DNSは空気じゃありません
- ほっといても動くと思ってませんか? -

民田雅人 <minmin@jprs.co.jp>
株式会社日本レジストリサービス
2009-01-23 JANOG 23@高知

DNSって何だっけ?

- ドメイン名からIPアドレスを検索する際に利用するインターネットの基盤サービス
  - RFC1034, 1035(なんと1987年11月!)で定義
  - 最近では、SPF、ENUM等、当初の用途以外のサービスにも活用
- ルーティングと並ぶインターネットの

  とても重要な基盤サービスの一つ

Kaminsky Methodの衝撃

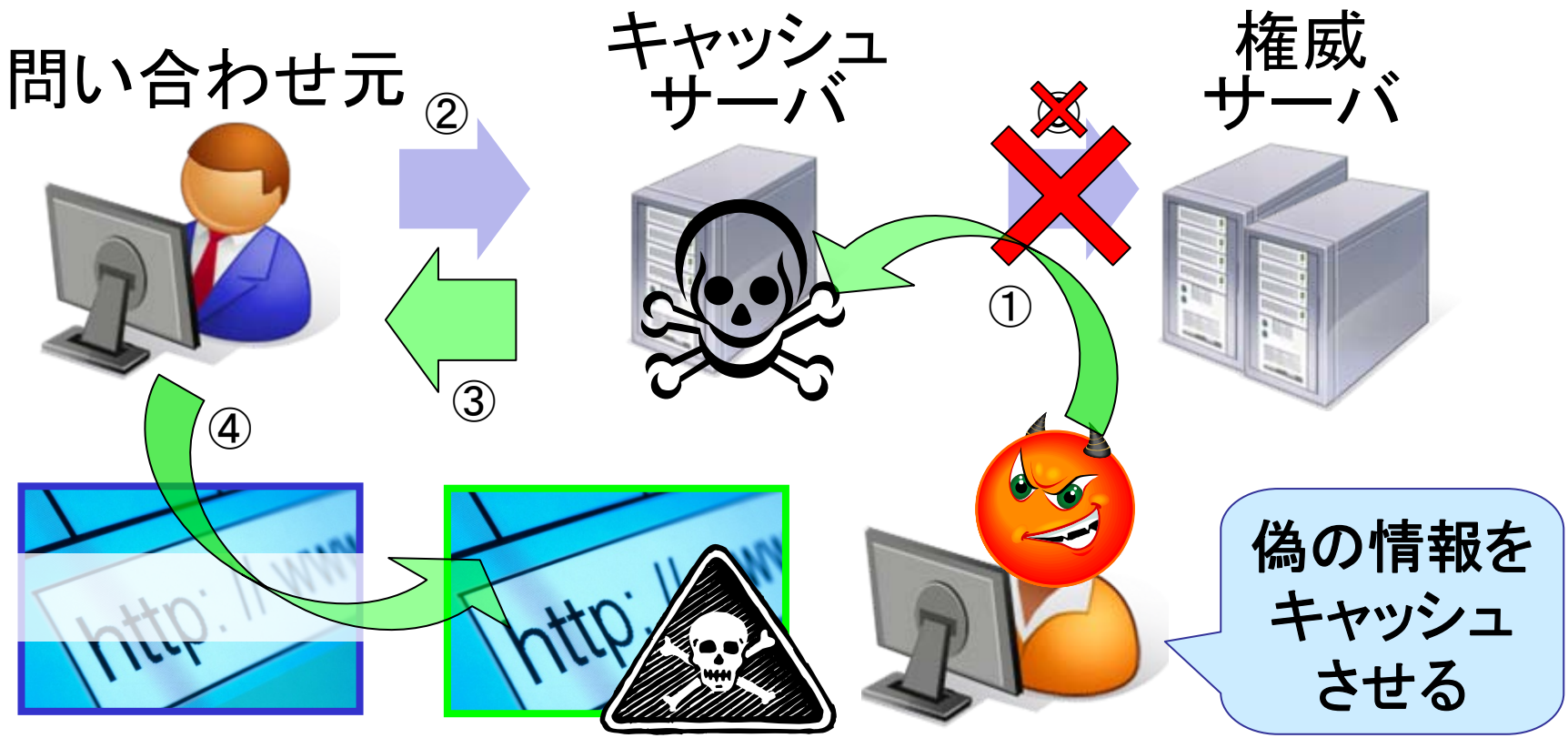
- Dan Kaminsky氏による、新たなキャッシュポイズニング攻撃手法の発見
- 2008-07-09　DNSの脆弱性情報と
  対策パッチ等の公開

  翌8月にKaminsky氏による
  攻撃手法の詳細の公開予定
- 2008-07-23　攻撃手法の漏洩と共に
  攻撃ツールが出回り始める

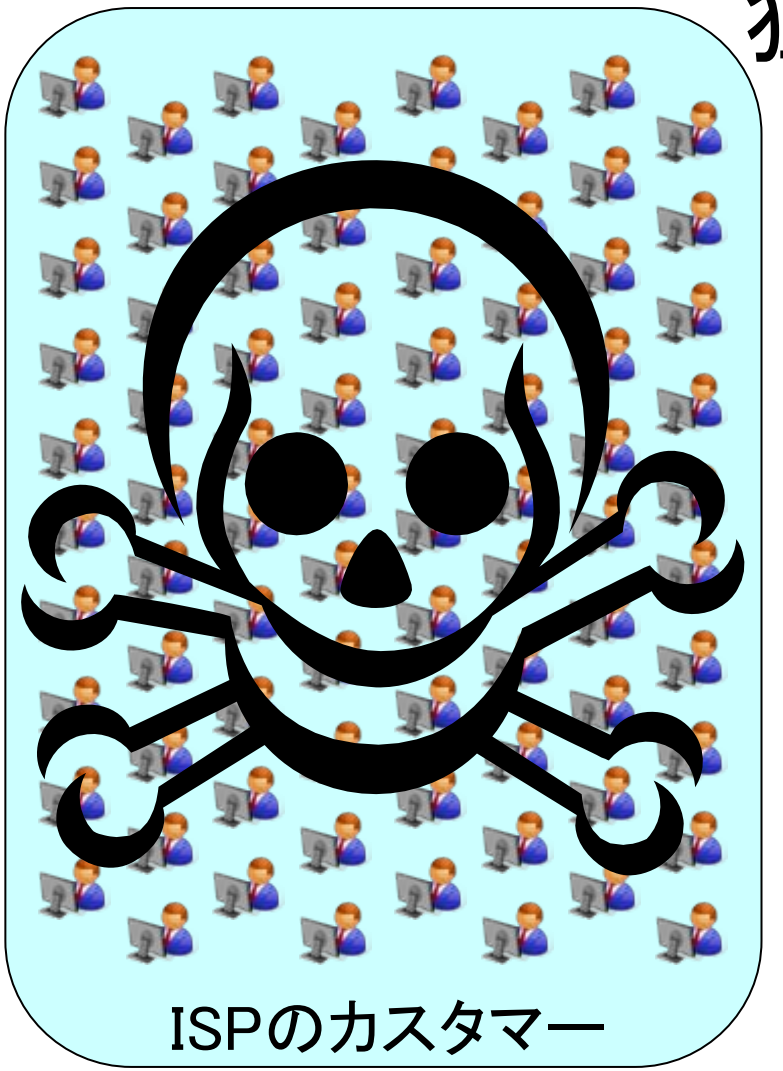
復習: DNSキャッシュポイズニング (キャッシュサーバへの毒入れ)

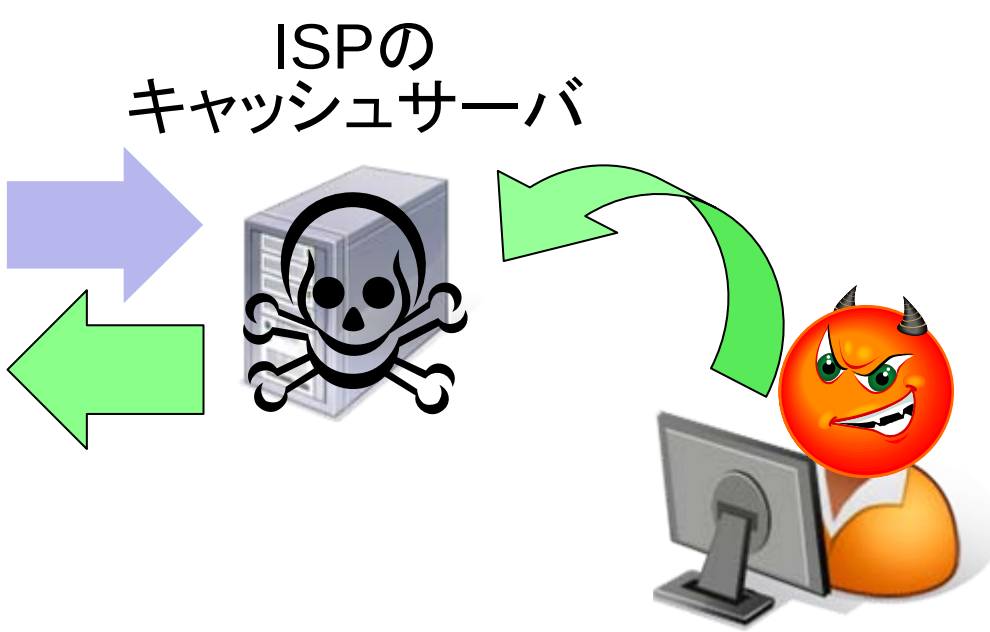
- 予めキャッシュDNSサーバ(以下キャッシュサーバ)に偽の情報を覚えこませ、ユーザが正しいアクセスを行ったつもりでも、偽装サイトへ誘導する手法
  - フィッシング(ファーミング)の為の攻撃手法の一つ

キャッシュサーバへの毒入れ攻撃



もしISPのキャッシュサーバが狙われたら

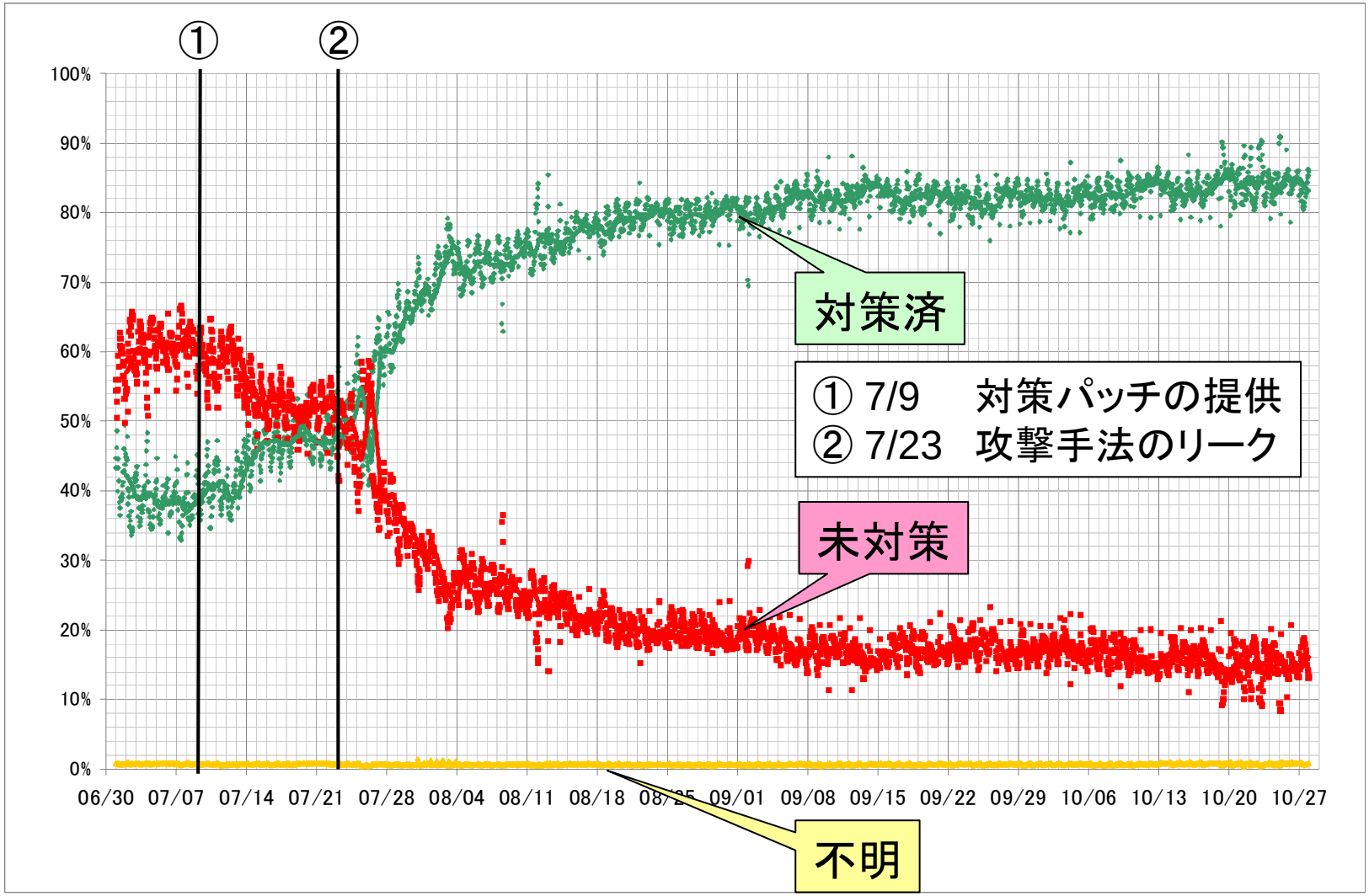




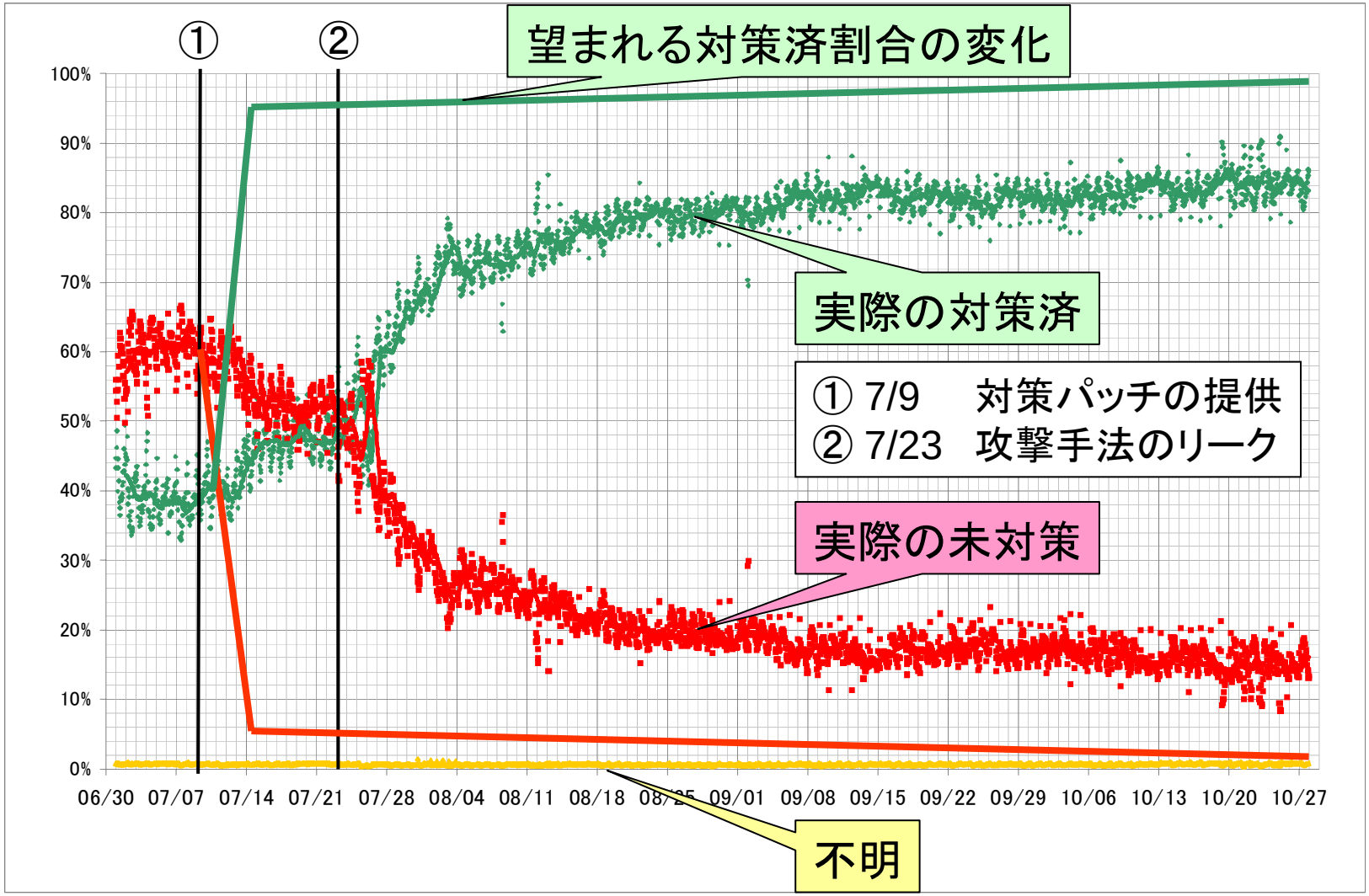
カスタマー全員が
被害を受ける

にも関わらず…

JPRSで観測した対策情況の変化



望まれる対策情況の変化



JANOG 23 初日に聞いた極端な実例
C: お客様　S: サポート

- C: トラブル起きてるでしょう
- S: 問題なく正常に稼働してます
- C: メールこないんですけど
- S: 最近なにか変更されませんでしたか?
- C: 1週間程前に古いサーバ1台捨てました
- C: 停止しても問題発生しなかったので
- S: DNS検索できなくなってますよ
- 捨てられたのは、プライマリDNSサーバ
  - 1週間程してセカンダリでゾーンがexpire

DNSでの対策はなにかと遅い
なぜ?

聞いてみました
ルータ運用 vs DNS運用

複数の組織へ軽くアンケート

運用体制の比較

- ルータ関連
  多くの組織で内部に専任の運用チーム
  - もちろん、複数人で24時間365日体制
- DNS関連
  (言葉は悪いが)片手間で運用されている
  - 専任体制を敷いている組織は稀
  - WEB/メールサーバ担当が兼任
  - 実はルータ担当が兼任(?)
  - 一応(?)、複数人で24時間365日体制

保守契約

- ルータ関連
  - 保守契約が存在する
  - 反対に保守契約がないとどうしようも無い
- DNS関連
  - 有償の実装(含アプライアンス)なら保守契約有
  - フリーウェアだと保守契約無(無くてもなんとか)
  - OS付属の場合、OSの保守契約に含まれる

予算確保

- ルータ関連
  保守の関係もあり、確実に予算を確保
- DNS関連
  DNSとして単独の予算は取らない
  - フリーウェアを使うから不要
  - サーバとしての予算は確保

Security Advisoryへの対応

- ルータ関連
  - 保守契約によりディーラーから連絡を受ける
  - リモートからやられちゃう場合24時間以内に対応
  - ローカルからの場合3日程度で対応
  - フィルターで暫定処置可能なら、しばらく凌ぐ
- DNS関連
  - フリーソフトだと自力でウォッチ
  - ルータと同程度で対応すべきはずのものだが、現実は1ヶ月経過しても多くが未対応

やっぱりDNS運用って
ルータ運用に比べて
虐げられてる?

うーん…

みなさんのDNS運用体制ってどうなってるの?

会場からの意見(1/2)

Aさん: パッチを当てるのが遅いのはなぜかというと、大手ではないところだと、他のところで確認してもらってから当てるというところもある。かもしれない。

みん: ルータでもそうなの?

Bさん: ルータなら早いのに。というものの実態はどうなのか？ISPやキャリアは即座に対応するだろうが、そうじゃないところの対策はどうなのか？大手のISPのキャッシュサーバも遅かったから、そういう結論にしたのですか？

みん: クエリパターンが急に変わった瞬間はある。なので、大手ISPの中でも対応に差がある。

Cさん: ルータの方は冗長されてる。DNSは一瞬でも止めたくないときがある。メンテナンスウィンドウにあわせてしか対応しない。

Dさん: 大量のドメインをDNSで扱っている。そのテストに時間がかかるので、簡単にはバージョンあげられない。ルータに関しては、ルータでも歩調をみてる感じ。

Eさん: 実害は発生したのか？カミンスキアタックも検出できるのでは。

みん: 実害のレポートは有名になった1件のみ。攻撃が起きているというレポートは他にでている。

Fさん: 対策が進まない理由。ルータは保守に入っているが、BINDなどフリーソフトは自分でウォッチしてないと情報が入らない。認識がルーズになる。キャッシュのDNSなら割と気軽(?)に触れるのでは。ロードバランスしているし。

Bさん: いつでもすぐにメンテナンスできる。アプリケーション全般で数限りないセキュリティインシデントがでているはず。保守がないから、という認識では使えないものが増えてしまう。世の中にはセキュリティ情報をだしてくれるサービスはある。公の情報はきちんとまとめてくれている。

会場からの意見(2/2)

Gさん: 監視が重要。気楽に落とせるかが重要。ルータならOSPFでは寄せてあげて寄せてあげてができる。そういう工夫重要。DNS-anycastで構成しているので、すき放題メンテナンスできる。メンテナンスをしやすい仕組みを作るのがいいのでは。

Hさん: あのアドバイザリでは深刻さがわからなかったのでは？よくよく考えて気づいた。

Eさん: BINDフォーラムなどでアドバイザリを先だししてもらえるのだし。ルータの保守に金をだすのなら出してもいいのでは。

Iさん: 顧客との関係。明確に影響範囲がわかってないとだめ。前回のIW2008で、IIJは5月の時点でRandomizationのうわさを聞いて、機器の強化を検討したと言っていた。同様にできないかどうか。

- 会場にDNS-OPSのML加入を問い合わせてみると役半数の手があがる。

Bさん: どういうチャネルで情報を手に入れるかだが、長年やってると伝手がある。ちゃんと情報をウォッチしていれば、狼少年ではないことがわかったんじゃないか。意識のギャップがある。なんとかしないといけない。

Hさん: 存在しない名前でやると聞いてピンときた。当初のAdvisoryのときはBINDのキャンペーンかと思った。

Jさん: コンテンツサーバ・権威サーバはお金もらえるので担当がはっきりしている。キャッシュサーバは空気みたいな存在で、キャッシュサーバ運用してるのだれだっけ？まさに担当者不在系。

まとめ

- 繰り返しになりますが…

  DNSはインターネットの重要基盤サービスの一つ
  - 決して空気みたいなものではなく、適正なメンテナンスを必要とするもの
  - ほっといたらある日突然動かなくなるかも
- あらためてDNS運用に目を向けてください
  - ルーティングばっかりに目を向けないでね☺

おしまい

本プログラム作成にあたって
以下の方々に感謝します

松下 和弘さん　西塚 要さん
JANOG 23プログラム委員の皆様