Deployment of TLD Anycast node to ISPs for stability and resiliency

APRICOT 2021

Takayasu Matsuura (JPRS)

Nagisa Yano (OPTAGE)

Agenda

- “.jprs” R&D Platform and Joint Research 2017
- Background of Joint Research 2021
- Overview of Joint Research
- Joint Research Report by ISPs
- Consideration of LN deployment in Japan

“.jprs” R&D Platform and Joint Research 2017

■ Concept of “.jprs”

In order for the Internet to keep growing, as a registry operator, we will need an environment in which to create innovations …

.jprs TLD can provide experimental environment for domain names and DNS

■ Joint Research 2017

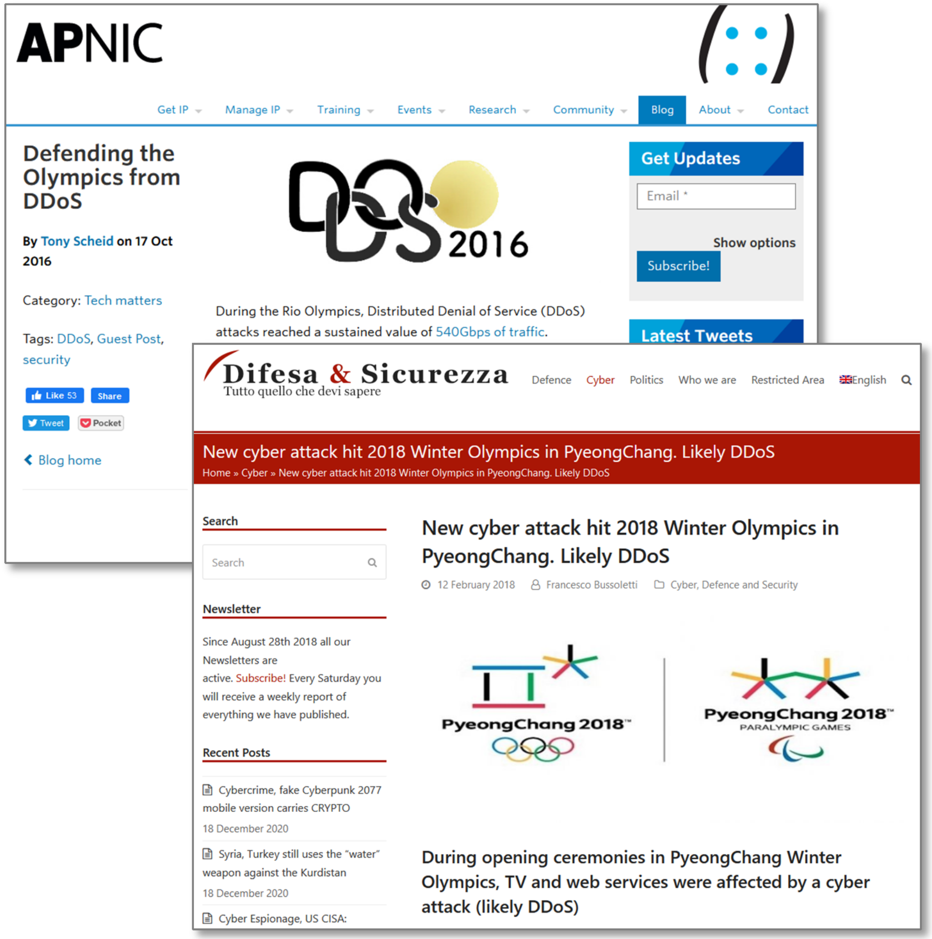
Japan as a disaster-prone country, joint experiments with domestic ISPs were conducted to verify the effectiveness of deploying TLD DNS Server inside the domestic ISPs against the physical Internet divide.

“TLD Anycast DNS servers to ISPs”

https://2017.apricot.net/program/schedule/#/day/9/network-operations-2

JPRS

Background of Joint Research 2021



Defending the Olympics from DDoS

By Tony Scheid on 17 Oct 2016

Category: Tech matters

Tags: DDoS, Guest Post, security

During the Rio Olympics, Distributed Denial of Service (DDoS) attacks reached a sustained value of 540Gbps of traffic.

New cyber attack hit 2018 Winter Olympics in PyeongChang. Likely DDoS

Home » Cyber » New cyber attack hit 2018 Winter Olympics in PyeongChang. Likely DDoS

New cyber attack hit 2018 Winter Olympics in PyeongChang. Likely DDoS

12 February 2018 Francesco Bussoletti Cyber, Defence and Security

During opening ceremonies in PyeongChang Winter Olympics, TV and web services were affected by a cyber attack (likely DDoS)

Newsletter

Since August 28th 2018 all our Newsletters are active. Subscribe! Every Saturday you will receive a weekly report of everything we have published.

Recent Posts

Cybercrime, fake Cyberpunk 2077 mobile version carries CRYPTO
18 December 2020

Syria, Turkey still uses the "water" weapon against the Kurdistan
18 December 2020

Cyber Espionage, US CISA:

TORCH RELAY

Revised Outline of Tokyo 2020 Olympic Torch Relay Announced

During the most recent Olympic Games, cyber-attacks such as malware and DDoS attacks of several hundred Gbps were launched against sites related to the Games.

The Tokyo Olympic Games are scheduled to take place in 2021. However, it is necessary to prepare for large-scale cyber-attacks that occur at every Olympic Games.

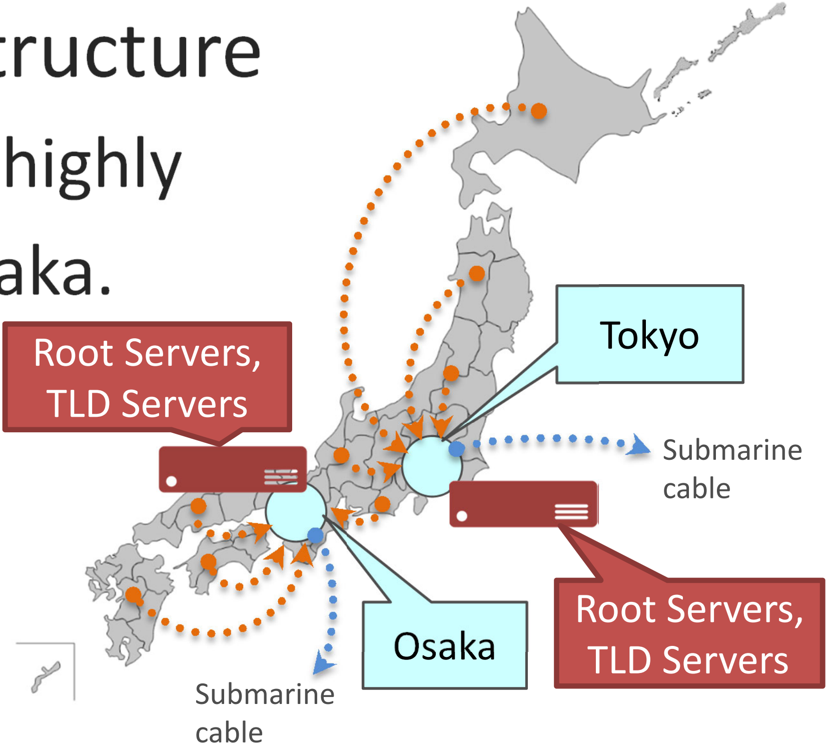
Need to prepare for massive DDoS attacks

Logical Structure of Internet in Japan

■ Characteristic of Internet structure

Critical Internet resources are highly Concentrated in Tokyo and Osaka.

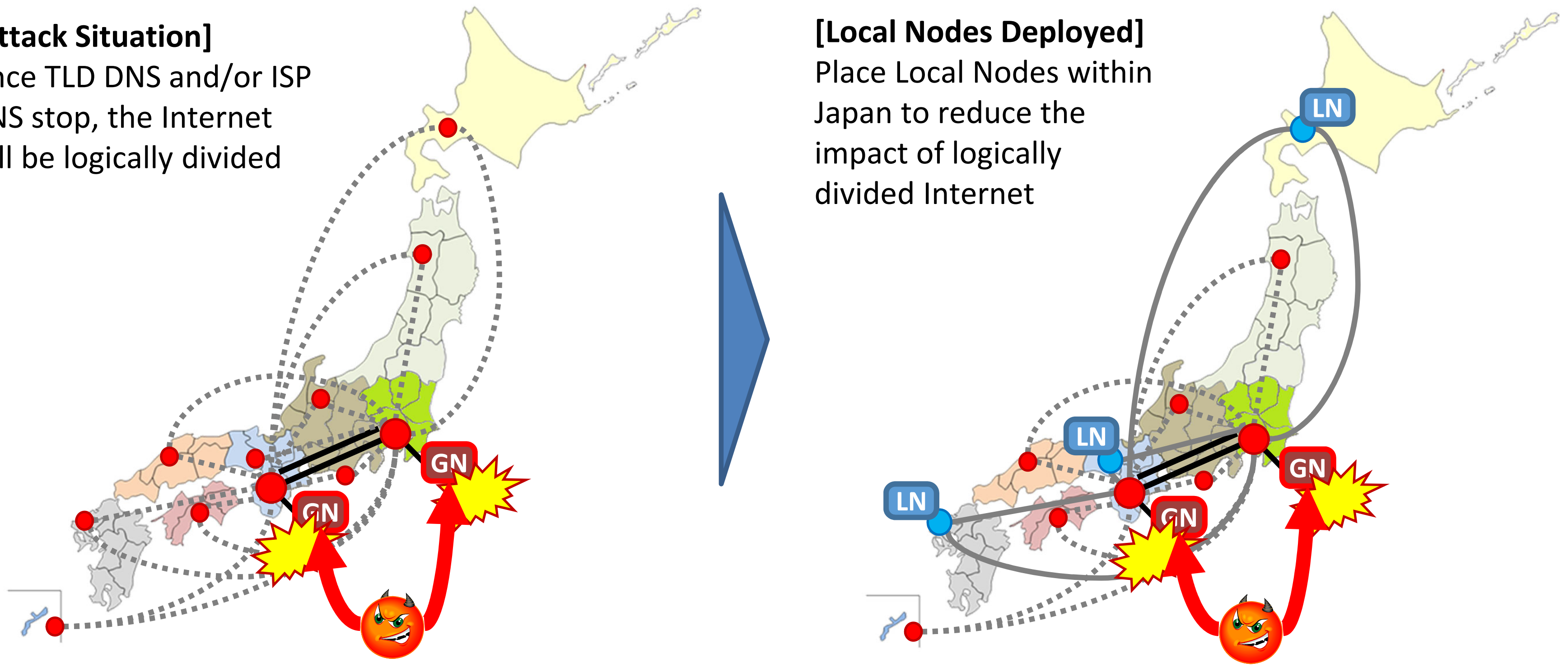
- Internet Exchanges (IXs), Transit connections, Data Centers, and so on
- Root Servers and TLD DNS Servers are also concentrated



When cyber attacks are targeted at facilities located in Tokyo and Osaka, ISPs in other regions will also not able to resolve names. They will virtually lose access to local internet resources. We call such situation “logical internet divide”.

Goal of the Project:
Enhance DNS Resiliency to logical Internet divide

- Prepare for Cyber Attacks toward 2021 Tokyo Olympic and Paralympic Games
  - Deploy local nodes, so that DNS name resolution can continue even in the event of a DDoS attack on DNS servers in Tokyo and Osaka.



[Attack Situation]
Once TLD DNS and/or ISP DNS stop, the Internet will be logically divided

[Local Nodes Deployed]
Place Local Nodes within Japan to reduce the impact of logically divided Internet

GN .jprs DNS Global Node

LN .jprs DNS Local Node (BGP NO-EXPORT)

● ISP (name resolution not affected)

● ISP (name resolution affected)

━ Circuit

┅ Circuit (logically divided)

✸ Traffic congestion by Cyber Attacks

Overview of Joint Research

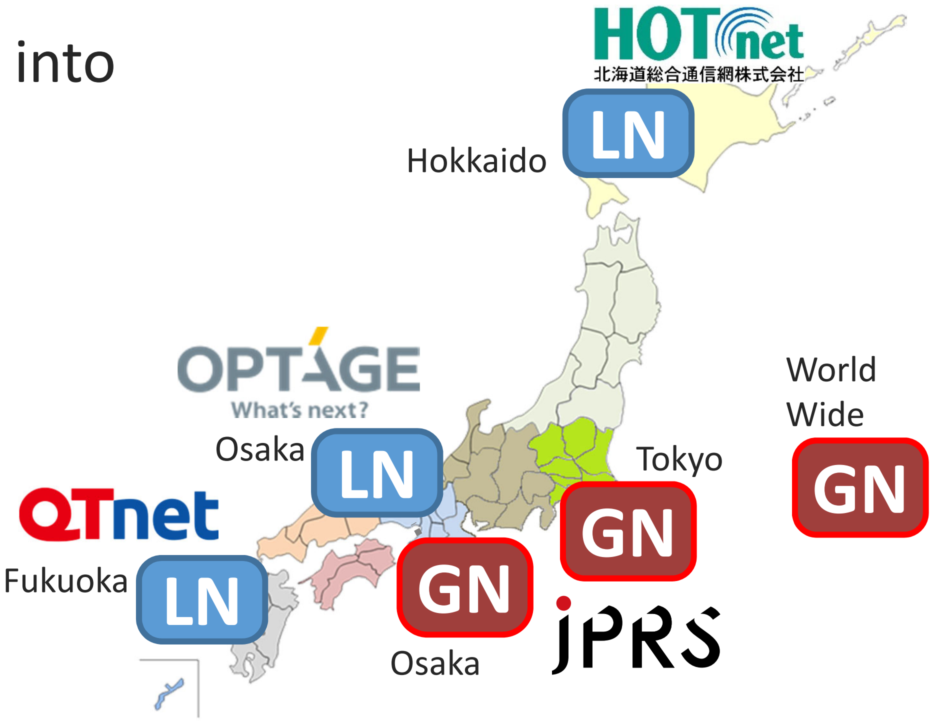
- Joint research effort with 3 domestic ISPs

  Each of their service area covers designated geographical area without overlap

- Way to direct DNS queries to Local Nodes

  Deploy ***tld4**.nic.jprs* DNS server into ISP networks as **Local Node**

  (BGP Anycast).



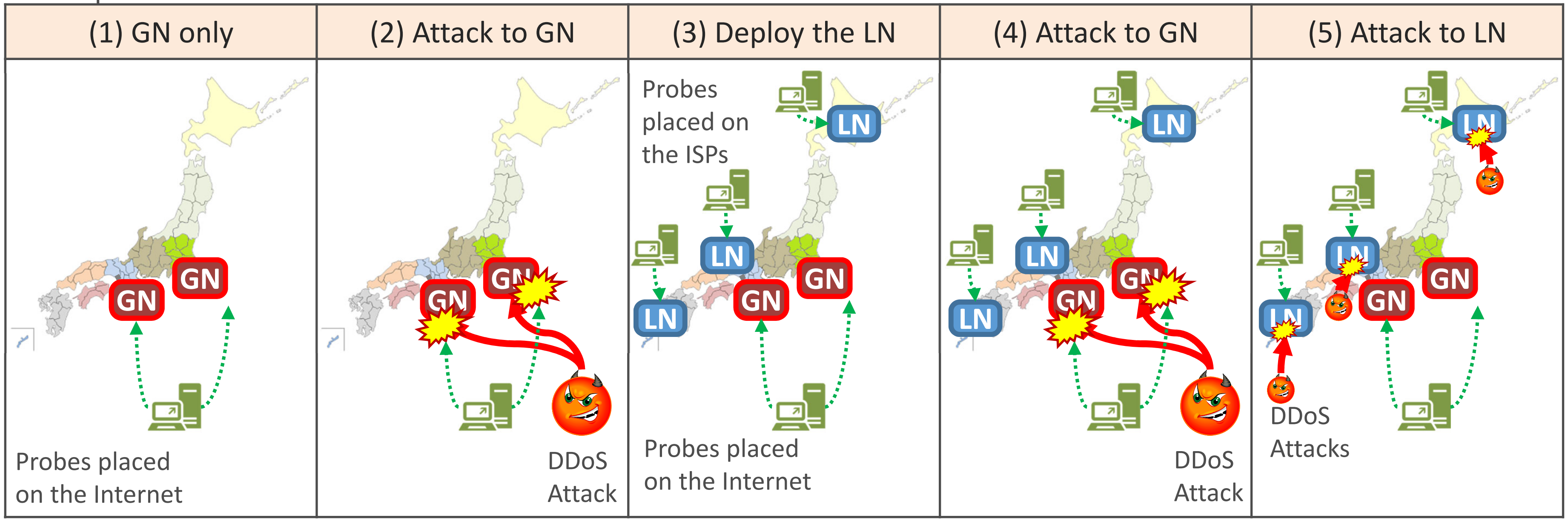
GN Global Node (JPRS)
tld[1-5].nic.jprs

LN Local Node (ISP)
tld4.nic.jprs (bgp no-export)

Scenarios and Measurements

- Performed DDoS attack scenarios
  - DDoS attack to DNS server without local nodes (global nodes only)
  - DDoS attack to DNS server with local nodes (and global nodes)
- Measurements
  - Verify continuity of name resolution from probes placed on the Internet and probes placed inside the ISP

Description of States



(1) GN only

(2) Attack to GN

(3) Deploy the LN

(4) Attack to GN

(5) Attack to LN

Probes placed on the Internet

DDoS Attack

Probes placed on the ISPs

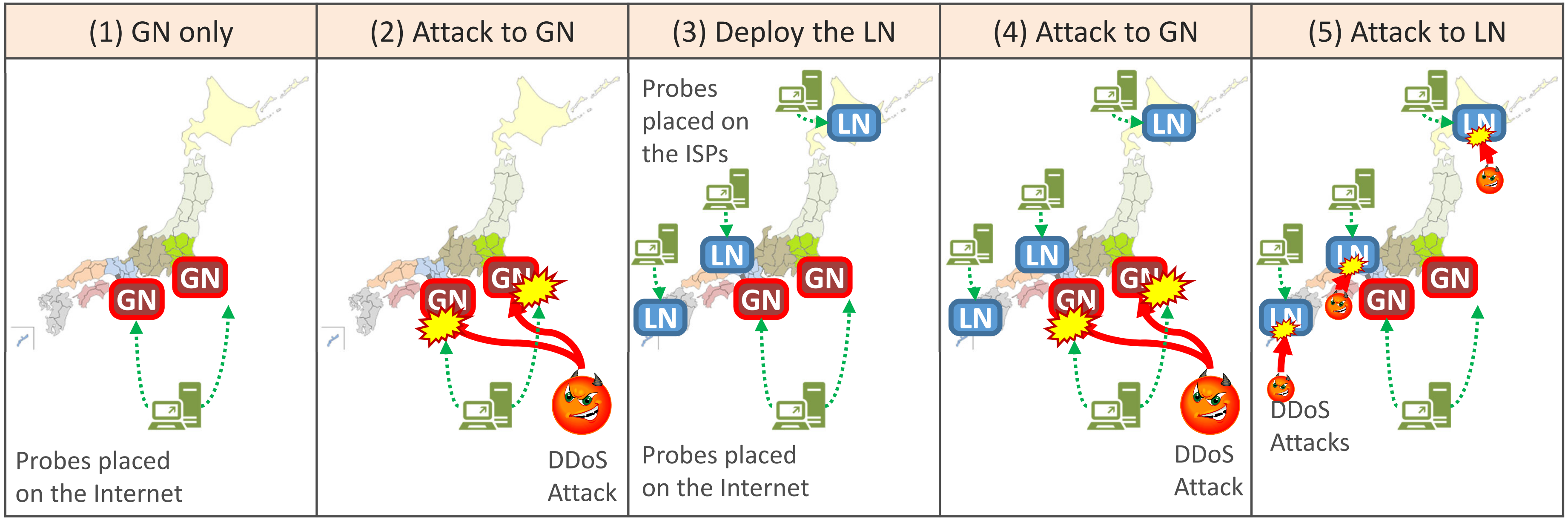
Probes placed on the Internet

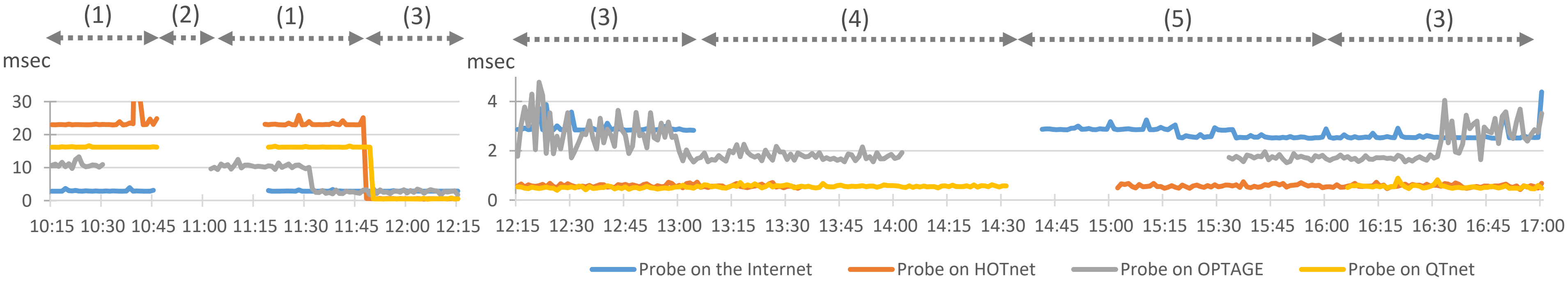
DDoS Attack

DDoS Attacks

Results of JPRS Experiment

Description of States





Some of the OPTAGE graphs are not stable because of the experimental network.

- JPRS monitored the status of Local Node from probes set up in each region. In Scenario No.4, we observed the LN servers name resolution unaffected locally.
- Scenario No.5 shows that the Local Node is able to absorb the attack.

Joint Research Report
by OPTAGE

(AS17511)

Company Name

OPTAGE Inc. (former: K-opticom Corporation)

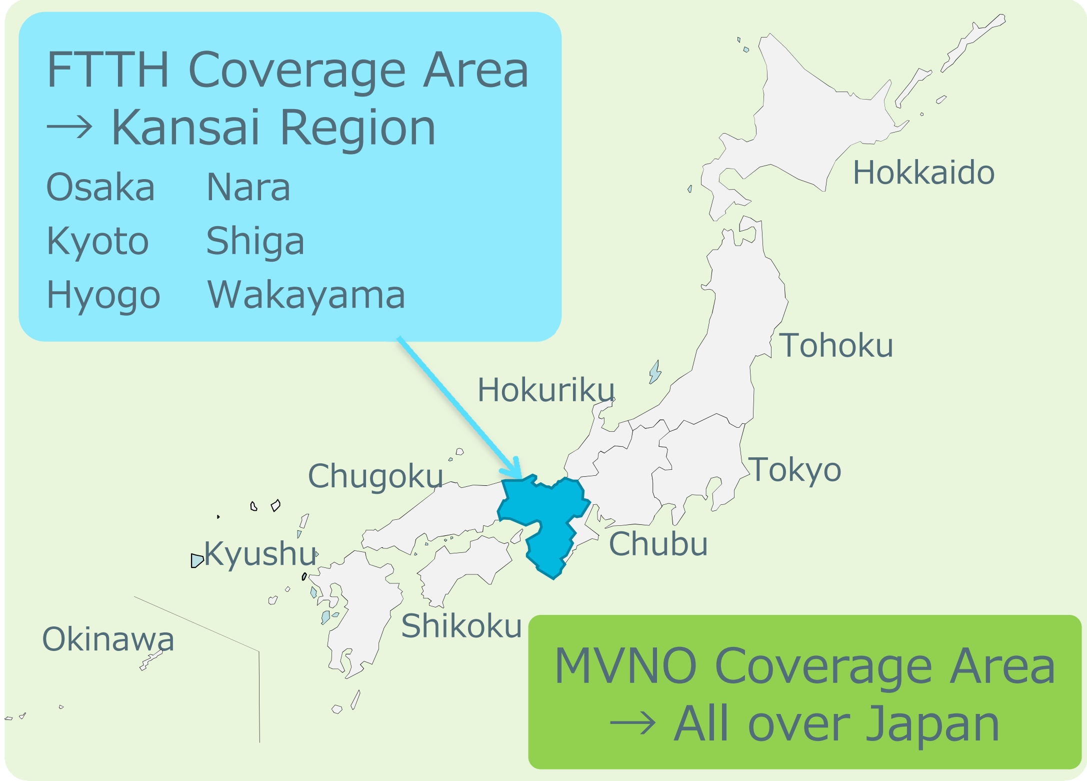
- ➢ Telecommunications carrier in Osaka , Japan

Services

- ➢ FTTH
  - ✓ Internet Access
  - ✓ VoIP
  - ✓ TV
- ➢ MVNO
- ➢ SI/ICT Solution, etc.

1.6 million Subscribers

1.2 million Subscribers



FTTH Coverage Area → Kansai Region

Osaka	Nara
Kyoto	Shiga
Hyogo	Wakayama

MVNO Coverage Area → All over Japan

Background

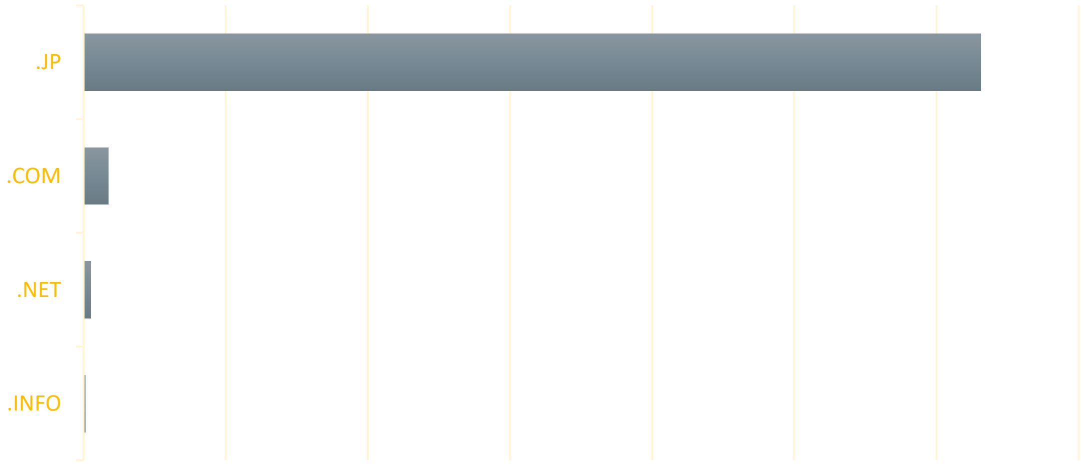
The advantage of using “.jprs”

- ".jprs" registry operator is the same as ".jp,"

  which is ccTLD for Japan.

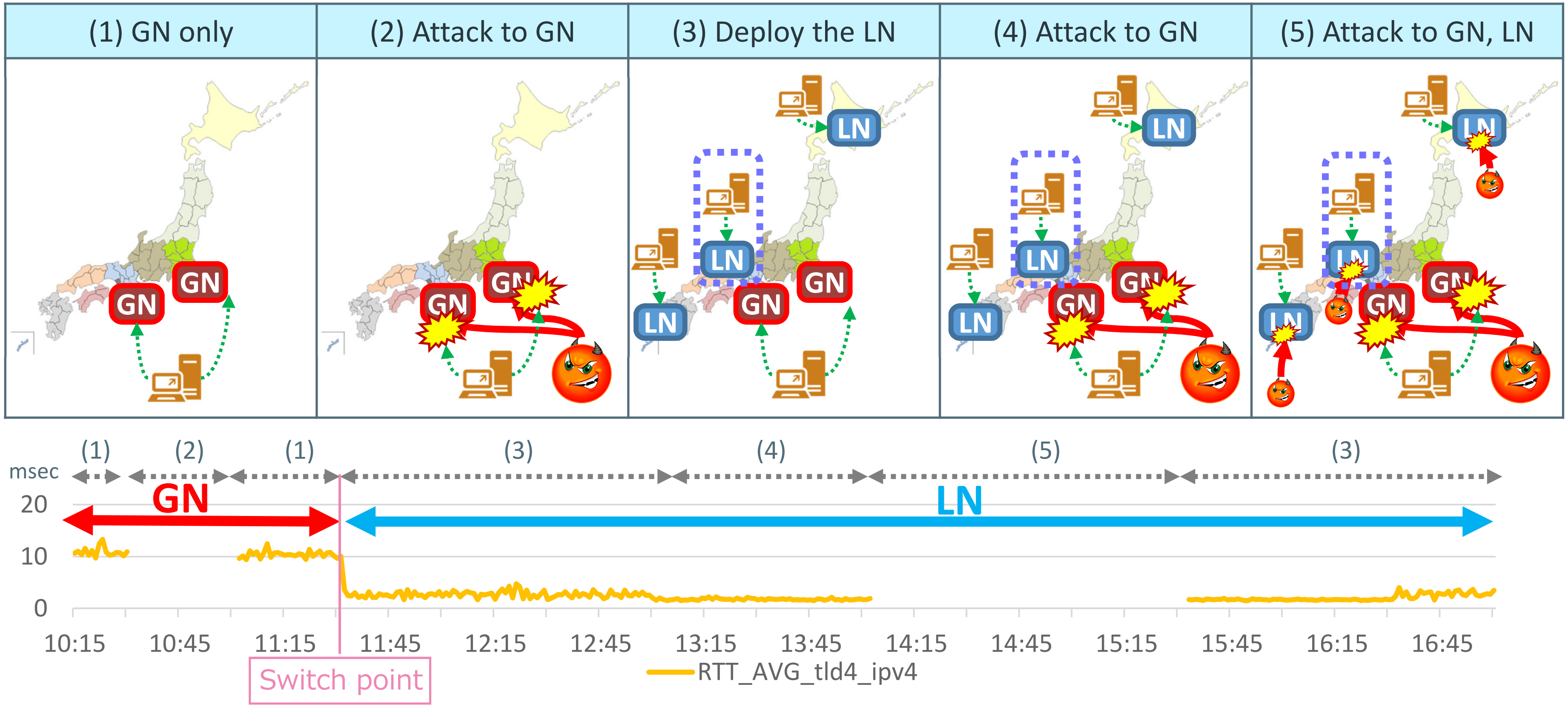
- The number of registered domains:“.jp”is 1st place.

Number of Registered Domains (OPTAGE)



Many important customers use“.jp.”

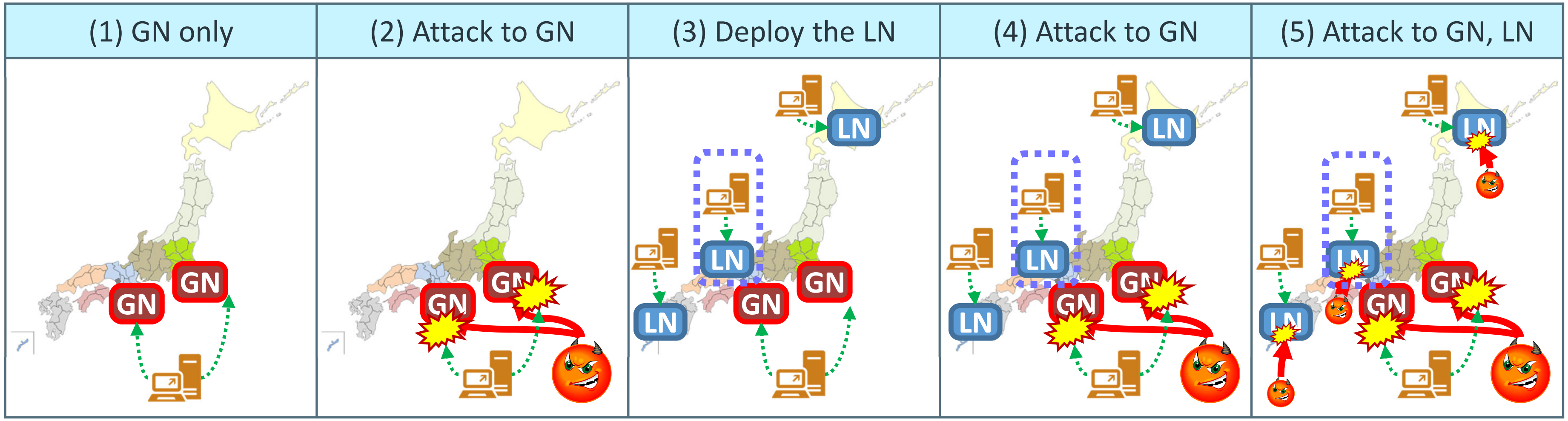
Results: ping RTT (1/2)



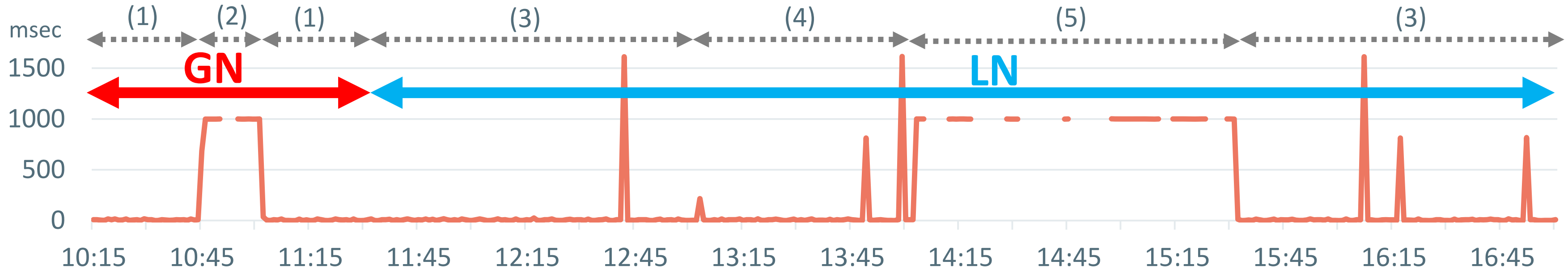
Note: The situation (1)~(2): LN is not in service.
The situation (3) or later LN works because BGP route to the same IP as GN is advertised.

- This graph indicates ping RTT from the full resolver inside of our experimental network to the authoritative name server.
- It shows the authoritative name server was switched from GN to LN at Switch point.
- At the situation (2) obviously it was not responding, but at the situation (4) it was.

Results: dig RTT (2/2)



(1) GN only | (2) Attack to GN | (3) Deploy the LN | (4) Attack to GN | (5) Attack to GN, LN



Note: The situation (1)~(2): LN is not in service.
The situation (3) or later LN works because BGP route to the same IP as GN is advertised.

- This graph indicates dig RTT from LN, the probe set up inside of our experimental network, to the full resolver which is also set up inside of ours.
- Domain name can be resolved by LN at the situation (4), which is the purpose of this experiment.
- We assume that some singular points (1500ms, but status:NOERROR) are caused by temporary server delay due to heavy load.

Conclusion

General comments

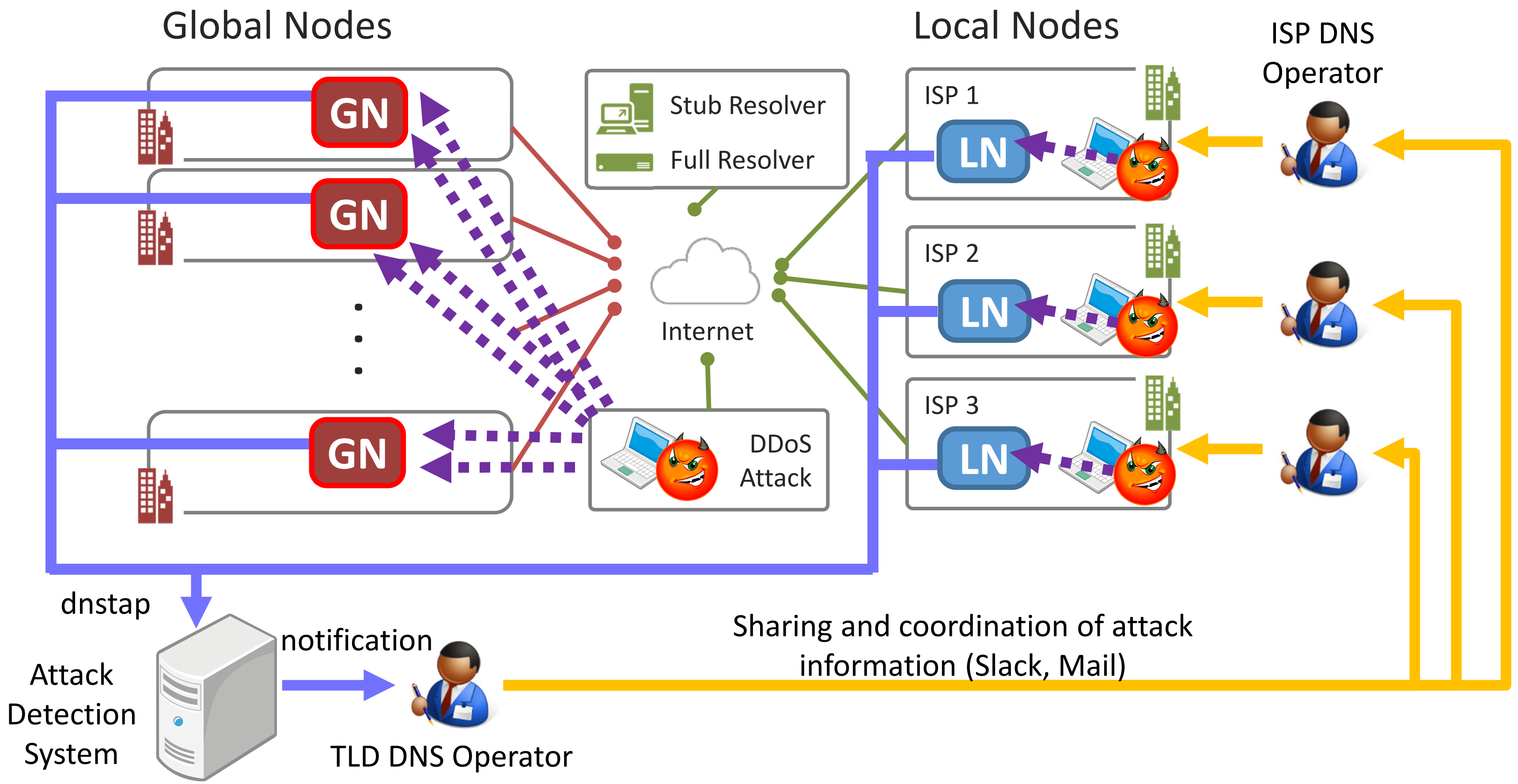
- Finally we found it effective to locate LN in ISP network.
- LN makes it possible to resolve domain name while GN is being attacked.
- Also we can deal with LN-down because it occurs only when attacker's source IP is ISP users'.

Future tasks

- The trigger and the timing to switch from GN to LN, and vice versa
- The method of zone data synchronization between GN and LN
- The redundancy of LN placement, which depends on the time it takes to recover GN

Cyber Attack Response Training

- In order to prepare for Cyber Attacks on LNs, exercises were conducted among TLD operators and ISP operators to ensure that they can detect, communicate and respond to attacks. (In general, LNs are often installed with smaller performance compared to GNs due to lower query volume in normal times.)

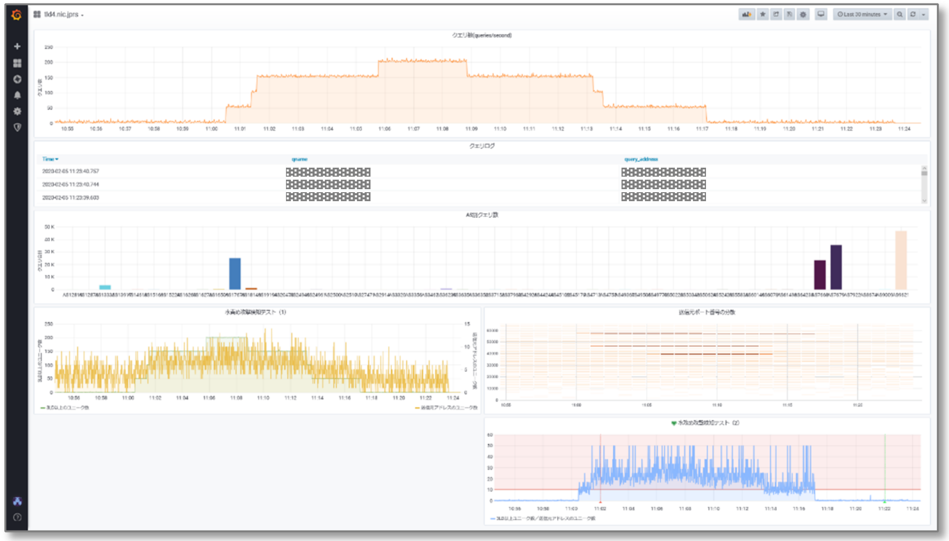


Lessons Learned from Training

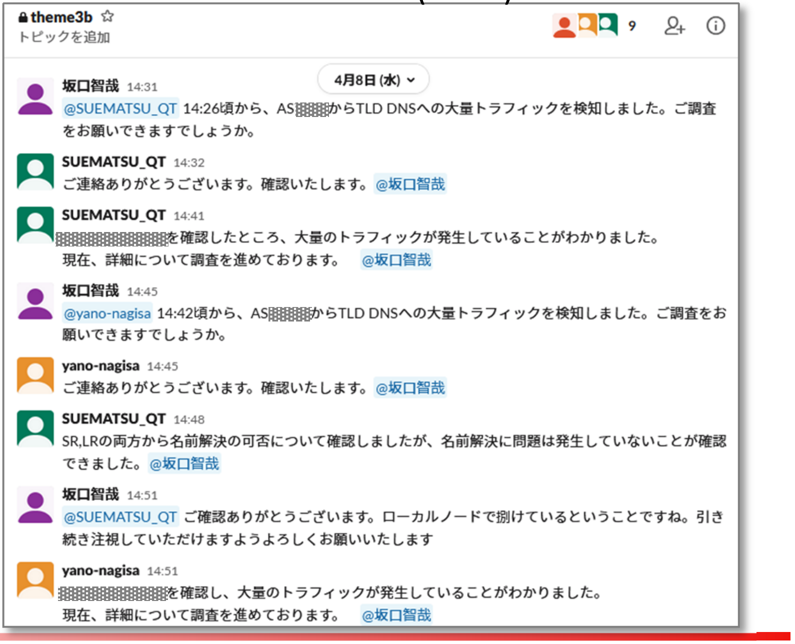
■ Lessons Learned

- ➢ Sharing information among TLD Operator and ISP Operators is quite useful
- ➢ In practice, each ISP has its own operation body and contact point, thus different contact paths and methods are required
- ➢ However, informal community to exchange information among ISPs and TLD Operators is also quite important

Attack Detection System



Sharing and collaboration of attack information (Slack)



坂口智哉 14:31
@SUEMATSU_QT 14:26頃から、AS[redacted]からTLD DNSへの大量トラフィックを検知しました。ご調査をお願いできますでしょうか。

SUEMATSU_QT 14:32
ご連絡ありがとうございます。確認いたします。@坂口智哉

SUEMATSU_QT 14:41
[redacted]を確認したところ、大量のトラフィックが発生していることがわかりました。
現在、詳細について調査を進めております。 @坂口智哉

坂口智哉 14:45
@yano-nagisa 14:42頃から、AS[redacted]からTLD DNSへの大量トラフィックを検知しました。ご調査をお願いできますでしょうか。

yano-nagisa 14:45
ご連絡ありがとうございます。確認いたします。@坂口智哉

SUEMATSU_QT 14:48
SR,LRの両方から名前解決の可否について確認しましたが、名前解決に問題は発生していないことが確認できました。@坂口智哉

坂口智哉 14:51
@SUEMATSU_QT ご確認ありがとうございます。ローカルノードで捌けているということですね。引き続き注視していただけますようよろしくお願いいたします

yano-nagisa 14:51
[redacted]を確認し、大量のトラフィックが発生していることがわかりました。
現在、詳細について調査を進めております。 @坂口智哉

Consideration of LN deployment in Japan

From Disaster Perspective

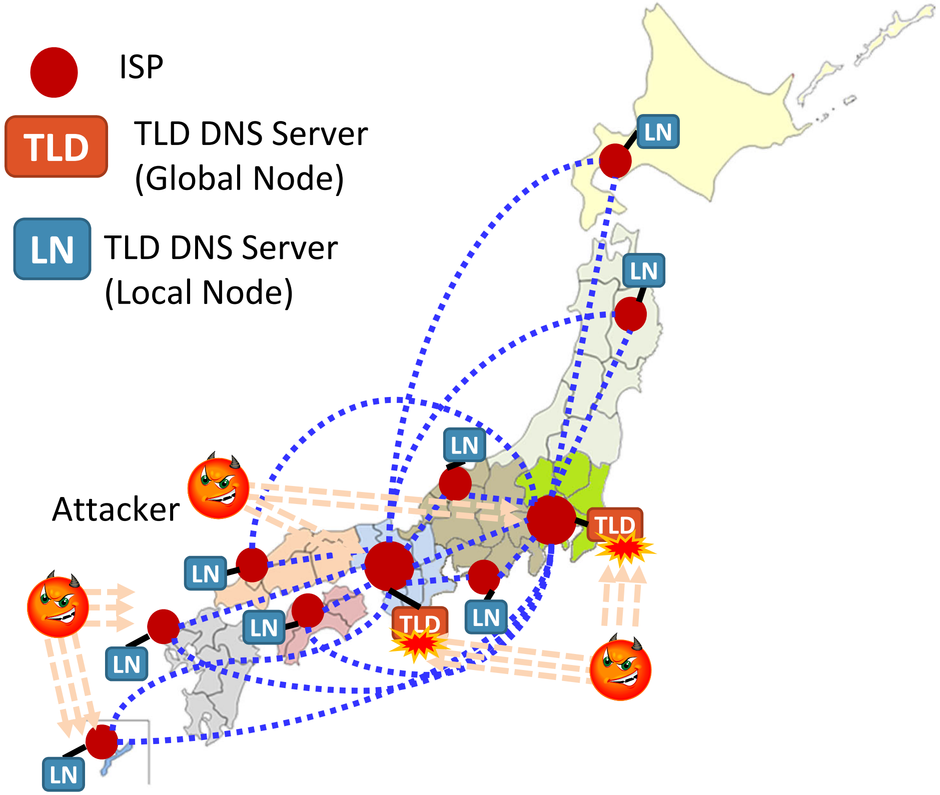
Japan as an island nation, the risk of submarine cables being cut by earthquakes and other disasters exists

- ➢ LNs are preferred to be placed on each island.

From Cyber Attack Perspective

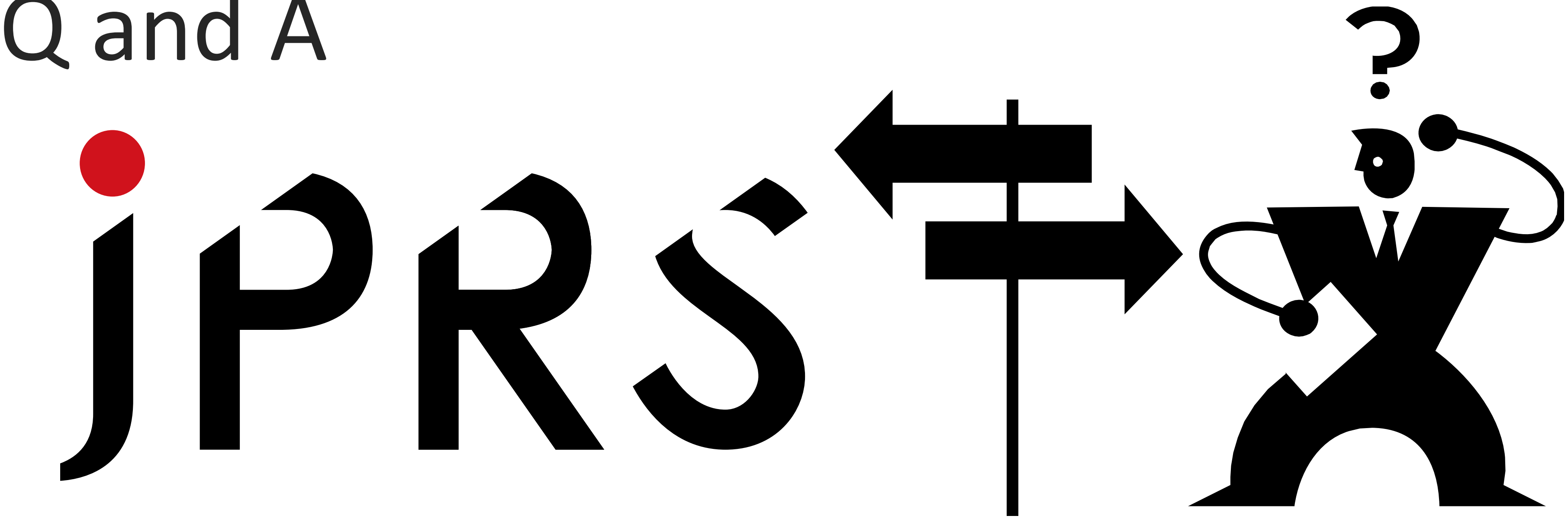
Since facilities are concentrated in Tokyo and Osaka, cyber attacks will also be concentrated there

- ➢ It is preferred to deploy LNs within ISPs which provide local services in their region


● ISP
TLD TLD DNS Server (Global Node)
LN TLD DNS Server (Local Node)
Attacker
LN
TLD

In general, since Japan is split in 8 regions, it is better to deploy LNs in each regional units first. (In terms of power supply and equipment as well. Fortunately, each region has local power provider and local ISP)

Q and A



- If anyone has experiences of doing this or that in the past Olympic Games, I would like to hear about it.

- Email:
  - dotjprstestbed-sec@jprs.co.jp
- URL:
  - https://tldlabs.jprs/en/