DNSSEC
キャッシュDNSへ導入

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

キャッシュサーバの設定

- サーバソフトウェア
  - 暗号技術のサポート (e.c. openssl)
- サーバ設定
  - 鍵の登録 (e.c. trusted-keys)
  - DNSSECを有効に (e.c. dnssec-enable yes)
  - 検証を有効に (e.c. dnssec-validation yes)
- 詳しくは各種ドキュメントを参照のこと

導入のうれしさ

- サーバでの導入は簡単
  - rootで署名が完了すれば、もっと簡単に
- さよなら、キャッシュポイズニング
  - ユーザが変なサイトに誘導されることも無い
  - メールの配送も安心
- 多少の設定で、安全な環境が実現
  - トラヒックが増えるのは権威サーバとの間だけ

さあいこう

でもでも、サービス設計の懸念

- 何かまずいことは起こらないのか
  - サーバは耐えられるのか
  - レコードはちゃんと引けるのか
- ユーザに影響するのか
  - 検証エラーの時にどうするのか

サーバリソース問題

- 既に何度も言われている
  - CPU
    - 検証によって忙しくなる
  - メモリ
    - 追加レコードでメモリを消費
  - 帯域
    - 追加のレコードで帯域を消費
- 最近のサーバであれば耐えられる程度

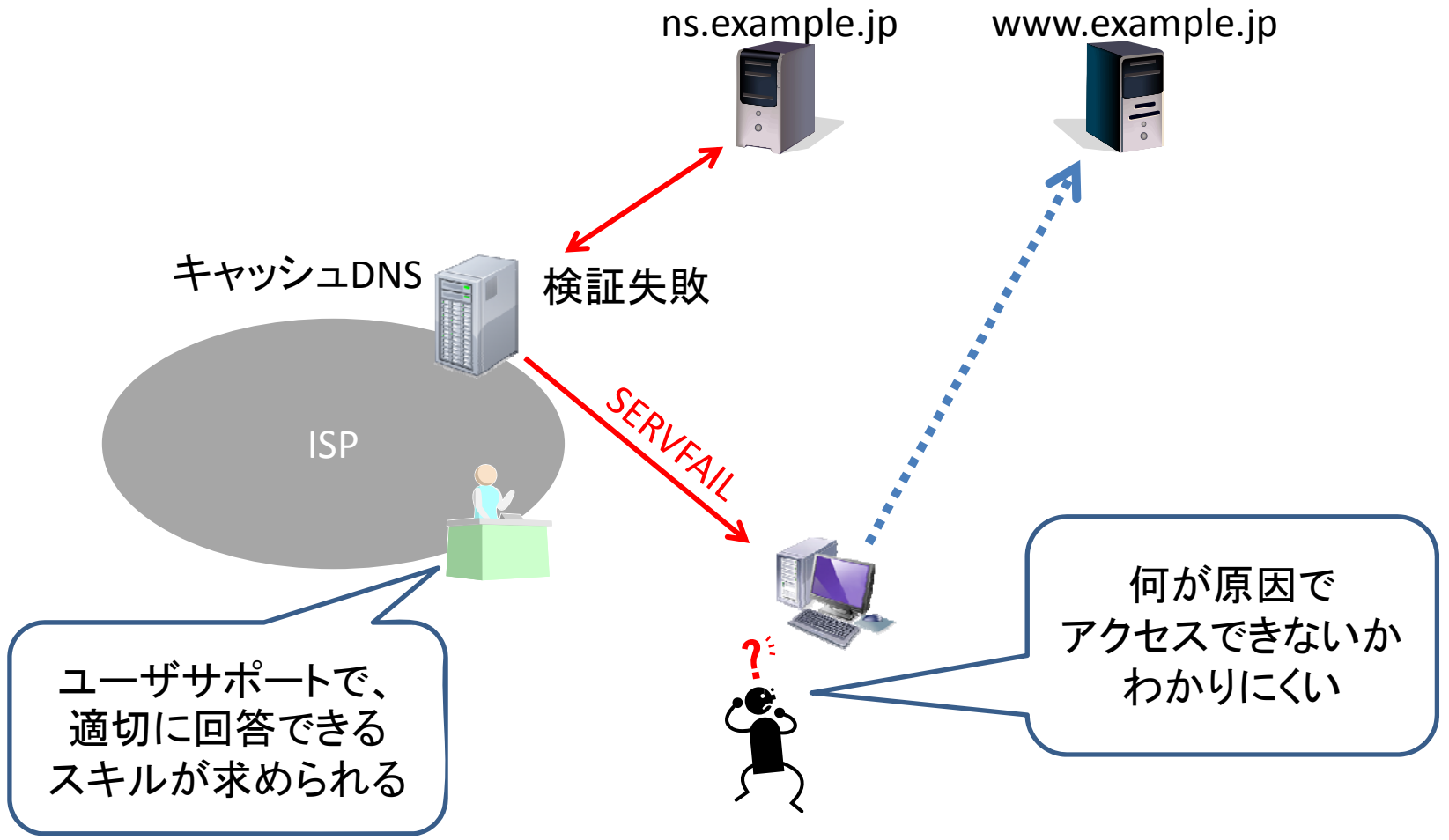
トランスポート問題

- EDNS0拡張でパケットサイズは大きく
  - UDP – ip fragmentへの対応
    - Firewallやパケットフィルタ
  - TCP – UDPに比べると負荷が高い
- この機会に見直しましょう
  - 大きなUDPでもちゃんと通る様に
    - 少なくともキャッシュサーバと他の権威サーバの間

エラー対応

- 検証でエラーになったらどうなる/どうする？
  - 仕様上、SERVFAILがユーザに応答される
    - つまり、ユーザはアクセスできない
- ユーザ側で制御できない
  - 単なるエラーか検証エラーか分からない
  - それでもアクセスするという手段は無い
  - SSL証明書のエラーと異なるところ
- 権威サーバの管理者にコンタクトが必要かも

サービスとユーザと



ISPを選ぶということ

- ISPはそれぞれポリシを持って運用している
  - 利用のされ方(AUP)
  - ルーティングやその他の技術事項
  - 値段が違うだけじゃない
- ポリシを含めてISPを選ばなければならない
  - キャッシュDNSの運用でもポリシの違いが出てきている

まとめ

- 導入の技術的ハードルは低い
- サービスの設計は必要
  - ポリシの策定
  - エラー時のユーザサポート
- エラー時には、権威サーバの管理者と協力して対応が必要かも
  - コンタクト先の検索
  - あるいはML等を通じて修正を呼びかけるか