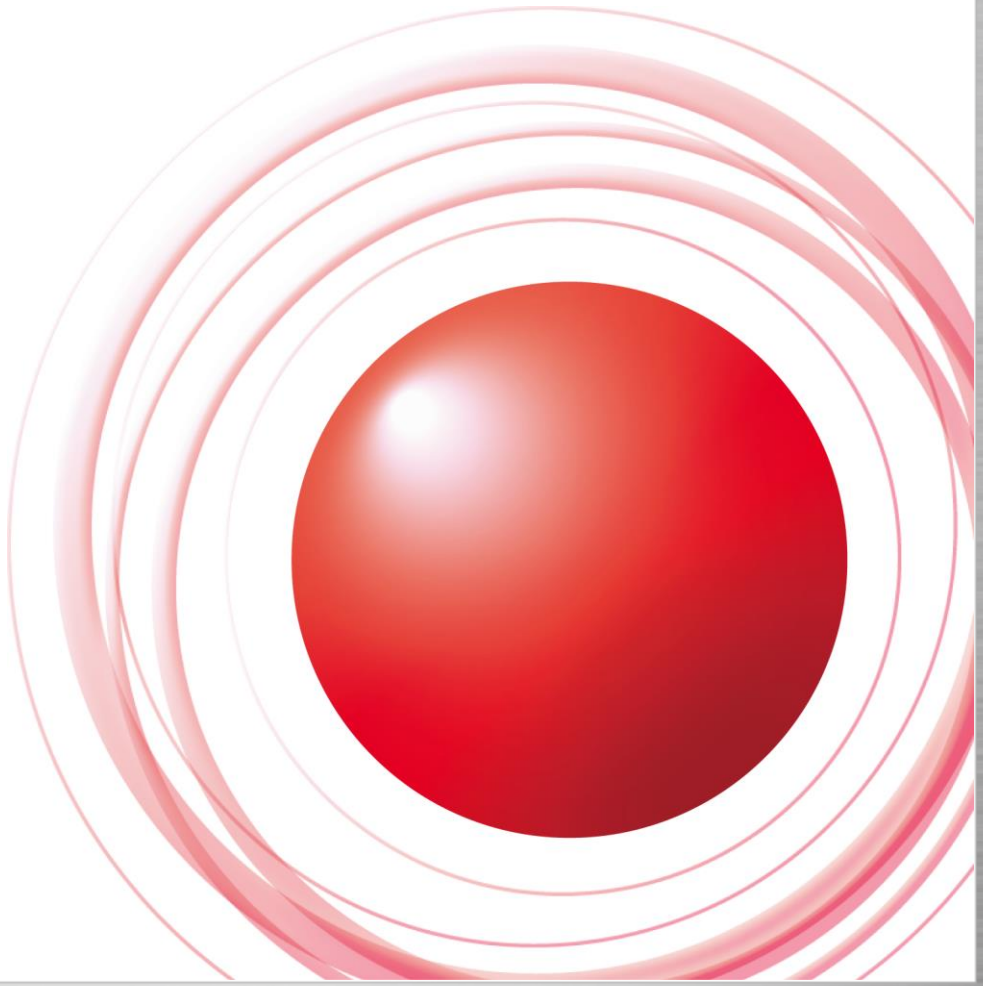
顧客向け参照用DNS管理者の憂鬱
～無償だと思っていたDNSBLが有償だったら～

IIJ
Internet Initiative Japan



株式会社インターネットイニシアティブ
島村 充 <simamura@iij.ad.jp>

Ongoing Innovation

「憂鬱」と言っていますが、今日は
(残念ながら？)水責め攻撃の話ではありません

はじめに

- IIJは回線サービスを販売しています
- 回線サービスのお客様向けに共用の参照用DNSサーバーを運用しています
- サーバーホスティングサービスも販売していて、そちらも共用の参照用DNSサーバーがあります
- 回線サービスは色々あり、また、お客様の利用目的も様々です
  - 回線事業者さんでトランジットを買ってる
  - 事業所のインターネットアクセス用
  - VPN用
  - メールサーバーを運用

DNSBL

- DNS BlackList (RFC5782 (知りませんでした))
- DNSを利用して、IPアドレスやらURIが黒かどうかを判定する仕組み
  - メールの送信元のIPアドレスがspam送信をしているか？
  - メールの本文(など)に書かれているURIがspamに記されているものか？
  - メール以外でも使える(Blog Spam Blocklist)
- 192.0.2.1を検索したい →1.2.0.192.all.rbl.jp
  - NXDOMAIN: 白, 127.X.X.X: 黒
    - IPアドレスの区分は事業者ごとに異なる

ある日…

- こんなメールが来ました。

Subject: Sp○mhausデータフィードサービスに関する重要なお知らせ

株式会社インターネットイニシアティブ
IPアドレス担当窓口 ご担当者様

平素より大変お世話になっております。
Sp○mhausデータフィード正規販売店のMXT○ols株式会社でございます。

標記の件につきまして、貴社におかれましては、
Sp○mhausデータフィードサービスを無料でご利用いただいておりますが、
本日現在、無料で利用できる条件を満たしておらず、有料サービスへ移行
していただく必要がございます。詳細は、添付のファイルをご参照ください。

なお、貴社がご利用のIPアドレスは以下のとおりです。
　あいぴーあどれす 逆引き名
　：

つきましては、今後のサービス継続のため、サービス利用および料金体系について、
一度お打ち合わせさせていただきたいと存じます。

ご不明点等ございましたら、末尾のメールアドレスまでお問い合わせください。
何卒宜しくお願いいたします。

はて…？

- 私は、参照用DNSの運用もやってますが、本業はメールサービスの運用です
- メールサービスではSp○mhausのDNSBLは利用していない
- 自社ドメインのメールシステムも関わっているが、そちらでも参照していない
- そもそも、メールに書いてあるIPアドレスは回線サービスやホスティングサービス向け参照用DNSの実体IPアドレス
  - 自社ASPサービスの参照用DNSは別立て

なにはなくともtcpdump

```
# tcpdump -i eth0 -nn -p dst port 53
  and dst host ${サービスしてるIPアドレス} ¥
  | grep -i sp○mhaus.org
```

どばーーー

なにが？

- どうやら
  - ホスティングサービスの顧客が、そこでメールサーバーを運用していて、DNSBLを参照するようにしていて、メールが1通来るたびに1クエリ。メールを大量にさばいてる模様
  - 回線サービスを購入されている顧客のメールサーバーが(略)
  - トランジットを購入されている顧客の、その先の顧客がメールサーバーが(略)
    - なんでIIJの参照用DNSを使ってるんですか…
- 1顧客で最大20qps程度。全体で200qps程度

利用条件

Free Use

1) Your use of the Sp○mhaus DNSBLs is non-commercial*, and
2) Your email traffic is less than 100,000 SMTP connections per day, and
3) Your DNSBL query volume is less than 300,000 queries per day.

If you do not fit all three of these criteria then please do not use our public DNSBL servers, instead see 'Professional Use'.

https://www.sp○mhaus.org/organization/dnsblusage/

たしかに、抵触はしていそう

ご来社いただきました

- ちなみに、MXt○olsさんがSp○mhausの代理店というのは本当です
  - 1年以上前に別のメールなイベントでお会いしていました。
  - そのあと、弊社IPアドレスがspam送信をしていないのに、何度delist申請をしてもBL入りするのでMXt○olsさん経由で対応をお願いして、対応いただけました。

ご来社いただきました (cont.)

- 曰く…
  - DNSサーバー側でクエリを集計して、大量に出しているところに契約のお願いをしている
  - 他ISPにも同様のメールを送っている
    - ISPじゃないところは…？ (聞きませんでした)
  - 来訪したのはIIJが初
  - そもそも、回線サービスで商売してるので、その参照用DNSサーバーから利用するのはnon-commercialではない (えっ？)
  - 有償契約をしてもらえない場合は、クエリ量の多寡によらず遮断の予定である。どのように遮断するかは未定 (え…？?)

遮断方法

- どの範囲で？
  - メールに記載された、大量にクエリを出しているIPアドレス？ (/32？ /24？)
  - IIJ全体？ (AS単位？)
- どういう手段で？
  - ICMP host/port unreachable?
  - REFUSED返す? だんまり？

→ **未定(よくわかってない)**

未定(というよりもわからない)って何!?

Google Public DNSとかどうするの？？

タイムライン

- メールが来たの: 8/5
- ご来社いただいたの: 8/20
- 契約してくれなきゃブロックするよ
  - 当初予定: 8月末日
    (当初、sp○mhausがMXT○olsに言っていたらしい)
  - 予告: 9月末日

そんないきなり言われましても、予算とかー…

というか、なんでうち(回線業者)が払わなきゃいけないの…

対応

- IIJが有償契約結ぶことは無し
  - 回線サービスの役務提供範囲を超えている
- 大量にクエリを送ってきている顧客には個別で対応を依頼
  - 自分で参照用DNSを建ててそちらを使う

    or **どこかの**public DNSを使う
    - 期限(9末)までには全顧客対応頂けました
    - 対応後: 全体で~10qpsくらい
      - それでも30万query/dayは超えているかな？
      - そもそも、この閾値がIPアドレス(/32)単位なのか、組織(AS?)単位なのか、よくわからない

対応 (cont.)

- 営業向けには

「遮断するとsp○haus/MXT○ols側から予告がありました。担当顧客が利用されている場合は自前で参照用DNSを構築の上、MXT○olsと有償契約を結んでいただくよう、ご案内ください」

と周知

  - 顧客には特にアナウンスせず

X-Day

- 10/1, 2(時差があるので)
- dig @IIJの参照用DNSサーバー

  2.0.0.127.zen.sp○mhaus.org

  – あれ？全部普通に応答返ってくるけど？？
  – その後数日、試してみたが、特に問題なし
  – 現在も問題なし
- 大量クエリの顧客に対応していただいて、彼らの閾値を下回ったから？
  – 藪蛇になりかねないので、聞いてません

他ISPさん

- ご来社いただいた頃に他ISPの、参照用DNSを運用されている方に聞いてみました
  - 同様の通知が来ているISPは何社かある
  - 会ってみた会社さんもチラホラ
  - 有償契約を結んだ、という話は聞かない
  - 遮断された、という話も聞かない
    - 特に何をしたわけでもないところも多そう

一体全体、なんだったんだ…

みなさんもお気をつけ下さい。

IIJ Internet Initiative Japan

Any Questions?

Ongoing Innovation