DNSSEC の現状 (DNS DAY2011)

株式会社ブロードバンドタワー
大本　貴

Who am I ?

- 職歴
  - 2000年 インターネット総合研究所入社
  - 2001年 プロデュースオンデマンド(PoD)に出向
    - ストリーミング配信技術担当
  - 2007年 インターネット総合研究所に帰任
    - 主に社内システムのサーバ運用、コンサルなど
    - 2010年春からDNSSECジャパンに参加
  - 2010年 ブロードバンドタワーに転籍

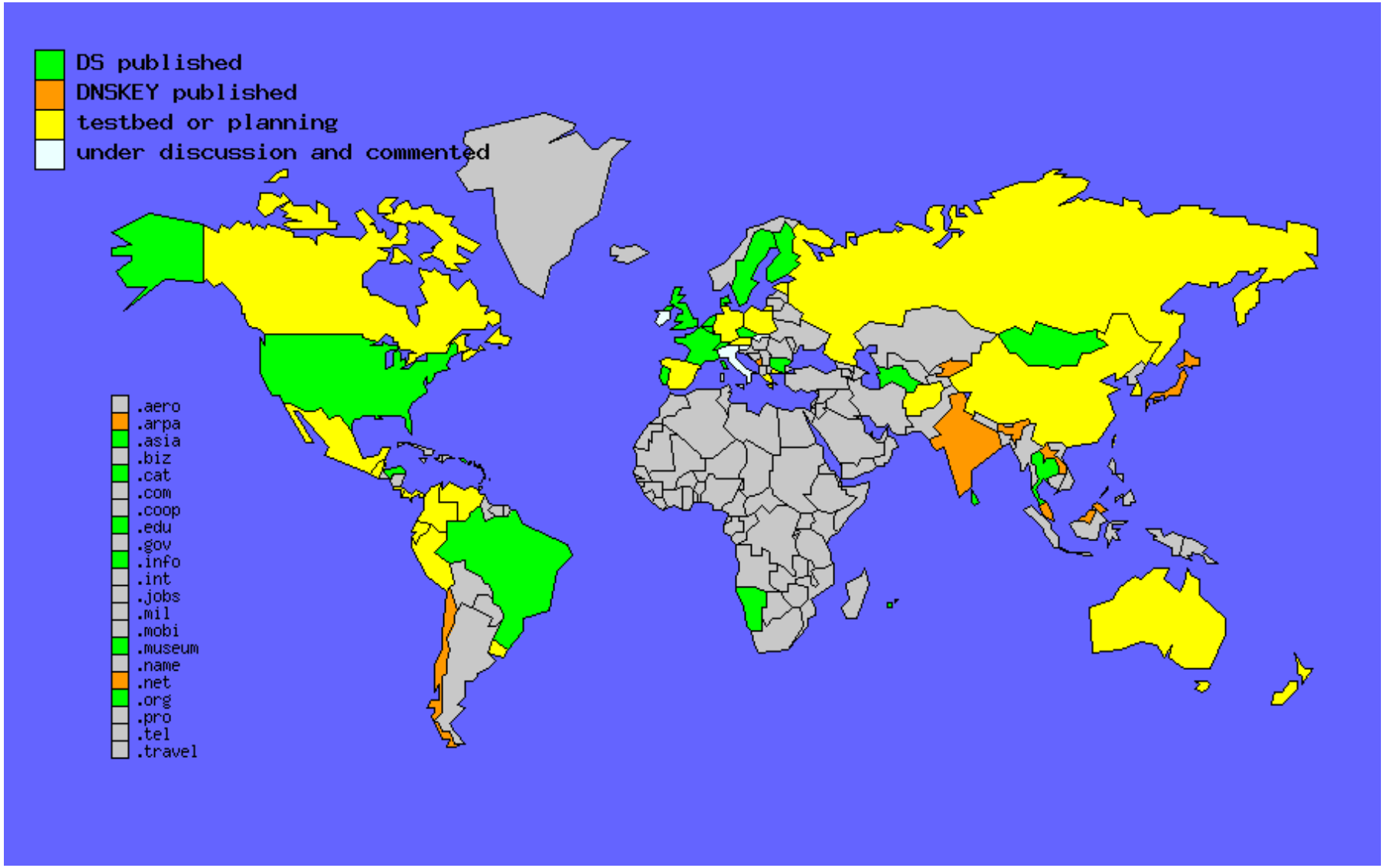
本日お話しすること

- この一年のDNSSECの動向update
- この一年のDNSSECジャパンの活動
  - 運用技術WGの紹介
  - ロゴWGの紹介

この一年(2010/11～)のDNSSEC Topics

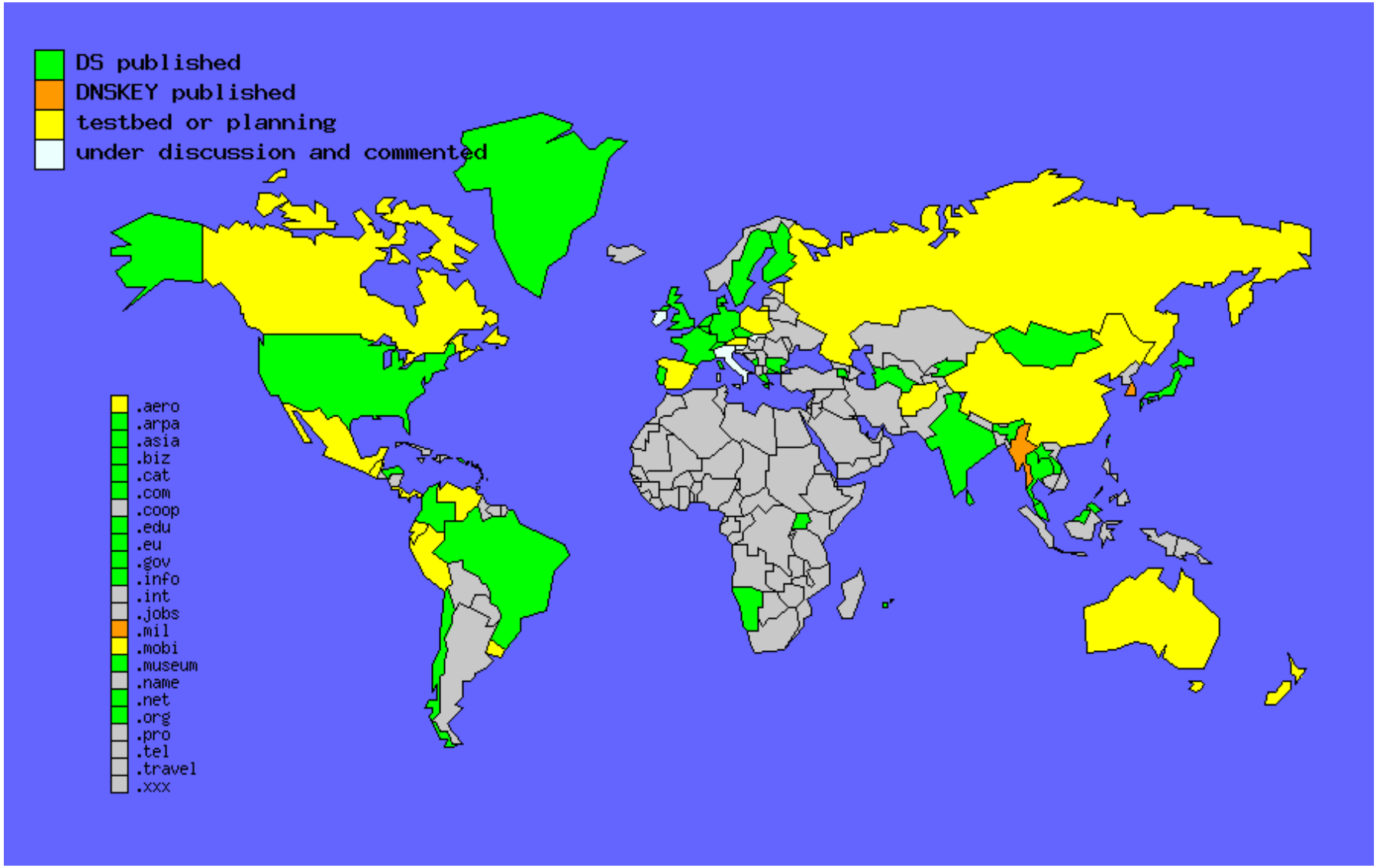
- rootに.netのDS登録 (2010/12)
- rootに.jpのDS登録(2010/12)
  - JPRSが.jpドメイン名サービスにDNSSEC導入(2011/1)
    - (2011/11にはキー ロールオーバーも実施)
- rootに.comのDS登録 (2011/3)
  (gTLDでの最大ドメイン数保持)
- rootに.deのDS登録 (2011/6)
  (ccTLDでの最大ドメイン数保持)
- 2010/11時点で34TLD→2011/11時点で**64**TLD
  (上記と別にIDN-TLDで導入済み 10TLD → **13**TLD)
- **合計77 TLDがDNSSEC導入済みになった(全310TLD中)**
  (2011/11/16 現在)
  - DNSKEY公開済みは加えて4TLD(+2 IDN-TLD) で
    合計**83**TLD/310TLD

2010/11/25 (Internetweek2010)



http://www.ohmo.to/dnssec/maps/

2011/11/17 現在



http://www.ohmo.to/dnssec/maps/

この一年(2010/11～)のDNSSEC Topics

- 公表されているドメイン数から見たDNSSEC対応状況

参考: 各TLDのドメイン登録数
(レジストリwebサイト等で公表されている数字に限る)

gTLD 合計 134,344,830 ドメイン
DNSSEC導入済みgTLDの管理ドメイン数 132,594,356ドメイン(98.69%)
前年(9%)

ccTLD 合計77,659,219ドメイン
DNSSEC導入済みccTLDの管理ドメイン数 49,446,395ドメイン (63.67%)
前年(27%)

TLDレベルでは、上記の比率までは”DNSSEC Ready“になってきている状態

- あとはレジストラの対応次第で、各ドメイン登録者がDNSSECを導入するかどうか選択できるところまで進んできている
- 現在、このうち何%がDNSSECに対応しているかというと・・・

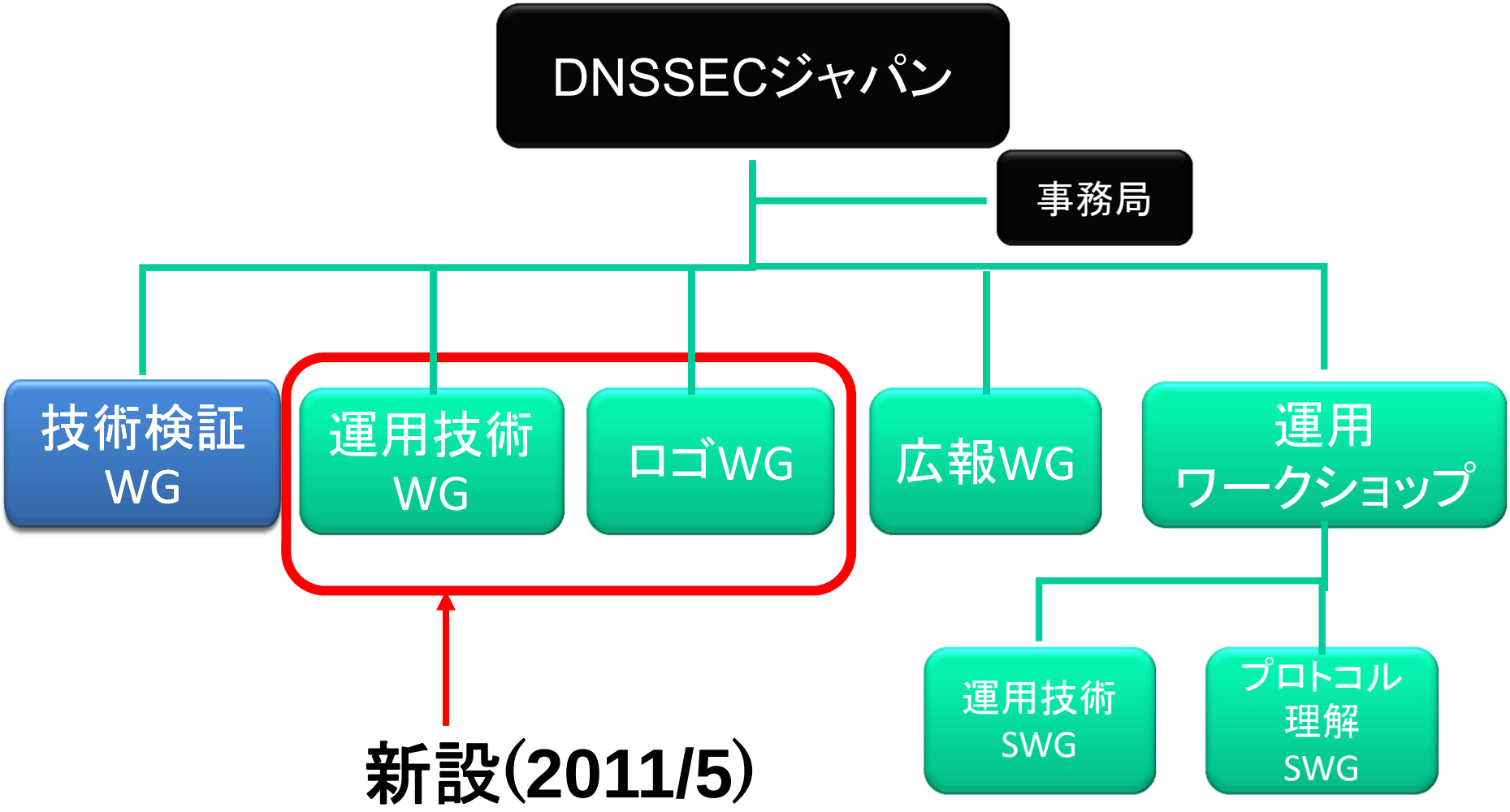
DNSSEC ジャパン　update

活動概要

- 2009/11/24設立、活動2年目
- DNSSECに関係するプレイヤーの相互扶助を目的
- ISP、IXP、ホスティング、ドメイン事業者、ベンダ、各種団体等、38組織が参加
- http://dnssec.jp

- 活動状況
  - 2010年12月22日 Security Day
  - 2011年2月24日 APRICOT-APAN2011
  - 2011年3月3日　Hosting-PRO2011
  - 2011年4月20日 DNSSEC 2011スプリングフォーラム

DNSSECジャパン　組織構成



技術検証WGの活動

- 期間
  - 約1年（2010/1/25～2011/4/11）
- 活動
  - 定例会合13回
    - 各検証項目、実証実験等にて不定期に打合せ
  - 調査
    - 国際動向・技術情報調査、関連ツールの比較調査など
  - 検証
    - レジストラ移転検証、ネットワーク接続機器検証など
    - 技術検証環境の提供
  - 成果はメンバ内で取りまとめ、資料公開
    - DNSSECジャパンのwebサイト(http://dnssec.jp/)にて資料公開中

技術検証WGが公開している資料(2010/11～)

- **レジストリの鍵登録インターフェースに関する調査報告**
  技術検証WGにおいて行った、レジストリの鍵登録インターフェースの調査についてまとめた資料
- **レジストラ移転ガイドライン**
  技術検証WGにおいて行ったDNSSEC導入後のレジストラ移転・DNSプロバイダ移転方法の検討の報告資料
- **キャッシュDNSサーバDNSSEC導入ガイドライン**
  キャッシュDNSサーバへのDNSSEC導入についてのガイドラインをまとめた資料
- **DNSサーバDNSSEC導入Load Balancer機能チェックリスト**
  DNSサーバへのDNSSEC導入に伴い、DNSサーバ上位のNW機器においても考慮しなければならない確認事項をとりまとめた資料
- **DNSSECツール調査報告**
  DNSSEC に対応するツールやサービス、ライブラリの調査を行いました。その結果をとりまとめた資料
- **DNSSECにおける鍵管理**
  DNSSECにおける鍵管理の基本的なライフサイクルを説明したガイドライン
- **DNSサーバDNSSEC導入鍵管理チェックリスト**
  DNSサーバへのDNSSEC導入に伴う、鍵の作成と管理において考慮すべき確認事項を取りまとめた資料

運用技術WG

- WGの活動目的
  - .jpでのDNSSEC運用も開始し、サービスへ導入した事業者も出てきている中で、先達が解決してきた様々な技術的知見を集約し、DNSSECの運用を行っていくのにあたり技術情報をまとめ、活用してもらいたい
  - また、現在、DNSSECへ足踏みしている技術的課題、政治的課題について調査し、導入への障壁を明らかにしたい
- 活動状況
  - これまでに8回のWGを開催。
    - 10年6月14日より3週間に1度の開催
  - 導入組織での失敗事例、HSM、DPSについての勉強会
  - アンケートの実施(DNSSEC導入への障壁は何かをヒアリング)
  - メンバは親会から参加
  - 成果はメンバ内で取りまとめ、資料公開をめざす。

運用技術WGの公開資料

- リリース5以前のRedHat Enterprise Linuxおよびその互換OSをセカンダリサーバとして用いるゾーンへのDNSSECの導入にあたっての注意喚起
  - http://dnssec.jp/?page_id=570
  - DNSSEC の validation を有効にしているキャッシュサーバが、再帰的問い合わせの過程でセカンダリサーバから応答を得ると、validation に失敗する
  - 当該ゾーンが不在証明の方式として NSEC3 を採用しているとき、DNSSEC の validation を有効にしているキャッシュサーバが、再帰的問い合わせの過程でセカンダリサーバから応答を得ると、不在証明に失敗する
  - RHEL系で「yum install bind 」な人は是非ご一読を
- その他これまでの活動成果は現在取りまとめ中
  - 年明けから年度末に向けて公開していく予定

ロゴWGの紹介

- DNSSEC Readyロゴを製作中
- 自組織のサービスや製品がDNSSEC Readyだと表明する素材を提供
- 4つのカテゴリーでチェックリストを作成
  - キャッシュDNSサーバ
  - 権威DNSサーバ
  - ドメイン登録(登録者、登録事業者等)
  - 製品(ネットワーク機器、DNSサーバ製品、鍵管理製品等)
- チェックリストを自己チェックして、適合していたらDNSSEC Readyロゴマークを利用してください

DNSSEC Readyロゴ

利用規定(抜粋)

- DNSSEC ReadyロゴおよびDNSSEC Readyチェックリスト(以降、本ロゴおよび本チェックリストとする)は、商用・非商用を問わず提供する製品やサービスがどの程度DNSSECに対応しているかを客観的に示すためのものである。

- 本ロゴおよび本チェックリストは、特定のサービスあるいは製品がDNSSECに対応していることを表明する手段として利用できる。

- 本ロゴおよび本チェックリスト利用者は、本規定第2項で定めるカテゴリーにおいて対象のサービスあるいは製品に該当するチェックリストを自らチェックし、適合が確認できた場合に、適合するサービスあるいは製品を明示した上で本ロゴを利用できる。

- ただし、本ロゴはDNSSECジャパンが何らかの認定を与えるものではない。

チェックリスト(抜粋)

キャッシュDNSサーバチェックリスト(2011年11月4日版)

このチェックリストは、キャッシュDNSサーバがDNSSECに関する問い合わせを正しく処理し、クライアントに適切な応答を返すことができることを確認する。利用者がDNSSEC Readyロゴマークを使用するためには、このチェックリストの中で該当する各項目に適合することが求められる。他のカテゴリーのチェックリストを参照している部分については、そのチェック結果を添付すること。

機能の確認	
ネットワーク機器(ルータ、F/W・IPS・IDSなどのセキュリティ機器、負荷分散装置など)を含むシステムとしての機能の確認	
☐	製品チェックリストの汎用ネットワーク機器製品に対応していること
キャッシュDNSサーバの機能の確認	
☐	EDNS0に対応していること
☐	TCP/UDPともSRCもしくはDSTのPort53宛てのパケットを送受信できること
☐	512バイトより大きいペイロードを持つパケットを送受信できること
☐	IPフラグメントパケットを送受信できること
☐	UDPフラグメントの再構成が正しく行われること
☐	権威DNSサーバにDO(DNSSEC OK、DNSSECの情報を要求する)ビットをつけて問い合わせ可能なこと
☐	クライアントからのDO、CD(Checking Disabled、DNSSEC検証を行わない)の要求を正しく解釈して取り扱えること
☐	署名検証成功時はAD(Authentic Data、DNSSEC検証の成功)ビットをつけて応答すること
☐	署名検証失敗時はSERVFAILを応答すること

DNSSECジャパン全体としての活動

- PGP鍵管理検討
  - ICANN/IANAが公開しているルートゾーンの鍵に署名しているPGP鍵の真正性をどうやって実証するか
  - ICANNのレターヘッドの付いたfinger printを、ICANN大久保さんが海外から持ってきてくれた。(JANOG28で読み上げていただいた。)

- DNSSECジャパンの今後の活動
  - 2011年3月に活動終了予定
  - 2011年春にイベント開催予定
  - 公開している資料等については公開継続