BGPMONとハイジャックされた話

Shishio Tsuchiya

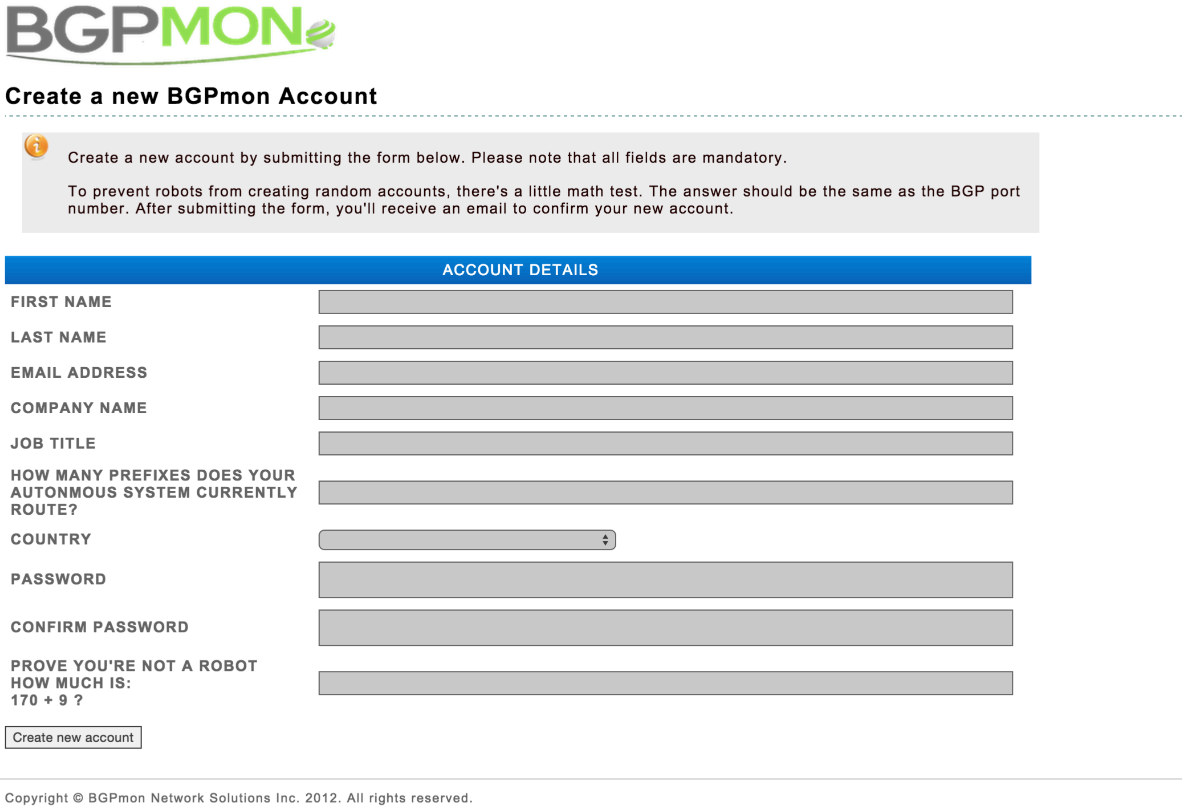
shtsuchi@cisco.com

BGPmonって？

- AS271 UBC/BCNETで使用してたScriptセット
- 2008年公開
- 数千ユーザーが使用しているBGPモニターツール
- Prefix Hijack
- Policy violations
- ROA validation failures

などのモニター可能

アカウント登録



Create a new BGPmon Account

Create a new account by submitting the form below. Please note that all fields are mandatory.

To prevent robots from creating random accounts, there's a little math test. The answer should be the same as the BGP port number. After submitting the form, you'll receive an email to confirm your new account.

ACCOUNT DETAILS

FIRST NAME

LAST NAME

EMAIL ADDRESS

COMPANY NAME

JOB TITLE

HOW MANY PREFIXES DOES YOUR AUTONMOUS SYSTEM CURRENTLY ROUTE?

COUNTRY

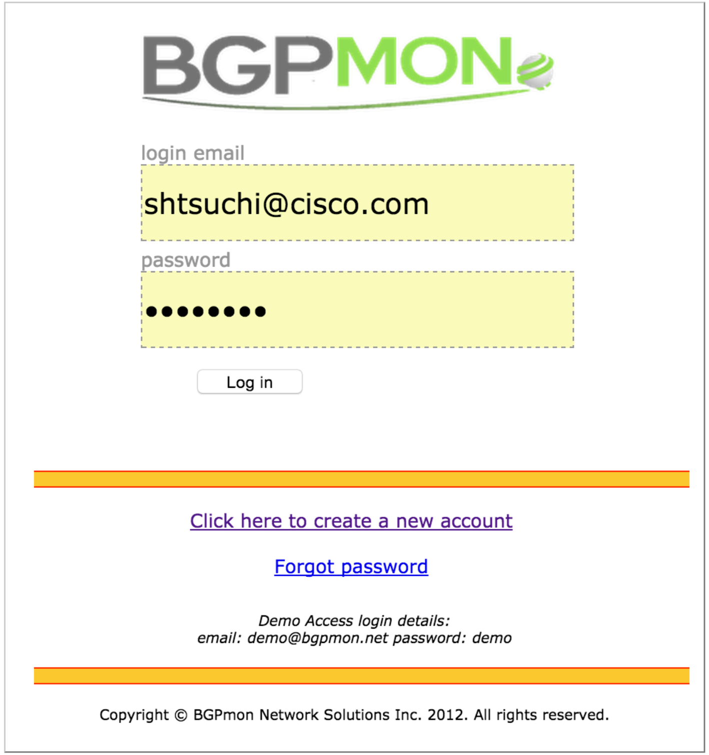
PASSWORD

CONFIRM PASSWORD

PROVE YOU'RE NOT A ROBOT
HOW MUCH IS:
170 + 9 ?

https://portal.bgpmon.net/register.php

ログイン



login email

shtsuchi@cisco.com

password

●●●●●●●●

Click here to create a new account

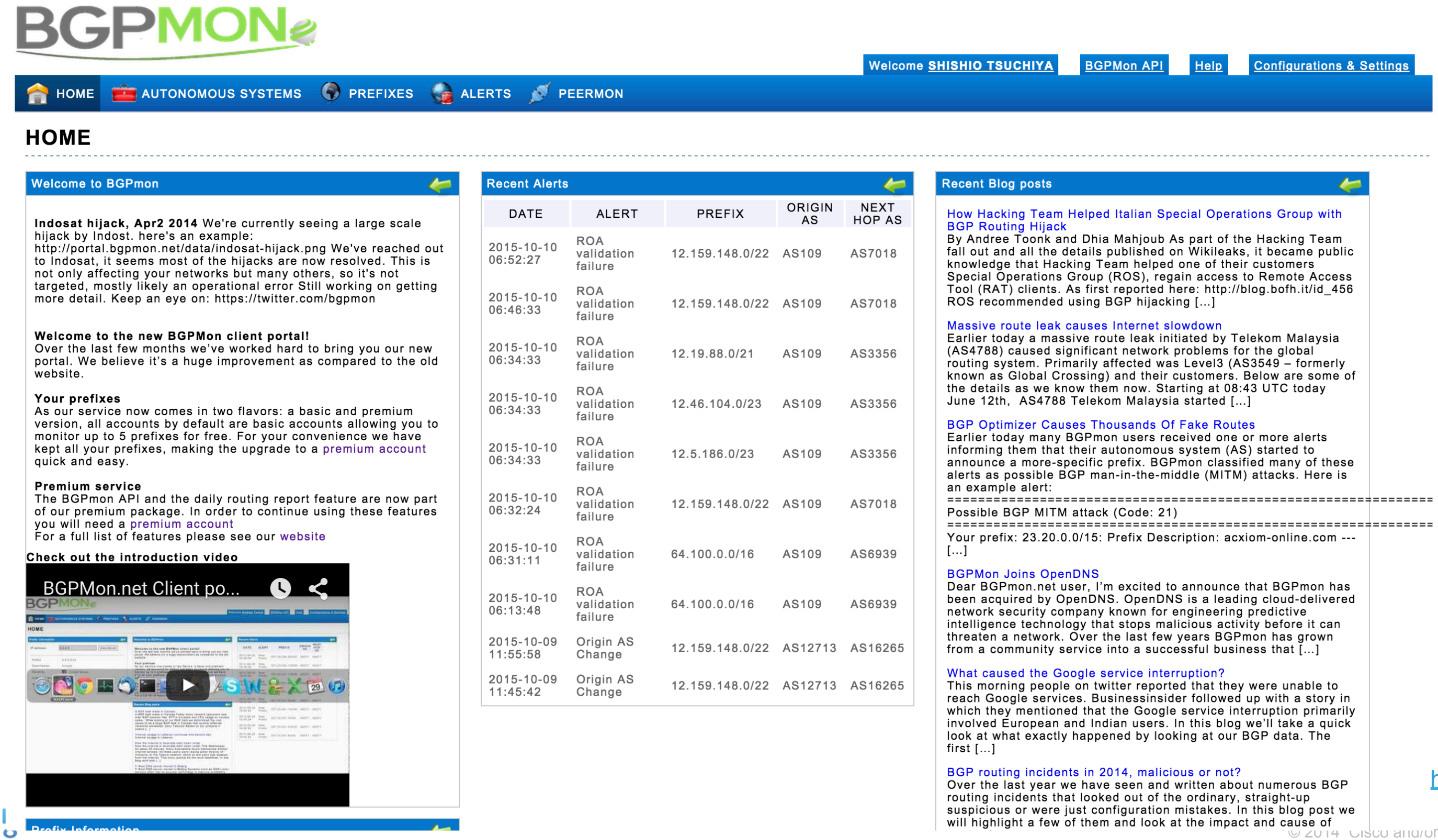
Forgot password

Demo Access login details:
email: demo@bgpmon.net password: demo

Copyright © BGPmon Network Solutions Inc. 2012. All rights reserved.

https://portal.bgpmon.net/login.php

ポータル画面



BGPMON

Welcome **SHISHIO TSUCHIYA** | BGPMon API | Help | Configurations & Settings

HOME | AUTONOMOUS SYSTEMS | PREFIXES | ALERTS | PEERMON

HOME

Welcome to BGPmon

Indosat hijack, Apr2 2014 We're currently seeing a large scale hijack by Indost. here's an example: http://portal.bgpmon.net/data/indosat-hijack.png We've reached out to Indosat, it seems most of the hijacks are now resolved. This is not only affecting your networks but many others, so it's not targeted, mostly likely an operational error Still working on getting more detail. Keep an eye on: https://twitter.com/bgpmon

Welcome to the new BGPMon client portal!
Over the last few months we've worked hard to bring you our new portal. We believe it's a huge improvement as compared to the old website.

Your prefixes
As our service now comes in two flavors: a basic and premium version, all accounts by default are basic accounts allowing you to monitor up to 5 prefixes for free. For your convenience we have kept all your prefixes, making the upgrade to a premium account quick and easy.

Premium service
The BGPmon API and the daily routing report feature are now part of our premium package. In order to continue using these features you will need a premium account
For a full list of features please see our website

Check out the introduction video

BGPMon.net Client po...

Prefix Information

Recent Alerts

DATE	ALERT	PREFIX	ORIGIN AS	NEXT HOP AS
2015-10-10 06:52:27	ROA validation failure	12.159.148.0/22	AS109	AS7018
2015-10-10 06:46:33	ROA validation failure	12.159.148.0/22	AS109	AS7018
2015-10-10 06:34:33	ROA validation failure	12.19.88.0/21	AS109	AS3356
2015-10-10 06:34:33	ROA validation failure	12.46.104.0/23	AS109	AS3356
2015-10-10 06:34:33	ROA validation failure	12.5.186.0/23	AS109	AS3356
2015-10-10 06:32:24	ROA validation failure	12.159.148.0/22	AS109	AS7018
2015-10-10 06:31:11	ROA validation failure	64.100.0.0/16	AS109	AS6939
2015-10-10 06:13:48	ROA validation failure	64.100.0.0/16	AS109	AS6939
2015-10-09 11:55:58	Origin AS Change	12.159.148.0/22	AS12713	AS16265
2015-10-09 11:45:42	Origin AS Change	12.159.148.0/22	AS12713	AS16265

Recent Blog posts

How Hacking Team Helped Italian Special Operations Group with BGP Routing Hijack
By Andree Toonk and Dhia Mahjoub As part of the Hacking Team fall out and all the details published on Wikileaks, it became public knowledge that Hacking Team helped one of their customers Special Operations Group (ROS), regain access to Remote Access Tool (RAT) clients. As first reported here: http://blog.bofh.it/id_456 ROS recommended using BGP hijacking […]

Massive route leak causes Internet slowdown
Earlier today a massive route leak initiated by Telekom Malaysia (AS4788) caused significant network problems for the global routing system. Primarily affected was Level3 (AS3549 – formerly known as Global Crossing) and their customers. Below are some of the details as we know them now. Starting at 08:43 UTC today June 12th, AS4788 Telekom Malaysia started […]

BGP Optimizer Causes Thousands Of Fake Routes
Earlier today many BGPmon users received one or more alerts informing them that their autonomous system (AS) started to announce a more-specific prefix. BGPmon classified many of these alerts as possible BGP man-in-the-middle (MITM) attacks. Here is an example alert:
==
Possible BGP MITM attack (Code: 21)
==
Your prefix: 23.20.0.0/15: Prefix Description: acxiom-online.com --- […]

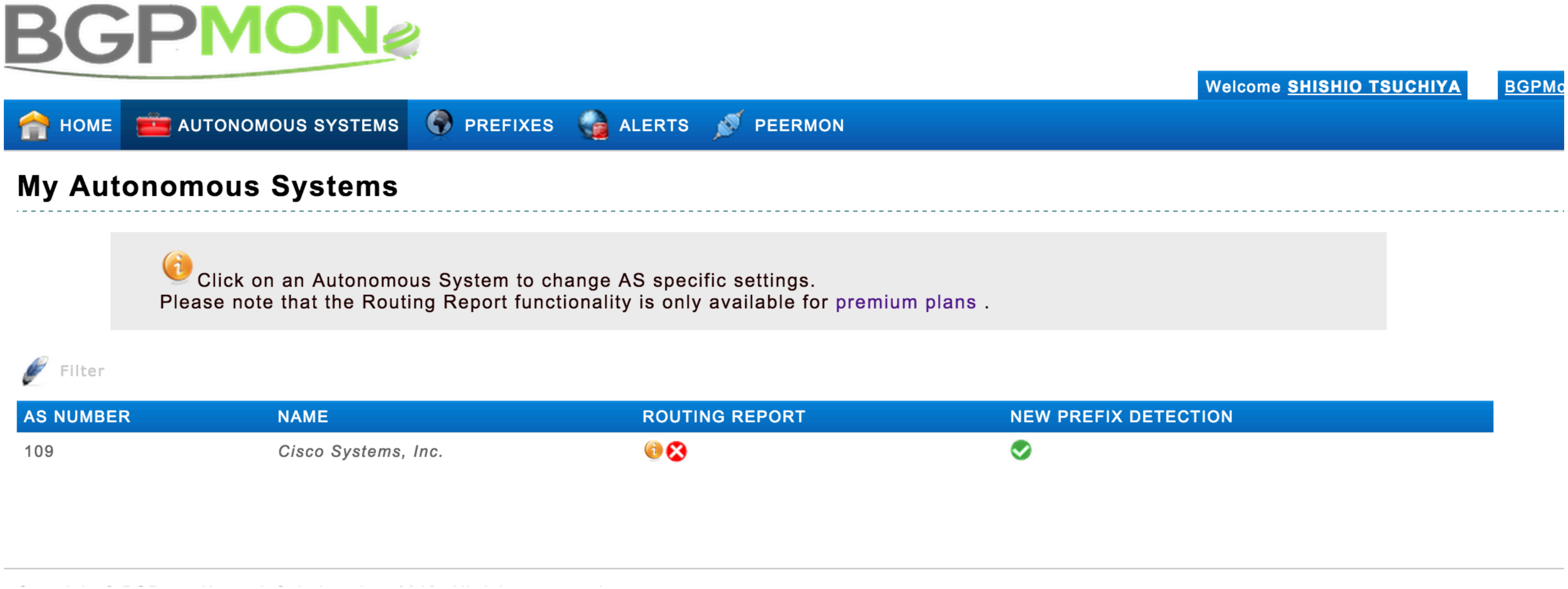
BGPMon Joins OpenDNS
Dear BGPmon.net user, I'm excited to announce that BGPmon has been acquired by OpenDNS. OpenDNS is a leading cloud-delivered network security company known for engineering predictive intelligence technology that stops malicious activity before it can threaten a network. Over the last few years BGPmon has grown from a community service into a successful business that […]

What caused the Google service interruption?
This morning people on twitter reported that they were unable to reach Google services. Businessinsider followed up with a story in which they mentioned that the Google service interruption primarily involved European and Indian users. In this blog we'll take a quick look at what exactly happened by looking at our BGP data. The first […]

BGP routing incidents in 2014, malicious or not?
Over the last year we have seen and written about numerous BGP routing incidents that looked out of the ordinary, straight-up suspicious or were just configuration mistakes. In this blog post we will highlight a few of them and look at the impact and cause of

https://portal.bgpmon.net/index.php

AS番号登録



My Autonomous Systems

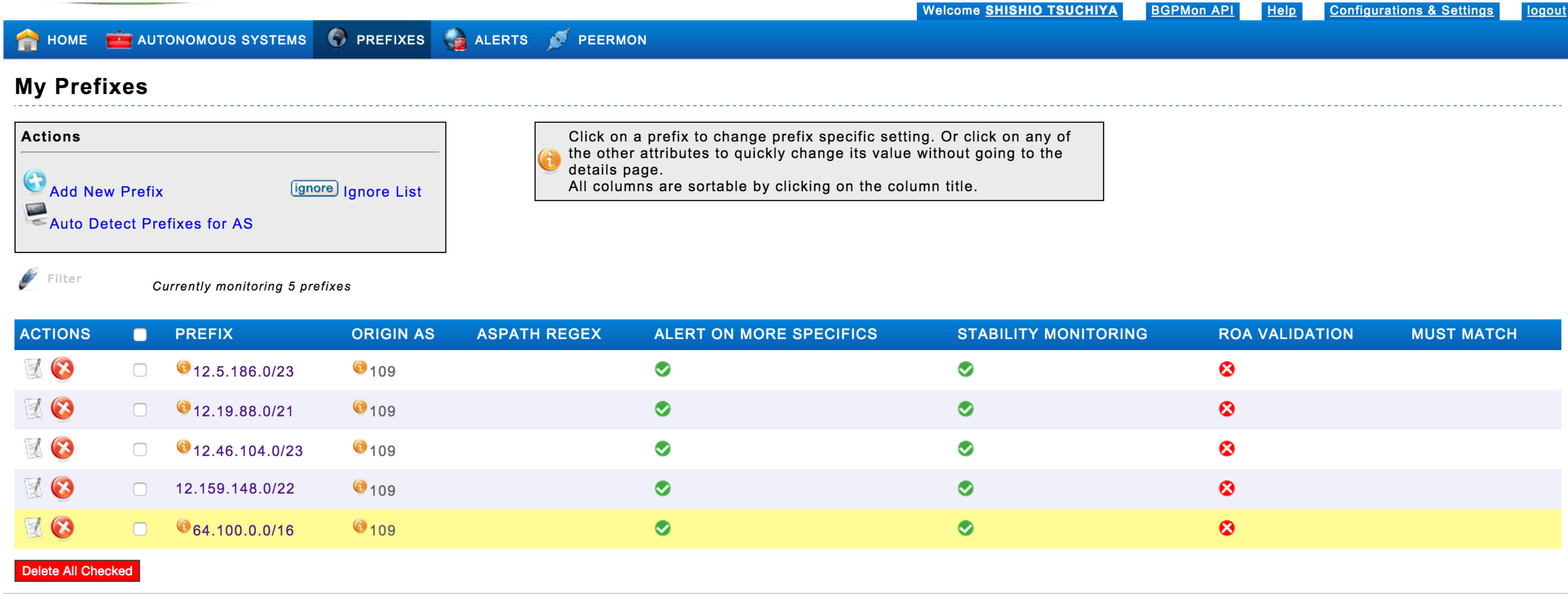
Click on an Autonomous System to change AS specific settings.
Please note that the Routing Report functionality is only available for premium plans .

Filter

AS NUMBER	NAME	ROUTING REPORT	NEW PREFIX DETECTION
109	*Cisco Systems, Inc.*	ⓘ ✗	✓

https://portal.bgpmon.net/myasn.php

Prefix登録



My Prefixes

Actions

Add New Prefix

ignore Ignore List

Auto Detect Prefixes for AS

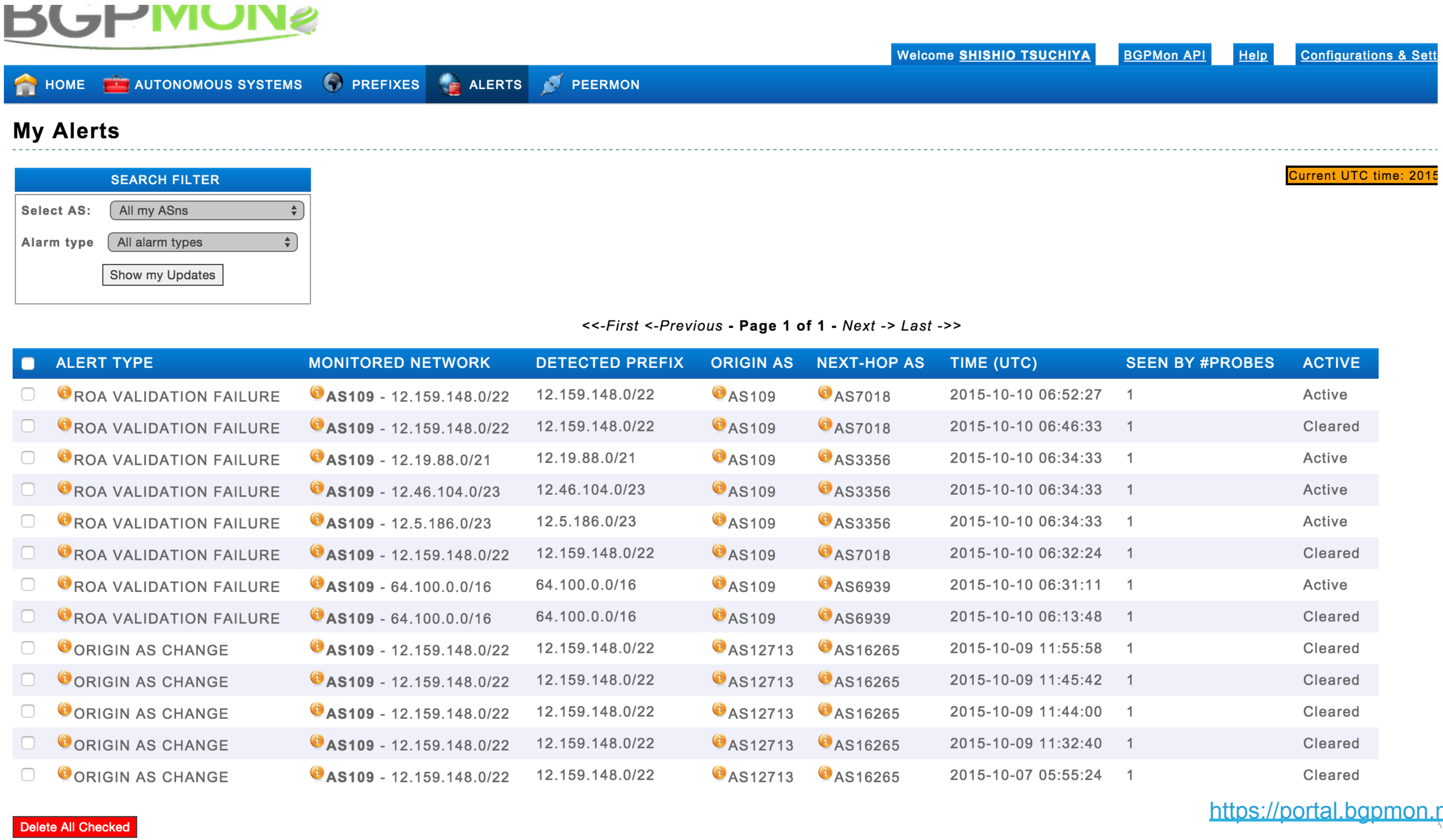
Click on a prefix to change prefix specific setting. Or click on any of the other attributes to quickly change its value without going to the details page.
All columns are sortable by clicking on the column title.

Currently monitoring 5 prefixes

ACTIONS	☐	PREFIX	ORIGIN AS	ASPATH REGEX	ALERT ON MORE SPECIFICS	STABILITY MONITORING	ROA VALIDATION	MUST MATCH
	☐	12.5.186.0/23	109		✓	✓	✗	
	☐	12.19.88.0/21	109		✓	✓	✗	
	☐	12.46.104.0/23	109		✓	✓	✗	
	☐	12.159.148.0/22	109		✓	✓	✗	
	☐	64.100.0.0/16	109		✓	✓	✗	

https://portal.bgpmon.net/myprefixes.php

アラート登録



My Alerts

Select AS: All my ASns

Alarm type: All alarm types

Show my Updates

<<-First <-Previous - **Page 1 of 1** - *Next -> Last ->>*

□	ALERT TYPE	MONITORED NETWORK	DETECTED PREFIX	ORIGIN AS	NEXT-HOP AS	TIME (UTC)	SEEN BY #PROBES	ACTIVE
□	ROA VALIDATION FAILURE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS109	AS7018	2015-10-10 06:52:27	1	Active
□	ROA VALIDATION FAILURE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS109	AS7018	2015-10-10 06:46:33	1	Cleared
□	ROA VALIDATION FAILURE	**AS109** - 12.19.88.0/21	12.19.88.0/21	AS109	AS3356	2015-10-10 06:34:33	1	Active
□	ROA VALIDATION FAILURE	**AS109** - 12.46.104.0/23	12.46.104.0/23	AS109	AS3356	2015-10-10 06:34:33	1	Active
□	ROA VALIDATION FAILURE	**AS109** - 12.5.186.0/23	12.5.186.0/23	AS109	AS3356	2015-10-10 06:34:33	1	Active
□	ROA VALIDATION FAILURE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS109	AS7018	2015-10-10 06:32:24	1	Cleared
□	ROA VALIDATION FAILURE	**AS109** - 64.100.0.0/16	64.100.0.0/16	AS109	AS6939	2015-10-10 06:31:11	1	Active
□	ROA VALIDATION FAILURE	**AS109** - 64.100.0.0/16	64.100.0.0/16	AS109	AS6939	2015-10-10 06:13:48	1	Cleared
□	ORIGIN AS CHANGE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS12713	AS16265	2015-10-09 11:55:58	1	Cleared
□	ORIGIN AS CHANGE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS12713	AS16265	2015-10-09 11:45:42	1	Cleared
□	ORIGIN AS CHANGE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS12713	AS16265	2015-10-09 11:44:00	1	Cleared
□	ORIGIN AS CHANGE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS12713	AS16265	2015-10-09 11:32:40	1	Cleared
□	ORIGIN AS CHANGE	**AS109** - 12.159.148.0/22	12.159.148.0/22	AS12713	AS16265	2015-10-07 05:55:24	1	Cleared

Delete All Checked

https://portal.bgpmon.net/myalerts.php

アラート一覧

- Code 9: RPKI ROA validation failure or warning
- Code 10: Origin AS and Prefix changed (more specific) Or Origin AS changed.
- Code 11: Origin AS and Prefix changed (more specific) Or Origin AS changed.
- Code 21: Possible MITM BGP attack
- Code 22: More specific detected
- Code 31: upstream AS changed.
- Code 41: ASpath Regex didn’t match
- Code 60: New prefix detected for your AS
- Code 97: Withdraw of one of your prefixes (only if you enabled this)

フリーサービス

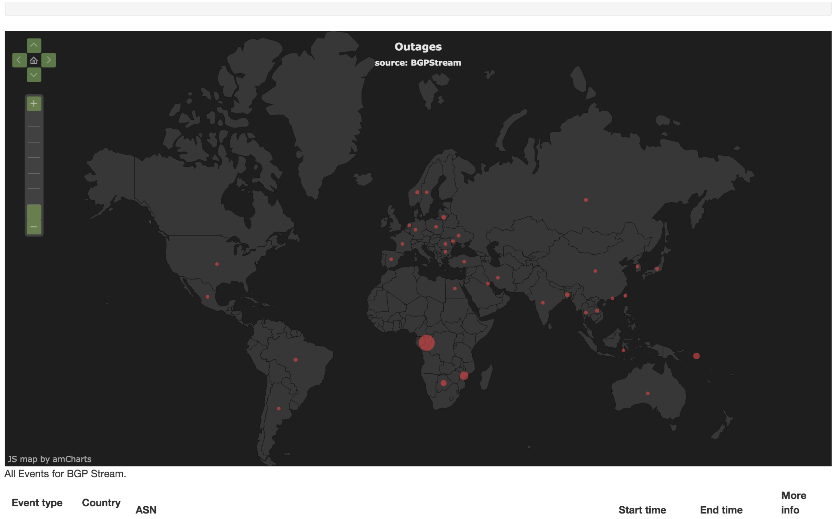
- 5 Prefixまでは無料
- プレミアムサービスは
  - 5以上のPrefix
  - フルアラート詳細へのアクセス
  - BGPmon APIへのアクセス
  - ディリールーティングレポート
  - アラートメッセージを送るメールアドレスの追加
  - Pagerへの送信（160文字以内）

まとめ

- bgpmon.netに登録してみた
- 5prefixまでならただで、ネットワーク管理者である必要はない
- フリーユーザであっても、連絡はしっかり来る

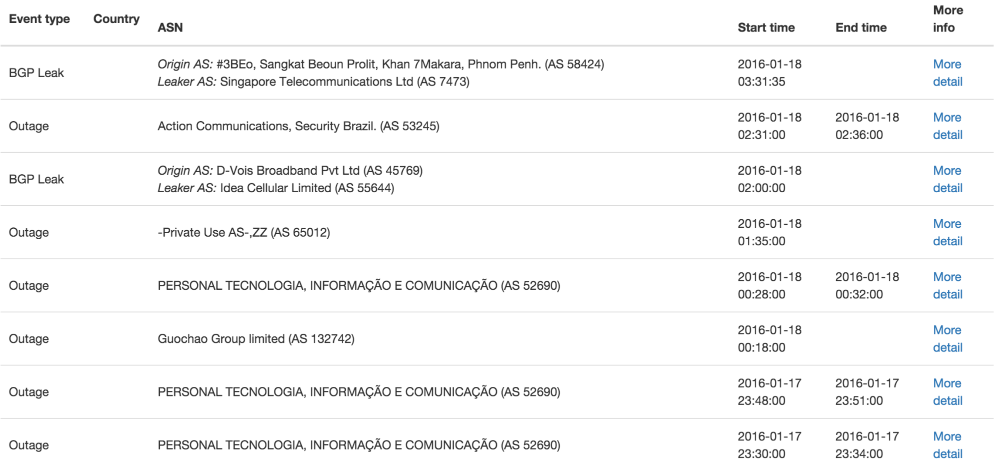
BGP Stream

https://bgpstream.com/



All Events for BGP Stream.

Event type	Country	ASN	Start time	End time	More info



Event type	Country	ASN	Start time	End time	More info
BGP Leak		*Origin AS:* #3BEo, Sangkat Beoun Prolit, Khan 7Makara, Phnom Penh. (AS 58424) *Leaker AS:* Singapore Telecommunications Ltd (AS 7473)	2016-01-18 03:31:35		More detail
Outage		Action Communications, Security Brazil. (AS 53245)	2016-01-18 02:31:00	2016-01-18 02:36:00	More detail
BGP Leak		*Origin AS:* D-Vois Broadband Pvt Ltd (AS 45769) *Leaker AS:* Idea Cellular Limited (AS 55644)	2016-01-18 02:00:00		More detail
Outage		-Private Use AS-,ZZ (AS 65012)	2016-01-18 01:35:00		More detail
Outage		PERSONAL TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO (AS 52690)	2016-01-18 00:28:00	2016-01-18 00:32:00	More detail
Outage		Guochao Group limited (AS 132742)	2016-01-18 00:18:00		More detail
Outage		PERSONAL TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO (AS 52690)	2016-01-17 23:48:00	2016-01-17 23:51:00	More detail
Outage		PERSONAL TECNOLOGIA, INFORMAÇÃO E COMUNICAÇÃO (AS 52690)	2016-01-17 23:30:00	2016-01-17 23:34:00	More detail

- より可視的に世界各国のイベントを見る事が出来る
- イベント通知は@bgpstreamでも実施

cisco *TOMORROW starts here.*