DNS運用の現実

民田雅人
株式会社日本レジストリサービス
2011-11-30 DNS DAY
Internet Week 2011

DNSとは

- ドメイン名をIPアドレスなどのレコードに変換するマッピングシステム
- ドメイン名で通信する限り、インターネットアクセスの際に必ず利用される
- ルーティングと並ぶインターネットにおける**極めて重要な基盤サービス**

① www.example.jpのIPアドレス?

② www.example.jp = 192.0.2.10

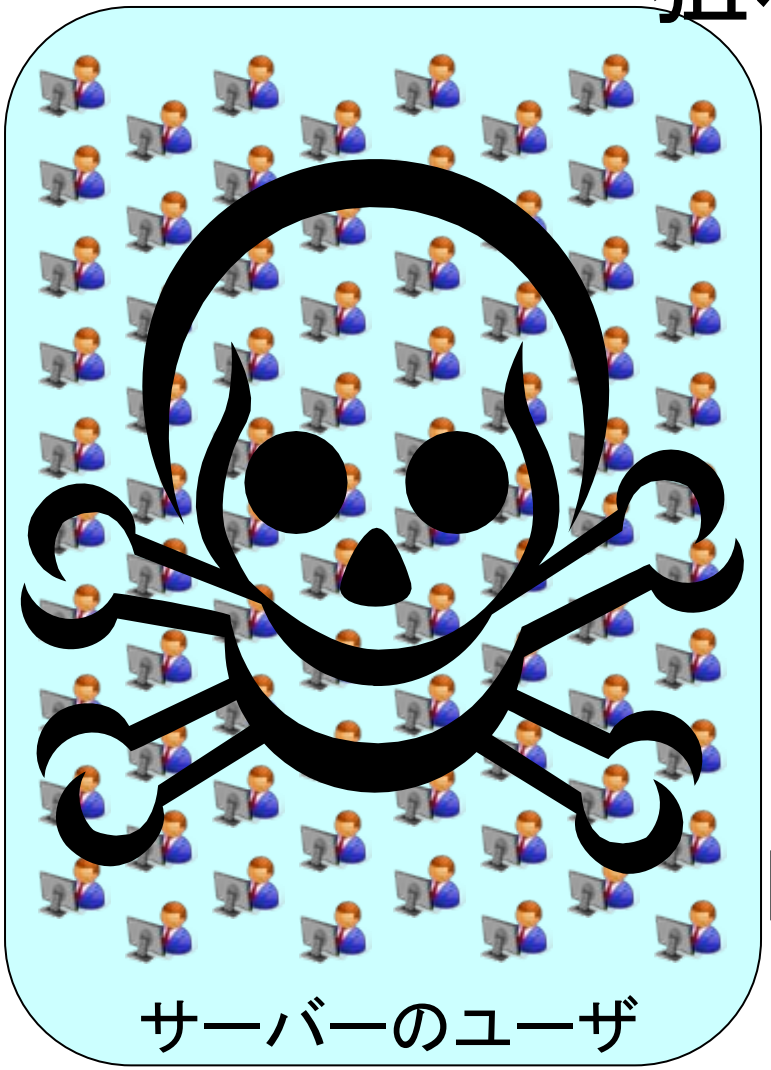
DNS
サーバー

2008年夏
Kaminsky型攻撃手法

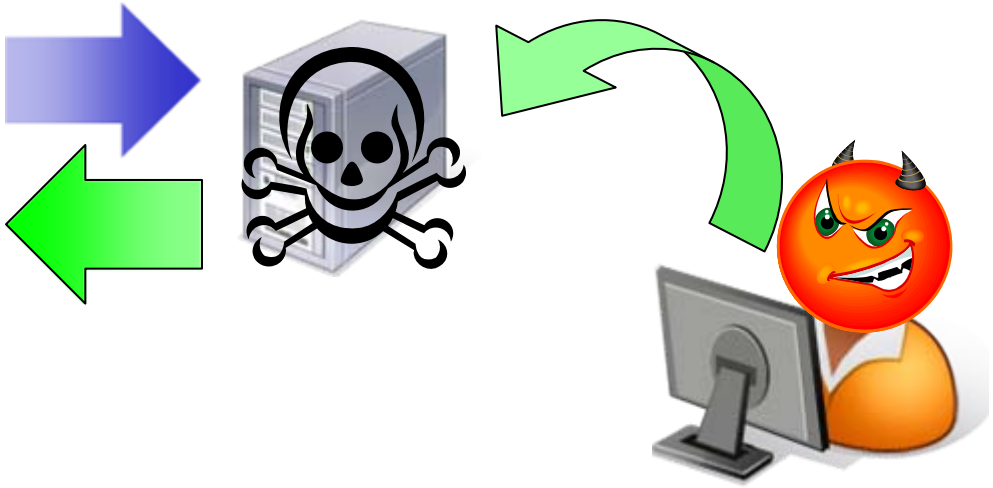
2008年夏の出来事

- Dan Kaminsky氏によるキャッシュDNSサーバーへの新たなる毒入れ攻撃手法の発見
- DNSの脆弱性情報とキャッシュDNSサーバーの問合せポート番号を可変にする対策パッチ等の公開 (2008-07-09)
  - ポート番号をランダムに変化させることで、攻撃成功確率を1/65000程度に低減する

キャッシュDNSサーバーが狙われたら



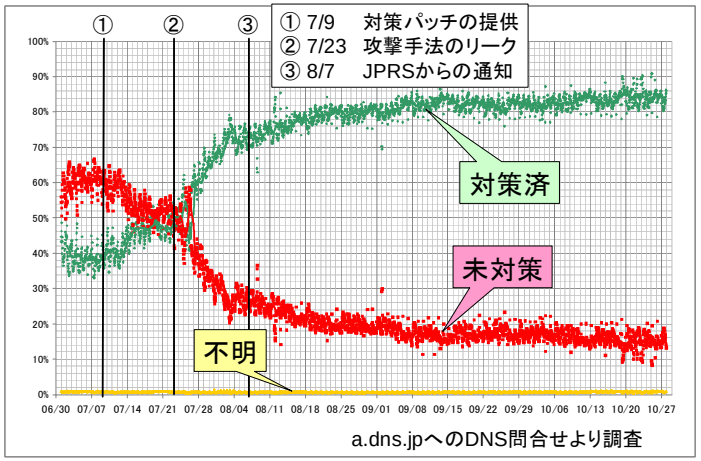
キャッシュDNSサーバー

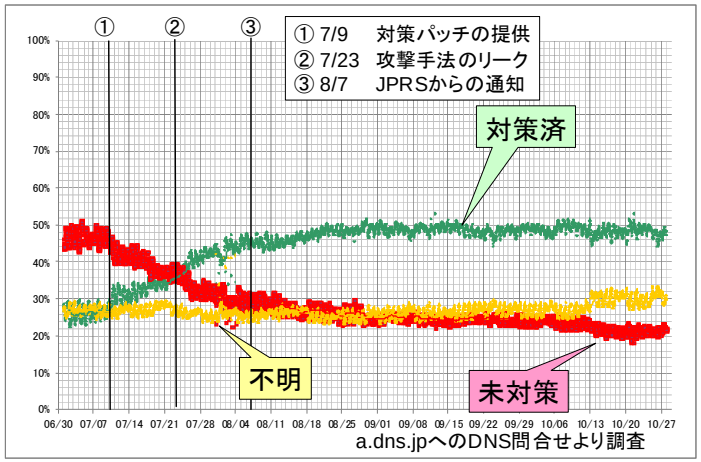


同じサーバーのユーザ全員が被害を受ける

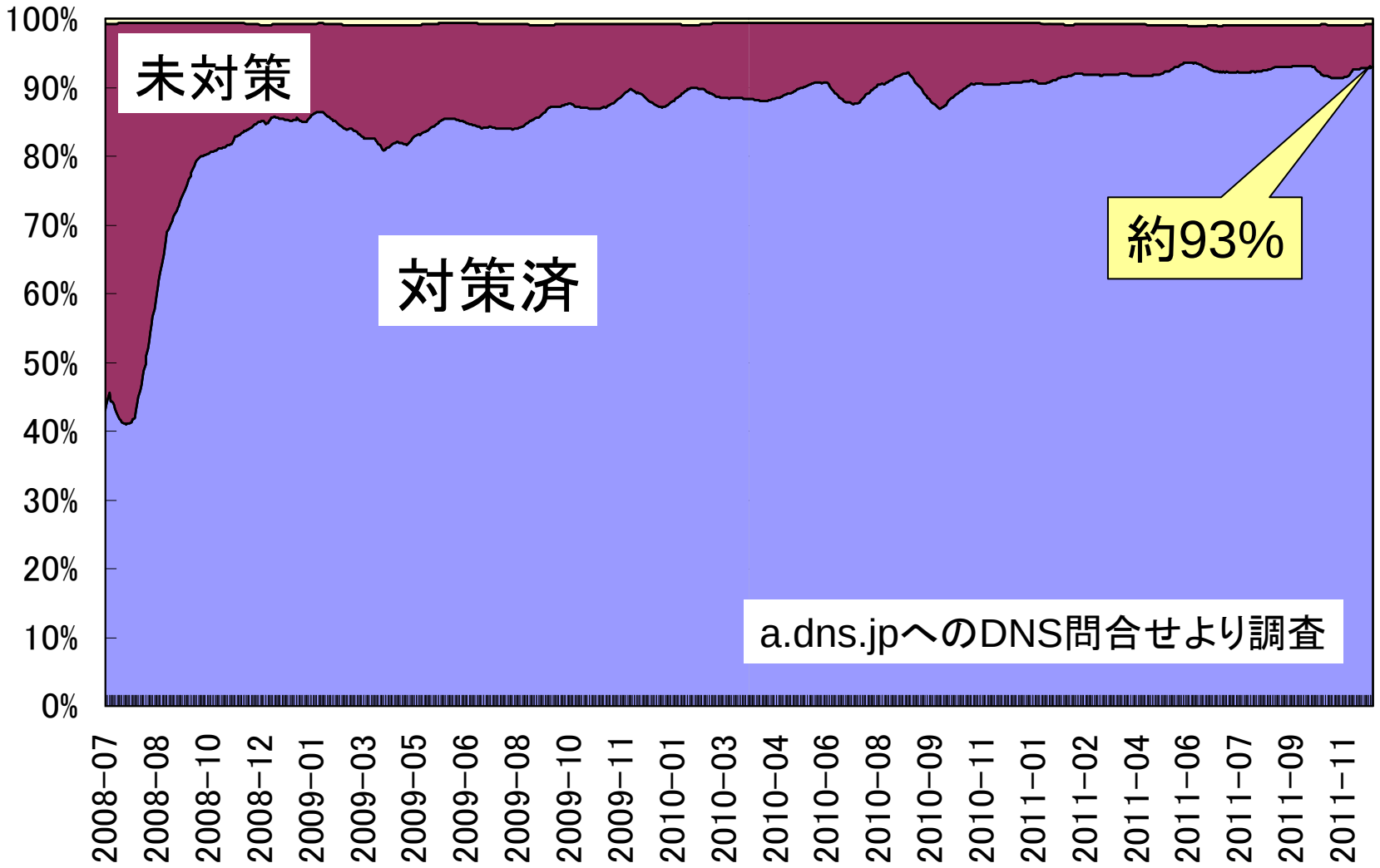
対策状況の変化 (1)
当時の状況

- 調査方法
  単位時間内に同じIPアドレスからのDNS問合せのソースポートが変化するかどうか
- 2008年10月末の対策済みの割合
  - 問合せ数 (グラフ上)
    約85%
  - IPアドレス数 (グラフ下)
    約48%

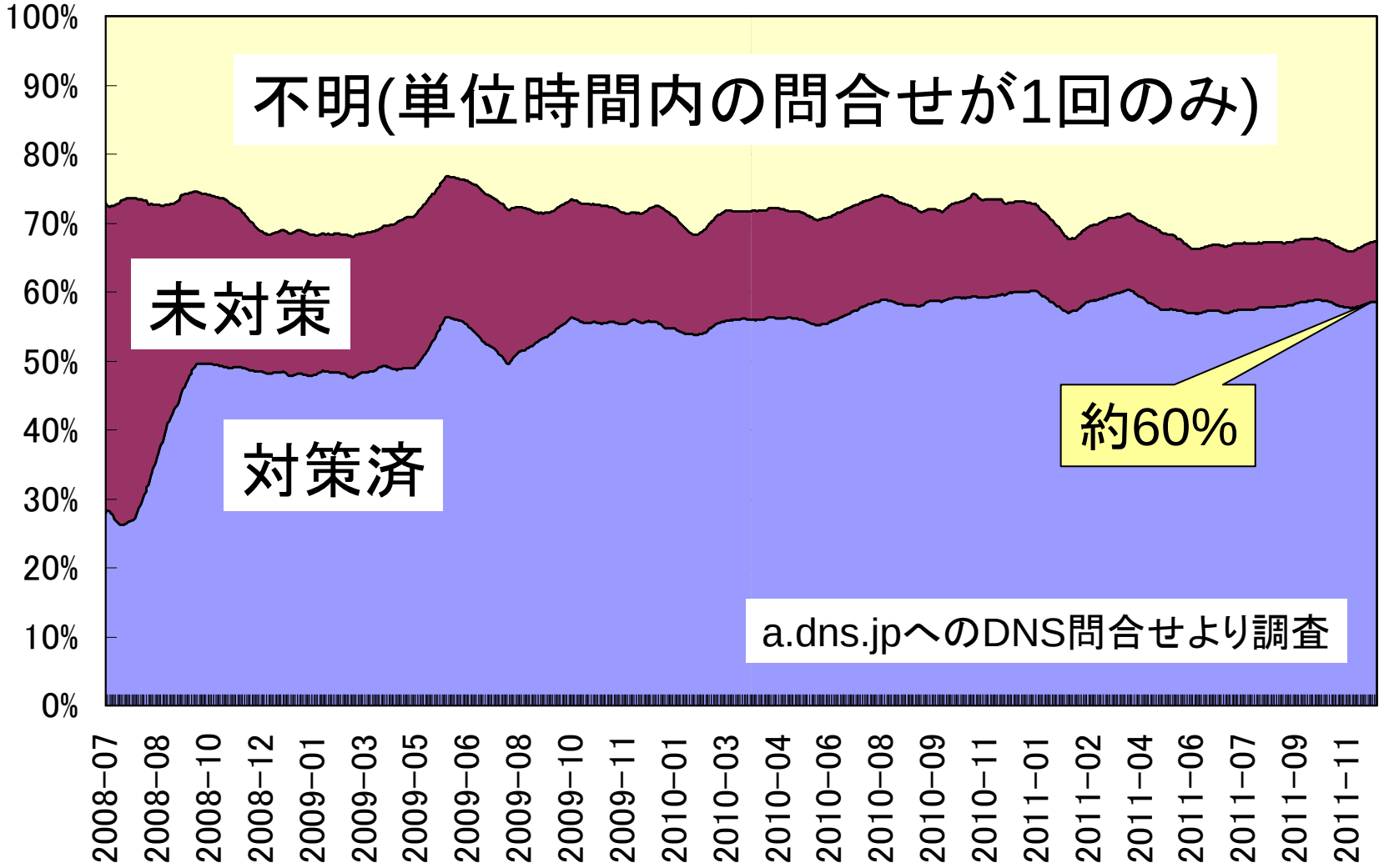




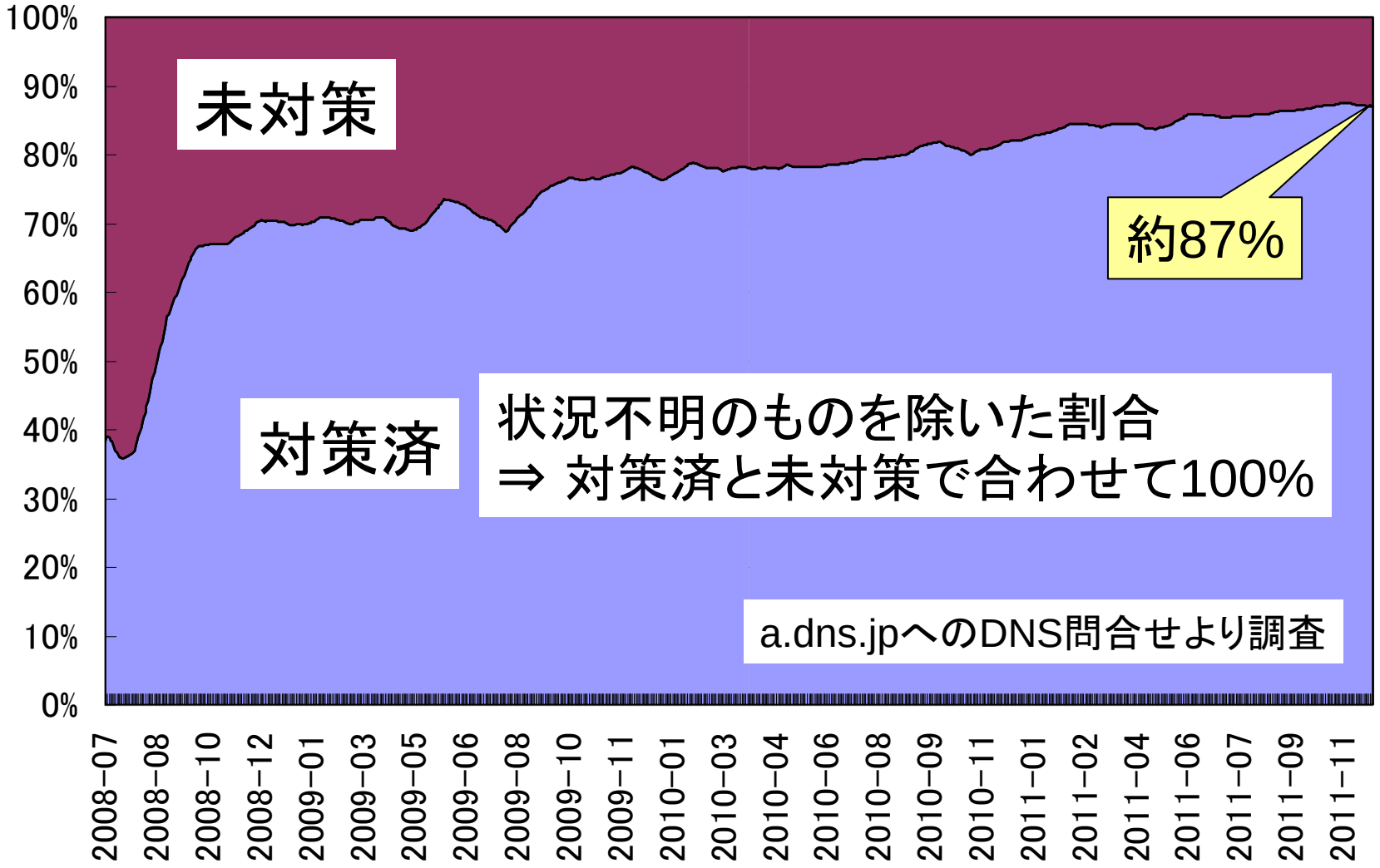
対策状況の変化 (2)
問合せ数に対する割合



対策状況の変化 (3)
IPアドレス数に対する割合 (1/2)



対策状況の変化 (4)
IPアドレス数に対する割合 (2/2)



2011年11月の状況

- 2008年10月当時に比べ徐々に改善
  - パッチをあてたものが増えたのか
  - サーバー機器の更新が行われたのか
- IPアドレス数で明らかに未対策が**10%**程度
  - ホスト数に換算すると、調査対象範囲で9万台程度存在する
  - 未対策のサーバは、その後発見された脆弱性に対しても未対策のままである可能性が高い

2011年夏
BIND 9.xへの脆弱性
(CVE-2011-2464)

CVE-2011-2464

- BIND 9がリモートからDoS攻撃を受ける
  - あるパケットを受けるとnamedが落ちる
  - 回避策は無く、バージョンアップのみ
- 7/5 ISCから情報公開
  JPRSからも情報を公開し注意喚起
  - ISCは本脆弱性の深刻度を**High**と評価

CVE-2011-2464情報公開後

- 一部の声「一般には**Middle**レベルで、**High**だと言われても何をしていいかわからない」
  - DNSサーバが**リモートからの攻撃で落ち**、しかも**一時回避策が存在しない**
- DNS屋(?)と他が感じる危険度の差異
  - DNSサーバが停止する
    ⇒ インターネットの基盤サービスが停止する
    ⇒ 極めて多くの人に影響を与える深刻な事象
  - そう思わない(気がつかない?)人も多い

DNSサーバーの現実

DNSサーバのシェア

2011年8月現在 JPRS調査

実装	ホスト数	割合
BIND 9	43539	40%
BIND 8	1779	2%
BIND 4	59	0%
Microsoft DNS	1041	1%
その他	426	0%
不明	63377	57%

調査対象台数 約11万台

BIND 9での割合

- BIND 9のうち
  - BIND 9.2 まで　　約33%
  - BIND 9.3　　約50%
  - BIND 9.4 - 9.5　　約　6%
  - BIND 9.6　　約　5%
  - BIND 9.7 - 9.8　　約　6%
- 古いBIND 9が、まだ数多く利用されている

古い実装が使われ続ける訳

- OSの標準で付属のものをそのまま採用
  - 例えば、RedHat Enterprise Linuxのバージョン5.xや、Solaris 10のBIND 9は9.3系
  - 新しい脆弱性の修正はベンダーがサポート
    ⇒ しかし新しい機能は導入されない
- 設定した人が去り、そのままになる
  - OSごと古い設定がそのまま使い続けられる
- その他

極端な実例
C: お客様　S: サポート

C: 何かトラブル起きてませんか?

S: 当社のネットワークに問題は起きていません

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
　　停止しても問題発生しなかったので…

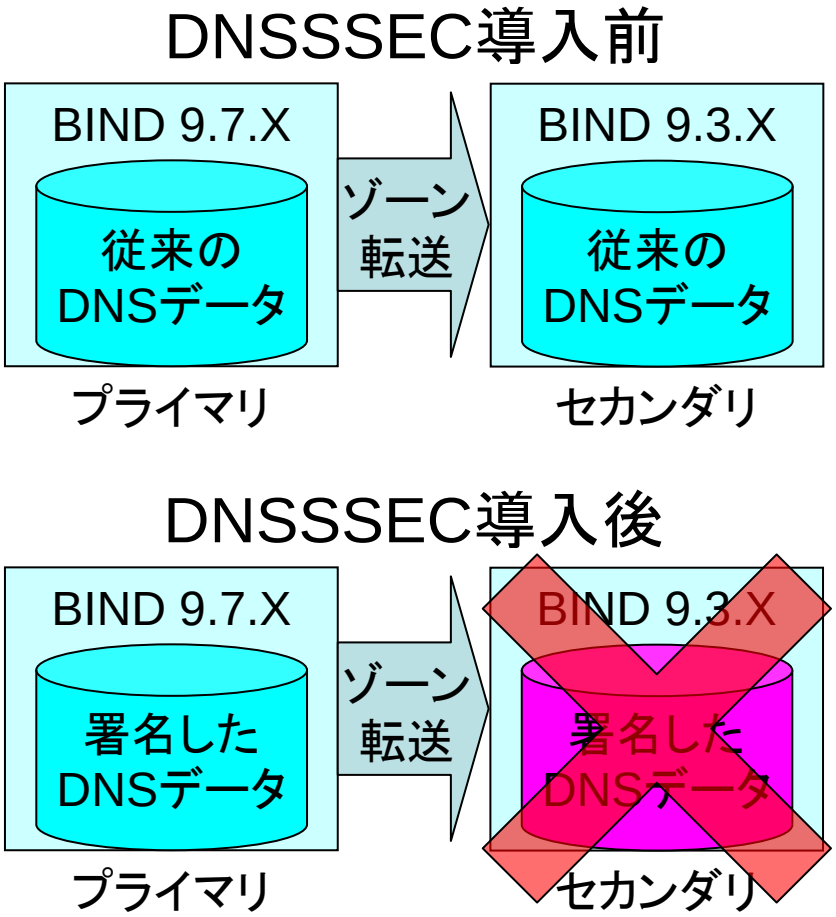
S: DNS検索できなくなってますよ

- 捨てられたのは、プライマリDNSサーバ
  - 1週間経過しセカンダリ側でゾーンがexpire

古いBIND 9の問題点

- 機能面での不具合が改善されない
- DNSSECに追従できない
  - ~ 9.2　現在のDNSSECそのものが未実装
  - ~ 9.3　dnssec-enableのデフォルトが ”no”
  - ~ 9.5　NSEC3方式を未実装
  - ~ 9.6.1　RSASHA256/RSASHA512を未実装
  - 自ドメイン名をDNSSEC対応しなくても、セカンダリサーバで注意が必要

DNSSEC導入時のありがちなトラブル



- DNSSEC導入前
  セカンダリ側のBIND 9のバージョンが古くても問題無し
- DNSSEC導入後
  セカンダリ側のBIND 9のバージョンが古いと署名データを正しく扱えず、DNSSEC対応クライアントが署名検証に失敗する
  - それぞれのサーバーの管理主体が違う場合に発生しやすい

まとめ

- 古い実装がいつまでも使い続けられ、そのままになる現実
  - DNSに限らない
- DNSSEC時代のDNSサーバは、新しい実装を使うことが必須とされる
  - OS付属では間に合わない可能性が高い

jPRS
JAPAN REGISTRY SERVICES