研究解説

UDC 621.391.037.3

通信における符号化の役割

The Role of Coding in Communications

今井秀樹*
Hideki IMAI

符号化は現在のディジタル通信において不可欠の技術となっている．たとえば，ディジタル自動車電話・携帯電話は正に符号化技術の粋を集めることにより，誕生したものと言えよう．符号化は情報伝送の効率化，高信頼化，高セキュリティ化を達成するもっとも有効な手段なのである．本稿では，まず，符号化の意味について論じた後，符号化が通信システムの中でどのように用いられるかを概観し，ついで，高信頼化のための誤り制御符号化と高セキュリティ化のための暗号化について述べる．

1. はじめに

通信分野における符号化とは，情報の形態を変換することを言う．通常は，変換された結果がディジタル情報である場合にこのことばを用いることが多い．元の情報はアナログ情報である場合も，ディジタル情報である場合もある．たとえば，音声をAD変換して0，1の系列に変換するのは，元の情報がアナログ情報で，変換した結果がディジタル情報となる例である．

符号化の逆の変換を復号と呼ぶ．ただし，厳密な意味で逆の変換とは限らない．たとえば，アナログ情報をディジタル情報に変換した場合は，通常その変換の過程で情報の一部が失われるから，厳密な意味での逆変換はありえない．このような場合，復号は，何らかの意味で変換前の元の情報に近い形に復元する過程ということになる．

多くの符号化は，n次元空間Aからm次元空間Bの中への写像として表される．例として，音声のAD変換を見てみよう．図1にあるように，音声波形は，まず標本化され，標本値の列として表される．標本値は実数値と考えてよい．この各標本値は量子化され，0，1の長さmの系列に対応づけられる．つまり，実数軸が2^m個の区間に分けられ，各区間に長さmの0，1の系列が対応づけられていて，標本値が入った区間に対応する系列が出力されるのである．この標本値から0，1の系列への変換の過程を符号化と見れば，これは1次元の実数空間Aから，0，1からなるm次元空間Bへの写像として表せることになる．Bは各点（各要素）が$(b_1, b_2, \cdots\cdots, b_m)$で表せる空間である．ただし，$b_1, b_2, \cdots\cdots, b_m$はそれぞれ0か1で

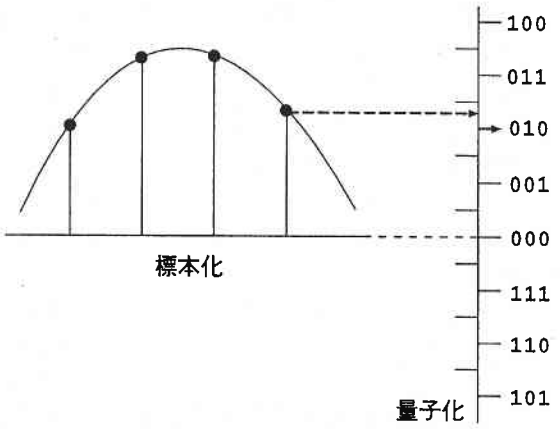

図1　AD変換

あり，全部で2^m個の点が存在する．以下では，このような空間をm次元2元空間と呼ぶことにしよう．もし，標本値n個を一括して符号化するなら，これは，n次元実数空間から，m次元2元空間への写像として表される符号化となる．このような符号化をベクトル量子化と呼ぶこともある．

実数空間から2元空間への符号化も重要であるが，ディジタル通信で最もよく現れる符号化は，n次元2元空間Aからm次元2元空間Bへの写像として表される符号化である．nとmの関係は目的によってさまざまであり，$n>m$，$n=m$，$n<m$のいずれも有り得る．このような有限次元空間から有限次元空間への写像として表せる符号化以外にも重要な符号化は多く存在する．しかし，そのような符号化も直観的には，有限次元の符号化と同様に扱える．

*東京大学生産技術研究所　第3部

2. 各種の符号化

さて，音声や画像などのアナログ情報をディジタル通信システムにより伝送するためには，まず符号化してディジタル情報に直さねばならないから，符号化はディジタル通信システムで音声・画像を送るために必須のものである．しかし，符号化の役割はそればかりではない．

ユーザの立場から言えば，通信はまず第一に送られた情報が正しく伝わり，コストも適正でなければならない．さらに，通信の秘密も保たれ，悪意の人がいる場合でも正当な相手に正しく情報が伝わるという意味で情報セキュリティが確保されねばならないし，またさまざまな意味で便利であることも望まれる．このような要求を満たすために，通信媒体，通信方式，通信機器の開発・改良等の努力が積み重ねられてきた．その中で，符号化の役割も次第に大きくなりつつある．たとえば，便利さという点から言えば，今後の通信において「いつでも，どこでも，だれとでも」という標語に象徴される移動体通信はきわめて大きな位置を占める．しかし，移動体通信の通信路は，容易に想像できるように非常に劣悪である．しかも，電波は限られた資源であるので，使える周波数帯も限定される．さらに，携帯機では，電力に対する制限も厳しいし，コンパクトに作らねばならない．このような制約のもとで，情報を正しく送るためには，符号化は必須の技術となる．符号化なくしては，ディジタル移動体通信はあり得ないと言っても過言ではない．

今後，通信される情報は増大の一途をたどるであろう．ハイビジョン映像をどこにでも送りたいという要求さえ，すでに顕在化しつつある．今後，このような増大する一方の情報を限りある通信路で送らねばならない．これを実現するには，符号化は正に中心的役割を演じていくことになる．

さて，通信における符号化には，次のようなものがある．

（a）**情報源符号化**：情報をできるだけ効率よく送るための符号化．高能率符号化，データ圧縮とも呼ぶ．

（b）**誤り制御符号化**：情報を正しく送るための符号化．通信路符号化とも呼ぶ．

（c）**伝送路符号化**：送出するパルス列を通信路の特性に整合させるための符号化．ディジタル変調とも呼ぶ．

（d）**符号分割多重符号化（CDM符号化）**：通信路を分離するための符号化．回線分離符号化とも呼ぶ．

（e）**暗号化**：情報セキュリティ向上のための符号化．情報が正当なものであることを確認するための認証も含む．

AD変換は，ここでは情報源符号化に含めて考えることにする．これらの符号化について，n次元2元空間からm次元2元空間への符号化の場合を考えると，情報源符号化では，$n>m$であり，誤り制御符号化，伝送路符号化および符号分割多重符号化では$n<m$，秘密を守るための暗号化の場合，通常$n=m$，認証の場合，通常$n<m$である．

実際のディジタル通信システムにおいて，これらの符号化すべてが使われる訳ではない．特に，CDM符号化が行われるのは，スペクトル拡散通信方式などの符号分割多重通信方式である．しかし，将来の移動体通信システムにおいては，CDM方式が重要な役割を演じると考えられるから，この符号化も，他の符号化と同列に取り上げるべきものであろう．

図2に，これらの符号化がすべて行われるディジタル通信システムのブロック図を示す．このように典型的には，情報源符号化，暗号化，誤り制御符号化，伝送路符号化，CDM符号化の順に符号化が行われるが，場合によっては，一部順序が逆転する場合も有り得る．

また，最近の符号化の研究の一つの大きな流れは，これらの符号化を融合して最適化を図るというものである．実際，ディジタル移動体通信システムの符号化・復号器（CODEC）では，情報源符号化と誤り制御符号化が密接に関連づけて行われている．そのようにして，はじめてアナログ方式よりも周波数利用効率がよく，信頼性の高いディジタル移動体通信が実現できたのである．

以下では，これらの符号化の中で，誤り制御符号化および暗号化についてさらに詳しく述べる．

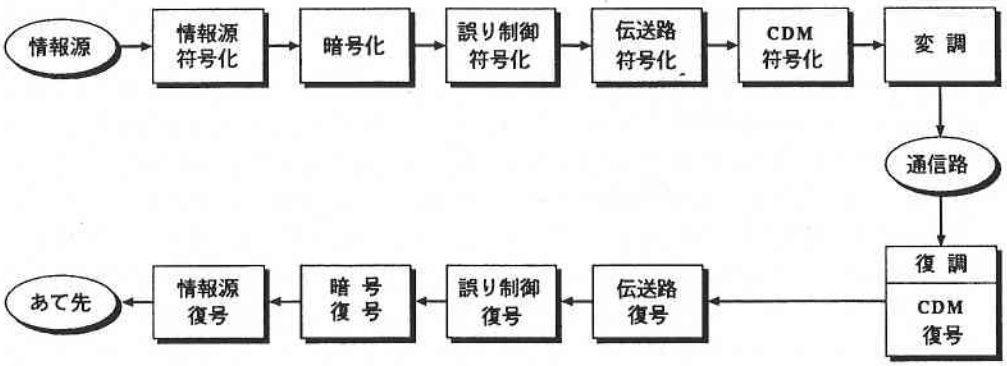

図2　ディジタル通信システムにおける符号化

3. 誤り制御符号化

誤り制御というのは，通信路で生じた誤りを検出・訂正することばかりではなく，誤りを検出した場合に，再送してもらい，正しい情報を得るという過程なども含む概念であるが，ここでは，その中心となっている．誤り検出・訂正について述べる．

3.1 誤り検出・訂正符号の基礎

符号化による誤り検出・訂正の原理は簡単である．0または1を伝達したいとき，たとえば，これを2回続けて送ると決めておく．00または11を送るのである．このようにすれば，誤りが1個生じたとき，01または10が受信される．これは，あらかじめ決められた00でも11でもないから，誤りが生じたことがわかる．つまり，誤りの検出ができるのである．誤りの訂正がしたいなら，0または1を3回続けて送ればよい．たとえば，0という情報を伝達したいとき，000を送る．このとき，誤りが1個生じ010が受信されたとしても，0が2個残っているから，（誤りが1個以下である限り）000が送られたと判断できる．これは，1個の誤りを訂正したことにほかならない．

このように，符号化による誤りの検出・訂正は，本来伝達すべき情報に余分なもの（冗長なもの）を一定の規則にしたがって付加して送り，それを受けたほうでは，受けたものがこの規則にしたがっているかどうかを調べ，その結果によって誤りの検出や訂正を行うのである．

このような冗長性の付加による誤りの検出・訂正を，人間は古くから自然に行っている．ことばを繰り返して誤りを防ぐのはごく日常的に行われるし，自然言語そのものが冗長性を持っているために，自然言語によるコミュニケーションの信頼性が上がっていることは，よく知られている事実である．符号化による誤り検出・訂正は，ディジタル情報に対し，より組織的に機械で処理しやすい形で冗長性を付加し，信頼性の向上を図る技術である．この冗長性を付加したもの（厳密にはその集合）を**符号**と言い，誤りの検出に用いられる符号を**誤り検出符号**，訂正に用いられる符号を**誤り訂正符号**と呼ぶ．両者を総称して誤り訂正符号と呼ぶこともある．

誤り訂正符号を用いるシステムは図3のようにモデル化されることが多い．ここで，簡単な誤り訂正符号の例を示し，基本的な概念を導入する．次の符号を考えよう．

情報		符号語
00	→	00000
01	→	01101
10	→	10110
11	→	11011

これは，次のようにして符号化されたものである．

$$i_1 i_2 \rightarrow i_1 i_2 p_1 p_2 p_3$$

ここで，i_1，i_2 を**情報ビット**，p_1，p_2，p_3 を**検査ビット**と呼ぶ．ただし，検査ビットは情報ビットから

$$p_1 = i_1 + i_2$$
$$p_2 = i_1$$
$$p_3 = i_2$$

により計算される．この演算はmod2の加算（排他的論理和）として行われる．すなわち，

$$0+0=0, \quad 0+1=1$$
$$1+0=1, \quad 1+1=0.$$

この符号は，**符号長**が5，**情報ビット数**が2，**符号化率**が2/5の符号であり，次に示すように1個の誤りを訂正できる．また，この符号のように，検査ビットが情報ビットの線形演算によって求められ符号を**線形符号**と呼ぶ．現在用いられている誤り訂正符号のほとんどは線形符号である．

この符号を例にとって，線形符号による誤り訂正の原理を説明しよう．この符号では，符号語の記号を図4のように2次元に配列したとき，情報ビットを含む各行，各列の1の数が偶数となるように符号化している．これらの行または列に誤りが1個生じると，1の数が奇数となり，そのような行と列の交点として誤りの位置を知ることができる．このように線形符号では，ある情報ビットの組に，1の数

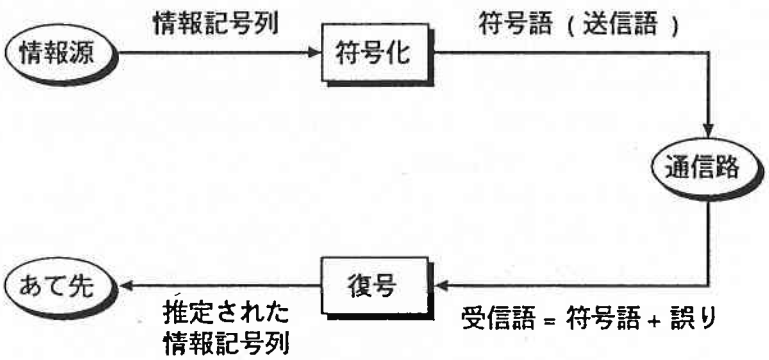

図3　誤り訂正符号化システム

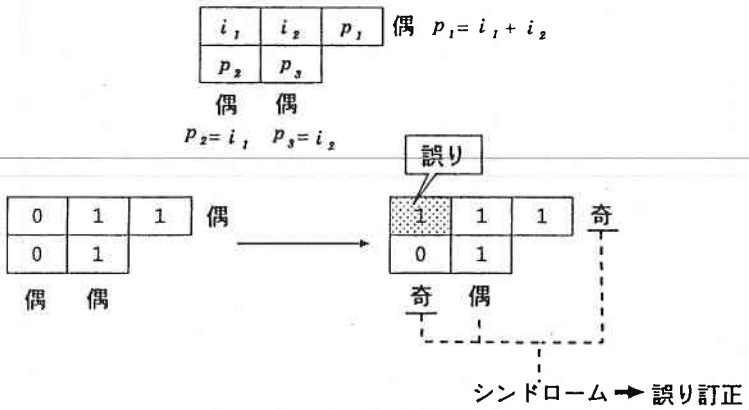

図4　線形符号による誤り訂正の原理

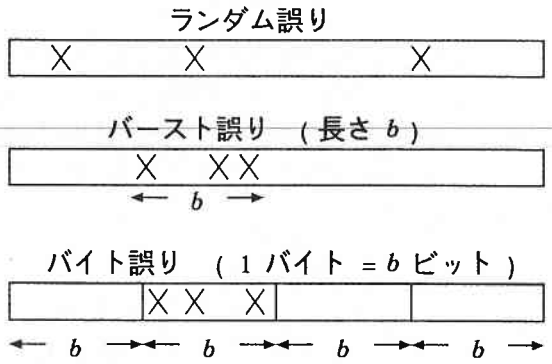

図5　誤り検出・訂正符号の主たる対象となる誤り

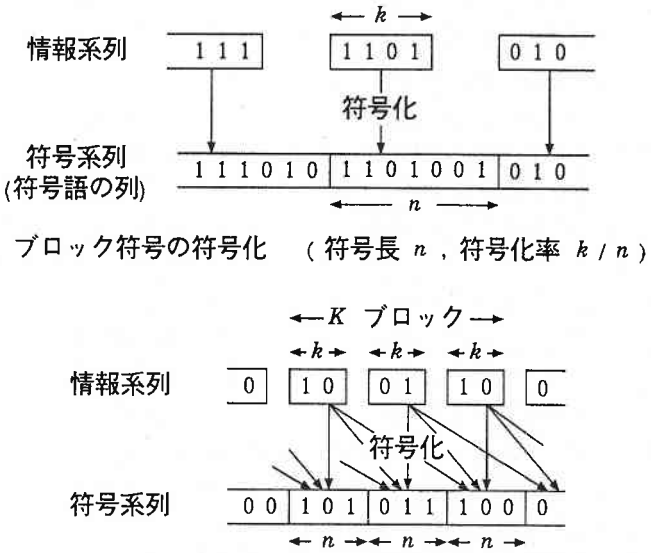

図6　ブロック符号と畳込み符号の符号化

が偶数となるように検査ビットを付けることにより符号化を行い，受信側では，この組の1の数が偶数か奇数かを調べ，その結果（シンドロームという）に基づいて誤りの訂正を行うのである．

誤り検出・訂正符号が検出・訂正の対象とする誤りの主なものは図5に示す**ランダム誤り**，集中して生じる**バースト誤り**，バイト単位で生じる**バイト誤り**の3種類である．ただし，1バイトは必ずしも8ビットとは限らない．また，誤り訂正符号をその構造から大きく分類すると**ブロック符号**と**畳込み符号**に分けられる．これまでの例はすべてブロック符号であった．図6ににブロック符号と畳込み符号の符号化の図を示す．

3.2　符号理論

誤り検出・訂正符号の基礎理論をふつう**符号理論**と呼ぶ．符号理論は，1948年シャノンが情報理論を創始したときに同時に生まれたとされることが多いが，今日の符号理論の実際の系譜は1950年の**ハミング符号**に始まると考える方が自然であろう．これはその当時開発された真空管式電子計算機の記憶装置の誤り訂正のために考案されたものであり，1個の誤りを訂正する符号である．これにより，初めて誤り訂正符号の組織的な構成法が与えられた．以後，符号理論は誤り訂正符号の構成理論として発展していくことになる．

1957年プランジにより符号の一つのタイプとして**巡回符号**が提案された．この符号は数学的に取り扱いやすい構造を持つため，それ以後の多くの研究は巡回符号を対象とするものとなった．また，1970年代には，今井らにより巡回符号は多次元に拡張された．これは，後に代数幾何符号の復号法の研究につながることになる．

ハミング符号の出現から10年経った1959年から61年に掛けて，実用上最も重要な符号が次々と生まれた．任意個数の誤りを訂正する符号を設計できる**BCH符号**，きわめて効率のよい非2元の誤り訂正符号である**リード・ソロモン符号**（RS符号）などである．また，1961年に出版されたピーターソンの著書は符号理論の基礎を固めるのに決定的役割を演じた．これにより，BCH符号やRS符号の復号法が与えられると共にガロア体の理論を基盤とする符号理論の綺麗な理論体系が構築されたのである．

しかし，この当時の符号理論は実用とは遠いものであった．非常に簡単な符号は別として，当時の技術水準からすると復号器が複雑になり過ぎて実用には耐えなかったのである．一般には，符号理論は理論のための理論と考えられていた．

復号をできるだけ簡単にしようという立場から，1963年**多数決論理復号法**がマッシイにより提案され，1960年代の後半，**差集合巡回符号**，**有限幾何的符号**など多数決論理復号可能な符号が次々と見いだされた．これらの符号の効率はBCH符号に劣るものの，復号は簡単である．特に差集合巡回符号は，後に日本の文字放送における誤り訂正への応用を契機として，FM多重放送など放送分野で広く実用化されるようになっていく．この種の符号の理論は組み合わせ数学と結び付いて発展し，符号理論の中でもユニークな一分野を形作っている．

また，比較的符号長が短く復号も簡単な符号を組み合わせて，符号長が長く誤り訂正能力の高い符号を構成しようという試みも早くから行われていた．1954年にエライアスによって発表されて**積符号**や1966年にフォーニーが提案した**連接符号**がそれである．これらは，理論的にも重要な手法であるが，訂正能力の高い符号の装置化がまだ難しかった時期には，実用上必須の技術であった．1980年代初頭に実用化されたコンパクトディスク（CD）で，2重誤り訂正RS符号の積符号が用いられたことはよく知られている．

他方，BCH符号などの効率のよい符号の復号を簡単化しようという研究も多くの研究者により行われ，1968年**バーレカンプ・マッシイ法**が発表された．これは復号法の大きな改善であり，後に訂正能力の高いBCH符号やRS符号の実用化を促進する原動力の一つとなった．また，1975年には，バーレカンプ・マッシイ法と同等の能力を持つが，非常に理解しやすいという特長を持つ**ユークリッド復号法**が杉山らにより提案され，今日では，バーレカンプ・マッシイ法と並んで広く実用化されている．さらにその後シストリックアレイによる復号の高速化の提案など，装置化に関する多くの研究が行われ，1980年代以降のRS符号やBCH符号の実用化の急速な進展に伴い，実用に即した要請を取り込みつつ，復号の理論は発展を続けている．

復号の理論の中で，復号特性の評価も地味ではあるが，重要な研究課題である．厳密に復号特性を評価するには，符号の構造の詳しい解折が必要になってくる．これは一般にかなり難しい問題であるが，1960年代から息の長い研究が行われており，マクウィリアムスや嵩らにより多くの成果が得られている．

また，復号特性をできるだけ改善しようという立場から，通信路から得られる各受信記号についての信頼度情報などを利用した復号法の研究も1960年代半ばから行われている．このような復号法の研究は，代数的符号理論の殻を破って，信号理論とも密接な関わりを持つようになってきた．

さて，ピーターソンの著書で扱われた符号のほとんどはブロック符号であった．それに象徴されるように，符号理論はブロック符号を中心にして発展してきた．しかし，もう一つのタイプの符号である畳み込み符号も，その歴史はブロック符号と同様に古く，実用上も重要である．

畳込み符号が提案されたのは，1955年エライアスによってであるが，その僅か2年後にボーゼンクラフトにより**逐次復号法**が見いだされた．この復号法は後にファノらにより改良され宇宙通信などに用いられている．

畳込み符号の歴史の中で実用上最も重要な研究成果は，1967年のビタビ復号法の発明である．これは当初，畳み込み符号の能力の限界を導くための理論的な道具として提案されたのであるが，後にフォーニーらにより，その実用上の価値が認められ，広く実用に供せられるようになった．また，その前後から畳み込み符号の理論もフォーニーらによって漸く整備され，符号理論の一翼を担うようになってきた．

畳み込み符号の理論は，ガロア体に基づくブロック符号の理論とはやや趣を異にし，有限状態機械の理論を基礎として，制御理論などとの共通点を持っている．また，復号理論が中心であり，符号構成はコンピュータに頼る部分が多い．しかし，最近符号構成の理論も着実に進展しつつある．

以上述べた符号は主として2元通信路におけるランダム誤りまたはランダムなバイト誤りを対象とするものである．しかし，現実の通信路はそう単純ではなく，さまざまなタイプの誤りが発生する．また，情報伝送速度を上げるため，多値の信号を送ることも増えてきた．このように，さまざまな通信路に対しより効率よく誤りを訂正する符号の研究も符号理論の一つの大きな流れとなっている．

そのような符号として，最も古くから研究された符号は密集して生じる誤り（バースト誤り）を効率よく訂正するバースト誤り訂正符号である．バースト誤り訂正符号として最初に現れたのは，BCH符号やRS符号とほぼ同時期に発明された**ファイア符号**であり，これは後にディスク装置などに使われた．また，より効率のよいバースト誤り訂正符号として，1963年に嵩により提案された符号が知られ

ている．一方，バースト誤り訂正畳み込み符号として最初のものは1960年の**ハーゲルバーガー符号**であるが，1968年により効率のよい**岩垂符号**が見いだされ，単純なバースト誤り訂正符号の理論は一応の完成をみた．

その後，このようなバースト誤り訂正符号の研究は，バースト誤りとランダム誤りの双方が発生する複合通信路に対する誤り訂正の研究へと発展していった．これは実用上重要な問題であるが，単純な評価が難しく，まだ完成の域に達しているとは言い難い．

多値通信路に対する誤り訂正の研究が本格化したのは，1970年代の中頃，ウンガーベックと今井・平川によってである．彼らはそれぞれ，振幅変調や位相変調などを行う通信路に対し，効率よく誤り訂正を行う方法を提案し，これによって誤り訂正符号化と変調とを一体化して行う**符号化変調**の基礎が築かれた．符号化変調は，その後符号理論の一つの大きな分野に発展していくことになる．

ある種の記録システムや光通信システムでは，誤りは非対称に生じることが知られている．たとえば，ほとんどの誤りが1から0への誤りであるような通信路もあり得る．このような通信路に整合した誤り訂正方式の研究も，1980年代になり実用化の可能性に刺激され，活発な研究が行われるようになってきた．この種の研究も符号理論における一つの分野に成長しつつある．

このように符号理論は，その実用化が進み，応用分野が広がるにつれ，それぞれの応用に適した符号化・復号法を求めて研究が進展してきた．この傾向は今後も変わらないであろう．また，信号理論，変調理論，情報源符号化の理論などとの境界領域では，符号理論とこれらの理論の融合が進んでいる．さらに，スペクトル拡散通信方式に用いられる系列やパターン認識，暗号理論などへの符号理論の応用も盛んである．しかも，符号理論の最も古典的な課題においても今なお活発な研究が行われているのである．

符号理論の最も古典的な課題は，復号が簡単で効率のよいランダム誤り訂正符号を構成することである．BCH符号やRS符号はそのような符号であるが，RS符号は符号長をあまり伸ばせないし，BCH符号は符号長が長くなると効率が下がってしまう．符号化や復号の遅延が許されるなら，符号長を長くする程，復号特性を改善できるので，符号長が長くしかも復号が簡単で効率のよい符号を構成することが符号理論の最も中心的課題であった．これに対し優れた研究成果が，最近得られたのである．それが1981年のゴッパによる**代数幾何符号**の発明と1989年から1993年にかけてのユステッセン，フェン，ラオ，坂田ら多くの研究者によるその復号法の確立である．これにより，復号法もRS符号やBCH符号と同程度の手間ででき，効率がよく符号長の長い符号が構成できることとなった．

符号理論は，このように，その最も古典的な課題でさえ現在も活発に研究が続けられ，理論として深化していくとともに，実用化の進展に伴い，その領域を絶えず拡大しているのである．

4. 暗　号　化

4.1 暗号とは

暗号は，通信・記録などの秘密を保持する仕組みとして古くから用いられてきた．また，一般にも，暗号は秘密を守るためのものと考えられている．しかし，現代の暗号理論では，暗号はより広く解釈されており，特定の知識（**鍵**）を使えるか否かによって，情報に対するある操作が効率よく行えるか否かを制御し，秘密を守ったりあるいは情報の正当性を確認したりする仕組み全般を意味するものと定義される．この定義からわかるように，暗号は，秘密を守ること（**守秘**）ばかりではなく，情報の正当性を確認すること（**認証**）にも用いられるし，さらに情報セキュリティを達成するためにさまざまな形で利用される．

4.2 守秘機構

図7に暗号による守秘機構を示す．情報の発信者は秘密に送りたい情報 M（**平文**と言う）を**暗号化鍵** K_1 を用いて暗号文 C に変換する．暗号文 C は平文 M と暗号化鍵 K_1 の関数である．この変換を**暗号化**と言う．受信者は**復号鍵** K_2 を用いて，暗号文を元の平文 M に戻す．この操作を復号と呼ぶ．

ここで，暗号化，復号はいずれも効率よく実行できなければならないが，復号鍵なしに暗号文から平文を求めるのは非常に困難でなければならない．また，復号鍵は秘密にし，あらかじめ認められた当事者以外はこれを入手できないようにしなければならないし，他の入手可能な情報から推定することも実際上不可能となるようにする必要がある．なお，暗号文を何らかの手段で入手して，復号鍵なしで平文に復元することを**解読**と言う．

ここで，例として，アルファベットの文字を一定数ずらすという暗号をとりあげよう．たとえば，3文字ずらすとすれば，ROMAはURPDと暗号化される．暗号化鍵は「アルファベットの文字を後ろに3文字ずらす」であり，復号鍵は「アルファベットの文字を前に3文字ずらす」である．この復号鍵を知っていれば，URPDをROMAに戻すのは何でもない．もちろん，暗号化鍵を知っていても，復号鍵は容易に推定できる．しかし，暗号化鍵も復号鍵も知らなければ，URPDがROMAであると判断するのは，そう簡単ではないだろう．

4.3 認証機構

図8に暗号による認証機構を示す．情報発信者は伝達したい平文 M から，**認証文生成鍵** L_1 を用いて**認証文** A を

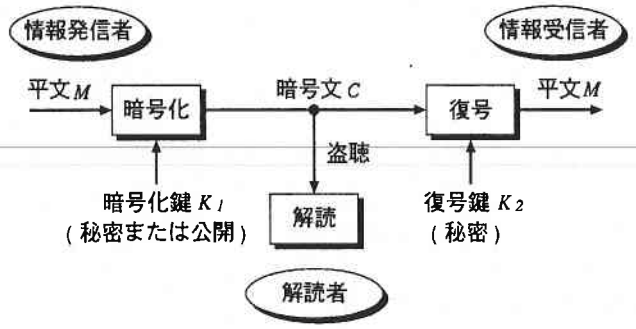

図7　暗号による守秘機構

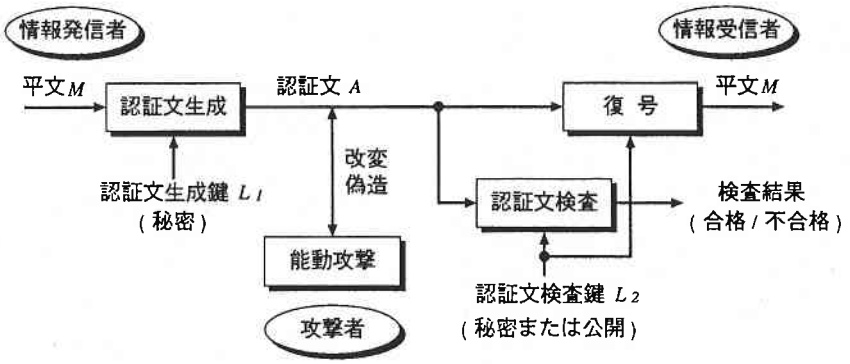

図8　暗号による認証機構

作る．認証文 A は M と L_1 の関数である．受信者は，**認証文検査鍵** L_2 を用いて認証文 A から平文 M を取り出す（復号する）とともに，この認証文が認証文生成鍵 L_1 を用いて作られたものかどうかを検査する．

この認証機構が有効に働くためには，認証文生成，復号，認証文検査がいずれも効率よく実行できるものでなければならない．しかし，認証文生成鍵を知らなければ，認証文検査をパスするような認証文を生成するのが，実際上不可能なようにしておく必要がある．そして，認証文生成鍵は秘密にし，あらかじめ認められた当事者以外はこれを入手できず，また他の入手可能な情報から推定することもきわめて困難となるようにしておかねばならない．

4.4　共通鍵暗号と公開鍵暗号

暗号を用いている情報発信者と受信者の鍵の一方から他方が容易に推定できるとき，この暗号を**共通鍵暗号**と呼ぶ．前述の文字をずらす暗号は共通鍵暗号の一つである．共通鍵暗号では，両者の鍵は実質的に同じものと見なす．

共通鍵暗号の代表的なものは，4.2の例のように文字を鍵に従って置き換える**換字暗号**である．もう一つよく知られているものに，鍵に従って文字の順序を入れ換える**転置暗号**がある．この二つの暗号は昔からよく使われていた．現在でも，共通鍵暗号としては，これらを複雑に組み合わせた方式が用いられてることが多い．1970年代半ばIBMが開発し米国連邦政府標準暗号として採用されたDES（Data Encryption Standard）は現代の代表的共通鍵暗号である．

米国ではDESの次世代暗号の開発も進み，スキップジャックという名の暗号をクリッパーチップと呼ばれるICに搭載して標準化しようという動きがあるが，その詳細は公表されていない．

このような共通鍵暗号に対して，情報発信者と受信者の鍵が異なり，一方から他方を推定するのがきわめて難しい場合，この暗号を**公開鍵暗号**と呼ぶ．公開鍵暗号を用いる場合，鍵の一方を公開しても他方を秘密に保つことができる．この秘密に保つ鍵を**秘密鍵**，公開してもよい鍵を**公開鍵**と呼ぶ．守秘機構の場合には，復号鍵 K_2 が秘密鍵であり，暗号化鍵 K_1 が公開鍵となり，認証機構の場合には，認証文生成鍵 L_1 が秘密鍵であり，認証文検査鍵 L_2 が公開鍵となる．

この公開鍵暗号の概念は1976年にディフィとヘルマンによって提案されたが，具体的な公開鍵暗号方式はリベスト，シャミア，エールマンの3人によって1977年に発明されたRSA方式が最初のものであり，また最も代表的な方式である．これは，100桁程度の二つの素数の積の因数分解の難しさを利用して公開鍵暗号を実現している．

共通鍵暗号では，情報発信者と受信者は共にそれぞれの鍵を秘密に保たねばならないが，公開鍵暗号では，秘密鍵

を持つのは，原則としてただ一人となる．このため，鍵の管理の簡単化や，当事者（発信者と受信者）間の争いの解決に有用となる．

4.5 暗号の安全性

暗号を守秘に用いる場合，解読ができるだけ難しくなるように暗号を設計しなければならない．このとき，解読者が入手可能な情報が何であるかによって，暗号に対する攻撃の種類を**①暗号文攻撃**，**②既知平文攻撃**，**③選択平文攻撃**の三つに分けることができる．暗号文攻撃は，解読者が暗号文のみを入手可能と想定することである．ただし，暗号文は大量に入手できると考えるのが普通である．既知平文攻撃は，平文と暗号文の対が入手可能な場合の攻撃である．これは，暗号文のみによる攻撃より厳しい攻撃であるが，このような状況は実際にしばしば生じることがあり，暗号を設計する場合，少なくとも既知平文攻撃を想定すべきである．選択平文攻撃は，解読者が任意に選んだ平文に対する暗号文が得られるという状況であり，最も厳しい攻撃である．共通鍵暗号の場合，暗号の使い方に十分な注意を払えば，このような状況はあまり生じそうにはないが，選択平文攻撃にも十分耐えられるように暗号を設計すべきであるという意見が強い．

暗号の安全性には，**情報理論的安全性**と**計算量的安全性**とがある．情報理論的に安全とは，平文を推定するのに必要なだけの情報を（復号鍵がなければ）暗号文は持っていないために，原理的に平文を復元できないことを言う．情報理論的に安全な暗号として代表的なものは，使い捨て乱数を用いたバーナム暗号である．バーナム暗号は，平文と同じ長さの乱数列または擬似乱数列を平文に1文字づつ適当な方法で加えて暗号化するというものである．バーナム暗号で，乱数列そのものを鍵とし，二度と同じ鍵を用いなければ情報理論的に安全である．このような暗号は鍵を知っていれば簡単に復号できるが，解読は原理的に不可能である．しかし，鍵が平文と同じ量だけ必要であるので，商用暗号としては実用的でない．

計算量的に安全であるとは，原理的には解読できても，膨大な計算量を要し，実際上解読不可能である場合をいう．商用暗号のほとんどは計算量的な安全性を目指して設計されている．たとえば，DESは既知平文攻撃の場合，平文と暗号文の対に対してすべての鍵を確かめるという総当たり攻撃を行えば，原理的には，鍵が求まり，解読可能となる．しかし，鍵の総数は2^{56}（約7.2×10^{16}）であり，百万分の一秒で一つの鍵を調べられたとしても，すべての鍵を調べるには二千年以上かかる．もっとも，並列計算により，これより遙かに短期間で，総当たり攻撃可能な装置を構成できるという研究発表もある．実用的な暗号について計算量的に安全であることを理論的に証明することはきわめて難しく，経験や勘に基づいて判断せざるを得ない場合が多い．

暗号の安全性には，このような暗号そのものの安全性ばかりではなく，それを用いる方法の安全性も考慮しなければならない．特に今後の大規模ネットワークでに用いられる暗号では，鍵をいかに配送し管理するかが最大の問題となる．松本，今井による**KPS**（Key Predistribution System）はその一つの解答を与えるものと言えよう．これは，注意深く作られたICカードのように，ある程度物理的に保護された装置（耐タンパー装置）を用いて，ネットワーク加入者の誰とでも，簡単に共通鍵暗号方式の鍵を共有する方式であり，安全性も高い．

6. む　す　び

ディジタル通信における符号化について，誤り制御符号化，暗号化を中心として述べたが，情報源符号化，伝送路符号化，符号分割多重符号化も含め，それぞれが現在大きな研究分野を作っており，それぞれに理論体系が構築されている．また，現在，それらを融合していこうという立場の研究も行われている．将来は，こられの多くが統一的に論じられるようになっていくかも知れない．

いずれにせよ，符号化は，基礎理論から応用まできわめてアクティブに研究され，発展し続けている研究分野であるとともに，今後の通信の進展を支える基盤技術でもある．本稿が，この分野への関心を少しでも高めることになれば，幸いである．

（1993年12月1日受理）

参　考　文　献

1) 宮川洋，原島博，今井秀樹：“情報と符号の理論”岩波書店（1983）．
2) 今井秀樹：“情報理論”昭晃堂（1984）．
3) 嵩忠雄：“情報と符号の理論入門”昭晃堂（1989）．
4) 今井秀樹：“符号理論”電子情報通信学会（1990）．
5) 岩垂好裕：“符号理論入門”昭晃堂（1992）．
6) 池野信一，小山謙二：“現代暗号理論”電子通信学会（1986）．
7) 岡本栄司：“暗号理論入門”共立出版（1993）．
8) 今井秀樹：“暗号のおはなし”日本規格協会（1993）．