

P 2 P ネットワークにおけるオープン D R M システム

Open DRM System over Peer-to-Peer Network

李 栄慶¹⁾

Rongqing Li

1) 慶応義塾大学理工学研究科 (〒223-8522 神奈川県横浜市港区日吉 3-14-1 矢上キャンパス
24 棟 315 室 E-mail: li0426jp@ybb.ne.jp)

ABSTRACT. An open digital rights management system, which is seamlessly integrated with a peer-to-peer network, is proposed in this paper. All necessary components, including packaging application for contents providers, access license delivery service for clearing houses, usage charging service for billing operators, and contents accessing application for end users, are developed as service/application over the peer-to-peer network. And XrML technology, a default world-standard rights expressing language, is used in this system for rights-related messaging and rights processing, so that an open, interoperable and transparent system is ensured.

1. 背景

デジタル技術の進展とブロードバンド時代の本格到来に伴い、インターネット上のデジタルコンテンツ流通市場が著しく拡大していることを無視できない状況となっている。人類は新しい技術に恵まれている一方で、いろいろな新しい脅威にも直面している。ハイテク技術により、デジタルコンテンツの不正利用や複製は、簡単且つ高品質に出来るようになってきている。この問題の解決に、国内外において注目されているデジタル・ライツ管理技術 (Digital Rights Management、以下 DRM と称す) は、情報化社会におけるデジタルコンテンツ流通の健全なる発展には不可欠であることが伺える。

その一方で、今まで伝統的なウェブベースのコンテンツ流通がメインであったが、インターネット上の情報データ量が爆発的に増加し続ける現在、将来のコンテンツ流通には適用できない多くの課題 (流通コストの高い、流通速度の低いこと等) をはらんでいる。

一つアプローチとして、近年、ピア・ツー・ピア (Peer to Peer、以下 P2P と称す) 技術が注目され、デジタルコンテンツ流通の革新的な促進の役割を果たすと考えられている。P2P の利用で、安価且つ高速なコンテンツ流通が期待され、研究者の焦点となっている。

しかし、Napster や Gnutella などの悪用で、P2P そのものが著作権侵害の張本人であるというダメージ的な印象付けがなされているケースが少なくない。P2P 技術の利点を最大限に利用し、著作権を完全保護する上でのコンテンツ流通においては、P2P における DRM が言うまでもなく重要である。

今まで、数多くの企業や研究機関は、様々な DRM 技術を開発していたが、殆どウェブベースの技術であり、P2P での応用には十分ではない。加えて、DRM ベンダー各社は、独自の仕様を採用しているため、コンテンツ・プロバイダーや電子商取引事業者らは、DRM を利用するビジネスシステム (課金システムやコンテンツ販売システム等) を構築する際、DRM による異なるシステムの構築が必要となっている。この問題の解決に、幾つかの標準団体は、XML の技術を用いるオープンな DRM 記述言語を W3C に提案しており、標準的なオープン DRM システム構築を

図っている。その中に、XrML (eXtensible rights Markup Language) [1] 技術は、その中でも最も注目されている一つである。

2. 目的

本システムは、従来の DRM システムが抱えている課題を解決し、安全・効率なコンテンツ流通の実現、それとオープン DRM 環境の創設を目的としている。

(1) 安全・効率なコンテンツ流通の実現

本システムは、コンテンツ流通において、P2P ネットワークの最大利点である高速・安価の特性を活用し、コンテンツの悪用を抑止する DRM 機能を P2P ネットワーク機能の一部として実装したことによって、P2P ネットワークと DRM 機能をシームレスに統合でき、従来 DRM システムと比べて、コンテンツ流通のトラフィック拡大に応じ、コンテンツの不正利用や権利処理などの技術課題も解決することを図っている。

(2) オープンな D R M 環境の創出

当システムは、デジタルコンテンツの権利情報について、オープンな DRM 記述言語である XrML を利用している。従来の DRM システムと比べて、ビジネスシステム相互接続性の向上やシステム 2 重開発の削減を実現できることを目的としている。

3. システム開発内容

(1) システム概要

本システムは、コンテンツ流通のための一つ P2P ネットワークを構築し、そのネットワークのサービス或いはアプリケーションとして、DRM 機能のエンド・ツー・エンドコンポーネントを開発した。コンテンツ流通ビジネスの関係者たちは、該当 P2P ネットワークにおいて、安全・合理かつ本格的な超流通 [2] を可能にするデジタルコンテンツ流通プラットフォームのプロトタイプを実現している。

システムのコア技術要素として、P2P ネットワークの

構築は JXTA[3] 技術を利用しており、オープン DRM における通信プロトコルおよび権利表現は XrM 技術を利用している。JXTA の採用は、ユビキタスデバイス (PC、PDA、携帯端末等) への拡張可能性、オープン性、それと優れる P2P 機能 (ピアグループの管理、ピア間のパイプ通信技術、サービス機能) 等の考慮である。XrML 技術の採用は、世界標準の最有力候補と見据え、Mpeg-21 などの国際標準団体に利用実績を有し、且つ拡張性・柔軟性 (豊富なビジネスモデルを記述可能) を評価する上の選択である。

完成しているシステムは、コンテンツ・プロバイダー (コンテンツホルダやコンテンツアグリゲータ等が含まれる。以下 “プロバイダー” と称す) 用のパッケージングアプリケーション、コンテンツ利用者 (以下 “エンドユーザ” と称す) 用のコンテンツ再生アプリケーション、クリーニングハウス (コンテンツ利用に必要なライセンスを発行する個人、或いは事業者を指す。以下、 “ライセンス発行者” と称す) 用のライセンス発行サービス、及び課金事業者 (有料コンテンツ利用に於いて、課金を行う個人、或いは事業者たちを指す。以下、 “課金事業者” と称す) 用の課金サービスの四つコンポーネントから構成される。

コンテンツ流通ビジネスの関係者であるプロバイダー、エンドユーザ、ライセンス発行者、それと課金事業者は、何れも、JXTA の P2P ネットワークに動作する Peer の一つとして実装され (複数機能を一つの Peer に実装するのも可能)、Peer と Peer の間の通信は、JXTA の Pipe やサービス等の技術を利用し、通信するメッセージのフォーマットはすべて XrML を採用している。

図 1 には、システム全体イメージを表した。

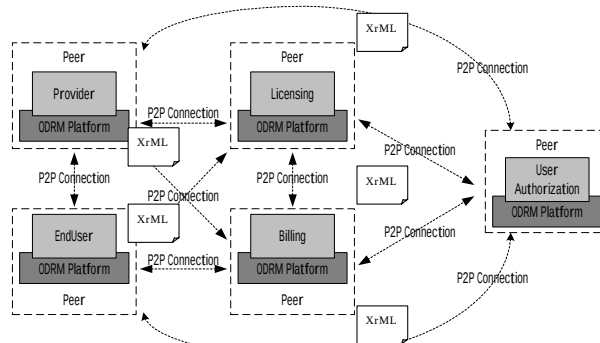


図 1 システム動作イメージ

上記、主に四つのピア群が存在し、それぞれがプロバイダー、エンドユーザ、課金事業者、及びライセンス発行者を代表する。さらに、同じ機能のピアがピアグループ (プロバイダ集合の ProviderPeerGroup、エンドユーザ集合の EnduserPeerGroup、ライセンス発行者集合の LicensingPeerGroup、課金事業者集合の BillingPeerGroup、それと全体ピア集合の ODRMPeerGroup) を結成し、各自のサービスをピアグループの機能として、関連するピアグループにあるピア同士にサービスを提供している。この手法で、機能を柔軟に拡張できる一方で、ピアグループにある一つピアが故障しても別のピアが機能代行でき、サービスを楽しむときにも相手の存在を意識しなくても利用できる利点がある。

(2) システムアーキテクチャ

P2P ネットワークの構築において、様々な技術が考えられるが、前節に説明したように、今回は Jxta 技術を利

用している。図 2 には、DRM コンポーネントを Jxta プラットフォームに実装する際のシステムアーキテクチャを表した。

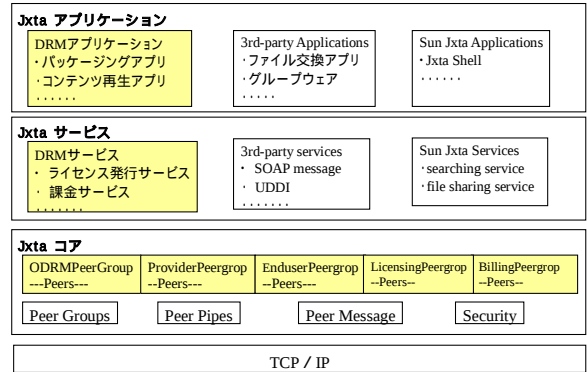


図 2 システムアーキテクチャ

Jxta プラットフォームは、TCP/IP 上のレアに実装されており、Jxta コア層、Jxta サービス層、及び Jxta アプリケーション層から構成されている。図 2 に塗りつぶす部分のブロックは、今回 DRM コンポーネントの実装範囲を表している。コンテンツ流通の各関係者を管理するために、五つ Peergroup を Jxta のコア層に実装した。加えて、ライセンス発行サービスと課金サービスは、Jxta のサービス層に、パッケージングアプリケーションやコンテンツ再生アプリケーションは、Jxta のアプリケーション層に、実装されている。

(3) 権利処理のデータモデル

本システムでは、権利に関わる処理について、XrML 技術採用し、システムの相互接続性、オープン性、それと今後の拡張性を保つことを図っている。図 3 には、XrML データモデルの概念図[1]を表したい。

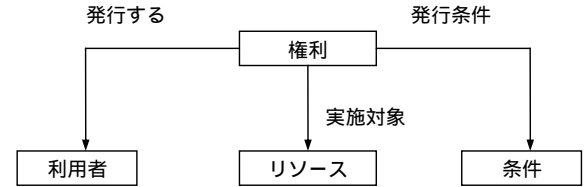


図 3 XrML データモデル

この図に、権利所有者はコンテンツ利用者にある条件を満たす時点で、あるリソースに対するある指定した権利を許諾することを表した。当システムは、コンテンツプロバイダがライセンス発行者へコンテンツのライセンス発行権利を付与する際、それとライセンス発行者がエンドユーザにコンテンツ再生権利を付与する際、XrML データモデルとのマッピング状況は、それぞれ表 1、表 2 に表した。

表 1 コンテンツプロバイダ権利実施のデータモデル	
権利	ライセンス発行
リソース	指定コンテンツ (音楽ファイル)
条件	無条件
利用者	ライセンス発行者

表 2 ライセンス発行者権利実施のデータモデル	
権利	視聴
リソース	指定コンテンツ

条件	一定料金で回数制限及び期間制限
利用者	エンドユーザ

すべての権利データは、規定している XrML スキーマに基づいて、XML ファイルで表現している。図 3 には、一つのユースケースを例として、XML で表現したファイルレイアウトを表した。

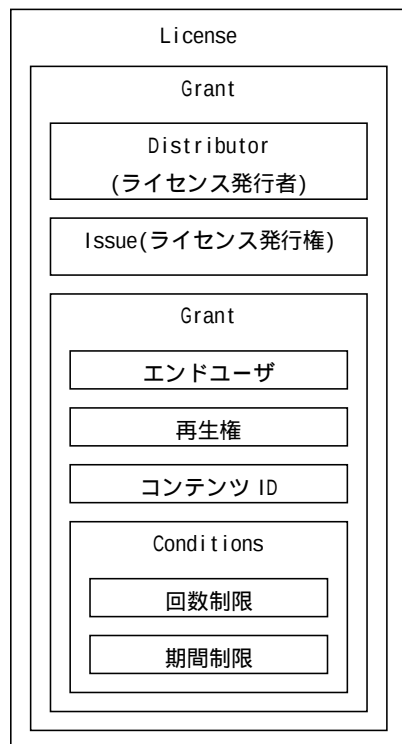


図 3 XrML ファイルレイアウト(例)

この XrML ファイルを解析すると、コンテンツプロバイダー（一次ディストリビューターとも言う）は、コンテンツファイル(リソース)をある条件（一定費用で回数や期間などの制限での条件）で、ライセンス発行者（一次の権利使用者、二次のディストリビューターとも言う）に授権し、ライセンス発行者は、この権利（視聴ライセンスを発行する権利）で、エンドユーザが課金事業者へ課金してから、コンテンツ視聴権利を有するライセンスを発行でき、エンドユーザは、このライセンスを利用しコンテンツを使用可能となると、意味する。

本システムには、XrML データモデルを処理するために、XrML ファイルの生成や構造解析などの共通モジュールを開発した。

（４）DRM コンポーネント

a) パッケージングアプリケーション

パッケージングアプリケーションは、コンテンツの暗号化処理、コンテンツ使用を制限する権利（以下、ビジネスルールを称す）生成、及びビジネスルールの発行処理を提供する。さらに、共通 XrML 機能及び暗号化機能（暗号化及びデジタルサイン機能を含む）を利用し、XrML の権利ファイルに対して暗号化とデジタルサインを行う。

b) コンテンツ再生アプリケーション

コンテンツ再生アプリケーションは、コンテンツの再生及び利用を中心に、コンテンツ利用のためのライセンス要求、課金要求、取得したライセンスの管理、コンテンツの解読及び再生などの一連処理を提供している。P2P ネットワーク上で流通するすべての情報は XrML で定義

され、送信側が暗号化及びデジタルサインを行い、受信側は暗号化解読やデジタルサインの検証を行っている。

c) ライセンス発行サービス

ライセンス発行サービスは、エンドユーザからのライセンス請求を受け取り、課金情報を検索した結果により、ライセンス発行或いは課金誘導情報発行のいずれを行う。

d) 課金サービス

エンドユーザから料金支払いを受け、ビジネスルールにより支払いを確認、課金済情報を発行する。加えて、課金済情報を管理し、ライセンス発行者からの課金済情報検索要求に応答する。特定な課金済情報でライセンスを発行されたら、該当課金済情報を削除する。

e) 共通管理機能

ODRM システムのユーザ、及びピアグループを管理するコンポーネントである。ピアグループの生成、追加及びグループに所属するユーザの作成、認証、および削除などの操作を行う。

4．評価

（１）評価目標

当システムは、「P2P ネットワークにおけるオープン DRM システム」のプロトタイプ完成を目標としている。機能面には、パッケージングアプリケーション、コンテンツ再生アプリケーション、ライセンス発行サービス、及び課金サービスの四つ機能群は、P2P ネットワークにおいて障害なく互いに通信でき、必要なコンテンツ保護、及び XrML で表現している権利処理を実現できることは、今期の目標となっている。性能面には、オープン性及び拡張性を強調しているが、レスポンス、セキュリティ、及び GUI は特に要求していない。

（２）機能評価

図 4 から図 7 までは、当システムのデモ画面を表した。DRM に必要な機能（暗号化処理からライセンス発行、疑似課金、コンテンツ再生まで）は JXTA の P2P ネットワークにて、すべて実現していることを評価できる。

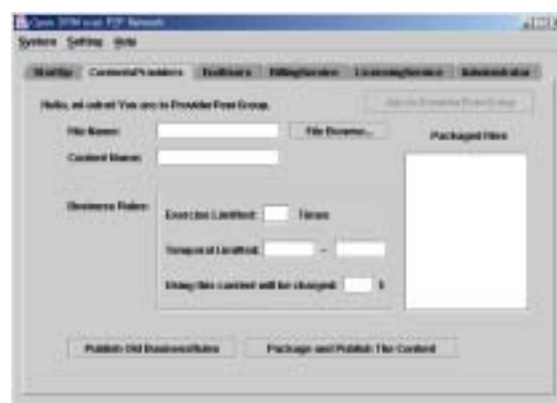


図 4 パッケージングアプリケーション



図5 コンテンツ再生アプリケーション

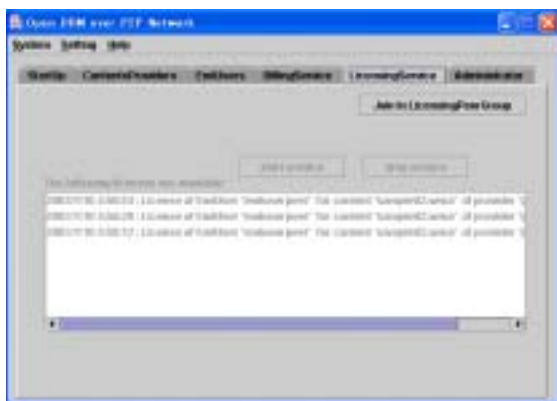


図6 ライセンス発行サービス

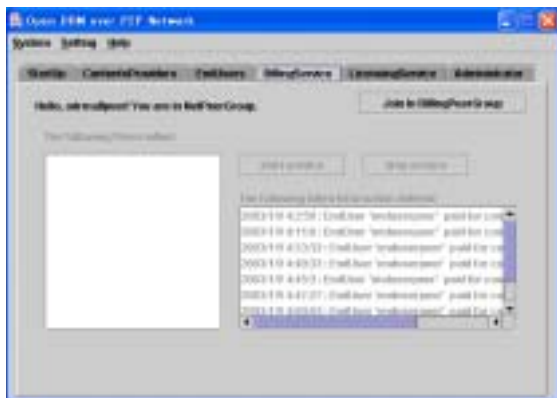


図7 課金サービス

(3) 性能評価

当システムは、すべての通信プロトコルは XrML を利用しているので、完全オープン、拡張性のよいシステムであると言える。また、JXTA の課題で、システムのレスポンスが低い一方で、セキュリティ面にも商用サービスに向けて改善すべき事項となっている。

5. システム特徴

本システムは、大きく、統合性、オープン性、利用性、拡張性、及び競合性の五つ特長があると述べる

(1) 統合性

当システムは、P2P ネットワークと DRM システムをシームレスに統合できたシステムである。今まで、P2P 流通プラットフォームでのコンテンツ不正利用は、P2P 技術の発展に大きくダメージを与えていた。最近、P2P 事業者は、DRM 技術の取り込みを検討し始まっているが、いずれも、P2P システムと DRM システムが完全分割しており、別々のシステムとして実装されているので、ユーザの利用性が低い一方で、コンテンツ流通効率性も低いという課題が指摘されている。

(2) オープン性

当システムは、オープン DRM 記述言語である XrML を採用することで、様々なビジネスモデル(レンタル、購買、および超流通など) に容易に対応できる一方で、DRM ベンダーに依存しない課金システムやライセンス発行システム等のビジネスシステム開発が可能となっており、システム 2 重投資の不要やシステム相互接続の向上などの面に、大きく意味を持っていると言える。

(3) 利用性

DRM コンポーネントは、任意のピアに実装できるので、コンテンツの専門プロバイダーから、一般企業、そして個人まで、コンテンツの出版利用及び対価支払が可能となっている。

(4) 拡張性

当プロトタイプシステムには、WMA(Windows Media Audio) ファイルのみを実装しているがピア間のメッセージ交換や暗号化システムは、すべてコンテンツタイプ(音楽・映像・文書等) に対応できるように設計しているので、強力な拡張性を持っている。

(5) 競合性

当システムは、「P2P ネットワーク」と「オープン DRM」の二つキーワードを基に、P2P ネットワークと DRM システムをシームレスに統合できる一方で、オープンな DRM システムを開発したので、非常に市場性と競合性のあるシステムであると言える。

6. 期待効果

当システムの利用に当たって、コンテンツ流通ビジネスの各関係者に対して、下記の効果が期待できる。

(1) プロバイダーへの効果

P2P 流通プラットフォームを利用することにより、流通コストを大幅に削減でき、流通速度も劇的に加速できることを期待できる。さらに、コンテンツ販売においても、様々なビジネスモデル(レンタル、購買、超流通、およびペイ・パー・ビュー等) を実現でき、事業の収入拡大が期待できる。

(2) エンドユーザへの効果

欲しいコンテンツを随時に安価で入手でき、最適なユーザパフォーマンスを追求できる。

(3) クリーニングハウス及び課金事業者への効果

DRM ベンダーに依存しないシステムを提供できるので、2 重投資の防止やシステムの信頼性、安全性、及び効率

性の向上を期待できる。

加えて、著作権保護を実現できる上に、P2P での最適なコンテンツ流通プラットフォームを提供することにより、アーティストの創作促進、コンテンツ関連事業者の流通促進などに貢献し、利用者の対価支払の意識向上、及び情報化社会の健全発展に重要な役割を果たすことも期待できる。

7. 残り課題

今回のプロジェクトは、プロトタイプシステム開発を目標としている。今後、商用化システムの完成に当たって、いくつかの課題が残っている。

(1) JXTA 技術課題

JXTA プロジェクトは、開発中の技術であり、レスポンスの向上やセキュリティの問題などの解決していない技術課題は多数残っている。

(2) 完全 P2P の分散処理は不現実

ユーザ認証や課金情報通信などにおいて、セキュリティ面も技術面にも、現在、完全な P2P システムの実現は困難となっている。当システムでは、当面、ユーザの登録・認証は中央サーバーにより集中管理を行っている。それと、課金処理やライセンス発行処理においても、任意のピアから利用できるのではなく、ピアグループを形成する際に、ある権利を獲得したピアのみ、それらの機能を行えるという「集中・分散」のハイブリッド手法を採用している。

(3) 利用者の普及が必要

当システムの利用性は、利用者の数と直接関連している。P2P ネットワークに参加しているピア数が多ければ、レスポンスを向上させ、利用価値も格段的に拡大できる。今後、商用サービスに当たって、如何に利用者を獲得できるのか、ビジネス成功のポイントとなる。

(4) XrML の普及

現在、XrML は世界標準の有力候補となっているが、利用している企業、それとシステムの数はまだ少ない。当システムのオープン性、相互交換性の長所は十分果たせない状況となっている。今後は、XrML の普及に伴い、当システムの利用価値も高まってくるでしょう。

8. 参加企業及び機関

(1) 京都高度技術研究所、プロジェクト管理実施組織

(2) 杭州サンゾンソフト有限公司、製造作業の外注先

9. 参考文献

- [1] Contents guard, INC.: <http://www.xrml.org>
- [2] 森亮一, 河原正治 : “歴史的必然としての超流通”, 情報処理学会「超編集・超流通・超管理のアーキテクチャシンポジウム」論文集, pp.67-76 (1994)
- [3] Sun Microsystems, INC.: <http://www.jxta.org>