インターネット経路ハイジャックの検知・回復・予防について

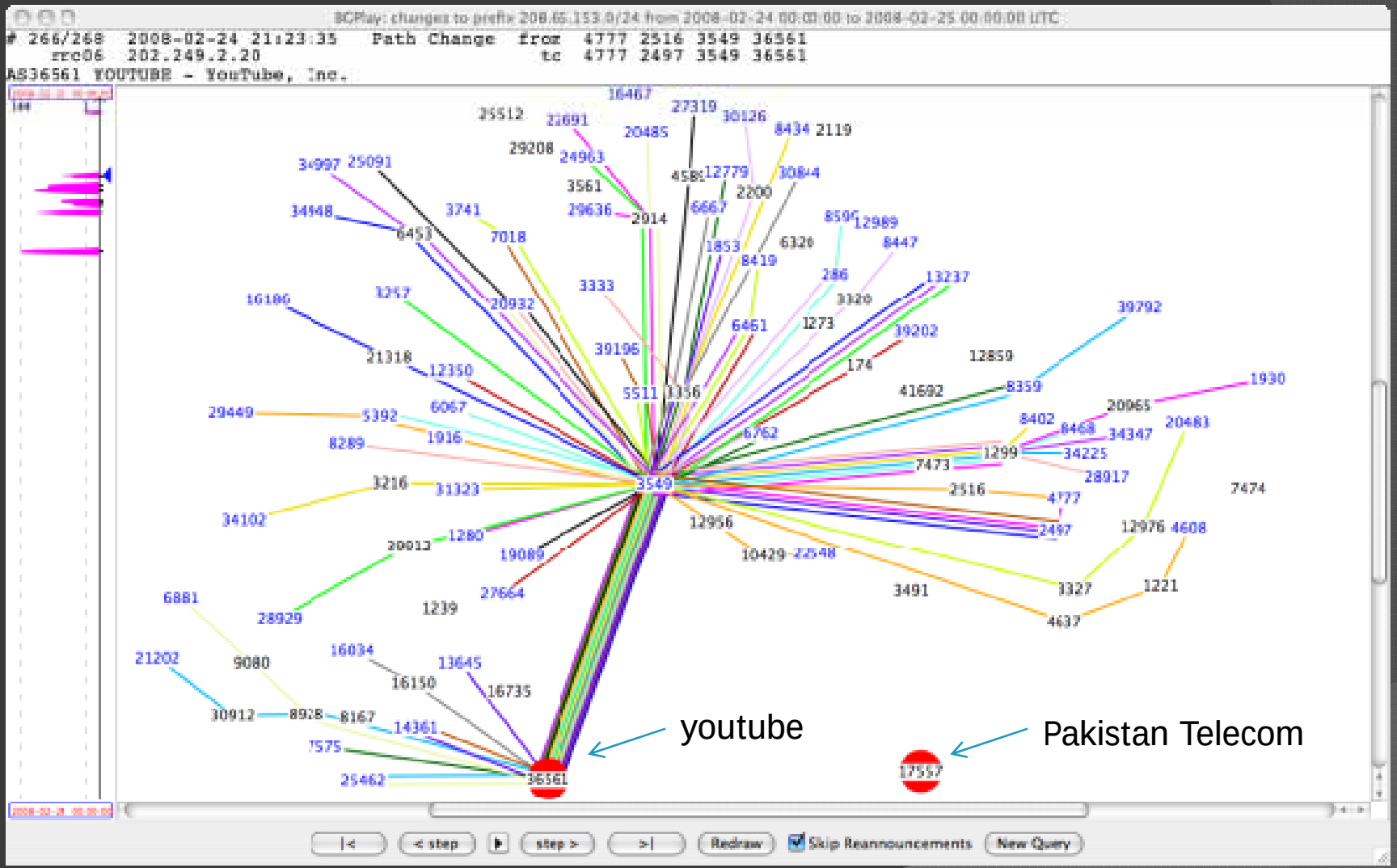
―あなたのネットワークは乗っ取られていませんか？―

Global IP Business Exchange
Feb. 2010

NTT Communications Corp.
先端IPアーキテクチャセンタ
ネットワークプロジェクト
担当部長　博士（工学）　宮川　晋

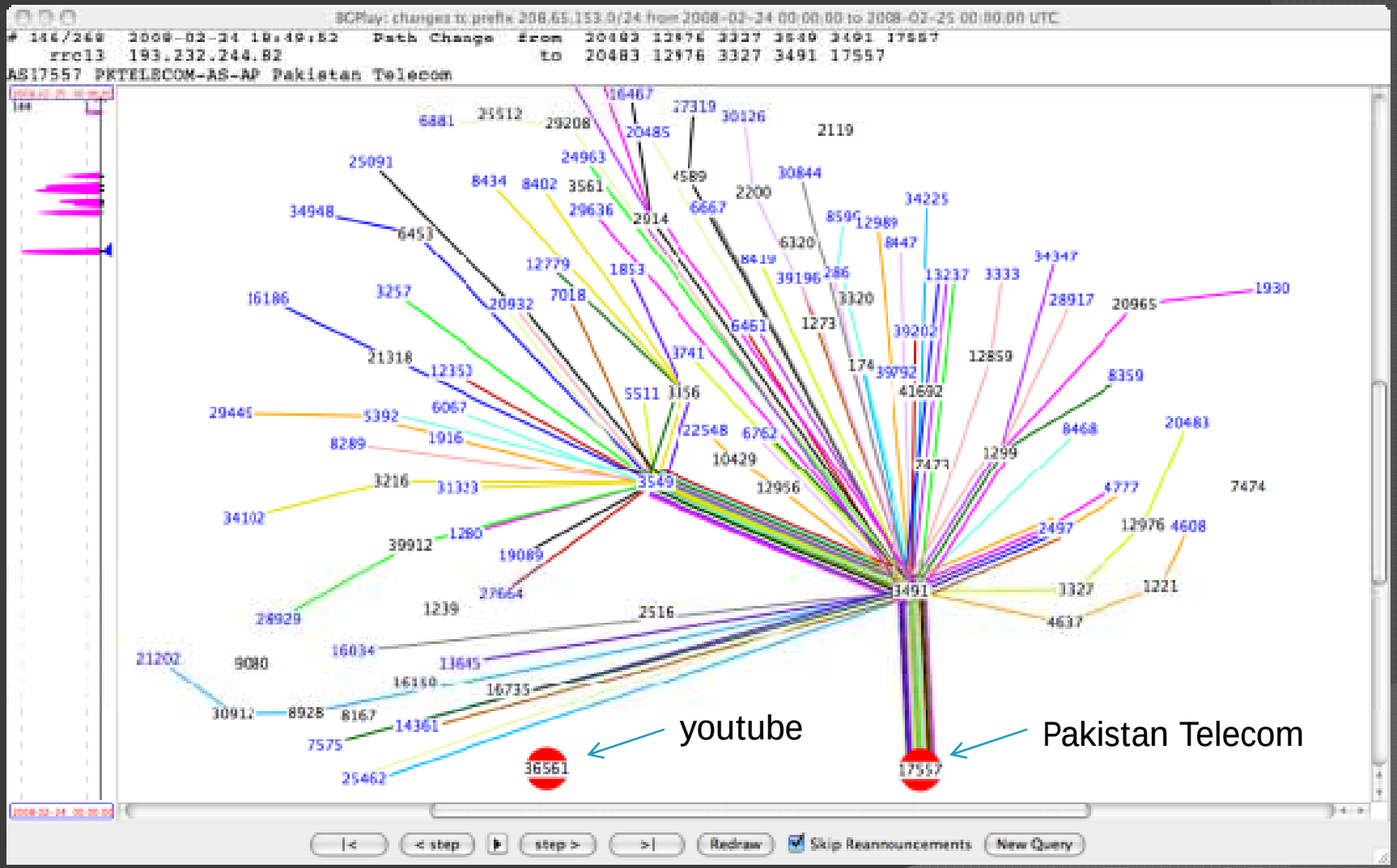
BGP Route Hijacking
- BGP経路ハイジャック -

通常状態のYoutube Feb.2008 当時



http://www.ripe.net/news/study-youtube-hijacking.html

youtube hijacked (Feb.2008)

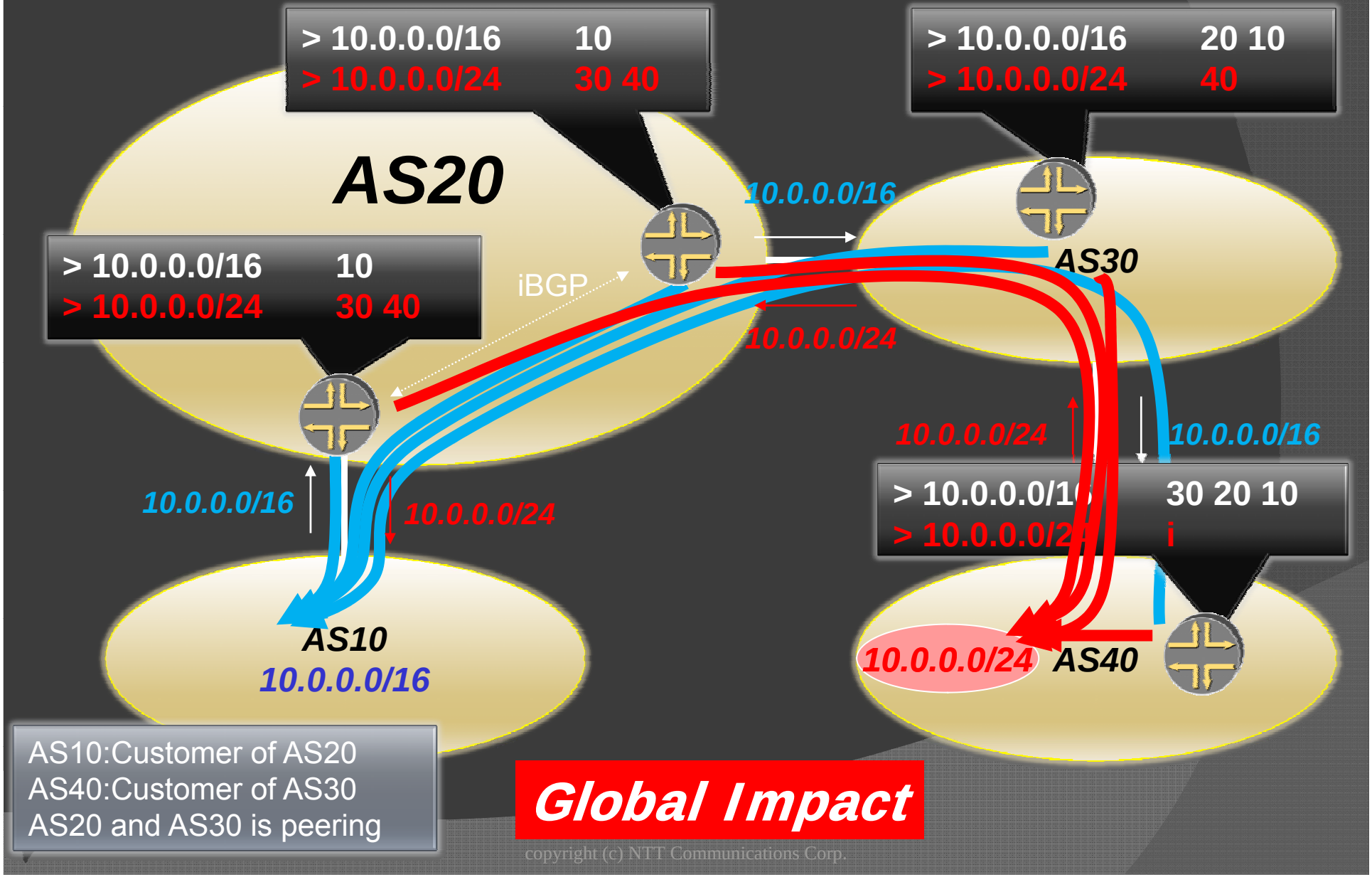


http://www.ripe.net/news/study-youtube-hijacking.html

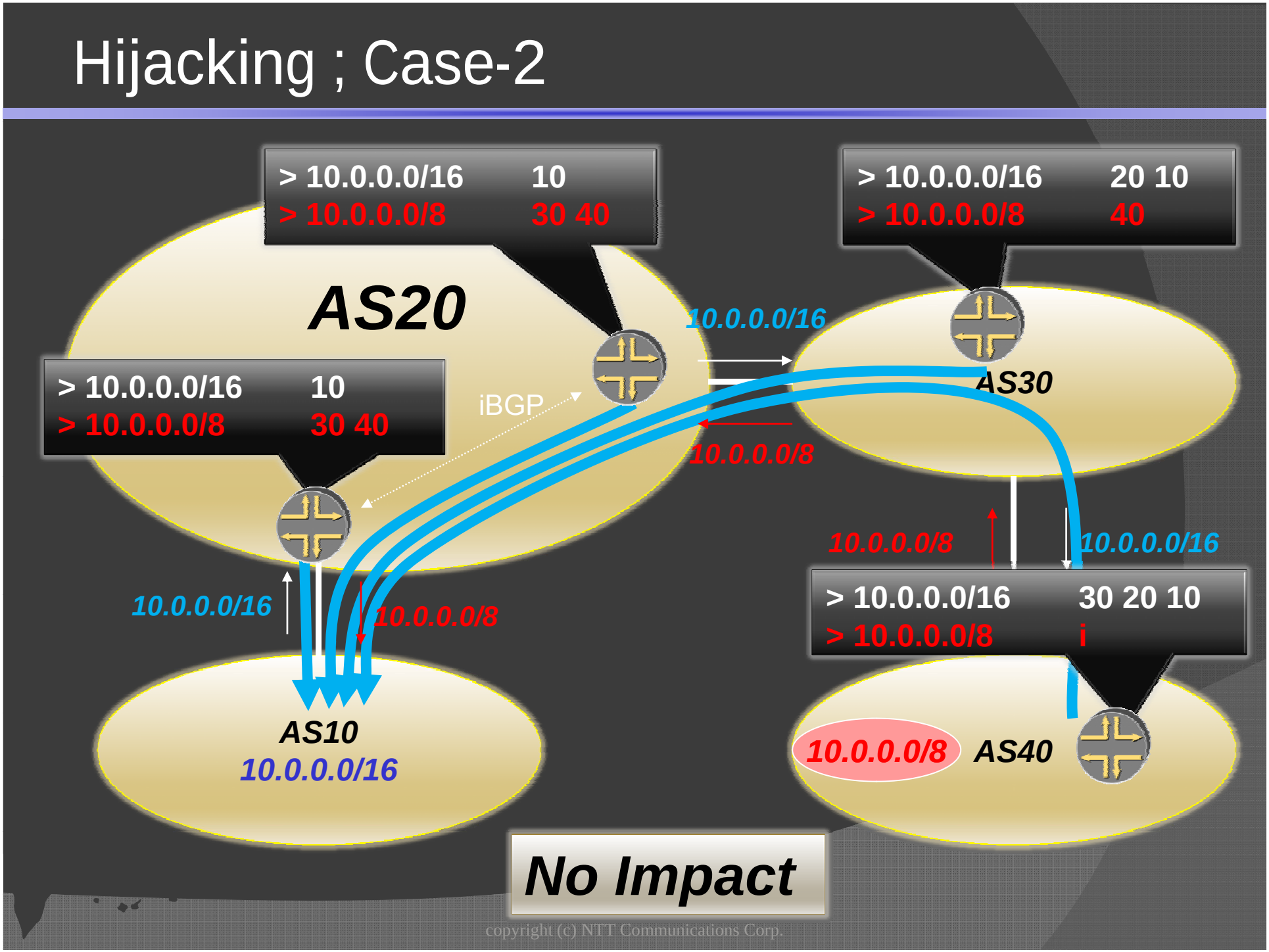
BGP Route Hijacking とは

- 不正なBGP経路広告がおこなわれて
- トラフィックが捻じ曲げられたり、到達不可能になったりすることです
- 検出は簡単ではありません
- 回復も簡単ではありません
- 頻繁におきてる、というわけではないですが、それなりにおきます
- 簡単に広がり、大きな影響が出ることもあります

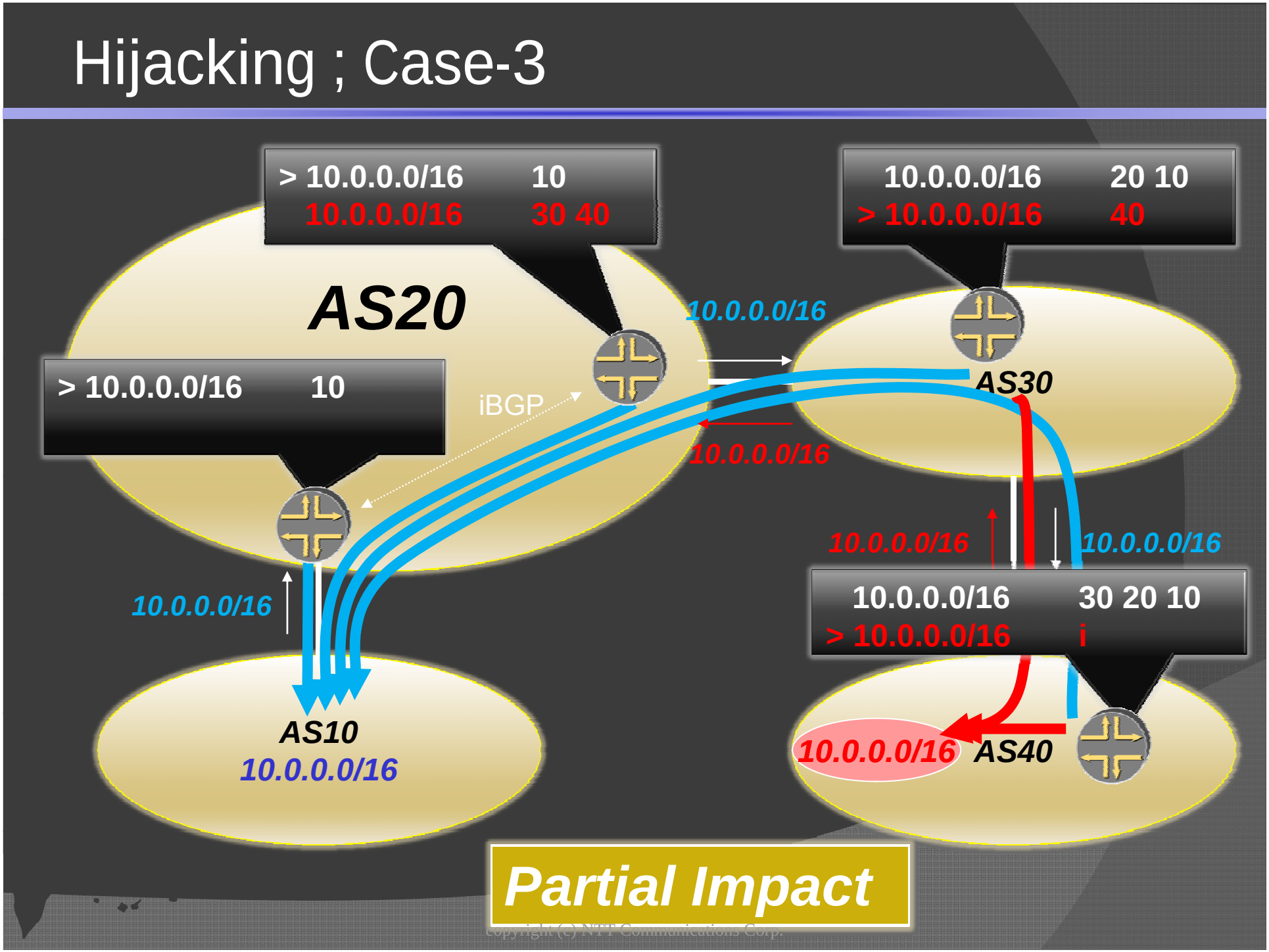
Hijacking ; Case-1



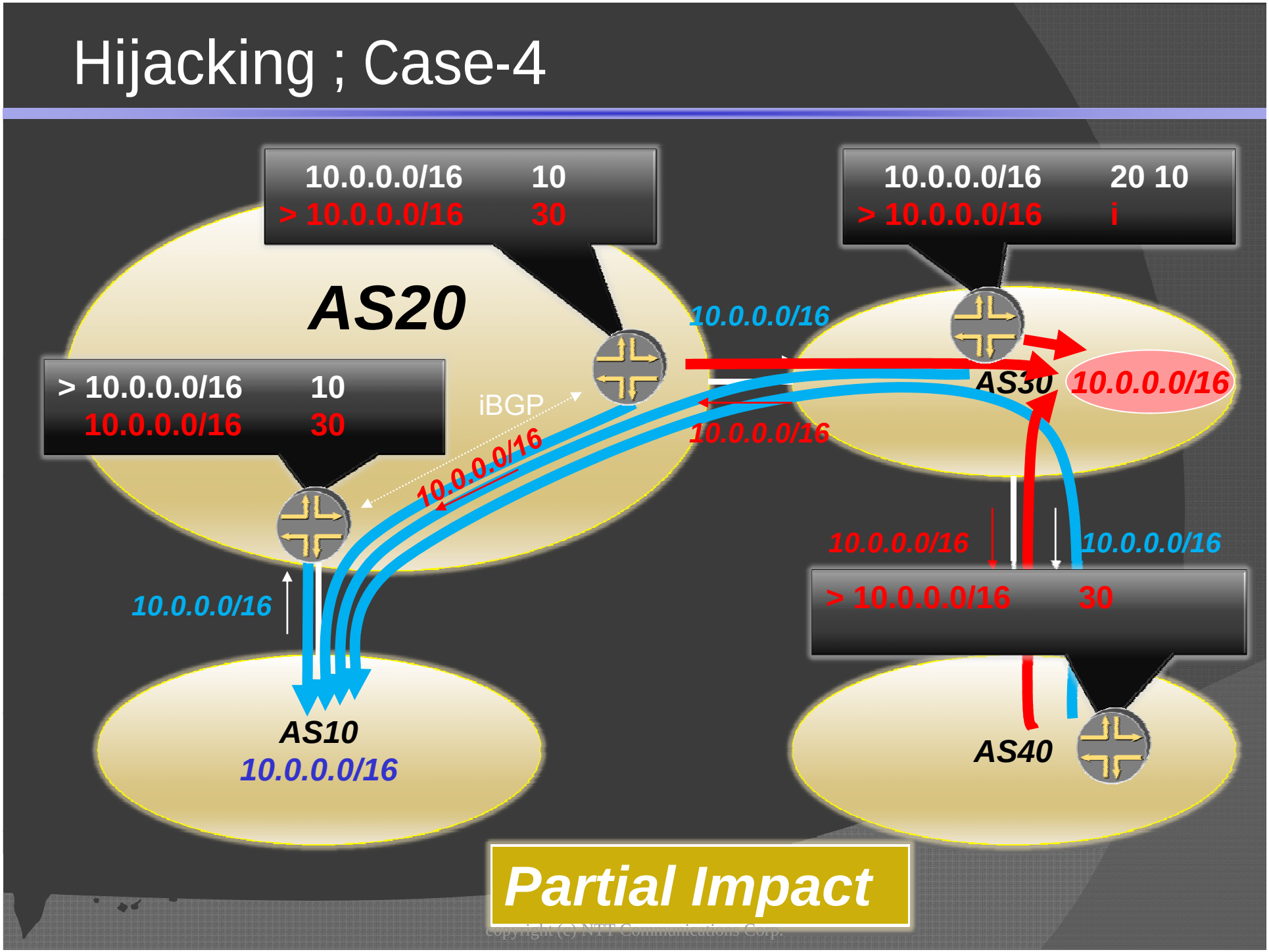
Hijacking ; Case-2



Hijacking ; Case-3



Hijacking ; Case-4



経路ハイジャックがおきると

- トラフィックがまげられるので
  - サービスができなくなったり、アプリケーション異常がおきます
  - たとえばDNSのRoot-serverのアドレスがHJされるととても…
- 意図的にやるとすれば…
  - トラフィックをねじまげて、パケットを記録
  - フィッシングやSPAMの送付
  - DoSアタックも
  - 他人になりすまして送受信することが出来る

経路HJの原因

- ほとんど意図しない設定エラーとおもわれる
  - コンフィギュレーションミス
    - フィルタのエラー（ローカルあるいはプライベート使用しているアドレスのもれとか…）
    - 単に書き間違いとか (wrong address/mask)
- もしも意図的なものだとすると
  - Spam/DDoS/Phishing…などを意図したIPアドレスの不正使用の可能性
  - Cyber Terrorismともいえる

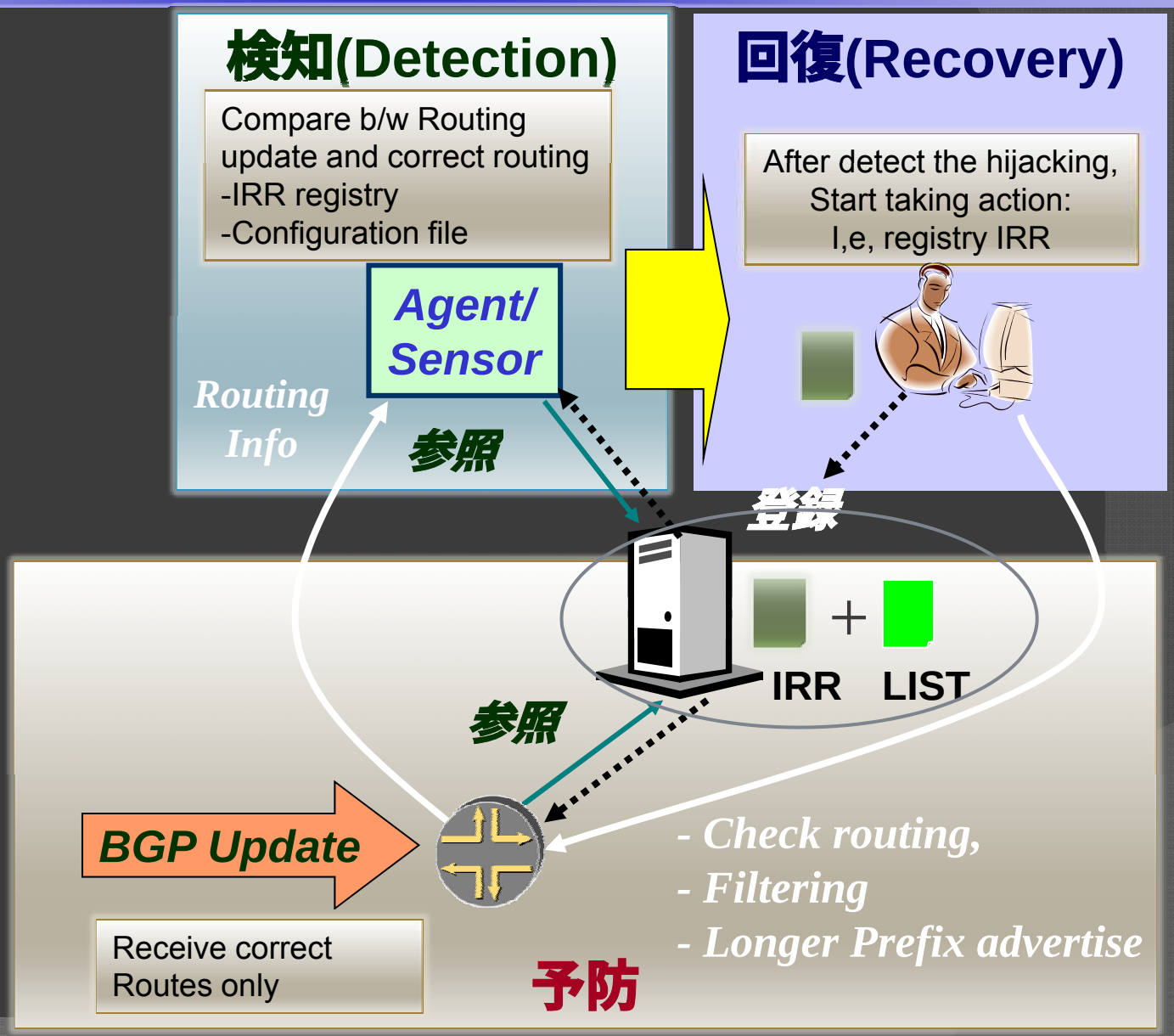
BGP経路ハイジャックへの対抗

日本におけるBGP経路ハイジャックに関する研究

- **日本国総務省による委託研究**
  - NTT Communicationsが主幹事
  - 4年間; 2006/6 - 2010/3
  - BGP経路HJの、検知・回復・予防技術の開発
- Telecom-ISAC Japan のBGP-WG
  - 日本国内のISPからのボランティアによる動き
  - BGP working group （2004～）

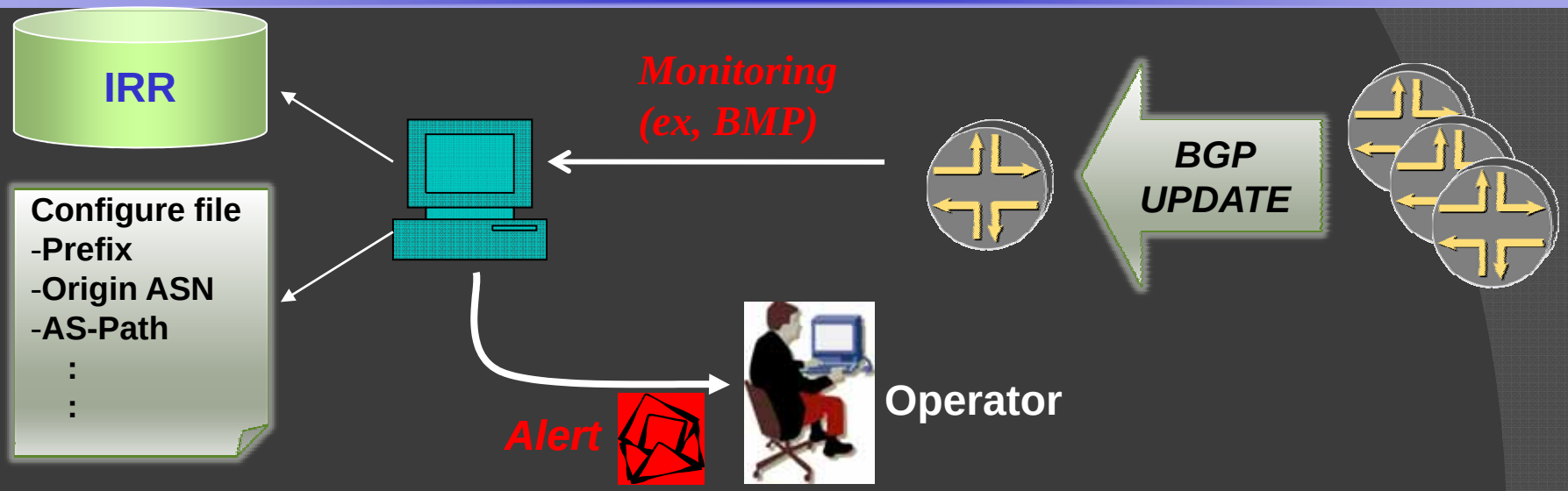
BGP経路HJ対策研究の概略

- 検知
- 回復
- 予防



検知 (Detection)

検知（Detection） system



- BGP updateを監視する
  - BGP　Updateメッセージによってやってきたアドレスprefix のAS_PATH属性の最後のAS番号と、IRRデータベースにorigin AS番号として登録されているものとを比較する
  - もしも違っていたらハイジャックを疑い、メールやSyslogや、SNMPトラップで警告する

世界の検知システム

- RIPE NCC MyASN Service
  - A part of RIPE NCC RIS (Routing Information Service)
  - Checking a prefix is announced with an incorrect AS path.
  - Alerting by email or to your own syslog server
- PHAS (Prefix Hijack Alert System)
  - UCLA
  - uses BGP data (with 3 hours' delay) from Oregon-Univ RouteViews
  - Checking origin, lasthop and sub-allocation set change
  - Alerting by email
- IAR (Internet Alert Registry)
  - Using PGBGP (Pretty Good BGP)
  - Alerting by email or search on the web
- ENCORE (an inter-AS diagnostic ENsemble system using OOoperative REflector agents)
  - NTT 研究所
  - インターネット上の多地点にエージェントをおき、経路を監視
  - メールよる警告
- 経路奉行（Route magistrate)
  - Telecom-ISAC Japan BGP-WG
  - local info (from IRR and manual maintain) とBGP UPDATEを比較
  - メールによる警告

日本で観察されたハイジャックの数

	2008						2009					
	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
# of detected ASes	15	15	15	15	15	15	15	15	5	5	12	15
# of Hijacks	0	0	0	14	1	0	2	0	0	3	0	0
# of Bogons	9	20	2	12	6	4	5	18	18	0	464	17
JPIRR ASes for detection	267	263	265	269	276	280	279	283	290	293	294	296
# of alerts except above detections of Hijacks/Bogons	2	3	19	4	1	4	0	9	14	2	1	1

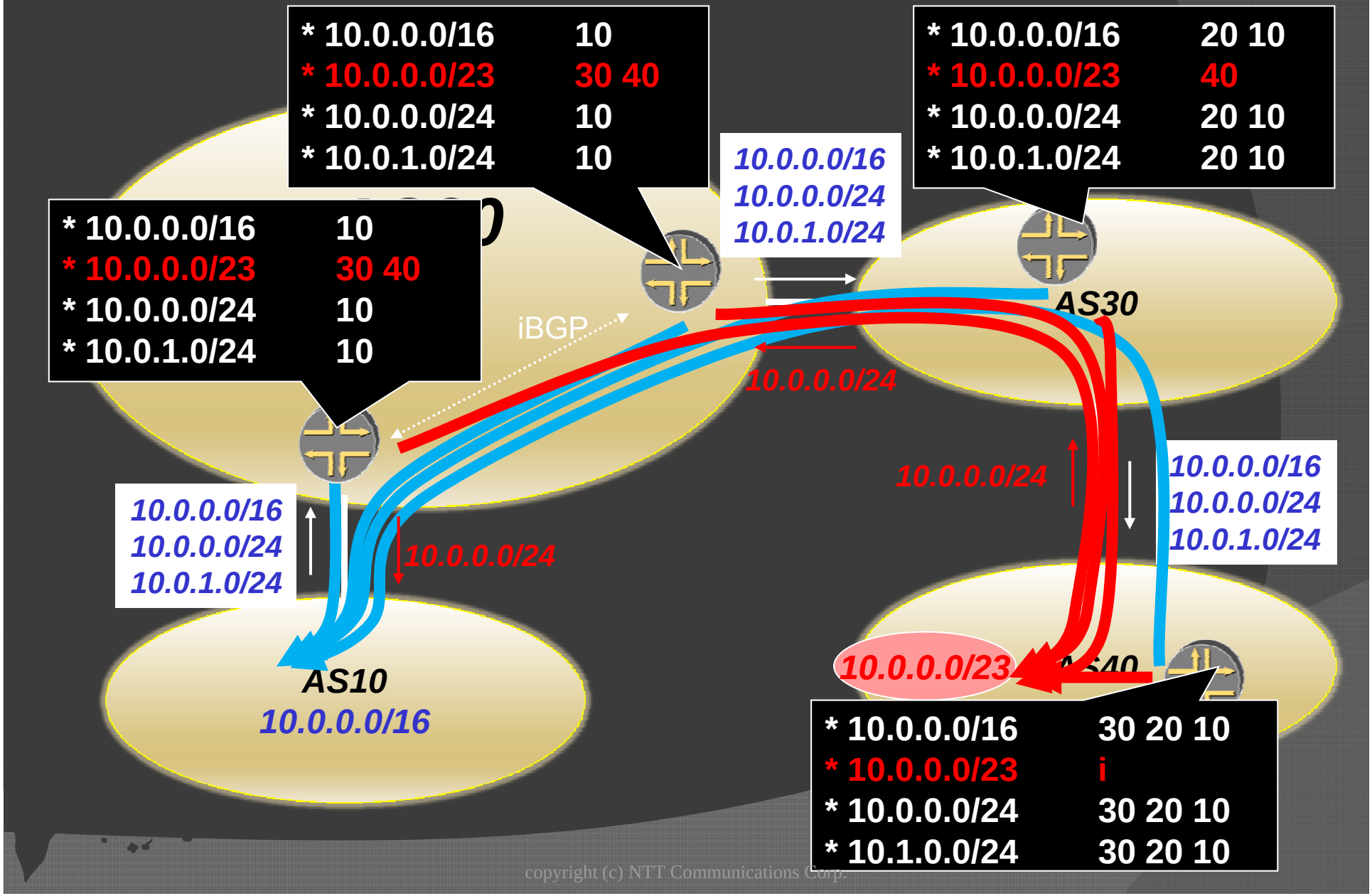
source: Keiro-bugyo / ENCORE project in telecom-isac JAPAN (15 ISPs)

回復 (Recorvery)

回復の仕方

- 影響の範囲を特定する
  - Global Impact? Partial Impact?
- いくつかの回復手法を試す
  - Hijackを引き起こしているASに止めるようにいう（恒久的な回復）
  - Hijack経路を伝播しているASにフィルタをかいてもらう (temporary)
  - より詳細な経路（BGPの性質上、詳細な経路のほうが優先的につかわれる）をアナウンスする (temporary)：「ハイジャック返し」

詳細なルートの再広告による回復



検知と予防 (実際のケース)

Real Hijacking Case (1)

- 2004/6
- Originated from Japanese ISP
- Longer prefix / Invalid origin
  - /24 x2, /25 x1, /29 x1
- Action
  - Contacted originated AS operator
  - Origin AS stopped invalid announcement
- Impact : about 150 minutes

Real Hijacking Case (2)

- 2004/9
- Originated from Asian ISP
- Longer prefix / Invalid origin
  - /24 x 2
- Action
  - Escalate peer ISP
    - Filtering on peer ISP
    - Origin AS stop announcement
- Impact : about 2 days

Real Hijacking Case (3)

- 2006/11
- Originated from *Asian* ISP
- Same prefix length / invalid origin
  - /17 x 2, /14 x 1
- Action
  - Not have been taken any action (Withdrawn soon)
- Impact : about 5 minutes

- By after analysis, we found this AS originated many other invalid routes at the same time

Real Hijacking Case (4)

- 2009/8 ; this year
- Originated from Asian ISP
- Longer prefix / Invalid origin
  - /22 x 1 ; dynamic pool address for Broadband user
- Action
  - Immediately Announce /23 x 2
  - Contact to ISP who originate the hijack route
    - Origin AS stop announcement invalid route
- Impact : about 1 hour

予防 (Prevention)

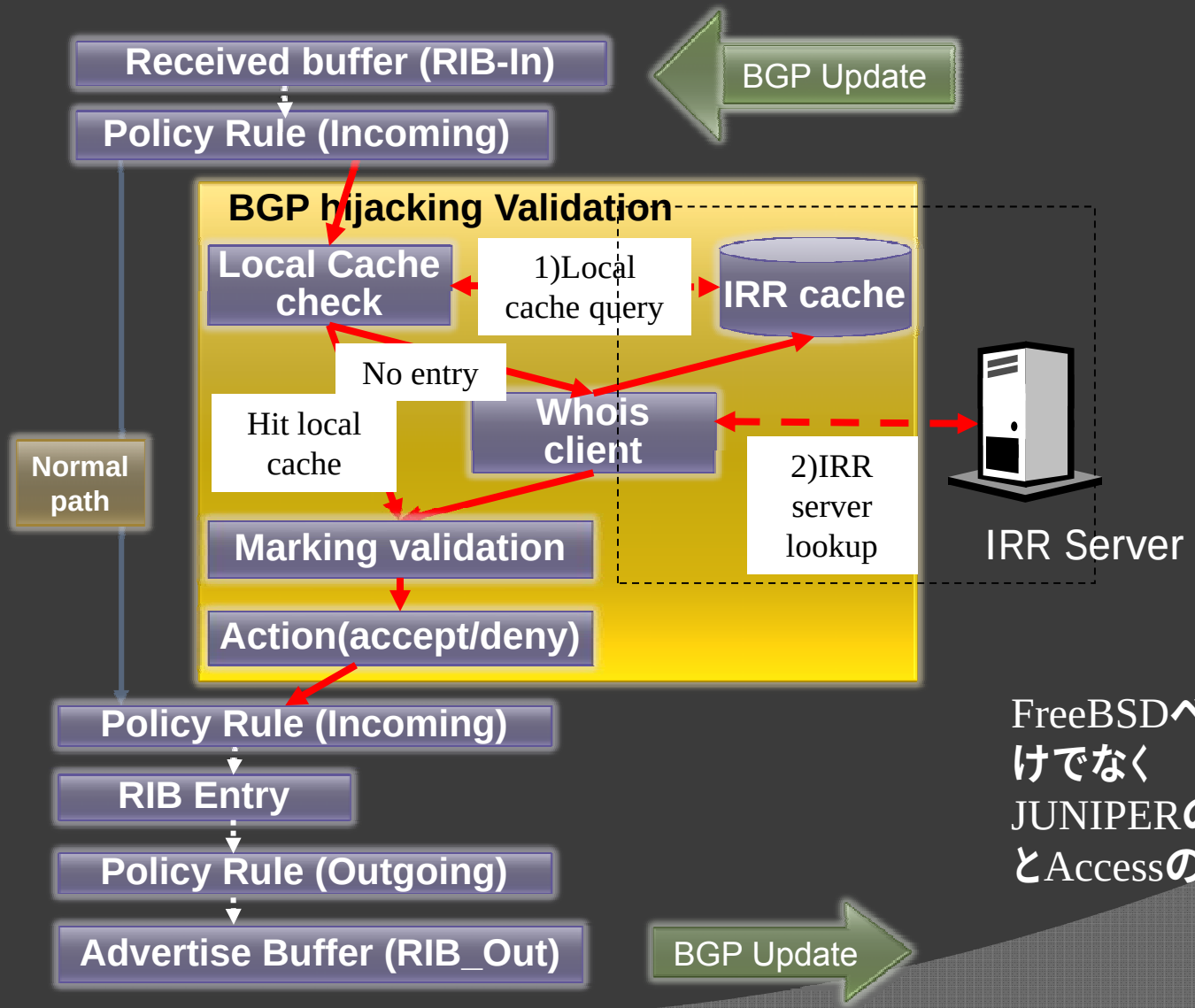
予防のためのKey Technologies

- 拡張されたIRRデータベースソフトウェア
  - 桁違いに速く、大規模で、なおかつ、電子署名つきのオブジェクトを扱えるように改造する
    - 電子証明のための正規形式を決める
    - High Availabilityと、ロードバランシングのために、データベースデュプリケーション機能を実装する
- 機能拡張されたルータ
  - ルータに拡張されたBGP機能をもたせる
  - E-BGP UPDATEが来るたびに、上記のIRRデータベースの中の署名されたオブジェクトと比較をおこない正当性を検証する

High Availability IRR ソフトウェアの開発

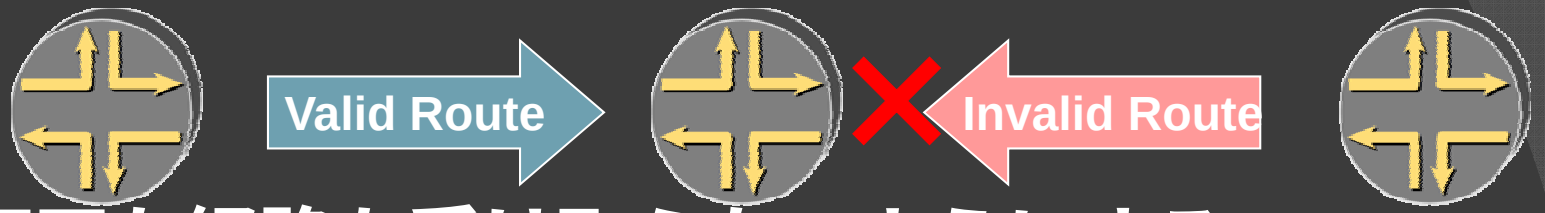
- 広くIRRDとしてつかわれているRIPE whois-server software をコアとする
  - 64bit CPU architectureサポート
  - Backend DB として、NDB Clusterを採用
  - SYNCER module (Redundancy, Radix Tree)追加
  - ダウンタイムの最小化
  - SQLのOptimization
- 我々は、RIPE NCCと協力し、いくつかの成果に関して、我々の開発したコードをオリジナルコードに組み入れる方向で調整が進んでいる
  - http://www.ripe.net/ripe/meetings/ripe-55/presentations/shirasaki-high-availability.pdf
  - http://www.ripe.net/ripe/meetings/ripe-56/presentations/Shirasaki-High_Availability_Software_Update_for_IRR.pdf

ルータ上の拡張されたBGPソフトウェア



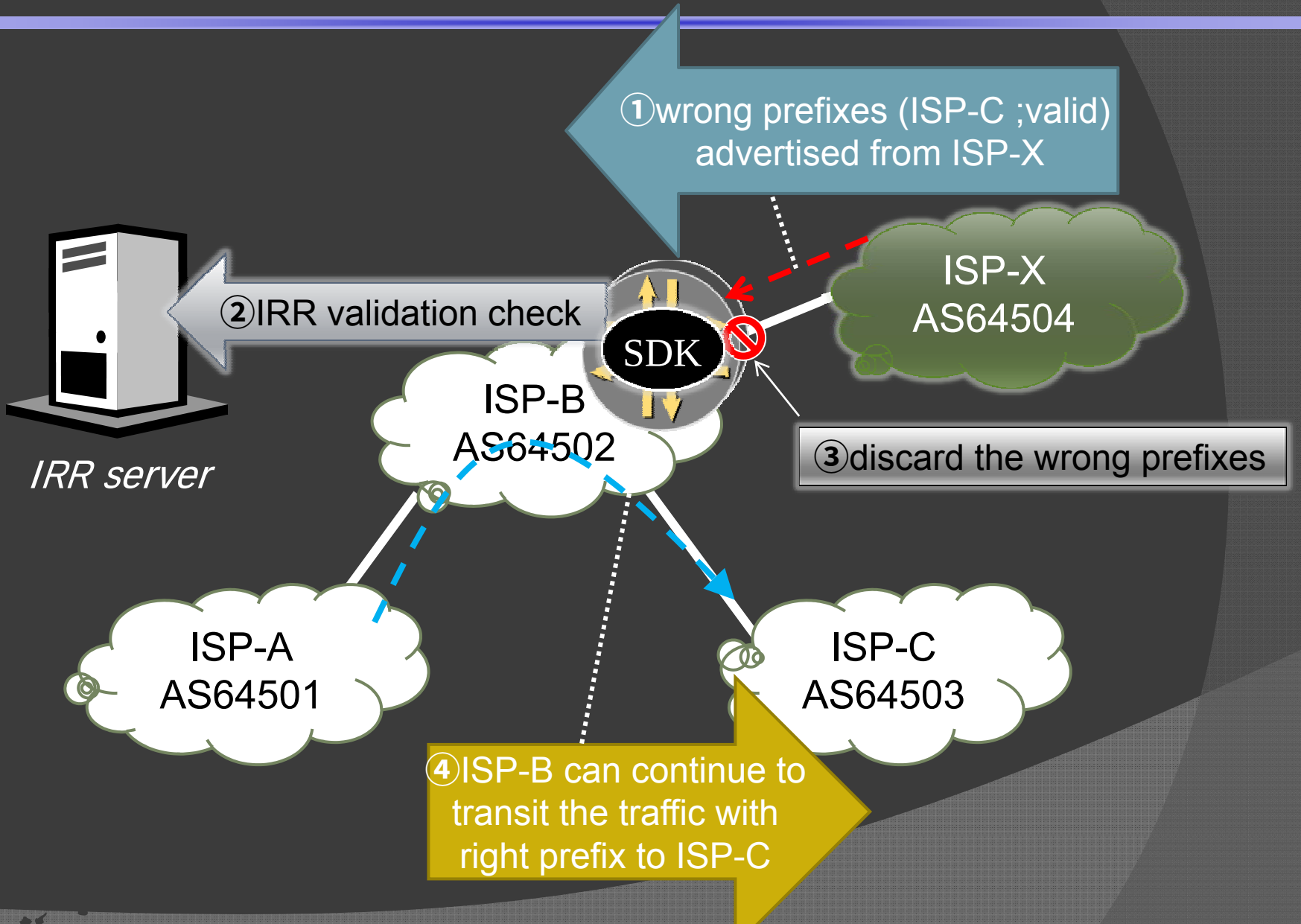
FreeBSDベースの手製ルータだけでなく
JUNIPERのSDKを使った実装とAccessのルータに実装がある

予防の考え方

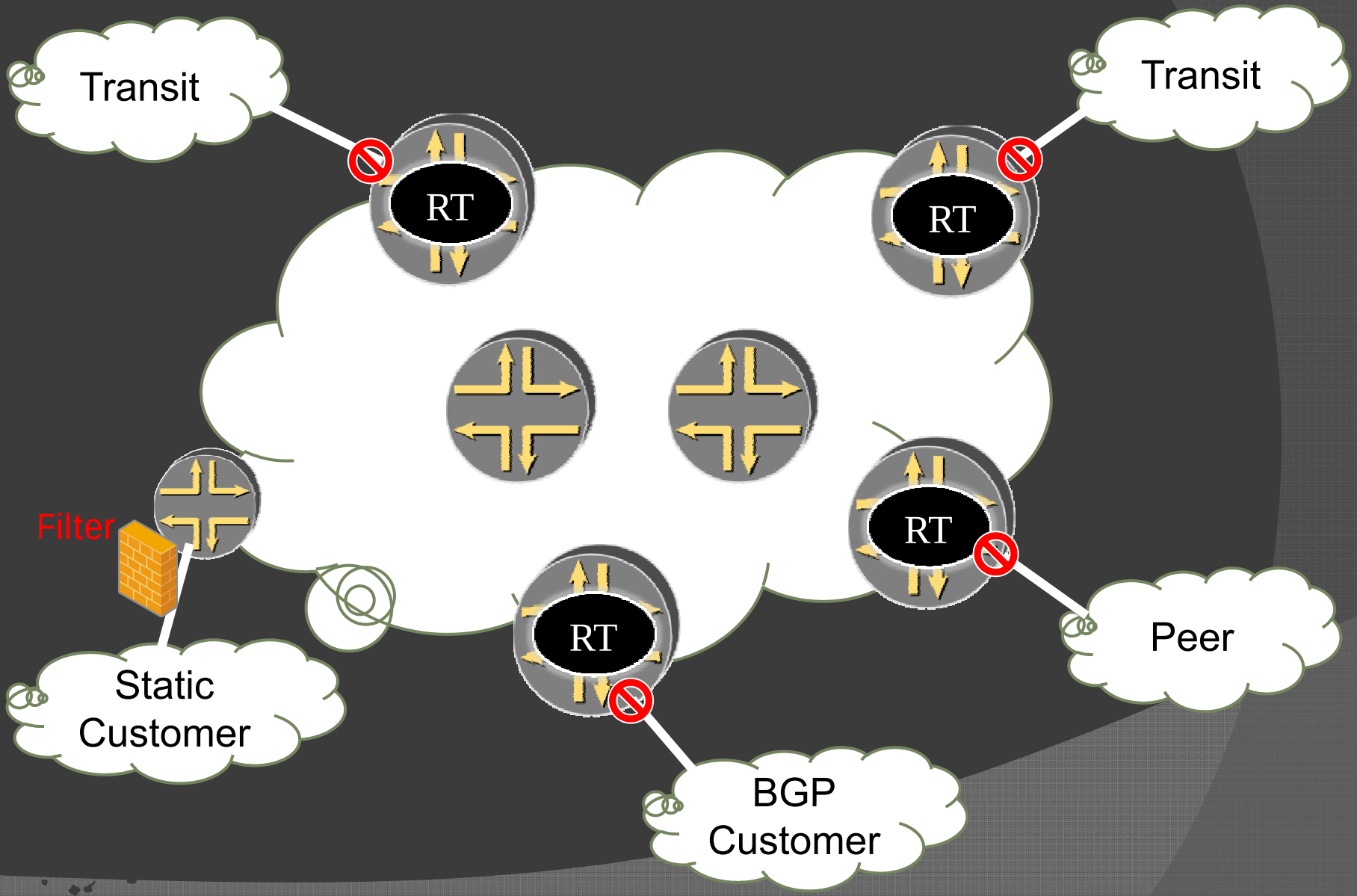


- 不正な経路を受け取らないようにする
  - どれが不正でどれが正当かを決めるようにする
- 二つのやり方がある
  - IRR base route validation :我々のやり方
    - オリジンASを保証する：完璧ではないが即効的で実際的
  - BGP base route validation :長期的にはこちら
    - オリジンASを保証し、かつ、BGPのPATHを保証する
    - sBGP, soBGP, pgBGP, psBGP
  - これらは背反しているわけではなく、共通のソフトウェアモジュールも使える

BGP経路ハイジャック予防



例えば大規模なISPのエッジに置けば・・・



結論

- BGP経路HJはそれなりに起きています
- NTTコミュニケーションズは総務省様からの予算を受け、検知システムを用意し、また、RIPEのWhois データベースソフトウェアの機能拡張を行い、商用ルータを含む参照実装をつくり、予防技術も開発しています
- NTT-Cは、他のISP様と強調して検知と回復の実験をするとともに、予防に関する実験も行いました
- 近い将来の実用化を目指して検討しており、また技術の公開もしております