

Open Resolver 対応状況

一般社団法人
JPCERTコーディネーションセンター
久保 啓司

■ APRICOT 2013 CloudFlare の発表

Country	Open Recursors	Country
Japan	4625	Banlade
China	3123	
Taiwan	3074	
South Korea	1410	
India	1119	
Pakistan	1099	
Australia	761	
Thailand	656	
Malaysia	529	
Hong Kong	435	
Indonesia	349	
Vietnam	342	



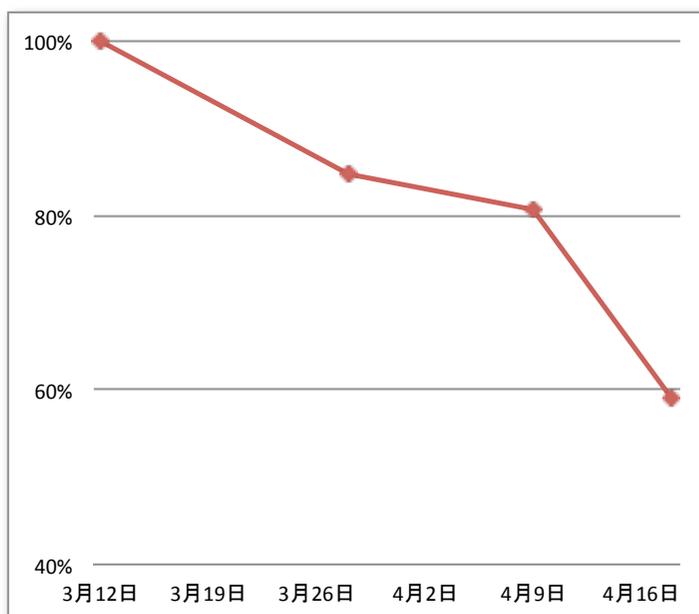
- 日本が一番 (アジア地域)
- JPCERT/CC が黙っているわけにも ;-)
 - > 情報提供いただきました

CloudFlare Tom Paseka
 The curse of the Open Recursor
 APRICOT 2013 Singapore
http://www.apricot2013.net/_data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf

■ 本当か？

-> 確認しました！
85%以上が Open

■ 順次連絡しています



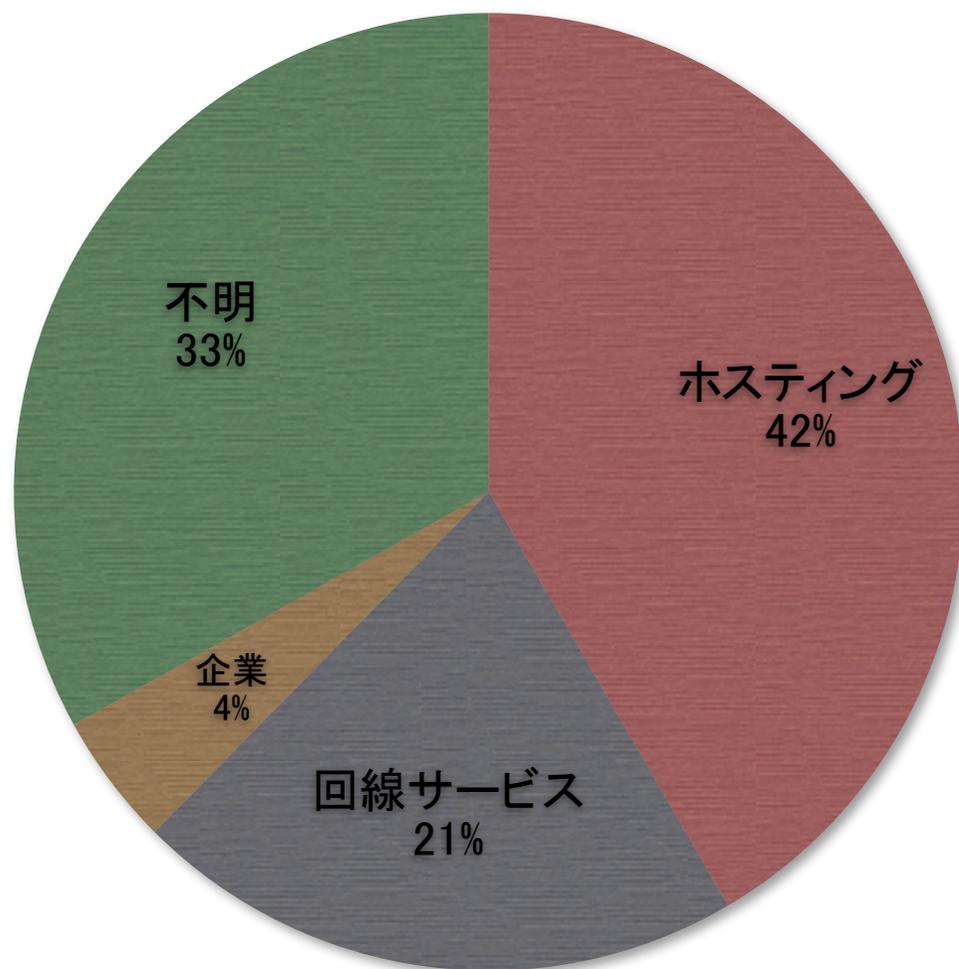
順調に減少しています

4月18日現在、40%程度対応いただいた模様
(連絡に対して)

皆様、ご協力ありがとうございます

どんなところ？

JPCERT/CC のカンと経験で分類



- ホスティングサービスのユーザホスト
- 回線サービスのユーザ宅
- 企業などの DNS サーバ
- ISP のキャッシュサーバ？
(わけあり？歴史的理由)

- ホスティングサービスのユーザホストが多い
 - － DNS サーバが動作しているのが不自然なホストも多い

- そもそもDNSサーバが動いていることを意識していない
 - － なにかのパッケージ？
 - サービス側が提供している OS イメージ
 - 管理ツール(Plesk, CPanel) で配るソフトウェアパッケージとか？

- メッセージが届いていないかも？
 - DNSサーバ管理者ではない人たち

- ぜひ情報提供を

2013年4月18日 JPNIC, JPRS, JPCERT/CC で注意喚起

スクリーンショット1: JPNICのウェブサイト「オープンリゾルバ(Open Resolver)について」のページ。2013年4月18日公開。国内のDNSの機能を持った多数のサーバが踏み台となり、国内外の下記の対策をご覧になり、ご対応、ご確認をお願いいたします。

オープンリゾルバとは

オープンリゾルバとは、インターネットを通じた不特定のDNSのオープンリゾルバになりうるものには、以下があります。

- DNSサーバ
- DNSの応答機能が有効になっているサーバやネットワーク機器デフォルト設定のままであるなど、気づかないうちにDNSの意図せずにオープンリゾルバとなっているサーバは、DDoS攻撃の踏み台となります。

DDoS攻撃の踏み台になってしまった場合の影響

管理しているサーバや機器が踏み台となってDDoS攻撃が行われてもかまわないように扱われてしまう可能性があります。

スクリーンショット2: JPRSのウェブサイト「DNSサーバの不適切な設定「オープンリゾルバ」について」のページ。2013年4月18日公開。株式会社日本レジストリサービス(JPRS)。

重要なお知らせ

2013年

DNSサーバの不適切な設定「オープンリゾルバ」について

2013/04/18公開

株式会社日本レジストリサービス(JPRS)

DNSサーバの不適切な設定である「オープンリゾルバ」は、「DNS Reflector Attacks (DNSリフレクター攻撃)」という分散サービス不能(DDoS)攻撃に悪用される恐れがあり、JPRSではこれまでも各所での情報提供や注意喚起を行ってまいりました。

2013年3月、海外で大規模な攻撃事例があり、一部地域においてインターネットが一時的に利用しにくくなるなどの障害が発生しました。JPRSでは、この問題に関する技術解説やDNSサーバの不適切な設定方法について、改めて以下の通りまとめ、公開しました。

自身の管理するDNSサーバがオープンリゾルバであると、DDoS攻撃の加害者や踏み台となる恐れがあります。DNSサーバ管理者や関係者の皆さまはご確認をお願いします。

- 技術解説:「DNS Reflector Attacks (DNSリフレクター攻撃)」について <http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html>
- 設定ガイド:オープンリゾルバ機能を停止するには【BIND編】 <http://jprs.jp/tech/notice/2013-04-18-fixing-bind-openresolver.html>

■参考URL

- DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起(JPCERT/CC) <https://www.jpccert.or.jp/at/2013/at130022.html>
- オープンリゾルバ(Open Resolver)について(JPNIC) <http://www.nic.ad.jp/ja/dns/openresolver/>

スクリーンショット3: JPCERT/CCのウェブサイト「DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起」のページ。2013年4月18日更新。

安全・安心なIT社会のための、国内・国際連携を支援する

JPCERT/CC

Japan Computer Emergency Response Team Coordination Center

JPCERTコーディネーションセンター

最新情報取得 (RSS | メーリングリスト) | HTTPS | モバイル

Home > 情報提供 > 注意喚起 > 2013 > DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起

DNSの再帰的な問い合わせを使ったDDoS攻撃に関する注意喚起

最終更新: 2013-04-18

JPCERT-AT-2013-0022
JPCERT/CC
2013-04-18

3-04-18 >>>

DDoS攻撃に関する注意喚起

3/at130022.html

本国内のDNSキャッシュサーバを受けています。

外部からの再帰的な問い合わせをオープンリゾルバを使用して、