IRS21

BGP Path Attribute
Optional Transitive Issues… again

2009年9月14日

河野 美也　Miya Kohno, mkohno@juniper.net

Agenda

- 問題は結構深い
  - History
  - 「世界をどう認識しているか」の問題
  - BGPは脆弱なのか
- 対処
  - 実装
  - 今後に向けて

History --- Optional transitive PA vulnerability

- **2007年12月 PATH Attribute==0**
  PA=0という、存在しないattributeを受信した時の動作

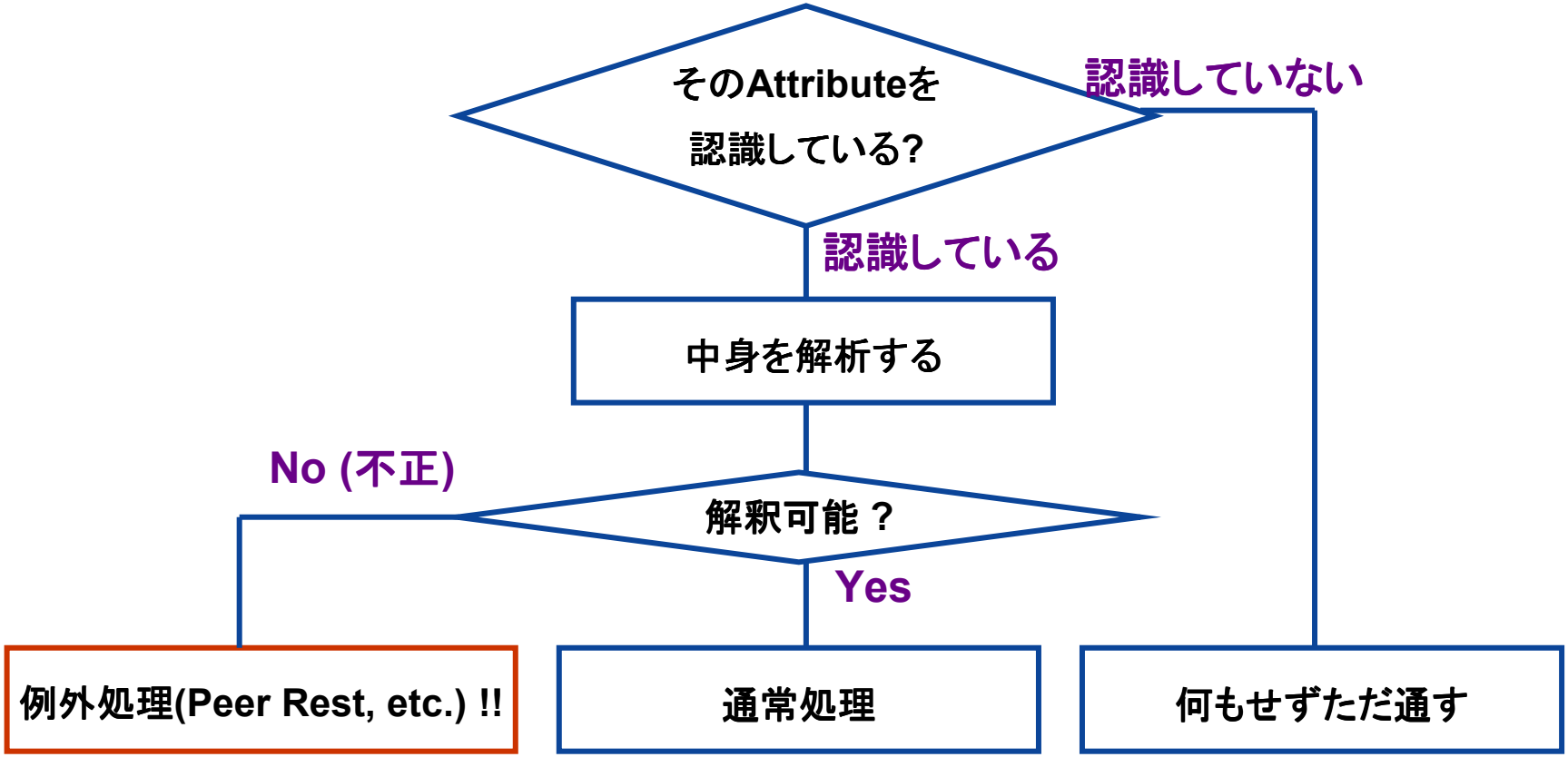
- **2009年2月 AS PATH too long**
  長すぎるAS PATHを受信したときの動作

- **2009年3月 AS_CONFED_SET/SEQUENCE in AS4_PATH**
  AS4_PATHには入るべきではないAS_CONFED_*を受信した時の動作
  → IRS19

- **2009年8月 AS4_PATH 0xE01100**
  不正AS4_PATH を受信した時の動作
  → IRS21(今回)

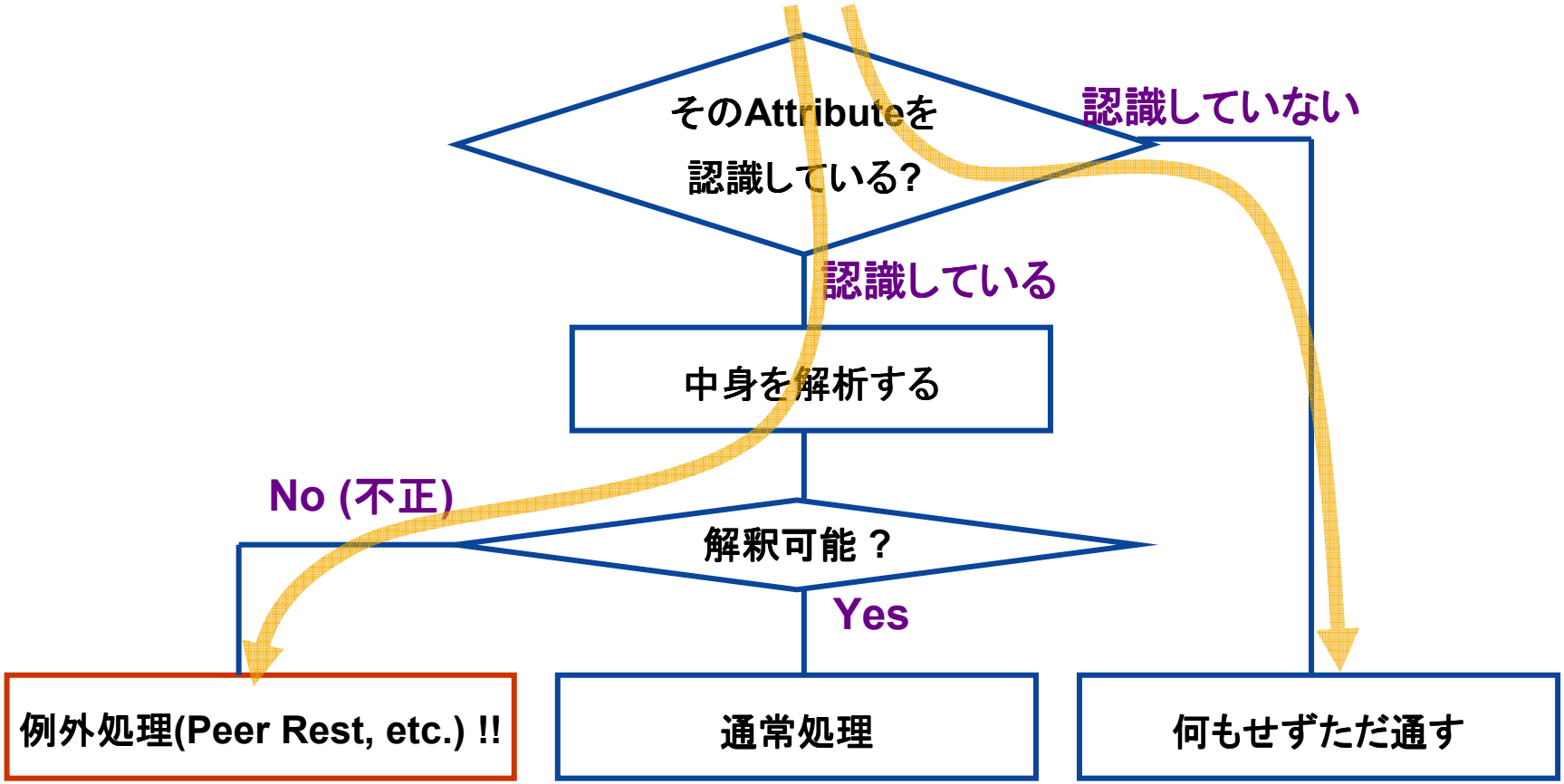
「世界をどう認識するか」の問題

それぞれのBGPスピーカーが、どう認識するか



「世界をどう認識するか」の問題

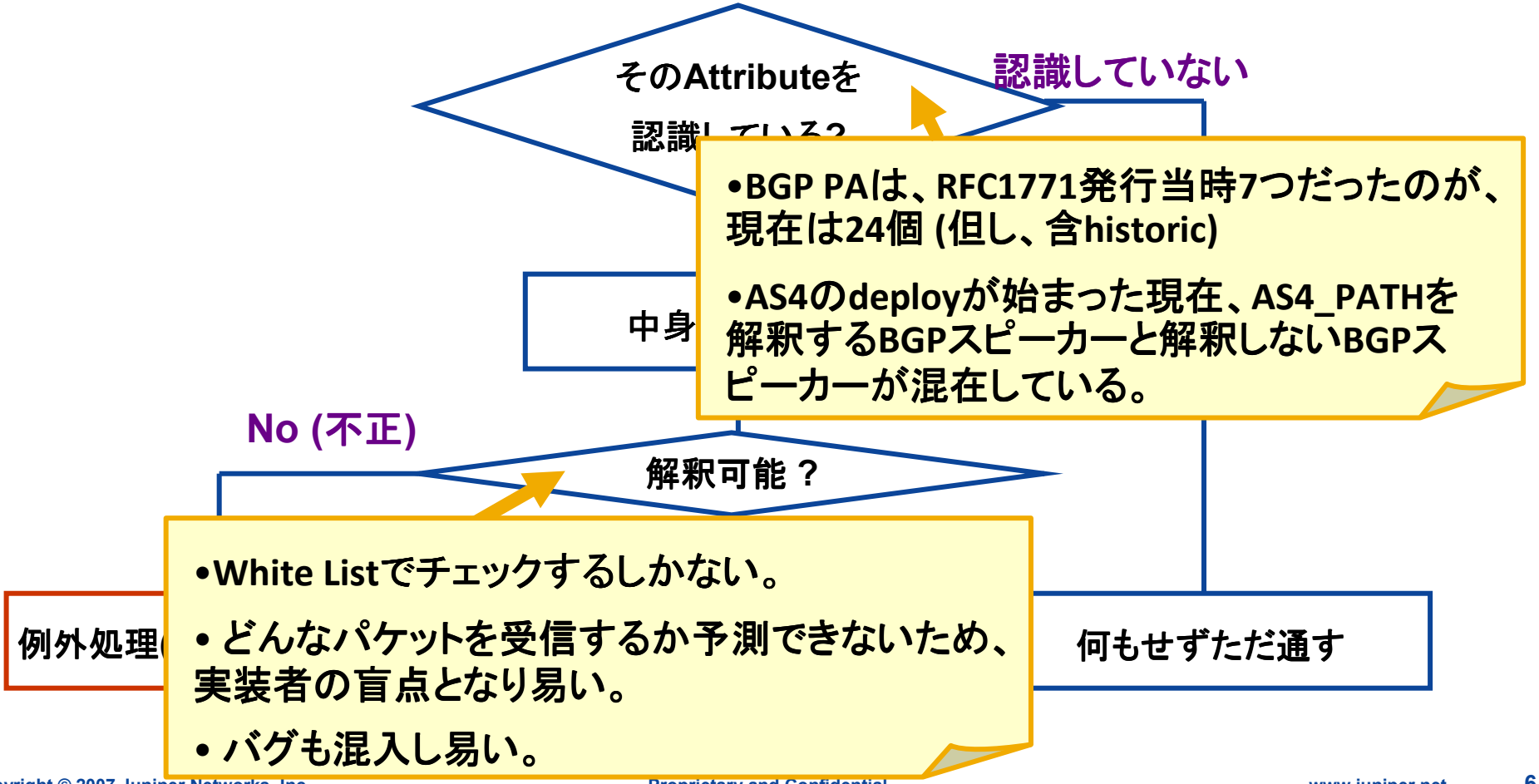
Malformedなパケットが到着すると、



ただ通すBGPスピーカーと、ピアを切るスピーカーが混在すると、remote attackになる。

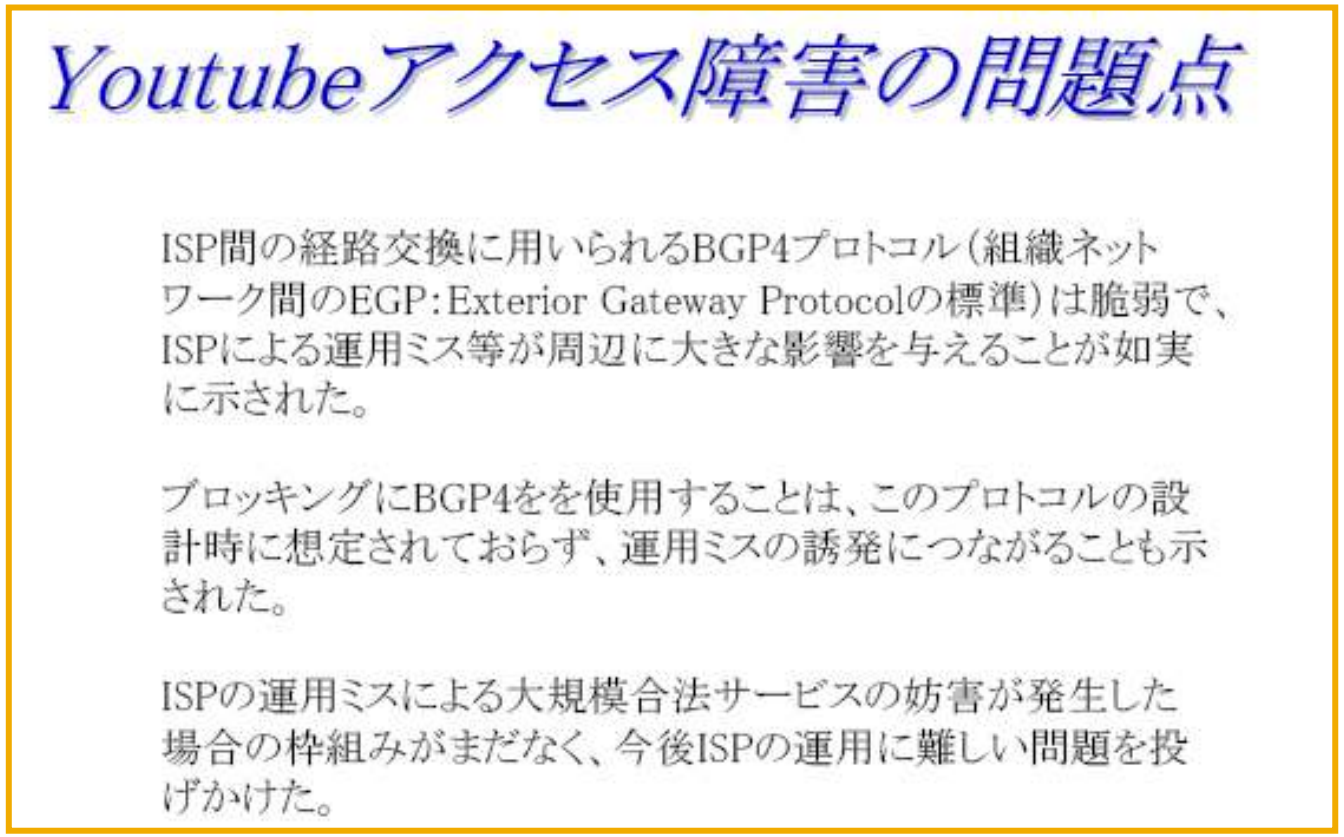
「世界をどう認識するか」の問題

「不確定環境」への適応問題 ！



BGPは脆弱なのか

「安心・安全インターネット推進協議会」資料より　http://www.scat.or.jp/stnf/



取り上げられているのは、運用ミスによるYoutube経路ハイジャック問題であるが、本質的には同じ。

BGPは脆弱なのか

…“Yes, it’s vulnerable. But it’s robust and evolving. “

- 各BGPスピーカーで「認識」、「解釈」が異なることが原因。
- しかし、
  - 4 bytes AS共存・移行のためには、Backward Compatibilityが必須。
  - 進化のためには、Diversityも必要。
- 必要な脆弱性であり、単に排除することはできない。乗り越えなくてはならない。

対処

- “Be liberal in what you accept, and conservative in what you send.“ - rfc1122 1.1.2 Robustness Principle
- しかし、ただ「切らなければよい」という訳ではない…。

- Malformed受信しても、Direct Peerでない場合は、Peer resetしないようにする。

draft-ietf-idr-optional-transitive-00.txt

(IRS19でご紹介した、draft-scudder…がWG documentになりました。)

Partial bit ONの場合、

- 受信したoptional transitive partial attributeがmalformedであった場合でもPeerはresetしない。

- 処理は、attribute種類によって動作が異なる。

JunOS実装

- **9.1より前**

  AS4 PATHに対応していないので、そのまま通過

- **9.1以降**

  draft-ietf-idr-optional-transitiveを、段階的に実装しています。まずは、P-bit付きの場合はPeer resetせずに、不正Attributeをstripします。その後の処理(Attributeにより異なる)については、まだ十分にdraft準拠ではありませんが(draftの方も、まだ変わる可能性もあり)、少なくとも、今回の件のようなmalformed attribute受信でPeer resetすることはありません。

今後に向けて

- 決定論的には扱えないけれども、
  (時々あるお問合わせ)
  - 「どのようなAttributeを不正と判断するか提示してほしい」
    → “無限定”なものを洗い出すのは不可能です。
  - 「Attribute解釈の仕様を提示してほしい」
    → 各ヴェンダー毎の、またはOS version毎の、Attribute解釈仕様の差は、そのままセキュリティリスクになります。
    → 仕様調査のメリットは何でしょう?
    今回のような不正attribute問題は、1）意図的、2）非意図的（バグやミス）に二分されますが、1）の場合は、仕様調査結果があった方が起こり易いし、2）の場合は予測不可能なので、仕様調査結果があったとしても、予防することは困難です。

今後に向けて

- 関係者の叡智で、適応・進化させることはできる。
  - 予期しないことは起こり得る。
  - しかし、状況を分析しながら、proactive/reactiveに対処することは可能。
  - JUNOS 9.4 show bgp statistics より ☺

```
4 Byte AS statistics

--------------------

inbound_merges          12620
outbound_splits         7729283

cache_hit_old_spkrs     10004672
cache_hit_new_spkrs     3664371

as4path_confeds         0
as4path_confed_errors   0

as4path_out_confed_drops 0
too_big_messages        0
```