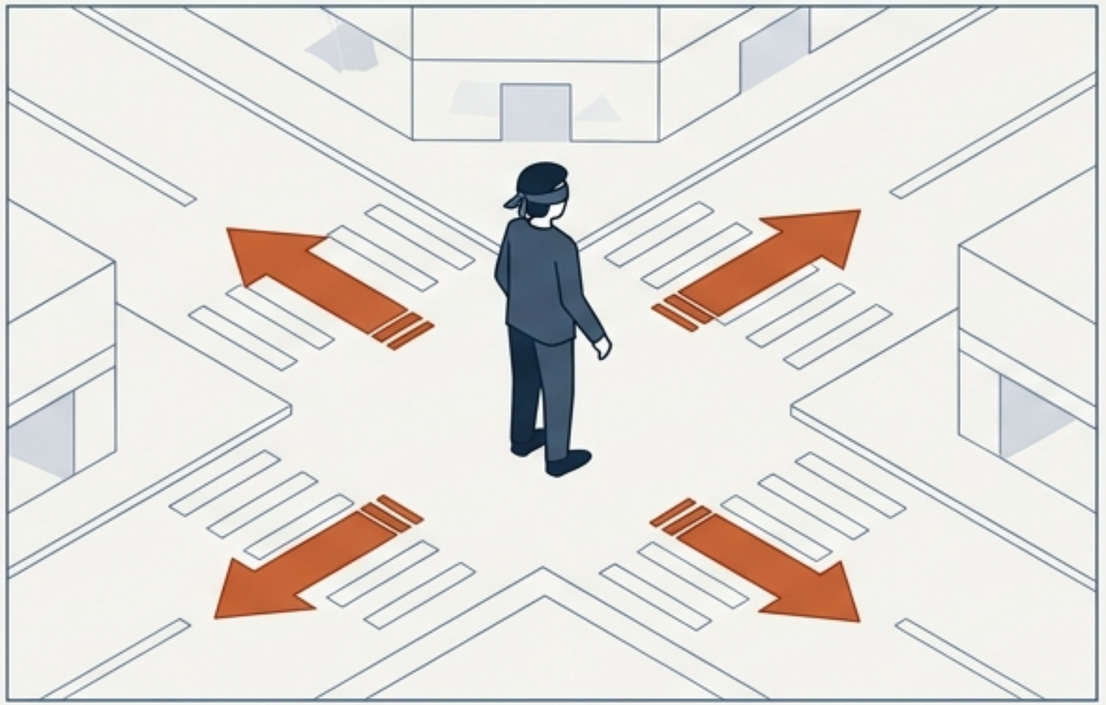
噂のネットワークを暗号化する

BGPの脆弱性、RPKIの実稼働環境、そして多世代にわたるルーティングセキュリティの軌跡

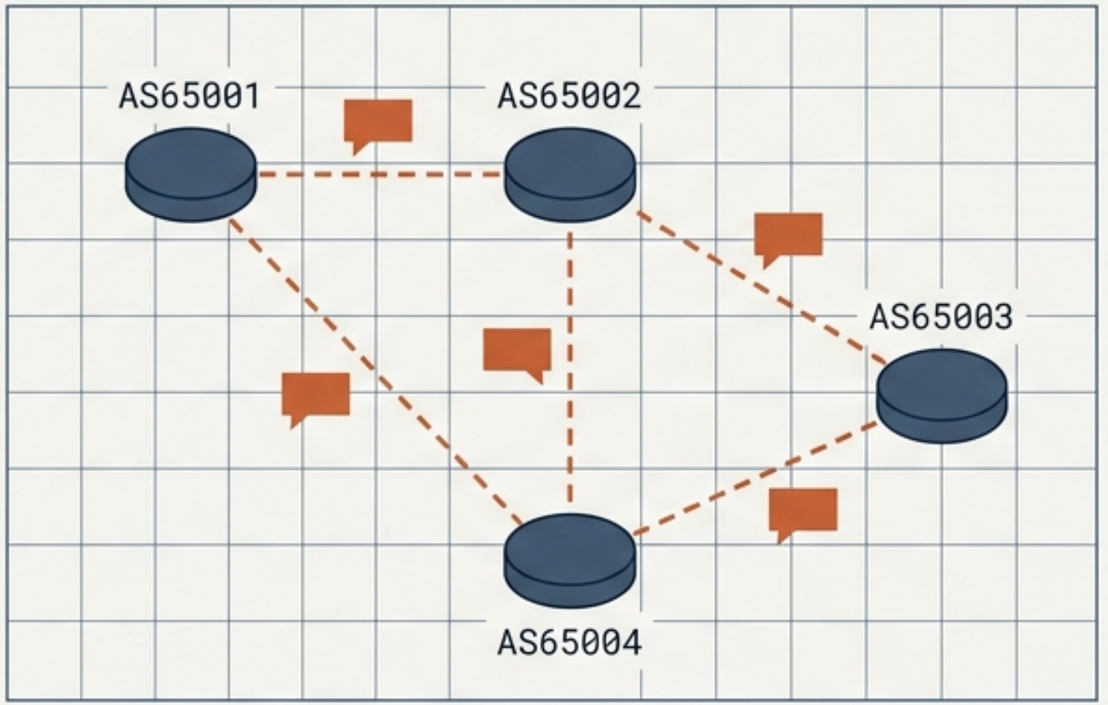
BGPには「絶対的な真実」が存在しない

目隠しでのナビゲーション



地図を持たず、周囲の指差す方向だけを頼りに進む

BGPルーターの現実

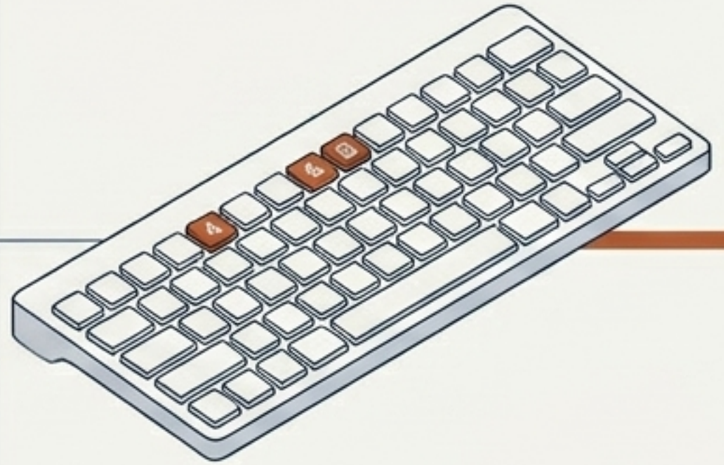


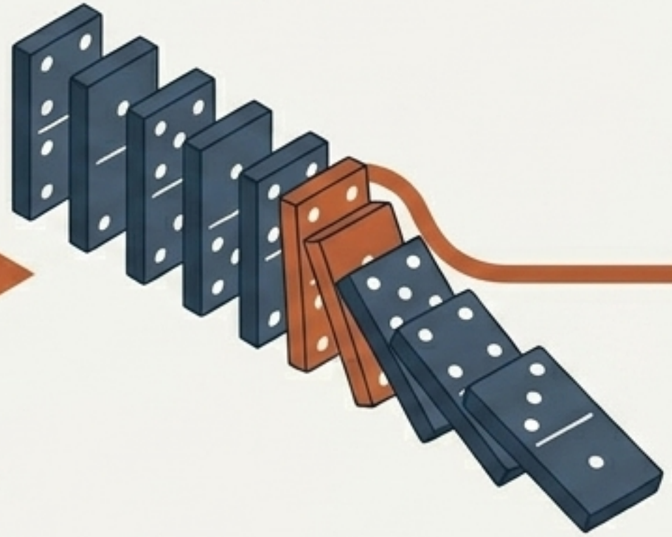
「真実の源」を持たず、隣接ルーターからの
「噂」のみを信じて経路表を構築

BGPには「絶対的な真実」が存在しない。全体を俯瞰する地図はなく、噂の伝播（Rumor Propagation）に依存している。

致命的な「タイポ」とドミノ効果

悪意あるハッキングよりも、運用デスクの安価なタイポが最大の脅威となる。





1. ヒューマンエラー (Fat Finger)

設定でIPプレフィックスを「48」から「84」へ打ち間違える

2. 噂の拡散 (Rumor Spread)

誤った経路情報がBGPを通じ世界中へ瞬時に伝播

3. トラフィックの消失 (Blackhole)

正規の通信が誤った宛先に吸い込まれ、世界規模の障害へ発展

変化するリスク環境：許容の時代から、規制と罰則の時代へ

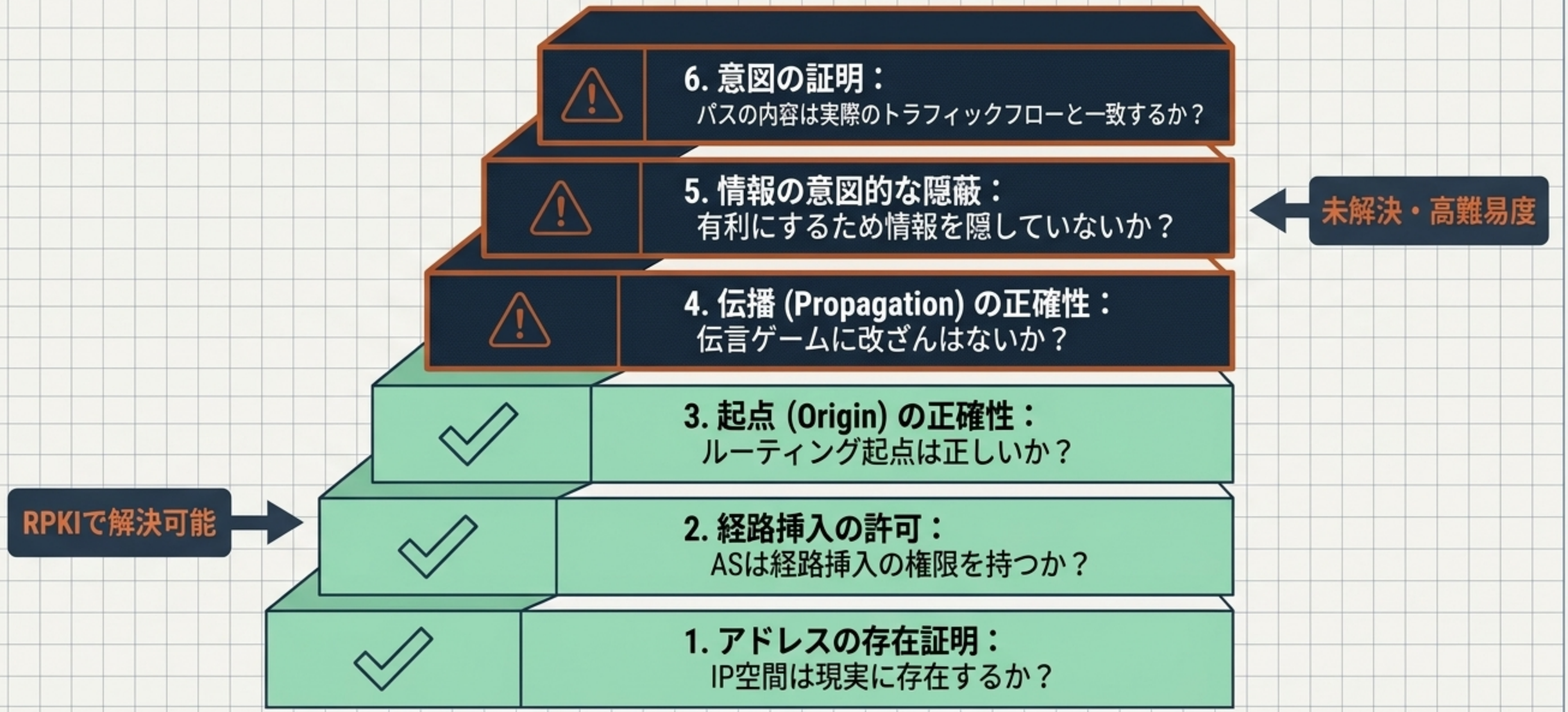
過去の文化：許容（Forgiving）

- 「お互い様」の精神
- 障害は起きるものとして許容
- インターネットはベストエフォートの実験

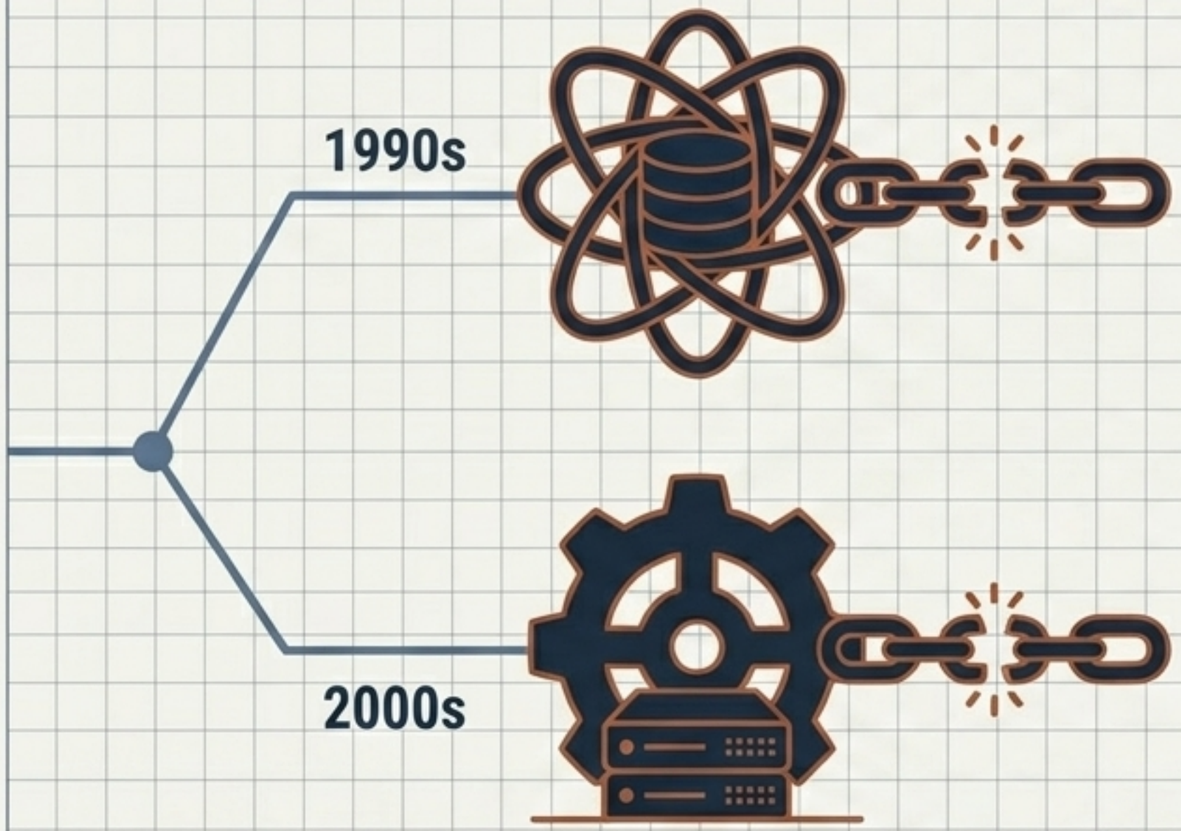
現在の現実：規制とゼロ・トレランス

- 緊急通報などライフライン停止への直結
- 規制当局の介入と巨額の罰金
- 「単なるミス」はもはや法的免罪符にならない

私たちが欲しいもの：ルーティングセキュリティの要件



歴史的失敗からの教訓：完璧主義の罠



IRR & RPSL (1990s)

- アプローチ: ポリシーを記述する中央データベース
- 失敗要因: 言語が複雑すぎた。真実の証明（権限監査）が組み込まれず破綻。

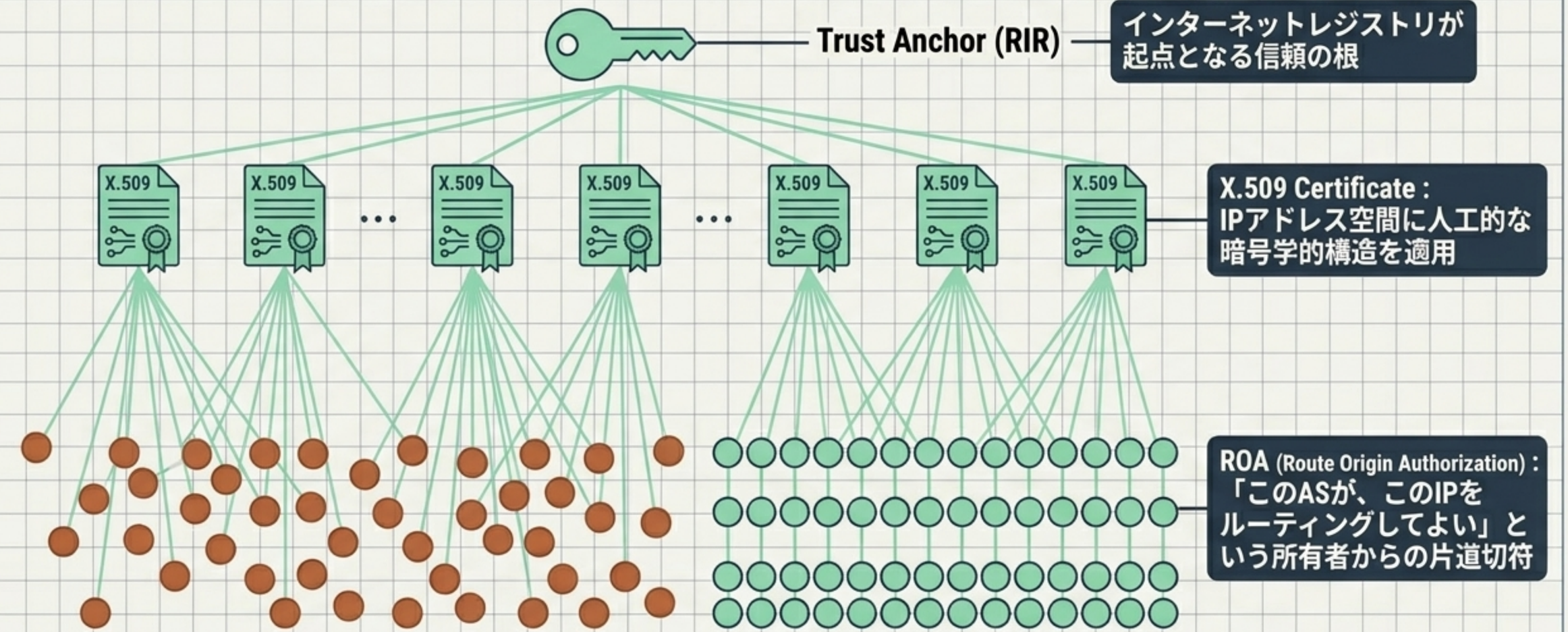
S-BGP (2000s)

- アプローチ: プロトコル全体に強力な暗号署名とパス検証を要求
- 失敗要因: 計算コストが膨大。全ルーターの同時導入が必須であり非現実的。

インターネットには中央管理者がいない。
誰もが同時に導入しなければ機能しない技術は、絶対に成功しない。

パラダイムシフト：RPKIの誕生

階層のないIPアドレスの世界に、デジタル署名による「真実の証明」を構築する



RPKI ROV（経路起点検証）のメカニズム

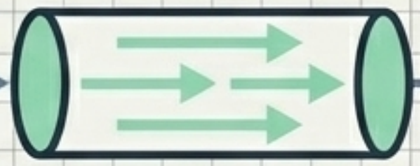
1. 発行 (Publish)

IP所有者がROAに署名し、分散リポジトリに公開

2. 収集と検証 (Validator)

ネットワーク外のキャッシュサーバーがROAを収集し、暗号学的検証を実行

3. 同期 (RTR Protocol)



検証済みの軽量なデータのみがBGPルーターへ送信される

4. フィルタリング (BGP Router)

ルーターは受信したBGPの「噂」を検証済みデータと照合し、不正な経路を破棄

ソリューションの進化とトレードオフ

テクノロジー	起点検証 (Origin)	経路検証 (Path)	計算コスト	導入の現実性
S-BGP	○ 完璧	○ 完璧	✕ 極めて高い	✕ 廃案
RPKI ROV	○ 良好	✕ なし	○ 低い (外部処理)	○ 広く普及
BGPsec	○ 完璧	○ 完璧 (暗号ベース)	✕ 高い	✕ 困難・限定的
ASPA	○ 良好	◐ 良好 (関係性ベース)	◐ 中程度	○ デプロイ進行中

BGPsecの「計算コストが高すぎる」問題を、ASPAは「暗号ではなく、AS間の関係性に基づくパス検証」で現実的なコストに抑えた。

RPKIの正体：「ルーティングプロトコル」ではない

誤解：RPKIはルーターの中で動くルーティングプロトコルである

現実：RPKIは地球規模の巨大な分散型データベースである

⚠ ・データの一貫性 (Consistency): 地域のノード間でレプリケーションの遅延と不一致が発生
⚠ ・レイテンシのブレ: タイポを修正しても、その修正が世界中に伝播するまでに時間差が生じる
⚠ ・新たな脆弱性: データベース自体が、ルートハイジャックのための新たな標的（攻撃ベクトル）となる

巨大なスケールと絶え間ない変動（Churn）

500,000

グローバルデータベースの総オブジェクト数

180,000 / 日

1日に変更（追加・削除）されるオブジェクト数

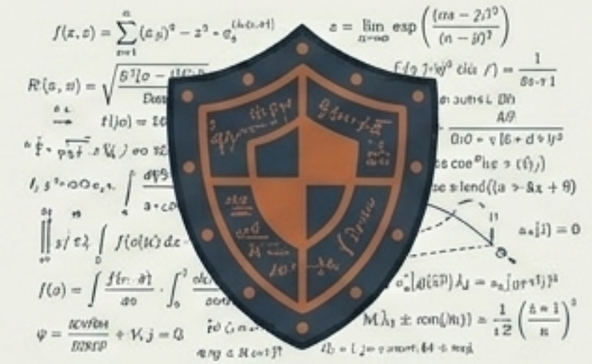
2 / 秒

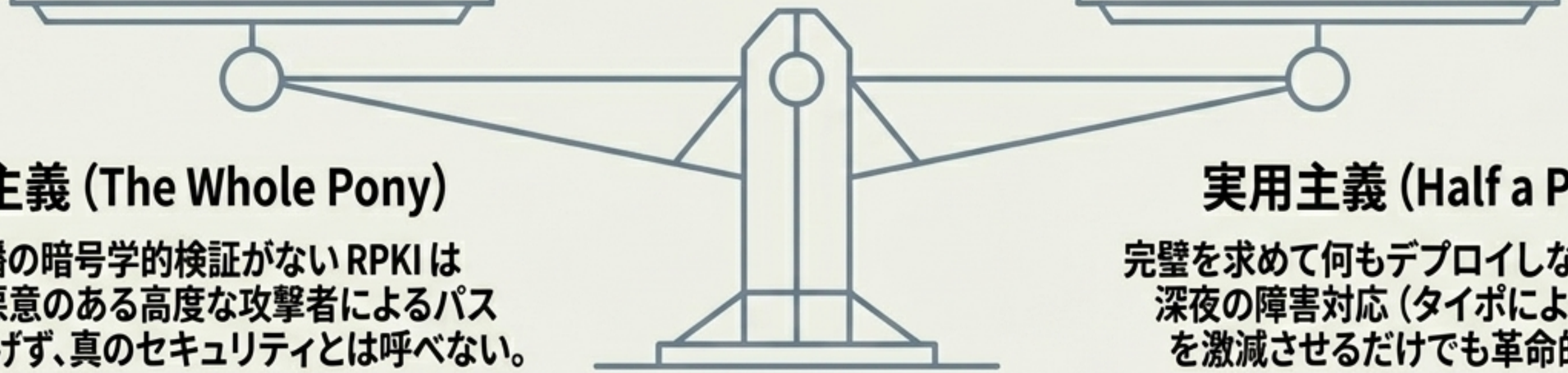
毎秒、地球上のどこかで生まれる新しいオブジェクト

巨大なスケールと絶え間ない変動（Churn）

この膨大な変更をいかに効率的に同期するか？現在、歴史的妥協であった「Rsync」から、スケーラブルな「RRDP」への移行という、飛行中の飛行機のエンジンを交換するような作業が進行している。

セキュリティの哲学：純粋主義 vs 実用主義





純粋主義（The Whole Pony）

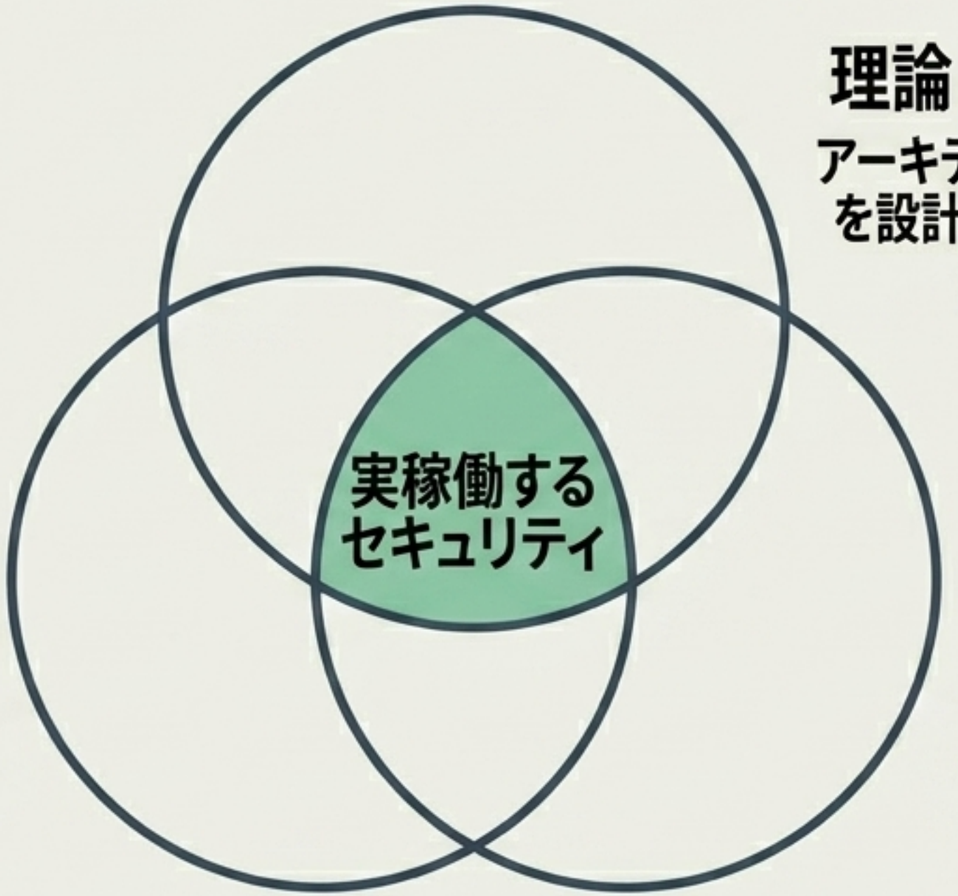
経路伝播の暗号学的検証がない RPKI は不完全。悪意のある高度な攻撃者によるパスの偽装は防げず、真のセキュリティとは呼べない。

実用主義（Half a Pony）

完璧を求めて何もデプロイしないよりマシ。深夜の障害対応（タイポによる大事故）を激減させるだけでも革命的である。

現在の現実解：実用主義（ROV）で実行可能な基盤を作り、その上に段階的に次世代の防壁（ASPA）を構築していくアプローチ。

ルーティングセキュリティを成立させる「3つの柱」



理論 (Theory)
アーキテクチャと暗号
を設計する理論家

コード (Code)
仕様をソフトウェアとして
実装を作て
実装する開発者

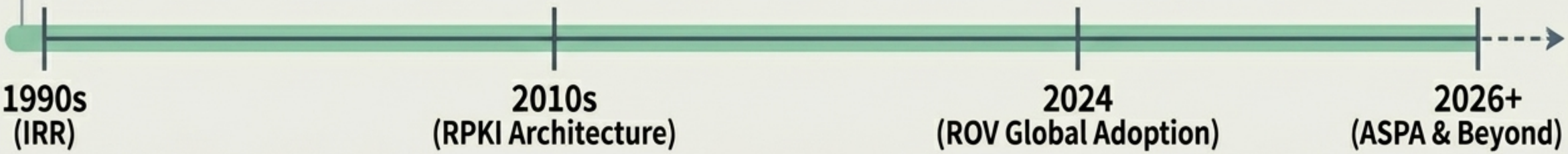
運用 (Operations)
運用 (Operations)
現場の制約を理解し、
請求書を支払う運用者

この3者のうち、どれか1つでも欠ければプロジェクトは失敗する。
現場の運用者の同意と「動くコード」なしに、机上の空論を標準化してはならない。

結び：多世代にわたるプロジェクト

インターネットのルーティングセキュリティは、1〜2年で完了するソフトウェアアップデートではない。
それは30年前に始まり、最初の設計者から新しい世代へと引き継がれる「多世代プロジェクト」である。

- 忍耐: 変革には数十年単位の時間が必要であるという現実の受容
- 相互信頼: 分散された自律システム間での、互いのアーキテクチャへの信頼
- 継続: 完璧なゴールが遠くとも、歩みを止めずインフラを改善し続けること



噂のネットワークは、ゆっくりと真実のネットワークへと変わりつつある。