若林　一平（文教大学国際学部教授）

ネットワーク時代の今を追う
<http://www.wakabayashi.com/internetroad21/>

タイムトラベル＝通底する情報文化の力
インターネットからパールハーバーへ

内部告発者キャサリン・ガン

2004年2月25日、英国の諜報機関の中枢であるGCHQ（General Communications Headquarters、政府通信本部）の内部告発者、キャサリン・ガンさん（29歳）は、情報漏洩と公務員秘密保持法違反容疑で訴えられていたのだが、検察側が証拠をいっさい提示しなかったため、彼女は無罪放免となった。

ガンさんはGCHQの元翻訳者なのだが、2002年3月の米国のイラク攻撃直前の国連安全保障理事会（安保理）における攻防の最中に、米国のスパイから英国の諜報員に対して、イラク戦争に反対する国々の国連代表の電話盗聴を依頼するeメールが出されている事実を新聞「オブザーバー」に流したのである。

法廷では冒頭、2003年1月30日から3月2日までの間、ガンさんは1989年に制定された公務員秘密保持法に反して国家安全ないし諜報活動についての情報を外部に流し続けていたという告訴状が明らかにされた。しかし、彼女が無罪を主張した後、マーク・エリソン検察官は、本件についての十分な証拠を揃えることは困難であり、よって裁判の続行は不能と宣言した。裁判長が被告人は無罪と判断したことは言うまでもない。

ガンさんは既にGCHQの職も失っていたのだが、かねがね「わたしは後悔していない、同じ立場におかれたら同じことを繰り返すだろう」と言い続けてきただけに、「ほんとうに嬉しい、これで気が晴れた」とのコメントを発表した。

訴えの取り下げにはGCHQの内部事情と政府の意向が関係しているのだろうが、ガンさんの告発で図らずもその名が表にでてしまったGCHQとは何ものか。少し、タイムトラベルに出かけてみたい。時代は30年ほどさかのぼる。

英国GCHQを内部告発したキャサリン・ガンさん
<http://www.liberty-human-rights.org.uk/> より

GCHQとインターネット

1973年、GCHQはインターネットで今日最も広く利用されている「公開鍵暗号方式」と呼ばれる暗号技術を開発していた。伝統的にはあらゆる安全な通信は送り手と受け手が同じ「鍵」を利用してきた。このやり方は「鍵」をどのようにして配布するのかという困難な問題をかかえてきたのである。「公開鍵暗号方式」は受け手のみが「非公開鍵」を持ち、送り手には広く「公開鍵」を配布する方式である。送り手は「公開鍵」で施錠してメッセージを受け手に送る。受け手は「非公開鍵」でこれを開けるのである。ビジネスをはじめとする今日のインターネットの隆盛はこの方式無しには存在し得ない。

「公開鍵暗号方式」の米国での開発の公表は1977年である。GCHQはこれに先立つこと4年前に既に開発に成功していたのである。ある意味で、表向きは「一番」でなくても構わぬという英国人の深謀遠慮がうかがえる。どうも表向きの「一番」と実質的な貢献とは大いに違っているようだ。

ここで、現在のGCHQの一端を見ておこう。まずは、ヨーロッパ最大のコンピュータユーザーの一つであり、一方では多言語の駆使にいたっては何と67カ国語だという。「太陽の沈まぬ国」は生きていたのである。多言語は当然ながら多文化に通じている。地球を理解しようとする志（こころざし）の高さはわれわれ現代日本人も学ぶべきところではない

だろうか。

GCHQの前身は第二次大戦の時代にさかのぼる。1939年、GC&CS（Government Code and Cipher School、政府暗号および暗号技術学校）はロンドン郊外ブレッチェリー・パークにあったレオン家の大邸宅を譲り受けて、当時最強と言われていたドイツの暗号「エニグマ」の解読作業を開始したのである。

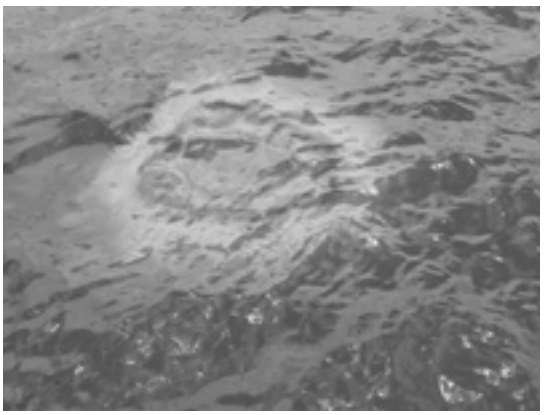
エニグマとITの父 チューリング

米国のシカゴの郊外にある「科学産業博物館」には、大西洋で米国海軍が捕獲したドイツの潜水艦Uボートの現物が展示してある。連合軍側はUボートの艦内で使用していたエニグマの暗号機械とそのマニュアルの入手に躍起になっていた。熾烈な海戦はまた熾烈な情報戦でもあったわけである。

暗号機械が手に入っても暗号がすぐに解読できるわけではない。暗号解読は、出力結果から入力内容を推測する作業に他ならない。エニグマが出力する暗号の組み合わせは百万の3乗のさらに150倍という気の遠くなるものであった。絶対に破られないと考えたドイツの自信作であった。

エニグマ暗号を破った最大の功労者は天才数学者で、奇人、変人でもあったアラン・チューリングであった。コンピュータを学ぶとき、必ずお目にかかるのがチューリング・マシンやチューリング・テストなどの言葉を通して、彼の理論家としてのコンピュータ科学への貢献が専ら強調されることである。

エニグマ暗号の解読にあたって、チューリングは解読専用の電子機械＝電子式コンピュータ「ボム」を開発し、実際に運用にあたったのである。エニグマの解読は一挙に進んだ。結果として、英国が最も恐れていたUボートの被害は急速に減少し、一方では空軍の迎撃体制も改善されたのである。それらが発展した最大の傑作は「コロサス」である。「コロサス」はヒトラーの個人専用暗号を解読し、またノルマンディ上陸作戦に貢献したのである。



日本海軍の攻撃で海底に沈んだ戦艦アリゾナの船体から漏れ出すオイルの波紋
（2004年8月、米国ハワイ州パールハーバーで筆者撮影）

情報（インテリジェンス）の世界では手の内を知られてしまったら、意味をなさない。したがって、60年を経過しても必ずしも真実はあかされない。しかし、チューリングに関して言えば、まさに「ITの父」と言っても言い過ぎではないであろう。

チューリングは英国と米国との情報戦協力のために、1942年から1943年にかけて米国に渡っている。暗号解読のための「ボム」の技術提供も実施された。既に日本の外交暗号、軍事暗号の解読を進めていた米国の情報戦対応能力にさらに磨きがかかったのである。われわれのタイムトラベルはハワイに行き着いたようである。

パープルとパールハーバー

日本の外交（官）の大失態として、太平洋戦争開戦時における米国への開戦通告が予定より遅れてしまったという大事件があった。現地ワシントン時間で、パールハーバー攻撃の日である1941年12月7日（東京は12月8日）の出来事である。このため、後々まで日本は「トレチャリ（treachery：背信行為、裏切り）」の汚名を着せられることになる。

当時外交用には九七式暗号機、通称「パープル」が使用されていた。実は米国は「パープル」の解読に成功しており、開戦にいたる日米交渉における日本の手の内はすべて丸見えだったのである。日本からの開戦通告も大統領ルーズベルトは日本の野村大使らの到着前に既に全文を読み終えていた。電報は当然ながら暗号で届いている。日本大使館員の解読作業は米国よりも遅かった。清書(タイプ)も間に合わなかった。まさかとは思うが、まともにタイプを打てる大使館員は一人しかいなかったという話もある。

要するに、情報（技術）もなければ文化（緊張）もなかった。この日の作戦の総責任者である山本五十六は参謀に対して「米国への通告は大丈夫か」と最後の最後まで繰り返し念を押していたという。早期決着を目指していた山本であるから、外交に失態があってはならないと考えたのは当然であろう。しかし、山本の不安は的中してしまった。パールハーバー攻撃は軍事的には成功したのだが、情報（および文化）戦では開戦当時、日本は既に負けていたのである。

英国の情報戦の拠点ブレッチェリー・パークには、奇人、変人が多数集められたという。もちろんチューリングもそのひとりである。彼らが見せつけたのは文化の持つ底力である。文化を忘れて技術無し。肝に銘ずべし。

（わかばやし・いっぺい）

関　連　情　報

●ドイツのエニグマ解読の歴史をもつ英国のGCHQ
<http://www.gchq.gov.uk/>

●日本のパープルを解読していた米国のNSA
<http://www.nsa.gov/>

● パールハーバーのアリゾナ追悼博物館
<http://www.arizonamemorial.org/>