JPドメイン名サービスへの導入

DNS DAY - DNSSECがやってくる

民田雅人
株式会社日本レジストリサービス
2009-11-24
Internet Week 2009

JPにもDNSSECがやってくる

- JPドメイン名サービスへの
  DNSSECの導入予定について

<http://jprs.jp/info/notice/20090709-dnssec.html>

(2009年7月9日公開)

JPRSでは、DNSのセキュリティ拡張方式であるDNSSECを、2010年中を目処にJPドメイン名サービスへ導入する予定で準備を進めています。

来年中にはJPドメイン名もDNSSEC対応!

JPドメイン名のDNSSEC化

- ルートゾーンがDNSSECで署名される
- JPゾーンをDNSSECで署名する
- JPドメイン名登録者が、自ゾーンをDNSSEC化し、DSをJPゾーンに登録する
- キャッシュDNSサーバが、ルートゾーンのKSK公開鍵をトラストアンカーとして設定し、DNSSECの署名検証を行う

全て揃ってJPドメイン名のDNSSEC化の完了

JPゾーンをDNSSECで署名するために

- ゾーンデータの鍵管理と運用ポリシーの策定
  - KSK、ZSKのそれぞれのビット長は?
  - KSK、ZSKの更新のタイミングは?
  - 署名の有効期間は?
  - KSKの生成と保管方法は?
- システムの負荷へのインパクト
  - ゾーンデータが大きくなることによるインパクト
  - DNSトラフィックが増えることによるインパクト

JPドメイン名登録者

- 登録者のドメイン名のDNSSEC化
  ⇒ DNSSECの理解
  - DNSSECに関する啓蒙、技術文章の発行、チュートリアルなどの実施
- DSをJPゾーンに登録する
  - JPゾーンにDSが登録できるようにする
  - レジストラがDNSSECを扱えるようにする

キャッシュDNSサーバ

- キャッシュサーバが署名検証できる
  - DNSSECの設定を行う
  - DNSSECによる署名データが、権威サーバからキャッシュサーバまで到達できる
- キャッシュサーバの負荷へのインパクト
  - 署名検証によるインパクト
  - DNS応答パケットサイズが大きくなる
    ⇒ DNSトラフィックが増えることによるインパクト
  - ゾーンデータが大きくなることによるインパクト

技術面での懸念点

- DNSの応答パケットのサイズが大きくなる
  - IPパケットとして1500バイトに収まらない場合もある
    ⇒ UDPでフラグメントが発生する
- 一部の(古い?)実装では、UDPでフラグメントしたパケットを扱えないことがある

  ⇒ 署名を伴ったDNSパケットが通過できない

  ⇒ 署名検証に失敗する

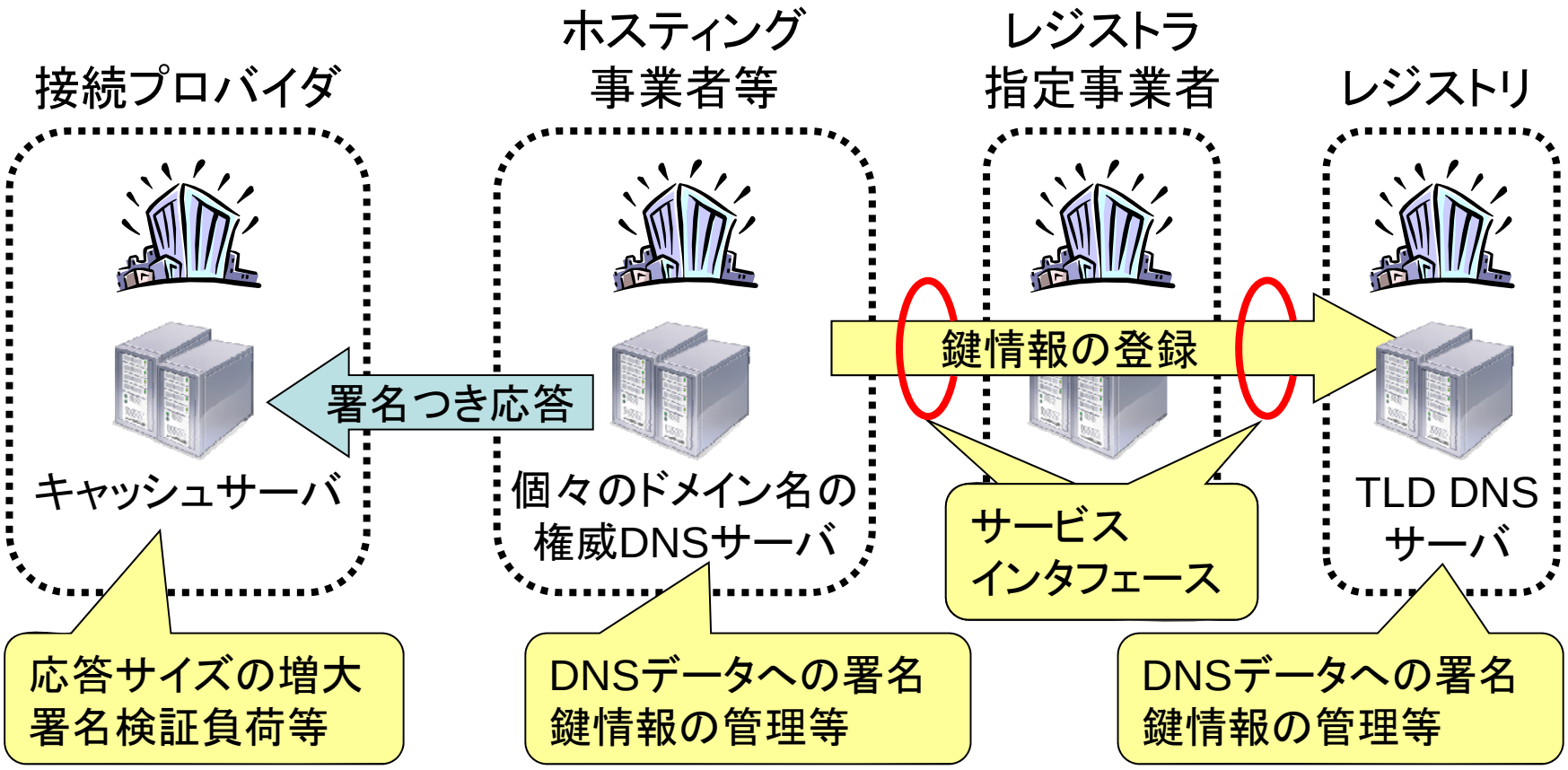
  ⇒ DNSの名前解決ができない ☹
- TCPを使ったDNS通信を禁止している場合もある

DNSSEC導入に関する技術検証

- JPRSでは、現在DNSSEC化した仮想のDNSツリーを用意し、各種テストを実施中
  - 一部のプロバイダ、ベンダーにも参加頂いております
    ⇒ ご協力ありがとうございます
- 結果をある程度まとまった段階で公開

DNSSECの導入に向けて

DNS運用に関わる各立場での検討・対応が必要



JPドメイン名へのDNSSEC導入