

Route Reflector構成での RPKIの動作検証

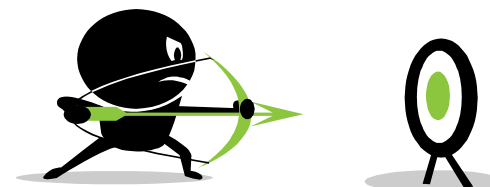
インフラストラクチャ本部 データセンターチーム 黒河内 倫

現行でているRouter/SwitchなどではRPKIを対応していない機器もある

RPKIのためにRouterをリブレースすることは難しい場合もあるため、Route Reflector構成で集中的に管理できる方法がないか検討をする

なお現状iBGPでRPKI Validationができる機種はJuniper製しかないため、今回はRouter ReflectorをJuniper製の機器で実装した

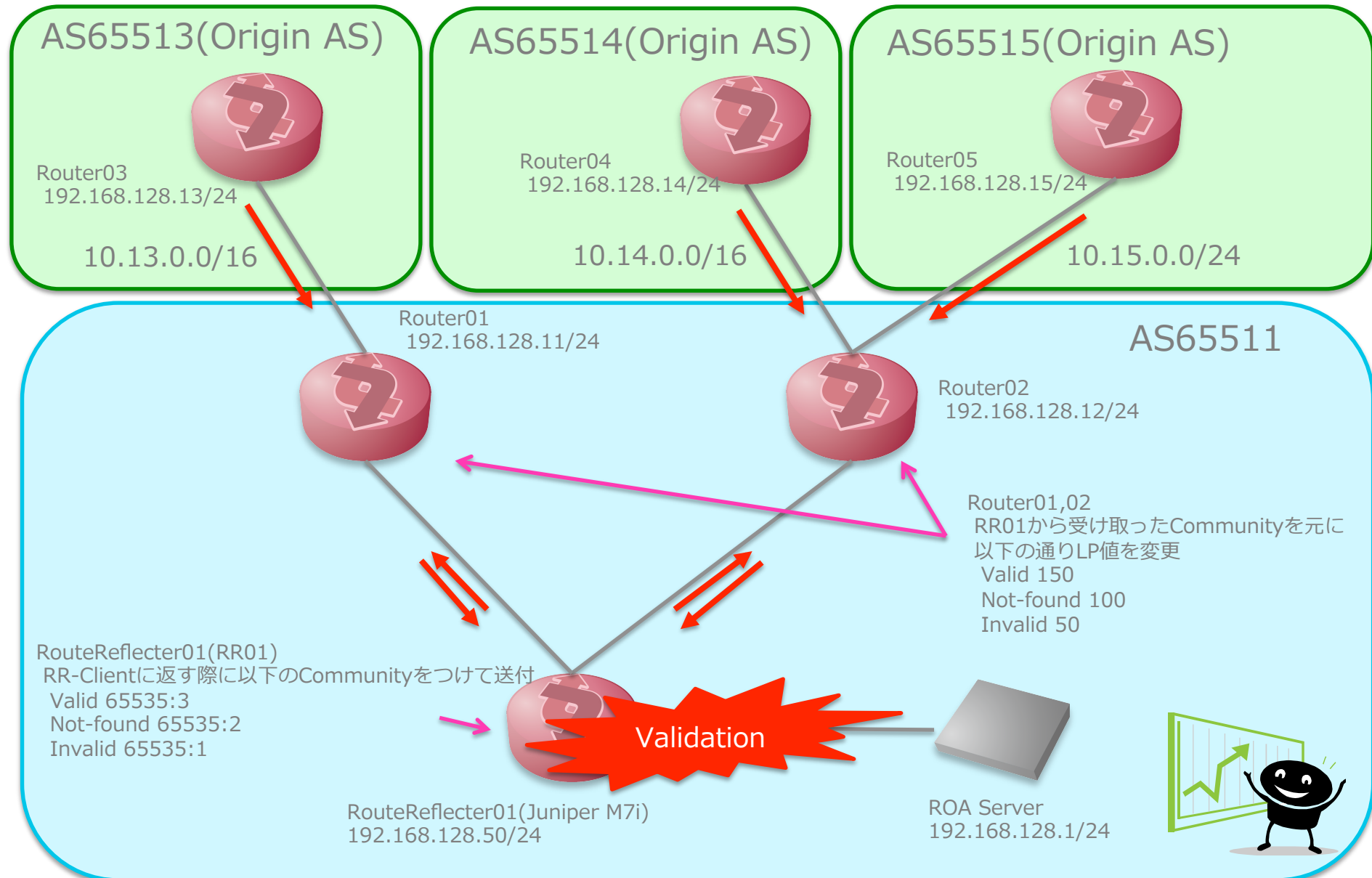
※JUNOSの実装上eBGPとiBGPを区別していないだけで、特にiBGPでのValidationを意識した実装というわけではないと予想される



基本情報



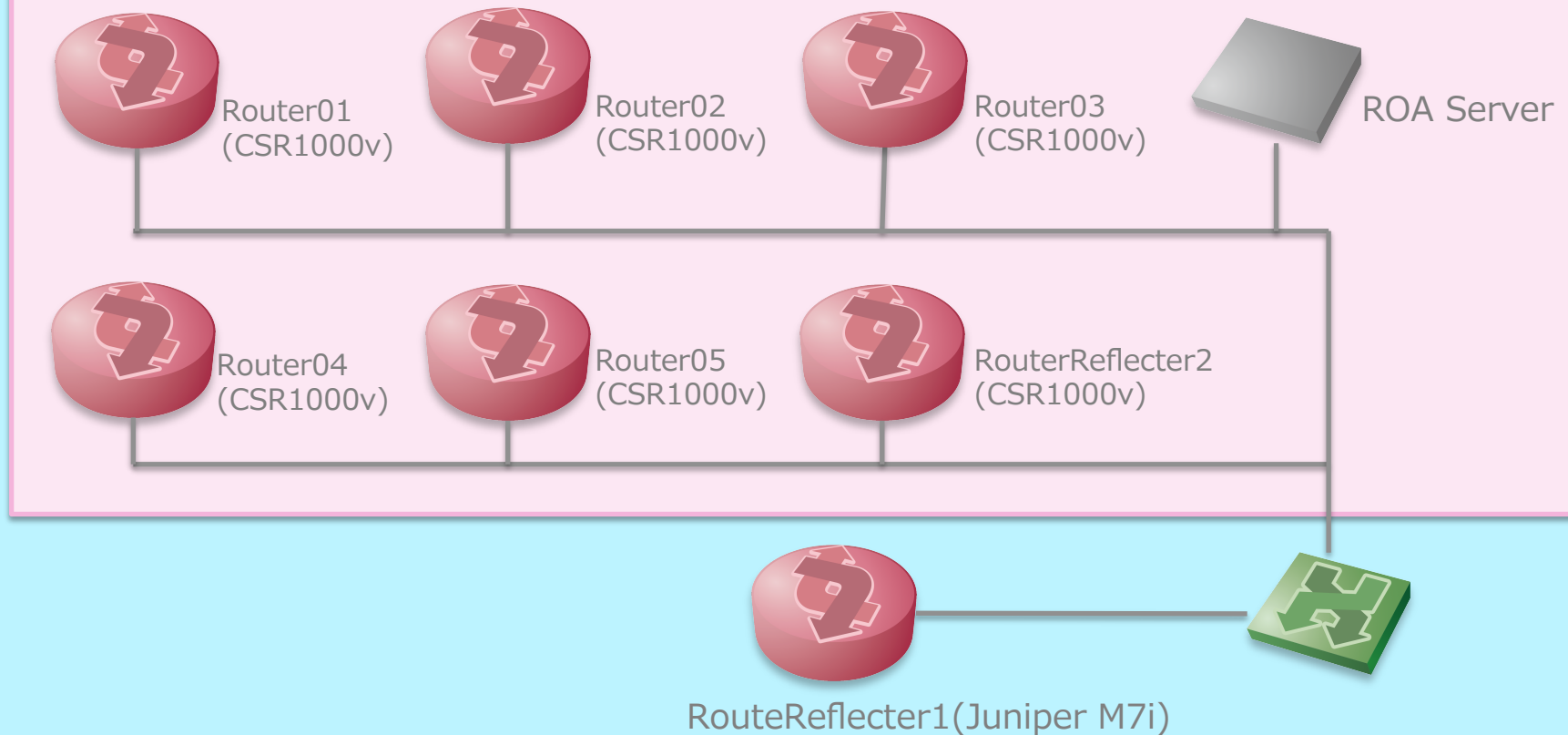
基本ネットワーク構成



物理結線図

192.168.128.0/24

VMware ESXi サーバ



OS

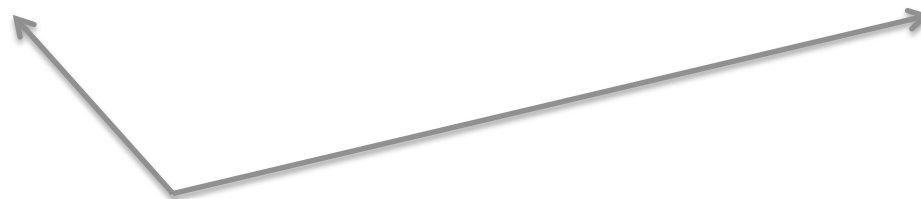
Juniper M7i : JUNOS 12.3R8.7

CSR1000v : IOS-XE 15.4



機材提供 : JPNIC様

Prefix	MaxLengeth	AS-Number
10.12.0.0/16	24	AS65512
10.13.0.0/16	24	AS65513
10.14.0.0/16	24	AS65514
10.15.0.0/16	24	AS65515



IPアドレスの2オクテット目とAS-Numberの下二桁が同じである

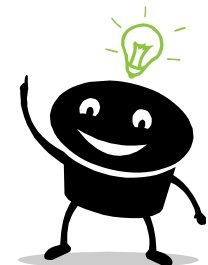
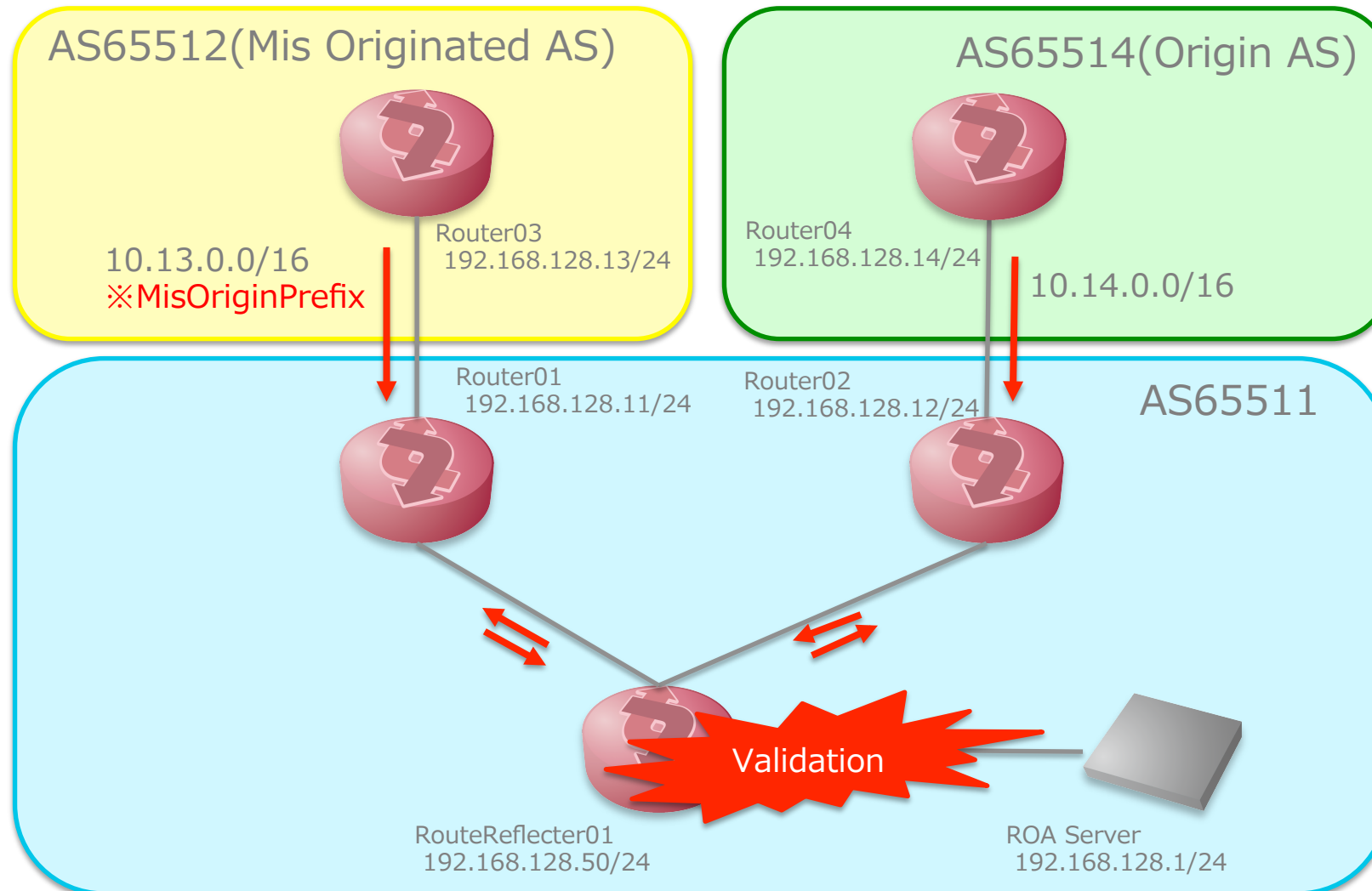


検証



検証1(Invalid経路の送付)

AS65512で広報する経路を、誤った経路に設定しRRでValidationできるか確認する



できた！

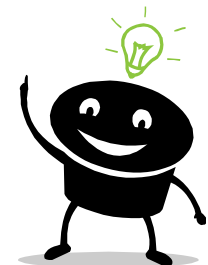
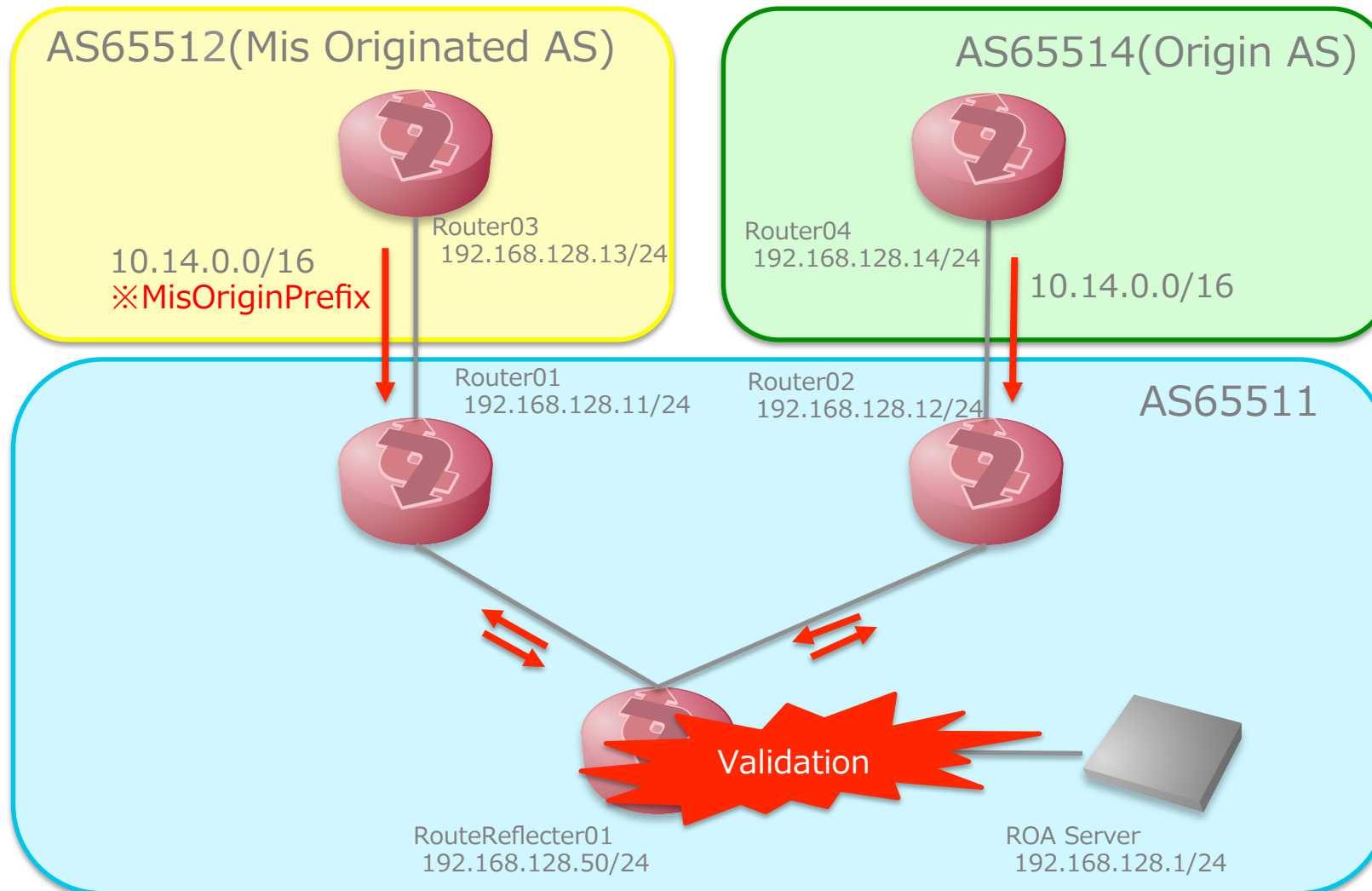
問題なく RouteReflector01にてValidationができ、
Client(Router01,02)側でもLPを変更がされてBestPathを選択できている



検証2(Invalid経路とBest Path Selection)



AS65512で広報する経路を、AS65514の経路に設定しRRでValidationできるか確認する
またその際に、Router01で10.14.0.0/16のBest PathがAS65514となるか



できた！

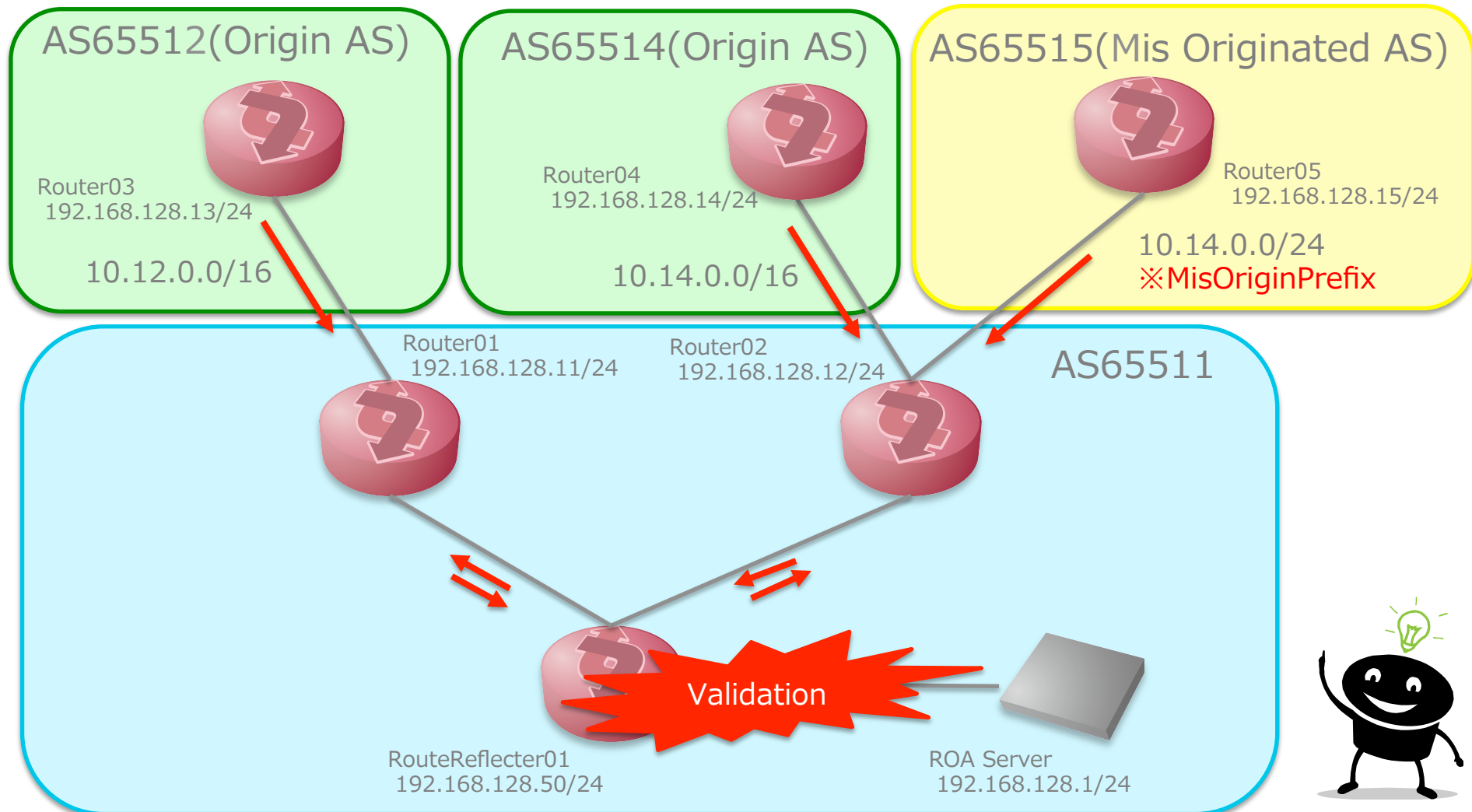
問題なく RouteReflector01にてValidationができ、
Client(Router01,02)側でもLPを変更がされBestPathを選択できている

10.14.0.0/16のNexthopが192.168.128.14@AS65514になり、
期待通りの動作となっている



検証3(Longest Match)

AS65515で広報する経路を、AS65514の経路に設定を行い、更に小さいサブネットに設定
この場合RR01でValidationできるか、またRouter01でAS65514をBestPathに選択できるか



できない

10.14.0.0/16@AS65514がRouteReflector01まで伝搬しない

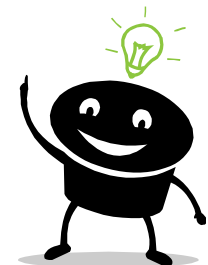
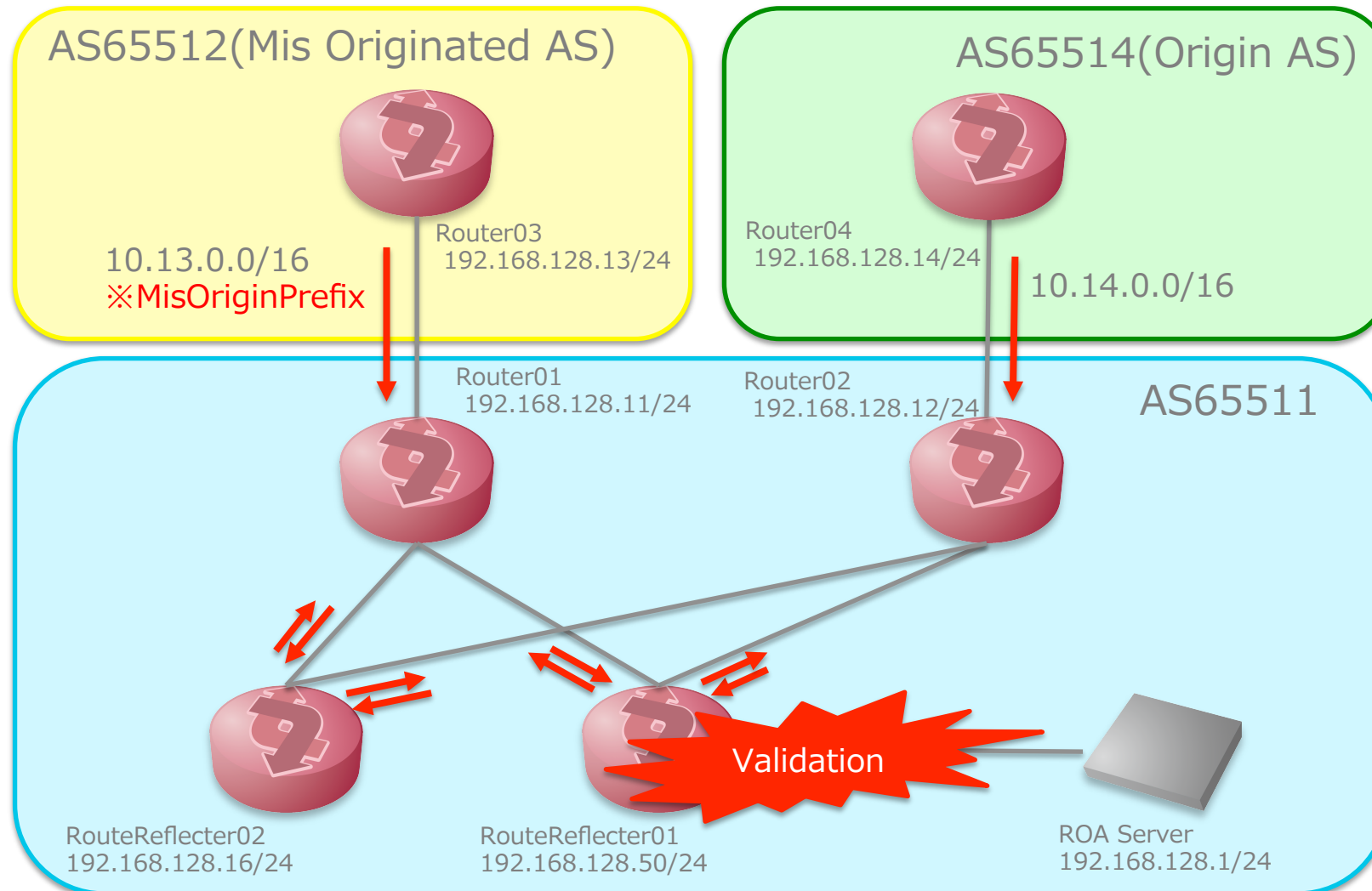
理由としては、Router02がBestPathを選択してから
RouteReflector01に経路広告をしている

そもそもRouter02内のLongestMatchで正しい経路である
10.14.0.0/24が負けてしまっているため、このような事象になっている



検証4(RR2台構成)

片側のRouter ReflectorのみRPKIが動作している状況で



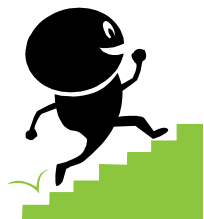
できるけど、 やめたほうがいい

Router01,02の経路情報は、Route Reflector01からの経路は
ValidationされたCommunityを受け取り、Route Reflector02からは
通常の経路情報で伝搬されている

ただし、そもそも同一AS内でRouteReflectorが2台があった場合は、
同じPolicyで運用しないと事故が起きる可能性が高い



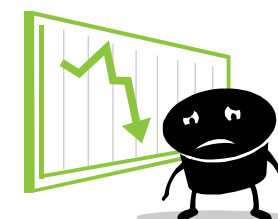
考察



Route ReflectorでのiBGPでのValidation自体は可能
※前提としてはiBGPでValidation可能なJuniperのみ

ただしBGPの特性上、同一AS上の経路については
BestPathのみ広報されるため、一つのRouterに同一経路で複数の
Pathがある場合は、Validになるはずの経路がRouter Reflectorまで
届かない

ADD-PathやBGP-Conederationを利用すれば、可能かもしれないが
今回は機器や時間の関係上、そこまではできなかった



まとめ



現在のところはASBR(eBGP)側でValidationを行うことが、
無難な実装方法であると考え

iBGPでの実装も可能ではあるものの、対応機器も限定的であり、
かつ内部の構成も複雑化させなければならないケースもある

ただし、RPKIの普及促進や経路の集中管理を考えた場合、
Route Reflectorでの集中管理ができた方がよいこともあると思う



Internet上のどこでValidationすべきか？

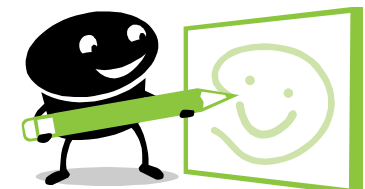


ただし、すべてのEndのASのすべてのASBRで
Validationを実装することは、おそらく難しいと思われる

そのため、TransitやIXなど上位の接続となるキャリアが
Validationした結果を、接続先のASに伝えることが望ましい

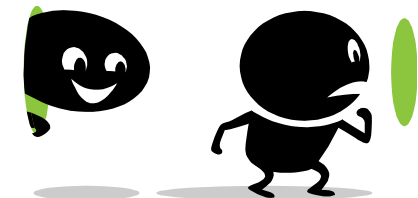
IXの場合はRoute Serverを利用した経路伝搬をサポートすればよい
※個別のPeeringで実装していくことは難しいだろう

提供方法としてはValidationした結果を
BGP-Communityで送付するのが現実的であろう



非常に限定的ではあるが、以下の構成を実装することで
Route Reflector構成でもValidationを実装することは可能である

1. ASBRにてすべての経路をRoute Reflectorに送信できる仕組みにする
ext) 1Routerに1Transitだけを収容し、
ASBRでBest Path Selectionをさせないなど
2. Route ReflectorにはiBGPでValidation可能な
Juniper製の機器を選定する
ただし今後のJunosの仕様方針によっては
iBGPでのValidationができなくなる可能性もある





最後に

今回の検証にご協力いただいた方



インターネットマルチフィード株式会社

川上 雄也さん

一般社団法人日本ネットワークインフォメーションセンター

岡田 雅之さん

ご協力ありがとうございました



