実践！ルーティングセキュリティ

実録！経路ハイジャック

株式会社ＳＴＮｅｔ
高橋　伸治

はじめに

- 当社で経験した経路ハイジャックについて、ＩＰアドレス割り振りから経路ハイジャックの発見そして問題解決までの実録情報です。
- 当社の対応方法がベストとは限りませんが一例としてご参考になれば幸いです。（当社でも状況によって見直しており当時とは部分的に異なる対応方法となっております）
- また、今回の経路ハイジャックはＩＰアドレス利用前に発覚したため実害（ユーザーへの影響）はありませんでした。
- 本資料では敬称を省略している場合がございます。ご了承ください。

時系列概要

- 2006/11/20 IPアドレス取得、RADb登録
- 2006/11/22 各社へ12/7にアナウンス追加する連絡実施
- 2006/11/30 （AS7018より広告開始）
- 2006/12/07 アナウンス追加前の確認でハイジャック発覚
  重複割り振りではないと判断しアナウンス開始
  JPNICへ問い合わせ →割り振り時には経路無かったと返答
- 2006/12/19 AS7018へ問い合わせ
- 2006/12/25 返答がないので宛先を増やし再度AS7018へ問い合わせ
- 2007/01/10 返答がないので上位のARINへ問い合わせ
  →止めさせる権限無しと返答
- 2007/01/11 JPNICへ再度問い合わせ →JPNICよりAS7018へメールを送付
- 2007/01/17 JPIRR登録
- 2007/01/26 JANOG19 in 沖縄にて“ハイジャックされてます宣言”
- 2007/01/29 IIJ 松崎さんよりAS7018へ問い合わせていただき4時間程度で
  問題解決しました。その後もMLにて対応方法などの議論有り
- 2012/11/19 登壇なう　これから実録の詳細を大公開！！

ＩＰアドレス取得

- ２００６年１１月２０日
  ＪＰＮＩＣより
  １２２．２４８．６４．０／１９
  １２３．２５４．０．０／１８
  の割り振りを受けた。

株式会社STNet(STNet) 御中

以下の IPアドレスブロックの割り当て業務を委任いたします。

STNet　委任 IPアドレスブロック: 122.248.64.0/19
123.254.0.0/18

ＲＡＤｂ登録

- ２００６年１１月２０日
  - 登録するオブジェクトが存在しないことを確認

    http://www.radb.net/

ここに入力してQueryボタンを押す

  - オブジェクト登録実施

```
NEW OBJECT CREATION:

route:      122.248.64.0/19
descr:      STCN
origin:     AS7522
notify:     stcn-adm@stnet.ad.jp
mnt-by:     MAINT-AS7522
changed:    stcn-adm@stnet.ad.jp 20061120  #10:10:29(UTC)
source:     RADB
```

```
NEW OBJECT CREATION:

route:      123.254.0.0/18
descr:      STCN
origin:     AS7522
notify:     stcn-adm@stnet.ad.jp
mnt-by:     MAINT-AS7522
changed:    stcn-adm@stnet.ad.jp 20061120  #10:07:50(UTC)
source:     RADB
```

アナウンス追加通知

- ２００６年１１月２２日
  上位プロバイダ及びｐｅｅｒ先にＩＰアドレスのアナウンスを追加する連絡を実施
  - 先方でフィルタ変更や他社への通知が必要であるため２週間程度先を追加予定日としている。

    今回は１２月７日

```
件名：アナウンス追加[122.248.64.0/19,123.254.0.0/18]

＜routeアナウンス追加＞
route: 123.254.0.0/18
descr: STCN
origin: AS7522
notify: stcn-adm@stnet.ad.jp
mnt-by: MAINT-AS7522
changed: stcn-adm@stnet.ad.jp 20061120 #10:07:50(UTC)
source: RADB

route: 122.248.64.0/19
[省略]

＜アナウンス追加作業予定日＞
2006/12/07
```

経路情報確認

- ２００６年１２月７日
  Ｉ Ｐアドレス追加前のチェック
  – トランジット接続用ルータでの確認

```
>sh ip bgp 122.248.64.0
  4713 2914 7018
  4725 3356 7018
  4716 3356 7018
>sh ip bgp 123.254.0.0
  4713 2914 7018
  4725 3356 7018
  4716 3356 7018
```

あれ？**ＡＳ７０１８から広告されている！！**

割り振り情報を再度確認しても間違っていない。

以前使っていたところがずっとルーティングしてる？

もっと情報を集めて判断しよう。

Looking Glass

- 当社外のところから経路情報を確認

  DTI Looking Glass http://neptune.dti.ad.jp/

  （Looking Glassのサイトがリストアップされていた。現在利用不可）

```
Router: cr1.ams2.nl.above.net
Command: show ip bgp 122.248.64.0/19
BGP routing table entry for 122.248.64.0/19, version 315788813
Bestpath Modifiers: always-compare-med
Paths: (1 available, best #1)
  Advertised to update-groups:
     1          3
  7018
    64.125.0.169 (metric 4217) from 64.125.0.169 (64.125.0.169)
      Origin incomplete, metric 389, localpref 100, valid, internal, best
      Community: 6461:1021 6461:1114 6461:1666 6461:2503 6461:2601 6461:2714 6461:2829
Command: show ip bgp 123.254.0.0/18
BGP routing table entry for 123.254.0.0/18, version 315788815
Bestpath Modifiers: always-compare-med
Paths: (1 available, best #1)
  Advertised to update-groups:
     1          3
  7018
    64.125.0.169 (metric 4217) from 64.125.0.169 (64.125.0.169)
      Origin incomplete, metric 389, localpref 100, valid, internal, best
      Community: 6461:1021 6461:1114 6461:1666 6461:2503 6461:2601 6461:2714 6461:2829
```

やっぱり、他社のLooking GlassでもAS7018から広告されているなぁ。

Whois(APNIC)

- Whoisで登録情報の確認

```
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:      122.248.64.0 - 122.248.95.255
netname:      STNet
descr:        STNet, Incorporated
descr:        1735-3, Kasuga, Takamatsu, Kagawa 761-0195, Japan
country:      JP
admin-c:      JNIC1-AP
tech-c:       JNIC1-AP
status:       ALLOCATED PORTABLE
remarks:      Email address for spam or abuse complaints : abuse@stnet.ad.jp
mnt-by:       MAINT-JPNIC
mnt-lower:    MAINT-JPNIC
changed:      hm-changed@apnic.net 20061120
source:       APNIC

role:         Japan Network Information Center
address:      Kokusai-Kougyou-Kanda Bldg 6F, 2-3-4 Uchi-Kanda
address:      Chiyoda-ku, Tokyo 101-0047, Japan
country:      JP
phone:        +81-3-5297-2311
fax-no:       +81-3-5297-2312
e-mail:       hostmaster@nic.ad.jp
admin-c:      JI13-AP
tech-c:       JE53-AP
nic-hdl:      JNIC1-AP
mnt-by:       MAINT-JPNIC
changed:      hm-changed@apnic.net 20041222
changed:      hm-changed@apnic.net 20050324
changed:      ip-apnic@nic.ad.jp 20051027
source:       APNIC
```

（123.254.0.0/18も同様）

Whois(JPNIC)

```
Network Information: [ネットワーク情報]
[IPネットワークアドレス]        122.248.64.0/19
[ネットワーク名]
[組織名]                        株式会社STNet
[Organization]                  STNet, Incorporated
[管理者連絡窓口]                KH853JP
[技術連絡担当者]                KH853JP
[Abuse]                         abuse@stnet.ad.jp
[割振年月日]                    2006/11/20
[最終更新]                      2006/11/20 17:00:45(JST)

Network Information: [ネットワーク情報]
a. [IPネットワークアドレス]     123.254.0.0/18
b. [ネットワーク名]             PIKARA
f. [組織名]                     Pikara(株式会社STNet)
g. [Organization]               Pikara(STNet, Incorporated)
m. [管理者連絡窓口]             JP00019853
n. [技術連絡担当者]             JP00019853
p. [ネームサーバ]               dns-p.pikara.ne.jp
p. [ネームサーバ]               dns-s.pikara.ne.jp
[割当年月日]                    2006/11/20
[返却年月日]
[最終更新]                      2006/11/20 17:53:03(JST)

上位情報
----------
株式会社STNet (STNet, Incorporated)
                    [割り振り]                          123.254.0.0/18
```

登録情報は問題なさそう。

IPアドレス国情報

STNet
Solution Technology & Network

- 割り振られたIPアドレスの国情報を念のため確認
  - 下記元データより検索

    ftp://ftp.arin.net/pub/stats/arin/delegated-arin-latest
    ftp://ftp.apnic.net/public/apnic/stats/apnic/delegated-apnic-latest
    ftp://ftp.ripe.net/ripe/stats/delegated-ripencc-latest
    ftp://lacnic.net/pub/stats/lacnic/delegated-lacnic-latest
    ftp://ftp.afrinic.net/pub/stats/afrinic/delegated-afrinic-latest

122.248.0.0	122.248.15.255	BD
122.248.16.0	122.248.31.255	HK
122.248.32.0	122.248.47.255	BD
122.248.48.0	122.248.63.255	CN
122.248.64.0	122.248.95.255	JP
122.248.128.0	122.248.191.255	JP

123.254.0.0	123.254.63.255	JP
123.254.64.0	123.254.95.255	KR
123.254.96.0	123.254.103.255	AU
123.254.128.0	123.254.255.255	KR

日本になっているので問題なさそう。

AS情報

- AS7018について元データから検索

  ftp://ftp.arin.net/info/asn.txt

  ftp://ftp.apnic.net/pub/apnic/dbase/data/apnic.an.gz

  ftp://ftp.ripe.net/ripe/dbase/split/ripe.db.aut-num.gz

  検索結果

  7018　ATT-INTERNET4

  ICC-ARIN (Tech), ATTAB-ARIN (Abuse),

  IPSWI-ARIN (Tech)

- ARIN管轄なのでARINのWhoisで調べることにした。

Whois（ARIN）

- AS7018について検索

```
OrgName:    AT&T WorldNet Services
OrgID:      ATTW
Address:    200 S. Laurel AVE.
City:       MIDDLETOWN
StateProv:  NJ
PostalCode: 07748
Country:    US

ASNumber:   7018
ASName:     ATT-INTERNET4
ASHandle:   AS7018
Comment:
RegDate:    1996-07-30
Updated:    2004-04-26

RTechHandle: ICC-ARIN
RTechName:   IP Customer Care
RTechPhone:  +1-888-613-6330
RTechEmail:  qhoang@att.com

OrgAbuseHandle: ATTAB-ARIN
OrgAbuseName:   ATT Abuse
OrgAbusePhone:  +1-919-319-8130
OrgAbuseEmail:  abuse@att.net

OrgTechHandle: ICC-ARIN
OrgTechName:   IP Customer Care
OrgTechPhone:  +1-888-613-6330
OrgTechEmail:  qhoang@att.com

OrgTechHandle: IPSWI-ARIN
OrgTechName:   IP SWIP
OrgTechPhone:  +1-888-613-6330
OrgTechEmail:  help@ip.att.net
```

問い合わせ先名とメールアドレスを入手

Whois（ARIN）

- 実はARINではAS7018に割り振られたとなっていないか確認してみる。（重複割り振り）

```
OrgName:    Asia Pacific Network Information Centre
OrgID:      APNIC
Address:    PO Box 2131
City:       Milton
StateProv:  QLD
PostalCode: 4064
Country:    AU

ReferralServer: whois://whois.apnic.net

NetRange:   122.0.0.0 - 122.255.255.255
CIDR:       122.0.0.0/8
NetName:    APNIC-122
NetHandle:  NET-122-0-0-0-1
Parent:
NetType:    Allocated to APNIC
NameServer: NS1.APNIC.NET
NameServer: NS3.APNIC.NET
NameServer: NS4.APNIC.NET
NameServer: NS.LACNIC.NET
NameServer: TINNIE.ARIN.NET
NameServer: NS-SEC.RIPE.NET
Comment:    This IP address range is not registered in the ARIN
database.
Comment:    For details, refer to the APNIC Whois Database via
Comment:    WHOIS.APNIC.NET or http://www.apnic.net/apnic-
bin/whois2.pl
Comment:    ** IMPORTANT NOTE: APNIC is the Regional Internet
Registry
Comment:    for the Asia Pacific region. APNIC does not operate
networks
Comment:    using this IP address range and is not able to
investigate
Comment:    spam or abuse reports relating to these addresses.
For more
Comment:    help, refer to http://www.apnic.net/info/faq/abuse
RegDate:    2006-01-06
Updated:    2006-01-10

OrgTechHandle: AWC12-ARIN
OrgTechName:   APNIC Whois Contact
OrgTechPhone:  +61 7 3858 3100
OrgTechEmail:  search-apnic-not-arin@apnic.net

# ARIN WHOIS database, last updated 2006-12-05 19:10
# Enter ? for additional hints on searching ARIN's WHOIS
database.
```

Whois（ARIN）

```
OrgName:    Asia Pacific Network Information Centre
OrgID:      APNIC
Address:    PO Box 2131
City:       Milton
StateProv:  QLD
PostalCode: 4064
Country:    AU

ReferralServer: whois://whois.apnic.net

NetRange:   123.0.0.0 - 123.255.255.255
CIDR:       123.0.0.0/8
NetName:    APNIC-123
NetHandle:  NET-123-0-0-0-1
Parent:
NetType:    Allocated to APNIC
NameServer: NS1.APNIC.NET
NameServer: NS3.APNIC.NET
NameServer: NS4.APNIC.NET
NameServer: NS.LACNIC.NET
NameServer: TINNIE.ARIN.NET
NameServer: NS-SEC.RIPE.NET
Comment:    This IP address range is not registered in the ARIN
database.
Comment:    For details, refer to the APNIC Whois Database via
Comment:    WHOIS.APNIC.NET or http://www.apnic.net/apnic-
bin/whois2.pl
Comment:    ** IMPORTANT NOTE: APNIC is the Regional Internet
Registry
Comment:    for the Asia Pacific region. APNIC does not operate
networks
Comment:    using this IP address range and is not able to
investigate
Comment:    spam or abuse reports relating to these addresses.
For more
Comment:    help, refer to http://www.apnic.net/info/faq/abuse
RegDate:    2006-01-06
Updated:    2006-01-10

OrgTechHandle: AWC12-ARIN
OrgTechName:   APNIC Whois Contact
OrgTechPhone:  +61 7 3858 3100
OrgTechEmail:  search-apnic-not-arin@apnic.net

# ARIN WHOIS database, last updated 2006-12-05 19:10
# Enter ? for additional hints on searching ARIN's WHOIS
database.
```

- APNICにアロケートされており問題なさそう

アナウンス開始

- ２００６年１２月７日
  - 調べた結果重複割り振りではなさそうなので予定通りアナウンスを開始することにした。
    - ＡＳ７０１８側が気づき何らかのアクションがあるかもしれない
    - 何かしているとすれば近く（特に国内）のベストパスは当社側に向いてほしい
  - また、細かいPrefixをアナウンスして取り返そうとも考えたが各社にお知らせしたPrefix長と異なることになるためそこまでは実施しなかった。

JPNICへの問い合わせ

- ２００６年１２月７日
  当社に割り振られる前の情報がわかるかもしれないと思い問い合わせを実施した。

弊社に割り振り頂いた 122.248.64.0/19 123.254.0.0/18 についてですが、AS7018 AT&T WorldNet Servicesからアナウンスされていました。
弊社に割り当てる以前はAS7018に割り振りしていたCIDRなのでしょうか？
JPNIC,APNIC,ARIN等のwhoisで調べると弊社に割り振りとなっておりましたが、それ以前のデータが参照できなかったので、以前割り振りしていたCIDRの消し忘れなのか、CIDRの乗っ取りなのか判断できなかったのでメールいたしました。

■確認した結果例(12/07 07:00 JST)
http://lg.above.net/lg.cgi
Router: cr1.ams2.nl.above.net
Command: show ip bgp 122.248.64.0/19
BGP routing table entry for 122.248.64.0/19, version 315788813
Bestpath Modifiers: always-compare-med
Paths: (1 available, best #1)
  Advertised to update-groups:
     1   3
  7018
    64.125.0.169 (metric 4217) from 64.125.0.169 (64.125.0.169)
      Origin incomplete, metric 389, localpref 100, valid, internal, best
      Community: 6461:1021 6461:1114 6461:1666 6461:2503 6461:2601 6461:2714 6461:2829
[省略]

JPNICからの回答

- 同日回答有り（２００６年１２月７日）

> IPv4アドレスの割り振りを行う場合には、APNICでは該当するアドレス空間が利用されていないことを、JPNICでは経路広告および、JPIRRをはじめとするIRRへの登録がないことを確認したうえで割り振りを行っております。
>
> 122.248.64.0/19と123.254.0.0/18の割り振りの際にも同様に、経路広告・IRRの登録がないことを確認しております。以前の割り振り先をお調べすることができず恐縮ですが、なにとぞご理解くださいますようお願い申し上げます。

この回答より、割り振り時にチェックいただいていることと、１１月２０日以降にＡＳ７０１８から該当経路がアナウンスされたことが判明した。

AS7018への問い合わせ

- ２００６年１２月１９日
  - 当社がアナウンス開始してから約２週間経過するがAS7018の経路広告は続いていたため、Whois情報から得られたメールアドレス宛に当社CIDRのBGPのアナウンスを止めてくださいとメールしてみた。

```
To: help@ip.att.net
Subject: Please stop the announcement of my CIDR.
X-Priority: 1
X-MSMail-Priority: High
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit
------------------------------------------------
AT&T[AS7018] messrs
Please stop the BGP announcement of my CIDR(122.248.64.0/19 & 123.254.0.0/18).
Your announcing data.
---
Router: cr1.ams2.nl.above.net
Command: show ip bgp 122.248.64.0/19
BGP routing table entry for 122.248.64.0/19, version 315788813
Bestpath Modifiers: always-compare-med
Paths: (1 available, best #1)
  Advertised to update-groups:
     1          3
  7018
[省略]
```

AS7018への問い合わせ（再）

- ２００６年１２月２５日
  - 返答がなかったため、宛先を２カ所増やしつつ、まだ止まってないので止めてとメールしてみる。

```
To:      abuse@att.net, qhoang@att.com, help@ip.att.net
Subject: [The second warning]Fw: Please stop the announcement of my CIDR.
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit
------------------------------------------------
The announcement has not stopped yet.
Please stop announcing immediately.
---
[元メール添付]
AT&T[AS7018] messrs
…
```

- 年明けまで待ってみたが何も返答がないため、上位のARINへ対応を依頼してみようと考えた。

ARINへの問い合わせ

- ２００７年１月１０日
  - AS7018から返答がないのでARINから止めるようにお願いできないかメールしてみた。

```
To: noc@arin.net
Subject: Please warn AS7018
Content-Type: text/plain; charset="US-ASCII"
Content-Transfer-Encoding: 7bit
------------------------------------------------
To: ARIN messrs
From: STNet[AS7522]

I sent mail to AS7018 twice.  But there was no answer.
Please warn to stop announcing from ARIN.

AS7522 CIDR 122.248.64.0/19
            123.254.0.0/18

Regards,
STNet[AS7522]
IP Control Division
〇〇
---
[AS7018へ送信したメール添付]
```

ARINからの回答

- ２００７年１月１１日
  - 止めなさいという権限がないので、この件については行動が起こせない趣旨の返答をいただく。

```
Hello:

ARIN has no authority to take action in this matter.

Regards,

American Registry for Internet Numbers
======================================
email               hostmaster@ARIN.NET
ftp                        ftp.arin.net
whois                    whois.arin.net
website             http://www.arin.net
phone                      703.227.0660
======================================
```

  - AS7018の連絡先を問い合わせしてもよかったが、Whois情報を答えられそうな気がしたので再度JPNICへコンタクトを取ることにした。

JPNICへの再コンタクト

- ２００７年１月１１日
  - 問い合わせを実施

> 昨年12月に弊社 ○○から問い合わせさせていただきました
> 新規割り振りアドレス(122.248.64.0/19 123.254.0.0/18)が
> AS7018 AT&T WorldNet Servicesからアナウンスされている件
> についてですが、弊社から連絡を試みましたが、下記の状況
> で為すすべが無い状況です。
> ・AT&T：返事無し
> ・ARIN：担当外という返事をいただく
> 対処策等、ご指導をいただけないでしょうか？

  - 同日回答をいただいた

> 現在の状況をお教えいただきありがとうございます。
> 取り急ぎ、当センターよりAS7018の割り当て先組織の窓口に一度連絡を
> 行いました(大変恐縮ですが、△△様の電子メールアドレスをCcに含め
> させていただきました)。状況が改善されない場合には改めてご相談を
> させていただければと考えております。
>
> お待たせすることになり恐縮ですが、よろしくお願いいたします。

  - 宛先はARIN DBで引けるPOCで返答無しだったみたい。
    （JANOG ML[janog:07479]より）

JPIRR登録

- ２００７年１月１７日
  - JANOG19 Meeting(沖縄)にて、経路ハイジャックのプログラムがありネタとしても使えるので話してみようと決意
  - 準備としてJPIRR登録未完了だったのでJPIRR登録権限がある△△へ登録を再度依頼（RADb登録時にも依頼していたがハイジャックの話があり中断となっていた）

```
- Date: Wed, 17 Jan 2007 20:37:41 +0900
ADD OK: [route] 122.248.64.0/19 AS7522
------------------------------------------------------------
JPNIC IRR (JPIRR) service is provided by JPNIC.

- Date: Wed, 17 Jan 2007 20:57:05 +0900
ADD OK: [route] 123.254.0.0/18 AS7522
------------------------------------------------------------
JPNIC IRR (JPIRR) service is provided by JPNIC.
```

JANOG19 Meetingにて

STNet
Solution Technology & Network

- ２００７年１月２６日
  - 経路ハイジャック～経路奉行 meets JPIRR～プログラムの質疑応答時に

“今ハイジャックされているんです”

と宣言してみた。

- 当日の朝ハイジャック継続中を念のため確認しました。
- ネタとしては面白かったと思う。
- MLに投げてみては？という意見をいただきました。
- プログラム終了後に登壇者へPrefixをお伝えし経路奉行での状況などを確認していただけることになりました。

JANOG ML

- ２００７年１月２９日～１月３１日

ＭＬから時系列に要点をピックアップ及び補足した内容です。

- 経路奉行・IRR-ZEBRAでの検知状況
  - １１月３０日よりAS7018(AT&T)より広告検知
  - １２月７日よりAS7522(STNet)より広告検知
  - それ以降は１ASからのみ検知（AS7522がベストパスに見えることが多いため）
  - １月１７日以降はハイジャックとして検出（ＪＰＩＲＲにオブジェクト登録したから）
- ＪＰＮＩＣ方面
  - ＩＰアドレス割り振り時には経路広告無しだった
  - リナンバリングはＡＰＮＩＣとの関係があり難しい
- ＩＩＪ　松崎さん
  - 連絡したら数時間後に返信があって1/29 16:30JST頃該当経路が消えていることを確認

> I have removed the statics and asked our customer care center to check how they even came into the network.
> I'm terribly sorry for the problem this might have caused to you and/or your customer

  - janog@janogに投げてみるのも解決手法の一つとして有効

JANOG ML続き

STNet
Solution Technology & Network

- JPNIC方面
  - ARIN DBで引けるPOCでのコンタクトでは応答無し
  - 太いパイプが必要かも
    - Peering Contact
    - 担当者同士が仲良い
  - 対応方法として
    - NANOGでは「ISP***の人、個人的にメール頂戴」なんてことを結構やりますのでNOGを使うというのは本質的な使い方
    - NOG以外ではアップストリームISPにお願いしてみる。顧客関係をたどると生成元にたどり着ける
  - 技術的な切り口として
    - なぜこの不正広告が発生したか？
      （AS7018からの回答待ち）

JANOG ML続き２

STNet
Solution Technology & Network

- ＩＩＪ　松崎さん
  - 今回はWebで公開されている情報からNOC contactを探し出して、簡単な英語でよろしくと投げた。
  - 対応依頼は担当者に読んでもらえるように
    - 事象
    - 証拠
    - 依頼内容

    を端的に書いておいて、内部での対応とかエスカレーションが適切に行われるように気をつけている。

    後は
    - Subjectに問題内容を簡潔に書く
    - Content-Typeに気をつける
  - もちろん、連絡できるパイプを色んなところに持っておくと、色んな場面で助かります。

JANOG ML続き３

– Subjectはどのように書く？
  - Routing complaint from asxxx
  - Hijacked netblocks – ATT/AS7018 ← 今回の返信有りパターン
– メールの宛先は？
  - Whoisで検索して出てきた宛先だと返信無しだった。
  - この手の話はNOCのエンジニアに届かないと話が進まないのでNOCの連絡先を探す。

    NOC list(http://puck.nether.net/netops/nocs.cgi)を調べたところNOC contactはそのままnoc@att～だったので、そこに連絡した。
– list
  - NOG http://www.bugest.net/nogs.html
  - Peering DB https://www.peeringdb.com/

参考：NOC List

- http://puck.nether.net/netops/nocs.cgi

To contribute your NOC's entry to this list, please fill out this form.

This list is to be used only to contact NSP's for urgent matters. Permission to mirror this list is permitted. Many thanks to everyone who has helped me to complete this list so far, and for everyone who submits their portion.

All nocs are assumed 24x7 unless otherwise noted in the hours column

Please report any problems with this page to me, includingout of data data reports, etc

You can search this list.

ここから検索できる

これは検索可能なインデックスです。検索キーワードを入力してください:

	Provider	Domain Name(s)	ASN(s)	NOC Toll Free Number	NOC Direct	Customer Service Toll Free	Customer Service Direct	E-Mail	Hours	
report as spam/invalid										Edit
report as spam/invalid	Akamai Technologies	akamai.com, akamai.net, akadns.net	20940	+1 877-625-2624	+1 617-444-3007	+1 617-444-4699		noc@akamai.com	24/7	Edit
report as spam/invalid	Arbinet-thexchange	arbinet.com, arbinet.net	18534, 18695, 12885	866-708-0809	703-456-4132	703-456-4132		support@arbinet.net	24x7	Edit
report as spam/invalid	Arcnet	arc.net.my	AS10204		+60-3-8311 2050			noc@arc.net.my	0900-1730	Edit
report as spam/invalid	Ardent Communications (CAIS Internet)	Ardentcomm.com	3491	888-224-7662, o				noc@nocshell.cais.net, noc@postal.a	24/7	Edit
report as spam/invalid	ArgoNet	ArgoNet.net		800-626-6515	1-310-263-4800	1-310-263-4800		noc@val.net	24x7	Edit
report as spam/invalid	Arrival Communications	arrival.net arrival.com	18876		1-661-716-9002			noc@arrival.com	24x7x365	Edit
report as spam/invalid	as250.net	as250.net	250		+491777761111			noc@as250.net	24/7	Edit
report as spam/invalid	Asia Online (Hong Kong) Ltd	asiaonline.net	4614		852-2612-2043			noc@asiaonline.net	7x24	Edit
report as spam/invalid	Assertive Networks	assertivenetworks.net	30092, 32286		604 687 4677	604 687 4678		noc@assertivenetworks.net	24/7/365	Edit
report as spam/invalid	Associated Networks Limited (AnlX)	anlx.net	25061		+448450034121			ipns@anlx.net	24x7	Edit
report as spam/invalid	Astra t/a (eu-X / VECNet GB / JIPPII UK)	astra.net.uk eu-X.com as8785.net	8785 9153	n/a	+44 (0) 7659 101 118	+44 (0) 207 152 1000		noc@eu-x.com	24/7	Edit
report as spam/invalid	Astral Telecom	astral.ro	6746		40311000510			noc@astral.ro	24x7	Edit
report as	Athena (Brasil)	athena-netsec.com.br			+55 61 321-0505			noc@athena-netsec.com.br	9-18 -300 GMT	Edit

- noc@～の登録が結構多いので宛先に入れてみるのも良いかも。

参考：NOG List

- http://www.bugest.net/nogs.html

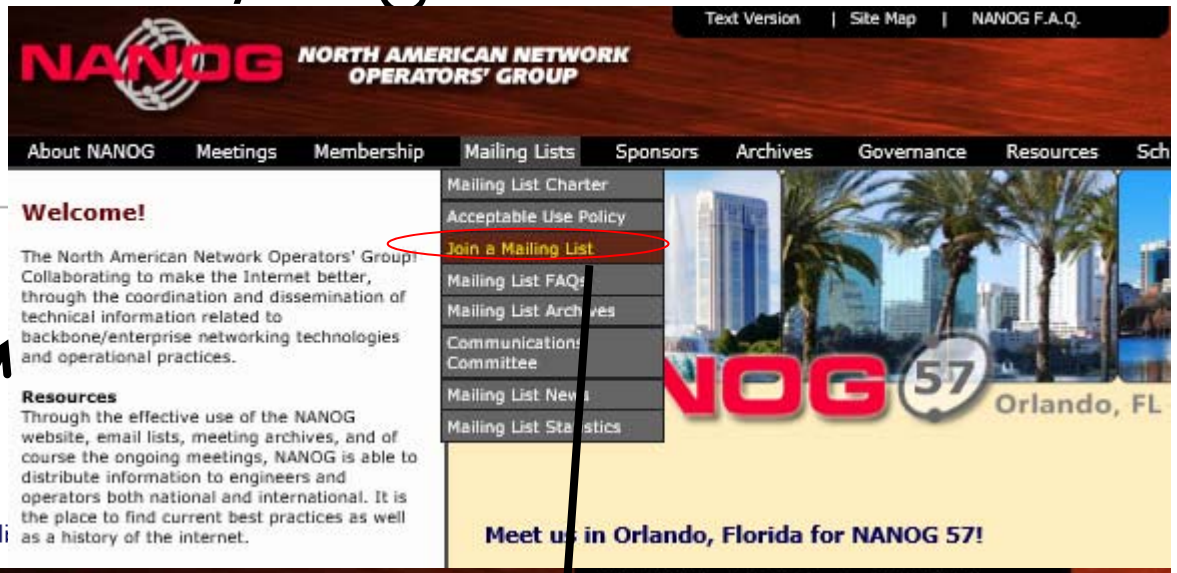
Network Operators Group List

JAPAN

- ANOG - Akita Network Operators' Group
- JANOG - Japan Network Operators' Group

World Wide

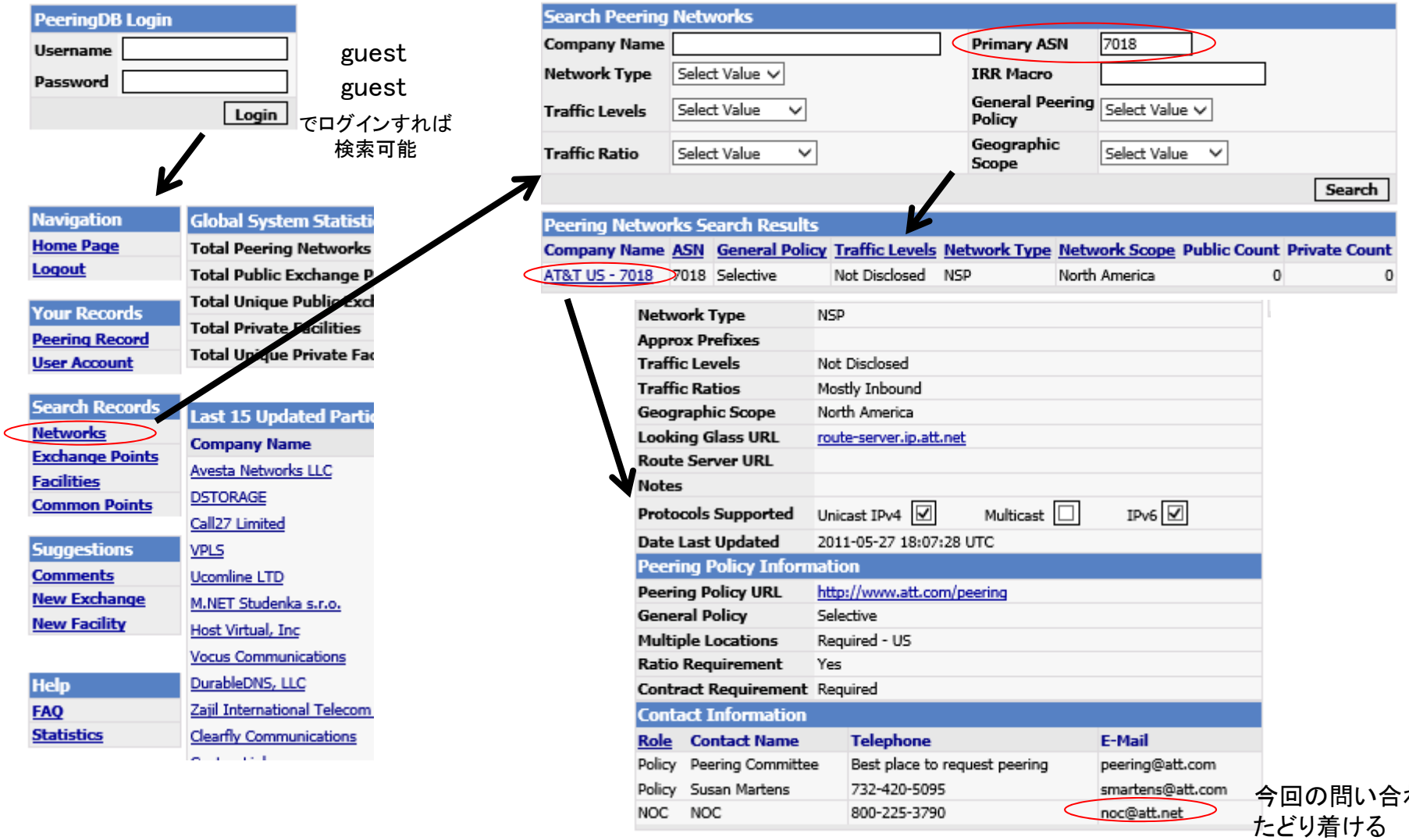
- AfNOG - The Africa Network Operators Group
- APOPS - The Asia Pacific OperatorS Forum
- AusNOG - The Australian Network Operators Group
  - aussie-isp - Australian ISP mail list (aussie-isp@aussie.net) -> This li
- CNNOG China Network Operators' Group
- DENOG - The German Network Operators Group
- FRnOG - The FRench Network Operators Group
- EOF - The European Operators Forum
- ESNOG/GORE - Grupo de Operadores de Red Espan˜ol
- GTER - Grupo de Trabalho de Engenharia e Operacao de Redes
- IE-NOG - Irish Network Operators Group
- INNOG - Indian Network Operators Group
- LACNOG - Latin America and Caribbean Region Network Operato
- MENOG - Middle East Network Operators Group
- NANOG - The North American Network Operators' Group
- ngNOG - Nigerian Network Operators' Group
- NLNOG - The Netherlands Network Operator Group (Dutch)
- NordNog - The Nordic Operator Group
- NSP - Networkers' Society of Pakistan
- NZNOG - New Zealand Network Operators' Group
- PACNOG - The Pacific Network Operators Group
- PhNOG - Philippine Network Operators Group
- PLNOG - Polish Network Operators Group
- SANOG - South Asian Network Operators Group
- SWINOG - Swiss Network Operators Group
- trnog - Turkiye Network Operatorleri Grubu
- UKNOF - The United Kingdom Network Operators' Forum



MLへの登録はこちらから

参考：Peering DB

- https://www.peeringdb.com/



今回の問い合わせ先にたどり着ける

まとめ（JANOGで解決）

STNet
Solution Technology & Network

- 約２ヶ月間続いていた経路ハイジャックがJANOGの皆様のおかけで数日間で解決いたしました。ありがとうございました。
- NOGを有効活用するのは良いと思いますが、まずは自らできることを実施し、その後協力を仰ぐ必要があると判断したら相談してみるのが良いかなぁと個人的には思います。
- まずは各種ツールやリストを活用しましょう。

  （けどwhois情報は・・・）
- 最近原因報告ありました？とIIJ 松崎さんに聞いたのですがあれからは音沙汰無しのようです。問題解決したと言えども気になりますが・・・。

参考：原因を想像

- オペミス？

  連続していない２つのPrefixを両方ともハイジャックされたので数字の打ち間違いは考えにくい。

- スパム送信に利用された？

  未割り振り空間より割り振られた空間の方がスパムメールの到達率は高いように思える。

  もしかしたら割り振られているのに使われていないPrefixとして狙われた？

  その場合、AT&T自体ではなく、恐らくその配下の利用者からPI登録の申請があって追加したとか・・・。

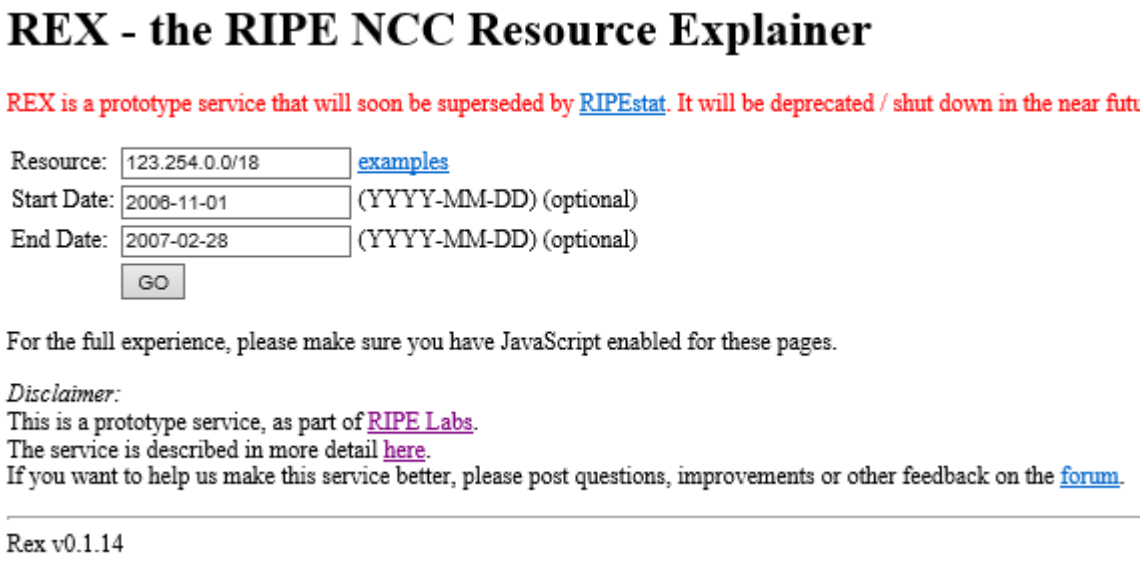
- 他には？　結局のところわかりませんでした

参考：いつ発生したか？

- 発生原因はわかりませんでしたが、いつ発生したかは下記サイトで検索できる可能性があります。

REX – the RIPE NCC Resource Explainer

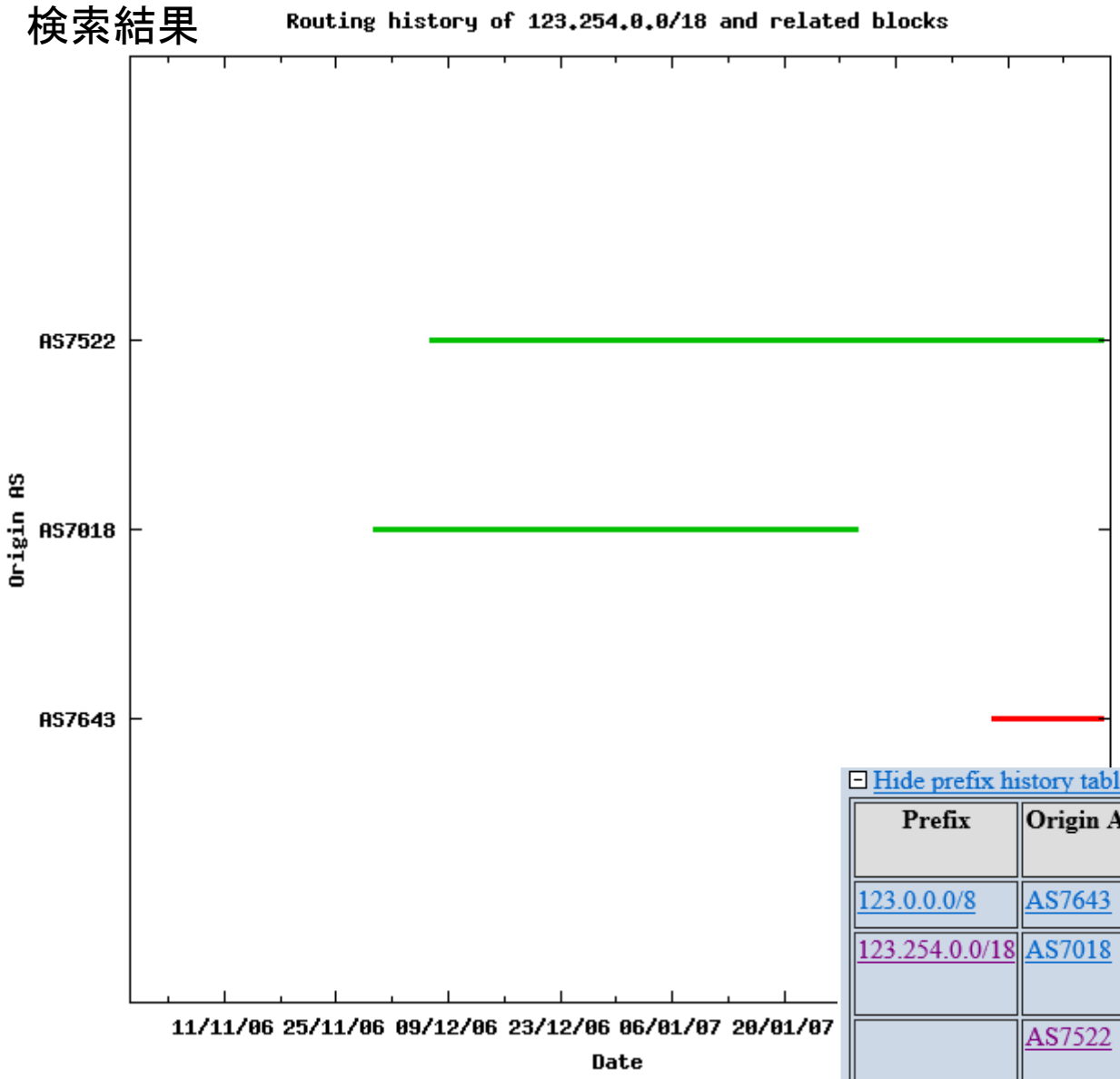
http://albatross.ripe.net/cgi-bin/rex.pl



ResourceにはIPアドレスやAS情報を入力
表示したい期間を設定しGOをクリック

参考：いつ発生したか？

検索結果



結果ページのprefix history tableをクリックすると観測された期間がわかります。

Hide prefix history table

Prefix	Origin AS	From	To	avg #peers
123.0.0.0/8	AS7643	2007-02-15 08:00Z	2007-02-28 16:00Z	88
123.254.0.0/18	AS7018	2006-11-30 00:00Z	2006-12-31 16:00Z	30
		2007-01-01 00:00Z	2007-01-29 00:00Z	18
	AS7522	2006-12-07 00:00Z	2006-12-31 16:00Z	78
		2007-01-01 00:00Z	2007-02-28 16:00Z	95

参考：ハイジャック検知方法

- 経路奉行を活用させていただく（期間限定）
  - **Telecom-ISAC Japan経路奉行とJPIRR間の連携実験について**
    http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html
    - 'X-Keiro: 電子メールアドレス'をオブジェクトに追加することでハイジャックを通知してくれます。
    - 利用するときはハイジャックを受けた際にメールが届かない可能性を想定し複数メールアドレス（サーバがNW的に分離されていること）を登録した方が良いと思います。
      - メールサーバの情報を登録しているDNSサーバが使っているPrefixがハイジャックされてしまったら、MXレコードのQueryが届かず通知不可となる。
      - メールサーバ自体が使っているPrefixがハイジャックされてしまったら、メールサーバに接続できずに通知不可となる。
    - **【※実験期間を2013年3月31日まで延長いたしました(2012年4月27日追記)】**となっていますがいつまで延長していただけるのだろう。

参考：その他の役立つサイト

STNet
Solution Technology & Network

- 経路ハイジャックが疑われる状態発生時の対応について
  - http://www.nic.ad.jp/ja/ip/irr/counter-hi-jack.html
- 最近利用させてもらっているLooking Glass
  - http://www.ris.ripe.net/cgi-bin/lg/index.cgi
  - http://lg.above.net/lg.cgi
  - http://bgp4.jp/

参考：実際使い始める前に

STNet
Solution Technology & Network

- 最近ではハイジャックされて無くてもIPアドレスを利用開始する前に確認することがあったりします。
  （IPアドレスの健全性チェック）
  - RBLに登録されていないか？
  - 特定サイトにアクセス可能か？
    - 米国系のESTA,台風情報,日食情報など
    - 韓国系のホテルサイトなど
    - 国内の動画コンテンツサイトやゲーム関係など
  - 経路情報の到達性は？

  ハイジャック同様に先方と連絡を取り問題解決してきましたが、先方はそういう状況に気付いてないことが多く結構大変だったりします。

  この辺の実録は機会があれば・・・。

皆様ご静聴ありがとうございました。

最終日の懇親会も出席しますのでご質問はお気軽に