技術の原点

ユークリッド復号法

Euclidean Decoding Method

平澤茂一 Shigeichi HIRASAWA
笠原正雄 Masao KASAHARA

アブストラクト　誤り訂正符号の代数的復号法の一つであるユークリッド復号法について解説する．ユークリッド復号法は BCH 符号や RS 符号の強力な復号法として知られ，数多くの適用例がある．まず，1950 年代に始まった誤り訂正符号の構成法の研究と，1960 年代から 1970 年代にかけての復号法の研究の歴史をたどり，ユークリッド復号法の位置付けを行う．次に，ユークリッド復号法の概要を紹介する．最後に，この復号法発見に至る筆者らの当時の環境や様子を，研究者の立場から経験談に私見を交えながら述べる．

キーワード　代数的復号法，ユークリッドアルゴリズム，誤り訂正符号，LSI，Goppa 符号，BCH 符号，RS 符号

1. はじめに

第 2 次世界大戦が終わって間もないころ，米国ベル研究所の中堅研究者 R. W. Hamming(注1)は，手動計算機では到底実行できないような問題をリレー式計算機で計算をしていた．当時の素子の信頼性は低く，コネクタの接触不良も多い．しかも動作速度は遅く，今日の PC があっという間に片付ける計算にも数日間を要することから，計算途中で停止したり暴走したりして結果が全く無に帰すのは残念でならない．そこで，少しくらいの誤りならこれを訂正し，計算を続行したい．有名なハミング符号はこのために考え出されたといわれている 1 ビット誤り訂正符号である．ほぼ同時期に登場した M. J. E. Golay によるゴーレイ符号とともに誤り訂正符号の理論がつぼみを付けたのである．両符号の論文発表は 1949–1950 年である．折りしも，C. E. Shannon の情報理論の誕生と相携えて，現在の情報化社会のインフラストラクチャを支える重要な理論が産声を上げたわけである(注2)．

その後，誤り訂正符号は 1950 年代に精力的な研究が続けられ，後に広く知られる巡回符号・BCH (Bose–Chaudhuri–Hocquenghem) 符号・RS (Reed–Solomon) 符号・RM (Reed–Muller) 符号・ファイア (Fire) 符号など現在でも重要な役割を持つ符号のほとんどが，この時期に発見されている．そしてこの分野の研究は 1961 年 W. W. Peterson による有名な著書 *Error-Correcting Codes* で一気に開花する(注3)．

1950 年代に発見された符号が，1960 年代後半に入ってそのプリミティブなものが（例えば，コンピュータの主メモリに）使われ始め，誤り検出符号としてコンピュータ通信の ARQ (Automatic Repeat reQuest) 方式に採用されている．

誤り訂正符号の性能を効率良く引き出すために，1960 年代から 1970 年代にかけて復号復号法が進化を遂げた．代表的なものに Peterson (Peterson–Gorenstein–Zierler) 復号法・Berlekamp–Massey 復号法・Berlekamp–Welch 復号法などがある．ユークリッド (Euclidean) 復号法[1]もここに入る．ユークリッド復号法は日本発のシンプルで理解しやすい復号法として知られ，多くのテキストに紹介されており，また実用化された例も多い．なお，これらの代数的復号法の計算量は，符号長を n とするとき，$O(n \log^2 n)$[2]から $O(n^3)$ 程度である．

この後，ゴッパ (Goppa) 符号の発見を契機に代数幾何符号の研究が進展し，1990 年代にはターボ符号とその復号法が精力的に研究された．このころ，ユークリッド復号法など代数的復号法を複数回用いて，最ゆう復号を達成する方法も数多く研究された(注4)．その後 2000 年代にかけて，1962 年 R. G. Gallager によって提案された低密度パリティ検査符号 (Low density parity check codes) が再発見され，復号計算量が $O(n)$ 程度と小さくなる特徴を生かした研究が盛んに行われている．

平澤茂一　正員：フェロー　サイバー大学 IT 総合学部
E-mail　hira@waseda.jp
笠原正雄　名誉員：フェロー　大阪学院大学情報学部
E-mail　kasahara@ogu.ac.jp
Shigeichi HIRASAWA, Fellow (Cyber University, Tokyo, 162-0853 Japan), Masao KASAHARA, Fellow, Honorary Member (Osaka Gakuin University, Osaka, 564-8511 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.4 No.3 pp.183–191 2011 年 1 月

(注1)：平澤は 1979 年 UCLA を訪問していたとき，J. Pearl 教授がゼミナールの前に Hamming 博士を紹介して下さる機会があった．当時計算機科学科のゼミナールは，毎回学外の著名な研究者を招いて講演会形式で進められていた．ユークリッド復号法についてもスライドに 1 行だけ触れられていたのを記憶している．
(注2)：誤り訂正符号の理論 (Theory of Error Correcting Codes)，あるいは符号理論 (Coding Theory) は情報理論に組み込まれることもあるが，異なる代数的手法を用いるため多くの場合別の体系として扱われている．
(注3)：1999 年，日本国際賞を受賞した Peterson 教授の功績は，今日の情報化社会の基礎としての符号理論の確立にあった．
(注4)：例えば、初期のもの[3]など．

1970 年代に開発された復号法は，1980 年代に入って LSI 化され，現在も我々の身の回りで活躍している．深宇宙通信・衛星通信・移動体通信などやコンピュータ通信・インターネット・携帯電話・CD (Compact Disk)・DVD (Digital Versatile Disk)・コンピュータの主メモリや補助メモリ (RAID ハードディスクを含む) など，日ごろ気がつかないところにも浸透している．もし情報の信頼度が低ければ，コンピュータの計算結果を信じることはできないし，火星から送られてくる画像を鮮明に見ることもできないであろう．ビルの谷間における携帯電話のクリアな通話も，地上ディジタルテレビ放送のくっきりした画面も全て符号理論が支えてくれている．通信や記憶における情報の信頼性が低いならば，銀行の ATM を使って現金の出し入れもできないであろう．符号理論が実用化されなければ，今日の社会は成り立たないのである．しかし，符号理論はめったにテレビの話題になることもない．情報基盤を担う地味な縁の下の力持ちなのである．

以下では，ユークリッド復号法の概要を説明する．復号器を開発した当時の資料を参考に，実際に試作した LSI についても触れる．更に，この復号法発見に至る筆者らの当時の環境や様子を，研究者の立場から経験談に私見を交えながら述べる．

なお，本稿は笠原・平澤が十分意見を交換・調整をしながら執筆している．ただし，書き下しは 1., 2., 4. を主として平澤が，3., 5. を主として笠原が担当した．

2. 代数的復号法

2.1 復号手順と基本方程式[1],[4]～[6]

q 元 (n,k,d)BCH 符号を考える．ここで，$q\,(\geqq 2)$ は素数のべき乗，n は符号長，k は情報記号数，d は最小距離である．$GF\left(q^m\right)$ 上の原始元を α とする生成多項式 $G(z)$ は $\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{2t}$ の $2t$ 個の連続根を持つ．**符号多項式**$x(z)$，**受信多項式**$y(z)$，**誤り多項式**$e(z)$ を，

$$\begin{aligned} x(z) &= x_0+x_1z+x_2z^2+\cdots \\ &\qquad \cdots+x_{n-1}z^{n-1}\ \left(x_i\in GF(q)\right), \qquad (1)\\ y(z) &= y_0+y_1z+y_2z^2+\cdots \\ &\qquad \cdots+y_{n-1}z^{n-1}\ \left(y_i\in GF(q)\right), \qquad (2)\\ e(z) &= e_0+e_1z+e_2z^2+\cdots \\ &\qquad \cdots+e_{n-1}z^{n-1}\ \left(e_i\in GF(q)\right), \qquad (3) \end{aligned}$$

と表す．ここで，$G(z)\mid x(z),x\left(\alpha^j\right)=0\ (j=1,2,\cdots,2t)$ を満足する．また，

$$y(z)=x(z)+e(z), \qquad (4)$$

である．このとき，$e(z)$ に生じた $2t+1\leqq d$ となる t 個の誤りを訂正することができる．

2.1.1 シンドローム多項式 $S(z)$

α^j に対するシンドロームを s_j とすると，

$$s_j=y\left(\alpha^j\right)=e\left(\alpha^j\right)\ (j=1,2,\cdots,2t), \qquad (5)$$

である．ここで，$s_j\in GF\left(q^m\right)$ である．もし誤りがなければ，$s_j=0\ (j=1,2,\cdots,2t)$ である．今，t 個以下の誤りの位置 $\mathscr{E}$ を

$$\mathscr{E}=\{i_1,i_2,\cdots,i_s\}\ (s\leqq t), \qquad (6)$$

すなわち，第 i_1+1，第 i_2+1，$\cdots$，第 i_s+1 番目に誤りが生じたとする(注5)．

$$\begin{aligned} s_j &= e_{i_1}\left(\alpha^j\right)^{i_1}+e_{i_2}\left(\alpha^j\right)^{i_2}+\cdots+e_{i_s}\left(\alpha^j\right)^{i_s}\\ &= \sum_{i\in\mathscr{E}}e_i\left(\alpha^j\right)^i, \qquad (7) \end{aligned}$$

である．ここで，

$$S(z)=s_1+s_2z+s_3z^2+\cdots+s_{2t}z^{2t-1}, \qquad (8)$$

と置く．このとき，$S(z)$ を**シンドローム多項式**という．これは，

$$S(z)=\sum_{i\in\mathscr{E}}\frac{e_i\alpha^i}{1-\alpha^iz}\ \left(\mathrm{mod}\,z^{2t}\right), \qquad (9)$$

と書き換えられる．なぜならば，$\frac{\alpha^i}{1-\alpha^iz}=\alpha^i+\alpha^{2i}z+\alpha^{3i}z^2+\cdots$，及び，

$$\begin{aligned} S(z) &= \sum_{j=1}^{2t}s_jz^{j-1}\\ &= \sum_{j=1}^{2t}\sum_{i\in\mathscr{E}}e_i\alpha^{ij}z^{j-1}\\ &= \sum_{i\in\mathscr{E}}e_i\sum_{j=1}^{2t}\alpha^{ij}z^{j-1}, \qquad (10) \end{aligned}$$

と表すことができるからである．

2.1.2 基本方程式

次に，

$$\sigma(z)=\prod_{i\in\mathscr{E}}\left(1-\alpha^iz\right), \qquad (11)$$

と置く．$\sigma(z)$ は $GF\left(q^m\right)$ 上の s 次の多項式で，誤り位置 $\mathscr{E}=\{i_1,i_2,\cdots,i_s\}$ に 1 対 1 に対応する $\alpha^{-i}\ (i\in\mathscr{E})$ から $\sigma(z)=0$ の根が求まれば位置が分かる．したがって，$\sigma(z)$ を**誤り位置多項式**という．式 (11) を式 (9) の両辺に乗じると，

$$\sigma(z)S(z)=\eta(z)\ \left(\mathrm{mod}\,z^{2t}\right), \qquad (12)$$

ただし，

$$\eta(z)=\sum_{i\in\mathscr{E}}e_i\alpha^i\prod_{l\neq i,l\in\mathscr{E}}\left(1-\alpha^lz\right), \qquad (13)$$

である．$\eta(z)$ を**誤り数値多項式**という．式 (12) は適当な関数 $\phi(z)$ を用いて，

(注5)：ここでは，記述を簡単にするために $\mathscr{E}\subset\{0,1,\cdots,n-1\}$ とする．したがって，$i\in\mathscr{E}$ は第 $i+1$ 番目の位置に誤りが生じたことを示す．

$$\sigma(z)S(z)+\phi(z)z^{2t}=\eta(z), \tag{14}$$

と書き表すことができる．式 (14) を**基本方程式** (key equation) という(注6)．この解法は次の **2.2** に示す．

2.1.3 誤り位置計算

基本方程式を解いて誤り位置多項式 $\sigma(z)$ が求まれば，α^{-i} を順次代入して $\sigma(\alpha^{-i})=0$ となる $i\in\mathscr{E}$，すなわち誤り位置を求める．これを**チェン** (Chien) **探索**という．二元符号であれば $e_i\in\{0,1\}$ であるから，誤り位置 i が分かれば $y_i\in\{0,1\}$ の 0 と 1 を反転させることによって復号は終了する．

2.1.4 誤り数値計算

非二元符号のとき，誤り数値 e_i を求めなければならない．式 (9) から $\sigma(z)$ の形式的微分 $\sigma'(z)$ を求めると，

$$\sigma'(z)=-\sum_{l\in\mathscr{E}}\alpha^l\prod_{i\in\mathscr{E},i\neq l}(1-\alpha^i z), \tag{15}$$

である．したがって誤り数値 e_i $(i\in\mathscr{E})$ は式 (13) から，

$$e_i=-\frac{\eta(\alpha^{-i})}{\sigma'(\alpha^{-i})}\ (i\in\mathscr{E}), \tag{16}$$

として求められる．

2.2 ユークリッドアルゴリズムの適用(4)〜(6)

ここでは，式 (14) の基本方程式の解き方について述べる．式 (14) では，既知である $S(z)$ と z^{2t} の最大公約多項式を求める**ユークリッド互除法**が使えることが分かる．$r_{-1}(z)=z^{2t}, r_0(z)=S(z)$ と置き，$\mathrm{GCD}(r_{-1}(z),r_0(z))$ を求める多項式のユークリッド互除法を実行する．このとき，剰余多項式の次数が初めて $t-1$ 以下となったときに停止すればよい．

すなわち，次のように示すことができる．

定理 1 (ユークリッド復号法)

$r_{-1}(z)=z^{2t}, r_0(z)=S(z)$ と置く．$\mathrm{GCD}(r_{-1}(z),r_0(z))$ を求める多項式のユークリッド互除法：

$$r_{i-2}(z)=q_i(z)r_{i-1}(z)+r_i(z), \tag{17}$$

$$\deg r_{i-2}(z)=\deg q_i(z)+\deg r_{i-1}(z), \tag{18}$$

$$\deg r_{i-1}(z)>\deg r_i(z),\ i=1,2,\cdots \tag{19}$$

を実行する．$\deg r_i(z)\leqq t-1$ のとき，これを停止する．このとき，

$$\sigma(z)=\gamma a_h(z), \tag{20}$$

$$\eta(z)=(-1)^h\gamma r_h(z), \tag{21}$$

で与えられる．ただし，γ は $\sigma(0)=1$ とするための係数であり，$a_h(z)$ は，

$$a_j(z)=-q_j(z)a_{j-1}(z)+a_{j-2}(z),\ j=1,2,\cdots,h \tag{22}$$

で与えられる．ここで，$a_{-1}(z)=0, a_0(z)=1$ である． □

なお，この復号法に要する計算量は $O(t^2)$ である．

例 1 (二元 $(15,5,7)$BCH 符号の誤り訂正)

二元 $(15,5,7)$BCH 符号を考える．$GF(2^4)$ の原始元 α を $GF(2)$ 上の x^4+x+1 の根とする．非ゼロの元は表 1 のように与えられる．ここで，$\alpha^{15}=1$ である．簡単のため送信符号多項式 $x(z)=0$, 受信多項式 $y(z)=z+z^4+z^6$ とする．したがって，$e(z)=y(z)$ である．

さて，シンドロームは，

$$s_1=\alpha+\alpha^4+\alpha^6=\alpha^{13}, \tag{23}$$

$$s_2=s_1^2=\alpha^{26}=\alpha^{11}, \tag{24}$$

$$s_3=\alpha^3+\alpha^{12}+\alpha^{18}=\alpha^{12}, \tag{25}$$

$$s_4=s_2^2=\alpha^{22}=\alpha^7, \tag{26}$$

$$s_5=\alpha^5+\alpha^{20}+\alpha^{30}=1, \tag{27}$$

$$s_6=s_3^2=\alpha^{24}=\alpha^9, \tag{28}$$

となる．したがって，

$$S(z)=\alpha^{13}+\alpha^{11}z+\alpha^{12}z^2+\alpha^7z^3+z^4+\alpha^9z^5, \tag{29}$$

である．

次に，$z^{2t}=z^6$ と $S(z)$ の最大公約数を求めるためユークリッド互除法を適用する．

$$r_{-1}(z)=z^6=(\alpha^6z+\alpha^{12})S(z)+r_1(z), \tag{30}$$

$$r_0(z)=S(z)=\alpha^8zr_1(z)+r_2(z), \tag{31}$$

$$r_1(z)=(\alpha^{13}z+\alpha^{13})r_2(z)+r_3(z), \tag{32}$$

表 1 $GF(2^4)$ **の非ゼロ元**

	α^3	α^2	α	1
α^0	0	0	0	1
α^1	0	0	1	0
α^2	0	1	0	0
α^3	1	0	0	0
α^4	0	0	1	1
α^5	0	1	1	0
α^6	1	1	0	0
α^7	1	0	1	1
α^8	0	1	0	1
α^9	1	0	1	0
α^{10}	0	1	1	1
α^{11}	1	1	1	0
α^{12}	1	1	1	1
α^{13}	1	1	0	1
α^{14}	1	0	0	1

ここで，

$$r_1(z)=\alpha z^4+\alpha^7z^3+\alpha^{11}z^2+\alpha^5z+\alpha^{10}, \tag{33}$$

(注6)：式 (12) を基本方程式と呼ぶこともある．

$$r_2(z) = \alpha^3 z^3 + \alpha z^2 + \alpha^5 z + \alpha^{13}, \tag{34}$$

$$r_3(z) = \alpha^{12} z^2 + \alpha^{14}, \tag{35}$$

$$\deg r_3(z) = 2 = t - 1, \tag{36}$$

であるから，ここで停止する．

一方，

$$a_{-1}(z) = 0, \tag{37}$$

$$a_0(z) = 1, \tag{38}$$

と置き，

$$a_1(z) = \left(\alpha^6 z + \alpha^{12}\right) + 0, \tag{39}$$

$$\begin{aligned} a_2(z) &= \alpha^8 z a_1(z) + 1 \\ &= \alpha^{14} z^2 + \alpha^5 z + 1, \end{aligned} \tag{40}$$

$$\begin{aligned} a_3(z) &= \left(\alpha^{13} z + \alpha^{13}\right) a_2(z) + a_1(z) \\ &= \alpha^{12} z^3 + \alpha^{10} z^2 + \alpha^{14} z + \alpha, \end{aligned} \tag{41}$$

から，

$$\sigma(z) = \alpha^{11} z^3 + \alpha^9 z^2 + \alpha^{13} z + 1, \tag{42}$$

を得る．

$\sigma(z) = 0$ を解いて，$z = \alpha^9, \alpha^{11}, \alpha^{14}$ を得る．$\alpha^i - z = \alpha^i\left(1 - \alpha^{-i} z\right)$ より，それぞれ，$\alpha^{-6}, \alpha^{-4}, \alpha^{-1}$ を用いて誤り位置 $\mathscr{E} = \{1, 4, 6\}$ となる．これは $e(z) = y(z)$ であることを示す． □

ここでは，二元符号を例に用いて説明したが，$q(>2)$ 元符号への拡張はさほど困難ではない．

2.3 試 作 機

ユークリッド復号法誕生時に筆者の一人・平澤が在籍した三菱電機株式会社で，1980 年代にその復号法をベースに開発された 3 世代にわたる試作機について説明しよう．第 1 世代は 1984 年頃，3 チップの LSI により実装されている[7],[8]．独自のフォーマット（三菱フォーマット）による RS 符号を用いた 130mm 追記形光ディスク用誤り訂正・誤り検出 LSI である．第 2 世代は 1987 年，RS 符号のフォーマットは ISO 規格に基づき標準化され 1 チップ化されている[9],[10]．第 3 世代は 1989 年，ROM も含め 1 チップ化されており，130mm 追記形・書換形光ディスク装置用で，90mm 書換形光ディスク装置用へとつながっていく[11]．ここでは，第 1 世代の試作機について述べる．

BCH 符号の非二元符号の一クラスである $GF(q)$ 上の (n, k, d)RS 符号は，$d = n - k + 1$ を満たす最大距離分離符号であり，性能が優れていることから連接符号の外部符号として利用されている．ただし，$n \leqq q + 1$ を満たさなければならない．$q = 2^m$ とした RS 符号は $2t \leqq d - 1$ を満たす t シンボル (バイト) 以下のランダム誤りを訂正でき，したがって $b \leqq m(t-1) + 1$ [ビット] のバースト誤りを訂正できる．1980 年代， RS 符号単独でも音楽用 CD(CD-DA) プレーヤ・PCM 録音機・DAT(Digital Audio Tape) 機器・磁気ディスク装置など

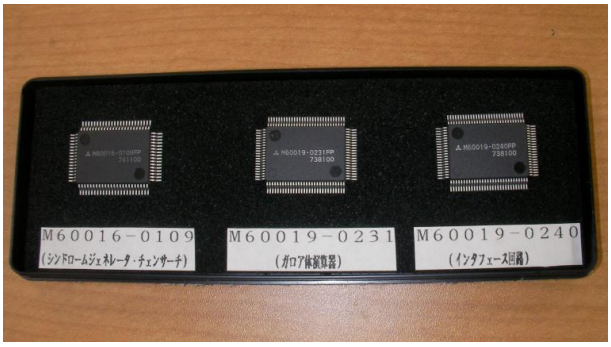


図 1 **誤り訂正・誤り検出 LSI**　左から (1) シンドロームジェネレータ・チェン探索部　(2) ガロア体演算器部　(3) インタフェース回路部

に用いられてきた．CD-DA は最小距離の小さい RS 符号を積符号形式に符号化し，中間でインタリーブした CIRC(Cross Interleaved Reed-Solomon Code) を用いている．

ここで取り上げるユークリッド復号法を用いた LSI は，130mm 追記形光ディスク用のもので，図 1 に示すとおり 3 種のゲートアレー LSI に分けられている．$GF(2^8)$ 上の $(146, 130, 17)$RS 符号の生成多項式は次式で与えられる．

$$G(z) = \prod_{i=0}^{15} (z - \alpha_i), \tag{43}$$

ここで，α は $GF(2^8)$ 上の原始多項式 $P(z) = z^8 + z^4 + z^3 + z^2 + 1$ の根，$\alpha_i = \alpha^{i+1}$ である．この符号を 4（または 8）相インタリーブしてセクタを構成する．

復号はユークリッド復号法を用いる．図 2 に全体の誤り訂正回路の構成図を示す．

各部の機能は次のとおりである．

(1) シンドロームジェネレータ・チェン探索部

式 (43) で与えられる符号のシンドロームを計算する．すなわち，受信多項式 $y(z)$ を入力し，式 (8) の $S(z)$ を出力する．これは線形帰還シフトレジスタ型の回路構成により，$y(z)$ を $(z - \alpha_j)$ で割った余り（剰余）s_{j+1} を求めればよい．これを，$j = 0, 1, \cdots, 15$ まで実行する．もし，誤りがなければ $(e(z) = 0), y(z) = x(z)$ であるから符号

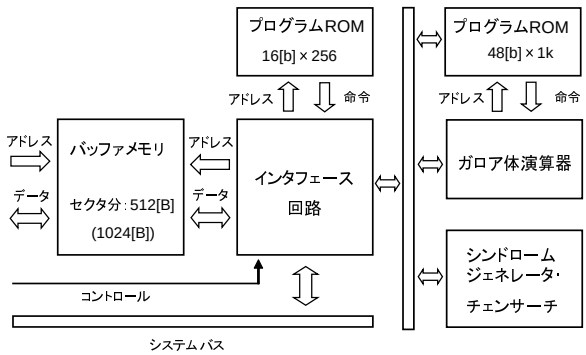


図 2 **誤り訂正回路の構成**　[b] はビット，[B] はバイト (8[b]) を表す

多項式 $x(z) = w(z)G(z)$ より $s_1 = s_2 = \cdots = s_{16} = 0$ となる． チェン（Chien）探索は基本方程式を解いて，誤り位置多項式 $\sigma(z)$ を求め，これに α^{-i} を順次代入し $\sigma(\alpha^{-i}) = 0$ となる $i \in \mathscr{E}$，すなわち誤り位置を求める．

(2) ガロア体演算器部

上記 (1) の部分は線形帰還シフトレジスタ型の回路構成に向いていた．しかし，ユークリッド互除法はハードウェアによるよりもアルゴリズムをプログラムで構成した方が実現しやすい．すなわち，ガロア体の多項式演算に適するアーキテクチャとして，$GF(2^8)$ 上の元の四則演算と 8 ビットの整数加減算を持つマイクロプログラム方式を採用し，プログラマブルな外部メモリ (ROM) により符号化・復号を行う．

(3) インタフェース回路部

図 2 のように (1) と (2) を結合し，高速なデータの転送を行うインタフェース回路である．回路規模は CMOS 8k ゲートアレーで，12MHz で動作する．

以上の構成により，基本クロック 12MHz で長さ 146Byte の単一符号語で生じた 8Byte 以下の誤りを 200μs 以下で訂正することができる．

その後，三菱電機の井上・山岸・吉田 3 氏らのグループは精力的な開発を進め，第 2 世代・第 3 世代と ISO 規格の標準化に適合した LSI を世に出している．

なお，符号化（符号構成法）は国際標準化されている．しかし，復号法はメーカーの自由である．性能はよくないがマイクロプロセッサを用いて低速・簡単・安価な復号器でもよいし，復号法を改良し高性能を引き出す工夫をしても良い．このように，メーカーが採用する復号法は標準化されない特徴がある．一方，復号法の LSI 化は技術をブラックボックスにし応用分野は進展するが，本質的な復号法の理解・改良・発展を妨げている面もある．

3. ユークリッド復号法，その履歴書

3.1 ユークリッド復号法，発見への道

1967 年秋からの 2 年間，笠原は米国ベル電話研究所（以後単にベル研究所，通常 Bell Lab. と呼ばれている）のホルムデル研究所で 400Mbit/s の超高速パルス通信の開発研究に携わっていた．

1965 年に大阪大学大学院工学研究科通信工学専攻博士課程を修了して「誤りを検出または訂正できる符号に関する研究」という今から考えると非常に大雑把な題名のもとに工学博士の学位を授与されていたので，ベル研究所所員になってからも余暇を見つけては誤り訂正符号の研究を続けていた．

こんなことから，同じベル研究所のマレーヒル研究所「符号理論研究グループ」の若き逸材，E. R. Berlekamp 博士と電話を通してお話をしていた．この交流が契機となって，出版直前の彼の著書 *Algebraic Coding Theory* の原稿全体のコピーを社内便で送ってもらった．図画はすべて手書き，それも走り書きという生々しい原稿であった．27 歳の若さでこんなすごい本を書くのか! カルチャーショックという表現を超えた驚きであった．秀逸そして斬新な内容に，笠原は**世界のレベルの高さ**を身近に，強く感じた．

帰国後，三菱電機在職中の平澤，故杉山博士とともに，土日祝日を利用しての勉強会が笠原の自宅で始まった．輪講のテーマはベル研究所で衝撃的な印象を受けたあの Berlekamp 博士の著書 *Algebraic Coding Theory* である．内容についての徹底的討論のスタートである．

厳しい輪講の中で得た結論の一つは “Srivastava 符号に大きな可能性あり” であった．

私たちの期待どおり，Srivastava 符号は幾つかの新しい発見をもたらしてくれた．例えば，その成果の一つは 1975 年に *IEEE IT Transaction* に掲載されている．

Srivastava 符号に大きな可能性があることを，私たちは Berlekamp 博士に伝えていたが，このことに対する回答が上記論文執筆中にあった．手紙には “ゴッパ符号により大きな可能性あり．ゴッパ符号を研究されよ” とあるではないか．

欧米の研究者の中で，いち早くゴッパ符号の秀逸性に気付いた人，その人こそ Berlekamp 博士であることを，後ほど知ることとなったが，私たちはそのときはこのことに気付かぬまま，Berlekamp 博士のアドバイスを素直に受け入れた．そして Berlekamp 博士から送ってもらったゴッパ符号についてのロシア語の論文を字引片手に読破した．そしてこのことがユークリッド復号法の誕生に結び付くこととなった．

3.2 ユークリッド復号法の誕生

3.2.1 ユークリッド復号法と Berlekamp 博士

ユークリッド復号法が土日勉強会の中で誕生したとき，実は喜びよりも不安の方がはるかに大きかった．“こんな簡単なアイデア，世界のどこかで既に発表されているのではないか?” という不安の方が大きかった．とにかくどこかの研究会で発表してみることも考えてみたけれど，“周知の考えとして，もの笑いになるかもしれない … ”，こんな心配が付きまとった．余りにも単純な考えであったからである．

しかし，とりあえず英文論文の形にまとめてみよう．私たちは数か月を費やして論文にまとめる作業をしていた．しかし，周知のことかもしれないという不安は解消されない．こんな悩みを払拭するために，書き上げた英文論文をそっくり Berlekamp 博士に送付するという選択を私たちは選んだ．

間を置かずに頂いた Berlekamp 博士からの手紙には，

“素晴らしい独創的なアイデアだ！ 実は自分は現在 *Information and Control* という雑誌の編集者を務めているが，編集者としての権限で即採録としたい．ただし *Information and Control* の発行部数は *IEEE IT Transaction* には及ばないの

で，IEEE への投稿を選択されてもよい．しかし，この場合は新たに査読者の選定作業等が入るので，世の中に出るタイミングが 1〜2 年遅れるでしょうね”
とあった．私たちは Berlekamp 博士の御好意に感謝するとともに，迷うことなく “*Information and Control* への掲載を希望する” という内容の手紙を送った．発行部数よりも早く世界に出した方がよい．私たちの選択である．

Berlekamp–Massey 復号法の考案者でもある Berlekamp 博士自身から，**独創的な素晴らしいアイデア**という最高の賛辞を頂いたこと，そして**即採録**という特段の御配慮を頂いたことは終生忘れることのできない記憶として残ることとなった．

3.2.2 ユークリッド復号法と嵩先生，そして Goppa 博士

符号理論の世界的権威，嵩先生とはキャンパスは異なるけれど同じ大阪大学ということで常に連絡を取り合っていたが，ある日，嵩先生から一通の手紙を受け取った．Goppa 博士の手紙のコピーが同封されていたと記憶するが，嵩先生直筆の字で，

“Goppa 博士からユークリッド互除法を用いた簡明な復号法を考えている，との手紙を受け取ったが，御提案の方法は日本人グループで発見され，既に周知のこととなっている，という回答をしておいた”
という内容の文章がつづられていた．

Goppa 博士は，嵩先生が符号理論の分野でのスーパースターであったからこそ，アイデアを思いついた瞬間に，このことを告げる手紙を送ったのである．これに対し嵩先生は間を置かず Goppa 博士に手紙を送って下さり，かつまた Goppa 博士はこの手紙を見てフェアプレーの精神で発表することを断念してくれた．このことによってユークリッド復号法についての**先陣争い**という日本人研究者には不利な戦場（いくさば）に駆り出されなくて済んだと思う．嵩先生の迅速な対応，Goppa 博士の寛大な判断によって救われたのである．

仮に Goppa 博士が嵩先生に手紙を送ることなく，また私たちの研究成果を知ることもなく，ロシア国内あるいはヨーロッパのどこかで発表していたなら，例え 1〜2 年こちらが早かったというしっかりした証拠が残っていたとしても，私たちのユークリッド復号法の先駆性を日本，アジアを含めた世界に認めさすためには耐え難い労力と長い年月の努力を強いられたことになったと思う．他の分野での幾つかの経験に基づくが，この戦場（いくさば）は研究とは全く無縁な余りにもつらい，過酷な世界である．

3.2.3 ユークリッド復号法と Sloane 博士，そして MacWilliams 博士

1960 年代後半〜1970 年代，笠原は IEEE ISIT に積極的に参加していた．1975 年ごろであったと思うが，ISIT に参加する直前，故 杉山博士とともにベル研究所の超高速通信研究グループ，そしてマレーヒル研究所の N. J. A. Sloane 博士を訪ねた．

Sloane 博士は数学者としての立場から，当時，与えられた符号長，冗長度に対し最大距離を有する符号の表（Best code table）の編さんに鋭意努力しており，世界中の研究者からデータを集めていた．

代数的符号の分野では，

- 符号構成問題
- 復号問題

がテーマとしての双璧であることに異論を挟む人は少ないであろう．1970 年代〜1980 年代，この二つの問題について私たちは基本的な部分を非常に精力的に取り組んでいた．符号構成問題については Sloane 博士の編さんした最良符号表において「KS 構成法」と名付けられた構成法，あるいは MacWilliams and Sloane 両博士による前述の著書[12] p. 583 の練習問題 13 の中で，

—The double tail construction has been successfully used by Kasahara et al. —
として紹介された「二重テイル構成法（double tail construction）」などがある．

英国の Honary and Markarian 両博士は一般化アレー符号（GAC）を提案し，1990 年代非常に精力的に研究を展開し，注目を集めていたが，1997 年に両博士によって出版された著書 *Trellis decoding of block codes*, 2.2 節の序言において，彼らの提唱する GAC の源流は 1970 年代提唱していた私たちの「アレー符号」にあるとして，

“This technique (GAC) generalizes the augmentation technique of Kasahara et al.”
と述べている[13]．この私たちの「アレー符号」は当時大きな注目を集め，MacWilliams and Sloane の著書[12]でも詳しく解説されている．

最良符号表の編さんという膨大な時間と忍耐を要する仕事を続ける Sloane 博士の良き協力者となるべく，私たちは発見した最良符号を逐次 Sloane 博士に報告していた．そのたびに Sloane 博士からは分厚い最良符号の最新データが送られてきていた．

こんなわけで Sloane 博士には初対面したという感じはなく，十年来の知己に久しぶりに会うという印象であった．Sloane 博士もそんな雰囲気で私たちを迎えてくれた．

彼のオフィスは早速ディスカッションの場となったが，この場には符号理論の女性研究者，というよりは気品あふれる貴婦人という印象の F. J. MacWilliams 博士も同席された．当時 MacWilliams and Sloane 両博士は名著 *The Theory of Error Correcting Codes*（1979 年出版）[12]を執筆中であった．

いろいろのテーマでディスカッションをしたが，ユークリッド復号法についての議論が一段落したとき，MacWilliams 博士は “Patterson 復号法[14]についてコメントをお持ちならば，聞かせてほしい”
と意見を求めた．私たちは Patterson 復号法との差を丁寧に説明した．

これに対し彼女は “私も同じ考えですよ” と優しくほほえみながら答えてくれた．そしてそれに続いて，彼女の口から出てきた言葉，私たちには忘れ難い内容の言葉であった．“実は Patterson は私の娘婿なのですよ” であった．このことが前もって分かっていたならば説明のトーンは微妙に変わっていたかもしれない．明白な差を何の気兼ねもなく堂々と論じた私たちの考えを終始ほほえみながら優しく受け入れてくれた MacWilliams

博士，忘れることができない研究者の一人である．

ユークリッド復号法の話が終わったとき，二人は，

“We like your Euclidean Decoding Algorithm among others!”

と力強く言ってくれた．

この言葉が通り一遍の言葉でなかったことを，この日から数年後に出版された MacWilliams and Sloane 著 *The Theory of Error Correcting Codes*[12] の p. 369 にある同じ内容の文章を読んで，私たちはしっかりと知ることができた．

自らが発見した手法に，自らが高い評価を与え，これを連綿として記述することはいかなる機会にも控えるべきであろう．その代わりに符号理論の世界だけでなく，数学の世界のスーパースターでもある Sloane 博士たちによる第三者評価を以下に紹介させて頂くことは許されよう．(Berlekamp 法など様々な復号法に対する最初の 13 行は省略し，残る 4 行を記述させていただく．)

“**Which decoding algorithm is best?**

—省略— Nevertheless, decoding using Euclidean algorithm is by far the simplest to understand, and is certainly at least comparable in speed with other methods ($n < 10^6$) and so it is the method we prefer.”[12]

両博士はベル研究所訪問時に言ってくれた言葉どおりに **best** と評価してくれた．

3.2.4 ユークリッド復号法は世界の舞台で活躍しているか?

“ユークリッド復号法は世界の舞台で活躍しているか?”

残念なことに私たちは，この問いかけに対しては，

“CD や DVD に記録されているコンテンツの高品質性を確保するために必須のツールとして活躍しているらしい”

ということをうわさ話として知り得ているだけである．解説論文等の文章の形での記事にも，三菱電機関係者の論文以外，いまだ接していない．何故であろうか．このことについての笠原の考えは別の機会が与えられれば詳しく述べてみたいと思うが，簡潔に述べれば，学会の縦割り的構造そして企業と学会との「距離を置いたぜい弱な関係」にある，ということであろう．

コンピュータの世界，メモリの世界，情報理論の世界とそれぞれに分かれ，これらを横につなぐ組織がない．研究者の研究面での自由な交流の場が乏しい．

“リードソロモン符号やユークリッド復号法がなければ，コンテンツの音そして絵は，実用に耐えず，CD や DVD を現在のような品質で楽しむことは到底できない．”

と言ってみたとしても，

“驚異的なヘッドの技術がすべてであった”

と反論されるだけかもしれない．昔，学生の一人が冗談半分で言ったことであるが，

“スイッチがなければ CD や DVD を楽しむことができない”

なのかもしれない．

とまれ専門分野が更に細かく分化し，互いの交流が日増しに薄れていくことを感じ，このことを憂慮する人は少なくないであろう．“自分の専門は何が専門なのか分からない…” こういった人たちがもっと増えていってもよいのではないか?

表 2　特許件数の比較

	P 法	BM 法	E 法
国内特許	87	160	284
海外特許	333	363	640

電子情報通信学会における会員減少の傾向，情報理論とその応用学会解消，これらの根底に専門分野の細分化の加速があると思う．

少し本題とずれたお話となってしまった．上記 “ユークリッド復号法の活躍は噂にしか聞いていない” の「勇み足」として日ごろ考えていたことを述べてしまったことをお許し願いたい．

さて，本題の “ユークリッド復号法は世界の舞台で活躍しているか?” に戻ろう．この問いかけに対する「Yes」を裏付ける客観的事実の一つとしては，日本だけでなく欧米出版の数多くの教科書において「シンプルで理解しやすい手法」として，かなりの紙幅を割いて解説されていることを挙げることができよう．

では実用の世界ではどうか? このことを裏付ける客観的事実としての「特許」を切り口にして，すなわち代数的復号法にかかわる特許を切り口にして考えてみよう．

代数的復号法の代表として，誕生の順に，

- Peterson 復号法（P 法）
- Berlekamp–Massey 復号法（BM 法）
- Euclidean 復号法（E 法）

を挙げることができよう．これらの復号法にかかわる内外の特許件数をネットを通じて調べてみると 2010 年 8 月の時点で表 2(注7) のようである．

表 2 によって実用の世界ではユークリッド復号法が主流となっていること，そして誕生した国，日本よりも，海外でその傾向が強いことが了解される．

4. ユークリッド復号法発見の裏話

4.1 笠原宅での休日ゼミ

ユークリッド復号法の最初の議論は，当時（昭和 47 年ごろから始まる）休日に故 杉山博士・平澤が笠原宅にお邪魔し，3 人でエンドレスのゼミをやった中であった．杉山博士が 1974 年 10 月に Notre Dame, IN, USA で開催された ISIT’74 に口頭発表[15]しているから，構想がまとまったのは 1973 年であると思う．E. R. Berlekamp の著書 *Algebraic Coding Theory* を輪講していて，Berlekamp–Massey の復号アルゴリズムが難解であることが発端である．したがって，アルゴリズムを追いかけプログラムを作り実行することは可能でも，ハードウェアに

(注7)：このデータは，

- 国内特許については，特許電子図書館「公報テキスト検索」（http://www7.ipdl.inpit.go.jp/Tokujitu/tjkta.ipdl?N0000=108）
- 海外特許については，米国特許庁「PatFT: Patents の advanced Search」（http://patft.uspto.gov/netahtml/PTO/search-adv.htm）

の特許検索システムを使用した全文のキーワード検索による結果である（2010 年 8 月 31 日現在）．

よる実現は困難であると思われた（当時のマイクロプロセッサのスピードから，プログラムで実現することは考えられなかった）．ゴッパ符号のゴッパ多項式 $g(z)$ が BCH 符号の場合，式 (12) の mod 計算が z^{2t} であり，これが式 (14) と等価であることがヒントである．式 (12)，式 (14) はいずれも基本方程式と呼ばれている．$S(z)$ は既知多項式，z^{2t} は定数，$\phi(z)$ をダミー多項式として，正整数の最大公約数を求めるユークリッド互除法に対し，多項式の最大公約多項式を求める計算をすればよい．この時点では，本当にこんな簡単な方法が先行研究にないのか，甚だ不安であった．しかし，ともかくたくさんの例題を分担して解き，アルゴリズムの停止条件，効率良いガロア体上の逆元の求め方などを検討した．かくして，ユークリッド復号法が出来上がったわけである．

4.2 ロシア語論文の杉山流読破法

Berlekamp 先生から頂いた V. D. Goppa の論文[16]～[18]は杉山博士が読破した．残念ながらロシア語ができるメンバーはいない．杉山博士は文法から取り組まないで，すべての単語を辞書で引いた．笠原宅のゼミの際配布される資料には，ことごとく単語の下に意味が書いてあった．まるで小学校 1 年生が 6 年生の教科書を読めるように，単語にルビが振られていたのである．ゼミが進むに従い，頻繁に用いる単語があるからだんだん単語のルビが減っていく．一方，数式はどんなに丁寧な説明より分かりやすい，この分野の共通言語である．このときほど，数式の力を思い知ったことはない．何を説明しているのか，極端にいえば式を追うだけで記述言語を問わず理解できる素晴らしい表現力を持っている．そのときの資料は，今はない．しかし，真っ黒になった資料は，記憶に残る素晴らしい私たちのまぎれもない key paper である．

4.3 三菱電機社内の評価

1975 年に *Information and Control* に掲載されたユークリッド復号法の論文[1]は，著者ら (杉山博士・平澤) が在籍した三菱電機社内で実用化するには時期尚早という評価であった．当時，アルゴリズムなどソフトウェア特許は，難しい局面であった．OR の分野で有名な**カーマーカ法**の特許が争われていたころである(注8)．米国で特許が申請された数理計画法の解法であるカーマーカ法に対し，中央大学教授・今野浩先生が裁判で争った事件がある．これと同時期であり，ユークリッド互除法は数論の定理でソフトウェア特許を取ることは困難であるというのが大方の見方であった．したがって，ユークリッド復号法は当時の三菱電機の特許にはなっていない．

このころ，杉山博士・平澤はこれから大々的に実用化される (であろう) というパーシャルレスポンス方式や変復調器（モデム）の特許出願に余念がなかった．また，よく知られた R. G. Gallager らの解説による ARQ 方式が全盛時代，本格的な実用化に向けて国際電信電話株式会社研究所（当時）と共同研究をしていた時代である．

一方，誤り訂正符号の実用化は最小距離が 4 の二元ハミング符号（いわゆる SEC/DED 符号）に対し，コンピュータ業界でようやく始まったばかりである．産業界では，最小距離 5 程度の BCH 符号が次々実用化されてきたが，誤り位置を高次の代数方程式を直接解いて求めることで十分である．符号長が大きく，保証する訂正個数も大きい符号・復号法の必要性は，当時の産業界には少なかった．1980 年代当初に音楽用 CD(CD-DA) の仕様が標準化され，家電業界で誤り訂正符号の復号法実用化のニーズが一気に高まるのである．これは 1970 年代，産業界で開発された先進技術が家電業界でも生かされるという図式が，1980 年代に入って逆転するという初期の顕著な例である．それほど量産効果が大きいということではなかろうか．その後，Philips 社・松下電器産業（当時）・NEC ほかが LSI 化し，CD プレーヤの心臓部として市場に出るようになる．前述のとおり，三菱電機でも LSI 化が進み，光ディスク装置やディジタルオーディオ分野などに適用されている．

5. むすびに代えて —Simple is best—

私たちがユークリッド復号法と命名した理由は何か．多くの符号，復号法には発見者の名が冠されている．リードソロモン符号，ビタビ復号法等，枚挙にいとまがない．しかし私たちは自らの名前を冠するということは全く考えていなかった．

笠原は最大公約数を求めるためのユークリッド互除法を学んだとき，その原理の神秘的な奥深さに感動し，すっかり興奮してその夜寝不足になったことを覚えている．読者諸賢にはこんな状況を理解してもらえないかもしれないが，実に奥深い．シンプルな考え，しかし高く高くそびえている！ 実際，このシンプルさ，奥深さによってユークリッド互除法は誤り制御技術，情報セキュリティ技術の両分野において，今日，トップにランクされる活躍をしている数学である．

本稿の本筋から話がずれて恐縮であるが，情報セキュリティ技術を支えるオイラーの定理もまた神秘的に奥が深い．この定理を学生たちに教える際には “真に学んだときは寝不足になることを覚悟せよ！” という気構え，迫力で教えてほしいと思う．必ず，学生たちは表面的な説明を越えた何か深いものを学ぶからである．

本題に戻るけれど，私たちが見いだした復号法にユークリッド復号法と名付けることは，以上の経緯によって，何の迷いもなかったのである．

本稿の結びに，僭越であるが，以下の言葉を記させて頂きたい．

“Simple is best,”

これが研究を進める上での基本である．より具体的には，

- 可及的優しい数学を使うこと
- 式はシンプル，そして可及的少なくすること

このことが基本の中の基本である(注9)．

(注8)：カーマーカ法が特許になるというのはおかしいと思う．しかし，1990 年代にアメリカでは特許となっている．日本では現在，ソフトウェア特許にはなっていない．

(注9)：そんなことが可能なのか？といぶかる読者には公開鍵暗号の代表として位

著者の一人・平澤は **2. 3** の試作機に関する資料収集に三菱電機・宮田好邦氏の御協力を頂いた．また，湘南工科大学・小林学先生にも貴重なコメントを頂いた．更に，閲読委員からも有益な御指摘を頂いた．心よりお礼申し上げたい．

最後に，執筆の機会を与えて下さった千葉大学グランドフェロー・中村勝洋先生，岐阜大学・毛利公美先生に感謝申し上げる．

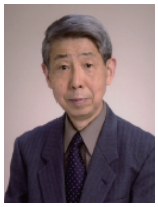
文　献

(1) Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, “A method for solving key equation for decoding Goppa codes,” Inf. Control, vol. 27, no. 1, pp. 87–99, Jan. 1975.
(2) J. Justesen, “On the complexity of decoding Reed-Solomon codes,” IEEE Trans. Inf. Theory, vol. IT-18, pp. 237–238, March 1976.
(3) T. Kaneko, T. Nishijima, H. Inazumi, and S. Hirasawa, “An efficient maximum-likelihood-decoding algorithm for linear block codes with algebraic decoder,” IEEE Trans. Inf. Theory, vol. 40, no. 2, pp. 320–327, March 1994.
(4) 平澤茂一，西島利尚，情報数理シリーズ (A-3)　符号理論入門，培風館，東京，1999.
(5) 平澤茂一，情報数理シリーズ (A-6)　情報理論入門，培風館，東京，2000.
(6) 情報理論とその応用シリーズ (3)　符号理論とその応用，情報理論とその応用学会（編），培風館，東京，2003.
(7) 山岸篤弘，吉田英夫，小田好明，尾崎　稔，井上　徹，“光ディスク用誤り訂正・検出 LSI,” 信学総大，1403, pp. 6-81, 1987.
(8) 井上　徹，山岸篤弘，吉田英夫，小田好明，“誤り訂正用 LSI,” 三菱電機技報，vol. 61, no. 9, pp. 732–735, Sept. 1987.
(9) 吉田英夫，松井　充，山岸篤弘，井上　徹，近藤潤一，井上善雄，尾崎　稔，“光ディスク用誤り訂正 LSI の開発，” 信学技報，no.IT88-65, ISEC88-28, pp. 53–60, Nov. 1988.
(10) 吉田英夫，山岸篤弘，井上　徹，石田禎宣，田中邦磨，“光ディスク用誤り訂正 LSI，” 信学論 (A)，vol. J73-A, no. 2, pp. 261–268, Feb. 1990.
(11) 森　信太郎，児玉幸夫，吉田英夫，井上　徹，清瀬泰広，“光ディスク用誤り訂正 LSI,” 三菱電機技報，vol. 65, no. 2, pp. 200–205, Feb. 1991.
(12) F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.
(13) B. Honary and G. Markarian, Trellis Decoding of Block Codes – A Practical Approach, Kluwer Academic Publishers, 1997.
(14) N. J. Patterson, “The algebraic decoding of Goppa codes,” IEEE Trans. Inf. Theory, vol. IT-21, no. 2, pp. 203–207, March 1975.
(15) Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, “A method for solving key equation for decoding Goppa codes,” ISIT 1974, Notre Dame, IN, USA, Oct. 1974.
(16) V. D. Goppa, “A new class of linear error correcting codes, (in Russian),” Probl. Pereda. Inf. vol. 6, pp. 24–30, 1970.
(17) V. D. Goppa, “Rational representation of codes and (L, g) codes, (in Russian),” Probl. Pereda. Inf. vol. 7, pp. 41–49, 1971.
(18) V. D. Goppa, “Some codes constructed on the basis of (L, g) codes, (in Russian),” Probl. Pereda. Inf. vol. 8, pp. 107–109, 1972.

（平成 22 年 10 月 20 日受付）

平澤　茂一（正員：フェロー）

昭 36 早大・理工・数学卒．昭 38 同・電気通信卒．同年三菱電機株式会社入社．昭 56 早大・理工・工業経営・(現 創造理工・経営システム）教授．平 21 同名誉教授．同理工総研研究員．同年サイバー大・IT 総合・教授．現在に至る．情報理論とその応用，データ伝送方式の研究，並びに計算機応用システムなどの開発に従事．工博．昭 54 UCLA 計算機科学客員研究員．昭 60 ハンガリー科学アカデミー，昭 61 伊トリエステ大客員研究員．平 5 本会小林記念特別賞，業績賞受賞．平 9 IEEE フェロー，平 20 IEEE ライフフェロー，情報理論とその応用学会，情報処理学会等各会員．



笠原　正雄（名誉員：フェロー）

昭 40 阪大大学院博士課程了．阪大助手，講師，助教授を経て昭 62 京都工繊大・教授．平 12 同大名誉教授．大阪学院大・教授．符号・暗号理論，情報倫理の研究に従事．平 5 年度本会小林記念特別賞，平 16 年度本会功績賞等受賞，IEEE ライフフェロー，著書「情報技術の人間学」など．

置付けられる RSA 暗号の原理がわずか数個の式で述べられることを見てほしい．RSA 暗号と同列に論じて大変僭越であるが，身近な例として，最近電子情報通信学会 ISEC 研究会（2010 年 9 月）で発表した公開鍵暗号 $K(II)\Sigma PKC$ もシンプルな一行だけの式，わずか 5 個でその原理が記述される．歳月がたたず，その安全性については必ずしも自信はないが，御高覧頂ければ幸いである．