# インターネット
# ルーティングセキュリティ
# ～の心構え～

Internet Week 2015

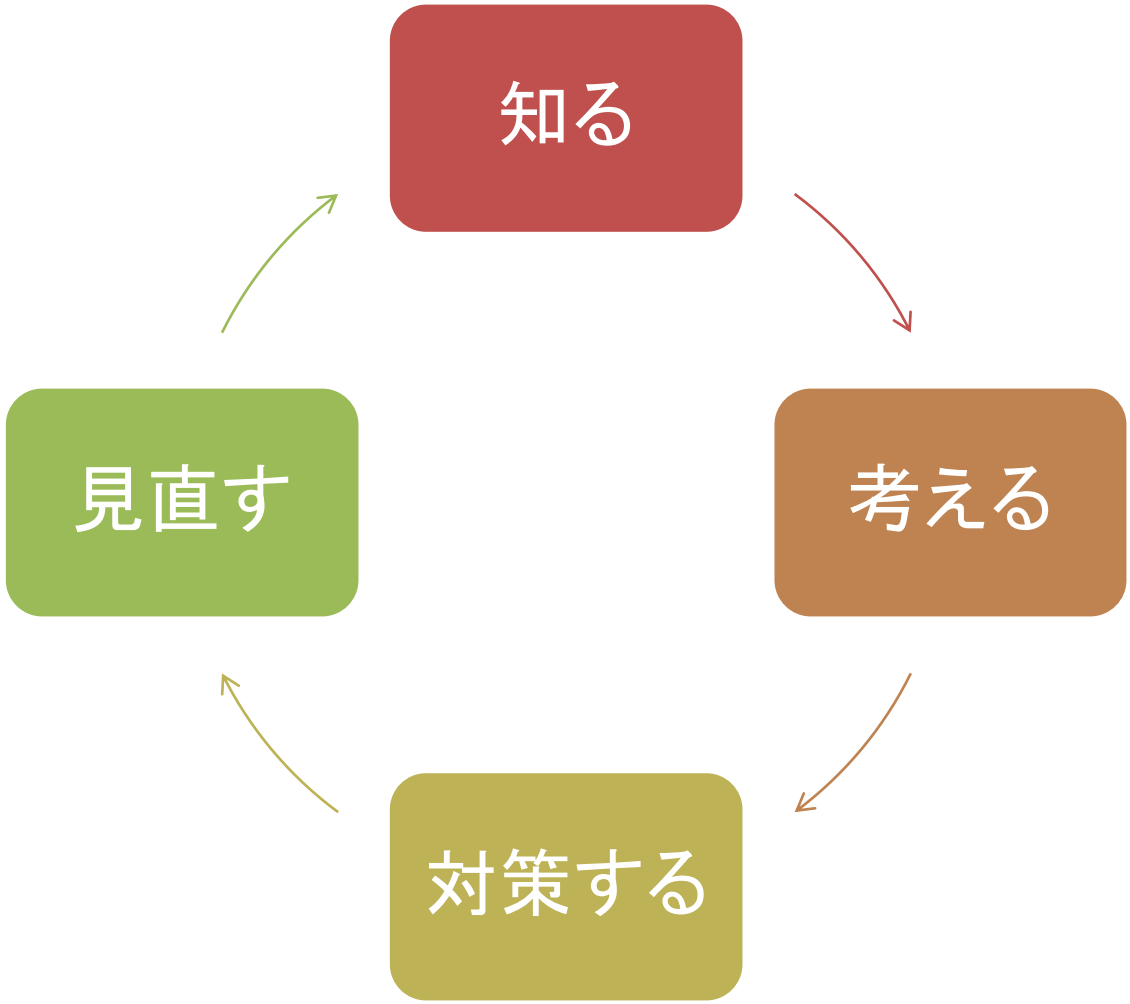
BIGLOBE Inc.
Seiichi Kawamura
kawamucho at mesh.ad.jp

# インターネットルーティングセキュリティの特徴

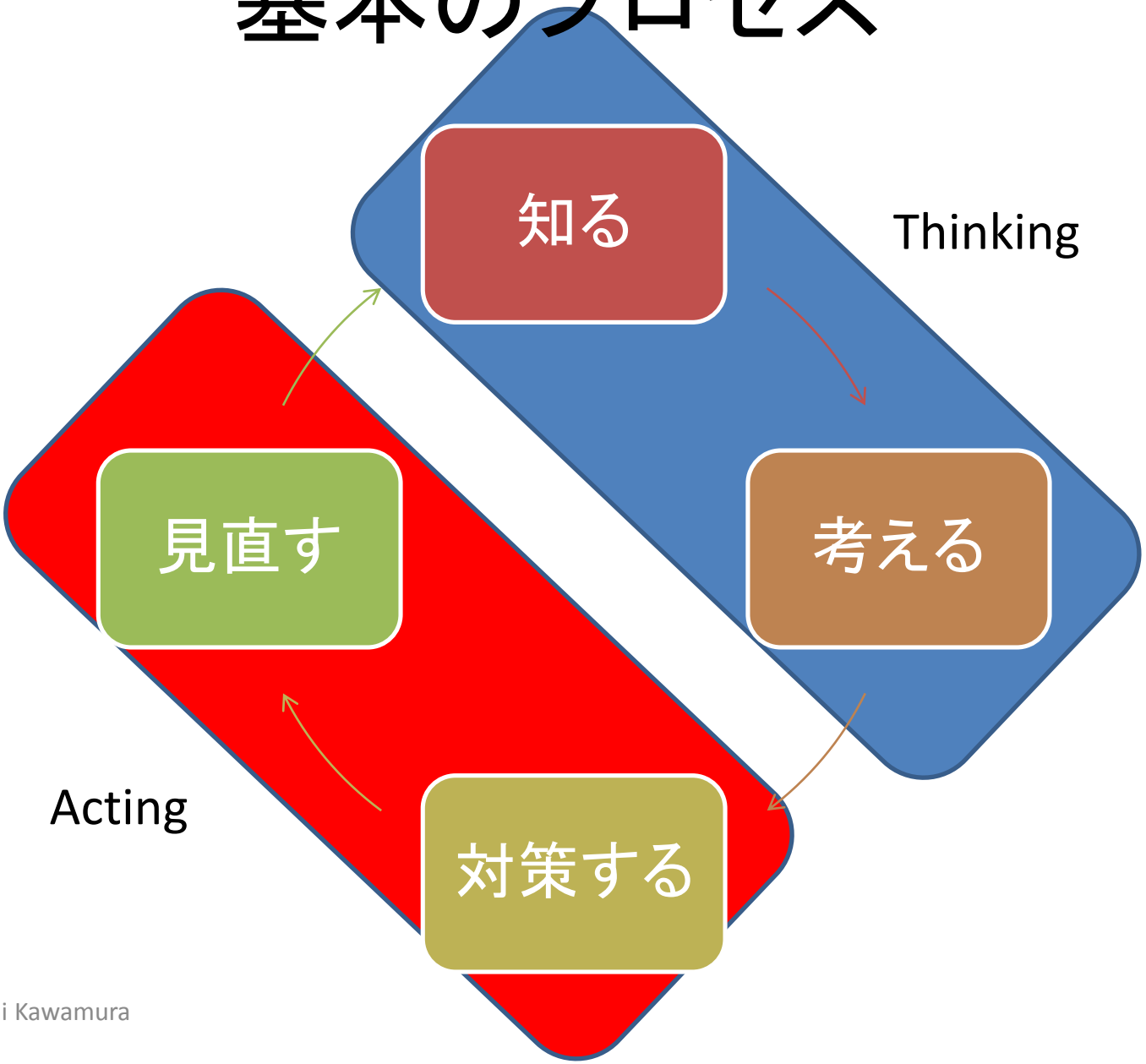
- 教科書は無い
  - つまり、本で勉強する事はできない
  - インターネットのように、常に変化しているもの
- 歴史を綴る事はできる
  - 「インターネットのカタチ」あきみち・空閑洋平著
- 過去事件、セキュリティに関するプレゼンテーションは多数存在する
  - 今日のお話もその一つ

時代とともに変わらない根本的な「心構え」とは何だろう

# 基本のプロセス



# 基本のプロセス



# Thinkingで大事なのは

頭は低く
アンテナは高く

# Actingで大事なのは

覚悟を決める

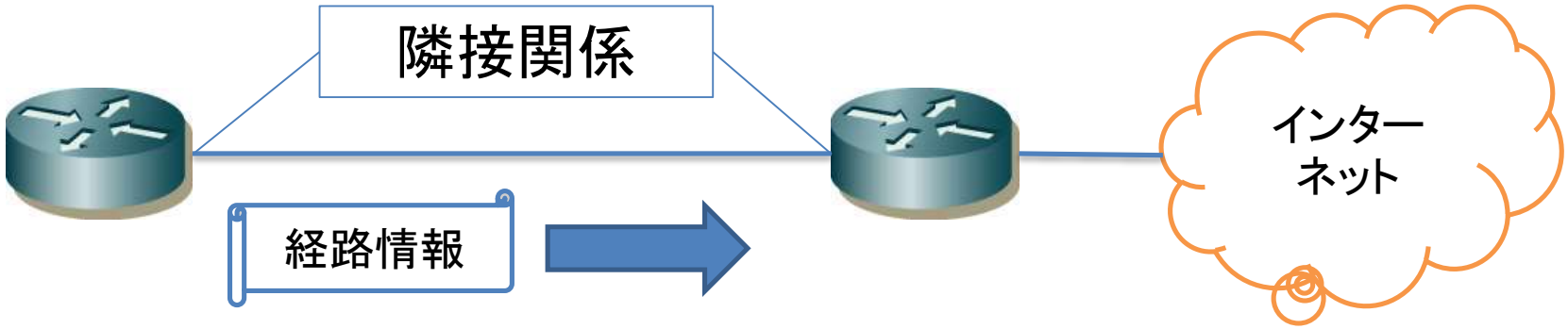
# バランスは重要

- 100%の防御策を打っても、ユーザ通信に不具合まで出してしまうのは本末転倒
  - ユーザがちゃんと通信できるように経路交換をやっている事を忘れてはいけない
- でもセキュリティをしっかりやることで
  - 安心して使えるInnovationの基盤を提供する
  - サービス、事業の継続性を守る
  - みんなが楽をできるようになる

何のためにやるか、を意識する事でルーティングセキュリティに関するポジティブなサイクルを生みだす

実際「インターネットのルーティングセキュリティ」というテーマではどういう脅威を考慮する必要があるのだろうか

# 個別の要素にブレイクダウン




① 隣接関係(Peer)

② 経路情報とパケット転送

③ インターネット(Transit)

# ①隣接関係

- 経路を受信するためのセッション
  - これが落ちると経路がそもそももらえない
  - 不安定状態でもユーザ影響は出る
- 一般的に、異なる事業者との隣接関係はBGP
  - 不思議な特性
  - 不正なパラメータを受信すると落ちる
- 脅威
  - なりすまし・意図しない隣接関係
  - 不正なパラメータ
  - 遠隔からの179port攻撃

# ②経路情報

- 到達性を確保するための情報
  - 自分の経路を相手に覚えてもらう
  - 相手の経路を受けて到達性を確保する
- 脅威
  - 不正な経路を受けて(または出して)しまう
    - 意図しない第三者にパケットを渡してしまう
  - 自分の経路を第三者に不正に広告される事により到達性がなくなる
    - 自分のユーザにとってサービス断

深刻！

# ②パケット転送

- ルーターは、一般的に宛先を見てパケットを転送する
- 正しい経路情報があっても、送信元が不正の可能性が高いパケット（例えばソースIPがプライベートIPだったり）はどこかしらにセキュリティ問題を引き起こす原因となる可能性が高い

# ③インターネット

# ③インターネット

- 不正な経路情報は簡単に伝搬する
- インターネット全体に対して伝搬する事もあれば、適切なセキュリティ措置により伝搬を最小限に防ぐ事もできる
- 自分の経路じゃなくても、自分の隣接関係じゃなくても、インターネットのどこかでセキュリティ問題が発生するとユーザ影響が出る
  - Youtubeが見れない、など
  - 問題：経路広報の正しさを証明する事は極めて難しい

# インターネットには色々な人（経路）がいる

- 常にIGP経路もBGPで出してくる人
  - なぜなのか聞いても「すみません、変えられません」としか答えがない。多くの場合は無視される
- 直接Peeringしないと見えない経路
  - Tier1には広告されないローカル経路
  - 通信ライセンスと検閲が絡んでいると（私は）推測
  - この経路がもれてくると突然トラフィックが増えたり、特殊な経路フィルターを書かないといけなかったりする

# インターネットには色々な人（経路）がいる

- 「適切なフィルターを実施していないTransit事業者」は実は珍しくない
  - ルーティングポリシーは、ビジネス判断や、政治判断で左右される
  - 例：経路updateがやたらと多い顧客+設定が自動化されていないISP+利益スレスレの営業＝フィルタ放置につながりやすい
- DDoS Protection ServiceがBGPで細かい経路を送ることでトラフィックを吸い込み一時的にTransitになる、というようなケースもある
  - 悪いことではないが、事業形態を知っているとその事業者に流れるトラフィックがよくわかる

# 日常の備え

# Thinking:

情報網を広げておく:

メーリングリスト: janog@janog.gr.jp, nanog@nanog.org, outages@outages.org ….

BGP neighborと仲良くなっておく

常日頃から経路テーブルを見ておく

社内外で、経路やルーティングセキュリティについて話し合う機会を設ける

たまには海外動向も気にする

# Acting:

- ルータのコンフィグみなおし
  - 隣接関係：MD5、IPsec、firewall (*次頁参照)
  - 経路情報：適切な経路フィルターポリシー
- データ参照ポイントの利用
  - IRR (RADB, RIPE,  etc)
  - Route Views / RIPE RIS　などの外部経路テーブル
  - Looking glass、NLNOG RINGなど調査ツール
  - 経路奉行　などの検知システム
  - Origin validation looking glass
- インシデント発生時の対応手順の用意
- 対処設定の事前準備
- 訓練の実施

# 昨日の常識は今日の非常識？

- 以前BGPセッションにMD5を付与するケースが多かったが、最近では有効性の低く、かつ通信不具合を発生させる可能性がある、として見直されている
- 経路とASの数が増えると共にAS-PATHを利用した経路フィルター更新はポピュラーでなくなり、Max Prefixでの制御が人気になりつつある
  - 両方ー長ー短だが、経路増とコスト考慮の結果の流れ
- ー律/24より長い経路を落とす設定をして安心、、、ではないかもしれない
  - RIRから受ける最小割り振りサイズ(IP アドレスブロックの大きさ)は定期的に変更になっている
  - 最近北米では23.128.0.0/10のアドレス帯では/28が最小割り振りサイズとなるようポリシー変更が行われたが、経路フィルタへの影響は未知数

**「対策」の有効性と価値は時間とともに変化する**

# しかしどんなに準備しても、インシデントはいつか起きる

- インターネットのルーティングの特性上、防げない事象は実際かなり多い

- 起きてしまった時は
  - 担当者を責めない
  - 急いでも、焦らない
  - 適切な範囲に情報共有する
  - 必要なら周り（社内、他社）に助けをもとめる事を躊躇しない
  - 収束した後、対策を見直す

基本行動をやっていれば、その時が来ても適切な行動がとれる

# 自分のネットワークがインシデントの元になってしまうことも

- なるべく自分のミスを防止してくれる経路フィルター設計

- Transitサービスを提供しているなら、顧客の経路広報ミスを拡散しないようなフィルター設計とフィルター更新業務設計

攻撃者にならない為の策は後回しにされがち

# 心構えまとめ

- 情報を収集し、自分には何ができるか、今何が適切なのか、古びたポリシーはないか：Thinking
- 具体的に対策を講じて未然に事故を防ぐファインプレー、インシデントが発生した時にすぐ行動できるファインプレー：Acting
- そして隠れたファインプレーを「研ぐ」ため再びThinking活動
- 正解はない、だから日常行動の一部に取り込み、常に考えながら策を見直し続ける
- 重要性を関係者/社内で語り合い、活動の「意義」を見いだす

# おしまい