ナチスの暗号「エニグマ」はなぜ解読困難だったか

Bundesarchiv, Bild 1011-241-2173-09
Foto: Grupp | 1943/1944

史上最強の暗号機「エニグマ」

エニグマは、1918 年代にドイツで発明され、その後ナチス・ドイツに採用された暗号装置。

その解読の困難さは、多くの敵国の暗号解読者を悩ませました。

絶対の自信を持ってナチスは大戦中、エニグマで暗号化した機密文書を送受信していましたが、**実は連合軍はエニグマの解読に成功**しており、

このことが第二次世界大戦の終結を早める1つの要員になったと言われています。

このエントリーでは、なぜエニグマがそこまで解読困難だったかと、エニグマの解読に成功し連合国の勝利に貢献した男たちを紹介します。

エニグマ暗号の特徴

Bundesarchiv, Bild 146-2006-0188
Foto: Lücke | 16. August 1941

強みは「日鍵」

エニグマ暗号の強みは、**当日しか使えない「日鍵」を使うこと**にありました。
オペレータは、月に一度毎月の日鍵のコードブックを受け取り、それに基づき毎日機械の設定を調整することで暗号の配列や規則性を変えていました。
例えば、ある日のコードブックには以下のように指定されます。

1. プラグボード設定　A / L-P / R-T / D - B / W-K / F-O / Y
2. スクランブラー配置　2-3-1
3. スクランブラー位置　Q-C-W

暗号オペレーターの作業

当日オペレータは作業を始める前に、コードブックに従い機械を調整します。

プラグボードというのは、ケーブルを繋いで2文字を交換するものです。例えば上記だと、L の穴と P の穴の間にケーブルを通すことで、**L を打つと P を出力**することができます。

スクランブラーというのは機械内部の歯車のことで、それぞれの歯車にアルファベットが設定されています。

上記だと、第二のスロットに一番目の歯車、第三のスロットに二番目の歯車、第一のスロットに三番目をセット。

そしてスロット1の上部に Q、スロット2の上部に C、スロット3の上部に W が来るように位置を調整します。

そのことで、**打った文章が全く異なる文字列となって出力**されてきます。

そうして暗号化された出力を書き取り、無線オペレータに渡し各地に送信してもらいます。

受信したオペレータは、コードブックの設定に基づき暗号を機械に打ち込むと、元の文章が出力される、という仕組みです。

確率的に、日鍵のパターン数は1京（100,000,000,000,000,000）にもなりました。

さらなる暗号強化策

エニグマの弱点

最大の弱点は、**「1日に大量に暗号が送信される」**ことでした。

第二次世界大戦になると情報送信量も膨大になっていたので、大量の命令・指令・確認が無線で飛んでくるのですが、暗号の量が多いと、その分**パターンのサンプルを多く提供すること**にもなり、いくら毎日変えているとはいえ、その大量のサンプルから法則を見抜かれてしまうことは大いにありえる、とナチスは考えました。

メッセージ鍵の活用

ナチスは新たに**「メッセージ鍵」を使い、「日鍵」はメッセージ鍵を送信するだけに使う**ことにしました。

どういうことかと言うと、暗号文の前に「メッセージ鍵」を入れ、それを日鍵に通し、そのメッセージ鍵を暗号復元に用いることでセキュリティ度を上げようとしました。

具体的に説明します。

例えば、その日の**スクランブラーの位置が Q-C-W** であったとします。まずオペレータはその指示通りに設定します。

次にオペレータは、**デタラメに3つのアルファベットを選びます**。仮にその日選んだのが P-G-H だったとします。

オペレータはその PGH という文字列を、日鍵を使って暗号化します。

確実に伝達するために、3つの文字列は2回打刻されました。

例えば、「PGHPGH」と打つと、「KIVBJE」のように暗号化されます。

エニグマはキーボードを打つたびに出力文字を変えることができたため、2回連続で文字を打っても異なる文字列が出力されました。

受信したオペレータは、まず**日鍵を用いて PGH という文字列を解読**し、

そこで**スクランブラーを P-G-H に設定しなおし解読すると、正常な文章が出てくる**、というワケです。

人によるランダムな文字列が混入しているし、一見解読するのは困難に思えます。

ポーランド人　マリヤン・レイフェスキ

天才レイフェスキの貢献

この解読困難な暗号を解読したのは、ポーランドの暗号解読班「ビュロ・シフロフ」に所属する、若き天才暗号解読者・レイフェスキでした。

レイフェスキは、**メッセージ鍵が2回反復されていることに注目**。

大量の暗号文を元にして文字と文字のつながりの法則を見つけ出し、1京通りある暗号パターンを 105,456 通りにまで削減することに成功します。

それから、105,456 通りの暗号文をパターン化して一覧表を作成。

その一覧表をデータベースにして、**スクランブラーの設定 17,576 通りを総当たりにチェックする装置を作成**。

これによって、その日のプラグボードの設定が分かれば、当日の暗号は全て解読できるようになったのです。

ポーランドの限界

1938 年、ドイツは暗号の安全性をさらに強化。

これまで3つだったスクランブラーが一気に10に増加。

スクランブラーがいくら増えようと、レイフェスキの理論を使えば理論的には解読できますが、物理的な限界がありました。

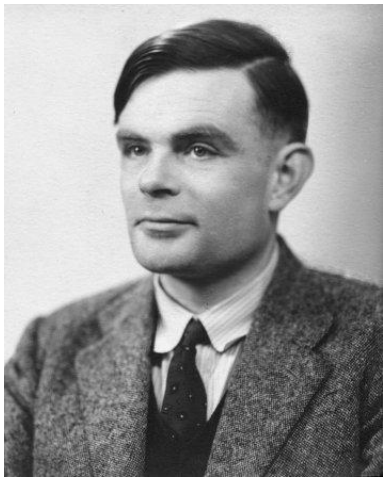
ポーランドの貧弱な解読装置ではスペック的に処理が難しかったのです。

そこでポーランドは思い切って、連合国であるイギリスとフランスの暗号解読機関に、これまでの成果と処理機械を公開することにします。

この成果を目の当たりにし、**イギリスとフランスの暗号解読班の職員は驚愕した**と言います。

自分たちがどれだけ苦労しても解けなかった暗号を、ヨーロッパの二流と侮っていたポーランドが解読に成功していたとは！

イギリス人　アラン・チューリング



鳴かないガチョウたち

もともとイギリスでは地味に暗号解読の研究が行われていましたが、**レイフェスキのメソッドが手に入ってから活気づき**始めます。

ポーランドに倣って大量の数学者・科学者を雇い、バッキンガムシャーのブレッチレー・パークでエニグマの研究を本格化させます。

ブレッチレー・パークは後に目覚ましい成果を上げていくのですが、ここで働いていた人物は、一癖も二癖もある人物ばかり。

全英チェスチャンピオン、古典学者、美術オタク、焼き物の名人、クロスワードマニア、トランプの名人などなど。

パークを訪れた英首相チャーチルは、その軍属とは思えない異様な雰囲気に驚きますが、大いに気に入り**「金の卵を生む鳴かないガチョウたち」**と呼びました。

コンピューターの基礎概念を作った天才

「万能チューリング・マシン」で有名なイギリスの数学者、アラン・チューリングもブレッチレー・パークで活躍した1人です。

チューリングは 26 歳の時に「テープ」を「出力機械」に通すことで**論理的に回答可能な問題ならどんな問題にも答えられる「万能チューリング・マシン」の概念**を発表。

現代のコンピューターの系譜を辿ると、この万能チューリング・マシンに行き着きます。

この論文は世界の数学者たちに賞賛され、チューリングはケンブリッジ大学で昇進。

ところが 1939 年に突然イギリス政府に招聘され、ブレッチレーの暗号解読者として働くことになります。

メッセージ鍵が無くなっても解読できる方法

レイフェスキの暗号解読方法は、「2回繰り返されたメッセージ鍵」がベースになっていました。

チューリングは

「いつかはドイツ軍も反復メッセージ鍵の危険性に気づくだろう」

と考え、反復メッセージ鍵に頼らない暗号解読方法を模索します。

チューリングが注目したのは**「文章の定型性」**です。

ドイツ人、しかも軍人ですから、暗号は**「定時」に「定型文」**で送られることが多くありました。

例えば、**気象情報は「毎日午前6時」に送られ、最初の文字は「wetter（天気）」という文字で始まって**いました。

そこで「wetter」と暗号解読装置に入力し、暗号が出力されるまで総当たりで調べると、その日の暗号パターンが判明する、というワケ。

実際に 1940 年 5 月 10 日にドイツ軍は、反復メッセージ鍵を中止しましたが、このチューリングによる新暗号解読方法によって、引き続き暗号を解読することができました。

まとめ

戦争は前線の将軍や兵士ばかりにスポットが当たりがちですが、兵站・輸送・諜報・解析など裏方の仕事があって初めて活きるのですよね。

派手ではありませんが、前線の兵士に負けず劣らず凄まじい戦いです。

にしても、暗号解読者ってカッコいいですね～。