Mongolian internet health overview by Mejiro, a risk visualization tool

October 4th, 2018

JPCERT/CC
Global Coordination Division
Cyber Metrics Line

Information security analyst
Katsuhiro Mori

Agenda

- Background
- Internet risk visualization service
- Mongolia case
- Cleanup activity
- Conclusion

Background

About CyberGreen project - concept

- CyberGreen is…
  The idea of The CyberGreen Project is to improve the healthiness of the Internet via the Green Index and the best current practices.

- it shall;

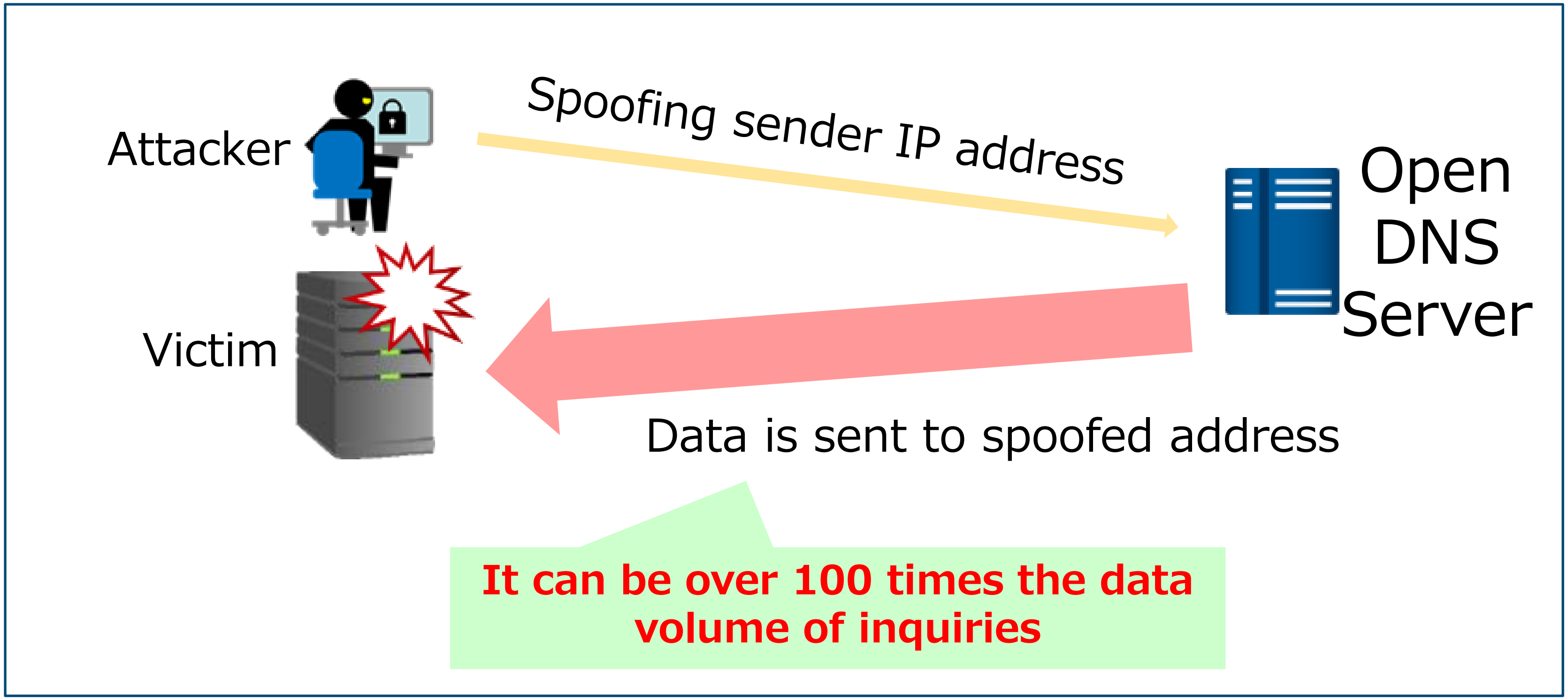
- collect measurement data on the Internet,
- calculate the Green Index using the data in quotative and reproducible method,
- comparably visualize the healthiness of the Internet,
- encourage national CSIRTs to mitigate using the best current practices,
- and thus, aim to improve the healthiness of the Internet.

Cyber Green Project
https://www.jpcert.or.jp/research/cybergreen.html

About DDoS

The example of Reflection Attacks and Amplification Attacks 【DNS amp.】

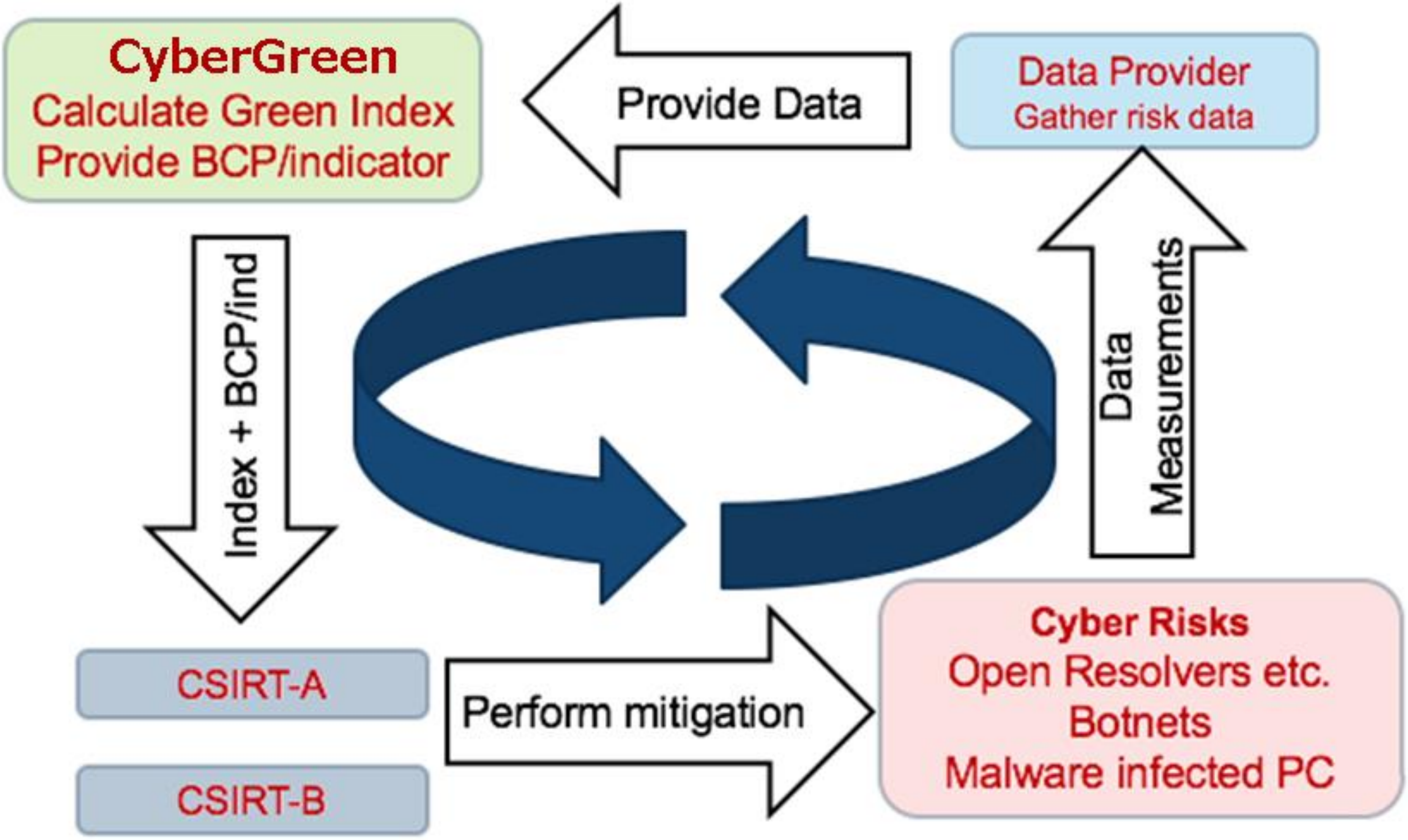
This attack abuses to amplify sending data using query for OpenDNS server and cache.



It can be over 100 times the data volume of inquiries

About CyberGreen project – purpose

- The purpose of this project



Providing for index

■ Assigned IP address count and risk node count

- Do we define the healthiness of the Internet to use only risk node count?

- Do we need to take into consideration for comparing with each country’s the healthiness of the Internet for IP address node count?

⇒Which is better cyber condition? Both countries have same risk IP node count, however one country has hundreds of millions of IP address count, another has several tens of thousands.

■ Therefore…

We are trying to compare in same situation with countries which is assigned a few IP addresses country and assigned many IP addresses country . ⇒ Let's create index by ourselves!

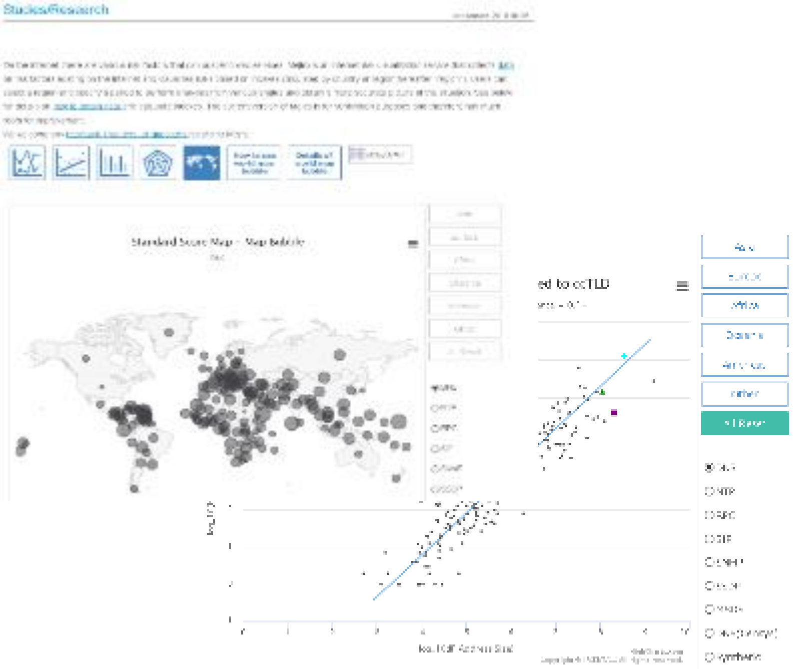
Internet risk visualization service

Internet risk visualization service -Mejiro

JPCERT/CC released Mejiro English version

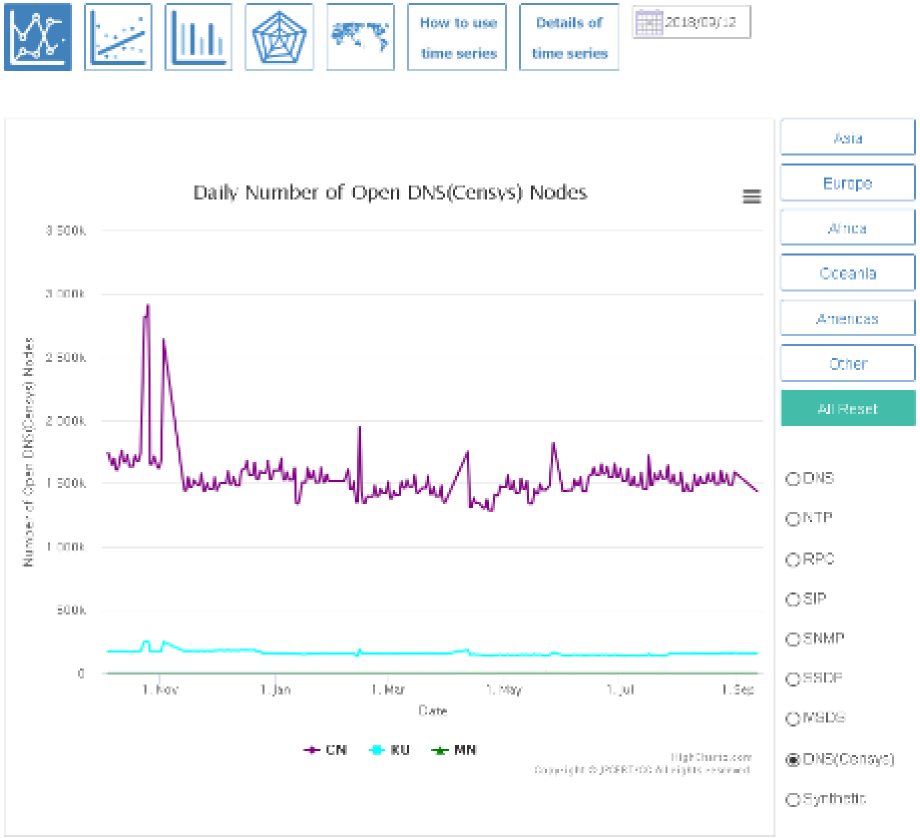
Mejiro is an Internet risk visualization service that collects data on risk factors existing on the Internet and visualizes risks based on indexes calculated by country or region. Mejiro creates objective risk indexes that can be compared and analyzes the information from various angles. **https://www.jpcert.or.jp/english/pub/sr/mejiro/mejiro.html**

Mejiro



Time series

Number of IP addresses and number of risk nodes by time series.



As of 12th September 2018

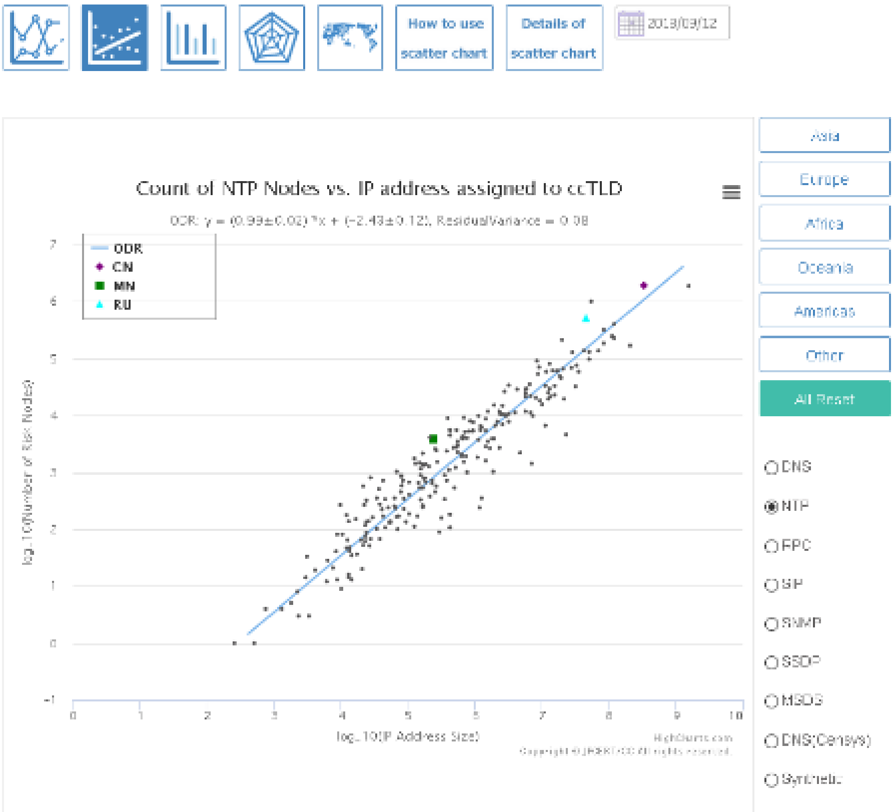
Protocol	Keyword	Recode count
DNS	Recursion: enabled	5M
NTP	NTP stratum:	10M
RPC	Port:111 portmap	2.3M
SIP	SIP/ /UDP	20M
SNMPv2	Port:161	3.4M
SSDP	upnp location:	4M
IP address	-	3,657M

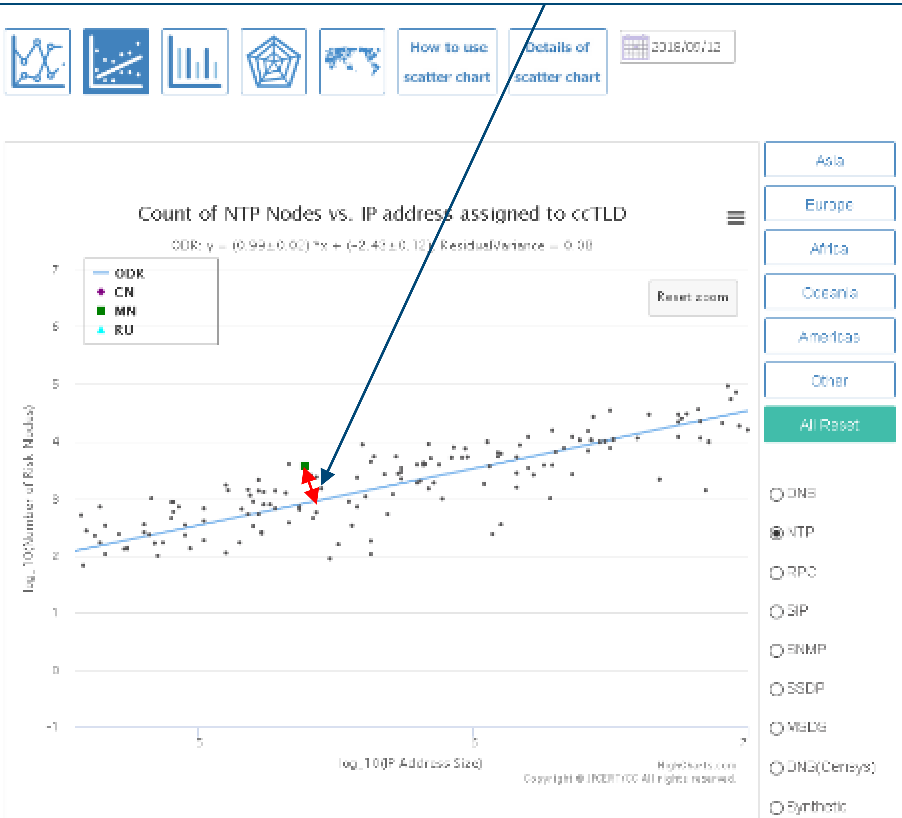
Scatter plot

Scatter plot of each country IP address count and each risk node count.

⇒ We tried to create index from the distance between the regression line and the data point.

The distance between the regression line and the data point





As of 12th September 2018

Indexing

- The distance between the regression line and the data point is;

$$d(cc2) = \frac{\left(ax_{cc_2} - b\right) - y_{cc_2}}{\sqrt{(-a)^2 + 1}}$$

- Then the mean of the d(cc2) , or μ is;

$$\boldsymbol{\mu} = \frac{1}{n}\sum^{n} d(cc2)$$

- And the standard deviation σ is;

$$\boldsymbol{\sigma} = \sqrt{\frac{1}{n}\sum^{n}\left(d(cc2) - \boldsymbol{\mu}\right)^{2}}$$

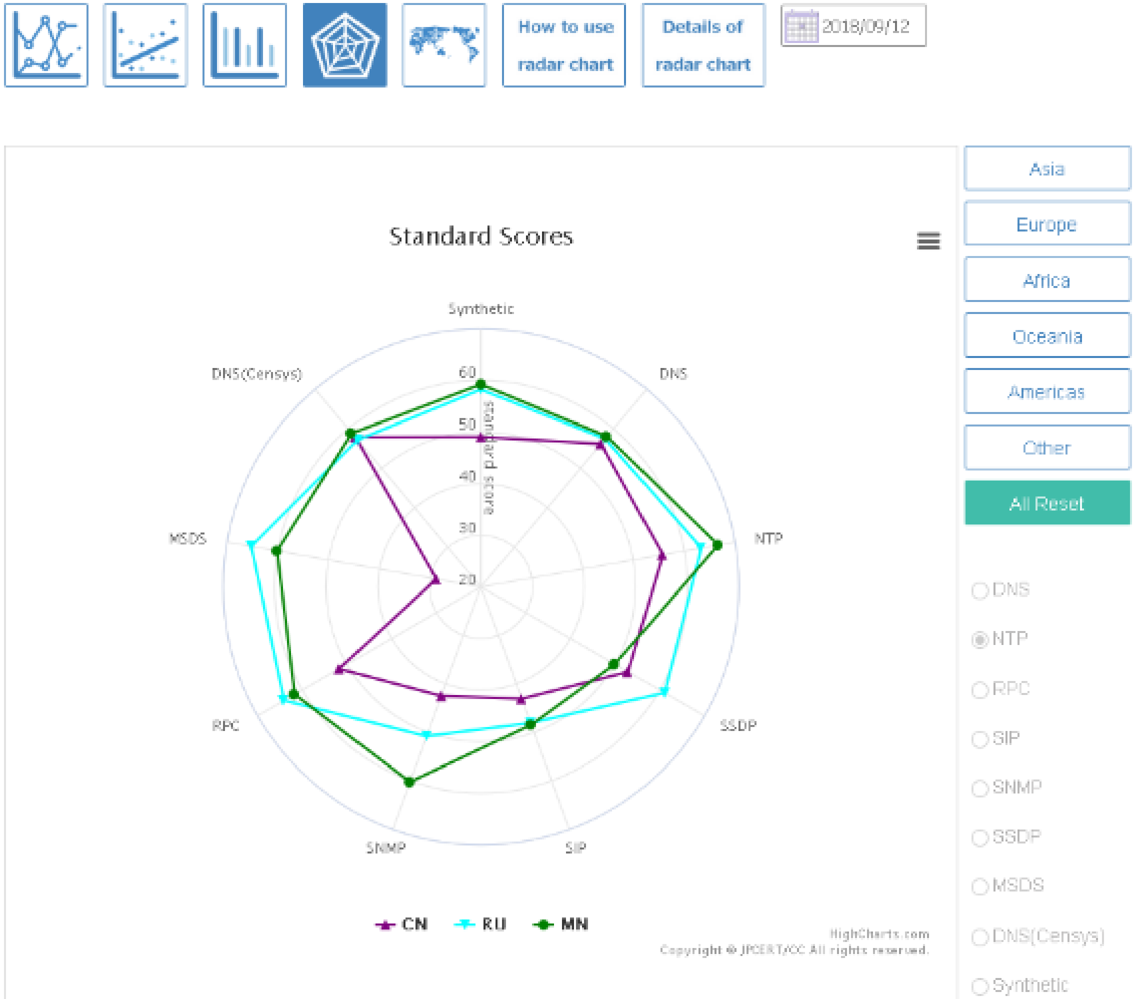
- Then we defined the standard score κ(cc2) as;

Index

$$\kappa(cc2) = \frac{d(cc2) - \boldsymbol{\mu}}{\boldsymbol{\sigma}} \times 10 + 50$$

Comparing with other countries

By comparing with the countries of the world weak places of our country will be brought out!

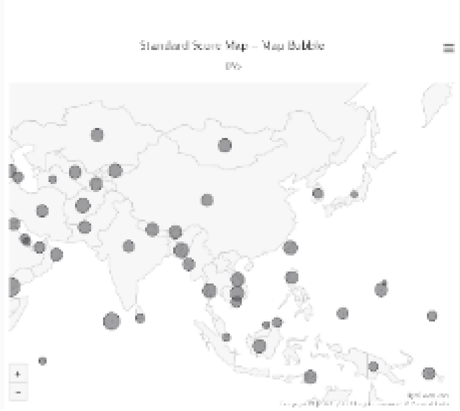


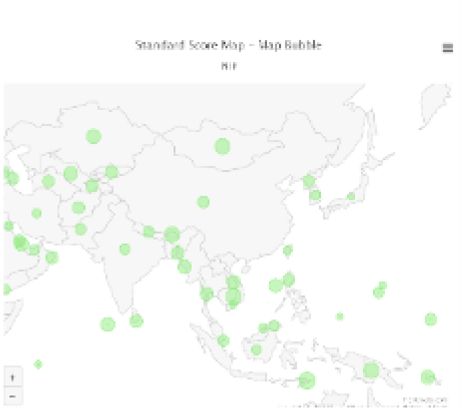
○ DNS
● NTP
○ RPC
○ SIP
○ SNMP
○ SSDP
○ MSDS
○ DNS(Censys)
○ Synthetic

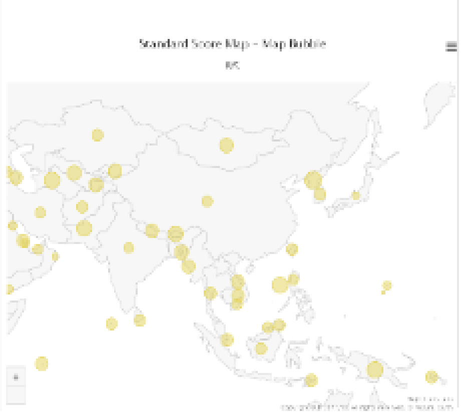
As of 12th September 2018

Visualization of risks by world map

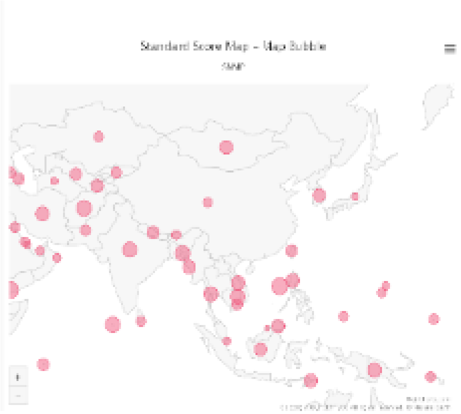
In order to effectively clean up activities, it is necessary to display each risk on the world map and think about which country to promote which risk cleanup activity.

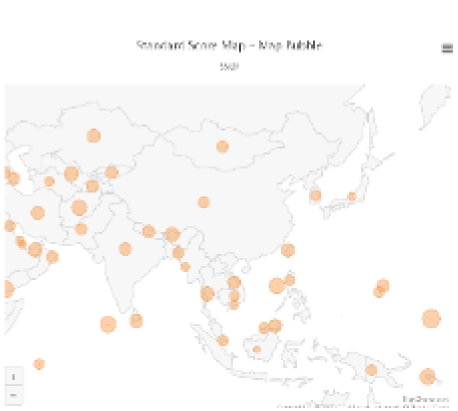


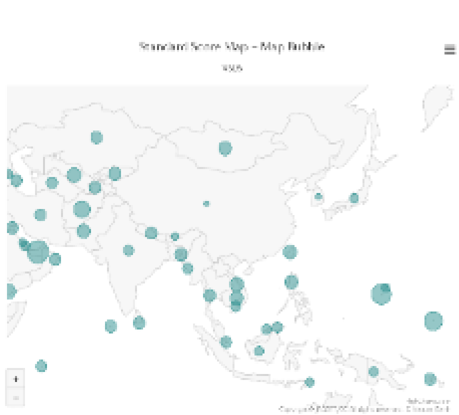




Standard Score Map – Map Bubble





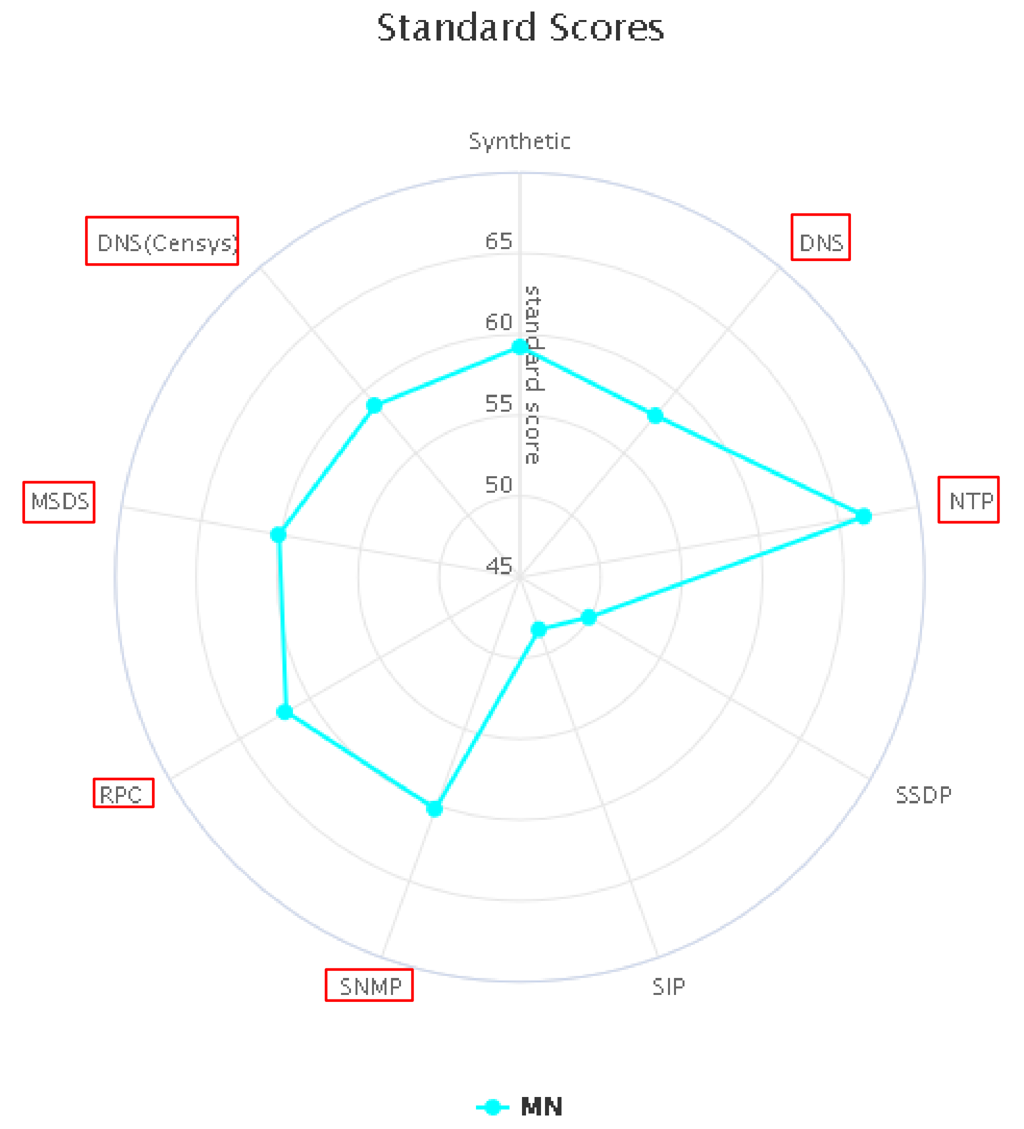


Standard Score Map – Map Bubble

As of 12th September 2018

Mongolia case

Mongolia Case



As of 12th September 2018

Mongolia Case

DNS

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS9484	Mobinet ISP, MobiCom Corporation	17408	403	66
AS58598	Comtel Ltd	2048	24	63.36
AS55805	MobiCom Corporation, Mongolia	3328	22	60.86
AS56293	Kewiko LLC	2048	11	58.84
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	83	54.13
AS38805	STXCitinet, Leading Internet & VOIP Service Provider, Ulaanbaatar, Mongolia STXCitinet LLC, Ulaanbaatar Mongolia	32768	79	53.79
AS56301	National Data Center building Tolgoit	1280	3	52.76
AS58439	ICNC LLC	5120	11	51.98
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator Ulaanbaatar, Mongolia	11264	22	51.6
AS63962	iTools JSC	2048	3	51.31

As of 12th September 2018

Mongolia Case

NTP

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS9484	Mobinet ISP, MobiCom Corporation	17408	1725	67.77
AS55408	MCS	512	23	66.9
AS58598	Comtel Ltd	2048	84	66.31
AS58439	ICNC LLC	5120	260	64.77
AS55805	MobiCom Corporation, Mongolia	3328	93	64.51
AS9934	Mongolia Telecom	9216	474	64.21
AS56301	National Data Center building Tolgoit	1280	41	63.79
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	299	60.29
AS133177	Wicom Networks LLC	2048	18	57.13
AS63962	iTools JSC	2048	16	56.43

As of 12th September 2018

Mongolia Case

SSDP

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS38805	STXCitinet, Leading Internet & VOIP Service Provider, Ulaanbaatar, Mongolia STXCitinet LLC, Ulaanbaatar Mongolia	32768	46	54.61
AS56293	Kewiko LLC	2048	2	54.06
AS55805	MobiCom Corporation, Mongolia	3328	1	48.56
AS9484	Mobinet ISP, MobiCom Corporation	17408	4	44.58
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	6	44.09
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	1	39.73

As of 12th September 2018

Mongolia Case

SIP

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS55408	MCS	512	2	59.79
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	17	53.82
AS9484	Mobinet ISP, MobiCom Corporation	17408	20	52.28
AS56301	National Data Center building Tolgoit	1280	1	50.3
AS58598	Comtel Ltd	2048	1	48.83
AS63962	iTools JSC	2048	1	48.83
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	12	46.59
AS9934	Mongolia Telecom	9216	3	44.78
AS58439	ICNC LLC	5120	1	41.9
AS38805	STXCitinet, Leading Internet & VOIP Service Provider, Ulaanbaatar, Mongolia STXCitinet LLC, Ulaanbaatar Mongolia	32768	4	40.19

As of 12th September 2018

Mongolia Case

SNMP

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS9484	Mobinet ISP, MobiCom Corporation	17408	462	67.52
AS58439	ICNC LLC	5120	36	59.35
AS55805	MobiCom Corporation, Mongolia	3328	13	58.18
AS45237	Bodicom ISP Ulaanbaatar	4864	20	55.37
AS9934	Mongolia Telecom	9216	27	54.32
AS56293	Kewiko LLC	2048	4	53.26
AS63962	iTools JSC	2048	3	51.58
AS38818	YOKOZUNANET LLC	41472	17	51.48
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	17	50.67
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	35	49.83

As of 12th September 2018

Mongolia Case

RPC

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS63962	iTools JSC	2048	33	67.05
AS56301	National Data Center building Tolgoit	1280	11	61.98
AS55408	MCS	512	1	53.09
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	14	51.24
AS9484	Mobinet ISP, MobiCom Corporation	17408	20	50.98
AS133177	Wicom Networks LLC	2048	2	50.58
AS58598	Comtel Ltd	2048	1	46.51
AS9934	Mongolia Telecom	9216	4	44.81
AS55805	MobiCom Corporation, Mongolia	3328	1	44.6
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	10	44.31

As of 12th September 2018

Mongolia Case

MSDS

ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS63962	iTools JSC	2048	31	68.66
AS56301	National Data Center building Tolgoit	1280	14	65.06
AS58598	Comtel Ltd	2048	8	59.83
AS9484	Mobinet ISP, MobiCom Corporation	17408	64	58.45
AS38805	STXCitinet, Leading Internet & VOIP Service Provider, Ulaanbaatar, Mongolia STXCitinet LLC, Ulaanbaatar Mongolia	32768	98	58.22
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	79	56.87
AS133177	Wicom Networks LLC	2048	5	56.76
AS55805	MobiCom Corporation, Mongolia	3328	4	53.14
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	11	49.64
AS45237	Bodicom ISP Ulaanbaatar	4864	5	48.67

As of 12th September 2018

Mongolia Case

DNS(Censys)

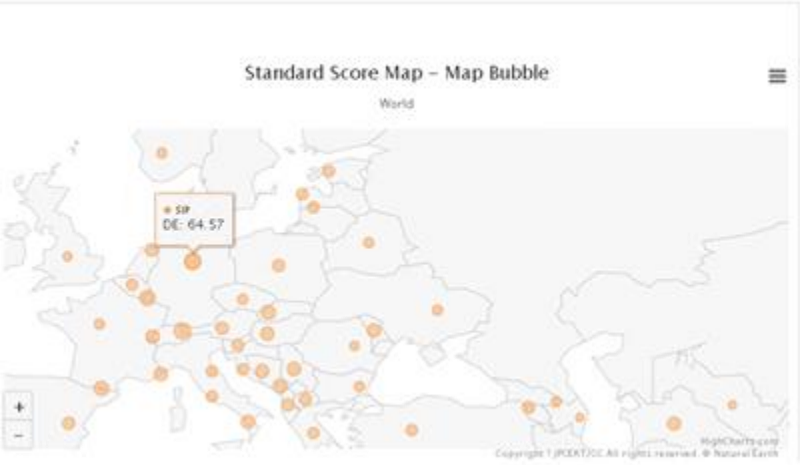
ASN	AS Name	ALL IP Count	Risk node	Mejiro Index
AS9484	Mobinet ISP, MobiCom Corporation	17408	346	67.03
AS58598	Comtel Ltd	2048	30	66.03
AS55805	MobiCom Corporation, Mongolia	3328	28	63.42
AS56293	Kewiko LLC	2048	10	58.91
AS56301	National Data Center building Tolgoit	1280	6	57.17
AS17882	ASN-MCS-AP # AS-MCS-AP converted to ASN-MCS-AP for RPSL compliance	31488	118	57.12
AS58439	ICNC LLC	5120	16	54.53
AS63962	iTools JSC	2048	5	54.42
AS9934	Mongolia Telecom	9216	24	53.45
AS10219	SKYMEDIA CORPORATION LLC ISP, Triple Play Service and VoIP operator, Ulaanbaatar, Mongolia	11264	24	52.4

As of 12th September 2018

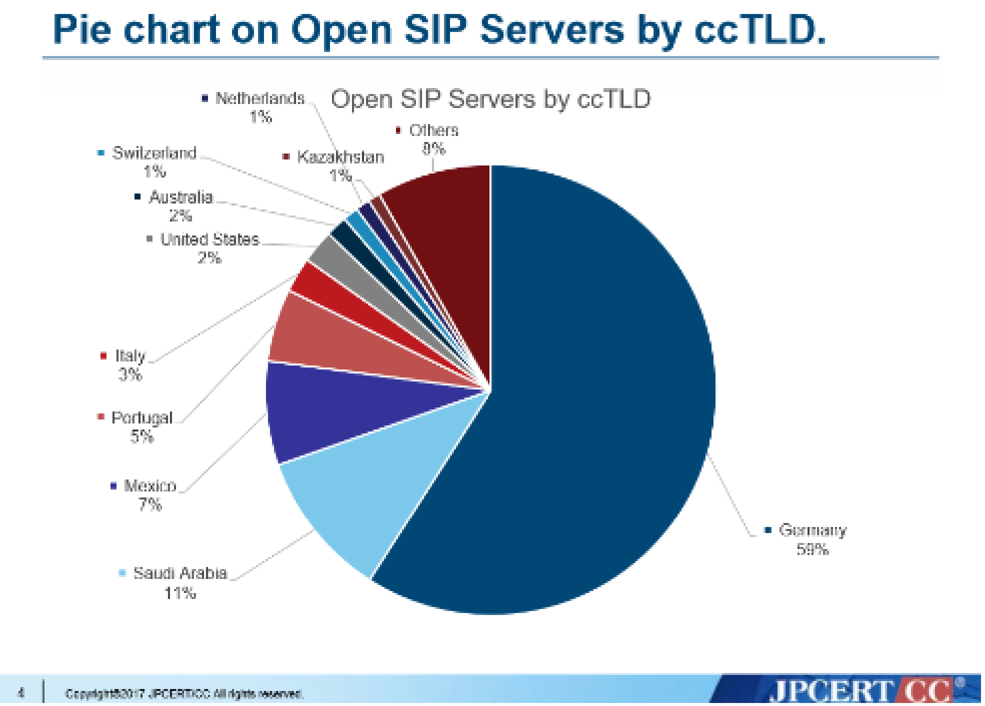
Cleanup activity

Cleanup activity for overseas(1)

In Germany, the OpenSIP terminal has about 6,000,000 IP addresses, and there is a possibility that it will be used for DDoS attacks in the future



Because the SIP index is high as 64.57
In spite of lower index without SIP, high overall result of 62.98



Pie chart on Open SIP Servers by ccTLD.

4 | Copyright©2017 JPCERT/CC All rights reserved. JPCERT CC

Request for OpenSIP to Germany (CERT-Bund)
(Excerpt of some materials)

Cleanup activity for overseas(2)

Cooperation of the government, CSIRT and ISP of each country is indispensable for overseas cleanup activities

- Request for overseas ISP stakeholders
- Implementation of relationship building activities

Lecture to overseas ISP officials (Fiji)

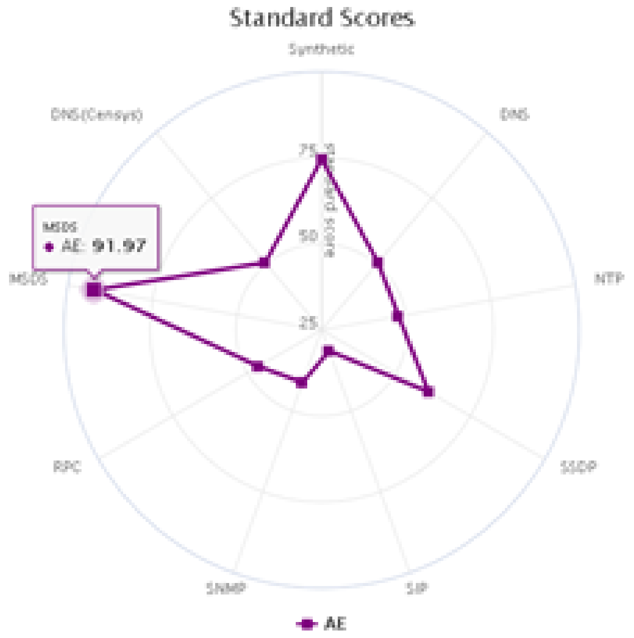
Cleanup activity for overseas(3)

Collaborate with TSUBAME

In United Arab Emirates, many devices use SMB protocol and are opened through the internet from SHODAN data.

Some packets are coming from UAE toward port 445 using TSUBAME(*) data.

*TSUBAME (Internet threat monitoring system)
https://www.jpcert.or.jp/english/tsubame/



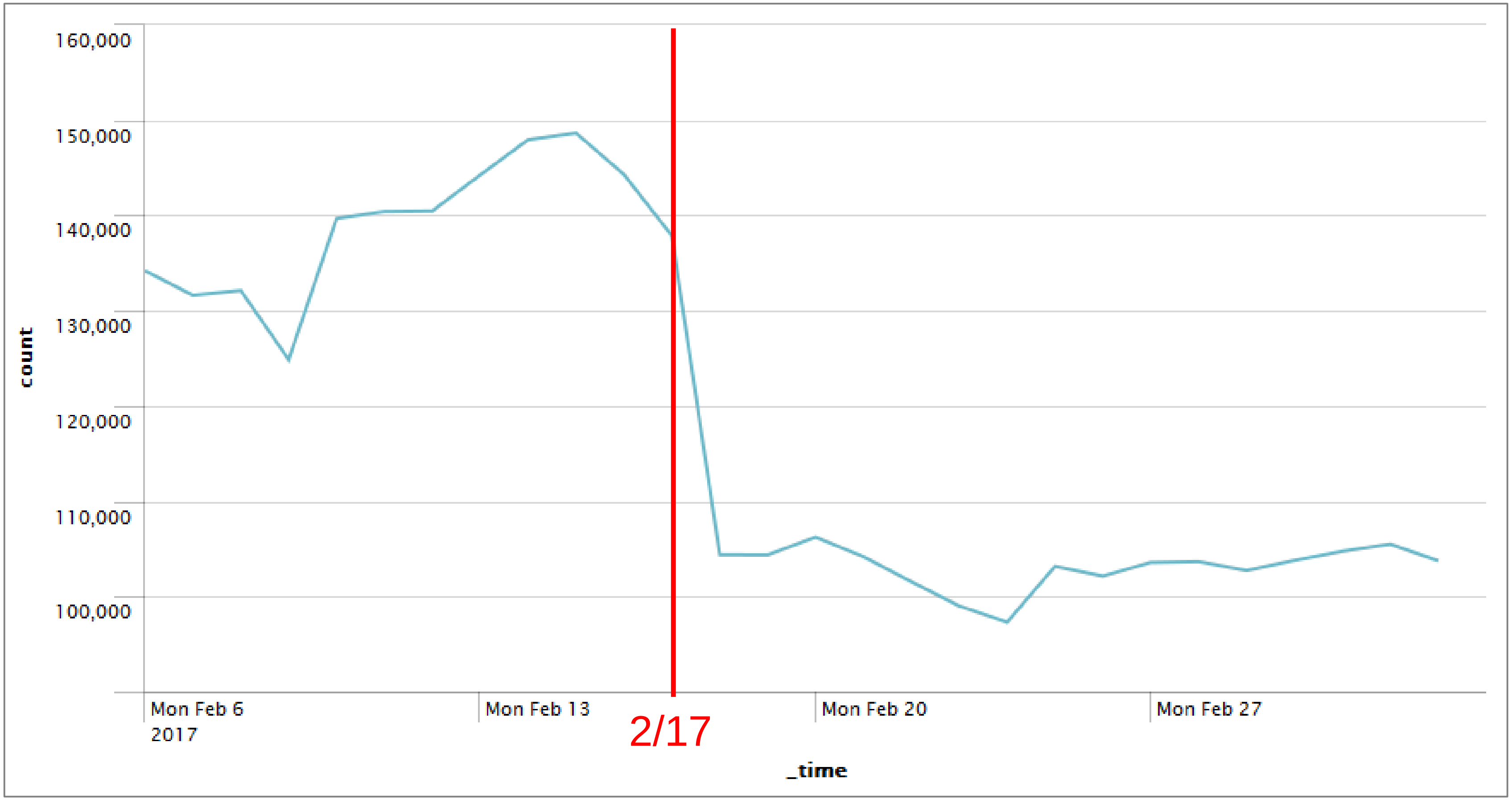
ccTLD	IP count(A)	Scan packet count(B)	Ratio(B/A)	Mejiro Index
AE	4,002,214	269	0.00672%	91.97
MN	242,176	177	0.07308%	60.18
JP	207,177,801	781	0.00038%	45.41

TSUBAME(16th Aug. 2017-17th Sep. 2018)
Mejiro(17th. Sep. 2018)

Cleanup activity for domestic(1)

Significant decrease in terminal of OpenNTP due to ISP interaction

Due to domestic ISP encouragement, about 30 thousand reductions were made from February 17th to 18th 2017.

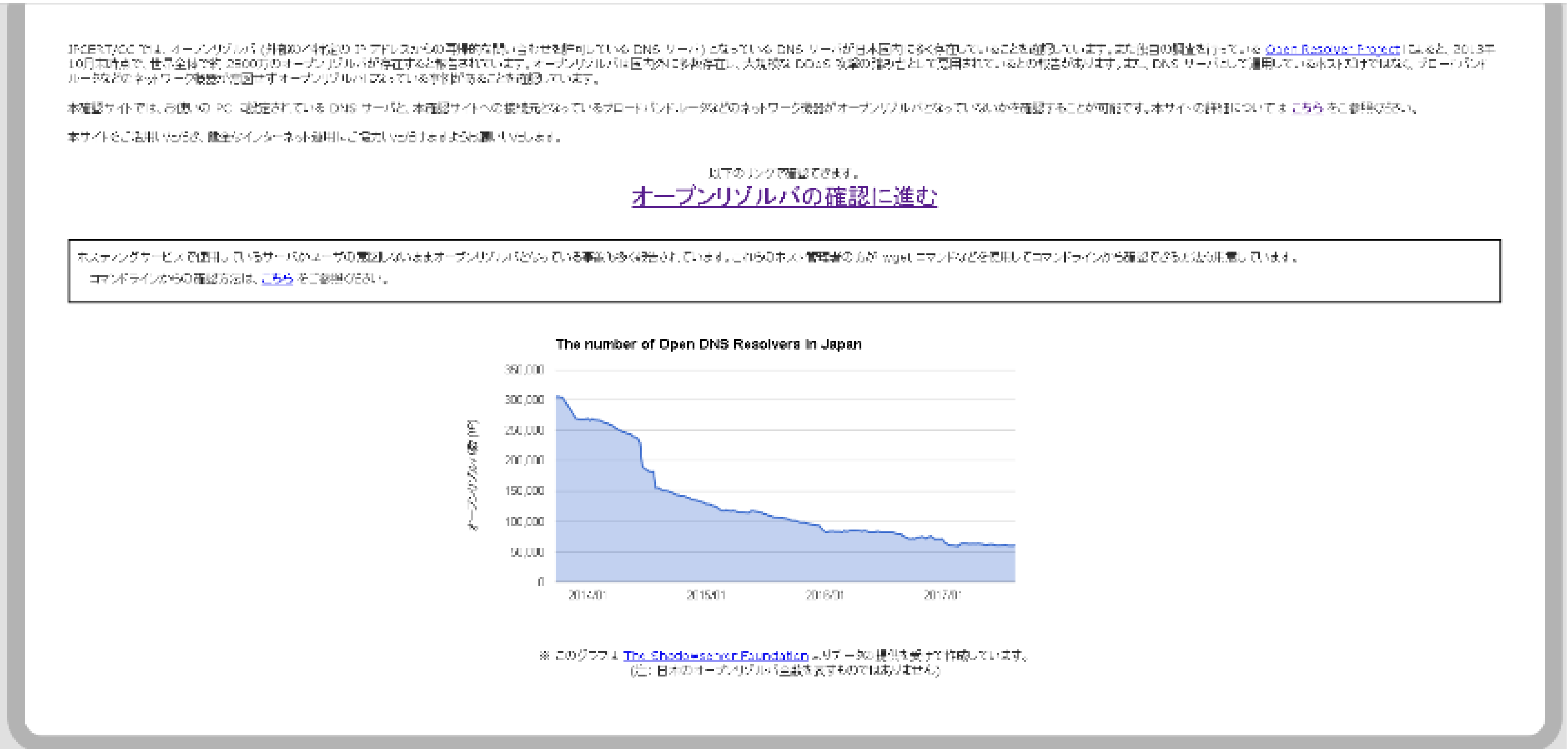


2/17

Cleanup activity for domestic(2)

Open Resolver check site

The open resolver check site operated by JPCERT / CC can be used not only by companies but also by individuals



JPCERT/CCでは、オープンリゾルバ（外部の不特定のIPアドレスからの再帰的な問い合わせを許可しているDNSサーバ）となっているDNSサーバが日本国内に多く存在していることを確認しています。また独自の調査を行っているOpen Resolver Projectによると、2013年10月末時点で、世界全体で約2500万のオープンリゾルバが存在すると報告されています。オープンリゾルバは国内外に多数存在し、大規模なDDoS攻撃の踏み台として悪用されているとの報告があります。また、DNSサーバとして運用しているホストだけではなく、ブロードバンドルーターなどのネットワーク機器が意図せずオープンリゾルバになっている事例があることも確認しています。

本確認サイトでは、お使いのPCに設定されているDNSサーバと、本確認サイトへの接続元となっているブロードバンドルータなどのネットワーク機器がオープンリゾルバとなっていないかを確認することが可能です。本サイトの詳細については こちら をご参照ください。

本サイトをご利用いただき、健全なインターネット運用にご協力いただけますようお願いいたします。

以下のリンクで確認できます。

オープンリゾルバの確認に進む

ホスティングサービスで使用しているサーバやユーザの意図しないままオープンリゾルバとなっている事例も多く発生しています。これらのホスト管理者の方がwgetコマンドなどを使用してコマンドラインから確認できるように用意しています。
コマンドラインからの確認方法は、こちら をご参照ください。

※ このグラフは The Shadowserver Foundation よりデータの提供を受けて作成しています。
(注: 日本のオープンリゾルバ全数を表すものではありません)

open resolver check site
http://www.openresolver.jp/

What’s benefit for …

It is essential for cooperation with ISP, hosting company, having ASN company or organization or etc.. This clean up activity is beneficial for their business as well.

■ ISP

- Network line speed up
- ISP's image enhancement(reputation)

■ Hosting company

- Network line speed up
- Hosting company's image enhancement(reputation)
- Hinder customer from be an accomplice in a crime

■ Having ASN company or Organization

- Network line speed up
- Correct settings
- Not be an accomplice in a crime

ALL user can effectively use network, memory and CPU resources for original purpose.

Conclusion

Cleanup activity

Internet space is dirty as well as the earth

Our strengths

Mejiro

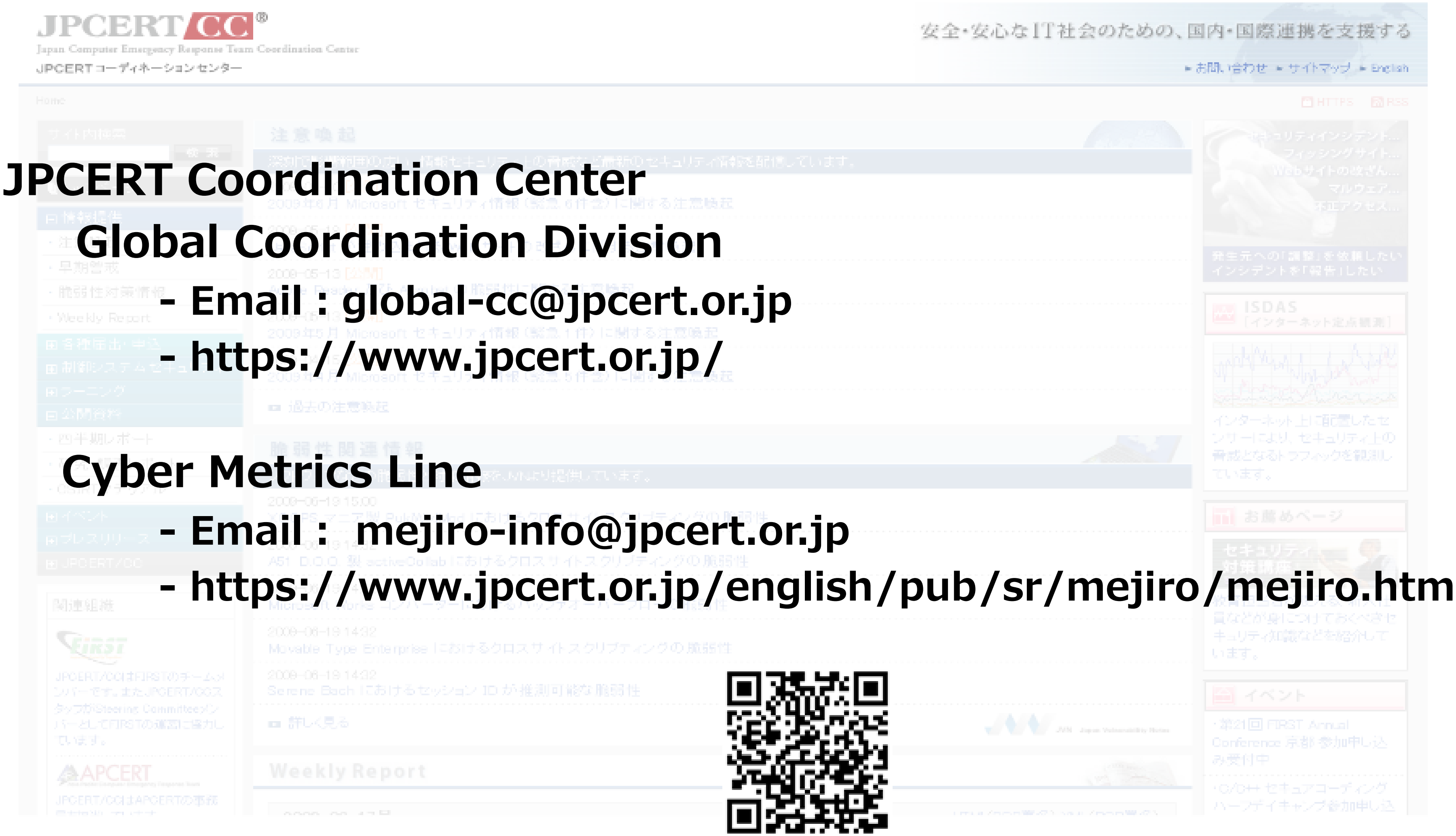
Tools

Cooperation

Conclusion

Our goal

Thank you very much for your kind cooperation as always.



JPCERT/CC®
Japan Computer Emergency Response Team Coordination Center
JPCERTコーディネーションセンター

安全･安心なIT社会のための、国内･国際連携を支援する

▸お問い合わせ ▸サイトマップ ▸English

JPCERT Coordination Center

Global Coordination Division

- **Email : global-cc@jpcert.or.jp**
- **https://www.jpcert.or.jp/**

Cyber Metrics Line

- **Email : mejiro-info@jpcert.or.jp**
- **https://www.jpcert.or.jp/english/pub/sr/mejiro/mejiro.html**