초고속연구망 침해사고 현황 및 대응 방안

글 _ **이정원** | 초고속연구망사업실 초청연구원 | jwl22@kisti.re.kr
권윤주 | 초고속연구망개발실 연구원 | yulli@kisti.re.kr

1. 서 론

인터넷을 통한 전자상거래, 온라인 뱅킹 등 여러 분야에 걸쳐 그 이용이 급증하고 있는 가운데 불법적인 해킹을 통한 중요 정보의 유출, 웜 바이러스, 분산 서비스 거부 공격(DDoS - Distributed Denial of Service) 등으로 인한 시스템 및 네트워크의 장애 사례도 급증하고 있는 추세에 있다.

이에 국내 주요 연구 인력들에게 초고속 R&D(Research and Development) 네트워크를 제공하는 한국과학기술정보연구원(KISTI)은 초고속연구망(KREONET)에서 발생할 수 있는 각종 침해사고를 예방하고, 침해사고 발생시 빠른 대응을 지원하기 위해 초고속연구망 정보보호팀 즉, CERT-KREONET(Computer Emergence Response Team for KREONET)을 구축하여 운영하고 있다.

또한 초고속연구망개발실에서는 급격히 발전하고 있는 각종 공격 기법에 대한 효과적인 대응을 위해 네트워크 차원의 모니터링 및 대응시스템을 연구·개발하여 초고속연구망에 적용함으로써 보다 안전하고 안정적인 네트워크 서비스가 가능하도록 노력하고 있다.

이에 따라 CERT-KREONET을 통해 2003년 처리되었던 침해사고 현황을 살펴보고, 이에 효과적으로 대응하기 위해 개발되고 있는 NetWRAP(NetWork Resource Abuse Preventive) 시스템을 설명하도록 한다.

2. 초고속연구망 침해사고 현황

1) 침해사고 유형

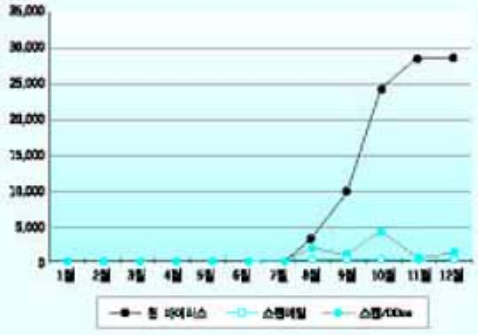
2003년 초고속연구망을 통해 발생한 침해사고 현황을 살펴보면, 국내 약 5천여개 기관과 관련하여 약 10만여 건의 침해사고 발생하였으며, 이들은 크게 웜 바이러스, 스캔(Scan) 및 분산 서비스 거부 공격, 스팸메일로 분류할 수 있다.

웜 바이러스는 Bluster, Nachi(Welchia) 등과 같은 인터넷 웜, Kuang2/3, Subseven과 같은 트로이목마 등이 이에 포함되며 초고속연구망을 통해 발생한 침해사고의 대부분을 차지하고 있다.

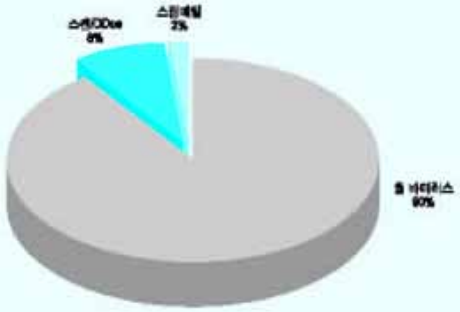
스캔 및 분산 서비스 거부 공격은 특정 IP에 해당하는 시스템이 존재하는지를 확인하기 위한 핑 스캔(Ping Scan)과 텔넷, FTP 등과 같은 특정 서비스가 제공되는지를 확인하기 위한 포트 스캔(Port Scan), 그리고 특정 서비스 및 시스템을 마비시켜 서비스를 제공하지 못하도록 하는 분산 서비스 거부 공격(DDoS -

Distribute Denial of Service) 등이 포함된다.

마지막으로 스팸메일은 상업적인 광고 메일인 스팸메일 발송과 메일 릴레이(relay) 허용으로 인한 스팸릴레이가 이에 포함된다.



〈그림 1〉 월별 침해사고 발생 추이



〈그림 2〉 유형별 침해사고 발생 비율

초고속연구망에서 발생하는 침해사고의 대부분은 웜 바이러스와 스캔 및 분산 서비스 거부 공격으로 이들 모두는 네트워크의 안정적인 서비스 제공에 있어 가장 위협적인 존재라 할 수 있다. 이에 따라 초고속연구망에 가장 큰 피해를 줄 수 있는 웜 바이러스와 스캔 및 분산 서비스 거부 공격의 특징과 그 영향을 살펴본다.

2) 침해사고 분석 및 영향

가. 웜 바이러스

웜 바이러스는 초고속연구망을 통해 가장 빈번히 발생하는 침해사고로 2003년 한 해 동안 발생한 침해사고만도 약 9천 4백여 건에 이른다. 2003년 한 해 동안 초고속연구망에서 가장 많은 침해사고를 유발시켰던 웜 바이러스의 종류를 살펴보면 〈표 1〉과 같다.

〈표 1〉 웜 바이러스 특징 (Top 5)

순 위	바이러스명	특 징	비 율
1	Nachi (Welchia)	• 인터넷 웜 • ICMP 패킷을 전송하면서 살아있는 시스템을 찾고 RPC 취약점을 이용하여 공격 시도 • TCP 707 포트 오픈	43%
2	Bugbear	• 인터넷 웜(백도어 기능 포함) • 메일과 네트워크 공유(암호가 설정되지 않은 공유)를 통해 전파됨 • TCP 1080 포트 오픈	13%
3	Blaster	• 인터넷 웜(백도어 기능 포함) • RPC 취약점을 이용하여 공격을 시도하며, 전파를 위한 135번 포트를 스캔 • TCP 4444 포트오픈, tftp를 통한 웜 파일 다운로드	10%
4	Nimda	• 바이러스 • 메일과 네트워크 공유를 통해 전파 • 모든 드라이브를 공유시키고 IIS(Internet Information Services)를 감염시킨 후 전파	8%
5	Lioten	• 인터넷 웜 • TCP 445 포트로 알기 쉬운 암호로 설정된 관리목적의 공유폴더를 공격	7%

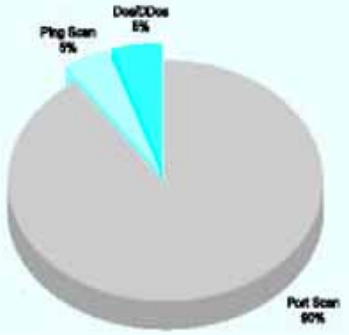
초고속연구망에서 주로 발생하는 웜 바이러스의 특징을 살펴보면 다음과 같다.

첫째, 대부분의 웜 바이러스가 MS 윈도우 운영체제를 대상으로 하고, 네트워크를 통해 급격히 전파되는 특성을 지닌다. 즉, 최신의 웜 바이러스는 각종 해킹 기법이 접목되어 네트워크를 통해 자동으로 보안 취약점이 있는 시스템을 스캔하고, 그 시스템을 감염시키는 것이다. 이러한 웜 바이러스의 피해는 어느 특정 시스템이 바이러스에 감염되는 것에 그치지 않고, 감염된 다수의 시스템들에 의한 취약점 스캔 및 공격으로 대량의 트래픽이 발생함으로 인해 네트워크 및 네트워크 보안장비를 마비시킬 수 있다는 것이다. 실제 2003년 8월에 발생한 Nachi 웜의 경우 살아있는 시스템을 찾기 위해 대량의 ICMP 패킷을 전송하여 네트워크에 과부하를 줌으로써 사용자들의 인터넷 사용을 방해하고, 심지어 네트워크 장비 및 방화벽(Firewall) 등을 마비시키는 결과를 낳았다.

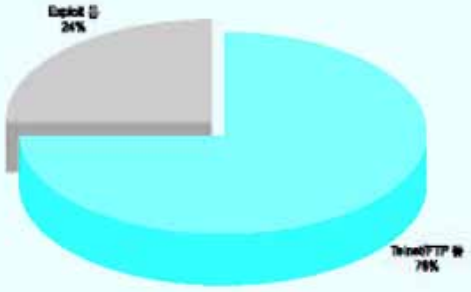
둘째, 웜 바이러스의 또 다른 특징은 Bugbear와 Blaster 웜과 같이 백도어(Backdoor) 기능을 포함한다는 것이다. 백도어란 해커나 해킹을 하고 나서 추후 그 사이트를 재침투하기 위해 만들어 두는 뒷구멍을 말하는데, 이러한 백도어를 이용하여 파일을 삭제하거나 특정 프로그램을 실행하고, 개인 정보를 유출하는 등의 피해가 야기될 수 있다. 또한 최근에는 Blaster 웜과 같이 감염된 PC의 백도어를 통해 대량의 스팸메일을 발송하는 경우가 급격히 증가하고 있다. 이러한 스팸메일 발송은 릴레이가 허용된 메일서버를 이용하는 것보다 한 번에 더 많은 양의 스팸메일을 보낼 수 있어 네트워크 트래픽이 급격히 증가한다. 또한 백도어를 이용한 스팸메일 발송의 경우 일일이 IP를 추적하기 어렵기 때문에 스팸메일을 막기가 훨씬 힘들어진다.

나. 스캔 및 분산 서비스 거부 공격

스캔 및 분산 서비스 거부 공격은 웜 바이러스 다음으로 초고속연구망에서 가장 빈번히 발생하는 침해사고로 약 7천 7백여 건에 이르며, 각 유형별 현황은 〈그림 3〉, 〈그림 4〉와 같다.



〈그림 3〉 스캔 및 분산 서비스 거부 공격 비율



〈그림 4〉 주요 포트 스캔 대상

초고속연구망에서 발생하고 있는 웜 바이러스의 특징을 살펴보면, 특정 서비스의 제공 유무를 탐지하기 위한 포트 스캔이 대부분을 차지하고 있다. 포트 스캔은 텔넷, FTP 등과 같은 일반 서비스의 유무를 탐지하는 경우와 THCunREAL,remote.exploit, Netbus 등과 같은 해킹 도구에 의한 탐지로 나눌 수 있다. 핑 스캔은 Ping 명령(ICMP)을 이용하여 특정 IP 대역에서 살아있는 시스템을 확인하는 것으로 특정 시스템을 공격하기 이전에 해당 시스템이 동작하고 있는지를 확인하기 위해 사용된다.

이러한 스캔들은 특정 시스템을 해킹하기 위한 사전작업인 경우가 많으므로 주의를 기울여야 한다. 예를 들어 Ping Scan을 통해 특정 시스템이 살아있는지를 확인하고, Port Scan을 통해 어떠한 서비스를 제공하고 있는지를 확인하여, 이를 통해 보안 취약점이 드러난 시스템 및 서비스를 확인하여 공격을 시도하는 것이다.

분산 서비스 거부 공격은 많은 수의 호스트들에 패킷을 보낼 수 있는 서비스 거부 공격(DoS)용 프로그램들이 분산 설치되어 이들이 서로 통합된 형태로 어느 목표 시스템 및 네트워크에 대하여 일제히 데이터 패킷을 전송시켜 그 시스템 및 네트워크의 성능저하 및 시스템 마비를 일으키는 공격을 말한다. 이러한 분산 서비스 거부 공격은 비교적 낮은 비율을 차지하고 있으나, 분산 서비스 거부 공격이 성공할 경우 그 피해는 다른 어떠한 공격유형보다 강력할 수 있다. 특히, 최근에는 대고객 서비스를 운영하고 있는 웹 서버, DNS 서버 등과 같은 운영 서버들을 공격하는 형태에서 라우터, 방화벽 등과 같은 네트워크 인프라를 완전히 마비시키는 형태로 발전해 가고 있어 각별한 주의가 요구된다.

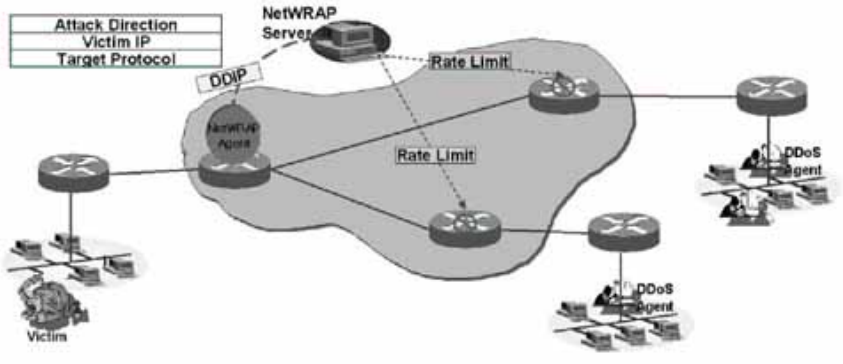
이러한 웜 바이러스나 스캔/DDoS로 인한 피해를 최소화하기 위해서는 빠른 탐지와 치료가 가장 중요하다. 따라서 초고속연구망에서 발생하는 침해사고를 실시간으로 탐지하고, 이를 즉시 대응이 가능하도록 하는 NetWRAP을 개발하여 적용하고 있다.

3. NetWRAP 시스템 개발

초고속연구망의 침해사고가 빈번히 발생함에 따라 네트워크 차원에서 침해사고를 대응을 할 수 있는 기술 개발 필요성이 증대되고 있다. 보안 뉴스 또는 IDS와 같은 보안 장비를 통해 침해사고를 일으키는 포트 또는 시스템 주소를 알게 되면, 라우터 설정과 같은 수동적인 대응을 하기도 하지만 이는 분산 서비스 거부 공격이나 웜 바이러스와 같은 공격 패킷의 전파를 막기에는 부족한 면이 있다. 이에 따라 초고속연구망에서는 분산 서비스 거부 공격이나 웜 바이러스와 같이 대량의 트래픽을 발생시키는 공격을 자동으로 탐지하고, 자동으로 공격 트래픽을 제어할 수 있는 시스템을 개발하고 있다. 네트워크 자원 오남용 트래픽 자동 탐지 및 대응 시스템의 이름은 NetWRAP(NetWork Resource Abuse Preventive) 시스템으로 '네트워크의 자원이 오남용 되는 것을 방지한다' 라는 뜻을 가지고 있다.

이 시스템은 하나의 ISP(Internet Service Provider) 기반에서 네트워크 오남용사건에 대하여 대응하며, 플로우(flow) 기반의 탐지를 하고, 네트워크 오남용 트래픽 발생지를 찾아 최하단의 라우터에 트래픽 제어 명령을 적용하도록 설계되어 있다.

1) NetWRAP Overview



〈그림 5〉 NetWRAP 시스템 동작 예

NetWRAP 시스템은 서버-에이전트 모델로서, 한 라우터에 대하여 트래픽 정보를 수집하고 분석하는 에이전트와 이들 에이전트에서 탐지한 정보를 이용하여 대응하는 서버로 구성되어 있다. 한 도메인에서 서버는 다

수의 에이전트를 이용하여 해당 도메인의 네트워크에서 발생되는 네트워크 남용 사건을 통보 받고, 그 정보를 이용하여 네트워크 자원이 남용되고 있는 패스의 라우터들에 적절한 트래픽 제어 명령을 적용함으로써 네트워크 자원 남용을 방지한다.

가. 탐지 방식

네트워크 자원 남용 이벤트를 탐지하기 위해서는 네트워크 트래픽에 대한 정보가 필요하다. 라우터에서 생성되는 'Netflow'라는 정보는 해당 네트워크의 트래픽 흐름을 파악하는 데 유용한 정보로서, 트래픽 측정 시스템에서 많이 사용되고 있는 자료이다.

탐지를 담당하는 NetWRAP 에이전트는 이러한 Netflow 자료를 이용하여 현재 네트워크의 흐름이 기존의 네트워크 흐름과 비교하여 정상적인지, 비정상적인지를 판단하고, 비정상적이라면 비정상적인 트래픽이 발생되거나 또는 목적되는 시스템이나 네트워크를 찾아내어 대응시스템인 NetWRAP 서버에 통지한다.

나. 대응 방식

NetWRAP 시스템은 NetWRAP 서버를 통하여 네트워크에 흐르는 공격 트래픽에 대해서 네트워크 자원을 보호할 수 있도록 대응을 한다. 그러한 공격에 대응하기 위해서 NetWRAP 서버는 다음과 같이 두 가지의 기능을 한다.

첫째는 자신의 네트워크에 있는 라우터마다 방문을 하여 어느 라우터에서 공격 트래픽을 유입시키고 있는지를 검사한 후, 공격 트래픽을 유입시키는 초입라우터를 찾아내는 것이다. 이를 위해 NetWRAP 서버는 기본적으로 해당 네트워크의 토폴로지를 가지고 있으며, 그 토폴로지 안에 있는 모든 라우터들은 Netflow 기능이 활성화 되어 있어야 한다. 라우터에 Netflow 기능을 활성화시켜두면 해당 라우터를 지나간 트래픽에 대한 정보를 저장해두게 된다. NetWRAP 서버는 네트워크 토폴로지와 캐쉬되어 있는 Netflow 정보를 이용하여 해당 네트워크의 경계 라우터까지 공격 트래픽을 역추적할 수 있다.

두번째 기능은 공격 트래픽을 제어하는 기능이다. 네트워크 자원이 보호되면서 해당 네트워크를 사용하는 사용자들이 피해를 입지 않게 하기 위해서 공격 트래픽을 제어하기 위한 적절한 명령의 라우터 적용은 매우 중요하다. 대응시스템인 NetWRAP 서버는 탐지시스템(에이전트)에서 전송된 비정상 트래픽 발원지 또는 목적지 정보와 서버의 첫번째 기능을 통해 구해진 비정상 트래픽 초입라우터와 인터페이스를 이용하여 적절하게 트래픽 제어 명령을 라우터에 적용시킬 수 있다. 이로써, NetWRAP 시스템은 효과적으로 네트워크 자원 남용 트래픽을 제거하면서 같은 네트워크를 사용하는 불특정다수 사용자들의 피해를 최소한으로 줄일 수 있다.

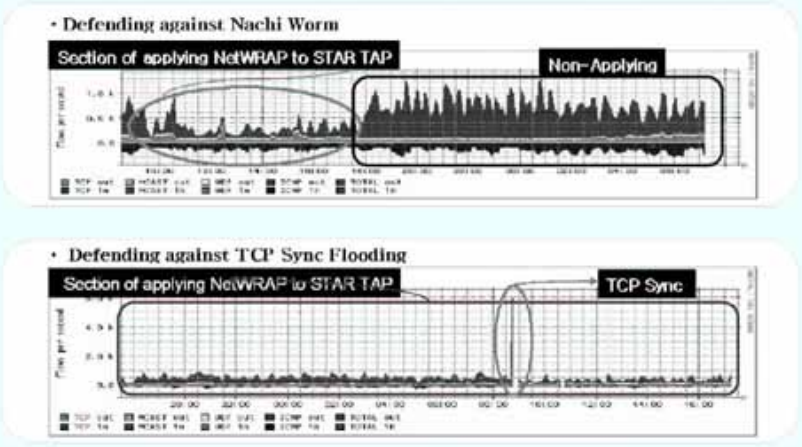
2) 적용

시스템 개발 후 테스트베드에서의 시험 적용을 거쳐, 특히 중요한 트래픽이 집중되고 있는 초고속연구망(KREONET)의 한 미 구간에서 시험 · 적용하여 웜바이러스 탐지 및 간헐적으로 나타나는 TCP Sync flooding을 이용한 DDoS 공격 탐지/대응을 하였다.

<그림 6>은 대응 결과의 예로써, 첫 번째 그래프는 2003년 9~12월동안 초고속연구망에는 Nachi Worm이 기승을 부리고 있었을 때 NetWRAP을 통하여 제어한 결과이며, 두 번째는 분산 서비스 거부 공격에 대한 제어 결과이다.

웜 바이러스의 경우 바이러스에 감염된 지역에서 대량의 트래픽이 흘러나오는 경향이 있으며 그 활동 주기가 매우 길었다. 웜 바이러스가 기승을 부리는 중 한 번씩 분산 서비스 거부 공격이 발생되기도 한다.

〈그림 6〉의 두 번째 그래프에서 보는 것처럼, 분산 서비스 거부 공격은 웜 바이러스에 의해 퍼진 공격 프로그램으로 인하여 일정시간에 한 곳의 목표 시스템을 공격하는 것으로 분석된다.



〈그림 6〉 NetWRAP을 이용한 네트워크 자원 남용 사건 대응 결과

4. 향후 과제

모든 공격 패킷들은 백본망을 경유해서 목적시스템에 도달한다. 그 중에서도 불특정다수가 피해를 받게 되는 분산 서비스 거부 공격이나 웜 바이러스는 백본망을 관리하고 있는 ISP에서 탐지 및 대응을 통하여 효과적으로 피해를 줄일 수 있다. 그에 일환으로 초고속연구망에서는 NetWRAP 시스템을 개발하게 되었고, 초고속연구망의 한-미 구간에 적용하여 분산 서비스 거부 공격 및 웜 바이러스에 대하여 대응하고 있다.

그러나 불특정다수가 피해를 받게 되는 공격형태인 분산 서비스 거부 공격 및 웜 바이러스 공격은 또 다른 형태로 진화하고 있다. 따라서 공격의 탐지를 수행하는 시스템이 정상적인 네트워크 트래픽 패턴을 잘 학습하여 끊임없이 변화하는 공격 트래픽의 유형을 탐지할 수 있는 탐지 방법의 연구가 꾸준히 필요할 것으로 보여진다.

알기 쉬운 과학용어

IPv6

IPv6(Internet Protocol version 6)는 최신의 인터넷 주소로서, 차세대 IP 주소체계라고도 불리고 있다. IPv6는 일련의 IETF(인터넷표준기관) 공식 규격으로서 현재 사용되고 있는 IP 버전4를 개선하기 위한 진화적 세트로서 설계되었다. IPv6가 IPv4에 보다 가장 명백하게 개선된 점은 IP주소의 길이가 32 비트에서 128 비트로 늘어났다는 점과 보안기능의 강화이다. 이러한 확장은 가까운 미래에 인터넷이 폭발적으로 성장할으로써, 네트웍 주소가 고갈할 것이라는 우려에 대한 대응책을 제시한다.

예를 들면, 유비쿼터스와 같이 휴대전화, TV, 휴대용단말기 등의 모든 비 PC 기기가 네트워크화될 경우 현재에도 부족한 IPv4의 주소로는 턱없이 부족하기 때문에 활용가능 주소가 상대적으로 많은 차세대 인터넷주소인 IPv6의 도입이 시급하며 정부에서도 의욕적으로 보급 및 확대를 추진하고 있다.

유비쿼터스

유비쿼터스(Ubiquitous)란 라틴어로 '편재하다(보편적으로 존재하다)'라는 의미이다. 모든 곳에 존재하는 네트워크라는 것은 지금처럼 책상 위 PC의 네트워크화뿐만 아니라 휴대전화, TV, 게임기, 휴대용 단말기, 카 네비게이터, 센서 등 PC가 아닌 모든 비 PC 기기가 네트워크화 되어 언제, 어디서나, 누구나 대용량의 통신망을 사용할 수 있고, 저요금으로 커뮤니케이션 할 수 있는 것을 가리킨다.

예를 들면, 차를 타고 여행을 갈 때 차안에서 디지털 방송을 통해 TV를 시청하고 휴대용 게임기를 사용하여 네트워크 게임을 하며 카 네비게이터로 위치정보를 받아서 정확한 목적지를 찾을 수 있고 여행 중에 집에 무슨 일이 있는지 확인할 수 있으며 돌아오면서 홈 네트워킹을 통해 히터를 켜서 집안에 온기를 유지시키며, 전기밥솥에 밥이 되도록 할 수 있는 그런 종류의 총체적인 네트워크 체계를 말한다.

QoS(Quality of Service) : 서비스 품질

인터넷이나 다른 네트웍 상에서, QoS는 전송율, 에러율, 그리고 측정과 개선이 가능하며, 어느 정도는 미리 보증할 수 있는 속성들에 관한 아이디어이다. QoS는 높은 대역의 비디오 및 멀티미디어 정보를 지속적으로 전송해야 하는 경우 특별한 의미를 갖는다. 이러한 종류의 콘텐츠를 공중 네트웍을 통해 신뢰할 수 있을 정도로 전송하는 것이 가능하도록 QoS에 대한 정책을 네트워크 정책서버(라우터, 스위치)를 통해 구현하는 기술이다.

예를 들면, 화상전화 사용자가 여러 가지 통신장애로 서비스를 잘 받을 수 없을 경우, 특정한 사용자에게 QoS를 적용하여 일반적인 사용자보다 고품질의 서비스를 제공함으로써 보다 원활한 통신이 가능하도록 유지할 수 있다. 기차에서 특실과 일반실을 구분하여 서비스(보통 IP Premium 서비스라 칭함)하는 것과 유사하며 특실의 고품격 서비스를 보장받은 사람은 일반실보다 많은 비용을 지불하듯 고비용을 지불해야 한다.

IP telephony

IP 전화방식은 전통적으로는 PSTN의 회선교환 접속을 사용해왔던 음성, 팩스, 기타 여러 가지 형태의 정보 교환에, IP 패킷교환 접속을 사용하는 기술을 더해서 통칭하는 용어이다. 인터넷 프로토콜을 이용하는 데이터망을 통한 통화는 PSTN의 사용 요금을 물지 않고, 공유 회선 상의 데이터 패킷으로서 전송된다. IP 전화방식이 해결해야할 문제는 음성, 팩스, 또는 비디오 패킷을 사용자에게 신뢰할만한 품질로 전송하는 것이다. IP 전화방식의 대부분은 이 문제의 해결에 초점을 맞추고 있다.

IP 전화방식은 컴퓨터, 전화, 그리고 TV를 하나의 통합된 정보환경으로 융합시키기 위한 중요한 부분이다. 즉, 하나의 기관에서 인터넷을 위한 전용회선을 가지고 있다면 이를 이용하여 데이터의 전송뿐만 아니라 전화, 팩스, 비디오 등의 서비스를 같이 이용하는 기술을 말한다. 현재는 기업의 본점과 지점간의 경우와 같이 사설 데이터 망을 통한 전화통화 및 관련 서비스에 주로 채택되어 사용되는 추세이다.

제공 김승혜 | 초고속연구망사업실 | shkim@kisti.re.kr