SD カードのコンテンツ保護

Content Protection for SD Memory Card

上林　達　　下田　乾二　　坂本　広幸
■ KAMBAYASHI Toru　■ SHIMODA Kenji　■ SAKAMOTO Hiroyuki

現在広く普及しているSDカードは，よく検討されたコンテンツ保護メカニズムを備えるメモリメディアである。SDカードにおけるコンテンツ保護メカニズムは，メディアバインド，リボケーション及びムーブで実現されている。これらは，SDカードにおいて初めて統合的に導入され，新しい世代のメディアにおけるコンテンツ保護メカニズムの基本概念となっている。高度なコンテンツ保護メカニズムを備えたSDカードは，使いやすい形状とサイズ，高速なデータ転送機能とあいまって，アプリケーションの多様な展開に対応可能である。SDカードは今後も，メモリメディア市場の拡大をリードし続ける。

The secure digital (SD) memory card, which has already become one of the most popular media, has a considered and well-defined mechanism for content protection. The most important concepts of the content protection mechanism are (1) binding of content to the medium, (2) revocation, and (3) moving of content. These three concepts, which were realized in integrated form for the first time in the SD memory card, have become fundamental concepts of content protection for a new generation of media. The SD memory card is very useful for a wide range of applications because of its advanced mechanism for content protection, its dimensions that make it easy to use, and its wide bandwidth for data transfer. The SD memory card will continue to be a leading medium in the expanding market for memory media.

1 まえがき

SDカードはメモリメディアの一つとして，既に，その地位を確立している。コンパクトで使いやすい外形とサイズ，高速なデータ転送など，メモリメディアとしての成功の要因はいくつか考えられる。SDカードの優位性を支える種々の特長の中で，コンテンツ保護メカニズムは重要な特長の一つであるとともに，SDカード開発の原点でもある。ここでは，コンテンツ保護メカニズムの一つの典型となっている，SDカードのコンテンツ保護メカニズムについて，その基礎概念と背景について述べる。

2 SDカードのコンテンツ保護

2.1 SDMI及び4C Entity

SDカードの開発当時，各国の音楽レーベルや家電メーカー，IT（情報技術）メーカーなどが設立主体となって，SDMI（Secure Digital Music Initiative）という団体が発足した。SDMI設立の主たる目的は，デジタル オーディオ コンテンツの利用，特にインターネット ダウンロード利用に関する，著作権保護の要求仕様を策定することにあった。SDMI準拠[(1)]のオーディオコンテンツ格納メディアとして，コンテンツ保護メカニズムは不可欠の要素であった。SDカードは第一義的には，SDMI準拠のメモリメディアとしてスタートした。

SDMIの要求仕様の中で特筆すべき点の一つは，コンテンツの“ムーブ（移動）”の概念であった。例えば，（個数限定の）1世代デジタルコピーでは，コピー先のコンテンツは，消去を例外として，コピー先メディア／デバイスに固定されなければならない。デジタル オーディオ コンテンツに対して許容される操作の一つとしてムーブを導入することにより，コンテンツの所在に関する自由度が増大し，ユーザーの利便性は大きく向上する。ただし，SDMIにおけるムーブは，“チェックイン／アウト”と呼ばれる特別な形に原則として限定されていた。チェック イン／アウトにおいては，コンテンツがメディア間やデバイス間を直接移動することは禁止されている。許容される操作は，LCM（Licensed Compliant Module）と呼ばれる一種の録音装置から，メディアやデバイスに，コンテンツをムーブすること（書出し）と，逆に，当該メディアやデバイスから，元のLCMに，コンテンツをムーブすること（読戻し）のみである。コンテンツの“移動”という概念の導入に先べんをつけたことは，SDMIの成果の一つであろう。技術的観点からも，チェックイン／アウトは制限付きムーブである。ムーブの技術的課題は，移動元コンテンツの消去を確実に行うことである。

SDMIがデジタルオーディオ格納メディアに関する要求仕様を定義する一方で，SDカードのコンテンツ保護の具体的な仕様とコンプライアンス ルールは，CPRM（Content Protection for Recordable Media）[(2)]というフレームワークの中で定義されている。CPRMは4Cが定めた一連のコンテンツ保護規格の総称であり，文字どおり，記録メディアにおけるコンテンツ保護に関する。4C Entity社はIBM社，Intel社，松下電器産業（株）及び東芝が，主としてメディアのコンテンツ保護規格をライセンスする目的で作った会社である。また，4C規格には，CPPM（Copy Protection for Prerecorded Media）と呼ばれる読み出し専用メディアに関するコンテンツ保護規格もあり，CPRMと主要な要素技術を共有している。CPPMはCPRMと同時期に検討が開始され，基本的な概念を共有しているからである。

コンテンツ保護仕様を除くSDカードの仕様はSDA（SD-card Association）が策定したが，コンテンツ保護仕様は4Cが策定した。SDカードのコンテンツ保護メカニズムについては，SDMIの動向を考慮しつつ，当社と松下電器産業（株）が共同で①メディアバインド，②リボケーション及び③ムーブの実現，の三つの基礎概念に基づくコンテンツ保護メカニズムを提案した。これらの概念については次節以降で説明を行い，ここではそれぞれの概念を実現するための技術手段について述べる。SDカードは，これらの概念の導入が検討された最初のCPRMメディアであり，そのコンテンツ保護メカニズムはCPRMのひな形となった。

2.2　メディアバインド

メディアバインドとは一般に，メディアID（IDentification）（個々のメディアに一意的に振られたID）と暗号技術とを用いてコンテンツをメディアに縛りつけることであり，暗号化されたコンテンツやコンテンツ復号鍵を，別のメディアにコピーすることが可能であるとする。コンテンツがメディアバインドされていれば，コピー先のコンテンツは再生不可能である。メディアバインドは，SDMIのPM（Portable Media）に対する要求仕様にも含まれている。メディアバインドを実現する技術手段にはいくつかのバリエーションがあり，その一例を**図1**に示す。

図1において，K_tはコンテンツ暗号化鍵である。ここでは対称暗号を想定しているので，K_tはコンテンツ復号鍵でもある。ID_{media}はメディアIDを表す。K_Mはレコーダとプレーヤとが共有する秘密の暗号鍵である。GはK_MとメディアIDの値を用いて計算される適当な関数を表す。レコーダはGの出力を用いてコンテンツ鍵を暗号化し，K_{te}としてメディアに記録する。再生時，プレーヤはメディアからメディアIDを読み取り，K_Mと合わせてGの値を計算する。プレーヤは，メディアからK_{te}を読み取り，Gの値を鍵として，K_{te}を復号する。レコーダが録音時に用いたメディアIDと，プレーヤがメディアから読み込んだメディアIDが一致していれば，K_{te}の復号結果として，正しいコンテンツ鍵を得る。

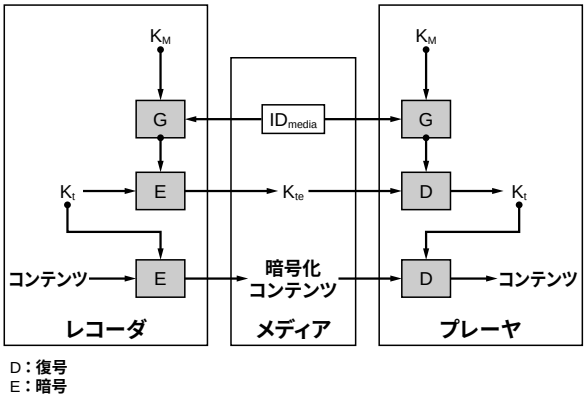

図1．メディアバインドの一例 ― メディアバインドを実現する一手法を示す。
Method of binding content to medium

これにより次のことが成立する。暗号化されたコンテンツ鍵K_{te}が，メディアIDの異なるメディアにコピーされたとしても，プレーヤはコンテンツ鍵を正しく復号することができない。もちろん，メディア上のメディアIDを書き換えたり，プレーヤに対してメディアIDを偽ったりすることはないという前提である。

2.3　リボケーション

SDカード上には，製造時にMKB（Media Key Block）というデータが記録される。このデータは，ホストデバイス（レコーダとプレーヤ）のリボケーションに用いられる。すなわち，ホストデバイスにおけるコンテンツの利用は，MKBによって制御される。個々のホストデバイスはデバイスキーという一組のデータによって区別される。例えば，あるホストデバイスの秘密が暴かれ，コンテンツが不正利用される状態になったとする。リボケーション機能を備えたシステムにおいては，他のホストデバイスにほとんど影響を及ぼすことなく，当該ホストデバイスによるコンテンツ利用を禁止すること（リボケーション）が可能である。SDカードは，MKBによるリボケーションをサポートした最初のメディアであった。リボケーションは現在，コンテンツ保護における重要な概念の一つになっている。

次に，MKBの原理を説明する。デバイスキー行列とは，暗号鍵を要素とする行列である。簡単のために3行4列のデバイスキー行列を考える。

$$(k_{ij})_{1<=i<=3,\ 1<=j<=4}$$

ここで，K_mをメディアキーとする。これは，MKB処理の結果として，すべてのデバイスが共有する秘密の情報である。(k_{ij})に対して，次の行列を考えることができる。

$$(k_{ij}\ [K_m])_{1<=i<=3,\ 1<=j<=4}$$

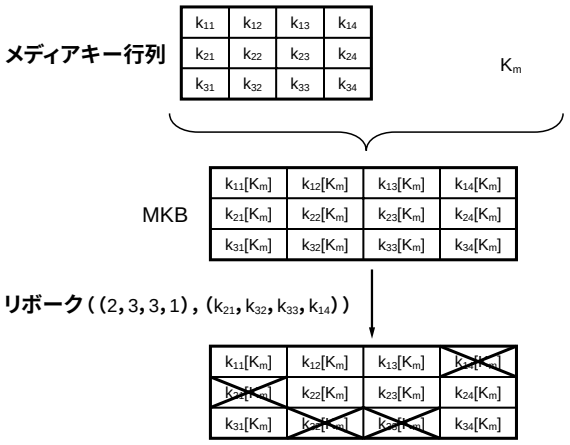

図2. MKB ― デバイスキー行列とメディアキーK_mから，MKBが構成される。特定のデバイスキーをリボークするには，各列の対応する行を無効なデータでつぶす。

Media key block (MKB)

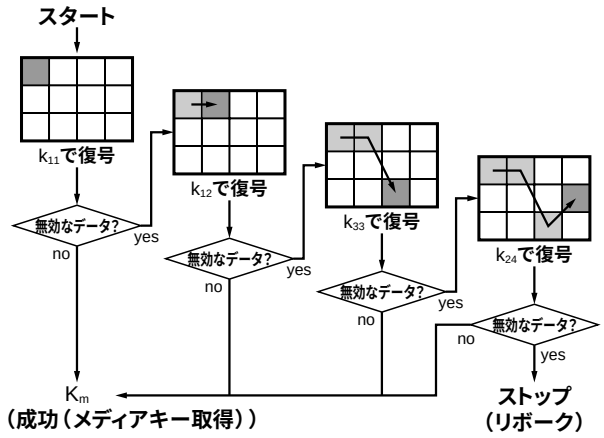

図3. MKB処理 ― ホストデバイスは，デバイスキーを用いて，順にMKBの対応する行を復号していく。ホストデバイスがリボークされているときは，フローの最後まで無効データしか得られない。

MKB process

この行列がMKBと呼ばれるものである。ここに，k_{ij}［K_m］は，暗号鍵k_{ij}によってK_mを暗号化したものである(**図2**)。

デバイスキー行列の各列から一つの行を選ぶ選び方を指定するベクトルと，当該ベクトルに従って選ばれたデバイスキー行列の要素が作るベクトルとの組をデバイスキーと呼ぶ。例えば，((1, 1, 3, 2), (k_{11}, k_{12}, k_{33}, k_{24}))はデバイスキーの一つである。各ホストデバイスはデバイスキーの一つを割り当てられており，それを保持しているものとする。リボケーションの観点からは，ホストデバイスは割り当てられたデバイスキーによって識別される。3行4列のデバイスキー行列を用いて割当て可能であるデバイスキーの数は$3^4 = 81$である。サイズの大きなMKBを用いることにより，膨大な数のデバイスキーを割り当てることが可能である。

MKBはメディア上に記録される。各ホストデバイスはメディアからMKBを読み取り，デバイスキーを用いてMKB処理を行う。上記のデバイスキーを持つホストデバイスによるMKB処理の概略を**図3**に示す。デバイスキー((1, 1, 3, 2), (k_{11}, k_{12}, k_{33}, k_{24}))を持つホストデバイスは，第1列の指定行(第1行)を鍵k_{11}で復号する。復号結果があらかじめ定められた“無効データ”に一致しない場合，その値をメディアキーK_mとみなして，次の処理に進む。もし，そうでなければ，2列目以降の指定行を順次与えられた鍵で復号していく。第4列で無効なデータを得た場合，ホストデバイスはK_mを取得することができず，以後の処理に進むことができない。すなわち，当該ホストデバイスはリボークされる。MKBによって，例えば((2, 3, 3, 1), (k_{21}, k_{32}, k_{33}, k_{14}))のホストデバイスをリボークするには，各列の対応する行を，無効データ(正確には，無効データを対応する鍵で暗号化したもの)でつぶせばよい(図2)。

2.4 ムーブの実現

図1において，ホストデバイスが共有する秘密情報であるK_Mを，MKBによって供給することにすると，**図4**に示すようなキーマネジメントが得られる。これは，先述のコピープロテクションにおける基本概念のうち，最初の二つを満足するものになっている。すなわち，メディアバインドとリボケーションという二つの重要なコンテンツ保護機能を実現する。ムーブ機能をサポートしない場合，これだけで十分なコンテンツ保護機能を実現することが可能である。しかし，ムーブの実現には，ホストデバイスによる暗号化コンテンツ鍵K_{te}の消去を担保する必要がある。暗号化コンテンツ鍵を含むメディア内部の状態をバックアップ保存し，コンテンツ鍵の消去後に復元・再利用することは容易である。

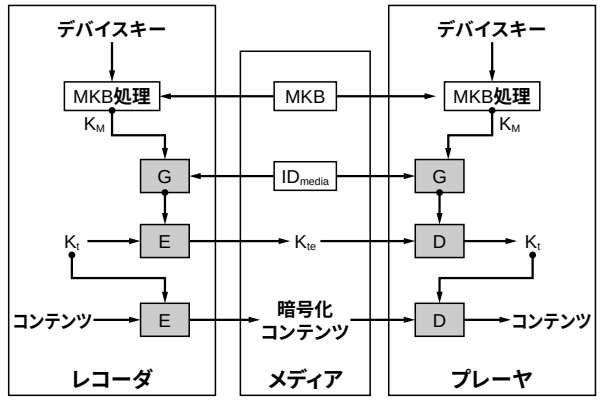

図4. キーマネジメントの例(1) ― メディアバインドとリボケーションとをサポートするキーマネジメントの一例である。

Example of key management for media-binding and revocation support

SDカードは，ムーブ機能実現のために“秘匿領域”を持っている。当該秘匿領域には，CPRM規格に準拠したホストデバイスのみがアクセス可能である。暗号化されたコンテンツ鍵を，この秘匿領域に記録することにより，上記の鍵のバックアップが防止される。SDカードの秘匿領域は，ホストデバイスとSDカードとの間のAKE（Authentication and Key Exchange）によって実現されている。AKEとは，秘密情報を共有する機器が，当該秘密情報を持つ機器だけに可能な仕方でデータを交換することによって，相手を認証する手続きである。SDカードにおいてこの手続きは，MKB処理の結果として得られるメディアキーに依存するチャレンジ アンドレスポンス プロトコルである。この手続きの結果として，ホストデバイスとSDカードとは一時的な暗号鍵を共有する。しかも，ホストデバイスとSDカードとの通信を中間で傍受する第三者（man in the middle）は，この共有鍵を知ることはできない。

図4にAKEをかぶせると，**図5**のようなキーマネジメントが得られる。これでSDカードのキーマネジメントの骨格が得られる。AKEの元になる共有秘密情報としては，メディアキーでメディアIDを暗号化したもの（メディアユニーク鍵K_{mu}）を用いる。SDカードは計算の便宜上，K_{mu}を内部に保持している。コンテンツ鍵は転送時に二重に暗号化される。AKEが既にメディアIDで個別化されているので，メディアバインドの目的にはコンテンツ鍵自体の暗号化は，実は冗長である。しかし，開発当時4Cでは，図4のような，ムーブ機能をサポートしないメモリメディアの標準化も検討されていた。4Cにおける検討の結果，キーマネジメントの共通性を意識して，SDカードではあえて二重の暗号化を行うこととした。

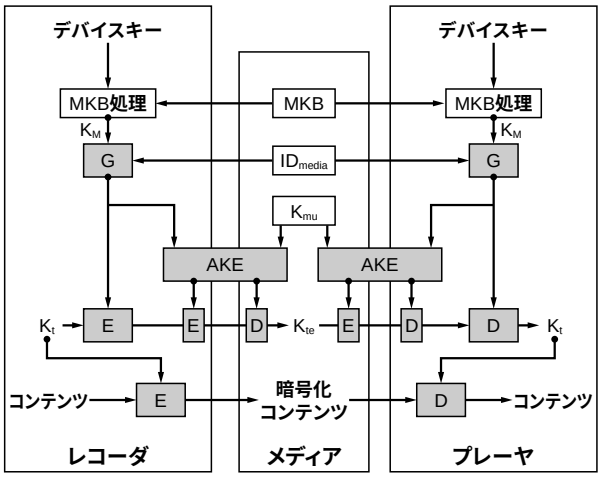

図5．キーマネジメントの例（2） ― 図4に加え，ムーブをサポート可能なキーマネジメントの一例で，SDカードのキーマネジメントのスケルトンを示す。

Example of key management for media-binding, revocation, and move support

ホストデバイスとSDカードとのAKEによって，ホストデバイスとSDカードとのデータの転送が，一時鍵による暗号化を用いて保護される。更に，転送データの保護だけなく，コマンド引数の改ざんなどの攻撃を防ぐ必要があり，コマンド引数の改ざん防止のためにユニークな方法が考案された。カードの秘匿領域に対する読込み／書出しコマンドに先立って，AKEが行われるので，このAKEのchallengeにコマンド引数を絡めて，カードに引き渡すという方法である。

秘匿領域のデータを消去する手続きについても，工夫が行われている。ホストデバイスは，カードからデータ消去の確認を取る必要がある。したがって，消去は単一の動作ではなく，セキュアな書込みと読出しからなる一連の動作から構成される。データの消去には，まず乱数を発生し，当該乱数によって消去すべきデータを上書きする。次いで，上書きされたデータの読出しを行い，書き込んだ乱数との一致を検証する。

3 あとがき

新しい概念に基づくセキュア ストレージとして，SDカードには，開発当初から様々なアイデアが盛り込まれた。SDカードのコンテンツ保護には，4C各社の英知と努力が傾注されている。SDカードは現在も，性能面のみならず形状面でも進化の途上にある。それはコンテンツ保護機能についても同様である。関係各社のたゆみない努力により，今後もSDカードは市場をリードしつつ，進化を続けるであろう。

文　献

(1) SDMI. SDMI Portable Device Specification Part I Version 1.0, July, 1999.
(2) 4C Entity, LLC. Content Protection for Recordable Media Specification SD Memory Card Book. Rev 0.95, April, 2001.

上林　達　KAMBAYASHI Toru

研究開発センター コンピュータ・ネットワーク研究所主務。著作権保護システムの開発に従事。情報処理学会，日本応用数理学会会員。

Computer Network Lab.

下田　乾二　SHIMODA Kenji

自動車システム事業統括部 自動車システム技術開発センターグループ長。メディアカード事業部在籍時にSDカードの規格化，技術，商品化全般，及びSD応用商品推進業務に従事。

Automotive Systems Development Center

坂本　広幸　SAKAMOTO Hiroyuki

セミコンダクター社 メモリ事業部 ファイルメモリ・マーケティング部グループ長。SDカードの開発，マーケティング，規格化に従事。

Memory Div.