

警察政策学会資料 第127号  
令和4（2022）年11月

**「クリプト社」と NSA**  
**～世紀の暗号攻略大作戦～**  
**（改訂版）**

**警察政策学会**  
**テロ・安保問題研究部会**

# 「クリプト社」と NSA ～世紀の暗号攻略大作戦～（改訂版）

“The intelligence coup of the century”

元日本大学危機管理学部教授 茂田忠良

## <目次>

初めに .....	2
第1章 「クリプト社作戦」全体像判明の経緯 .....	2
第2章 クリプト社と米国の協力の経緯 .....	5
第3章 クリプト社の協力による情報成果 .....	11
第4章 困った情報成果の副産物 .....	13
第5章 「クリプト社作戦」の終了 .....	14
第6章 教訓：インテリジェンスの実態と論理 .....	17
第7章 補足：その他諸国諜報機関の関与 .....	22

## 「改訂版の発行について」

本論考の初版は、2020年11月に発行した警察政策学会資料第113号所収の論考である。初版執筆後、米国とドイツの他に、更にスウェーデン、フランス、スイスなどの他の欧州諸国の関与を明らかにする資料が入手できたので、今回、改訂版を発行することとした。改訂部分は、新たに第7章を起こして、これら諸国の関与状況について加筆した。また、既述部分についても新資料に基づき若干の加筆補正を施した。

## 初めに

「クリプト社」は、世界的な暗号機メーカーであるが、その暗号機メーカーは 60 年以上にわたり秘密裡に米国シグント機関・国家安全保障庁 NSA (National Security Agency) など米国インテリジェンスと協力関係にあった。この協力関係についてはこれまで何度も断片的な疑惑報道や研究がなされてきたのであるが、2020 年に至り遂に協力関係の全体像が明らかになった。

この協力関係は、20 世紀における「世紀の暗号攻略大作戦」と呼べるものであり、また、最近注目を集めている「供給網工作」(supply chain operation) の典型でもあった。

以下、その協力関係の判明の経緯を見たのちに、クリプト社と米国インテリジェンスの協力の全体像(即ち、協力の経緯、協力の成果、協力関係の終了)を概観し、最後にインテリジェンスの世界においてこの協力関係が持つ意味、そこから読み取れるインテリジェンス世界の実態と論理について考察する<sup>1</sup>。

更に、第 7 章補足として、スウェーデン、フランスなどの欧州諸国の関与も記述した。

米国インテリジェンスによるクリプト社から協力を得る作戦を、本稿では「クリプト社作戦」と記述する。

## 第 1 章 「クリプト社作戦」全体像判明の経緯

### 1 「クリプト社」とは如何なる企業か？

#### (1) 世界的な暗号機メーカー「クリプト社」

クリプト社は、もともと 1920 年代にスウェーデンにあった暗号機メーカーであるが、第二次世界後の 1952 年スイスに移転し、スイスを拠点として活躍した世界的な暗号機メーカーである。

そもそも、秘匿強度の高い暗号機を自力で製作するのは、それ程容易なことではなかった。そのため、第二次世界大戦後、多くの国々が外交通信や軍事通信に欧州民間企業の販売する製品を使ってきた。その中でも、クリプト社の製品は「性能」が良く且つ会社が「中立国」スイスに所在することもあり、最も普及した製品であった。

その暗号機は、20 世紀後半から 21 世紀にかけて実に世界の 120 ヶ国以上で使用され、世界の(共産圏を除く)民間暗号機市場の 70~80%を占有していたと言われる。採用国は、アジア、中近東、アフリカ、中南米など多くの国々に及び、イラン、リビア、エジプト、ジョルダン、シリア、アルゼンチン、アイルランドも含まれていた。但し、ソ連及びその衛星国、中国、北朝鮮は、中立国といえども西側の国であるスイス企業の暗号機は決して使わなかった。

---

<sup>1</sup> 本稿の大幅な要約版は「クリプト社作戦」として、『治安フォーラム』令和 2 年 11 月号(2020 年 11 月 5 日、立花書房)に掲載している。

## (2) クリプト社と米国の秘密の協力関係 (1950年代～2018年)

このクリプト社は、実は 1950 年代から 2018 年に至るまで、秘密裡に米国に協力しており、クリプト社の販売する暗号機について、米国による暗号解読に協力してきたのである。

この間、クリプト社は、米国国家安全保障庁 NSA や独連邦情報局 BND と密接な関係を持ち、また、米モトローラ社や独シーメンス社とも協力関係を築いていた。特に米国とは、第二次世界大戦中から関係を持っていたが、戦後、更に継続して密接な関係を保ってきた。即ち、NSA の支援を受け、且つ NSA による暗号解読が容易になるように協力していたのである。従って、このクリプト社の暗号機を採用してきた国々の外交・軍事通信は、一部の例外を除いて、全て米国 NSA によって解読可能であった。

## 2 米国との協力関係全体像の判明の経緯

### (1) 従来 of 疑惑報道

クリプト社と米 (独) 諜報機関の協力関係についての出版や報道は度々なされてきた。特に、1993 年と 1994 年元社員ハンス・ビューラーによる告発、1995 年米『ボルチモア・サン』紙による根拠を示した調査報道があった。

しかし、その度に、クリプト社幹部は断固とした否定会見などを行い、疑惑は有耶無耶にされてきた。また疑惑報道による顧客の流出も一部に止まった。

### (2) 2014 年ウィリアム・フリードマン関係文書の開示<sup>2</sup>

ウィリアム・フリードマンは、米国「暗号解読の父」とも呼ばれ、第二次世界大戦前から陸軍の暗号解読の中心人物であり、また、戦後の国家シグント機関 NSA の暗号解読の第一人者でもあった。2014 年にフリードマン関係文書の多くが (一部黒塗りながら) 開示され、これによってフリードマンとクリプト社の実質的な創業者ボリス・ハーゲリンとの親密な交流が浮き彫りになった。そして、1950 年代に NSA とクリプト社との間に一定の協力関係があったことが明白となった<sup>3</sup>。

但し、開示されたフリードマン文書から明確なことは、1950 年代にクリプト社が新型の暗号機を NSA に販売したこと、高度な最新式暗号機の販売先の限定に合意したことなどであり、それに加えて、米国による暗号解読に積極的に協力したか否か、また、1960 年代以降も

---

<sup>2</sup> フリードマン開示文書は、現在 NSA, *William F. Friedman Collection of Official Paper*, <https://www.nsa.gov/News-Features/Declassified-Documents/Friedman-Documents/> でアクセス可能。

フリードマン開示文書の内、クリプト社関係の主要文書は次のウェブサイトにもまとめられている。National Security Archive, *Hagelin and Friedman: The Gentlemen's Understanding Behind "The Intelligence Coup of the Century,"* accessed 3 March 2020, <https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-02-19/hagelin-friedman-gentlemens-understanding-behind-intelligence-coup-century>.

<sup>3</sup> フリードマン開示文書については次の分析がある。特に前者の分析は詳細である。

--"The gentleman's agreement," *Crypto Museum*, last updated February 2020, accessed 3 March 2020, <https://www.cryptomuseum.com/manuf/crypto/friedman.htm>

--Gordon Corera, "How NSA and GCHQ spied on the Cold War world," *BBC*, 28 July 2015, accessed 6 May 2016, <http://www.bbc.com/news/uk-33676028>

協力関係が継続したか否かについては、明確でなかった。開示されたフリードマン文書からは、協力関係はフリードマンとハーゲリンの個人的関係に基づくもので、その後は中断したようにも解釈できたからである。

### (3) 2020年2月 WP 報道・独 ZDF 報道

ところが、2020年2月11日『ワシントン・ポスト』紙とドイツの公共放送 ZDF は共同調査に基づく報道を行い、これによって、米国とクリプト社の協力関係のほぼ全体像が判明したのである。

『ワシントン・ポスト』紙の報道（国家安全保障担当グレッグ・ミラー記者）<sup>4</sup>とドイツ公共放送 ZDF の報道<sup>5</sup>によれば、両者は、「クリプト社作戦」の経緯に関する米国中央諜報庁 CIA 秘密文書と独連邦諜報庁 BND 口述記録を入手し、これを調査分析した。

CIA 秘密文書は、CIA のインテリジェンス研究センターが 2004 年作成した「MINERVA<sup>6</sup>-A HISTORY」と称する「クリプト社作戦」の包括資料（96 頁）であり、BND 口述記録（オーラル・ヒストリー）は、BND の複数の職員が 2008 年に作成した記録であるとされる<sup>7</sup>。

同調査報道（以下「WP 報道」「ZDF 報道」と呼ぶ）は、これら秘密文書の分析と付随調査<sup>8</sup>に基づくもので、その内容は従来の疑惑報道やフリードマン文書と斉合性を有しており、信憑性は極めて高いと評価できる。

なお、WP 報道は CIA 文書提供者の意思であるとして CIA 文書全体は開示していないが、同文書から 22 箇所を抜粋しており、その記述（以下「CIA 文書抜粋」<sup>9</sup>と呼ぶ）も情報価値の高い資料である。

## 3 クリプト社と米国諜報機関の協力関係を見る意味

CIA 文書抜粋によれば、「クリプト社作戦」は、「世紀の諜報成功事例である (the intelligence coup of the century)」「外国政府は米国と西独両国に費用を払った上で、少なくとも 2 カ国

<sup>4</sup> Greg Miller, “The intelligence coup of the century,” *Washington Post*, 11 February 2020, accessed 14 February 2020, <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>. 以下、「WP 報道」と呼ぶ。

次の豪州ラジオ局によるインタビューも興味深い。Greg Miller, interview by Phillip Adams, *ABC Late Night Live*, 17 February 2020, accessed 3 March 2020, <https://www.abc.net.au/radionational/programs/latenightlive/intelligence-coup-of-the-century:-the-cias-private-spying-busi/11972630>

<sup>5</sup> “Operation Rubicon: How BND and CIA eavesdrop on the world,” by Eomar Thevessen, Peter Mueller and Ulrich Stoll, aired 11 February 2020, on ZDF, accessed 5 March 2020, <https://www.zdf.de/politik/frontal-21/operation-rubikon-100.html>. 本放送の内容は、次の記事に記載されている。Eomar Thevessen, Peter Mueller and Ulrich Stoll, “#Cryptoleaks: How BND and CIA Deceived Everyone,” *ZDF*, 11 February 2020, accessed 5 March 2020, <https://www.zdf.de/nachrichten/politik/cryptoleaks-bnd-cia-operation-rubikon-100.html>. 以下、「ZDF 報道」と呼ぶ。

<sup>6</sup> MINERVA とは、クリプト社に付されたコード名である。

<sup>7</sup> クリプト社と関係を持った米側インテリジェンスは、NSA と CIA 両機関である。今回の報道は、CIA 側資料のみによっており、NSA 側資料がないので、完全解明とまでは言えないが、ほぼ全体像が判明したとは言える。

<sup>8</sup> 付随調査には、現職や元職の諜報機関員やクリプト社社員のインタビューが含まれるが、事案が機微な内容であるため、多くは匿名を条件として応じたということである。

<sup>9</sup> 「CIA 文書抜粋」の内容は、全て脚註 4 の WP 紙記事に添付されている。

(多ければ5又は6ヵ国)の外国政府に機密通信を読ませる特権を付与していたのである」<sup>10</sup>。

このような、米国(及びドイツ)インテリジェンスの大成功事例を研究することは、それ自体が意味あることであるが、それと同時に、それを通じて、インテリジェンスの本質、その実態と論理について、また「供給網工作」(supply chain operation)など現下の課題について、理解を深めることができる。

以下、WP報道、CIA文書抜粋、ZDF報道、フリードマン文書、その他の現在までの開示資料や報道を基にして、本作戦について見ていくこととする。

## 第2章 クリプト社と米国の協力の経緯

### 1 クリプト社創設者ボリス・ハーゲリンの生立ち

CIA文書抜粋によれば、ボリス・ハーゲリンは、1892年にロシアの石油生産地として有名なアゼルバイジャン・バクー市近郊で、スウェーデン人実業家の家に生まれた。父親カールは有名なノーベル家の友人で、当時欧州最大の石油会社ノーベル兄弟社のバクー油田の経営を任されていた。ハーゲリンは、幼少期をロシアで過ごした後、大学教育を母国で受けるため帰国、スウェーデン王立工科大学で機械工学を専攻し1914年に卒業した。やがて父親の役割を引き継ぐ前提で、経営修行のためにストックホルムの総合電機企業に勤務していたが、ロシア革命が勃発したためロシアへの帰還が出来なくなった。

ボリス・ハーゲリンは、その後スウェーデンや一時米国で働いていたが、暗号機会社(スウェーデンのクリプト社。ハーゲリン家が以前から出資していた。)を1925年頃から経営するようになった。

### 2 M-209暗号機の開発と米国陸軍の採用：フリードマンとの友情

CIA文書抜粋によれば、ボリス・ハーゲリンは1930年代にC-36という機械式暗号機を開発した。これは電力不要で軽量可搬型であり、秘匿強度は必ずしも高くはなく時間をかければ解読可能であったが、戦場での使用には最適の暗号機であった<sup>11</sup>。ハーゲリンは、この暗号機の売込のため、米国を1937年と1939年の二度に亘り訪問したが、その際に、米国「暗号解読の父」ウィリアム・フリードマンの知遇を得て友人となった。(フリードマンはロシア生れで幼少期に米国に移住したユダヤ人である。暗号研究者であり、1920年代以降米陸軍の暗号責任者であった。)

WP報道によれば、1940年にドイツがノルウェーを占領すると、ハーゲリンは米国に亡命

<sup>10</sup> WP報道は、「クリプト社作戦」について、当事者である米独2ヵ国の他、少なくとも英国、スウェーデン、スイス、イスラエルはその存在を知っていたか、情報成果の分け前に預かっていたとしている。第7章で補足するように、実際はそれ以上の国々が情報成果を享受していたのである。

<sup>11</sup> 戦術通信用の暗号機としては、秘匿強度よりも、戦場での使用のため電力不要で軽量可搬型であることが重要であった。戦術通信では、仮に一定時間後に解読されたとしても、既に通信内容は情報的に無価値となっている場合が多いからである。

したが、暗号機 C-36 を改良して米軍の戦術通信用暗号機 M-209 を開発した。M-209 は米陸軍が採用するところとなり、大戦中 14 万台も生産された。ハーグリンは、特許料で 860 万ドルを得たという<sup>12</sup>。このためハーグリンは米国に恩義を感じることとなった。

### 3 ハーグリンとフリードマンの（不文の）紳士協定時代（1950 年代）

ハーグリンは大戦後、クリプト社をスイスに移転し、暗号機の開発を続けた。WP 報道によれば、ハーグリンは 1951 年には CX-52 という新製品を製造したが、これは従来の暗号機と比べて秘匿強度が高く、当時の米国シグント機関・軍安全保障庁 AFSA (NSA の前身組織) でさえ解読が困難なものであった。本製品が世界に幅広く販売されると、米国としては世界各国の情報収集に支障を来すことになる。

そこで CIA 文書抜粋によれば、ハーグリンが 1951 年に米国を訪問した際、フリードマンはハーグリンと会食をした。その際フリードマンは、クリプト社の最新の暗号機の販売対象国を制限するように申し入れ、ハーグリンは交渉に応じる意向を表明した。

フリードマン文書（1955 年の出張報告書<sup>13</sup>）によれば、その後 1954 年 1 月にフリードマンとハーグリンは協力関係に関する紳士了解（gentlemen's understanding）に至った。

その了解を基に、米国諜報コミュニティでは協力関係について検討が進められてきたが、米国コミント委員会（当時）は 1954 年 12 月漸く正式提案<sup>14</sup>を決定した（提案内容には英国のロンドン・シグント委員会も同意している）。

フリードマンはその提案を持って 1955 年 2 月にクリプト社を訪問。ハーグリンは米国の正式提案に即座に同意し紳士協定が成立した。合意内容そのものは現在でも不開示であるが、フリードマン出張報告の開示部分から分かるのは、クリプト社が、次の方法によって NSA による暗号解読が容易になるように協力していることである。

- ・ （開発中を含む）暗号機やその技術情報の提供
- ・ 暗号機の世界各国への販売状況についての情報提供
- ・ 最新式暗号機の販売時期の調整（必要に応じて販売延期）
- ・ 特定国への販売は（解読容易な）旧式暗号機に限定

これに対して、NSA はハーグリン一族に対して多くの便宜を図ってきた。ハーグリンは、NSA の働き掛けにより娘婿コンラディの米空軍での継続勤務が可能になったことや NSA が妻の従妹バースを採用してくれたことについて、感謝を述べている。他方、ハーグリンは NSA に対する協力に関して、特別に何かをする（例えば、積極的に暗号機に弱点を挿入する）訳ではないとして、金銭報酬の受領には拒否感を示していた。ハーグリンの NSA への協力の

<sup>12</sup> ハーグリンは、暗号機で百万長者になった世界初の事業家とされる。

<sup>13</sup> 2014 年 NSA 開示資料、William F. Friedman, *Report of Visit to Crypto A. G. (Adapted Final Draft)*, 28 March 1955, accessed 31 August 2015, <https://cryptome.org/2015/07/nsa-crypto-ag.pdf>.

--2014 年 NSA 開示資料、William F. Friedman, *Report of Visit to Crypto A. G. (Final Draft)*, 28 March 1955, accessed 3 March 2020,

[https://www.cryptomuseum.com/manuf/crypto/files/19550328\\_VisitToCryptoAG.pdf](https://www.cryptomuseum.com/manuf/crypto/files/19550328_VisitToCryptoAG.pdf)

--2014 年 NSA 開示資料、William F. Friedman, *Report of Visit to Crypto A. G. (Second Draft)*, 15 March 1955, accessed 31 August 2015, <https://cryptome.org/2015/07/nsa-crypto-ag-draft.pdf>.

<sup>14</sup> USCIB: 29.14/29 dated 27 December 1954. 内容は現在も非開示である。

動機は、米国に対する恩義・親近感とフリードマンとの友情を基礎にしたものであったと見られる<sup>15</sup>。

しかし CIA 文書を基にした WP 報道によると、1955 年の合意ではクリプト社は協力の代償として 70 万ドルの支払い<sup>16</sup>を受けることとなっていた。米国政府内の調整に手間取りなかなか支出に至らなかったが、その間も、ハーゲリンは紳士協定を守り、最新式暗号機は特定の国にしか販売しなかったとされる。ハーゲリンの拒否感の表明にも拘らず、1955 年合意には（最新式暗号機の販売機会の損失補償（逸失利益の代償）などの）何らかの名目で金銭的対価が含まれていたと見られるが、ハーゲリンは元々金銭的対価を重視していなかったので、支出が遅れても不満がなかったのであろう<sup>17</sup>。

なお、フリードマン文書（1957 年の出張報告書<sup>18</sup>）は、クリプト社が 1950 年代に、ドイツ企業シーメンス社とも取引し交流していたこと、スウェーデン政府とスイス政府の意向を汲みながら経営を行っていたことも示している。

---

<sup>15</sup> フリードマンは、1955 年や 1957 年のクリプト社訪問の際は、1 週間以上もハーゲリン家に宿泊して滞在している。ハーゲリン家との交流は家族ぐるみのものである。

<sup>16</sup> 代償としての 70 万ドルという金額は既に 1951 年の米シグント機関 AFSA 内の議論で言及されている。具体的な協力内容としては、コミント（この場合は暗号解読）面に加え、通信保全（米軍用暗号機開発への協力）面も含まれているようである。参照：2014 年 NSA 開示資料 William Friedman, *Negotiations with Mr. Hagelin*, 22 May 1951, accessed 4 March 2020, [https://www.cryptomuseum.com/manuf/crypto/files/negotiations\\_1951.pdf](https://www.cryptomuseum.com/manuf/crypto/files/negotiations_1951.pdf)

<sup>17</sup> 1950 年代の協力関係については、従来ハーゲリンは金銭的対価を得ていないという解釈が一般的であったようである。（“The gentleman’s agreement,” *Crypto Museum* 中の “The Hagelin Deal 1955” の記述を参照）。その理由は、①本文中に記載したように、フリードマンの 1955 年出張報告によれば、ハーゲリンが金銭的報酬に拒否感を示していたこと、②協力内容に関する米国コミント委員会の提案自体は今以て情報開示されていないこと、以上二つから導かれた推論であらう。

しかし、実際は金銭的対価 70 万ドル支払の約束と実行はあった判断するのが妥当である。その根拠は、①1951 年 5 月フリードマン自身がシグント機関 AFSA 内部での検討で 70 万ドルの支払いを積極的に主張していること（参照：Friedman, *Negotiations with Mr. Hagelin*, 22 May 1951）、②今回の WP 報道が、CIA 秘密文書（MINERVA-A HISTORY）に基づき（関係部分は公表していないものの）1950 年代の協力の対価として 70 万ドルが支払われたとしていること、③米国側の事情で対価の支払が遅れてもハーゲリンは不満を示さなかったという展開は、正に 1955 年フリードマン出張報告の内容と斉合性があること、以上三つである。

こうして見ると、2014 年のフリードマン関係文書の開示自体に、一つの情報作戦が含まれていたと考えることができる。即ち、1955 年フリードマン出張報告の開示により、クリプト社の協力は、①最新式暗号機の販売対象国の制限という消極的な協力に過ぎないこと、②協力は金銭的対価の伴わないハーゲリンの自発的協力であって、フリードマンとの個人的関係によるところが大きいというイメージを流布させることに成功している。つまり、クリプト社の暗号解読における対米協力は、過去のものであるという印象創出を意図したものであろう。即ち、フリードマンもハーゲリンも故人となって久しく両者の個人的関係も終了し（協力の基礎は既に消滅し）、且つ 2014 年現在で関係フリードマン文書を開示できる位に秘密保持の必要が低下した、従って 2014 年現在では協力関係は継続していないという暗黙の主張である。しかし、現実はその時点でも協力関係は存続していたのである。

<sup>18</sup> 2014 年 NSA 開示資料、William F. Friedman, *Memorandum for the Record; Hagelin Negotiations (Draft)*, 18 December 1957, accessed 3 March 2020, <https://nsarchive2.gwu.edu/dc.html?doc=6779397-National-Security-Archive-20-Draft-of-William>

#### 4 特許契約による販売制限協定時代（1960年代）

CIA 文書抜粋によれば、1950年代の協力関係は不文の紳士協定によってきたが、1960年にはそれが特許契約という形で文書化された。それによれば、クリプト社は NATO 諸国とスイス、スウェーデンには最新式の解読困難な暗号機を自由に販売できるが、他の諸国に対しては国別に販売できる暗号機の種類（即ち性能）が制限されていた。その代償に、米国はクリプト社の全ての暗号機に対して特許料を払うという取決であった。WP 報道によれば、特許料は 1970 年に一時払いで 85 万 5 千ドル、加えて、毎年、契約更新料として 7 万ドル、クリプト社の（NSA にとって解読可能な）暗号機の販売促進費用として 1 万ドルが支払われることとなった。

この段階でのクリプト社の協力は、いわゆる「拒否作戦」であり、クリプト社の（NSA が解読不能な）高度暗号機を販売しないという、NSA の暗号解読に対する消極的な協力であった。

#### 5 NSA によるクリプト社暗号機の回路設計の始まり（1967年）

1960年代半ばには電子回路が発達し、暗号機も従来の機械式暗号機から電子式暗号機への変換が迫られた。

しかし、クリプト社には必ずしも電子回路に関して十分な技術力がなかった。他方、NSA は電子式暗号機によって秘匿強度が増大し解読不能となることを危惧していた。

折しも NSA の専門家ピーター・ジェンクスは、一見無限乱数を生成しているように見えて実は有限乱数を生成するに過ぎない電子式暗号機を製造することが可能であることを発見した。勿論この有限乱数は、NSA のコンピュータで解読可能なものである。

その結果、1967年にクリプト社は最初の電子式暗号機（テレプリンター型）H-460 の販売を開始したが、その電子回路は NSA の技術者が設計したものであった。勿論、NSA にとって、電子式暗号機 H-460 であっても通信傍受と解読の手間はかかったのであるが、それまでの機械式暗号機よりも遥かに迅速に解読できるようになったという。

クリプト社の一見高性能に見える電子式暗号機に対して、諸外国政府の需要は高く売上は急増した。同時に、クリプト社は益々 NSA に依存するようになった。クリプト社では、暗号機は常に 2 種類以上製造し、1 種類は解読困難な友好国用であり、その他は解読可能な機種とした。

NSA による暗号機の回路設計の開始により、クリプト社製暗号機販売は、弱点を仕込んだ暗号機を販売するという「積極工作」の段階に入ったのである。

#### 6 米独によるクリプト社共有時代（1970年～1993年）

##### （1）米独によるクリプト社買収

WP 報道によれば、1960年代末には、ハーゲリンも 80 才近くと老齢に達し、クリプト社の事業承継を考えるようになった。他方、CIA はハーゲリンの突然死やクリプト社の売却を危惧するようになった。そこで、クリプト社の買収が検討されたが、CIA と NSA 間の調整が進まず具体的な動きにまでは進まなかった。

そうこうする内に、仏独諜報機関がハーゲリンの引退希望を察知して、クリプト社への接近を始めた。仏独と幾つかの欧州諜報機関は、同社と米諜報機関との関係について、米国から知らされ、或いは自ら探知して知っており、かねてからクリプト社と米国同様の関係を築きたいと模索していた。そこで 1967 年には、仏諜報機関が独諜報機関と共同で、ハーゲリンに同社買収を持ち掛けたが、ハーゲリンはこれを拒否して CIA に通報した。次に 1969 年初に、独 BND のシギント部門 ZfCh<sup>19</sup>責任者ヴィルヘルム・ゲーイングが、CIA に対して米仏独共同によるクリプト社買収を提案したところ、CIA はフランスを排除した米独共同による買収を逆提案し、ドイツはこれに同意した。

### (2) 米独によるクリプト社経営の構造

CIA 文書抜粋によれば、1970 年 6 月に秘密裡にクリプト社の全株式が米国政府とドイツ政府に譲渡された。同月締結された CIA と BND の覚書によれば、両組織が費用を折半して合計 2500 万スイス・フランで全株式を取得し、両者の合意の下に運営することとされたが、形式上は BND のフロント企業が所有する形を取った (WP 報道によれば、会社の登記他の文書作業にはリヒテンシュタイン公国の法律事務所 Marxer and Goop が関与して、所有者の正体隠匿に協力した)。このクリプト社の秘密共同経営作戦は、暗号名「シソーラス作戦」と命名された (1980 年代末には「ルビコン作戦」と改名。以下「ルビコン作戦」と呼ぶ)。

WP 報道によれば、クリプト社の運営について、CIA はミュンヘンに秘密事務所を設置して、独 BND と定期会合を持った。クリプト社では、取締役の内唯一人、ハーゲリンから経営を引き継いだシュトゥーレ・ニイベルグ (Sture Nyberg) のみが、米独諜報機関との関係を知っていた。また、諜報機関は、企業経営には疎いので、民間企業も巻き込んでいた。ドイツはシーメンス社を引き込み、売上の 5% の顧問料でクリプト社の営業と技術問題について助言を得るようにした。また、米国は後にモトローラ社を引き入れ、大型製品について技術支援を得るようにした。

CIA 文書抜粋によれば、クリプト社の運営に関係した組織は、政府機関では米国は CIA と NSA、ドイツは BND と傘下シギント部門 ZfCh、民間会社では独シーメンス社と米モトローラ社である。

クリプト社は、米独諜報機関と両民間大企業の支援を得て成長して、1970 年の売上高 1500 万スイス・フラン、従業員数 180 人以上から、1975 年の売上高 5100 万スイス・フラン、従業員数 250 人以上となった<sup>20</sup>。

### (3) クリプト社従業員に対する協力関係の秘匿

クリプト社の社員で米独諜報機関との関係を知っていたのは、ごく少数であった。当初は、取締役ニイベルグ唯一人であり、彼が 1976 年に引退するとその地位は Heinz Wagner に引き継がれ、更に後に Michel Grupe に引き継がれた<sup>21</sup>。

<sup>19</sup> Zentralstelle fuer das Chiffrierwesen。現在のドイツの BSI (Bundesamt fuer Sicherheit in der Informationstechnik) の前身組織である。

<sup>20</sup> CIA 資料抜粋。同抜粋によれば、1970 年から 1975 年までの 6 年間の純益合計は 1711 万スイス・フランであり、当時の為替相場で 20 億円近くの利益を上げていた。その後も 1990 年前後までは純益を上げ続けていたと見られる。

<sup>21</sup> WP 報道

一般の従業員に対しては、協力関係は秘匿されており、外部（実は NSA）から提供される暗号機の設計アルゴリズムは、協力関係にあるシーメンス社から提供されていると説明されていた。従業員の中には、暗号設計の欠陥に気付いて、勝手に改良して NSA が解読不能の製品を製造する者も現れたが、解雇されたり、改良を中断させられたりした。開発部門の幹部に対しては、暗号アルゴリズムの秘匿強度には規制が掛かっている旨の説明をして、ドイツ政府による規制のため已むを得ないものと思わせたりした<sup>22</sup>。

#### （4）暗号学の大家ヘンリー・ウィドマン招聘 1979 年

しかし CIA と BND は、このままでは秘密保持が難しいと考え、1979 年にスウェーデンの数学教授で暗号学の大家であるヘンリー・ウィドマン<sup>23</sup>を技術顧問に招聘した。その役割は、クリプト社の開発部門が納得する（即ち、気が付かない）高度な弱点を暗号アルゴリズムに仕込むことであり、スウェーデン諜報機関の推薦による人選であった。この後、クリプト社の暗号アルゴリズムはウィドマンが設計することとなったが、その設計目的は通常の統計学的解読手法では探知不可能な弱点を仕込むことであり、万が一弱点を発見されても製造段階或いは使用段階での人為的ミスと言い訳できるものを設計することであった。ウィドマンは不可欠の人物となり、その招聘は「ルビコン作戦」の歴史で最重要な人事であったという<sup>24</sup>。ウィドマンは 1994 年まで技術顧問を務めた。

## 7 米国単独のクリプト社経営時代（1993 年～2018 年）

1993 年、後述する経緯で、ドイツ BND はクリプト社の経営から手を引いた。同年 9 月ドイツ駐在の CIA 代表と BND は合意に達し、CIA はクリプト社の BND 所有株を 1700 万ドルで購入した<sup>25</sup>。この後は、米国単独でのクリプト社経営となる。

1990 年代には新たな暗号通信方式が発達し、次第にクリプト社製暗号機の販売は減少した。その結果、赤字に沈み込んだが、インテリジェンス収集プラットフォームとしては 21 世紀に入っても依然有効であった。それは、各国政府の官僚制の惰性によるもので、特に発展途上国ほどクリプト社製品を惰性で使い続けたとされる<sup>26</sup>。

しかし、暗号技術市場がハードウェアからソフトウェアに移行すると、遂にクリプト社も追従が困難となり、2018 年に会社を分割譲渡して解散した。

なお、米国 NSA は、クリプト社経営で蓄積した利益を使って、他の暗号機メーカーも買収したとされる。それは、同じくスイスの暗号機メーカー「グレターク社」である。同社は 1995 年に形式上元 NSA 職員が設立した会社を買収したが、2004 年に解散している。

---

<sup>22</sup> WP 報道

<sup>23</sup> 本名は Kjell-Ove Widman であるが、学生の頃米国に交換留学した際に発音し難いので、Henry Widman を通称としていた。留学経験もあり親米派であった。

<sup>24</sup> WP 報道

<sup>25</sup> WP 報道

<sup>26</sup> WP 報道

## 第3章 クリプト社の協力による情報成果

### 1 米国にとっての全体的成果

クリプト社の暗号機は多くの政府によって使用され、その暗号機の殆どは NSA にとって解読可能であったので、米国に大きな情報成果を生み出した。クリプト社製暗号機の使用国は、1950年代から2000年代にかけて120カ国以上に及んでいるとされる<sup>27</sup>。

WP 報道によれば、使用国には次の各国が含まれる。

○ 米州： アルゼンチン、ブラジル、チリ、コロンビア、ホンジュラス、メキシコ、ニカラグア、ペルー、ウルグアイ、ベネズエラ

○ 欧州： オーストリア、チェコスロバキア、ギリシャ、ハンガリー、アイルランド、イタリア、ポルトガル、ルーマニア、スペイン、トルコ、バチカン市国、ユーゴスラビア

（註：旧共産国がクリプト社製暗号機の使用を始めたのは、ソ連の崩壊後の事と考えられる。ユーゴスラビアは戦後初期にも購入したことがある。）

○ アフリカ： アルジェリア、アンゴラ、エジプト、エチオピア、ガボン、ガーナ、ギニア、象牙海岸、リビア、モーリシャス、モロッコ、ナイジェリア、コンゴ共和国、南アフリカ、スーダン、タンザニア、チュニジア、コンゴ民主共和国（ザイール）、ジンバブエ

○ 中東： イラン、イラク、ジョルダン、クウェート、レバノン、オマーン、カタール、サウジアラビア、シリア、UAE

○ アジア： バングラデシュ、ビルマ、インド、インドネシア、日本<sup>28</sup>、マレーシア、モーリシャス、パキスタン、フィリピン、韓国、タイ、ヴェトナム

なお、ソ連や中国はクリプト社製暗号機を使用せず、米国はそれらの国の暗号通信は解読できなかったが、クリプト社製暗号機を使用する諸国の在モスクワや在北京大使館と本国間の通信を解読することにより、ソ連と中国について相当の情報を入手することが可能であったという<sup>29</sup>。

### 2 米独協力期間中（1970年～1993年）の成果

#### （1）全体的な成果

CIA 文書抜粋によれば、米独協力期間中、米 NSA にとって、その暗号解読の40%以上が「ルビコン作戦」の成果であり、代替不可能な重要な情報源であった。更に独 BND にとっては、その外交関係情報報告の90%が本作戦の成果であり、本作戦が米独諜報協力の根幹であったという。

NSA はシギント機関であり、その通信暗号解読の40%以上が本作戦由来であったということは、米国諜報コミュニティにとって極めて大きな意味がある。ところが更に、BND はオールソース・インテリジェンス機関であり、ヒューミントを含む全外交関係情報報告の90%

<sup>27</sup> WP 報道。ZDF 報道によれば、クリプト社の最盛期には、世界の130を超える政府（軍、諜報機関の通信を含む）を顧客にしていたという。

<sup>28</sup> 日本について、使用組織と使用台数については特定できなかった。

<sup>29</sup> WP 報道

がシギントの本作戦由来であったということは、BND の外交情報源の殆どが本作戦であったということであり、ドイツにとって如何に大きな位置を占めていたかを示すものである。

## (2) 地域別、個別国の成果

地域別では、1980年代、NSA の G グループ（ソ連圏とアジアを除く全世界担当）の情報報告の 50%以上は、クリプト暗号機解読由来であった<sup>30</sup>。

クリプト社の暗号機の使用国は世界中に及んでいるが、1981年時点で、大口購入国は、サウジアラビア、イラン、イタリア、インドネシア、イラク、リビア、ジョルダン、韓国の順であった<sup>31</sup>。

国別で成果が大きかったのはイランである。「ルビコン作戦」のお蔭で、イランの諜報対象の 80～90%の通信は解読可能であった。1988年にはイラン通信 1万9千件が解読され情報化されたという<sup>32</sup>。

## 3 個別の情報成果

「クリプト社作戦」の情報成果を、個別具体的な事例で見てみよう。

### (1) 1978年キャンプ・デービッド会談（エジプト通信解読）

1978年9月、米カーター大統領の仲介で米国の大統領別荘キャンプ・デービッドで、エジプトのサダト大統領、イスラエルのベギン首相を迎えて、両国の和平交渉が行われた。

この交渉では、サダト大統領とカイロ間の（クリプト暗号機を使用した）通信を米 NSA が傍受して、エジプトの立場に関して情報を入手した<sup>33</sup>。

### (2) 1980年イラン米大使館員人質の解放交渉（アルジェリア通信解読）

イラン革命防衛隊に指導された学生達は、1979年11月テヘランの米国大使館を占拠して大使館員 52 人を人質に取った。

人質の解放交渉ではアルジェリアが仲介した。アルジェリアはクリプト社の暗号機を外交通信に使用していたので、米国はアルジェリア本国と大使館間の秘密通信を解読できた。当時の NSA 長官ボビー・インマンによれば、この解読情報は、当時のカーター大統領にとって、イランの状況を把握して人質解放交渉を管理するために絶対に重要な情報であり、カーター大統領は頻りに NSA 長官に電話をしてアルジェリアの通信情報を要求したという<sup>34</sup>。

### (3) 1982年フォークランド戦争（アルゼンチン通信解読）

アルゼンチン沖のフォークランド諸島は、19世紀以来英国が海外領土として実効支配していたが、領有権を主張するアルゼンチンが 1982年に軍事侵攻し占領した。これに対して、英国は米国や EU 諸国の支援を受け、軍事作戦を展開して同諸島を奪回した。

その際、アルゼンチン海軍はクリプト社の暗号機を作戦用にも使用していたため、米国 NSA が解読情報を提供し、英国が情報優位を活用して戦闘でも優位に立ち戦勝に貢献した<sup>35</sup>。

---

<sup>30</sup> WP 報道

<sup>31</sup> WP 報道

<sup>32</sup> CIA 抜粋資料

<sup>33</sup> WP 報道

<sup>34</sup> CIA 資料抜粋

<sup>35</sup> WP 報道、ZDF 報道。

アルゼンチンは、クリプト社の暗号機が解読されていることを疑い、クリプト社の技術顧問ヘンリー・ウィドマンを召喚して詰問したが、ウィドマンはクリプト社の暗号機は解読不能であり、秘匿強度の低いアナログ秘話装置が解読されたのではないかと主張して切り抜けた。その結果アルゼンチンはその後もクリプト社の暗号機を使用し続けた<sup>36</sup>。

#### (4) 1986年西ベルリンのディスコ爆破事件（リビア通信解読）

1986年4月西ベルリンのディスコ「ラ・ベル」が爆破された。同ディスコは駐留米国兵が良く集まる場所であり、米兵多数が負傷し2人が死亡した。

これに対して、レーガン大統領（当時）は、米国はリビア関与の証拠を握っている、その証拠とは事件1週間前に東ベルリンのリビア大使館が攻撃命令を受け、事件翌日にはトリポリに任務達成の報告をしていることであると述べた。そして同月、米軍が報復措置としてリビアの首都トリポリを爆撃した。

リビアもクリプト社の暗号機を使用しており、米国NSAがリビアの首都トリポリと東ベルリンの外交通信を傍受解読していたのである<sup>37</sup>。

#### (5) 1989年パナマの独裁者ノリエガ将軍の所在把握（バチカン市国通信解読）

パナマの独裁者ノリエガ将軍は1989年5月の選挙で敗北したにも拘らず、そのまま居座ろうとしたが、米国は米海兵隊員の殺害等を理由にパナマに軍事侵攻した。ノリエガ将軍はバチカン市国大使館に逃げ込んだが、その所在を把握され投降した。

ノリエガ将軍がバチカン市国大使館に逃げ込んだ事実は、バチカン市国の本国と同大使館の間のクリプト社暗号機による通信の解読によって判明したものである<sup>38</sup>。

## 第4章 困った情報成果の副産物

クリプト社の暗号機解読による情報成果は、関係国に大きな情報成果をもたらし、国益増進に貢献したのであるが、時には必ずしも好ましくない情報をももたらした。

その典型は、南米諸国による「コンドル」の通信システム「コンドル・テル」の傍受解読である。

1974年、南米4か国の左翼革命組織が「革命調整会議」という協力組織を設立した。参加組織は、アルゼンチン人民革命軍、ボリビア民族解放軍、チリ革命左派運動、ウルグアイ民

---

<sup>36</sup> CIA 資料抜粋

<sup>37</sup> WP 報道

なお、本事件と類似した事件に1991年パリにおける元イラン首相バクチアール暗殺事件がある。これはイラン政府の仕業であったが、それが判明したのはイランがクリプト社の暗号機を使用していたためと言われることがある。これに対して、オランダの研究者は、イランの暗殺部隊と本国との暗号通信が補足解読されたのは事実であるが、彼らを使用したのはクリプト社暗号機でなく複雑な手製暗号であって、これはオランダのシグント機関 TIVC 他多くの機関によって解読されていたという。-- Bart Jacobs, "Maximator: European signals intelligence cooperation, from a Dutch perspective," *Intelligence and National Security*, 7 April 2020, p. 664, accessed 8 September 2021, <https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538>

<sup>38</sup> WP 報道

族解放運動ツパロマスであり、これら組織はキューバの支援を受け、革命を目指して、国内だけではなく欧州においてもテロを敢行している。

これらのテロ・革命運動に対抗して 1976 年に発足したのが「コンドル」である。参加国は、アルゼンチン、ボリビア、チリ、ウルグアイ、パラグアイ、ブラジルであり、1977 年末にはエクアドル、ペルーが加わった。「コンドル」はこれら南米諸国の国家諜報機関の調整機関である。チリのサンチャゴに情報センターを設置してテロ・革命勢力に関する情報交換を行うと共に、関係機関の秘匿通信システム「コンドル・テル」を導入し、通信用暗号機にクリプト社製を採用したのである<sup>39</sup>。

ところで、南米諸国の軍事独裁政権の多くは、革命勢力に対抗して、拉致、暗殺、拷問その他の超法規的な対抗措置を取り、多大な人権侵害をもたらしていた。その超法規的対抗措置は、国内にとどまらず欧州など国外にも及んでいた。当然のことながら、その関連通信が、関係諸国の諜報機関間の通信システム「コンドル・テル」でなされており、米独両国は、クリプト社暗号機による通信解読を通じて、その人権侵害を知り得る立場にあった。

独 ZDF 報道によれば、BND がその北ドイツの施設で傍受解読した情報には、アルゼンチンやチリにおける人権侵害事態が含まれていたという。アルゼンチンでは 1970 年代は軍事政権で、政権に対する反対者を誘拐、拷問、殺害していた。軍用機から数千人を大西洋上に突き落として殺害するなど合わせて 3 万人以上を殺害したという。米独ともこのような人権侵害の事態を知っていたにもかかわらず、これを放置していたのである<sup>40</sup>。

## 第 5 章 「クリプト社作戦」の終了

### 1 疑惑報道による打撃

クリプト社と米独諜報機関の協力関係についての出版物や報道は度々なされてきたが、次の報道は協力関係を阻害する影響を及ぼした<sup>41</sup>。

---

<sup>39</sup> 開示資料、CIA, *Counterterrorism in the Southern Cone*, 9 May 1977, accessed 8 March 2020, <https://nsarchive2.gwu.edu/dc.html?doc=6773840-National-Security-Archive-Doc-2-CIA-report>  
--開示資料、CIA, *Communications System Employed by the Condor Organization*, 1 February 1977, accessed 8 March 2020, <https://nsarchive2.gwu.edu/dc.html?doc=6773841-National-Security-Archive-Doc-3-CIA-cable>

—開示資料、DIA Intelligence Appraisal, *Latin America: Counterterrorism and Trends in Terrorism*, 11 August 1978, accessed 8 March 2020, <https://nsarchive2.gwu.edu/dc.html?doc=6773842-National-Security-Archive-Doc-4-DIA-Intelligence>

<sup>40</sup> ZDF 報道。

--Greg Miller and Peter Mueller, "Compromised encryption machines gave CIA window into major human rights abuses in South America," *Washington Post*, 17 February 2020, accessed 25 February 2020, [https://www.washingtonpost.com/national-security/compromised-encryption-machines-gave-cia-window-into-major-human-rights-abuses-in-south-america/2020/02/15/bbfa5e56-4f63-11ea-b721-9f4cdc90bc1c\\_story.html](https://www.washingtonpost.com/national-security/compromised-encryption-machines-gave-cia-window-into-major-human-rights-abuses-in-south-america/2020/02/15/bbfa5e56-4f63-11ea-b721-9f4cdc90bc1c_story.html)

<sup>41</sup> 本文に述べた報道の前にも、1977 年出版のウィリアム・フリードマンの伝記（ロナルド・クラーク著）は、1957 年のフリードマンのクリプト社ハーゲリン訪問を記述、また、1982 年出版の『パズル・パレス』（ジェームス・バムフォード著の NSA 研究の古典的名著）は、フリードマンとハーゲリ

### (1) 1993年、1994年元クリプト社社員による告発

クリプト社社員ハンス・ビューラーはイラン担当の営業員であったが、イランはクリプト社暗号機による通信内容の漏洩を疑い 1992年に同人を拘束して厳しく訊問をした。ビューラーは米独諜報機関とクリプト社との協力については全く知らされていず、9か月後の1993年初めクリプト社が100万ドルの身代金を払って解放された<sup>42</sup>。

しかし精神的外傷を負って帰国したビューラーは、クリプト社と米独諜報機関の協力を疑うようになり、疑惑を語り始めた。1994年には更に別の匿名の元社員と共にテレビに登場して米独諜報機関との協力疑惑を告発した<sup>43</sup>。

### (2) 1995年『ボルチモア・サン』紙による疑惑報道

米国の『ボルチモア・サン』紙は、クリプト社とNSAの協力関係の具体的証拠を入手したと報道した<sup>44</sup>。同紙によれば、1975年にNSA暗号専門家ノラ・マカビーがクリプト社における暗号機の詳細設計に関する議論に参加しており、これは同紙が入手した資料<sup>45</sup>と同席したモトローラ社技術者ボブ・ニューマンの証言があったとした。更に、クリプト社の元社員ユルグ・スポルンデリは1970年代後半に秘匿強度を下げるようにアルゴリズム変更を指示されたと述べ、同元技術者ルディ・フグは技術顧問ウイドマンが暗号機の秘匿強度には制限がある旨を述べたと、協力関係の根拠を示して報道した。

### (3) 一部顧客の流出

これらの疑惑報道に対して、クリプト社は断固として否定したが、これら報道の影響を受けて、少なくとも半ダース程の顧客がクリプト社製品の使用を停止した。それらの国は、アルゼンチン、イタリア、サウジアラビア、インドネシア、エジプトが含まれる。ところが、驚くべき事に、イランはクリプト社製暗号機の購入を直ぐに再開したのである<sup>46</sup>。

## 2 1993年ドイツの離脱

---

ンの協力関係の存在について記述したが、影響は殆ど無かった。

<sup>42</sup> CIA資料抜粋によれば、身代金はBNDが支払った。米国は身代金の支払いは国策に反するとして支払わなかった。

<sup>43</sup> WP報道。CIA資料抜粋によれば、1994年ビューラー等のテレビ告発の際は、当時のクリプト社取締役Michael Grupeが反論のテレビ会見を行ったが、なかなか上手な対応であり、疑惑を有耶無耶に終わらせた。

<sup>44</sup> Scott Shane and Tom bowman, “RIGGING THE GAME Spy sting: Few at the Swiss factory knew the mysterious visitors were pulling off a stunning intelligence coup—perhaps the most audacious in the National Security Agency’s long war on foreign codes; NO SUCH AGENCY,” *The Baltimore Sun*, 10 December 1995, last accessed 3 March 2020, <https://www.baltimoresun.com/news/bs-xpm-1995-12-10-1995344001-story.html>

本記事は、NSAによる暗号解読手法として、他に、スーパーコンピューターによる純理論的暗号解読、米国国内でのFBI要員の外国施設侵入による暗号の入手、米国外でのCIAの協力者工作による暗号の入手、米国企業に対する輸出許可権限をテコにした協力取付け（秘匿強度の制限、バックドア設置）などを挙げている。

<sup>45</sup> 資料自体は2020年2月11日にScott Shaneがツイッターで公表している。

”CIA/IA/Motorola Meeting—August 19-20, 1975,” in Scott Shane, Twitter post, 11 February 2020 (11:14pm), accessed 3 March 2020,

<https://twitter.com/ScottShaneNYT/status/1227242088057565190>

<sup>46</sup> CIA資料抜粋。

ビューラー事件によって協力関係の暴露の虞もあり、ドイツは 1993 年「ルビコン作戦」を離脱したが、その基本的原因は米独の国益の違いである。

CIA 文書抜粋によれば、米独共有時代の煩わしい問題は、解読困難な暗号機の販売可能対象国の範囲であった。ドイツとしては NATO の同盟諸国には解読困難な暗号機を販売したいと考えていたが、他方米国は、解読困難な暗号機の販売対象をできるだけ限定しようとした。当初 NATO 諸国は全て解読困難暗号機の販売対象であったが、初めにギリシャとトルコが除外され、スペインやイタリア他の国々も次々に販売対象国から除外されるようになったのである。この点について米国 NSA は極めて執拗であって、最終的には、解読困難な暗号機の販売対象国は、「ルビコン作戦」に直接又は間接に関与する一部の NATO 諸国<sup>47</sup>とスウェーデンとスイスのみとなってしまったという。

ところが、冷戦が終結して 1990 年にドイツ再統一が実現すると、ドイツにとっては、欧州諸国との友好関係がより重要となってきた。万が一「ルビコン作戦」へのドイツの関与に EU 諸国が気付いた場合、その政治的悪影響は大きく、懸念が広がった<sup>48</sup>。NATO 加盟の友好国といえども躊躇なく標的とする米国の方針にドイツが附いていけなくなったのである。

また、1970 年代は、クリプト社は優良企業であり、純益を生み出していたが、1990 年代に入ると、電子機械式暗号機への需要が減少<sup>49</sup>して赤字体質となり、資金援助が必要となった。米国にとっては赤字補填をしても得られる情報に価値があったが、再統一後のドイツには財政的余裕が失われて、関与を嫌うようになったという<sup>50</sup>。

以上の事情で、1993 年ドイツ BND はクリプト社の経営から手を引いた。同年 9 月ドイツ駐在の CIA 代表と BND は合意に達し、クリプト社の BND 所有株は CIA が買い取り、この後は、米国単独でのクリプト社経営となる。

なお、ドイツはクリプト社の経営からは手を引いたものの、第 7 章で述べるように、その後も 21 世紀に至るまで別の手段によって、クリプト社の暗号機の解読は継続できたと推定できる<sup>51</sup>。

### 3 2018 年クリプト社の持株会社 AEH の解散

1993 年以降は、米国（CIA と NSA）が単独でクリプト社を運営してきたが、その後イン

---

<sup>47</sup> これら一部の国とは、直接関与しているドイツの他、UKUSA シギント同盟の一員として情報成果の分け前を得ている英国、カナダ程度と推定できる。

<sup>48</sup> CIA 資料抜粋

<sup>49</sup> 例えば、現在でも使用されている公開鍵暗号 Pretty Good Privacy は 1991 年に開発され、前世紀中に世界中で使用可能となった。本暗号は、NSA 文書を漏洩したウィリアム・スノーデンも 2013 年漏洩準備のための秘密通信に使用している。

<sup>50</sup> CIA 資料抜粋

<sup>51</sup> 1993 年にドイツはクリプト社の経営から手を引いたが、その後も 21 世紀に至るまで、クリプト社暗号機の解読を継続できたと推定できる。後述するように、クリプト社の暗号の秘密は、そのスウェーデン人幹部を通じて、スウェーデンのシギント機関 FRA に漏洩していたと推定されており、ドイツ BND は協力関係にある FRA を通じて解読に必要な情報を入手していた可能性が高い。Peter F. Müller, Ulrich Stoll and David Ridd, "Exklusiv-Recherche: BND spionierte jahrzehntelang am Parlament vorbei," *Frankfurter Rundschau*, 1 July 2020, accessed 8 September 2021, <https://www.fr.de/politik/geheimoperation-bnd-maximator-13818604.html>

ターネット通信の発達、Pretty Good Privacy など公開鍵方式の普及によって、世界の暗号通信に占めるクリプト社製暗号機の重要性は急速に低下してきたと見られる。その結果、CIA と NSA にとって諜報源としてのクリプト社経営の重要性が低下し、遂に「クリプト社作戦」も終了を迎えた。

即ち、2018年にクリプト社の持株会社 AEH（リヒテンシュタインに登記）は解散し、2社がクリプト社の資産を買収した。一つは、CyOne Security 社であり、経営陣買収によってクリプト社元経営者が設立したもので、専らスイス政府にセキュリティ・システムを提供するスイス政府御用達専門企業である。もう一つは、Crypto International 社であり、クリプト社の国際事業を引き継いでいる。CyOne Security 社 CEO の Giuliano Otth は 2001 年以來クリプト社の CEO であり、米国インテリジェンス機関との協力の事情を良く知っていると思われるが、Crypto International 社の新経営者は、事情を全く知らないようである<sup>52</sup>。世界の顧客を相手とする Crypto International 社にとって、NSA との関係暴露する報道がなされた現在、経営に対する悪影響は大きく、新経営者はとんだ不良資産を掴まされてしまったと言えよう。

## 第6章 教訓：インテリジェンスの実態と論理

以上、「クリプト社作戦」の全体像を概観してきたが、インテリジェンスの世界において同作戦の持つ意味、同作戦から読み取れる諜報世界の実態と論理について考察してみよう。

### 1 暗号解読・暗号攻略におけるヒューミント手法の役割

通信諜報の世界では、暗号解読・暗号攻略は主要な情報入手手法である。

その暗号解読・暗号攻略の歴史では、第二次世界大戦時の米国による日本外交暗号や海軍暗号の解読、或いは英国によるドイツ・エニグマ暗号の解読が有名であるが、ともすると暗号解読は数学的天才や異才の活躍の結果であるようなイメージが流布している。また、現代の NSA による解読手法として、スーパーコンピューターと高等数学を活用した純粹理論的な解読が知られている。

しかし、暗号解読では、天才や異才或いはスパコンと高等数学よりも、実は広義のヒューミントによる貢献が大きいのである<sup>53</sup>。その中には、在米外国公館への侵入<sup>54</sup>、協力者工作に

---

<sup>52</sup> WP 報道

<sup>53</sup> グレゴリー・トレバートンはインテリジェンス専門家であり、2014～2016年に亘って米国の国家諜報会議（National Intelligence Council）議長を務めた人物であるが、NSAによる暗号解読は、多分高等数学やスパコンによるよりも暗号書の窃取の方が多いと、2001年に記述している。Gregory Treverton, “Intelligence Crisis,” *Government Executive Magazine*, 1 November 2001, last accessed 9 March 2020, <http://www.govexec.com/magazine/magazine-national-security/2001/11/intelligence-crisis/10254/>

<sup>54</sup> 実際、NSAの開示文書によって、第二次世界大戦前の1920年代と1930年代に米国当局（この場合は海軍情報部であるが）は少なくとも3回、在ニューヨーク日本領事館に侵入して暗号書を複写したことが明らかにされている。

よる暗号の入手、民間企業への働掛け（民間暗号技術の政策・規準への影響力行使、民間の暗号システムやネットワークへの弱点挿入）、配送途中の製品に対する工作などが挙げられる<sup>55</sup>。

そして、今回の「クリプト社作戦」の全体像の判明により、そのヒューミント的手法の暗号攻略に占める大きさが再確認されたのである。通信の秘密保全に関心を有する者は、このことを肝に銘じて、ヒューミント的手法による攻撃可能性も含めて広汎な通信保全措置を構築することが重要である。

## 2 友好国に対するインテリジェンス

「クリプト社作戦」では、単に第三世界の諸国だけではなく、米独の友好国も情報収集の標的とされていた。この背景にある友好国に対する諜報の在り方に関するインテリジェンスの論理は如何なるものであろうか。

その論理を明白に示した資料が NSA の開示資料<sup>56</sup>にある。それは友好国を含む第三国<sup>57</sup>との関係について述べたものであるが、表題「サード・パーティ諸国：パートナーにして標的」が本質を明確に示している。友好国も標的であることが前提とされているのである。同資料は更に「国家には友人も敵も存在しない、在るのは国家利益だけであると言われる」「今日の友人や同盟国も、いつまでも友人や同盟国である訳ではない」と記述しており、冷厳な国益追求が国家関係の基礎とされている。即ち、インテリジェンスでは、国益が合致する限りで協力し、一致しない範囲では互いを標的として諜報対象とすることが前提とされているのである<sup>58</sup>。

<sup>55</sup> 茂田忠良『米国国家安全保障庁の実態研究』（警察政策学会資料第 82 号、2015 年）第 2 部第 3 章 3 「暗号対策」中 126-130 頁参照。

<sup>56</sup> 開示資料、NSA、"Third Party Nations: Partners and Targets," *Cryptologic Quarterly*, Vol. 7 No 4, winter 1989, accessed 9 March 2020, [https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/third\\_part\\_nations.pdf](https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-quarterly/third_part_nations.pdf).

<sup>57</sup> NSA にとってセカンド・パーティとは、UKUSA シグント同盟を構築している英加豪ニューゼーランド 4 カ国であるが、UKUSA 同盟は極めて密接強固な特別関係であり、この同盟諸国間では互いを標的にしないとされている。しかし米国 NSA は、これにも例外を設定し、国益が要求するならば UKUSA 同盟諸国であろうと標的とすることが許されるとしている。茂田『実態研究』第 3 部第 1 章 1 「英 GCHQ 概観と NSA との協力関係」188 頁参照。

<sup>58</sup> 茂田『実態研究』第 3 部第 2 章 1 「サード・パーティ関係とは」219-220 頁参照。

NSA 渉外局の資料でも、サード・パーティとの協力関係は無条件のものではなく、常にギブ・アンド・テイクの関係であり、協力関係の進展は、あくまで米国の国家諜報要求が相手国の国家諜報要求と交叉する場合に限られるとしている。

「米国と相手国の国家諜報要求が交叉する場合」とは、筆者の解釈では、シグント協力がそれぞれの国の国家諜報要求の充足に貢献する場合ということである。即ち、シグントに関する国家諜報要求の充足という面においてギブ・アンド・テイクの関係が成り立つ場合にのみ協力するし、シグント協力関係が進展するということである。

なお、危機的状況に於いては一方的なシグント支援があり得るとしている。これは、危機的状況にある国を支援することに米国の国益が合致する場合は、シグント面だけを見ればギブ・アンド・テイクの関係は成り立たないが、国益全体の立場からシグント支援をすることがあり得るということである。

何れにしろ、ここには、博愛主義もなければ、一方的なインテリジェンスやサービスの提供も存在

実際、米国の友好国であるイスラエル、フランスや韓国は、米国に対する積極的な諜報活動を行っている国として、米国 NSA の監視対象とされている<sup>59</sup>

なお、ドイツ BND は、「クリプト社作戦」が NATO 同盟諸国を標的としていたこともあって、同社の経営から離脱したが、それもソ連崩壊とドイツ統合という世界の歴史的構造変化に伴う政治判断であって、離脱前は友好国に対する諜報成果を享有していたのである。

何れにしろ、インテリジェンスの世界における冷厳な国家関係を忘れるべきではない。

### 3 供給網工作～現代の「クリプト社作戦」

「クリプト社作戦」は、当初 NSA が解読困難な暗号機の販売時期と対象国を制限する「拒否作戦」から出発して、やがて解読を容易にする弱点を仕込んだ暗号機を販売する「積極工作」に至った。同作戦は 2018 年に終了したが、このように製品に弱点を仕込んで標的組織に届ける作戦は他に実施していないのであろうか。

実は、NSA は供給網工作 (supply chain operation) の名の下に現在も同様の作戦を実施しているのである<sup>60</sup>。

即ち、供給網工作は製造段階での工作と製品配送段階での工作の二つに分けられる。「クリプト社作戦」は製造段階での工作であるが、スノーデン漏洩資料で判明したのは、後者の配送経路介入である。これは、標的組織がサーバーやルーター等のコンピュータ・ネットワーク関連製品を発注した場合、その製品を配送途中で一旦確保して、これにマルウェアを注入し或はマルウェア入りハードウェアを装入した上で、配送経路に戻して発注元に届ける方法である。具体例としては次の例が挙げられている。

#### ○ シリアのインターネット基幹部品への工作

2010 年 6 月の NSA 内部資料によれば、「シリア通信事業機構」のインターネット基幹部品の製品（中枢ルータと推定される）に対して配送経路介入を実施した結果、シリアのインターネット通信の基幹部品に侵入できた。同基幹部品は携帯電話通信にも使用されていたため、極めて大きな情報成果を挙げたという。

#### ○ 中国製 VoIP 通信機材への工作

2013 年 4 月の NSA 内部資料によれば、NSA は中国から輸出される暗号化 VoIP 通信機材に対して配送経路介入を計画し、ヒューミント機関と第三国当局の協力を得て、海外におい

---

しない。インテリジェンス活動が、国民からの付託を受けて且つ国民の負担の上に成り立っている以上（そして場合によっては構成員の人命の犠牲の上に成り立っている以上）、これは当然のことであり、世界のインテリジェンス業界の常識を述べたものである。

この点に関して元 NSA 長官マイケル・ロジャースの次の発言は味わい深い。「ファイブアイについてよくある勘違いは、全ての情報が一方的にもらえるということです。情報をもらいたいなら、出す覚悟も必要です。」マイケル・ロジャース、土屋大洋によるインタビュー。『朝日新聞』2020 年 1 月 29 日付「サイバー監視は正義？」

<sup>59</sup> 茂田『実態研究』第 2 部第 1 章 2 「戦略的任務リスト」 31 頁参照。

<sup>60</sup> 以下の本文の記述は、次を参照。

茂田忠良『サイバーセキュリティとシグント機関～NSA 他 UKUSA 諸機関の取組～』（情報セキュリティ総合科学第 11 号、2019 年 11 月）22-23 頁。

て物理的介入を行っている<sup>61</sup>。

#### 4 米国以外の国は紳士か ～他の諸国による供給網工作

それでは、米国・UKUSA 諸国以外の国々はどうかであろうか。他の国は紳士であってこのような「汚い」作戦は実施していないのであろうか。

既に、「クリプト社作戦」で見たように決してそんな事はないのである。そもそも、フランスもドイツも、クリプト社に食指を動かしていたのである。「クリプト社作戦」以外にも次のような例が判明している。

##### (1) ドイツ諜報機関 BND<sup>62</sup>

2005年10月時点で、供給網工作を行うために幾つかのフロント企業を設立していた。(情報源：公式のNSA 渉外情報)

##### (2) フランス諜報機関 DGSE<sup>63</sup>

2002年にセネガルのセキュリティ・サービスにコンピュータとファックスを提供したが、その結果2004年までにこれらのシステム上の全情報にアクセスできるようになった。(情報源：間接的に情報アクセスのあるNSA 協力者)

##### (3) オランダのシギント機関 TIVC<sup>64</sup>

オランダ海軍諜報部傘下のシギント機関 TIVC (Technisch Informatie Verwerkings Centrum:英語名 Technical Information Processing Centre)も「クリプト社作戦」と同様の、製造段階における供給網工作を実施していた。

1970年代末、オランダのフィリップス社とドイツのシーメンス社は共同で、NATO 組織用にテレックス暗号機「アロフレックス」を開発した。アロフレックスは暗号強度の高いことで知られ、一部のNATO 諸国政府には政府使用目的でも販売されたが、一般商用での販売は禁止されていた。

そこで、フィリップス社は、商用販売目的でアロフレックスの商用版 T1000CA を開発し

---

<sup>61</sup> NSAは海外における配送経路介入作戦のため、「海外遠征チーム (Expeditionary Access Operations)」という専門部署を設置しており、作戦実施においては、在外公館に設置した「特別収集サービス (SCS)」拠点なども活用している。

<sup>62</sup> 茂田『サイバーセキュリティとシギント機関』23頁

<sup>63</sup> 茂田『サイバーセキュリティとシギント機関』24頁

<sup>64</sup> Huib Modderkolk, “Nederland luisterde jarenlang landen af dankzij superchip,” *de Volkskrant*, 20 February 2020, accessed 25 February 2020,

<https://www.volkskrant.nl/nieuws-achtergrond/nederland-luisterde-jarenlang-landen-af-dankzij-superchip~bc9a9ce4/> 本報道によれば、本文の事実がCIA 秘密文書「MINERVA – A HISTORY」

(CIA インテリジェンス研究センター、2004年)の内容から読み取れるという。

-- Bart Jacobs, “Maximator: European signals intelligence cooperation, from a Dutch perspective,” *Intelligence and National Security*, 7 April 2020, accessed 8 September 2021,

<https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538> 本論文によれば、フィリップス社は、他に米国にも協力している。即ち、NATO 加盟国トルコは自国使用目的でクリプト社暗号機の購入を計画したが、その際に、どのタイプの暗号機を販売するか、つまり弱点を仕込んだ暗号機を販売するか否かで、米独間で意見が対立して合意が得られなかった。そこで、米国は、オランダ通信保全機関NBVを介してフィリップス社に接近し、トルコ用に弱点を挿入したアロフレックス製作を依頼し、これをトルコに納入させたという。Ibid., p664.

た。その暗号アルゴリズムはシグント機関 TIVC の提案を採用したものであり、NATO 仕様よりも暗号強度は低くしていた。しかし、それでも当時のスーパーコンピュータで解読すると、1 か月半を要したという。そこでフィリップス社の研究所は TIVC の依頼に応じて、1977 年に解読用の専用マイクロチップの開発に着手し 1979 年春には完成させ、T1000CA 用の専用解読機を製作した。この専用解読機を使えば、解読所要時間は 40 分に短縮できた。

フィリップス社は、この解読専用機を、蘭 TIVC、米 NSA や独 BND などに販売した。つまり、T1000CA を軍通信或いは外交通信用で購入した諸国は、蘭、米、独など諸国シグント機関の容易な餌食となったのである。

#### (4) 中国、ロシアによる工作<sup>65</sup>

さて、では西側民主主義国家以外の国はどうであろうか。

当然、中国もロシアも取り組んでいるのである。

詳細は不明であるが、スノーデン漏洩資料によれば、2012 年時点では、中露両国とも、コンピュータ部品のバイオスを工作対象として注目しており、米企業の American Megatrends(AMI)と Phoenix Technologies の製品が攻略されていたとされる。

供給網工作は、世界の諜報機関が取り組んでいる標準的な情報収集手法であるということである。

## 5 華為、カスペルスキーとの関係

米国は近年、中国の巨大通信企業華為と中国政府との関係やサイバーセキュリティ会社カスペルスキー社とロシア政府との関係に疑惑の目を向けている。

例えば華為について、米国政府は中国政府の供給網工作などの情報収集に協力しているとの証拠は掴んでいないようである<sup>66</sup>にも拘らず、5G における華為製品の普及を抑制しようと、友好国に圧力を加えている。

米国が、何故、これら企業に危惧を持つのであろうか。それは米国自体がクリプト社など企業の協力を得て、或いは供給網工作を行って、諜報工作活動を成功させてきた歴史があるからである。

しかし、米国政府の危惧が自己のミラーイメージに基づく単なる杞憂かと言えば、そうとは言えないであろう。ソ連共産党によるロシア革命以来ソ連崩壊に至るまでの世界を対象にした 70 年間を超えるインテリジェンスの歴史、中国共産党による結党以来 100 年間に及ぶインテリジェンスの歴史を振り返れば、ロシア、中国両国のインテリジェンスは米国に勝るとも劣らない実績を誇っているのである。インテリジェンスにおける民間企業利用において、ロシア中国両国が米国より劣ると判断する根拠は全く存在しないのである。

これがインテリジェンスの世界である。

「クリプト社作戦」は、これらインテリジェンスの実態と論理を再認識できるケーススタ

<sup>65</sup> 茂田『サイバーセキュリティとシグント機関』58 頁

<sup>66</sup> 茂田『サイバーセキュリティとシグント機関』〈補論〉 対中国サイバーセキュリティ対策の話題 2 華為問題（中国による Supply Chain Operation）86-91 頁参照。

ディの教材なのである。

## 第7章 補足：その他諸国諜報機関の関与（2022年新規加筆）

さて、「クリプト社作戦」の利益は、独り米国とドイツの2か国が享受していたのであろうか。実は、本稿冒頭で紹介した WP 報道・ZDF 報道の後、オランダ人研究者による関連論文<sup>67</sup>が発表されたり、政府広報がされたり、関連報道がなされ、クリプト社の暗号を巡る真相が更に判明してきている。それによれば、米独2か国の他、少なくとも7か国もがクリプト社の暗号解読法を提供されており、これらの国々は、クリプト社の暗号解読の恩恵を受けてきたのである。

### 1 Maximator 諸国（デンマーク、スウェーデン、独、蘭、仏）

シギントに関する多国間協力では、UKUSA シギント同盟が有名であるが、実は、この他にも Maximator という名称の欧州の多国間協力枠組が存在する。これは、1976年にデンマークの提案にドイツ、スウェーデンが応じて始まった多国間協力であるが、遅れてオランダとフランスが参加した。協力内容は、通信傍受と暗号解読の両面での協力である。

この多国間協力の枠組の中で、クリプト社の暗号解読法が、ドイツ BND から他の4か国シギント機関に提供されたと推定される<sup>68</sup>。但し、その暗号解読法の入手手法（＝クリプト社を米独両国の諜報機関が運営していた事実）までは、知らされていない。

### 2 スウェーデン

スウェーデンは、上記1で述べたように、Maximator 加盟国としてドイツからクリプト社の暗号情報を入手できる立場にあったが、スウェーデン独自でも暗号情報を入手していたと見られる。その情報入手経路は、クリプト社のスウェーデン人幹部である。そもそも、クリプト社創業者のハーゲリン自身がスウェーデン人であるが、その後継者のシュトゥーレ・ニイベルグも、その後、技術顧問となったヘンリー・ウィドマンもスウェーデン人である。この他にも同社にはスウェーデン人の幹部がおり、これらスウェーデン人幹部は、スウェーデン FRA に秘密裡に暗号情報を提供していたと見られ、この関係は21世紀に至るまで保持されていたと見られる<sup>69</sup>。また、上記 Maximator 諸国のシギント機関は、1993年にドイツがクリプト社の経営から離脱した後は、スウェーデン経由で暗号情報を入手するようになった

---

<sup>67</sup> Bart Jacobs, “Maximator: European signals intelligence cooperation, from a Dutch perspective,” *Intelligence and National Security*, 7 April 2020, accessed 8 September 2021, <https://www.tandfonline.com/doi/full/10.1080/02684527.2020.1743538>

Jacobs は、サイバーセキュリティを専門とする大学教授であるが、オランダ政府のインテリジェンスやサイバーセキュリティ関係の役職についており、その論文の信頼性は極めて高い。

<sup>68</sup> Internal BND document, “Einführung: Die Operation THESAURUS/ RUBICON,” cited by Jacobs, “Maximator,” pp. 662,666.

<sup>69</sup> Internal BND document, “Einführung: Die Operation THESAURUS/ RUBICON,” cited by Müller, Stoll and Ridd, “Exklusiv-Recherche.”

と推定する。

### 3 英国

1982年のフォークランド戦争では、英国はアルゼンチンの軍通信・外交通信の解読の必要性に迫られ、UKUSAの協力関係から米国NSAに、また同時に、オランダ海軍情報部のシギント組織TIVCに協力を求めた。オランダも積極的に協力して、アルゼンチン軍と外務省が使用しているクリプト社の暗号法を提供したという<sup>70</sup>。(なお、第2章の3で述べた通り、1950年代のクリプト社との協力関係については、英国GCHQは米国NSAから知らされている。)

### 4 イスラエル

イスラエルも、クリプト社の暗号解読法を知っていたという<sup>71</sup>。イスラエルが米独どちらから暗号解読法を提供されたかは不明であるが、ホロコーストという過去の負債を持つドイツが提供した可能性が高いと思われる。

### 5 スイス

さて、クリプト社が所在するスイスの当局との関係は、如何なるものであったのだろうか。この点については、2020年11月に、スイス連邦議会の諜報監督委員会が報告書を公表<sup>72</sup>した。その関係を一言でいうと、スイス諜報当局も、21世紀には米国「クリプト社作戦」の恩恵(おこぼれ)に与かっていたのである。その経緯を報告書を基に見ていこう。

#### (1) スイス当局による探知と暗号解読資料の取得

第1章で述べたように、1993年には、クリプト社元社員ハンス・ビューラーが、クリプト社と米諜報機関の協力関係についてマスメディアを通じて告発した。

スイスのシギント担当組織である「戦略諜報局」(SND: Strategischer Nachrichtendienst、英語名 Strategic Intelligence Service)は、情報収集を始め、1993年秋には信頼できる情報の入手に成功した。即ち、クリプト社は英独両国の諜報機関が所有していること、同社は「弱点」を仕込んだ暗号機を輸出しており、その暗号は解読可能であることである。そこで、戦略諜報局は、同社暗号機の解読を計画し、同社の暗号機についての技術情報の入手に努力した。

ところで、戦略諜報局は、国防省参謀本部諜報部傘下の軍事組織であったが、2001年に国

<sup>70</sup> Jacobs, "Maximator," p.663.

<sup>71</sup> Internal BND document, "Einführung: Die Operation THESAURUS/ RUBICON," cited by Jacobs, "Maximator," pp. 662,666.

<sup>72</sup> Die Bundesversammlung, *Politische Mitverantwortung der Schweizer Behörden für die Aktivitäten der Crypto AG (Press Release)*, 10 November 2020, accessed 4 September 2021, <https://www.parlament.ch/press-releases/Pages/mm-gpdel-2020-11-10.aspx?lang=1031>

-- Die Bundesversammlung, *Fall Crypto AG Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte*, 2 November 2020, accessed 4 September 2021, <https://www.parlament.ch/centers/documents/de/bericht-gpdel-2020-11-10-d.pdf> 特に本報告書の20~23頁が関連している。

防相直轄の行政組織に改編された。改変後も戦略諜報局は、クリプト社暗号機の解読方法についての情報入手に努めたが、解読可能となったのは、結局、21世紀初頭に米諜報機関の同意を得て一定必要範囲の技術情報が入手できるようになってからである。その後、スイス当局は、2018年に米国の「クリプト社作戦」が終了するまで、情報入手で利益を得てきた。

SNDは、解読対象の通信入手は、当初は短波通信傍受（スイス陸軍担当）で行い、2006年以降は衛星通信傍受（コードネーム Onyx）を行った。

## （2） 連邦諜報局への改編とその関与の露呈

「戦略諜報局」は、2010年には「連邦諜報局」（NDB: Nachrichtendienst des Bundes、英語名 Foreign Intelligence Service）に改称されるとともに、組織が拡充された。

「連邦諜報局」初代局長 Markus Seiler は、クリプト社暗号機の弱点と米諜報機関との関係について口頭説明を受けたが、特別の行動は取らなかった。更に2017年には更に詳しく報告を受け、今後の対処方針について提案を受けたが、局長はそのまま放置しておいた。

2019年春、後任の連邦諜報局長 Jean-Philippe Gaudin はクリプト社について説明を受け、6月中旬にクリプト社関係について担当者に包括的な内部報告書の作成と提出を指示した。また、6月下旬には米独メディアがクリプト社について取材活動をしていることを知った。そこで、同局長は、8月に初めて国防相にクリプト社と米諜報機関との関係、そしてスイス当局も情報を得ていることを報告した。その後、連邦諜報局は、9月中旬には内部報告書を完成、また、10月中旬にはCIA秘密文書「MINERVA-A History」を入手した。そこで、10月下旬には国防相に再度報告すると共に、11月には連邦議会の諜報監督委員会にも報告した<sup>73</sup>。

この一連の経緯の中で、スイス諜報当局で、クリプト社の暗号解読資料の入手方法を知っていたのは、諜報当局の局長他ほんの2～3人であった。また、所管の国防相は2019年8月に至って初めて知らされるなど、政治指導者は知らないままに本活動は開始されそして終了していたのである。

以上、デンマーク、スウェーデン、蘭、仏、英国、イスラエル、スイスの各諜報当局の動きを見ても分かるように、インテリジェンス機関というものは常に情報源の開拓に熱意を持って活動するものなのである。

---

<sup>73</sup> 連邦議会の諜報監督委員会は、2020年2月のWP報道・毒ZDF報道を受け、委員会としての調査を開始し、本件報告書を同年11月2日に作成し同10日に公表したものである。

警察政策学会資料 第127号

「クリプト社」とNSA ～世紀の暗号攻略大作戦～  
(改訂版)

令和4(2022)年11月

編集 テロ・安保問題研究部会  
発行 警察政策学会

〒1002-0093

東京都千代田区平河町1-5-5 後藤ビル2階

電話 (03) 3230-2918・(03) 3230-7520

FAX (03) 3230-7007