

01 インターネットを守る技術普及について
考える

～インターネットワーキングのススメ～

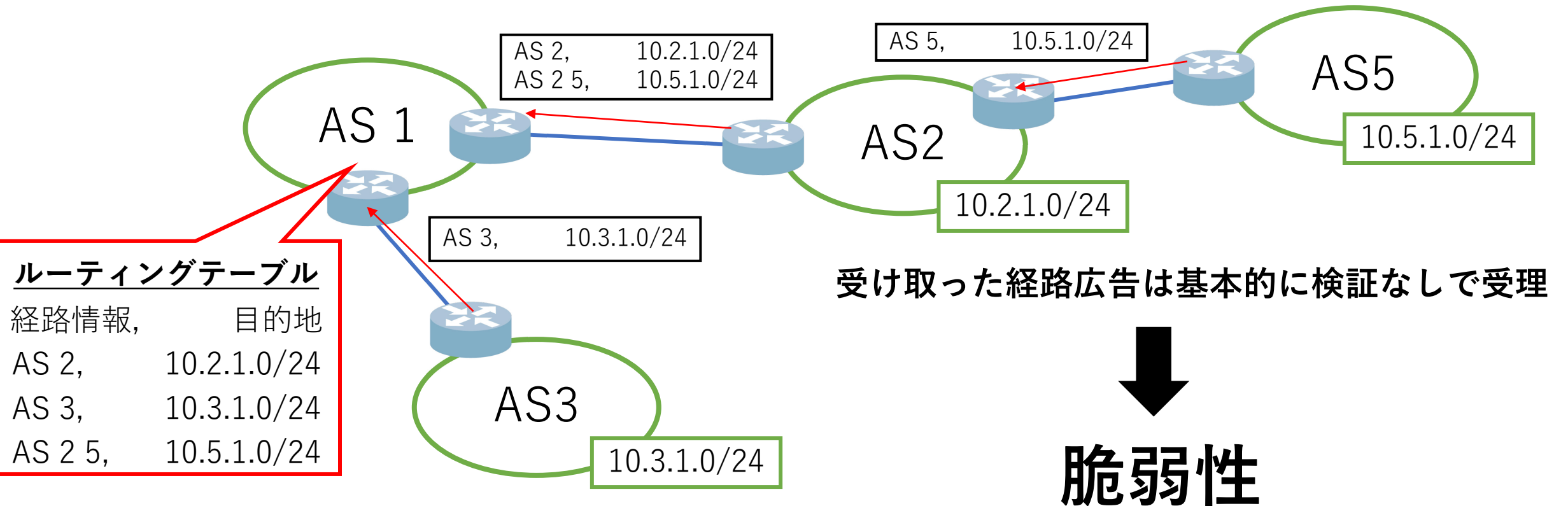
大阪大学

矢内直人

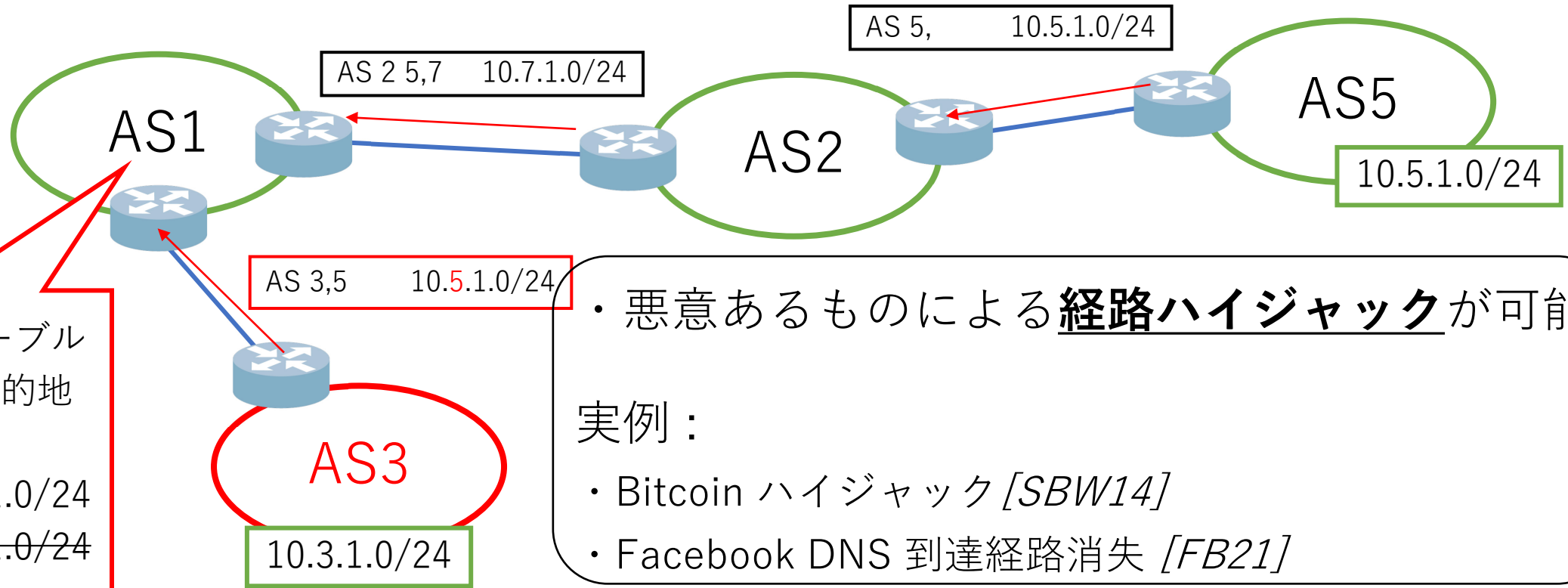
Internet Week 2023

Border Gateway Protocol [RFC4271]

- インターネットは 自律システム(AS) によって構成
- BGP : AS 間で経路情報の交換を行うプロトコル
- ある AS に到達するまでに経由する ASをやりとりする



不正経路伝搬



ルーティングテーブル
経路情報, 目的地
:
AS 3 5 , 10.7.1.0/24
~~AS 2 5 , 10.7.1.0/24~~
:
:

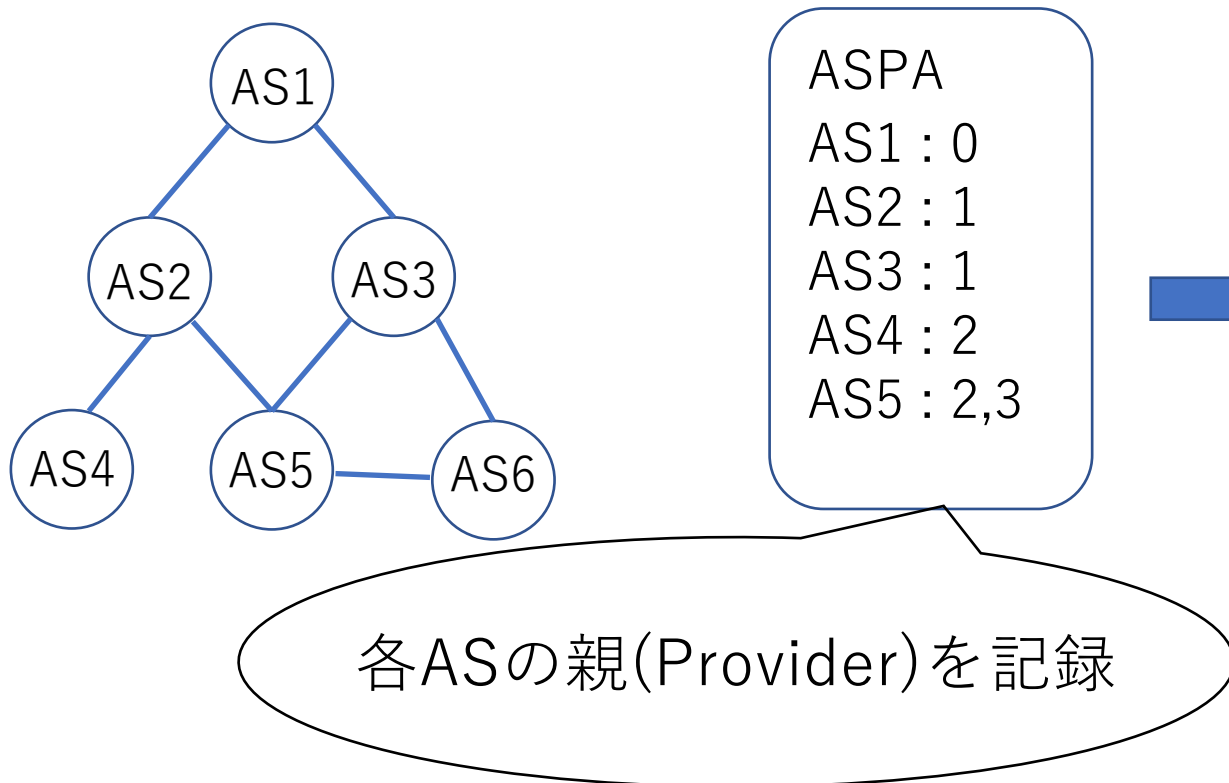
・ 悪意あるものによる **経路ハイジャック** が可能
实例：
・ Bitcoin ハイジャック [SBW14]
・ Facebook DNS 到達経路消失 [FB21]

-> 不正経路の伝搬防ぐ対策として **ASPA**

[SBW14] Hacker Redirects Traffic From 19 Internet Providers to Steal Bitcoins | WIRED <https://www.wired.com/2014/08/isp-bitcoin-theft/>
[FB21] Understanding How Facebook Disappeared from the Internet <https://blog.cloudflare.com/october-2021-facebook-outage/>

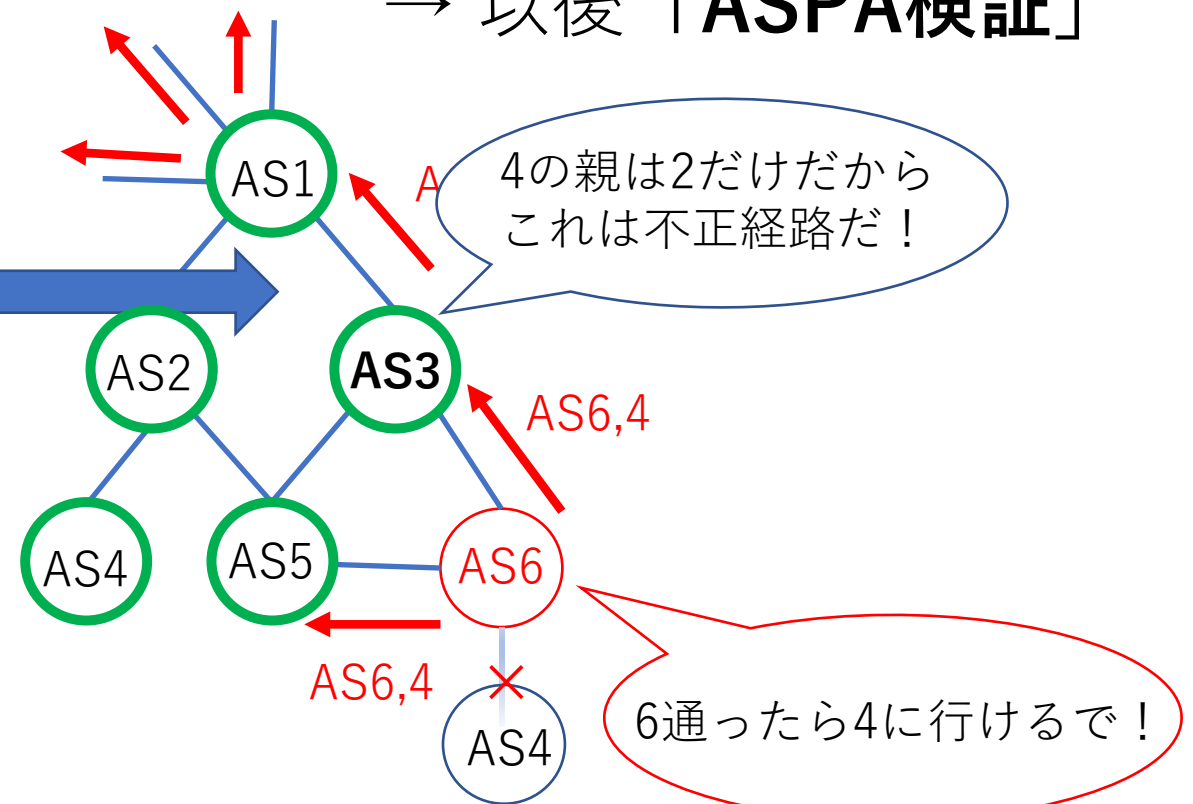
Autonomous System Provider Authorization (ASPA) [AER22]

ASPA = データオブジェクト



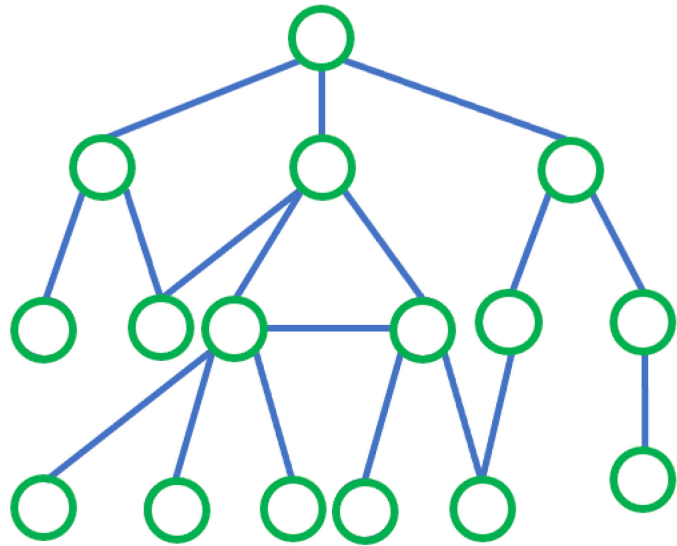
経路検証 → 「ASPAを用いた検証」

→ 以後「ASPA検証」

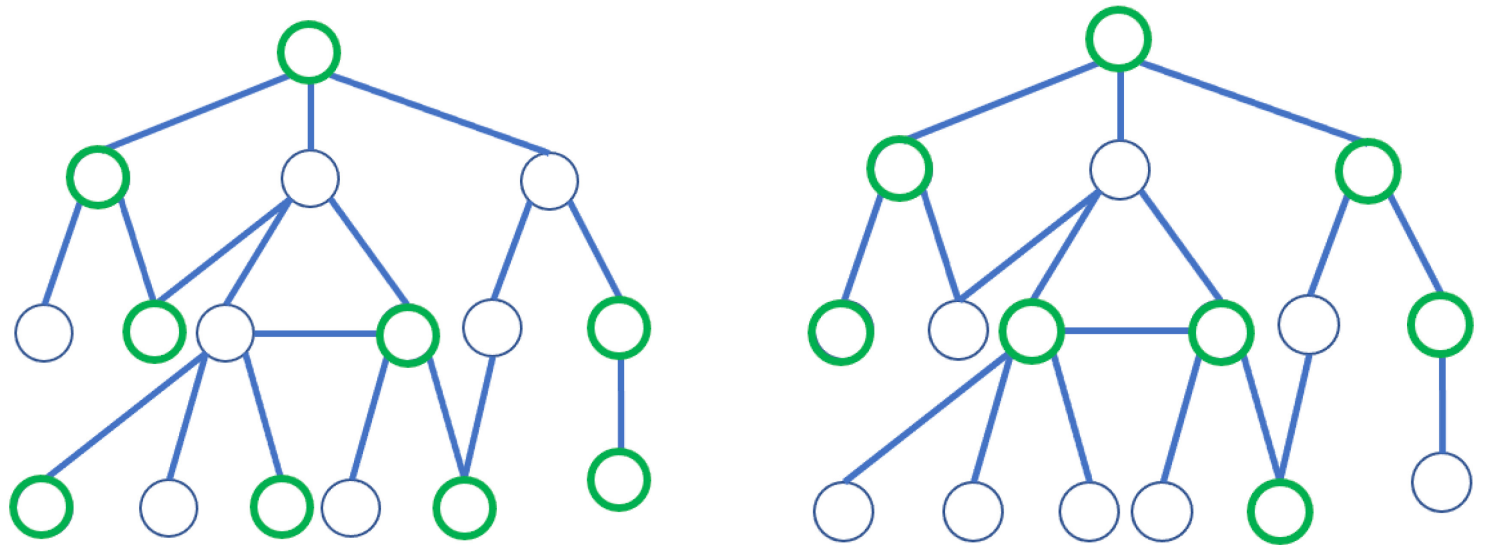


理想と現実

理想



現実



要因：BGPでは新しい技術を各ASが各自で導入する必要がある

- ・ 経済的な理由
- ・ セキュリティへの意識の低さ

段階的導入

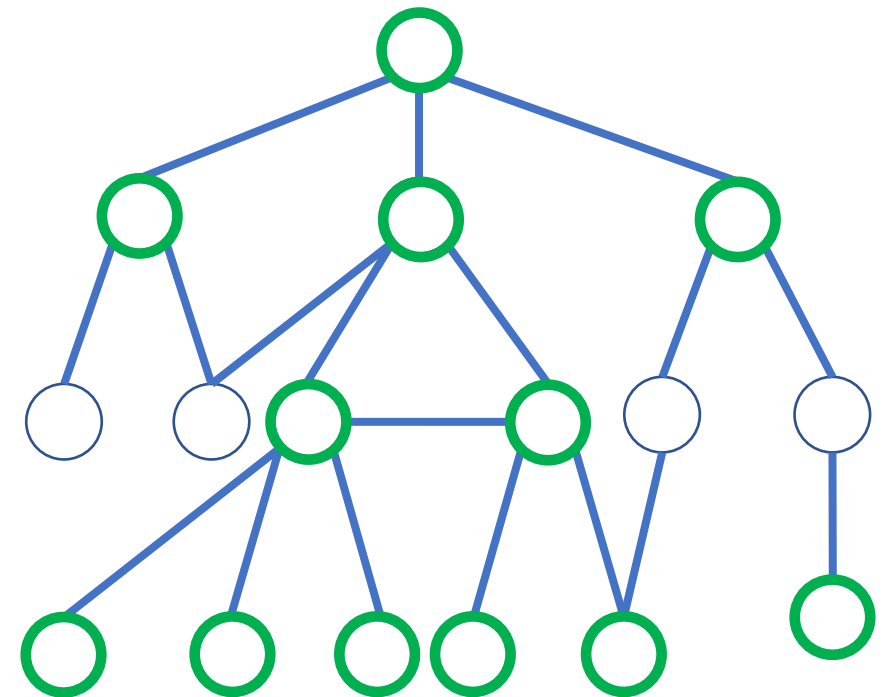
新しい技術が段階的にその導入数を増やしていくこと

現実世界への適用を考えると、ASPA検証が段階的導入に有効であることが重要

どのようなASに何ヶ所導入すれば
どれくらい効果があるか知りたい



もしかすると導入率が低いと効果が
ないかもしれない？



これまでの研究

- 既存の経路検証技術は段階的導入に有効性がないことが示された [LRSM13] → 普及に至らず
- ASPA [NTN23]
 - 日本のトポロジでASPAの段階的導入に有効性があることを示した
 - 末端ASへの段階的導入は効果がないことを示した [NTN23]

全世界には**10万個**以上のASが存在

→ 今後はより大規模なトポロジでのASPAの段階的導入の
検証が必要

[NTN23] Naoki Umeda, Taiji Kimura, and Naoto Yanai. The juice is worth the squeeze: analysis of autonomous system provider authorization in partial deployment. *IEEE Open Journal of the Communications Society*, 2023

[LRSM13] Lychev, Robert, Sharon Goldberg, and Michael Schapira. "BGP security in partial deployment: Is the juice worth the squeeze?." *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*. 2013.

これまでの知見

<運用上の観点>

- ASPA導入によって不具合が出るケースがある
 - 期待に反して不適切経路の伝播を防げないケース
 - 関連コンポーネントの障害や運用ミスが接続性に影響を与えるケース



ASPA の仕様を理解したうえでの運用が重要

<導入上の観点>

- BGPの特性から最短経路で経由されるAS(媒介中心性の高いAS)に導入した方が効果が現れやすいのは必然
- 接続数の多いASは媒介中心性が高くなる傾向があるため、ある程度の導入が進むとその差はなくなる



導入初期段階では媒介中心性の高いASに導入するほうが高い有効性を得られる

補足資料

本報告

<目的>

- ・ ASPAの大規模ネットワークへの段階的導入による不正経路の伝搬防止効果を明らかにする
- ・ より効果の大きいASPAの導入パターンを調べる

<手法>

実際に存在する大規模なネットワークトポロジでシミュレーション実験を行う

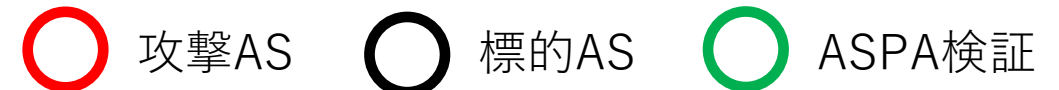
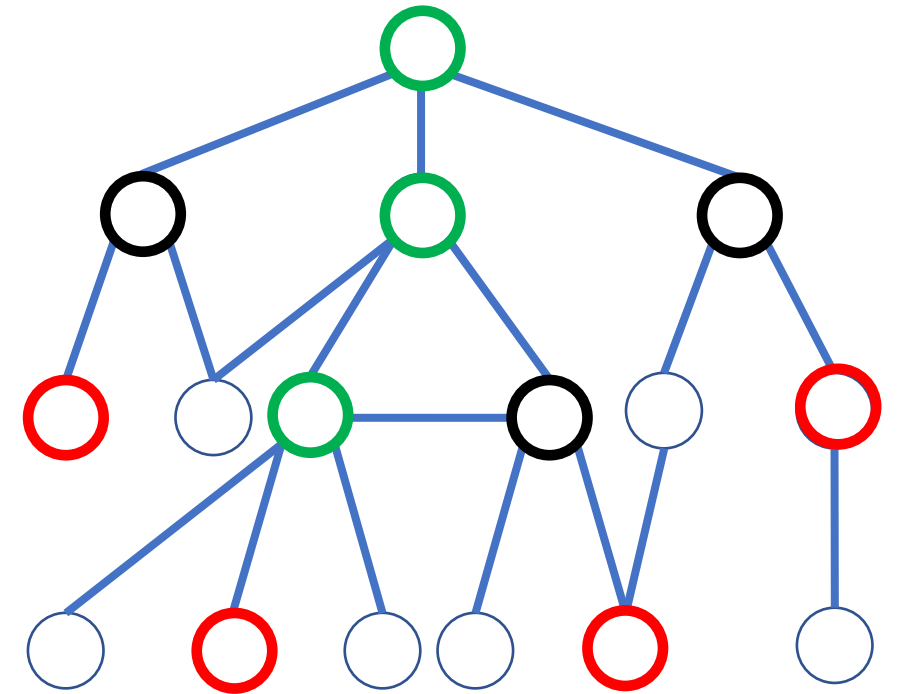
実験概要

<対象ネットワーク>

42531個のASからなるヨーロッパ全体の実在するネットワーク
(トポロジはBGPviewから取得)

<実験方法>

1. プログラム内でトポロジを構築
2. 攻撃ASと標的ASを決定
3. ASPA検証の導入ASを決定
4. 不正経路を広告
5. 被害ASを算出



実験設定 (攻撃設定)

<攻撃AS>

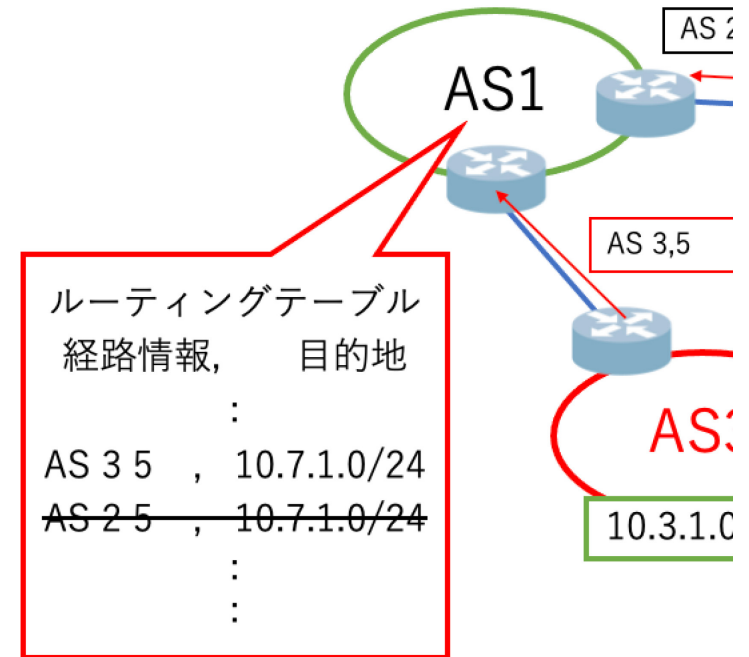
42531個からランダムに10個選ぶ

<標的AS>

42531個からランダムに10個選ぶ

<被害AS>

不正経路伝搬によってルーティングテーブルが変更されたAS



実験設定 (ASPA検証の導入パターン)

☆どこにASPA検証を導入するか

- **次数中心性** (既存研究 [NTN23] で扱われた)
他ASとの接続数によって評価される指標
接続数の多いASが次数中心性の高いASといえる
- **媒介中心性** (新たな指標)
あるASからあるASへの最短経路のながで経由される回数によって評価される指標
媒介中心性の値が高いほど、情報流通のなかにいることを表す

実験設定（有効性の評価方法）

<有効性>

a個のASPA検証を導入した時の有効性を以下の式で定義する

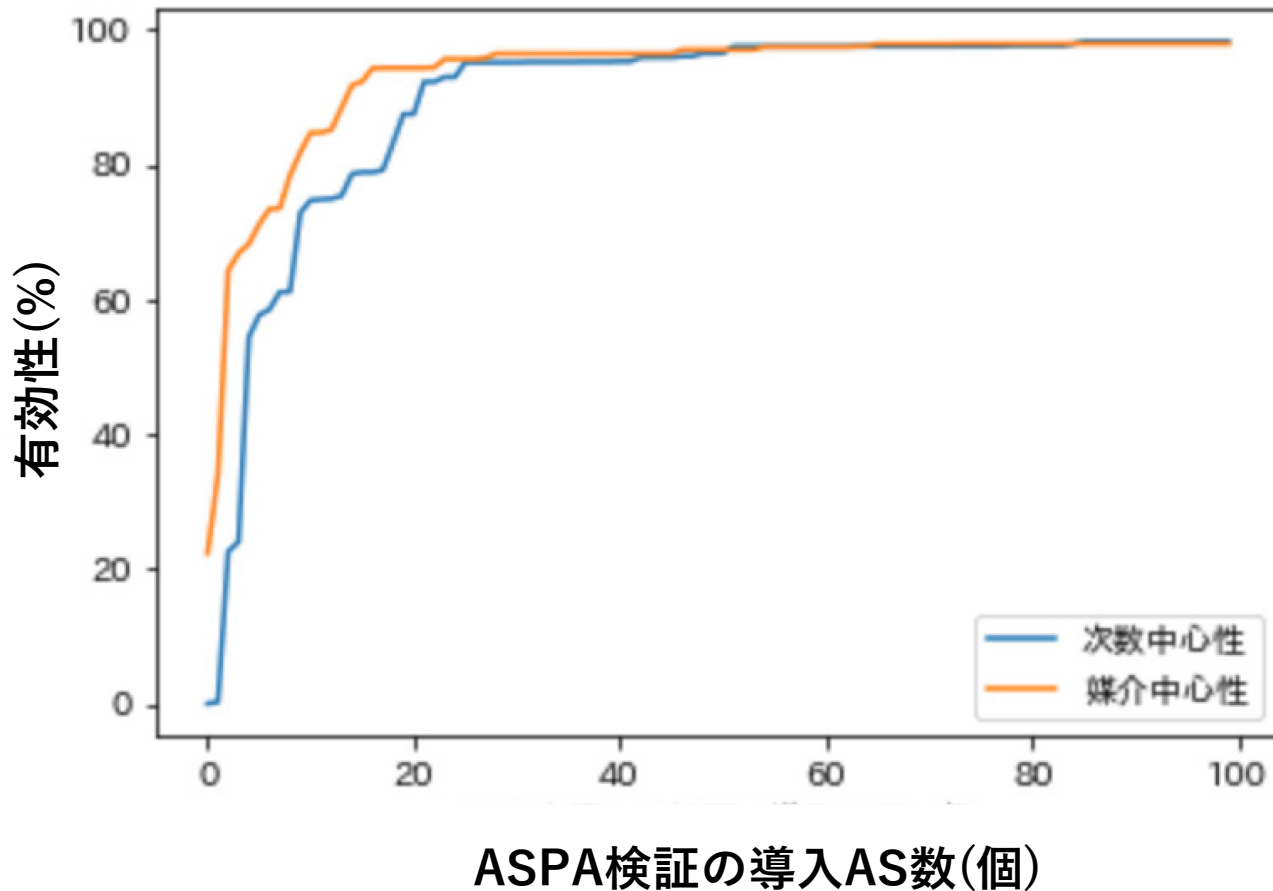
$$\text{有効性}(a) = \left(1 - \frac{\text{ASPA検証を} a \text{個導入後の被害AS数}}{\text{ASPA検証導入前の被害AS数}}\right) \times 100$$

☆簡単に言うと,, ,検証導入前と後でどれだけ被害ASが減ったか

<被害AS> *p10参照

不正経路伝搬によってルーティングテーブルが変更されたAS

実験結果



95%の有効性に必要な導入AS数

次数中心性：26個

媒介中心性：24個

段階的導入初期段階での有効性

次数中心性 < 媒介中心性