Panasonic
ideas for life

バリデーション対応サーバの状況

DNSOPS.JP
2012年4月25日

三洋ITソリューションズ株式会社
SANNET BU
其田　学

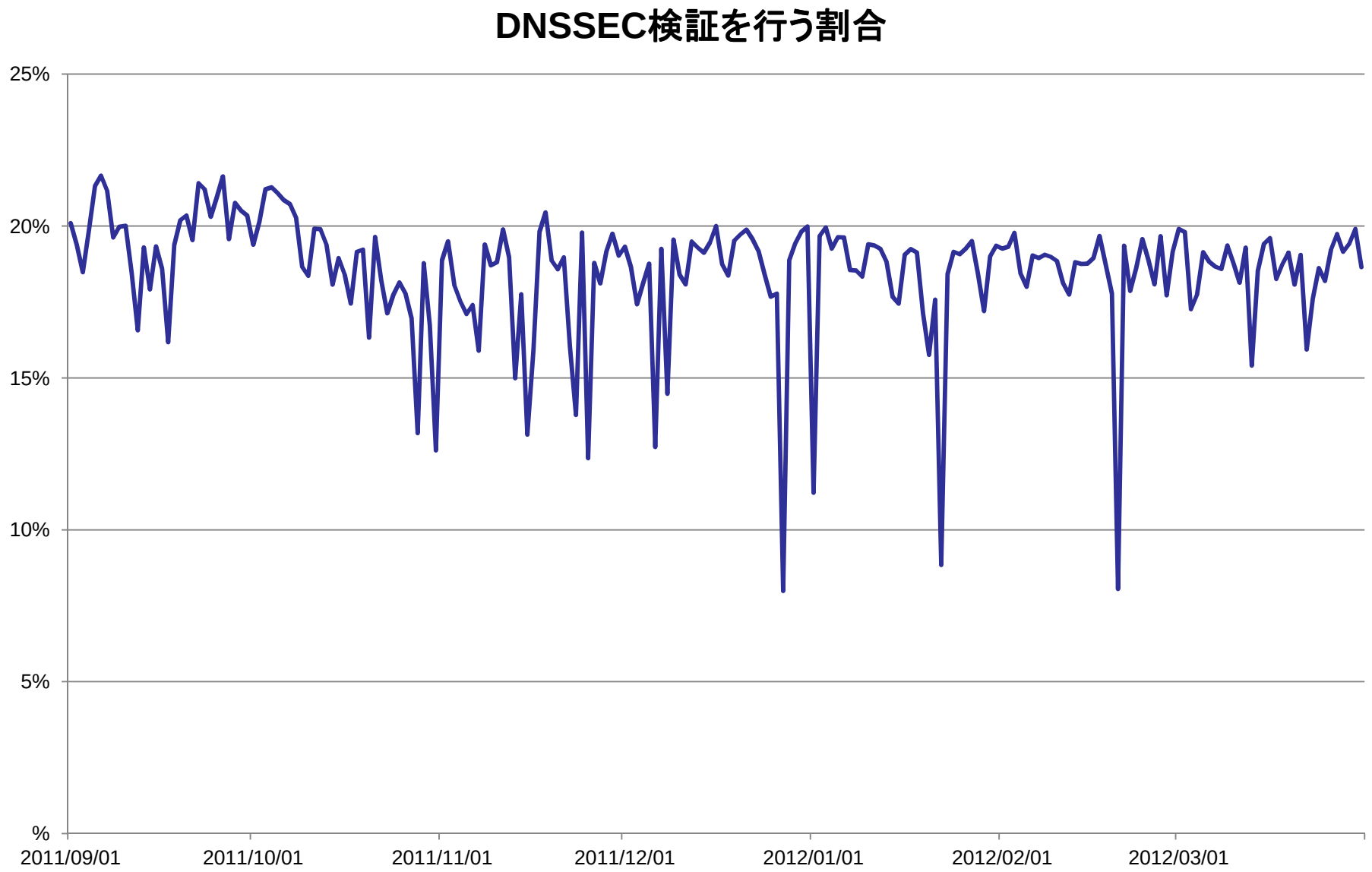
アジェンダ

- DNSSECのバリデーションの状況
- 検証失敗事例
- TLD失敗時の自己防衛策

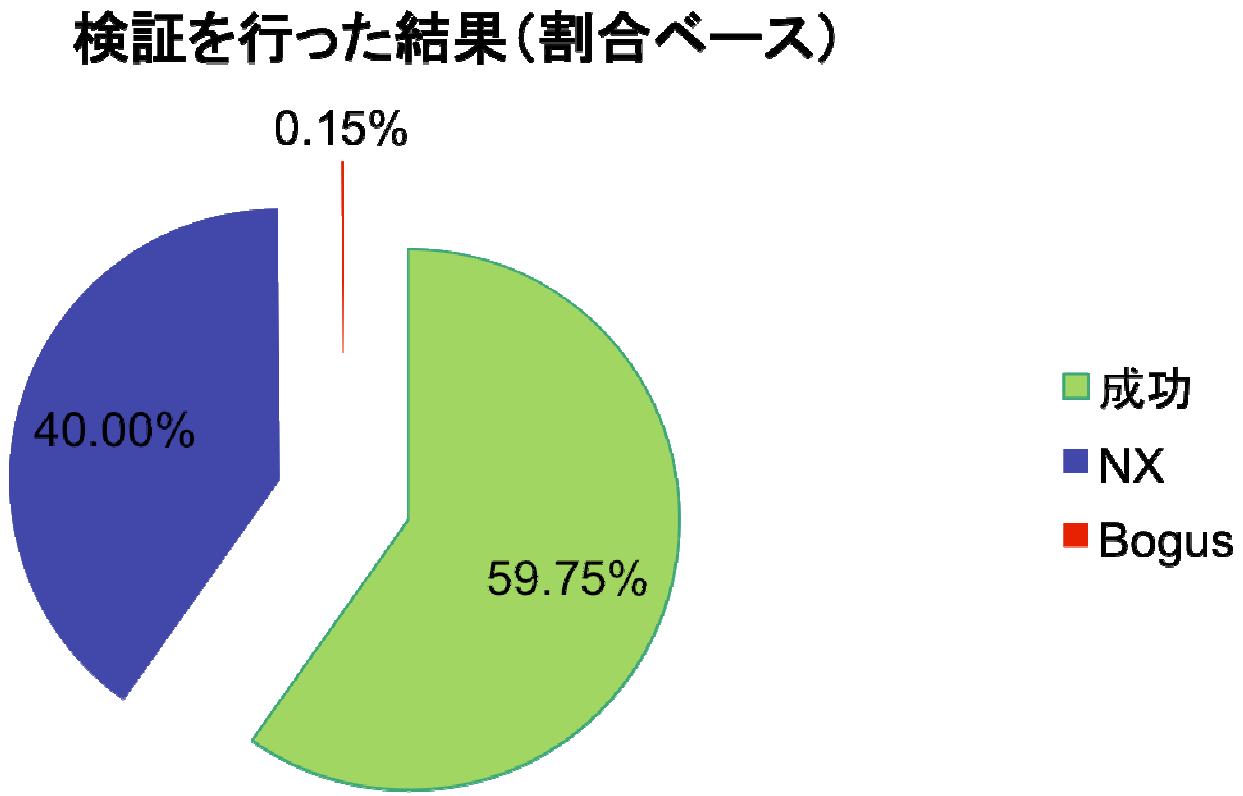
データでみるバリデーションの状況

DNSSECのバリデーションの状況

DNSSEC検証を行う割合の推移（2011年9月1日-2012年3月31日）



DNSSEC検証の状況（2011年9月1日-2012年3月31日）



検証失敗事例

2012年1月25日にこんなメール流しました。

其田@AS4704です。

もし、メール見ておられましたらtus.ac.jp.の
署名更新してほしいです。

```
bash-3.00$ dig tusns.tus.ac.jp.

; <<>> DiG 9.7.2-P2 <<>> tusns.tus.ac.jp.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 9357
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;tusns.tus.ac.jp.               IN      A
```

- サポートセンターにお客様から入電がありHPが見れないとの連絡。
- DNSSEC絡みっぽいと判断
- サポートセンターからエスカレーションを受ける
- 状況確認すると、署名が古いことを確認

- 直接コンタクトが取れないので、とりあえずMLに流してみる。

- Twitterでつぶやいてみる…
  - Orangeさんが反応してくれた♪

- 署名されて解決

この事件以降変更したこと

- ログ収集しているキャッシュサーバにDNSSEC関連のログを吐き出させるように変更

- ログの中からInsecureを除いたbogusログを毎日残すように変更

ときどき面白いログが取れます。

事例2:とある通信事業者の子会社のドメイン

bogusログ中にある.jpドメインは定期的に
チェックしてます。

Nameserverを見て連絡取れる会社だった為、
ご連絡して即日復旧

ROOT/TLDでの事故発生時の自己防衛策

自己防衛策

バリデータ導入したと言うと結構聞かれること

- 「ROOTで失敗したら全滅しますよね」
- 「JPとか鍵更新失敗したりしたら大変ですよね」

すべて引けなくなる訳ではありません。

1.キャッシュに残っているものは大丈夫
2.TLDがキャッシュに入っていれば、そのTLD配下のドメインのうち、DS登録されてないものは大丈夫。
3.DS登録されているものは…残念ながら…

TLDのキャッシュがなくなる前にバリデートを止めれば被害は最小ですみます。

- 各キャッシュDNSサーバ上で5分おきに下記のROOT/TLDをチェック
  - root
  - com
  - net
  - jp

- 検証失敗と判定されると検証を停止


Panasonic
ideas for life