ドイツが誇る傑作暗号機

エニグマへの挑戦

第2次世界大戦における情報戦に
その名を残すドイツの暗号機――エニグマ。
これが作り出す暗号は戦局をも大きく左右した。
やがてその解読のために、膨大な知性と
未来を予感させる最新テクノロジーが投入される。
天文学的な組み合わせに挑む
イギリス情報機関の苦闘と勝利。

文=廣田厚司

Enigma vs Ultra Secret

近代暗号の確立

遠く紀元前五世紀にペルシャ帝国のクセルクセス一世が、ギリシャ軍と戦ったサラミスの海戦で、軍事暗号を用いたのが西洋暗号の始まりとされる。そして、暗号＝cipher（サイファー）とはアラビア語のsifr＝0（ゼロ）から転化したもので、ギリシャが起源であることを示している。しかし実際に暗号の表記法が成熟したのは十九世紀になってからで、一八四四年にサミュエル・モールスが発明した長距離無線電信と、電文記号化の考案からである。

この無線電信によって、戦時には前線部隊と後方司令部間の迅速な連絡が可能となり、やがて通信専門部隊が設置されるにおよび、防諜上の必要性から電文の暗号化が行われた。他方、この方式には欠点もあり、両軍が対峙する一次大戦の塹壕戦などでは旨く機能するが、機動戦や海戦のような場合には時間的差が生じるなど不都合があった。また、遠距離通信は逆に敵国や第三国でも簡単に傍受することが容易であった。しかし、無線電信機器の迅速性や簡便性はこのような欠点を補って余りあるもので、その後この無線通信ベースの暗号作成が世界の潮流となっていった。

第一次大戦におけるもっとも重要な暗号解読の例としては、駐米ドイツ大使ニゲル・ド・グレイが発信した外交用0075号暗号と13040号暗号がある。これはドイツ外務大臣の名にちなみ「ツィンマーマン電文」と呼ばれたもので、欧州戦に米国が参戦しないように対米謀略活動を指令したものだった。英海軍省四〇号室の暗号班は、これを全文ではなかったが解読して米国に通報し、結果的に米国は英仏側に立ち、力の均衡が崩れてプロイセン・ドイツは敗れたのである。

機械暗号の登場

一次大戦中の暗号解析は数字、文字、記号群あるいは、文節や語句の出現頻度・反復や慣用句および文体をベースにして平文化を試みた。他方、暗号を用いる側は前線の激しい砲火の中で、命令の解読や報告電文の暗号化に時間を割かれる結果となった。

そこで、一九一五年に米国人の暗号解読家だったエドワード・ヘバーンが、電動タイプで機械合成する暗号コードを考案した。機械暗号の出現である。機械暗号は換字式、コード式、サイファー式などの既存の暗号よりもランダム性に優れ、さらに迅速、正確に暗号が作成できるという大きな利点があった。

電動タイプライターは文字を電磁作動で印字するが、ヘバーンはそのタイプライターの配線を変えて「A」を打つと「K」や「E」などに変化するようにした。例えば「ATTACK TONIGHT＝今夜攻撃」と打つと、受信側には「SGGSKMOLYPOCT」などの暗号になる。そして受信側は、同じ電気回路の機械を用いて解読した。

だが、この機械暗号は単にアルファベットの組み合わせだけなので、暗号専門家にとってその解読はそう難解ではなく、電文の長さや文字の頻度、文の切れ目の感じから母音と子音を割り出すなどして解析が可能だった。

ヘバーンはこれに気付き、一九一七年に二番目の暗号機械を造った。同じ文字の出現頻度を避けるために可変ローター（回転板）を採り入れ、タイプの文字キーを押すたびにローターが回転して、絶えず異なる文字に変化するようにしたのである。いうなれば、回転するローターを介在させることで、さらにランダム性が高くなり、同じアルファベットの出現をなくすこととなった。このヘバーンの二号機は米国で特許が出願され少数が一九二九年に米海軍で使用されたが、これがドイツの「エニグマ」暗号機の原型となったのである。

さて、ヘバーンの改良暗号機はタイプライターと金銭登録機（レジスター）を併せたような形状で、手前に二六個の大型文字キーがある。中央の斜板上にはアルファベット文字窓が点灯するボードがあり、その上方には五個の回転ローターと、それを挟み込むように左右両端に別の歯車が文字キーと連動していた。各ローター部の円周上には二六個のアルファベット文字が刻印され、ローター・カバーの小窓から突出する歯車を回して文字をセットすることができた。

暗号員が例えば「B」の文字を打つと、電気スプリング作動でローターがスロットマシーンのように不規則回転をして、コード化された文字がもし「P」と変化すれば、点灯ボード上の「P」が点灯する。だが、次に再び「B」を打っても不規則回転により「M」や「R」に変化して点灯するのである。一方、受信側はこれとは反対にローターの小窓にあらかじめ決められたコード文字を最初にセットし電気回路を反対に辿ることで解読ができた。

一個のローターは二六の組み合わせで、一個目が完全回転すると次のローターに回転が移る。これが五個となれば、二六の五乗、つまり一一八八万一三七六通りの暗号化が可能になった。このような膨大なパターンは暗号管理の安全性を飛躍的に高め、欠点だった「出現頻度」の問題を解消した。しかしそれでも複雑な数学的理論と気の遠くなるような解析蓄積によって、解読への道筋はあったのである。

エニグマ暗号機の登場

一次大戦終了後の一九一九年にドイツ・デルフトのヒューゴー・コッホがヘバーンの特許を取得して、秘密印字機（ゲヘイムシュリフマシーネ）の商品化を試みたが実現せず、工場を経営し自らも技師だったアルツール・シュルビウスという人物に特許を売却した。シュルビウスはヘバーンの機械を改良して商品名を「エニグマ」と名付

けた。エニグマとは英国の作曲家エドワード・エルガーが友人や知人を音符で表現し、それを「エニグマ変奏曲」と呼んだエピソードから思いついたものである。

エニグマの基本構造はヘバーンの暗号機と同じだが、三個になったローターの三番目が回転を終了すると、また一番目に戻るように電気回路を設定した結果、実質的に六個ローターと同じ組み合わせが得られるようになったのが特徴だった。

シュルビウスは一九二三年にこのエニグマを自分の工場で製品化し、ライプチッヒで開かれた万国郵便・貿易博覧会に出展して、商業無線や電報が安全に送受信できる「安全機械」だと銘打った。ドイツ郵政省もエニグマを使って祝賀電文を暗号で打ち、大衆の目前で解読する実演を行って見せたほどで、事業の幸先も期待された。

当時ドイツはまだヴェルサイユ条約下にあって、軍隊は一〇万人のヴァイマール共和国軍に制限されていたが、小規模な暗号課（シファレ・アプタイルング）の設置は許可されていた。暗号課の長は後にヒトラー暗殺計画に加わる、有能な通信将校エーリッヒ・フェルギーベル大佐である。大佐は密かに博覧会場からエニグマを引き揚げさせて実験した結果、その性能に満足し、ついで一般市場から機械を全て回収させ、軍用暗号機に必要な改良を施して生産を秘密裏に続行させたのである。

エニグマの出現は実にタイムリーだった。というのも、当時陸軍は密かに大規模な機械化集団と戦術空軍による電撃戦の研究を行っており、それには迅速で安全な通信システムが不可欠であり、「エニグマ」は軽量でバッテリー作動も可能で、かつ戦闘車両上での運用もできる理想的なものだったからである。

初めてドイツ三軍に供給されたエニグマは、三個ローター方式だったが次第に改良されて、後に素晴らしい暗号機となった。当時、ドイツの暗号課は理論的にエニグマの解読は可能だが、現実には同じ機械がなければ解読は不可能だと信じていた。

ポーランドのBS4課

ポーランドは四周を強力な国家に囲まれ、その脅威から優れた情報機関が発達していた。ドイツ対策は暗号局BS4課（ビロウ・スジィフロー）が担当、ワルシャワに本部を置きジビド・ランガー大佐が機関長としてドイツ暗号を解読していたが、一九二八年になってから急に暗号が解読不能となり、ドイツが機械暗号に転換したことを知った。そして、かつてBS4課の情報員が万国博覧会で注目したエニグマ暗号機が、その後市場から姿を消した点に疑いの目を向けたのである。

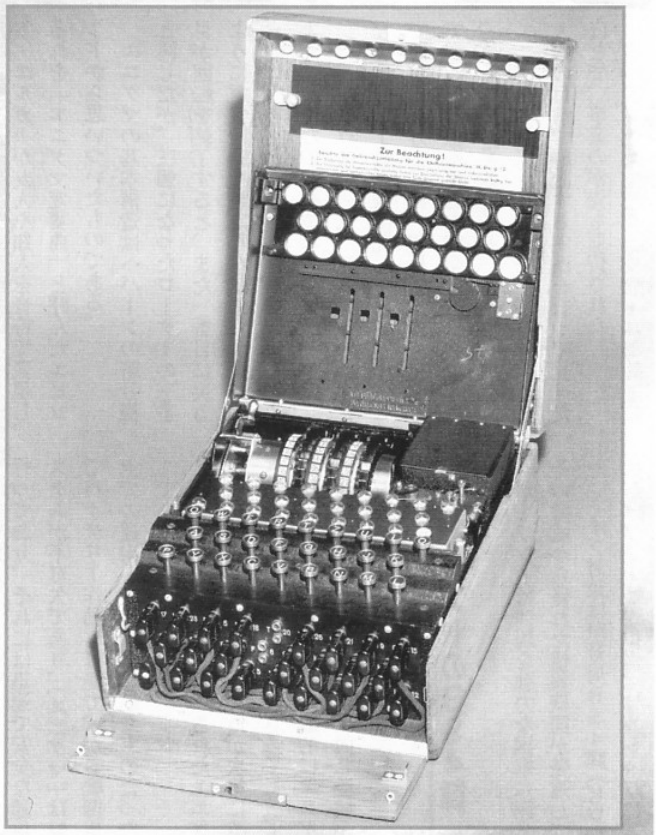
一九二八年某月のある金曜日に在ワルシャワのドイツ大使が、ベルリンの外務省から送られた「荷物」の所在と早期通関を鉄道税関に依頼した。鉄道税関はBS4課の情報担当者を立ち合わせて荷物を開け、中からエニグマ暗号機を発見した。すぐに専門家が集まり機械は徹底的に調べ上げられ、後に注意深く元通りに梱包された。この調査で三個ローターと文字ボードを繋ぐ文字変換配線システムが解明できた。

BS4課は暗号の解析に優秀な数学者が必要となり、ポズナン大学からマリアン・レジェヴスキー、イエルジー・ロツヴィッキー、ヘンリキ・ズガルスキーという三人の若い数学者を獲得した。ポズナンはかつてドイツの占領期間が長かったドイツ語圏であり、この数学者たちのドイツ語もまた完璧だった。

一方、一九三一年の初期にフランス対敵情報部に、ドイツ国防省の事務員がエニグマ暗号と関連書類の売却を持ちかけた。この人物はシュミットといい、暗号名は「アッシュ（灰）」と呼ばれた。当初は信頼されなかったが、対ドイツ暗号課のグスタフ・ベルトラン大尉は、これは本物だと直感して自ら接触し、アッシュの兄弟が高度な機密を入手し得る立場にあることを知ったのである。

一九三一年から三九年までに大尉はアッシュと十数回も欧州諸都市で会い、機密書類のマイクロフィルムが引き渡された。ことに三二年に受け取ったドイツ陸軍のエニグマ・コード・ブックは電文解読キーのサンプルとして貴重なものだった。当時フランスとポーランドは情報活動を協同して行

エニグマを使用中のドイツ兵。傑作暗号機であるエニグマは第２次大戦における情報戦の主役だった。



っていたので、ベルトラン大尉はこれらの情報をBS4課に提供したのである。

やがて一九三三年にヒトラーが政権を奪取して再軍備が急ピッチで進められた。翌三四年になるとBS4課はドイツ陸軍暗号書に記載されている、エニグマの日替わり暗号キーを解読していた。だが、エニグマは絶えず改良され、解読を続行するには最新のエニグマの保有が不可欠と考えられるようになった。

そこでポーランドは六年前にワルシャワ税関で調査したエニグマの複製を、数学的理論で構造を補完しワルシャワのAVA電気通信工場で極秘裏に製造した。しかし、一九三六年になるとドイツ側はエニグマに大きな改良を加え、さらに三七年には回転ローターの配線をも変更した。大きなポイントは「反復指示」技術の応用により、暗号員がプラグ・ボード上のジャックの抜き差しでも電気回路を変更してローター位置を決められる点だった。これによりローター外側の二個のリングが一緒に回転して二六文字のアルファベットを絶えず不規則に暗号化できたのである。

実際の暗号発信はあらかじめ定められた三文字のコード（例えばAAA）を回転ローターの小窓にまずセットする。次にランダムに選んだ三文字（例えばLOX）をキーボードで確実性を得るために二回繰り返して打つと、「L」はキーボードから電気回路を変換するプラグボードを経て「T」に変換される。次に第一ローター、第二、第三ローターを経由して、再び第一ローターに戻る過程を繰り返して変換され、「U」となって再びプラグボードに送られる。ここでもう一度プラグボードの回路変換による換字が行われ、最終過程の点灯ボード上に「A」となって点灯するので、暗号員はこの「A」を控えておくのである。なお、続行する文字の変換も同様に行われ「AOBBMV」の六文字暗号に変換される。

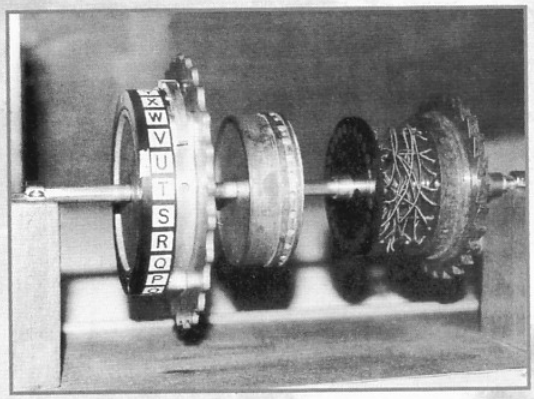
第二段作業では「AAA」に代って今度はランダム三文字「LOX」をセットして平文をキーボードで打つと、以降は五文字群の暗号となって発信される。この時解読コードとなる最初の六文字暗号「AOBBMV」とともに〝コールサイン〟が発信されて送信者と受信者を識別するのである。

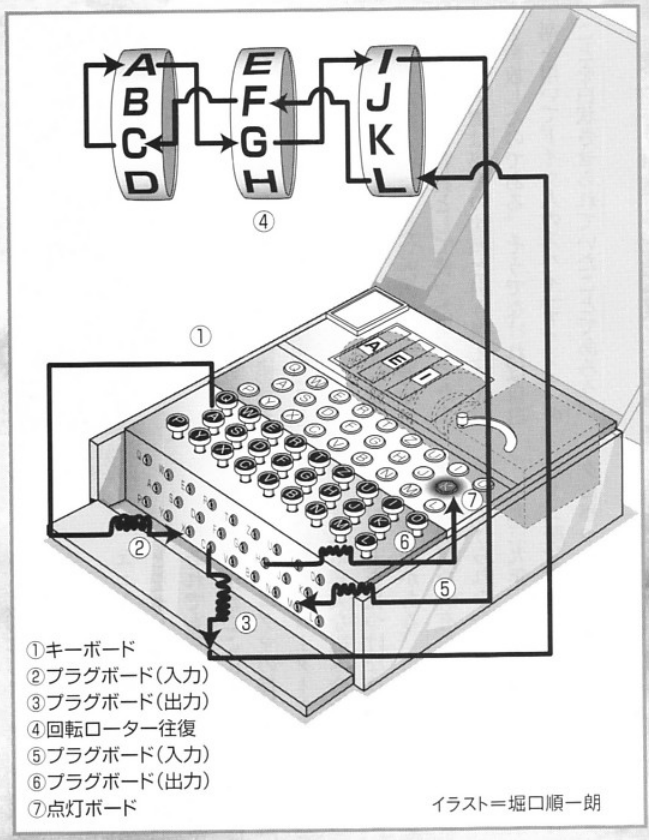
解読はエニグマに既定の三文字コード「AAA」をセットして、最初の六文字換字の「AOBBMV」を打てば、点灯ボードには「LOXLOX」と点灯する。そこで、今度は解読コードを「AAA」から「LOX」に代えてセットして続く五文字電文を打てば、平文となった文字が次々と点灯ボード上に表れて解読ができるのである。つまり、「AAA」は送信者がランダムに決定する解読コード（例では「LOX」）を解読するためのコードなのである。

以上のようにエニグマのポイントはランダム入力の三文字であり、安全性が高くスパイや情報員が知ることはできない。このため暗号送信者は同じ三文字を使用しないように厳しく言われたが、実際には同じものが頻繁に使用され、これが後に解読のきっかけを与えることになった。

エニグマ解読のため、ポーランドのBS4課の数学者たちは数理論に基づいて電気機械式暗号解析機「ボンバ」（爆弾、またはアイスクリームと呼んだ）を開発した。この解析機の中に電文を通過させ、エニグマが設定したアルファベットの組み合わせを見つけてから、エニグマ複製機に解読コードを与えて解読しようとしたのである。この機械はドイツの侵攻時に破壊され、正確にどのような構造でどう作動したのかは定かではないが、完全解読には至らず、ある種の欠点があったことは確かである。

ボンバは非常に高価な機械で、エニグマ一個のローターの動きに追随するのに一台が充てられ、三個ローター・エニグマには五台以上のボンバが必要だった。ところが、大戦直前の一九三八年十二月十五日、エニグマは五個ローターへと改良されて暗号はさらに複雑になった。このためBS4課はボンバを六台から六〇台に増加する必要に迫られたが、平時の予算不足によりついに対応することができなかった。





イラスト＝堀口順一朗

→イラストはエニグマの暗号変換の仕組みを模式化したもの。①キーボードで平文のアルファベットを打つ。②③打たれた文字情報はまずプラグボードに向かい、異なった回路に入ってから出力される。④3個の回転ローターによって変換される。各ローター内には多数の配線があり、次のローターの配線と繋がっている。図ではLの文字の配線は隣のローターのFの文字と繋がっていることを表している。⑤再びプラグボードに向かい、別の回路に入って変換される。⑥結果が点灯ボード上に表れる。これを書き取り改めて小窓にセットして平文を打ち送信するのである。エニグマで注意すべきは、Aの穴や配線から入力されてBの穴や配線に出力されたとしても、文字情報がBに変換されるということではなく、Aの穴（あるいは配線）に入ることで全く別の回路に向かう、ということである。したがって、図のようにLに変換されて回転ローターのLに入るのではない。→（前ページ）エニグマ暗号機の現物。表面カバーが開けられて、内部の3個のローターや、点灯ボードの電球が見える。プラグが多数差し込まれているプラグボードに注意。↑回転ローター1個を分解したところ。向かって右側の部品に多数の配線が確認できる。

フランス情報部のベルトラン大尉はこの事態を知り、英国秘密情報部と接触してポーランドへの支援を呼びかけ、ドイツ・スパイ「アッシュ」のエニグマ情報とポーランドの解析技術を提供した。英国は新たな欧州戦争の危機を感じ、ポーランドとは友好協定前だったが、この支援案に賛同したのである。

英・仏・ポーランド秘密情報会議

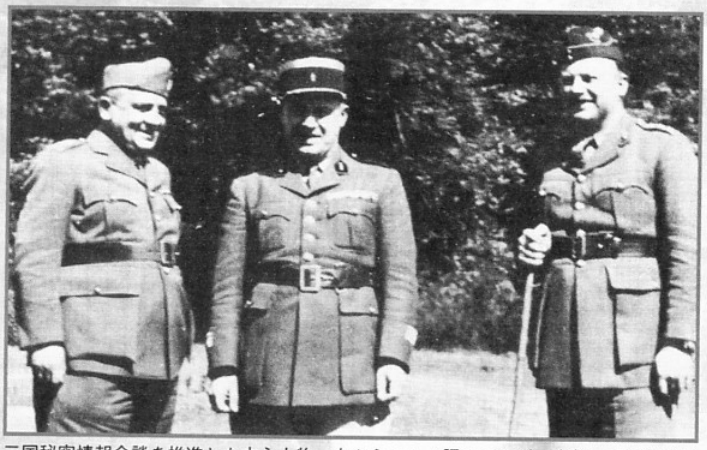
一九三九年七月二十四日に英・仏・ポーランド三者情報会談が、ワルシャワ南東二〇キロのピーリーの「疾風」と暗号名で呼ばれた森林の中で開かれた。BS4課のランガー大佐、数学者のレジェヴスキー、フランス側はベルトラン大尉と解析者のブルックニー大尉、英国側は暗号学校（CC&CS）長のA・デニソンと解読の責任者だったデルウィン・ノックス、そして英国の暗号解読で中心的役割を果たした数学者のアラン・チューリングと「サンドウィッチ」教授と名乗る権限ある人物だった。ポーランド側のソースではサンドウィッチ教授とはMI・5（情報第5課）の長だったメンジースだという説と、そうではないというベルトラン大尉の否定説があり、誰だったのか今日に至るも機密のベールの中である。

さて、三者の情報会議でポーランドは数理論上の暗号解析を続行し、フランスは引き続きドイツの「アッシュ」からエニグマ情報を得る。そして英国は五個ローター型エニグマ解読用に六〇台以上のボンバ解析機を製造することなどが決められた。そしてポーランドの数学者たちはボンバの構造や詳細情報を提供し、AVAエニグマ複製機はフランスに引き渡されてパリへ外交行嚢で運ばれた。

一九三九年九月一日、ドイツ軍がポーランドを席巻し、同月末、BS4課を含む情報部門と数学者たちはパリへと脱出した。十月二十日、ベルトラン大尉はパリ郊外四〇キロにあるクレーの城、暗号名「プルノ」に脱出ポーランド人を集め、フランス情報部の「Z」解読班とともに数台のAVAエニグマ複製機を組み立てた。だが、複製機はボンバ解析機がなければその価値は半減せざるを得なかった。

ドイツ軍が迫り、ベルトラン大尉は地下に潜行して、ムッシュー・バルザックと名乗るレジスタンス要員となり、活動の隠れ蓑としてマルセイユに「地方農業会社」を設立した。そして、九〇キロほど離れたアビニヨンに城を購入し、かつての「Z」班員も合流した。彼らは第300部隊と呼ばれ、六七三本の暗号電文を傍受し、英国が中立国ポルトガルのリスボンに配置していた送信機を入手して、電文をロンドンに送り続けたのである。

この活動は一九四二年十一月八日にドイツ軍がフランス全土を占領して活動を停止するが、組織員の多くは秘密ルートを経て英国に渡った。だが、不幸にもゲシュタポに捕まり強制収容所で命を落とした者も少



三国秘密情報会談を推進した中心人物。左からＢＳ４課のランガー大佐、フランス情報部のベルトラン大尉。

エニグマ暗号解読のための地道な努力

エニグマの三個ローターの組み合わせは「二六×二六×二六」で一万七五七六通りから始まり、後の五個ローターと、アルファベット変換プラグ・ボードのジャックの抜き差しによる電気回路変換を加えると、最終的に二〇兆通りという天文学的な組み合わせを達成していた。陸軍と空軍のエニグマは一〇個ローターのセットも可能であり、おまけに海軍のものは一〇個ローターのうち八個を使用し、さらに四個のローターを随時選択する複雑なシステムだった。

ドイツは戦時ともなれば数台のエニグマが鹵獲されるであろうことをあらかじめ想定していたが、それでも秘匿性に大きな自信を持っていた理由がここにある。エニグマ暗号の解読は、エニグマの機械構造に秘密があるのではなく、ローターや電気回路の変換で生まれる膨大な組み合わせの中から、正しいコードを見つけなければならないことにポイントがある。このため、英国はエニグマの複製を所有しても、解読に大きな効果を上げられなかったのである。

一九三九年、英国のＧＣ（政府暗号）とＧＳ（暗号学校）はブレッチェリー・パークに移った。責任者のエドワード・トラビス中佐はケンブリッジ大学の優れた数学者たちを解析要員として動員、これに最初に加わったのが、一九三六年に現代コンピューター理論を発表したアラン・チューリングだった。数学的才能の他に機械技術の面でも非凡な才能を持っていた彼は、後にポーランドのボンバ解析機を引き継ぎ、その英国版「ボム」を開発した。

この他、ロンドンの暗号教室で数理論を教えていたゴードン・ウェルチマンが、ブレッチェリーに合流した。ボムとエニグマ複製を知らなかったウェルチマンは、モールス電信のコール・サインが送受信者の「所在」を知らせる点に注目し、ついで海軍のＹサービス（通信情報部隊）の支援を得て、膨大なエニグマ電文の中から主要な国防軍部隊の暗号に的を絞る方法を編み出した。

そのウェルチマンの提案で傍受局の無線オペレーター、英帝国海軍婦人奉仕団（ＷＲＮＳ）の暗号解読事務員、技術者、数理学者、情報専門員など、機密保持を誓った一万人以上の男女要員からなる巨大な解読組織が編成された。暗号解読のスタッフの中には、チェスの大会の優勝者、美術館の学芸員、トランプ・ゲームの練達者など、さまざまなタイプの人間が集まっていた。

ブレッチェリーには第一棟から第八棟まで、と、空軍棟、陸軍棟、Ｆ棟、Ｇ棟などがあり、第六棟は陸・空軍用、第八棟は海軍用の無線暗号を解読していた。

この暗号解読の総本山とも言うべきブレッチェリーでは、さまざまな方法で解読のためのコードを手に入れていった。ドイツ軍は二〇万台といわれる膨大な数の暗号機を使用し、日々大量の暗号電文を発信していたが、反面それだけ膨大な数の「手がかり」を発信していたことになる。ブレッチェリーでは、ドイツ軍の電文にある「司令官宛て」、「総統万歳―ハイル・ヒトラー」、「総統ヒトラー」などの宛先や発信元で使う常用語や繰り返し用語を解析のヒントとして比較する解析作業を行った。この他、英国はドイツ空軍が送る気象予報の形態を熟知していて、実際の気象や報告内容を比較することで傍受した暗号気象情報の解析を行い、エニグマ解読に役立てたのである。またドイツ軍は本部指令の伝達にケングルッペ（通信専門部隊）通信網を使用していたことから、ある宛先の暗号電文の一つを解読すると、コードが変更されるまでその系統の電文は解読できたという。

さらにドイツの暗号員がエニグマで打つランダムな「三文字」を雑に扱い、「ＸＹＺ」や「ＡＢＣ」あるいはガール・フレンドや家族の名前の頭文字を用いたことや、句読点がないエニグマ暗号の文末によく「ＹＹ」が用いられたことも解読の手がかりとなった。

また、本来ドイツ語では「Ｑ」はほとんど使用せず、「ＣＨ」が使われるが、その「ＣＨ」の代わりに「Ｑ」を用いるなど、不注意な扱いと繰り返し電文から発信部隊が明らかになり、解読コードを得ることができたのである。

なくない。一方、ゲシュタポの過酷な尋問から、エニグマ暗号の解読が与えた影響が裏付けられる結果となったのは皮肉なことだった。

ベルトラン大尉もまたゲシュタポに捕らえられたが、実に幸運だったのは尋問者はかつて大尉が情報員として使った男だった！

この人物は秘密の沈黙と引き換えに大尉を釈放したのである。そうでなければ自白剤を用いてドイツ人のスパイ「アッシュ」のことを白状させられていたことであろう。

暗号作成には繰り返しはタブーである。「繰り返し・常用語」は「規則性」に他ならず、規則性は解読の鍵となるからである。

ある時など、ドイツの魚雷艇が英仏海峡のカレー沖で機雷を敷設中に、暗号解読のために哨戒機を送ったこともあった。魚雷艇は英国がすでに解読していた哨戒機の接近を示す警告文「エアレッシェン・イスト・ロイヒトネ（浮標は去った）」を暗号化して発信した。英国は傍受した暗号文の中の「APZQF KOLSM」と、「LEUCH TONNE（ロイヒ・トネ）」を比較した。こうすれば「L」は「A」に、「E」は「P」に変換されたことが分かり、これが変換時のエニグマ・ローターの配置やプラグの差し込み位置を解き明かす手がかりとなった。こうして得られたコードを基に暗号解読に大きな貢献をしたのが「ボンバ」の後継機である解析機「ボム」だったのである。

エニグマ解読の功労者「ボム」

ドイツはブレッチェリーの秘匿名「ボム」を知ってはいた。しかし英国爆撃機の航続距離の分析結果と「ボム」という秘匿名称から、英国は原子爆弾の開発を行っているのではないかと推定していたようである。

ブレッチェリーで働いた数学者の一人だったI・J・グッド博士は、一九七六年に、「私はボムについて詳述することはできないが、ゴードン・ウェルチマンの組織的解読の考えに基づいて、アラン・チューリングが実現したとのみ云える」と述べている。

英国の「ボム」は「ボンバ」よりずっと迅速確実に作動した。高さ三メートルの巨大な電気機械式装置で、基本構造はエニグマ暗号機のローターの動きを電磁的に復元するシミュレート・マシーンであり、入力メニューによりプラグ・ボードの電気的変換にも対応する素晴らしい性能の解析機となった。「ボム」は側面カバー板にアルファベットを表示した、三個一セットの色別回転ローターが、一二列並んだものが二段になって合計二四セット・七二個設置されていた。三個一組のローターはエニグマの各ローターの動きに対応し、その配線はエニグマと全く同じで、エニグマ電流の動きをそのまま復元する装置だった。暗号文の読み取りは電動装置で送られる鑽孔（さんこう）テープが回転しつつ延々と検索を行い、第一組のローター回転がアルファベットの一文字を探し当てると、二つ目、三つ目へと移る。他の二三セットのローターも同じ動きをした。

また、電話交換機のような横列型プラグ・ボードには二六個のアルファベットを表示した差込ジャックが用意され、メニューの入力で回転ローターを修正位置に動かすことができた。結果的に、五個ローターを用いるエニグマの三個ローターの動きを解読することができたのである。

ここで注意すべきは、「ボム」は暗号自体を解読するものではなく、既述のエニグマ暗号の最初に入力されるランダム三文字を復元する装置である。あらゆる組み合わせ

①第3棟
②第4棟
③第6棟
④第8棟
⑤第3棟（一九四二年まで）
⑥旧邸宅（ウルトラ情報）
⑦陸軍棟
⑧G棟
⑨空軍棟
⑩F棟

ブレッチェリー・パークのGC（政府暗号）&GS（暗号学校）の全景。ゴルフ場が2つ入るほどの総面積を誇る。第3、第6、第8棟は情報分析だが、特に第6棟では陸・空軍用、第8棟では海軍用の無線暗号を解読していた。、壮麗なおもむきの旧邸宅はウルトラ情報を扱う施設である。これら広大な施設の中で「ボム」は複数が分散配置されていた。

＊鑽孔テープ＝信号読み取り用の穴の空いたテープ。

西方電撃戦でのグデーリアン。左下にエニグマが見える。エニグマは前線で使用するのに最適であり、電撃戦の影の立て役者となった。

を高速演算で検索する、今日のコンピューター的概念による解析機だったという点にある。

「ボム」によって復元されたキー文字は、今度は複製エニグマ暗号機にかけることで暗号を平文化した。識別キー文字が正しければ平文になるが、暗号化されたままの状態も無論あった。なお、面白いことにブレッチェリーのエニグマ暗号機は英国製だが、ドイツのオリジナルより迅速性に優れていたという。

ブレッチェリーに何台の「ボム」があったのかは秘密のままだが、極秘に警備された広い田園地帯の大きな田舎の邸宅に分散配置され、WRNSの婦人要員が八時間交代三シフト二四時間を通して作業を行った。だが、本当の暗号解析者たちは第六棟と第八棟にいて彼らが頭脳の役目を果たしたのである。

暗号解読の恩恵とウルトラ情報

戦後三〇年を経て公開された一部のウルトラ情報や、ウェルチマンの話によれば、英国の最初の暗号解読は一九四〇年四月のドイツ軍のノルウェー侵攻戦だった。やがて、傍受暗号が急増し、電文の方位探知とコール・サインを関連付ける方法により、五月のフランス戦までに第六棟では重要な電文をかなり解読していたが、まだ全体からすれば部分的なものだった。

やがてドイツの装甲部隊はフランスを席巻したが、ハインツ・グデーリアン大将はエニグマを搭載した装甲指揮車に乗り、無線を使って前進部隊と連携した。これはエニグマ軍事暗号を使用した初期の典型的な例である。

ゴードン・ウェルチマンは、「初期の暗号解読がフランス戦で重要な貢献をなしたとすれば、それは欧州戦の絶望的情況を明らかにしたことと、あらゆる小型船舶を動員してダンケルクから、三四万人もの兵士を救出する僅かな時間と機会を得たことである」と述べている。

しかし、エニグマ暗号の解読は、情報戦という広い意味では「小さな」部分情報にすぎないと言える。次の段階は、その集積された部分情報をつきあわせて分析しなければならない。これは主に第三棟の熟練したドイツ語通訳たちが、些細な情報を繋ぎ合わせて局面を判断できるようにした。

どんな微細な情報でも順に揃えられ、膨大なカード索引が作られた。そこには数千、数万の名前、部隊、階級、補給の要請、軍法会議あるいは軍人の休職やその期間にいたるまでカバーされていた。その結果、空軍の一少尉の転属がある作戦の攻撃が迫ったことを示したこともあった。

このような膨大な情報を処理し集積する組織が必要となり、一九四〇年の春に「ボム」による解読暗号を「ウルトラ」情報と呼び、その秘匿管理はMI・5のスチュワート・グラハム・メンジースの指揮下に置かれることになった。そして英空軍情報部のウインターバザム大佐が特別な審査を通過した空軍の将校や無線手、暗号員、情報員からなる特別連絡部（SLU(s)）を編成し、チャーチルを始めとする英国の最高統帥部にのみ配布した。なお「ウルトラ」とは、ネルソン提督がトラファルガー海戦で用いた秘匿名称に由来する。

戦争の進展とともにブレッチェリーの組織はいよいよ重要となり強化されていった。無線の傍受局は北スコットランド、ドーセット、ミッドランド東海岸方面に点在し、六〇〇名以上の地区補助奉仕団（ATS）の女性要員が、干渉電波をカットできる米国製のRCA・AR88水晶受信機で、二四時間体制でモールス信号を書き取り、それをテレプリンターでブレッチェリーに送った。

大英航空決戦でゲーリング元帥が制空権を得られぬことに苛立ち、戦闘機隊に対して「英空軍を戦闘に引き込み撃滅せよ」と命じ、大規模な戦闘機隊を投入して挑発したが、英空軍戦闘機軍団司令官ダウディング大将はこの方針をウルトラ情報で知り、数個飛行中隊を投入するだけで迎撃戦力を温存することができた。一九四〇年九月頃、英空軍基地撃滅からロンドン爆撃に変更されたゲーリングの戦術転換をもウルトラによって知り、英国は救われたのである。

だが、一九四〇年十一月十四日にドイツ

空軍の「月光のソナタ」作戦により、コヴェントリー市が五〇〇機のドイツ爆撃機に襲われて焼け野原となった。ブレッチェリーのウルトラ情報は少なくとも二日前にこれを察知して、チャーチルに警告していたが、エニグマ暗号解読の事実が知られることを恐れて手を打たなかったとされている。ただし、英空軍の公刊戦史ではこの点には全く触れられていない。

大戦の後半になって、米第3軍のパットン中将はウルトラの優れた運用者となった。パットンはグデーリアンのように指揮車に乗って戦車とともに戦場を疾駆していたので、ウルトラ情報の活用が容易だったからである。

他方、パットンのライバルだったモントゴメリー元帥はあまりウルトラ情報に重きをおかず、一九四四年九月のオランダ・アルンヘム空挺作戦では、情報は無視されたとウィンターバザムは述べている。ウルトラ情報は「ドイツの強力な戦車連隊が英空挺部隊に対抗する」と警告したが、モントゴメリーは注意を払わなかった。しかもモントゴメリーは、空挺部隊がアルンヘムへ降下する一日前に彼の司令部を訪れた情報特使の「雀蜂の中に空挺隊を降下させるようなもの」との警告文を開かずに脇に置いた。この作戦の結果は、周知の通りである。

ドイツ海軍のエニグマ

ドイツ海軍は一次大戦における英海軍省四〇号室の活動を知り、陸空軍よりずっと保全管理と秘匿に注意を払い、「シュリセル(鍵)M」として知られる独特の海軍暗号を用いていた。実際に一三種の暗号が使用されたが、連合軍側から見ると北大西洋で猛威を振るったUボート作戦に用いられた「ヒュードラ(海蛇)」暗号が最も重要なものだった。

Uボートのエニグマは八個の回転ローターから任意に四個を選択するのが特徴で、海軍暗号員は訓練が行き届き、暗号化にともなうミスは極めて少なかった。このため一九四〇年～四一年夏まで、英国はヒュードラ暗号の解読ができなかったのである。

英海軍省のUボート追跡室にいた海軍情報局のパトリック・ビーズレーによれば、ドイツのトロール船三隻から貴重なエニグマの予備ローターを奪取したが、それでもブレッチェリーの海軍第八棟ではまだヒュードラ暗号の解読に至らなかったという。

ただし、一九四一年五月八日、U110がグリーンランド沖で、英海軍の爆雷攻撃を受けて損傷浮上した際に捕獲されたことがあった。臨検隊によってエニグマ暗号機は英海軍の手中に入り、しかも無傷の回転ローターと現用暗号書までもが捕獲されたが、翌日、U110は曳航途中で沈没した。そして、U110の捕獲が公表されたのは一九五八年であり、エニグマ暗号機の捕獲は公表されていない。だが、ビーズレーはこれを知り得る立場にあり、これが契機となってヒュードラ暗号が解読されるようになったと語っている。

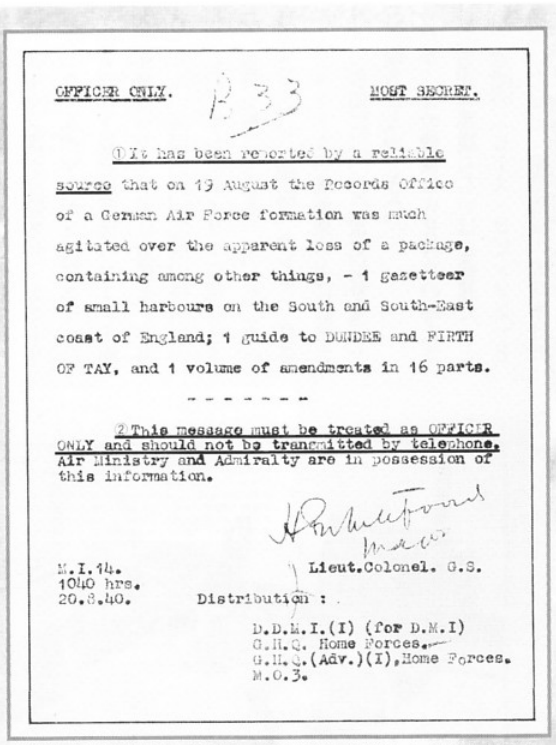
ドイツ海軍は慎重に新たな「トリートン(平身平魚の海神)」暗号に変更するが、英国は改良された「ボム」と「ヒュードラ暗号」の経験を生かして、一九四三年四月になってこの新暗号を解読した。この結果、注意深い欺瞞計画を実施してから主要な船団の航路を変更することで、Uボートの狼群攻撃を避けることができたのである。

さらにそれ以上の収穫があった。UボートIX型で「ミルヒキューエ(乳牛)」と呼ばれる潜水補給艦によって、Uボートは基地に帰ることなく、洋上で燃料、水、食料などを受けて長期間通商破壊戦を可能にしていた。この「乳牛」の所在を突き止めて撃沈したのである。

ゲヘイムシュライバー

英国で密かに暗号名を「フィッシュ」と称された、エニグマと並ぶもう一種の高度な暗号機があった。それはドイツでゲヘイムシュライバー(秘密印字機)と呼ばれる自動暗号作成・解読機である。

エニグマは軍事面で使用されたが、ゲヘイムシュライバーはドイツ外務省が中立国や枢軸国の大使館と連携して送る、最も機密度の高い外交通信に使用された。ドイツ



OFFICER ONLY. B33 MOST SECRET.

①It has been reported by a reliable source that on 15 August the Records Office of a German Air Force formation was much agitated over the apparent loss of a package, containing among other things, - 1 gazetteer of small harbours on the South and South-East coast of England; 1 guide to DUNDEE and FIRTH OF TAY, and 1 volume of amendments in 16 parts.

- - - - - - -

②This message must be treated as OFFICER ONLY and should not be transmitted by telephone. Air Ministry and Admiralty are in possession of this information.

Lieut.Colonel. G.S.

M.I.14.
1040 hrs.
20.8.40.

Distribution :

D.D.M.I.(I) (for D.M.I)
C.H.Q. Home Forces.
G.H.Q.(Adv.)(I),Home Forces.
M.O.3.

イギリス軍の報告書。内容は、地名便覧を紛失したドイツ空軍の一組織が「微細な動揺」に陥っていることを報せている。下線①の「信頼すべき筋によれば…」とはウルトラ情報を示している。こうした組織内の報告書でも、ウルトラ情報の名は伏せられていた。下線②には取り扱いは将校のみ、電話送信の禁止が明記されている。

はこの暗号の解読は不可能ではないが、非常に長い時間を要し、解読できた時には無価値になるであろうと考えていた。

この暗号機はドイツ電話電報会社が解読不能な暗号機の製作をと、ジーメンス・ウント・ハルスケ社に依頼して開発されたもので、暗号化と解読が一作業で済む特徴をもつ大型電動タイプのようなものだった。訓練された暗号員を使わずに事務員が平文を自動暗号化して電話線か無線電信で送信し、解読側は同じ機械で受信し逆操作により平文を打ち出すことができた。

ゲヘイムシュライバーの基本は、マーレー電報コードを用いるテレプリンターの一種である。このコードは二進法を用い、「A」は「+・+・スペース・スペース」と表され、二進演算によってデータや物理量を数字で表現する今日のデジタル記号である。

ゲヘイムシュライバーは一九一七年に米国の電信電話会社の技師だったギルバート・バーナムが考案した電信暗号機械をベースにしたものである。バーナムは簡単な記号原則（記号＋記号＝スペース、あるいは記号＋スペース＝記号など）を考案し、この記号を数字の1に、スペースを0に置き換えた。この方法により、平文の「A」は1・1・0・0・0という五文字で表示されることになる。

バーナムが造ったこの五文字暗号機は暗号文が長文となる欠点があったが、充分安全な暗号機として二次大戦中に米陸軍が使用したもので、ジーメンス社のゲヘイムシュライバーが初めて二進法を用いた機械ではなかったのである。

ゲヘイムシュライバーはエニグマのような回転ローターを使用し、五個のローターで解読コードを設定する。そのあとはエニグマと異なり一文字入力ごとに五文字のマーレー記号に変換されるが、バーナムの暗号機より優れていた。事務員はタイプのようにキーで平文を打ち、一分間に六六文字が暗号化され電話線や無線電信で送信される。万一、回線から異なる暗号が送り込まれる妨害を受けても、プリント段階で数字や句読点ばかりの無意味な文に変化する。なお、この機械は後の改良型ではさらに進化したものとなった。このように優れた暗号機であったが、理論的には有限であり反復パターン解析による電文解読が試みられた。しかし、戦争初期における英国の解読はほんの僅かなものであったようだ。

ジーメンス社の幹部によれば、この暗号機は細部を含めると五種類の型が開発され、一九三九年型は52B型と呼ばれ、さらに安全度を増した型は52C型で一〇個のローターに非常に複雑な暗号化構造を加え、さらに一部の回転ローターに不規則回転を与える装置が搭載されたもので、戦後も西ドイツで使用されたといわれている。

ブレッチェリーでは、テスター少佐の調査班に数学者のW・T・チュッテとM・H・A・ニューマンが加わり、ゲヘイムシュライバーの暗号解読に挑んだ。四二年に同班は暗号化の過程を類推し、暗号機械の複製が必要だとする結論に到った。そして新たにニューマン班が設置され、チューリングとウェルチマンが支援役となった。

複製機の主設計は英国のレーダー開発の中核だったTRE研究所と、ドリス・ヒルの英国郵便研究所の技術者が担当した。ブレッチェリーに運び込まれた複製機械は二台あって、八〇本の真空管を用い、幅四八センチ、高さ二・七メートルの郵便架の上に設置され、一秒間に二〇〇〇電気信号文字を読み取ることができた。

だが、この機械はWRNSの婦人要員たちが「馬鹿らしいほど複雑だ」という意味の「ヒース・ロビンソン」と名付けたほど、暗号解読の成功率は低いものであった。

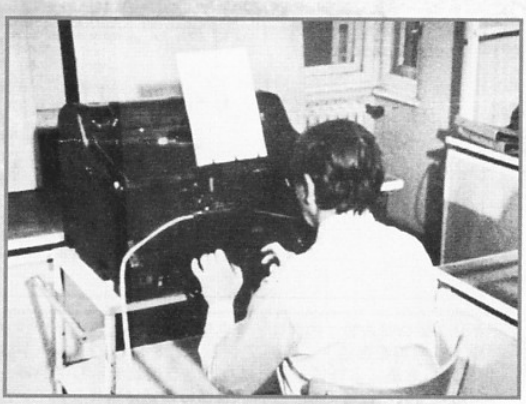
究極の解析機コロサス

一九四三年一月、郵政省の技術者で高速電路制御機の専門家だった、T・H・フラワーとS・W・ブロードハーストの二人が暗号解読に加わった。フラワーは自動電話交換機を設計した人物だが、信頼性の高い高速制御スイッチによって精度を高めて問題を解決すべく、全く新しい概念を打ち出した。これが世界最初のコンピューター「コロサス（巨像）」である。

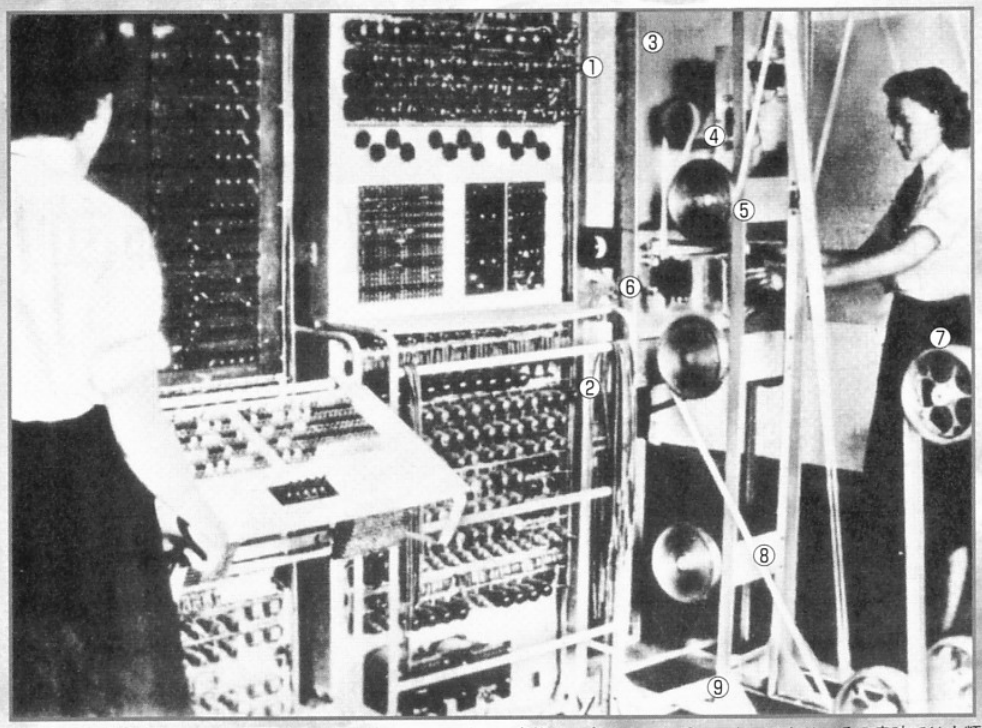
高価なコロサスの製作が許可され、一五〇〇本の真空管と多くの電子機器が組み込まれ、コロサスMkIとして完成したのは四三年二月のことである。不確実な鑽孔テープによる信号の再現から、電子的な処理方法に生まれ変わっていた。

コロサスMkIのサイアトロン・トリオード（ガス封入熱陰極放電管：のちに電子制御機能を持つサイアトロン・トランジスターに発展する）が、高圧電流を高速制御できたので、ゲヘイムシュライバーの動きに瞬時に反応し、その電気的な動きを再現することが可能となった。そして、二進演算とボーレン論理動作という処理を行うことで、読取速度は毎秒五〇〇〇文字という驚くべき速度を達成した。

操作方法は今日良く使われる、通信回線をオンラインでホスト機に接続するオンライン・プログラミングを用いた。機械と人



ドイツのゲヘイムシュライバー。エニグマに比べて、かなり大きいことがわかる。



究極の暗号解析機、コロサス。写真はMkIである。コロサスの実態は、今日のコンピューターであり、その意味では人類初のコンピューターだったといえよう。コンピューターの歴史では、人類初のコンピューターはアメリカが開発したENIAC(エニアック)とされている。コロサスは暗号解読という機密性の高い分野に属していたので、戦後には設計図は焼却され、現物も破壊されてその存在が葬られたのである。

間の対話方式は現代のコンピューターでは一般的なものだが、これが今から六〇年も昔のことと考えれば、驚くべきことではなかろうか。

コロサスMkIは完全な電子装置で、暗号解読が正確に再現でき、前型の機械式と違ってエラーすることはなかった。そして一度正しいキー・コードを発見するとそれ以降に続く電文全部が解読されていった。

一方、一〇個ローターの複雑な不規則回転に対応するため、一九四四年の初めにコロサスMkIを改良したMkIIが製作された。MkIIはいわば今日の「イフ論理」とも言うべき回路を分岐させ、ローターの不規則回転に対応して機械が条件を選択できた。これはコンピューターでは重要な能力で、すでにこの機能が付与されていたとは驚くばかりである。

MkIIはMkIより大型で、二五〇〇本の真空管を用いて毎秒五〇〇〇字の速度で文字を読み取ったが、五文字暗号を読む能力は毎秒二万五〇〇〇文字であり、戦後一〇年間、商業用コンピューターもこの性能を超えられなかった。一方、プリンター出力は電動タイプが使用され毎秒一五字だった。

一九四四年六月に英米連合軍は大陸反攻のノルマンディー上陸戦を予定し、その直前の三月に一〇台のコロサスMkIIが極秘で発注され、同年六月一日までに稼動するように要求された。一時は不可能と考えられたが、専門家と技術者を集中してぴたりと予定日から作動を開始した。そしてそれまでの機械で悪戦苦闘した、二五〇名のWRNSの要員たちは、操作に熟達して非常に高度なウルトラ情報を生み出した。しかしながら、理由は分からないが、このコロサスMkIIがその解析性能を生かしてエニグマ暗号の解読に使用されることはなかった。

「ボム」や「コロサス」によってもたらされたウルトラ情報は戦争の深奥部で大きな影響を与え、大局面では連合軍の将兵の生命を救い勝利に貢献した。しかし、情報の使用には厳重な注意が払われ、ソースが捕虜尋問や偵察、偶然、あるいは占領地での地下活動から得られたようにカバーがかけられ、その実態は徹底的に秘匿された。

当時ドイツの情報関係者は、ウルトラ情報は英国秘密情報機関の活動結果と考えたし、実際にドイツ軍人たちは長いこと暗号が破られたとは信じようとしなかった。

また、ドイツは一九四五年に新たなエニグマ暗号機の実用化を計画していたので、もし戦争が長引いてこの新エニグマが配置されたなら、ブレッチェリーでの解読は再び振り出しに戻ることになっていたであろう。だが、ドイツにとってV2号やMe262ジェット機などの革新的兵器と同じように、時すでに遅かったのである。

本稿のために貴重な資料を提供願った、英国ウェスト・ヨークス在住のジェフ・パベィ氏に感謝したい。

For their valuable contributions the author wishes to thanks: Mr. Jeff Pavey, West Yorks England.