日本IT書紀

059 新兵器

04 含牙篇
巻之七 乾坤

佃 均

第五十九

新兵器

一

第一次世界大戦では、潜水艦、爆撃機や戦闘機、水上機母艦、戦車、地雷、毒ガスといった「新兵器」が登場した。ここで「新兵器」とかぎカッコで括ったのは、個々に見れば、いずれも十九世紀末までに登場していたからである。

例えば潜水艦は、一六二〇年にロンドンのテムズ川で初の潜行航行に成功し、一七七六年に初めて兵器として使用されている。

また飛行機はアメリカのライト兄弟によって一九〇三年に発明され、第一次大戦で初めての空爆と空中戦が行われた。戦争が使用法を変え、使用法が変わることで新しい機能が追加された、といっていい。

一九一四年九月、第一次世界大戦で膠着状態にあった西部戦線に登場した「タンク」（戦車）と「地雷」もそうだった。

車輪が付いた戦場を駆け巡る利器という意味での「戦車」は、紀元前のシュメール文明で発生している。中国では三国志のころ、車体の両脇に長い刃を装着して歩兵を撫で斬りにする戦車があった。自動車を分厚い鉄の板で覆い、機関砲を備え、車輪に無限軌道を装備したという点で、イギリス軍が投入した四十九台の「タンク」は画期的だった。

さらに東部戦線では毒ガスも使われている。

さらに画期的だったのは、水上機母艦である。

そもそもは輸送船に過ぎなかったが、それにクレーンと格納庫を備えつけ、敵陣の近くの海面に水上艇を下ろして発進させたのである。さらにイギリスは建造中だった大型巡洋艦「フューリアス」の設計を変更して、前甲板と後甲板を改造した。ここに世界最初の航空母艦が誕生した。

フューリアスは巡洋艦として設計されたために、艦の真中に高い艦橋と煙突がそびえていた。そこでイギリスは、建造に着手したばかりの大型商船の設計を改め、艦首から艦尾までを飛行甲板にして飛行機の発着を専門とする特殊な船「アーガス」を建造した。これがのちの航空母艦の基本型となった。

ついでなので航空母艦について書いておくと、当初から航空母艦として設計された最初の艦船は、日本の「鳳翔」である。この船は浅野造船所で一九二二年に竣工し、翌二三年に就役した。ところが航空機が発着するには甲板の形

状が不備であったり、海洋のうねりによって艦が安定しないなど、大きな問題が潜んでいることが判明した。

「鳳翔」が実戦に配備されたのは一九三三年のことだった。上海事変に動員され、そのとき同艦から発進した日本の戦闘機がアメリカ人パイロットの操縦する中国軍機と初の空中戦を行っている。

太平洋戦争ではミッドウエー海戦に参加したのち、広島の呉港で飛行兵の発着練習用に使用された。米軍の空襲で軽微な損傷を受けたが、一九四五年八月十五日の時点で帝国海軍の空母としていまだに健在だった。

イギリスは日本の「鳳翔」から遅れること二年で「ハーミズ」を竣工し、ほぼ同時に「イーグル」を完成させた。アメリカは石炭運搬船として建造中の「ジュピター」の設計を途中から航空母艦に改め、「ラングレー」の名で就役させた。

その後、イギリス海軍は「カレイジャス」「グロリアス」「アークロイヤル」「イラストリアス」「コロッサス」などを、アメリカ海軍は「レキシントン」「サラトガ」「レンジャー」「ヨークタウン」「ワスプ」「エセックス」などを、フランス海軍は「ベアルン」を、大日本帝国海軍は「龍驤」「蒼龍」「飛龍」「翔鶴」「大鳳」「信濃」「雲龍」「千歳」「瑞鳳」などを建造している。

不思議なことにナチス・ドイツとファシスト・イタリアは空母を建造しなかった。ナチス・ドイツは代わりに潜水艦を作った。このあたり、思想の違いというほかはない。

各国が航空母艦を相次いで建造したのは、ロンドンとワシントンの二度の軍縮会議で、戦艦と巡洋艦の新規建造が規制されたためだった。航空母艦は規制の対象ではなかった。それと空からの敵地爆撃の効果が認識され始めていた。

艦数だけだとイギリスが七、アメリカが七、フランスが一、日本が十と、日本が最も多い。しかしイギリスとアメリカは並行して、航空母艦に転換することを前提とした輸送船を建造していた。

潜在的な航空母艦を合わせると、第二次世界大戦の初期、イギリスは二十四隻、アメリカは四十八隻を保有していた。日本は戦ってはならなかったのだ。

二

第二次大戦で登場した「新兵器」は何であったろう。

戦車、航空母艦、戦闘機、潜水艦などは、第一次大戦から二十五年の間に改良が重ねられ、大きな変貌を遂げていた。なるほど大戦の末期に原子爆弾が発明されたが、通常の使用に供する兵器ではない。

その意味ではおそらく、
――レーダーと暗号装置である。
ということになる。
このうちレーダーについては、すでに書いた。
暗号装置は、コンピュータの基本原理を形成した一要素として、しばしば紹介されている。
最も有名なのは、ナチス・ドイツが使用した「エニグマ」(Enigma)である。
ドイツ語で「謎」を意味するこの装置は、一九一八年にその原理に特許が与えられ、一九二〇年代には商用機が発売されていた。タイプライターと同じキーボード（ただしドイツ語用にウムラウトのキーがあった）からアルファベットを入力すると、内部に装着されたローターでランダムに別のアルファベットに置き換えられ、最終的にはまったく意味をなさないアルファベットと記号の列に変換される。
原理はこうである。
キーボードが動いて何かの文字が打たれると、電流が流れる。すると第一のローターが動いて、第二のローターに信号が送られる。
第一のローターが「A」を発信すると、第二のローターで一つあとの「B」に変換される。第一のローターの「B」が第二のローターで二つあとの「C」に置き換えられる。
すると原文「AB」は、二度の置き換えで「CD」に変換される。
むろん、これでは単純すぎて暗号にならない。
そこで、ローターの周期を違える。
第一、第三のローターが十五回転する間に第二、第四のローターが十七回転する。初期のモデルはローター一個に二十八の電極があったから、電極の数と回転数の相乗によって理論上、三百九十九億六千八百万六千四百通りの組み合わせができる。
ドイツの陸軍が制式に採用したのは一九二八年だった。
ここでエニグマは軍用に改良され、ローター一個当たりの電極が二十六個に、ローターは三個に減らされたが、反転ローターとプラグボード（統計会計機械装置の配電盤と同じ原理）が採用された。
三個のローターの回転周期を二十六、二十五、十六に高速化したので、文字を変換する理論上の組み合わせは一億八千二百七十九万四百通りだった。そこでさらにプラグボードの配線を変えることで、ほとんど無限大の組み合わせが生成されるというわけだった。
とはいえ、以上はあくまでも理論上の数字であって、実際にはいくつかのパターンが使用された。送り手が生成した暗号を受け手が解読できなければ何の役にも立たないし、

現場の部隊に数学の専門家がいるわけではなかった。このことは、装置の原理とパターンが判明すれば、傍受者が解読できることを意味していた。

ナチス・ドイツの膨張がソ連を指向していることが明らかになった一九三〇年代、自国が理不尽な戦場となることを恐れたポーランドのマリアン・レイェフスキという数学者が、初期の「エニグマ」の暗号を解読することに成功した。

彼はナチス・ドイツ軍の部隊の間で交わされる暗号文に、

――〇〇から〇〇へ。

――本日、異常なし。

といった定型的な文章が繰り返し入っているに違いないと考えた。

そこで彼は傍受した暗号を丹念に分析して、いくつかの定型文を見つけ出した。仮説と推理によって単語が解読され、個々のアルファベットを元のアルファベットに置き換える方法が発見された。

一九三八年の十月頃、レイェフスキはポーランド軍の参謀本部第二部暗号局に属していたヘンリク・ジガルスキ、イェジ・ルジツキという二人の若い研究者をチームに加えて、符号を一致・不一致を照合して解析する仕組みを考え出した。

これが「ｂｏｍｂａ」（ボンパ：爆弾）という暗号解読機となった。しかしポーランドは「ｂｏｍｂａ」の存在をイギリスやフランス、アメリカなどにも秘匿していた。

暗号が解読されているらしいことを察知したナチス・ドイツは、ローターの数を五個に増やし、ローターの回転周期を変更した。これにより理論上の暗号生成機能が一気に一千倍に引き上げられた。ただし交信のパターンまで変わったわけではなかった。

ポーランドの学者たちはなおも解明の努力を続けたが、ナチス・ドイツ軍の侵攻によって彼らの研究は途絶えてしまった。ただしナチスが侵攻する直前、「ｂｏｍｂａ」の情報はイギリスに引き渡された。

これがイギリスで改良されて「ＢＯＭＢＥ」と名付けられ、さらに改良されて「Colossus」（コロッサス）となっていく。

三

一九四〇年の二月、イギリス軍は最新の「エニグマ」のローターを手に入れることができた。大西洋上で捕獲したドイツ海軍潜水艦（Ｕボート）「Ｕ33」号の乗組員が、ポケットの中のローター二個を破棄するのを忘れたためだっ

た。

そのローターはただちにケンブリッジ大学のキングスカレッジに送られて、暗号解読研究チームに渡された。

次いで同年五月、同じく大西洋上でトロール漁船を偽装していたドイツのスパイ船から、大量の通信文書が接収された。これもまたキングスカレッジに送られた。暗号文とそれを解読した文書を照合すれば、仕組みが解明できるはずである。

ここにマックス・ニューマンという数学者がいた。

彼はイギリス郵政省の研究班と共同で、暗号解読装置の開発を行っていた。その装置はナチス・ドイツ総統ヒトラーが連絡に使う専用の暗号「フィッシュ」を解読するのが目的だった。彼はフィッシュ暗号を統計的に解析する装置の開発を進めていた。

彼は、教え子で英米首脳間秘話装置の開発を担当していたアラン・チューリングを中心に、アメリカの研究者を交えたチームを作り、エニグマ暗号を解読する作業に着手した。

イギリス政府はキングスカレッジに約一千人の科学者、数学者などを集めて解読に当たったという。しかるにアラン・チューリングが初めて「エニグマ」の暗号体系を解明した。

彼が作成した「チューリング・マシン」および、一九四三年に開発した暗号解読装置「コロッサス」がヨーロッパ戦線の状況を一変させた。ナチス・ドイツ空軍機の爆撃目標が事前に把握できるようになっていく。

――イギリス政府は解読に成功したことをナチス・ドイツに知られたくなかったので、コベントリーにドイツ軍の空襲があることを承知していながら、住民に避難を勧告しなかった。

という話がある。

だが、これはどうやら後世の創作であるらしい。

当時の研究者たちは、ドイツ空軍が使用していたイギリスの都市名のコードまでは解読できなかった。エニグマ暗号を解読したとき「ＫＯＲＮ」で示された都市を、彼らはロンドンだと考えていた。暗号とは別に符号の解読も必要だったのである。

四

ナチス・ドイツと同盟を結んでいた日本にもＵボートによって「エニグマ」の技術が伝えられた。そのまま適用されなかったのは、アルファベットと日本語の違いゆえだった。

日本語にはアルファベット、数字のほかにカナがある。通信文をカタカナにして、受信側で漢字交じり文に直すにしても、文字種が倍も多い。

このため日本では独自の改良を重ね、「エニグマ」と同じ原理ながら異なる機構を採用した「紫」を外交文書や外交指令に適用した。また海軍は「九七式欧文印字装置」を開発し、陸軍は「三式換字機」を作った。

このうち「紫」は日米交渉中にあらかたが解読され、海軍の「九七式」は太平洋戦争が始まった半年後から一年後の間にほとんど役に立たなくなった。アメリカの政府や軍にとっての重要度の順と考えればいい。

エニグマを真似たとはいえ、「紫」は日本語を暗号化する独自のコード体系を持っていた。そこでアメリカ連邦政府は専用の解読装置を開発することにした。

初期の解読は人手によって行われ、次いで「エニグマ」用に開発された「ＢＯＭＢＥ」という装置が適用された。この装置の開発にはイギリスのチューリングもかかわった。

一九四一年に入って、ウィリアム・フリードマンが「紫」の解読に成功した。彼は「紫」のコードを解明したばかりでなく、海軍の「九七式欧文印字装置」の模造機を作ってもいる。

フリードマンが作製した「紫」解読装置は「パープルマシン」と名付けられ、日米開戦までに八台が作られた。そのうちの二台がイギリスに手渡され、ロンドンの北方七十キロのブレッチリーという町にあった「政府通信本部」（ブレッチリー・パーク）に設置された。

ブレッチリー・パークのスタート時は二百人程度だったが、第二次大戦末期には補助要員も含めると一万人にのぼる人々が働いていた。そこでベルリンの駐独日本大使館が発信する暗号文を傍受して解読した。

首相チャーチルが側近に「ブレッチリーは私のウルトラシークレットだ」と語ったことから、同本部で解読されたナチス・ドイツや日本の暗号通信文は「ウルトラ」と総称された。ドイツで開発された暗号技術が日本を経由してアメリカからイギリスに渡り、太平洋戦争の戦況を左右したことになる。

ワシントンの駐米日本大使館は、「九七式欧文印刷装置」と「紫」で本国と電信文をやり取りしていた。「海軍甲」と称された方式である。

少なくとも一九四一年十月以後、アメリカ連邦政府の対日交渉グループは日本政府の対米英開戦決意や「帝国国策遂行要領」を周知していたわけだった。ドイツ・ベルリンにある日本大使館から発信される情報と照らし合わせていたアメリカ連邦政府は、日米交渉の主導権を完全に握って

いた。

しかし、だからといってアメリカ連邦政府は、日本がいつ宣戦を布告してくるかまで承知していたわけではなかった。というのは、日本帝国陸軍は「三式換字機」という別の暗号装置を使っていたし、海軍は外務省とは異なるコード体系を持っていた。

海軍には「甲」「乙」「丙」「丁」「戊」「辛」「巳」のほか、「D」「F」「G」「H」「J」「S」「W」の計十四種があり、かつ独特の略語、符号などがあった。

こうした体系を整えたのは、中央大学法学部を出た藤崎栄である。藤崎ははじめ警察官となったが、独力で暗号を研究して外務省の入省試験を受けた。一次試験は首位で合格したが、従兄弟が思想問題で憲兵に連行されていたために最終選考で不合格となった。

ところが彼の論文が中野高等無線学校の創立者である高木章（第二次大戦後、衆議院議員）の目にとまった。高木は藤崎を中野高等無線学校の教師として招き、ややあって、海軍航空本部技術部長（少将）だった山本五十六に校長となってもらえるよう請願した。

藤崎が交渉の窓口となった。

高木の請願は実現しなかったが、後日、山本から藤崎に

――海軍の仕事をしろ。

という指示がきた。

これ以後、藤崎は海軍の暗号に関わるようになる。

日米開戦の前夜、日本の外務省はワシントンの駐米日本大使館に長大な通信文を送信した。対米交渉の打ち切りを告げる「対米覚書」すなわち最後通告である。

全部で十四部から成る長文であったため、外務省は細かく区切って送信した。最初のパイロット・メッセージ「九〇一号電」の送信が開始されたのは、一九四一年十二月六日午前六時三十分だった。

それは外相・東郷茂徳の名で、

「十一月二十六日決定の「対米覚書」（英文）を送る」

「長文なので分割して順次送る」

「極秘扱いである」

「手交時刻はのちに指定する」

「いつでも手交できるよう文書作成に万端の手配をせよ」

などが指示されていた。

日米覚書の最後となる第十四部が送信されたのは十二月七日午前二時、エンディング・メッセージ「九〇七号電」は同日午前三時三十分である。

その九〇七号電には

本件は七日午後一時を期し米側に（なるべく国務長官に）

貴大使より直接手交ありたし

となっていた。「七日午後一時」とは、もちろんワシントン現地時間である。

ところが日本大使館の上層部には危機感が薄かった。その結果、駐米日本大使・野村吉三郎がアメリカ国務長官コーデル・ハルに文書を手交したのは、日本軍の航空機がハワイ真珠湾を攻撃したあとだった。このため日本は騙し討ちをしたことになった。

一九四一年十二月八日にかかわるもう一つの暗号がある。連合艦隊司令長官・山本五十六が戦闘開始を命令した「ニイタカヤマノボレ一二〇八」でも、南方軍が上陸に成功したことを知らせる「ハナサクハナサク」でも、機動部隊長官・南雲忠一が発した真珠湾攻撃に成功したことを知らせる「トラトラトラ」でもない。

それは日本の大本営（陸軍参謀本部と海軍作戦本部で組織）が開戦の最終決定を関係機関や諸部隊に通知する暗号であって、のちに「風暗語」と呼ばれている。

日本政府が陸海軍と協議して一九四一年十一月十九日に取り決めた符号で、海外向けラジオ短波放送で発せられる天気予報である。

――アメリカとの開戦を決定した場合は「東の風、雨」を挿入する。

というものだった。

また英蘭仏と戦争を開始する場合には「西の風、晴」、ソビエトを攻撃する場合は「北の風、曇」と合図されることになっていた。

十二月五日、

「東の風、雨」

「西の風、晴」

のメッセージが、外地の諸部隊に向けて発せられた。

〜〜〜〜　補　注　〜〜〜〜

潜水艦　これに類する乗り物の記録は古代にもある。しかし近代的な意味での潜水艦の元祖は、ロンドンに住んでいたオランダ人の船大工であるコーネリウス・ドレベルが考案した。グリースを塗った皮で木造船を包み、十二人の乗員が船体から突き出したオールを漕いでテムズ川を潜水したまま数　マイルさかのぼることができた。二〇〇三年に民間団体が復元しその事実を確認した。

　潜水艦が戦闘に使用された最初はアメリカ南北戦争で、一七七六年南軍のデービッド・ブッシュネルが作った「タートル号」がニューヨーク沖に停泊していたイギリス戦艦「イーグル号」に機雷を仕掛けようとして失敗した。タートル号は手動のスクリュー二基で航行し、のちの潜水艦と同様、船体に装備したタンクに水を出し入れする機構を備えていた。

飛行機による世界最初の爆撃　一九一四年八月、ドイツ帝国陸軍の複葉飛行機がフランスのリュネビル上空に飛来し、操縦士が爆弾を手でつかんで二発の爆弾を投下した。日本帝国軍における空爆は同年八月、陸軍所属の五機および、海軍所属の飛行艇六機がドイツ帝国租借地だった中国山東省の青島に爆弾を投下したのが最初とされる。海軍は横須賀の海軍工廠で「若宮丸」という運送船を改造して水上機搭載設備を備え、青島近海から飛行機を発進させた。

タンク（戦車）と地雷　第一次大戦の西部戦線でドイツと英仏連合軍は長大な塹壕を築いて膠着状態に陥っていた。ここに「スペイン風邪」と呼ばれた悪性のインフルエンザが発生した。長期戦による倦怠感と病人の続出で士気が低下した。これを打破するためにイギリスが投入したのが「タンク」だった。ドイツ帝国もすぐに採用した。タンクから陣地を守るために開発されたのが地雷である。

　ドイツ帝国は対ロシアの東部戦線も展開していたため経済的に二面作戦を維持することが困難になった。そこで投入したのがマスタードガスだった。これにより近代戦争は、機械化による大量破壊、大量殺戮に変質していった。

水上機母艦　最初に実戦に使用したのはイギリスだった。ドイツ帝国軍の潜水艦が無差別攻撃を行ったことへの報復として、イギリスはドイツ空襲を思いつき、二千トンから一万トンの商船を改造して水上艇をドイツ近海に運び、数機編成で空爆した。

フューリアス　一九一六年八月進水、一七年六月に巡洋戦艦として就役した。全長二百四十メートル／最大排水量二万八千五百トン。その後、主砲を撤去して全通式発艦甲板を備えた航空母艦となった。最大四十機を搭載することができた。

アーガス　イタリアのトリノに本社を置く旅客サービス会社ロイド・サバイド社が発注した貨客船をイギリス海軍が買い取って航空母艦に仕立てた。就役は一九一八年九月だった。全長百七十二・五メートル、最大幅二十・七メートル、最大排水量一万五千七百七十五トンだった。最大二十期を搭載することができた。

空母「鳳翔」　ほうしょう：九千四百九十四トン。第二次大戦後、復員船として一九四六年八月まで就航し、一九四七年五月に日立造船で解体された。

エニグマ　ギリシア語で「謎」の意味。特許を出願し認められたのはアルトゥール・シェルビウス（Arthur Scherbius／１８７８

～1929）というドイツの数学者だった。彼の特許を用いてシフレン・マシーネン社が一九二三年に製品化し発売した。当初は秘匿情報を知られたくない証券取引きや軍事用の通信などに利用された。

マリアン・レイェフスキ　Marian Adam Rejewski／1905～1980。プロイセン王国ポズナン州（一七九三～一九一八年までドイツ領だった）で生まれたことからドイツ語を自在に操ることができた。一九二九年ポーランド軍参謀本部の暗号局でドイツ海軍の暗号研究に従事し、三二年ごろからエニグマの解読に取り組んだ。

ヘンリク・ジガルスキ　Henryk Zygalski／1908～1978。ポーランドのポズナン大学の同窓生であるマリアン・レイェフスキ、イェジ・ルジツキと共同でエニグマの解読方法と解読装置の開発に取り組んだ。のちイギリスに亡命して大学で教鞭を取った。

イェジ・ルジツキ　Jerzy Witold Różycki／1909～1942。ポーランドがナチス・ドイツとソ連に分割され事実上消滅したあともフランスに亡命してエニグマの解読に取り組んだ。

マックス・ニューマン　Maxwell Herman Alexander Newman／1897～1984。父親がユダヤ人だったためナチス・ドイツとの戦いに参加する意味から、四十五歳のとき（一九四二年）イギリス政府通信部でドイツのテレタイプ端末用暗号「Ｔｕｎｎｙ」を研究した。ここで「ヒース・ロビンソン」と名付けた暗号解読装置を開発した。

トミー・フラワーズ　Thomas Harold Flowers／1905～1998。「ヒース・ロビンソン」に真空管を適用して信頼性を高めたのが世界初のデジタル計算機「Ｃｏｌｏｓｓｕｓ」となった。

Ｃｏｌｏｓｓｕｓ　コロッサス：「ロードス島の巨像」（Colossus of Rhodes）のこと。台座を含めると高さ約五十メートルの太陽神ヘリオンの像だったという。紀元前二二六年の地震で倒壊したが、その残骸は六五四年にイスラム教徒が持ち去るまで見物客を集めていた。

計算機「Ｃｏｌｏｓｓｕｓ」　第二次大戦中に「ＭａｒｋⅠ」「ＭａｒｋⅡ」の二機種計十台が製造された。ＭａｒｋⅡが解析したナチス・ドイツの情報に基づいてノルマンディ上陸作戦が策定されたといわれる。

Ｕボート　Unterseeboot：ドイツ海軍の保有する潜水艦の総称で、第一次世界大戦のとき三百隻が建造され商船五千三百隻、戦艦十隻を撃沈させた。第二次世界対戦では千百三十一隻が建造され、商船三千隻、戦艦二隻、空母二隻を沈めた。ヨーロッパ戦線だけでなく、インド洋でイギリス連邦の商船を攻撃している。また日本にも模造艦建造のために一隻が贈呈された。ちなみに「U33」はドイツ海軍第二潜水隊群所属の潜水艦だった。

アラン・チューリング　Alan Mathison Turing／1912～1954。ロンドンで生まれ、一九三一年ケンブリッジ大学のキングス・カレッジに入学し、数学を専攻した。一九三六年から三八年まで米国プリンストン大学に留学、ここで教授をしていたフォン・ノイマンから助手として誘われたが、それを断ってケンブリッジ大学に戻った。三八年、ナチス・ドイツの暗号「フィッシュ」「エニグマ」の解析に当たり、独自の解読装置を作ることに成功した。四二年、暗号解読技術の交流のためアメリカに派遣され、帰国後、真空管を使った新たな暗号解析機「コロッサス」の開発に従事した。戦争が終わった一九四五年、イギリス国立物理学研

究所に入り、ここでイギリスの国産コンピューター開発プロジェクト「ACE」に参加、四八年にアメリカに移ってマンチェスター大学の計算機担当になった。論文「計算機構と知能」（一九五〇）は人工知能の先駆けとなった。五四年、青酸カリで自殺した。

コベントリー　Coventry：ロンドン北西約百キロにある中規模都市。第二次大戦では、聖ミッシェル教会がドイツ軍空爆の目標とされ、現在も廃墟が残されている。この町の伝説にいわく――。中世の領主リオフリクの夫人ゴダイヴァは、重税に苦しむ住民の税を軽くするよう王に願い出た。すると王は「白馬に乗り裸で町を歩いたら願いをかなえよう」といった。彼女は裸で馬に乗り町に出たが、住民は戸を下ろして見ようとしなかった。ところが一人だけこっそりとのぞき見した男がいた――それが「ピーピング・トム（のぞき見男）」の由来になったという。

映画『エニグマ』　ダグレー・スコット主演、マイケル・アプテッド監督、二〇〇一、イギリス。

紫（パープル）　ワシントンで野村―ハル会談が続けられていた一九四一年の早い時期にアメリカ情報部に知られ、「パープル」と名付けられた。このほかに九一式欧文印字機は「レッド」、三式換字機は「グリーン」などと呼ばれた。

ウィリアム・フリードマン　William Frederick Friedman／1891～1969。米陸軍シグナル・インテリジェンス・サービス（SIS）に属して暗号の解読に当たった。一般的に暗号を解読するには、多くの暗号文の中から多用される反復文を探し出し、これから暗号を解く鍵を見つけていく。しかしフリードマンはいきなり模造機を作った。このため多くの専門家は、アメリカ連邦政府は何らかの工作で日本から暗号機の設計図ないし機構に関する情報を入手したのではないか、と疑っている。そのことについて連邦政府は「国家機密」として明らかにしていない。

妻のエリザベス（Elizebeth Smith Friedman／1826～1980）も暗号解読の研究者で、彼女は中南米に潜むドイツ系反米勢力の攻撃を警戒する任に当たっていた。

二台のパープルマシン　一台は、本来はハワイのアメリカ軍基地に設置される予定だった。日米開戦直後にキンメル中将は罷免されたが、「ワシントンが十分な情報を提供していなかった」とする名誉回復の裁判で「パープルマシン」の配備が焦点となり、キンメルの主張が認められている。

フリードマンが作った「パープルマシン」は、ロンドンの北方七十キロのブレッチリーという町にあった「政府通信本部」（ブレッチリー・パーク）に設置された。スタート時は二百人程度のスタッフだったが、第二次大戦末期には補助要員も含めると一万人にのぼる人々が働いていたという。

その所在は枢軸国側には全く知られなかった。首相チャーチルが側近に「ブレッチリーは私のウルトラシークレットだ」と語ったことから、同本部で解読されたナチス・ドイツや日本の暗号通信文は「ウルトラ」と総称された。

海軍甲　カタカナ四文字のコードブックに基づき、カナ乱字で暗号化していた。まず通信文の語句をコードブックでカタカナ四文字に置き換える。その符字の下にカナ乱字を記入する。こうして生成された〔符字＋乱字〕の縦列二字を九七式和文印字機で叩くと秘匿用算用数字がタイプされる。海軍甲暗号は通信量が大きくなるため、帝国海軍では大本営海軍部発の作戦命令などに限定して使用した。

対米覚書　当初、最後通告の発信開始時刻は「六日午前二時」となっていた。それが四時間半も遅れたのは、通信文を暗号化するのに手間取ったためだった。

日本IT書紀　059 新兵器

著　者：佃 均

発行者：（特非）オープンソースソフトウェア協会
http://www.ossaj.org/
info@ossaj.org

発行日：2023年4月10日