

# Open Resolver 問題について

一般社団法人JPCERTコーディネーションセンター  
インシデントレスポンスグループ 久保 啓司

# Open Resolver 問題

- 古くからある問題
- 2006年にも大きな問題になりました

JPCERT/CC Alert 2006-03-29

DNS の再帰的な問合せを使ったDDoS 攻撃に関する注意喚起

Measurement Factory が継続的に観測（サンプリング）



# 最近のOpen ResolverによるDDoS攻撃事例

## ■ SpamHaus

- 2013/3/19 から
- 300Gbps? 一週間以上継続?
- CloudFlare が詳しい報告

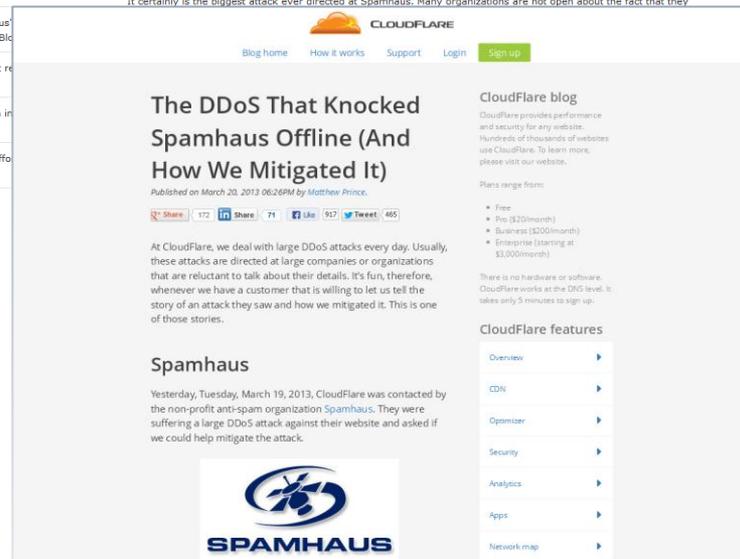
## — Open Resolver Project

### ■ 2170万台のリスト

—リストの取り扱いについて

## ■他にも様々な情報頂いています

## ■小規模な攻撃は日々発生



# JPCERT/CCの対応

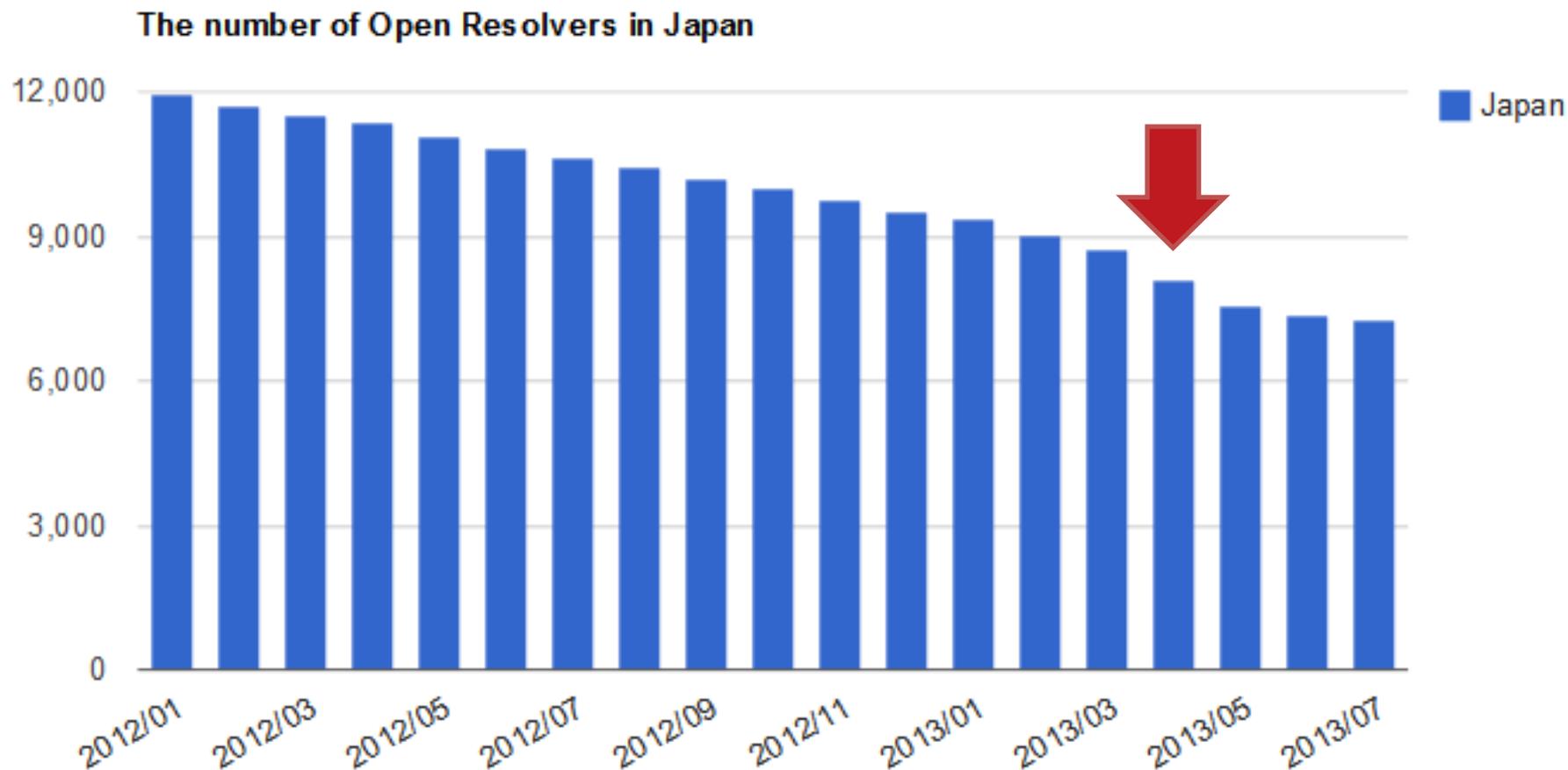
## ■ APRICOT 2013 CloudFlare の発表 (2013/2/26)



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](http://www.apricot2013.net/data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf)

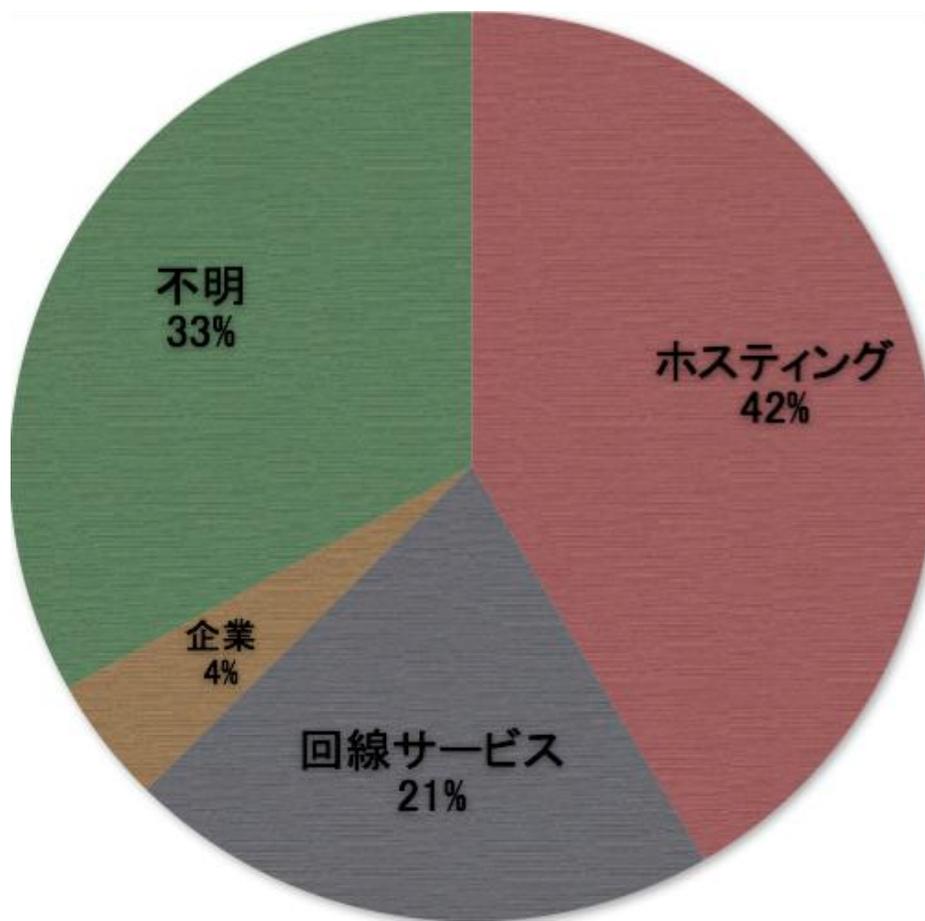
- 日本が一番 (アジア地域)
- JPCERT/CC が黙っているわけにも...  
-> 情報提供いただきました

# 効果



# ホストの分類

## ■ 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

---

- 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

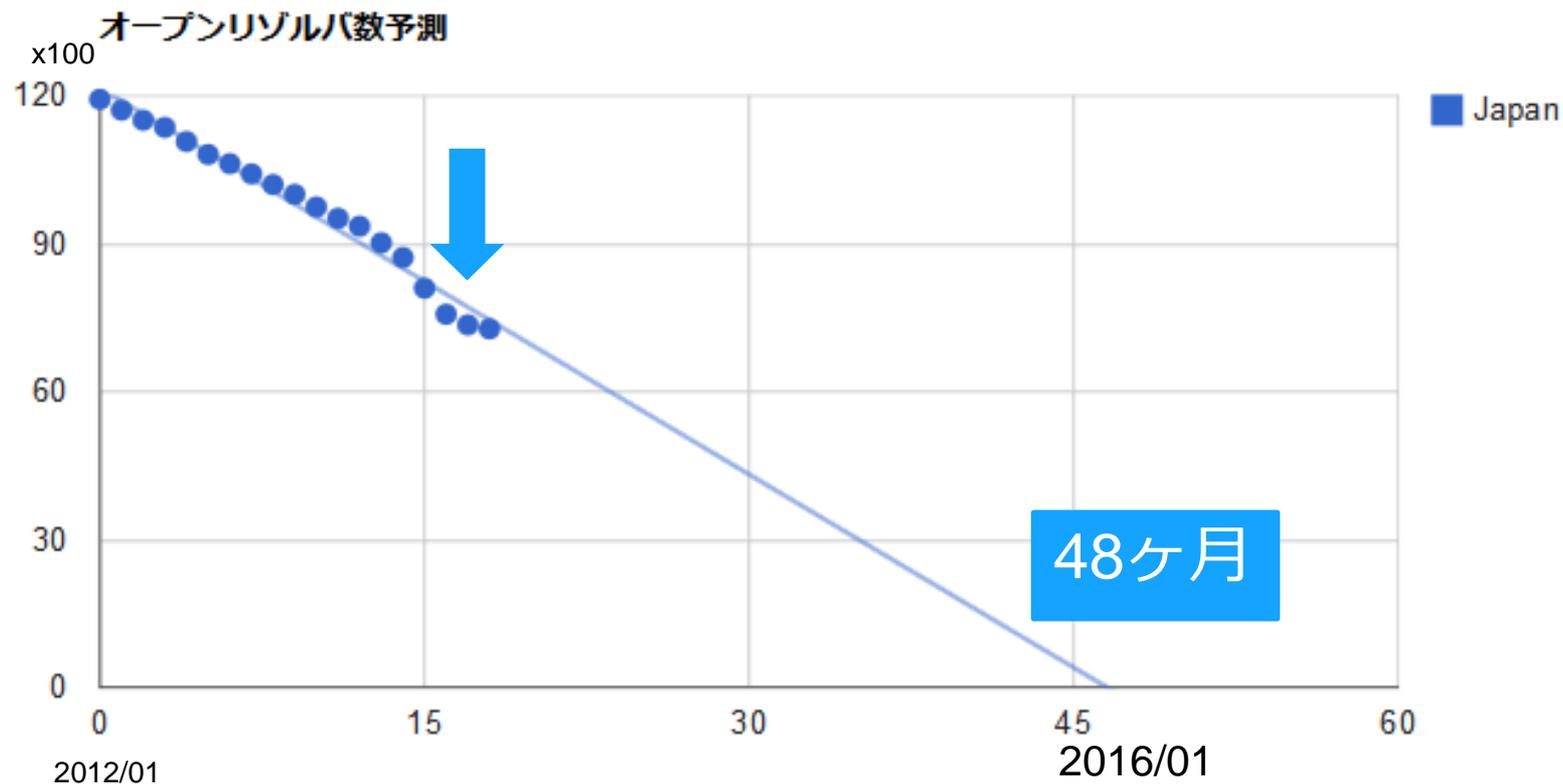
# JPCERT/CCの対応でわかったこと

---

- 連絡をすると対応してもらえる
- JPCERT/CC からの連絡
  - 実際に攻撃に使用されたという情報
  - Open Resolver ということだけでは連絡はしていません
    - ⇒ Open なネームサーバはまだまだあります...

# 今後の予測

■ 2012年1月からの数値で外挿してみました



# Open Resolver 対策サイト

## ■ 現在準備中



### あなたのオープンリゾルバ確認サイト

接続元 IP の状態: 未確認  
設定されているリゾルバの状態: 未確認

確認

接続元 IP アドレス  
設定されているリゾルバ

### あなたのオープンリゾルバ確認サイト

接続元 IP の状態: 無問題  
設定されているリゾルバの状態: 無問題

確認

接続元 IP アドレス: ~~211.55.29.11 (232841.dynippproxy.net)~~  
設定されているリゾルバ: ~~211.55.29.11 (232841.dynippproxy.net)~~

### あなたのオープンリゾルバ確認サイト

接続元 IP の状態: オープン  
設定されているリゾルバの状態: オープン

確認

接続元 IP アドレス: ~~211.55.29.11 (232841.dynippproxy.net)~~  
設定されているリゾルバの IP アドレス: ~~211.55.29.11 (232841.dynippproxy.net)~~

# お問合せ、インシデント対応のご依頼は

## JPCERT コーディネーションセンター

— Email : [office@jpcert.or.jp](mailto:office@jpcert.or.jp)

— Tel : 03-3518-4600

— <https://www.jpcert.or.jp/>

## インシデント報告

— Email : [info@jpcert.or.jp](mailto:info@jpcert.or.jp)

— <https://www.jpcert.or.jp/form/>

## 制御システムインシデントの報告

— Email : [icsr-ir@jpcert.or.jp](mailto:icsr-ir@jpcert.or.jp)

— <https://www.jpcert.or.jp/ics/ics-form>

- Home
- サイト内検索
- トップページ
- 情報提供
  - 注意喚起
  - 早期警戒
  - 脆弱性対策情報
  - Weekly Report
- 各種届出・申込
  - 制御システムセキュリティ
  - ラウンジ
  - 公開資料
    - 四半期レポート
    - 研究・調査レポート
    - CSIRTマテリアル
- イベント
  - プレスリリース
  - JPCERT/CC

関連組織

**FIRST**  
JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。

**APCERT**  
JPCERT/CCはAPCERTの事務局長として協力しています。

### 注意喚起

- 深刻な影響を受ける脆弱性に関する注意喚起
- 2009-06-10 [公開] 2009年6月 Microsoft セキュリティ情報(緊急5件)に関する注意喚起
- 2009-05-13 [公開] JavaScript が埋め込まれる Web サイトの悪化に関する注意喚起
- 2009-06-13 [公開] Adobe Reader 脆弱性に関する注意喚起
- 2009-05-13 [公開] 2009年5月 Microsoft セキュリティ情報(緊急1件)に関する注意喚起
- 2009-04-15 [公開] 2009年4月 Microsoft セキュリティ情報(緊急5件)に関する注意喚起

### 脆弱性関連情報

- ソフトウェア脆弱性
- 2009-06-19 15:00 XOOOPS マニア製 Pkcs7Module におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 AS1 D.O.O 製 activeCollab におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 Movable Type 5.0.2 におけるクロスサイトスクリプティングの脆弱性
- 2009-06-19 14:32 Serene Bach におけるセッション ID が推測可能な脆弱性

### Weekly Report

セキュリティインシデント...  
フィッシングサイト...  
Webサイトの改ざん...  
マルウェア...  
不正アクセス...

発生元への「調査」を依頼したい  
インシデントを「報告」したい

**ISDAS**  
[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

お薦めページ

**セキュリティ対策講座**

教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント

- 第21回 FIRST Annual Conference 京都 参加申し込み受付中
- O/O+ セキュアコーディング ハーフデイキャンプ参加申し込み

Home

HTTPS RSS

サイト内検索

検索

トップページ

情報提供

注意喚起

早期警戒

脆弱性対策情報

Weekly Report

各種届出・申込

制御システムセキュリティ

ラーニング

公開資料

四半期レポート

研究・調査レポート

CSIRT マテリアル

イベント

プレスリリース

JPCERT/CC

関連組織



JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。



JPCERT/CCはAPCERTの事務局長の事務局です。

## 注意喚起

深刻に影響範囲の広い、情報セキュリティ上の脅威など最新のセキュリティ情報を配信しています。

2009-06-10 [\[公開\]](#)

2009年6月 Microsoft セキュリティ情報(緊急6件含)に関する注意喚起

2009-06-19 [\[公開\]](#)

JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起

2009-06-13 [\[公開\]](#)

Adobe Reader 及び Acrobat の脆弱性に関する注意喚起

2009-06-13 [\[公開\]](#)

2009年5月 Microsoft セキュリティ情報(緊急1件)に関する注意喚起

2009-04-15 [\[公開\]](#)

2009年4月 Microsoft セキュリティ情報(緊急5件含)に関する注意喚起

脆弱性関連情報

ソフトウェアなどの脆弱性と対策情報をJVNより提供しています。

2009-06-19 15:00

XOOPS マニア製 PukiWikiMod におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32

A51 D.O.O. 製 activeCollab におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32

Microsoft Works コンバーターにおけるバッファオーバーフローの脆弱性

2009-06-19 14:32

Movable Type Enterprise におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32

Serene Bach におけるセッション ID が推測可能な脆弱性

[詳しく見る](#)

## Weekly Report

2009-06-12日

セキュリティインシデント...  
フィッシングサイト...  
Webサイトの改ざん...  
マルウェア...  
不正アクセス...

発生元への「調整」を依頼したい  
インシデントを「報告」したい

ISDAS  
[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

お薦めページ  
セキュリティ対策講座  
Security  
教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント  
第21回 FIRST Annual Conference 京都 参加申し込み受付中  
C/O++ セキュアコーディング ハーフデイキャンプ参加申し込み

# ご静聴ありがとうございました

Home

HTTPS RSS

サイト内検索

検索

トップページ

情報提供

注意喚起

早期警戒

脆弱性対策情報

Weekly Report

各種届出・申込

制御システムセキュリティ

ラーニング

公開資料

四半期レポート

研究・調査レポート

CSIRT マテリアル

イベント

プレスリリース

JPCERT/CC

関連組織



JPCERT/CCはFIRSTのチームメンバーです。またJPCERT/CCスタッフがSteering CommitteeメンバーとしてFIRSTの運営に協力しています。



JPCERT/CCはAPCERTの事務局長が兼任しています。

## 注意喚起

深刻に影響範囲の広い、情報セキュリティ上の脅威など最新のセキュリティ情報を配信しています。

2009-06-10 [\[公開\]](#)

2009年6月 Microsoft セキュリティ情報(緊急 6件含)に関する注意喚起

2009-06-19 [\[公開\]](#)

JavaScript が埋め込まれる Web サイトの改ざんに関する注意喚起

2009-05-13 [\[公開\]](#)

Adobe Reader 及び Acrobat の脆弱性に関する注意喚起

2009-05-13 [\[公開\]](#)

2009年5月 Microsoft セキュリティ情報(緊急 1件)に関する注意喚起

2009-04-15 [\[公開\]](#)

2009年4月 Microsoft セキュリティ情報(緊急 5件含)に関する注意喚起

[過去の注意喚起](#)

## 脆弱性関連情報

ソフトウェアなどの脆弱性と対策情報をJVNより提供しています。

2009-06-19 15:00

XOOPS マニア製 PukiWikiMod におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32

A51 D.O.O. 製 activeCollab におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32

Microsoft Works コンバーターにおけるバッファオーバーフローの脆弱性

2009-06-19 14:32

Movable Type Enterprise におけるクロスサイトスクリプティングの脆弱性

2009-06-19 14:32

Serene Bach におけるセッション ID が推測可能な脆弱性

[詳しく見る](#)

## Weekly Report

2009-06-12日

# Thank you!

セキュリティインシデント...  
フィッシングサイト...  
Webサイトの改ざん...  
マルウェア...  
不正アクセス...

発生元への「調整」を依頼したい  
インシデントを「報告」したい

ISDAS  
[インターネット定点観測]

インターネット上に配置したセンサーにより、セキュリティ上の脅威となるトラフィックを観測しています。

お薦めページ  
セキュリティ対策講座  
Security  
教育担当者が使える、新入社員などが身につけておくべきセキュリティ知識などを紹介しています。

イベント  
第21回 FIRST Annual Conference 京都 参加申し込み受付中  
C/O++ セキュアコーディング ハーフデイキャンプ参加申し込み