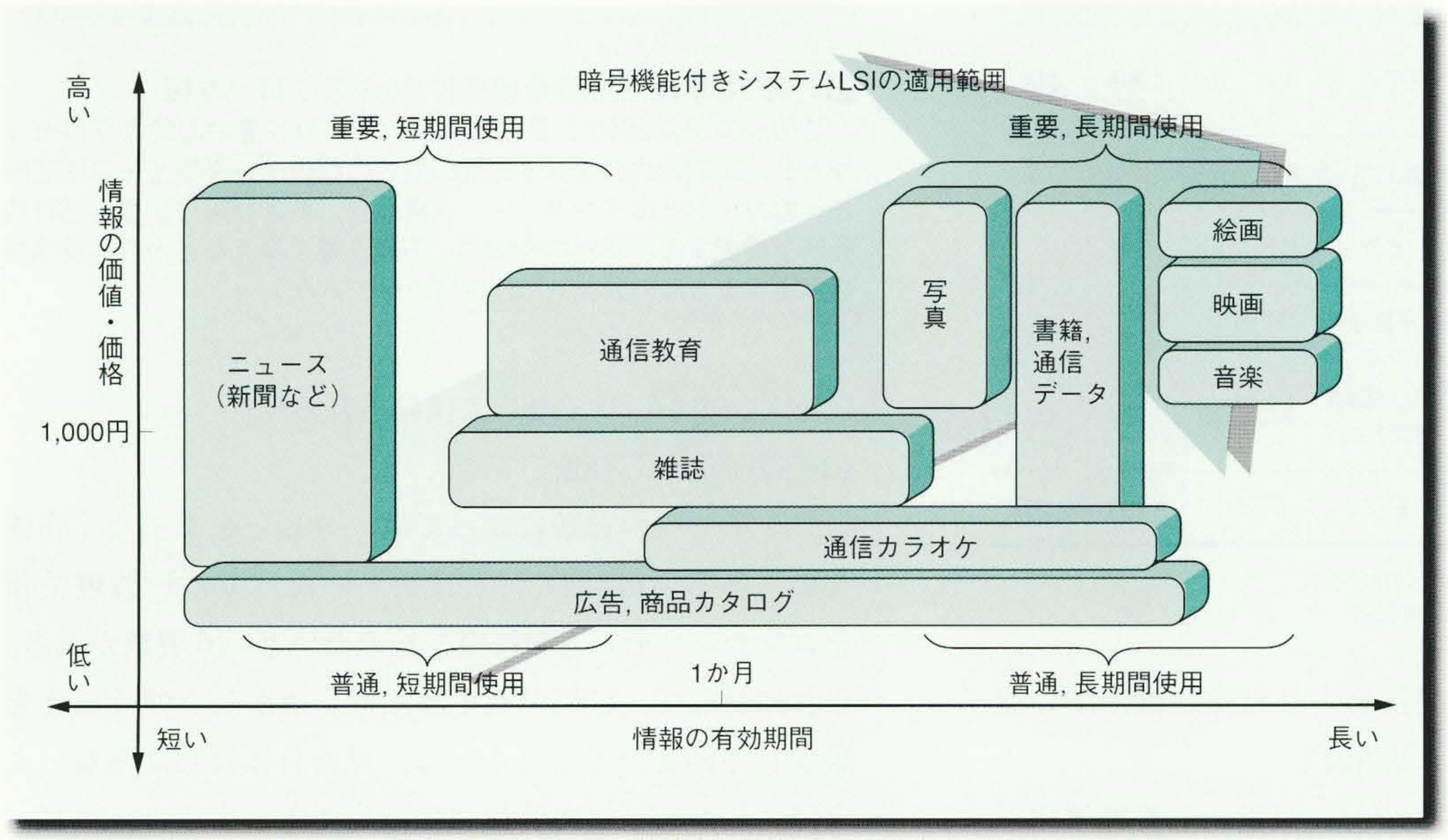
# 暗号機能付きシステムLSIとその応用

## System LSIs with Cryptographic Function and Their Applications

宝木和夫　*Kazuo Takaragi*　荒井孝雄　*Takao Arai*
中田邦彦　*Kunihiko Nakada*　原　秀幸　*Hideyuki Hara*
山田　徹　*Tôru Yamada*




**暗号による保護を必要とするディジタルデータ**

インターネットなどで使われるディジタルのデータは，情報の価値や価格の高いほど，また情報の有効期間の長いほど，不正行為の対象としてねらわれる傾向がある。暗号機能付きシステムLSIは，このようなデータを不正行為から保護するために使われる。

インターネットの急速な発展をきっかけとして，金融情報や画像など，実にさまざまな大量の情報がディジタルデータに変換され，高速に伝送されるようになった。しかし，これらディジタルデータは，盗み見や改ざんなど，第三者に悪用される危険性をはらんでおり，情報セキュリティ(安全性)対策が急務となってきている。この問題を解決する基本となる技術が暗号であり，特に暗号機能付きシステムLSIを用いる方法が注目されている。

日立製作所は，ディジタル放送など，種々のシステムに適用可能なMULTI2暗号LSIなどを提案し，急速なディジタル化時代のニーズにこたえている。

## 1　はじめに

インターネットをきっかけにして，われわれが日ごろなじんできた文書や音声，画像などのさまざまな情報が，ディジタルデータに大量に変換されるようになってきた。ディジタルデータは，0-1ビットの集まりであり，インターネットで送信したり，コンピュータ上で容易に切り張りなどができる。そうした便利さの反面，ディジタルデータには，簡単に盗まれたり，改ざんや不正利用されるという情報セキュリティ(安全性)面での問題がある。現に，インターネット上での不正行為の被害が急速に増えている。

この問題を解決する基本となるのが，暗号技術である。暗号はシステムLSIの一部として組み込まれ，そこを通過するデータは，暗号に変換される。暗号変換されたデータは，インターネットのような危険な場所に送出されても，不正利用や改ざんがされないように保護される。

ここでは，電子商取引や著作権保護，自動料金収受方式の標準化に関連した新しい暗号機能付きシステムLSI利用の動き，代表的な暗号である公開かぎ暗号“RSA”と共通かぎ暗号“MULTI2”をそれぞれ内蔵した二つのシステムLSI製品，およびその応用例について述べる。

## 2　セキュリティ確保技術の必要性と現状

一般に，データの価値や価格の高いほど，また有効期間の長いほど，保護の必要性が高い傾向がある(上の図参照)。この分野のデータを扱うビジネスでは，情報セキュリティ対策に不備があれば大きな損害を被るおそれがあるので，情報セキュリティ技術に対して大きなニーズが生じる。

最近，情報セキュリティ技術の業界標準化が進んでいる(**表1**参照)。日立製作所は，それらの幾つかで暗号方

**表1 主な業界標準化の動き**

国内外で業界標準化の動きが急である。そこで決められた暗号アルゴリズムを内蔵したシステムLSIがメーカーから供給される。

| 種別 | 機 関 | 標準化内容 | 代表的技術 | 採択暗号 | 採択年 | 関連記述 |
|---|---|---|---|---|---|---|
| 国際標準 | SETCo | インターネット利用電子商取引手順 | SET v1.0 | RSA, DES | 1998 | 3章 |
| | MAOSCO | 電子商取引用ICカード方式 | MULTOS v3 | RSA, DES | 1998 | 3章 |
| | CPTWG | ディジタル著作物の不正コピー防止方式 | 5C | だ円, M6 | 1998 | 2.1節 |
| | | | (電子透かし) | (評価中) | 1999(予定) | |
| 国内標準 | 郵政省 | CS, BSディジタル放送の限定受信 | (CS, BS限定受信方式) | MULTI2 | 1994 | 4章 |
| | 運輸省 | 高速道路の自動料金収受方式 | ETC | (評価中) | 1999 | 2.2節 |

注：略語説明 CS(Communication Satellite)
BS(Broadcasting Satellite)

式を提案してきた[1]。そこで決められた標準は，暗号機能付きシステムLSIの形で実現される。

このような標準化の流れの中で，最近新しく標準化され，注目されている技術について以下に述べる。

### 2.1 不正コピー防止システム

以前，大容量のDVD(Digital Video Disc)が出現したとき，劣化のない複製物などが容易に作成できるので，無許可の再頒布や加工編集が頻繁に行われるのではないかという問題が浮上した。近年の高性能パソコンの出現が，この問題に拍車をかけている。1996年5月，MPAA(映画業界)，CEMA(家電業界)，ITI(コンピュータ業界)が参加した，映画のコンテンツ(内容)などの不正コピー防止技術を議論する“CPTWG(Copy Protection Technical Working Group)”が結成された。

この不正コピー防止技術は，次の3要素に分けられる。

(1) コンテンツの暗号化

DVDでは，映像や音声などのコンテンツは，CSS(Contents Scramble System)と呼ばれる暗号システムを用いて暗号化される。正規のDVDプレーヤでは，DVDの再生機能にこの暗号を解く回路が内蔵されており，元のコンテンツを復元する。

(2) ディジタル インタフェース バスの暗号化

家電製品やコンピュータなどの間を接続するネットワーク上のデータを保護するため，暗号をかけて伝送する。この暗号システムはDTCP(Digital Transmission Copy Protection)と呼ばれ，暗号方式として日立製作所のM6暗号が採用された。詳細情報は，日立製作所のほか，株式会社東芝，松下電器産業株式会社，ソニー株式会社，Intel Corp.からライセンス供給される[2]。

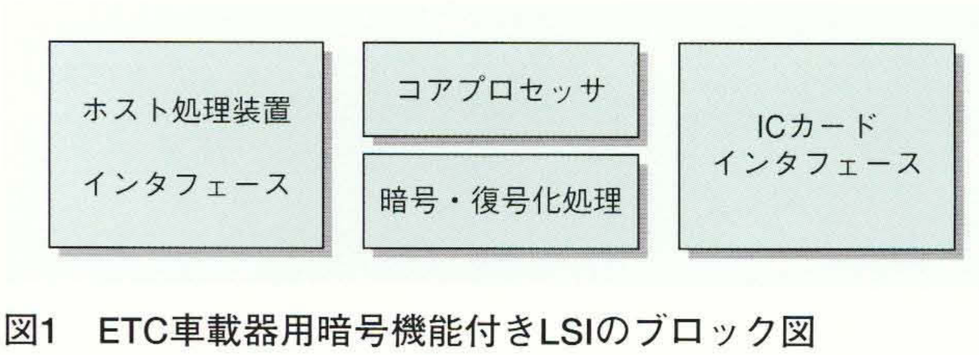



**図1 ETC車載器用暗号機能付きLSIのブロック図**

このシステムLSIは，日立製作所のマイコンを中心的なプロセッサとし，車載器内のホスト処理装置との間のインタフェース機能部と，ICカードとのインタフェース機能部，および暗号・復号処理機能部で構成する。チップ全体に，不当な書き換えなどから内部情報を保護するための耐タンパ性を持たせている。

(3) 電子透かし技術

コンテンツの種類によっては，コピーをまったく許さない，あるいは1回だけ許すといった，コピー管理情報をコンテンツそのものに書き込みたいという要求がある。これに対して，CPTWGでは，電子透かしを使うことを議論している。電子透かしは，見た目にはわからないように，しかし正規の装置には認識できるように，コピー管理情報をコンテンツの中に埋め込むものである。この電子透かしとコンテンツは容易に切り離せないようにして，コンテンツの不当利用を防止する。日立製作所は“Galaxy”(加盟企業：日立製作所，IBM Corp.，日本電気株式会社，パイオニア株式会社，ソニー株式会社)に参加し，国際標準化活動を進めている。

### 2.2 ETCシステム

ETC(Electronic Toll Collection：自動料金収受)システムは，無線通信によって有料道路の料金を自動的に支払い，料金所でのノンストップ通行を可能とする，新しい道路交通用のシステムである。

ETCのサービスを受けようとする車両には，あらかじめ専用の車載器が搭載される。利用者は契約情報などが記録されたICカードを車載器に挿入し，有料道路を走行する。車両が有料道路の料金所に近づくと，アンテナを通じて車載器が暗号化されたデータを無線で送り，車両を停止させることなく，料金支払いなどが自動的に行われる。

日立製作所は，このETC用の車載器のセキュリティ機能を集約した暗号機能付きシステムLSIを開発中である(**図1**参照)。

一方，既存の標準を実現するLSIの利用も拡大している。代表的な実現例について以下に述べる。

## 3 電子決済システムICカード用LSI

磁気カードなどに比べて偽造されにくく，かつディジ

タル署名や暗号処理を行えるICカードが注目されている。

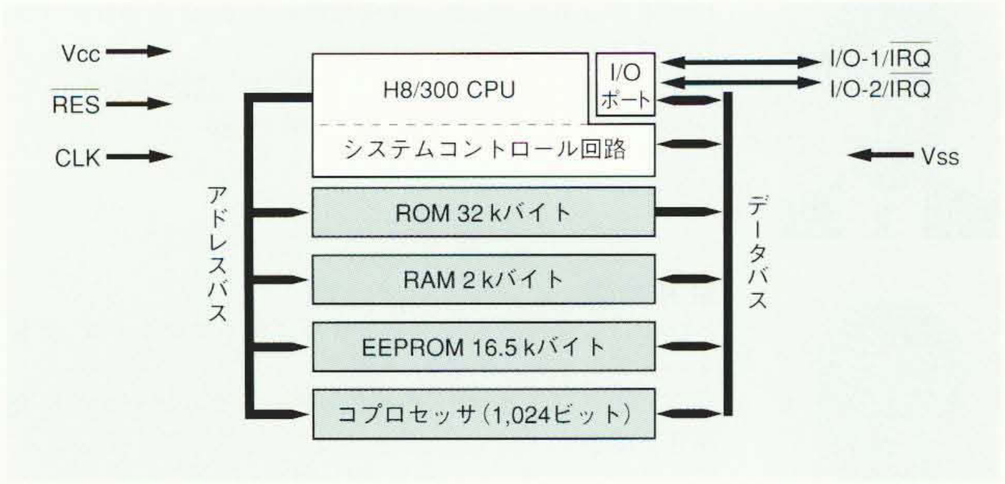
ICチップにCPU(Central Processing Unit)などを内蔵したICカードは「スマートカード」とも呼ばれており，高いセキュリティを持つ。例えば，金融情報などの特にセキュリティが要求される情報を，内蔵の不揮発性メモリに格納することにより，外部からのデータの改ざんや複製などの不正行為を防ぐことができる。また，ICカード用マイコンにより，種々の暗号処理が実現できる。

日立製作所は，1986年からICカード用マイコンを生産し，1995年には，電子決済システム用途として，暗号処理を高速化するコプロセッサを内蔵したICカード用マイコンを量産化した。

電子決済システム用途に開発したICカード用マイコン“H8/3113”のブロック図を**図2**に示す。H8/3113は，高性能8ビットCPU，大容量の不揮発性メモリEEPROM(Electrically Erasable Programmable Read-Only Memory)，ROM(Read-Only Memory)，RAM(Random Access Memory)を内蔵している。CPUは，EEPROM内のデータ管理や入出力端子による通信制御のほか，送受信データの暗号化処理などを行う。CPUにより，日立製作所のMULTI2[3]や米国暗号標準DES(Data Encryption Standard)などの共通かぎ暗号を高速に処理することができる。

H8/3113は，さらに，公開かぎ暗号のデファクトスタンダード(事実上の標準)的存在であるRSA暗号などを高速に処理するコプロセッサを内蔵している。これにより，1,024ビットのべき乗剰余演算を約0.5秒で実行できる。

また，日立製作所は，次世代の公開かぎ暗号方式として近年注目されている「だ円曲線暗号」をH8/3113上で処理するプログラムを開発した。これを使えば，上述した1,024ビット演算によるRSA暗号と同様の安全性を持つ，160ビットだ円曲線暗号“ECDSA(Elliptic Curve Digital Signature Algorithm)”[4]を約0.2秒で生成することができる。




注：略語説明
Vcc(電源)，RES(リセット)，CLK(クロック)
I/O(入出力)，IRQ(割込み要求)，Vss(接地)

**図2　H8/3113のブロック図**
H8/3113は，高性能8ビットCPU，大容量の不揮発性メモリEEPROM，ROM，RAMを内蔵している。CPUにより，日立製作所のMULTI2や米国暗号標準DESなどの共通かぎ暗号，およびRSAやだ円曲線暗号などの公開かぎ暗号を高速に処理することができる。


注：略語説明
RISC(Reduced Instruction Set Computer)
OS(Operating System)，I/F(Interface)

**図3　ICカード用マイコンのロードマップ**
ICカード用マイコンは今後も進化し，メモリ容量やコプロセッサ，さらに非接触機能などが充実していく。

日立製作所のICカード用マイコンのロードマップを**図3**に示す。今後，メモリ容量のバリエーションをそろえた標準品「H8/3160シリーズ」では，コプロセッサを内蔵した製品群のラインアップを充実し，さらに，非接触仕様にも対応していく考えである。また，不揮発性メモリEEPROMの実現技術や，0.35・0.18 μmなどの微細化プロセス技術，高性能CPUアーキテクチャ技術などを駆使することにより，使いやすく，信頼性の高いICカード用マイコンを今後も開発していく。

## 4　ディジタル放送システム用LSI

### 4.1　ディジタル放送と暗号

長らくアナログ技術でサービスが提供されていたラジオやテレビ放送にも，ディジタル化の波が押し寄せている。ディジタル化を可能にした主なものは，画像・音声のディジタル圧縮技術と暗号技術である。特に暗号技術は，ディジタル情報の保護に必要な(1)スクランブル，(2)限定受信(有料放送契約に基づく視聴管理)，(3)コピー防止などを，安全かつ効率的に行うことを可能にする。

### 4.2　ディジタル放送のスクランブル技術

ディジタル放送を立ち上げる際に，暗号技術によるスクランブルがいち早く導入された。アナログの場合は，走査線の順序を入れ替えるなど間接的な手段によってスクランブルを実現している。ディジタル放送では，映像・音声がディジタル化されており，細分化された0-1ビットの信号ごとに暗号を直接適用してスクランブルを

**表2　世界の主要なスクランブル方式**

ディジタル放送用暗号では，わが国はMULTI2を，欧州はDVBをそれぞれ統一的に採用している。米国は，事業者ごとに独自の方式を採用している。

| 地　域 | 方　式 | 備　考 |
|---|---|---|
| 日　本 | MULTI2 | 統一規格 |
| 欧　州 | DVB | 統一規格 |
| 米　国 | (DES) | 放送事業者ごとに独自採用 |

注：略語説明　DVB(Digital Video Broadcasting)

実現することにより，高い秘匿性を得る。

また，ICカードによる契約管理機能とスクランブルかぎ管理機能を融合することにより，試聴した分だけを払う「ペイ パー ビュー」やインタラクティブ(対話型)サービスなどのさまざまな有料放送の形態に対応するシステム構築が可能となった。

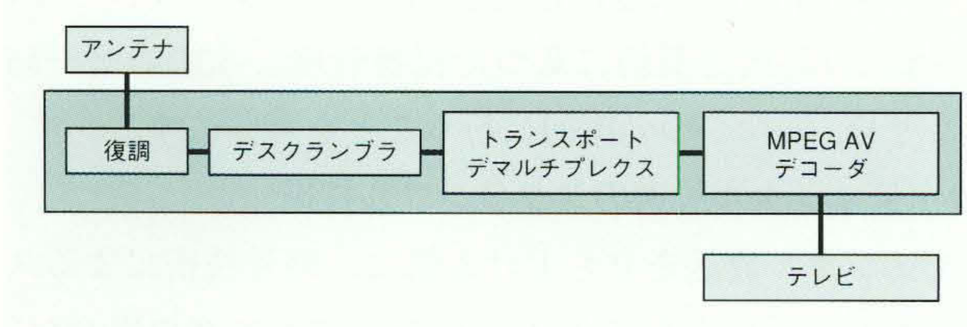
わが国のディジタル放送のスクランブル方式は，日立製作所が開発したMULTI2暗号[3]に一本化されている。これは，メディア横断的にインターオペラビリティ(相互運用性)を確保することによって普及を促進するという目的によるものである。1996年から開始されたCS(通信衛星)放送で実現されており，2000年にはBS(放送衛星)放送で実施され，その後，地上波ディジタル放送，地上波ディジタル音声放送，衛星ディジタル音声放送と実施されていく予定である。

世界の主要なスクランブル方式を**表2**に示す。

### 4.3　暗号機能付きディジタル放送LSI

ディジタル放送受信機の機能概要を**図4**に示す。

日立製作所は，ディジタル放送受信機用のシステムLSIとしてHD814250というLSIを開発している。HD814250は，暗号機能としてMULTI2デスクランブラを含むとともに，国際標準規格ISO/IEC13818準拠のMPEG2トランスポートデマルチプレクサなど多数の標準化対応の技術を盛り込んだLSIである。




注：略語説明　MPEG(Moving Picture Expert Group)
AV(Audio-Visual)

**図4　ディジタル放送受信機の機能概要**

アンテナで受信されたデータはデスクランブラでMULTI2方式によって復号され，さらに，MPEG AVデコーダで伸張(データ圧縮の逆操作)された後，テレビに送られて視聴が可能な情報になる。

## 5　おわりに

ここでは，標準化に関連した新しい暗号機能付きシステムLSI利用の動きと，製品およびその応用例について述べた。

今後も，ディジタル化の進展とともに，暗号機能付きシステムLSIの利用は拡大していくものと考える。日立製作所は，ディジタル化時代のニーズに合わせた技術の開発と製品やシステムの提案を進めていく考えである。

### 参考文献など

1) 佐々木，外：進歩する情報システムセキュリティ技術と日立製作所の取組み，日立評論，**81**，6，388～392(平11-6)
2) DTLA(Digital Transmission Licensing Administrator), http://www.dtcp.com/
3) Hitachi, Ltd.：MULTI2, Registration of Cryptographic Algorithms, ISO9979/0009, NCC, UK(1994)
4) IEEE P1363, Standard Specifications for Public Key Cryptography, http://grouper.ieee.org/groups/1363/draft.html(1999)

### 執筆者紹介

**宝木和夫**
1977年日立製作所入社，システム開発研究所 セキュリティシステム研究センタ 所属
現在，暗号と情報セキュリティ技術の研究に従事
工学博士
情報処理学会会員，電子情報通信学会会員，電気学会会員，IEEE会員
E-mail：takara@sdl.hitachi.co.jp

**中田邦彦**
1982年日立製作所入社，半導体グループ システムLSI事業部 ICカード設計部 所属
現在，ICカードマイコンLSIの設計・開発に従事
E-mail：knakada@cm.musashi.hitachi.co.jp

**山田　徹**
1985年日立製作所入社，宇宙技術推進本部 宇宙システム設計部 所属
現在，ディジタル衛星放送技術の開発・設計に従事
E-mail：tyamada@cm.ssd.hitachi.co.jp

**荒井孝雄**
1968年日立製作所入社，デジタルメディアグループ デジタルメディア製品事業部 所属
現在，ディジタルオーディオ，ディジタルビデオの研究開発に従事
E-mail：t-arai@cm.tookai.hitachi.co.jp

**原　秀幸**
1978年日立製作所入社，電力・電機グループ 大みか制御本部 情報システム開発部 所属
現在，自動料金収受システム用車載LSIの開発に従事
E-mail：hara@omika.hitachi.co.jp