モバイル衛星デジタル放送向け限定受信LSI

Conditional Access LSI for Broadcast Satellite Service for Mobile Receivers

由良　浩司　YURA Koji
秋山　浩一郎　AKIYAMA Koichiro
石川　敏朗　ISHIKAWA Toshio

放送のデジタル化が急速に進展するなか，当社ではモバイル向け衛星デジタル放送の開発を進めている。この受信機用LSIチップセットの一つとして，限定受信LSI（CALSI：Conditional Access LSI）を開発した。モバイル衛星デジタル放送では，放送方式の特性に合った限定受信の新しいシンタックス（文法）が規定されており，CALSIは，このシンタックスに沿った新たでセキュア（安全）な限定受信方式を実装している。CALSIは受信機用LSIチップセットの一つとして評価装置に実装され，新しい限定受信方式の有効性が実証された。

Many digital broadcasting services have been realized in recent years.　Toshiba is developing a broadcast satellite service (BSS) for mobile receivers.　We have developed a conditional access LSI (CALSI) as one LSI of the BSS receiver chip set. CALSI has a new conditional access function based on a new standard conditional access syntax that is suited to BSS.　We have confirmed the functionality of the LSI in a test system and verified the effectiveness of the new CA system.

1　まえがき

放送のデジタル化が急速に進展するなか，当社ではSバンド（2.6 GHz帯）モバイル衛星デジタル放送の開発を進めている。1999年7月には，電気通信技術審議会から，「2.6 GHz帯の電波を利用する衛星デジタル音声放送システムの技術的条件」が答申された。この答申の中で，限定受信方式については，既存の関連情報シンタックスに加えて，Sバンドモバイル衛星デジタル放送の特性を考慮した新シンタックスを規定している。

当社では，この答申に沿って，2000年度に受信機用LSIチップセットを開発した。CALSIは，この受信機用LSIチップセットの一つであり，新シンタックスに沿った限定受信機能を実現するLSIとして開発された。ここでは，このCALSIについて述べる。

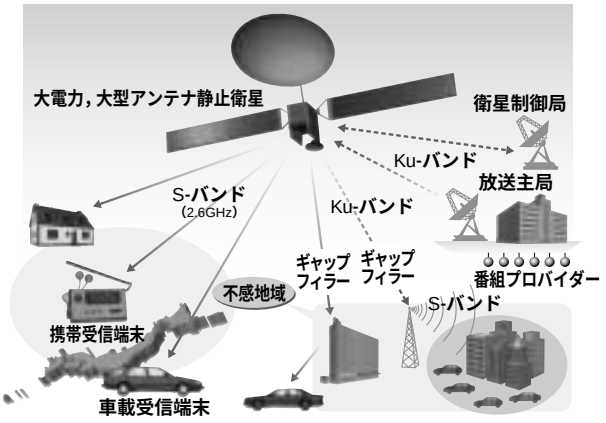

図1．モバイル衛星デジタル放送システム　衛星を通じて全国の移動端末への放送を実現する。
Broadcast satellite service for mobile receivers

2　CALSI開発の背景

当社は，Sバンドモバイル衛星デジタル放送のシステムやサービスの開発を行っている。モバイル衛星デジタル放送は，次の実現を目指している（**図1**）。

⑴　日本全国向け衛星デジタル放送
⑵　日本初の移動体向けマルチメディア放送
⑶　多チャンネルで多彩な番組提供
⑷　高速移動中でも安定した受信が可能
⑸　道路・渋滞情報などのITS（高度道路交通システム）関連情報提供

Sバンドモバイル衛星デジタル放送方式については，99年7月に電気通信技術審議会から「2.6 GHz帯の電波を利用する衛星デジタル音声放送システムの技術的条件」が答申されている。この中で，限定受信方式の関連情報サブシステムに関しては，CS（通信衛星）・BS（放送衛星）デジタル放送方式と同じ既存の関連情報シンタックスに加えて，新しい関連情報シンタックスが併記されている。新シンタックスは，Sバンドモバイル衛星デジタル放送の特性を考慮して規定された。

Sバンドモバイル衛星デジタル放送は，CS・BSデジタル放送と比べて送信できる情報量が少ない。また，移動体に設置された受信機では，常時受信を期待できないため，端末個別の情報を長い期間にわたって繰返し送信する必要があ

る。新シンタックスはこの点を考慮して，端末個別の情報を圧縮した構造になっている。当社は，この新シンタックスに適した限定受信方式の開発を進めてきた[1]。

3 CALSI開発の目的

当社では，Sバンドモバイル衛星デジタル放送受信機用の主要なLSIチップセットとして，次の3種のLSIを開発した。

⑴ 符号分割多重（CDM）受信用のパスサーチLSI及びRAKE受信（複数のパスを解析・合成する）LSI

⑵ 有料放送に対応するCALSI

⑶ トランスポートストリーム（TS：Transport Stream）分離，AAC（Advanced Audio Coding）音声及びMPEG4（Moving Picture Experts Group 4）映像のデコードを行うマルチメディアLSI

これらのLSIチップセットを組み込んだ評価装置を開発し，性能評価を終了した。CALSIは，前述の新シンタックスに沿った限定受信方式の検証を目的として開発された（**図2**）。

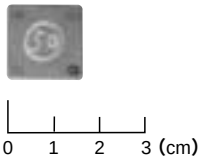

図2. CALSI　100ピンプラスチックパッケージである。
Conditional access LSI

4 関連情報新シンタックス

関連情報新シンタックスは，既存のシンタックスと同様，2種類の情報ユニットで構成される。ECM―S（Entitlement Control Message for S-band）とEMM―S（Entitlement Management Message for S-band）である。また，これらの情報はMPEG2 TSのセクション形式の通常形式で構成される。

4.1 ECM－S

ECM―Sは，既存のシンタックスにおけるECMと同様にPMT（Program Map Table）から参照される関連情報である。ECM―Sは**表1**の項目で構成される。

セクションヘッダは，MPEG2セクション形式の通常形式である。ワーク鍵（かぎ）識別は，このセクションの暗号化鍵を示す識別子である。ワーク鍵の内容はEMM―Sで送信される。

契約情報記述子は，各受信端末に契約情報を設定するための情報である。構成要素は，各受信機の契約情報をリストに列挙した契約登録リストと，偽造を困難にするためのデジタル署名などで構成される。

表1. ECM－Sの構成
ECM-S data format

項　目	
セクションヘッダ	
ワーク鍵識別	
契約情報記述子	記述子タグ
	記述子長
	契約登録リスト
	更新番号
	署名検証鍵識別子
	デジタル署名
	拡張領域
番組情報記述子	記述子タグ
	記述子長
	放送番組番号識別
	スクランブル鍵
	契約参照情報
	拡張領域
改ざん検出	

番組情報記述子は，端末に設定された契約情報に基いてコンテンツをデスクランブルするための情報である。構成要素は，コンテンツを識別するための放送番組番号識別子，番組のスクランブル鍵と，受信の可否を判定するための契約参照情報などで構成される。改ざん検出は，受信エラー及びデータの改変による誤ったセクションの排除に使われる。

4.2 EMM－S

EMM―Sは，既存のシンタックスにおけるEMMと同様にCAT（Conditional Access Table）から参照される関連情報である。EMM―Sは**表2**の項目で構成される。

表2. EMM－Sの構成
EMM-S data format

項　目	
セクションヘッダ	
ワーク鍵情報記述子	記述子タグ
	記述子長
	有料事業体識別コード
	年月日
	ワーク鍵識別
	ワーク鍵
	拡張領域
署名検証鍵情報記述子	記述子タグ
	記述子長
	有料事業体識別コード
	年月日
	ワーク鍵識別
	署名検証鍵識別子
	署名検証鍵情報
	デジタル署名
	拡張領域
改ざん検出	

セクションヘッダは，MPEG 2セクション形式の通常形式である。

ワーク鍵情報記述子は，関連情報を暗号化するためのワーク鍵を端末に設定するための情報である。構成要素は，有料事業体識別コード，関連情報の復号時に鍵を特定するためのワーク鍵識別，ワーク鍵のデータなどで構成される。

署名検証鍵情報記述子は，契約情報記述子に付与されているデジタル署名を検証する鍵の情報である。有料事業体識別コード，署名検証鍵データを復号するためのワーク鍵識別子，契約情報のデジタル署名の検証で検証鍵を特定するための署名検証鍵識別子，鍵情報の本体である署名検証鍵情報，署名検証鍵情報の偽造を困難にするためのデジタル署名などで構成される。

5 CALSIの機能

当社が開発したCALSIの機能構成を**図3**に示す。

このLSIの基本動作は，MPEG2 TSを入力し，契約情報に基いてスクランブルされたコンテンツをデスクランブルして，TSとして出力することである。また，このLSIの制御をホストCPUから行うために，初期化やEMM―SやECM―SのPID（Packet IDentifier）の指定などをコマンドとして受け付ける。

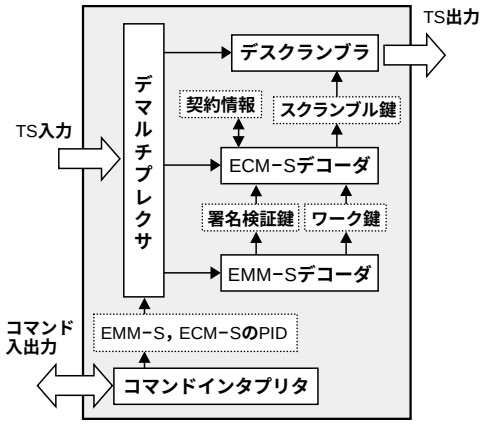

図3．CALSIの機能構成　CALSIは関連情報から契約情報を取得し，この契約情報に基づいてコンテンツのデスクランブルを行う。
Functional configuration of CALSI

5.1 デマルチプレクサ

デマルチプレクサは，TSパケットヘッダのPIDにより，TSパケットを関連情報のECM―S，EMM―S，及びそれ以外に分ける機能である。ECM―S，EMM―SのPIDは，受信端末のホストプロセッサなどがPMT，CATを解析して値を取得し，このLSIにコマンドとして設定する。

5.2 デスクランブラ

デスクランブラは，ECM―S，EMM―S以外のTSパケットを入力とする。TSパケットヘッダからスクランブルの有無を検出し，スクランブルされているパケットについては，LSI内部に保持するスクランブル鍵を参照し，適用可能なスクランブル鍵があれば，その鍵によりパケットのデスクランブルを行い，TS出力に出力する。スクランブルされていないパケットやLSI内部に鍵を保持していないパケットについては，そのままTS出力に出力する。

5.3 ECM－Sデコーダ

ECM―Sデコーダは，ECM―Sを入力とする。ECM―Sをワーク鍵で復号し，改ざん検出を行い，改ざんがなければ内容を解析する。契約情報記述子からは，自端末の契約登録情報の有無をチェックし，あればデジタル署名を検証のうえ，契約情報としてLSI内部に登録する。登録された契約情報は，スクランブル鍵取得の際に受信可否の判定に用いられる。

番組情報記述子からは，受信しているコンテンツのスクランブル鍵であるかを確認し，次にLSIに登録された契約情報と番組情報記述子の中の契約参照情報から受信可否を判定して，受信可であればスクランブル鍵を取得する。取得したスクランブル鍵は，デスクランブラで利用される。

5.4 EMM－Sデコーダ

EMM―Sデコーダは，EMM―Sを入力とする。まず改ざん検出を行い，改ざんがなければ内容を解析する。ワーク鍵情報記述子からはワーク鍵識別をチェックし，保持していないワーク鍵であればこのワーク鍵データを取得する。取得したワーク鍵は，この後関連情報の復号に利用する。

署名検証鍵情報記述子からは，署名検証鍵識別子をチェックし，保持していない署名検証鍵であれば，デジタル署名を検証してこの署名検証鍵を取得する。取得した署名検証鍵は，契約情報の取得の際に利用する。

6 CALSIの内部構成

このような機能を実現するための，CALSIの内部構成を**図4**に示す。

コマンド入出力部は，このLSIを制御する外部のホストCPUからコマンドを受け付け，処理した結果を返すためのインタフェース機能を持つユニットである。

TS入力部，TS出力部は，TSパケットを入出力するインタフェースである。TS入力部は，コンテンツ，関連情報，その他の情報の区別なくTSパケットはすべてここから入力する。TS出力部からは，ECM―S，EMM―Sを出力しないが，他の入力されたパケットはすべて出力する。

メモリ部は，実行用のワークRAM（Random Access Memory），コントローラの制御プログラムROM（Read Only

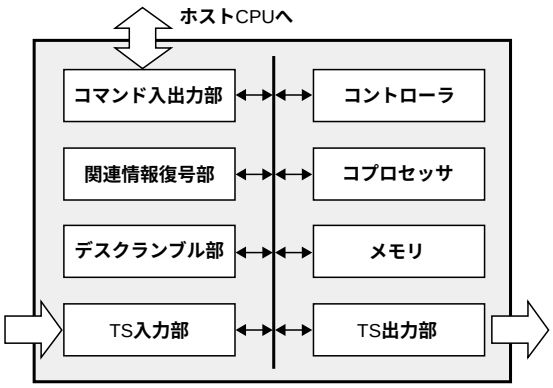

図4．CALSIの内部構成　デスクランブル，関連情報復号，署名検証の各セキュリティ機能と，コントローラ，メモリ，入出力部で構成している。
Architecture of CALSI

Memory），端末固有のパラメータや契約情報を保持するEEPROM（Electrically Erasable and Programmable ROM）などで構成している。

デスクランブル部は，コンテンツのデスクランブルを行うユニットである。コントローラは，ECM―Sから取得したスクランブル鍵をメモリ上に保持し，スクランブルされたコンテンツのTSパケットが入力されると，対応するスクランブル鍵をメモリ上から検索し，鍵があればデスクランブル部でデスクランブルしてTS出力部から出力する。

関連情報復号部は，関連情報の復号を行うためのユニットである。コントローラEMM―Sからワーク鍵を取得してメモリ部に保持し，その後にEMM―S，ECM―Sが入力されると，このワーク鍵を適用して，関連情報復号部で暗号化範囲の復号を行う。

デスクランブル部，関連情報復号部の共通鍵暗号ブロックは，当社が開発した高位合成SIDER（Synthesis by Initial Design Extension and Refinement）を用いてCプログラムからの高位合成により作成した[2]。データパスの基本構造を初期回路として与え，設計空間の探索を大幅に減らす高位合成方法であるため，適切な処理速度の回路を実用的な規模で実現し，かつ設計期間を大幅に短縮することができた。

コプロセッサは，デジタル署名の検証で必要となる，多倍長整数演算を実行するユニットである。コントローラは，これらの各ユニットを制御し，処理シーケンスを実行するユニットである。TS入力インタフェースにTSパケットが入力されると，TSパケットの処理を開始し，一定の制限時間内でTSパケットの実時間処理を行う。これにより，入力されたTSパケットを常に一定の遅れ時間で出力している。ただし，関連情報の解析において，デジタル署名の検証はこの制限時間内に終えることができない。このような処理は，実時間処理から通常の処理に引継いで，実時間処理の間で処理を実行している。

7　機能検証

CALSIは，Sバンドモバイル衛星デジタル放送受信機用のLSIチップセットの一つとして開発し，これらのLSIチップセットを組み込んだ評価装置で機能検証を行った。

この結果，コンテンツのデスクランブル，ECM―Sによる契約情報の取得と契約情報に基いたスクランブル鍵の取得，及びEMM―Sによるワーク鍵と署名検証鍵の取得が仕様どおり行われることを確認した。

8　あとがき

当社は，Sバンドモバイル衛星デジタル放送受信機用のLSIチップセットの一つとして，モバイル端末向けの音声放送に適した新方式によるCALSIを開発した。このCALSIは，他のLSIチップセットとともに評価装置に実装され，新しいシンタックスによる限定受信の機能を確認した。

今後は実用化を目指したLSIの開発を進めていく。

文　献

(1)　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．**54**，7，1999，p.38－40.

(2)　増田篤司，ほか．探索空間を縮小する高位合成手法．東芝レビュー．**50**，6，1995，p.465－467.

由良　浩司　YURA Koji

e-ソリューション社　SI技術開発センター　SI技術担当主務。セキュリティ技術の応用開発に従事。電子情報通信学会会員。

Systems Integration Technology Center

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。セキュリティ技術開発に従事。電子情報通信学会会員。

Computer and Network Systems Lab.

石川　敏朗　ISHIKAWA Toshio

e-ソリューション社　メディア＆コンテンツ事業部 モバイル放送事業開発部主務。放送システムの開発などに従事。日本音響学会会員。

Media & Contents Business Div.