権者はバインド数を著作権者の秘密鍵によって暗号化した（暗号化バインド数と呼ぶ）後、信頼できる第三者機関によっ

てコンテンツ ID と暗号バインド数を電子透かしでコンテンツに埋め込む。

コンテンツはパッケージあるいはインターネット等で利用者に流通する。利用者はコンテンツ ID を検出することができるが、バインド数を知るのは困難である。著作権者は暗号化された暗号化バインド数を平文に直すための公開鍵をコンテンツ仲介者に送信する。

2.2 メタデータ

本方式ではメタデータを XML で記述する。XML には著作権者名、コンテンツ名、価格、コンテンツ ID、コンテンツ流通のための条件等が書き込まれる。

また、コンテンツとメタデータの一致性を保証するためにチェック値を導入する。チェック値はハッシュ関数 MD5 を用いて

チェック値＝

MD5(メタデータの一部、バインド数)

である。計算後、XML にチェック値を記入する。このチェック値により、コンテンツとコンテンツメタデータの対応確認が可能となる。

メタデータはコンテンツと付随して流通される。メタデータには著作権者による電子署名がされていて、改ざんができないようになっている。電子署名を確認するための公開鍵はメタデータと同時に流通される。

3 実際のコンテンツ流通の仕組み

本方式の流通システムでは著作権者（製作者）、コンテンツ送信者、コンテンツ受信者、コンテンツ仲介者の 4 者から成り立つ。(図 1) 流通の手順を説明する。

*Prevention from Fabricating Content and Content Metadata

†Tomohiro Nishitani

‡Kenji Takahashi

¹NTT Information Sharing Platform Laboratories

- (1) 著作権者はコンテンツ、メタデータを作成する。コンテンツにコンテンツ ID、暗号化バインド数を電子透かしで埋め込む。コンテンツの電子透かし処理は第三者機関に委託する。
- (2) 暗号化バインド数の公開鍵、電子署名確認用公開鍵を仲介者に登録する
- (3) 送信者は著作権者からコンテンツとメタデータを入手する
- (4) 送信者はコンテンツに埋めこめられたコンテンツ ID、暗号化バインド数を読み取り仲介者に渡す。
- (5) 仲介者は公開鍵で暗号化バインド数をバインド数になおし、メタデータを使って仮チェック値[MD5(送信されたメタデータの一部、バインド数)]を計算する。この値がメタデータのチェック値と等しければ、コンテンツ及びコンテンツメタデータは信頼できるとする。
- (6) 受信者は仲介者からメタデータを検索し、コンテンツを直接送信者から入手する。コンテンツを送信終了後、受信者は課金される。
- (7) 著作権者に著作権料が仲介者から支払われる。

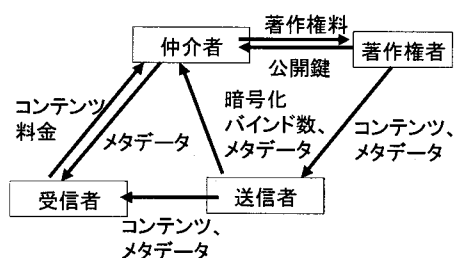


図1 流通構成図

4 検証

上記のシステムで改ざん及び成りすましが可能かどうか検証する。

4.1 メタデータの改ざん

メタデータは著作権者によって電子署名がされているので利用者がメタデータを改ざんすることは難しい。

4.2 メタデータ、コンテンツの偽造

利用者はコンテンツに埋め込まれている暗号化バインド数からバインド数を推測することは困難である。よって、メタデータを偽造しても仲介者側の手続き中で仮チェック値とチェック値の値が合わず、不正を発見することが可能である。コンテンツ偽造については信頼ある第三者機関によって方式非公開の電子透かしでバインド数が埋め込まれると、第三者によってコンテンツにバインド数を埋め込むことができないので上記と同様の理由でコンテンツの偽造は防止できる。よってコンテンツとメタデータの一致性は保証される。

4.3 フィルタリング

万が一、不正コンテンツが流通した場合にはそのバインド数及びメタデータを記録しておき、それに一致したものを仲介者システムで排除し、流通できなくする。

5 Napster との比較

1) メタデータ

本システムではメタデータが改ざんできないようになっている。Napster の場合、利用者のファイル名によって著作物を判断しているためにコンテンツを別名で名乗ることで流通可能となる恐れがある。

2) コンテンツ、メタデータの一致性

Napster ではファイル名、ファイルサイズ等によってファイルが正当であるかを区別するしかない。本システムでは仲介者がバインド数を用いてコンテンツ及びコンテンツメタデータの正当性を保証するため、課金決済等も可能である。