# 解説書

版:2022 年 8 月 27 日

# メタの暗号

## CipherS×KeyS×SplitS

## 目次



## 本ソフトの特徴

- メタ暗号化とは、暗号化したいファイルを、1 つでも複数でも、「複数に分割(注 1)し、複数の方式／複数の鍵(注 2)で暗号化し、複数のファイルに結合(注 3)」します。作成したファイルを分散して保存しやすくするためです。
- 独自の暗号化／復号 exe も使用可能です(注 4)。ユーザー自身での鍵生成も、当方(注 5)での生成も可能です。
- 暗号化したファイル群から、一部のファイルのみ復元できるように、パスワードで制限できます。
- パスワードには、Unicode 文字(日本の漢字・平仮名・片仮名・等)と半角文字を使用できます。お気に入りの小説の一節はいかがでしょうか。パスワードは、QR コードに変換し、紙に印刷して管理します。紙で保存すれば、第三者が電子的に読み取ることはできません。また、QR コードであれば、たくさんの文字数でも、入力ミスはほとんどなくなります。
- 分散／復元ともに、"ネット"との接続は不要です。このため、「metacipher」のサイトが閉鎖されても問題なく動きます。

メタ暗号での「分散」と「復元」について

通常の暗号関連では、平文を暗号文にすることを「encode」、暗号文を平文にすることを「decode」といいます。メタ暗号では、メタ「encode」のことを「分散」、メタ「decode」のことを「復元」とよびます。

注

1:分割した部分ごとに異なる暗号方式・異なる暗号鍵を使用します。例えば、よく使用される RSA 方式は、鍵長で強度を調整した単一の鍵を使用します。現在推奨の鍵長は「短期:3072bit 長期:15360bit(下ガイダンス参照)」で、スパコンでも解読に数十年かかるとされていますが(同参照)、量子コンピューターだと瞬時に解読できる可能性があります。しかし、例えば分割した2部分を鍵のみが異なるRSA方式で暗号化して結合した場合、分割部分を特定できない限り、解読はできません。つまり、切り分ける場所、暗号方式と鍵、全てを同時に解読しなければなりません。区切り位置特定×暗号解読の処理は、計算量が莫大になり、強度が飛躍的に増します。

「暗号鍵設定ガイダンス」:https://www.ipa.go.jp/files/000099765.pdf 44 頁図 7 参照

2:複数の暗号化方式を使用するのは、DES のように、解読方法が発見されることがあるからです。しかし、1 暗号方式を解読できても、異なる方式が混在すればより安全になります。

3:オンラインストレージを使用する場合、通常は暗号化します。ストレージの管理者は、保管しているファイルを技術的には読めるからです。しかし、ファイルを分割し、部分ごとに異なるストレージに保管すれば、暗号を破られても、ファイル全体を読むことはできません。

ファイルにまとめる場合でも、各部分をランダムに並べることで、簡単な転置暗号となります。また、分割部分が判りにくいことは、暗号方式の特定が難しくなります。第三者には、分割結果できるファイル数がわかりません。また、ダミーデータも使用します。これらを合わせると、どこまで解析すればよいか判らなくなります。「木の葉は木の葉に隠す」のイメージです。

4:RSA の様な公開鍵暗号方式は、公開する以上方法を秘匿できないため、解読に必要な演算量(鍵長)で暗号強度を調整します。使用方法にもよりますが、公開しない条件で自分専用の独自暗号化プログラムを使用することで、一般には解読できない暗号を作成することが可能です。当サイトからダウンロードできる暗号化プログラムも参考にしてください。

5:「当方」とは、「分散 exe／復元.exe」の作成者を指します。「https://metacipher」から連絡して下さい。

本書で使用している知的財産権について



本アプリケーションについて

動作確認 OS:Windows7、8、10、11(ただし、全てのバージョンを確認したわけではありません。暗号／復号 exe についてもすべてを確認したわけではありません。)

マイクロソフトの利用規約による制限ですので、日本国内で利用して下さい。マイクロソフトの利用制限の対象でなければ、日本国内に限定するものではありません。

## 1.本ソフトの動作概念

暗号化したファイルは分散(分割)して保管、復元する時は分散(分割)したファイルを組み立てなおして復元します。

復元の制御単位を Group とよび、Group 毎に暗号化対象のファイル(群)やフォルダー(群)の登録とパスワードの登録を行うことで、復元できる Group を制限できます。Group 相互の対応を指定することもできます(4 頁参照)。

### 分散 exe

1.図 1 のように各 Group に登録したファイル群を、Group 毎に A ファイルにまとめ、ランダムな長さに区切ります(B ファイル)。図 1 の Group 数は 1、4 頁図 2 は 6 です。

2.各 B ファイルを、ランダムに選択した暗号化方式(「Keys-*.txt」によります。5 頁図 5 も参照)で、暗号化した C ファイルに変換します。

3.暗号化した C ファイルをランダムかつ、任意の容量比率(5 頁図 4Ⓝで指定)になるように結合し、暗号化した D ファイル群を作成します。

4.作成した個々の D ファイルは、保管時は異なるストレージに格納します。送信時は異なる経路で送信します。

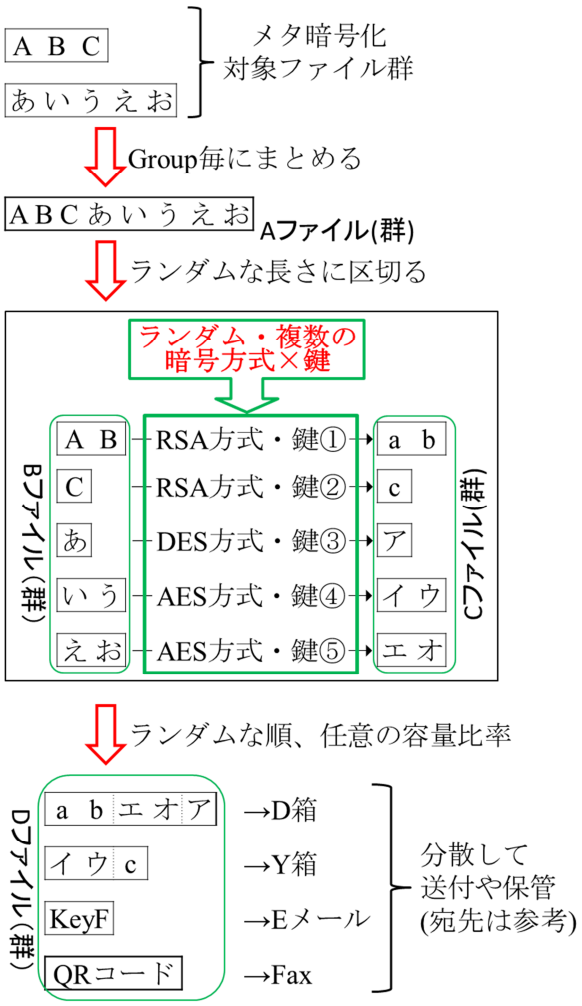


図1　分散のイメージ

作成する QR コードのファイルは、「パスワード(「Password-*1-*2.bmp」)」と「鍵(Password-Keys.bmp)」です。初期設定では、Word 文書に埋め込む形式で出力し、ファイルを消去します。

「Password-*1-*2.bmp」:*1 はパスワードの対応する Group 番号、*2 は Group 内の通し番号です。復元時(6 頁)のパスワードには、該当 Group の*1 のすべてが必要です(7 頁図 8 参照)。

「Password-Keys.bmp」:復元に使用するパスワードです。

「KeyF」:パスワードで暗号化した復元 exe(群)です。

### 復元 exe

分散の逆を行います。

1.D ファイルを分割し、E ファイル(C ファイル相当)とします。

2.E ファイルを復元し、F ファイル(B ファイル相当)とします。

3.F ファイルを結合し、G ファイル(A ファイル相当)とします。

4.G ファイルより、ファイル群を抽出します。

## 2.メタ暗号化を行う手順

1 つ以上の暗号化したいファイル群を、複数の暗号化方式、複数の鍵、複数のファイルに分割することを、「メタ暗号化」とよびます。方式、鍵、分割数は、ユーザー自身で設定できます。

### 2.1.分散方法(分散.exe)

最初に暗号化したいファイル(群)を Group 分けします。

#### 「Group とファイルの対応」タブ

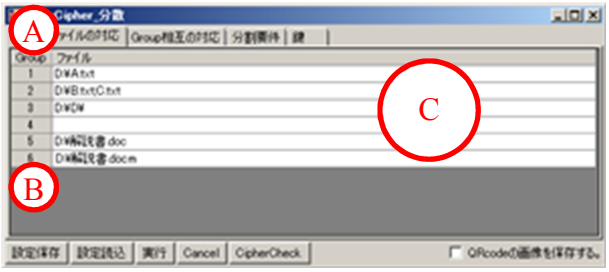

図2 「Groupとファイルの対応」タブ

Group(図 2Ⓐ)をクリックで Group の行を追加します。
「Ctrl キー」を押しながら Group の番号(Ⓑ)をクリックすることで、Group(対象行)を削除できます。

Group へのファイルとディレクトリーの登録
方法 1.Ⓒに D&D で追加。
方法 2.該当セルをクリックし、手入力する。「F2」でも、入力状態になります。

例：
Group「1」は、ファイルを指定しています。
Group「2」は、複数のファイルを指定しています。
Group「3」は、ディレクトリーを指定しています。
Group「4」は、なにも指定していません。

#### 「Group 相互の対応」タブ

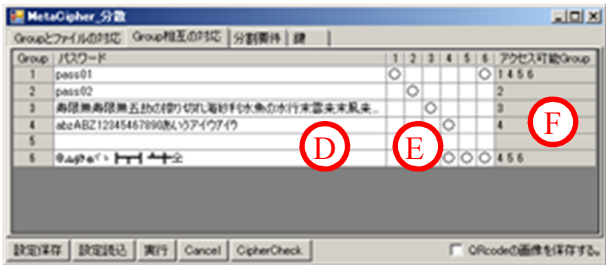

図 3 「Group 相互の対応」タブ

Ⓓはパスワードを入力します。Unicode 文字(全角の漢字・平仮名・片仮名・等)・半角を使用できます。パスワードが設定されていない Group には、直接アクセスできなくなります(下記 Group「5」参照)。他の Group から間接的にアクセスすることは、設定次第で可能です(下記 Group「1」参照)。
Ⓔで Group 間のアクセスの設定をします。該当のセルをクリックして下さい。図 3 では、Group「6」のパスワードで、Group「4・5・6」にアクセスできます。また、アクセス先がアクセスできる Group にもアクセスできます。Group「1」のパスワードで、Group「1・6」と、Group「6」のアクセス可能な Group「4・5」にアクセスできます。
Ⓕは Group 間のアクセスの状態を示します。

例：
Group「1」は、Group「6」を介して、Group「4・5・6」にアクセスする例です。
Group「3」は、全角文字の長いパスワードを使用した例です。上限は、約 1 億文字数が目安です。搭載メモリにもよります。
Group「4」は、半角文字と全角文字を併用した例です。
Group「5」は、パスワードを指定していません。このため、直接の復元はできません。

Group「6」は、Unicode 文字を使用した例です。OS によっては、文字順が異なる場合もありますが、使用可能です。
注：説明のために、Group「1・2」では、6 文字のパスワードを使用しています。128 文字以上使用して下さい。

**「分割要件」タブ**

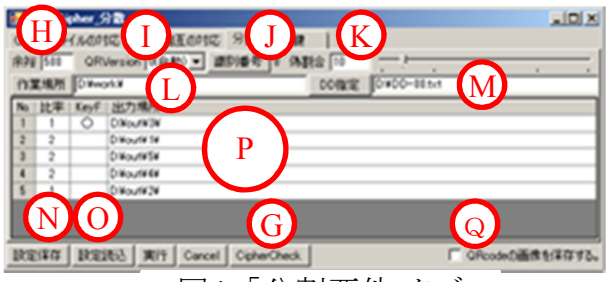

図4 「分割要件」タブ

Ⓖは、「余裕(Ⓗ)」の推奨値を提示します。処理後に表示される「CC 結果.txt」の 1 行目の「推奨値」のことです。
Ⓗは、暗号化に伴う容量変化に対処する容量の余裕を指定します。Byte 単位です。
Ⓘは、パスワードと鍵の QR コードのサイズです。
Ⓙは、暗号 exe の組み合わせの識別番号です。変更するには「Keys-*.txt」ファイル(8 頁『5.「Keys-*.txt」の書式』参照)が必要です。ユーザーによる自作や当方で作成することも可能です。クリックして変更します。
Ⓚは、D ファイル(3 頁『本ソフトの動作概念』参照)に混入する偽データの割合(%)です。100 以上は手入力します。
Ⓛは、メタ暗号化処理に使用する一時ファイルの作成場所を指定します。Ⓒで指定したファイルの合計容量の 3 倍以上の空き容量が目安です。この場所のファイルはすべて削除されます。
Ⓜは、D ファイルに混入する偽データファイル(9 頁参照)を指定します。
Ⓝは、D ファイルを複数作成する場合に、この複数の D ファイル相互の容量比率の目安です。例えば、「1:2:2:2:1」であれば、「100:200:200:200:100[KB]」や、「2:4:4:4:2[MB]」等となります。容量の合計は、分散対象のファイル容量や暗号化方式によります。保管や送信に容量制限がある場合等に使用します。「＋(プラス)」と「－(マイナス)」のキーで変更します。
Ⓞは、「鍵」ファイルを作成する場所を指定します。中身は同じものですが、複数の場所に作成することも可能です。
Ⓟは、D ファイルの出力場所です。同一場所に出力することも可能です。
Ⓠをチェックすると、パスワードと「鍵」の QR コードファイルを作業場所(図 4Ⓛ)に作成しますが、PC 内に保存してある電子データを第三者が盗み見る事件はよくありますので、削除することを強く推奨します。Word ファイルも同様です。「紙に印刷」などの保管処理後、確実に PC 上から削除して下さい。なお、ゴミ箱を空にするだけではなく、HDD 上に残されたデータも必ず削除して下さい。Windows の場合は、「cipher /w:」等で消去して下さい。

**「鍵」タブ**

暗号化方式・exe 名称・暗号化鍵・復号化鍵を確認できます。「Keys-*.txt(8 頁参照)」の記載内容です。暗号 exe(8 頁参照)と暗号鍵・復号鍵(8 頁参照)は、ユーザーによる自作や当方での作成も可能です。


図5 「鍵」タブ

**下部のボタン**

「実行」で、処理を開始します。

「設定保存」は、入力した設定を保存します。パスワードも保存しますので、第三者に読み取られない様に保存して下さい。

「設定読込」は、保存した設定を読み込みます。

## 2.2.復元方法(復元.exe)


図6　復元

Ⓐ QR コードを読み取るカメラの Fps(Frame/s)です。

Ⓑ同カメラの解像度の横の長さです。

Ⓒ同カメラの解像度の縦の長さです。

Ⓓ同カメラが対応する、Fps、Width、Height を取得します。複数ある場合は、解像度の高い組み合わせを推奨します。

Ⓔ一時ファイルの作成場所を指定します。Ⓖのファイル容量の合計の 3 倍以上を目安に、空き容量を確保して下さい。

Ⓕ復元したファイル(群)を出力する場所を指定します。

Ⓖ1 以上の D ファイルと、1 つの「KeyF」ファイルを指定します。D&D か、手打ちします。分散で作成したすべての D ファイルを揃える必要はありません。Group の復元に必要なデータが揃っていれば復元できます。

Ⓗカメラでパスワードの QR コードを読取ります。複数の場合は、全て読取って下さい。右クリックで画像ファイルを指定できます。

Ⓘパスワードを手入力できます。

Ⓙカメラで鍵の QR コードを読取ります。右クリックで画像ファイルを指定できます。

Ⓚ分散前のファイルの復元処理を行います。

## 2.3.Sample(ソフトに同梱)の説明

「分散.exe」「復元.exe」によるメタ暗号化方式の具体例を示します。当サイトよりダウンロードした「bunsan.zip」もしくは「gousei.zip」を展開すると、作成される「Sample」フォルダーの中に、「メタ暗号化前」フォルダーにメタ暗号化前のファイル群が、「メタ暗号化後」フォルダーに分散処理後にできたファイル群(メタ暗号化済み)ができます。

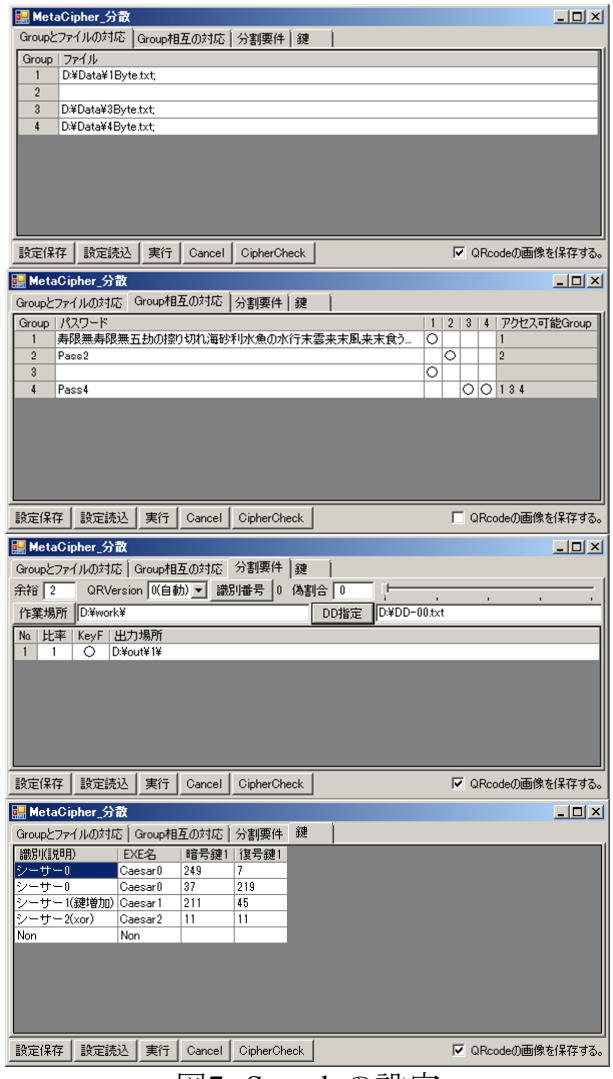


図7　Sampleの設定

**分散**

図 7 はメタ暗号化(分散.exe)の設定です。

Group1 のパスワードは、漢字を使用した例です。Group2・4 は説明のために簡単にしています。Group3 は

パスワードがないため、Group4 のパスワードを使用しないと復元できません。

Group「4」は Group「3・4」にアクセス可能です。この時、Group「4」は Group「3」を介することで、Group「1」にアクセス可能です。

「実行」ボタンから分散処理で作成したファイルは 9 個で、以下になります。

10453889387629044568.d

KeyF

Password-1-0.bmp　Password-1-1.bmp　Password-1-2.bmp

Password-2-0.bmp　Password-3-0.bmp

Password-Keys.bmp

QR.docm

注：「Sample」は、保管状態としては悪い例です。

「Password-*.bmp」と「QR.docm」はパスワードが記述してあります。実際のファイルでメタ暗号化処理後は、紙に印刷する等してから両方とも削除して下さい。第三者が電子的には入手できないようにするためです。

図8の、2頁の3つのQRコードの画像が「Password-1-0.bmp Password-1-1.bmp Password-1-2.bmp」、3頁が「Password-2-0.bmp」、4頁が「Password-3-0.bmp」、5頁が「Password-Keys.bmp」、になります。

これらの画像ファイルがあればパスワードを容易に入手できます。"ネット"に繋がる場所には保管しないで下さい。

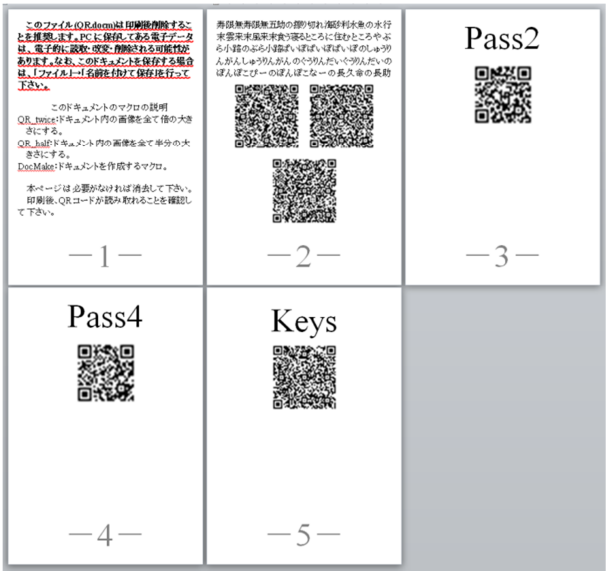


図8　出力するQR.docmの一例
注:初期状態より改変しています。

**復元**

図 9 の「①ファイルを下に D&D～」欄に 2 つのファイルを D&D します。

1.「②パスワードを下に入力～」欄にパスワードを入力します。QR コードをカメラで読み取る方法と手作業で入力する方法の 2 種があります。ここでは、手入力でパスワード「Pass4」を入力します。「③QR 読込(鍵)」をクリックして、「鍵」を読込後、「④実行」をクリックすることで、復元処理を行います。結果として、「1Byte.txt」「3Byte.txt」「4Byte.txt」を復元します(図 7『Group とファイルの対応』参照)。

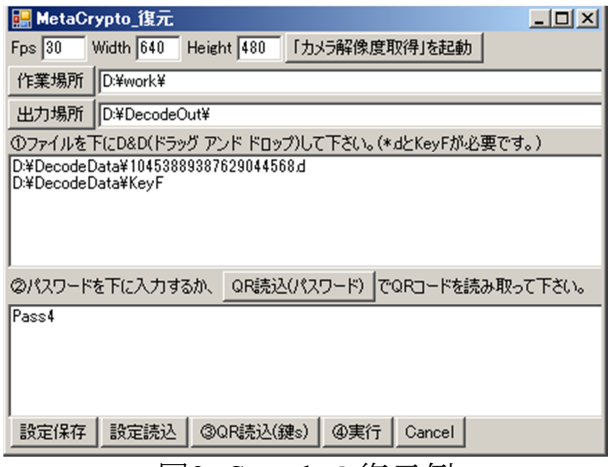


図9　Sampleの復元例

2.パスワードをカメラで読み取る例です。「QR 読込(パスワード)」をクリックして、図 8 の 2 頁の QR コードをカメラで読み取ると、パスワード欄に「寿限無寿限無～略～長久命の長助」と入力されます。③、④とクリックすることで、結果として「1Byte.txt」を復元します。

3.パスワードを「Pass2」とすると、なにも復元しません。図 7 の Group2 からアクセスできるのは Group2 のみで、Group2 にはファイルの登録がないからです。

このように、Group のアクセスを設定することで、復元するファイルを制御できます。

## 3.暗号／復号 exe の指定方法

1.暗号／復号 exe を、ダウンロード、ユーザーによる自作(『4.暗号／復号 exe の作成要件(8 頁)』参照)、などで、用意します。

2.識別番号を、当方による(正式)、もしくは、独自(18000000000000000000 以降から自由に選択)で、規定する。

3.「Keys-識別番号.txt」を作成し(『5.「Keys-*.txt」の書式(8 頁)』参照)、

4.「分散.exe」の「分割要件」タブの「識別番号」ボタンから、「Keys-識別番号.txt」を選択する。

## 4.暗号／復号 exe の作成要件

表1　引数要件

| | |
|---|---|
| argv[1] | 入力ファイル名(フルパス)　Null の時は鍵生成モード |
| argv[2] | 出力ファイル名(フルパス) |
| argv[3] | Log ファイル名(フルパス) |
| argv[4] | 0：通常モード(省略可)<br>1：簡易出力モード(関数の名称程度の目安)<br>2：詳細出力デバッグモード（デバッグできる程度） |
| argv[5]～ | 鍵(暗号鍵 or 復号鍵) |

暗号 exe は「*_E.exe」、復号 exe は「*_D.exe」とします。プログラム名(*部分)は自由ですが、他プログラムと重複がないように配慮して下さい。必要な場合は当方で変更します。両プログラムとも、Windows では、アプリから「stdio.h」の「_wsystem(引数)」でよび出します。下記「開発環境」も参考にしてください。

引数：絶対パスの bat ファイル名[ ]絶対パスの B ファイル名[ ]絶対パスの C ファイル名[ ]絶対パスの Log ファイル名[ ]モード("[ ]"は半角空白 1 文字のこと)

bat ファイルは、アプリが識別番号フォルダーを対象に、「Keys-識別番号.txt」により作成します。

書式

"*_E.exe"[ ]"%1"[ ]"%2"[ ]"%3"[ ]"%4"[ ]"暗号鍵 1"[ ]…　(例："Caesar0_E.exe" "%1" "%2" "%3" "%4" "7")

"*_D.exe"[ ]"%1"[ ]"%2"[ ]"%3"[ ]"%4"[ ]"復号鍵 1"[ ]…　(例："Caesar0_D.exe" "%1" "%2" "%3" "%4" "249")

分散プログラムは、設定の識別番号フォルダー内のすべての復号 exe を「KeyF」ファイルにまとめます。使用していないものもまとめます。復号時の依存関係にも留意して下さい。

また、復号鍵を QR コードの「鍵」とします。

参考　「暗号／復号 exe」の開発環境

Microsoft Visual Studio Community 2019 Version 16.11.11+32228.343

Microsoft .NET Framework Version 4.8.03761

Microsoft Visual C++ 2019 00435-00000-00000-AA302

Visual Basic ツール 3.11.0-4.22108.8+d9bef045c4362fbcab27ef35daec4e95c8ff47e1

## 5.「Keys-*.txt」の書式

1 行目　使用するプログラム数(行数)、複数回使用も可能です。

2 行目以降

各行はタブ区切り、ここでは列とします。下記例では、区切り文字を「(Tab)」と表記しています。
1 列目　暗号鍵の数
2 列目　復号鍵の数
3 列目　説明(簡潔に)
4 列目　プログラム名、「*_E.exe」の*部分のみ　例　Caesar0 は「Caesar0_E.exe」と「Caesar0_D.exe」とします。
5 列目以降　鍵を並べる。暗号鍵、復号鍵の順です。

例//次行以下は、以上をまとめた例です。
3
1(Tab)1(Tab)シーサー0(Tab)Caesar0(Tab)249(Tab)7
1(Tab)1(Tab)シーサー2(xor 方式)(Tab)Caesar2(Tab)11(Tab)11
1(Tab)1(Tab)シーサー0(Tab)Caesar0(Tab)64(Tab)192
//例ここまで

### 6.偽データ

ファイル名は「DD-*.txt」となります。C ファイル(3 頁参照)を組み合わせる際の隙間に、このファイルの中身をそのまま Binary データとして書き込みます。第三者の手間を増やすことが目的です。いらないデータを簡単に暗号化して使用することを推奨します。あなた専用のデータ、他と区別がつきやすいデータ、等を、ユーザーによる自作や当方での作成も可能です。

本説明中で用いる用語について

「プログラム」は、実行形式(*.exe)のファイル単体を指し、「アプリケーション」はメタ暗号化の分散／復元を行う「プログラム」群全般を指します。

「暗号 exe」は、入力したファイルを、暗号化したファイルとして出力する機能を有するプログラムとします。例：初期に添付の「Non_E.exe」は何も変換しませんが、「暗号 exe」です。

「復号 exe」は、これの逆処理の機能を有するプログラムを指します。例：初期に添付の「Non_D.exe」は何も変換しませんが、「復号 exe」です。

「分散 exe」は、「暗号 exe」群を使用し、メタ暗号化の分散処理を行います。

「合成 exe」は、「分散 exe」群を使用し、メタ暗号化の復元処理を行います。

「A ファイル」～「G ファイル」は、拡張子が A～G のファイルを指します。「D ファイル」以外は、一時ファイルで、初期設定では処理後に消去されます(3 頁参照)。

「ランダム」は、C 言語の「mt19937_64」による"疑似"ランダムを指します。