暗号・情報保全史特論
History of Cryptograph and Signal Security Advanced Course

第7回: 多表式暗号の解読技法と暗号の運用

佐藤永欣

多表式暗号に対する攻撃手法

- 多表式暗号では換字表が切り替わるためランダム性が高い
  - 多表の枚数を増やすことは困難
    - 手作業の場合は暗号化・復号化の作業が困難になる。機械式の場合は手作業の場合よりも増やせるが暗号機が大きくなる
  - 換字表を規則的に切り替える: 大抵は順次切り替え→切り替え周期が発生
  - 切り替え周期を知ることができれば鍵の発見が容易になる
- カシスキーの方法
  - Cribを頑張って発見→鍵長を推定
- ケルクホフの重ね合わせ
  - 資料がない…。つらい
- フリードマンの一致反復率
  - 統計的な攻撃

多表式暗号に対する攻撃手法: カシスキーの方法

- カシスキー(プロイセン, １９世紀後半の人)
  - C.バベッジ(イギリス人, 解析機関や階差機関などの業績がある)がヴィジュネル暗号への攻撃手法を考案(軍の要求により秘密)、数年後に同じ方法を独立に考案したカシスキーが公表したため、カシスキーの方法と呼ばれている
- 暗号文に使われている鍵の繰り返しを発見し、鍵を推定する
    - 自然言語の綴りには同じようなパターンが含まれる
    - 同じ語も繰り返し使われる
  - 鍵の長さの推定
  - 鍵の推定
- 鍵の繰り返し回数が少ない場合はこの攻撃手法はほぼ効かない
  - 理論的には１回を超える繰り返し(ex.暗号文101文字、鍵100文字)より多ければ有効だが、現実的には?

多表式暗号に対する攻撃手法: カシスキーの方法

手順:

- 暗号文中から反復する文字列を見つける。文字列は長いほど確からしい結果が得られる
- 反復している文字間の距離の最大公約数を求める
  - 推定される鍵の長さ。反復が少ない場合でも最大公約数の約数になるはず
  - 鍵の長さ個の問題に分解できる
    - Ex) 3文字キーのヴィジュネル暗号→3つのシーザー暗号の繰り返し
- 例
  - tobeornottobethatisthequestion（平文）
  - BOYBOYBOYBOYBOYBOYBOYBOYBOYBOY（キー）
  - UCZFCPOCRUCZF*HF*BHGT*HF*FESFGRJCL（ヴィジュネル暗号で暗号化）
  - UCZFが9文字間隔、HFが6文字→キーは3文字
  - シーザー暗号と同じ: t+B=U, e+B=F, n+B=O, … o+O=C, …, b+Y=Z, …, n+Y=L

多表式暗号に対する攻撃手法:
ケルクホフの重ね合わせ

- カシスキーの方法が知られてくる→対抗するために鍵長が長くなる

- 同じ換字表・鍵を使っている暗号文を多数集める
  - 換字状態が同じになるように複数の暗号文を重ね合わせる
  - 暗号文の同じ位置にクリブが現れる→解読の糸口
    - 該当しそうな単語を推測する等
- 多数の暗号文が必要なので平時にはあまり向かない
- 戦時には通信量が激増するのでチャンスが増える
  - 報告書や官僚的な文書における定型的な書き出し、言い回しが問題になる

多表式暗号に対する攻撃手法: フリードマンの一致反復率

- 一致指数(普通の情報学の分野)
  - 二つの文字列の一致度合い(レーベンシュタイン距離ではない)
- 古典暗号では(普通の情報学の分野とは違う意味で使っている)
  - ある文字列から二つ文字を抽出したとき、一致する割合
  - 文字列s: LGSOPXEWMSKRBXPLDAL　　sの長さ$L(s)$
  - sの異なる位置から文字を二つ取ってくる→一致する割合を計算
  - $C(s, x)$を文字列sに文字xが含まれている数とすると一致指数は

$$\frac{C(s,x)}{L(s)} \times \frac{C(s,x)-1}{L(s)-1}$$

  - xは26種類あるのでA-Z全ての総和を求めるとフリードマンの一致反復率

$$\sum_{x \in Aplhabet} \frac{C(s,x)}{L(s)} \times \frac{C(s,x)-1}{L(s)-1}$$

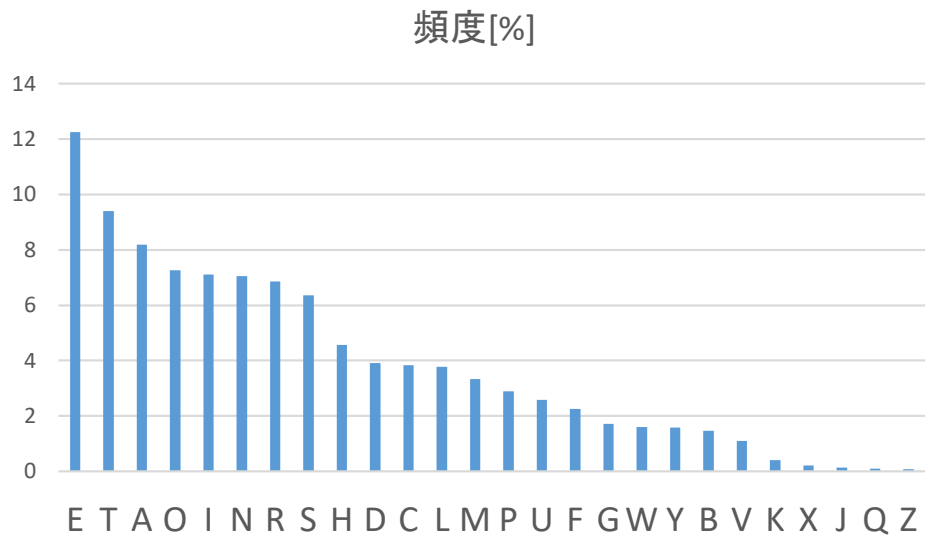
多表式暗号に対する攻撃手法: フリードマンの一致反復率

- 英語の平文に対する一致反復率: 0.0661
  - シーザー暗号や単一換字暗号のように1:1対応の暗号であれば0.0661になるはず
    - 文字の出現頻度が多い順に並べ替えてグラフを描くと平文と暗号文で同じ形になる
  - 平文と(適当な鍵を仮定したシーザー暗号の)暗号文から1文字ずつ取って一致反復率を計算
  - 鍵が正しければ0.0661に近い一致反復率になるはず
- 多表式暗号の暗号文に対しては(2文字とも暗号文からとる場合)
  - 鍵の長さ=1 → 単一換字暗号と同じ → 0.0661
  - 鍵の長さ=2 → 出てくる文字のランダム性が少し上がる → 少し小さくなる
  - 鍵の長さ=n →ランダム性が少し上がる → 一致反復率がさらに小さくなるはず
    - 鍵長11のヴィジュネル暗号で0.040前後、エニグマで0.0385前後

多表式暗号に対する攻撃手法: フリードマンの一致反復率

一致反復率と文字の出現頻度の分布の関係; この分布なら0.0661になる
出現頻度が一様分布だと1/26=0.0385になる

文字	頻度[%]	文字	頻度[%]	文字	頻度[%]
E	12.25	D	3.91	Y	1.58
T	9.41	C	3.83	B	1.47
A	8.19	L	3.77	V	1.09
O	7.26	M	3.34	K	0.41
I	7.10	P	2.89	X	0.21
N	7.06	U	2.58	J	0.14
R	6.85	F	2.26	Q	0.09
S	6.36	G	1.71	Z	0.08
H	4.57	W	1.59		



シーザー暗号・単一換字暗号ならば横軸の文字が入れ替わるだけで分布の形は同じ

多表式暗号に対する攻撃手法: フリードマンの一致反復率

- 多表式暗号を攻略するには鍵の長さ＝繰り返し周期が重要
  - 鍵がわからなくても、鍵の長さが一致すればランダム性が下がるはず
    - 多表式暗号でも個々の表は1:1変換しかしていない→個々の表で見れば暗号文も平文と同じ分布をしているはず
  - 鍵の長さがわかれば、鍵の各文字ごとに頻度分析etcをすればよい
    - 鍵の長さがLであればL個の単一換字暗号の解読問題に置き換えられる
- 鍵長の推定: フリードマンテスト(統計学のフリードマン検定とは違う)
  - 鍵長2, 3, 4, …に対して:
    鍵はよくわからないのでとりあえず適当に選ぶ
    一致反復率を計算→鍵長が一致すれば平文の場合とほぼ等しくなるはず
  - 鍵長2の場合: 1,3,5,…文字目からなる暗号文の一致反復率を計算、2,4,6,…文字目からなる暗号文の一致反復率を計算→足して2で割る

多表式暗号に対する攻撃手法: フリードマンの一致反復率

- 平文とシーザー暗号、単一換字暗号に対する一致反復率
  - FreeBSDのlsコマンドの英語マニュアルの場合の例:
    - 平文: 0.0665674851736 4018
    - シーザー暗号: 0.0665674851736 4018
    - 単一換字暗号: 0.0665674851736 4017
    - ヴィジュネル暗号(鍵長2,3,4,5,6,…,13,…,26): 0.0537, 0.0473, 0.0445, 0.0429, 0.0419,…, 0.0388, …, 0.0385
    - エニグマに対する一致反復率: 0.0385
- ヴィジュネル暗号に対する一致反復率による鍵長推定
  - 真の鍵長13文字: 鍵長を13と仮定した場合0.0665、それ以外で0.0385前後
  - 真の鍵長12文字の暗号文に対して一致反復率を計算:
    - 仮定鍵長2文字→0.0413, 3文字→0.0429, 4文字→0.0487, 5文字→0.0391,6文字→0.0515, 7文字→0.0391, 8文字→0.0487, 9文字→0.0429, 10文字→0.0412, 11文字→0.0391, **12文字→0.0667**, 13文字→0.0391
  - 真の鍵長と一致したときのほか、公約数がある場合に一致反復率が大きくなる

多表式暗号に対する攻撃手法: 鍵長推定の次の段階

- 鍵推定は以下の2段階に分けられる
- 鍵の使用パターン推定
  - 送信側と受信側で事前に鍵を共有→頻繁に鍵を更新できない
  - 鍵を複数用意して使い分ける: 曜日、日付の1の位、送信者etc.
  - 鍵の使用パターンを確定できなくても切り替えタイミングがわかればよいはず。よって、解読時にはありそうな使い分けパターンで電文を分類する
- 鍵そのものの推定
  - ケルクホフの重ね合わせ: 暗号化の状態が同じになるように暗号文を重ね合わせる
  - 平文が一致している部分は暗号文も同じになる→平文推定の手掛かり
  - 平文が一致していなくても度数分布を分析できる

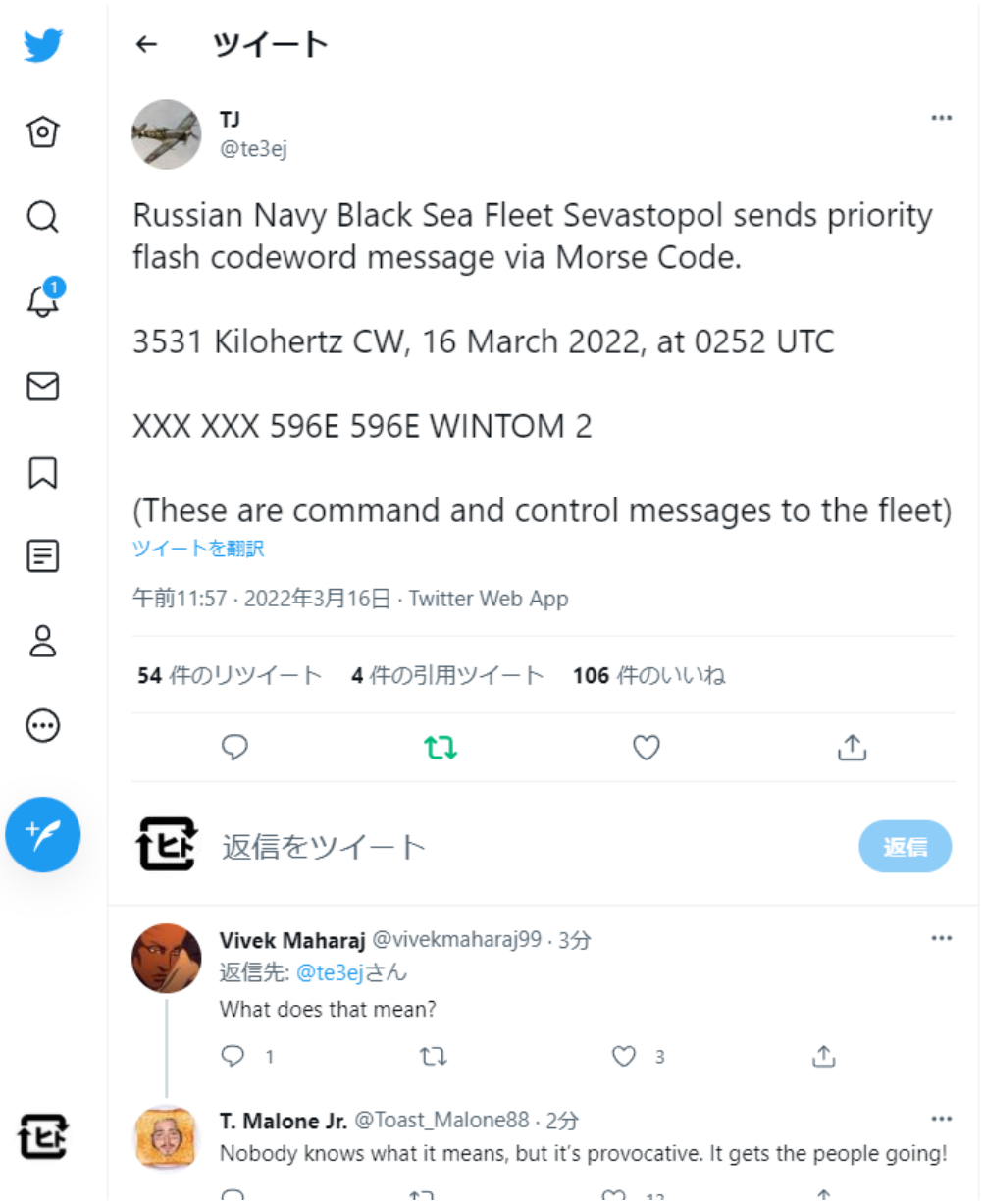
暗号文の送信: 電信の発明以降

- 電報の送信誤り・受信誤りによる乱数開始符の異常→解読の糸口の話(海軍D暗号関連)
  - 数字をモールス符号で送っていた
  - 1: .----　2: ..---　3: ...--　4: ....-　5: .....　6: -....　7: --...　8: ---..　9: ----.　0: -----
    - 聴き間違えやすい・送信時に押し間違えやすい
    - 乱数開始符: 乱数表のページ、行、列番号。乱数表自体は共有。D暗号については後述
- 電報の送信誤り対策
  - ADFGX暗号、ADFGVX暗号
    - 間違えにくいモールス符号だけをつかっていた
    - A: .-　D: -..　F: ..-.　G: --.　V: ...-　X: -..-
    - 26文字あるところを5文字～6文字にするので電文は長くなる
  - 乱数表の開始位置や暗号文ごとに異なる鍵を送受信ミスすると復号化できない
    - 対策として2回送信

暗号文の送信: 電信の発明以降

- 2022年の例
  - https://twitter.com/te3ej/status/1503928362804334592
- 和訳

  ロシアの黒海艦隊のセバストポリが優先コードワードの通信文をモールス符号で送った
  3531KHzのCW、3月16日0252UTC
  XXX XXX 596E 596E WINTOM2
  (これらは艦隊に対する指揮統制通信文)
- 解説
  - セバストポリ: 司令部の所在地(帝政ロシア時代には戦艦セバストポリがあったが)
  - 596Eが繰り返されている
    - 多分暗号書の開始位置を指示
  - WINTOM 2
    - 何らかのコード



無限乱数式暗号への展開

- 無限乱数
  - 繰り返しがない乱数: 理論上は無限に続く
  - (本当に無限に続く乱数なら)数学的にはワンタイムパッドと同じ
    - 解読不能（絶対安全）なことが数理的に証明: いくつかの条件が必要
    - Claude Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, Vol. 28, No. 4, pp. 656-715. (1949)
  - ワンタイムパッドの絶対安全を実現するために
    - 平文と同じ長さの鍵を用意する → 平文より短い鍵は鍵の再使用と等価
    - 鍵は乱数で生成する。周期性があってはいけない
    - 鍵は再使用しない。再使用すると解読され得る
- 乱数を繰り返し使用すると解読される(=無限乱数なら安全)ということには陸海軍は気づいていた
  - 繰り返しがないと解読できないことには各国の暗号関係者も気づいていた

無限乱数式暗号への展開

- 有限乱数
  - 戦前: 1万語を超えない乱数表
  - 戦後: 真の意味で無限に続く乱数表以外
- 無限乱数
  - 戦前: 1万語を超える乱数表。長さは有限
  - 戦後: 繰り返しが一切ない、真の意味で無限に続く乱数表
- 特別乱数
  - 陸軍の用語: 繰り返しが一切ない、完全に使い捨ての無限に続く乱数表
- 用語の意味に揺れがあるので、戦後に軍関係者が「無限乱数」と発言・書いている場合は注意が必要
  - 戦時中に「無限乱数なら解読できない」などと発言しているのは「十分に長い乱数表なら」と理解すべき（特に海軍関係者）?
  - どうやら海軍は乱数表の繰り返し使用については意識が低かったらしい

無限乱数式暗号への展開

- 乱数表更新の限界
  - 乱数表は物理的に運ぶ以外なかった
    - 乱数表を乱数表で暗号化して電報で送信?→乱数表を繰り返し使わないためには意味がない。安全にするにはワンタイムパッドと同じにしなければならない
  - 海軍の場合インド洋東部～西太平洋全域に艦船と拠点が散らばっていた
    - 制海権を持っていても乱数表の更新には1か月以上の準備期間が必要
    - 制海権がなくなれば乱数表更新どころではなく、燃料、弾薬、食料の補給が問題になった
  - 海軍特有の問題:
    - 船舶なので自由に動き回れる
    - 一部の艦艇を別の部隊の指揮下に入れたりもする
    - 方面や部隊ごとに違う乱数表を使用するわけにもいかなかった
- 乱数の繰り返し使用回数
  - 海軍D暗号乱数表は昭和17年5月に更新されるまで最大で83回ほど繰り返し使用された

海軍D暗号書

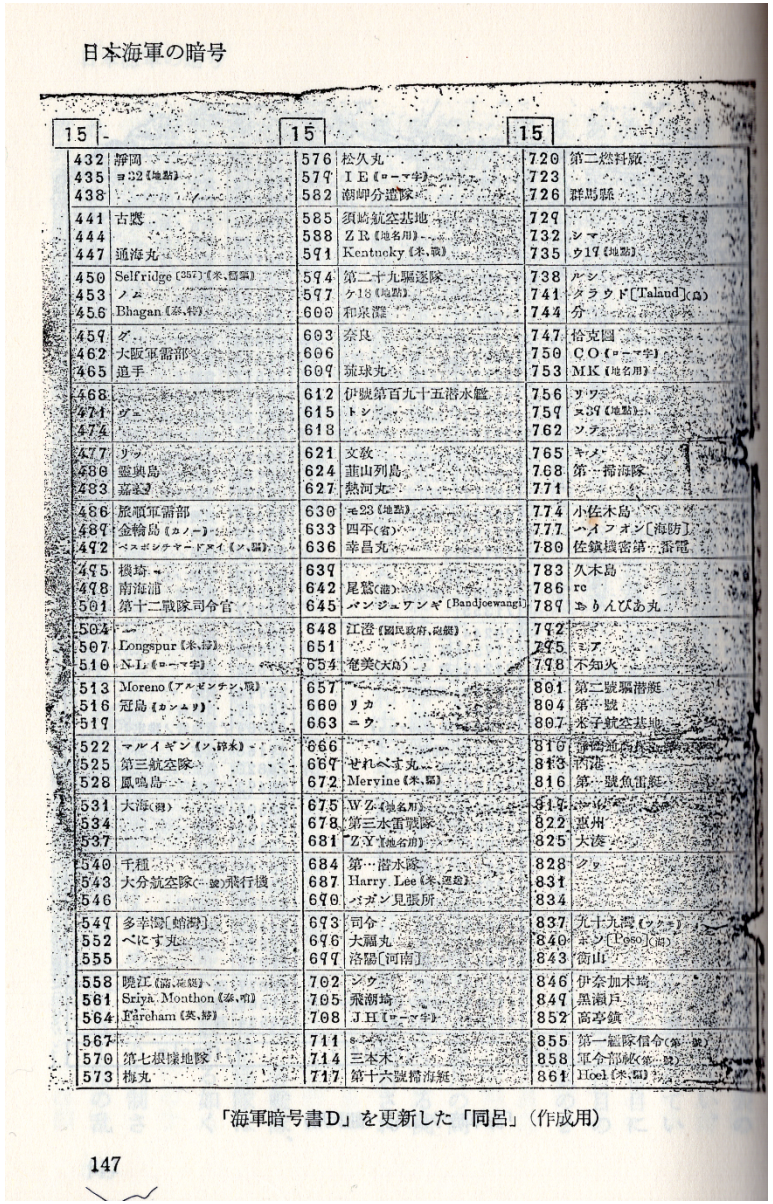
- 戦略常務用暗号: ほとんどの重要な通信がD暗号で行われた
- コード表と乱数表からなる
  - 昭和15年12月から17年5月まで使用された
- 乱数表の構成
  - 5桁数字、重複なし: 電文の送信数が計10万語未満ならワンタイムパッドと数学的には同じ
    - 平時では十分だったが真珠湾攻撃以降では電文の送信数が激増して圧倒的に不足
  - 00000, 11111, 22222, …, 99999は除外されていた
  - 1ページ当たり10行10列の5桁乱数が並ぶ。計100ページ
- 乱数表の使用開始位置(ページ番号、行番号、列番号)は部隊ごとに指定されていた
  - 開始位置が均等に分散するようにしていた模様。が、部隊や司令部のレベルによって送信する文字数が違うので割と無駄な努力に近かった
- 巧妙だったが安全と信じられていた→ミッドウェー海戦の前に解読されていたと言われている

海軍D暗号書

- コード表: コードは5桁数字。暗号化用と復号化用の表があった
  - コード化の対象
    - 固有名詞: 地名、人名、船舶・艦船名、航空隊や補給処の名称
    - その他の名詞・動詞・形容詞
  - 艦船の名称の秘匿について
    - 海軍の艦船には名前がついている
    - 名前がわかる→攻撃力や防御力を特定できる
    - どの方面にどんな艦が何隻いるかも秘匿したい
    - 部隊の編成替えや艦単独での行動もあるので個別の艦船を区別できる必要はある

海軍D暗号書

- 原本が見つからないので宮内寒彌「追跡戦記新高山登レー二〇八」より引用



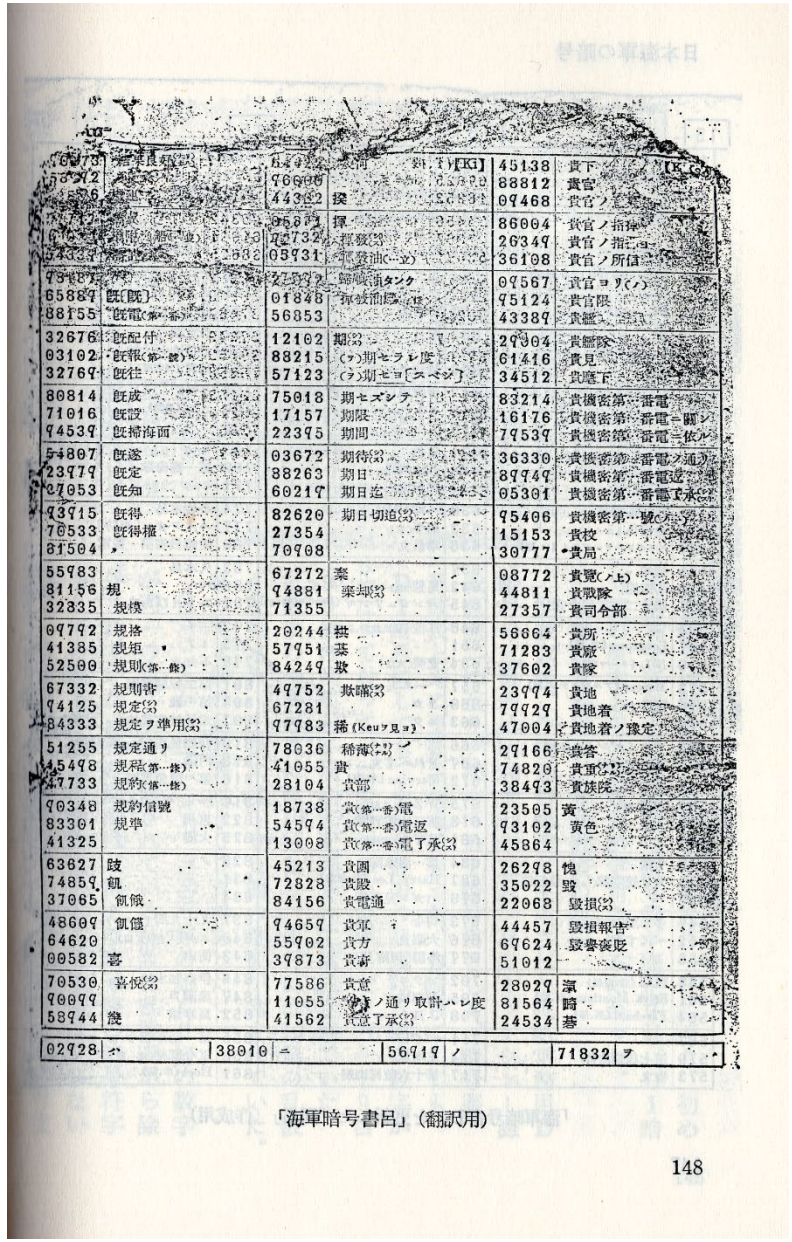
日本海軍の暗号

15 | 15 | 15

432	静岡	576	松久丸	720	第二燃料廠
435	ヨ32(地點)	577	IE(ローマ字)	723	
438		582	潮岬分遣隊	726	群馬縣
441	古鷹	585	須崎航空基地	729	
444		588	ZR(地名用)	732	シマ
447	通海丸	591	Kentucky(米、國)	735	ウ17(地點)
450	Selfridge(357)(米、驅逐)	594	第二十九驅逐隊	738	ルシ
453	ノム	597	ケ18(地點)	741	タラウド[Talaud](蘭)
456	Bhagan(器、名)	600	和泉灘	744	分
459	ゲ	603	奈良	747	拾克國
462	大阪軍需部	606		750	CO(ローマ字)
465	追手	609	琉球丸	753	MK(地名用)
468		612	伊號第百九十五潜水艦	756	ソワ
471	ヴェ	615	トシ	759	ヌ37(地點)
474		618		762	ソテ
477	ソッ	621	文敎	765	キノ
480	靈與島	624	韮山列島	768	第一掃海隊
483	嘉義	627	熱河丸	771	
486	旅順軍需部	630	モ23(地點)	774	小佐木島
489	金輪島(カノー)	633	四平(省)	777	ハイフォン[海防]
492	ベスボシケヤードアイ(ノ、蘭)	636	幸昌丸	780	佐鎮機密第…番電
495	機場	639		783	久木島
498	南海浦	642	尾鷲(港)	786	rc
501	第十二戰隊司令官	645	バンジュワンギ(Bandjoewangi)	789	おりんぴあ丸
504		648	江澄(國民政府、砲艦)	792	
507	Longspur(米、砲)	651		795	ミア
510	N-L(ローマ字)	654	奄美(大島)	798	不知火
513	Moreno(アルゼンチン、艦)	657		801	第二號驅潜艇
516	冠島(カンムリ)	660	リカ	804	第…號
519		663	ニク	807	米子航空基地
522	マルイギン(ン、詩水)	666		810	伊號第百九
525	第三航空隊	669	せれべす丸	813	酒匂
528	鳳鳴島	672	Mervine(米、驅)	816	第…號魚雷艇
531	大海(艦)	675	WZ(地名用)	819	ハル
534		678	第三水雷戰隊	822	恵州
537		681	ZX(地名用)	825	大湊
540	千種	684	第…潜水隊	828	クヲ
543	大分航空隊(…號)飛行機	687	Harry Lee(米、巡艦)	831	
546		690	バガン見張所	834	
549	多幸湖[蛸湖]	693	司令	837	九十九艦(フネ)
552	べにす丸	696	大福丸	840	ペソ[Peso](國)
555		699	洛陽[河南]	843	衛山
558	隈江(艦、驅艦)	702	ンク	846	伊奈加木場
561	Sriya Monthon(器、砲)	705	飛潮場	849	黒瀬戸
564	Fareham(英、艦)	708	JH(ローマ字)	852	高亭鎮
567		711	s	855	第一艦隊信令(第…號)
570	第七根據地隊	714	三本木	858	軍令部艦(第…號)
573	梅丸	717	第十六號掃海艇	861	Hoel(米、艦)

「海軍暗号書D」を更新した「同呂」(作成用)

147



45138	貴下				
88812	貴官				
09468	貴官ノ				
86004	貴官ノ指揮				
26349	貴官ノ指示				
36108	貴官ノ所信				
09567	貴官ヨリ(ノ)				
95124	貴官限				
43389	貴艦				
29904	貴艦隊				
61416	貴見				
34512	貴應下				
83214	貴機密第…番電				
16176	貴機密第…番電ニ關シ				
79539	貴機密第…番電ニ依ル				
36330	貴機密第…番電ノ通				
89749	貴機密第…番電返				
05301	貴機密第…番電了承				
95406	貴機密第…號ノ				
15153	貴校				
30777	貴局				
08772	貴覺(ノ上)				
44811	貴戰隊				
27357	貴司令部				
56664	貴所				
71283	貴廠				
37602	貴隊				
23994	貴地				
79929	貴地着				
47004	貴地着ノ豫定				
29166	貴答				
74820	貴重(ス)				
38493	貴族院				
23505	黄				
93102	黄色				
45864					
26298	愧				
35022	毀				
22068	毀損(ス)				
44457	毀損報告				
69624	毀譽褒貶				
51012					
28029	潰				
81564	潰				
24534	碁				

02928	か	38010	ニ	56719	ノ	71832	ヲ

「海軍暗号書呂」(翻訳用)

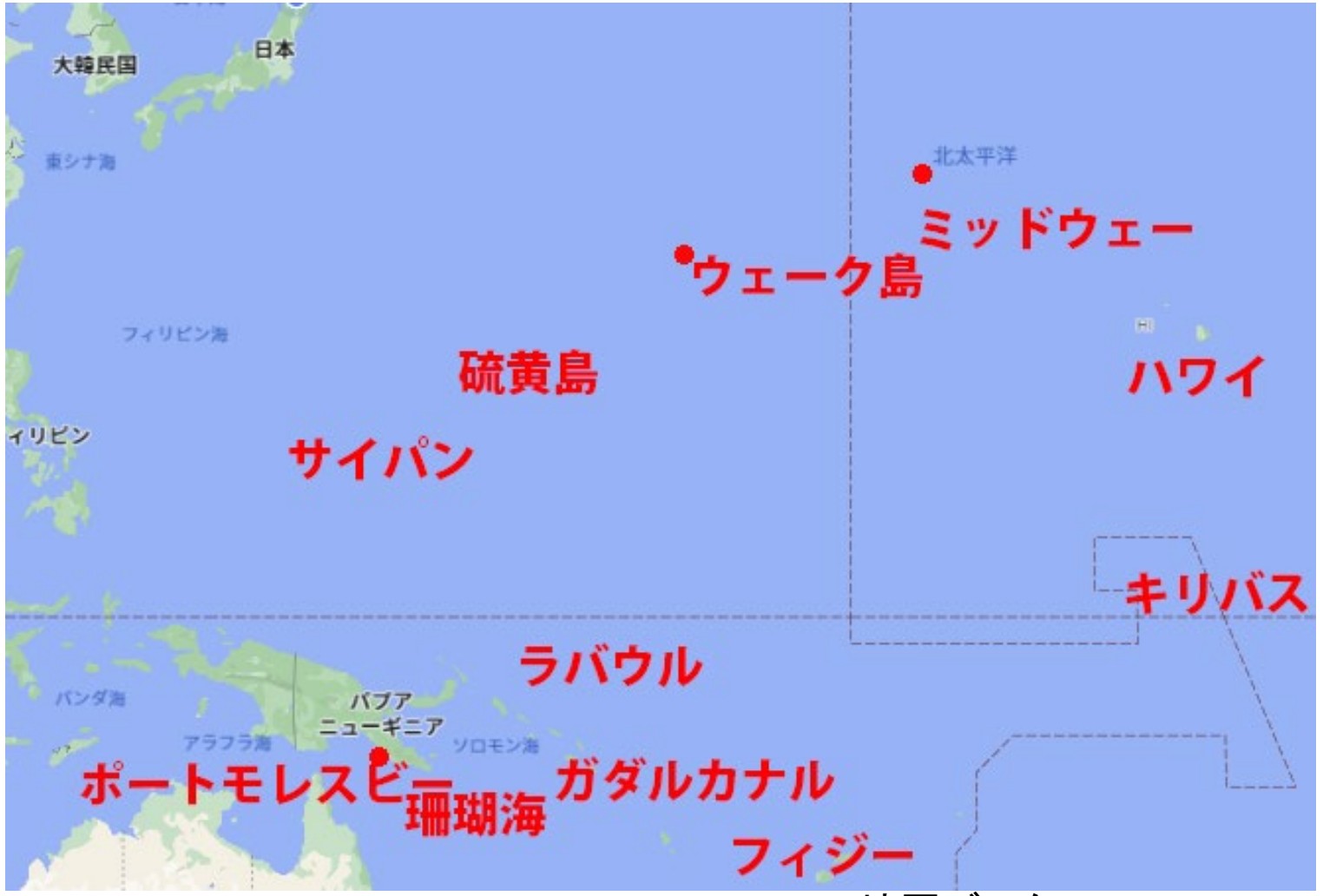
148

海軍D暗号書

- 呼び出し符号
  - 鎮守府、要港司令部、艦隊、艦船、航空基地などごとに数文字の符号があった
  - 定期的に変更した
  - 無線通信では呼び出し符号を受信して、本文を受信する必要があるかどうかを判断した
    - モールス符号なので手間・コード表etcによる復号化もしなければならなかった
    - 無関係な通信は受信したくない

ミッドウェー海戦と海軍D暗号

- 1941年12月真珠湾攻撃・マレー半島上陸
- 1942年1月ラバウル占領
  - フィリピン、マレーシア、インドネシア方面はこの時期までに占領
  - パプアニューギニアも北側は占領。山脈の南側はオーストラリア
- 1942年4月パプアニューギニアの南側に空爆・侵攻(MO作戦)
- 1942年5月珊瑚海海戦
- 1942年6月ミッドウェー海戦
- 1942年8月～1943年2月ガダルカナルの戦い
- 1945年硫黄島の戦い



地図データ: Google map

ミッドウェー海戦と海軍D暗号

- ミッドウェー島
  - 日本から見るとハワイの一歩手前
  - ミッドウェー島を落とせばハワイに重大な脅威を与えられる
- ミッドウェー海戦
  - 太平洋戦争の帰趨を分けた戦い(日本側の負け)
    - 日本側: 空母4隻沈没(真珠湾を攻撃した空母は6隻。ミッドウェー海戦に参加した空母は全滅)、艦載機290機喪失
    - アメリカ側: 空母1隻沈没(ハワイへの帰投途中)1隻残存
- 敗因
  - 日本がミッドウェー攻略をすることがバレバレだった
    - (1)ニューカレドニアやフィジー方面を占領してアメリカとオーストラリアの間の交通を遮断、(2)ハワイを攻略する、の前段階として予測可能性はあった
  - 攻撃日時・編成などが暗号解読によって知られていた(といわれている)

ミッドウェー海戦と海軍D暗号

- 米軍によるD暗号解読に関する傍証
  - シカゴトリビューンの記事: 6月7日朝刊
    - 「信頼すべき米海軍情報筋が今夜明かしたところによると、現在なおミッドウェー島西方海上で続行中の日米海戦は、今次大戦における最大の海上戦闘であるが、来航した日本の兵力内容は、戦闘が開始される数日前、米海軍によって探知されていた」
    - この記事は日本側には知られていなかった。防諜上の問題として司法省関連の事件になった
  - ニミッツ提督の発言: 著書 太平洋戦史
    - 「アメリカは日本の暗号電報を解読できたので、日本の計画に関する情報は極めて完全であった」
  - 暗号解読者に対する栄典授与
    - NSAを定年退職する際に、F.B.ロウレット氏に国家安全保障勲章を大統領が手づから授与(文官には最高位の勲章、大統領による直接の授与はかなり異例)
    - 議会が日本海軍の暗号解読の慰労金として10万ドルを与える決議をしていた(3人目)
      - 1人目は開戦前に外務省の97式暗号機を模造したフリードマン、二人目は米海軍の暗号解読組織創設者のサフォード

ミッドウェー海戦と海軍D暗号

- 暗号が解読されていたのではないかという日本側の疑問と対応
  - アメリカ側があまりにもピンポイントで日本を迎撃できたので、情報が洩れているのではないかという議論が起きた(戦後も含む)
- 議論の材料
  - 前提: 無限乱数を使用していれば理論的に解読不能
  - 日本海軍の認識ではD暗号は無限乱数を使っている(実際には有限乱数、再使用しまくり)
  - ミッドウェー占領後に派遣される予定の部隊指揮官が戦術用乙暗号でミッドウェーを宛先に指定した電報を発した
  - 「ミッドウェーでは蒸留機が故障して真水が不足」というアメリカ海軍の平文の通信を、日本海軍が「AFでは真水が不足」とD暗号で打電した
  - 地点略称「AF」は作戦関連の電報で頻用されていた→「AF」は次の作戦目標だろうということはだれが見てもわかる

ミッドウェー海戦と海軍D暗号

- 議論の材料(続き)
  - 呉・横須賀などの軍港の状況から大規模な作戦を準備しているのは明らかだった
    - 床屋も知ってたという話があったり(戦後の回想なので真偽不明)
  - ミッドウェーへの出撃後に無線封止していたが、給油艦鳴門が無線封止を破って電波を発信した
- 日本側の議論
  - 通信でAFという地名が頻出することや軍港の様子から大規模な攻勢作戦を実施する企図を察知できたはず
  - 戦略上はAFがミッドウェー、キリバス、フィジー、オーストラリア北東部のいずれか
    - 米艦隊がミッドウェーに戦力を集中できていたのはAF=ミッドウェーを特定できていた?
  - アメリカがAF=ミッドウェーに掛けたにしても作戦の細部までは察知できないはず
  - すると、D暗号を解読されていた可能性を排除できない
  - 無限乱数を使っているから通信文をいくら集めても解読できないはず(まちがい)

ミッドウェー海戦と海軍D暗号

- 議論(続き)
  - そうすると、暗号書が米軍に鹵獲されたに違いない
  - 沈没した艦艇から鹵獲された?
    - 疾風、如月など→水深が深いので可能性は低い
    - 伊124→1942年1月14日以降行方不明。1月20日に撃沈されていた(日本側には戦後判明)
      - 1月20日に伊124を追跡していたUSS Houstonがポートダーウィンに入港したのを日本側は確認している
      - 日本側: 2月3日伊124の行方を気遣う電報、2月25日伊124を予備潜水艦に編入
      - アメリカ側は潜水夫を投入して暗号書を実際に回収したとされている(潜水夫の投入自体は戦後に確認。回収された暗号書は諸説あり未確認。D暗号だったのか不明)
    - 1942年4月30日付で、どこかで撃沈されたと判断して除籍
    - 伊124の沈没地点は水深25メートル
- 結論
  - D暗号書を更新する必要がある
  - この結論に従ってD暗号書のコード表と乱数表を更新した
  - 乱数用の運用自体は全く変わらなかった(-∧-;)　ナムー

ミッドウェー海戦と海軍D暗号

- 長田順行氏による指摘

- 暗号文重ね合わせの状態の例

暗号強度別の使い分け

- D暗号の暗号化･復号化の作業にはそれぞれ30分以上かかった
  - 暗号作業という。それぞれ1時間程度必要とすることを前提にしていた模様
- 戦闘中のような急を要する場合にはこれでは間に合わない
  - 戦術レベル⇔戦略レベルで暗号強度が違った
  - 拙速を重んじる、暗号強度が低い代わりに暗号化と復号化が速くできる暗号も使用されていた
    - 乙暗号書、戊暗号書、暗号書F (航空用?)、暗号書G (Gun? 砲戦)
    - 暗号強度が低いのは認識されていた→2～3か月ごとに全面更新された
    - 電話用の暗号もあった。Cipherでは発音困難なのでコード。人名や地名を使った
      - 「愛知県11管区*山本大佐*森下特務少尉」→*10*30より敵に対し砲撃開始の予定
  - 戦闘中に使用するような暗号は、仮に敵が解読しても解読できたころには状況が変わって無価値な情報になると考えられていた

海軍乙暗号書

- 戦術用暗号: 海上部隊の戦術レベルの通信に多用された
  - 艦隊決戦の開始直前、途中で使用された
- 比較的拙速を重んじる構成
  - 味方との通信・連絡に手間取っているうちにやられてしまうよりは、暗号強度が低くても暗号化・復号化の作業が簡単で手早い方が良い

気象暗号

- 複数の乱数表があった
  - 陸海軍・気象台共用の乱数表
  - 各機関専用の乱数表
  - 他機関に観測データを送るときは共用の乱数表を利用した
- 気象暗号の強度について
  - 根本的にかなり強度が低い
  - 電文も定型: 観測データが定時送信される
    - 地点名称、風向、風速、気温、気圧、露点etc.
  - 米軍側でも気象暗号は変更されてもすぐに解読できていたという証言がある

海軍における通信と暗号の扱い

- 通信は裏方扱い、暗号は通信の中の日陰者扱い
  - 海軍大学校の卒業生の士官の専門は砲術126名、水雷114名、航海46名、通信28名(海軍大学校を卒業しないと将官になれない)
- 下士官兵の教育課程に暗号が入ったのが昭和13年
  - 実際に暗号文の作成・平文への翻訳作業をするのが下士官兵
    - それ以前は下士官兵は暗号に関する教育を受けずに暗号を扱っていた
  - 暗号文の機密レベルによっては士官が自分で作業した(真珠湾攻撃の日時を司令する電報など)
- 通信学校の電信術練習生や飛行予科練習生のうち、適性がないと判断された人が回されたという
  - 志願兵の場合: 高等小学校卒、(旧制)中学2年修了者以上。最年少で14歳、大体16歳ぐらい
  - 徴兵された場合: 20歳以上

陸軍暗号

- 1937年以前は換字式暗号を使用、その後コードブックを併用
- 中枢部の通信
  - 参謀本部-総軍-方面軍-軍-師団の縦の命令で使用。乱数式
  - 通信相手が広い範囲に散らばっている→乱数表の更新が困難→ワンタイムパットではない
- 末端の部隊の通信
  - 暗号化・複合化の手順は中枢部よりも簡単
  - コードブックで表現できる語数が少ない
  - ワンタイムパッドを指向していた
  - 末端の部隊であれば伝令が行き来できる範囲に収まっている
  - よって、乱数表や暗号書共有の問題は陸軍中枢部・海軍のようには起きない
- その他
  - 航空部隊用、気象観測用、孤立した南方の部隊用の暗号など、必要に応じて作られた

連隊以下の暗号の例

- 平文を部隊換字表と無限乱数表で暗号化
- 平文
  - 第2大隊電第1414号 大隊は白瀬環小隊の兵を収容し逃走せし敵を追撃す。敵の遺棄死体約200。
- 部隊換字表で変換: コードブックを適用
  - 252 222 389 111 444 111 444 734 210 807 230 300 600 110 584 531 040 304 155 477 487 477 588 222 000 000
  - 「てにをは」は適当に無視したり借用したりする
- 資料が残っているのは沖縄戦に参加した部隊の暗号
  - 暗号書・暗号教範(下士官兵への教育資料)などが米軍に鹵獲された
  - ワシントンの国立公文書館にある

連隊以下の暗号の例

- 乱数表から同じ長さで乱数を取り出す
  - 458 363 389 575 923 281 790 147 213 056 241 584 734 208 198 197 479 504 364 397 278 678 531 023 819 885
- 非算術加算する: ワンタイムパッドで暗号化
  - 600 585 668 686 367 392 334 871 423 853 471 884 334 318 672 628 419 808 419 764 655 045 019 245 819 885
  - 非算術加算: 陸軍用語。繰り上りを無視した加算
- 先頭に乱数表のページ番号をつけて電信で送る

部隊換字表

154 付録C コードブックの例

組立表 の…(ノ、ヲ、ニ) し…(ン、ス、ル)

000 0	599	990 ア	635 其訣ヲ認ノ	577 内(ウチ)
111 1	911 其ノ一	001 ア イ	751 (ニ)移動 し	443 馬(ウマ)
222 2	922 其ノ二	086 ア サ	276 如何(ニテル)	030 エ(エ)
333 3	933 其ノ三	008 ア ツ	745 何 時	031 エ イ
444 4	711	005 ア テ	588 遺棄死體	033 エ キ
555 5	114	285 アラズ、ザル	352 致シ度	039 エ ン
666 6	886 (續)	052 アラバ	650 (ニ)空ヲ利ル	146 (シ)得ズ
777 7	998 (終)	007 (ニ)アリル	692 (ニ)空利ラレバ	495 衛生隊の
888 8	327 地名符	856 アリ度	974 一小隊	411 延期 し
999 9	488 附錄符	658 (ニ)アリヤ	858 一分隊	354 掩護 し
070 0. (〇)	449	968 アルガ如シ	185 一同志氣旺盛(ナリ)	626 演 習
171 1. (一)	567 年	009 ア ン	775 一個(ニノ)	040 オ(ヲ)
272 2. (二)	678 月	548 相成度	194 一般(ニ)	042 オ ウ
373 3. (三)	789 日	418 暗 號	967 一部 の	048 オ ツ
474 4. (四)	890 時	010 イ(井)	388 一部ヲ以テ	899 (ニ)於テ
575 5. (五)	901 分	041 イ チ	473 一等兵	085 概 ネ
676 6. (六)	776	019 イ ン	461 未 ダ	603 行ハ(レル)
707 7. (七)	788	274 以 上	020 ウ	355 及
878 8. (八)	880 萬	936 以 下	029 ウ ン	100 カ
979 9. (九)	770 千	633 以下〇名	727 右方面 の	101 カ イ
055 、句切點	660 百	038 以來	988 右翼 の	104 カ ク
066 ー長 音	456	771 依 然	337 有 無	432 カ タ
077 」段 落	654 電第〇號	971 依頼 し	994 (ヲ)空ケル	108 カ ツ
088 ( )括 弧	765 第〇號	148 (ニ)位置 し	081 (ノ)上 の	109 カ ン
099 」括 弧	876 號 外	165 其歌ナシ	892 承リ度	983 下士官

図 16.1 組立部 (1/8)

C.2. 部隊換字表 2 号 155

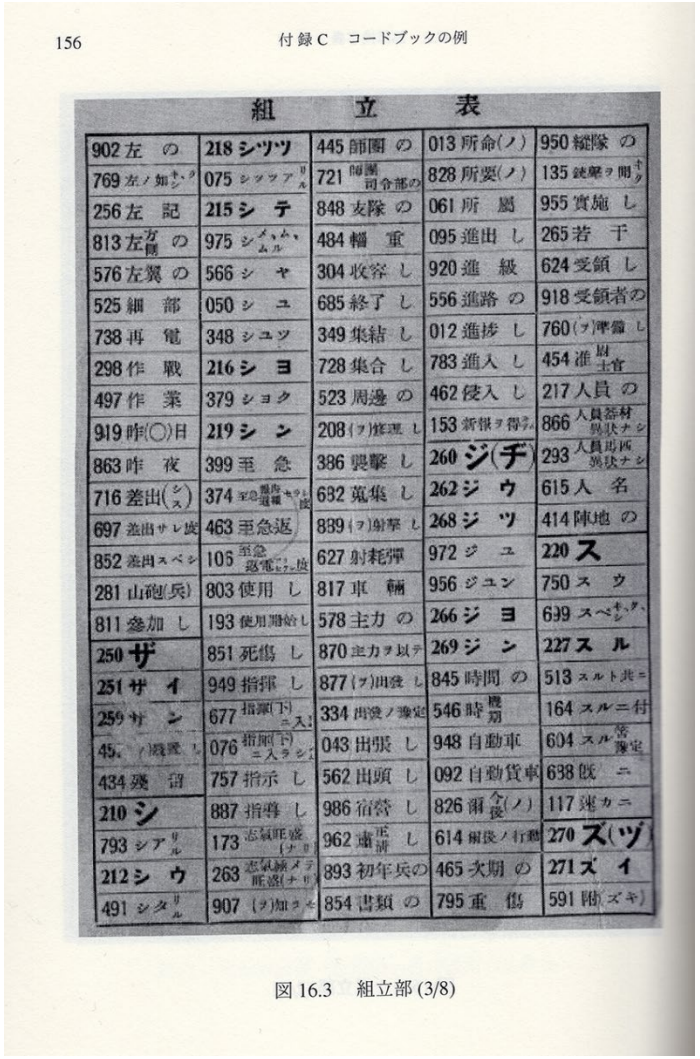
組 立 表

118 (ヲ)開始 し	119 キ ン	179 グ ン	189 ゲ ン	581 (ト)交代 し	
078 開設 し	849 機關銃	884 軍 曹	468 (ヲ)撃退 し	062 交 通	
016 潰走 し	469 貴 所	130 ケ	926 (ヲ)撃滅 し	611 (ト)交信 し	
881 各部隊の	927 貴 地	131 ケ イ	923 現 在	829 高地 の	
478 確實(ナリ)	455 貴(部)隊 の	132 ケ ウ	188 現在地	725 高地(ヲ)占領 し	
896 (ヲ)確保 し	537 希望 し	138 ケ ツ	433 現在地(ヲ)出發 し	802 工兵隊 の	
003 河(川)	234 歸還 し	139 ケ ン	661 原態勢ニ復舊 し	023 (ヲ)乞(ヒヲ)	
898 (ニ)關シテハ	498 歸隊 し	181 航空機關銃	258 原駐地の	534 谷 地	
991 (ニ)關シテハ	681 騎兵 の	264 輕 傷	140 コ	671 此 ノ	
691 關 係	357 (ヲ)企圖 し	071 携行 し	142 コ ウ	441 之 の	
724 完了成 し	288 器材 の	818 携帯 し	144 コ ク	683 (ノ)頃	
326 患 者	017 急襲 し	846 警戒 し	154 コ ト	934 困難(ニナル)	
199 監視 し	787 給養 し	385 警備 し	957 故 障	451 今 次	
316 感 度	652 率(ラル、リ、レ)	046 警備隊	655 (ヲ)攻撃 し	648 混 信	
647 乾電池	002 極 力	551 警備地區	226 攻撃(ヲ)準備 し	190 ゴ	
150 ガ	158 勤務 し	499 (ト)(ニ)協力し	361 攻撃前進 し	192 ゴ ウ	
151 ガ イ	335 粁	623 (ト)(ニ)協同し	296 (ヲ)攻撃中(ナリ)	687 伍 長	
159 ガ ン	161 キロサイクル(K.C.)	435 橋梁 の	779 行 軍	382 語 數	
273 該地 の	160 ギ	613 教育 し	365 行動 し	115 (ノヲ)知ラン	
364 頑強ニ抵抗し	120 ク	367 結 果	261 行動(ヲ)開始 し	200 サ	
110 キ	122 ク ウ	083 決定 し	766 行 李	201 サ イ	
112 キ ウ	129 ク ン	515 拳 銃	024 後送 し	204 サ ク	
985 キ タ	737 區 分	180 ゲ	149 後退 し	552 サ レ	
116 キ ヨ	170 グ	182 ゲ ウ	903 (ト)交戦 し	383 サレ度	
105 キヨク	172 グ ウ	183 ゲ キ	761 (ト)交戦中(ナリ)	209 サ ン	

図 16.2 組立部 (2/8)

伊藤秀美 日本陸軍暗号の敗北、付録Cより抜粋

部隊換字表

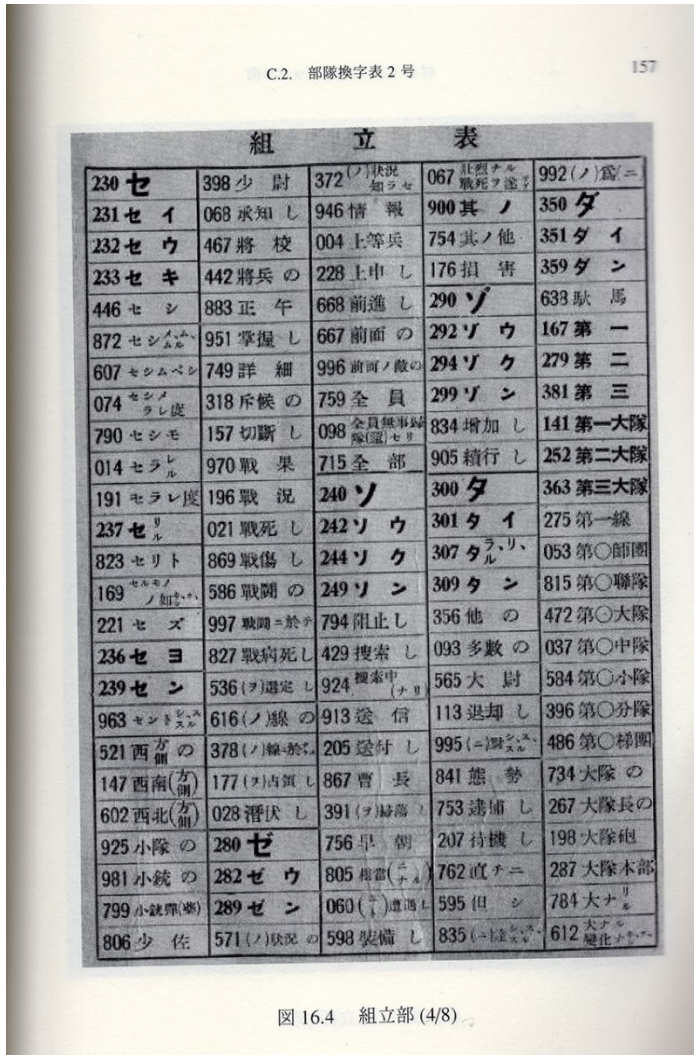


156 付録C コードブックの例

組立表

902 左 の	218 シツツ	445 師團 の	013 所命(ノ)	950 縦隊 の
769 左ノ如シ	075 シツツアリ	721 師團司令部の	828 所要(ノ)	135 銃撃ヲ開ケ
256 左 記	215 シ テ	848 支隊 の	061 所 属	955 實施 し
813 左方面 の	975 シメムル、ムル	484 幅 重	095 進出 し	265 若 干
576 左翼 の	566 シ ヤ	304 收容 し	920 進 級	624 受領 し
525 細 部	050 シ ユ	685 終了 し	556 進路 の	918 受領者の
738 再 電	348 シユツ	349 集結 し	012 進捗 し	760(ヲ)準備 し
298 作 戦	216 シ ヨ	728 集合 し	783 進入 し	454 准尉士官
497 作 業	379 ショク	523 周邊 の	462 侵入 し	217 人員 の
919 昨(〇)日	219 シ ン	208(ヲ)修理 し	153 新報ヲ得テ	866 人員器材異狀ナシ
863 昨 夜	399 至 急	386 襲撃 し	260 ジ(ヂ)	293 人員馬匹異狀ナシ
716 差出(シ)(スノ)	374 至急暗号電報セヨ(シ)度	632 蒐集 し	262 ジ ウ	615 人 名
697 差出サレ度	463 至急返	839(ヲ)射撃 し	268 ジ ツ	414 陣地 の
852 差出スベシ	105 至急発電セヨ(シ)度	627 射耗弾	972 ジ ユ	220 ス
281 山砲(兵)	803 使用 し	817 車 輛	956 ジユン	750 ス ウ
811 參加 し	193 使用開始し	578 主力 の	266 ジ ヨ	699 スベキ、シ
250 ザ	851 死傷 し	870 主力ヲ以テ	269 ジ ン	227 ス ル
251 サ イ	949 指揮 し	877(ヲ)出發 し	845 時間 の	513 スルト共ニ
259 サ ン	677 指揮(下)ニ入ル	334 出發ノ豫定	546 時期	164 スルニ付
45. (ノ)殘置 し	076 指揮(下)ニ入ラシム	043 出張 し	948 自動車	604 スル筈豫定
434 殘 留	757 指示 し	562 出頭 し	092 自動貨車	638 既 ニ
210 シ	887 指導 し	986 宿營 し	826 爾後(ノ)	117 連カニ
793 シアリル	173 志氣旺盛(ナリ)	962 準正常 し	614 爾後ノ行動	270 ズ(ヅ)
212 シ ウ	263 志氣統メテ旺盛(ナリ)	893 初年兵の	465 次期 の	271 ズ イ
491 シタリル	907 (ヲ)知ラセ	854 書類 の	795 重 傷	591 (ズキ)

図 16.3 組立部 (3/8)



C.2. 部隊換字表 2 号 157

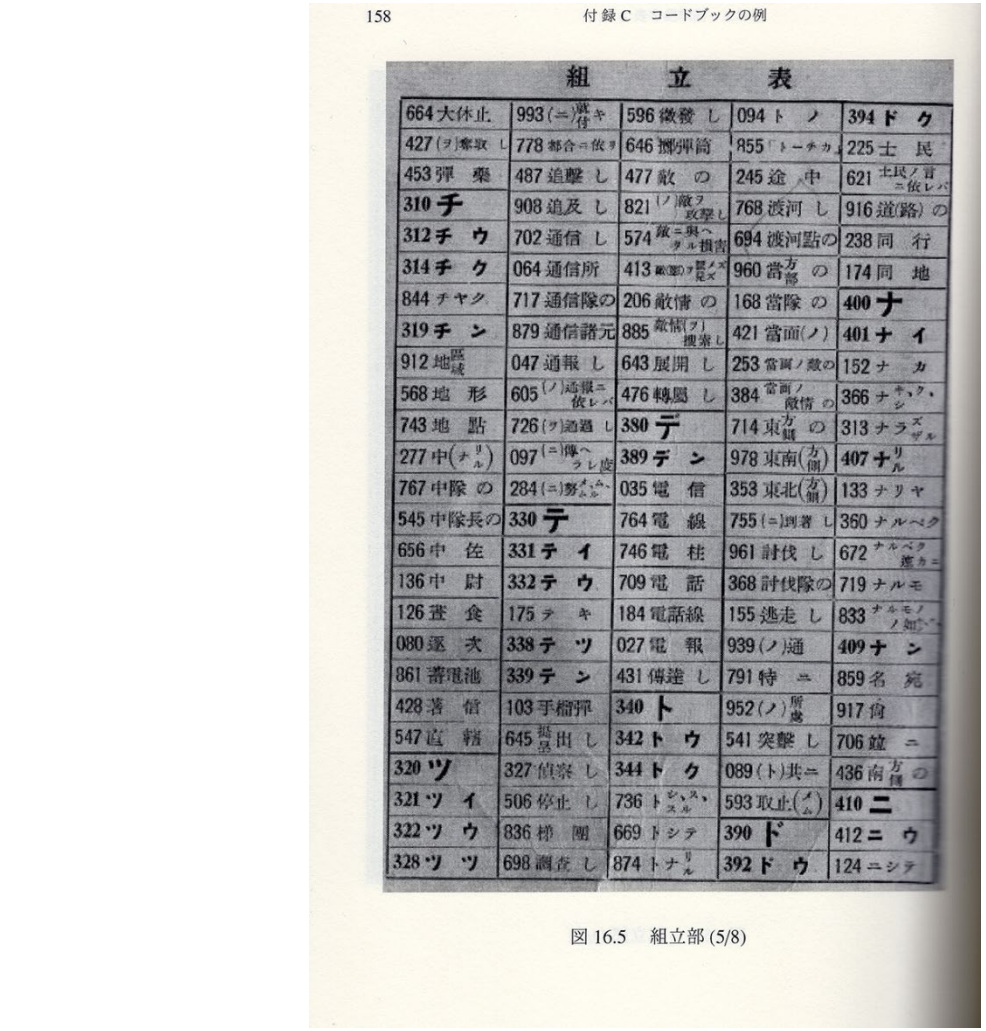
組立表

230 セ	398 少 尉	372(ノ)狀況知ラセ	067 壯烈ナル戰死ヲ遂ゲ	992(ノ)爲ニ
231 セ イ	068 承知 し	946 情 報	900 其 ノ	350 ダ
232 セ ウ	467 將 校	004 上等兵	754 其ノ他	351 ダ イ
233 セ キ	442 將兵 の	228 上申 し	176 損 害	359 ダ ン
446 セ シ	883 正 午	668 前進 し	290 ゾ	633 馱 馬
872 セシメムル	951 掌握 し	667 前面 の	292 ゾ ウ	167 第 一
607 セシムベシ	749 詳 細	996 前面ノ敵の	294 ゾ ク	279 第 二
074 セシメラレ度	318 庶候 の	759 全 員	299 ゾ ン	381 第 三
790 セシモ	157 切斷 し	098 全員無事歸隊(還)セリ	834 增加 し	141 第一大隊
014 セラレル	970 戰 果	715 全 部	905 續行 し	252 第二大隊
191 セラレ度	196 戰 況	240 ソ	300 タ	363 第三大隊
237 セリル	021 戰死 し	242 ソ ウ	301 タ イ	275 第一線
823 セリト	869 戰傷 し	244 ソ ク	307 タラ、リ、ル	053 第〇師團
169 セルモノ如シ	586 戰鬪 の	249 ソ ン	309 タ ン	815 第〇聯隊
221 セ ズ	997 戰鬪ニ於テ	794 阻止 し	356 他 の	472 第〇大隊
236 セ ヨ	827 戰病死し	429 捜索 し	093 多數 の	037 第〇中隊
239 セ ン	536(ヲ)選定 し	924 捜索中(ナリ)	565 大 尉	584 第〇小隊
963 センドシスベシ	616(ノ)線 の	913 送 信	113 退却 し	396 第〇分隊
521 西方面 の	378(ノ)線ニ於テ	205 送付 し	995(ニ)對シスベシ	486 第〇梯團
147 西南(方面)	177(ヲ)占領 し	867 曹 長	841 態 勢	734 大隊 の
602 西北(方面)	028 潜伏 し	391(ヲ)隠蔽 し	753 逮捕 し	267 大隊長の
925 小隊 の	280 ゼ	756 早 朝	207 待機 し	198 大隊砲
981 小銃 の	282 ゼ ウ	805 想像(ニナル)	762 直チニ	287 大隊本部
799 小銃弾(薬)	289 ゼ ン	060(ニ)遭遇し	595 但 シ	784 大ナリル
806 少 佐	571(ノ)狀況 の	598 裝備 し	835(ニ)注シスベシ	612 大ナル變化ナキモ

図 16.4 組立部 (4/8)

伊藤秀美 日本陸軍暗号の敗北、付録Cより抜粋

部隊換字表

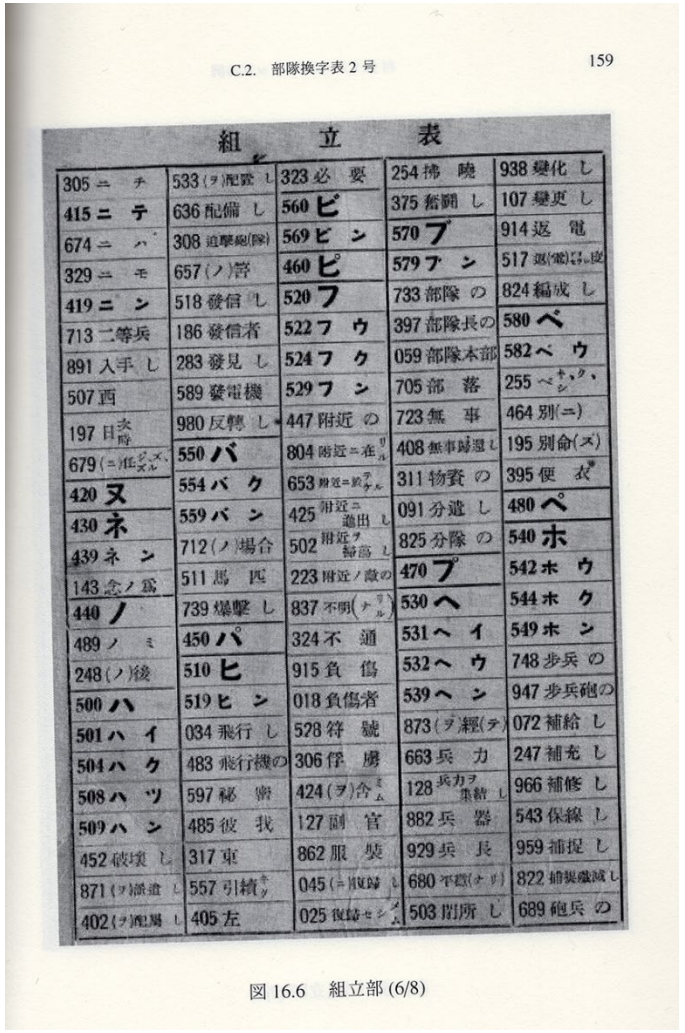


158 付録C コードブックの例

組立表

664 大休止	993 (ニ)就役キ	596 徴發し	094 トノ	394 ドク
427 (ヲ)奪取し	778 都合ニ依リ	646 擲弾筒	855 トーチカ	225 士民
453 弾薬	487 追撃し	477 敵の	245 途中	621 士民ノ言ニ依レバ
310 チ	908 追及し	821 (ノ)敵ヲ攻撃し	768 渡河し	916 道(路)の
312 チウ	702 通信し	574 敵ニ與ヘタル損害	694 渡河點の	238 同行
314 チク	064 通信所	413 敵ノ	960 當方部の	174 同地
844 チヤク	717 通信隊の	206 敵情の	168 當隊の	400 ナ
319 チン	879 通信諸元	885 敵情(ヲ)捜索し	421 當面(ノ)	401 ナイ
912 地區	047 通報し	643 展開し	253 當面ノ敵の	152 ナカ
568 地形	605 (ノ)通報ニ依レバ	476 轉換し	384 當面ノ敵情の	366 ナキ、クシ、
743 地點	726 (ヲ)通過し	380 デ	714 東方面の	313 ナラズザル
277 中(ナリ)	097 (ニ)傳ヘラレ度	389 デン	978 東南(方面)	407 ナリル
767 中隊の	284 (ニ)努メムルヨル	035 電信	353 東北(方面)	133 ナリヤ
545 中隊長の	330 テ	764 電線	755 (ニ)到著し	360 ナルベク
656 中佐	331 テイ	746 電柱	961 討伐し	672 ナルベク速カニ
136 中尉	332 テウ	709 電話	368 討伐隊の	719 ナルモ
126 晝食	175 テキ	184 電話線	155 逃走し	833 ナルモノノ如ク
080 逐次	338 テツ	027 電報	939 (ノ)通	409 ナン
861 蓄電池	339 テン	431 傳達し	791 特ニ	859 名宛
428 著信	103 手榴弾	340 ト	952 (ノ)所處	917 向
547 直轄	645 搜索出し	342 トウ	541 突撃し	706 竝ニ
320 ツ	327 偵察し	344 トク	089 (ト)共ニ	436 南方面の
321 ツイ	506 停止し	736 トシ、スル、	593 取止(メム)	410 ニ
322 ツウ	836 梯團	669 トシテ	390 ド	412 ニウ
328 ツツ	698 調査し	874 トナリル	392 ドウ	124 ニシテ

図 16.5 組立部 (5/8)



C.2. 部隊換字表 2 号 159

組立表

305 ニチ	533 (ヲ)配置し	323 必要	254 拂暁	938 變化し
415 ニテ	636 配備し	560 ピ	375 舊聞し	107 變更し
674 ニハ	308 追撃砲(隊)	569 ピン	570 プ	914 返電
329 ニモ	657 (ノ)管	460 ピ	579 プン	517 返(電)ニ依レ度
419 ニン	518 發信し	520 フ	733 部隊の	824 編成し
713 二等兵	186 發信者	522 フウ	397 部隊長の	580 ペ
891 入手し	283 發見し	524 フク	059 部隊本部	582 ペウ
507 西	589 發電機	529 フン	705 部落	255 ベキ、クシ、
197 日次時	980 反轉し	447 附近の	723 無事	464 別(ニ)
679 (ニ)任ジ、ズル	550 バ	804 附近ニ在リル	408 無事歸還し	195 別命(ズ)
420 ヌ	554 バク	653 附近ニ於テル	311 物資の	395 便衣
430 ネ	559 バン	425 附近ニ進出し	091 分遣し	480 ペ
439 ネン	712 (ノ)場合	502 附近ヲ掃蕩し	825 分隊の	540 ホ
143 念ノ爲	511 馬匹	223 附近ノ敵の	470 プ	542 ホウ
440 ノ	739 爆撃し	837 不明(ナリル)	530 ヘ	544 ホク
489 ノミ	450 パ	324 不通	531 ヘイ	549 ホン
248 (ノ)後	510 ヒ	915 負傷	532 ヘウ	748 歩兵の
500 ハ	519 ヒン	018 負傷者	539 ヘン	947 歩兵砲の
501 ハイ	034 飛行し	528 符號	873 (ヲ)經(テ)	072 補給し
504 ハク	483 飛行機の	306 俘虜	663 兵力	247 補充し
508 ハツ	597 秘密	424 (ヲ)含ミム	128 兵力ヲ集結し	966 補修し
509 ハン	485 彼我	127 副官	882 兵器	543 保線し
452 破壊し	317 東	862 服裝	929 兵長	959 捕捉し
871 (ヲ)遺棄し	557 引續キツ	045 (ニ)歸還し	680 平穩(ナリ)	822 補給ヲ絶タレ
402 (ヲ)配屬し	405 左	025 復歸セシメム	503 閉所し	689 砲兵の

図 16.6 組立部 (6/8)

伊藤秀美 日本陸軍暗号の敗北、付録Cより抜粋

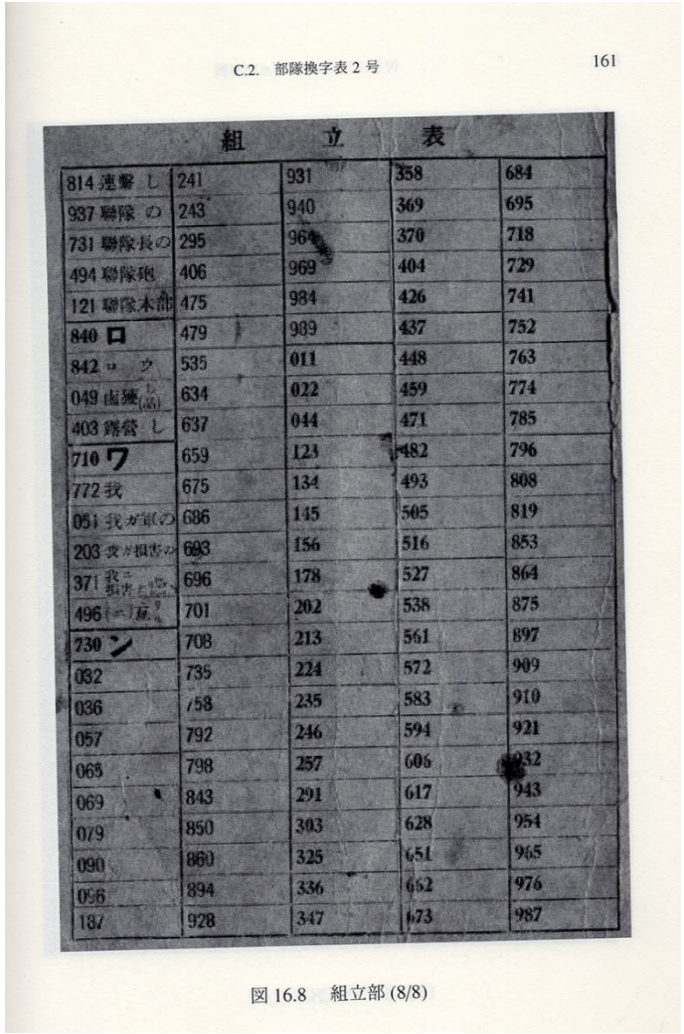
部隊換字表

160 付録C コードブックの例

組立表

166 方面の	610 ミ	935 明朝	438 稍,	800 ラ
622 方向の	618 ミツ	944 米(メートル)	720 ユ	801 ラ イ
773 報告し	619 ミン	640 モ	722 ユウ	341 ラシヤモノ
362 報告アリタシ度	564 (ヲ)見ズ	642 モウ	058 輸送し	807 ラレル
958 報告ニ依レバ	297 見習士官	644 モク	315 夕刻	393 ラレ度
214 (ノ)外	857 未詳	015 モト	026 友軍	809 ラン
082 北方面の	732 右の	422 モノ	514 (ヲ)有し	163 亂數(表)
063 本隊の	942 密偵	781 モノト	865 有線	810 リ
423 本部の	816 密偵報	629 モノノ如シ	558 有利ニ	812 リウ
466 本(○)日	670 (ヲ)認メム、ムル	649 モン	084 優勢(ナル)	786 リク
056 本文	512 南	625 (ノ)模様(ニ)	740 ヨ	278 リヨ
376 本夜	620 ム	526 目的	742 ヨウ	847 リン
590 ボ	868 ムラ	641 目下	744 ヨク	703 利用し
592 ボウ	945 無線(機)	906 (ヲ)以テ	553 ヨシ	982 榴弾
782 妨害し	102 無線分隊	481 (ニ)基キ	747 ヨリル	211 陸軍
490 ポ	977 (ニ)向ヒテ	904 (ヲ)求メム、ムル、索ムル	585 豫定(ナリ)	820 ル
492 ポウ	797 (ニ)向ヒ直進し	700 ヤ	346 豫定ノ如シ	830 レ
600 マ	630 メ	704 ヤク	416 豫備	831 レイ
601 マイ	631 メイ	302 ヤマ	343 (ニ)依リルレバ	832 レウ
608 マツ	632 メウ	125 野戦	780 (ヲ)要し	838 レツ
609 マン	639 メン	973 野砲(兵)	941 要員	839 レン
563 又(ハ)	006 命令	073 夜間	587 要求し	054 糧秣
690 全ク	895 命令受領者の	137 約○粁	387 要旨	417 列車
953 (ヲ)集結(ヲ)終リ	286 (ヲ)命ゼラレル	930 約○米	458 要點	345 連絡し
229 迄(ニ)	665 明(○)日	573 約○名	162 呼出符號	087 連絡者の

図 16.7 組立部 (7/8)



C.2. 部隊換字表 2 号 161

組立表

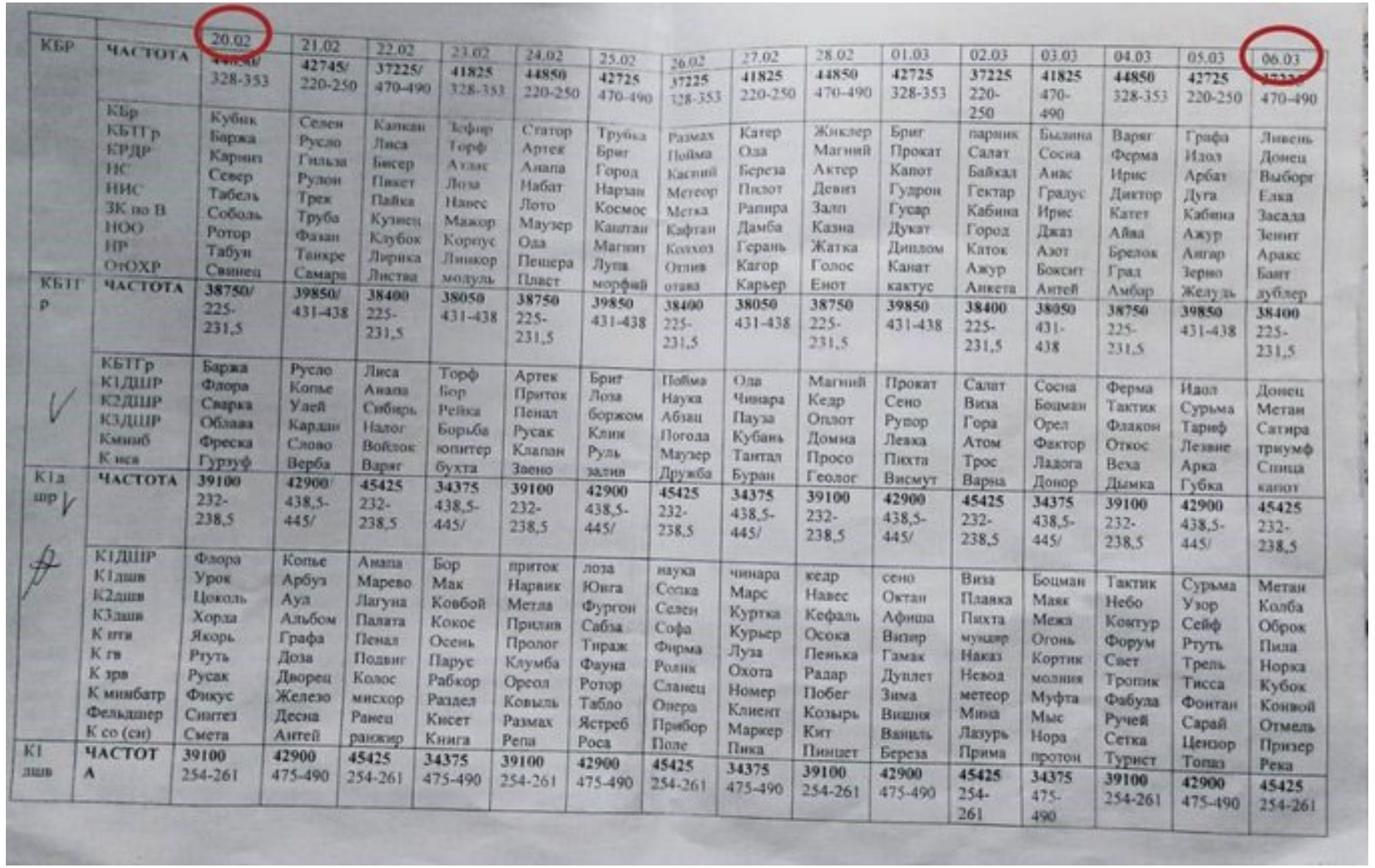
814 連繫し	241	931	358	684
937 聯隊の	243	940	369	695
731 聯隊長の	295	964	370	718
494 聯隊砲	406	969	404	729
121 聯隊本部	475	984	426	741
840 ロ	479	989	437	752
842 ロツ	535	011	448	763
049 鹵獲し(品)	634	022	459	774
403 露營し	637	044	471	785
710 ワ	659	123	482	796
772 我	675	134	493	808
051 我ガ軍の	686	145	505	819
203 我ガ損害の	693	156	516	853
371 我ニ損害ヲ與フ	696	178	527	864
496 (ニ)反シ	701	202	538	875
730 ン	708	213	561	897
032	735	224	572	909
036	758	235	583	910
057	792	246	594	921
065	798	257	606	932
069	843	291	617	943
079	850	303	628	954
090	860	325	651	965
096	894	336	662	976
187	928	347	673	987

図 16.8 組立部 (8/8)

伊藤秀美 日本陸軍暗号の敗北、付録Cより抜粋

呼び出し符号表の例

- 在東京ウクライナ大使館が2022年3月3日に公開したロシア軍のものとされる呼び出し符号表
  - 黒海で艦船から鹵獲したらしい
- 日替わり: 2月20日～3月6日
  - 周波数
  - 中隊ごとの呼び出しコードネーム
- いくらなんでも雑すぎ
  - アナログ無線なのか?
  - 周波数の下の数字はチャネル番号? それならデジタル?
  - ベトナム戦争のころのアメリカ軍の方がまだ精緻なことしてた気がする…



КБР	ЧАСТОТА	20.02 [illegible] 328-353	21.02 42745/ 220-250	22.02 37225/ 470-490	23.02 41825 328-353	24.02 44850 220-250	25.02 42725 470-490	26.02 37225 328-353	27.02 41825 220-250	28.02 44850 470-490	01.03 42725 328-353	02.03 37225 220-250	03.03 41825 470-490	04.03 44850 328-353	05.03 42725 220-250	06.03 [illegible] 470-490
	КБр КБТГр КРДР НС НИС ЗК по В НОО НР ОтОХР	Кубик Баржа Карниз Север Табель Соболь Ротор Табун Свинец	Селен Русло Гильза Рулон Трек Труба Фазан Танкре Самара	Капкан Лиса Бисер Пакет Пайка Кузнец Клубок Лирика Листва	Эфир Торф Атлас Лоза Нанес Мажор Корпус Линкор модуль	Стратор Артек Анапа Набат Лото Маузер Ода Пещера Пласт	Трубка Бриг Город Нарзан Космос Кантан Магнит Лупа морфий	Размах Поймa Касний Метеор Метка Кафтан Колхоз Отлив отвод	Катер Ода Береза Пилот Рапира Дамба Герань Кагор Карьер	Жиклер Магний Актер Девиз Залп Казна Жатка Голос Енот	Бриг Прокат Капот Гудрон Гусар Дукат Диплом Канат кактус	парник Салат Байкал Гектар Кабина Город Каток Ажур Анкета	Былина Сосна Анис Градус Ирис Джаз Азот Боксит Антей	Варяг Ферма Ирис Диктор Катет Айва Брелок Град Амбар	Графа Идол Арбат Дуга Кабина Ажур Ангар Зерно Желудь	Ливень Донец Выборг Елка Засада Зенит Аракс Бант дублер
КБТГр	ЧАСТОТА	38750/ 225-231,5	39850/ 431-438	38400 225-231,5	38050 431-438	38750 225-231,5	39850 431-438	38400 225-231,5	38050 431-438	38750 225-231,5	39850 431-438	38400 225-231,5	38050 431-438	38750 225-231,5	39850 431-438	38400 225-231,5
	КБТГр К1ДШР К2ДШР К3ДШР Кминиб К инса	Баржа Флора Сварка Облава Фреска Гурзуф	Русло Копье Улей Карданн Слово Верба	Лиса Анапа Сибирь Налог Войлок Варяг	Торф Бор Рейка Борьба юпитер бухта	Артек Приток Пенал Русак Клапан Звено	Бриг Лоза боржом Клин Руль залив	Поймa Наука Абзац Погода Маузер Дружба	Ода Чинара Пауза Кубань Тантал Буран	Магний Кедр Оплот Домна Просо Геолог	Прокат Сено Рупор Левка Пихта Висмут	Салат Виза Гора Атом Трос Варна	Сосна Боцман Орел Фактор Ладога Донор	Ферма Тактик Флакон Откос Веха Дымка	Идол Сурьма Тариф Лезвие Арка Губка	Донец Метан Сатира триумф Спица капот
К1д шр	ЧАСТОТА	39100 232-238,5	42900/ 438,5-445/	45425 232-238,5	34375 438,5-445/	39100 232-238,5	42900 438,5-445/	45425 232-238,5	34375 438,5-445/	39100 232-238,5	42900 438,5-445/	45425 232-238,5	34375 438,5-445/	39100 232-238,5	42900 438,5-445/	45425 232-238,5
	К1ДШР К1дшв К2дшв К3дшв К итн К гв К зрв К минбатр Фельдшер К со (см)	Флора Урок Цоколь Хорда Якорь Ртуть Русак Фикус Синтез Смета	Копье Арбуз Аул Альбом Графа Доза Дворец Железо Десна Антей	Анапа Марево Лагуна Палата Пенал Подвиг Колос мискор Ранец ранжир	Бор Мак Ковбой Кокос Осень Парус Рабкор Раздел Кисет Книга	приток Нарвик Метла Прилив Пролог Клумба Ореол Ковыль Размах Репа	лоза Юнга Фургон Сабля Тираж Фауна Ротор Табло Ястреб Роса	наука Сосна Селен Софа Фирма Ролик Сланец Опера Прибор Поле	чинара Марс Куртка Курьер Луза Охота Номер Клиент Маркер Пика	кедр Навес Кефаль Осока Пенька Радар Побег Козырь Кит Пинцет	сено Октан Афиша Вигвам Гамак Дуплет Зима Вишня Ваниль Береза	Виза Плавка Пихта мундир Наказ Невод метеор Мина Лазурь Прима	Боцман Маяк Межа Огонь Кортик молния Муфта Мыс Нора протон	Тактик Небо Ковтур Форум Свет Тропик Фабула Ручей Сетка Турист	Сурьма Узор Сейф Ртуть Трель Тисса Фонтан Сарай Цензор Топаз	Метан Колба Оброк Пила Норка Кубок Конвой Отмель Призер Река
К1 дшв	ЧАСТОТА	39100 254-261	42900 475-490	45425 254-261	34375 475-490	39100 254-261	42900 475-490	45425 254-261	34375 475-490	39100 254-261	42900 475-490	45425 254-261	34375 475-490	39100 254-261	42900 475-490	45425 254-261