

序

現在、それ自体で、日本暗号史分野で利用できる標準的で信頼のおける単一の参考文献は、事実上存在しない。日本暗号史に言及した研究者らの論文は、前提とすべき知識の不足によって、論理展開に矛盾を来たしているものも数多く、これが誤謬を拡大再生産させる原因となっている。これは、是正さるべきことである。

戦前・戦中の暗号研究は、日本においては政府機関の独占するところであった。政府の事業は膨大な公文書を発生させる。この種の歴史研究で、歴史学者が主として努力を傾けるのはこうした公文書記録に対してであるが、終戦時に旧軍公文書の大半が焼却されたため、暗号研究の全体像の把握に困難を来たしている。しかし、決定と報告という公式の歴史と並んで、本当に起きた事の一つの解釈に批判的な別の種類の歴史、当事者たちが自らに課された任務に関して何を考え、どのように感じ、夜遅くまで互いに何を話し合ったかを巡る歴史が存在する。この歴史の証拠は、私的な手紙、人間の記憶、GHQ のファイルなどに散逸している。その乏しさ、時には出所の不確かさ、そしてとりわけその秘密主義が禍して、歴史学者がそれを蒐集し、分析するのを難しくしている。筆者は、当該分野において、多様な評価を積み上げ、(現段階で明らかになっている証言・史料からは)日本人数学者の戦時中の暗号動員が成功しなかったであろうという推論を得た。

本論文は、加藤正隆「Information&Computing ex.3 基礎暗号学 I 情報セキュリティのために」(サイエンス社,1989)の知識を前提するものである。

数学者動員までの軌跡

日本暗号学は、ドイツ・ソ連と国境を面し、利害関係の薄いポーランドから、対ソ暗号解読の専門家である Jan Kowalewski 歩兵大尉を招聘して、陸軍の語学将校(英語・フランス語・ロシア語・ドイツ語)に対して講習をさせた。1923 年春に一大飛躍を遂げた。関係者の証言から推定すれば、講習内容は「ソ連暗号(乱数式・同期転置式)、ドイツの二重転置式、各種の諜者用暗号の構成と解読要領など」であり、ドイツ外務省の数学者 Werner Kunze らが開発し、1921 年頃から実際に外交暗号用に使用した無限乱数暗号や、ビジュネル多表には踏み込んでいなかったと結論される。当時の暗号解読の世界的趨勢は、「言語学と初歩の統計」が重視される段階にあり、Kowalewski の講習も時代を反映したものと判断される¹⁾²⁾。

この講習を受けた百武晴吉(1888.5.25-1947.3.10)は、1925 年にポーランド参謀本部に留学して対露無線諜報の実施要領とソ連暗号解読の技術を修得し、語学偏重の暗号解読者として初期陸軍暗号を主導する立場となった。

ポーランドから対ソ暗号解読技術を学んだことは、日本にとって極めて有益であったが、輸入学問特有の問題点から逃れることはできなかった。ポーランドは、1932 年頃にボズナン大学数学科の Marian Rejewski(1906-80)らを動員することでドイツの初期型エニグマ暗号を解読し、暗号史上に大きな足跡を残したが、これは日本側には全く伝えられていない(国益上、意図的に伏せたと判断される)。イギリスは、1939 年 7 月にポーランドからエニグマ暗号解読情報を提供されたことで、暗号解読における数学の重要性を理解し、Alan Turing のような数学者を動員するに至った。結果、エニグマ暗号を解読した成果で対独戦争を有利に運んでいる。膨大な計算量に依存するエニグマ暗号は、数学的アプローチによって初めて解読されたのであるが、この情報が日

本に伝わっていれば、世界史は大きく変貌していたであろう。輸入学問は、その機密性が高いほど輸出先が情報を制限することが容易になるのである。

ポーランドから帰国した百武晴吉は、新設された参謀本部第三部通信課暗号班の班長に就任し、暗号作製(日本陸軍が使用する暗号の作製)と暗号解読を担当することになった。暗号班の初期スタッフは、英語の工藤勝彦(1893.3.16-1945.1.4)、中国語の鶴田登実、ロシア語の大久保俊次郎(?-1967.12.10)・酒井直次(1891.3.26-1942.5.28)・中野勇(1894.4.23-1945.1.4)らである⁴⁾。砲兵将校の中野勇は、陸軍暗号の数学的・理論的指導者として名を残すことになるが、その数学的能力を評価されて暗号班に入ったわけではなく、ロシア語に通じていたからと推測される。このように、参謀本部暗号班は当初数学を重視してはいなかったことが明らかであるが、これは日本に限ったことではなかった。

1930年、暗号班は参謀本部第三部通信課から参謀本部第二部支那課に配置転換された。これは、暗号班による重慶政府暗号の解読成功が、済南事変を有利に進める上で大きく貢献したことに起因する。このため、情報部である参謀本部第二部が、暗号班を指揮下にしようと企図したからであった。この移籍は、暗号解読情報を利用する支那課にとっては有益であったが、暗号班としては、元来理工系の将校が集まる通信課から切り離されたため、陸軍暗号の数学的な進歩を阻害する要因となった。

1931年、アメリカの暗号解読者であった Herbert Osborn Yardley(1889.4.13-1958.8.7)によって、アメリカとイギリスの暗号解読の内幕が暴露された⁵⁾。Yardleyの公表した内容には、アメリカが日本の外国公館から暗号書を盗写したという記述もあり、日本側が組織的な暗号書盗写工作に踏み切る契機となった。日本は各国の暗号書を盗写したが、この中にはアメリカ國務省が1939年に導入したストリップ暗号のように、高度に数学的な技法を必要とするものがあつた。1939年に導入されたストリップ暗号は、戦時中はアメリカ海軍暗号として使用され、陸海軍による理論解読の研究が本格着手されるに至つたが、完全には成功しなかつた⁶⁾。盗写工作は、戦前におけるストリップ暗号の理論解読研究の緊急性を失わせ、暗号解読の学理的発展の阻害要因ともなつた。

1933年以降になつて、参謀本部は毎年将校を集めて暗号解読教育を施すことで、暗号解読要員を増強した。参謀本部は、東京外国語学校でロシア語・中国語・英語を学んだ語学将校が、語学の点数17点以上の制限をクリアした将校を抽出して教育したことから、暗号解読への語学偏重が更に顕著になる原因となつた⁷⁾⁸⁾。

1936年、第七師団暗号班長の原久(?-1974.5.27)は、解読不可能な暗号として無限乱数暗号を提唱した。有限乱数暗号は、当時の参謀本部暗号班では解読可能なものとして棄却されていたが、無限乱数暗号ならば解読できないことが統計的に認められたため、陸軍は全面的に無限乱数暗号を採用するに至つた。統計的結論が数学的真実と一致するとは限らないが、日本陸軍は無限乱数暗号の安全性に対する数学的証明を与えることには無関心であつたと判断される。無限乱数暗号の情報理論的安全性は、Claude Elwood Shannon(1916.4.30-2001.2.24)が1948年に数学的証明を発表しているが、Shannon以前に同様の証明を試みた研究者の存在は知られていないようである。原は、無限乱数暗号の導入に力があつたが、強度上の問題から機械暗号の導入に強く反対した。このため、機械暗号研究が他国より遅延した点を指摘することができる。

1937年、参謀本部第二部暗号班から、暗号作製班が第三部通信課に分離した。暗号作製班は、通信学校出身の理工系将校によって構成されたため、暗号作製班に数学の導入が図られる契機となつた。暗号作製班の初期スタッフは、中野勇・原久のような数学偏重の暗号将校であつた。

1939年、第三部通信課暗号作製班に、通信学校次席の釜賀一夫(1917.1.01-2003.11.23)が配属された⁹⁾。釜賀は、陸軍士官学校在学中から“数学の天才”と呼ばれた砲兵将校で、同年にn進法を利用した乱字式陸軍武官暗号を導入して電報料を240

万円節約することに成功するなど、数学の暗号学への導入に関する日本のパイオニアとなった。

同年、暗号解読班は第二部第十八班と改称され、独立した。第十八班長は、1940年8月まで激職の第二部長が兼務したが、これによって第十八班を監督する人間が実質的に不在となり、指揮監督面で不具合を来た。「朝出勤してきますと、まずみんなお茶を飲んで雑談をし、やれるだけやって、その日処理できなかったものは通信の資料もみんなボツになってしまうのです」と、第十八班の砲兵将校広瀬栄一(1911-88.5.1)は回顧している¹⁰⁾。結果、第十八班の機能は一時的に低下した。

数学者の動員への道のり

1941年初期、第十八班の広瀬栄一は、「暗号研究に数学者を動員すべきである。故に高給で東大などの数学者に協力を得よう」と思い立ったが、同年6月中旬に広瀬がフィンランド大使館駐在武官輔佐官として転出してから間も無く、この数学者(氏名不詳)は去ったという。同時期、東北帝国大学数学教室教授の微分幾何学者である高須鶴三郎が、アメリカ数学会による数学者の戦時研究動員の事実を訴えた記録はあるが¹¹⁾、広瀬が高須の訴えを取り上げたという記録は見当たらない。当時の陸軍が解読していたソ連と中国の暗号解読に高等数学は不要で、アメリカ大使館の使用していたストリップ暗号は盗写工作で読んでおり、エニグマのような機械暗号を使用している敵性国家も無かったため、広瀬の卓見は時代に先駆けたものであったが、環境が整っておらず不発に終わった。

開戦後間も無く、スウェーデン駐在陸軍武官の小野寺信は、精密機械製造会社の社長ベックシェフトから「米英仏が500台ずつ当社の暗号機械クリプトテクニークを購入して使用している。アメリカに勝つためには日本も購入しなさい」と商談を持ち込まれた、という情報を参謀本部に通報した。参謀本部通信課暗号作製班は、これを3台購入するよう依頼し、下交渉を広瀬栄一が行った¹²⁾。暗号機械クリプトテクニークは1942年春に届き、暗号作製班で検討を行ったが、原久は「アルファベットで暗号強度に不安があり、手動機械は速度が遅く、スパイ用暗号以外には使用不適当である」と結論を下した。しかし第十八班は、実際の暗号解読に忙殺されていたため、使用されているかどうか不明なクリプトテクニークの解読研究に本格着手せず、第五技術研究所に保管された。クリプトテクニークは、ピンと紙を操作することで1億以上の乱字を得られる画期的な暗号機械であるが、米軍が日本との戦線に投入するのは2年後のことであり、第十八班の判断にはやむを得ない点があった。しかし、研究人員を割かなかつた第十八班が怠慢であるという批判は成立する。敵性国家がどのような暗号運用を行い、どのような研究を進めているかの情報は、高度な国家機密に属する事項に該当するため、通常知ることが困難である。参謀本部暗号班は、Yardleyの暴露で米英が暗号解読機関で“秘密インクや小型カメラなど”に代表される謀略器材の研究を進めていることを知るや、謀略器材開発を一貫して手掛けた陸軍技術研究所の篠田鎌(1894.1.25-1979.8.5)を暗号班に兼任させてこの方面の充実を図り、暗号通信に無線電信が主流になりつつあることを察知すれば、陸軍の電波関係の権威である三木勝一を暗号班に兼任させるなど、“研究の外部委託”による適切な対処を行っていたにも関わらず、“研究が外部委託できない”機械暗号解読については適当な処置を行ったとは言い難い。クリプトテクニークによって作成された暗号の解読には数学的知識が不可欠であるが、第十八班はその結論に到達するに至らず、問題を棚上げした。

1942年3月、釜賀一夫は参謀本部付のまま陸軍科学学校普通科に入校し、土曜日のみ参謀本部に出勤した。学生となって自由時間が増えた釜賀は、陸軍科学学校では字差(暗語を構成する数字群のうち、同一位置における数字の異なることを指す)の研究を進めた。釜賀の字差理論研究は、日本における符号理論の先駆である。釜賀がこの研究に着手した目的は明らかではないが、空電によって生じる暗号電文のノイズ除去に関する数学的理論の構築が理由の一つであったことは確かである。

1942年5月7日、日本軍はコレヒドール要塞を占領した。この際、米軍が暗号解読に利用していたIBM統計会計機405型を鹵獲したが、陸海軍ともにIBM統計会計機405型の鑑定に手間取り、これが暗号解読に利用されていたことに気付いた者は、鑑定した数学者や技術者を含めて、恐らくは戦後まで皆無であった¹³⁾¹⁴⁾。IBM統計会計機405型は、暗号通信文中にある反復調査に利用可能であるが、日本側は暗号解読に計算器械を導入していなかったせいも、全くの想像外であったと推測される。陸軍兵器行政本部技術部長の小池国英中将(1892-1959)は、「アメリカには計算機があるくらいだから数学を使っているらしい。日本でも集めたらどうか」と、電気試験所第三部長兼第六部長であった山内二郎(1898-1984)に持ちかけたが、数理統計学に造詣が深かった山内は、数理統計学者を集めて品質管理の実際の方面に進んだ¹⁵⁾。

1942年末、釜賀一夫は、字差理論研究にFermat最終定理研究の第一人者である森嶋太郎教授の助力を得た。釜賀は、森嶋の数学的能力に感嘆し、陸軍暗号強化の研究には数学者の助力が必要である、と論理的に推論するに至った。

釜賀は、雀部峻三教授(1900.2.02-?)の斡旋で、高木貞治(1875-1960)と接触した。釜賀が、「高木の下に数学者を集めて協力して頂けないか」と(恐らくは低姿勢で)持ちかけたところ、高木は拒絶せず、「役立つかどうかわからない。考えさせて欲しい」と言質を与えなかった。高木を再訪した釜賀は、「暗号については全く知らないで、一度、役立つかどうか話を聞かせて欲しい」という回答を得ている。「暗号については全く知らない」という高木の発言は、厳密には偽証である。高木は、1937年に海軍技術研究所の田辺一雄技師が開発した九七式印字機の性能試験を引き受けている¹⁶⁾¹⁷⁾。田辺技師は、九七式印字機を開発したものの、どの程度の組合せがあるものか不明確であったため、最終的に整数論の権威者である高木に相談した。高木は、「兆以上の変化のあることは間違いないが、それ以上の正確な計算はちょっと出ない」と回答し、結果、九七式印字機が海軍・外務省で採用されたという経緯がある。高木の結論は正しいが、九七式欧文印字機による暗号はアメリカのWilliam Frederick Friedman(1891.9.24-1969.11.12)によって解読された。

広瀬や釜賀と独立して暗号に数学が必要だと判断した陸軍軍人は、他にも存在した。1943年初頭、軍部が奥多摩に民間の科学者を集め、話を聞く会が設定された。暗号関係として名古屋大学教授の小野勝次、歯車の最高権威である東北大学教授の成瀬政男などが招かれたという。血気盛んな論調でマスコミに顔が知られ、統計会計機開発に関係していた小野を暗号関係者として選抜した陸軍の担当者は卓見であったが、このルートは立ち消えになった。暗号機械開発に経験がある陸軍兵器行政本部が、第十八班・参謀本部通信課とは独立に話を進めようとしたのであろう。暗号関係で呼ばれたことについて小野は、「自分を呼んでも仕方がない」というニュアンスで回顧しているように、Turingの対置物として活躍することは無かった。

1943年3月、釜賀一夫は陸軍科学学校を卒業し、参謀本部通信課に復帰した。

1943年7月、参謀本部第二部第十八班が陸軍中央特種情報部に改組された。初代部長は、第十八班長の中野良次少将が就任し、参謀本部の外局となったことで、暗号解読組織の人員・組織が拡充された。

1943年8月、参謀本部第三部通信課の課長に通信課高級参謀の仲野好雄大佐(1903.2.5-99.1.20)が昇格した。釜賀は、暗号強度を向上するために、民間数学者を集めて数学研究会を組織することを計画したが、それまでは上層部の反対で実現していなかった。仲野は、通信課長に就任した際、この問題に早速着手した¹⁸⁾。「東大の教授から各大学の数学の天才を集めて、陸軍暗号を堅くする研究をしようという上司に持ったんだ。そうしたら、若松閣下(註・若松只一第三部長)も反対されました。参謀次長は、もちろんいかんという。そこで私は、このままじゃ暗号の責任持てません。手や足は学者に研究させますけれども、ある所からは上は参謀本部の通信暗号参謀にやらせます。もしものことがあれば、私が腹切りますと。貴様が腹切るというならということで、やっと許してもらったんだ」と仲野は回顧しているが、数学者動員に一番強く反対したのは暗号解読の責任者であ

る中野良次陸軍中央特種情報部長であった。機密漏洩を恐れて強硬に反対した中野良次の主張は、戦後裏付けられた。

1943年夏から10月まで10回程度、釜賀は「数学の特に必要だと思われる暗号」、「暗号の基礎から関連の未解決問題」について数学者に対する講習の席を設定した。高木貞治は、当初東大数学科出身の数学者である彌永昌吉、小平邦彦、河田敬義、岩澤健吉を伴って出席している。講習の結果、数学者は暗号研究に協力可能だという結論が導かれたという。出席した数学者の人は、恐らくは彌永昌吉によるものである。

1943年秋、釜賀は暗語構成上の非重複文字数を調べ、重複のない語に同一原語群を配当する方式を確立した。現在、「誤り訂正符合のハミング距離の理論」に相当するものである。釜賀は、この研究を敷衍して、「字差概論」という論文を完成させた。「字差概論」は符号理論における先駆的成果であり、高木貞治と彌永昌吉は博士論文としての提出を薦め、合格を保証した。しかし、博士号取得には論文審査の他に語学試験もあり、釜賀は語学試験を受けるほどの時間的余裕が無かった。

1943年11月、同年9月に東大数学科を卒業した山本幸一(1921.5.11-91.4.23)が、彌永昌吉の推薦で陸軍技手となり、参謀本部通信課に配属された。当時、徴兵検査で合格した数学科学生は卒業後に陸軍技術将校・海軍数学教授として後方に残る事例が多いのであるが、文官として参謀本部に勤務したのは山本だけであろう。なお、陸軍における文官の身分は、技師(高等官)・技手(判任官)・雇員・傭員の4階級制に分かれており、帝大卒が技手に就任するのは通常の人事である。

1943年12月、海軍軍令部では、海軍暗号解読の専門家で、予備役少将の伊藤利三郎・中杉久次郎を充員召集し、特務研究室を設置した。研究室では、海軍大学校教授の山梨進一(1908-2001)、東京文理科大学数学科助教授の尾崎繁雄を含む数学者・言語学者約20名が動員されてストリップ暗号の研究に従事した¹⁹⁾²⁰⁾。反復調査機を設置し、ストリップ暗号の正攻解読に従事したが、解読には成功しなかった。山梨は、陸軍が先に優秀な数学者を動員したので、自分のような人材が引っ張り出されたのだ、と語ったとされている。日本における数学者の戦時研究動員は世界的に見ても遅く、1943年初頭から本格的に開始されたのであるが、その動員主体は陸軍・学術研究会議・大日本航空技術協会であり、海軍は出遅れた。このため、海軍軍令部が暗号研究に数学者を動員しようと企図した時点で、主要な数学者の大半が払底していた。

1944年1月、豊橋予備士官学校を卒業した東大数学科卒業生の福富節男少尉は、中央特種情報部に配属された。この配属に当って、豊橋予備士官学校の上官は、「諸君は軍中央において勤務するの光栄に浴し…」という訓辞を福富に垂れたが、福富は光栄という気分を感じなかった。しかし、「暗号解読はクイズより複雑で数学めいた所もあり、米暗号の解読という仕事に、かなり力をそそいだ。当時東京に母たちと暮らして、情報部という役所への往復の電車の中でも、暗号のキイのことを考えていた」と回顧している²¹⁾。

1944年4月3日、暗号強化を主眼として陸軍数学研究会が発足した²²⁾。陸軍数学研究会の委員名簿は以下の通り。

表 1. 陸軍数学研究会委員

| 研究会職名 | 現職 | 官位 | 氏名 |
|-------|-----------------|------|-------|
| 会長 | 大本営陸軍部第三部長 | 陸軍少将 | 額田 坦 |
| 副会長 | 東京帝国大学名誉教授 | 理学博士 | 高木 貞治 |
| 幹事長 | 大本営陸軍部第十一課長 | 陸軍大佐 | 仲野 好雄 |
| 幹事 | 大本営陸軍参謀 | 陸軍少佐 | 金子 昌雄 |
| 委員 | 陸軍中央通信調査部第一課長 | 陸軍大佐 | 吉川 猛 |
| 同 | 陸軍兵器行政本部技術部技術課長 | 同 | 野村 恭雄 |

| | | | |
|---|----------------|------|--------|
| 同 | 第五陸軍技術研究所第一科長 | 陸軍中佐 | 植田 正一 |
| 同 | 陸軍航空本部技術部航空器課長 | 陸軍大佐 | 有森 三雄 |
| 同 | 第四陸軍航空技術研究所長 | 同 | 山崎 武夫 |
| 同 | 陸軍科学学校陸軍教授 | 理学博士 | 森島 太郎 |
| 同 | 陸軍予科士官学校陸軍教授 | 同 | 成実 清松 |
| 同 | 同 | 陸軍中尉 | 加藤 武四 |
| 同 | 同 | | 酒井 政雄 |
| 同 | 同 | | 小島 浩 |
| 同 | 同 | | 渡辺 武 |
| 同 | 同 | | 小松崎 均 |
| 同 | 東京帝国大学教授 | 理学博士 | 彌永 昌吉 |
| 同 | 同 助教授 | | 小平 邦彦 |
| 同 | 東北帝国大学教授 | 理学博士 | 泉 信一 |
| 同 | 大阪帝国大学教授 | 同 | 清水 辰次郎 |
| 同 | 同 助教授 | 同 | 角谷 静夫 |
| 同 | 東京文理科大学助教授 | | 河田 敬義 |
| 同 | 大阪高等学校教授 | | 掛谷 金二 |
| 同 | 中央航空研究所研究官 | | 古屋 茂 |
| 同 | 藤原工業大学講師 | | 岩澤 健吉 |

陸軍部内暗号機関委員委員

| | | | |
|----|-------------|--------|-------|
| 委員 | 大本營陸軍部第十一課 | 陸軍少佐 | 保坂 豊和 |
| 同 | 同 | 陸軍大尉 | 藤原 邦樹 |
| 同 | 同 | 陸軍技手 | 山本 幸一 |
| 同 | 陸軍中央通信調査部 | 陸軍大佐 | 中野 勇 |
| 同 | 同 | 陸軍少佐 | 原 久 |
| 同 | 同 | 陸軍少尉 | 山本 純恭 |
| 同 | 同 | 同 | 谷口 敬治 |
| 同 | 第五陸軍技術研究所 | 陸軍兵技大尉 | 桑田 正信 |
| 同 | 第四陸軍航空技術研究所 | 陸軍中佐 | 村岡 勝 |

新に委員に加はりしもの

| | | | |
|--|--------------|----|-------|
| | 陸軍航空通信学校陸軍教授 | | 高崎 光久 |
| | 通信院工務局機械係長 | 技師 | 鳥海 登 |
| | 中央气象台報道課長 | 技師 | 石丸 雄吉 |

| | | | |
|--|--------|------|--------|
| | 陸軍気象部付 | 陸軍中尉 | 土井 喜久一 |
|--|--------|------|--------|

特に研究に加はりしもの

| | | | |
|--|---------|------|-------|
| | 陸軍科学学校付 | 陸軍少佐 | 釜賀 一夫 |
|--|---------|------|-------|

研究会の人員構成は、様々な事情を考慮したものである。

会長の額田坦は、参謀本部通信課長の直屬上官であるという理由で選出されたものであり、暗号専門家ではないため、形式的存在である。

高木貞治は、数学者側の最高責任者であり、階級としては大将相当待遇であったため、副会長に就任したと判断される。既に大学を停年退官し、第一線の数学者と日常的に接触しない環境にあったこともあり、半ば名目的な存在に位置し、愛弟子の彌永昌吉が副会長代理の権能を果たしたと推論される。

幹事長の仲野好雄は、陸軍数学研究会設立の推進者であり、研究会の陸軍側における実質的な責任者である。工兵出身の仲野大佐は暗号専門家ではないため、研究会は幹事長が全ての方向性を決めるトップダウン型ではなくボトムアップ型の意志決定スタイルをとることになる。

幹事の金子昌雄は、参謀本部通信課暗号作製班の責任者で、陸軍数学研究会の研究の方向性を決定する立場にあったが、暗号将校ではなく通信将校であったため、研究内容に対して立ち入った数学的理解をしていたとは言い難い。但し、金子が研究会の為すべき著作編述内容として構想策定した一覧は、ともすれば目先の業務に囚われがちな将校に高次な目標を設定するものであった。

委員の吉川猛は、陸軍中央通信調査部(陸軍中央特種情報部の秘匿名)の高級参謀で、中野良次少将の意向を代弁する立場にあった。陸軍中央特種情報部には吉川と同じ大佐の将校もいたが、彼らは陸軍士官学校卒業年度が仲野好雄幹事長より上であるため仲野の下に配置するのに不都合があり、バランスをとって陸士同期生の吉川を委員会に加えたものと見られる。

野村恭雄・植田正一・有森三雄・山崎武夫は、陸軍における兵器技術関係の優秀な電気工学と機械工学の研究責任者で、彼らに機械暗号研究に協力を要請しなければならない場合の布石として選出されたものと見られる。しかし、この4名は兵器開発の本業に従事しており、現実的には委員会に対して全面的な協力を行える環境には無かった。

森嶋太郎・成実清松・加藤武四・酒井政雄・小島浩・渡辺武・小松崎均・高崎光久は、陸軍が擁する数学教官であるが、森嶋と成実以外は、数学史に名を残す人材とはいえない。

古屋茂は、航空力学の研究者と共同研究を行い、流れの統計的性質の数学的研究における第一人者として知られた人物である。

清水辰次郎は、東大数学教室助手から阪大教授に就任した応用数学者で、この頃は非線形振動論・計算器械研究を行っていた。学術研究会議その他における戦時研究の主任者も兼ねていたため、暗号研究に全力投球できる立場には無かった。

泉信一は、戦時研究への熱心さでは最右翼にあった解析学者で、フーリエ解析のほぼ全分野において精細で深い研究を行っていた。

角谷静夫・掛谷金二は、清水辰次郎と地理的に近いことから陸軍数学研究会に参加したと推論される。

保坂豊和・藤原邦樹・山本幸一は、参謀本部通信課暗号作製班のスタッフである。藤原は数学者側との折衝に従事したが、数学者に問題を提出するに当っては釜賀一夫に全面的に依存したという。

中野勇・原久・山本純恭・谷口敬治は、陸軍中央特種情報部の暗号解読将校である。

桑田正信・村岡勝・鳥海登は電気工学の研究者で、電波傍受などの研究に従事したと推測されるが、彼らも本務の兵器開発に従事しており、暗号研究に本格着手できる環境ではなかった。

石丸雄吉は気象学者、土井喜久一は自然地理学者で、気象暗号解読に必要な能力と人脈があった。後年、仲野好雄は「大東亜全域の気象予報に成功」したと記述しているが、これは各国の気象暗号解読によって為したものであり、特に石丸の貢献が大きい。

陸軍暗号の硬度強化を目的としていた陸軍数学研究会は、一つの到達点である無限乱数暗号を導入している以上、立ち遅れていた暗号解読に重点が移行するのは必然的であった。しかし数学者の研究内容が数学的に高度であればあるほど、これを理解できる陸軍の人材が限定される。陸軍の数学教授を除けば、中野勇、原久、釜賀一夫、数学科出身の山本幸一・山本純恭の5名がその人材であるが、数学者の成果を利用できるレベルに引き下げ、或いは暗号学上の直面した問題をある程度数学的に定式化して数学者に提示できる人材は、数学と暗号学の双方に通じた釜賀一夫ただ一人であった。故に、研究会の成功の可能性は、釜賀に大きく依存した。

数学者が暗号解読に関与するのは、1944年7月9日のことであった。陸軍中央特種情報部研究部長の中野勇が、当時東大物理学科の員外学生であった釜賀一夫の下宿を訪問し、「1943年10月から米軍が新暗号を使い出した。暗号機械クリプトテクニークを使用しているらしい」と、クリプトテクニークと傍受暗号文約500通を渡し、解読への協力を依頼して帰った。釜賀は、東大が夏休みだったので直ちに解読研究に着手し、山本幸一を下宿に呼んだ。釜賀と山本は暗号の数学的問題を話し合える関係で、山本の死まで交流は続いた。釜賀と山本は、アリューション方面からの暗号文を検討し、クリプトテクニーク固有の特徴と一致していることから、米軍がクリプトテクニークを使用しているものと判断し、クリプトテクニークで暗号文を作成して解読法を研究することにした。結果、乱字が100字程度判明した場合、その際のピンと銚の組合せを解く方法を開発した(約10の50乗ある組合せ数のうち1種類に特定できる)。更に、同一の組合せを使用した他の暗号文に対し、どこの部分の乱字が適用されたか知る方法(乱字の開始位置解析)を提案した。この時釜賀が個人的に購入したタイガー計算機が、この解読のための計算(Eulerの解法等)に威力を発揮している。ここまでを二人は7月10日から14日までの短期間で電撃的に遂行し、15日には中央特種情報部で報告した。釜賀と山本の成果は、暗号学者と数学者(大学卒業程度の学力をもつ)の共同研究による画期的なものである。山本は、「終日血走った眼で、指に血豆を作りながらタイガー計算機に取り組んだ」という²³⁾。

この直後、陸軍は釜賀を繰上げ卒業扱いとして、第7技術研究所研究員を命じ、輸送用潜水艦の潜望鏡の設計に従事させた。釜賀は、研究所に出勤しながら、帰りには中央特種情報部に立ち寄って、暗号解読だけでなく解読教育も行った。

1944年7月23日、南方軍特種情報部が米ビルマ方面航空部隊の通信を傍受し、その暗号文を飛行機で中央特種情報部に送付した。この暗号文は、同一の乱字を8回使用していることまで解明したが、クリプトテクニークによる暗号文と仮定して解読を行ったものの、解読できなかった。この頃、南方軍から「暗号兵を捕虜にした」という連絡があり、中央特種情報部はマニラ捕虜収容所に岩田実少尉(-1988)を派遣し、暗号兵を尋問した。

1944年8月1日10時頃、岩田少尉がマニラから帰国して伝えた尋問結果により、同日14時30分に西岡勝彦少尉が米ビルマ方面航空部隊による暗号の原文解読に成功した。クリプトテクニークは暗号文組立ての際、単語と単語の間にXの字を使用し、

翻訳の際には自動的に X を消して印字するため、X が通信文の単文字度数の最高頻度になる。しかし、米軍の暗号機は、単語と単語の間に Z の字を入れるように改造していたことが訊問から判明し、Z が通信文の単文字度数の最高頻度になると仮定して暗号を解読した。

米軍暗号の解読文から、使用された乱字が特定されたが、これはクリプトテクニークによって得られないことも判明した。釜賀と山本は「米軍暗号機はクリプトテクニークを原型として、ピン・鋸等を変更した」と推論した。山本は、クリプトテクニークの暗号原理を数式で表現して、もし自分が改良するなら数式をどう変更するかを思考実験し、これを米軍暗号機の示す乱字と対比して、米軍暗号機の模造品を完成させた。事実米軍は、クリプトテクニークを改良して暗号硬度を高め、M-209 という呼称で使用していたが、山本の研究は米軍の改造を正しく見極めたものであった。陸軍は、M-209 による米軍暗号を、“Z 暗号”と呼称することにした。

釜賀・山本の成果を受けて、陸軍数学研究会の数学者もまた、暗号解読の研究を委託されることになった。基本的には大学数学科の課程を終了しただけの山本が、半年以上解読不能であった米軍暗号に対して画期的な成果を挙げたのであるから、数学専門家かけられる期待は当然大きかったはずである。

1944 年 11 月、清水辰次郎が「IBM 統計会計機 405 型が暗号解読に役立つのではないかと提案したことを受けて、陸軍数学研究会幹事長は、第一生命保険と日本生命保険が保有する IBM 統計会計機の微発令状を送付した²⁴⁾。両社は、IBM 統計会計機 405 型が微発されれば経営に差し支えると反対したため、陸軍は使用したい時に保険会社に出向いて利用する形をとった。結果としては、暗号解読に画期的な展望を開くものであったという。現代の視点から見れば、計算機を暗号解読に利用することは自明な考えであるが、当時の日本では計算機を科学計算に使用し始めた時期で、陸軍側が計算器械の利用に思い至らなかったのも不可解ではなかった。そして、当時の日本の数学界で計算器械そのものを研究対象とする数学者は小野勝次・清水辰次郎・城憲三・近藤基吉など 5 人以上 10 人未満と貧弱で、彌永昌吉・小平邦彦ら純粋数学者は、そもそも計算器械の暗号解読への利用を思い立つ思想風土にはなかった。

同月、陸軍暗号学理研究会は機関紙第 1 号を発刊した。その中で、高木貞治・彌永昌吉はラテン方陣を、河田敬義はある洋書の単文字度数の頻度分析を、小平邦彦は釜賀の字差研究の展開、岩澤健吉は乱数生成法のラフな提案を論述しているが、河田・泉・清水の成果を除いてはさほど見るべき内容とは言い難い。

1945 年 1 月、フィリピンに派遣されていた中野勇が戦死した。

1945 年 1 月以降、東京文理大学の数学科学生が、陸軍中央特種情報部に学徒動員されて暗号解読に従事した。河田敬義の引率で動員された中には、この件について書き残した中岡稔がいるが、中岡は健康上の問題で早期に暗号解読から離れたので、詳細は不明であるという²⁵⁾。

1945 年 4 月、東大理学部物理学・数学・天文学教室は長野県に疎開した。この疎開は、1945 年 2 月に小平邦彦が物理学教室の疎開を提案したことに端を発する。物理学教室の疎開が決定すると、一年生の授業が重複する数学教室・天文学教室も疎開に合流することになったという²⁶⁾²⁷⁾²⁸⁾。長野県は、陸軍の研究機関の疎開先でもあり、理学部の学生はこれらの研究機関に多く動員された。東大数学教室では、茅野に疎開した二年生が“参謀本部数学研究室”名義で疎開していた陸軍中央特種情報部諏訪分室で暗号解読に動員されることになった²⁹⁾。二年生は、上川畔の酒井家(休業中の銭湯)の 2 階と小川家(休業中の料理屋)の 2 階に分宿した。物資不足のために両家は休業中で、入浴のためには汽車で隣の上諏訪まで行く必要があったが、宿泊費と食費は軍が支給していた。

小川家に宿泊したのは、稲田獻一、小西弘、竹内外史、田中実、西村広隆、浜田一巳、一松信、森明、門馬直美の9名である。

酒井家に宿泊したのは、近藤芳夫、柴田敬一、高島巳千雄、竹之内脩、玉河恒夫、長田潤一、鍋谷清治、本田欣哉、武藤徹、山辺英彦の10名である。

本田欣哉は、「4月から8月の終戦までの数か月間は、食糧事情の悪さなどで、苦しいといえば苦しい生活でしたが、同級生たちと一緒にくらすわけですから、戦時下とはいえ奇妙な明るさや楽しさもある日々でした」と記述している³⁰⁾。

鍋谷清治は、「酒井家での通常の食事は、大豆または甘藷入りのご飯が軽く1皿に漬け物が少々」、「(武藤徹)が時々カレーライスを作ってくれて、それが一番のご馳走でした。材料をどうして手に入れたのか、全く覚えていません」と語り、長田潤一は、「兎も角、空腹で空腹で、栄養失調のため、道をまっすぐに歩けなかったこと、食事のことで山辺君ともう一人の学生がけんかしたことをかすかに記憶し、小西弘は、「諏訪で差し入れのカルピスが旨かったこと、ところてんを食べ過ぎて(?)大きいできものが出来たこと」を覚えているという。

東大航空研究所佐々木達治郎研究室と参謀本部数学研究室が疎開した宮川国民学校(現在の茅野市立宮川小学校)で、小平邦彦はルベーク積分、彌永昌吉は幾何学、岩澤健吉は代数学の講義を行ったという。

学生の暗号解読能力が余り向上せず、岩澤が練習問題を作成して解読させたことがあったが、解読結果はLev Semyonovich Pontryagin『*Topological groups*』の序文の一部であったという。こういった演習に対して、「この暗号は普通の推理小説にも出てくるような単純なもので私自身既に解読法を知っているようなもの」と小西弘は評している。

釜賀一夫と藤原邦樹は時折茅野に訪れ、研究会を諏訪市にある上諏訪温泉の通信省寮で開いた(現在のNTT上諏訪保養所・鷺湖荘)。諏訪に疎開していた彌永、小平、岩澤、東京から来た高木貞治、河田敬義、古屋茂、山本幸一が参加したという。

この席上で釜賀は、米軍捕虜の尋問による情報として、米軍で使用していたZ暗号とストリップ暗号を紹介した。この二種類の暗号解読を、酒井組・小川組がそれぞれ担当している。

二年生は、午前中は教官と離れて暗号解読に従事し、午後は数学の講義を受けた。

一松信によれば、解読内容は同盟通信社による沖縄戦の情報やルントシュテット攻勢の外電の概略などで、「本当に仕事をしたんでしょうか?」、「その後の資料から判断すると、我々の作業は「ドンキホーテ」にすぎなかったという印象がぬぐえない」と述懐する程度のものであったようである。

小川家組の担当したZ暗号は、竹内外史による基本構想を森明が発展させた解読方法で、竹内曰く「大体において解ける様になっていました。(同じプログラムで作った暗号が何通かあるという假定のもとに)」。竹内・森のZ暗号に対する貢献について、稲田獻一は存在を知っていたが、小西弘・一松信は同じ組に配属されていたにも関わらず記憶がないと証言している。一松信は、「暗号の解析法を五十字ぐらいでやる方法を疎開先の諏訪の研究会で発表したことがあるが、暗号解読を適当に済ませていたということである。山辺英彦は、「ストリップ暗号の解読法に画期的な方法を考え出してくれた」。

酒井家組によるストリップ暗号解読は、極めて熱心な武藤徹・竹之内脩・「ストリップ暗号の解読法に画期的な方法を考え出してくれた」山辺英彦や、「不熱心な方のトップ」で命令以上のことは何もしなかった長田潤一など当事者の熱意は一樣ではなかった。玉河恒夫は、ストリップ暗号について「原理は簡単なのですが解法はむづかしく」、「遂に実用になる迄にはいかなかったようです」と証言している。

1945年7月から、二年生は連日上諏訪に列車で通勤するようになった。この頃、福富節男が暗号解読のスタッフとして上諏訪

に滞在している。

1945年8月11日、陸軍中央特種情報部は、日本がポツダム宣言受諾を決したことをシドニー放送から把握した。その日の夕方から、各出張所を含めて、暗号関係の資料と暗号解読関係の機械処分に移った。

1945年8月15日、東京の陸軍中央特種情報部は玉音放送を聞き、その場で一人残らず全国に散って地下に潜伏した。

同日朝、長野県では、武藤徹が茅野の宿舎から諏訪分室のある諏訪に向かう途中、大東亜省に勤務する公務員の叔父に偶然会った。武藤の叔父は、昨日の御前会議でポツダム宣言を受諾して和平が決まったと言って立ち去った。諏訪分室では、「書類など可燃物は全て焼却し、不燃物は諏訪湖に投棄せよ」という指示のもとに証拠隠滅が進んでいた³¹⁾。

彌永昌吉と東大二年生は、諏訪分室の庭で玉音放送を聞いた。粗悪な録音状況と難解な言回しもあって、小西弘は、「戦争が終わったのか、もっと竹槍で頑張れということなのかよくわからなかったというのが本音」で、「どうも大多数の友人も同じだったと記憶している」。

鍋谷清治の証言によれば、玉音放送を聞き終えた彌永昌吉は、開口一番に「これで戦争が終わっておめでたいのだが…」と発言し、午前まで暗号解読に従事していた二年生達に衝撃を与えた。

一松信は「やっとこれで、数学が勉強できるようになりましたね」と彌永が語ったと記憶しており、「さっぱりした」と考えた一松信を含む学生の一部は憤慨したという。

武藤徹の証言では、放送後に彌永が、「めでたし、めでたし。これで、また世界の人が仲良くなれる」と語ったが、学生の中には泣いた者もいたという。武藤自身は和平を喜んだが、めでたいという気分からはかけ離れていた。

彌永本人は、終戦の知らせが「私には、本当に嬉しかった。'研究'の結果は、ただちに破棄した。同時に、私も戦争協力者ではなかったか、戦争犯罪者ではないのか、という思いにさいなまれた。せめて、これから戦争などというものないように、できるだけのことをしなければ、と思った」と記述している³²⁾。

放送後、原久が藤原邦樹に指示して、諏訪分室にあった資金全てを、「協力と尽力とに対するお礼として」全員に分与した。将校は米を俵で運び出し、数学科学生は方眼紙の残ったものを何十枚か分与された。

米俵を確保し、地下に潜伏する計画を立てていた釜賀一夫らの下に、山辺英彦が2、3回来訪して「山に閉じこもって米軍の暗号を取り解読しよう」と提案した。米軍が上陸したら何をするか分からないが、情報を掴んでおけば、何とか手が打てる、どうしてもひどいことをするときには反撃しましょう、と具申したという。これは実現することなく、原は北海道に、釜賀は九州に潜伏した。

数学者は、こうした悲嘆・衝撃からは自由であったようである。矢野健太郎によれば、疎開していた東大の数学者と物理学者は、直ちに、「戦争直前まではわれわれの良く知っている外国の研究が、この戦争中にどのような方面に進んだであろうか、また戦争中孤立していたわれわれの研究が、外国のそれと同じ方向をたどったであろうか、またちがう方向をたどったであろうか、さらにまた同じ方向をたどったとすればこちらが進んでいだろうか」と議論したという³³⁾。

小平邦彦は、「必勝であるといっていた戦争に負けても別に何の騒ぎも起らなかった。皆内心必敗と思っていたのであろう」と冷めた記述を残している。

戦後の展開

1945年8月16日、福富節男は東京の中央特種情報部に出勤すると、経理将校に退職手当として100円を手渡され、上級将校らが、金のほかにトラックに米・味噌・砂糖のような物資を積載して姿を消したと聞かされた。

1945年9月5日、参謀本部第二部長の有末精三がGHQの訊問を受け、中央特種情報部について質問された。その数日後に、中央特種情報部第二代部長の西村敏雄が喚問されたが、数学者の動員に関しては一切漏洩しなかった³⁴⁾。

1945年9月20日から10月25日まで、参謀本部通信課長の仲野好雄、暗号作製班長西田寿雄、一般暗号担当の円山秀男が、文書の往復による調査のほか、21回の直接面談で陸軍暗号について訊問を行った。この時も、数学者の動員については口外しなかった。

1945年9月28日、東大校舎が占領軍の使用候補から外れたことにより、二年生以上の学生は動員を解除して帰校させ、一年生もひとまず東京へ集めることになり、月末までに数学教室は東京に引揚げ、学問に戻る事になった。

1946年1月、陸軍次官秘書官となっていた広瀬栄一が巢鴨プリズンに収監され、暗号解読に関する訊問を受けたが、米軍暗号を解読するだけの能力を、日本陸軍は持っていなかったとGHQに印象付けた³⁵⁾。

1946年3月24日、スウェーデンから帰国した小野寺信は、即日巢鴨プリズンに収監され、「お前はアメリカの暗号を盗んだな」と問い詰められたが、知らないと回答した。小野寺がクリプトテクニークを購入した件に関する質問であったと推測されるが、日本で暗号解読の状況を知らなかった小野寺は、クリプトテクニーク購入についても証言しなかったようである。

1946年4月、山本幸一は東京帝国大学理学部大学院に入学し、末綱恕一の下に戻って「不足だった勉強を補う事にした」³⁶⁾。

数学者の戦時協力の露見

1948年10月、日本陸軍が米軍暗号を解読していたという情報が、GHQに漏洩した。漏洩の経過には、竹内外史と釜賀一夫による2種類の証言がある。竹内によれば、「山辺英彦が、占領軍の者とブリッジをしながら戦時中に米国の暗号を解読していたことを漏洩したため、CIAが山辺を召喚して事情聴取を行った。山辺がオーガナイザーとしての彌永と活躍した竹内の名前を告げたため、彌永・山辺・竹内が召喚されて事情聴取を受けることになった。この時点で既に、竹内は自分の研究を記憶していなかった」というものである。釜賀によれば、「山辺英彦が、芦屋の実家で米軍機械暗号を解読した経験を話し、東京女子大学に通う妹・山辺朝子が友人にそれを伝え、その友人が、米軍の二世の中尉と結婚して、寝物語に「私の友人の兄はアメリカの暗号を解読していたようだ」と話したため、中尉は翌朝に朝食も摂取せずに司令部に報告に及んだ。そこで、まず山辺が呼び出され、それから合計して数学者8名へ出頭命令が下されたという。出頭した数学者は、陸軍暗号の中心人物である原久と釜賀の名前を挙げた為、米軍は二人に出頭命令を下した”。

1949年1月、潜伏していた原久と釜賀一夫はGHQに出頭し、「ソ連が勝って日本に入るようなことになったら大変だから、どうせならアメリカに勝たせたい。そのためには、アメリカの暗号の悪いところを全て教えて、アメリカの暗号を強くしてやろう、ということ二人の話は一致し、M-209の解読について率直に証言した。潜伏期間を終えた原と釜賀は、この後陸上自衛隊の暗号部門に就職し、数学研究会の関係者を訪ねて歩いた。

気象学者・石丸雄吉は「陸軍数学研究会」の会誌第1号と、藤原邦樹の編纂になる「乱数式暗号学理」を、彌永昌吉は「字差概論」を焼却せずに保管しており、これを釜賀に引き渡した。防衛庁は、この3冊の復刻版を作成して参考資料としたが、後に「乱数式暗号学理」と「字差概論」は口語文に改め、若干修正して再版した。

釜賀が山辺英彦と学会で再会した際、山辺は「自分が戦時中に考えたストリップ暗号の解読法は、戦後もずっと考えていたが、やはり正しい」ということを、夜を徹して語り合ったという。

数学者の協力状況について

陸軍数学研究会に關与した数学者は、暗号解読に關する協力についてほとんど何も書き残しておらず、情報は極めて少ない。

參謀本部通信課長であった仲野好雄は、陸軍数学研究会の数学者による研究成果を、

倍数方式字差暗号の数に關する研究

字差暗語の構成基礎原理に關する研究

Euler 方陣及びピラテン方陣に關する諸研究

反復の形態と之が統計的處理

反復の分散に關する理論的研究

エニグマ式暗号機の配線解析に關する研究

機械暗号に於ける置換群の研究

Z 暗号機乱字解析の研究

ストリップ暗号の周期判定に關する研究

ストリップ暗号の抜取判定に關する研究

合成乱数(字)の解析に關する方程式の解法

機械暗号の解読研究

暗号に於けるフーリエ級数の利用

2 進法暗号機に關する研究

に分類し、これに通信課暗号作製班の研究成果と結合して、「字差概論」、「乱数式暗号学理」、「機械暗号の原理と解読」、「Z 暗号及ストリップ暗号解読の原理」、「反復の理論」などを極めて短期間にまとめたが、「字差概論」を除いて全て終戦時に焼却されたとした上で、数学研究会の成果を極めて高く評価し、数学者たちへの感謝の念を露わにした³⁷⁾。これは、釜賀一夫の回顧とも共通している。

しかし、数学者側の証言は、陸軍側の証言からは大分異なる側面を見せるものであった。

高木貞治は、1944年2月に、「数学遊戯として有名であったオイレル方陣の問題は、近頃思いもかけない或る實用問題と密接なる關係にあることが指摘されて、とみに興味を覚えたのである」と語っており³⁸⁾。彌永昌吉と Euler 方陣の研究を行ったが、年齢的に研究能力が下り坂にあったこともあり顕著な貢獻をしたとは考え難い。山梨県谷村町に疎開していた高木は、戦後間もなく、東大理学部对学生に対して「整数とは何か」という講話を行うべく長野に宿泊しているが、この時に物理学科の学生である藤井弥平が茶を振舞っている。

「君はいつもお茶を立てているのですか」と質問する高木に、藤井は「そういうわけではありません。今日は特別です」と答えると、「私のためにやってくれたのですね。平和っていうのは素晴らしい。平和っていうのは」と高木は返したという。この会話から、高木が敗戦という状況を、むしろ喜んでいと見ることができる。

彌永昌吉は、戦時研究に対して「少なくとも私自身や私の周囲では、それほどお役に立つほどのことはできなかったように思います」と、低い評価しか与えていない³⁹⁾。

小平邦彦は、福富節男の証言によれば、熱心に暗号研究をしたということであるが、内心は全く違っていたようである。「透明な青空の一万メートルの上空を編隊をなして飛ぶ、銀色に輝く B-29 は実に美しかった。薄暗い地下室に避難しているわれわれと同じ人間の仕業とは到底考えられなかった。何か宇宙人にも攻撃されているような感じで、一向敵愾心が湧かなかった」と語る小平は、まず感情的な動機付けを欠いている。

暗号研究の唯一人の助手として長野に疎開したゼミ生の河竹俊雄は、「戦時研究は暗号の解読のはずだったが、ついに何もせず終わってしまった。で、私は東京へたまに連絡に行くほかは、読書と、先生や先輩との歓談にあげられた」、「陸軍の委託で暗号解読の研究に携っていたのは事実ですが、具体的な内容は全く知らず、また私に仕事を命じられたことも一度もなく、「あんな大きな金持の国に勝ってありませんよ。指導者は日本は負けたことがないからなんていうけど、アメリカだって負けたことはないんですからね」と聞かされている⁴⁰⁾。小平は、サボタージュをしていたのである。

小平は、1945年7月24日に天文学教室の藤田良雄助教授に「統計数値表」を借りたいと依頼し、同月27日に受け取ったという⁴¹⁾。「統計数値表」は、河田敬義や泉信一が論文で引用しているように、暗号研究に必要な文献であるが、個人としては保有していなかった。

小平のゼミ生である西島和彦は、「暗号の話聞いた事は無く、小平は栄養失調のために長男和彦(1944-47)を失ったほど食糧探して苦労していて、暗号どころではなかったはずだ。また、数学的にもっと重要な問題に集中していたことから、暗号研究の時間は無かったであろう。暗号研究をしていたというなら、戦時研究をしているという形式を整える為だったとしか考えられない」と証言している。

小平の弟である小平信彦の証言によれば、戦後の小平が会話の折に「暗号も数学的に見ると中々面白いものだよ」と語ったのを聞いている。

これらの証言を総合すると、小平は、釜賀一夫による暗号のゼミによって、暗号の数学的側面にはそれなりの興味を覚え、陸軍側には熱心に研究する素振りを見せたが、内心では敗戦を予期しており、大胆なサボタージュをも遂行したことになる。そもそも研究会に何故参加せざるを得なかったのか疑問であるが、陸軍技術将校として応召した弟の立場への配慮や、家族のことを考えた上での保険であったのかもしれない。

岩澤健吉は、暗号研究に消極的であったと考えられる。福富節男は、「東大数学科の I 助手が非協力的だ」と軍人が非難するのを見たという。消去法から、I 助手とは岩澤健吉と特定される。長野への疎開に同行した岩澤は、大戦末期には健康上の理由で療養生活に入っていたという証言もあり、暗号解読に対する貢献は低く見積もられる。岩澤の露骨に非協力的な態度の理由は不明であるが、岩沢の一年下の後輩で、将来を囑望された群論研究者の小暮勝美が、名古屋大学助手に任官する前に応召して、戦死したことも理由の一つであったのかもしれない。

泉信一は、当初乱数表の評価の研究に関与し、参謀本部編纂の乱数理論のテキストを利用しながら、出てくる数字の頻度から始めて次々の数字の階差、第二階差などの分布状態を分析した。泉研究室の学生だった土倉保は、フィリピンの日本軍基地が空襲で何機被害を受けたかなどの報告が暗号で送られた事例及び間諜が用いる暗号の作成法の事例を聞いたことがあり、ストリップ式暗号の解読には Lattice Theory の基本を学ぶ必要があるということで、泉などと George David Birkhoff「Lattice theory」を読んだ記憶がある。終戦後、この他にも戦時研究を引き受けていた泉は、戦犯とされるのを恐れて、一時的に身を隠している。

喜安善市の証言によれば、泉と協力した淡中忠郎も、超越数である自然対数の底と円周率の乱数性の方向から暗号研究に

従事していたという。

泉は、積極的に暗号研究を行ったが、他の戦時研究に多忙で、暗号研究に専念できる環境にはなかった。戦時研究に積極的に、比較的応用方面に近い数学者は、多方面から研究課題を持ちかけられる傾向にあり、一つのテーマに専念できないという動員上の問題は、ついに解消されることはなかった。

河田敬義は、確率論の束論的基礎に関する学位論文で1945年12月に博士号を取得するなど、確率論の深い知識をもつ人物で、その論文からは明らかな熱意を伺うことができる。1945年3月には、在宅していた両親と妹を空襲による爆弾の直撃で失っており、暗号解読を行う十分な動機もあった。しかし、詳細は明らかではない。

清水辰次郎も、暗号以外にも戦時研究計画を多数推進しており、暗号研究に専念できなかったようである。学術研究会議第1部第6研究班の主任研究員として電気工学者と共同研究を行い、「高射砲弾に鎖を付けて打ち上げ、米軍機の前面に文字通り弾幕を張って米軍機をからめおとす」という内容の研究を大阪大学で推進し、海軍技術研究所技師に就任したディオファンタス近似論の権威森本清吾と、上京するたびに研究上の接触を持っていたという。清水が極めて多忙な数学者であったことが伺える。

古屋茂も、逓信省中央航空所研究官として、空気力学者の山内正男と超音速機用の翼型について共同研究を行っていた。暗号研究に専念できる立場とは言えない。

角谷静夫は、プリンストン高等学術研究所滞在中に開戦したために、捕虜交換船グリッpsホルム号で帰国したが、同乗した鶴見俊輔は、「研究所にはフォン・ノイマンがいて、ノイマンとの交流は非情に刺激になったようなんです。日本に戻るようになって、しょんぼりしていた」と語り、船内には1500人の日本人がいたが、学問に関係ある人間は15から16人程度で「角谷さんは他の千五百人と話すことが何もないんですね。数学の話しかできない人なんですよ。で私なんかを相手に、ずうっと。二ヵ月半ですよ。私はその時初めて、大きい無限と小さい無限があることを知った」。鶴見の誕生日である1942年6月25日に、角谷は何かを書いて瓶に入れて海に流そうと提案し、鶴見は「覚えるに値しないことしか書かなかった」が、角谷は自分が最初に証明した定理を書いた。「火星人がこれを見ても、解読できるはずだ。同じ法則が宇宙のどこでも成り立っていて、彼らに知性があれば、きっと分かる」と意図を語り、鶴見は知性の差を感じたという⁴²⁾。帰国後の1943年8月には、東北帝国大学教授の窪田忠彦に、「先生、米国の国力、戦力の現状からみて、今度の戦争で日本が勝るとは思わない。この勝目のない戦争が早くおわり、本来の仕事の数学の研究に帰りたい」と語っている⁴³⁾。角谷のようなタイプの人物が、暗号研究に積極的に関わる事は考え難い。

結論

一般に若手数学者は、戦時研究に関与することに対して、早く自分の純粋数学上の研究テーマに戻りたいと考えていたが、後に国際的な数学者となる陸軍数学研究会の委員は、その優秀さ故にこの傾向が強かったはずである。職業的数学者は、純粋数学至上主義の価値観と、戦時研究という応用数学によって乖離していたのである。陸軍にとっての不幸は、動員した優秀な数学者が、その価値観から暗号研究に熱意を持ちえないという点を見逃したことにある。

数学科新卒の山本幸一・福富節男、東大二年生が活躍した原因の一つは、追い求めるべき純粋数学の研究テーマの欠落があったことを見逃さないであろう。

数学者による暗号研究が不首尾に終わったのは、主として純粋数学至上主義の価値観によるものである。陸軍側が高く評価しているのは、数学者が暗号学を高度に洗練させた事実であるが、暗号解読における数学導入期であったればこそ、目覚ましい成果

を挙げ得たといえる。

去りながら、数学者が陸軍の暗号学者に負の感情を抱いていたとは言えず、むしろ釜賀一夫は好感すら持たれていたことも指摘できる。

彌永と高木が、釜賀に学位取得を勧めた事実は、歓心を買おうとしたものとは考えられない。東大数学教室は、亀田豊治朗に対して1919年に「母函数論及ソノ確率論ニ於ケル応用」で博士号を与えて以来、応用数学では学位を与えていない。それだけ、釜賀の研究を高く評価したものであった。彌永は、自らの研究成果を焼却しながら、釜賀の研究成果を焼却することはせず、戦後に快く引き渡している。これらの事実は、彌永が釜賀に好意を持っていたことを論証するものである。

小平も、暗号の数学的側面が興味深いと語っているが、その小平が研究したのは、釜賀の研究した字差の理論であった。

福富は、軍部に好感を持っていると言い難い価値観の持主であるが、それでも釜賀のことを尊敬しているという。

これから言える事は、釜賀一夫が接点とならなければ、数学者の暗号研究の成果は更に低調なものになり得たという点である。

だが、ここには極めて興味深いディレンマがある。釜賀は、数学者を尊敬した為、数学者に対して低姿勢で臨んだ。結果、暗号のゼミを行わざるを得なくなるなど、暗号研究上のイニシアティブを一部数学者側に奪われ、研究効率が低下したのである。

脚注

- 1) 「通信講演会に将校差遣の件」、防衛庁防衛研究所蔵『密大日記 大正 12 年 6 冊の内 2 冊』所載
- 2) 防衛庁防衛研究所蔵 大久保俊次郎「対露暗号解読に関する創始並びに戦訓等に関する資料」
- 3) 宮内寒彌「新高山登レー二〇八 追跡戦記 日本海軍の暗号付」(六興出版,1975)
- 4) 靖国借行文庫所蔵「参謀本部高等官職員表 昭和四年二月～昭和十八年五月」
- 5) ハーバート・オー・ヤードリ著 大阪毎日新聞社訳「ブラック・チェンバ 米国はいかにして外交秘電を盗んだか?」(大阪毎日新聞社,1931.8)
- 6) 檜山良昭「光人社 NF 文庫 暗号を盗んだ男たち 人物・日本陸軍暗号史」(光人社,1994)など
- 7) 防衛庁防衛研究所蔵 元陸軍中佐萩野健雄「特情に関する戦訓」
- 8) [小原豊他:第二航空軍特種情報部 “特情”裏面史 裏方に徹した人びとの記録, 借行, 462(1989.6),pp.2-10]
- 9) 防衛庁防衛研究所蔵「大本営陸軍部職員表 将校、各部将校、高等文官」
- 10) 広瀬栄一:「フィンランドにおける通信諜報」,同台クラブ講演集編集委員会編『昭和軍事秘話』同台クラブ講演集 上』(同台経済懇話会,1987.12),pp.57-86 所載
- 11) [高須鶴三郎:米國數學會の開戦準備体制,朝日新聞,19627(1940.11.20),p.5]
- 12) 小野寺百合子「バルト海のほとりにて 武官の妻の大東亞戦争」(共同通信社,1985)
- 13) [茅野健他:OR のはじまり, オペレーションズ・リサーチ,vol.27,no.10,(1982),pp.564-577]
- 14) 「日本における統計学の発展 第 5 卷(米田桂三)」文部省科学研究費総合 A(1980, 81, 82)報告書,pp.6-33
- 15) 山内二郎先生追悼集刊行委員会編「山内二郎先生 人と業績」(日本規格協会,1985),pp.71-78
- 16) 畠山清行「陸軍中野学校 1 謀報戦史」(番町書房,1971)

- 17) [小沢義雄:恐怖の暗号解読機械“マジック”の謎, 丸.,243(1967.8),pp.226-233]
- 18) [仲野好雄他:先輩は語る 35 期 仲野好雄大佐 2, 偕行.,455(1988.11),pp.9-25]
- 19) David Kahn 著 秦郁彦・関野英夫訳「ハヤカワ文庫 NF 暗号戦争」(早川書房,1978)
- 20) 有賀伝「日本陸海軍の情報機構とその活動」(近代文芸社,1994)
- 21) 福富節男「デモと自由と好奇心と」(第三書館,1991),pp.47-54
- 22) 筆者蔵「陸軍数学研究会機関紙 1 号 原本複写版」
- 23) 木村登:「三つの鎮魂歌, 今野勉責任編集『昭和の戦争 ジャーナリストの証言 8 謀報戦争』(講談社,1985),pp.177-200 所載
- 24) [釜賀一夫他:座談会 日本陸軍暗号はなぜ破られなかったか, 歴史と人物.,171(1985.12.1),pp.150-165]
- 25) [中岡稔:幸運にめぐまれた数学者に, 数学のたのしみ.,21(2000),pp.9-16]
- 26) 城島明彦「不撓の軌跡 昭和 20 年東大物理学教室の男たち」(ダイヤモンド社,1992)
- 27) 小平邦彦「ボクは算数しか出来なかった」(日本経済新聞社,1987),pp.68-77
- 28) [無署名:諏訪の会 8 会食中に疎開決める, 毎日新聞夕刊.,40142(1988.1.20),p.3]
- 29) 諏訪教育会沿革史委員会「諏訪教育会百年の歩み」(諏訪教育会,1982),pp.183-185
- 30) [本田欣哉:お話二編, 蟻塔.,328(1985.1.1),pp.8-11]
- 31) 武藤徹「武藤徹教育論集 5 自然・社会・数学 私の学んだこと」(民衆社,1986),pp.63-67
- 32) [彌永昌吉:四半世紀, 数学セミナー.,vol.10,no.9(1971),p.1]
- 33) 矢野健太郎「新潮選書 アインシュタイン伝」(新潮社,1968),p.239
- 34) 有末精三「終戦秘史 有末機関長の手記」(芙蓉書房,1987)
- 35) 堀栄三「大本営参謀の情報戦記 情報なき国家の悲劇」(文藝春秋,1989)
- 36) [山本幸一:納得のいく数学を, 数学セミナー.,vol.21,no.12(1982),pp.37-40]
- 37) 靖国偕行文庫蔵 仲野好雄「通信戦の回顧と通信戦施策に関する一考察(完結篇)」
- 38) [高木貞治:オイレル方陣について, 科学.,vol.14,no.2(1944),pp.42-44]
- 39) [彌永昌吉:戦後の日本の数学の発展 私の思い出, 数学.,vol.47,no.2(1995),pp.184-192]
- 40) 河竹登志夫「酒は道づれ」(南窓社,1983),pp.202-208
- 41) 東京大学理学部天文学教室 OB 編「されど天界は変わらず 東京大学天文学教室諏訪疎開の記録」(龍鳳書房,1993)
- 42) 立花隆+東京大学教養学部立花隆ゼミ「二十歳のころ」(新潮社,1998),pp.409-417
- 43) 堀内義和「菌車の小径をたずねて」(自費出版,1999)

この他、陸上自衛隊の原久・釜賀一夫の下で、暗号解読に従事した元自衛官・近藤昭氏氏が、陸軍士官学校卒業生の親睦団体である偕行社の機関紙『偕行』に、1999年12月から連載している「暗号戦シリーズ」を適宜参照した。近藤氏は、「陸軍数学研究会機関紙 1 号 原本複写版」をも快く提供された。この史料は、独占すべき機密性を最早喪失しているので、読者諸兄に何らかの形で閲覧可能な環境を整えたいものとする。

謝辞

本論文に関して、貴重な証言を賜った方々は以下の通りである(以下敬称略)。

稲田獻一・海野和二郎・小尾信彌・河竹俊雄・喜安善市・小平信彦・小西弘・近藤昭氏・竹内外史・玉河恒夫・壇原毅・土倉保・長田潤一・鍋谷清治・西島和彦・一松信・藤田良雄・別宮貞雄・武藤徹・茂木勇・守山史生・山内正男・山梨寿恵子。

過去の再構成に貢献した証言者の方々に感謝すると同時に、本論文が事実と食い違う場合の責は全て筆者が負うものであることを銘記して摺筆することにする。

日本暗号解読史年表

| | |
|----------|---|
| 1923年1月 | ポーランド陸軍暗号解読班の将校 Jan Kowalewski が参謀本部構内で「通信講演会」なる講習を行った。受講したのは、英語・フランス語・ロシア語・ドイツ語の陸軍語学将校 |
| 1924年春 | 海軍将校の降幡敏(後に中将)が、ドイツ警察の使用している暗号機を購入。日本における暗号機械の第一号機 |
| 1925年12月 | 参謀本部部員の百武晴吉ほか一名が、ポーランド参謀本部において対露無線諜報の実施要領を見学し、かつソ連暗号解読の技術を修得した |
| 1926年 | 4省部協定が成立し、陸軍省・海軍省・外務省・通信省から専門家が外務省に集まり、主要国の外交暗号を研究することとなった |
| 1927年7月 | 参謀本部部員の百武晴吉がポーランドから帰国し、参謀本部第三部第七課(通信課)に新設された暗号班長に就任した(1931年8月まで) |
| 1929年5月 | 参謀本部部員の大久保俊次郎ほか一名が、ポーランド参謀本部において対露無線諜報の実施要領を見学し、かつソ連暗号解読の技術を修得 |
| 1929年 | 主要国の外交暗号研究に関する4省部協定が廃止された |
| 1930年7月 | 参謀本部第三部通信課暗号班は、参謀本部第二部支那課第五班となり、欧米課と支那課は部員各1名、通信課は2名を暗号班に配置転換した |
| 1931年8月 | ハーバート・オー・ヤードリ著 大阪毎日新聞社訳「ブラック・チェンバ 米国はいかにして外交秘電を盗んだか?」(大阪毎日新聞社,1931.8)が発売され、日本では35000部以上を売り上げた |
| 1931年夏 | 九州陸軍大演習で、通信学校暗号係の鈴木少佐が有限乱数暗号を解読した。結果、乱数式暗号は役立たないと結論される |
| 1932年頃 | ポズナン大学数学科の学生であった Marian Rejewski(統計学)が、初期型エニグマ暗号を解読した |
| 1933年4月 | 参謀本部で第1回暗号解読要員教育が行われる(1943年まで毎年開催される)。ロシア語・中国語・英語の語学将校が受講生 |
| 1934年夏 | 憲兵が、神戸のアメリカ領事館で外交暗号書 Gray Code を盗写する。以降、各国の外交暗号を盗写する |
| 1935年 | 参謀本部部員の桜井信太ほか一名が、ポーランド参謀本部において対露無線諜報の実施要領を見学し、かつソ連暗号解読の技術を修得 |
| 1936年夏 | 北海道陸軍大演習で、第7師団暗号班長の原久中尉は無限乱数暗号の使用を上申し、有効性が統計的に認められた。原久は参謀本部第三部通信課に転属となる |

| | |
|----------|---|
| 1937年3月 | 参謀本部第二部支那課第五班の暗号作成業務が参謀本部第三部通信課に戻され、同時に第二部支那課第五班は第一班に名称変更し、暗号解読を専門にすることになる |
| 1937年11月 | 参謀本部第二部支那課第一班が、参謀本部第二部謀略課に移籍 |
| 1937年12月 | 陸軍が無限乱数暗号を導入した |
| 1939年3月 | 暗号解読班が参謀本部第十八班として独立 |
| 1939年末 | GCCSのアラン・チューリングが、エニグマ暗号の理論的解析に成功 |
| 1940年4月 | ポーランドの暗号解読専門家であるミッツェル予備役中尉が来日し、終戦までソ連軍暗号解読に従事した |
| 1940年11月 | 東北大学教授の高須鶴三郎が、アメリカ数学会が数学者を組織的に戦時研究動員していることを朝日新聞紙上で訴える |
| 1941年初頭 | 第十八班員の広瀬栄一が「暗号研究に数学者を動員すべきである、故に高給で東大などの数学者に協力を得よう」と思い立ち、雇用したが、短期間で辞任した |
| 1941年2月 | 東北大学教授の高須鶴三郎が、アメリカ数学会が数学者を組織的に戦時研究動員していることを『現地報告』誌上で訴える |
| 1941年12月 | 日本が米英と開戦 |
| 1942年春 | チェルページ社から暗号機械クリプトテクニークを購入 |
| 1942年5月 | コレヒドール要塞を占領。米軍が暗号解読に利用していたIBM統計会計機405型を鹵獲した |
| 1942年末 | 陸軍科学学校学生の釜賀一夫が、符号理論研究に森嶋太郎教授の助力を得る。釜賀は、森嶋のルートから高木貞治と接触し、暗号研究に協力を要請した(第十八班長の中野良次は反対) |
| 1943年初頭 | 軍部が奥多摩に民間の科学者を集めた。名古屋大学教授の小野勝次(暗号関係として)、歯車の最高権威である東北大学教授の成瀬政男などが招かれた |
| 1943年7月 | 第三部通信課暗号班の釜賀一夫が市ヶ谷の将校集会所で数学者への暗号説明の会合を開く(10月まで毎週土曜日に開催) |
| 1943年7月 | 第十八班が陸軍中央特種情報部に改組 |
| 1943年8月 | 第三部通信課長に仲野好雄が就任、数学研究会問題を手掛け、上官の反対を押し切る |
| 1943年秋 | 第三部通信課暗号班の釜賀一夫が暗語構成上の非重複文字数を調べ、重複のない語に同一原語群を配当する方式を確立(誤り訂正符合のハミング距離の理論) |
| 1943年12月 | 海軍軍令部が、数学者・語学者を加えた数十名の専門家からなる特務研究室を設立し、正攻法でストリップ暗号を研究 |
| 1944年1月 | 福富節男が中央特種情報部に転属 |
| 1944年4月 | 陸軍数学研究会が発足 |
| 1944年8月 | 釜賀一夫と第三部通信課暗号班技手の山本幸一が、クリプトテクニークを改造したM209暗号機の暗号を一部解読に成功 |
| 1944年11月 | 陸軍数学研究会幹事長名で第一生命保険と日本生命保険保有のIBM統計会計機の徴発令状を送付 |

| | |
|----------|--|
| 1944年11月 | 陸軍暗号学理研究会機関紙第1号が発刊(戦後, 防衛庁の参考資料として復刻) |
| 1945年1月 | 東京文理大数学科学生の中岡稔らが参謀本部に動員されて暗号解読に従事 |
| 1945年4月 | 東大理学部数学科が長野県に疎開. 学生が暗号解読に, 数学者が暗号研究に従事 |
| 1945年8月 | 終戦 |
| 1948年10月 | 彌永昌吉・竹内外史・山辺英彦ら8名の数学者が, GHQに訊問を受ける |