

利用権の固定先に着目した不正利用防止方式の提案

3X-6

庵 祥子

三宅延久

NTT情報流通プラットフォーム研究所

1. はじめに

インターネットが急速に普及したことに伴い、デジタルコンテンツがさまざまな分野で利用されるようになった。近年ではデジタルコンテンツをあらかじめ暗号化して配送し、そのコンテンツの利用権である復号鍵を決済とともに安全確実に配送する技術[1]が確立されたことによってさらにその需要が伸びている。その反面でデジタルコンテンツにはコピーが非常に容易であるという特徴があるため不正利用が後をたたない。そこでこのような不正利用を防止する仕組みを確立することが重要な課題となっている。

本提案では上記のような形態で配送されるデジタルコンテンツの利用権（復号鍵）を、目的に応じて購入者や機器の固有情報で暗号化することにより固定し、他者や他機器で利用不可能にすることにより様々な利用形態に対応可能な不正利用防止方式を提案する。さらに本方式を利用して、実在する要求に合致する不正利用防止の実現例について報告する。

2. 利用権の固定先に関する検討と実現

利用権の固定先は以下の3つの条件を備える必要がある。

- ・他者による書き換えが不可能な情報を保持
- ・コンテンツ購入時に情報の入手が可能
- ・固定した利用権の保存が可能

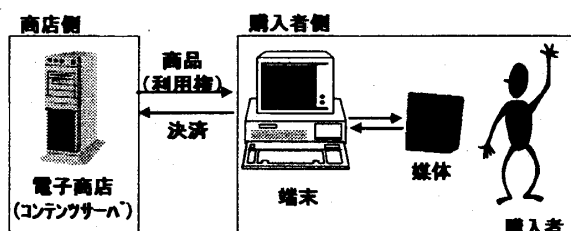


図1：購入フロー

図1より購入フローに際に関わるのは「購入者」「端末」「記憶媒体(購入したコンテンツを保存するメモリを指す。以下媒体と略す)」であるため、これらについて利用権の固定先としての検討を行う。

購入者の場合、購入者固有の情報は購入時に入力させることにより取得可能である。購入者固有情報で暗号化して固定した利用権の保存は端末や媒体を利用する場合に限り可能である。従って購入者への利用権の固定は、端末や媒体の補助がある限り条件を満たす。

端末の場合、端末固有の情報は購入時に自動的に取得が可能であり、かつ端末固有情報で暗号化して固定した利用権の保存も可能である。よって端末は利用権の固定先としての条件を満たす。

コンテンツの利用に媒体が介在し、かつ媒体に書き換え不能な固有情報が存在する場合、媒体への固定も考えられる。この場合媒体固有の情報は購入時に端末により取得可能にしなければならない。媒体固有情報で暗号化し固定した利用権の保存は、媒体あるいは端末を利用することにより可能である。よって端末の補助が可能であれば媒体を利用権の固定先とすることが可能である。

いずれの固定先の場合においても、利用権を固定先の固有情報を使って暗号化もしくは保存することにより異なる固有情報を持つ環境では利用できなくすることが可能である。これにより利用権を固定することができる。

3. 利用権の固定先による特徴

次に、利用権を「購入者」「端末」「媒体」の各々に固定するデジタルコンテンツの特徴について表1にまとめる。

	コンテンツ保護	利用者の使い勝手	ポータビリティ	他人への譲渡	オープン性
購入者固定	○	×	○	×	○
端末固定	○	○	×	×	○
媒体固定	○	○	○	○	△

表 1: 固定先別特徴比較表

購入者に利用権を固定する方式では、コンテンツ利用時に購入者情報を入力させる必要があり、購入者の使い勝手が悪い。また購入者であればどの端末でも利用することができるが、購入したコンテンツを他人に譲渡できないという問題がある。

これに対し端末に利用権を固定する方式では端末側で認証を行うので購入者が情報を入力する必要がない。しかしながら正規の購入者であっても購入した端末以外ではそのコンテンツを利用できないという問題が発生し（例えば会社の端末で買ったコンテンツを家の端末では使えない等）、デジタルコンテンツの特徴の一つでもあるポータビリティが損なわれる。また他人への譲渡も不可能であることが問題である。

媒体固有の情報で利用権を固定する方式では常に購入者情報を入力する必要がない。また媒体を移動することによりコンテンツも移動可能なためポータビリティもよく他人への譲渡も可能である。しかしながらこの方式では媒体を利用するシステムであり、かつ媒体が固有情報を持っていないかならなという制限があるためオープン性が低い。

4. 利用権を固定した不正利用防止実現例

これらの特徴を実際のサービスの要求と合わせて不正利用防止方式を実現した例について以下に報告する。

4.1 音楽コンテンツ販売[2]

音楽コンテンツは不正利用防止が唱えられているが、現存するCDやMDと同等のポータビリティを備えた不正利用防止を行わなければならない。利用権を媒体に固定する方式では、媒体があれば誰でもどの再生端末でも再生可能であり、かつ利用権が媒体に固定されているため他の媒体にコピーしても再生が不可能であるためこの要求を満た

すことが可能である。そこで我々は利用権を媒体に固定し、購入後のコンテンツを専用再生端末で再生する方式(InfoBind)で実現した。

具体的には、媒体にはID付スマートメディアを、再生端末としてはSolidAudioを採用している。購入時に購入端末を通して媒体固有情報の授受を行い、媒体固有情報で暗号化することによって固定した利用権を取得し、この利用権と暗号化コンテンツをスマートメディアに保存して再生時にはリアルタイムで復号するというものである。

4.2 PDF販売[3]

PDFファイルは基本的にパソコン上で閲覧されることが多く、購入者が複数の端末にて購入したコンテンツを閲覧する可能性が高い。このようなコンテンツの場合、複数端末での購入者の使い勝手を考慮しなければならない。この要求を満たすために我々はコンテンツの利用権を購入者と端末の双方に固定して不正利用を防止することによってを実現した。

具体的には情報流通プラットフォームであるInfoketの拡張としてAcrobatReaderのPlug-inで実装した。利用権は購入者と端末のそれぞれの固有情報で暗号化することによって固定し、購入端末利用時は端末情報を利用して、他へ購入者が移動して使用する場合には購入者情報を利用して利用権を復号し、コンテンツの利用を可能にしている。またAcrobatReaderのPlug-in機能を利用して画面上でのカット&ペーストの禁止や、ポストスクリプトファイルへの保存の禁止などを実現している。

5. おわりに

本提案で、利用権の固定先として購入者、端末、媒体が有効であることがわかった。今後は本方式に基づいて、さまざまな要求に応じた不正利用防止を実現する予定である。

[参考文献]

- [1]インターネットを用いた情報流通プラットフォーム, 明石修, 森保健治, NTT R&D Vol.46
- [2] <http://www.solidaudio.jp.net/>
- [3]不正コピー防止を考慮した情報販売方式, 庵祥子, 玉井誠, 三宅延久, 情報処理学会 99-DPS-91