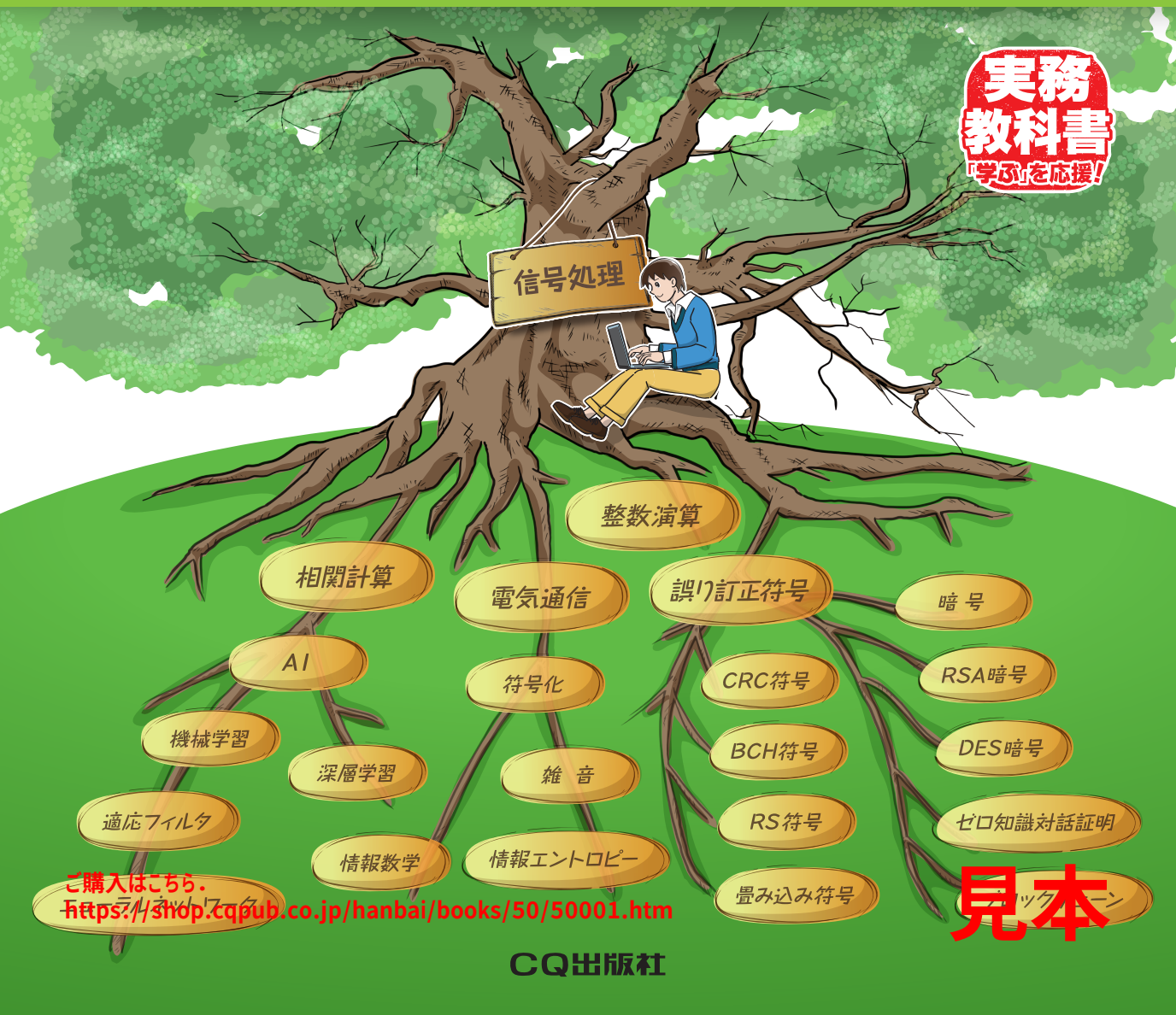
基礎作りシリーズ

学び直しのための実用情報数学

AI，情報数理，誤り訂正符号，暗号

三谷 政昭［著］



CQ出版社

プロローグ

情報数学で広がる多彩な信号処理応用

● はじめに

近年,「情報通信技術(ICT:Information and Communication Technology)」,「マルチメディア情報ネットワーク」,「プライバシー情報」,「情報セキュリティ」……などなど,“**情報**”という2文字を含んだ言葉が世の中をとびかっている.よく耳にする“情報”は,コンピュータ通信ネットワークの世界にどっぷりと浸って生きていく私たち,とくに技術者にとって必要不可欠のものであり,その本質をしっかりと見据えておかなければならない.

また,画像や音声などのマルチメディア情報やビッグデータを処理・解析するための製品開発,ソフト作成などの仕事面では,情報理論的な思考方法やセンスが要求されていることも事実である.さらには,広範な分野(ゲーム,経済,自動運転,ロボットなど)で利活用されつつある知的な情報処理手法として**人工知能**(**AI**:Artificial Intelligence)技術が脚光を浴びており,人材育成が急務である.

情報理論的な側面(確率,統計など)をもう一度基礎からやり直したい人,**情報数学**(符号,暗号,データ圧縮などの基礎理論)をしっかりと理解しておきたい人,新しいインテリジェントな情報処理(人工知能)の基本を知りたい人……,第1部『人工知能(AI)』は,そういったみなさんにとって大いなる知識,知恵を提供するものである.

ところで,わたしたちの身の周りには,インターネットを基軸に据える「**IoT**(Internet of Things)」,電子メール/SNS/スマホ,デジカメやAIを搭載した家電製品,4K/8K超高精細ディジタルテレビ放送などの多種多様な利用シーンにおいて,文書,画像,音声などのさまざまなマルチメディア情報が氾濫している.

一般にマルチメディア情報は,ディジタル信号(0と1の数字並び)として一元化されることが大前提であり,これまでのテキスト処理とは異なり,画像を中心とした大容量情報処理が主体となっている.

こうしたマルチメディア情報ネットワーク時代に必要とされる数学的な基礎をしっかりと理解しておくことは,ディジタル情報処理全般にわたる総合的な理解を深める際に大いに役に立つことに疑問の余地はない.

プロローグでは,おもに情報数学が根幹をなす広範かつ多彩な信号処理の代表的な活用事例とともに,整数的な処理,知的な情報処理応用の概要などについて説明する.その際,“数学”的な難しい説明はほどほどに,情報数学のもつ“とっつきにくさ”を解消してもらうことを最大の目標にして,ていねいに解説する.とくにプロローグは,みなさんに情報理論的なセンスを身に付けてもらううえでのウォーミングアップになるものなので,しっかりと読み進めていってもらいたい.

1　情報数学で何ができるのか?

情報数学といえば,確率,統計という実用的ではない数学だというイメージがつきまとうようである.実生活の場面では,せいぜい天気予報で「今日は雨が降る確率が高いから,傘をもっていこう」とか,競輪競馬などのギャンブルや宝くじなどでの当たり/はずれで「○△という馬が勝つ確率が高い」,「宝くじは当たらないね」,という言い方がされるぐらいであろう(**図1**).

ところが,情報数学に土台をなす情報理論となると,さまざまな実生活の場面で登場してくるのであ

図1　情報数学の利用される分野

る．たとえば，スマホ（高機能携帯電話）などを使って友達と話をしたり，CDやUSBメモリで音楽を聴いたり，DVDやブルーレイ，ネットワーク経由でビデオ映画を観たり……など，ほとんどの日常場面で，知らず知らずのうちに**情報理論**の恩恵にあずかっているといっても過言ではない．無線，有線が入り乱れたディジタル通信ネットワークシステムにしても情報理論のかたまりであるし，CDやUSBメモリではディジタル信号の**誤り訂正**機能を利用して少々の傷ぐらいでは，ガリガリと耳障りな雑音が入らずクリアな音楽を再生できるようになっている（**図2**）．

こうした現在のディジタル社会情報化を実現する基盤が情報数学に根差しているわけで，基本的な考え方や数学的表現に精通していることは，21世紀に生きる技術者にとっては絶対に必要な知識であると言い切れよう．

まずは，情報数学の適用例をたとえ話にして，そのイメージの具体的な解説を行う．なお，情報数学は従来はアナログ信号をおもな対象としていたが，現在は画像や音声を一元化したマルチメディア情報でディジタル信号である．「ディジタル情報数学」，あるいは「ディジタル情報理論」と言い換えるのも妥当な感じがする．

● データ圧縮（図3）

わかりやすい例をあげると，「トラギ」(3文字) といえば，賢明なる本書の読者のみなさんなら「トランジスタギジュツ」(10文字で，トランジスタ技術のこと) だと理解されるであろう．ここに，データ圧縮の基本的なコンセプトが眠っているというわけである．正確にいうと10文字かかるところが，たったの3文字でわかるというわけで，データ量が3/10で済むことが理解される．

また，「勉強する」という動詞の活用形は，「勉強しよう（未然形），勉強します（連用形），勉強する（終止形），勉強すること（連体形），勉強すれば（仮定形），勉強しろ（命令形）」となるが，「運動する」や「処理する」なども同様で，変化したところだけ，つまり活用語尾「しよう，します，する，すること，すれば，しろ」を記憶すると，他の類似した動詞にも適用できるのである．こうした変化した部分のみを情報として浮きだたせる処理も，データ圧縮の一手法であるといえる．

● 符号化/復号化

何人かが順に，限られた時間内で話を伝えていって最後の人が理解した内容と原文との違い，すなわち最初の人の話をどれだけ正確に伝えられたかという伝言ゲームは，符号化/復号化の概念に近いものがある（**図4**）．

まず，かなり長い話を限られた時間にまとめるという作業（符号化）を行って次の人に伝達し，話を聞いた人は頭の中で原文の内容を再構築するという作業（復号化）を行い，また次の人に伝えていくという処理（情報伝送）を繰り返す．こうした繰り返しの作業では情報が失われるという**情報誤り**がつきもので，原文とは似ても似つかぬ内容が伝達されることが往々にして起きる．伝言ゲームは，内容変化のプロセスを楽しむのである．

ところが，スマホでの通信，インターネットなどのデータ伝送では，こうした情報誤りは絶対に避けなければならないわけで，誤りが発生しにくい仕組みを組み込む必要性（**誤り検出**，**誤り訂正**）が出てくる．

たとえば「トラギ」という言葉を誤りなく正確に相手に伝えるためには，「トラギトラギトラギトラギ」と同じことを繰り返して言うとか，「とまとのト」，「らいおんのラ」，「ぎんこうのギ」と言うとか，みなさんもごく自然に誤りが起きにくいような工夫をして

図2　ディジタル化による利点

図4　符号化/復号化ー悪い例

	データ圧縮	略語
Internet of Things	→	IoT
Integrated Circuit	→	IC
パワーステアリング	→	パワー

図3　データ圧縮の基本的な考え方

第1章 人工知能（AI）の基礎数学

第1章では，AIの基本知識と必要最小限の数理的な取り扱いについて説明するので，気楽に読み進めていってもらいたい．

1.1 AIと機械学習

● さまざまな分野との関係性

AIは「知能」というキーワードをもとに，心理学，工学，情報科学，数学，哲学，脳科学など，さまざまな分野と関係をもっている．じつはこれらの関係性こそが，AIそのものなのである．

AIの歴史は，「**第一世代**」においては人の知的作業を支援することから始まり，「**第二世代**」では，主としてルールベース（**if ～ then**形式という）に基づき，第五世代コンピュータとかエキスパート（専門家）システムと称するAIとして盛んに研究された．これは，プログラミングでいうところの「if ～ then ～ else」のように，専門家の知識をルールで記述して専門家と同様のことを行えるようにするという設計思想である．しかし，専門家の知識を抽出するのは困難であった．何よりもメンテナンスが大変だったため実用化に至らず，AI研究はしぼんでいったのである．

ところが現在は，脳モデルや学習モデルに基づき知識処理を飛躍的に向上させる「**第三世代**」のAI大ブームとなっている．if ～ then 形式のルールを超越し，人の脳の再現（エミュレート）によって，はるかに汎用的で柔軟性の高い「**電子頭脳**」の実現を目ざしている．

● どのような意味でAIが使われているか

AIがどういう意味の使われ方をされているのか，一般的な言い方で整理すると，

(1) 人手では処理しきれない大量のデータを使って，これまで発見できていなかったような相互関係を見い出す
(2) 定義が一様ではないデータをカテゴリ分類して，ラベル付けし，そのルールを獲得する
(3) 既存データからルールを獲得して，未知のデータを予測する

となる．つまるところ，「単なる1対1，あるいは場合分け，if ～ then形式ではないルールで出力を返す．また，単なる経験および訓練データからの事実抽出だけではなく，先読みに適用できるようなツールがAIである」と言い換えることもできる．

このようなAIブームの先駆けとなった計算手法は，複数の技術を組み合わせて実現されているが，昨今，一世をふうびしている気になるワードは，“**機械学習**（**マシンラーニング**）”あたりだろう．

じつは機械学習においては，人が複雑で面倒なルールを記述することなく，楽できるのである．たとえば猫の画像認識では，猫というタグを画像に付け，機械学習アルゴリズムに流し込みさえすれば，自動的に猫を識別・判断して分類するルールを見いだしてくれる．

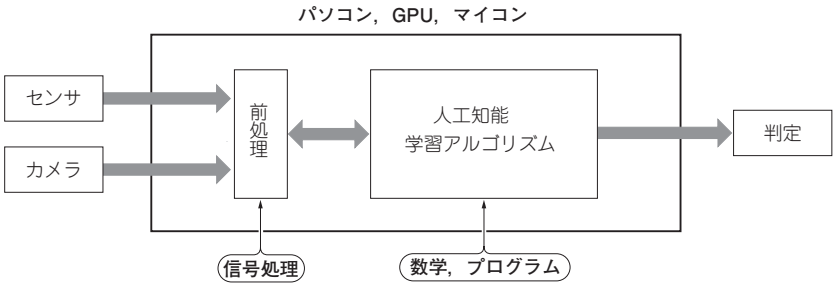
それでは，機械学習で実現できる身近にある例を，いくつか紹介しておこう（**図1.1**）．

● 機械学習で実現できる例

[1] 届いたメールがスパムか否かを自動判定するルールを導き出す
[2] 過去の購買履歴から類似する購入者を探して，購入してもらえそうな商品を予測して推奨する
[3] 車載カメラの映像から歩行者を検出して，車の事故防止に役立てる
[4] コンピュータに，囲碁や将棋などのゲームを行わせる
[5] アップル社の「Siri（しりと読む）」やNTTドコモの「しゃべってコンシェル」などの対話インターフェースを作ってコンピュータと会話する
[6] 医療用CT画像を解析して病気の原因をコンピュータに探させる

ザックリいうと，“機械学習”とは「経験（データ）によって学習して賢くなる**進化処理アルゴリズム**で，コンピュータが知識やルールを自動的に獲得する手法」となる．つまり，訓練データから**ルール**，**パターン**，**規則性**などを発見し，それに基づいて新たなデータのカテゴリ分類や認識，さらには予測をコンピュータに行わせる学習計算アルゴリズムであり，データ分析手法の一つである．

なお，最先端のAI研究成果として，「[illegible]も注



（a）人工知能を実現するハードウェア構成の例

（b）コンピュータと棋士（囲碁）が対局している

（c）医療用CT画像を取り込み診断結果を示す判定

（d）車載カメラの映像，歩行者を認識して事故を防止する

図1.1　人工知能（AI）の世界

および訓練データを必要としない機械学習アルゴリズム」が提案されており，注目を浴びている．

● 機械学習のやり方

機械学習のやり方にもいくつかの種類があり，以下の三つに大別される．

［1］**教師あり学習**
［2］**教師なし学習**
［3］**強化学習**

「教師」というのは，お手本，正解例のことである．たとえば，お母さんが子供に猫の絵や本物を見せて，「これはネコ，猫ですよ」と何度も繰り返しているうちに，子供は絵を見たり，言葉を聞いたり，あるいは口の動きを見て，少しずつ‘ネコ’という言葉と，‘猫’という動物を結びつけていく（知識を獲得する）学習プロセスにそっくりなのである．お母さんがまさしく「教師」役で「お手本」というわけだ．このように「お手本あり」が「教師あり学習」である．

一方，「お手本なし」で多数の入力データ間の相互関係やつながりから，似たものをまとめるモデル（データ間の相互関係）やルール（データのカテゴリ分類）を作るのが「教師なし学習」と呼ばれる．

そして，とりあえず導き出した粗っぽいモデルやルールをもとに，徐々に正解へと近づけていくという**改善学習プロセス**と言える手法が，**“強化学習”**である．ちょうど，子供が正解を言い当てたらお母さんがご褒美のお菓子を与え，学習を進めていくような感じである．

● ディープ・ラーニングとは

一方，AIブームを牽引し，ディープ・ラーニング（Deep Learning；**深層学習**）と称される“機械学習”を支えるアルゴリズムのアプローチの一つが「**ニューラルネットワーク**」である（詳細は，**第3章**と**第4章**を参照）．

ニューラル・ネットワークは，人間の脳の生物学的な仕組みから着想を得たものである．ただ，ニューラル・ネットワーク学習に際して最大のネックは，きわめて高速な計算処理能力を要することであった．

ところが近年，高速で比較的安価に，しかも強力な並列処理ができる「**GPU**（Graphics Processing Unit）コンピューティング」の普及，**ビッグ・データ**技術の進展，そして「実質的に無限にデータ蓄積できる**ストレージ技術**」の進歩と相まって，AI技術の進化を阻害していた課題が一挙に解決されたのである．その結果，2016年以降のAI技術の急速な盛り上がりにつながっていった．

現在では，たとえばディープ・ラーニングを利用して機械学習したコンピュータシステムによる画像認識性能が，専門家（例：MRIスキャン画像を用いた癌の兆候の発見／診断，防犯カメラの顔画像による犯人特定など）の域を超えるまでに進歩を遂げ…

第2章 適応フィルタと適応処理アルゴリズム

第1章では，AIにつながる「機械学習」アルゴリズムの基本になる数理的な取り扱いにフォーカスして，「勾配（最急）降下法」，「最小2乗法」，「線形予測」などの物理的な意味，考え方や計算処理の流れを説明した．

本章では，AIの基本的な機能「学習して賢くなるコンピュータ」の前準備として，**システムがその利用環境に合わせて自動的に特性を変えること**のできる適応信号処理について解説する．

じつは，脳の情報処理方式を模擬しようとするニューラル・ネットワークにおける「機械学習」は，適応信号処理の最適化計算アルゴリズムを拡張したもので，「勾配（最急）降下法」を利用する．

2.1 システムが自動学習する適応フィルタ

● 適応って，なんだろう？

もともと生物学の用語であって，「外界や周囲環境の変化に応じて，自己の特性をそれに順応できるよう，自動的に再調整していく機能」を指している．

外界の変化にすばやく対応して変身する‘擬態’生物のようでもある．たとえば，カメレオンが外界の色に応じて皮膚の色を変えていくがごとくに．

生物系に見られるこの優れた機能を，工学システムに導入しようとする試みは，身近なところではエアコンの温度や湿度の自動制御，ロボットのインテリジェント化と称される適応制御など，多種多彩である．

さて，「学習して賢くなるコンピュータ，そんなのあるわけないよ」と思われるかもしれない．でも，知る人ぞ知る『**適応フィルタ**（**ADF**：adaptive digital filter）』と呼ばれる**ディジタル信号処理**がある．

適応フィルタ（別名，学習フィルタ）とは，信号の性質が時間的に変動するような場合に，フィルタ係数を自動更新し，その変動に追従させながら適応的・自律的な信号処理を行うものである．従来の時間的に特性が変化しない固定的なしくみより，一歩進んだ信号処理形態といえる．

昨今スマホなどの無線機器を，ビルの狭間や，移動する列車や自動車で使用することも多い．このようなとき電波の伝搬特性はさまざま変動しているが，明瞭な音声通信や正確なデータ通信が可能であるのは，電波環境に適切に応じて，最適な送受信技術が確立されているからである．こんなことが保証されているのも，適応的な信号処理形態が支えているというわけだ．

● 適応システムの基本構成

一般的な適応フィルタを用いたシステムの基本的な構成要素のブロック図を，**図2.1**に示す．「適応フィルタ」という用語は，図中の適応処理アルゴリズムに基づいて自動的に係数更新する機能を有するブロックを指す．

図2.1の適応システムには，適応フィルタの入力$x[k]$以外にもう一つの入力端子がある．所望（目標）の信号$d[k]$として，別のシステムから出力された信号が入力される．

所望の信号$d[k]$と適応フィルタからの出力$y[k]$の差が適応システムの出力，すなわち，

$$\varepsilon[k] = d[k] - y[k] \quad \cdots\cdots(1)$$

となり，これは誤差と呼ばれる．ただし，通常，適応フィルタの出力$y[k]$は，入力$x[k]$に対して，

$$y[k] = w_0[k]x[k] + w_1[k]x[k-1] + \cdots + w_M[k]x[k-M] \quad \cdots\cdots(2)$$

で表される重み付け総和（積和計算）として計算される．式(2)の$\{w_m[k]\}_{m=0}^{m=M}$は，乗算するときの係数で．自動更新されて時々刻々と変化する．

一般的に，適応システムでは実際の適応フィルタの

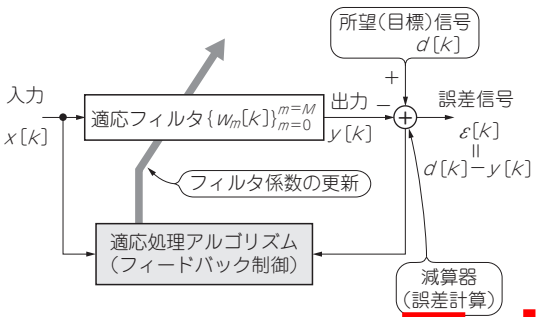


図2.1　適応システムの基本構成

出力$y[k]$を所望の出力$d[k]$に近づけていく計算処理が行われる．すなわち誤差の2乗値$\varepsilon^2[k]$が最小になるよう，適応フィルタの係数を何回も自動更新する仕掛けが組み込まれている．そうして，$\varepsilon^2[k] \fallingdotseq 0$になるように係数が収束すれば，$y[k] \fallingdotseq d[k]$となる．原理的に，適応処理アルゴリズムは誤差$\varepsilon^2[k]$の値が最小になるように収束動作を行う．

適応処理アルゴリズム（係数の自動更新）の中身は後回しすることにして，まずは適応フィルタを用いて具体的にどのようなアプリケーションが実現可能なのか，代表的な4種類の応用例を紹介しよう．

●［例1］システム同定

図2.2は，システム同定（**システム推定**ともいう．**未知システムの動的モデルを構築**）するための適応システムである．

この適応システムでは，ある信号$x[k]$を周波数特性$H(\omega)$の未知システムに入力したときの出力が，所望の信号$d[k]$となる．

すなわち，式(1)の誤差$\varepsilon[k]$の2乗値$\varepsilon^2[k]$を最小化するように適応処理アルゴリズムを動作させたとき，信号$y[k]$を出力する適応フィルタの周波数特性$W(\omega)$は未知システムに一致し，$W(\omega) = H(\omega)$となる．つまり，**図2.2**のシステムは，同一入力に対して同一出力が得られるよう係数更新を繰り返す処理で，未知システムの信号処理の中身が解明できて，周波数特性$H(\omega)$が推定されるというわけだ．

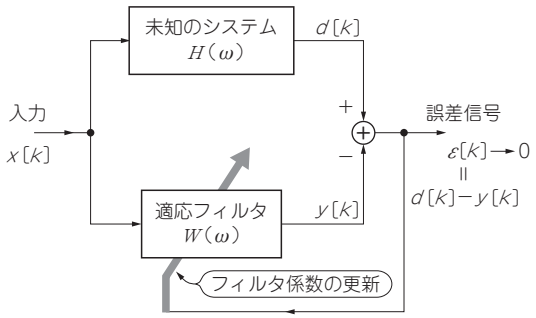


図2.2　適応システムは未知システムを同定（推定）する

●［例2］予測器

図2.3は，信号予測する適応システムである．システムの入力$x[k]$は，遅延回路でnサンプル前に入力された$x[k-n]$が適応フィルタの入力になる．

適応フィルタは，過去の信号$x[k-n]$から未来の信号$x[k]$を予測して，適応フィルタの出力$y[k]$が$x[k]$を近似するように動作する．「未来の信号を予測することは不可能だ，こんなことできない」と思われるかもしれない．しかし，入力$x[k]$が**周期的に変動する性質**をもっていれば，過去の値から未来の値を求めることは可能である．

この予測器に，ランダム雑音が混じった周期性を有する信号を入力すると，適応フィルタは周期性信号に対してだけ予測動作が機能することになる．結果，適応フィルタからはランダム雑音が取り除かれた‘きれいな信号$y[k]$’が出力され，誤差$\varepsilon[k]$の端子にはランダム雑音が得られる．

●［例3］等化器（イコライザ）

図2.4は，等化器の機能をもつ適応システムであり，任意の周波数特性$H(\omega)$をもつシステムと周波数特性$W(\omega)$の適応フィルタが直列接続されている．

また，遅延回路は直列接続した二つのシステムの処理遅延の影響をキャンセルするためのものである．このとき，所望の信号$d[k]$は，入力$x[k]$をnサンプル遅延された信号$x[k-n]$なので，入力$x[k]$と同じ周波数特性をもつことになる．

適応フィルタは，任意のシステムの周波数特性$H(\omega)$を補正して得られる出力$y[k]$と遅延させた$x[k-n]$との誤差$\varepsilon[k]$，すなわち，

$$\varepsilon[k] = x[k-n] - y[k] \quad \cdots\cdots(3)$$

の2乗値$\varepsilon^2[k]$を最小化するように動作する．このとき，

$$\begin{pmatrix}\text{遅延回路の}\\ \text{周波数特性}\end{pmatrix} = \begin{pmatrix}\text{直列接続した二つの}\\ \text{システムの周波数特性}\end{pmatrix}$$

となり，遅延回路の周波数特性（振幅）は1なので，

$$|H(\omega)||W(\omega)| = 1 \quad \cdots\cdots(4)$$

で表される関係が成立し，等化器の働きをする．この結果に基づき，

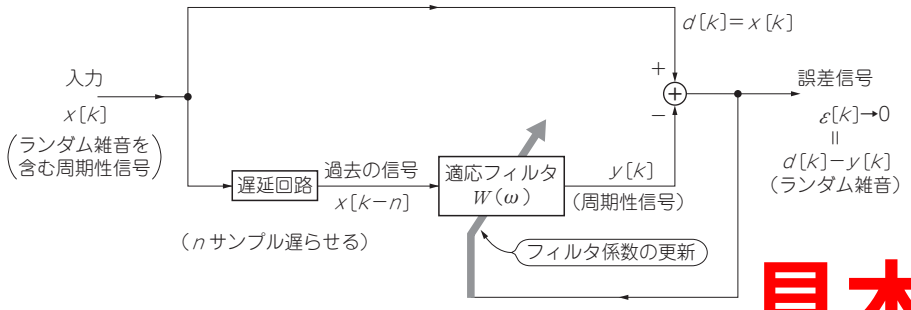


図2.3　適応システムは未来の信号を予測する

第10章 誤り訂正符号の基礎

本章では，具体的な誤り訂正符号の第一歩として「ハミング符号」を取り上げ，ハミング符号がパリティ符号を拡張したものであること，そして符号化と復号化のしくみについてわかりやすい形で説明する．さらに，より汎用性の高い線形符号の導入を行う．

10.1 誤り検出/訂正のしくみ

ある一定のハミング距離を保った符号語の中から，いくつかの符号語を用いることは，別の視点から見てみると，任意に選んだ冗長度のない符号系列に適当な符号を付加して冗長度を増すことであるとも考えられる．つまり，情報を送る符号と誤りの検出訂正の検査符号を分ける考え方に，誤り検出/訂正の基本的なコンセプトが隠されている．

たとえば，家庭の主婦が洗濯した後，物干しに干そうとして，「あれっ，靴下が足りない」とすっとんきょうな声を発したとする．これは，靴下の数をかぞえていたのではなく，靴下には「偶数である」という情報があることに基づいている（**図10.1**）．

この「偶数である」という情報は靴下に冗長度として付加されているもので，実はこれだけでも意外と多くの情報を誤りなく伝えることができる．これに反し，たとえば同時にハンカチがなくなっていたとしても，なかなか気づきにくいことも事実である．

靴下と同じように，情報符号に検査符号として「偶数である」という情報を常にもたせるようなしくみが誤り検出/訂正の考え方の基本であり，これが**パリティ検査**とよばれるものである．

一つの例を挙げてみよう．いま，**図10.2**の左の3ビットの情報符号にもう1ビットの検査符号を付加して0000からの**ハミング距離**（**重み**ということもある）が偶数個になるようにする．それが右の誤り検出のための検査符号（パリティ・ビット）を付加した4ビットの符号である．

また，**図10.2**の符号を1列ずつ縦に並べて8列にし，さらに1行ごとに偶数パリティを付けてみることにしよう（**図10.3**）．ここで，○で囲んだビットが誤ったと

図10.1　偶数パリティで洗濯物をチェック

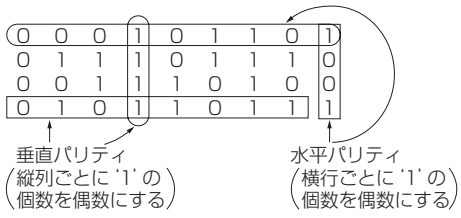


図10.3　垂直水平パリティ符号の構成

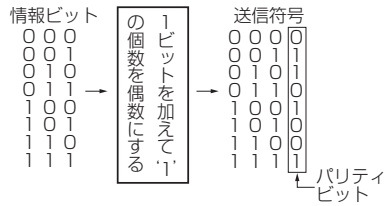


図10.2　パリティ検査とは

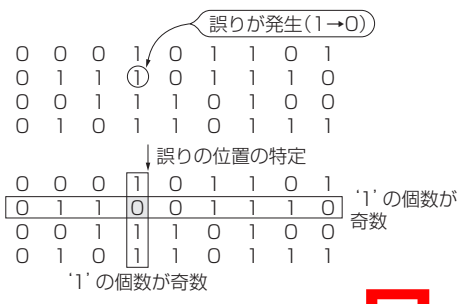


図10.4　垂直水平パリティ符号による誤り訂正例

すると，○を含んだ行と列（□の中）に含まれる‘1’の個数が奇数個に変化することから，誤りが発生したビットを特定して誤りを訂正できることになる（**図10.4**）．

つまり，パリティ検査のビットを組み合せることで誤りの訂正が可能になる．ここに，誤りビットを特定するしくみとなる誤り訂正符号の基礎をなす考え方がある．

このように，パリティ符号を二次元化したものとして行と列の縦/横のパリティ検査ビットを付加したものは磁気テープなどで用いられ，**垂直水平パリティ符号**と呼ばれる．もちろん，2個以上の誤りがあると訂正できない．

10.2 ハミング符号を作ってみよう

一般に，各符号語間相互のハミング距離の最小値がd_{min}であれば，$(d_{min}-1)$個までの誤りを検出でき，$\lfloor (d_{min}-1)/2 \rfloor$個の誤りまで訂正することができる（**9.6**を参照）．ここで，$\lfloor x \rfloor$はガウス記号で，xを越えない最大の整数値を表す．

誤り訂正符号を構成する方法として，パリティ検査を利用した**ハミングの方法**がある．いま，kビットの情報符号（情報数は最大2^k個）のそれぞれにmビットの検査符号（冗長ビット）を付加し，全体の符号長がnビット（$n = k+m$）となる符号系列を考えることにする（**図10.5**）．

つまり，

n：全体の符号ビット数（$n = k+m$）

k：情報ビット数

m：検査ビット数（冗長ビット数）

とするとき，nビットの符号系列の中に1ビット以下の誤りがあると仮定してみよう．このとき，mビットの検査符号の情報（最大2^m個の組み合わせ）から誤りの発生したビットを特定する必要があるわけで，

- まったく誤りのない場合
- 第1ビット目に誤りがある場合
- 第2ビット目に誤りがある場合
- ⋮
- 第nビット目に誤りがある場合

の$(n+1)$個の区別が必要である．

したがって，

$$\begin{pmatrix}\text{検査符号で表される}\\ \text{情報数}\end{pmatrix} \geqq \begin{pmatrix}\text{誤りが発生する}\\ \text{場合の数}\end{pmatrix}$$

であり，すなわち，

$$2^m \geqq n+1 \quad \cdots\cdots (1)$$

となる．ここで$n = m+k$を代入して整理すると，

$$2^m - m \geqq k+1 \quad \cdots\cdots (2)$$

という関係が，情報ビット数kと検査ビット数m（$= n-k$）との間に成立しなければならない．このような形で，情報ビットにいくつかの検査ビットをある規則に基づいて付加したものの全体から作られた符号のことを**組織符号**という．とくに，全体の符号長がnビットで，そのうちの情報ビットがkビットである符号のことを，一般に(n, k)符号と呼ぶ．たとえば，式(2)の等号が成立するときのnとkの組み合わせを**表10.1**に示す．

たとえば，もとの情報が4ビットの符号系列であれば$(m=4)$，**表10.1**より少なくとも3ビットの検査符号$(k=3)$が必要となる（**図10.6**）．

ここで，誤りの発生の有無をチェックするためのパリティをs_1，s_2，s_3としよう．次に，このs_1，s_2，s_3を2進数とみなし，計算した値がちょうど誤りが発生したビットを示すようにパリティチェックすることを考えてみることにする．そのためには，**表10.2**に示す関係が成立しなければならないことは明らかである．

表10.2から，誤りの発生したビットが，x_4，c_1，c_2，c_3であれば，$s_1 = 1$でなければならないことがわかる．つまり，

$$s_1 = x_4 \oplus c_1 \oplus c_2 \oplus c_3 \quad \cdots\cdots (3)$$

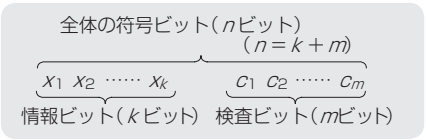


図10.5　ハミング符号の構成

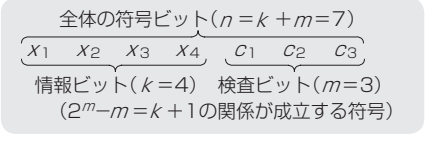


図10.6　(7, 4) ハミング符号の構成

表10.1　(n, k) ハミング符号の例

符号全体のビット数（n）	3	7	15	31	63
情報ビット数（k）	1	4	11	26	57
検査ビット数（m）	2	3	4	5	6

表10.2
検査ビット

s_1	s_2	s_3	誤りの位置
0	0	0	誤りなし
0	0	1	x_1
0	1	0	x_2
0	1	1	x_3
1	0	0	x_4
1	0	1	c_1
1	1	0	c_2
1	1	1	c_3

第19章 暗号応用——ゼロ知識対話証明，認証，ディジタル署名

第18章では，実際に使用されている1ブロックが64ビットのDES暗号の一般的構成，DES暗号アルゴリズムを活用した連鎖式ブロック暗号，ストリーム暗号を例示した．

本章では，暗号数学の今後の展開をにらみながら，ゼロ知識対話証明，個人の認証，ディジタル署名，ブロックチェーンなどについて，基本的な考え方を中心にわかりやすく説明する．

19.1 ゼロ(零)知識対話証明

‘ゼロ知識対話証明’という言葉から，みなさんはどんなことを想像されるであろうか？ おそらくは，多くの方々が「知識がゼロでも（何も知らなくても），何らかの事柄を証明する（暗号の話なのだから，個人の認証を行う）ことができる」という意味なのかな，というイメージがおぼろげながら湧くのではなかろうか．わかりやすく言えば，

『自分の秘密情報（たとえば，パスワードなど）を漏らさずに（ゼロ知識），相手に自分がその秘密を持っているという事実だけを信じてもらう（証明）という数理マジック』

がゼロ知識対話証明と呼ばれるものである（**図19.1**）．

最近のカード社会では，クレジットカードを使って国際電話をかけた人が，その番号を電話機に入力するところを何者かに望遠鏡で覗き見されてパスワードがばれたり，デパートで買い物代金のカード支払いのときにカード情報をすべて読み取られてしまい，多額の料金を請求されるといった‘なりすまし’事件も多発しているようである．

このように，本人確認のために，その人（カード）の秘密が外に漏れてしまうことには，大いなる危険がつきまとうことになる．そこで，秘密については一切漏らさず（ゼロ知識），本人の確認（カードの真正性）を相手に認めてもらう（証明）方法が必要不可欠になってくるのである．

こうした要求に応える方法として，1985年にGoldwasser，Micali，Rackoffにより，‘ゼロ知識対話証明’という概念が示された．

ゼロ知識対話証明は，自分の持っているカードの真正性を相手（カード会社）に証明する方法である．その際，カード自体の秘密（パスワードで，たとえば10進数で100桁以上の乱数）に関する情報は一切漏らさない．このような，

『秘密の乱数は教えないけれど，自分を証明するための乱数を持っていることは信じてほしい』

という，虫のいい話がゼロ知識対話証明なのである．こんな虫のいい話が，厳密な暗号数学の理論をもとに，何とも信じがたいことなのではあるけれど，実現できるのである．その実現方法について，準備段階と実行段階とに分けて説明することにしよう．

● 準備段階

ゼロ知識対話証明における数理マジックの仕かけのためには，まずは信頼すべきセンタ（検証者）を設けることが必要である．例を挙げて説明しよう．

① 全ユーザに公開する合成数Nの設定

センタは二つの素数（p，q）を用意し，さらに積をとって合成数N，すなわち，

$$N = pq \quad \cdots\cdots(1)$$

をセンタの秘密とする．実際は，100桁程度の巨大な素数を利用するわけだが，ここでは簡単な例として，2桁の素数13（$= p$）と19（$= q$）を用いることにする．これら二つの素数の積Nは，

$$N = 13 \times 19 = 247$$

の3桁の合成数である．この合成数Nは，全ユーザに公開する．ただし，実用システムでは，合成数$N = pq$

図19.1　ゼロ知識対話証明とは？

を知ったとしても元の素数pとqに分解することが，どのようなスーパコンピュータを用いたとしても難しい程度に大きな桁数を有する素数を用意する．

② 各ユーザのIDをセンタに登録

IDとは，IDentificationの略で，各ユーザが公開している数値（公開鍵に相当）であり，その人と1対1の対応がとれている，つまり各ユーザを識別できる公開された数値であり，ここではIDと称することにする．

各ユーザは，これをセンタに登録することになる．たとえば，ここではユーザAのIDをID_Aで表すことにする．

③ センタによる各ユーザの秘密鍵の計算と通知

センタは各ユーザからの登録されたIDをもとに，そのIDの平方根を計算する．

実数における平方根の計算は，だれでも計算できるわけだが，整数の世界では合成数Nの二つの素数pとqを知っている場合のみ，その平方根が容易に求められるという性質があることが知られている．この平方根を計算する難しさを利用して，ゼロ知識対話証明の仕かけが作られている．

いまの場合，センタだけが素数13と19を知っているので，各ユーザから登録されたIDの平方根を計算できるというわけである（秘密が漏れない）．仮にID_A（ユーザAのID）を101としよう．このとき，その平方根は71となる．

$$\sqrt{101} \pmod{247} = 71$$

逆に，71を2乗したものは，

$$71^2 \pmod{247} = 101$$

となるというわけである．この71がユーザAの秘密鍵S_Aであり，秘密裏にユーザAに届けられる．実用上は100桁以上の数字が使われるので，Aが覚えられる数ではない．一般的には，ユーザAのID（ID_A）と秘密鍵S_Aとの間には，

$$\sqrt{ID_A} \pmod{N} = S_A \quad \cdots\cdots(2)$$

$$(S_A)^2 \pmod{N} = ID_A \quad \cdots\cdots(3)$$

という関係が成立している．

なお，秘密鍵S_Aの目的は，ユーザAその人自身の確認ではなく，Aが所持するカードの真正性を確かめることにあるわけで，Aが銀行でのキャッシュカードの暗証番号のように記憶しておく必要もないのである．その他のユーザに対しても同様な手順で各々の秘密鍵が配られる（**図19.2**）．

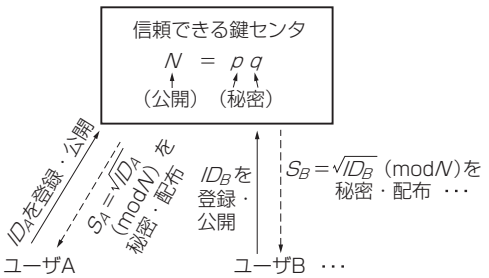


図19.2　鍵の配布

● 実行段階（証明手順）

いま，ユーザAがユーザBに対して，自分が正真正銘のAである（自分が所持しているカードが本物である）ことを証明したいとして，その証明手順を以下に示す．

［ステップ1］ユーザAからユーザBへの証明依頼（その1）

まず，ユーザAは適当に乱数r_Aを選んで2乗し，合成数Nで割って余りを求め，この余りy_A，すなわち，

$$y_A = (r_A)^2 \pmod{N} \quad \cdots\cdots(4)$$

をユーザBに送る．たとえば，ユーザAが乱数r_Aとして50を選んだとしよう．このとき，

$$y_A = 50^2 = 2500 = 30 \pmod{247}$$

であるから，30をユーザBに送る．

［ステップ2］ユーザAからユーザBへの証明依頼（その2）

次に，ユーザAは自分がセンタからもらった秘密鍵S_Aと**［ステップ1］**で選択した乱数r_Aとの積に対して合成数Nを法とする計算，すなわち，

$$z_A = S_A r_A \pmod{N} \quad \cdots\cdots(5)$$

を行ってユーザBに送る．先に乱数r_Aとして選んだ50を例について言えば，

$$z_A = 71 \times 50 = 92 \pmod{247}$$

をユーザBに送ることになる．

［ステップ3］ユーザBによるAの真正性の確認作業（その1）

まず，ユーザBはユーザAから**［ステップ2］**で送られてきたz_Aを2乗して合成数Nを法とする計算，すなわち，

$$v_A = (z_A)^2 \pmod{N} \quad \cdots\cdots(6)$$

$$= (S_A r_A)^2 \pmod{N} \quad \cdots\cdots(7)$$

を行う．いまの例では，$z_A = 92$であるから，

$$v_A = 92^2 = 8464 = 66 \pmod{247}$$

となる．

［ステップ4］ユーザBによるAの真正性の確認作業（その2）

さらに，ユーザBは**［ステップ3］**で求めたv_Aを**［ステップ1］**でユーザAから送られてきたy_Aで割った値，すなわち，

$$w_A = \frac{v_A}{y_A} \pmod{N} \quad \cdots\cdots(8)$$

$$= v_A \times \left(y_A^{-1}\right) \pmod{N} \quad \cdots\cdots(9)$$

を計算する．もちろん，すべての計算は法Nを

ISBN978-4-7898-5000-1
C3055 ￥2300E
CQ出版社

定価：本体2,300円（税別）

9784789850001
1923055023000

情報処理・信号処理応用の未来はAIにある

AI（人工知能）の核になる処理は，
　推論…知識をもとに新しい結論を得ること
　学習…情報から将来使えそうな知識を見つけること
に大別され，以下の5タイプがあります．

- ▶「言語」を扱うAI
- ▶「画像」を扱うAI
- ▶「音声」を扱うAI
- ▶「制御」を扱うAI
- ▶「最適化や推論」を扱うAI

本書は，AI社会での情報数学応用を見据えて，現実生活に登場するさまざまな情報理論を系統立て，ていねいに解説します．

本書は「やり直しのための工業数学」（三谷政昭著，2001年1月CQ出版社刊），「改訂新版 やり直しのための工業数学 情報通信編」（三谷政昭著，2011年5月CQ出版社刊），「改訂新版 やり直しのための工業数学 信号処理&解析編」（三谷政昭著，2012年5月CQ出版社刊）の一部を流用し，4部構成とした加筆改訂版です．