

オープンリゾルバ状態確認マニュアル

第 1.1 版 2013 年 5 月 16 日

近畿大学 総合情報システム部 (KUDOS)

目的

本書では、DNS サーバが「オープンリゾルバ」の状態かどうかの確認手順を説明いたします。

本書での確認の結果、「オープンリゾルバ」(DNS サーバが学外からの再帰問合せを許可している)の状態の場合、その DNS サーバが DNS アンプ攻撃・DNS ポイズニング攻撃等に悪用される可能性が、大阪府サイバーテロ対策連絡協議会事務局から指摘されております。

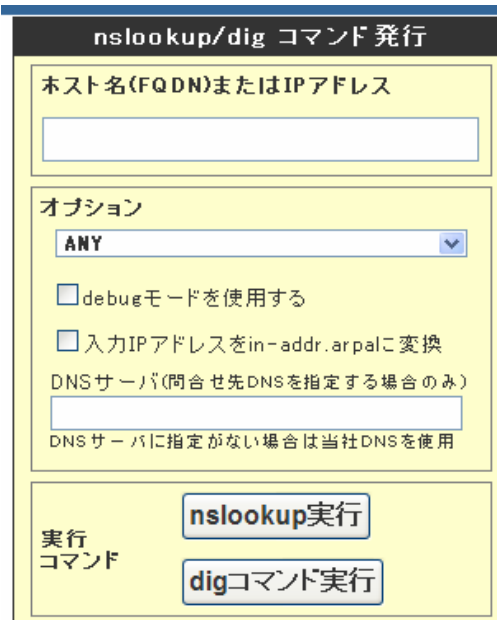
参考 URL (<https://www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf>)

確認手順

手順1、「nslookup(dig)テスト【DNS サーバ接続確認】」サイトを開く。

URL:(<http://www.cman.jp/network/support/nslookup.html>)をクリックする。

(図 1-1)の画面が埋め込まれたサイトが開きます。



The screenshot shows a web form titled "nslookup/dig コマンド 発行". It has three main sections: 1. "ホスト名(FQDN)またはIPアドレス" with an empty text input field. 2. "オプション" section containing a dropdown menu set to "ANY", two unchecked checkboxes for "debugモードを使用する" and "入力IPアドレスをin-addr.arpaに変換", and a text input field for "DNSサーバ(問合せ先DNSを指定する場合のみ)" with a note below it stating "DNSサーバに指定がない場合は当社DNSを使用". 3. "実行コマンド" section with two buttons: "nslookup実行" and "digコマンド実行".

(図 1-1)


手順2、「ホスト名」「DNS サーバ」を入力し、「nslookup 実行」ボタンを押します。

【入力内容】

「ホスト名」:学外のホスト名(画面例:「www.google.co.jp」等)

「DNS サーバ」:確認したい DNS サーバの IP アドレス

参考例:(図 2-1)



This screenshot is identical to Figure 1-1 but with input fields filled. The "ホスト名" field contains "www.google.co.jp", the "DNSサーバ" field contains "163.51.XX.XXX", and the "nslookup実行" button is highlighted with a red box.

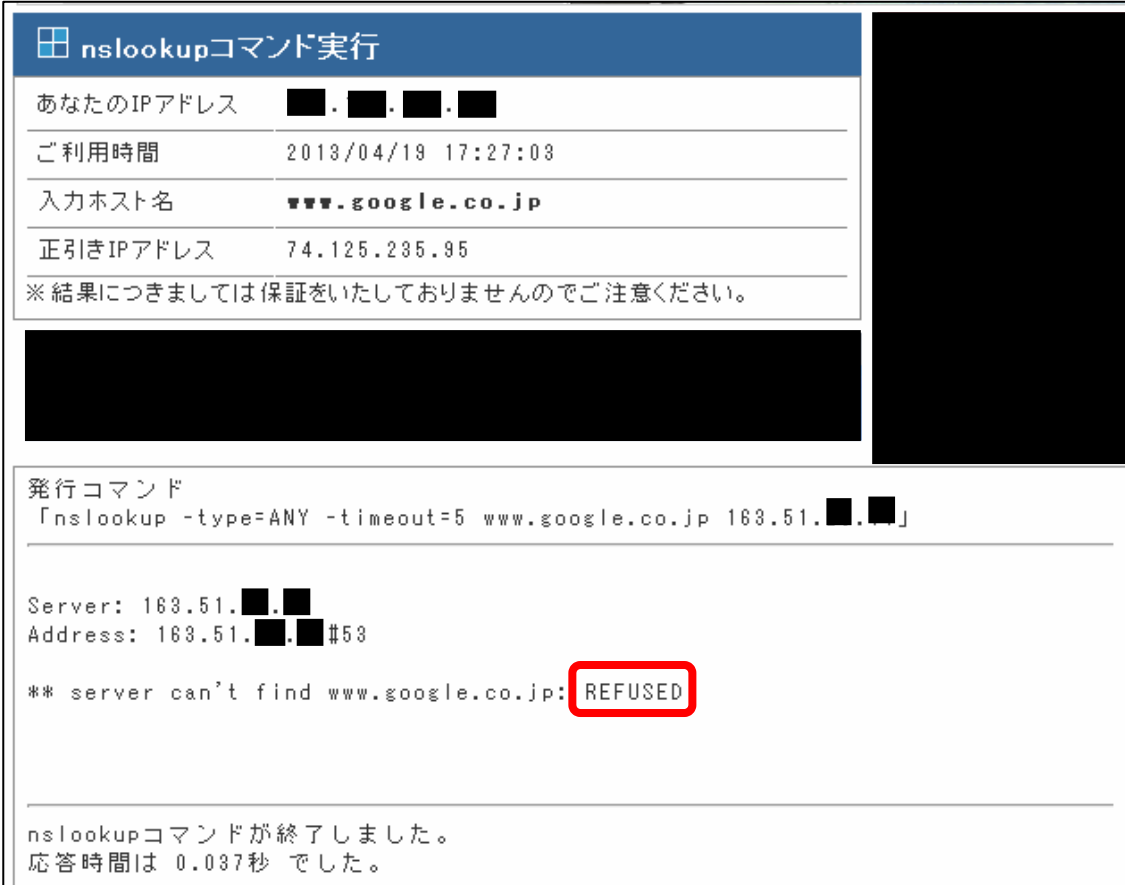
(図 2-1)

手順3、「nslookup コマンド実行」ページが開くので、結果を確認する。

DNS サーバの設定により、下記の 2 パターンのうち、どちらかの結果が返ってきます。

<結果パターン1> : 「REFUSED」 (図 3-1)

この結果が返ってきた場合は「**オープンリゾルバではない**」状態ですので、問題ありません。
確認作業は以上で完了となります。



The screenshot shows a web interface titled "nslookupコマンド実行". It contains a table with the following information:

あなたのIPアドレス	■■.■■.■■.■■
ご利用時間	2018/04/19 17:27:03
入力ホスト名	www.google.co.jp
正引きIPアドレス	74.125.235.95

※ 結果につきましては保証をいたしておりませんのでご注意ください。

発行コマンド
「nslookup -type=ANY -timeout=5 www.google.co.jp 168.51.■■.■■」

Server: 168.51.■■.■■
Address: 168.51.■■.■■ #53

** server can't find www.google.co.jp: **REFUSED**

nslookupコマンドが終了しました。
応答時間は 0.037秒 でした。

(図 3-1)

<結果パターン2> : 「Authoritative answers can be found」 (図 3-2)

この結果が返ってきた場合は、「**オープンリゾルバ**」状態ですので早急に対策が必要です。

「手順4:対策について」に進んでください。

nslookupコマンド実行	
あなたのIPアドレス	■■.■■.■■.■■
ご利用時間	2013/04/19 17:57:35
入力ホスト名	www.google.co.jp
正引きIPアドレス	74.125.235.88
※結果につきましては保証をいたしておりませんのでご注意ください。	

```
発行コマンド
「nslookup -type=ANY -timeout=5 www.google.co.jp 163.51.■■.■■」

Server: 163.51.■■.■■
Address: 163.51.■■.■■#53

Non-authoritative answer:
www.google.co.jp has AAAA address 2404:6800:400a:800::101f
Name: www.google.co.jp
Address: 74.125.235.215
Name: www.google.co.jp
Address: 74.125.235.216
Name: www.google.co.jp
Address: 74.125.235.223

Authoritative answers can be found from:
google.co.jp nameserver = ns4.google.com.
google.co.jp nameserver = ns1.google.com.
google.co.jp nameserver = ns2.google.com.
google.co.jp nameserver = ns3.google.com.
ns1.google.com internet address = 216.239.32.10
ns2.google.com internet address = 216.239.34.10
ns3.google.com internet address = 216.239.36.10
ns4.google.com internet address = 216.239.38.10

nslookupコマンドが終了しました。
応答時間は 0.071秒 でした。
```

(図 3-2)

手順4、対策について

方針:「オープンリゾルバ」状態を「オープンリゾルバではない」状態に設定変更を行ってください。

【設定変更例: BIND を利用されている場合】

<変更内容>

「オープンリゾルバ」(すべての再帰問合せを回答する)状態を
「オープンリゾルバではない」(学内ネットワークのみ再帰問合せを回答する)状態に変更する。

<変更対象ファイル>

「named.conf」ファイル内の下記の記述を変更してください。

<変更前>

```
allow-query-cache { any; };  
allow-recursion { any; };
```

<変更後>

```
allow-query-cache { localhost; 163.51.0.0/16; };  
allow-recursion { localhost; 163.51.0.0/16; };
```

詳細についてご不明な点は、KUDOS までご相談ください。

【問合せ先】

総合情報システム部 (KUDOS)

内線: 3450 メールアドレス: kudos_support@ml.kindai.ac.jp