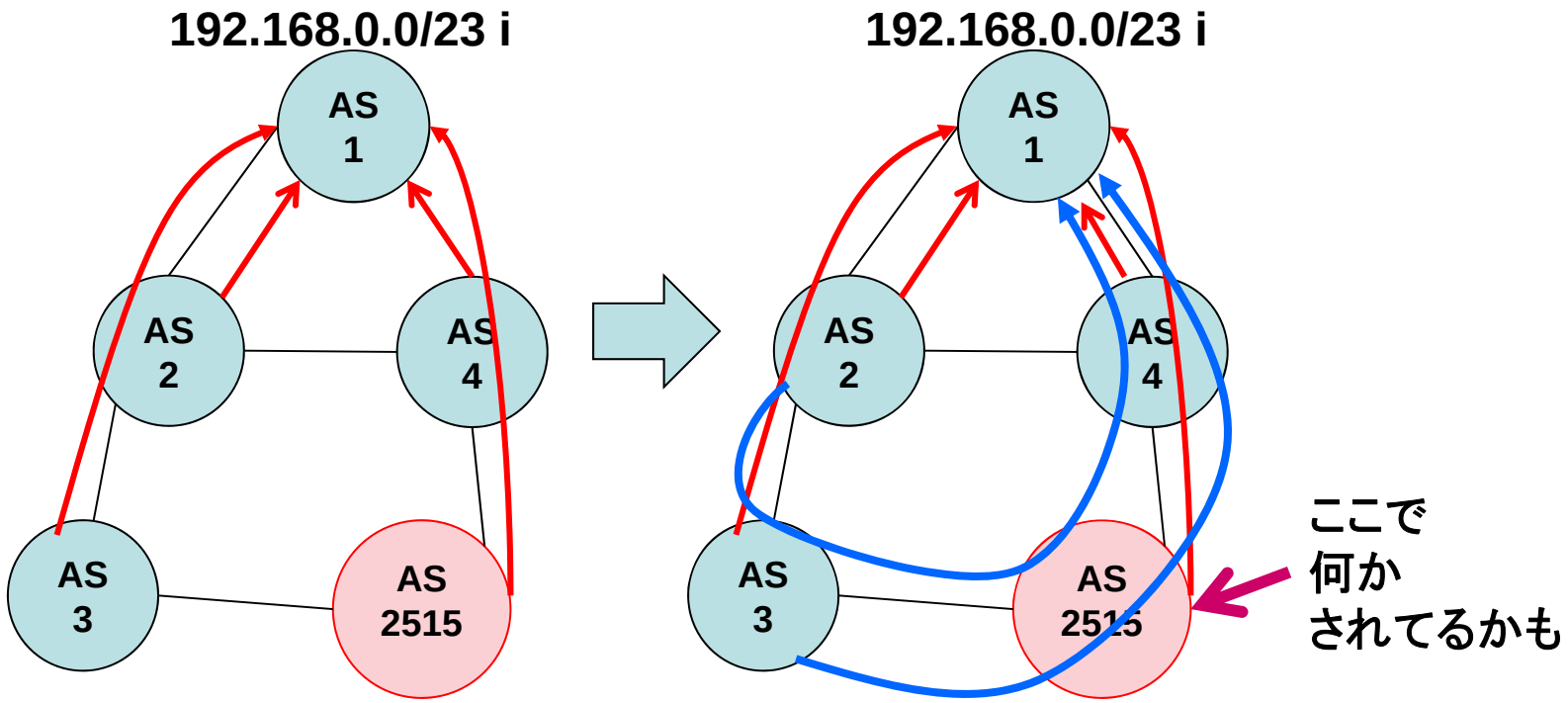
備える！インターネットルーティングセキュリティ実践

その時のために

KDDI株式会社
中野 達也

今、起きている事

- AS-PATHを捻じ曲げているASがいるらしい



BGP Man-In-The-Middle Attack

192.168.0.0/24 i AS4 AS1
192.168.1.0/24 i AS4 AS1

「経路ハイジャック」という言葉について

「権威のない経路広告」が行われることにより
経路情報誤りが発生し
それにより引き起こされる通信障害

↓

悪意の有無・故意・過失にかかわらず
この言葉が使われている
ほとんどが過失によるもの

↓

<u>見直すべき時期に来ているのではないか</u>

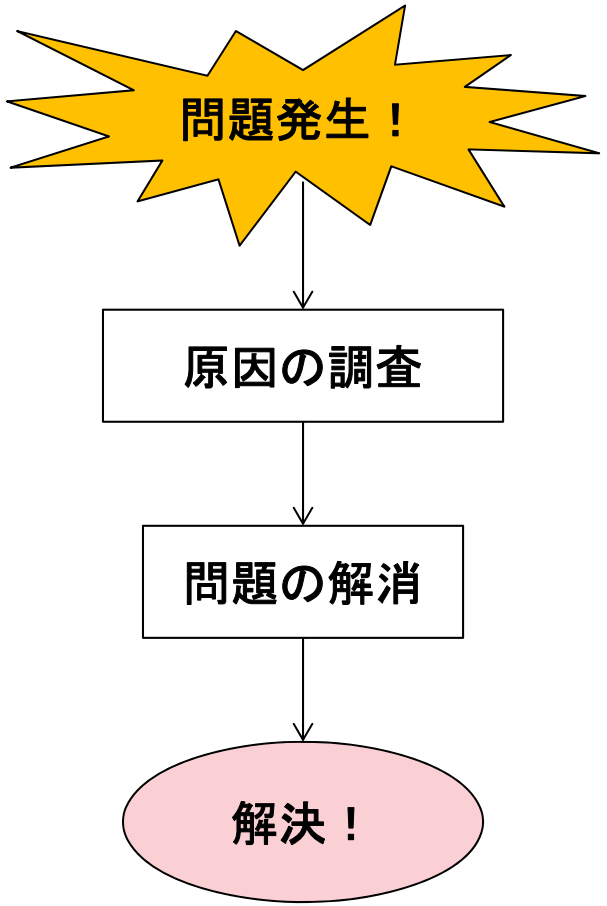
もくじ

1. 権威のない経路広告が身近で起こったら
2. 誤広報を自分がやってしまったら
3. 身近で起きたら･その時のために

1.権威のない経路広告が身近で起こったら

やられちゃったらどうなる?
解決するには?

解決までの流れ

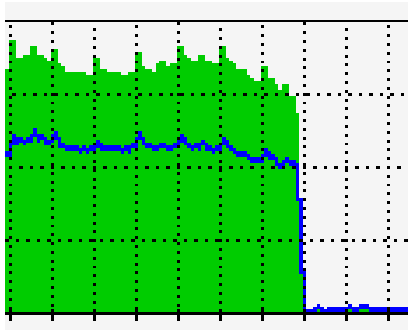


何が起きる？
どうやって気づく？

どうやって調べる？
何を調べる？

どうやって解消する？

何が起こる?



トラフィックの急落

webサイト閲覧NG

外部からの接続NG
Mail送受信NG
その他通信NG

etc…

しかも気づけないことも多い
だから気づけるようにしよう

どうやって気づけるようにするか

BGP mon

RIPE NCC RIPE NETWORK COORDINATION CENTRE

renesys

BGPMON	http://bgpmon.net/
Cyclops	http://cyclops.cs.ucla.edu/
ISAlarm	https://www.ripe.net/is/alarms/
Renesys	http://www.renesys.com/
経路奉行	http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html

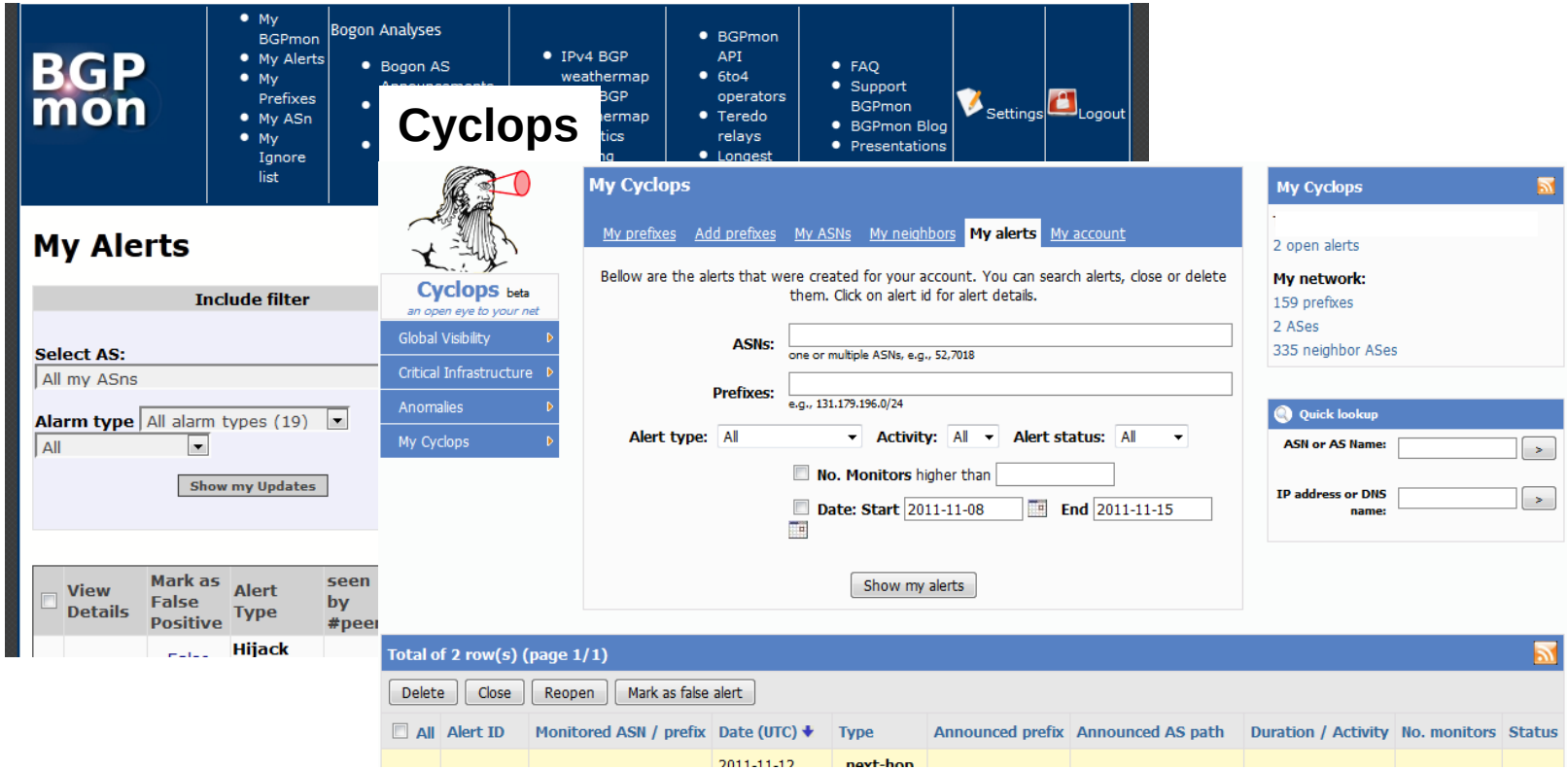
各システムの比較

	BGPmon.net	IS Alarms	Cyclops	Renesys	経路奉行
経路の情報源	RIPE-RIS Route views	RIPE-RIS	RIPE-RIS RouteViews etc…	More than 350 prividers	国内ISPの経路情報
経路情報との比較方法	ユーザ入力情報				JPIRR
通知、確認方法	Web メール	Web メール Syslog	Web メール RSS	Web	メール
備考	事前登録要 ASNでPrefixも登録可	事前登録要 Prefix手入力	事前登録要 ASNでPrefixも登録可	有料	Objectに登録すれば監視対象になる (通知には条件あり)

BGPmon / Cyclops

いずれも、GUIのWeb-IFがある

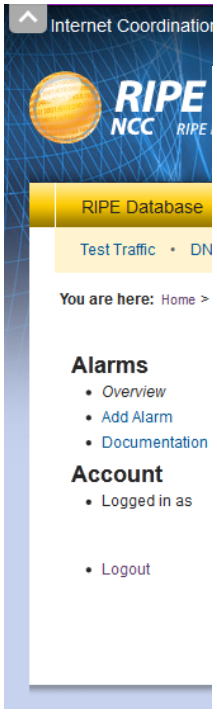
BGPMON



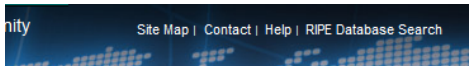
IS Alarms / renesys

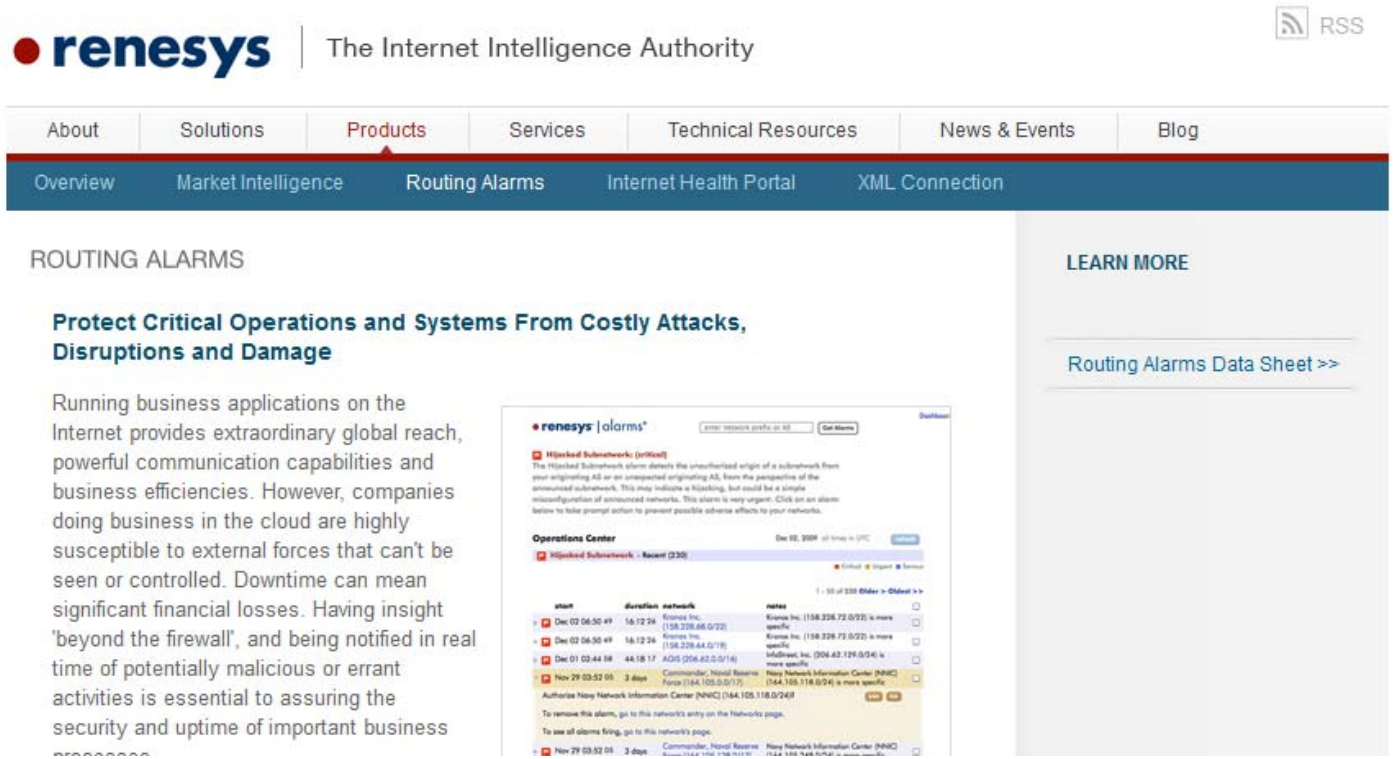
いずれも、GUIのWeb-IFがある

IS Alarms



renesys Routing Alarms





経路奉行

- 経路ハイジャック通知実験メール
  - JPIRRにRouteオブジェクトを登録していること
  - descrにX-Keiroを設定していること

```
ご担当者様

以下の通り、経路ハイジャックが疑われる状態を検知しました。

----------------------------------------
検知日時                    : Fri 28 Mar 2008 10:50:30 +0900
Routeオブジェクト           : 192.0.2.0/24
RouteオブジェクトのOrigin   : AS2515
検知したPrefix              : 192.0.2.0/24
----------------------------------------
```

X-keiroの登録

- メンテナーオブジェクトやRouteオブジェクトにメールアドレスを登録する
  - 例 whois –h jpirr.nic.ad.jp MAINT-AS2515

```
mntner:      MAINT-AS2515
descr:       Japan Network Information Center
             People authorized to make changes for AS2515
             X-Keiro: okadams@nic.ad.jp
```

参考サイト　http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html
http://www.nic.ad.jp/doc/jpnic-01077.html

広報元がどこかを調べる

- show ip bgp <prefix>
- traceroute
  - 自ASルータで
  - Looking Glassで
- RouteViewsのmrtdump archiveを参照

DTI Looking Glass	http://neptune.dti.ad.jp/
traceroute.org	http://www.traceroute.org/
RouteViews	http://archive.routeviews.org/

Looking Glass

- Looking Glassで調べる
  - show ip bgp の結果に自AS以外のOriginが存在するかを確認する

経路ハイジャックが疑われる例(正しいOriginASを2515とした場合)

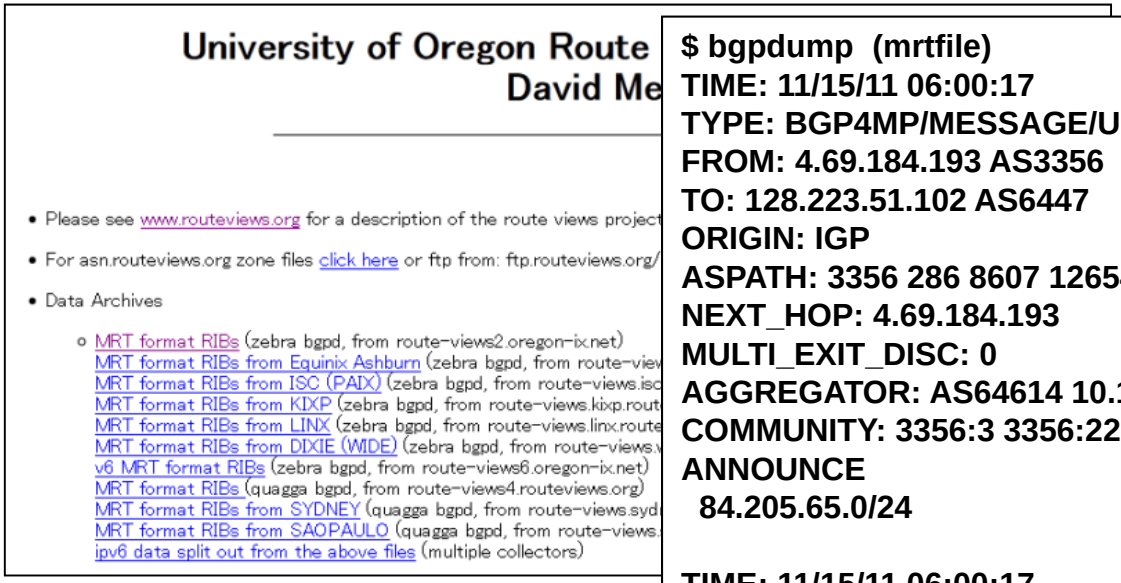
```
BGP routing table entry for 192.168.100.0/19

  2513 2514 2515
    218.189.6.2 from 218.189.6.2 (218.189.6.2)
      Origin IGP, localpref 100, valid, external
      Last update: Mon Oct 14 12:53:42 2011

                                  ← ???
  666 666 2516
    195.47.235.100 from 195.47.235.100 (195.47.235.100)
      Origin IGP, localpref 100, valid, external
      Last update: Sun Oct 20 09:40:50 2011
```

mrtdumpの参照

Route Views Archive http://archive.routeviews.org/


University of Oregon Route
David Me

- Please see www.routeviews.org for a description of the route views project
- For asn.routeviews.org zone files click here or ftp from: ftp.routeviews.org/
- Data Archives
  - MRT format RIBs (zebra bgpd, from route-views2.oregon-ix.net)
    MRT format RIBs from Equinix Ashburn (zebra bgpd, from route-view
    MRT format RIBs from ISC (PAIX) (zebra bgpd, from route-views.isc
    MRT format RIBs from KIXP (zebra bgpd, from route-views.kixp.rout
    MRT format RIBs from LINX (zebra bgpd, from route-views.linx.route
    MRT format RIBs from DIXIE (WIDE) (zebra bgpd, from route-views.
    v6 MRT format RIBs (zebra bgpd, from route-views6.oregon-ix.net)
    MRT format RIBs (quagga bgpd, from route-views4.routeviews.org)
    MRT format RIBs from SYDNEY (quagga bgpd, from route-views.syd
    MRT format RIBs from SAOPAULO (quagga bgpd, from route-views.
    ipv6 data split out from the above files (multiple collectors)

```
$ bgpdump  (mrtfile)
TIME: 11/15/11 06:00:17
TYPE: BGP4MP/MESSAGE/Update
FROM: 4.69.184.193 AS3356
TO: 128.223.51.102 AS6447
ORIGIN: IGP
ASPATH: 3356 286 8607 12654
NEXT_HOP: 4.69.184.193
MULTI_EXIT_DISC: 0
AGGREGATOR: AS64614 10.18.173.65
COMMUNITY: 3356:3 3356:22 3356:86 3356:575 3356:666 3356:2011
ANNOUNCE
  84.205.65.0/24

TIME: 11/15/11 06:00:17
TYPE: BGP4MP/MESSAGE/Update
...
```

例

bgpdump (mrtfile) | grep ‘prefix'
bgpdump (mrtfile) | grep '^ASPATH:' | more | sort | uniq
bgpdump (mrtfile) | grep '^TIME:¥|^ASPATH:¥|^WITHDRAW¥|^ANNOUNCE'

bgpdump　　http://www.ris.ripe.net/source/bgpdump/

広報元の連絡先を調べる

- Whoisで調べてみる
  - JPNIC Whois
  - RADB …etc
- PeeringDBを参照する
- HurricaneElectricのBGP Toolkitを参照する

Whois	(JPNIC/RADB/ARIN etc…)
PeeringDB	https://www.peeringdb.com/
HE BGP toolkit	http://bgp.he.net

Whois(JPNIC/RADB etc…)

- whois -h whois.nic.ad.jp <AS番号>
  JPNICハンドル(グループハンドル)を確認する
- whois -h whois.radb.net <AS番号>
  notifyやmnt-byを確認する

検索例(AS2516)

```
aut-num:    AS2516
as-name:    KDDI
descr:      KDDI CORPORATION
admin-c:    *** ****
tech-c:     *** ****
notify:     maint@example.jp
mnt-by:     MAINT-AS2516
changed:    maint@example.jp
```

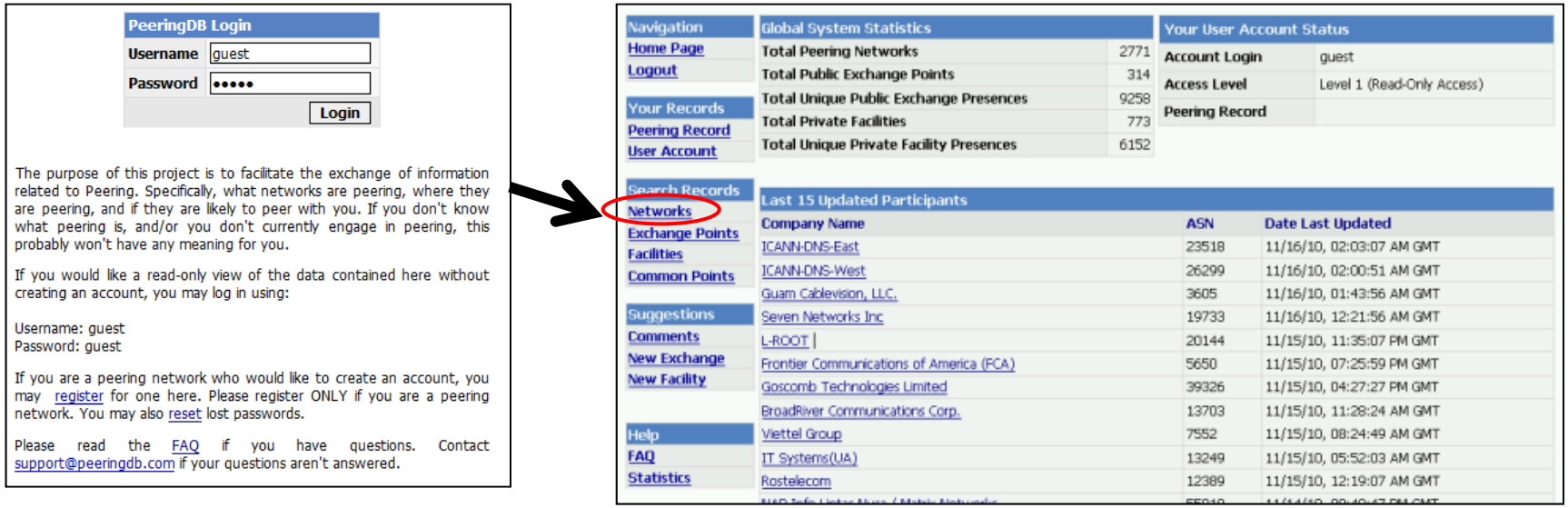
検索例(MAINT-AS2516)

```
mntner:     MAINT-AS2516
descr:      KDDI Corporation
admin-c:    *** ****
tech-c:     *** ****
upd-to:     update@example.jp
notify:     admin@example.jp
mnt-nfy:    maint@example.jp
```

PeeringDB

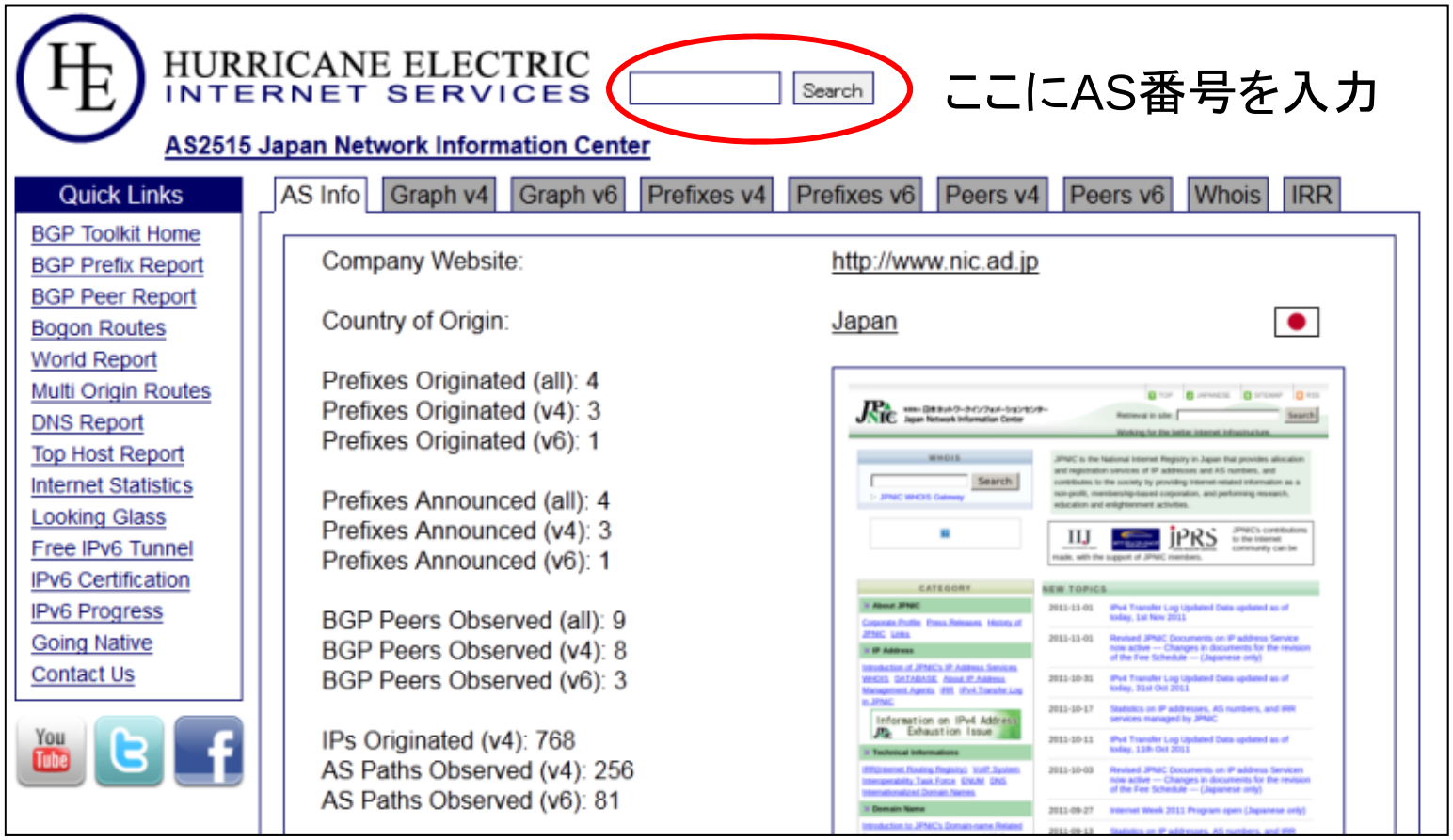
調べるだけなら

Username : guest / Password : guest でOK



https://www.peeringdb.com/

HE BGP toolkit



http://bgp.he.net/

どう解決する?

不正なOriginASに問い合わせてみる

- Looking Glassの結果等を張り付けておくとよい
- peering@やadmin@等のアドレスにも送ってみる

返事がない・知らないと言われた場合

上位ASに掛け合ってみる

- 不正なOriginASのさらに上位にあるASにコンタクトを取ってみる

奪い返す?

- 不正なOriginASが広報しているPrefixよりも
  さらにlongerなPrefixを広報して奪い返す

でも・・・

address maskフィルタに引っかかるかも

奪い返すときに設定をミスしたら??

根本的な解決方法は
不正なOriginASからの広報を停止させること

最後の手段

- janogやnanogのMLに現状を説明してみる
  - 同じようなASが他にもいるかも
  - その情報が、解決の糸口になるかも?

情報共有しましょう

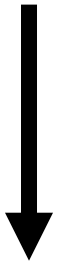
2.誤広報を自分がやってしまったら

やってしまったら

なぜ起きるか

タイプミスだって立派な誤設定

キーの打ち間違い? と思われる事例あり



外から見れば
皆同じ

誤設定による誤広報

- AS内のみに伝播させるべき経路を誤って世界中に広報した
- IPv6になったら、タイプミスが絶対増える桁も多いし、数字も多い
- やってしまった側は、なかなか気づけない

ミスに気づいたら/指摘を受けたら
すぐに解消させましょう！！

3.身近で起きたら・その時のために

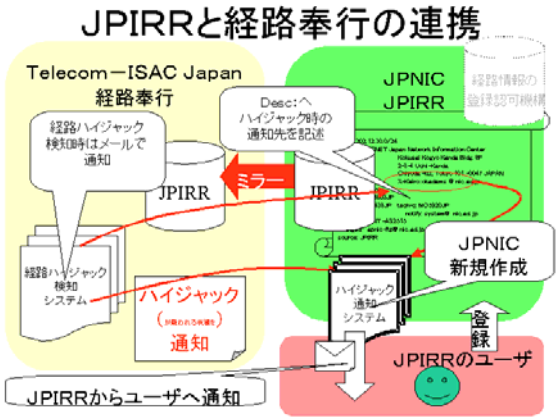
今からでもできること

起きたことを気づけるように

- JPIRRに経路情報を登録しましょう
  - X-Keiroの登録内容にも留意する
- 経路奉行以外の手段も併用する
  - IS Alarm
  - BGPMON
  - Cyclops, etc…

起きた時にどうするかを考えておく

- 対応手順の整備
  - 調査方法の詳細手順化
  - 取り返す手順等の整備　etc…



JPNICから対応についての文書が出ています

http://www.nic.ad.jp/ja/ip/irr/counter-hi-jack.html

まとめ

- 権威のない経路広告が身近で起きた時に
  - 何が起こるか理解しておく
  - 何をするべきか決めておく
- なによりも気づくことができるように
  - 検知する手段を構築する
- 自分が加害者にならないよう、十分注意する

これらの説明を踏まえて
次はIIJ 松崎さんの事例紹介