デジタル放送に対応した限定受信システム

Conditional Access System for Digital Satellite Broadcasting Services

米谷　寿子 YONETANI Toshiko
山下　幹雄 YAMASHITA Mikio
藤原　純一 FUJIWARA Junichi

特定の視聴者だけに番組をサービスするシステムのことを限定受信システムと言う。デジタル放送には数多くの番組があり，視聴者を獲得するためには，サービス内容の差別化が必要である。このため，有料放送を可能とする限定受信システムの実現が強く望まれている。

当社は，このようなニーズにこたえるために，アナログ放送（BS（放送衛星）及びCS（通信衛星）による衛星放送）における限定受信システム納入の実績をベースとして，デジタル放送に対応した限定受信システムを開発した。このシステムは，構成機器を変更することなく，アプリケーションソフトウェアの追加変更で，いろいろなニーズに対応することができる設計となっており，非常に汎用性の高いシステムとなっている。

A conditional access system is a system that allows broadcasters to restrict their services so that they can be accessed only by their subscribers. There is strong demand from digital satellite broadcasters for such systems in order to provide pay-TV services, so that their services can be distinguished from various other services.

Toshiba has developed the Conditional Access System for Digital Satellite Broadcasting (D-CAS), based on the experience accumulated in developing conditional access systems for analog broadcasters. The system is designed to flexibly meet the different requirements of each customer, with minor modification of the application software and without changing the hardware components of D-CAS.

1 まえがき

デジタル放送の大きな特長の一つとして,複数の放送局が,複数のサービス(テレビ放送, ラジオ放送, データ放送, など)を提供するということが挙げられる。この結果, 視聴者にとっては, 番組選択の幅が大きく広がることになる。しかし, 放送局にとっては, サービス内容の充実や差別化が必要となる。そこで, サービス内容の差別化を実現するための一つの手段として, 有料放送が可能な限定受信システムの必要性が高まっている。

そこで, 当社は, アナログ放送における限定受信システム納入の実績をベースとして, 松下電器産業(株)と共同で, デジタル放送に対応した限定受信システムを開発した。

2 限定受信の仕組み

デジタル放送対応型限定受信システム(以下, D-CASと略記)は, 特定の視聴者だけが視聴可能となるように, 番組を暗号化(スクランブル)し送出するシステムである。視聴者が, スクランブルされた番組を見ること(デスクランブル)が可能か否かは, 受信機で判定される。スクランブルされた番組を視聴できるまでの過程を図1に示す。配信される番組には, 番組の情報と視聴可否に関する情報(この番組はスポーツ番組で有料, など)が付加されている。この番組に関する情報と受信機の制御に関する情報を合わせて, 共通情報(ECM：Entitlement Control Message)と言い, D-CASのECM系サブシステムで生成・暗号化されている。

受信機内のICカードには, 加入者ごとに固有の番号が与えられており, 個人契約情報(どのような番組を契約しているか, など)が登録される。この個人契約情報及び共通情報の暗号を解くための情報を個別情報(EMM：Entitlement Management Message)と言い, D-CASのEMM系サブシステムで生成・暗号化される。受信機は, ECMとEMMを取得し, 番組が視聴可能であるか否かを判断する。

受信機は, 次のステップでデスクランブルを行う。

(1) 暗号化されたEMMをICカード固有の鍵(かぎ)(マスタ鍵)で復号する。
(2) 復号したEMMから鍵(ワーク鍵)を取り出す。
(3) ワーク鍵を用いてECMを復号する。
(4) 復号したECMから鍵(スクランブル鍵)を取り出す。
(5) スクランブル鍵を用いて映像などの情報を復号する。

D-CASにおいては, 受信機で復号できるように, 対応した鍵を用いて暗号化を行わなければならない。すなわち, 次のステップでスクランブルを行う。

(1) EMM(ワーク鍵を含む)をマスタ鍵で暗号化(EMM系サブシステムで行われる)。
(2) ECM(スクランブル鍵を含む)をワーク鍵で暗号化(ECM系サブシステムで行われる)。

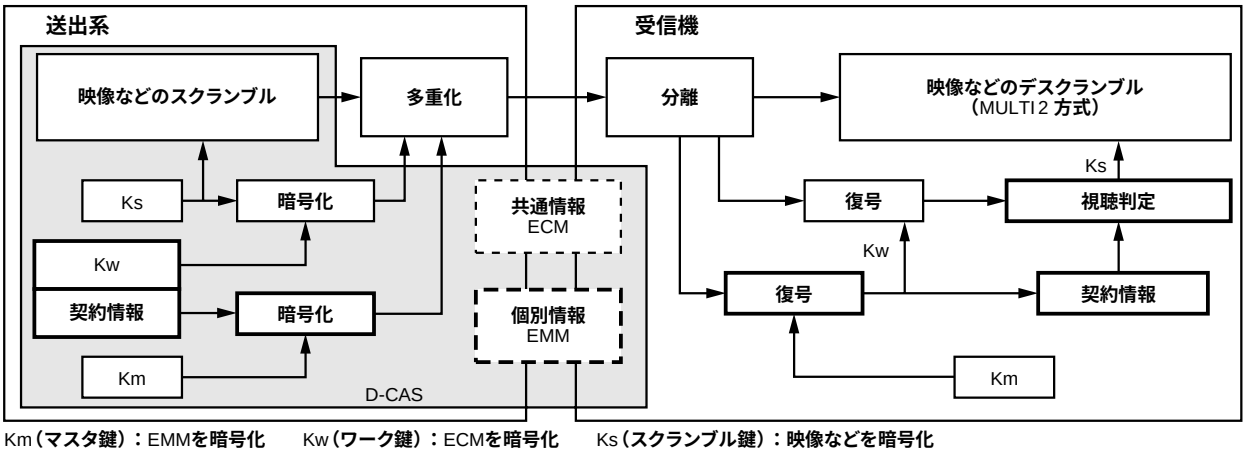

図1．限定受信方式の仕組み　D-CASは，マスタ鍵，ワーク鍵，スクランブル鍵の3種類の鍵でスクランブルを行い，受信機は，この3種類の鍵を用いて，デスクランブルを行う。
Functional block diagram of Conditional Access System

⑶　暗号化されたECMとEMMは，映像や音声などとともに多重化装置（D-CASの構成外機器）で多重化され，映像や音声などの情報をスクランブル鍵で暗号化（暗号化装置（スクランブラ）で行われる）。

当社は，D-CASのうちECM系サブシステム及び暗号化装置（スクランブラ）の開発を担当した。

3　システムの概要

D-CASのシステム構成を図2に示す。

ECMコントローラ（ECMC）は，以下の基本機能を備えている。

⑴　データサーバ（DS：Data Server）から，ECMの元データやスクランブル用元データを受信する。

⑵　自動番組送出制御装置（APC：Automatic Program Controller）から，番組切替指示（スクランブル開始／停止指示）を受信する。

⑶　EMM系機器から，ワーク鍵や課金情報を受信する。

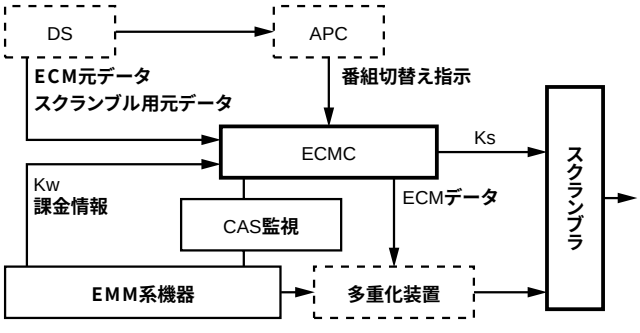

図2．D-CASのシステム構成　ECM系，EMM系から構成され，CAS監視で一元的に管理される。
Configuration of D-CAS

⑷　ECM元データや課金情報からECMデータを生成し，ワーク鍵を用いて暗号化後，多重化装置へ送出する。

⑸　スクランブル用元データから，スクランブルデータを生成し，スクランブラに送信する。

⑹　スクランブル鍵を生成し，スクランブラに送信する。

⑺　APCからのスクランブル開始／停止指示に従い，スクランブルのON/OFFを行う。

⑻　ECMC内部の異常やスクランブラの異常をCAS監視に伝達する。

スクランブラは，ECMCからの制御により，スクランブルのON/OFF制御を行う。スクランブルがONの場合には，ECMCから受信したスクランブル鍵を用いて，多重化装置から出力されたデータに対して，ISO9979/0009に準拠した方式（MULTI2）でスクランブルを掛ける。スクランブルがOFFの場合には，多重化装置から出力されたデータをそのまま出力する。

なお，CAS監視は，下記の機能を持つ，D-CASを一元的に監視及び管理する端末である。

⑴　ECM系機器及びEMM系機器の状態（正常，異常）を表示する（異常の詳細情報も検索可能）。

⑵　ECM系機器及びEMM系機器の異常を上位のシステムへ通知する。

⑶　ECM系機器及びEMM系機器が保持しているデータを参照する。

⑷　ECM系機器及びEMM系機器へ指示を出す。

4　アナログ用限定受信システム技術の継承

アナログ用限定受信システムとD-CASでは，取り扱っているデータが異なっているため，システムとしては多くの相違点がある。しかし，アナログ用限定受信システムで培った技

術は，D-CASを開発するうえで，大変重要である。

⑴ 鍵の利用方法　　スクランブルを行うために，マスタ鍵，ワーク鍵，スクランブル鍵を使用することは，D-CASと共通であるため，アナログ用限定受信システムの技術が流用できる。

⑵ データの受信　　上位システムから，事前に必要なデータを受信して動作する方式は，D-CASと共通であるため流用できる。

5 システムの特長

システムの主な特長をまとめると以下のとおりである。

5.1 高信頼性

放送機器のトラブルは，映像・音声の中断などの放送事故に直接つながる。特に，D-CAS関連機器の故障は，有料番組が無料となってしまう放送事故や，視聴可能な加入者が視聴不可となってしまう重大放送事故を引き起こす原因となる。そのため，D-CASに対しては，高度な信頼性が要求される。

D-CASは，下記の手段により高信頼性を確保している。

⑴ 二系統化　　D-CAS構成機器は，**図3**に示すように，ネットワークで接続されている。D-CASの主要機器に関しては二系統化されており，1系，2系には同一のデータが送信され，同一の出力が得られる設計になっている。どちらの系の出力を使用するかは，ポストスプライサで選択される。万が一，使用している系統の機器に異常が発生した場合には，ポストスプライサによる系統切替えを行い，放送事故を防ぐ設計となっている。また，1系，2系に保持されたデータの整合性チェックや，1系のデータを2系にコピーするという機能を備えており，障害発生後のデータ復旧をできる限りECM系統内部で行えるような設計となっている。

⑵ 機器内部の二重化　　ECM関連データは，高信頼性の産業用ワークステーション（WS）に記録される。この産業用WSは，ハードディスクを二重化しており，一つのハードディスクの障害に対して，運行に障害が生じない設計となっている。

⑶ 停電対策　　ECMCの構成機器は，産業用WSを除き，停電復帰後にも問題なく動作する。産業用WSは，停電による故障を防ぐために，無停電電源に接続されている。

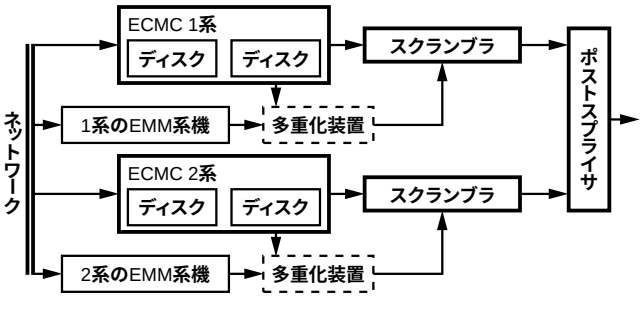

図3．二系統による運用　　異常が発生した場合には，系統を切り替えることにより，放送事故を防ぐことが可能である。
Parallel systematic usage of D-CAS

5.2 外部機器故障対策

ECM系外部の機器が障害により動作停止になった場合でも，放送事故を防止する工夫がなされている。

⑴ DSの障害に対して　　DS，もしくはDSとの通信に障害が発生した場合には，ECMの元データやスクランブル用元データが受信できなくなる。

ECMCは，上記障害を想定し，障害対策としてECMC構成機器の産業用WSにECM元データやスクランブル用元データを保持している。APCからの番組切替指示により，このデータを送出し，放送事故を防止する。

⑵ APCの障害に対して　　APC，もしくはAPCとの通信に障害が発生した場合には，スクランブルの開始／停止指示が受信できなくなる。

上記障害発生時には，ECMCは障害を検知し，CAS監視に通知する。その後，CAS監視から手動操作で番組切替指示を送信することにより，ECMCは予定どおりのスクランブル制御をすることができる。

⑶ EMMサーバの障害に対して　　EMMサーバ，もしくはEMMサーバとの通信に障害が発生した場合には，ワーク鍵や課金情報の受信ができなくなる。

ECMCは，上記障害を想定し，障害対策としてECMC構成機器の産業用WSにワーク鍵や課金情報をデータとして保持している。ECMCは，保持データを使用してECM送出を行う。なお，ワーク鍵や課金情報は，CAS監視から手動操作により転送することも可能である。

5.3 高操作性

D-CAS構成機器の状態は，EMM系機器及びECM系機器ともに，CAS監視で一元的に管理することにより，機器状態の正常／異常や，スクランブルのON/OFF状態などを，ひと目見て判別でき，また，D-CAS構成機器に生じた異常及びその異常に対する対処方法を上位システムに通知し，緊急時の早急な対応を可能とする容易な操作性を実現した。更に，異常の詳細な内容及び対処方法を検索することも可能である。

5.4 高機能

D-CASは，ユーザーからの要求に応じて，様々な課金方式に対応が可能である。

⑴ ペイパービュー契約　　視聴者が，有料番組を購入することにより，見た番組分だけ料金が加算される契約

のことである。なお，D-CASでは，番組開始から無料で視聴できる時間を指定したり，追加料金により録画可能となる番組や副音声だけペイパービューといった番組も実現可能である。

⑵　ティア（tier）契約　　月ぎめ，年ぎめなど，あらかじめ視聴者と契約することにより，チャンネル全部あるいは部分的に視聴が可能となる契約のことである。D-CASでは，ジャンルごとの番組，シリーズ番組，週末番組，シーズン番組，などの契約に対応可能である。

また，D-CASでは，下記に示すような流動番組編成についても，対応している。

⑴　有料番組の予定が急に無料の番組に差し替わる場合
　　例：有料の野球中継が雨天中止になった場合，など

⑵　有料番組の終了時間が急に延びた場合
　　例：有料の野球中継が延長戦で放送時間を延長した場合，など

5.5　高汎用性

D-CASを構成する機器は，他システムと共通の機器を使用しており，汎用性に富んでいる。ECMCで使用している産業用WSは，当社の開発したCA契約情報生成装置にも使用されている。CA契約情報とは，デジタル放送において，録画などの番組予約をする際に必要な情報である。受信機は，CA契約情報を参照して，予約しようとしている番組が視聴可能であるかを判断し，視聴不可能である場合には，視聴者にその旨を通知する。CA契約情報生成装置は，CA契約情報を生成し，DSに送出する装置である。また，D-CAS内でも，D-CASに時刻情報を送信する時計インタフェースとスクランブルのON/OFFの状態をモニタに表示する機能を持つスクランブル表示インタフェースは，同一のハードウェアを使用している。これらの装置は，ソフトウェアを変えることにより，それぞれの機能を実現している。なお，D-CASと接続するサブシステムを新規に増設する場合には，ECMCのソフトウェアを修正するのではなく，インタフェース装置を追加することで対応が可能な汎用性のあるシステムを実現した。

図4．ECM系機器ラック実装　　すべての機器設定及び状態が前面からひと目でわかる構造である。
Entitlement control message (ECM) subsystem of D-CAS

5.6　高収納性・高保守性

D-CASを構成する機器は，図4に示すようにラックに実装される。キーボードや保守用コンピュータなどは，必要時に引き出して使うことができるスライドボード上に配置し，高収納性を実現している。また，高保守性を下記に示す設計により実現した。

⑴　機器ごとに棚が分かれており，必要最小限の取外しで機器の交換ができる。

⑵　機器の電源スイッチや設定スイッチ，機器の稼働状態を表示するランプなどはすべて前面に配置されているので，保守後の点検が容易に実施できる。

6　あとがき

アナログ衛星放送用限定受信システムで培った技術を継承しながら，BSデジタル衛星放送用限定受信システムを実現した。加えて，高信頼性，高保守性を備え，デジタル放送限定受信システムの汎用設備として，ユーザーニーズにこたえていけるものと期待している。

今後は，D-CASの実績を踏まえ，CSデジタル放送，地上波デジタル放送と展開していくデジタル放送に対応した限定受信システムを開発していく所存である。

謝　辞

システムの開発にあたり，ご意見，ご指導いただいた松下電器産業（株）の関係各位に深く感謝の意を表します。

米谷　寿子　YONETANI Toshiko
情報・社会システム社 小向工場 放送映像機器設計部主務。
放送映像機器の設計・開発業務に従事。
Komukai Operations

山下　幹雄　YAMASHITA Mikio
情報・社会システム社 小向工場 放送映像機器設計部主務。
放送映像機器の設計・開発業務に従事。
Komukai Operations

藤原　純一　FUJIWARA Junichi
情報・社会システム社 小向工場 放送映像機器設計部。
放送映像機器の設計・開発業務に従事。日本機械学会会員。
Komukai Operations