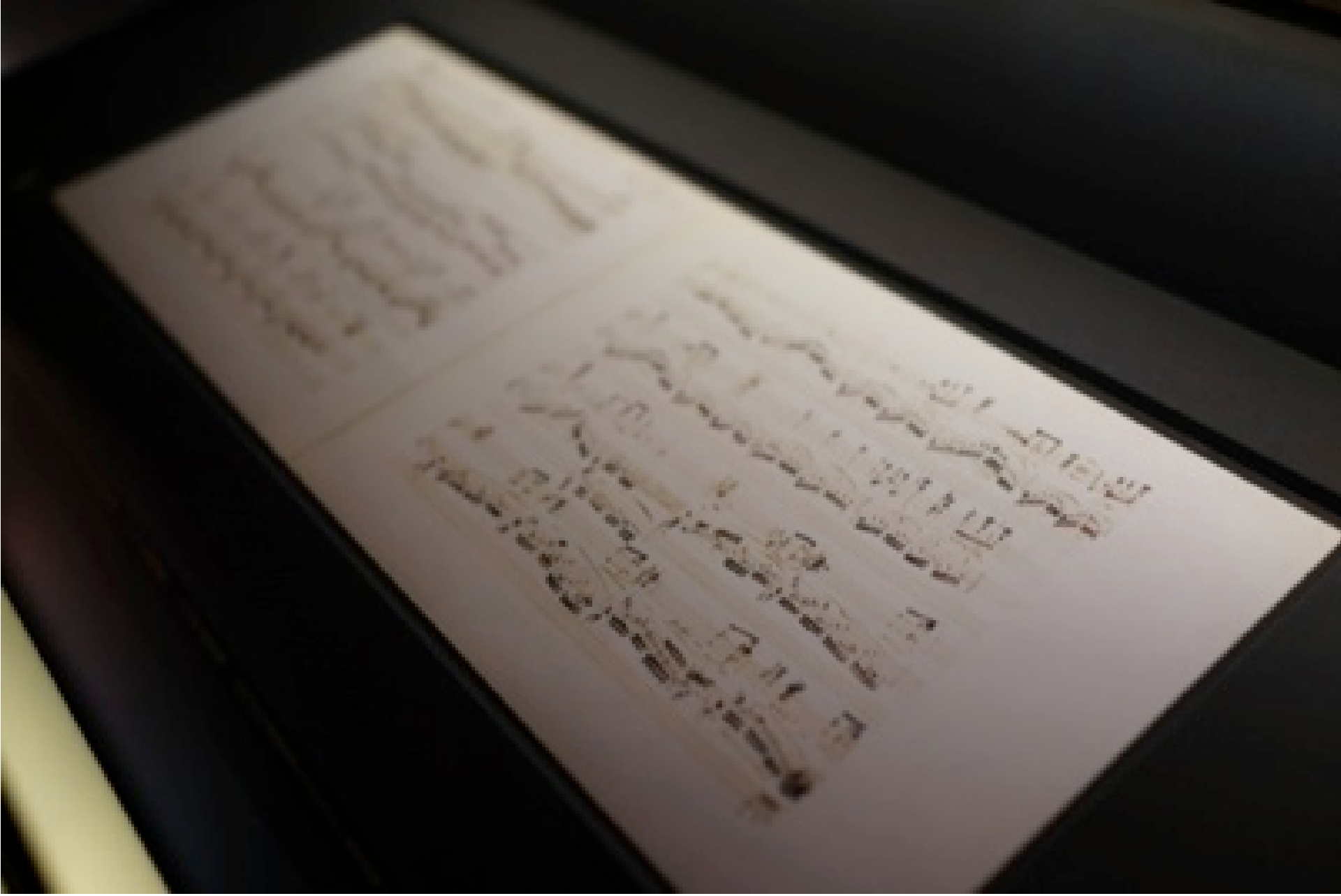
インターネットルーティング セキュリティのマインド

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>



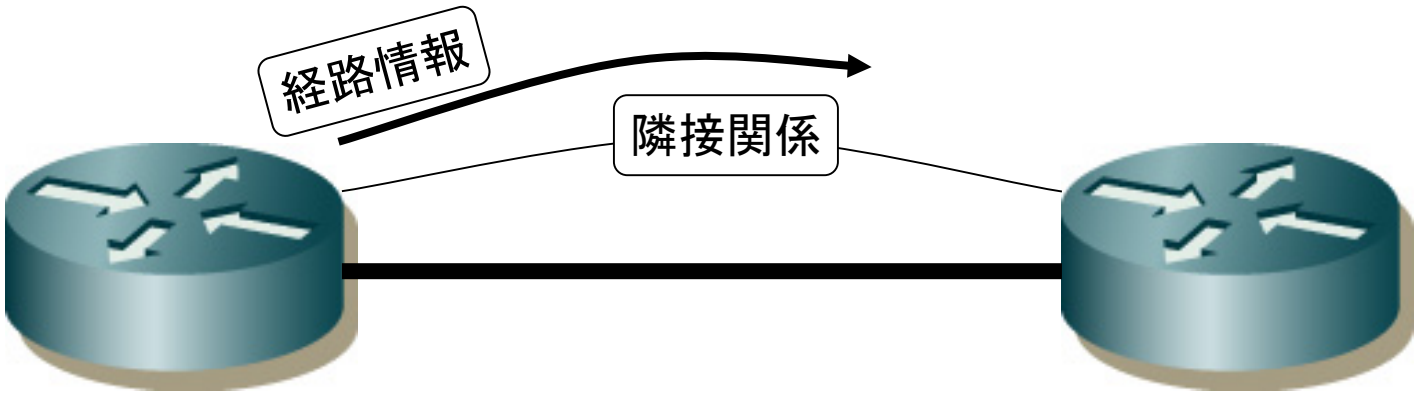
守りたいモノ

- ユーザがよろしく通信できる環境
  - 環境を作ってるのが経路制御
- 経路制御を守らなきゃいけない
  - サービス/事業が継続できる
  - より面白いアプリケーションが出てくる
  - みんな幸せ

何から守るか

- 心配しだすとキリがない
  - 費用対効果
- 段々心配事は増えていく
  - 時代に応じたちょうど良さが求められる
- 現実的な範囲を押さえていく
  - 技術的に可能な程度
  - 世の中で実装されている程度
  - 意図した経路制御を維持できるように

一般的な経路制御



- 何らか隣接関係を利用して、経路情報を交換

経路制御全般の脅威

- 隣接関係
  - 間違った隣接関係が構築される
  - 勝手に切断される
  - なりすましに騙される
- 経路情報
  - 間違った経路情報が流れる
  - 意図しない経路制御になる
  - 機器の処理能力を超える

BGPの隣接関係

- TCPセッションを頑張って守る
  - md5認証
  - IPSEC
  - GTSM(Generalized TTL Security Mechanism)
    - IP TTL 255のパケットで隣接だと判断
- 今のところ、md5認証が多用されている
  - 完全性や機密性より、とりあえずの認証
- 他組織と接続するときに事前の交渉ができる

BGPは経路情報のほうが問題

- 今時はほとんどの経路情報をBGPで処理
  - 経路制御の多くを担う
- しかも他の組織と経路情報を交換する
  - 直接の接続先は知っている
    - でもその先は知らない組織
  - 信頼できない組織からの経路情報も受け取る

網内で死守すべき経路情報

- ピアを張っているIPアドレス
  - 大抵の場合、IGPでも広報
    - 同じprefix長であればIGPが優先される場合が多い
- BGP経路のnexthopになっているIPアドレス
  - 絶対に外部から受け取ってはいけない
  - 全eBGPで確実にprefixフィルタを実装
    - more specific経路にも注意
  - bgp nexthopになりうるIPアドレス
    - 経路を生成しているルータ
    - 相互接続アドレス
      - IXやプライベートピア

問題はASの外

- 何せユーザは“インターネット”を期待する
  - 僕だって期待する
- 手の届かないところで制御されている経路
  - 他のASが受信している経路
  - 他のASから広報されてくる経路

他のASが受信している経路

- 自身のprefixが別なASから広報された場合
  - それを最適経路だと思ったASとは通信できない
    - more specific
    - as_path長で近傍に見える
  - 検出には他のASの協力が必要
- メールや電話で連絡して、広報停止を依頼
  - IRのwhois情報などでこちらの正当性を主張する

他のASから広報される経路

- 正当性の確認が難しい
  - 正当性の根拠として使える情報が無い
    - RADBなどは、不正確な登録情報が多い
    - JPIRRのみが抜群に頑張ってる
      - 次点はRIPE DBかなあ
  - RPKIによるorigin AS検証が使えるかも
- どこまで確認したいかも問題
  - 実装するなら、ある程度の期間は安心していたい
  - AS path検証とか

利用できる技術

- 正当性の維持
  - IR, IRRに登録した情報の整備
  - 将来は、さらにRPKIを利用した広報
- ポリシの実装
  - 経路フィルタ
  - 将来は、さらにRPKIを利用した検証
- 異常の検出
  - 経路奉行、トラヒック変動

まとめ

- まずは自分のできる範囲を
  - 自身の経路制御ポリシを守る
  - 自身の広報/トランジットする経路はばっちり確認
  - IRやIRRなどの登記情報もきちんと更新
- 世界を巻き込んで、みんなでインターネットの経路制御を良くしていくことが課題