

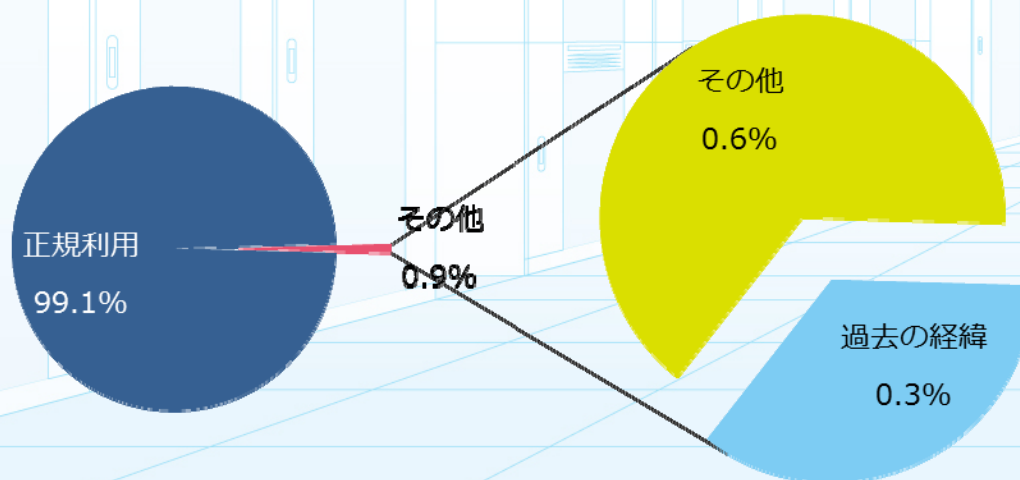
ホスティングサービスでのオープンリゾルバ対応

さくらインターネット株式会社
井上 昌之

- サービス開始当初よりキャッシュDNSサーバを提供
 - 当時はオープンリゾルバではなかった
- 2003年頃からオープンリゾルバ
 - ホスティングをはじめ、全サービスで利用しているキャッシュDNSサーバがオープンリゾルバに
- 2013年に入って問合せが来るように
 - キャッシュDNSサーバは接続元を制限しているか
 - 攻撃につかわれていないか
- 2013年4月頃から検討を開始
 - 利用状況調査・対応方法の検討…etc

- 事前調査では正規利用が全体の99%以上
- 外部の利用は1%未満
 - 過去に提供していたサービスでの利用（事業譲渡）
 - その他 = 完全に第三者の利用ではない
 - お客様が他事業者等で利用されているケースも考えられる

クエリ送信元調査結果



- 現在のサービス利用者以外の許可も必要
 - 過去の事情で許可したものははっきり切れない
 - ある程度の期間は許可が必要
 - 数が増えるとACL設定数の上限にも注意
- 運用面の整備
 - IPアドレス割当時の対応フローの整備
 - 特別に許可したもののリストと期限の管理

- 対策前のアナウンスに対する問合せ
 - 自身に影響が及ぶか ...2件
- 対策後の問合せ
 - 名前解決が行えなくなった ...4件
 - 他事業者からの利用
 - 弊社までアクセスが来ていない
 - XXXの障害が起きているが関連はないか ...1件



ホスティングサービスの現状

- 設定変更しての提供が難しい
 - 利用目的が様々で正解がない
 - 特殊な設定は混乱を招く
- 利用方法の把握が困難
 - 単にトラフィックの急な増加 = 異常とは言えない
 - 通信の内容には関与できない
- 現在の対応
 - BINDをインストールせずに提供
 - 昔はBINDをインストールして提供していた時期も

- ホストサーバを通るパケット数監視
 - 通信品質に影響を与える前に検知
 - 他のお客様に影響を与える前に制限等を実施
- 元々はオープンリゾルバ対策目的ではない
 - 検知できないケースもある

- 問合せベースの対応を継続
 - 状況を確認して対応方法を提案
- ホスティング利用者へ働きかけを検討
 - 構成や用途が様々で案内方法の検討が必要
 - 対応方法に言及が必要なケースも
 - 単純にオープンリゾルバやめようでは難しい



ご清聴ありがとうございました