Internet Week 2007 C2 : DNS Day **パネルディスカッション**

DNS 運用管理者の苦悩

MKIネットワーク・ソリューションズ株式会社
iDCマネジメント部 技術グループ
Ryoko ‘maro’ NAKANISHI

今回お話しする帽子

- 普段はデータセンター事業者/ホスティング事業者ですが、今日は企業相手のDNS管理者の帽子です。
- 『エンタープライズの運用事例を話して下さい』と、チェアに頼まれたけど、このサービスについてはあんまり面白い事例が無いので、プレゼンの後半は運用に関する話に変わっちゃった。(w
  - ごめんね、米谷さん。

DNSアウトソースサービスの内容

- 企業さんのDNS (Primary/secondary) を預かって管理/運用の代行をする
  - 企業さんの1つのサーバとして預かる事もあれば、
  - レコードだけ貰って弊社のDNSサーバに設定する事もある
  - 一応、ドメイン名の管理もする

外部と内部の DNS

- 外部 DNS
  - F/Wの DMZ 側に置く
  - 一般的なネームサーバ。レジストラに登録する DNS はこれ。
  - グローバルなIPアドレスとホスト名の紐付けを行っている
- 内部DNS
  - F/Wの Internal 側に置く
  - プライベートIPアドレスとホスト名の紐付けを行う
  - ユーザは当然、F/Wの内側の人
- 運用上の注意
  - 片方のみのDNSの設定変更は不整合を生む

企業 DNS 運用管理における最近の悩み

- 企業の合併、統合、分割、買収で情報がよれる
  - ドメインを変えたりサブドメインを切ってみたり・・・
  - 拠点をVPNで繋いだけどDNSの設定変更が微妙に間違ってたり・・・
  - それぞれの拠点(や、元違う会社)F/Wのポリシーが統一されてなかったり・・・
  - 関係会社が裏で一緒のDNS使ってるけど経路はバラバラだったり・・・
  - やたらDNSが増えたり・・・
  - レコードが増えたり・・・でもサーバは同じだったり・・・
- そもそも顧客が技術や概念を理解してない
  - 新規契約で顧客のDNSを預かってみたらBINDのバージョンが奇跡的に古いなんて事は日常茶飯事
  - CNAMEだなんだってもう、お手上げ

DNS の良いところ

- DNSの運用負荷は少ない
  - ちゃんとお金は取れてるらしい。
  - でも障害が発生すると影響はでかいという諸刃の剣つき。(後述)
- 管理が分散されている
  - 「ココはオイラね。」「そっちは上位のISP」「ココから下はあんた達がんばって」が成立する
  - Primary/Secondary がちゃんとみんな存在する。
    - だから厄介なときもある。(後述)
- (良くも悪くも)BIND の一人勝ち

DNS の悪いところ

- 障害の復旧に時間が掛かる
  - サーバの移設時に前のレジストラやISPが古い情報を残してくれたままだったりするとメールの受信が出来なかったり色々面倒
  - キャッシュとかがあるので、障害を復旧しても完全な環境復旧までに時間がかかる。その間、顧客が怒鳴ってくる。
- 障害が発生すると被害が大きい
  - 良くも悪くも The Internet と人を繋ぐインフラなので何でもかんでも出来なくなる。やっぱり顧客は怒鳴る。
- だれかれ構わず答える。
- しかも直ぐ毒を飲み込む
  - 実装に問題がある。でもその緩い地盤の上に The Internet は牙城を築いてしまったので今更どうする事も出来ない感じ

DNS運用管理の対策 (と、心構え)

- 脚光は浴びない。脚光を浴びることを期待しない
- 被害はでかいので傷を負いたくなければ慎重に
- わからないやつに任せない。
- 対応しても効果が現れるには時間が必要、それを顧客に分からせるには忍耐が必要
- ほんのちょっとの開き直りとたくさんの根性が運用者を支える

DNSを管理運用するにあたって

- 監視をしましょう。
  - 『DNSの監視』なので、ICMP の死活監視ではなく、サービスの監視をちゃんとしましょう
    - 『サーバは生きてます。BIND死んでます』では、意味がないんです。(涙)
- メンテナンスはこまめに。
  - 気を抜くと、 ROOT server が変わってたりする。
- BINDだけが DNS の技術ではない。
  - Web や mail 等 DNSを利用したサービスやその仕組みはちゃんと理解する
    - どんなサービスがDNSを使っているが確認する
  - レジストラ、指定事業者、DNSの概念は割りと必須
    - (何にも知らない)顧客に説明できます？
  - キャッシュの問題を理解してくれる顧客は少数
    - 「常識でしょ？」と思って企業を相手にすると涙がとまらなくなる

付録 –今だから言えるDNS障害と運用管理者の傷跡-

- よくあるミス
  - とりあえず FQDN を間違えるのは基本
  - サーバ移設時にシリアル番号の桁を間違えると激痛
  - TTL値を短くしっぱなし
- 思わぬ被害
  - spam filter のサービスでmaster/agent の信頼関係をDNSが取り持っているときにDNSが逝くとサービスも逝く
    - しかもサービスが違うので担当者間での情報共有が無かったりすると最悪の時間が続く
    - 普通にメンテナンスしてた他のサービスが炎上してた･･･って事もあるので注意が必要