巻頭言

Alan TuringとBletchley Park

理化学研究所計算科学研究機構副機構長
宇川　　彰

ブレッチリー（Bletchley）は、ロンドンのユーストン駅から近郊線（Midland Express）に乗って１時間、距離にして70km程北北西に行ったところにある小さな町である。ブレッチリーパーク（Bletchley Park）（図１）は、駅を出て右手の方に5分程歩いたところにある。

ブレッチリーパークは、第二次世界大戦中に、ナチスドイツの軍事暗号エニグマを解読する拠点だったところである。最盛期には12,000人が働いていたという。その活動は、戦後長らく軍事機密として公開されず、ブレッチリーパークも荒れるに任されてきた。最近漸くイギリスの歴史的な遺産として整備が行われ2013年から一般に公開されている。私は2015年１月にこの地を訪れる機会があった。

アラン・チューリング（Alan Turing）は、1939年から1945年までブレッチリーパークでエニグマ暗号の解読に従事した。1912年生まれなので、入所時には27歳、ケンブリッジ大学の数学研究員であった。1935年の論文「計算可能な数と決定問題への応用」でドイツの大数学者ダビッド・ヒルベルト（David Hilbert）の提出した決定問題に決着をつけると同時に計算機械の論理的基礎づけを行った俊秀だったが、世間的には全くの無名だったと思われる。

エニグマ暗号機は26の電気入力・出力を持つ歯車（ロータ）を複数個連結することによりアルファベットの置換を実現する電気装置である。３個のロータを持つエニグマは約1.5×10^{19}通りの連結が可能で、その初期設定は毎日変更された。ドイツ軍はこれだけの複雑さを持つエニグマ暗号は解読できないと信じていた。

チューリングは、エニグマ暗号機の初期設定を探り出す装置ボム（Bombe）を開発してエニグマ暗号の解読を可能にした。第二次大戦を通じて200台を超えるボムが製作され、その解読によって連合軍はドイツ軍の多くの作

図１　ブレッチリーパーク。左手に司令部の置かれていたマンションが見える。中央から右手奥が、暗号解読がおこなわれていたhutと呼ばれた建物群である。

戦を察知して戦いを有利に導くことができたと言われている。

ボムはエニグマ暗号機の初期設定を探り出す電気的機械であり、電子計算機ではない。最初の電子計算機は、アメリカ合衆国で弾道計算を目的に製作されたENIAC（1946年完成）と言われることが多い。しかし、それを遡る3年前の1943年に、ブレッチリーパークではコロッサス（Colossus）という電子計算機が製作され暗号解読に使われていた。

ドイツ軍はエニグマ暗号と並んでロレンツ暗号と呼ばれる暗号を用いていた。ロレンツ暗号は原文にビット列を結合することにより暗号化する方式で、ビット列の生成に複数個の歯車が使われた。コロッサスは、ロレンツ暗号機を電子的にエミュレートして暗号文を生成し、それを元の暗号文と比較することにより、ロレンツ暗号機の歯車の設定を探り出すことができた。

コロッサスは、技術者のトミー・フラワーズ（Tommy Flowers）と数学者マックス・ニューマン（Max Newman）により開発された。真空管1500本を使い、背面にあるプラグボードの配線変更によりブール演算のプログラムが可能で、汎用ではないものの、電子計算機と呼べる機械である。

以上の背景を知ると、戦後の電子計算機の開発はイギリスを中心に進んでもよかったと思える。しかし歴史はそうはならなかった。

アメリカ合衆国では、ENIACに続いて、プログラム内蔵方式の電子計算機EDVACの開発が進められた。その過程で数学者フォン・ノイマンによってEDVACレポートとして1945年にまとめられた論理的基礎づけや、1946年にペンシルベニア大学ムーア・スクールで行われた一連の講義によって、この間の知識と経験が幅広く研究者の共有するところとなった。政府による強力な後押しや、IBMなど多くの企業の参入もあって、アメリカにおけるその後の電子計算機の圧倒的な発展に繋がった。

一方、英国では、ブレッチリーパークの成果は軍事機密として戦後長く非公開とされ、ボムやコロッサスのハードウェアや資料の大部分も廃棄されてしまった。チューリングは自らのチューリング・マシンの理論を基礎に、アメリカの動きとは独立にプログラム内蔵方式の電子計算機を設計し、1945年にACEレポートとしてまとめた。しかし、その製作は遅々として進まず、漸く完成したのは1957年だった。それに先立つこと3年、1954年にすでにチューリングは世を去っていた。

世界最初のプログラム内蔵方式の電子計算機は、ケンブリッジ大学のモーリス・ウィルクス（Maurice Wilkes）が製作したEDSAC（1949年完成）である。皮肉なことに、この計算機はアメリカ合州国のEDVACの流れを学んだもので、チューリングやニューマンの系譜につながるものではなかった。

ブレッチリーパークには再現されたボムが置かれている（図2）。隣にある国立計算博物館には、コロッサスも再現され、その姿を見ることができる（図3）。

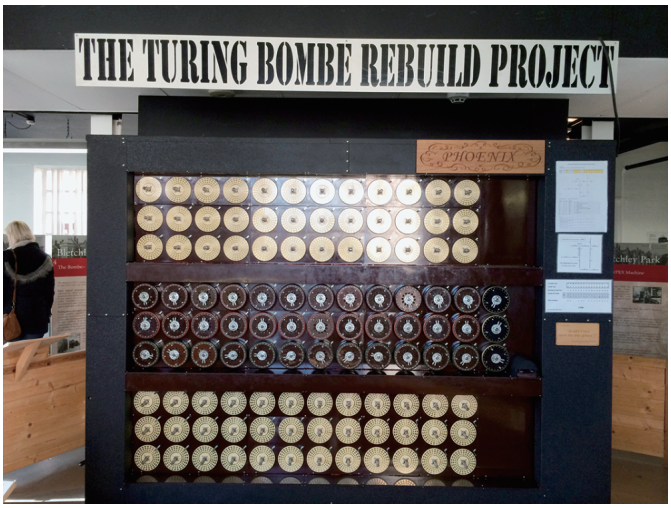

図２　再現されたボム。円板状の部品が回転してエニグマ暗号機のロータの動作をエミュレートする。

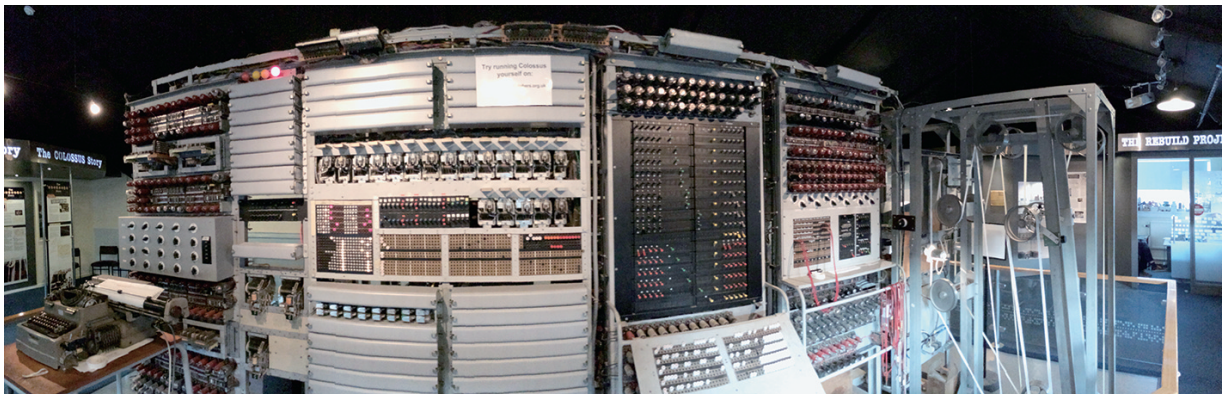

図３　再現されたコロッサス。右手のテープ装置が入力装置、左手のテレタイプが出力装置。