



DNS Tutorial :

DNS 기초

2020. 8. 21.

(주)엔에스컨설팅
석원진 팀장

DNS 개념

- ❖ DNS란 무엇인가?
- ❖ DNS의 등장배경
- ❖ DNS와 관련, 실무에서 접하는 기본 개념 및 용어
- ❖ DNS의 중요성

DNS란 무엇인가?

■ Domain Name System

- 1983년에 최초 개발되어 현재까지 사용 중
- 최초 개발 시 네트워크상에서 외우기 어렵고 복잡한 IP주소를 호스트이름(Domain Name)에 매핑시키는 방법론

192.168.0.1  my-domain.re.kr

2001:DB8::  your-domain.re.kr

DNS의 등장 배경

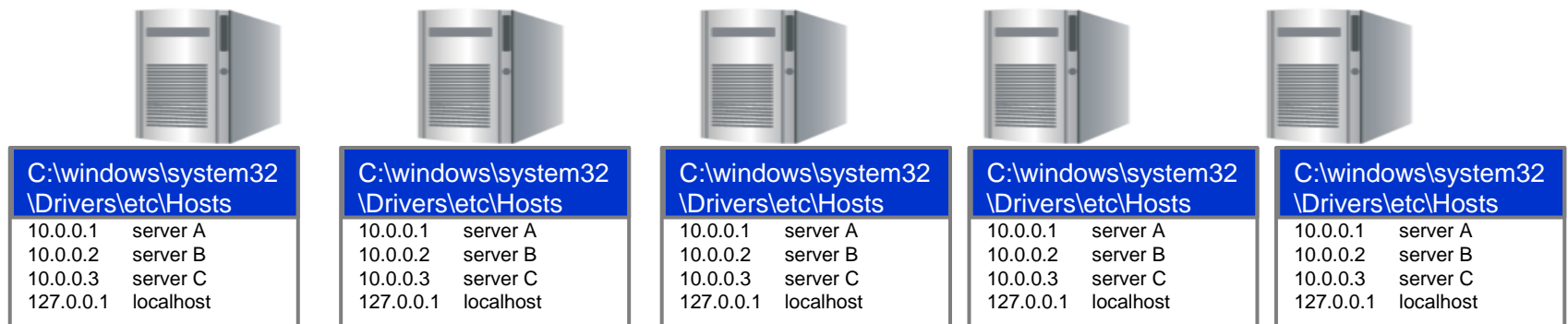
■ 인터넷 초기 환경과 DNS의 등장 배경

■ 1970년대 미국에서 인터넷 태동

- ❖ 1970년대 중반 인터넷 프로토콜로 TCP/IP 도입 적용
- ❖ TCP/IP 기반 인터넷에서의 시스템 접속은 IP 주소 사용

■ 인터넷에 연결된 호스트가 늘어남에 따라 호스트별 IP 주소 기억이 곤란

- ❖ 호스트 네임과 IP 주소를 매핑하는 간단한 테이블 파일(HOSTS.TXT) 사용
- ❖ HOSTS.TXT는 ARPAnet NIC에서 관리, 각 호스트에서 다운로드하여 사용



■ 인터넷 연결 호스트의 증가로, HOSTS.TXT 파일내용 갱신/관리 곤란 문제 발생

- ❖ “도메인 네임” 체계 설계, DNS(Domain Name System) 개발 도입 및 표준화
- ❖ DNS 도입으로 도메인 네임을 사용한 호스트 접속, 웹 서비스 접속 등이 가능하게 됨
- ❖ 특히, 전자메일 송수신을 위한 전자메일 라우팅 체계가 DNS를 기반으로 확립

DNS 관련, 실무에서 접하는 기본 개념 및 용어(1/2)

■ 도메인 네임 공간 및 리소스 레코드

- ❖ 도메인 네임 공간 : 루트 도메인을 정점으로 하는 트리 구조의 네이밍(naming) 구성 체계
- ❖ 리소스 레코드 : 도메인 네임에 매핑되는 각종 인터넷 자원 정보 레코드 데이터 타입 (예: IPv4 주소, 메일수신 메일서버의 도메인 네임 등)

■ 네임서버

- ❖ 도메인 영역(존)의 데이터를 보유하여 질의에 대한 응답을 수행하는 S/W 구현물 (Authoritative 네임서버에 해당)

■ 리졸버

- ❖ 어플리케이션으로부터 요청받은 도메인 네임의 특정 데이터 조회를 루트 도메인 네임서버로부터 순차적으로 수행하는 루틴(routine)

■ 리커시브(캐시) 네임서버와 스템브 리졸버

❖ 리커시브(캐시) 네임서버

- ✓ 네임서버 기능과 리졸버 기능을 조합하여 다수 호스트의 DNS 질의에 대한 조회(resolution)을 대신 수행하는 S/W 구현물

❖ 스템브 리졸버 :

- ✓ 리커시브 네임서버에 의존하는 호스트에 구현된 간략화된 리졸버 루틴(routine)

DNS 관련, 실무에서 접하는 기본 개념 및 용어(2/2)

도메인 네임 공간에서 확보한 도메인 영역에서
도메인 네임 생성
(예: www.my-domain.re.kr)

도메인 네임에 설정할 데이터를
미리 정의된 리소스 레코드 타입 사용. 설정
(예: IPv4 주소 A 타입 레코드 설정, A 192.168.1.80)

도메인 네임
(Domain Name)

리소스 레코드
(Resource Record)

도메인 네임별 레코드 데이터를
존 파일 포맷으로 표현,
네임서버 DB에 존 데이터 적용

존 파일 (Zone File)

네임서버 (Name Server)

도메인 존 데이터

DNS 질의응답
UDP/TCP 53 포트

호스트 (Host)

어플리케이션

함수
(Socket API)

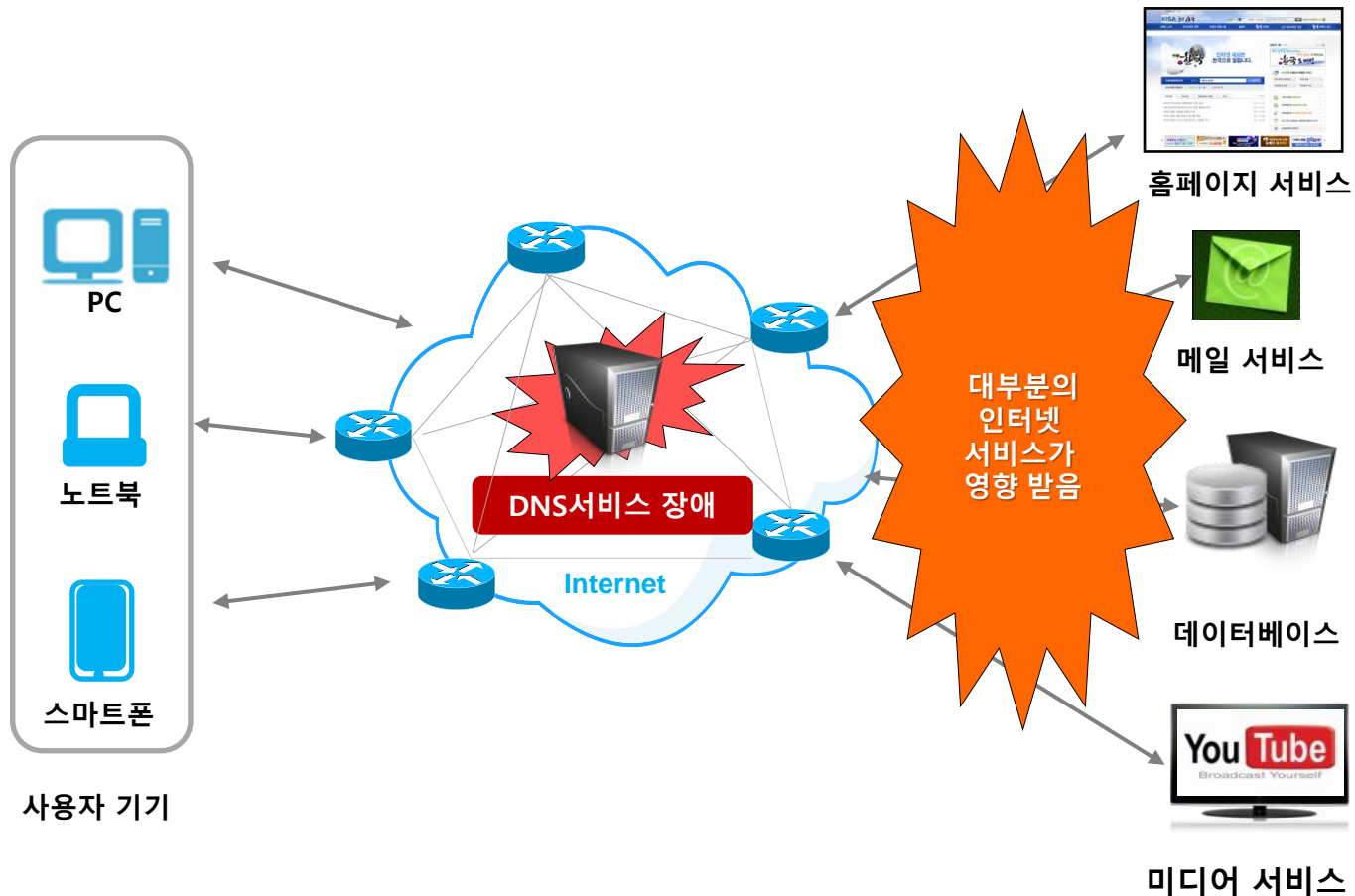
리졸버 (Resolver)

캐시 데이터

DNS의 중요성

■ 장애 발생 시 대부분의 인터넷 서비스가 영향을 받음

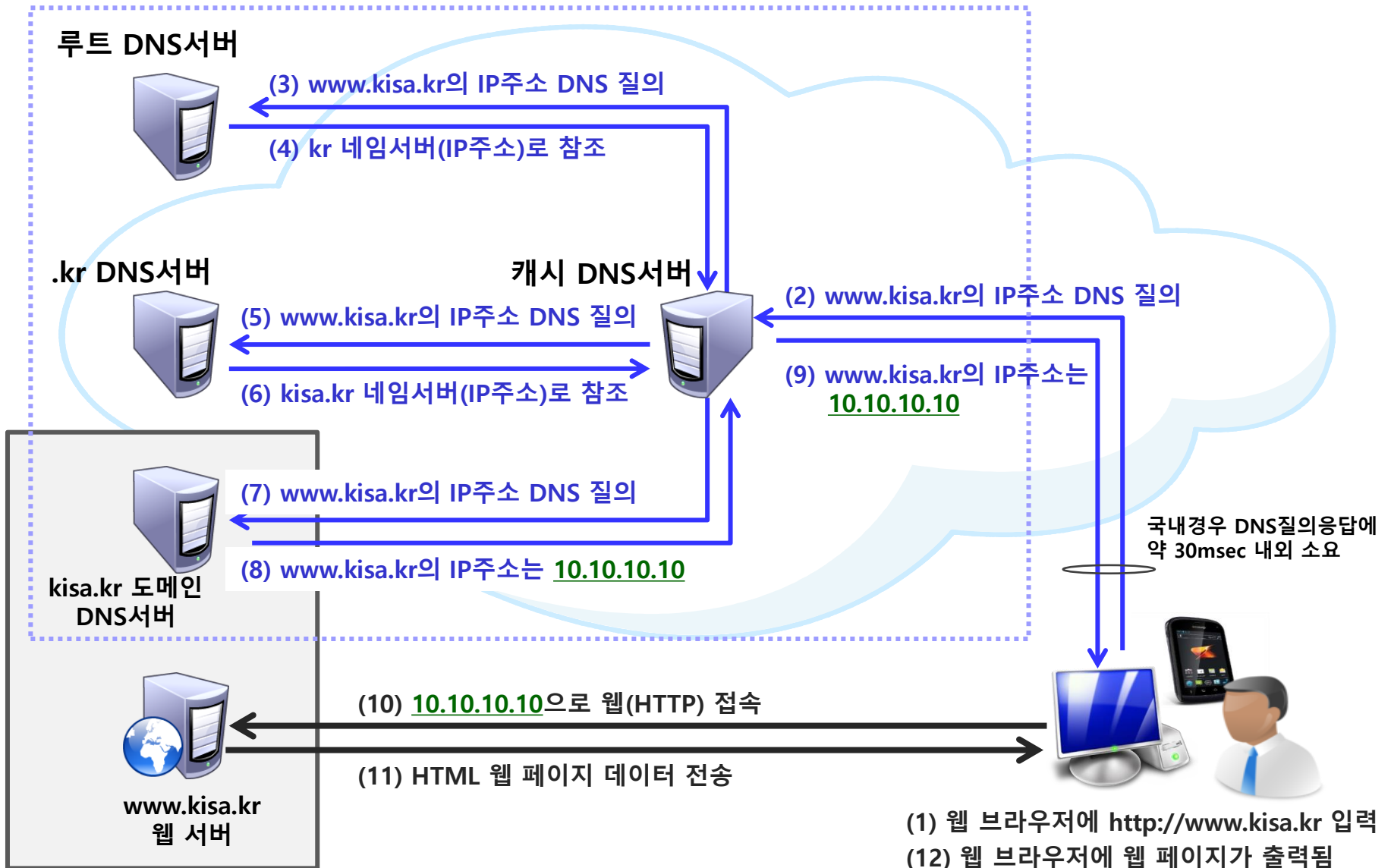
- ❖ 우리가 일상생활에서 자주 사용하는 서비스 대부분은 접속 시 DNS 기술을 기반으로 함
 - Ex) 네○○, 인○○그램, ○튜브, ○마켓, 카○○톡
- ❖ 장애가 아닌 설정오류도 이용자의 서비스 접속 시 시간지연의 영향을 줄 수 있음



DNS 작동원리

- ❖ 인터넷 서비스 이용에서 DNS는 어떻게 동작하는가?
- ❖ DNS 특징
- ❖ 분산 구조와 도메인 네임 체계
- ❖ DNS 레코드

인터넷 서비스 이용에서 DNS는 어떻게 동작하는가?



DNS 특징

■ 분산구조형 데이터베이스

- ❖ 데이터베이스 시스템(DNS 네임서버)의 분산 구성
- ❖ 데이터의 영역별 구분(Domain Zone) 및 분산관리
- ❖ 도메인의 네임서버 및 도메인 데이터는 해당 관리주체에 의해 독립적으로 관리됨
 - HOSTS.TXT는 중앙의 NIC에서 일괄 관리. → 호스트 증가에 따라 갱신 관리 문제 발생
 - DNS는 각 기관에서 자신의 도메인 데이터 관리, NIC은 도메인의 할당 위임만 관리

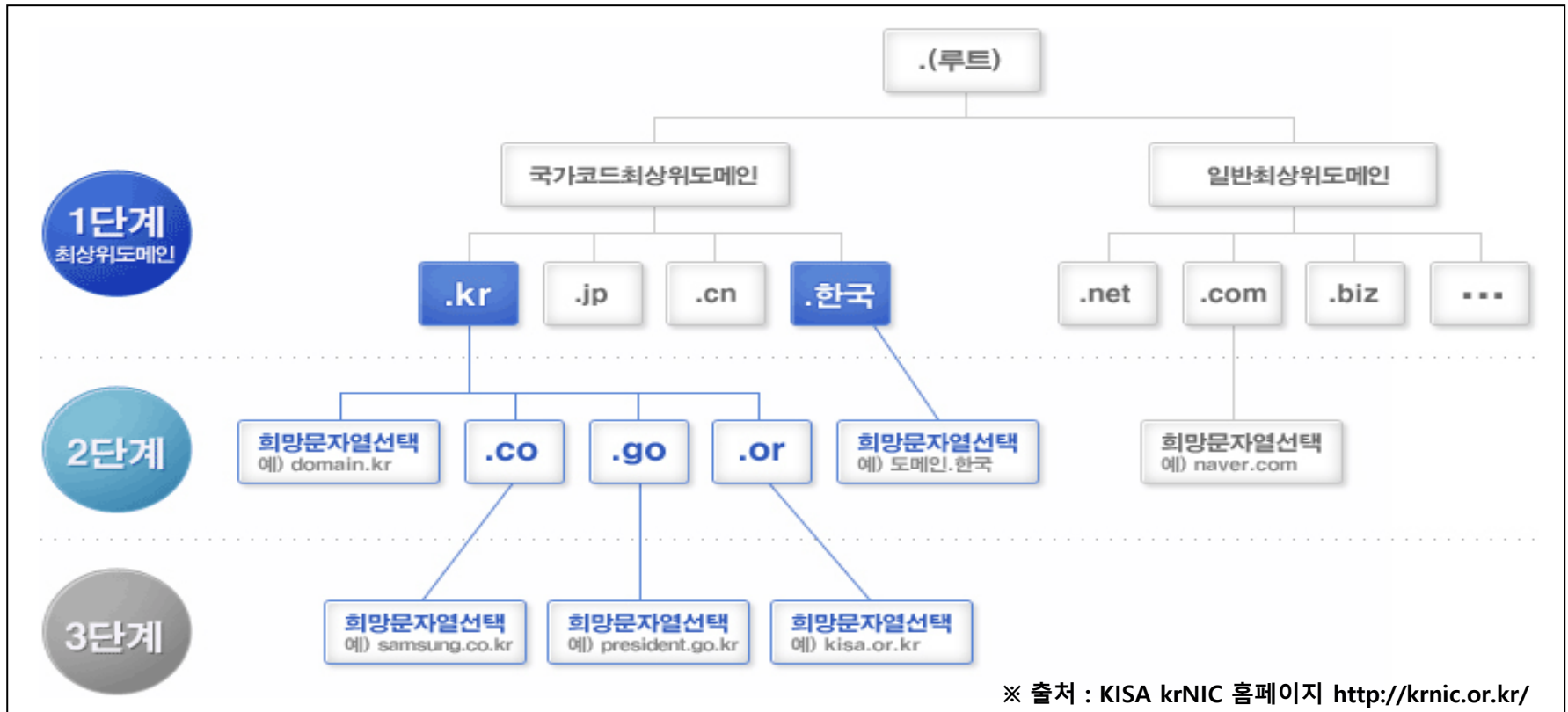
■ 트리(Tree) 구조의 도메인 네임(Domain Name) 체계

- ❖ Domain Name Space: 영역, 영토를 의미
- ❖ 도메인 네임의 자율적 생성
- ❖ 생성된 도메인 네임은 언제나 유일(Unique)하도록 네임 체계 구성

■ DNS 레코드를 이용한 다양한 정보 제공

- ❖ IP 주소만이 아니라, 다양한 데이터의 설정 가능
- ❖ 전자메일 라우팅 정보, RFID 정보 등 다양한 정보 설정 가능한 데이터베이스
- ❖ 도메인 네임에 설정하는 데이터 유형은 리소스 레코드(Resource Record)로 정의

분산 구조와 도메인 네임(Domain Name) 체계



■ Ex) 도메인 kisa.or.kr.에 담겨있는 도메인 네임 트리 상의 위임정보

- ❖ 도메인 kisa.or.kr.은 or.kr.으로부터 위임되었으며,
- ❖ or.kr.은 다시 kr.으로부터 위임되었고,
- ❖ kr.은 루트(.)로부터 위임되었음

DNS 레코드

■ DNS 레코드 (DNS 리소스 레코드 resource record)

- DNS에서 응답하는 정보의 종류를 정의
- 웹 서버 www.kisa.kr의 IPv4주소는 어떻게 저장하고 질의하는가?
 - ❖ DNS 레코드 타입 중 IPv4 주소 데이터를 저장하는 A 레코드를 사용
 - ❖ IPv4주소 질의할 때, "www.kisa.kr.의 A 레코드는?"와 같은 방식으로 질의

■ 주로 사용하는 DNS 레코드 타입 개요

- ❖ A 레코드(A RR) - ex) www.kisa.kr. A 202.30.50.88 (IPv4 주소)
- ❖ AAAA 레코드(AAAA RR) - ex) www.vsix.kr. AAAA 2001:2b8:1::101 (IPv6 주소)
- ❖ MX 레코드(MX RR) - ex) kisa.or.kr. MX 0 sniper.kisa.or.kr. (메일서버 네임)
- ❖ NS 레코드(NS RR) - ex) kisa.or.kr. NS ns0.kisa.or.kr. (네임서버 네임)
- ❖ NAPTR(NAPTR)
 - ex) 27.1.oid.res.org NAPTR 0 http://www.rfidcode.kr/ods_dodc/rinfo-27.1.-oid-res.org.xml

■ DNS 레코드 타입은 필요에 따라 표준으로 추가 정의되고 있음

- ❖ 현재 약 79개의 DNS 레코드 타입을 표준으로 정의 (<http://www.iana.org/>)
- ❖ 새로운 포맷의 데이터 설정 필요한 경우, 신규 DNS 레코드 타입 표준 정의

도메인 네임 구성

- ❖ 도메인 네임의 구성
- ❖ 다국어 도메인 네임과 퓨니코드(PunyCode)
- ❖ 도메인 네임 체계

도메인 네임의 구성

■ 도메인 네임

■ (레이블) 도메인 네임은 레이블(label)의 조합으로 구성

- ❖ Ex) "www.kisa.kr" → "www", "kisa", "kr", ""의 4개 레이블(label)로 구성
- ❖ 레이블 ""은 특수한 레이블로써 루트 도메인을 의미
- ❖ 레이블은 최대 63바이트를 초과할 수 없음
 - 각 도메인 등록체계에 따라 등록가능 레이블 최대길이를 정책적으로 제한함
- ❖ 각 레이블로 구성된 도메인 네임 전체 길이는 255바이트를 초과할 수 없음

■ (이름 유일성) 하나의 도메인 네임은 인터넷에 유일하게 존재해야 함

- ❖ "도메인 등록체계"를 통해, 동일 네임이 중복 등록되지 않도록 관리
- ❖ 동일 레이블을 사용하더라도 상위 도메인이 다르면 이름 유일성유지
 - Ex) kisa.kr. vs. kisa.com., kisa.net.

■ FQDN = Fully Qualified Domain Name (도메인 네임의 완전한 표현)

- ❖ Ex) "www.kisa.kr."은 FQDN이지만, "www.kisa.kr"은 FQDN이 아님
- ❖ DNS 질의응답을 할 때 DNS 네임서버는 항상 FQDN을 사용

다국어 도메인 네임과 퓨니코드(Punycode)

■ 다국어 도메인

- Internationalized Domain Name
- 영어 이외의 언어를 사용하는 DNS 도메인 (한글.kr, 한글.한국)
- 다국어 도메인은 퓨니코드(Punycode)로 변환하여 DNS에 적용

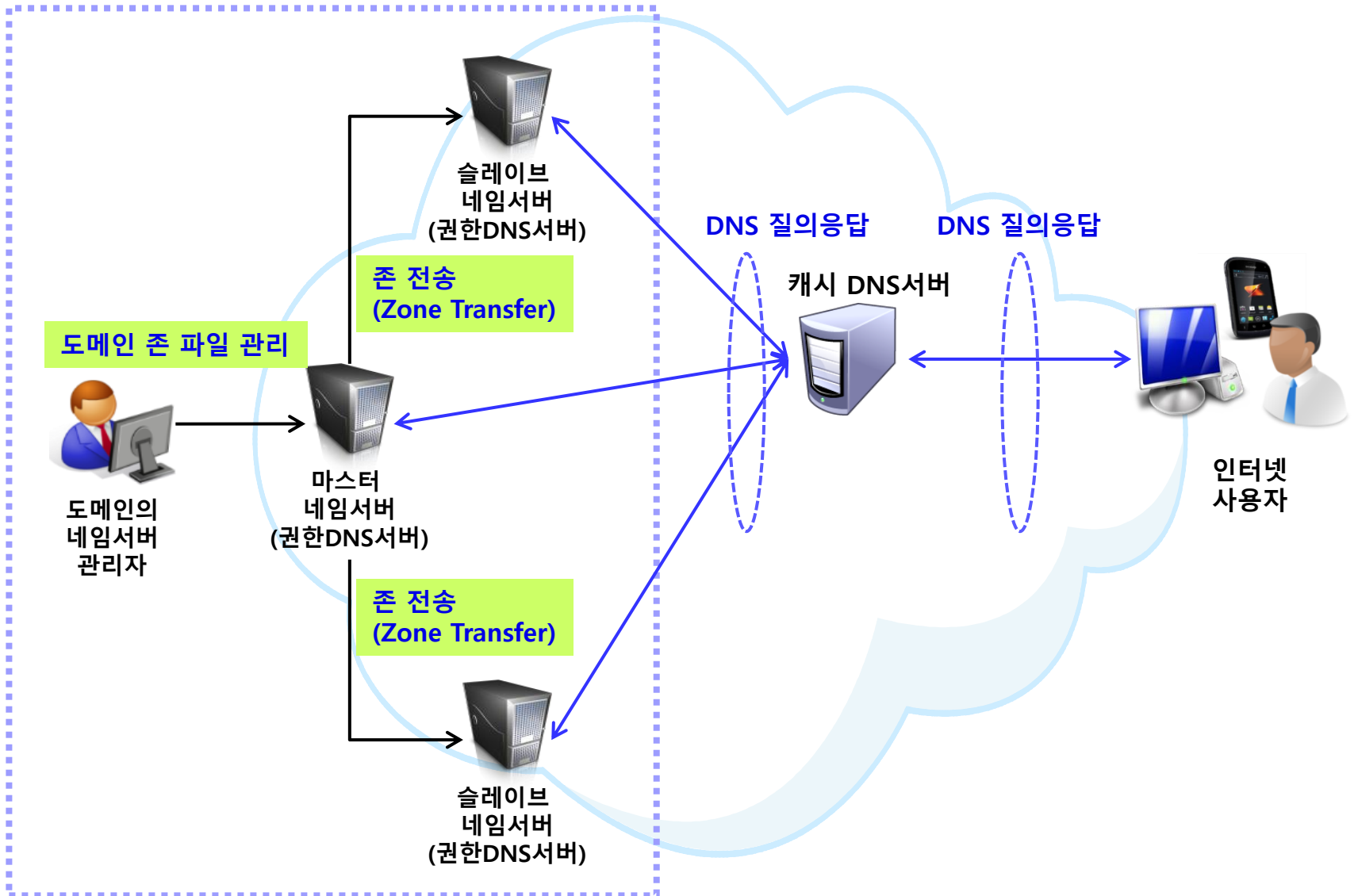
■ 퓨니코드 (Punycode)

- 다국어 도메인을 표준 변환규칙에 의해 변환하여 ASCII 코드로 표현된 문자열을 의미
 - ❖ Ex) 웹브라우저 주소창에 "한국인터넷진흥원.한국" 입력하면 → 실제로는 **xn--3e0bx5e6xzftae3gxzpskhile.xn--3e0b707e** 로 변환해서 질의 응답
 - ❖ ASCII 코드 : 영문 기준으로 정의된 컴퓨터용 코드 체계. 영문자판에 있는 영문자 및 특수기호 등이 대략 이에 해당
- 한글.kr, 한글.한국 : 최대 17개의 한글/영문/숫자, "-" 문자로 구성된 레이블 등록가능
 - ❖ 한글도메인을 퓨니코드로 변환 시 퓨니코드 문자 개수가 늘어나므로,
 - ❖ 도메인 등록정책에서 등록 가능한 레이블 문자개수를 17개로 제한
 - ❖ ASCII 문자표현 기준, 레이블 최대길이 63바이트 초과 방지 위한 제한사항

DNS 관리

- ❖ DNS 관리는 기본적으로 어떻게 이루어지나?
- ❖ DNS 네임서버 구성
- ❖ 도메인의 네임서버 구성 설정 단계
- ❖ 도메인 위임설정 등록

DNS 관리는 기본적으로 어떻게 이루어지나?



네임서버의 구성(1/2)

■ 네임서버 구분

- 권한 DNS (Authoritative 네임서버)
 - ❖ **도메인 존 데이터**를 적재하여 응답처리하는 네임서버 (authority를 갖는 서버)
- 캐시 DNS서버(리커시브 네임서버)
 - ❖ 타 호스트를 대신하여 인터넷 전체에서 질의된 DNS 데이터를 조회, 응답하는 네임서버
 - ❖ 네임서버 기능부와 리졸버 기능부를 조합하여 구현한 서버 프로세스 S/W
 - ❖ 캐시(cache) 관리, 질의응답 절차를 통해 파악된 데이터의 캐싱
 - ❖ 리졸버 기능을 위해, 루트 네임서버 IP 주소 정보(root hint)의 설정을 필요로 함

■ 권한 DNS의 마스터/슬레이브 네임서버 구분

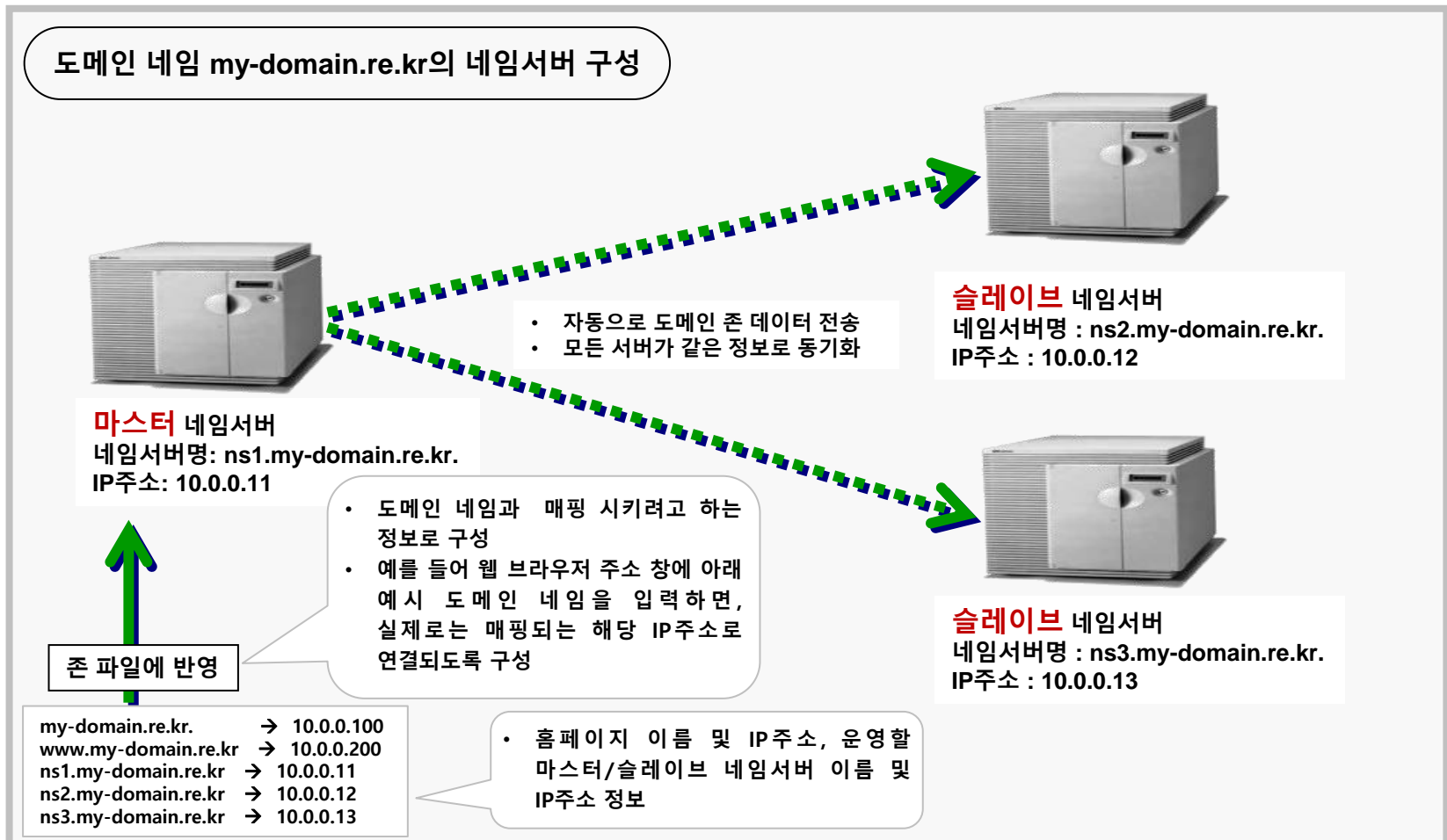
- **도메인 존이 설정된 네임서버 = Authoritative 네임서버**
- 도메인 존 설정 네임서버는 마스터 네임서버, 슬레이브 네임서버로 구분
 - ❖ **마스터 네임서버** : 도메인 존 데이터의 추가, 변경, 갱신 작업 및 네임서버 반영
 - ❖ **슬레이브 네임서버** : 마스터 네임서버로부터 도메인 존 데이터 수신, 동기화
 - ❖ 마스터/슬레이브 네임서버 구성은 **네임서버 다중화**를 위한 구분 및 구성방법
 - ❖ 네임서버 다중화 경우, **도메인 존 데이터의 동기화** 필수 → 마스터/슬레이브 간 동기화
 - 데이터 동기화 방향 : 마스터 네임서버 → 다수의 슬레이브 네임서버

네임서버의 구성(2/2)

- **마스터/슬레이브 DNS서버 구성의 목적**
 - “도메인 존 데이터” 이중화/다중화 구성 구현
 - ❖ 도메인 존이 위치한 DNS서버를 2식 이상으로 구성 이중화/다중화 구현
 - ❖ 일부 DNS서버 시스템의 장애시에도 도메인 존 데이터는 언제나 가용 상태 유지
- **마스터/슬레이브 DNS서버의 구분 기준**
 - “도메인 존에 대하여 마스터 DNS서버, 슬레이브 DNS서버” 구분
 - ❖ 하나의 DNS서버는 도메인 A에 대하여 슬레이브 DNS서버, 다른 도메인 B에 대해서는 마스터 DNS서버로 동작할 수 있음
 - ❖ BIND의 경우, named.conf 파일의 zone 설정에서 “type master;”이면 해당 도메인 존에 대해 이 DNS서버는 마스터 DNS서버 역할
- **마스터/슬레이브 DNS서버의 도메인 존 데이터 동기화 자동 관리**
 - 존 데이터의 SOA 레코드 필드 설정 값에 의존하여 존 데이터 자동 동기화
 - DNS서버 환경설정 파일에 의해 마스터 존/슬레이브 존 구분 관리

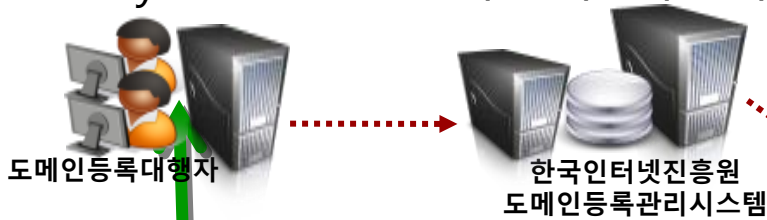
네임서버 구성 설정 1단계 - 네임서버 구성

- 도메인의 마스터 네임서버와 슬레이브 네임서버 구성
 - 도메인 네임과 매핑시키려는 정보를 마스터 네임서버의 존 파일에 반영
 - ❖ 마스터 네임서버에 도메인 존 반영시, 마스터 → 슬레이브 데이터 동기화는 자동 실행



네임서버 구성 설정 2단계 - 도메인의 위임설정 등록

- 도메인 등록 대행자를 통해 네임서버 정보를 상위 네임서버에 등록
 - ❖ my-domain.re.kr의 경우 네임서버 정보를 .kr 네임서버에 등록



도메인의 위임정보 설정등록

my-domain.re.kr의 네임서버 정보

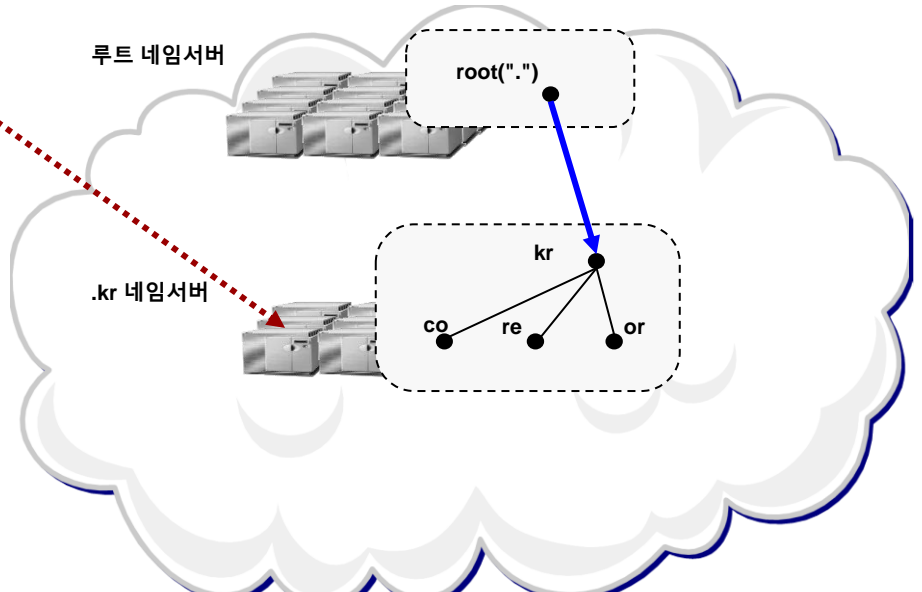
ns1.my-domain.re.kr → 10.0.0.11
 ns2.my-domain.re.kr → 10.0.0.12
 ns3.my-domain.re.kr → 10.0.0.13

도메인 등록관리자

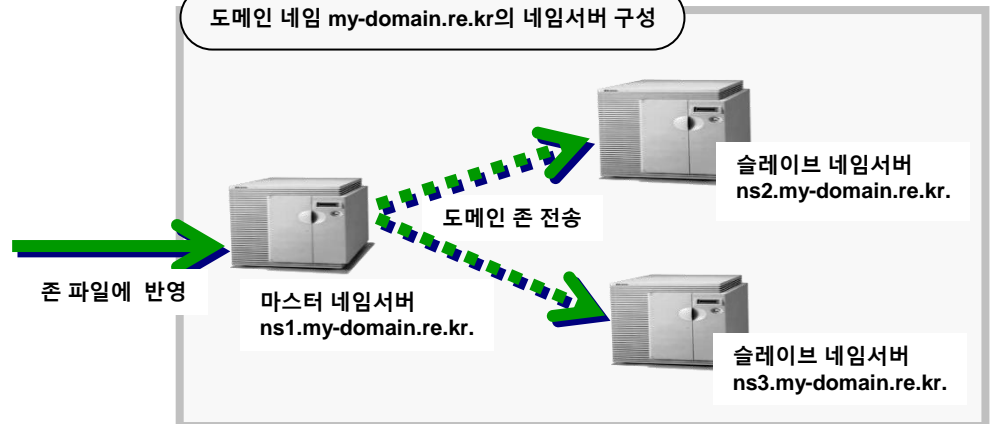
my-domain.re.kr 존 파일

도메인 네임과 매핑 시키려고 하는 정보로 구성
 예를 들어 웹 브라우저 주소 창에 아래 예시 도메인 네임을 입력하면,
 실제로는 매핑되는 해당 IP주소로 연결되도록 구성

my-domain.re.kr → 10.0.0.100
 www.my-domain.re.kr → 10.0.0.200
 ns1.my-domain.re.kr → 10.0.0.11
 ns2.my-domain.re.kr → 10.0.0.12
 ns3.my-domain.re.kr → 10.0.0.13

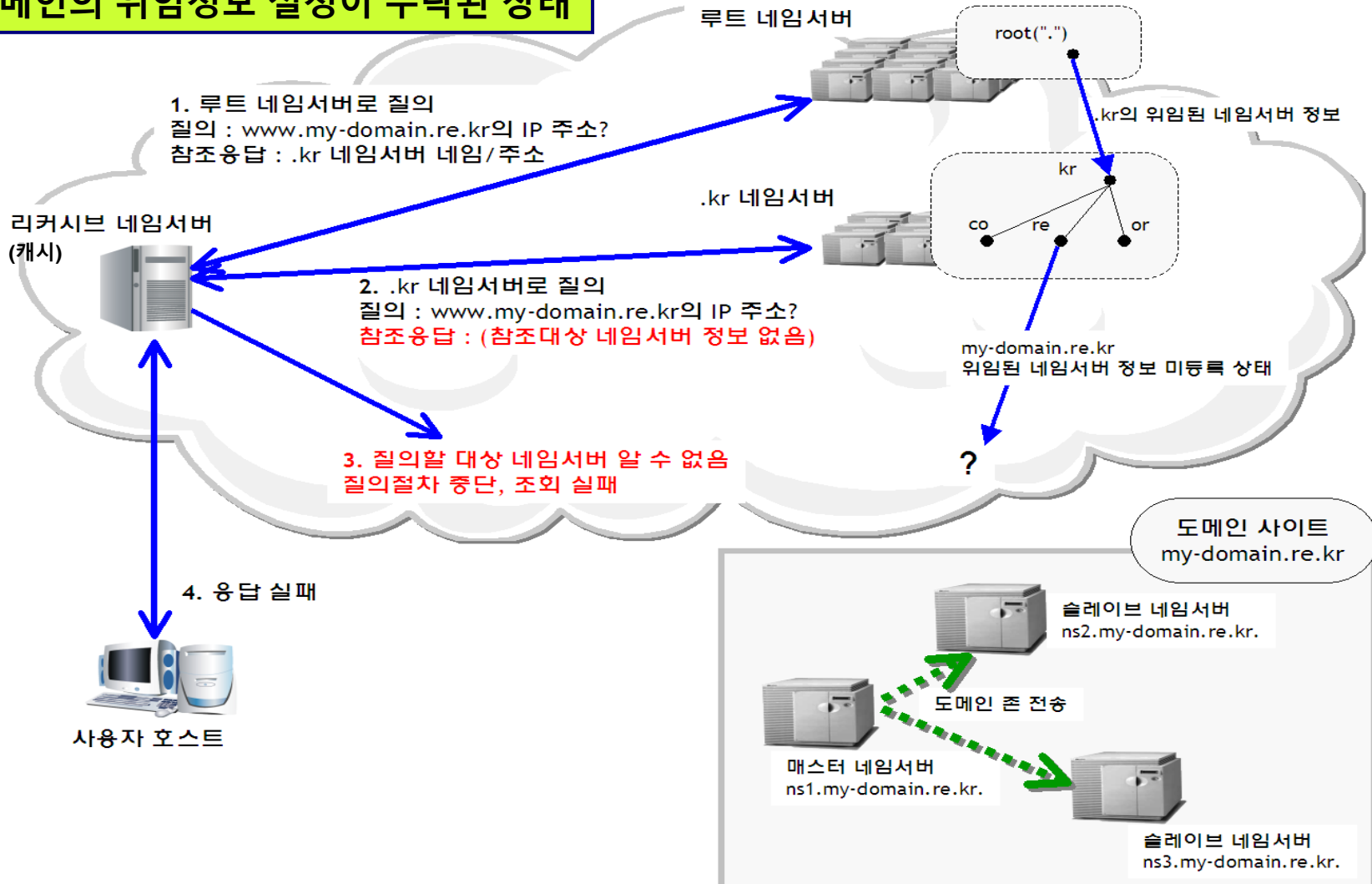


도메인 네임 my-domain.re.kr의 네임서버 구성



도메인 위임정보 설정의 중요성

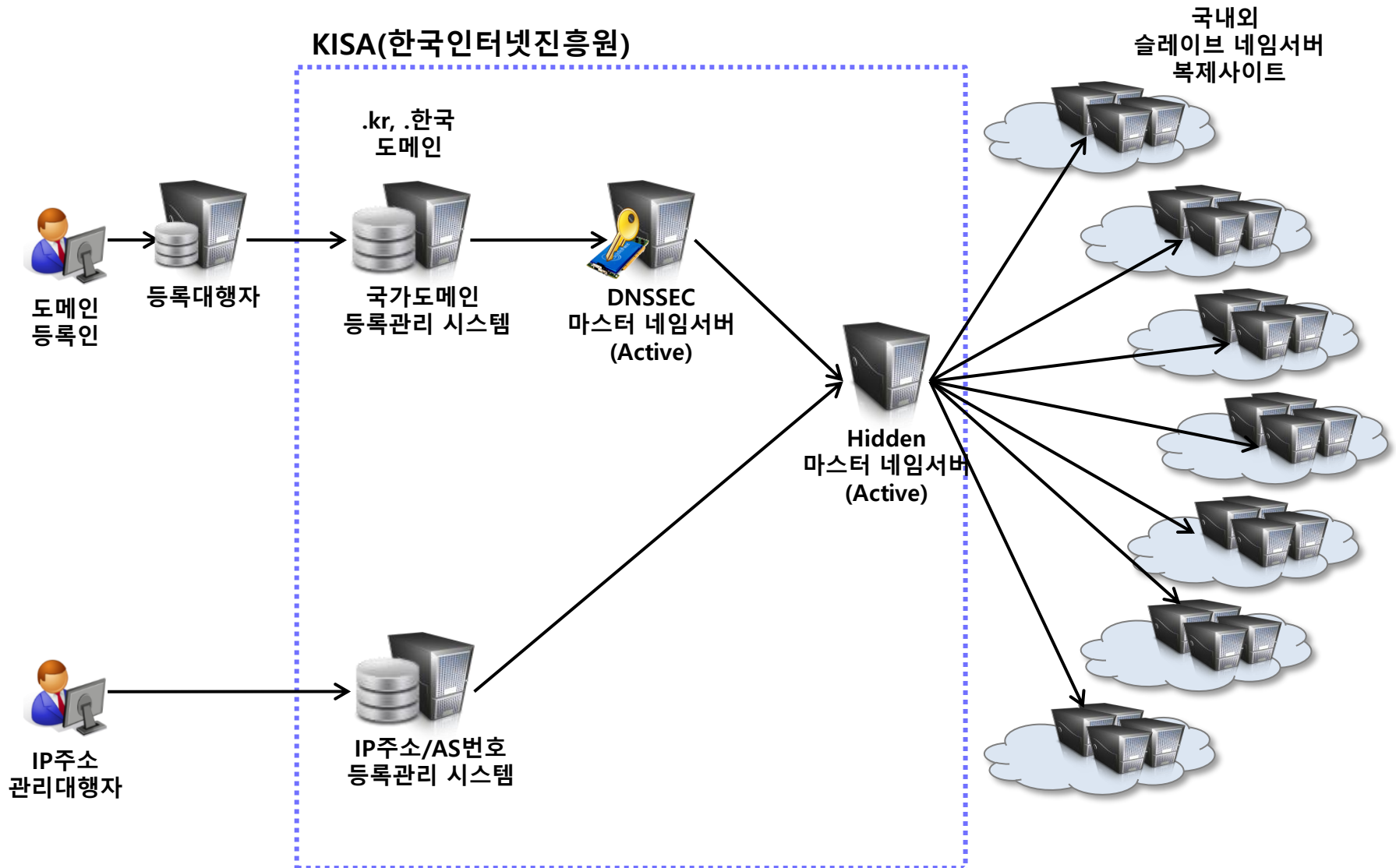
도메인의 위임정보 설정이 누락된 상태



KR DNS 운영현황

- ❖ 도메인 등록정보는 어떤 절차로 kr DNS에 반영되는가?
- ❖ kr DNS가 서비스 중인 도메인

도메인 등록정보는 어떤 절차로 kr DNS에 반영되는가?



kr DNS가 서비스 중인 도메인

구분	도메인	개요
ccTLD	.kr	<ul style="list-style-type: none"> ❖ .kr 도메인 ❖ 총 30개 도메인 존으로 구성(co.kr, go.kr 등) ❖ 한글.kr, 영문.kr 도메인은 kr 존에 설정
다국어(IDN) ccTLD	.한국	<ul style="list-style-type: none"> ❖ .한국 도메인 (한글.한국) ❖ .한국 1개 존으로만 구성
인버스 도메인 (Inverse Domain)	.in-addr.arpa	<ul style="list-style-type: none"> ❖ IPv4 주소에 대한 DNS 역질의 용 도메인 ❖ 할당된 IPv4 프리픽스 당 1개 존으로 구성 (현재 1551개 존)
		<ul style="list-style-type: none"> ❖ IPv6 주소 경우의 인버스 도메인 설정 <ul style="list-style-type: none"> ▪ KISA는 IPv6 주소할당은 하지만, 인버스 도메인은 APNIC에서 설정 ❖ IPv6 주소의 인버스 도메인은 ip6.arpa 도메인 영역 사용

- ※ TLD : Top-Level Domain (최상위 도메인)
- ※ ccTLD : country code TLD (국가 최상위도메인)
- ※ IDN : internationalized domain name (다국어 도메인)
- ※ 한글.kr : 다국어 도메인으로 한글을 포함하는 2단계 .kr 도메인 (한국인터넷진흥원.kr)
- ※ 영문.kr : 영문으로만 구성된 2단계 .kr 도메인 (ex: kisa.kr)
- ※ .한국 : 한글을 사용하는 다국어 국가최상위 도메인
- ※ 인버스 도메인 (Inverse Domain) : IP주소 → 도메인네임 파악에 사용되는 DNS 역질의 용 도메인

감사합니다.