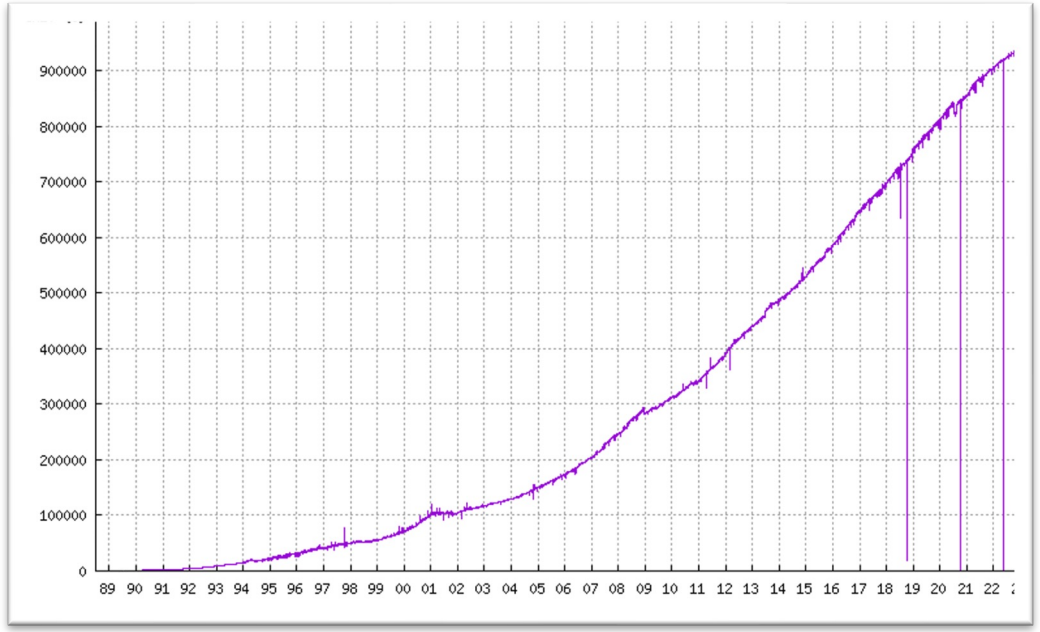
BGP運用

先に進む一歩

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

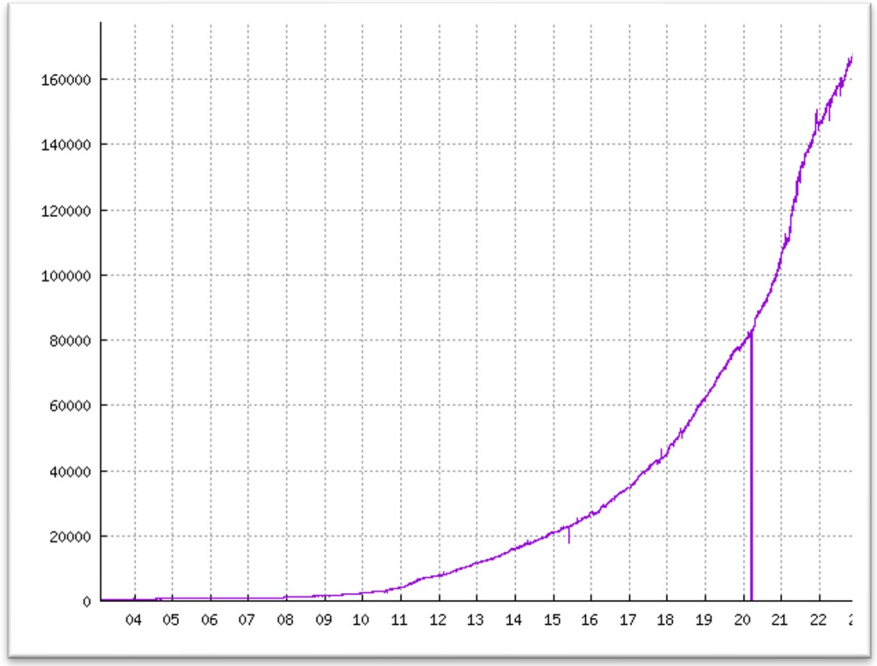
BGP経路数増え続けてますね

IPv4 90万経路越え



https://bgp.potaroo.net/as2.0/bgp-active.htmlより

IPv6 15万経路越え



https://bgp.potaroo.net/v6/as2.0/index.html より

マスク長別のBGP経路数 IPv4

https://www.iij.ad.jp/dev/report/iir/057.html より

年月	/8	/9	/10	/11	/12	/13	/14	/15	/16	/17	/18	/19	/20	/21	/22	/23	/24	total
2013年9月	16	11	30	93	250	480	903	1613	12748	6652	10971	22588	32202	34900	48915	42440	244822	459634
2014年9月	16	12	30	90	261	500	983	1702	13009	7013	11659	24527	35175	37560	54065	47372	268660	502634
2015年9月	18	13	36	96	261	500	999	1731	12863	7190	12317	25485	35904	38572	60900	52904	301381	551170
2016年9月	16	13	36	101	267	515	1050	1767	13106	7782	12917	25229	38459	40066	67270	58965	335884	603443
2017年9月	15	13	36	104	284	552	1047	1861	13391	7619	13385	24672	38704	41630	78779	64549	367474	654115
2018年9月	14	11	36	99	292	567	1094	1891	13325	7906	13771	25307	39408	45578	88476	72030	400488	710293
2019年9月	10	11	37	98	288	573	1142	1914	13243	7999	13730	25531	40128	47248	95983	77581	438926	764442
2020年9月	9	11	39	100	286	576	1172	1932	13438	8251	14003	25800	40821	49108	101799	84773	473899	816017
2021年9月	16	13	41	101	303	589	1191	2007	13408	8231	13934	25276	41915	50664	106763	91436	497703	853591
2022年9月	16	13	39	101	298	592	1208	2064	13502	8292	13909	25051	43972	52203	109071	96909	536520	903760

- 大体/24経路の伸び
  - 新規メンバーへの分配がまだ継続中
  - 地域によって違うけどAPNIC地域だと最大/23

マスク長別のBGP経路数 IPv6

https://www.iij.ad.jp/dev/report/iir/057.html より

年月	/16-/28	/29	/30-/31	/32	/33-/39	/40	/41-/43	/44	/45-/47	/48	total
2013年9月	117	256	92	5249	1067	660	119	474	266	5442	13742
2014年9月	134	481	133	6025	1447	825	248	709	592	7949	18543
2015年9月	142	771	168	6846	1808	1150	386	990	648	10570	23479
2016年9月	153	1294	216	8110	3092	1445	371	1492	1006	14291	31470
2017年9月	158	1757	256	9089	3588	2117	580	1999	1983	18347	39874
2018年9月	168	2279	328	10897	4828	2940	906	4015	2270	24616	53247
2019年9月	192	2671	606	12664	6914	3870	1566	4590	4165	34224	71462
2020年9月	205	3164	641	14520	9063	4815	2663	5501	4562	45160	90294
2021年9月	223	3628	705	20650	13050	10233	4170	11545	5204	61024	130432
2022年9月	298	4247	895	21926	15147	12509	4108	13840	6994	73244	153208

- /64単位で数えると爆裂に増加中
  - /21-/30といった大きなブロックが増加
  - おそらく大規模な通信事業者がIPv6対応し始めた

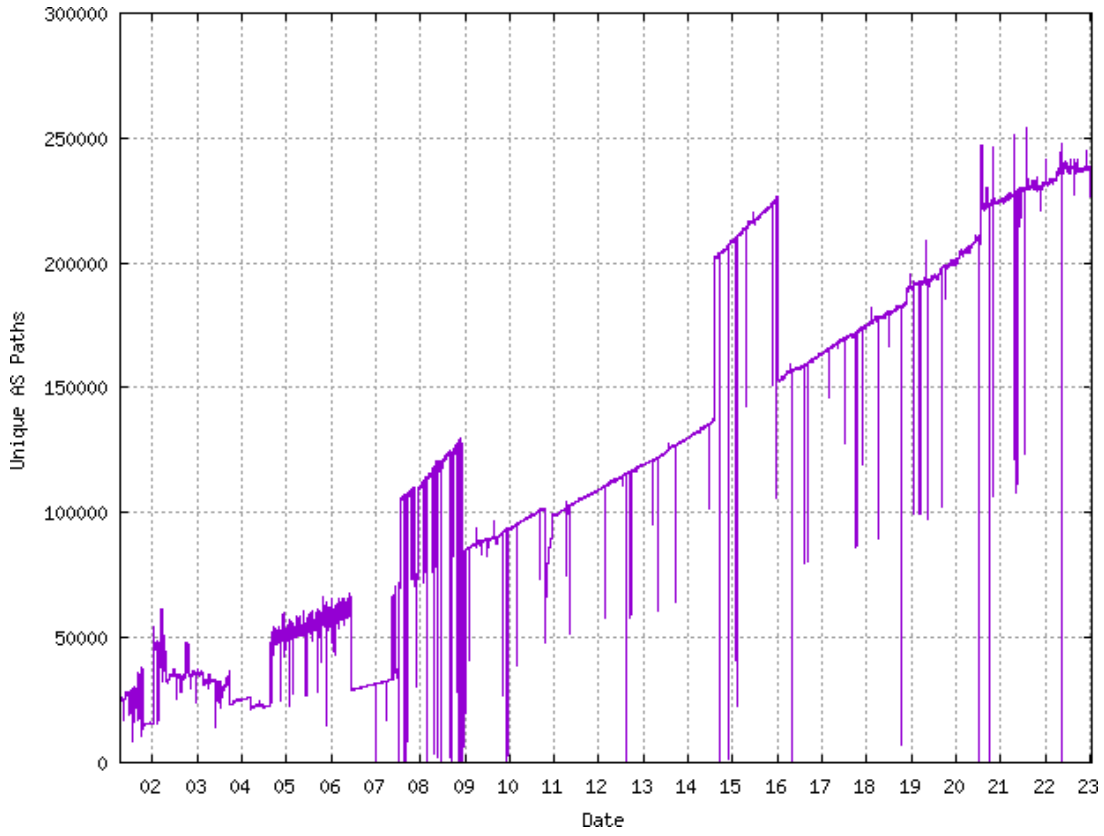
生きてるASの動向

https://www.iij.ad.jp/dev/report/iir/057.html より

AS番号	16-bit(1～64495)					32-bit only(131072～4199999999)				
広報経路	IPv4+IPv6	IPv4のみ	IPv6のみ	total	(IPv6 -enabled)	IPv4+IPv6	IPv4のみ	IPv6のみ	total	(IPv6 -enabled)
2013年9月	6579	34108	131	40818	(16.4%)	496	3390	28	3914	(13.4%)
2014年9月	7405	34555	128	42088	(17.9%)	868	4749	55	5672	(16.3%)
2015年9月	8228	34544	137	42909	(19.5%)	1424	6801	78	8303	(18.1%)
2016年9月	9116	33555	158	42829	(21.7%)	2406	9391	146	11943	(21.4%)
2017年9月	9603	32731	181	42515	(23.0%)	3214	12379	207	15800	(21.7%)
2018年9月	10199	31960	176	42335	(24.5%)	4379	14874	308	19561	(24.0%)
2019年9月	10642	31164	206	42012	(25.8%)	5790	17409	432	23631	(26.3%)
2020年9月	11107	30374	229	41710	(27.2%)	7653	19668	574	27895	(29.5%)
2021年9月	11465	29219	302	40986	(28.7%)	9514	21108	5242	35864	(41.1%)
2022年9月	11613	28398	369	40380	(29.7%)	10816	22211	5764	38791	(42.7%)

- IPv6対応は増加中
  - IPv6のみを広報するASも増えてきている
- 全体としては増加するものの、2022年はASの増減変化が少し鈍化

ユニークなAS_PATH数の傾向

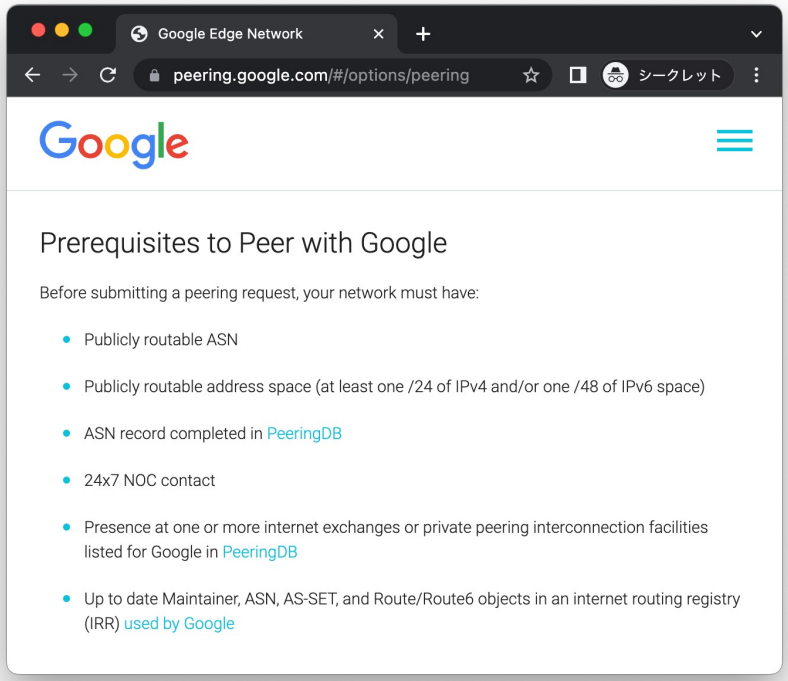


https://bgp.potaroo.net/as2.0/bgp-active.htmlより

- 比較的線形に増加
- 2020年以降増加が少し鈍化?

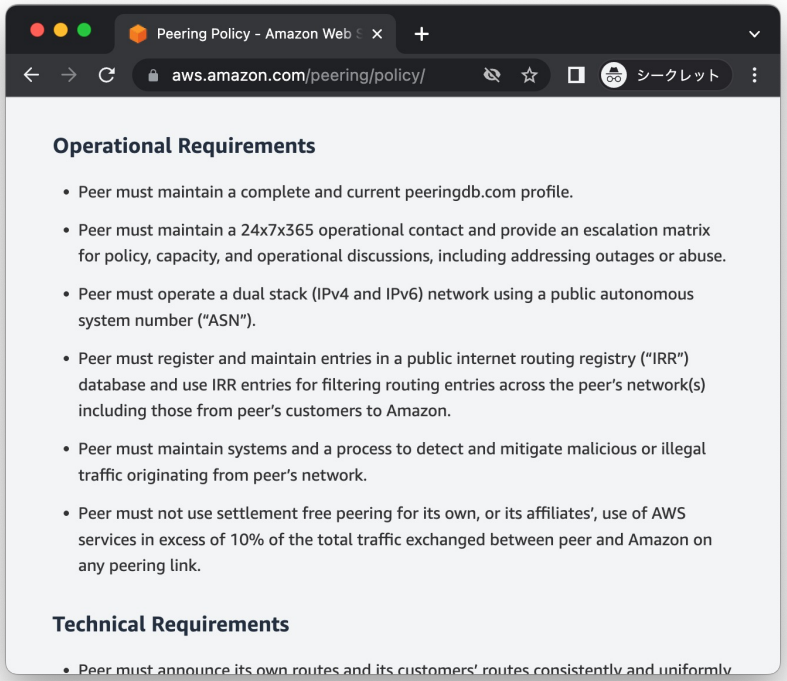
IRRへの登録が要求事項に入ってる

AS15169の場合



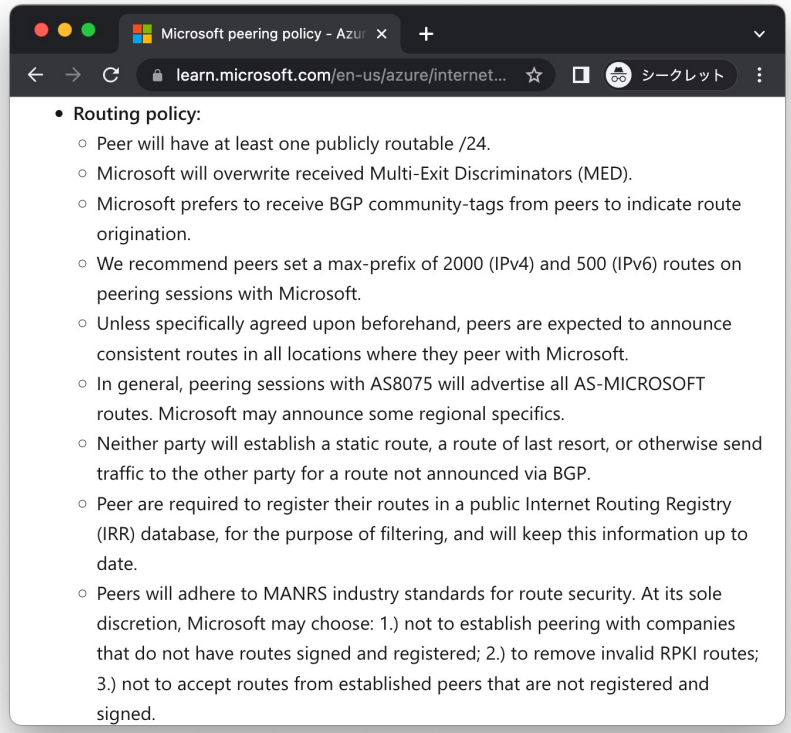
https://peering.google.com/#/options/peering

AS16509の場合



https://aws.amazon.com/peering/policy/

AS8075の場合



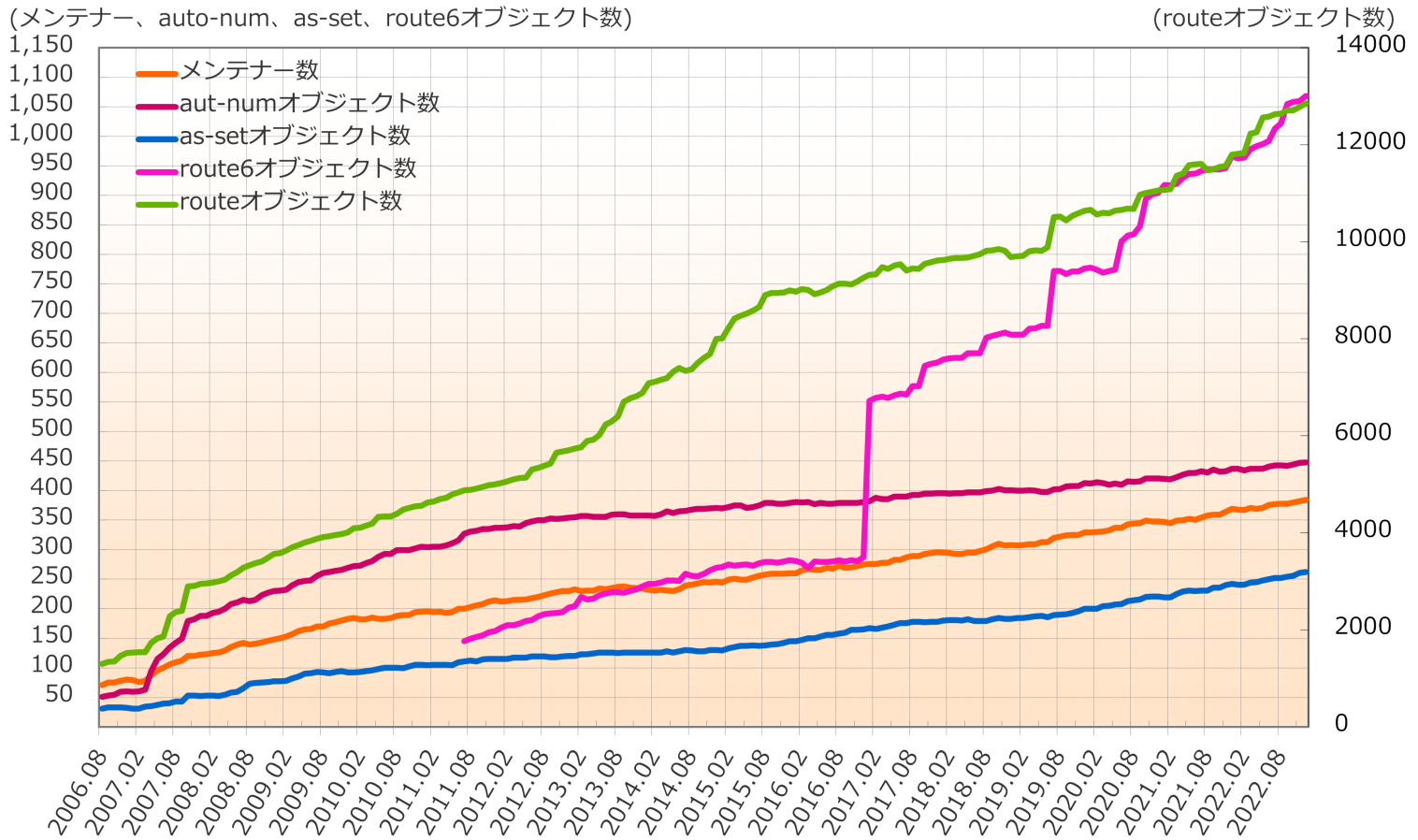
https://learn.microsoft.com/en-us/azure/internet-peering/policy

つまり、IRRに登録しているオブジェクトってAS運用にとって大事！

IRR（Internet Routing Registry）

- 経路制御ポリシーを登録して公開できるサービス
- as-set
  - 自ASを含めてトランジット対象のAS（広報するAS）を示すオブジェクト
  - 例：https://jpirr.nic.ad.jp/cgi-bin/search-object.pl?param=MAINT-AS2497
- route/route6
  - Prefixと広報元のASのペアを示すオブジェクト
  - 例：https://jpirr.nic.ad.jp/cgi-bin/search-object.pl?param=2001:240::/32
- mntner
  - 上記のオブジェクトなどを登録するため、認証情報などを記述できる管理用オブジェクト

みんな大体、JPIRR使うよね



https://www.nic.ad.jp/ja/stat/ip/ より

JPIRRで使える認証方式は二つだけ

- 登録、更新するには電子メールをJPIRRシステムに送信
  - 管理用オブジェクト(mntner)に認証方式(auth)を記載
  - authは複数書けて、どれかで認証できればOK

1. パスワード認証（CRYPT-PW認証）
   - 平文パスワードを申請メールに記載して送信
2. PGP認証（PGPKEY認証）
   - PGPで電子署名して申請メールを送信

JPIRRでみんなが使っている認証

- 大体みんなパスワード認証（CRYPT-PW認証）
  - 99%超がパスワード認証を有効にしている
- PGP認証で運用している人も（全体の1.4%ぐらい）
  - パスワード認証を併用してる人もいる(バックアップ用？)

- MAIL-FROM認証も書けるけど、JPIRRでは無視される模様
  - 2005年11月に廃止（JPNIC川端さん、情報ありがと）
  - 念の為、MAIL-FROMを書いている人は消しとくのが良いよ

認証の拠り所

- パスワード認証（CRYPT-PW認証）
  - 拠り所は共有パスワード、でも漏れやすい
  - 運用が大事
    - 申請者が変わったら、パスワードも変更しないとだめ？
    - 申請メールを見られると、パスワードが漏洩
- PGP認証（PGPKEY認証）
  - 拠り所はPGP秘密鍵＆鍵のパスフレーズ
  - みんな担当者個人のPGP鍵を登録している

- 可能であればPGP認証を利用するのが良い

ただし、PGP認証でも注意は必要

- 再送攻撃に脆弱
  - 昔の情報で上書きされる危険性がある
  - オブジェクトに毎回変わる何があれば良かったですね
- 継続的に変化しそうなのはas-setぐらい
  - route/route6は登録時からほぼ変わらない
  - mntnerもあんまり変わらない
- 検出は可能
  - 意図しない変更時にもJPIRRからメールが届く
  - notify/upd-to/mnt-nfy で指定した宛先

IRRの今後

- 認証どうしますか？

- ちなみに、他のIRRではWebベースの申請システムもあるみたい
  - RADB/APNICなどなど
- RADBのWeb UI使ってる人いますか？
  - アカウント管理どうしてます？

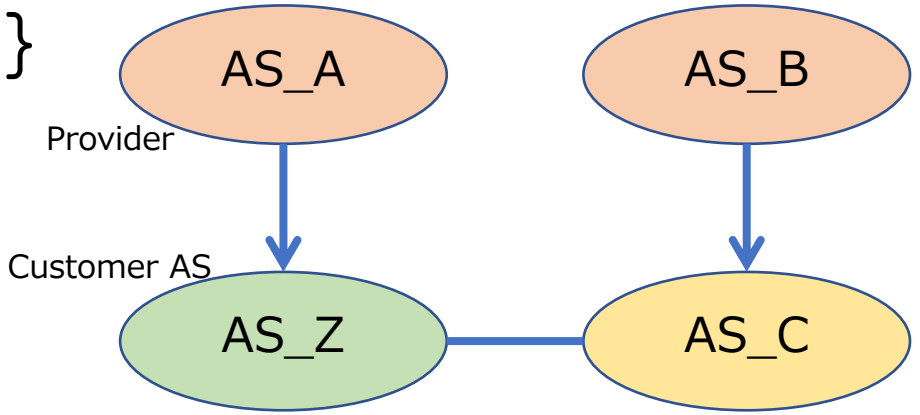
RPKI (Resource PKI)

- IPアドレスとかAS番号の分配を証明できる認証基盤
  - 分配に基づいてROAなどの電子証明書を発行できる
  - コンピュータで自動処理しやすい
- 経路制御に活用が広がりつつある
  - ROA → あるprefixの生成元ASを記載する証明書
    - IRRのroute/route6オブジェクトみたいなもの
  - ROAを収集して経路フィルタに適用
    - 間違った経路生成(Origin)ASからの経路を判別して破棄できる

ASPA（AS Provider Authorization）

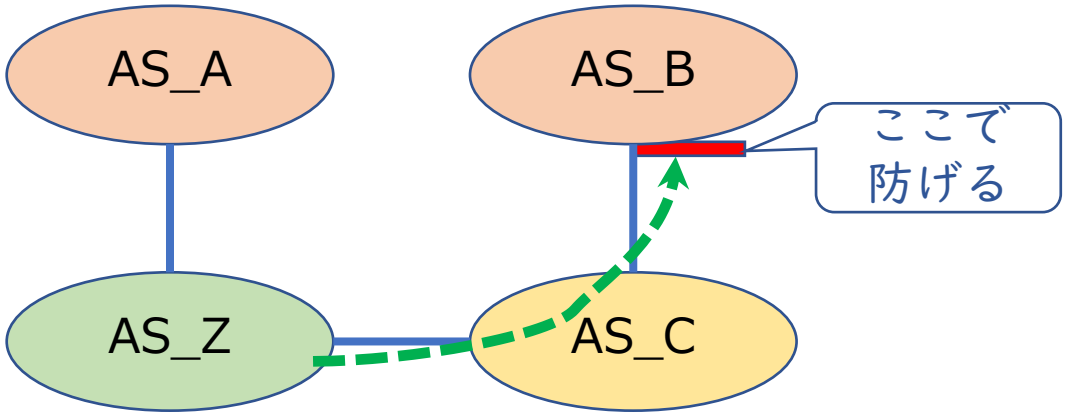
- そのASのプロバイダーとなっているASを記載する証明書
  - 一つのASが発行できるASPAは一つだけ
  - 一つのASPAに複数のプロバイダーASを記載できる

- ASPA {Customer AS, [Provider Set]}
  - AS_ZがASPAを発行するとすると
    ASPA {AS_Z, [AS_A]}



矢印はトランジットの提供方向

ASPAで経路フィルタ



- AS_ZのASPA
  - ASPA {AS_Z, [AS_A]}
- AS_CがAS_Zを誤トランジットしても
  ASPAで識別できる
  - AS_ZのASPA ProviderにAS_Cが含まれていない
- 無論、AS_Zに偽装して経路広報するみたいな攻撃にも有効

- ってな世界が検討されてる・・・

ASPAの利点欠点

利点

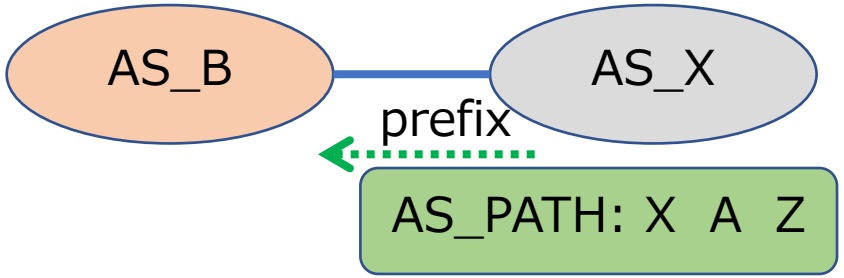
- 多分ルータにとって軽い
  - 恐らく証明書検証は外部
  - ルータには検証後のリストだけ
  - 経路送受信時に比較するだけ
- 人にとって軽い
  - ROAと同じく発行するだけ
- 段階導入できる
  - AS_PATHの一部でも適用可能

欠点

- わからない箇所はある
  - 上流のピアは信頼できるか
- AS単位の制御なので表現できないこともある
  - 例えば、部分トランジット
  - 例えば、Prefix毎に上流を変える
  - 注：あるASがIPv4とIPv6で異なるASPAを発行することは可能

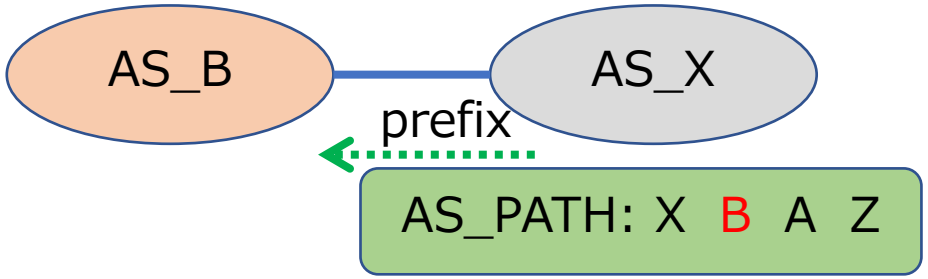
ASPA下での経路ハイジャック手法

- 悪意のAS_Xが、AS_Zの経路を乗っ取る
- 攻撃対象の環境
  - ROAが発行されている　＝ 広報元ASを偽装しないといけない
  - ASPAが発行されている ＝ 広報するAS_PATHを偽装しないといけない
    - AS_ZのASPA: ASPA {AS_Z, [AS_A]}
- AS_Zが経路生成、AS_Aがトランジットしたように見えれば良い
  - 技術的には可能
  - AS_PATH長は伸びる



ASPAはみんなが発行するほど強くなる

- AS_PATHの中で検証できる範囲が広がる
- 例えばAS_AがASPAを発行していたら
  - AS_ZのASPA: ASPA {AS_Z, [AS_A]}
  - AS_AのASPA: ASPA {AS_A, [AS_B]}
- 偽装しなきゃいけないAS_PATHが伸びる→ B A Z
  - AS_PATH長が伸びて、乗っ取りできなくなるかも
  - AS_PATHループ判定で、乗っ取りできなくなるかも



ピア先の確認大事

- ASPAはトランジット関係を検証できるが、ピア関係は検証できない
- ピアを張ろうとしている相手は本当にそのASですか？
- 偽物である危険性もある
  - 経路ハイジャックの影響を受ける
- 悪者がちゃんとお金を払って顧客になってくることもある
  - トランジット費用
  - IXP接続費用

- ご注意を！

ピアを張る前に相手の確認が大事

- あんまり知らない相手との調整時が特に危ない
- 調整の連絡時には、公式窓口にも念の為Ccしておく
  - peeringdbに書いてあるpolicy/noc窓口とか
- 連絡先メールアドレスが不審じゃないか
  - 悪い人は似たドメイン名を登録するぐらいのことやるよ

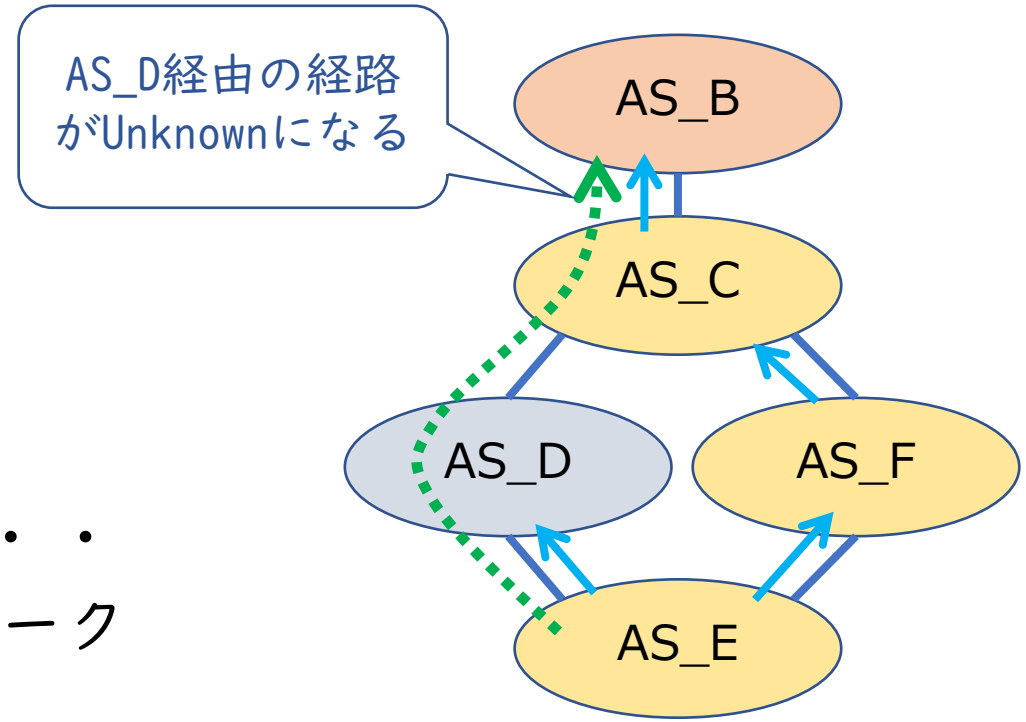
- スケールしないねえ
  - これ、将来は何か素敵な手順を作らないといけないですかね
  - BGP接続の変化はそんなに多くないと思えばスケールしなくてもいいのかもしれない

ASPAはAS_PATHフィルタを代用できるか？

- ピア向け、顧客向けのAS_PATHフィルタ
  - 受信対象の経路のみ受け取る（知らないASを受け取らない）
  - 現状はメール連絡 or IRR as-setでフィルタ生成
- ASPA
  - Valid:　　受け取って大丈夫
  - Invalid:　　破棄して大丈夫
  - Unknown:　　AS_PATHフィルタの代用にするなら受け取っちゃだめ

歯抜けなASPA

- AS_D以外はみんなASPAを発行
  - ASPA {AS_C, [AS_B]}
  - ASPA {AS_F, [AS_C]}
  - ASPA {AS_E, [AS_D, AS_F]}
- AS_DがASPAを発行していないので、AS_D経由の経路はASPA的Unknown・・・
  - これをAS_Bが受け取っちゃうと経路リークなどの事故も防げない
- みんながASPAを発行してくれればValidだけを受け取るようできる



← ASPAで示されるプロバイダ関係
矢印方向経由で経路が
トランジットされる

ASPAはAS_PATHフィルタを代用できるか？

- みんながASPAを発行すれば可能
  - ASPA Validな経路だけを受信する
    - 顧客から
    - ピアから
    - 上流から
- ASPAを集めれば、静的なAS_PATHフィルタも自動生成できる
  - 古いルータでもASPAの恩恵を受けられる
  - 後方互換のためにASPAからas-setを生成して更新もできる
- ルータがASPA検証に対応すれば、もうちょっと自動化も捗る

ポイント

- IRR登録頑張ろう
- RPKI ROA発行もよろしく

- ASPAが発行できる世界になったら、みんなで頑張ろう
  - IETF/RIR/JPNICの動向を注視しておきましょう

- ピア先の確認大事
  - IXP Route-Server
  - 新規ピアとか追加作業とか

対応できそうですか？

- IRR route/route6登録
- IRR as-set登録

- RPKI ROA発行
- RPKI ASPA発行

JPIRRに思うこと

- 更新の手段に要望ありますか？
  - メールでも大丈夫
  - Webベース？
  - API欲しい？
- 世界的な認知度は高い
  - だけど、階層構造はうまく動いてなさそう
    - APNIC IRRに問い合わせてもJPIRRの情報は得られない
  - RIRベースのIRRが徐々に推奨される中、JPIRRの今後も考えないとね

IRR Hierarchical as-set

- 現状の問題点
  - as-setの名前空間はIRR毎に独立。たまにぶつかってる
  - 例：AS-AMAZON これRIPEのは空。RADBのはAS16509が使ってる
- 解決案(Hierarchical as-set)
  - as-setの最初をAS番号にして、:以降に好きな文字を書けるようにする
  - 例：AS4826:AS-VOCUS
- 状況
  - RIPEではポリシー実装済み。APNICは提案出てきた
  - RADBは自由空間
  - JPIRRはどうする？

IRR Hierarchical as-setへの移行案

- 現状、IIJ/AS2497のas-setは AS-IIJ

- 段階1: AS2497:AS-IIJ を同じ内容で作成
  - AS-IIJ と AS2497:AS-IIJ を維持
  - ピア先に AS2497:AS-IIJ への移行を通知
- 段階2: AS-IIJの内容を member: AS2497:AS-IIJ に変更
  - AS-IIJは維持するが、内容は AS2497:AS-IIJ を参照するようにする
  - AS2497:AS-IIJ のみを更新していく

RPKIに思うこと

- ROAの発行は分配を受けたアカウント
  - IRR route/route6とは異なり、ISPがよろしく代理登録はできない
  - JPNICアカウントとかAPNICアカウントは強力なんだよねえ
  - 持ち込みPIブロックが多いネットワークだと対応が大変
- ASPAの発行はASの分配を受けたアカウント
  - ISPにとってはROAよりも楽かも
  - IXPなどで利用されているRoute-Serverが、AS_PATHに自身のASを追加する場合には、ASPAにRoute-Server ASを加えておかないといけない
  - さっさとASPAが発行できるようになって欲しいなあ