IEEE1394 コンテンツ保護システム
IEEE 1394 Content Protection System

加藤　拓 KATOH Taku
遠藤　直樹 ENDOH Naoki
山田　尚志 YAMADA Hisashi

IEEE1394(注1)は，ホームネットワークの担い手として急速に普及し始めている次世代ディジタル通信路の伝送規格である。今後，このIEEE1394がDVDプレーヤ，ディジタルVCR，ディジタル放送受信機などに装備されることが期待されている。しかし，これらの機器間で映画や音楽などのディジタル コンテンツ(ソフトウェアの中身や内容)を伝送する場合には，コンテンツが伝送路上から不正に盗まれてしまわないように，暗号化などを施すことでコンテンツを保護する必要がある。このシステムは，機器認証やコンテンツ暗号化などを備えたディジタル コンテンツの安全な伝送手段を提供するシステムである。

The IEEE 1394 standard for high-speed two-way digital networks will shape the digital home network. DVD players, digital VCRs, set-top boxes, and other devices will be equipped with the IEEE1394 interface. To transmit copyrighted content such as movies and music, it is necessary to protect it from unauthorized access because the copyright providers will not allow the transmission of such content if the device concerned does not support protection.

This paper describes the IEEE1394 content protection system, which is licensed by the digital transmission licensing administrator (DTLA) and offers protection satisfying the requirements of content providers.

1 まえがき

DVD(Digital Versatile Disc)，ディジタルVCR(Video Cassette Recorder)やディジタル放送などによって，家庭内でも高品位なディジタル映像／音声コンテンツを楽しめる環境が整いつつある。しかし，コンテンツの二次利用に関しては，コンテンツ提供者からの厳しい要求があるのが現実である。現在のアナログVCRではコピー防止信号が，CD(Compact Disc)では世代コピー管理情報がおのおのの実際に採用されており，高品位かつ劣化のないコピーが可能なディジタル コンテンツの場合には，さらに強い要求がある。そのため，伝送路上からコンテンツを不正に盗むことのできないシステムを作る必要がある。

ここでは，ホームネットワークの担い手として普及し始めているIEEE1394に対応したコンテンツ保護システムについて述べる。この保護システムは，コンテンツ提供者の要求を満たすコンテンツ保護技術を提供しており，これによって魅力のあるコンテンツを家庭内で扱うことができるようになる。

2 DFS(事実上の業界標準)化に向けての動き

不正コピー防止技術を検討するために，家電業界，パソコン(PC)業界，映画／音楽業界などが集まって業界団体CPTWG(Copy Protection Technical Working Group)が組織されており，そのサブグループであるDTDG(Digital Transmission Discussion Group)において，データ伝送時のコンテンツ保護技術が検討された。このシステムは，当社およびインテル社，松下電器産業㈱，㈱日立製作所，ソニー㈱(以下，5社と略記)が共同で提案した技術であり，5社が共同設立したDTLA(Digital Transmission Licensing Administrator, http://www. dtcp. com/)によって1998年9月から同技術のライセンスが開始されている。

このシステムは，ディジタル インタフェースのためのCableLabs(注2)OpenCableプロジェクトの要求に合致しており，ケーブル業界からの支持も受けている。また，このシステムを利用するためには，一定の会費を支払うことでライセンスが受けられ，さらに各機器ごとに機器証明書の発行手数料を支払うことで機器を製造することができる。

3 保護システムの構成

この保護システムは，大きく分けて以下の四つの要素から構成されている。

(1) 認証および鍵(かぎ)交換
(2) コンテンツ暗号化
(3) コピー制御情報
(4) システム リニューアビリティ

(注1) IEEEは米国電気電子学会のこと。
(注2) CATV(有線テレビ)を用いたマルチメディアサービスに必要な伝送方式の策定，送信機・受信機の互換性などを米国内でまとめている研究機関。

機器間でコンテンツの送受信を行うためには，まず互いに相手の機器を認証してコンテンツの暗号化に必要な鍵を共有する。ただし，保護コンテンツには，copy-never/copy-one-generation/no-more-copies の3種類の保護形態があるため，コピー形態に応じて次の二つのレベルの認証が用意されている。

(1) 完全認証　copy-never コンテンツを含むすべてのコンテンツ保護に使用可能

(2) 制限認証　copy-one-generation および no-more-copies コンテンツの保護に使用可能

DV(Digital Video)レコーダなどで，copy-never コンテンツを扱わない機器は，制限認証だけをサポートすればよい。当然ながら，copy-freely コンテンツの伝送にはこのような認証は必要ない。

コンテンツの暗号化には，すべての機器が共通にもつベースライン暗号として㈱日立製作所の共通鍵暗号M6が，オプション暗号として Modified Blowfish と DES(Data Encryption Standard)が定義されている。

コンテンツの提供者は，提供するコンテンツの保護形態を決め，それに対応したコピー制御情報(CCI:Copy Control Information)を設定する。送信機器によって暗号化されたコンテンツがどの形態で保護されているかを，受信機器が簡単に理解できるための情報として，CCI に対応した暗号モードインジケータ(EMI:Encryption Mode Indicator)がコンテンツには付けられている。なお，この EMI 情報がコンテンツ暗号化に使われているため，EMI を不正に書き換えて不正にコピーをしようとした場合には，暗号化されたコンテンツを正しく復号できないようになっている。

さらに，完全認証をサポートしている機器は，システムの完全性の維持と不正機器の排除を目的とした，SRM (System Renewability Messages)を処理することができる。SRM には不正機器のリストが含まれており，このリストに載っている機器からの認証および鍵交換の要求は受け付けないようになっている。

このコンテンツ保護システムの概要を図1に示す。

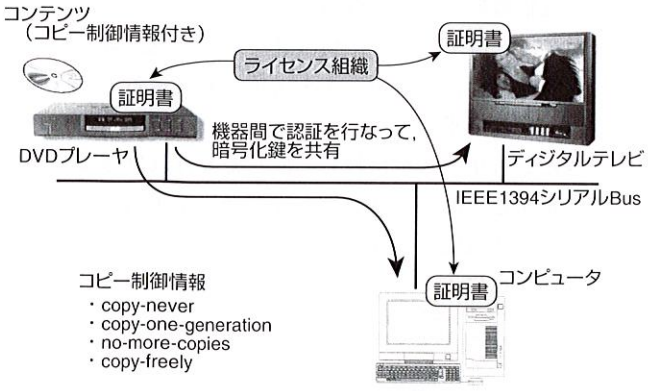

図1．IEEE1394 コンテンツ保護システム　コンテンツのコピー制御情報に従って，暗号化されたコンテンツを送信する。

IEEE1394 content protection system

4 コンテンツ保護プロトコル

このシステムのプロトコル(注3)を図2に示す。コンテンツの送信側を送信機器，受信側を受信機器と表し，機器間では以下の処理が行われる。

(1) 送信機器はコンテンツの CCI に従って，適切な保護を掛けた暗号化コンテンツを送信する。その際には，対応する EMI を付ける。

(2) 受信機器は EMI を見て暗号化コンテンツの保護状態を調べる。保護状態が copy-never である場合は，完全認証を要求し，それ以外の場合にはどちらかの認証を要求する。

(3) 互いに認証および鍵交換を行う。ただし，受信機器からの要求が完全認証であっても，送信機器が制限認証しかサポートしていなければ制限認証が行われる。

(4) 認証および鍵交換が終了すると，コンテンツ暗号化鍵(以下，コンテンツ鍵と略記)の交換が可能になり，受信側は暗号化コンテンツを復号できるようになる。

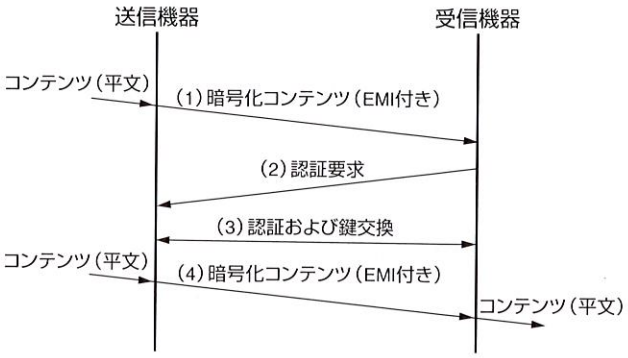

図2．コンテンツ保護の流れ　EMI 情報によって保護状態を確認し，認証および鍵交換を行なった上で，暗号化コンテンツを受信する。

Flow of content protection

5 認証および鍵交換

5.1 完全認証

完全認証は，ディジタル署名アルゴリズム EC-DSA(Elliptic Curve Digital Signature Algorithm)と鍵交換アルゴリズム EC-DH(Elliptic Curve Diffie-Hellman)を利用して

(注3)　データ送受信のための手順や規約。

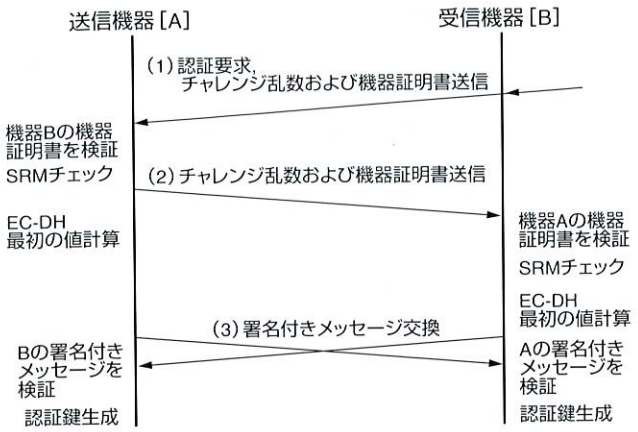

図3．完全認証　copy-never を含めすべての保護コンテンツの伝送に使用可能な認証方式である。

Full authentication

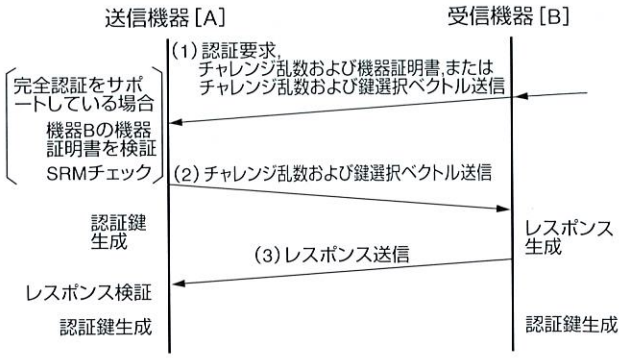

図4．制限認証　copy-one-generation と no-more-copies である保護コンテンツの伝送に使用可能な認証方式である。

Restricted authentication

おり，copy-never を含めすべての保護コンテンツの伝送に使用することができる。完全認証は図3および以下に示す手順で実行される。

(1) 受信機器は自身が生成したチャレンジ乱数と自身の機器証明書(Certificate)を送ることによって認証を要求する。

(2) 送信機器は自身が生成したチャレンジ乱数と自身の機器証明書を送り返す。互いのチャレンジ乱数と機器証明書が交換されると，各機器は DTLA の公開鍵を用いて，EC-DSA によって相手の機器証明書の正当性を検証する。もし，署名が正当でなければ認証処理を中止する。署名が正当であれば，相手の機器がすでに廃止された機器でないかどうかを，SRM 内の証明書廃止リスト(CRL：Certificate Revocation List)を調べる。相手機器が廃止されていなければ，EC-DH 鍵交換の最初の値を計算する。

(3) ステップ(2)で計算された EC-DH 鍵交換の最初の値や SRM に関連した値を含んだ“メッセージ”と，相手のチャレンジ乱数を含んだメッセージに対する“署名”を，互いに交換する。各機器は相手機器から送られてきた機器証明書に格納されている相手機器の公開鍵を用いて，EC-DSA によって相手機器から送られてきた署名の正当性を検証する。受信した署名が，自身が送ったチャレンジ乱数を含んだメッセージに対応する正当な署名でなければ認証処理を中止する。正当な署名であれば，相手が正当な機器であると認証し，EC-DH によって認証鍵の生成を行うとともに，SRM の更新処理を行う。

以上の処理によって，互いに同じ認証鍵が共有される。

5.2 制限認証

制限認証は計算能力の制限された機器で使用するための認証手段である。制限認証は，チャレンジ乱数に応答するためのハッシュ関数と共通の秘密を利用しており，保護状態が copy-one-generation と no-more-copies である保護コンテンツの伝送に使用することができる。制限認証は図4および以下に示す手順で実行される。

(1) 送信機器が完全認証をサポートしている場合には，受信機器は自身が生成したチャレンジ乱数と自身の機器証明書を送るが，送信機器が制限認証だけをサポートしている場合には，自身が発生したチャレンジ乱数と自身の鍵選択ベクトルを送ることによって認証を要求する。

(2) 送信機器は，自身が生成したチャレンジ乱数と自身の鍵選択ベクトルを送り返す。さらに，完全認証をサポートしていれば DTLA の公開鍵を用いて，EC-DSA によって受信機器の機器証明書の正当性を検証し，正当であれば SRM 内の CRL によって受信機器が廃止されていないかどうかを調べる。これらの検証で問題がなければ，受信機器が正当であると判断する。受信機器が正当でない，あるいは CRL に登録されている場合には，認証を中止する。続いて検証鍵を生成する。

(3) 受信機器は，送信機器からのチャンレンジ乱数を受信後，自身で生成した検証鍵を用いて認証鍵とレスポンスを求め，レスポンスを送信機器に送る。送信機器は，自身で求めたレスポンスと受信機器から送られてきたレスポンスを比較し，同じでなければ認証処理を中止する。同じであれば，受信機器が正当であると認証し，認証鍵を生成する。

以上の処理によって，互いに同じ認証鍵が共有される。

6 コンテンツ暗号化

暗号化コンテンツを送受信するためには，機器間で事前に完全認証または制限認証を完了しておく必要がある。送

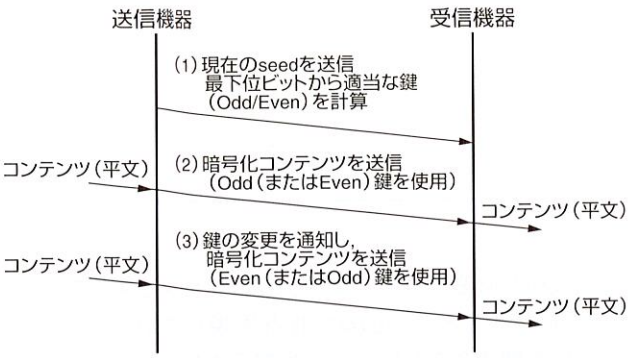

図5．コンテンツ鍵の確立と更新　コンテンツ暗号化に必要な鍵の設定とOdd/Evenビットを利用した暗号化鍵の更新方式である。
Content channel establishment and management

信機器は，共有された認証鍵で暗号化した交換鍵を受信機器に送信する。コンテンツ鍵の確立と更新は図5および以下に示す手順で実行される。

(1) 送信機器は，コンテンツ送信の際に乱数を発生し，コンテンツ鍵を計算するために必要な値(seed)の初期値とする。初期値は，最下位ビットの値からOdd(最下位ビットの値が1)あるいはEven(最下位ビットの値が0)として参照される。

(2) 送信機器は，初期値に対応したOddあるいはEvenのコンテンツ鍵を用いて，コンテンツの送信を開始する。コンテンツが，Odd/Evenのどちらのコンテンツ鍵で暗号化されているかを示すために，IEEE 1394のパケットヘッダ(注4)内の1ビットが用意されている。

受信機器はseedを受信すると，その最下位ビットがOdd/Evenビットと一致しているかを確かめる。同じであれば，現在のコンテンツ鍵を計算し，違っていれば，鍵が更新されたと判断して，新しいコンテンツ鍵を計算する。送信機器はseedの値を増やして，あらかじめ次のコンテンツ鍵を生成しておく。

(3) 送信機器は，コンテンツ保護の耐性を維持するために，コンテンツ鍵を定期的に更新しなければならない。鍵を更新するために，送信機器はあらかじめ計算しておいた新しい鍵を用いて暗号化を開始するとともに，IEEE1394パケットヘッダ内のOdd/Evenビットを反転することによって，鍵が更新されたことを受信機器に伝える。なお，コンテンツ鍵は30秒から120秒の間で更新される。

(注4) 分割されて伝送されるデータの一つ一つをパケットと呼ぶ。また，受信側で元の連続した値に戻すために必要な情報が各パケットごとに付けられているが，この付加情報が付けられている部分をパケットヘッダと呼ぶ。
(注5) テレビにCATVやインターネットを接続するための装置。

7 システムリニューアビリティ

システムリニューアビリティは，システムの完全性の維持と不正機器の排除を目的としている。完全認証をサポートしている機器は，DTLAが作成し，新しいコンテンツや新しい機器を使って配布されるSRMを受信することが可能である。SRMは，自身よりも新しいリストをもった正当な機器，DVDなどの記録済みメディアあるいは外部との通信手段(インターネット，電話線，ケーブルなど)を備えた正当な機器から更新することができる。なお，これは認証および鍵交換が完了した後で実行されるべき処理である。

この機能を備えることによって，新しく現れた不正機器に対しても，正当機器では認証要求を拒絶するといった対応がなされる。

8 あとがき

ディジタルコンテンツが広まるにつれ，不正コピー防止技術は非常に重要になってきている。個々の機器ごとにもいろいろな方式が検討されているが，それらの機器をつなぐ伝送路上での保護も重要な問題である。今後，ディジタルテレビ，STB(Set Top Box)(注5)，DVD，PCなどさまざまな機器にIEEE1394インタフェースが装備され，そのなかの多くの機器は，コンテンツ保護が必要な情報を扱うことになるだろう。

そのような状況において，この技術は重要な役割を担っていくことが期待されている。

文　献

(1) 5 C Digital Transmission Content Protection White Paper Revision 1.0, http://www.dtcp.com/, 1998.
(2) 高橋史忠，浅見直樹．IEEE1394のコピー防止技術，公開鍵／共通鍵併用で一本化．日経エレクトロニクス．712, 1998, p.47-53.


加藤　拓　KATOH Taku, D.Eng.
情報・社会システム社 SI技術開発センター SI技術担当，工博。情報セキュリティ技術および応用システムの研究・開発に従事。電子情報通信学会会員。
System Integration Technology Center


遠藤　直樹　ENDOH Naoki
情報・社会システム社 SI技術開発センター 戦略企画担当主幹。情報セキュリティ技術および同技術応用システムの開発に従事。電子情報通信学会，日本セキュリティマネジメント学会会員。
System Integration Technology Center


山田　尚志　YAMADA Hisashi
ディジタルメディア機器社 首席技監。アナログLSIの研究・開発，LSI用CAD，DVD，コピープロテクションシステムなどの開発に従事。IEEE，電子情報通信学会会員。
Digital Media Equipment & Services Co.