

実践！インターネット ルーティングセキュリティ

Matsuzaki 'maz' Yoshinobu

<maz@iij.ad.jp>

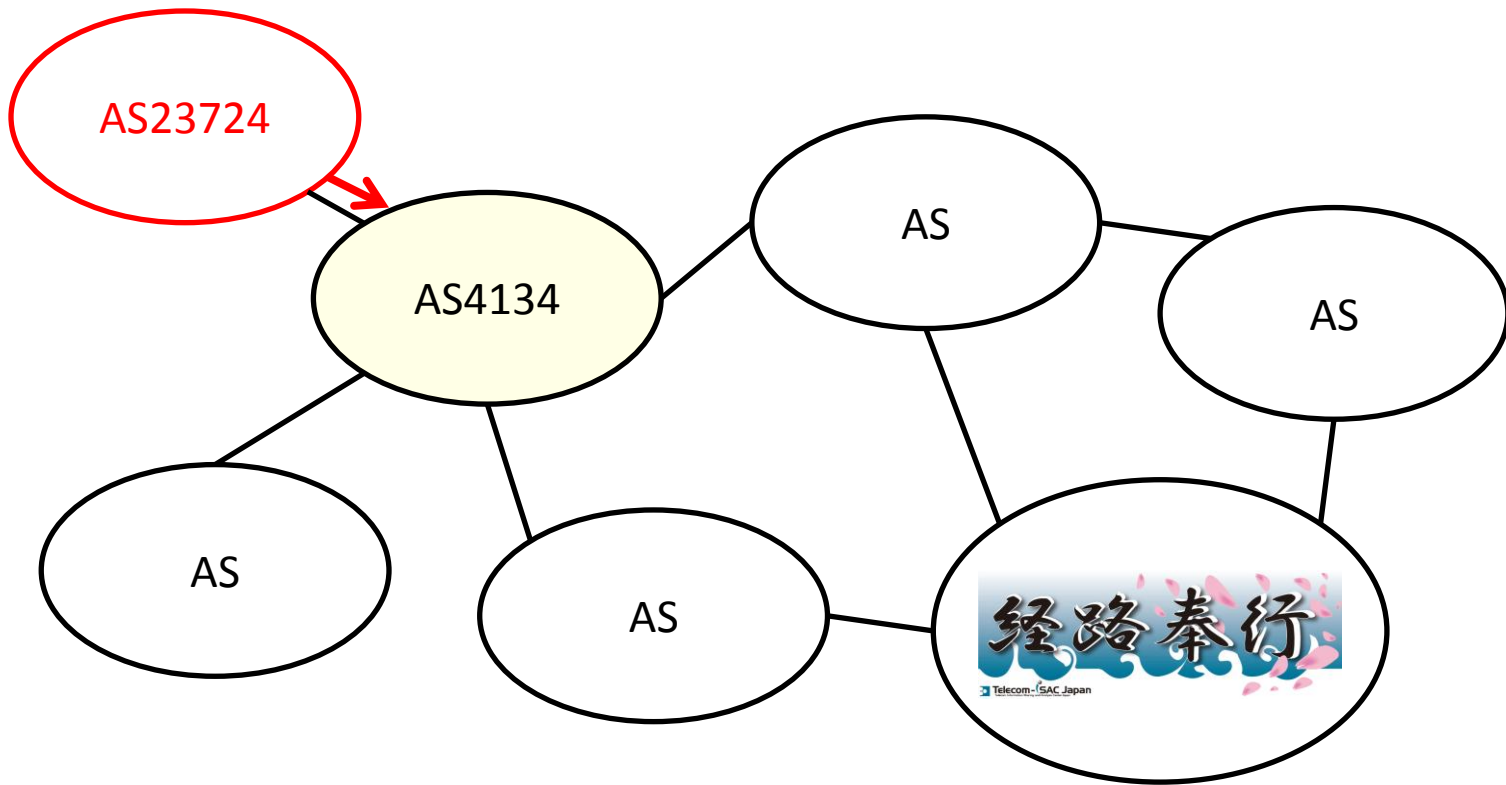
ただし書き

- ML等で公開されている情報は書いちゃってますが、公開の場に出されていない情報は伏せています
- 事例から学ぼうという試みです
 - 特定の組織を非難するものではありません
 - 特定の個人を非難するものではありません
 - 特定の対応を非難するものではありません
- 時刻は基本的にJSTです

事例1 – 誤生成

- 2010年4月9日
- AS23724を広報元として、他のネットワークの経路が大量に生成されて広報された
 - 数万経路程度が広報された模様
- 概ね、元の経路サイズと同じprefix長で広報
- AS4134を経由して、他のASに伝搬
 - 4134 23724 23724

事例1 - 誤生成



事例1 – 誤生成



事象発生

04/09 00:54 経路奉行で検知

広報元で対応？

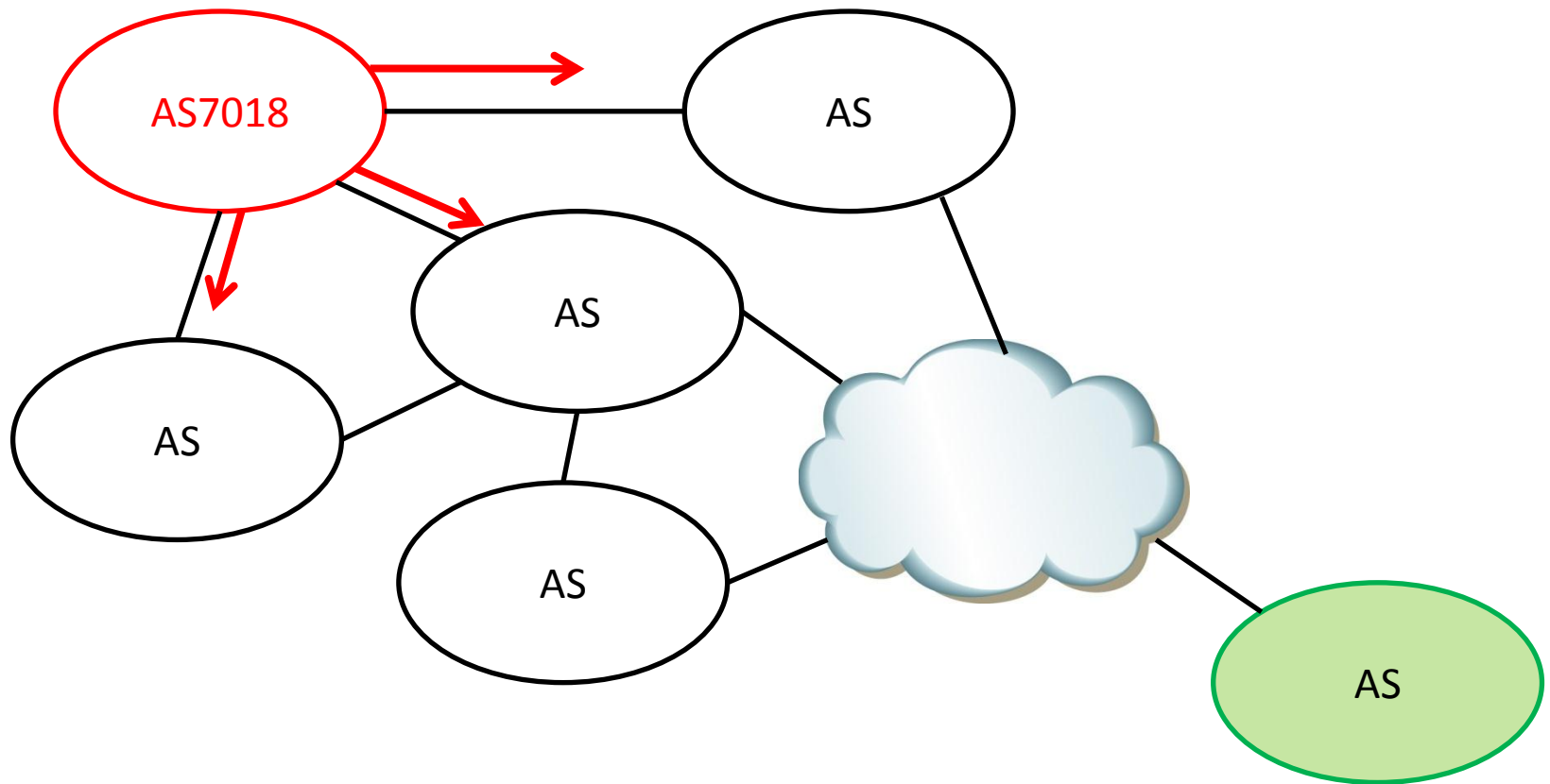
04/09 01:02 経路奉行で回復検知

04/09 01時頃 NANOGにポスト

事例2 – 誤生成

- 2006年11月30日
- AS7018を広報元として、他のネットワークの経路が生成されて広報された
 - 2経路が生成された
- 割り振りされたネットワークを利用しようとしたら、既に広報されていることに気が付いた

事例2 - 誤生成



事例2 – 誤生成



2006/11/30 00時頃 事象発生

2007/01/26 JANOG19で報告

2007/01/29 12時頃 広報元に連絡

2007/01/29 16時頃 広報元で対応

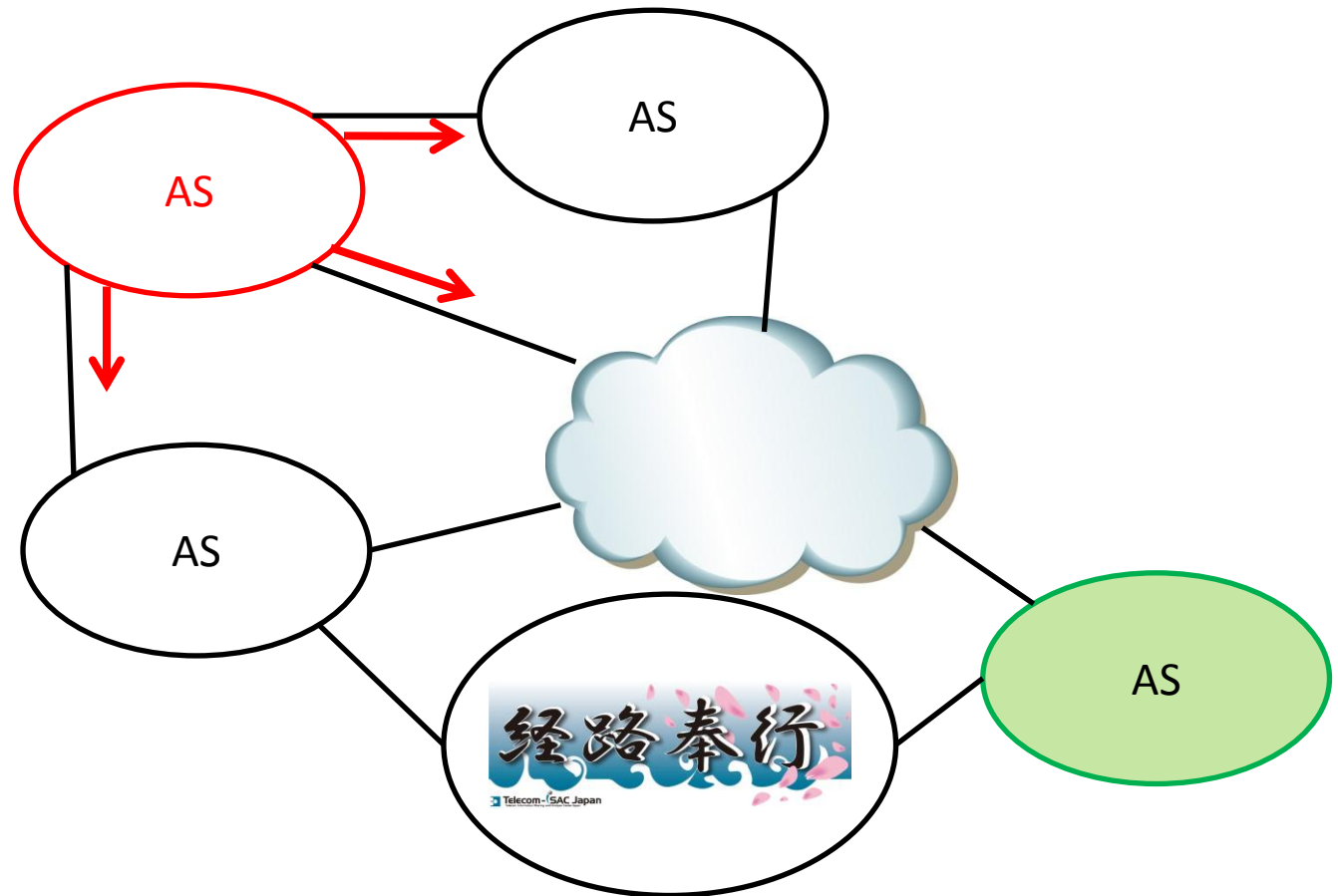
2007/01/29 16時頃 広報元から解決連絡

2007/01/29 16時頃 JANOG宛に解決連絡

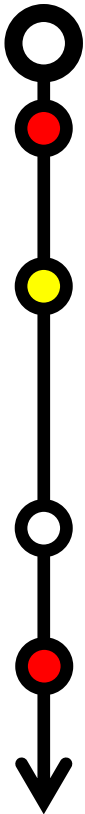
事例3 – 誤生成

- 2011年10月6日
- あるASを広報元として、他のネットワークの経路が生成されて広報された
 - 1経路が生成された模様
 - /64で広報 ← IPv6 prefix
- 上流のISPやピアを経由して、他のASに伝搬
 - 経路奉行でも受信

事例3 – 誤生成



事例3 – 誤生成



事象発生

10/06 15:51 経路奉行で検知

経路奉行の検地を元に広報元に連絡
- 広報の停止を依頼

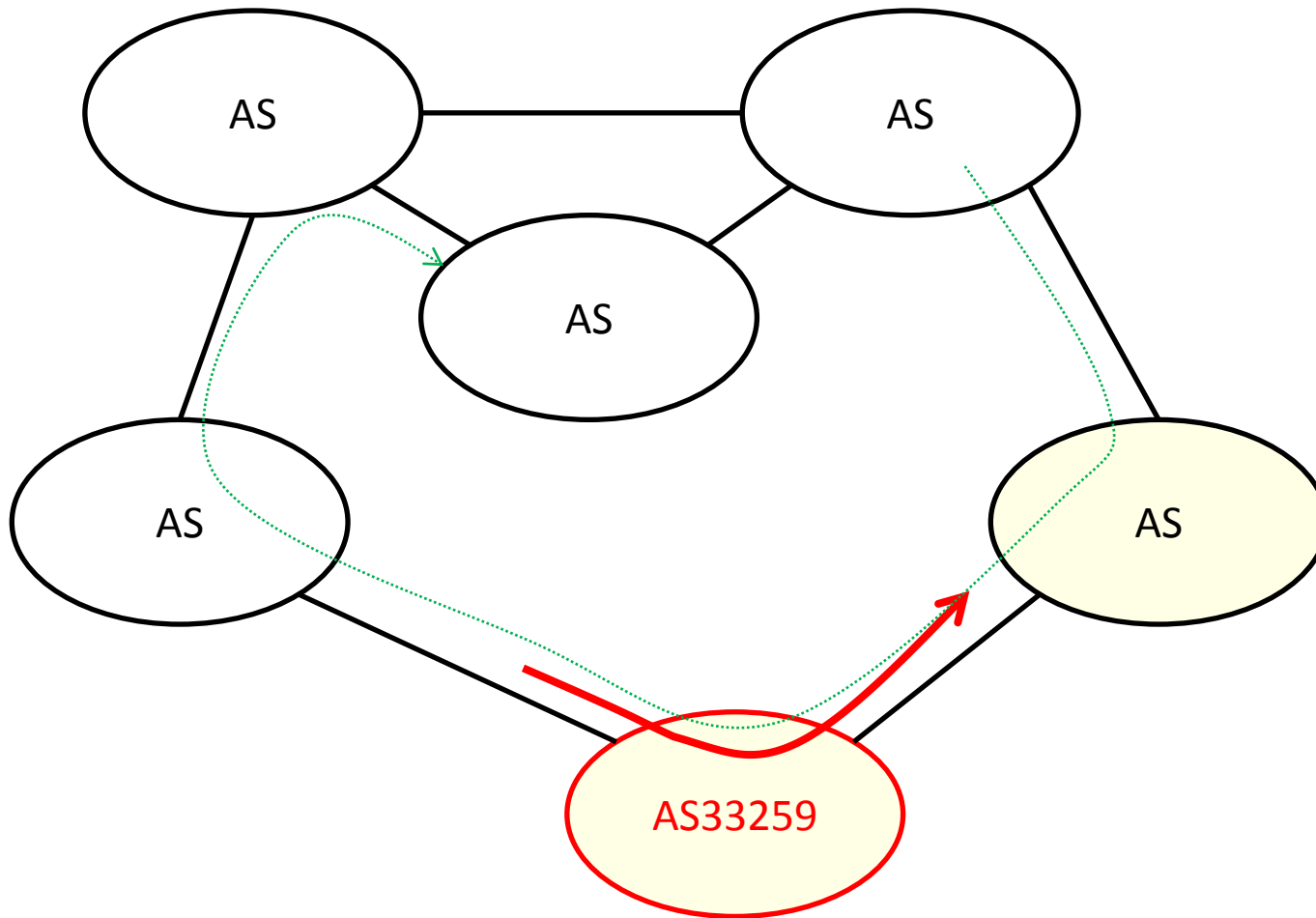
広報元で対応

10/06 16:09 経路奉行で回復検知

事例4 – 誤トランジット

- 2010年2月19日
- AS33259が、上流から受けとった経路をもう一方の上流にトランジットした
 - 数万程度の経路がトランジットされた模様
- 上流のISPで誤トランジットされた経路を受信し、優先したために広く伝搬した

事例4 – 誤トランジット



事例4 – 誤トランジット



事象発生

02/19 18時頃 品質劣化通知

02/19 19時頃 一次対応

- 直接リンクに引き込むように調整
- 問題のASとその上流に連絡

02/19 20時頃 NANOGにポスト

02/20 00時頃 上流のISPで経路フィルタ投入

まとめ

- 大事なこと
 - 事象の検知
 - 素早い連絡、頑張って連絡
- 助けになること
 - IR, IRRの情報整備
 - コンタクト先の確保