DNSSEC導入に関する世界的動向

2010年11月25日
DNS DAY, Internet Week 2010

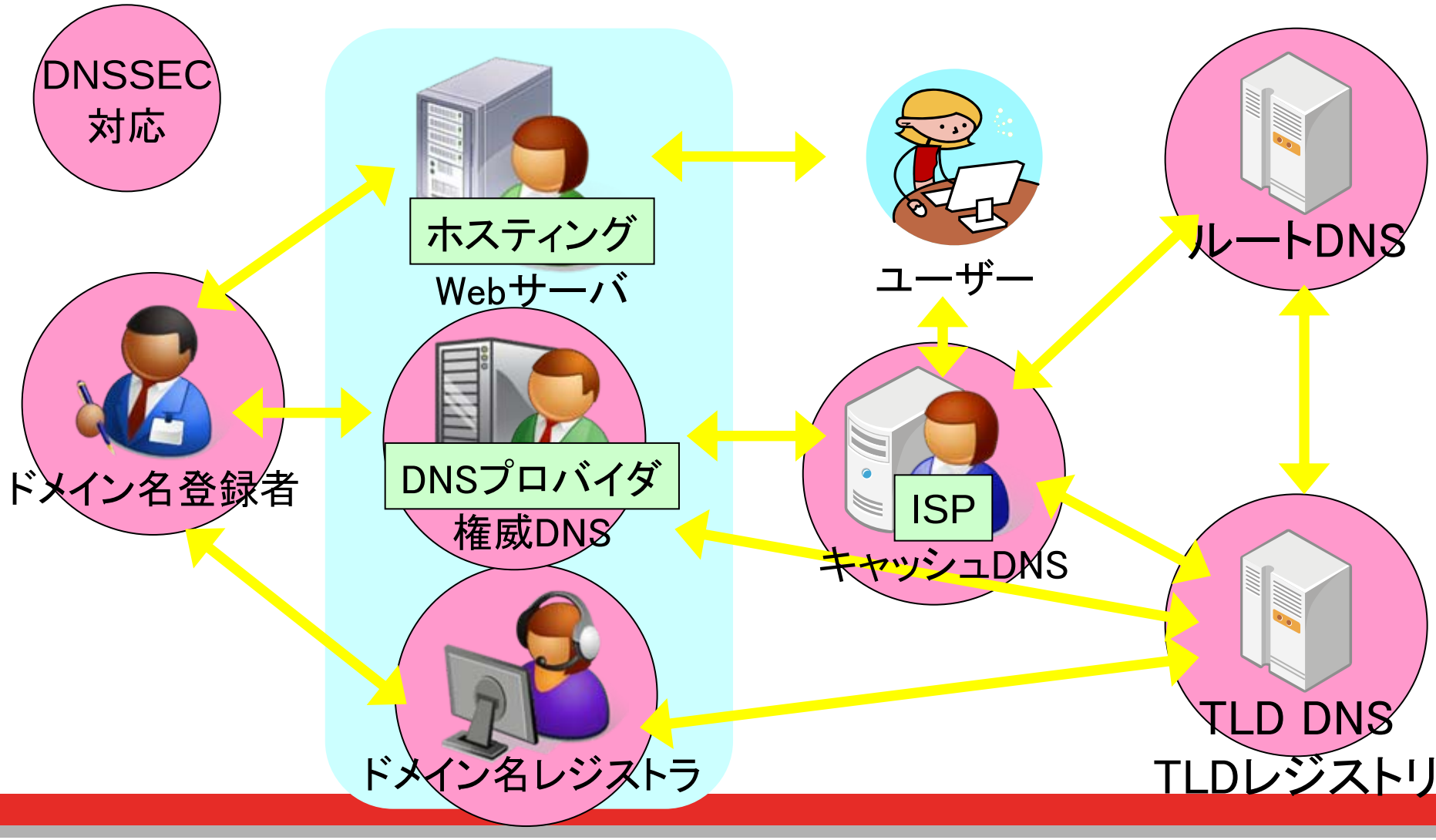
佐藤 新太 <shinta@jprs.co.jp>
株式会社日本レジストリサービス

内容

- 2010年に急速に展開が進んだDNSSECに関し、ルート、gTLD、ccTLDにおけるDNSSECの導入状況を紹介する

- 目次
  - DNSSEC対応が必要な関係者
  - ルート、TLDでの対応状況
  - DNSSECを用いたサービス、技術
  - DNSSEC導入推進の活動

DNSSEC対応が必要な関係者



DNSSEC対応作業の概要

- ドメイン名登録者
  - DNSSEC導入の決定
- ドメイン名レジストラ
  - 鍵情報のレジストリへの取次ぎ
- TLD DNS、ルートDNS
  - 権威DNSサーバのDNSSEC対応化
  - ゾーンへの署名
- DNSプロバイダ
  - 権威DNSサーバのDNSSEC対応化
  - 秘密鍵・公開鍵を作成し、ゾーンに署名
- ISP
  - キャッシュDNSサーバのDNSSEC対応化
  - (キャッシュDNSサーバでの)署名の検証

2010年はルート、TLDでのDNSSEC対応が急速に進んだ

世界のDNSSEC導入の概況

- ルート
  - 2010年7月15日よりDNSSECの正式運用開始

- DNSSEC導入済TLD (2010年11月11日時点)
  ルートゾーンにある全294のTLDのうち
  - 49のTLDが署名+ルートゾーンのDS登録済(11のテストTLDを含む)
  - 14のTLDが署名のみ実施済み
  2009年末は10のTLDが署名のみ実施済みだった

- 今後の動き
  - .jpは2010年1月16日より登録受付サービス開始
  - .netは2010年12月、.comは2011年3月にルートゾーンへのDS登録予定
  - 他に導入予定のTLDが多数

ルートにおける導入状況(1)

- 2009年10月　　2010年7月からの正式運用を発表
- 2009年12月　　実験的な署名を内部で開始
  - 署名したゾーンファイルの作成を開始
- 2010年1月～5月　ルートサーバでの公開
  - ルートサーバ単位で段階的に署名付き情報に切替え
- 2010年6月16日　KSKセレモニー1の開催
  - コミュニティの代表と共にKSKの生成を実施
- 2010年6月23日　ルートゾーンへのDSレコード登録開始
  - .br、.uk、.czが最初の登録に
- 2010年7月15日　正式運用を開始
  - トラストアンカーを公開、署名検証が可能に
- 2010年11月　　ITARの終了を発表
  - 2011年1月にITARのサービスを終了

ルートにおける導入状況(2)

- DURZを用いた慎重な導入
  - DURZ: Deliberately Unvalidatable Root Zone
    検証できないダミーの署名データを追加したルートゾーン
  - L ⇒ A ⇒ M, I ⇒ D, K, E ⇒ B, H, C, G, F ⇒ J
  - 全サーバでDURZを導入し、問題が発生しない事を確認
  - http://www.root-dnssec.org/

- KSKセレモニーによるコミュニティと連携した鍵管理
  - TCR: Trusted Community Representatives
    信頼されたコミュニティの代表
  - Crypto Officer(14名)、Recovery Key Share Holder(7名)
  - ルートゾーンのKSKの生成・利用には、TCRの参加が必須
  - http://dns.icann.org/ksk/ceremony

gTLDのDNSSEC導入状況

- 7つのgTLDが署名+ルートゾーンのDS登録済み
- 3つのgTLDが署名のみ実施済

(2010年11月11日時点)

TLD	導入状況	登録数
.aero		6,959
.arpa	署名済	–
.asia	署名済	182,232
.biz	DS登録済	2,087,299
.cat	DS登録済	43,416
.com	2011Q1予定	90,798,616
.coop		6,920
.edu	DS登録済	–
.gov	DS登録済	–
.info	DS登録済	6,586,510
.int		–

TLD	導入状況	登録数
.jobs		33,038
.mil		–
.mobi		975,967
.museum	DS登録済	462
.name		241,278
.net	署名済	13,543,361
.org	DS登録済	8,477,095
.pro		48,316
.tel		–
.travel		254,964

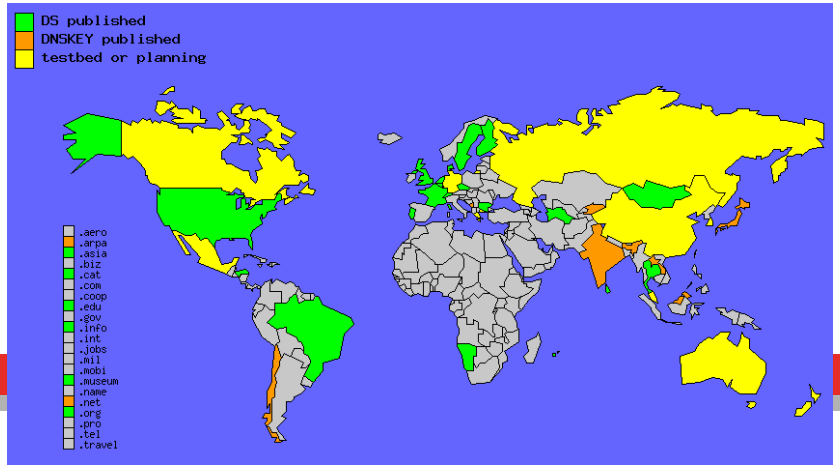
登録数は2010/7月現在

最大手の.com、.netのDNSSEC導入も既に発表済み

ccTLDのDNSSEC導入状況

- 全262のccTLD (ASCII 247、IDN 15)の中で、
  - 31のccTLDが署名+ルートゾーンのDS登録済
    - .uk(イギリス)、.br(ブラジル)、.cz(チェコ)、.eu(欧州連合)、.fr(フランス)、.us(アメリカ)、.ch(スイス)、.nl(オランダ)、.se(スウェーデン)、...
  - 11のccTLDが署名のみ実施済み (2010年11月11日時点)
    - .jp(日本)、.cl(チリ)、.in(インド)、...
  - 導入計画中、テスト中は多数
    - 既に全情報を追いきれない状況
- 各国でDNSSEC導入の動きが活発
  - 日毎に署名済み、DS登録済みのccTLDが増えていく
  - ICANNによる自動調査(*1)
  - BBTower大本氏の世界地図(*2)

(*2)



(*1) http://stats.research.icann.org/dns/tld_report/

(*2) http://www.ohmo.to/dnssec/maps/

DNSSECを用いたサービスの開始

ルート、TLDでのDNSSEC対応が進んだだけでなく、
DNSSEC運用のサービスが開始

- DNSプロバイダ
  - チェコ(.cz)の大手レジストラであるWEB4Uが自社でDNS運用している.czドメイン名約1.5万を全て署名(2010/1)
  - Akamaiが米国政府(.gov)向けにDNSSEC管理を行うDNS運用サービスを開始(2010/8)
- ISP
  - NTTデータ三洋システムが会員のキャッシュサーバでDNSSEC検証を開始 (2010/8)
  - 米国大手ISPのComcast社がDNSSEC検証を行うサービスの導入を発表(2010/10)

DNSSECを用いた次の技術

- KIDNS (Keys In DNS)
  - 公開鍵暗号方式を使った各種プロトコルにおいて、DNS経由でデジタル証明書等を提供する事によって、運用性の向上を図ったもの
  - DNSSECの普及により、証明書の信頼性が従来のDNSから拡張されている
  - IETF 79 北京(2010/11)にてBoF開催、今後検討が進められる予定

DNSSEC導入推進の活動

- DNSSEC Deployment Initiative
  - エキスパートや先駆者による技術情報交換、サポートの場
  - http://dnssec-deployment.org/
- DNSSEC Industry Coalition
  - DNSSEC導入を進める企業の連合
  - http://dnsseccoalition.org/
- Practice safe DNS
  - .orgによるDNSSEC普及のキャンペーン
  - http://practicesafedns.org/

まとめ

- 2010年は世界的にみて、DNSSEC導入のためのハードルが急速に低くなった年である
  - インフラ側の整備(ルート、TLD)
  - 技術検証から、実環境への展開
  - DNSSECを用いたサービスの開始

⇒次は利用者が実践する事で、さらなる普及が始まる

⇒今後はDNSSECというセキュリティ拡張の恩恵を実際に手にする事が可能に

Q and A