

コンテンツ埋込み権利情報を参照・管理可能な端末ソフトウェア

内田 典佳, 小林 直樹, 関谷 博 (NTT 東日本研究開発センター),
一玖 秀一 (NTT 東日本法人営業本部),
松村 季樹 (NTT サイバーソリューション研究所)

コンテンツ ID フォーラム(cIDf)では, デジタルコンテンツの流通促進を目的に各コンテンツにユニークな共通識別子を付与する cIDf 仕様を制定している. この cIDf 仕様のなかには, Distributed Content Descriptor (DCD) という, デジタルコンテンツに付随して流通する流通コンテンツ記述子が規定されている. 本稿では DCD を実現するコンテンツ埋込み権利情報を参照・管理可能な端末ソフトウェアの実装について報告する.

The terminal software refer to and manege rights ownership attributes
embedding in the package.

Noriyoshi Uchida, Naoki Kobayashi, Hiroshi Sekiya (NTT EAST Research and Development center),
Shuichi Ichiku (NTT EAST Business Communication Headquarters),
Sueki Matsumura (NTT Cyber Solutions Laboratories)

The Content ID Forum defined specification cIDF which was a common identifier embedded in each digital content for the purpose of promoting digital content commerce. In this specification, The Distributed Content Descriptor (DCD) was intended to be distributed with the package of digital content itself. In order to realization DCD, we develop the terminal software which can refer to and manage rights ownership attributes embedding in package and report its implementation.

1. はじめに

コンテンツ ID フォーラム(cIDf)では, デジタルコンテンツの著作権を保護しつつ, その健全な流通を実現するためには, まずコンテンツ ID を付与をすることが必須だと考え, コンテンツ ID の枠組みを規定した cIDf 仕様を制定している [1]. この cIDf 仕様のなかには, Distributed Content Descriptor (DCD) という, デジタルコンテンツに付随して流通する流通コンテンツ記述子が規定されている. DCD はコンテンツ ID のうち, ユニークコードと属性情報の一部を XML で表現したものである. 実際にコンテンツに DCD を付随して流通させるための DCD の付与形態は, 挿入形式 (コンテンツヘッダに挿入する形態) と分離形式 (DCD をコンテンツと別形式で保持する形態) が規定されている. 以下では MPEG, JPEG コンテンツを対象とした挿入形式の

DCD を実現する「コンテンツ埋込み権利情報を参照・管理可能な端末ソフトウェア」の実装について述べる.

2. ソフトウェアの仕様の検討

現実に利用可能な状態で DCD を実現するためには, cIDf 仕様に詳細がない部分や明確にされていない部分をあらかじめ確定する必要がある.

(a) 属性情報の明確化

DCD は必須項目であるユニークコードと属性情報のサブセットを XML で表現したものである. 属性情報に具体的にどの項目を採用するかは, 実装に任されており, 具体的な項目は決定する必要がある. また記述方式も具体的なタグ名などは決まっていないので, DCD の生成・参照・変更が容易に出来るような記述形式を

規格化する。

(b) ソフトウェアの構成

DCD は、実際の利用方法としてネットワークのない環境下で、コンテンツと付随する DCD のみからによって、DCD に埋め込まれたユニークコードと属性情報をローカルに参照することが想定されている。DCD のコンテンツへの付与形態は、挿入形式（コンテンツヘッダに挿入する形態）と分離形式（DCD をコンテンツと別形式で保持する形態）が規定されている。本稿では挿入形式のみを実現することとし、DCD をコンテンツに挿入形式で埋め込みの処理をする“DCD 埋め込みツール”と、ネットワークのない環境下で挿入形式の DCD が埋め込まれたコンテンツから、ユニークコードと属性情報を表示可能な“DCD ビューア”を実装する。

(c) 対象とするフォーマット

対応するコンテンツは、動画フォーマットとして MPEG1・MPEG2-PS・ASF、静止画フォーマットとして JPEG をサポートする。

(d) コンテンツ真正性検証技術

DCD ビューアの機能として、ハッシュとデジタル署名技術を組み合わせて、コンテンツ本体の改ざん及び、DCD の改ざん検出機能の両方を実装する。署名手順として、現在、W3C で規格化が進められている”XML Signature”を採用する。

(e) ソフトウェアの動作環境

ソフトウェア動作環境を以下に示す。

項目	必須環境
OS	日本語版 Microsoft Windows 2000 Professional (SP2 以上) および Windows NT 4.0 Workstation (SP6 以上)
CPU	Intel PentiumIII 500MHz 以上 およびそれに準ずる互換 CPU
メモリ	128MByte 以上
インストール容量	50MByte 以上の空き容量

推奨環境を下記に示す。

項目	推奨環境
OS	日本語版 Microsoft Windows 2000

	Professional (SP2 以上) および Windows NT 4.0 Workstation (SP6 以上)
CPU	Intel PentiumIII 1GHz 以上 およびそれに準ずる互換 CPU
メモリ	512MByte 以上 + 仮想メモリ 512MByte 以上 (最大埋め込みコンテンツと同容量のメモリ)
HDD	UltraATA66 (66MB/sec) もしくは Ultra2-SCSI (80MB/sec) 以上
インストール容量	50MByte 以上の空き容量

3. ソフトウェアの具体的な仕様

(a) 属性情報

DCD の具体的な属性項目は、コンテンツおよび DCD の改竄検出を検証することを目的に、以下のようこの項目を選択した（ユニーク ID、コンテンツ属性、権利属性、セキュリティ）。

同時にコンテンツ流通時に、DCD に自由に書き込み（メモ、コンテンツ閲覧利便性情報など）の出来る自由領域（改ざん検出領域の範囲外）を設定した。

(b) DCD 埋め込み・読み込み処理

MPEG1, MPEG2-PS の場合は、システム層先頭パック内の先頭 PES パケットに対してプライベート 2 パケットとして格納し、DCD Embedding Format (以下、DCD-EF) 読み込み時に、先頭 PES パケット中に DCD-EF が格納されているかどうかをチェックすることにより埋め込み済みかを判定する。

ASF の場合は、cIDf-DCD をキーとした属性情報としてヘッダーオブジェクト内に格納し、DCD-EF 読み込み時には、そのキーを元に読み込み処理を行う。

JPEG の場合は、ファイル末尾にコメントデータとして DCD-EF を格納し、読み込み時にその領域に格納されているかどうかをチェックすることにより埋め込み済みかを判定する。

(c) MPEG1, MPEG2-PS 埋め込み・読み込み

システム層先頭パック内先頭 PES パケットにプライベート 2 パケットとして格納する。MPEG システムの性格上、0x000001 および 0xFF を使用することができないため、DCD (XML 文書) のエンコード方式として S-JIS

(Shift-JIS) を用いて埋め込むこととする。

読み込みの際は、先頭 PES パケットのみチェックし、DCD-EF が格納されていない場合は未検出とする。これは、他のパケットに妥当な DCD-EF が格納されていた場合であっても、検出されないことを意味する。

図2に PES パケットとして DCD-EF を埋め込んだ際の例を示す。

(d) ASF 埋め込み・読み込み

ヘッダーオブジェクトの属性情報である Extend Content Description Object として埋め込まれる。読み込みの際は、識別子「cIdf-DCD」にて属性情報が設定されているかをチェックし、該当データが存在しない場合を未検出とする。図3にヘッダーオブジェクト属性情報として DCD-EF を埋め込んだ際の例を示す

(e) JPEG 埋め込み・読み込み

ファイル末尾にコメントデータとして DCD-EF を埋め込む。フォーマットの統一を図るため、MPEG と同様に DCD (XML 文書) のエンコード方式として S-JIS を用いて埋め込む。

読み込みの際は、最終コメントデータのみチェックし、DCD-EF が格納されていない場合は未検出とする。これは、他のコメントデータに妥当な DCD-EF が格納されていた場合であっても、検出されないことを意味する。

図4にコメントデータとしてを埋め込んだ際の例を示す。

(f) コンテンツハッシュ処理

コンテンツ改竄を検出するため、SHA1 を用いたコンテンツハッシュ値を計算する。

埋め込みアプリにてコンテンツハッシュ値を計算し、その値を DCD の要素として DCD 内に保存し、DCD ビューアではその値とコンテンツハッシュ値が合致するかで改竄判定を行う。

既に DCD が埋め込まれたコンテンツに対する処理においては、埋め込み済み DCD 領域を除外した領域からコンテンツハッシュ値を計算することにより、埋め込み前のコンテンツと同一のハッシュ値を取得する。また、ハッシュ計算処理部分はアセンブラで実装されたモジュールを用いることで処理の高速化を図る。

(g) デジタル署名

DCD 自体の改竄を検出するため、RSA+SHA1 を用いたデジタル署名処理を行う。

署名処理を行うにあたり、処理モジュールとしてボルチモア社製 KeyTools Pro および KeyTools XML を使

用する。

署名対象領域は、DCD 自由領域およびデジタル署名領域以外のコンテンツを対象とする。

4. まとめ

DCD を実現する「コンテンツ埋込み権利情報を参照・管理可能な端末ソフトウェア」の実装を行い、以下のような結果を得た。

(a) DCD をコンテンツに挿入形式で埋め込みの処理をする“DCD 埋め込みツール”と、“DCD ビューア”を実現した。実際に“DCD 埋め込みツール”によってコンテンツに埋め込まれた DCD が、DCD ビューア埋め込みコードと属性情報を表示可能なことを確認した。

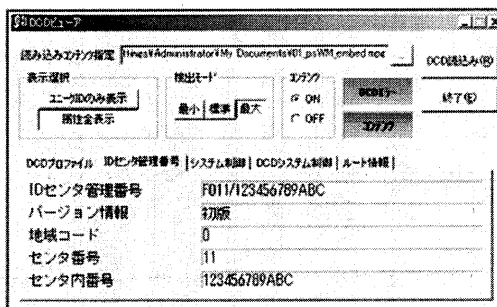


図1: DCD ビューア表示画面イメージ

(b) DCD の具体的な属性項目 (ユニーク ID, コンテンツ属性, 権利属性, セキュリティ) を選定し、さらにその記述形式 (XML 記述, タグ名) を明確化した。特に、コンテンツ本体及び DCD の改ざん検出 (ハッシュ・デジタル署名技術を用いた XML の機能を実現しセキュリティ強化を図った。

コンテンツ流通時に、DCD に自由に書き込み (メモ, コンテンツ閲覧利便性情報など) の出来る自由領域 (改ざん検出領域の範囲外) を設定した。

今後は実装した各プログラムの評価や改良について検討をしていきたい。

参考文献

- [1] コンテンツ ID フォーラム
<http://www.cidf.org/>
- [2] 通信・放送機構 研究発表会予稿集 2002.5

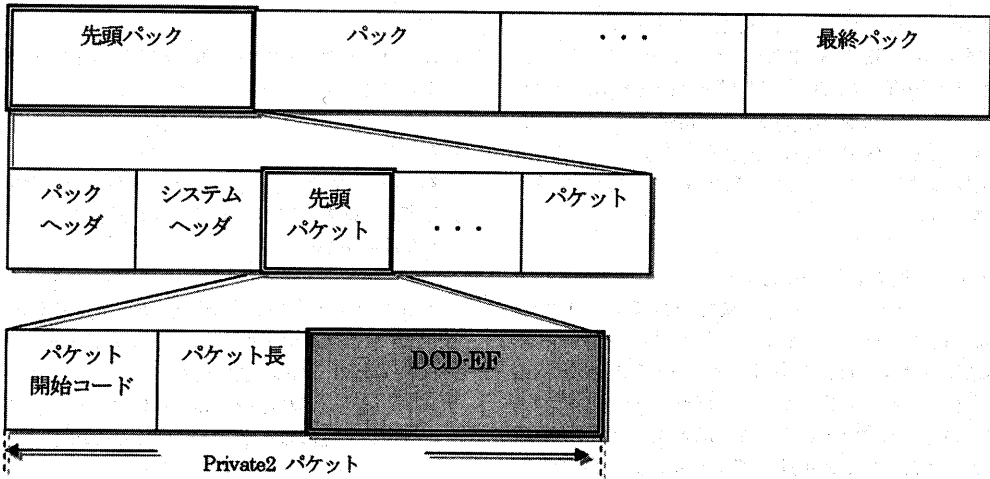


図2 MPEG1, MPEG2-PS ファイルの DCD-EF 埋め込みフォーマット

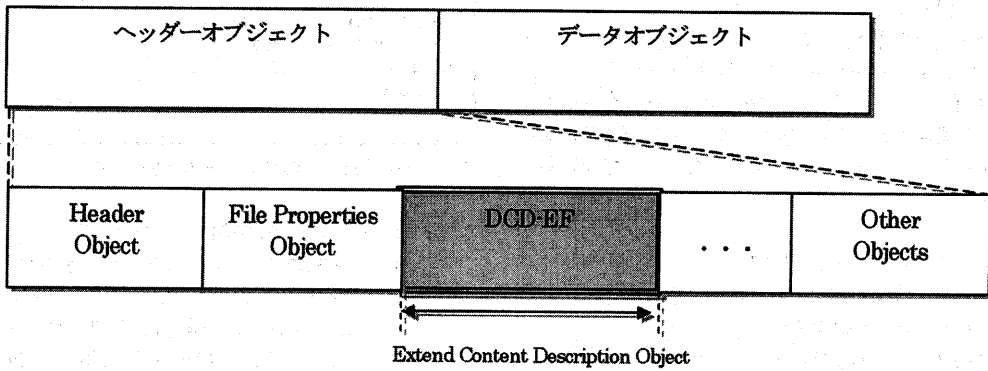


図3 ASF の DCD-EF 埋め込みフォーマット

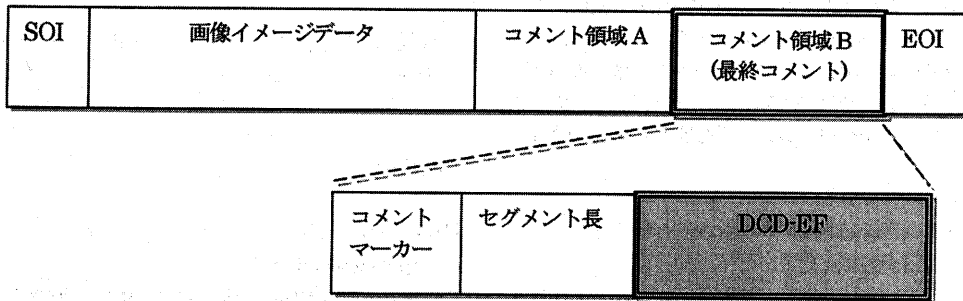


図4 JPEG の DCD-EF 埋め込みフォーマット