

VIRTUAL ENIGMA USER'S MANYUAL

Ver. 1.00

1. 本ソフトの動作原理	P2.
2. 基本使用法	P6
3. 諸注意	P9

Copyright (C) 2006 Ironnitride

このたびは **Virtual ENIGMA**（以下本ソフト）をダウンロードしていただきありがとうございます。
このファイルでは、本ソフトの基本的な動作原理および歴史と使用法を解説しています。動作原理および歴史の部分はきっちりと書くと本が一冊書けるほどになるため、だいぶ端折った表現となっていることをあらかじめお断りしておきます。

1. 本ソフトの動作原理と歴史

1. 1 概要

本ソフトは第二次大戦時にドイツが使用した暗号機 **ENIGMA**（エニグマと読みます）の挙動をエミュレートしたものです。

ENIGMA は、文字を入力するキーボード、暗号化を行うプラグボード、ローター、リフレクタ、および暗号化された文字を表示するランプボードからなっていました。当時としては極めて高い暗号強度（解読されにくさ）を持っており、多用されたものです。機械内部では、電流の流れる端子を順次きり変えることにより、文字を 1 字ずつ別の文字へと変更——暗号化——を行っていました。

1. 2. **ENIGMA** の動作原理

1. 2. 1 文字の入力～プラグボード

この項以降しばらくは、アルファベットが A～F までの 6 種類しかないとして解説します。

まず、キーボードより入力された文字はプラグボードを通り、別の文字に置換されます（図 1）。ただし、これは一部の文字の組み合わせについてののみであり、置き換えが行われない文字もあります

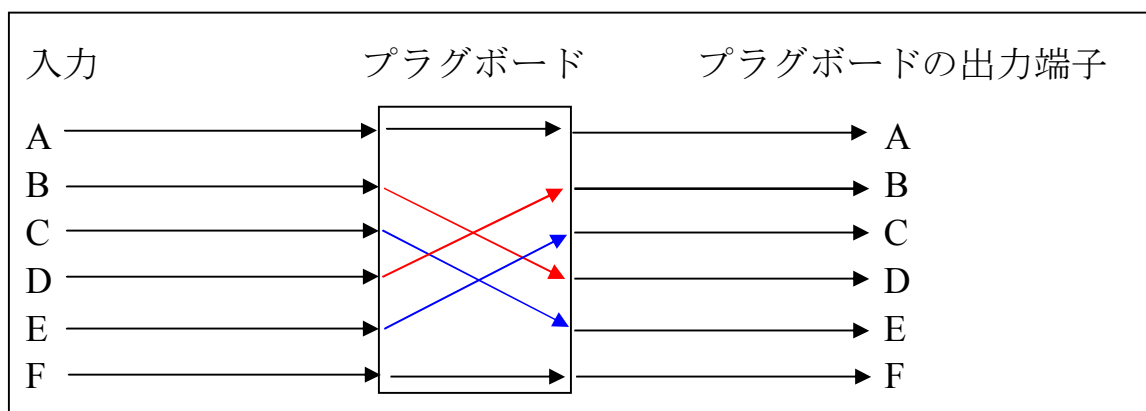


図 1 プラグボードによる変換の模式図

ご覧のように、図 1 ではプラグボードの結線により、入力 B の端子から入った電流は出力 D の端子に流れています。同様に入力 C の端子から入った電流は出力 E の端子。入力 D の端子から入った電流は出力 B の端子からといったように出力される端子が切り替わります。これが次にローターにより変化させられます。

1. 2. 2 プラグボード～ローター

ローターでは、プラグボードと違い、A が B ランダムに文字と文字を結ぶものだったからです（図 2.）。

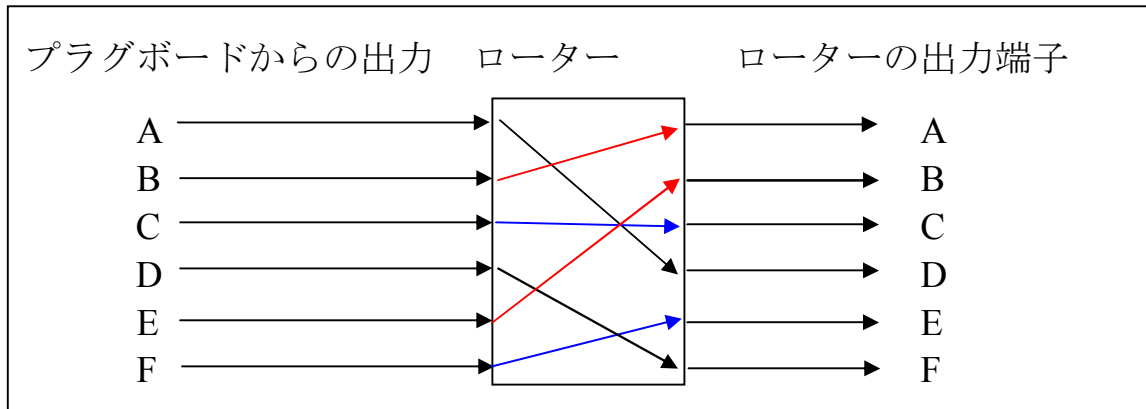


図 2. ローターによる回路の変化

ここでは、プラグボードの出力 A 端子からローターの入力 A 端子に入った電流はローターの出力 D 端子に流れています。実際には複数の結線状況の異なるローターを 3 個～4 個使用し、暗号強度を増していましたが、煩雑になりますので省略します。

1. 2. 3 ローター～リフレクタ～出力

ローターから出力されてきた電流は、リフレクタ（反射器）と呼ばれる部品により、これまでとは逆にローターの出力端子から入って入力端子から出るようになります（図 3）

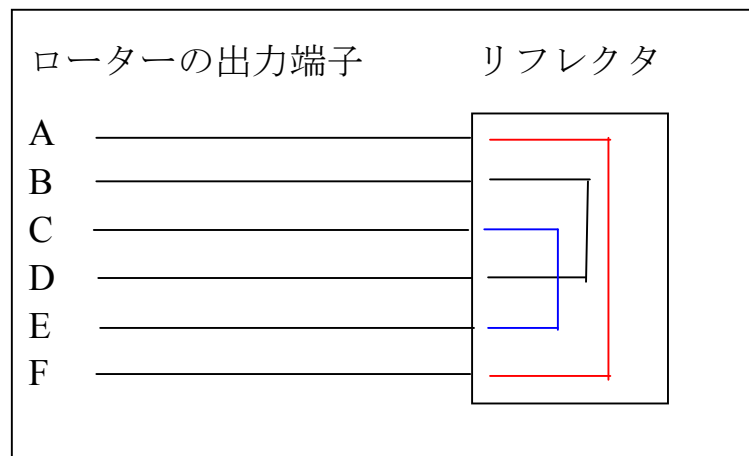


図 3 リフレクタの概念図

図 3 では電流はローターの出力 A 端子から出てリフレクタを通り、ローターの出力 F 端子に入力されます。なお、リフレクタでは、A は F に、F は A にといったようにプラグボードと同じような変換をしますが、全ての文字が変換される点が違います。そして、電流は今までとは逆の変換をたどり、ランプボードに出力されます。図 4 に A という文字を入力した場合の電流の流れと結果を示します。

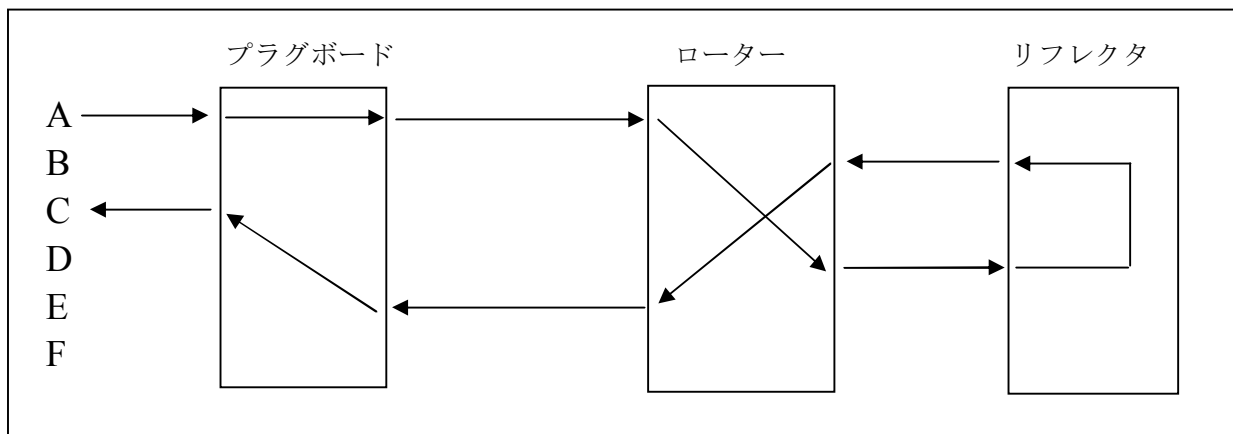


図4 入出力の一例

図4では、キーボードからAを入力するとランプボードにCが出力されます。このとき、AとCは電氣的に繋がっており、キーボードからCを入力するとAがランプボードに出力されます。これが、ENIGMAの基本的な動作原理です。

1. 3 現実の ENIGMA における工夫

まず、プラグボードはその日の指示に従い繋ぎ変えられていました。また、ローターも数種類を指示された順番通りに設置していました。さらに、ローターはキーボードを押すごとに、一番右のものが1/26回転し、一周する(Zの表示からAの表示に変わる)とその左隣のローターも同時に1/26回転するように工夫されていました。

1. 4 ENIGMA の弱点

リフレクタにおいて、文字を一対一で変換しているため、入力した文字は絶対に出力されないという弱点がありました。つまり、Aという文字は決してAとして出力されないというわけです。これにより通信文中の定型句と比較して、解読開始位置を探ることが可能だったのです。これが、エニグマの弱点です。本ソフトでは、Improve ReflectorのチェックをONにすることにより、この弱点を克服することが出来ます。

1. 5 実際の運用法

まず、何月何日の何時から何時まではこのようにセットすること、と書かれた文書(コードブック)が、各部署に配布されます。そして、通信手はそのコードブックに従い、ENIGMAをセッティングします。その内容は、といいますと、

1. プラグボードの繋ぎかた
2. 使用するローターの順番
3. 各ローターの開始位置

この3つです。さらに、実際に文章を送信する時には先頭に数文字の無意味な文字列を挿入することがルールとされていました。(このとき、面倒くさがって隣り合ったキーを押す癖のある通信手があり、そういった手抜き運用からも連合国側は解読の手がかりを得ていました)。一字ずつ暗号化、記録し、電信により、通信を行っていたのです。

受信側は受け取った文字列をコードブックに従い同じようにセッティングした ENIGMA に入力しま

す。すると、今度は元の文章（平文といいます）が現れるようになっていました。

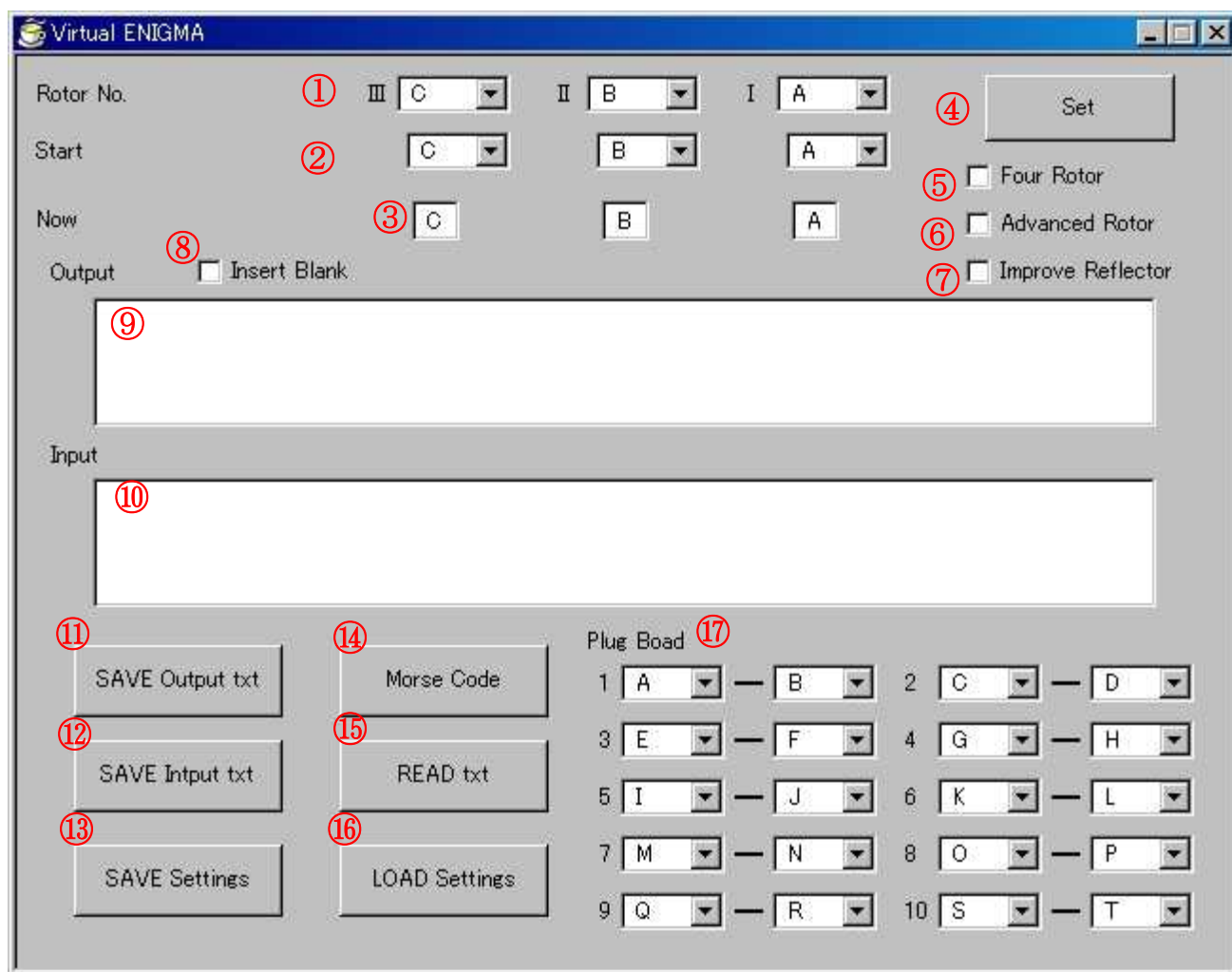
最後に、実際のエニグマにおけるキーボードの配置を図 5 に示します。現在コンピュータで使用されている配列とは少し違うことが判ると思います。

Q	W	E	R	T	Z	U	I	O
A	S	D	F	G	H	J	K	
P	Y	X	C	V	B	N	M	L

図 5 ENIGMA のキーボード配列

2. 使用方法

本ソフトを起動すると次の図 6 のようなウインドウが開きます(ご使用の Windows のバージョンにより細部が異なります)。



①	ローター指定部	②	ローター初期位置指定部
③	ローター現在位置表示部	④	設定ボタン
⑤	4 ローター使用指示	⑥	拡張ローター使用指示
⑦	改良型リフレクタ使用指示	⑧	空白挿入指示
⑨	出力文字表示ウインドウ	⑩	入力文字ウインドウ
⑪	出力文字列セーブボタン	⑫	入力文字セーブボタン
⑬	設定保存ボタン	⑭	モールス信号発信ボタン
⑮	テキストファイル読み込みボタン	⑯	設定読み込みボタン
⑰	プラグボード設定部		

図 6 本ソフトの外見

2. 1 ローター指定部

この部分では、使用するローターファイルを指示します。使用可能なローターファイルは本プログラムに内蔵の A～F までの 6 種類と同梱の **rotor maker.exe** を使用することにより **rotor** フォルダ内に作成される連番のファイルです。拡張子は通常のローターですと **.rot**、拡張型ローターですと **.eni** になります。

右から 1 番、2 番、3 番となっており、4 ローター使用指示のチェックを入れると 3 番の左側に 4 番の指定部が開きます。

2. 2. ローター初期位置指定部

ローターをスタートさせる位置を指定します。

2. 3 ローター現在位置表示部

ローターは一文字打つごとに位置が変化しますので、現在の位置を表示します。

2. 4 設定ボタン

ローターの位置や 4 ローター使用指定などの設定は指定してやるだけでは有効になりません。このボタンをクリックすることにより有効になります。同時にそれまでに入力していた文字列もリセットされます。F12 キーでも同様の効果があります。

2. 5 4 ローター使用指示

通常ではローターを 3 つ使用しますが、ここにチェックを入れることにより、ローターを 4 つ使用します。

2. 6 拡張ローター使用指示

通常使用可能なのはアルファベット 26 文字だけですが、ここにチェックを入れることにより、数字 0～9 および一部の記号（**, . @ - : ¥ ^** およびスペース）が使用可能になります。

2. 7 改良型リフレクタ使用指示

実際に使用されたエニグマは入力した文字が出力されることはありませんでしたが、ここにチェックを入れることにより、入力した文字がそのまま出力されることもあるようになります。

2. 8 空白挿入指示

表示 5 文字ごとに空白を入れ、表示を読みやすくします。実際の暗号作成には干渉しません。また、このチェックのみ設定ボタンを押さなくても動作しますが、トラブルの元になりますので注意して下さい。

2. 9 出力文字表示ウインドウ

暗号化処理が施された文字列が表示されます。平文を入力した場合は暗号文が、暗号文を入力した場合は平文が表示されます。なお、**Insert Brank** にチェックを入れていた場合は 5 文字ごとに区切られます。この場合と区別するため半角スペースは **_**（アンダーバー）で表示されます。

2. 10 入力文字表示ウインドウ

キーボードから入力した文字がそのまま出力されます。半角スペースは_（アンダーバー）で表示されます。

2. 11 出力文字列セーブボタン

このボタンをクリックすることにより、暗号化処理を行った文章を TXT ファイルとして保存できます。

2. 12 入力文字列セーブボタン

このボタンをクリックすることにより、キーボードから入力した文字列を TXT ファイルとして保存できます。

2. 13 設定保存ボタン

このボタンをクリックすることにより、その時点でのローターの番号、初期位置、プラグボードの設定などが保存されます。拡張子は .vef です。なお、終了時の設定は別に保存されます。

2. 14 モールス信号発信ボタン

このボタンをクリックすると、モールス信号を音声として出力します。音声出力中は一切の操作を受け付けませんのでご注意ください。

2. 15 テキストファイル読み込みボタン

このボタンをクリックし、開いたダイアログにより選択した TXT ファイルを読み込みます。TXT ファイルとして保存し暗号文を、自動的に復号（解読）させる時などにご使用下さい。読み込み時には全角・半角の区別はしませんが、その時点の設定で認識しない文字があるとそこで読み込みを停止します（たとえば、拡張ローター使用時はスペースを認識しますが、未使用時はそこまでで停止します。また、ひらがなカタカナ漢字があるとそこまでで停止します）。

最大認識文字数は 2048 文字です。

2. 16 設定読み込みボタン

保存しておいた本ソフトの設定を読み込みます（拡張子は .vef）。読みこむとその時点で入力していた文字列が消えますのでご注意ください。

2. 17 プラグボード設定部

プラグボードの設定を行います。1 A-B とした場合は、プラグボードにおいて A を B に、B を A に入れ替えることを意味します。振ってある番号は優先順位です。よって、1 A-B、2 A-C とした場合は、A を B にする設定が優先されますが、2 番目には適用されません。すなわち、C は C のままとなります。

2. 18 最大文字数

入力できる文字数は最大で 2048 文字です。それ以上は処理を行いません。

2. 19 キーボードショートカット一覧

F1	モールス信号発信
F5	TXT ファイル読み込み
F12	設定実行
ESC	強制終了
ALT+F4	強制終了

また F11 INS SHIFT の順に押すとローターやリフレクタの入出力状態が見られますが、F12 キーによる設定実行によってのみ元の画面に戻ることとなり、入力した文字列等は保存されませんのでご注意ください（作者用デバッグモードです）。また、このコマンドに関するご質問はご遠慮下さい。

3. 諸注意

1 本ソフトおよびこのファイルはフリーソフトとします。著作権等、本プログラムに関する一切の権利は作者である、Ironnitride が所有します。本プログラムを使用したことにより生じたいかなる障害、損害に対し（例え Virtual ENIGMA 自体のバグによるものであろうとも）、作者は一切責任を負わないものとします。各自の責任において使用してください。又、作者は Virtual ENIGMA のバグが発見された場合においても、その修正、バージョンアップの義務を負わないものとします。

2 本ソフトは作者が純粋に学術的好奇心から作成したものであり、第二次世界大戦時における政治状況について全く関係がありません（平たく言いますと、ナチスとは関係ありません）。

3 本ソフトによる暗号文の生成はすでに解読法が確立しておりますので、安全とは言えません。純粋に学問としてご使用下さい。作者は解読されたことによる不具合について一切関知いたしません。

4 他ネットへの転載や再配布に関しては以下の条件に従う限りは自由に行っていただいて結構です。なお、転載に際し連絡の必要はありません。又、転載先でのバージョンアップ等の処理は転載者の方が責任を持って行ってください。

- ・アーカイブの内容を変更しないこと(ただし、圧縮方式の変換は可)
- ・受け渡しに必要な実費以上の金品の授受を行わないこと
- ・著作権表示を変更しないこと

雑誌・書籍に紹介や収録を希望される場合には、事前に連絡をしてくださるようお願いします。