どうする？経路ハイジャック

ソフトバンクBB株式会社
平井 則輔
norisuke.hirai@g.softbank.co.jp

SoftBank

はじめに、簡単な自己紹介

SoftBank

平井　則輔(ひらい のりすけ)

- ソフトバンクBB
  - AS17676の対外接続設計/構築
  - IPアドレス管理/設計
- JANOG
  - 発表
    - ✓ J23@高知 IPアドレス移転
    - ✓ J25@新潟 6rd

  - 3月から運営委員になりました。
    宜しくお願いします。 m(_ _)m

モチベーション

SoftBank

JANOG31.5 Interim Meeting

開催概要
プログラム
会場案内
出席登録

プログラム詳細

タイトル

どうする？経路ハイジャック

概要

経路ハイジャックされたら大変だし、自分もコンフィグミスで経路ハイジャックしちゃうこともあるかもしれない。だから、フィルタリングや経路広報は慎重にやろうというのは、誰も異論のない共通のコンセンサスだと思います。
でも、心のどこかに、「インターネットだから、世界のどこかで誤って経路広報されちゃうこともあるよね」と、他人事とはいかないまでも、そういうものだという、諦観に似た気持ちを持っていたりしませんか？正直、自ASの経路がハイジャックされるまで、僕はそうでした。

最近、実際に経路ハイジャックされ、たくさんのことを感じました。
その時感じたことをもとに、みなさんとより良いオペレーションについて議論し、一緒に考えられたらと思います。

発表者

平井 則輔(ソフトバンクBB株式会社)

http://www.janog.gr.jp/meeting/janog31.5/program/bgp-route-hijacking.html

モチベーション

SoftBank

JANOG31.5 Interim Meeting

- 開催概要
- プログラム
- 会場案内
- 出席登録

プログラム詳細

タイトル

どうする？経路ハイジャック

概要

経路ハイジャックされたら大変だし、自分もコンフィグミスで経路ハイジャックしちゃうこともあるかもしれない。だから、フィルタリングや経路広報は慎重にやろうというのは、誰も異論のない共通のコンセンサスだと思います。
でも、心のどこかに、「インターネットだから、世界のどこかで誤って経路広報されちゃうこともあるよね」と、他人事とはいかないまでも、そういうものだという、諦観に似た気持ちを持っていた

2013年1月11日と3月6日　3か月で2回

で、僕はそうでした。

最近、実際に経路ハイジャックされ、たくさんのことを感じました。
その時感じたことをもとに、みなさんとより良いオペレーションについて議論し、一緒に考えられたらと思います。

発表者

平井 則輔(ソフトバンクBB株式会社)

http://www.janog.gr.jp/meeting/janog31.5/program/bgp-route-hijacking.html

まず、みなさまに質問

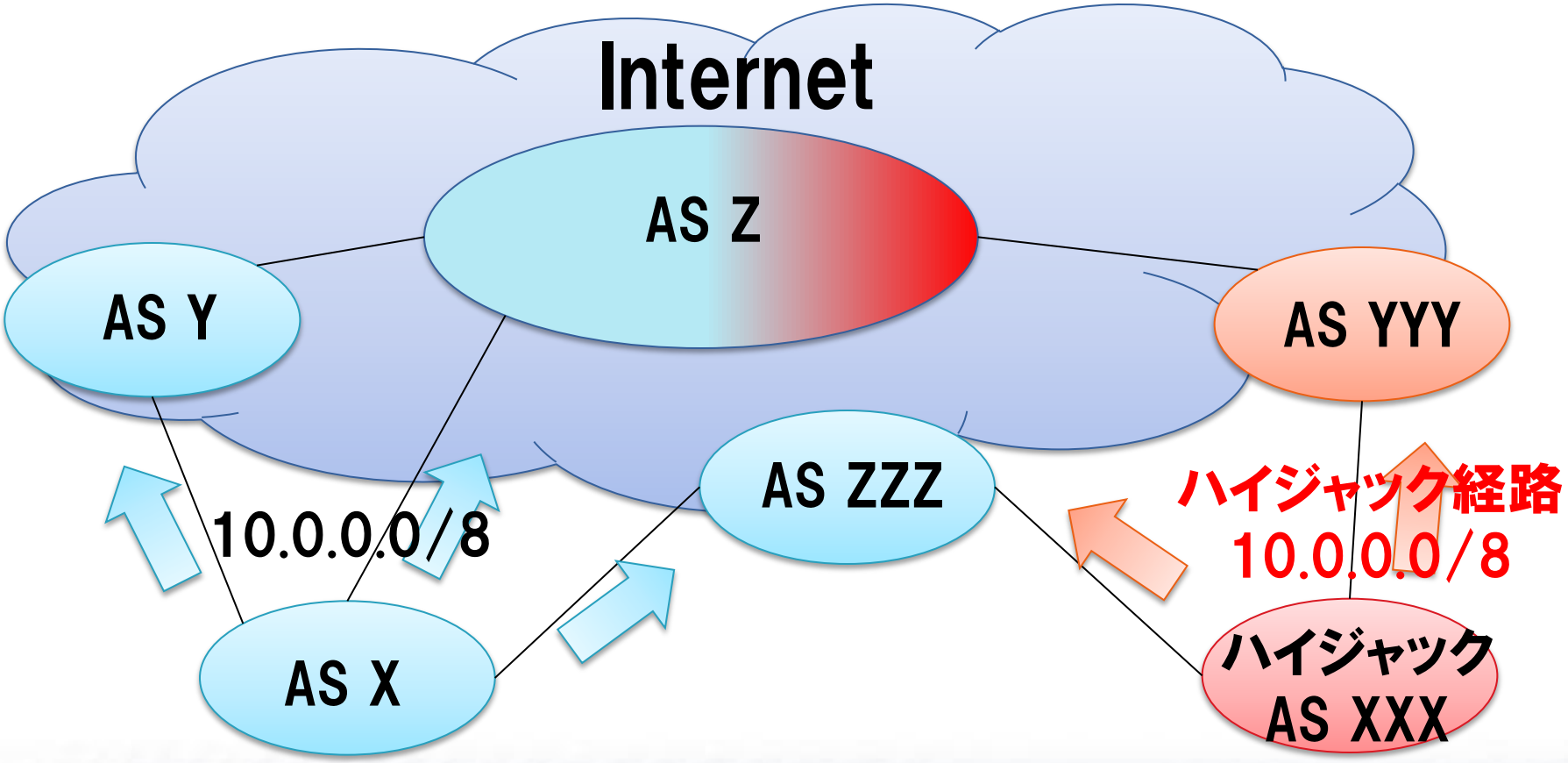
SoftBank

- ISPの方どれくらい？
- 経路ハイジャックに遭った人？
- 経路ハイジャック対応準備は万端？

経路ハイジャック

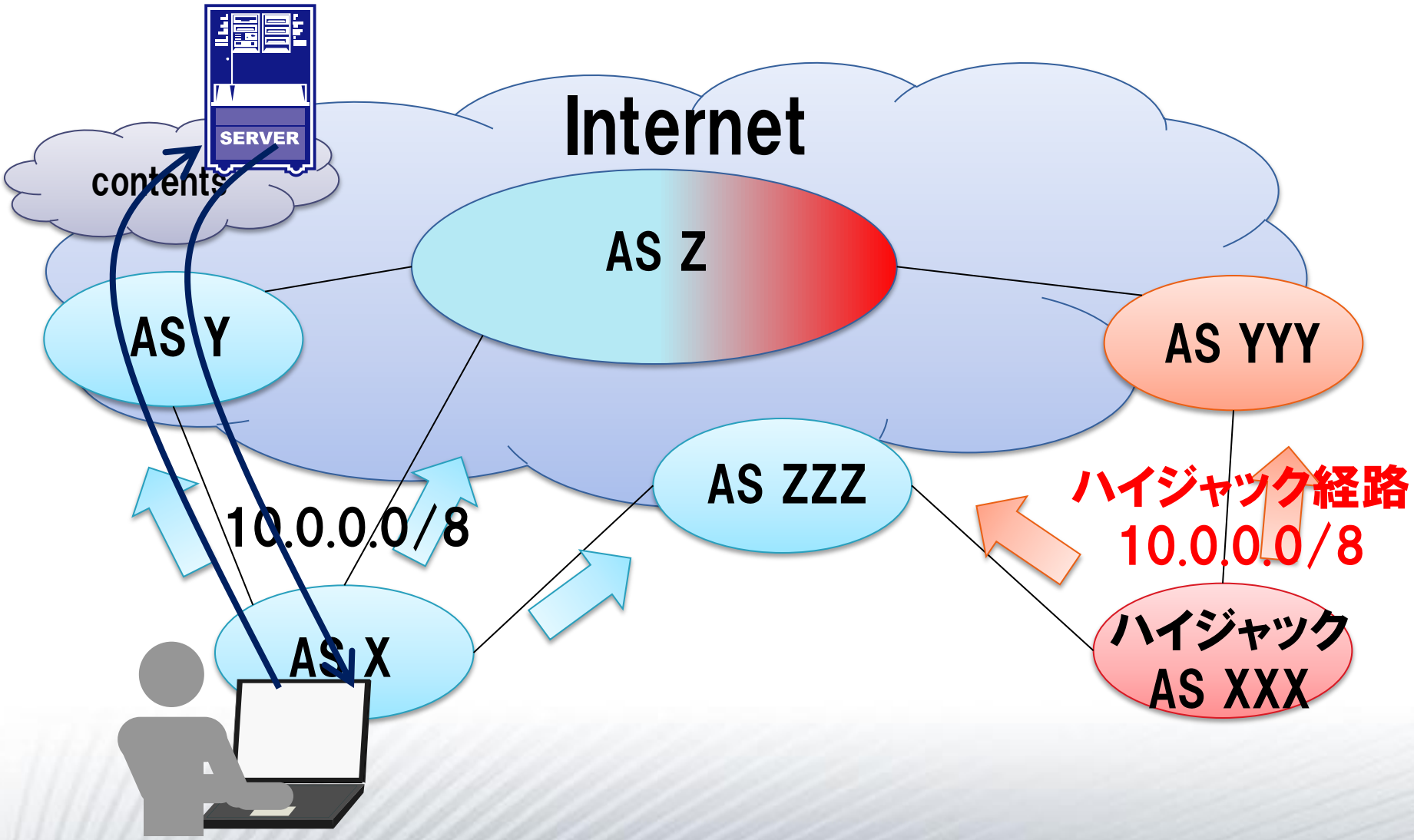
SoftBank

故意もしくは誤って他ASの経路を広報してしまうこと。



経路ハイジャック

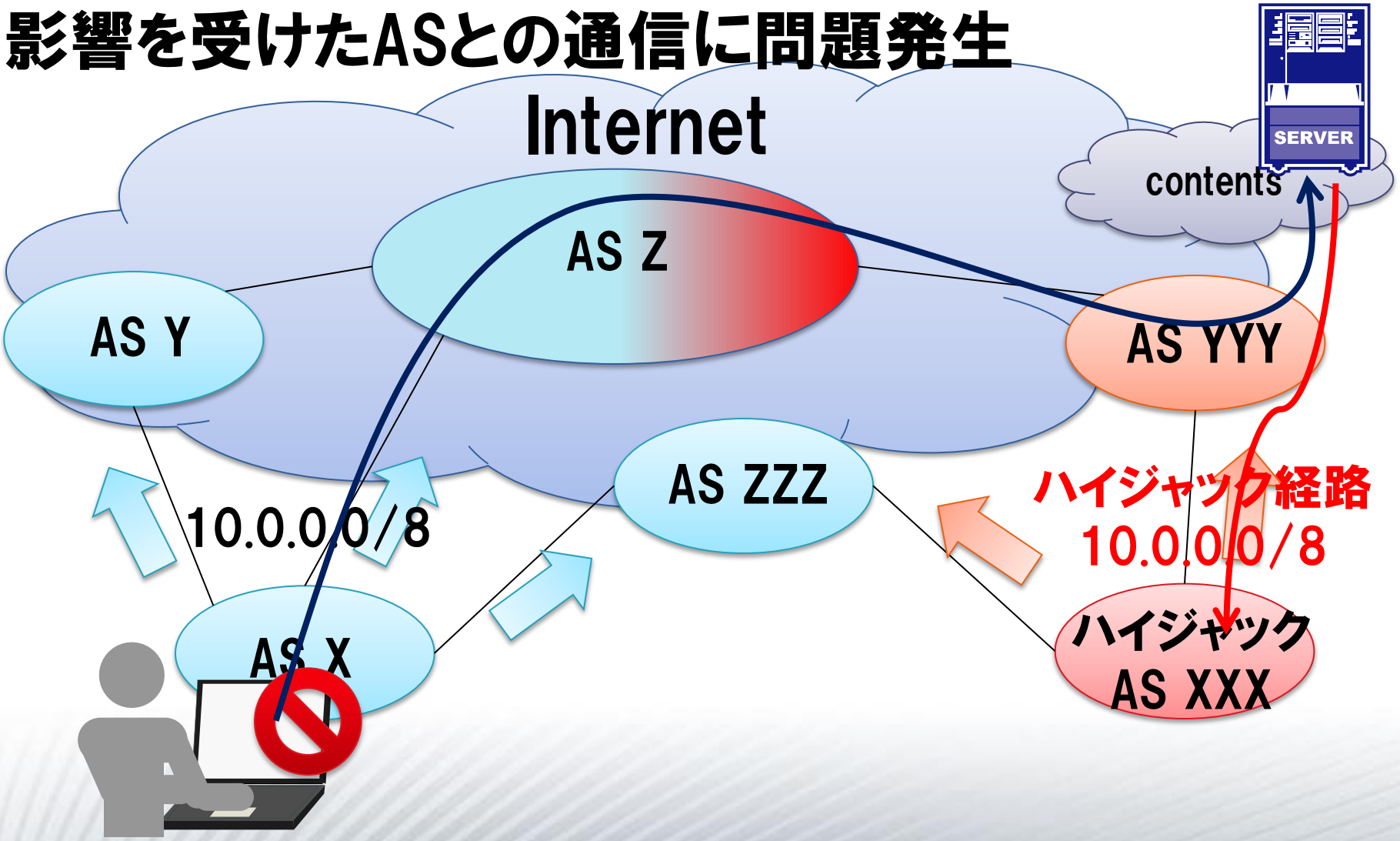
ハイジャックの影響を受けていないASとの通信は問題なし



経路ハイジャック

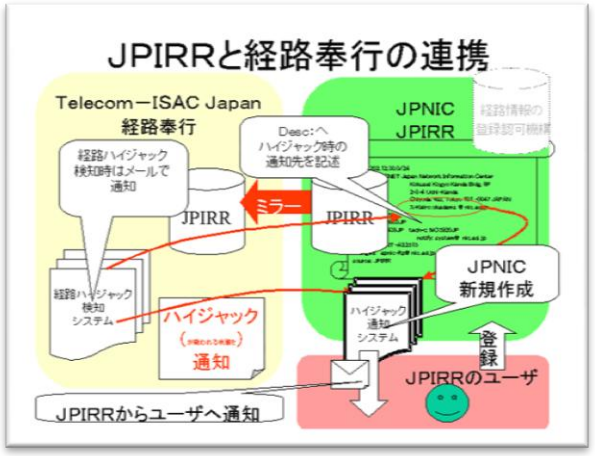
SoftBank

ハイジャックされた経路配下のユーザと、影響を受けたASとの通信に問題発生



経路ハイジャック検知について

SoftBank



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

Telecom－ISAC Japan 経路奉行

↓

JPIRR 通知システム

アラートメール →

NOCなど

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　6 Mar 2013 18:05:10 +0900 (JST)
Routeオブジェクト　　：　aaa.bbb.ccc.ddd/XX
RouteオブジェクトのOrigin:　ASXXXXX
検知したPrefix　　：　aaa.bbb.ccc.ddd/YY

SoftBank

実際に起きた経路ハイジャック
1回目 2013年1月11日(金)

世界中で最大110ASが影響を受けました

1回目 2013年1月11日の動き

SoftBank

- 23:15:25 Hijack alert from JPIRR

- 00:10:00ころには沈静化

1回目 2013年1月11日の動き

SoftBank

- 23:15:25 Hijack alert from JPIRR

経路ハイジャックに対する
対抗措置とらず終了。
しかし、、、
確認することは多かった。

- 00:10:00ころには沈静化

1回目 2013年1月11日の動き

SoftBank

- 23:15:25 Hijack alert from JPIRR
  - 3 Prefix ハイジャックされた模様
  - （AS26347 Dreamhostさんが被疑者）
- まず、ハイジャックされたPrefixの確認
  - サービスの確認
    法人なのか個人なのか、はたまた。。。
  - どの地域・県に割り当てられているか
- 世界中のLooking Glassでの確認
  - 国内のほとんどのLGではHJされてないように見える
  - 海外でも一部のLGではHJされているが、
    HJされていないようにも見える
- 00:10:00ころには沈静化

検知

確認

経路ハイジャック後

SoftBank

■改めて、ハイジャック発生時のフロー確認

- 検知後のエスカレーションフロー
- 影響確認の方法
- 経路ハイジャックへの対抗措置手順

経路ハイジャック後

SoftBank

■改めて、ハイジャック発生時のフロー確認

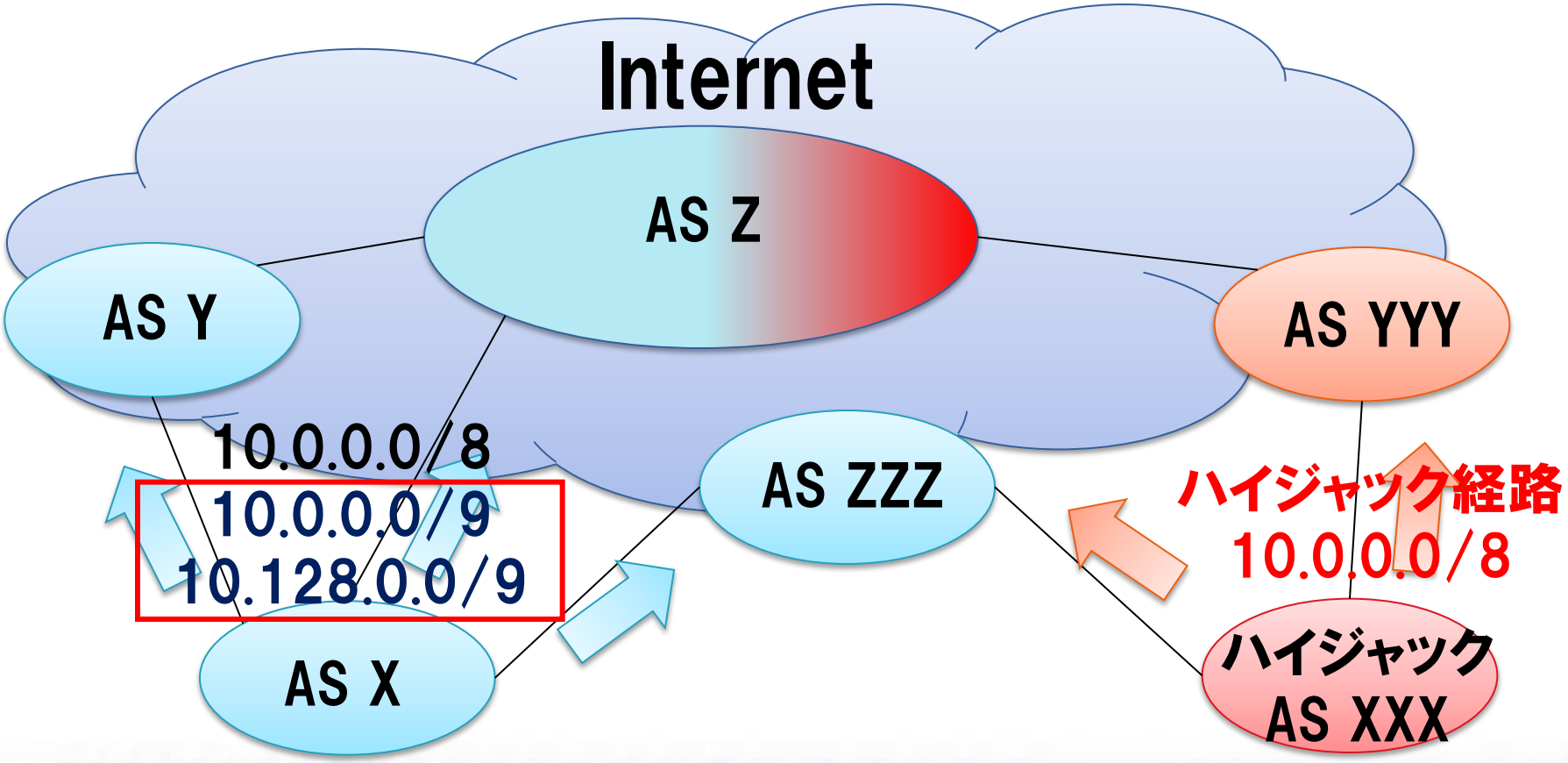
- 検知後のエスカレーションフロー
- 影響確認の方法
- 経路ハイジャックへの対抗措置手順

後から振り返ると、
このときの確認が非常に重要でした。

経路ハイジャックへの対抗措置

SoftBank

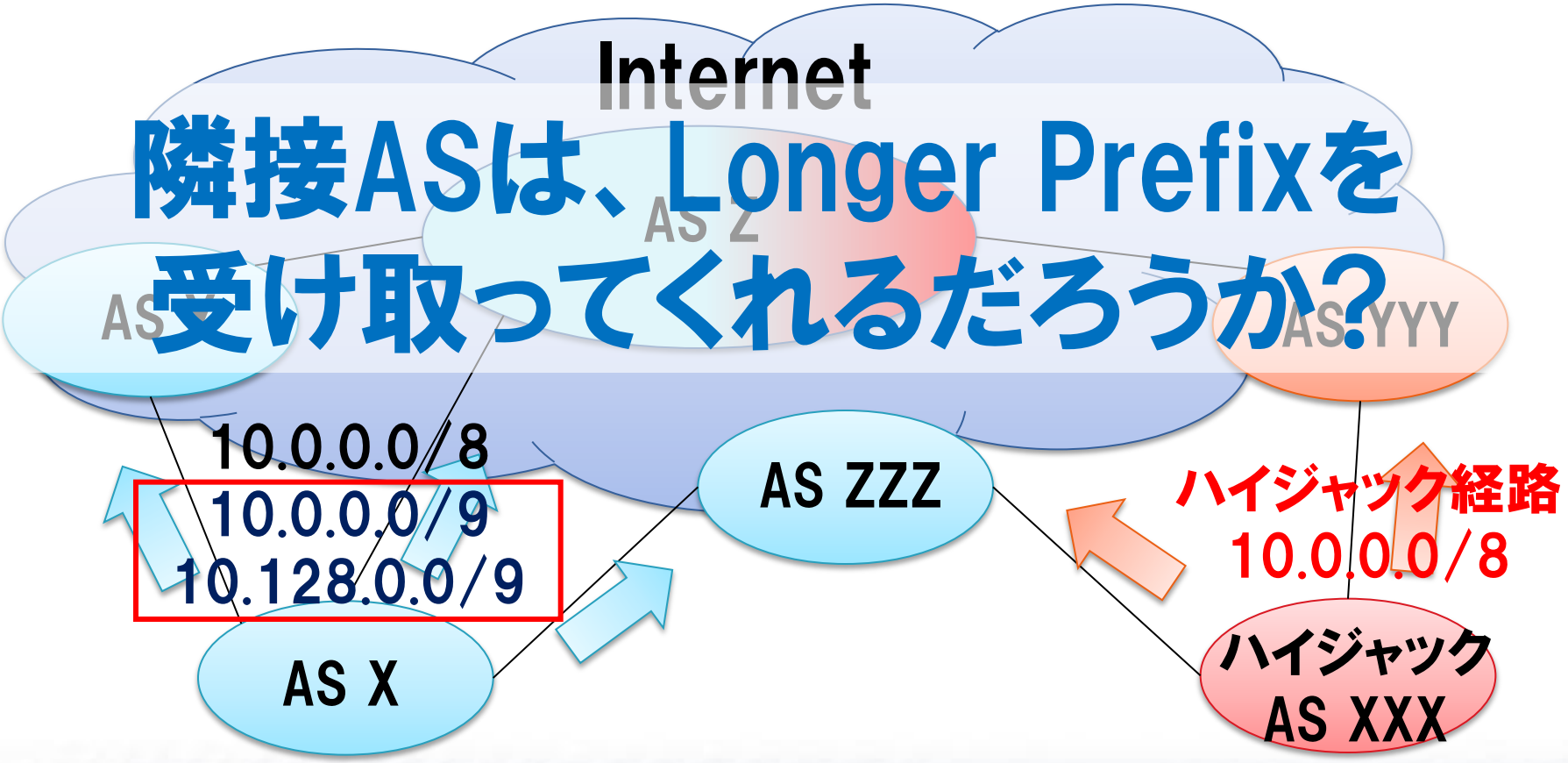
ハイジャック経路よりLonger Prefixを広報



経路ハイジャックへの対抗措置

SoftBank

ハイジャック経路よりLonger Prefixを広報



経路ハイジャック後

SoftBank

■改めて、ハイジャック発生時のフロー確認

- 検知後のエスカレーションフロー
- 影響確認の方法
- 経路ハイジャックへの対抗措置手順
  - ✓ 隣接ASがLonger Prefix受け取ってくれるか？

後から振り返ると、
このときの確認が非常に重要でした。

SoftBank

実際に起きた経路ハイジャック
2回目 2013年3月6日（水）

世界中で**約200経路**が影響を受けました

2回目 2013年3月6日の動き

SoftBank

- 16:59:18 Hijack alert from JPIRR
  - 1 Prefix Hijackされた模様
  - AS26347 Dreamhostさんが今回も被疑者
- 即、取り返し準備
  - Longer Prefixを広報する準備
- 18:31:50 Longer Prefix広報で取り返した！

RISで確認される情報

SoftBank

Routing Information Service (RIS)　http://www.ripe.net/ris/

Update entries (92)

- 17676 origin AS : 6 event(s)
  - Announcement of prefix 126.162.144.0/21 : Seen between 2013-03-06 09:31:50 UTC and 2013-03-06 09:32:39 UTC , through 1 of AS17676 neighbours.
  - Announcement of prefix 126.162.152.0/21 : Seen between 2013-03-06 09:31:50 UTC and 2013-03-06 09:32:39 UTC , through 1 of AS17676 neighbours.
  - Withdrawal of prefix 126.162.144.0/21 : Seen between 2013-03-06 09:31:58 UTC and 2013-03-06 09:32:39 UTC
  - Withdrawal of prefix 126.162.152.0/21 : Seen between 2013-03-06 09:31:58 UTC and 2013-03-06 09:32:39 UTC
  - Announcement of prefix 126.0.0.0/8 : Seen between 2013-03-06 09:50:22 UTC and 2013-03-06 09:50:22 UTC , through 1 of AS17676 neighbours.
  - Announcement of prefix 126.162.0.0/16 : Seen between 2013-03-06 09:50:22 UTC and 2013-03-06 09:50:22 UTC , through 1 of AS17676 neighbours.
- 26347 origin AS : 13 event(s)
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 07:59:07 UTC and 2013-03-06 07:59:07 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:00:39 UTC and 2013-03-06 08:01:04 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:05:43 UTC and 2013-03-06 08:05:43 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:07:13 UTC and 2013-03-06 08:07:37 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:11:43 UTC and 2013-03-06 08:11:43 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:13:13 UTC and 2013-03-06 08:13:41 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:18:37 UTC and 2013-03-06 08:18:37 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:20:09 UTC and 2013-03-06 08:20:44 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:24:43 UTC and 2013-03-06 08:24:43 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:26:15 UTC and 2013-03-06 08:26:47 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:31:26 UTC and 2013-03-06 08:33:56 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:32:56 UTC and 2013-03-06 08:33:20 UTC
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 09:12:10 UTC and 2013-03-06 09:12:10 UTC

ハイジャック経路がAnnounceされたりWithdrawされたり不安定な状態

RISで確認される情報

SoftBank

Routing Information Service (RIS)　http://www.ripe.net/ris/

Update entries (92)

対抗措置実施！

- 17676 origin AS : 6 event(s)
  - Announcement of prefix 126.162.144.0/21 : Seen between 2013-03-06 09:31:50 UTC and 2013-03-06 09:32:39 UTC , through 1 of AS17676 neighbours.
  - Announcement of prefix 126.162.152.0/21 : Seen between 2013-03-06 09:31:50 UTC and 2013-03-06 09:32:39 UTC , through 1 of AS17676 neighbours.
  - Withdrawal of prefix 126.162.144.0/21 : Seen between 2013-03-06 09:31:58 UTC and 2013-03-06 09:32:39 UTC
  - Withdrawal of prefix 126.162.152.0/21 : Seen between 2013-03-06 09:31:58 UTC and 2013-03-06 09:32:39 UTC
  - Announcement of prefix 126.0.0.0/8 : Seen between 2013-03-06 09:50:22 UTC and 2013-03-06 09:50:22 UTC , through 1 of AS17676 neighbours.
  - Announcement of prefix 126.162.0.0/16 : Seen between 2013-03-06 09:50:22 UTC and 2013-03-06 09:50:22 UTC , through 1 of AS17676 neighbours.
- 26347 origin AS : 13 event(s)
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 07:59:07 UTC and 2013-03-06 07:59:07 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:00:39 UTC and 2013-03-06 08:01:04 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:05:43 UTC and 2013-03-06 08:05:43 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:07:13 UTC and 2013-03-06 08:07:37 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:11:43 UTC and 2013-03-06 08:11:43 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:13:13 UTC and 2013-03-06 08:13:41 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:18:37 UTC and 2013-03-06 08:18:37 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:20:09 UTC and 2013-03-06 08:20:44 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:24:43 UTC and 2013-03-06 08:24:43 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:26:15 UTC and 2013-03-06 08:26:47 UTC
  - Announcement of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:31:26 UTC and 2013-03-06 08:33:56 UTC , through 1 of AS26347 neighbours.
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 08:32:56 UTC and 2013-03-06 08:33:20 UTC
  - Withdrawal of prefix 126.162.144.0/20 : Seen between 2013-03-06 09:12:10 UTC and 2013-03-06 09:12:10 UTC

経路ハイジャックの原因

SoftBank

NANOGの投稿を見ると。。。

ASxxに経路ハイジャックに
遭ったんだけど。。。

おたくとはPeerしてないし、広報してないよ。

あれ？Route Serverから
受け取ってるよ。ASxx originで。

え！？マジで？
広報してないよ。頼む信じてくれ。

経路ハイジャックの原因

SoftBank

NANOGの投稿を見ると。。。

その後、第3者がコンフィグ
確認し、問題なさそうと証言あり。
（本当に問題なかったかは不明）
Route Server側の情報はなし。
真相は藪の中。。。

まとめ

SoftBank

- 経路ハイジャックに対する準備はとても大事
  - ハイジャック発生時のフローを決めておく
- 対抗措置(Longer Prefix広報)は隣接ASが受け取ってくれないと機能しない
  - Peer先や上流Transitに相談しましょう

まとめ　cont.

SoftBank

- Route Server
  - 不特定多数のASの経路を受けます
- Hijack alertは心臓に悪い
  - 4半期に1回くらいReminderやった方がいい
    - ✓ちゃんと機能してるって分かる
    - ✓監視メンバーでアラートメール見たことない人多かった
  - そのときにハイジャック時の対応を確認するといいかも

ディスカッション

SoftBank

- 経路ハイジャックの経験談
- CGNとか増えたし、影響が以前より大きくなってるけれど、今までの対応で大丈夫？
- Route ServerとPeerするときに気をつけること、実際気をつけてることは？
- 影響ってどう報告します？
- Looking Glass重いよね

SoftBank

ご清聴ありがとうございました。

参考資料

SoftBank

- Hijack event 2013-01-11 by AS26347
  http://portal.bgpmon.net/data/hijack20130111.txt