안내서	KISA-GD-2011-0002

DNS 설정 안내서

2011. 9.

KISA 한국인터넷진흥원
Korea Internet & Security Agency

KISA-GD-2011-0002

DNS 설정 안내서

2011.9

KISA
한국인터넷진흥원

제·개정 이력

순번	제·개정일	변경내용	발간팀	연락처
1	2009.9	제정	시스템관리팀	405-6647
2	2010.2	개정	시스템관리팀	405-6477
3	2010.6	개정	시스템관리팀	405-6477
4	2011.9	개정	인터넷기반기술팀	405-6475

<목 차>

1. DNS 기본 개념

가. 도메인 네임

도메인 네임은 인터넷 사용에 있어, 사람이 기억하기 어려운 인터넷 IP 주소 대신에 문자로 구성된 이름을 사용할 수 있도록 하는 일종의 명칭(naming) 체계입니다. 영문명으로는 “domain name”이라 하며, 이를 ”도메인 이름“이라 번역하기도 합니다. 단순히 ”도메인“이라고 칭하기도 합니다. 본 가이드에서는 ”도메인 네임“을 사용합니다.

나. 도메인 네임 시스템 (DNS) 구성

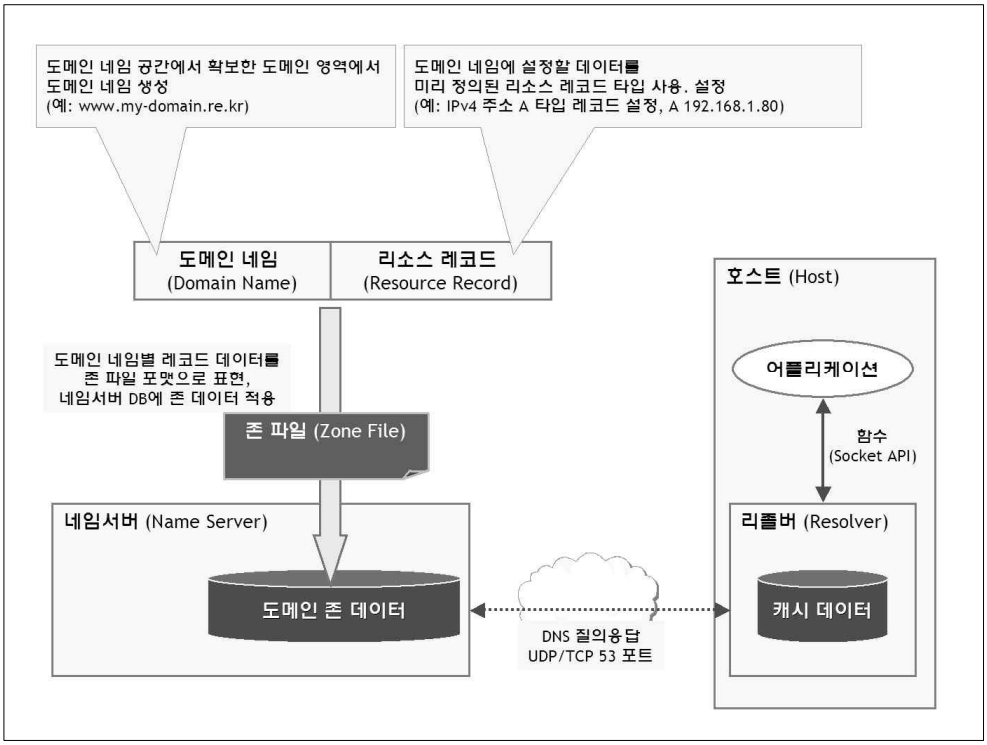
도메인 네임 시스템(Domain Name System)은 인터넷 도메인 네임을 위한 제반 체계를 통칭하는 용어입니다. 흔히 DNS라고 하면 네임서버를 지칭하는 것으로 이해하고 사용하고 있지만, 도메인 네임서버는 도메인 네임 시스템을 구성하고 있는 일부 요소입니다.

도메인 네임 시스템은 초기 인터넷에서 호스트 네임별 IP 주소 정보를 시스템의 HOSTS.TXT 파일로 관리하던 것을 보다 체계적으로 관리할 수 있도록 하기 위한 일종의 데이터베이스 시스템으로써 개발되었습니다. 도메인 네임 시스템은 각 사이트에서 자신의 도메인 데이터 영역을 자체 관리하고, 분산 관리하의 모든 도메인들이 단일한 전체 도메인 체계에 통합될 수 있는 구조로 설계된 분산구조의 데이터베이스 시스템입니다.

도메인 네임 시스템은 세 가지 요소로 구성되어 있습니다.

첫 번째 요소는 도메인 네임 공간(Domain Name Space)과 리소스 레코드(Resource Record)입니다.
두 번째 요소는 네임서버(Name Server)입니다.
세 번째 요소는 리졸버(Resolver)입니다.

다음 그림은 이 세 가지 요소로 구성되는 도메인 네임 시스템의 기본 구조를 보여줍니다.



1) 도메인 네임 공간과 리소스 레코드

데이터베이스 시스템으로써의 도메인 네임 시스템에서 사용할 데이터 자료 구조를 정의하는 사항에 해당합니다.

도메인 네임 공간은 도메인 네임을 중복되지 않게 네임을 생성하여 사용하도록 정의된 도메인 네임 구성 체계입니다. 흔히 최상위에 루트 도메인으로부터 뻗어나가는 트리 구조의 도메인 네임 체계가 이에 해당합니다. 도메인 네임 시스템에서 하나의 도메인 네임은 유일한 값을 갖습니다.

리소스 레코드는 도메인 네임에 설정할 수 있는 데이터 타입입니다. 데이터베이스 시스템으로써의 도메인 네임 시스템은 도메인 네임을 키(key)로 하여 이 도메인 네임에 필요한 데이터를 설정하게 됩니다. 도메인 네임의 데이터는 사전에 약속된 데이터 타입과 포맷(FQDN)으로 적용해야 합니다. 리소스 레코드는 이렇게 도메인 네임에 설정할 수 있는 데이터의 종류를 정의한 것입니다. 리소스 레코드 타입에는 잘 알려진 IPv4 주소의 A 타입 레코드 외에도 다양한 레코드 타입이 정의되어 있습니다.

2) 네임서버

도메인의 데이터를 보유하고, 외부 인터넷으로부터 도메인 네임에 대한 데이터 질의가 있을 때, 보유한 데이터를 조회하여 응답하는 역할을 담당합니다. 여기서 네임서버는 도메인 존만 설정하고 리커시브 기능을 갖지 않아야 합니다. 네임서버는 주로 내부 메모리에 데이터베이스 구조를 구현하여 존 파일을 통해 읽어 들인 데이터를 도메인 존 데이터로 저장합니다. 외부의 별도 데이터베이스 시스템에서 도메인 존 데이터를 관리하고, 네임서버는 데이터베이스 시스템으로부터 도메인 존 데이터를 읽어 들여 DNS 응답에 사용하도록 구현한 네임서버도 있습니다.

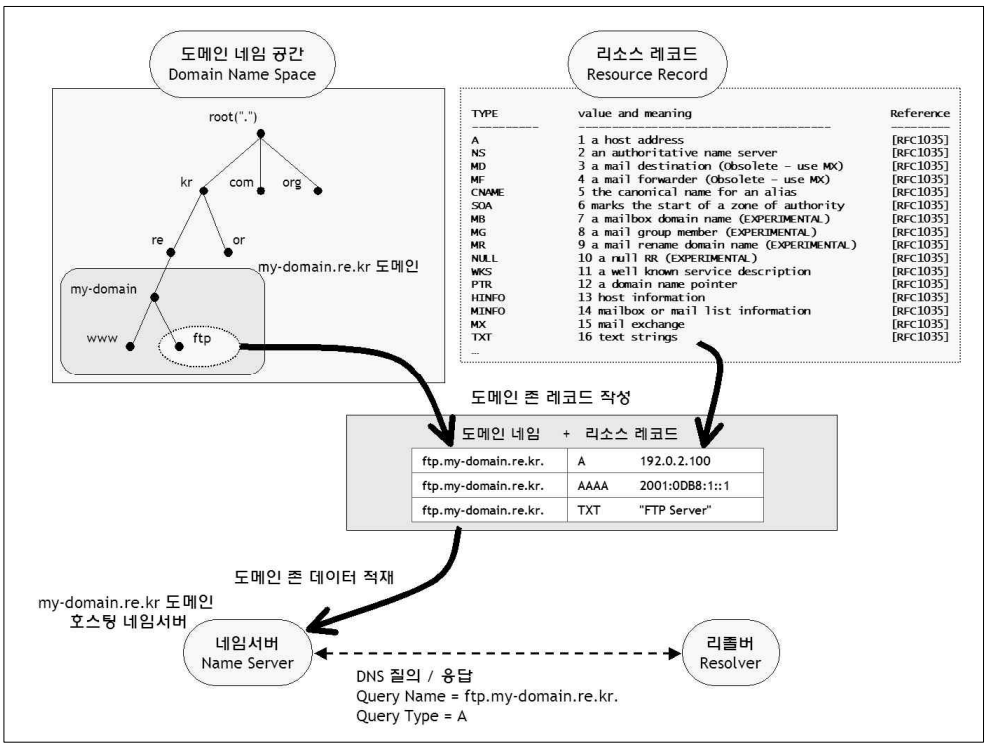
3) 리졸버

도메인 네임의 데이터 조회기능을 수행하는 S/W 라이브러리 형태의 루틴을 가리킵니다. 리졸버는 응용 어플리케이션으로부터 도메인 네임과 조회대상 레코드 타입을 입력받아 인터넷 상에서 해당 도메인이 설정되어 있는 네임서버를 자동으로 추적 탐색하여 원하는 데이터를 응답받아 최종 결과를 응용 어플리케이션으로 되돌려 주는 기능을 합니다. 도메인 네임 시스템이 분산구조 방식의 데이터베이스이기 때문에, 데이터가 하나의 시스템이 아니라 인터넷 각 네임서버에 흩어져 산재하고 있어 이를 조회하기 위한 리졸버가 필요합니다.

원래 리졸버는 호스트에서만 시스템이 구현되는 요소였지만 DNS 질의응답이 많아지면서 트래픽이 과다하게 발생하는 문제가 있었습니다. 지금은 미미한 수준이지만 1980년대 당시 인터넷 백본은 56Kbps ~ 1.5Mbps 정도로 DNS 트래픽이 약 20% 이상을 차지하고 있었습니다. DNS 트래픽 발생을 감소시키기 위해 리커시브 네임서버(캐싱 네임서버)를 사용하게 됩니다.

현재 인터넷에서는 리졸버를 DNS 질의응답 트래픽의 절감 및 질의응답 절차의 효율성을 위해 데이터 캐싱 기능을 갖는 별도의 시스템인 리커시브 네임서버로 주로 구현하여 구성하고 있습니다. (이 리커시브 네임서버를 캐싱 네임서버라고도 합니다.) 이 경우에도 호스트에는 응용 어플리케이션의 조회요청을 처리할 리졸버가 필요합니다. 리커시브 네임서버를 사용하는 경우, 호스트에는 단순화된 리졸버 기능만을 갖는 “스터브 리졸버(stub resolver)” 루틴을 적용합니다.

다음은 도메인 네임 시스템의 세 가지 구성 요소를 보다 구체적으로 예시하여 보이는 그림입니다.



그림의 예시와 같이, 도메인 네임 공간에서 “my-domain.re.kr” 도메인을 상위의 도메인 트리 중 “re.kr” 노드로부터 위임받아 확보합니다. “도메인 등록 절차”가 이에 해당합니다.

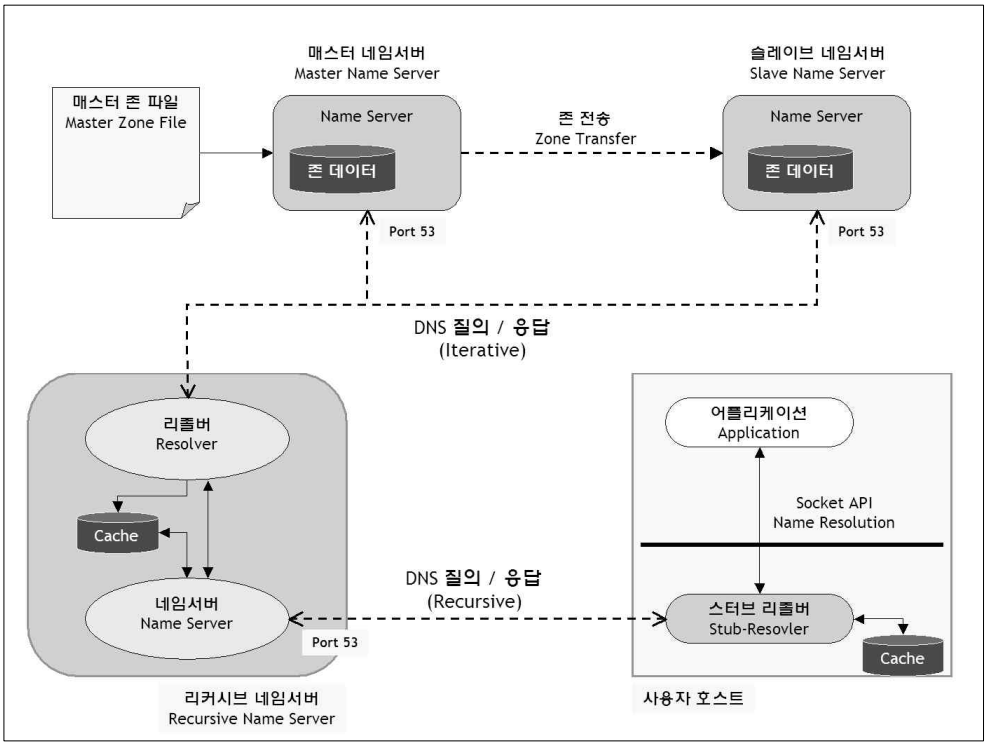
등록한 도메인 영역에서 필요한 도메인 네임을 생성하고, 이 도메인 네임에 대한 데이터를 데이터의 성격에 맞게 리소스 레코드 타입과 그 포맷을 적용하여 설정합니다. 이는 주로 존 파일 포맷으로 작성합니다. 존 파일 포맷은 인터넷 표준으로 정의되어 있으므로, 대부분의 DNS 표준을 구현한 네임서버는 존 파일을 인식하여 처리할 수 있습니다.

작성된 도메인 존의 데이터는 네임서버에 반영함으로써 인터넷에서 조회 가능한 상태가 됩니다. 원격의 리졸버는 도메인이 설정된 네임서버를 추적하여 원하는 도메인 네임의 데이터를 질의합니다. 그림과 같이 도메인 네임

ftp.my-domain.re.kr에 대한 A 타입 레코드를 질의한 경우, 이 도메인 네임에 여러 타입의 레코드가 있지만, A 타입 레코드만을 검색하여 응답 처리합니다.

다. 재귀적 질의와 반복적 질의

네임서버와 리졸버를 중심으로 한 DNS 질의응답 관계는 다음의 그림과 같습니다.



위 그림에서 사용자 호스트는 스터브 리졸버를 이용하여 리커시브 네임서버와 DNS 질의응답을 주고받습니다. 리커시브 네임서버는 네임서버 기능부와 리졸버 기능부로 구성된 것으로 표현되어 있습니다. 네임서버 기능부는 질의 메시지를 수신하고 다시 결과를 응답하는 서버 역할을 합니다. 이에 비해 리졸버는 자신의 캐시 영역에 데이터가 없는 경우 인터넷의 네임서버들로부터 질의대상 데이터의 조회를 수행하는 기능을 합니다. 질의대상 데이터가 캐시 영역에 있는 경우(TTL 값에 따라 만료되지 않은 과거 질의응답 데이터), 네

임서버 기능부는 호스트로 바로 응답처리 합니다. 그렇지 않은 경우, 질의 메시지의 유형에 따라 응답 데이터를 외부 인터넷에서 조회하기 위해 리졸버를 구동하거나 또는 응답 메시지 없이 호스트로 바로 응답 처리합니다.

DNS 질의에는 두 가지 유형이 있습니다. 하나는 재귀적(recursive) 질의이고, 다른 하나는 반복적(iterative) 질의입니다.

재귀적 질의(recursive query)는 사용자 호스트의 스터브 리졸버가 리커시브 네임서버로 질의할 때 사용합니다. 재귀적 질의는 리커시브 네임서버가 대신해서 도메인의 데이터를 인터넷에서 조회하여 응답해주는 질의 유형입니다.
 재귀적 질의를 받은 리커시브 네임서버는 캐시 데이터 영역에서 질의된 대상 데이터를 조회합니다. 캐시 영역에 데이터가 없는 경우, 리졸버 루틴을 가동시켜 인터넷 루트 네임서버로부터 질의절차를 순차적으로 수행하여 질의대상 데이터를 파악해 나갑니다. 리커시브 네임서버는 최종 데이터를 파악한 경우, 이를 사용자 호스트의 스터브 리졸버에게 응답처리 합니다.

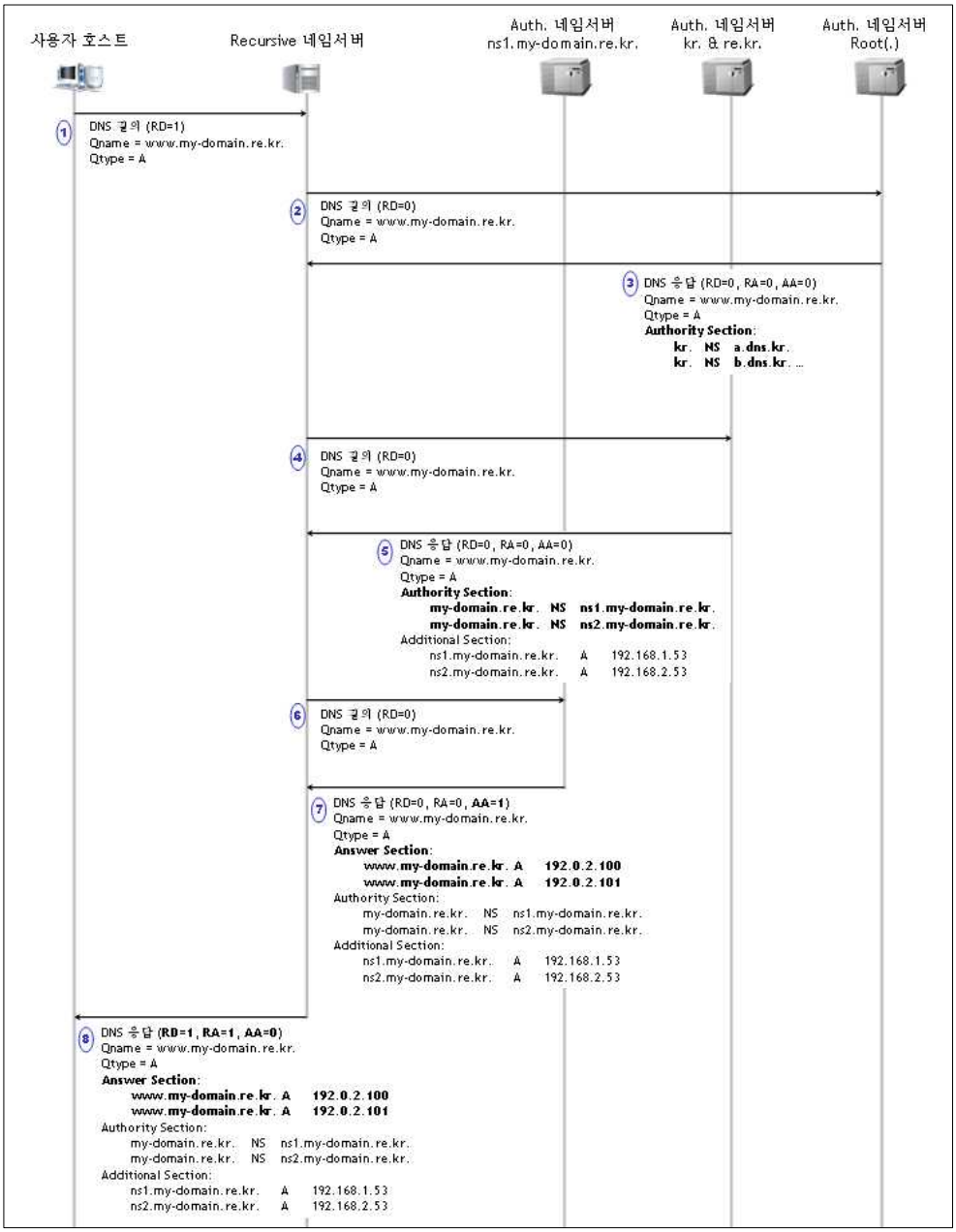
반복적 질의(iterative query)는 리커시브 네임서버의 캐시 영역의 데이터와는 무관하게 리졸버 루틴에 의해 사용됩니다. 도메인이 설정된 각 네임서버의 루트 네임서버부터 도메인의 트리형태 계층구조를 따라 순차적으로 반복하여 진행하는 질의입니다. 이때, 루트 네임서버로부터 질의하는 대상 도메인의 네임서버에 이르기까지 각 네임서버가 응답하는 위임된 네임서버 정보를 따라 네임서버들을 순차적으로 탐색해 나갑니다.

재귀적 질의와 반복적 질의는 DNS 질의 메시지에 헤더 플래그 정보에 의해 결정됩니다. DNS 질의 메시지 헤더의 RD(Recursive Desired) 플래그가 1로 세팅되어 있는 경우, 재귀적 질의(recursive query)입니다. 이 플래그가 0인 경우, 반복적 질의(iterative query)가 됩니다.

호스트의 스터브 리졸버는 항상 재귀적 질의 메시지를 리커시브 네임서버로 송출합니다.

반복적 질의를 리커시브 네임서버로 보낸 경우, 리커시브 네임서버는 재귀적 질의를 요청한 것이 아니므로 캐시에 데이터 없는 경우 리졸버를 구동하지 않고, 응답 레코드 없이 응답 메시지로 바로 응답 처리합니다.

2. DNS 질의응답 절차

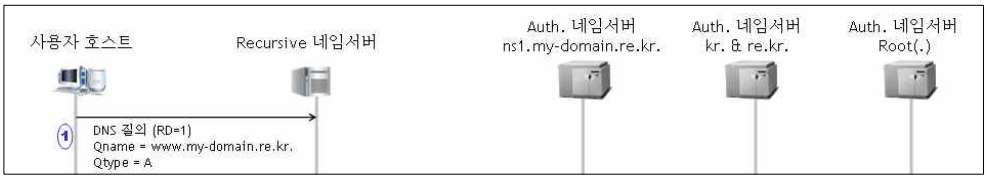

사용자 호스트
Recursive 네임서버
Auth. 네임서버 ns1.my-domain.re.kr.
Auth. 네임서버 kr. & re.kr.
Auth. 네임서버 Root(.)
1 DNS 질의 (RD=1)
Qname = www.my-domain.re.kr.
Qtype = A
2 DNS 질의 (RD=0)
Qname = www.my-domain.re.kr.
Qtype = A
3 DNS 응답 (RD=0, RA=0, AA=0)
Qname = www.my-domain.re.kr.
Qtype = A
Authority Section:
kr. NS a.dns.kr.
kr. NS b.dns.kr. ...
4 DNS 질의 (RD=0)
Qname = www.my-domain.re.kr.
Qtype = A
5 DNS 응답 (RD=0, RA=0, AA=0)
Qname = www.my-domain.re.kr.
Qtype = A
Authority Section:
my-domain.re.kr. NS ns1.my-domain.re.kr.
my-domain.re.kr. NS ns2.my-domain.re.kr.
Additional Section:
ns1.my-domain.re.kr. A 192.168.1.53
ns2.my-domain.re.kr. A 192.168.2.53
6 DNS 질의 (RD=0)
Qname = www.my-domain.re.kr.
Qtype = A
7 DNS 응답 (RD=0, RA=0, AA=1)
Qname = www.my-domain.re.kr.
Qtype = A
Answer Section:
www.my-domain.re.kr. A 192.0.2.100
www.my-domain.re.kr. A 192.0.2.101
Authority Section:
my-domain.re.kr. NS ns1.my-domain.re.kr.
my-domain.re.kr. NS ns2.my-domain.re.kr.
Additional Section:
ns1.my-domain.re.kr. A 192.168.1.53
ns2.my-domain.re.kr. A 192.168.2.53
8 DNS 응답 (RD=1, RA=1, AA=0)
Qname = www.my-domain.re.kr.
Qtype = A
Answer Section:
www.my-domain.re.kr. A 192.0.2.100
www.my-domain.re.kr. A 192.0.2.101
Authority Section:
my-domain.re.kr. NS ns1.my-domain.re.kr.
my-domain.re.kr. NS ns2.my-domain.re.kr.
Additional Section:
ns1.my-domain.re.kr. A 192.168.1.53
ns2.my-domain.re.kr. A 192.168.2.53

도메인 네임의 레코드를 조회하기 위해, 사용자 호스트의 스터브 리졸버는 리커시브 네임서버로 재귀적 질의(recursive query)를 합니다. 리커시브 네임서버는 자신의 캐시에 질의된 데이터가 없는 경우, 네임서버의 리졸버 루틴을 구동합니다. 리커시브 네임서버의 리졸버는 인터넷에서 루트 도메인의 네임서버부터 순차적으로 위임된 네임서버를 추적하여 질의응답 과정을 수행합니다. 최종적으로 데이터를 보유한 네임서버에서 응답 데이터를 얻습니다.

리커시브 네임서버의 리졸버가 루트 도메인의 네임서버로부터 위임된 연결을 따라 최종 네임서버까지 이르는 DNS 질의응답을 반복적 질의(iterative query)라 합니다.

다음은 리커시브 네임서버의 반복적 질의(iterative query) 절차를 도식적으로 보인 그림입니다. 각 단계별로 절차를 설명합니다.

1) Recursive 네임서버의 DNS 질의



사용자 호스트에 “네임서버 주소” 또는 “DNS 서버 주소”로 설정된 리커시브 네임서버로 DNS 질의 메시지를 송출합니다.

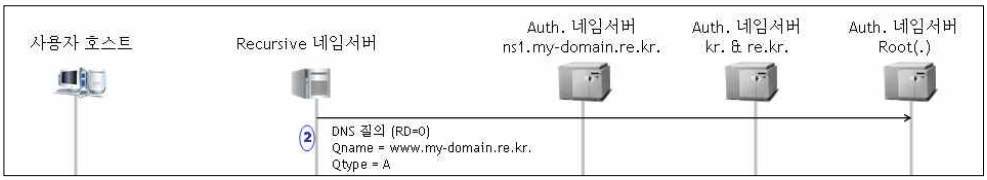
이때, DNS 메시지 헤더의 RD 플래그[1]는 1로 세팅합니다. 만일 RD 플래그를 세팅하지 않고 질의한다면, 리커시브 네임서버는 반복적 질의를 수행하지 않습니다. 대신 네임서버의 도메인 존 데이터 영역과 캐시 영역에서만 해당 데이터가 있는지 검색하여 그 결과로 응답처리 합니다. 이때 데이터가 없다면, 응답 데이터 없이 DNS 응답처리 합니다. RD 플래그는 네임서버로 하여금 DNS 질의 메시지가 재귀적 질의를 요청하는 것인지, 아니면 반복적 질의인지를 판단하여 관련 동작을 수행하게 합니다.

---

1) RD(Recursive Desired) 플래그: 리커시브 네임서버로 하여금 재귀적(recursive) 질의(항목 1.3. 참고) 요청을 표시함. RD 플레그 값이 “0”이면 반복적(iterative)질의를 요청

점검도구인 nslookup이나 dig은 명시적인 옵션을 사용하지 않으면 디폴트로 재귀적 질의(recursive query)를 합니다. 사용자 호스트의 입장에서 점검용 질의 메시지를 대상 네임서버로 재귀적 질의를 사용하여 송출합니다. 하지만 도메인 존이 없더라도 도메인 존 응답이 가능할 수도 있는데 이는 리커시브 네임서버의 캐시영역에 데이터가 있을 경우 대신 응답이 되기 때문에 착각을 일으킬 수 있습니다. 이 경우 AA 플래그[2]에 1로 세팅이 되었는지 확인할 필요가 있습니다.

2) Root 네임서버 질의



리커시브 네임서버는 재귀적 질의로 요청된 데이터가 캐시 영역과 도메인 존 데이터 영역에 존재하지 않을 때, 반복적 질의(iterative query) 절차를 개시합니다. 여기서는 캐시 영역이 비어 있다는 가정을 하여 예시합니다. 리커시브 네임서버는 루트 네임서버부터 질의를 시작합니다.
리커시브 네임서버의 리졸버가 반복적 질의(iterative query)에 사용하는 DNS 질의 메시지는 헤더 RD 플래그에 0으로 세팅합니다. 리커시브 네임서버의 리졸버가 질의하는 루트 네임서버 및 이하 최종 도메인까지의 네임서버들은 기본적으로 authoritative네임서버[3]입니다. 도메인 존을 설정하는 네임서버는 authoritative 네임서버로 구성하는 것이 원칙입니다.

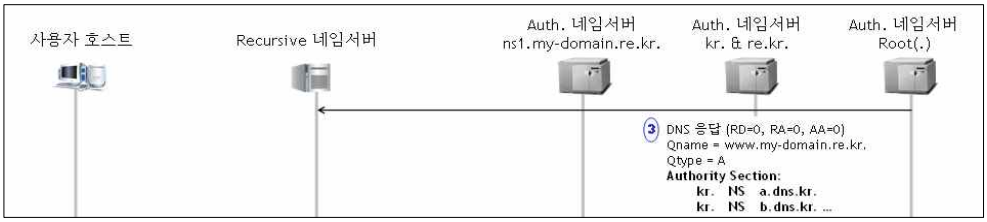
점검도구 nslookup이나 dig을 사용하여 리커시브 네임서버의 질의를 모사하여 점검하는 경우, 반복적 질의(iterative query)를 하도록 옵션을 명시해야 합니다. nslookup을 사용하는 경우, “set norecurse” 옵션으로 지정합니다.
dig의 경우, “+norecurse” 옵션과 함께 질의합니다.

---

2) AA 플래그: Authoritative Answer의 약자로써, 네임서버가 해당 응답 데이터를 자신이 보유하고 있는지 유무를 표시

3) Authoritative 네임서버: 도메인 존 데이터를 자신이 데이터로 보유하여 이 데이터만 사용하여 응답 처리하는 네임서버

3) Root DNS 응답



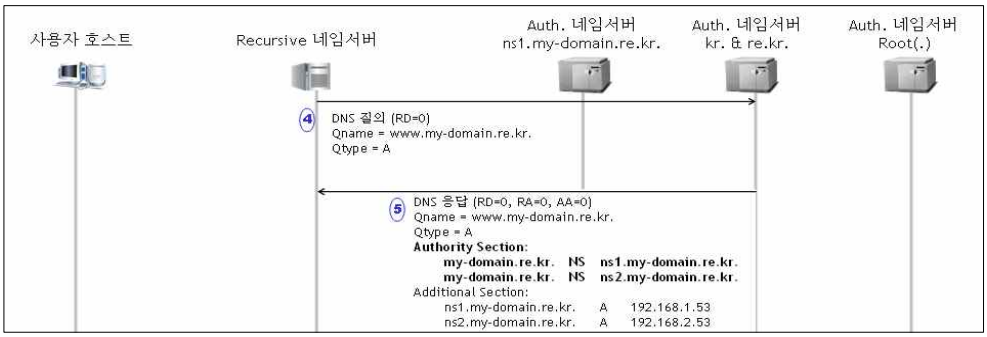
루트 네임서버는 질의된 도메인 네임 “www.my-domain.re.kr.”을 분석하여 이 도메인 네임이 속하고 있는 위임된 하위 도메인 존의 네임서버 정보를 authority 섹션과 additional 섹션에 설정하여 응답합니다.

이때 루트 네임서버가 응답하는 위임된 네임서버의 네임과 IP 주소 정보는 루트 도메인 존이 관리권한을 가진 데이터(authoritative data)가 아니므로, 응답 메시지 헤더의 AA 플래그는 0의 값을 가집니다.
위 사례에서, 질의된 도메인 네임이 .kr 도메인 영역에 속하므로, 루트 네임서버는 응답 메시지의 authority 섹션에는 .kr 도메인의 네임서버 네임 정보를, additional 섹션에는 .kr 도메인 네임서버의 IP 주소 정보를 설정합니다. Answer 섹션은 비어 있게 됩니다. 루트 도메인 존에는 질의된 데이터가 없기 때문입니다. 이는 “루트 존에는 질의된 데이터가 없고, 그 데이터는 authority 섹션에 나열된 네임서버가 관리하는 해당 도메인 영역에 속해 있다. 그 네임서버들의 IP 주소는 additional 섹션에 제시되어 있다. 해당 네임서버로 질의해 보라”라는 의미입니다.

도메인 네임 시스템을 분산구조의 데이터베이스라고 하는 것은 데이터를 한 곳에 집중하여 관리하는 것이 아니라, 도메인 영역으로 구분하여 각각의 네임서버에서 분산 관리하고 있기 때문입니다. 분산구조의 데이터베이스 체계에서는 “조회하고자 하는 데이터가 어느 네임서버에 저장되어 있는지”를 효율적으로 파악하는 방법이 중요합니다. 이를 위해, 도메인 네임 시스템은 도메인의 위임체계를 통하여 해결하고 있습니다. 루트 도메인 존에서는 .kr 도메인 영역을 구분하는 위임정보를 보유하고 있습니다. 그래서 위 사례와 같이 질의가 있을 때, 해당하는 위임된 도메인의 네임서버 정보를 알려주어 해당 네임서버로 바로 찾아갈 수 있게 합니다.

만일, 이 위임된 도메인의 네임서버 정보에 오류가 있다면, 해당 위임된 도메인이 어디에 있는지 전혀 찾을 수 없게 될 수도 있습니다. 도메인의 네임서버 정보는 네임서버 존 파일에서만 관리하면 되는 것이 아닙니다. 상위 도메인, .kr 도메인인 경우 .kr 도메인 존에 네임서버 정보가 정확히 등록되어 있어야 인터넷 상의 리커시브 네임서버가 정확하게 네임서버를 찾아 질의해 올 수 있습니다.

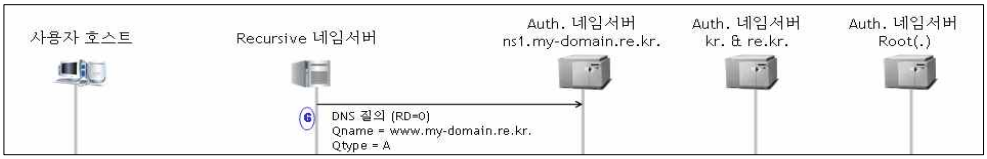
4) .kr 네임서버 질의응답



리커시브 네임서버는 루트 네임서버로 부터 얻은 .kr 도메인의 네임서버의 IP 주소를 사용하여 동일한 DNS 질의 메시지를 송출합니다. .kr 네임서버는 루트 네임서버의 응답과 같은 방식으로 my-domain.re.kr의 네임서버 정보를 참조 정보로 제시하여 응답합니다.

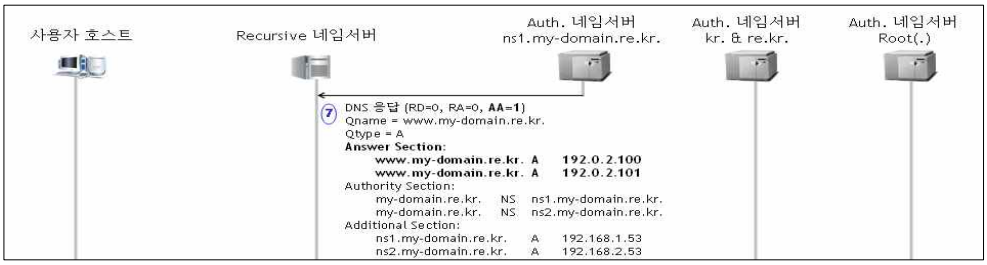
이때, .kr 도메인의 네임서버는 re.kr 존도 함께 설정하고 있으므로, 리커시브 네임서버로 응답할 때, re.kr 존에 설정된 my-domain.re.kr 도메인의 위임된 네임서버 정보로 응답합니다.

5) my-domain.re.kr 존 네임서버 질의



리커시브 네임서버는 my-domain.re.kr 존의 네임서버로 동일한 DNS 질의 메시지를 송출합니다.

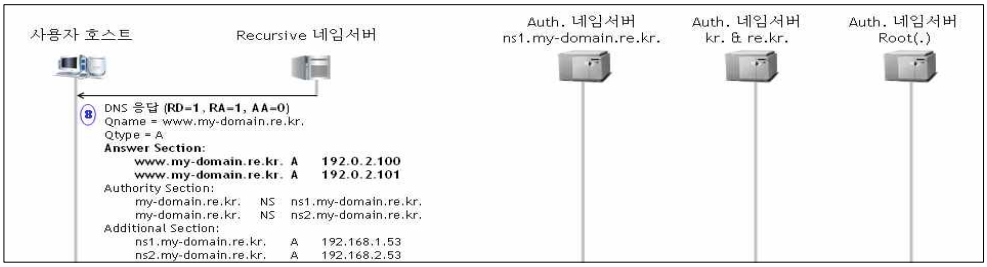
6) my-domain.re.kr 존 네임서버 응답



my-domain.re.kr 존의 네임서버는 자신에게 설정된 존의 데이터 중 요청된 데이터를 검색하여 그 결과 데이터로 응답합니다.

이때, 응답 메시지 헤더의 AA 플래그는 1의 값을 가집니다. Answer 섹션에는 질의된 도메인 네임 및 레코드 타입을 갖는 데이터를 설정하여 응답합니다.

7) DNS 응답 메시지 송출



리커시브 네임서버는 응답받은 데이터를 캐시에 저장처리 합니다. 동시에 질의요청을 한 호스트에게 DNS 응답 메시지를 송출합니다.

이 메시지의 RD 플래그와 RA 플래그[4] 모두는 1의 값을 갖습니다. 반면에 AA 플래그는 0의 값을 갖습니다. 이 응답 데이터가 리커시브 네임서버 자신이 보유한 존 데이터 영역에서 유래한 것이 아니기 때문입니다.

만일 위 사례에서 리커시브 네임서버가 authoritative 네임서버 기능을 겸하고 있고, my-domain.re.kr 도메인 존을 설정하고 있다면, 위 절차에서 호스트에 대한 최종 응답 메시지의 AA 플래그가 1로 세팅되어 응답됩니다. 이는 캐시가 아니라, 자신이 보유하고 있는 존 데이터로 응답하고 있음을 표시합니다.

도메인 설정 상태를 점검할 때 nslookup이나 dig에서 출력되는 응답 메시지 헤더의 플래그 값 체크가 필요합니다. 도메인의 네임서버를 지정하여 직접 질의를 했을 때, 그 응답 메시지 헤더의 AA 플래그 값이 0이고, RA 플래그 값이 1이라면, 이 네임서버는 도메인 존을 가지지 않고 리커시브 네임서버 역할을 하여 응답하고 있는 것을 의미합니다. 도메인 존 설정이 누락되어 있는 리커시브 기능의 네임서버이므로 도메인 구성에 결함이 있는 상태입니다.

4) RA 플래그: Recursive Available의 약자로써, 응답하는 네임서버가 리커시브 기능을 갖는 네임서버인지를 표시

3. DNS S/W 기본설치 방법

네임서버는 리눅스/유닉스 계열의 시스템에서는 주로 BIND라는 S/W를 사용하며, 전 세계적으로 약 70%정도가 사용되고 있습니다. 윈도우 서버 계열에서는 관리 도구의 DNS에서 설정할 수 있습니다.

윈도우 서버 계열의 DNS는 별도의 설치과정이 필요 없으므로 본 지침서에서는 유닉스 계열의 BIND S/W의 설치에 관해 설명하도록 하겠습니다.

BIND S/W의 설치 순서는 다음과 같다.

가) BIND 다운로드

BIND는 “http://www.isc.org” 에서 받을 수 있습니다. 설치 순서는 다음과 같습니다.

① SOFTWARE 메뉴의 BIND메뉴를 클릭합니다.

② unix, linux 압축 파일인 tar.gz을 받습니다.

나) BIND 업로드

다운받은 BIND 9.X.X를 설치할 서버에 업로드합니다. 업로드 프로그램으로는 주로 sftp나 ftp를 이용하여 업로드 하면 됩니다.

다) BIND 압축해제

업로드한 서버에 telnet이나 ssh로 접속합니다. gzip, tar명령어를 이용하여 압축을 해제합니다.

```
#gzip -d bind-9.X.X.tar.gz
#tar -xvf bind9.X.X.tar
```

라) BIND 컴파일

컴파일시 옵션은 기본 설정을 사용합니다.

```
# ./configure --prefix=설치위치 --with-openssl=설치된 위치
  --sysconfdir=설정위치
# make
# make install
```

```
#./configure --prefix=/usr/local/bind --with-openssl=/usrl/local/ssl --sysconfdir=/etc
#make
#make install
```

마) BIND 설정

BIND를 구성하고 있는 파일과 그 파일의 위치, 용도는 아래 표와 같습니다.

구성파일	위치	용도 및 설명
named.conf	/etc	named가 실행 시에 Name Server의 데이터베이스에 대한 기본적인 정보를 취급합니다. 설정 파일의 디렉터리, 파일 위치 등을 지정하며 secondary 옵션으로 2차 Name Server를 지정할 수도 있습니다.
host.conf	/etc	resolver의 옵션을 가지고 있는 파일. host 파일을 먼저 검색할 것인지 아니면 DNS에 의한 쿼리를 먼저 할 것인지의 순서를 정하는 설정이 order 옵션으로 설정되어 있습니다.
hosts	/etc	mini DNS의 역할을 하는 파일
resolv.conf	/etc	시스템에서 사용할 Name Server의 주소를 가짐
rndc.conf	/etc	named의 안전한 reload를 위해 사용
zone file	/var/named	일반적인 위치는 \var\named 디렉터리이며 각 도메인들에 대한 실제 정보들을 공유하고 있는 DNS의 핵심 파일입니다.
named.ca	/var/named	루트 Name Server의 IP 주소를 정의하여 더 빨리 찾을 수 있도록 최적화 되어 있는 파일
named.local	/var/named	IP Address를 도메인으로 변경해주는 reverse mapping을 정의한 파일
reverse mapping	/etc	대표 도메인에 대한 inverse domain 정보를 기록. \etc\named.conf에서 이름을 정의합니다.

BIND를 구동하기 위해서는 구성파일 중 다음 네 가지를 반드시 설정하여야 합니다.

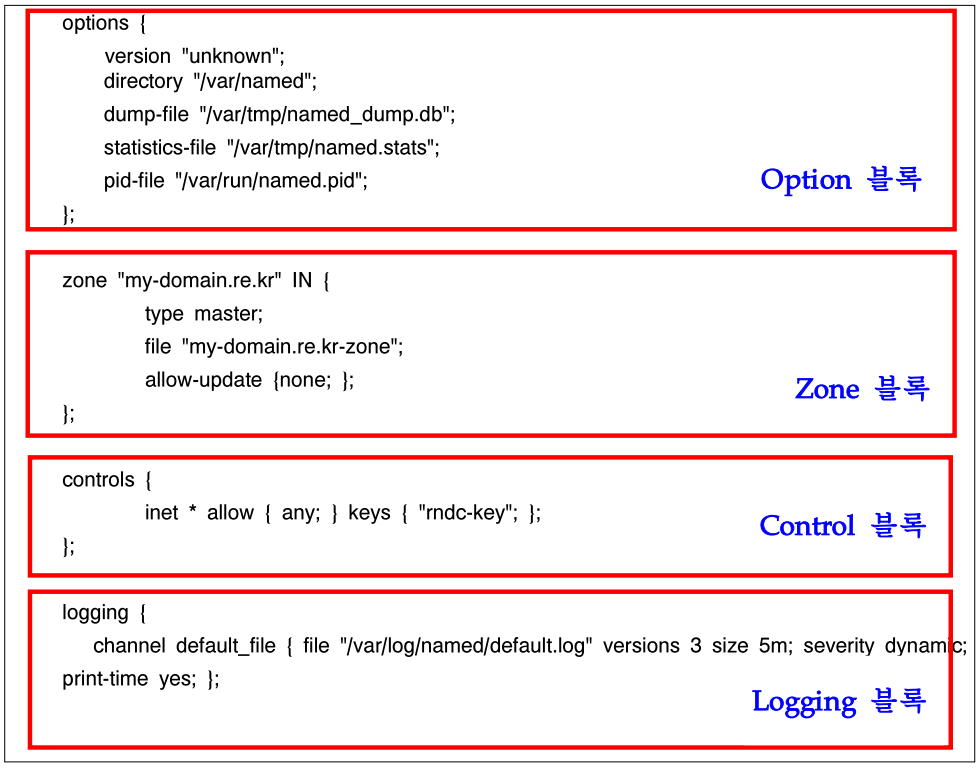
- named.conf
- zone file
- named.ca
- named.local

(1) named.conf 설정

named.conf는 설치자가 직접 작성해야 하며 그 위치는 “/etc”입니다.

named.conf 파일은 options 블록, zone 블록, controls 블록, logging 블록으로 구성되어 있습니다.

named.conf를 설정하기 위해서는 options 블록과 도메인 혹은 FQDN에 대한 zone 블록의 설정이 필수적이기 때문에 이 두가지 블록에 대한 구성 및 설정방법에 대해 상세하게 설명하도록 하겠습니다..



① Options 블록 설정

options 블록은 named.conf 설정에 필수적이며 사용하는 옵션은 아래와 같습니다.

옵션	설명
version	bind의 버전을 강제로 지정한다.
directory	zone file이 위치할 곳을 지정
pid-file	PID가 담긴 파일 생성 경로를 지정
allow-transfer	Primary 네임 서버의 네임서버 관련 내용을 secondary 네임 서버로의 전송을 지정

```
options {
        version "unknown";
        // 보안을 위해 버전정보를 숨기는 것이 좋습니다..

           directory "/var/named";
        // 각 도메인의 설정파일들이 위치할 디렉터리를 정의합니다. 보통 기본값으로 /var/named를 많이 사
           용합니다.

           pid-file   "/var/run/named.pid";
        // named를 실행하면 named의 process id를 기록한 파일을 /var/run에 생성.
          이 옵션은 이 pid 파일의 위치를 변경할 수 있도록 합니다.

           allow-transfer { 192.168.0.1; };
        // secondary 네임 서버로 운영할 서버의 아이피 주소를 적어줍니다. primary만 운영할 경우
           적어주지 않아도 됩니다.
  };
```

② Zone 블록 설정

zone 블록은 다음과 같이 크게 5가지 분류를 통해 설명할 수 있습니다.

- 캐시 네임서버 Zone, localhost Zone, 로컬 네트워크의 inverse domain Zone,
- 운영하고자 하는 실제 FQDN에 관한 Zone,
- 네임서버가 위치하는 네트워크에 대한 inverse domain,
- secondary 네임서버의 named.conf 설정,
- primary 네임서버가 위치하는 네트워크에 대한 inverse domain

만약, 네임서버가 secondary의 역할을 하지 않는다면 가장 마지막의 secondary domain과 primary 네임서버가 위치하는 네트워크에 대한 inverse domain은 설정할 필요가 없습니다. 상기 5가지 분류를 문법위주로 설명하면 다음과 같습니다.

첫째, 캐시 네임서버, 로컬 호스트 관련 설정입니다.

일반적으로 모든 ODS에서 캐시 네임서버와 로컬호스트에 관한 설정은 동일하며 아래와 같은 형식을 그대로 사용합니다.

```
// 캐시네임서버 및 로컬호스트, 그리고 로컬네트워크의 inverse domain Zone에 대한 // 설정은 아래와 같은 설정을 디폴트로 사용한다.
 zone "." IN {
            type hint;
            file "named.ca";
  };

  zone "localhost" IN {
            type master;
            file "localhost.zone";
            allow-update { none; };
  };

  zone "0.0.127.in-addr.arpa" IN {
            type master;
            file "named.local";
            allow-update { none; };
  };
```

둘째, 운영하고자 하는 실제 FQDN Zone 설정은 아래의 문법 형식을 따릅니다.

```
zone "ORIGIN" IN {
// ORIGIN 이라는 것은 설정할 domain name을 의미합니다.
// 이 ORIGIN은 zone 파일에서 @으로 표현을 하게 됩니다.
//즉, zone file 에서 @이란 named.conf의 ORIGIN에 설정된 domain name을 의미.

type master;
//  primary domain을 설정하고 있다는 것을 정의

file /path/filename;
// Zone 파일의 경로를 지정

allow-update { none; };
//dynamic update 시도를 허락할 ip 대역이나, dnssec key를 지정
// nsupdate라는 유틸리티를 이용하여 로컬, 또는 원격에서 네임서버의
//재시작 없이 record를 수정/삭제/생성 할 수 있게 해 주는 기능을 의미
//기본 값은 none
};
```

셋째, inverse domain의 경우 ISP로부터 할당을 받고 앞쪽 서브넷 관리자가 위임 작업을 해주어야 합니다.. 필수적인 사항이 아니므로 본 지침서에서는 설정 방법만 설명하고 넘어가도록 하겠습니다..

inverse domain은 reverse mapping을 가능하게 하며, reverse mapping 이라는 것은 ip address로 domain을 찾는 것을 의미합니다.

inverse domain의 정의 역시 운영하고자하는 FQDN Zone을 정의하는 것과 동일합니다.

```
...
zone "ORIGIN" IN {
   type master;
   file /path/filename;
   allow-update { none; };
};
...
```

inverse domain의 ORIGIN은 네트워크대역.in-addr.arpa로 설정합니다.
네트워크 대역은 거꾸로 표현한다는 것에 주의합니다. 예를 들어 1.2.3.0 네트워크에 대한 inverse domain을 설정한다면, 3.2.1.in-addr.arpa가 된다는 것입니다. 각 클래스별 예제를 참고하도록 합니다.

```
A class 1.0.0.0    =] 1.in-addr.arpa
B class 162.1.0.0 =] 1.162.in-addr.arpa
C class 210.1.1.0 =] 1.1.210.in-addr.arpa
```

넷째, secondary 네임서버의 named.conf 설정은 아래의 문법 형식을 따르며 FQDN Zone을 정의하는 것과 동일하며 master 네임서버의 위치를 기록하는 부분만 다릅니다.

```
zone "ORIGIN" IN {
//ORIGIN은 secondary로 정의 할 domain 이름
      type slave;
// secondary 네임서버임을 정의
      file /path/filename
      masters { PRIMARY_SERVER_IP; };
//primary name server의 ip를 적습니다.
};
```

```
// secondary name server 설정


zone "my-domain.re.kr" IN {
        type slave;
        file "my-domain.re.kr-zone";
        masters { 192.168.0.1; };
};
```

③ named.conf 파일

상기의 문법형식에 따라 아래와 같이 named.conf 파일을 만들 수 있습니다.

```
options {
    version "unknown";
    directory "/var/named";
    dump-file "/var/tmp/named_dump.db";
    statistics-file "/var/tmp/named.stats";
    pid-file "/var/run/named.pid";
};

zone "my-domain.re.kr" IN {
        type master;
        file "my-domain.re.kr-zone";
        allow-update {none; };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
};
```

named.conf 작성이 완료 되었으면, 이제 named.conf에서 설정한 각 Zone에 대한 설정을 해주어야 합니다.

(2) Zone 파일 설정

Zone File은 BIND 설정 시 가장 중요한 도메인 데이터베이스 파일입니다. BIND 가동 시에 Zone File을 읽어 들여서 네임서버 서비스가 가동됩니다.

① Zone File의 역할 및 리소스 레코드

Zone File은 도메인을 IP 주소 또는 URL 등으로 변환해 주는 역할을 합니다. Zone File은 SOA 영역과 응답레코드 영역으로 나누어진다. Zone File에서 주의할 점은 FQDN(도메인명) 뒤에 꼭 "."가 존재해야만 완전한 도메인명으로 인식 된다는 것입니다.

다음은 Zone File을 영역별로 구분한 것입니다.

```
$TTL 86400      ; 1 day
@       IN SOA  ns.my-domain.re.kr. hostmaster.company.co.kr. (
                                2006102001 ; serial
                                21600      ; refresh (6 hours)
                                1800       ; retry (30 minutes)
                                1209600    ; expire (2 weeks)
                                86400      ; minimum (1 day)
                                )

                        IN      NS      ns1.my-domain.re.kr. ; 1차 네임서버
ns1.my-domain.re.kr     IN      A       192.168.1.53 ; 1차네임서버 IP 주소
                        IN      NS      ns2.my-domain.re.kr. ; 2차 네임서버
ns2.my-domain.re.kr     IN      A       192.168.2.53 ; 2차네임서버 IP 주소

$ORIGIN my-domain.re.kr.
www                     IN      A       192.168.1.21
ftp                     IN      A       192.168.1.22
```

SOA 영역

응답레코드 영역

SOA(Start Of Authority) 레코드부분만 다시 별도로 분류하여 설명하면 다음과 같습니다.

```
$TTL 86400      ; 1 day
@               IN SOA  ns.my-domain.re.kr. hostmaster.company.co.kr. (
                                2006082942 ; serial
                                21600      ; refresh (6 hours)
                                1800       ; retry (30 minutes)
                                1209600    ; expire (2 weeks)
                                86400      ; minimum (1 day)
                                )
```

Zone File은 항상 SOA 레코드로 시작한다. SOA 레코드는 해당 도메인에 대해 네임서버가 인증(authoritative)된 자료를 갖고 있음을 의미하며, 자료가 최적의 상태로 유지, 관리될 수 있도록 합니다.

SOA 레코드에서는 priamry 서버와 secondary 서버간의 data를 유지하는 시간, cache 한 정보들을 얼마동안 유지할 것인지 등을 정의하게 됩니다.

칼럼	설명
첫째 칼럼	· Zone 파일에 대한 도메인 네임을 지칭 · '@' or FQDN
둘째 칼럼	· 클래스 명 · HS, HESIOD, CHAOS와 같은 클래스도 존재하지만 일반적으로 IN만이 사용
셋째 칼럼	· 리소스 레코드의 유형을 지정하는 필드 · SOA를 기재
넷째 칼럼	· Primary 네임 서버의 도메인 네임
다섯째 칼럼	· 관리자 Email 주소 · 일반적인 Email 표기법에서 '@'를 '.'으로 바꾸어 표기 ex) hostmaster@company.co.kr은 hostmaster.company.co.kr.로 표기

이메일은 해당 도메인에 문제가 발생할 경우 이를 알리는 Contact 포인트입니다.

다음은 “SOA" 영역 필드들에 대한 설명입니다.

필드	설명
Serial	secondary 네임 서버가 이 시리얼 번호를 보고 정보가 갱신되었는지 아닌지를 판단하게 됩니다. 현재의 것보다 숫자가 높을 경우 정보를 업데이트 하게 됩니다. primary 네임 서버에서 설정을 변경한 후에는 반드시 시리얼을 높여줄 필요가 있습니다. Serial은 일반적으로 YYYYMMDDNN의 형식으로 표기합니다.
Refresh	secondary 네임 서버가 primary 네임 서버에 접속해서 설정 내용이 갱신 되었는지 확인하는 시간 주기를 나타냅니다. 네트워크의 변경이 잦아 zone 파일이 자주 수정된다면 3H(10800) 정도로 설정합니다. zone이 안정되는 시점에서는 일반적으로 6H(21600) - 12H로 설정합니다.
Retry	secondary 네임 서버가 primary 네임 서버에 접속해서 설정 내용을 읽어 들일 수 없을 경우 재요청 하는 시간주기입니다. Refresh 기간보다 적을 때 의미가 있으며, 대부분의 경우 30M(1800) - 1H로 설정합니다.
Expire	secondary 네임 서버가 primary 네임 서버에서 설정 내용을 읽어 들일 수 없을 경우 언제까지 계속해서 정보를 요청할 것인지 지정하는 부분으로 만약 해당 시간이 지나버리면 기존의 secondary 네임 서버의 저장 내용은 무효가 됩니다. 보통 1W - 2W(1209600)로 설정합니다.
Minimum	타 네임 서버가 본 zone에 기술된 자료를 가지고 갔을 경우, 그 자료에 대한 유효기간(캐시에 살아 있는 기간)을 설정합니다. TTL 값이 명시되지 않은 레코드는 본 값을 기본으로 갖게 됩니다. 특정 레코드가 변경되었을 때 이것이 인터넷에 전파되어 업데이트 되는 주기는 전적으로 이 Minimum 값에 의존합니다. 일반적으로 SOA에서는 1D(86400)를 설정하여 전체 레코드에 적용하고, 잦은 변경이 예상되는 레코드만 명시적으로 1H - 3H 정도로 낮추는 방법을 사용합니다. 0은 캐싱을 하지 말라는 의미이다.

응답레코드 영역을 살펴보면 아래와 같이 "A" 라는 Resource Record 형식을 이용하여 Zone파일을 구성합니다.

```
$ORIGIN my-domain.re.kr.
www                 IN      A       192.168.1.21
ftp                 IN      A       192.168.1.22
```

② Zone File 생성

"my-domain.re.kr" Zone의 Zone 파일을 생성하기 위해 “/var/named” 위치에 파일명을 "my-domain.re.kr-zone" 로 하여 아래와 같이 설정해준 뒤 저장합니다.

```
$TTL 86400      ; 1 day
@       IN SOA  ns.my-domain.re.kr. hostmaster.company.co.kr. (
                                2006102001 ; serial
                                21600      ; refresh (6 hours)
                                1800       ; retry (30 minutes)
                                1209600    ; expire (2 weeks)
                                86400      ; minimum (1 day)
                                )

                        IN      NS      ns1.my-domain.re.kr. ; 1차 네임서버
ns1.my-domain.re.kr.    IN      A       192.168.1.53 ; 1차네임서버 IP 주소
                        IN      NS      ns2.my-domain.re.kr. ; 2차 네임서버
ns2.my-domain.re.kr.    IN      A       192.168.2.53 ; 2차네임서버 IP 주소

$ORIGIN my-domain.re.kr.
www                 IN      A       192.168.1.21
ftp                 IN      A       192.168.1.22
```

(3) named.ca 설정

ROOT name server 의 IP 주소를 정의하여, 더 빨리 찾을 수 있도록 최적화 되어 있는 file입니다. 이 파일은 네임서버를 구축하려는 자가 작성하는 것이 아니라 "ftp://rs.internic.net/domain"에서 구할 수도 있고 ROOT SERVER 에 query를 날려서 cache server list를 만들어 사용합니다. named.ca 파일의 전형적인 위치는 "/var/named" 디렉터리입니다.

ROOT SERVER에 query를 날려서 named.ca를 생성하기 위해서는 명령 프롬프트상에서 다음과 같이 명령어를 입력하면 됩니다.

```
#/usr/local/bin/dig @a.root-servers.net . ns > /var/named/named.ca
```

(4) named.local 설정

loop back IP address에 대한 reverse mapping을 정의한 파일입니다. reverse mapping이란 IP address로 domain name을 찾는 것을 말합니다. reverse mapping 설정을 하는 것을 inverse domain을 설정한다고 하기도 합니다.

named.local의 전형적인 위치는 "/var/named" 이며, 파일의 내용은 아래 기술한 내용을 디폴트로 하여 그대로 사용하면 됩니다.

```
@       IN      SOA     localhost. root.localhost. (
                        2006092700 ; serial
                        28800 ; refresh
                        14400 ; retry
                        3600000 ; expire
                        86400 ; default_ttl
                        )
@       IN      NS      localhost.
1       IN      PTR     localhost.
```

바) BIND 설치 테스트

BIND 설치 및 설정이 완료되었다면 네임서버 구축 과정이 끝난 것이므로 정상 가동 유무를 확인해 보아야 합니다. 테스트에는 네임서버를 운영하고 관리하는데 문제를 발견하고 해결하기 위한 도구인 dig (Domain Information Groper)를 이용하면 편리합니다. dig는 사용이 간결하고 출력이 상세하여 주로 사용되는 대표적인 DNS 도구 중 하나입니다.

dig 명령어의 간단한 사용법은 다음과 같습니다.

```
dig [@네임서버] 도메인 [쿼리타입] [+쿼리옵션]
```

구성	의미
네임서버	사용할 네임서버를 의미하는 것으로 생략되면 기본적으로 자신이 설정된 기본 DNS Server를 이용
도메인	정보를 구하고자 하는 도메인
쿼리-타입	질의문의 속성을 의미하는 것으로 A, SOA, NS등을 의미 RFC 1035에 정의되어 있으며 생략되면 'a'가 기본 값
쿼리-클래스	요청된 질의문의 Network Class를 의미 생략되면 'in'이 기본 값 -in : Internet Class Domain -any : All/Any Class Information

BIND가 올바르게 설치되었는지에 대한 테스트 순서는 다음과 같습니다.

① BIND 구동
설치 확인을 위하여 named 데몬을 구동 시킵니다.

```
#/usr/local/sbin/named
```

② dig 명령어 실행
네임서버 127.0.0.1을 통해 "my-domain.re.kr"의 A 레코드를 검색합니다.

BIND가 정상적으로 설치되었다면 그 결과는 아래와 같을 것입니다.

```
dig @127.0.0.1 my-domain.re.kr A
```

```
; <<>> DiG 9.3.2 <<>> @127.0.0.1 my-domain.re.kr A
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; -]]HEADER[[- opcode: QUERY, status: NOERROR, id: 1295
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;my-domain.re.kr.                IN          A

;; ANSWER SECTION:
my-domain.re.kr.          86400   IN          A       192.168.1.21

;; AUTHORITY SECTION:
my-domain.re.kr           86400   IN          NS      ns1.my-domain.re.kr
my-domain.re.kr           86400   IN          NS      ns2.my-domain.re.kr


;; ADDITIONAL SECTION:
ns1.my-domain.re.kr.    86400   IN          A       192.168.1.53
ns2.my-domain.re.kr.    86400   IN          A       192.168.2.53


;; Query time: 15 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Sep 21 14:47:27 2006
;; MSG SIZE  rcvd: 184
```

4. DNS 구성 및 설정

가. 도메인의 네임서버 구성

네임서버는 도메인의 존 데이터를 저장하는 데이터베이스 서버입니다.
본 장은 인터넷 상에 도메인이 실제로 존재하게 되는 물리적 장소로써의 네임서버 구성 및 설정 사항을 제시합니다.

1) 도메인 네임서버 구성의 기본 충족 요건

도메인의 네임서버는 다음의 요건을 충족하는 네임서버를 사용합니다.

1. 정상 가동 운영 중인 네임서버
2. 리커시브 서비스 제한 설정된 네임서버
3. 2대 이상의 네임서버

정상 가동 운영 중인 네임서버

도메인의 네임서버는 UDP 53번 포트를 사용한 DNS 질의에 대해 DNS 응답 가능한 상태의 네임서버를 사용합니다.

DNS 질의에 반응이 없는 네임서버를 도메인의 네임서버로 설정하는 경우가 예상보다 많이 발견되고 있습니다. 이미 설치되어 운영 중인 네임서버를 도메인의 네임서버로 선택할 때, 반드시 해당 네임서버가 정상 운영 중인지 확인하고 선택하는 것이 필요합니다.

네임서버가 위치해 있는 사이트 내부에서는 DNS 질의응답에 문제가 없지만, 외부 인터넷에서 질의하는 경우, UDP 응답이 없는 경우가 있을 수 있습니다. 중간에 놓인 방화벽 등의 장비에 의해 DNS 질의응답이 차단되고 있을 수가 있습니다. 외부 인터넷에서 네임서버로 도메인에 대한 질의를 했을 때 정상 응답이 이루어지고 있는지를 확인할 필요가 있습니다.

리커시브 서비스 제한 설정된 네임서버

도메인 네임서버는 외부 인터넷에 대해 리커시브(recursive) 서비스를 제공하지 않는 네임서버를 사용하는 것이 안전합니다.

도메인 네임서버는 도메인 존에 대하여 위임된 네임서버로써, 도메인의 authoritative 네임서버이어야 합니다. 도메인의 authoritative 네임서버라는 것은 해당 도메인의 존 설정을 가지고 있는 네임서버를 의미합니다. 도메인 존이 설정된 네임서버는 해당 도메인에 대한 질의에 대하여 authoritative 응답을 합니다.

도메인의 네임서버는 리커시브 네임서버 기능을 겸하지 않고, authoritative 네임서버로만 동작하는 네임서버를 사용할 것을 권고합니다. BIND DNS와 같이 리커시브 기능과 authoritative 기능 모두를 지원하는 네임서버의 경우, 되도록 리커시브 기능을 해제한 네임서버를 사용하는 것이 바람직합니다.

이는 리커시브 서비스가 제한 없이 허용된 상태의 네임서버는 DNS 캐시 포이즈닝 공격 및 DDoS 공격에 악용될 수 있는 등 여러 가지 보안 침해 사고가 발생할 소지를 안고 있기 때문입니다.

도메인의 네임서버를 authoritative 네임서버와 함께 리커시브 네임서버로 겸용해야 하는 상황이라면, 리커시브 질의응답을 제공할 대상 호스트의 IP 주소 대역을 제한 설정하는 것이 바람직합니다. 리커시브 서비스 제한 설정 후에는 외부 인터넷 일반에 대해 리커시브 제공 기능이 적절하게 제한되어 있는지를 확인할 필요가 있습니다.

2대 이상의 네임서버

도메인의 네임서버는 최소한 2대 이상으로 구성하는 것이 바람직합니다.

이는 도메인의 안정성 유지를 최소한의 권고 사항입니다. 1대의 네임서버를 사용하여 도메인의 네임서버를 구성했을 때, 이 단일한 네임서버에 문제가 발생하여 동작이 중단되는 경우, 더 이상 도메인에 대한 DNS 질의에 응답을

할 수 있는 네임서버가 없기 때문에 도메인을 사용하는 인터넷 서비스 전체가 중단되는 심각한 장애가 발생할 수 있습니다.

2대 이상의 네임서버로 구성했을 때에는 2대의 네임서버거가 동시에 시스템 문제가 발생할 확률은 극히 적으므로 한 대가 응답할 수 없는 상황이 되도 또 다른 한 대로 DNS 정상응답 상태를 유지할 수 있습니다.

최근에는 자연적인 시스템 장애 외에 인위적인 서비스 방해를 목적으로 하는 분산서비스 거부(DDoS) 공격에 의해 네임서버가 정상적인 서비스를 제공하지 못하는 상황이 발생할 위험이 증가하고 있습니다. DDoS 공격의 가능성을 고려한다면 도메인의 네임서버를 2대의 네임서버로 구성하는 것이 충분하지 않을 수 있습니다. 도메인의 인터넷 서비스 성격과 서비스 안정성 요구 정도를 판단하여 DDoS 공격에 대한 최소한의 저항력을 가질 수 있도록 네임서버 대수를 적절히 조정할 필요성이 있습니다.

2대이상의 네임서버로 도메인의 네임서버 구성 요건에는 보다 강화된 2가지 구성 요건을 들 수 있다.

1) 모든 네임서버가 동일한 서브 네트워크에 있지 않도록 구성
2) 네임서버는 최소 둘 이상의 ISP 네트워크(서로 다른 ASN의 네트워크)에 분산 구성할 것을 제시

이는 서브 네트워크를 제공하는 라우터의 단일 인터페이스의 장애, 특정 ASN 번호를 갖는 ISP 망의 장애에 대해서 도메인의 모든 네임서버가 영향을 받아 장애를 겪는 상황을 방지하기위한 구성 요건입니다. 도메인의 인터넷 서비스 성격을 감안하여 최상 수준의 서비스 가용성 유지가 요구되는 경우에 추가 구성요건에 따라 구성하는 것이 바람직합니다.

2) 네임서버 이중화 및 네트워크 분산 구성

□ 설정 기준 (참고사항)

도메인의 네임서버는 2식 이상의 네임서버로 구성 권고
도메인의 네임서버는 서로 다른 서브 네트워크에 분산 구성 권고
도메인의 네임서버는 서로 다른 ISP 망에 분산 구성 권고

□ 설정의 필요성

네임서버는 도메인 존 데이터를 저장하여 인터넷에 제공합니다. 도메인 존 데이터는 도메인을 사용하는 인터넷 서비스 접속에 필요한 정보를 가지고 있습니다. 만일 도메인 존 데이터가 네임서버의 장애로 인해 인터넷에 제공될 수 없는 상태가 된다면, 이 도메인을 사용하는 인터넷 서비스의 접속이 불가능한 상태가 됩니다. 도메인 존 데이터는 인터넷 사용자의 호스트가 언제나 조회 질의하여 응답 받을 수 있는 상태를 유지하는 것이 필요합니다.

네임서버의 이중화는 도메인 존 데이터가 언제나 인터넷으로부터의 질의에 응답 가능한 상태를 유지하기 위한 요건입니다. 물론 도메인의 인터넷 서비스가 항상 접속 가능한 상태를 유지하지 않아도 무방한 서비스라면, 네임서버 이중화 구성의 필요성이 없을 수 있습니다.

네임서버 서버 플랫폼의 이중화와 함께 네트워크 분산 구성이 필요합니다. 이는 네임서버가 속해 있는 네트워크에 발생할 수 있는 네트워크 장애에 대응하기 위함입니다.

높은 수준의 인터넷 서비스 가용성을 유지할 필요가 있는 중요한 사이트인 경우에는 네임서버 이중화 및 분산구성 요건을 충족하도록 구성하는 것이 바람직합니다.

최근에는 도메인의 안정성 자체보다도 DDoS 공격 위협에 대한 대응으로써 다수 네임서버를 사용한 다중화와 서로 다른 ISP 네트워크에 분산 구성함으로써 DDoS 공격에 대한 저항력의 강화 필요성이 증가하고 있는 추세입니다.

□ 설정 방법

네임서버의 이중화 및 네트워크 분산구성은 서버 시스템 및 네트워크 구성과 관련된 사항입니다. 따라서 구체적인 네임서버 S/W의 구성사항이 아닌 네임서버의 시스템 구성 요건과 네트워크 구성 요건을 중심으로 설명합니다.

네임서버의 이중화 및 네트워크 분산구성 설정은 비교적 많은 비용이 소요될 수 있는 사항입니다. 인터넷 서비스의 가용성 요구 정도를 판단하여 적절한 요건의 충족 수준으로 구성하는 것이 필요합니다. 365일 중단 없는 인터넷 서비스 제공이 요구되는 사이트인 경우, 네임서버의 다중화 및 네트워크 분산구성 요건까지 충족하는 것이 필요할 수 있습니다.

1) 도메인의 네임서버는 최소 2식 이상의 서버 시스템을 사용하여 구성합니다.

이 요건은 최소한의 요건으로써 가능한 한 충족하는 것이 필요합니다.

도메인의 네임서버로 사용할 2식 이상의 서버 시스템을 준비합니다. 시스템 장애가 동시에 발생하지 않도록 서로 분리된 서버 시스템을 사용합니다.

2식 이상의 네임서버 구성을 권고하는 것은 서버 시스템 장애에 대응하는 것이 주된 목적입니다.

근래에는 DDoS 공격 위협이 증가하고 있음에 따라 중요한 서비스를 운영하고 있는 사이트의 경우, 3식 이상 네임서버로 구성 등 보다 강화된 네임서버 다중화 구성을 검토할 필요가 있습니다.

도메인의 네임서버들은 매스터/슬레이브 구성 절차에 따라 구성 설정합니다. 2식 이상의 네임서버로 구성하는 경우, 각 네임서버의 도메인 존 데이터를 항상 동일하게 유지해야 합니다. 데이터베이스 시스템의 이중화 경우와 마찬가지로 네임서버의 경우에도 데이터 동기화가 중요한 이슈입니다. DNS 프로토콜은 네임서버 다중화에 따른 도메인 존 데이터의 자동 동기화 관리기능을 지원하기 위한 표준절차와 기능을 정의하고 있습니다. 도메인의 매스터/슬레이브 네임서버 구성은 DNS 표준 프로토콜을 활용하여 네임서버 간에 도메인 존 데이터의 동기화를 자동으로 수행하도록 구성하는 방법에 해당합니다.

도메인의 매스터/슬레이브 네임서버 구성 절차는 “3) 도메인의 매스터/슬레이브 네임서버 구성 설정” 장에서 구체적으로 제시하고 있습니다.

2) 도메인의 각 네임서버 IP 주소는 서로 다른 서브 네트워크의 IP 주소로 할당 구성합니다.

서로 다른 서브 네트워크의 IP 주소 사용 요건은 국지적인 네트워크 장애에 대응하기 위한 요건입니다. 도메인의 모든 네임서버가 동일한 서브 네트워크에 속하도록 구성한 경우, 이 서브 네트워크에 한정된 장애가 발생하는 경우, 모든 네임서버가 통신 불능 상태가 됨으로써 도메인의 인터넷 서비스에 접속 불능 장애가 발생하게 됩니다. 이러한 경우를 방지하기 위해 네임서버의 네트워크 분산 구성 요건을 권고하고 있습니다.

여기에서의 서브 네트워크란 라우터 기능을 하는 네트워크 장비의 단일한 물리적 인터페이스를 사용하여 여기에 설정된 네트워크를 지칭합니다. 인터페이스에 장애가 발생하는 경우, 이 인터페이스의 서브 네트워크에 속한 모든 호스트는 접속 장애 상태에 있게 됩니다. 서브 네트워크를 제공하는 인터페이스는 라우터 장비의 인터페이스인 경우가 대부분이지만, 라우팅 기능을 갖는 방화벽 장비의 인터페이스일 수도 있습니다.

서브 네트워크는 인터페이스에 실제로 설정된 서브 네트워크 주소 범위를 기준으로 합니다. 예를 들어 도메인의 네임서버가 각각 192.168.1.53과 192.168.1.153을 주소로 사용하고 있다고 가정합니다. 이 네트워크에 대하여 라우팅 기능을 제공하고 있는 물리적 인터페이스에 192.168.1.254/24와 같이 주소가 설정되어 있다면, 서브 네트워크는 192.168.1.1~192.168.1.253의 IP 주소 범위를 갖고 있으므로, 이 2식의 네임서버는 동일한 서브 네트워크에 속해 있는 상태입니다. 이 경우, 네트워크 192.168.1.0/24 네트워크를 2개로 분리하여 192.168.1.0/25를 제공하는 물리 인터페이스와 192.168.1.128/25를 제공하는 물리 인터페이스로 분리하여 구성한다면, 192.168.1.53과 192.168.1.153의 주소는 서로 다른 서브 네트워크에 위치한 네임서버 구성 요건을 충족할 수 있습니다. 이 작업은 네트워크 관리자에 의한 검토가 필요한 구성 작업입니다.

서로 다른 서브 네트워크에 네임서버 주소가 분리되면서 네트워크 인터페이

스 장애 시 네임서버 전체에 장애가 발생하는 것을 방지할 수 있습니다. 두 개의 물리적 인터페이스에 동시에 장애가 발생하는 경우는 희소하다는 경험적 사실에 의거한 것입니다. 물론 이 경우에 라우터 장비 자체에 장애가 발생한 경우나 라우터의 외부 인터넷 연동 인터페이스에 장애가 발생한 경우에는 모든 네임서버에 접속 불능 장애가 발생할 가능성이 있습니다. 이러한 장애 발생을 예방하기위해서는 서로 다른 라우터 장비의 인터페이스가 제공하는 서브 네트워크에 네임서버들이 분산 구성되도록 구성할 필요성이 있습니다.

3) 도메인의 각 네임서버를 서로 다른 ISP 망에 분산 구성합니다.

세 번째 요건은 가장 비용이 많이 소요되는 분산 구성 요건으로써, 아주 중요한 인터넷 서비스를 제공하는 사이트인 경우에 한하여 반영 적용을 고려할 수 있는 사항이라 할 수 있습니다.

도메인의 네임서버를 2개 이상의 서로 다른 ISP 망에 설치 구성합니다. 보다 정확한 구성 요건은 “서로 다른 ASN을 갖는 네트워크에 네임서버를 분산 구성”입니다. 흔히 ISP 망은 독자적인 ASN을 갖습니다. ASN이란 Autonomous System Number의 약자로써, 독자적인 라우팅 체계를 갖고 운영하는 네트워크에 부여하는 번호입니다. ASN을 갖는 네트워크는 기본적으로 타 네트워크와 2개 이상의 이중화된 연동을 갖는 네트워크입니다. 주로 ISP와 주요한 금융서비스 사이트, 정부기관 사이트 등이 ASN 번호를 보유하고 있습니다. 따라서 서로 다른 ASN을 갖는 네트워크에 분산 구성함이란 현실적으로는 서로 다른 ISP 망에 분산 구성함을 의미하는 것으로 이해할 수 있습니다.

서로 다른 ISP 망(서로 다른 ASN의 망)에 분산 구성한다는 것은 특정 ISP의 심각한 네트워크 장애에 대응하기 위한 조치를 취한다는 의미입니다. 단일한 ISP로부터 인터넷 연결 서비스를 받고 있을 때, 이 ISP에 네트워크 장애가 발생하는 경우, 도메인의 네임서버 역시 인터넷으로부터 접속이 되지 않는 장애가 발생할 수 있습니다. 이를 방지하기 위해 둘 이상의 ISP에 네임서버를 분산 구성하는 대응조치를 할 수 있습니다.

위와 같이 네임서버 이중화 및 네트워크 분산 구성 요건은 본래 네임서버

시스템과 네트워크에 발생할 수 있는 각종 장애에 효과적으로 대응하기 위한 구성 방법으로 권고하고 있는 사항입니다. 도메인의 안정성을 제고하기 위한 권고사항입니다. 하지만 근래에는 DDoS 공격 위협과 같은 보안침해 위협에 효과적으로 대응하기 위한 측면에서 고려되어야 할 사항이 되고 있습니다. 도메인의 구성 네임서버 시스템 대수를 증가시키고 서로 다른 네트워크에 네임서버를 분산시킴으로써 DDoS 공격에 대한 저항능력을 향상시키기 위한 조치로써 네임서버의 분산구성이 강화되고 있습니다.

□ 인터넷 서비스 영향

도메인의 네임서버 이중화 또는 네트워크 분산구성이 미흡한 경우, 도메인의 안정성은 취약한 상태이게 됩니다.

도메인을 단일 네임서버로 구성하는 경우, 이 네임서버의 시스템 장애 또는 네임서버 S/W 프로세스의 동작중단 장애 발생 시 이 도메인의 인터넷 서비스 전체에 서비스 접속 중단상태가 발생하게 됩니다.

DDoS 공격 대상이 될 수 있는 위험을 갖는 중요 인터넷 서비스 사이트의 경우, 네임서버의 구성 대수를 보다 증가시키거나 네트워크 분산 구성을 고려하는 것이 필요합니다. DDoS 공격 형태 중 가장 위험한 경우는 바로 도메인 네임서버에 대한 DDoS 공격입니다. 네임서버가 DDoS 공격으로 인해 정상적 동작이 중단되는 경우, 도메인의 인터넷 서비스 전체가 마비될 수 있는 위험성 때문입니다.

3) 도메인의 매스터/슬레이브 네임서버 구성 설정

□ 설정 기준 (필수사항)

- 도메인의 모든 네임서버에 도메인 존 설정
- 도메인의 매스터 네임서버와 슬레이브 네임서버 구성 설정

□ 설정의 필요성

도메인의 모든 네임서버는 도메인의 존 데이터에 대해 authoritative 응답을 할 수 있어야 합니다. 이것은 필수사항입니다.

네임서버가 도메인에 대하여 authoritative 응답 가능 필수사항
1) 도메인의 존 설정
2) 도메인의 모든 네임서버가 존 데이터를 보유하고 있는 상태

만일 도메인의 네임서버 중 일부 또는 전체에 도메인 존 설정이 누락되어 있다면, 이 도메인에 대한 DNS 질의응답 절차에서 응답지연 또는 응답실패가 발생하게 됩니다. 결과적으로 이 도메인을 사용하고 있는 인터넷 서비스의 품질 저하가 발생합니다.

설정미흡의 경우에 따라, 심각한 보안 침해 문제가 발생할 수 있습니다. DNS 캐시 포이즈닝(cache poisoning) 공격에 노출될 수 있습니다.

□ 설정 방법

도메인의 네임서버는 도메인 존 데이터 관리 측면에서 매스터 네임서버와 슬레이브 네임서버로 구분합니다.

매스터 네임서버와 슬레이브 네임서버의 도메인 존 설정 방법에는 차이가 있습니다.

네임서버 S/W 마다 설정방식이 다르므로, 먼저 일반적인 설정 방법을 다음에 제시하고, 이어 BIND DNS 네임서버와 Windows DNS 서버의 설정방식을 각각 예시합니다.

도메인의 매스터 네임서버의 존 설정 절차

1. 네임서버에서 도메인을 “매스터 존”으로 지정하여 설정합니다.
2. 도메인 존 데이터를 설정합니다. 주로 존 파일로 작성하여 설정합니다.

도메인의 슬레이브 네임서버의 존 설정 절차

1. 네임서버에서 도메인을 “슬레이브 존”으로 지정하여 설정합니다.
2. 도메인의 매스터 네임서버 IP 주소를 지정하여 설정합니다.

다음은 BIND DNS 네임서버에서의 도메인 존 설정 방법입니다.

도메인 존 설정 설정방법 예시 환경

다음과 같은 도메인과 네임서버를 사용한다고 가정하여 설정방법을 예시합니다.

도메인 : my-domain.re.kr
매스터 네임서버 : ns1.my-domain.re.kr (192.168.1.53)
슬레이브 네임서버 : ns2.my-domain.re.kr (192.168.2.53)
슬레이브 네임서버 : ns3.my-domain.re.kr (192.168.3.53)
매스터 네임서버 존 파일 저장 디렉토리 : /var/named

※ 최근에는 BIND DNS 설치 시 보안을 위해 가상 루트 디렉토리(chroot)를 적용하는 경우가 많습니다. 이때 환경설정 파일 디렉토리와 존 파일 디렉토리는 주로 /var/named/chroot 하위에 위치하게 됩니다.

도메인 존 지정 설정

BIND DNS 환경설정 파일인 named.conf 파일에 다음과 같은 사항을 추가 설정합니다.

매스터 네임서버 경우:

```
zone "my-domain.re.kr" IN {
    type master;                // “매스터 존”으로 지정
    file "my-domain.kr.zone";  // 도메인 존 파일명 지정
    allow-transfer { 192.168.2.53; 192.168.3.53; };
          // 도메인의 슬레이브 네임서버에 대해 존 전송 허용 설정
};
```

슬레이브 네임서버 경우:

```
zone "my-domain.re.kr" IN {
    type slave;                 // "슬레이브 존"으로 지정
    masters { 192.168.1.53; }; // 매스터 네임서버 IP 주소 지정
    allow-transfer { none; };  // 타 서버로 존 전송 차단 설정
};
```

도메인의 매스터 네임서버에서 도메인 존 파일 설정

BIND DNS 에서는 도메인 존 데이터를 주로 존 파일로 작성하여 네임서버에 반영합니다. 작성된 존 파일은 named.conf에서 지정한 디렉토리에 저장합니다. 여기 예시에서는 /var/named 디렉토리에 저장합니다.

다음은 도메인의 SOA 레코드와 네임서버 관련 레코드를 중심으로 예시한 도메인 존 파일의 내용입니다.

```
$ORIGIN my-domain.re.kr.
$TTL 300
@           SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr (
                    2009090101    ; serial
                    1800          ; refresh (30 minutes)
                    300           ; retry (5 minutes)
                    3600000       ; expire (5 weeks 6 days 16 hours)
                    300           ; minimum (5 minutes)
                    )
            NS      ns1.my-domain.re.kr.
            NS      ns2.my-domain.re.kr.
            NS      ns3.my-domain.re.kr.

ns1         A       192.168.1.53
ns2         A       192.168.2.53
ns3         A       192.168.3.53
```

다음은 Windows DNS 서버에서의 도메인 존 설정 방법입니다.

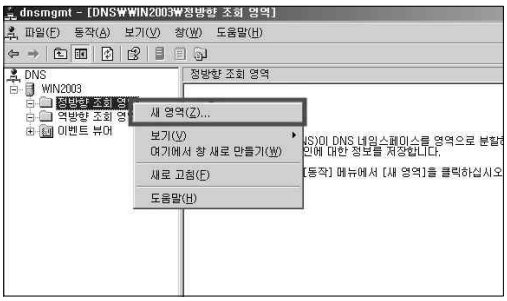
도메인 존 설정 설정방법 예시 환경

다음과 같은 도메인과 네임서버를 사용한다고 가정하여 설정방법을 예시합니다.

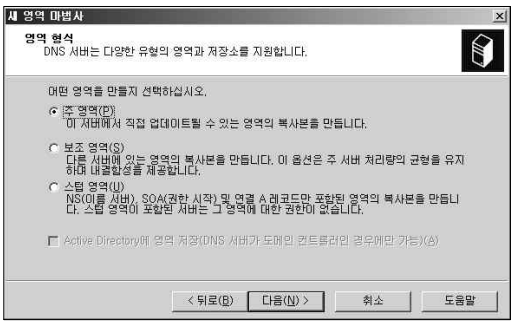
도메인 : my-domain.re.kr
매스터 네임서버 : ns1.my-domain.re.kr (192.168.1.53)
슬레이브 네임서버 : ns2.my-domain.re.kr (192.168.2.53)
슬레이브 네임서버 : ns3.my-domain.re.kr (192.168.3.53)

도메인의 매스터 네임서버에서 도메인 설정

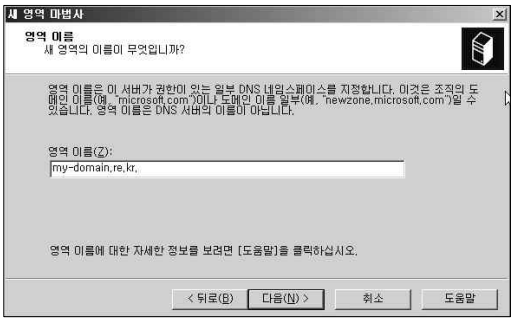
Windows DNS 서버의 “정방향 조회 영역”에서 “새 영역” 선택



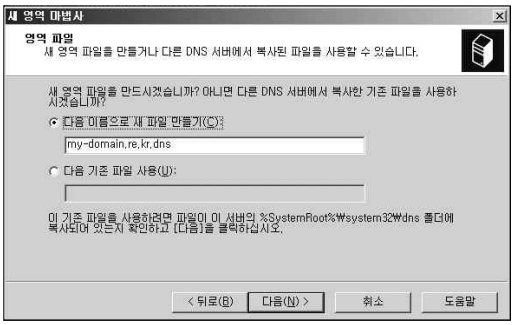
“새 영역 마법사”에서 도메인 존 타입으로 “주 영역” 선택, “매스터 존” 타입으로 지정



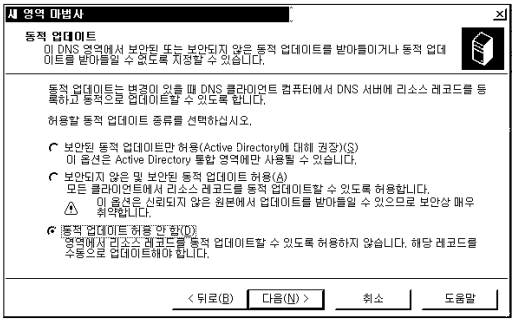
영역 이름에 도메인 존 네임 입력



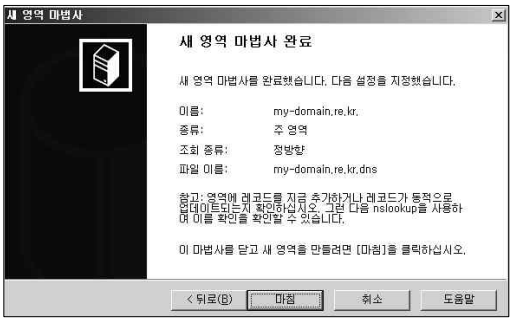
도메인 존 파일 지정. 여기서는 마법사를 통한 존 파일 생성.



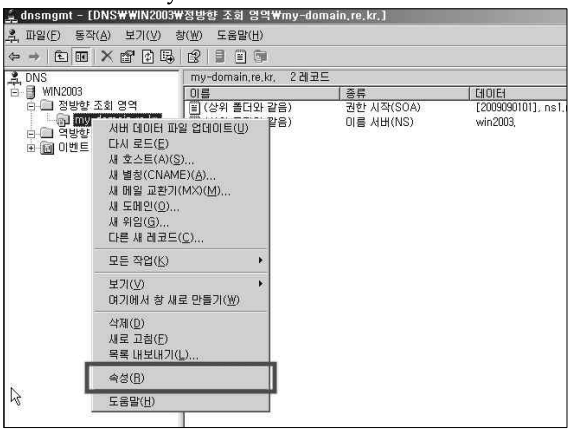
특별한 경우가 아니면, 보안을 위한 동적 업데이트 차단 설정



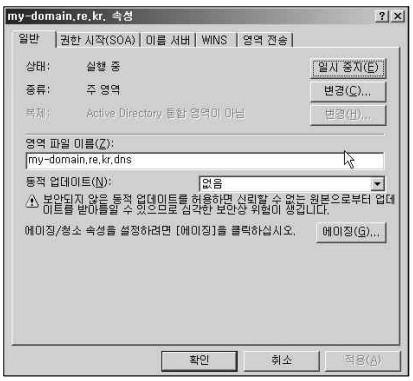
매스터 도메인 존 생성 완료



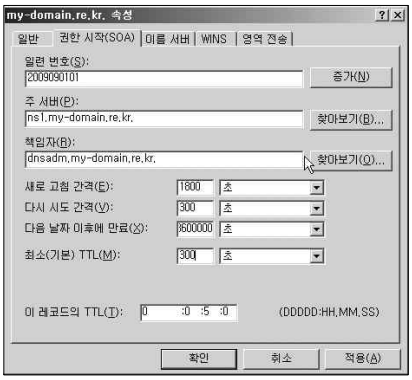
매스터 도메인 존의 기본 데이터 설정
도메인 존 my-domain.re.kr의 "속성" 선택



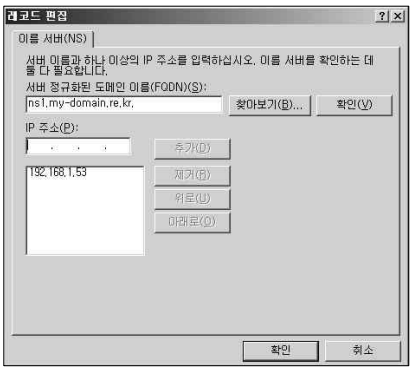
도메인 존의 일반 정보



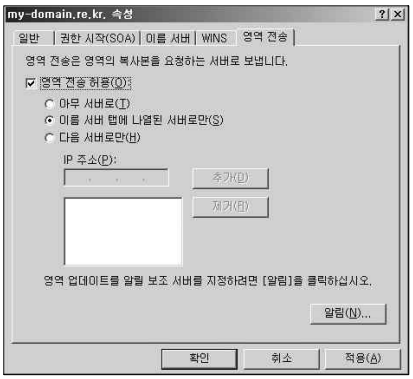
도메인 존의 SOA 레코드 값 설정



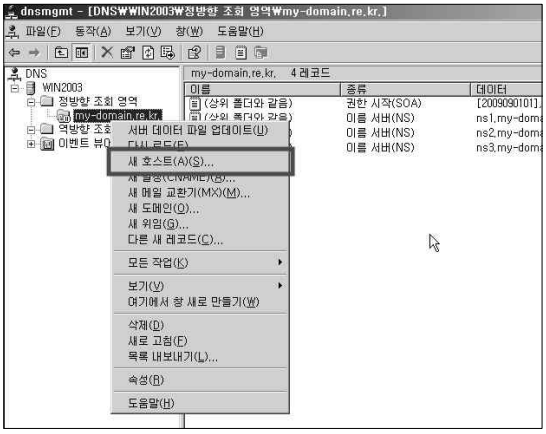
도메인 존의 NS 레코드 값 설정.
네임서버 ns2.my-domain.re.kr, ns3.my-domain.re.kr도 아래와 같은 방식으로 추가 설정



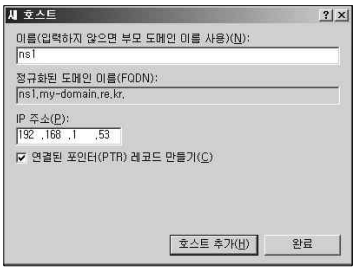
존 전송(Zone Transfer) 허용 제한 설정. 여기서는 슬레이브 네임서버에 한정하여 허용 설정



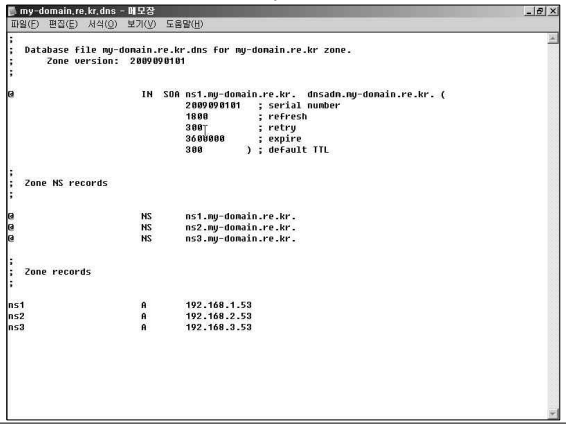
네임서버 호스트 레코드 생성 위해 “새 호스트” 선택



네임서버 호스트의 IP 주소 레코드 설정
이와 동일한 방법으로 ns2.my-domain.re.kr, ns3.my-domain.re.kr에 대한 호스트 네임 레코드 생성

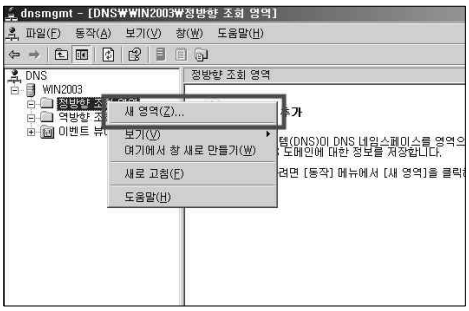


자동 생성 도메인 존 파일 내용 확인
Windows DNS 서버는 존 파일을 C:\Windows\system32\dns 디렉토리에 생성, 여기서는 my-domain.re.kr.dns 파일명으로 생성

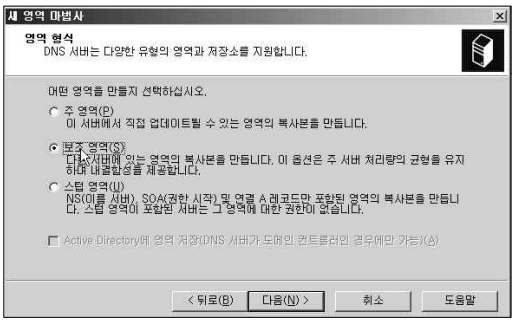


도메인의 슬레이브 네임서버에서 도메인 설정

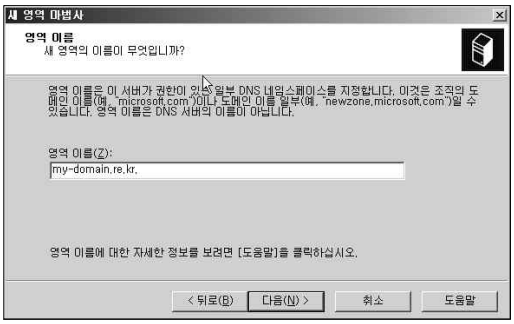
"정방향 조회 영역"에서 "새 영역" 선택



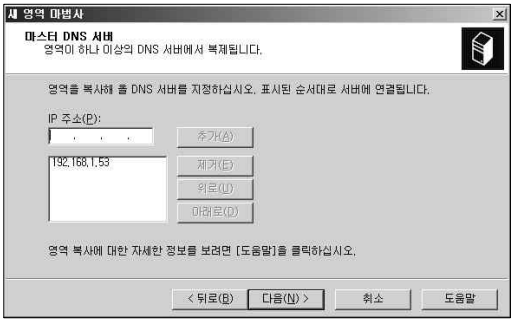
"새 영역 마법사"에서 도메인 존 타입으로 "보조 영역" 선택, "슬레이브 존" 타입으로 지정



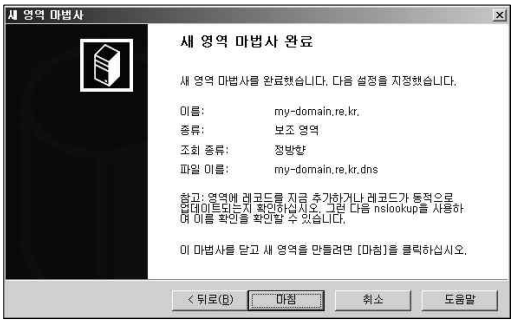
영역 이름에 도메인 존 네임 입력



매스터 존을 설정한 매스터 네임서버의 IP 주소 입력 설정



슬레이브 도메인 존 설정 완료



□ 인터넷 서비스 영향

도메인 존 설정이 누락된 네임서버가 있는 경우, 다음과 같은 장애현상이 발생할 수 있습니다.

- DNS 질의응답 실패로 인한 인터넷 서비스 접속 지연 또는 접속 실패
- DNS 캐시 포이즈닝(파밍) 공격에 취약

도메인의 일부 네임서버가 DNS 질의에 대해 아무런 응답이 없는 경우, 인터넷 서비스에 발생할 수 있는 문제점은 p. 138 “가. 위임된 네임서버 일부가 무응답 경우” 장에서 사례를 예시하여 구체적으로 설명합니다.

도메인의 일부 네임서버가 도메인 존 설정 누락으로 인해 authoritative 응답을 하지 못하는 경우, 인터넷 서비스에 발생할 수 있는 문제점은 p.153 “다. 위임된 네임서버 일부에 존 설정 누락 경우” 장의 사례 설명을 참조하시기 바랍니다.

도메인의 위임된 네임서버를 도메인 존 설정이 되어 있지 않은 리커시브 네임서버로 사용하는 경우도 종종 발견되고 있습니다. 이 경우, 인터넷 서비스에 발생할 수 있는 문제점에 대해서는 p.145 “나. 위임된 네임서버 일부가 리커시브 네임서버인 경우” 장의 사례를 참조하시기 바랍니다.

리커시브 네임서버를 도메인 존의 네임서버로 설정하는 경우가 많은 것은 해당 리커시브 네임서버가 도메인에 대하여 정상 응답하는 것처럼 보일 수 있기 때문인 것으로 추정됩니다. 서버 관리자의 입장에서 nslookup이나 dig와 같은 DNS 점검도구로 질의해서 데이터가 응답되면 정상적인 설정상태라고 판단하기 쉽습니다. 하지만 DNS 점검도구가 질의하는 디폴트 방식은 재귀적(recursive) 질의이기 때문에 ISP 리커시브 네임서버에 캐싱 데이터가 있을 경우 응답을 대신해주기 때문에 해당 네임서버의 존 데이터가 존재하지 않더라도 정상정인 응답처럼 착각할 수 있습니다. 인터넷의 리커시브 네임서버는 도메인의 네임서버로 반복적(iterative) 질의를 하기 때문에, 실제로는 정상적으로 동작하는 상태가 아닙니다. 인터넷의 리커시브 네임서버는 도메인의 네임서버로 반복적(iterative) 질의를 사례를 참조하시어 이로 인해 발생할 수 있는 문제점을 검토하시기 바랍니다.

4) 네임서버 S/W 정보 노출방지 설정

□ 설정 기준 (참고사항)

- 네임서버 S/W 종류 및 버전 정보가 외부에 노출되지 않도록 설정

□ 설정의 필요성

네임서버 S/W 정보는 S/W의 버전별 취약점 정보를 악용한 보안침해 공격의 단서를 제공할 수 있습니다. DNS 보안 안정성 강화를 위해 네임서버의 S/W 정보가 외부에 노출되지 않도록 추가 설정하는 것이 바람직합니다.

□ 설정 방법

네임서버 S/W에 따라 네임서버 S/W 정보의 외부 노출여부가 달라집니다.

네임서버 S/W 정보제공 기능이 있는 네임서버로는 BIND DNS 네임서버, PowerDNS 네임서버, NSD 네임서버, Nomium 사의 ANS 네임서버 등이 있습니다. 이들 네임서버들은 네임서버 S/W 정보 노출 방지 설정이 필요 합니다.

Windows DNS 서버의 경우에는 해당 설정이 필요치 않습니다.

이외의 네임서버 S/W 경우도, 네임서버의 매뉴얼을 확인하여 S/W 정보제공 기능이 있을시 노출 방지 설정방법을 파악하여 방지 설정하는 것이 필요합니다.

다음은 네임서버가 S/W 정보 노출 상태인지 여부를 확인하는 방법입니다.

dig을 사용한 확인 방법

도메인 네임 “version.bind”에 대하여 CHAOS 클래스(CH), 질의타입 TXT를 사용하여 대상 네임서버로 질의하여 네임서버 S/W 정보가 문자열로 응답되는지 확인합니다.

다음은 네임서버 S/W 정보 노출 상태인 경우입니다.

```
$ dig @211.182.233.3 version.bind ch txt +short
"BIND 8.3.3"
$ dig @193.0.14.129 version.bind ch txt +short
"NSD 2.3.7"
$ dig @152.99.1.10 version.bind ch txt +short
"Nominum ANS 2.6.0.1"
$ dig @222.239.76.130 version.bind ch txt +short
"Served by POWERDNS 2.9.21 $Id: packethandler.cc 1036 2007-04-19
20:43:14Z ahu $"
```

다음은 네임서버 S/W 정보 노출방지 설정 상태인 경우입니다.

```
$ dig @203.255.112.34 version.bind ch txt +short
"To err is human, to fix is divine - domain@higlobe.net"
$ dig @210.204.251.22 version.bind ch txt +short
"No!!"
```

S/W 노출 방지 설정 상태인 경우
1) 엉뚱한 문자열로 수정 설정한 경우
2) DNS 에러응답 경우
3) 응답 문자열 데이터 없이 응답한 경우

nslookup을 사용한 확인 방법

dig을 사용하는 경우와 동일하게, 도메인 네임 “version.bind”에 대하여 CH 클래스, 질의타입 TXT를 사용하여 대상 네임서버로 질의하여 확인합니다.

DNS 질의내용은 dig의 경우와 다르지 않으므로, 여기서는 nslookup의 경우에 설정하는 사항에 대한 예시만 보입니다. 아래는 네임서버 S/W 정보 노출 상태인 경우에 대한 예시입니다.

```
C:\>nslookup.exe
<출력 사항 생략>
> server 211.182.233.3
<출력 사항 생략>
> set class=chaos
> set type=txt
> version.bind
Server:  [211.182.233.3]
Address:  211.182.233.3

VERSION.BIND    text =

       "BIND 8.3.3"
> exit
```

네임서버 S/W 정보가 노출되고 있는 상태라면, 노출 방지 설정을 합니다.

네임서버 S/W 정보 노출방지 설정 방법입니다. 여기서는 BIND DNS의 경우에 한정하여 방법을 제시합니다.

BIND DNS의 네임서버 S/W 정보노출 방지 설정방법

네임서버에서 환경설정 파일인 named.conf 파일을 열고, options 설정부에서 다음과 같은 설정 사항을 추가 작성합니다.

버전정보 노출 방지는 2가지 방식으로 설정
1) 버전정보 문자열 레코드를 제거
2) 버전정보를 의미 없는 문자열로 대체

다음은 버전정보 문자열 레코드를 제거하는 설정방법입니다.

```
options {
     ... 기존 설정 생략 ...
     version none;              // 버전정보 문자열 레코드 제거
};
```

위와 같이 설정한 경우, version.bind에 대한 질의를 수행하면 아래와 같이 응답할 문자열 데이터가 없는 상태로 응답합니다.

```
$ dig @localhost version.bind ch txt

; <<>> DiG 9.3.1 <<>> @localhost version.bind ch txt
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1146
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; AUTHORITY SECTION:
version.bind.           86400   CH      SOA     version.bind. hostmaster.version.bind. 0 28800 7200
604800 86400

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jun 12 19:09:52 2009
;; MSG SIZE  rcvd: 77
```

다음은 버전정보를 의미 없는 문자열로 대체하는 설정방법입니다.

```
options {
      ... 기존 설정 생략 ...
      version "UNKNOWN";  // 의미없는 문자열로 대체 설정
};
```

위와 같이 설정한 경우, version.bind에 대한 질의를 수행하면 아래와 같이 임의로 지정한 문자열 "UNKOWN"으로 네임서버 S/W 정보를 대체하여 응답합니다.

```
$ dig @localhost version.bind ch txt

; <<>> DiG 9.3.1 <<>> @localhost version.bind ch txt
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 953
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "UNKOWN"
```

```
;; AUTHORITY SECTION:
version.bind.          0       CH      NS      version.bind.

;; Query time: 10 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Fri Jun 12 19:10:35 2009
;; MSG SIZE  rcvd: 63
```

참고: BIND DNS에 의한 호스트네임 정보 노출방지

BIND DNS의 경우, 네임서버 호스트의 호스트네임을 hostname.bind에 의한 질의로 파악할 수 있습니다. 네임서버가 설치된 호스트의 호스트네임 정보가 외부에 노출됨으로 인해 문제 발생이 우려되는 경우, named.conf 파일에서 노출 방지 설정을 합니다.

다음은 호스트네임 정보를 삭제하는 설정입니다.

```
options {
      ... 기존 설정 생략 ...
      hostname none;        // 호스트네임 문자열 레코드 제거
};
```

또는 다음과 같이 의미 없는 정보로 대체할 수 있습니다.

```
options {
      ... 기존 설정 생략 ...
      hostname "ns";        // 호스트네임 문자열 내용 대체
};
```

의미 없는 문자열 "ns"으로 대체한 경우, 호스트네임 정보 질의를 다음과 수행하여 정상적으로 변경 설정되어 있는지 확인할 수 있습니다.

```
$ dig @202.30.50.51 hostname.bind ch txt

; <<>> DiG 9.3.1 <<>> @202.30.50.51 hostname.bind ch txt
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2038
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;hostname.bind.              CH      TXT

;; ANSWER SECTION:
```

```
HOSTNAME.BIND.          0       CH      TXT     "ns"

;; Query time: 5 msec
;; SERVER: 202.30.50.51#53(202.30.50.51)
;; WHEN: Fri Jun 26 20:35:25 2009
;; MSG SIZE  rcvd: 60
```

□ 인터넷 서비스 영향

네임서버 S/W 정보 노출의 경우, 네임서버 S/W의 취약점을 악용한 공격에 의한 피해를 입을 수 있습니다.

특히, 네임서버 S/W를 오랫동안 업그레이드 하지 않고 있는 네임서버의 경우, 네임서버 S/W 정보 노출 방지 설정이 필수적입니다. 오래된 버전의 네임서버 S/W 취약점 사항은 잘 알려져 있어 쉽게 파악할 수 있기 때문입니다.

도메인의 네임서버가 모두 동일한 버전, 동일한 S/W로써 오래된 버전의 네임서버로 운영되고 있는 경우, 그 위험성은 증가합니다. 모두를 동일한 방법으로 공격함으로서 도메인의 모든 네임서버가 동시에 비정상 동작을 하도록 유도할 수 있는 가능성이 높아지기 때문입니다. 이 경우, 관련 인터넷 서비스에 예상치 못한 중대한 장애가 발생 할 수 있습니다.

5) 네임서버의 리커시브 서비스 제한 설정

□ 설정 기준 (참고사항)

- 도메인의 네임서버가 리커시브 서비스 제공 경우, 한정된 범위의 호스트로 리커시브 서비스 제한 설정
- 가능한 한 리커시브 서비스 비활성 상태의 authoritative 네임서버로 설정 운영 권장

□ 설정의 필요성

리커시브 서비스는 PC 호스트를 위해 대신 인터넷에서 DNS 데이터를 조회하여 응답해주는 기능을 지칭합니다. 리커시브 서비스를 제공하는 대표적인 예로는 인터넷 서비스를 신청했을 때, ISP에서 제공하는 DNS 서버들이 그것입니다.

도메인의 네임서버들은 가능한 한 리커시브 서비스를 해제하여 운영하도록 권고하고 있습니다. 도메인 안정성과 네임서버 보안성을 강화하기 위하여 authoritative 전용 네임서버와 리커시브 전용 네임서버를 각각 목적에 따라 별도 구성하여 사용하는 것이 바람직합니다.

때때로 도메인의 네임서버를 리커시브 네임서버 용도와 함께 사용해야 하는 경우가 있습니다. 이 경우에는 리커시브 서비스를 제공받는 호스트에게만 서비스 제한설정하는 것이 필요합니다. 역시 보안상의 이유로써, DNS 관련 침해 공격의 피해를 입지 않도록 예방하는 것이 필요하기 때문입니다.

리커시브 서비스를 제공하는 네임서버가 서비스 제한 설정을 하지 않는 경우, 인터넷의 모든 호스트가 이 네임서버의 리커시브 서비스를 이용이 가능합니다. 악의를 가진 공격자는 이 네임서버의 취약점을 공격하거나 또는 다른 사이트에 대한 공격에 이 호스트를 무단으로 이용할 수 있습니다.

리커시브 서비스 제공 네임서버는 호스트의 질의요청에 의해 정해진 절차를 수행하게 됩니다. 이 과정에서 DNS의 동작 원리를 악용하여 네임서버의 리커시브 서비스를 악용할 수 있습니다. 2006년에 서비스 제공 제한이 되어 있지 않은 네임서버들로 하여금 특정 사이트로 엄청난 트래픽을 발생시키도록

하여 DDoS 공격이 발생한 사례가 실제로 발생하였습니다. 이 경우, 공격의 대상이 된 사이트는 서비스가 중단되는 피해를 입었습니다. 공격에 동원된 리커시브 네임서버들에 대해서 리커시브 서비스 제공 범위의 제한 설정을 권고하는 조치가 이루어졌습니다. 이 공격을 “Reflector Attacks”라고 부르고 있습니다.

□ 설정 방법

도메인 네임서버는 가능한 한 리커시브 서비스를 제공하지 않는 네임서버로 구성 설정 합니다.

만일 도메인 네임서버가 동시에 리커시브 네임서버로 동작해야 하는 상황이라면, 리커시브 서비스 제공대상 호스트 범위를 제한 설정합니다.

DNS S/W 중 BIND DNS와 Windows DNS S/W의 사용비중이 가장 높은 편인데 이 두 S/W는 특별한 설정이 없는 경우 authoritative 네임서버와 리커시브 네임서버 기능을 모두 가지고 있습니다. 이와 같은 네임서버들을 사용하는 경우에는 리커시브 서비스 기능해제 또는 서비스 제공대상 호스트 범위 제한설정이 필요합니다.

일부 네임서버의 경우는 authoritative 네임서버 기능만 구현한 경우가 있습니다. NLnet Lab의 오픈 소스 NSD 네임서버나 Nominum사의 상용 네임서버인 ANS 등이 이에 해당합니다. 이 경우 리커시브 서비스 기능 자체가 없으므로 별다른 설정이 필요하지 않습니다.

다음은 BIND DNS의 경우, 리커시브 서비스 기능 해제 설정방법과 리커시브 서비스 제공대상 호스트 범위 제한 설정방법입니다.

아래 설정 방법은 BIND 9.4.1-P1 버전 이전의 BIND DNS에서 설정하는 방법입니다. BIND 9.4.1-P1 이후 버전에서는 디폴트로 리커시브 서비스 기능이 해제되어 동작하므로, 필요시 이를 해제 설정하는 방식으로 설정을 하는 것이 필요합니다.

리커시브 서비스 기능 해제 설정방법

도메인 네임서버에서 리커시브 서비스 기능을 해제하는 설정 방법입니다. 아래와 같이 설정하여 반영하면, 이 네임서버는 리커시브 서비스 기능을 하지 않습니다. 네임서버에 설정된 도메인 존에 대한 질의응답만 합니다.

```
options {
     ...
     recursion no;        // 리커시브 서비스 해제 설정
};
```

리커시브 서비스 제공 대상 호스트 범위 제한 설정방법

도메인의 네임서버가 리커시브 네임서버로도 기능해야 하는 경우, 리커시브 서비스 제공 대상 호스트 범위를 제한하는 설정방법입니다. 아래의 경우, 네임서버 자체 호스트(localhost), 네임서버가 있는 서브 네트워크(localnets), 그리고 리커시브 서비스가 필요한 내부 호스트들의 서브 네트워크에 한정하여 리커시브 서비스를 제한적으로 제공합니다.

```
// 내부 호스트의 서브 네트워크 지정
acl internal-hosts { localhost; localnets; 192.168.1.0/24;
192.168.5.0/24; };

options {
     ...
     allow-recursion { internal-hosts; };     // 리커시브 서비스 제한 설
                    정
};
```

주의사항: allow-query 설정의 주의 사항

allow-query 설정은 모든 유형의 DNS 질의에 대하여 제한을 설정하는 옵션입니다.

도메인의 네임서버인 경우, 누구나 도메인에 대한 DNS 질의응답이 이루어져야 합니다. 만약 도메인의 네임서버에 이 옵션을 사용하는 경우, 도메인에 대한 DNS 질의응답이 일부 호스트에게는 제공되지 않아, 이들 호스트들은 도메인의 인터넷 서비스를 이용할 수 없는 상태가 되고 맙니다.

allow-query를 사용한 설정은 “리커시브 서비스 전용 네임서버를 구성할 때, 리커시브 서비스를 제공 대상 호스트를 제한 설정하려는 경우”에 적용 사용될 수 있습니다. 도메인 네임서버의 경우는 여기에 해당될 수 없습니다.

참고사항: View 설정 방법

위에 제시된 방법 외에 사이트 내부/외부의 질의를 구분하여 동일한 도메인 존에 대한 응답 데이터를 달리하여 응답처리 하도록 뷰(view) 설정을 하는 방법이 있을 수 있습니다. 뷰(view) 구성을 통해 사이트 내부/외부의 질의를 구분하여 리커시브 서비스 제한 설정을 할 수 있습니다. 위에 제시한 방법은 뷰(view) 기반의 제한설정에 동일한 방식으로 적용됩니다. 본 안내서에서는 관련 설명을 생략합니다.

BIND DNS 9.4.1-P1 이후의 네임서버에서는 특별히 명시하지 않을 경우 리커시브 기능을 최소한으로 제한한 상태에서 동작하도록 변경되었습니다. 이는 리커시브 기능에 의한 심각한 보안 문제가 할 수 있으므로, 기본적으로 리커시브 서비스가 제한된 상태로 동작하도록 한 것입니다.

BIND 9.4.1-P1 이후 버전의 네임서버에 대해서는 다음과 같은 방법으로 설정합니다.

리커시브 서비스 기능 해제 설정방법

리커시브 기능을 사용하지 않도록 하는 설정입니다.

```
options {
     ...
     recursion no;        // 리커시브 서비스 해제 설정
};
```

위와 같은 설정을 하지 않는 경우, 네임서버는 리커시브 네임서버로 동작하지만, 리커시브 질의를 할 수 있는 호스트는 네임서버가 있는 호스트 자신(localhost)과 네임서버가 있는 서브 네트워크(localnets)에만 한정된 상태로 동작합니다.

리커시브 서비스 제공 대상 호스트 범위 제한 설정방법

BIND 9.4.1-P1 버전부터는 반대로 리커시브 질의를 할 수 있는 호스트를 추가 지정하는 방식으로 설정하는 것이 필요합니다.

특별히 지정하지 않으면, 네임서버 호스트 자신(localhost)과 네임서버가 있는 서브 네트워크(localnets)에 한정하여 리커시브 서비스가 제공됩니다.

```
// 내부 호스트의 서브 네트워크 지정
acl internal-hosts { localhost; localnets; 192.168.1.0/24;
192.168.5.0/24; };

options {
    ...
     allow-query { any; }; // 명시적 설정
     allow-recursion { internal-hosts; };     // 리커시브 서비스 제한 설
                    정
    allow-query-cache { internal-hosts; }; // 캐시영역 조회 제한 설정
};
```

도메인의 네임서버로 설정하는 네임서버에는 allow-query를 인터넷의 모든 호스트에 대해 허용해야 합니다. allow-query는 디폴트로 모든 호스트에 대해 허용하는 값을 갖지만, 위와 같이 명시적으로 설정하는 것이 관리상의 실수를 방지할 수 있습니다.

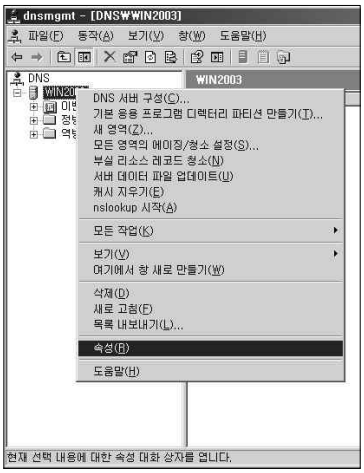
다음은 Windows DNS 서버의 리커시브 서비스 기능 해제 설정방법입니다.

리커시브 서비스 기능 해제 설정방법

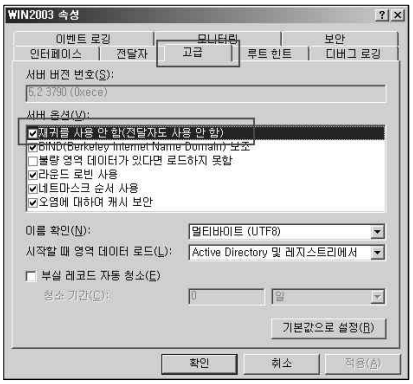
Windows DNS 서버의 경우, 리커시브 서비스의 특정호스트 제한설정이 불가능합니다. 리커시브 서비스의 활성/비활성만 가능합니다. Windows DNS는 보안을 위해 authoritative 전용 DNS 서버와 리커시브 전용 DNS 서버를 각각 별도로 구성하여 리커시브 네임서버용 DNS 서버의 경우 방화벽을 사용하여 외부 인터넷의 호스트가 접근하지 못하도록 설정하는 것을 권하고 있습니다.

여기서는 Windows DNS 서버의 리커시브 기능 해제 설정방법을 예시합니다. 리커시브 기능 해제 설정에 의해 Windows DNS 서버는 authoritative 네임서버로만 동작합니다. 리커시브 네임서버로는 사용할 수 없습니다.

Windows DNS 서버의 “속성” 선택



Windows DNS 서버의 “속성” 중 “고급” 탭 선택
“재귀를 사용 안 함(전달자도 사용 안 함)”을 선택하고 체크 설정
“확인” 클릭



네임서버의 리커시브 서비스 제공 제한 설정 후 외부 인터넷에서 이 네임서버로 리커시브 질의가 허용되고 있는지 여부를 확인할 수 있는 방법은 다음과 같습니다.

인터넷 일반에 대해 리커시브 서비스 제공 상태 여부 확인 방법

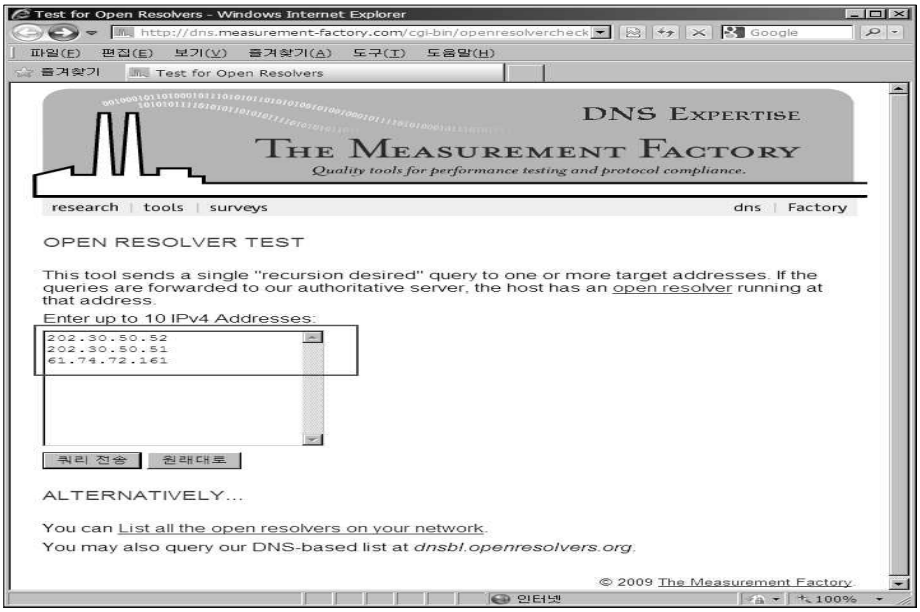
관리하고 있는 네임서버가 외부 인터넷에 대하여 리커시브 서비스 제공 상태인지 여부를 스스로 원격에서 체크할 수 있도록 하는 해외 소재의 웹 사이트가 있습니다.

Open Resolver Test 웹 사이트 (미국 소재)
http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl

"Open Resolver Test" 웹 사이트는 원격 사이트에서 특정 네임서버에 대하여 이 네임서버가 외부 인터넷에 리커시브 질의응답 서비스가 제한 없이 허용되어 있는지 여부를 체크하고 그 결과를 알려 줍니다.

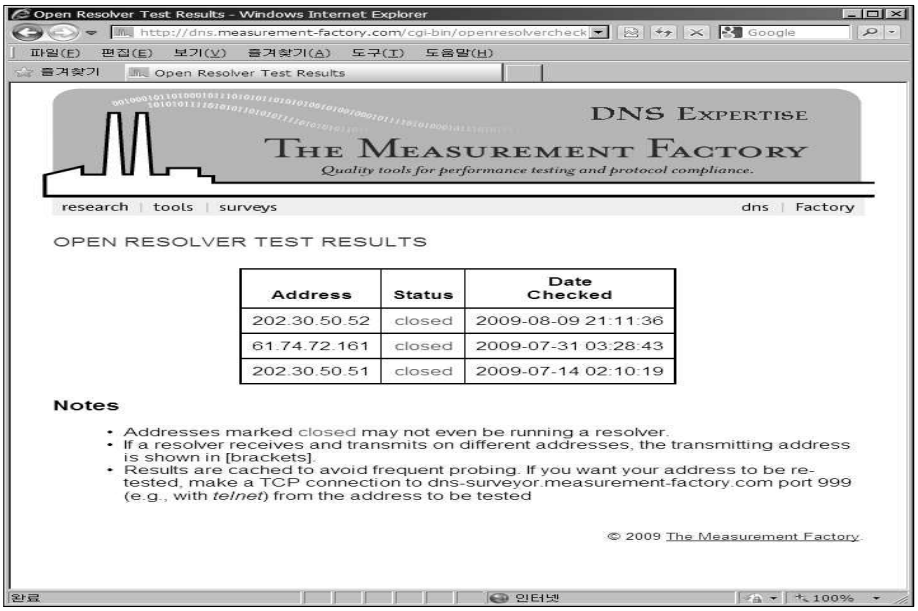
웹 사이트에 접속하면, 최대 10개의 네임서버 IP 주소를 입력하는 페이지가 다음 화면과 같이 출력됩니다.

아래 화면은 3개의 네임서버 IP 주소를 입력한 경우를 보인 것입니다.

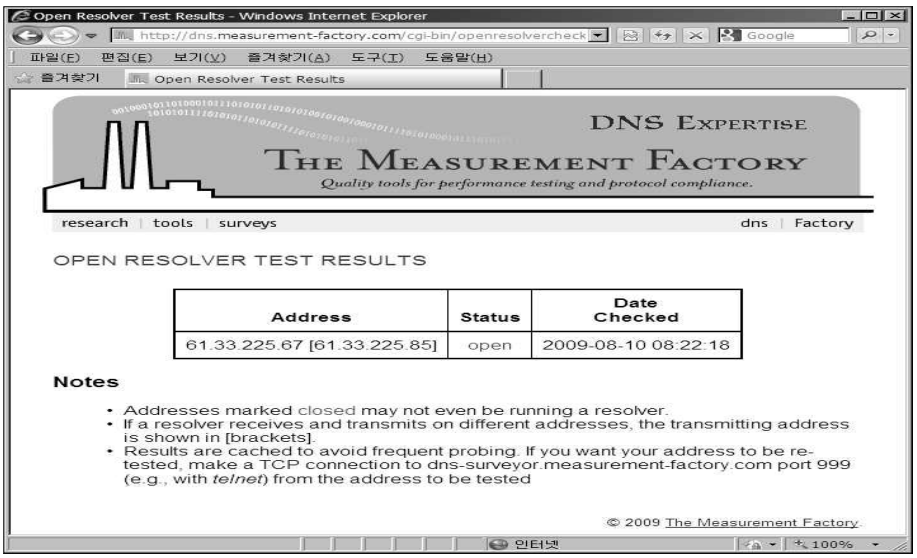


"쿼리 전송" 버튼을 클릭하면, 체크를 시작합니다.

잠시 기다리면 입력한 네임서버 IP 주소별로 네임서버의 상태 체크결과가 출력됩니다. Status 칼럼에 "closed"일 때, 인터넷 일반에 대해 리커시브 제한 설정이 되어 있는 상태입니다.



인터넷 일반에 대해 제한 없이 리커시브 질의응답이 제공되고 있는 경우는 아래와 같이 Status 칼럼에 “open” 상태로 결과가 출력됩니다.



□ 인터넷 서비스 영향

별다른 제한 설정 없이 리커시브 서비스를 제공하고 있는 네임서버는 악의를 가진 공격자의 직접적인 공격 대상이 되거나 타 사이트를 공격하기 위한 수단으로 악용될 가능성이 있습니다. 이 네임서버가 도메인의 네임서버인 경우, 도메인의 인터넷 서비스에 크고 작은 영향이 발생할 수 있습니다.

리커시브 서비스 제공 대상 제한이 없는 네임서버들을 이용하여 특정 사이트에 원하는 크기의 패킷 트래픽을 발생하도록 원격에서 조작이 가능합니다. 실제로 2006년에 발생했던 "반사공격(Reflector Attacks)"이라는 공격 형태가 있었는데 리커시브 서비스 제공대상 제한이 없는 네임서버들을 인터넷 상에서 파악하고 이들을 동원하여 특정 사이트로 4096 바이트 크기의 DNS 응답 패킷을 집중 발송하게 함으로써 전 세계의 DNS 네임서버를 악용하여 분산 서비스 거부 공격(DDOS)을 유발 한 바 있습니다. 이러한 형태의 공격은 제공 제한 없는 리커시브 네임서버가 제3의 사이트에 공격에 필요한 트래픽과 시스템 부하를 도와주면서 네임서버의 정상적인 서비스 제공에 성능저하를 유발할 수 있습니다.

리커시브 서비스가 제한 없이 공개된 네임서버는 DNS 캐시 포이즈닝(cache poisoning) 공격에 취약할 수 있습니다. 이런 유형의 공격을 가리켜 파밍(pharming)이라고도 합니다. 이 공격은 도메인에 네임에 위조 또는 변조된 IP주소 데이터를 PC 호스트에 응답하도록 조작함으로써 개인의 금융정보나 개인정보를 탈취하는 것을 주된 목적으로 합니다. 리커시브 서비스가 제한 없이 열려 있을 때, 공격자의 호스트가 접근이 허용되면서 가능한 공격입니다. 리커시브 서비스가 제한된 호스트에게만 제공되도록 설정되어 있을 때, 외부 원격지에서 이 네임서버에 대한 DNS 캐시 포이즈닝 공격이 원천적으로 차단됩니다.

6) 도메인 존 전송 허용 호스트의 제한 설정

□ 설정 기준 (참고사항)

- 사이트 구성정보 노출방지 위해 도메인 존 전송 허용 호스트 제한 설정
- 가급적 네임서버의 TCP 53번 포트는 질의응답 허용 유지

□ 설정의 필요성

원칙적으로 네임서버에 설정된 도메인 존 데이터는 인터넷 상에서 어느 누구에게나 공개되어야 하는 데이터입니다. 하지만 이들 데이터 중에는 사이트의 구조를 유추해 낼 수 있는 정보를 포함하는 경우가 있습니다. 보안 정책상, 사이트 구성정보를 외부에서 쉽게 파악할 수 없도록 조치할 필요성이 있습니다.

DNS 표준은 AXFR 질의 타입을 통하여 도메인 존의 모든 데이터 리스트를 한 번의 질의로 파악할 수 있게 제공합니다. 주로 AXFR 질의는 도메인의 네임서버 간 도메인 존 전송(Zone Transfer) 절차에 사용됩니다. 도메인의 슬레이브 네임서버가 매스터 네임서버로부터 갱신된 도메인 존 데이터를 전송받을 때 TCP 53 포트를 사용한 AXFR 질의를 사용합니다. 그러나 dig 나 nslookup 과 같은 일반적인 DNS 질의점검 도구를 사용하여 쉽게 AXFR 질의를 수행할 수도 있어 사이트의 구성현황 정보를 파악하려는 목적에 활용될 수 있습니다.

도메인 존 데이터가 임의의 호스트로 일괄 전송되는 것을 방지하기 위해 도메인 존 전송 허용 호스트의 제한 설정이 필요합니다. 도메인 존 전송 제한 설정은 거의 모든 네임서버 S/W에서 제공하고 있습니다.

일부 사이트에서는 방화벽의 TCP 53번 포트를 외부 인터넷으로부터 차단 설정하여 도메인 존 데이터 전송을 허용하지 않는 경우가 많습니다. 하지만 이와 같은 방법은 바람직하지 않습니다. 그 이유는 DNS 표준 질의응답 절차에는 UDP 53번 포트와 TCP 53번 포트를 모두 사용하도록 정의되어 있기 때문입니다. 대부분의 DNS 질의응답은 UDP 53번 포트로 이루어지지만 응답 데이터가 512 바이트를 초과 할 경우 TCP 53번 포트로 전환하여 TCP 스트리밍 데이터 전송을 통하여 전달하는 동작이 이루어집니다. 따라서 방화벽에

서 TCP 53포트를 차단하였다면 512 바이트를 초과하는 DNS 응답은 실패하게 됩니다.

하지만, DNS 응답 데이터가 512 바이트를 초과하는 경우는 극히 드물게 발생합니다. 그리고 최근의 EDNS0를 지원하는 네임서버 S/W를 사용하고 있다면 TCP 53번 포트를 차단하고 있더라도 512 바이트를 초과하는 DNS 응답 처리가 원활히 이루어질 수 있습니다. EDNS0(DNS Extension version 0)는 512 바이트 초과 응답 데이터도 UDP 패킷을 사용하여 처리할 수 있도록 하는 확장 표준 규격입니다. 다만, 리커시브 네임서버도 EDNS0를 지원하는 최근의 네임서버여야만 이와 같은 동작이 가능합니다.

네임서버의 EDNS0 지원이 보편화 된 점을 고려할 때, 반드시 TCP 53번 포트 허용은 하지 않아도 무방하다고 보입니다. 다만 DNS 네임서버에 특수한 용도의 대량 데이터를 갖는 도메인 존을 구성하여 사용하려는 경우나 현재로써 모든 리커시브 네임서버가 EDNS0을 지원하고 있다는 보장을 할 수 없기 때문에 포트 차단에 의한 문제 발생 가능성 여부를 파악하여 확인한 후 결정해야 합니다.

여기서는 네임서버에서의 도메인 존 전송 허용 호스트의 제한 설정 방법을 제시합니다.

□ 설정 방법

도메인 존 전송의 허용 제한은 도메인별로 설정합니다. 존 전송 허용 대상 호스트는 주로 도메인의 슬레이브 네임서버이고 IP 주소를 대상으로 허용 설정합니다. 보안상의 이유로 TSIG를 적용한 보안키 대상으로 허용설정 할 수도 있습니다. 지정된 보안키를 포함하여 존 전송 요청을 하는 호스트로 존 전송을 허용하도록 하는 방식입니다.
한 가지 주의사항은, 존 전송 허용 제한 설정은 매스터 도메인 존 뿐만 아니라 슬레이브 도메인 존에서도 설정이 필요하다는 점입니다. 매스터 도메인 존에서만 존 전송 허용 제한이 설정되어있다면 제한 된 호스트가 슬레이브 네임서버를 통해 AXFR 질의로 충분히 파악될 수 있기 때문에 반드시 슬레이브 도메인 존에서는 존 전송 완전차단설정이 필요합니다. 외부에서 볼 때

는 매스터, 슬레이브 네임서버는 authoritative 네임서버 일 뿐이고 모든 authoritative 네임서버는 기본적으로 도메인에 대한 존 전송요청에 대해 응답 처리하도록 구현되어 있기 때문입니다.

도메인 존 전송(Zone Trnasfer) 제한 설정

네임서버에서 도메인의 존 전송 제한설정
1) 네임서버 전체 영역의 존 전송 차단 설정
2) 각 도메인별 존 전송 제한 허용 설정

다음은 각 네임서버 전체 영역에서의 존 전송 차단 설정입니다.

매스터/슬레이브 네임서버 공통 설정:

```
options {
     allow-transfer { none; };
};
```

네임서버 전체 영역에 대하여 존 설정을 차단 설정하는 것은 기본적으로 존 전송을 차단하기 위한 설정입니다. 매스터 네임서버와 슬레이브 네임서버 모두에 공통적으로 설정합니다.

도메인 존의 설정영역에서 도메인 존 마다 존 설정 허용 설정을 합니다. 도메인 존마다 설정하는 존 전송 허용 설정은 네임서버 전체 영역에 대한 존 전송 차단 설정보다 우선합니다. 따라서 존 전송 허용이 필요한 도메인 존에서만 존 설정 허용 사항이 적용됩니다.

다음은 도메인 존에서의 존 전송 제한 허용 설정입니다.

매스터 네임서버 경우:

```
zone "my-domain.re.kr" IN {
     type master;                // “매스터 존”으로 지정
     file "my-domain.kr";        // 도메인 존 파일명 지정
     allow-transfer { 192.168.2.53; 192.168.3.53; };
     // 도메인의 슬레이브 네임서버에 한정하여 존 전송 허용 설정
};
```

슬레이브 네임서버 경우:

아래와 같이 존 전송 차단을 명시적으로 설정할 수 있습니다.

```
zone "my-domain.re.kr" IN {
    type slave;                 // "슬레이브 존"으로 지정
    masters { 192.168.1.53; }; // 매스터 네임서버 IP 주소 지정
    allow-transfer { none; };  // 타 서버로 존 전송 차단 설정
};
```

또는 아래와 같이 존 전송 차단을 생략해도 안전합니다. 네임서버의 전역 설정인 options 설정에 존 전송 차단 설정이 되어 있는 경우에 그렇습니다.

```
zone "my-domain.re.kr" IN {
    type slave;                 // "슬레이브 존"으로 지정
    masters { 192.168.1.53; }; // 매스터 네임서버 IP 주소 지정
};
```

네임서버별 도메인의 존 전송 허용 호스트 제한 설정 상태에 대하여 dig을 사용한 점검 방법을 보입니다.

dig을 사용하여 다음과 같이 도메인 존 네임에 대하여 AXFR 질의를 함으로써 존 전송 제한 설정이 적용되어 있는지 확인할 수 있습니다.

다음은 존 전송 허용 대상이 아닌 호스트에서 질의한 결과로써 존 전송 요청에 대해 존 전송 거부된 경우입니다.

```
$ dig @192.168.2.53 my-domain.re.kr axfr +norec +multi

; <<>> DiG 9.3.1 <<>> @192.168.2.53 my-domain.re.kr axfr +norec +multi
; (1 server found)
;; global options:  printcmd
; Transfer failed.
```

다음은 존 전송 허용 대상 호스트에서 질의한 결과로써 도메인 존의 모든 데이터가 응답된 경우입니다.

```
$ dig @192.168.2.53 my-domain.re.kr axfr +norec +multi

; <<>> DiG 9.3.1 <<>> @192.168.2.53 my-domain.re.kr axfr +norec +multi
; (1 server found)
;; global options:  printcmd
my-domain.re.kr.        300 IN SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr. (
                            2009090105 ; serial
```

```
                            1800      ; refresh (30 minutes)
                            300       ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300       ; minimum (5 minutes)
                            )
my-domain.re.kr.        300 IN NS ns1.my-domain.re.kr.
my-domain.re.kr.        300 IN NS ns2.my-domain.re.kr.
my-domain.re.kr.        300 IN NS ns3.my-domain.re.kr.
ns1.my-domain.re.kr.     300 IN A 192.168.1.53
ns2.my-domain.re.kr.     300 IN A 192.168.2.53
ns3.my-domain.re.kr.     300 IN A 192.168.3.53
www.my-domain.re.kr.     300 IN A 192.168.80.80
my-domain.re.kr.        300 IN SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr. (
                            2009090105 ; serial
                            1800      ; refresh (30 minutes)
                            300       ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300       ; minimum (5 minutes)
                            )
;; Query time: 19 msec
;; SERVER: 192.168.2.53#53(192.168.2.53)
;; WHEN: Tue Aug 11 16:56:00 2009
;; XFR size: 9 records (messages 1)
```

□ 인터넷 서비스 영향

도메인 존 전송 제한 설정 누락으로 인해 발생할 수 있는 문제점은 사이트에 대한 보안 침해 공격으로 이어질 수 있는 구성현황 정보를 제공할 수 있다는 점에 있습니다.

대규모 사이트에서는 각종 사이트 구성 장비에 도메인 네임을 부여하여 관리하는 경우가 있어 도메인 존의 외부 노출 제한 설정이 필요합니다. 방화벽 장비의 IP 주소나 라우터 장비의 인터페이스 IP 주소 등이 외부에 상세히 노출된다면, 이러한 기초 데이터를 기반으로 사이트 내부 네트워크 구조와 서버 시스템 구조 등을 유추하여 파악할 가능성이 있기 때문입니다. 가능한 한

외부 인터넷에 제공하는 도메인 존에는 인터넷 서비스에 필수적인 데이터만 설정하고, 내부 네트워크 관리나 서버 시스템 관리 등을 위한 데이터는 내부용 도메인 존에 구성하고 이들 두 개의 도메인 존을 BIND DNS의 view 기능을 활용하여 분리 설정하는 것이 바람직합니다.

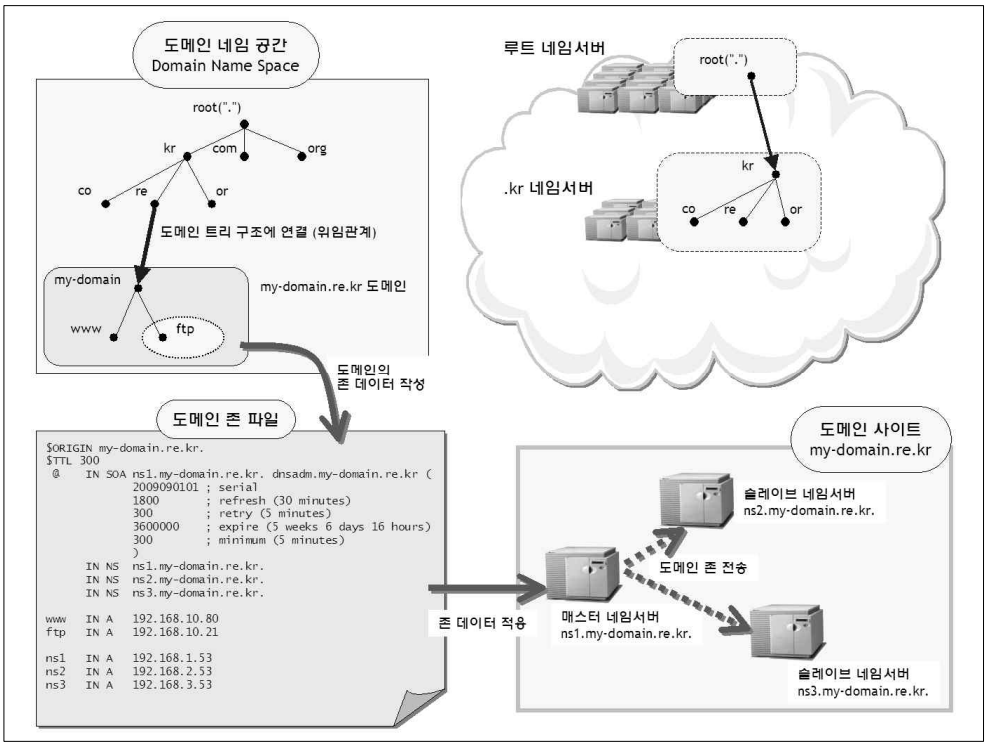
나. 도메인의 위임설정

1) 도메인 등록정보의 네임서버 정보 관리 중요성

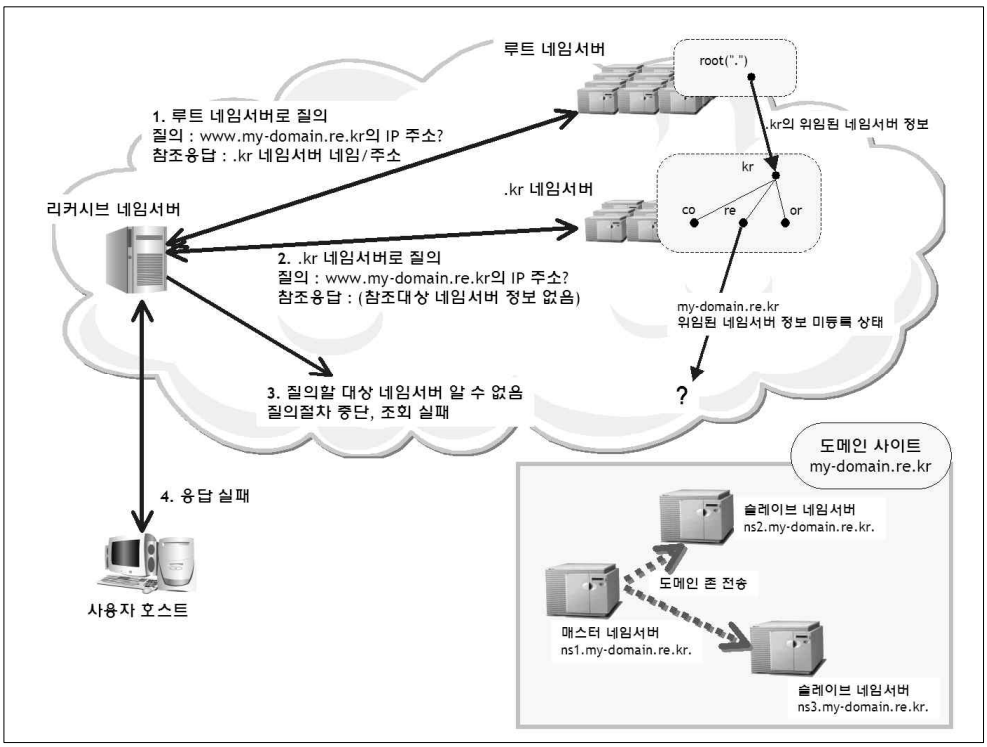
도메인을 등록한 후, 도메인의 존 데이터를 구성하고 네임서버에 적용했더라도 아직 도메인 등록정보에 네임서버 정보를 설정하지 않았다면 이 도메인은 인터넷에서 사용이 불가능한 상태입니다. 아직 인터넷의 루트 도메인으로부터 등록 도메인까지의 연결이 이루어지지 않은 상태이기 때문입니다.

이를 예시하기 위해 도메인 my-domain.re.kr을 등록하고 구성하는 경우를 가정합니다.

다음의 그림은 도메인을 등록하고 네임서버에 도메인 존 데이터를 구성하였습니다. 네임서버는 1대는 매스터, 2대는 슬레이브 운영으로 총 3대를 구성한 상태입니다. 아직 이 네임서버들은 상위 .kr 도메인 존에 반영하지 않은 상태입니다.



이 상태에서는 다음의 그림과 같이 인터넷 사용자가 리커시브 네임서버를 경유하여 www.my-domain.re.kr의 IP 주소 질의 시 응답 실패가 발생합니다. 이는 .kr 도메인 존에 my-domain.re.kr 도메인 존 데이터가 어느 네임서버에 있는지 알려주는 "도메인의 위임된 네임서버 정보"가 아직 없는 상태이기 때문입니다. 리커시브 네임서버는 my-domain.re.kr 도메인 존의 소재를 .kr 도메인 존에서 파악할 수 없게 되어 DNS 질의응답 절차를 더 이상 진행할 수 없습니다.

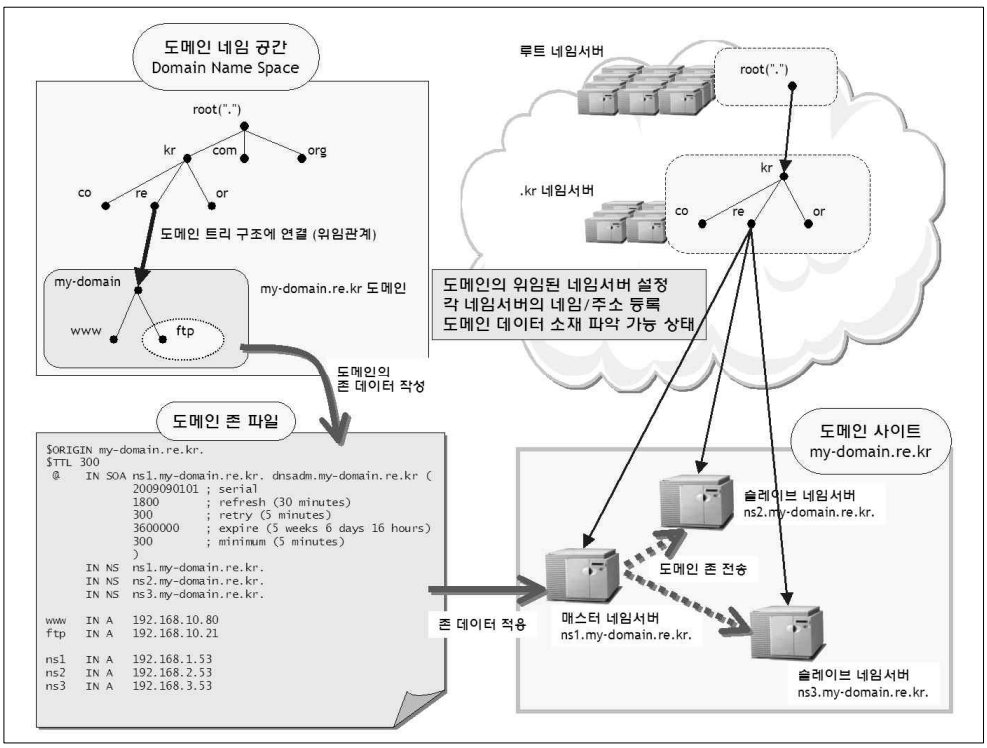


도메인의 관리자는 도메인 존이 설정된 네임서버 리스트를 .kr 도메인 존에 정확한 정보로 등록해야 합니다.

.kr 도메인 존에 my-domain.re.kr 도메인의 네임서버 정보를 설정하기 위해서는 도메인을 등록 신청하였던 도메인 등록대행 기관의 도메인 등록정보 페이지에서 네임서버 정보를 등록하면 됩니다. 입력하는 네임서버 정보는 네임서버 도메인 네임과 서버의 IP 주소 정보입니다. 이 정보는 도메인의 존이 어디에 있는지 알려주는 중요한 정보이기 때문에, 실수 없이 정확한 정보로

입력하는 것이 필요합니다. 이 네임서버 정보를 “위임된 네임서버 정보”라고 합니다.

.kr 도메인 존에 도메인의 위임된 네임서버 정보가 정확히 반영된 상태는 다음의 그림과 같습니다.



그림의 왼편은 인터넷 도메인 네임 중에서 my-domain.re.kr이라는 중복되지 않은 네임을 확보하여 데이터를 구성하는 것을 나타냅니다. 여기까지는 이름의 확보와 도메인 존 데이터 구성 계획 단계에 해당합니다.

오른편은 실제로 도메인을 인터넷 상에 구체적으로 반영하여 구성하는 작업을 나타냅니다. 도메인의 존 데이터를 각 네임서버에 적용 구성하고, 상위 .kr 도메인 존에 이 네임서버 리스트를 등록 반영합니다. 도메인이 최상위 루트 도메인 네임서버부터 .kr 도메인 네임서버, 그리고 최종적으로 도메인 자신의 네임서버들까지 위임설정이 올바르게 설정되도록 하는 것이 필요합니다. 만일 이 위임설정이 재대로 설정이 되지 않았을 경우 도메인의 DNS

질의응답은 다양한 형태의 문제를 겪게 됩니다.

.kr 도메인 존에 설정된 도메인의 네임서버 정보에 오류가 있는 경우, 해당 도메인의 안정성이 크게 훼손될 수 있습니다. 작게는 DNS 질의응답 절차 중 응답 실패로 인한 인터넷 서비스 접속 지연 내지는 불안정 접속 문제가 있을 수 있습니다. 크게는 DNS 관련 침해 공격에 의해 보안 침해사고가 발생할 수 있습니다. 이 같은 DNS 관련 공격은 도메인의 인터넷 서비스 전반에 심각한 피해를 입힐 수 있습니다.

도메인의 위임된 네임서버 설정 오류 유형에 따라 발생할 수 있는 문제점은 다음 장에서 설명합니다.

도메인의 안정성을 확보하기 위해서는 도메인의 위임된 네임서버 정보에 대한 관리에 만전을 기울이는 것이 필수적으로 요구됩니다.

2) 도메인 등록정보의 위임 네임서버 설정

□ 설정 기준 (필수사항)

- 도메인의 모든 네임서버에 도메인 존 지정 설정
- 도메인의 모든 네임서버를 도메인 등록정보의 위임 네임서버로 설정

□ 설정의 필요성

도메인을 등록할 때 작성하는 도메인 등록정보 중 도메인의 네임서버 정보를 “도메인의 위임된 네임서버 정보”라 합니다. “도메인의 위임된 네임서버 정보”는 .kr 도메인 존의 NS 레코드로 변환하여 반영되는 데이터입니다.

“도메인의 위임된 네임서버 정보”는 이 도메인이 인터넷의 루트 도메인과 문제없이 연결되기 위한 연결고리 역할을 합니다. 도메인 체계 상 루트 도메인에서 .kr 도메인이 위임되어 있고, 이 .kr 도메인에서 다시 각 사용자의 도메인 네임서버를 위임하는 연결고리가 형성되어 있어야 사용자 도메인에 대한 질의응답이 신속하고 정확하게 수행될 수 있습니다.

만약 “도메인의 위임된 네임서버 정보”에 잘못된 데이터를 등록한다면 인터넷 상에서 이 도메인에 대한 DNS 질의응답 절차가 원활하게 이루어지지 않는 문제가 발생할 수 있습니다. 또한 최악의 경우에는 도메인 구성상의 보안 취약성을 갖게 될 수도 있습니다.

“도메인의 위임된 네임서버 정보” 설정에 있어 가장 이상적인 설정은 .kr 도메인 존의 네임서버 정보와 도메인 존에 설정된 NS 레코드 정보가 서로 일치하는 설정입니다. 물론 네임서버 IP 주소 정보도 정확히 일치 하는 경우입니다. .kr 도메인 존에 설정된 사용자 도메인의 NS 레코드는 “위임된 네임서버 정보”이고 도메인 존에 설정된 NS 레코드는 이 도메인의 “네임서버 정보”입니다. “위임된 네임서버 정보”와 “네임서버 정보”가 정확히 일치할 때, DNS 질의응답에 있어 가장 최적의 상태가 된다고 볼 수 있습니다. 서로 불일치 할 경우 지연이나 불필요한 질의가 발생할 수도 있습니다.

위와 같은 이상적인 설정을 우선적으로 권고합니다.

.kr 도메인 존에 설정 된 네임서버는 최소한의 설정 요건 2가지를 충족해야 합니다.

1) DNS 응답을 하는 가동상태
2) 네임서버에 도메인 존이 지정 설정되어 있는 상태

하지만 도메인 존이 설정되어 있지 않은 네임서버나 DNS 응답 자체가 없는 가동이 중단되거나 DNS 서버가 아닌 서버를 설정한 경우가 있습니다. 이 같은 경우 때에 따라 심각한 문제 발생의 원인이 될 수 있습니다.

위 최소한의 설정 요건을 충족하지 못하고 설정에 오류가 있는 경우, 도메인 구성 미흡사항 중에 가장 위험한 상태를 유발할 수 있습니다. 특히 보안상 취약점이 발생하여 최악의 경우 특수한 형태의 "도메인네임 무단점유(domain name hijacking)"에 의한 피해가 발생할 수도 있습니다. 도메인 존이 알지 못하는 제 3자의 관리 하에 놓이게 되어 각종 불법적인 데이터 변조에 의한 피해를 입을 수 있습니다.

도메인의 위임된 네임서버 설정에 오류가 있는 경우에 대하여 "단원 3. DNS 설정 주요 문제점 사례" 장의 각 사례 및 사례별 발생가능 문제점 사항을 참고하시기 바랍니다.

□ 설정 방법

다음의 순서를 따라 설정합니다.

1) 도메인 존의 네임서버로 사용할 네임서버를 준비합니다. 이 네임서버들은 DNS 응답이 가능하여야 합니다.
2) 모든 네임서버에 도메인 존을 지정 설정합니다. BIND DNS의 경우, named.conf 파일에 해당 도메인 존을 zone 옵션을 사용하여 설정 합니다.
3) 도메인의 존 파일에 모든 네임서버의 NS 레코드 리스트를 모두 구성하여 네임서버에 반영합니다. 모든 네임서버의 도메인 존 파일 NS 레코드 리스트는 동일해야 합니다.
4) 도메인 등록정보의 네임서버 정보에 모든 네임서버의 NS 레코드 리스트와 동일하게 등록 설정합니다.

도메인 존 설정 설정방법 예시 환경

다음과 같은 도메인과 네임서버를 사용한다고 가정하여 설정방법을 예시합니다.

도메인 : my-domain.re.kr
매스터 네임서버 : ns1.my-domain.re.kr (192.168.1.53)
슬레이브 네임서버 : ns2.my-domain.re.kr (192.168.2.53)
슬레이브 네임서버 : ns3.my-domain.re.kr (192.168.3.53)
매스터 네임서버 존 파일 저장 디렉토리 : /var/named

도메인의 네임서버 리스트

다음과 같이 도메인의 네임서버로 사용할 네임서버 리스트를 산출합니다. 각 서버는 네임서버가 구동되어 DNS 응답이 가능한 네임서버인지 확인합니다.

매스터 네임서버 : ns1.my-domain.re.kr (192.168.1.53)
슬레이브 네임서버 : ns2.my-domain.re.kr (192.168.2.53)
슬레이브 네임서버 : ns3.my-domain.re.kr (192.168.3.53)

도메인 존 지정 설정

BIND DNS 환경설정 파일인 named.conf 파일에 다음과 같은 사항을 추가 설정합니다.

매스터 네임서버 경우:

```
zone "my-domain.re.kr" IN {
    type master;                // "매스터 존"으로 지정
    file "my-domain.kr.zone";  // 도메인 존 파일명 지정
    allow-transfer { 192.168.2.53; 192.168.3.53; };
          // 도메인의 슬레이브 네임서버에 대해 존 전송 허용 설정
};
```

슬레이브 네임서버 경우:

```
zone "my-domain.re.kr" IN {
    type slave;                 // “슬레이브 존“으로 지정
    masters { 192.168.1.53; }; // 매스터 네임서버 IP 주소 지정
    allow-transfer { none; };  // 타 서버로 존 전송 차단 설정
};
```

도메인의 매스터 네임서버에서 도메인 존 파일 설정

도메인 존 파일에 다음과 같이, 도메인의 모든 네임서버 정보를 NS 레코드를 사용하여 작성 설정합니다. 예시와 같이, 네임서버 네임이 자체 도메인 영역에 속하는 경우, 네임서버 네임에 대한 A 레코드까지 아래와 같이 빠짐없이 작성하여 설정합니다.

도메인 존 파일 저장 디렉토리인 /var/named에 “my-domain.kr.zone”의 파일이름으로 저장합니다.

```
$ORIGIN my-domain.re.kr.
$TTL 300
@           SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr (
                    2009090101    ; serial
                    1800          ; refresh (30 minutes)
                    300           ; retry (5 minutes)
                    3600000       ; expire (5 weeks 6 days 16 hours)
                    300           ; minimum (5 minutes)
                    )
            NS      ns1.my-domain.re.kr.
            NS      ns2.my-domain.re.kr.
            NS      ns3.my-domain.re.kr.

ns1         A       192.168.1.53
ns2         A       192.168.2.53
ns3         A       192.168.3.53
```

모든 네임서버 리스트를 도메인 등록정보의 네임서버 정보에 설정 등록

도메인의 모든 네임서버 정보를 빠짐없이 도메인 등록정보의 네임서버 정보 필드에 입력하여 등록합니다. 만약 기존에 도메인 존이 없는 네임서버가 등록되어 있다면 삭제합니다. 네임서버 정보가 도메인의 존 파일 NS 레코드의 정보와 일치하도록 설정합니다.

매스터 네임서버 (1차 네임서버): ns1.my-domain.re.kr (192.168.1.53)
슬레이브 네임서버 (2차 네임서버): ns2.my-domain.re.kr (192.168.2.53)
슬레이브 네임서버 (2차 네임서버): ns3.my-domain.re.kr (192.168.3.53)

□ 인터넷 서비스 영향

도메인의 등록정보에 설정된 네임서버들 중 도메인 존이 설정되어 있지 않아 도메인에 대한 정상적인 도메인 응답이 불가능한 상태의 네임서버가 있는 경우, 여러 가지 심각한 문제가 발생할 수 있습니다. 이러한 상태에 있는 도메인을 “불완전 위임(lame delegation) 도메인”이라 합니다.

불완전 위임(lame delegation) 도메인은 다음의 4 가지 비정상 응답 상태에 있는 도메인들로 구분할 수 있습니다. 각 경우에 따라 심각성 정도가 서로 다른 문제가 인터넷 서비스에 발생할 수 있습니다.

사례 1)
도메인의 위임된 네임서버에 질의했을 때 DNS 응답이 전혀 없는 경우입니다. 주로 해당 IP 주소의 네임서버가 운영되고 있지 않은 경우에 해당합니다. 도메인의 위임된 네임서버 정보를 설정할 당시에는 정상 운영되고 있었지만 어느 시점에 이 네임서버가 가동 중단 된 상태의 경우입니다..

이 경우, 인터넷 서비스 접속이 지연 및 불안정한 현상이 발생합니다. 응답 실패 네임서버로 질의 시 3~5초간 응답대기를 한 후 응답 가능한 다른 위임 네임서버에 재질의 하기 때문에 시간지연이 발생합니다. 서비스 접속에 있어서는 빈번하게 접속시간 지연현상 발생이 유발됩니다.

경우에 따라서는 불법적인 “도메인네임 무단점유(domain name hijacking)”에 의한 피해가 발생할 수 있습니다. 도메인네임 무단점유는 해당 도메인의 정당한 웹 사이트 IP 주소를 변조하여, 전혀 다른 웹 사이트로 인터넷 서비스 접속을 전환시킴으로써 심각한 문제를 야기할 수 있습니다.
이는 도메인의 일부 네임서버가 서비스 중단되거나 또 이 네임서버가 사용하던 도메인이 사용 종료되어 있을 때, 제3자에 의한 네임서버 도메인의 합법적 등록을 통해 도메인의 존 데이터를 임의로 변조 설정한 데이터로 인터넷의 DNS 질의에 대해 응답해 주는 경우에 발생할 수 있습니다. 이때 파밍(pharming)으로 인한 피해와 유사한 피해를 입을 수 있습니다.

DNS 캐시 포이즈닝 공격이 성공 가능성이 높아집니다. 네임서버가 응답 하지 않을 경우, 리커시브 네임서버는 3~5초간 응답 대기하게 됩니다. 이시간은 DNS 캐시 포이즈닝 공격자의 입장에서는 충분히 공격이 성공할 시간입니다. 이 시간 동안 리커시브 네임서버로 많은 수의 위조된 DNS 응답 패킷을 공격 시도할 수 있습니다. 공격이 성공하게 되면 공격자가 원하는 웹 사이트의 IP 주소로 위조되어 리커시브 네임서버에 캐싱되는 침해사고가 발생합니다. 이러한 공격유형을 “파밍(pharming)”이라 합니다.

사례 2)

도메인에 대해 위임된 네임서버로 DNS 질의했을 때 DNS 응답은 하지만 해당 도메인에 대한 응답은 없는 경우입니다. 이 경우 네임서버가 작동은 되고 있지만, 도메인의 존 설정이 되어있지 않은 경우에 해당합니다. 이와 같은 설정 오류는 도메인 존이 누락된 네임서버를 도메인 등록정보의 네임서버정보에 등록하였거나 초기에는 존 설정이 되어있었으나 웹 호스팅 서비스 이전 등으로 인해 네임서버를 이전하고 기존 네임서버에서는 도메인 존이 삭제 된 경우입니다. 도메인의 위임 네임서버에 변경사항이 있을 시 도메인의 네임서버 등록정보에 반영이 되어야 하는데 그렇지 못 할 경우 발생합니다.

이 경우, 인터넷 서비스에 지연이 발생합니다. 네임서버가 가동 중단된 경우보다는 시간지연이 그리 심하지는 않습니다. 도메인 존이 누락 된 네임서버에 DNS 질의 시 응답이 없기 때문에 다시 다른 네임서버에 질의를 통해 도메인에 대한 응답을 받습니다. 이렇게 불필요한 추가 질의 동작을 수행합니다.

이 경우, 사례 1처럼 불법적인 “도메인네임 무단점유(domain name hijacking)”에 의한 피해를 입을 가능성과 “DNS 캐시 포이즈닝” 공격에 의한 피해의 위험은 거의 없습니다. 도메인 존이 설정되지 않은 네임서버는 질의를 받는 즉시 응답 데이터가 없는 응답 메시지로 응답처리하기 때문입니다. 인터넷 서비스 지연 발생 외에 큰 위험요소는 없지만 네임서버 운영기관이 어느 날 해당 네임서버를 가동 중단하거나 네임서버 네임의 도메인을 사용 종료하여 제3자의 등록이 가능해지는 상황이 되면, 첫 번째 사례와 동일한 상태가 될 수 있습니다.

사례 3)
네임서버가 도메인에 대하여 에러 응답하는 경우입니다. 이는 주로 네임서버의 도메인 존 설정에 문제가 있는 경우에 해당합니다. 주로 DNS 질의 가능한 호스트의 제한 IP 주소 설정에 오류가 있는 경우, BIND DNS 네임서버 등에서 제공하고 있는 뷰(view) 설정에 오류가 있는 경우에 해당합니다.

이 경우의 서비스에 대한 영향 정도는 두 번째의 경우와 동일합니다.

사례 4)
위임된 네임서버가 도메인 존 설정이 되어 있지 않은 리커시브 네임서버인 경우입니다. 이는 앞서의 두 번째 사례에 해당할 수 있지만, 국내에 이러한 경우가 많아 네 번째 사례로 따로 분류하였습니다. 이 경우 네임서버는 자신의 캐시에 도메인의 데이터가 남아 있는 상태이면 응답 데이터로 응답하지만, 캐시에 데이터가 없는 경우는 응답 데이터 없이 응답합니다.

이 경우, 인터넷 서비스 접속 상태가 일정하지 않는 문제가 발생합니다. 네임서버의 DNS 응답 데이터가 시간에 따라 불안정하기 때문입니다. 도메인의 모든 위임된 네임서버가 이러한 상태에 있는 경우에는 간혹 인터넷 서비스 접속이 실패하는 현상이 발생합니다.

DNS 캐시 포이즈닝 공격에 의해 도메인의 인터넷 서비스 사용자가 광범위한 피해를 입을 수 있습니다. DNS 캐시 포이즈닝 공격은 리커시브 네임서버를 대상으로 하여 캐시에 위조-변조된 데이터를 저장시키는 것이 목적인 공격입니다. 위임된 네임서버가 도메인 존 설정이 없는 리커시브 네임서버인 경우, DNS 캐시 포이즈닝 공격에 의해 위조-변조된 DNS 데이터가 이 위임된 네임서버 캐시에 저장되면, 위조-변조된 데이터에 의한 피해는 이 도메인 사이트로 접속하고자 하는 인터넷 사용자 모두에게 미칠 수 있습니다. 도메인의 위임 네임서버는 리커시브 서비스를 사용하지 않는 것이 안전합니다.

도메인의 위임된 네임서버의 정확한 정보등록 관리는 인터넷 서비스의 접속 지연 방지 및 접속 불안정 현상 방지를 위해 필수적인 사항입니다. 또한 특수한 경우에는 보안 침해사고가 발생할 수 있는 취약점으로 작용하므로 더욱 중요한 관리대상 사항이라 할 수 있습니다.

현재 국내 도메인의 운영현황을 전반적으로 보면, 네임서버의 경우 호스팅 기관에 위탁하여 사용하는 경우가 많기 때문에 존 파일 데이터는 잘 관리가 되고 있는 반면에, 도메인의 관리업무는 도메인을 구입한 기관의 비전문 관리자가 담당하는 경우가 많아 제대로 관리가 되지 않는 경우가 많습니다. 도메인 관리업무 범위는 크게 3가지로 나눌 수 있습니다.

1) 도메인 네임서버 설정
2) 도메인의 존 파일 데이터
3) 도메인 등록정보의 네임서버 정보 관리

다. 도메인 SOA 레코드 설정

1) SOA 레코드 필드 설정 개요

□ 설정 기준 (참고사항)

- SOA mname 필드에 매스터 네임서버 네임을 FQDN 형식으로 설정
- SOA rname 필드에 도메인 관리자 전자메일 주소를 도메인 네임 형식으로 변환 설정
- SOA serial 필드에 도메인 존의 버전번호 설정
- SOA refresh, retry, expire, minimum 필드에 적정한 time 값 설정

□ 설정의 필요성

도메인 존의 SOA 레코드는 도메인 존 자체를 대표하는 레코드입니다. SOA 레코드가 설정된 도메인 네임은 도메인 존 네임이 됩니다. SOA 레코드는 도메인 존이 구분되어 독립적으로 관리되고 있음을 표시합니다. 따라서 도메인 존에 SOA 레코드는 단 하나만 존재할 수 있습니다.

도메인 존의 SOA 레코드에는 도메인의 각 네임서버가 도메인 존을 어떻게 관리되어야 하는지의 정보가 설정되어 있다. 또한 도메인 관리자의 전자메일 주소가 설정되어 있어 도메인 존의 관리 담당자를 표시하고 있습니다.

도메인 존은 SOA 레코드의 정보를 토대로 존 자동 관리절차를 수행합니다. 존 자동 관리절차에는 존 데이터의 초기설정, 최신 존 데이터를 요청수신하고 존 데이터를 갱신처리 하는 등의 명령이 구성되어 있고 이 명령은 매스터/슬레이브의 운영 상태에 따라 적용을 받습니다. 이 외에 존 데이터의 업데이트 여부주기, 존 데이터 업데이트 실패 시에 슬레이브 네임서버는 얼마 동안 도메인 존 데이터를 유지한 후 폐기 할 것인가 등의 값도 지정명령 합니다.

본 장에서는 SOA 레코드 설정 사항에 대한 기본적인 방법과 권고하는 설정 값 기준을 SOA 레코드의 각 필드별로 제시합니다.

SOA 레코드 설정 사항은 각 사이트 환경에 의해 결정될 수 있는 사항입니다. 여기에서 제시하는 사항은 참고를 위해 제시하고 있는 권고 사항입니다.

□ 설정 방법

다음의 각 장에서 필드별 설정 사항을 제시합니다.

□ 인터넷 서비스 영향

SOA 레코드의 필드 설정 값은 해당 필드에 따라 설정에 문제가 있는 경우, 도메인 존 데이터의 관리 안정성에 영향을 줄 수 있습니다. 네임서버에 의한 도메인 존 데이터 관리 안정성에 문제가 있는 경우, 관련 인터넷 서비스의 안정성에도 경우에 따라 접속 지연, 접속 불안정 등의 영향을 줄 수 있습니다.

2) 매스터 네임서버 도메인 네임 설정

□ 설정 기준 (참고사항)

- SOA mname 필드에 매스터 네임서버 네임을 FQDN 형식으로 설정

□ 설정의 필요성

SOA 레코드의 첫 번째 필드인 mname(master name) 필드는 도메인 존의 매스터 네임서버 도메인 네임을 설정하는 필드입니다.

mname 필드는 SOA 타입 바로 다음에 위치하며 아래와 같이 “ns1.kisa-ex.or.kr”의 네임서버 도메인 네임을 지정합니다. NS 레코드로 지정된 네임서버들 중 “ns1.kisa-ex.or.kr”이 매스터 네임서버 임을 표시하고 있습니다.

```
kisa-ex.or.kr.          300 IN SOA ns1.kisa-ex.or.kr. domain.kisa-ex.or.kr. (
                          2009072201 ; serial
                          1800       ; refresh (30 minutes)
                          300        ; retry (5 minutes)
                          3600000    ; expire (5 weeks 6 days 16 hours)
                          300        ; minimum (5 minutes)
                          )
```

mname 필드의 값은 네임서버 동작에 있어 영향을 거의 미치지 않습니다. 도메인 존의 존 전송을 할 때에도 참조되지 않고 named.conf의 매스터 서버의 IP주소 정보를 사용합니다.

하지만 후에 추가된 DNS 확장표준 기능을 적용하는 경우, SOA mname 필드에 설정된 값이 네임서버의 관련 동작에 영향을 미치는 경우가 있습니다.

DNS 동적업데이트(Dynamic Update) 기능을 사용할 경우 외부 인터넷에 있는 호스트가 DNS Update 패킷을 보낼 매스터 네임서버를 파악할 때 이 SOA의 mname 필드의 값을 이용하여 도메인 존 데이터의 변경 등의 명령을 수행합니다.

DNS Notify/IXFR을 사용하여 도메인 존 전송 방식을 사용할 경우, 매스터 도메인 존의 변경사항을 DNS Notify 메시지를 사용하여 알릴 때 SOA mname 필드를 사용하여 슬레이브 네임서버 리스트를 결정하게 됩니다. DNS Notify(RFC1996)는 매스터 도메인 존의 변경사항 발생 시 매스터가 슬레이브 네임서버로 즉시 그 변경 사실을 통지하는 방법을 정의한 표준기능입니다. IXFR은 AXFR을 대체하는 존 전송을 위한 질의타입으로 도메인 존의 증분 존 전송(Incremental Zone Transfer, RFC1995)을 위한 표준 메커니즘으로 사용됩니다. IXFR은 도메인 존 전체 전송이 아니라 새로이 변경된 사항의 데이터만 전송하게 되는 효율적인 존 데이터 전송 방식입니다. AXFR보다 더욱 효과적인 도메인 존 데이터 동기화 관리 메커니즘을 구현할 수 있게 합니다. DNS Notify 패킷을 송출할 때 도메인의 존의 NS 레코드 리스트를 먼저 산출하게 되고 그 중에서 SOA mname 필드에 지정 네임서버를 제외한 나머지 네임서버를 슬레이브 네임서버 간주하여 이들에게 DNS Notify 메시지를 송출하게 됩니다. 따라서 SOA mname 필드에 매스터가 아닌 슬레이브 네임서버가 설정된 경우 DNS Notify/IXFR 메커니즘 적용 환경에서 매스터 도메인의 변경사항 통지를 이 슬레이브 네임서버만 받지 못하여 도메인 존의 데이터 동기화 관리에 문제가 발생할 수 있습니다. 이 사항은 표준 정의된 기능을 설명한 것이며, 네임서버 S/W는 관련 존 전송 동작을 세부적으로 변경 조정할 수 있는 설정 옵션을 제공합니다.

□ 설정 방법

도메인 존 파일의 SOA mname 필드 값에 매스터 네임서버의 도메인 네임을 FQDN 형식으로 설정합니다. FQDN(Fully Qualified Domain Name, 정규화된 도메인 이름)이란 도메인 네임을 전체 네임으로 표기하는 것을 의미합니다. 예를 들어 일반적으로 사용하는 도메인 네임 “www.kisa-ex.or.kr”의 FQDN 형식은 루트 도메인 네임(“.”)까지 표시된 네임 “www.kisa-ex.or.kr.” 입니다.

<예시 1>

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 네임서버 :
ns1.my-domain.re.kr. 192.168.1.53 (매스터 네임서버)
ns2.my-domain.re.kr. 192.168.2.53
ns3.my-domain.re.kr. 192.168.3.53

이 경우 도메인 존 파일의 SOA 레코드는 다음과 같이 설정합니다.

```
my-domain.re.kr.    300 IN SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr. (
                           2009090105 ; serial
                           1800       ; refresh (30 minutes)
                           300        ; retry (5 minutes)
                           3600000    ; expire (5 weeks 6 days 16 hours)
                           300        ; minimum (5 minutes)
                           )
                    300 IN NS ns1.my-domain.re.kr.
                    300 IN NS ns2.my-domain.re.kr.
                    300 IN NS ns3.my-domain.re.kr.
```

이 경우는, 존 파일에 $ORIGIN을 지정하지 않은 경우입니다. 이 경우 SOA mname 필드에는 “ns1.my-domain.re.kr.”과 같이 FQDN 형식으로 매스터 네임서버 네임을 설정합니다.

만일, 존 파일에 $ORIGIN 지시자를 사용하여 도메인 존 네임을 지정한다면, 아래와 같이 도메인 존 네임 부분을 생략하여 설정할 수 있습니다.

```
$ORIGIN my-domain.re.kr.
@                   300 IN SOA ns1 dnsadm (
                           2009090105 ; serial
                           1800       ; refresh (30 minutes)
                           300        ; retry (5 minutes)
                           3600000    ; expire (5 weeks 6 days 16 hours)
                           300        ; minimum (5 minutes)
                           )
                    300 IN NS ns1.my-domain.re.kr.
                    300 IN NS ns2.my-domain.re.kr.
                    300 IN NS ns3.my-domain.re.kr.
```

$ORIGIN 지시자 란? 도메인 존 파일 작성의 편의를 위한 표준사항입니다. 네임서버의 존 파일은 FQDN이 아닌 네임은 $ORIGIN에 설정 된 도메인

네임이 뒤에 추가되어 있는 것으로 간주하여 FQDN의 도메인 네임으로 번역하고 DNS 존 데이터 영역의 반영처리를 합니다.

주의 사항

아래와 같이 “ns1.my-domain.re.kr”과 같은 FQDN이 아닌 네임으로 지정한 경우, 설정에 오류가 발생할 수 있다는 점입니다.

```
$ORIGIN my-domain.re.kr.
@                   300 IN SOA ns1.my-domain.re.kr dnsadm.my-domain.re.kr ( ... )
```

이 경우, 네임서버는 존 파일에서 SOA mname을 “ns1.my-domain.re.kr.”이 아니라 “ns1.my-domain.re.kr.my-domain.re.kr”으로 해석하여 네임서버에 반영합니다. “ns1.my-domain.re.kr”의 네임이 FQDN의 네임이 아니므로 이 네임에 $ORIGIN으로 지정된 도메인 네임을 부가하여 해석하기 때문에 반드시 데이터 마지막에 “.“을 붙이도록 해야 합니다.

만일 매스터 네임서버 도메인 네임이 도메인 영역을 벗어난 영역에 있는 네임이라면, 반드시 FQDN의 네임으로 표기해야 합니다.

<예시 2>

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 네임서버 :
ns1.example.kr. 192.168.1.53 (매스터 네임서버)
ns2.example.kr. 192.168.2.53
ns3.example.kr. 192.168.3.53

이 경우, SOA mname 필드의 네임서버 네임은 반드시 $ORIGIN의 지정 데이터가 아닌 “ns1.example.kr.”의 FQDN으로 아래와 같이 표기해야 합니다. 도메인 존 영역에 속해 있지 않은 도메인 네임은 FQDN의 네임으로 표기해야 합니다.

```
$ORIGIN my-domain.re.kr.
@               300 IN SOA ns1.example.kr. dnsadm (
                       2009090105 ; serial
                       1800       ; refresh (30 minutes)
                       300        ; retry (5 minutes)
                       3600000    ; expire (5 weeks 6 days 16 hours)
```

```
                        300       ; minimum (5 minutes)
                        )
                300 IN NS ns1.example.kr.
                300 IN NS ns2.example.kr.
                300 IN NS ns3.example.kr.
```

□ 인터넷 서비스 영향

DNS 확장 표준 기능인 DNS Update 기능이나 DNS Notify/IXFR 메커니즘을 사용하지 않는다면 SOA mname 설정이 잘못 설정되어 있어도 별다른 문제점이 발생하지 않습니다.

DNS 동적 업데이트 기능이나 DNS Notify/IXFR 메커니즘을 사용하는 환경에서는 SOA mname 설정 오류로 인해 원하지 않았던 동작 오류 현상을 겪을 수 있습니다.

특히 DNS Notify/IXFR 메커니즘을 사용하는 경우, SOA mname 필드에 매스터 네임서버 네임이 아닌 슬레이브 네임서버 네임이 설정되어 있는 경우, SOA mname에 설정된 슬레이브 네임서버를 매스터 네임서버로 간주하여 DNS Notify 메시지가 송출되지 않아 해당 슬레이브 네임서버는 존 데이터가 갱신되지 않습니다. 이럴 경우 네임서버들 간의 도메인 존 데이터 동기화 실패 문제점이 발생하게 됩니다. 도메인 존 데이터 동기화 실패는 인터넷 서비스 접속에 혼란을 발생시키는 장애를 유발할 수 있습니다.

3) 도메인 관리자 전자메일 설정

□ 설정 기준 (참고사항)

- SOA rname 필드에 도메인 관리자 전자메일 주소를 도메인 네임 형식으로 변환 설정

□ 설정의 필요성

SOA rname은 도메인 관리 책임자(responsible person)의 전자메일 주소을 지정하는 필드입니다.

SOA rname은 네임서버의 동작에 영향을 미치지 않습니다. 도메인 관리 상 상호 업무 협력의 용이성을 위해 도메인의 관리자 연락처 정보를 공개하는 용도로 설정합니다.

□ 설정 방법

SOA rname 필드는 SOA mname 필드의 다음에 위치해 있으며, 다음의 예시에서 “domain.kisa-ex.or.kr.”에 해당합니다.

```
kisa-ex.or.kr.          300 IN SOA ns1.kisa-ex.or.kr. domain.kisa-ex.or.kr. (
                          2009072201 ; serial
                          1800       ; refresh (30 minutes)
                          300        ; retry (5 minutes)
                          3600000    ; expire (5 weeks 6 days 16 hours)
                          300        ; minimum (5 minutes)
                          )
```

SOA rname 필드는 도메인 네임 포맷의 데이터를 갖도록 정의되어 있습니다. 따라서 전자메일 주소 그대로 설정하지 않고, 도메인 네임 형식으로 변환하여 설정합니다. 위 예시에서 “domain.kisa-ex.or.kr.”는 전자메일 주소 “domain@kisa-ex.or.kr”을 FQDN 도메인 네임으로 변환하여 설정한 데이터입니다.

전자메일 주소를 SOA rname 필드의 도메인 네임으로 변환하는 규칙은 단순합니다. 전자메일 주소 문자열에서 사용자 계정명과 도메인 명을 구분하는 "@" 문자를 "."으로 대치하고 이 문자열을 도메인 네임으로 간주하여 FQDN 형식으로 표기하기 위해 마지막에 "."을 추가합니다. FQDN 형식의 도메인 네임 문자열 "domain.kisa-ex.or.kr."을 SOA rname 필드에 설정합니다.

전자메일 주소의 사용자 계정에 "." 문자가 포함되어 있다면, 이를 "\."으로 대치한 후 위의 변환을 수행합니다. 예를 들어 전자메일 주소로 "dns.admin@kisa-ex.or.kr"를 사용하고 있다면, 먼저 메일주소 사용자 계정의 "." 문자를 "\."으로 대치하여 "dns\.admin@kisa-ex.or.kr"의 문자열을 산출하고, 이에 대해 앞서의 변환 규칙을 적용하여 "dns\.admin.kisa-ex.or.kr."을 최종적으로 산출하여 이를 SOA rname 필드에 적용합니다.

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 관리자 메일 계정 :
dnsadm@my-domain.re.kr

이 경우 도메인 존 파일의 SOA 레코드는 다음과 같이 설정합니다.

```
my-domain.re.kr.    300 IN SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr. (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                        300 IN NS ns1.my-domain.re.kr.
                        300 IN NS ns2.my-domain.re.kr.
                        300 IN NS ns3.my-domain.re.kr.
```

존 파일에 $ORIGIN 지시자를 사용하여 도메인 존 네임을 지정한다면, 아래와 같이 도메인 존 네임 부분을 생략하여 설정할 수 있습니다.

```
$ORIGIN my-domain.re.kr.
```

```
@                   300 IN SOA ns1 dnsadm (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                    300 IN NS ns1.my-domain.re.kr.
                    300 IN NS ns2.my-domain.re.kr.
                    300 IN NS ns3.my-domain.re.kr.
```

만일 전자메일 계정이 "dnsadm@example.kr"과 같이 도메인 영역에 속하지 않는다면, 반드시 FQDN의 네임으로 설정해야 합니다. 다음은 이 경우의 예시입니다.

```
$ORIGIN my-domain.re.kr.
@                   300 IN SOA ns1 dnsadm.example.kr. (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                    300 IN NS ns1.my-domain.re.kr.
                    300 IN NS ns2.my-domain.re.kr.
                    300 IN NS ns3.my-domain.re.kr.
```

□ 인터넷 서비스 영향

SOA rname 필드 설정에 문제가 있어도 인터넷 서비스에는 문제가 발생하지 않습니다.

4) Serial 번호 설정

□ 설정 기준 (참고사항)

- SOA serial 필드에 도메인 존의 버전번호 설정

□ 설정의 필요성

SOA serial 필드는 도메인 존 데이터의 버전 정보를 표시하는 역할을 합니다. 특히 매스터 네임서버와 슬레이브 네임서버 간의 도메인 존 데이터 갱신 절차에서 도메인 존 데이터의 변경 여부를 판단하는 기준이 됩니다.

SOA serial 필드의 데이터 형식은 숫자입니다. 0 ~ 4,294,967,295 사이의 숫자 값으로 설정할 수 있습니다. SOA serial 필드에 "YYYYMMDDnn"의 형식을 갖는 번호를 설정하는 것이 바람직하다는 권고 사항이 있지만, 꼭 이렇게 설정할 필요는 없습니다. "YYYYMMDDnn" 형식의 표기는 도메인 존 데이터 변경이 일어난 일자와 순번을 표기하는 형식으로, 2009년 10월 8일에 두 번째 존 데이터 수정을 하였다면 "2009100802"과 같이 표기하는 방식을 의미합니다. 이는 도메인 존이 언제 변경된 것인지를 누구나 쉽게 바로 파악할 수 있도록 하기 위해 제안된 형식입니다. DNS 동적 업데이트를 적용한 환경에서는 네임서버가 도메인 존 데이터를 변경하고 동시에 해당 도메인 존의 SOA serial 번호를 자동으로 하나 증가시키기 때문에 이 경우에는 네임서버가 주로 SOA serial 번호를 관리하게 됩니다.

□ 설정 방법

SOA serial 필드는 rname 필드 바로 다음에 위치합니다. 아래 예시에서는 "2009072201"에 해당합니다.

```
kisa-ex.or.kr.          300 IN SOA ns1.kisa-ex.or.kr. domain.kisa-ex.or.kr. (
                          2009072201 ; serial
                          1800       ; refresh (30 minutes)
                          300        ; retry (5 minutes)
                          3600000    ; expire (5 weeks 6 days 16 hours)
                          300        ; minimum (5 minutes)
                          )
```

SOA serial 번호는 관리상의 편이성에 따라 설정합니다. 다만, 음수 또는 4,294,967,295의 값을 초과하는 값을 설정하지 않도록 합니다.

도메인 존 데이터를 수작업으로 변경하는 경우, SOA serial 번호 역시 증가된 번호로 수정하여 네임서버에 반영합니다. 특히 네임서버를 중단시키지 않고 변경된 도메인 존 파일을 반영하는 작업의 경우, 슬레이브 네임서버는 매스터 네임서버의 수정된 도메인 존 파일의 SOA serial 번호를 검사하는데 serial 번호가 동일한 경우, 수정된 도메인 존 파일의 데이터를 무시하여 존 데이터의 갱신을 처리하지 않습니다.

SOA serial 번호를 관리하지 않는 경우, 네임서버들 간의 도메인 존 데이터 불일치 문제가 발생할 수 있습니다. 도메인 존 파일의 데이터를 수정하고 나서 SOA serial 번호를 수정하지 않았다고 가정합니다. 이때 매스터 네임서버를 중단시키고 다시 구동하면 수정된 존 파일은 이전 버전정보를 갖고 있지 않기 때문에 초기 버전 데이터로 처리하여 네임서버에 정상적으로 반영됩니다. 관리자는 작업이 정상적으로 완료되었다고 생각합니다. 하지만 슬레이브 네임서버에서 문제가 발생합니다. 슬레이브 네임서버들은 주기적으로 매스터 네임서버에 SOA 질의를 하여 존 데이터 갱신 여부를 확인하는 과정에서 serial 번호가 동일하기 때문에 도메인 존 전송 요청을 하지 않습니다. 결과적으로 매스터 네임서버와 슬레이브 네임서버 간 존 데이터 불일치 상태로 됩니다. 모든 네임서버가 serial 번호는 동일하지만 존 데이터 불일치 상태가 되는 것입니다. 이런 상황은 생각보다 쉽게 일어날 수 있습니다.

□ 인터넷 서비스 영향

SOA serial 번호 관리에 실수가 있는 경우, 네임서버들 간의 존 데이터 불일치 문제가 발생할 우려가 있습니다. 이 경우, 변경되지 않은 존 데이터를 유지하고 있는 네임서버를 사용하여 인터넷 서비스에 접근하는 사용자는 접속 장애를 겪을 수 있습니다. 변경된 웹 사이트 주소가 아닌, 이미 동작이 중단된 이전의 웹 사이트 주소를 응답받아 접속 시도 할 수 있기 때문입니다.

5) 기타 Timeout 필드 설정

□ 설정 기준 (참고사항)

- SOA refresh, retry, expire, minimum 필드에 적정한 time 값 설정

□ 설정의 필요성

SOA 필드 중 refresh, retry, expire, minimum 필드는 도메인 존 데이터 관리를 수행하는 데에 필요한 각종 time 값을 지정하는 필드입니다.

SOA refresh, retry, expire 필드는 슬레이브 네임서버가 도메인 존 데이터 전체의 관리를 수행하는 과정에서 필요한 time 값을 지정합니다.

1) refresh - 얼마의 주기로 매스터 도메인 존 데이터의 변경 여부를 체크할 것인지를 지정
2) retry - SOA refresh에 지정된 주기에 존 데이터의 갱신에 실패한 경우, 얼마의 시간 후에 다시 존 데이터 갱신을 시도할 것인지를 지정
3) expire - SOA refresh 주기에 존 데이터 갱신 시도 실패가 계속 이어질 때, 얼마의 시간 동안 이 도메인 존을 슬레이브 네임서버가 유지하여 DNS 응답을 수행할 것인지를 지정. SOA expire에 지정된 시간이 다하면 슬레이브 네임서버는 이 도메인 존 데이터를 폐기처리 합니다.
4) minimum - 리커시브 네임서버가 이 도메인 존에 없는 레코드 응답을 받았을 때 해당 레코드 정보를 얼마동안 캐시에 저장할 것인지를 설정하는 timeout 값을 지정

SOA refresh, retry, expire, minimum 필드는 설정 값의 적절성 여부에 의해 도메인 데이터의 자동 관리 메커니즘의 안정성에 영향을 끼칠 수 있습니다. 너무 작은 값의 설정이나 너무 큰 값의 설정 모두 부정적인 문제를 유발할 수 있습니다. 그러나 어떤 특정한 값을 반드시 설정해야 한다는 고정된 기준은 없습니다.

여기서는 인터넷 표준 문서들 가운데 제시된 권고 설정 값을 소개합니다. 이는 표준 규정 사항은 아니며, 참고 정보에 해당합니다.

□ 설정 방법

SOA refresh, retry, expire, minimum 필드의 time 값은 모두 초 단위의 값으로 설정합니다. 네임서버 S/W에 따라서는 존 파일이나 입력 화면에서 분 단위나 시간 단위 등으로 값을 표시할 수 있도록 하는 경우가 있습니다. 이는 네임서버 S/W가 이러한 입력 형식의 값을 분석할 수 있는 기능을 가지고 있는 경우에 가능합니다.

SOA refresh 필드는 슬레이브 네임서버가 매스터 도메인 존의 SOA serial 번호를 체크하여 존 데이터 갱신을 실행하는 주기 시간을 지정합니다. 슬레이브 네임서버는 매스터 네임서버의 도메인 존에 SOA 질의를 하여 serial 값이 증가한 것을 확인하면 데이터 업데이트 처리절차를 수행합니다. SOA refresh값 주기가 길면 매스터/슬레이브 네임서버의 존 데이터가 불일치 상태가 해당 주기만큼 길게 유지하게 됩니다. 도메인 존의 데이터 변동이 자주 발생하는 경우에는 SOA refresh 필드 값을 길지 않게 설정하는 것이 필요합니다.

슬레이브 네임서버는 매스터 네임서버로 도메인의 SOA 질의를 하여 SOA serial 번호를 파악하여 존 데이터의 버전 번호가 증가해 있는 경우에 존 전송 요청을 하여 존 데이터 업데이트 처리절차를 수행합니다. SOA refresh 시간이 너무 길면 매스터 도메인 존 데이터의 수정 시점과 슬레이브 존 업데이트 시점 간격이 길어질 수 있어 매스터/슬레이브 네임서버의 존 데이터가 불일치 상태에 오랫동안 있을 수 있습니다. 특히 도메인 존의 데이터 변동이 자주 발생하는 경우에는 SOA refresh 필드 값을 길지 않게 설정하는 것이 필요합니다.

다만, DNS Notify를 적용한 존 전송 메커니즘을 적용한 경우에는 SOA refresh 값에 큰 영향을 받지 않게 됩니다. DNS Notify 메시지를 통해 매스터 존 데이터의 변경 사실을 매스터 네임서버가 즉시 슬레이브 네임서버로 통지하여 바로 슬레이브 네임서버에 의한 SOA serial 번호 체크 및 존 전송 절차를 개시할 수 있기 때문입니다.

SOA refresh :
- 최소/최대 값 범위 : 20분 (1,200초) ~ 2일 (172,800초)

DNS Notify 미적용 시 SOA refresh 권고 설정 값 범위:
- 권고 설정 값 범위 : 20분 (1,200초) ~ 2 시간 (7,200초)

SOA retry 필드는 슬레이브 네임서버가 SOA refresh 주기에 의한 매스터 존 업데이트에 실패한 경우, 다시 재시도하는 시간 간격을 지정합니다. 이 시간은 적정한 값으로 설정하되, SOA refresh 주기 시간보다는 짧은 시간으로 설정하는 것이 필요합니다. SOA refresh 주기보다 긴 SOA retry의 재시도 수행 시간 간격은 무의미하기 때문입니다.

SOA retry :
- 설정 값 : SOA refresh 설정 값 보다 작은 값

SOA expire 필드는 네임서버가 SOA refresh에 의한 존 데이터 갱신을 시도하는데 계속 유효한 실패가 지속된다면 처음 실패가 발생한 시간부터 SOA expire필드의 지정 시간까지 경과하면 슬레이브 네임서버는 이 도메인의 데이터를 폐기처리하고 더 이상 질의응답을 하지 않습니다.

SOA expire 필드 값은 매스터 네임서버에 장애가 발생했을 때, 복구하는 데에 소요되는 최대 시간을 감안하여 충분히 긴 시간을 설정하는 것이 바람직합니다. 이 시간에는 매스터 네임서버의 장애발생 감지에 실패하여 경과될 수 있는 시간도 포함합니다. 경험적으로 SOA expire 필드 값은 최소한 SOA refresh 값의 약 7배에 해당하는 값보다 크게 설정하는 것을 권고하고 있습니다.

SOA expire :
- 최소/최대 값 범위 : 1주(604,800초) ~ 약 6주(3,600,000초) 또는 그 이상
- SOA refresh 값의 7배 값보다 큰 값

SOA minimum 필드는 원래 도메인 존의 리소스 레코드 중 TTL(Time To Live) 값이 지정되지 않은 레코드에 적용하는 최소 TTL 값을 지정하는 용도로 정의되었습니다. 현재는 음성 캐싱(negative caching) 레코드의 TTL 값으로 주로 작용하고 있습니다. 음성 캐싱(negative caching)은 네임서버에 질의한 결과 질의한 도메인 네임의 레코드 데이터가 존재하지 않은 경우, minimum 필드의 값을 TTL 값으로 대체하여 부재 데이터를 리커시브 네임서버의 캐시 영역에 minimum 필드의 시간동안 저장하게 됩니다. 또 다시 존재하지 않는 레코드 질의 시 캐싱 데이터로 응답을 받게 됩니다.

따라서 SOA minimum 필드에 지정하는 시간 값은 도메인 존 데이터에 설정되지 않은 레코드에 대한 응답 결과를 리커시브 네임서버 캐시에 저장하는 시간을 지정하는 역할을 합니다. 이 시간이 길면 존에 설정되어 있지 않는 레코드에 대한 불필요한 질의 트래픽이 감소하게 됩니다. 그러나 너무 긴 시간을 설정하여 새로운 레코드를 도메인에 추가 설정하는 경우, 문제가 발생할 수도 있습니다. 예로써 도메인 존에 www.my-domain.re.kr의 레코드가 누락된 상태에서 호스트 측에서 질의를 통해 부재 데이터가 리커시브 네임서버에 음성 캐싱(negative caching)되어있는 상태라고 가정합니다. 이때 SOA minimum 필드 값은 12주의 시간으로 설정되어 있었고, 후에 호스트 측에서 질의를 할 경우 www.my-domain.re.kr의 레코드가 12주의 TTL을 갖고 있기 때문에 최대 12주의 시간동안 부재 데이터를 응답받아 www.my-domain.re.kr을 사용한 접속이 불가능해집니다. 이 시간이 경과하여 데이터가 소멸되어야 리커시브 네임서버가 www.my-domain.re.kr에 대한 새로운 질의를 비로소 시작하기 때문입니다.

SOA minimum :
- 최소/최대 값 범위 : 3분 (180초) ~ 2시간 (7,200초)
- 특별한 사유가 없다면 1시간 ~ 2시간 사이의 값 설정 권고

□ 인터넷 서비스 영향

도메인 존의 SOA refresh, retry, expire, minimum 필드는 도메인의 네임서버 사이에서 도메인 존 데이터의 유지관리 동작 수행을 위한 시간 정보를 담고 있습니다.

SOA refresh, retry, expire, minimum 필드 값은 반드시 설정해야 할 설정 기준 값은 없으며 사이트마다 사이트 운영환경 특성에 따라 값을 설정합니다. 다만, 각 필드의 정의에 따라 너무 큰 값이나 너무 작은 값은 안정적인 도메인 존 데이터 유지관리에 있어 문제를 야기할 수 있습니다.

SOA refresh, retry, expire, minimum 필드의 적절치 않은 설정에 의해 발생할 수 있는 문제로는 아래와 같다.

1) SOA refresh, retry 필드의 부적절 값 설정으로 인해 각 네임서버의 도메인 존 데이터 동기화 지연 및 이로 인한 응답 데이터 불일치 문제
2) SOA expire 필드의 시간이 너무 짧을 경우 매스터 네임서버 장애 시 슬레이브 네임서버의 도메인 존 데이터 유지기간이 짧아 도메인 질의응답이 전면 중단 될 수 있다.
3) SOA minimum 필드의 시간을 너무 길게 지정하면 신규 추가 레코드의 질의응답 불능이 장기화 될 수 있다.

6) 무난한 SOA 레코드 설정 방법 예시

도메인의 SOA 필드 설정에 있어서 기준으로 삼을 수 있는 설정 내용을 제시합니다. 이는 SOA 필드 설정 값의 결정에 곤란을 겪을 경우 대체로 무난한 설정 값을 제시하기 위한 것으로 단지 참고 사항으로 제시하는 것입니다.

예시 도메인 정보
도메인: my-domain.re.kr
매스터 네임서버 네임 : ns1.my-domain.re.kr
도메인 담당자 전자메일 주소 : dnsadmin@my-domain.re.kr

이 경우, 다음과 같은 사항으로 설정합니다.

```
my-domain.re.kr.    300 IN SOA ns1.my-domain.re.kr. dnsadim.my-domain.re.kr. (
                            2009100101 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
```

SOA serial 번호는 DNS 동적 업데이트(DNS Update)를 적용하는 도메인이 아닌 경우, 데이터 변경작업 일자와 일련번호 형태의 "2009100101"으로 설정하는 것이 좋습니다. 도메인 존 버전의 변경 여부 및 이력을 한 눈에 파악할 수 있어 문제가 발생했을 때 보다 용이하게 도메인 버전을 확인할 수 있습니다.

SOA refresh 필드 값은 약 30분으로 설정하는 것이 무난한 것으로 보입니다. 최대 약 30분이 경과한 후에는 모든 네임서버의 도메인 존 데이터가 새로이 갱신된 데이터로 동기화 된 것을 확인할 수 있을 것입니다.

SOA retry 필드 값은 약 5분으로 설정합니다. SOA refresh 필드 값을 약 30분으로 설정했으므로, 만일 도메인 존 갱신 체크 중에 문제가 발생하면 5분 간격으로 도메인 존 데이터 갱신을 다시 시도하도록 설정합니다. 도메인 존

갱신 체크가 실패하는 경우는 주로 매스터 네임서버의 장애 또는 매스터 네임서버까지의 네트워크 구간에 장애가 발생한 경우에 해당합니다. 약 5분의 재시도 시간 간격을 통해 일시적인 장애에 의한 도메인 동기화 불일치 상황은 큰 지연 없이 복구될 수 있을 것으로 보입니다.

SOA expire 필드 값은 1,000 시간으로 설정합니다. 이는 약 5 주간 6 일 16 시간에 해당합니다. 매스터 네임서버의 심각한 시스템 장애가 발생하여 동작 중단되었을 경우, 적어도 한 달에 한번 정도는 점검이 이루어질 것으로 보고 약 5주정도면 충분히 매스터 네임서버의 장애가 파악 될 것이라는 가정에 의한 것입니다. 슬레이브 네임서버는 이 기간에 이전 도메인 존 데이터를 보유하게 됩니다.

SOA minimum 필드 값은 약 5분으로 설정합니다. 현재 도메인 존에 없는 레코드를 신규로 추가 설정했을 때, 최대 약 5분 후에는 사용자가 이 신규 레코드의 조회가 가능해 집니다. 만약 12시간이나 24시간 등으로 길게 설정했을 경우, 이 시간동안 사용자는 신규 레코드의 조회를 하지 못하게 됩니다.

위 사항은 최근의 국내 일반적 인터넷 환경에 비추어 제시하는 설정 값입니다. 각 사이트의 특유한 운영환경 특성에 따라 조정된 값의 적용이 필요할 수 있습니다.

라. 도메인 NS 레코드 설정

□ 설정 기준 (참고사항)

- NS 레코드에 도메인의 네임서버 네임을 FQDN 형식으로 설정
- 네임서버 네임에 대해 CNAME 레코드 설정 금지 권고

□ 설정의 필요성

NS 레코드는 도메인 존이 설정된 네임서버를 지정 설정하는 레코드입니다.

NS 레코드는 도메인의 네임서버의 도메인 네임을 지정하는 레코드입니다. 하지만 간혹 가다가 네임서버 IPv4의 주소를 지정하는 경우가 있는데 도메인 존파일 파싱과정에서 오류검출이 되지 않고 IPv4 주소를 네임서버 도메인 네임으로 인식하는 경우가 있습니다. 이런 경우 오류이기 때문에 주의해야 할 사항입니다.

리커시브 네임서버는 도메인 존에 설정된 네임서버 설정 정보를 참조하여 DNS 질의를 수행합니다. 리커시브 네임서버는 상위 도메인인 .kr 도메인으로부터 파악한 위임된 네임서버 정보보다 도메인 존에 설정된 NS 레코드의 네임서버 정보를 우선적으로 신뢰하여 이를 기준으로 동작합니다. 곧 도메인 존에 설정된 NS 레코드의 네임서버가 실제 리커시브 네임서버가 지속적인 DNS 질의대상으로 삼는 네임서버이게 됩니다.

NS 레코드 설정에 있어서 주의할 사항은 NS 레코드로 설정된 네임서버 네임은 CNAME 레코드를 갖지 않도록 해야 한다는 점입니다. 네임서버 네임에 CNAME 레코드가 지정되어 있는 경우, 네임서버가 도메인의 네임서버 리스트를 응답함에 있어 최소한의 응답 메시지로 응답처리하지 못하고 추가적인 질의응답 절차 혹은 응답 지연이 발생할 수 있기 때문입니다. NS 레코드로 지정하는 네임서버의 도메인 네임에는 CNAME 레코드를 설정하지 않도록 권고하고 있습니다.

□ 설정 방법

NS 레코드에는 도메인의 네임서버 도메인 네임을 FQDN의 도메인 네임을 사용하여 설정합니다. 그리고 네임서버 도메인 네임이 이 도메인에 속한 경우, 네임서버의 IP 주소 레코드를 함께 설정합니다.

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 네임서버 :
ns1.my-domain.re.kr. 192.168.1.53 (매스터 네임서버)
ns2.my-domain.re.kr. 192.168.2.53
ns3.my-domain.re.kr. 192.168.3.53

이 경우 도메인 존 파일의 NS 레코드는 다음과 같이 설정합니다.

```
my-domain.re.kr.    300 IN SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr. (
                           2009090105 ; serial
                           1800       ; refresh (30 minutes)
                           300        ; retry (5 minutes)
                           3600000    ; expire (5 weeks 6 days 16 hours)
                           300        ; minimum (5 minutes)
                           )
                    300 IN NS ns1.my-domain.re.kr.
                    300 IN NS ns2.my-domain.re.kr.
                    300 IN NS ns3.my-domain.re.kr.


ns1.my-domain.re.kr.   300 IN A  192.168.1.53
ns2.my-domain.re.kr.   300 IN A  192.168.2.53
ns3.my-domain.re.kr.   300 IN A  192.168.3.53
```

이 경우는, 존 파일에 $ORIGIN을 지정하지 않은 경우입니다. 이 경우 NS 레코드의 네임서버 네임 필드에 “ns1.my-domain.re.kr.”과 같이 FQDN 형식으로 네임서버 네임을 설정합니다.

만일, 존 파일에 $ORIGIN 지시자를 사용하여 도메인 존 네임을 지정한다면, 아래와 같이 도메인 존 네임 부분을 생략하여 설정할 수 있습니다.

```
$ORIGIN my-domain.re.kr.
```

```
@                   300 IN SOA ns1 dnsadm (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                    300 IN NS ns1
                    300 IN NS ns2
                    300 IN NS ns3
ns1                  300 IN A  192.168.1.53
ns2                  300 IN A  192.168.2.53
ns3                  300 IN A  192.168.3.53
```

$ORIGIN 지시자 란? 도메인 존 파일 작성의 편의를 위한 표준사항입니다. 네임서버의 존 파일은 FQDN이 아닌 네임은 $ORIGIN에 설정 된 도메인 네임이 뒤에 추가되어 있는 것으로 간주하여 FQDN의 도메인 네임으로 번역하고 DNS 존 데이터 영역의 반영처리를 합니다.

NS 레코드로 지정하여 설정한 네임서버의 네임에 CNAME 레코드를 사용하지 않습니다.

아래와 같이 네임서버 네임 ns1.my-domain.re.kr에 대하여 CNAME 레코드를 사용하여 ns1.my-domain.re.kr로 설정한 경우, 도메인의 네임서버 리스트 정보를 응답할 때 불필요한 시간 지연이 발생할 수 있으며 DNS 질의응답의 효율성을 떨어뜨리는 요인이 될 수 있다. 그리고 CNAME 레코드의 잘못된 설정으로 IP 주소를 응답하지 못하는 경우도 발생할 수 있으므로, 네임서버의 네임에 대해서는 CNAME 레코드를 설정하지 않고 직접 IP주소 레코드(A 레코드, AAAA레코드)를 설정하는 것이 바람직합니다.

```
$ORIGIN my-domain.re.kr.
@                   300 IN SOA ns1 dnsadm (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                    300 IN NS ns1
                    300 IN NS ns2
                    300 IN NS ns3
ns1                  300 IN CNAME dns1
ns2                  300 IN CNAME dns2
```

```
ns3                 300 IN CNAME dns3
dns1                300 IN A  192.168.1.53
dns2                300 IN A  192.168.2.53
dns3                300 IN A  192.168.3.53
```

만일 네임서버의 도메인 네임이 도메인 영역을 벗어난 영역에 있는 네임이라면, 반드시 FQDN의 네임으로 표기해야 합니다.

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 네임서버 :
ns1.example.kr. 192.168.1.53 (매스터 네임서버)
ns2.example.kr. 192.168.2.53
ns3.example.kr. 192.168.3.53

이 경우, 네임서버 네임은 반드시 "ns1.example.kr."의 FQDN으로 아래와 같이 표기해야 합니다. 다른 네임서버 네임도 마찬가지입니다. 도메인 존 영역에 속해 있지 않은 도메인 네임은 FQDN의 네임으로 표기해야 합니다.

주의사항
네임서버 네임이 해당 도메인 존 영역에 속하지 않는 네임인 경우, 이 도메인 존에 네임서버의 IP 주소 레코드를 설정할 수 없습니다. 도메인 존에 설정하는 데이터는 이 도메인 존에 속하는 도메인 네임에 대한 레코드만 설정 가능하기 때문입니다. 따라서 아래와 같이 NS 레코드만 설정하고, 각 네임서버의 네임에 대한 IP 주소 설정 데이터는 등록하지 않습니다.

```
$ORIGIN my-domain.re.kr.
@               300 IN SOA ns1.example.kr. dnsadm (
                       2009090105 ; serial
                       1800       ; refresh (30 minutes)
                       300        ; retry (5 minutes)
                       3600000    ; expire (5 weeks 6 days 16 hours)
                       300        ; minimum (5 minutes)
                       )
                300 IN NS ns1.example.kr.
                300 IN NS ns2.example.kr.
                300 IN NS ns3.example.kr.
```

이 경우, ns1.example.kr의 네임서버 IP 주소는 리커시브 네임서버가 별도의 질의를 거쳐 example.kr 도메인의 네임서버로부터 파악하게 됩니다.

□ 인터넷 서비스 영향

NS 레코드에는 네임서버의 도메인 네임을 설정합니다.

도메인의 NS 레코드는 도메인의 SOA 레코드와 함께 도메인이 설정된 네임서버 구성을 정의하는 역할을 하는 레코드입니다. 곧 도메인의 구성 정보를 표현합니다.

NS 레코드에 오류가 있는 네임서버를 설정하는 경우, 도메인에 대한 질의응답이 원활하지 않을 수도 있습니다.

NS 레코드에 네임서버의 도메인 네임이 아닌 IP 주소를 설정한 경우, 인터넷의 리커시브 네임서버들은 이 도메인의 네임서버 정보를 올바로 파악할 수 없게 됩니다.

아래와 같이, NS 레코드에 IP 주소를 지정 설정한 경우, 네임서버는 별다른 오류 메시지를 출력하지 않고 존 파일을 반영 처리합니다.

```
$ORIGIN my-domain.re.kr.
@               300 IN SOA ns1 dnsadm (
                       2009090105 ; serial
                       1800       ; refresh (30 minutes)
                       300        ; retry (5 minutes)
                       3600000    ; expire (5 weeks 6 days 16 hours)
                       300        ; minimum (5 minutes)
                       )
                300 IN NS 192.168.1.53
                300 IN NS 192.168.2.53
                300 IN NS 192.168.3.53
```

그러나 이 도메인의 네임서버 도메인 네임은 FQDN 형식이 아니기 때문에 "192.168.1.53.my-domain.re.kr."과 같은 방식으로 해석되어 도메인 존 데이터에 적용되며, 이와 같은 내용으로 DNS 응답에 사용됩니다. 관리자는 NS 타입의 레코드를 착오로 네임서버의 IP 주소로 설정하는 실수를 범하여 결국에는 이 도메인의 네임서버 정보가 정확히 설정되지 않아 운영환경에 따라서 DNS 질의응답이 불안정하게 됩니다.

마. 도메인 MX 레코드 설정

□ 설정 기준 (참고사항)

- MX 레코드에 도메인의 메일서버 네임을 FQDN 형식으로 설정
- 메일서버 네임에 대해 CNAME 레코드 설정 금지 권고

□ 설정의 필요성

MX 레코드는 수신용 메일서버의 도메인 네임을 설정하는 레코드입니다. 메일발송용 전자메일은 설정하지 않으며, 도메인의 전자메일을 수신할 수 있는 메일서버를 외부에 널리 알리기 위한 레코드 타입입니다.

MX 레코드는 전자메일 서비스를 위한 레코드로써, 전자메일 메시지의 라우팅 정보를 제공하는 역할을 합니다.

전자메일을 이 도메인으로 발송할 때 발송하는 메일서버는 도메인의 네임서버 도메인 존에 MX 레코드를 조회하여 도메인의 메일서버와 IP주소를 파악합니다. 이때 MX 레코드가 없는 경우, 도메인의 A(AAAA)레코드를 조회하여 응답한 데이터를 전자메일서버의 주소로 간주합니다.

전자메일 서비스를 사용하지 않는 경우에도 MX 레코드를 명시적으로 설정하는 것이 바람직합니다. 그렇지 않은 경우, 도메인의 A 레코드(AAAA 레코드)로 지정한 엉뚱한 서버 시스템으로 전자메일이 전송 시도될 가능성이 있습니다.

MX 레코드에 설정된 메일서버의 도메인 네임에 대해서는 CNAME 레코드를 설정하지 않도록 권고하고 있습니다. DNS 응답 메시지 하나로 전자메일 서버의 IP 주소까지 신속하게 응답 처리할 수 있도록 하기 위해서는 CNAME 레코드를 전자메일의 도메인 네임에 설정하지 않는 것이 필요합니다.

□ 설정 방법

MX 레코드에는 도메인의 메일서버 도메인 네임을 FQDN의 도메인 네임을 사용하여 설정합니다. 그리고 메일서버 도메인 네임이 이 도메인에 속한 경우, 메일서버의 IP 주소 레코드를 함께 설정합니다.

다른 타입의 레코드와는 달리 MX 레코드는 우선순위 필드를 함께 가지고 있습니다. MX 레코드의 우선순위(preference) 필드에는 전자메일 수신 우선순위를 0 ~ 65,535의 값으로 표현하여 설정할 수 있습니다. 작은 값일수록 높은 우선순위를 갖습니다. 외부 인터넷의 메일발송 메일서버는 작은 값의 우선순위를 갖는 메일서버를 우선하여 접속 시도합니다.

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 네임서버 :
  ns1.my-domain.re.kr. 192.168.1.53 (매스터 네임서버)
  ns2.my-domain.re.kr. 192.168.2.53
  ns3.my-domain.re.kr. 192.168.3.53
도메인의 메일서버 (우선순위 순):
  smtp1.my-domain.re.kr. 192.168.1.25
  smtp2.my-domain.re.kr. 192.168.2.25
  smtp3.my-domain.re.kr. 192.168.3.25

이 경우 도메인 존 파일의 MX 레코드는 다음과 같이 설정합니다.

```
my-domain.re.kr.    300 IN SOA ns1.my-domain.re.kr. dnsadm.my-domain.re.kr. (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                        300 IN NS ns1.my-domain.re.kr.
                        300 IN NS ns2.my-domain.re.kr.
                        300 IN NS ns3.my-domain.re.kr.

                        300 IN MX 10 smtp1.my-domain.re.kr.
                        300 IN MX 20 smtp2.my-domain.re.kr.
                        300 IN MX 30 smtp3.my-domain.re.kr.

smtp1.my-domain.re.kr.  300 IN A  192.168.1.25
smtp2.my-domain.re.kr.  300 IN A  192.168.2.25
smtp3.my-domain.re.kr.  300 IN A  192.168.3.25

ns1.my-domain.re.kr.    300 IN A  192.168.1.53
ns2.my-domain.re.kr.    300 IN A  192.168.2.53
ns3.my-domain.re.kr.    300 IN A  192.168.3.53
```

이 경우는, 존 파일에 $ORIGIN을 지정하지 않은 경우입니다. 이 경우 NS 레코드의 네임서버 네임 필드에 "smtp1.my-domain.re.kr."과 같이 FQDN 형식으로 네임서버 네임을 설정합니다.

만일, 존 파일에 $ORIGIN 지시자를 사용하여 도메인 존 네임을 지정한다면, 아래와 같이 도메인 존 네임 부분을 생략하여 설정할 수 있습니다.

```
$ORIGIN my-domain.re.kr.
@                   300 IN SOA ns1 dnsadm (
                            2009090105 ; serial
                            1800       ; refresh (30 minutes)
                            300        ; retry (5 minutes)
                            3600000    ; expire (5 weeks 6 days 16 hours)
                            300        ; minimum (5 minutes)
                            )
                        300 IN NS ns1
                        300 IN NS ns2
                        300 IN NS ns3

                        300 IN MX 10 smtp1
                        300 IN MX 20 smtp2
                        300 IN MX 30 smtp3

smtp1                    300 IN A  192.168.1.25
```

```
smtp2                300 IN A  192.168.2.25
smtp3                300 IN A  192.168.3.25

ns1                  300 IN A  192.168.1.53
ns2                  300 IN A  192.168.2.53
ns3                  300 IN A  192.168.3.53
```

$ORIGIN 지시자 란? 도메인 존 파일 작성의 편의를 위한 표준사항입니다. 네임서버의 존 파일은 FQDN이 아닌 네임은 $ORIGIN에 설정 된 도메인 네임이 뒤에 추가되어 있는 것으로 간주하여 FQDN의 도메인 네임으로 번역하고 DNS 존 데이터 영역의 반영처리를 합니다.

MX 레코드로 지정하여 설정한 메일서버의 네임에 CNAME 레코드를 사용하지 않습니다. 아래와 같이 메일서버 네임 smtp1.my-domain.re.kr에 대하여 CNAME 레코드를 사용하여 mail1.my-domain.re.kr로 설정한 경우, 도메인의 메일서버 리스트 정보를 응답할 때 불필요한 시간 지연이 발생할 수 있으며 하나의 응답에 필요한 메일서버 IP 주소를 응답하지 못하는 경우도 발생할 수 있습니다. 이는 DNS 질의응답의 효율성을 떨어뜨리는 요인이 될 수 있으므로, 메일서버의 네임에 대해서는 CNAME 레코드를 설정하지 않고 직접 IP 주소 레코드(A 레코드, AAAA 레코드)를 설정하는 것이 바람직합니다.

도메인의 네임서버 리스트 정보를 응답할 때 불필요한 시간 지연이 발생할 수 있으며 DNS 질의응답의 효율성을 떨어뜨리는 요인이 될 수 있습니다. 그리고 CNAME 레코드의 잘못된 설정으로 IP 주소를 응답하지 못하는 경우도 발생할 수 있으므로, 네임서버의 네임에 대해서는 CNAME 레코드를 설정하지 않고 직접 IP주소 레코드(A 레코드, AAAA레코드)를 설정하는 것이 바람직합니다.

```
$ORIGIN my-domain.re.kr.
@                    300 IN SOA ns1 dnsadm (
                             2009090105 ; serial
                             1800       ; refresh (30 minutes)
                             300        ; retry (5 minutes)
                             3600000    ; expire (5 weeks 6 days 16 hours)
                             300        ; minimum (5 minutes)
                             )
                     300 IN NS ns1
                     300 IN NS ns2
                     300 IN NS ns3

                     300 IN MX 10 smtp1
                     300 IN MX 20 smtp2
```

```
                    300 IN MX 30 smtp3

  smtp1              300 IN CNAME mail1
  smtp2              300 IN CNAME mail2
  smtp3              300 IN CNAME mail3

  mail1              300 IN A  192.168.1.25
  mail2              300 IN A  192.168.2.25
  mail3              300 IN A  192.168.3.25

  ns1               300 IN A  192.168.1.53
  ns2               300 IN A  192.168.2.53
  ns3               300 IN A  192.168.3.53
```

만일 메일서버의 도메인 네임이 도메인 영역을 벗어난 영역에 있는 네임이라면, 반드시 FQDN의 네임으로 표기해야 합니다.

다음과 같은 도메인이 있다고 가정합니다.

도메인 명 : my-domain.re.kr
도메인의 네임서버 :
  ns1.example.kr. 192.168.1.53 (매스터 네임서버)
  ns2.example.kr. 192.168.2.53
  ns3.example.kr. 192.168.3.53
도메인의 메일서버 (우선순위 순):
  smtp1.example.kr. 192.168.1.25
  smtp2.example.kr. 192.168.2.25
  smtp3.example.kr. 192.168.3.25

이 경우, 메일서버 네임은 반드시 “smtp1.example.kr.”의 FQDN으로 아래와 같이 표기해야 합니다. 다른 네임서버 네임도 마찬가지입니다. 도메인 존 영역에 속해 있지 않은 도메인 네임은 FQDN의 네임으로 표기해야 합니다.

주의사항
메일서버 네임이 해당 도메인 존 영역에 속하지 않는 네임인 경우, 이 도메인 존에 메일서버의 IP 주소 레코드를 설정할 수 없습니다. 도메인 존에 설정하는 데이터는 이 도메인 존에 속하는 도메인 네임에 대한 레코드만 설정 가능하기 때문입니다. 따라서 아래와 같이 MX 레코드만 설정하고, 각 메일서버의 네임에 대한 IP 주소 설정 데이터는 등록하지 않습니다.

```
$ORIGIN my-domain.re.kr.
@               300 IN SOA ns1.example.kr. dnsadm (
                       2009090105 ; serial
                       1800       ; refresh (30 minutes)
                       300        ; retry (5 minutes)
                       3600000    ; expire (5 weeks 6 days 16 hours)
                       300        ; minimum (5 minutes)
                       )

                300 IN NS ns1.example.kr.
                300 IN NS ns2.example.kr.
                300 IN NS ns3.example.kr.

                300 IN MX 10 smtp1.example.kr.
                300 IN MX 20 smtp2.example.kr.
                300 IN MX 30 smtp3.example.kr.
```

이 경우, smtp1.example.kr의 메일서버 IP 주소는 리커시브 네임서버가 별도의 질의를 거쳐 example.kr 도메인 존의 네임서버로부터 파악하게 됩니다.

□ 인터넷 서비스 영향

MX 레코드는 전자메일 인터넷 서비스에 직접 영향을 미치는 레코드입니다. MX 레코드의 설정오류는 전자메일 서비스의 정상적인 동작을 저해할 수 있습니다.

바. 도메인의 전자메일 발송정책(SPF) 설정

□ 설정의 필요성

SFP는 “메일서버등록제(Sender Policy Framework)”의 약어입니다. 메일서버 정보를 사전에 DNS에 공개 등록함으로써 수신자로 하여금 이메일에 표시된 발송자 정보가 실제 메일서버의 정보와 일치하는지를 확인할 수 있도록 하는 인증기술입니다. (한국정보보호진흥원 http://www.kisarbl.or.kr)

□ 설정 방법

SPF의 설정은 도메인 존에서 TXT 타입의 레코드를 이용하여 사이트의 메일 발송을 수행하는 메일서버 리스트를 외부에 공개하여 공지하는 역할을 담당합니다.

MX 레코드를 사용하는 메일서버 도메인과 동일할 수도 있지만 MX 레코드에 설정된 메일서버는 수신을 위한 메일서버이고 SPF용 TXT 레코드로 공개된 네임서버는 외부로 메일을 발송하는 네임서버가 대상이 됩니다. 보통은 동일하지만 상이할 수도 있습니다.

도메인의 SPF 레코드 설정작업은 다음의 한국정보보호진흥원 RBL 사이트에서 제공하고 있는 “SPF Record 작성 도우미” 웹 페이지를 활용하여 작업지시에 따라 생성하고 네임서버에 반영하는 절차를 수행합니다. SPF 레코드 문자열 내용을 직접 작성하는 것이 필요한 경우, 아래 제시된 “SPF 기술문서” 자료를 참고하여 작성합니다.

한국정보보호진흥원 RBL 사이트 (http://www.kisarbl.or.kr)

다음은 DNS의 SPF 레코드 및 관련 메일서비스 설정사항에 대하여 한국정보보호진흥원이 배포하고 있는 기술자료 정보입니다.

SPF 설치 및 운영 지침서
배포 : 한국정보보호진흥원 불법스팸대응센터 (http://www.spamcop.or.kr)
"자료실"의 2005년 10월 7일자 게시물 "SPF 설치 및 운영 지침서"
DNS 네임서버와 메일서버의 SPF 관련 설정사항

SPF 기술문서
배포 : 한국정보보호진흥원 불법스팸대응센터 (http://www.spamcop.or.kr)
"자료실"의 2005년 10월 7일자 게시물 "SPF 기술문서"
SPF 세부 기술사항 및 SPF 레코드 문자열 정의어 상세 사항

□ 인터넷 서비스 영향

SPF 레코드의 올바른 설정은 해당 도메인 사이트에서 합법적으로 발송하고 있는 전자메일이 스팸으로 오인 받지 않고 정상적으로 송달될 수 있도록 합니다.

□ 주의사항

SPF 레코드는 주로 DNS의 TXT 레코드를 사용하여 설정합니다. TXT 타입 레코드는 문자열을 설정하기 위한 레코드입니다. SPF 타입 레코드가 별도로 정의되어 있으나, 이를 지원하지 않는 네임서버가 많을 수 있으므로, TXT 타입 레코드를 사용하여 설정합니다.

SPF를 위한 TXT 타입 레코드는 도메인에 대하여 설정합니다. 도메인 my-domain.re.kr의 경우 아래와 같은 형태로 설정합니다.

```
my-domain.re.kr.    IN TXT  "v=spf1 ip4:1.2.3.4 ip4:1.2.3.5 -all"
```

SPF를 위한 TXT 타입 레코드는 하나의 레코드만 설정할 수 있습니다. 아래와 같이 2개 이상의 TXT 레코드를 설정한 경우는 설정에 오류가 있는 경우입니다.

```
my-domain.re.kr.    IN TXT  "v=spf1 ip4:1.2.3.4 -all"
my-domain.re.kr.    IN TXT  "v=spf1 ip4:1.2.3.5 -all"
```

5. DNS 설정오류 점검 방법

도메인의 안정적 구성에 있어 가장 중요한 사항은 “도메인의 위임 설정”입니다. “도메인의 위임설정”에 오류가 있거나 미흡한 구성일 경우, 도메인 전체 및 이 도메인을 사용하는 인터넷 서비스에 영향을 끼치는 문제를 발생시킬 수 있습니다.

“도메인의 위임설정”은 도메인을 등록했을 때, 이 도메인의 네임서버 정보를 상위의 부모 도메인 존에 설정하는 것을 말합니다. 네임서버를 ‘도메인의 위임된 네임서버’라 하며, 네임서버 정보를 ‘위임정보’라 합니다. .kr 도메인을 등록한 경우는 그 부모 도메인은 .kr 도메인 존에 설정합니다. 이때 설정하는 네임서버 위임정보 데이터는 도메인의 네임서버 네임과 도메인의 네임서버 IP 주소입니다.

도메인의 네임서버 정보는 인터넷에서 해당 도메인에 대한 DNS 질의응답이 원활히 진행되도록 하기 위한 중요한 정보로 작용합니다.

도메인의 위임된 네임서버 설정은 도메인 등록대행을 하였던 기관의 웹 사이트의 “도메인 등록정보”의 “네임서버 정보” 메뉴를 통해 설정 요청합니다. 설정 요청한 정보는 .kr 도메인 등록관리 시스템으로 전달되어 .kr 도메인 네임서버의 .kr 도메인 존에 반영 처리하는 절차를 거치게 됩니다. .kr 도메인의 경우, DNS 동적 업데이트 기능을 도입입하여 적용하고 있어서, 도메인 등록 대행 기관에서 네임서버 정보변경 신청을 하면 거의 실시간으로 .kr 네임서버에 해당 데이터가 반영 처리되고 있습니다.

다음으로 도메인의 위임설정 상태 점검을 하는 방법에 대해 설명합니다. 이를 위해서 DNS 점검도구에 대한 간단한 소개를 하고, 이어 도메인의 위임설정 상태 점검 방법을 예시를 사용하여 구체적으로 설명합니다.

도메인의 설정 상태 점검을 하기 위해서 DNS 점검도구를 사용하여 반복적 질의를 하는 방법을 먼저 파악하는 것이 필요합니다.

가장 일반적인 DNS 점검도구로는 dig과 nslookup이 있습니다.

dig과 nslookup은 시스템 OS 설치 패키지에 포함되어 있는 경우가 대부분입니다. 기본적으로 제공되지 않는 경우, BIND DNS 배포 패키지를 사용하여 어렵지 않게 설치하여 사용할 수 있습니다.

가. dig 기본 사용법

dig(domain information groper)은 BIND DNS 네임서버 패키지에 포함하여 배포되고 있는 DNS 점검용 유틸리티입니다.

dig은 네임서버에 대한 DNS 질의응답 절차를 다양한 형태로 수행할 수 있고, 네임서버의 응답 메시지의 상세한 내용을 확인할 수 있도록 합니다.

BIND DNS 패키지에 포함된 dig 유틸리티는 BIND DNS 네임서버의 질의응답 절차 라이브러리 루틴을 그대로 사용하여 동작하기 때문에 네임서버의 DNS 질의응답 절차 중에 발생하는 문제점을 검출해낼 수 있습니다.

BIND DNS 네임서버가 설치된 Unix/Linux 시스템에서는 기본적으로 dig 유틸리티가 설치되어 있습니다. Windows PC의 경우 dig을 사용하려면, 별도의 설치 및 설정 절차가 필요합니다. Windows PC에서의 dig 설치 절차는 다음 장에서 제시합니다.

dig은 다양한 형태의 DNS 질의응답 점검 작업을 지원하기 위해 옵션을 제공합니다. 여기서는 도메인 구성 상태 점검에 필요한 기본적인 사항을 중심으로 사용법을 설명하고 예시를 보입니다.

O dig 사용 명령어 구문

dig의 기본적인 명령어 구문은 다음과 같습니다. dig의 모든 옵션을 참조하려면 “dig -h”를 실행하여 사용법을 참조합니다.

```
dig [@server] [name] [type] [class] [queryopt...]
```

@server	: 질의대상 네임서버 IP 주소 또는 도메인 네임
name	: 질의 도메인 네임 (예: www.my-domain.re.kr)
type	: 질의 리소스 레코드 타입 (예: A)
class	: 질의 클래스 (예: IN)
queryopt	: dig 유틸리티에 부가할 수 있는 다양한 옵션

인자들을 "[]"으로 표시한 것은 이들 인자들이 생략 가능하다는 의미입니다. 인자를 주지 않고 "dig"만 수행한 경우, 시스템의 디폴트 네임서버로 루트 도메인('.')에 대한 A 타입 질의를 수행합니다.

각 인자를 생략하는 경우, 기본 값을 적용하여 동작합니다. 다음은 각 인자를 생략한 경우, 적용되는 기본 값입니다.

@server	: 시스템에 설정되어 있는 질의대상 기본 네임서버 IP 주소
name	: 루트 도메인 ('.')
type	: IPv4 주소 레코드 타입 (A)
class	: 인터넷 클래스 (IN)

dig을 사용한 일반적인 질의의 예시입니다. www.kisa-ex.or.kr 도메인 네임에 대한 IPv4 주소를 질의하는 경우입니다.

```
$ dig www.kisa-ex.or.kr

; <<>> DiG 9.3.1 <<>> www.kisa-ex.or.kr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1797
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL:
0

;; QUESTION SECTION:
;www.kisa-ex.or.kr.                     IN      A

;; ANSWER SECTION:
www.kisa-ex.or.kr.        300     IN      A       169.254.50.86
```

```
;; AUTHORITY SECTION:
kisa-ex.or.kr.          300     IN      NS      ns0.kisa-ex.or.kr.
kisa-ex.or.kr.          300     IN      NS      ns1.kisa-ex.or.kr.
kisa-ex.or.kr.          300     IN      NS      ns2.kisa-ex.or.kr.

;; Query time: 59 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Jul  7 13:22:36 2009
;; MSG SIZE  rcvd: 102
```

위 예시를 기준으로 DNS 응답 메시지의 구성을 간단히 설명합니다.

DNS 응답 메시지는 1) 헤더, 2) Query 섹션, 3) Answer 섹션, 4) Authority 섹션, 5) Additional 섹션으로 구성되어 있습니다.

DNS 메시지의 헤더에 해당하는 부분은 다음의 부분입니다. DNS 헤더의 각 필드를 파싱하여 아래와 같이 수치를 출력해 주고 있습니다.

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1797
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL:
0
```

“status: NOERROR” : NOERROR는 조회 과정에서 에러 없이 처리되어 정상적으로 응답하고 있음을 의미합니다. 이 필드는 질의에 대한 응답상태 코드를 나타냅니다. 에러가 발생한 경우 이 필드 값은 NOERROR가 아닌 다른 코드 값을 가집니다. 아래의 코드뿐만 아니라 정의된 응답코드가 더 있으나, 특수한 경우에 발생하는 경우에 해당하므로, 설명을 생략합니다.

status 에러 코드 설명

1) NXDOMAIN: 질의된 도메인 네임이 존재하지 않음을 나타냅니다.
2) SERVFAIL: 네임서버가 조회과정 중에 에러가 발생하여 질의된 사항을 처리하지 못했음을 의미합니다.
3) REFUSED: 네임서버가 해당 질의에 대해 처리를 거부함을 의미합니다.

4) NOTIMP: 질의된 사항에 대해 네임서버가 아직 구현되지 않아 지원할 수 없음을 의미합니다.

Query 섹션에 해당하는 부분입니다. 응답 메시지는 Query 섹션에 질의했던 사항을 그대로 반영하여 응답합니다.

```
;; QUESTION SECTION:
;www.kisa-ex.or.kr.                    IN      A
```

Answer 섹션에 해당하는 부분입니다. 질의한 사항에 대한 응답 데이터를 설정합니다. 이 경우 www.kisa-ex.or.kr의 IPv4 주소인 A 레코드 데이터가 응답되고 있습니다.

```
;; ANSWER SECTION:
www.kisa-ex.or.kr.        300     IN      A       169.254.50.86
```

Authority 섹션에 해당하는 부분입니다. Authority 섹션에는 응답된 데이터가 속한 도메인 존에 대한 정보를 설정하여 응답합니다. 이 사례와 같이 응답 데이터로 응답된 경우, NS 레코드로 네임서버 정보를 설정하여 응답합니다. 응답 데이터가 없는 경우는, 도메인 존의 SOA 레코드가 설정됩니다.

```
;; AUTHORITY SECTION:
kisa-ex.or.kr.          300     IN      NS      ns0.kisa-ex.or.kr.
kisa-ex.or.kr.          300     IN      NS      ns1.kisa-ex.or.kr.
kisa-ex.or.kr.          300     IN      NS      ns2.kisa-ex.or.kr.
```

O authoritative 네임서버에 대한 반복적 질의

dig은 기본동작으로 재귀적(recursive) 질의를 요청합니다.

도메인 존 보유 네임서버에 대한 점검용 질의인 경우, 반복적 질의(iterative)

를 수행하는 것이 필요합니다.

dig에서 반복적 질의는 “+norecurse” 옵션을 사용하여 수행합니다.

다음은 kisa-ex.or.kr 네임서버에 대해 www.kisa-ex.or.kr의 IPv4 주소를 질의하는 예시입니다. 이 경우는 도메인 존이 정상 설정된 네임서버로 질의한 경우에 해당합니다.

```
$ dig @ns0.kisa-ex.or.kr www.kisa-ex.or.kr +norecurse

; <<>> DiG 9.3.1 <<>> @ns0.kisa-ex.or.kr www.kisa-ex.or.kr
+norecurse
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 811
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4

;; QUESTION SECTION:
;www.kisa-ex.or.kr.                     IN      A

;; ANSWER SECTION:
www.kisa-ex.or.kr.        300     IN      A       169.254.50.86

;; AUTHORITY SECTION:
kisa-ex.or.kr.            300     IN      NS      ns1.kisa-ex.or.kr.
kisa-ex.or.kr.            300     IN      NS      ns2.kisa-ex.or.kr.
kisa-ex.or.kr.            300     IN      NS      ns0.kisa-ex.or.kr.

;; ADDITIONAL SECTION:
ns0.kisa-ex.or.kr.        300     IN      A       169.254.1.53
ns0.kisa-ex.or.kr.                300           IN            AAAA
2001:dc5:0:10:169:254:50:52
ns1.kisa-ex.or.kr.        300     IN      A       169.254.50.51
```

```
ns2.kisa-ex.or.kr.        300     IN      A       169.254.100.53

;; Query time: 413 msec
;; SERVER: 169.254.1.53#53(169.254.1.53)
;; WHEN: Tue Jul  7 15:09:27 2009
;; MSG SIZE  rcvd: 178
```

다음의 응답 메시지의 헤더 부분을 보면, flags 필드에 “aa”를 설정하여 응답하고 있습니다.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 811
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4
```

이 “aa" flag는 Authoritatie 로 응답이 되었다는 것을 의미합니다. 이 네임서버에는 kisa-ex.or.kr의 도메인 존이 설정되어있고, 응답 데이터인 www.kisa-ex.or.kr의 A 레코드는 도메인 kisa-ex.or.kr 존 데이터로부터 직접 응답된 것임을 표시합니다. 리커시브 네임서버로 질의하여 응답된 메시지에는 flag에 “aa" 없이 응답합니다. 이 경우 응답한 리커시브 네임서버에는 해당 도메인 존이 없고 대신 인터넷 상의 네임서버에서 조회하여 응답받은 데이터로 응답하고 있음을 표시합니다.

이 사항은 “도메인 존이 설정되어 있어야 할 네임서버에 도메인 존이 제대로 설정되어 있는지” 점검할 때 활용합니다.

O 계층적 위임설정 상태 확인용 trace 기능

dig의 “+trace” 옵션을 사용하면, 루트 도메인부터 질의대상 도메인에 이르기까지의 도메인 계층구조에 따른 질의절차를 수행시켜 도메인 구성상의 문제가 없는지 점검할 수 있습니다.

www.kisa-ex.or.kr에 대한 IPv4 주소 질의에 대해 “+trace” 옵션을 적용한 경우입니다.

```
$ dig www.kisa-ex.or.kr +trace

; <<>> DiG 9.3.1 <<>> www.kisa-ex.or.kr +trace
;; global options:  printcmd
.                       508599  IN      NS      F.ROOT-SERVERS.NET.
.                       508599  IN      NS      G.ROOT-SERVERS.NET.
.                       508599  IN      NS      H.ROOT-SERVERS.NET.
.                       508599  IN      NS      I.ROOT-SERVERS.NET.
.                       508599  IN      NS      J.ROOT-SERVERS.NET.
.                       508599  IN      NS      K.ROOT-SERVERS.NET.
.                       508599  IN      NS      L.ROOT-SERVERS.NET.
.                       508599  IN      NS      M.ROOT-SERVERS.NET.
.                       508599  IN      NS      A.ROOT-SERVERS.NET.
.                       508599  IN      NS      B.ROOT-SERVERS.NET.
.                       508599  IN      NS      C.ROOT-SERVERS.NET.
.                       508599  IN      NS      D.ROOT-SERVERS.NET.
.                       508599  IN      NS      E.ROOT-SERVERS.NET.
;; Received 456 bytes from 127.0.0.1#53(127.0.0.1) in 5 ms

kr.                     172800  IN      NS      G.DNS.kr.
kr.                     172800  IN      NS      B.DNS.kr.
kr.                     172800  IN      NS      C.DNS.kr.
kr.                     172800  IN      NS      D.DNS.kr.
kr.                     172800  IN      NS      E.DNS.kr.
kr.                     172800  IN      NS      F.DNS.kr.
;; Received 284 bytes from 192.5.5.241#53(F.ROOT-SERVERS.NET) in
6 ms

kisa-ex.or.kr.                          86400      IN           NS
ns0.kisa-ex.or.kr.
kisa-ex.or.kr.                          86400      IN           NS
ns1.kisa-ex.or.kr.
kisa-ex.or.kr.                          86400      IN           NS
ns2.kisa-ex.or.kr.
;; Received 162 bytes from 202.31.190.1#53(G.DNS.kr) in 4 ms

www.kisa-ex.or.kr.        300     IN      A       169.254.50.86
kisa-ex.or.kr.           300     IN      NS      ns1.kisa-ex.or.kr.
kisa-ex.or.kr.           300     IN      NS      ns2.kisa-ex.or.kr.
kisa-ex.or.kr.           300     IN      NS      ns0.kisa-ex.or.kr.
;; Received 178 bytes from 169.254.1.53#53(ns0.kisa-ex.or.kr) in
3 ms
```

루트 도메인 존으로부터 질의대상 도메인 존까지의 위임을 따라 dig이 질의하는 절차를 위와 같이 출력합니다.

“+trace" 옵션은 대상 도메인이 인터넷에서 원활하게 사용되고 있는지 확인하는 수단으로 사용될 수 있습니다. 다만 반복수행하여 항상 정상적인 응답이 이루어지는지 확인하는 것이 필요합니다. 이유는 ”trace" 옵션에 의한 dig 질의절차가 도메인의 모든 네임서버에 대해 질의하는 것이 아니기 때문에 질의를 하지 않은 일부 설정미흡 네임서버를 발견하지 못하기 때문입니다.

도메인의 위임설정 상태 점검을 위해 “+trace” 옵션을 적용한 dig 질의 외에 추가적으로 다음에 소개하는 “+nssearch” 옵션을 사용한 점검을 수행하는 것을 권고합니다.

O 도메인의 네임서버 구성 상태 점검 nssearch 기능

도메인의 네임서버들이 모두 도메인 존 설정이 되어 있는지 여부에 대한 점검은 중요합니다.

dig의 옵션 중 “+nssearch” 옵션은 도메인에 설정된 모든 네임서버를 추적하여 도메인의 SOA 레코드 응답내용을 일괄 점검하는 기능을 제공합니다.
사용법은 다음과 같습니다.

```
dig 도메인 +nssearch

  도메인 : 점검하고자 하는 도메인 명 (SOA 레코드를 갖는 도메인명)
```

다음은 “+nssearch” 옵션을 사용하여 도메인에 대하여 도메인의 모든 네임서버에 대해 SOA 레코드를 점검하는 경우를 예시합니다.

```
$ dig safedns.kr +nssearch
SOA ns1.safedns.kr. domain-manager.nic.or.kr. 2009070701 3600 900 604800 7200 from server
ns1.safedns.kr in 109 ms.
SOA ns1.safedns.kr. domain-manager.nic.or.kr. 2009070701 3600 900 604800 7200 from server
ns2.safedns.kr in 125 ms.
```

수행결과 각 네임서버로부터 응답된 SOA 레코드 내용을 위와 같이 출력합니다. 이 도메인의 경우, 2개의 네임서버가 SOA 레코드를 정상적으로 응답하고 있으며, 2개 네임서버의 응답 SOA 레코드 내용이 모두 일치합니다. 만일, 이 도메인의 네임서버가 위의 2개 네임서버가 전부라면 이 도메인은 모든 네임서버에 도메인 존이 정상적으로 설정되어 있고, SOA 레코드가 모두 동일하게 유지되고 있음을 확인할 수 있습니다.

하지만 도메인의 모든 네임서버 리스트를 사전에 알고 있는 상태에서 dig의 "+nssearch" 옵션을 사용한 질의가 이루어져야 합니다. 그 이유는 도메인의 네임서버들 중 일부 네임서버에 도메인 존 설정이 되어 있지 않은 상태라면 해당 네임서버의 응답은 무시되고 dig의 출력에서 제외되기 때문입니다

O dig 출력사항 조정 및 활용

1) +short

dig의 출력사항 중 Answer 섹션의 응답 데이터만을 간단히 파악하려 경우, dig의 옵션 중 "+short" 옵션을 사용합니다.

www.kisa-ex.or.kr 도메인 네임의 IPv4 주소를 질의하는 사례입니다.

```
$ dig www.kisa-ex.or.kr +short
169.254.50.86
```

시스템에서 쉘 스크립트나 기타 스크립트 프로그램을 사용하여 DNS 질의 결과를 처리하려는 경우, "+short"를 사용한 단순한 출력을 유용하게 활용할 수 있습니다.

2) +noall, +comments, +answer

응답 데이터만이 아니라, DNS 응답 메시지 헤더 정보까지 필요한 경우가 있을 수 있습니다.

다음은 DNS 응답 메시지의 헤더 정보와 Answer 섹션의 데이터만을 출력하도록 하는 경우입니다.

```
$ dig www.kisa-ex.or.kr +noall +comments +answer

; <<>> DiG 9.3.1 <<>> www.kisa-ex.or.kr +noall +comments +answer
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1996
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL:
0

;; ANSWER SECTION:
www.kisa-ex.or.kr.        281     IN      A       169.254.50.86
```

이때 사용하는 옵션은 “+noall”, “+comments”, “+answer”입니다.
“+noall”은 모든 출력을 보이지 않게 하는 옵션입니다.
“+comments”는 헤더부분의 코멘트 내용을 출력하라는 옵션입니다.
“+answer”는 Answer 섹션의 내용을 출력하라는 옵션입니다.
모든 내용을 출력하지 않도록 한 후, 출력이 필요한 요소들을 추가하여 지정하는 방식으로 사용한 사례입니다.

dig은 도메인 존 파일의 구문규칙을 그대로 준수하여 응답 결과를 출력합니다.

다음의 출력 결과 중 “;;”으로 시작하는 라인들은 도메인 존 파일 구문에서 코멘트 문으로 처리됩니다. dig은 도메인 존 파일의 리소스 레코드 부분이 아닌 모든 출력내용을 코멘트 문으로 처리하여 출력합니다.

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1996
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL:
0

;; ANSWER SECTION:
www.kisa-ex.or.kr.        281     IN      A       169.254.50.86
```

3) “>” 활용

이와 같은 출력방식은 dig의 출력내용을 그대로 카피하여 도메인 존 파일에 붙여 넣을 수 있게 합니다.

예로써 루트 힌트 파일의 업데이트가 필요한 경우, b.root-servsers.net 네임서버로 루트 네임서버 정보를 질의한 후 dig의 출력내용을 그대로 루트 힌트 파일 named.root로 저장하여 네임서버에서 사용할 수 있습니다.

```
$ dig @b.root-servers.net . ns > named.root
```

위 방식은 원격 네임서버에 있는 도메인 존 파일을 dig을 이용하여 바로 존 파일로 저장하여 네임서버에 반영이 되게 합니다. 신규 네임서버에서 지체없이 원격의 존 데이터를 적용을 원할 경우에 존 전송(zone transter)의 주기에 관계없이 활용이 가능합니다. 물론 이 경우, 원격 네임서버에서 로컬 서버에 해당 도메인의 존 전송(zone transfer) 허용 설정을 해주어야 합니다.

다음은 원격 네임서버 192.168.1.53으로부터 my-domain.re.kr 도메인 존을 dig으로 도메인 존 데이터 전체를 응답받아 도메인 존 파일로 저장하는 예시입니다. 예시의 my-domain.re.kr-zone 파일을 네임서버의 존 파일 디렉토리에 저장하고 네임서버에 반영 설정할 수 있습니다. 물론, 이 경우 네임서버 이전으로 인한 데이터 변경사항을 my-domain.re.kr-zone 파일에서 찾아 적절하게 수정한 후 반영합니다.

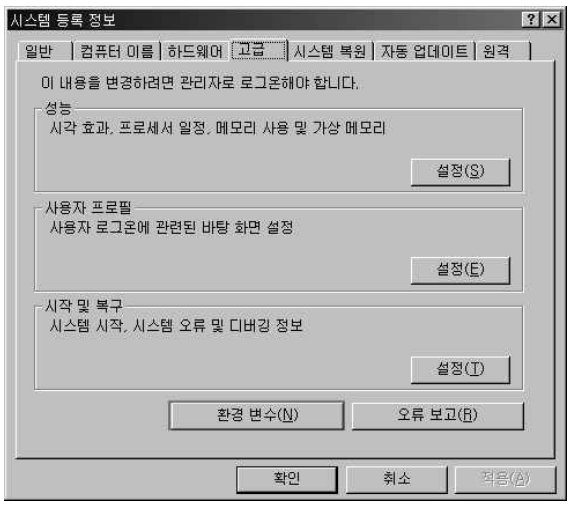
```
dig @192.168.1.53 my-domain.re.kr axfr +multiline > my-domain.re.kr-zone
```

1) Windows 호스트의 dig 설치 구성 방법

BIND DNS 패키지의 dig 유틸리티를 Windows PC에 설치하여 사용하려는 경우, 다음과 같은 절차에 따라 설치 및 설정합니다.

1. 다음의 ISC 웹 사이트에서 Windows용 바이너리 패키지 다운로드
   - BIND DNS 페이지 : http://www.isc.org/download/software/current
   - 최신 버전 BIND DNS의 "Windows Download" 링크 클릭
   - File Download: 아래 " 해당 파일 링크 클릭하여 다운로드
   - 임의의 폴더에 압축파일 압축해제 (여기서는 c:\bin에 압축해제 가정)
   - PC에서 BIND 네임서버 구동이 필요하지 않은 경우, BINDInstall.exe와 named.exe 삭제

2. 다음과 같이 "c:\bin" 디렉토리를 환경변수 PATH에 추가 설정
   - "Windows 탐색기"를 열고, "내 컴퓨터" 선택
   - 마우스 오른쪽 버튼 클릭, "내 컴퓨터"의 "속성" 선택
   - "시스템 등록정보" 화면에서 "고급" 탭 선택, "환경변수" 클릭



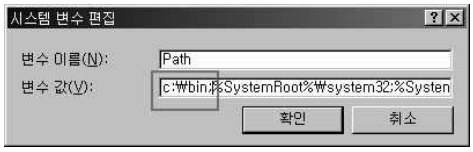
■ “환경변수” 화면에서, “시스템 변수” 항목 중 “Path” 선택

■ “편집” 클릭

■ “시스템 변수 편집” 화면에서 “변수 값” 필드의 맨 처음에

■ 다음 그림과 같이 BIND DNS 패키지 디렉토리 “c:\bin;”을 추가 설정

■ 이때, 디렉토리 구분자 “;”을 반드시 표기 필요



■ “확인”을 클릭, 변경 사항 적용

3. “명령 프롬프트” 창에서 dig 실행 테스트

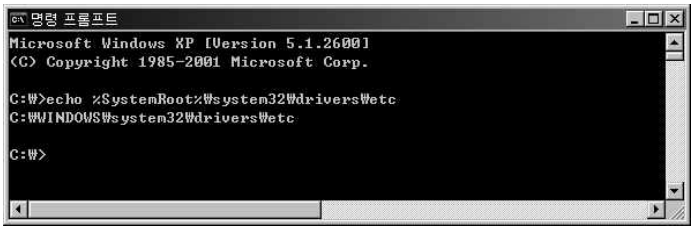
- “dig www.kisa.or.kr +short” 수행, 응답결과 확인
- 다음과 같이 IP 주소가 출력되면 정상 동작

Windows에 설치한 dig은 Windows PC에 설정되어 있는 DNS 서버를 기본 질의대상 네임서버로 사용합니다.

dig의 질의대상 기본 네임서버를 달리하여 사용하려면, resolv.conf 파일에 네임서버 리스트를 작성하여 저장합니다. resolv.conf 파일에는 다음과 같은 형식으로 네임서버 IP주소를 지정합니다.

```
nameserver 127.0.0.1
nameserver 192.168.0.53
```

resolv.conf 파일은 PC의 “%SystemRoot%\system32\drivers\etc” 시스템 디렉토리에 저장합니다. “%SystemRoot%” 값은 Windows 마다 다를 수 있습니다. “명령 프롬프트” 창에서 다음과 같이 echo 명령을 사용하여 출력되는 디렉토리에 저장합니다.



dig은 “%SystemRoot%\system32\drivers\etc” 디렉토리에서 resolv.conf 파일을 찾고, 만일 이 파일이 없는 경우, Windows PC에 설정된 네임서버 정보를 참조하여 동작합니다.

나. nslookup 기본 사용법

nslookup은 잘 알려져 있는 DNS 점검도구입니다. Windows 호스트에서 기본적으로 제공하는 유틸리티입니다. BIND DNS 패키지에도 포함되어 있으나, BIND의 개발자는 dig 사용을 권고하고 있습니다.

Windows의 nslookup 유틸리티의 사용법은 다음의 웹 페이지에 자세히 설명되어 있습니다.

- "NSlookup.exe 사용" : http://support.microsoft.com/kb/200525

nslookup은 대화형 모드 또는 명령형 모드로 사용할 수 있습니다.

다음은 대화형 모드를 사용한 기본 질의응답을 수행한 예시입니다.

```
C:\>nslookup
Default Server:  localhost
Address:  127.0.0.1

> www.kisa-ex.or.kr
Server:  localhost
Address:  127.0.0.1

Non-authoritative answer:
Name:    www.kisa-ex.or.kr
Address:  169.254.50.86

> exit

C:\>
```

다음은 명령형 모드를 사용하여 동일한 기본 질의응답을 수행한 예시입니다.

```
C:\>nslookup www.kisa-ex.or.kr
Server:  localhost
Address:  127.0.0.1
```

```
Non-authoritative answer:
Name:    www.kisa-ex.or.kr
Address:  169.254.50.86

C:\>
```

O authoritative 네임서버에 대한 반복적 질의

nslookup에서 반복적(iterative) 질의를 하기 위해서는 "norecurse"을 명시적으로 지정하는 것이 필요합니다. 대화형 모드에서는 “set norecurse” 명령을, 명령형 모드에서는 옵션 “-norecurse”를 부가하여 실행합니다.

다음의 dig을 이용한 반복적 질의의 경우를 nslookup을 사용한 반복적 질의를 예시합니다.

```
$ dig @ns0.kisa-ex.or.kr www.kisa-ex.or.kr +norecurse
```

반복적 질의를 할 대상 네임서버를 “server ns0.kisa-ex.or.kr”를 사용하여 지정하고, 반복적 질의 옵션은 “set norecurse”를 사용하여 지정합니다. 그 이후에 질의대상 도메인 네임을 입력하여 질의합니다.

```
C:\>nslookup
Default Server:  localhost
Address:  127.0.0.1

> server ns0.kisa-ex.or.kr
Default Server:  ns0.kisa-ex.or.kr
Address:  169.254.1.53

> set norecurse
> www.kisa-ex.or.kr
Server:  ns0.kisa-ex.or.kr
Address:  169.254.1.53

Name:    www.kisa-ex.or.kr
Address:  169.254.50.86

> exit
```

O IPv4 주소가 아닌 다른 타입 질의

nslookup을 사용하여 IPv4 주소가 아닌 다른 타입의 질의를 수행하려는 경우, "set type=XX" 설정을 통해 원하는 질의타입을 지정합니다.

다음은 도메인의 전자메일 수신 메일서버 정보를 얻기 위해 MX 타입 질의를 하는 경우를 예시합니다. 이 경우, 질의타입을 "set type=MX"를 사용하여 지정한 후 질의합니다.

```
C:\>nslookup
Default Server:  localhost
Address:  127.0.0.1

> set type=MX
> kisa-ex.or.kr
Server:  localhost
Address:  127.0.0.1

Non-authoritative answer:
kisa-ex.or.kr           MX  preference  =  0,  mail  exchanger  =
mailgw.kisa-ex.or.kr

kisa-ex.or.kr     nameserver = ns2.kisa-ex.or.kr
kisa-ex.or.kr     nameserver = ns0.kisa-ex.or.kr
kisa-ex.or.kr     nameserver = ns1.kisa-ex.or.kr
mailgw.kisa-ex.or.kr      internet address = 169.254.50.169
ns0.kisa-ex.or.kr  internet address = 169.254.1.53
ns0.kisa-ex.or.kr             AAAA       IPv6       address       =
2001:dc5:0:10:169:254:50:52
ns1.kisa-ex.or.kr  internet address = 169.254.50.51
ns2.kisa-ex.or.kr  internet address = 169.254.100.53
> exit
```

O DNS 응답 메시지의 상세 내용 출력

자세한 DNS 응답 메시지를 보기를 원하는 경우, 옵션 “debug”를 다음과 같이 “set debug”로 설정하여 DNS 메시지 내용을 확인할 수 있습니다.

```
C:\>nslookup
Default Server:  localhost
Address:  127.0.0.1

> server ns0.kisa-ex.or.kr
Default Server:  ns0.kisa-ex.or.kr
Address:  169.254.1.53

> set norecurse
> set debug
> www.kisa-ex.or.kr
Server:  ns0.kisa-ex.or.kr
Address:  169.254.1.53

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, auth. answer
        questions = 1,   answers = 1,   authority records = 3,
additional = 4

    QUESTIONS:
        www.kisa-ex.or.kr, type = A, class = IN
    ANSWERS:
    ->  www.kisa-ex.or.kr
        internet address = 169.254.50.86
        ttl = 300 (5 mins)
    AUTHORITY RECORDS:
    ->  kisa-ex.or.kr
        nameserver = ns0.kisa-ex.or.kr
        ttl = 300 (5 mins)
    ->  kisa-ex.or.kr
        nameserver = ns1.kisa-ex.or.kr
        ttl = 300 (5 mins)
```

```
   ->  kisa-ex.or.kr
       nameserver = ns2.kisa-ex.or.kr
       ttl = 300 (5 mins)
   ADDITIONAL RECORDS:
   ->  ns0.kisa-ex.or.kr
       internet address = 169.254.1.53
       ttl = 300 (5 mins)
   ->  ns0.kisa-ex.or.kr
       AAAA IPv6 address = 2001:dc5:0:10:169:254:50:52
       ttl = 300 (5 mins)
   ->  ns1.kisa-ex.or.kr
       internet address = 169.254.50.51
       ttl = 300 (5 mins)
   ->  ns2.kisa-ex.or.kr
       internet address = 169.254.100.53
       ttl = 300 (5 mins)

------------
Name:    www.kisa-ex.or.kr
Address:  169.254.50.86

> exit
```

보다 상세한 정보가 필요한 경우, “set d2”를 사용하여 지정하면, 질의 및 응답 메시지 모두를 출력합니다.

“debug” 또는 “d2” 옵션 지정을 해제하려는 경우, 각각 “set nodebug”와 “set nod2”을 사용하여 설정 해제합니다.

6. DNS 설정 주요 문제점 사례 및 개선 방법

가. 위임된 네임서버 일부가 무응답 경우

□ 문제점 요약

도메인의 위임된 네임서버로 질의했을 때, 이 중 일부 네임서버가 아무런 응답을 하지 않는 경우

이는 “불완전 위임(lame delegation) 도메인“ 설정오류 경우에 해당

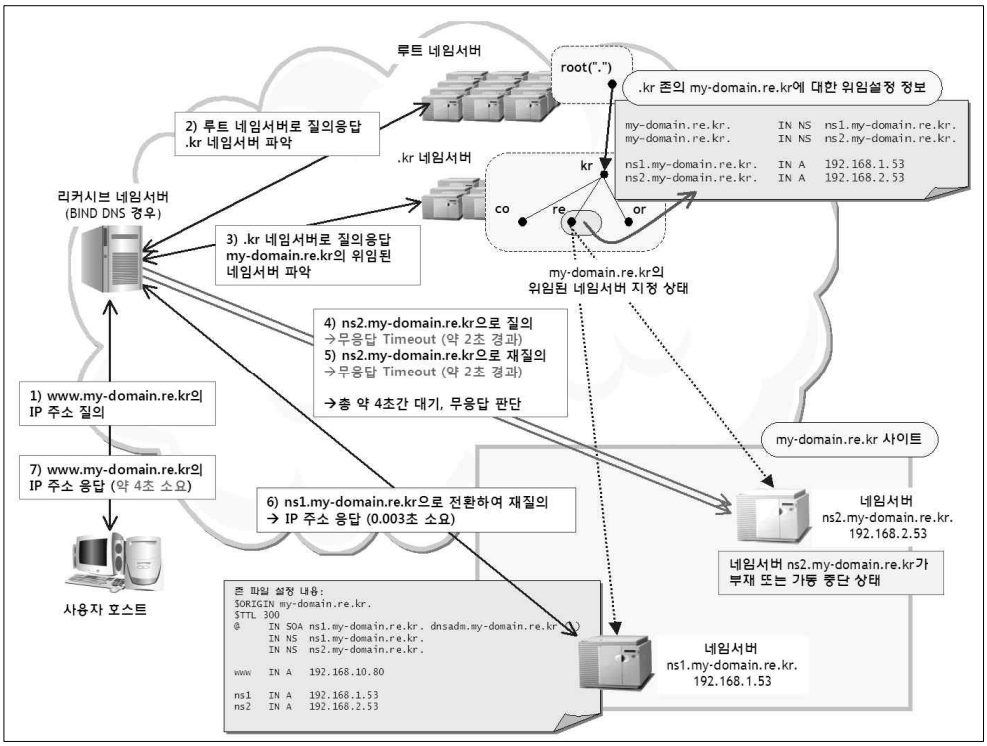
□ 위험도 : 경우에 따라 심각한 위험

1. 도메인네임 무단점유(domain name hijacking) 피해 발생 위험
   - ■ 무응답 네임서버의 도메인 네임이 사용종료 상태인 경우
   - ■ 무응답 네임서버의 도메인 네임을 알지 못하는 제3자가 등록 사용하고 있는 경우
   - ■ 무응답 네임서버의 IP 주소가 알지 못하는 제3자의 사용 IP 주소 대역에 포함되어 있는 경우
2. 서비스 접속 지연

□ 사례 예시 및 분석

도메인의 위임된 네임서버 중 일부가 아무런 응답을 하지 않는 상태인 경우의 사례를 예시합니다. 나머지 네임서버들은 모두 도메인 존 설정이 정상적으로 설정되어 있어 authoritative DNS 응답을 하고 있는 경우에 한정합니다. 도메인 존이 설정되어 있지 않은 경우는 따로 분류하여 예시합니다. 실제 사례를 중심으로 하되, 해당 도메인 정보의 보호를 위해 도메인명과 IP 주소를 임의 변경하여 예시합니다.

첫 번째 사례는, 다음 그림과 같이 자신의 도메인 영역에 네임서버 네임을 정하여 2개의 네임서버로 위임 설정하였으나, 이 중에 하나가 DNS 질의에 응답하지 않는 경우입니다.



호스트의 질의절차 (1)에 의해 리커시브 네임서버는 루트 네임서버로부터 .kr 네임서버까지 질의 절차 (2), (3)을 수행합니다. .kr 네임서버에서 도메인의 네임서버 ns1.my-domain.re.kr과 ns2.my-domain.re.kr을 파악합니다.

리커시브 네임서버는 2개 네임서버 중 ns2.my-domain.re.kr을 임의로 선택하여 www.my-domain.re.kr의 IP 주소에 대한 질의절차 (4)를 수행합니다. 응답을 기다리지만 ns1.my-domain.re.kr은 응답하지 않습니다. BIND DNS 네임서버인 경우, 응답 타임아웃 시간인 2초간 기다린 후 다시 동일한 네임서버인 ns2.my-domain.re.kr 서버로 재질의 절차 (5)를 수행합니다. 이는 서버까지의 네트워크 경로 중간에서 질의 패킷이 순간적으로 소실되어 응답되지 않을 수 있으므로, 재시도해 보는 것입니다. 다시 응답 타임아웃 시간인 2초가 경과하여 응답 실패처리 합니다. 이때까지 약 4초간의 응답대기 시간이 경과합니다. 레커시브 네임서버는 ns2.my-domain.re.kr 네임서버의 응답을 포기하고 다른 네임서버인 ns1.my-domain.re.kr 네임서버로 재질의 절차 (6)을 수행합니다. ns1.my-domain.re.kr 네임서버는 정상 동작하고 있으므로, 0.003 초 정도의 응답시간으로 빠르게 응답합니다. 국내 인터넷에서는 네임

서버가 정상적으로 동작하고 있다면 대부분 약 0.02 초 이내에 응답합니다. 리커시브 네임서버는 응답을 받은 후 사용자 호스트로 응답된 IP 주소로 응답처리 합니다.

이 경우, 가장 두드러진 문제점은 DNS 응답지연 문제입니다. 사용자 호스트는 IP 주소를 응답받기까지 약 4초간을 대기하여야 합니다. 4초 이후에 비로소 웹 사이트 www.my-domain.re.kr의 IP 주소를 파악하여 웹 사이트에 접속하기 시작합니다. 이때 발생한 4초간의 지연은 위임된 네임서버 중 DNS 응답을 하지 않는 네임서버의 응답을 기다리면 소요된 지연 시간으로 인한 것입니다. 만일 네임서버 ns2.my-domain.re.kr 서버가 정상 동작하고 있다면, 이 사용자 호스트는 최대 0.1초 안에 IP 주소를 파악하여 웹 사이트 접속을 시작했을 것입니다.

위 사례는 최악의 경우에 해당합니다. 실제로 사용자 호스트는 주로 둘 이상의 리커시브 네임서버를 DNS 서버로 설정합니다. 리커시브 네임서버는 도메인의 위임된 네임서버들 중 하나를 임의로 선택합니다. Windows OS의 경우 DNS 질의는 설정되어 있는 리커시브 네임서버 모두에 대해 동시에 질의를 시작하도록 구현되어 있습니다. 위 사례와 같이 응답하지 않는 네임서버를 선택한 리커시브 네임서버가 기다리는 동안, 다른 리커시브 네임서버에서는 응답 가능한 네임서버가 우연히 선택되어 빠른 질의응답을 통해 호스트에 응답을 해 줌으로써 호스트는 먼저 도착한 응답을 통해 웹 사이트 IP 주소를 신속하게 파악할 수 있습니다. 그렇지만, 두 개의 리커시브 네임서버 모두 응답하지 않는 네임서버를 선택한 경우가 발생하면 위 사례와 같이 4초 이상의 시간지연이 발생하게 됩니다.

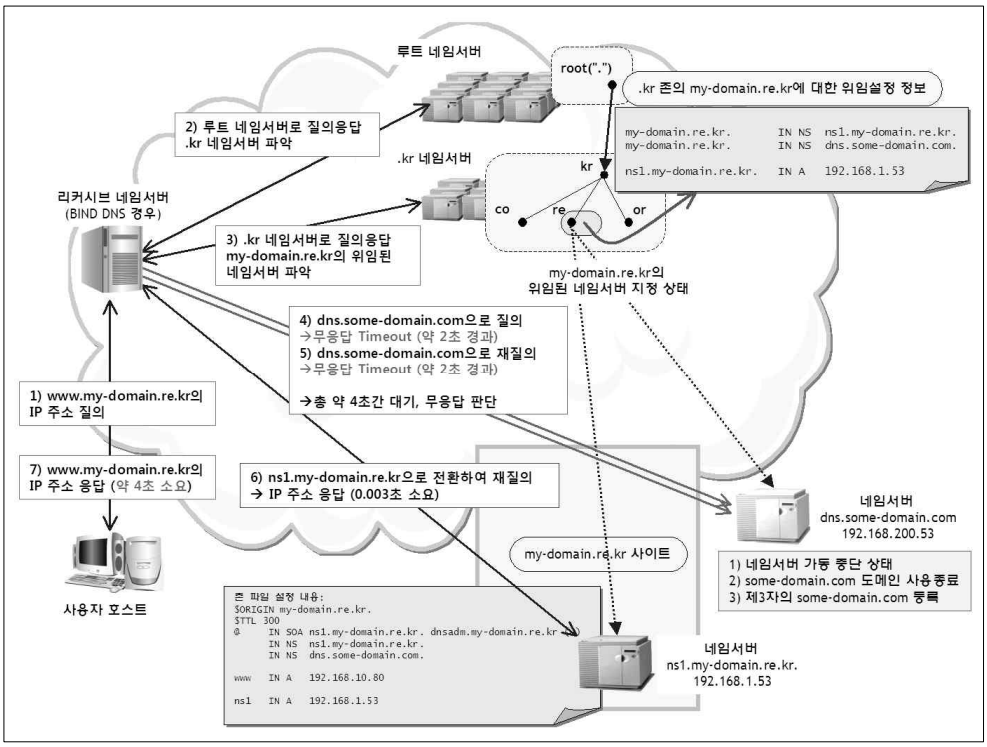
이 경우, 때때로 인터넷 서비스 접속이 잘 안 되는 현상이 발생합니다. 하지만 항상 문제가 있는 것이 아니기 때문에 웹 서버가 순간적으로 과부하 상태이거나 네트워크에 순간적인 문제가 있어서 그렇다고 생각해 버리기 쉽습니다. 이는 DNS 도메인의 설정 문제가 파악되지 않고 그대로 방치되는 결과를 낳습니다. 설정에 문제가 있음에도 리커시브 네임서버의 캐싱 데이터 관리로 인해 응답이 신속하게 이루어질 수 있습니다. 캐싱 데이터에 사용자가 질의하는 도메인 네임의 리소스 레코드 데이터가 있는 경우, 응답은 신속하게 이루어집니다. 이 점은 문제의 발견을 어렵게 하는 역할을 합니다. 인터넷 서비스 접속에 문제가 있음을 신고 받은 관리자가 일반적인 방식

으로 DNS 질의를 수차례 시도해 보았을 때, 첫 번째에는 느리게 응답될 수 있지만 그 이후에는 계속해서 모두 빠르게 응답되므로 DNS 도메인 설정에는 별 문제가 없다는 그릇된 판단을 하게 할 수 있습니다. 이 문제를 정확히 파악하여 검출하기 위해서는 리커시브 네임서버로 질의하는 것이 아니라 도메인의 네임서버 각각에 대해 직접 질의하는 점검이 필요합니다.

정상동작 중인 한 개 네임서버에 장애가 발생하면 도메인 전체가 인터넷으로부터 단절되는 장애가 발생할 위험을 안고 있습니다. 현재 이 도메인은 .kr 존으로부터 2개 네임서버로 위임되어 있으나, 이 중 하나는 무응답 상태로써 무용지물인 네임서버입니다. 현재 이 도메인은 단 하나의 네임서버로만 운영되고 있는 것과 동일합니다. 정상 가동 중인 네임서버에 장애가 발생하면, 이 도메인의 인터넷 서비스는 전면 서비스 중단될 위험을 안고 있습니다.

첫 번째 사례는 2가지 위험을 안고 있습니다. 1) 서비스 접속에 있어서 간헐적인 시간지연 발생, 2) 네임서버 이중화 실패로 인한 서비스 중단 발생 위험성 증가가 그것입니다. 이 사례의 경우, 네임서버 네임과 네임서버 IP 주소는 사이트에서 관리하는 영역에 속하므로, 도메인네임 무단점유(domain name hijacking) 피해 발생 위험성은 크지 않다고 할 수 있습니다.

두 번째 사례는, 다음 그림과 같이 도메인의 위임된 네임서버로 2개 네임서버로 구성하되 하나는 도메인 영역의 네임을 갖는 네임서버로, 다른 하나는 다른 도메인 영역의 도메인 네임을 갖는 네임서버로 구성한 경우입니다. 그리고 이 중 다른 도메인 영역의 네임서버가 응답이 없는 경우의 사례입니다.

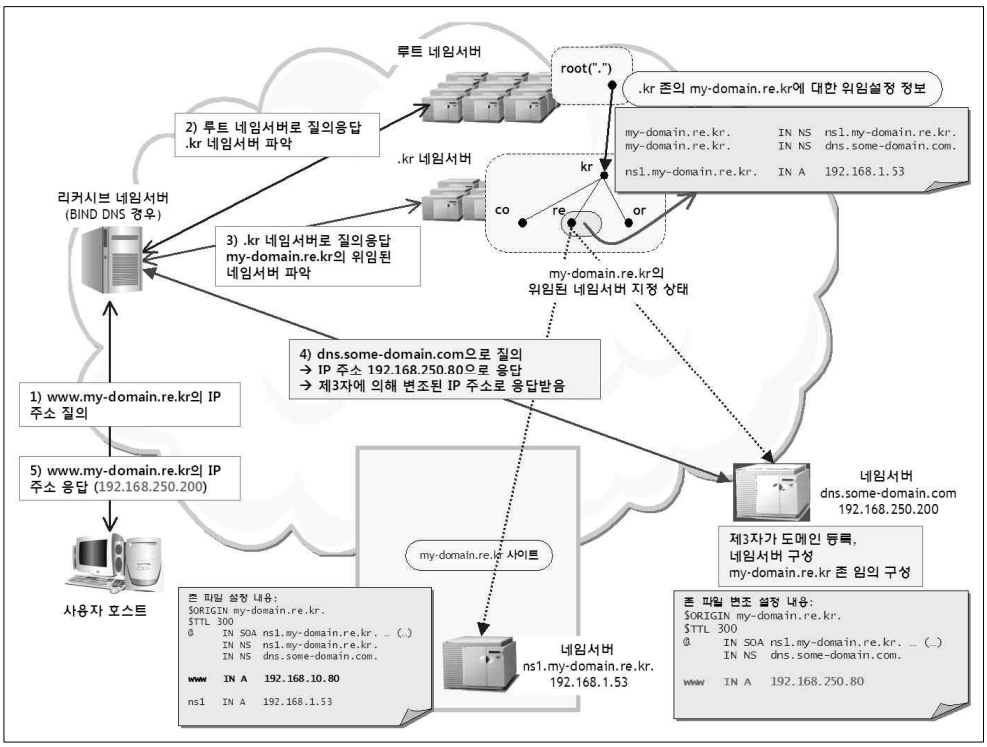


이 경우, 리커시브 네임서버의 질의응답 절차에서 응답시간 지연이 발생하는 현상은 첫 번째 사례와 동일합니다. 이에 대한 설명은 생략합니다.

이 경우에 심각한 위험요소인 "도메인네임 무단점유(domain name hijacking)"로 인한 피해 발생 위험이 있을 수 있습니다. 이 도메인의 네임서버 중 가동이 중단된 네임서버 dns.some-domain.com은 my-domain.re.kr 도메인 등록 사이트가 관할하지 않는 도메인 영역 some-domain.com에 속해 있습니다. 그런데 이 네임서버가 가동 중단 상태가 된 경우에 해당합니다. 심각한 문제가 있는 경우는 도메인 some-domain.com이 사용종료 상태가 되고 제 3자에 의해 도메인 등록이 가능한 상태가 되는 경우입니다. 만일 알 수 없는 제 3자가 some-domain.com을 도메인 등록한 후 my-domain.re.kr의

네임서버 중 하나인 dns.some-domain.com을 생성하고 그 네임서버를 구축한다면 심각한 문제가 발생할 수 있습니다. 이 제 3자가 악의를 가지고 네임서버 dns.some-domain.com에 엉뚱한 데이터를 갖는 my-domain.re.kr 도메인 존 파일을 설정하여 가동하는 경우, my-domain.re.kr 도메인은 인터넷에서 조회될 때, some-domain.com 도메인 소유자가 설정한 데이터로 응답되어 인터넷 서비스 접속이 엉뚱한 사이트로 전환되어 버리는 일이 발생할 수 있습니다. 이는 파밍(pharming)의 피해와 유사한 피해를 유발하게 됩니다. my-domain.re.kr의 웹 사이트를 모방하여 위장한 웹 사이트로 트래픽이 전환 접속되고, 전자메일 수신이 전환되어 버린다면 my-domain.re.kr의 인터넷 서비스 전체는 큰 위험에 직면하게 됩니다.

다음은 제 3자에 의해 변조된 my-domain.re.kr 도메인 존이 위임된 네임서버 중 하나에 설정된 상태를 나타냅니다.



이 상태에서 리커시브 네임서버가 질의절차 (4)를 수행하면서 위임된 네임서버 중 dns.some-domain.com 네임서버를 임의 선택하는 경우가 발생합니다.

제 3자에 의해 dns.some-domain.com 네임서버가 my-domain.re.kr 도메인 존을 갖도록 구축되어 있다면, 질의절차 (4)에서 dns.some-domain.com 서버가 즉시 IP 주소로 응답을 합니다. www.my-domain.re.kr 사이트의 실제 IP 주소는 192.168.10.80이지만 dns.some-domain.com 네임서버는 변조된 주소 192.168.250.80으로 응답합니다. 리커시브 네임서버는 이 응답이 정상적으로 응답된 것으로 판단하고 더 이상의 질의를 수행하지 않습니다. 리커시브 네임서버 입장에서는 dns.some-domain.com 서버가 my-domain.re.kr의 위임된 네임서버이므로 응답된 IP 주소를 캐싱 메모리에 저장 처리합니다. 그리고 호스트에는 dns.some-domain.net 네임서버가 응답한 주소 192.168.250.80으로 응답하고, 호스트의 웹 브라우저는 이 주소로 접속을 바로 개시합니다. 이와 같은 절차는 전자메일의 배달과정에도 동일하게 적용됩니다. 전자메일 배송과정에서 my-domain.re.kr 사이트의 메일서버는 DNS 질의에 의해 파악됩니다. dns.some-domain.com 네임서버의 존 파일에서 임의의 MX 레코드 설정에 의해 전자메일은 전혀 엉뚱한 메일서버로 배송될 수 있습니다.

이와 같은 경우는 도메인 존의 매스터 네임서버를 자신이 관리하는 네임서버로 설정하고, 슬레이브 네임서버는 타 사이트의 네임서버에 설정하여 운영하고 있는 경우에 발생할 수 있습니다. 타 사이트가 사업상의 문제로 네임서버 가동을 중단하고, 도메인 사용을 종료했을 때 my-domain.re.kr의 관리자가 이 사실을 파악하지 못하고 있을 때 이러한 경우가 발생할 수 있습니다. 도메인의 네임서버 모두를 관리하고 있지 않은 경우, 타 도메인에 속한 네임서버가 정상 동작하고 있는지, 그리고 그 도메인이 믿을 수 있는 기관이나 사업자에 의하여 정상적으로 유지되고 있는지 여부를 주기적으로 확인하는 것이 필요합니다.

이 경우의 긴급 조치사항은 도메인의 위임된 네임서버 정보에서 타 도메인을 사용한 네임서버 dns.some-domain.com을 삭제하는 것입니다. 그리고 난 후 별도의 네임서버를 마련하여 도메인의 위임된 네임서버 정보에 추가 등록합니다.

두 번째 사례는 3가지 위험을 안고 있습니다. 1) 도메인네임 무단점유 (domain name hijacking) 피해 발생 위험, 2) 서비스 접속에 있어서 간헐적인 시간지연 발생, 3) 네임서버 이중화 실패로 인한 서비스 중단 발생 위험성 증가가 그것입니다.

나. 위임된 네임서버 일부가 리커시브 네임서버인 경우

□ 문제점 요약

도메인의 위임된 네임서버로 질의했을 때, 이 중 일부 네임서버가 도메인 존이 설정되어 있지 않은 상태인 동시에 리커시브 서비스 제공 상태로 응답 데이터 없이 DNS 응답하고 있는 경우

“불완전 위임(lame delegation) 도메인“ 설정오류 경우에 포함

□ 위험도 : 경우에 따라 심각한 위험

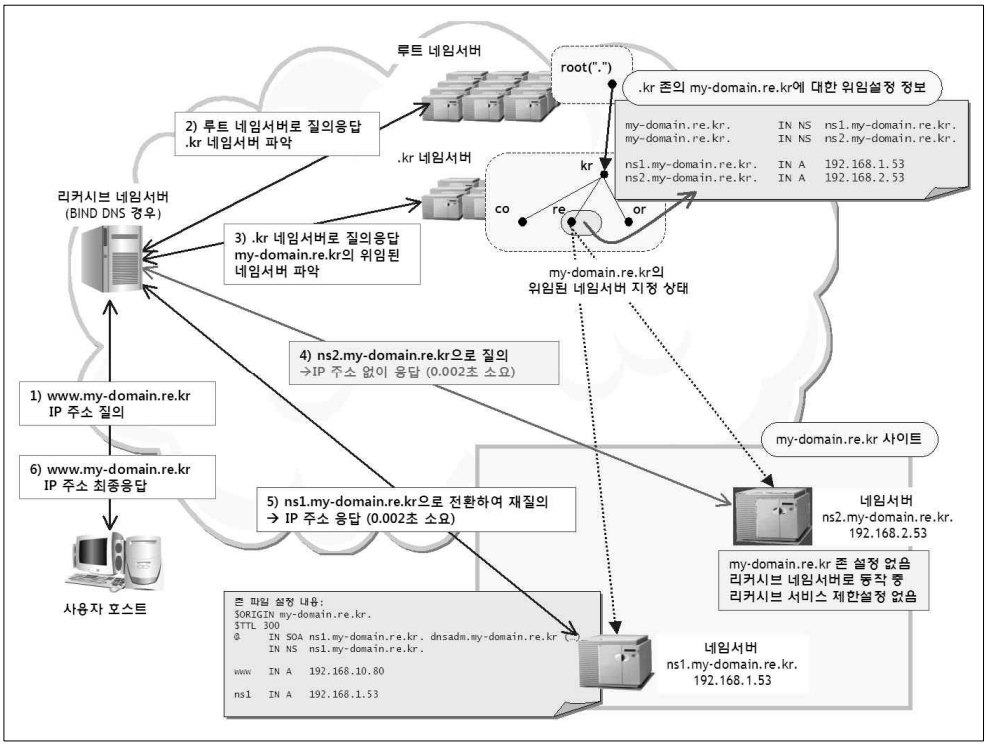
1. DNS 캐시 포이즈닝 공격에 의한 피해 발생의 심각한 위험
   - ■ 위임된 네임서버로 지정된 리커시브 서비스 제공 네임서버가 도메인 존 설정 없이 구성된 경우
   - ■ 동시에 리커시브 서비스 제공대상 제한이 되어 있지 않은 경우
2. 캐싱 네임서버를 동원한 DDoS 공격에 악용될 위험성
   - ■ 네임서버에서 리커시브 서비스 제공대상 제한이 되어 있지 않은 경우
3. 서비스 접속에서 경미한 지연

□ 사례 예시 및 분석

도메인의 위임된 네임서버 중 일부가 응답 데이터 없이 응답하는 경우로 이 네임서버가 리커시브 서비스를 제공하고 있는 경우입니다. 도메인의 나머지 네임서버들은 모두 도메인 존 설정이 정상적으로 설정된 경우입니다. 실제 사례를 중심으로 하되, 해당 도메인 정보의 보호를 위해 도메인명과 IP 주소를 임의 변경하여 예시합니다.

도메인의 네임서버들은 모두 authoritative 네임서버로 구성하는 것을 권장하고 있습니다. 도메인의 authoritative 네임서버는 도메인 존 설정에 의해 존 데이터를 보유하고 있으며, DNS 질의에 대해 자신이 보유하고 있는 도메인 존 데이터를 사용하여 응답하는 네임서버를 의미합니다. 도메인의 네임서버는 가급적 순수한 authoritative 네임서버로 구성하는 것을 권고하고 있습니다. 곧, 동일한 네임서버가 authoritative 네임서버와 리커시브 네임서버 역할을 겸하지 않도록 설정하는 것을 권장합니다. 이는 다음의 예시에서와 같이 자칫하면 심각한 위험상황에 처할 수 있기 때문입니다.

예시 사례는 다음 그림과 같이 2개의 네임서버로 도메인의 위임 네임서버 설정을 하였으나, 이 중 하나의 네임서버에 도메인 존 설정이 되어 있지 않고, 이 네임서버가 리커시브 서비스 제공 상태에 있는 경우입니다. 리커시브 네임서버로 동작하더라도, 리커시브 서비스 제공대상 제한 설정을 한 경우에는 이에 해당하지 않습니다.



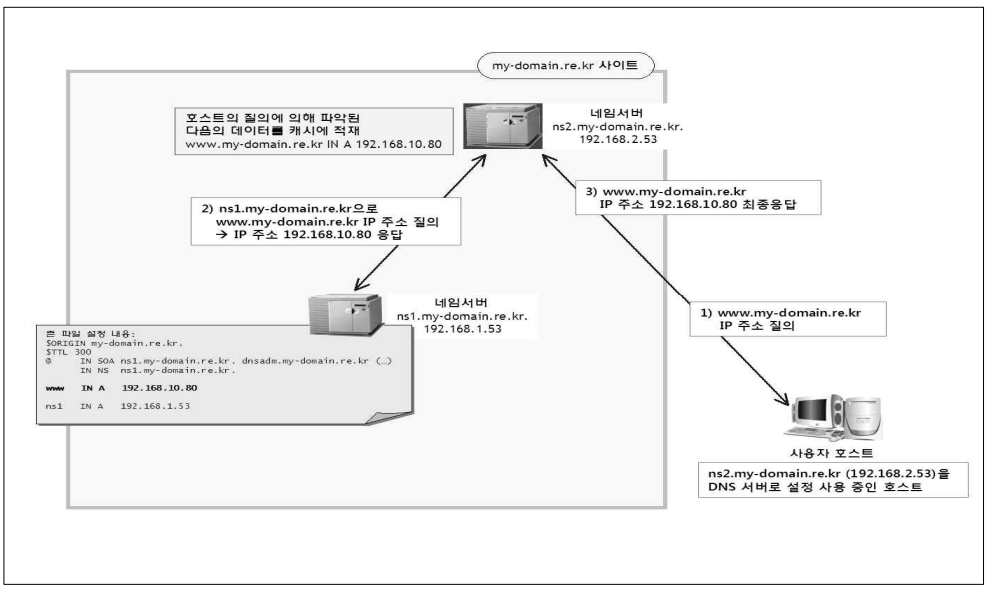
호스트의 질의절차 (1)에 의해 리커시브 네임서버는 루트 네임서버로부터 .kr 네임서버까지 질의 절차 (2), (3)을 수행합니다. .kr 네임서버에서 도메인의 네임서버 ns1.my-domain.re.kr과 ns2.my-domain.re.kr을 파악합니다.

리커시브 네임서버는 2개 네임서버 중 ns2.my-domain.re.kr을 임의로 선택하여 www.my-domain.re.kr의 IP 주소에 대한 질의절차 (4)를 수행합니다. 이 때 네임서버 ns2.my-domain.re.kr는 정상 동작하고 있지만, 도메인 존이 설정되어 있지 않은 상태입니다. 그리고 ns2.my-domain.re.kr 네임서버는 리커시브 네임서버로 동작하고 있습니다. 질의절차 (4)에서 ns2.my-domain.re.kr 네임서버는 도메인 존 데이터를 보유하고 있지 않으므로 IP 주소 응답 데이

터 없이 바로 DNS 응답 처리를 합니다. 이 사례에서는 응답에 0.002초가 소요되었습니다. 비록 응답 데이터가 없는 응답이지만 신속한 응답을 받은 사용자 호스트 측의 리커시브 네임서버는 바로 질의절차 (5)를 수행합니다. 또 다른 위임된 네임서버 ns1.my-domain.re.kr에 대하여 동일한 질의를 다시 시도합니다. 네임서버 ns1.my-domain.re.kr는 도메인 존을 보유하고 있으므로 존 데이터를 사용하여 즉각 응답합니다. 사용자 호스트 측의 리커시브 네임서버는 응답을 받은 후 사용자 호스트로 응답된 IP 주소로 응답처리 합니다.

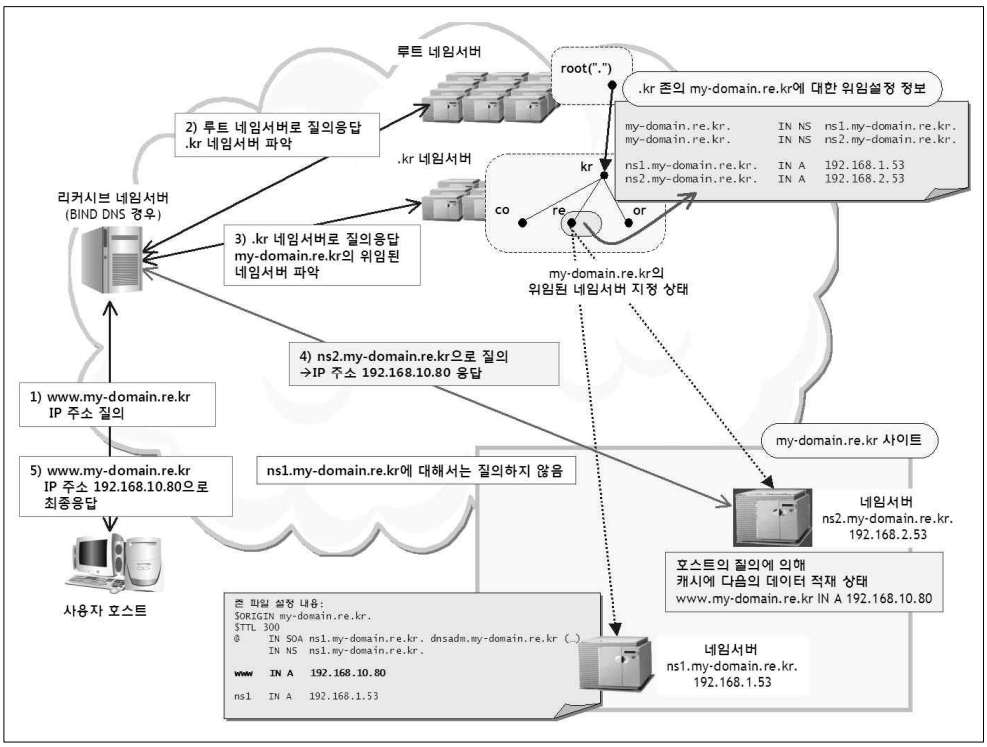
예시한 절차는 최악의 경우에 해당합니다. 리커시브 네임서버가 도메인의 위임된 네임서버들 중 도메인 존 설정이 되지 않은 ns2.my-domain.re.kr 네임서버가 아니라 도메인 존 설정이 된 ns1.my-domain.re.kr 네임서버를 처음에 임의로 선택한 경우에는 ns1.my-domain.re.kr 네임서버로부터 바로 원하는 IP 주소 데이터를 응답받게 됩니다. 질의절차 (4)가 필요 없이 질의응답 절차를 단축하여 완료하게 됩니다. 하지만, 이 사례에서는 네임서버 모두가 동작 상태이기 때문에 응답시간 지연 등의 문제는 발생하지 않고 신속한 최종 응답이 이루어집니다.

리커시브 네임서버인 ns2.my-domain.re.kr 서버는 캐시에 질의대상 데이터가 있을 경우, 바로 IP 주소로 응답하기도 합니다. 다음의 그림과 같이 네임서버 ns2.my-domain.re.kr 캐시에 일시적으로 www.my-domain.re.kr의 IP 주소 데이터가 저장되는 경우입니다.



그림과 같이 리커시브 네임서버 ns2.my-domain.re.kr을 DNS 서버로 설정하고 있는 사용자 호스트가 www.my-domain.re.kr에 대한 IP 주소 질의를 하면 캐시에 그 응답 데이터가 ns2.my-domain.re.kr 네임서버의 캐시에 저장됩니다. 이는 ns2.my-domain.re.kr 네임서버가 도메인 존 데이터를 보유하고 있는 ns1.my-domain.re.kr 네임서버로 질의절차 (2)를 수행하는 과정에서 응답을 통해 파악된 www.my-domain.re.kr의 IP 주소 데이터를 자신의 캐시에 저장처리 합니다. 캐시에 저장된 IP 주소 데이터는 동일한 질의에 대한 응답으로 사용됩니다. 캐시 저장 데이터는 일정한 기간이 경과하면 캐시에서 자동 삭제됩니다.

네임서버 ns2.my-domain.re.kr의 캐시에 www.my-domain.re.kr의 IP 주소 데이터가 있는 경우, 질의절차는 다음의 그림과 같이 진행됩니다.



네임서버 ns2.my-domain.re.kr는 질의절차 (4)에서 자신의 캐시에 질의대상 데이터인 www.my-domain.re.kr의 IP 주소를 발견하고 이 데이터를 응답 데

이터로 응답 처리합니다. 사용자 호스트 측 리커시브 네임서버는 응답된 IP 주소를 사용하여 사용자 호스트로 최종 응답하는 절차 (5)를 수행합니다. 이와 같은 상태에서는 아무런 문제가 없는 것처럼 질의응답 절차가 순조롭게 이루어집니다.

문제는 네임서버 ns2.my-domain.re.kr의 캐시에 my-domain.re.kr 도메인의 전체 데이터가 항상 있는 것이 아니라는 점에 있습니다. 캐시에 질의된 데이터가 있으면 응답 데이터로 응답하지만, 그렇지 않을 경우에는 데이터 없이 응답하게 되고, 이는 또 다른 네임서버에 대한 재 질의를 불가피하게 합니다.

더욱 심각한 문제는 만일 네임서버 ns2.my-domain.re.kr의 캐시에 저장되어 있는 my-domain.re.kr 도메인의 데이터가 위조-변조된 비정상적인 데이터인 경우입니다.

첫 번째 사례의 심각한 위험요소는 1) DNS 캐시 포이즈닝 공격에 의한 피해 발생 위험과 2) DDoS 공격에 동원되어 악용될 위험성이 있습니다.

DNS 캐시 포이즈닝 공격에 의한 피해는 ns2.my-domain.re.kr 네임서버에 대한 공격이 성공하여 캐시 메모리에 위조-변조된 데이터가 저장된 경우에서 발생합니다.

DNS 캐시 포이즈닝 공격은 다음의 조건들이 모두 충족하는 경우 공격이 가능 합니다.

- 인터넷 전체에 대하여 제한 없이 리커시브 서비스 제공 설정 경우
- 공격대상 도메인 존이 대상 네임서버에 설정되어 있지 않은 경우

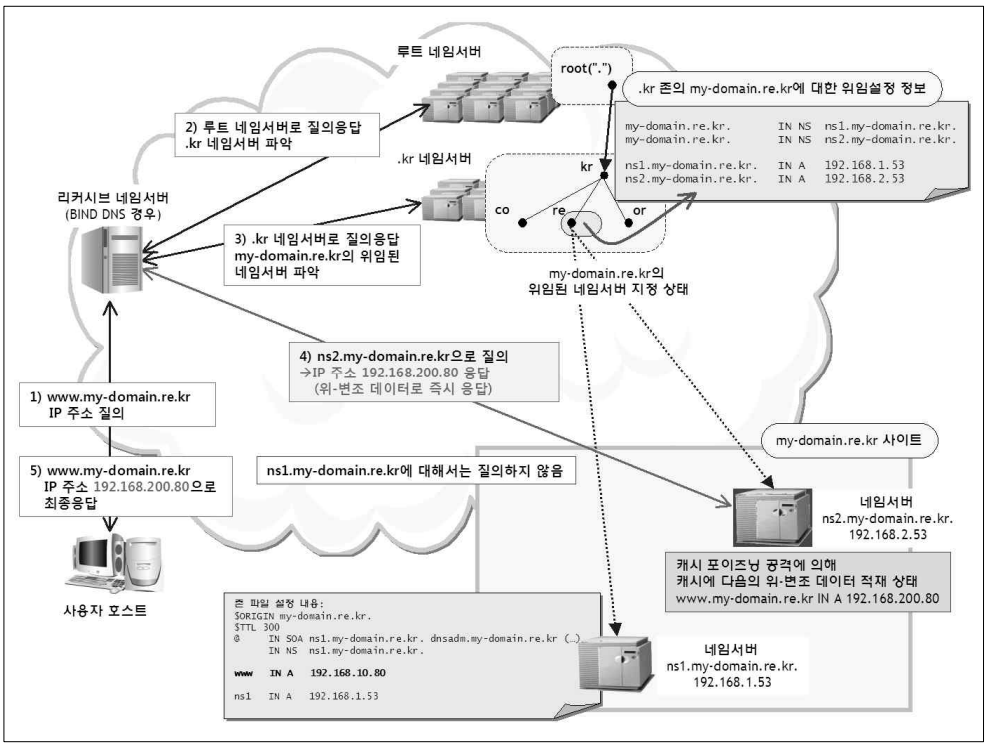
다음의 조건이 만족되면, 공격의 성공 가능성은 증가합니다.

- 오래된 버전의 네임서버 SW를 사용하고 있는 경우

특히, 2008년 8월 이전에 설치된 네임서버 S/W를 패치 또는 업그레이드하지 않고 그대로 사용하고 있는 경우, DNS 캐시 포이즈닝 공격에 취약한 상태에 있습니다. 2008년 카민스키 취약점을 보완하여 배포한 네임서버 S/W 버전이 아니면, DNS 캐시 포이즈닝 공격에 취약한 상태이기 때문입니다. 국내에서

주로 사용하고 있는 BIND DNS와 Windows 서버의 DNS 모두 취약점을 가지고 있었고, 이를 보완한 패치 버전이 배포된 바 있습니다.

위의 예시 사례에 대하여 DNS 캐시 포이즈닝 공격의 피해를 입었을 경우를 다음에 예시합니다. 여기에서 네임서버 ns2.my-domain.re.kr가 이미 공격에 의해 캐시에 www.my-domain.re.kr의 IP 주소 데이터가 저장되어 있다고 가정합니다. 웹 사이트의 원래 IP 주소는 192.168.10.80이지만, 캐시에는 192.168.200.80으로 변조된 데이터가 설정되어 있는 상태로 가정합니다.

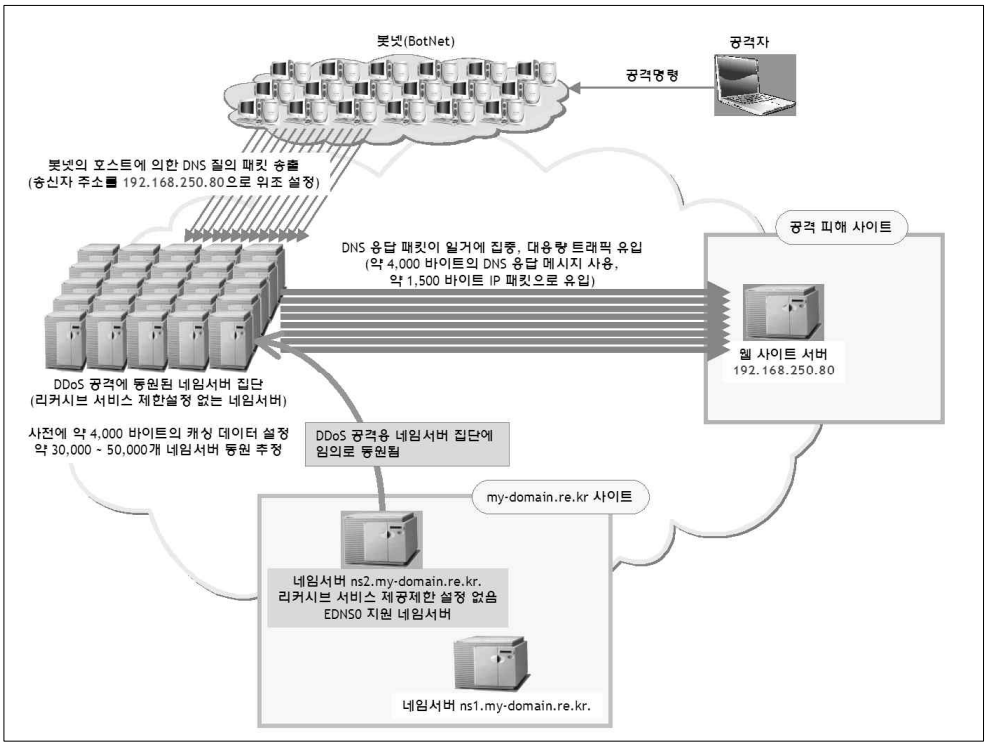


질의절차 (1)부터 (3)까지는 이전과 동일합니다. 질의절차 (4)의 수행과정에서 네임서버 ns2.my-domain.re.kr는 캐시에서 IP 주소 데이터를 검색해 내어 이 데이터로 즉각 응답 처리합니다. 사용자 호스트 측 리커시브 네임서버는 이 응답 데이터를 믿고 사용자 호스트에게 응답처리 합니다. 이 경우, 사용자 호스트는 정상적인 www.my-domain.re.kr 웹 사이트가 아닌 공격자가 의도하는 엉뚱한 웹 사이트에 접속하게 됨으로써 피해를 입을 수 있습니다. 이처럼 DNS 캐시 포이즈닝을 사용하여 개인정보 탈취를 시도하는 경우, 이를 파

밍(pharming) 공격이라 합니다.

또 다른 위험요소로써 네임서버를 악용한 DDoS 공격에 악용될 위험성이 있습니다.

다음 그림은 2006년에 발생했던 DNS 네임서버를 악용한 DDoS 공격 사례입니다. 이 공격은 네임서버의 응답 패킷을 이용하여 특정 사이트에 DDoS 공격을 하는 것을 목적으로 합니다. "DNS Reflector Attack"이라 합니다. 캐싱 DNS 네임서버를 트래픽 증폭 반사경처럼 활용한 공격이라는 의미입니다.



공격자는 사전에 공격에 사용할 네임서버들을 인터넷 상에서 조사합니다.

DDoS 공격에 사용 가능한 네임서버는 "리커시브 서비스가 제한설정 없이 인터넷에 허용되어 있는 네임서버"입니다. 곧, 공격자가 해당 네임서버에 대한 DNS 질의를 함으로써 자신이 미리 설정한 4,000 바이트 가량의 레코드를 그 네임서버의 캐시에 저장시켜 둘 수 있는 네임서버가 조사 대상입니다.

공격에 동원할 네임서버들의 IP 주소 리스트를 확보한 후, 공격에 사용할 약 4,000 바이트 크기의 레코드를 각 네임서버의 캐시에 저장되도록 작업합니다. 공격에 사용할 해당 레코드에 대한 DNS 질의를 각 네임서버로 송출함으로써 캐시에 데이터를 저장합니다. 공격자는 봇넷(BotNet)에 소속된 좀비 호스트들에게 공격명령을 내리면, 각 좀비 호스트들은 네임서버들로 송신자 주소가 공격대상 호스트 주소로 위조된 DNS 질의 패킷을 송출합니다.

네임서버들의 입장에서는 DNS 질의를 받았을 때, 캐시에 저장되어 있는 4,000 바이트 크기의 레코드에 대하여 공격대상 호스트가 질의한 것으로 인식합니다. 네임서버는 캐시의 저장된 4,000 바이트의 레코드를 사용하여 공격대상 호스트로 DNS 응답 처리 합니다. 이 응답 메시지는 인터넷 각 곳의 네임서버로부터 공격대상 사이트로 일거에 집중됩니다. 공격의 피해 사이트는 네임서버들의 응답 메시지 트래픽으로 인해 서비스 중단상태에 빠지게 됩니다.

DNS Reflector 공격에 악용될 소지가 있는 네임서버는 리커시브 서비스 제공제한 설정이 되어 있지 않은 네임서버입니다. 리커시브 기능이 없거나 리커시브 기능을 사용하지 않는 네임서버의 경우는 이와 같은 공격에 이용될 수 없습니다.

DNS Reflector 공격에 악용되는 경우, 제3의 공격대상 사이트로 많은 트래픽이 발생하므로 인터넷 서비스에 다소간의 영향을 미칠 수 있습니다.

이와 같은 경우가 발생하는 것을 사전에 방지하기 위해서는 리커시브 서비스 제공대상 호스트를 제한 설정하는 조치가 필요합니다. 도메인의 네임서버인 경우에는, 가급적 네임서버의 리커시브 기능을 비활성화 설정 처리하여 authoritative 전용 네임서버로 운영하는 것을 권고하고 있습니다. 공격자가 네임서버를 악용할 수 있는 것은 공격자가 임의로 이 네임서버에 대해 리커시브 질의(recursive query)를 하여 응답을 수신하고 캐시에 원하는 데이터가 저장되도록 조작하는 것이 가능한 상태이기 때문입니다. 이는 리커시브 서비스 제공대상 호스트를 한정하여 허용된 호스트가 아닌 경우, 리커시브 질의에 대해 서비스를 제공하지 않도록 설정함으로써 방지할 수 있습니다.

다. 위임된 네임서버 일부에 존 설정 누락 경우

□ 문제점 요약

도메인의 위임된 네임서버로 질의했을 때, 이 중 일부 네임서버가 도메인 존이 설정되어 있지 않아 응답 데이터 없이 DNS 응답하는 경우

※ “불완전 위임(lame delegation) 도메인“ 설정오류 경우에 포함

□ 위험도 : 경미한 지연

1. 서비스 접속에서 경미한 지연
   - ■ 도메인 존 설정이 없는 네임서버가 응답 데이터 없이 응답

□ 사례 예시 및 분석

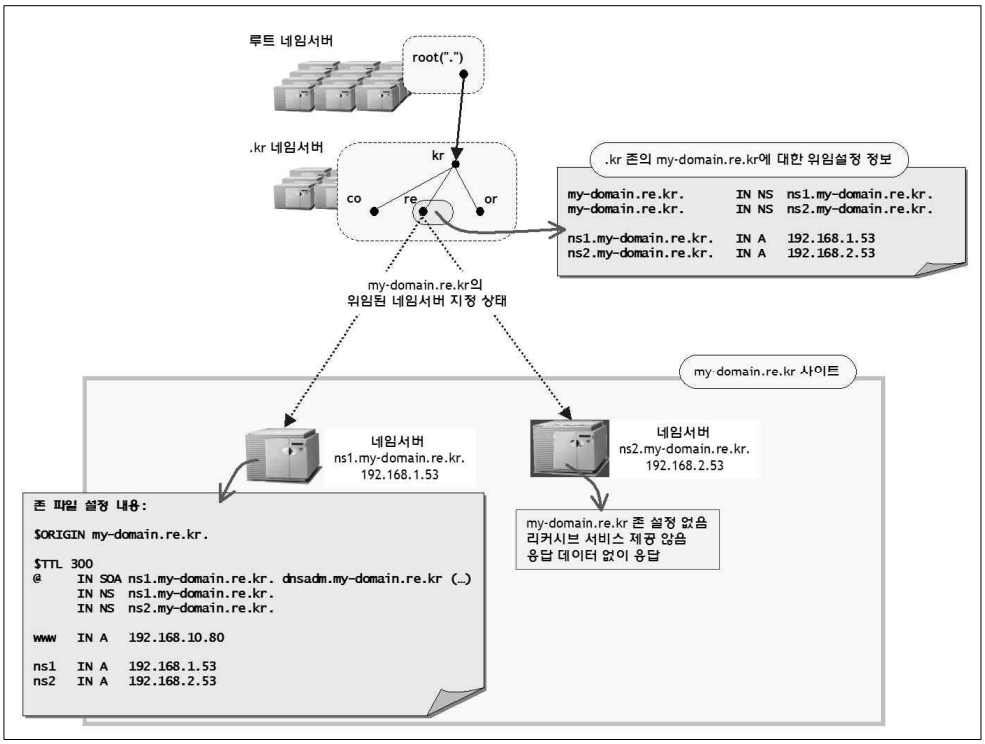
도메인의 위임된 네임서버 중 일부가 DNS 정상 응답은 하되 응답 데이터 없이 응답하는 경우로 이 네임서버가 리커시브 서비스를 제공하지 않는 경우입니다. 도메인의 나머지 네임서버들은 모두 도메인 존 설정이 정상적으로 설정된 경우입니다. 실제 사례를 중심으로 하되, 해당 도메인 정보의 보호를 위해 도메인명과 IP 주소를 임의 변경하여 예시합니다.

다음은 도메인의 위임된 네임서버 중 일부 네임서버에 도메인 존 설정이 되어 있지 않은 경우의 구성 사례입니다.

my-domain.re.kr 도메인은 상위 .kr 도메인에 위임된 네임서버로써 2개의 네임서버 ns1.my-domain.re.kr과 ns2.my-domain.re.kr을 설정하고 있는 상태입니다.

그런데, 실제 네임서버 구성 시 ns1.my-domain.re.kr 네임서버에는 도메인 존 my-domain.re.kr을 설정하였으나, ns2.my-domain.re.kr 네임서버에는 도메인 my-domain.re.kr의 도메인 존 설정을 하지 않은 상태입니다.

이 상태에서 도메인 my-domain.re.kr에 대한 DNS 질의를 하면, 네임서버 ns1.my-domain.re.kr는 정상적으로 응답하지만, 도메인 존 설정이 되어 있지 않은 네임서버 ns2.my-domain.re.kr는 응답 데이터 없이 응답합니다.



이 문제는 관리자의 네임서버 설정상의 착오로 인해 발생할 수도 있습니다. 그러나 대부분은 ns2.my-domain.re.kr 네임서버에 my-domain.re.kr 도메인 존이 원래 설정되어 있었으나, 이후에 네임서버 ns2.my-domain.re.kr에서 도메인 존 설정이 삭제됨으로써 문제가 발생하고 있는 것으로 파악되고 있습니다. 웹 호스팅 서비스를 사용하다가 호스팅 서비스 업체를 변경하는 경우, 웹 호스팅 서비스 업체의 네임서버에서 서비스 계약해지에 따라 도메인 존 설정을 삭제처리 함으로써 이러한 문제가 발생할 수 있습니다.

라. 위임된 네임서버 중 .kr 도메인 존 위임정보 누락으로 인해 DNS 질의를 할 수 없는 경우

□ 문제점 요약

도메인의 .kr 도메인 존 위임정보 누락으로 인해 실제 2대의 네임서버가 정상 운영되고 있지만 실제로 1대의 네임서버로부터 DNS 질의응답을 받을 수 없는 상태

이는 1식의 네임서버 운영으로 인해 발생 할 수 있는 취약점을 가지고 있는 경우에 해당 (3식이상 제외)

□ 위험도 : 경우에 따라 심각한 위험

1. 인터넷 서비스 중단

■ .kr 도메인 존 위임네임서버의 중단으로 인해 실제 도메인 존 질의응답 가능 네임서버가 있지만 DNS 질의응답을 받을 수 없는 상황 발생

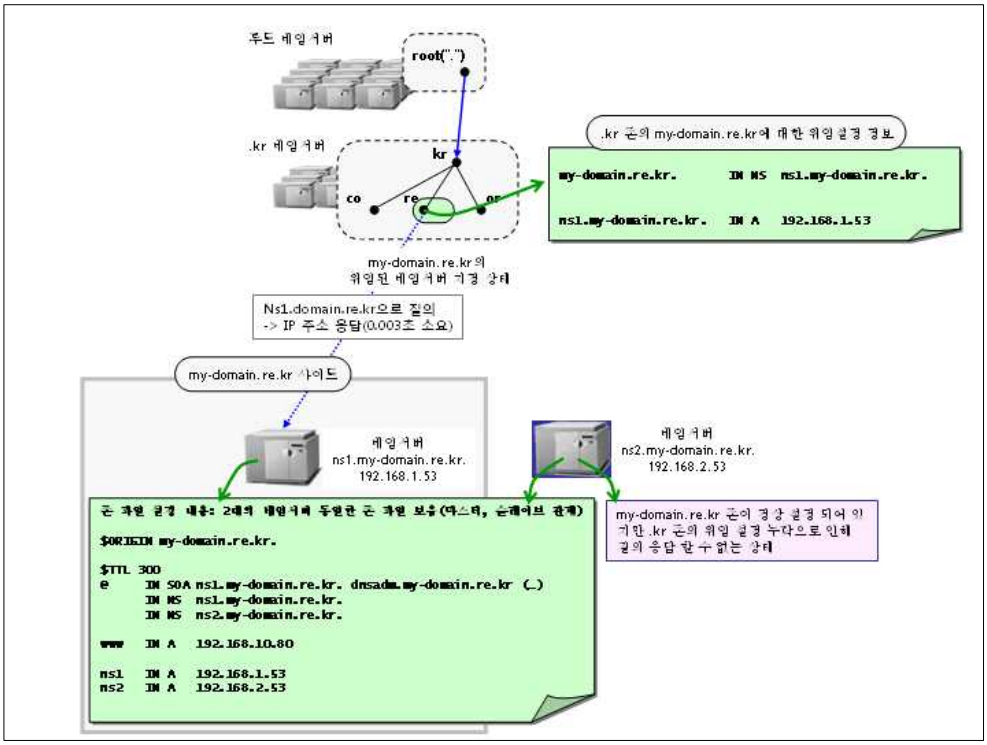
2. 서비스 불안정

■ DNS 질의 분산 불가로 네임서버 트래픽 과다 발생 유발

□ 사례 예시 및 분석

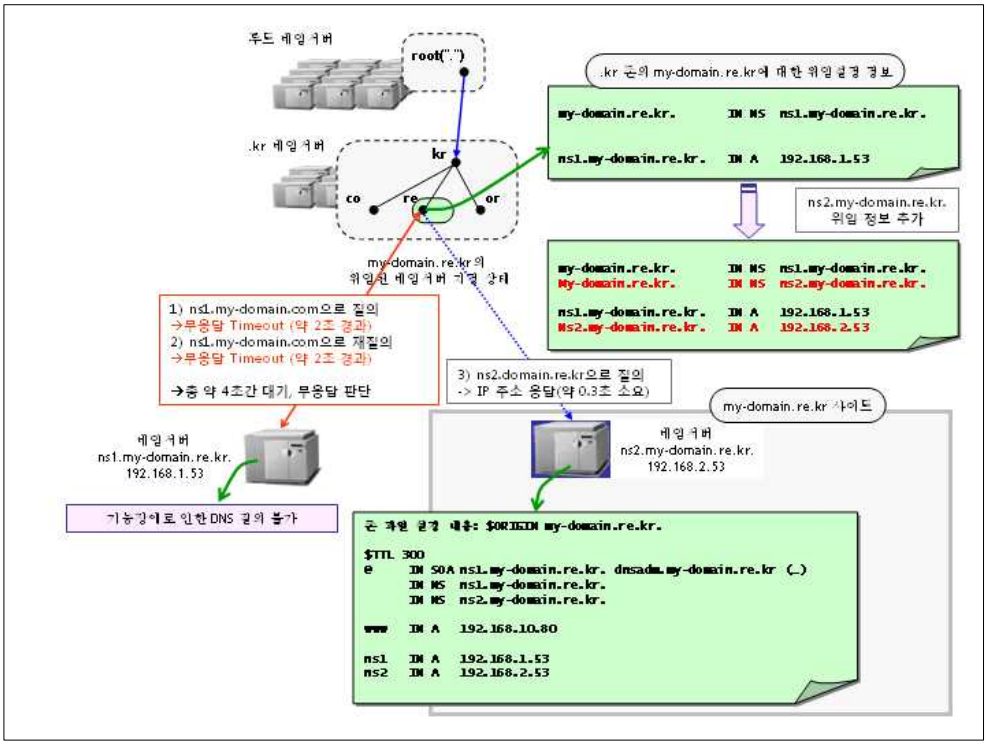
2식의 네임서버가 도메인 존을 보유하고 있고, .kr 도메인 존에는 1식의 네임서버만 등록되어있는 상태입니다. .kr 도메인 존에 등록되어 있는 네임서버가 기능장애로 더 이상 질의응답을 할 수 없는 상태의 사례를 예시합니다.
그리고 .kr 도메인 존에 등록되지 않는 네임서버는 authoritative DNS 응답을 정상적으로 하고 있는 경우에 한정합니다. 실제 사례를 중심으로 하되, 해당 도메인 정보의 보호를 위해 도메인명과 IP 주소를 임의 변경하여 예시합니다.

ns1.domain.re.kr과 ns2.domain.re.kr의 네임서버가 my-domain.re.kr의 도메인 존을 정상 보유한 상태이나, .kr 도메인 존에서 ns2.domain.re.kr의 위임정보를 등록하지 않아 DNS 응답을 하지 못하는 경우입니다. 이럴 경우 ns1.my-domain.re.kr 네임서버만이 my.domain.re.kr의 DNS 응답을 할 수 있습니다.



예시한 절차는 최악의 경우에 해당합니다.

이 경우에 1식의 네임서버 운영으로 인한 인터넷서비스 중단의 우려를 안게 됩니다. 사용자 호스트는 도메인 my-domain.re.kr에 대한 DNS 질의의 응답을 ns1.my-domain.re.kr의 네임서버를 통해서만 응답을 받고 있습니다. ns2.my-domain.re.kr의 네임서버는 KR 도메인 존 위임정보에서 누락되어 my-domain.re.kr의 DNS 질의에 정상 응답이 가능하지만 응답을 하지 못하게 됩니다. ns1.my-domain.re.kr의 네임서버가 기능장애로 더 이상 DNS 응답을 하지 못하는 경우 더 이상 DNS 응답을 받을 네임서버가 없기 때문에 도메인에 관련 된 인터넷 서비스가 모두 중단되는 사태가 발생 합니다.



ns2.my-domain.re.kr의 네임서버에서 my-domain.re.kr의 DNS 응답을 받기 위해서는 누락되어있는 .kr 도메인 존 위임정보에 등록이 필요합니다.
등록이 완료되면 my-domain.re.kr의 대한 질의응답이 가능해 짐으로써 1식의 운영으로 인한 서비스 중단의 우려 및 ns1.my-domain.re.kr의 질의를 분산함으로써 트래픽 과부하 완화 효과를 얻을 수 있습니다. 이런 이유 때문에 2대 이상의 네임서버 구성을 권장 드리고 있습니다.

2대의 도메인 보유 위임네임서버가 정상적으로 KR 도메인 존에 등록이 되었더라면 한 대의 네임서버가 질의응답이 불가능하게 되더라도 (1)~(2)의 질의로 약 4초정도의 시간지연이 발생하지만 (3)2차 네임서버의 재 질의를 통해 도메인에 대한 인터넷 서비스를 중단 없이 받을 수 있게 됩니다.
이 사례의 경우, DNS 보안상의 문제는 없습니다.

마. .kr 도메인 존과 위임된 네임서버 간 위임정보가 불일치한 경우

□ 문제점 요약

도메인 등록 관리자와 네임서버 관리자 간 정보 공유 부족으로 인해 존 보유 네임서버 들의 위임정보와 .kr 도메인 존 위임정보가 불일치한 경우 이는 지연이나 불필요한 추가질의 발생원인 유발

□ 위험도 : 불안정 및 지연의 원인

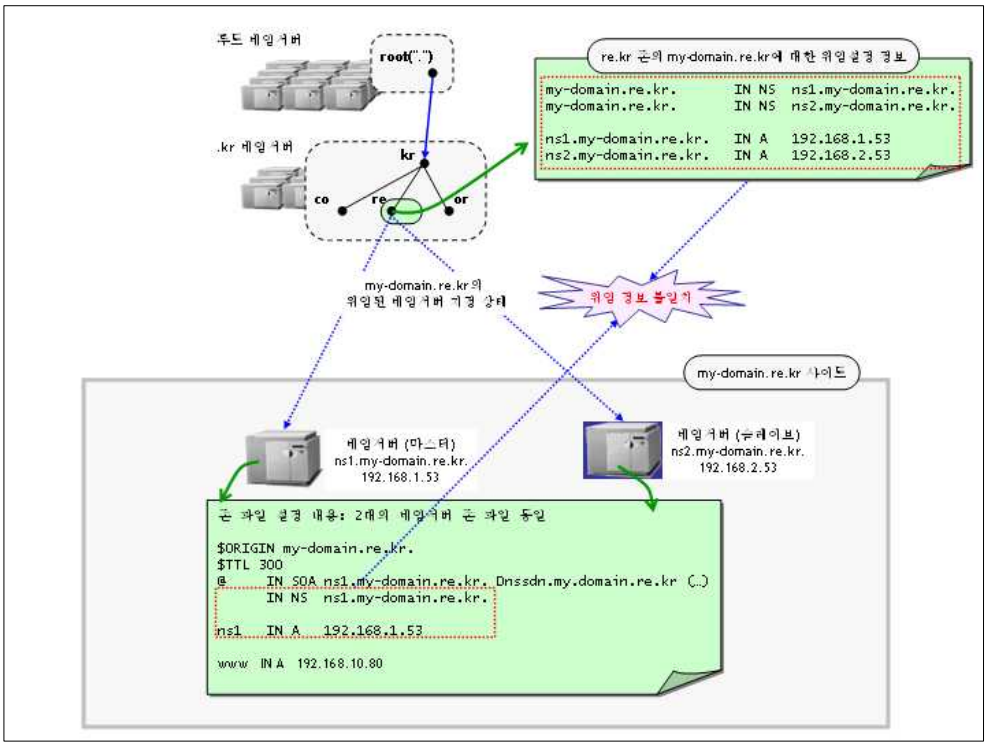
DNS 질의응답 지연

1. KR 도메인 존의 위임정보와 위임된 네임서버 간 위임정보 불일치 하여 혼동 유발
2. 불필요한 추가질의 발생

□ 사례 예시 및 분석

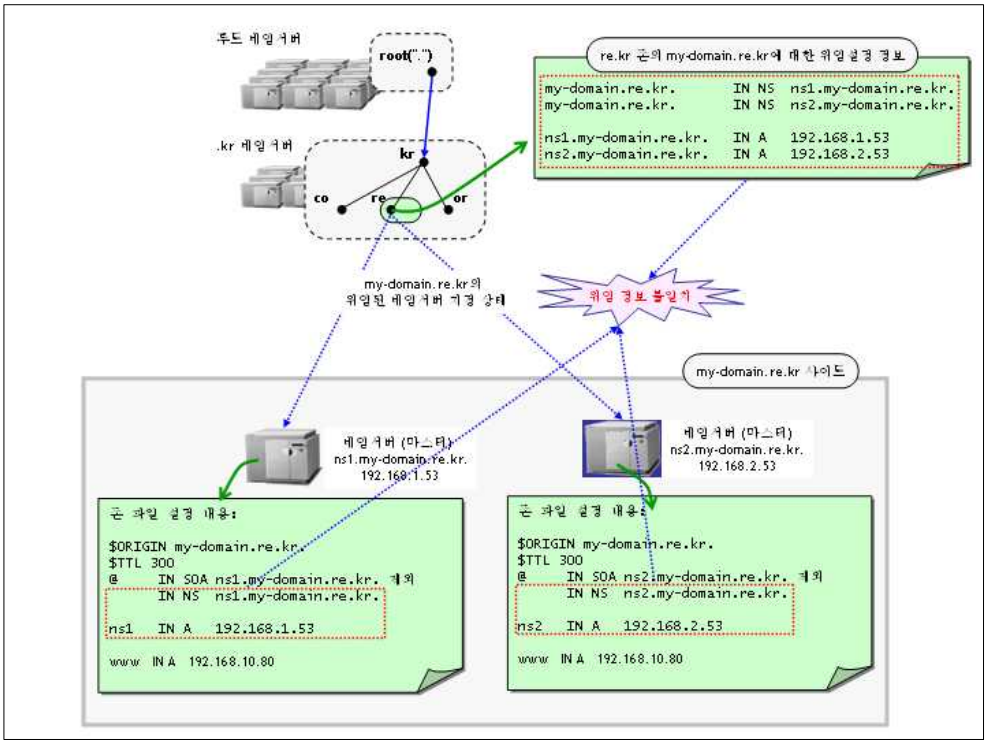
도메인의 위임된 네임서버 들은 모두 DNS 정상 응답을 하고 리커시브 서비스를 제공하지 않는 경우입니다. 하지만 도메인의 위임된 네임서버 들은 모두 .kr 도메인 존의 위임정보와 불일치한 경우입니다. 실제 사례를 중심으로 하되, 해당 도메인 정보의 보호를 위해 도메인명과 IP주소를 임의 변경하여 예시합니다.

사례1, 마스터 네임서버의 존에 자신의 ns1.my-domain.re.kr 위임정보만 가지고 있는 경우, 이를 슬레이브 네임서버가 복재운영 하면서 .kr 도메인 존 위임정보와 불일치하는 경우입니다. 도메인 보유 네임서버들 간 위임정보는 일치하는 경우입니다. 이 같은 경우는 마스터 네임서버 관리자가 도메인의 위임된 네임서버정보를 알지 못하였기 때문에 생기는 문제점입니다.



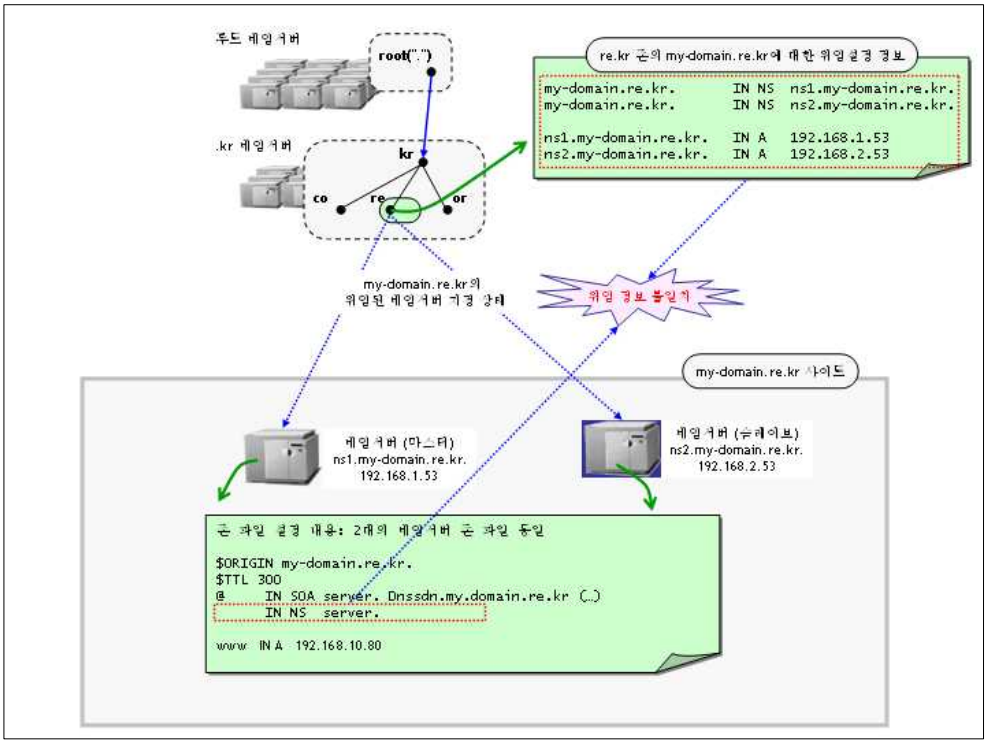
도메인 등록관리자는 도메인의 위임된 네임서버 관리자에게 .kr 도메인 존의 정보를 알려 줄 필요가 있습니다. 마스터 운영의 네임서버에서만 .kr 도메인 존의 위임정보와 동일하게 도메인 존을 수정한다면 슬레이브 운영의 네임서버도 정상적인 존을 복재 운영할 수 있게 됨으로써 모든 위임정보가 일치하게 됩니다.

사례2, .kr 도메인 존의 위임정보와 위임네임서버의 위임정보 뿐만 아니라 위임네임서버들 간의 위임정보도 전혀 일치하지 않는 경우입니다. 이럴 경우 위임네임서버들 간 마스터, 슬레이브 관계가 아닌 경우입니다. 위임네임서버들 간 서로 상대방의 도메인 존 정보 존재를 전혀 알지 못하는 상황일 때 발생합니다. 그렇기 때문에 각각의 네임서버들은 자신의 위임정보만을 보유한 채 운영이 되고 있습니다.



도메인의 네임서버들 중 1대는 매스터 그리고 나머지는 슬레이브 운영을 권장하고 있습니다. .kr 도메인 존의 위임정보와 위임네임서버 간 위임정보가 일치하기 위해서는 2가지의 변경 작업이 필요합니다. 첫 번째로 도메인 등록 관리자는 임의로 슬레이브로 전환할 네임서버를 지정하여 운영 변경 요청을 하여야 합니다. 슬레이브 변경 방법은 '2.1.3 도메인의 매스터/슬레이브 네임서버 구성 설정' 항목 참고하여 구성하면 됩니다. 두 번째로 매스터로 운영되는 네임서버에 .kr과 동일한 위임정보를 등록함으로써 모든 위임정보가 일치하게 됩니다.

사례3, 사례 1번과 같이 위임내임서버들 간의 위임정보는 일치하나 .kr 도메인 존의 위임정보와 불일치한 경우입니다. 다른 점은 위임네임서버의 위임정보에 서버의 호스트명인 'server.'으로 등록이 되어있고, 글루레코드(네임서버 IP주소) 값은 누락되어 있는 경우입니다. 이와 같은 설정은 Windows DNS를 이용할 경우 흔히 발견되는 설정입니다. 도메인 존 구성 시, '새 영역 마법사' 툴을 이용하게 되는데 수동으로 네임서버를 입력하지 않으면 자동으로 서버의 호스트명을 도메인의 네임서버로 등록하게 됩니다.



위임네임서버 간 마스터, 슬레이브 관계이기 때문에 마스터 네임서버의 위임정보만 .kr도메인 존의 위임정보와 일치시켜 주면 됩니다. Windows DNS에서 도메인 존을 구성할 시, 수동으로 위임네임서버 등록을 하여야 합니다. 위임네임서버 수동 등록방법은 p.39 '도메인의 매스터/슬레이브 네임서버 구성 설정' 항목의 Windows DNS 구성 방법을 참고하여 .kr 도메인 존 위임정보와 동일한 정보를 등록하면 됩니다. 이로써 슬레이브 운영의 네임서버도 정상적인 존을 복재 운영할 수 있게 됨으로써 모든 위임정보가 일치하게 됩니다.

위와 같은 상황을 미연에 방지하기 위해서는 도메인 등록관리자와 네임서버 관리자 간 정보전달이 원활히 이루어져야 합니다. 인터넷 서비스에 눈에 띄는 불편함이 없기 때문에 감지하지 못하는 경우가 많습니다. 최적의 DNS 질의응답환경을 구성하기위해서 권장하고 있습니다. 이 사례의 경우, DNS 보안상의 문제는 없습니다.

7. DNS 설정관련 FAQ

1. 리커시브 네임서버의 용도에 대해서 알고 싶습니다.

- DNS 질의응답 트래픽의 절감 및 질의응답 절차의 효율성을 위해 데이터 캐싱 기능을 가지고 있는 네임서버입니다.

2. 도메인의 네임서버를 2대 이상 사용을 권장하는 이유는 무엇인가요?

- 단일 네임서버로 운영하다가 네임서버에 문제가 발생하여 동작이 중단되는 경우 DNS 질의에 더 이상 응답해 줄 수 있는 네임서버가 없기 때문에 도메인을 사용하는 인터넷 서비스 전체가 중단되는 심각한 장애가 발생합니다. E 또, 최근에는 DDoS와 같은 공격에 대한 최소한의 저항력을 가질 수 있도록 하기 위함이기도 합니다. 그리고 2대 이상 구성할 경우, 동일한 서브 네트워크에 있지 않도록 분산 구성과 최소 둘 이상의 ISP 네트워크에 분산 구성할 것을 권장하는데 이유는 동시에 응답이 중단되는 것을 방지하기 위함입니다.

3. 네임서버에 도메인 존이 실제로 존재하는지 점검하는 방법을 알고 싶습니다.

- DIG나 nslookup의 점검 툴은 recursive(재귀적) 타입을 기본으로 질의를 합니다. 그렇기 때문에 리커시브 네임서버의 캐시 영역에 존 데이터가 존재할 경우 대신하여 응답이 되기 때문에 도메인의 네임서버 존 파일 존재 유/무와는 무관하게 응답 데이터가 출력될 수 있습니다. 점검 툴에서 "+norecuse"의 옵션을 사용하여 iteractive 질의로 실제 네임서버의 존 데이터 존재 유/무를 확인 할 수 있고, 존재한다면 플레그 값 “AA"가 출력이 되게 됩니다.
예) $ dig @ns.my-domain.re.kr my-domain.re.kr +norecurse

4. 도메인의 네임서버를 2대 구성하였는데 점검 시, 1대의 네임서버로만 DNS 질의응답이 되고 있습니다. 다른 한 대의 네임서버로 질의응답이 되지 않는 이유를 알고 싶습니다.

- DNS 질의시, 2대의 네임서버로 트래픽분산을 위해 균등하게 질의가 들어

가게 되고 네임서버는 모든 호스트에 대해 DNS 응답이 가능해야 합니다. 먼저 kr 도메인 존에서 내임서버 등록이 되어있는지 확인해야 합니다. 확인은 도메인을 등록한 업체의 웹 사이트에서 도메인 등록정보 메뉴의 네임서버 정보를 통해 가능합니다. 만약에 등록이 되어있다면 다음으로 해당 네임서버에 질의 차단 설정이 되어있는지 확인합니다. named.conf 의 options 영역 안 allow-query 옵션으로 차단설정이 되어 있는지 확인하여 차단 해제 합니다. 그래도 질의가 되지 않을시 방화벽 등을 의심해 바야 합니다.

5. 도메인의 위임이 왜 필요하나요?

- DNS는 분산 데이터베이스 시스템의 일종입니다. 그렇기 때문에 루트 도메인부터 하위의 도메인을 거쳐서 웹 서버를 찾아가는 방식입니다. 그렇기 때문에 상위 도메인 존에서 하위도메인을 찾아갈 수 있도록 하는 위임정보가 필요합니다. 위임정보에는 네임서버의 도메인 명과 네임서버의 IP 주소가 필요 합니다.

6. 도메인의 네임서버는 왜 리커시브 기능이 없거나 제한해야 하나요?

- DNS 캐시 포이즈닝 공격 및 DDoS 공격 등에 악용될 수 있기 때문입니다. 리커시브 기능이 활성화되어있다면 캐시 영역의 도메인 존 데이터의 위조/변조 공격이 가능하게 되고, 리커시브 제한 설정이 되어있지 않은 경우에는 낯선 호스트에 의해 대용량의 존 데이터를 캐시에 저장시켜둘 수 있어 공격대상 네임서버에 피해를 줄 수 있기 때문입니다.

7. 매스터 네임서버와 슬레이브 네임서버의 구성상 차이점은 무엇입니까?

- named.conf 에서의 존 지정 및 존 파일 구성 상 구분이 되겠지만 가장 큰 차이점은 도메인 존을 관리하는 방식의 차이가 가장 큽니다. 매스터는 도메인 존을 생성하고 슬레이브는 매스터의 도메인을 복재(zone-transfer)합니다. 이때 매스터는 named.conf 파일의 해당 도메인 존에 zone-transfer 기능을 슬레이브에 허용해주어야 하며, 슬레이브도 매스터 네임서버를 지정함으로써 AXFR 질의를 통해 존 데이터를 전송 받아오게 됩니다.

8. DNS 질의할 때 통신포트는 무엇을 사용하나요?

- DNS 데이터전송은 UDP/TCP 포트를 통해서 이루어진다. 기본적으로 UDP 포트를 이용하지만 AXFR 질의 등 512K 이상의 대량 데이터를 전송할 경우 TCP 포트로 전송되게 됩니다.

9. 루트 DNS 존 파일은 어디서 구할 수 있나요?

- 루트 DNS의 항상 고정적인 것이 아니기 때문에 주기적으로 업데이트 할 필요가 있습니다. dig을 이용하여 루트 네임서버에 질의하여 데이터를 가져올 수 있다.
예) $ dig @a.root-servers.net . ns >named.root

10. 서브 도메인을 관리하는데 CNAME 레코드를 활용하면 편리하다고 들었는데 어떻게 설정하는 것인지 알고 싶습니다.

- 동일한 IP주소를 사용하는 서브 도메인관리에 효과적입니다. 설정 방법은 하나의 서브 도메인에 대한 A 레코드를 설정하고 나머지 서브 도메인들을 CNAME 레코드로 지정하면 됩니다. 이렇게 설정하게 되면 IP 주소가 변경되더라도 하나의 A 레코드만 변경하게 되면 CNAME으로 설정한 모든 서브 도메인도 적용이 됩니다. 하지만 DNS 설정 안내서에서는 NS, MX 레코드에서 CNAME의 설정 금지를 권고 하고 있습니다. 이유는 CNAME의 설정으로 인해 CNAME에 대한 질의를 한번 더하기 때문에 질의 지연이 되기 때문입니다.

CNAME 사용 예

(기존 레코드 설정)

```
www.my-domain.re.kr.    IN      A       192.168.80.80
ftp.my-domain.re.kr.    IN      A       192.168.80.80
mail.my-domain.re.kr.   IN      A       192.168.80.80
```

(CNAME 설정 후)

```
www.my-domain.re.kr.    IN      A       192.168.80.80
ftp.my-domain.re.kr.    IN      CNAME   www.my-domain.re.kr.
mail.my-domain.re.kr.   IN      CNAME   www.my-domain.re.kr.
```

8. DNS 참고자료

가. 웹 사이트

DNS 배움터

http://dns.kisa.or.kr

한국인터넷진흥원의 DNS 소개 및 관련 자료 제공 포털 사이트

DNS, 한글.kr, DNSSEC 관련 소개, 동향 및 자료실

웹 기반 DNS 점검 등

도메인 배움터

http://domain.kisa.or.kr

한국인터넷진흥원의 도메인 관련 정보 제공 사이트

도메인 소개 및 .kr 도메인 체계, 도메인 등록절차, 관련 자료 제공

ISC : BIND DNS 배포 사이트

http://www.isc.org

BIND DNS 네임서버 개발 및 배포 사이트

BIND DNS 웹 페이지 : http://www.isc.org/software/bind

Bind9.net : BIND DNS 관련 포털 사이트

http://www.bind9.net

BIND DNS 관련 자료 제공 해외 포털 사이트

나. 서적

DNS와 BIND

한빛미디어 출판
"DNS and BIND"의 번역판
개정 4판까지 번역 출간

DNS and BIND

Paul Albitz, Cricket Liu 저
O'Reilly Media 출판
DNS 관련 서적 중 고전이라 할 수 있는 책
DNS 전반에 대한 자세한 소개와 BIND DNS 네임서버 관련 사항 기술
현재 개정 5판까지 출간

DNS on Windows Server 2003

Cricket Liu, Matt Larson, Robbie Allen 저
O'Reilly Media 출판
Windows 2003 서버의 DNS를 위한 "DNS and BIND"의 특별판
이외에 Windows 서버 버전별로 "DNS on Windows NT", "DNS on Windows 2000"이 출간되어 있는 상태
한국어 번역판은 아직 없는 상태

DNS & Bind Cookbook

Cricket Liu 저
O'Reilly Media 출판
네임서버 관리자가 현업에서 당면하게 되는 다양한 문제점에 대한 구체적인 해결방법을 각 문제 항목별로 분류 정리하여 제시하고 있는 책
한국어 번역판은 아직 없는 상태

Pro DNS and BIND

Ron Aitchison 저

Apress 출판

DNS 전반에 대하여 아주 상세하게 설명한 책

DNSSECbis 표준(2005년)에 대한 소상한 소개

한국어 번역판은 아직 없는 상태

POWERED BY DNS

김승영 저

홍릉과학출판사 출판

서적은 절판 상태이며, 현재 인터넷으로 공개 배포

공개 웹 페이지 : http://www.ziom.co.kr/doc/PoweredByDNS

DNS 설정 안내서

2011년 9월 인쇄
2003년 9월 발행

발행처: **한국인터넷진흥원**

서울특별시 송파구 가락동 79-3번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118

인쇄처: 신우디앤피
Tel: (02) 2678-5554

<비매품>

○ 본 안내서·해설서는 한국인터넷 홈페이지(www.kisa.or.kr)자료실에서 내려 받으실 수 있습니다.

한국인터넷진흥원
138-950 서울시 송파구 중대로 109번지 대동빌딩
Tel 02-405-4118 | **Fax** 02-405-5119
www.kisa.or.kr