L_068

狭帯域放送のための放送による契約情報の配信技術

A Contract Information Transmission System Using Broadcasting for Narrow-band Mobile Broadcasting Systems

西本 友成† 藤津 智† 砂崎 俊二† 木村 武史† 今泉 浩幸†
Yusei Nishimoto† Satoshi Fujitsu† Shunji Sunasaki† Takeshi Kimura† Hiroyuki Imaizumi†

1. まえがき

ワンセグやデジタルラジオなどの携帯受信機向けの狭帯域放送において、デジタルコンテンツの利用方法を制御するためには、アクセス制御方式である CAS(Conditional Access System)が必須である。今回、携帯受信機として、携帯電話だけではなく、PDA 端末、ゲーム機や車載型受信機など通信機能を必須で持たない携帯受信機も想定する。

CAS は、受信契約者のみに放送受信やコンテンツ再生を限定させる仕組みを提供する。受信契約者と非契約者を区別するために、受信機それぞれに契約情報を配信する必要があり、通信機能を持たない携帯受信機においては、この契約情報を放送で配信する必要がある。衛星デジタル放送の B-CAS[1]では、放送波により契約情報を配信している。しかし、受信機個別の契約情報を送るために、300kbps 程度の幅広い伝送帯域を必要とするため、現行の B-CAS による契約情報の配信技術を狭帯域放送に適用できない。また、2.6GHz 帯衛星デジタル音声放送[1][2]では、契約情報の送出のために、256kbps の専用チャンネルを設け契約情報の圧縮配信を行っている。ワンセグやデジタルラジオでは、専用チャンネルを設けることが難しく、数 kbps から数十 kbps 程度の狭い帯域で契約情報を配信する必要がある。

そのため、狭帯域放送における携帯受信機のための契約情報の配信技術を新たに開発する必要がある。

本稿では、まず研究課題と契約情報の配信技術の要求条件について述べ、開発した狭帯域放送のための契約情報の配信技術の概要を説明し、本技術の検証結果と安全性に関する検討結果について報告する。

2. 契約情報の配信における課題と要求条件

通信機能を持たない携帯受信機においてアクセス制御を実現するためには、放送により契約情報を受信機毎に、効率的に配信する必要がある。B-CAS の契約情報の配信技術を狭帯域放送に適用した場合、契約情報の送出レートを 1.5kbps と仮定すると、1000 万台すべての受信機に契約情報を送出するのに、約 470 時間要する。つまり、契約情報の送出周期が長くなり、携帯受信機に契約情報を確実に受信させることが困難になるという課題がある。また、B-CAS は、固定受信機を想定して、契約情報を常時受信できる環境を前提として設計されており、不安定な受信環境である携帯受信機には適用できない。

今回、以下に示す要求条件を設定し、それを満足する狭帯域放送における携帯受信機のための契約情報の配信技術を開発した。

- 狭帯域放送の伝送帯域と、低消費電力化を考慮して、契約情報を圧縮し、契約情報の送出レートを低くすること
- 受信時間が短いモバイル利用環境においても、受信機に契約状態を反映できること

3. 開発した契約情報の配信技術

図 1(a)に、現行方式として B-CAS の概要を示す。受信機個別の情報である個別情報(EMM: Entitlement Management Message)と、受信機共通の情報である共通情報(ECM: Entitlement Control Message)で構成される。契約情報を受信機に固有のマスター鍵で暗号化して、受信機 ID(CAS_ID)を宛先として付与し個別情報として配信する。受信機では、受信機 ID の一致する個別情報を受信したときに、マスター鍵で暗号復号し契約情報を取得する。

図 1(b)に、開発した契約情報の配信技術の概要を示す。契約情報を共通情報として配信することで、複数の受信者向けの契約情報を一斉配信することができる。図 2 に、本技術で用いる共通情報の構成を示す。受信機 ID を付与せずに、各々の受信機をグループ毎に分けてビット列化し、複数の受信者の契約情報を束ね契約情報を圧縮する。さらに、ビット列化した契約情報に対して、可逆圧縮を施し伝送効率を高めることができる。受信機では、すべての共通

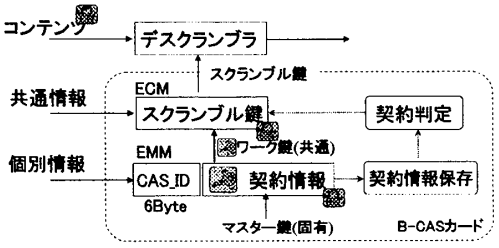

図 1(a) 現行技術の概要

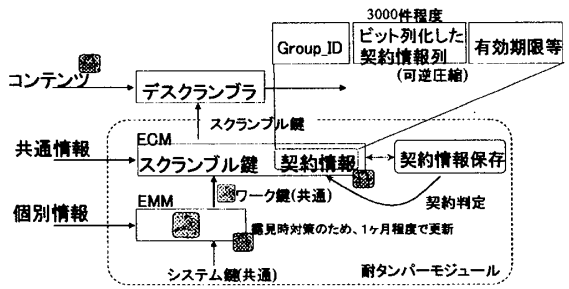

図 1(b) 開発した契約情報の配信技術の概要

†NHK 放送技術研究所
†NHK Science and Technical Research Labs.

情報を暗号復号し、受信機の Group_ID と一致する時に、ビット列化された契約情報から自分宛の契約情報のみを取得する。また、ビット列化した契約情報は、契約状態を示す情報を含んでおり、契約中であれば 1、未契約であれば 0 の値を持つ。

B-CAS では、受信機 ID を付与して契約情報を送出するので、受信機を選択して送出できる。一方、本技術では、受信機 ID を持つすべての受信機に対して連続的にカルーセル伝送する。

図 3 に、各技術の契約者数に対する契約情報の送出周期を示す。契約情報の送出レートは、1.5kbps で算出した。B-CAS では、契約者 1 千万件で送出周期が 450 時間を越えてしまうが、本技術では、2.5 時間と大幅に短縮できる。

本技術は、契約情報の高圧縮配信が期待できるが、受信機 ID を持つすべての受信機に対して契約情報を配信するため、受信機 ID の発行数が増加するほど契約情報の送出周期が長くなる欠点を持つ。そこで、本技術の運用スキームに関する評価を行った。

4. 評価結果

契約情報の配信技術では、契約情報の送出レート、送出周期、想定する契約者数や携帯受信機の電源 ON 時間などのパラメータを考慮しなければならない。相反するパラメータもあるので、運用スキームに応じてこれらのパラメータの最適値を選定する必要がある。

図 4 に、受信機 ID の発行数に対する契約情報の送出周期を示す。実線は、契約情報列に対する可逆圧縮がない場合、破線は、契約情報列に可逆圧縮を行ったときの送出周期を示している。可逆圧縮は、ランレングス・ハフマン符号化を用い、受信契約率 5%で算出した。

B-CAS において狭帯域放送での契約情報の配信は不可能とされてきたが、本技術では、次の条件下で契約情報の配信を可能にする。厳しい条件として、契約情報の送出レートを約 1.5kbps とし、1 日 5 分間の視聴[3]で送出周期を 2.5 時間とした場合、契約情報の未受信は 1 年間で 100 万件に対して 5 件程度の割合で発生すると算出される。この時、受信機 ID を 1 千万個程度まで発行可能である。また、契約情報の送出レートを 15kbps とし、夜間は常時放送受信可能と想定した場合、送出周期は 5〜7 時間程度でよい。この時、受信機 ID を最大 5 億個程度発行する運用が可能である。

このように、発行可能な受信機 ID の総数は有限であるが、以下に示す方法により、受信機 ID の発行数における運用上の制限を緩和することが可能である。

・B-CAS で使用する EMM(受信機固有のマスター鍵で暗号化)を併用することで、受信契約時に放送により編成チャンネル単位で受信機 ID を付与するこが可能である。つまり、受信機 ID を運用時に随時変更できるので、想定する契約者数だけ受信機 ID を発行できればよい。

5. 安全性に関する検討

提案技術の導入による安全性への影響について検討した。契約情報を共通情報として配送するため、偽造した契約情報の注入による不正視聴の恐れがある。このため、共通情報の暗号鍵であるワーク鍵を定期的に更新できる設計とした。また、正規の契約情報で上書きするために、常に契約情報を継続的に送出する設計とした。

契約情報とコンテンツの復号鍵であるスクランブル鍵を同封しており、すべての契約情報を耐タンパーモジュールで処理するので、契約情報の不正な除去も防止できる。受信機への負荷を抑えながら、従来の方式と同等の安全性を保持している。

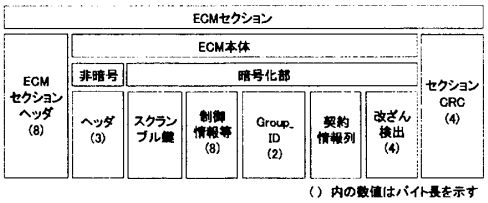

図 2　使用する ECM の構成

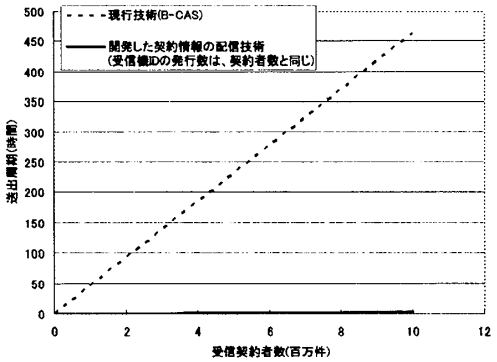

図 3　契約者数に対する契約情報の送出周期

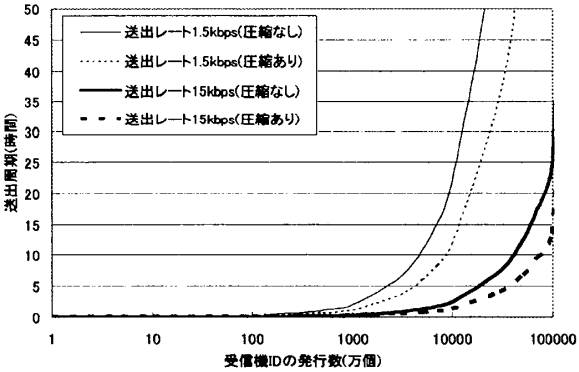

図 4 受信機 ID の発行数に対する契約情報の送出周期

6. まとめ

狭帯域放送用のアクセス制御方式のための契約情報の配信技術を考案し、本技術を実用化した場合の運用スキームを明らかにした。また、本技術の安全性を示した。今後は、本技術の実装評価を行う。

【参考文献】

[1]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 (2006)
[2]秋山ほか:“有料モバイル音声放送における限定受信方式の設計,” 情報処理学会論文誌, Vol. 44, No. 12, pp. 3071-3080(2003)
[3]ビデオリサーチ:時間行動分析, 情報メディア白書(1997)