ISPにおけるDNS運用TIPS

株式会社オン･ザ･エッヂ
山崎徳之

DNSサーバの配置

- キャッシュサーバとゾーンサーバ
  - 大原則として分離する
    - キャッシュサーバに「も」ゾーンを持たせるか
      - 運用性とパフォーマンスのバランスを考慮する
    - キャッシュサーバはアクセス制限を掛ける
      - 何処からでもアクセスされるべきものではない
    - ゾーンサーバはアクセス制限は掛けない
      - 何処からでもアクセスされるべきものである

キャッシュサーバ

- あるネットワーク内での補助解決手段
  - 全ての機器が自力で解決できるなら不要
    - DNSサーバになれないresolverの解決を補助する
    - 自力解決がfailしている場合に解決を補助する
    - そのネットワーク外部からアクセスされるべきものではない
      - アクセス制限を適切に適用する
  - ネットワークの何処に配置するべきか
    - DNS解決のトラフィックに応じて適宜配置する
    - 拠点毎、OSPFエリア毎、サブネット毎など

ゾーンサーバ

- 委譲されたドメインを管理する場合は必要
  - 管理すべき委譲されたドメインが無ければ不要
    - 外部ネットワークからアクセスされるべきものである
    - 内部ネットワークのIPをDNS管理する場合にも必要
  - ゾーンサーバを設置する場合には冗長化すべき
    - 様々なレベルでの冗長化を考慮する
      - サーバ、ネットワーク、建物、地域
  - どの程度の数のゾーンを引き受けるか
    - DNS解決のトラフィックに応じて分散していく

ゾーンの管理

- 大規模ゾーンの管理方法
  - ゾーン編集方法
    - ゾーンファイルを全て直接書く
    - テンプレート、データから変換する
      - Perl等でスクリプトを作成する
      - ダイアルアッププールの管理などに便利
  - ゾーン管理方法
    - RCS
    - CVS
    - RDB

ゾーンの管理(2)

- CVSを使用した管理方法
  - メリット
    - ディレクトリ階層を含めて管理できる
    - 履歴管理できる
    - 複数人の編集をマージできる
  - 構成
    - 編集する端末、ゾーンサーバがCVSクライアントになる

ゾーンの管理(3)

- ゾーンサーバ間のゾーン共有
  - ゾーン転送を使用
    - デメリット
      - ゾーンサーバにマスター、スレーブという概念が発生する
      - 管理コストが増える
      - シリアルインクリメントなど注意すべき点が増える
  - CVSを使用
  - rsync、scp等を使用

信頼性とパフォーマンス

- 信頼性と負荷分散は表裏一体
  - DNSは複数サーバへのqueryを実装している
    - 複数のDNSサーバを置くだけで冗長化が可能
      - 奇妙なresolverの場合には問題が発生
  - 負荷の増大には対応しづらい
    - L4スイッチの利用
      - udpの対応が必要
      - スイッチ自体の冗長化も必要
    - サーバ自身の増強
    - ゾーン構成の見直し

信頼性とパフォーマンス(2)

- ゾーンとネットワークの設計が重要
  - ゾーンの分散とゾーンサーバへの配置
    - どのゾーンサーバにどのゾーンを置くか
    - ゾーン自体委譲するかどうか
      - 単なるサブドメインで良いかどうか
  - ネットワークとキャッシュサーバの配置
    - resolverは極力他に依存しないことが望ましい
    - resolverも含めた設計を行うべき

セキュリティ

- DNSサーバ自身のセキュリティ
  - OSおよびDNSサーバのセキュリティホールへの対応
    - そもそもセキュリティホールの少ないものを選択する
  - 不要なサービスの削除
    - DNSとsshのみ
      - sshはRSA Authenticationを利用
  - 不要なプロセスの削除

セキュリティ(2)

- DNSサービスのセキュリティ
  - query制限
    - DNSサービス + フィルタリング
  - ゾーン転送アクセス制限(使用する場合)
  - ゾーンコピー時の途中経路の暗号化
  - 正しい委譲の設定