C2:DNS DAY

～DNSにおけるセキュリティ再考～

開催報告

DNSOPS.JP

石田慶樹

DNS DAY概要

- **日　時**：12月6日(水) 15:00-18:00
- **場　所**：パシフィコ横浜　小ホール
- **主　催**：
  日本ネットワークインフォメーションセンター
- **プログラム策定協力**：DNSOPS.JP
- **参加者数**：240名

DNS DAY

[**前半**] DNS updates

1. JP-DNS report

   白井 出 [**株式会社日本レジストリサービス**]

2. root DNS report

   関谷 勇司 [WIDEプロジェクト]

3. DNS**最新トピック**
   - AS112 report

     吉村 知夏 [NTTコミュニケーションズ株式会社]
   - **逆引き**DNS lame report

     小山 祐司 [JPNIC]
   - DNS･**ドメインに関する世界的な政策動向**

     宇井 隆晴 [**株式会社日本レジストリサービス**]
     川端 宏生 [JPNIC]

DNS DAY

[後半] DNSにおけるセキュリティ再考

1. コンテンツデータ肥大化の問題とその対応
   伊藤 高一 [株式会社インターネット総合研究所]
   森 拓也 [住商情報システム株式会社]
2. DNSプロトコルの落とし穴
   - DNS reflector attack
     松崎 吉伸 [株式会社インターネットイニシアティブ]
   - DNSレコードのTTLを短くすることのリスク
     民田 雅人 [株式会社日本レジストリサービス

DNOPS.JP BoF

DNS 今年のトピック

2006/ 1 JP DNS **不適切な**DNS**サーバ**(Lame Delegation) **の設定削除**

2006/ 1 **「日本**ENUM**トライアル」用番号登録を開始** (1.8.e164.arpa)

2006/ 4 JP DNS BIND9**化と更新間隔の短縮**

2006/ 6 DNSOPS.JP**の発足**

2006/ 6 ip6.int**の逆引きゾーン廃止**

2006/11 SOA MNAME**の変更**

2006/12 DNS DAY/DNSOPS.JP BoF

- **全般的に**
  - DNS reflector attacks**の流行**
  - DNS Cache Server Poisoning**の事例発生**

DNS DAY 内容紹介(1/5)

DNS updates

JP-DNS report　　白井 出 [株式会社日本レジストリサービス]

root DNS report　　関谷 勇司 [WIDEプロジェクト]

- JPルートサーバのBIND9化
- JP ゾーンの更新間隔の短縮　24時間から15分へ
- Anycastの効果の測定

DNS DAY 内容紹介(2/5)

DNS最新トピック

AS112 report　　吉村 知夏 [NTTコミュニケーションズ株式会社]

- プライベートアドレスの逆引きに答えるサーバの状況
- クエリの量は逆引きの中の20%(全体の約4%)
- Dynamic Updateによりホスト名が外部に流失するケースも
- AS112がないのが理想

Lame delegationの改善に関するポリシーの実装案

小山 祐司 [JPNIC]

- 逆引きのLameはJPNICのゾーン委任の中で10%前後
- 長期間解消しないLameについては手順を踏んで委任を停止

DNS DAY 内容紹介(3/5)

DNS最新トピック

DNS・ドメインに関する世界的な政策動向

宇井 隆晴 [株式会社日本レジストリサービス]
川端 宏生 [JPNIC]

どのようにポリシーが決まるかの解説

「.日本」のようにTLDにIDNをいれるかを2007年末までに検討

2008年に開始されるわけではない

逆引きポリシーの策定プロセスについて紹介

DNS DAY 内容紹介(4/5)

DNSにおけるセキュリティ再考

コンテンツデータ肥大化の問題とその対応

伊藤 高一 [株式会社インターネット総合研究所]
森 拓也 [住商情報システム株式会社]

- DNSのコンテンツの肥大化 (IPv6、SPAM対策、電話番号、DNSSEC等)
- DNSには512オクテットの壁
- EDNS0やTCPを使わざるを得ないケースが出現
- EDNS0やTCPが使えるようになっているかは微妙
- TCPも使えるようにすべき(should)

DNS DAY 内容紹介(5/5)

DNSプロトコルの落とし穴

DNS reflector attack　松崎 吉伸 [株式会社インターネットイニシアティブ]

- DNS reflector attack(アンプアタック)は断続的に発生
- オープンキャッシュサーバは直ちに停止すべき
- 必要なアドレス範囲にだけ提供する
- Source Address Validationも実装すべき

DNSレコードのTTLを短くすることのリスク　民田 雅人 [株式会社日本レジストリサービス]

- ある攻撃手法によりキャッシュサーバに毒入れが可能
- TTLが短いコンテンツではかなり想像している以上に容易
- このような攻撃の検出は必ずしも容易ではない
- 事例の発生の状況証拠はあるが本当にこれによるものかは不明
- 対策はSource Address Validation

DNSOPS.JP BoF

2006/12/6 18:30-20:30

at **パシフィコ横浜**301

Agenda

- DNSOPS.JPステータスレポート
- アンプアタックについて
- サイバー攻撃対応演習について
- DNSSECのディプロイメントのための課題
- TCP53問題
- Windows VISTA問題

DNSOPS.JPとは

- DNS運用者のコミュニティ作りのために2006年6月に設立
- MLでの議論およびBoFの開催
- 現在の登録者数1100名超
- 今回のBoFの参加者は80名以上
- 世話役として幹事会と事務局が存在
- http://dnsops.jp/

DNSOPS.JP BoFの内容

- アンプアタックについて
  - コンテンツの肥大に伴いコンテンツサーバ側もリスク
  - Source Address Validationは必須
  - 実現には越えるべき障壁が存在
- サイバー攻撃対応演習が実施
  - 主要なISP間
  - ISP間の連絡体制の整備が課題
- DNSSECディプロイのために
  - サーバの負荷
  - ネットワーク負荷
  - パケットサイズの増加

DNS関連イベントのまとめ

- コンテンツサイズの増大が問題という共通認識とEDNS0, TCPの利用への課題
- DNSを多少なりとも安全に使うためにSource Address Validationを実装すべし
- DNSは終わっているという人もいるがDNSへの依存度は相変わらず非常に高い
- それにも関わらず日陰の存在

Internet 2.0とは?

- Internetに2.0はありえない
  - もう、新たに“何とか2.0”というBuzz Wordを使うのは止めませんか?
  - という、冗談は止めて (半分本気)
  - そもそも“Internet”もしくは“Internet Protocol(IP)”とは網と網を接続したもの／接続するプロトコル
  - 網(企業ネット、個人、NGN、モバイル)と網(々)を相互接続したもの＝Inter+Net
  - したがって、Internetとは本来はメタな系なんだから、メタな系にバージョンはそぐわない

DNS 2.0

- DNS 2.0に向けた課題
  - AAAAレコードのroot zoneへの追加
  - DNSSECによるroot zoneの署名
  - Lame Delegationの根絶
  - Domain Name Hijackingの防止
  - セキュリティ対策

DNS 1.0

⇒すべてを解決できれば、~~DNS 2.0~~

DNS 2.0?

- もしDNS 2.0があるとすると
  - DNS 2.0とは
    - 新サービス／新アプリケーションに適したDNSに替わる広域分散データベースの開発
  - NGNではDNSはOut of SCOPE
    - Routingも考慮対象外
  - 検討すべきいろいろな要素
    - UDPを使い続けるのか？
    - コンテンツのリッチ化
    - P2P
    - コンテンツサーバとキャッシュサーバの分離
    - 強力なセキュリティ機能

- 技術屋が正義に「勝とう」なんて思ったら、これはもうすばやく立ち回るしかないんだけれど、技術の継承がきちんと行われないと、たぶん技術系の負けは確定。
- 技術屋には、それが生まれてから一般化するまでの第一世代と、それが一般化したあと、「洗練の競争」を勝ち抜いてきた第二世代とがいる。
- この道具はなぜこの形をしているのか。これを変えたときに何がおきるのか。
- そういう逸話を伝えられるのは、第一世代の技術者の特権。
- 第二世代の人達も、もちろん師匠からそういう 話を聞かされただろうけれど、技術はもう完成しているし、舗装されていない道なんかより高速道路のほうが早い。そんなヨタ話に耳を傾けていては競争に勝ち抜けないから、みんなムダというものがない。

「レジデント初期研修用資料　個人的なメモ」より
http://medt00lz.s59.xrea.com/blog/archives/2006/11/post_418.html