端末フィンガープリント情報を用いたハイブリッド暗号化方式

陳, 春璐
九州大学

穴田, 啓晃
九州先端科学技術研究所

川本, 淳平
九州大学

櫻井, 幸一
九州大学

出版情報：平成27年度（第68回）電気・情報関係学会九州支部連合大会, pp.09-2P-04-, 2015-09-26
バージョン：
権利関係：

P2P 技術に基づくデジタル著作権管理の特徴と電子マネーとの比較による考察

陳　春璐* 穴田　啓晃** 川本　淳平*,** 櫻井　幸一*,**
(*九州大学院システム情報科学情報学専攻 **財団法人九州先端科学技術研究所)

1　はじめに

インターネットの普及に伴い，インターネットを利用したデジタルコンテンツの伝播が増えている．一方，P2P(peer to peer)という技術があり，他の技術より簡単にファイルを共有できる．そのため，デジタルコンテンツの違法コピーと違法伝播が容易となり問題となっている．技術で違法コピーや不正使用などを防止するのは，今の研究の焦点になっている．その対策として，P2P に基づくデジタル著作権管理(DRM; Digital Right Management)は沢山の研究が行われている．P2P に基づくデジタル著作権管理システムは，デジタルコンテンツ提供者の利益を保護する．さらに，ユーザの間でデジタルコンテンツの転送と共有を実現する．本稿では，既存のP2P に基づくデジタル著作権管理技術を分析する．また，既存の電子マネーシステムを検討し，その特徴を分析することにより，P2P 型デジタル著作権管理システムに応用できる点を考察する．

2　P2P に基づくデジタル著作権管理システム

2.1 一般的なデジタル著作権管理システム

デジタル著作権管理（Digital Rights Management）はインターネット環境で発展してきたデジタルコンテンツを保護する技術である．特に，違法使用と違法コピーを防ぐことを目的としている．ユーザはDRM に権限を申請しない限り，デジタルコンテンツの使用ができない．

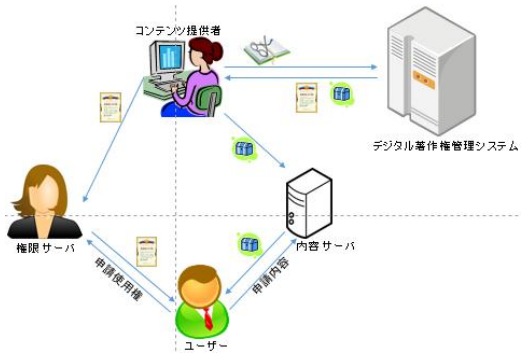

図１：一般的なデジタル著作権管理システム

図1に，一般的なデジタル著作権管理システム[1]の構成を示す．コンテンツ提供者は著作権管理システムを利用して，カプセル化されたコンテンツと認証証を生成する．暗号化されたコンテンツをコンテンツサーバにアップロードして，認証証は権限サーバにアップロードする．ユーザはダウンロードしたコンテンツを利用するため権限サーバに申請使用方式で認証証を手に入れ，コンテンツを利用する．一般的なデジタル著作権管理システムは利用者数が増加すると，著作権管理システムサーバの通信量も増大し，サーバが混雑した状態になりやすいという問題点がある．

2.2 P2P に基づくデジタル著作権管理システム[2]

P2P ネットワークの構成にはいくつかの種類があるが，本稿では，中央集権的なサーバを必要としないピュア P2P を考える．この方式では，サーバを経由する必要がないため，ネットワーク通信方式として効率的な利用が可能となる．P2P 技術の主な目標は，すべてのユーザにストリームを提供することある．提供された資源はブロードバンド，ストレージスペースと計算能力を含めているため，我々が前述したP2P ネットワークのメリット利用できる．

P2P に基づくデジタル著作権管理システムは幾つかのモデルがある：1）既存のクライアント・サーバに基づくP2P モデル．2）分散型P2P モデル．3）ハイブリッド型P2P モデル．その他，スーパーコンピュータに基づく P2P モデルがあるが，スーパーコンピュータは普及していないので，本稿は検討しない．

表１：三種類の P2P モデルの比較

モデル	メリット	問題点
集中型P2P	P2P の配分技術でユーザのストリームを利用する	サーバが落ち込む状態になりやすい
分散型P2P	ノード(ユーザ端)で DRM 関連のサービス機能が付いている	ルートノードだけ復号鍵と認証証を発行できる
ハイブリッド型	安全性が高くなる	上記の問題がある

表１に以上三種類の P2P モデルの比較を示す．既存のクライアント・サーバに基づく P2P モデルはすべての DRM 関連サービス機能（コンテンツのカプセル化や認証証の発行）は伝統的な DRM サーバで処理される．分散型 P2P モデルはすべてのノード(ユーザ側)で DRM 関連のサービス機能を付けている．ハイブリッド型P2P モデルと分散型 P2P モデルの唯一違う点は，ユーザの認証機能を DRM サーバで行う点である．

3　電子マネー

電子マネーとは，現金をデジタルデータの形に変換し，デジタル情報伝達で現実の金銭授受を実現する仮想通貨である．実質的に貨幣という物品によってやり取りされていた所を，デジタルデータによって決済する手法である．

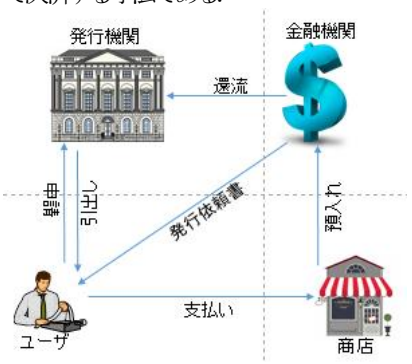

図2：電子マネーの構成図

図2は，一般的な電子マネーの構成を示す．利用者は電子マネーを利用する際に発行機関に申請した後，金融機関から発行依頼書を取得，発行機関から電子マネーを取得する．商店に電子マネーを支払い，商店はこの電子マネーを預入れる．金融機関は受け取った電子マネー情報を発行機関に送信する．

[3] によれば，この電子マネーには次のような特徴がある．

表2:電子マネーシステムとDRMシステムの比較

性質	集中型電子マネー	分散型電子マネー	P2Pに基づくDRMシステム
事前対策	コピー等不正行為の防止	コピー等不正行為の防止	コピー等不正行為の防止
事後対策	不正が行われた場合不正者が発覚すること等	不正が行われた場合不正者が発覚すること等	不正が行われた場合不正者が発覚すること等
分割利用可能性	保有する価値を任意の単位に分割して利用可能	保有する価値を単位に分割して利用可能	分割利用可能，Freeの部分とお金をかかる部分
店頭・ネットワーク双方にて支払い可能	店頭・ネットワーク双方にて支払い可能	店頭・ネットワーク双方にて支払い可能	店頭・ネットワーク双方にて支払い可能
効率的な発行管理	電子マネーの発行・管理を効率的に行う，発行コストを抑えるとともに，高速な処理を可能	新しいcoinの開発に，時間がかかる．開発権利の申請は高速な処理を可能	認証証明書の発行・管理を効率的に行う，発行コストを抑えるとともに，高速な処理を可能
プライバシー保護(追跡不能性)	利用者の購買に関するプライバシーが小売店や金融機関等が結託しても露見しない	利用者の情報を保護不可，追跡可能	利用者の利用回数に関するプライバシーがコンテンツ提供者または代理人だけが見える
プライバシー保護(関連づけ不能性)	同一利用者により使用された電子マネー情報が相互に関連づけられない	利用者の情報を保護不可，関連づけ可能	同一利用者によりコンテンツの使用回数情報が関連しているが，異なるコンテンツの使用情報が相互に関連づけられない
オフライン性	当事者のみで支払処理可能	合法利用者のみで利用が可能	合法利用者のみで利用が可能
転々流通性	受け取った電子マネーをそのまま他の支払い等に使用可能	受け取った電子マネーをそのまま他の支払い等に使用可能	第三者に転売する可能
携帯性	IC カード等の持ち運び可能な媒体で処理できる	メモリ等で持ち運び可能な媒体で処理できる	メモリ等で認証証明書の持ち運び可能な媒体で処理できる

- 安全性:電子マネーシステムは違法コピーや不正ユーザ発見など違法行為を防ぐことができる.
- 電子マネー特有の利便性:分割利用可能性;便利な支払い方式;効率的で安全な発行管理
- 現金が持つメリットの継承:ユーザ情報の保護;マネーの転々流通性;携帯やすい;複数の金融機関の対応

4　電子マネー利用したP2Pに基づくデジタル著作権管理システムの考察

電子マネーシステムとDRMシステムの区別を示すため，表2に電子マネーシステムとDRMシステムの比較をまとめた．この表を元に，P2PにおけるDRMシステムが参考にできる点をまとめると次のようになる.

- **独立性**：外部条件を依存せず，複数の金融機関が同一の電子マネーを利用できる.DRMの文脈ではコンテンツの使用権は外部条件を依存しない．言い換えれば，どのプラットフォームでも利用できることを意味する.
- **プライバシー保護**：電子マネーでは利用者の情報を保護している．DRMにおいても，ユーザの情報は保護されるべきである.
- **効率的な発行**：電子マネーでは，発行・管理が効率的に行えるとともに，偽造不可の性質がある.安全性と効率は電子マネーシステム設計の二つの重要な条件であり，違法コピーは電子マネーシステムの中で禁止しなければならない.DRMにおいても，安全かつ効率的にコンテンツの使用と転送が行える必要がある.
- **分割区別可能性**:電子マネーでは,定められた粒度の中で,保有する価値を任意の単位に分割して利用することができる.資源を有効利用するため，保護されたコンテンツを分割利用できるべきである.

上記の比較を通じて，P2Pに基づくDRMシステムを改善するため，電子マネーシステムのメリットを利用できる.効率的かつ安全性が高いP2Pに基づくDRMシステムを構築できると考える.

5　まとめ

本稿は一般的なDRMシステムとP2Pに基づくDRMシステムを検討し，それらの問題点を分析した．また，電子マネーシステムとDRMシステムを比較した．これらにより，電子マネーシステムの利点をDRMシステムに活用できると考える.柔軟性，安全性高い効率的なP2Pに基づくDRMシステムを構築することが今後の課題である.

謝辞

本研究の一部は，日本学術振興会 科学研究費補助金 基盤研究(C) (課題番号24500084) による補助のもとで行われた.

参考文献

[1] k. Wlliam, C. Chi-Hung, “Survey on the technological aspects of Digital Rights Management,” 7th International Conference, ISC2004. Palo Alto, CA, USA. pp.391-403

[2] J, Lin. D, Yu. S, Xiao. B, Yu. “IMS-based P2P Streaming Service System”. ICCASM2010. pp.61-66

[3] 中山 靖司，森島 秀実，阿部 正幸，藤崎 英一郎，“電子マネーの実現方式について―安全性，利便性に配慮した新しい電子マネー実現方式の提案―”，IMES Discussion Paper Series 97-J-5.