実践！ルーティング

困ったときのために

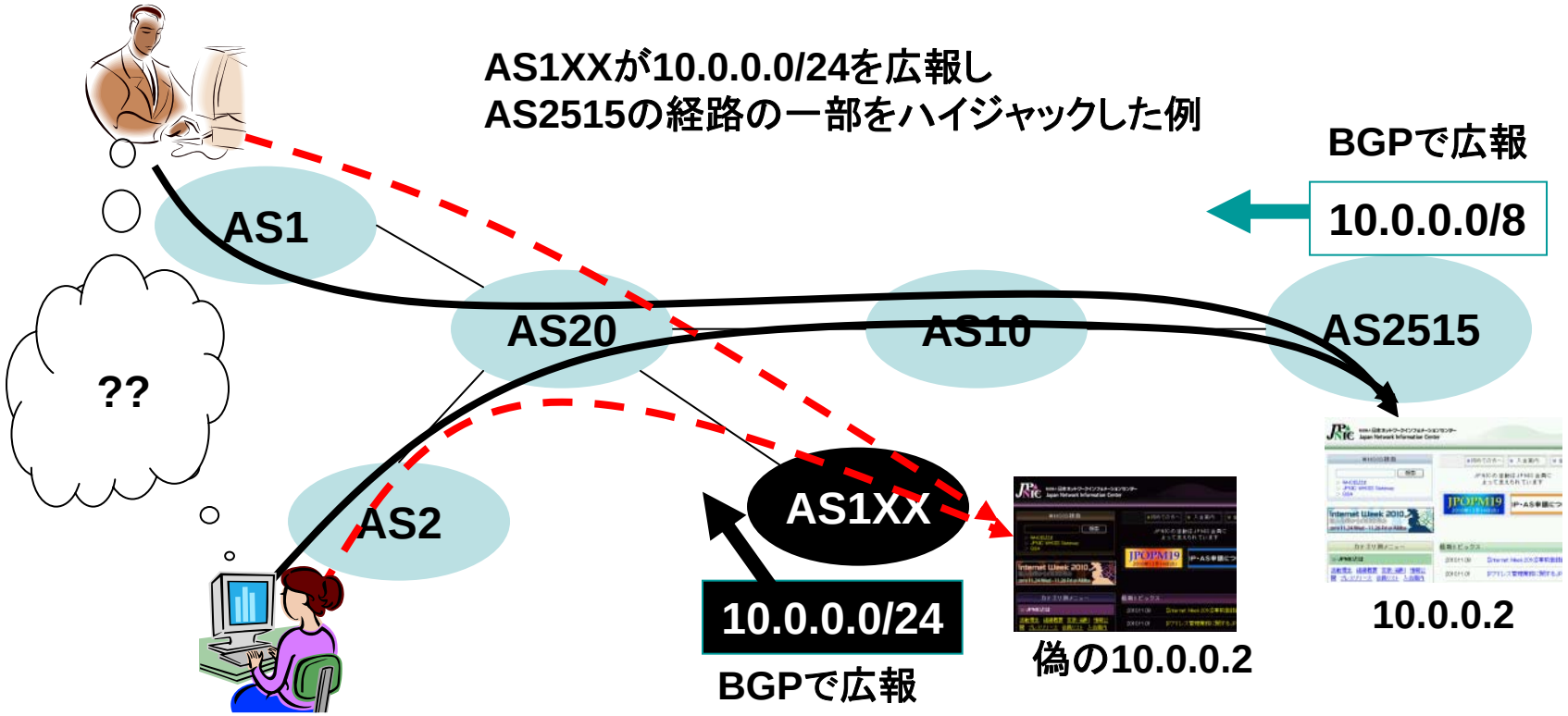
KDDI株式会社 / Telecom-ISAC JAPAN
中野 達也

自己紹介

- 2000年4月 TTNet(東京通信ネットワーク株式会社)に入社
  出向・合併を経て今の会社(KDDI株式会社)に至る
- 10年在職して、そのほとんどが運用・保守部門
- インターネット関連業務(TTCN/PoweredInternet/KDDI InternetGateway)と
  広域イーサネット関連業務(PoweredEthernet)に従事
  (いずれも約5年従事)
- Telecom-ISAC JAPANとの関係：2008年10月からBGPWGに参加。今年度は書記担当

経路ハイジャックについて

「不正な経路情報が交換(広報)されることにより、インターネットにおける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」



もくじ

1. 経路ハイジャックの被害を受けた場合
   - 何が起こる?
   - どうやって調べる?
   - どうすればよい?
   - お客様が被害を受けていたら?
2. 経路ハイジャックに関わってしまったら
   - 誤設定による誤広報
3. 今からでもできること
   - すぐに分かるようにする
   - 起きた時にどうするかを考えておく

1.経路ハイジャックの被害を受けた場合

被害者になったら

何が起こる?(1)

トラフィックが急減する・エンドユーザからの申告
何も起きない???・短時間だったから気づけない

↓ 困ったことに

発生してすぐに検知する手段がなかった
(海外にはあるけど、日本国内では・・・)

↓ そこで

経路ハイジャック通知実験(Powered by 経路奉行)

海外の検知システムとの比較

	ISAlarm	BGPmon	経路奉行
経路の情報源	RIPE-RIS	RIPE-RIS Route-view	国内ISP(複数)の経路情報
検知方法	ユーザ入力情報との比較	ユーザ入力情報・IRRとの比較	JPIRRとの比較
通知方法	Web、メール syslog	Web、メール RSS	JPNIC連携によるメール通知

BGPMON http://bgpmon.net/
ISAlarm https://www.ripe.net/is/account/login
(いずれも事前登録要)

何が起こる?(2)

- 経路ハイジャック通知実験メールが届きます
  - 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

何が起こる?(3)

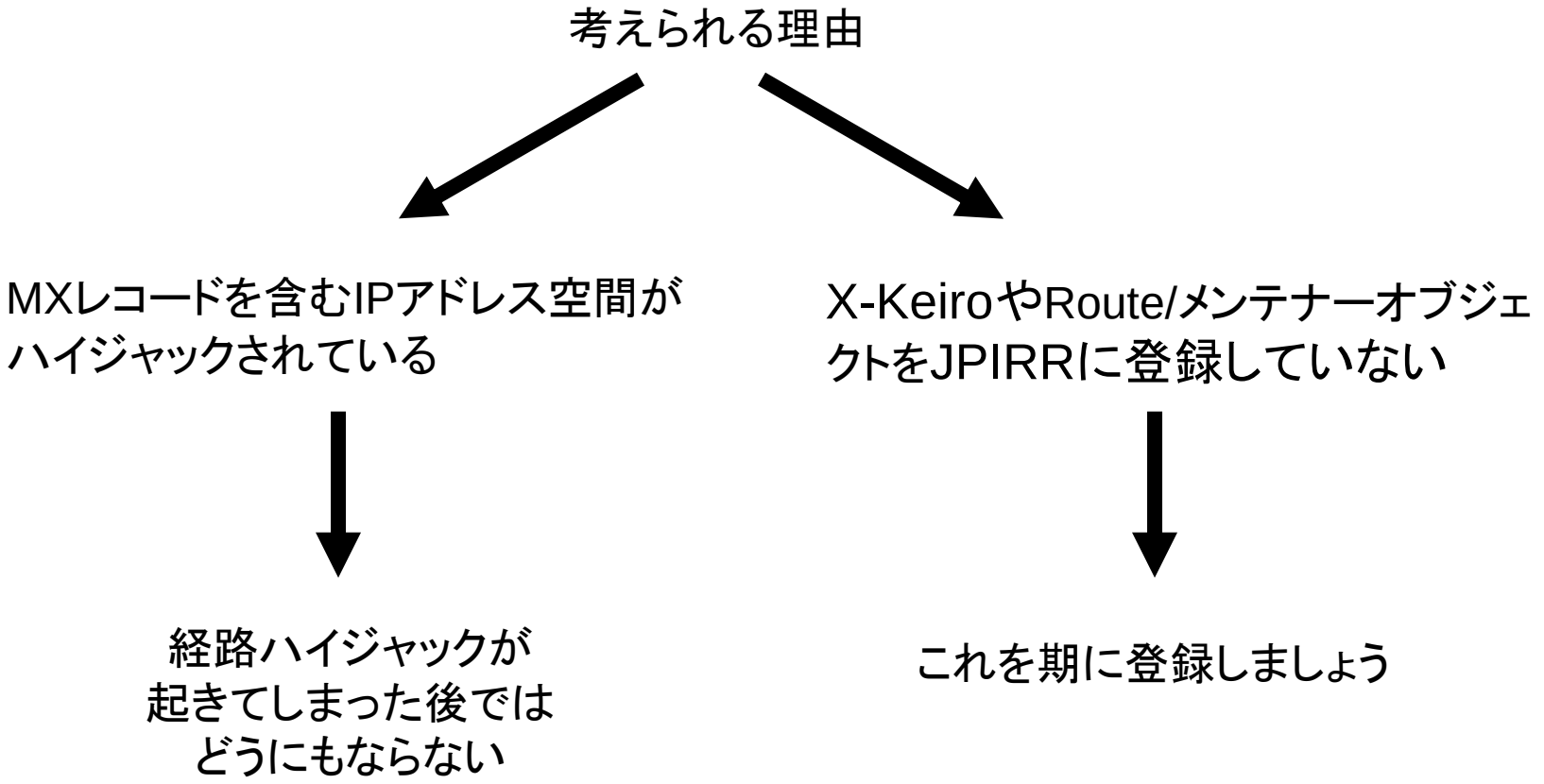
- X-Keiro?
  - 登録例
    whois –h jpirr.nic.ad.jp MAINT-AS2515

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

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

何が起こる?(4)

- 経路ハイジャック通知実験のメールが来ない



どうやって調べる?(1)

- JPNICから来た「経路ハイジャック通知実験」メールを参照・確認する

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	: Wed 24 Nov 2010 10:30:00 +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
検知したOrigin	: AS4716

「検知したOrigin」という項目が追加されます(予定)

どうやって調べる?(2)

- Looking Glassで調べる
  - show ip bgp
    自AS以外のOriginが存在するかを確認できる
  - traceroute
    どこのASに流れているかを確認できる

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

traceroute.org
http://www.traceroute.org/

どうやって調べる?(3)

- 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

大丈夫そうな例

```
BGP routing table entry for 192.168.0.0/17

 1930 20965 2516  2515
  193.136.5.1 from 193.136.5.1 (193.136.5.1)
    Origin IGP, localpref 100, valid, external
    Last update: Fri Oct 15 19:51:37 2010

 9304  4713 2515
  218.189.6.2 from 218.189.6.2 (218.189.6.2)
    Origin IGP, localpref 100, valid, external
    Last update: Thu Oct 14 12:53:42 2010
```

OriginASが自ASである

経路ハイジャックが疑われる例

```
BGP routing table entry for 172.18.100.0/19

 17676 4713  2515
  218.189.6.2 from 218.189.6.2 (218.189.6.2)
    Origin IGP, localpref 100, valid, external
    Last update: Thu Oct 14 12:53:42 2010

 23456 23456 2516 4716
  195.47.235.100 from 195.47.235.100 (195.47.235.100)
    Origin IGP, localpref 100, valid, external
    Last update: Thu Sep 30 09:40:50 2010
```

OriginASに意図しないASが混じっている
(意図しないASしかない場合も)

どうやって調べる?(4)

- 不正なOriginASがわかったら
  そのASの連絡先を調べる
  - whoisで調べてみる
    例 whois –h whois.nic.ad.jp “AS 4716”
    - JPNICハンドルを確認しましょう

whois –h whois.nic.ad.jp “AS 4716”

```
Autonomous System Information: [AS情報]
a. [AS番号]                    4716
b. [AS名]                      POWEREDCOM
f. [組織名]                    KDDI株式会社
g. [Organization]              KDDI Corporation
m. [管理者連絡窓口]            DK1011JP
n. [技術連絡担当者]            DK1011JP
（以下、省略）
```

whois –h whois.nic.ad.jp “DK1011JP”

```
Contact Information: [担当者情報]
a. [JPNICハンドル]             DK1011JP
b. [氏名]                      古俣 大吾
c. [Last, First]               Komata, Daigo
d. [電子メイル]                dkomata@example.jp

（以下、省略）
```

どうやって調べる?(5)

- whoisで調べてみる
  - 例 whois –h whois.radb.net AS4716
  - notifyやmnt-byを確認しましょう

whois –h whois.radb.net AS4716

```
aut-num:     AS4716
as-name:     POWEREDCOM
descr:       POWEREDCOM, Garden Air Tower,
             3-10-10,Iidabashi,Tiyoda-ku,Tokyo,
             102-8460,Japan
admin-c:     Daigo Komata
tech-c:      Daigo Komata
mnt-by:      MAINT-AS4716
changed:     wataru@example.jp 20071019
source:      RADB
```

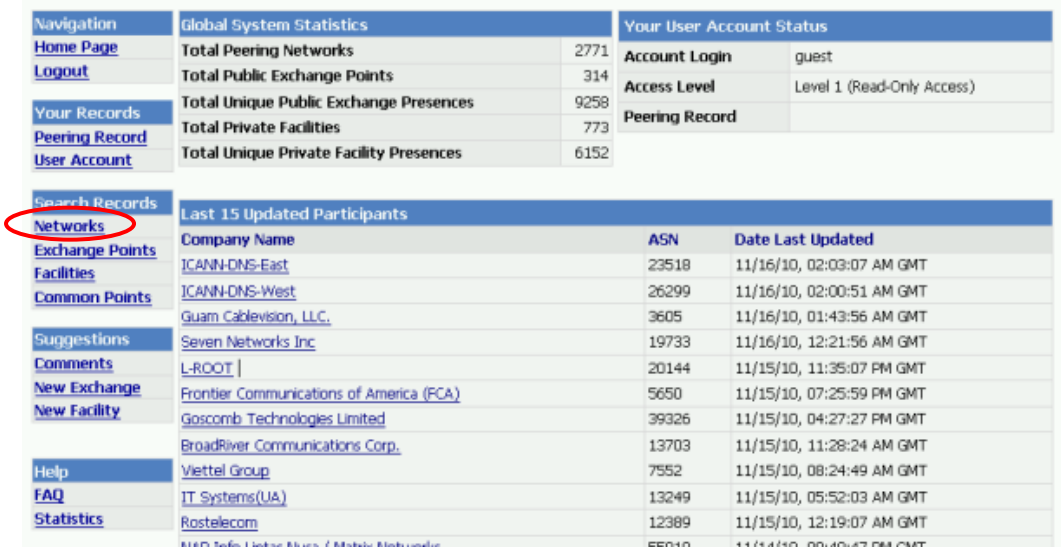
whois –h whois.radb.net MAINT-AS4716

```
mntner:      MAINT-AS4716
descr:       KDDI Corporation
admin-c:     Daigo Komata
tech-c:      Daigo Komata
upd-to:      dkomata@example.jp
mnt-nfy:     dkomata@example.jp
auth:        PGPKEY-9F8D53C0
auth:        PGPKEY-E73E1C50
auth:        PGPKEY-25D4A18E
mnt-by:      MAINT-AS4716
changed:     mine@example.jp 20100228
source:      RADB
```

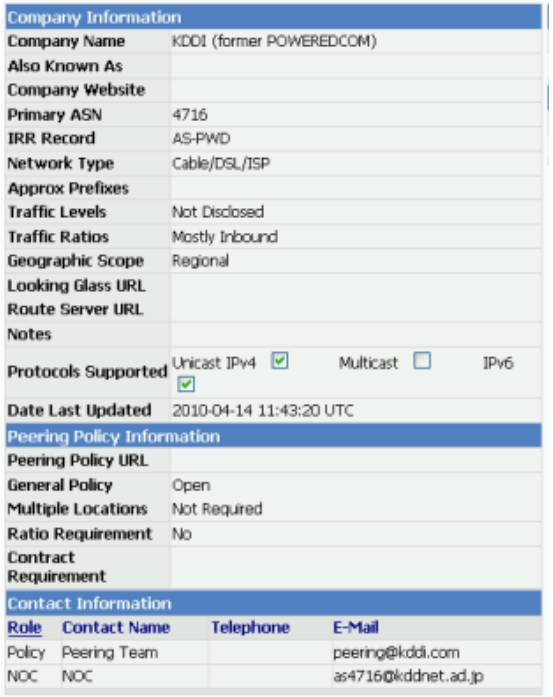
どうやって調べる?(6)

- PeeringDBで調べる

  調べるだけなら Username : guest 、Password : guest でOKです



PeeringDB https://www.peeringdb.com/



結果出力例

どうすればよい?(1)

不正なOriginASに問い合わせてみる

- noc@やpeering@等のアドレスにも送ってみる
- ミスオペレーションに気づいていないだけかも
- いきなりけんか腰はやめる

それでもだめなら

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

どうすればよい?(2)

- それでも反応がない場合の最終手段
  - janogやnanogのMLに現状を説明してみる
  - 同じように被害を受けているASが他にもいるかもしれません
  - あなたの情報が、解決の糸口になるかもしれません

情報共有は大事です

どうすればよい?(3)

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

↓

  - さらにlongerなPrefixを広報してきたら・・・
  - address maskフィルタに引っかかる可能性がある
  - 奪い返すときに設定をミスしたら??
  - インターネット上の経路数を増やすことになる

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

お客様が被害を受けていたら?

- 自ASのIPアドレス(PA)割り当て空間なら
  自社(自AS)で対応しましょう
  ※ PA : Provider Aggregatable : プロバイダ集約可能アドレス

- お客様がAS番号を取得されている場合
  最低限、以下のことをお聞きしましょう
  - ハイジャックされている疑いのあるPrefix
  - (分かっていれば)不正なOriginAS
  - 経路ハイジャック通知実験のメールがあれば
    見せていただく

2.経路ハイジャックに関わってしまったら

気づかないうちに
加害者になってしまったら

誤設定による誤広報(1)

- 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

そんな間違いだって
経路ハイジャックです！！

誤設定による誤広報(2)

- 問題は設定ミス
  - 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
    - private ASや不要トラフィック遮断のためのBlackhole設定を世界中に広報してしまった
  - IPv6になったら、タイプミスを含めて絶対増える

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.今からでもできること

経路ハイジャックが
自分の身に降りかかる前にできること

すぐに分かるようにする

- 検知できるようにする
  - JPIRRに登録しましょう
    ルートオブジェクト or メンテナーオブジェクトに
    X-Keiroを登録すると、**経路奉行**の監視対象になる
    →JPNICからの通知実験メールが届くようになる
  - X-KeiroはMXを含む空間がハイジャックされたときのことも考慮しましょう(複数のMXを登録する、等)
  - PIアドレスに対するケアも忘れずに行いましょう
    登録・変更漏れは、誤報や検知漏れを生みます
    ※PI : Provider Independent : プロバイダ非依存アドレス

起きた時にどうするかを考えておく

- 調査方法をまとめておく
- エスカレーション体制を整える
- 細かい経路を広報する手順を作成する

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

- 経路ハイジャックの被害を受けたとき
  どうするかを考えておきましょう
- もしものために、すぐに検知できる
  体制をえましょう
  – そのためにJPIRRへの登録を是非
- 自分が加害者にならないよう
  十分注意しましょう