agenda

- current status of reverse dns(rdns)
- dns cache poisoning
- breaking trust chain
- reverse dns and DNSESEC

summary

- current status
  - Many businesses are utilizing this service . Therefore , those operators are expecting a stable operation of this service .
- cache poisoning
  - Exploitable attack to cache poisoning has occurred in 2014
- breaking trust chain
  - DNSSEC is effective to prevent such attacks . However, since we have not introduced a DNSSEC, the user is not able to determine the accuracy of the answers
- reverse dns and DNSSEC
  - We establish a chain of trust by introducing a DNSSEC to Reverse DNS.

current status of reverse dns

Survey on the usage of Reverse DNS

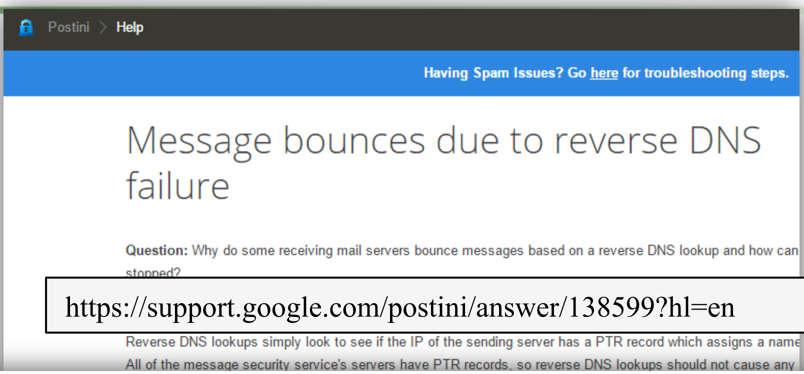
purpose	To know the usage of Rev DNS in 2014
Survey target	Operators of • Network, servers • e-mail services • IP address reputation services • cloud service/data center • Security services
# of valid responses	11 (out of 14 targets)
Survey period	August to October 2014
hearing item	✓ Use cases ✓ importance of utilizing Reverse DNS ✓ demand for Reverse DNS ✓ degree of dependence on Reverse DNS ✓ Other comments

Result

“Utilizing RevDNS for the services” (”not ustilizing”)	1 0 out of 11 (1 out of 11)
Use Cases	• reachability improvement of e-mails • Sender validation of e-mails • web log analysis. • Reference for server/network operation.
Degree of dependence	Most respondents answered “one of the key measures”
Other comments	“Stable responses for queries are indispensable”

Usecases in Cloud services

- Google Gmail/ Apps
  - Validate the Senders/ receipients by RevDNS
- Amazon EC2
  - PTR record registration supported
- Microsoft AzureCloud
  - PTR record registration started



Having Spam Issues? Go here for troubleshooting steps.

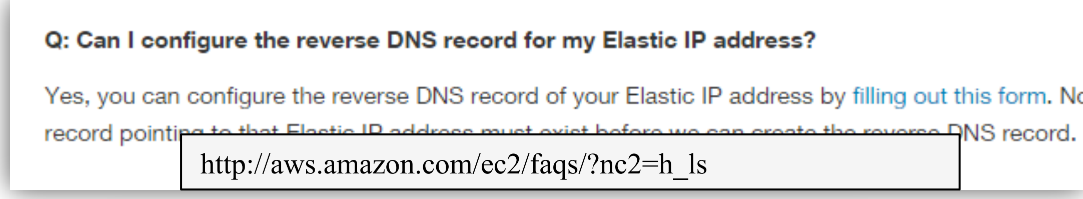
Message bounces due to reverse DNS failure

Question: Why do some receiving mail servers bounce messages based on a reverse DNS lookup and how can stopped?

Reverse DNS lookups simply look to see if the IP of the sending server has a PTR record which assigns a name

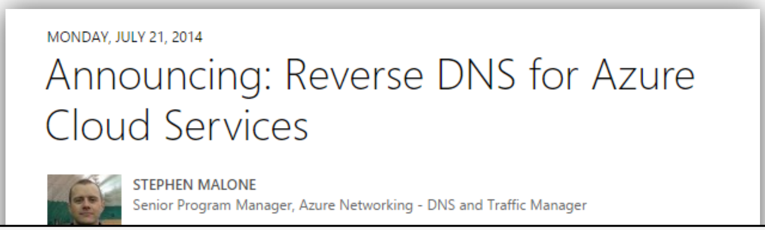
All of the message security service's servers have PTR records, so reverse DNS lookups should not cause any

https://support.google.com/postini/answer/138599?hl=en


Q: Can I configure the reverse DNS record for my Elastic IP address?

Yes, you can configure the reverse DNS record of your Elastic IP address by filling out this form. No record pointing to that Elastic IP address must exist before we can create the reverse DNS record.

http://aws.amazon.com/ec2/faqs/?nc2=h_ls


MONDAY, JULY 21, 2014

Announcing: Reverse DNS for Azure Cloud Services

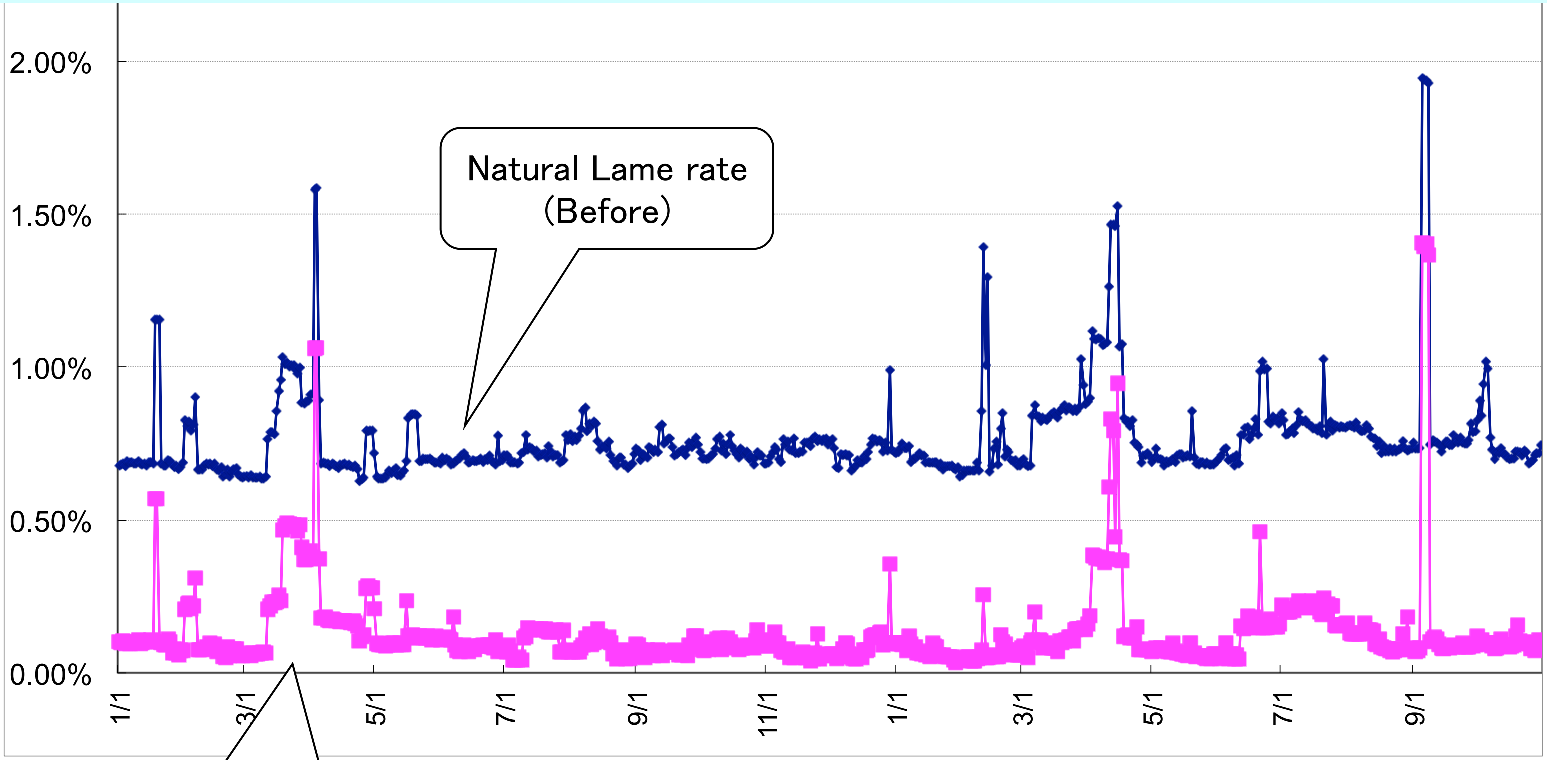
STEPHEN MALONE
Senior Program Manager, Azure Networking - DNS and Traffic Manager

http://azure.microsoft.com/blog/2014/07/21/announcing-reverse-dns-for-azure-cloud-services/

Many operators depend on reverse DNS for their service provision and need the stable and continuous provision of reverse DNS

Reference: Notification and Take-down of Lame Delegation under JPNIC management

Works for keeping operators very conscious on reverse DNS, as well as direct benefit of lowering lame delegation rate



Natural Lame rate (Before)

After taking down Lame Delegation

In 720,000 NS RR with Only 4,500RR (0.1%) were Lame.

cache poisoning

what is “cache poisoning”

- Sending false data to cache dns server
  - It is possible to pollute DNS data

- nherent vulnerability of the DNS

- problem that has been raised since 20years ago

cache poisoning

- 2008
  - Technique of efficient attack was discovered
- 2014
  - Exploitable DDoS attack applicable cache poisoning in some operators
  - A method with much wider impact re-confirmed

Risk by cache poisoning has been significantly increased

risk of cache poisoning

- problem
  - Introducing mis-behavior of DNS application
  - derivation to phishing sites and counterfeit e-mail server
- Especially in case of reverse DNS
  - Introducing wrong behavior of e-mail service operation
  - Bigger zones than name-to-number resolution
  - IPv6: many zones without an NS record

Reverce DNSSEC is
able to address these problem

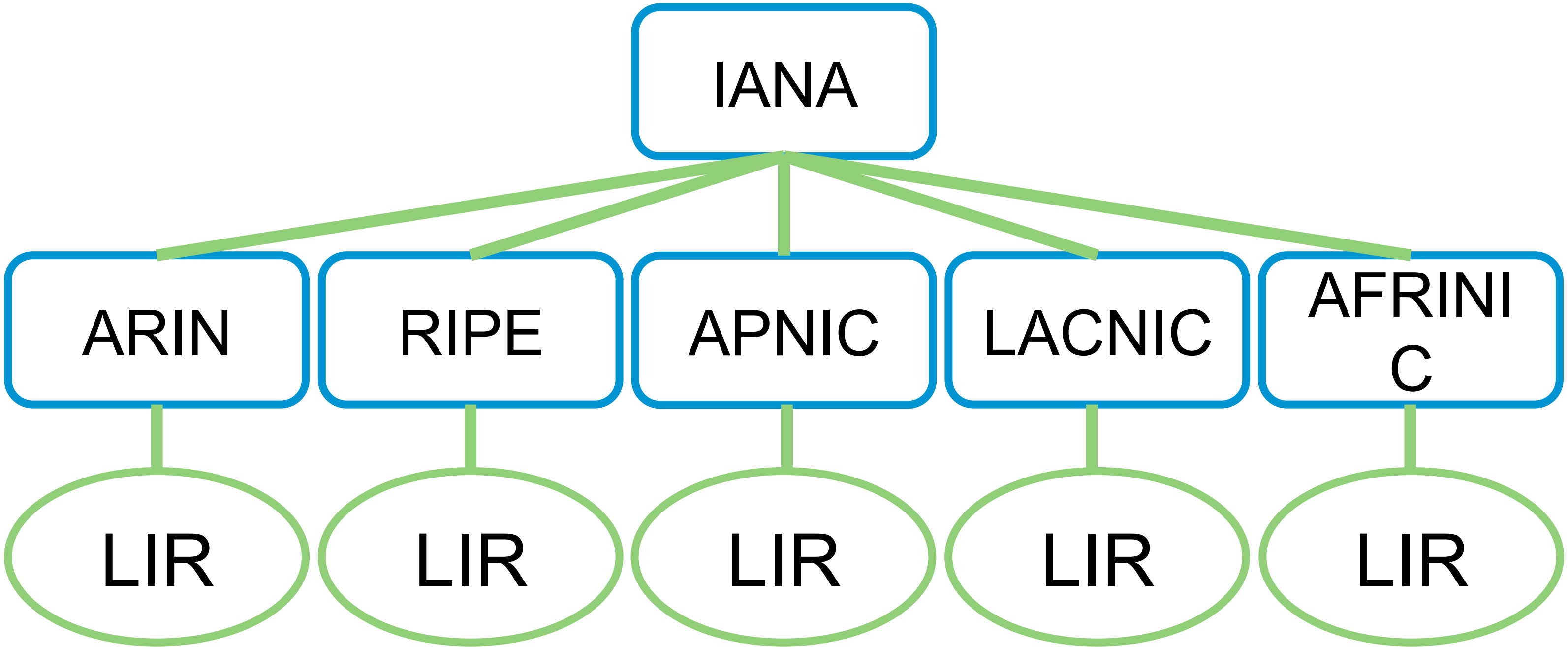
Benefit by DNSSEC

- What is dnssec
  - extending DNS protocol
    - ✓ DNS with PKI = DNSSEC
  - It is possible to identify valid or invalid response
- cache dns server
  - identify dns query by DNSSEC validation
  - cache server is protected from cache poisoning

Problem at JPNIC and other NIRs: breaking trust chain

IANA and RIR: trust chain exists

- IANA and RIRs already provide DNSSEC system for members
  - created trust chain(LIR can use reverse DNSSEC)



DNSSEC Records Statistics in Reverse DNS

- APNIC/RIPE/ARIN
  - Public ftp site updated daily
    - ✓ Format(example):

> ✧ APNIC.203.in-addr.arpa. IN TXT "Generated at 2014-09-12 06:50:41 EST with 65180 NS records and **74 DS records** from APNIC.“
>
> countable

- LACNIC/AFRINIC
  - No similar format public data
  - Inquired in cooperation with APNIC tech staff at APNIC38

DNSSEC records statistics:result

RIR	number of records	number of zones
APNIC	184	405,818
RIPE	1,244	666,219
ARIN	457※	486,403
LACNIC	4~5	n/a
AFRINIC	20	28,188

※91 operators

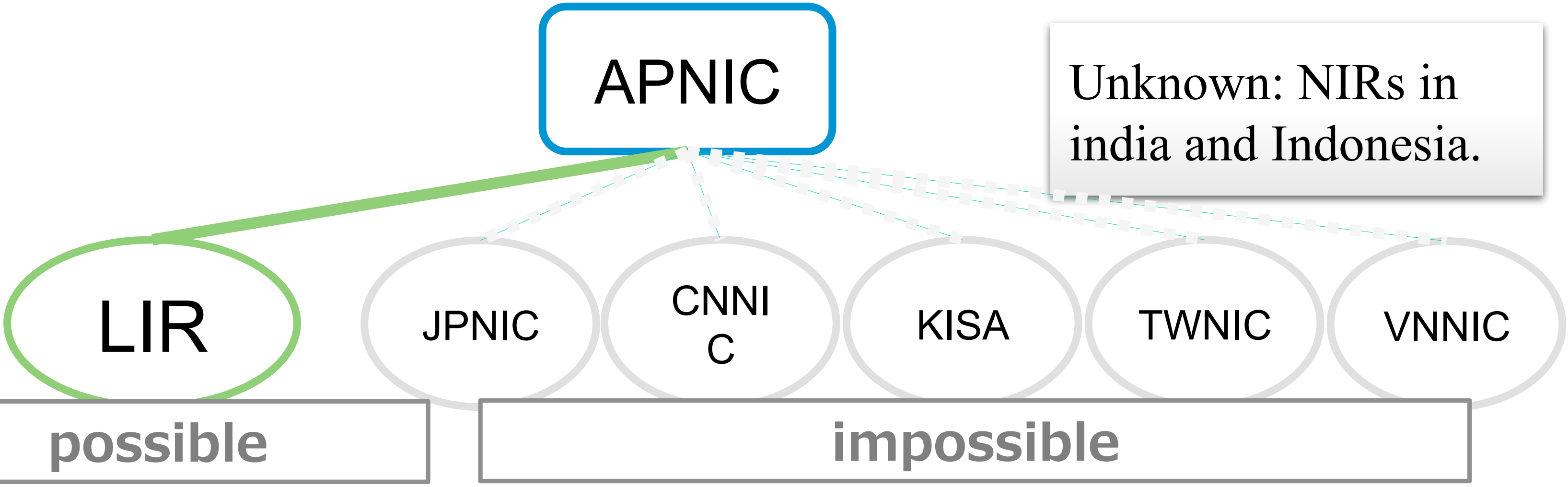
APNIC’s analysis:
Percentage of queries with DNSSEC enabled: 12%

NIR’s condition

- APNIC’s LIR can use reverse DNSSEC
- APNIC’s NIR DO NOT implement reverse DNSSEC
  - It is breaking between APNIC to NIRs trust chain.

It is impossible to use

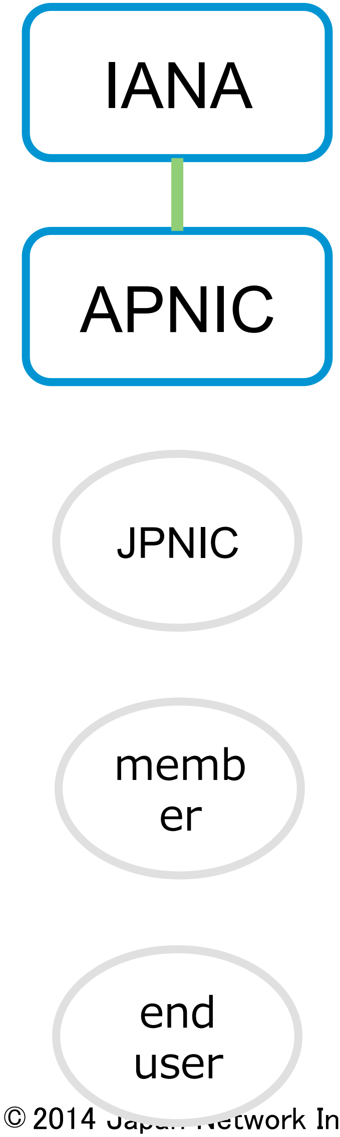
Reverse DNSSEC under NIR.....

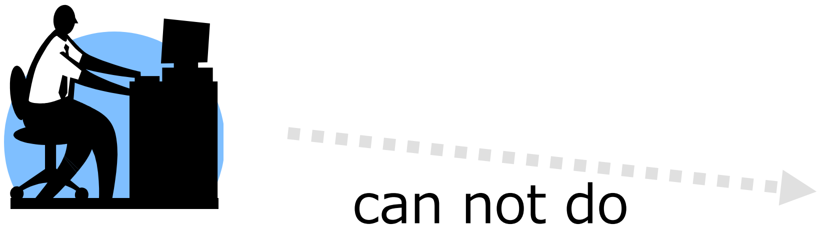


Unknown: NIRs in india and Indonesia.

Current Situation in JPNIC area

- trust chain is implemented between IANA to APNIC
- APNIC-JPNIC **<u>no trust chain</u>**
- end user and member can not use reverse DNSSEC





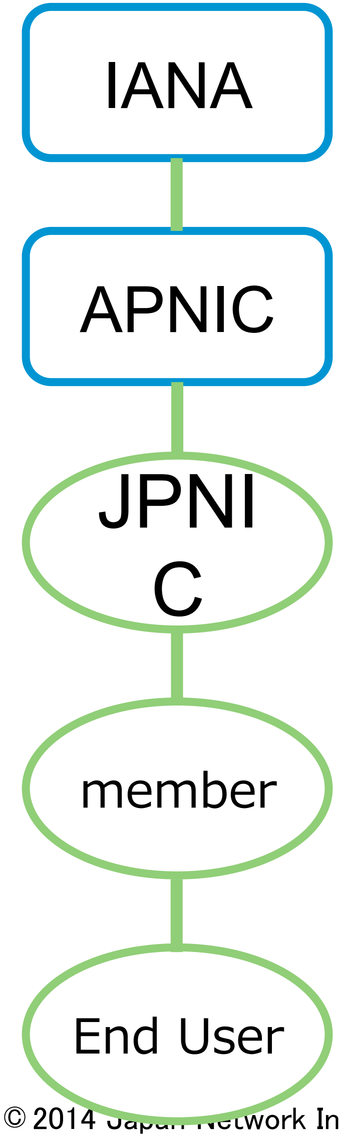
can not do DNSSEC validation

(Near)Future situation in JPNIC area

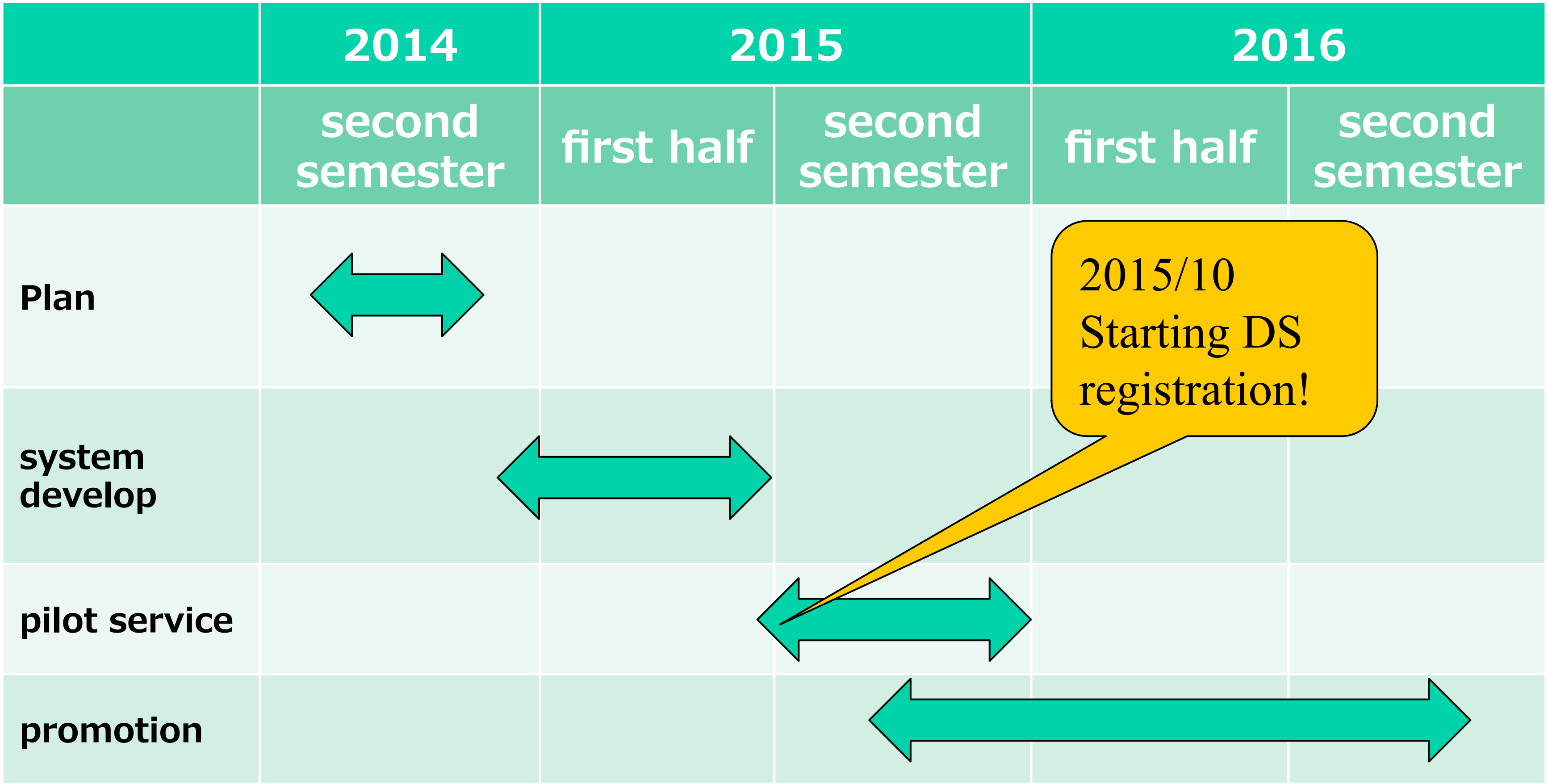
- JPNIC will implement reverse DNSSEC in 2015

Creating trust chain and promote other NIRs!!

Validation



JPNIC rdns dnssec schedule



	2014	2015		2016	
	second semester	first half	second semester	first half	second semester
Plan	↔				
system develop		↔			
pilot service			↔		
promotion			↔	↔	↔

2015/10 Starting DS registration!

(japan's financial year is starting Apr to March)

Q and A