IETF報告会（90th トロント）

RPKI/SIDR関連

木村泰司

taiji-k at nic.ad.jp

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター

発表者について

- **IETFミーティング参加について**
  - RPKI関連の調整とセキュリティ関連の動向調査
  - インターネットのアーキテクチャを考える場としてのIETFの話題をサーベイ
  - MLは1997年頃、ミーティングは2003年頃から参加
- **所属と氏名**
  - 日本ネットワークインフォメーションセンター
    - インターネット推進部／技術部
      木村泰司
      - 調査研究担当
      - 認証局・システムの企画・開発・運用・ユーザサポート

内容

- RPKI
- BGPSECに関わる標準化の最新動向
- BGPSECの導入効果

RPKI

パケット交換と分散ネットワーク

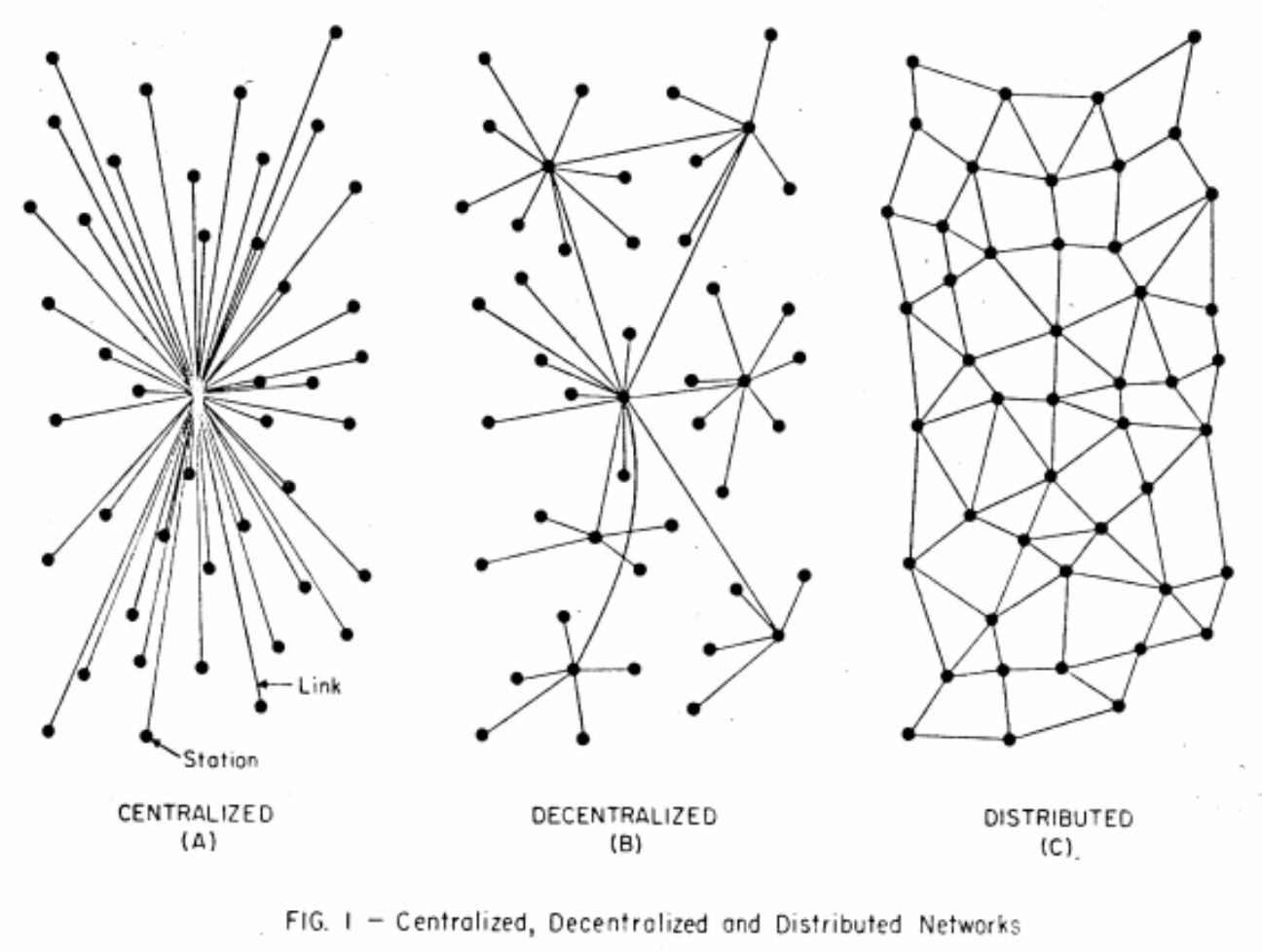
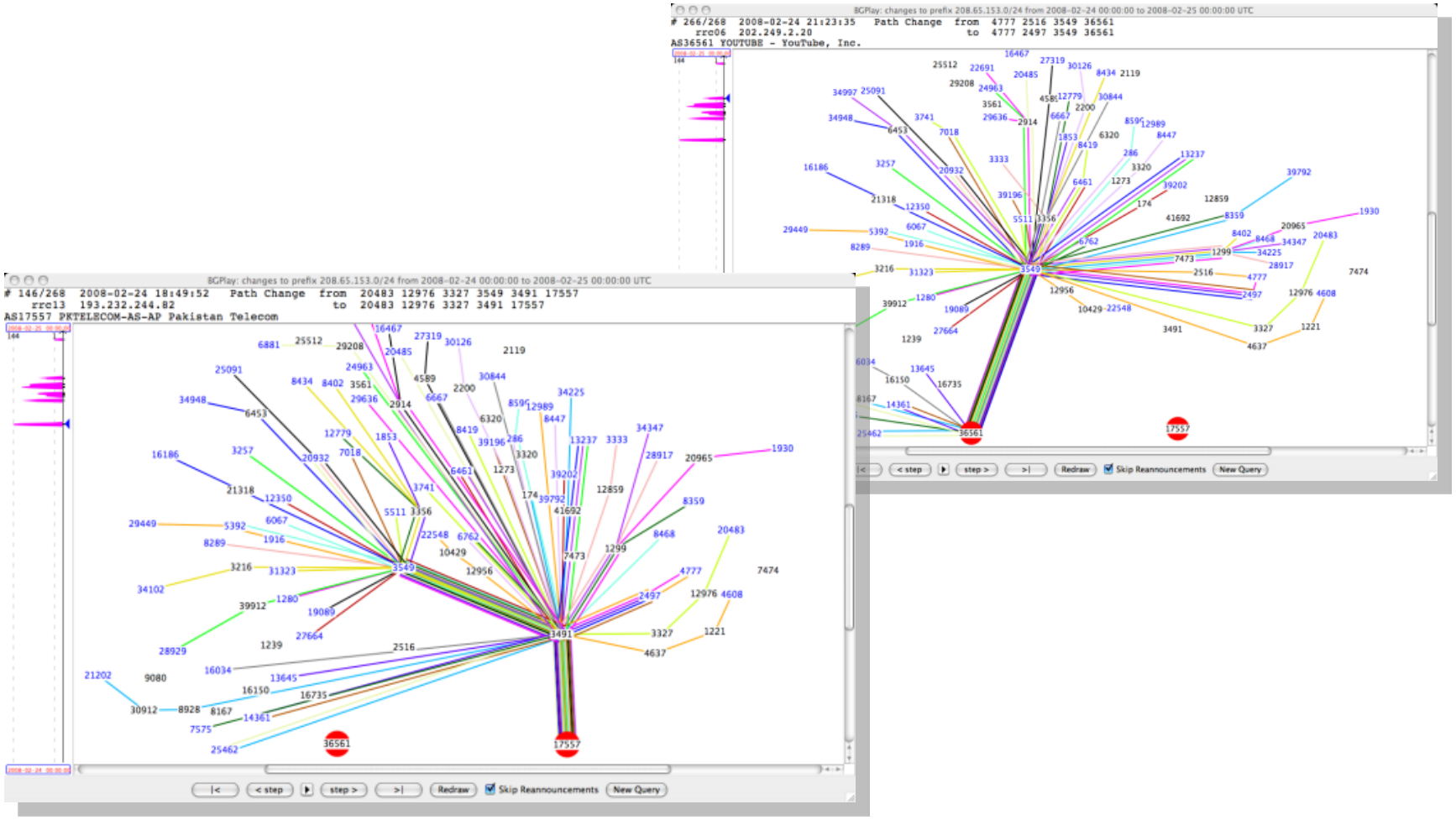


FIG. 1 — Centralized, Decentralized and Distributed Networks

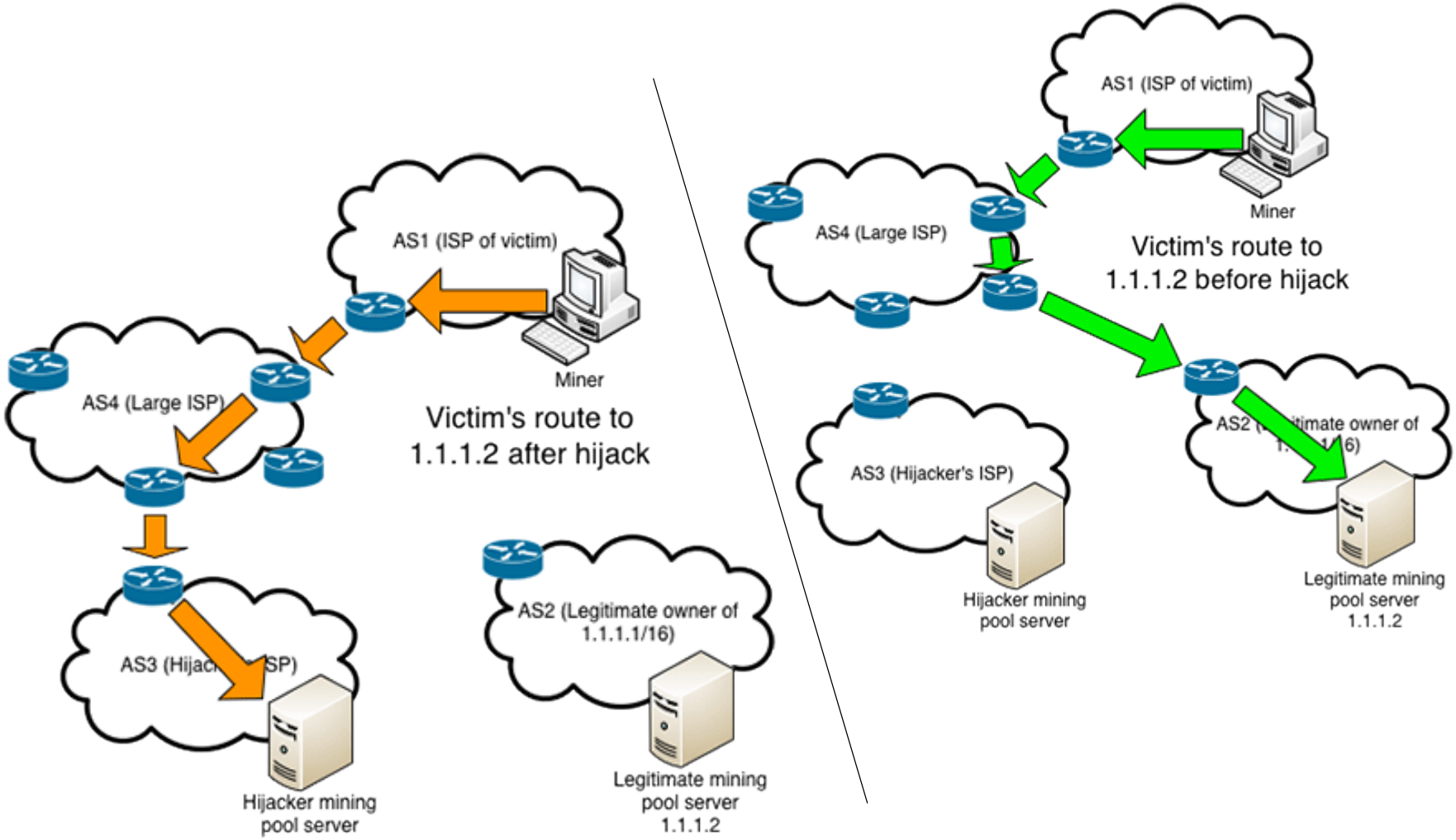
“On Distributed Communications Networks”, 1962年9月, ポール・バラン

YouTube経路ハイジャック事件



YouTube Hijacking: A RIPE NCC RIS case study, 17 Mar 2008, RIPE NCC,
http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

BitCoinのマイニングプールへの経路をハイジャック



BGP Hijacking for Cryptocurrency Profit, 7 August 2014
Pat Litke and Joe Stewart, Dell SecureWorks Counter Threat Unit
http://www.secureworks.com/cyber-threat-intelligence/threats/bgp-hijacking-for-cryptocurrency-profit/

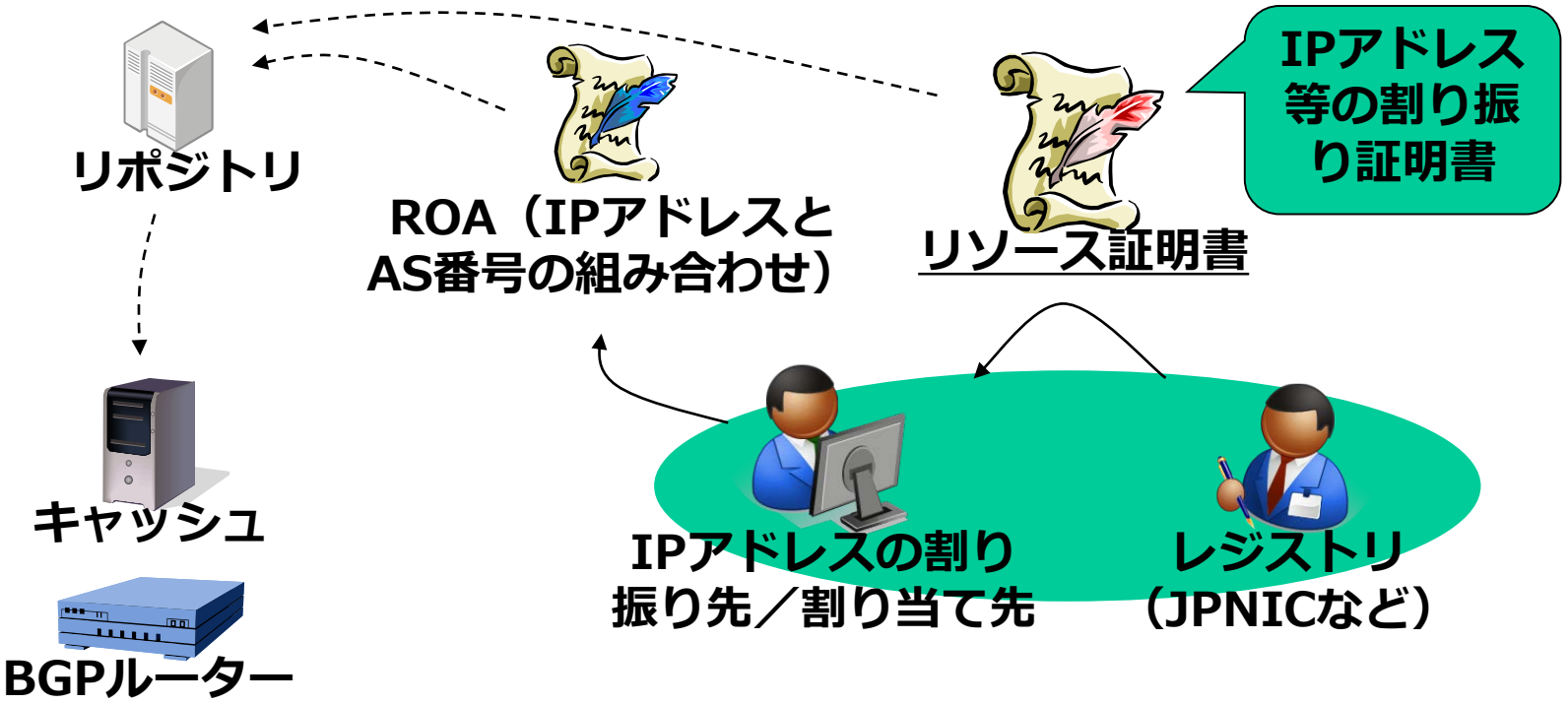
対策としての経路フィルターとその情報源

- **経路フィルター**
  - BGPルーターにおいて経路表に反映させる経路情報をフィルタリング
    ⇒その情報源や確認手続きの重要さ
- **ルーティングレジストリー**
  IRR : Internet Routing Registry
  - 国際的には多数のIRRが運用されており、情報の同期や正確性が一定ではない。
  - JPNICのJPIRRやRIPE NCCのWHOISデータベースは情報通知などの機能がある。

RPKIとは

RPKI　（リソースPKI）

⇒ Resource Public-Key Infrastructure



RPKIのこれまで

- **BBN Report 8217, “An Architecture for BGP Countermeasures,” November, 1997**
  - IPアドレスの割り振り構造に沿って認証局を置き、インターネット経路制御のセキュリティ向上のためにIPアドレスとAS番号を確認できるような電子署名のアーキテクチャを提唱
- **Secure Inter-Domain Routing WG発足, 2006年4月**
- **2008年2月YouTube経路ハイジャック事件**
- **2011年4月のIPv4アドレス在庫枯渇に先立ち地域インターネットレジストリが「アドレスの割り振り証明」として導入を急ぐ**

RPKIの基本となるRFC

- RFC 5280 : X.509 Public Key Infrastructure
- RFC 3779 : Extensions for IP addresses and ASNs

リソース証明書のイメージ

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=D5BBADA3
    Validity
      Not Before: Apr 15 10:24:39 2014 GMT
      Not After : Apr 14 10:24:39 2019 GMT
    Subject: CN=D5BBADA3
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)

    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE
      X509v3 Subject Key Identifier:
        18:CE:ED:52:F0:99:02:8A:58:3C:F1:7B:53:71:0E:1F:5D:37:4F:8D
      X509v3 Key Usage: critical
        Certificate Sign, CRL Sign
      Subject Information Access:
        CA Repository - URI:rsync://rpki01.nic.ad.jp/repository/
        1.3.6.1.5.5.7.48.10 - URI:rsync://rpki01.nic.ad.jp/repository/jpnic-ta-03.mft

sbgp-autonomousSysNum: critical
        Autonomous System Numbers:
          0-4294967295

sbgp-ipAddrBlock: critical
        IPv4:
          0.0.0.0/0
        IPv6:
          ::/0

BGPSECに関わる標準化の最新動向

JPNIC 一般社団法人 日本ネットワークインフォメーションセンター

BGPSEC

- **IPアドレスの設定ミスや不正な設定を、BGPルーターで検知できる仕組み**
  - Origin Validation
    - 他のネットワークが自ASのIPアドレスを使い始めたことが検知できる
  - Path Validation
    - ASパスが途中で変えられてしまったことが検知できる

BGPSEC
＝Origin Validation＋Path Validation（PATHSEC）

Origin Validationの仕組みとRFC

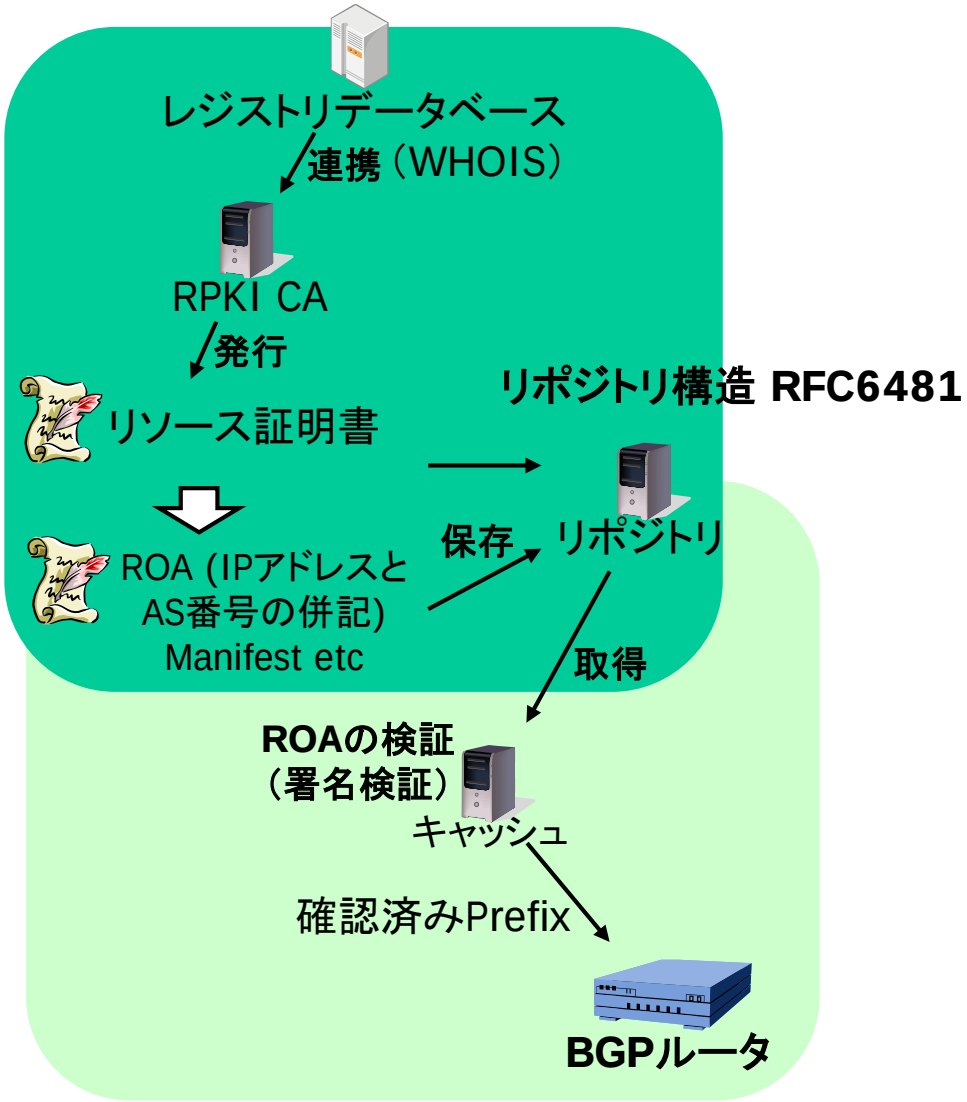
アーキテクチャ RFC6480

証明書プロファイル RFC6487
証明書ポリシー RFC6484
アルゴリズム RFC6485
発行処理 RFC6492

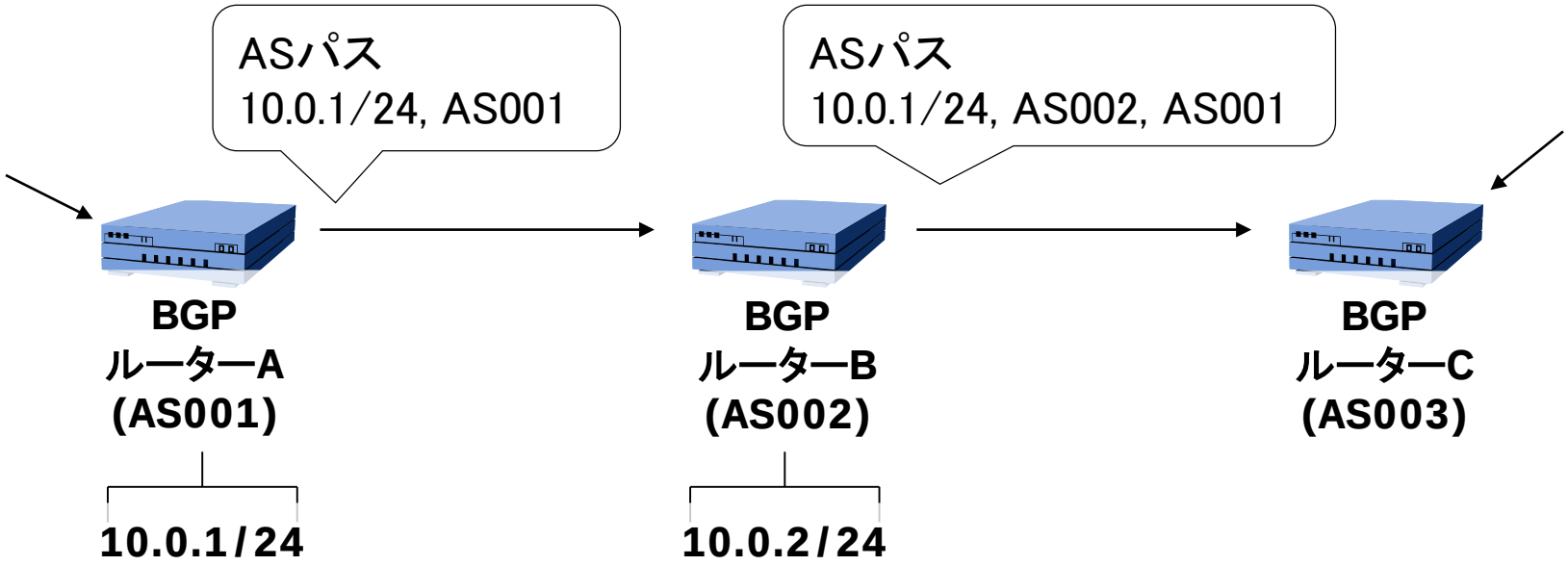
Manifest RFC6486
Ghostbusters RFC6493
ROA書式 RFC6482

トラストアンカー RFC6490
ROA検証 RFC6483
prefix検証 RFC6811
Origin Validation運用 RFC7115

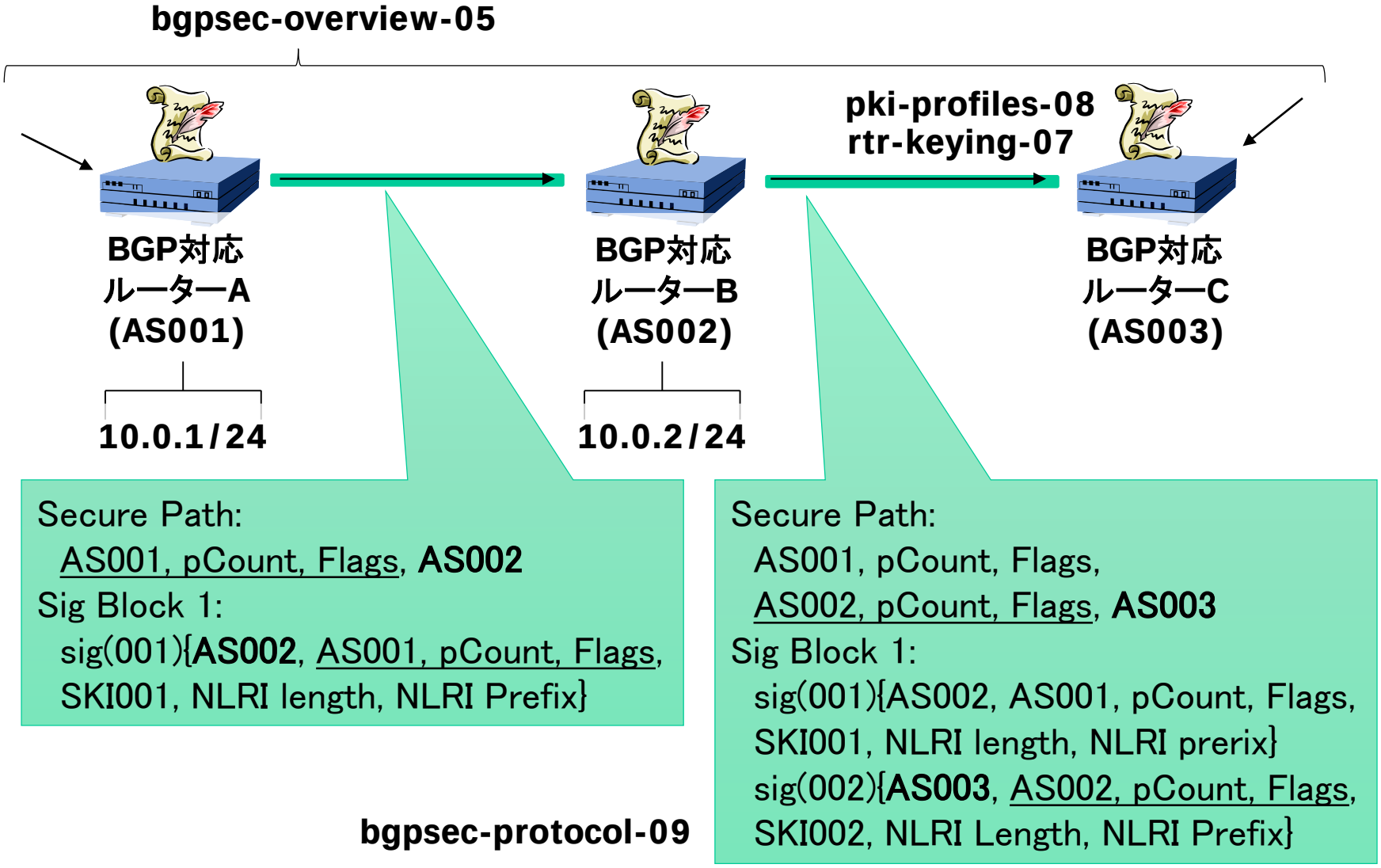
RPKI-to-Router RFC6810



Path Validation(PATHSEC)の仕組みとInternet-Draft/RFC（１）



Path Validation(PATHSEC)の仕組みとInternet-Draft/RFC（２）



BGPSEC関連のドキュメント状況

2014年8月22日現在

RFC

Threat Model for BGP Path Security （BGPパスのセキュリティにおける脅威モデル）	RFC 7132 2014-02
Security Requirements for BGP Path Validation （BGPパス検証のためのセキュリティ要件）	RFC 7353 2014-08
Policy Qualifiers in RPKI Certificates （policyQualifierを入れるための証明書（RFC6487）の変更点）	RFC 7318 2014-07

Internet-Draft（draft-ietf-sidr を省略）

An Overview of BGPSEC （BGPSECの概要）	bgpsec-overview-05 2014-07-04（**大きな変更なし**）
BGPSEC Protocol Specification （ASパスへの電子署名を格納するBGPSEC_Path属性）	bgpsec-protocol-09 2014-07-04（**署名の削除、セキュリティ考察を整理**)
A Profile for BGPSEC Router Certificates, Certificate Revocation Lists, and Certification Requests （ルーター証明書、CRL、発行要求のデータ書式）	bgpsec-pki-profiles-08 2014-08-13（**大きな変更なし**）

BGPSEC関連のドキュメント状況

2014年8月22日現在

Internet-Draft（draft-ietf-sidr を省略）

BGP Algorithms, Key Formats, & Signature Formats （鍵のアルゴリズム、書式、署名形式）	bgpsec-algs-08 2014-07-02（**大きな変更なし**）
Router Keying for BGPsec （BGPSEC対応ルーターのための鍵管理）	rtr-keying-07 2014-5-23（**変化なし**）
BGP Prefix Origin Validation State Extended Community （BGPルータにおける状態のエンコード方式）	origin-validation-signaling-04 *2014-02-14*（**変化なし**）

SIDR WGミーティング

- **日時**
  - 2014年7月25日（金）
    9時～11時30分 70名ほど
- **アジェンダ**
  - BGPSEC Protocolの仕様
  - BGPSECにおけるASの移転
  - Extended community の利用
  - ローカルトラストアンカー他
  - Origin Validationの再検討

第90回IETFにおけるSIDR WG – アジェンダと議論(1)

- **BGPSEC Protocolの仕様(bgpsec-protocol-09)**
  - (内容) PATHSECの各種書式や署名検証
  - (議論) Path Validationに対してOrigin Validationは必須とするか、それとも独立させるか
    ⇒ 独立したものとして考える方向に
- **BGPSECにおけるASの移転(as-migration-02)**
  - (内容)カスタマーASが上流ISPを変えるときのBGPSECのやり方。
  - (議論)ドキュメントを他とマージするか
    ⇒ マージせず継続検討

第90回IETFにおけるSIDR WG－アジェンダと議論(2)

- **BGPSECにおけるルーターの証明書発行**
  - (内容)証明書発行要求をどこで作りどう証明書を発行するか
  - (議論)一つのAS番号に一つの証明書を発行する仕組みか、それとも一つのルーターに一つの証明書を発行する仕組みか
    ⇒ 一つのAS番号に一つの証明書の方向に（一台のBGPルーターに複数のAS番号が設定されていていても）
- **extended community の利用（origin-validation-signaling-04）**
  - (内容)BGPのextended communityを使ってBGPSECの検証結果を伝え経路の決定プロセスに反映する仕組みについてのIDR WGによるレビュー結果
  - (議論)IDR WGでのレビュー結果を受けて決定プロセスへの言及をなくす方向に

第90回IETFにおけるSIDR WG－アジェンダと議論(3)

- **ローカルトラストアンカー他 (slurm-01/suspenders-02/lta-use-cases-01)**
  - (内容)Origin ValidationのCAや検証結果をグローバルなリソースとは異なる管理をするための仕組み
  - (議論)RPKIの仕組みの一つとして考えるべきなのか。レジストリが国の裁判所の命令に従わざるを得ないという性質を使った「オランダ裁判所攻撃（Dutch Court attack）」を避ける手段になりうるのか
    ⇒ 継続議論

第90回IETFにおけるSIDR WG－アジェンダと議論(4)

- **Origin Validationの再検討(validation-reconsidered-00)**
  - (内容)上位のRPKI CAが一部のアドレスの割り振りの変更やオペミスのために、証明書に入ったアドレス一式（例えば1NIR分）がinvalidになるリスクを避けるには？証明書の解釈をゆるくすべきではないか。
  - (議論)賛否両論。ルーティングの場面では証明書検証の結果によらずに経路制御できるように考えるべきという意見も。

BGPSECの導入効果
（IRTF Openミーティングより）

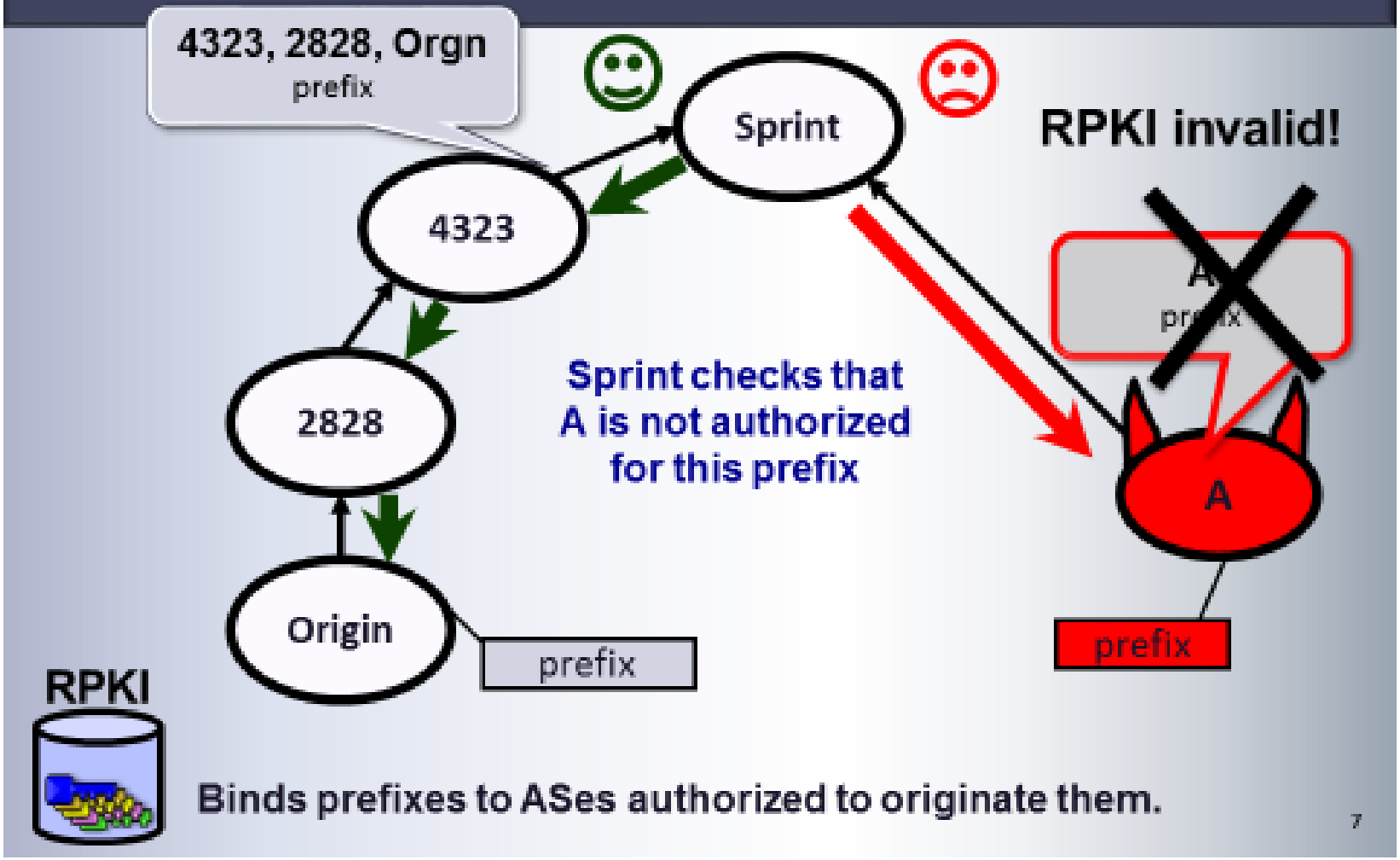
BGPSECの導入効果に関するリサーチ

- **「部分的に導入されるBGPセキュリティ：導入する価値は？」**
  - ロバート・リチェフ（ジョージア工科大学/ボストン大学）
  - シャロン・ゴールドバーグ（ボストン大学）
  - マイケル・シャピラ（ヘブライ大学）
- **BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?**
  - Robert Lychev(Georgia Tech / Boston University)
  - Sharon Goldberg(Boston University)
  - Michael Schapira(Hebrew University)
- **受賞：First 2014 Applied Networking Research Prize**

部分的に導入されるBGPセキュリティ：導入する価値は？

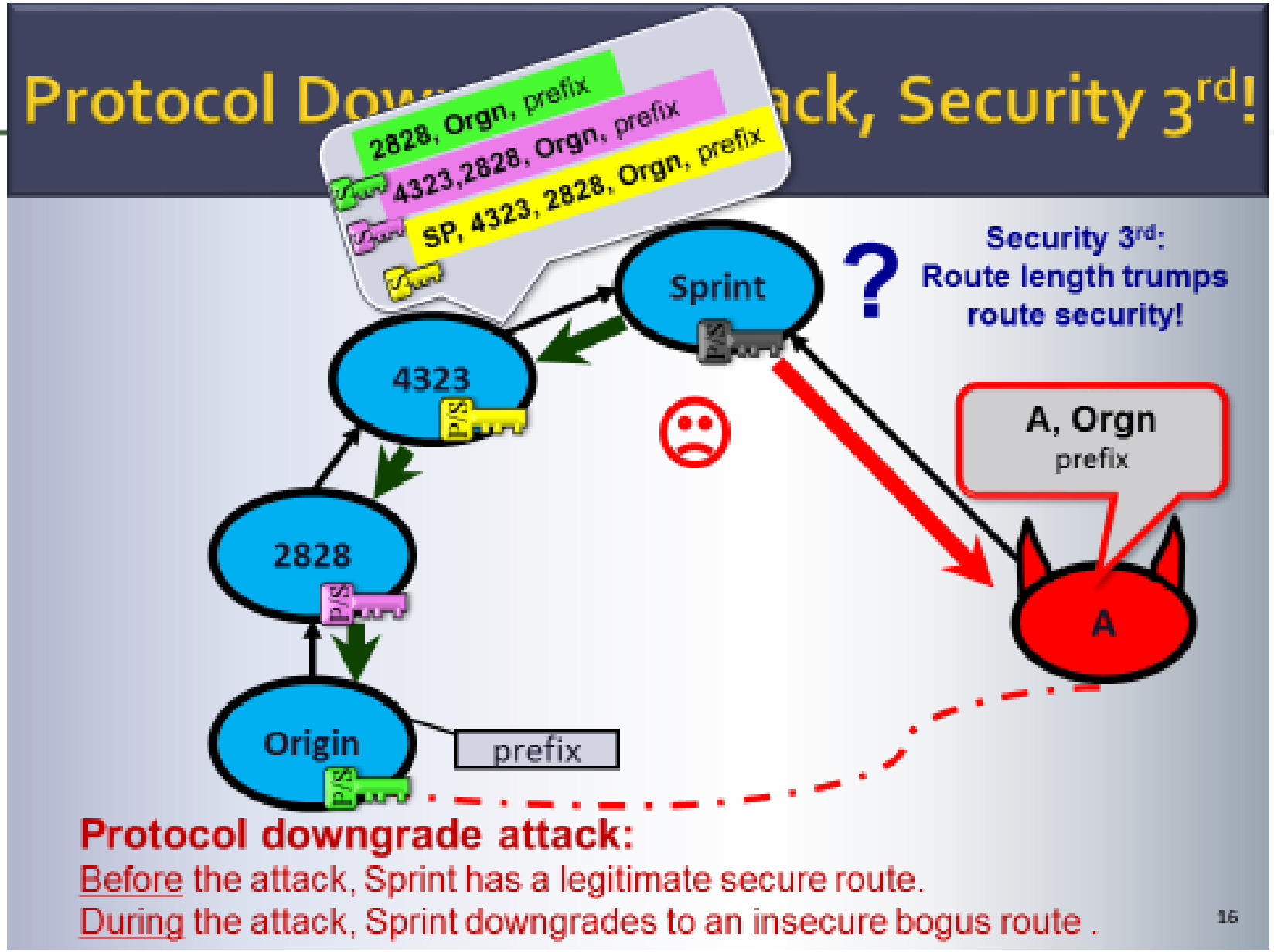
- **前提**
  - RPKIのOrigin Validationが導入された状態
  - AS Pathの詐称はできてしまう
- **テーマ**
  - BGPSECとBGPのルーティングが共存しているときにBGPSECの恩恵を受けるASはどれくらいあるのか？

RPKI Prevents Prefix Hijacks



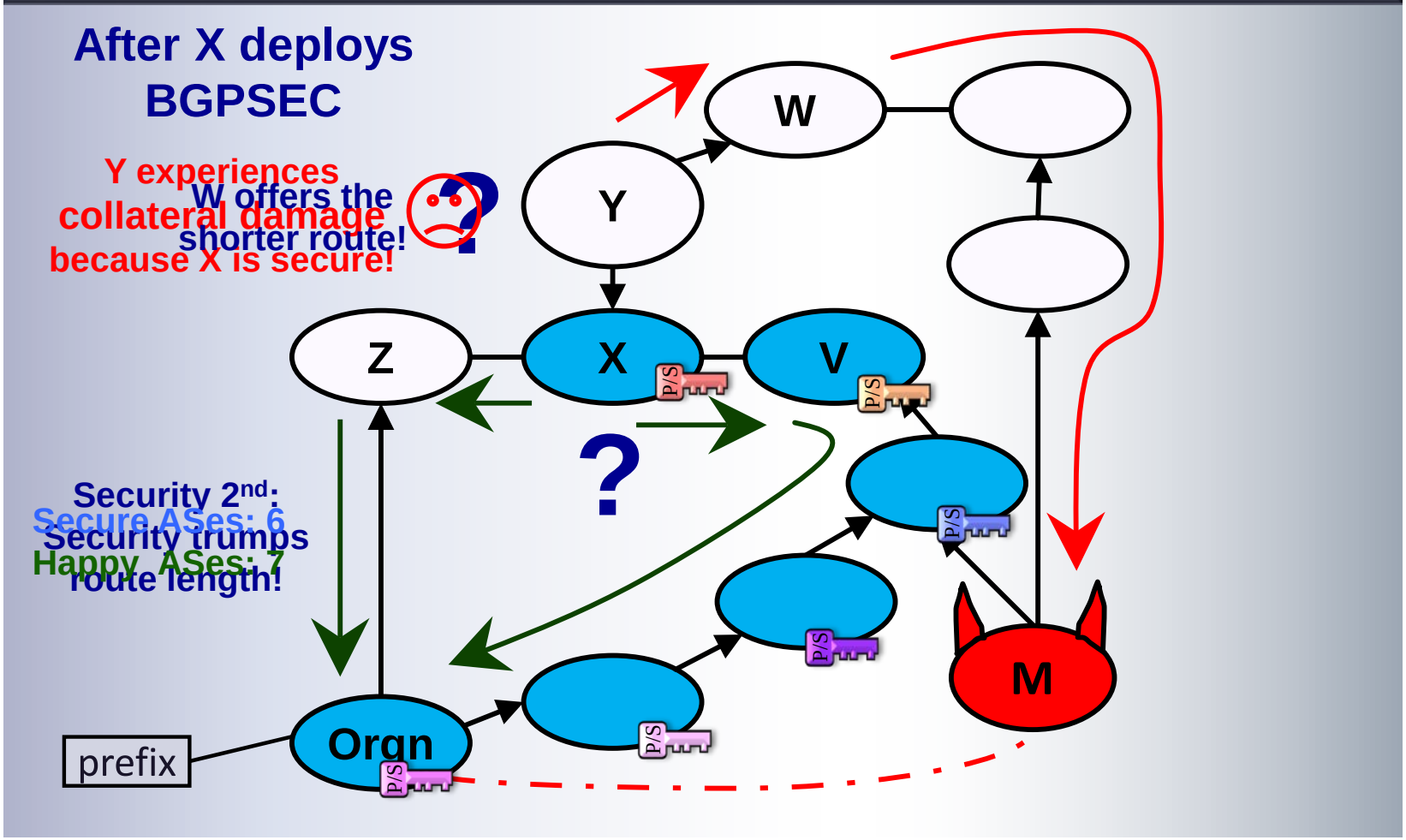
"BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", Robert Lychev, Sharon Goldberg, Michael Schapira, http://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pptx

Protocol Dow…ack, Security 3rd!



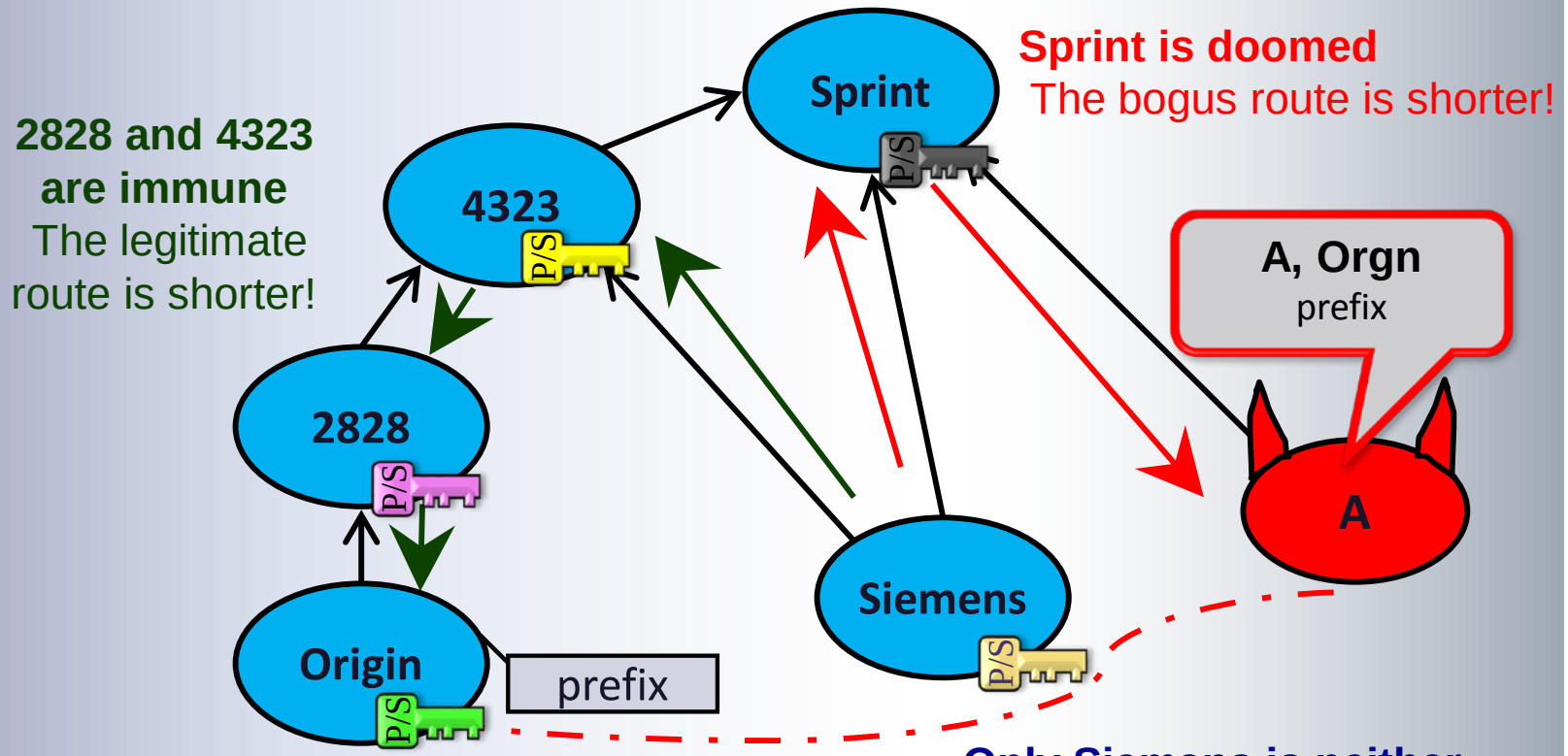
"BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", Robert Lychev, Sharon Goldberg, Michael Schapira, http://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pptx

Collateral Damages; Security 2nd



"BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", Robert Lychev, Sharon Goldberg, Michael Schapira, http://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pptx

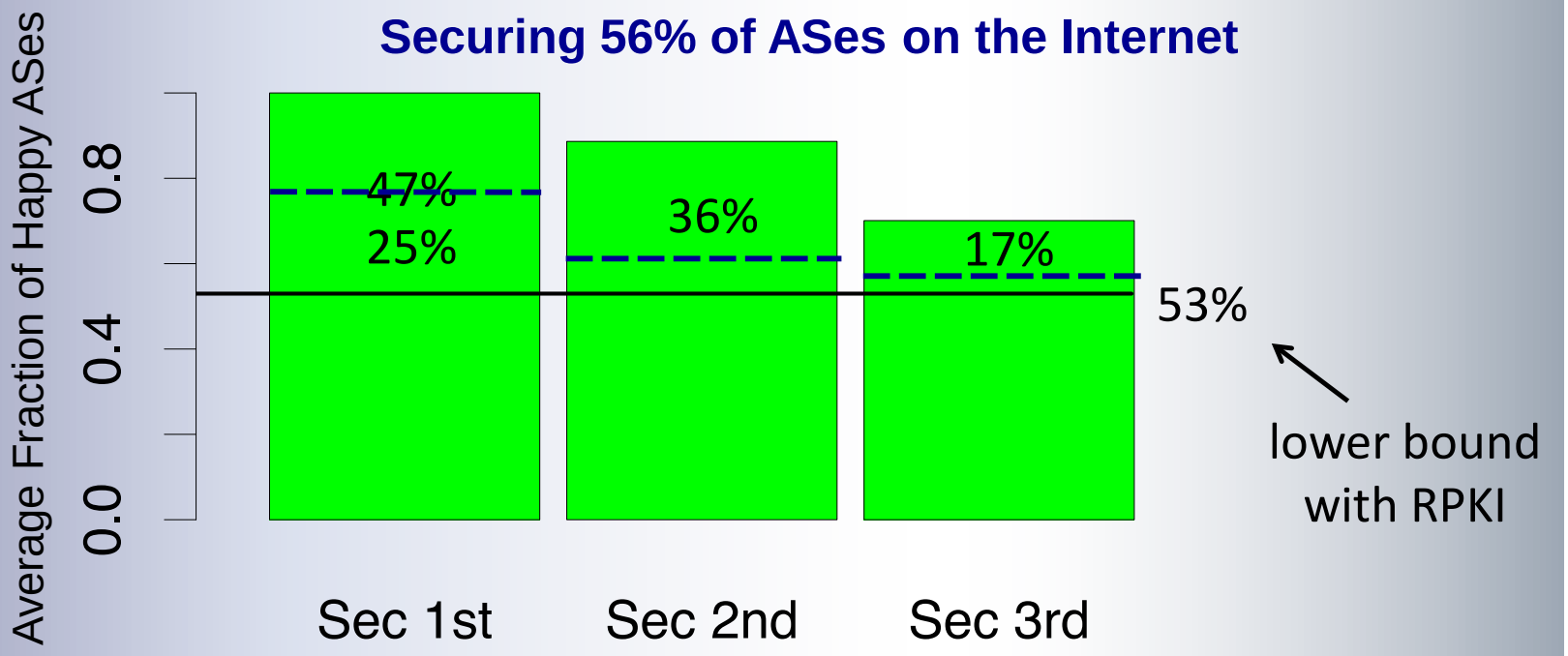
Bounding BGPSEC Benefits: Security 3rd



"BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", Robert Lychev, Sharon Goldberg, Michael Schapira, http://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pptx

Securing 213 High Degree ASes & their Stubs

(13 Tier 1's + 100 Tier 2's + 100 Tier 3's + all their stubs)



Improvements in the security 3rd and 2nd models are only 5% and 10% respectively.

39

"BGP Security in Partial Deployment: Is the Juice Worth the Squeeze?", Robert Lychev, Sharon Goldberg, Michael Schapira, http://www.ietf.org/proceedings/90/slides/slides-90-irtfopen-1.pptx

シミュレーションの結果

- **（AS数）Tier 1: 13, Tier 2: 100, Tier 300 AS**
- **（条件）BGPルータの優先の仕方**
  - Sec 1st：local prefefence 優先
    （NANOGでの100ASアンケートでは10%）
  - Sec 2nd: shorter path優先（〃 20%）
  - Sec 3rd: 個別のルール（〃 41%）
- **（結果）BGPSEC導入で直接的に助かるAS**
  - **Sec 2nd: +10%**
  - **Sec 3rd: +5%**

導入効果が直接あるASは合計で60%弱

BGP Security in Partial Deployment: Is the Juice Worth the Squeeze? (full version)

http://arxiv.org/abs/1307.2690

第90回IETFに見るRPKIの技術動向まとめ

- **SIDR WG**
  - BGPSECの基本的な仕様を議論中
    - Origin ValidationとPath Validationは独立か
  - Origin Validationの署名検証見直しの可能性
    - 大規模な署名検証失敗を、RPKI CA運用のリスク
- **導入効果に関するリサーチ**
  - BGPSEC導入によって不正なパスから正常なパスに変わるASは意外に少ない

おわり

参考資料

- **BGPSEC Protocol Specification, Matt Lepinski, IETF-88**
  - http://tools.ietf.org/agenda/80/slides/sidr-18.pdf
- **An Overview of BGPSEC**
  - http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-overview-05
- **BGPSEC Protocol Specification**
  - http://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-09