- mis-operation -

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

2009 (c) Internet Initiative Japan Inc.

注意書き

- 特定のミスや実装について誹謗するものではありません
- 過去の設計や状況に依存した事例もありますが、そんな事例から学べることも多いので収録してあります

2009 (c) Internet Initiative Japan Inc.

僕たちは多くのミスを犯した

- 場合によっては冷汗をかくぐらいで済むこともあるけど、時に大きな障害に繋がっちゃう

- まずは、どんなミスをしてきたかみてみよう
  - 影響の大きそうなものを重点的に
- 以降は、実際に発生した事象の紹介です
  - 事例の収集にご協力いただいた皆さん、ありがとうございました

2009 (c) Internet Initiative Japan Inc.

No.1 設定のcut & paste

- ルータ設定時に他のルータの設定を参照してcut & pasteしていた
- IPアドレスまで含めて、そのまま再利用してしまった
- 意図しない経路制御になったり、アドレスの重複が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.1 設定のcut & paste

IPアドレスを適切に
書き換えるのを
忘れてしまった

設定流用

```
Interface Bundle-Ether1
 ipv4 address 10.0.0.1 255.255.255.0
 ipv6 address 2001:db8::1/64
 bundle minimum-active links 2
!
```

```
Interface Bundle-Ether1
 ipv4 address 10.0.0.1 255.255.255.0
 ipv6 address 2001:db8::1/64
 bundle minimum-active links 2
!
```

2009 (c) Internet Initiative Japan Inc.

No.2 ルータの置き換え

- IPアドレスなどの設定はそのままで、ルータを新しいものに置き換えようとしていた
- 旧ルータが稼働中にも関わらず、適当なインタフェースを設定して新ルータをネットワークに繋いでしまった
- 同じルータIDとloopbackのIPアドレスを持つルータが網内に2台存在することになり、経路障害に

2009 (c) Internet Initiative Japan Inc.

No.2 ルータの置き換え

旧ルータ

```
Interface loopback0
 ipv4 address 10.0.0.1 255.255.255.255
 ipv6 address 2001:db8::1/128
!
```

新ルータ

```
Interface loopback0
 ipv4 address 10.0.0.1 255.255.255.255
 ipv6 address 2001:db8::1/128
!
```

旧ルータを取り除いてから繋ぐ必要があったのに、先にネットワークに繋いでOSPFを動かしてしまった

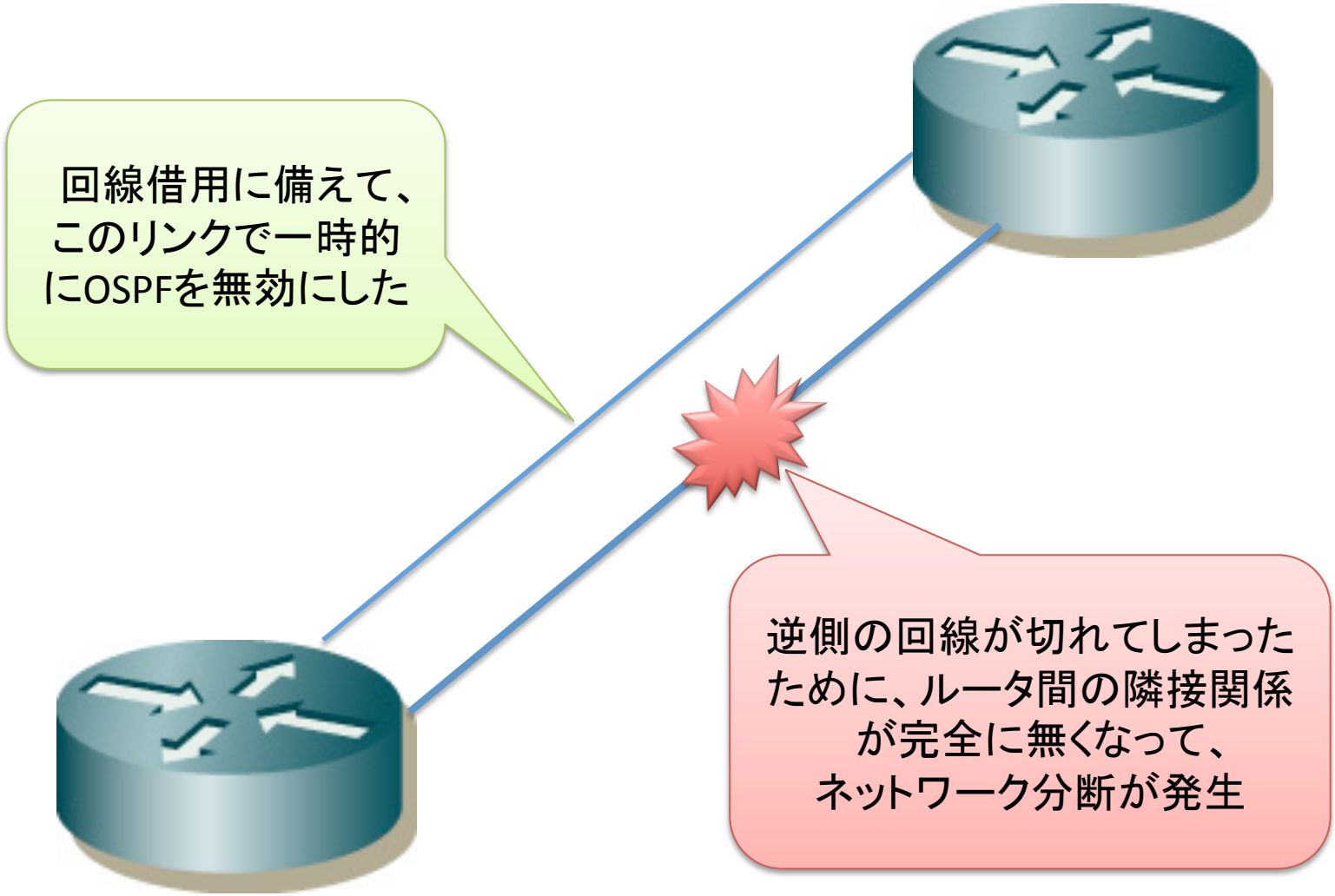
2009 (c) Internet Initiative Japan Inc.

No.3 回線借用

- 回線借用に備えて、事前に迂回設定しようとしていた
- 切断時のばたつきを嫌って、一時的に該当回線でOSPFを無効にしてしまった
- 作業時、迂回設定した回線とは別な回線が切断されてしまった
- ネットワーク分断に

2009 (c) Internet Initiative Japan Inc.

No.3 回線借用



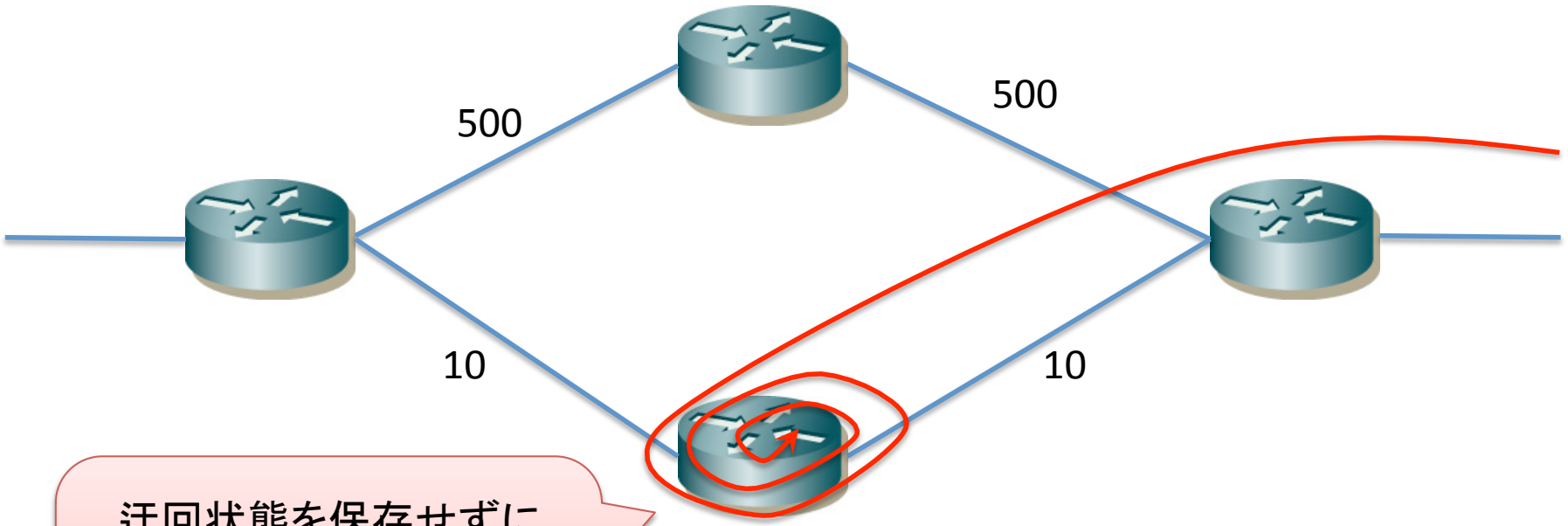
2009 (c) Internet Initiative Japan Inc.

No.4 バックボーンルータ再起動

- ファームウェア更新のために、バックボーンルータで迂回をかけて再起動を実施しようとしていた
- 迂回状態を保存せずに再起動してしまった
- 再起動後、OSPFが収束してからBGPの収束まで吸い込んだパケットを破棄してしまった
  - OSPF Stub Router Advertisement [RFC3137]を再起同時に適用することで改善

2009 (c) Internet Initiative Japan Inc.

No.4 バックボーンルータ再起動



迂回状態を保存せずに
再起動したためBGPが
収束するまでパケットロス
が発生してしまう

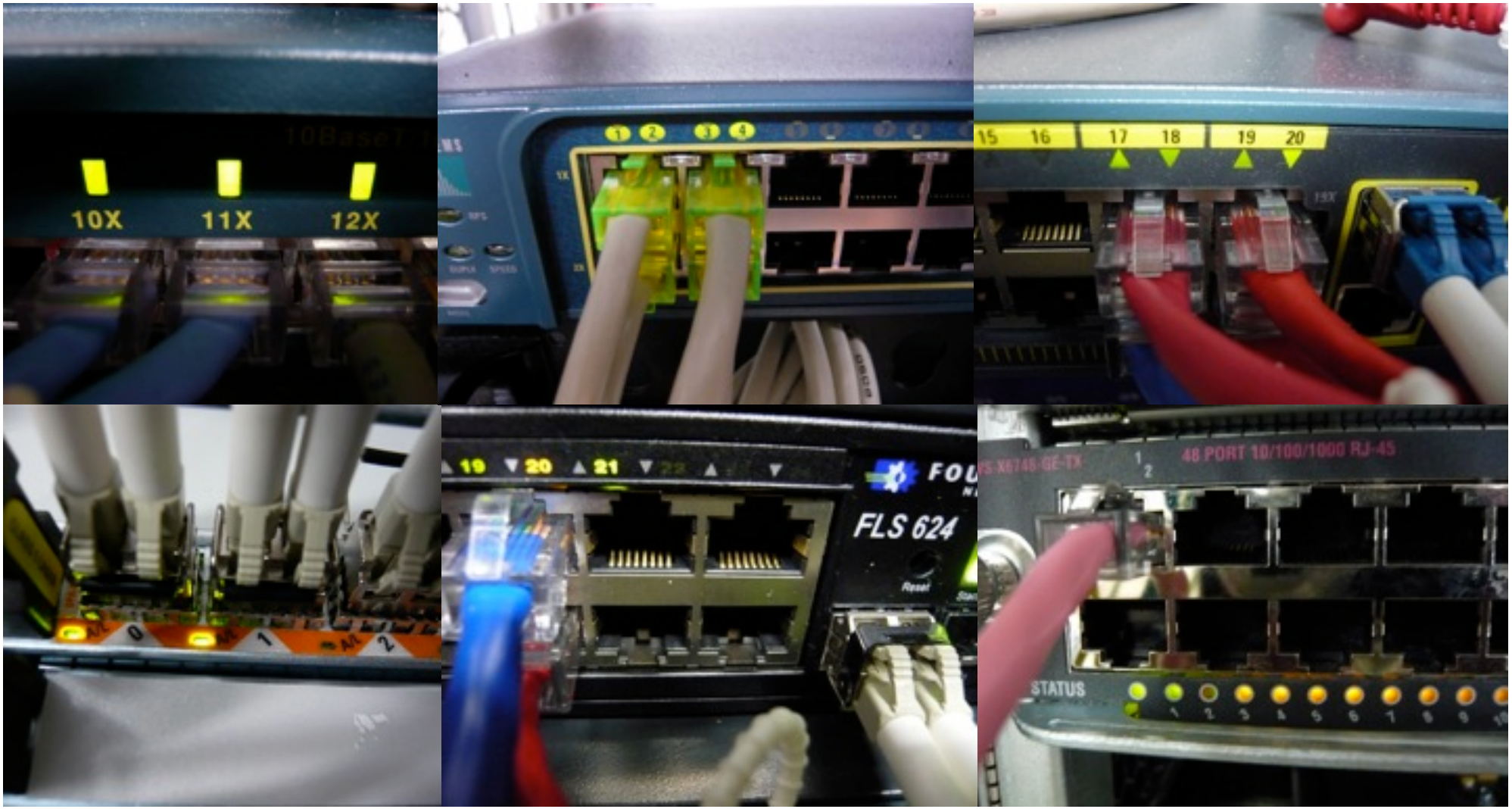
2009 (c) Internet Initiative Japan Inc.

No.5 ケーブル抜きかえ

- セグメントの移設のため、ルータとスイッチ間のケーブルを抜きかえる作業を行っていた
- ポート番号とLEDの消灯でケーブルを確認して移設しようとしていた
- スイッチ側でLEDの位置がポートとずれていて、異なるケーブルを抜いてしまった
- 思わぬセグメントで接続断に

2009 (c) Internet Initiative Japan Inc.

No.5 ケーブル抜きかえ



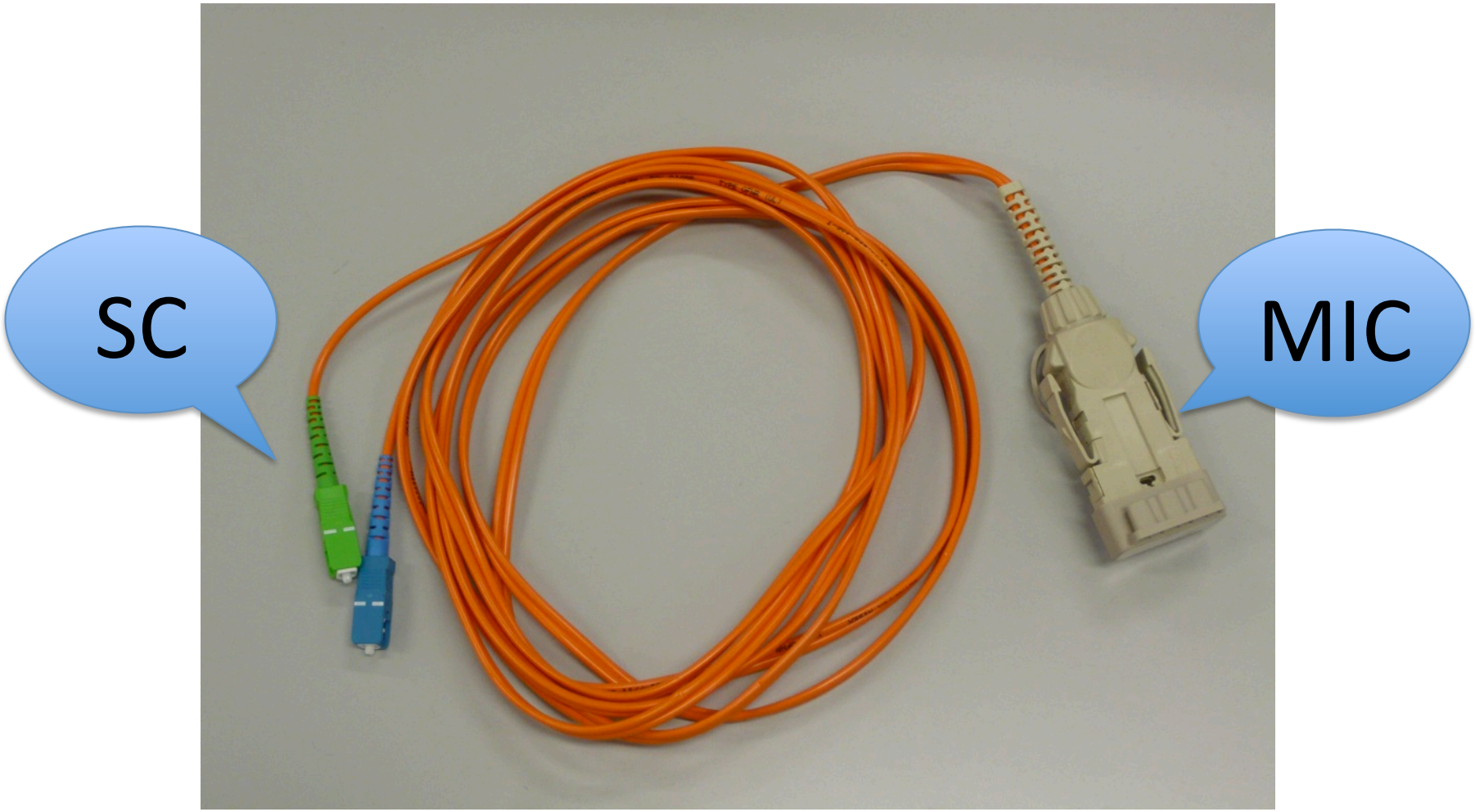
2009 (c) Internet Initiative Japan Inc.

No.6 ケーブル撤去

- ラック下の不要なケーブルの両端を切断して、撤去する作業を行っていた
- MICコネクタで接続されたファイバを、FDDIで利用していた古いファイバだと誤認して切断してしまった
- 実はこれはマルチモードファイバをGbEに転用していた回線で、接続断が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.6 ケーブル撤去



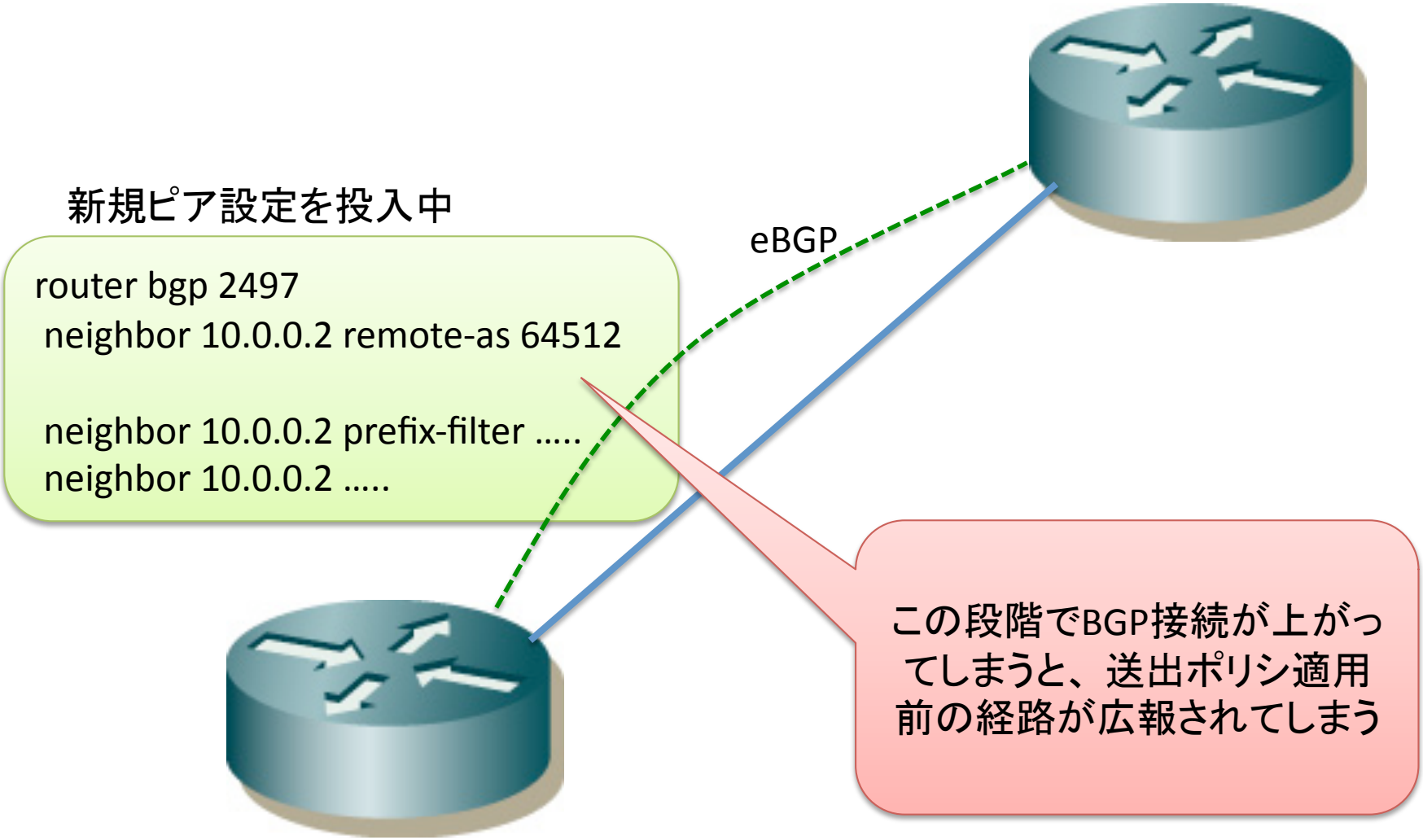
2009 (c) Internet Initiative Japan Inc.

No.7 ciscoで新規BGPピア設定

- ciscoルータで新規にeBGP接続を設定しようとしていた
- 設定を順次投入していたら、フィルタ等を入れる前にピアが上がってしまった
- 細かい経路まで含んだ全経路をピア先に広報してしまった
  - Conf netなどで変更箇所の一括適用で対応
  - 最初のneighbor行で嘘のremote-asを設定して、フィルタなどを設定後に正しいremote-asで上書き

2009 (c) Internet Initiative Japan Inc.

No.7 ciscoで新規BGPピア設定



2009 (c) Internet Initiative Japan Inc.

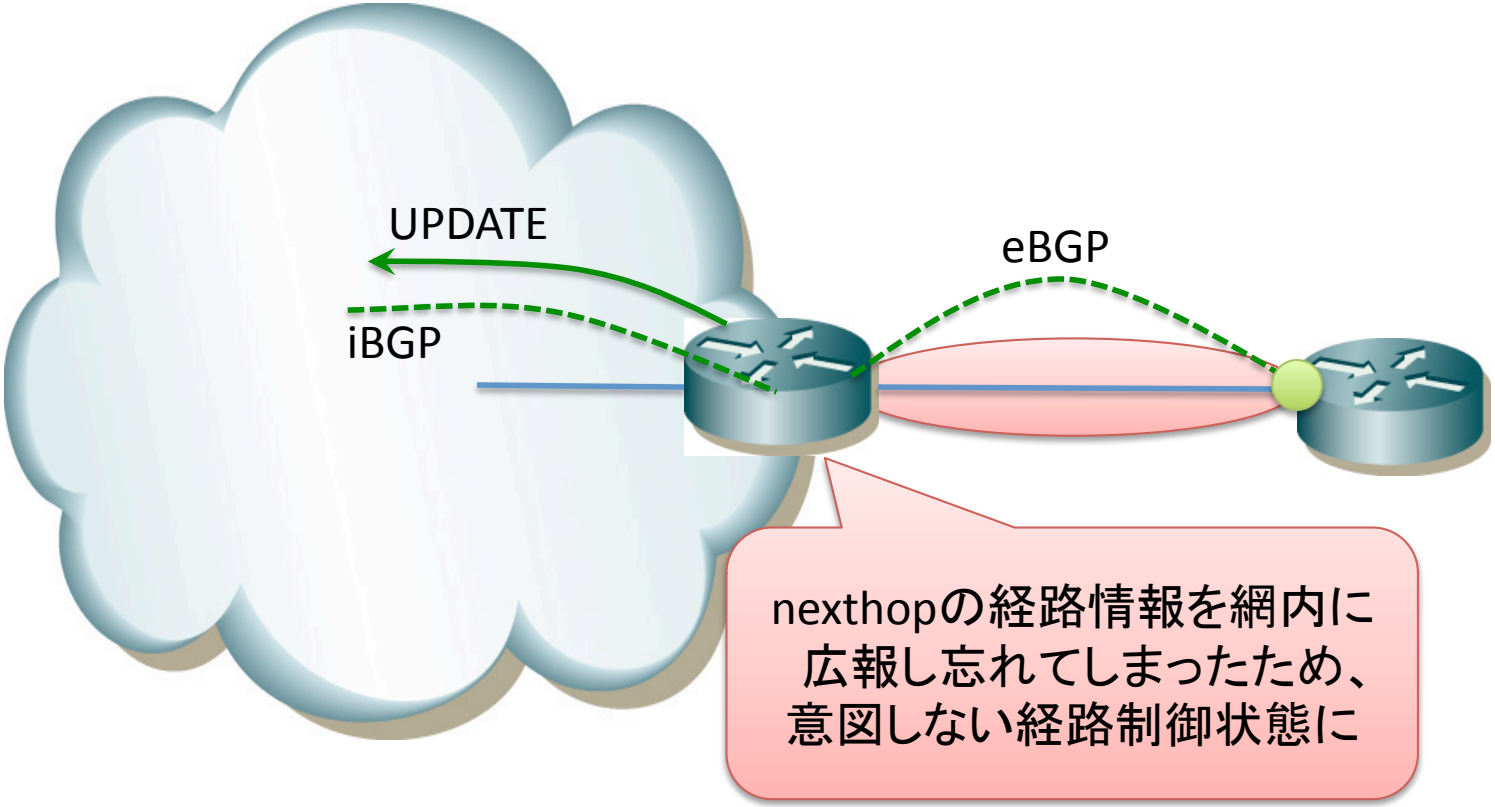
No.8 新規ピア用のインタフェース設定

- eBGPから受け取った経路のnexthopは変更せずにそのまま網内に広報するポリシのASで、新規にプライベートピア接続しようとしていた
- OSPFで接続用インタフェースのネットワークを広報する前に、eBGP接続を上げてしまった
- 思ったようにトラヒックが流れなかったり、経路が不安定になってしまった
  - BGPではnexthop解決にBGP経路が利用できます

2009 (c) Internet Initiative Japan Inc.

No.8 新規ピア用のインタフェース設定

eBGPで受信したnexthopをそのまま網内に流すポリシ



2009 (c) Internet Initiative Japan Inc.

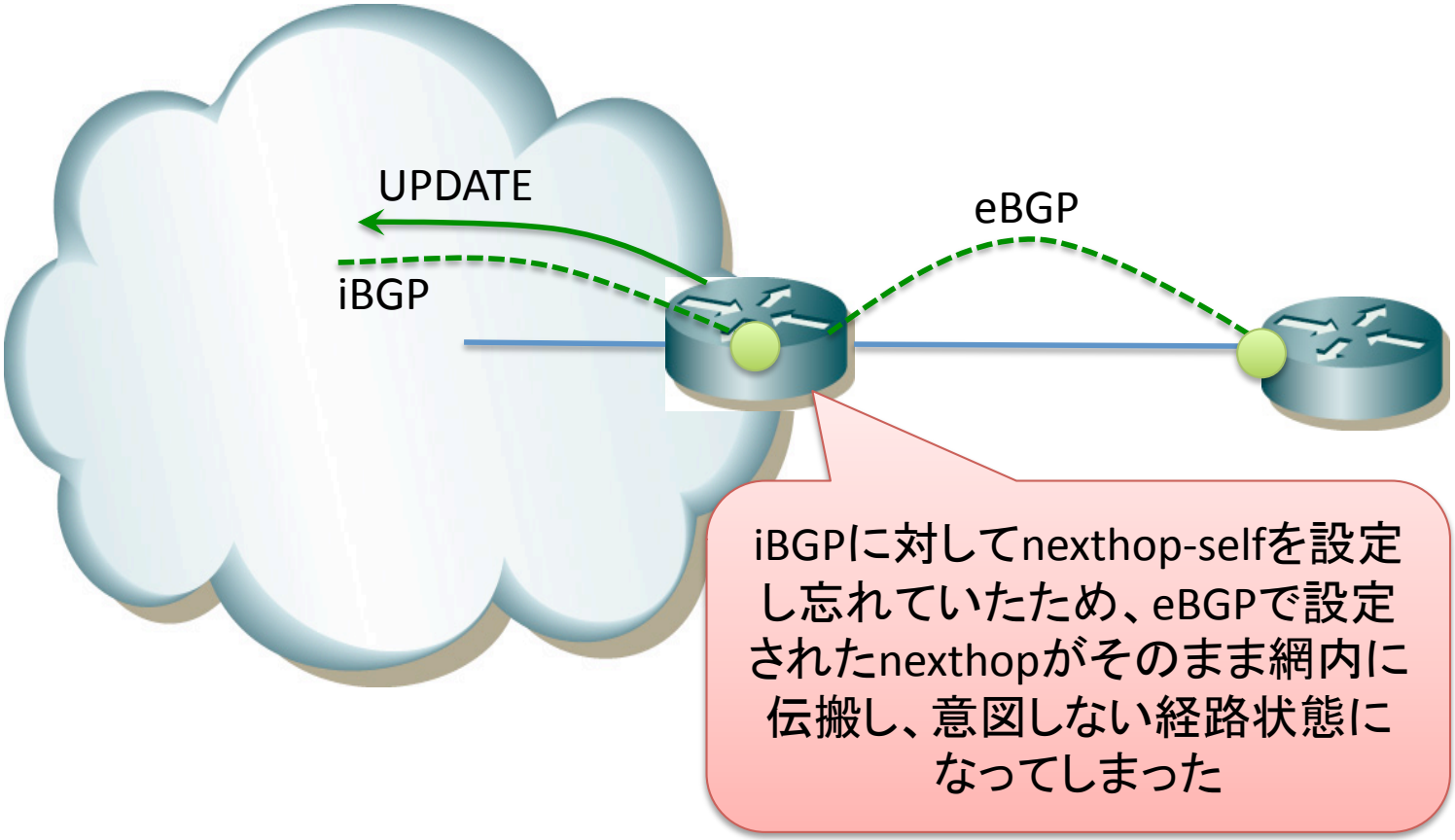
No.9 新規ルータでeBGPピア設定

- eBGPから受け取った経路はnexthop-selfして網内に広報するポリシのASで、新規ルータを設置し、eBGPを設定しようとしていた
- このルータの設定で、バックボーン側へのiBGP接続にnexthop-selfを忘れていた
- 他ASとBGP接続後、nexthopの解決で思わぬところにトラヒックが向いてしまった
  - BGPではnexthop解決にBGP経路が利用できます

2009 (c) Internet Initiative Japan Inc.

No.9 新規ルータでeBGPピア設定

eBGPで受信した経路はnexthop-selfして網内に流すポリシ



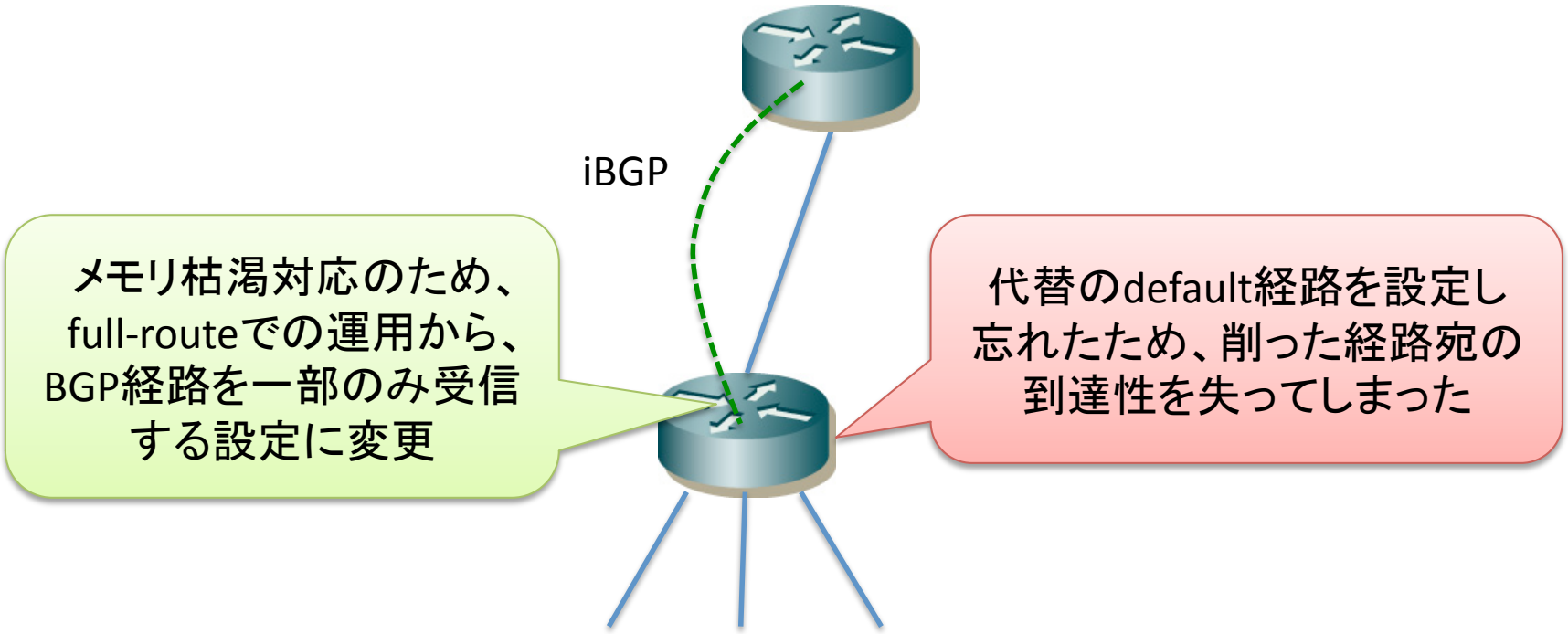
2009 (c) Internet Initiative Japan Inc.

No.10 BGP経路削減

- エッジのルータでメモリ枯渇対処のため、BGP経路を一部フィルタして削ろうとしていた
- 代替のdefault経路を設定し忘れてしまった
- 削った経路宛の到達性が無くなり、パケットを破棄してしまった

2009 (c) Internet Initiative Japan Inc.

No.10 BGP経路削減



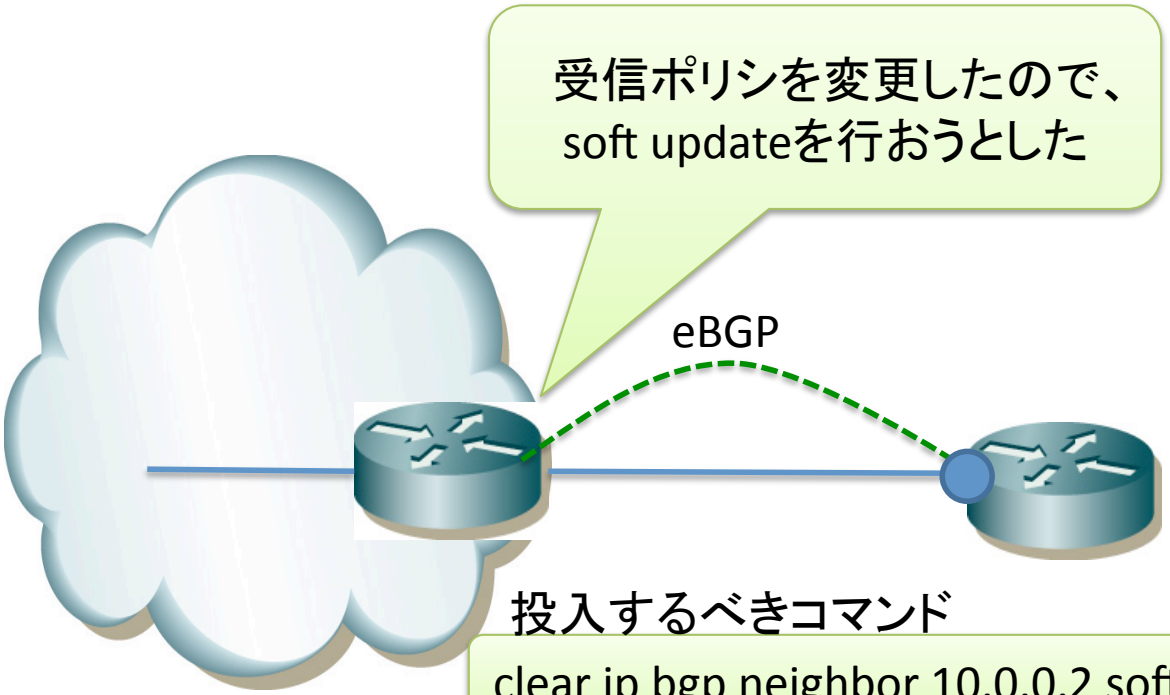
2009 (c) Internet Initiative Japan Inc.

No.11 BGP soft reconfiguration

- CiscoルータでeBGPピアの受信ポリシを変更したため、soft reconfigurationで経路を再評価しようとしていた
- コマンド投入時に、soft キーワードを忘れたため、BGPのピアがリセットされてしまった
- 不必要な経路のばたつきが発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.11 BGP soft reconfiguration



投入するべきコマンド

clear ip bgp neighbor 10.0.0.2 soft in

投入してしまったコマンド

clear ip bgp neighbor 10.0.0.2

eBGPピアがリセットし、
不要な経路のばたつきを
発生させてしまった

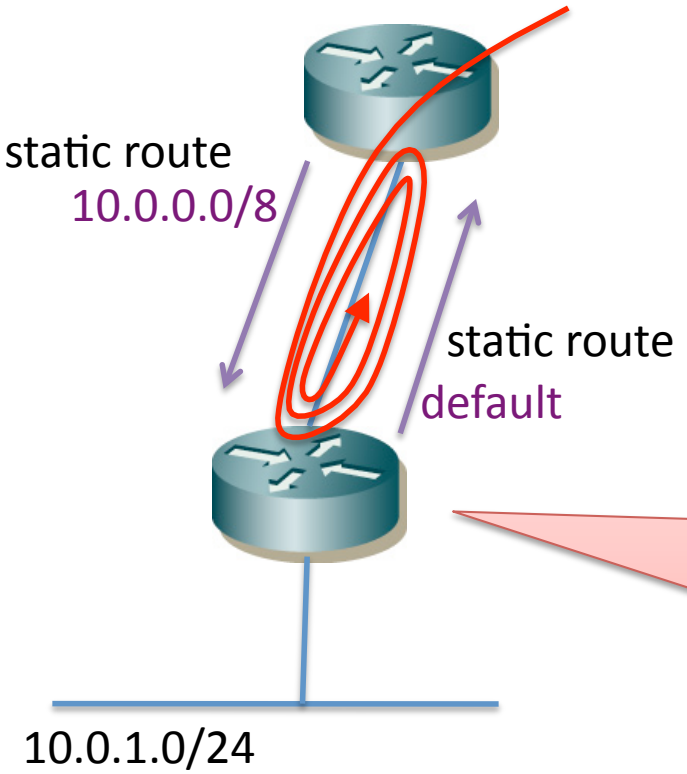
2009 (c) Internet Initiative Japan Inc.

No.12 経路の終端

- 上流向けにはdefault経路を設定し、上流からはstatic経路が設定されている環境で、向けられたネットワークの一部のみを利用していた
- 上流から向けられた経路のうち、利用していないネットワーク宛のことを考慮していなかったため、経路ループが発生していた
- ポートスキャンなどで、利用していないアドレス宛のパケットが届くと、上流との間でパケットがループして輻輳が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.12 経路の終端



上流から向けられている/16の内、/24しか利用しておらず、残りのネットワーク宛の経路をnullに落とすなどの処理を行っていなかったため、ここ宛のパケットが回線上をloopしてしまった

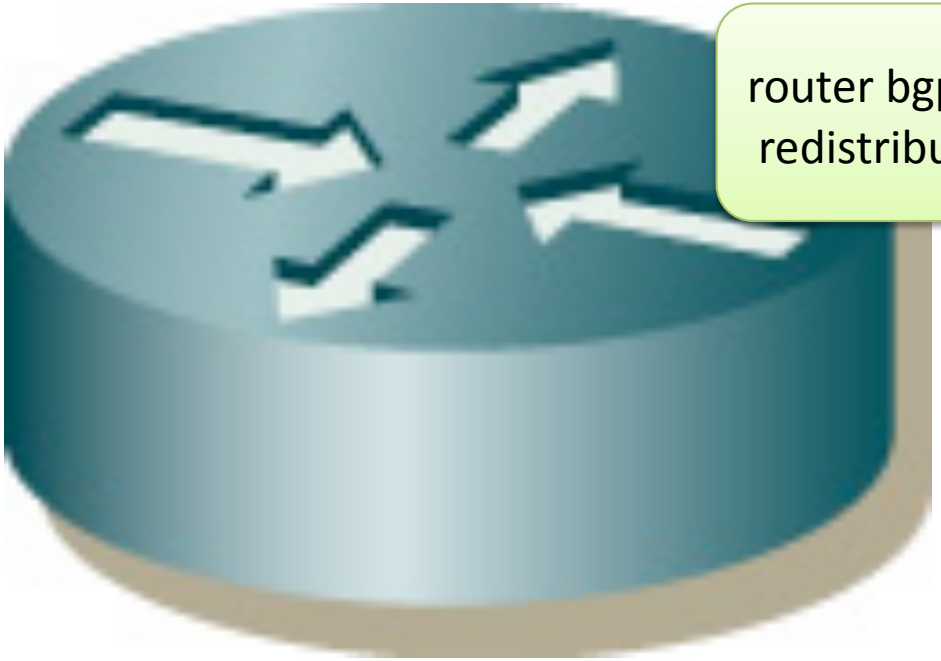
2009 (c) Internet Initiative Japan Inc.

No.13 redistribute

- OSPFからBGPにredistributeしているポリシを変更しようとした
- 設定変更時に、redistributeに適用しているフィルタが外れてしまった
- 意図しない経路がBGPで他ASに広報され、経路障害が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.13 redistribute



```
router bgp 2497
 redistribute ospf 2497 route-map ospf-to-bgp
```

設定変更中に不必要なOSPF経路までBGPに注入してしまい、意図しない経路制御になってしまった

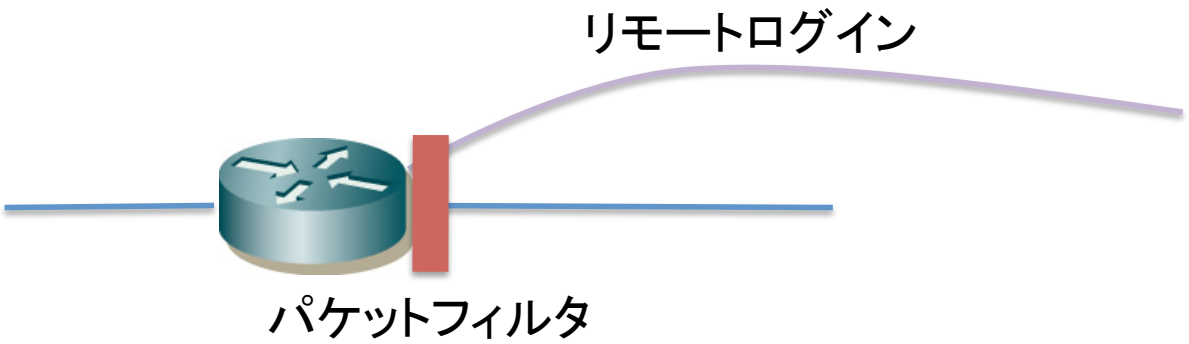
2009 (c) Internet Initiative Japan Inc.

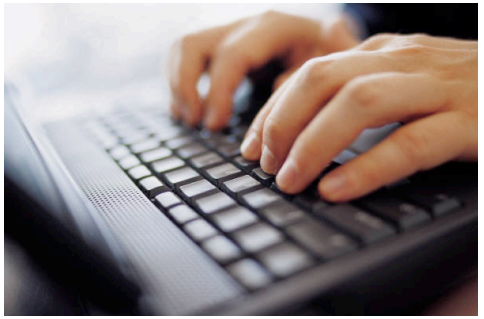
No.14 パケットフィルタ

- リモートのルータに、パケットフィルタを適用しようとしていた
- パケットフィルタにマネージメント用のルールを追加するのを忘れてしまった
- 適用直後から、リモートアクセスもフィルタされてしまい、操作不能に

2009 (c) Internet Initiative Japan Inc.

No.14 パケットフィルタ





リモートからパケットフィルタを変更している際に、自身のログインセッションもフィルタしてしまって、リモートからは制御不能になってしまった

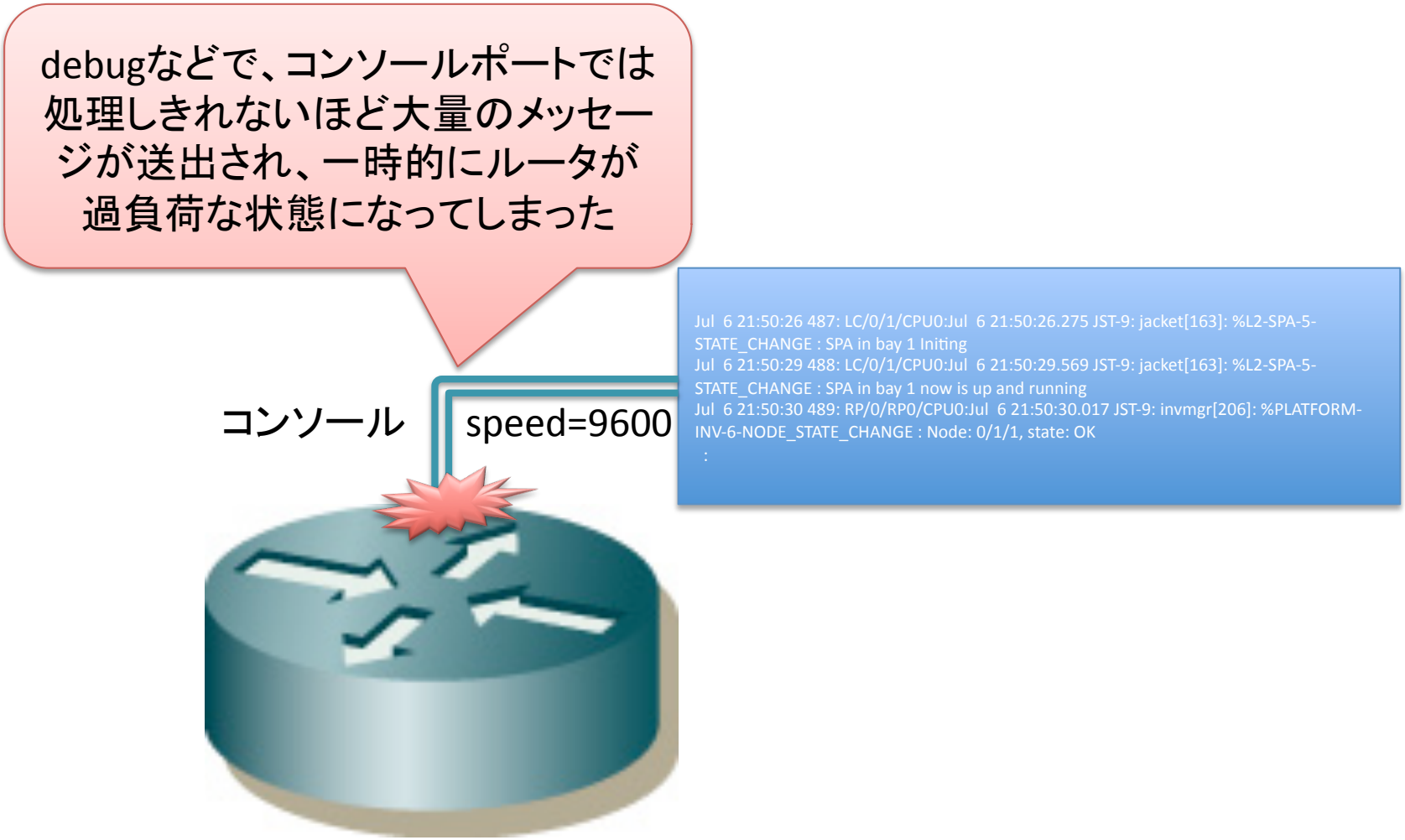
2009 (c) Internet Initiative Japan Inc.

No.15 コンソールロギング

- ルータのシリアルコンソールにもログメッセージを送信する設定になっていた
- デバッグなど、大量のログメッセージが発生する状況が発生してしまった
- シリアルコンソールが低速であったため、バッファにメッセージが滞留するなど、ルータが高負荷で不安定な状態になってしまった

2009 (c) Internet Initiative Japan Inc.

No.15 コンソールロギング



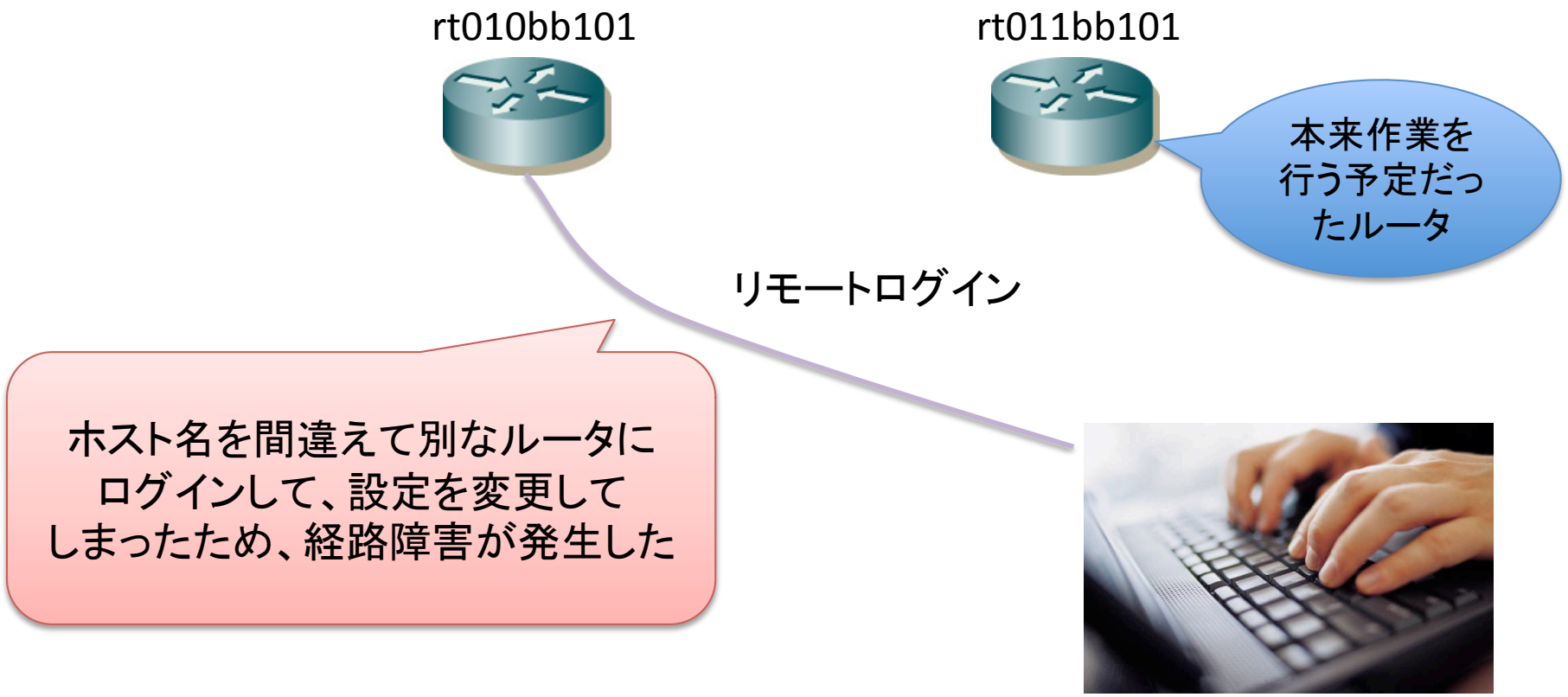
2009 (c) Internet Initiative Japan Inc.

No.16 ルータへのリモートログイン

- ホスト名を指定してルータにログインしている環境で、設定変更を行おうとしていた
- ホスト名を間違えて隣のルータにログインし、そのまま設定作業を実施してしまった
  - 同様の事例として、複数ターミナルを使用して作業中に選択するターミナルを間違う事例もあった
- 意図しないルータで設定変更が行われたため、経路障害が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.16 ルータへのリモートログイン



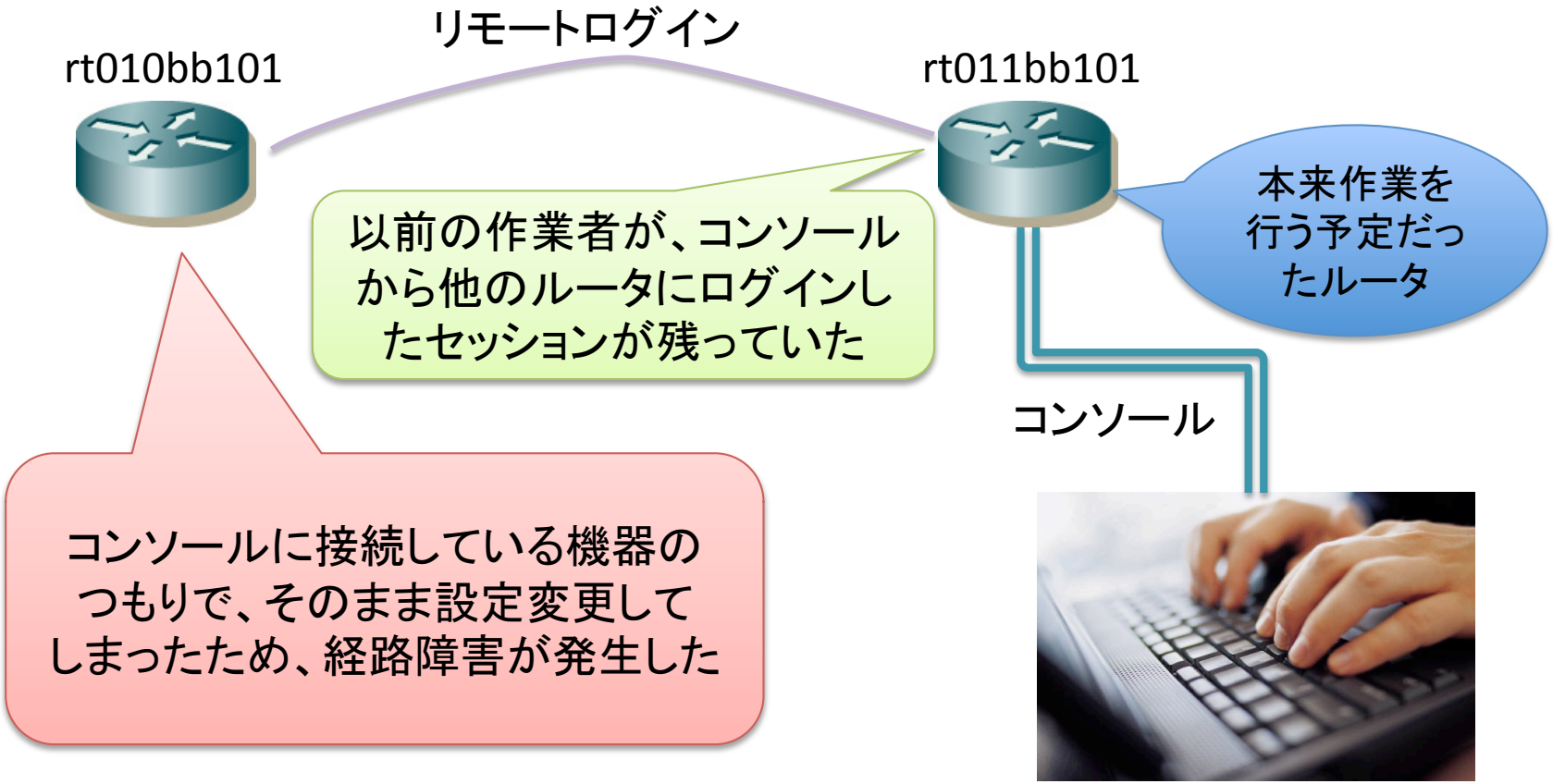
2009 (c) Internet Initiative Japan Inc.

No.17 シリアル経由のログイン

- ルータにシリアルコンソール経由でアクセスして設定変更しようとしていた
- そこには他のルータへのリモートアクセスセッションが残っていたが、それに気がつかず、そのまま他のルータを操作してしまった
- 意図しないルータで設定変更が行われたため、経路障害が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.17 シリアル経由のログイン



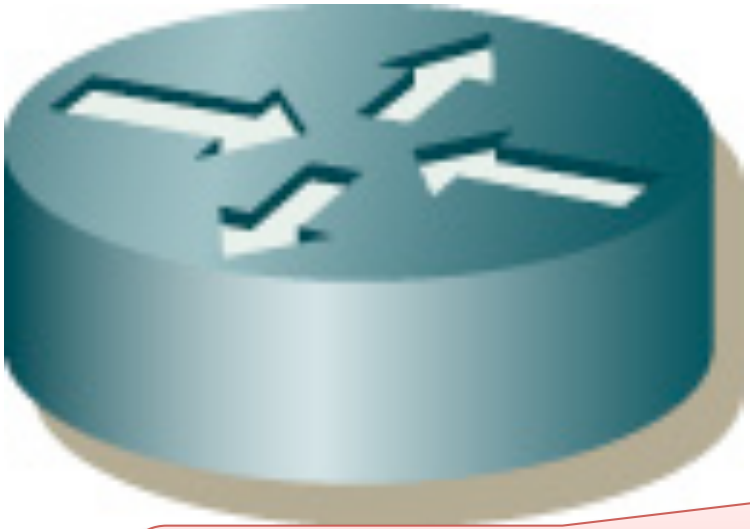
2009 (c) Internet Initiative Japan Inc.

No.18 設定削除

- Ciscoルータで不要になった経路設定を削除しようとしていた
- 消そうとする設定の前に順次 no をつけて設定削除していたところ、誤ってルーティングプロセスまで消してしまった
  - 例えば、no router ospf xxxx
- ルーティングプロセスが停止し、経路障害が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.18 設定削除



投入したかったコマンド

```
router ospf 2497
 no network 10.0.0.0 0.0.0.3 area 0
```

投入してしまったコマンド

```
no router ospf 2497
 no network 10.0.0.0 0.0.0.3 area 0
```

ルーティングプロセスが停止し、
経路障害が発生してしまった

2009 (c) Internet Initiative Japan Inc.

No.19 バグ踏み

- ちょっと違う状況、新しいファームウェア、新しい機能、たまたま叩いたコマンドなどなど
- 実網で使ってみたら意図と違う挙動になってしまった
- 通信障害など

2009 (c) Internet Initiative Japan Inc.

No.19 バグ踏み

2009 (c) Internet Initiative Japan Inc.

No.20 家庭から作業

- 家庭からルータにログインして、作業しようとしていた
- 「おとーさーん」と子供が後ろからぶつかって来た拍子に、ターミナルにpasteバッファを貼付けてしまった
- 幸い、設定変更や致命的なコマンドとは解釈されなかった

2009 (c) Internet Initiative Japan Inc.

No.20 家庭から作業

2009 (c) Internet Initiative Japan Inc.

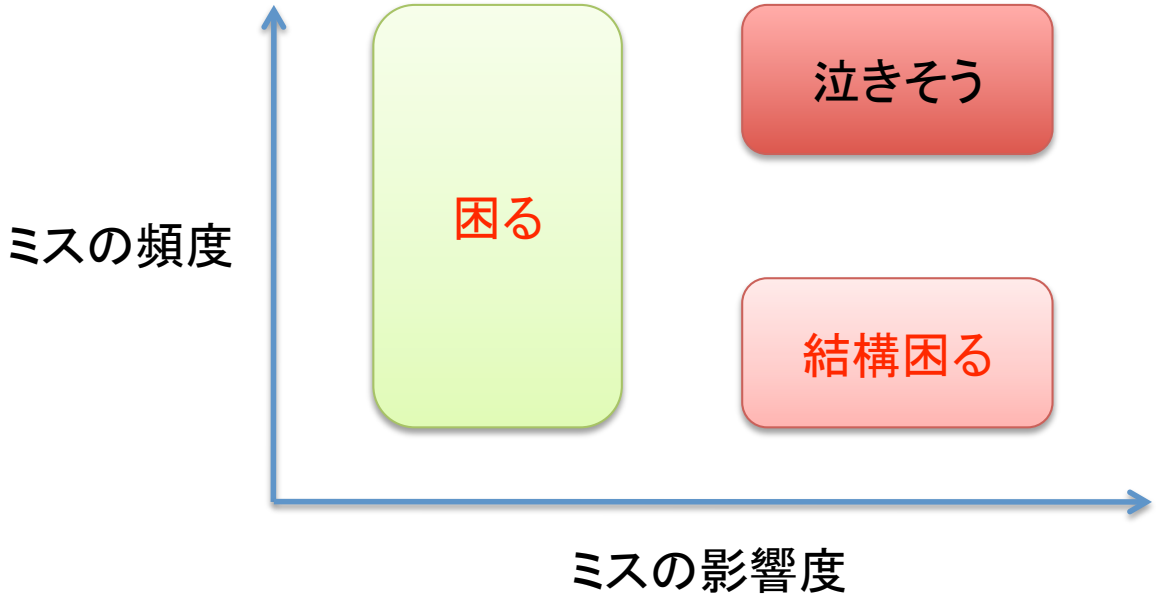
実現したいことは単純

- サービスの品質を守りたい
  - サービスの劣化に繋がる、あらゆる事象に対応
  - ミスもサービスを劣化させる一つの事象
  - 隙あらば、より良い品質を目指す
- ミスによる品質の劣化を最小限に抑えたい
  - 劣化が起きないなら、なお良し

2009 (c) Internet Initiative Japan Inc.

ミスへの対応

- ミスによる影響を減らす
- ミス自体を減らす



2009 (c) Internet Initiative Japan Inc.

ミスによる影響を減らす

- 保護
  - ミスの影響範囲を狭める
    - 多段の経路フィルタなど
- 回復
  - ミスを早期に検知する
    - ルータ設定やトラヒックの異常検知
  - ミスを適切に通知する
    - 作業を行っている人にミスだと知らせる
  - ミスから素早く回復する
    - 問題箇所を切り離したり、作業前の状態に復帰させる

2009 (c) Internet Initiative Japan Inc.

ミス自体を減らす

- ほとんどの場合、運用者がきちんと注意していればミスを防げる
  - 細かい原因を分類しだすと、きっと果てしない
  - なんせ人間難しい
- でも人間、そこまで完璧な訳じゃない

2009 (c) Internet Initiative Japan Inc.

ミスと人と注意力

- 何か、いけそうな仮定をおいてみよう

- 注意力には限度があり、人や状況で異なる
  - 注意力の範囲なら、ミスせずに作業ができる
  - 限度を超えると、ミスする可能性が高まる

2009 (c) Internet Initiative Japan Inc.

注意力に応じた運用方針

- 少数精鋭のみで運用
  - 特別対応も難なくこなせる
  - 運用者の負荷は高い
- 誰でもやれる様な運用
  - 運用者を支援する様々なシステムを用意する
  - 最小限の注意力でも効果的に運用できるように設計する

2009 (c) Internet Initiative Japan Inc.

現状を見るに

- まだミスは発生している
- つまり僕たちは十分な能力を持っていない

- 故に、ミスを減らすための支援環境が必要

2009 (c) Internet Initiative Japan Inc.

支援環境

- 必要最小限の作業で済む
  - 自動化、システム化
- 作業を明確にする
  - 手順化、定型化

既にみんな頑張ってる

- 注意を必要な箇所に集中させる
  - 良いユーザインタフェース
- ミスの影響を軽減する方策も実施

2009 (c) Internet Initiative Japan Inc.

考えどころ

- 運用者を取り巻く環境は変化し続ける
  - ネットワークの構成変更
  - 使用機器の入れ替え
    - ファームウェアのバージョンで書式が変わる場合も
- 支援環境も追従しないと、逆に運用の品質を劣化させてしまう

2009 (c) Internet Initiative Japan Inc.

というわけで

- やってしまったミス
- ミスを減らす工夫
- ミスの影響を減らす工夫

2009 (c) Internet Initiative Japan Inc.

他の事例研究など

- JR西日本 安全研究所
  - http://www.westjr.co.jp/security/labs/
- 失敗知識データベース
  - http://shippai.jst.go.jp/fkd/Search/
- 特定非営利活動法人　失敗学会
  - http://www.shippai.org/

2009 (c) Internet Initiative Japan Inc.

おわり

2009 (c) Internet Initiative Japan Inc.