誰かに教えたくなる科学技術の話　62

歴史の裏側で暗躍した「暗号」

東京大学名誉教授　月尾　嘉男

暗号には数千年間の歴史があるが、共和政ローマの末期に活躍したG・カエサルは文書の伝達に暗号を使用していたことで有名である。それはAをDに、Bを Eにというように三字ずらして記述する単純な仕組みで換字暗号と名付けられている。現在ではコンピュータの発達などによって容易には解読できない複雑な暗号が使用されているが、今回は歴史に登場した有名な暗号事件を紹介する。

暗号筒抜けで処刑されたメアリー女王

イギリスの正式名称はグレートブリテン・アンド・ノーザンアイルランド連合王国で、さらにグレートブリテンはイングランド、ウェールズ、スコットランドにより構成されている。これらは十八世紀初頭までは独立した王国であった。そのスコットランド王国に一五四二年に誕生し、父王ジェームズ五世が急逝したため生後六日でスコットランド女王に即位したのがメアリー一世である（図1）。

一五四七年にイングランド王国から攻撃されたため、翌年、アンリ二世の統治するヴァロア王朝時代のフランスに逃避し、五八年にアンリ二世の子供フランソワ王子と結婚したが、翌年にアンリ二世が、さらに翌年、後継の国王となっていたフランソワ二世も死亡し、メアリーは母国に帰国した。様々な事情からメアリーはしばらく再婚できなかったが、六五年に従弟のダーンリー卿と再婚した。

当初は良好であったダーンリー卿との関係は急速に冷却し、一五六七年にダーンリー卿が暗殺された。この黒幕とされたメアリーは廃位となって軟禁状態となる。しかしメアリーは自身がイングランド王国の正当な王位継承権者であると主張、イングランド女王のエリザベス一世を廃位にする陰謀を企画する。この軟禁状態から外部との連絡に「ノーメンクラター」という暗号が使用された。

図1 メアリー1世（1542-87）

これは文字だけではなく頻出する単語も記号に置換する暗号であるが、エリザベス一世の臣下F・ウォルシンガムの配下に暗号解読が得意なT・フェリペスという人間がおり、メアリーの秘密の手紙の内容は筒抜けであった。エリザベス一世は血縁関係にあるメアリーの死刑は回避したかったが、証拠が次々と露見したため関係する全員を処刑し、一五八七年二月八日にメアリーも処刑した。

古代エジプトを解明した暗号

秘密文書の解読とは相違するが、古代エジプトの遺跡に彫刻されていた**ヒエログリフ**という文字の解読の経緯も暗号解読に匹敵する興味ある物語である。紀元前四〇〇〇年頃からの遺跡にはヒエラティック、デモティック、ヒエログリフという三種の文字が刻字されていた。とりわけ生物などを象形したヒエログリフは十六世紀から何人かの学者が挑戦したが解読できなかった。

ところが十八世紀の最後になって、偶然、解読の手懸りが発見された。エジプトを経由して植民地であるインドと連絡していたイギリスを牽制するため、ナポレオンは一七九八年からエジプトへの攻撃を開始、軍隊はアレキサンドリアに上陸してカイロに進軍した。その途上のロゼッタに要塞を建造するため、遺跡の石材を使用していたが、奇妙な石碑が発見された。

縦一一四センチメートル、横七二センチメートル、重量七六〇キログラムの石碑で、表面にヒエログリフ、デモティック、ギリシャ文字という三種の文字が刻字され、「**ロゼッタストーン**」と名付けられた（図2）。三種の文字は同一の内容を記録していると推定され、ギリシャ文字は簡単に解読できたので、二種の古代文字も解読できると期待され、何人かの学者が挑戦したが、予想以上に難航した。

図2 ロゼッタストーン

そこに登場したのが十以上の言語を習得し、中東の言葉にも精通していたフランスの語学の天才**J＝F・シャンポリオン**である。最初の手懸りとしたのはプトレマイオスやクレオパトラなど国王の名前で、幸運にもヒエログリフは表音文字であったため、ヒエログリフとアルファベットを対応させることに成功し、以後、エジプト各地の史跡にある碑文が解読できるようになった。

難攻不落の暗号を解読した天才

暗号が必須の技術とされるのは戦争である。近代の戦争で使用された暗号装置で難攻不落とされたのはナチスドイツが使用した「**エニグマ**」である。一九一八年にドイツの技師が発明したが、高価なこともありドイツの軍隊は見向きもしなかった。しかし第一次世界大戦中にドイツが使用していた暗号の大半が解読されていたことが判明し、戦後になって新型装置は軍隊に採用された。

タイプライターのような外観で、キーボードで文字を打鍵すると内部の歯車（スクランブラー）が作動して暗号に変換したアルファベットが点灯する。その暗号を受信したら、同一の歯車を内蔵し

ている装置のキーボードで一文字一文字入力していくと、平文に変換された文字が点灯する（図3）。一九三〇年代からイギリス、フランス、アメリカが解読に挑戦したが成功しなかった。

そこでイギリスはロンドンの七〇キロメートル北西のブレッチリーにイギリス情報局秘密情報部の暗号解読センターを開設し、多数の学者がエニグマの解読作業に従事した。最大に能力を発揮したのが数学の天才**A・チューリング**で、ドイツの軍部がエニグマを使用して発信する情報を解読する機械を発明した。これはイギリスが世界最初のコンピュータを開発する契機にもなっている。

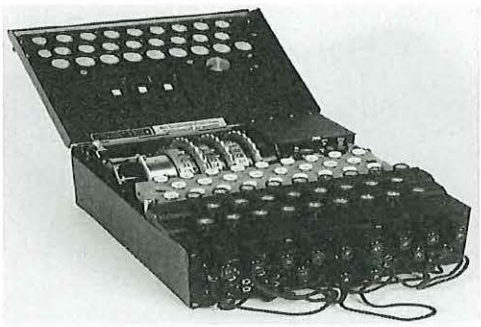

図3 エニグマ（Enigma）

当然、イギリスはエニグマの解読に成功したことは極秘にしていたため、ドイツの軍部は終戦までエニグマを使用していたし、さらに戦後はインドなどイギリスの旧植民地に装置を提供して利用を推奨し、それらの国々の秘密通信を傍受して解読していた。解読したことを公表したのは一九七四年であり、三十年近く隠蔽してきたことになる。諜報世界の現実を彷彿させる策略である。

第二次世界大戦を左右した暗号

日本が皇紀二五九七（一九三七）年に開発した外務省用の暗号機械「**九七式欧文印字機**」は三九年から使用が開始された。それに気付いたアメリカは「**パープル暗号**」という名前で解読を開始し、四一年初めには解読に成功した（図4）。アメリカは四一年十二月八日のパールハーバー攻撃は宣戦布告文書手交以前の卑劣な攻撃と日本を非難したが、実際は暗号解読により承知していた。

ドイツは日本の大島駐独大使から野村駐米大使への暗号電文がアメリカに解読されていると警告した。その背景にはベルリンのアメリカ大使館員がドイツのソビエト侵攻計画の詳細な情報を本国に送信していた事実がある。ドイツにとっては重大事件であり、情報の出所を精査した結果、日本の暗号が解読されていることが推定され、前述のような警告になったのである。

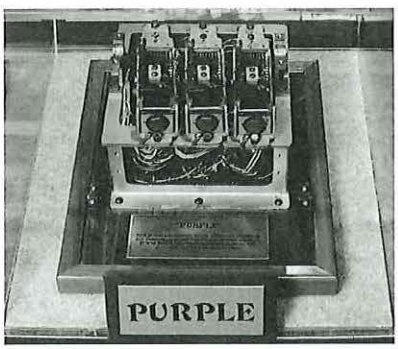

図4 パープル暗号装置の一部

しかし、その警告への対応は十分ではなく、大島大使が東京に送信した電文の大半はアメリカに解読されていた。これはドイツにとっても迷惑なことで、大使が日本に送信したドイツの機密情報をアメリカは解読してドイツへの作戦に利用

していた。一例として一九四三年に解読された電文にはフランス戦線の視察報告があり、その情報は連合国側のノルマンディ上陸作戦に貢献している。

日本の暗号通信の不備は数多くの悲劇の原因になっている。一九四三年四月十八日、山本五十六連合艦隊司令長官はラバウル基地から飛行機で出発したが、搭乗機はソロモン諸島ブーゲンビル上空で待機していたアメリカの戦闘機に撃墜され長官は死亡した。これは日本の戦局の転機になったが、日本の暗号通信がアメリカに完全に解読されており、長官の移動日程も筒抜けであった悲劇である。

暗号になった方言

暗号というと高度な理論と複雑な装置が連想されるが、意外な暗号を紹介したい。北米大陸には現在でも六百近い先住民族が存在しており、その一族**ナヴァホ**は約一〇〇万人が生活している。その使用言語は文法も発音も複雑で、外部の人間で理解できるのは三十名弱の言語学者だけであった。そこで太平洋戦争中にアメリカはナヴァホ族出身者を暗号要員として徴兵した（図5）。

ナヴァホの言語には近代戦争の軍事用語に対応する言葉は存在しないので、それらを補充した暗号を作成し、それを使用して平文で通信することにした。ナヴァホの言葉の話者であっても、暗号にされた言葉の意味は承知していないので暗号が突破されることはなかった、実際にナヴァホ出身のアメリカ陸軍軍曹が日本の捕虜になったが、秘密が漏洩することはなかった。

図5 ナヴァホ部族の暗号隊員

太平洋戦争中に日本でも方言が暗号通信として使用されたことがある。すでに開戦していた一九四三年にドイツから日本に二隻のUボート（潜水艦）が無償譲渡されることになり、ドイツに滞在していた野村直邦中将も乗艦して日本に帰国することになった。暗号電文は盗聴解読される危険があり、登場した作戦が国際電話で**鹿児島弁**を使用して通話するという大胆な手段であった。

そこで鹿児島県出身のドイツ大使館員と日本の外務省職員が選抜され「ノムラノオヤジャ／ハヨタタセニャイカンガナ／モ　タッタケナ」「ノムラノオヤジャ／モ　イッキタツモス」「モグイヤッタドカイ」「モグリャッタ」という通話が実施された。この通話を傍受したアメリカ軍情報局は特殊な暗号と誤解したため、解読できたのは二ヶ月後であり、方言は見事に暗号として役立った。

今回紹介した五例からも理解できるように、暗号は個人、組織、国家の命運を左右する技術である。したがって暗号には最新の科学技術が投入され、現在では量子科学を応用した暗号が開発の先端にある。同時に暗号の弱点は使用する人間にあることも歴史の教訓である。暗号という言葉には薄暗い印象があるが、個人から国家までの安全を維持する技術であることを認識することが重要である。