

Interdomain Routing Security Workshop

フィルターについて、まとめた話



馬渡 将隆 [MAWATARI Masataka]

株式会社 ドリーム・トレイン・インターネット



1. 大前提

- ✚ エンドユーザの通信には影響しない！！
- ✚ インターネットのインフラを安定したものにす る ひとつの手段として
 - ☐ 不必要な経路は出さない/受け取らない
 - ☐ 不必要なパケットは出さない/受け取らない
- ✚ ISP相互運用でのセキュリティ意識を大切に！！
 - ☐ 1つのISP だけでフィルターをしていても意味がありません





と、言う事を前提にフィルターについてのガイドライン
を考えたいと思います。

2. フィルターを区分してみると

AS内部でのフィルター

-  顧客に対するパケットフィルタリング
-  ルータ自体へのアクセスに対するフィルター

AS間でのフィルター

-  ピアおよびトランジットに対するフィルター
 -  パケットフィルタリング
 -  経路フィルタリング
-  IX セグメントに対するフィルター

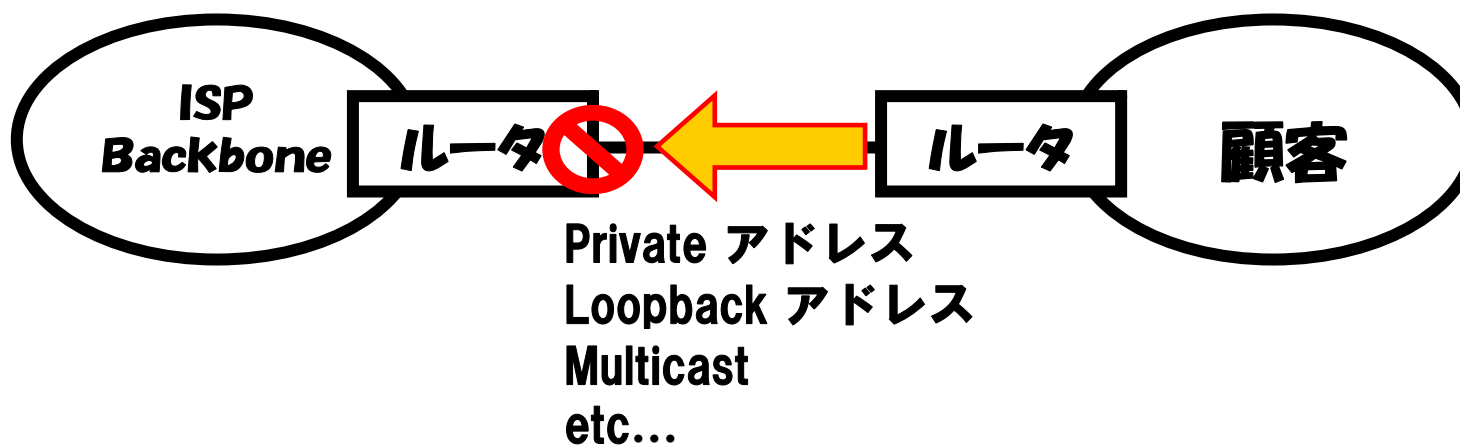
3. AS内部でのフィルター（1）

顧客に対するパケットフィルタリング

⊕ Sourceアドレスフィルタリング（reject ルール）

☐ プライベートアドレス, Loopback アドレス, Multicast...
などを reject する

☐ [参考] RFC3330（どこまでフィルタをして良いか？）



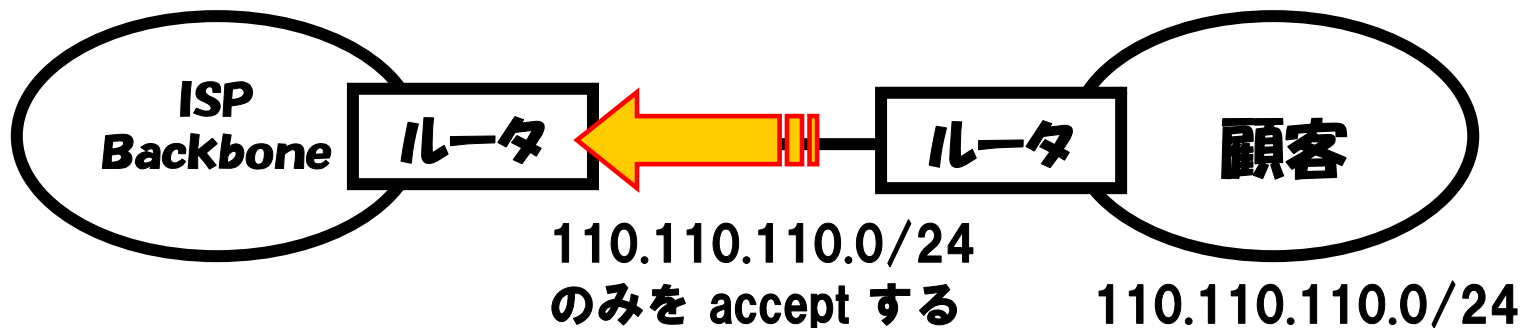
3. AS内部でのフィルター（1）

顧客に対するパケットフィルタリング（続き）

⊕ Sourceアドレスフィルタリング（accept ルール）

☐ 顧客に割り当てたアドレスのみ accept する


☐ 動的にアドレスを割り当てるサービスではプールを
しているアドレスブロック単位で accept する



3. AS内部でのフィルター（2）


ルータ自体へのアクセスに対するフィルター

必要なサービス以外は アクセス不可にする

-  必要なサービスについては、アクセスが可能な Source アドレスを限定する

リモートアクセス用 : telnet, snmp, ftp, ssh ..。

その他には : syslog, ntp, DNS ..。

-  ルータ宛の ICMP パケットは RateLimit / Low Priority ?

Receive ACL

-  ルータのリソースを無駄に使わない為に

4. AS 内部のフィルターをどうやるべきか

AS 内部でのパケットフィルター

それほど動的に変化はしないので、設定はしやすいと思われる

フィルター対象	どうする？
顧客に対しては、以下の source アドレスを <u>reject</u> する Private アドレス [RFC1918] Host Loopback アドレス [127.0.0.0/8] Multicast アドレス [224.0.0.0/3] TEST-NET アドレス [192.0.2.0/24] Link-Local アドレス [169.254.0.0/16] Default [0.0.0.0/8]	どちらかのフィルターの設定を Must で実施する (accept フィルターの方がよりセキュア)
顧客に割り当てているアドレスのみを <u>accept</u> する	
ルータ自体へのアクセスに対するフィルター	Must

5. AS間でのフィルター（経路フィルター）

ピアおよびトランジットに対する Ingress Prefix フィルター ←

✚ プライベートアドレス, Loopback アドレス, Multicast...
などを reject する

📦 [参考] RFC3330（どこまでフィルタするかどうか）

✚ 自 AS が持っている Prefix の or longer を reject する




本来は、自 AS の外部から来るはずの無い経路は止めてしまう

5. AS間でのフィルター（経路フィルター）

ピアおよびトランジットに対する Ingress Prefix フィルター（続き）

細かい経路のフィルタリング

-  環境により異なるが、細かい経路は reject にしておきたい（到達性がなくなる場所も出てくる？）

Max-Prefix Limits

-  異常な経路数を受け取らないようにする

未割り当てブロックの reject フィルタリング

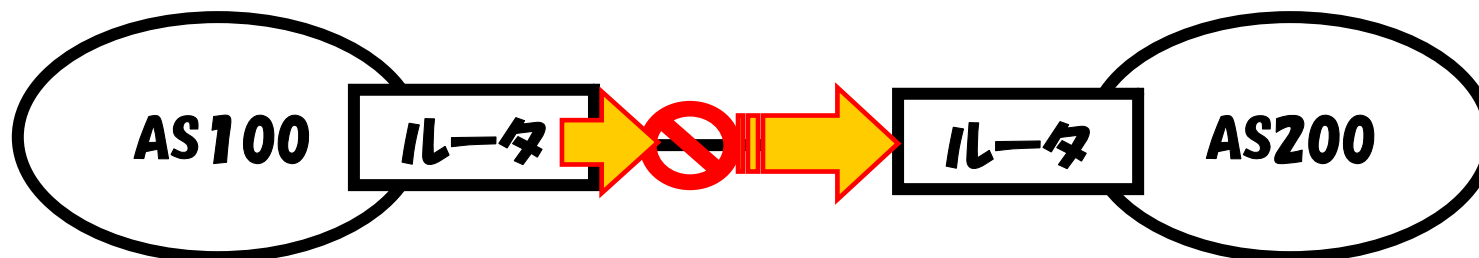
-  Bogon list

5. AS間でのフィルター（経路フィルター）

ピアおよびトランジットに対する Egress Prefix フィルター

⊕ （自 AS が持っている）経路で、広告をする Prefix のみ
accept する

📦 AS 内部で使っている細かい経路はきちんと aggregate
をする

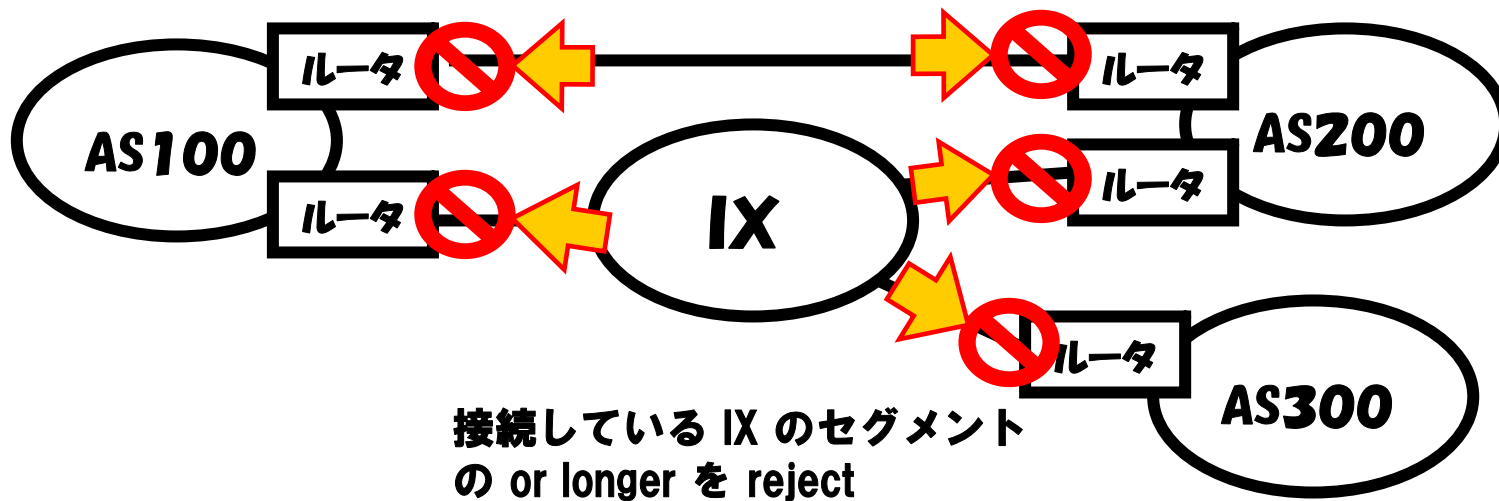


自 AS から外部へは過不足の無い経路を広報する

5. AS間でのフィルター（経路フィルター）

IXセグメントに対する Prefix フィルター

- 自 AS が接続（connected）をしている IX のセグメントの or longer を reject する



本来、自 AS の外部から来るはずの無い（来られたら困る）経路は止めてしまう

6. Prefix フィルターをどうやるべきか

ピアおよびトランジットに対するフィルター

下記のフィルターは、それほど動的に変化はしないので、設定はしやすいと思われる

フィルター対象	どうする？
Private アドレス [RFC1918] Host Loopback アドレス [127.0.0.0/8 or longer] Multicast アドレス [224.0.0.0/3 or longer] TEST-NET アドレス [192.0.2.0/24 or longer] Link-Local アドレス [169.254.0.0/16 or longer] Default [0.0.0.0/8 or longer] を <u>reject</u> する	Must
自 AS が持っている Prefix の or longer を <u>reject</u> する	Must
接続をしている I X のセグメントの or longer を <u>reject</u> する	Must

6. Prefix フィルターをどうやるべきか（続き）

ピアおよびトランジットに対するフィルター

下記のフィルターは、比較的動的に変化していき、設定行数も多くなってくるので、人的リソースおよびルータのパワーと相談

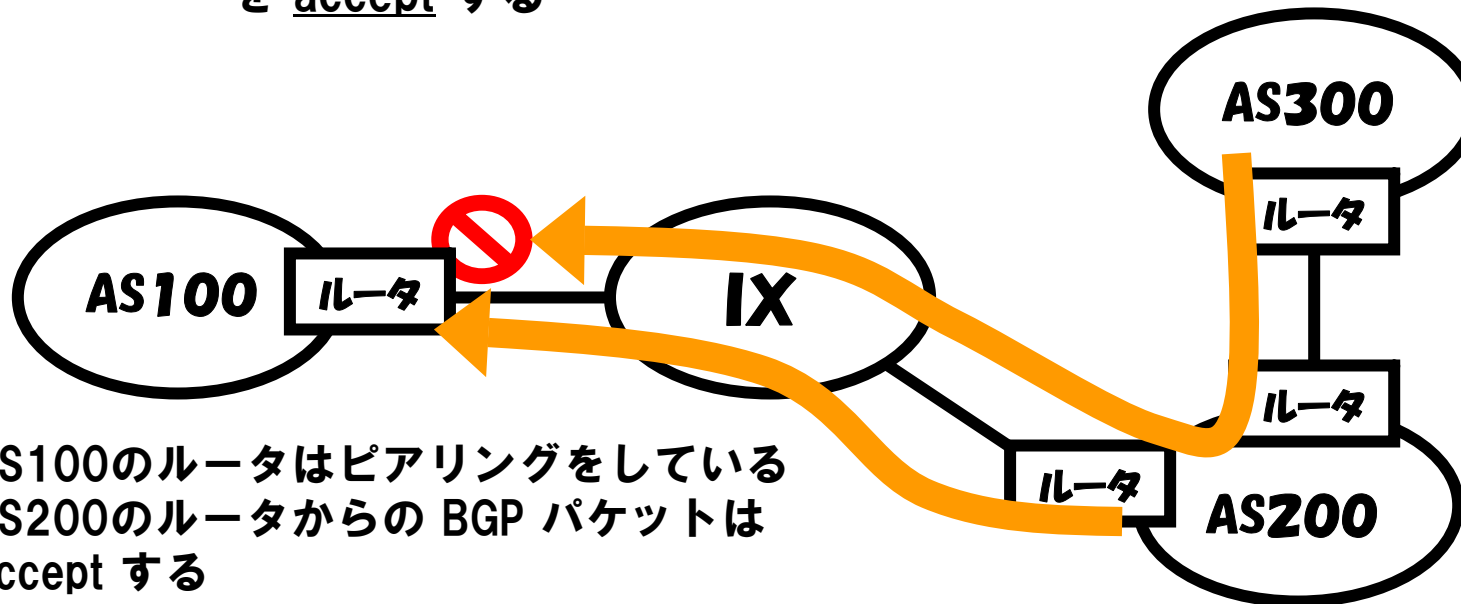
フィルター対象	どうする？
Max-Prefix Limits	厳密に考えるとピア接続先毎に閾値が違ってくる
細かい経路を <u>reject</u> する	/25 or longer の大きさを細かい経路とする例が多いが、環境により適応ができない場合もある
未割り当てブロックを <u>reject</u> する	リソースと要相談

7. AS間でのフィルター（パケットフィルター）

ピアおよびトランジットに対するパケットフィルター

⊕ BGPパケットのフィルタリング

- ▣ ピア接続先（iBGP, eBGP）からの BGP パケットのみを accept する

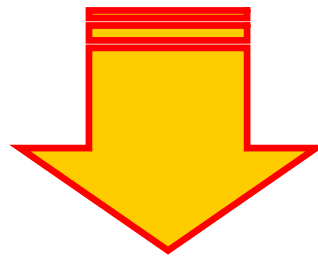


◎AS100のルータはピアリングをしている
AS200のルータからの BGP パケットは
accept する

◎AS100のルータはピアリングをしていない
AS300のルータからの BGP パケットは reject する

8. フィルターをうまく使うにあたって


- ✚ ピア毎に Prefix フィルタリングをしっかりと設定して運用をしていくのはかなり大変。
- ✚ ピア毎に AS-PATH フィルタリングをしっかりと設定をして運用をしていくのはかなり大変。
- ✚ 未割り当てブロックのフィルタリングも結構大変に感じる



フィルターをしっかりと設定/運用していく為には、使えるツールがほしくなる。

9. フィルター運用管理ツール


ほしいと思うフィルター運用管理ツールとは？

 フィルターを作成/更新する

 フィルターの自動作成/自動更新をしたい

 フィルターの内容を確認する

 フィルターの設定内容を分かりやすく閲覧したい

 フィルターに match したパケット数・Byte 数の閲覧をする（ルータ側でカウントをする実装が必要）

 運用に活用をしていく為の情報として重要

10. まとめ

- ✚ Ingress では（来ると困る）不要な経路は受け取らない
 - ☐ テンプレートを作成しておき、一度、設定をしておけばそれほど変更する必要の無いものは完全にしておきましょう

- ✚ Egress では、必要な経路のみを広報する

- ☐ 最悪の事態では、他の ISP に迷惑をかけてしまう事があります。

- ✚ ルータ自体のアクセスに対するフィルター

- ☐ 灯台下暗しにならないように

**設定をした後も、定期的なチェックを忘れないように。
忘れた頃になにかがやってきます。:-)**

11. おわり



コメントをお願い致します。