

# IP53Bはじめました



DNS Summer Day 2016  
2016-06-24

株式会社 朝日ネット  
関本義久

# アジェンダ

- IP53B実施までの経緯
  - IP53Bの案内ページ
  - DNSキャッシュサーバへのDDoS攻撃の概要
  - これまでの対策
  - トラブル当日の経緯
  - DDoS攻撃トラフィックの分析
  - IP53B実施の是非について
  - IP53B解除申請
- IP53Bの実装について
  - 実装、課題、今後の展開予定

# IP53B実施まで の経緯

## 会員サポート

🔒 会員専用ページログイン >

WEBメール

> 法人会

会員サポートトップ

各種手続き

サービスのお申し込み

設定ガイド

保守

## IP53Bの実施について

ASAHIネットでは、「IP53B (Inbound Port 53 Blocking)」を実施しております。このページではIP53Bの詳細及び解除方法についてご案内いたします。

### IP53B (Inbound Port 53 Blocking) とは

IP53B (Inbound Port 53 Blocking) とは、オープンリゾルバになっているサーバや通信端末が、DDoS攻撃※1などの踏み台として利用されないように、UDP53番ポート※2をあらかじめブロックする手法です。外部ネットワークからのお客様のIPアドレスに対するアクセスを遮断することで、DDoS攻撃の踏み台にされるなどの不正利用を未然に防ぎます。

※1 DDoS攻撃：通信量を増大させ、通信処理を行うサーバーに高負荷をかけサービス機能を停止させること。

※2 UDP53番ポート：端末がDNSサーバーに問合せを行う際に利用する経路。

<http://asahi-net.jp/support/security/ip53b.html>

# 案内ページ(つづき)

## お客様への影響

通常のインターネット接続や、メールの送受信に支障はありません。DNSサーバーをお客様ご自身で運用しインターネット上に公開されている場合、UDP53番ポートが規制されるため、IPアドレスの問い合わせに回答できなくなりますのでご注意ください。

## 対象のサービス

- ・ASAHIネット auひかりを除く、インターネット接続サービス全て

## IP53Bの解除方法

固定IPアドレスをご利用のお客様へは、個別にIP53Bの解除申請を承っております。  
お手数ではございますが、以下のフォームより必要事項を入力の上、ご依頼ください。

### [▶ IP53B解除申請](#)

お客様が運用しているDNSサーバやルーターが、オープンリゾルバの場合は解除できません。  
弊社にてオープンリゾルバでないことを確認させていただきます。

# 障害事象の概要

- 発生日時:

2015-12-14 12:00頃～15:30頃

- 障害事象:

DNSキャッシュサービスが過負荷状態となり、名前解決がしづらい状態

- 原因:

DNSキャッシュサーバへの処理しきれないDNSクエリ

- 対処:

IP53Bをすべてのユーザに適用した

# 障害当日のトラフィック状況

当日限り

# これまでの対策

- 2012年頃

自社ネットワーク外からのキャッシュDNS利用禁止

- 2014年頃から

攻撃DNSクエリをロードバランサで特定リアルサーバに振り分ける

クエリログ解析をして攻撃に利用されているドメイン単位でブロック

- 攻撃があまりに頻繁に発生し運用が疲弊

unbound化、自動防御モジュール実装

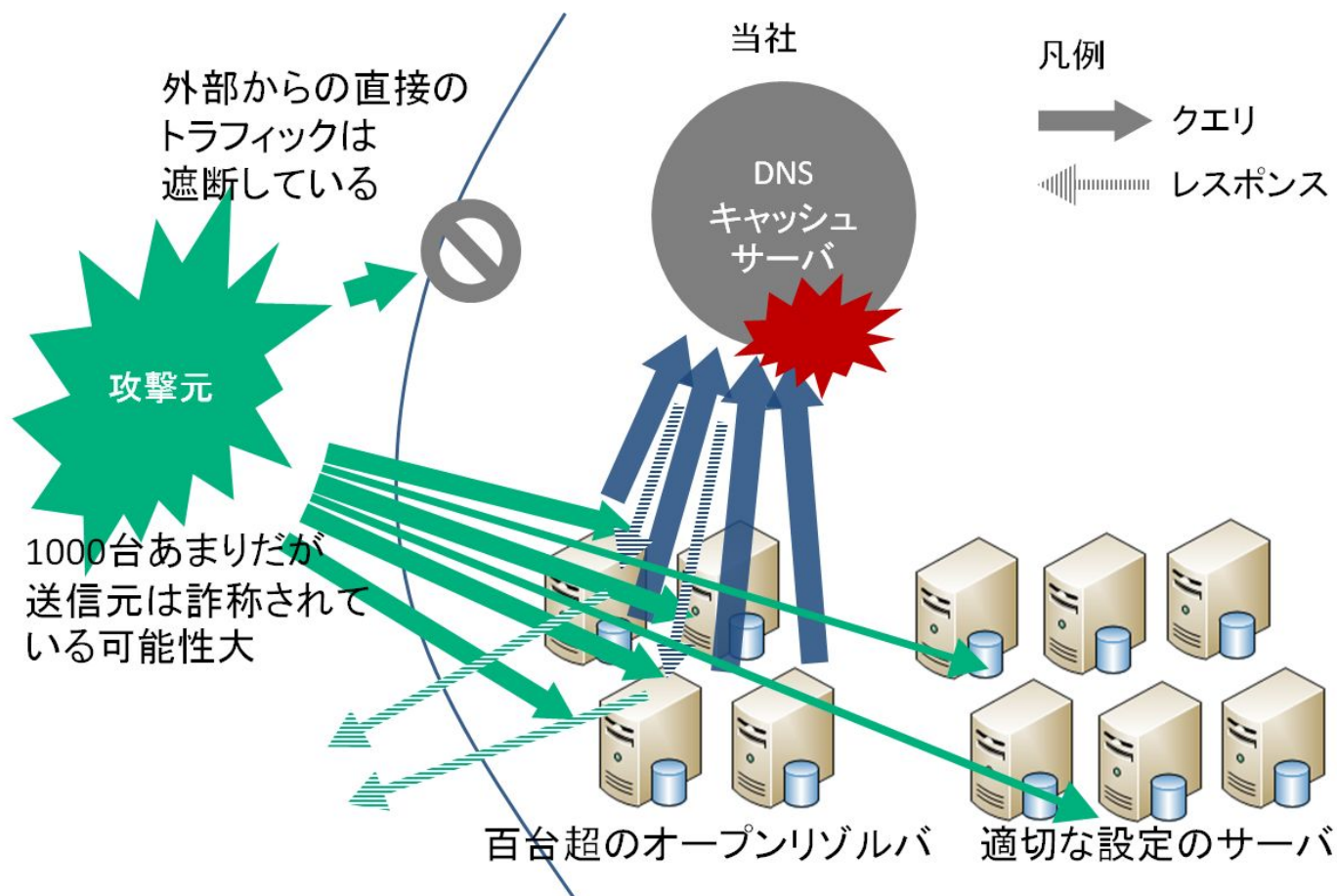


## これまでの対策(つづき)

- 新しいパターンが次々に現れる  
その都度、攻撃判定ロジックをアップデート
- もうIP53Bするしかない？  
とりあえず実装だけは準備しておこう

# 攻撃の仕組み

オープンリゾルバを悪用したリフレクション攻撃の仕組み



# システムのメルトダウン

システムの処理能力を超えてエンドユーザからのクエリの一部に処理されなくなると、再送クエリが大量発生しシステムがメルトダウンした(事後分析)

当日限り

# 障害当日の対応

- 12:00頃 障害発生

クエリログ解析、flow解析等を行うも成果なし

サーバやロードバランサのパラメータ修正等も成果なし

- 15:20頃 全ユーザにIP53B適用
- 17:10頃 固定IPアドレスにIP53B適用除外

再度メルトダウン

- 17:30頃 (再度)全ユーザにIP53B適用

## DNSクエリ分析(事後)

当日限り

# IP53B実施の是非について

- 緊急避難か恒久対策か
  - 当初は緊急避難策であったが、恒久対策として各種文書でお客様への案内を徹底した
- 固定IPアドレスへの適用解除
  - 結果的に適用継続とした
  - サービス申込WebページにもIP53Bの注記を記載
  - DNSサーバを運用されているお客様向けのIP53B解除申請も継続的に受け入れる

# 会員規約と運用ポリシーでの案内



サービス ラインナップ  
SERVICE LINEUP

法人のお客様  
for BUSINESS

会員サポート  
SUPPORT

プロバイダ・インターネット接続のASAHIネットTOP > インターネットサービス一覧 > 会員規約と運用ポリシー > 快適で安全な接続サービス提供への取り組みについて

## 快適で安全な接続サービス提供への取り組みについて

ASAHIネットでは会員の皆様が安心して、ご利用いただくために、以下の取り組みを行っております。

### 1. より多くのお客様に快適にご利用いただくための取り組み

インターネットの利用方法の多様化などによる通信速度が著しく低下する事象が発生して一定期間に大量の通信をご利用されるお客様

#### 実施している内容

- お客様の回線を収容する設備で通信速度の低下がお客様と同じ水準まで自動的に制御し、他のお客様への影響を最小限に抑えます。なお、制御は通信速度の低下が緩和された次第

### 2. 安心してインターネット接続サービスをご利用いただくための取り組み

迷惑メールの通り道を遮断する「25番ポートブロック」を実施しております。

プロバイダー各社が「25番ポートブロック」を導入することで、ウイルスなどによる意図しない迷惑メールの発信を防ぐと共に、迷惑メールの受信も減らすことが可能となります。

詳細は以下のページをご確認ください。

▶ 25番ポートブロック

お客様が利用されているIPアドレスの53番ポートへのUDP通信制御を実施しております。

外部ネットワークからのお客様のIPアドレスに対するアクセスを遮断することで、DDoS攻撃の踏み台にされることによる正常な利用への妨害を未然に防ぎます。

詳細は以下のページをご確認ください。

▶ IP53Bの実施について

# 重要事項説明書での案内

## 提供サービスに関する重要事項説明書

本書面は、電気通信事業法第 26 条（消費者保護ルール）に基づくサービス説明となります。  
契約内容に関する重要なご説明になりますので、内容をご確認いただいたうえでお申込み下さい。

### 1. ご提供サービス（電気通信役務）の内容

説明項目	内容
名称	AsahiNet 光
種類	光回線接続（FTTH アクセスサービス）

NTT 東日本エリア AsahiNet 光ブ AsahiNet 光 AsahiNet 光		
	説明項目	内容
	青少年有害情報フィルタリングサービス	—
	その他利用制限	<ul style="list-style-type: none"><li>・通信品質およびネットワークの公平性確保のため、一定期間に大量の通信をご利用される一部のお客様に対して、通信速度の制御を実施することがあります。</li><li>・通信の安全性確保のため、不正なトラフィックの遮断などお客様の IP アドレスに対して通信ポートの制御を実施することがあります。</li></ul> 詳細は ASAHI ネットホームページにてご確認ください。

最大概ね通信速度

[http://asahi-net.jp/support/account/pdf/important/asahinethikari\\_asahi-web\\_now.pdf](http://asahi-net.jp/support/account/pdf/important/asahinethikari_asahi-web_now.pdf)



# 固定IPサービスページでの案内



ASAHIネットの固定IPアドレスは

# 800円/月

大手プロバイダの中で、一番安い。断然安い。

大好評! 固定IP 無料セット

オプション

かんたん! 会員様 お申し込み

電話

大好評! 固定IP無料セット

フレッツ光、WiMAX、固定IPアドレスの3点セット 固定IPアドレス月額利用料800円/月が無料

フレッツ + WiMAX + 固定IPアドレス

固定IPアドレス 利用料800円/月

無料分の固定IPはフレッツ、WiMAX、どちらにも適用できます。

VPN構築やWebカメラ、オンラインゲームなどで固定IPアドレスをご利用なら、ASAHIネットが

料金	
初期費用	800円
月額利用料	800円/月 <開始月無料! >

※上記の価格はすべて税別です。  
※初期費用は、固定IPアドレスを用いて接続を開始した月に請求いたします。  
※月額利用料は、利用開始の翌日より請求いたします(開始月無料の為)。

## 固定IPアドレス対応接続コース一覧

- AsahiNet 光
- ASAHIネット 光 with フレッツ コース
- フレッツ光ネクスト コース
- Bフレッツ コース
- ASAHIネット WiMAX2+
- ハイスピードモバイル (Xi & FOMA対応) コース
- フレッツISDNコース
- ASAHIネット ドコモ光
- フレッツ・光プレミアム コース
- フレッツ 光ライト コース
- ASAHIネット LTE
- ASAHIモバイル WiMAX
- フレッツADSL BBエントリーコース
- フレッツADSLコース

- 店舗や自宅にWebカメラを設置して遠隔地から設置先の様子を確認することができます。
- 固定IPアドレスを必要とする、オンラインゲームやネット証券などのサービスを利用できます。
- グループウェア「アサワン」でのアクセス制限に利用すれば、セキュリティをさらに強化することができます。

## 固定IPアドレスのインターネット接続設定

### 接続設定ガイド

## よくあるご質問

固定IPアドレスに関するQ&Aは、下記リンク先をご参照ください。

### よくあるご質問 (Q&A) : 固定IPアドレスオプション

ASAHIネットではIP53Bを実施しております。詳細はこちらにてご確認ください。

# IP53B解除申請

## IP53B解除申請

### このフォームについて

- 弊社で実施している「IP53B」の解除について承ります。**必須** は必須項目です。

### ご注意事項

- 弊社にてご利用されている固定IPアドレスが対象となります。
  - お客様が運用しているDNSサーバやルーターが、オープンリソルバの場合は解除できません。弊社にてオープンリソルバでないことを確認させていただきます。
- 固定IPアドレス8個オプションをご利用されているお客様へ
- DNSサーバにてご利用されているIPアドレスのみ記入をお願いいたします。

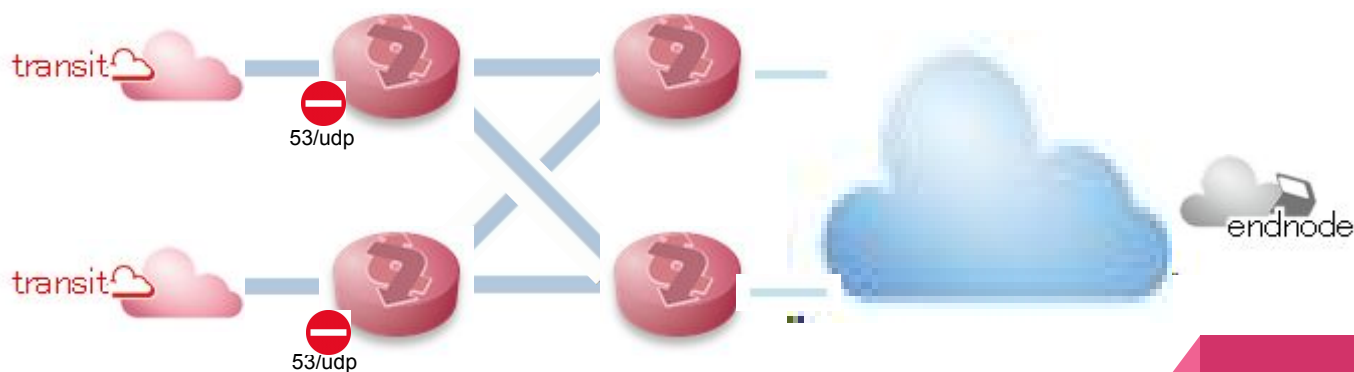
### お客様情報

お名前／法  
人名 **必須**

# IP53Bの実装

# IP53Bの実装方法

- ルータのACLで実施(inbound filter)
  - Core Routerの入りロインターフェイスで制限
- IP123Bなど実装方法の検討
  - IP123B(NTP)など実装方法を検討していたため、IP53Bは迅速に対応



# IP53Bの課題

- ルータのACLには限界がある
  - ホワイトリストの限界
  - 固定IPを売りにしてる為、/32 のACLがたくさん必要
- たくさんACLを書きたい
  - 機種によってまちまち
  - 1024とか、4096とかしか書けない
  - 固定IPサービスをやってるとホワイトリスト管理で直ぐに溢れる
- BGPルータに ACLを都度書くのはちょっと...
  - パフォーマンスの懸念
  - ACL数の上限
  - 事故やオペミスリスク
  - ユーザー毎の個別の設定をここに定義するのは...

## PBR + LB (検討構成)

当日限り

# まとめ

- IP53Bの実施によりDNSキャッシュの障害はなくなった
- 上位の権威DNSサーバに迷惑をかけることもなくなった
- これで戦いは終わったのだろうか。。。

ご清聴  
ありがとうございました