家庭ネットワークにおける著作権保護

Home Network Content Protection

斉藤　健　　**磯崎　宏**

■ SAITO Takeshi　　■ ISOZAKI Hiroshi

著作権保護は放送，録画，他機器への伝送といった各段階で考慮する必要があり，家庭ネットワークにおいても，この原則が適用される。この原則を考慮した家庭ネットワークのための著作権保護として，東芝を含めた5社が策定し，伝送系著作権保護のデファクトスタンダードとなっているDTCP（Digital Transmission Content Protection）を紹介する。今後，家庭へのコンテンツの流入形態の多様化や，新しい家庭ネットワークの伝送媒体の普及に伴い，様々なアプリケーションに対応していくことが必要である。

Content protection needs to be taken into consideration when creating a digital audiovisual (AV) system, including broadcasting, recording, and data transmission. Home networks are one of the targets of a content protection system.

This paper introduces digital transmission content protection (DTCP), a technology standardized by five companies including Toshiba, as a de-facto standard for home network content protection. In the near future it will be necessary to support several new applications, such as the inflow of various types of AV content to the home and new home network media.

1 まえがき

近年，デジタル放送やパソコン（PC），インターネットなどの普及に伴い，家庭は，情報・通信・放送・AV・家電の融合の場となっている。また，社会環境の大きな変化（放送のデジタル化，携帯電話の普及，ADSL（Asymmetric Digital Subscriber Line）やFTTH（Fiber To The Home）などのブロードバンドインターネット環境の普及，リモートオフィスなど）を伴い，家庭にもデジタル化の波が押し寄せている。

AVの世界においても，DVDの急激な普及，各種デジタル放送の開始など，デジタル化の流れは急である。デジタル化は，劣化がない点や，メディアによってランダムアクセスが可能である，コピーが容易であるなどのメリットがあるが，これは，一方では，合法的でない不正なコピーも，劣化なしに容易に行うことができることを意味している。これを未然に防ぐために，著作権保護のための様々な技術が開発されている。

ここでは，特に家庭ネットワークの観点から，著作権保護に関する動向と，今後の展望について論じる。

2 家庭ネットワークの最近の動向と技術

2.1 セキュリティチェーン（CPSA）

例えば，“デジタル放送を録画して，後からテレビで再生して楽しむ”といった典型的な使い方を考える。これは，具体的には，① AVコンテンツが放送波に乗って，家庭内のチューナ（レコーダ）に到達する，② これを録画する，③ これを家庭内ネットワークを経由してテレビに配信する，④ テレビにて再生する，といった流れに分解できる。デジタル放送コンテンツが著作権を保護されるべきものである場合，これらの各段階において著作権保護を考慮する必要がある（**図1**）。

著作権保護のために，伝送経路やストレージにおいて，一般的に保護されるべきデジタルAVコンテンツは，暗号化されたうえで，伝送されたり蓄積されたりする。図1のような流れの中で，どこか1か所に“弱い点（セキュリティホール）”が存在すると，ここを突いて，AVコンテンツを不正にコピーす

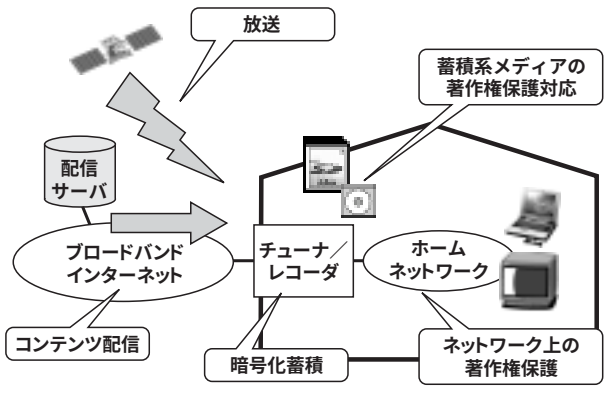

図1．家庭ネットワークにおける著作権保護 ― 著作権保護は，放送，配信，蓄積，伝送の各段階において考慮されるべきものである。

Home network content protection

ることができてしまうことになる。このため，図1の一連の流れについて，著作権保護が連続的に守られる必要がある。

これを一般的に論じているのがCPSA（Content Protection System Architecture）である（**図2**）[(1)]。CPSAでは，例えば“AVコンテンツを蓄積し，その後家庭ネットワーク上を伝送する”というように，複数の著作権保護技術をまたがってAVコンテンツのやり取りをする場合に，各々の技術が互いに関係し，有機的に機能するように（つまり，有効な保護がなされた状態で，次の著作権保護技術に移れるように）するためのアーキテクチャを定めているものであり，東芝，IBM社，Intel社，松下電器産業（株）の4社（4Cと呼ばれる）によって策定された。

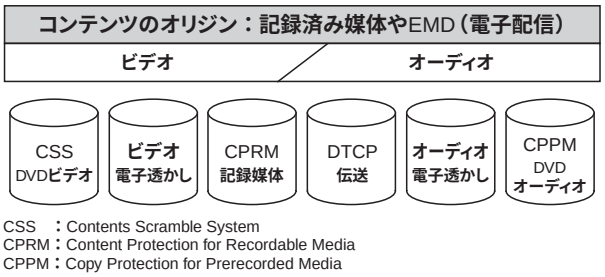

図2．CPSAの考え方 ― 複数の著作権保護技術が，相互に有機的に機能するように設計されている。
Content protection system architecture

家庭においても，この原則が適用される。著作権保護を行うべきAVコンテンツは，放送，配信，蓄積，伝送（あるいは，その繰返し）の各段階において，各々の領域で定義された著作権保護方式に従うとともに，その境界においてセキュリティホールが生じないような作りであることが要求される。このために，コンプライアンスルールやロバストネスルールといった，境界となる装置が守るべきルールが著作権保護方式ごとに定められていることが多い。

以下では，上記のCPSAを考慮した家庭ネットワーク（伝送系）のための著作権保護の方式として，DTCP[(2)]について述べる。なお，蓄積系著作権保護については，この特集のp.8～11を参照されたい。

2.2 DTCP

2.2.1 DTCPの技術

DTCPは，東芝，（株）日立製作所，Intel社，松下電器産業（株），ソニー（株）の5社（5Cと呼ばれる）により策定された，デジタル伝送用の著作権保護技術である。DTCPには，認証・鍵交換，コピー制御情報の設定，伝送するAVコンテンツの暗号化，システムリニューアビリティ（不正機器の排除）などの仕組みが備わっている。

DTCPはライセンスに基づく技術である。DTCPは，ライセンス組織DTLA（Digital Transmission Licensing Administrator）社が発行した機器証明書を各機器が持つことを前提とする。ネットワークに接続された各機器がAVコンテンツの伝送を行う場合，この機器証明書を相互に検証し，認証・鍵交換を行い，暗号鍵を共有する。そのうえで，AVコンテンツの暗号化を施して伝送する（**図3**）。暗号化アルゴリズムはM6と呼ばれる共通鍵に基づいた暗号アルゴリズムを用いる。ここでは56ビットブロック暗号が使われている。

上記の基本的な機能のほかに，DTCPには次のような仕組みも用意されている。

⑴ SRM（System Renewability Message）を使って，無効化すべき機器の一覧を共有する仕組みを持ち，ここに記されている機器との通信を拒絶する仕組み

⑵ あるAVストリームを受信可能な受信デバイス数の上限を定め，無制限なコピーを未然に防止する仕組み

DTCPは，国内のネットワーク対応のデジタル放送機器などに搭載が義務づけられており，また，IEEE1394（米国電気電子技術者協会規格1394）やUSB（Universal Serial Bus）などの各種の伝送路に対応した，伝送系著作権保護のデファクトスタンダードとなっている。

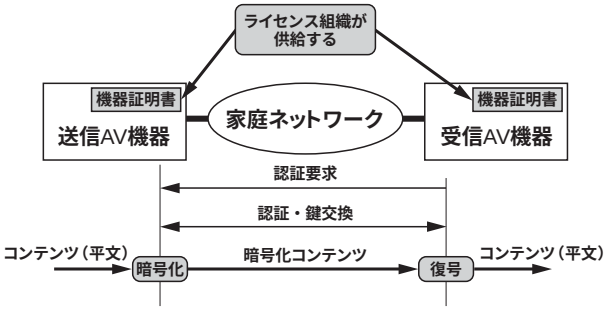

図3．DTCPの概要 ― DTCPでは，ライセンス組織が発行した機器証明書を使って認証・鍵交換が行われたうえで，コンテンツを暗号化し伝送を行う。
Outline of DTCP content protection system

2.2.2 適用例（IEEE1394）

IEEE1394は，その高速性（高精細度テレビ（HDTV）映像を数チャンネル伝送することが可能），同期転送機能や帯域予約などのAV伝送に適した特性を持っていること，上位にAV転送プロトコルが定義されていることから，デジタル放送対応機器などへの搭載が始まっている有線ネットワーク技術である。IEEE1394では，各種のAV制御コマンドがAV/C（Audio/Video Control）コマンドとして，各種フォーマットのAVデータの伝送仕様がIEC61883（国際電気標準会議規格61883）として，それぞれ定められている。IEEE1394向けのDTCPは，その認証・鍵交換がAV/Cのセキュリティコマンド上に，コンテンツの暗号化（と必要なコピー制御情報などの伝送）がIEC61883に追加する形でそれぞれ実現されている（**図4**）。

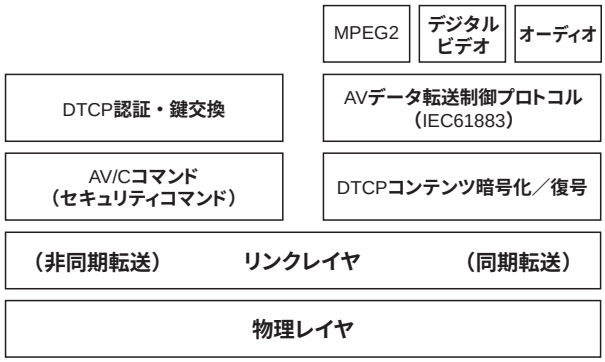

図4．IEEE1394プロトコルスタックにおけるDTCP ― IEEE1394においては，DTCPの認証・鍵交換は非同期転送のAV/Cコマンド上で，暗号化コンテンツの転送は同期チャネル上で行われる。

Content protection on IEEE1394

詳細は，この特集のp.36～39を参照されたい。

2.2.3　適用例（Bluetooth™ (注1)）　Bluetooth™は，小型，低消費電力，低価格などのモバイル通信に適した仕様を持つ近距離無線通信方式であり，携帯電話などのモバイル機器を中心として，コンシューマ機器への搭載が進んでいる。

Bluetooth™では，高品質オーディオアプリケーションのための仕様とプロファイルが定義されており，これらは著作権保護のサポートができるように考慮されている[3]。DTCPも，これにマッピングすることが可能である。Bluetooth™ AVに著作権保護を適用する場合の一般的なシーケンス例を**図5**に示す。Bluetooth™では，①サポートする著作権保護方式の確認，②通信で使用する著作権保護方式の設定，③著作権保護のための認証・鍵交換，④実際の暗号化，AVコンテンツの伝送，という手順で行われる。

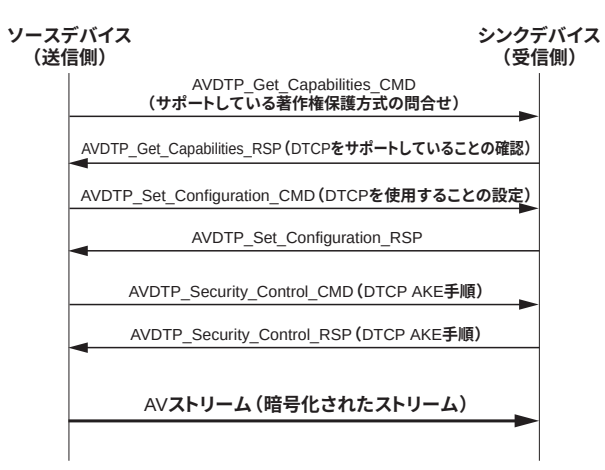

図5．Bluetooth™ AVにおける著作権保護のシーケンス例 ― 最初に，相手の機器がサポートしている著作権保護方式の問合せと方式の決定が行われ，続いて各方式の認証・鍵交換手順が行われる。

Content protection on Bluetooth™ AV

なお，Bluetooth™では“Bluetooth™ Security”なる，無線伝送路上の暗号化方式の規格が定められているが，DTCPとは目的が異なる（Bluetooth™ Securityはプライバシー保護の目的，DTCPは著作権保護が目的であり，対象とするレイヤが異なる）。このため，一般に“片方のセキュリティ方式を用いたことで，もう片方の目的にも流用する”（例えば，著作権保護を目的として，Bluetooth™ Securityをそのまま適用させる）といったことはできない。

2.3　家庭へのコンテンツの流入

家庭へのコンテンツの流入の経路は多様である。主なものとして，放送，ネットワーク，パッケージメディア（DVDなど）が挙げられよう。ここでは，家庭ネットワークの観点から，デジタル放送とコンテンツ配信の2点について説明する。

2.3.1　デジタル放送　国内では1996年にCS（通信衛星）デジタル放送が，2000年にBS（放送衛星）デジタル放送が開始され，更に2003年には地上波デジタル放送が開始される予定となっている。今後は，家庭での放送サービスの中心は，徐々にアナログ放送からデジタル放送に移行していくことが考えられる。

BSデジタル放送においては，有料デジタルコンテンツについてはスクランブルがかけられたうえで放送波上を伝送される。また，伝送されるMPEG-2（Moving Picture Experts Group-phase 2）-TS（Transport Stream）パケット内に，DTCP用のCCI（コピー制御情報）を埋め込むことが可能になっており，DTCPに準拠した受信機器（放送チューナ）は，ネットワーク上に受信した放送コンテンツを伝送する場合には，このCCIに従った制御を行うことが要求される。

2.3.2　コンテンツ配信（SDMIを例に）　家庭におけるPCの普及に伴って，デジタル音楽データの配信をインターネットを経由して行うためのフレームワークの検討がSDMI（Secure Digital Music Initiative）にて行われた[4]。SDMI規格では，①配信される音楽データに電子透かし（p.16～19を参照）を埋め込み，不正にコピーされた音楽データなどの再生を防ぐ，②“SDMIドメイン”なる考え方を導入し，配信経路から機器での蓄積，機器からの伝送などの一連の流れについて，暗号化の義務づけなどの要求条件を定めた。このルールは，一部の携帯電話への音楽配信などの基本ルールとなっている。

このほかにも，いくつかのコンテンツ配信の仕組みが提供されているが，それらの多くはPC向けの各社独自方式であり，現在のところ，コンシューマ機器も含めてサポートされるような一般的な方式は存在しない。

（注1）　Bluetoothは，Bluetooth SIG,Inc.の商標。

3 今後の展望

近年,“ ブロードバンド ”の通称で代表されるように，ADSLやFTTH技術を使った，広帯域のインターネットアクセスが急激に普及してきた。これに伴って，家庭内にもネットワークを敷設して，PCやプリンタなどをこれにつなぎ，インターネットアクセスやプリンタの共用化などを行うことが一般的になりつつある。こうした家庭内ネットワークの代表例がEthernet(注2)[5]，あるいはIEEE802.11無線LAN[6,7]である。

最近では，当社のDVDレコーダやTransCube™[8]のように，Ethernet端子や無線LANインタフェースを持ち，PCとつながることや，携帯電話からインターネット経由で遠隔操作ができることを特長とするデジタルAV機器が続々と登場している。このように，従来のIEEE1394に加えて，様々な伝送メディアが家庭内ネットワークに浸透していくことが考えられる。

これまで述べてきたように，現在の著作権保護技術は，DTCPに代表されるように伝送メディアごとに仕様が規定されていたり，放送や携帯電話によるコンテンツ配信など，伝送経路ごとに異なる技術が適用されていたりしている。例えば，現状ではパッケージメディア（DVDなど）で購入した映画と，放送波から送られてきた映画とでは，内容が同じコンテンツであったとしても異なる保護方式で蓄積される。一般消費者の視点に立つと，そのコンテンツがどのような著作権保護技術で保護されているかといったことに関して注意を払う必要がなく，AVコンテンツをPCでライブラリ化するなど，家庭内ネットワークにおいては著作権を遵守する限りにおいて，自由にコンテンツの閲覧や送受信を行いたいという要求は当然のことである

また，PCとAV機器，インターネットが融合することによって，今後は，自宅のホームサーバに蓄積したコンテンツを車や携帯電話などのモバイル機器，更には別荘など遠隔地から宅内ネットワークにアクセスして視聴するといったような，新しいサービスを提供する機器も登場するだろう。

このような家庭ネットワークやコンテンツの移動形態の多様化に伴い，従来のコンテンツ保護方式の枠を越え，メディア横断でコンテンツを取り扱えるようにするための技術が必要となると予想される。例えば，家庭内に接続されている機器を一つのドメインととらえ，お互いの機器が共通するドメインに所属していることを認証すれば，自由にコンテンツの移動や閲覧ができるといった概念が提案されている[9]。

しかし，従来の著作権保護技術は，あくまでその接続範囲が有線物理ネットワークにて制限されることを前提としていた。このため，接続範囲を拡張した場合，家庭内ネットワークをどのように定義するのか，その機器が同一人物によって保有されていることをどのように管理し認証するのか，その仕組みは利用者の使い勝手を低下させることなく実現可能なのかといった，これまで考えてこなかったような新しい課題を解決する必要があり，今後様々なアプローチから議論されていくものと思われる。

（注2） Ethernetは，富士ゼロックス（株）の商標。

4 あとがき

家庭ネットワークの観点から，著作権保護の現状と展望を概観した。今後は，デジタル放送やブロードバンド配信など家庭へのコンテンツの流入が更に多様化し，また家庭内においても，ネットワーク伝送媒体や次世代DVDなどの新しい蓄積メディアの登場により，新アプリケーションソフトウェアなど様々な動きがあると考えられる。前述のCPSAを考慮しつつ，これらの動きに対応した体系の検討，及び構築を行っていく必要がある。

文　献

(1) 4C Entity. Content Protection System Architecture. ＜http://www.4centity.com＞, (accessed 2003-4-8).
(2) Digital Transmission Licensing Administrator. Digital Transmission Content Protection specification. ＜http://www.dtcp.com＞, (accessed 2003-4-8).
(3) Bluetooth SIG. Bluetooth Audio/Video Distribution Transport Protocol Specification. ＜http://www.bluetooth.org＞, (accessed 2003-4-8).
(4) Secure Digital Music Initiative. ＜http://www.sdmi.org＞, (accessed 2003-4-8).
(5) IEEE802.3 (ISO/IEC 8802-3).
(6) IEEE802.11, 1999 Edition (ISO/IEC 8802-11: 1999).
(7) 高木雅裕, ほか. IEEE802.11の動向とその製品化状況. 東芝レビュー. **57**, 10, 2002, p.16－19.
(8) 佐藤重信, ほか. ワイヤレスメディアステーション TransCube™10. 東芝レビュー. **57**, 9, 2002, p.6－9.
(9) Lotspiech, J., et al. Broadcast encryption's bright future. IEEE Computer Magazine. **35**, 8, 2002.

斉藤　健　SAITO Takeshi

研究開発センター 研究企画室 企画担当参事。
ホームネットワークにおける研究・開発に従事。
Research Planning Office

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・セキュリティ技術に関する研究・開発に従事。
Computer Network Lab.