```
======================================================================
3rd Interdomain Routing Security Workshop
----------------------------------------------------------------------
日　時： 2005/01/13 14:00-18:00
場　所： Cisco赤坂オフィス 13F
参加者： 50名
議事録： 白畑さん、鈴木さん、（編集：近藤）
======================================================================

1. Agenda

  1) (D)DoS対策いろいろ
       シスコシステムズ　横山さん

  2) ISPのルータにおいて設定を推奨するフィルタ項目
       DTI 馬渡さん

  3) JPNICが公開しているデータベース
       JPNIC 川端さん

  ※予定されていたプログラムは、都合により変更になっています。

2. 議事

2.1 (D)DoS対策いろいろ

  - プレゼンの内容
    - DDoS
    - RiverHead
      →Cisco が買収した DDoS 対策製品
    - ISP で利用可能かもしれない DDoS 対策
        - uRPF
        - Remote Triggered Blackhole
        - IP source tracker
        - Netflow/sFlow

  - DDoSのこのセッション的な定義
    - クライアント/サーバ型
      →一番メジャーだと思われる。
      →攻撃ゾンビ+そのゾンビのコントローラ
        →一般的にはエージェントをゾンビと呼ぶ
      →トロイの木馬とかWormとかで、攻撃ゾンビを広める
          e.g.) IRCをゾンビコントロールに使った例 (BOTnet)
    - 人海戦術でツール利用
      →仲間にツールを配って一斉に攻撃
          e.g.) 「田代砲」
      →Reload繰返し
        →悪意が無くとも攻撃となる可能性がある。（F5アタック）
          →速報サイト等は悪意なくリロードを連打する可能性がある
            例: イチロー選手の新記録達成直前のスポーツサイト
    - 特性
        - ゾンビを増やす準備段階では脆弱性を使い不正なプログラムを感染
          させるが、攻撃そのものは脆弱性をつかない。
        - DDoS 攻撃そのものは脆弱性を突いてくるわけではない
          →DDoS の攻撃対象にされるような立派なサイトはパッチ管理もしっ
            かりしているはず
        - トラフィック量は異常でも、Flow の性格自体は通常に近い
          →個々の flow だけをみて判断するのは困難
            http://www.ddosworld.com/

    - Reference
        - Distributed Denial of Service (DDoS) Attacks/tools -
        http://staff.washington.edu/dittrich/misc/ddos/
        - DDoS World
```



```
          http://www.ddosworld.com/
          - Bots &; Botnet: An Overview
          http://www.sans.org/rr/whitepapers/malicious/1299.php

          SANS の資料: 概要を把握するためにおすすめ

  - Cisco DDoS対策製品(旧:RiverHead)
    - 概要
      - DDoSを受けてもサービスは継続することを重視
      - 100%遮断することは考えてない
      - 定常状態からのズレを検知し、攻撃を緩和する
      - 得意分野
        - セグメント全体ではなく、特定のサーバを守ること

    - 製品
      - 攻撃を検知するアプライアンス
        →Cisco Traffic Anomaly Detector XT5600
        - Detector
          - TAP, ポートミラーリングなどでパッシブに異常を発見
          -通信には影響しない
      - 攻撃の検知結果を基に緩和するアプライアンス
        →Cisco Guard XT5650
        - 通信に一時的に介入し、詳細に調査
        - 異常があればトラフィックを絞るなど対応を行う
      - 両方とも 2Uのアプライアンス

    - 大まかな動き
      - 守りたいサーバの近くにAnomaly Detectorを配置しトラフィック観測
      - ルータの近くにGuardを配置
      - Detectorの要求に基づき、filtering/shaping
      - 実際にはiBGP routingでルータから攻撃されているサーバへのトラフ
        ィックを迂回させる
      - Guardから出てきたパケットを、
        - Policy routingでルータに戻す
        - サーバ～ルータのL2に流す

    - トラフィックを戻す手法
      - L3 構成
        - uplink ルータの横に置く
        - ループしないように Policy Routing を設定する
      - L2 構成
        - L2 セグメント経由でルータに戻す
        - Guard から見て下位ルータが next hop

    - 広帯域環境の場合
      - 1Gbps を超えるようなリンクではクラスタリングで対処
        - CEF の load sharing を利用
      - Next-hop がたくさん出てくるので、ロードシェアリング

    - ここまでのQ&A
      Q:使ってる人はいる?
        A:海外にいる
      Q:NPボードのは?
        A:内緒
      Q: (11ページ前後の Diversion Architecture の)図の下の部分の検知
        の単位は？
        A:サブネット単位で指定する。ゾーン一個に一台ではなく、一つの
          ゾーンに複数の保護対象を設定可能
      Q: BGP peer は iBGP peer か?
        A: iBGP でも eBGP でも良い。
      Q:経路制御的には?
        A:RiverHead向けの経路はmore-specificなeBGPを流す。これにより
          トラフィックを誘導する。本来のサーバ向けは何でもOK (e.g. OSPF,
          static)、longest matchでRiverHead行きは、RiverHeadにいくはず。
```

Q:ProtectedZone に該当する経路が OSPF で流れている場合には問題ではないか？
A:Cisco は eBGP (20) の administrative distances が OSPF (110) より強い。また、OSPF で /24 を持っていたとしても、/25で流して最長一致規則で優先される。
Q:Protected Zone は iBGP だとすると、BGP の peer を Boarder router が張ることになるか
A: Yes
Q:通常経路がhost経路だと本当に動く?
A:そもそもそういう構成だと観測が難しいかも
Q:DDoS を受けたら切り替わるのはわかるが、切り戻しはどうするか？
A:Guard の方でも学習をしている。プロファイルをあらかじめ作っておき、定常状態になったら切り戻すか、手動で切り戻すか設定可能。
Q:Guardの性能はどれくらいか？
A:1Mpps程度
Q:Guard は戻す方法としても、トンネリングも利用可能だが、MTU が変わるのでお勧めできないということか?
A:日本のお客さんにはいないが、遠く離れた場所に Guard 配置する場合することも可能。その場合にはトンネルしかない
Q:ルータは Cisco が推奨されているか？
A:マニュアルには Juniper の設定例もある
Q:ロードバランスで CEF は特殊な使い方をしているのか？
A: CEF は特殊な使い方をしているわけではない、Cisco の場合には CEF の限界に依存する
Q:保護対象のルーティングプロトコルについてはどうか？
A:保護対象自体は static で保護する必要がある。保護するサーバが5台であれば、/32 を 5個流してよい。
Q:全部のゾーンを一緒に守りたい場合、実際の経路がもっと細かい経路で流れていて、ホストルートが流れている場合にはどうか？
A:エンドノードを守るのが主眼なので、広い範囲を守るのは苦手。あまりゾーンが広いとプロファイリングの精度が低くなってしまう問題があり、運用しにくい。

- 内部動作の仕組み
  - まず「定常状態」を学習
    - policy construction (トラフィック確認)
    - threshold tuning (内部的な統計情報の閾値学習)
      →Detector だけで学習しているのではなく、Guard の方でも学習している。
        - 内部で詳細な統計情報を持つ
        - 保護対象のゾーン毎にトラフィックのプロファイルを作成し、はずれたものをアノーマリとして判断
  - プロファイリングの精度が重要
    →短い運用経験からは、サーバを絞った方がよい
  - アノーマリとみなしたものは Guard の中へルーティングされる、Guard では攻撃かどうかを精査する
    →Multi-stage Verification Processといっている

  - Multi-stage Verification Process
    1)スタティックフィルタ
    2)ダイナミックフィルタ
    3)Anti-Spoofing
    4)統計情報を計測
      →プロファイルを取る
      →統計情報に異常がある場合ダイナミックにフィルタをいれるようにフィードバック
        →この時点で一旦、2)のダイナミックフィルタの処理に戻り、再度処理される。
        ※名前はフィルタだが、必ずしもトラフィックを落とすわけではなく、さまざまな仕組みがあり、特定のフローに関して特定の手法を適用する
    5)最後はrate limit
      →攻撃だとわからなかったものに関しては、帯域を絞ってサーバに

戻す。

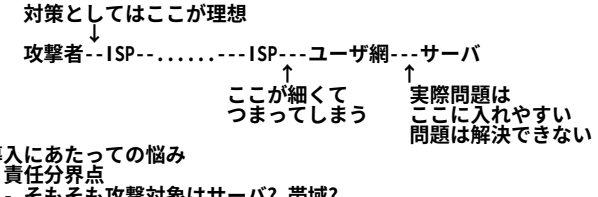
  - Anti-Spoofing手法
    - プロトコル毎に別手法
      →HTTP, DNS, SMTP, IRC, ...
      →L4まで、HTTPだけはもうちょっと細かく
        - 接続元の有効性確認など
    - プロトコルとレベルによってさまざまな手法を使い分ける。
      →SYN cookie, Safe reset, TTL, DNS Authentication, Redirect
    - Anti-Spoofingのレベル
      - 単なるanalysis
        - static-filterを適用するだけ
          →閾値を越えるとbasic protection
          - basic anti-spoof
            - SYN Cookie や redirection により、あからさまな攻撃トラフィックを排除。HTTPでは、最初のGETに関しては同じGuardにRedirectする。
            - 再び帰ってこれば正しいclientと判断
        - まだ閾値を越えるとstrong protection
        - strong anti-spoof
          - HTTPの場合、Guard が HTTP Proxy として動作する。それを行っても、著しく高い場合には、極端な例ではdrop
          - デフォルトでは、drop は極端な動作なので、通常では届かない程度の閾値でdropを設定
      - 移行プロセス
        - 一つのソースIPアドレスから来ているSYNアタックの数が一定量を超えたら、Analysis から Basic Protection に回される。
      - Basic Protection でもトラフィック量が減らなければ、Strong Protection にまわされ、それでも解決しなければdrop される

- ここまでのQ&A
  Q:gray-zoneなトラフィックってどうなる?
  A:黒と判断されれば落とす。めちゃくちゃrateが大きければ落とす。そうでなければrate limitされるだけ
  Q:random port攻撃は?
  A:「port番号の分布が怪しい」ということでguard処理対象のはず
  Q:学習期間はどれくらい？
  A:最低限1日をおすすめ。
  季節変動があるところも多い。ただ「今すぐ対策して」というお客さんも多い...
  Q:学習中にアタックが来てるのは?
  A:サービスに影響がない程度のDDoSは、サービスを継続できているので気にしない方向でお願いしたい。
  Q:flowを跨った攻撃は?
  A:同じsource addressで違うアドレス/ポートを叩く位のは調査範囲内
  Q:HTTPアクセスが異常に増えた場合、それが正常じゃないと判断できることは多いと思うが、そのことを機械に教えておかないといけないのか？あいまいなトラフィックが多いのではないか？
  A:anti-spoofing ではさまざまな手法を使っているが、異常がない場合には、極端なものだけがrate limitにひっかかる
  Q:ユーザが介入して、遷移させることも可能か？
  A:ユーザーアクションは定義可能
  Q:DNSでの例はあるか
  A: trucked flagをつけて、TCPに変えて対応するという例はある。
  Q:Detectorのデータベースを Guard が使うようになっていないようだが。
  A: そのような要望は多い
  Q:DetectorとDuardのデータベースは目的が違うから別々に作っているということか？
  A: 近い目的。Guardの方が細かい。一緒のデータベースを使ってほしいとのリクエストをもらっている。
  Q: Guard は学習させたいサイトのトラフィックだけ曲げることはできる
  A: 特定のゾーンだけ曲げることは可能
  Q: プロトコルはどこまでみれるか

A: L4だけ。HTTPだけはヘッダまでみる
Q: ポート番号を変えている場合には？
A:L4なのでわからないが、HTTPのポート番号を変える場合には設定は可能
Q:ポート番号が次々変わる場合には？
A:同じIPアドレスから多数のポート番号へのアクセスがある場合には異常と判断する
Q:フローはsrc/dst ipだが、フローをまたがった検知も出来るか？
A:実はsocketのうち、srcは見ていないフローをまたがって統計として取っている
Q:最近あったのはaddress spoofもやられて、port scanをやられたケースもあったが、大丈夫か？
A:対応している
Q:truncateしやもののコネクションの扱いについてはどうなるか？DNSのキャッシュサーバとコンテンツでは違うのではないか
A: キャッシュサーバでは保護対象から外す運用方法もある
Q:特別な処理はDNSだけか
A:特別な処理はDNSだけ。それ以外はポート番号のペア等をみて判断している。

Q:学習の過程で、フィードバックは行わない
A:フィードバックはない。より詳しい検査を行うためのトリガとして利用する。

- 導入時構成&使われ方
  - コストが高い線に無駄なトラフィックを流したくない
  - なるべく入口の近くで止めたい



- 導入にあたっての悩み
  - 責任分界点
    - そもそも攻撃対象はサーバ? 帯域?
    - だれが運用するのか
    - 誰が検知して、トラフィックの迂回を決断するのか
  - 攻撃対象にされる部分は何か
    - End Point か
    - 細いリンクか
      →サービスを止めるような攻撃に対して有効だが、細い帯域を埋めるような攻撃には効果が薄い
  - トラフィックの迂回方法
    - 集中処理型
      - ISPの真ん中に集中してGuard/Detectorを配置し、そこにトラフィックを誘導
        →管理は楽だが、Routingが汚い (tunnelはりまくり)
        Guardで見きれるzone数の上限の制限 (30)
    - Peering point配置
      - ISPの境界で弾く
    - BGPの peer をはってあげないといけない
      - 上位ルータとの間で BGP peer が張れるか
      - 自動か、インタラクティブか
      - 誰が迂回の決断をするか

- 導入モデル
  - ISP の助けを借りないモデル
    - メリット
      - ISPと交渉する必要がない

    - デメリット
      - リンクの帯域が消費されるような攻撃には有効ではない
      - 攻撃を受ける頻度が高ければ、運用の負荷は大きい
  - Guard を ISP/iDC型にco-locationするモデル
    - メリット
      - 攻撃トラフィックをISP網内で止められるのでアクセス回線を無駄遣いされない
      - Guard が自分の管理下にあるので細かく制御できる
    - デメリット
      - ISP のエッジルータでBGP peerを張らないと行けないため特別対応が必要
      - co-locationが必要
  - Guard を ISP/iDC型がサービスするモデル
    - メリット
      - 攻撃トラフィックをISP網内で止められるのでアクセス回線を無駄遣いされない
      - 運用工数を減らせる
    - デメリット
      - Guardの運用をISPに依存するため、ユーザが細かく制御するのは難しい
  - 集中処理
    - 集中管理できるので管理コストが低いGuard Cluster までトンネルを張らないといけない

- ここまでのQ&A
  Q:集中処理型では、いくつものGuardが動作できるとのことだが、どれくらいまで処理能力的にはできるのか？
  A:Guardの同時稼働数に上限がある。30ゾーンまで保護できる30台という意味ではなく、一台のGuardで保護できるゾーンが30までである。
  C:具体的には良くわからないところもあり、実験してみたい。
  C:実験場については、調整可能かもしれないので、別途相談したい。
  Q:オペレータが調べれば、白、黒、グレーがあると思うが、何を想定しているか？
  A:黒ならば落とす、レートの高いグレーは黒として扱う、それ以外の場合には、サービスできる程度まで絞る。
  Q:オペレータが調べれば黒と判断できるものに関して、黒と判断できるか？
  A:製品提供者としては黒というしかないLabで作るトラフィックは実際と違う。
  C:ACCSに対して毎月1日、必ずDoSがくる月頭に700MbpsのDoSが来る。
  Q:iDCでは顧客にBGPではなくstaticで出している例もあるが、対応できるか？
  A:現在のところはBGPしか利用できない
  C:ISPの考え方からすれば、お客さんがプロテクテッドゾーンになる。お客さん自体が/25など、トラフィックが入ってしまうベースはサーバを守りたいというのがあれば、カスタマのサービスとして守りたい。
  C:100Mbps程度に対応した安いデバイスをたくさんばらまきたい

* Cisco Traffic Anomaly Detector
  http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/tad/
* Cisco Guard DDoS軽減対策アプライアンス
  http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/gdma/

- その他のDDoS対策について
  - uRPF
    - Strict Mode
      - エッジ加入者を収容しているルータに適用
        - BAS位ならよいのではないか?
          - ISP運用者 != BAS運用者
            →誰か人柱ほしいな:-)
        - BASでuRPFやるのはパフォーマンス的にはきついなのではないだろうか?
          - それならstaticなingress filterでもいいんじゃない

- 技術的には等価だけど、運用の手間的には?
- Source IP address spoofing を適用?

- Loose Mode
  - 他ISPと接続しているルータに適用
  - 完全ではないが、明らかなアドレス詐称の防止は可能

- コメント:
  - 日本特有の問題として、BASとISPが違う
  - Strict Mode で運用しない理由
    - 他でやってくれれば…。
    - RPF を適用したら、知らないうちに multi-home していた顧客からクレームが..

- Remote Triggered Black Hole
  - 攻撃トラフィックを網の入口で捨てる
  - エッジルータにblackhole経路をBGPで広告
  - 実際にやった場合
    - 全パケットを捨てるのでアクセスできなくなる。
      →shaperを使うならかろうじてアクセスは可能
      →サービスを停止させてしまえば、攻撃者の目的は達成される、
    - DNSを利用する方もある
      - やはり全員アクセスできなくなる
    - 電気通信事業法的に「検閲」「秘密保護」等の問題はないか？
      - サービス維持のための必要最小限の話ならOKのはずである。
      - そこで調べた内容をバラすともちろん問題がある。

  - RTBH応用: Sourceベース
    - uRPF loose modeを応用
      - 指定するSource IP addressに対して、存在しないnext-hopを指定
    - RTBH応用: communityによるグルーピング
      - 基本のRTBHにcommunityチェックを付加
    - triggerをかける際にstaticにtagを付加し、tagに応じて異なるcommunity を付加して update

  - 属性毎にエッジルータをグルーピング
    - 海外線グループ、全エッジルータグループ…
      →black hole が有効になるエッジを制限

  - コメント: 一部のISPでは、コミュニティ属性によって外部に広報しないことが可能

  - RTBH応用: Customer Trigger Blackhole
    - リスクさえ低ければ、オペレーションは楽になりそう
    - サンプル:
      http://www.secsup.org/CustomerBlackHole/

- IP source tracker
  - 非対象routingの場合でも、送信元を正しくI/Fを把握
    - tracerouteの逆までは難しいが...
  - tracking対象のIPアドレスを事前に指定、そこ宛パケットのsourceの入力I/Fを把握

- NetFlow利用の攻撃検知
  - e.g.) Arbor Networks
    - 経路表エントリベースの分析になってしまうので、傾向は見れるが、それを基にして防御は難しい
  - 何が難しい
    - Ciscoの場合、GSRクラス以上でないとSamplingがないため負荷的に問題がでる。
    - NetFlow/sFlowをオペレータがONに設定してくれない
      →パフォーマンスの問題。

- 他のmanaged service

AT&T
DDoS defense
Sprint
IP defender
rackspace
DDoS Mitigation service

  - Reference
    - ISP Security Essentials
      http://www.getitmm.com/bootcampflash/launch.html
    - A Summary of DoS/DDoS Prevention, Monitoring and Mitigation
      http://www.sans.org/rr/papers/70/1212.pdf
    - Cisco ISP resource
      ftp://ftp-eng.cisco.com/cons/isp/security/
    - AT&T News Release
      http://www.att.com/news/2004/06/01-13096
    - Sprint gussying up security offerings
      http://www.nwfusion.com/news/2004/101804-sprint.html
    - Riverhead Protects Rackspace
      http://www.lightreading.com/document.asp?site=lightreading&doc_id=39120

2.2 ISPのルータにおいて設定を推奨するフィルタ項目

- 背景
  - 過去のIRS workshopの話のまとめ
  - まずは目次を作りました
    - 項目のbrush upに御協力お願いします

- 対象読者
  - xSP operator

- 大前提
  - エンドユーザの正常な通信には影響しない
  - 不要な経路は出さない/受けない
  - 不要なパケットは出さない/受けない

- 言葉の定義
  - Prefixフィルタ
    - Prefix-basedフィルタ
  - 経路フィルタ
    - Prefixフィルタ+AS-PATHフィルタ
  - Transit
    - フルルートを受けてる接続点 or 状態

- あらすじ
  1. 最低限必要なフィルタ
  1.1 AS内部のパケットフィルタ
  1.2 peer/transitに対するパケットフィルタ,経路フィルタ
  1.3 IXセグメントに対する経路フィルタ
  2. リソースに余裕があれば設定が推奨されるフィルタ
  2.1 AS内部のパケットフィルタ
  2.2 peer/transitに対するパケットフィルタ,経路フィルタ
  2.3 IXセグメントに対する経路フィルタ
  3. 1,2の設定作業負荷を軽減する技術

2.2.1 最低限必要なフィルタ

- AS内部のパケットフィルタ
  - 顧客接続ルータでのingress source address filter
    - special-use IP addressを廃棄するfilter
      (RFC1908, loopback, multicast...)

- 顧客接続ルータでのegress source address filter

- special-use IP addressを廃棄するfilter
  (RFC1908, loopback, multicast...)

Q:egress filterは設定されてることは少ない?
A:そもそもegress filterを設定する効果/デメリットは?
A:○オペミスを補償
×xSP内のprivate addressから端末へ戻る
Q:パケット(e.g. ICMP error)が戻らなくなる?
C:「最低限な推奨」ではない気がする
→ 2.1節に回そう

- ルータ自体へのアクセスに対するパケットフィルタ
  - フィルタをかける場所はそのルータ自身
    - xSPの境界ルータではない
    C: 章立て的にそうとはちょっと読みにくいな
  - フィルタを掛けるサービス
    - telnet, snmp, syslog, ssh ...
  - 運用管理者がいないネットワーク以外からのアクセス禁止

C:顧客接続ルータでのingress destination address filterをすべきか?
C:destinationがRFC1908 addressなパケットが顧客から届いたら、xSPの入口で廃棄すべき?
C:そもそもそ、このドキュメントの目的(他に迷惑をかけないフィルタリング)的に合わないのではないか?

→pending

C:フィルタしたとして、silent discardにするのか?
C:ICMP unreachを返すべきだ。
C:そもそもspoofされてるsourceにICMP errorは返せない。しかし、返してあげた方が親切だとは思う。

→pending

- AS間(peer/transitに対する)パケットフィルタ
  - BGPルータでのBGP ingress packet filter
    - 自AS内, IXセグメント, private-peer segmentからのみのBGPパケットをacceptするパケットフィルタ

- AS間(peer/transitに対する)経路フィルタ
  - ingress prefix filter
    - special-use IP addressを廃棄
      (RFC1908, loopback, multicast, ...)
    - 自ASが持っているprefix(or longer prefix)を廃棄
      - defaultを廃棄
  - egress prefix filter
    - special-use IP addressを出さないfilter
      (RFC1908, loopback, multicast, ...)
    - defaultを出さない
    - AS-PATHフィルタでも同様な項目が必要
      - Private ASを広告しないとすfilter (e.g. "remove-private-as")

- IXセグメントに対する経路フィルタ
  - 自分がつながっているIXセグメント(or longer)を廃棄

```
        e.g.)
        AS200からAS100へ10.10.10.0/24が届いたら廃棄
                        IX
                AS100---|---AS200
                        | 10.10.10.0/24
```

  - 「AS間(peer/transitに対する)経路フィルタ」の一貫で書いた方がいい

C:上の例で、10.10.10.0/24を広告するのは一般的なのか?

C:アメリカでは一般的に広告していた
→ISPに10.10.10.0/24の広告責任があった
→ISPがIXにつながってることの証拠作り

- CDPなんかもIXセグメント的に流してほしくないのでは?
  - CDP, XDP, STP, IGMP, OSPF, ...
  - IXによって違うかも
  - JPIXで使ってるドキュメントをベースにして、別ドキュメントとして作成する方法もある。
  - IXに限った話ではないが、インパクトが大きいと思われる。
    C:やっぱりpeer/transitにも流したくないんで、上の範疇では?
    C:ただfilterの話とは逸れている気がするやるなら、別ドキュメントでがよいだろう。
    C:逆にport 179とICMP-ECHOだけ通すのがよいのか?
    C:確かに層であるが、「最低限」ではない

2.2.2 リソースに余裕があれば設定が推奨されるフィルタ

- AS内部のパケットフィルタ
  - 顧客接続ルータでのingress source address filter
    - 顧客に割り当てたアドレスのみをacceptするパケットフィルタ

- peer/transitに対する経路フィルタ
  - ピアから受け取るprefixのingress prefix filter
    - ピアリング元ISPからの更新通知を基にフィルタ運用
  - 細かい経路をrejectするingress prefix filter
    C:これは、punching holeは駄目であるということを暗に示している。
    C:「細かい」の定義次第

    →賛否両論ありすぎるので削除

- unallocated ingress prefix filter
  - Bogon List参照

- RIRの最小割当sizeのingress filter
  - RIRの最小割当sizeの正しい値が常時入手できない
  - 「細かい経路をrejectするingress prefix filter」でカバーされる可能性大

  →削除

- フィルタの運用の手間を軽減できる技術
  - uRPF, max-prefix-limit, TTL sanity check
  C:便利だがフィルタとはいえないのではないか?
  C:そもそもドキュメントとして、「BGPオペレータのためのTips集」や、「BGPオペレータのためのフィルタ設定集」なら適合するのだが・・

- Q&A
  Q:アプリケーションフィルタリングは?
  A:基本的にout of scopeだが、インフラ系アプリ(telnet, snmp...)は対象とする。
  Q:これらアプリケーション関係として、別のミーティングでも語られているが、そちらとの連携はしているのか?
  A:ここではせいぜいpointerを示す程度と考えている。
  Q:そもそも場所によってどのフィルタが必要かは全然違わないだろうか?
  A:文書中に、設定すべき場所は明示するようにするつもりである。
  Q:逆に適用場所別に「お勧めフィルタリスト」のようなものを書いた方がいいのでは?
  A:そう思う。

- 次バージョンの予定。
  - 今回のコメントなどを鑑みながら、次回のIRSのミーティングにあわせるよう、2〜3カ月後を目処に内容を更に詰めてDraft版を書く予定であ

る。

2.3 JPNICが公開しているデータベース

- ねらい
  - JPNICで公開している各種リストに関するインタビュー
    - オペレーションへの利用方法
    - リストがないとどう困るか

- 今提供しているリスト
  - 今回の対象
    - IPアドレス管理指定事業者リスト
      - 事業者の連絡先とIPアドレス割振り
    - JPNICが割り当てたAS番号リスト
      - AS番号とAS名と連絡先
    - 今回の議論の非対象
      - whois
      - JPNICが逆引きを管理しているJPNICのアドレスリスト
      - APNICが逆引きを管理しているJPNICのアドレスリスト

- 今考えているプラン
  - IPアドレス管理指定事業者リスト
    - 「どんなIPアドレスを割り振ったか?」を削除しようと思ってる
      →(WHOISで等価な情報がわかるようにする)
  - JPNICが割り当てたAS番号リスト
    - リスト自体の廃止
      →(WHOISで等価な情報がわかるから)

- 問題ないですか?
  C: リストのtext fileをscriptにかけて管理してるから、保ってほしい
  C: JPNICのAS番号リストでassignedなモノのリストがほしい
     e.g.) whois -h whois.nic.ad.jp "AS ALL"

  C: このようになったとき、whois DBのメンテはJPNICがメンテすると思ってよいか?
     →IPアドレス管理指定事業者がメンテする、というのは嫌
  C: whoisへの問い合わせが激しくなるが、大丈夫?

  Q: assignされたアドレスのnetmaskがわからなくならないか?
    A: JPNICが握ってる(歴史的な)PI address listを新たに作ったほうが良いのか?
    C: ERXが終われば問題は無いはずなので、不要だと思う。

3. 次回ミーティングについて

- 時期
  - 4月ごろを予定、決定後JANOGメーリングリストにてお知らせする。

- 次回予定のAgenda
  - IXでのフィルタリングガイドライン（JPXI：平尾さん）
  - フィルタリングポリシの次バージョン(DTI：馬渡さん)

以上