有料モバイル音声放送における限定受信方式の設計

秋山 浩一郎[†,☆] 上林 達[†] 由良 浩司[††]

日本初の自動車向け有料モバイル音声放送（モバイル放送）が 2004 年春を目処に開始される．モバイル放送は有料放送であるため，従来の衛星放送と同様に視聴契約者のみが視聴可能とする限定受信方式が必要になる．一方で，移動体に適した S バンドを利用するため帯域が狭い（256 Kbps）ことから，多くの限定受信情報が送信できず，従来の方式では無料視聴防止の観点において十分な安全性が確保できない．そこで著者らは従来方式の鍵構成を変更し，限定受信情報の送信頻度を工夫することによって，安全性を確保しながら送信すべき限定受信情報を大幅に削減できる方式を提案した．本稿では，著者らが提案したモバイル放送の限定受信方式とその設計指針，ならびにその標準化の状況について述べる．

Conditional Access System Design for Subscription Mobile Audio Broadcasting

Koichiro Akiyama,[†,☆] Toru Kamibayashi[†] and Koji Yura[††]

The first subscription mobile audio broadcasting (mobile broadcasting) service in Japan is to be launched in spring 2004. Mobile broadcasting requires a conditional access system (CAS) that provides service only to those who have concluded the necessary contract, like the current subscription satellite broadcasting. However, mobile broadcasting uses a restricted band (256 Kbps) within the S-band. The current CAS is unable to provide sufficient security at an acceptable cost, because that is necessary to transmit a large amount of CAS data. To tackle this problem, the authors have employed a new key configuration and event-driven transmission, thereby decreasing the amount of data to be transmitted. In this paper, we describe our CAS adapted for mobile broadcasting and its design concept and the present state of standardization.

1. はじめに

デジタル放送は情報圧縮技術の導入により，従来の 10 倍以上の情報送信が可能になり，次世代の放送方式として，BS/CS 衛星放送を中心に実用化が始まっている．特に CS 放送では 100 チャネルを超える豊富なコンテンツと最新の映画などの高付加価値コンテンツが提供されており，有料放送としてすでに 200 万以上の加入者を有するものとなっている．

このような中，日本初の自動車向け有料モバイル音声放送（モバイル放送）が 2004 年春を目処に開始される．モバイル放送は自動車や電車で移動中でもクリアな音声放送が提供できるばかりでなく，カーナビをはじめとする車載情報システム向けのデータ放送としても期待されている．だが一方で移動体での受信に適した，携帯電話と類似の S バンドを使用するため放送帯域が狭く，1 チャネルに割り当てられる伝送容量が 256 Kbps にすぎないという問題点がある☆☆．その一方で，モバイル放送ではこの帯域を利用して音楽番組を約 60 チャネル，簡易動画番組を約 10 チャネルの計 70 チャネル程度を提供し，高品質なサービスを目指すために，有料放送を前提としている．

有料放送を実現するためには，受信契約者のみが視聴可能となるアクセス制御方式が必要である．このようなアクセス制御方式は限定受信方式（conditional access system）と呼ばれており，現行方式では放送コンテンツを全受信装置に共通のワーク鍵で暗号化して送信し，ワーク鍵は契約情報とともに契約期間（1 カ

† 株式会社東芝研究開発センター
R&D Center, Toshiba Corporation
†† 東芝ソリューション株式会社 SI 技術開発センター
Systems Integration Technology Center, Toshiba Solutions Corporation
☆ 現在，中央大学大学院理工学研究科
Presently with Graduate School of Science and Engineering, Chuo University

☆☆ これは CS 放送の 1 チャネル 4 Mbps と比べると 1/16 でしかない．

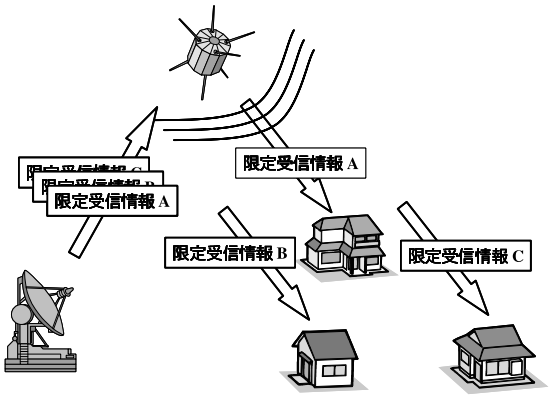

図 1 限定受信情報の送受信
Fig. 1 Conditional access data transmission.

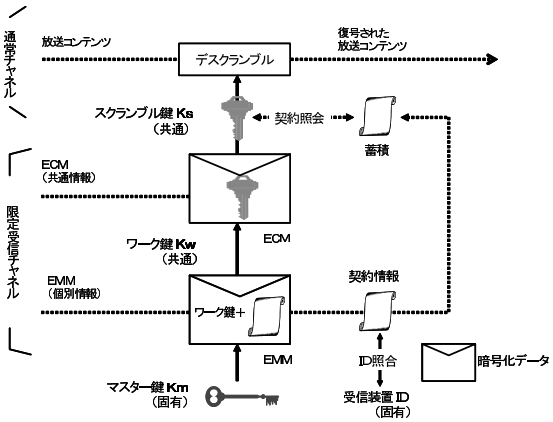

図 2 現行の限定受信方式
Fig. 2 The current conditional access system.

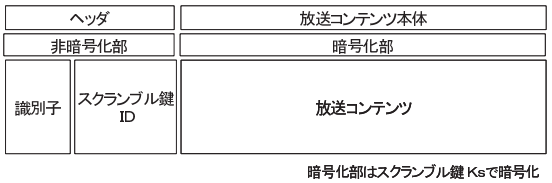

図 3 放送コンテンツの構成
Fig. 3 The structure of broadcasting contents.

月）ごとに受信装置個別に設定されたマスタ鍵で暗号化して，定期的に送信する 3 段鍵方式が採用されている[1),4)]．ここで放送コンテンツをデスクランブルするために必要な情報，すなわち現行方式におけるスクランブル鍵，ワーク鍵ならびに契約情報などは限定受信情報と呼ばれており，限定受信情報をいかに安全かつ効率的に受信契約者に配信するかという問題が限定受信方式の設計上最大の問題点となっている．もちろん限定受信情報のうち個別の受信装置向けの情報（本稿ではこれを個別限定受信情報と呼ぶ）を郵送など放送によらない手段で行ってもよいが，現状ではコストがかかるため放送によって配信する方式が通例である．すなわち，現行方式の個別限定受信情報には対応する受信装置の ID が記載されており，各受信装置は**図 1** のように自装置の ID が記載された限定受信情報のみを選択的に受信することによって正確な配信が可能となる．

CS 放送では帯域が広いため，1 カ月に 1 回の割合で個別限定受信情報を更新する現行方式が採用でき，安全性も高いが，狭帯域放送では 1 カ月ごとにすべての契約受信装置に対し個別限定受信情報を送信することは効率的とはいえない．さらに，モバイル放送は狭帯域であることに加えて，移動体向けであるため，自動車が車庫に入っていたり，受信装置が地下など受信不可能な位置に置かれていたりすることも多く，常時受信が期待できない．以上のことから現行方式をそのままの形で適応することができず，限定受信情報の送信量削減が強く望まれていた．

本稿では，2 章で従来方式とその問題点を詳しく述べ，3 章でモバイル放送における限定受信方式の要求条件をより具体的に述べる．4 章では 3 章の要求条件を受けて提案した限定受信方式の概要と設計方針を述べ，5 章ではその特徴をまとめる．6 章においては提案方式の送信量の評価を行い，提案方式がモバイル放送において実現可能であることを示す．7 章では提案方式の無料視聴に対する安全性を検証し，8 章では 4 章で示したような機能が LSI で実現できることを示す．さらに 9 章では提案方式の標準化動向について触れる．

2. 従来の限定受信方式とその問題点

現行の BS/CS 放送の限定受信方式は**図 2** のように構成され，受信装置は限定受信情報が送信される限定受信チャネルを常時受信し，番組視聴時には当該チャネルの放送コンテンツが送信される通常チャネルをあわせて受信する．

本章では現行方式において限定受信チャネルと通常チャネルで配信される情報の内容および，限定受信処理の概要とその問題点について述べる．

2.1 通常チャネル

通常チャネルにはスクランブル鍵 K_s で暗号化された放送コンテンツが送信される．

放送コンテンツは**図 3** に示すようにヘッダ部に識別子とスクランブル鍵 ID を含み，本体はヘッダ部に記述されたスクランブル鍵 ID に対応するスクランブル鍵 K_s で暗号化された放送コンテンツで構成されてい

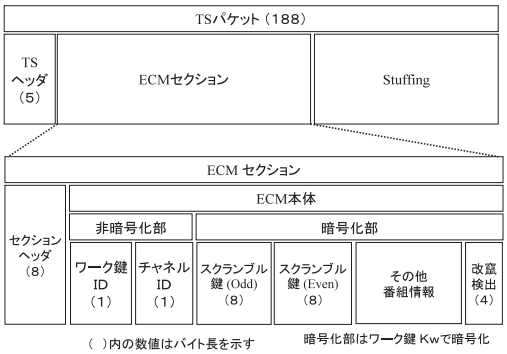

図 4 ECM の構成
Fig. 4 The structure of ECM.

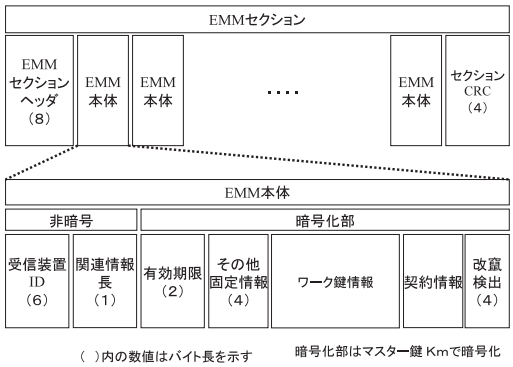

図 5 EMM の構成
Fig. 5 The structure of EMM.

る．ここでスクランブル鍵 ID は odd/even の 1 ビットの情報である．

2.2 限定受信チャネル

限定受信チャネルには ECM（Entitlement Control Message）と呼ばれる契約者に共通の限定受信情報（**図 4** 参照）と EMM（Entitlement Management Message）と呼ばれる契約者個別の限定受信情報（**図 5** 参照）が混在して送信される．なお，ECM と EMM は TS（Transport Stream）ヘッダ（5 bytes）に書かれた識別子で識別され，後に述べるように別々に処理される．

2.2.1 ECM

ECM は図 4 に示すように TS パケット（188 bytes）中の ECM セクションとして記述され，1 つの ECM セクションにはセクションヘッダ（8 bytes）のほかに 1 つの ECM 本体が含まれている．ECM 本体は非暗号化部と暗号化部に分れ，非暗号化部にはワーク鍵 ID（1 byte）とチャネル ID（1 byte）が含まれ，それぞれ暗号化部を復号するためのワーク鍵の識別情報，暗号化部にある 1 組のスクランブル鍵が利用されているチャネルの識別子を表している．また，スクランブル鍵は放送コンテンツの標準的な暗号化方式である Multi2 の復号鍵（8 bytes）で，odd/even が 1 組として送信される．その他の番組情報には当該番組の録画の可否情報など，より詳細な利用制限情報が含まれており可変長である．さらに最後に改竄検出コード（4 bytes）が付加されている．

2.2.2 EMM

EMM は TS パケット（188 bytes）中の EMM セクションとして記述され，図 5 に示すように 1 つの EMM セクションにはセクションヘッダ（8 bytes）のほかに複数の EMM 本体が含まれている．EMM 本体は非暗号化部に受信装置 ID（6 bytes）と関連情報長（1 byte）を含み，関連情報長に示すだけのバイト長が受信装置 ID の有するマスタ鍵で暗号化されていることを示している．暗号化部には有効期限（2bytes），その他固定情報（4 bytes）および改竄検出コード（4 bytes）とともにワーク鍵情報および契約情報が可変長☆で含まれている．なお，これらの長さは放送サービスによっても異なる．

2.3 限定受信処理の概要

このような構成の下で現行の限定受信処理は以下のように行われる（図 2 参照）．

受信装置は，まずワーク鍵と契約情報を（限定受信チャネルで定期的に送られる）EMM から取得する．EMM は個別情報であり，復号鍵は（受信装置内に）個別に設定されたマスタ鍵 K_m であるので，EMM の非暗号化部にある受信装置 ID を自装置の ID と比較して一致したときのみ復号処理を行う．こうして得られたワーク鍵 K_w はワーク鍵 ID とともにワーク鍵メモリに，契約情報は契約情報メモリに蓄えられる．

次に得られたワーク鍵をもとに ECM を順次復号し，スクランブル鍵を取得する．ここでワーク鍵は順次更新されるので，ECM のヘッダ部にあるワーク鍵 ID に対応した ID を持つワーク鍵をワーク鍵メモリ内から検索して抽出する必要がある☆☆．取得されたスクランブル鍵はチャネル ID に対応したスクランブル鍵メモリに蓄えられる．

通常チャネルで送信される放送コンテンツを視聴する際は，契約情報メモリ上の契約情報で当該チャネル

☆ ワーク鍵は通常，チャネルごとに設定され，契約者により契約しているチャネル数に差があるためワーク鍵情報の長さは可変である．

☆☆ 鍵の更新の際には（受信中断を防ぐために）新しい鍵をそれが使われる前に送信して，（現在使われている鍵とともに）メモリに蓄積しておくことが原則となる．よって同時に 2 つ以上の鍵がメモリ上に存在することになる．

表 1 現行の 3 段鍵構成
Table 1 The current 3 key configuration.

鍵	役割	固有/共通	更新頻度	更新頻度の理由
スクランブル鍵	放送コンテンツの復号	共通	1 回/1 秒	既知平文攻撃の回避
ワーク鍵	スクランブル鍵の復号	共通	1 回/1 カ月	契約単位が 1 カ月
マスタ鍵	ワーク鍵の復号	受信装置固有	更新せず	最上位鍵であるため

が受信可能であることが確認される．確認された段階でヘッダ部からスクランブル鍵 ID の odd/even にしたがって対応したスクランブル鍵を抽出し，復号を行う．なお，これらの処理は IC カードなどの内部のデータを簡単に書き込み/読み出しできない耐タンパ構造のハードウェア内で行われることを前提としている．したがって（放送波によらず）契約情報を改竄することはきわめて困難である．

2.3.1 鍵構成と更新頻度

この限定受信処理を鍵構成の点で見ると**表 1** に示すような 3 段の鍵構成になっていることが分かる．このような鍵構成と更新頻度になった理由は以下のとおりである．放送コンテンツのスクランブル方式である Multi2 に対する既知平文攻撃を避けるため 1 秒に 1 回程度の頻度でスクランブル鍵を更新する必要がある[6]が，このスクランブル鍵を個別の受信装置に設定されたマスタ鍵で暗号化し，すべての受信装置に対して送信することは送信量の点で不可能である．そこでチャネルごとに，すべての受信装置に共通のワーク鍵 K_w が設定され，変更されるスクランブル鍵を順次暗号化して ECM として送信する．またワーク鍵 K_w は契約期間（通常 1 カ月）ごとに EMM で変更することにより，当該チャネルを解約した加入者には新たなワーク鍵を送信しないことで，確実な契約管理が可能となる．

2.4 現行限定受信方式の問題点

現行方式は安全性の高い方式であるが，個別限定受信情報（特にワーク鍵）を更新するため，EMM を定期的にすべての契約者に送信しなくてはならず送信量が膨大となっている．このため広帯域の BS/CS 放送で可能であっても，狭帯域しか確保できないモバイル放送では実現が難しい．さらに，モバイル放送は移動体での受信であるため常時受信が仮定できない．このため同一の EMM を従来よりも長い期間繰り返し送信しなくてはならないため，現行方式では鍵更新が間に合わずに契約していても受信が途切れる可能性が高い．

このような問題点を解決するためモバイル放送向けに新しい方式を開発しなければならなかった．

3. 有料モバイル音声放送の要求条件

2004 年春の運用開始に向けて準備を行っている有料モバイル音声放送（モバイル放送）は**図 6** に示すように自動車や電車などで移動中でも高品質な放送が楽しめる新しい形態の衛星放送である．だが，使用帯域が移動体に適した S バンドであるため帯域が狭く，1 チャネルに 256 Kbps 程度の伝送容量しか割り当てられない．そこで当面は音声放送を主体とした 70 チャネル程度でサービスを開始する予定である．また，高品質なサービスとするため小額ながら視聴料金を徴収する有料放送とすることが決まっている．加入者については営業開始 3 年で 200 万加入者を実現し，その後最大 1,000 万加入者まで伸びることを想定している．

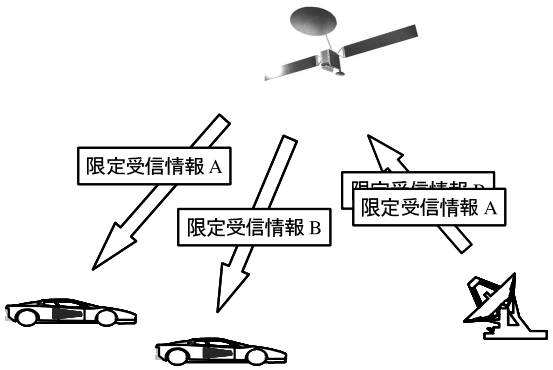

図 6 有料モバイル音声放送
Fig. 6 Subscription mobile audio broadcasting.

表 2 システム運用上の要求条件
Table 2 Requirements concerned with system management.

	条件
最大加入件数	1,000 万件
限定受信チャネルの送信容量	256 Kbps
受信状態	不定期受信

3.1 放送システムに関する要求条件

モバイル放送は有料放送であるため限定受信方式を導入し，限定受信チャネルに 1 チャネル（256 Kbps）を割り当てることになっている☆．以上のことから**表 2** に示す運用上の要求条件があげられた．

☆ これは従来の衛星放送における限定受信チャネルの伝送容量の 1/16 であるが，限定受信チャネルを増設することは通常チャネルを圧迫することになるので運用上許容できるものではない．

表 3 契約送信件数に関する前提条件
Table 3 Requirements concerned with contract data transmission.

送信事由	送信頻度	理由
新規加入	12 万件/月	装置耐用年数を 7 年に設定
解約	12 万件/月	新規加入と同数に設定
変更	84 万件/月	1 回/年で契約変更をする

表 4 契約情報の送信頻度に関する要求条件
Table 4 Requirements concerned with frequency of contract data transmission.

送信事由	送信頻度	理由
新規加入	1 回/15 分	現行の衛星放送と同程度
解約	1 回/1 時間以上	長期にわたっての送信が前提
更新	1 回/15 分	現行の衛星放送と同程度

3.2 契約変更件数と送信頻度に関する要求条件

効率的に限定受信情報を送信するためには送信事由によって契約情報の送信頻度を変える必要がある．このため契約変更件数に関して**表 3** に示す前提条件を設定する．なお，加入者は 1,000 万人で平衡状態に達すると考えているため，新規加入件数と解約件数は同数に設定している．さらに，送信事由ごとに契約情報の送信頻度を決定する必要がある．契約情報の送信頻度は加入者に届くまでにかかる時間と関係があり，**表 4** のように要求されている．

4. 有料モバイル音声放送の限定受信方式の設計

前章において限定受信情報（特に個別限定受信情報）の送信頻度を現行の衛星放送と同様にしつつ，現行の 1/16 の帯域に収めなくてはならないという要求条件が示された．そこで，有料モバイル音声放送（モバイル放送）では現行方式と同程度の安全性を保ちつつ，限定受信情報の大半を占める個別限定受信情報を大幅に削減する必要がある．これには以下の 2 つの方法が考えられる．

(1) 個別限定受信情報を圧縮．
共通の鍵で暗号化することで情報圧縮を図る．

(2) 個別限定受信情報の送信機会を削減．
定期的な送信を削減し，変更時のみの送信を基本とする．

これらの観点から以下に述べる個別限定受信情報を共通のワーク鍵で暗号化して圧縮し，イベント型に送信する新しい限定受信方式を設計した．**図 7** が有料モバイル音声放送（モバイル放送）限定受信方式の概念図である．受信装置は（受信状態にあるとき）限定受信情報が送信される限定受信チャネルを受信し，番組

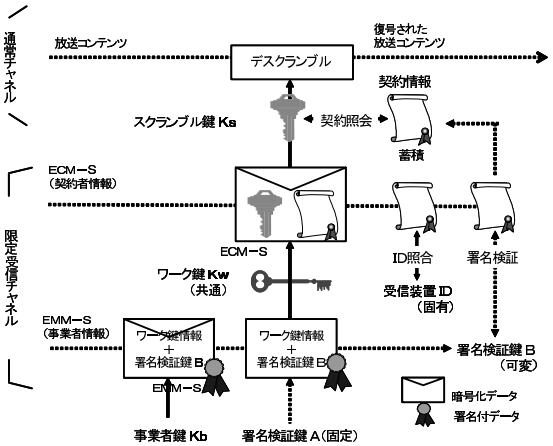

図 7 有料モバイル放送の限定受信方式
Fig. 7 Proposed conditional access system for subscription mobile broadcasting.

視聴時にはさらに当該チャネルの放送コンテンツが送信される通常チャネルを受信する．

4.1 通常チャネル

通常チャネルは現行方式と同様にスクランブル鍵 K_s で暗号化された放送コンテンツが送信される（図 3 参照）．

4.2 限定受信チャネル

契約情報チャネルには ECM-S（Entitlement Control Message for S-band）と呼ばれる契約者情報（**図 8** 参照）と EMM-S（Entitlement Management Message for S-band）と呼ばれる事業者情報（**図 9** 参照）が混在して送信される．なお，ECM-S と EMM-S は TS ヘッダ部に書かれた識別子で識別され，後に述べるように別々に処理される．

4.2.1 ECM-S

ECM-S は図 8 に示すように TS パケット中の ECM-S セクションとして記述され，1 つの ECM-S セクションにはセクションヘッダ（3 bytes）のほかに 1 つの ECM-S 本体が含まれている．ECM-S 本体には非暗号部と暗号化部があり，非暗号化部にはワーク鍵 ID（1 byte）が含まれており，暗号化部を復号するためのワーク鍵の識別情報となっている．また暗号化部には契約情報とその有効期限（2 bytes）およびデジタル署名（40 bytes），スクランブル鍵情報（17 bytes），改竄検出コード（8 bytes）が含まれている．契約情報は個別加入者向けの契約情報が書かれているがその形式に関しては 6.1 節で示す．また，スクランブル鍵情報には 1 組のスクランブル鍵（16 bytes）とそれが利用されているチャネル ID（1 byte）が記入されている．

提案方式の ECM-S は共通のワーク鍵で暗号化され

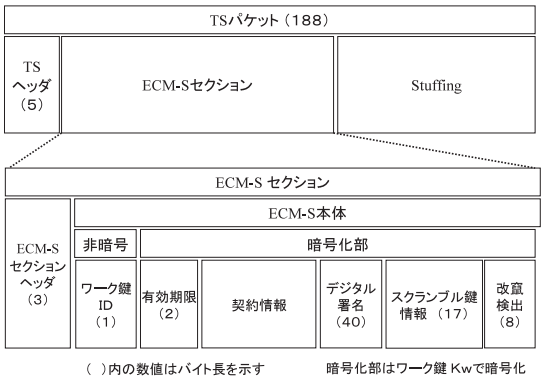

図 8 ECM-S の構成
Fig. 8 The construction of ECM-S.

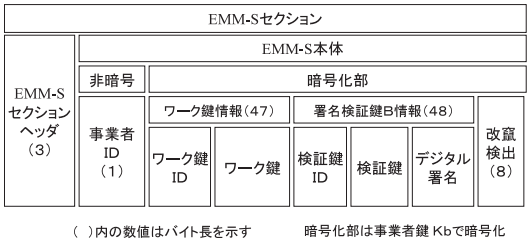

図 9 EMM-S の構成
Fig. 9 The construction of EMM-S.

ている一方で，共通限定受信情報であるスクランブル鍵以外に個別受信装置向けの契約情報を含んでいるところが特徴である．

4.2.2 EMM-S

EMM-S は TS パケット中の EMM-S セクションとして記述され，図 9 に示すように 1 つの EMM-S セクションにはセクションヘッダ（3 bytes）のほかに 1 つの EMM-S 本体が含まれている．EMM 本体は非暗号化部と暗号化部に分かれており，非暗号化部に事業者 ID（1 byte）が含まれ，暗号化部にはワーク鍵情報（47 bytes）と署名検証鍵 B 情報（48 bytes）と改竄検出（8 bytes）が含まれ，事業者 ID で示された事業者の事業者鍵 K_b で暗号化されている．ここで，ワーク鍵情報はワーク鍵更新のためのワーク鍵とその識別子の情報であり，署名検証鍵 B 情報は ECM-S におけるデジタル署名の検証のための（全受信装置共通の）署名検証鍵 B とその識別子の情報であって，楕円曲線暗号の署名検証鍵（40 bytes）が含まれている．

4.3 限定受信処理の概要

このような構成のうえで提案の限定受信処理は以下のように行われる（図 7 参照）．

まず，ワーク鍵情報と署名検証鍵 B 情報を（限定受信情報チャネルから定期的に送られる）EMM-S から取得する．EMM-S は放送事業者ごとに設定された事業者鍵 K_b で復号される．復号して得られたワーク鍵情報はワーク鍵とワーク鍵 ID とに分離され，ワーク鍵 ID とともにワーク鍵メモリに蓄えられる．署名検証鍵 B 情報も同様に署名検証鍵 B と署名検証鍵 ID に分離されたのち，署名検証鍵メモリに蓄積される．

ワーク鍵や署名検証鍵 B を変更する際は必ず事業者固有の署名検証鍵 A によるデジタル署名の検証を行う．これにより万一事業者鍵が露見した場合でもワーク鍵や署名検証鍵 B の偽造を防ぐことができる．また，署名検証鍵 A は事業者固有の鍵情報で更新されることはなく，一般に EMM-S で送信される署名検証鍵 B よりも鍵長が長いため，より解読されにくい．さらに，これらのデジタル署名には公開鍵暗号の中でも署名データサイズの小さい楕円曲線暗号を用い，送信量を節約している．

次に得られたワーク鍵をもとに ECM-S を順次復号し，スクランブル鍵および契約情報を取得する．ここでワーク鍵は表 5 のように更新を行うので，ECM-S のヘッダ部にあるワーク鍵 ID に対応したワーク鍵をワーク鍵メモリ内から検索して抽出する必要がある．

復号した結果得られたスクランブル鍵はチャネル ID，スクランブル鍵 ID とともにスクランブル鍵メモリに蓄えられる．同様に得られた契約情報は受信装置 ID と契約記述子に分離され，受信装置 ID は自装置の受信装置 ID と比較され，一致したときのみ署名検証鍵 B でデジタル署名を検証したうえで，対応した契約記述子を契約情報メモリに書き込む．提案方式では契約情報の有効期限を従来の 1 カ月から 1 年に伸ばし，実質的に契約変更時にしか送信を行わないようにしている．

通常チャネルで受信される放送コンテンツは契約情報メモリに蓄積された契約情報記述子によって当該チャネルが受信可能であることが確認される．確認された段階でヘッダ部からスクランブル鍵 ID を抽出し，この ID に対応したスクランブル鍵をスクランブル鍵メモリから取得して，復号される．

4.4 鍵構成と更新頻度

この限定受信処理を鍵構成とその更新頻度の点で見ると**表 5** 上段に示すように現行方式では受信装置固有であるマスタ鍵を事業者固有の事業者鍵とする新 3 段鍵方式となっている．また現行方式においてマスタ鍵で暗号化されている契約情報を提案方式では共通のワーク鍵で暗号化するように鍵の役割を変更することにより 6 章に示すような送信量の大幅削減に成功した．さらに，提案方式では表 5 下段に示すようにデジ

表 5 新 3 段鍵構成
Table 5 The proposed 3 key configuration.

鍵	役割	固有/共通	更新頻度	更新頻度設定の理由
スクランブル鍵	放送コンテンツの復号	共通	1 回/10 秒	既知平文攻撃の回避
ワーク鍵	スクランブル鍵と契約情報の復号	共通	1 回/月程度	ワーク鍵の露見時対策
事業者鍵	ワーク鍵の復号	事業者固有	更新せず	最上位鍵であるため
署名検証鍵 B	契約情報の署名検証	共通	1 回/月程度	署名検証鍵 B の露見時対策
署名検証鍵 A	署名検証鍵 B 情報の署名検証	事業者固有	更新せず	最上位鍵であるため

表 6 1 時間あたりの契約情報送信頻度
Table 6 Contract data transmission frequency par hour.

	1〜2 週	3〜4 週	5 週〜2 カ月	3〜6 カ月
新規加入	4 回			
解約	2 回	2 回	2 回	1 回
更新 1	4 回			
更新 2	4 回	4 回		

タル署名の検証鍵を 2 段鍵構成で実現している．

4.5 契約情報の送信頻度

モバイル放送では常時受信が仮定できないことから，車載ラジオの平均視聴時間しか限定受信チャネルを受信できないという前提で検討した．車載ラジオの平均視聴時間は平日 8 分，土曜 7 分，日曜 5 分のようにかなり短い[3]．本研究では視聴時間を曜日によらず一律平均 5 分と考えて，各契約者に対して 1 時間あたりの送信頻度を**表 6** のように設定した．ここで更新 1 は契約者の自主的な契約変更による更新を意味し，更新 2 は契約情報の有効期限切れによる更新を意味する．

表 6 に示した頻度は，表 4 に示したモバイル放送の要求条件を満たすという理由ばかりでなく，以下のような考え方から設定されている．すなわち，新規加入者および契約変更者（更新 1）は早期受信を希望するので新規加入および契約変更時点から短い期間に頻度多く送信する．ここで，受信し損なった契約者には個別に追加送信することになるが，日常的に受信していれば件数はそう多くないと考えられる．表 6 の頻度であると 15 分待てば視聴可能となり，現行 CS 放送の実態と近い．

解約者は受信回避を行うことが考えられ，短期間に集中的に送信すると，受信回避の可能性が大きい．このため頻度を犠牲にし，解約時点から契約情報の有効期限である 1 年後まで頻度を抑えて送信する．上記の頻度であると（1 日 5 分の視聴時間を仮定すれば）最初の 2 カ月経過時点で，視聴し続けられるのは 10 万件に 2 件程度である☆．さらに，たとえ 2 カ月を超えて視聴できたとしても，1 年後には契約情報の有効期限が来るため確実に視聴できなくなるので無料視聴に対する事業者の損害はそう大きくない．

有効期限切れの更新者（更新 2）については更新と同様に早期受信を希望するので，継続契約を行った契約者に対しては継続契約を行った時点から 1 カ月間集中的に送信する．

5. 提案方式の特徴

本方式は以下のような特徴を持つ．

(1) ワーク鍵の送信量を大幅に削減
ワーク鍵を事業者固有の鍵で暗号化するため，全受信装置共通の情報として送信でき，送信量が大幅に削減された（6 章参照）．

(2) 個別情報の圧縮送信
個別受信装置向けの契約情報を共通のワーク鍵で暗号化するため 1 パケットに多数の契約情報を詰め込めるようになり，送信量が削減された（6 章参照）．

(3) 契約情報のイベント型送信
契約情報の有効期限を 1 年とし，送信を実質上契約変更時のみとすることで，送信量を削減した（6 章参照）．

(4) デジタル署名の導入
公開鍵暗号を使ったデジタル署名を施すことにより，データの偽造や流用を防止した（7 章参照）．

これらによって，現行方式と比較して同程度の安全性を保ちながら送信量の大幅な削減（93% 程度の送信量を削減）を実現している．

☆ 1 日の視聴時間が 5 分であり 30 分に 1 回のペースで送信していることから，ある 1 日に回避できる確率は 5/6．これが 2 カ月続くと $(5/6)^{60} (= 1.7 * 10^{-5})$ となり 2 カ月間視聴し続けられるのは 10 万件に 2 件程度である．

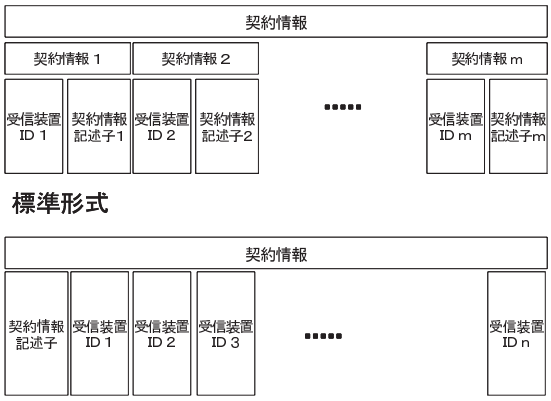

図 10 提案方式における契約情報の構成
Fig. 10 The construction of contract data in proposed system.

6. 限定受信情報の送信量評価

モバイル放送の前提条件の下で本方式と現行方式を限定受信情報（EMM と ECM）の送信量の観点から比較する．なお，モバイル放送においては受信装置 ID が 6 bytes，契約情報記述子が 70 チャネル相当分で 80 bits（=10 bytes）となっており，以下ではこれを前提に議論を進める．

6.1 TS パケットあたりの限定受信情報量の比較

現行方式での契約情報は契約情報記述子（10 bytes）だけからなり，ワーク鍵情報を含まない EMM 本体は 27 bytes となる（図 5 参照）．したがって 1TS パケットに詰め込める契約情報の数は TS パケットが TS ヘッダ，EMM セクションヘッダ，セクション CRC を含む 188 bytes であることから，6 となる☆．さらに，現行方式でのワーク鍵はサービスにより異なるが少なくともスクランブル鍵のサイズ（8 bytes）以上であり，契約情報を含まない EMM 本体は 25 bytes となる．したがって 1TS パケットに詰め込めるワーク鍵情報の数は 6 となる．

一方，提案方式では個別受信装置向けの契約情報を共通のワーク鍵で暗号化するため**図 10** 上段のように契約情報を構成することができ（標準形式），現行方式と同様の計算により，1TS パケットに 7 件の契約情報を詰め込こむことができる☆☆．さらに，同じ契約記述子を持つ受信装置 ID を集めて図 10 下段のような圧縮形式で記述することが可能で，圧縮形式では 17 件の契約情報を詰め込むことが可能である．

表 7 1 パケットに含まれる契約情報の数
Table 7 Number of contract data included one packet.

	送信形式	N/P	割合 (%)
現行方式	標準形式	6	100
提案方式	標準形式	7	30
	圧縮形式	17	70

以上により 1TS パケットに詰め込める契約情報の数（N/P）とその割合は**表 7** のように考えることができる．ここで標準形式と圧縮形式の割合はチャネル数が最大 70 であり，現状でもほとんどの契約者がパッケージ契約であることから圧縮形式がとれる場合が多いと考え設定した．一方，スクランブル鍵は 10 秒に 1 回の更新であるため，1 秒に 1 回程度の送信で十分であり，256 Kbps では 1 秒間に 174TS パケット流れるため 70 チャネル分のスクランブル鍵を提案方式で送信することにまったく問題はない．

また，現行方式のワーク鍵の送信頻度は（ワーク鍵の有効期限切れにともなうものなので）有効期限切れの契約更新（更新 2）と同じとし，かつ提案方式のワーク鍵情報を含む EMM-S の送信頻度を 1 秒に 1 回として計算する．

6.2 送信量の比較

以上のような準備の下で，**表 8** と**表 9** において 1 時間あたりに送信しなくてはならない限定受信パケットの数を比較する．まず，表 3 に示した 1 カ月単位の契約変更件数と，表 7 に示した 1 パケットに収まる契約情報件数およびその割合に基づいて，現行方式と提案方式の 1 時間あたりに送信しなくてはならないパケット数を算出する☆☆☆．これに表 6 で示した 1 時間あたりの送信頻度を掛けることで 1 時間あたりの送信量（送信パケット数）を算出する．なお，このとき当月送信しなければならない契約情報の件数は最大 1 年前の変更まで遡ることに配慮している．また新規加入に関しては 2 週間しか送信しないため，ある 1 時間をとってみると表 3 で示した件数の半分しか送信されていないことになる．そこで以下の計算においては新規加入の送信件数を表 3 の半分としている．このことは更新 1 に関しても同様である．

表 8 と表 9 にそれぞれ提案方式，現行方式の送信量を示した．これによれば現行方式が 1 時間あたり 7,826,668 パケット送信しなければならないのに対し，提案方式では 546,130 パケット送信するだけでよく，

☆ $(188-(5+8+4))/27 \approx 6.3$
☆☆ $(188-(5+3+1+2+40+17+8))/16 = 7$
☆☆☆ ここで表 8 の件数の右欄は表 7 の割合から算出されている．

表 8 提案方式での 1 時間あたりの契約情報送信量
Table 8 Number of packets par hour in proposed system.

	送信形式	件数 (N)		N/P	パケット数 (P)	頻度 (/H)	送信量 (P/H)
新規	標準形式	6 万	1.8 万	7	5,043	4	20,172
	圧縮形式		4.2 万	17			
解約	標準形式	12 万	–	–	7,059	2+2+1*10	98,826
	圧縮形式		12 万	17			
更新 1	標準形式	42 万	12.6 万	7	35,294	4	141,176
	圧縮形式		29.4 万	17			
更新 2	標準形式	84 万	25.2 万	7	70,589	4*1	282,356
	圧縮形式		58.8 万	17			
ワーク鍵	標準形式	1	1	1	1	3,600	3,600
合計							546,130

表 9 現行方式での 1 時間あたりの契約情報送信量
Table 9 Number of packets par hour in the current system.

	送信形式	件数 (N)	N/P	パケット数 (P)	頻度 (/H)	送信量 (P/H)
新規	標準形式	6 万	6	10,000	4	40,000
解約	標準形式	12 万	6	20,000	2+2+1*10	280,000
更新 1	標準形式	42 万	6	70,000	4	280,000
更新 2	標準形式	84 万	6	140,000	4*1	560,000
ワーク鍵	標準形式	1,000 万	6	1,666,667	4*1	6,666,668
合計						7,826,668

93% 程度送信量が削減されている☆.

さらに，モバイル音声放送では 1 チャネルあたり 256 Kbps の伝送容量であるため，1 時間にパケット送信できるパケット数が 626,400 であり，現行方式では（契約情報の送信だけで）13 チャネルも必要になるが，提案方式では 1 チャネルで実現できる.

7. 安全性評価

提案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，契約情報を共通のワーク鍵で暗号化するため，ワーク鍵を 1 台の受信装置から取り出すことにより，全受信装置に対する契約情報を暗号化できるため，契約情報が偽造もしくは流用される可能性が高くなった．さらに，契約情報がイベント型で送信されるため契約情報チャネルの受信拒否により解約後も視聴を継続する可能性が生じる．このため本方式では以下のような安全対策が施されている.

7.1 契約情報の偽造/流用防止対策

提案の限定受信方式において限定受信部は（現行方式と同様に）内部のデータを簡単に書き込み/読み出しできない耐タンパ構造を仮定しているので，契約情報の偽造は自受信装置に対応する契約情報の契約情報記述子を変更すること，契約情報の流用は他受信装置に対する契約情報の受信装置 ID を自受信装置に変更して限定受信部に送信することととらえることができる.

このような偽造/流用は公開鍵暗号によるデジタル署名によって防止している．すなわち，契約情報にはすべてデジタル署名を付加し，自受信装置宛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，（あらかじめ受信装置内に埋め込まれている）公開鍵でデジタル署名を検証して偽造/流用の検出を行っている．また，公開鍵暗号のデ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，受信装置内を解析しても偽造や流用のための情報を見出すことはできない.

さらに本方式では公開鍵暗号として 2020 年頃まで安全性に問題がないと考えられている[7] 160 bit の楕円曲線暗号を用いるため，デジタル署名を偽造できる可能性はきわめて低い.

7.2 契約情報の受信拒否対策

受信拒否は契約情報とスクランブル鍵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，ECM-S 内部に契約情報とスクランブル鍵を包含しているため，契約情報を受信拒否するとスクランブル鍵が得られず，放送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．このためスクランブル鍵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

☆ 実際には現行方式はこれに加えて ECM の送信量を考慮しなくてはならない.

ことができる．

8. 実装評価

本稿で提案した限定受信方式は文献 8) で報告しているとおり，LSI として実現され，機能検証されている．処理時間の点で最も問題となったのは楕円曲線暗号によるデジタル署名の検証処理であるが，実現した LSI ではこの部分を多倍長演算コプロセッサを利用することによって，高速化を図り，1 回の署名検証を数十ミリ秒で処理できるようになった．また，新しい契約情報やワーク鍵，署名検証鍵が来る頻度は多くとも 1 カ月に 1 回であるので，実用上はまったく問題とならない．

9. 標準化について

提案方式をモバイル放送の限定受信方式として利用するためには，誰でも提案方式に対応したモバイル放送の受信装置が製造できるように仕様を公開する目的で，標準化を行う必要がある．衛星放送の限定受信方式にはすでに現行方式が存在したが，本稿に述べた理由により，モバイル放送では十分な安全性が確保できないため，2003 年 1 月 17 日新たな規格として提案方式が総務省令告示[9]され，ARIB 規格としても成立した[5]．

10. ま と め

モバイル音声放送は移動体向けの放送であるため放送帯域が狭く，1 チャネルの伝送容量が 256 Kbps と少ないこと，モバイルであるために常時限定受信情報を受信することが仮定できないことから，限定受信情報の送信量を可能な限り少なくする必要があった．

提案した限定受信方式は現行方式の限定受信情報の送信量を可能な限り削減するとともに，削減により低下した安全性を公開鍵暗号（楕円曲線暗号）によるデジタル署名や契約情報とスクランブル鍵の一体化のような暗号技術によってカバーした方式である．本稿では，これを送信量と安全性の観点から現行方式との比較検討を行い，十分に実用化できる方式であることを示した．

また，本方式は安全性を損なわず，送信量を削減するという観点から設計した方式であり，今後運用される有料放送に対する限定受信方式としても十分利用可能であると考えられる．

参 考 文 献

1) 小林喜三郎ほか：有料テレビジョン放送設備，東芝レビュー，Vol.47, No.6, pp.474–476 (1992).
2) 秋山浩一郎ほか：有料モバイル音声放送方式，東芝レビュー，Vol.54, No.7, pp.38–40 (1999).
3) （株）ビデオリサーチ：時間行動分析，情報メディア白書，p.237 (1997).
4) 橋本和彦ほか：70 近くの多チャンネルを実現する日本初のディジタル衛星放送，日経エレクトロニクス，No.669, pp.149–164 (1996).
5) 電波産業会：デジタル放送におけるアクセス制御方式標準規格（ARIB STD-B25 4.1 版）(2003).
6) 青木和麻呂：Multi2 暗号の線形解読における一考察，SCIS95-A4.1 (1995).
7) Lenstra, A.K. and Verheul, E.R.: Selecting Cryptographic Key Sizes, *J. of Cryptology*, Vol.14, No.4, pp.255–293 (2001).
8) 由良浩司ほか：モバイル衛星デジタル放送向け限定受信 LSI，東芝レビュー，Vol.56, No.7, pp.30–33 (2001).
9) 総務省：標準テレビジョン放送等のうちデジタル放送に関する送信の標準方式，平成 15 年 1 月 17 日総務省令第 26 号 (2003).

(平成 15 年 3 月 31 日受付)
(平成 15 年 9 月 5 日採録)

秋山浩一郎（正会員）

1986 年立教大学理学部数学科卒業．1988 年上智大学大学院理工学研究科博士前期課程修了．同年（株）東芝入社．情報セキュリティ技術の研究開発に従事．電子情報通信学会，日本数学会各会員．

上林　達（正会員）

1987 年京都大学理学部卒業（数学専攻）．1989 年名古屋大学大学院理学研究科博士課程前期課程修了．同年（株）東芝入社．情報セキュリティ技術の研究開発に従事．応用数理学会会員．

由良　浩司

1985 年東京大学工学部計数工学科卒業．同年（株）東芝入社．情報セキュリティ技術の研究開発に従事．電子情報通信学会会員．