

# 世界をORする視線 (17)

## 第I部 通信・デジタル技術の発展

### (3) コンピュータの発展：コンピュータ科学の 数学的基礎 (続き 4)

住田 潮

(注：本稿は前回からの続きであるので、文献リストは継続し、新たに必要となる分を追加する)

#### 1. ベル研究所における短期滞在の成果

1940年の夏、シャノンはプリンストン高等研究所 (Institute for Advanced Study) に赴任する前の限定的な期間を、ベル研究所で過ごした。どのような研究機関であっても、どのように短い滞在期間であっても、その期間に達成すべき目標を掲げて臨むことを常としていたシャノンは、ここでも二つの大きな結果を残した [12]。一つは、ワイヤーを撚り合わせてケーブルを作る際のワイヤーの配色問題である。A, B, ..., K で表される多くの中継器やスイッチを接続するために、あるポイントではケーブルのワイヤーの一部をAのリード線として用い、別のポイントではBのリード線として... といった具合に使っていく。接続に要するワイヤー数は、ポイントごとに異なる。このような状況でワイヤーを識別するため、同じポイントで使われるワイヤーのすべてを異なる色に配色しなければならない。たとえば、AとBは4本、BとCは2本、CとDは3本、AとDは1本のワイヤーで結ばれているとする。

- ① AとBを結ぶ4本のワイヤーは、すべて異なった色にする必要がある
- ② その4本の色は、BとCを結ぶ2本、AとDを結ぶ1本のワイヤーの色と重なってはならない
- ③ CとDを結ぶ3本のワイヤーの色は、AとBを結ぶ4本のワイヤーの色と重なっても構わない
- ④ AとDを結ぶ1本のワイヤーの色は、BとCを結ぶ2本のワイヤーのどちらかと同じでも構わない

任意のポイントのリード線の本数が最大で  $m$  本とすると、ネットワーク全体で必要となるワイヤーの色の最小数を問うことが問題となる。これに対し、シャノンは厳密な証明を添えて、「 $1.5 \times m$ 、あるいは、それ未満の最大の整数が必要となる色の最小数である」との回答を提出した。上述の例では、 $1.5 \times 4 = 6$  本となる。このシャノンにとっては簡明な謎解きは、大きな経済的効果をもたらした。

シャノンの二番目の成果は、電話の呼び出しを繋ぐために使われる中継器の簡略化と効率化をテーマとするものであった。修士論文のときと同様に、回路設定に関する二つの新しい選択肢、すなわち、熟練者の直感的方法とブール代数に基づく方法とを考え出し、どちらの方法にも欠点があることを認めつつ、それらを組み合わせることにより、現状で提供されているものより優れた方式となるアルゴリズムを提案した。恩師のブッシュに宛てた手紙の中で、シャノンは「中継器にブール代数を応用するほくのアイデアを研究所が実際に設計に取り入れてくれたときは、最高の気分でした」と書いている [12]。

#### 2. 天才たちとの出会い

ベル研究所での夏を終えてプリンストン高等研究所に移った頃には、「クロード・シャノン」の名声は、既に数学や工学の世界で知れ渡っていた。シャノンはこの研究所で、通信の数学理論の確立に取り組み始める。この理論開発の萌芽期に、多くの天才から直接的に刺激を受けたことは、若き天才シャノンの創造力をさらに掻き立てたに違いない。

シャノンの憧れのスターであったジョン・フォン・ノイマン (John von Neumann) [44] について、「ほくはただの駆け出しにすぎないけれど、向こうは世界で

すみた うしお  
筑波大学名誉教授

〒305-8573 茨城県つくば市天王台 1-1-1

も飛びきり優秀な数学者の1人、過去に出会った誰よりも頭の切れる人物だ」と語っている。後に2人は人工知能の分野でパイオニア的存在になり、肩を並べるまでになる。ノイマンについては、この連載で項を改めて論じる予定である。

ナチス・ドイツの迫害を逃れてきた難民であるヘルマン・クラウス・フーゲー・ワイル (Hermann Klaus Hugo Weyl) [45] は、一般相対性理論と電磁気学を数学的に結び付け、量子力学と古典物理学の原理を融和させることに貢献した研究者であるが、プリンストン高等研究所ではシャノンのアドバイザーの役割を果たした。シャノンは、取り組み始めたばかりの通信の数学的理論と、量子力学における量子の奇異な振る舞いの類似性に気付いた。ワイヤーを通して送られる通信メッセージの数学的モデルと素粒子の運動モデルが、機械的決定論でもなく、正反対のランダムで無意味な動きでもなく、確率的プロセスに従っていることを見出したのである。こうしたテーマについて議論を交わすことを通して、2人は意気投合したと思われる。

そしてもちろん、アルベルト・アインシュタイン (Albert Einstein) とも触れ合う機会があったに違いない。物理学はシャノンの専門分野ではなく、アインシュタインから格別、注目されるようなことはなかったかも知れない。シャノンはどちらかと言えば人見知りであり、ほかの研究者とは異なり、世界で最も有名で人気のある科学者の取り巻きに割り込もうと努力した形跡は残されていない。しかし、ジャグリング仲間であった友人の口伝で、次のようなエピソードが伝えられている [12]。

「シャノンがプリンストン大学で講義を行っている最中、教室の扉が開いてアインシュタインが入ってきた。アインシュタインは数分間講義に耳を傾けてから、後ろの方に座っている学生に何やら囁き、教室を出て行った。講義が終了するや、シャノンは教室の奥へと急ぎ、アインシュタインが耳打ちしていた学生を見つけると、偉大な科学者が自分の講義について何を語ったのかを訪ねた。その答えは——『お茶とクッキーを楽しめる場所はどちらかね』であった。」

そのほかでは、午前中、車で研究所へ向かう途中、しばしば歩いているアインシュタインを追い抜いたエピソードを回想している。「大体は寝室用スリッパのようなものを履いて、古びた服を新調するわけでもなく、まるで日雇い労働者のようだった。ぼくが車で追い抜くときに手を振ると、手を振り返してくれた。きっと、ぼくのことなど知らなかったのだと思うけれど、変人だと思ったんだろうね。」

### 3. 戦争の影と結婚生活の破綻

1939年、ヒトラー率いるナチス・ドイツはポーランドに侵攻してこれを占領、1940年に入ると中立国デンマークとノルウェーに進出、これも占領した。さらにドイツ軍は、戦略的に重要なベルギー、オランダ、ルクセンブルクのベネルクス三国に侵攻、オランダは5月15日に降伏し、政府は王室ともどもロンドンに亡命した。またベルギー政府もイギリスに亡命し、5月28日にドイツと休戦条約を結ぶ。イギリスではウィンストン・チャーチルが首相に就任し、戦時挙国一致内閣が成立した。

欧州におけるドイツ軍の進撃は止まらず、フランスの対ドイツ巨大地下要塞・マジノ線を迂回し、侵攻不可能といわれていたアルデンス地方の深い森をあさり突破してフランス東部に侵入、電撃戦で瞬間にフランス・イギリスの連合軍をイギリス海峡に面するダンケルクへと追い詰めた。さらにドイツ軍は首都パリを目指し、敗色濃厚なフランス軍は散発的な抵抗しかできず、6月10日にはパリを戦火から守るべく無防備都市宣言を出した。同日、フランスが敗北濃厚になったのを見たイタリアのムッソリーニも、ドイツの勝利に相乗りせんとばかりにイギリスとフランスに対し宣戦布告した [46]。

シャノンの恩師であるブッシュは、第1次世界大戦の際、軍部と民間の科学者のあいだのコミュニケーションの断絶を直接的に体験していた。ナチスの横暴を目の当たりにし、遅かれ早かれアメリカの参戦は免れないと判断したブッシュは、1940年6月12日、ワシントンに乗り込み、NDRS (National Defense Research Committee: 国防研究委員会) の設立が急務であるとフランクリン・デラノ・ルーズベルト (Franklin Delano Roosevelt) 大統領 [47] に直談判した。これを受けて、大統領はその設立をその場で即決した。

全体主義の脅威に危機感を募らせたアメリカ政府は戦争準備を急ぎ、シャノンがプリンストンに到着してからわずか数日後の1940年9月16日、ルーズベルト大統領は Selective Training and Service Act (選抜訓練徴兵法) に署名した。21~36歳の男子を徴兵適齢者として登録させ、健康・家族・年齢などを考慮して順序をつけ、その順序で徴集、軍事訓練を施す内容である。署名に際し、大統領は次のような演説を行った。

「アメリカは、運命の岐路に立っている。時間も距離も残されてはいない。この数週間で、欧州の偉大な国々が陥落して来た。現在、暴れ回っている勢力の

信条に対し、これ以上、無関心でいることは許されない。わが国の海岸線に戦火が及ぶことを回避するため、大きな潜在能力を結集しなければならず、実際、私はそうする覚悟である。」

24歳のシャノンにとって、こうした言葉の意味するところは、徴兵され海外の戦場へ派兵される可能性が出てきたということである。彼が徴兵を忌避しようとした形跡は残されていないが、登録カードに署名したあと、自分の研究を中断し軍服に袖を通さなければならなくなる可能性に、内心、恐々としたに違いない。

この頃シャノンは、私生活においても苦しい状況にあった。妻のノーマは知的で活潑な女性であったが、ニューヨーク、パリ、ボストンと大都会で青春を過ごした後、家族や友人から切り離され、活気のない大学の町で20歳の若さで専業主婦としての生活を余儀なくされている状況に鬱屈していた。シャノンはノーマの左翼政治への情熱を共有することなく、結婚は始まりと同じように、突然、終わりを告げた。

最後の夫婦喧嘩の後、ノーマはプリンストンから列車に飛び乗ってマンハッタンに戻り、1941年に離婚が成立すると、今度こそは本来の生活を始めようと西を目指し、ハリウッドに腰を据えて脚本家となった。1942年には同じく脚本家のベン・バーズマン (Ben Barzman) と結婚、彼は後にジョン・ウェイン (John Wayne) 主演の「Back to Bataan (バターンを奪回せよ)」(1945年) やチャールトン・ヘストン (Charlton Heston) 主演の「El Cid (エル・シド)」(1961年) などの脚本を書いた人物である。ノーマ自身、今や古典となったロバート・ミッチャム (Robert Mitchum) 主演の「The Locket (危険な女)」(1946年) の脚本を書いている。2人は公然と共産主義に対する支持を表明し、戦後、1950年代に吹き荒れた反共産主義運動であるマッカーシー旋風に巻き込まれ、危険人物としてブラックリストに載せられたため、9年間、フランスへの逃亡を余儀なくされた。

#### 4. ベル研究所における戦時プロジェクトへの参加

プリンストン高等研究所で1年間の滞在を終え、また独りになったシャノンは、1941年、ベル研究所に数学研究者として迎えられた。そこでかつてアドバイザーであったフライを頼り、プッシュが設立したNDRCで解析処理を行う契約を確保することに成功、徴兵委員会から呼び出される不安から解放されることとなる。自分がひ弱な人間であることを自覚しており、戦場で

戦うよりもNDRCのメンバーとなって頭脳で戦争に貢献する方が、国家にとっても自分にとってもより良い結果が得られると確信していた。フライはNDRCの同僚のウォーレン・ウィーバー (Warren Weaver) [48] に連絡し、シャノンにふさわしいプロジェクトを見つけてくれるよう依頼した。

ウィーバーはシャノンと同じく、アメリカの片田舎にルーツをもち、手作業を好む科学者であった。工学、数学、機械学習、翻訳、生物学、自然科学、確率など幅広い領域で研究に取り組み、数多くの論文を発表していた。後に、人間の使う一言語から別の言語へ、コンピュータを用いて文書を自動翻訳する可能性を示唆し、機械翻訳の先駆者として知られるようになる。ルイス・キャロル (Lewis Carroll) の『不思議の国のアリス』をこよなく愛し、42ヶ国語、160の版を収集し、同作品の翻訳の歴史について『多言語で書かれたアリス：不思議の国のアリスの翻訳 (Alice in Many Tongues: The translations of Alice in Wonderland)』という本を出版している。シャノンが無神論者であることを公言していたのに比し、ウィーバーは信仰が篤く、「科学において新しい発見がなされるたびに、神が宇宙に組み込んだ秩序が明らかにされている」と信じて疑わなかった。

1948年、シャノンは情報と通信に関する記念碑的論文である「The Mathematical Theory of Communication (通信の数学的理論)」を発表し、翌年、書籍版が出版されるが、ウィーバーはこの本の中で長文の解説を執筆している。しかし、シャノンが情報理論から一切の意味論を削ぎ取ることを意図したにもかかわらず、ウィーバーの解説はシャノンの体系の意味論的考察に終始しており、恐らくシャノンは苦い思いをしたに違いない。敬虔なクリスチャンであったウィーバーは常に哲学的であり、この解説を通して、純粋に論理を貫くことを研究の方針としたシャノンとの違いが顕著になった。もちろん、振り返って見れば、シャノンが意味論を削ぎ落としたからこそ、その体系が今日のマルチメディアの基盤となる汎化性を宿すことができたことは確かである。

少し話が先走り過ぎたが、2人が出会ったときにはウィーバーはシャノンの能力を認めて親切に対応し、「射撃統制に対する数学的研究」というプロジェクトにシャノンを参加させることを決め、300ドルで10ヶ月の契約を結んだ。射撃統制とは、飛行機やロケットや弾道ミサイルなど、敵が空中に放つものを標的として、それを打ち落とす砲弾を制御するシステムを意味する。

連載第 15 回で、第 1 次世界大戦においてフォードが艦船からの砲撃制御用に開発したアナログコンピュータ Ford Mark 1A Computer について触れたが、標的の規模やスピードは格段の進歩を遂げており、戦争が始まって直ぐに、連合軍は防衛システムのグレードアップの必要性を思い知らされていたのである。

ドイツは、第 1 次世界大戦の敗北によってベルサイユ条約の受託を強いられた。この条約によって、海外植民地を失い、アルザス・ロレーヌをフランスに返還し、ヨーロッパにおける領土を削減された。また、第 1 次世界大戦の開始における戦争責任を断定されて、連合国の損害に対して賠償支払いを課せられ、軍備は厳しく制限された。しかし、ドイツ空軍はヒトラーとゲーリングのもとで見事に復活を遂げ、スペイン内戦におけるゲルニカ爆撃やロンドン大空襲で、その実力を余すところなく示した。さらに、戦争が長引くにつれて、世界で初めての巡航ミサイルや弾道ミサイルの開発に成功し、配備していった。

通信に関する研究と射撃統制システムの開発の間には、概念だけでなく機械構造的にも類似性が認められ、ベル研究所の数学者・技術者たちは目覚ましい成果を挙げた。特に、ベル研究所の若きエンジニアであったデイビッド・パーキンソン (David Parkinson) は、通信技術で用いる可変式抵抗器ポテンシオメーター (potentiometer) を高射砲の一部として作り変えることを着想し、シャノンを含む多くの研究者が参加する開発プロジェクトが組織された。数年を経て M-9 と命名された装置が 1,500 個以上製造され、戦場で大活躍する。高射砲に搭載された M-9 によって、敵機を打ち落とすのに要する砲弾の数は 1,000 発からわずか 10 発に減少した。後にシャノンは、

「バズ爆弾や V1 ロケット弾は、適度なスピードで完璧な直線を描いて飛んでくる。われわれの開発した高射装置で進路を正確に予測することが可能で、イギリスに到達する前に 95% を打ち落とすことができた。あれがなければ、イギリスは戦争に負けていたよ」と回想している。シャノンの功績は主として、間違っただけを取り除くデータ・スムージングを効率的に行う統計的方法の確立にあり、彼の書いたレポートはその分野における重要な成果として評価された。

第 2 次世界大戦中、トップクラスの数学者、科学者、技術者を数多く戦時プロジェクトに動員し、多大な成果を挙げた事実は、アメリカという若い国の凄まじいまでの底力を感じさせる。特定のタイプの標的に一定のダメージを与えるためには、爆弾から何トンの爆発

力を放出すべきか、爆撃機の編隊飛行の最良の形は何か、戦闘機から投下される対潜水艦爆弾は水深何メートルで爆破させれば良いか、などの質問に対する回答を技術者だけで取り組んだならば、多くの実験を繰り返すことに要する時間は膨大なものとなっていたに違いない。そこに数学者や科学者が加わることにより、開発スピードは劇的に削減されたのである。もちろん、アインシュタインの警告を受け、ドイツに先駆けて原子爆弾の開発に成功した例は、その最たるものである。

かくして世界トップクラスの頭脳が、自らの研究を棚上げにし、ロス・アラモス (Los Alamos) 国立研究所、ベル研究所、そしてタキシード・パーク (Tuxedo Park) においてアルフレッド・リー・ルूमス (Alfred Lee Loomis) が牽引した放射線科学研究所などに集結した。シャノンの師であるブッシュ、化学兵器の開発に携わったジェームス・ブライアント・コナント (James Bryant Conant) [49]、フォン・ノイマン、ロス・アラモス国立研究所の初代所長としてマンハッタン計画を主導した理論物理学者の J・ロバート・オッペンハイマー (J. Robert Oppenheimer) [50] らは、戦争をきっかけに政府の委員会に招かれ、脚光を浴びるようになった。大統領への助言を求められ、膨大な予算を駆使して人員や資材を取り仕切り、その功績は学界を超えて一般にも認められるようになった。シャノンも、望むならば政府関連の高い地位に登り詰めるだけの実績・経歴はもっていたが、そうはしなかった。自分の研究を中断して国に奉仕することに忠実ではあったが、胸には苦い思いを抱いていたに違いない。その後の生涯において、この時期の自分について語ることは、ほとんどなかった。

## 5. 暗号学と情報理論

シャノンの戦時プロジェクトへの参加は、やがて秘密通信システムの開発と暗号学へと重心を移して行く。このプロジェクトは、本意ながら取り組んだ研究ではあったものの、コンピュータ技術がどれほど素晴らしい成果を挙げられるものかを身近に体験させてくれた点で、戦後のシャノンの研究に大いに役立つこととなる。

暗号の歴史は古く、連載第 9 回でバベッジが確立したヴィジュネル暗号の解法について概説したが、暗号学はその後も進化を続け、指数的に複雑さを増していた。暗号化されたメッセージの送受信や敵の暗号メッセージの解読は軍事力を構成する重要な要素の一つとなり、ベル研究所は、アメリカにおけるこの戦いで中心的役



割を担った。その最も大きな成果の一つが、天才と呼ばれたホーマー・ダッドリー (Homer Dudley) [51] が牽引した、盗聴されても理解されない安全な音声通信システムの開発プロジェクト SIGSALY [52] である。

1896年、宣教師の父と古典や宗教を学生に教えていた母との間にバージニア州で生まれたダッドリーは、小学校に上がると家族でペンシルバニア州に引っ越し、高校の教師となることを期待されて育てられた。しかし自分には向いていないと察し、ペンシルバニア州立大学に進んで電気工学を学んだ。2, 3科目を履修した後、ベル研究所の前身である Western Electric Company の技術部門に就職、その後、40年の長きにわたってベル研究所に勤務し、音声合成に関する研究により、37もの特許を獲得した。

人間の音声は空気振動の連続に過ぎないとしたら、その振動を機械で再現できない理由はないと思いついたのが、ダッドリーの研究の始まりである。人間の声は、音源である声帯の音の特性や有声・無声の区別と、咽喉と口腔、鼻腔、舌、歯、唇などの調音機構の共鳴による周波数選択特性によってモデル化できる。音声波形はかなり速い振動成分を含むが、調音機構などの動きはそれと比べると比較的緩やかであり、それらを適切にパラメータ化することができれば、音声通信に必要な帯域を大幅に減らすことができるとダッドリーは考えた。当時の電信用大陸間横断ケーブルが伝送可能な周波数帯域はせいぜい100ヘルツ程度で、3,000~4,000ヘルツの帯域をもつ音声を送信することができなかった。音声をより狭い帯域で送信するという切実な課題に応えるべく取り組んだもので、この研究計画を1928年に発表した。

11年の歳月を経た1939年、ダッドリーはこの発想を元に、音声の周波数スペクトルを帯域フィルターによって複数チャンネルに分け、声帯の音の基本周期や有声・無声の区別とともに送信、これを受信側で再び音声として合成するチャンネルヴォコーダーを完成させた。また、音声を合成する部分と鍵盤とを組み合わせ、鍵盤演奏型のスピーチシンセサイザーであるヴォーダー (voder) を1939年のニューヨーク・ワールドフェアで一般公開した。

当時の技術水準ではチャンネルヴォコーダーは大掛かりな装置となってしまう、また音声の品質が悪く機械的な声になってしまうため、民間で使われることはなかったが、人間の音声からデータを創造する軍事研究プロジェクト SIGSALY に携わる技術者たちにとっては、チャンネルヴォコーダーは、基本要素としてプロジェ

クトの目的にピッタリ合致するものとして受け止められた。人間の会話から母音と子音を再現するのに必要な最小の帯域を絞り込み、それを暗号化して特殊なノイズを加えて送信するので、解読される恐れはほとんどなかった。1943年、チャーチル首相とルーズベルト大統領の秘密会談が SIGSALY を通して行われたのは有名な話である。SIGSALY プロジェクトには30名近いメンバーが参加しており、シャノンはメッセージが受信側で適切かつ安全に再生されるためのアルゴリズムを担当した [12]。秘密保持が徹底していたので、参加メンバーであるシャノンにも、複雑な計算の全体像について知らされることはなかった。

暗号学におけるシャノンのもう一つの大きな貢献は、ワнтаイム・パッド方式 [53] の安全性と強度に関し、数学的な根拠を与えたことである。メッセージと、それと同じ長さの記号から成る乱数鍵を用いて暗号化と復号化を行い、乱数鍵は1度使われたら破棄されるワнтаイム・パッド方式は、既に1882年には考案されていたが、SIGSALY プロジェクトの基礎概念としても採用されていた。ここでは、文献 [53] にある簡単な例を紹介する。たとえば、送信側、受信側で、以下の2点に関して同意しているものとしよう。

- 1) 乱数鍵を抽出する方式 (この例では1冊の本を用い、送受信の日付によってその本のページを決めそこから選ぶ方式: 同じページを選ばないように作られており、ページがなくなれば、また、別の本を用いる; もちろん、その都度、生成する方式でも良い)
- 2) 各文字に数値を割り当て、暗号化・復号化を行う方式 (この例では“A”は0, “B”は1, ..., “Z”は25のように割り当て、26のモジュール計算を用いるが、各文字を5桁の2進数で表わし、ビットごとに排他的論理和 (XOR) 演算を行うなどほかの方式でも良い)

平文が“HELLO”, 鍵が“XMCKL”であるとする、送受信のやり取りは図1のようになる。

1度用いた乱数鍵は破棄してしまうので、解読側が周期的な解析方法を適用できない点に特徴がある。

鍵が通信文の文字数と同じ文字数を必要とする点で、手作業で暗号化を行っている限りではワнтаイム・パッド方式は非効率である。しかし、SIGSALY ではフーリエ解析を活用して暗号化・復号化の手順を機械化しており、機密保持の安全性と強度には極めて高いものがあつた。実際、シャノンは、鍵が確率的に独立で同じ分布に従う手続きを繰り返すことで生成されるならば、

送信側		23(X)	12(M)	2(C)	10(K)	11(L)
	+(Module 26)	7(H)	4(E)	11(L)	11(L)	14(O)
		4(E)	16(Q)	13(N)	21(V)	25(Z)
受信側		4(E)	16(Q)	13(N)	21(V)	25(Z)
	-(Module 26)	23(X)	12(M)	2(C)	10(K)	11(L)
		7(H)	4(E)	11(L)	11(L)	14(O)

図1 ワンタイム・パッド方式の暗号化と復号化

ワンタイム・パッド方式は解読不可能であることを数学的に証明した。「A Mathematical Theory of Cryptography (暗号の数学理論)」というタイトルのこの論文は、日本が戦艦ミズリー艦上で降伏文書に署名する前日の1945年9月1日に発表されたが機密扱いとされ、4年後の1949年、タイトルを「Communication Theory of Secrecy Systems (暗号システムの通信理論)」と変えてBell System Technical Journalに掲載された。この論文の真の成果は、ワンタイム・パッド方式の解読不可能性の証明に留まらず、その洞察を、シャノンが後に確立することになる革命的な情報理論の核心に活かしている点にある。

余談であるが、太平洋戦争中に日本陸軍も無限式乱数と称してワンタイム・パッド方式を採用していた。日本の暗号学のパイオニアである陸軍軍人、釜賀一夫が開発と採用に指導性を発揮し、第一線部隊で全面採用された結果、「第一線部隊の暗号は弱い」との常識を覆した。戦後、GHQ尋問官は、この暗号を理論解読することができなかったことを彼に示唆したと伝えられている[54]。釜賀は戦後も陸上自衛隊で暗号解読に従事し、2003年、86歳で亡くなった。

## 6. チューリングとの出会い

1939年、27歳になっていたチューリングは、イギリスの対独開戦日に、ヴィクトリア朝の邸宅ブレッチリー・パークに居を移し、ドイツ軍のタイプライター型暗号機エニグマ(Enigma)を解読する戦いの最前線に立った[15]。巧みな解読ソフトウェアを開発した後、機械には機械で対抗すべく、エニグマ対策の解読機ボンブ(Bombe)を設計、1940年の春に本格的に稼働し始め、1943年には、毎月、48,000という驚異的な数の通信文の解読に成功していた。さらに、ドイツ軍がエニグマを洗練させて新たに開発し、それをイギリス軍がタニー(Tunny)と呼んだ暗号機の解読にも、即座に取り組み始めた。これらについては、チューリングの項で改めて紹介する予定である。

1942年11月、チューリングはアメリカの暗号学者と連絡を取るために船で旅立った。その月には、ドイ

ツの潜水艦Uボートが大西洋で連合軍の船を百隻以上も沈めており、最も危険な時期に海を渡ったことになる。まるで浮かぶ兵舎のごとく軍人を満載した船の中で、彼はたった1人の民間人であった。将校専用の居間には600人以上が詰め込まれ、チューリングは気絶しそうになったと述懐している。旅の主要な目的は、マンハッタン島にあるベル研究所を訪れることであったが、当初、アメリカはこれを歓迎せず、チューリングのベル研究所への立ち入りを禁止した。1月になって、アメリカ陸軍参謀総長とチャーチルの個人的な代理人が長い手紙を交わすことで、ベル研究所はようやくその重い扉を開き、チューリングはその後2ヶ月間、滞在することを許された。

当時、イギリスとアメリカの同盟関係は、全面的な信頼関係に基づいているとは言い難い状況にあった。たとえば、チューリングの尽力でドイツ軍の暗号解読に成功していたイギリスは、その一部をアメリカに伏せたままにした。一方、アメリカは、軍需品の製造を強化すると口にしなが、アメリカの規模とスピードにペースを合わせられないイギリスに不満を抱いていた。チューリングのような地位と名誉をもった人間でさえ、イギリスとアメリカがどこまで積極的に協力関係を進めるのかについて判断することはできなかったのである。こうした微妙な両国関係を背景に、チューリングとシャノンは、みすほらしいベル研究所のカフェテリアで、毎日、お茶を飲みながら話し合ったという。後に、シャノンは、次のように述懐している[12]。

「チューリングは偉大な人物、凄い人物だと思う。ぼくたちは、暗号技術については、一言も言葉を交わさなかった。でも興味を持つ問題が驚くほど共通していたから、そんな問題について話し合った。当時、既に彼はチューリング・マシンに関する論文を執筆していた。そういう呼び名は、未だ定着していなかったけれどね。他に、人間の脳の中身はどうなっているかについて、ずいぶん議論した。脳はどんな構造をしていて、どのように機能するのか、機械に何ができるのかも考えたな。人間の脳にできることは機械にもできるんじゃないかとかね。それから、ぼくの情報理論の概念についても何度か話をした。興味を持ってくれたよ。」

シャノンは内向的な人物で、科学界での名声と地位のわりには親密な友人は少なく、会議に招待されても出席するのは希だった。このような人物像を考えると、その後も熱心にチューリングとコンタクトを取り続けた事実そのものに、2人で交わした会話の内容の深さ

を窺い知ることができる。

第2次世界戦後、2人はもう一度だけ会っている。1950年、シャノンが会議のためにロンドンを訪れた際、時間を割いてマンチェスター大学の研究所にチューリングを訪問した。当時は、コンピュータの揺籃期であったが、チューリングはチェスをするプログラムの開発に夢中で、それはシャノンの興味でもあった。情報時代の基礎を築いた2人の巨人は、再会を心から楽しんだ。しかし、これが2人にとって直接話し合う最後の機会となった。同性愛が違法とされる時代に、チューリングは「わいせつ行為」で有罪判決を受け、シャノンとの再会から4年後の1954年、青酸中毒による若すぎる死を迎えた。警察は自殺と断定したが、詳しい状況は未だに謎のままである。2009年9月、イギリス政府はチューリングに対して正式に謝罪し、その名誉を回復している。

## 7. 先行研究：「インテリジェンス (Intelligence)」から「情報 (Information)」へ

シャノンが勤め始めた頃、ベル研究所では人間のオペレーターが外部との電話を取り次いだ。やがてベル研究所は自動交換台を開発し、機械が自動的に電話を取り次ぐようになる。この自動交換台は、当時、「人工頭脳」という大仰な名前と呼ばれた。産業革命時代の科学者たちがさまざまな蒸気機関を組み立てるプロセスを通して「熱」に対する理解を深めていったように、シャノンの世代の科学者たちは、自動交換機に代表される人間労働を代替する機械を組み立て洗練させるプロセスを通して、「情報」を理解するようになった [12]。そのような時代の流れの中で、シャノンは「情報」という概念を定義し、さまざまな内容をそこに統合することにより、最終的に「情報理論」という新しい科学を創造した。しかし、どのように偉大な知的創造であっても、そこには必ず先行研究がある。ベル研究所には、シャノンに先駆けてこのテーマに取り組み、シャノンの思考形成に大きな影響を与えた2人の重要な研究者がいた。ハリー・ナイキスト (Harry Nyquist) [55] とラルフ・ハートレー (Ralph Vinton Lyon Hartley) [56] である。

ナイキストは1989年、スウェーデンの片田舎の農場に生まれた。14歳のときから4年間、工事現場で働いて船賃を稼ぎ、1907年、18歳のときに、家族共々、スカンジナビア移民の波に加わり、アメリカにやってきた。1912年にノースダコタ大学に入学、電気工学を専門に選び、1914年に学士、翌年の1915年には修

士号を得た。その後、イエール大学に進み、1917年に物理学で博士号を取得、Western Electric Companyの研究部門であったベル・システム社に科学者として採用された。着任早々、登場したばかりのファクスの試作品開発の責任者に抜擢され、1918年に「電送写真」の企画を提出、1924年には実用モデルを完成させた。この機械は、写真をスキャンすると画像の基本単位面積ごとに濃淡を確定し、その情報を電流に変換して電話線を通して送信、受信された電流は写真のネガに変換され、暗室へ送り込まれるという仕組みであった。この機械は鮮烈な印象を与えたが、市場はほとんど興味を示さなかった。小さな写真を一枚伝送するのに、7分も掛かることが障害となったのである。

ナイキストは市場の期待外れの反応に臆することなく、1920年当時、既に旧世代技術と見なされていた電信技術に関しても、新たな取り組みを始めた。通信ネットワークでは、利用可能な周波数の幅があり、この帯域幅が広く確保されるほど、充実した内容を伝えることができる。ドット、ダッシュ、0と1の列を送信するだけの電信ネットワークは狭い帯域幅で済むが、電話の会話を効果的に伝えるためには200ヘルツから3,200ヘルツの帯域幅が必要であり、テレビの送信網は電話網の2,000倍の帯域幅が必要となる。ナイキストが示したのは、どんな通信回線であっても、その帯域幅が与えられたとき、それに対応して、所定の速度で送られる「インテリジェンス」の量には上限が存在するという事実であった。

この事実を、ナイキストは以下の数式で表現した。

$$W = k \times \log(m) \quad (7.1)$$

ここで、 $m$  は単位時間内に送信できる文字数を表わす。振幅と周波数の組み合わせを考え、単位時間内に観測される電波の振幅がある閾値以上であれば1、それ以下であれば0とすれば  $m = 2$  である。同様に、単位時間内に観測される電波の周波数がある閾値以上であれば1、以下であれば0としても  $m = 2$  である。両方を同時に観測し、H (High) と L (Low) を用いて、 $LL = 00$ ,  $LH = 01$ ,  $HL = 10$ ,  $HH = 11$  と定めれば  $m = 4$  となる。本連載で後に登場するモデム (modem) とは、まさにこの考え方にに基づき、電話回線を用いてデジタル信号を送信する仕組みである。対数を取っているのは、光度の強さや重さを感じる人間の感覚になぞらえ、文字数が2乗倍になれば、内容が2倍豊富になったと感じる人間感覚を表わしている。 $k$  は1秒間に送信できる単位時間の数で、通信回線がもつ帯域幅によって



定まる。

式 (7.1) を  $W$  の定義式と読むと、 $W$  は 1 秒当たり受信する内容の豊富さを表わし、ナイキストはこれを「インテリジェンス」と名付けた。言葉の表現としては曖昧さを残すが、人間が感じる受信内容の豊富さを定量的に把握する試みとしては、世界で初めてのものである。1924 年、ナイキストはこの考えをわずか四つのパラグラフから成る短い論文で Bell System Technical Journal に発表した。シャノンがその革命的な論文の中で引用するまで、注目を浴びることはなかった。

ナイキストのモデルは、文字数を文章や図形に対応させれば、一般的な情報を取り扱うまでに汎化できる内容を孕んでいた。しかし彼は、効率的なシステムを設計することに興味を抱く傾向が強く、「インテリジェンス」の性質について熟考することはなかった。同僚に対し、「すべての通信システムは本質的にデジタルであり、そのネットワーク設計に際しては、 $m$  と  $k$  を大きくする努力をするべきだ」という貴重な提言を残してほかの研究に移ってしまった。

1928 年、ナイキストは「すべての通信システムは本質的にデジタルである」という自らの信念に基づき、「アナログ信号をデジタルサンプリングして再現するには、アナログ信号の周波数の 2 倍が必要である」という予測を発表した。これをシャノンが 1949 年の論文で証明し、現在ではナイキスト-シャノンの標準化定理と呼ばれている。ほかには、熱雑音、フィードバック増幅器の安定性などをテーマとする研究に携わり、晩年はテキサス州で隠居し、1976 年、87 歳の生涯を終えた。

情報に対して「インテリジェンス (Intelligence)」という表現は不適切であることを見抜き、「情報 (Information)」という言葉を考案したのがハートレーである。1888 年、ネバダ州のスプルースモント (Sprucemont) に生まれ、1909 年、ユタ大学を卒業後、ローズ奨学生として海を渡り、イギリスのオックスフォード大学に留学した。1912 年に学士、1913 年に科学学士を得て卒業後、アメリカに戻ったハートレーは、ベル・システム社に就職した。着任早々に、電線ではなく電波で大西洋の両側を結ぶ最初の音声通話の受信機の設計を任された。テストの準備が整った 1915 年、ベル社の技術者たちはフランス政府に対し、欧州大陸で一番高いアンテナ、すなわち、エッフェル塔のてっぺんにある無線アンテナの使用許可を申請した。しかし、当時、欧州は第 1 次世界大戦の真っ最中であり、それは重要な軍事資産として活用されていたので、使用許可が下

りたのはわずか数分間だけであった。それでも、ハートレーの受信機は成功を収め、バージニアから送られた音声は、世界で初めて大西洋を横断し、エッフェル塔のてっぺんまで届いた [12]。

通信ネットワークに対するハートレーの興味は極めて包括的なものであり、いかなる媒体の情報伝達力も包含できる単一の枠組を最初から追い求めた。すなわち、電信や電話や無線やテレビを、同じ土俵で比較分析できる体系の確立を志したのである。1927 年、イタリアのコモ湖で開催された科学会議で発表した論文は、ナイキストの論文の抽象化をさらに高いレベルまで押し上げる内容をもち、それにふさわしく「Transmission of Information (情報の伝達)」というタイトルが付けられた [12]。この論文で、ハートレーは、「伝達し得る情報量は、通信線の帯域幅と通信時間に比例する」という法則を証明した。

アルプスの麓で開かれたこの会議には、錚々たる顔ぶれが参加していた。量子物理学の創始者であるニールス・ヘンリック・ダヴィド・ボーア (Niels Henrik David Bohr) とヴェルナー・カール・ハイゼンベルク (Werner Karl Heisenberg)、世界で初めて原子炉を完成させ原子力時代の幕開けを実現することになるエンリコ・フェルミ (Enrico Fermi) など、世界的名声をもつ研究者が見守る中での発表は、若きハートレーにとって、酷く緊張を強いるものであったに違いない。ハートレーは講演の中で、マイナス、オフ、プラスの三つの電流値を持つ電信システムで、素人が無作為に選んだ電鍵を接続するという思考実験を提示した。それは、傾斜のある板の下にポケットを用意し、三色のボールのうち、どれかを板の上から無作為に次々と転がし、ポケットにボールが蓄積されて行くという実験と同等である。ここでハートレーは聴衆に、このようにして送信されたメッセージには意味があるだろうか、と問いかけた。その答えは、「意味がある」という言葉の解釈次第だとハートレーは答える。電線が頑丈でひずみがなければ、明快な符号が次々と受信されるという意味で、この実験内容は物理的な意味をもつ。しかし、人間が理解できるか否かという観点からは、「符号列があらかじめ定められた規則に従う場合にのみ、それは意味をもつ」という結論になる。

たとえば、この思考実験をモールス信号 (連載第 2 回) になぞらえると、モールス信号が符号列として送信され、受信された符号列をモールス信号の取り決めに従って言葉に変換したとき、その結果が文法的に解釈可能な場合にのみ内容が了解されることになる。モールス



信号の場合、了解可能性を定める規則は明快であるが、解釈に統一感のない符号は多い。電話による音声伝達でも、それが聞き手にいかに了解されるかは、用いられる言語、個性、気分、体調、1日の時間帯など、さまざまな要素に影響される。ましてや、絵画や音楽に至っては、意味了解のための統一的規格を定めることさえ極めて困難である。ハートレーが拓いた新境地は、「物理的なシステムが情報を伝える能力を評価するためには、解釈に関連する意味論を無視すべきで、受信者が解釈の判断の基礎とする符号列の1秒間当たりの量と正確性のみを問題とすべきだ」という点にある。

ハートレーは、ナイキストがインテリジェンスを計量化するために用いた式 (7.1) を次のように一般化した。1秒ごとに送信できる符号の数を  $k$ 、メッセージを構成するのに使用される符号の数を  $s$ 、メッセージの長さを  $n$  としたとき、その通信システムの持つ1秒当たりの情報量  $H$  を次式で定義した。

$$H = k \times \log(s^n) = k \times n \times \log(s) \quad (7.2)$$

たとえば、アルファベット 26 文字 ( $s = 26$ ) から、二つの文字を並べて作られるメッセージの集合を考えると、そのサイズは  $26^2 = 676$ 、文字が三つになるとサイズは  $26^3 = 17,576$  となる。この指数的膨張を線型の水準に押さえているのが対数関数で、それは「20 文字の長さの電報は 10 文字の長さの場合の 2 倍の情報量をもっている」との人間の感覚と合致する。

連続信号であろうと離散信号であろうと適用し得るハートレーの定式化は、ナイキストのモデルを特殊な場合として含むものであり、彼の「すべての通信システムは本質的にデジタルである」という直感をより具体的に裏付けるものとなった。シャノンは、ハートレーの研究から重要な影響を受けたことを認めている。1939 年に書いた手紙で初めて通信の研究に言及したが、そこではナイキストの「インテリジェンス (Intelligence)」という言葉を使っていた。しかし、1940 年代後半、研究が完成する頃にはハートレーの「情報 (Information)」という言葉を使うようになっていた [12]。

ハートレーはさらに通信ノイズの研究に進み、通信路上で、確実に区別して転送可能な信号振幅のレベルの最大の数は、信号の振幅の変動幅と受信側がその振幅レベルを識別できる精度によって制限されるという法則を見出した。具体的には、転送される信号の振幅が  $[-A, A]$  に制限され、受信側の受信精度が  $\pm \Delta V$  ボルトであるとき、識別可能な最大のパルスレベル数  $M$  が次式で与えられることを示した。

$$M = 1 + \frac{A}{\Delta V} \quad (7.3)$$

この式は、ハートレーの法則と呼ばれ、シャノンの伝送化理論の重要な先駆けとなった。すなわち、シャノンはハートレーの研究成果を用いて、「有限の帯域幅を持ち、その強度が正規分布に従うノイズに晒される通信路の連続時間の通信容量」を明らかにした。具体的には、通信路の帯域幅を  $B$  (ヘルツ)、帯域幅上の信号の総電力を  $S$  (ワット)、帯域幅上の正規分布に従うノイズの総電力を  $N$  (ワット) とすると、その通信線の通信容量  $C$  (ビット/秒) は、次式で与えられることを証明した。

$$C = B \times \log_2 \left( 1 + \frac{S}{N} \right) \quad (7.4)$$

この結果は、シャノン・ハートレーの定理と名付けられている。ハートレーは 1950 年にベル研究所を退職し、1970 年、81 歳の生涯を閉じた。

シャノンの革命的な知的創造に大きな影響を与えた先行研究が存在したこと、また、ナイキストが、旧世代技術と目されていた電信システムの研究に立ち返り、そこから「すべての通信システムは本質的にデジタルであり、そのネットワーク設計に際しては、 $m$  と  $k$  を大きくする努力をするべきだ」という時代を超える洞察を導き出したことは、多くの示唆を含む。これを技術革新の法則 (17) として纏めておく。

#### 技術革新の法則 (17) 知的創造の継承性:

- ① どのような偉大な知的創造にも、時代の流れを形成した先行研究が必ず存在する
- ② どのような旧世代技術にも、時代を超える新技術を生み出す可能性が潜んでいる

(この項、なお続く)

#### 参考文献

- [1] H. Goldstine, *The Computer from Pascal to von Neumann*, Princeton University Press, 1972. (末包良太, 米口肇, 犬伏茂之訳, 『復刊 計算機の歴史—パスカからノイマンまで—』, 共立出版, 2016.)
- [2] S. McCartney, *The Triumphs and Tragedies of the World's First Computer*, Walker, 1999. (日暮雅通訳, 『エニアック—世界最初のコンピュータ開発秘話—』, パーソナルメディア, 2001.)
- [3] 坂村健, 『痛快! コンピュータ学』, 集英社, 1999 (文庫版 2002).
- [4] 竹内伸, 『実物でたどるコンピュータの歴史—石ころからリンゴへ—』, 東京理科大学出版センター(編), 東京書籍, 2012.
- [5] 小田徹, 『コンピュータ開発のはてしない物語—起源から驚きの近未来まで—』, 技術評論社, 2016.

- [6] Wikipedia, Francois Viète, [https://en.wikipedia.org/wiki/Francois\\_Viète](https://en.wikipedia.org/wiki/Francois_Viète) (2021年12月14日閲覧)
- [7] E. T. Bell, *Men of Mathematics Volume 1*, Simon & Schuster, 1937. (田中勇・銀林浩訳, 『数学をつくった人びと上』, 東京図書, 1976.)
- [8] Wikipedia, René Descartes, [https://en.wikipedia.org/wiki/René\\_Descartes](https://en.wikipedia.org/wiki/René_Descartes) (2021年12月21日閲覧)
- [9] E. T. Bell, *Men of Mathematics Volume 2*, Simon & Schuster, 1937. (田中勇・銀林浩訳, 『数学をつくった人びと下』, 東京図書, 1976.)
- [10] Wikipedia, George Boole, [https://en.wikipedia.org/wiki/George\\_Boole](https://en.wikipedia.org/wiki/George_Boole) (2021年12月14日閲覧)
- [11] P. J. Nahin, *The Logician and the Engineer: How George Boole and Claude Shannon Created the Information Age*, Princeton University Press, 2012. (松浦俊輔訳, 『0と1の話—ブール代数とシャノン理論—』, 青土社, 2013.)
- [12] J. Soni and R. Goodman, *A Mind at Play: How Claude Shannon Invented the Information Age*, Simon & Schuster, 2017. (小坂恵理訳, 『クロード・シャノン—情報時代を発明した男—』, 筑摩書房, 2019.)
- [13] Wikipedia, Claude Shannon, [https://en.wikipedia.org/wiki/Claude\\_Shannon](https://en.wikipedia.org/wiki/Claude_Shannon) (2021年12月20日閲覧)
- [14] Wikipedia, Alan Turing, [https://en.wikipedia.org/wiki/Alan\\_Turing](https://en.wikipedia.org/wiki/Alan_Turing) (2021年12月20日閲覧)
- [15] B. J. Copeland, *Turing: Pioneer of the Information Age*, Oxford University Press, 2012. (服部桂訳, 『チューリング—情報時代のパイオニア—』, NTT出版, 2013.)
- [16] A. Hodges, *Alan Turing: The Enigma*, Princeton University Press, 2014. (土屋俊・土屋希和子訳, 『エニグマ—アラン・チューリング伝—』, 勁草書房, 2015.)
- [17] 高岡詠子, 『チューリングの計算理論入門—チューリングマシンからコンピュータへ—』, 講談社, 2014.
- [18] Wikipedia, Galileo Galilei, [https://en.wikipedia.org/wiki/Galileo\\_Galilei](https://en.wikipedia.org/wiki/Galileo_Galilei) (2021年12月21日閲覧)
- [19] Wikipedia, Nicolaus Copernicus, [https://en.wikipedia.org/wiki/Nicolaus\\_Copernicus](https://en.wikipedia.org/wiki/Nicolaus_Copernicus) (2021年12月21日閲覧)
- [20] Wikipedia, Marin Mersenne, [https://en.wikipedia.org/wiki/Marin\\_Mersenne](https://en.wikipedia.org/wiki/Marin_Mersenne) (2021年12月21日閲覧)
- [21] Wikipedia, Isaac Beeckman, [https://en.wikipedia.org/wiki/Isaac\\_Beeckman](https://en.wikipedia.org/wiki/Isaac_Beeckman) (2022年1月2日閲覧)
- [22] Wikipedia, Adrien Baillet, [https://en.wikipedia.org/wiki/Adrien\\_Baillet](https://en.wikipedia.org/wiki/Adrien_Baillet) (2022年1月2日閲覧)
- [23] Wikipedia, Elisabeth of the Palatinate, [https://en.wikipedia.org/wiki/Elisabeth\\_of\\_the\\_Palatinate](https://en.wikipedia.org/wiki/Elisabeth_of_the_Palatinate) (2022年1月2日閲覧)
- [24] Wikipedia, エリーザベト・フォン・デア・ブファルト (1618-1680), <https://ja.wikipedia.org/wiki/エリーザベト・フォン・デア・ブファルト> (1618-1680) (2022年1月2日閲覧)
- [25] 有賀暢迪, “合理力学の一例としての衝突理論 1720–1730年”, 科学哲学科学史研究, **6**, pp. 17–37, 2012.
- [26] Wikipedia, ソデイの6球連鎖, <https://ja.wikipedia.org/wiki/ソデイの6球連鎖> (2022年1月4日閲覧)
- [27] Wikipedia, Thorold Gosset, [https://en.wikipedia.org/wiki/Thorold\\_Gosset](https://en.wikipedia.org/wiki/Thorold_Gosset) (2022年1月4日閲覧)
- [28] 寒川町ガイド, <https://samukawaguide.blogspot.com/2019/12/6.html> (2022年1月4日閲覧)
- [29] Wikipedia, Gottfried Wilhelm Leibniz, [https://en.wikipedia.org/wiki/Gottfried\\_Wilhelm\\_Leibniz](https://en.wikipedia.org/wiki/Gottfried_Wilhelm_Leibniz) (2022年1月4日閲覧)
- [30] Wikipedia, Christina, Queen of Sweden, [https://en.wikipedia.org/wiki/Christina,\\_Queen\\_of\\_Sweden](https://en.wikipedia.org/wiki/Christina,_Queen_of_Sweden) (2022年1月4日閲覧)
- [31] Wikipedia, Isaac Newton, [https://en.wikipedia.org/wiki/Isaac\\_Newton](https://en.wikipedia.org/wiki/Isaac_Newton) (2022年1月4日閲覧)
- [32] 向井茂, “不変式の話.” 数学セミナー連載, 2005年12月号, 2006年1, 2, 4月号.
- [33] 日本医学会ホームページ, <https://jams.med.or.jp/news/013.html> (2022年2月4日閲覧)
- [34] Wikipedia, Vannevar Bush, [https://en.wikipedia.org/wiki/Vannevar\\_Bush](https://en.wikipedia.org/wiki/Vannevar_Bush) (2022年2月25日閲覧)
- [35] Britanica, William-Thomson-Baron-Kelvin, <https://www.britannica.com/biography/William-Thomson-Baron-Kelvin> (2022年3月6日閲覧)
- [36] Wikipedia, Hannibal Ford, [https://en.wikipedia.org/wiki/Hannibal\\_Ford](https://en.wikipedia.org/wiki/Hannibal_Ford) (2022年3月6日閲覧)
- [37] Wikipedia, Joseph Fourier, [https://en.wikipedia.org/wiki/Joseph\\_Fourier](https://en.wikipedia.org/wiki/Joseph_Fourier) (2022年3月6日閲覧)
- [38] Wikipedia, ユトランド沖海戦, <https://ja.wikipedia.org/wiki/ユトランド沖海戦> (2022年3月6日閲覧)
- [39] Wikipedia, Mark I Fire Control Computer, [https://en.wikipedia.org/wiki/Mark\\_I\\_Fire\\_Control\\_Computer](https://en.wikipedia.org/wiki/Mark_I_Fire_Control_Computer) (2022年3月7日閲覧)
- [40] Wikipedia, Bell Labs, [https://en.wikipedia.org/wiki/Bell\\_Labs](https://en.wikipedia.org/wiki/Bell_Labs) (2022年4月7日閲覧)
- [41] Wikipedia, Thornton Carle Fry, [https://en.wikipedia.org/wiki/Thornton\\_Carle\\_Fry](https://en.wikipedia.org/wiki/Thornton_Carle_Fry) (2022年4月7日閲覧)
- [42] Wikipedia, Schön scandal, [https://en.wikipedia.org/wiki/Schön\\_scandal](https://en.wikipedia.org/wiki/Schön_scandal) (2022年4月7日閲覧)
- [43] Wikipedia, ヘンドリック・シェーン, <https://ja.wikipedia.org/wiki/ヘンドリック・シェーン> (2022年4月7日閲覧)
- [44] Wikipedia, ジョン・フォン・ノイマン, <https://ja.wikipedia.org/wiki/ジョン・フォン・ノイマン> (2022年4月29日閲覧)
- [45] Wikipedia, ヘルマン・ワイル, <https://ja.wikipedia.org/wiki/ヘルマン・ワイル> (2022年4月29日閲覧)
- [46] Wikipedia, 第二次世界大戦, <https://ja.wikipedia.org/wiki/第二次世界大戦> (2022年5月31日閲覧)
- [47] Wikipedia, フランクリン・ルーズベルト, <https://ja.wikipedia.org/wiki/フランクリン・ルーズベルト> (2022年4月30日閲覧)
- [48] Wikipedia, ウォーレン・ウィーバー, <https://ja.wikipedia.org/wiki/ウォーレン・ウィーバー> (2022年5月3日閲覧)
- [49] Wikipedia, ジェイムス・コナント, <https://ja.wikipedia.org/wiki/ジェイムス・コナント> (2022年5月3日閲覧)
- [50] Wikipedia, ロバート・オッペンハイマー, <https://ja.wikipedia.org/wiki/ロバート・オッペンハイマー> (2022年5月3日閲覧)
- [51] Wikipedia, Homer Dudley, [https://en.wikipedia.org/wiki/Homer\\_Dudley](https://en.wikipedia.org/wiki/Homer_Dudley) (2022年4月7日閲覧)
- [52] Wikipedia, SIGSALY, <https://ja.wikipedia.org/wiki/SIGSALY> (2022年5月31日閲覧)
- [53] Wikipedia, ワンタイムパッド, <https://ja.wikipedia.org/wiki/ワンタイムパッド> (2022年5月3日閲覧)
- [54] 釜賀一夫, 藤原邦樹, 吉村昭, “座談会 日本陸軍暗号はなぜ破られなかったか,” 歴史と人物—太平洋戦争シリーズ—, 昭和60年冬号, 1985.
- [55] Wikipedia, Harry Nyquist, [https://en.wikipedia.org/wiki/Harry\\_Nyquist](https://en.wikipedia.org/wiki/Harry_Nyquist) (2022年5月7日閲覧)
- [56] Wikipedia, Ralph Hartley, [https://en.wikipedia.org/wiki/Ralph\\_Hartley](https://en.wikipedia.org/wiki/Ralph_Hartley) (2022年5月7日閲覧)