

DNSSEC 도입현황 및 참고자료

DNSSEC 적용은 특정 기관이나 기업이 시행할 수 없는 전 세계적인 프로젝트다. 물론 기업이나 기관이 자신의 도메인의 보안 안정성을 강화하기 위해 DNSSEC을 적용할 수 있다. 그러나 지난 호에서 설명했듯이, DNSSEC이 적용된 존을 검증할 수 있는 리커시브 DNS 서버를 DNS 클라이언트가 사용할 수 없다면 무의미한 일이 된다.

DNSSEC을 원활히 적용하기 위해서는 상위 도메인(루트와 ccTLD 등)과 타 도메인들의 적용상황을 관심 있게 주시하고, 우리 기관 또는 기업에 적용하기 위해 필요한 자원과 사항에 대해 준비가 필요하다.

이번 호에서는 .com, .org, .net 등의 도메인을 보유하고 있는 기업 및 기관들과 연관된 최상위 도메인들의 DNSSEC 적용 움직임과 .kr, go.kr, co.kr 등의 국내 도메인을 보유하고 있는 기업 및 기관들과 연관된 국내 DNSSEC 도입현황과 예정에 대해 살펴본다.

또한 DNSSEC 적용에 사용할 수 있는 소프트웨어 & 하드웨어 툴과 다양한 자료를 얻을 수 있는 참고 사이트들을 살펴보자.

전 세계 DNSSEC 도입 진행사항

인터넷 포털 사이트들과 몇몇 기업들이 소유하고 있는 .net 과 .com 도메인은 베리사인(VeriSign)이나 ICANN(Internet Corporation for Assigned Names and Numbers)에서 관리 운영하고 있다. 이들이 관리 중인 루트 도메인을 포함하여 다양한 국가 도메인들의 DNSSEC 적용이 가속화되고 있다.

- 2010년 5월 25일을 기준으로 전 세계 약 20,786개 도메인의 존이 서명되었으며 이중 19,186개는 상용 서비스에 사용되고 있다.
- .br(브라질), .bg(불가리아), .ch(스위스), .cz(체코공화국), .pt(포르투갈), .se(스웨덴) 등 다수의 국가도메인이 서명을 완료하였고 다른 국가의 도메인들도 적용을 진행 중이다.
- 2009년 6월에 Public Interest Registry 가 최상위 도메인 중 최초로 .org 존에 서명을 완료하고 나머지 루트 도메인들도 DNSSEC 적용을 진행 중이다.
- 미국의 NTIA/DoC 는 2010년 7월 1일까지 루트 존의 서명을 완료할 예정이고, FISMA 는 2010년 여름까지 정부 기관의 인터넷 존에 DNSSEC 을 적용하도록 권고하였다.
- 베리사인(VeriSign)은, .net 존은 2010년까지 .com 은 2011년까지 서명하겠다고 발표하였다.

World Wide DNSSEC Deployment

See also [DNSSEC Threat and Work \(Risk\) Deployment](#) by Paul Wouters, November 21, 2007, [RFC49](#)



그림 1> 전세계 DNSSEC 도입현황(<http://www.xelerance.com/dnssec/>)

DNSSEC 국내 도입 진행사항

우리나라의 Kr 도메인을 관리하고 있는 한국인터넷진흥원은 DNSSEC 적용을 위해 시험 시스템을 구축하고 DNSSEC 교육과 홍보 강화, 가이드라인 작성 배포와 주요 ISP 에 DNSSEC 도입을 촉진시키기 위해 다양한 활동을 시행하고 있다.

- 2006 년에 DNSSEC 시험 시스템을 구축하여 DNSSEC 의 기술적 검증을 시행하고 있다.
- 2007 년도부터 DNSSEC 시범 서비스인 safenet.kr 을 통해 몇몇 기관과 기업을 대상으로 서비스를 시험하고 있다.
- 2008 년도에 DNSSEC 키 관리방안 연구와 2009 년 키 관리 및 존 서명 기본정책 등을 수립하였다.
- Kr 도메인에 DNSSEC 을 적용하는 순서는 safedns.kr 에서 시범 서비스를 제공하고 미국의 .gov 에 해당하는 .go.kr 을 2010 년도에 그리고 2011 년부터는 Kr 전체 도메인에 적용할 예정이다.

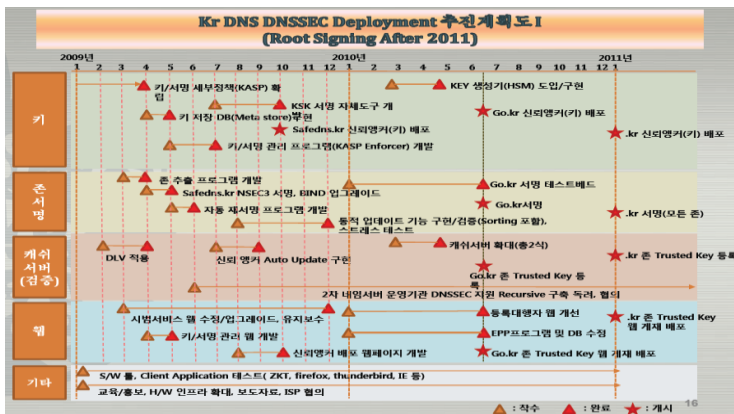


그림 2> Kr DNS DNSSEC 도입 추진도(출처: ICT Forum KOREA 2009)

참고 사이트 및 소프트웨어/하드웨어 툴 소개

DNSSEC 도입이 활발해짐에 따라 다양한 참고 사이트와 DNSSEC 적용을 돕는 툴들이 개발되고 있다. 검색엔진 등을 통해 각자에게 유용한 자료를 검색하여 사용할 수 있지만, 여기서 몇 가지

유용한 사이트와 툴들을 소개한다.

DNSSEC 관련 조직과 웹 사이트

- DNSSEC.net(<http://www.dnssec.net/>): DNSSEC 관련 기술자료와 서버 소프트웨어 및 유틸리티 등 DNSSEC 관련 정보를 제공한다.
- DNSEXT(<http://datatracker.ietf.org/wg/dnsext/charter/>): DNS 확장에 대한 IETF 워킹그룹으로 다양한 표준을 개발하고 있다.
- CircleID(<http://www.circleid.com/topics/dnssec/>): DNSSEC 관련 이슈에 대한 뉴스와 의견을 게재하여 원하는 정보를 찾아볼 수 있다.
- DNSSEC-Tools Project(<http://www.dnssec-tools.org/>): DNSSEC과 관련된 기술을 쉽게 적용할 수 있는 소프트웨어 툴, 패치, 어플리케이션 등을 개발 및 배포한다.
- 한국인터넷진흥원 DNSSEC 자료실(<https://dnssec.kisa.or.kr/>): Kr 도메인의 DNSSEC 적용에 대한 진행사항, 기술문서와 교육자료 등 다양한 정보를 제공한다.

DNSSEC을 적용하는데 유용한 툴

DNSSEC은 인터넷 표준 프로토콜인 DNS와 가장 보편적인 보안 기술인 공개키 암호화 방식이 사용되었다. 쉽지않은 두가지 기술을 오류없이 적용할 있도록 도와주는 다양한 툴들이 있다. 여기서 소개하는 툴들은 [dnssec-deployment.org](https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources)가 제공하는 Tools and Resources 페이지(https://www.dnssec-deployment.org/wiki/index.php/Tools_and_Resources)의 내용을 정리한 것으로, 광범위한 툴에 대한 정보를 제공하니 방문해보기 바란다.

DNSSEC의 핵심 3 요소는 키를 생성하고 존을 서명한 후 이를 검증하는 것이다.

다음은 키를 생성하고 생성된 키로 존을 서명하며 키가 만료되기전에 키를 롤오버하는 툴들이다.

툴	설명	관리 기관	링크
dnssec-keygen, dnssec-signzone	BIND 배포 본이 제공하는 표준 툴	ISC	http://www.isc.org
nom_keytool, ans_signer	ANS 배포 본이 제공하는 표준 툴	Nominum	http://www.nominum.com
jdnssec-keygen, jdnssec-signzone	jdnssec-tools 세트	Verisign Labs	http://www.verisignlabs.com/dnssec-tools/
ldns-keygen, ldns-signzone	Ldns 툴 세트	NLNet Labs	http://www.nlnetlabs.nl/ldns/
pdnssec-keygen, pdnssec-signzone,	DNSSEC perltools 배포 본이 제공하는 툴	Roy Arends	http://www.nsec3.org/cgi-bin/trac.cgi/browser/dnssec/perltools/
zonesigner	dnssec-tools 세트의 툴로 BIND 툴을 래핑	SPARTA, Inc	http://www.dnssec-tools.org/wiki/index.php/Zonesigner
dnssec-zkt와 dnssec-sign	BIND 툴 래핑	HZNET	http://www.hznet.de/dns/zkt/
ldns-zsplit와 ldns-zcat	대량의 존을 병렬로 서명하는 Ldns 툴	NLNetLabs	http://www.nlnetlabs.nl/ldns/
maintkeydb, dnssigner	DNSSEC 키 관리 툴 세트	RIPE NCC	https://www.ripe.net/projects/dnssec/maint_tool/
Rollerd와 rollctl	ZSK와 KSK 롤오버의 다른 단계를 관리하기 위한 dnssec-tools 패키지	SPARTA, Inc	http://www.dnssec-tools.org/wiki/index.php/Rollerd
Maintkeydb	DNSSEC 키를 저장한 데이터베이스의 명령어라인 인터페이스	RIPE NCC	https://www.ripe.net/projects/dnssec/maint_tool/
OpenDNSSEC	DNSSEC 관리를 위한 오픈 소스 키 솔루션	OpenDNSSEC	http://www.opendnssec.org

표 1> 키 생성, 존 서명, 키 롤 오버 툴

다음은 서명한 존에 이상이 없는지를 확인하고 모니터링 하는 툴들이다.

툴	설명	관리 기관	링크
SZIT 모니터 확장팩	베스트 프랙티스와 보안에 맞춰 존 콘텐츠를 테스트하는 툴	NIST	http://snad.ncsl.nist.gov/dnssec/
donuts과donutsd	dnslint처럼 존 파일을 분석하기 위해 dnssec-tools 세트가 제공함	SPARTA, Inc	http://www.dnssec-tools.org/wiki/index.php/Donuts
Mapper	존 파일의 내용을 그래프로 보여주는 툴	SPARTA, Inc	http://www.dnssec-tools.org/wiki/index.php/Mapper
jdnssec-verifyzone	암호학적으로 존의 서명 검증	Verisign Labs	http://www.verisignlabs.com/dnssec-tools/
named-checkzone	BIND 배포 본에서 제공하는 표준 툴	ISC, BIND	http://www.isc.org
DNSCheck	존 상태 체크	.SE	http://dnscheck.iis.se
nagios plugin	만료된 DNSSEC 서명을 확인하는 플러그인	The Measurement Factory	http://dns.measurement-factory.com/tools/nagios-plugins/check_zone_rrsig_expiration.html
OpenDNSSEC	공개된 네임서버 존의 DNSSEC 메타-데이터를 체크함	OpenDNSSEC	http://www.opendnssec.org
SecSpider	전 세계적에 분산되어 DNSSEC 컴플라이언스와 가용유무 확인	UCLA, Colorado State	http://secspider.cs.ucla.edu/
Vantages	DNSKEY 동기화를 포함하여 DNSSEC 적용을 지원하는 툴	Colorado State	http://www.vantage-points.org/
ZoneCheck	설정 오류나 불일치를 해결하는 오픈 소스 프로그램	Stephane D'Alu, AFNIC Team	http://www.zonecheck.fr/
DNSViz	DNSSEC 인증 체인을 그래프로 보여주어 DNS 네임 공간의 설정 오류를 탐지	Sandia National Laboratories	http://dnsviz.net/

표 2> 존 장애 지원 및 모니터링 툴

다음은 리커시브 네임 서버에서 DNSSEC이 적용된 존을 검증하는데 필요한 신뢰앵커(Trust Anchor)를 관리하는 툴들이다.

툴	설명	관리 기관	링크
trustman	검증 리졸버에서 신뢰앵커를 자동으로 롤 오버 하는 툴	SPARTA, Inc	http://www.dnssec-tools.org/wiki/index.php/Trustman
Autotrust	신뢰 앵커를 자동으로 업데이트하는 명령어 라인 툴	NLnetLabs	http://www.nlnetlabs.nl/projects/autotrust/
ldns-keyfetcher	지정한 도메인의 DNSKEY를 받아오는 툴	NLnetLabs	http://www.nlnetlabs.nl/ldns/
getdnskeys	DNS 존에서 DNSKEY의 리스트를 받아와서 비교하고 저장하는 툴	SPARTA, Inc	http://www.dnssec-tools.org
dnssec-conf	DNSSEC의 주요 환경을 설정하는 툴	Xelerance	ftp://ftp.xelerance.com/dnssec-conf/dnssec-conf-1.08.tar.gz
vantaged	신뢰 앵커 관리 서비스	Colorado State Univ	http://vantage-points.org/vant-apps.html#dnskey
dnskey-grab	지정한 존의 DNSKEY를 받아옴	Colorado State Univ	http://vantage-points.org

표 3> 신뢰 앵커(Trust Anchor) 관리 툴

다음은 DNSSEC이 기본적으로 적용된 상용 DNS 어플라이언스에 대한 정보다.

툴	설명	관리 기관	링크
---	----	-------	----

DNS Signer	DNSSEC 관리 업무를 자동화하는 어플라이언스	Secure64	http://www.secure64.com/
Infoblox	DNS/DHCP/IPAM 전용 솔루션	Infoblox	http://infoblox.com/
dnsX	보안 서명, 캐싱 리졸버와 권한 네임 서버 기능을 수행하는 어플라이언스	Xelerance	http://www.xelerance.com/
SolidDNS	DNS 서비스를 쉽고 효율적으로 관리하는 어플라이언스	InfoWeapons	http://www.infoweapons.com
IPControl Sapphire	DNS/DHCP/IPAM 전용 솔루션	INS	http://btdiamondip.com/
NameSurfer	DNS/DHCP/IPAM 전용 솔루션	Nixu	http://www.nixusoftware.com/

표 4> DNSSEC 전용 어플라이언스

DNSSEC 도입에 관하여

DNSSEC 은 1990 년대 말에 초안이 발표되었지만 전세계 수만 대의 DNS 에 도입되기까지 앞으로 얼마나 많은 시간이 걸릴지 알지 못한다. 전세계 루트 도메인 서버와 ccTLD 그리고 정부 기관들의 도입현황을 보면 몇 년 안에 대다수 DNS 에 DNSSEC 적용이 보편화될 것으로 기대된다.

“미 백악관 관리예산처(OMB)가 2009 년까지 국토안전부를 포함하여 정부기관의 인터넷 도메인에 대해 서명하도록 지시하였으나 80%가 진행하지 않은 문제에 대해 전문가들은 미국 정부가 사이버 안보에 우선순위를 두지 않는다고 지적하고 있다. 일반적으로 카민스키(Kaminsky) 버그로 알려진 인터넷의 도메인 네임 시스템의 중대한 버그가 발견된 후에, OMB 의 DNSSEC 적용에 대한 마감 시한이 통보되었다.”

위의 기사는 DNSSEC 이 단순하게 특정 기한까지 적용하도록 지시한다고 해서 쉽게 시행되는 사안이 아님을 단적으로 보여주는 예다. DNSSEC 이 우리 일상의 보편적인 틀이 된 인터넷의 기반 기술을 더욱 안전하게 하고 이를 토대로 신뢰할 수 있는 서비스를 제공할 수 있음을 인지해야 한다. DNSSEC 적용을 전체적으로 원활히 확산하기 위해 홍보와 교육 그리고 감독기관들의 가이드라인, 지침서와 구체적인 보안 정책들이 제공되어야 한다.

4 월호에서 인터넷의 가장 핵심 프로토콜인 DNS 의 다양한 문제점을 짚어보고, 이중 가장 큰 파급 효과를 가진 캐시포이즈닝 공격과 DNS 의 근본적인 보안 이슈에 대해 설명하였다. 이들 공격을 방지할 수 있고 전세계 모든 DNS 의 트렌드가 된 DNSSEC 이 무엇이며 어떻게 동작하는지 살펴보고, 이번 호에서는 DNSSEC 도입 진행사항과 활용할 수 있는 자료 그리고 다양한 툴들을 소개하였다.

이 글을 통해 DNSSEC 에 대해 관심을 가질 수 있는 개기가 되기를 기대한다.

[솔루션 문의]

☞오픈베이스 시스템사업본부 infrasales@openbase.co.kr