

# 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

The screenshot shows the 'IETF Warm-Up!' website with a navigation bar containing 'Registration', 'Directions', 'Co-located IETF Events', 'Sponsor', 'Team', and 'Contact'. The main heading is 'Co-located IETF Events'. Three event cards are displayed:

- Workshop on Security Incident Information Sharing (SIIS)**: Friday, July 26, 2013, Berlin, Germany. The card includes an introduction, workshop style, and a date of July 26, 2013. The title is 'Workshop on Security Incident Information Sharing (SIIS)'. The text describes a half-day workshop to discuss the current state of standardization and deployment efforts, share operational experience, and brainstorm.
- Workshop on RPKI: Tutorial and Deployment Strategies**: July 26 - 27, 2013, Berlin, Germany. The card includes an 'About' section and a date of July 26 - 27, 2013. The title is 'RPKI Workshop'. The text states: 'The current Internet backbone is quite vulnerable against threats. Misconfigurations as well as intended attacks lead to disturbances on the BGP layer. Current efforts of the Secure-Inter Domain (SIDR) working group'.
- MANIAC Challenge 2013**: July 27 - 28, 2013. The card includes a 'WHAT IS THE MANIAC CHALLENGE?' section and a date of July 27 - 28, 2013. The title is 'MANIAC Challenge 2013'. The text states: 'The MANIAC Challenge is a competition to better understand cooperation and interoperability in ad hoc networks. The specific focus of this year is on developing and comparatively evaluating strategies to offload infrastructure'.

At the bottom left of the screenshot, there is a small text: 'warmup.realmv6.org からデータを転送しています。'.

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

# RPKI workshop

**WORKSHOP ON RPKI: TUTORIAL AND DEPLOYMENT STRATEGIES FOR SECURE INTERNET ROUTING**

**JULY 26 - 27, 2013, BERLIN, GERMANY**

HOME ABOUT REGISTRATION PROGRAM VENUE ORGANIZERS CONTACT

## ABOUT

### OVERVIEW

The current Internet backbone is quite vulnerable against threats. Intended attacks as well as misconfigurations lead to disturbances on the BGP layer. Prominent examples include hijacking of YouTube's IP prefix, and incorrect redirection of 15% of the US Internet traffic to China Telecom in April 2010.

Current efforts of the **Secure-Inter Domain (SIDR)** working group within the **IETF** lie in the standardization of protocols to enhance the security of BGP, taking practical deployability into consideration. They focus on solving two problems: enable a router (a) to verify that a BGP update did originate at an authorized AS

### HALF-DAY EVENT: RPKI TUTORIAL

This tutorial is designed for operators of autonomous systems. We give background about state of the art protection mechanisms against prefix hijacking. The course is complemented by hands-on experiments, where you get experiences of how to protect IP prefixes. After this tutorial you should be able to enable prefix origin validation in your network. We will have an English and German speaking tutorial.

### FULL-DAY EVENT: RPKI DEPLOYMENT STRATEGIES

The aim of this workshop is to bring together Internet operators, policy makers

<http://rpkiws.realmv6.org/>


# プログラム

[HOME](#)[ABOUT](#)[REGISTRATION](#)[PROGRAM](#)[VENUE](#)[ORGANIZERS](#)[CONTACT](#)

## PROGRAM

### JULY 26, 2013: RPKI TUTORIAL (HALF-DAY)

INSTRUCTORS: RANDY BUSH, MATTHIAS WÄHLISCH

 Please bring your laptop for the hands-on part.

12:00 – 13:00 Introduction RPKI

13:00 – 14:00 Basic Tools, Hands-on Cache Server

14:00 – 14:30 Break

14:30 – 16:30 Hands-on Prefix Origin Validation

16:30 – 17:00 Break

17:30 – 18:30 Hands-on experiments & Wrap-up

19:00 Group Dinner together with [SBS Workshop](#).  
This is not sponsored ;), you pay on your own.

### JULY 27, 2013: RPKI DEPLOYMENT STRATEGIES (FULL-DAY)

10:00 Status, Road-Map

Implementations

Deployment Practices

Monitoring

Gap Analysis

Wrap Up

19:00 [ETF Warm-Up!](#) BBQ@Freie Universität Berlin.  
Sponsored by BCDX. [Separate registration](#) required.

<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
	<ul style="list-style-type: none"><li>• Value / Risk</li><li>• Legacy / PI</li><li>• Control (Gov)</li></ul>	<ul style="list-style-type: none"><li>• Monitoring</li><li>• Route (support)</li><li>• Stability</li><li>• Reliability (includes implementation.)</li></ul>	<ul style="list-style-type: none"><li>• BCP / Deployment which people<ul style="list-style-type: none"><li>- ISP</li><li>- Legacy Holder</li><li>- BMN&amp;Co</li></ul></li></ul>

### その他の話題

○Single Root

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

○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

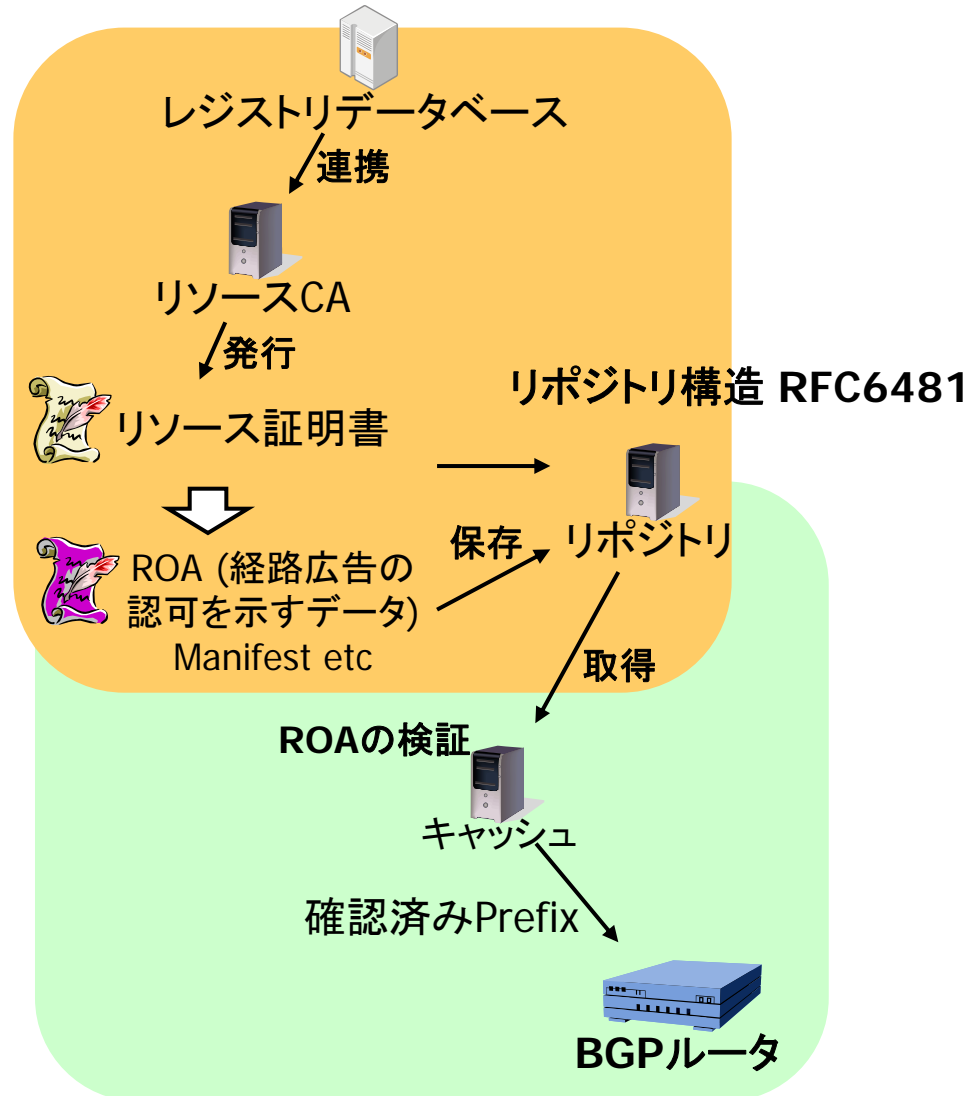
ROA書式 RFC6482

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 (BGPSEC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 — Deployment

- Some available RPKI tools, Carlos, Benno
  - Origin Validation Looking Glass
    - [http://www.labs.lacnic.net/rpkitools/looking\\_glass/](http://www.labs.lacnic.net/rpkitools/looking_glass/)

Origin Validation LG

Available at: [http://www.labs.lacnic.net/rpkitools/looking\\_glass/](http://www.labs.lacnic.net/rpkitools/looking_glass/)

lacniclabs

Origin Validation looking glass

**Search form:**

Query current RPKI Dataset:

Select your query type: Prefix CIDR query (v4 and v6)

Refine your search scope: Search All Routes

Time frame: Last 24 hours

Search

Valid and invalids as of today

Category	Percentage
Valid Routes	86.45%
Invalid / Bad Origins	1.07%
Invalid / Bad Masklen	8.88%
Invalid / Bad Masklen	3.60%

Highcharts.com

4

# アジェンダと議論 — Deployment

## – Origin Validation Looking Glass

Origin Validation LG

lacniclabs Origin Validation looking glass

Query string: 28000 | Query type: asn2 | Query scope: all | Query timeframe: 7 days | Result count: 4  
Bookmark this query as a REST URI: [http://www.labs.lacnic.net/rpkitools/looking\\_glass/rest/all/asn2/28000/](http://www.labs.lacnic.net/rpkitools/looking_glass/rest/all/asn2/28000/)

Prefix	SIDR Status	OriginAS	Last Seen	More info
200.7.84.0/23	Valid	28000	Aug. 1, 2013, 8:52 a.m.	<a href="#">More info...</a>
200.7.87.0/24	Valid	28000	Aug. 1, 2013, 8:52 a.m.	<a href="#">More info...</a>
2001:13c7:7001::/48	Valid	28000	Aug. 1, 2013, 8:52 a.m.	<a href="#">More info...</a>
200.10.62.0/23	Valid	28000	Aug. 1, 2013, 8:52 a.m.	<a href="#">More info...</a>

lacniclabs

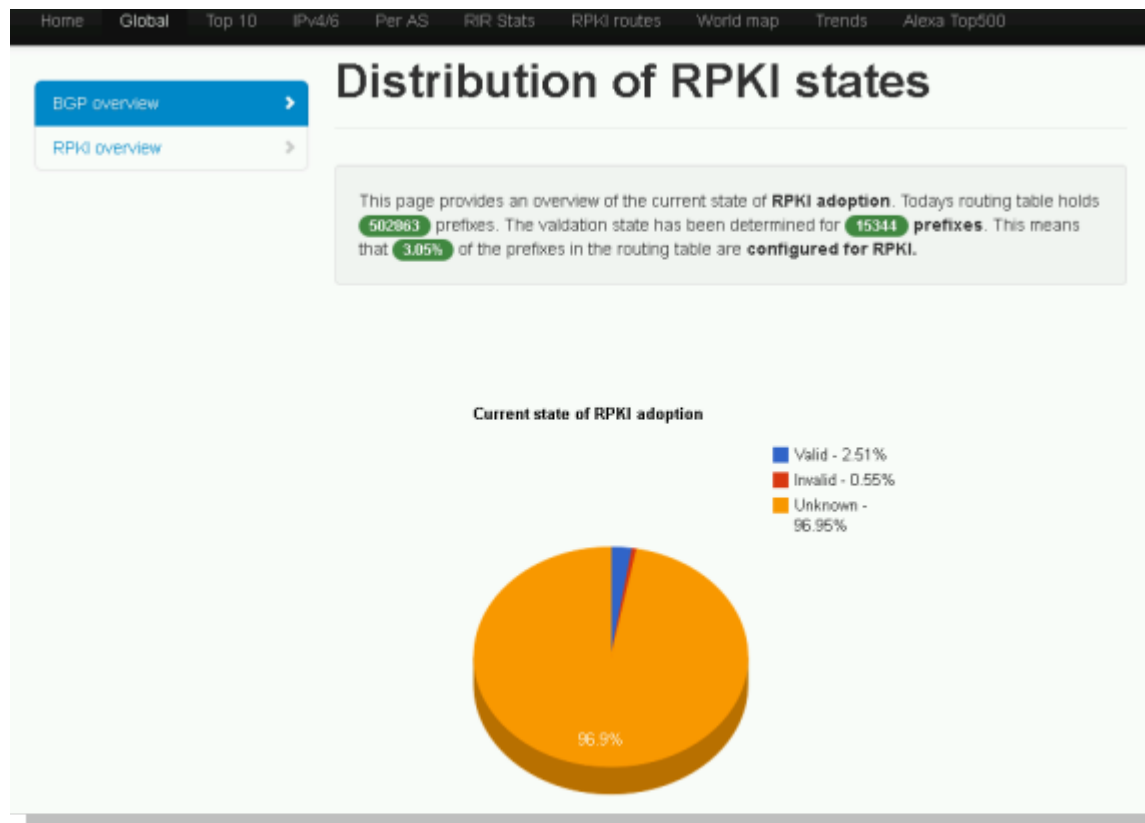
[www.labs.lacnic.net/rpkitools/looking\\_glass/rest/all/asn2/28000/](http://www.labs.lacnic.net/rpkitools/looking_glass/rest/all/asn2/28000/)

```
200.7.84.0/23|Valid|28000
200.7.87.0/24|Valid|28000
2001:13c7:7001::/48|Valid|28000
200.10.62.0/23|Valid|28000
```

# アジェンダと議論 — Deployment

## – RPKI Dashboard

- <http://rpki.surfnet.nl/>



# アジェンダと議論 — Deployment

## – ROA Wizard

The screenshot shows the 'rpki roa wizard' interface. At the top left is the logo. A blue callout bubble on the right says 'User enters his/hers LACNIC ORG-ID'. Below this, the 'Org ID:' field contains 'UY-ANTA-LACNIC'. A red arrow points from this field to a table of recommended prefixes for 'ROA - AS6057: (Criterio 1)'. The table has two columns: 'Prefix' and 'Max length'. The table contains the following data:

Prefix	Max length
179.24.0.0/13	20
186.48.0.0/14	20
186.52.0.0/14	20
190.0.128.0/19	20
190.132.0.0/16	20
190.133.0.0/16	20
190.134.0.0/15	20
190.64.0.0/17	20

A small number '6' is visible in the bottom right corner of the interface.

# アジェンダと議論 — Deployment

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

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	11256 (100%)	16 (0.14%)	39 (0.35%)	11201 (99.51%)	29.09%	0.49%
APNIC	117349 (100%)	85 (0.07%)	214 (0.18%)	117050 (99.75%)	28.43%	0.25%
ARIN	183166 (100%)	224 (0.12%)	31 (0.02%)	182911 (99.86%)	87.84%	0.14%
LACNIC	56913 (100%)	5517 (9.69%)	1148 (2.02%)	50248 (88.29%)	82.78%	11.71%
RIPE NCC	129120 (100%)	6503 (5.04%)	1151 (0.89%)	121466 (94.07%)	84.96%	5.93%

Much Better Than IPv6

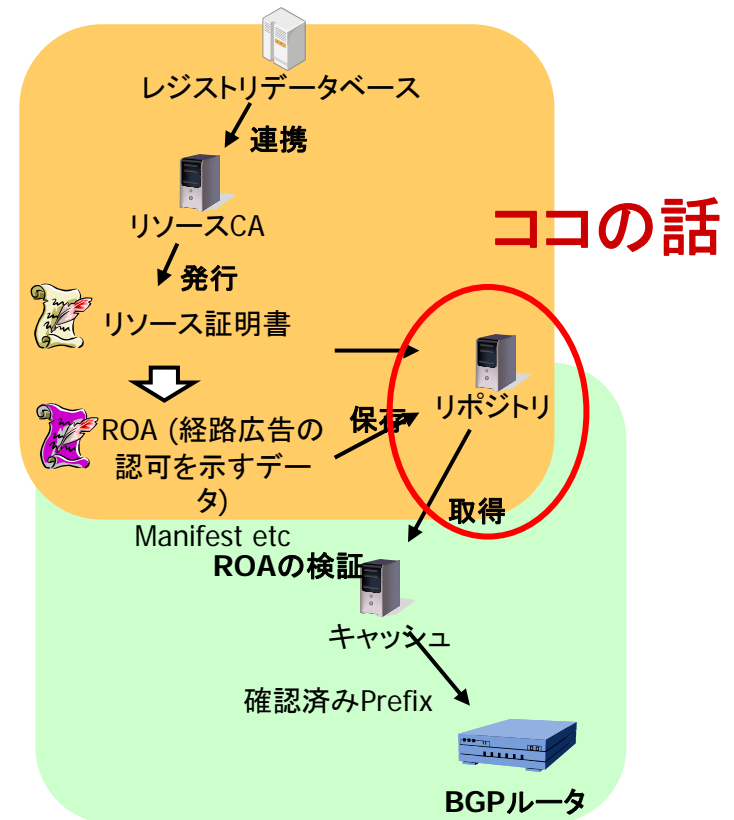
Half are Two LIRs

Embarrassing

2013.07.26 Berlin RPKI 73

# アジェンダと議論 — Revised

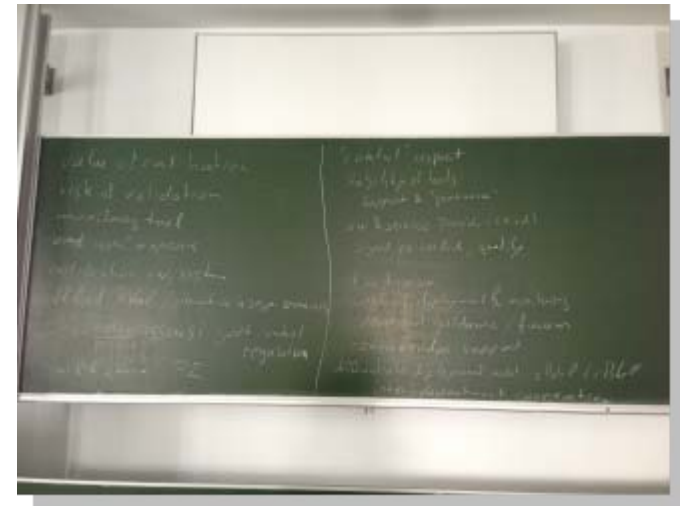
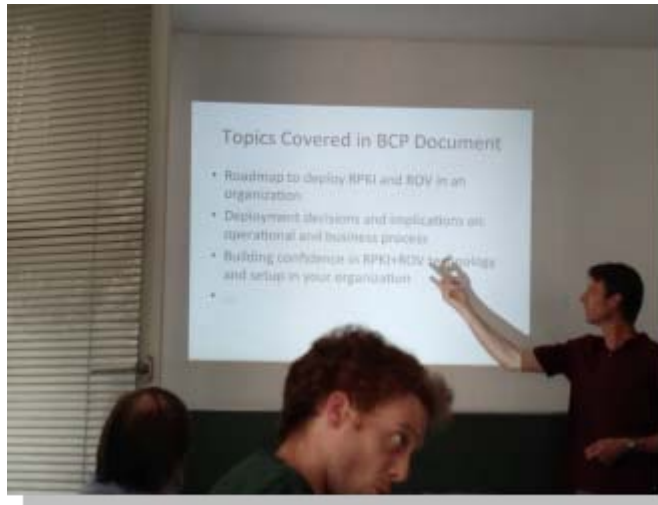
- RSYNC Performance Study
  - RPKIオブジェクトを集めてクライアント数をシミュレートして時間を計測。
  - slides-87-sidr-11.pdf





# 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）



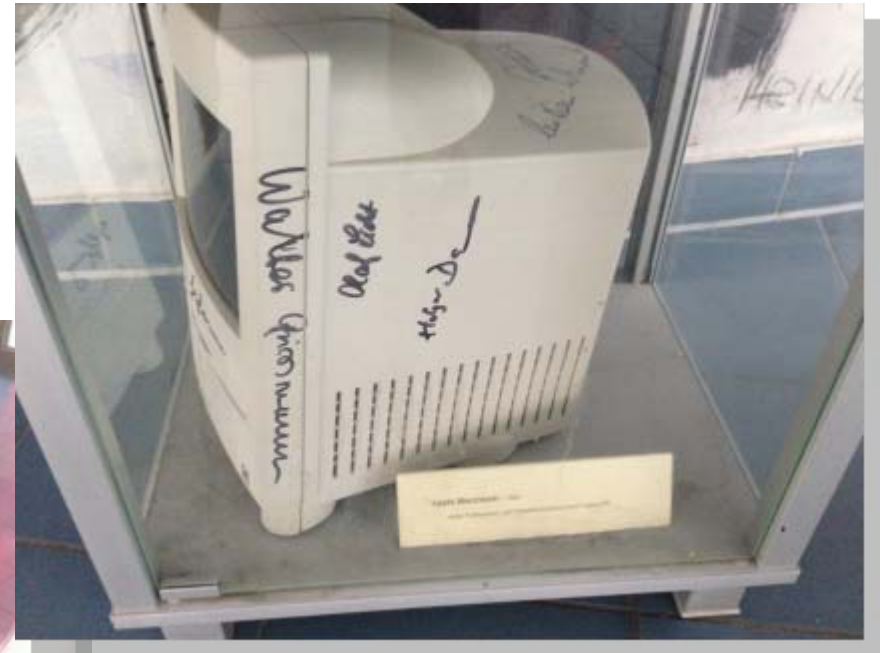
# 会場のInterContinental



# 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

