第 31 回諜報研究会　　2020 年 5 月 23 日

無線諜報　日本海軍の暗号「D」の解読

報告者　原勝洋（戦史研究）

1）　**「ウルトラ」とは？**　GET　YAMAMOTO 作戦の追加情報の補充として「ウルトラ」が情報源。この「ウルトラ」の解明がきっかけとなった。国益に属する特別な機密区分された暗号解読を含む通信諜報の「暗号名」と判明。

2）　**国家機密の壁「マジック」と「ウルトラ」情報。**　アーキヴィスト：ジョン・テイラーは、メモ用紙に（「ウルトラ」はパール・ハーバーに関係しているので現在は見ることができない）と書いてゴミ箱に捨てた。「マジック」は閲覧させてくれた。

3）　**1979 年「ウルトラ」情報の機密解除**　1997 年、米公文書館から「ウルトラ」に関する葉書に「6 ヵ月間史料を吟味するから待ってほしい」との回答。感激と期待。

4）　**メリーランド州カレッジパークの公文書館Ⅱの存在。**　RG457 の中に日本海軍暗号関係資料　「海軍無線交信規程」「海軍通信規程別冊　通信電波・通信時間表」

5）　**RG457　の検索がカギに。**　1479 箱 4293 項目からお目当てのドキュメントを探し出しだすのは大変だった。「Instructions for The recovery of messages in The AN-1 CODE」は、日本海軍暗号「D」電文の解析であった。

6）　**RG457 の中に日本海軍暗号書「D 壹」発受信用暗号書　発見。**　RG457 Enty9032　Item「Japanese　Codebook－3Pats」には電報番号とリンクした対の乱数「加算符」が示されていた。米解読陣の「cipher-KEY　subtractive　Table　for『AN』cipher」が「加算符」表の訳と判明。ガダルカナル島で海兵隊員が鹵獲。

7）　**暗号一次史料を入手しても翻訳できない。**日本海軍　暗号用語　がないので専門用語を米海軍資料として翻訳する方策がなかった。米軍作製「英・日」暗号辞典発見

8）　**RG38　の解読資料が太平洋戦争諸作戦の解明に…**　新たに機密解除された暗号関係資料が　「RG457」でなく「RG38」に属することが判明。

9）　**日本海軍の暗号「D」は解読されていた。**R.I.P.（Radio　Intelligence Publication）暗号書と乱数表「D」、「D 壹」、「呂」「波」「留」「天」などの分析解説書

１０）　**「YAMAMOTO　shootdown」資料の機密解除**　そして OP-20-GY 記録の発見　山本巡視電に使用された乱数表は使用期間外の乱数表 **E-14** だった。E-14 は日本海軍暗号波一、乱数表第 2 号を意味した。日本海軍は、当時チャンネルⅠに「呂」、そしてチャンネルⅡに「波」を採用していた。チャンネルⅡで使用されていた乱数表第 2 号（E-14）は、第 3 号（E-15）に更新された。その時、前日までチャンネルⅡ使用されていた波一乱数表第 2 号（D-14 となる）が、チャンネルⅠ「呂」に代わって使用さ

れる使いまわしが実施された。そしてチャンネルⅠは、波一乱数表第 2 号（D-14）を 4 月 1 日に、呂一乱数表第 4 号（D18-a）と更新した。4 月 13 日、チャンネルⅡから山本巡視電は、既に更新された波一、乱数表第 2 号（E-14）で打電された。その使用法は「謎」である。海軍通信規程　第 9 章　通信諸記録「発着信」保存 1 ヵ月である。

膨大な暗号関係資料は　計り知れない文書量で保管されていた。

日本海軍は、暗号書「D」に引き続き、主用暗号に「D 壹」、「呂」、「波」、「天」、「留」「登」などを使用した。乱数表の更新数は 89 冊にのぼった。しかし、冒頭部と末尾に定型化した「鍵」の使用は、その本質が変わらないので空き巣に強盗するごとく「解読・翻訳」できたと米解読陣は記録した。

その情報は、RG38 と RG80、そして RG457 に日本陸海軍の暗号関係資料として閲覧可能である。しかし、とても個人の力では及ばない量であった。

1）　唯一現存する日本海軍暗号書「D 壹」の原本を影印復刻した「海軍暗号書 D 壹　（発信用）」ゆまに書房

2）　計測制御工学・システム工学専攻工学博士北村新三神戸大学名誉教授との共著「暗号に敗れた日本」PHP 研究所

3）　世界で最初に日本海軍暗号の無線諜報解説書（R.I.P.）を掲載した「暗号はこうして解読された」KK ベストセラーズ

4）　外務省の在外大使館使用の暗号機交信は解読されたことは「マジック」情報として有名である、しかし、どのように暗号化された電文かを検証した記録はない。米公文書館に保管されていた日米交渉時の「第十四部」と「貴地午後 13 時手交電」の暗号文を掲載、なぜ、複雑難解な暗号文が解読されたのかを不思議に感じさせる「日米開戦時における日本外交暗号の検証」ゆまに書房

5）　米海軍が作成した日本語と英語比較の「日本陸海軍・軍事技術用語辞典」ゆまに書房

6）　日本海軍武官の情報漏洩がノルマンディ上陸作戦の連合国に勝利のヒントを与えた逸話、正午位置報告電が輸送船舶を危機に追いやった真相、鹵獲された歴代暗号機を含む戦史の裏側に迫る別冊 2548 号「米軍から見た太平洋戦争」株式会社宝島社

7）　「文藝春秋」1980（昭和 55）年 5 月号掲載の「暗号名ウルトラ　山本長官機撃墜す」は、英訳され米国立公文書館Ⅱ保管の米軍資料「Yamamoto　shootdown」ファイルに収録されている。

以上すべて米国立公文書館発掘史料による構成である。上梓できたことを誇りに感じます。

はじめに

75 年前に大東亜戦争（太平洋戦争）は日本降伏として終結した。その敗因には、連合国の物量、原子爆弾の開発・投下などが伝えられて来た。
しかし、実際は秘密のヴェールに包まれた「諜報戦争」にあった。
この際の「情報漏洩」に関する証拠が、機密解除された膨大な米国の諜報史料から明らかになった。
米国首都ワシントン DC 南東地区の NAVYYARD 内にある米海軍省海軍歴史史料部作戦記録保管所（現在の U.S.Naval History and Heritage Command)、そして首都 DC とメリーランド州カレッジパークにある National.ARCHIVES Ⅰ とⅡに保管されていた。
合衆国政府の書類、歴史的価値ある資料を保存する公文書記録保管局には、機密解除された諜報が保管され、永遠にみることはないだろうとされていた暗号解読に関する一次史料も、一般に閲覧可能となった。
筒抜けだった欧州在任中の海軍武官の使用する暗号機「九七式和文印字機Ⅲ」「秘匿名（茂)」、在外大使館用「九七式欧文印字機（B)」は開戦前から「コーラル」「パープル」と呼ばれ米陸海軍諜報部に解読されていた。

日本海軍　暗号「D」の解析・解読を年代順に示した記録。

解読班の成果

「**TOP SECRET PROPOSAL for ONE LARGE CENTRAL UNIT and SEVERAL SMALL EXPLOITATION UNITS** 18 May 1944」から解読経過が判明した。

OP-20-GY（Includes GZ（翻訳斑） projects）
Project Unfinished or CONTINUOUS
1940 年 3 月 1 日（5）Reduction of 5 -numeral system （Orange Navy）
Remarks First break made by Mrs. Driscoll. Solution progressing satisfactorily
1940 年 6 月 5 日（d）5-numeral（A）Naval Administrative）Very secure system-employs additive key System broken Keys partially recovered
（e) 5-numaral (B) (Air Force Code) Very secure system-employs additive key System broken Keys partially recovered
1940 年 7 月 3 日　（d）5-numeral（A）　（e）5-numaeral（B）
1940 年 8 月 1 日　（d）AN Code （Administrative）(current) Numerical additive key system。Keys being recovered. 3000 code groups obtained.
1940 年 9 月 3 日　（2）Orange Navy Systems
（d) AN Code (Administrative) (current) Numerical additive key system. Keys being recovered. Garble table recovered. Initial break in code itself.（注：

JN25A）

1940 年 10 月 1 日 （ｄ）AN code（Operations）（current） Code book in preparation

1940 年 12 月 1 日 （d）AN Code（Administrative）（current）approximately 1300 values recovered.

1941 年 1 月 1 日 （d）AN code（Operations）（current）approximately 1400 values recovered.

1941 年 2 月 1 日 （d））AN code（Operations）（current）.Numerical additive key system. Keys being recovered. Approximately 1500 values recovered. Change in Method of encipherment effective 1940 年 10 月 1 日

1941 年 3 月 1 日 同上 Approximately 1600 values recovered.

1941 年 4 月 1 日 （ｄ）AN Code（Operations）（old）Keys being recovered.Approximately1800 values recovered. New Method of Encipherment effective 1940 年 10 月 1 日.

（e）AN-1 Code（Operations）（current）.New code effective 1941 年 2 月 1 日. Approximately 300 values recovered.

1941 年 4 月 1 日 （d）AN Code（Operations）（old）Keys being recovered. Approximately 1800 values recovered.

（e）AN-1 Code（Operations）（current）.（注：昭和 15 年度暗号書「D」） New code effective 1941 年 2 月 1 日

Approximately 300 values recovered.

1941 年 5 月 1 日 （d）AN Code（Operations）（old）Keys being recovered. Approximately 1900 values recovered.

（e）AN-1 Code（Operations）（current）. New code effective 1941 年 2 月 1 日. Approximately 400 values recovered.

1941 年 6 月 1 日 （d）AN Code（Operations）（old）Keys being recovered. Approximately 1900 values recovered.

（e）AN-1 Code（Operations）（current）. New code effective 1941 年 2 月 1 日. Approximately 1100 values recovered.

1941 年 7 月 1 日 （d）AN Code（Operations）（old）. Numerical additive key system. Keys being recovered. Approximately 2100 values recovered.

（e）AN-1 Code（Operations）（current）. New code effective 1941 年 2 月 1 日. Approximately 1100 values recovered.

1941 年 8 月 1 日 （d）AN Code（Operations）（old）.Approximately 2200 values recovered.

（e）AN Cipher No.5（old）. Additive key cipher for AN and AN-1 Code.

All Starting point subtractives recovered. 7500 text additives recovered.
(f) AN-1 Code (Operations) (current) .Effective 1940 年 12 月 1 日. Approximately 2000 values recovered.
（g） AN-1 Cipher No.1 （current） 16District project. All starting point subtractives recovered. 4800 text additives recovered.
1941 年 9 月 1 日 (d) AN Code (Operations) (old) . Approximately 2350 values recovered.
（e） AN Cipher No.5 （old） Additive key cipher for AN and AN-1 Code. All Starting point subtractives recovered. 10000 text additives recovered.
(f) AN-1 Code (Operations) (current) . Effective 1940 年 12 月 1 日（注 : JN25B-7） Approximately 2000 values recovered.
（g） AN-1 Cipher No.1 （old） 16District project. All starting point subtractives recovered. 5400 text additives recovered.
（h） AN-1 Cipher No.2 （current） Effective 1941 年 8 月 1 日予備段階
1941 年 10 月 1 日 （d） AN Code （Operations） （old） . Approximately 2500 values recovered.
（e） AN Cipher No.5 （old） Additive key cipher for AN and AN-1 Code. All Starting point subtractives recovered. 14000 text additives recovered.
(f) AN-1 Code (Operations) (current) . Effective 1940 年 12 月 1 日（注 : JN25B-7） Approximately 2400 values recovered.
（g） AN-1 Cipher No.1 （old） 16 District project. All starting point subtractives recovered. 7200 text additives recovered.
（h） AN-1 Cipher No.2 （current） Effective 1941 年 8 月 1 日 49 starting point subtractives recovered.
1941 年 11 月 1 日 （b） AN Code （Operation） （old） .200 values recovered.
（c） AN Cipher No.5 （old） 4000 text additives recovered.
（d） AN-1 Code （Operations） （current） . 600 values recovered.
（e） AN-1 Cipher No.2 （current） 201 starting point subtractives recovered.
1941 年 12 月 1 日 （b） AN Code （Operation） （old） .4000 values recovered.
（c） AN Cipher No.5 （old） 800 text additives recovered.
（d） AN-1 Code （Operations） （current） . 500 text additives recovered.
（e） AN-1 Cipher No.2 （current） 16 District project 900 starting point subtractives and 2500 text additives recovered.
1942 年 1 月 1 日 1941 年 12 月の間に達成 （b） AN Code （Operation） （old） .1939 年 6 月 1 日から実施、1940 年 11 月 30 日.1941 年 12 月 12 日 Recovery discontinued 5366 values recovered.

(c) AN Cipher No. 5 (old). Effective Oct. 1、1939、to Nov.30、1940. Recovery discontinued. 22000 out of possible 50000 additives recovered.
(d) AN-1 Code (Operations) (current). 2380 values recovered.
(e) AN Cipher No. 1 (old). 4167 text additives recovered.
Unfinished or Continuous（継続事項）
(d) AN-1 Code (Operations) (current). Effective Dec. 1、1940. Approximately 6180 values recovered.
(e) AN-1 Cipher No. 1 (old)（注：JN25-6）.16 District project 11867 text additives recovered.
(f) AN-1 Cipher No. 2 (old)（注：JN25-7）Effective Aug. 11、1941. 900 starting point subtractives recovered. 2500 text additives recovered.
(g) AN-1 Cipher No. 3 (current) (注:JN25B-8) 14 and 16 District Project.
日本海軍の主要暗号となった暗号「D」と同乱数表はどうして破られ、暗号文はどこまで解読されていたのだろうか？

先に転送した記事をこの部分に挿入していただければと思います。

日本海軍は、戦争 2 年半前の昭和 14 年 6 月 1 日から「ミッドウェー海戦」前の昭和 16 年 5 月 27 日迄に、ふたつの暗号書 D（初版　昭和 13 年度改版と昭和一五年度改版）と 8 個の乱数表を使用した。この暗号の解読に臨んだのが米海軍通信局内の日本海軍暗号「D」を担当する「暗号解読陣」（OP-20-GY）だった。
日本海軍の暗号電報はどのようなものであったのか？

米海軍暗号解読陣は、この当時月平均 7000 通の「D」暗号による日本海軍暗号電報を傍受していた。主要な暗号解読の機能構想は、第 2 エシュロン処理センターと呼ぶ、主要分野の分析センターである首都ワシントン DC の　分析、管理、調整の中枢センター(NEGAT 局)1930 年 6 月、試験的傍受所と 1933 年、ハワイ・ヒーイアの（H 局)、そして第 1 エシュロン処理活動又は傍受の先端と呼ぶ前哨の処理班（フィリピン・コレヒドールの CAST 局・昭和 16 年 10 月 15 日活動開始）と主要な作戦指揮官のため近接支援用の機動班を確立させた。
今ではアングロサクソン諸国による世界的通信傍受体制を指す言葉として「エシュロン」が使われているが、既に 84 年前の対日通信傍受作戦が最初であった。

その組織とは？
米海軍通信局内 OP−20−G（機密保全課）の暗号解読を含む通信諜報、行政、調整管理の中枢となる米本土首都ワシントン DC 海軍省内のネガト班 NEGAT、
ハワイの第 2 エシュロン・ハイポ班 HYPO（ハワイ無線諜報部総員 100 名・士官 16 名、暗号要員 24 名、傍受要員 60 名で日本艦船の追跡、もっぱら「D」暗号を除く気象暗号等の日本海軍電文の解読を行なっていた)、
そしてフィリピン・マニラ湾内コレヒドール島モンキー・ポイントの空調設備の整った防弾地下壕内第 1 エシュロン・キャスト班 CAST（アジア無線諜報部；総員 70 名・士官 9 名、暗号要員 19 名、傍受要員 42 名で日本海軍主要暗号「D」の他に中国、満洲、蘭印と日本間の外交暗号を網羅していた）であった。
更に、太平洋無線傍受網エシュロンとなるダッチ・ハーバー、グァム「Able」、ミッドウェー「AF」、サモア、アダク「AX」などの前哨傍受・方位測定所が活動、傍受電を解読班に供給していた。
解読班内部は暗号解読（GY)、翻訳と暗号探知（GZ)、傍受・方位測定（GX)、自軍暗号の秘密保全（GC)、IBM 処理（GS）の得意分野に区分されていた。

日本海軍の無線暗号電報が米海軍暗号解読陣に解読されたのは、適切な想定に基づき電文型式の秘匿法が解析され、同じ乱数表による二重送信にあった。

誰が、どのような方法で「D」暗号を解読したのだろうか？
日本海軍の主要暗号「D」（昭和 13 年度改版・初版）を破ったのは、女性の暗号解読者、アグネス・メイヤー・ドリスコルであった。昭和 14（1939）年夏以降、ドリスコル夫人を含む六名が初版 D 暗号及び同乱数表第 1 号（JN25A―1）への攻撃を開始した。
傍受された暗号文は、IBM カードにパンチされ、どんな特徴をもつ暗号構成か、どんな暗号符字の組成並びに配列かを発見するため索引化された。

そして同じ日に送信されたすべての傍受電に適用される「日々の鍵」となる「アラビア数字」を示す「乱数グループ」があるとの**仮説**に基づき、IBM 分類機でこのような配列の特質を示す「乱数グループ」を探すため、傍受電文すべてが洗いざらい調査された。
AN 暗号（初版 D 暗号）の最初の 10 字の 3 数字は発信者の一連番号、4 と 5 字目の 00・区別符、二番目の 5 数字乱数は「乱数開始符」、そして結尾の 10 字数中最初の 5 数字乱数は乱数開始符の繰り返し、6 と 7 番目は発令日、最後の 3 字は発令時刻とする暗号方式は、乱数表第 4 号（JN25A―4）の昭和 15 年 9 月 30 日迄で完了した。
乱数開始位置を解読するには、乱数開始符と別に用意される「日替り乱数鍵表」の解析が必要だった。
AN 暗号（初版 D）の乱数表はページ総数 200、暗号化は、乱数開始位置から各ページの最初の横欄から左から右、引き続き下方に、電文の同じ長さの乱数まで進むことになる。

最初の手がかりは、各電文の始めと終わりに繰り返される乱数は「何かを分類」する**指示符**、そして最後の乱数は「発令日時グループ」として識別され、日時を示す乱数の直前に繰り返される指示符は意味のあるものとみなされた。
それは同じ日に送信されるすべての電文に適用できる日替りの鍵となる乱数表があるという**仮説**が正しいことが判明した。

暗号解読のための**第一段階**は、D 暗号通信文を大量に集めることにあった。
当時の太平洋のグァム、フィリピンのカビテ、ハワイのホノルルの三つの米海軍傍受所では、特別に日本海軍モールス符号・数字の訓練を受けた傍受員がこの通信文を傍受した。
傍受された電文は、ドル海運会社のプレジデント汽船の一つを経由して一週間で西海岸に着くと、書留郵便でワシントンに送られた。
また急ぎの場合はパン・アメリカン航空のクリッパー（大型四発飛行艇）の機体に取り付けられた収納箱に収められワシントンに運ばれた。

二ヶ月後の夏以降、ネガト班には乱数列の連続する暗号電文が相当量蓄積された。
そこで最も経験豊かな暗号解読者がその**系統的な学習を開**始することになる。

こうして昭和一四年早秋には、完全に初版 D 暗号及び同乱数表第 2 号は解析され、晩秋と冬にかけて確実に解読・翻訳される方向に向かっていたのである。
最初の手掛りは、昭和一四年六月一日（JN25A―1）に使用した最初の乱数が、三ヶ月後の同年九月一日（JN25A―2）に**別の乱数**によって取り替えられていることを発見した時だった。

この段階で基本となる暗号書は変更されていないという想定は、今まで実施してきたすべての仮説ががしかし、推測は正しいことが証明された。
Able―2 から想定のすべてを確認できたことが**「break」**をもたらした。
この 2 通の暗号文は、同じ発信者から送信された、同一の日時、同一の乱数開始符（key indicator）
そこで、最初の乱数は Able−１、そして二番目の乱数を Able−2 と
日本海軍 D 暗号に米国式名前で AN 暗号と呼称、後に **JN25** と呼称され広く知られることになる。
ネガト班で D 暗号を破った後、解読作業はコレヒドールのキャスト班で始められ、シンガポールの英軍解読チームも参加したが、どのチームも D 暗号の解読に成功していなかった。

1940 年同年一０月一日 Able−５・新乱数表第五号（JN25A―5）が開始されると、暗号文の新しい形式から暗号方式の変更が直ぐに明らかになった。
電文最初の二０字（乱数四個分）の最初のグループに一連番号（機密第　番電）が残っていたが、二番目のグループに以前の指示符はなかった。
代わりに最初の 3 字は発信者の一連番号が繰り返され、最後の 2 字は常に 11、33、55、77 または 99（注；分割符）となった。
電文の最後のグループは、おなじみの５数字・発令日時であった。

一連番号が繰り返された理由が注意深く調査され、同じ一連番号を持つすべての電文は、その 3 番と 4 番目のグループ間の差は同じであることを暴露した。

以前に使用された日替り乱数鍵表の代わりに日本海軍は、乱数表全体の寿命延ばすため 1000（001～999）に及ぶ指示符（乱数加算符）を採用した。
これが**乱数加算符表**という作成と翻訳時の乱数開始位置を示すもので、001 から 999 の電報番号（電番号）に対応する乱数加算符、一組で構成されていた。
電文の結尾にあった再乱数開始符は放棄された。

また、乱数表総ページが 300 から 500 に増加し、開始位置を各ページの最初の欄から始める規程も廃止して、「横行と縦列の交差」する開始位置を採用した。

この暗号方式は昭和 15 年度改版の D 暗号（JN25B－5）にも適用した。

？の 23300　79994　70557（以下乱数七個略）79994　27140
次に、複数の電文の中にある同じ又は異なった位置にある、繰り返し暗号化しているグループを持つ暗号文が入念に調査された。

JN25 暗号の解読・翻訳を妨げていたのは、更新される乱数表の大量のデーター精査と解読要員の不足にあった。

JN25 の暗号方式は完全に解析されていたが情報として読むことができるまで越えなければならない多くの作業が残っていた。

暗号符字自体は算用数字を除いて全て仮の暗号符字は本物の日本語の原文に当てはめねばならなかった。
乱数列の探知は、根気のいる骨の折れる作業としてもやり遂げねばならなかった。

日本の運命は、女性でありながら最高の暗号解読家アグネス・メイヤー・ドリスコルの存在に大きな影響を受けることになる。

電文内には、通信文の字数、送信番号、乱数開始位置、暗号種類の確認、送信日時等の指示符が秘匿されていた。
日本海軍の暗号陣は、新乱数表への**更新を唯一の機密保全**とし、**電文の冒頭と結尾に秘匿した 0～9 の算用数字を無秩序に配列する選択符（乱数開始位置と発令日時）が解読されることはないと確信していた。**
米解読陣は何を突破口としたのだろうか？

Ｊ．Ｓ．ホルトウィク著の「米海軍秘密保全グループの歴史」の中に現れる米海軍民間暗号解読家アグネス．メイ．マイヤー（一八八九年七月二十四日生まれ）がその人だった。
　ミス・アギーと呼ばれた彼女は　後に弁護士マイケル．Ｂ．ドリスコルと結婚してドリスコル夫人となるが、一九一八（大正七）年六月二十九歳で海軍予備員として応募、それ以前は数学の教師、翌年七月に米海軍省通信秘密保全グループ暗号と記号課に暗号事務員として契約し、日本海軍の暗号の大部文を破った以来、海軍通信部、三軍安全保障局、国家安全保障局を経て一九五九（昭和三十四）年に引退するまで、合衆国における暗号解読に対する絶大な貢献によって最高の評価を得ていた。
　ミス、アギーと貴族的に呼ばれた彼女は背が高く、ほっそりとしていて、物静かだがきわめて献身的な女性だった。
　彼女は一九一一年オハイオ州立大学で独語、仏語、ラテン語、物理、工学、統計学を習得し卒業、テキサス州アマリヨの高校で数学科主任として勤務、第一次世界大戦(1914－18)中に海軍予備隊に参加した。ミス．アギーは日本海軍の主要暗号の解読に深くかかわり、奇跡的な任務に没頭、その解読の主役を演じたのである。
　米海軍において彼女に匹敵する暗号解読者はいなかった。ドリスコル夫人となった彼女

は、同僚からマダムＸと呼ばれていた。
　というのも彼女は、　男の世界の中にあって女性として国家の安全保障に関連した機密情報を扱う任務に就いていたので、できる限り孤独を保った。
　そこで同僚の誰もが、ドリスコル夫妻から社交的に招待されることはなかった。
　アグネス自身は優しい気持ちと友好的である反面、いつも毅然とした態度をとり、化粧らしい化粧もせず、婦人服を男仕立てにすることでその毅然さをより強調していた。
　しばしば彼女は水兵顔負けの悪態をついた。
　しかし、**彼女の最大の力量**は問題の根本に迫り、その重要な構成要素を選り分け、解決の方策を見つけ出す手腕にあった。
　彼女は、暗号調査部門を立ち上げたローレンス．Ｆ．　サフォード、ミッドウェーの情報戦で大活躍をしたジョセフ．Ｊ．ロシュフォートほか第一級となる米海軍のほとんどの暗号解読者に暗号解読術を教え込んだといわれている。
　暗号破りにおける彼女のすばらしい才能と決断力を疑う者は、誰一人としていなかった。一九二〇（大正九）年，アグネス嬢は海軍民間職員の身分を確保すると、ＯＰ－２０Ｇ、暗号と記号課そしてシカゴ織物貿易商ジョージ．フェビアンが幾分趣味的に設立したイリノイ州ジェネヴァにあるリヴァーバンク研究所に送り込まれた。
　本研究所は、音響学、化学、遺伝子学、暗号装置製作の科目を含む海軍士官用の教育コースを主目的としていた。

当時の解読作業、全てが中央部ネガト班で行われた。
JN25 の暗号方式は完全に解析されていたが、情報として読むことが出来る前に、やるべき膨大な解読作業が残っていた。
暗号自体は算用数字以外すべての意味を探知・復元しなければならなかった。まして乱数の連続して続く乱数を復元する骨の折れる仕事であった。
ワシントンの全体暗号解読要員はわずか三六名、大部分は、JN25 の仕事より別の任務に手一杯だった。二から五人が未だに読むことができない JN25 に割くことができた。
昭和一五年初秋には**暗号方式は完全に解明**されていたが、晩秋と冬の記録は沈滞気味だが、暗号を読む方向に前進していた。
日本語は習得するのに難しい、しかし、如何なる国の海軍用語極端に定型化して、頻度の高い用語は、飛びぬけた問題を示さない。
既に破っている D 暗号用乱数表第一号と第二号に対する乱数と暗号探知は、現行の乱数の断片的な解読作業より貴重な暗号學的情報を示すだろう。
鍵となる指示符の全ては、新乱数表毎に復元された。通信量は最後の学習のために満たされていた。
この理由、コレヒドールは改版 D 暗号書都現行の乱数第 6 号）二月一日の JN25Baker6 の解読に集中した。ワシントンは Able5 と Baker5 に活用する人員を配置した。

最初の手がかりの第一は、暗号化された暗号で処理されている、第二は各電文の始めと終わりに繰り返される乱数は何かを分類する指示符であると想定したことにある。
最後の乱数は、発令日時グループとして識別され、日時を示す乱数の直前に繰り返される指示符は意味のあるものとみなされた。
それは同じ日に送信されるすべての電文に適用できる日替りの鍵となる乱数表があることを仮説とした。

例えば、乱数表第一号用日替り鍵乱数表 Daily　key　additive と呼ばれる表の六月一日＝2562、七月一日＝6664、八月一日＝9520 の一日から末日迄。毎日の通信文は IBM 装置で分類され、この疑わしい指示符グループの中にある数字順に表示された。
また、乱数の最初の探知・復元の手がかりは、昭和一四年六月一日に使用された最初の乱数列が九月一日に別の乱数列に置き換えられたことを発見したことから判明した。
最初の乱数を Able–1（乱数表第一号）、第二の乱数を Able–2（乱数表第二号）と呼んだ。
最初の乱数表の更新だった。
これは乱数表を変えたが基本となる暗号書（初版 D 暗号）は変わらないこと意味していた。
この二通の電文の同じ発信者から打電され内容から同一の日時符と指示符を持っていることが判明した。
そして 89904 や 95596 の乱数と 51036・13884 乱数列の繰り返しから、日本海軍の暗号は乱数により暗号化された五数字暗号であるとの想定を持つことになる。
と同時に 0～9 の算用数字が使われていることも判明した。
次に電文の中に同じ又は異なる位置に暗号化されたグループが繰り返されている電文が念入りに調査された。
ＩＢM装置がこの調査の手助けになった。
その結果、多くの場合に通信文の最初の四グループの中に繰り返されるグループが見つかった。
こうして米海軍暗号陣は、日本海軍の初版 D 暗号を解いていったのである。
結果、暗号書の内容は第一と第二の二部制、乱数表は三００ページ、日替り鍵表の存在を明らかにした。

昭和一四年六月一から昭和一五年九月三０日までに乱数表を使用していた。
その期間は三ヶ月であった。
第三号は六ヶ月使用された。
交信符にはW＝字数、NR＝電信番号、TI＝着信者、HA＝発信者に続き、23300　79994　中略　79994　27140　となる。
最初の 233 は発信者一連番号（電報番號）、00 は区別符、通信文内の指示符 79994 は、結尾の一０字の最初の五数字・79994 は、六と七番目の 27 は電報の発令日、残りの三字 140

は発令時刻を示すものであった。
乱数開始位置を出すには、指示符の左から四文字 7999 に別に用意された
日替り鍵表の例えば九月一四日から 2582 を選び非加算し、9471 の最初の三数字目に 1 を加算、948 となる。
これを 3 で割ると 316 となる。乱数の開始位置は、ページ数と横行で示される。
JN25 は完全に解明されていたが、

米海軍は、便宜上日本海軍の新しい五数字宛乱数を JN25 と呼称した。
そして、JN25 は、その数字の計は三で割り切れる想定。
この時点米海軍が呼称する JN25 とは、日本海軍暗号書 D・昭和一五年度改版を意味する。

改版 D 暗号（以下呼称）は、原語・語彙を換字した五数字符号を記載する発信用と受信用の暗号書二冊と乱数表（五００ページ）から構成されていた。
約四００ページからなる暗号書の内容は第一部〇数、〇年月日、〇記号類、第二部〇慣用信文、〇説話、第三部（付録辞典）〇記号及び慣用信文、〇部内廠部隊、〇帝國艦船、〇帝國主要艦船、〇外国艦船、〇地名、〇漢字電報書用記号、〇ローマ字綴、〇仮名綴、〇臨時特定信文を約五万、暗号符字を収録する辞書のようなもので、例えば「水」は第二部説話欄に五数字の暗号符字「50796」に換字して併記してあった。
換字された暗号符字で作成された通信文を更に暗号化するための乱数表（注：無作為の数字五字宛の乱数は例；48282 で 4・8・2・8・2＝和 24 は 3 で割り切れる。
001 ページから 500 ページ、各ページに横行と縦列 0 から九の欄に乱数一００個）が使用されていた。
その他にも地名を秘匿するために使用する特別地点略語表（注：暗号書にも第三部地名欄あり）、仮名組合せの日歴換字表（注：暗号書にも第一部年月日欄あり）などを活用して通信文を組立てていた。
この乱数列の暗号通信文を米海軍はどのようにして解読したのだろうか？
開戦二年半前、昭和一四年六月一日日本海軍は主要暗号書を仮名で暗号化した通信文を数字・乱数で組み立てる暗号文に変更した。

D 暗号はどのようにして秘密を突破されたか？
ＩＢＭの装置が主要武器だった。集められた電文は IBM カードにパンチされ、そこで何か特徴が暴露されないかを発見するためインデックス化された。
本文用（Text）乱数の探知用暗号機械として Parker　machine が昭和一六年初期段階に導入、昭和一七（1942）年には Shinn　machine が、そして 1943 年になると National　Cash Register　Company により特別に作製された電動機械が導入された。

最初は暗号化された暗号に対処することがはじめだった。
二番目には、電文の最初と最後にある繰り返される算用数字グループがある種の指示符と想定した。最後のグループは明らかに日付と時刻として組み立てられていた。日時グループの直前に繰り返される指示符は意義深いように思えた。
通信文は、IBM 装置で日付毎に分類され、この推測される指示符グループ内の数字順で印刷された。
海兵隊麾下の上海傍受局は日本外交暗号を担当していた。
開戦当時、JN25 暗号の解読は主としてキャストで行われ、ワシントンでは二、三名が担当していた。
昭和一五年秋から主要暗号を解読する努力は、コレヒドールで行われた。
JN25 暗号の乱数の探知に成功した時に、ネガト局は調査班としての責任から解放された。と言っても二、三名が乱数の復元を継続していた。
暗号書初版 D、同一乱数表第四号までは、乱数開始位置は日替り鍵表、第六号からは、乱数加算符が導入された。
そして、翌昭和一六年六月より JN25 を解読作業に専念する正式なグループが発足された。
三つの発見が解読作業を飛躍的に進歩させた。
それは、差表により乱数探知のテクニック、二つ目に日付を生成する算用数字の分類、三つ目はパターン電文の原則にあった。
ハワイは JN25 の暗号解読には参加していなかったが､ハワイの惨事後に JN25 の解読に取り組むように命令されることになる。

コレヒドールが日本軍に手に落ちる危険が迫ると、これを正しく認識した、キングは日本海軍の暗号と乱数の解読の成功を危険にさらすこと避けるため、暗号解読班の完全撤退を決定した。
この出来事に伴いハワイの披弱性が問題となった。
ワシントンの OP−20−G は支援作戦の必要性に気づいた。
この結果、計画が発動された。また、OP−20−G の太平洋戦争への積極的な関与が明らかになり、OP−20−G は調整任務以上のことをしなければないと決めた。
活用する情報源を最大限に、効果的に、また努力の重複を避けるための直接関与する必要を感じた。
当時ハワイのハイポでは、惨事からの衝撃から立ち直り太平洋艦隊司令長官への諜報提供を確立していた。
この状況において、OP−20−G による統制の確立にハワイは強く反対した。
それは、暗号解読班同士の能力と情報評価の確執となった。

発端は、海軍長官フランク・ノックスが大統領フランクリン・D・ルーズヴェルトに提案し

た米海軍の劇的な再編成にあった。
合衆国艦隊司令長官にはアーネスト・J・キング大将が就任、彼はパール・ハーバー惨事にかかわる失敗を犯した者、敗北者とみなしたものを放り出し情報組織を自己の統括下に置くことを考えていた。
海軍情報部長と通信部長が標的になり、彼らは海上勤務に回された。
通信傍受を中央で管理したい考えのジョゼフ R・・レッドマン大佐が通信部長となり、OP−20−G で同じ考えを持つ弟ジョン・R・レッドマン中佐と提案を実行するため副部長ジョゼフ・N・ウェンガー中佐が同調者だった。

組織合理化指令をきっかけに指揮官ローレンス・L・サフォード中佐（1936 年 5 月～1942 年 2 月 14 日）は、左遷された。

ハワイの太平洋艦隊では惨事と結びつくハズバンド・E・キンメル大将はその地位を追われ、チェスター・W・ニミッツ少将が二階級特進して太平洋艦隊司令長官に抜擢された。
合衆国艦隊司令長官に就任したアーネスト・J・キング大将は、昭和一六年一二月七日（日本時間一二月八日）日本海軍のパール・ハーバーの奇襲攻撃以降、大統領に対し海軍長官は、米海軍の劇的な再編成を提案した。
パール・ハーバー惨事と結びつく太平洋艦隊司令長官キンメルはその地位をおわれ

米軍が JN25 と呼称し､太平洋戦争中に使用された暗号はどのようにして解読されたのであろうか。
太平洋戦争が始まる四年前の昭和一二年（一九三七）年六月三０日、米海軍省は次第に進化する OP−20−G・暗号解読班（指揮官 L・F・サフォード、1924 年以降暗号と信号部調査デスクの最初の士官、1936 年中期～1942 年 2 月まで機密保全グループ内 OP−20−G の長。大統領は日本が攻撃する前に先立つ警告を与えた諜報を見ていたと信じていた）の再編成を計画していた。

なぜ、解読できたか？
日本海軍の暗号使用の懲りない怠慢、乱数の重複使用にあった。
パール・ハーバー惨事の一週間内にコレヒドールの無線諜報班は、日本海軍の一般用暗号は基本的な乱数表が変更されたのにもかかわらず、同じ乱数表が残っていたことを突き止めた。
日本海軍は暗号の機密保全に乱数表を変えることを唯一の方法と考えていた。

明らかに日本海軍の暗号士官は過ちを犯した。
その重要な要因には、同一暗号書を異なる乱数表で組み立てる愚かな事実があった。

日本海軍暗号員のミスにあった。同乱数表で新暗号に使用する二重送信。

第一六海軍管区から昭和一六年一二月一五日発、海軍作戦部宛電報により「一二月六日と一三日の二通の AN 平文で傍受した既に探知されていた乱数開始位置を示す指示符を確認した。既に数学の減算で探知されていた、PM 暗号が変更されることなく残っていた」
PM 暗号とは（調査の必要あり）
冒頭の一語目の番電（75800）、二語目の番電（75811）の繰り返しの中に 00 と奇数二字 11（常に 11、33、55、77、又は 99）で本規程の暗号であることを確認する区別符を含み、暗号化された乱数開始位置を示す番電 758 に対応する乱数加算符（Key　Additive）表からの三語（67316）と四語目（21672）の五字宛加算符（乱数・その差は同じ）の形式は変わらず、語尾の発信日と時刻前に暗号化された乱数終了符（02658）が加えられていただけであった。

最初の解読電は、第一四海軍管区に準備された戦闘諜報班による昭和一七年一月二０日、攻撃中（解読）の AN 方式、無線諜報班はアジア艦隊司令長官に解読電の翻訳から「二つの船団の編成、速度、目的地、予定到着時間」を報告したことを第一六海軍管区に通報した。
　昭和一六年一二月二日、一五二０　機密第九０二番電　海軍大臣（官房）発、各鎮守府司令長官、各警備府司令長官、各艦隊司令長官、満洲国在海軍武官、軍令部任務 F−1−C、台北在海軍武官、南洋在海軍武官、海軍兵学校校長宛　昭和一六年一二月四日より海軍暗号書 D 及び同乱数表第八号を実施し、同乱数表第七号を停止す。海軍通信士官から。乱数表第八号を受領していない国内の通信隊がある、同通信隊は乱数表第七号を使用する。（OP—20—N 編纂・Pre−Pearl　Harbor　Dispatches）

　乱数加算符表 001～999。電番号・乱数加算符。
　K 作戦の気象情報
第二十四航空戦隊戦闘詳報第十一号「南洋部隊基地航空部隊戦闘詳報・第十一号」二四航戦機密第二八号ノ一二
昭和十七年四月二十日　第二十四航空戦隊司令部・第三令達報告等「発三月三日二〇三〇大海一部長　受三月四日宛 24sf 司令官 4F、6F 各長官通報 GF 長官浜空司令・大海機密八五四番電　天気豫察　三月四日乃五日布哇方面両日共北東乃至東北東十五米半晴積雲又沿層雲五乃至積乱雲ノ発達ナキ見込「フレンチフリゲート」方面両日共東十米晴乃至曇雲量七以上「ミッドウェー」方面四日ハ東五日ハ南東乃至南南東共ニ十米程度半晴」

ミッドウェー・アリューシャン作戦
第五航空戦隊司令部「第五航空戦隊戦時日誌・作戦及一般之部」第五航戦機密第二九号ノ

九　発二〇日一六五〇GF 長官　受二一日一五〇〇宛 GF 各長官 GF 各司令官各所轄長通報総通信隊司令
「GF 機密第一九六番電　第二期作戦期間ニ於ケル第二地点表示法ノ基点略語（括弧内略語）ヲ次ノ通定ム AF（midway）（ミ）AFG（curl　）（ユ）AFH（French・Frigate）（フ）
第五航空戦隊司令部「第五航空戦隊戦時日誌・作戦及一般之部」
発二一日一二〇〇電信課長受二二日二一四〇宛各鎮各警各艦隊参謀長「海電機密第七八一番電　昭和十七年五月二十八日ヨリ官房機密第七七三番電ニ依ル海軍暗号書 D 一同乱數表第九號ヲ実施セシメラル」

5 月 20 日　1650　GF 長官　GF 機密第 196 番電「第二期作戦期間に於ける第二地点標示法の基点略語　AF（Midway）（ミ）、AFG(Curel)（ユ）、AFH（French　FRIGATE）（フ）、AGD(LouysanI)（レ）、ヤルート島（ヤ）」
21 日　1200　海電機密第 781 番電　「昭和一七年五月二八日より官房機密第七七三番電による海軍暗号書 D 壱同乱数表第九号を実施セシメラル」
2330　電信課長　22 日 1435　各艦隊、各鎮守府、各警、参謀長、第十一、第二海上護衛隊、　海電機密第 785 番電　「最近交信上の誤字増加等の為翻訳困難なる暗号電報少なからず。五月二五日以降重要なる語句には案ずれば暗号書（発信用による）中に於ける其の所在員及び行目に数字使用数または行数のみを二重括弧内に付記せしめられた度」

日本軍のパール・ハーバーに対する攻撃後、二週間、古い暗号が新しい key と共に再び使用された。
サフォードによる合衆国通信諜報小史

自軍の通信機密保全に関する分野 GC 班、無線傍受の分野 GX 班、暗号解読の分野 GY 班、翻訳と暗号探知の分野の GZ 班で構成されていた。

戦争勃発後のパール・ハーバー惨事の反発の中で昭和一七年二月に OP−20−G の劇的な再編成が行われた。
合衆国艦隊司令長官にアーネスト・J・キング大将が任命され時点で太平洋艦隊司令長官は解任された。
戦争計画課所属の J・N・ウェンガー中佐の提起した最も強い勧告は、あらゆる通信諜報活動中央集権化で、以前の OP−20−G の責務を制限することにあった。
通信諜報と通信機密保持を分割することに反対だった。
1941 年三月から 24 時間体制。
昭和一七年二月、統制と調整、通信解析、暗号解読、情報の相互交換（電子コペック回路）、計画・訓練・人事・装備、調査と運営管理の提案に沿って再編成が開始された。

パープル暗号機は、1939 年二月一九日導入された。1934 年以来のレッド暗号機に代って。陸軍は 1940 年一０月破った。三台コレヒドール、ロンドン。

どのような電文だったのだろうか？

昭和一四年六月一日から昭和一五年九月三０日まで実施の電文の冒頭一語目 23300 は、発信者の一連番号 233 と区別符 00、二語目は暗号化された乱数開始位置指示符 79994、
そして結尾 10 文字には、再度暗号化された乱数開始位置指示符 79994、27140 の発信日 27 と発令時刻 140（時間配分は分の TENS）
それが、昭和一五年一０月一日より昭和一六年一二月三日まで通信文の前置部となる送受信所、数字符・語数、電信番号 473 に次いで冒頭一語目 75800、発信者の一連番号（機密第 758 番電）、区別符 00 を含む、二語目に機密番電の繰り返し 758 と奇数数字 11 又は 55 を含む、と暗号化された乱数開始位置を示す指示符（001 から 999 までの番電表 758 に対応する乱数加算符；67316　21672）、結尾 27150 に発信日 27 と発信時刻 150 のパターンに変りがなかった。

フィリピン・コレヒドールに測定所（CAST）を建設することになり昭和一三年より取り掛かり一六年九月に完成させ実働は一０月一五日と一七日からだった。

開戦前には D 改版は解読されていないとの通説を覆す記録には、昭和一七年一月一日、米海軍暗号解読班（OP−20−GY）は以下のプロジェクトの解読作業を完了させたとある。
（b）昭和一四年六月一日に実施され昭和一五年一一月三０日まで使用された D 暗号・初版（米軍呼称・旧 AN 暗号）の探知・復元は昭和一六年一二月一二日に中止、成果は暗号書に収録されている暗語符字の意味五三六六語を探知・復元した。
（c）昭和一五年一０月一日から昭和一六年一月三一日まで実施された暗号書 D・初版同乱数表（米軍呼称・旧 AN 乱数表第五号）も探知を中止、同乱数表に収録される五数字宛乱数五万個の内二二００個を探知・復元した。
（d）現行暗号書 D・昭和一五年度改版（米軍呼称 AN−1 暗号）の収録暗語の意味二三八０個を探知・復元した。
（e）暗号書 D 改版同乱数表第六号（米軍呼称・旧 AN−1 乱数表第一号）の乱数四一六七個を探知・復元した。
そして、プロジェクトの継続。
コレヒドールにおいて現行の AN−1 暗号・昭和一五年一二月一日実施の暗号書約六一八０語を探知・復元し、旧 AN−1 乱数表第一号一万一八六七を探知・復元した。
（f）AN−1 乱数表第七号、昭和一六年八月一日実施の乱数加算符九００を復元、乱数二五００を探知・復元した。

そして、(G) 第一四海軍管区（一二月一０日）と第一六海軍管区が現行の AN−1 乱数表第八号へのプロジェクトを開始した。
月平均約七０００通、GY により受信された日本海軍電文の六０から七五％は JN25 であった。
ネガト局暗号解読要員 GY は昭和一六年一から三月に士官七名、下士官三名計一０名、
四月から六月に士官九名、下士官五名、民間人二名計一六名、
七月から九月まで士官八名、下士官一０名、民間人二名計二０名、
一０月から一二月まで士官九名、下士官一０名、民間人三名計二二名、
昭和一七年一月から三月士官一二名、下士官七０名、民間人一名、緊急軍務用志願に受け入れられた婦人（WAVRS）一五名計九八名、
四月から六月まで士官一七名、下士官一二五名、民間人一五名、WAVRS 五０名計二０七名。
暗号書（暗語を五字宛数字に換字）と乱数表（乱数加算符と乱数五万）

解読の飛躍的な進展は、昭和一六年一二月に差分表を導入してからであった。

乱数表第五号の実施日数一二三日間（昭和一五年一二月一日から一六年一月三一日まで)、乱数五万の内二二九００を探知・復元した。
乱数表第六号の実施日数一七四日間（昭和一六年二月一日から同年七月三一日まで)、乱数五万の内四七０００を探知・復元した。
乱数表第七号の実施日数一三二日間（昭和一六年八月一日から同年一二月三日まで)、乱数五万の内三六六０を探知・復元した。
乱数表第八号の実施日数一七五日間（昭和一六年一二月四日から昭和一七年五月二七日まで)、乱数五万の内四七七０を探知・復元した。

米国の命運を左右する重大問題となったのが日本海軍の使用する地点略語 AF の解明だった。
皮肉なことに、当時この略語 AF は米海軍にとっては、中部太平洋無線傍受・方位測定網ミッドウェー海軍無線局・AF 局（昭和一六年秋完成、DF 装備 DAB／DP）を意味していた。
この「AF」確認が日本軍の攻撃目標を知る手掛かりとなっていたので、米海軍省は日本軍が米海軍と同じ略語を使用するわけがないとの認識にあった。
この AF 確認の過程で米海軍暗号解読班内に葛藤が表面化したことはあまり知られていない。
当時の日本海軍は、無線交信用に暗号書（例；「水」は第二部説話欄に五数字の暗号符字「50796」に換字して併記）発信と受信用の二冊、更に暗号化するための乱数表（注：無作為の数字五字宛の乱数で 001 から 500 ページ、各ページに横行と縦列 0 から九の乱数一００個)、そして地名を秘匿するために使用する特別地点略語表（注：暗号書にも第三部地名

欄あり)、仮名組合せの日歴換字表（注：暗号書にも第一部年月日欄あり）などを使用して暗号電文を組立てていた。ローマ字二語及び三語で構成される地点略語は地域園と特定の場所を示していた。

傍受通信文の冒頭部が算用数字を表示する暗号の意味を含んでいるという仮説を導き出した。冒頭部には暗号文解読のための乱数開始位置を示す指示符や区分符などが暗号化されていた。
数字用暗号グループに規則正しいパターンで生成していることを掴んだ。原語（収録語）と五字宛数字の相対配列位置の変更により暗号の更新となる。
同じパターンの選択間の正確な種類を描き出した。
アルファベット計算機、横行分類機、
算用数字を表示しない暗号グループ（収録語・語彙を意味する）を含む不確実な暗号グループ全てに対する三で割り切れるグループの乱数列を変換。
数字五字宛で組み合わせる各数字の和は三の倍数になるよう組成することが解読された。
電番号（機密第　番電で示す）には二つの乱数加算符を付、乱数開始位置剥ぎ取り表としていた。
偏ったページを何ども使用する傾向から、縦烈区分表に重ね合わせ統計的な頻度を生み始めた。非減算で得た差を差分表として作成。
JN25B―7（昭和一六年八月一日から同年一二月四日まで実施）の解読例；日本海軍の電報送信は、対手符号（三回以下)、自己符号（ホへ)、指定符（ホホ)、冒頭・字（語）数（ヤ＝仮名モールスでは W)、着信者名符号（チ)、受報者名符号（ツホ）発信者符号（ハ)、本文・本文（ホネ＝DQ？)、結尾・対手符号、自己符号（ホへ=DE？）の順で行われた。
そして暗語化した通信文の三語目と四語目に乱数開始位置を示す秘匿指示符を乱数加算符として挿入していた。
この秘匿したカラクリを米海軍暗号解読者は解いていたのである。
傍受した暗号文の冒頭一語目に機密第七五八番電（区別符＝本規程による暗号を他の同一型式の暗号と区別するため。
本暗号の固有番号は 00 又は 11 などを含む)、二語目も番電の繰り返し、三語目と四語目が乱数表の乱数開始位置を示す暗号化した指示符（乱数加算符)、結尾に発信日付と発信時刻が含まれていた。
米海軍暗号陣はこの日本海軍のカラクリを解読していたのであった。
受信側の確認事項ヤ（W）の字数
JN25B―8　昭和一六年一二月四日から昭和一七年五月二七日実施。例電文）TOHE3 IMU3　DE（送信局）　OSI0　―SUU（数字符）　W（字数＝ヤ）15　NR（タナ＝発信番号・タナ）429　NENENE（不明）　TI（着信者）　TUKO　KERO44　MORU249　HA（発信者）　NO849　一語目「422（機密第　番電）00（Part　Designation)」二語目「422

（機密第　番電）　55（常時奇数）注；区別符・本規程による暗号を確認」　三語目「48282」四語目「71340」　五語目「10796」　中略　「02658」　「06（日付）　145」（発信時刻）暗号化のため乱数開始位置表　左端に機密番電　例）001　から 999 までがある。
機密第四二二番電の欄には乱数第一 IND　SUB「20681」　第二 IND　SUB「53749」　と併記されている。
そこで、乱数表の乱数開始位置を示すため　冒頭一語目の機密第四二二番電から乱数開始位置剥ぎ取り表の四二二の欄にある 20681 と 53749 を取出し、暗号文にある「48282」から「20681」を非減算、更に「71340」から「53749」を非減算するとその差が共に 28601 となり第 1、第 2、第 3 字は乱数表のページ数 286 頁、第 4 字は横行を表示 0、第 5 字は縦列 1 の交差欄にある「35200」から始まる乱数列「18809」　「289609」　中略　一五語目「01821」の乱数を使用することになる。
SPSIB―1・日本暗号用語の辞書（昭和一九年九月二０日作成）日本語–英語暗号用語辞書
ANGO（暗語）＝Code　group、RANSUHYO（乱数表）＝Additive　group（乱数の集団）、IKA　SOUJI（以下挿字）＝Rest　is　padding、INNGO 隠語＝Open　code、UNA（ウナ）＝Urgent（至急の形式的な表現法）

航空攻撃は大兵力集中をもって勝負を決するというのが、当時の航空関係者一般、一航空艦隊首脳陣の用兵思想であった。
低速戦艦部隊には、空母部隊の約一昼夜航程、後方に占位させ、水上戦闘が起こった場合これを急行させる。
また空母が損傷して航行不能となった場合、戦艦ではなければこれが曳航はむずかしい。それで参加させることになった。
しかし、先頭の部隊に戦闘が起こっても、まずは戦艦部隊がこれに加入できないような後方に配した。
作戦の必要性からではなく、空母と行動を共にするのが無理な低速戦艦部隊乗員に長期間内地待機による士気の低下の傾向にあったので、士気振作を主目的として参加させた。
特に第二戦隊に関してはその傾向が強い。出撃直前になって第一機動部隊はついに戦備が完成しないため、同部隊のミッドウェー攻撃開始が一日遅れることになった。
その他の部隊もほとんど訓練を行う余裕がなく、戦力を回復しないまま出撃する有様であった。

それは単なる情報評価の問題ではなく、暗号解読の本拠地であるネガト（ワシントン DC にある暗号解読を含む通信諜報班）と第二エシュロン・ハイポ（ハワイ・ホノルルにある戦闘諜報班）の暗号解読と情報評能力を示すものであった。
日本軍をトリックに掛け攻撃目標となる地点略語 AF がミッドウェーであることを確認するための逸話は、戦時中ハワイの一部通信諜報関係者間のみが知る話題であった。

日本軍にばれることを見据えたうえで平文を使用して蒸留プラントの故障を告げる無電をハワイ第一四海軍管区からミッドウェーに送ることを指示したものであった。
この暴露記事以降、ミッドウェー海戦における米軍大勝利の要因には、このトリック偽電の記述が付きものとなっていた。
しかし、二七年前の昭和六０年、語り伝えられたトリック偽電に関する真相が、当事者から明らかにされると更に深い別の局面が暴露された。
ネガトとハイポのどちらが情報をうまく評価できるかというライバル意識に油を注いだ。
「ミッドウェーに関して記述したあらゆる歴史家によって賞賛され、誤って解釈された才気あふれる一片の偽電に着手したのは、ワシントンの懐疑的な指導者（日本軍の攻撃目標は、米本土西海岸または南西太平洋方面であると信じ、ハイポは手の込んだ日本軍の罠にはまっている）を黙らせることにあった」というのであった。
ハワイ・パール・ハーバーの戦闘電諜報班・ウルトラ・シークレット、ブラック・チェンバーの賢明な若き士官ジョセフ・J・ロシュフォート指揮官が指示させた。

19　MAY1942　　190913 送信形式 CABLE　発：CINCPAC、 宛：CO　NAS　MIDWAY　通報：COM14　「DECODE　CINCPACS　＃190725　USING　20th　SETUP」。
そして二日後、暗号解読陣は「現在、われわれは二週間分の水しかない。至急送られたし」という日本軍高級指揮官の電報を傍受した。
こうして、計画された日本軍の大規模な攻撃目標が、ミッドウェーと確認した。
この物語は、数多く出されるミッドェー海戦に関する戦記に必ず出てくる挿話である。
物語はそのような単純な話ではなく、この背景には海軍内部通信諜報班内における争いがあった。

ミ文書とッドウェーの暗号解読の裏舞台；
硫黄島上陸地点の**うずら石**＝白と黒の混ざった、みためは渋い灰色でうずら模様があった。

三年八ヶ月に及ぶ日米太平洋戦争において、日本敗北要因となる最初のつまずきがミッドウェー作戦にあったことは今では広く知れ渡っている。
日本海軍が誇り、最強と確信していた主要航空母艦四隻と精鋭の艦上機二九九機（補用機と二式艦上機一一型二機を含む）が失われ、大打撃となった。
その舞台となった太平洋に浮かぶミッドウェー環礁は、直径一一キロメートルの礁内南部西側にサンド島、東側にイースタン島そして礁湖からなっていた。
横須賀から直線距離で約四一七六キロメートル、ハワイ・オアフ島からは約二一二三キロ

メートルに位置していた。
今でも飛行機定期便がない本環礁は米合衆国の領土ではあるが、いずれの州にも属さない連邦政府直轄の「離島領土」である。
その切っ掛けとなったのが同環礁に生息するコアホウドリの価値ある羽根をとる日本人密猟にあった。
米政府が日本の実効支配を恐れ米海軍の管理下に置いたことを公表したのが明治三六（一九０三）年一月二五日であった。
そして、現在では米国内務省の魚類野生生物局（FWS）の管理下、ミッドウェー環礁国立野生生物保護区となっている。
この辺境の環礁が一般に注目を浴びたのは、終戦四年目の昭和二四年三月二六日付サターデー・イーブニング・ポスト誌に掲載された**J・ブライアン、Ⅲ世**による記事「Never　Battle like　Midway」（ミドウェーのような戦いはなかった）にあった。
この記事より、七０年前に日米戦の勝敗を逆転させミッドウェー海戦前、日本の攻撃目標を知るため日本海軍をトリックにかけ地点略語 AF がミッドウェーであることを確認した米暗号解読者の秘話が明らかにされた。
それは、日本軍への同環礁の真水不足に関する、やらせ電文「現在、われわれは二週間分の水しかない。至急送られたし」にあった。
この逸話は、米海軍がミッドウェー海戦勝利の象徴「日本海軍を罠にかけた電文」としてこれまで歴史家に数え切れないほど引用されてきた。
しかし、当時の米太平洋艦隊司令部情報参謀エドウィン・T・レートン中佐（主筆途中亡くなられたので、ロジャー・ピノーとジョン・コステロの共著で完成）が昭和六０（一九八五）年に上梓した「AND　I　WAS　THERE　Pearl　Harbor　and　Midway—Breaking the　Secrets」（TBS ブリタニカ；太平洋戦争暗号作戦・アメリカ太平洋艦隊情報参謀の証言。邦訳毎日新聞外信グループ）のなかでこのやらせ電文が練り上げられた真相は、実は米海軍省内にある暗号解読班の誤りを正すことにあったことを四三年ぶりに暴露した。
「ミッドウェーに関して今までに記述した歴史家が誤って解釈してきた騙しの電文が発案された狙いは、ハワイ第一四海軍管区（一九二五年日本外交通信コピー操作員一名）戦闘諜報班指揮官ジョセフ・J・ロシュフォート中佐が、パール・ハーバー惨事の記憶が生ナマしく、その時に警告を出せなかった無線諜報班を信じないワシントン DC の懐疑的な提督（日本軍の攻撃目標を米本土西海岸または南西太平洋方面と信ずる）たちを黙らせることにあり、また、この偽電の対象が、海軍省内の暗号解読者にあることを疑わせないことが最も重要なことであった」という。

ミッドウェー作戦を前にして米海軍内部で一体何が起こっていたのか、また日
ドウリットルの任務は、日本の工業地区を爆撃すること、その爆撃効果は、物理的と心理面両方を望んでいた。

物質的な損害は、日本の工業生産の妨害と混乱を引き起こすような特別な標的を破壊すること。
心理的効果は、米国民の戦意高揚を得る。連合国の関係を好転させ、そして日本国民に恐怖と脅迫観念を増長させる。
さらに、本土防衛のたねの第一線から兵力の一部を引き揚げさせることを目論んだ。

解読は配列の特質を示す乱数列が特定の
昭和一六年七月一日、RIP73D は、日本海軍暗号 D と昭和一五年度改版 D の additive　key（乱数加算符）一０月から一月と現行までの乱数加算符　一五日頃に RIP74D（AN と AN―1 暗号の加算符）と RIP79（AN―1）が完成予定。
昭和一六年八月一日、RIP74D と RIP79（AN―1）が七月一日に完成した。
旧式 AN 暗号の意味約二二００語を探知・復元。AN 暗号乱数表第五号のすべての乱数加算符の剥ぎ取り探知。七五００の乱数探知。
AN―1 暗号昭和一五年一二月一日実施の約二０００語の意味を探知・復元。
コレヒドール・プロジェクト；AN―1 暗号乱数表第六号、すべての乱数開始位置の剥ぎ取り探知。四八００の乱数を探知・復元。
昭和一六年九月、AN 暗号を約二三五０語の意味を探知・復元。旧式 AN 暗号乱数表第五号の乱数開始位置の剥ぎ取りを探知、一万の乱数を探知・復元。
第一六海軍区プロジェクト；AN―1 暗号乱数表第五号（旧式第一号）すべての乱数開始位置の剥ぎ取り探知、五四００の乱数探知・復元。
第一六海軍区プロジェクト；AN―1 暗号乱数表第七号（旧第二号）昭和一六年八月一日実施、準備段階。
昭和一六年一０月一日、AN 暗号旧式約二五００語の意味を探知・復元。AN 乱数表第五号（旧）AN と AN―1 暗号用加算符（additive　key　cipher）すべての乱数開始位置剥ぎ取り探知・復元。一万四００の乱数を探知・復元。
AN―1 暗号現行、改版 D 暗号約二四００語の意味を探知・復元。
第一六海軍区プロジェクト；AN―1 乱数第一号（旧）すべての乱数開始位置の剥ぎ取りの探知、七二００の乱数を探知・復元。AN―1 乱数表第七号（第二号）現行四九の乱数開始位置の剥ぎ取り探知。
昭和一六年一一月一日、AN 暗号（旧）二００語の意味を探知・復元、AN 乱数表第五号（旧）四０００の乱数を探知。
AN―1 暗号現行六００語を」探知・復元。AN―1 乱数表第七号（第二号）、二０一の乱数開始一の剥ぎ取り探知・復元。
昭和一六年一二月一日、AN 乱数表第五号（旧）四０００の乱数を探知・復元。AN―1 暗号現行八００語の意味を探知・復元。第一六海軍区プロジェクト；AN―1 乱数表第六号（第一号）現行九００の乱数開始位置と二五００の乱数を探知・復元。

昭和一七年一月一日、昭和一六年一二月に完了。AN 暗号（旧）昭和一四年六月一日から昭和一五年一一月三０日間実施、探知は昭和一六年一二月一二日中止。五三六六語の意味を探知・復元した。AN 乱数表第五号（旧）昭和一五年一０月一日から昭和一六年一月三一日に実施。探知を中止。おそらく五万の乱数の内約二万二０００を探知・復元。AN―1 暗号現行二三八０語の意味を復元・探知。AN―1 乱数表第六号（旧第一号）四一六七の乱数を探知・復元。
継続されるプロジェクト、AN―1 暗号現行、昭和一五年一二月一日実施、約六一八０語の意味を探知・復元。AN―1 乱数表第一号（旧）第一六海軍区プロジェクト；一万一八六七の乱数を探知・復元。AN―1 乱数表第二号（旧）昭和一六年八月一日実施、九００の乱数開始位置の剥ぎ取りを探知・復元。二五００語の意味を探知・復元。
第一四海軍区と第一六海軍区プロジェクトは昭和一六年一二月一０日開始された；AN―1 乱数表第八号（現行第三号)。コレヒドールからパール・ハーバーに昭和一六年一一月に到着するはず。

戦争の始めの三年間､日本海軍の主要暗号方式は米海軍暗号陣により JN25 として指定された方式であった。乱数により暗号化された乱数五字暗号であった。昭和一四年六月一日に現れ、この暗号方式は、

主戦場は、イースタン島の北三七０・四キロメートルの海域であった。
200 海里（370・4km）現在でも簡単には渡れない。
ミッドウェー（環礁西側にサンド島、東側にイースタン島）への飛行機定期便はない、集団を募ってのチャーター旅客機のみである。
ハワイ・ホノルルから西に約三時間 B–17　投下爆弾三一七発　命中率の分析は四・一%であったが、全弾外れた。

第一六任務部隊
六月四日第一次攻撃　12 時 25 分～12 時５０分　加賀、赤城、蒼龍　一０００ポンドと五００ポンドが数度命中
第二次攻撃　19 時 05 分～19 時 15 分飛龍 100 ポンドと 500 ポンド爆弾が繰り返し命中。艦首から艦尾にかけて激しく炎上。攻撃位置　北緯二九度三三分、西経一七五度三五分
JN25B の改版暗暗号書収録語探知は、昭和 16 年 4 月 1 日から 12 月 1 日までに延べ約 1 万 700 個を探知していた。Text 乱数の探知用暗号機械として Parker　machine が昭和一六年初期段階に導入、昭和一七（1942）年には Shinn　machine が、そして 1943 年になると National　Cash　Register　Company により特別に作製された電動機械が導入され昭和一六年の乱数表第五号・実施日数 123 日間収録数五万、復元・探知数 22900 個、第六号 174 日間収録数五万、復元・探知数 4700 個、パール・ハーバー前の第七号 132 日間収

録数五万、復元・探知数 36600 個、ミッドウェー作戦前の昭和一七年の第八号・実施日数 175 日間収録数五万、復元・探知数 47700 個だった。乱数探知の最大躍進には、一二月一日に導入された「差分の表」があった。

特定地点略語表 AF＝ミッドウェーにまつわる解読秘話　41×36＝1476　5・6／36 枚
主力空母の搭載機数
主力空母部隊は、開戦後の戦訓により昭和一七年四月編制が改正され、従来各航空戦隊に編入されていた警戒駆逐艦（空母随伴駆逐艦・通称とんぼ釣り）を廃止、
新たに第一０戦隊を加えた。
第一０戦隊は、三駆逐隊で編成され、その一隊が一二糎七高角砲八門を装備し、航続力も大きな防空駆逐艦、一隊は新鋭の航続力が大きい駆逐艦、他の一隊は比較的に古い駆逐艦で編成されていた。
長良（九四式水偵一機）、
第七駆逐隊（）、
第一０駆逐隊（秋雲、夕雲、巻雲、風雲）、
第一七駆逐隊（谷風、浦風、濱風、磯風）。計画は、軽巡洋艦を旗艦とする防空駆逐艦四個・駆逐隊とする。
五月三日、一航戦・赤城（零式艦戦一八／補用機三機、九九式艦爆一八／補用機三機、九七式艦攻一八／補用機三機）と
加賀（零式艦戦一八／三補用機、九九式艦爆一八／三補用機、九七式艦攻三０／補用機三機）、
二航戦・蒼龍（零式艦戦一八／補用機三機、九九式艦爆一八／補用機三機、九七式艦攻一八／補用機三機、二式艦偵二機）、
飛龍（零式艦戦一八／補用機三機、九九式艦爆一八／補用機三機）、
四航戦・龍驤、祥鳳（五月七日沈没）、隼鷹（五月三日編入）、
五航戦・翔鶴、瑞鶴であった。
第一機動部隊（指揮官・司令長官南雲忠一中将）ミッドウェー作戦時には、一航戦、二航戦の四隻、五航戦は内地に待機とされた。
警戒兵力は、第八戦隊（利根・九五式水偵二機、零式水偵三機）、
筑摩（九五式水偵二機、零式水偵三機）、
第三戦隊第二小隊・霧島（九五式水偵三機）
榛名（九五式水偵三機）、
第一０戦隊（欠・第七駆逐隊）
第四水雷戦隊の第四駆逐隊（野風、嵐、萩風、舞風）、
給油艦五隻（旭東丸、神國丸、東邦丸、日本丸、國洋丸）が付された。
補用機三六機と臨時搭載二式艦偵二機を含む損失は、合計二九九機であった。

洋上における最大攻撃距離おおむね二五０浬であった。
当時の機動部隊は源田艦隊と評する者があった。
従って、一航艦司令部の航空作戦指導は、源田参謀の用兵思想に影響されることが絶大であった。
源田参謀は、空母を集団使用すれば防空戦闘機を多数配備できるので、敵の攻撃に対処できると考えていた。
「空母を集団使用して上空警戒機を多数集中すれば、敵の航空攻撃を阻止できる」と断言していた。
一航艦首脳部の用兵思想は、航空攻撃は大兵力を集中して、一撃をもって勝敗を決める。
南雲司令長官は、航空作戦の計画や指導などには少なくとも、ほとんどイニシチアブルをとることはなく、幕僚の意見を「うんよかろう」と決裁していた。
参謀長草鹿中将もまた、ほとんど口を出さなかった。
参謀長宇垣纏と二航戦司令官山口との会話。一航艦司令部は誰が握り居るやの質問に対し「長官は一言も言わない。首席参謀大石保中佐航空甲参謀源田實中佐、航空乙参謀吉岡忠一少佐、航海、通信、機関参謀虚空作戦の計画も指導も、源田参謀の意見がほとんど全部とおる有様であった。
源田参謀は、自己の案画した計画や指導がなんの批判もなく長官、参謀長をとおることが、さびしい、ともらしていた。機関参謀坂上五郎参謀機少佐の回想。

作戦要領；第一機動部隊は、N マイナス一一日内海西部を出撃、対潜警戒を厳にしつつ第一航路を採って進出する。
N マイナス二日黎明、ミッドウェーの北西二五０浬付近に進出し、ミッドウェー攻撃隊を発進させて同島を奇襲、所在の敵機、防備施設を撃滅する。
蒼龍の艦攻一八機爆装、飛龍艦攻一八機爆装、赤城艦爆一八機爆装、加賀艦爆一八機爆装。制空隊赤城、加賀、蒼龍、飛龍各艦戦九機。艦船攻撃の編制；赤城艦攻一七機、加賀艦攻二六機を雷装、蒼龍、飛龍各艦爆一八機を爆装、各艦戦闘機六機。
状況により同島の北方から攻撃することがある。
また状況により同日再度ミッドウェーを攻撃することがある。
索敵はミッドウェー付近の広範囲警戒を厳にする。
ミッドウェー攻撃の間、母艦搭載機の半数は敵艦隊の出現に備えて艦上待機を行う。
現実には攻撃日はＮマイナス二日になった。
その前日に船団部隊が敵哨戒機に発見される公算が大きくなったが、なお奇襲が成り立つものとして、新事態に応ずる攻撃計画の変更を行わなかった。
五月一八日鹿屋基地において航空関係者だけの、また出撃前日二六日「赤城」艦上において作戦計画の説明と打ち合わせを行なった。
重要な作戦転換は聯合艦隊が指示することに落ち着いた。

1944 年 11 月 2 日、太平洋艦隊無線班用の場所名。無線局 H＝ワヒアワ、A＝グァム、AF＝ミッドウェー、AH＝パルミラ、AI＝ジョンストン島、AL＝ガダルカナル、
OP―20―GY　昭和一六年一二月の完了プロジェクト ; AN 暗号　（旧式）昭和一四年六月一日実施、昭和一五年一一月三０日まで。探知・復元を昭和一二月一二日に打ち切る。意味五三六六語を探知・復元した。
AN 暗号乱数表第五号　（旧式）昭和一五年一０月一日から昭和一六年一月三一日まで実施。探知を打ち切る。約五万の乱数の内二二００を探知・復元した。
現行の AN―1 暗号　二三八０語を探知・復元した。

1942 年１月１日　AN―1 暗号　現行　実施日は昭和一五年一二月一日　およそ六一八０を探知・復元した。AN―1 第一号（旧式）一六海軍管区プロジェクト一万一八六七の乱数を探知・復元した。
AN―１第二号（旧式）昭和一六年八月一日実施、九００の加算符を探知・復元、二五００の乱数を探知・復元
AN―1 第三号　第一四と第一六海軍管区プロジェクト

ワシントンの懐疑的なものを黙らせるために、ロシュフォートはミッドウェーの真水不足に関するいかさま電文を送信する計略をでっち上げたとき、彼の意図は、ニミッツが正しいことを納得させるためではなく、ワシントンの誤りを分からせることにあった。その発想は、ジャスパー・オルムズからもたらされた。ミッドウェーに関していままでに書いたすべての歴史家によって誤って解釈された（誤って説明）才気あふれる一片の電文に着手した。

昭和一五（一九四０）年八月一九日、ドリスコル、テリイ、クラーク、カイソルム、マックグロウジャ、コッケンの六名が担当した。
一０月四日、暗号書と共に乱数の中に鍵となる乱数が使用されている。
探知の方法は充分に意味を理解しているが、その過程は多くの時間と労力を要する根気がいる。
個々の電文には、それは一時間から数日を必要としている。
専用の暗号機は目下製作中である。解法の応用に助けとなるメカニカル部品は、現在製作中である。しかし、直ぐには活用できないことを受け入れなければならない。

数個の暗号の意味は既に探知されているが、完全に電文を読むことができるまでに少なくとも六ヶ月要するであろう。
探知・復元は、ワシントンにより追求されている。その詳細は、後に公表される。

OP―20―GY（暗号解読課）　GY―１班は、JN25 の新しい鍵となる使用規程、乱数加算符表の探知・復元、乱数表（完全ではないが、通信の大部分を解読するに十分な探知・復元）
定員；一九四一年一月から三月に士官七名、下士官三名の計一０名、
四月から六月に士官九名、下士官五名、民間人二名の計一六名、
七月から九月に士官八名、下士官一０名、民間人二名の計二０名、
一０月から一二月間に九名、一０名、三名の計二二名、

昭和一七（一九四二）年一月から三月に士官一二名、七０名、民間人一名、婦人一五名の計九八名、
四月から六月に士官一七名一二五名、民間人一五名、婦人五０名の計二０八名。

本当にミッドウェー水不足のトリックにより米軍は、AF＝ミッドウェーを知ったのか！
何時 AF がミッドウェーをしったか。
昭和一七年三月四日、早くも気象通報の解読からしった。
どう語り継がれたか？
1942 年五月一五日、ルーズヴェルト大統領は、婦人陸軍設立を、七月三０日海軍に婦人を受け入れする申請書に署名した。

日本海軍暗号の大部分を破ったとして
ミッドウェー環礁が日本に実効支配されるのを恐れた米大統領の判断
日本海軍の暗号は、どうして解読されたのか！
作戦が決定された背景
南雲忠一中将（海兵三六期）は、水雷出身で航空の経験は皆無であった。
指揮官に任命されたのは年功序列からであった。
参謀長草鹿龍之介少将（海兵四一期）は航空関係の仕事を経験していた。
新編の第一航空艦隊の航空参謀には、ハワイ作戦の原案を作成した源田実が起用された。
これ以上の適任者はいなかった。
聯合艦隊司令部は、主張するセイロン攻略作戦が陸軍に反対で取りやめとなり、同司令部はそれが認められなかった憤激も加わって、独自のミッドウェー作戦を含む一連の作戦を力強く進めていた。
その頃迄には軍令部の聯合艦隊司令部を引き締める手綱はほとんどその効果がなくなっていた。
日本海軍の作戦に関する限り、最高司令部が二つ存在するという異常な状態になっていた。
風化させてはならない歴史的な教訓の一つにミッドウェーの戦いがある。太平洋戦争三年八ヶ月、の最初の敗北がこの戦いであった。

歴史として伝えられていることが、その出来事の真相を伝えているとは限らない。
歴史とは、現在との連続性をもつに至った過去と生きている現在との対話である。
現在は、過去と未来とからなる連続線上を動く極めて小さな点に過ぎない。
過去に対する判断基準として未来というものを強調することは、全く論理的である。
歴史とは、過去と未来とを一本の連続する線に結び合わせようとするものである。

官僚組織の中で温存、継続、再生、日本人の習性、教育、制度が情報の軽視、専門知識の不足、その場凌ぎの対応がある。

占領後の名前は「水無月島（みなずき)」と予定されていた。
仮称・秘密保全法案提出難航（平成 24・2012）年 3 月 4 日「知る権利」妨げる懸念　政府高官は、「秘密保全法案は反対も強く、優先順位も高くはない。
今国会に出す方針を決めた手前は、出すだけ出すかもしれないが、成立は難しい」と語っていた。
重要情報の管理がずさんでは、日本の国際信用が失墜、政府内の情報共有にも支障が生じかねないと「政府における情報保全に関する検討委員会が発足した。
報告書は、「国の安全」「外交」「公共の安全と秩序維持」の三分野で特に秘匿を要する情報を「特別秘密」に指定。故意に漏洩した国家公務員らに厳罰を科すとした。
こうした動きに対し、日本新聞協会は昨年一一月、「憲法が保証する取材、報道の自由や国民の知る権利を侵害する恐れがあるとして、「運用次第では通常の取材活動も罪に問われかねない」との懸念を示した。

Additive　Applying　Position
作業電文の順序　1）桃色　2）緑色　3）黄色　4）白色　5）オレンジ色カード電文は、同じ色の作業紙に関するほかの全て以上に優先権を持つ。暗号解読は、暗号法（方式）の解析に左右される。乱数復元作業者は、少なくとも 6 ヶ月から 9 ヶ月を継続して訓練する。

気象暗号と事務電が深く関わっていた。
海軍作戦の様相に関する山本司令長官の読みが当を得たもので、当然、山本の成果は急上昇、それと同時に山本のハワイ作戦に執拗に反対した軍令部が、山本に対してある種の負い目を感じたのも事実であった。

1347 日　引き上げられた暗号書は、伊 33 号潜水艦のもの。
昭和 28 年 7 月 23 日、愛媛県興居島西方 13km において引揚　行政文書の開示実施方法などの申出書　軍極祕　海軍暗號書呂　特定地点略語表（甲)、留第一乱数表（第二號）

海軍書 D と原語と符字（五数字）の相対配列位置の変更以外には形式も内容も殆ど変わりないと伝えられている。
収録されている原語と暗号符字（乱数）を入れ替えて、別の暗号符字（乱数）に変更、一新し、新しい暗号書として印刷することを更新と呼ぶ。
部分的な更新は、使用頻度の高いだけを更新すること。

二十一世紀の情報戦は、無線電波の傍受や妨害を対象とした電子戦、コンピュター・ソフトウェアを対象としたサイバー戦、敵の指揮統制機能を混乱、妨害する意図をもつものとなる。

実効支配
米内務省の魚類野生生物局（FWS）の管理下にありミッドウェー環礁国立野生生物保護区となっている。
ミッドウェーは 70 年前に日米戦の勝敗の流れを逆転させる舞台となった。
本環礁は合衆国の領土ではあるが、いずれの州にも属さない、連邦政府直轄の「離島領土」である。
米軍の沈没は空母一隻、駆逐艦一隻、戦死者米側三六二名（内搭乗員二０八名)、日本側は空母四隻と重巡洋艦一隻が沈没、三０五七名（内搭乗員一二一名）であった。
実効支配の原因は、栄壽丸（木造帆船 77 トン 32）コアホウドリの乱獲。
1949 年 3 月のサタデイ・イヴニング・ポスト紙に
米軍が平文で打った「ミッドウェー・AF に真水が不足している」との偽電に引っかかり、それをご丁寧にも暗号化して打電､それが傍受され AF がミッドウェーと確認されてしまう。
佐薙毅海軍大佐「あの頃暗号書を変えている」
関口鐵造海軍中佐　第一水雷戦隊の暗号
海軍暗号書 D は、数字暗号にして使用に慣熟、大部の通信は本暗号書に依った。

MI 作戦迄は順調に経過し、冒頭強化用の統一暗号書定。海軍特定暗語書 A は、隠語書であった。
多表解読の一般的方法；必要量は縦列段数によって決定する。同一形式必要量は、原文の性質と原文に関する事前の知識によって異なる。
JN25 復元（Code　Recovery）解読経験による感の働き　数字は発音通り。
長音は母音を重複　拗音をX。
暗号文を解くには原文の特徴を調査しておかねばならない。
暗号文の縦列毎に P の縦列の文字を書き込みながら、2 文字連接度表を作る。この表を使用しながら長反復調査をする。その結果、暗号文に線で印をする。原文の縦列表と暗号文の調査表を比較しながら推論する。

各縦列毎に異なる文字換字表で換字されており原文は横に文字ずらすことを頭に入れて拠点を入れる。ここで文字の度数分布に関　連接特徴　原文仮定と推論（特に連接度数）演錬　田辺一徳　鈴木正治助手
原文が何か分からない場合には、反復に形及び算用数字から原文の性質　原語の種類などを特定する。
単文字反復組成と推定　2 文字連接　3 文字連接　反復生起率　資料が増加するに連れて縦推定は確度を増す。
一致反復をその数と分布　単文字　形態修正連続反復の真偽判定　判定図表の作成　分布曲線を描き　真反復　偽り反復　開始位置の秘匿法が完全でないため、いくつかの組の縦列区分したものを比較総合して解読できる。
LOG　SMS　START　W／C　MO　DAY　LINE（0~9）
縦列区分された多表式暗号文は、区分された縦列の長さ、及び段数か形式に応じる条件を満す量（七～八段）に達すると解読可能になる。
ワシントンとハワイは、コルヒドオールのみに対して、1941 年秋には現行の JN25 に対する作業はしていなかった。

聯合艦隊司令長官山本五十六大将は、「日本本土、特に帝都空襲を絶対にさせてはならぬ」との固い信念をもっていた。
ハワイ奇襲攻撃で打ち漏らした米空母が日本軍の南方作戦の虚をついて、マーシャル諸島、ウェーキ島、南鳥島に奇襲をかけてきた。聯合艦隊は、その対応に苦慮していた。
一九四二年三月八日、聯合艦隊司令部は軍令部に伝えたセイロン島攻略作戦（中止の要因；GF は陸軍三個師団の使用を予定していたが陸軍の反対によって計画が成り立たなくなった）が陸軍の反対、軍令部も反対とあって作戦はお流れとなったことを知った。

そこで聯合艦隊は、陸軍兵力を使用しないで、例え戦力不充分でも米海軍に立ち直りを与えない海軍単独の、応急的、支作戦の採用を考えた。
それが、米空母の誘出撃滅を目的としたミッドウェー作戦であった。

哨戒線の前進も第二義的なものであった。
本作戦に絶対反対を作戦課全員で表明した軍令部軍令部作戦課三代一就中佐と同期の聯合艦隊参謀主務者渡邊安次中佐の間で大激論となった。
不沈の航空基地に空母で攻撃する戦術的な愚策、奇襲は考えられない強襲になる、占領（軍政事項になる）しても維持は困難、補給は誰がやるのか等、軍令部の反対理由に対し渡邊参謀は、一歩も引かず、議論で説得できないと思うと四月五日「この案が通らなければ山本司令長官は辞職すると言っておられる」と伝家の宝刀を出した。
これは軍令部に来る前に山本司令長官の下で聯合艦隊参謀長をやって、山本がどんな人物

か知っていて説得し易い軍令部伊藤整一次長、軍令部福留繁第一部長を引っ張り出した。
そこで福留一部長の「お任せしましょうか」に伊藤次長が「そうですな」と答え作戦が決まった。
そうなれば、永野修身総長もハワイ作戦の時と同様に「山本に自信があるなら」ということになり、その代わりの交換条件である軍令部立案のフィジー・サモア攻略作戦を聯合艦隊に承諾させ、上からの決定でミッドウェー作戦に断が下った。
山本司令長官には、真珠湾奇襲、ミッドウェーにしても、これ以外に戦争の早期終結を図る決め手はない、もし作戦が不成功に終わったら、それによって中央で講和を考えてもらえばいいくらいの強い意図と、いうに言われぬ決意があったといわれている。
長期戦を避け可能な限り短期戦、速戦即決が海軍戦争指導者の願望であった。
四月一九日のドウリットル空襲後、陸軍は突如、MI にも AO にも、補給は海軍担任として、なるべく速やかに陸軍部隊を返すよう考慮する条件の下に陸軍兵力を出す旨申し入れがあった。
MI 作戦は益々哨戒線の前進が第一目的の様相を呈し、軍令部作戦課は、敵艦隊捕捉撃滅より要地攻略して哨戒線を前進させることの主眼を置くようになった。

「赤城」航空通信電波の水晶発振子量不足の為、甲種通信の予備電波、制空隊戦隊嚮導、所定の電波に対し三割の余裕を供給し、作戦開始前の人事異動は艦隊乗組員の戦力の低下を来たし、その回復は容易ではなかった。

二０一二年六月、太平洋戦争の勝利の流れの転換点となったミッドウェー海戦は、日本軍の攻撃目的、時期、兵力が相手側に漏れたことが要因となって米側の勝利に終わった。
焦点となった日本海軍地点略語表示「ミッドウェー」を意味する「AF」の解釈は、奇しくも日米両海軍がミッドウェーの略語を「AF」として使用したことにあった。
米海軍傍受班が使用する略語「AF」をめぐりワシントンとハワイの諜報班の対立を呼ぶことになる。

可能性が濃厚だった。

一九八三年一一月三０日付大統領行政命令第 12356 号による機密解除文書・History of COMINT Operations 1917―1959 は日本海軍がパール・ハーバーに対する攻撃後の二週間、古い暗号がサンゴ海の戦いの間中、使用され続けた。
そして、ミッドウェーの戦いを立ち上げた。
その解読法は、これら二つの戦いにおいて作戦中の部隊に大きな手助けとなった。（一九九三年一一月に公文書館入りした）

1347 日間・日本敗戦の原因第一号となったミッドウェー海戦の敗北　加賀と蒼龍は 179 日目、赤城と飛龍は 180 日目で失われた。

地点略語 AF がミッドウェーは、米海軍に海戦が始まるおよそ三ヶ月前・昭和一七年三月四日に探知され、四月二三日にジョン・レッドマンに「AF はミッドウェーに訂正された」と報告されていた。

隠蔽工作のはじまり　ミッドウェー・アリューシャン作戦、ずさんな戦闘報告による「い」号作戦と台湾沖海戦の大勝利報告は、全く事実と異なるものであった。

米海軍は情報の勝利と高らかに謳いあげた理由　暗号解読を含む通信諜報、他には日本軍が破壊しなかった真珠軍港の燃料タンク、航空燃料を満載してきた給油艦「ネオショウ」を見逃したことが、米軍の反撃を可能にした。日本軍は開戦の利用として燃料欠乏による戦わずして敗れることを極度に恐れながら、米軍がハワイの燃料を失い行動の自由を失うことは考慮しなかった。
なぜ、日本海軍の暗号は解読されたか　同一暗号書に旧新乱数表を使用した
絶対安全という日本海軍の暗号方式の中身
使用規定の過ちを繰り返す懲りない暗号員
懲りない面々
テレビで草鹿参謀長は怠慢があったと謝ると一緒に参加していた下士官兵が怒った「我々はいつも一生懸命　何も言えず

「アイゼンハワー将軍の指揮する欧州戦線だけでなく、太平洋戦域の於ける全作戦が暗号解読にもとづく情報に依存している。日本軍に対する暗号解読情報は、現在の諸作戦を円滑に進めているだけでなく、戦争の早期終結を可能にするため、さらなる勝利と多くの米兵の生命を救うことに、計り知れないほどの貢献をしている」現在のジレンマは連合軍が日本軍の複数の暗号を解読する最大の努力を続けていると同時に日本軍の暗号同様にドイツ軍の暗号も解読していることにある。
連合軍のヨーロッパに於けるに関する主要な情報源は、ヒットラーと他の高官とのインタヴィューを報告する大島浩男爵のベルリンから日本政府に打電される電報から入手されている。
これらの情報には、一九八三年一一月、惨事の中にあった暗号がまだ使用されている。
もし、ほんの些細な疑念を相手側に感づかれると、一瞬に失われる。

K 作戦の気象情報

第二十四航空戦隊戦闘詳報第十一号「南洋部隊基地航空部隊戦闘詳報・第十一号」二四航戦機密第二八号ノ一二

昭和十七年四月二十日　第二十四航空戦隊司令部・第三令達報告等「発三月三日二〇三〇大海一部長　受三月四日宛 24sf 司令官 4F、6F 各長官通報 GF 長官浜空司令・大海機密八五四番電　天気豫察　三月四日乃五日布哇方面両日共北東乃至東北東十五米半晴積雲又沿層雲五乃至積乱雲ノ発達ナキ見込『フレンチフリゲート』方面両日共東十米晴乃至曇雲量七以上『ミッドウェー』方面四日ハ東五日ハ南東乃至南南東共ニ十米程度半晴」

ミッドウェー・アリューシャン作戦

第五航空戦隊司令部「第五航空戦隊戦時日誌・作戦及一般之部」第五航戦機密第二九号ノ九　発二〇日一六五〇GF 長官　受二一日一五〇〇宛 GF 各長官 GF 各司令官各所轄長通報総通信隊司令　「GF 機密第一九六番電　第二期作戦期間ニ於ケル第二地点表示法ノ基点略語（括弧内略語）ヲ次ノ通定ム AF（midway）（ミ）、AFG（curl　）（ユ）、AFH（French・Frigate）（フ）

第五航空戦隊司令部「第五航空戦隊戦時日誌・作戦及一般之部」発二一日一二〇〇電信課長受二二日二一四〇宛各鎮各警各艦隊参謀長「海電機密第七八一番電　昭和十七年五月二十八日ヨリ官房機密第七七三番電ニ依ル海軍暗号書 D 一同乱數表第九號ヲ実施セシメラル」

海電機密第七八五番電　最近交信上の誤字増加等の為翻訳困難なる暗号電報少なからず五月二十五日以降重要なる語句には要すれば暗号書（発信用に依る）中に於ける其の所在頁及行目に数字使用数または行数のみを二重括弧内に付記せしめられ度」