DNSSEC超入門

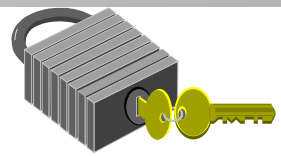
2004年6月14日 第1.1版

JPRS

内容

- DNSSECとは
- DNSSECの概念
- Delegation Signer (DS)方式
- DNSSECの現状
- DNSSECの課題

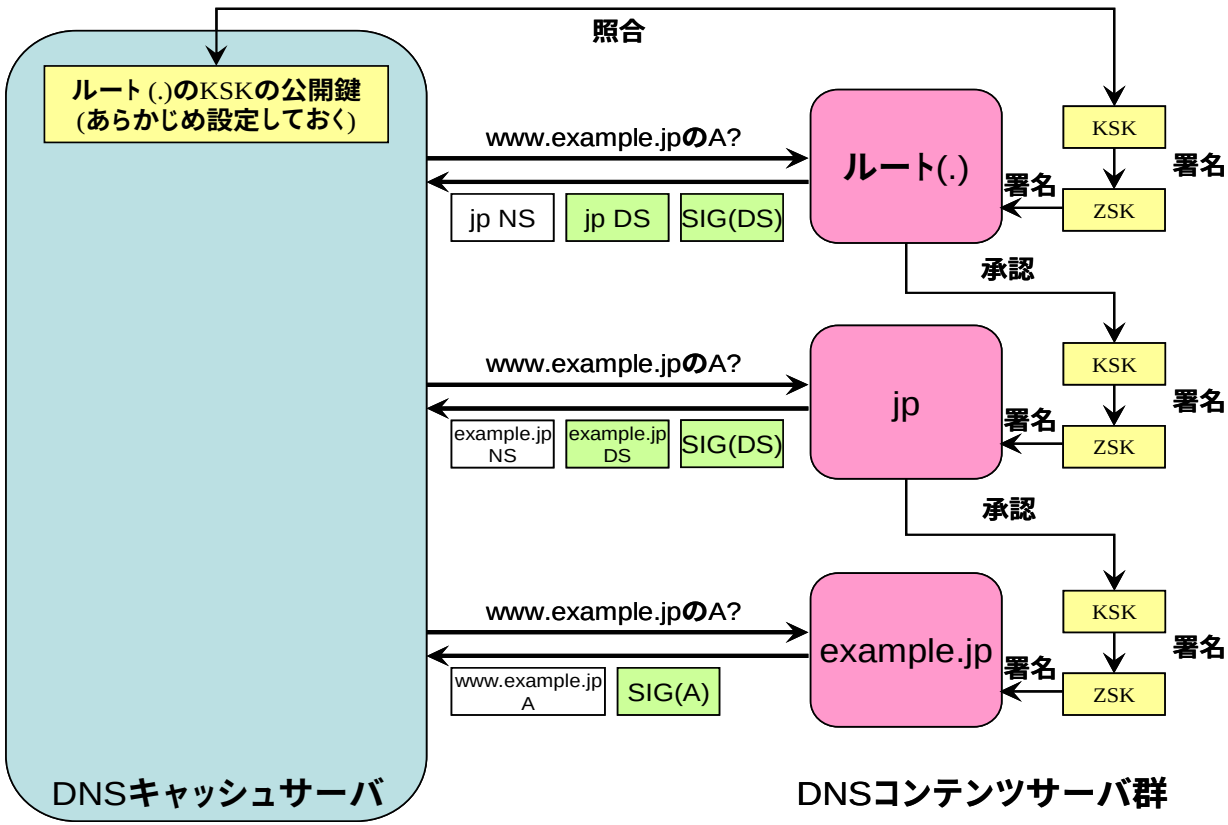
DNSSECとは



- DNSゾーンに権限を持つ管理者が、公開暗号鍵技術を用いて、自らのゾーン情報に署名を行うDNSの運用方式
  - そのゾーン情報の第三者による改ざん･騙りを検証することが可能となる技術
  - これにより、万一にも騙りを許したくないDNSレコードを守ることが可能となる

DNSSECの概念

- 鍵による信頼の連鎖 (chain of trust)を形成
- 現在のDS方式では、KSKとZSKの2つの鍵を使用(後述)



Delegation Signer (DS)方式

- 従来のDNSSEC(RFC 2535)にかわる新しい方式
- RFC 3658で定義
- DS (Delegation Signer)資源レコードを使用
  - DSは子ゾーンのKSKと暗号論的に等価
  - DSにより子ゾーンのKSKの所持を親ゾーンが承認
- ゾーン管理者は2つの鍵を使用
  - KSK (Key Signing Key): 自分のZSKの署名のための鍵
  - ZSK (Zone Signing Key): 自ゾーンの署名のための鍵
- 鍵を2つにした理由
  - 運用上の便宜を図るため
  - 鍵を2つにすることにより、従来必要であった子ゾーンの署名用の鍵を、親ゾーンの鍵により署名したうえで子ゾーンに戻す手順が不要となる
  - DS方式では親ゾーンには自分のKSKのみを一方的に送ればよい

DNSSECの現状

- IETFにおける現状
  - IETFのdnsext wgにおいて、DS方式による新しいDNSSECプロトコルを策定中
  - 以下の3つのInternet Draftにまとめられている
    - draft-ietf-dnsext-dnssec-intro-09.txt
    - draft-ietf-dnsext-dnssec-protocol-05.txt
    - draft-ietf-dnsext-dnssec-records-07.txt

DNSSECの課題

- 大きな2つの課題
  - 普及(deployment)
    - 従来の方式は運用コストが大きかった
      - DSの導入による運用コストの削減
      - ただしDS方式は従来の方法と非互換
    - 利用するためにはキャッシュサーバの更新が必須
    - 安全な鍵配布･鍵更新の手順が別途必要
  - 実装(implement)
    - BIND 9が事実上唯一のDNSSECの実装であった
      - BIND 9.2系列では従来方式によるDNSSECをサポート
      - BIND 9.3系列でDS方式をサポート
        - » 現在評価版が9.3beta4として公開
      - NSD 2.0.0以降ではDS方式によるDNSSECをサポート
        - » ただしNSDはDNSコンテンツサーバ機能のみを提供