DNSSEC Technology Experiment Report

Operational Design

Japan Registry Services Co., Ltd.

http: //jprs.co.jp/

2010-12-17 Ver. 1.0

(2011-11-28 English Translation)

Note about this translation

This English translation is provided only for reference. The original verion of this document was written in Japanese and is available from following URI:
<http://jprs.jp/dnssec/doc/DNSSEC-testbed-report-odv1.0.pdf>

Acknowledgement

This translation is contributed by APNIC (Asia Pacific Network Information Centre). We would like to express our sincere thanks to APNIC.

Table of Contents

Summary of the DNSSEC Technology Experiment

When DNSSEC services are provided by Internet Service Providers (ISPs) and .JP registrars which act as intermediaries in the registration of domain names, there are new items which should be discussed and designed related to the operation and service combination. Among a range of such items, the transfer of .JP domain name registrars, in particular, involves significant changes in the operation and service flow and requires the establishment of a basic flow and measures for anticipated troubles. In addition, anticipated questions and answers related to DNSSEC services for customers and end users can be used as verification points when discussing and designing the operation and service combination.

We conducted an experiment based on a .JP domain name registrar transfer scenario in order to deploy DNSSEC services smoothly. Furthermore, anticipated questions were collated and classified into common questions and specific questions.

Through this experiment, we obtained findings on the transfer of .JP domain name registrars as well as a FAQ with verification points which could be used when discussing and designing DNSSEC services.

This report summarizes results of the experiment conducted between July and November 2010 as individual case studies.

Registrar Transfer Experiment

Background of Experiment Implementation

There are cases where domain name registrants change their .JP registrar, an intermediary of the domain name registration, to another .JP registrar due to some circumstances. This is generally called a “registrar transfer (“.JP registrar transfer” for .JP domain names.)” Many .JP registrars provide not only intermediary service for the domain name registration but also hosting service of authoritative DNS servers for the name resolution of applicable domain names (DNS operator service). Therefore, registrar transfers often accompany a DNS operator transfer in addition to intermediary service for the domain name registration.

In the case of the registrar transfer for the domain name that is not DNSSEC-compliant (without DNSSEC signatures) and which accompanies the transfer of a DNS operator, the transfers can be completed smoothly without causing any interruption to the name resolution of the domain name by changing registered information on the name server at the same time. On the other hand, in the case of the registrar transfer for the domain name that is DNSSEC-compliant (with DNSSEC signatures) and which accompanies the transfer of a DNS operator, not only registered information on the name server but also signature key information need to be changed. Because such changes have to be done in a certain order, an error in the procedure could cause interruption to the name resolution of the domain name.

Since there are no procedures for the existing registrar transfer to complete the transfer without causing any interruption to the name resolution of the DNSSEC-compliant domain name, new procedures have to be set up for each .JP registrar. We think that it is useful in designing services provided by .JP registrars to prepare procedures deemed to be standard, actually testing to verify that the registrar transfer can be completed without causing any interruption to the name resolution, and making sure the countermeasures in the case of a trouble caused by an error in the procedures.

In this experiment, situations and procedures deemed to be standard were prepared as scenarios and a simulation of the registrar transfer was conducted by several organizations who took part in the roles of the parties involved in the registrar registration.

Experiment Scenario

In the preparation of scenarios of the registrar transfer experiment, firstly, we made a list of combinations based on items including “Loosing registrar is DNSSEC-compliant or not,” “Gaining registrar is DNSSEC-compliant or not,” “DNS operator is transferred or not” and “Registrar is transferred or not.” With this list, we verified that other combinations can be covered if we focus on the following combination: “Both the loosing and gaining registrars are DNSSEC-compliant and both the DNS operator and registrar are transferred.” Fig. 1 below shows the list of combinations.

No	DNSSEC-compliant		DNS operator transfer	Registrar transfer	Experiment subject	Note
	Loosing	Gaining				
1	Yes	Yes	Yes	Yes	Yes	
2	Yes	Yes	Yes	No	Yes	
3	Yes	Yes	No	Yes		No change in DNSSEC. Existing registrar transfer procedures can be implemented.
4	Yes	Yes	No	No		Neither DNS operator nor the registrar are transferred.
5	Yes	No	Yes			Break down the procedures into two steps. Firstly, deactivate DNSSEC and secondly, execute the existing DNS operator and registrar transfers after the TTL expiry of L-DS. (*1)
6	Yes	No	Yes	No		
7	Yes	No	No	Yes		
8	Yes	No	No	No		This is out of scope of the experiment because neither the DNS operator nor the registrar will be transferred.
9	No	Yes	Yes	Yes		Break down the procedures into two steps. Firstly, execute the existing process of DNS operator and registrar transfers and secondly, activate DNSSEC. (*2)
10	No	Yes	Yes	No		
11	No	Yes	No	Yes		
12	No	Yes	No	No		Neither the DNS operator nor the registrar will be transferred
13	No	No	Yes	Yes		No impact of DNSSEC. (Same as the existing DNS operator transfer + registrar transfer)
14	No	No	Yes	No		No impact of DNSSEC. (Same as the existing DNS operator transfer.)
15	No	No	No	Yes		No impact of DNSSEC. (Same as the existing registrar transfer.)
16	No	No	No	No		Neither the DNS operator nor the registrar will be transferred

Yes: compliant
No: non-compliant

Yes: transfer
No: no transfer

(*1) If the registrar transfer is executed without waiting for the TTL expiry, there will be a period of time during which the name resolution fails. In addition, in cases where the gaining registrar is not DNSSEC-compliant, the loosing DS cannot be removed if the registrar transfer is executed without deactivating DNSSEC. However, for the case of a .JP domain name, the TTL issue is not avoidable but it does not lead to a significant issue because DS is automatically removed when NS is updated.
(*2) It is mandatory that both the gaining DNS operator and registrar are DNSSEC-compliant. DNSSEC must be activated in order of the zone disclosure and the DS registration.

Fig. 1: List of Combinations

Next, we listed up the parties involved in the registrar transfer as well as the information to be exchanged among the parties involved at the time of the registrar transfer. Chart 1 shows the list of the parties involved.

Chart 1: List of Parties Involved in the Registrar Transfer

Parties Involved	Explanation
Registrant	A domain name registrant
Registrant's ISP	An Internet service provider which provides Internet connection service (including cache DNS server) to registrants
Loosing DNS operator	An operator which had provided an authoritative DNS server for the name resolution of the domain name held by the registrant prior to the registrar transfer.
Loosing reseller	A business operator which was the main contact for the registrant with regard to the administrative procedures related to the domain name registration prior to the registrar transfer
Loosing registrar	A business operator which was in charge of the management of the domain name registration related-information for the registrant and acting as an intermediary between the registrant and the registry with regard to necessary information prior to the registrar transfer
Gaining DNS operator	An operator which will provide an authoritative DNS server for the name resolution of the domain name held by the registrant after the registrar transfer
Gaining reseller	A business operator which is the main contact for the registrant with regard to the administrative procedures related to the domain name registration after the registrar transfer.
Gaining registrar	A business operator which is in charge of the management of the domain name registration-related information for the registrant and acting as an intermediary between the registrant and the registry with regard to necessary information after the registrar transfer
Registry	A business operator which is in charge of the central management of registered domain names and reflecting the domain names on DNS to enable the name resolution on the Internet
End user	A end user who accesses services provided under the domain name of a registrant
End users' ISP	An Internet service provider which provides Internet connection service (including cache DNS server) to end users

Chart 2 shows information exchanged among the parties involved.

Chart 2: Information Exchanged Among the Parties Involved in the Registrar Transfer

Category	Exchanged information	Parties involved in the exchange of information
1. Contract	DNS hosting application	Registrant <- -> Gaining DNS operator or Gaining reseller or Gaining registrar (*1)
	DNS zone setting request	
	DNSSEC service application	
	Application for the loosing DNS hosting contract termination	Registrant <- -> Loosing DNS operator
	Application for the loosing registrar contract termination	Registrant <- -> Loosing reseller or Loosing registrar (*2)
2. Registrar transfer	Registrar transfer application	Registrant -> Gaining reseller -> Gaining registrar -> Registry (*2)
	Registrar transfer approval request/notification	Registry <- -> Loosing registrar <- -> Loosing reseller -> Registrant (*2)
	Registrar transfer completion notification	Registry -> Loosing registrar Registry -> Gaining registrar -> Gaining reseller -> Registrant (*2)
3. DNS operator transfer	Gaining DS information request	Registrant <- -> Gaining reseller <- -> Gaining registrar
	Loosing DS setting check	Gaining registrar <- -> Registry
	Gaining NS setting request	
	Loosing NS removal request	
	Gaining DS setting request	
	Loosing DS removal request	
4. Name resolution	Name resolution of domain names	Registrant <- -> Registrant's ISP End user <- -> End users' ISP

(*1) There are cases where a gaining reseller or a gaining registrar concurrently serves as a DNS operator.
(*2) There are cases where a gaining reseller does not exist and a gaining registrar becomes a main contact for the registrant. In such cases, gaining reseller is omitted. The same applies for the loosing reseller.

Based on this, we prepared a registrant transfer scenario using the most complicated model in which all parties involved are independent (Chart 3: Registrar Transfer Scenario with a Complicated Model) and a flow chart (Fig. 2: Flow Chart of Registrar Transfer with a Complicated Model). Anticipated troubles were included in such a scenario. Furthermore, there are many cases where a hosting business operator concurrently serves as a .JP registrar in Japan. Therefore, we also prepared a scenario in which loosing and gaining .JP registrars concurrently serve as DNS operators and resellers do not exist (Chart 4: Registrar Transfer Scenario with a Realistic Model) as a realistic model.

Chart 3: Registrar Transfer Scenario with a Complicated Model

Preconditions
The loosing registrar and the gaining registrar do not exchange key information.
The DNS delegation status should be continued even during the registrar and DNS operator transfer period. (The DNSSEC chain should be temporarily suspended for that purpose.)

Parties involved
Registrant
Registrant's ISP (Cache DNS)
Loosing DNS operator
Loosing reseller
Loosing registrar
Gaining DNS operator
Gaining reseller
Gaining registrar
Registry
End user
End users' ISP (Cache DNS)

Anticipated scenarios

I DNS setting by the gaining DNS operator

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
1	Registrant	Gaining DNS operator	1. DNS hosting service application		
2	Gaining DNS operator	Registrant	1. DNS hosting service application	The DNS server (NS) information is also notified.	
3	Registrant	Gaining DNS operator	1. DNS zone setting request		
4	Gaining DNS operator	Registrant	1. DNS zone setting request		
5	Registrant	Gaining DNS operator	1. DNSSEC service application		
6	Gaining DNS operator	Registrant	1. DNSSEC service application	The DNSSEC (DS) information is also notified.	

II Registrar change (registrar transfer)

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
7	Registrant	Gaining reseller	2. Registrar transfer application		
8	Gaining reseller	Gaining registrar	2. Registrar transfer application		
9	Gaining registrar	Registry	2. Registrar transfer application		
10	Registry	Loosing registrar	2. Registrar transfer approval request/notification		
11	Loosing registrar	Loosing reseller	2. Registrar transfer approval request/notification		
12	Loosing reseller	Registrant	2. Registrar transfer approval request/notification		
13	Registrant	Loosing reseller	2. Registrar transfer approval request/notification		
14	Loosing reseller	Loosing registrar	2. Registrar transfer approval request/notification		
15	Loosing registrar	Registry	2. Registrar transfer approval request/notification		
16	Registry	Gaining registrar	2. Registrar transfer completion notification	The domain name setting authority is transferred to the gaining registrar.	
17	Registry	Loosing registrar	2. Registrar transfer completion notification		
18	Gaining registrar	Gaining reseller	2. Registrar transfer completion notification		
19	Gaining reseller	Registrant	2. Registrar transfer completion notification		

III Changing of the DNS setting information (DNS operator transfer)

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
20	Registrant	Gaining reseller	3. Gaining NS setting request		
21	Gaining reseller	Gaining registrar	3. Gaining NS setting request		
22	Gaining registrar	Registry	3. Loosing DS setting check	**A voluntary action by the gaining registrar**	Because the gaining registrar submits the NS setting change application without checking the DS setting, end users become unable to access the registrant's domain name server. / The gaining registrar submits the L-DS removal application and requests the end users' ISP to clear the registrant's domain name cache.
23	Registry	Gaining registrar	3. Loosing DS setting check		
24	Gaining registrar	Gaining reseller	3. Gaining DS information request	The gaining registrar explains the transfer procedures to the	
25	Gaining reseller	Registrant	3. Gaining DS information request	The gaining reseller explains the transfer procedures to the registrant.	
26	Registrant	Gaining reseller	3. Gaining DS setting request		
27	Gaining reseller	Gaining registrar	3. Gaining DS setting request		
28	Gaining registrar	Registry	3. Loosing DS removal request		
29	Registry	Gaining registrar	3. Loosing DS removal request		
30	Gaining registrar		Waiting for the TTL expiry of L-DS	**A voluntary action by the gaining registrar**	
31	Gaining registrar	Registry	3. L-NS removal and G-NS setting request		Because the gaining registrar changes the NS setting without waiting for the TTL expiry of L-DS, end users become unable to access the registrant's domain name server. / The gaining registrar submits the application for the registration of G-DS and requests the end users' ISP to clear the registrant's domain name cache.
32	Registry	Gaining registrar	3. L-NS removal and G-NS setting request		
33	Gaining registrar		Waiting for the TTL expiry of L-NS	**A voluntary action by the gaining registrar**	
34	Gaining registrar	Registry	3. G-DS setting application		The gaining registrar registers G-DS without waiting for the TTL expiry of L-NS and end users become unable to access the registrant's domain name server. / The gaining registrar requests to the end users' ISP to clear the registrant's domain name cache.
35	Registry	Gaining registrar	3. G-DS setting application		
36	Gaining registrar		Waiting for the TTL expiry of G-NS	**A voluntary action by the gaining registrar**	
37	Gaining registrar	Gaining reseller	3. G-DS setting application		Because the registrant's domain name zone has CNAME and the destination of CNAME is an external domain name which is not DNSSEC-compliant, end users complain to the registrant that the registrant's domain name is not DNSSEC-compliant. The registrant changes CNAME to A/AAAA.
38	Loosing reseller	Registrant	3. G-DS setting application		

IV Termination of the loosing reseller / registrar / loosing DNS operator

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
39	Registrant	Loosing reseller	1. Application for the loosing registrar contract termination		
40	Loosing reseller	Registrant	1. Application for the loosing registrar contract termination		
41	Registrant	Loosing DNS operator	1. Application for the DNS operator contract termination		
42	Loosing DNS operator	Registrant	1. Application for the DNS operator contract termination		

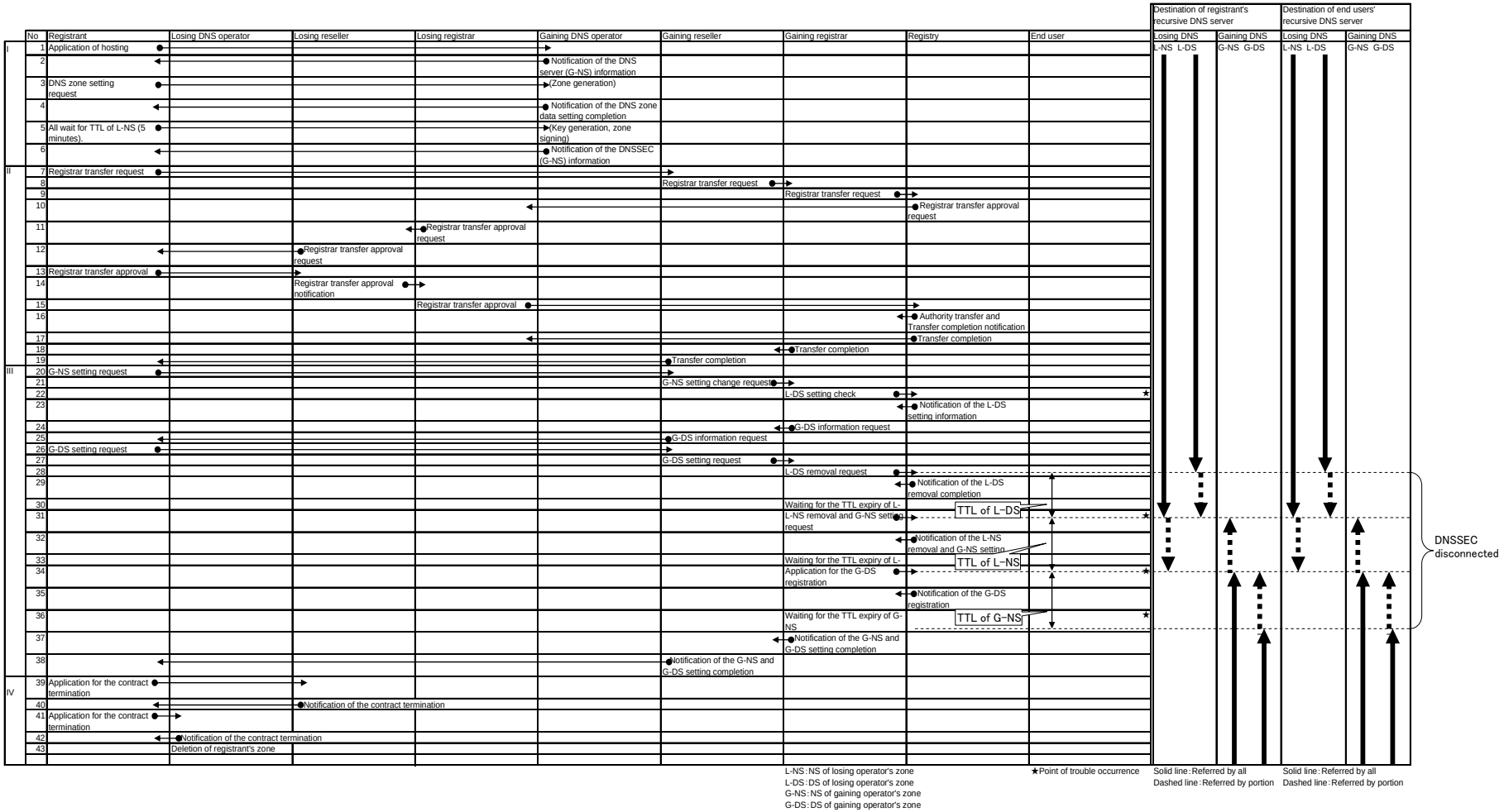


Fig. 2: Flow Chart of Registrar Transfer with a Complicated Model

Chart 4: Registrar Transfer Scenario with a Realistic Model

Pre-conditions
The loosing registrar and the gaining registrar do not exchange key information.
The DNS delegation status should be continued even during the registrar and DNS operator transfer period. (The DNSSEC chain should be temporarily suspended for that purpose.)
The loosing registrar which concurrently serves as a DNS operator does not remove the registrant's zone data soon after the registrar transfer.

Parties involved
Registrant
Registrant's ISP (Cache DNS)
Loosing registrar (which concurrently serves as the loosing DNS operator)
Loosing registrar (which concurrently serves as the loosing DNS operator)
Registry
End user
End users' ISP (Cache DNS)

Anticipated scenarios

I DNS setting by the gaining DNS operator

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
1	Registrant	Gaining registrar	1. DNS hosting service application		
2	Sender of the information	Registrant	1. DNS hosting service application	The DNS server (NS) information is also notified.	
3	Registrant	Gaining registrar	1. DNS zone setting request		
4	Gaining registrar	Registrant	1. DNS zone setting request		
5	Registrant	Gaining registrar	1. DNSSEC service application		
6	Gaining registrar	Registrant	1. DNSSEC service application	The DNSSEC (DS) information is also notified.	

II Registrar change (registrar tran G-DS setting request

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
7	Registrant	Gaining registrar	2. Registrar transfer application		
8					
9	Gaining registrar	Registry	2. Registrar transfer application		
10	Registry	Loosing registrar	2. Registrar transfer approval request/notification		
11					
12	Loosing registrar	Registrant	2. Registrar transfer approval request/notification		
13	Registrant	Loosing registrar	2. Registrar transfer approval request/notification		
14					
15	Loosing registrar	Registry	2. Registrar transfer approval request/notification		
16	Registry	Gaining registrar	2. Registrar transfer completion notification	The domain name setting authorization is transferred to the gaining registrar.	
17	Registry	Loosing registrar	2. Registrar transfer completion notification		
18					
19	Gaining registrar	Registrant	2. Registrar transfer completion notification	The gaining registrar explains the DNS operator transfer procedures to the registrant.	

III Changing of the DNS setting information (DNS operator transfer)

No	Sender of the information	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
20					
21					
22	Gaining registrar	Registry	3. Loosing DS setting check	**A voluntary action by the gaining registrar**	Because the gaining registrar submits the NS setting change application without checking the DS setting, end users become unable to access the registrant's domain name server. / The gaining registrar submits the L-DS removal application and requests the end users' ISP to clear the registrant's domain name cache.
23	Registry	Gaining registrar	3. Loosing DS setting check		
24					
25					
26					
27					
28	Gaining registrar	Registry	3. Loosing DS removal request		
29	Registry	Gaining registrar	3. Loosing DS removal request		
30	Gaining registrar		Waiting for the TTL expiry of L-DS	**A voluntary action by the gaining registrar**	
31	Gaining registrar	Registry	3. L-NS removal and G-NS setting request		Because the gaining registrar changes the NS setting without waiting for the TTL expiry of L-DS, end users become unable to access the registrant's domain name server. / The gaining registrar submits the application for the registration of G-DS and requests the end users' ISP to clear the registrant's domain name cache.
32	Registry	Gaining registrar	3. L-NS removal and G-NS setting request		
33	Gaining registrar		Waiting for the TTL expiry of L-NS	**A voluntary action by the gaining registrar**	
34	Gaining registrar	Registry	3. G-DS setting application		Because the gaining registrar registers G-DS without waiting for the TTL expiry of L-NS, end users become unable to access the registrant's domain name server. / The gaining registrar requests the end users' ISP to clear the registrant's domain name cache.
35	Registry	Gaining registrar	3. G-DS setting application		
36	Gaining registrar		Waiting for the TTL expiry of L-NS	**A voluntary action by the gaining registrar**	
37	Gaining registrar	Registrant	3. G-DS setting application		Because the registrant's domain name zone has CNAME and the destination of CNAME is an external domain name which is not DNSSEC-compliant, end users complain to the registrant that the registrant's domain name is not DNSSEC-compliant. / The registrant changes CNAME to A/AAAA.
38					

IV Termination of the loosing reseller / registrar / loosing DNS operator

No	Termination of the loosing resell	Receiver of the information	Exchanged information	Supplementary explanation	Troubles/Countermeasures
39	Registrant	Loosing registrar	1. Application for the loosing registrar contract termi	Also serves as the application for the DNS operator termination.	
40	Loosing registrar	Registrant	1. Application for the loosing registrar contract termination		
41					
42					
43	Loosing registrar		Registrant's zone data removal		

Based on the above, the following five scenarios were prepared as detailed scenarios for specific experiments.

1. Successful Condition

   A transfer scenario based on a realistic model

2. Failed Condition 1

   The gaining NS is set up and the loosing NS is removed without the removal of the loosing DS.

3. Failed Condition 2

   The gaining NS is set up and the loosing NS is removed without waiting for the TTL expiry after the removal of the loosing DS.

4. Failed Condition 3

   The gaining DS is set up without the TTL expiry after the setting of the gaining NS and the removal of the loosing NS.

5. Failed Condition 4

   Destination of CNAME, which is included in the DNSSEC signed zone, dose not have a DNSSEC signature and the AD bit is not set at the time of the name (address) resolution. (This is in accordance with the DNS specifications, but it looks like as if the domain names which are supposed to be DNSSEC-compliant are not DNSSEC-compliant from end users' perspective.)

In the experiment, <crisp.jp> was used as a pseudo TLD (registry) and <transfer.crisp.jp>, and a domain name under <crisp.jp> was transferred from the loosing registrar to the gaining registrar. Fig. 3 shows an experimental environment configuration.

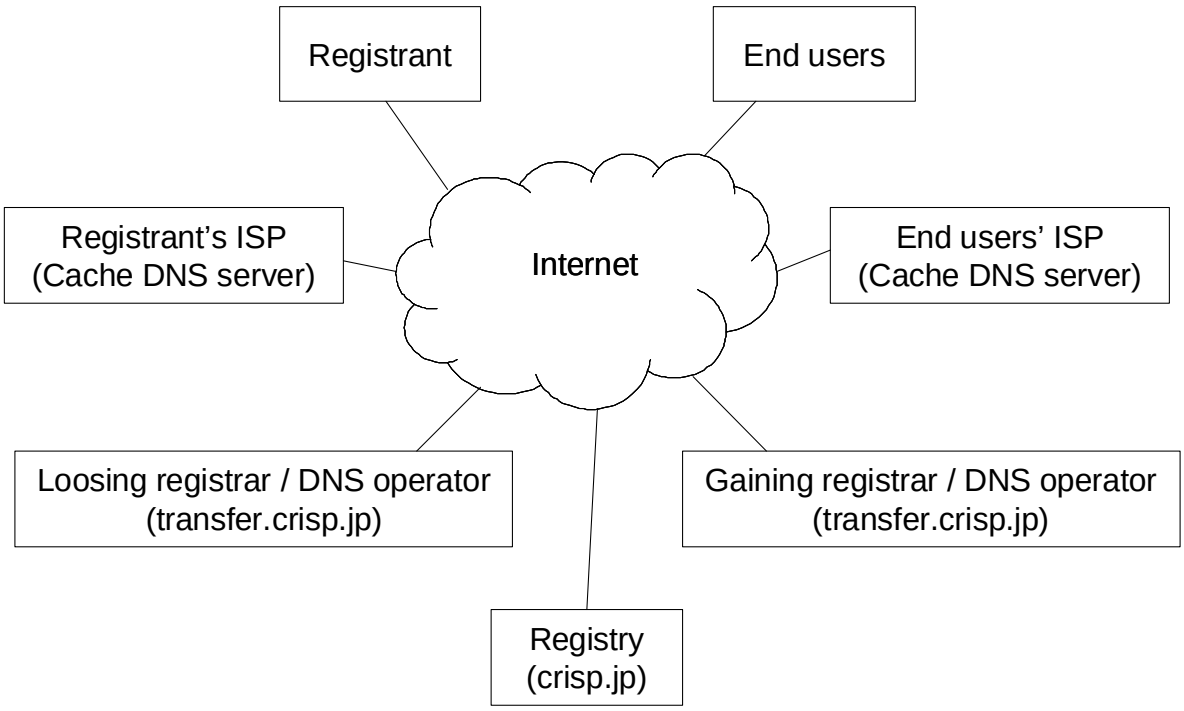


Fig. 3: Experimental Environment Configuration

Charts 5-9 show Detailed Scenarios (Successful Condition and Failed Conditions 1-5). Although the time included in the “Detailed Scenarios” in this chapter indicates scheduled elapse time since the inception of the experiment, the time included in the individual case studies in the “Experimental Results” indicates the actual time of the experiment.

Chart 5: Detailed Scenario (Successful Condition)

I. DNS setting by the gaining DNS operator		
Time	No.	Task
0:00	--	Start of the "Successful Condition"
0:01	1	The registrant requests hosting of <transfer.crisp.jp> to the gaining registrar.
0:02	2	The gaining registrar returns <ack> to the registrant in order to acknowledge the order acceptance. The NS information is returned at the same time.
0:03	3	The registrant requests setting of <transfer.co.jp> to the gaining registrar.
0:04	4	The gaining registrar returns <ack> to the registrant in order to acknowledge the completion of the setting.
0:05	5	The registrant sends an application for the DNSSEC service to the gaining registrar.
0:06	6	The gaining registrar returns <ack> to the registrant in order to acknowledge the completion of signing.

II. Registrar change (registrar transfer)		
Time	No	Task
0:10	7	The registrant sends an application for the .JP registrar transfer of <transfer.crisp.jp> to the gaining registrar.
0:11	9	The gaining registrar sends an application for the .JP registrar transfer of <transfer.crisp.jp> to the registry.
0:12	10	The registry requests the loosing registrar to approve the .JP registrar transfer of <transfer.crisp.jp>.
0:13	12	The loosing registrar requests the registrant to approve the .JP registrar transfer of <transfer.crisp.jp>.
0:14	13	The registrant notifies the loosing registrar of the approval for the .JP registrar transfer of <transfer.crisp.jp>.
0:15	15	The loosing registrar passes <transfer.crisp.jp> to the registry using the transfer function of a simplified registration system and notifies of the approval for the .JP registrar transfer.
0:20	16	The registry passes <transfer.crisp.jp> to the gaining registrar using the transfer function of a simplified registration system and notifies of the completion of the .JP registrar transfer.
0:25	--	The gaining registrar confirms that management authority of <transfer.crisp.jp> has been transferred.
0:25	17	The registry notifies the loosing registrar of the completion of the .JP registrar transfer of <transfer.crisp.jp>.
0:26	19	The gaining registrar notifies the registrant of the completion of the .JP registrar transfer of <transfer.crisp.jp>. The gaining registrar explains about the DNS operator transfer procedures to the registrant at the same time. (Only sends a message about the explanation.)

III. Changing of the DNS setting information (DNS operator transfer)		
Time	No	Task
0:30	22	The gaining registrar verifies L-DS of <transfer.crisp.jp> using a simplified registration system. Make a copy of the L-DS value for the future use (preparation of the failed condition).
0:31	28	The gaining registrar removes L-DS of <transfer.crisp.jp> using a simplified registration system.
0:32	30	The gaining registrar waits for TTL of L-DS (10 minutes).
0:42	31	The gaining registrar removes L-NS of <transfer.crisp.jp> and adds G-NS of <transfer.crisp.jp> using a simplified registration system. Make a copy of the L-NS value for the future use (preparation of the failed condition).
0:43	33	The gaining registrar waits for TTL of L-NS (5 minutes).
0:48	34	The gaining registrar adds G-DS of <transfer.crisp.jp> using a simplified registration system.
0:49	36	The gaining registrar waits for TTL of G-NS (5 minutes).
0:54	37	The gaining registrar notifies the registrant of the completio of the .JP registrar and DNS operator transfers.

IV. Termination of the loosing reseller / registrar / loosing DNS operator		
Time	No	Task
0:55	39	The registrant sends an application for the hosting and registrar contract termination to the loosing registrar.
0:56	40	The loosing registrar returns <ack> to the registrant in order to acknowledge the contract termination
0:57	--	End of the "Successful Condition"

* (No.) corresponds with No. in Chart 3. (--) indicates that the item does not match.

Chart 6: Detailed Scenario (Failed Condition 1)

III. Changing of the DNS setting information (DNS operator transfer)		
Time	No.	Task
0:00	--	Start of the "Failed Condition 1"
0:01	--	Name resolution of <www.transfer.crisp.jp> by the end user Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP
0:02	31	The gaining registrar removes L-NS of <transfer.crisp.jp> and adds G-NS of <transfer.crisp.jp> using a simplified registration system.
0:03	--	All wait for TTL of L-NS (5 minutes).
0:08	--	The end user verifies the failure in name resolution of <transfer.crisp.jp>. (Cache = L-DS, G-NS.) Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP <= SERVFAIL Ex. dig +dnssec +cd www.transfer.crisp.jp @ cache DNS server of end users' ISP <= NOERROR http://dnsviz.net/ <= Check the link status of <transfer.crisp.jp>
0:09	--	The end user notifies the registrant that the name cannot be looked up.
0:10	--	The registrant notifies the gaining registrar that the name cannot be looked up..
0:11	28 34	The gaining registrar removes L-DS of <transfer.crisp.jp> using a simplified registration system. The gaining registrar adds G-DS of <transfer.crisp.jp> using a simplified registration system at the same time.
0:12	--	The gaining registrar requests the registrant's ISP and end users' ISP to clear cache of <transfer.crisp.jp>.
0:13	--	The registrant's ISP and end users' ISP clear cache of <transfer.crisp.jp>. Ex. rndc flushname transfer.crisp.jp
0:14	--	The end user verifies the success in name resolution of <transfer.crisp.jp>. Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP <= NOERROR
0:15	--	End of the "Failed Condition 1"

* (No.) corresponds with No. in Chart 3. (--) indicates that the item does not match.

Chart 7: Detailed Scenario (Failed Condition 2)

III. Changing of the DNS setting information (DNS operator transfer)		
Time	No.	Task
0:00	--	Start of the "Failed Condition 2"
0:01	--	Name resolution of <www.transfer.crisp.jp> by the end user Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP
0:02	28	The gaining registrar removes L-DS of <transfer.crisp.jp> using a simplified registration system. The gaining registrar removes L-NS of <transfer.crisp.jp> and adds G-NS of <transfer.crisp.jp> using a simplified registration system at the same time.
0:03	--	All wait for TTL of L-NS (5 minutes).
0:08	--	The end user verifies the failure in name resolution of <transfer.crisp.jp>. (Cache = L-DS, G-NS.) Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP <= SERVFAIL Ex. dig +dnssec +cd www.transfer.crisp.jp @ cache DNS server of end users' ISP <= NOERROR http://dnsviz.net/ <= Check the link status of <transfer.crisp.jp>
0:09	--	The end user notifies the registrant that the name cannot be looked up.
0:10	--	The registrant notifies the gaining registrar that the name cannot be looked up.
0:11	34	The gaining registrar adds G-DS of <transfer.crisp.jp> using a simplified registration system.
0:12	--	The gaining registrar requests the registrant's ISP and end users' ISP to clear cache of <transfer.crisp.jp>.
0:13	--	The registrant's ISP and end users' ISP clear cache of <transfer.crisp.jp>. Ex. rndc flushname transfer.crisp.jp
0:14	--	The end user verifies the success in name resolution of <transfer.crisp.jp>. Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP <= NOERROR
0:15	--	End of the "Failed Condition 2"

* (No.) corresponds with No. in Chart 3. (--) indicates that the item does not match.

Chart 8: Detailed Scenario (Failed Condition 3)

III. Changing of the DNS setting information (DNS operator transfer)		
Time	No.	Task
0:00	--	Start of the "Failed Condition 3"
0:01	31	The gaining registrar removes L-NS of <transfer.crisp.jp> and adds G-NS of <transfer.crisp.jp> using a simplified registration system.
0:02	--	Name resolution of <www.transfer.crisp.jp> by the registrant's ISP Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP
0:03	34	The gaining registrar adds G-DS of <transfer.crisp.jp> using a simplified registration system.
0:04	--	The registrant's ISP verifies the failure in name resolution of <transfer.crisp.jp>. (Cache = L-DS, G-NS.) Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP <= SERVFAIL Ex. dig +dnssec +cd www.transfer.crisp.jp @ cache DNS server of end users' ISP <= NOERROR http://dnsviz.net/ <= Check the link status of <transfer.crisp.jp>
0:05	--	The registrant's ISP notifies the registrant that the name cannot be looked up.
0:06	--	The registrant notifies the gaining registrar that the name cannot be looked up.
0:07	--	The gaining registrar requests the registrant's ISP and end users' ISP to clear cache of <transfer.crisp.jp>.
0:08	--	The registrant's ISP and end users' ISP clear cache of <transfer.crisp.jp>. Ex. rndc flushname transfer.crisp.jp
0:09	--	The registrant's ISP verifies the success in name resolution of <transfer.crisp.jp>. Ex. dig +dnssec www.transfer.crisp.jp @ cache DNS server of end users' ISP <= NOERROR
0:10	--	End of the "Failed Condition 3"

* (No.) corresponds with No. in Chart 3. (--) indicates that the item does not match.

Chart 9: Detailed Scenario (Failed Condition 4)

III. Changing of the DNS setting information (DNS operator transfer)		
Time	No	Task
0:00	--	Start of the "Failed Condition 4"
0:01	--	Name resolution of <www.transfer.crisp.jp> by the end user Ex. dig +dnssec <alias.transfer.crisp.jp> @ cache DNS server of end users' ISP <= NOERROR, AD bit is not set.
0:02	--	The end user notifies the registrant that <alias.transfer.crisp.jp> is not protected by DNSSEC.
0:03	--	The registrant requests the gaining registrar to change CNAME of <alias.transfer.crisp.jp> to A/AAAA.
0:04	--	The gaining registrar changes <alias.transfer.crisp.jp>.
0:09	--	The end user verifies that <alias.transfer.crisp.jp> is protected by DNSSEC. Ex. dig +dnssec <alias.transfer.crisp.jp> @ cache DNS server of end users' ISP <= NOERROR, AD bit is set.
0:10	--	End of the "Failed Condition 4"

* (No.) corresponds with No. in Chart 3. (--) indicates that the item does not match.

Experimental Results

In this experiment, DS-TTL was set to 600 seconds and NS-TTL was set to 300 seconds (600 seconds for the TTL in the parent zone) in consideration of efficiency. The following results are based on the case studies in the experimental environment.

■ Case Study 1: Registrant

- Experimental Environment

- Summary of Experimental Results

  The experiments were conducted in accordance with the “Detailed Scenario.”

- Detailed Experimental Results

  <Successful Condition>
  - DNS delegation was not disconnected.
  - The disconnection time of the DNSSEC delegation was as predicted.
  - The name resolution was successful.

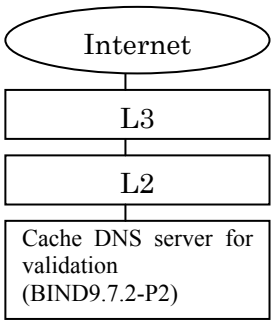
  <Failed Condition>
  - DNSSEC inconsistency (name resolution failure) was recovered.
  - The DNSSEC validation succeeded by changing CNAME of <alias.transfer.crisp.jp> to A/AAAA.

- Obtained Findings

  We found it difficult to segregate responsibilities for the transfer procedures between the end users and business operators.

■ Case Study 2: Registrant's ISP

・ Experimental Environment



・ Summary of Experimental Results

The experiment was conducted in accordance with the Detailed Scenario for the cache DNS server of the registrant's ISP (the reporter was in charge of this.) However, when we checked the logs captured at the 30-second intervals, there were operational errors in cache clearance at the start of each scenario. (It is likely that cache was cleared for the cache DNS sever which was not included in the experiment.)

・ Detailed Experimental Results

(i) Successful Condition

Disconnection of the DNS delegation: None

Disconnection time of the DNSSEC delegation: As predicted

Name resolution: Successful

(ii) Failed Condition 1

Recovery from the inconsistency due to cache clearance: Successful

(iii) Failed Condition 2

Recovery from the inconsistency due to cache clearance: Successful

(iv) Failed Condition 3

Recovery from the inconsistency due to cache clearance: Successful

(v) Failed Condition 4

N/A

・ Obtained Findings

As predicted as a registrant's ISP, it was verified that the inconsistency was recovered by clearing cache of the cache DNS server.

It was also verified that the SERVFAIL status was reflected at the TTL expiry although cache was not cleared at the start of each scenario.

■ Case Study 3: Loosing registrar

・ Experimental Environment

OS: FreeBSD 7.1 x86 / Guest OS on KVM
Authoritative DNS server: ANS 5.1 for FreeBSD

・ Summary of Experimental Results

The experiment was conducted smoothly in accordance with the “Detailed Scenario.”

・ Detailed Experimental Results

<Successful Condition> Registrar transfer: The experiment was completed in accordance with the scenario.
<Successful Condition> DNS operator transfer: The experiment was completed in accordance with the scenario.
<Failed Condition>No events which would require countermeasures by the loosing registrar occurred.

・ Obtained Findings

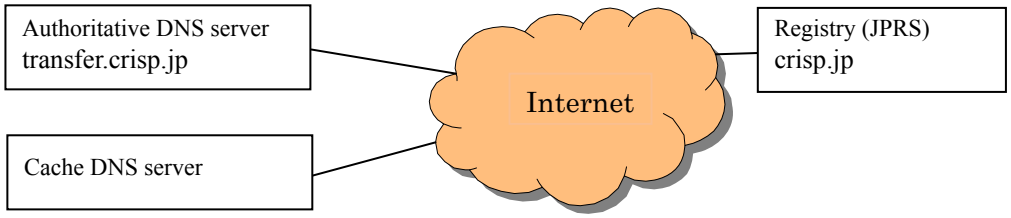
We believe that it was verified that there were no procedures to be changed by the loosing registrar.
We felt that the gaining registrar would have more complicated tasks and countermeasures for the failed conditions.

This experiment was conducted on the assumption that the DNS operator and the registrar were the same business operator. However, in reality, they could be different business operators and the procedures are expected to be more complicated. Therefore, we think that it is necessary to prepare guidelines for countermeasures for failed conditions.

■ Case Study 4: Gaining registrar

- Experimental Environment

An authoritative DNS server (DNSSEC-compliant) and a cache DNS server were set up and a transfer test domain (transfer.crisp.jp) zone was registered within the authoritative DNS server.



- Summary of Experimental Results

The domain name and DNS operator transfer tests were completed without any issues both for the successful and failed conditions in accordance with the Detailed Scenario of the Registrar Transfer Experiment by JPRS.

- Detailed Experimental Results

<Successful Condition>

Registrar transfer: No error

DNS operator transfer: No error

<Failed Condition>

Failed Condition 1 L-DS + G-NS = inconsistency: No error

Failed Condition 2 No DS + G-NS = inconsistency: No error

Failed Condition 3 G-DS + L-NS = inconsistency: No error

Failed Condition 4 Error (Destination of CNAME was not DNSSEC-compliant): No error

- Obtained Findings

- There were incidences in which new NS did not reach the cache DNS server sufficiently even after waiting for the TTL expiry after the change of NS.
- We found it difficult to judge how much of the procedures in this experiment we should ask end users to do in the actual transfer and how much detail we should explain.

■ Case Study 5: Registry

- Experimental Environment

We prepared a terminal for the registry task (to access the system to change the zone management authority in the domain for the experiment) and participated in the experiment via the Internet.
Furthermore, a cache DNS server which can resolve the domain name for the experiment was prepared in order to check the DNS delegation status and the continuity of name resolution and the data was recoded by sending queries at set intervals.

- Summary of Experimental Results

It was verified that the registrar can be transferred without any issues if we follow the scenario of the successful condition Furthermore, as predicted in the failed condition, it was verified that a failure in name resolution (SERVFAIL) occurs during the DNSSEC validation, if there is a twist between cached NS and DS in the cache DNS server (one is loosing and the other is gaining).

- Detailed Experimental Results

With regard to the successful condition, it was verified that the registrar can be transferred in accordance with the scenario without any issues.
With regard to the failed condition, we had no issues as there was no task for the registry. However, despite the assumption in the Failed Condition Scenario 3," the failure in name resolution (SERVFAIL) was not recorded in the data for which the continuity of name resolution was recorded by sending queries at set intervals. We think that it was because the experiment did not proceed in accordance with the scenario and there was no twist between NS and DS.

- Obtained Findings

Although we anticipated troubles for the failed condition in consideration of the cache status of TTL of NS and DS, we should have considered a possibility that other DNSSEC-related records such as DNSKEY and RRSIG were cached at different times. Depending on the cache DNS server implementation, it is possible to look up NS and DS again after the TTL expiry of such records. (Such behaviors can be seen with BIND and Unbound.) It is difficult to replicate troubles according to a theory in a small experimental zone with a short TTL. Based on the above, we think that we should keep the TTL value of the DNSSEC-related records below the TTL value of NS.

■ Case Study 6: End User

・ Experimental Environment

Used device: A NEC server
Network: Internet connection 100M/FULL
Used DNS: BIND-9.7.2-P2
Experimental Environment: The following commands were sent at the 30-second intervals from the aforementioned server to the two ISP cache DNS servers.

dig +dnssec www.transfer.crisp.jp @ cache DNS server
dig +dnssec alias.transfer.crisp.jp @ cache DNS server
dig +dnssec +cd www.transfer.crisp.jp @ cache DNS server
dig +dnssec +cd alias.transfer.crisp.jp @ cache DNS server

・ Summary of Experimental Results

Successful Condition:
In one cache DNS server, the registrar transfer was conducted without any issues. However, we could not obtain results in accordance with the scenario in the other cache DNS server because the validation continued to indicate OK even after L-DS was removed and G-NS was added.

Failed Condition 1:
In one cache DNS server, we could obtain results in accordance with the scenario. However, we could not obtain results in accordance with the scenario in the other cache DNS server because cache clearance after SERVFAIL was incomplete.

Failed Condition 2:
Depending on the TTL of NS, response for each cache DNS server varied.
In one cache DNS server, we could obtain results in accordance with the scenario. However, we could not obtain results in accordance with the scenario in the other cache DNS server because of an unpredicted SERVFAIL.

Failed Condition 3:
Failed condition continued since the start of the experiment and we could not obtain results in accordance with the scenario for both cache DNS servers.

Failed Condition 4:

Results in accordance with the scenario

- Detailed Experimental Results

Successful Condition:

・The registrar transfer was completed in accordance with the scenario for the cache DNS server 2.

・Although there was a failure in <+dnssec alias> of the cache DNS server 1, we decided not to take this into consideration as it was verified to be a FW issue.

・In the case of a zone whose DNSSEC validation was OK, we could see differences in response for each DNS server. While the <+cd> response flag from the loosing DNS was <qr rd ra cd> server, the <+cd> response flag from the gaining DNS server was <qr rd ra ad cd>.

・There was an event in which the DNSSEC validation remained OK even after the TTL expiry of DS. Furthermore, there was an event in which there was no change in RRSIG and the DNSSEC validation remained OK even after NS was switched over. Although TTL was cut off a few times after that, there was no change in RRSIG. At 13:51 when TTL was expired, RRSIG was finally changed to the gaining side. However, it seemed that DS cache was still there and the result showed SERVFAIL.

・ It was verified that the TTL of A decreased but the TTL of RRSIG did not decrease as a result of a <+cd> query after SERVFAIL.

・See the following page for detailed chorological chart.

Successful Condition Scenario		Cache DNS server 1				Cache DNS server 2			
Time	Scenario	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
13:00	Start of the experiment	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra ad Validation OK Resolution OK	qa rd ra Validation Error Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra cd No validation Resolution OK
13:09	Completion of the DNSSEC zone setting for the gaining DNS								
13:20	Registrar transfer completion								
13:22	L-DS removal by the gaining registrar								
13:32	TTL expiry of DS (10 minutes)								
13:37	NS change by the gaining registrar								
13:39	-					NS is switched. qr rd ra Validation Error Resolution OK	NS is switched.	NS is switched.	NS is switched.
13:42	TTL expiry of L-NS (5 minutes)								
13:45	-	NS is switched.	NS is switched.	NS is switched. qr rd ra ad cd No validation Resolution OK	NS is switched.				
13:47	G-DS registration								
13:48	-		qr rd ra SERVFAIL						
13:50	-					qr rd ra ad Validation OK Resolution OK			
13:51	-	qr rd ra SERVFAIL		qr rd ra cd No validation Resolution OK					
13:52	TTL expiry of G-NS (5 minutes)								
13:54	-							qr rd ra cd No validation Resolution OK	
13:55	DNS transfer completion	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK					
13:58	Removal of L-DNS zone End of the experiment								

Failed Condition 1:

・The experiment was completed in accordance with the scenario for the cache DNS server 2.

・It was as predicted that NS was switched over and the status: SERVFAIL was returned for the cache DNS server 1. However, it seemed that DS cache was not cleared at 14:19 when the cache was cleared and the status: SERVFAIL continued. (TTL of RRSIG remained stopped.)

・The event improved when cache was cleared at 14:23. The validation was successful because it was after the registration of G-DS.

・See the following page for detailed chorological chart.

Failed Condition 1 (No.22) Scenario		Cache DNS server 1				Cache DNS server 2			
Time	Scenario	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
14:07	Start of the experiment	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra ad Validation OK Resolution OK	qa rd ra Validation Error Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra cd No validation Resolution OK
14:07	Assuming that the registrar transfer has been completed, the gaining registrar removes L-DS.								
14:10	-							qr rd ra ad cd No validation Resolution OK	
14:14	-					NS is switched. qr rd ra SERVFAIL	NS is switched. qr rd ra SERVFAIL	NS is switched. qr rd ra cd SERVFAIL	NS is switched. qr rd ra cd SERVFAIL
14:15	TTL expiry of NS (5 minutes)							qr rd ra cd No validation Resolution OK	qr rd ra cd No validation Resolution OK
14:16	-	NS is switched. qr rd ra SERVFAIL	NS is switched. qr rd ra SERVFAIL	NS is switched.	NS is switched.				
14:18	Removal of L-DS								
14:19	Cache clearance by each cache server					qa rd ra Validation Error Resolution OK	qa rd ra Validation Error Resolution OK		
14:20	-								
14:23	Cache clearance by each cache server which registers G-DS	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK		qr rd ra ad Validation OK Resolution OK		qr rd ra ad cd No validation Resolution OK	
14:27	End of the experiment								

Failed Condition 2:

・Although DS-TTL was set to 10 minutes and NS-TTL was set to 5 minutes, NS-TTL reflected the TTL value of the parent server. In this case, the TTL value of DS and NS was both 10 minutes because the TTL value of <crisp.jp> was 10 minutes. Therefore, in cases where DS-TTL expired conveniently before NS-TTL expired, we could not obtain results in accordance with the scenario because SERVFAIL did not occur unlike the cache DNS server 2.

・It was verified that SERVFAIL occurred as predicted for the cache DNS server 1.
When we checked <+cd > at the same time, we found that the TTL value of not only RRSIG but also A did not decrease. (NS-TTL decreased.)

・Immediately prior to the cache clearance of the cache DNS sever 2, an unintended SERVFAIL occurred suddenly. Although the validation became possible by clearing cache right after that, it's not known exactly why SERVAIL occurred.

・See the following page for detailed chorological chart.

Failed Condition 2 (No.30) Scenario		Cache DNS server 1				Cache DNS server 2			
Time	Scenario	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	(Zone generation)	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
14:30	Start of the experiment	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra ad Validation OK Resolution OK	qa rd ra Validation Error Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra cd No validation Resolution OK
14:34	Assuming that the registrar transfer has been completed, the gaining registrar removes L-DS and changes NS.								
14:39	TTL expiry of NS (5 minutes)								
14:40	-					NS is switched. qa rd ra Validation Error Resolution OK	NS is switched.	NS is switched.	NS is switched.
14:41	-	NS is switched. qr rd ra SERVFAIL	NS is switched. qr rd ra SERVFAIL	NS is switched.	NS is switched.				
14:44	DS registration								
14:45	-					qr rd ra SERVFAIL	qr rd ra SERVFAIL		
14:46	Cache clearance by each cache server	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK		qa rd ra Validation Error Resolution OK	qa rd ra Validation Error Resolution OK	qr rd ra ad cd No validation Resolution OK	
14:47	End of the experiment								

Failed Condition 3:

・Because the both cache DNS servers were not on a normal condition since the start of the experiment, results turned out to be completely different from the scenario.

・This is assumed to be due to the fact that the cache DNS server 1 failed in cache clearance at the start of the experiment and the transmission from the Failed Condition 2 to the Failed Condition 3 was not conducted smoothly.

・There is a possibility that a chain of trust was not established for the cache DNS server 2 from the beginning because L-DS had not been registered at the start of the experiment.

・See the following page for detailed chorological chart.

Failed Condition 3 (No.33) Scenario		Cache DNS server 1				Cache DNS server 2			
Time	Scenario	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	(Zone generation)	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
14:52	Start of the experiment	qr rd ra SERVFAIL	qr rd ra SERVFAIL	qr rd ra ad cd No validation Resolution OK	qr rd ra cd No validation Resolution OK	qa rd ra Validation Error Resolution OK	qa rd ra Validation Error Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra cd No validation Resolution OK
14:53	Assuming that the registrar transfer has been completed, the gaining registrar changes NS.								
14:58	TTL expiry of NS (5 minutes)								
14:59	G-DS registration								
15:02	-	NS is switched. qr rd ra ad Validation OK Resolution OK	NS is switched. connection timed out	NS is switched. qr rd ra ad cd No validation Resolution OK	NS is switched.	NS is switched. qr rd ra ad Validation OK Resolution OK	NS is switched.	NS is switched. qr rd ra ad cd No validation Resolution OK	NS is switched.
15:06	End of the experiment								

Failed Condition 4:

・Because another domain was designated by CNAME, the validation for <alias.transfer.crisp.jp> failed. The validation became possible after changing to the A/AAAA record.

・The validation was completed without any issues.

・See the following page for detailed chorological chart.

Failed Condition 4 (No.36) Scenario		Cache DNS server 1				Cache DNS server 2			
Time	Scenario	+dnssec www	+dnssec alias	+dnssec +cd www	+dnssec +cd alias	(Zone generation)	+dnssec alias	+dnssec +cd www	+dnssec +cd alias
15:07	Start the experiment on the assumption that the registrar and DNS operator transfers have been	qr rd ra ad Validation OK Resolution OK	connection timed out	qr rd ra ad cd No validation Resolution OK	qr rd ra cd No validation Resolution OK	qr rd ra ad Validation OK Resolution OK	qa rd ra Validation Error Resolution OK	qr rd ra ad cd No validation Resolution OK	qr rd ra cd No validation Resolution OK
15:14	Changed alias from CNAME to A/AAAA.								
15:17	-		qr rd ra ad Validation OK Resolution OK		qr rd ra ad cd No validation Resolution OK		qr rd ra ad Validation OK Resolution OK		qr rd ra ad cd No validation Resolution OK
15:18	End of the experiment								

・ Obtained Findings

Successful Condition:

・As some of the procedures for the transfer were not conducted in accordance with the scenario, we think that it is necessary to list up preconditions for the DNS server and the server setting if these procedures are used in the future.
We need to bear in mind that some DNS servers could experience SERVFAIL using these procedures.

・It was verified that the TTL of RRSIG without validation did not decrease as a result of a <+cd> lookup after SERVFAIL.

Failed Condition 1:

・We verified a condition in which cache clearance was not conducted successfully. It is necessary to verify the behavior as we think that cache clearance by ISPs will be necessary for some situations with DNSSEC.

Failed Condition 2:

・TTL is extremely important for DNSSEC. TTL errors will significantly increase a risk of SERVFAIL. It is important to understand exactly which TTL the servers are linked to.

・As we experienced an unexpected SERVFAIL suddenly, the registrar transfer always entails SERVFAIL risks. We need to discuss whether we should assure to our clients that SERVFAIL will not happen.

Failed Condition 3:

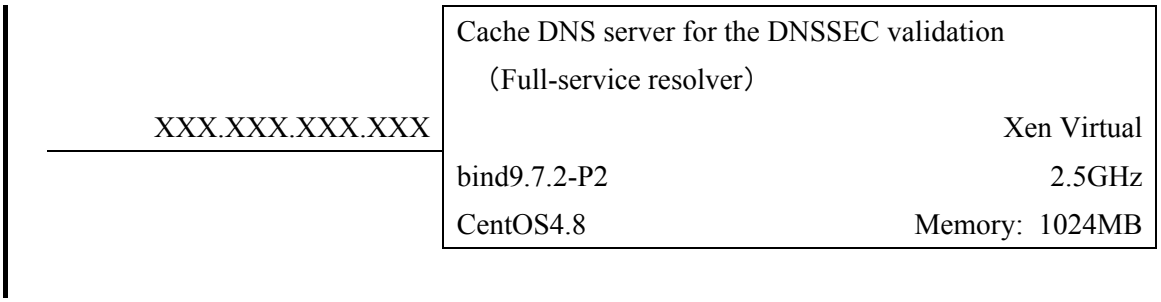
・None.

Failed Condition 4:

・Validation was not possible with CNAME. It was verified that validation become possible by changing to the A/AAAA record.

■ Case Study 7: End Users' ISP

・ Experimental Environment



・ Summary of Experimental Results

Our experiment for the Successful Condition was completed in accordance with our schedule without any issues.

With regard to the Failed Conditions, although we could not create failed conditions for some tests, others went as scheduled.
Name resolution was recovered by clearing cache.

・ Detailed Experimental Results

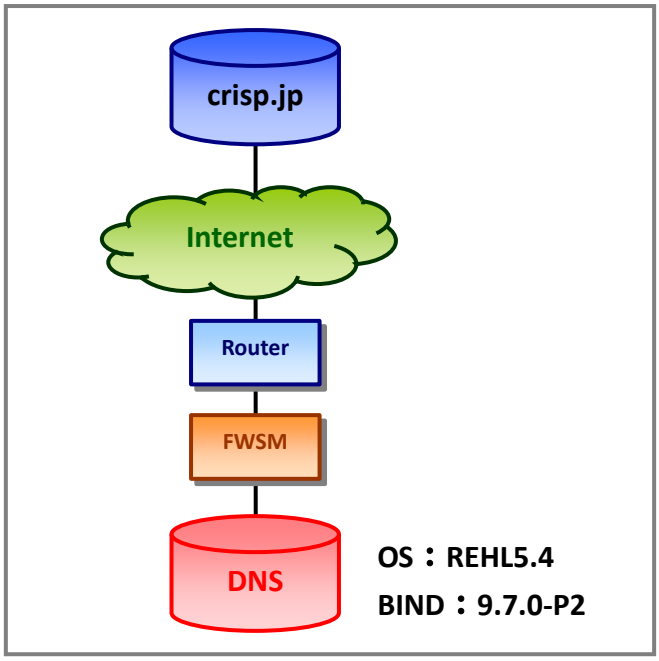
Successful Condition: The DNS delegation was maintained successfully and the disconnection time of the DNSSEC delegation was as predicted. The transfer was completed successfully by switching after the TTL expiry.
Failed Condition: Although there was a case in which we could not replicate a failed condition, other tests went in accordance with the scenario and name resolution was recovered by clearing cache.

・ Obtained Findings

Complexity of DNS increased due to added records by DNSSEC and the TTL of cache. Although in this experiment, we recovered name resolution by clearing cache, it is almost impossible to do this in reality and an error is likely to result in a prolonged trouble. We were reminded that the registrar transfer should be conducted carefully.

■ Case Study 8: End Users' ISP

・ Experimental Environment



・ Summary of Experimental Results

- <Connection timed out> was returned as a result of a <+dnssec alias> query from the beginning and we could not obtain test results as expected. It turned out that it was a FW issue as a result of an error in verification prior to the test.
  No analysis report on alias.
- In <+dnssec www>, cache behavior in line with TTL was unstable and there was a general tendency that NS-TTL of 10 minutes was maintained.
- The status immediately after the cache clearance was unstable as SERVFAIL was returned for www even after cache was cleared. The cause behind this is unknown.

・ Detailed Experimental Results

（1） Verification of the Successful Condition

End Users' ISP made an analysis based on the results of the following commands which were sent at the 30-second intervals. There was no change in RRSIG after NS was switched over and the validation remained OK. We need to reconsider the TTL of DS, NS and RRSIG.

```
# dig +dnssec www.transfer.crisp.jp a @ cache DNS server
# dig +dnssec ns.transfer.crisp.jp a @ cache DNS server
# dig +dnssec transfer.crisp.jp ds @ cache DNS server

**********
13: 32   TTL expiry of DS (10 minutes)   =>     Name resolution OK by caching
**********
# dig +dnssec www.transfer.crisp.jp a @127.1
www.transfer.crisp.jp.   150      IN       A        203.178.129.44
www.transfer.crisp.jp.   150      IN       RRSIG    A 8 4 300 20101109042353

# dig +dnssec transfer.crisp.jp ds @127.1
crisp.jp.    180   IN   SOA   ns.crisp.jp. root.crisp.jp. 1288931410 3600 900 604800
crisp.jp.                180      IN       RRSIG    SOA 8 2 600 20101205033010
transfer.crisp.jp.       180      IN       RRSIG    NSEC 8 3 300 20101205033010
transfer.crisp.jp.       180      IN       NSEC     unsecure.crisp.jp. NS RRSIG NSEC

# dig +dnssec ns.transfer.crisp.jp a @127.1
ns.transfer.crisp.jp.    210      IN       A        59.106.114.121
ns.transfer.crisp.jp.    210      IN       RRSIG    A 8 4 300 20101109042353

**********
13: 42   TTL expiry of L-NS (5 minutes)   =>   No change in status
**********
# dig +dnssec www.transfer.crisp.jp a @127.1
www.transfer.crisp.jp.   150      IN       A        203.178.129.44
www.transfer.crisp.jp.   150      IN       RRSIG    A 8 4 300 20101109042353

# dig +dnssec transfer.crisp.jp ds @127.1
crisp.jp.   210   IN   SOA      ns.crisp.jp. root.crisp.jp. 1288932003 3600 900 604800
crisp.jp.                210      IN       RRSIG    SOA 8 2 600 20101205034003
transfer.crisp.jp.       210      IN       RRSIG    NSEC 8 3 300 20101205034003
transfer.crisp.jp.       210      IN       NSEC     unsecure.crisp.jp. NS RRSIG NSEC

# dig +dnssec ns.transfer.crisp.jp a @127.1
ns.transfer.crisp.jp.    210      IN       A        59.106.114.121
```

ns.transfer.crisp.jp. 210 IN RRSIG A 8 4 300 20101109042353

****

13: 45 NS change

****

****

13: 50 SERVFAIL as a result of the cache expiry

****

dig +dnssec www.transfer.crisp.jp a @127.1

No ANSWER SECTION

dig +dnssec ns.transfer.crisp.jp a @127.1

No ANSWER SECTION

dig +dnssec transfer.crisp.jp ds @127.1

transfer.crisp.jp. 299 IN DS 36886 8 2

transfer.crisp.jp. 299 IN DS 36886 8 1

transfer.crisp.jp. 299 IN RRSIG DS 8 3 600 20101205035027

****

13: 54 Approx. 10 minutes after the NS change => name resolution OK

****

dig +dnssec www.transfer.crisp.jp a @127.1

www.transfer.crisp.jp. 295 IN A 203.178.129.44

www.transfer.crisp.jp. 295 IN RRSIG A 8 4 300 20101204033032

dig +dnssec ns.transfer.crisp.jp a @127.1

ns.transfer.crisp.jp. 270 IN A 202.212.225.172

ns.transfer.crisp.jp. 270 IN RRSIG A 8 4 300 20101204033032

dig +dnssec transfer.crisp.jp ds @127.1

transfer.crisp.jp. 29 IN DS 36886 8 1

transfer.crisp.jp. 29 IN DS 36886 8 2

transfer.crisp.jp. 29 IN RRSIG DS 8 3 600 20101205035027

（2） Failed Condition Test 1（No22）

It was verified that cache was not cleared properly at the time of cache clearance.

The test conducted from the users' side went OK after the second cache clearance.

（3） Failed Condition Test 2（No30）

The cause of the SERVFAIL event after the NS change is unknown.

（4） Failed Condition Test 3（No33）

SERVFAIL at the start of the experiment was a result of a failure in cache clearance.

After the NS switch over, cache was cleared and name resolution was conducted without any issues.

・ Obtained Findings

Because cache was cleared on a timely basis along with the transfer in this experiment, we could forecast how long it would take before name resolution became possible. However, in the actual service operation, we cannot conduct cache clearance manually on a timely basis. Therefore, we thought it is necessary to set the TTL value of each DNSSEC record in a careful manner.

In addition, it will be necessary to conduct ongoing tests on the retention of the DNSSEC cache information and understand how it works.

FAQ for the Discussion of Service Combination

Background of FAQ Preparation

It is important for business operators which have not started DNSSEC services to anticipate questions and troubles which may be raised or reported by customers and end users with regard to the provision of DNSSEC services. Such anticipated questions and answers can be used as verification points when discussing and designing new operation and service combination resulting from the deployment of DNSSEC services. We think that preparing a list of anticipated questions by the organizations which participated in the DNSSEC technology experiment based on obtained findings through the experiment will be useful in designing services provided by DNSSEC service operators such as ISPs and .JP registrars.

In this experiment, anticipated questions selected by each organization which participated in the DNSSEC Technology Experiment were collated and classified into the following eight categories based on the content.

1. Questions on Advantages and Disadvantages of DNSSEC
2. Questions on Fees
3. Questions on Services
4. Questions on the Registrant
5. Technical Questions
6. Questions on Operations
7. Questions on Industry Trend
8. General Questions

FAQ was created after classifying each question into two categories: questions for which common answers are anticipated for all business operators (Common Questions) and questions for which different answers are anticipated for each business operator (Specific Questions).

FAQ: Common Questions

The “FAQ: Common Questions” summarizes questions (Q) for which common answers (A) are anticipated for all business operators. Answers (A) were prepared by the experiment participants.

▼Questions on Advantages and Disadvantages of DNSSEC

Q Is the deployment of DNSSEC mandatory? Is DNSSEC really necessary? What will happen if we don’t introduce DNSSEC?

A It is not mandatory, but if you don’t introduce DNSSEC, you cannot have improved security.

Q What are advantages of the deployment of DNSSEC? What will improve when DNSSEC is deployed? How much Internet security improvement will be secured by the deployment of DNSSEC?

A There was no way to verify whether DNS data was accurate or not in the past. However, by using DNSSEC, you will be able to verify accuracy of received DNS data and protect your data from DNS cache poisoning attacks.

Q What are disadvantages of the deployment of DNSSEC? What are challenges in the deployment of DNSSEC?

A On the authoritative DNS server side, management cost for keys and signatures required for the DNSSEC processing will increase. On the cache DNS server side, there will be an increase in cost of the DNSSEC validation. In either case, increases in operational cost can be regarded as disadvantages.

▼Questions on Services

Q What will happen if keys are leaked?

A Those who obtain leaked keys will be able to fabricate false DNS data and the DNS data will not be protected by DNSSEC. Therefore, it is necessary to roll over keys without delay in the case of key leakage.

Q What will happen when a domain name is transferred?

A Please see the “DNSSEC Technology Experiment Report: Operational Design” by JPRS and the “Registrar Transfer Guidelines” by DNSSEC Japan.

▼Questions on the Registrant

Q How can we verify that DNSSEC works normally?

A You can verify that DNSSEC works normally if <ad> is shown for the flags when a query (dig +dnssec domain name A @ cache DNS server) is sent using a dig command to the cache DNS server for which DNSSEC has been set.

Q Is security assured if the authoritative DNS server of my domain name is DNSSEC-compliant?

A No. In DNSSEC, signed data is sent from the authoritative DNS server and the signature is validated by the cache DNS server. Therefore, it is necessary that the cache DNS server is DNSSEC-compliant.

▼Technical Questions

Q Can you explain how DNS works in detail?

A DNS is a "name resolution" mechanism which associates domain names which are parts of Internet addresses with IP addresses. For more detail, see the JPRS Topics & Column "Mechanism and Principles of DNS: DNS as a Backbone of the Internet" <http://jpinfo.jp/topics-column/010.pdf>.

Q Can you explain how DNSSEC works in detail?

A DNSSEC is a security extension specification which has been implemented in order to address fundamental vulnerability of DNS specifications. For more detail, see the DNSSEC Series (No.13 <http://jpinfo.jp/topics-column/013.pdf>, No.14 <http://jpinfo.jp/topics-column/014.pdf>, No.15 <http://jpinfo.jp/topics-column/015.pdf>, No.16 <http://jpinfo.jp/topics-column/016.pdf>) of the JPRS Topics & Column <http: //jpinfo.jp/topics-column/>.

Q What services will DNSSEC cover? (Authoritative, cache, secondary, reverse lookup)

A Everything which uses the DNS protocol will be covered.

Q How can the security of "last one mile" be assured?

A There are several plans and two methods: end node validation and security enhancement of communication channel.

Plan 1: End node validation

Plan 2: Security enhancement of communication channel using IPsec (Implementation on Windows7)

Plan 3: Security enhancement of communication channel using TSIG (Key exchange with users in advance)

Plan 4: Regard it secure as there are no third parties between ISPs and end users.

Q Can we identify if the accessed domain is DNSSEC-compliant or not even without a prior verification?

A 1. The DNSSEC validation can be verified for the cache DNS server with Trust Anchors.

2. With regard to the stub resolver for which the cache DNS serve conducts the DNSSEC validation, it can be verified whether the DNSSEC validation was successful or not by checking the AD bit after sending a query with the DO bit set to 1.

Q How can a client check whether DNSSEC is valid or not?

A Currently, there are not many client applications for which we can check whether DNSSEC is valid or not.

For example, FireFox has an add-on for the DNSSEC validation. This add-on allows you to check whether currently displayed websites are DNSSEC-compliant and whether a client uses DNSSEC-compliant DNS server.

DNSSEC Validator
http: //www.dnssec-validator.cz/
CZ.NIC Labs

Furthermore, some websites provide an easy way for you to check whether the cache DNS server currently in use is DNSSEC-compliant or not.

http: //test.dnssec-or-not.org/
VeriSign Labs
Different web pages will be displayed depending on the DNSSEC status.

http: //www.dnssec-failed.org/
Comcast (Deliberately Broken DNSSEC Validation Test Site)
Because it is deliberately set to fail by the DNSSEC validation test, an error is shown if the DNS cache server is DNSSEC-compliant.

Q If the DNSSEC is valid, will it take an extra time to look up DNS? Will the Internet access slow down?

A At the time of the DNSSEC validation, the number of queries by the cache DNS server increased compared with the situation without DNSSEC. Because of this, the time required to look up DNS will become longer. However, DNS response is fast enough for most cases and we think that there are few cases where users will find the Internet access slow.

Q What should we do for the setting of DNSSEC on the client side?

A You should designate a cache DNS server used by a client for the DNSSEC validation. In cases where you use the ISP's cache DNS server, such ISP needs to be DNSSEC-compliant.

In addition, DNS-OARC provides a cache DNS server with which users can try the DNSSEC validation.

OARC's Open DNSSEC Validating Resolver
https://www.dns-oarc.net/oarc/services/odvr

Q How can we check if my home broadband router is DNSSEC-compliant or not?

A Please check with the manufacturer if your broadband router is DNSSEC-compliant or not.
NIC.CZ develops its own verification tools and collects and releases related information

DNSSEC Hardware Tester
http://www.nic.cz/dnssectests/
CZ.NIC Labs

Q Is it necessary to change the setting of broadband routers in order to use DNSSEC? What kind of setting is required?

A In cases where the client side (device such as PC, etc.) is not DNSSEC-compliant, no setting change is required.
In cases where the client side is DNSSEC-compliant (conducts the DNSSEC validation), the following procedures are required.

In cases where explicit setting requirements for DNSSEC exist, follow the instructions and configure the settings.

In cases where explicit setting requirements do not exist, verify whether the broadband router is DNSSEC-compliant or not and implement necessary procedures by updating firmware. The latest firmware may be DNSSEC-compliant.

Q Will it be necessary for the client side (device such as PC, etc.) to configure any setting changes to OS, browser, application, etc.?

A It will be necessary to configure the OS setting to allow the usage of the cache DNS server for the DNSSEC validation.

Even with the current browser and application, DNSSEC works as an error message is shown when you access the domain name which is affected by the DNS cache poisoning.

Currently, there are not many browsers and application which are DNSSEC-compliant.

For example, FireFox has an add-on for the DNSSEC validation. This add-on allows you to check whether currently displayed websites are DNSSEC-compliant and whether a client uses DNSSEC-compliant DNS server.

DNSSEC Validator
http: //www.dnssec-validator.cz/
CZ.NIC Labs

Q Which DNS applications are DNSSEC-compliant? (Version, etc.)

A DNS applications which support RSASHA256 should be used as a cache DNS server in order to use root zone signatures.

BIND 9.6.2 and above, 9.7 and above
Unbound 1.4.0 and above

Q Are special devices required in order to use DNSSEC?

A No special devices are required. However, when the DNSSEC validation is conducted on the client side (device such as PC, etc.), some broadband routers may experience issues such as incompatibility with increased DNS response size, etc.

▼Questions on Operations

Q Will the network performance be affected by increased load as a result of DNSSEC?

A It is predicted that as a result of the deployment of DNSSEC, CPU load to the full-service resolver will be doubled due to key signature and validation and the transfer data volume will increase by three to five times. It is necessary to expand the capacity of devices as required.

Q How much will the record size and load increase, specifically?

A The size of DNS response packets will increase by approximately three to five times and the load to the full-service resolver will be approximately doubled.

Q How much traffic increase is expected?

A In cases where all major TLDs become DNSSEC-compliant, traffic is expected to increase by three to five times.

Q What will happen if a key is leaked?

A You will be vulnerable against DNS poisoning attacks like prior to the deployment of DNSSEC,.

Q What will happen if a key rollover fails? How much will be a scope of the impact?

A In cases where the cache DNS server used by users who loop up that domain name is DNSSEC-compliant, name resolution will fail due to a failure in the DNSSEC validation.
In cases where the cache DNS server of an ISP, etc. is DNSSEC-compliant, its customers will be affected.

Q What will happen when a key has expired?

A Keys do not have the expiration period. However, there is a recommended usage period, so rollover keys appropriately, depending on the strength of key encryption.

Q When should we conduct zone re-signing?

A When zone information is changed, re-signing is required.
In addition, for the operation of DNSSEC, re-signing should be completed during the safety period well before the signature expiration.
As for the safety period, it is necessary to secure the period which is at least the same as the TTL value of RRSIG or longer.

Q What kind of impact is expected as a result of setting error of a trust anchor?

A All domain name validations for which the trust anchor is set will fail and name resolutions cannot be conducted.

Q What should we set for trust anchors?

A Unless there are special circumstances, root zone trust anchors should be set. Root zone trust anchors are available on <https: //data.iana.org/root-anchors/>.

▼Questions on Industry Trend

Q How much has DNSSEC been introduced around the world?

A The DNSSEC signature for root zones started on July 15 2010. The number of TLDs for which the DNSSEC signature has started is also increasing. For the latest situation, see <http://stats.research.icann.org/dns/tld_report/>.

The situation as of July 2010 is summarized in the "Situation of ccTLD and gTLD by Country" <http://dnssec.jp/wp-content/uploads/2010/07/20100721-tld_dnssec_deployment-koreeda.pdf> which was presented at the DNSSEC 2010 Summer Forum by DNSSEC Japan.

▼General Questions

Q Who uses DNSSEC?

A DNSSEC users are Internet users. DNSSEC is an extension of DNS. If their domain name registrants and ISPs are DNSSEC-compliant, end users do not really think about DNSSEC.

Q Why did DNSSEC not exist before? Is it because of a new threat?

A More than ten years have passed since the start of DNSSEC specification implementation. DNSSEC is an extension specification to address vulnerability of DNS. Because a method to easily attack DNS vulnerability was revealed in the summer of 2008, it caught people's attention and countermeasures were developed.

For more detail on the attack method, see of the JPRS Topics & Column "New DNS Cache Poisoning Threat: Emergence of Kaminsky's Attack" <http://jpinfo.jp/topics-column/009.pdf>.

Q What is DNS?

A DNS is a "name resolution" mechanism which associates domain names which are parts of Internet addresses with IP addresses. For more detail, see the JPRS Topics & Column "Mechanism and Principles of DNS: DNS as a Backbone of the Internet" <http://jpinfo.jp/topics-column/010.pdf>.

Q What is DNSSEC?

A DNSSEC is a security extension specification which has been implemented in order to address fundamental vulnerability of DNS specifications. For more detail, see the DNSSEC Series (No.13 <http://jpinfo.jp/topics-column/013.pdf>, No.14 <http://jpinfo.jp/topics-column/014.pdf>, No.15 <http://jpinfo.jp/topics-column/015.pdf>, No.16 <http://jpinfo.jp/topics-column/016.pdf>) of the JPRS Topics & Column <http: //jpinfo.jp/topics-column/>.

Q What does DNSSEC stand for?

A DNSSEC stands for “DNS Security Extensions.”

Q Can we use DNSSEC overseas?

A Because DNSSEC services is provided via the Internet, you can use it in Japan or overseas as long as you can access the Internet.

FAQ: Specific Questions

"FAQ: Specific Questions" summarize questions for which different answers are anticipated for each business operator and answers (A) are not included.

▼Questions on Fees

Q How much cost will be incurred for the DNSSEC setting? Will DNSSEC be a fee-based service?

Q Can we charge our customers in providing DNSSEC services?

▼Questions on Services

Q How can we explain about DNSSEC to our customers?

Q When will DNSSEC be deployed?

Q Where is the main contact for DNSSEC?

Q Can we delegate necessary procedures of DNSSEC such as user key management, etc. to JPRS?

Q The lower domain wishes to become DNSSEC-compliant. In cases where my DNS is not DNSSEC-compliant, is it possible to provide DNSSEC services only to the lower domain?

Q If the DNS master server is DNSSEC-compliant, can we assume that the procedures are completed?

Q I manage a DNS master server. Is there a plan to introduce DNSSEC to secondary DNS servers?

Q Is there anything we should prepare for the introduction of DNSSEC?

Q Where do we need the DNSSEC setting?

Q What domains will be covered by the registration of DS?

Q Is a special application required in order to start the registration of DS?

Q Can we use DNSSEC only by sending a registration to JPRS?

Q How should we process applications from customers? What is an interface?

Q How can we register DS to the parent authoritative DNS server?

Q What kind of impact is anticipated if we fail in the DS record registration in the parent DNS server?

Q What will happen to our customers if we fail in the setting?

Q Are re-signing and switching of DS registered in the parent DNS server necessary every time we change the content of zone files? Who should we contact for the procedures?

Q Won't customers change keys frequently?

Q How will the integration flow of .JP registrar transfer and domain transfer be impacted by the deployment of DNSSEC?

Q Is there a window period for the registrar transfer?

Q Are there any support measures in cases where we receive no response from the loosing registrar?

Q Are there any transfer fees?

Q What kind of method is used for the exchange of keys for the .JP registrar transfer?

Q We will transfer registrars from a DNSSEC-compliant registrar to a registrar which is not DNSSEC-compliant. Can you remove DS after the transfer?

Q The loosing registrar removed DNS immediately after the approval following the registrar transfer.

▼Questions on the Registrant

Q Is there anything that customers have to do for the introduction of DNSSEC?

Q Will there be any impact on customers' own services (financial, securities, etc.)?

Q Who will take responsibility if customers' services are impacted?

▼Technical Questions

Q Can you explain about the DNSSEC implementation status and setting methods other than BIND (PowerDNS, etc.)?

Q Can/Should we use it for the DDNS service?

▼Questions on Operations

Q Will the load to devices increase?

Q In line with increases in NW / server load as a result of the deployment of DNSSEC, how much reinforcement will be required for specific devices?

Q Is there anything we should consider for devices other than servers (L4SW, etc.)?

Q How often should we roll over keys?

Q Who is in charge of key rollover?

Q How key rollover should be managed?

Q Is there anything we should pay attention to at the time of key rollover?

Q How much operation is required for key rollover?

Q What are the causes of failure in key rollover?

Q Is it possible to switch back immediately after the failure in key rollover?

Q How long is the expiration period for keys?

Q How long is an appropriate expiration period for signatures?

Q What is the scope of the signing requirement? Is it necessary to sign internal domains?

Q Is there a supplementary tool for the operation of DNSSEC?

Q It is possible to automate the key information expiration management?

Q Isn't the manual operation difficult as key management and rollover are complicated and carry significant risk in the case of failure.

Q Is there technical support before and after the deployment of DNSSEC? What are countermeasures in case of a trouble?

Q What is necessary in using DNSSEC?

Q Do we need to monitor anything in order to avoid problems?

Q Are there any concerns at the time of the DNS maintenance?

Q Are there any words of advice in introducing DNSSEC?

Q How should we configure the setting in order to use DNSSEC?

Q Are complex settings required on our end?

Q How much cost will be incurred for the deployment and operation of DNSSEC?

Q Will zone transfer be affected?

Q Is it necessary to adjust SOA expire value in using DNSSEC?

Q What are appropriate DNSKEY and DS-TTL values?

Q How will security be assured during the handover of DS?

▼Questions on Industry Trend

Q When will ISPs and .JP registrars become DNSSEC-compliant?

Q How much is the DNSSEC penetration rate for the .JP domain?

Q Is there a plan to make the reverse lookup (IPv4, IPv6) domain tree DNSSEC-compliant?

▼General Questions

Q Will DNSSEC be a fee-based service?

Q Do we have to enter into a special contract with an ISP in order to use DNSSEC? Who should we contact?

Individual Experiment

Individual Experiment: Case Study 1

- Experimental Environment

XXX.XXX.XXX.XXX	DNSSEC master server for verification	
		Xen Virtual
	bind9.7.2-p2	2.5GHz
	CentOS4.8	Memory: 1024MB

XXX.XXX.XXX.XXX	DNSSEC slave server for verification	
		Xen Virtual
	bind9.7.2-p2	2.5GHz
	CentOS4.8	Memory: 1024MB

- Summary of Experimental Results

  It was verified that no issues were identified as a result of the DNS zone signature and validation of the DS record registration procedures using .JP registrar I/F (Web) for the experiment.
  In addition, the registrar transfer on the key management I/F level was conducted.

- Detailed Experimental Results

  Because only an “Error” was displayed when a DS record for a wrong filed was entered, it took time for us to identify the cause of the problem. Although it was due to unfamiliarity, we thought it would be helpful if more detailed message was shown or examples of entry could be referred to. The registrar transfer was reflected immediately without a verification message or anything, which made us feel a bit anxious.

- Obtained Findings

  Because the evaluation was conducted by people in the section which did not have background knowledge on DNSSEC, they seemed to have felt uncomfortable without knowing successful conditions. We think that preparing a comprehensive operational manual and understanding operating principles in order to deal with any contingency will help to avoid errors as a result.

Individual Experiment: Case Study 2

- Experimental Environment

  Prior to the DNSSEC operational test of an inhouse server using the DNSSEC technology experimental environment, we established the DNSSEC operational method for our company. We set up an experimental environment with one authoritative DNS server, one secondary server and one cache DNS server and conducted an operational verification using the aforementioned operational flow by connecting to the technology experimental environment via the Internet.

- Summary of Experimental Results

  It was verified that the operation of DNSSEC using the Web interface of the DNSSEC technology experimental environment could be conducted without any issues.

- Detailed Experimental Results

  The Web interface of the DNSSEC technology experimental environment was used and domain registrations, etc. were tested.
  It was tested if the registration to the registry could be conducted properly.
  In addition, it was verified that the cache DNS server validation completed successfully.
  Based on the above, policies toward the actual operation were set with regard to the DNSSEC operational methods and measures going forward. The validation for transaction interface is scheduled to be conducted in the future.

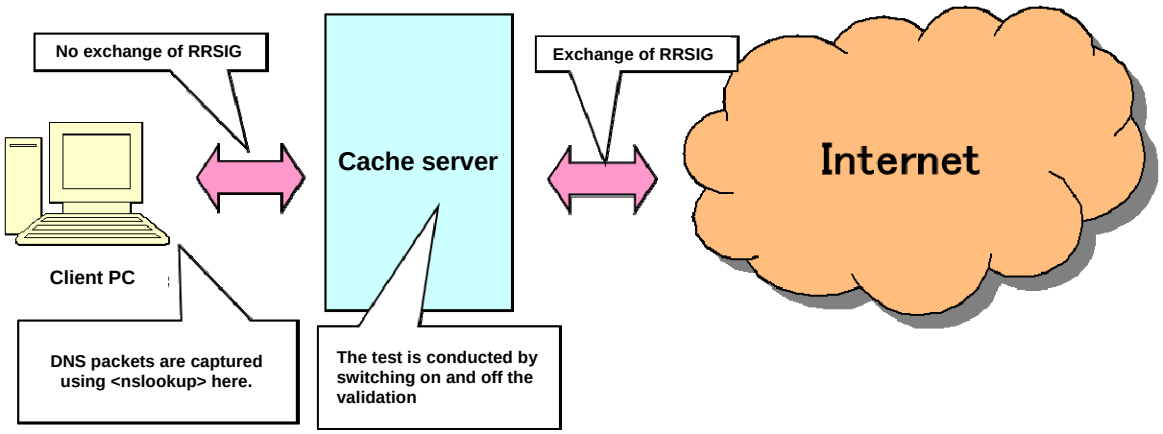
- Obtained Findings

  Registration to the registry using the Web interface can be conducted without any issues and it can be used like the current interface without any significant differences.

Individual Experiment: Case Study 3

- Experimental Environment

The test was conducted in order to measure if there were any significant changes in the size of packets received by end users when the DNSSEC validation was ON and OFF.



- Summary of Experimental Results

It was verified that the packet size between end users and the cache DNS server did not change significantly when the DNSSEC validation was On and OFF.

- Detailed Experimental Results

Domain name	With validation		Without validation		Note
	Response	Packet size	Response	Packet size	
www.isc.org	NOERROR	318byte	NOERROR	186byte	Fully DNSSEC-compliant domain
dnssec-deployment.org	NOERROR	97byte	NOERROR	260byte	Fully DNSSEC-compliant domain
www.sub118.crisp.jp	SERVFAIL	79byte	NOERROR	121byte	Domain with expired DNSSEC
yahoo.co.jp	NOERROR	151byte	NOERROR	151byte	Domain without DNSSEC

・ Obtained Findings

・We think that there will be no significant impact on end users even if the DNSSEC validation for the cache DNS server is ON.

・The difference in packet size between when DNSSEC was ON and OFF was due to the existence of additional records.