

# ASSDカードおよびOMA-SRMの規格化

ASSD Card Standardization and OMA-SRM Standardization

中垣 浩文  
Hiroyumi Nakagaki

櫻井 博  
Hiroshi Sakurai

小来田 重一  
Shigekazu Kogita

上村 知範  
Tomonori Uemura

宗 広和  
Hirokazu So

## 要 旨

ネットワークで配信されるAVコンテンツなどを、SDメモリーカードに格納して利用する場合、従来であれば、コンテンツ配信時に用いられるDRM (Digital Rights Management: コンテンツ保護・管理の仕組み) から、SDメモリーカードの著作権保護方式であるCPRM (Content Protection for Recordable Media) へのエクスポートという手法が用いられてきた。この手法では、DRMのコンテンツ利用のUsage rule (回数制御や期間制御など) をDRM規格が規定する形式のまま記録することができなかつた。Usage ruleをリムーバブルメディアにDRM規格が規定する形式で保存できれば、別の受信端末に移動してもDRMの仕組みを使って提供される各種のサービスを利用することができる。そこで、筆者らは携帯電話の配信に使われるOMA-DRM (Open Mobile Alliance-Digital Rights Management) を拡張しASSD (Advanced Security SD) カードにDRMのコンテンツと権利情報を格納する仕組みを、SDA (SD Card Association) およびOMA (Open Mobile Alliance) にて規格化した。

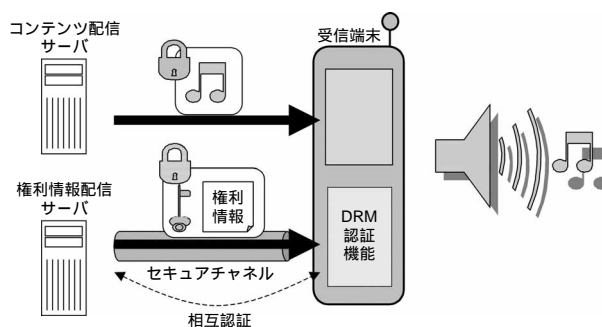
## Abstract

We have standardized the ASSD card (Advanced Security SD card) specification in the SD Association and contributed to the standardization of the DRM (Digital Rights Management) extension for Secure Removable Media in the Open Mobile Alliance. To store DRM-protected downloaded content such as music, video, and games on an SD memory card, the content was exported from DRM to CPRM (Content Protection for Recordable Media) of SD memory card. After the export, the end user could not receive desirable services which should be provided for the downloaded content under the DRM mechanism. The ASSD card can remove this defect with a new security mechanism. Downloaded content stored in an ASSD card remains protected by DRM without being exported to CPRM so that the end user can enjoy the downloaded content with various services.

## 1. はじめに

ネットワークのブロードバンド化、オンライン電子決済システムの進化により、携帯電話に音楽・動画・書籍・ゲームといったコンテンツを、ネットワークを通じて販売するサービスが普及している。こうしたサービスでは、デジタル著作権管理 (以下、DRMと記す) 技術を使ってコンテンツの視聴回数や視聴期間などの権利情報を自由に設定できるため、サービス事業者はエンドユーザーのニーズに応じた柔軟なサービスの提供が可能である。

一般的なDRMの仕組みを、第1図に示す。コンテンツは暗号化して配信され、受信端末において復号して再生される。コンテンツを復号するための鍵および権利情報も別の安全な経路 (セキュアチャネル) により受信端末に配信される。セキュアチャネルとは、コンテンツの不正利用につながる第三者による傍受・改竄 (かいざん) などを防止することが可能な経路であり、権利情報配信サーバと受信端末があらかじめ相互認証を行うことによって確立される。相互認証では、互いの信頼性を証明する情報の交換と検証を行い、処理成功後に通信データを暗復号するための鍵を共有できる。



第1図 一般的なDRMの仕組み

Fig. 1 Mechanism of general DRM

ところで、ここ数年でmicroSDカードなどのリムーバブルメディアを使える携帯電話が普及した。コンテンツと共に権利情報をリムーバブルメディアに保存することができると、携帯電話の買い替え時にリムーバブルメディアを差し替えて購入済みのコンテンツを新しい携帯電話で利用できる。また、携帯電話以外の機器でコンテンツを再生するといったことも可能となり、エンドユーザーの利便性が高まる。

リムーバブルメディアに権利情報を保存する場合、安

全に権利情報を移動させるために、携帯電話とリムーバブルメディア間の通信にもセキュアチャネルを確立する必要がある。ところが、携帯電話で利用されるDRMでは、携帯電話とリムーバブルメディア間の通信を保護する仕組みまでは規定されていなかった。そのため、携帯電話のDRMからリムーバブルメディアの著作権保護方式に変換するエクスポートという手法が用いられている。しかしながら、エクスポートには課題があった。

そこで、筆者らはOMAで標準化されている携帯電話向けのDRMを、携帯電話とSDメモリーカード間の通信にも適用するために、OMA-DRM規格とSDメモリーカード規格の拡張を行った。これらの規格に準拠するSDメモリーカードをASSDカードと呼ぶ。

まず、2章にてエクスポートにおける課題の詳細を、3章にて課題に対するアプローチを述べる。4章でASSDカードの技術を、5章でOMA-DRM拡張の技術を紹介し、6章で本技術の成果をまとめる。

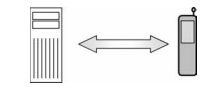
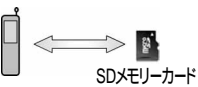
## 2. コンテンツのエクスポートにおける課題

SDメモリーカードは、コンテンツの不正利用を防ぐためのCPRMと呼ばれる著作権保護方式をサポートしており、音楽や動画などの商用コンテンツをSDメモリーカードに格納する際の違法コピー防止技術として使用されている。

CPRMとOMA-DRMとの比較を、第1表に示す。CPRMとOMA-DRMは、コンテンツ暗号方式や権利情報フォーマットなどが異なっている。そのため、OMA-DRMからCPRMへエクスポートするには、受信端末上でOMA-DRMの暗号化コンテンツを復号し、CPRMの暗号方式で再暗号

第1表 OMA-DRMとCPRMの比較

Table 1 Comparison between OMA-DRM and CPRM

|             | OMA-DRM  | CPRM   |
|-------------|--|--|
| 適用範囲        |  配信サーバ ↔ 受信端末 |  受信端末 ↔ SDメモリーカード |
| コンテンツ暗号方式   | AES暗号 (鍵長 128 bit)   | C2暗号 (鍵長 56 bit)   |
| 権利情報フォーマット  | XML形式  | 独自形式   |
| 相互認証暗号方式    | 公開鍵 (RSA暗号 鍵長1024 bit)   | 共通鍵 (C2暗号 鍵長 56 bit)   |
| 不正端末のリポーク方式 | CRL (端末1台単位)   | MKB (一定台数単位)   |

AES: Advanced Encryption Standard  
RSA: Rivest Shamir Adleman

XML: eXtended Markup Language  
MKB: Media Key Block

化を行う。コンテンツの暗号鍵は受信端末で生成される。再暗号化されたコンテンツは、SDメモリーカードのユーザー領域に格納される。また、受信端末上でOMA-DRMの権利情報は、CPRM形式に変換される。受信端末とSDメモリーカードは相互認証を行い、相互認証によってアクセス可能となるSDメモリーカードの認証領域に、フォーマット変換された権利情報とコンテンツの暗号鍵が格納される。

OMA-DRMの権利情報をCPRM形式に変換する際のルールはCMLA (Content Management License Administrator)にて規定されているが、実際の運用上は以下に示す4つの課題が予測される。

- (1) 暗号方式・鍵長・認証方式などの違いによりセキュリティ強度がOMA-DRMとCPRMで異なるため、サービス事業者が特定のコンテンツのエクスポートを許可しない場合がある。
- (2) 不正端末のリポーク (無効化すること) の管理がOMA-DRMからCPRMへ移ると、サービス事業者はOMA-DRMの仕組みを使って端末のコンテンツ不正利用を防止できなくなる。
- (3) 権利情報がOMA-DRMからCPRMへ移ると、サービス事業者はOMA-DRMの仕組みを使ってコンテンツの利用状況を管理できなくなる。たとえば、サブスクリプションサービス (定額で一定期間視聴) やメータリング (視聴情報の収集) で制限が生じる。
- (4) CPRMにエクスポートされたコンテンツと権利情報が、CPRMのコンプライアンス (遵守) ルールの範囲でさらに他のDRMにエクスポートされる可能性がある。その結果、サービス事業者が意図しないコンテンツの使用・流通が行われる恐れがある。

ユーザーにとっては、SDメモリーカードに格納することが許可されたコンテンツが十分に提供されなかったり、提供されたとしてもサービス料が高額になったり、サブスクリプションサービスが提供されないという課題がある。

こうした課題を解決するために、筆者らはSDメモリーカードにCPRM以外のDRM機能 (DRMが定める方式でコンテンツや権利情報を管理する機能) を搭載したASSDカードが必要であると考えた。

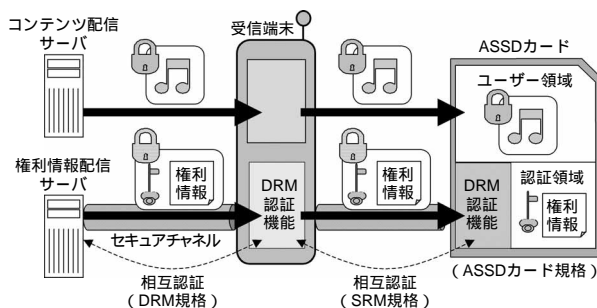
## 3. ASSDカードのDRM機能とは

ASSDカード上でDRM機能を実現するためには、DRMごとにDRM規格を拡張し、受信端末とASSDカード間の相互認証方式と通信プロトコルを規定しなければならない。ここでは、その規定をSecure Removable Media (SRM)

規格と呼ぶ。SRM拡張されたDRMの認証処理や、権利情報を格納する認証領域の管理など、ASSDカード上でDRM機能を実現する仕組みについては、今回ASSDカード規格としてSDAで策定した。

受信端末に配信されたコンテンツと権利情報を、ASSDカードのDRM機能を使って格納する方法を説明する。

ASSDカードでは、コンテンツ暗号鍵を含むDRMの権利情報を変換することなく保存できるので、受信端末上の暗号化コンテンツは復号・再暗号化することなくASSDカードのユーザー領域に格納する（第2図）。



第2図 DRM/SRM規格とASSDカード規格の関係

Fig. 2 Relation between DRM/SRM and ASSD card specification

権利情報をASSDカードに保存するために、受信端末とASSDカード間でSRM規格で定められた相互認証を行い、セキュアチャネルを確立する。この相互認証の方式には、権利情報配信サーバと受信端末間の相互認証（DRM規格で規定）と同様の方式を採用する。これにより、受信端末は配信サーバとの通信に用いる認証方式・リポーク方式を、ASSDカードとの通信にも適用できる。

セキュアチャネルでASSDカードに送られた権利情報は、ASSDカード内に設けられたDRM用の認証領域に格納する。この認証領域はDRMが定める相互認証に成功した端末だけがアクセスできる領域であり、不正な端末による権利情報の悪用を防止できる。権利情報はDRMが定めるフォーマットを変換することなく、ASSDカードに格納・保存する。

こうした仕組みをSDAにて標準化し、以下のようにエクスポートに伴う課題を解決した。

- (1) セキュリティ強度を変えることなく、ASSDカードに暗号化コンテンツと権利情報を保存する。
- (2) 受信端末とASSDカードに対するリポーク管理は、SRM拡張されたDRMの仕組みを使って行う。
- (3) サービス事業者はSRM拡張されたDRMの仕組みを使ってコンテンツの利用管理を行う。
- (4) コンテンツ流通は、SRM拡張されたDRMの範囲に

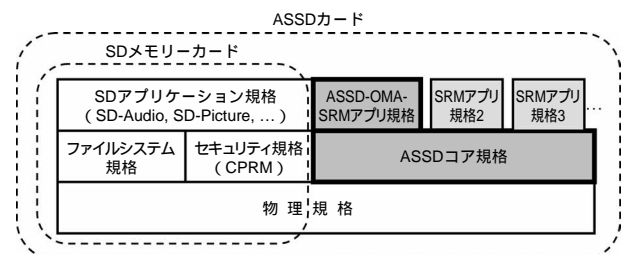
限られ、サービス事業者が意図しないコンテンツの使用・流通を防止する。

## 4. ASSDカード規格とその技術

### 4.1 規格の概要

SDメモリーカードはさまざまな機器で使用され、メモリーカードのデファクトスタンダードになっている。一方、DRM方式には携帯電話で使われているOMA-DRMをはじめとして、パソコンやテレビ向けにさまざまなDRMが存在する。仮にASSDカードが1方式のDRMのみに対応する場合、エンドユーザーはサービスごとにどのDRMが使われているかを把握し、そのDRMに対応したASSDカードを選択して使い分けなければならない。筆者らは、1枚のASSDカードで複数のDRM方式に対応できること、ならびにエンドユーザーが新たなDRM機能を必要としたときに、そのDRM機能を追加インストールできることがASSDカード規格の必須要件と考えた。そこで、ASSDカードではDRM機能をSRM Agent (SRMA) と呼ぶプログラムで実現し、SRMAをASSDカードにインストール可能とした。

ASSDカードの規格構成を、第3図に示す。SDメモリーカードの物理規格の上位階層にASSDコア規格を策定し、SRMAの実行環境や、インストール方法、実行するSRMAを選択する方法を規定している。さらに、その上位階層では各DRMに対応した規格（SRMアプリ規格）を複数定義できるようにした。その1つとして、第5章で説明するOMA-DRMの拡張規格（OMA-SRM）に対応したASSD-OMA-SRMアプリ規格を策定した。ASSD-OMA-SRMアプリ規格で定義しているのは、OMA-SRM規格で定められたメッセージをSDカードインターフェース上のコマンドで搬送する仕組みのみである。



第3図 ASSDカードの規格構成

Fig. 3 Structure of ASSD specifications

## 4.2 ASSDコア規格の機能

### 〔1〕SRMAのインストール機能

受信端末は、はじめに従来のSDモードからASSDモードへの状態遷移コマンドを発行する。状態遷移が成功するとASSDカードの機能が有効となる。受信端末は、インストールするSRMAプログラムをインストールコマンドを使ってASSDカードに転送する。ASSDカードは、不正なSRMAプログラムのインストールを阻止する機能を備えている。正当なSRMAプログラムはフラッシュメモリー上のSRMAプログラム格納領域に格納され、SRMAプログラムには後述するSRMA認証領域が同時に割り当てられる。

### 〔2〕SRMAの選択機能

ASSDカードには複数のSRMAプログラムをインストールできるので、受信端末は使用するDRMに対応したSRMAプログラムを選択するために、セレクトコマンドを発行しなければならない。このとき、ASSDカードのCPUはフラッシュメモリーから該当するSRMAプログラムをRAMにロードし、実行する。これにより、受信端末はSRMAプログラムと通信可能になる。

### 〔3〕SRMAの相互認証

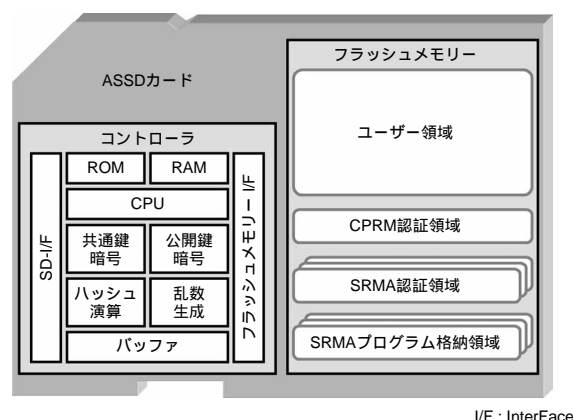
ASSDコア規格では、一般的なDRMで用いられている共通鍵暗号、公開鍵暗号、ハッシュ演算、乱数生成の機能をあらかじめ備えることが規定されている。SRMAプログラムは、これらの暗号機能を用いて受信端末との相互認証を行う。この相互認証は、使用するDRMで定められた方式に準拠する（OMA-DRMの場合は、その拡張規格であるOMA-SRM規格で規定している）。相互認証が成功すると、受信端末はSRMA認証領域へのアクセスが可能となる。

### 〔4〕権利情報の格納

受信端末は、SRMAプログラムを介して権利情報をASSDカードのSRMA認証領域へ格納できる。相互認証および権利情報を格納するためのコマンドは、各SRMA規格で規定する。

ASSDカード内のフラッシュメモリーは、従来のSDメモリーカードのユーザー領域、CPRM認証領域に加え、ASSDカード特有のSRMA認証領域、SRMAプログラム格納領域に分割される（第4図）。SRMA認証領域は、ほかのSRMAプログラムからはアクセスできないように排他的に管理される。

SDメモリーカードにこれらの仕組みを導入することにより、1枚で複数のDRM方式に対応でき、かつDRM機能の追加インストールも可能なASSDカードが実現する。



I/F : InterFace

第4図 ASSDカードのシステム構成

Fig. 4 Block diagram of ASSD card

## 5. OMA-SRMの規格化

本章ではASSDカードに適用できるDRMの一例として、OMA-DRMの拡張規格であるOMA-SRM規格について説明する。

### 5.1 OMA-SRM規格の概要

OMA-SRM規格は、OMA-DRMの権利情報をリムーバブルメディアへ安全に移動・保存するために策定した規格である。受信端末とリムーバブルメディア間の通信をリクエストとレスポンスの1対1からなるメッセージ形式で定義した。メッセージを物理的なインターフェース上で送受信するためのコマンドは、リムーバブルメディアの規格で規定される。リムーバブルメディアとしては、携帯電話のSIMカード（Subscriber Identity Module Card）やSDメモリーカードなどを想定している。

OMA-SRMでは計23種類のメッセージを規定しており、その中でも主要な機能は、以下の3つである。

受信端末とリムーバブルメディア間の相互認証

受信端末-SRM間における権利情報の移動

SRM上での権利の消費

OMA-SRM規格に準拠したリムーバブルメディアを、以降ではSRMと表現する。

### 5.2 OMA-SRMの仕組み

#### 〔1〕OMA-SRMの相互認証

受信端末とSRM間の認証方式には、OMA-DRMと同等のセキュリティ強度を保つために、配信サーバ・受信端末間と同じPKI（Public Key Infrastructure）ベースの認証方式を使う。

相互認証の前に、受信端末とSRMは相互にPKIのトラス

トアンカー（信用の起点となる認証局の識別情報）、規格のバージョン、受信端末およびSRMの識別情報などを交換する。トランスアンカーなどが適合すれば、相互認証を行う。相互認証前には、お互いのもつCRL（Certificate Revocation List）を確認し、古いICRLは更新する。相互認証において双方は証明書の検証を行い、CRLによって証明書の失効確認を行う。証明書の失効確認は、SRM内でCRLを使って行う方法だけでなく、処理負荷を軽減するために、OCSP（Online Certificate Status Protocol）を利用することも可能である。

### 【2】受信端末-SRM間における権利情報の移動

受信端末は、SRMとの相互認証を完了してセキュアチャネルを確立すると、権利情報をSRMに格納することができる。権利情報をSRMに送信する方法はメッセージ形式であり、一般的なアドレス指定によるメモリアクセスではない。SRM内部で権利情報を格納する方法はSRMの実装依存であるが、SRMは権利情報のデータベース機能をもつ。

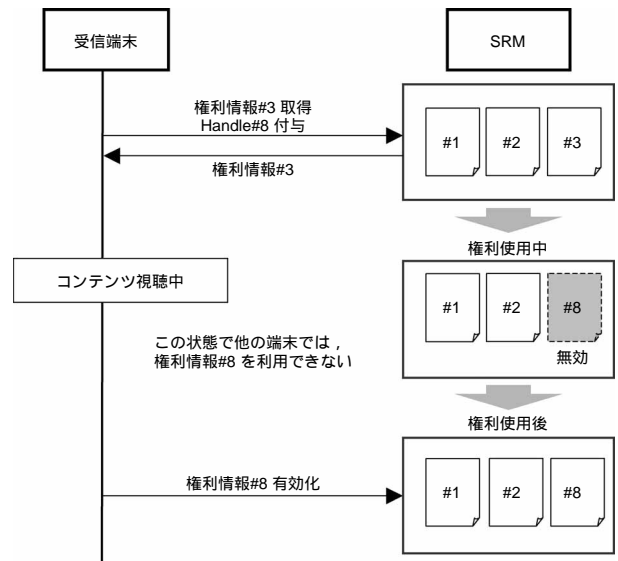
権利情報の移動処理中に、たとえばSRMが抜き出された場合、権利情報が消失する恐れがある。これを防止するために、受信端末は処理操作のログを常に保持しておき、SRMが再度挿入されると、受信端末はログを参照してリカバリー処理を行う。

### 【3】SRM上での権利の消費

OMA-DRMの権利情報には、再生可能回数や再生可能時間などの制約情報を含むことができる。受信端末は、コンテンツの視聴に応じて制約情報を更新する。これを権利の消費と呼ぶ。

受信端末がSRM上の権利を消費する場合、SRMから権利情報を読み出し、視聴後にSRM上の制約情報を更新する。ところが、コンテンツを視聴中にSRMが受信端末から抜き出されると、SRM上の制約情報が更新されないため、他の端末で同じ権利を重複して消費される恐れがある。

解決方法として、受信端末がSRM上の権利を消費する場合は、SRM内部でその権利情報を一時的に読み出せないようにすること（無効化と呼ぶ）が考えられる。無効化された権利情報を再び読み出せるように（有効化と呼ぶ）できるのは、その権利を使用している受信端末に限定しなければならない（ほかの受信端末によって有効化されてはならない）。この仕組みを、**第5図**に示した。SRMに3つの権利情報が格納されており、それぞれの権利情報には識別番号（Handle値）として#1、#2、#3が付与されている。受信端末がHandle値 #3の権利情報を取得する際に、#3の無効化と同時に、その受信端末だけが知っているHandle値（たとえば、#8）を付与する。ほかの受



第5図 SRM上での権利消費

Fig. 5 Local rights consumption

信端末は、そのHandle値 #8を知らないで権利情報の有効化も読み出しもできない。なお、実際にはHandle値は10バイトの乱数を使用する。

これらの仕組みにより、OMA-DRMと同等のセキュリティ強度を実現し、リムーバブルメディア特有の課題をも解決した。

## 6. まとめ

SDメモリーカードにおいて各DRMが定めるコンテンツ保護が適用可能となる仕組みを規格化した。今回は、携帯電話のネットワーク配信サービスで利用することを想定してOMA-DRMの対応を優先的に行った。OMA以外のDRMについても、SRMアプリ規格の策定とDRM規格の拡張により、ASSDカードに適用することが可能となる。ASSDカードは1枚で複数のDRMに対応できるため、エンドユーザーは従来のSDメモリーカードと同様に、さまざまな機器でASSDカードを利用可能となる。携帯電話以外の民生機器やパソコンにおいてもASSDカードが幅広く活用されることを期待する。

### 参考文献

- 1) Open Mobile Alliance : DRM Specification. OMA-TS-DRM-DRM-V2\_0\_2-20080226-A.
- 2) Open Mobile Alliance : OMA Secure Removable Media Specification. OMA-TS-SRM-V1\_0-20080128-C.
- 3) 4C Entity : Content Protection for Recordable Media Specification, SD Memory Card Book Common Part.

- 4) 高橋栄治 他：携帯電話向けコンテンツ利用管理（OMA DRM）の規格化推進 Matsushita Tech. Journal 52, No. 2, p. 85 (2006).
- 5) 塚田孝則：企業システムのためのPKI-公開鍵インフラストラクチャの構築・導入・運用（日経BP社）.

### 著者紹介



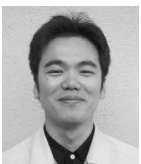
中垣浩文 Hirofumi Nakagaki  
AVCネットワークス社 技術統括センター  
Technology Planning & Development Center,  
AVC Networks Company



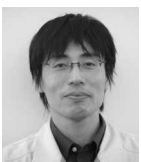
櫻井 博 Hiroshi Sakurai  
AVCネットワークス社 デバイス事業グループ  
Device Business Group, AVC Networks Company



小来田重一 Shigekazu Kogita  
AVCネットワークス社 技術統括センター  
Technology Planning & Development Center,  
AVC Networks Company



上村知範 Tomonori Uemura  
AVCネットワークス社 技術統括センター  
Technology Planning & Development Center,  
AVC Networks Company



宗 広和 Hirokazu So  
AVCネットワークス社 技術統括センター  
Technology Planning & Development Center,  
AVC Networks Company