M-089

通信ネットワーク利用放送における映像暗号鍵管理方法の提案

Proposal of a key management method for the broadcast service using the Internet

小尾 高史 1　鈴木裕之 2　谷内田益義 2　山口雅浩 2　大山永昭 3
Takashi Obi　Hiroyuki Suzuki　Masuyoshi Yachida　Masahiro Yamaguchi　Nagaaki Ohyama

１．はじめに

通信と放送の融合を望ましい形で実現するには、高精細動画像の安定した配信技術を構築するだけでなく、同時に通信ネットワークの持つ特性である双方向機能を有効に活用した放送技術が必要になる。特に、通信が１対１を原則とした情報の伝送方式であるのに対して、放送は１対不特定多数との間で情報を共有することを目的とした伝送方式であり、現在の放送技術では、視聴者の受像機の性能等によらず同一の情報を送信する必要があり、たとえスケーラブル符号化を適用した映像メディアを配信する場合においても、視聴者が閲覧可能なコンテンツの品質とそれに対する価値・対価とのバランスをとることが難しい。本研究ではこれら課題を解決するために，オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤として研究開発が進められている Secure e-Key Network (SeKNW)を利用してネットワーク接続機器の安全確実な利用のための認証を実施し，認証結果に基づいて利用可能な機能や情報を制御するシステムを提案する。

２．鍵管理配送システム

２．１構成要素

本システムを実現するために必要な構成要素には、鍵管理配送を実現するための機器管理機関、放送サービス登録センタ、放送局、機器組み込み型多機能ＩＣチップ（e-Key チップ）搭載映像受信機器がある。本論文では鍵管理配送システムを e-Key チップの管理運用モデルとして検討が進められているフレームワークである Secure e-Key Network[1] と整合性を取るために必要となる改良を実施するとともに、それぞれの機関の役割の整理を行った。以下に要素とその役割について説明する。

- 機器管理機関

利用者が購入した映像受信機器を、利用者との契約により登録、管理代行する機関。この機関において、機器内に配置された認証用デバイスである e-Key チップの状態管理を行うとともに、放送サービス登録センタに対して、映像受信機の性能等に対する保証を行う。

- 放送サービス登録センター

放送サービスを受けるために、利用者がその利用申請を行う機関。機器管理機関から映像受像機へのサービス搭載許可書を取得し、e-Key チップに対して機種に対応した放送サービスを利用するためのサービス利用ＡＰをダウンロードする。さらに、サービス利用ＡＰに対して、映像管理鍵を設定する。

- 放送局

放送サービスを行う主体。放送サービス登録センタにより管理される映像メディアパッケージ化の鍵を利用して、暗号化されたストリーミングを放送する。

- e-Key チップ搭載映像受信機器

e-Key チップを搭載し、放送サービスにより提供されるストリーミングデータを受信する機器。ストリーミングデータの復号鍵は、e-Key チップに配送されるが、復号化処理自体は機器内で行われる。

ネットワークを利用して機器に映像メディアを配信する場合、映像メディアがサーバ側の管理を離れて流通、利用される可能性があるばかりでなく、通信路上で傍受された映像メディアが不正に利用されることも考えられる。図１に示す課題を解決するためには、ネットワークを通じて放送サービスを受ける機器が、放送局との間で相互の正当性を認証でき、その上で認証結果に基づいて利用可能な機能や情報を制御できる必要がある。

２．２ 機器登録・映像管理鍵管理システムの検討

ここでは、映像メディアアクセス制御を実現する際の、機器の登録、放送サービス利用の登録、放送受信時のそれぞれのシーンにおける処理の検討を行った。

- 製造時における映像受信機器の登録

本シーケンスについては、Secure e-Key Network フレームワークで検討されている登録手順を利用することになるため、本来は利用者は購入した映像受信機器を機器管理機関に登録し、登録されたことを認証するための鍵をチップ内に埋め込むことになる。しかしながら、放送サービスの実施に関しては、利用者の個人情報を保護する観点から、機器利用機関への個人情報の登録なしに、当フェーズと同じ機能を実現する仕組みが必要となると考えられる。この場合、機器管理機関を業界団体等が設置し、機器製造段階であらかじめ e-Key チップ内に機器登録鍵及び機器機能を

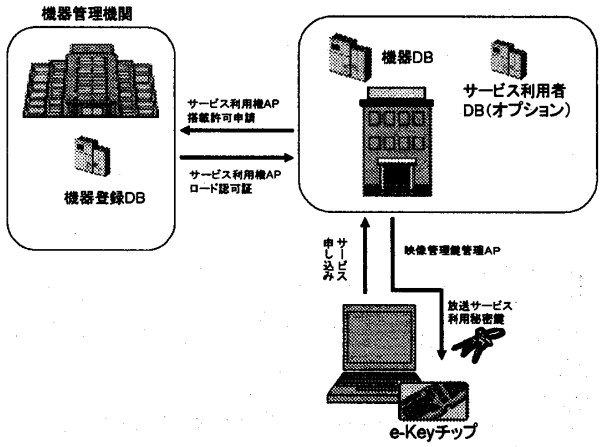

図１ 放送サービス登録

1　東京工業大学総合理工学研究科
2　東京工業大学像情報工学研究施設
3　東京工業大学フロンティア創造共同研究センタ

証明するための機器登録書を設定しておくことが必要となる。

- 放送サービス利用登録

放送サービスの利用に当たっては、放送サービスの利用登録を行う必要がある。この際機器の性能等に応じて、機器に応じた映像管理鍵の管理を行うチップアプリケーションが配送される。また、チップアプリケーションには、放送サービス登録センタの発行する機器に応じた放送サービス利用秘密鍵及びそれに対応する公開鍵証明書が格納され、機器が特定の品質の映像を受信可能かどうかの管理及び機器の認証に利用される。また、有料放送などを提供するサービスを受ける際には、放送サービス登録センタに対して利用者は個人情報を提供し、サービス利用者情報の登録を行う必要がある。

- 放送受信

放送サービス提供時には、映像受信機器からの要求に従い、放送サービスを利用するための鍵（映像メディアを復号するために利用する鍵を生成する映像管理鍵）が配送される。通信ネットワークを利用した放送サービスは、マルチキャストを利用したストリーム配信を行うことが想定されているため、放送受信時の鍵配送については、映像受信機器に近いエッジルータについても e-Key チップを搭載し、一定の時間間隔で放送サービス登録センタはエッジルータ内の e-Key チップに対して、映像管理鍵を配送することを想定する。この際、映像受信機器は、エッジルータとの間で放送サービス利用権の認証を行い、利用権に応じた映像管理の配送を受けることになる。

３．基本機能検証プロトタイプシステムの開発

上記提案システムの基本機能を検証するために、放送サービス登録センタとしての役割を持つ登録認証サーバ、多機能ＩＣカードにより e-Key チップを模擬した映像受信機器、放送局を想定した配信サーバからなる実験システムを構築し、機器の性能に基づくサービス登録及び鍵配送を行う実験を行った。

具体的な実験手順は以下のとおりになる。

１．利用に際しては，機器の性能に基づくサービス登録から実施することとなるため，まず，製造メーカにより予め e-Key チップに格納しておく情報として，機器登録証，登録認証サーバ公開鍵証明書の検証用公開鍵証明書，これに対応する秘密鍵を設定する．この際，機器登録証には，機器の性能に関する情報が書き込まれているものとする．

２．利用者は，映像受信機内の e-Key チップに保持されている機器登録証を放送サービス登録センタに送付し，放送サービス登録センタは機器登録証の機器製造メーカの署名を検証し，機器の機能を取得する．さらに機器の e-Key チップとの間で相互認証を行い，通信先の機器の正当性を確認した後，機器の機能に応じた放送サービス利用秘密鍵及び放送利用許可証（公開鍵証明書）を設定する．

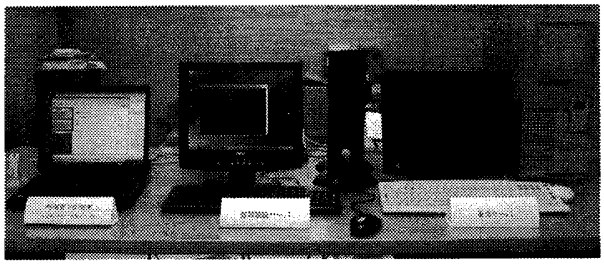

図３　基本機能検証プロトタイプシステム
（右から配信、登録認証各サーバ、チップ搭載機器）

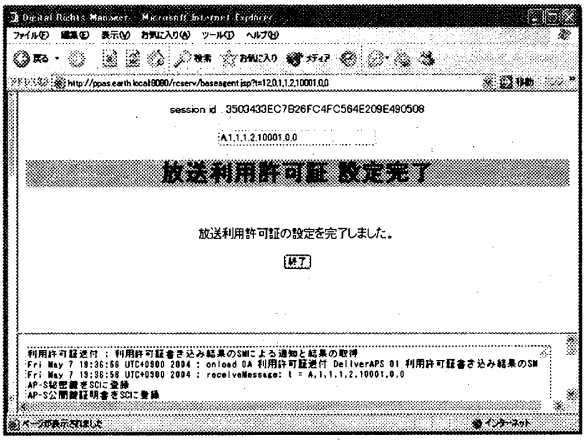

図２　機器に対する放送利用許可書の設定

３．放送受信時には，放送サービス登録センタ（又はエッジルータ）が放送利用許可書を利用して機器の認証を行い，認証後に放送サービス利用秘密鍵により設定されるセキュアメッセージングにより e-Key チップに対して直接映像管理鍵を送付する．

４．e-Key チップは，この映像暗号鍵より複数のストリーミングデータ暗号鍵を生成し，放送局より送信される暗号化ストリームデータを復号化することで利用者に対して放送コンテンツを提供する．現段階では，チップ内での暗号鍵生成を行う手法が確立されていないため，３で送付された映像管理鍵と IPSec 用のセッション鍵は同一のものとして扱っている．

そしてこれら実験システムを用いて，機器の登録及び異なる品質の映像メディアへのアクセスを許可する映像管理鍵を配送可能であること確認した。

４．まとめ

映像メディアアクセス管理のための鍵配送技術の研究として、スケーラブル映像メディアアクセス管理に必要となる鍵配送方法の決定及び提案方法の検証のためのプロトタイプシステムの構築を行った。しかしながら、視聴者が閲覧可能なコンテンツの品質とそれに対する価値・対価とのバランスをとるためには、異なる品質のコンテンツ毎に異なる暗号鍵を用いて配信する必要があり、e-Key チップ内で複数の鍵生成を行う手法の検討を今後進めていく必要がある。

謝辞

本研究の一部は、情報通信研究機構の委託研究「通信ネットワーク利用放送技術の研究開発」により行なわれた。

参考文献

１．小尾他、オープンネットワーク環境で安全な鍵配送を実現するネットワーク基盤として研究開発-Secure e-Key Network-,電子情報通信学会総合大会，2004.