概要

このガイドでは Phobos 及び 8 base グループのランサムウェアによって暗号化されたファイルの復号を試みるための手順について説明します。

本ツールにおいて対応する暗号化されたファイルの特徴は次のとおりです。

- ファイル名のルールについて

※暗号化されたファイル名のルール（Encrypted file name rule）
{元のファイル名}.id[{8 文字のランダムな英数字}–{4 桁の数字}].[{メールアドレス}].{拡張子}

- ファイルの拡張子について
.phobos　.8base　.elbie　.faust　.LIZARD
※ 上記の拡張子以外にも複数の拡張子が確認されています。前記ファイル名のルールに該当する場合は復号することができる可能性があります。

(注意)

Phobos 及び 8base のランサムウェアによって暗号化されたファイルであっても、暗号化の際の不具合でファイルが壊れている場合があり、この場合は復号することができません。

また、復号されたファイルについて、ファイルの完全性を保証しません。

復号の手順

Step1 ダウンロード及び起動

警察庁 Web サイト（https://www.npa.go.jp）の「サイバー警察局」のページから

「個別事案への対策」→「ランサムウェア被害防止対策」→「被害回復」→「警察庁開発の復号ツールについて」→「ランサムウェア Phobos/8Base により暗号化されたファイルの復号ツールの利用について」

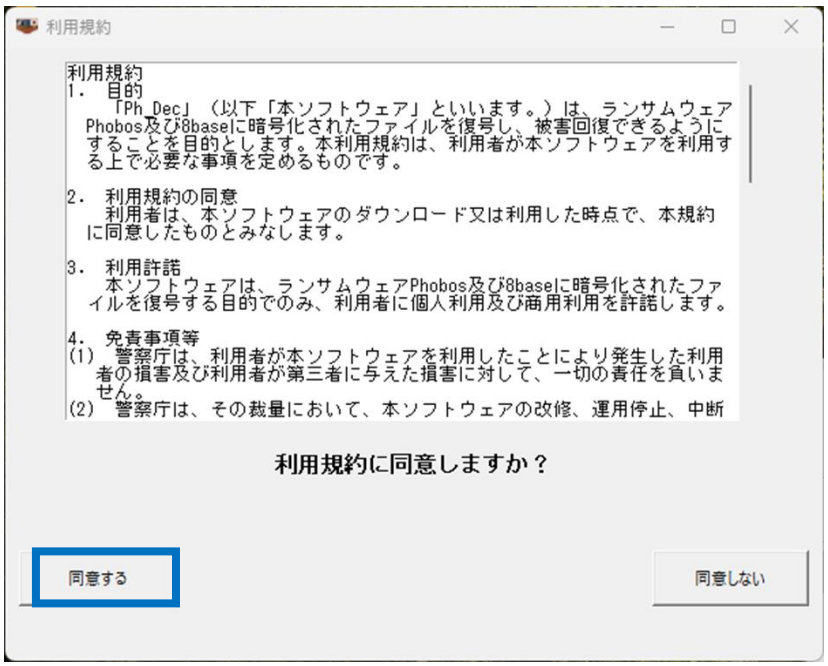
から復号ツールをダウンロードし、復号ツール”Phdec_gui_v***.exe”を起動します。

(注意)

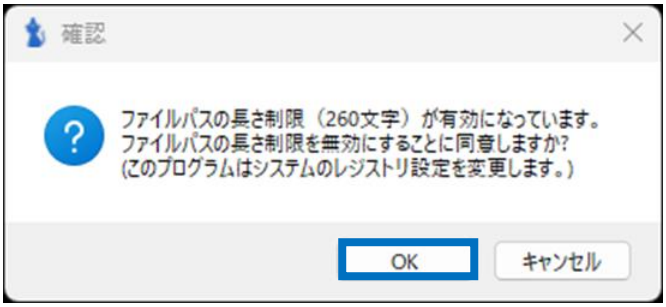
このツールはウィルス対策ソフトにマルウェアと誤検知される場合があります。

Step2 利用規約への同意

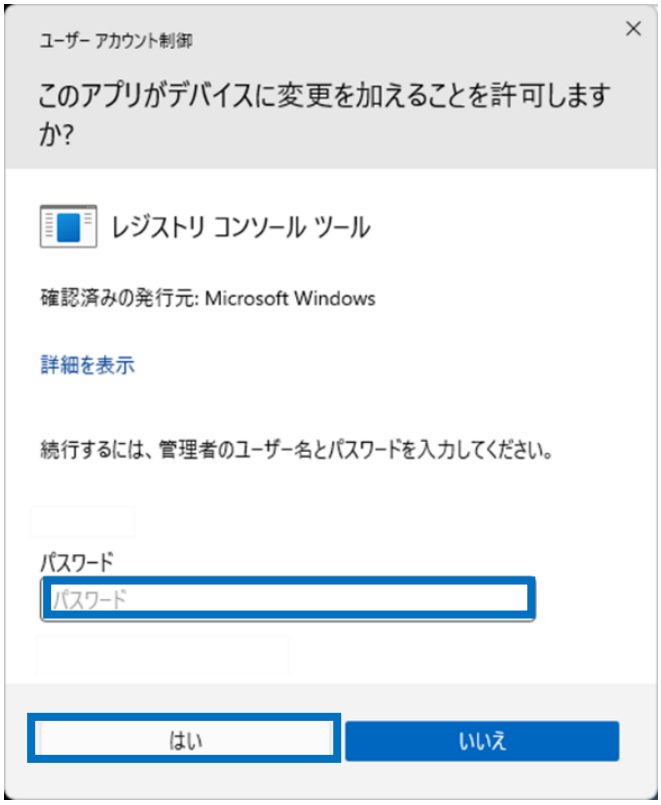
利用規約を確認してください。同意する場合は「同意する」ボタンをクリックします。



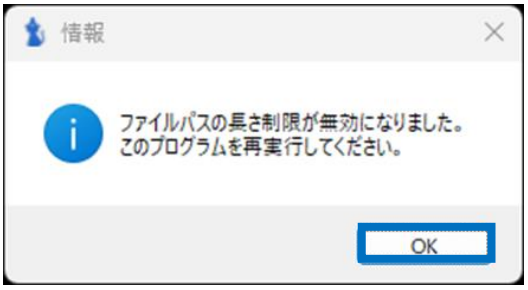
次のメッセージが表示された場合、「OK」ボタンをクリックします。



次のメッセージが表示された場合、パスワードを入力し、「はい」ボタンをクリックします。



次のメッセージが表示された場合は、「OK」ボタンをクリックし、再度復号ツールを実行してください。



Step3 暗号化されたフォルダ又はファイルのフルパスを選択

Step3-1 フォルダを選択する場合

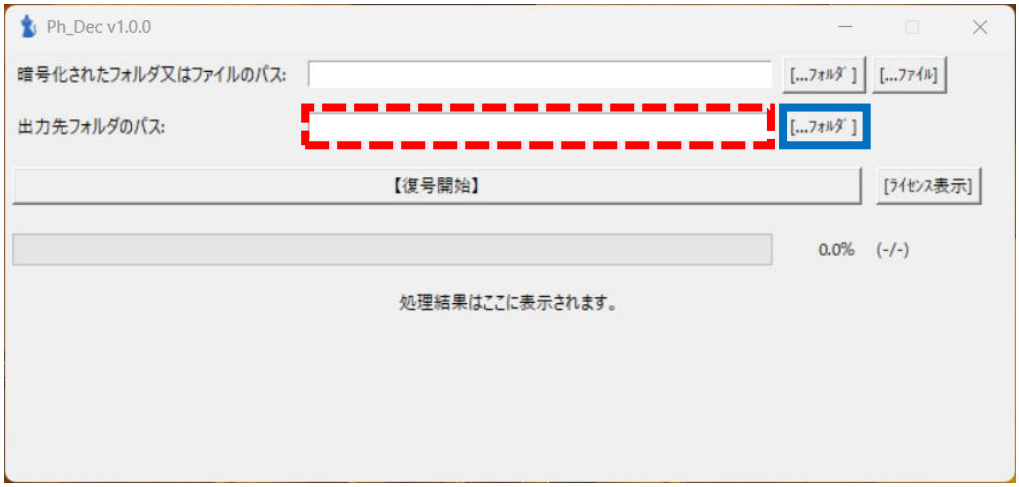
フォルダを選択する場合は選択されたフォルダ及びサブフォルダ内のすべてのファイルの復号を試みます。 の「...フォルダ」ボタンをクリックし、フォルダを選択します。または 内に、ドラッグアンドドロップをします。

Step3-2 ファイルを選択する場合

ファイルを選択する場合、選択されたファイルの復号を試みます。 の「...ファイル」ボタンをクリックし、暗号化されたファイルを選択します。または 内に、ドラッグアンドドロップをします。

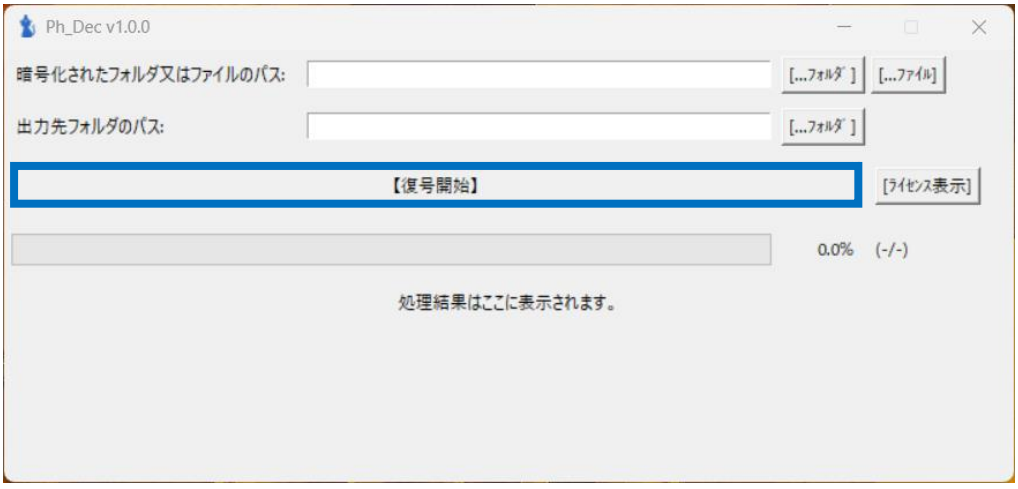
Step4 出力フォルダのフルパスを選択

の「...フォルダ」ボタンをクリックし、暗号化されたファイルを復号した際の出力先のフォルダのパスを選択します。または 内に、ドラッグアンドドロップをします。



Step5 ファイル復号の開始

【復号開始】ボタンをクリックすると復号が開始します。



Step6 ファイル復号の完了

復号が完了すると"完了"というメッセージが画面に表示されます。
復号されたファイルは Step4 で選択したフォルダに保存されています。

- 対象ファイル:復号対象のファイル数
  - 成功:復号に成功した対象ファイル数
  - 失敗:失敗した対象ファイル数
  - 未処理:未処理の対象ファイル数
- 対象外ファイル:復号対象外のファイル数（ファイルが破損等）

参考

このツールは復号した結果を output_{日時}.txt、output_{日時}.csv 及び error.log に保存します。

output.csv ファイルはツールの保存場所に作成された「log」フォルダの中に保存されます。

output.csv は「filepath」と「decrypted」の項目があります。「decrypted」にはそれぞれのファイルの復号結果が記録され、記録される内容は

「yes」：復号成功
「no」：復号失敗（詳細はログに記載されます。）
「no_keys」：鍵情報破損
「corrupted」：ファイル破損又は暗号化未完了

です。