

CDIR Learning ユーザーガイド

動作環境

- Windows OS
 - ローカルストレージ対応の Web ブラウザ
 - Google Chrome、Mozilla Firefox、Microsoft Edge、Opera、Safari 等
- ※ WebBook の閲覧はオフライン環境でも可能です。

アプリケーション構成

CDIR Learning は、

1. **cdirlweb.exe**

学習テキストの WebBook をホストするスタンドアロン型 Web サーバ実行ファイル

2. **_data** (フォルダ)

Hands-on や Mission で解析対象とする演習データの格納フォルダ

で構成されます。



※ **CE 版**（無償の Community Edition）では、Web サーバ実行ファイル名が「**cdirlweb_ce.exe**」となります。また、「_data」フォルダは提供されません。

インストール方法(ZIP ファイル)

- ZIP ファイルを任意のディレクトリへ解凍します。解凍後は以下の構成となります（※有償版の例）。

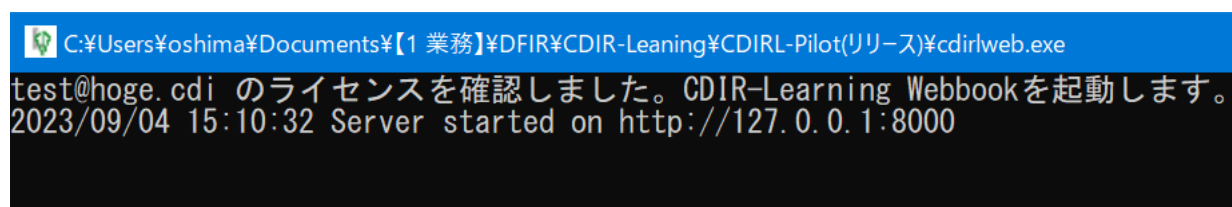
名前	種類
_data	ファイル フォルダ
cdirlweb.exe	アプリケーション

- Hands-on や Mission で使用する一部の解析用ツールは、日本語名のディレクトリパスを認識しません。日本語名のパス配下にインストールする場合、「_data」フォルダは**日本語名が含まれないパス**に移動して下さい。

WebBook 閲覧方法

- 発行された**ライセンスファイル**（拡張子：.lcd）を、インストールしたフォルダ直下（cdirlweb.exe と同じ階層）へ保存します。 **※CE 版はライセンスファイル不要です。**
- 同フォルダの「**cdirlweb.exe**」（CE 版は「cdirlweb_ce.exe」）をダブルクリック等で実行します。
- ローカルループバック：**127.0.0.1** /ポート番号：**8000** で WebBook のホスティングが開始されます。続いて自動的に Web ブラウザが起動され、WebBook のトップページが表示されます。

【cdirlweb.exe による WebBook のホスティング起動画面】



※ WebBook 閲覧中は終了しないで下さい

【WebBook トップページ】



【留意事項】

- Windows に既定として設定された Web ブラウザが起動されます。
- 誤って Web ブラウザやタブ画面を閉じてしまった場合は、cdirlweb.exe を終了して再起動するか、Web ブラウザのアドレス欄に「http://127.0.0.1:8000」を入力して再表示して下さい。なお、ローカルループバックにのみバインドしていますので、外部からはアクセスできません。また、外部への通信も行いませんので、オフライン環境でも利用可能です。
- 初回起動時、Windows の SmartScreen 等による保護機能で、実行ブロックのメッセージが表示されることがあります。その際は、cdirlweb.exe (cdirlweb_ce.exe) のデジタル署名（ファイルを右クリック → 「プロパティ」 → 「デジタル署名」タブ → 「詳細」ボタン）を確認のうえ、実行を許可してください。

- cdirlweb.exe (cdirlweb_ce.exe) が初めて WebBook のホスティングを開始する際、Window ファイアウォール等の許可設定が必要になる場合があります。警告が表示された場合は許可をお願いします。
- ポート番号：8000 が別のプロセスで使用中の場合は、エラーメッセージが表示されます。その場合、使用中のプロセスを終了させるか、コマンドプロンプトから cdirlweb.exe に未使用のポート番号（1024 以上）を引数として指定のうえ、再度実行して下さい。
 - 実行例 `> cdirlweb.exe 9000`
 - 常に 8000 番以外の固定のポート番号で起動する場合は、「cdirlweb.exe」のショートカットを作成し、上記実行例のようにポート番号を指定した形でリンク先を設定して下さい。

演習データの利用方法

- インストールフォルダ内の「_data」フォルダに、各章の演習用データが保存されています。
- 同フォルダは、適宜作業しやすいディレクトリパスや別の PC へコピー／移動して利用することができます。ただし前述のとおり、日本語名を含まないディレクトリパスへ保存して下さい。
- 解析に使用するツールは、WebBook の学習テキストに記載された案内に従い、適宜必要に応じて各ツールの公式サイトからダウンロード／セットアップして下さい。最低限セットアップが必要となる解析ツールは次のとおりです（いずれも無償利用可能）。
 - CDIR-C/CDIR-A : ファストフォレンジック用証拠保全/解析ツール
 - <https://www.cyberdefense.jp/products/cdir.html>
 - FTK Imager : ディスクイメージの取得および解析
 - <https://www.exterro.com/digital-forensics-software/ftk-imager>
 - Detect-It-Easy : マルウェア検体等の実行ファイル表層解析
 - <https://github.com/horsicq/DIE-engine/releases>
 - UPX : マルウェア検体等のパック／アンパック
 - <https://upx.github.io/>
 - Strings : バイナリファイル内の文字列抽出
 - <https://docs.microsoft.com/ja-jp/sysinternals/downloads/strings>

-
- PECmd : プリフェッチファイル解析
 - <https://www.sans.org/tools/pecmd/>
- Log Parser (CUI) 日本語版 : イベントログ解析
 - <https://www.microsoft.com/ja-jp/download/details.aspx?id=24659>
- Log Parser Studio (GUI) : イベントログ解析用 GUI
 - <https://techcommunity.microsoft.com/gxcuf89792/attachments/gxcuf89792/Exchange/16744/1/LPSV2.D2.zip>
 - 上記 Log Parser がインストール済みである必要あり
- CyberChef : マルチエンコーダ・デコーダ (BASE64 デコードや URL デコード等に使用)
 - <https://gchq.github.io/CyberChef/>
- BrowsingHistoryView : 各種 Web ブラウザの Web ヒストリー解析
 - http://www.nirsoft.net/utils/browsing_history_view.html
- ChromeCacheView : Google Chrome のキャッシュリスト解析
 - http://www.nirsoft.net/utils/chrome_cache_view.html
- MS Excel や LibreOffice の Calc 等、表計算ソフト (CSV ファイル解析に使用)
 - ※ LibreOffice を推奨 --> <https://ja.libreoffice.org/>

学習スコア

- 学習スコアは、サイドバーの「学習スコア確認」をクリックして参照できます。
- 学習スコアのデータは、各 Web ブラウザのローカルストレージに保存されます。そのため、利用する PC や Web ブラウザを変更した場合は、データが引き継がれません。
- ローカルストレージは、URL を単位として管理されますので、同じ PC で同じ Web ブラウザを利用しても、ポート番号を変更した場合は引き継がれません。
 - 例 - `http://127.0.0.1:8000` で 50 点獲得 → `http://127.0.0.1:9000` で起動し、同じ PC・同じ Web ブラウザでアクセスしても 0 点
- Web ブラウザのキャッシュや履歴をクリアしても、ローカルストレージのデータはクリアされません。