

wx_whois_log V2 ツールについて

いろいろな形式のログやテキストファイル（Web サーバーのアクセスログ、Twitter 回答データ等）を入力ファイルに指定すると、記録された複数の IP アドレスを自動抽出して、Whois 情報を一括取得するツールです。

ステルス端末及びインターネットに直接接続した PC で使用できます。

※ V2 から、**IPv6 に対応**しました。

使用上の注意点

- ・ 大量の IP アドレスを含む入力ファイルに対応しますが、1 行に複数の IP アドレスが含まれる場合は、その行の最初に出現した IP アドレスのみ抽出します（改良バージョン検討中）。
- ・ 処理時間の目安は、IP アドレス 1 0 0 件あたり、4 分程度です。
- ・ Whois 情報の取得先は、<https://tools.wmflabs.org/whois/> です。（情報精度は厳密なものではありませんので、あくまで目安として使ってください！）

使用方法

起動すると下記画面が表示されますので、入力ファイルと結果出力先・出力オプションを指定して実行ボタンを押してください。

ステルス端末を使用する場合は、チェックボックスをオンにし、プロキシ認証の「k+職番+M コード」とパスワードを入力してください。

※ チェックボックスをオフのままステルス端末で実行した場合、見た目上の処理は完了しますが、出力ファイルの Whois 情報はすべて空欄になりますので注意してください。

Whois情報自動取得ツール V2 by ooshima

入力ファイル（ログ等に含まれるIPアドレスを自動検出してWhois情報を出力します）

C:\Users\cyber\Desktop\【Toolz】\MyPython\wxpython版\log_whois_V2\testdata\in.txt

参照

出力ファイル

C:\Users\cyber\Desktop\【Toolz】\MyPython\wxpython版\log_whois_V2\testdata\out.txt

参照

出力オプション

i... IPとWhois情報のみ出力

t... タブ区切りで元データにWhois情報を追加

s... スペース区切りで元データにWhois情報を追加

c... カンマ区切りで元データにWhois情報を追加（デフォルト）

☒ ステルス端末を使用

k職番+M k1111112

パスワード ●●●●●●

実行

C:\Users\cyber\Desktop\【Toolz】\MyPython\wxpython版\log_whois_V2\testdata\in.txt

に含まれるIPアドレスのWhois情報を取得します

出力オプション: i

ステルス端末を使用しない（インターネットに直接接続）

Start! 2018/10/09 18:19:54

処理中...

Done!! 2018/10/09 18:20:02

実行結果の例 (Twitter 回答データ)

入力データ

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA512  
↓  
account_id: 900290881885880322 ↓  
created_at: 2017-10-20 03:41:52 +0000 ↓  
last_login_ip: 1.72.6.250 ↓  
***** ↓  
account_id: 900290881885880322 ↓  
created_at: 2017-10-20 05:45:23 +0000 ↓  
last_login_ip: 1.75.212.128 ↓  
***** ↓  
account_id: 900290881885880322 ↓  
created_at: 2017-10-20 05:47:09 +0000 ↓  
last_login_ip: 182.251.229.91 ↓  
***** ↓  
account_id: 900290881885880322 ↓  
created_at: 2017-10-20 06:48:22 +0000 ↓  
last_login_ip: 180.198.242.65 ↓
```



出力データ例 1 (「c」オプションにより、カンマ区切りで情報追加)

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA512  
↓  
account_id: 900290881885880322  
created_at: 2017-10-20 03:41:52 +0000  
last_login_ip: 1.72.6.250, netname=NTTDoCoMo, country=JP, host=sp1-72-6-25.msc.spmode.ne.jp.  
*****  
account_id: 900290881885880322  
created_at: 2017-10-20 05:45:23 +0000  
last_login_ip: 1.75.212.128, netname=NTTDoCoMo, country=JP, host=sp1-75-212-12.msb.spmode.ne.jp.  
*****  
account_id: 900290881885880322  
created_at: 2017-10-20 05:47:09 +0000  
last_login_ip: 182.251.229.91, netname=KDDI, country=JP, host=KD182251229091.au-net.ne.jp.  
*****  
account_id: 900290881885880322  
created_at: 2017-10-20 06:48:22 +0000  
last_login_ip: 180.198.242.65, netname=commufa, country=JP, host=180-198-242-65.nagoya1.commufa.jp.  
*****
```

出力データ例 2 (「i」オプションにより、IP アドレスと Whois 情報のみ出力)

```
1.72.6.25, netname=NTTDoCoMo, country=JP, host=sp1-72-6-25.msc.spmode.ne.jp.  
1.75.212.12, netname=NTTDoCoMo, country=JP, host=sp1-75-212-12.msb.spmode.ne.jp.  
182.251.229.91, netname=KDDI, country=JP, host=KD182251229091.au-net.ne.jp.  
180.198.242.65, netname=commufa, country=JP, host=180-198-242-65.nagoya1.commufa.jp.  
182.251.221.17, netname=KDDI, country=JP, host=KD182251221017.au-net.ne.jp.
```