

# ほんとにあったRPKIの話



2018/11/27

- 2008年4月  
株式会社TOKAIコミュニケーションズ入社  
(当時は株式会社ビック東海)
- 主な業務  
OISPの運用
  - トラフィックの監視、NW構成変更
  - 一般家庭ユーザからの問い合わせ対応 など



- 2017年12月 1件の問い合わせを受領

**あるドイツのサイトにアクセスできません。**

- いただいた情報①

- 現象は2017年秋頃より発生

- ユーザーータの再起動で改善せず

- スマートフォンからのテザリングでは、アクセス可能

- **いただいた情報②**

- ユーザの社内ネット環境(他社キャリア)からはアクセス可能

- 対象のドイツのサイトへ問い合わせたところ、個人からの問い合わせは**対応不可**と回答されたとのこと

• いただいた情報③

–traceroute

対象サイトのAS

AS②  
国際AS

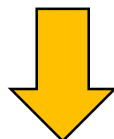
←ここまで応答ある

AS①  
国内AS

AS10010

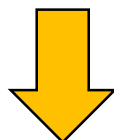
AS②の網内か  
対象サイトのAS内が怪しい？

まずは自社試験環境から再現試験を実施

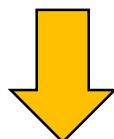


対象サイトへアクセス可能

traceroute問題無し

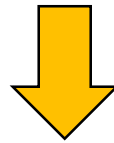


再現不可

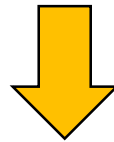


果たして原因は??

対象のサイトの問い合わせフォームより、  
問い合わせを実施



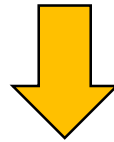
数日後、、、応答なし



もしかして**ドイツ語**が必須！？



IPv6での接続は可能？



ユーザにてアクセス可能！！！！

新たな情報として、

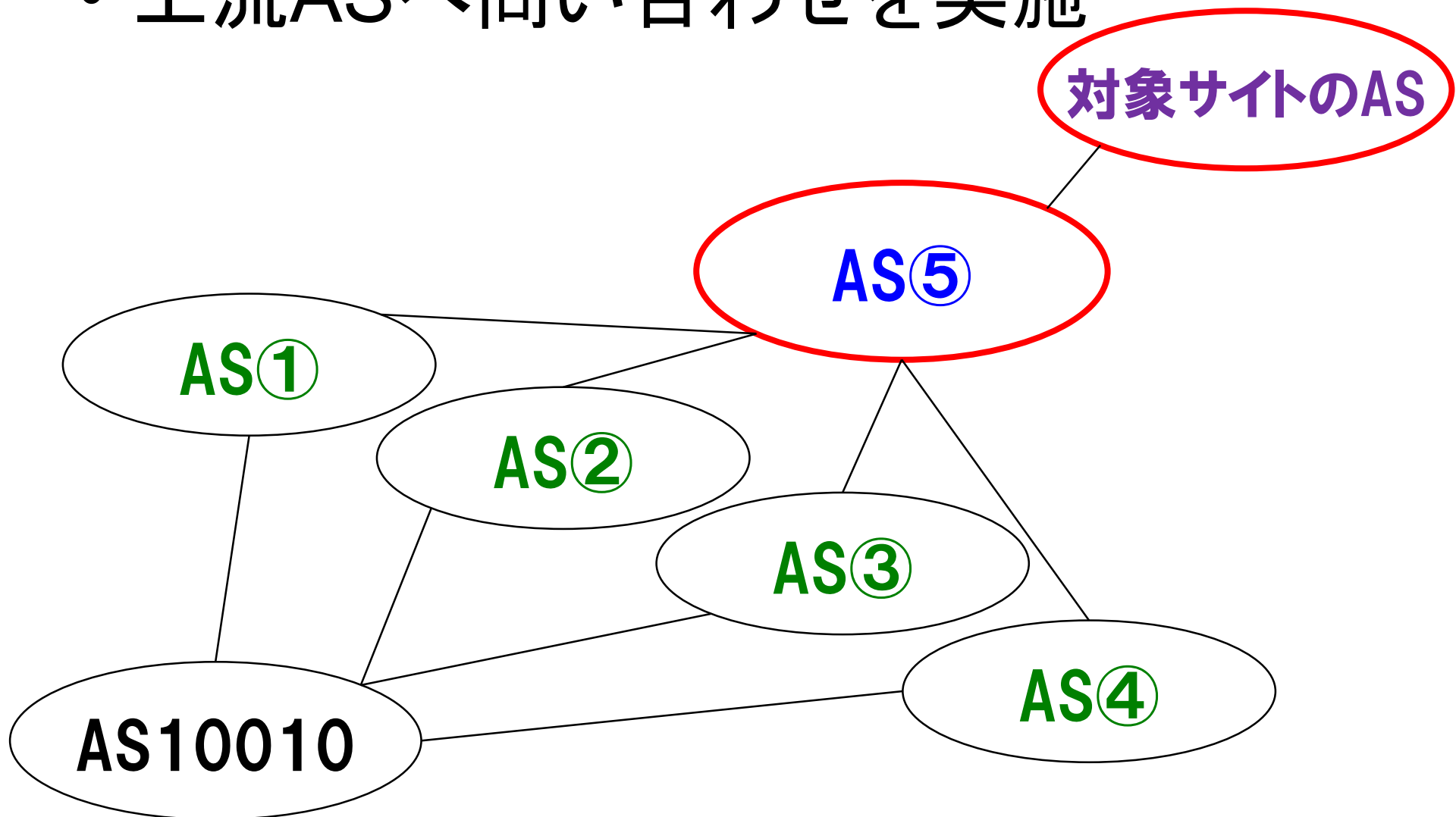
IPv4アクセス**不可**だが

IPv6ではアクセス**可能**

ということが判明。

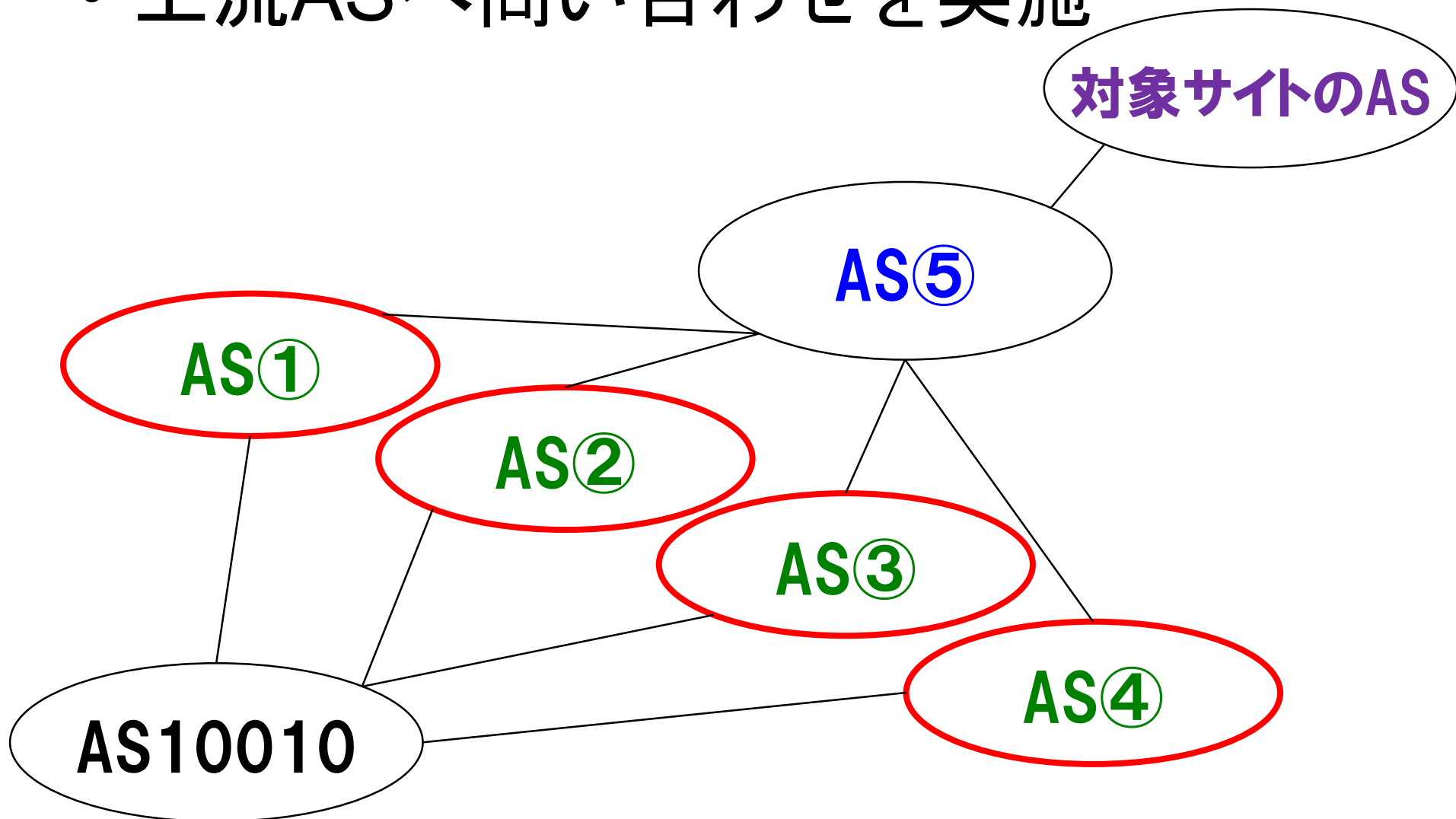
※IPv6でアクセスしていただきユーザから更なる調査の時間をいただきました。

- 上流ASへ問い合わせを実施



- 対象サイトのASについては、問い合わせ先を把握していなかったため、問い合わせ不可
- AS⑤に対して、調査の協力を依頼したが弊社と直接接続がなかったため、受け付けていただけなかった。

- 上流ASへ問い合わせを実施

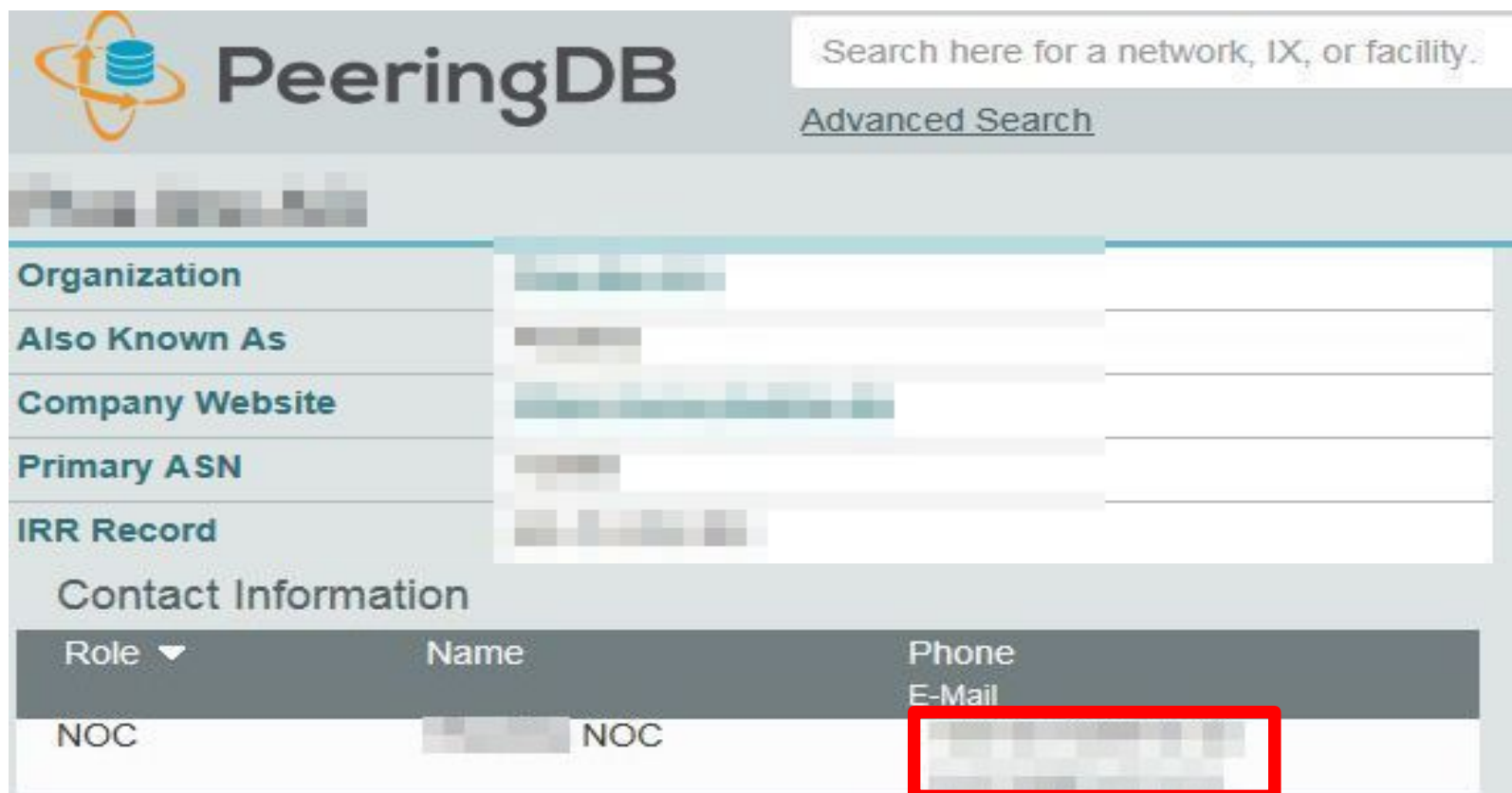


- AS①②③④へ、網内で同様の事象が発生していないか。  
また、AS⑤に対して同問い合わせを投げ  
ていただけませんか？

- 返信されてくるメールには
  - 「網内からの接続に問題なし」
  - 「別ASへの問い合わせは対応不可」とのこと、、、

やはり対象ASに連絡したい！

問い合わせ窓口からでは応じていただけなかったが、**ピアリング**窓口へ投げてみてはどうか！？



PeeringDB Search here for a network, IX, or facility. Advanced Search

Organization: [Redacted]

Also Known As: [Redacted]

Company Website: [Redacted]

Primary ASN: [Redacted]

IRR Record: [Redacted]

Contact Information

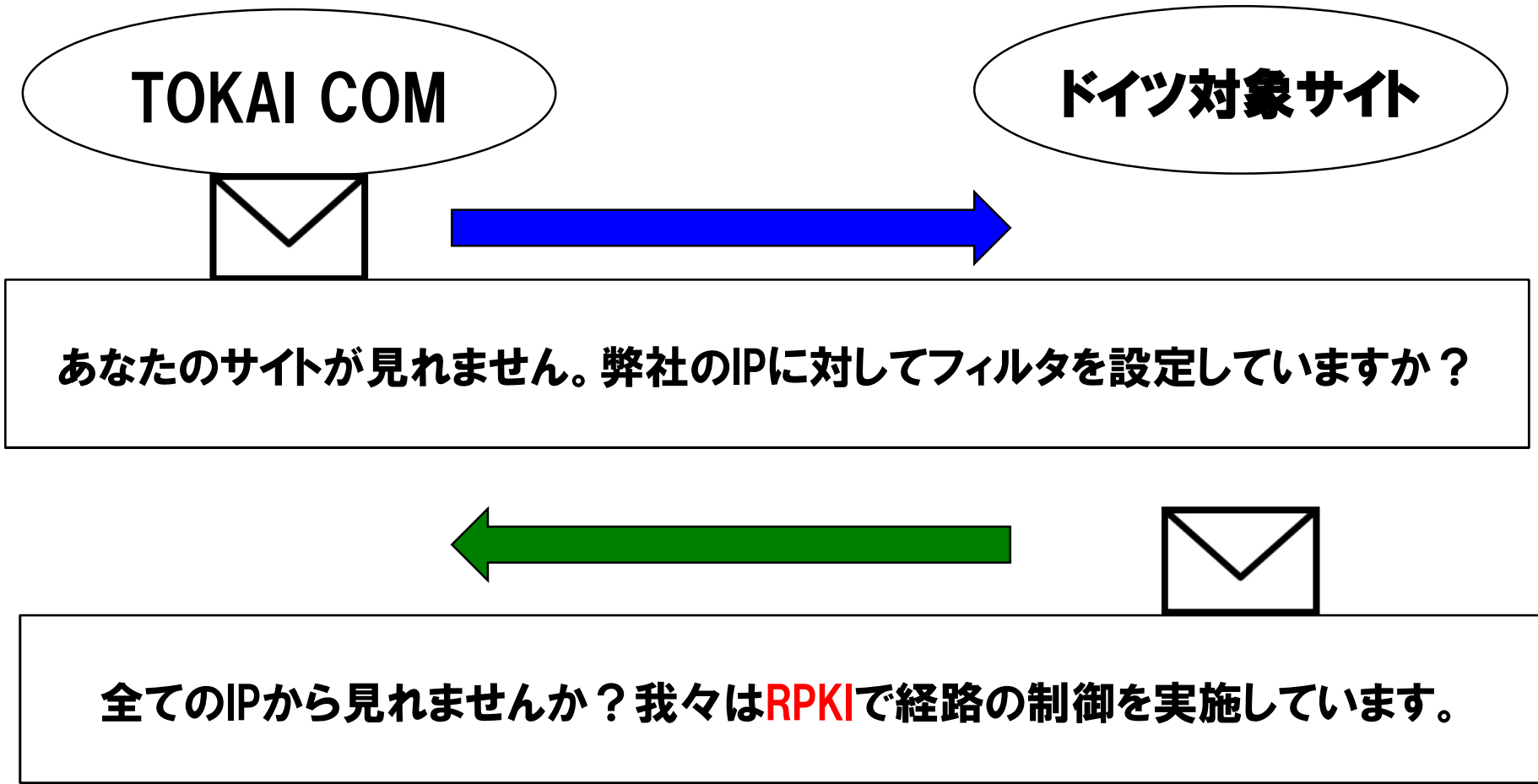
Role ▼	Name	Phone	E-Mail
NOC	[Redacted] NOC	[Redacted]	[Redacted]

<https://www.peeringdb.com/>



**対象ASから待望の返信がきた！！！！**

・対象サイトへ問い合わせ



あーるぴーけーあい??

- JPNICのサイトで確認

AS番号	プリフィックス	状態
10010	[REDACTED]	INVALID LENGTH

<http://roa2.nic.ad.jp:8080/bgp-preview>

登録自体はしっかり行われている(?)

- JPNICのサイトで確認

AS番号	プリフィックス	状態
10010	[REDACTED]	INVALID LENGTH

<http://roa2.nic.ad.jp:8080/bgp-preview>

**INVALID ! ?**

# INVALID

→ROA登録とOriginASが不一致の経路

○2015年頃

「RPKIの試験運用のご協力をお願いします！」

と案内され、RPKIを登録しておりました。

その後、弊社から広報される経路の状況が様々な用途により日々変化していきました、、、

※杉山自らが登録

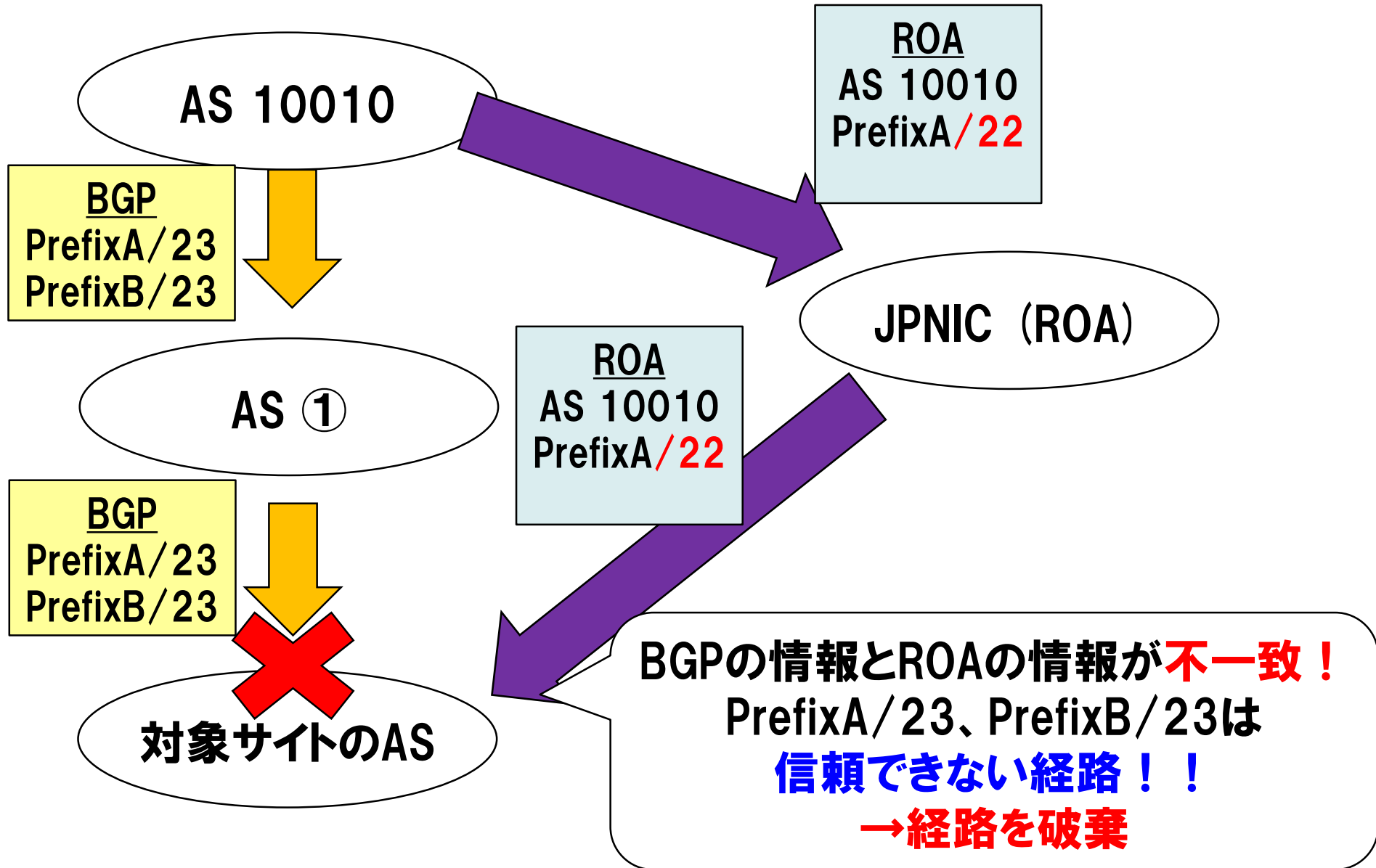
- JPNICのサイトで登録内容を修正

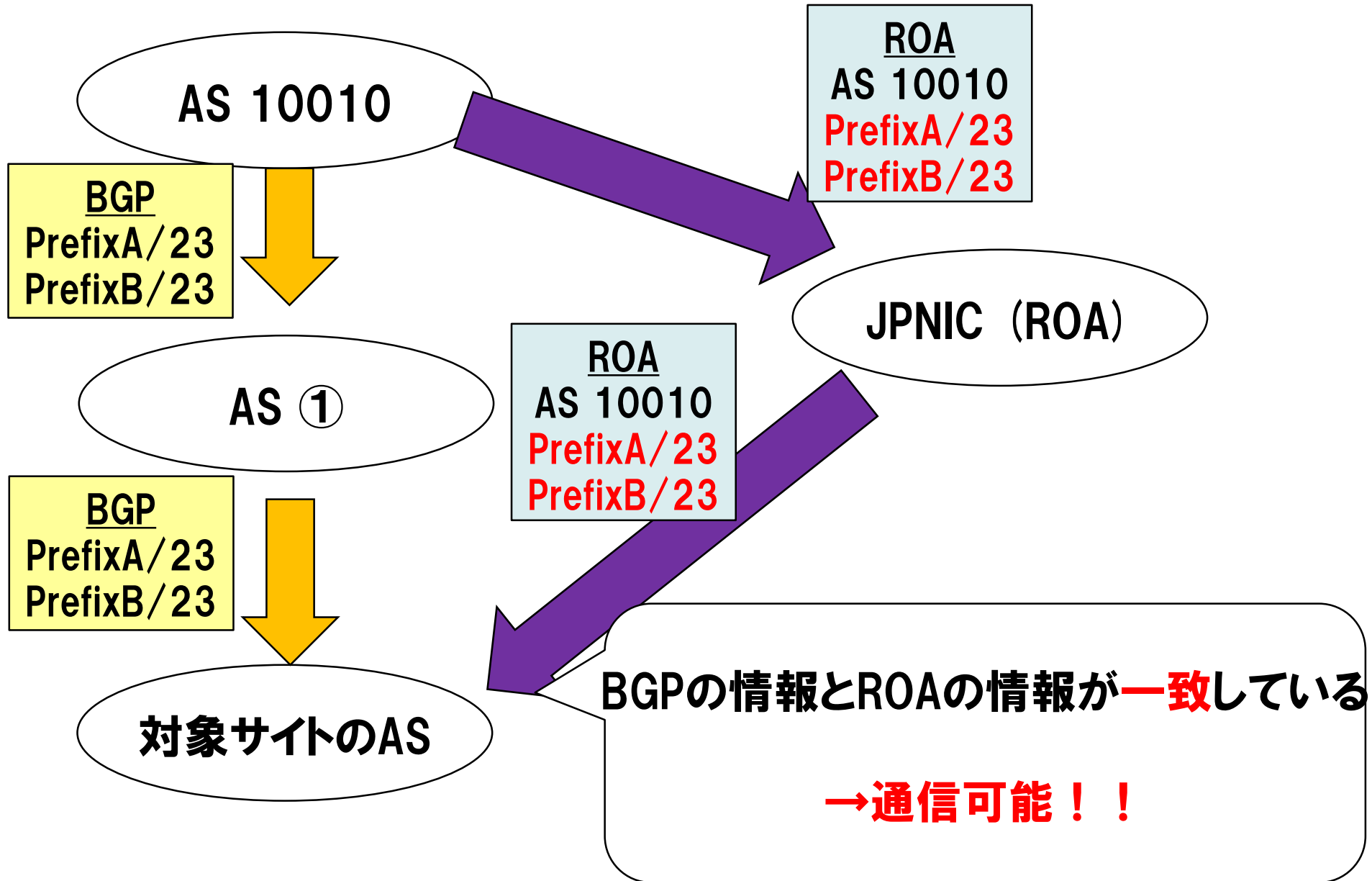
AS番号	プリフィックス	状態
10010	[REDACTED]	VALID

<http://roa2.nic.ad.jp:8080/bgp-preview>

※反映まで約1日かかりました







# 祝 復旧！！！！

- IPv4の分割されたIP(ユーザ)からの通信は不可となり、分割されていないIP (試験環境)からの通信は問題なかった
- IPv6に関しては、経路分割が行われなかったため、INVALIDとはなっていなかった

- RPKIを管理・運用について

## ○事象発生時

maximum prefix length「指定なし」

→exact matchした経路のみ有効

## ○修正後

maximum prefix length「24」

→プレフィックス長が「/24」以下の経路が有効

## • RPKIを管理・運用について



一般社団法人 日本ネットワークインフォメーションセンター  
Japan Network Information Center

最新の情報に更新(メイン画面)

ROA Webの利用を停止

### 詳細

Prefix	最大長	AS番号
[REDACTED]	24	10010

設定当初は経路情報として、**prefix長まで考慮**する必要があると判断したが、  
経路防御において、ASと経路の組み合わせが重要であることと、運用の負荷への観点から、  
**/24まで許容する**設定としました。

この設定により

**今回のような経路分割による経路情報の不一致は防げる！**

- RPKIの運用をしっかりとしましょう
- INVALIDに気付ける仕組みがあったら嬉しい(メール通知など)
- INVALID経路をdropする運用ってされています??

- IPアドレス依存のトラブルシューティングでどのように対応されています？
- 海外ASへの問い合わせは大変
- 直接ピアしてないところへ問い合わせる手段がほしい(切実)

なにかいい方法があったら教えてくださいm(\_\_)m



ご清聴ありがとうございました