JP DNS Update

2011年11月30日
Internet Week 2011　DNS DAY

株式会社日本レジストリサービス

あはれん　よしたか
阿波連　良尚

目次

- JP DNSとは
- 統計情報
  - JPドメイン名登録数
  - JP DNSへのクエリ数の増加傾向
- トピックス
  - JPドメイン名のDNSSECサービス開始
  - DNS応答サイズの削減
  - BIND 9.xの脆弱性（CVE-2011-2464）

JP DNSとは

1. JP DNSとは

- JPゾーンを管理するDNSサーバ
  - JPRSが登録管理しているJPゾーンを提供
  - JPNICが割り振りを管理している一部のIPアドレスブロックの逆引きゾーンも提供（C.DNS.JPを除く）
- JP DNSサーバの構成

※http://www.dns.jp/ より引用

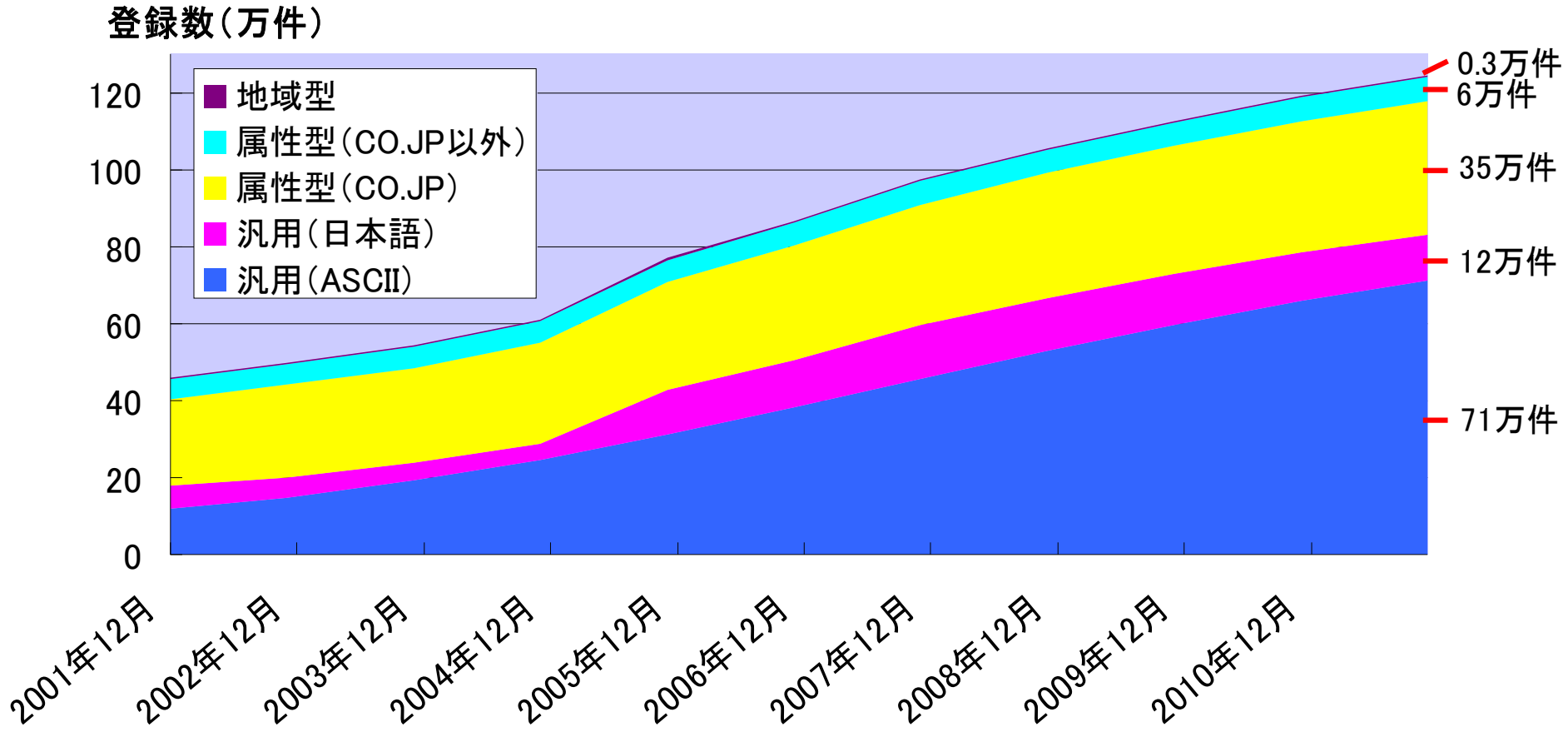
サーバ	運用組織	ネットワーク	管理ゾーン
A.DNS.JP	JPRS	IPv4/IPv6 + Anycast	JP, 逆引き
B.DNS.JP	JPNIC	IPv4/IPv6	JP, 逆引き
C.DNS.JP	JPRS	IPv4/IPv6 + Anycast	JP
D.DNS.JP	IIJ	IPv4/IPv6 + Anycast	JP, 逆引き
E.DNS.JP	WIDE Project	IPv4/IPv6 + Anycast	JP, 逆引き
F.DNS.JP	NII	IPv4/IPv6	JP, 逆引き
G.DNS.JP	JPRS	IPv4	JP, 逆引き

10/17
リナンバ

統計情報

2. 統計情報 –JPドメイン名登録数-

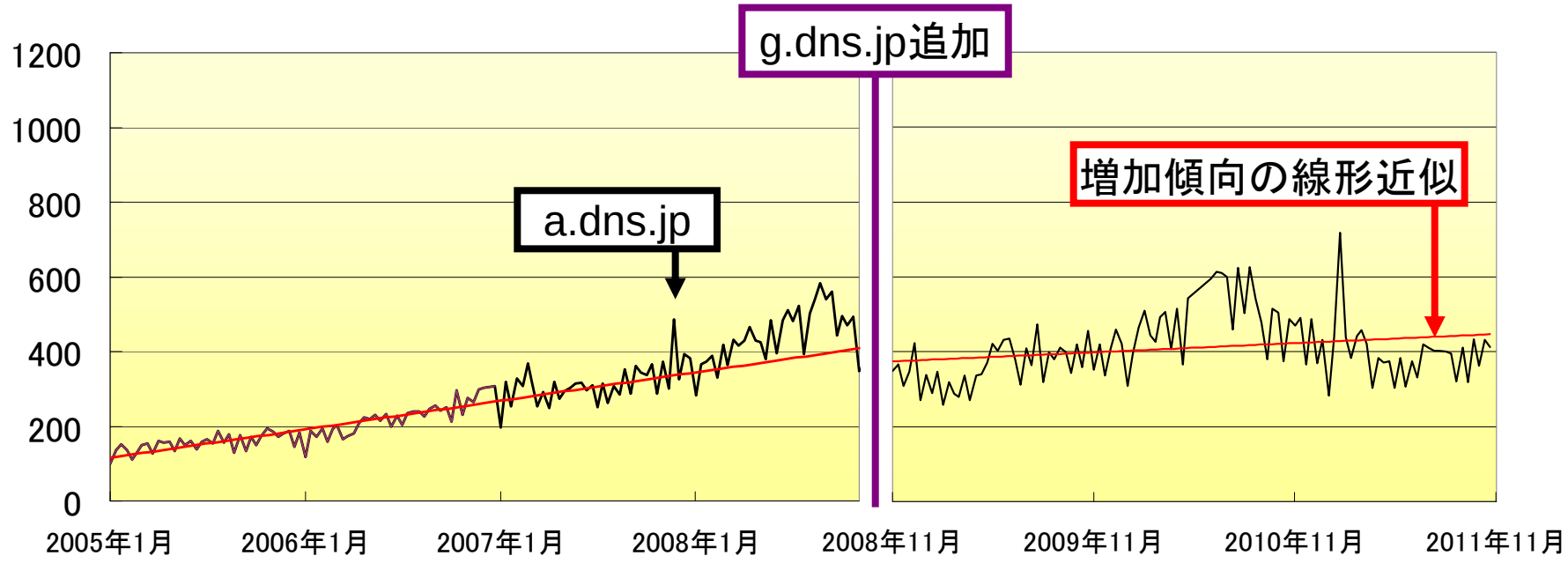
2011年11月1日現在：約124万件



出典：http://jpinfo.jp/stats/domains.html

2. 統計情報 –クエリ数の増加傾向-

伸び率（%） 2005年1月のa.dns.jpへのクエリ数を100とした伸び率と予測



- g.dns.jpの追加や2010年8月のネットワーク構成変更により、a.dns.jpへのクエリの増加傾向は緩やかになったが、全体としては引き続き増加傾向にある

トピック1

DNSSECサービス開始

これまでの流れ

2010年

10/4	第1回 .jp DNSSEC キーセレモニー実施
10/17	.jpゾーンのDNSSEC署名を開始
12/10	ルートゾーンに.jpゾーンのDSレコードを登録し、信頼の連鎖が構築される

2011年

1/16	JPドメイン名のDNSSECサービス開始
6/18	DNSKEYレコードへの署名内容の変更（後述）
7/7	ZSK公開個数の変更（後述）
10/4	第2回 .jp DNSSEC キーセレモニー実施
10/7～11/4	.jpゾーンで初のKSKロールオーバー実施

DNSSECサービス開始

- 2011年1月16日より、JPドメイン名に対する指定事業者からのDSレコードの登録申請受付を開始
- jprs.jp、jprs.co.jpはDNSSEC署名済
  - DNSSECの検証機能を有効にしたキャッシュDNSサーバ（バリデータ）で検証可能

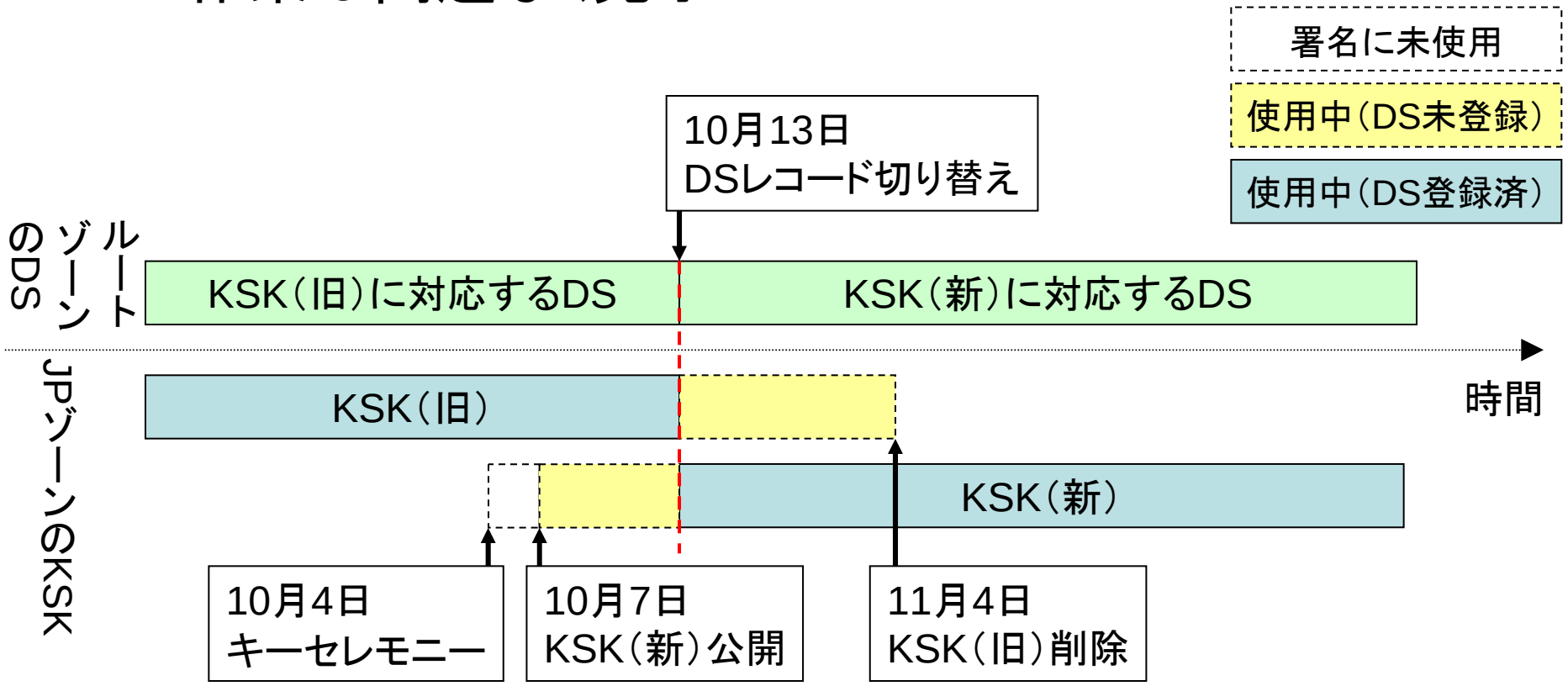
第2回 .jp DNSSECキーセレモニー

- 2011年10月4日実施
  - 「JPドメイン名におけるDNSSEC運用ステートメント（JP DPS）★」に基づき、年次でKSKを作成
  - 第1回は2010年10月4日に実施
  - WIDEの加藤朗氏、ICANNの大久保智史氏が立会人として参加

★: https://jprs.jp/doc/dnssec/jp-dps-jpn.v1.1.html

KSKのロールオーバー

- .jpゾーンでは初めてのKSKロールオーバー
  - 作業は問題なく完了

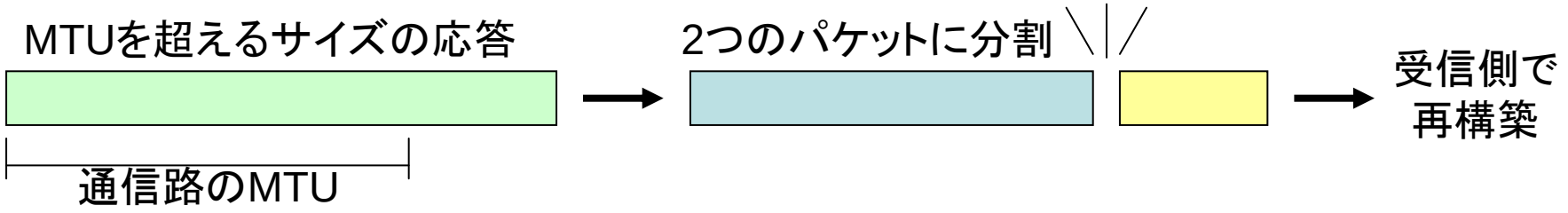


トピック2

DNSKEYの応答サイズ削減

DNSKEYレコードの応答

- DNSKEYレコードに対する応答には、ZSK・KSKの公開鍵とその署名が含まれる
- ロールオーバーの時期には、鍵の個数が増えるため応答サイズが大きくなる
- 応答サイズが大きいと、IPパケットが分割される可能性が大きくなる
  - MTU（最大転送単位）が小さい環境では、何らかの悪影響が出る可能性がある



削減内容(1)DNSKEYレコードへの署名内容の変更

- ZSKによるDNSKEYレコードへの署名を廃止
  - 以前は、KSKだけでなくZSKでもDNSKEYレコードを署名していた
  - DNSSECの検証に実害はない
  - dnssec-signzoneコマンドのオプション”-x”で制御できる

削減内容（2）ZSK公開個数の変更

- .jpゾーンで公開するZSKの数を削減
  - ZSKの公開タイミングを変更し、ZSK公開個数を常時2つにした
  - KSKロールオーバー期間中は、ゾーン署名に利用されているZSK（1つ）のみ公開するよう設定

DNSKEYの応答内容の比較

KSKロールオーバー期間中

削減前

応答サイズ（IPヘッダ除く） 1,769octet

ほとんどの環境で
IPパケット分割が発生

削減後

応答サイズ（IPヘッダ除く）: 1,311octet

DNS応答サイズを削減することで、
IPパケットの分割を抑制

トピック3

BIND 9.xの脆弱性

（CVE-2011-2464）

DoS攻撃が可能な脆弱性（CVE-2011-2464）

- 危険度が高い
  - 特殊に作成したDNSパケットにより、リモートからnamedを異常終了させることが可能
- 影響範囲が広い
  - BIND 9系の多くのバージョンが対象
  - キャッシュDNSサーバ・権威DNSサーバの双方が対象で、外部に公開しているサーバにおける回避策なし
- 2011年7月5日に、JPRSからも情報を公開して注意喚起
  - JP DNSの全ノードは、影響を受けないバージョンに更新済

- 影響を受けるバージョンをお使いの方は、**速やかに**バージョンアップを行うことを**強く**推奨します

Q and A