有料モバイル音声放送方式
Pay Mobile-Audio Broadcasting System

秋山　浩一郎 AKIYAMA Koichiro
上林　達 KAMIBAYASHI Tooru
由良　浩司 YURA Koji

有料放送を実現するには，契約者にだけ視聴可能となるような技術が必要である。衛星テレビジョンで実施されている有料放送方式は，契約情報を受信装置ごとに定期的に送信することで高い安全性を実現している。反面，契約情報の送信量が多く，送信帯域が限定され，かつ常時受信が期待できないモバイル環境でのディジタル音声放送事業においては，契約情報の送信量を減らす改良が望まれている。

当社では，マスター鍵(かぎ)の共通化および契約情報のイベント型送信によって契約情報の送信量を減らすとともに，最先端の暗号技術を用いることによって，モバイル環境であっても現行システムと同程度の安全性をもつ方式の開発に成功した。

A pay broadcasting system is a conditional-access(CA) system which provides information only to those who have concluded the necessary contract. Current CA systems for satellite broadcasting offer high security by periodically transmitting CA information to each receiving apparatus. However, these systems are required to transmit a large amount of CA information. The need has therefore arisen for improvements to reduce the amount of CA information, especially in the case of mobile-audio broadcasting systems which have a restricted band and cannot expect to receive CA information regularly.

In response to this problem, we have employed new concepts for both key configuration and event-driven transmission, which have decreased the amount of data to be transmitted. In addition, the application of advanced cryptographic technologies enable a system that is supported in the mobile environment to be as secure as current systems.

1 まえがき

有料放送を実現するためには，放送局側で番組コンテンツをスクランブルして送信し，受信装置側ではその復号鍵(チャネルキー)を別途放送局から送付された契約情報に基づいて制御する必要がある。契約情報の送付はコストや安全性などの観点から図1のように暗号化して放送波にのせて送信する方式が一般的である。

ここで，各契約情報には契約対象の受信装置の識別子(受信装置ID(IDentification))が記載されおり，各受信装置では自受信装置のIDが記載された契約情報だけを選択的に受信する。

衛星テレビジョン放送では，放送帯域が広いことから契約情報をすべて個別情報として送信する方式が採用されている。この方式は送信量が多いが，確実に契約者だけに限定視聴できるという特徴がある。

一方，近年計画されている(車のような)モバイル環境下での音声放送においては，放送帯域が狭く，常時受信が期待できないため現行方式をそのまま適応することができず，契約情報の送信量の削減が強く望まれている。

ここでは，契約情報を復号するマスター鍵を共通化し，情報を圧縮するとともに，契約情報を無期限化することにより，個別情報の送信量を削減し，ディジタル署名を始めとする最新の暗号技術を導入することで現行方式と同程度の安全性を確保する当社方式について述べる。

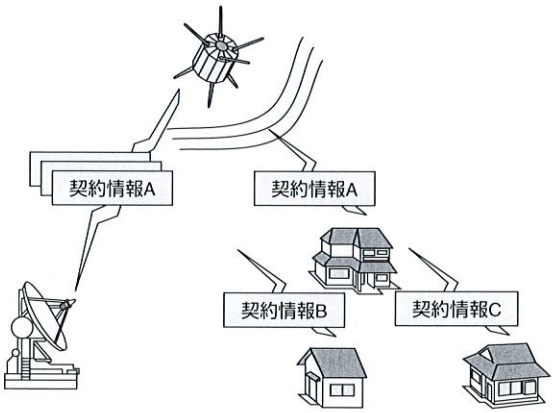

図1．放送波による契約情報送付　契約情報は放送波にのせて送信する。
Conditional-access information broadcast

2 有料衛星テレビジョン方式

現行の有料衛星テレビジョン受信装置は図2のような契約情報による受信管理を行なっている。この方式を送信量

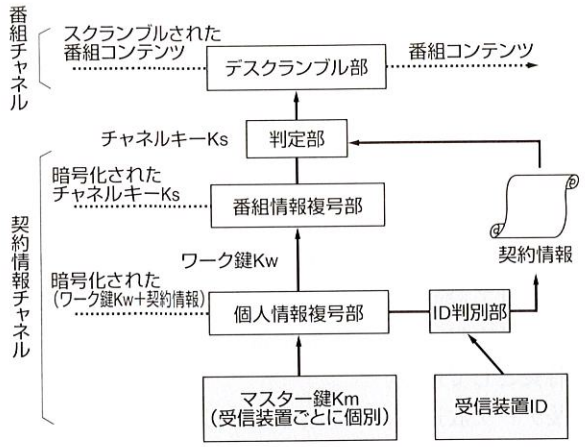

図2．現行の有料放送方式　受信装置個別のマスター鍵で契約情報が暗号化されているため送信量が多い。

Current pay broadcasting system

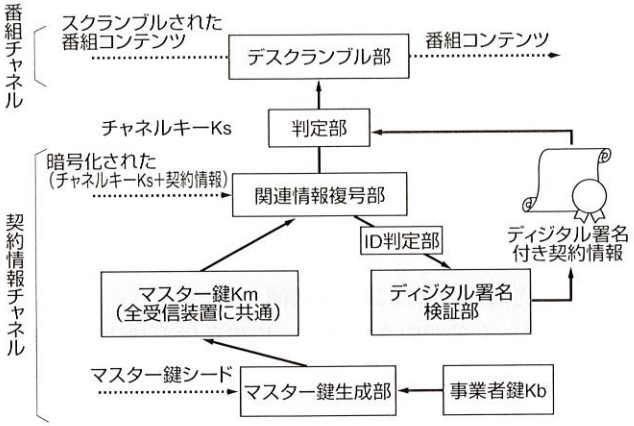

図3．有料モバイル音声放送方式　マスター鍵が共通であるため送信量が削減されるうえ，契約情報に付加されたディジタル署名により契約情報の偽造が防止できる。

Pay mobile-audio broadcasting system

の観点で見ると，次のような特徴がある。

(1) マスター鍵の個別化　契約情報が受信装置ごとに個別に保持されているマスター鍵で暗号化される。

(2) 契約情報の有期限化　契約情報に有効期限が設定されており，有効期間ごとに契約情報を送信する。

このため，一つの受信装置を分解してマスター鍵を獲得した場合でも，その他の受信装置にまでは適用できないうえ，契約情報の受信拒否が一定期間以上は不可能となるなど安全性が高い方式になっている。

3 有料モバイル音声放送方式の概要

車のようなモバイル環境下での音声放送においては，放送帯域が狭く，常時受信が期待できないことから個別情報の送信量を削減したうえで繰り返し送信を行う方式が求められる。

この意味で現行方式は送信量が多く，送信量削減のための改良が必要になる。図3はこの課題を解決するため当社が開発した方式である。

この方式では，受信装置はつねに契約情報チャネルを受信し，番組視聴時は視聴するチャネルも同時に受信する。番組コンテンツは放送局側でチャネルキーKsによって暗号化されて送信される。チャネルキーKsは同時受信している契約情報チャネルで個別受信装置あての個別契約情報とともに図4のような形式でパケット化され，暗号化されて送信される。

契約情報パケットの暗号化には共通のマスター鍵Kmが使われ，マスター鍵は契約情報チャネルで随時送信されているマスター鍵シードから事業者鍵Kbを使って定期的に更新される。

図4．モバイル音声放送の契約情報パケット　マスター鍵が共通なので，複数受信装置の契約情報を1パケットにまとめて送信できる。

Conditional-access information packet for mobile-audio broadcasting

受信装置は契約情報パケットを順次復号し，契約情報を抽出して契約情報に含まれる受信装置IDと受信装置内の受信装置IDを比較して，自装置あての契約情報が存在すればその契約情報を不揮発性メモリに格納する。

さて，番組視聴時はチャネルIDから契約情報を参照して，契約情報において当該チャネルの視聴が許可されている場合には送信されてきた契約情報パケットに含まれるチャネルキーKsの中から当該チャネルのチャネルキーKsを取り出して，デスクランブル部に出力する。許可されていない場合はデスクランブルを行わないことにより契約管理を行う。

4 有料モバイル音声放送方式の特長

この方式は以下の特長により，契約情報の送信量を削減し，モバイル音声放送に対応した有料放送システムとなっている。

4.1 マスター鍵の共通化

共通のマスター鍵で暗号化することにより，図4に示すように同一の契約情報パケットに複数の契約受信装置あての契約情報を包含することが可能になり，図5に示す現行方式と比較して，契約情報を圧縮して送信することが可能となった。

図5．現行の契約情報パケット　マスター鍵が受信装置ごとに異なるため，受信装置ごとにパケットが必要。
Current conditional-access information packet

4.2 契約情報のイベント型送信

契約情報に有効期限を設けず，情報送信を契約変更時だけとすることで，送信の絶対量を削減した。

5 安全対策

この方式は送信量を削減するため，現行方式と比較し，以下の２点において安全性が低下している。まず，マスター鍵が共通であるため，契約情報が偽造される可能性が高くなった。また，契約情報がイベント型で送信されるため受信拒否による解約後視聴の可能性もある。このため以下のような安全対策が施されている。

5.1 契約情報の偽造防止対策

契約情報の偽造は，公開鍵暗号によるディジタル署名によって防止する。すなわち，契約情報にはすべてディジタル署名を付加し，自受信装置あての契約情報を含む契約情報パケットを取得した際には，公開鍵(予め受信装置内に埋め込まれている)でディジタル署名を検証する。

公開鍵暗号のディジタル署名は放送局側にしか存在しない秘密鍵で生成されるため，受信装置内を分析しても偽造のための情報を見出すことはできない。このことにより偽造を防ぐことができる。また公開鍵暗号方式には署名データ量を小さくするため楕円曲線暗号方式が効果的である。

5.2 契約情報の受信拒否対策

受信拒否は契約情報とチャネルキーを一体化して暗号化することにより解決している。すなわち，契約情報パケット内部にチャネルキーを包含し，契約情報を受信拒否するとチャネルキーが得られず，番組コンテンツを視聴できないという関係になるように設計している。チャネルキーを比較的頻繁に変更することにより十分に受信拒否を防ぐことができる。

6 あとがき

ここで述べた有料放送方式は車で視聴する音声放送の特質に合わせて設計したものであるが，現行方式と同程度以上の安全性を保った上で契約情報の送信量が削減されることを特長としている。

今後データ放送などのさまざまな形態のディジタル放送サービスが事業化されているなかで，モバイル音声放送に限らず数多くの応用があるものと考えられる。

文　献

(1) 小林喜三郎, 他. 有料テレビジョン放送設備, 東芝レビュー, **47**, 6, 1992, p.474-476.

秋山　浩一郎　AKIYAMA Koichiro
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研究主務。セキュリティ技術の開発に従事。電子情報通信学会会員。
Computer & Network Systems Lab.

上林　　達　KAMIBAYASHI Tooru
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研究主務。セキュリティ技術の開発に従事。応用数理学会会員。
Computer & Network Systems Lab.

由良　浩司　YURA Koji
情報・社会システム社 SI技術開発センター主務。セキュリティ技術の開発に従事。電子情報通信学会会員。
System Integration Technology Center