九州大学学術情報リポジトリ
Kyushu University Institutional Repository

電子現金プロトコルを用いた著作権管理システムの提案

北原, 基貴
九州大学

川本, 淳平
筑波大学

櫻井, 幸一
九州大学

https://hdl.handle.net/2324/1662079

出版情報：コンピュータセキュリティシンポジウム. 2013, pp.3D2-3-, 2013-10-23
バージョン：
権利関係：

KYUSHU UNIVERSITY

電子現金プロトコルを用いた著作権管理システムの提案

北原 基貴† 川本 淳平‡ 櫻井 幸一†

†九州大学
819-0395 福岡県福岡市西区元岡 744 番地

‡筑波大学
305-0006 茨城県つくば市天王台１－１－１

あらまし デジタル上における著作物は、保存や複製が容易というその特徴から、違法コピーが大量に作られてきた。これを防ぐために用いられるのが著作権保護システムである。コンテンツ提供者が正規購入者を判別するための認証サーバを導入し、コンテンツを一元管理するという手法が多く用いられてきたが、そのサーバにアクセスが集中してしまうことや、サーバが故障してしまうとコンテンツ自体を使えなくなるという問題が存在した。本論文では P2P をベースとした暗号のみに安全性を依存している Bitcoin に注目し、このシステムを利用して著作権保護に用いることを考える。P2P を用いることにより配布用サーバにかかる負担を最低限にコンテンツの配布が可能となる。また、本提案方式では従来の P2P における方式と比べ、二次配布ができることや誰もが正規利用者かどうかの認証が可能という利点が存在する。

A Method of Digital Rights Management based on Electric Commerce Protocol

Motoki Kitahara† Junpei Kawamoto† Kouichi Sakurai†

†Kyushu University.
744 motooka, Fukuoka, Fukuoka prefecture, 819-0395, JAPAN

‡University of Tsukuba.
1-1-1 Tennodai, Tsukuba, Ibaraki, 305-0006, JAPAN

Abstract In digital world, so many copyrighted works are made in illegal way because it is easy to keep and copy. Digital Rights Management has proposed to prevent this theft. Contents providers often bring in one server which have charge of managing the normal user, but there are some problems that it flock to the server and the contents become unusable if the server has broken. In this paper, we propose new DRM based on Bitcoin which is one of the electric commerce. There is no need to prepare the server to verify and everyone can verify.

1 序章

1.1 背景

インターネットの普及とコンピュータの発展に伴い，様々なコンテンツが情報媒体として取り扱われるようになってきた．音楽データや画像データ，文書データなどが主な例である．こういったデータはデータそのものに価値があり，デジタルな媒体として使用することが可能である．小型端末で大量にデータを持ち歩くことができるという利点により，特に音楽データを筆頭として広まってきた．しかし，このデジタル媒体はインターネットを通して不特定多数と媒体を共有できてしまうという問題がある．これ

を防ぐ，正規の購入者のみが利用可能にするために導入されたのが著作権管理システムであるDRM(Digital Rights Management) である．

1.2 DRM の現状と問題

DRM を使用する場合，利用者が購入できるコンテンツは暗号化されたものとなる．この暗号化されたコンテンツを利用する際の手順は以下となる．

1. 正規の購入者は直接コンテンツ配布者のサーバと通信を行い，自身が正規の購入者であると認証を行う．
2. 正規の購入者であると証明できたら，コンテンツ配布者のサーバは購入者が持つパソコンのコンテンツ再生用ソフトウェアに対して復号鍵を送る．この際，正規の購入者であっても復号鍵を自由に使うことはできない．
3. コンテンツを利用する際，利用者はコンテンツ再生用ソフトウェアのみを用いてコンテンツを利用する．コンテンツ再生用ソフトウェアは自身が持つ復号鍵を利用し，コンテンツを復号しつつ再生する．
4. コンテンツの再生が終了したら，コンテンツ再生用ソフトウェアは復号鍵を廃棄する．

以上の通り，正規の利用者でもコンテンツを復号しつつ再生するため，暗号化されていないコンテンツを得ることはできない，このことにより，暗号化されていないコンテンツの二次配布を防ぐ事ができるといえる．この DRM の問題点として，コンテンツ配布者のサーバに掛かる負担が大きいという点が存在する．正規の利用者がコンテンツを利用したいと思った場合，復号鍵を得るためにこのコンテンツ配布者のサーバと通信することが必要となる．利用者の数が増加すればするほどこの通信は増え，認証にかかる負担も増加する．もしこのサーバが負担に負け，落ちてしまった場合，全ての正規の利用者はコンテンツを再生することができなくなる．この点は DRM を利用しない場合と比べて正規の利用者に負担をかける，利便性を低下させるということであり，大きな問題といえる．

1.3 関連研究

DRM には，通信方式を元にするとサーバ・クライアント型方式と P2P 型方式の二つが提案されている．本章では，これらの型での実現手法と違いについて検討する．DRM では，以下の二段階の暗号化を行うことで，コンテンツの暗号化を行う．

- コンテンツを暗号化する．
- 暗号化されたコンテンツに対し，コンテンツを利用するための条件とコンテンツを扱うプログラムを付加し，カプセル化する．

1.3.1 サーバ・クライアント型 DRM

DRM が導入された初期は，こちらの通信方式が主だった．この方式ではコンテンツ配布者が管理専用のサーバを導入し，そのサーバがユーザに対して暗号化コンテンツを復号するための鍵を配布，正規ユーザかの検証など，全ユーザの管理を行うシステムであった．この手法におけるコンテンツを利用するための条件は，サーバから秘密鍵を受け取ること，となる．利点としては，管理が一元化でき，ユーザの調査や課金の管理が容易であるという点がある．しかし，この手法の問題点として，コンテンツを利用するユーザが増えれば増えるほどそのサーバに対する負荷が増大するという問題があった．このため，検証用のサーバを複数作成し，負担を減らすという手法が取られてきた．人数に応じてサーバの数を増やすことで，ある程度拡張性に関しても動的に対応できる．しかし，サーバの増設の問題やユーザの人数は読みづらいという問題の根本的な解決にはなっておらず，以下の P2P 型 DRM が提案された．

1.3.2 P2P 型 DRM

DRM の実装ではユーザの ID を用いて検証を行うという手法が考えられている．コンテンツ

再生用ソフトウェアを，コンテンツの初回起動時に自分の ID を管理サーバに送るような仕様にし，管理サーバは登録されている ID に対して後日代金を請求するというものである．この手法では，利用条件は特にない．このような仕様にすることで，自由に配布することが可能となる．コンテンツを希望するユーザが一度に大量に出たとしても，コンテンツ保持者から P2P を利用してダウンロードが可能であり，サーバに負担をかけることもなくなる．コンテンツの不正利用に関しては，コンテンツの初回起動時に自分の ID を送る，という点にかかっている．

この P2P を利用した DRM 方式として，岩田らの提案した手法が知られている [2]．この手法では P2P を利用した DRM を複数提案すると共にその実装も行い，速度の検証を行なっている．また，オプションとしてピア間のみの通信で完結する分散 P2P ベースの DRM システムと，管理を行うサーバを導入した半分散 P2P システムの両方が提案されている．

- 分散 P2P ベース DRM システム
  分散 P2P ベースの DRM システムでは，あるユーザにメタ情報や ID のカプセル化の許可を与え，そのユーザが正規利用者の管理を行うという手法である．この手法では全体の規模の大小やサーバの負荷の問題は解消されるが，利用状況の調査や金銭面の管理の難しさなどが問題となる．
- 半分散 P2P ベース DRM システム
  半分散 P2P ベースの DRM では，あるユーザにメタ情報や ID のカプセル化の許可を与えるのは同じだが，こちらでは正規ユーザの管理のみ，DRM 管理サーバで行う．この手法の利点として，ユーザの管理を管理サーバで行うため，利用状況の調査や金銭的な管理は行い易いという点がある．欠点としては，アカウントが膨大になりすぎた場合，管理が難しくなるため，前者と比較して拡張性に限界があるという点がある．現実世界において，著者らはこちらの方がより適していると主張している．

1.4 提案方式について

本論文では，P2P をベースとした DRM システムの考案を行う．この実現において，ユーザ間通信のみでセキュリティを保つ Bitcoin に注目し，同様のシステムを取り入れることで管理サーバの負担を軽減することを目的とする．

1.5 貢献

本論文では，P2P 通信による新たな DRM の方式を提案する．この手法では，電子現金の一種である Bitcoin に注目し，ここで用いられているプロトコルを DRM に利用することで，十分な安全性と分散性，拡張性が得られる．実際に，コンテンツ購入者による売却や善意の二次配布者に対する利得付けが実現できる．

1.6 先行研究との比較

ここでは，先行研究である P2P ベースの手法と比較を行う．先にあげた岩田らの手法では，利用したユーザの ID を収集し，この ID をもとに認証を行う [2]．誰がどう配布したかに関わらず，コンテンツを利用したユーザの利用のみ可能な手法である．よってシンプルかつ最低限であり，それ以上の拡張性はないものとなっている．本提案手法では，利用券をコインとして受け渡す．このため，コンテンツの購入者によるコンテンツの売却が可能である他，どういった経路でコンテンツが受け渡されたのかのデータの収集も可能である．P2P 通信において，ユーザがコンテンツを配布する上で，利点となることは基本的には存在しない．そのため，アップロードを嫌うユーザが多い現状となってしまっている．よって，コンテンツ配布の経路が明らかであれば，コンテンツをより多く配布したユーザに利点をつけることも可能となり，より実用性が高まると考えられる．
提案方式と比較したものを表 1 に表す．

	サーバ・クライアント型	P2P 型分散	P2P 型半分散	提案手法
拡張性	低い	高い	高い	高い
サーバに対する負荷	大きい	小さい	小さい	小さい
課金の容易さ	容易	困難	容易	負担有り
サーバの処理の速さ	遅い	速い	速い	速い
アカウント管理	容易	困難	容易	容易
クライアントの処理の負担	再生時	配布時	配布時	配布時
配布の追跡性	サーバが行う	なし	なし	あり
中古売買の可否	不可	可能	可能	可能

表 1: 既存手法との比較

2 電子現金システムについて

現金の代わりに，インターネット上で用いることのできるデータをお金として使うシステムのことである．銀行等が金銭と同等の価値があるとしたデータを利用者に売り，インターネット上で簡単に売買が可能になるものが一般的である．この場合，データと現実の貨幣の価値は常に等価であり，銀行がその価値を保証する．しかし，電子現金の中には，Bitcoin のようにコイン自体に価値があるものが存在する．

2.1 Bitcoin について

Bitcoin は電子現金の一種であり，以下の特徴を持つ．

- 中央集権的なサーバを持たない
  BitcoinはP2P通信で行われる．これはサーバ・クライアント型のような主従関係が存在せず，コンピュータ同士が互いに同じ立場から通信を行うシステムである．
- コインの受け渡しは、署名により行う
  送りたい相手の財布（公開鍵）と自身の持つコインに自身の秘密鍵で署名することで，コインの受け渡しが行われる．Bitcoin システムにおいて，コインは電子署名の連鎖によって表されている．その中の前の所有者の署名がそのコインの正当性を保証し，コインに書かれている自身の公開鍵がコインの所有者を保証する．このため，コインはコイン所有者がそれぞれ持っているのではなく，全ネットワーク上で公開することができ，その正当性も参加者全員が検証可能となっている．

従来の電子現金とは異なり，Bitcoin におけるコインは現実の貨幣と同等に扱われる．

2.2 Bitcoin のプロトコル

- 利用者は自分の ID から公開鍵を作成する．この公開鍵は匿名のものであり，いくつでも作成することができる．
- Bitcoin において，コインはネットワーク上で公開されており，誰もがコインがどの公開鍵に紐付けられているか確認することができる．
- コインを渡す場合，送りたい相手の公開鍵で自身の持つコインを暗号化し，得たものに対して自身の秘密鍵で署名を行う．
- コインの所有者の正しさ確認は，コインの前所有者の署名を検証することにより行う．
- 2 重使用を防ぐため，タイムスタンプサーバを用いて取引は全て記録される．
- 最初のコインの所有者は自動生成されたものとし，コインを発見した人が持つ．

3 提案方式

ここからは，上記の Bitcoin のプロトコルを利用した DRM システムの作成について考える．

DRM には用いられる状況により多くのシステムがあり，構成法も多岐にわたっている．

今回はそれらのうち特に用いられている二種について Bitcoin システムでの実現法を考察する．どちらの手法でも，コインをコンテンツ利用券とみなし，すべての利用者はコインを持つ利用者を正規な利用者として検証することができるとする．また，今回はオンライン上で使われるコンテンツのみを対象とする．

3.1 提案方式 1

第一の例として，コンテンツを購入したユーザが自身の持つコンテンツを別のユーザに送った場合、使用不可となる DRM について考える．これは，コンテンツを買った利用者が第三者に売ることができることを意味する．この場合，コンテンツを売った利用者は以後使うことはできなくなる．またこの際全てのトランザクションを全員がチェックできるため，売買の度にコンテンツホルダーへ一定額支払うということも可能といえる．この方式の実現のためには，Bitcoin システムと同じように利用者はお金とコインの取引を行う．タイムスタンプサーバも導入を行い，一度手放したコインに関しては手放した記録が残るようにする．コインを持っている間のみコンテンツが利用可能とし，コインを売ってしまうとその時点からコンテンツの利用はできなくなる．

3.1.1 プロトコル

- コンテンツプロバイダーは売りたい商品の数だけコインを作成する．商品を売る際にコインを作成してもよい．
- コンテンツは最新のコインを利用することにより利用可能とする．そのため，コンテンツは
- 一次購入者はコンテンツプロバイダーと取引を行う．現金を渡し，コンテンツとコインを受け取る．小売が買う場合は多くの代金を払い，複数のコインを受け取る．
- 一次購入者が第三者にコンテンツを売却する場合，自身の持つコインを取引相手のコインに変換する．コンテンツ自体はそのまま渡す．
- コンテンツを購入した二次購入者は代金を払い，コンテンツとコインを受け取る．
- コインはネット上で公開されているため，最新のコインの所有者を検証することで誰もが正規利用者の検証が可能である．

3.2 提案方式 2

次に，中古システムを考えない場合の DRM について考える．こちらは，正規に得たコインをコピーして配布することができるとする．ただし，コインは現金と交換するものとし，得た現金はコンテンツホルダーに送ることとする．これらの条件が満たされているかは任意のユーザから容易に検証できる．これにより，電子透かしに似た機能をもたせる．こちらはその性質上，タイムスタンプサーバでの監視を行う必要がないといえる．

3.2.1 プロトコル

- コンテンツプロバイダーは売りたい商品の数だけコインを作成する．商品を売る際にコインを作成してもよい．
- コンテンツは，一度でもコインを受け取っていれば利用可能とする．
- 一次購入者はコンテンツプロバイダーと取引を行う．現金を渡し，コンテンツとコインを受け取る．
- 一次購入者以外の利用者がコンテンツを購入する場合，既にコンテンツを持っている利用者が自身の持つコインから取引相手のコインを作成し，取引を行う．
- 取引において交換された代金は，コインを配布した利用者によってコンテンツプロバイダーに届けられる．

- コインはネットワーク上で公開されているため，コインを持つ全ての利用者を検証することで正規利用者の検証が可能である．

4　結論

DRM において，電子現金のシステムを利用した手法の提案を行った．この手法では

- 中央サーバに負担をかけず，DRM をもたせた状態で第三者にコンテンツ配布が可能
- bitcoin のプロトコルをそのまま不正検知に利用することができる

という特徴がある．

参考文献

[1] Nakamoto Satoshi, “Bitcoin: A peer-to-peer electrooni c cash system.” *In http://bitcoin.org/bitcoin.pdf, (unpublished)*. 2008

[2] Iwata, Tetsuya and Abe, Takehito and Ueda, Kiyoshi and Sunaga, Hiroshi, “A DRM system suitable for P2P content delivery and the study on its implementation.”*In Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on.* vol.2, p.p.806-811. IEEE, 2003