インターネットルーティング セキュリティ入門 ～心構え編～

Internet Week 2011

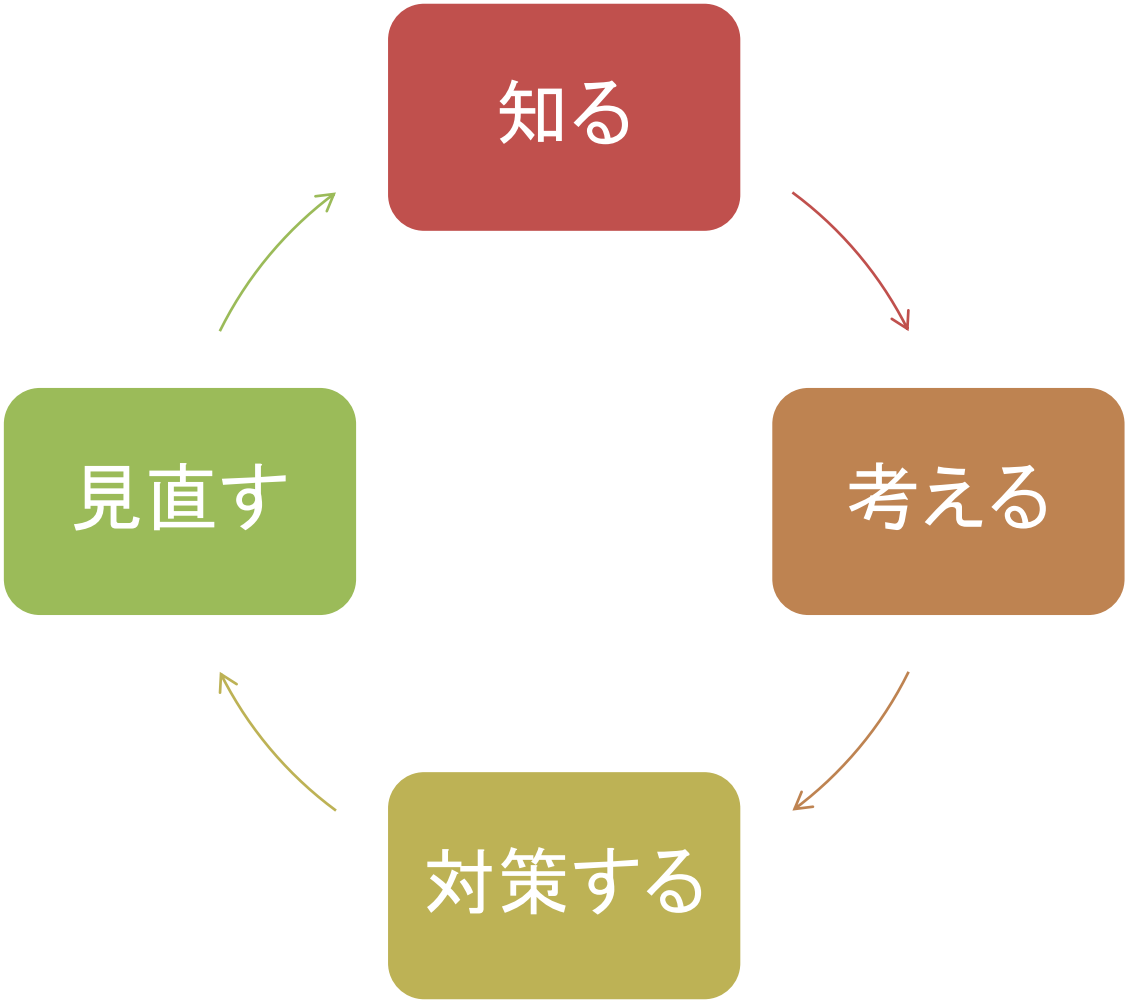
NEC BIGLOBE, Ltd.
Seiichi Kawamura
kawamucho at mesh.ad.jp

インターネットルーティングセキュリティの特徴

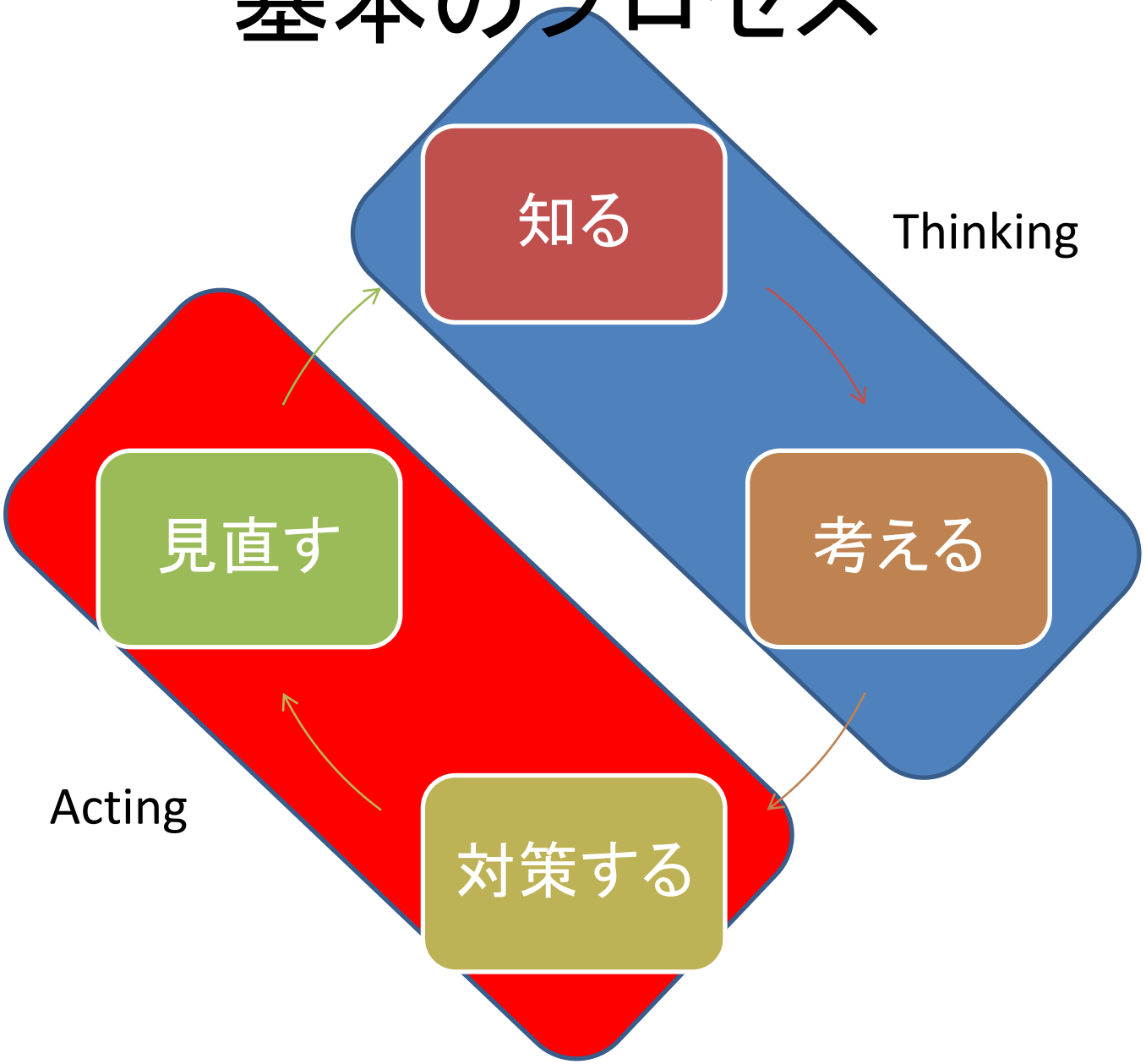
- 教科書は無い
  - つまり、本で勉強する事はできない
  - インターネットのように、常に変化しているもの
- 歴史を綴る事はできる
  - 「インターネットのカタチ」あきみち・空閑洋平著
- 過去事件、セキュリティに関するプレゼンテーションは多数存在する
  - 今日のお話もその一つ

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

アンテナを高く

Actingで大事なのは

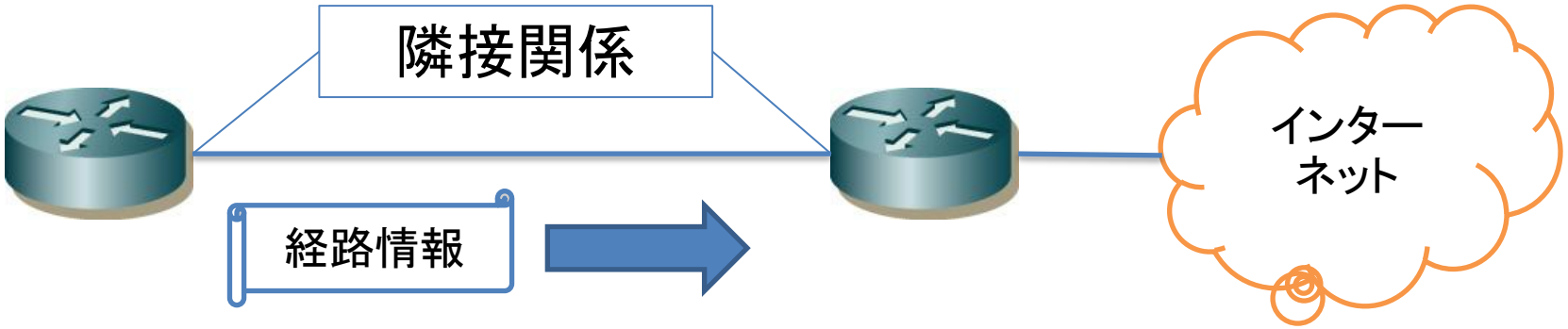
覚悟を決める

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

ルーティングを守るとは



- 隣接関係
- 経路情報
- インターネット

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

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！

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

ルーティングセキュリティを守るとは

- 直接自分のユーザを守るだけではない
  - 第三者のユーザを守る事でもある
  - ネットワークは「面」なので、結局自分のユーザにも影響はある
- 簡単に加害者になれてしまう
  - Internet Protocolはとても自由
  - 意識しなくても、ネットワーク層では簡単に加害者になれてしまう
  - これを防止する事で自分の身を結果的に守る
- 大事件を食い止める
  - Transit提供者は、顧客のミスをカバーするのも仕事の一つ

Acting:取り組みポイント

- ルータのコンフィグ検討
  - 隣接関係：MD5、IPsec
  - 経路情報：経路フィルター
- ツールの用意
- データ参照ポイントの利用
  - IRR (RADB, RIPE, etc)
  - Route Views / RIS　などの外部経路テーブル
  - 経路奉行　などの検知システム
  - 将来的にはRPKI

Thinking:備えるための日常

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

心構えまとめ

- ルーティングセキュリティを守り続けられるかどうかは、それに価値を見いだし続けられるかどうか、にかかっています
- 価値を見いだし、適切な情報を収集するためのThinking活動
- 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のActing活動
- そして隠れたファインプレーの「価値」を高めるため再びThinking活動

おしまい