AV ネットワークのコンテンツ保護

Content Protection for Audiovisual Network

小久保　隆　　**奥山　武彦**
■ KOKUBO Takashi　　■ OKUYAMA Takehiko

最近，高品位のデジタルコンテンツを視聴し記録する，新しい種類の AV 製品が市場に出ている。デジタルデータは品質の劣化なくコピーできるという特徴を持つため，これらの製品の間でコンテンツをデジタル転送する際には，コンテンツ保護機構を備えることが必要である。DTCP（Digital Transmission Content Protection）はネットワーク上でコンテンツを保護する規格であり，デジタル放送受信機や記録機などで採用されている。東芝は，デジタルテレビ（TV）などの DTCP 準拠の製品を開発し，商品化している。

New types of audiovisual products enabling users to view, listen to, or record high-definition digital contents have recently appeared on the market. A feature of digitized data is that it can be copied without degradation of quality. It is therefore necessary to have a content protection mechanism when digital contents are transmitted between such products.

Digital transmission content protection (DTCP), a standard by which contents on a network are protected, is being adopted for digital-broadcast receivers, recording devices, and so on. Toshiba is developing and commercializing digital products based on DTCP, such as digital television.

1　まえがき

インターネットの普及や，デジタル放送，DVD などにより，高品位のデジタルコンテンツを視聴し記録するようになると，これを家庭内ネットワークとして活用する新しい AV 市場の需要が出てくる。しかし，このようなデジタルコンテンツは，簡単にネットワーク経由で劣化のないコピーができてしまうため，コンテンツホルダーにとっては，著作権を保護する仕組みの範囲内でのコンテンツの流通しか認められない。このコンテンツホルダーに認められた AV コンテンツ用ネットワークの著作権保護規格が DTCP である。DTCP は，東芝，松下電器産業（株），ソニー（株），（株）日立製作所，Intel 社の５社が開発し，DTLA（Digital Transmission Licensing Administrator）社がライセンス供与している。DTCP の対象となるネットワークとしては，まず，デジタル放送機器と記録機器との間でコンテンツ伝送のネットワーク技術として使われている IEEE1394（米国電気電子技術者協会規格 1394）（通称：i.LINK(注1)）が最初であり，デジタル TV と DVHS（Digital Video Home System）やハードディスクビデオレコーダ（AV 用 HDD（磁気ディスク装置））との接続などで，既に使われている。

当社で開発した製品の中では，国内では最初の IEEE1394 準拠の BS（放送衛星）デジタル放送受信機である TT-D2000 から DTCP 機能を搭載し[1]，その後，BS デジタル放送と CS110 °（通信衛星）デジタル放送を受信できるデジタル TV D3000（**図1**）や，CS110 °デジタル放送の蓄積型双方向サービスに対応した HDD 内蔵の BS デジタル・CS110 °デジタル放送受信機 ep ステーション™ (注2) EP-T100（**図2**）などの製品が DTCP に対応している。ここでは，最近追加・改定された最新の内容を含む DTCP 規格の概要と，国内デジタル放送での DTCP の取扱いについて述べる。

図1. デジタル HDTV 36D3000 ― BS デジタル放送，CS110 °デジタル放送に対応している。
36D3000 broadcast satellite/communications satellite (BS/CS) digital high-definition TV

（注1）　i.LINK は，商標。
（注2）　ep ステーションは，イーピー（株）の商標。

図2. ep ステーション™ EP-T100 ― HDD を内蔵し，BS デジタル放送やCS110 °デジタル放送が受信できる。
ep station™ model EP-T100

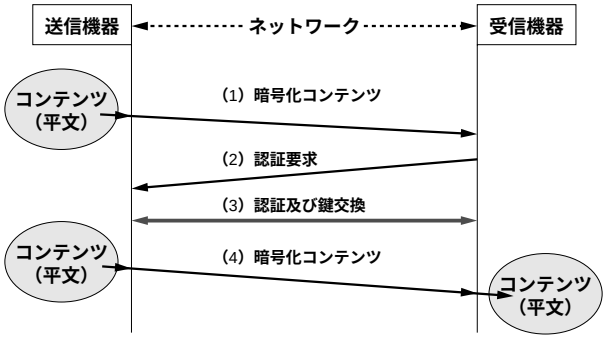

図3. コンテンツ保護の流れ ― 認証及び鍵交換を行った後，暗号化コンテンツを復号化できる。
Flow of content protection

2 DTCP の特徴

ネットワーク上でコンテンツを伝送する場合には，第三者から傍受される可能性がある。また，接続した相手機器がコンテンツを伝送してよい機器なのかどうか不明である。これらの問題を解決するために，DTCP 規格[(2)]では大きく以下の四つが定められている。

(1) 接続した機器がDTCP規格に合致した正しい機器であることを認証する(機器の種類を認証するのではない)(3.1節参照)。
(2) 機器間での伝送データを暗号化する(3.2節参照)。
(3) コンテンツとともにコピー管理情報(CCI：Copy Control Information)を伝送する(3.3節参照)。
(4) 不正機器として認定された機器はシステムから排除される。この情報を伝送するためにSRM(System Renewability Message)が定められ，SRMが示す機器を認証時に排除する(3.4節参照)。

3 DTCP コンテンツ保護技術

DTCPにおける処理の流れを**図3**に示す[(3)]。認証及び鍵交換を行った後に，暗号化コンテンツを受信機器が正しく復号できる。

3.1 認証と鍵交換

DTLA 社は機器ごとに異なる証明書をDTCP機器へ配布する。接続したDTCP機器は，この証明書を確認することにより，相手機器がDTCP規格に合致した正しい機器であるかどうかを確認する。

認証には次の2種類があり，それぞれ利用可能なCCIが異なる。

(1) 完全認証(Full authentication)
　(a) 公開鍵暗号を利用
　(b) すべてのコピー管理情報のコンテンツに対応
(2) 制限認証(Restricted authentication)
　(a) 共通鍵暗号を利用
　(b) 1世代コピー可とノーモアコピーコンテンツに対応(3.3節参照)

完全認証のプロトコルを**図4**に示す。完全認証では次の処理を行う。

(1) 相手機器が持つ証明書を相手機器の公開鍵で検証する。
(2) DH(Diffie Hellman)法により認証鍵(K_{Auth})を共有する。
(3) K_{Auth}を共有するための情報やSRMに関する情報も，デジタル署名を付加してお互いに検証する。

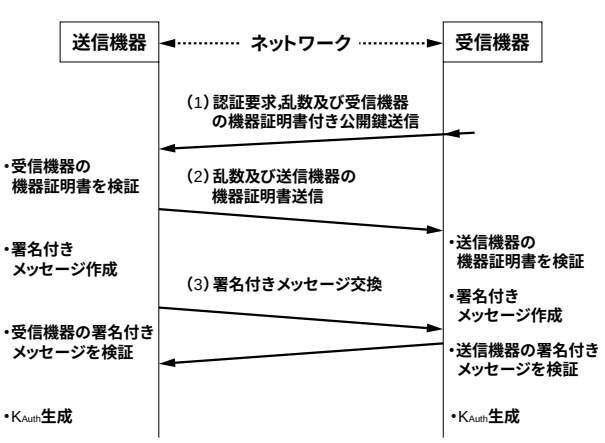

図4. 完全認証 ― すべてのCCIのコンテンツ伝送に使用可能な認証方式である。
Full authentication

制限認証のプロトコルを**図5**に示す。制限認証では次の処理を行う。

(1) お互いの機器が持つ秘密鍵を元にK_{Auth}を共有する。
(2) 送信機器が受信機器の生成するレスポンスを検証する。

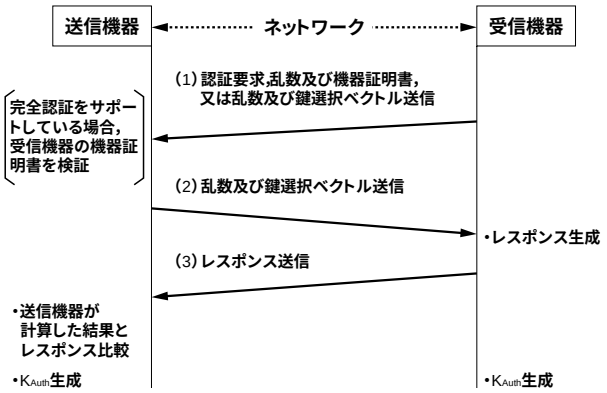

図5. 制限認証 ― 1世代コピー可とノーモアコピーのコンテンツ伝送に使用可能な認証方式である。
Restricted authentication

なお, 送信機器が完全認証に対応した機器の場合, 受信機器の証明書を検証するが, この認証を強化された制限認証(Enhanced restricted authentication)と呼ぶ。

送信機器と受信機器が対応している認証の種類に応じて, 実行される認証の種類も変わる(**表1**)。

制限認証は, 完全認証に比べて扱えるコンテンツの種類が少なくなるが, 認証処理が軽いので, 処理能力の低いAV機器でも実装することができる。

表1. 認証処理の組合せ
Pattern of authentication procedure

		受信機器	
		制限認証対応機器	完全認証対応機器
送信機器	制限認証対応機器	制限認証	制限認証
	完全認証対応機器	強化された制限認証	完全認証

3.2 コンテンツ暗号

DTCPでは, コンテンツの暗号にM6と呼ばれる64ビットブロック暗号を使っている。認証後に送信機器と受信機器とで共有した認証鍵により, コンテンツを暗号化する際に使うコンテンツ鍵を生成する。コンテンツ鍵は56ビットでCCIごとに異なる。また, コンテンツ鍵は時間とともに変化する時変鍵であり, これにより暗号強度を高めている。

3.3 CCIとEMI

CCIには次の4種類があり, 著作権のあるコンテンツにはストリーム内に記述されている。

(1) コピー不可: Copy-never
(2) 1世代コピー可: Copy-one-generation
(3) ノーモアコピー: No-more-copies　1世代コピー可のコンテンツを記録するとノーモアコピーになる。
(4) コピーフリー: Copy-free

送信機器はコンテンツのCCIに応じて, IEEE1394のパケットヘッダのEMI(Encryption Mode Indicator)に暗号化モードを設定する。これにより, 受信機器はコンテンツのCCIを簡単に理解できる。EMIによってコンテンツのフォーマットを認識しないストリーマでも正しくコピー制御ができることになる。

送信機器はCCIが異なるいくつかのストリームを送信する際には, その中のもっとも厳しい値(もっともコピー数が少ない値)をEMIとして使う。

3.4 SRM

鍵などの秘密情報は, 露呈しないように管理される必要がある。万が一露呈した場合には, コンテンツのデジタルコピーが容易に作成される可能性があるため, そのようにセキュリティ上の理由などから無効になった鍵を持つ機器に対して, 認証を失敗させる仕組みを備えている。

完全認証対応機器は新たなSRM(無効になった鍵のリスト)を受信した場合, 自機器が持つSRMのバージョンと比較し新しいバージョンのSRMを採用する。このような更新の仕組みによって, システムの完全性を長期間確保することができる。

3.5 その他の特徴

DTCPにはコンテンツ供給者の様々な要求に応えられるような規格がある。ここではそれらについて述べる。

(1) 受信機器の台数制限　同じストリームを同時に受信可能な受信機器数は最大62台である。送信機器は63台目以降の受信機器からの認証要求を受け付けてはならない。
(2) Move　AV用HDDのようなPVR(Personal Video Recorder)においては, ノーモアコピーのコンテンツはMove(移動)が可能である。Moveの際には, 受信機器にコンテンツを記録後1分以内に元のコンテンツを削除するか使用不可能な状態にする。送信機器はMove中であることを示しながらCCIを1世代コピー可として送信し, 受信機器はそれをノーモアコピーとして記録する。
　Moveは繰返しが可能で, 回数に制限はない。ただしDVHSのようなテープメディアによる記録機器はPVRではないので, それ以上Moveすることはできない。
(3) Retention　PVRにおいてはコピー不可のコンテンツは最低でも90分間Retention(保持)することが可能であり, 保持する時間が設定されればそれ以上の時間Retentionすることが可能である。設定された時間を過ぎたら, そのコンテンツは削除又は利用不可能にしなければならない。また, Retentionは一度しか許されない。
(4) 画質制限　コンテンツを受信した機器がアナログ映像を出力する際に, その画質を制限させる仕組みがある。コンテンツ受信機器は, 画質制限が設定された場

合には，52万画素以下に制限してアナログ映像を出力しなければならない。高品位TV（HDTV）出力の場合，標準TV（SDTV）出力に制限される。

4 DTCPライセンス

機器が持つ秘密情報が露呈しないように，コンプライアンスルールやロバストネスルールがDTLA社において定められている。

ライセンスを受けた者は，コンプライアンスルールを遵守して機器を製造，販売しなければならない。コンプライアンスルールには，コンテンツの送信機器が使用できるCCI，受信機器がコンテンツを受信した際のCCIに応じた処理（記録動作やコンテンツ出力処理）に関するルールなどが記述してある。

例えば，送信機器においては，その送信機器のサービス形態（有料放送か無料放送か，など）に応じて使用できるCCIの種類が定まっている。また，証明書を一つ持つ受信機器においては，記録デバイスや記録フォーマットが異なっていれば，1世代コピー可のコンテンツを同時に二つまで作成可能である。

更に，オーディオデータの伝送に関するコンプライアンスルールもある。オーディオデータにはIEC-60958（国際電気標準会議規格60958）対応データ，DVD-Audio，SACD（Super Audio CD）の三つのタイプが定義されている。なお，オーディオデータのみを記録する機器に関しては，コンテンツのフォーマットを認識できない機器は認められていない（AVデータに関してはコンテンツのフォーマットを認識できない機器（DVHSやAV用HDDなど）に記録することは認められている）。

ロバストネスルールには，DTCP技術を機器に実装する際の規則，特に機器のコンテンツ保護に対する耐性が記述されている。例えば，すべての機器はDTCP機能を無効にするようなスイッチ（ハードウェアによるものでもソフトウェアによるものでも）を設けてはならないし，また，復号したコンテンツを使用者がアクセスできるバスに通してはならない，などが記載されている。

5 デジタル放送受信機器への適用

国内におけるデジタル放送受信機の望ましい仕様に関しては，（社）電波産業会（ARIB）標準規格 STD-B21で規定されている。また，BSデジタル放送及び広帯域CSデジタル放送での運用規定はARIB技術資料 TR-B15で，地上デジタルTV放送に関してはTR-B14で規定されている。標準規格においてメディア横断的に共通な規定がなされ，運用規定で各メディアの詳細な規定が定められている。

例えばSTD-B21で，高速デジタルシリアルインタフェースとしてはIEEE1394を使用する，と規定されている。また，具体的運用を定める運用規定TR-B15，TR-B14の第二編 受信機機能仕様書で，高速デジタルインタフェースを搭載するかどうかは商品企画によるが，搭載する場合はコンテンツ保護方式としてDTCP方式の指定とDTCP記述子の挿入を規定している。

また運用規定は，第八編 コンテンツ保護規定にまとめて記載されており，ここでも，IEEE1394ではDTCP規定に従った保護を施すことを規定している。

6 あとがき

AVネットワーク上に適切な保護手段を備えることにより，良質なコンテンツを低価格で視聴者に提供することができる。DTCPは最初IEEE1394用に規格化されたが，現在ではUSB（Universal Serial Bus）やMOST（Media Oriented Systems Transport）用にも拡張され適用範囲が広がっている。USBはパソコンと周辺機器を接続するためのネットワーク規格であり，また，MOSTは自動車車内用のマルチメディアネットワーク規格の一つである。

近年，2.5GHz帯を利用するBluetooth™ (注3)や，2.5GHz帯又は5GHz帯を利用する無線LANなど，無線による伝送ネットワークが広まりつつある。このような無線ネットワーク上にAVコンテンツを伝送する場合にもコンテンツを保護する必要があり，そのための保護技術を考えていく必要がある。

文 献

(1) 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.
(2) DTLA社．DTLA HOME PAGE．<http://www.dtcp.com>，（参照2003-04-10）.
(3) 加藤 拓，ほか．IEEE1394コンテンツ保護システム．東芝レビュー．**54**，7，1999，p.34－37.

小久保 隆 KOKUBO Takashi

デジタルメディアネットワーク社 コアテクノロジーセンター ワイヤレスシステム開発部主務。デジタルAV機器，ホームネットワーク技術の開発に従事。

Core Technology Center

奥山 武彦 OKUYAMA Takehiko

デジタルメディアネットワーク社 コアテクノロジーセンター ワイヤレスシステム開発部グループ長。デジタルAV機器，IEEE1394ネットワーク規格化活動，LSI，ファームウェアの開発・設計に従事。映像情報メディア学会会員。

Core Technology Center

（注3） Bluetoothは，Bluetooth SIG，Inc．の商標。