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

つなぐをつくる、つなぐをささえる。
AsahiNet

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

案内ページ

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応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ふり分ける

  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）

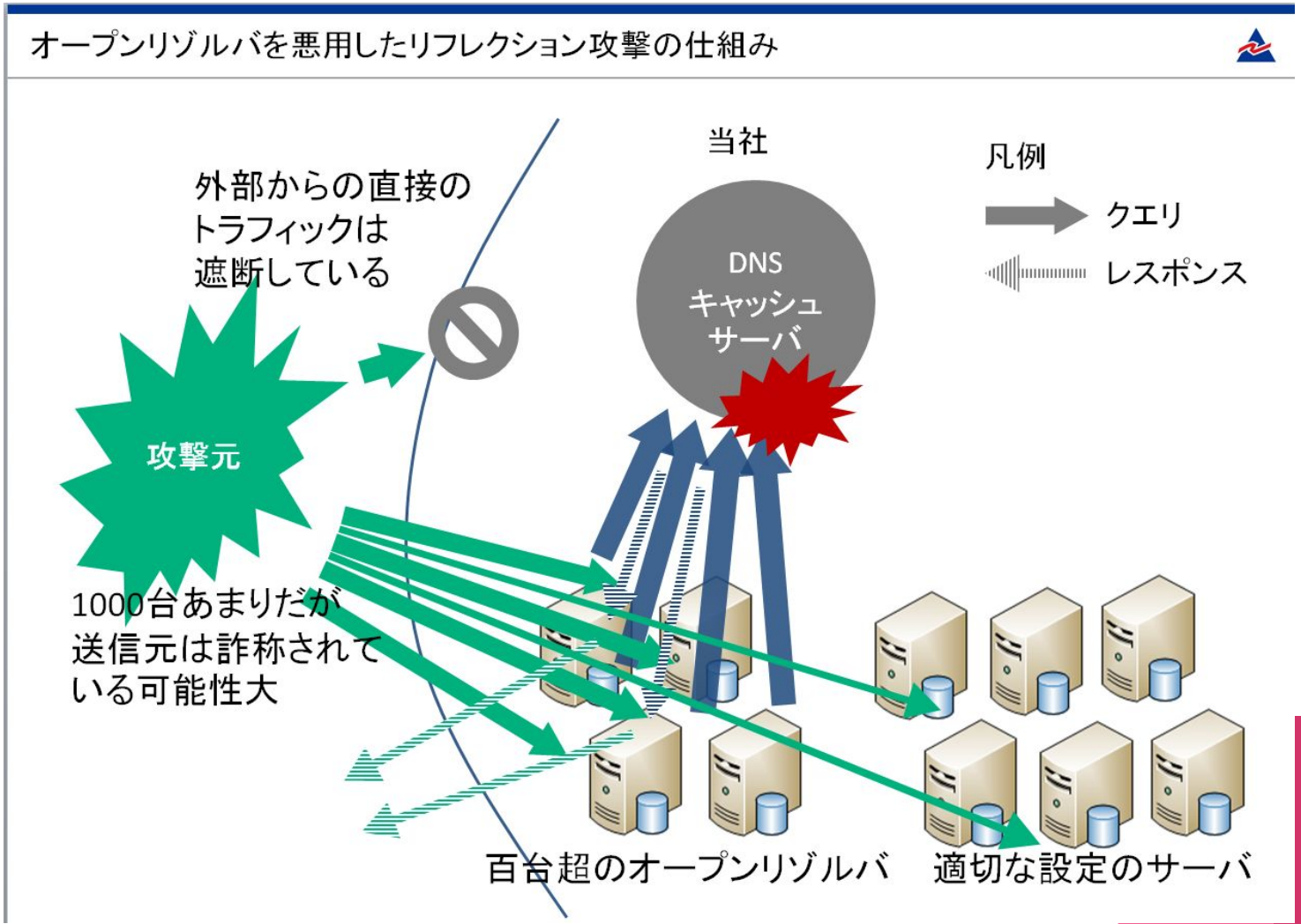
- 新しいパターンが次々に現れる

  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



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応えられなくなると、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

http://asahi-net.jp/service/agreement/networkquality.html

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）
最大概ね通信速度	NTT 東日本エリア AsahiNet 光プ 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	・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。 ・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。 詳細は ASAHI ネットホームページにてご確認ください。

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

 http://asahi-net.jp/service/option/fixedip/

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。

■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

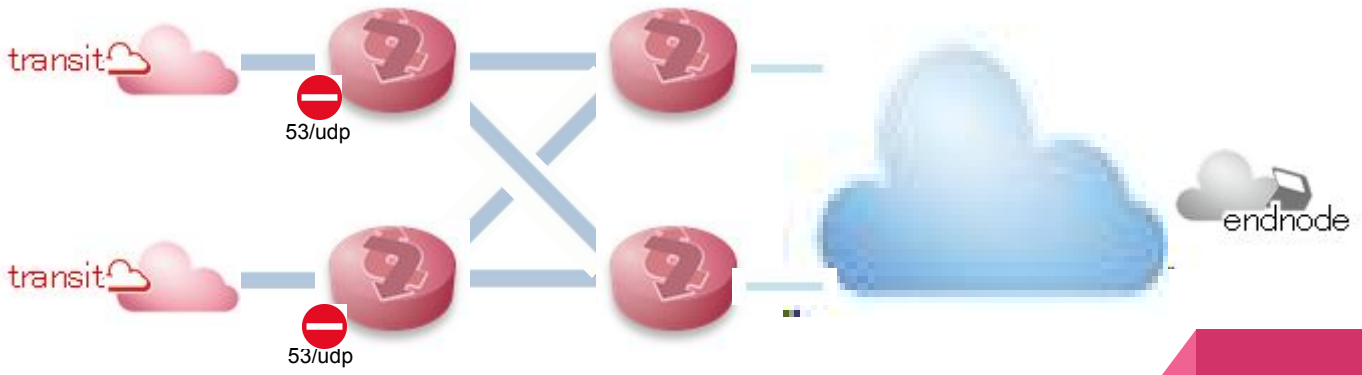
お名前／法人名 必須

https://asahi-net.jp/support/contact/IP53B_unlock.html

IP53Bの実装

IP53Bの実装方法

- ルータのACLで実施(inbound filter)
  - Core Routerの入り口インターフェースで制限
- 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
  - 事故やオペミスのリスク
  - 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

つなぐをつくる、つなぐをささえる。
AsahiNet