IETF報告会（87th ベルリン）

RPKI関連

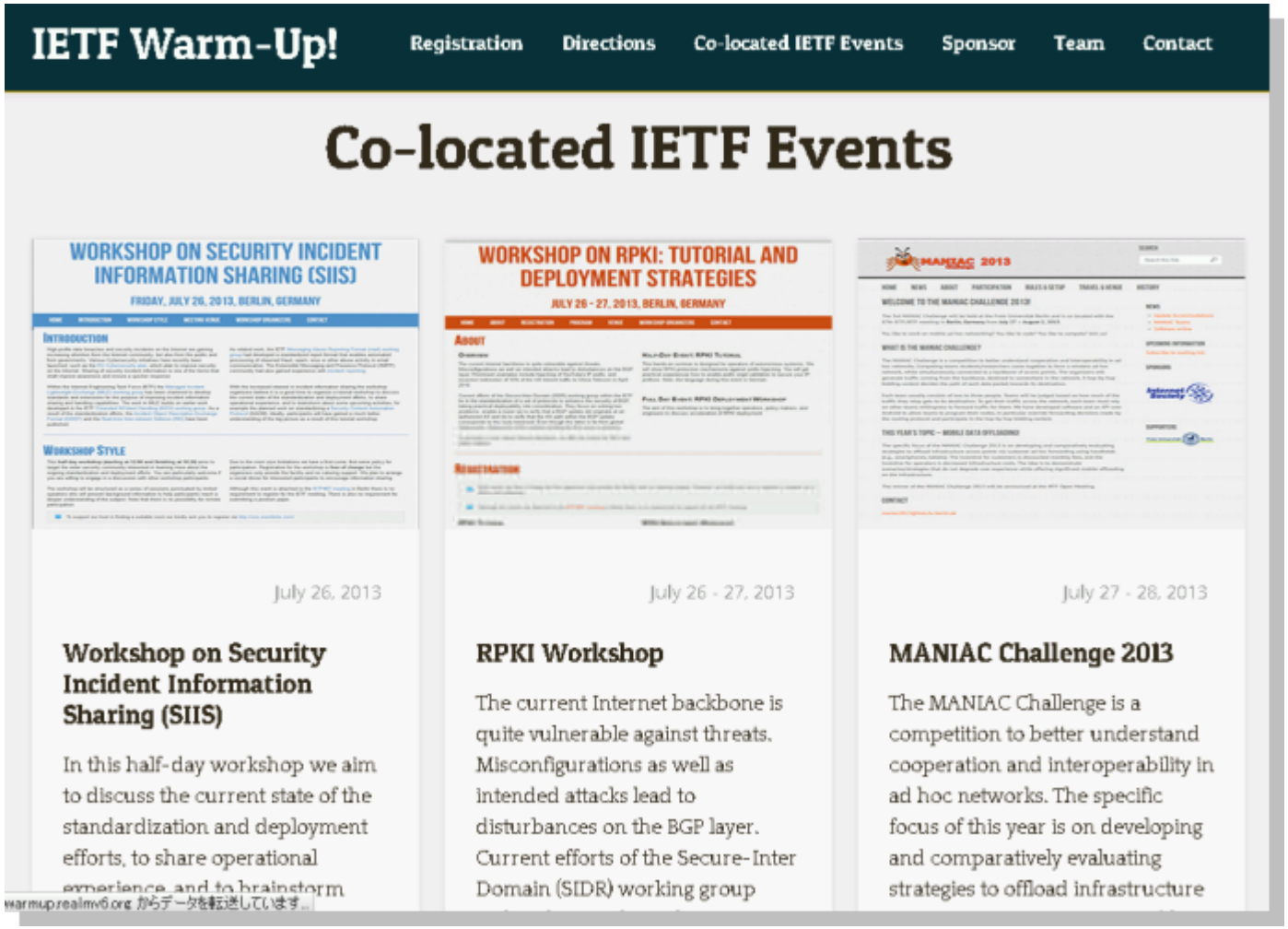
木村泰司
taiji-k at nic.ad.jp

内容

- RPKI workshop (pre-IETF event)
- Secure Inter-Domain Routing (SIDR) WG

RPKI workshop (pre-IETF event)

pre-IETF イベント

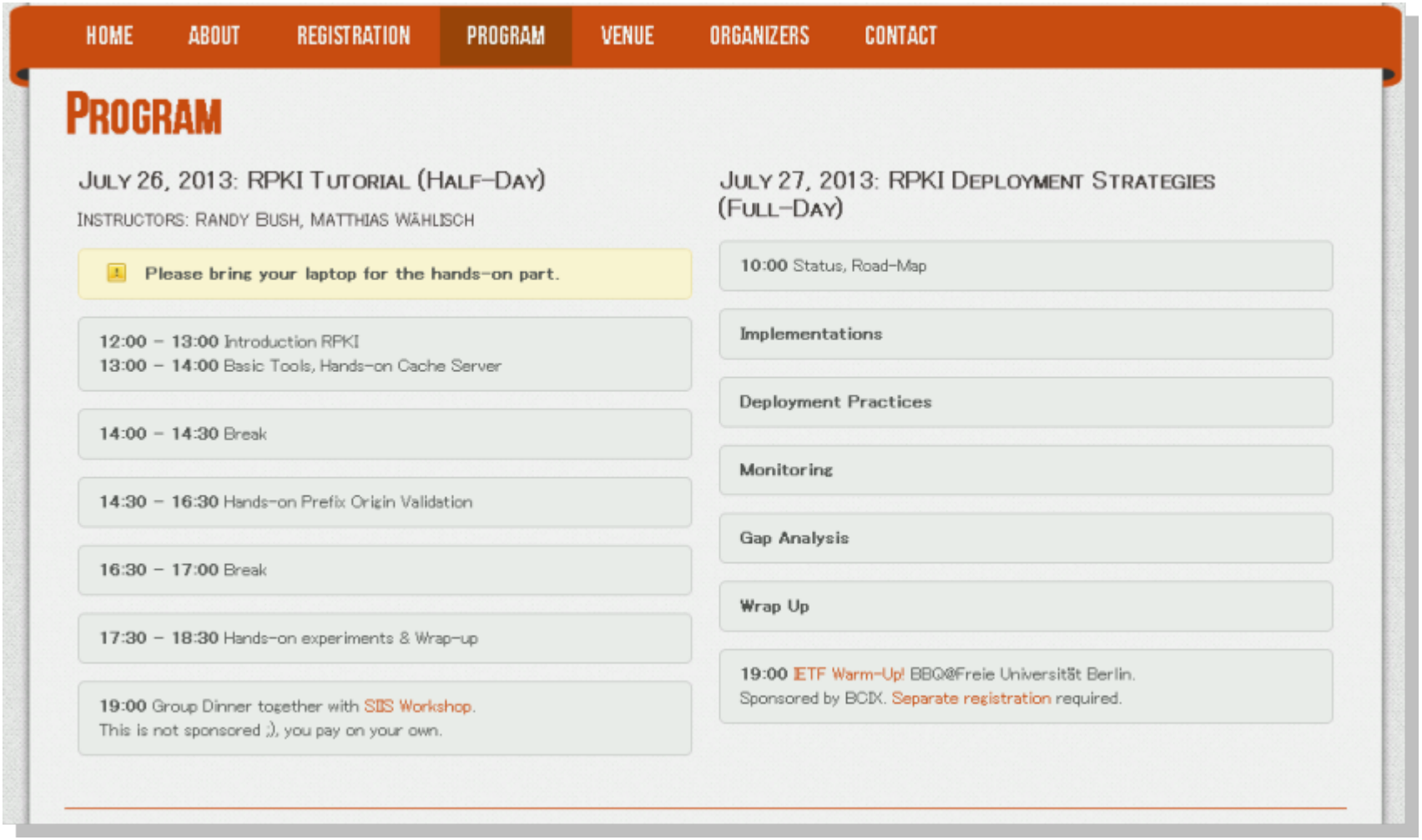


http://ietf87-warmup.realmv6.org/#events

RPKI workshop

http://rpkiws.realmv6.org/

プログラム



http://rpkiws.realmv6.org/#program

RPKI workshop Day1（1/2）

- Randy Bush氏によるハンズオンセミナー
  - 日時　2013年7月26日（金）10:20-17:00
  - 場所　ベルリン自由大学
  - 参加者　6名（全員設定を完了）
  - 内容　（https://psg.com/130726.pdf, JANOG32チュートリアルと同じ）
    - RPKI ToolsのGUIを使ったROAの発行
    - RPソフトウェア（rcynic、rtr-origin）とBGPルータを設定
    - 仮想サーバにRPKI Toolsをインストールして RPソフトウェアを設定



RPKI workshop Day1（2/2）

- チュートリアル中にあがった質問
  - ROAの90%がNot Foundな状態で経路制御はどうなるのか？
    ⇒試験的に導入されたIETF87ではDropする設定になっている。（会場補足：今後、最適な設定がなされていくであろう）
  - sshのクライアントがないがどうしたらいいか？
    ⇒会場補佐：PuTTYをインストール
  - RPKIのサービスをビジネスでできるか？
    ⇒リポジトリなどはなるかも知れない。RPKIキャッシュは手元に置くことになるが。
    ＃木村補足：国内ではRPKIキャッシュさえも？

RPKI workshop Day2（1/4）

- ディスカッション
  - 日時　2013年7月27日（土）10:35-18:30
  - 場所　ベルリン自由大学
  - 参加者　18名
  - 内容　（Rudiger Folk氏とPeter Koch氏のモデレート）
    - 午前　自己紹介と取り組みの紹介
    - 午後　デプロイメントと実装、RPKIの今後の課題

RPKI workshop Day2（2/4）

- Day2の目標とテーマ
  - 議論の目標
    - グローバルインターネットの信頼性の向上
      （回復力、高い信頼が置けるネットワーク）
  - 前提
    - RPKIはInter-domainの経路制御に資すると考える
  - やること
    - だれがどの活動を行っているのかかなどを理解する
    - 運用に役立つためにRPKIの導入において足りないことがないかを知る
    - 関係者がRPKIを導入しやすくする

RPKI workshop Day2（3/4）

- 午前　自己紹介と取り組みの紹介
  - LACNIC, NIST ITL, RIPE NCC, nlNetLabs, ISP(Orange), JPNIC
    - 国内とAPNIC地域のRPKIハンズオンを紹介（木村）
      - 業務課題：　IPアドレス担当者と経路制御オペレーターの違い、JPIRRとROA管理の違い、経路制御セキュリティニーズの温度差
- 午後　デプロイメントと実装
  - BRITE, BGP-SRX,Quagga-SRX紹介 (NIST ITL) https://brite.antd.nist.gov/
  - RPKI Dashboard, nlNetLabs http://rpki.surfnet.nl/
  - RPKI ROA wizard (LACNIC)

RPKI workshop Day2（4/4）

- RPKIの今後の課題 – Deployment Strategy

黒板	Policy&Regal	Tools&Infrastructure	How To
	• Value / Risk • Legacy / PI • Control (Gov)	• Monitoring • Route (support) • Stability • Reliability (includes implementation.)	• BCP / Deployment which people - ISP - Legacy Holder - BMN&Co

その他の話題

〇Single Root

〇Monitoring (RPKI Dashboard)、Legacy Holder（RIPEで発行対象でない）

〇RPKIの導入価値：発行数の増加が価値なのではなく、運用者による不正な経路情報を検知し、復旧できることにこそ価値があるのではないか（木村）。
⇒RPKI Dashboardで変化を表示しては。

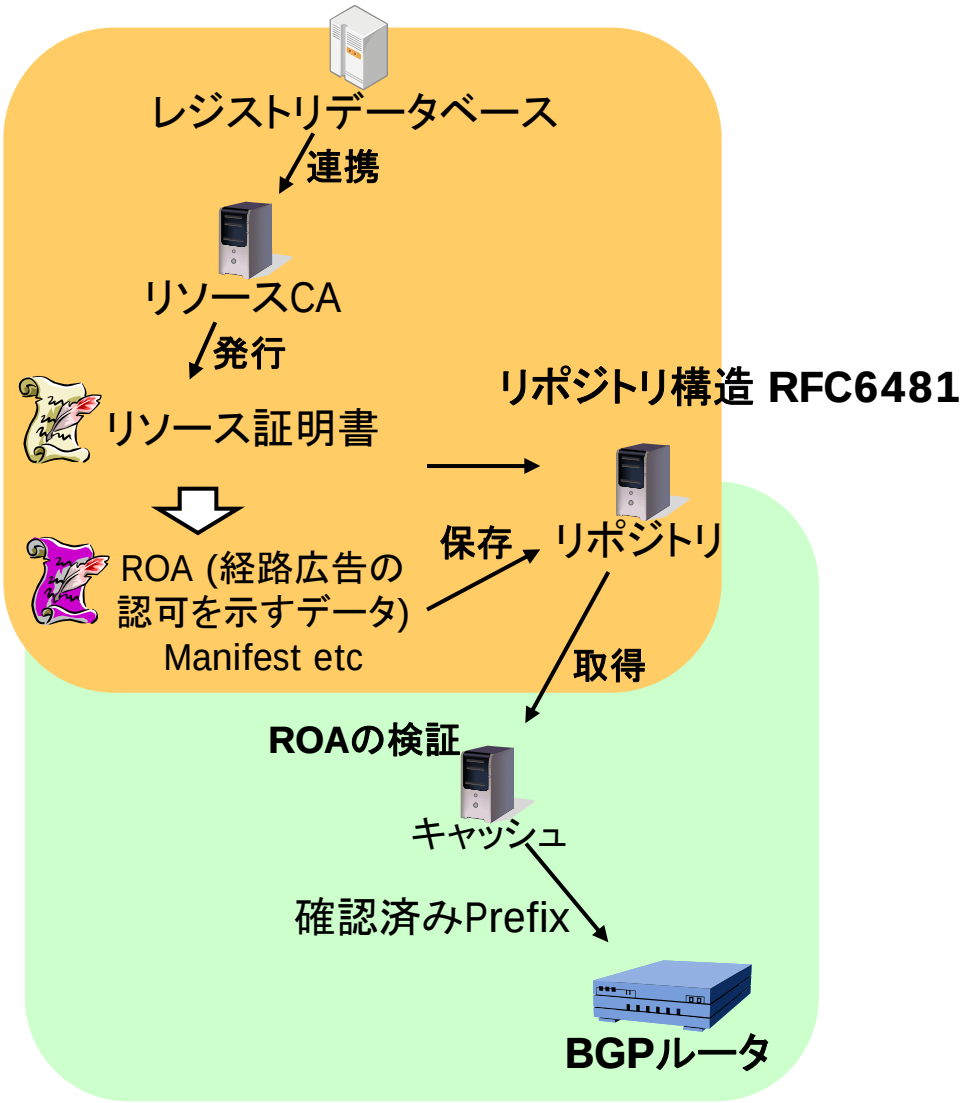
Secure Inter-Domain Routing WG (SIDR)

RPKIとSIDR WG

SIDR WG関連の
ドキュメント

⇒ Origin Validation はほぼRFC化

- 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
- RPKI-to-Router RFC6810



RPKIとSecure BGPの目指すもの

- 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

SIDR WG – ドキュメント状況

- BGPSEC

draft-ietf-sidr を省略

An Overview of BGPSEC （BGPSECの概要）	bgpsec-overview-03
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-05
BGPSEC Protocol Specification （BCPSECのプロトコル仕様）	bgpsec-protocol-07
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）	bgpsec-threats-05
Security Requirements for BGP Path Validation （BGPパス検証のためのセキュリティ要求）	bgpsec-reqs-07
BGP Algorithms, Key Formats, & Signature Formats （鍵のアルゴリズム、書式、署名形式）	bgpsec-algs-04
BGPSEC router key rollover as an alternative to beaconing （ルーターにおけるキーロールオーバー）	bgpsec-rollover-02

SIDR WGの概要

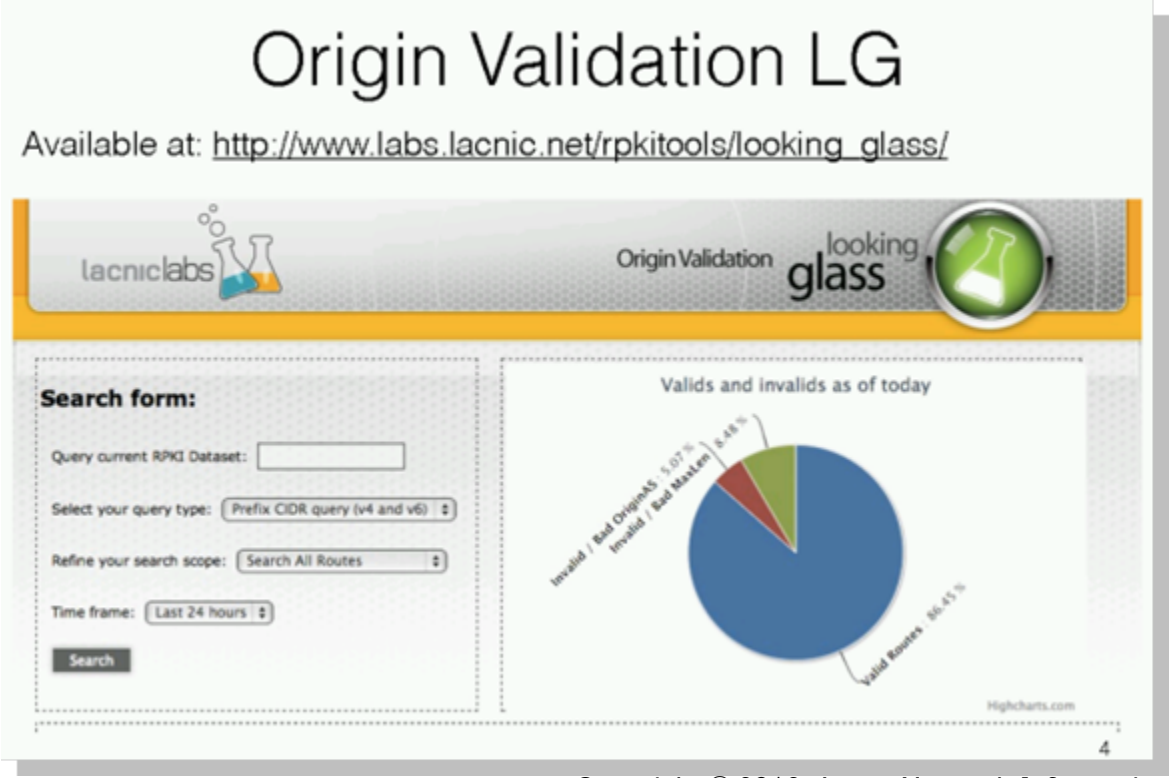
- Secure Inter-Domain Routing WGミーティング
  - 第一回
    - 2013年7月31日 15:10-16:13 (60名ほど)
  - 第二回
    - 2013年8月2日 11:20-13:33 (15名ほど)

アジェンダと議論　－　WG documents

- Revisiting the RPKI LTAM (Local Trust Anchor Management), Stephen Kent (BBN Technology)
  - トラストアンカーをRP内で管理して、独自のトラストアンカーを設けられる仕組み
- Multiple Repository Publication Points support in the Resource Public Key Infrastructure (RPKI), Carlos (LACNIC)
  - リソース証明書とROAの公開サーバを冗長化させるために、Trust Anchor Locatorファイルに URLを複数書く案
- Manifest EE Certificate Validity Times, RFC6486 & EE certificates, Tim Bruijnzeels (RIPE NCC)
  - 発行済みROAの一覧であるManifestの有効期限が、全てのROAの有効期限を内包するように修正。

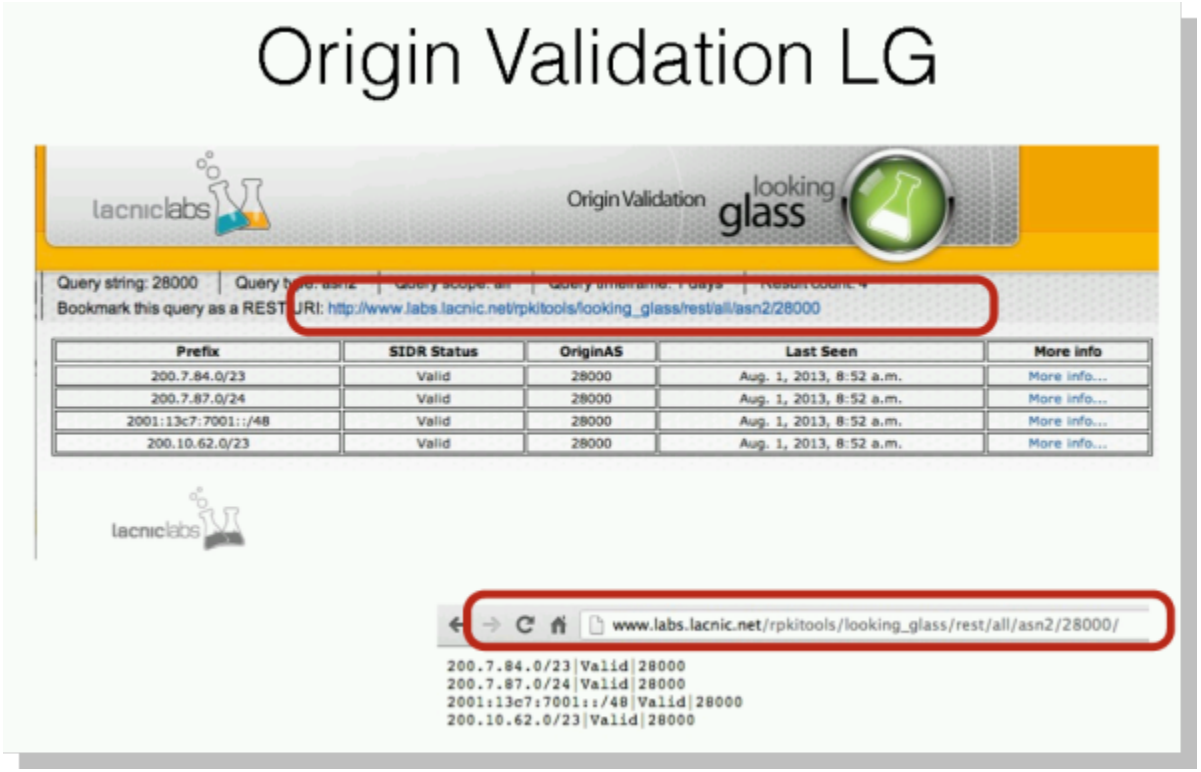
アジェンダと議論 ー Deployment

- Some available RPKI tools, Carlos, Benno
  - Origin Validation Looking Glass
    - http://www.labs.lacnic.net/rpkitools/looking_glass/



アジェンダと議論 ー Deployment

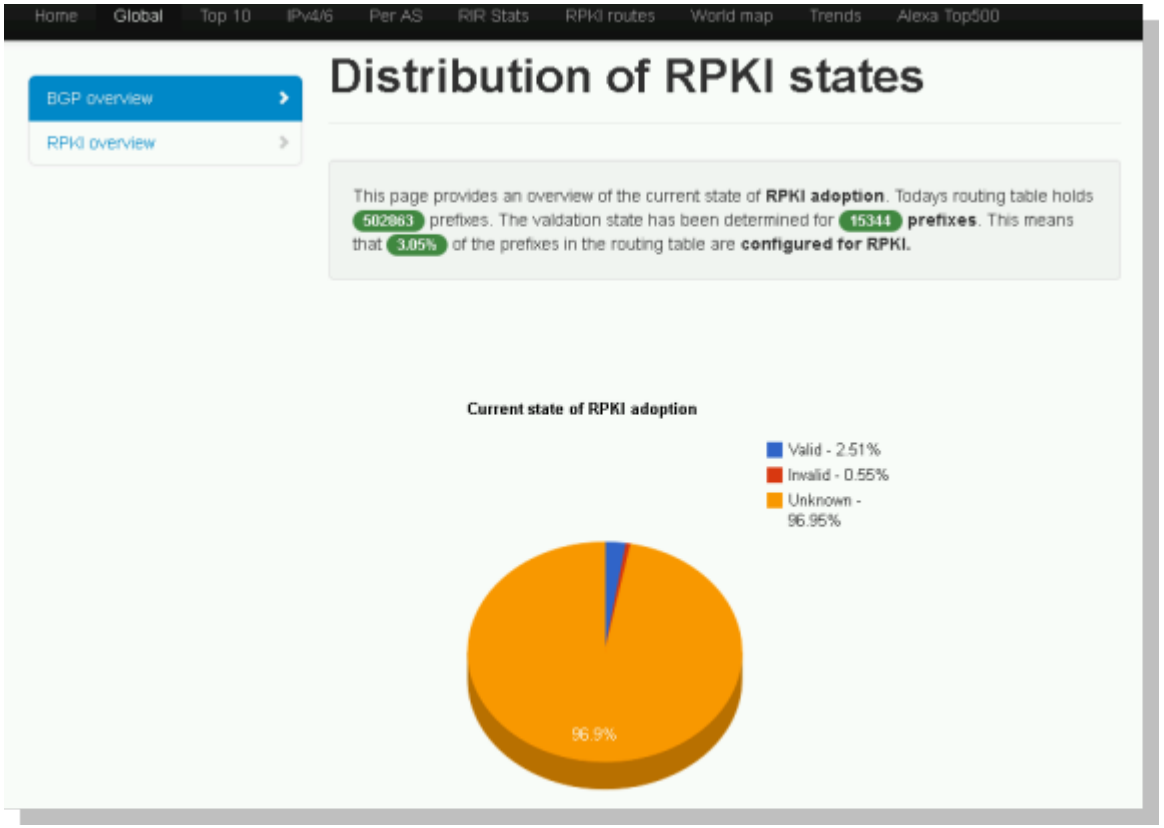
– Origin Validation Looking Glass



アジェンダと議論 ー Deployment

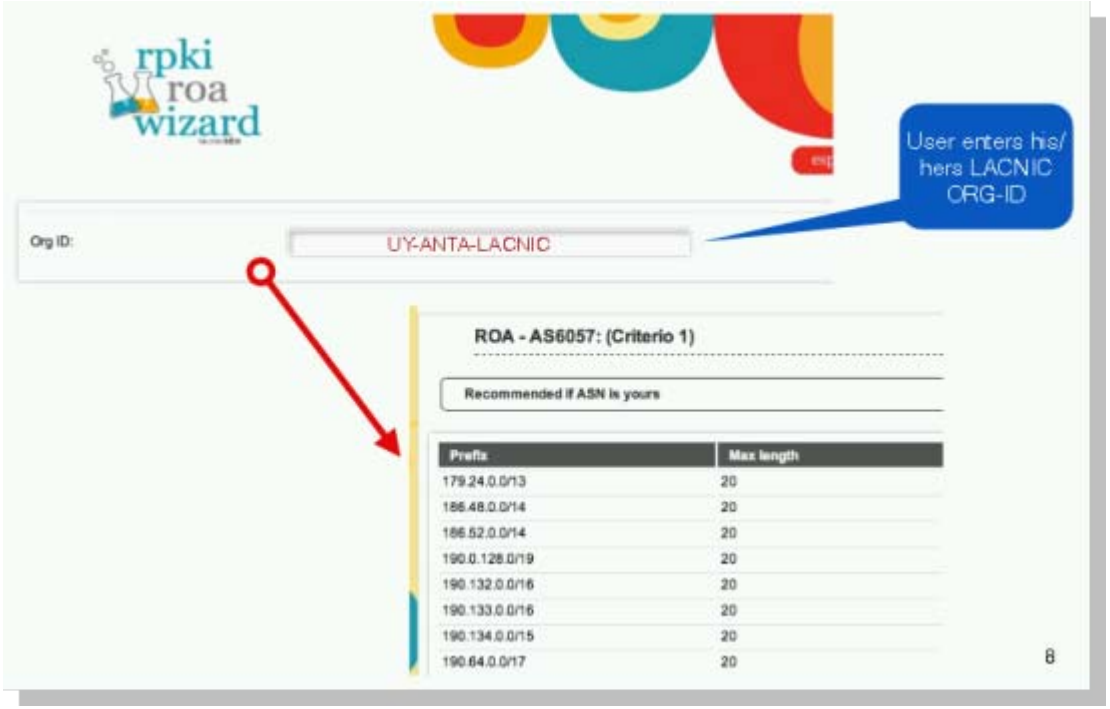
– RPKI Dashboard

- http://rpki.surfnet.nl/



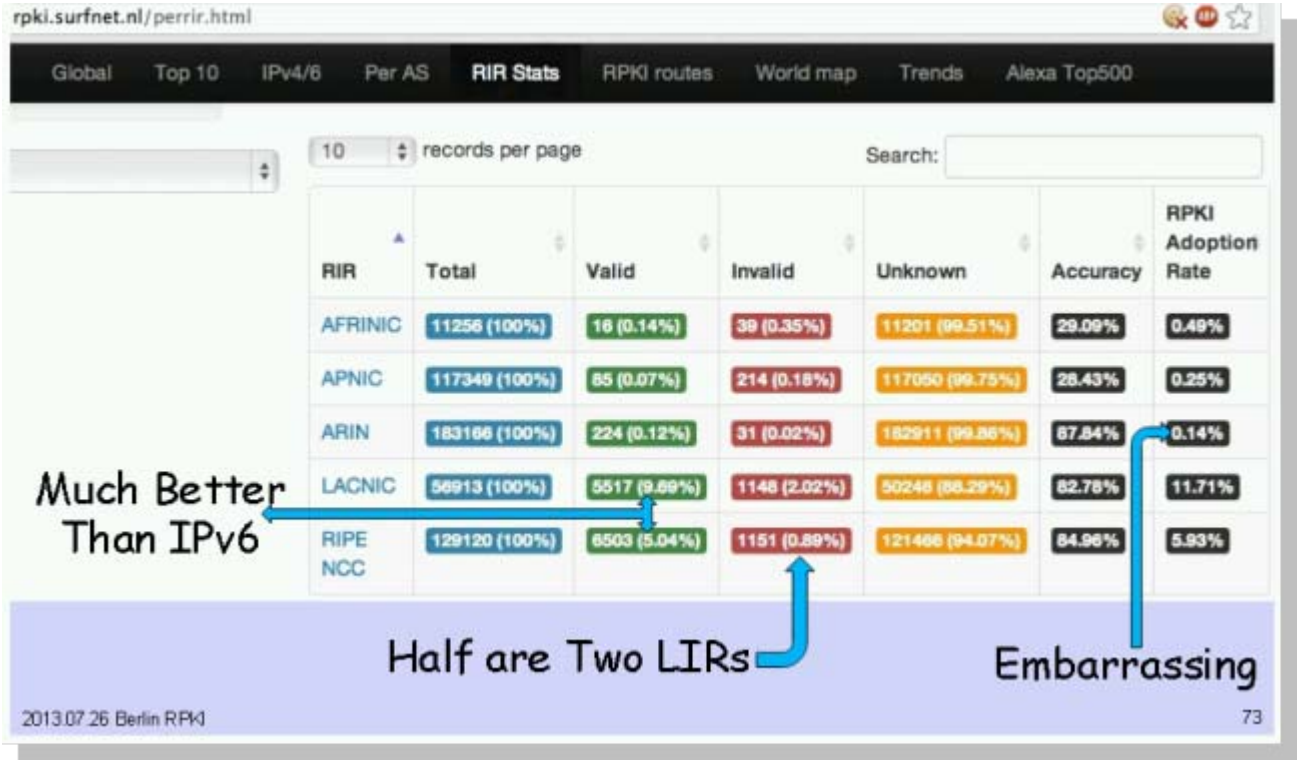
アジェンダと議論 ー Deployment

– ROA Wizard



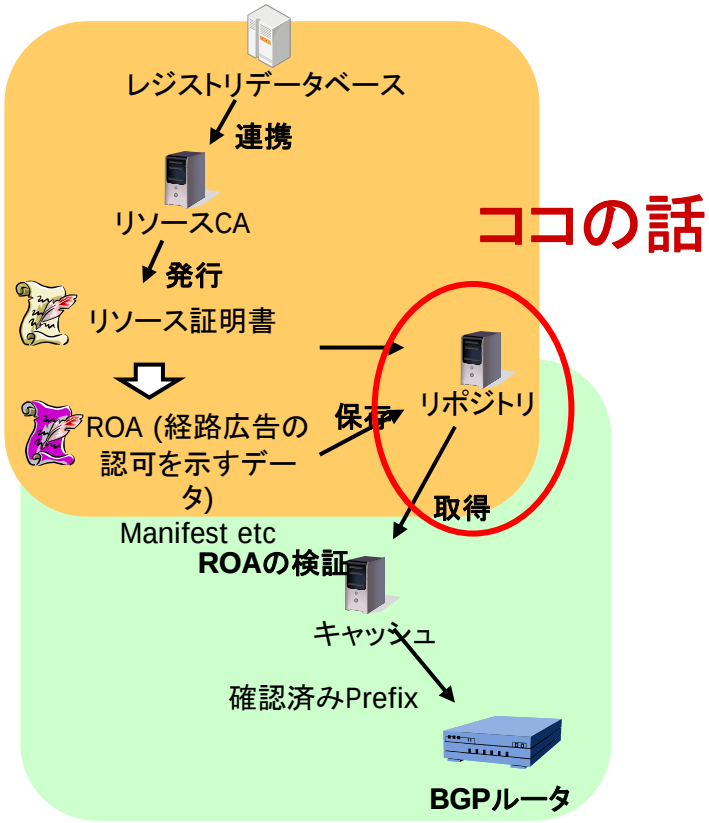
アジェンダと議論 ー Deployment

- Per-RIR Statistics and A Very Real Problem, Randy Bush



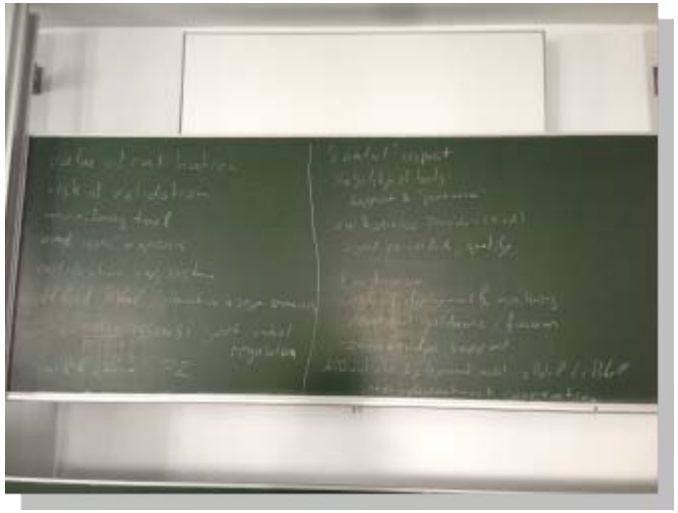
アジェンダと議論　－　Revised

- RSYNC Performance Study
  - RPKIオブジェクトを集めてクライアント数をシミュレートして時間を計測。
  - slides-87-sidr-11.pdf



写真

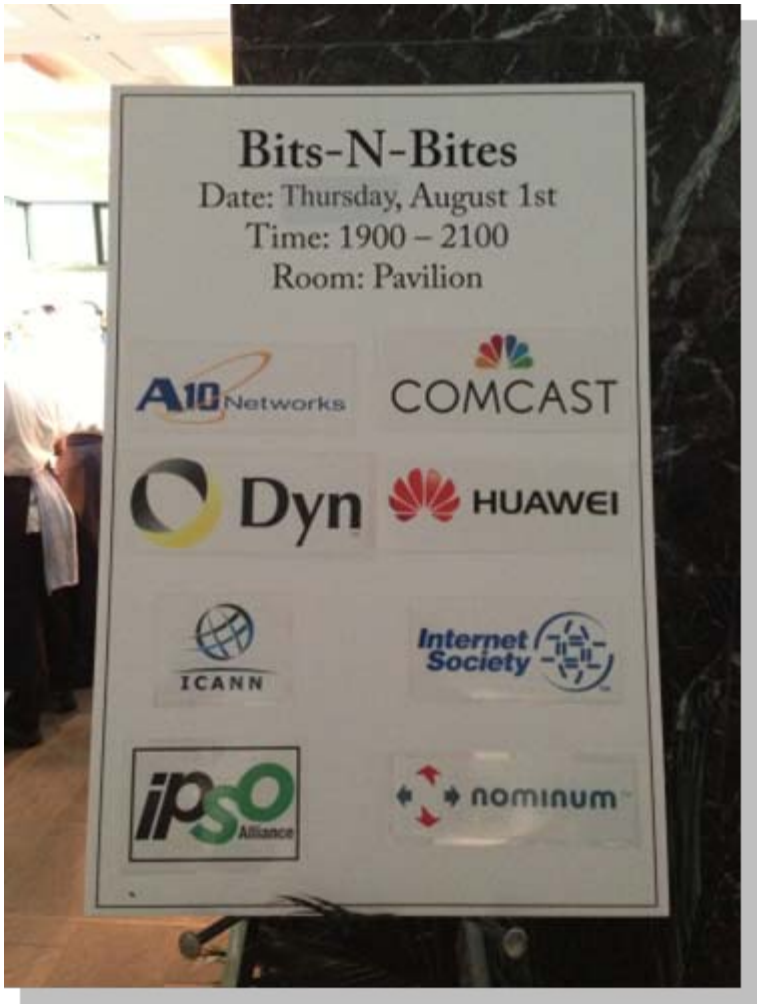
RPKIワークショップが行われた
ベルリン自由大学



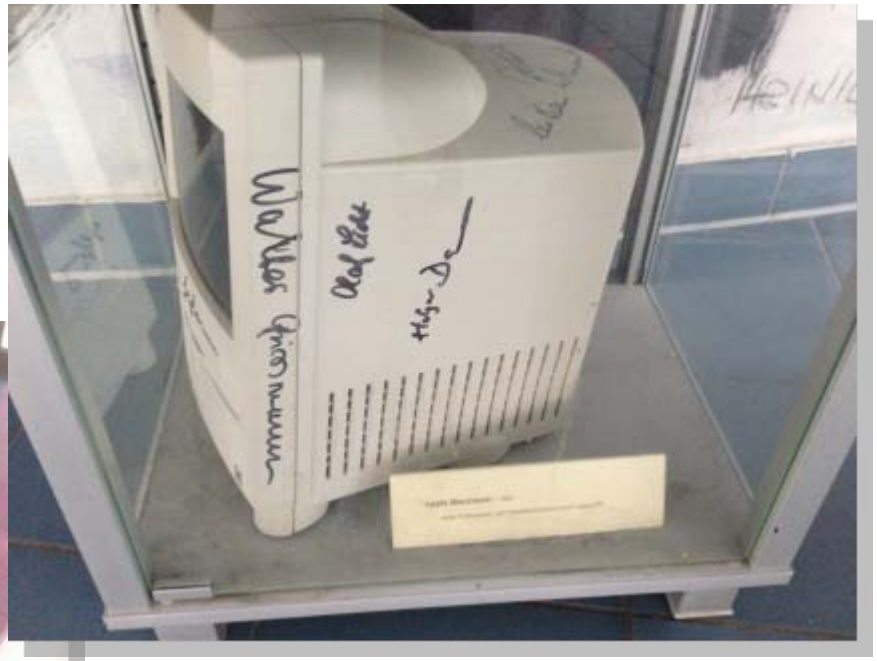
RPKIワークショップ後の バーベキュー（pre-IETFイベント）

会場のInterContinental

Bits-N-Bites



ベルリン自由大学の展示



ベルリン自由大学の展示

ベルリン自由大学の展示

ベルリン自由大学の展示

おわり