主題

인터넷대란과 대응방안

한국인터넷정보센터 원장 송 관 호

차 례

Ⅰ. 서 론

세계적인 규모와 품질의 초고속 통신 인프라를 기반으로 각종 인터넷 서비스는 비약적으로 성장하고 있으며, 세계 각 국의 기업들은 자사의 신기술에 대한 실험의 장으로 우리나라를 선택하고 있는 실정이다. 우리는 이미 정치, 문화, 사회, 경제 등 생활의 거의 모든 기반이 인터넷에 융합되는 현상을 경험하였으며, 이를 자연스럽게 받아들이고 있다. 전 국민의 64.1%가 인터넷을 이용하는, 인터넷이용자수 2천8백만명[1] 시대를 맞은 인터넷은 이젠 단순히 연결만 하면 알아서 작동하는 매체가 아니라 각종 위협과 장애로부터 세밀한 관리를 해줘야 할 중요 사회 기반시설로 자리를 잡았다.

이렇게 중요한 인프라에 대해 2003년도에 있었던, 최대사건은 바로 1월 25일 발생한 MS SQL 서버의 취약점을 이용한 '슬래머(Slammer) 웜'의 확산 이었다. 이 웜에 의해 우리나라 뿐 아니라 전 세계 인터넷 망이 영향을 받는 초유의 사태가 발생하였는데, 피해를 입은 국가중에서도, 한국은 그 피해가 다른 국가에 비해 상대적으로 크게 나타나 '정보통신 강국'이라는 이름에 오명을 남기게 되었다.

이에 본 고에서는 인터넷대란의 진행과정, 원인 등을 정리하고, 중요성이 부각되고 있는 인터넷 기반시설의 운영현황을 살펴본 뒤, 향후 이와 유사한 사고의 재발방지를 위해 주로 DNS (Domain Name System)의 측면에서 개선방안을 중점적으로 제시 하고자 한다.

Ⅱ. 인터넷 대란 개요

1. 인터넷대란 진행과정

2003년 1월 25일 14시경부터 국내 ISP (Internet Service Provider)업체의 국제 트래픽에서 이상현상이 발견되면서 인터넷 대란은 시작된

표 1. 인터넷대란 시간별 진행상황

1. 25일 14:10	- 미국, 호주 등을 통해 국내로 슬래머 웜이 유입된 것으로 추정 - 드림라인에서 최초로 트래픽 이상 징후 발견
1. 25일 14:35	- 국제회선 및 ISP의 주요 DNS서버, IDC내부망 과부하 현상 발생
1. 25일 15:30	- 정통부, 장애현상 인지 및 긴급대책반 구성
1. 25일 16:00	- KISA, MS-SQL관련 취약점을 이용한 공격으로 추정하고 각 ISP에 UDP 1433, 1434번 포트 차단을 권고 - 각 ISP는 15:40~17:00사이에 긴급조치를 실시하여 백본 라우터의 UDP 1433, 1434 포트를 차단
1. 25일 20:00	- 정통부와 KISA는 이번 장애의 원인을 "MS-SQL 슬래머웜"으로 확정하고, 메일링리스트(Sec-Info), 시큐어메신저, 홈페이지를 통해 대처방안 및 긴급경보를 발령(21:00)
1. 26일 14:30	- KT 및 하나로통신, 가입자 수용 라우터의 1433, 1434 포트차단
1. 26~27일	- KT, 구로 인터넷센터에 DNS 부하가 증가하여 DNS 수용구조를 지방으로 분산하고, 혜화 및 구로에 DNS 서버 17대를 증설 (혜화 : 12 → 27, 구로 : 3 → 5)

다. 채 한 시간도 되기 전에 국내 거의 모든 네트워크가 영향을 받게 되어 전체 인터넷이 느려지고, 급기야 인터넷 접속이 안 되는 사태에 이르게 된다. 정보통신부에서 구성한 합동조사반의 '정보통신망 침해사고 조사결과' 보고서[2]에 따르면, 당시 상황은 표 1. 과 같다.

2. 인터넷 대란 피해와 원인

1.25 대란은 "Microsoft SQL 서버 2000 및 MSDE 2000 시스템의 버퍼오버플로우 취약점"을 이용한 슬래머 웜이 네트워크를 공격한데서 비롯되었다. 2003년 1월 25일 오후 해외로부터 유입된 슬래머 웜은 크기가 약 404byte 정도의 패킷을 초당 1만 ~ 5만 개씩 대량 생성하여 전송하는 악성 프로그램으로 국내에 8천 8백여 시스템을 급속히 감염시킴으로서 네트워크 장애를 유발

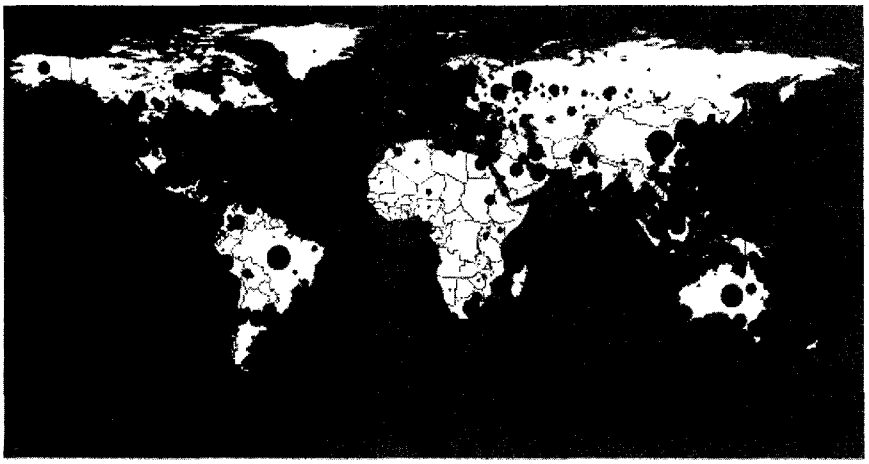


그림 1. 슬래머 웜 확산 30분간 감염분포

시켰다[2].

CAIDA(Cooperative Association for Internet Data Analysis)의 보고에 따르면, 1월 25일 출현한 웜에 의해 전세계의 취약점이 존재하는 Microsoft SQL 서버 2000의 90%가 10분이내에 감염이 되었으며, 국내에서는 전 세계 감염시스템(약 7만5천개)의 11.8%인 8천8백여개가 감염되어 일본의 약 7배, 중국의 약 2배에 달한다고 밝혔다[3].

슬래머 웜은 패킷의 크기가 매우 작아 서버의 성능 및 네트워크 환경에 따라 초당 약 1만~5만개의 UDP패킷을 생성하여 무작위로 생성된 목적지 IP주소로 보낼 수 있다[2].

감염된 서버는 다른 일을 하지 못하는 과부하가 발생하여 결과적으로는 서버에 대한 서비스거부(DoS, Denial of Service) 공격을 받은 것과 같은 결과를 초래하게 되며, 슬래머 웜은 취약점이 있는 서버뿐만이 아니라, 임의의 IP 주소를 선택하여 공격패킷을 보냄으로써 네트워크 과부하를 유발시키게 된다.

당시 슬래머 웜은 보안 취약점이 있는 윈도우 서버(Microsoft SQL서버 2000)를 감염시켜 해당 감염서버를 운영하는 대학, 연구소, 기업내 이용자의 인터넷 사용에 장애를 발생시켰고, 감염 서버는 다시 불특정 다수의 다른 컴퓨터를 공격함으로서, 네트워크 트래픽을 폭발적으로 증가시켜 감염 서버 주변의 이용자들도 인터넷 접근이 차단되는 결과를 초래하게 되었다[2].

또한, 감염된 서버가 있는 인터넷 사이트인 경우 서비스 제공이 불가능하여 접속경로에 장애가 없는 이용자들도 인터넷 서비스를 이용할 수 없는 상황이 발생하게 되었다. 특히, 정보통신시설이 집적되어 있는 IDC(Internet Data Center)에서 LAN(Local Area Network)으로 연결되어 있는 서버중의 하나가 감염된 경우 내부망 트래픽이 폭주하여 연결된 서버전체(포탈, 쇼핑몰, 게임 등)에 인터넷 접속장애가 발생하게 되었던 것이다[2].

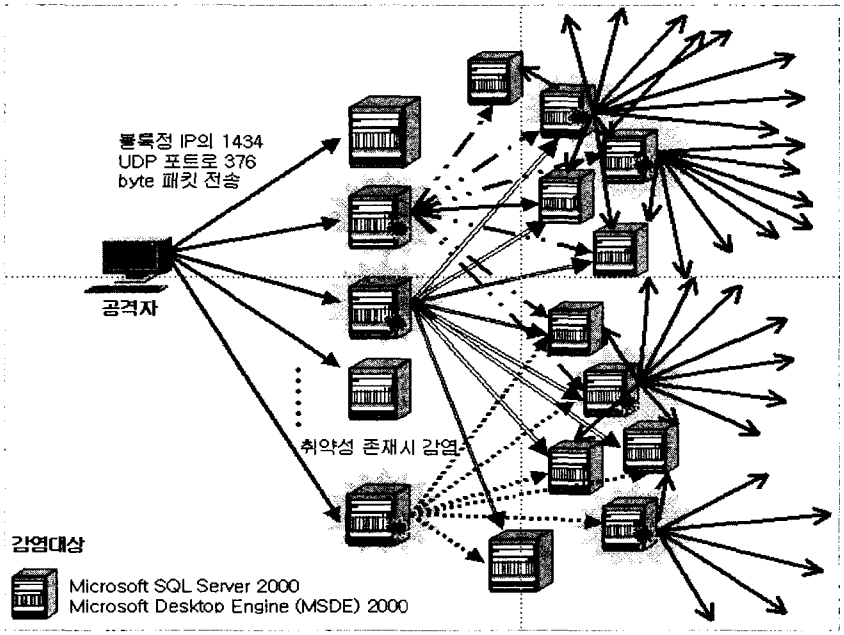


그림 2. 슬래머 웜의 확산 경로

이렇게 감염된 서버로부터 발생한 공격패킷의 목적지 IP주소는 임의로 부여되는데, 국제 인터넷 주소할당 분포상 확률적으로 93.2%의 패킷은 국제관문국에 집중되므로 각 ISP의 국제관문국에서 심한 병목현상이 발생하여 해외 인터넷 사이트 및 해외 Root DNS에 접속할 수 없었고, Root DNS 접속 재시도를 하는 과정에서 각 ISP들의 DNS에 과부하가 발생하여 국내 인터넷 소통에도 지장을 초래하였다[2].

.KR 과 같은 국가 최상위 도메인(ccTLD: Country Code Top Level Domain)은 국내에 DNS서버가 있어, 국제 관문국이 막혔던 상황에서도 정상적인 서비스가 가능했던 반면, .COM, .NET과 같은 일반 최상위 도메인(gTLD : Generic Top Level Domain)은 국제관문국 병목현상으로 인해 외국의 DNS서버와 제대로 통신을 할 수 없어, 인터넷 이용자들이 해당 도메인 네임을 가진 사이트에 접근할 수가 없었다.

Ⅲ. 인터넷 기반시설의 이해

1. 인터넷 기반시설과 DNS

인터넷 기반시설이라고 하면, 통신의 근간이 될 수 있는 라우터와 DNS서버가 반드시 포함된다. 통신의 근간이기 때문에, 라우터나, DNS서버가 장애를 일으킨다면, 네트워크가 지연되거나 아예 단절될 수 도 있기 때문이다. 이러한 인터넷 기반시설 중 최근 공격대상으로 가장 주목을 받는 것은 바로 DNS이다. 비교적 단순한 구조의 통신 프로토콜을 사용해서, 공격시 난이도가 낮고, 공격에 성공 했을 때는 그 파급효과가 매우 크기 때문이다.

정보통신부의 조사결과도 인터넷대란의 간접적인 원인으로 DNS서버의 과부하에 따른 서비스 장애를 들었다. DNS가 직접 공격을 받은 것은 아니었으나, 국제 관문국의 정체에 의한 재질의의 증가로 DNS서버의 CPU에 과부하가 발생해 이용자들의 요청을 제때 처리해주지 못한 것이다[2].

DNS(Domain Name System)는 일반 인터넷 이용자가 쉽게 이해하는 도메인 이름을 호스트의 통신기반인 IP(Internet Protocol)주소로 변환해 주는 인터넷 응용체계 이다. DNS는 호스트 정보의 분산 데이터베이스로 아래와 같은 계층적인 구조로 구성되어 최상위의 루트(root) DNS 서버는 그 하위의 gTLD(Generic Top Level Domain: .com, .net 등), ccTLD(Country Code Top Level Domain: .kr, .jp 등) 등의 DNS서버 정보를 보유

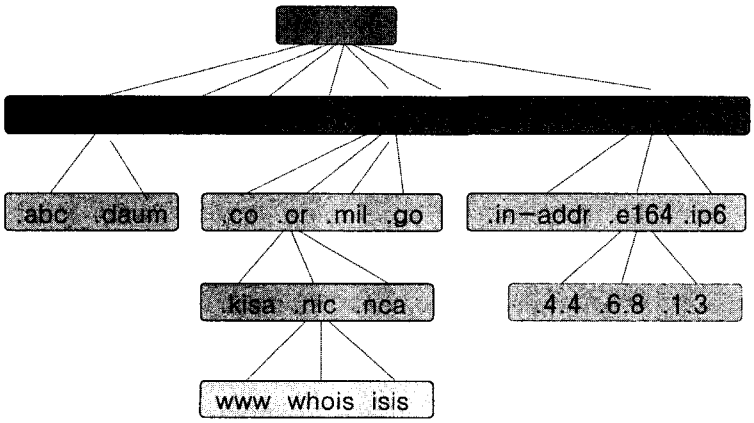


그림 3. DNS 운영 계층구조

하고 있다[6].

그리고 DNS는 캐싱(caching)을 이용해 이미 질의된 내용을 메모리에 기억하는데, 이를 통해, 대량으로 들어오는 동일한 질의를 빠르게 처리함으로서 DNS서버의 처리성능을 향상시킨다. 이는 매우 중요한 기능으로, 그림 4. 와 그림 5.를 살펴보면, 캐싱이 되었을 때와 그렇지 않을 때의 질의과정의 차이점을 명백히 알 수 있다. 이러한 과정에 따라 이용자는 DNS서버를 통해 도메인 네임을 IP주소로 변환할 수 있다.

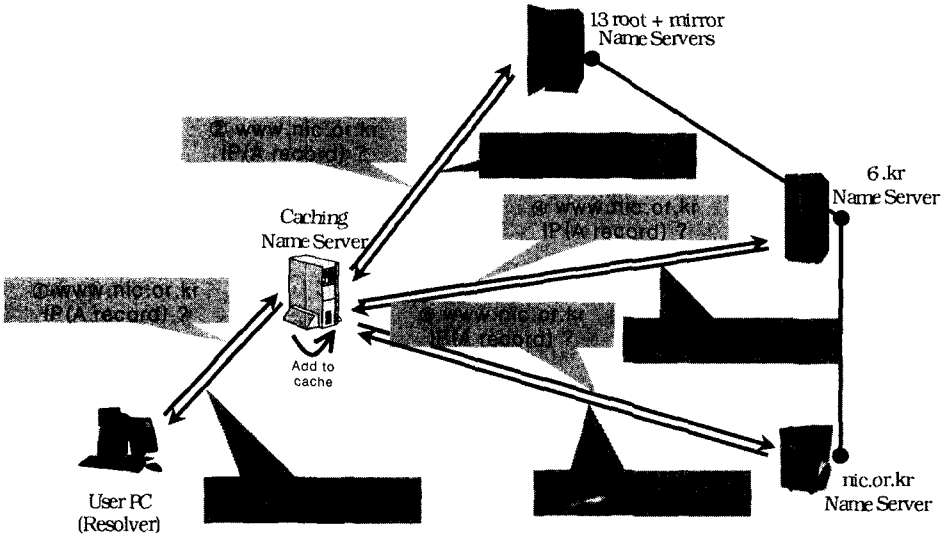


그림 4. DNS 서비스체계도(Cache 정보가 없는 경우)

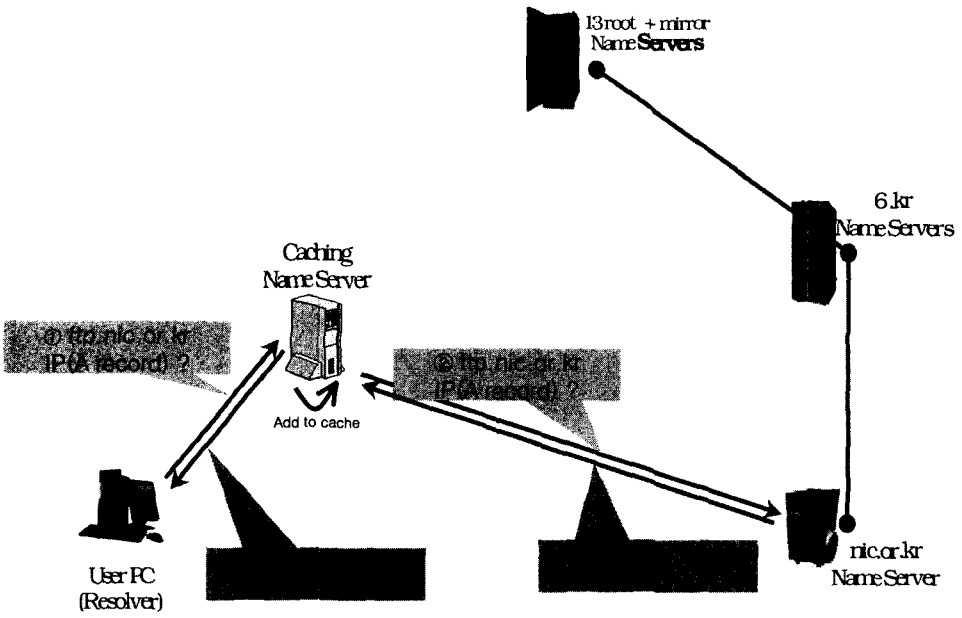


그림 5. DNS 서비스체계도(Cache 정보가 있는 경우)

표 2. 최근 1년간 발생한 DNS에 대한 대표적인 공격 및 장애 내역

사건종류	일시	피해대상	파급효과
루트DNS서버 서비스거부공격	2002.10.21	전세계13개 루트DNS서버	1시간사이 약 2대에서 접속지연 발생
1.25 인터넷 대란	2003.01.25	전국 DNS서버	DNS 처리불가
미국 동부 정전에 의한 네트워크 순간지연	2003.08.14	미국내 루트DNS서버	사고당일 미국내 일부 루트DNS서버에 접속지연 발생 (정전으로 인한 접근경로상의 네트워크 장애로 추정)

2. 기반시설에 대한 위협

과거와는 달리, 호스트 및 네트워크에 접근제어 등 어느 정도 기본적인 보안장치가 되어있어 단일 자원에 대한 공격이 쉽지 않고, 성공하더라도 파급효과가 미비하여, 상대적으로 공격이 쉽고, 그 파급효과가 큰 인터넷 기반시설에 대한 공격이 성행하고 있다.

최근 1년 사이 인터넷 기반시설에 대한 공격 및 장애 관련 사건을 봤을 때, 이는 더욱 분명해진다[5].

표 2. 와 같이 최근 1년 사이 직·간접적으로 최상위 DNS에 3건의 공격이 있었으며, 앞으로도 이러한 추세는 계속될 것으로 예상된다.

Ⅳ. 대응방안

인터넷 대란과 같은 사고를 극복하기 위한 방안으론, 중앙에서 보안기술과 관리체계를 총동원하여 대응하는 방안과 DNS와 같은 인터넷 기반시설을 안정화 시키는 방안이 있다. 본 고에서는 이를 차례대로 살펴보고, 특히 DNS위주로 인터넷 기반을 안정화 시켜 대응하는 방안을 중점적으로 제시하고자 한다.

1. 보안기술 및 관리체계의 통합

수 분 안에 국가 인터넷망을 마비시킬 정도로 강력한 웜은 앞으로도 얼마든지 출현 가능하다는 것이 인터넷대란을 통해 증명되었다. 그렇다면, 과연 이토록 강력한 웜에 대한 대처가 현재 기술수준에서 가능할 것인가? 이 문제를 풀려면 기술과 관리의 두 가지 측면을 동시에 고려해 보아야 한다.

우선 기술적 측면에서는 알려진 특정 공격 패턴만 모니터링 하는 방법에서 벗어나, 네트워크 전체에서 발생하고 있는 이상현상을 파악하는 방법으로의 확대가 필요하다. 이상현상에 대한 모니터링은 기존에 알려지지 않은 공격이 시도되더라도 이를 공격시도로 인지하고, 빠른 대응을 가능케 해주는 장점이 있는 반면, 통계론적 방법이 지나치게 적용되어 오탐지 횟수가 증가하는 단점이 있다. 물론 오탐지를 줄이기 위해 제한된 이상현상만 모니터링 하겠다면, 이번에는 공격탐지 확률이 저하될 수 있다.

기술적으로 어느 정도 자동화된 모니터링이 가능하나, 예전과는 달리 초고속인터넷의 발전과 인터넷 서비스의 다양화로 인해, 정상상태인 네트워크에서도 이상현상으로 보이는 트래픽이 계속적으로 모니터링 될 수 있다. 알려지지 않은 해킹에 대한 탐지를 완전히 자동화 시키기는 현재상태에서 매우 어렵다. 그래서, 관리적 측면에서 이에 대한 보완책을 찾아야 한다.

표 3. DNS 운영시 권고사항

DNS 운영시 권고사항	기대 효과
내부용 캐시(cache) DNS 서버와 자사 도메인을 서비스하는 DNS서버는 분리운영	처리량이 많은 내부 캐시DNS서버를 분리하여 보안성과 안정성 강화
원격지에 2차 DNS서버의 운영	기관내 DNS서버에 장애 발생시 연속적인 서비스 가능
DNS 서버의 정기적인 정검(H/W, S/W)	DNS프로그램의 정기적인 업그레이드를 통해 보안성과 성능 향상

관리적 측면에서 대응을 하면, 기술적 부분에서 발생하는 탐지시의 다양한 오류를 축적된 모니터링 경험과 다양한 분야 전문가들의 의견조율을 통해 극복할 수 있으며, 대응에 있어서도 단편적이고 협소한 조치를 벗어나, 보다 근복적이고 광범위한 조치가 가능하다.

적절한 기술, 장비, 이를 다룰 전문인력, 모든 자원이 위치할 동일한 물리적 공간, 그리고 운영 및 대응체계가 확보되어야 하고, 경우에 따라서는 어느 정도의 권한도 주어져야 한다.

이렇듯, 인터넷 기반시설을 안전하게 운영하기 위한 필수요소는 기술뿐 아니라 적절한 대응이 가능한 관리체계라는 것은 중요한 사실이다. 기술이 아무리 뛰어나더라도, 수 분 내에 네트워크를 포화시키는 신종 웜에는 어느 정도 피해를 입을 수밖에 없으며, 그렇다면 피해 발생시 대응 및 피해확산 방지를 위한 체계가 준비되어 있어야 한다.

2. 기관의 DNS서버 운영 관리

기관이나 일반기업체에 있어 DNS관리의 중요성은 평시에는 쉽게 간과되는 사항이다. 하지만 상위의 DNS서버뿐만 아니라, 하위의 DNS서버들도 평소대비를 통해 인터넷대란과 같은 사태를 예방하는데 기여할 수 있다.

이미 기업내의 수많은 호스트, 네트워크 장비들은 관리의 효용성을 높이기 위해 직·간접적으로 도메인네임과 연결되어 있는데, DNS에서 문제가 생기기 시작하면, 잘 동작되던 호스트들이 서로를 찾기 위해 혼란에 빠지게 된다. 결국엔 간단한 이메일 한통 보낼 수 없게 되어서야 문제의 심각성을 알게 되는 것이다.

1.25대란은 슬래머 웜이 DNS를 직접 공격한 것이 아니라, 단순히 전체적인 네트워크 트래픽을 증가시켜 사방에 병목구간을 만들고, 이런 병목구간이 DNS트래픽의 정상적인 처리를 방해했다는 것이 현재까지의 공식적인 의견이다.

병목 구간이 늘어감에 따라 패킷 재전송 횟수와 이를 처리해야하는 호스트들의 부하는 자연스럽게 증가해 간다. 그리고 DNS질의는 평소에는 간과하기 쉬울 정도로 작은 양이지만 모든 응용프로그램의 통신에서 기본적으로 발생하기 때문에, 한꺼번에 요청이 몰릴 때에는 실로 위력적이라 할 수 있다.

따라서, 이런 상황에 대처하기 위해서는 위기상황을 고려한 표 3. 과 같은 노력이 있어야 한다.

첫째, 사내의 직원들이 이용하는 캐시(cache) DNS서버와 회사의 도메인이름을 서비스하는 DNS서버는 분리하는 것을 권고한다. 그리고 동시에 사내의 캐시DNS서버는 사내에서 발생하는 DNS 트래픽만 처리해야 하

고, 외부로부터 오는 요청은 보안상 차단하는 것이 좋다.

둘째, 원격지에 2차 DNS서버의 운영해야 한다. 사외의 원격지에 현 DNS서버와 똑같은 내용의 2차 DNS서버를 운영하면, 평소에는 DNS 부하분산이 가능하고, 사내 전산망 작업시나 사내 DNS장애시에는 백업 기능을 수행하여 연속적인 서비스가 가능하다.

마지막으로, DNS서버의 정기적인 점검이 중요하다. DNS서버는 한번 제대로 작동하면, 관리자조차 그 중요성을 간과하여 문제가 생기기 전까지는 방치되는 경우가 있는데, 이는 바람직하지 않다. 정기적으로 DNS 프로그램을 최신버전으로 업그레이드 해주고, 하드웨어를 점검함으로서, 꾸준히 전체 네트워크의 안정성을 유지할 수 있다.

3. 주요 DNS서버의 유치 및 운영개선

인터넷 대란 때문이 아니더라도 꼭 선행되어야 할 과제는 바로 전 세계 주요(gTLD, ccTLD) DNS서버의 국내 유치이다. 현재는 미국이 인터넷 기술, 이용자수 등에서 우세하지만, 전 세계인이 사용하는 인터넷이 된 이상 언제까지나 과거의 논리만을 내세울 수 없을 것이다. 인터넷 이용자 2천8백만명을 자랑하는 우리나라가 이미 규모와 관련 문화면에서 아태지역을 선도하고 있고, 향후 아사아권의 성장 잠재력을 보았을 때, 인터넷의 중심이 세계로 분산되어야 할 때가 온 것이다. 한국인터넷정보센터가 추진중인 주요 DNS서버의 유치 및 운영개선 내용은 다음과 같이 세 가지로 요약된다.

첫째, 루트DNS서버의 국내 유치가 필요하다. 인터넷 초창기부터 최근까지 인터넷의 핵심 기반시설인 최상위의 루트 DNS서버는 표 5. 와 같이 전 세계에 13개가 운영중이며, 그중 10개가 미국에, 2개가 유럽에, 1개가 일본에 위치하고 있다. DNS 이용자는 자신의 위치에서 가장 가까운 DNS서버를 찾아가므로, 이러한 핵심자원이 국내망에 설치될 수 있다면, 국내 이용자들의 인터넷 이용환경 개선과 예기치 못한 사고에 좀더 유연하게 대처할 수 있는 체계를 갖출 수 있게 될 것이다[4,7].

이러한 이유로, 이미 2003년 8월 국내에는 처음으로 최상위 루트DNS서버 중 하나인 'F 루트 DNS'서버(mirror)를 국내의 한국인터넷정보센터내에 유치하여, 국가 인터넷 기반의 안정성 향상에 기여하고, 향후 또 다른 중요 기반시설의 추가도입 가능성을 높이는 계기를 마련하였다.

둘째, 루트 DNS서버 뿐만 아니라, 국내 이용자들의 사용빈도가 높은 DNS서버도 국내유치가 필요하다. 그래서 2004년도에 국내 유치예정인 COM, NET 도메인을 관리하는 gTLD DNS서버까지 유치된다면, 우리나라는 인터넷 대란 1년여 만에 국내 사용빈도가 높은 .KR, .COM,

표 4. 유치 및 운영개선 대상

유치 및 운영개선 대상	내용
루트DNS서버의 국내유치	F 루트 DNS서버(mirror)의 국내유치(03년 완료)
gTLD(COM, NET) DNS서버의 국내유치	13대 gTLD(COM, NET) DNS서버중 1대 국내유치(04년 예정)
.KR 2차 DNS서버의 운영 개선	현재 5대인 .KR 2차 DNS서버의 수를 늘리고, 지역적 분산을 고려해 전국에 고루 설치

.NET 도메인네임을 모두 국내에서 처리하게 된다. 향후 또 다시 국제 관문국 병목현상이 나타나더라도, DNS 트래픽은 국외로 나갈 필요 없이 국내에서 모두 처리가 가능하기 때문에, 최악의 경우라도, 국내 사이트는 자유롭게 사용할 수 있을 것으로 기대한다.

셋째, .KR 도메인의 안정성을 높이기 위해 .KR 2차 DNS서버의 운영체계 개선이 필요하다. 현재는 우리나라와 미국에 총 5대의 .KR 2차 DNS서버가 각각 분산되어 운영중인데, .KR 도메인의 성장과 향후 각종 DNS관련 응용서비스(한글도메인, ENUM, DNSSEC 등)의 적용을 고려해 서버 시스템의 성능 개선과 운영대수를 늘려 보다 세밀한 분산배치가 필요한 시점이다.

표 5. 전세계 루트DNS서버 운영현황

서버명	IP주소	기관명	위 치
A	198.41.0.4	VeriSign Global Registry Services	Dulles, VA, USA
B	128.9.0.107	Information Sciences Institute	Marina del Rey, CA, USA
C	192.33.4.12	Cogent Communications	Herndon, VA, USA
D	128.8.10.90	University of Maryland	College Park, MD, USA
E	192.203.230.10	NASA Ames Research Center	Mountain View CA, USA
F	192.5.5.241	Internet Software Consortium	Palo Alto, CA, USA
G	192.112.36.4	U.S. DOD Network Information Center	Vienna, VA, USA
H	128.63.2.53	U.S. Army Research Lab	Aberdeen, MD, USA
I	192.36.148.17	Autonomica	Stockholm, Sweden
J	192.58.128.30	VeriSign Global Registry Services	Dulles, VA, USA
K	193.0.14.129	Reseaux IP Europeens - Network Coordination Centre	London, United Kingdom
L	198.32.64.12	Internet Corporation for Assigned Names and Numbers	Los Angeles, CA, USA
M	202.12.27.33	WIDE Project	Tokyo, Japan

표 6. 전세계 gTLD(generic Top Levl Domain: COM, NET) DNS서버 운영 현황

서버명	IP주소	기관명	위 치
A	192.5.6.30	VeriSign	Herndon, VA
B	192.33.14.30	VeriSign	Mountain View, CA
C	192.26.92.30	VeriSign	Dulles, VA
D	192.31.80.30	VeriSign	Sterling, CA
E	192.12.94.30	VeriSign	Los Angeles, CA
F	192.35.51.30	VeriSign	Seattle, CA
G	192.42.93.30	VeriSign	Mountain View, CA
H	192.54.112.30	VeriSign	Amsterdam, Netherlands
I	192.43.172.30	VeriSign	Stockholm, Sweden
J	192.48.79.30	VeriSign	Tokyo, Japan
K	192.52.178.30	VeriSign	London, United Kingdom
L	192.41.162.30	VeriSign	Atlanta, GA
M	192.55.83.30	VeriSign	Hong Kong, China

V. 결론

이상에서 인터넷 대란의 개요, 인터넷 기반시설의 및 DNS의 의미, 그리고 대응방안에 관해 종합적으로 기술하였다.

2003년 초의 화두였던 인터넷대란은 인터넷 의존도가 높은 상태에서 처음으로 국가적 차원에서 겪은 최대의 인터넷 위기라고 할 수 있다. 이 사건을 계기로, 정부주도의 다양한 재발방지 및 피해발생을 최소화 시키는 대응책이 급속도로 논의됐고, 정부, 학계, 업계 등 다양한 분야에서 여러 공감대도 형성될 수 있었다. 뿐만 아니라, 정보통신부 및 국가 정보기관 등에서는 국내 인터넷 침해사고를 감시하고, 대응하기 위한 대응센터를 동시에 준비하는 등 발빠른 대응을 보였다[8].

이러한 모든 노력들이 향후 신종 웜의 등장시 파급효과를 줄여주고, 상황에 효과적으로 대처할 수 있게 하여, 제 2의 인터넷대란을 예방해 주는 역할을 할 것이다.

특히 본 고에서 다룬 인터넷 기반시설(특히 DNS)의 안정적인 운영은 제2, 제3의 인터넷 대란이나 유사한 사고의 발생으로 피해가 발생 하더라도 최소한 국내 인터넷 이용자들에게는 안정적인 인터넷 서비스를 제공하는데 기여할 것이다.

참고문헌

[1]인터넷통계정보검색시스템, http://isis.nic.or.kr, 한국인터넷정보센터

[2] 정보통신망 침해사고 합동조사반, "정보통신망 침해사고 조사결과", 정보통신부, 2003. 2

[3] CAIDA, http://www.caida.org

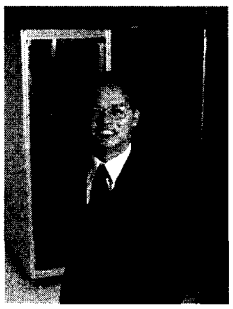
[4] 송관호, "'루트 DNS 미러 사이트' 도입 의미와 과제", 전자신문, 2003. 5

[5] 김원, "PKI 이용 DNS 보안", 전자신문, 2003. 3

[6] Paul Albitz & Cricket Liu, "DNS and BIND", 4th Ed., O'Reilly, 2001

[7] Milton L. Mueller, "Ruling the Root: Internet Governance and the Taming of Cyberspace", MIT Press, 2002. 5

[8] 디지털타임스, "국가 사이버테러 대응체계 가동", 2003.12



송 관 호

1980년 : 서울대학교 공과대학 전자공학과(공학사)
1984년 : 한양대학교 산업대학원 전자공학과(공학석사)
1995년 : 광운대학교 대학원 전자통신공학과(공학박사)
1997년 : 서울대학교 행정대학원 정보통신정책과 수료
1979년 ~ 1985년 : LG전선 정보시스템 과장
1985년 ~ 1987년 : 데이콤 미래연구실장
1987년 ~ 1995년 : 한국전산원 초고속국가망구축실장(연구위원)
1995년 ~ 1997년 : 숭실대학교 정보과학대학원 겸임교수
1996년 ~ 1997년 : 한국전산원 표준본부 본부장
1998년 ~ 1999년 : Visiting Professor University of Maryland
1999년 : 한국전산원 국가정보화센터 단장, 건국대학교 정보통신대학원 겸임교수
1999년 ~ 현재 : 한국인터넷정보센터 원장

<주관심분야> 인터넷응용, 초고속인터넷, 멀티미디어통신