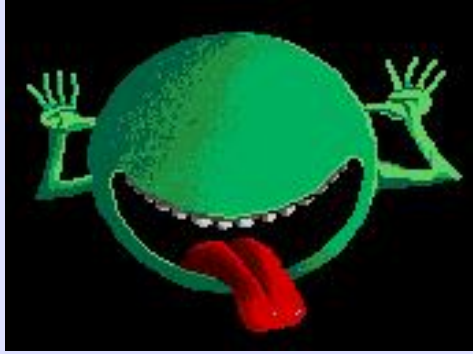# Measuring RPKI Repositories

JaNOG / Kurashiki
2012.05.06
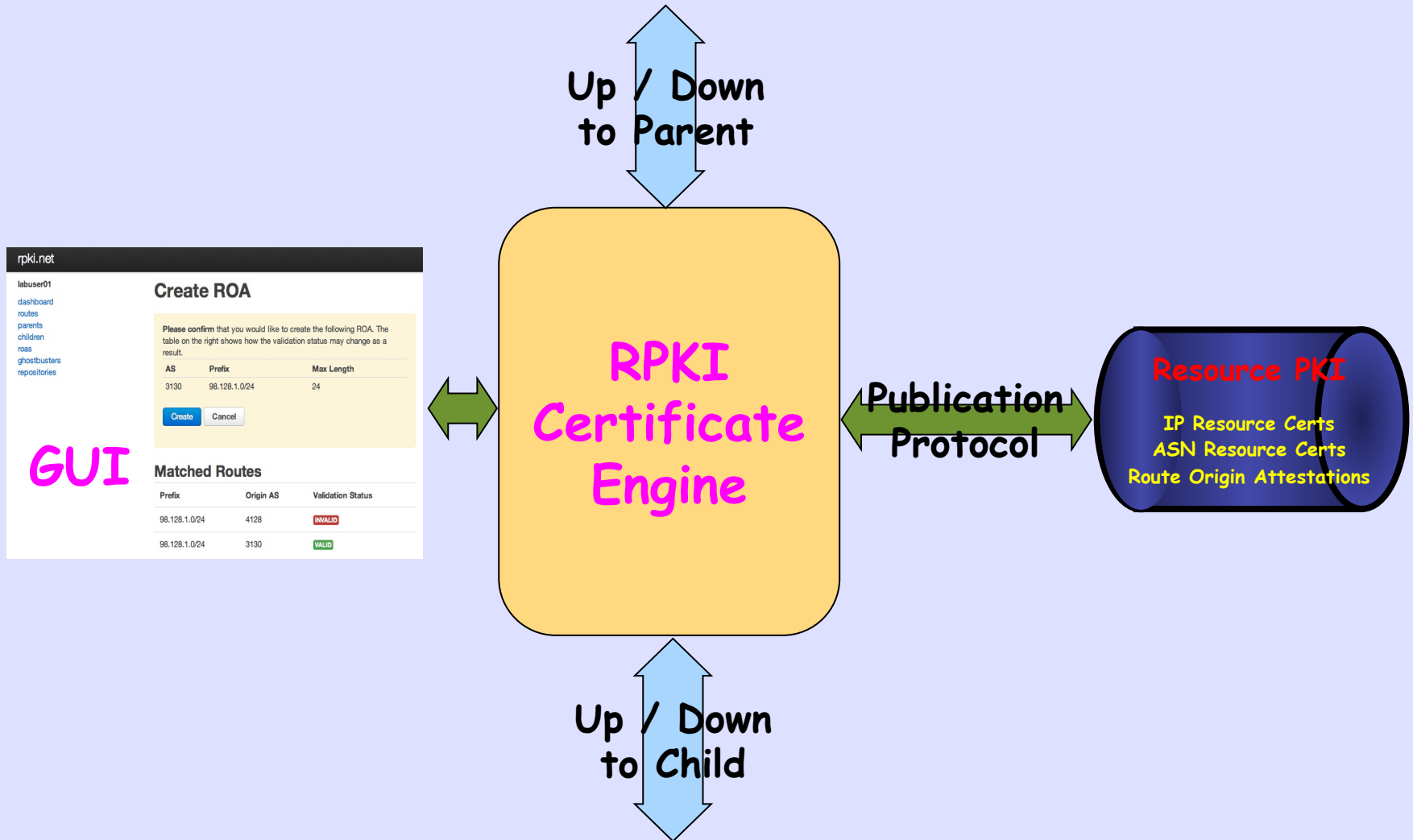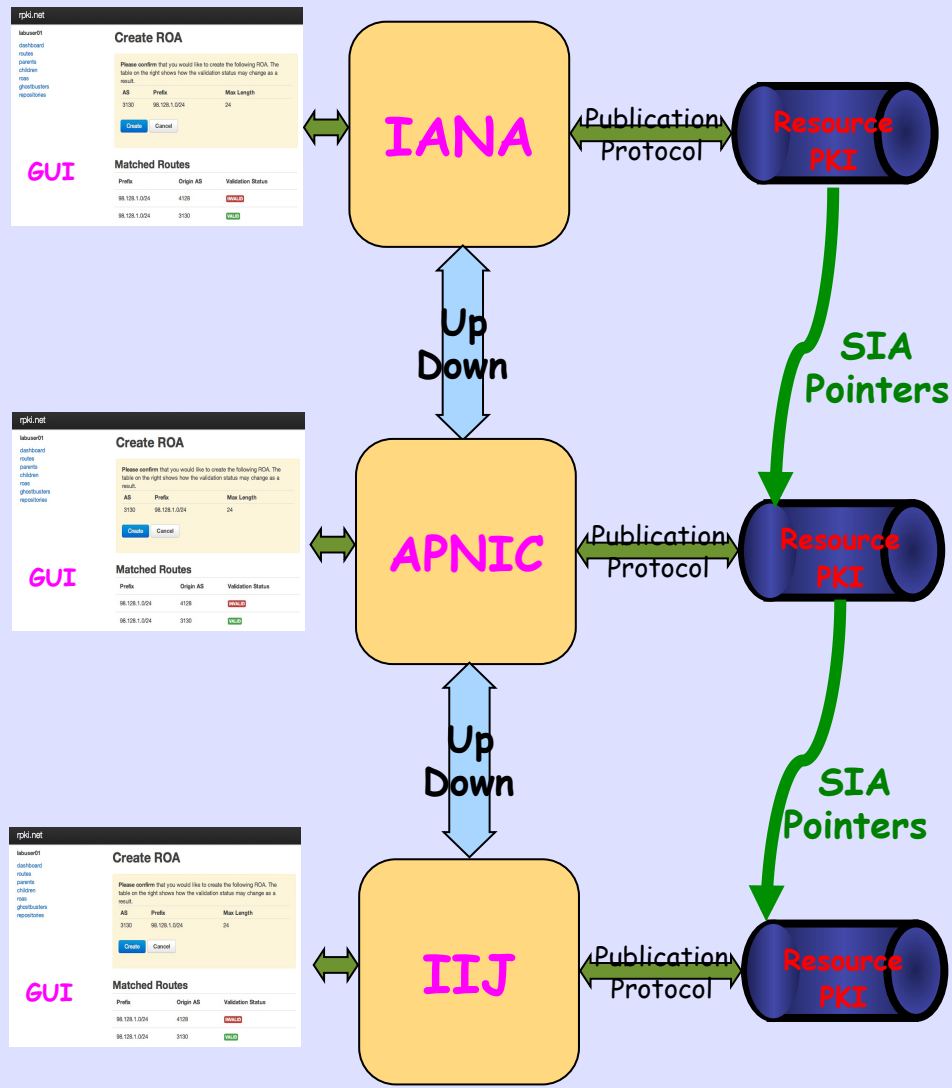
Randy Bush <randy@psg.com>

Don't Panic

- 私はエンジニアなんで、問題点にフォーカスするのは当然のこと

- そして研究者であるため、問題にしか興味ない

- **RPKI**は実は順調です（キリッ

- だけど、今日は主に問題点についてお話します

Review
of
RPKI Structure
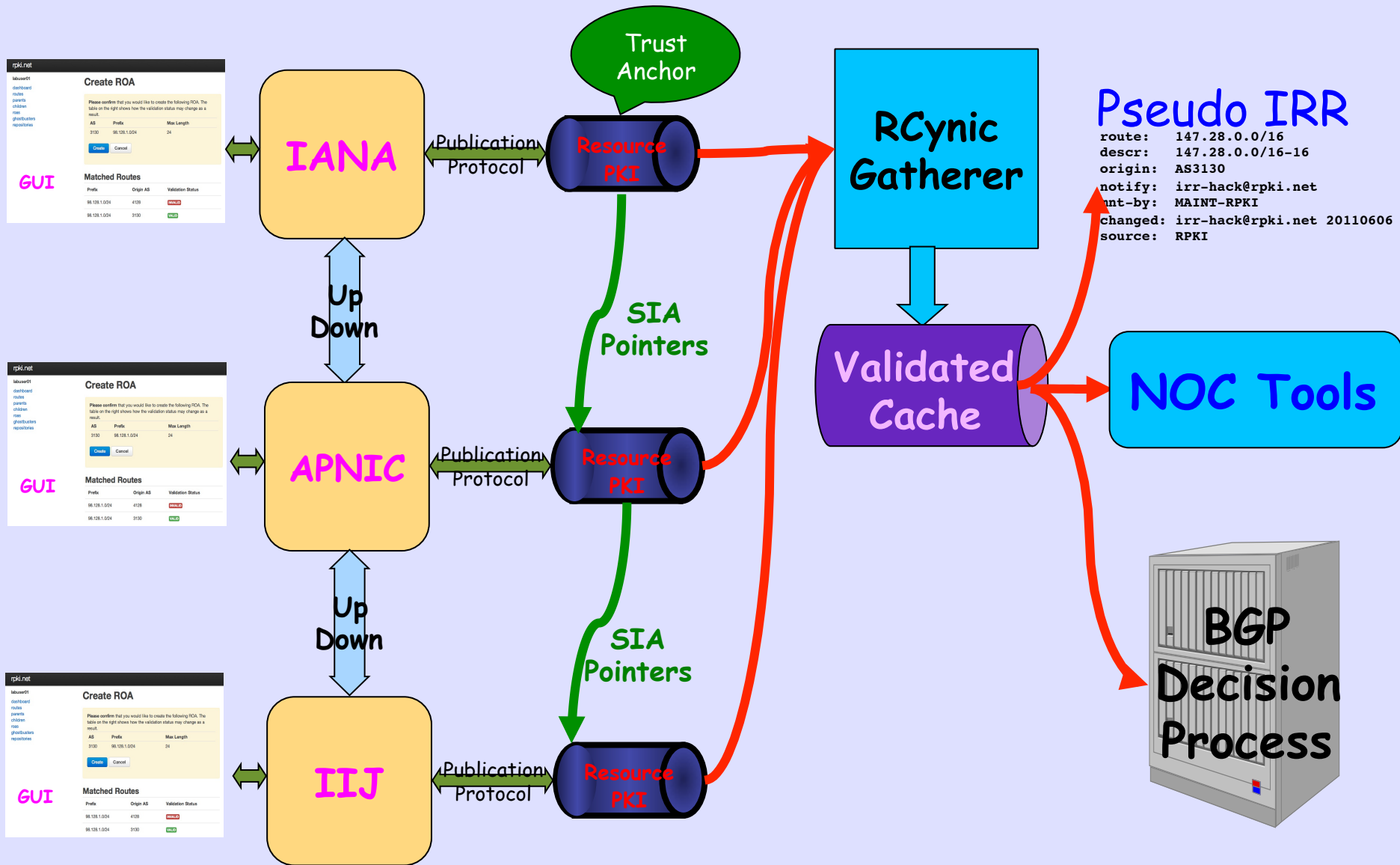
Publishing / Issuing Party

Up / Down to Parent

RPKI Certificate Engine

GUI

rpki.net

labuser01

dashboard
routes
parents
children
roas
ghostbusters
repositories

Create ROA

Please confirm that you would like to create the following ROA. The table on the right shows how the validation status may change as a result.

AS	Prefix	Max Length
3130	98.128.1.0/24	24

Create | Cancel

Matched Routes

Prefix	Origin AS	Validation Status
98.128.1.0/24	4128	INVALID
98.128.1.0/24	3130	VALID

Publication Protocol

Resource PKI

IP Resource Certs
ASN Resource Certs
Route Origin Attestations

Up / Down to Child

Issuing Parties

GUI

IANA ⟷ Publication Protocol ⟷ Resource PKI

Up Down

SIA Pointers

GUI

APNIC ⟷ Publication Protocol ⟷ Resource PKI

Up Down

SIA Pointers

GUI

IIJ ⟷ Publication Protocol ⟷ Resource PKI

Issuing Parties

Relying Parties

Trust Anchor

IANA

GUI

Publication Protocol

Resource PKI

Up Down

APNIC

GUI

Publication Protocol

Resource PKI

SIA Pointers

Up Down

IIJ

GUI

Publication Protocol

Resource PKI

SIA Pointers

RCynic Gatherer

Validated Cache

Pseudo IRR

```
route:    147.28.0.0/16
descr:    147.28.0.0/16-16
origin:   AS3130
notify:   irr-hack@rpki.net
mnt-by:   MAINT-RPKI
changed:  irr-hack@rpki.net 20110606
source:   RPKI
```

NOC Tools

BGP Decision Process

My Routing Relies on It!

- ルーティングを**RPKI**に依存させるなら、**publication**の仕組の信頼性はとっても大事

- **relying party**用ソフトウェアは、当然障害が発生する事を想定してコーディングされているはず、、、なのでそんなに深刻じゃない

- でも今の**publication**を見ると、運用品質とはほど遠い

- これは修正が必要

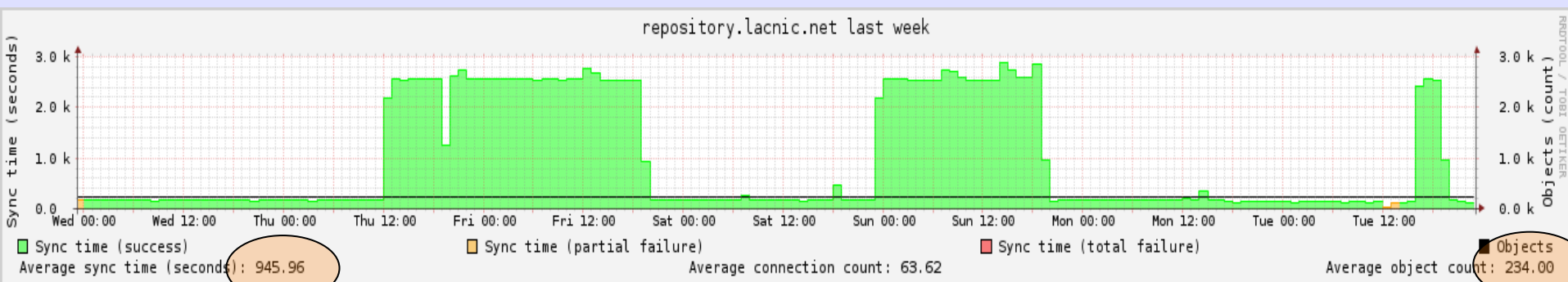# These Graphs are from rpki.net's Relying Party Software Web Page it Makes for You
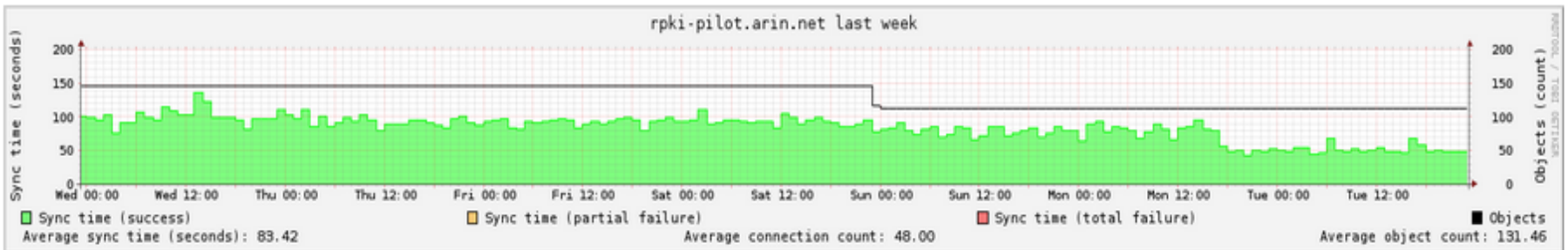
Not Bad

An ISP

pubd-pilot.lab.dtag.de last week

Legend: Sync time (success) | Sync time (partial failure) | Sync time (total failure) | Objects

Average sync time (seconds): 3.14 | Average connection count: 1.00 | Average object count: 3.00

An RIR

repository.lacnic.net last week

Legend: Sync time (success) | Sync time (partial failure) | Sync time (total failure) | Objects

Average sync time (seconds): 945.96 | Average connection count: 63.62 | Average object count: 234.00

Not So Good

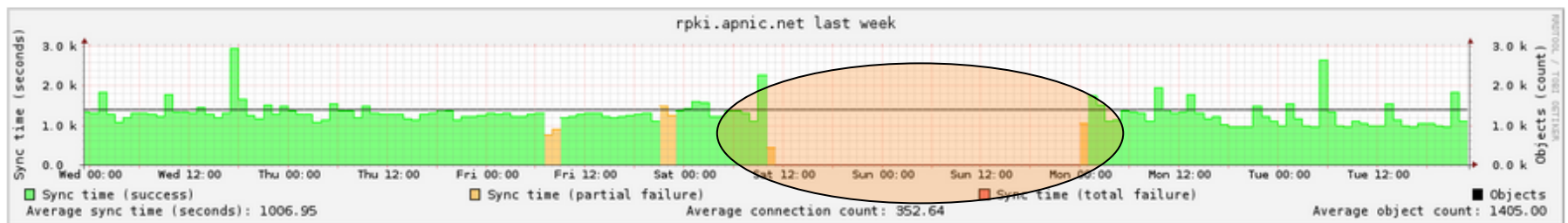## Overview for repository rpki-pilot.arin.net

	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
																		48
current .cer										18					48		48	
current .crl																	2	
current .mnf		48					48		18	11								
current .roa		14					14		5	5					14			
Total		62					62		23	34					62		50	48

rpki-pilot.arin.net last week

Sync time (success) · Sync time (partial failure) · Sync time (total failure) · Objects
Average sync time (seconds): 83.42   Average connection count: 48.00   Average object count: 131.46

Very Bad

Overview for repository rpki.apnic.net

	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
																		459
current .cer									457	1							459	
current .crl									1								459	
current .mft									1								459	
current .roa								15									28	
Total								15	459	1							1405	459

rpki.apnic.net last week

Sync time (success) — Sync time (partial failure) — Sync time (total failure) — Objects
Average sync time (seconds): 1006.95   Average connection count: 352.64   Average object count: 1405.00

- They do not monitor and have no real NOC
- They do not work weekends
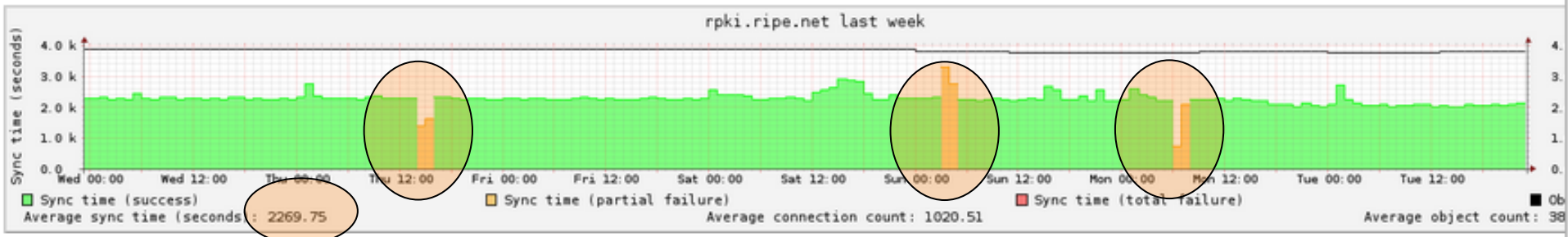- I had to write a friend in APNIC Engineering

RIPE Stayed Up

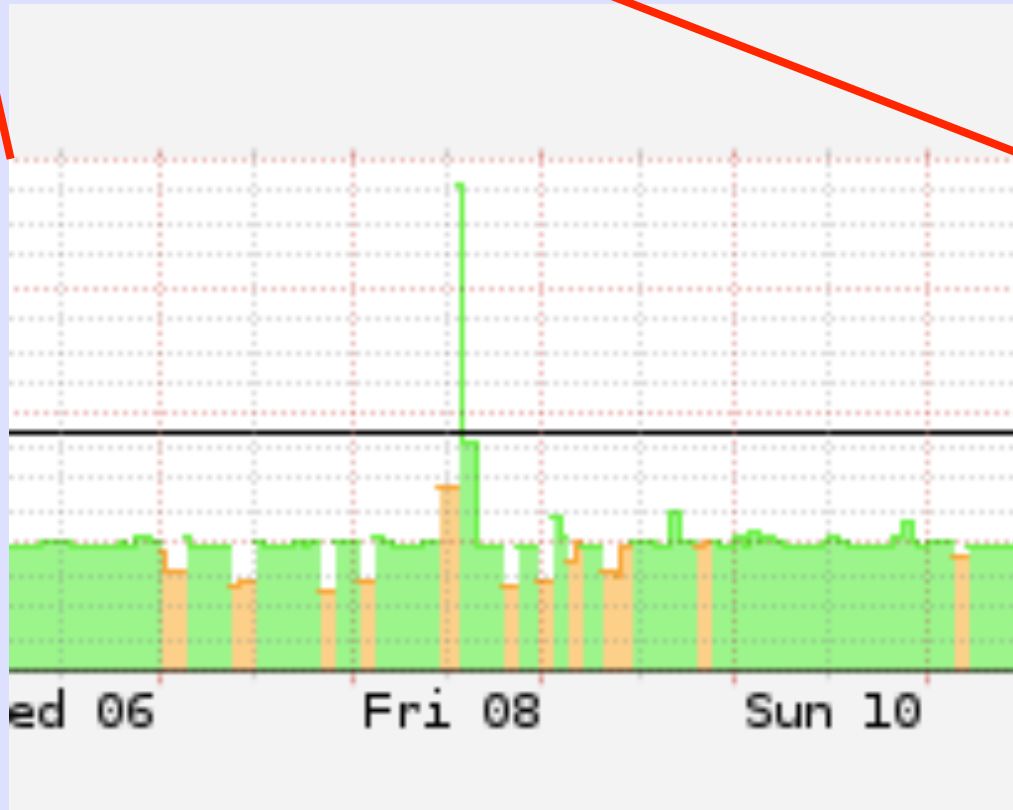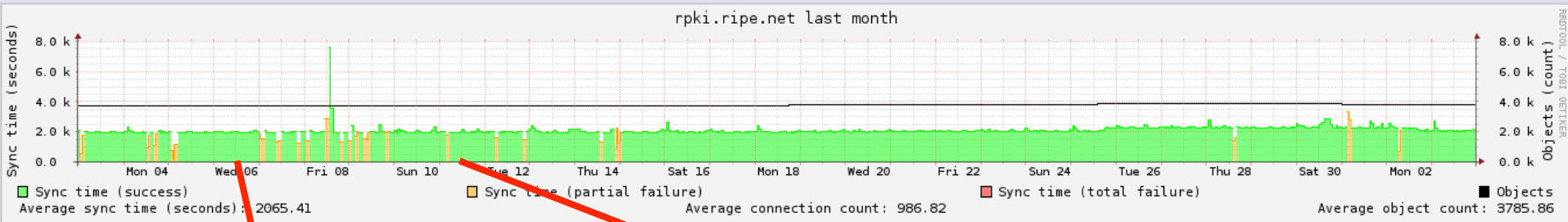## Repository details for rpki.ripe.net 2012-07-03T23:10:13Z

Overview   Repositories   Problems   All Details

	certificate has expired	Bad keyUsage	Certificate failed validation	CRL not yet valid	CRLDP doesn't match issuer's SIA	Manifest not yet valid	Object rejected	EE certificate with 1024 bit key	Nonconformant X.509 issuer name	Nonconformant X.509 subject name	rsync partial transfer	Stale CRL or manifest	Tainted by stale CRL	Tainted by stale manifest	Tainted by not being in manifest	Non-rsync URI in extension	Object accepted	rsync transfer succeeded
																		1036
current .cer									1033	101							1035	
current .crl									101								1035	
current .mft									101	1							1035	
backup .roa								17	6						35		35	
current .roa								500	78								693	
Total								517	1319	102					35		3833	1036

rpki.ripe.net over last week

rpki.ripe.net last week

Average sync time (seconds): 2269.75   Average connection count: 1020.51   Average object count: 38

RIPE has Bad History

rpki.ripe.net last month

Sync time (success) Sync time (partial failure) Sync time (total failure) Objects
Average sync time (seconds): 2065.41   Average connection count: 986.82   Average object count: 3785.86

Cause

- 原因はNFS (NFS is Evil!)
- 数ヶ月続いた
- RPKI.NET のログを見ると"NFS"とはっきりわかる
- でも「RIRで問題が起きるなんて考えられない」
- やっとなおったけど、課題は残っている

The RIRs are Not Network Operators

## They're 電話会社, "There can be no problem"

Good Software Will Save US

- relying party softwareが障害時の対応をうまくやってくれれば、さほど深刻でない

- rpki.net relying party software は、新しいデータが取得できない場合古いデータを使い続ける
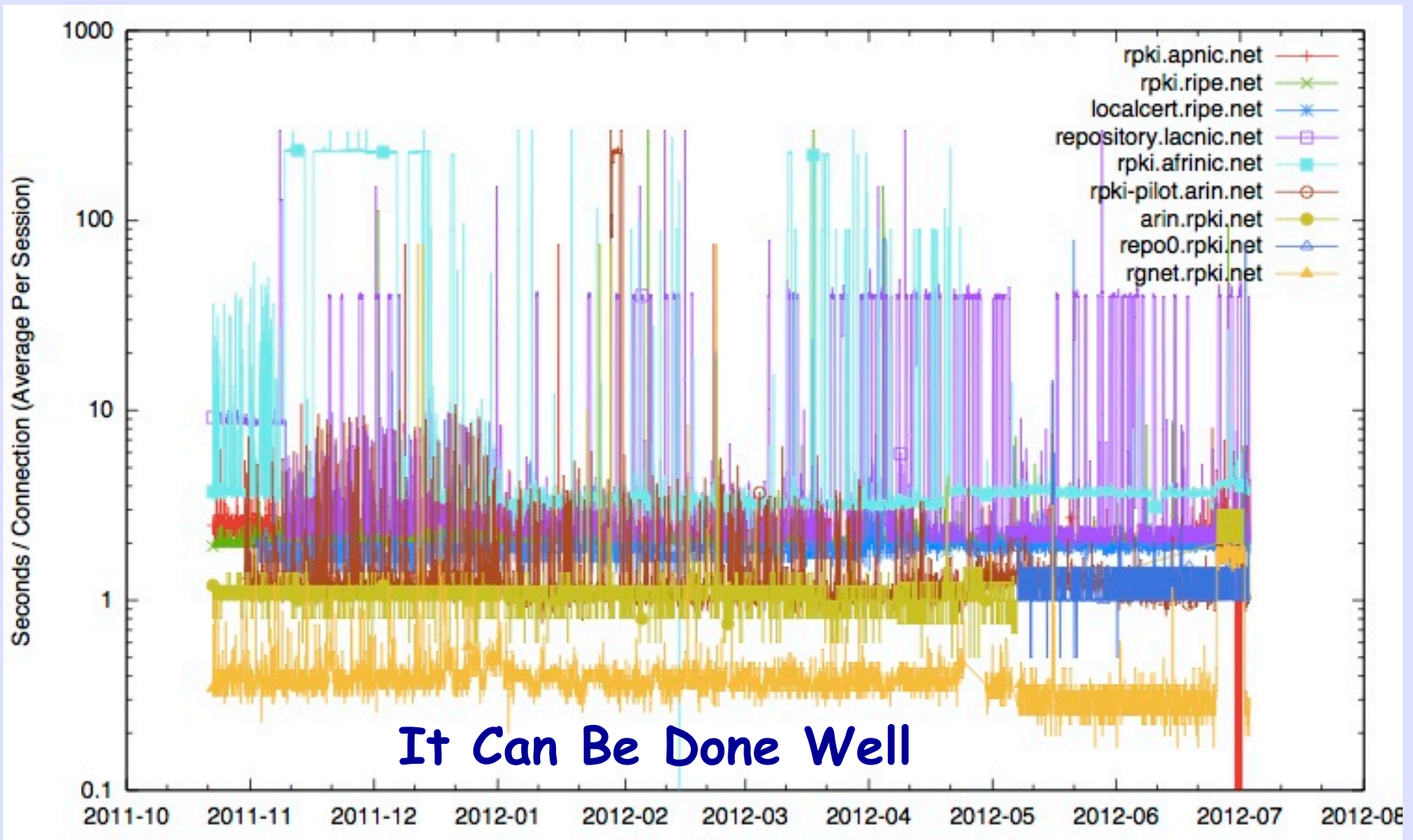
- RPKIデータはわりと安定してるからまぁOK

- しかし、RIPEの逆引きは5日間も障害継続した

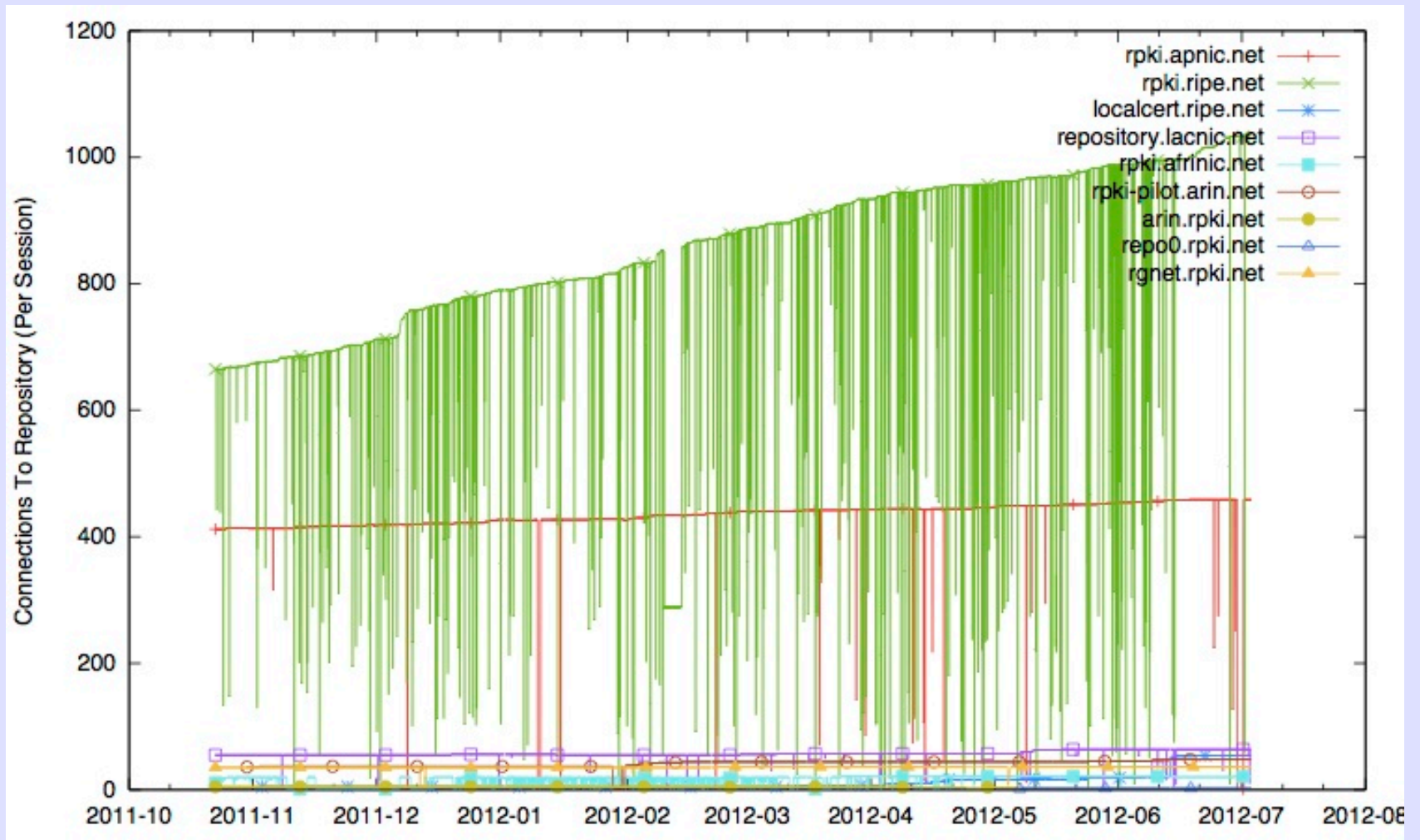# Some Statistics

Again, from rpki.net Relying Party Software

Connect Time (linear)

RIPE & APNIC Very Slow
Deliberately Bad Directory Structure
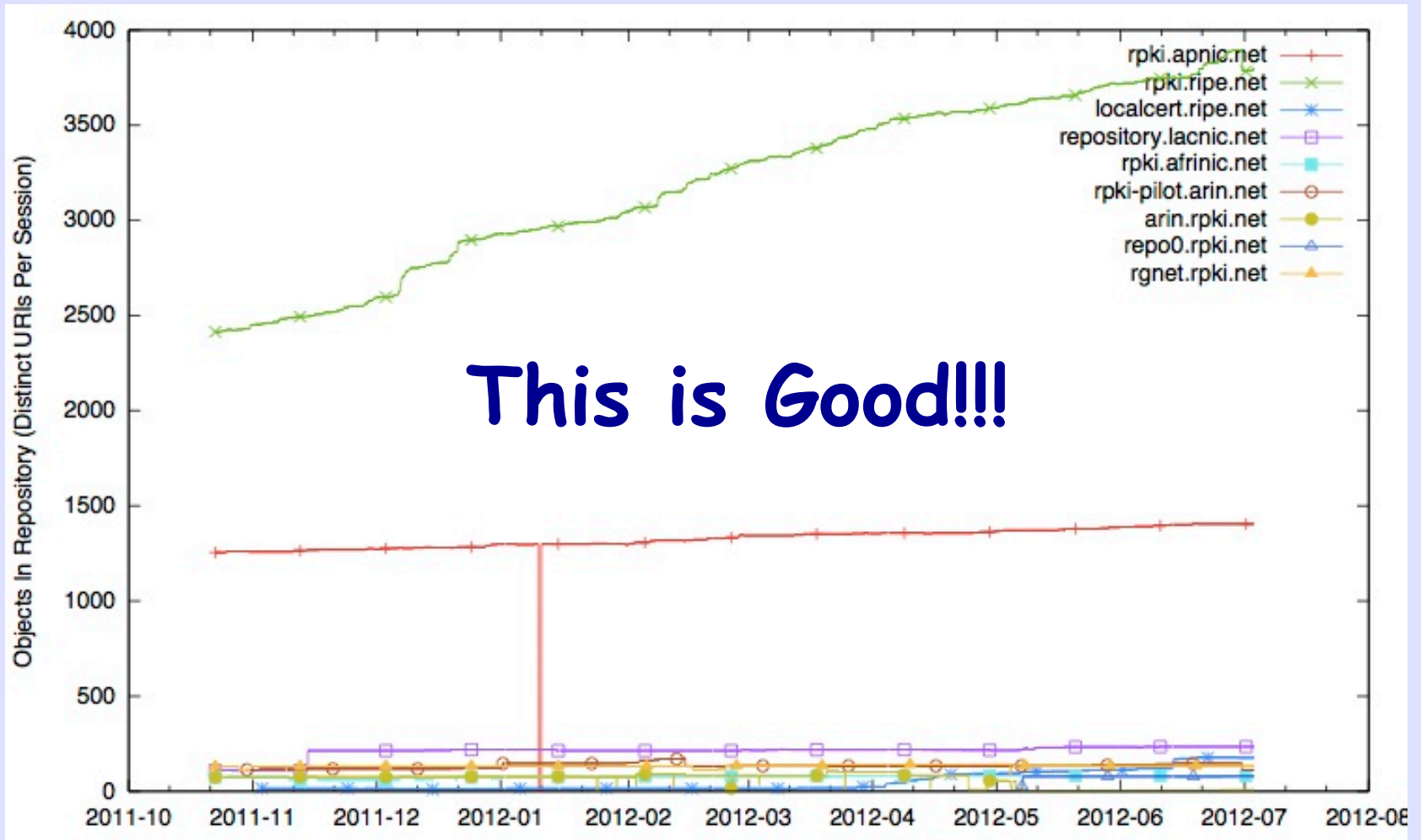
Connect Time (log)

It Can Be Done Well
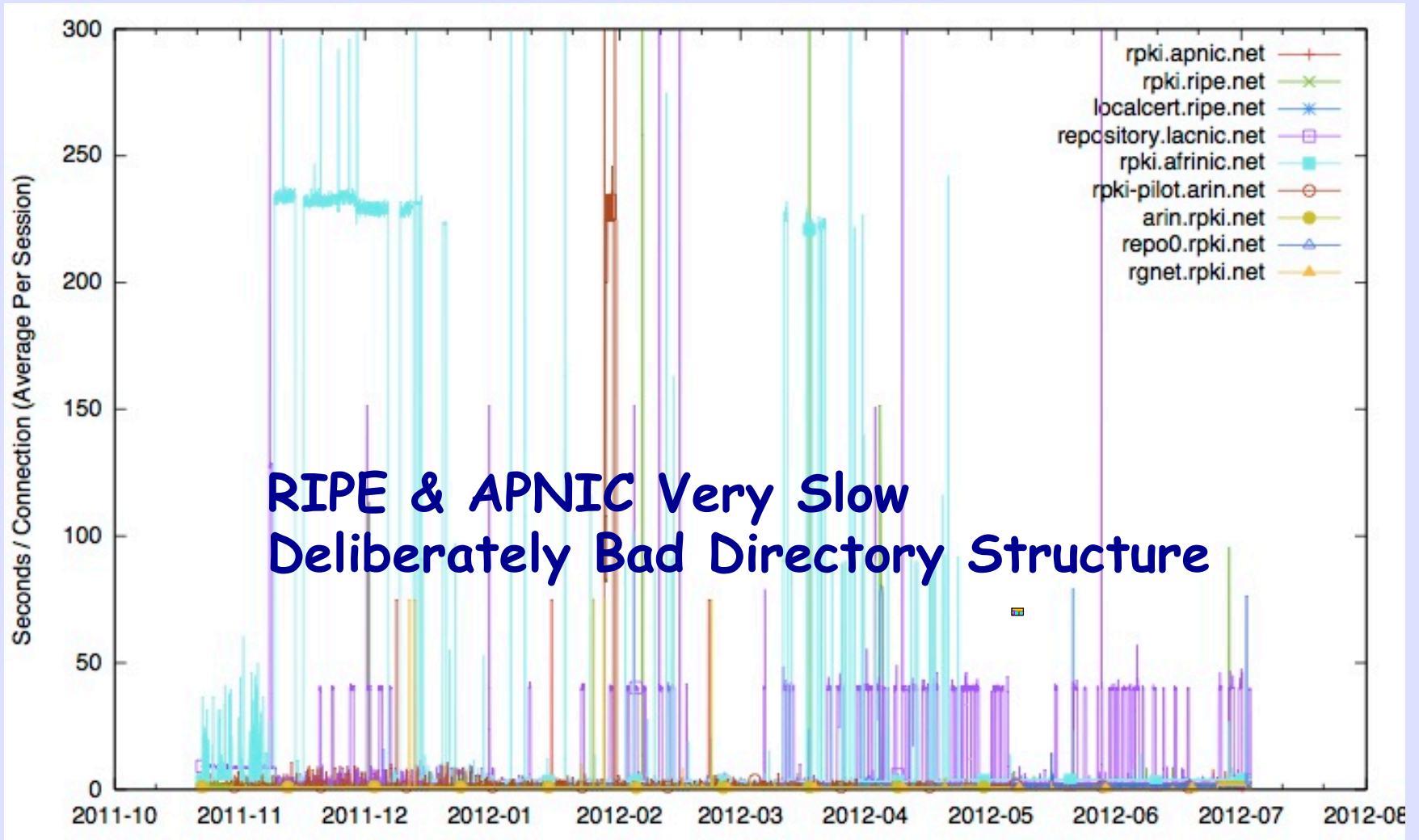
Connection Counts

Number of Objects

This is Good!!!

Conclusions

- RPKI は本気でdeployされはじめている、特にRIPE地域で活発

- RIRは運用品質からほど遠い

- JPNIC はお手本になれる

- APNIC & RIPE Publication 構造は修正が必要

- Relying Party software の機能で問題回避

- More Measurement and Monitoring

I do not deserve the credit. I have no plan or goals. I was raised by strong women, and learned to follow 'suggestions'. So I have simply done what folk asked of me. It just happened that a lot of people said "Teach us," or "Connect us to the Internet."

The hard work was and is done by many SE Asians, Africans, Pacific Islanders, American Indians, etc. I had the privilege of working with many. They are wonderful people. It is they who deserve awards.

For example, the first workshops were done by Alvise Nobile in Trieste in the late '80s (I taught there). People such as Michuki Mwangi, Aminu Ibrahim, Dorcas Muthoni of Linux Chicks, are doing great work in Africa now, ask them what you can do to help. Kanchana can use some help with a joomla break-in on the TH ccTLD provisioning system in Bangkok right now.

I owe a deep debt to IIJ and previously NTT for supporting my work for many years.