

Root/.JPの状況

株式会社日本レジストリサービス
佐藤 新太

DNSSEC 2012 スプリングフォーラム
2012年4月25日

目次

- 前回(2011-04)までのおさらい
- Rootの状況
- .JPの状況

前回(2011-04)までのおさらい

	Rootの動き	.JPの動き
2009-07-09		導入タイムライン発表
2009-10	導入タイムライン発表	
2010-01 ~05	DURZによるルートサーバの署名対応	
2010-05-21	Root KSK DPS公開	
2010-06-16	Root KSK セレモニー	
2010-06-23	DS登録開始	
2010-07-15	TA公開	
2010-10-04		.jp DNSSECキーセレモニー
2010-10-17		DNSSECによる署名開始
2010-12-10		ルートゾーンへのDS登録
2011-01-14		JP DPS公開
2011-01-16		.jpゾーンのDS登録受付開始

Rootの状況

- キーセレモニーの実施

<http://dns.icann.org/ksk/ceremony/>

- 毎回TCRのメンバーが3名以上集まり実施
- これまでに8回開催 (年4回、概ね3ヶ月毎)
- セレモニーの次のタイミングでZSK更新
- 手順が少しずつ改善
 - 第4回 133 ステップ ⇒ 第8回 94ステップ

- IANA申請のWeb化

<https://rzm.iana.org/>

- 2011-07にIANAからアナウンス
- 長年にわたりメール受付だった申請がWebで実施可能に
- 人が介在するための往復の時間の短縮、誤作業の抑制
- 2011-10にJPの申請でも利用

IANA RZMのサンプル画面



Internet Assigned Numbers Authority

RZM (Root Zone Management)

[Logout](#) | [Change Password](#) | [Home](#)

Edit Nameserver Details

Current Details

The following data is currently in the IANA database:

A.DNS.JP	203.119.1.1 2001:DC4:0:0:0:0:1
B.DNS.JP	202.12.30.131 2001:DC2:0:0:0:0:1
C.DNS.JP	156.154.100.5 2001:502:AD09:0:0:0:5
D.DNS.JP	210.138.175.244 2001:240:0:0:0:0:53
E.DNS.JP	192.50.43.53 2001:200:C000:0:0:0:35
F.DNS.JP	150.100.2.3 2001:2F8:0:100:0:0:153
G.DNS.JP	203.119.40.1

New Details

Please provide the new list of authoritative nameservers, plus the relevant IP addresses for building glue records.

<input type="text" value="A.DNS.JP"/>	<input type="text" value="203.119.1.1 2001:DC4:0:0:0:0:1"/>	<input type="checkbox"/>
<input type="text" value="B.DNS.JP"/>	<input type="text" value="202.12.30.131 2001:DC2:0:0:0:0:1"/>	<input type="checkbox"/>
<input type="text" value="C.DNS.JP"/>	<input type="text" value="156.154.100.5 2001:502:AD09:0:0:0:5"/>	<input type="checkbox"/>
<input type="text" value="D.DNS.JP"/>	<input type="text" value="210.138.175.244 2001:240:0:0:0:0:53"/>	<input type="checkbox"/>
<input type="text" value="E.DNS.JP"/>	<input type="text" value="192.50.43.53 2001:200:C000:0:0:0:35"/>	<input type="checkbox"/>
<input type="text" value="F.DNS.JP"/>	<input type="text" value="150.100.6.8 2001:2F8:0:100:0:0:153"/>	<input type="checkbox"/>
<input type="text" value="G.DNS.JP"/>	<input type="text" value="203.119.40.1"/>	<input type="checkbox"/>
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

< Revert Changes

Save Changes >

.JPの状況

- DNSSEC関連情報の一部変更
 - 2011-06-18 DNSKEYの署名をKSKのみに変更
 - 2011-07-07 ZSKの個数を2個に変更

<http://jprs.jp/tech/notice/2011-07-29-jpdns-dnskey-and-rrsig-change.html>
- キーセレモニーの実施
 - 2011-10-04 第2回「.jp DNSSECキーセレモニー」
- KSKロールオーバーの初回実施
 - 2011-10-07 新KSKをJPゾーンで公開
 - 2011-10-13 ルートでの新DS公開
 - 2011-11-04 旧KSKのJPゾーンでの公開停止
- ZSKロールオーバーの実施
 - 毎月定期的に実施

.jp DNSSECキーセレモニーの結果

資料B

jp DNSSECキーセレモニー 作業用チェックシート

作業日 2011 年 10 月 4 日

作業時間 12 : 42 - 18 : 17

	開始時刻	終了時刻
1. 金庫鍵搬送～作業場所への集合	12 : 42	13 : 27
2. 金庫の開放	13 : 38	13 : 57
3. KSK/ZSK操作用PCのセットアップ	14 : 04	14 : 16
4. KSK管理用記憶媒体の初期設定	14 : 19	14 : 34
5. KSK鍵ペアの生成	14 : 48	15 : 04
6. DSの生成	15 : 06	15 : 14
7. ZSK鍵ペアの削除	15 : 17	15 : 25
8. ZSK鍵ペアの署名	15 : 27	15 : 40
9. 署名済みZSK公開鍵の.jpゾーン署名サーバへの格納	16 : 00	16 : 46
10. 管理情報の複製	16 : 51	17 : 01
11. KSKロールオーバー期間中の管理情報の複製	17 : 06	17 : 30
12. 金庫の施錠	17 : 31	17 : 52
13. メインサイト作業解散 金庫鍵搬送	18 : 07	-

以上の作業が手順書どおり行われたことを確認しました。

立会人

立会人

責任者

坂田 博文



<http://jprs.jp/info/notice/20111006-keyceremony.html>

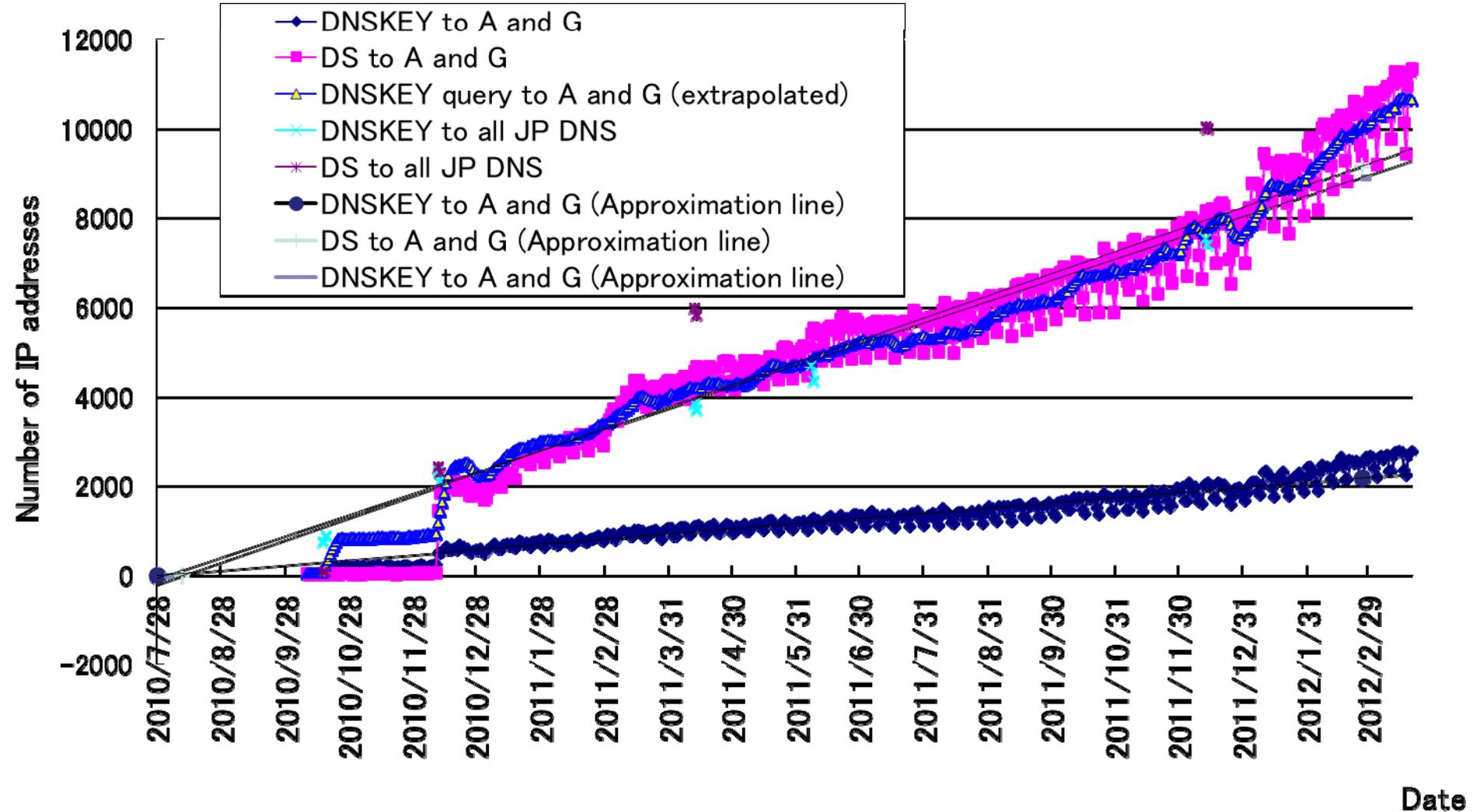
JPRSのDNSSEC関連活動(1/2)

- DNSSEC validator数の計測
 - JP DNSに来るDNSKEYとDSのクエリを計測
 - validatorの可能性のあるIPアドレスが一日あたりで約1万
 - 計測当初より徐々に増加の傾向

Number of possible DNSSEC Validators seen at JP, 1 year difference
(2012-03 IEPGミーティング @パリ、JPRS藤原)
<http://iepg.org/2012-03-ietf83/>

DNSSEC validator数の推移

(2012-03 IEPGミーティング資料より)



JPRSのDNSSEC関連活動(2/2)

- DNS本出版

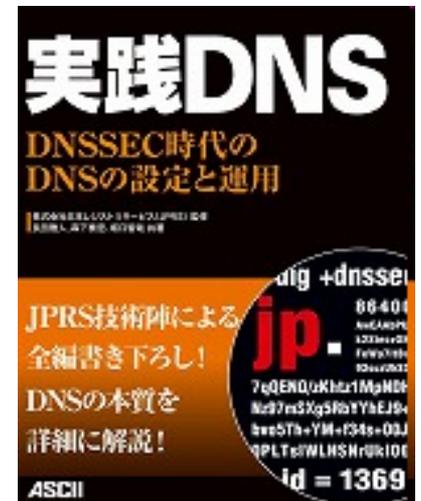
「実践DNS – DNSSEC時代のDNSの設定と運用」

2011-05-27 アスキー・メディアワークス発行

著者：民田雅人、森下泰宏、坂口智哉

ISBN: 978-4-04-870073-3

<http://jprs.co.jp/publish/> (正誤表あり)



まとめ

- ルートおよびJPがDNSSEC対応してから1年以上経過し、定常運用が安定した
 - 年間に発生するイベントを一通り経験
 - ★JPはKSKロールオーバーを経験
- DNSSEC検証を行うキャッシュサーバも徐々に増加の様相

(参考) Root KSK Ceremony実施日

回	開催日	開催場所	ZSKへの署名期間
1	2010-06-16	Culpeper	2010-07-01 / 2010-10-05
2	2010-07-12	El Segundo	2010-10-01 / 2011-01-05
3	2010-11-01	Culpeper	2011-01-01 / 2011-04-05
4	2011-02-07	El Segundo	2011-04-01 / 2011-07-05
5	2011-05-11	Culpeper	2011-07-01 / 2011-10-05
6	2011-07-20	El Segundo	2011-10-01 / 2012-01-05
7	2011-09-30	Culpeper	2012-01-01 / 2012-04-05
8	2012-02-02	El Segundo	2012-04-01 / 2012-07-05
9 ※	2012-05-22	Culpeper	2012-07-01 / 2012-10-05
10 ※	2012-07-26	El Segundo	2012-10-01 / 2013-01-05

- Culpeper ICANNの米国東海岸(バージニア州)の設備
- El Segundo ICANNの米国西海岸(カリフォルニア州)の設備

※ 9, 10回は予定