



RFC7606 Revised Error Handling for BGP UPDATE Messages

Shishio Tsuchiya

shtsuchi@arista.com

JANOG56 LTにて

採用プログラム

LT1: BGP malformed update/attribute list

発表者

土屋 師子生(アリスタネットワークスジャパン合同会社)

発表概要

NANOGのメーリングリストで2025年5月20日不正のBGPアップデートによるBGPのセッションリセットが観測されたとの報告があった。
RFC7606 Error Handling for BGP UPDATE Messagesは2015年に改定されたRFCであり、多くの機器で実装されているが、なぜこんな現象が起こったのか。NANOGメーリングリスト,Blog <https://blog.benjojo.co.uk/post/bgp-attr-40-junos-arista-session-reset-incident>
メーカーの情報よりまとめてみました。

応募資料

[BGP malformed update/attribute list](#)

採点結果

有益性: 22(平均 4.4)

話題性: 23(平均 4.6)

明瞭性: 22(平均 4.4)

Total: 67(平均 13.4)

トップ選考!!

そもそもの目的

- ・ BGPの不具合があった
- ・ 社内でも世界でもそこそこ話題になった
 - 日本でも2-3個？
- ・ 早めに多くの目にふれる場所で公開したほうが良いと思った
 - EOSのRFC7606 Revised Error Handling for BGP UPDATE Messages対応について
- ・ プログラムは締め切られてるのでLT
- ・ 難しい問題ではあるけど伝わるか....

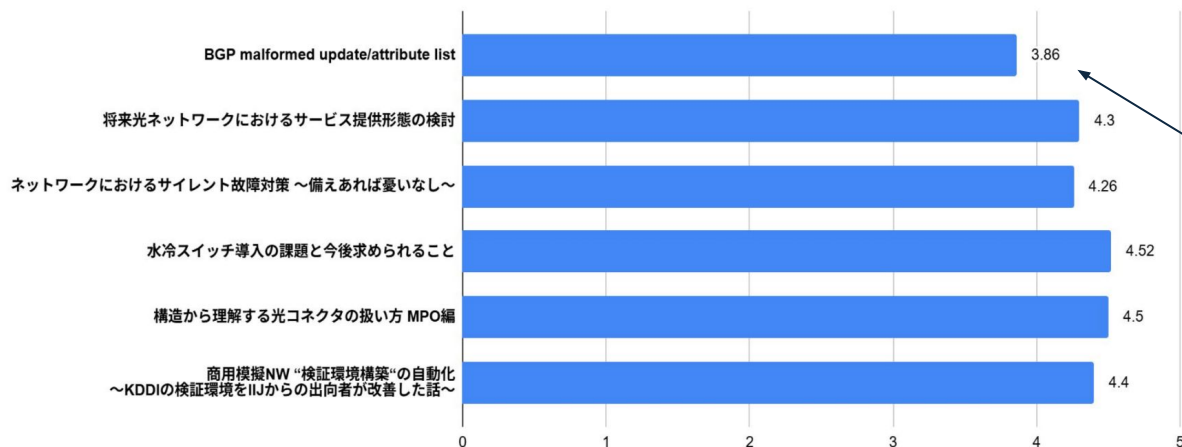


アンケート結果

https://www.janog.gr.jp/meeting/janog56/wp-content/uploads/2025/08/JANOG56_SurveyResults.pdf

JANOG
56

[Day3] ライトニングトーク



ダントツに悪い



42

アンケート結果

https://www.janog.gr.jp/meeting/janog56/wp-content/uploads/2025/08/JANOG56_SurveyResults.pdf

LT1: BGP malformed update/attribute list

ベンダーの方が他社を貶めるような内容に見えたため不快である。運用者など中立的な立場の方が解説すると見え方が良いと思う。

LTという質疑応答やコメントをすることができない形態の発表で、他社の製品についてネガティブとも取られかねないような意見を一方的にコンペティターの立場から喧伝するようなセッションをする、またANOGとしてそれを許容するのはいかがなものかと思う

- 点数悪いのは良いけど、悪さがなんか違う
- どちらかというと自虐...
- ベンダーの方って発言しちゃいけないの？



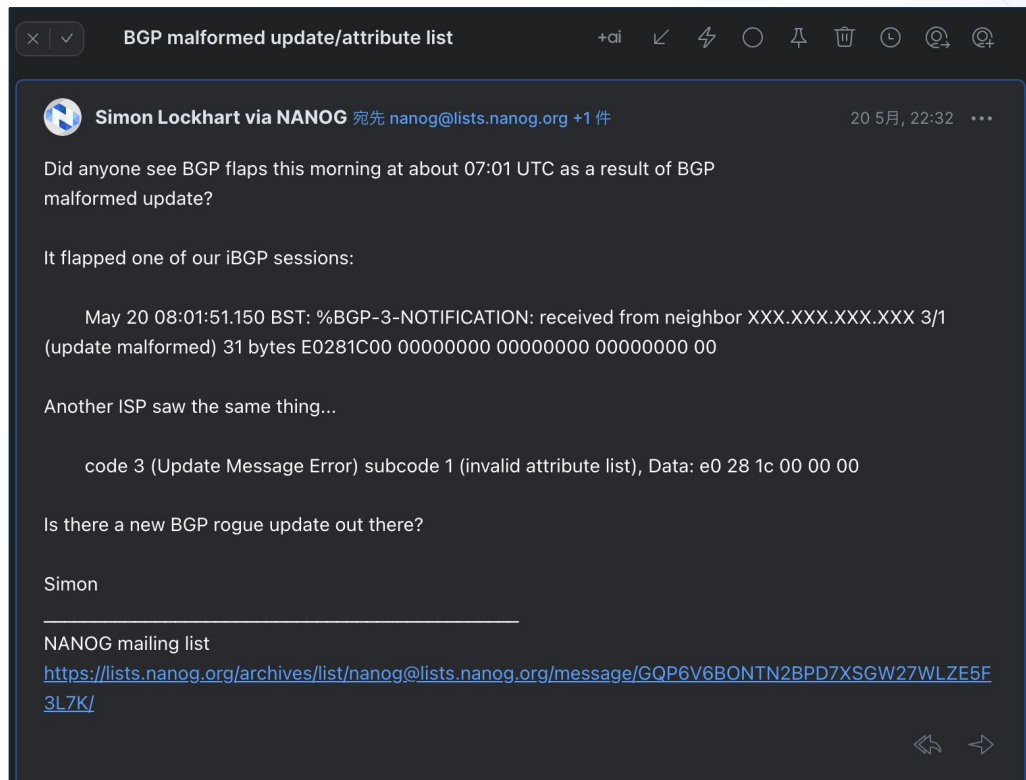
それでは

しっかり時間を割いて説明してみよう！！



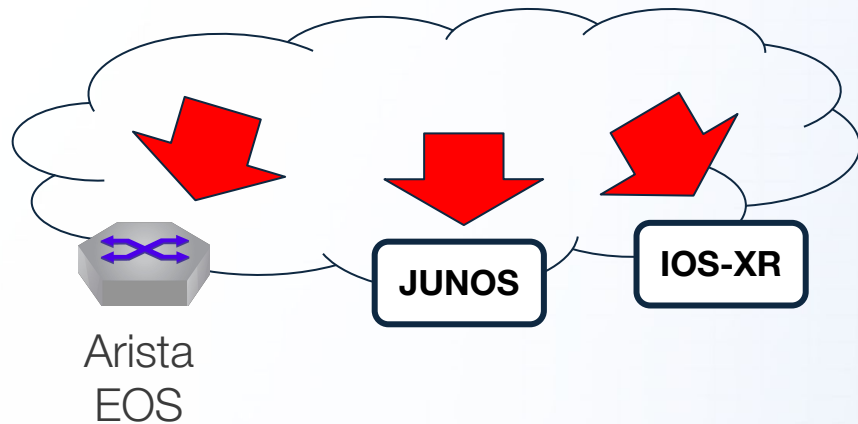
BGP malformed update/attribute list

<https://lists.nanog.org/archives/list/nanog@lists.nanog.org/thread/GQP6V6BONTN2BPD7XSGW27WLZE5F3L7K/>



- NANOGメーリングリスト
2025.5.20
 - 不正アップデートが原因でBGPがフラップした人いるか？
 - 他のISPでも起きてる

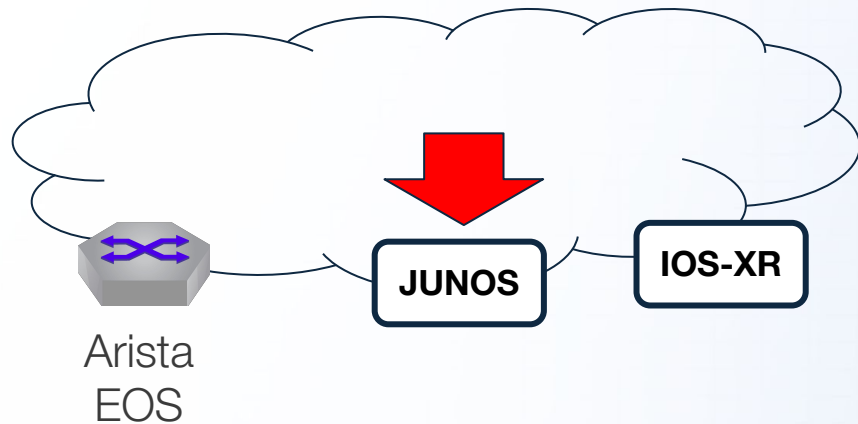
各ベンダー毎の不正メッセージを受けた時の挙動



1. Juniper JUNOS
2. Cisco IOS-XR
3. Arista EOS

各ベンダー毎の不正メッセージを受けた時の挙動 -JUNOS

<https://www.juniper.net/documentation/us/en/software/junos/bgp/topics/topic-map/bgp-error-messages.html#id-understanding-error-handling-for-bgp-update-messages>



- Juniperを使ってるがBGPのセッションは保てた
- “bgp-error-tolerance” を有効にしているJunos OS Release 24.2R1からはデフォルトで有効になっている

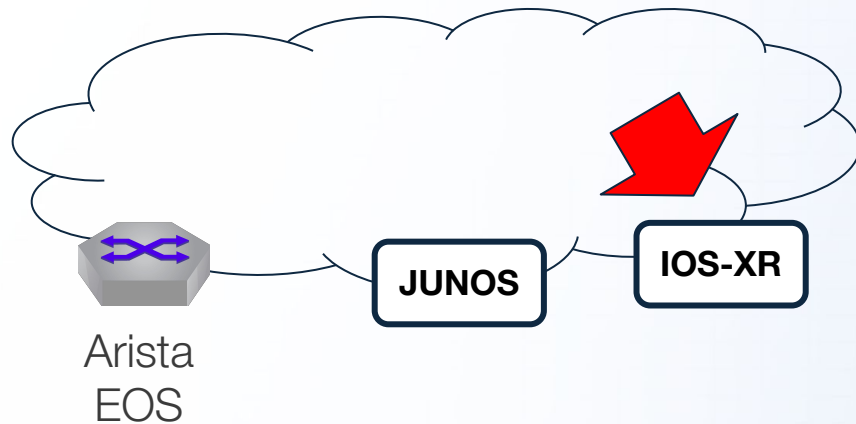
各ベンダー毎の不正メッセージを受けた時の挙動-JUNOS

```
May 20 07:01:51 router rpd[34930]: %DAEMON-4: bgp_read_v4_update:13937:
NOTIFICATION sent to a.b.c.d (Internal AS xxx): code 3 (Update Message Error)
subcode 131 (invalid), Data: 00 00 00 00 00 00
May 20 07:01:51 router rpd[34930]: %DAEMON-3: Received malformed update from
a.b.c.d (Internal AS xxx)
May 20 07:01:51 router rpd[34930]: %DAEMON-3: Family inet-vpn-unicast, prefix
a.b.c.d:32767:156.230.0.0/40 (label 114)
May 20 07:01:51 router rpd[34930]: %DAEMON-3: Malformed Attribute PREFIX_SID(40)
flag 0x80 length 28 error 131 (TLV length error).
```

PrefixSIDをアップデートで受け取っている

各ベンダー毎の不正メッセージを受けた時の挙動 -IOS-XR

https://www.cisco.com/c/en/us/td/docs/routers/xr12000/software/xr12k_r4-3/routing/command/reference/b_routing_cr43xxr12k/b_routing_cr43xxr12k_chapter_01.html#wp9225075190

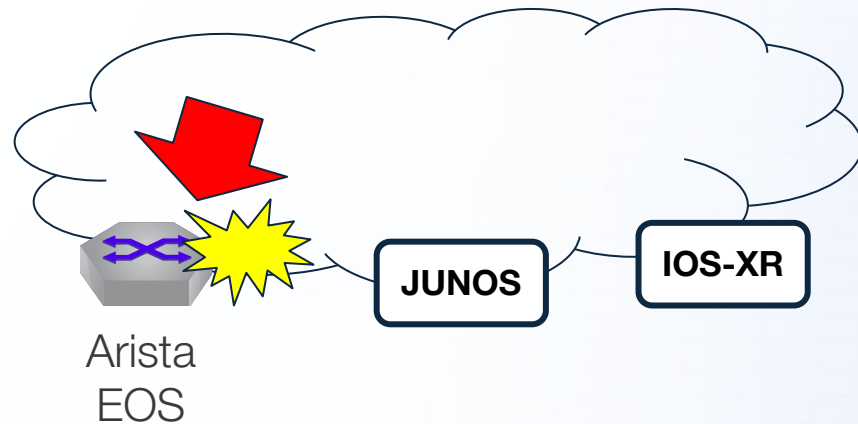


```
May 20 07:01:51 r2.f00 16869308:
RP/0/RSP0/CPU0:May 20 07:01:51.437 :
bgp[1059]:
%ROUTING-BGP-3-MALFORM_UPDATE :
Malformed UPDATE message received from
neighbor 123.45.67.89 (VRF: default) -
message length 106 bytes, error flags
0x000c0000, action taken "DiscardAttr".
Error details: "Error 0x00040000, Field
"Attr-length", Attribute 40 (Flags
0xe0, Length 28), Data [e0281c]".
NLRI: [IPv4 Unicast] 45.198.25.0/24
```

- こんなエラーが見えた
- show bgp update in errorのoutputと思われる

各ベンダー毎の不正メッセージを受けた時の挙動 -Arista EOS

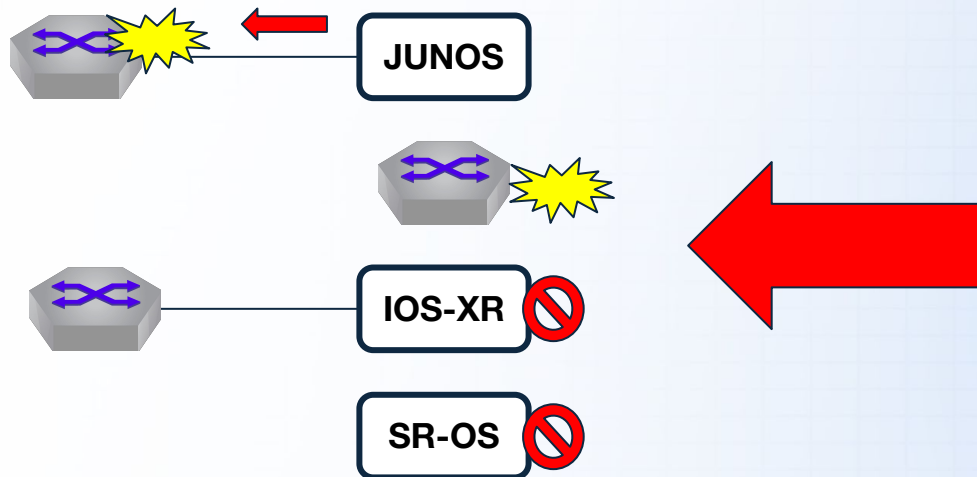
https://www.arista.com/en/support/software-bug-portal/bugdetail?bug_id=899981



- 7280R 4.29.7でリセットされた
- BUG899981: A malformed Prefix-SID BGP path attribute will result in a session reset rather than attribute discard.
- BUGがあり不正なPrefix-SIDのBGPアトリビュートは破棄では無くリセットしてしまう。

BGP handling bug causes widespread internet routing instability

<https://blog.benjojo.co.uk/post/bgp-attr-40-junos-arista-session-reset-incident>



Prefix SIDを/16で
送った尚且つデータ
部が全て0x00で壊
れていた

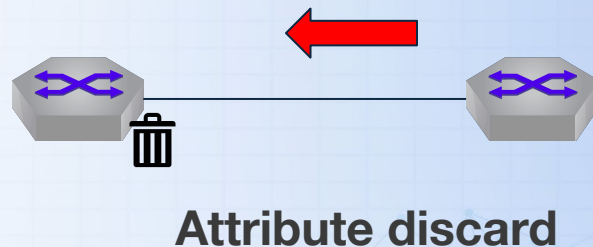
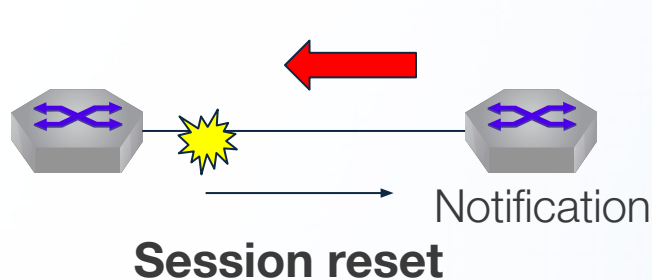
- JUNOSはセッションはリセットをしないがダウストリームにそれを送ってしまう
- Arista EOSにBUG899981があり、不正な Prefix SID の場合はBGPセッションをリセットしてしまう。
- IOS-XR/SR-OSはRFC7606 Revised Error Handling for BGPのAttribute discardの通りの実装で破棄する
 - RFC8669 Segment Routing Prefix Segment Identifier Extensions for BGP
<https://datatracker.ietf.org/doc/html/rfc8669#name-error-handling-of-bgp-prefix>

まとめ

- 不正なBGP Prefix SIDのアップデートが2025年5月20日に送信された
- Hutchison/AS9304にあるBIRDがBGP Prefix SIDはノンサポートである為、これを拡散した
- Cisco IOS-XR/NOKIA SR-OSはRFC7606 Revised Error Handling for BGPのAttribute discard記載どおりこれを廃棄した。つまりRFC8669の記載の通り
- Juniperはこれを透過し、他のピアに拡散した
- Arista EOSにはBUG899981があり、BGPセッションをリセットした
 - 修正済:4.28.11/4.29.8/4.30.6/4.31.2
 - https://www.arista.com/en/support/software-bug-portal/bugdetail?bug_id=89998
 - 特定のAttributeに対してのBUGであり、RFC7606はデフォルトで対応している

Appendix:RFC7606 Revised Error Handling for BGP UPDATE Messages

<https://datatracker.ietf.org/doc/html/rfc7606>



- RFC4271では不正なBGPアップデートメッセージはセッションをリセットするようになっていた
- 様々なBGPインシデントがあり、2011年に改定のドラフトが提案されRFC7606では既存の属性の取り扱いと、新しい属性についてのガイドラインが記載された

様々なBGPインシデント

<https://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h10/iw2009-h10-03.pdf>

- 2007年12月 PATH Attribute=0
- 2009年2月 AS_PATH too long
- 2009年3月 AS_CONFED_SET/SEQUENCE in AS4_PATH
- 2009年8月 AS4_PATH 0xE01100

多くのBGPセッションリセットが起こった

少量のルート的不正アップデートが原因なものもあり

非常に影響が大きい

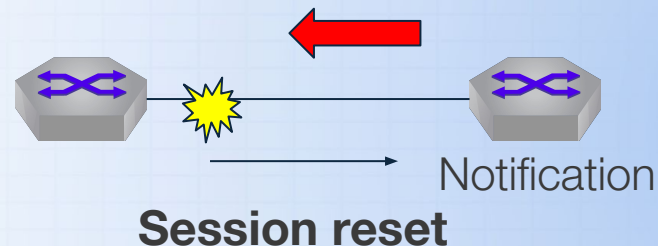
下記でそれらを改善

Optional Transitive Error Handling

<https://datatracker.ietf.org/doc/html/draft-scudder-idr-optional-transitive-00>

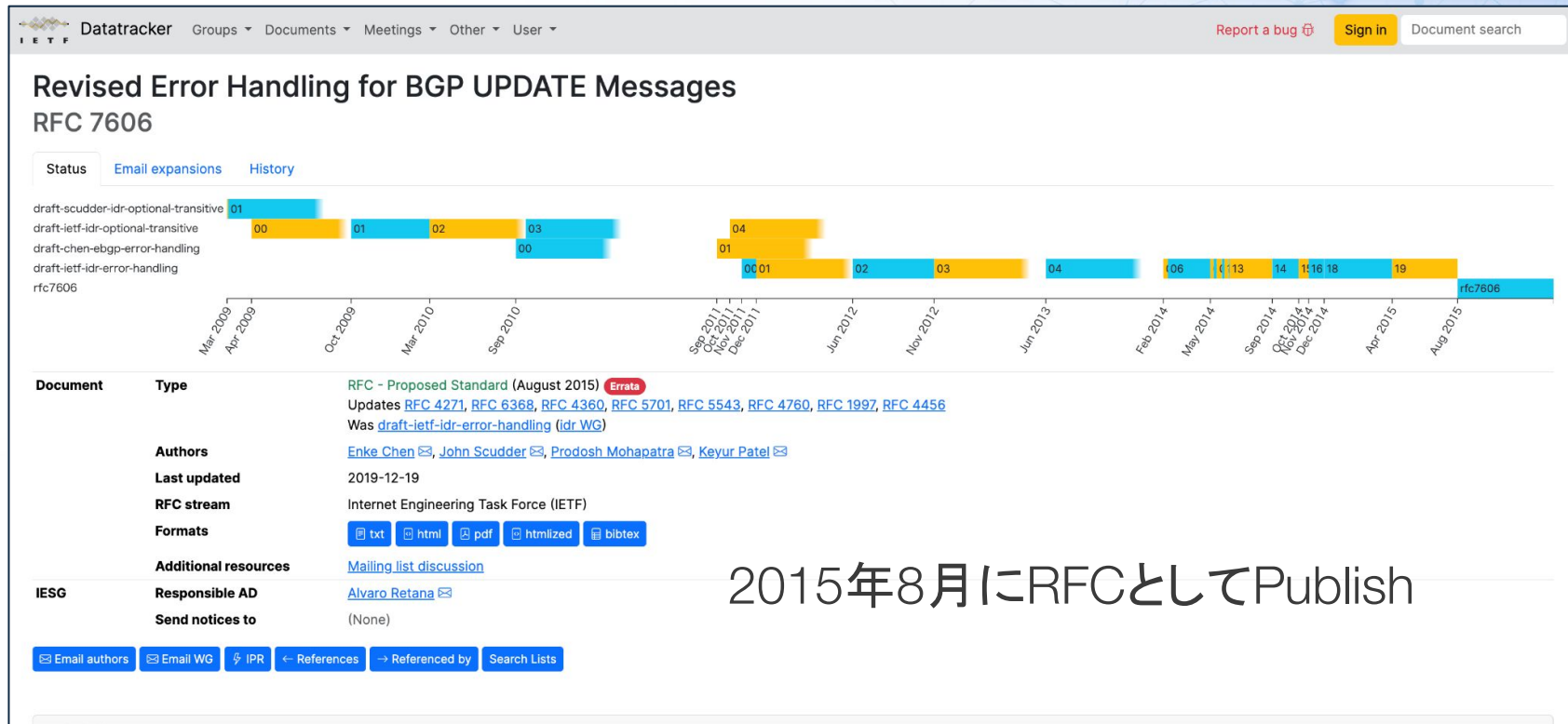
Revised Error Handling for BGP Updates from External Neighbors

<https://datatracker.ietf.org/doc/html/draft-chen-ebgp-error-handling-00>



Revised Error Handling for BGP UPDATE Messages RFC 7606

<https://datatracker.ietf.org/doc/rfc7606/>



Revised Error Handling for BGP UPDATE Messages RFC 7606

<https://datatracker.ietf.org/doc/rfc7606/>

属性	推奨アクション
ORIGIN	treat-as-withdraw
AS_PATH	treat-as-withdraw
NEXT_HOP	treat-as-withdraw
MULTI_EXIT_DISC	treat-as-withdraw
LOCAL_PREF	treat-as-withdraw
ATOMIC_AGGREGATE	attribute discard
AGGREGATOR	attribute discard
Community	treat-as-withdraw

属性	推奨アクション
ORIGINATOR_ID	eBGP attribute discard iBGP treat-as-withdraw
CLUSTER_LIST	eBGP attribute discard iBGP treat-as-withdraw
MP_REACH_NLRI	"session reset" or "AFI/SAFI disable"
MP_UNREACH_NLRI	NOTIFICATION
Traffic Engineering Path Attribute	treat-as-withdraw

Revised Error Handling for BGP UPDATEMessages RFC 7606

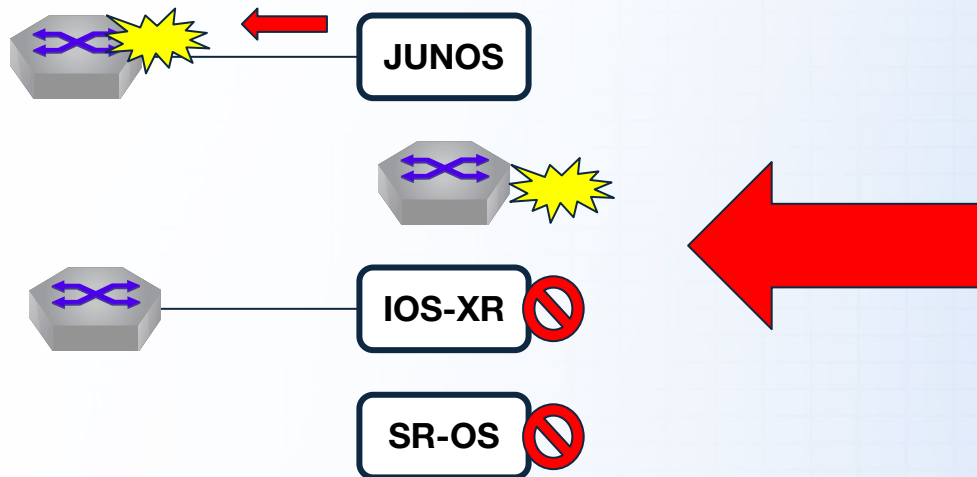
<https://datatracker.ietf.org/doc/rfc7606/>

属性	推奨アクション
Extended Community	treat-as-withdraw
IPv6 Address Specific BGP Extended Community Attribute	treat-as-withdraw
ATTR_SET	treat as withdraw

- RFC7606では既存の属性の取り扱いと、新しい属性に関してのガイドラインが記載された
- 新しいBGP属性を提示する文章にはその属性のエラー構成要素とエラー処理方法を記載しなければならない
- 一般的には"treat-as-withdraw"が好まれ、"session reset"は推奨されない
- "attribute discard"は潜在的な影響をよく検討すべき

BGP handling bug causes widespread internet routing instability

<https://blog.benjojo.co.uk/post/bgp-attr-40-junos-arista-session-reset-incident>



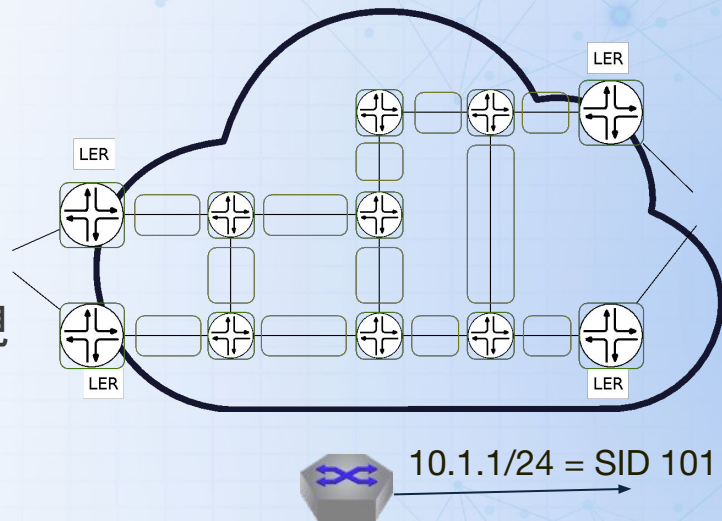
Prefix SIDを/16で
送った尚且つデータ
部が全て0x00で壊
れていた

- JUNOSはセッションはリセットをしないがダウストリームにそれを送ってしまう
- Arista EOSにBUG899981があり、不正な Prefix SID の場合はBGPセッションをリセットしてしまう。
- IOS-XR/SR-OSはRFC7606 Revised Error Handling for BGPのAttribute discardの通りの実装で破棄する
 - RFC8669 Segment Routing Prefix Segment Identifier Extensions for BGP
<https://datatracker.ietf.org/doc/html/rfc8669#name-error-handling-of-bgp-prefi>

RFC8669 Segment Routing Prefix Segment Identifier Extensions for BGP

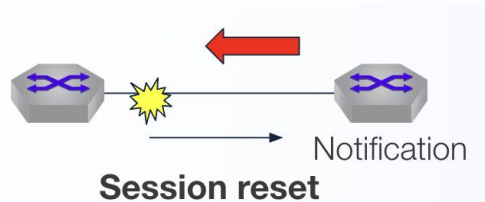
<https://datatracker.ietf.org/doc/html/rfc8669>

- BGPでPrefix SIDを伝える為のRFC
- 6. Error Handling of BGP Prefix-SID Attribute
 - 不正な形式または無効なBGP PrefixSID属性を含むBGP UPDATEメッセージを受信した場合、受信したBGP PrefixSID属性を無視し、他のBGPピアにアドバタイズしてはならない。
 - これはRFC7606の"Attribute discard"に値する

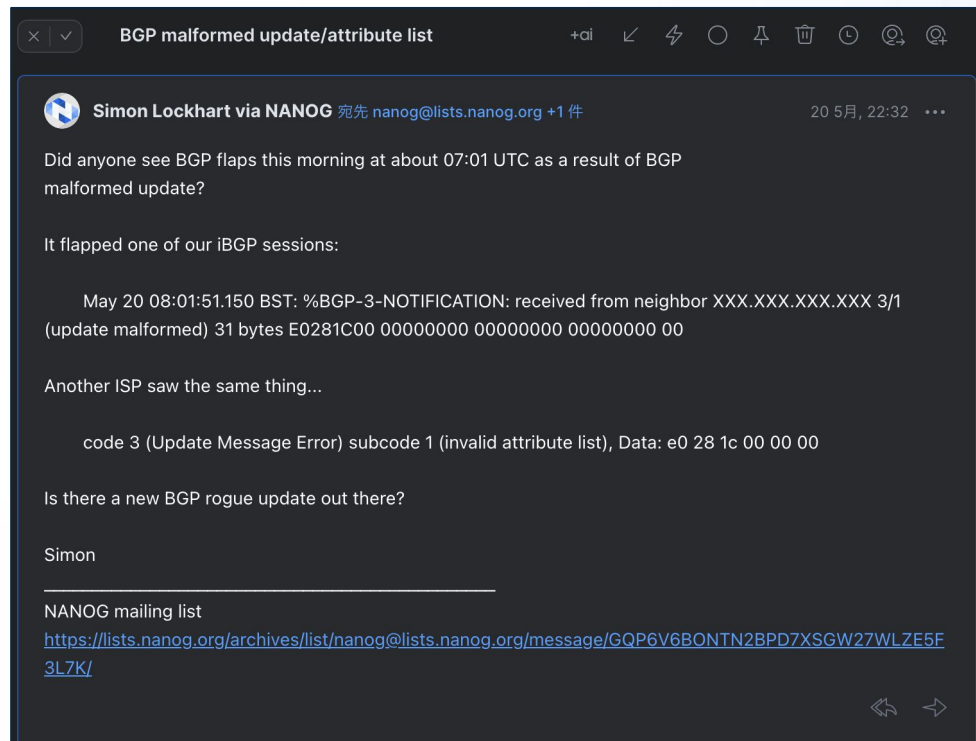


結構難しい話

- RFC4271では不正なアップデートはBGPのセッションをリセット
- RFC4271は改定されRFC7606を実装することが求められた
- RFC7606では新しい属性の不正なアップデートでは一般的には treat-as-withdraw が好まれることが記載/また各新しい属性に関しては エラーハンドルの手法を記載する事を記載
- RFC8669ではAttribute discardと記載



最初の感想



- なんか久しぶりー
- えっうちRFC7606対応してないの??
- メッセージめっちゃ見やすいな

Appendix:RFC 7606: BGP enhanced error handling

<https://www.arista.com/en/support/toi/eos-4-20-1f/13921-rfc-7606-bgp-enhanced-error-handling>

```
router#show ip bgp neighbors update errors
BGP update-error information for VRF None
Neighbor: 1.0.0.2
Malformed Action: Withdraw-Route Attribute: Community
Update Buffer: 0x40010101400204020100644003040100000240050400000014c00805000000fde9
Malformed Action: Attribute-Ignore Attribute: Local Preference
Update Buffer: 0x40010101400204020100644003040100000240050400000014c00805000000fde9
```

```
router#show ip bgp neighbors 10.0.0.2
BGP neighbor is 10.0.0.2, remote AS 64512, external link
BGP version 4, remote router ID 1.0.2.1, VRF default
Negotiated BGP version 4
Last read 00:13:48, last write 00:14:06
-snip-
Number of transitions to established: 1
Inbound updates with attribute errors:
Resulting in removal of all paths in update (treat-as-withdraw): 10
Resulting in AFI/SAFI disable: 0
Resulting in attribute ignore: 5
Last treat-as-withdraw attribute error: Community
Last ignored attribute error: Local Preference
Last update with error received at: 00:13:48
```

- EOSではすでに RFC7606は実装されていて、不正アップデートを受信した際の取り扱いに関しても showコマンドで表示される

まとめ

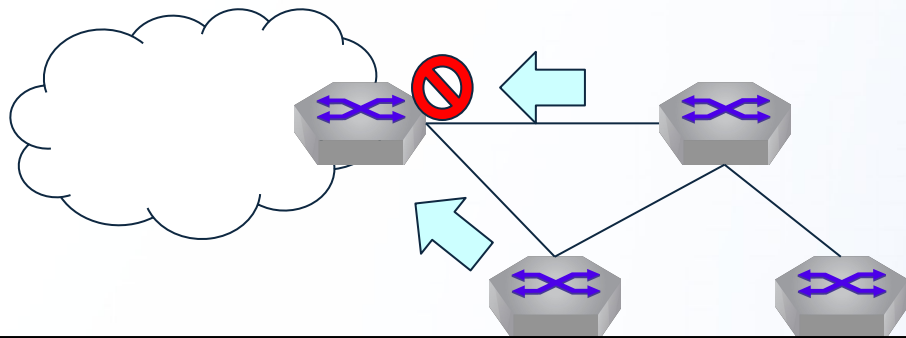
- 不正なBGP Prefix SIDのアップデートが2025年5月20日に送信された
- Hutchison/AS9304にある**BIRDがBGP Prefix SIDはノンサポートである為、これを拡散した**
- **Cisco IOS-XR/NOKIA SR-OSはRFC7606 Revised Error Handling for BGPのAttribute discard記載どおりこれを廃棄した。**つまりRFC8669の記載の通り
- **Juniperはこれを透過し、他のピアに拡散した**
 - この挙動は2026年1月15日にCVE-2025-60011として公開された
<https://nvd.nist.gov/vuln/detail/CVE-2025-60011>
- **Arista EOSにはBUG899981があり,BGPセッションをリセットした**
 - 修正済:4.28.11/4.29.8/4.30.6/4.31.2
 - https://www.arista.com/en/support/software-bug-portal/bugdetail?bug_id=89998
 - 特定のAttributeに対してのBUGであり,RFC7606はデフォルトで対応している

いいなかった事

- 難しくない？？？
- 全BGP属性をサポートしなければいけない。もしくはエラーハンドルは理解してなきゃいけない
- メーカーとしては新しい属性をサポートして、きれいにエラーハンドルも実装する(これはそう)
- 1つのワークアラウンドになるかもしれない

Appendix.Ignore BGP attributes

<https://www.arista.com/en/support/toi/eos-4-29-2f/17038-ignore-received-bgp-attributes>



- EOSでは特定のネイバーに対してAFIにて受け取るattributeを指定する事が出来る

```
router(config-router-bgp)#neighbor default received attribute discard 4-255
! To make this command effective for existing BGP sessions, clear all the routes by issuing "clear ip bgp *"
router(config-router-bgp-vrf-vrf1)#neighbor default received attribute discard disabled
! To make this command effective for existing BGP sessions, clear all the routes by issuing "clear ip bgp *"
router(config-router-bgp)#show active
router bgp 1
  router-id 0.0.0.1
  neighbor default received attribute discard 4-255
vrf vrf1
  router-id 0.0.0.2
  neighbor default received attribute discard disabled
```

これも一つの運用回避になりますか？

- デフォルトで必要な属性のみを受け取る
- もしくは現在定義されているものだけ。
 - <https://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml#bgp-parameters-2>
- 現実的にはこんな事は二度と起こらないのかもしれない？ そうかな？
- 他ベンダーおよびBIRDにも同様な設定コマンドはある
- 下流のBGPスピーカーに迷惑をかけてる実装があり、それが自身には影響無い時、あなたはそのソフトウェアをバージョンアップしますか？
- ルートサーバーもメーカー実装のルータOSと同様にBGPの最新標準化技術をサポートしてますか？



ARISTA

Thank You

www.arista.com