SDメモリカードを利用したデジタル著作権保護技術 SDconnect™

SDconnect Digital Rights Management System Technology Using SD Memory Card

中野　一典　■ NAKANO Kazunori
松川　伸一　■ MATSUKAWA Shinichi
笠原　章裕　■ KASAHARA Akihiro

音楽や映像，地図，書籍などのデジタルコンテンツを不正コピーから守るために，記録された媒体以外へコンテンツを勝手に複製することを防止する技術が利用されてきた。この技術では，コンテンツの自由な流通や個人利用に制限を加えてしまうという課題があった。東芝は，この課題を解決するためにSDメモリカード（以下，SDカードと呼ぶ。）を活用したデジタル著作権保護技術 SDconnect™を開発した。この技術では“コンテンツ鍵”だけを特定のSDカードで利用するようにし，コンテンツの記録媒体を制限しないようにした。これによりコンテンツのバックアップや移動が著作権を保護した形で自由に行えるようになった。また，コンテンツはインターネットで入手し，コンテンツ鍵は携帯電話で入手するような仕組みを構築できるようになった。この結果，コンテンツを購入するユーザーとコンテンツの配信事業者の双方にとって利便性が向上した。

To prevent illegal copying of digital contents such as music, videos, maps, and books, content protection technologies to bind content to a specific medium have been used. In such systems, however, content distribution or handling of content in a personal environment has been restricted.

Toshiba has developed SDconnect, a technology that utilizes SD Memory Cards. It enables contents to be stored in any medium, with only the content keys being stored in a specific medium. This accommodates flexibility of content backup and move functions, and allows separate distribution of contents and content keys, improving convenience for both content distributors and users.

1　まえがき

SDconnect™とは，東芝が提唱する“SDカードをコンテンツ鍵の記録メディアとして用いて，サーバから機器へ配信されたコンテンツの管理利用はもとより，機器間でのコンテンツ利用連携をスムーズに実現するデジタル著作権管理の新しい仕組み”を構築するための技術である。この技術は，SD Card Associationが定めるアプリケーション規格SD-SD（SD-Separate Delivery）とその規格に適用された4C Entity，LLC(注1)が定めるコンテンツ保護規格CPRM（Content Protection for Recordable Media）for SD-SD[1]で構成される。

当社は，主導してこれらの規格化を推進するとともに，ネットワーク サービスモデルのシステム構築，及びこのモデルを実現する機器に搭載するハードウェアとソフトウェアの開発も同時に行い，市場開拓を行っている。

ここでは，SDconnect™の概要と活用方法について述べる。

2　SDconnect™の概要

SDカード内の物理的構造とCPRM処理について概要を述べる。

（注1）　デジタルコンテンツの著作権保護技術をライセンスする目的で構成された，四つの企業（IBM Corporation，Intel Corporation，松下電器産業（株），（株）東芝）から成る組織体。

SDカード内の記録領域は，それぞれユーザー領域，保護領域，秘匿領域，及びシステム領域の四つの領域に分かれている。ユーザー領域へのアクセスは制限がなく，通常のカードの利用ではこの領域が用いられる。しかし，CPRMを利用する際にはほかの記録領域も用いられる。

従来のCPRMとCPRM for SD-SD の違いを**図1**に示す。従来のCPRMでは，暗号化されたコンテンツはユーザー領域に書かれ，そのSDカードのメディア固有鍵をベースに復号する必要があった。したがって，コンテンツをほかの媒体へコピーした場合には復号ができなくなる特徴を持っていた。一方CPRM for SD-SDでは，暗号化された“コンテンツ鍵”がユーザー領域に書かれる。このコンテンツ鍵は，そのSDカードのメディア固有鍵をベースに暗号化され，不正な複製を防止している。暗号化コンテンツはどの媒体に記録されていてもよく，そのSDカードとの組合せで利用が可能になる。

2.1　従来のCPRMの仕組み

従来のCPRMでは，暗号化コンテンツを復号するために次のような処理を行う。ホスト機器（以下，ホストと略記）は，所有するデバイス鍵と，SDカードのシステム領域に記録されたMKB（Media Key Block）及びメディアID（Identification）から，所定の手続きを経てメディア固有鍵を計算する。ホストとそのSDカードの双方が同じメディア固有鍵を所有することを確認する認証処理を行い，認証に成功するとアクセス可能な保護領域から暗号化タイトル鍵を読み出し，メディア固有鍵で

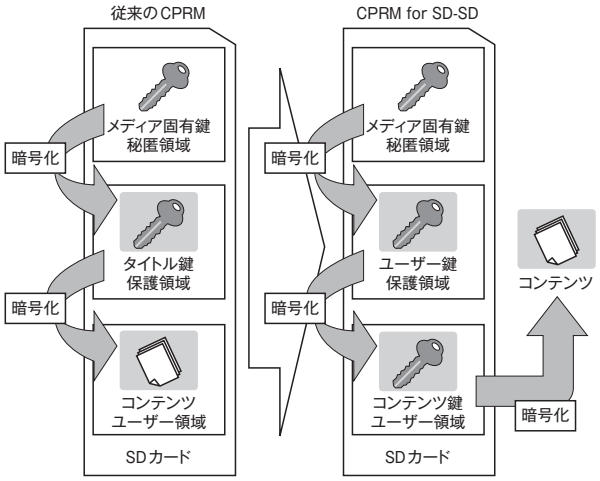


図1. 従来のCPRMとCPRM for SD-SDの違い — 従来のCPRMでは，暗号化されたコンテンツはユーザー領域に書かれるため，ほかの媒体にコピーした場合に復号できなくなる特徴があった。CPRM for SD-SDでは，暗号化されたコンテンツ鍵だけがユーザー領域に書かれ，不正な複製を防止できる。

Difference between conventional content protection for recordable media (CPRM) and CPRM for SD-separate delivery (SD-SD)

復号しタイトル鍵を取り出す。このタイトル鍵を使って暗号化コンテンツを復号する。

CPRMのライセンスを受けた機器にはデバイス鍵を他人へ漏えいしないような実装が義務付けられており，万が一漏えいなどによりあるデバイス鍵が不正に利用されていることが判明した場合，そのデバイス鍵ではメディア固有鍵が計算できないような新しいMKBを発行できる。新しいMKBが記録されたカードに対しては，不正に利用されているデバイス鍵ではメディア固有鍵が計算できないため，そのカードに保護記録されたコンテンツの復号ができなくなる。

2.2 CPRM for SD-SDの仕組み

CPRM for SD-SDでは，従来のCPRMの仕組みを拡張してユーザー鍵，コンテンツ鍵と呼ばれる二つの鍵（二重鍵）を用意し，それぞれユーザー鍵を保護領域に，コンテンツ鍵をユーザー領域に記録する。コンテンツは，暗号化された状態でSDカード内部あるいは外部に記録される。それぞれのデータは正規のCPRMのライセンスを受けた機器だけがアクセスできるように，コンテンツはコンテンツ鍵で，コンテンツ鍵はユーザー鍵で，ユーザー鍵はSDカード固有のメディア固有鍵で暗号化されて格納される。また，コンテンツ鍵には鍵以外にも再生回数や再生可能時刻などのUsage Ruleと呼ばれる利用規定情報も付加されており，改変や改ざんなどへの対策が施される。ここでは，コンテンツ鍵はUsage Ruleも含まれたものとして呼ぶことにする。

この仕組みにより，暗号化コンテンツと鍵とを分離して扱うことが可能となる。従来の記録媒体でのコンテンツ保護の仕組みでは，暗号化コンテンツを記録媒体に縛り付ける形で記録されていたが，SD-SDではコンテンツ鍵だけがカードに記録され，暗号化コンテンツの記録場所や複製などの取扱いには制限が設けられていない。そのため，常にカード内にコンテンツを記録しておく必要はない。あらかじめ暗号化コンテンツがネットワークなどを介して複製されていれば，CPRMのライセンスを受けた機器にカードを挿入することで再生することができる仕組みを構築できる。

2.3 SDconnect$_{TM}$の利点

カードに常にコンテンツを記録する場合に比べて，いくつかの利点が挙げられる。まず，カード容量はコンテンツ鍵が入るサイズであればよい。暗号化コンテンツの転送速度は，SDカードの物理インタフェースに依存しないため，例えばデータは家庭内インターネットなどの転送速度の速い通信を利用して機器間で共有するなど，環境に合わせて最適な組合せを取ることができる。

また，複製や移動という概念はコンテンツ鍵に適用される。コンテンツの複製あるいは移動とは，それを再生するためのコンテンツ鍵を複製することあるいは移動することと同義として考えることができ，コンテンツそのものは格納先を自由に選択することが可能になる。

3 SDconnect$_{TM}$の活用方法と利用モデル

鍵とコンテンツを分離して扱うため，SDカードをコンテンツ鍵記録メディアとして利用する，というのが基本的な考え方になる。SDconnect$_{TM}$利用の概要を**図2**に示す。暗号化コンテンツと鍵が別々に配信され，暗号化コンテンツは機器間で共有され，鍵が記録されたカードをそれらの機器に挿してコンテンツの再生などを行う。

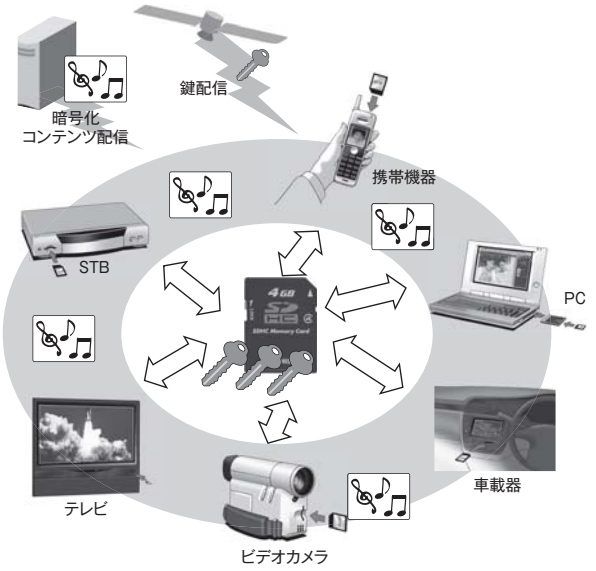
コンテンツそのものの容量は，音楽圧縮データ1曲当たり数Mバイトから高品質動画や高解像度地図データで数十Gバイトなど様々である。SDconnect$_{TM}$では，コンテンツの記録媒体や伝送路に関しては制約がないため，その時点での最新記録媒体，伝送，及び通信技術を活用することが可能である。

具体的な利用シーンについて，車載機器や民生機器などでのコンテンツデータの私的利用継承モデルと，ネットワーク配信技術及び利用モデルの二つの事例を以下に述べる。

3.1 車載機器や民生機器などでのコンテンツデータの私的利用継承モデル

従来，カーナビゲーションシステムなどに搭載されたハードディスク装置（HDD）へ私的複製された音楽コンテンツは移動できないようにされていた。

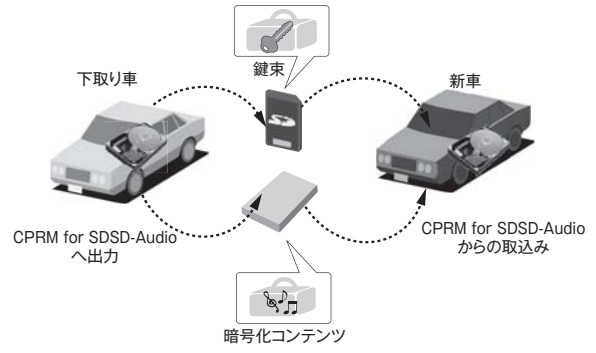
ここではSDconnect$_{TM}$を利用することにより，コンテンツ移動を実現する方法について述べる。**図3**は，その概要を示したものである。ここでは車の買い替えを想定しており，古い車で



STB：Set Top Box
PC　：パソコン

図2．SDconnect$_{TM}$利用の概要 ― 様々なネットワーク経由で暗号化コンテンツを入手し，再生のためのコンテンツ鍵はネットワークや携帯電話などを経由してSDカードに格納する。コンテンツと鍵を，SDカードを利用して機器間で移動することも実現できる。

Overview of SDconnect



SDSD-Audio：CPRM for SD-SD規格のアプリケーションフォーマット

図3．車載機器を例としたコンテンツデータの継承モデル ― 車載リッピング音楽コンテンツ継承モデルの例である。新車購入時に，下取り車に蓄積したCDリッピングコンテンツを合法的に新車に移動する。コンテンツ鍵と暗号化コンテンツをSDカードに一度格納した後に，新車にそのSDカード内データを格納しなおす。暗号化コンテンツは，USB（Universal Serial Bus）デバイスなど，ほかの媒体で移動することが可能である。

Example of usage model of moving contents for automotive audiovisual system

蓄積したり私的複製した音楽コンテンツをほかの車へ移動させる場合，私的複製と認められる範囲で許可する技術が必要となる。特に，私的複製の範囲に入らない場合の移動は問題がある。SDconnect$_{TM}$では，コンテンツを利用するためのコンテンツ鍵の可搬型媒体としてSDカードを活用する。暗号化コンテンツは，少量の場合はカードに鍵といっしょに記録し持ち運ぶか，若しくは可搬型HDDなどを利用して，古い車からほかの車へコピーする。この作業は一般のユーザーでも可能であり，SDカードとほかの記録媒体を組み合わせたSDconnect$_{TM}$の特徴を生かした利用形態である。

3.2　ネットワーク配信技術及び利用モデル

音楽データのネットワーク配信市場にはApple社のiTunesなど様々なサービスが存在する。また動画データのネットワーク配信市場も立ち上がりつつある。ここでは，SDconnect$_{TM}$によるネットワーク配信の実現について述べる。その概要を**図4**に示す。

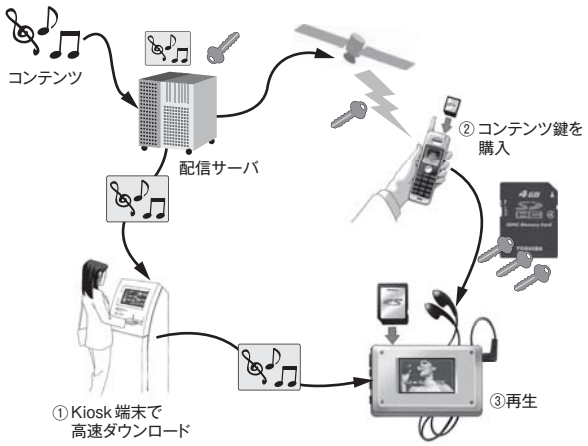


図4．ネットワーク配信技術及び利用モデル ― ネットワークによるコンテンツ及び鍵の配信と利用モデルの例である。映像などの大容量コンテンツはKiosk端末でモバイル機器へ高速ダウンロード格納し，再生のためのコンテンツ鍵は携帯電話経由で購入し，SDカードへ格納する。そのSDカードをモバイル機器へ挿入して再生する。新たなビジネスモデルが実現できる。

Usage model of network distribution based on SDconnect devices

ユーザーはこのサービスの利用にあたり，あらかじめユーザー鍵が記録されたSDカードを所有している。コンテンツはKiosk端末(注2)やインターネット，DVDなどの物理媒体を通じて利用者の手元に配信される。実際のダウンロードサービスでは，ダウンロードに時間が掛かり過ぎることが懸念されるが，Kiosk端末で高速ダウンロードをサポートする機器へ転送する方式も採用可能である。

入手したコンテンツは暗号化されており，そのままでは再生することはできない。利用者は，このデータの中から再生したいものを選択する。端末は，選択されたコンテンツに対応するコンテンツ鍵をサーバに要求する。このとき，端末はあらかじめ用意したユーザー鍵に与えられたユーザー鍵IDもいっしょに送る。なお，このユーザー鍵IDは秘密にする必要はない。サーバは要求を受けて，ユーザー鍵IDに対応するユーザー鍵で暗号化したコンテンツ鍵を端末へ配信する。ここで端末は，

（注2）　街頭や店舗内に設置される情報端末機器で，コンビニエンスストアでのチケット販促，銀行でのATM（現金自動預払機），及び図書館での蔵書検索などに利用される。

サーバからコンテンツ鍵を受け取る通信を行い，SDカードに記録する。コンテンツと比較して小さなデータのため，携帯電話などでの受信や記録でも利用者はストレスを感じることなく行うことができる。

最後に，コンテンツ鍵が記録されたSDカードを暗号化コンテンツが記録された端末に挿入することで，その端末での再生を行うことができる。

実際にサービスを行ううえで障害となる，ダウンロードに要する時間やコンテンツの可搬性といった問題に対して，SDconnect$_{TM}$では，コンテンツにアクセスするための鍵情報だけを記録したSDカードとほかの機器との組合せを可能にすることで解決している。

ここでは配信コンテンツを動画としているが，CPRMが対象としている商用コンテンツである音楽や電子文書などの著作物も同様に扱うことができる。

また機器間の連携例として，Bluetooth^{TM}(注3)通信などを鍵伝送に併用することも可能である。SDカードは携帯電話のような小型機器の場合，通常，機器に挿入したまま取り出さずに使用することが多い。SDカードを抜き差しする手間は，ワイヤレス通信により解消できる。

4　あとがき

SDconnect$_{TM}$では，携帯電話，パソコン（PC）やデジタルカメラなどの民生機器分野で普及が著しいSDカードを利用し，コンテンツ保護の標準規格“CPRM”を活用しながら，二重鍵生成ソフトウェア，コンテンツ配信サーバ，鍵配信サーバ，及び端末など，当社独自の製品やモジュール群によってシステムが実現される。

SDconnect$_{TM}$普及のため，製品やモジュール群の設計開発，市場への展開，及びパートナー戦略が不可欠となる。当社は，SDconnect$_{TM}$対応機器の普及を実現するためのSDカードホストコントローラ及び，それを取り扱うドライバソフトウェアなどのコンポーネントを開発中である（**図5**）。

（注3）　Bluetoothは，Bluetooth SIG，Inc.が所有する登録商標であり，東芝は，許可を受けて使用。

図5．SDconnect半導体部品とシステム構成 — SDconnect$_{TM}$に対応したSDカードとSDカードホストコントローラ，ホストコントローラドライバ（FW）で構成される。このホストコントローラとドライバによりSDカードに向けた二重鍵の生成と管理が可能である。

Components and system configuration of SDconnect

更にPC環境においては，SDconnect$_{TM}$対応アプリケーションに必要なSDK（Software Development Kit）の開発に着手している。また鍵配信サーバは，配信サービスシステム構築とともに提供することが可能である。

文　献

（1）　4C Entity, LLC. "Publications and Current Versions". 4C Entity Home page. ＜http://www.4centity.com/docs/versions.html＞,（参照2008-03-10）.

中野　一典　NAKANO Kazunori
セミコンダクター社 技術企画部 システム技術企画担当参事。
セキュリティシステムの商品企画・開発に従事。
Technology Planning Div.

松川　伸一　MATSUKAWA Shinichi
東芝ソリューション（株）IT技術研究所 研究開発部。
著作権保護技術規格の策定及び要素技術の開発に従事。
Toshiba Solutions Corp.

笠原　章裕　KASAHARA Akihiro
研究開発センター 事業開発室技監。
Business Development Office