HD DVDで利用されるコンテンツ保護技術

Content Protection Technology Applied to HD DVD

加藤　拓　■ KATO Taku
磯崎　宏　■ ISOZAKI Hiroshi
石原　淳　■ ISHIHARA Atsushi

HD DVDでは高画質コンテンツやインタラクティブコンテンツが扱われるために，これまでのDVD以上に強固なコンテンツ保護技術が要求されている。そのため，東芝を含む8社は，次世代DVD向けのコンテンツ保護技術であるAACS（Advanced Access Content System）を共同開発した。

AACSは，HD DVDプレーヤやレコーダなどに既に採用されており，高品位デジタルコンテンツを扱う機器やメディアによって広く普及することが期待されている。また，この技術は，利用する暗号アルゴリズムを強化しただけでなく，機器の不正改造や不正コンテンツの流通など様々な脅威に対抗するための技術を取り入れており，パッケージメディアや記録メディア上での利用にとどまらず，ネットワークを利用したサービスにも利用できる。

HD DVD, the "next-generation DVD," offers new experiences to users including high-definition video contents and interactive contents. However, the importance of content protection technology has increased. For this reason, a new content protection technology called the advanced access content system (AACS) has been developed.

AACS has been adopted for HD DVD players and recorders and is expected to be widely used in many types of devices and media. This technology contains a number of security protection elements to assist content providers. It can be applied not only to contents stored on media but also to networking technologies.

1　まえがき

1996年にDVDが登場してから約10年が経った2006年3月にHD DVDが世の中に登場したが，これは，放送がアナログからデジタルに移行するとともに，ユーザーが手軽に高画質（HD：High Definition）コンテンツを享受できる環境が整い始めた世の中の流れにも符合している。HD DVDは，HDコンテンツをそのままの画質で手軽に記録するためのメディアとしてはもちろんのこと，放送では得られないような高画質かつ魅力的なパッケージコンテンツを提供するメディアとしても期待されている。それに対して映画会社や放送事業者などのコンテンツ提供者からは，付加価値の高いコンテンツを記録するために必要不可欠な機能として，より強固なコンテンツ保護技術が求められている。

ここでは，コンテンツ保護技術としてHD DVDで採用されているAACS（Advanced Access Content System）について述べる。

2　DVDにおけるこれまでのコンテンツ保護技術

DVDビデオではCSS（Content Scramble System）と呼ばれるコンテンツ保護技術が採用されており，CSSでは次の三つの特徴的な機能が採用されている。

（1）階層的な暗号化鍵管理
（2）コンテンツ スクランブル
（3）パソコン（PC）環境でのバス認証

その後登場したDVDオーディオでは，暗号アルゴリズムをより強固なものに見直すとともに，CSSで採用された三つの機能に加えて，メディアによる不正機器の無効化やオーディオ電子透かしといった新たな機能が盛り込まれたCPPM（Content Protection for Prerecorded Media）と呼ばれるコンテンツ保護技術が採用された。特に不正機器の無効化機能は，AACSにおいてももちろんのこと，その後に続いて登場したコンテンツ保護技術には必要不可欠な機能要件となっている。

DVDオーディオとほぼ同時期には，DVD-R（Recordable）/RW（Re-recordable）/RAM（Rewritable）用のコンテンツ保護技術として，CPPMとほぼ同等の機能が採用されたCPRM（Content Protection for Recordable Media）のライセンスも開始された[1]。

これらのコンテンツ保護技術がライセンスされる際には，技術仕様だけでなく実装時の遵守規定（Compliance Rule）や強じん性規定（Robustness Rule）を課すことによって，コンテンツ保護機能をより確実に働かせるようになっている。

しかし，どのコンテンツ保護技術も仕様策定時に決められていた輸出管理規制内で暗号アルゴリズムが選定されていることや，インターネットによって急速に普及したファイル交換な

どのネットワーク機能の強化に適応するためには，これまでのコンテンツ保護技術をそのままHD DVDの保護に採用するだけではコンテンツ提供者の要求を満たすことはできない。

3　AACSの概要と基本要素

AACSはインテル社，IBM社，マイクロソフト社，ソニー(株)，松下電器産業（株），ワーナー・ブラザーズ社，ウォルト・ディズニー社，及び東芝の8社が共同で開発した技術であり，AACS LA（Advanced Access Content System Licensing Administrator, LLC, http://www.aacsla.com/）がライセンスを行っている技術である。AACSは，設立メンバーに映画会社が参加していることからもわかるとおり，技術規格作成時点からコンテンツ所有者の意見を取り入れており，様々な技術が採用されている[2]。

AACSは，パッケージメディアであるHD DVDビデオ[3]と記録形メディア[4]であるHD DVD-R/RAMメディアのどちらにも適用されているが，HD DVDビデオ用のほうがより多くの要素技術が盛り込まれている。その主な理由としては，記録形メディアの保護はレコーダがリアルタイムで行わなければならないのに対して，パッケージメディアの場合にはディスク作成（オーサリング）に時間と手間を掛けることができるので，より複雑な機能を採用できるためである。そこで，ここではHD DVDビデオを中心にしてAACSについて述べる。HD DVDビデオでは以下のような要素技術が採用されている。

(1)　階層的な鍵管理

(2)　ハードウェア（H/W）機器とソフトウェア（S/W）機器の分離

(3)　不正機器の無効化
- 定期的なS/Wの更新

(4)　再生機器の同定

(5)　不正コンテンツの無効化

(6)　コンテンツの暗号化

(7)　PC環境向けのバス認証
- 不正S/Wの排除
- 不正ドライブの排除

AACSでは，コンテンツや鍵情報の暗号化には鍵長128ビットのAES（Advanced Encryption Standard）が，また，データの正当性を示すためのデジタル署名やバス認証に使われる鍵共有には，位数160ビットのだ円曲線上の暗号アルゴリズムが採用されている。

4　不正機器の無効化

AACSでは不正機器の無効化のためにMKB（Media Key Block）と呼ばれる技術が採用されており，コンテンツの暗号化／復号に必要なすべての鍵は，デバイスが持つ秘密鍵（デバイス鍵）を使ってMKBを処理しなければ復号できないようになっている。同様の鍵構造はCPPM及びCPRMでも既に採用されているが，AACSではMKBを利用してS/W機器とH/W機器で使われるデバイス鍵を分離している。**図1**の“S/W機器とH/W機器の分離”部分で示しているように，S/W機

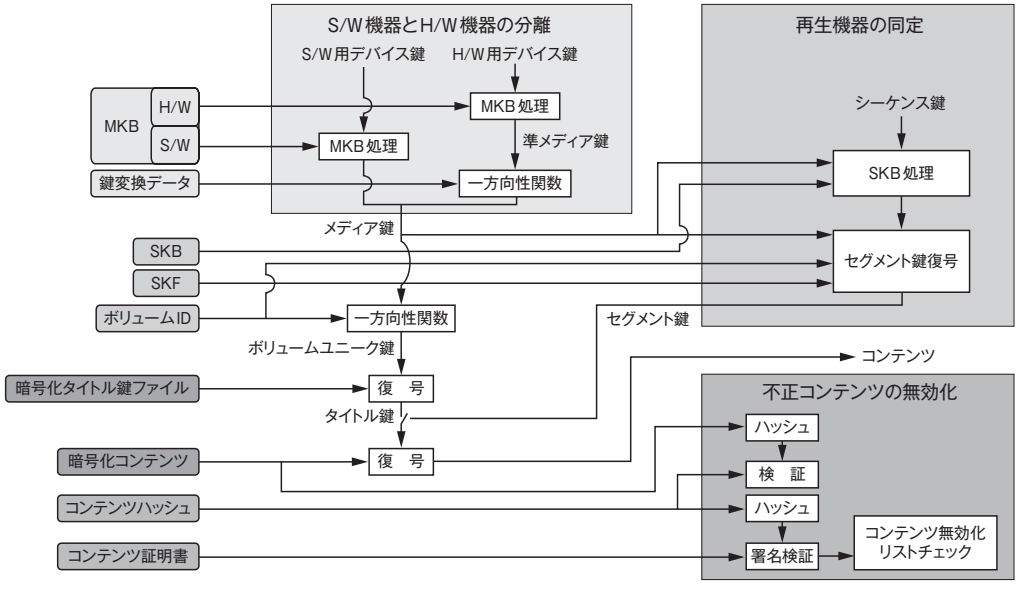

図1. HD DVDビデオの保護に利用されるAACS要素技術と処理の流れ ― 想定される攻撃に対して用意された様々な保護技術処理をすることによって，HD DVD-Videoコンテンツが再生される。

AACS security components and their process flow to secure HD DVD contents

器では，MKBを処理することによりその後の処理に必要なメディア鍵が得られるが，H/W機器では，メディア鍵を得るためには，MKB処理して得られた準メディア鍵に加えて別の手段でメディアに記録された鍵変換データを読み出す必要がある。この鍵変換データの読出しに必要な仕様は，AACSではなく東芝アメリカ情報システム社からライセンスされているが，S/W機器では鍵変換データを扱う必要がないため，PC用のS/W機器やHD DVDドライブには鍵変換データを読み出す機能は備えられていない。

そのほかにH/W機器とS/W機器の違いとしては，一般的なH/W機器は1台ごとに異なるデバイス鍵セット（1台の機器には253個のデバイス鍵が割り当てられる）が使用されているが，S/W機器ではS/Wが同じであれば同じデバイス鍵セットを使用することが許され，その代わりにデバイス鍵セットの定期的な更新義務が課せられている。なお，このデバイス鍵セットはHD DVDビデオ再生機器だけでなく，HD DVD記録機器用途にも利用可能である。

この更新情報はMKB生成時に反映されており，デバイス鍵の更新を怠った場合には，更新期間経過後に発売されるHD DVDビデオタイトルが再生できなくなるため，かりにS/W機器になんらかの攻撃が加えられ，使用されているデバイス鍵セットが不正に利用される状況が表面化しなかった場合でも，そのS/W機器の更新期間経過後には，新しいHD DVDビデオタイトルが不正に再生できないようになっている。

5　再生機器の同定

ある機器を攻撃あるいは実装不備箇所を不正に利用することによってAACSで保護されていたコンテンツが不正に流出された際には，当該機器の無効化が実施されるが，流出元となった機器が明らかでない場合が考えられる。そのようなときに流出したコンテンツから流出元機器を特定するために用意されているのが，シーケンス鍵（Sequence Key）技術である。同じく図1の“再生機器の同定”部分で示しているように，シーケンス鍵技術は，機器に割り当てられるシーケンス鍵セット，メディアに記録されたSKB（Sequence Key Block）とセグメント鍵ファイル（SKF：Segment Key File），及び複数のセグメントを備えた暗号化コンテンツによって実現されている。

シーケンス鍵技術を採用したコンテンツは，**図2**に示すように，コンテンツの一部がシーケンス鍵セクションと呼ばれる多重化されたコンテンツ（セグメントと呼ぶ）で構成されており，一つのシーケンス鍵セクションは八つのセグメントから構成される。個々のセグメントに電子透かしなどを利用して人間に知覚できない異なる情報を埋め込んでおくことによって，流出したコンテンツから流出元機器で使用されているデバイス鍵セットの特定が可能になる。

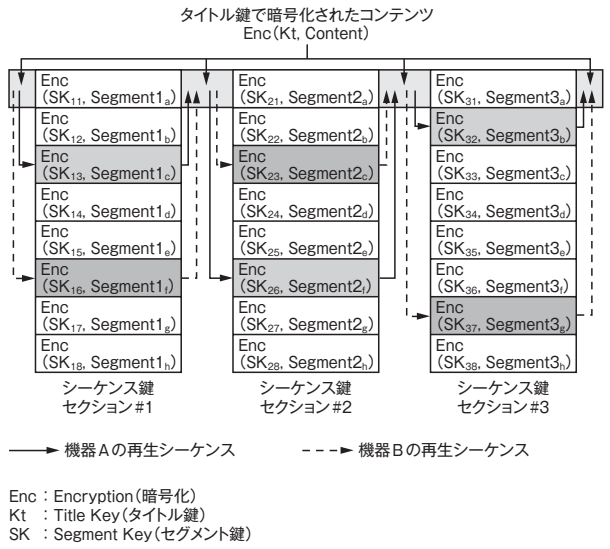

図2．シーケンス鍵を利用したコンテンツ保護 ― シーケンス鍵を利用して機器ごとに再生されるコンテンツに差異を加えることにより，再生機器の特定が実現される。

Example of content protection with exclusive sequence key embedded in content data to identify players

シーケンス鍵セクションは一つのメディア内で最大192か所用意することができ，一つ一つのセグメントはSKFに格納されているセグメント鍵によって暗号化されている。個々の機器は，自身に割り当てられたシーケンス鍵セットでSKBとSKFを処理することによって復号されるシーケンス鍵セクションごとに一つのセグメント鍵を使って，指定されたセグメントを復号する。

このように，機器ごとに復号可能なセグメントが指定されているため，図2で例示しているように，ある機器Aによって再生されるセグメントの組合せは，別の機器Bを含むそのほかすべての機器によって再生されるセグメントの組合せとは異なる。

6　不正コンテンツの無効化

AACSでは，不正コンテンツの再生を止めるために，正当なコンテンツにはコンテンツ証明書（Content Certificate）が付けられている。コンテンツをコンテンツ証明書に関連付けるための処理を**図3**に示す。コンテンツはEVOBU（Enhanced Video OBject Unit）と呼ばれるHD DVDビデオフォーマットで決められたデータ単位ごとに区切られ，すべてのデータ単位ごとに計算されたハッシュ値がCHT（Content Hash Table）に記録される。コンテンツ証明書にはCHTのハッシュ値（代表ハッシュ値）が記録されたうえで，AACS LAによってデジタル署名が付けられる。

コンテンツ再生時には，コンテンツ証明書のデジタル署名を検証するとともに，再生コンテンツのハッシュ値を計算して，CHTに記録されたハッシュ値に一致することを確認しなけれ

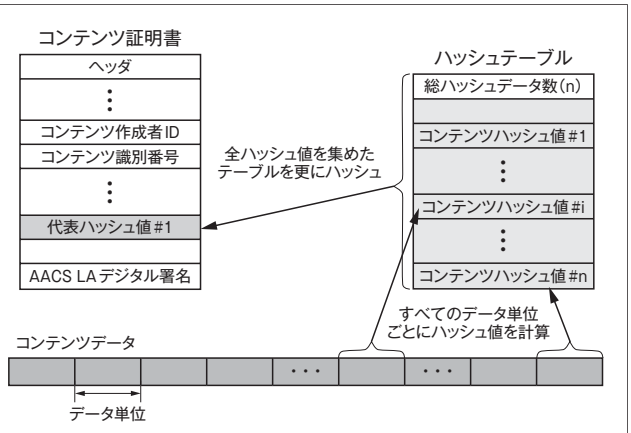

図3. コンテンツ証明書の作成手順 — コンテンツを一定単位ごとに区切ってハッシュ値を求めることにより，コンテンツを特定するためのコンテンツ証明書を作成する。

Calculation scheme of content certificate

ばならない。署名が合わない場合や計算したハッシュ値が一致しない場合には，再生が停止される。

更に，AACSからはコンテンツ無効化リスト（CRL：Content Revocation List）と呼ばれるデータが発行されてコンテンツといっしょにメディアに記録されており，CRLには，海賊版などの不正コンテンツに付けられているコンテンツ証明書に記録された，コンテンツ識別番号が登録されている。機器は，コンテンツ再生時には，メディアに記録されているCRLを利用して内部メモリに格納したCRLを最新の状態に更新しなければならず，そのコンテンツのコンテンツ識別番号が自身のメモリに格納したCRLに登録されていた場合には，再生が停止される。

7　ドライブ認証

AACSでも，CSS，CPPM，及びCPRMと同じく，PC用のS/W機器がHD DVDドライブからAACSで保護されたデータを読み出すためには，ドライブ認証を行わなければならない。AACSのドライブ認証では，だ円曲線上の公開鍵暗号アルゴリズムであるECDSA（Elliptic Curve Digital Signature Algorithm）とECDH（Elliptic Curve Diffie-Hellman）を採用することで，相互に接続された相手の正当性を検証している。ドライブとS/W機器には，AACS LAからライセンスされたドライブ証明書（Drive Certificate）あるいはホスト証明書（Host Certificate）と呼ばれる個別の公開鍵証明書が割り当てられ，各証明書にはドライブあるいはS/W機器のID（IDentification）が記録されている。

実装の不備や攻撃を受けたことによって必要なセキュリティ要件を満たせなくなったドライブやS/W機器のIDは，HRL（Host Revocation List）あるいはDRL（Drive Revocation List）に登録され，MKBの一部として配布される。ドライブ認証時に相手から受け取る証明書内のIDがHRL/DRLに登録されている場合には，認証処理を停止することで，不正ドライブや不正S/W機器を利用してAACS保護データが読み出されることを防止している。

8　あとがき

HD DVDやAACSではネットワーク連携機能もサポートされており，今後は様々なサービスが提供されることが期待されている。特に，AACSではManaged Copyと呼ばれる機能のサポートの準備が進められている。Managed Copyとは，HD DVDビデオコンテンツをコンテンツ保護された状態でPCのハードディスク装置などへコピーできるようにする機能であり，これによりHD DVDビデオで販売されたコンテンツをポータブル機器にコピーして楽しむなど，様々な環境で利用できるようになる。

AACSでは，そのほかにも，新しい機能やサービスを実現するために必要な要素技術が検討されている。

文　献

(1) 加藤　拓. コンテンツ保護アーキテクチャ. 東芝レビュー. 58, 6, 2003, p.8－11.
(2) AACS. Introduction and Common Cryptographic Elements Rev.0.91. 2006. <http://www.aacsla.com/specifications/>,（参照2007-05-10）.
(3) AACS. HD DVD and DVD Pre-recorded Book Rev.0.912. 2006. <http://www.aacsla.com/specifications/>,（参照2007-05-10）.
(4) AACS. HD DVD Recordable Book Rev.0.921. 2006. <http://www.aacsla.com/specifications/>,（参照2007-05-10）.

加藤　　拓　KATO Taku, D.Eng.
研究開発センター コンピュータ・ネットワークラボラトリー研究主務，工博。情報セキュリティ技術及びコンテンツ保護技術の研究・開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.

磯崎　　宏　ISOZAKI Hiroshi
研究開発センター コンピュータ・ネットワークラボラトリー。ホームネットワーク及びセキュリティ技術に関する研究・開発に従事。
Computer & Network Systems Lab.

石原　　淳　ISHIHARA Atsushi
デジタルメディアネットワーク社 HD DVD事業統括部 光ディスク開発部参事。光ディスク機器の開発，規格化，及びコンテンツ保護技術の開発に従事。
HD DVD Div.