

ルーティングセキュリティ インシデント事例の紹介

2013/11/26

KDDI株式会社 中野 達也

もくじ

1. ルーティングセキュリティ インシデントの紹介
2. なぜこういったインシデントが起きるのか
3. 早期解決のために
4. まとめ

ルーティングセキュリティ インシデントの紹介

ルーティングにまつわるインシデント

1. ソフトウェアバグ等によるもの
2. 人為的な問題(主にミス)によるもの

ルーティングにまつわるインシデント

1. ソフトウェアバグ等によるもの

2. 人為的な問題(主にミス)によるもの

過去の事例(1)

- 2009年 大量のAS-PATH prependによるセッション断

<http://www.gossamer-threads.com/lists/cisco/nsp/103838>

<http://www.geekpage.jp/blog/?id=2009/2/20/2>

– AS-PATH長が異常に長い経路情報が広告される

- 一部ルータが異常としてセッションを切断
- 再接続されるも、同じ経路を受け再切断
- 切断と接続の繰り返し。。。

– 対策として

- (短期的対応) 長すぎるAS-PATHをフィルタ
- (長期的対応) ソフトウェアVersion up

過去の事例(2)

- 2009年 4bytesAS関連の不具合

<http://venus.gr.jp/opf-jp/events/showcase3/showcase3-4byte-tech.pdf>

- 4bytesASを含むPATHを持った経路が Confederation ASを通過する際 AS-PATHにPrivateASNが紛れ込んでしまう不具合

→不正なアトリビュートを含むupdateとしてセッション断するルータが発生(実は正しい動作)

- そもそもPrivateASNを出してしまうのが悪い
→ VersionUPで対応

ルーティングにまつわるインシデント

1. ソフトウェアバグ等によるもの

2. 人為的な問題(主にミス)によるもの

人為的ミスの内訳

- 他ASのPrefixを誤って広告してしまい、一時的にPrefixを奪い取ってしまう
→ Mis-Origination
- 上位ISP(Transit)から受信した経路を誤って別の上位ISPやPeerに広告してしまう
→ 誤トランジット

Mis-Originationについて

経路ハイジャック / IP Hijacking / Prefix Hijack



実態としてはハイジャックは少ないのでは？

権威のない経路広告



ちょっと言いにくいよね。。。

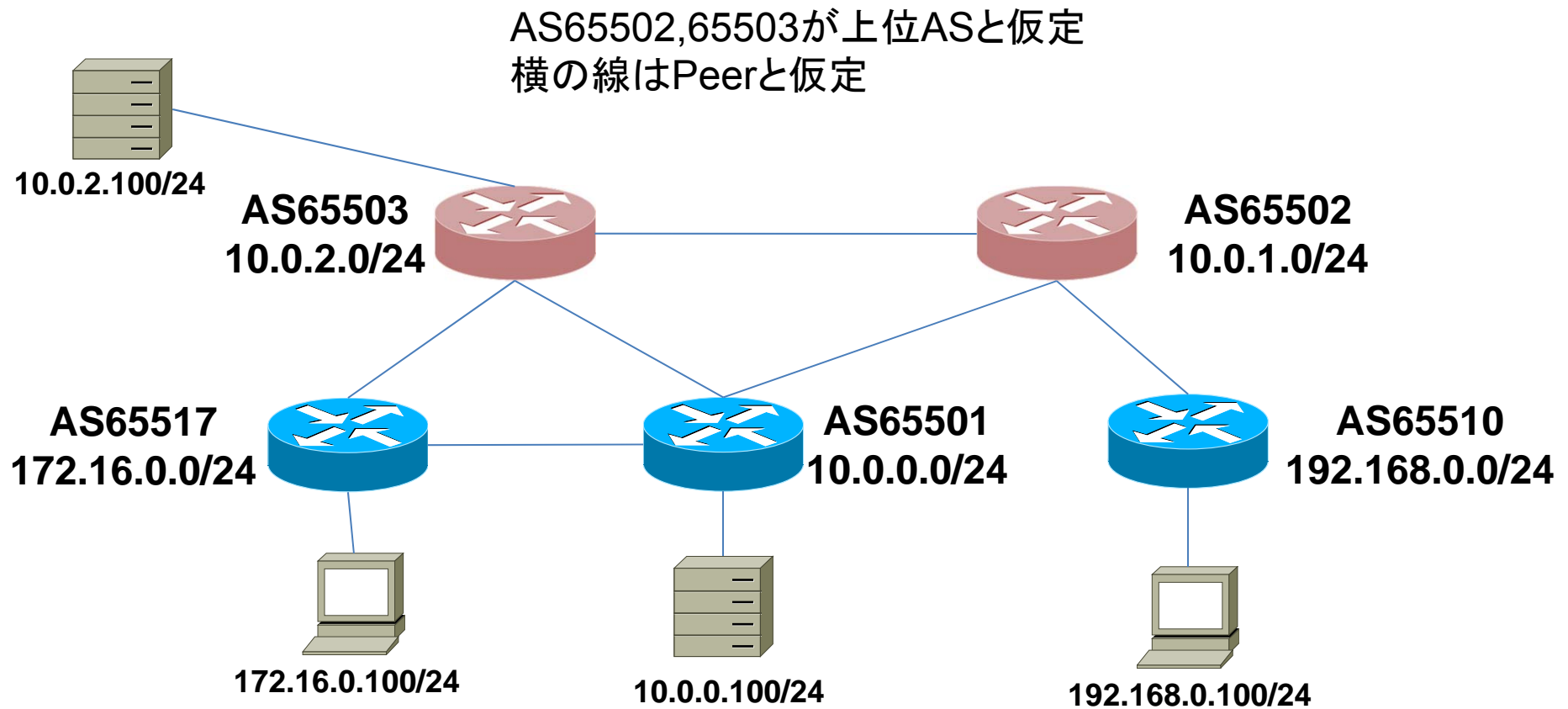
Mis-Origination (By Randy Bush)

Mis-Originationで何が起きるのか？

- トラフィックの急変、品質劣化
- (影響範囲が各種サーバの場合)
名前解決、コンテンツ提供、メール送受信NG
- (影響範囲がお客様割り当て空間の場合)
お客様からの不通問い合わせ

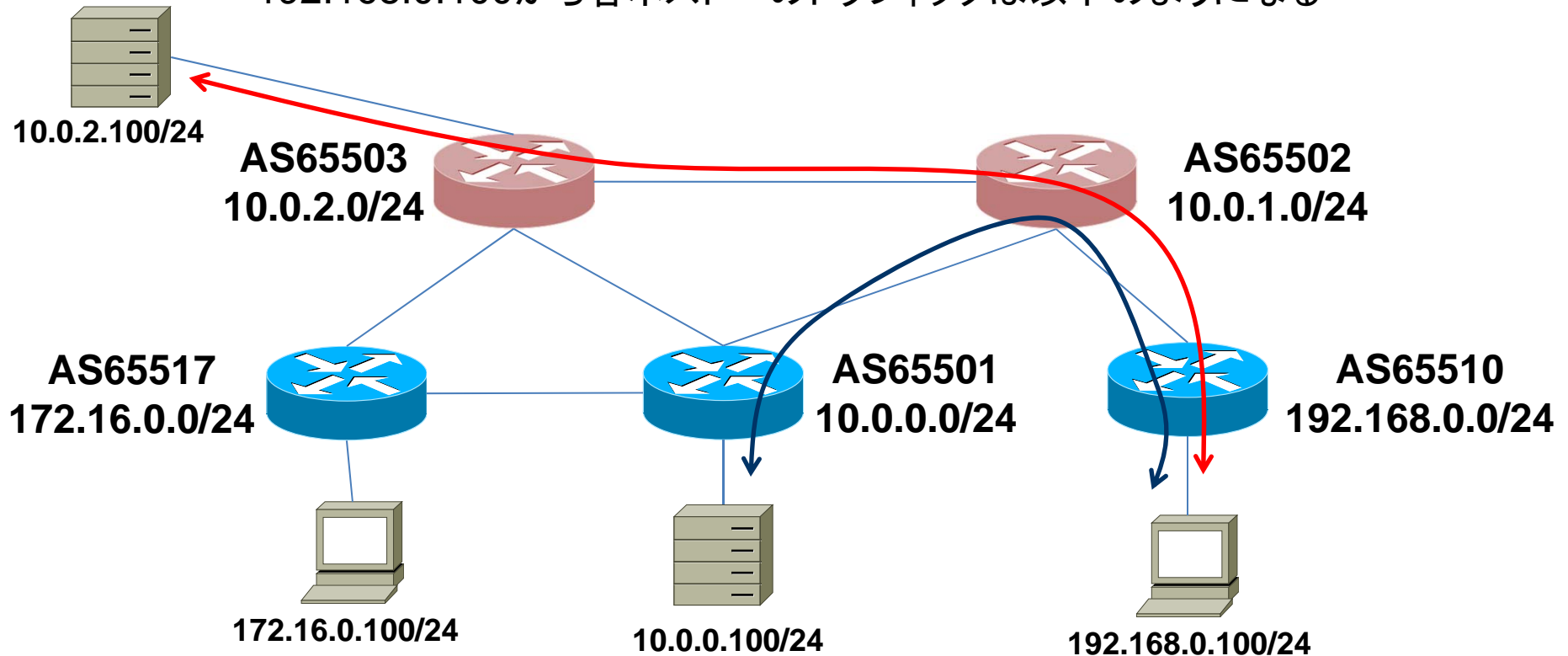


Mis-Originationと誤トランジットの例



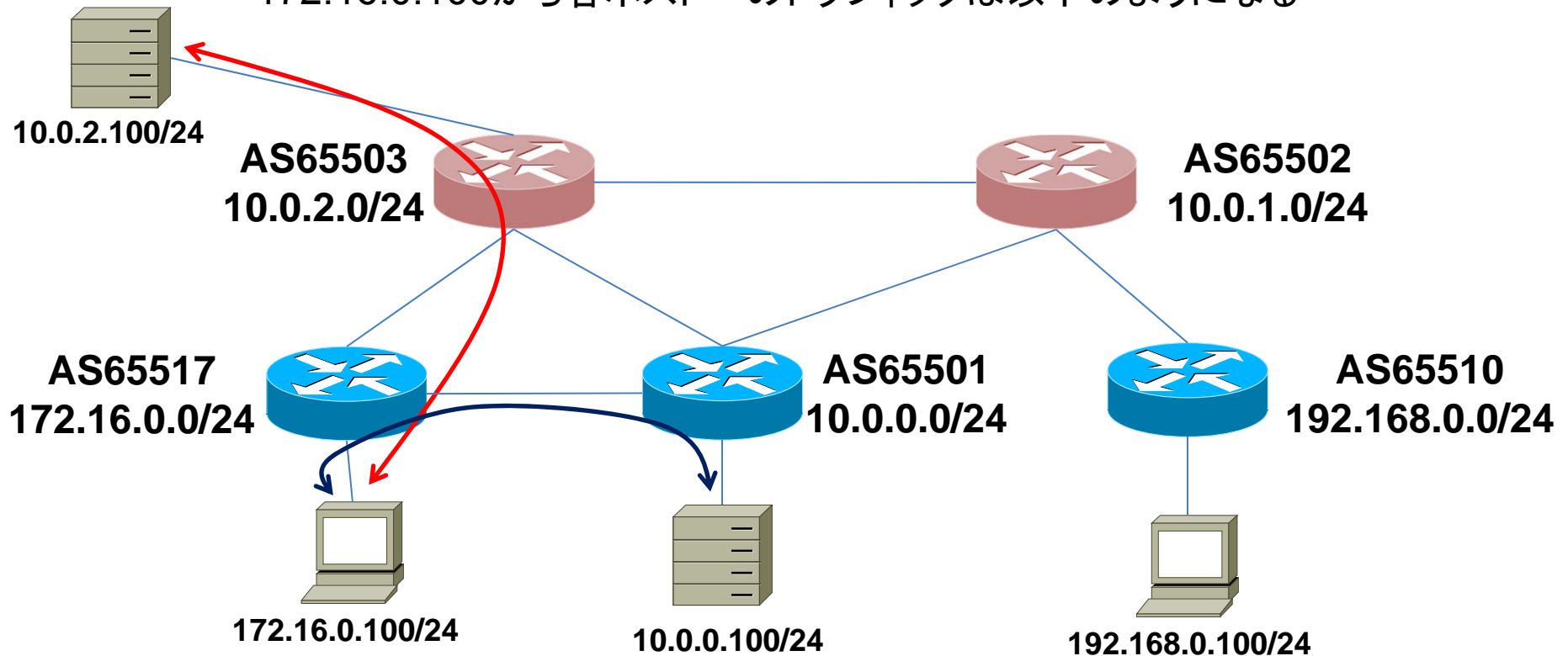
Mis-Originationの例 通常時のトラフィック

192.168.0.100から各ホストへのトラフィックは以下ようになる



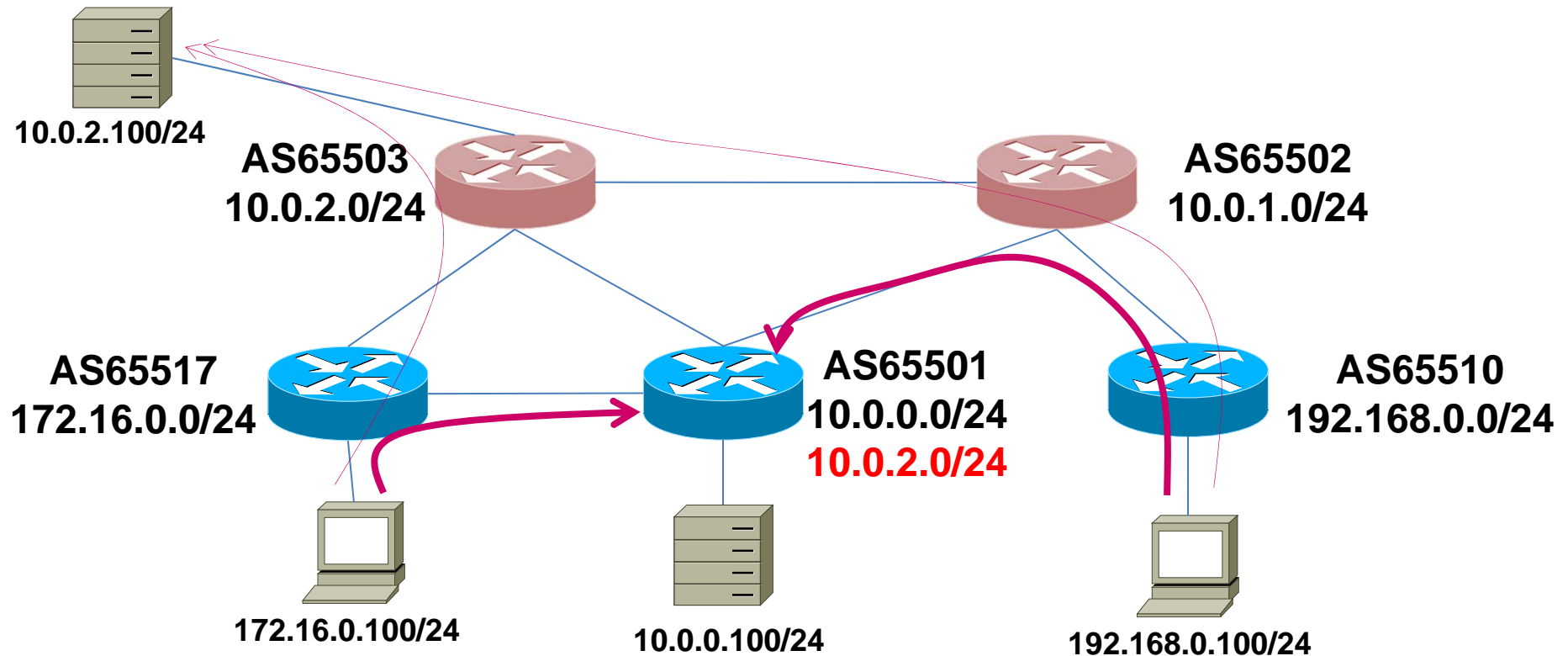
Mis-Originationの例 通常時のトラフィック

172.16.0.100から各ホストへのトラフィックは以下ようになる



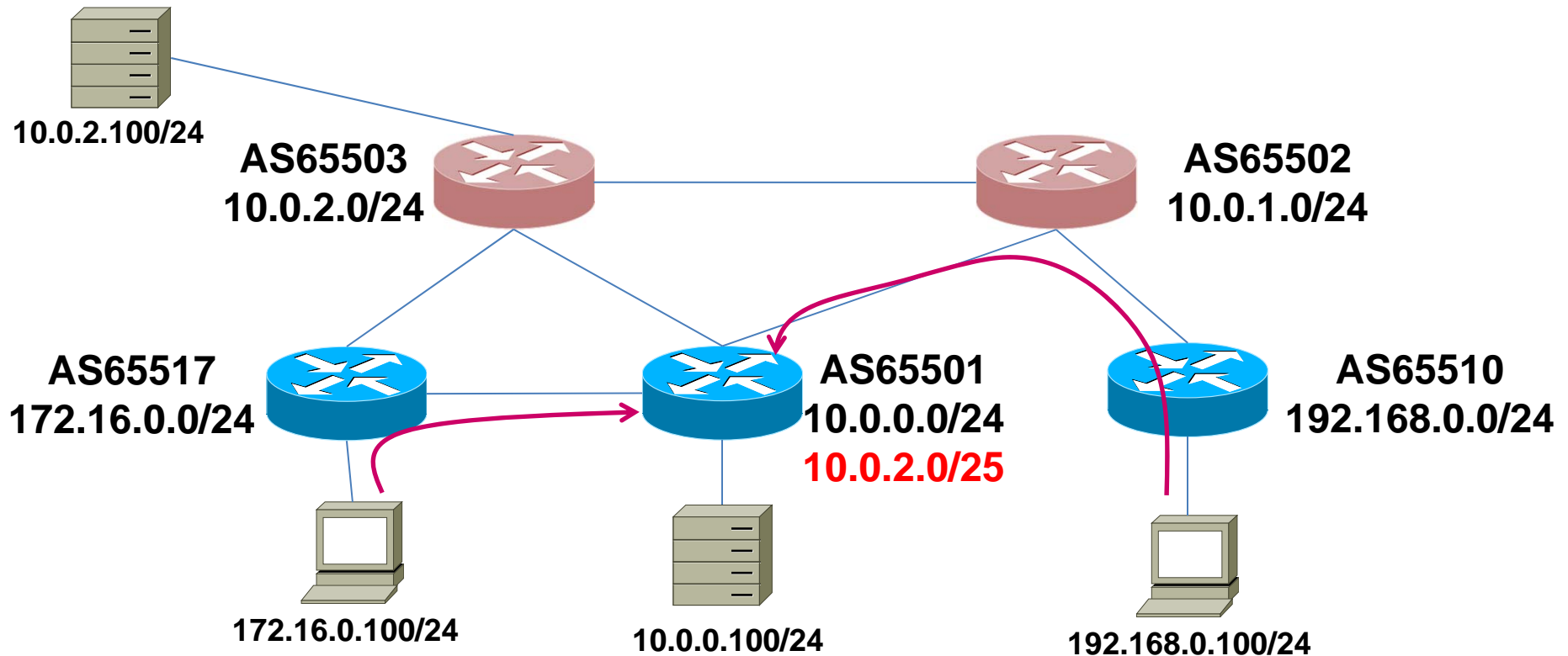
Mis-Originationの例(1)

AS65501が10.0.2.0/24をMis-Originationした場合
各ASのポリシーによっては10.0.2.100へのトラフィックに影響が出る

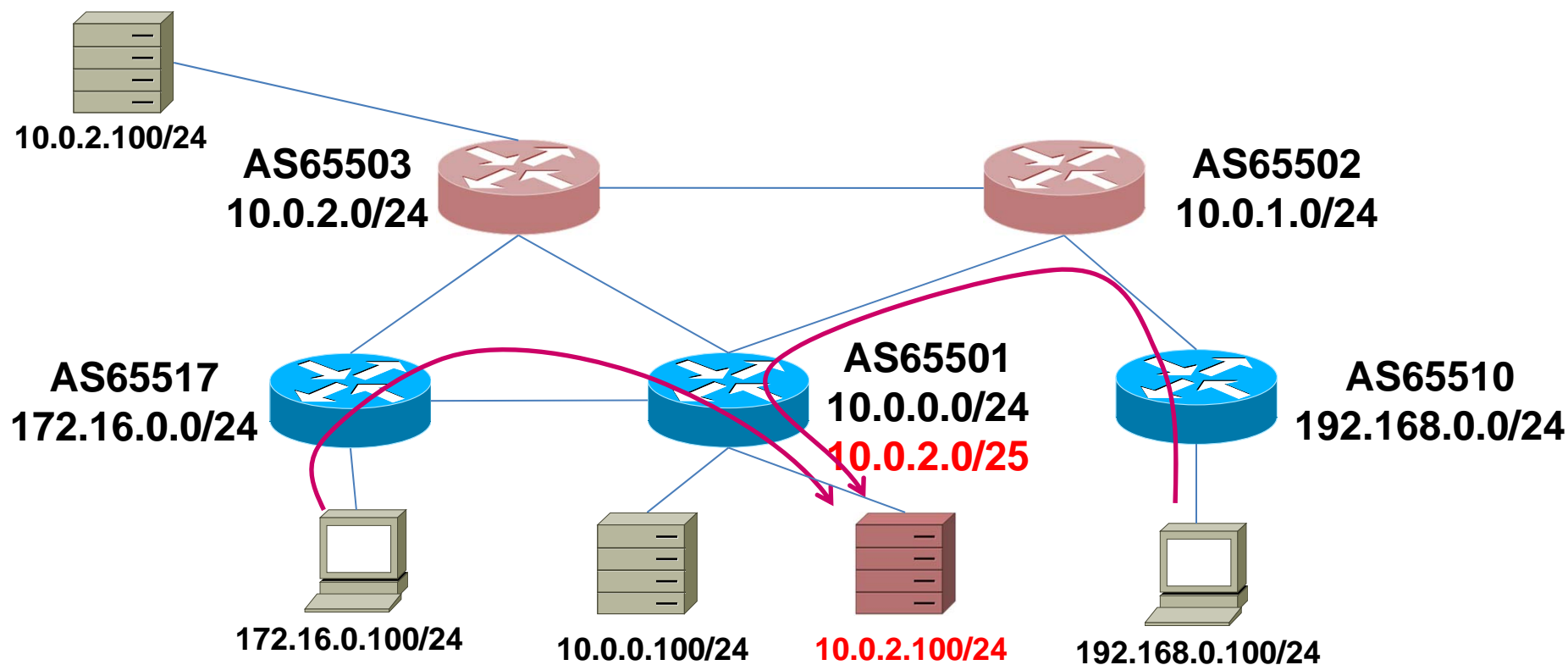


Mis-Originationの例(2)

AS65501が10.0.2.0/25をMis-Originationした場合
10.0.2.100へのトラフィックはAS65501に吸い込まれる

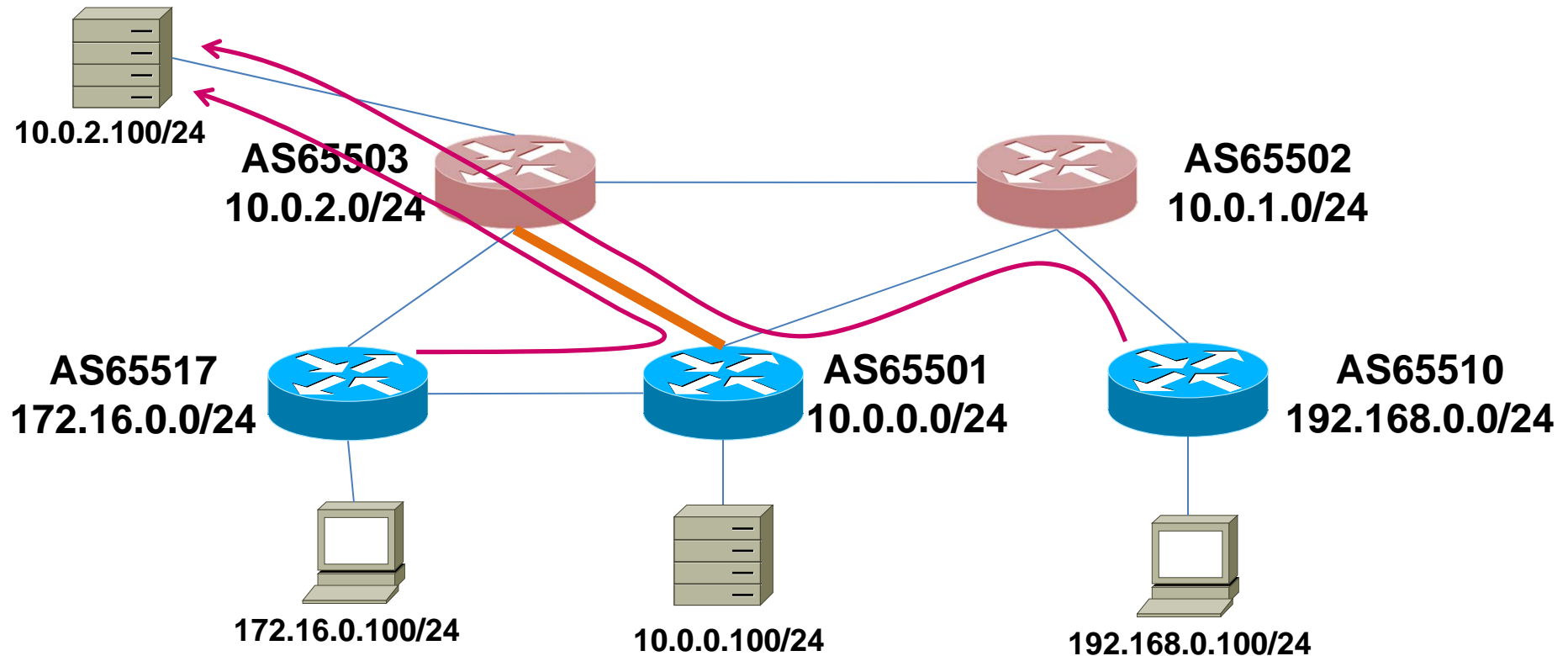


こんなことも。。。



誤トランジットの例

- AS65501がAS65503からの経路を誤って隣接ASに広告してしまった場合
- 多くのトラフィックがAS65501経由になる可能性
- AS65503～AS65501間のトラフィックが増え、帯域が圧迫される可能性



こんなことって
本当にあるの？

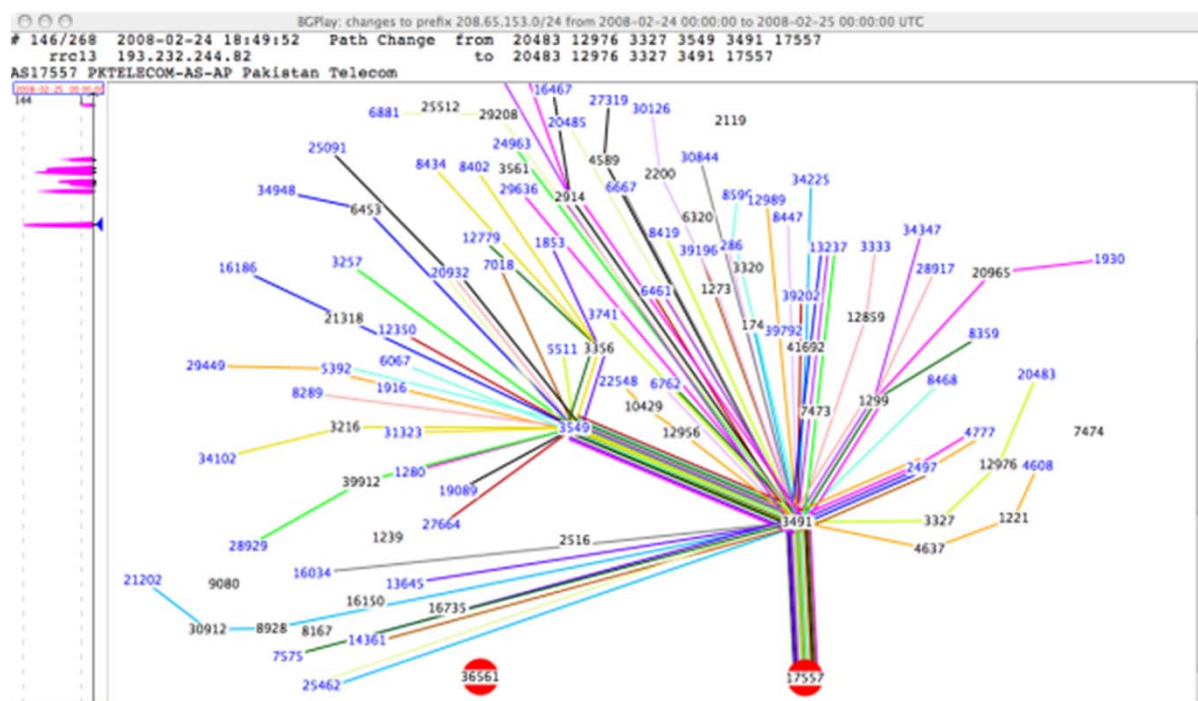
実際にありました

Mis-Originationの事例

- 2008年 パキスタンテレコムによる
YouTube PrefixのMis-Origination

<http://www.renesitys.com/blog/2008/02/pakistan-hijacks-youtube-1.shtml>

<http://itpro.nikkeibp.co.jp/article/COLUMN/20090225/325481/>



<http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>

誤トランジットの事例

- 2004年トルコのISPが(当時の)FullRouteを誤って広告した
http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml
<http://www.renesys.com/wp-content/uploads/2013/05/renesys-nanog34.pdf>
- 2010年 米国のISPが上位ISPから受信した経路を他の上位ISPに広告した
<http://mailman.nanog.org/pipermail/nanog/2010-February/018523.html>
- 2012年 AU地域で誤トランジットが発生し複数のISPが孤立
<http://labs.apnic.net/blabs/?p=139>

インターネットへの接続性が誤トランジットを行ったISP経由となり、品質劣化が発生した

他にもいくつか

その他 過去の事例(1)

- 2009年 AS-PATHを捻じ曲げて遠回りをさせた例がBlackhatで公開された
- 2011年 一部のISPがFacebookに到達する際、中国・韓国を経由するという事例がBGPMONで紹介された

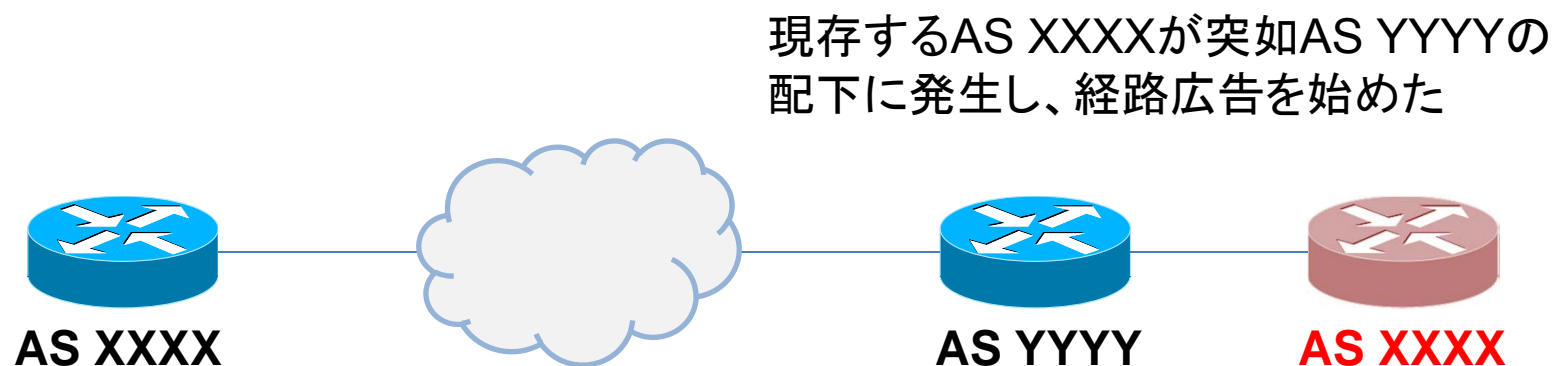
情報の不正取得
(MITM: 中間者攻撃)が
懸念される



<http://www.renesys.com/wp-content/uploads/2013/05/blackhat-09.pdf>

その他 過去の事例(2)

- 2013年 AS番号ごと詐称された事例
 - JANOG MLに相談がPOSTされた
 - BGPのPeerは双方の設定があってできる事なので、こういう事象は想定されていなかった。。。



インシデント事例のまとめ

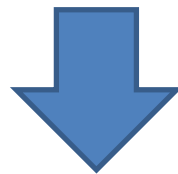
世の中いろんなことがあります

思ってもみなかったものが原因で
問題が起こりえます

なぜこういった インシデントが起きるのか

なぜ起きるのか

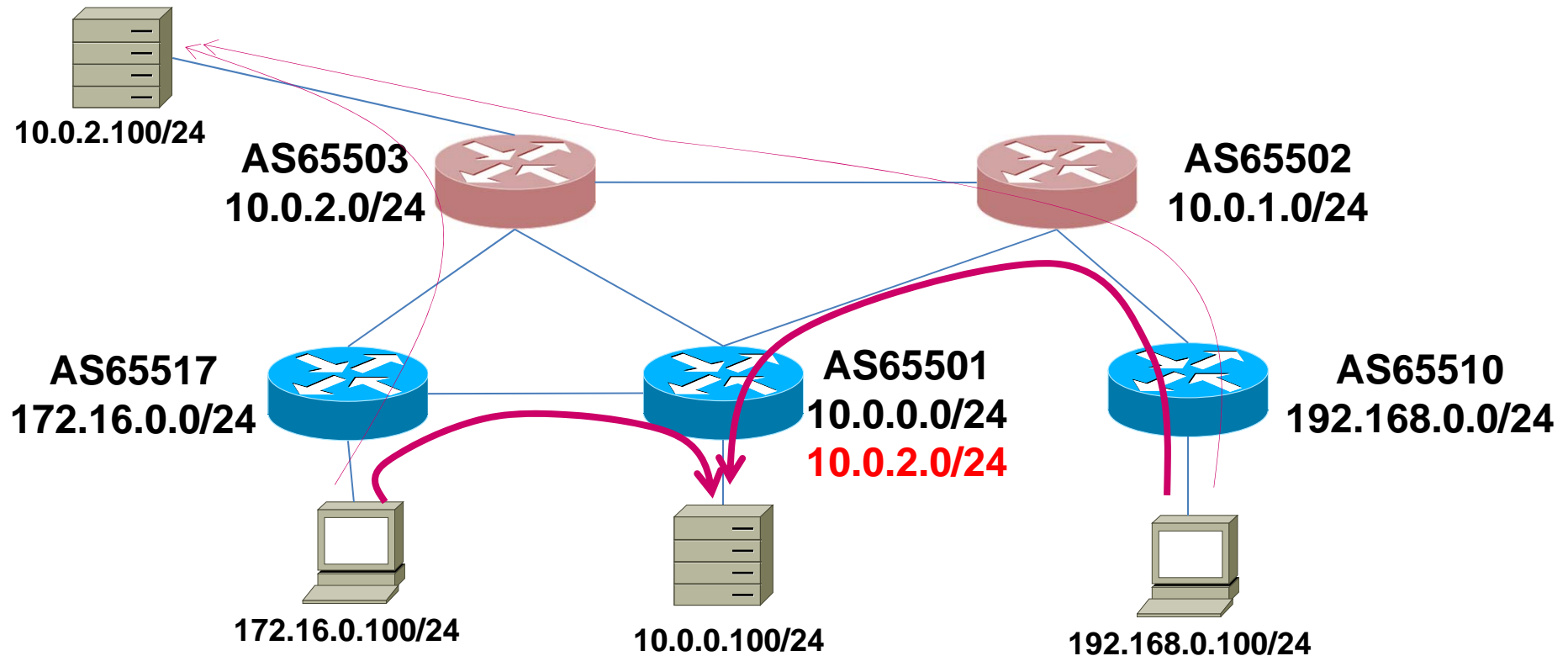
- 設定ミスっぽい経路広告がたまにある
- 検証や研修のために生成した経路を誤広告?
- 誤トランジットは設定ミスと断言できそう



大半は故意ではなく過失と思われる
なので「経路ハイジャック」という言い方はやめよう

問題発生時 (再掲)

AS65501が10.0.2.0/24をMis-Originationした場合
各ASのポリシーによっては10.0.2.100へのトラフィックに影響が出る



誤ったconfig例

現状のconfig

```
router bgp 65501
neighbor 10.0.1.X remote-as 65502
neighbor 10.0.1.X route-map myASout out
...
network 10.0.0.0 mask 255.255.255.0
...
route-map myASout
match ip address prefix-list myPrefix
...
ip prefix-list myPrefix seq 10 10.0.0.0/24 le 32
...
ip route 10.0.0.0 255.255.255.0 null0
```


自ASのPrefixに10.2.0.0/24を
追加しようとして
(手順書の記載ミス等の理由で)
間違えてしまうことも考えられる

誤って追加したconfig

```
conf t
ip route 10.0.2.0 255.255.255.0 null0

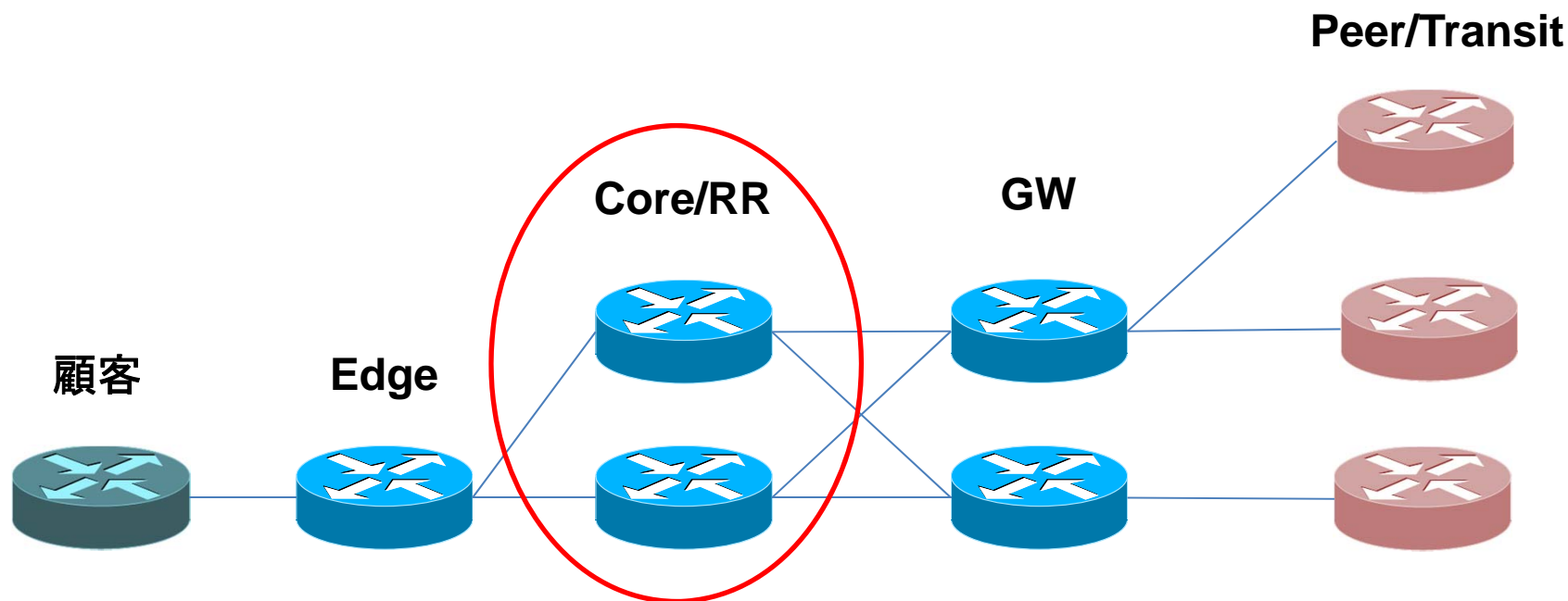
no ip prefix-list myPrefix
ip prefix-list myPrefix seq 10 10.0.0.0/24 le 32
ip prefix-list myPrefix seq 20 10.0.2.0/24 le 32

router bgp 65501
network 10.0.2.0 mask 255.255.255.0
end
```



AS65501
10.0.0.0/24
10.0.2.0/24

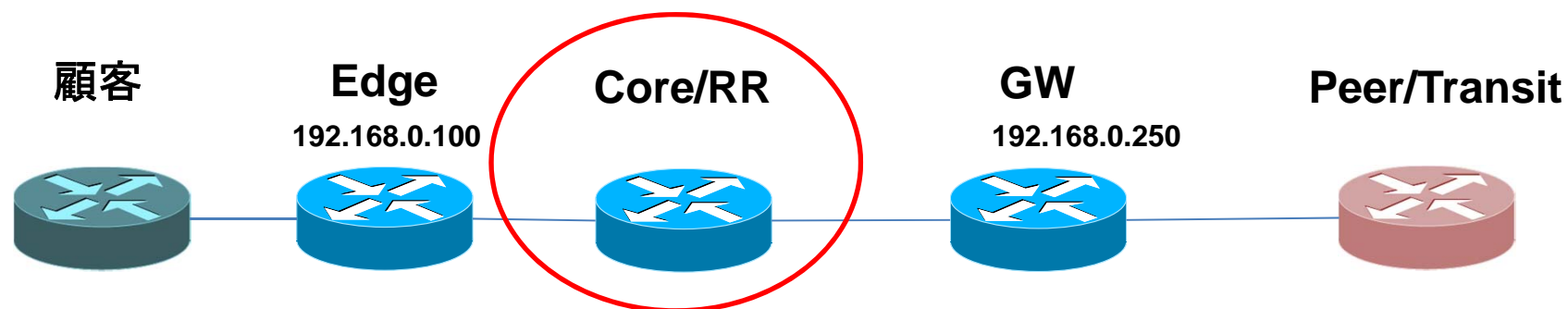
中規模以上の網だと



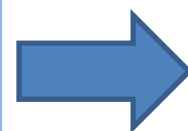
Core/RRで経路生成してる人が多いと思われる
そこで設定ミス
→ GWからPeer/Transitへ
→ Edgeから顧客へ
誤った経路を広告してしまう

Youtube Mis-Origination (2008年)の推測

- 内部でブラックホールするつもりが誤って広告してしまった?



```
router bgp 17557
redistribute static
neighbor 192.168.0.250 remote-as 17557
neighbor 192.168.0.250 description GW
neighbor 192.168.0.250 soft-reconfiguration inbound
neighbor 192.168.0.100 remote-as 17557
neighbor 192.168.0.100 description Edge
...以下略
```



```
conf t
ip route <YouTubeのPrefix> null0
```


インシデント発生についてのまとめ

誰かのちょっとしたミスで
被害者になってしまいます

自分のちょっとしたミスで
加害者になってしまいます

何ができるか、どうするか

早期解決のために

どうすればよいか

- 検知システムの活用
- Mis-Originationを止めてもらう
- (一時的な手段として)取り返す
- (自ASが) Mis-Originationした際に
教えてもらえるようにする
- 復旧を待つ

どうすればよいか

- 検知システムの活用
- Mis-Originationを止めてもらう
- (一時的な手段として)取り返す
- (自ASが) Mis-Originationした際に教えてもらえるようにする
- ~~復旧を待つ~~

検知システムの活用



経路奉行

http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html

BGP MON

<http://bgpmon.net/>

Cyclops

<http://cyclops.cs.ucla.edu/>

Renesys

<http://www.renesys.com/products/routing-alarms/>

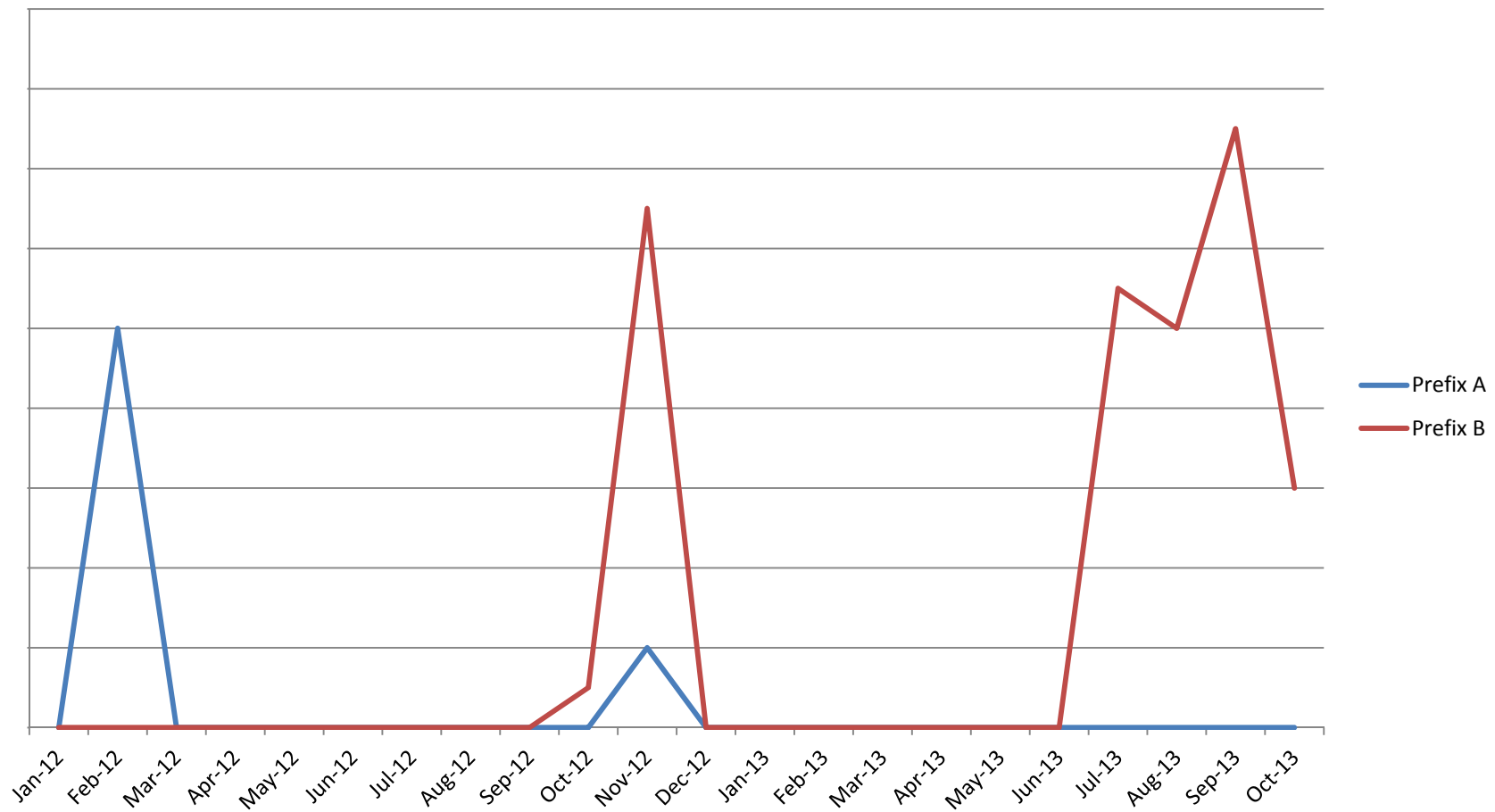
ISAlarm(RIPE)

<https://www.ripe.net/is/alarms/>

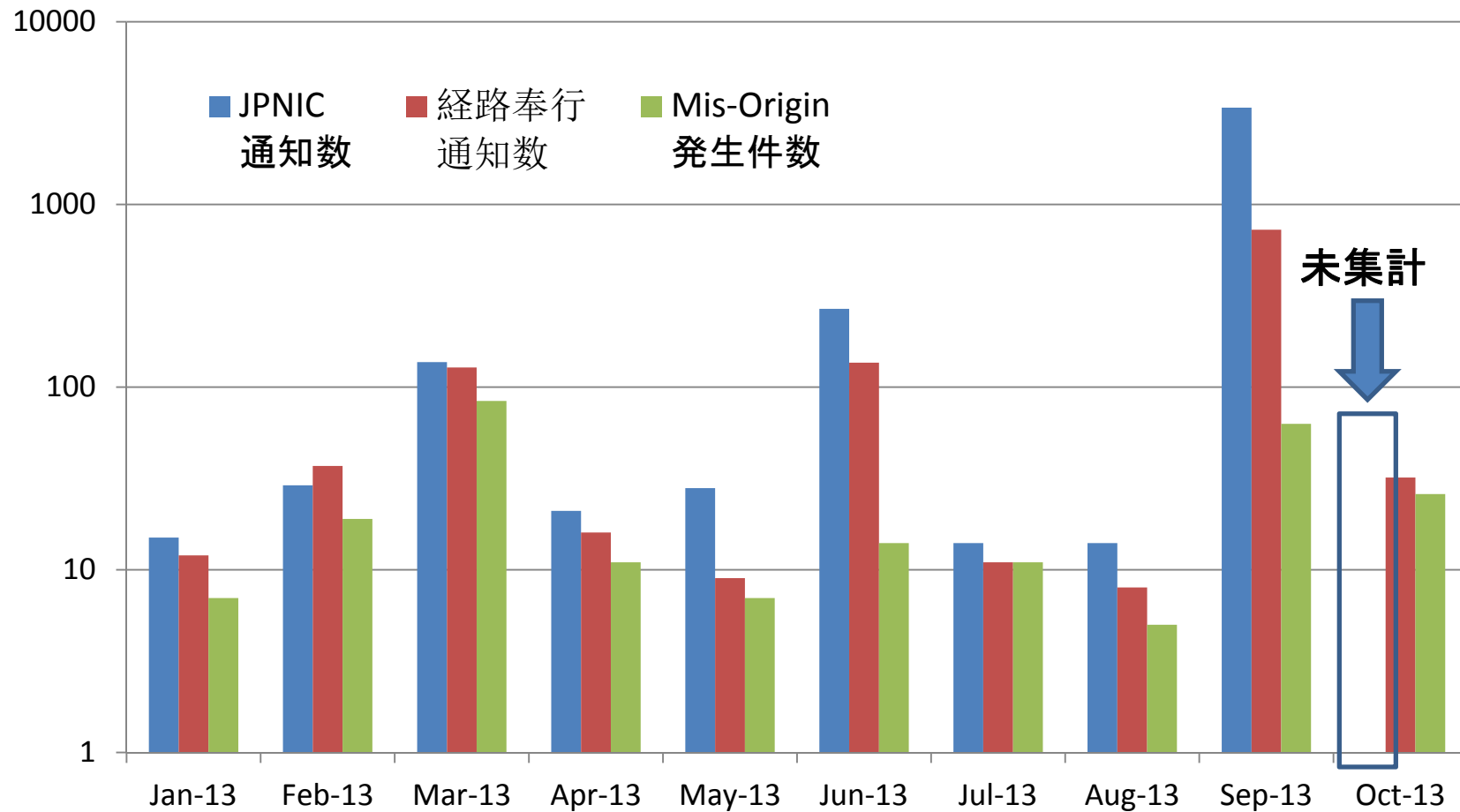
検知システム比較

	経路奉行	BGPmon	Cyclops	IS Alarms	Renesisys
経路の情報源	国内ISPの経路情報	RIPE-RIS / Route views		RIPE-RIS	More than 360 sites
情報源との比較方法	JPIRR	ユーザ入力情報			
通知、確認方法	メール	Web/メール SMS	Web メール RSS	Web メール Syslog	Web
備考	JPIRRにObject登録で監視対象 X-keiro登録で通知対象	有料 (5prefixまでは無料) ROA対応らしい	事前登録要 ASNでPrefixも登録可 MITM検知	事前登録要 Prefix手入力 MITM検知	有料
その他	国内最強	遠回りする事例 (MITMの可能性)や AS詐称も検知できた	動いてないかも	現在停止中	MITM検知できるとある

(参考)とあるASにおける BGPMONからのMis-Origination 通知状況



経路奉行での検知・通知状況(2013年)



どうすればよいか

- 検知システムの活用
- Mis-Originationを止めてもらう
- (一時的な手段として)取り返す
- (自ASが)Mis-Originationした際に教えてもらえるようにする
- ~~• 復旧を待つ~~

どうやって対応するか

広告元を突き止め、止めてもらう

- `show ip bgp <prefix>` 広報元の確認
- `traceroute` 結果の確認
 - 自ASルータで
 - Looking Glass で
- RouteViewsのmrtdump archiveを参照

どうやって対応するか

広告元の連絡先を調べて、連絡を試みる

- Whoisで調べてみる
 - JPNIC Whois ,RADB ...etc
 - mnt-byやグループハンドル等も参照する
- PeeringDBを参照する
 - <https://www.peeringdb.com/>
- HurricaneElectricのBGP Toolkitを参照する
 - <http://bgp.he.net/>

どんな問い合わせをするか

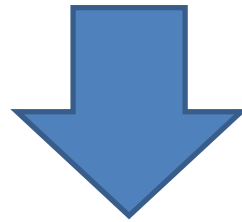
- 担当者以外にもCCする
 - noc@ / peering@ / admin@等をCCに
- 事実を淡々と書く
 - テンプレートを作っておくとなおよい
 - Looking Glass / whoisの結果を張り付け
 - 客観的な事実を突きつける
- 返事がなければ先方の上位ASにも相談
- 最終手段はnanogやjanogにPOSTしてみる

取り返すという手段

- 広告元よりもさらに細かい経路を広告する
→ 広告するPrefixを間違えないよう注意
- 細かいPrefixが広告できるか、自ASの上位ISP
にあらかじめ確認したほうがよい

やってしまった時のために

自身のwhois/IRR情報は最新の状態を保つ
peeringDB等もやっておくとさらによい



なぜ？

- やってしまった側が気づくのは難しい
- 被害者側はwhois/IRR/peeringDB等の情報を頼りにすることがあるから

まとめ

全体のまとめ

- Mis-Originationで何が起こるかを理解する
 - 起こさないための方法も考えましょう
- 今からできることをやっておく
 - 発生時の対応手順確立
 - 各種DBの更新

経路奉行/ BGPMON / Cyclopsについて

APPENDIX

経路奉行ってどんなもの？

- 経路情報(BGP Fullroute)を蓄積
- 経路情報をJPIRRの登録情報(origin AS)と比較
- originとIRRの情報に差分が発生した場合、IRRの登録元に通知

経路奉行について

- 経路ハイジャック通知実験
 - 特定の条件でMis-Originを検知・管理者へ通知
 - **当面の間実験は続きます**

(メール例)
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

通知条件

- JPIRRにルートオブジェクトを登録している
- ルート or メンテナーオブジェクトのdescrに「X-Keiro」の記述とメールアドレスがある

(whois 記入例)

```
> 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
```

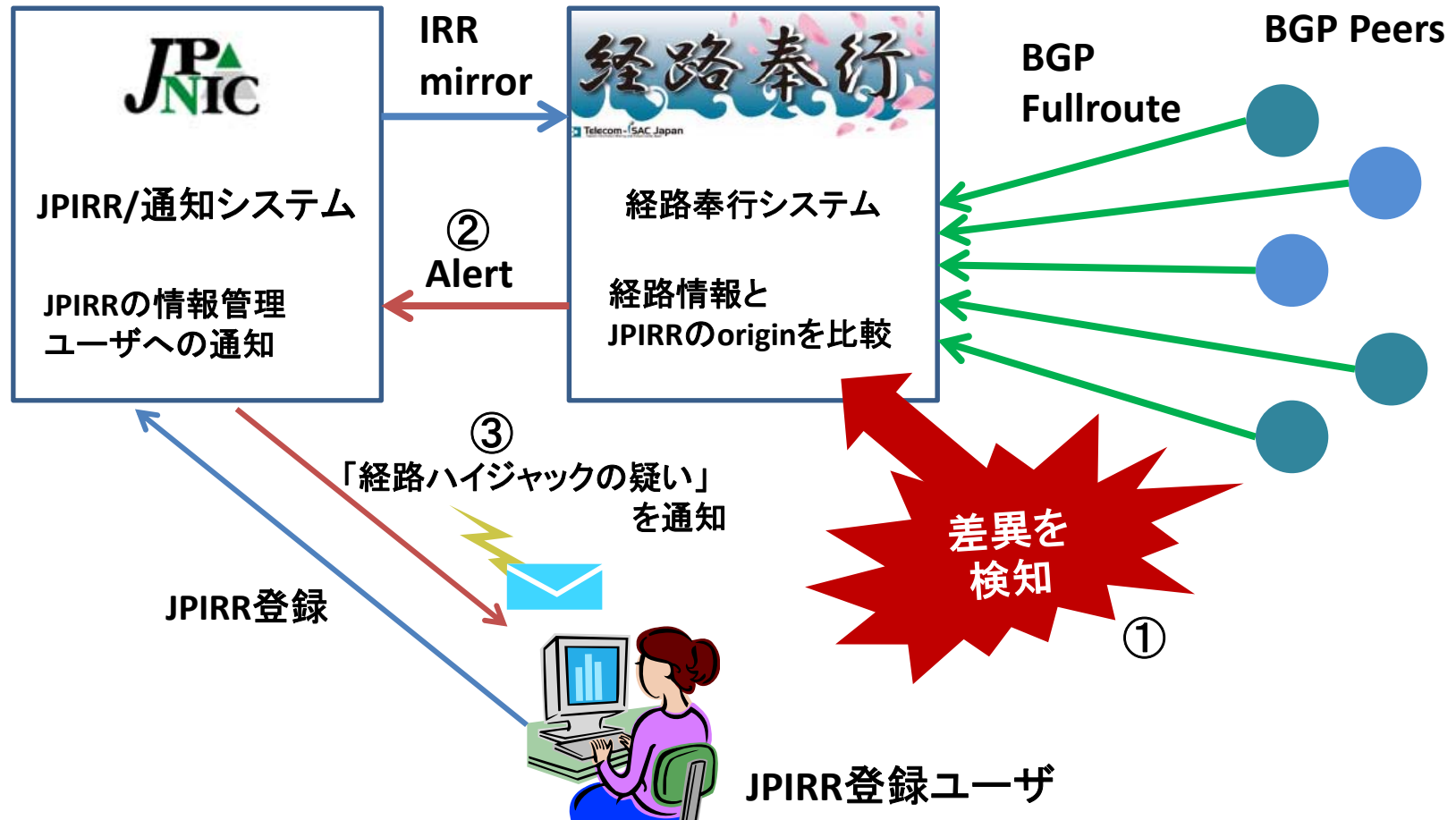
(以下省略)

参考サイト

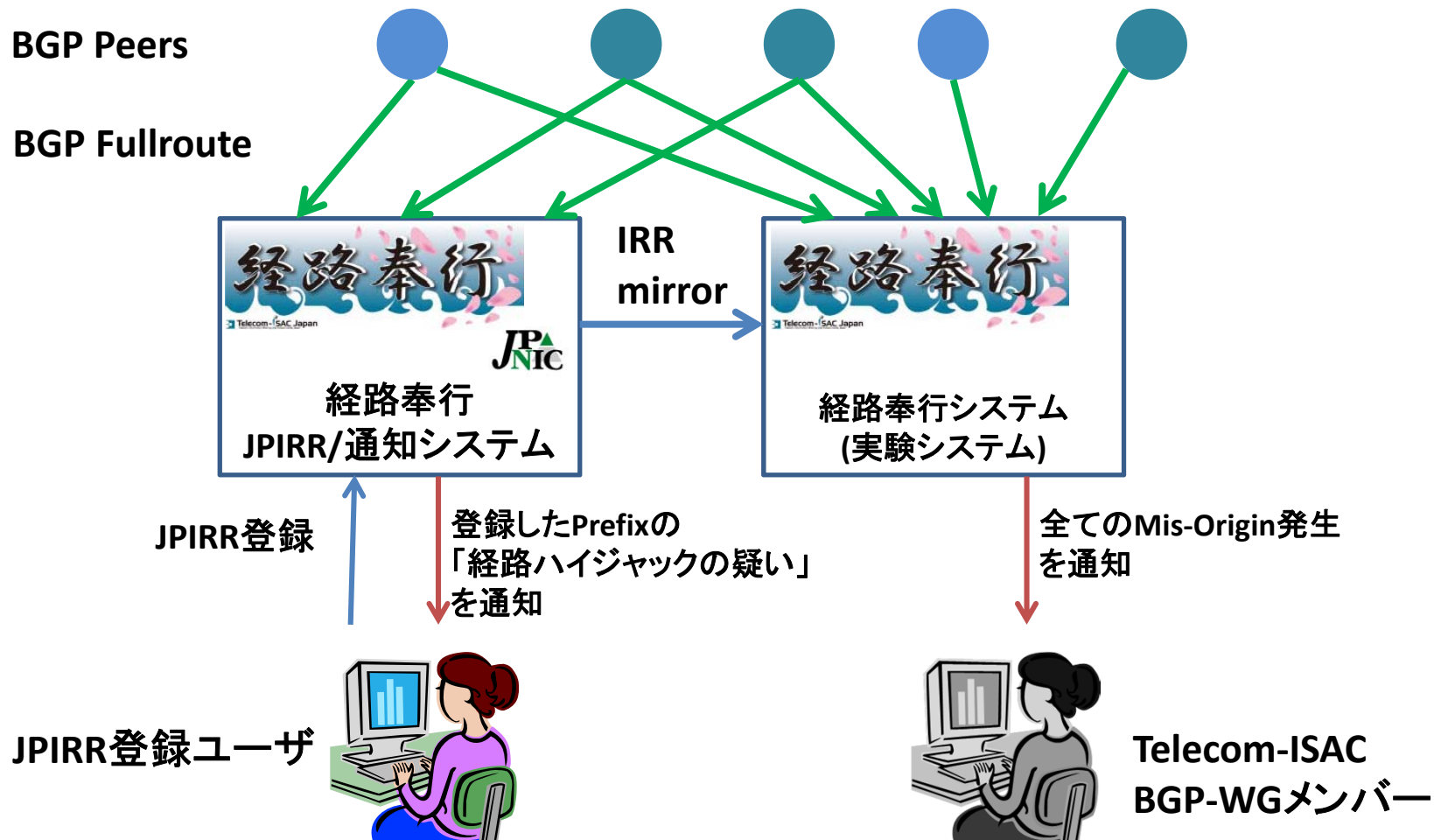
http://www.nic.ad.jp/ja/ip/irr/jpirr_exp.html

<http://www.nic.ad.jp/doc/jpnic-01077.html>

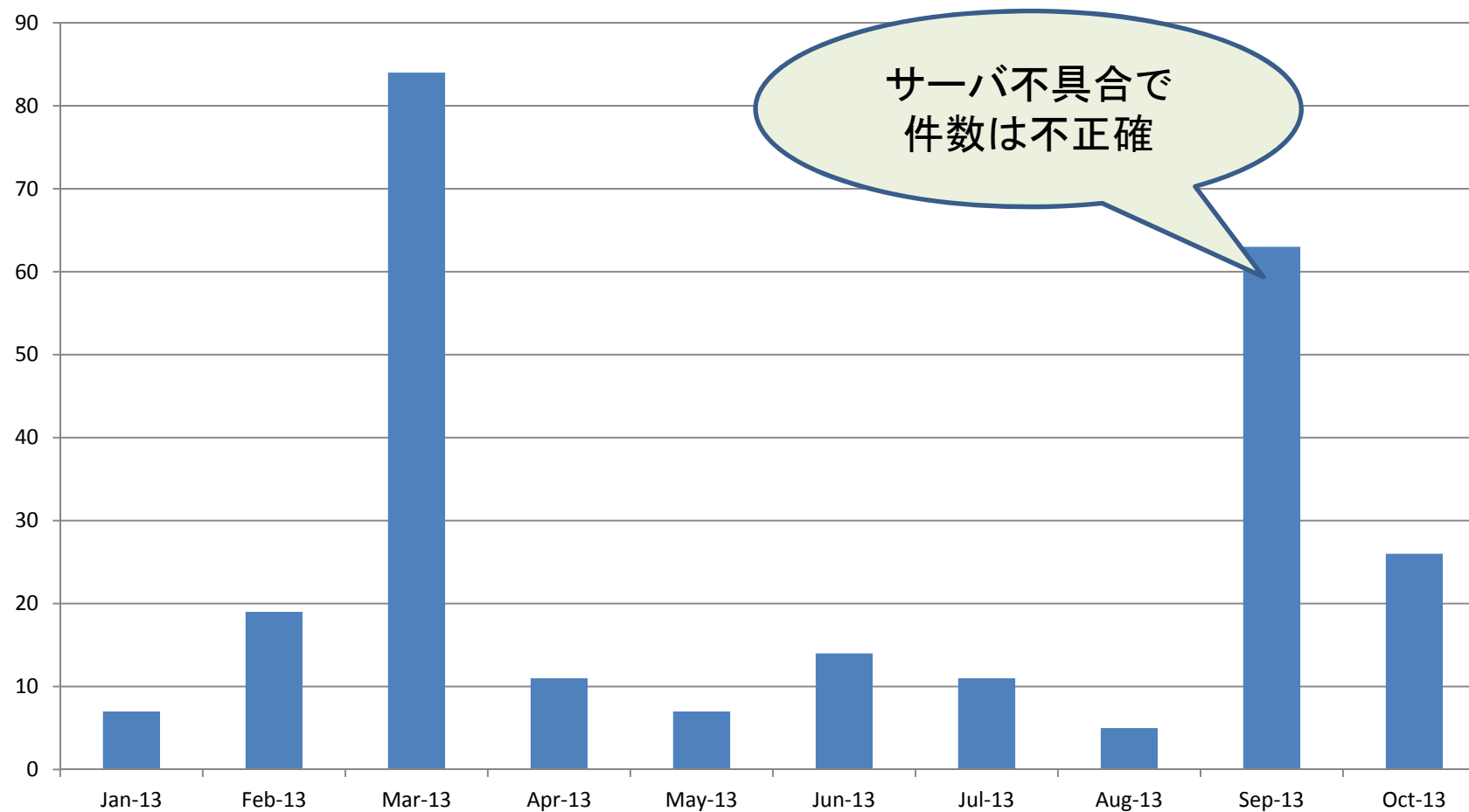
今までの経路奉行



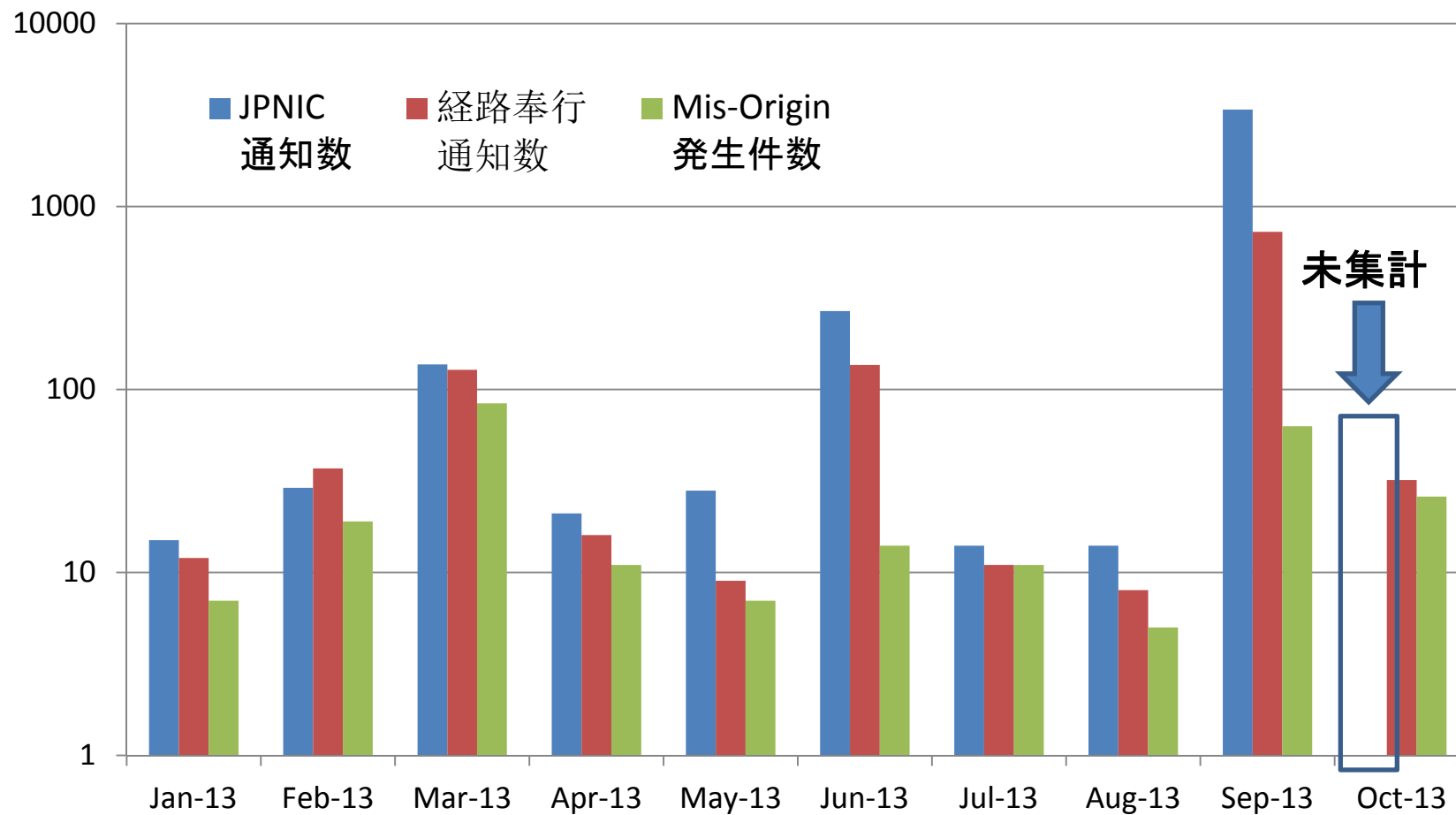
経路奉行なう



2013年 Mis-Origination検知数



2013年メール通知状況



BGPMONについて

<http://www.bgpmon.net/>

The screenshot shows the BGPmon website homepage. At the top is the BGPmon logo. Below it is a navigation bar with links for HOME, AUTONOMOUS SYSTEMS, PREFIXES, ALERTS, and PEERMON. A secondary navigation bar contains links for Welcome Tatsuya Hakano, BGPmon API, Help, Configurations & Settings, and Logout. The main content area is titled 'HOME' and is divided into three columns. The left column, 'Welcome to BGPmon', contains a welcome message, information about prefix services (basic and premium), and a link to an introduction video. The middle column, 'Recent Alerts', features a 'Prefix Information' section with an input field for an IP address and a 'Show Result' button. The right column, 'Recent Blog posts', lists three articles: 'Looking at the spamhaus DDOS from a BGP perspective', 'Accidentally stealing the internet', and 'Syria shuts down the Internet', each with a brief summary and a link to the full post.

BGPmon

Welcome Tatsuya Hakano | BGPmon API | Help | Configurations & Settings | Logout

HOME | AUTONOMOUS SYSTEMS | PREFIXES | ALERTS | PEERMON

HOME

Welcome to BGPmon

Welcome to the new BGPmon client portal! Over the last few months we've worked hard to bring you our new portal. We believe it's a huge improvement as compared to the old website.

Your prefixes
As our service now comes in two flavors: a basic and premium version, all accounts by default are basic accounts allowing you to monitor up to 5 prefixes for free. For your convenience we have kept all your prefixes, making the upgrade to a premium account quick and easy.

Premium service
The BGPmon API and the daily routing report feature are now part of our premium package. In order to continue using these features you will need a premium account. For a full list of features please see our website.

[Check out the introduction video](#)

Recent Alerts

Prefix Information

IP address:

Recent Blog posts

Looking at the spamhaus DDOS from a BGP perspective
It's been a busy week for network engineers world wide, rerouting around broken optical links and of course the 300Gb/s DDOS attack towards Spamhaus and Cloudflare. This DDOS has been classified as the largest DDOS attack ever recorded and has been written about quite a bit in mainstream media. There's been a bit of discussion [...]

Accidentally stealing the internet
Just a few days ago we learned about an incident involving a mis-issued SSL certificate that was used in a Man in the Middle attack to intercept Gmail data. In this blog post we'll talk about how Man in the Middle (MITM) attacks work and we'll look at recent BGP MITM event that caused traffic [...]

Syria shuts down the Internet
As of 10:27 UTC this morning the majority of the Internet in Syria is no longer connected to the rest of the world and can be considered as offline. Syria has only one major provider, AS29256 The Syrian Telecommunications Establishment. This provider is government owned and originates 58 out of 62 Syrian prefixes. This morning between [...]

BGPMON新規登録方法

<https://portal.bgpmon.net/register.php>

フォームに必要事項を入力すると、メールが届く → 指示に従い登録



Create a new BGPmon Account



Create a new account by submitting the form below. Please note that all fields are mandatory.

To prevent robots from creating random accounts, there's a little math test. The answer should be the same as the BGP port number. After submitting the form, you'll receive an email to confirm your new account.

ACCOUNT DETAILS	
FIRST NAME	<input type="text"/>
LAST NAME	<input type="text"/>
EMAIL ADDRESS	<input type="text"/>
COMPANY NAME	<input type="text"/>
COUNTRY	<input type="text"/>
PASSWORD	<input type="password"/>
CONFIRM PASSWORD	<input type="password"/>
PROVE YOU'RE NOT A ROBOT HOW MUCH IS: 170 + 9 ?	<input type="text"/>

=179?

Copyright © BGPmon Network Solutions Inc. 2012. All rights reserved.

| Questions or remarks: BGPmon.net |

BGPMONサービスの価格

CHOOSE YOUR PLAN

Up to 10 Prefixes	\$59 Monthly	\$649 Annually
Up to 20 Prefixes	\$99 Monthly	\$1089 Annually
Up to 50 Prefixes	\$179 Monthly	\$1969 Annually
Up to 100 Prefixes	\$219 Monthly	\$2409 Annually
Up to 250 Prefixes	\$399 Monthly	\$4389 Annually
Up to 500 Prefixes	\$699 Monthly	\$7689 Annually
Up to 1000 Prefixes	\$1099 Monthly	\$12089 Annually


※ 5Prefixまでは無料(ただしフルサービスは受けられない)

Cyclopsについて

<http://cyclops.cs.ucla.edu/>

ゲストログインも可

Tatsuya Nakano tt-nakano@int-gw.kddi.ne.jp [My Cyclops](#) | [Logout](#) Last login: 2013-11-11 02:15:58 UTC [Home](#) | [FAQ](#) | [About Cyclops](#)



Cyclops beta
an open eye to your net

- Global Visibility ▶
- Critical Infrastructure ▶
- Anomalies ▶
- My Cyclops ▶

My Cyclops

[My prefixes](#) [Add prefixes](#) **My ASNs** [My neighbors](#) [My alerts](#) [My account](#)

To see all origin ASNs leave "My origin ASN" empty below. Your neighbor ASNs will automatically be added to your neighbor list once you add an origin ASN, please check them at [My Neighbors](#) tab.

Note: by default you will start receiving **New prefix** alerts if you don't configure your prefixes after you add ASNs. You can configure your prefixes at [Add prefixes](#) tab.

ASNs:
enter list of ASNs, e.g., 7018,701,52

My Cyclops

0 open alerts

My network:
2 prefixes
1 ASes
0 neighbor ASes

Quick lookup

ASN or AS Name: >

IP address or DNS name: >

Total of 1 origin ASNs

	ASN ↓	AS name	Date Edit (UTC)	Alert on:		
				new prefix Yes No	new neighbor Yes No	transit Yes No
<input type="checkbox"/>	2516	KDDI KDDI CORPORATION	2011-11-13 02:11:15	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cyclops新規登録方法

<http://cyclops.cs.ucla.edu/register/>


Home | Login | FAQ | About Cyclops



Cyclops beta
an open eye to your net

- Global Visibility ▶
- Critical Infrastructure ▶
- Anomalies ▶

Welcome to Cyclops



Cyclops is a network audit tool for service providers and enterprise networks, providing a mechanism to compare the **observed** behavior of the network and its **intended** behavior. Cyclops is able to detect several forms of **route hijack** attacks, i.e. when Internet routes are maliciously diverted from their original state. Recent incidents such as the **Youtube hijack in Feb'08** show that route hijacking is currently a real threat in the Internet.

If you just want to have a sneak peek of Cyclops, use the guest account:

Username: guest
Password: guest

You will not receive alerts if you use the guest account. For that you need to **Sign Up** for an user account, it's completely **free**.

Cyclops uses data from thousands of routers from [RouteViews](#), [RIPE-RIS](#), [Abilene](#), [Packet Clearing House](#) and [Bgpmon](#) from Colorado State University, making it the widest and fastest free tool to assess how the rest of the world is reaching your network. We plan to incorporate additional data in the future such as active measurement and internal ISP data (router configs, iBGP, IS-IS, OSPF, MPLS VPN). If you're willing to provide us the data and want your network data to be audited by Cyclops, please drop a message to [cyclops at 6watch dot net](mailto:cyclops@6watch.net).

Cyclops was presented at [Nanog 40](#) and [NANOG 43](#). Please read the [Cyclops FAQ](#) for further details.

Cyclops Registration

Name *

Title *

Organization *

Organization type *
Internet Service Provider

Country *
United States

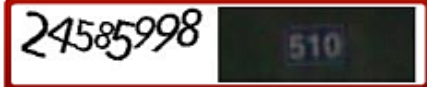
Username *

Email *

New password *

Retype new password *

Security Code *



テキストを入力

Sign Up

Already registered?