ま　え　が　き

本書は，通信理論の解説書である．ここでいう通信とは，距離あるいは時間の隔たりを越えて情報を伝達/交換することを指す．東京から大阪の友人に電話やメールをしたり，映像や音楽を記録メディアに記録し，あとで観賞したりするのは，距離ならびに時間を超えた通信の例である．

例えば，人間の発する声/言葉などの情報を即時に遠方まで運ぶには，声などをそれが可能な物理量に変換して伝達する必要がある．この条件を満たしてくれたのがいわゆる電気通信である．

電気通信においては，人や計算機などが発する情報を距離的あるいは時間的に隔たった宛先 (相手) へ届けるため，送信機などと呼ばれる装置によって情報を加工して光 (電磁波) や電気信号に変換し，通信路 (自由空間や光ファイバケーブルや記録媒体など) を通して，宛先 (受信側) へ伝達する．受信側では，受信機などと呼ばれる装置によって，受信された電気信号から人や計算機が発した元の情報を復元することになる．このとき，いずれの通信路においても

(a) 物理的な障害 (雑音，帯域制限，歪など)，(b) 人為的な妨害

などが存在するため，送信された信号がそのまま形を変えずに受信側に現れることはない．したがって，これらの妨害を克服して，情報をいかに，

(1)「正確」，かつ (2) 速く (大量に)，そして (3) 安全に

伝えるか，が通信工学の課題となる [†1]．通信理論の目的は，上記の (1)，(2)，(3) を最大限実現する通信方式の解明にある．

まず情報を「速く」あるいは「大量に」という要請であるが，これに答えるためには，そもそも情報はどう測られるべきかを知らなくてはならない．その答えは 2 章に述べられている．

[†1] 「正確」であることは大前提である．不正確な情報をいくら速く送っても意味がない．

すると次には，情報表現の冗長性が問題になる．一つのことを 1 回話しても，3 回話しても，相手に伝わる本質的な情報の量は変わらないと考えられる．3 回話すのは無駄で 1 回話せば十分ということである．自然言語などは普通多くの無駄を含む．このような無駄 (冗長性) を除くと，情報はどこまで短く簡潔に表現できるであろうか？「情報圧縮の限界」と「その限界を達成する方法」が 3 章，4 章に述べられている．

次に，与えられた通信路を通して，情報を伝達しようとしたとき，誤りなく伝達できる情報量の限界が問題になる．上に述べたように，通信路には雑音などの妨害が存在する．このとき，その雑音の性質や大きさにより，各通信路は「通信路容量」と呼ばれる，通信路固有の特徴量 C を持つことが示される (5 章)．ここで，k シンボルで表される情報に $n-k$ 個の冗長シンボルを付け加え，n シンボルの符号語に変換して通信路に送出するとする．すると，情報伝達のスピード $R := k/n$ が $R < C$ を満たすならば，冗長シンボルを「うまく」選ぶことにより，この通信路を通して誤りなく情報を伝達できることが示される．この事実は通信路符号化定理として知られ，通信理論の最も重要な結果の一つである (6 章)．近年この情報伝達速度の限界 (通信路容量) を達成する具体的な符号の有力な候補として LDPC 符号が注目されている．本書ではその入門的な解説をやや丁寧に述べるようにした (6 章)．

最後に，悪意のない単なるミスを含む人為的な妨害による情報の変化などを排して情報を安全に通信することが要請される．このための技術が「セキュリティ技術」であり，その中心に「暗号技術」がある．これに関する入門的解説を述べたのが 8 章である．

さて，本書を著すにあたっては次の点に留意した．必要な予備知識はできるだけ少ないこと，しかし証明などは省かず本書だけで完結して読み切れること，である．具体的には，予備知識としては大学入学程度の数学的基礎だけを仮定し，残りは本書を読み進むことによって理解できるよう，一通りの証明は漏らさないように心掛けた．そのため，いくつかの章に付録という形で，必要な数学的基礎事項をまとめている．

本書の内容は，基本的にシャノン (C.E. Shannon) によって提唱された「通信の数学的理論 (A Mathematical Theory of Communication)」(巻末の参考文献 1)) に述べられた内容である．日本では，この内容の書物は「情報理論」ということが多い．しかし本書では原点に立ち返るという意味でも，また内容をより的確に表す意味でも「通信理論」とすることが適切と考えた．また記述に関しても，できるだけ原典に近い記述を心掛けるように努めた．科学技術を切り開いてきた先人達の考え方に触れることは，自らが新しい発見をしていく際の助けになるであろうと考えたからである．

講義のテキストとして使用されるときには，多少具体的な例を付け加えて説明いただくとよいように考える．学生はこれにより，話の概要を理解し，その後にこのテキストを読み返すことで，数学的/理論的内容まで理解を進めることができるようになると期待される．

世の中に通信理論 (情報理論) に関する名著/良書は少なくない．したがって，本書にどれほどの存在意義があるかについては疑問が残らないわけではないが，上に述べた点において，内容/記述法において多少の特色はあるものと考える．本書が，通信理論を学ぼうとする学生諸君にとって，何らかの意味でお役に立つことができれば，著者にとって望外の喜びである．

最後に，原稿に目を通して多くの貴重な指摘とコメントをいただいた，神奈川大学野崎隆之博士に感謝する．また辛抱強く原稿を待って下さったコロナ社に感謝する．

平成 26 年 7 月

坂庭好一，笠井健太

目　　次

1. 通信理論の概要

2. 情報源のモデルと情報量

3. 情報源符号化定理

4. 代表的な情報源符号

5. 通信路モデルと通信路容量

6. 通信路符号化定理

7. 連続情報と連続通信路

8. 情報セキュリティの基礎 ―暗号理論の初歩―

1 通信理論の概要

1.1 通信の目的とモデル

〔**1.1.1**〕**通信**の目的は，距離的あるいは時間的な隔たりを越えて情報を交換することにある．距離的な隔たりを越えた通信の具体例としては，東京から大阪へ電話を掛けたり，アメリカからテレビ中継したりすることが挙げられる．このような距離を越えた通信においては，即時 (リアルタイム) 性が要求されることが多い．一方，CD (Compact Disc) に録音された音楽を鑑賞したり，DVD (Digital Versatile Disc) や BD (Blu-ray Disc) に記録された映画やテレビ番組を見たりするのは，時間を超えた通信の例である [†1]．

最も基本的な音声による通信を考えてみよう．大昔から人間が行ってきた通信のやり方は対面して話をすることである．しかし，この方法では遠く離れた相手と話をすることはできない．音は距離が隔たるにつれて大きく減衰するため，遠くまで到達しないからである．したがって，距離を克服して通信を行うには，人間の発する情報を即時に遠くまで伝達可能な物理量に変換して伝達する必要がある．この条件を満たしてくれたのがいわゆる**電気通信**である．

〔**1.1.2**〕電気通信においては人やコンピュータなどが発する情報を距離的あるいは時間的に隔たった宛先 (相手) へ届けるため，**送信機**あるいは**符号器**と呼ばれる装置によって情報を加工した後，光 (電磁波) や電気信号に変換し，**通信**

[†1] 時間を超えた通信 (記録) では，情報の誤りが心配されても問い合わせできないことが多い．したがって，特に正確性に対する要求の強いことが考えられる．

路 (自由空間や光ファイバケーブルや記録媒体など) を通して，受信側へ伝達する．受信側では，**受信機**あるいは**復号器**と呼ばれる装置によって，受信信号を人やコンピュータが発したもとの情報に戻すことになる．これを図示すると**図 1.1** のように書くことができる．通信は双方向が基本であるが，**図 1.1** はその片方を記述していることになる．また，多数が会議を行うような通信も考えられるが，その場合も**図 1.1** が基本の構成要素である．

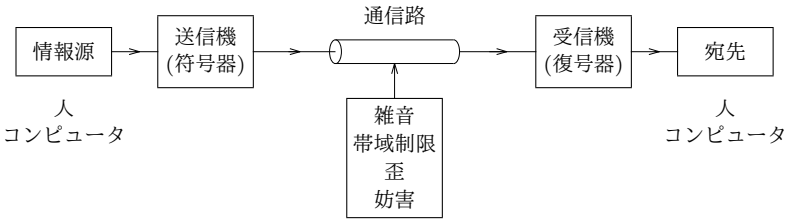

図 1.1　電気通信のモデル

さて，**図 1.1** において通信路と記した部分は，空間伝搬路であったり，光ファイバやメタリックケーブルであったり，CD，DVD，BD などの記録媒体であったりする．いずれの通信路においても幸か不幸か送信された情報がそのままの形で受信されることはない．通信路には，

(1) 物理的な障害 (雑音，帯域制限，歪など)，(2) 人為的な妨害

が存在する．したがって，これらの障害や妨害を克服して，情報をいかに，

(1)「正確」，かつ (2) 速く (大量に)，そして (3) 安全に

伝えるか，が通信工学の課題となる [†1]．

[†1] 情報は「正確」であることが大前提である．不正確 (デタラメ) な情報をいくら (速く，安全に) 送っても意味がない．

1.2 通信理論の概要と本書の構成

前節最後に述べた通信工学の課題は，現在どのように解決されているのであろうか？その概要は次のようにまとめられる．(この結果のすべてが本質的にシャノン (C.E. Shannon) の貢献[1),2)]によっている．また巻末に示すように多くの優れたテキストが存在する[3)~9),11)~19)]).

〔**1.2.1**〕まず情報を「速く」あるいは「大量に」という要請であるが，それにはそもそも情報はどう測られるべきかが問題になる．情報の測り方が決まらなければ，「速く」も「大量に」も議論できない．

情報の例として，人の話や文章を考えてみよう．人の話や文章は，文字 (シンボル) の集合 $A := \{a_1, a_2, \ldots, a_M\}$ [†1] から発せられる文字 (シンボル) の系列 $x_1 x_2 \cdots$ $(x_i \in A)$ と捉えることができる．このとき，情報の測り方に関する検討を行うと，**2 章**に述べるように，各文字の情報は $-\log_2 p(a_i)$［ビット］のように測るのが妥当であることが導かれる．ただし，$p(a_i)$ は文字 (シンボル) a_i が発生する確率である．

〔**1.2.2**〕次に，与えられた情報の表現に無駄がないかどうかが問題になる．例えば人の言葉 (自然言語) は多分に「冗長」である [†2]．逆にいうと，話の本質的な内容 (情報の量) は変えることなく，もっと簡潔に表現できるのである．では，情報はどこまで簡潔に表現できるのであろうか？

表現の簡潔さを，情報表現に必要な「文字列の (平均的) 長さ」で測ることにすると，その下限は**平均情報量** (あるいは**エントロピー**)

$$H(A) := \sum_{i=1}^{M} -p(a_i) \log p(a_i) \tag{1.1}$$

---

†1 A は，英語ならば $A := \{a, b, \ldots, z, \sqcup\}$，日本語ならば $A :=$ { あ, い, う, . . . , ん } で与えられるアルファベットである．

†2 この冗長さのために，多少「話」を聞き漏らしても，意味を取り違えることを少なくできている．人間同士の会話では，この冗長さは有効に機能していると考えられる．

で与えられることが示される †1．逆に $H(A)$ に限りなく近い長さの簡潔な表現が可能なことも導かれる．表現を簡潔にする操作は**情報源符号化**または**情報圧縮，データ圧縮**などと呼ばれ，情報を記録したり，伝達したりするときに，事前になすべき重要な操作となる．情報圧縮の限界が式 (1.1) によって与えられることは **3 章**で，またその限界を達成すべく考案された圧縮アルゴリズムについては **4 章**に述べる．

〔1.2.3〕 その次には，(簡潔に表現された) 情報を，(1) 遠く離れた場所へ送信してそれを受信したり，(2) 記録してそれを再生したり，することが行われる．このとき，受信したり再生したりした情報は，一般にもとの情報とは異なる．この原因の第一に挙げられるのが，**雑音**と呼ばれる物理的障害である．

〔5.1.1〕で見るように，実際に広く用いられている通信方式として，情報を 2 値 (正，負のパルスや $\{0,1\}$) の系列によって表現し，それを伝送したり，記録したりする方式がある．このとき，上に述べた雑音の影響は，**図 1.2** に示すような通信路モデル (遷移図) によって表すことができる †2．この通信路モデルは **2 元対称通信路 (BSC)** と呼ばれ，ε は**ビット誤り率**と呼ばれる．

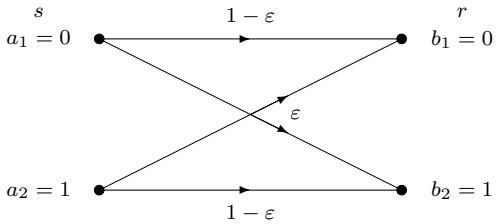

図 1.2　2 元対称通信路 (BSC)

†1　記号「:=」は定義を表す．$A := B$ は「A は B で定義される」ことを表す．

†2　**図 1.2** において，送信シンボル s ならびに受信シンボル r は，共に 2 値のシンボル $a_1 = 0$，$a_2 = 1$ ならびに $b_1 = 0$，$b_2 = 1$ をとるとしている．

〔**1.2.4**〕 さて，**図 1.2** に示したような通信路を通して，送信シンボル一つ (a_i とする) を送信して，受信シンボル一つ (b_j とする) が受信されたとしよう．(これが通信の基本機能である)．このとき，この通信によって，どれだけの情報が伝えられたのであろうか？

通信が行われる前，送信シンボル a_i の持っていた情報量は，$-\log_2 p_s(a_i)$ [ビット] であった．通信が行われた後を考えると，受信側ではシンボル b_j が受信されている．したがって，送信シンボル a_i の情報量は，$-\log_2 p_s(a_i)$ [ビット] から，$-\log_2 p_{s|r}(a_i|b_j)$ [ビット] に変化していることになる．($p_{s|r}(a_i|b_j)$ は条件付き確率．〔1.3.6〕参照)．送信シンボル a_i に関するこの情報量の変化分

$$I(a_i;b_j) := -\log_2 p_s(a_i) - [-\log_2 p_{s|r}(a_i|b_j)] \tag{1.2}$$

が，a_i が送信されて b_j が受信されたという「通信」によって，送信側から受信側へ伝達された情報量 (**伝達情報量**と呼ぶ) と解釈することができる．

〔**1.2.5**〕 情報源の平均情報量 (エントロピー) を考えたのと同様に，(1 シンボル当たりの) 伝達情報量 $I(a_i;b_j)$ を，(**図 1.2** の) 通信システム全体にわたって平均した量

$$I(A;B) := E\left[I(a_i;b_j)\right] = \sum_i \sum_j p_{s,r}(a_i,b_j) I(a_i;b_j) \tag{1.3}$$

を考える (**平均伝達情報量**と呼ぶ)．そして，この平均伝達情報量 $I(A,B)$ を，送信シンボルの出現確率 $\{p(a_i)\}_i$ に関して最大化した値を

$$C := \max_{\{p(a_i)\}_i} I(A;B) \tag{1.4}$$

とおく．C は，通信路 $\{p_{r|s}(b_j|a_i)\}_{i,j}$ だけで決まる，通信路固有の量で，**通信路容量**と呼ばれる．**図 1.2** の BSC の通信路容量は

$$C = 1 - \mathcal{H}_2(\varepsilon), \quad \mathcal{H}_2(x) := -x\log_2 x - (1-x)\log_2(1-x) \tag{1.5}$$

で与えられることが示される．通信路容量については，**5 章**，**7 章**で述べる．(**5 章**では，いわゆる**離散無記憶通信路**について，また **7 章**では，物理的実体である**連続通信路**について述べている)．

〔**1.2.6**〕与えられた (**図 1.2** の) 2 元通信路を通して，情報を (できるだけ) 誤りなく伝達するために，k シンボルで表される情報 $(c_1, c_2, \ldots, c_k)$ に $n-k$ 個の冗長シンボル $(c_{k+1}, \ldots, c_n)$ を付け加え，長さ n の 2 元符号語

$$\boldsymbol{c} = (c_1, c_2, \ldots, c_k, c_{k+1}, \ldots, c_n), \quad c_i \in \{0, 1\} \tag{1.6}$$

に変換して通信路に送出するものとする．(この操作を**通信路符号化**と呼ぶ).

このとき，通信路容量 C は，その通信路を使って誤りなく伝達できる情報伝達速度の最大値を与える．すなわち，概(おおむ)ね次の関係が成り立つ：

> **定理**： 誤りのない情報伝達を実現する式 (1.6) の形式の符号が存在するための必要十分条件は，「**情報伝達速度** $R := k/n$ が $R < C$ を満たす」ことである．

この定理は**通信路符号化定理**と呼ばれ，通信理論の最も重要な結果の一つである．これに関する，より一般的な議論は，**6 章**に述べられる．

〔**1.2.7**〕最後に，人為的な妨害などを排して情報を安全に通信する技術が残されている．残念ながら，世の中には悪事を企む不逞(ふてい)の輩(やから)もおり，情報の盗聴や改竄(かいざん)などに備えなければならない．また，現代のネットワーク社会では，悪意のない単なる「ミス」によっても情報が変化し，結果において，悪意による情報操作と変わらない影響を及ぼす可能性もある．このような，情報に対する人為的妨害から情報を保護する技術が「セキュリティ技術」であり，その中心に「暗号技術」がある．これに関する入門的解説を述べたのが **8 章**である．

1.3　付録：確率の初歩

ここでは，本書の内容を理解する上で基本的である，確率の初歩と (ガウス雑音の根拠を与える) 中心極限定理などについて簡単にまとめている．

1.3.1 テイラー展開とロピタルの定理

補題〔1.3.1〕テイラー展開[†1]：$f(x)$ を，一つの区間 $I \subseteq \mathbb{R}$ (実数全体の集合) で m 回連続微分可能な関数とする．すると，$a < b$ $(a, b \in I)$ を固定したとき，

$$f(b) = \sum_{k=0}^{m-1} \frac{f^{(k)}(a)}{k!}(b-a)^k + \frac{f^{(m)}(c)}{m!}(b-a)^m \tag{1.7}$$

を満たす実数 $c \in (a, b)$ が存在する．ただし，$f^{(k)}(x)$ は $f(x)$ の k 階微分を表す．($a > b$ の場合もまったく同様に式 (1.7) が成立する)．

(証明) 与えられた $f(x)$ ならびに a, b に対して，K_m を

$$f(b) = \sum_{k=0}^{m-1} \frac{f^{(k)}(a)}{k!}(b-a)^k + K_m(b-a)^m$$

が成り立つように定める (常に可能)．そして，$a \leqq t \leqq b$ として，

$$F(t) := f(b) - \sum_{k=0}^{m-1} \frac{f^{(k)}(t)}{k!}(b-t)^k - K_m(b-t)^m$$

とおく．すると，$F(b) = 0$，$F(a) = f(b) - f(b) = 0$ が成り立つ．したがって，**ロールの定理**[45)] [†2] により，$c \in (a, b)$ が存在して，$F'(c) = 0$ が成立する．ここで，実際に $F'(t)$ を計算すれば，

$$F'(c) = -\frac{f^{(m)}(c)}{(m-1)!}(b-c)^{m-1} + mK_m(b-c)^{m-1}$$

が得られ，$K_m = \dfrac{f^{(m)}(c)}{m!}$ となって，式 (1.7) が成立する．

補題〔1.3.2〕ロピタルの定理：m 回連続微分可能な関数 $f(x)$，$g(x)$ があり，$f(a) = \cdots = f^{(m-1)}(a) = 0$，$g(a) = \cdots = g^{(m-1)}(a) = 0$，$g^{(m)}(a) \neq 0$ であるとする．すると，下記が成立する [†3]：

$$\lim_{b \to a} \frac{f(b)}{g(b)} = \frac{f^{(m)}(a)}{g^{(m)}(a)}. \tag{1.8}$$

(証明) 式 (1.7) より直ちに得られる．

[†1] **テイラーの定理**とも呼ばれる．また，$a = 0$ のときには，**マクローリン展開**と呼ばれる．

[†2] 片かっこ”・)” で示した番号は，巻末の引用・参考文献の番号を表す．

[†3] ロピタルの定理は，$f(a) = g(a) = 0$ である関数の比 $\lim_{b \to a} f(b)/g(b)$ の簡便な計算法を与える．$f(a) = g(a) = \pm\infty$ の場合にも同様の結果が成立する．

索　　引

【さ】

【し】

【す】

【せ】

—— 著 者 略 歴 ——

坂庭　好一（さかにわ　こういち）
1972 年　東京工業大学工学部電子工学科卒業
1974 年　東京工業大学大学院修士課程修了
（電子工学専攻）
1977 年　東京工業大学大学院博士課程修了
（電子工学専攻）
工学博士
1977 年　東京工業大学助手
1983 年　東京工業大学助教授
1991 年　東京工業大学教授
2014 年　東京工業大学名誉教授

笠井　健太（かさい　けんた）
2001 年　東京工業大学工学部情報工学科卒業
2003 年　東京工業大学大学院修士課程修了
（集積システム専攻）
2006 年　東京工業大学大学院博士課程修了
（集積システム専攻）
博士（学術）
2006 年　東京工業大学助手
2007 年　東京工業大学助教
2012 年　東京工業大学准教授
現在に至る

通信理論入門

Introduction to Communication Theory

2014 年 9 月 22 日　初版第 1 刷発行

検印省略

著　者　坂庭好一
　　笠井健太
発行者　株式会社　コロナ社
　　代表者　牛来真也
印刷所　三美印刷株式会社

112–0011　東京都文京区千石 4–46–10
発行所　株式会社　コロナ社
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替 00140–8–14844・電話(03)3941–3131(代)
ホームページ http://www.coronasha.co.jp

ISBN 978–4–339–02464–7　（金）　（製本：愛千製本所）
Printed in Japan