3M－09　デジタルコンテンツの階層的な情報利用制御方法

庵　祥子　　三宅　延久　　桑名　栄二
ＮＴＴ情報流通プラットフォーム研究所

1. はじめに

近年、MP３コンテンツの普及を背景として、不正コピーされた音楽コンテンツがネットワーク上で爆発的な広がるなど、デジタルコンテンツの不正利用が問題となっている。この問題を回避するために、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手法([1], 図 1)を用いてコンテンツを配送し、利用権の行使環境を制御するという不正利用防止策が現在一般的に行われている[2]。

本発表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）を組織や集団で共有可能な形でバインドすることにより、会社、学校、家庭等での集団による利用に対応可能な情報利用制御方式を提案する。さらに本方式を利用して、情報利用制御の実現例を提案する。

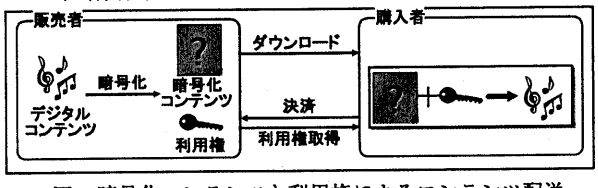

図 1:暗号化コンテンツと利用権によるコンテンツ配送

2.コンテンツの利用制御方法の現状

コンテンツの不正利用を防止する仕組みとして、利用者には書き換え不可能であり、かつ利用者／端末／媒体等（以下、行使環境とする）の識別子情報（以下 ID とする）を利用して暗号化するなどの手法によって利用権をバインドする方法が一般的に用いられている。この方法にはこれらの ID を利用できる行使環境でのみ利用権の行使を可能にするという特徴がある。

例えば、媒体 ID を利用してコンテンツの利用権を暗号化し、この媒体 ID を持った媒体上でのみ利用権の復号を可能する InfoBind 方式[3]が挙げられる(図 2)。この方式では媒体 ID を用いることにより、コンテンツを他媒体にコピーした場合に媒体 ID が不一致になることを利用して不正利用を防止している。このように行使環境の ID で利用権をバインドし、利用できる行使環境を制御する方式は実サービスに広く利用されている[4]。

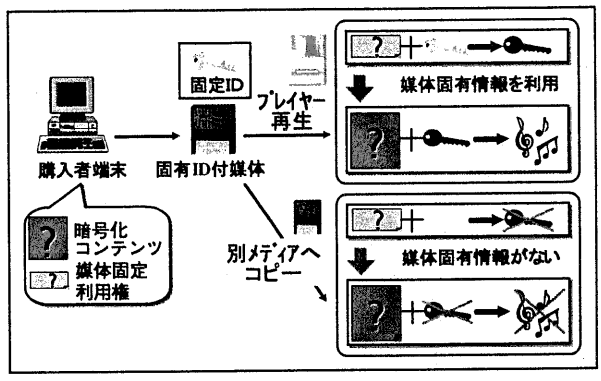

図 2 ：ID バインドの利用例

しかしながら、この方式は実用化に耐えうる不正利用防止策である反面、利便性において問題点が浮上している。それはこの方式では利用権の行使環境個々の ID を基にして制御しているため、制御単位が一人あるいは一台等になってしまい、企業や学校等でのコンテンツの集団利用に適していないというものである。

3. 階層的な情報利用制御方法の提案

そこで本発表では利用権の行使環境の ID を階層化可能にすることにより、コンテンツの階層的な情報利用制御方法を提案し、利用権の行使環境による利用制御が集団利用に適していないという問題点を解決する。

The hierarchal usage control method for digital contents
Shoko Ihori,　Nobuhisa Miyake,　Eiji Kuwana
NTT Information Sharing Platform Laboratories

問題点の解決策として、利用権の行使環境の制御に利用されている行使環境 ID を個々で捕らえるのではなく、それぞれ複数の集まりとして捕らえ、階層化することを提案する。そして ID の階層構造を行使環境の集団（企業であるならば、部・課・個人所有物等）に割り当てる。そして利用権制御には「行使環境 ID」と行使環境 ID のどの階層を利用するかを定める「利用階層情報」を用い、コンテンツごとに対象とする階層を可変にしてコンテンツの利用権の行使環境を自由に変化することを可能にする。

これにより利用権の行使環境 ID でコンテンツをバインドするという従来の手法を踏襲しつつ、コンテンツの利用権を集団に割り当てて集団で利用可能なコンテンツを提供することが可能になる。

4.階層的な利用制御方法の実現例

3 章で提案したコンテンツの階層的な利用制御方法を用いた実現例を社内コンテンツ共有システムを例に説明する。本実装例では階層的な ID としてＩＰアドレスを利用する。なぜならネットワークを用いたコンテンツの共有を行う場合、各端末にはＩＰアドレスが階層的に付与されていることが多いため利用権の行使環境の ID として利用しやすいためである。またＩＰアドレスを行使環境 ID にした場合、特別な情報のやり取りを行わなくてもコンテンツのやり取りを行う機器が容易に行使環境 ID を取得できるという利点もある。

社内コンテンツ共有システムにおける利用制御とは、社内に蓄積するコンテンツに対する閲覧許可を部や課内全員、あるいは個人のみに与えるなどの利用制御を行うことである。利用制御の階層としては、社内・部課・個人を想定し、それぞれ社内コード、部課コード、個人コードを利用するものとし、これらをＩＰアドレスに割り当てるものとする。

例えば、ＩＰアドレスを 8bit 単位で扱い、X氏の所属する部課の部課コードを 100、X氏の個人コードを 101 にした場合、X氏が利用する端末のＩＰアドレスは 10.100.101.XXX になる。X氏は、自分の所属する部課内のみにコンテンツの利用を許可する場合には利用階層情報を上位 16bit として利用権を暗号化する。この場合同じ部課に属するＹ氏はコンテンツを利用できるが、部課の異なるＺ氏は利用権が復号できないため利用不可能である（図 3）。同様に個人利用コンテンツを生成する場合は利用階層情報を上位 24bit とする。この場合は同じ部課に属していても氏名コードの異なるＹ氏にもコンテンツの利用が不可能になる。

これによりコンテンツを社内の共有ディスクサーバ等に保存する際にコンテンツの利用制御さえ行えば、許可している部課あるいは個人に割り当てられた IP アドレスを利用している機器以外にコンテンツの利用を不可能にすることができる。

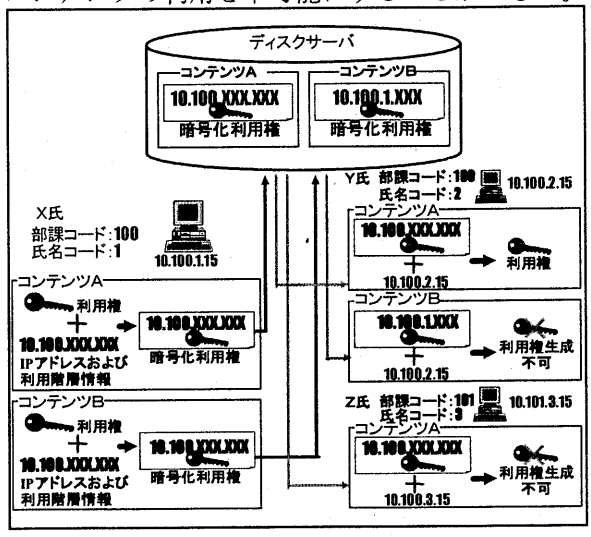

図 3 ：階層的な利用制御方法の実現

5. おわりに

本提案により、利用権の行使環境を制御する手法でもコンテンツの利用権を集団に割り当てることが可能であることがわかった。今後の課題としては、本提案を実装および検証が挙げられる。

[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] 利用権の固定先に着目した不正利用防止方式の提案,庵祥子,三宅延久,情報処理学会第 59 回全国大会

[3] 不正コピー防止を考慮したコンテンツ販売システム,上野正巳,庵祥子他, 情報メディア 36-3 電子化知的財産・社会基盤 7-3

[4]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