コンテンツ保護技術のＡＶ機器への実装

Implementation of Copy Protection Technologies for Audiovisual Equipment

馬渡　正彦　　**澤　繁隆**　　**東　一樹**

■ MAWATARI Masahiko　■ SAWA Shigetaka　■ AZUMA Kazuki

コンテンツ保護の仕組みを実装する製品開発にあたっては，製品に組み込まれた秘密情報が暴露されないよう堅牢（けんろう）に設計しなければならない。また，製造工程においても，秘密が漏れないよう情報管理を行う必要がある。

東芝は，DVDレコーダやデジタルテレビ（TV）などを開発するにあたって，秘密情報を閉じ込めたコンテンツ保護用LSIと，製品1台ごとに異なる値の秘密デバイス鍵の書込みツールを開発した。

A licensee has to comply with the robustness rules and confidentiality of content protection technology when manufacturing licensed products. This includes maintaining the secrecy of the algorithm of the content protection cryptography technology and/or device keys for each product, as well as maintaining secrecy when delivering or writing the device keys.

Toshiba has developed not only content protection LSIs but also tools for writing device keys in order to meet these security requirements.

1　まえがき

1996年にDVDビデオプレーヤを発売するにあたり，その映画などの著作物（コンテンツ）を保護するためにCSS（Content Scramble System）というコンテンツ保護技術方式が開発されライセンスされた[(1)]。その後，AVコンテンツの広まりに伴い，デジタルTV，DVDオーディオプレーヤ，DVDレコーダ，SDメモリカードなどの機器や記録媒体，及びそれらが結合されたネットワークでの保護技術が開発された[(2)]。

コンテンツ保護技術には，**図1**に示すように，コンテンツの暗号化／復号やそれに用いる鍵の取得に関する規格がある。これらの技術のライセンスを受けて製品を開発製造する際には，製品そのものに含まれている秘密情報が暴露されないよう十分に堅牢（ロバスト）にすることが要求されている。更に製品の製造工程においてすら，これらの秘密情報が漏れないよう安全に管理することも求められる。

保護の仕組みをLSIとしてパッケージの中に閉じ込めて実現することは，製品の堅牢性を確保するうえで非常に有効な方法である。ここでは，二つの代表的な保護規格を実装したLSIについて述べる。一つはIEEE1394（米国電気電子技術者協会規格1394）ネットワーク上でコンテンツを伝送するときの保護規格であるDTCP（Digital Transmission Content Protection）準拠のLSIであり，もう一つはDVDオーディオプレーヤの保護規格であるCPPM（Content Protection for Prerecorded Media）準拠のLSIである。

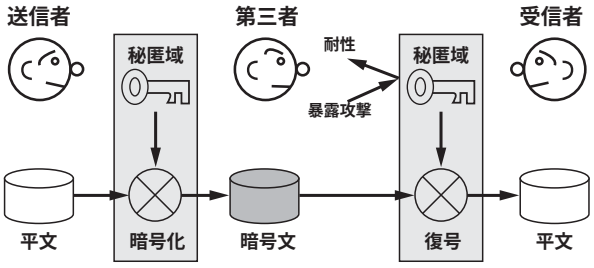

図1．情報秘匿と暴露攻撃の耐性 ― 秘密情報は暴露攻撃に対して耐性のレベルが規定されている。

Data secrecy and robustness against disclosure attack

更に，これらのLSIには，暗号化されたコンテンツの復号鍵に関する機密情報が，一つ一つのLSIごと（製品ごと）に記録されている。この秘密情報は，LSI実装時に書き込まれるため，製品製造段階での秘密管理の仕組みが必要であり，この管理方法についても解説する。

2　IEEE1394のコンテンツ保護LSI

2.1　DTCP仕様の秘密情報

IEEE1394伝送路でのコンテンツ保護規格は，DTLA（Digital Transmission Licensing Administrator）社が技術供与しているDTCP仕様[(2)]を採用している。この仕様の特徴は，完全認証（Full Authentication）と制限認証（Restrict Authentication）のどちらかで通信相手の認証と共通鍵の配

送を行うことである。

完全認証では，コピー不可（Copy-never）コンテンツを配信するときに使用しなければならない。更に，次のような仕様がある。

⑴ DTLA社署名付きの認可証（Device Certificate）を，コンテンツを送り出す機器（ソース）とコンテンツを受け取る機器（シンク）で交換し，それぞれ署名検証を行う。

⑵ ソースとシンクでそれぞれECDH第一段階値（Elliptic Curve Diffie Hellman first phase value）を発生して機器署名を行い，互いに交換する。

⑶ 交換した機器署名を検証し，ECDH交換鍵の計算をして，共通鍵を得る。

制限認証は，1世代コピー可（Copy-one-generation）又はノーモアコピー（No-more-copies）のコンテンツを配信するときに利用する。

DTCP仕様の秘密情報には，(1)暗号／復号器のアルゴリズム，(2)完全認証用楕円（だえん）関数のパラメータなどの値，(3)認可証とともにDTLA社から購入するデバイス鍵値，(4)共通鍵などの演算途中の値，がある。より具体的な例としてECDH共通鍵配送とコンテンツ暗号化／復号の処理を**図2**に示す。この図の中で，乱数（X_A/X_B），楕円曲線上のベースポイント（G），共通鍵（Ka），コンテンツ（C）の暗号器と復号器のアルゴリズムは秘密情報である。

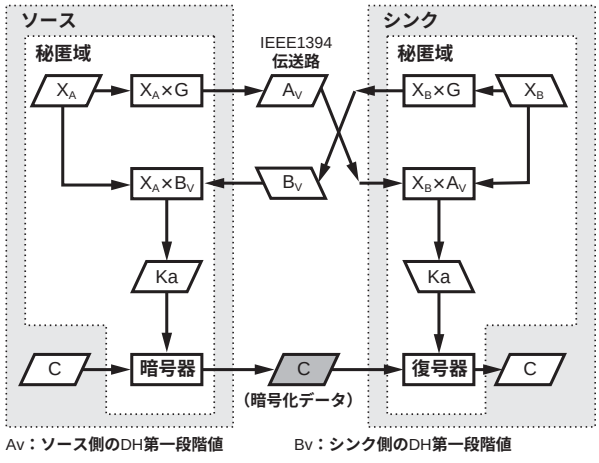

図2．共通鍵配送とコンテンツ暗号化／復号 ― 完全認証ではECDHアルゴリズムによる共通鍵を得ている。

Shared secret derivation and content ciphering/deciphering

2.2 DTCP対応LSI概要

2000年夏に発売のデジタルTV向けに開発した[3]DTCP準拠LSIのチップの機能ブロック図を**図3**に示す。

このLSIには，次の特徴がある。

⑴ 2チャネル（CH）のコンテンツ暗号／復号器を持つ。

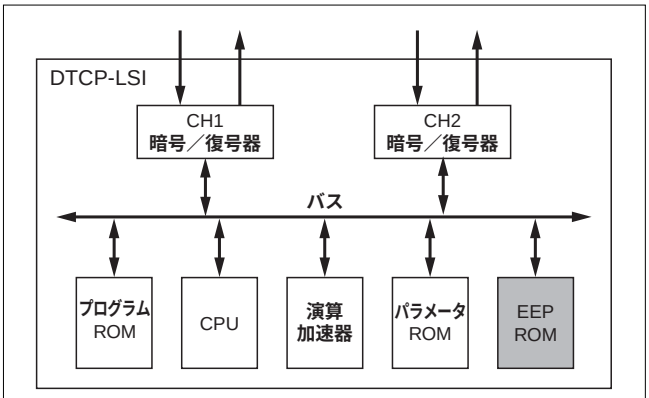

図3．DTCP準拠LSIのブロック図 ― 通信相手方との認証を行うプロセッサ部分とコンテンツを暗号化／復号する部分から構成される。

Block diagram of digital transmission content protection (DTCP) -compliant LSI

⑵ DTLA社から購入する機器ごと（チップごと）に異なるデバイス鍵の記憶用EEPROMを内蔵している。

⑶ 完全認証用楕円暗号処理のため，CPUと演算加速器を組み込んでいる。

相手機器との認証命令や，チップ動作モードの設定，チップの動作状態は，外部にあるコントローラ（図示せず）にて図3に示すバスを介して設定する。TS（Transport Stream）パケットは，暗号／復号器に直接入出力する。

DTCP仕様の秘密情報のうち，暗号／復号器のアルゴリズムは暗号／復号器とプログラムROMにある。また，完全認証用楕円関数のパラメータなどの値はパラメータROMに，デバイス鍵値は内蔵EEPROMに，演算途中の値は，CPUや演算加速器あるいは暗号／復号器のレジスタにある。

機器にこのLSIを実装したときに，これの秘密情報が容易に観測されないように，そして，LSI製造検査工程上のテストデータにも現れることのないように，外部コントローラからバスを介してのアクセス禁止回路とBIST（Build-In Self Test）回路を組み込んでいる。

3 DVD向けコンテンツ保護LSI

3.1 DVDのコンテンツ保護概要

DVD-Video規格のコンテンツ保護規格はCSSを定めていたが，その後，DVD-Audio規格のそれはCPPM規格[4]を採用し，また，DVD-VR（Video Recording）規格のそれにはCPRM（Content Protection for Recordable Media）規格を採用している。

CPPMの概要を**図4**に示す。メディア鍵（MK）を元にしたコンテンツ鍵（Kc）で，コンテンツ（C）を暗号化したコンテンツと，メディア鍵を用いて鍵ブロックを暗号化したメディア鍵ブロック（MKB）を記録する。DVDオーディオプレーヤでは，

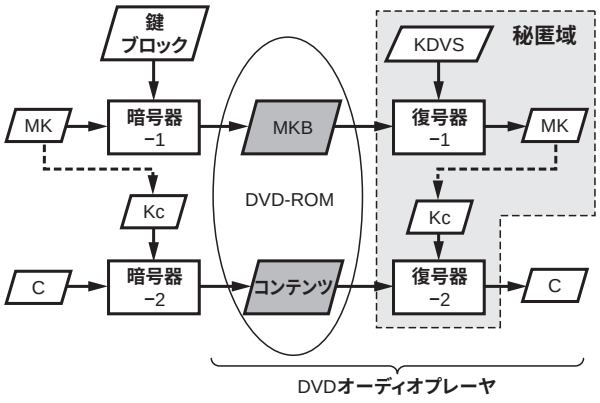

図4．CPPMの概要 ― ネットワークでの共通鍵配送と異なり，そのメディア鍵（MK）の配送は一方向である。

Schematic diagram of content protection for prerecorded media (CPPM)

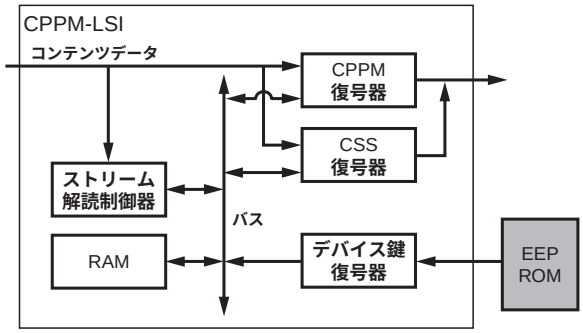

図5．CPPM準拠LSIのブロック構成 ― 機器ごとに異なるデバイス鍵は，外部のEEPROMに暗号化して記録している。

Block diagram of CPPM-compliant LSI

これらの復号を行う。まず，鍵ブロックのサブセットであるデバイス鍵（KDVS）を用いて，メディア鍵を復号する。次に，このメディア鍵を使って暗号化と同様の方法でコンテンツ鍵を得て，コンテンツを復号する。

図4中のCPPM仕様の秘密情報は，復号器－1や復号器－2にあるS-Boxと言われる数表（図示せず）や，また，デバイス鍵，メディア鍵やコンテンツ鍵などの値である。

CSSとCPPMあるいはCPRMの違いは，CSSのマスター鍵（図4中のKDVSに相当する）がデコーダ（ボードあるいはソフトウェアやLSI）の生産会社ごとに異なるのに対して，CPPMやCPRMの各デバイス鍵は，DVDプレーヤ1台ごとに異なることである。それゆえにCPPMやCPRMの実装時は，DTCPと同様にデバイス鍵の書込みのためのEEPROMが必要であり，また，その鍵の書込みツールも必要である。

3.2 CPPM/CPRM準拠LSI概要

CPPMやCPRM準拠LSIは，DTCP準拠のLSIの場合と異なり，それらのデバイス鍵記憶用のEEPROMはLSIの外部に設けた。CPPM準拠LSIの構成を**図5**に示す。

EEPROMに書き込まれた暗号化デバイス鍵は，DVDプレーヤの電源投入時にLSIに読み込まれ，デバイス鍵復号器にて復号され，RAMに保持される。メディア鍵ブロックデータをコンテンツデータバスに入力して，RAM上のデバイス鍵にて復号して，メディア鍵を得る。この得られたメディア鍵を元にそのほかの処理を経てコンテンツ鍵を得た後，このコンテンツ鍵にて暗号化コンテンツの復号を行う。ストリーム解読制御器は，これらメディア鍵の復号やコンテンツを復号するため，ストリームを解読し，RAMにあるデバイス鍵を利用し，コンテンツデータを復号制御している。

CPRM準拠のLSIもほとんど構成は変わらず，図5中のCPPM復号器の部分が，CPRM暗号／復号器となる。

CPPMやCPRM仕様の秘密情報は，S-BoxはCPPM復号器あるいはCPRM暗号／復号器にあり，デバイス鍵やコンテンツ鍵などの値は，EEPROMやRAM，あるいはレジスタ上にある。EEPROM上のデバイス鍵は独自方式の暗号化がされており，このデバイス鍵復号器も秘密となる。

これらのデータやそのレジスタは外部から観測できないように封印している。

4 デバイス鍵の書込み処理

DTCPとCPPM/CPRM仕様の秘密情報とLSI構成について述べた。同じくライセンサーから供与を受けるデバイス鍵について述べる。このデバイス鍵は製品1台ごとに異なるため，そのLSIの生産工程又はその搭載ボードや搭載機器の生産工程でEEPROMへの書込みを行っている。

DTCP準拠LSIの場合はLSIの検査工程で，CPPM/CPRM準拠LSIの場合はDVDプレーヤやレコーダ機器生産工程でデバイス鍵の書込みを行っている。そしてこのデバイス鍵は秘密情報であるため，その値が暴露されないように書込み後の状態を堅牢にするだけでなく，書込み工程についても情報の漏えいについて十分に管理しなければならない。

外部EEPROMとしたCPPM/CPRM準拠のLSIに採用したデバイス鍵書込み関係の作業フローを**図6**に示す。

設計部などのパソコンPC-1に暗号化ツールを，また，製造ラインのパソコンPC-2に書込みツールを設置している。

ライセンサーから購入したデバイス鍵データファイルは，(1)設計部などで受領され，ファイルに暗号化されているので復号した後，(2)パソコンPC-1で個々のデバイス鍵ごとに独自方式の暗号化され，(3)各工場に発送される。

工場では，LSIが搭載されたボードごとにあるいはプレーヤごとに，(4)パソコンPC-2でデバイス鍵の書込み処理を行う。(5)この暗号化デバイス鍵の復号は，上述したようにLSI

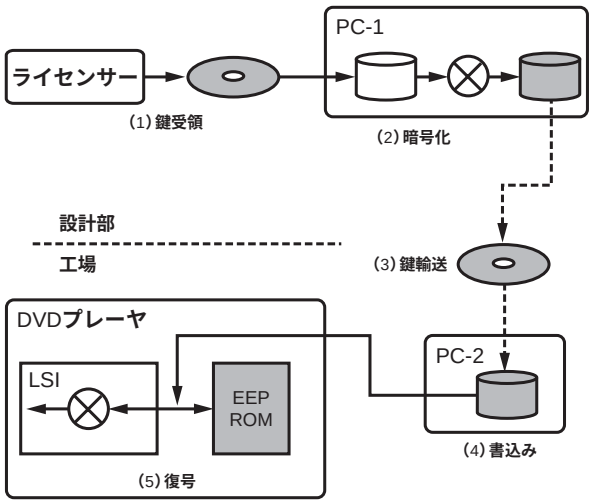

図6．CPPMデバイス鍵処理フロー ― デバイス鍵は，工場の製造ラインでは暗号化されたデータのままである。
Flowchart of CPPM device key data

内部で行っており，ユーザーがDVDプレーヤやレコーダの電源を投入したときに，LSIがEEPROMから自動的に読み込み，復号を行う。

デバイス鍵の復号器をLSI内部のハードウェアで行っていることと同様に，PC-1上の暗号器もハードウェアによって処理している。

このように，デバイス鍵の平文は設計部などでデバイス鍵の暗号化を行うときだけであり，工場への輸送途上や，製造工程では常に暗号化されたデバイス鍵データとなり，ライセンサーの指定する秘密保全が確保できている。

5 あとがき

コンテンツ保護技術の実装について，秘密情報とLSIでの秘匿方法，それに付帯するデバイス鍵の暗号化・書込みツールについて述べた。

ライセンス契約上のロバストネスルールや秘密保全に沿うことはもちろんであるが，秘密データのセキュリティレベルをどれだけ確保すればよいかは定量的に表現しにくく，評価が困難である。製品の企画段階からコンテンツ保護を正しく組み込むことや，製造工程での機密が漏れないようにしておくことが大切であり，それらの秘密情報の漏えい防止策が堅牢であるかを審査する，社内機構を設けることが大切である。

今後は，既存のコンテンツ保護規格への対応のみならず，HDTV（高精細度TV）の高精細映像を再生できるDVDなど新しいコンテンツ保護規格に準拠したLSIや，デバイス鍵の暗号化・書込みツールに対応していく。

文　献

(1) Jeffery A. Bloom, et al. “ Copy Protection for DVD Video ”. Proceedings of the IEEE. **87,** 7, 1999, p.1267－1276.
(2) DTLA. DTCP Specification Volume 1 Version 1.2a (Informational Version). <http://www.dtcp.com/>,（参照2003-3-13）.
(3) 桜井　優，ほか．BSデジタルハイビジョンテレビ用LSI．東芝レビュー．**55**，8，2000，p.44－57.
(4) 加藤　拓，ほか，DVD-Audioにおけるコンテンツ保護技術．東芝レビュー．**56**，7，2001，p.54－57.

馬渡　正彦　MAWATARI Masahiko
デジタルメディアネットワーク社 デジタルメディアデベロップメントセンター LSI開発センター主幹。VTR・DVD用LSIの開発に従事。
Digital Media Development Center

澤　繁隆　SAWA Shigetaka
セミコンダクタ社 システムLSI事業部 システムLSI統括第一部主幹。TV・VTR・DVD・デジタルTV用LSIの開発に従事。
System LSI Div.

東　一樹　AZUMA Kazuki
デジタルメディアネットワーク社 デジタルメディアデベロップメントセンター ソフトウェア第一部主務。記録AV機器のソフトウェア開発・設計業務に従事。
Digital Media Development Center