Interdomain Routing Security Workshop ミーティングメモ
日時：2004/10/15 14:00-18:00
場所：神田神保町広瀬ビル４階　貸し会議室
参加者：約60名
==========

■soBGPとS-BGP
NTT情報流通プラットフォーム研究所
外山さん　重松さん
14:20-15:30

□背景
ドメイン間の動的経路制御に関する脆弱性
* 受け取った経路情報の origin AS が本当に正しいのか
* 正しい AS PATH で伝搬してきているか

TCP 脆弱性対策
* BGP peer を MD5 を使って守る
* IPSec を利用する
soBGP, S-BGP では IPSec を通す方向

中身の経路情報が本当に正しいか
* 実際に経路の hijacking が起きている
* (正しい経路が) more-specific な経路に負けてしまう

□現在のアプローチ
IRR+経路フィルタ
- Prefixフィルタ
- AS PATHフィルタ
-> 情報が正しいことを確かめる

□電子証明を導入するアプローチ
soBGP
Cisco の James Ng, Russ White らがIETF55(2002)で提案
S-BGP
BBN (Verizon) の Stephen Kent, Charles Lynn らが
IETF42 (1998) の IDR で提案

解こうとしている問題はほぼ同じ
* 経路情報の Origin AS が正しいことを検証する
* 経路情報の AS PATH が正しいことを検証する

□soBGP の考え方
いかなる種類の Central Authority にも依存しない

** 証明書類
* EntityCert
- あるASNと、そのASで利用する公開鍵の束の関係を証明するもの
- 例：ある公開鍵がAS7521だと証明
* AuthCert
- 例: AS7521 は 210.173.160.0/19を広告できる
- 証明書の上位 = ASを割り当てているところ
アドレス空間の広告を認可する
* PrefixPolicyCert
AuthCertとprefixに関するポリシー
例: /19 のアドレスブロックの中で /21 まで許す、
細かい経路が流れてきた際、PrefixPolicyCert
に書いてあれば受け付ける、など
* ASPolicyCert
あるASから見たAS間の接続関係を記述
AS7521とAS2497が繋がっていることを書くなど

上記の証明書を1つずつ確認する

* ある AS が持っている公開鍵をどのように公開していくか？
  APNIC から割り当てられている AS -> APNIC の秘密鍵で
  署名してもらう

中央で全てを見るのではなく、信用できるところ(VeriSignとか
Tier-1 ISP)が、root になってそれぞれの鍵を証明することが
よいのではないかといわれている

* Web-of-Trust
  - 必ずしもICANN->APNICのような階層構造を使う必要はない

* AuthCert
- アナウンスする prefix、AS
  上位 AS があれば上位 AS が証明する
  上位の AS は必ずしも AS を持っているとは限らないが、
  JPNIC/APNIC が上位 AS という形になり証明書にサインする

- 例: APNIC から AS65000 に 10.0.0.0/8 を割り当て
  APNIC の EntityCert に AS65000 や 65001 がある
  65000 が 10.0.0.0/16 をアナウンスできる
  65000 の証明書を持ってアナウンスする

- 受け取った側は 10.0.0.0/16 を受け取ると、AuthCertを
  持ってきて受け取った内容を確認する
- /8 の AuthCert を使い、誰の署名がされているかを確認する
  APNIC が持っているならば、その署名を確認する

- どの prefix を origin としているか確認する
  prefix をいくつでも広告できる
  prefix をまとめて AuthCert を作成する
  prefix 毎に AuthCert を作成しても良い

* PrefixPolicyCert
- AuthCert を含む
- PrefixPolicyCert の内容には、
  最大 prefix 長はどれぐらいか？
  /16に対して/18を切って流す
  どういうAS PATHでなければならない
といった制約を記述可能
- 上記に関して署名

□soBGP と証明書
- AuthCert は 単独で流されない
- AuthCert は PrefixPolicyCert に含まれる

□AS PATHの認証
- ASPolicyCert を利用
  65000 は 65002, 65003 につながっているなど
  Transitか、Non-transitかを記述
  全体の PATH に関する合成図を作っていく
  -> どこからどこへの PATH があるかを知る

□証明書の配送
* セキュリティ情報を配送するのは課題
  - 経路に関する情報を経路システムとして配送したくない
* Update message に Security message を定義
  - EntityCert / ASPolicy Certなどを配送
* BGP の peer を通じて配送したくない場合
  - outband で証明書を配送することも可能

* option 1
  ルータ自身が証明書を処理
  証明書は update の経路をそのまま通る
* option 2

offload - 別サーバにまかせる
証明書は update の経路をそのまま通る
* option 3
証明書の配送、処理は outband

□soBGPの普及
* 広範囲なオプションを用意している
- 仮に直接 soBGP をサポートしていないルータでも、
外付け装置を利用することで可能
* ルータ自身が証明された経路を確認する何らかの手段は必要

□質疑応答

Q: APNIC などが sign などの情報があれば、(APNICなどに)具体的に意見を聞いたことはあるのか。
A: 不明である。いまあるレジストリの階層を使っていけばいいのではないかという記述はあるが、オーソライズされているかはわからない。

Q: PKIみたいなものを利用すると証明書の revokation が重要だと思うが、上位 AS との接続が切れたら、ルータが revoke の状況を確認するなどの仕組みは考えられているか？
A: 仕組みはある。どこにどう埋め込まれているかはわからないが、発行されて証明書を revokation できる。

Q: 証明書があって、キーに載っていないものがあれば、テーブルに載せないのか、フィルタアウトするのか。
A: 載せない形になる

Q(石井さん): 証明書はリモート側によって判断されているが、蹴られているのはわかるか？たとえば punching hole ではなく、/20を通したい、一つのテーブル にprefix長も載るが、判断が難しくなる。たとえば、/19で書いておいて/20で出したい場合には？
A: PrefixPolicyCert に/24と書いてあれば/20は通ると思われる。/19しか書かれていないのに/20が来た場合には蹴られるとはず。

Q: 故意的にやりたい場合には、明示的に書く必要があるか
A: 書く必要がある。prefix filterは明示的に書くから違う

Q: Layer3 IX では、punching hole しているつもりはないが、(結果として) punching hole になってしまう場合、そちらに流れるのを防ぎたい。例えば1つのASが、1つはIX, IXにはupstreamもつながっている環境で、上位には/19、domesticには/20を三つ投げると、上位プロバイダは/19を使いたいが、/20を使ってしまう。トランジットを買っているが、ただでトランジットをすることになってしまう。
(図1: http://dynamo.sohgoh.net/~shin/tmp/punchinghole-on-l3ix.gif 参照)

PrefixPolicyCertを二つ使った場合、全部細かい部分をまわってしまうということをさしているか？BGP の Path selection には触れているかおしえてほしい。

A: ただ正当性だけを調べている。AS PATH 的にではなく、単に経路を認証することはできる。このような状況は、故意的に行わなくとも、普通の運用でも発生する。個々に調査して、filter-out する必要がある。やはり、証明書で出来るところと、他でやらなければならないところはある。

(吉田さん): ポリシでやらなければならない部分はある
(石井さん): ポリシに近いと思う

コメント: トランジットに近い、他の人の経路をコントロールしようとした場合には違ってくる

Q(吉田さん): Security message で AS PATH 等を交換する際、最初に交換する相手と一発目の通信はどうするのか。
A: 通信の中身に署名書が入っている。受け取ったものはルータなり箱でためて

おき、EntityCertが正しいかどうかを確認する。公開鍵をとるといったところが一発目になるのではないかと思う。

□S-BGP
- PKI を利用し AS とか prefix に公開鍵を利用
- IPSec 利用

* Address attestation
prefix と AS を関連づける(soBGPでいうAuthCertに対応)
証明書を溜めておくレポジトリに保管し、後で参照される
(PKIレポジトリ)

* Router attestation

* PKIレポジトリ
- 公開鍵の証明
  ISP公開鍵とASの関連付け
- CRL(失効証明書リスト)
- RIR/LIRが登録を行う

- updateの有効性チェック
  AS(1)からAS(N)まで

1.データを定期的に収集する
  公開鍵類, CRL, Address Attestation
2. 経路を update する
  NIR では、AS65002 の公開鍵と証明書をとってくる
  - AS65001 でも公開鍵をとっておく
  - AS65001 から広報できるアドレスをとる
  - 1.1.1.0/16 がアナウンスされる

* Path attribute を拡張
  - ルータが情報に署名して送信
  - ルータはNOCに集めてあるAddress attestationを確認
    使っている公開鍵が正しいかを確認
    アナウンスしている経路を確認
  - 65002から65003に署名したものを送信
  - S-BGP は update message に path attribute
  (ATTEST)を付加して送信

  - 4096バイトの制限
    メッセージがはみだしてしまう懸念
    溢れた際には次のメッセージに載せる、
    といった話にはなっていない

□soBGP と S-BGP の比較

soBGP:
* web-of-trust
  root がいろいろ
* Security messageを利用
* AS PATHの確認処理は後でよい

S-BGP:
* LIR/RIRのレポジトリに登録
  - レポジトリを参照するのはBGP以外のセッション
  - attribute 属性を利用して参照
* 現在のレジストリ階層に基づいている
  - レジストリがyesといっているかは不明
* Path attributeに追加
* AS PATHの確認処理はメッセージを受けた際にはルータで実施
  - Best pathではないなら後でも良い
  - 基本的にルータでやる

パフォーマンス
データ量、計算量、必要な処理能力

実装は S-BGP しかない
- 机上で比較するしかない
- S-BGP の文章では、一応計算量を見積もっている

□まとめ
* origin AS の認証
- 比較的認証しやすそう
- S-BGP / soBGP

* AS PATH の認証
どの方法がよいか
実際にグラフを作成できるのか

□質疑応答

Q: CRL をチェックするとなると、DNS root server よりも危険性が高い箇所が発生する恐れがある。アタックを受ける危険があると思う。
A: あまり考慮されていない模様。公開されている文章はプロトコルが多く、正常系が中心。運用で発生する異常系の話までは到達していないように見える。

Q: soBGP の話だが、不要なものはルールを書いてrejectするようなものをPolicyCertで見て落とす場合には、routing engineとforwarding engineがわかれていると、蹴飛ばして保存しておくのか、蹴飛ばした経路は落としてしまうのか。
A: 来た経路で証明できないものは捨てると思う。実装の際には、蹴飛ばした経路も保存しておいた方がトラブルシューティングしやすい。利用するものはforwarding engineに突っ込む

Q(石井さん): パフォーマンス的に問題がでてくる恐れがある。
A(河野さん): 実装するとしても、ルータに載せるかどうかは微妙なところ。そんなにリアルタイムでやる必要はないのではないか。これをいれることによって、convergence が遅くなることは避けたい。

Q(石井さん): BGPルータにacceptするなというのか?
ルートリフレクタに対して出す機能もあるのか知りたい. チェックした後の経路をルータに返さないといけないのか。

A: どういう実装になるかはわからないが、来たもので証明できていないものは、pending しておくといったことになるのでは。
後から実際にBGPのテーブルから外せという形も考えられる。
コメント(近藤さん): よくある実装だと、証明できた経路のみを流す。認証から漏れた経路は、優先度を下げて activate したままにする。
証明できていない経路は、何か問題があったときにコマンドを叩くと消える程度の扱い。

Q: dampening しているものと priority は同じ？
A: RIB にもフォワーディングデータベースにも載っている。そのため、引っ張り続けてしまう。認証されない経路が正しくないとは誰も言えないため、deploy していく際の問題になるだろう。

コメント: Ciscoのルータにハードディスクを載せる必要が出てくる可能性もある
コメント: ルートリフレクタのように別出しするなど、全く別の機器になる
コメント: 全ボーダーに対して、別なプロトコルで交換する方法もある

コメント: そもそも証明書を AS 間で交換しないといけない。その経路がないと配送できない。いっそインターネットを使わないことになるのでは。
outband でやる。電話やFAXなども考えられる。
コメント: MD5のキーの交換は電話でやっている人もいる

コメント: soBGP は実装されておらず、Ciscoも実装していない。まだ選択肢
の一つといった段階。まだ先が長そう。

■フィルタリングポリシー
「フィルターについてまとめた話」
DTI 馬渡さん

□自己紹介
* DTI でオペレーションをしている

□フィルタリングの前提
* エンドユーザの通信には影響しないこと
* インターネットのインフラを安定したものにする一つの手段
- 不必要な経路を出さない/受け取らない
- 不必要なパケットを出さない/受け取らない

- どこまでがユーザのトラフィックなのか
- ISPの相互運用でのセキュリティ意識が大切
一つのISPだけでフィルターをしていても意味がない

□フィルターについてガイドラインを考えたい

* 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
パケットフィルタリング/経路フィルタリング

* AS 内部のフィルタリング
- ISP でなくとも設定している場合も多い
- private address/loopback/multicast などを reject
- 参考：RFC3330 (Special-Use IPv4 Addresses)

- Source address filtering
acceptルール
顧客に割り当てたアドレスのみ受け入れる

□質疑応答
Q(吉田さん): わざとsource addressをかえている場合にはどうするのか。衛星
インターネットなど、Source ip addressのAS が(自ASと)違う場合もある
A: サービスとしてそういうのもあるが、通常は上流と話をする

コメント(石田さん): 最近は暗黙のうちに期待されているフィルタであるエン
ドユーザに対しては暗黙のうちに掛けるようになっている。
コメント(水越さん): ユーザが意識しているか意識していないかが問題。マル
チホームされた際に発生する。
どっちのアドレスが意識しているか、意識していないでマルチホームする
際に発生。正しい運用ではないが、起こりうる事態
A(高田さん): Staticの顧客に対してingress filteringを実施している

Q: 客からフィルタリングを外してくれといわれたことはないか?
A: データセンターの場合にはISPと違う
コメント: Flets's はクローズドなネットワーク内でNTTのクラスBアドレスを
つけている。これらのパケットがインターネットに出て行った場合、行き
はあるが、戻りはない。
コメント: 行きだけでも影響を及ぼすパケットもありうる
* ルータ宛のicmpパケットはrate-limit/low priorityにする
* ルータ自身のIPアドレスを広報しない
- うまく prefix を割り当てていれば可能
- バックボーンとユーザのIPアドレスを分ければ可能
- MPLS はそれに近いものがある

コメント: Path MTU Discovery が働かない可能性も考えられるのではないか。
コメント: プライベートアドレスがソースアドレスの場合には、よく落とされている

□質疑応答
Q: rate-limit を行うと ISP 間の協調運用で支障が出る恐れは？
A: パケットの大きさや、来る頻度による。rate-limitをかける意図はDoS 対策なので、通常の ping や traceroute に関しては問題ない。
コメント: 顧客/ゲームユーザに ICMP は Low priority であることを教育する
コメント: 前提として、管理外の箇所から来るパケットに rate-limit をかけたい
コメント: 実際問題としては区別できない
コメント: 内側から外側から考慮する必要はある

Q: ICMP の rate-limit を掛けている人は？
A: ICMP の rate-limit をかけている。たまに効果はある
コメント(高田さん): peer が切れた際に、テストをしたらrate-limit がかかっていて困った場合があった。 最近あったWorm のトラフィックに、通信確認用の ICMP が載って制限がかかった模様。Private peer でも ping ぐらい打ちたい

* AS内部でのパケットフィルタのまとめ
  - 顧客に対してのソースアドレスを reject する
  - 顧客に割り当てているアドレスのみを accept する
* AS間でのフィルタ
  - プライベートアドレス/Loopback アドレス等を reject
  - 自ASが持っているprefix or longerをフィルタする
* 付加的な手段のフィルタ
  - 細かい経路のフィルタリング
  - ISPのポリシによる
* maximum-prefix limit
  - 相手のルータの設定ミス、発狂対策
  - 異常な数の経路を受け取らないように設定
* 未割り当てブロックのアドレスフィルタ

□prefix filter
* 自ASが持っている経路で、広告をする prefix のみ accept する
* IXセグメントに対する prefix filter
  - 自ASが直接 connect しているIXのセグメントの prefix or longer を reject する
  - 本来 AS 外部から来るはずのない経路

* ピアおよびトランジットに対するフィルター
  - maximum-prefix filter が手軽だが、厳密に考えると prefix の数もかわる

□質疑応答
Q: 何を元に厳密に考えるのか
A: peerだと自分の経路と顧客の経路しか流れないので、それの数十パーセント増しの値を設定するなどが考えられる。
Q: やっているASはあるか
A: ある。個別のピアごとにやるのは煩雑なため、1〜100経路の組織ならば上限を200に設定するなど、グループ毎に設定している。
いま心配なのは、ピア先に多くの経路数を持っている顧客が出現し、そのASとのピアが落ちないかという点。落とすか、warningを出して受け続けるか。
コメント: warningを出してそのままの方がオペレーション的にはよいのではないか。maximum prefix limitは、個別のフィルタを書くのが面倒なので、さぼろうという意図がある。
コメント: maximum prefix limitはそのような目的でインプリされたのか？それともメモリがしんどいとか、VPNのBGP系でリソースを制限したい目的で実装されたのかが気になる。
コメント: 5年ぐらい前のUUNet事件を防ぐために作られた。
コメント: ピアのところに設定するなら、10万を設定してフルルートをくべら

れるのを防げればよいのではないか。そもそも AS PATH filter をやっていない時、いきなり自発で出すのを防ぎたい。
コメント: すごい prefix 数だが、originも正しい場合も想定される。
prefix 長を見ないで、or longerでフィルタするというのが有効では。
フィルターについては、何でそうしたいか、ステートメントにないと、資料だけ見た際にわかりにくくなる。
コメント: よくルータを設置して、一年後にみるとわからないフィルタが残っていることがある。あとから心がわかるようにしたい。

□prefix filter(続き)
* 細かい経路をrejectする
- /25 or longer を reject する例が多いようだ
- 環境によって適用できるかできないか
* 未割り当てブロックをrejectする
- 設定行数も長くなる、管理も大変

□BGPパケットのフィルタ
* ピア接続先(iBGP/eBGP)からの BGP パケットのみを accept する
- peerをしないところは BGP のパケットを受け取らない
* ピアごとにprefixフィルタリングをしっかりして運用するのはかなり大変

* フィルタを管理するツール
欲しいと思うフィルタ管理運用ツールとは？
- 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
フィルターの設定内容をわかりやすく閲覧

Q: 買ってきてカスタマイズしているところはあるか
コメント: config管理方法はcvsでひっぱってきて、管理する
コメント: CRS-1はロールバック可能
コメント: 履歴の保管は必須

コメント: フィルタに特化したツールは利用していない
コメント: Juniper の config に変えてくれるツールを作っているベンチャーがある
コメント: 5月ぐらいにレジストリの情報を持ってきて prefix の allocation 情報によってフィルタを出力するツールを作った。
APNIC/RIPE/ARIN の情報を持ってくる必要があるが、フォーマットが異なるためわからない。

コメント: IRRにroute-objectがあり、ちゃんと管理されている

A(前村さん): IRRの情報を正しくアップデートしよう

コメント: allocation の情報があれば結構フィルタできる。ある /8 のブロックは /21 or longerでフィルタすればよい
コメント: いつアップデートしたという情報がこない
コメント: フォーマットが決まっていない

コメント: IRR(のroute-object)にはシーケンス番号があるか？
コメント: あがったのを通知して欲しい
コメント: polling するにしても間隔が問題
コメント: そもそも allocation をまめにフィルタしているのか

コメント: フィルタはそもそもやばい情報が来るから掛けるものである。
あるfull routeを流す人がいて、そこから全てのrouteが来ている場合、安全性のためにもう一本必要で、さらに細かい経路等のprivate peerにながす、など。

コメント: bogonをかけている人の気持ちは、spammerの人たちが勝手なアドレスを使って広報しているから止めたい。ミスオペレーションではなく悪いヤツがいるからというのが理由。allocationの真正性を保証しないといけ

ない

□まとめ
* ingress 不要な経路は受け取らない
- templateを作成して、受け取らない
* egress については必要な経路のみを広報
* ルータ自体のセキュリティ
* 定期的なチェック

□質疑応答
Q: JANOG14 で発表された null/static を使って広報する方法は?
A: フィルタの実装の一種で、sinkhole/blackholeなどがある。
MPLSを使った実装もある

A(横山さん):
riverhead: (D)DoS検知箱
* DDoSと思われるパケットだけを検知して、正常だと思われるパケットのみをネットワークに戻す
* DoS Attackの分類を行っている

■「uRPF と DNS Anycast は仲良しか」
MEX 石田さん、OCN 吉田さん

□背景
uPRF が deploy されつつある。一方で、BGP Anycast も普及してきた。しかし、uRPF と BGP Anycast は相互に干渉する恐れがあるため、問題意識を共有したい。

ストックホルムの root DNS サーバは(BGP Anycastを使い)サーバを増やしているが、deploy には慎重さが必要ではないか。このトピックを DNS Operator に投げかけたが、反応はよくなかった。

手間をかけずに Ingress Filtering を実装する方法として uRPF が使われ始めている。これが BGP Anycast と相互に技術の干渉が起こるのではないか。

□uRPF とは
* 経路情報を利用した Ingress Filtering の手法
* unicast Reverse Path Forwarding
- メリット
静的な設定の整合性を保つ必要がない
経路情報の変化に応じて動的に対応可能
-> オペレータにとって楽に運用可能
- デメリット
経路制御変更に細心の注意が必要
local preference, MED

* RFC 3704 (BCP84)
Ingress Filtering for Multihomed Networks として公開

* Strict Reverse Path Forwarding
- パケットのソースアドレスはFIBを参照する
- パケットを受け取ったインタフェースが forward すべきインタフェースなら、そのパケットは通過可能
* SRPF ではパスの対称性があることを前提としている
- 実際には対称性がないケースもあるため、利用にあたって注意が必要
- 複数の ISP 間でのピアリングでは対称性は期待できない
- community を使ったり weight を使ったりして解決できると書かれているが、運用は難しそう

* Feasible FRPF
- パケットのソースアドレスについてはRIBを参照

- パケットを受け取ったインタフェースが best でなくとも
  大丈夫(代替経路として利用されるインタフェースならOK)
- 非対称のパスでもよい

* Loose Reverse Path Forwarding
- パケットのソースアドレスがルーティングテーブルにあるか
  どうかのみを確認
- 正確にいうと、Reverse Path forwarding ではない
- デフォルトルートの処理をどうするかでさらに扱いが分か
  れるinter-domain 向きではない感じ

□uRPF は使えるか?
* そこそこ使い勝手がある

- BGPカスタマに対してエッジで利用可能
- トランジットサービスでも利用可能かも
- JP内での利用はあまり聞かない
(会場からもほとんど反応なし)

- USのトランジットISPでは4,5年前から利用していた模様
  uRPFそのものかはわからないが、それに
  近いことはやっていたようだ

* BGPルータへのインプリ具合
- USのメーカ系はインプリ済み?
  一部L3スイッチでは未実装
- 現状は strict と Loose のみか
- JPのメーカーは?

□DNS Anycast とは?
* RFC3258
Distributing Authoritative Name Servers via
Shared Unicast Addresses
* 13個しかないルートネームサーバの負荷分散・耐障害性
+ international politics...

* DNSの特性を利用
- UDPで 1 packet で完結
- 必ずclient 側からのみ initiate される

* 欠点
- 監視できない
* 利点
- 独自の AS をとって BGP の経路をアナウンス
- BGP 的に最も近いところに引き込まれていく
→DDoS 発生時の影響が限定される
- サーバ処理能力の増強

* どれだけdeployしているか
http://www.root-servers.org

コメント: 監視できないということだが、前回のJANOGでIIJの人が
発表していたが、BIND9ではどこを見ているかぐらいはわかる

* DNS AnycastはBGPオペレータに認知されているか
そこそこ

□uRPF vs BGP Anycast

* Trouble Case 1
途中ASで、経路が一部からしか広報されていないとuRPFをかけられて
しまうのでは。BGPでの経路の広報は恣意的に行われる

* trouble case 2

- multihome でも起こりうる問題
  サブセットの問題
  Anycast でアナウンスされる root DNS サーバのアドレスの1個について、ping が答えなかったが、経路を向ける方向を変えてもらい解決した

□考察
Q(水越さん): multihome で発生する問題を引きずっているにすぎない
A: Anycast はネットワークの実態が異なるので問題を複雑にしているいろいろケースが起こりうる

□DNS Anycast を気にしなくていいのか？
* Yesの立場
  - n/13 の一部で発生する問題にしかすぎない
  - root server についてはどれかにたどり着ければ OK
* Noの立場
  - 13個ある全ての root server にたどりつけるべき
  - トラブルの当事者には解決できない問題

* もっと恐ろしいことに...
  - Alternative root server
    AS番号でしか見ていない
  - root server hijack
    コメント: 可能性は低いのではないか
    コメント: Anycast が始まる前から起きていた問題である
    コメント: traceroute であさっての方向へ行ってもウソか本当かわからなくなった

□思いつき
* IPv4 の uRPF では root-server のアドレスを除外する
  - しかし、root serverのソースアドレスを持つ DoS が流行する恐れがある..

Q: uRPF の実装で、uRPF で例外を設定することはできないか
A: 全部のケースに対応できないので、考慮したい。
ルーティングテーブルを操作することで uRPF の挙動を変えることはできる

□ hijack 対策
* DNSSEC の deploy を待つ？
* ip verify reverse-path でかける方法
* CARで書いて落とす方法
→ 問題点がありそうなので、後日まとめて提出する方向で

■次回のWorkshop
1月13日(木)
Cisco 赤坂オフィスの方向で
