Keywords you should know. 第5回

知っておきたいキーワード

DTCP-IP

嶋　久登†

†ソニー株式会社 技術開発本部 MT開発部
"DTCP-IP" by Hisato Shima (Media Technology Development Dept., Sony Corporation, Tokyo)
キーワード：DTCP-IP，DTCP，AKE，PCP，RTT，EMI，DLNA，ホームネットワーク

DTCP

DTCP (Digital Transmission Content Protection) は，DTLA (Digital Transmission Licensing Administrator, http://www.dtcp.com/) がライセンスする著作権保護技術です．DTCPはIEEE1394やUSBなど，いろいろなインタフェース上で規定されており，IPインタフェースのためのものをDTCP-IPと呼びます．家庭内のディジタルコンテンツは，さまざまな著作権保護技術で守られています．例えば，デジタル放送の保護には，CAS (Conditional Access System) 技術が使われており，DVDコンテンツにはCSS (Content Scramble System) やCPRM (Content Protection for Recordable Media) などの技術が使われています．これらのコンテンツを，送信側の機器 (ソース機器) がDTCP-IPでの保護に変換して，ホームネットワークに出力し，受信側の機器 (シンク機器) は，DTCP-IPに対応することで，ホームネットワークの互換性が実現できます．

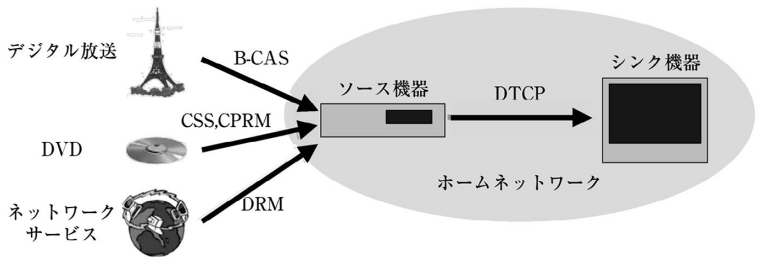

図1　DTCPの仕組み

AKE

通信相手が正規のライセンスを得た機器であるかどうかを確認したうえで，鍵の共有を行うため手順をAKE (Authentication and Key Exchange: 認証および鍵共有) と呼びます．DTCP-IPでは，この認証のために，各機器はDTLAが発行する証明書を持っています．この証明書には，DTLAの署名と各機器の公開鍵が入っています．AKE手順では，この証明書のDTLAの署名を確認するとともに，鍵共有のパラメータを交換するときに相手の機器の署名を確認します．これにより，DTCPのライセンスを受けていない機器が，コンテンツの暗号化のための鍵を取得することを防止しています．

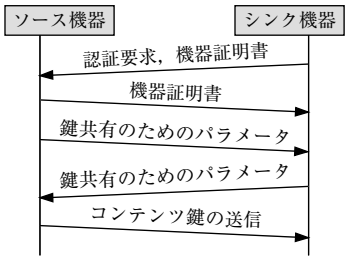

図2　AKEの手順

映像情報メディア学会誌 Vol. 60, No. 5, pp. 746～747 (2006)

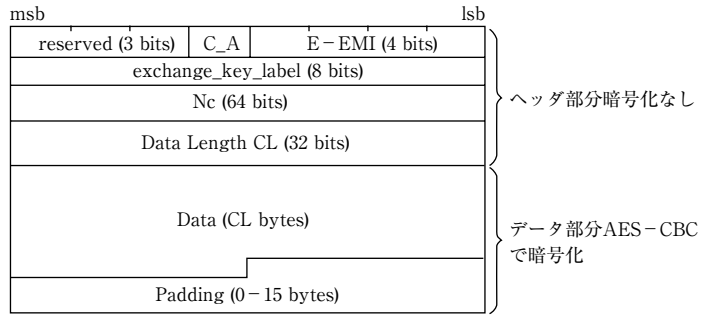

図3　PCPの構造

表1　E－EMI

EMI	暗号化モード	意　味
1100	Mode A0	コピー禁止（Copy Never）
1010	Mode B1	1世代コピー可（Copy One Generation）
1000	Mode B0	1世代コピー可（Copy One Generation）
0110	Mode C1	コンテンツ移動中（Move）
0100	Mode C0	再コピー禁止（No More Copies）
0010	Mode D0	暗号化は行うが制限なしにコピー可（EPN）
0000	暗号化なし	制限なしにコピー可（Copy Free）

DTCP-IPのコンテンツ暗号化

DTCP-IPでは，コンテンツのフォーマットに依存せずにコンテンツを暗号化して伝送するために，PCP（Protected Content Packet）と呼ばれる構造を使います． PCPの構造を**図3**に示します．ヘッダ部分には暗号化モードを示すE-EMI（Extended Encryption Mode Indicator），コンテンツ鍵の更新に用いるNc，コンテンツの長さを示すCLなどのフィールドがあります．コンテンツは16バイトの整数倍になるように，パディングしたうえで，AES-CBCの暗号化をします．

E-EMIは，**表1**に示すように，コンテンツのコピー制御情報に対応しています．

伝送のローカライズ

IPネットワークを用いると，著作権保護されたコンテンツのコピーや視聴が，通常の家庭内での使用を超えて行われる懸念があります．インターネットなどを通しての伝送ができないようすることを，伝送のローカライズと呼びます．

DTCP-IPでは，TTL（Time to Live）による制限と，ソース機器とシンク機器の間の往復遅延時間（RTT: Round Trip Time）による制限で，伝送のローカライズをしています．

具体的には，AKE手順での通信でTTLを3以下とすることで，ルータを3段以上通した認証はしないようにしています． また，往復遅延時間が7ms以内であると確認できなければ，鍵共有を行わないようにしています．

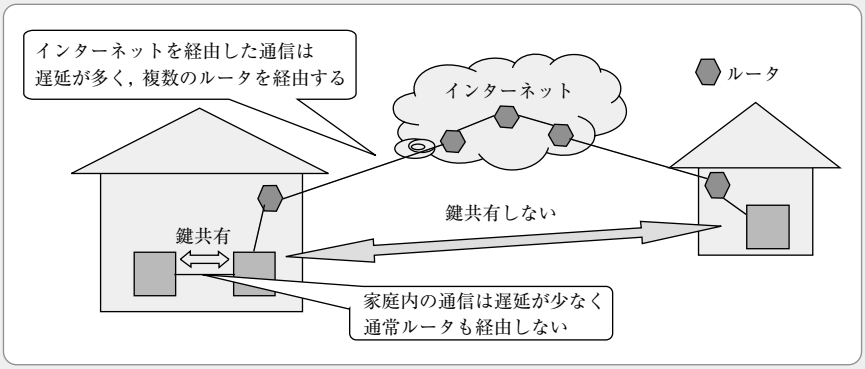

図4　伝送のローカライズ

嶋　久登（しま　ひさと）　1983年，大阪大学大学院工学研究科機械工学専攻修了．同年，ソニー（株）入社．1987年，米国スタンフォード大学より，MSCS取得．1993年より，同社にて，IEEE1394およびIPネットワークを用いたホームネットワークの開発に従事．

DTCP-IPとホームネットワーク

DTCP-IPは，DLNA（Digital Living Network Alliance）で規定されているIPホームネットワークの技術と組合せて使われます．

DTCP-IPとDLNAを用いたコンテンツ伝送の全体の流れは，次のようになります．

まず，シンク機器はDLNAの規定にしたがって，ソース機器からコンテンツのリストを取得します．ユーザはコンテンツリストから視聴するコンテンツを選択します．選択されたコンテンツがDTCP-IPで暗号化されるコンテンツである場合は，ソース機器とシンク機器の間でDTCPのAKEとローカライズの確認を行います．この後で，シンク機器はコンテンツ伝送を要求し，ソース機器はコンテンツをDTCP-IPで暗号化して送信します．シンク機器はAKEで入手した鍵を用いて，受信したコンテンツを復号します．

（2006年2月28日受付）

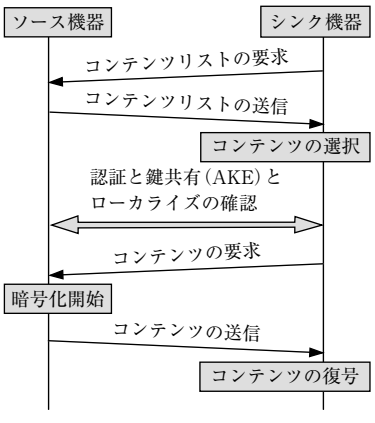

図5　コンテンツ伝送の流れ