あなたのDNS運用は
来るべきDNSSEC時代に耐えられますか

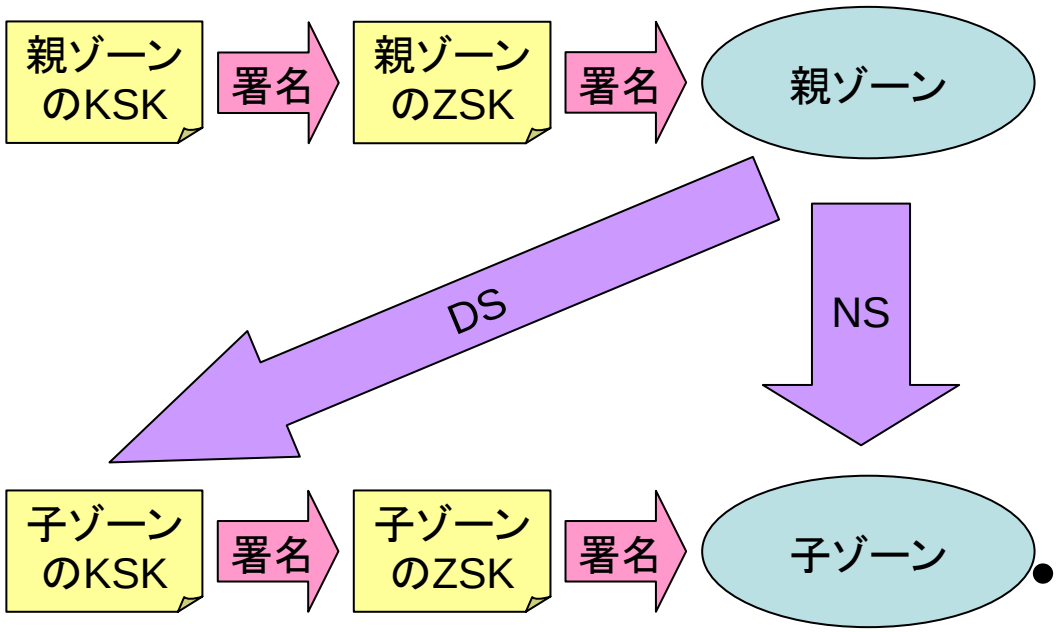
JANOG 24事前資料

民田雅人 <minmin@jprs.co.jp>
株式会社日本レジストリサービス
2009-07-09 JANOG 24@東京

DNSSECとは

- DNS SECurity extension
  - 公開鍵暗号技術の応用
- ゾーン情報に秘密鍵で署名
  - DNSの応答パケットに署名情報を付加
- クライアントが公開鍵で署名を検証
  - ゾーン情報の第三者による改ざんや騙りを公開鍵を用いて検証
- DNSキャッシュサーバへの毒入れ攻撃による被害を防ぐ、現時点で唯一の現実解
  - 短いTTLのリスク(JANOG 19)やKaminsky型の攻撃による被害を**完全**に防ぐことができる技術

DNSSECの信頼の連鎖



- 公開鍵暗号による信頼の連鎖を形成
  - KSK - Key Signing Key
  - ZSK - Zone Signing Key
  - DS RR- Delegation Signer RR
- キャッシュサーバが、ルートゾーンのKSKの公開鍵を使って署名を検証

いくつかのTLDが DNSSEC対応済 or 対応を表明

- gTLD
  - .ORG　.GOV　.MUSEUM
- ccTLD (試験運用を含む)
  - .BG　.BR　.CZ　.PR　.SE　.TH
- VeriSign (.com .net等)も対応表明
- ROOTゾーンのDNSSEC対応も時間の問題
  - http://www.nist.gov/public_affairs/releases/dnssec_060309.html
  - http://www.icann.org/en/announcements/announcement-2-03jun09-en.htm
- 時間の問題でDNSSECはみなさんのお手元に

DNSSEC対応しますか？

- 対応します：キャッシュDNSサーバ側
  - 設定はそれほどむずかしくない
  - 署名検証による負荷の増大は大変
- 対応します：権威DNSサーバ側
  - やることいっぱい
  - 鍵管理：鍵生成、鍵更新
  - ゾーンの署名、再署名、親ゾーンへのDSの登録

でも今回議論したいのは、これらとは別の視点

DNSSEC対応しますか？ (続き)

- (まだ)対応しません：キャッシュDNSサーバ側
  - すぐにやらないけど、そのうち対応します。
    ⇒ だから、今は何もしません
  - 事情により今は対応できないので、次の機器更新とともに対応します
    ⇒ だから、今は何もしません

- DNSSEC対応しないので、何も起きないと考えるのは大きな誤り

DNSSECによって DNSの通信はどうなるのか

- 署名がつくため、DNSパケットは大きくなる
  - ここまでは誰もが知っている(よね?)
- うちのキャッシュDNSサーバ、まだDNSSEC対応の設定してないから大丈夫

本当？

続きはJANOG 24本会議で