Vol.88 No.07 592-593

*Professional Report*

# 公開鍵暗号HIME(R)〔ハイムアール〕を中心とした日立の暗号化技術

Hitachi's Cryptographic Technologies Focusing on Public Key Cryptosystem HIME(R)

寶木 和夫 Kazuo Takaragi　西岡 玄次 Mototsugu Nishioka

**低消費電力性などに優れ，携帯電話やICカード，ICタグなどで暗号化に有利な日立の公開鍵暗号「HIME(R)」（ハイムアール）がISO世界標準として採択された。HIME(R)は，平文メッセージを入力したとき，(1) $p^dq$の形の3個以上の素数の積を法とし，(2)指数2のべき乗暗号変換を，(3) OAEP(Optimal Asymmetric Encryption Padding)変換という手法を併用しながら行うという，安全性と高速性を両立させる3種類の処理を組み合わせる点が特徴である。これにより，従来のデファクト方式RSA-OAEPと比べて，より強い形で最強安全性IND-CCM2（Indistinguishable Against Adaptive Chosen Ciphertext Attack)を実現しつつ消費電力を10分の1程度に低減することができた。この開発により，従来から開発し，世界トップレベル性能のデジタル署名実装技術ECDSA-wNAF，およびISO世界標準となった日立のストリーム暗号MUGI，MULTI-S01とを併せ，ユビキタス情報社会にふさわしい軽量かつ安全性に優れた暗号のラインアップを提供することが可能となった。**

寶木　和夫
1977年日立製作所入社
システム開発研究所 所属
現在，情報セキュリティの研究に従事
IEEE会員，IACR会員，電子情報通信学会会員，情報処理学会会員，電気学会会員
工学博士

西岡　玄次
1990年日立製作所入社
システム開発研究所
第7部 所属
現在，暗号の研究に従事
IACR会員，電子情報通信学会会員

## 1　はじめに

現在，ユビキタス情報社会が進展中である。例えば，携帯電話，非接触ICカード，あるいは，ICタグなど無線機能を持つ小さな電子装置〔広い意味でのRFID (Radio-Frequency Identification)〕の出荷数は年々増加している。これらRFIDは，人々の日常生活から交通，健康医療，産業基盤，さらに，政府，通信・資源インフラへと広く適用範囲を拡大することが検討されており，近いうちに社会の主要な機能になっていくと予想されている。ここで問題になるのが，セキュリティである。小さな装置ゆえに，誰かに簡単に手に取られ不正行為を仕掛けられる危険性がある。例えば，駅の改札でよく見かけるように，多数のRFIDが一つのサービス側装置に対して次々に交信を行うシーンが生じる。そこでは，RFID自体の成り済ましがされていないこと，データの改ざんや盗聴がされていないことなどを保証することが，安全性や業務の信頼性を確保するうえで重要となる。多対1の通信においては，RFIDの回路規模が許せば暗号化鍵（公開鍵）と復号化鍵（秘密鍵）配布の仕方も同様に多対1の構造を持つ公開鍵暗号が有力な対策手段になる。

従来，日立製作所は，耐タンパー楕（だ）円曲線暗号技術ECDSA-wNAFを用いることで公開鍵暗号に備わる高セキュリティ特性に加え，高速な認証処理も可能にしたデジタル署名技術を開発するなど，安全性と高速処理を共に実現する非接触型ICカード搭載認証システムの開発に努めてきた[1)]。しかし，認証機能だけでは電波盗聴によるデータ暴露を防ぐことはできない。2005年4月に施行された個人情報保護法に伴うプライバシー保護の機運の高まりの中，非接触型ICカードから送出されるデータに対しても暗号化を高速に行う技術

が求められていた。

今回開発し，ISO世界標準として採択されたHIME(R)[2),3)]は，前述のような送信者多数，受信者１の応用環境において，1kビット程度の短いデータを高速に暗号化することを特徴とし，例えば，電子決済システムにおいては，公開鍵暗号による暗号化処理時間は最短で１ミリ秒以下を達成し，従来の認証処理時間（15ミリ秒程度）にほとんど影響を与えずに暗号化処理を追加できるようになった。

ここでは，HIME（R）の新技術について述べ，関連技術として日立が開発した世界最高レベル性能を持つECDSA-wNAFや，ISO世界標準として採択されたストリーム暗号MUGI，MULTI-S01とを併せ，日立製作所がユビキタス情報社会に推し進める強セキュリティ向けラインアップ暗号として，有効に活用可能なことを示す。

## 2　公開鍵暗号とは

よく知られているように，データを暗号化するための方式として，共通鍵暗号（対称暗号）と公開鍵暗号（非対称暗号）がある。簡単に言うと，同一の暗号化鍵（暗号化するための鍵情報）と復号化鍵（復号化するための鍵情報）を用いてデータの暗号・復号化を行うのが共通鍵暗号であり，異なった鍵を用いて暗号・復号化を行うのが公開鍵暗号である。公開鍵暗号では，暗号化鍵を公開できるので（このことから，暗号化鍵を公開鍵と呼ぶこともある。），任意のユーザーが暗号文を作ることが可能となり，共通鍵暗号のように鍵情報を共有するためのプロセスを必要としない。

公開鍵暗号の安全性については，1990年の後半ごろから，安全性のモデルが確立され，暗号アルゴリズムの安全性証明の手法の研究が進み，理論的かつ体系的な議論ができるようになってきた。公開鍵暗号の安全性は，「攻撃レベル」と「安全レベル」の組み合わせによって定義される。

まず，公開鍵暗号に対する攻撃は次のように分けることができる。

（1）選択平文攻撃（CPA：Chosen Plaintext Attack）

攻撃者は，常に任意の平文に対する暗号文を手に入れることができる環境にある。このとき，攻撃者は与えられた（ターゲットの）暗号文に対して攻撃を行う。

（2）非適応的選択暗号文攻撃

（CCA1：Non-adaptive Chosen Ciphertext Attack）

攻撃者は，解読したいターゲットとなる暗号文が与えられる前にのみ，任意の暗号文に対して，その復号化結果を手に入れることができる環境にある。このとき，攻撃者は与えられた（ターゲットの）暗号文に対して攻撃を行う。

（3）適応的選択暗号文攻撃

（CCA2：Adaptive Chosen Ciphertext Attack）

攻撃者は，常に任意の暗号文（ターゲット以外）に対して，その復号化結果を手に入れることができる環境にある。このとき，攻撃者は与えられた（ターゲットの）暗号文に対して攻撃を行う。

公開鍵暗号では，暗号化鍵は公開されているため，常に任意の平文に対する暗号文を手に入れることができる環境にある。よって，公開鍵暗号では，少なくとも選択平文攻撃に対して安全である必要がある。また，暗号通信の際に復号化結果の一部などをリプライとして返信する場合などには，選択暗号文攻撃に対する安全性が必要になる。上記の定義から，適応的選択暗号文攻撃が最も強力な攻撃レベルである。

次に安全性レベルの分類について述べる。

（1）一方向性（OW：One-Wayness ）

攻撃者にとって，暗号文からメッセージ文全体を求めることが難しい。

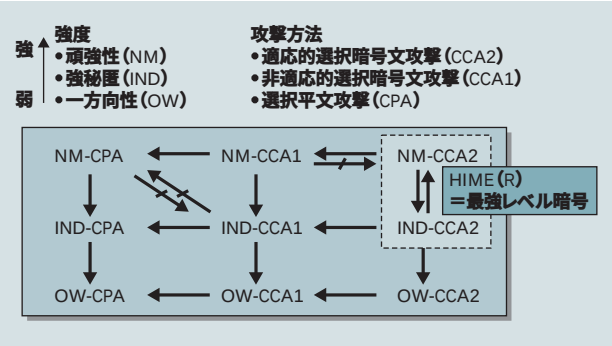
（2）強秘匿（IND：Semantic Security/Indistinguishability）

攻撃者にとって，暗号文からメッセージ文に関するいかなる（non-trivial な）部分情報も求めることが難しい。

（3）頑強性（NM：Non-Malleability）

攻撃者にとって，与えられた暗号文 C に対して，C の平文と（non-trivial な）関係 R を満たすメッセージ文を持つ暗号文 $C_i$（および関係 R）を求めることは難しい。

安全性のフォーマルな定義については，他文献に譲る。上記の下，公開鍵暗号の安全性は，「攻撃レベル」と「安全レベル」の対によって表現される。例えば，ある公開鍵暗号は IND-CCA2 の意味で安全であるとは，適




注：略語説明　NM（Non-Malleability），IND（Indistinguishability），OW（One-Wayness），CCA2（Adaptive Chosen Ciphertext Attack），CCA1（Non-adaptive Chosen Ciphertext Attack），CPA（Chosen Plaintext Attack）

**図1　公開鍵暗号の安全性の分類**

**HIME(R)は，最大の攻撃である選択的暗号文攻撃にも耐える最強レベルの暗号である。**

応的選択暗号文攻撃（CCA2）に対して semantic security（IND）の意味での安全性を持つことを意味する。**図1**は，公開鍵暗号における安全性の概念の関係について示したものである〔文献4）から引用〕。ここで，A → B とは，公開鍵暗号が A の意味で安全であるならば，それは B の意味でも安全であることを意味する（A ↛ B は，それの否定）。IND-CCA2 と NM-CCA2 は等価であることが知られており，最も高いレベルの安全性の概念であると考えられている。

## 3　公開鍵暗号HIME(R)

### 3.1 特徴

HIME（R）は，合成数 $n=p^dq$（d>1）を法とするRabin暗号タイプの公開鍵暗号であり，次の特徴を持つ。

（1）安全性

ランダムオラクルモデル上で $n=p^dq$型の素因数分解問題の計算量困難性を前提としてIND-CCA2の意味で安全である（第2章参照）。

（2）効率性

（a）nが1,024ビット長の場合，RSA※）暗号に比べ，暗号化で約10倍，復号化で約2〜3倍の高速処理性能を持つ。

（b）楕円曲線暗号に比べて，メッセージ空間を大きくとれる。メッセージ文に対する暗号文の長さの比が１に近い。

（c）小さなメモリサイズで実装可能である。

HIME（R） では，合成数$n=p^dq$ のビット長について，1,024ビット程度ではd=2を推奨している。しかし，4,096ビットのように長く取りたい場合には，d=3とすることで，d=2の場合に比べて，復号化処理において約40%の効率性アップが得られる（後述の3.4参照）。このように，$n=p^dq$（d>1）タイプの合成数を法に選び，独自の高速計算方法を用いることにより，計算機の高速性に対応して将来的に大きくなるnのビット長に対して，dの値を（nの素因数分解問題が難しい範囲内で）変えることにより，復号化処理の向上が得られるメリットがある。

※）RSAは，RSA Security，Inc.の商標である。

### 3.2　安全性

HIME（R） では，最強レベルの安全性であるIND-CCA2を実現するために，Bellare[5]らによって提案された OAEP（Optimal Asymmetric Encryption Padding）の手法を利用している。HIME（R）では，ランダムオラクルモデル上でIND-CCA2の意味で安全であることと，$n=p^dq$の素因数分解の困難性は等価であることが証明できる。一方，従来のRSA，および，RSA-OAEPでは，この等価性が完全に保証されているわけではなく，これは安全性におけるHIME（R）の優位性を示すものである。ここで，ランダムオラクルモデルとは，ランダム関数をオラクル（神託）として利用するモデルであり，システムのユーザーおよび攻撃者は，ランダムオラクルに対して質問を行い，その結果（乱数）を得ることができる。わかりやすく説明しよう。ランダムオラクルとは，日本語で言えばサイコロ振りの神様である。1から6の目が出る確率が厳密に1/6になるようなサイコロを利用できる存在のことである。このような理想的サイコロを人間業で作ることは難しい。例えば，何かのはずみでサイコロの角が1分子でも多く欠ければ，各目が厳密に1/6の確率で出るサイコロではなくなる。

HIME（R）では**図2**に示すようなランダムオラクルを想定し，それをコンピュータの処理によって擬似的に実現する。ここで想定するランダムオラクルは，メモリ，および，各目の出る確率が厳密に1/6となるようなサイコロを持っている。データwが入力されると，まず，

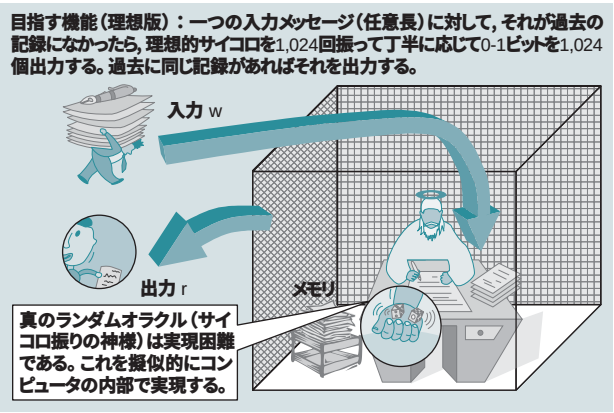



**図2　ランダムオラクルモデルとは**
**ランダムオラクル，日本語で言えばサイコロ振りの神様をコンピュータで擬似的に実現する。**

メモリを検索してデータwがすでに記録済みであるかどうかを調べる。もし，記録済みでなければ，サイコロを1,024回振って，それぞれの回で丁か半になるかによって，0か1のビットを選び，トータル1,024ビットを得る。そして，この1,024ビットを出力するとともに，データwと1,024ビットのペアをメモリに記録する。もし，上記データwの入力時に，データwがすでにメモリに記録済みであれば，ペアとして記録されている1,024ビットを出力する。このようなランダムオラクルは，同じデータが入力されたときは，必ず同じ出力を出すので一種の関数になっている。

実際には，既存のハッシュ関数SHA256などを用いて擬似的にこの機能を実現している。しかし，このようなランダムオラクルモデル特有の前提を用いても，有効な安全性指標を与えると考えられる。また，通常の計算機モデル上で安全性証明可能な暗号方式に比べて，効率的な暗号化・復号化処理が可能なアルゴリズムが数多く存在する。ISO 世界標準として認可されたすべての暗号アルゴリズム（ACE を除く）がランダムオラクルモデル上での安全性証明な公開鍵暗号である。

### 3.3　HIME(R)の暗号化・復号化

HIME（R）の暗号化処理を図3に示す。900ビットのメッセージmが入力されたら，124ビットの固定データ（オールゼロのデータ）をその後ろに結合する。そして，ランダム関数を使って1,024ビットの乱数rを生成する。乱数rをランダム関数Gに入力して1,024ビットのG（r）を得る。そして，上記の最初に生成した1,024ビットとG（r）のビットごとの排他的論理和をとる。つまり，

$$z=(m\|00\cdots0)\oplus G(r) \quad \cdots\cdots (3)$$

の計算を行う。さらに，得られたzをランダム関数Fに入力してF（z）を得，乱数rとF（z）のビット毎の排他的論理和をとる。つまり，

$$y=r\oplus F(z) \quad \cdots\cdots (4)$$

の計算を行う。さらに，得られたyの2乗（平方剰余）を計算する。つまり，

$$c=y^2 \bmod n \quad \cdots\cdots (5)$$

を計算する。得られた1,024ビットのcが暗号文である。ここで，式（5）の計算がべき乗剰余算を含み，処理時間を多く要する部分である（図4参照）。このように，

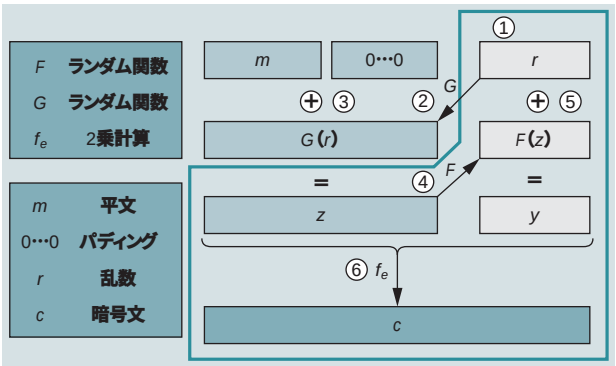



**図3　HIME(R)の暗号化処理**
**平文メッセージに固定パターン（オールゼロ）を接続したものに対して，ランダム関数を用いた処理を行った後，2乗（平方剰余）したものが暗号文となる。**

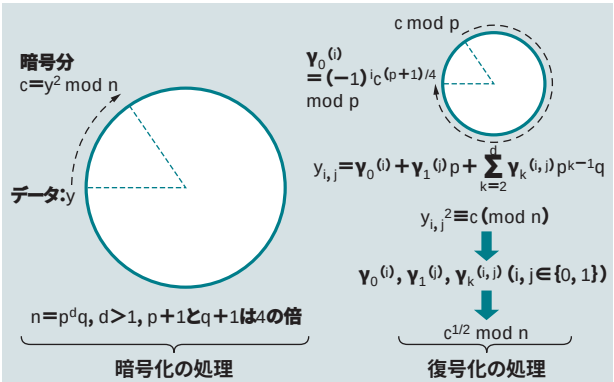



**図4　HIME(R)の主要な処理**
**処理途中のデータyを法 n（=p^d q）のもとで2乗した c=y² mod n が暗号文となる。復号化においては，上記のような $y_{i,j}$（i,j∈{0,1}）を $\gamma_0^{(i)}$，$\gamma_1^{(i)}$，$\gamma_k^{(i,j)}$ の各値を計算することで，暗号文 c の平方根を求める。**

HIME（R）の暗号化処理においては，ハッシュ関数値の計算などのほかには，たった１回の剰余乗算を行うのみである。

HIME（R）の復号化処理は**図5**のように行われる。復号化に用いる秘密鍵はnの素因数であるpとqである。さきほどの暗号化処理と逆方向の処理となるが，HIME（R）では，独自の高速計算法を用いて，

$$y = c^{1/2} \bmod n \quad \cdots\cdots (6)$$

を得る。このとき，正しい平文に対応するyの値として4とおりの候補が得られる。このうち正しいyの選定方法は種々あるが，その一例としては，4とおりのyに対して，**図5**に示す復号化の残りの処理を進める方法がある。(6)の処理が終わると，

$$m \| 00\cdots0 = G(r) \oplus z \quad \cdots\cdots (7)$$

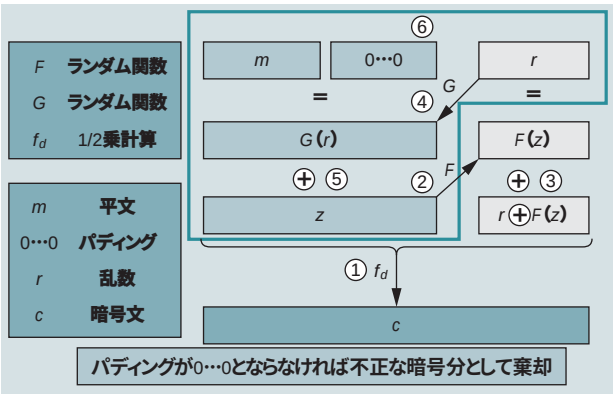



**図5　HIME(R)の復号化処理**
**暗号文に対して，秘密鍵である素因数を用いて1/2乗計算を行う。その結果に対して，さらに，ランダム関数を使った処理を行い，復元された平文メッセージに続いて固定パターンが現れれば受理し，現れなければ棄却する。**

| 暗号方式 | 法nの長さ（ビット） | 暗号化乗算剰余回数 | 復号化乗算剰余回数 | 素因数分解問題との等価性 | ISO標準 |
|---|---|---|---|---|---|
| RSA-OAEP | 1,024 | 2〜1,536 | 388 | △ | ○ |
| Rabin-SAEP | 1,024 | 1 | 388 | ○ | × |
| HIME(R) ($n=p^2q$) | 1,024 | 1 | 124 | ○ | ○ |
| RSA-OAEP | 2,048 | 8〜12,288 | 3,088 | △ | ○ |
| Rabin-SAEP | 2,048 | 4 | 3,088 | ○ | × |
| HIME(R) ($n=p^2q$) | 2,304 | 6 | 1,347 | ○ | ○ |
| HIME(R) ($n=p^3q$) | 3,072 | 9 | 1,320 | ○ | ○ |
| RSA-OAEP | 4,096 | 32〜98,324 | 24,640 | △ | ○ |
| Rabin-SAEP | 4,096 | 16 | 24,640 | ○ | × |
| HIME(R) ($n=p^2q$) | 4,096 | 16 | 4,104 | ○ | ○ |
| HIME(R) ($n=p^3q$) | 4,928 | 23 | 5,411 | ○ | ○ |

**表1　HIME(R)の高速性，安全性比較**
**HIME(R)は，素因数分解の困難性に基づく同類の従来方式（RSA，Rabin）と比べて安全性面，速度面で優れている。**

のように復号化結果のmの後ろに，00…0のように0が124ビット続いているものがあれば，それが正しい平文mとなる。正しく処理された場合，4とおりの異なるyに対して，1とおりのyだけが式(7)の形式を満足する。もしも，式(7)のような形が一つも現れない場合，不正な暗号文が入力されたものとみなして処理を止め，その由の警告信号を発する。詳細は文献[2), 3)]を参照されたい。

### 3.4　性能

RSA-OAEP，Rabin-SAEPと HIME（R）の暗号化および復号化における剰余乗算の個数の比較を**表1** に示す。ここでは，HIME（R）と同様，素因数分解問題の困難性を安全性の根拠とする安全性証明可能な方式を取り上げた。RSA 暗号のような乗法群の演算により，暗号化および復号化計算を行う暗号方式の場合，（一つの目安として）剰余乗算の個数により暗号化および復号化の効率性（速度）の比較評価を行うことができる。これは実際の計算処理において，剰余乗算の計算コストが大きいことによる。nが1,024 ビット長の場合，HIME（R）は16ビット暗号化鍵の RSA-OAEPと比べて，暗号化で約 10倍，復号化では約2〜3倍の高速処理能力を持つ。また，**表1** からわかるように，計算機の発展とともに将来的に鍵長（nのビット長）が大きくなった場合においても，合成数$n=p^dq$におけるdの値を（nの素因数分解が困難な範囲で）変えることにより，HIME（R）の効率面における優位性はいっそう増すことになる。

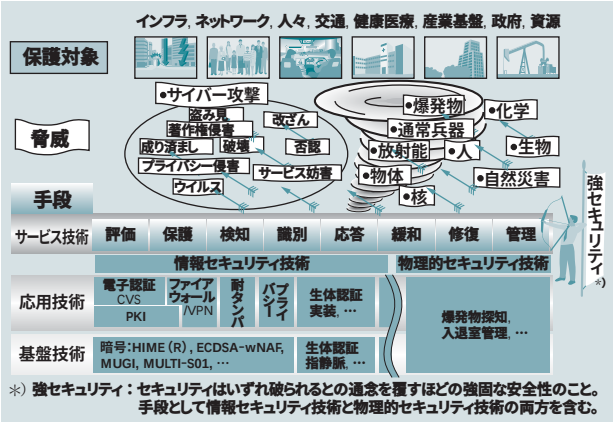
## 4　他の暗号との補完関係

現在，本格化しつつあるユビキタス情報社会をにらみ，HIME（R）で実現されるような比較的短い情報の秘匿だけでなく，通信相手の認証，情報の改ざん防止，著作権保護，プライバシー保護といった多様な要求が本格化するのに向けて，さまざまな要求に対応できる暗号方式が必要となる。日立製作所はデファクトの利点を生かせる公開鍵暗号RSAやブロック暗号AES，MULTI2，ハッシュ関数SHA256などを製品化するとともに，前述のHIME（R）のほか，小型の電子機器でデ

参考文献など
1）宝木：情報セキュリティ技術，日立評論，87，5，463～468（2005.5）
2）M. Nishioka，et al.："Design and analysis of fast provably secure public key cryptosystems based on a modular squaring，" Proceedings of ICISC2001，LNCS2288，pp. 81－102，Springer -Verlag，2001
3）ISO/IEC 18033-2："Encryption Algorithms - Part 2 : Asymmetric Ciphers"，International Organization for Standardization (ISO)，Switzerland，May 2006
4）M. Bellare，et al.：Relations among notions of security for public-key encryption schemes，Crypto'98，LNCS 1462，pp.26－45，Springer-Verlag
5）M. Bellare，et.al.：Optimal asymmetric encryption – How to encrypt with RSA，Eurocrypt'94，LNCS 950，pp.92 - 111，Springer-Verlag，1994

| 技術分類 | 日立製規格暗号 | 従来デファクト暗号 |
|---|---|---|
| 公開鍵暗号（暗号化用） | ○ HIME（R）暗号化で 1ミリ秒（ICカード） | △ RSA暗号化で 5ミリ秒（ICカード） |
| 公開鍵暗号（認証用） | ○ ECDSA-wNAFで 15ミリ秒（ICカード） | △ RSA署名で 140ミリ秒（ICカード） |
| 共通鍵暗号（本体部） | ○ MUGI暗号化で 14.4 Gバイト/s（専用LSI） | △ AES暗号化で 2.3 Gバイト/s（専用LSI） |
| 共通鍵暗号（運用モード） | ○ MULTI-S01で データ秘匿と改ざん検知 | △ CBCで データ秘匿のみ |

**表2　各暗号のデファクト方式との比較**
**ユビキタス情報社会においてさまざまな用途，電子機器向けに種々の暗号が必要になる。日立製作所では，従来のデファクト標準暗号を有効活用しながらも，特徴を持つ暗号技術も独自に開発，国際標準化，製品化を行うことで，そのような要求に応えている。**




注：略語説明　CVS（Certificate Validation Server），VPN（Virtual Private Network），PKI（Public Key Infrastructure）

**図6　強セキュリティの実現に向けて**
**強セキュリティの実現に向け，基本となる暗号技術は他技術とのシステマティックな連携が重要となる。**

ジタル署名を生成するのに適したECDSA-wNAF，大容量データの暗号化に向いたストリーム暗号MUGIやMULTI-S01を独自に開発し，すべて製品化して良好な結果を得ている。開発技術は**表2**に示すようにデファクト技術に比べ高速性などで優位なものであり，消費電力などの使用条件に制約が生じやすいユビキタス情報機器において有効に用いることが可能である。

## 5　強セキュリティの実現に向けて

企業において，最近多発している個人情報漏洩事件や内部情報不正操作事件を契機に，情報そのものの安全性をいかに確保するかに注意が向けられている。さらに，世の中全体を見れば，2001年9月11日の米国同時多発テロ事件以降，情報の不正操作に連動して生じる物理的攻撃，あるいはテロの危険性も増している。従来，セキュリティとはどちらかというと最低限の防止でよく，事件が起きるまでは放っておかれる傾向があったが，これからはそうはいかない。ある種の設備，システムにおいては，セキュリティ事故は決して起きてはならないもので，情報，物理の両面から対策が必要となる。

日立製作所は，従来から強セキュリティの概念を提案している[1)]。強セキュリティとは，「セキュリティはいずれ破られるという通念を覆すほどの強固な安全性」のことであり，手段としては情報セキュリティと物理セキュリティの両方を含む。ユビキタス情報社会においては，例えば，無線機能を持つ小さな電子装置（RFID）が入退室管理，不正者追跡などの物理的安全性確保に役立つ一方で，それ自身が容易に不正に操作される対象になり得る。今回，開発したような暗号機能は基本ではあるが，それとともに**図6**に示す多数の要素技術との連携により，システム全体として強セキュリティを確保することが重要となる。

## 6　おわりに

ユビキタス情報社会において，安全性を確保するうえで基本となる暗号として，日立製作所が開発したHIME（R）の技術内容と関連する暗号技術との位置付け，狙う効果などについて述べた。

最後に，この開発にあたって貴重なご討論をいただいたドイツ・ダルムシュタット工科大学のブックマン教授はじめ関係者の方々，日立製作所のセキュリティ関連技術の研究者の方々，製品化に携わった事業部の方々をはじめ関係各位に深く感謝の意を表す。