光ブロードバンド BBIQ ビビック

DNS Summer Days 2013

児童ポルノブロッキングの実装と運用自動化

九州通信ネットワーク株式会社 久米拓馬

きらきらつながる QTNet

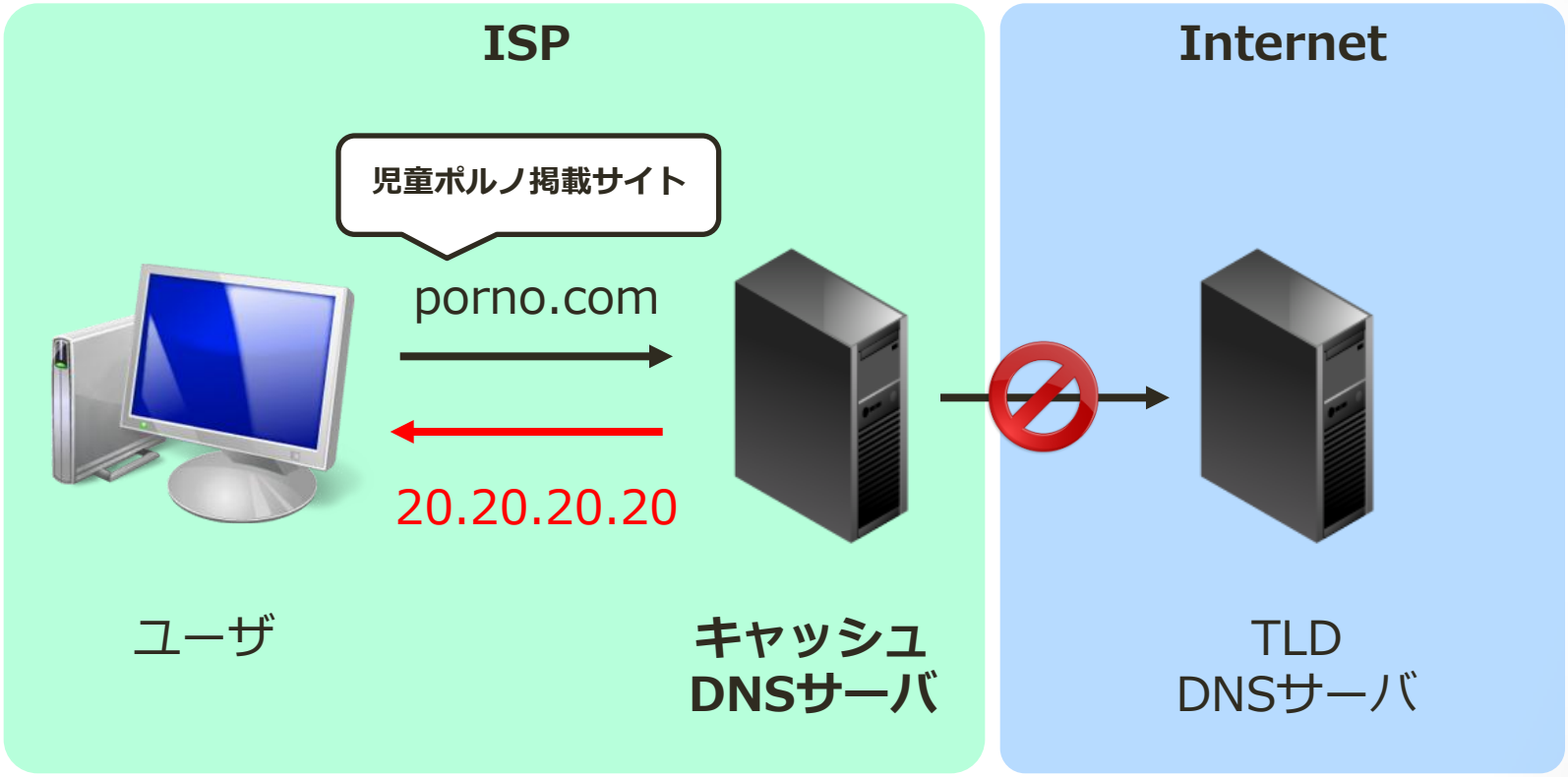
前置き

弊社では児童ポルノブロッキングを、
BINDの機能であるRPZを用いて
自動で運用しています。

本日はRPZを利用するに至った経緯と
運用について紹介させていただきます！

ブロッキングについて簡単に

<例>



ウソの応答を返す！

児童ポルノ掲載サイトについて

ICSA
（一般社団法人インターネットコンテンツセーフティ協会）

- 児童ポルノ掲載サイトのリスト化。
- ICSA会員はリストをダウンロード可能。
- リストはCSVでドメインなどのブロッキングに必要な情報が記載されている。

http://www.netsafety.or.jp/

◎RPZ導入の経緯

RPZとは

- **R**esponse **P**olicy **Z**one の略
- BINDの機能の一部
- BIND-9.8.0以降で標準利用可能
- 元はSPAMなどをブロックするための機能として開発

ブロッキング実装手段

- **ゾーン上書き方式**
- **RPZ方式**

ゾーン上書き方式

- ブロッキングドメインを通常のゾーンとして定義
- 共通のゾーンファイルを設定
- 応答は権威として返す

BINDの場合

named.conf

```
zone "porno1.com" {
        type master;
        file "block.zone";
};
zone "porno2.com" {
…
```

block.zone

```
@       IN      A       20.20.20.20
```

dig @localhost porno1.com

```
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; ANSWER SECTION:
porno1.com.                86400   IN      A       20.20.20.20
```

RPZ方式

- RPZゾーンを指定する。
- RPZ用のゾーンにブロッキングドメインを設定する。

BINDの場合

named.conf

```
options { response-policy { zone "rpz.com" }; };
zone "rpz.com" {
        type master;
        file "rpz.com.zone";
};
```

rpz.com.zone

```
porno1.com    IN    A    20.20.20.20
porno2.com    IN    A    20.20.20.20
…
```

末尾の「.」は不要

dig @localhost porno1.com

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; ANSWER SECTION:
porno1.com.             5       IN      A       20.20.20.20
```

想定される運用

- **共通**
  - リストからブロックドメイン部分を抽出
  - リストは毎週更新される
- **ゾーン上書き方式**
  - named.confにブロックドメインを設定
  - rndc reconfig
- **RPZ方式**
  - 一度RPZゾーンを指定すればnamed.confの変更は必要ない
  - RPZゾーンファイルにブロックドメインを設定
  - RPZゾーンのrndc reload

これを毎週,複数台運用するのは
非常に大変…

自動化しよう！

自動化するならどっちを選ぶ？

- **ゾーン上書き方式**
  - named.confにブロックドメインを設定
    →ブロッキングゾーン定義部分だけ自動生成しInclude
  - rndc reconfig
    →全サーバ自動で実行する → 不安

- **RPZ方式**
  - RPZゾーンファイルにブロックドメインを設定
    →シリアルを上げてゾーンファイルを自動生成する

    ゾーンファイル形式なので複数台あってもAXFRで転送できる！

  - RPZゾーンのrndc reload
    →RPZゾーンのプライマリサーバのみゾーン単位で。

    ゾーン単位のリロードなので他に影響が少なくて安心！

DNSの運用者の方々にRPZを
使ってるとお話しすると

「アレ使ってる人っていたんだ」

とよく言われます。

選ばれない理由

- **RPZが出る前にゾーン上書き方式で実装を完了していた**

- **バグが存在した**
  - ブロックしているドメインのRRSIGを引くと落ちる（現在はバグFIX）

- **利用実績がほとんどない**

それでもRPZを導入したい

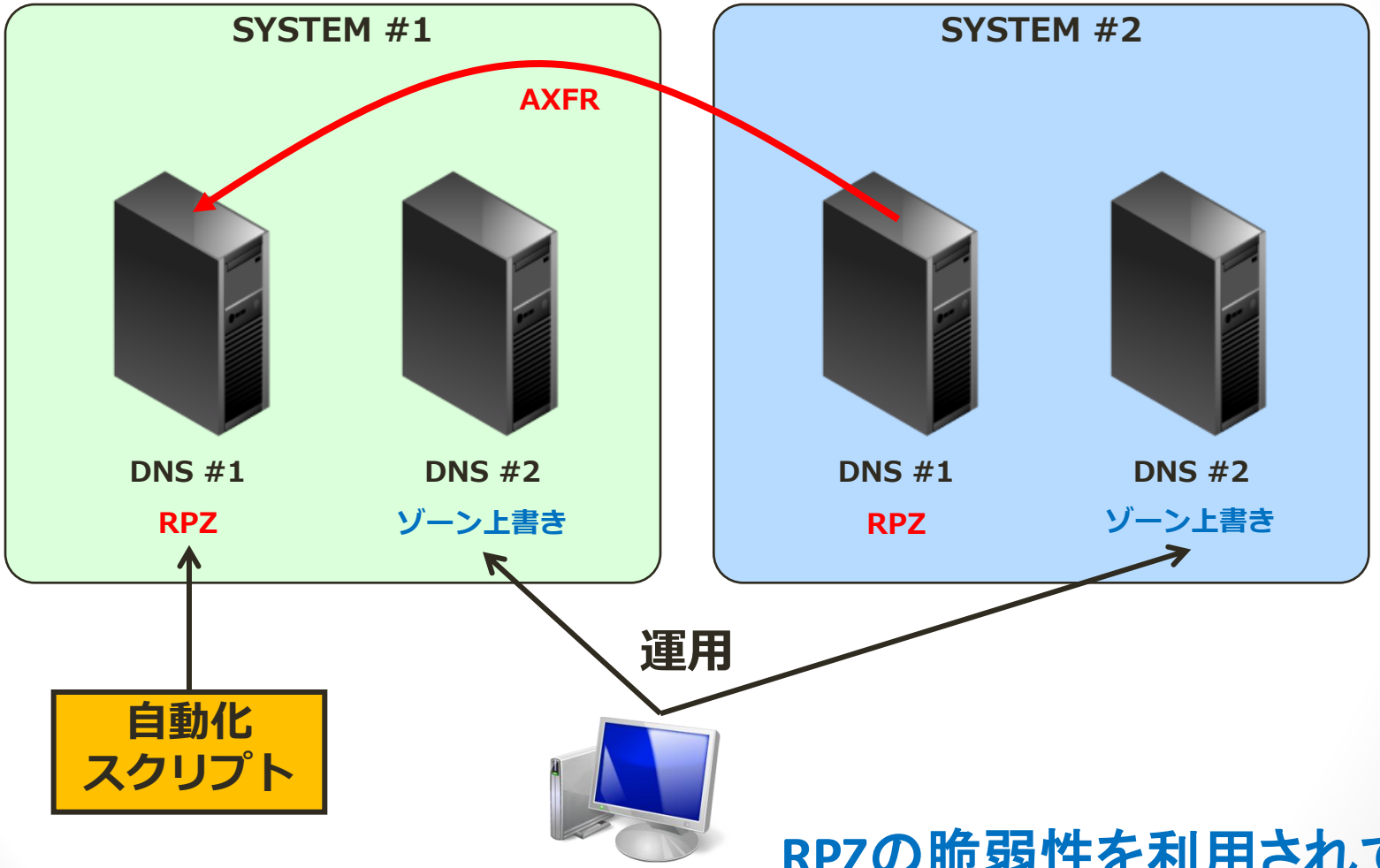
○ 理由…

- **AXFRで転送が可能であり運用が非常に楽。**
- **サーバ増設時の設定が容易。**
  →RPZのゾーンを指定と定義のみ
- **自動化時の影響範囲が狭い。**
  →ゾーン単位のリロード、実行台数最低１台
  →さらに自動化して人為的ミスの削減、効率化
- **RPZの実績を作りブロッキング普及に繋げたい。**

○ 導入するために…

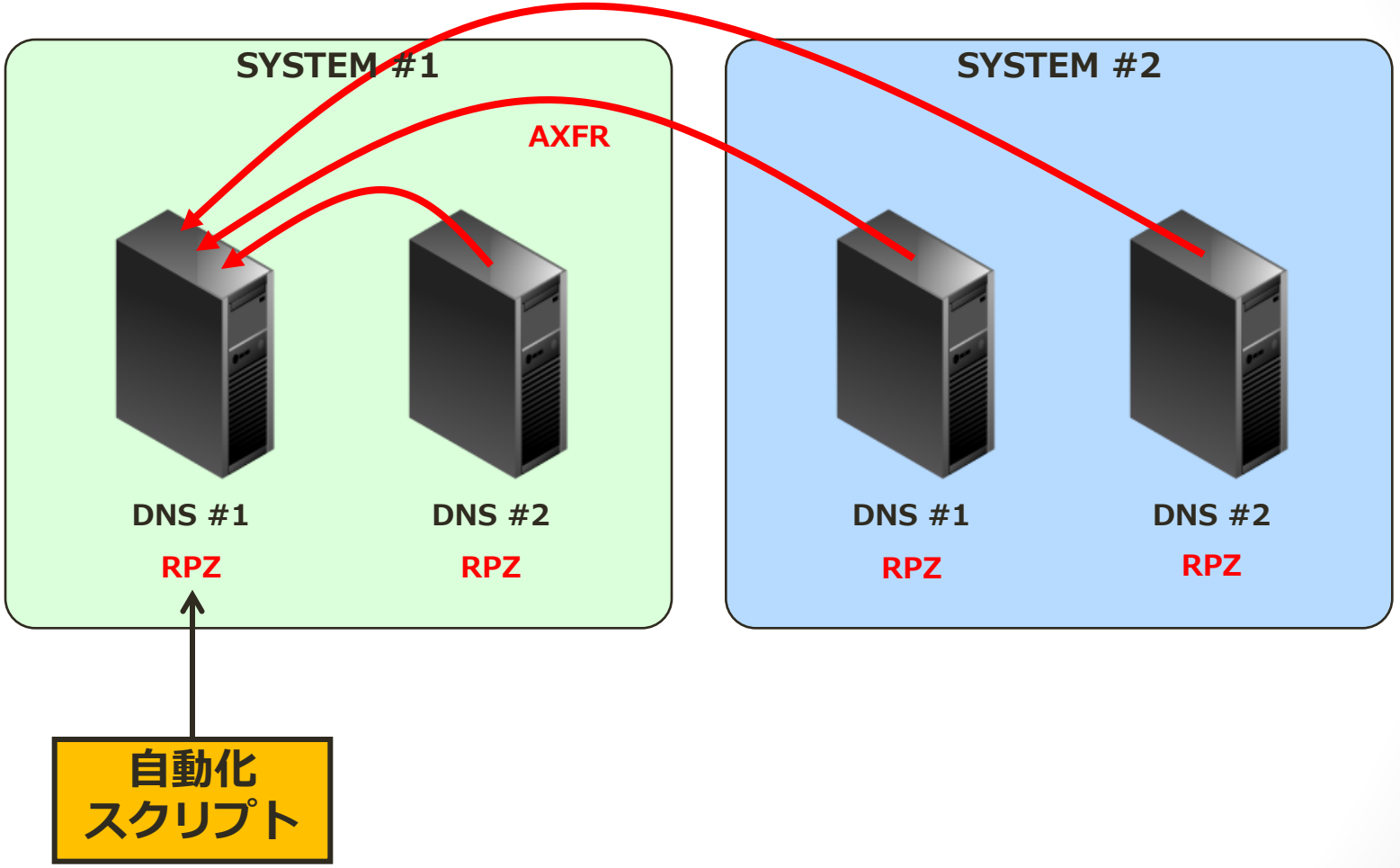
弊社のDNSシステムに一定期間、ゾーン上書き方式とRPZ方式の両方を導入してRPZの実績を作る。

並行運用イメージ



RPZの脆弱性を利用されても
システム全体が落ちない

現行運用イメージ


SYSTEM #1
AXFR
SYSTEM #2
DNS #1
RPZ
DNS #2
RPZ
DNS #1
RPZ
DNS #2
RPZ
自動化
スクリプト

◎RPZ運用の自動化

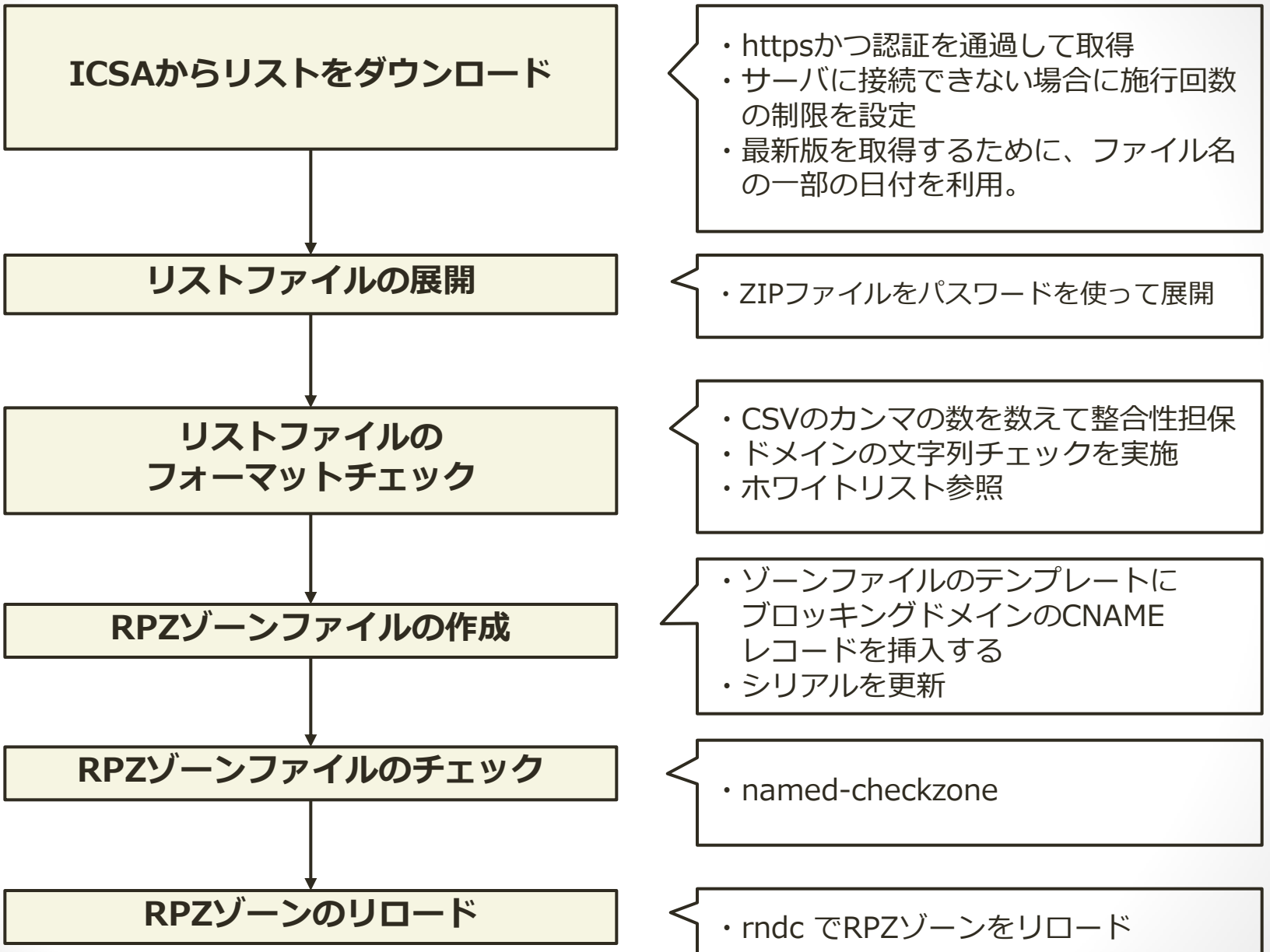
自動化にあたりケアしたところ

- **ICSAからリストが取得できない場合**
  - サーバに接続できない
  - ファイル名が変わった

- **配布されるリストに万が一のミス**
  - ドメインに使用できない文字列
  - ドメインに誤って「.」等のTLD
  - CSVファイルのカラム数などに不整合

これらを想定してスクリプトの開発を実施！

自動化処理の流れ


ICSAからリストをダウンロード
・httpsかつ認証を通過して取得
・サーバに接続できない場合に施行回数の制限を設定
・最新版を取得するために、ファイル名の一部の日付を利用。
リストファイルの展開
・ZIPファイルをパスワードを使って展開
リストファイルの
フォーマットチェック
・CSVのカンマの数を数えて整合性担保
・ドメインの文字列チェックを実施
・ホワイトリスト参照
RPZゾーンファイルの作成
・ゾーンファイルのテンプレートにブロッキングドメインのCNAMEレコードを挿入する
・シリアルを更新
RPZゾーンファイルのチェック
・named-checkzone
RPZゾーンのリロード
・rndc でRPZゾーンをリロード

自動化の運用

- **作成したスクリプトを毎週CRONで実行**
  - ・実行サーバはRPZゾーンを管理するマスターのみ
  - ・実行日はリスト配布日の２日後に設定

  →リストに万が一問題があった場合でも2日間のバッファがあれば感知できるであろう。

- **唯一の手動運用**
  - ・定期的に変更されるリストファイルのパスワードのスクリプトへの適応

  →この先何年も運用する中で自動化機構が実装されていることを忘れてしまわないため。
  （人事異動など）

課題

- **ダイバーシティ構成のDNSシステムに導入しにくい**
  - BIND特有の機能であるためUnboundなどには導入できない。

- **0-Day Attack に弱い**
  - RPZの脆弱性を突かれた場合、システム全体に影響

まとめ

- DNSブロッキングにはゾーン上書き方式とRPZ方式がある。
- 自動化自体は容易で、ポイントさえ押さえておけば比較的安全で運用の手間はほとんどない。
- RPZはダイバーシティ構成のシステムには向かない。
- RPZは現在のところ安定稼働している。

ご清聴ありがとうございました。