Empowered by Innovation NEC

オープンリゾルバ機能停止の取り組み

Internet Week 2013 DNS DAY

NECビッグローブ（株）基盤システム本部
小野　雅弘
mono@biglobe.co.jp

2013年11月28日

目次

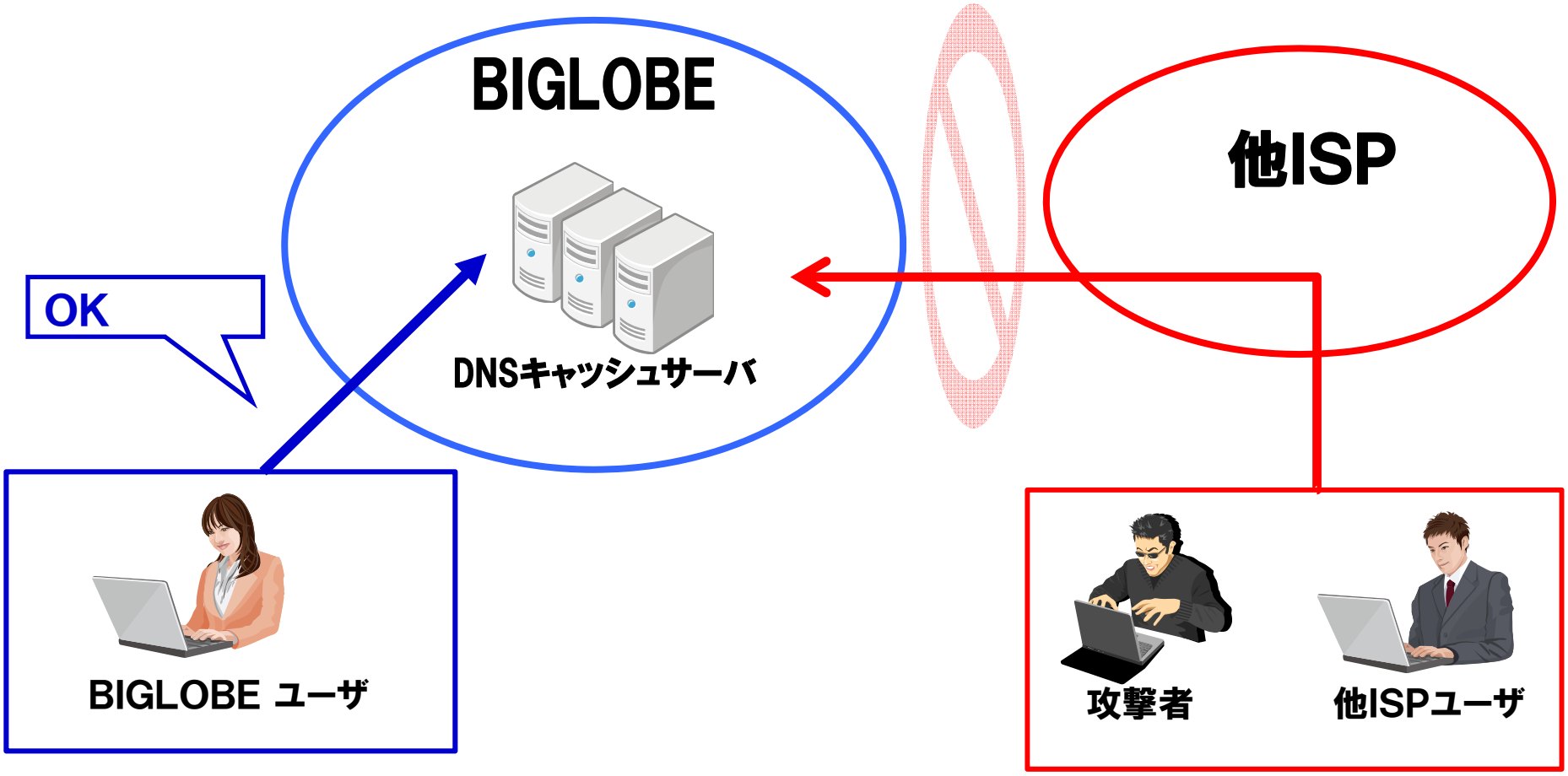
- オープンリゾルバについて
- ビッグローブの取り組み（失敗編）
- 再試行（成功編）
- これからの取り組み

NEC ビッグローブについて

- 1995年 ISP mesh事業開始
- 1996年 PC-VANとmeshを統合BIGLOBE開始
- 2006年 NEC ビッグローブ株式会社設立
  - インターネット等ネットワークを利用した情報サービスの提供および、これに付帯または関連する業務
  - ユーザ数 300万人以上
  - URL http://www.biglobe.co.jp

オープンリゾルバとは

- 送信元を制限していないキャッシュDNS
  - DNSリフレクション攻撃などの踏み台にされる



最近注目

- オープンリゾルバがインターネット全体を脅かす脅威となっている
  - 2013年3月Spamhaus(スパム対策組織)へ、オープンリゾルバを利用したDDoS攻撃が発生
    - ピーク時300Gbpsのトラヒックが発生
  - 各団体、公的機関から注意喚起
    - JPCERT
      - https://www.jpcert.or.jp/at/2013/at130022.html
    - JPNIC
      - https://www.nic.ad.jp/ja/dns/openresolver/
    - JPRS
      - http://jprs.jp/important/2013/130418.html
    - 警察庁
      - https://www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf

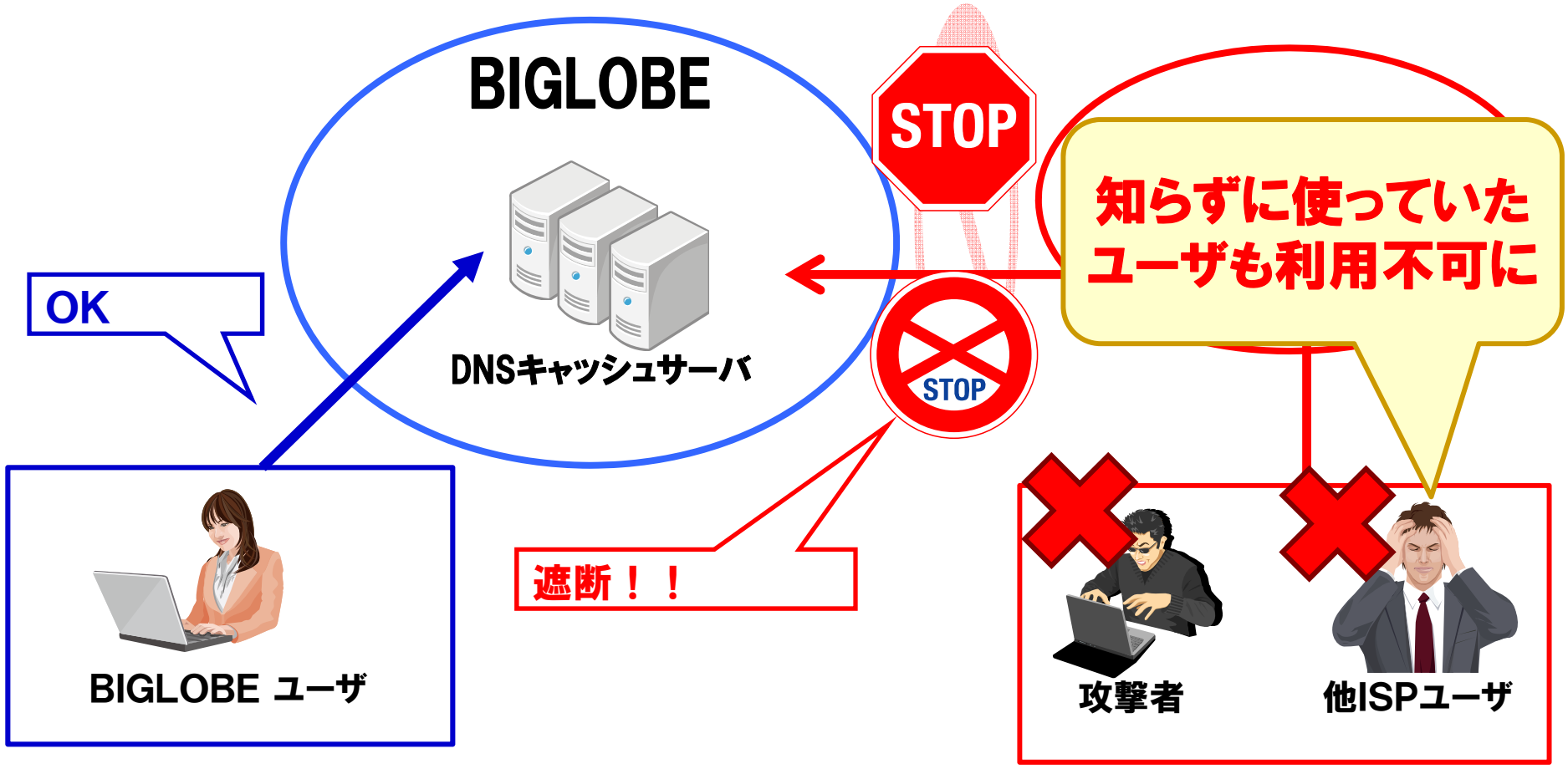
オープンリゾルバの問題点

- DNSリフレクション攻撃などに加担してしまう
- DNSキャッシュサーバのサービス停止
  - ISP会員様が利用不可に
- DNSキャッシュポイズニングの危険

不適切な設定の認識は
あれど

オープンリゾルバの機能停止

- リゾルバがISP副次サービス扱いで利用者を管理していなかったため、変更を連絡することも困難



ビッグローブの
取り組み

最初の取り組み

- 2002年(１１年前)閉塞を試みた
- 社内にDNS運用健全化推進連絡会を発足
- お客様・利用者対応手順整備
  - 申告があった場合、IPアドレスベースで2か月猶予
- 事前のログ解析で利用者への事前連絡
  - 数社１０数IPの閉塞猶予依頼受ける
- アクセス制限は、３つのブロックに分けて週の半ば午前中に実施

2003年のビッグローブのDNSキャッシュサーバ

	DC　基盤	現行ユーザ向け	レガシーDNS
利用者	サーバ 内部運用者	ISPユーザ（3年間） 自動割り当て	2000年以前に個別 設定したISPユーザ
ユーザ通知	なし	あり	あり
ビックローブ外から 利用の割合	0．3％	28．4％	71．3％
Openresolver 機能停止成否	○	×（3回トライ）	×（試行できず）

オープンリゾルバー機能停止失敗(2003年対応)

- 1回目、以前ビッグローブをご利用していた役務提供関係がない法人からサービス障害申告
  利用IPアドレスブロックが不明で想定外
- 2回目、アライアンス契約先の複数ユーザがインターネット利用不可の申告。独立のIP、キャッシュDNSを運用だが、forwarders設定でクエリーが転送されていた。役務提供範囲でも障害
- 3回目、以前ビッグローブをご利用していた1回目とは別の法人からサービス障害申告。契約形態とは別のパワーゲームとなり失敗
- 申告は、3－4時間程度でやってくる

ギブアップ

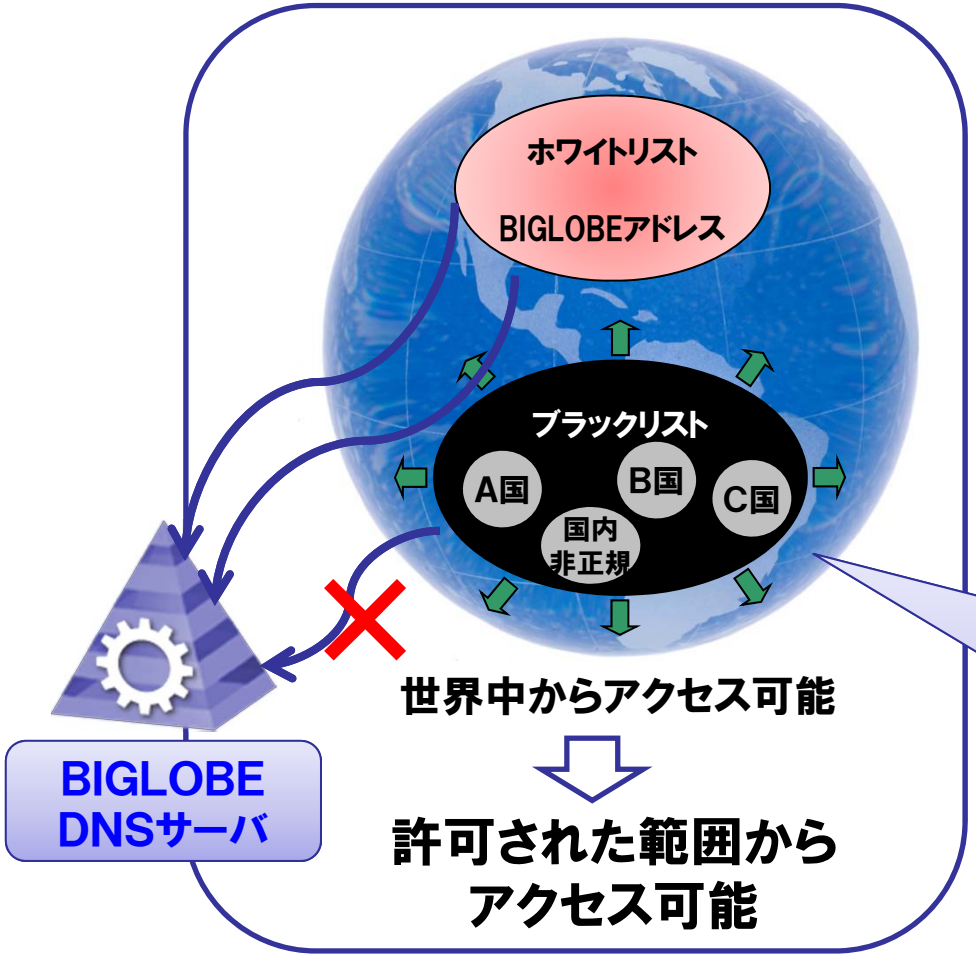
もう、無理～

再び、挑戦（2009～2年間対応）

- 時は流れ、2009年、セキュリティチーム主催のDDOS対策WGに申請しリベンジ
- 前回の失敗を元に作戦を変更
  - アクセス制限したDNSへの引っ越しを促進
    - 工事費の関係で新サービス中心で対応率3割に留まる。
  - クレームに負けないようにトップダウン体制
  - アクセスできる範囲を段階的に絞る
    - 国外　→　日本　→　ビッグローブ
    - フィルタの性能限界範囲内でACLを調整
  - 関係がありそうなISP様にも連絡
  - 検索エンジンで該当DNSサーバを事前調査

オープンリゾルバ機能停止方法

徐々にブラックリストを拡大し、利用者を抑制



ホワイトリスト(新規ユーザ):
アクセスを許可するIPアドレス(ホワイトリスト)を設定
ホワイトリストはBIGLOBE管理のIPアドレス(ローミング等含)
素性が明らかな利用者をホワイトリストサーバに誘導

ブラックリスト(既存ユーザ):
アクセスを拒否するIPアドレス(ブラックリスト)を設定
現時点ではブラックリストは空
随時ブラックリストにIPアドレスを追加

ブラックリストを徐々に拡大
1st (2009.3Q): A国
2nd (2009.3Q): B国
…
国内のBIGLOBE以外のISP

新規ユーザへの影響なし、既存ユーザへの影響を最小限に

機能停止完了（～2011年対応）

- 以前閉塞できなかった法人へは、早い段階で対応を依頼
  - アドレスリストと対応期間を約束
- 検索エンジンで数年前にアライアンス契約していたISPさんがビッグローブのDNSを指定する設定マニュアルを提供していることを発見
  - 6か月の猶予で変更を調整
- 閉塞は、結局5段にわけて実施

2011年ビッグローブ管理のDNSキャッシュサーバ
98％でオープンリゾルバーの機能を停止成功

現在のビッグローブのDNSキャッシュサーバ

	DC　基盤	現行ユーザ向け	レガシーDNS
利用者	サーバ 内部運用者	ISPユーザ 自動割り当て	2007年以前に個別 設定したISPユーザ
ユーザ通知	なし	あり	あり
ビックローブ外から 利用の割合	0%	0%	100%
Openresolver 機能停止	○	○	×（これから）

そして2013年

- 残り2％のDNSサーバが、オープンリゾルバーであると連絡あり（JPCERTさん）
- 他社もオープンリゾルバ機能停止に向けた活動が活発化。啓蒙活動や実害もでており、機は熟している。
- 国外・ビックローブの2段階で、2014年1月(海外)から閉塞作業を行います。
- 創業開始当時のDNSサーバなどで、ご迷惑をお掛けするかもしれませんが、みなさんのご協力をお願いします。

まとめ

- オープンリゾルバを機能停止した際は、重大な影響が出る可能性もあり、すぐには利用IPリストは出てこないことが多いので対応方針を決めておく
- アクセスリストが管理できることを第一目標に
- 長期戦になることも
- トップを巻き込んで体制作り
- 段階的に閉塞したほうが失敗しにくい

以上

ご清聴ありがとうございました