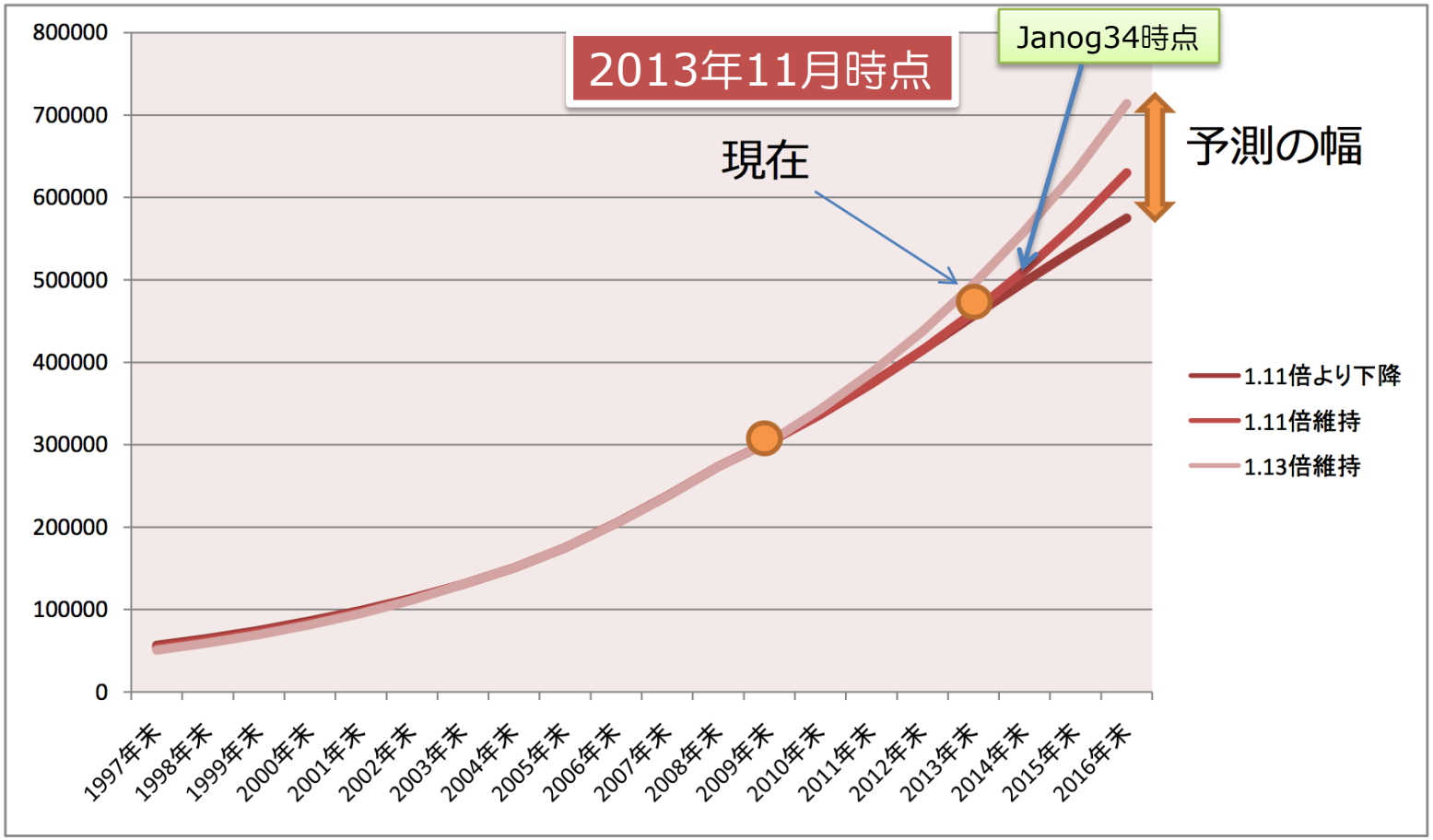
ルーティングテーブルを覗きたい
～BGP経路解析とBMPの使い道～

インターネットマルチフィード（株）
吉田友哉 yoshida@mfeed.ad.jp

Agenda

- BGPの (プチ)トレンド
- BMPが無かった時代にやっていたこと
- JPNAPのルートサーバで今やっていること
- トラブル解析にあたり念頭におくこと
- BMPの使い方（主にディスカッション）
- おまけ

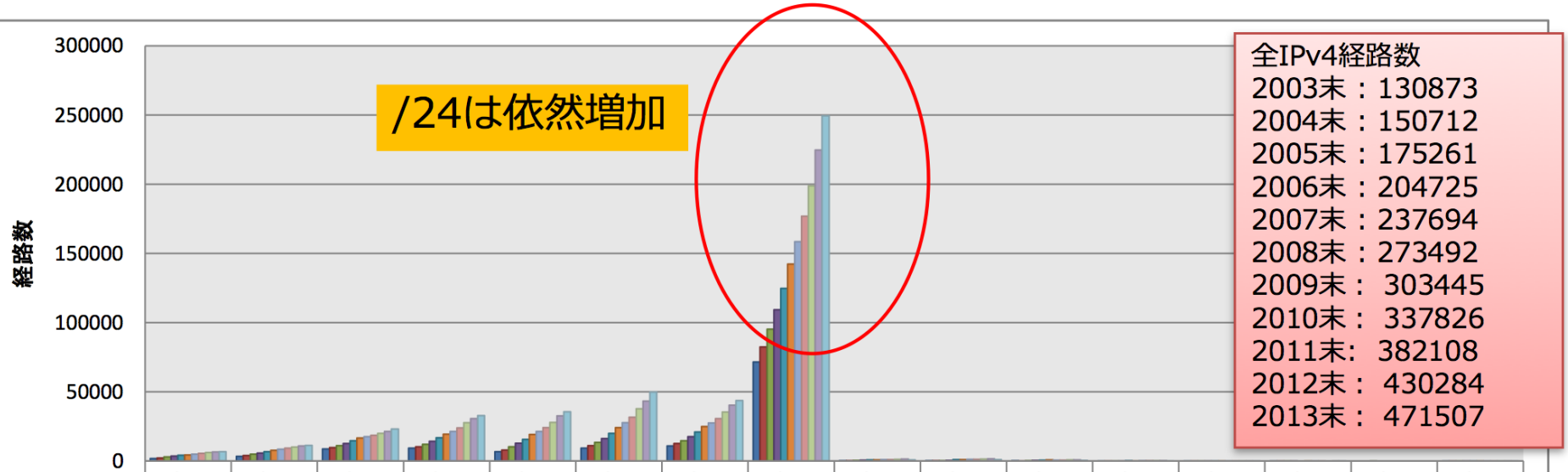
IPv4経路数推移予測
(4年前の2009年末予測)



2011年、2012年は枯渇後もほぼ従来相当の増加傾向
枯渇要因は来年あたりから顕著に見られる可能性があり

2013年11月 InternetWeek2013 IP Meeting 資料より

IPv4経路数の推移

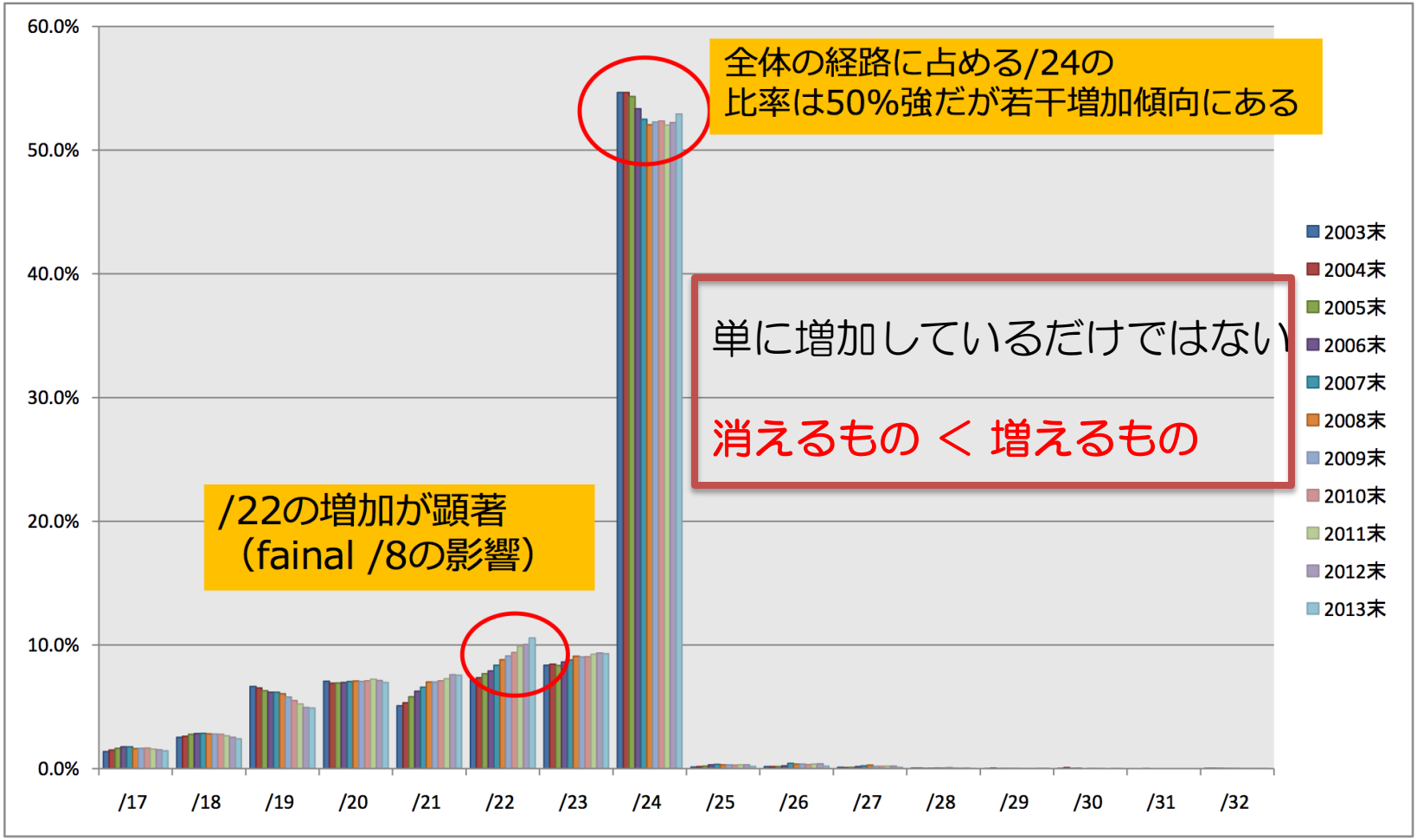


全IPv4経路数
2003末：130873
2004末：150712
2005末：175261
2006末：204725
2007末：237694
2008末：273492
2009末： 303445
2010末： 337826
2011末: 382108
2012末： 430284
2013末： 471507

	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
2003末	1829	3334	8716	9249	6656	9386	10943	71541	182	233	156	70	21	50	0	41
2004末	2270	3933	9818	10402	8007	11066	12707	82382	252	239	130	69	54	120	0	40
2005末	2880	4871	11026	12142	10194	13440	14626	95225	345	292	194	26	12	36	3	30
2006末	3625	5826	12664	14281	12838	16203	17682	109219	658	468	364	69	44	80	0	31
2007末	4192	6767	14670	16753	15656	19873	20885	124763	814	1013	544	114	5	0	0	8
2008末	4444	7678	16540	19394	19123	24098	24829	142338	831	1000	798	92	9	1	0	7
2009末	4977	8507	17591	21348	21260	27614	27395	158588	955	1128	565	224	11	8	0	8
2010末	5584	9343	18618	23987	24029	31706	30591	176852	992	1102	585	151	12	2	0	7
2011末	6065	10115	19979	27645	27788	37839	35374	198775	1148	1364	762	166	4	0	0	5
2012末	6533	10880	21269	30693	32699	43237	40249	224766	1356	1689	903	181	79	17	0	24
2013末	6761	11348	23134	32798	35561	49863	43778	249471	880	1002	477	50	79	20	0	14

2013年11月 InternetWeek2013 IP Meeting 資料より

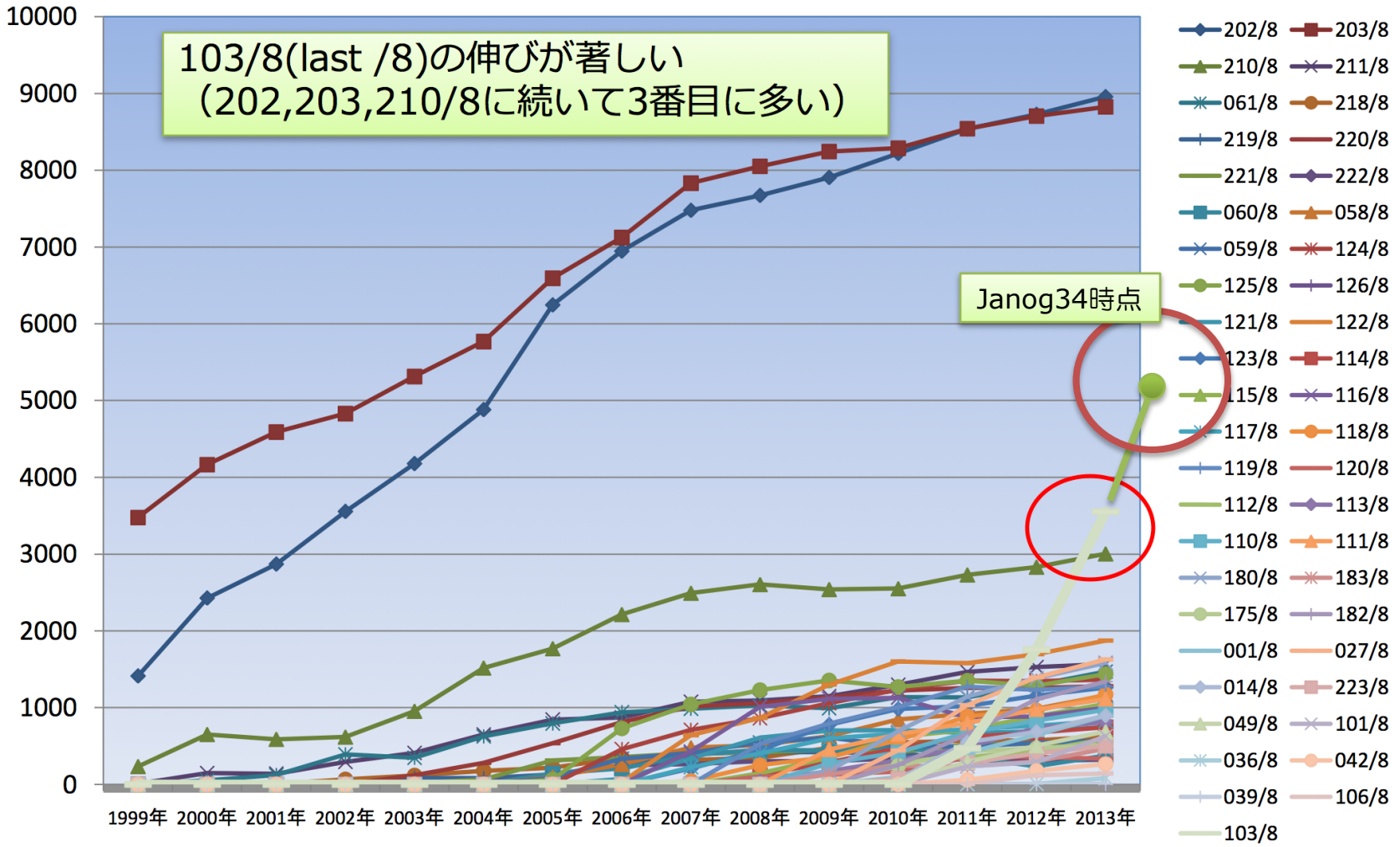
IPv4経路数の推移（割合）



2013年11月 InternetWeek2013 IP Meeting 資料より

AP地域の/24の推移

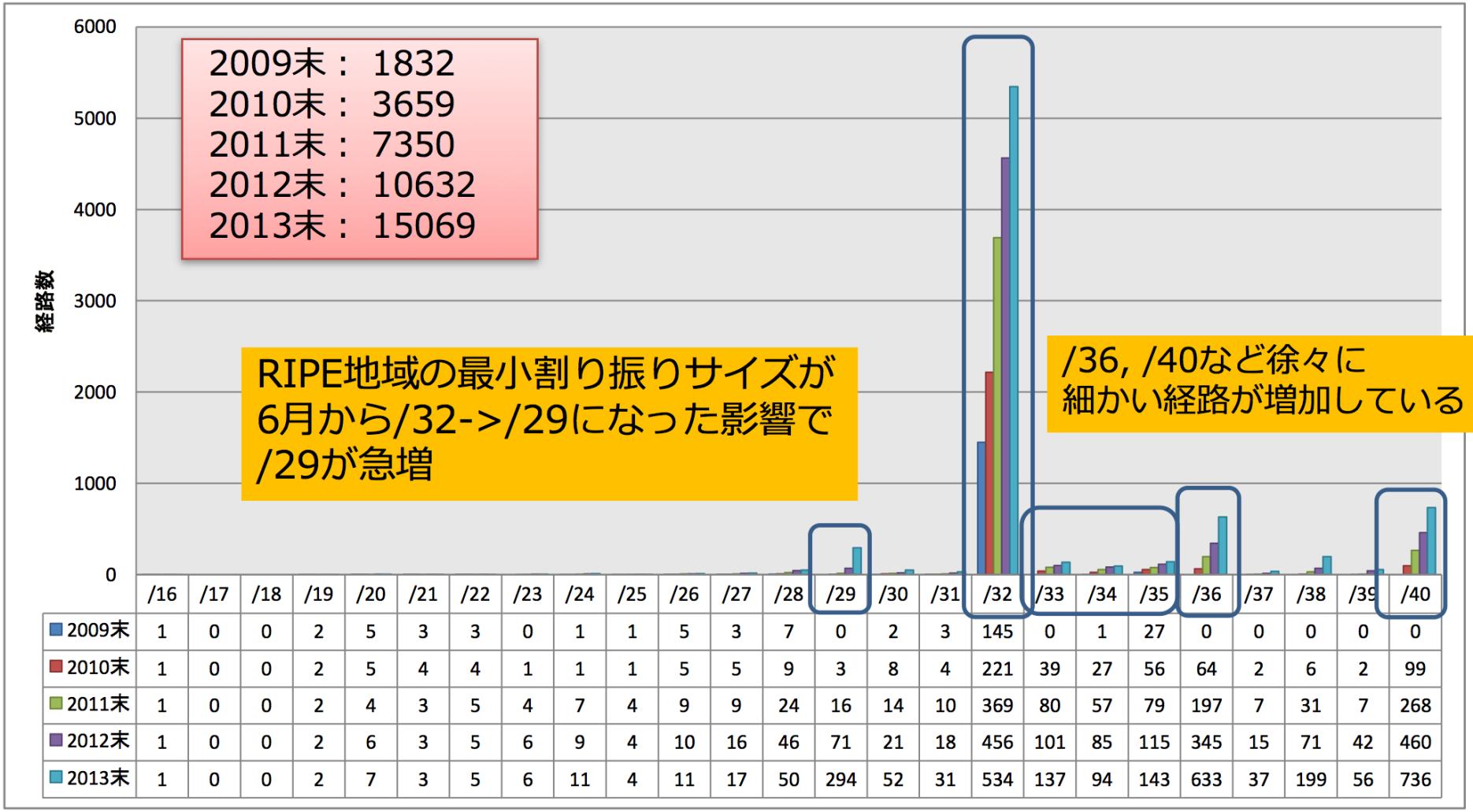
103/8の範囲の/24の数が急増している



2013年11月 InternetWeek2013 IP Meeting 資料より

47

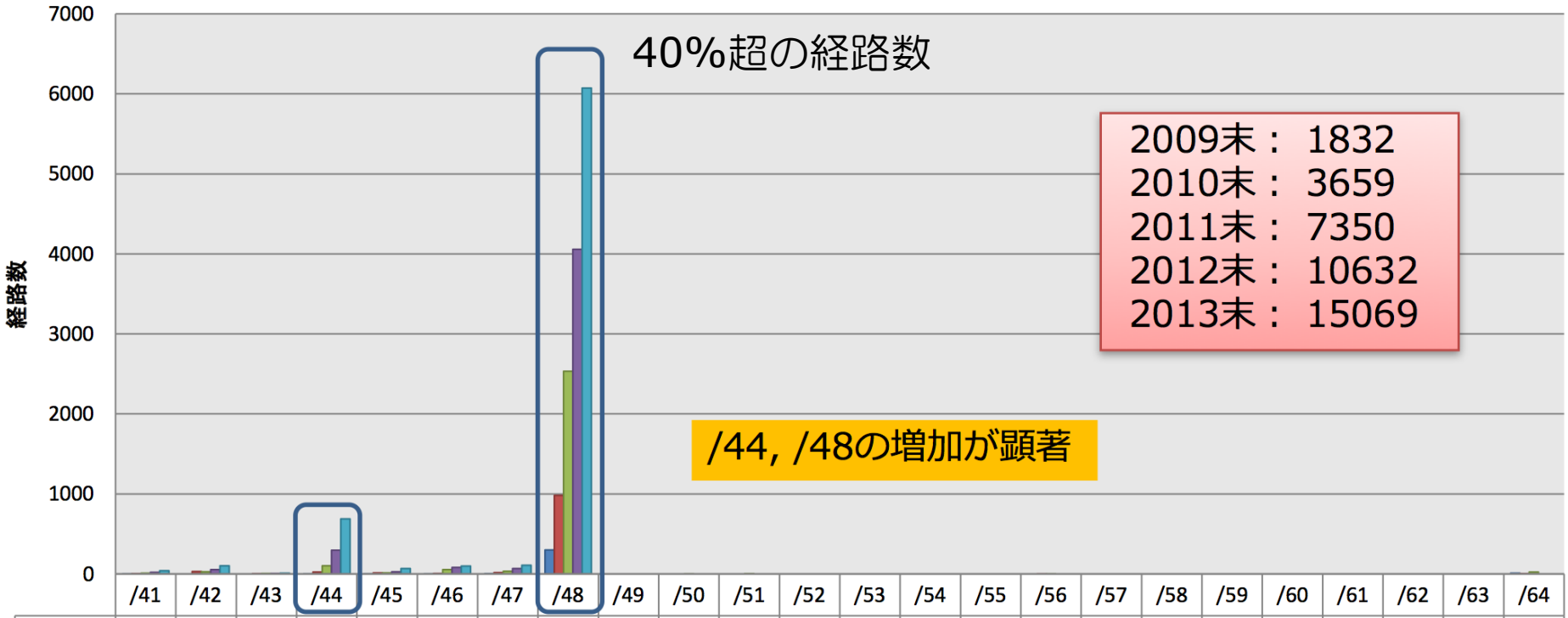
IPv6経路数の推移



	/16	/17	/18	/19	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32	/33	/34	/35	/36	/37	/38	/39	/40
2009末	1	0	0	2	5	3	3	0	1	1	5	3	7	0	2	3	145	0	1	27	0	0	0	0	0
2010末	1	0	0	2	5	4	4	1	1	1	5	5	9	3	8	4	221	39	27	56	64	2	6	2	99
2011末	1	0	0	2	4	3	5	4	7	4	9	9	24	16	14	10	369	80	57	79	197	7	31	7	268
2012末	1	0	0	2	6	3	5	6	9	4	10	16	46	71	21	18	456	101	85	115	345	15	71	42	460
2013末	1	0	0	2	7	3	5	6	11	4	11	17	50	294	52	31	534	137	94	143	633	37	199	56	736

2013年11月 InternetWeek2013 IP Meeting 資料より

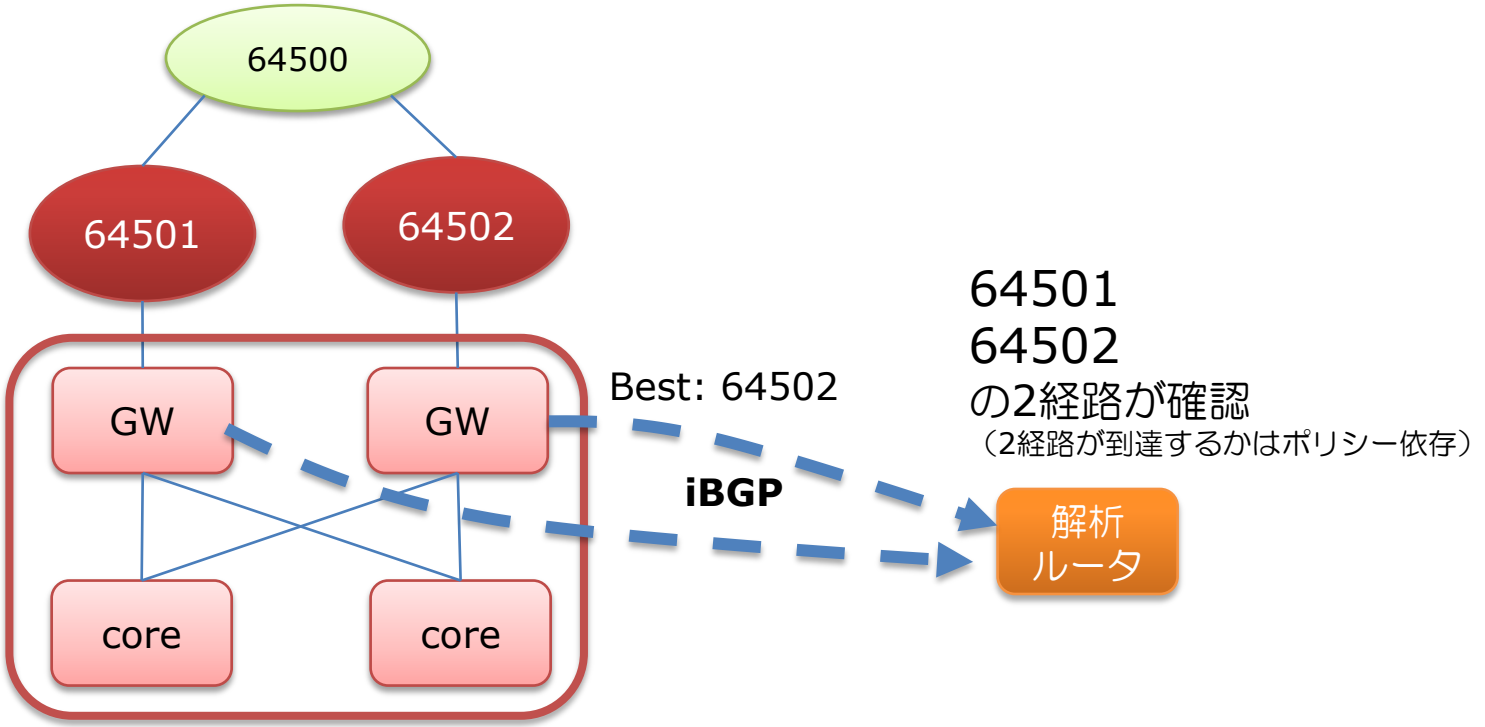
IPv6経路数の推移



	/41	/42	/43	/44	/45	/46	/47	/48	/49	/50	/51	/52	/53	/54	/55	/56	/57	/58	/59	/60	/61	/62	/63	/64
2009末	1	0	0	1	1	2	3	300	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	10
2010末	5	30	3	24	15	9	18	984	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	5
2011末	10	27	8	104	13	57	36	2534	0	1	3	0	0	0	0	1	0	0	0	0	0	0	0	26
2012末	21	55	8	298	27	81	69	4057	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2013末	42	102	10	688	68	100	109	6072	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

BMPが無かった時代にやっていたこと

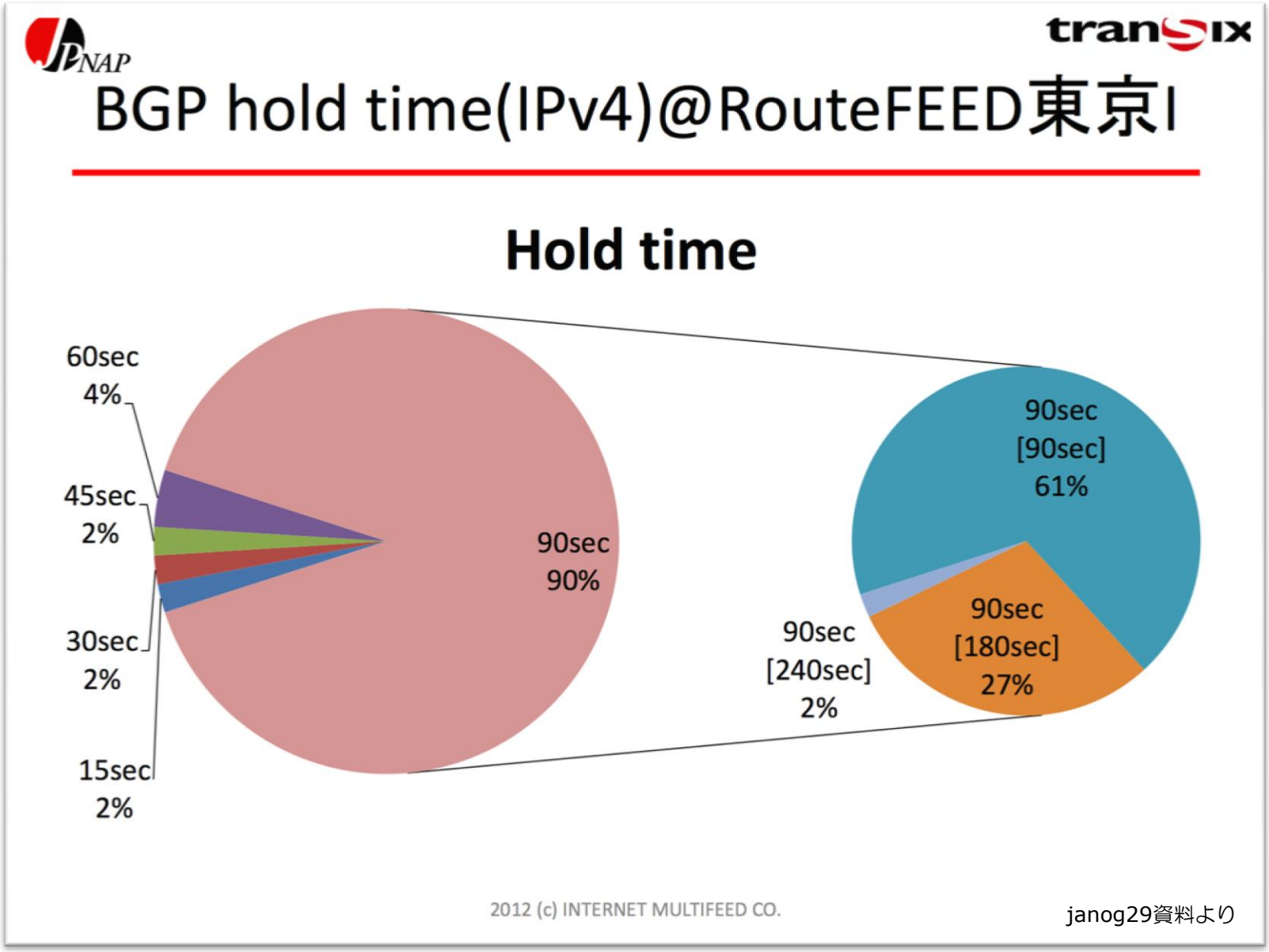
- GWからiBGP peerを解析ルータに設定
  - 自ASに流入される、なるべく多くのBGP(best)経路を収集する
    - BGP multipath 利用時に、coreでは複数ルートが見えているけど１経路しかbestにならないので、GWでの収集がbetter
  - 特定の経路ポリシー変更後にどうなるか
  - 解析ルータで経路が一元的に確認可能なので便利



現在JPNAPのルートサーバで収集しているBGP情報

- JPNAPのルートサーバではBGP updateをフルパケットキャプチャ
  - 何かあったときの解析用
  - Openメッセージでやり取りされる、BGP capabilityやholdtimeなどの各種パラメータなども拾いたい
- BMPでも見れるとは思う
  - でも全部(パケットとして真実を)とっておきたい病…

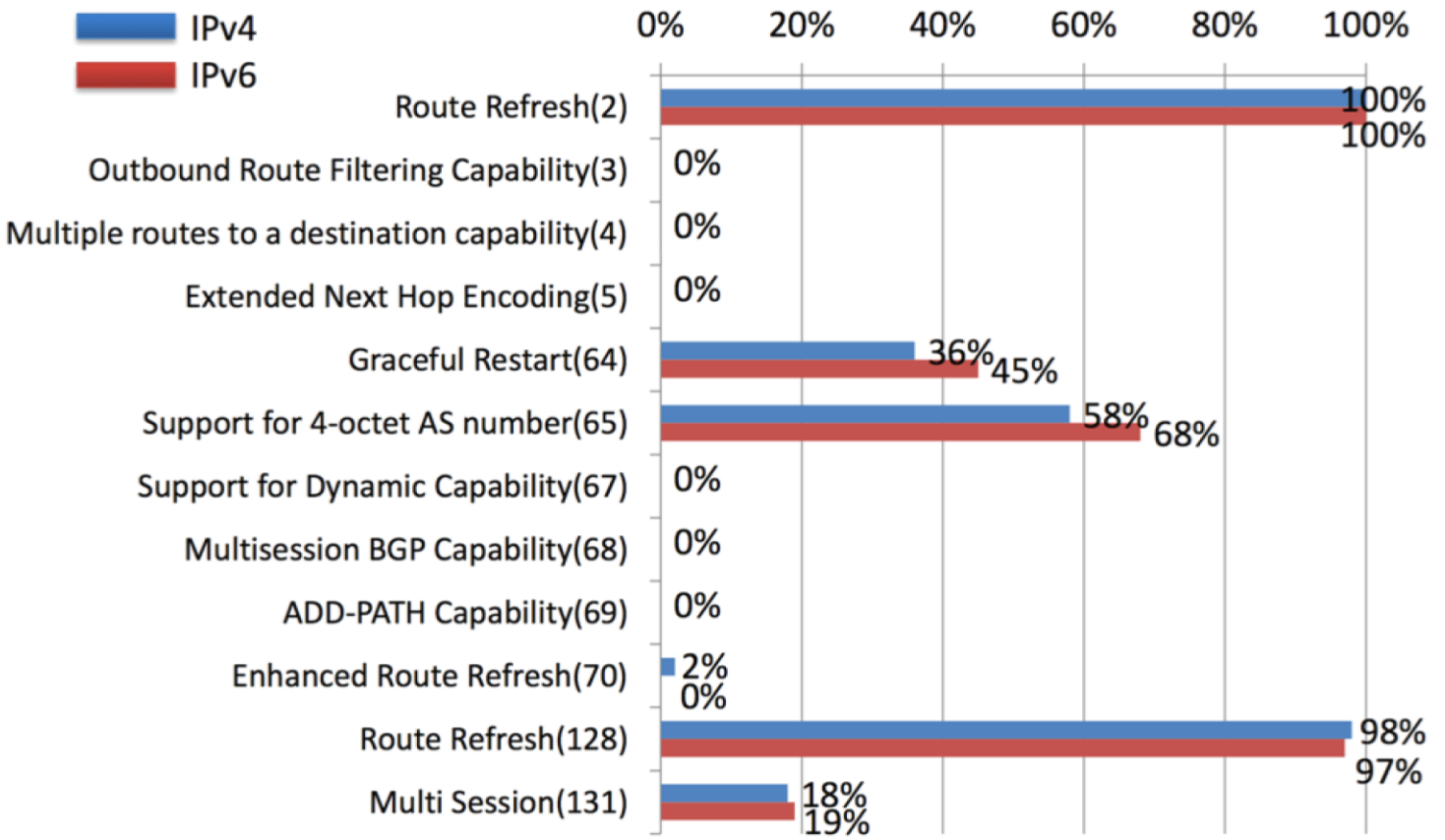
BGP hold time



janog29資料より

BGP Capability

BGP Capability(IPv4/IPv6) @ RouteFEED東京I



2012 (c) INTERNET MULTIFEED CO.

janog29資料より

トラブル解析にあたって考えるべきこと

- BGPのモニターはルーティング解析の一部
  - OSPFのLSDBを眺めておく等の必要がある
  - RouteExplorerとかospfviewとか
    - 各エリア毎に代表ルータからospf neighborが張れると理想的
      たまに幽霊LSAなども存在するので解析に有用
- ルータの時刻が合っていることが大事
  - BMPのtimestampを使うなら必須
  - 一般的に時刻の精度はトラブル解析に重要
- パケットの到達性確認と連動した経路解析
- BMPパケットを収集するNWはBGP非依存がよい

経路情報とパケットの到達性確認

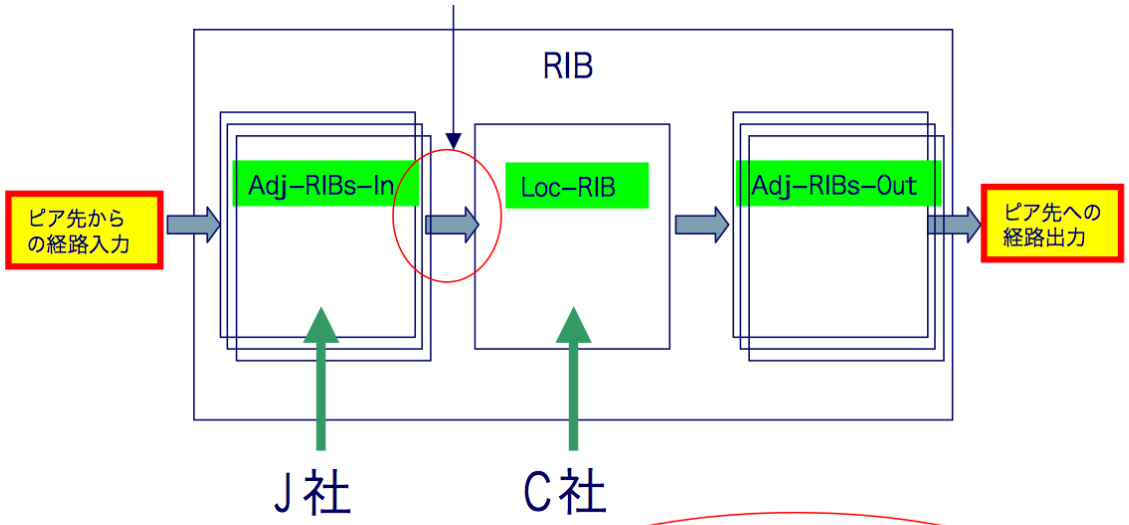
- 通信できていたのか、否か
  - パケットの到達性確認がまずは大事
  - その後原因究明と再発防止
- 自分の経路と他人の経路
  - 自分の経路が適切に世の中でハンドリングされてるか
  - 他人の経路を自分が適切にハンドリングできているか

便利そうなBMPをどう使う？

- Vendor freeなBMPは基本素敵だなと
- GW？特定のルータのみBMP？IBGPは？
- 運用フローにどう組み込むとよい？
- フルルート運用に耐えうる？ルータの性能や取り漏れは？
- ルータにログインしなくてすめば嬉しいけど…
- 個人的にはまずは記録簿として利用するのかな
- 情報が整理されて表示や検索が出来ると嬉しい
- BMP filterって可能？（特定regexpのみBMP）
- max-prefix運用での適応
  - Thresholdの手前でwarningメッセージが欲しい
    - なので完全にsyslogの代替には成らないのでは？

max-prefix

BGP Max Prefix、Prefix Limit



max-prefix以外のFilterを適応している場合には、その該当Filter適応後に、上限値を超えている場合には、limit制限がかかる

そもそも各社でどのRIBを見てmax-prefixを適応するかの違いがあるので要注意。自分は落ちる前に気づきたい

2005/12/7 Copyright © 2005 Tomoya Yoshida 150

https://www.nic.ad.jp/ja/materials/iw/2005/proceedings/T14.pdf

便利そうなBMPをどう使う？

- Vendor freeなBMPは基本素敵だなと
- GW？特定のルータのみBMP？IBGPは？
- 運用フローにどう組み込むとよい？
- フルルート運用に耐えうる？ルータの性能は？取り漏れは？
- ルータにログインしなくてすめば嬉しいけど…
- 個人的にはまずは記録簿として利用するのかな
- 情報が整理された表示できたり検索できたりするとうれしい
- BMP filterって可能？（特定regexpのみBMP）
- max-prefix運用での適応

おまけ：最近きになっていること

- プライベートアドレスの利用が拡大されてtracerouteが戻りにくくなっている。トラブルシュートしにくい
- 昔はアドレスを見ると地域がわかったが今後はそうもいかなくなる
- IPv4の1経路あたりのトラフィックが増大
- short ribed bgp + SPAM送信は身近にある
- RPKIがとあるところで突然適応されると、突然到達性が失われる可能性がある
  - multiple originの経路や、パンチングホールの経路は要注意