

# DNSSEC

얼마 전 "한국 가정, 인터넷 없이 살수 있을까"라는 기사를 보았다. 기사는 영국 BBC 방송이 세계에서 인터넷이 제일 발달한 한국의 가정을 대상으로 인터넷을 사용할 수 없는 생활을 실험하는 내용이었다. BBC는 많은 어려움 속에 2가정의 승낙을 얻어 일주일간 인터넷 사용을 차단하고 실험을 진행하였다. 참가자들은 일주일간의 인터넷 없는 생활에 많은 어려움을 호소하였고 앞으로는 이런 일을 다시 겪고 싶지 않다고 했다. 이들 참가자들의 실험을 통해 인터넷이 삶에 얼마나 큰 영향을 주고 우리의 인터넷 의존도가 얼마나 광범위한지 새삼 돌아볼 수 있는 기회였다.

오늘날 과거 2003년 1월 25일에 발생한 속칭 '1.25 대란'처럼 전체 인터넷이 마비된다면 어떤 상황이 발생할까? 2003년 당시 생활이 불가능할 것 같은 불편함과 다양한 문제가 발생하였다. 인터넷 의존도가 더욱 높은 현대에 이러한 재앙이 발생한다면 요즘 이슈가 되고 있는 자연 재해와도 비견되는 영향을 끼칠 것이다.

## 도메인 네임 시스템

다른 대부분의 인터넷 서비스와 시스템의 장애와 달리, 앞서 '1.25대란'처럼 전체 인터넷에 가장 큰 영향을 끼친 재앙은 인터넷에서 가장 중요한 요소인 도메인 네임 시스템(이하 DNS)의 서비스 장애에 의한 것이었다.

DNS는 사람의 나이로 따지면 벌써 30살을 넘긴 성년이다. DNS가 처음 탄생하던 당시 인터넷은 굉장히 작고 좋은 용도에만 사용되어 이러한 공격에 대한 방어 능력을 고려하지 않았다. DNS는 30년 이상을 지내오면서 다양한 보안/기능 문제가 발견되고 또한 수정/개선되며 진화해오고 있다.

DNS는 일반적으로 인터넷의 전화번호부라고 많이들 표현한다. 사람이 기억하기 어렵지만 컴퓨터에게 필요한 IP주소를, 사람이 기억하기 쉬운 문자를 통해 변환하는 시스템이다. 예를 들어 네이버에 접속하기 위해 '202.131.29.70'이라는 IP주소를 웹 브라우저에 넣고, 네이버 메일을 사용하기 위해 '202.131.27.109'라는 IP주소를 기억해야 된다면 인터넷은 너무 어렵고 혼란스러운 곳이 된다. DNS를 사용하면 '[www.naver.com](http://www.naver.com)', 'mail.naver.com'이라는 이름을 또는 '서울시청' 등과 같이 한글을 입력해도 컴퓨터가 이해할 수 있는 IP주소로 자동으로 변경해서 연결해준다. 또한 거꾸로 IP주소를 호스트 이름으로 변경해주고 메일 라우팅 정보 등과 같은 도메인이나 호스트에 대한 다른 정보들도 제공해준다.

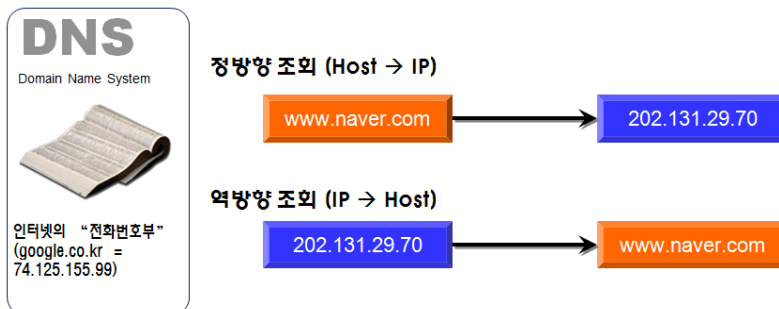


그림 1> DNS는 인터넷의 전화번호부

DNS는 분산형 데이터베이스 시스템으로 다음과 같은 구성요소를 가지고 있다.

### DNS의 구성요소

- 도메인 네임 공간: 인터넷에서 사용되고 있는 도메인 네임의 계층적 구조 공간
- 리소스레코드 (RR, Resource Records): 도메인 네임이 갖는 속성값
- 네임 서버: 도메인 존(domain zone) 정보를 소유하고 이에 대한 질의에 응답하는 역할 수행
  - 마스터 네임 서버: 도메인에 대한 소유권을 가지고 있는 네임서버로 Zone file에서 자료를 로딩
  - 슬레이브 네임 서버: 마스터가 비정상 작동시 부하를 분산시키기 위해 운영하며 zone transfer를 통해 마스터로부터 복제된 자료를 전송 받고 여러 대를 운영할 수 있음
  - 리커시브(Recursive) 네임 서버: 도메인에 대한 정보는 관리하지 않고 도메인 네임만 해석 (분해)하고 성능 향상을 위해 한번 응답된 정보는 일정기간 메모리에 캐싱한다. 비슷한 기능으로 다른 캐싱서버를 이용하는 캐싱서버인 Forwarder가 있음
- 응용 프로그램: 웹 브라우저, 전자메일 클라이언트, 메신저 등 서버와 통신을 위해 리졸버 (Resolver)와 통신하는 프로그램들
- 리졸버(resolver): 네임서버에 질의(query)를 보내고 응답을 해석한 뒤 요청했던 응용 프로그램에 정보를 되돌려 줌

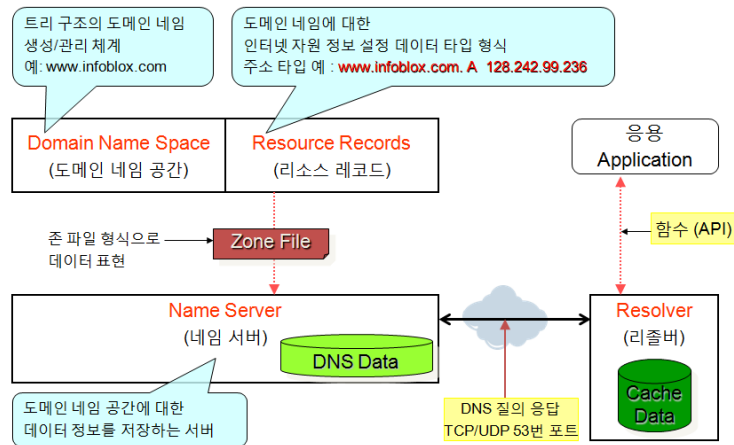


그림 2> DNS의 구성요소

### DNS 동작 방식

도메인 네임은 그림과 같이 서로 계층적으로 연결되어 있는 공간에 존재한다. 이 공간을 사람으로 표현하면 시조(root domain)가 되는 조상이 있고, 이분 밑으로 할아버지(Top level)에 할아버지(Second level)들이 존재하여 아버지(Third or Sub domains)까지 내려온다. 여기서 아버지가 결혼을 하면서 새로운 가정이 탄생하듯이, 도메인 공간에서는 원하는 부모 도메인에 새로운 도메인 네임을 등록한다. 한 가정의 가장이 해당 가정을 대표하듯이, 할당 받은 도메인 공간도 모든 권한을 가진 도메인 네임 서버가 해당 도메인 공간을 관리/운영한다.

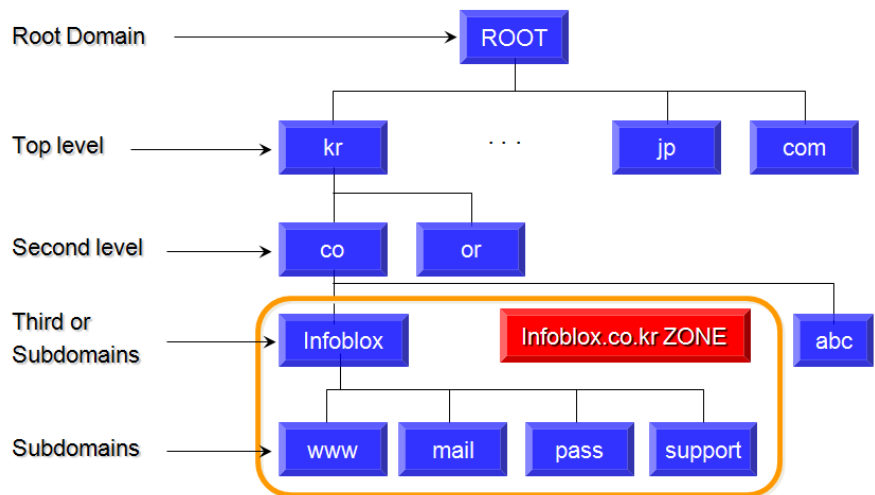


그림 3> 도메인 네임 공간

이 도메인 네임 공간에서 'infoblox.co.kr'이라는 신규 도메인의 웹 서버인 '[www.infoblox.co.kr](http://www.infoblox.co.kr)'은 어떻게 찾을 수 있을까? 사용자는 'Local DNS' 또는 PC에 기본적으로 설정된 DNS 서버에게 '[www.infoblox.co.kr](http://www.infoblox.co.kr)'의 IP주소를 질의한다. 'Local DNS'가 해당 웹 서버의 IP주소를 캐시로 저장하고 있다면 바로 알려주겠지만 그렇지 않다면 재귀 쿼리(recursive query)를 행한다. 'Local DNS'는 루트(".") 도메인 → top 레벨 도메인 → second 레벨 도메인 → third 또는 서브 도메인 등까지 계층적으로 정보를 요청한다. 상위 도메인들은 각 하위 도메인에 대한 정보만 알고 있어서 루트 도메인은 top 레벨 도메인 정보만 알고 있고, top 레벨 도메인은 second 레벨 도메인만 알고 있어서 순차적으로 목표를 찾아가야 된다.

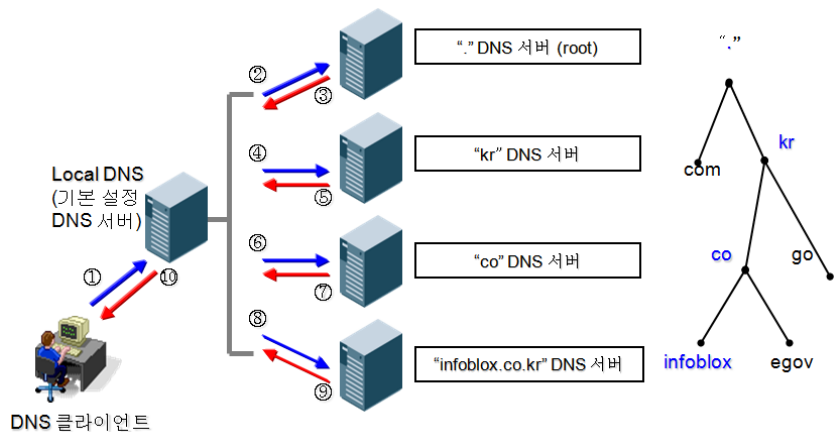


그림 4> DNS 동작 프로세스

### 도메인 데이터 캐싱

'Local DNS'는 루트 도메인부터 쿼리를 수행하면서 얻은 결과를 일정기간 저장해두고 동일한 요청이 반복되면 다시 루트 도메인부터 쿼리를 하지 않고 저장된 내용을 재사용한다. 이와 같이 관리하는 도메인 네임 없이 재귀 쿼리(recursive)만 수행하는 도메인 네임 서버를 리커시브 네임 서버 또는 캐싱 네임 서버라고 한다. 우리가 일반적으로 알고 있는 KT DNS 서버 168.126.63.1~2, 데이콤 164.124.101.31과 203.248.240.3 등이 이에 해당한다. 이들 DNS 서버는 클라이언트가 요청

한 도메인을 해석하면서 이 과정에서 발생하는 정보를 저장하여 다시 사용하는 역할을 수행한다. 리커시브 네임서버의 공로는 다음과 같이 네트워크에서 DNS 트래픽을 감소시키고, 클라이언트에게 빠른 응답을 제공하며 루트 DNS의 부하를 분배하는 역할을 한다.

년도	DNS 트래픽 비율	리포팅
1990	14%	Danzig <i>et al.</i>
1992	8%	
1995	5%	Frazer
1997	3%	Thompson <i>et al</i>

표 1> 리커시브 네임서버의 DNS 캐싱으로 발생한 DNS 트래픽의 감소 율

### DNS 시스템 보안

대부분의 새로운 서비스와 프로토콜이 그러하듯 DNS도 보안을 고려하지 않고 설계되었다. 인터넷의 거의 모든 시스템은 DNS에 의존되어 운영되고 서비스를 제공한다. 침해공격에 의해 서비스 불안정 또는 서비스 중단 사태가 발생할 경우 DNS에 의존하는 거의 모든 인터넷 서비스도 같이 장애가 발생된다. 이 규모는 특정 호스트나 서비스 장애와 달리 영향도가 굉장히 커서 심각한 문제를 유발한다.

DNS에 대한 위협은 크게 세 가지로 분류할 수 있다.

서비스거부(DoS 또는 DDoS) 공격, DNS 서버 취약점, DNS 데이터 변조(spoofing) 취약점이 있다.

‘서비스거부(Denial of Service)’ 공격은 공격자가 악의적인 질의(query)를 대량으로 발생시켜 목표 네임서버가 해당 질의를 처리하는 동안 다른 정상 서비스요청에 대해서는 응답을 못하게 하는 공격이다. 특히 2007년 2월 6일 전 세계 최상위에 있는 13개 루트서버 중 6대에 대해 이 공격이 시도되었다. 약 2시 30분 동안 진행된 공격에 의해 g루트와 l루트 서버의 서비스에 영향을 받았다.

‘DNS 서버 취약점’은 네임서버 프로그램 버그에 의한 취약점을 의미한다. 이 취약점에 의해 네임서버 프로그램이 중지되거나 시스템 전체가 공격자의 손에 넘어갈 수 있다. 현재는 네임서버 프로그램의 버그 발견시 영향을 고려하여 최단 시간 안에 수정용 패치 프로그램이 배포되고 있다.

‘데이터 변조 취약점’은 말 그대로 네임서버가 주고받는 정보를 악의적인 공격자가 임의로 조작하여 인터넷상에 퍼뜨리는 공격이다. 공격을 받았는지 여부를 발견하기 어려워 그에 따른 피해가 매우 커질 수도 있다.

### DNS 데이터 위-변조 취약점, DNS 캐시 포이즈닝

이들 취약점들이 모두 큰 위협이 될 수 있지만 궁극적으로 가장 위험한 취약점은 일명 ‘스푸핑(spoofing)’으로 알려진 네임서버 정보에 대한 위변조 위협이다. 예를 들어 인터넷 뱅킹을 이용할 때 사용하는 도메인네임이 공격자에 의해 위변조 되었다면, 실제 인터넷 뱅킹사이트가 아닌 공격

자가 만들어둔 거짓 사이트에 자신의 금융/개인정보를 그대로 노출시킬 수도 있다.

이러한 형태의 공격을 "DNS 캐시 포이즈닝(DNS cache Poisoning)"이라 부른다.

리커시브 네임서버 또는 캐시 DNS가 관리하는 캐시(cache)에 위-변조된 데이터를 저장하도록 유도하기 위한 공격 형태다.

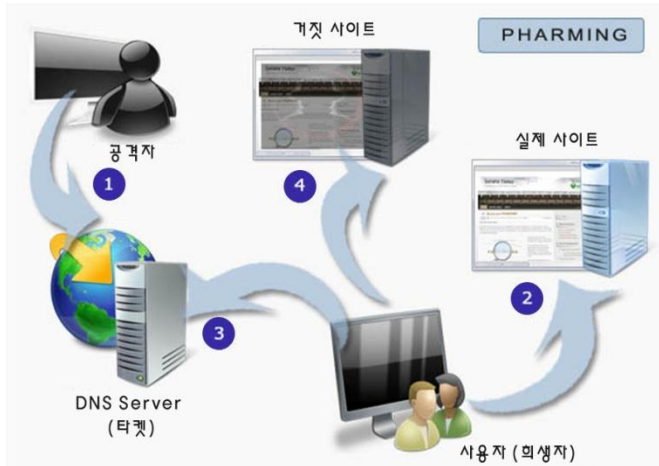


그림 5> 파밍(Pharming) 공격방법

"DNS 캐시 포이즈닝" 공격은 "파밍(Pharming)"이라는 공격형태에 포함된다.

파밍(Pharming)은 사이트 접속 트래픽을 진짜 사이트처럼 위장된 사이트로 전환시키는 것을 목적으로 하는 모든 형태의 공격을 가리킨다.

우리가 익히 알고 있는 피싱(Phishing)은 사용자를 도메인 네임과 철자가 유사한 도메인 네임을 사용하여 위장된 사이트로 접속을 유도한다. 그러나 파밍(Pharming)은 사용자가 올바른 도메인 네임을 확인하는 등의 충분한 주의를 기울이더라도 이 도메인 네임의 IP 주소가 이미 위-변조된 주소로 매핑되어 위장된 서버에 접속하는 것을 피할 수 없다.

이 점에서 위협적인 공격 형태로 인식되고 있다. 사용자가 아무리 주의하더라도 자신이 가짜 IP 주소를 갖는 사이트에 접속하고 있다는 사실을 사용자는 쉽게 알아챌 수 없다.

특히 DNS 캐시 포이즈닝의 경우, 공격 대상인 리커시브 네임서버를 사용하고 있는 수많은 호스트들이 모두 동시에 이 공격의 피해자가 될 수 있다는 점에서 심각한 위협요인을 가지고 있다.

이번 호에서는 DNS의 기본적인 개념과 보안 위협에 대해 살펴보았다. 다음 호에는 DNS 위협의 가장 큰 파장을 일으킬 수 있는 "DNS 캐시 포이즈닝" 공격을 방지하고 DNS 보안을 한층 강화시키는 DNS 보안확장(DNSSEC)에 대해 알아보겠다.

[솔루션 문의]

㈜오픈베이스 시스템사업본부 [infrasales@openbase.co.kr](mailto:infrasales@openbase.co.kr)