情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

P2P(Peer to peer) 환경에서의 정보보호 위협과 정보보호 서비스

김 봉 한*, 임 명 현**, 임 재 명**, 이 재 광***

요 약

P2P(peer to peer)는 인터넷에서 중간에 서버 컴퓨터를 거치지 않고 정보를 찾는 사람과 정보를 가지고 있는 사람의 컴퓨터를 직접 연결시켜 데이터를 공유할 수 있게 해주는 기술과 그 기술을 응용해서 제공되는 서비스를 말한다. P2P 서비스는 서버 없이 컴퓨터와 컴퓨터간에 데이터를 전송함으로서 의도적이거나 고의적인 공격자에 의해 정보보호 위협에 상당히 노출되어 있는 실정이다. 본 연구는 P2P 서비스 모델의 분류와 현재 제공되고 있는 대표적인 P2P 서비스인 냅스터와 그누텔라의 어플리케이션 구조에 대해 분석하였고 P2P 환경에서 발생할 수 있는 정보보호 위협과 안전한 통신을 위해 요구되는 정보보호 서비스에 대해 고찰하였다.

Ⅰ. 서 론

P2P(peer to peer)는 인터넷에서 중간에 서버 컴퓨터를 거치지 않고 정보를 찾는 사람과 정보를 가지고 있는 사람의 컴퓨터를 직접 연결시켜 데이터를 공유할 수 있게 해주는 기술과 그 기술을 응용해서 제공되는 서비스를 말한다. 인터넷에서 정보를 검색엔진을 거쳐 찾아야 하는 기존 방식과는 달리 인터넷에 연결된 모든 개인 컴퓨터로부터 직접 정보를 검색하고 제공받을 수 있다[1].

근거리통신망(LAN)을 인터넷으로 확대한 개념으로 이 기술을 이용하면 컴퓨터 사용자가 별도의 서버나 고정 IP(전용선) 없이도 인터넷으로 서로의 컴퓨터를 자유롭게 접근하여 필요한 자료를 주고받을 수 있기 때문에 일반 컴퓨터 사용자는 MP3 파일이나 다른 컴퓨터 파일을 중간 서버 없이 직접 주고받을 수 있다. P2P를 이용하여 제공될 수 있는 서비스는 멀티미디어 파일 전송, 인터넷 쇼핑 및 경매 서비스, 인터넷 컨텐츠 검색과 제공, 협동 작업을 위한 업무용 도구, 기업 어플리케이션 서비스 제공(ASP)등과 같이 멀티미디어 환경에서 널리 사용될 수 있다[2].

그러나 P2P 서비스는 서버 없이 컴퓨터와 컴퓨터간에 데이터를 전송함으로서 의도적이거나 고의적인 공격자에 의해 정보보호 위협에 상당히 노출되어 있는 실정이다. 현재 정보보호업계에 따르면 국내에 본격 서비스되고 있는 P2P 방식으로 교환되는 파일에는 백오리피스·링제로 등 백도어 프로그램을 몰래 심어놓을 수 있어, 이를 알지 못하는 사용자는 자신의 컴퓨터를 쉽게 해킹 당할 수 있다. 더구나 공격자가 온라인 주식투자나 홈뱅킹에서 사용되는 패스워드를 알아낼 경우 경제적인 손실도 입게 돼 문제가 심각해지고 있다. 또한 P2P 서비스는 문서파일을 MP3파일 등으로 바꾸는 등 확장자를 전환할 수 있기 때문에 회사 기밀정보를 외부로 손쉽게 빼낼 수도 있으며, 이 경우 추적이 거의 불가능하다[4].

그러므로 이러한 정보보호 위협에 대해 안전한 P2P 서비스를 제공하기 위한 정보보호 환경을 위해서 정보보호 위협 요소들과 정보보호 서비스에 관한 연구가 필요하다. 따라서 본 연구는 P2P 서비스의 분류와 현재 제공되고 있는 대표적인 P2P 서비스인 냅스터와 그누텔라의 어플리케이션 구조에 대해 분

본 연구는 2002년도 한국정보보호진흥원 지원으로 수행하였습니다.
* 청주대학교 컴퓨터정보공학과 (bhkim@chongju.ac.kr)
** 한국정보보호진흥원 해킹·바이러스상담지원센터 ({shlim, mlim}@cert.certcc.or.kr)
*** 한남대학교 컴퓨터공학과 (jklee@netwk.hannam.ac.kr)

석하였고 P2P 환경에서 발생하는 정보보호 위협과 안전한 통신을 위해 요구되는 정보보호 서비스를 고찰하였다.

Ⅱ. P2P 어플리케이션

2.1 P2P 어플리케이션의 분류

P2P는 모델들은 다음과 같은 형태로 구분된다[2, 3].

- 순수한 P2P
- 간단한 조회 기능 서버를 가진 P2P
- 조회 서버와 룩업 서버를 가진 P2P
- 조회/룩업/컨텐트 제공 기능의 서버를 가진 P2P

2.1.1 순수한 P2P

순수한 P2P모델은 어떠한 중앙의 서버에도 의존하지 않고 작동한다. 일단 P2P 어플리케이션이 클라이언트의 메모리에 다운로드 되면 피어들은 네트워크에 접속된 다른 피어들을 동적으로 찾는다 연결된 피어들 사이의 모든 통신은 어떠한 서버의 도움도 받지 않는다.

순수한 P2P 모델의 이러한 특징은 모든 통신 프로세스에서 서버가 지정한 규칙에 근거해서 실행되는 클라이언트/서버 모델의 전통적인 통신방법을 사용하지 않고 사용자들 자신이 나름의 규칙을 지정할 수 있도록 해 주며, 그들 자신의 네트워크 환경을 설정할 수 도 있게 해준다. 이 P2P 모델은 인터넷을 이용하기 위해 특정 서버 또는 ISP에 가입해야 하는 불편을 완전히 해결해 준다.

순수한 P2P 모델의 단 한가지 문제점은 피어들에 대한 검색이 네트워크 상에서 이루어진다는 것이다. 네트워크에 로그인한 피어들의 목록을 등록해 주는 중앙관리자의 역할을 담당하는 것이 없기 때문에 사용자들 스스로 다른 피어들의 위치를 찾아야 한다.

2.1.2 간단한 조회기능 서버를 가진 P2P

이 모델은 서버를 실질적으로 포함하고 있는 것은 아니다. 약간의 관리를 위해 서버의 역할이 이 모델에 포함되어 있기는 하지만 이 모델에서 서버의 역할은 접속하는 피어에게 이미 접속된 피어들의 이름을 제공하는 것으로 한정된다. 접속하는 피어는 로그인함으로서 서버에게 자신의 존재를 알리게 된다. 다시 말해서, 서버는 단지 피어들로 하여금 접속하는 피어들의 목록을 제공함으로서 피어들을 돕는 것이며, 접속을 수립하는 것과 통신을 수행하는 것은 여전히 피어들 자신의 몫이다. 이런 P2P 모델은 이미 접속된 다른 피어들의 목록을 제공하여 많은 수의 피어들을 조회할 수 있는 가능성이 높아지기 때문에 순수한 P2P 모델에 비해서 우월하다. 자원을 다운로드받기 위해서 피어는 접속된 각각의 피어들에게 개별적으로 접근해서 요청을 보낸다. 이때 요청을 보내는데 처리 시간이 길어지기도 한다.

2.1.3 조회 서버와 룩업 서버를 가진 P2P

서버의 역할은 접속된 피어들의 목록을 각각의 이용 가능한 자원들과 함께 제공하는 것이다. 따라서 이 모델은 서버의 향상된 기능을 위해 순수한 P2P 모델과 간단한 조회 서버를 가진 P2P 모델의 특징을 통합하고 있다.

이 모델에서는 피어들이 자신이 필요한 정보를 얻기 위해 각각의 피어를 일일이 방문할 필요가 없기 때문에 피어들에게 주어지는 부담이 적다. 이 모델에서 서버는 두 피어들 사이에 통신을 개시한다. 두 개의 연결된 피어들은 통신을 개시하고 유지하면서 다양한 활동을 수행하게 된다. 피어들이 수행하는 활동들에는 접속하는 피어들에 대한 정보를 얻기 위해 데이터베이스에 로그인하거나 공유된 자원들의 목록을 조회하는 것 등이 있다.

2.1.4 조회/룩업/컨텐트 제공 기능의 서버를 가진 P2P

이 모델에서 서버는 전형적인 클라이언트/서버 구조와 같은 지배권을 가진다. 피어들의 요청을 들어주는 모든 것들은 피어의 영역에 있는 것이 아니라 서버에 존재한다.

또한 모든 자원들이 중앙에 위치한 서버의 데이터베이스에 저장되어 있기 때문에, 피어들이 서로 직접 연결하는 것을 허용하지 않는다. 만약 한 피어가 정보를 요청하면 다른 피어와 통신을 하는 대신 서버에 접근한다. 서버는 요청을 처리해서 정보를 제공한다.

이 모델의 큰 단점은 많은 요청이 동시에 쇄도할 경우 서버가 느려진다는 것이다. 서버가 데이터를 관리, 저장해야하고, 스스로 모든 요청을 처리해야 하기 때문에 비용이 늘어난다는 단점도 있다.

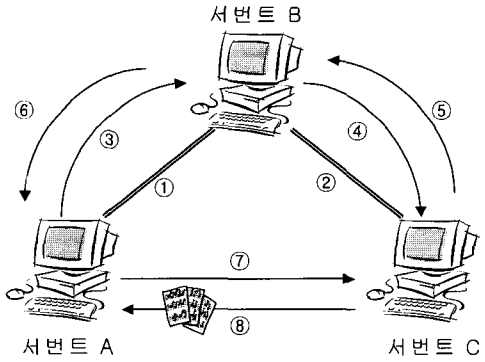
이런 모델은 중앙의 서버에 전적으로 의존하기 때

문에, 단일 지점에 기인한 고장이 발생할 가능성이 높아지고 결과적으로 전체 시스템에 부정적인 영향을 미친다. 앞에서 언급한 P2P 모델의 경우 이런 문제가 발생하지 않는다.

2.2 대표적인 P2P 어플리케이션 분석

2.2.1 그누텔라(Gnutella)

그누텔라는 중앙 서버를 사용하지 않는다. 각 컴퓨터는 서버뿐만 아니라 클라이언트로서 동작한다. 따라서 서번트(servent)라고 부른다. 서번트는 서버와 클라이언트의 합성어이다. 이러한 P2P 네트워킹 모델은 신뢰성, 속도, 검색 능력은 감소하면서 네트워크 트래픽은 증가한다. [그림 1]는 파일을 전송하기 위한 통신 처리를 보여주고 있다.



[그림 1] 그누텔라의 파일 전송 방식

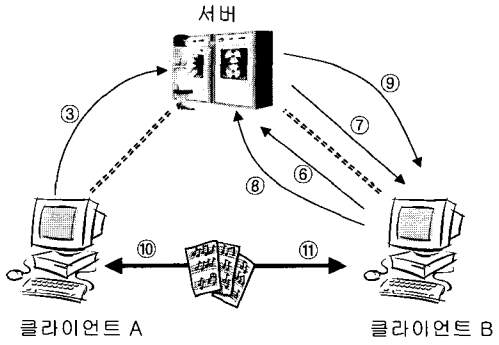
① 서번트 A는 서번트 B에게 연결한다.
② 서번트 C는 서번트 B에게 연결한다.
③ 서번트 A는 파일 이름 질의를 전송한다.
④ 서번트 B는 질의에 맞는 지역 데이터를 검색한다. 질의에 맞는 데이터가 없을 경우, 서번트 B는 서번트 C에게 질의를 전송한다.
⑤ 서번트 C는 질의에 맞는 지역 데이터를 검색한다. 질의에 맞는 데이터가 있을 경우, 서번트 C는 서번트 B에게 질의 응답을 전송한다.
⑥ 서번트 B는 서번트 A에게 질의 응답을 전달한다.
⑦ 서번트 A는 파일을 다운로드하기 위하여 직접 서번트 C에 연결한다.
⑧ 서번트 C는 서번트 A에게 파일을 전달한다.

만약 서번트 C가 방화벽 뒤에 있고 초기화되지 않은 연결을 수신할 수 없다면, 메시지는 파일을 푸쉬하는 형태로 서번트 C가 서번트 A와 연결을 초기화시키기 위해 네트워크를 통해 전달될 수 있다.

그누텔라 프로토콜에서는 그누텔라 네트워크로 초기화 링크를 제공하기 전에 서번트의 위치 정보를 가지고 있어야 한다. 이러한 서번트 목록 작성은 그누텔라 프로토콜의 일부분은 아니다. 가까운 서번트들을 탐지하는 많은 디렉토리 서비스들이 있다.

2.2.2 냅스터(Napster)

냅스터 P2P 네트워크는 중앙 디렉토리 서버를 포함한다. 클라이언트는 우선 클라이언트 사이에서 메시지를 전달하고 클라이언트의 특정한 상태를 관리하는 디렉토리 서버와 통신하고 한다. (그림 2)는 냅스터 프로토콜에서 파일을 전송하기 위한 통신 처리를 보여준다.



[그림 2] 냅스터의 파일 전송 방식

① 클라이언트 A는 서버에 로그온 한다.
② 서버는 성공한 메시지를 응답한다.
③ 클라이언트 A는 공유를 위해 사용 가능한 파일의 파일 이름을 전송한다.
④ 클라이언트 B는 서버에 로그온 한다.
⑤ 서버는 성공한 메시지를 응답한다.
⑥ 클라이언트 B는 서버에게 특정한 파일 이름을 위한 검색하는 메시지를 전달한다.
⑦ 서버는 일치하는 파일 이름에 대해 사용 가능한 클라이언트들의 목록을 응답한다.
⑧ 클라이언트 B는 서버에게 클라이언트 A에 위치하는 파일에 대해 다운로드 요구를 전송한다.
⑨ 서버는 클라이언트 A에 대한 IP 주소와 수신 포트를 포함하는 자세한 정보를 응답한다.
⑩ 클라이언트 B는 클라이언트 A와 연결하고 파

일 요구를 전송한다.
⑪ 클라이언트 A는 파일을 응답한다.

만약 클라이언트 A가 방화벽에 의해 초기화되지 않은 직접 연결을 수신하지 못한다면 다음과 같이 8단계부터는 달라질 것이다.

⑧ 클라이언트 B는 서버에게 클라이언트 A에 위치하는 파일에 대한 대안적인 다운로드 요구를 전송한다.
⑨ 서버는 클라이언트 B로 파일의 전송을 초기화하는 클라이언트 A에게 메시지를 전송한다.
⑩ 클라이언트 A는 클라이언트 B에게 연결하고 파일을 전송한다.

이것은 경우에 따라 냅스터의 권한을 제한하고 파일의 이름에 의해 필터링 하거나 제어하는 중앙 서버를 방지한다. 그러나 클라이언트는 중앙 디렉토리 서비스를 이용해 그들 자신을 등록한다.

〔표 1〕은 냅스터와 그누텔라의 장단점을 비교한 것이다.

〔표 1〕 냅스터와 그누텔라의 비교

	냅스터	그누텔라
장점	• 전 세계에 걸친 광범위한 사용 • 서버를 이용한 인증 가능 • 편리한 사용 • 다운로드 및 설치의 용이	• 단일지점에 의한 고장 배제 • 여러 형태의 파일 공유 (MP3, EXE, JPG 등) • 요청의 리다이렉트에 대한 방지기능
단점	• 병목현상 발생 • MP3만 공유 • 음반산업에 의한 저작권 시비	• 요청 쇄도시 중단 기능의 부재 • 데이터의 발신지 위치 인식 불가 • 어플리케이션에서 패킷 손실 • 많은 버그

III. P2P 환경에서의 정보보호 위협

기업이 P2P를 이용하는 것은 불특정다수의 이용자에 대해 자사의 PC의 자원이나 서비스의 이용을 가능하도록 하기 위해서이다. 따라서 이것에 의해 새로운 취약성이 발생한다.

P2P 네트워크의 사용은 악의적인 소프트웨어를 전달하는 능력뿐만 아니라 악의적인 소프트웨어에 의해 통신하는 프로토콜의 사용까지도 허가한다.

많은 기관에서 백 오리피스 같은 백도어 트로이 목마는 방화벽 때문에 효과적으로 침입할 수가 없다. 이 같은 프로그램은 조심스럽게 연결을 개방하고 연결하기 위한 기관의 외부에 있는 클라이언트를 기다린다. 왜냐하면 방화벽은 특별히 정의된 시스템이나 포트를 제외한 수신 연결을 방지한다.

그런데, P2P 소프트웨어는 일반적으로 방화벽에 의해 방지되지 않는다. 왜냐하면 이것이 중앙 디렉토리 서비스 또는 다른 서버트들과 송신 연결을 하기 때문이다. 일단 송신 연결이 발생하면, 중앙 디렉토리 서비스 또는 서버트는 클라이언트로 정보를 전달할 수 있다.

현재의 대부분 백도어 트로이 목마는 이러한 송신 연결을 수행하지 못한다. 왜냐하면 트로이 목마는 정의된 대기 서버로의 연결을 필요로 하기 때문이다. 어떤 백도어 트로이 목마는 IRC 또는 비슷한 중앙 서비스에 송신 연결을 하는 방법을 회피한다. W32.PrettyPark는 IRC로 송신 연결을 생성하는 웜의 예이다. 이것은 일반적인 방화벽 구성에 의해 방지되지 않는다. 일단 웜이 IRC로 연결이 되면, 해커는 같은 채널에 가입할 수 있고 원격 접속 명령을 전송할 수 있다.

이 같은 방법은 P2P 네트워크를 불법적으로 사용하도록 수행되어진다. 예를 들면, 악의적인 위협은 냅스터의 중앙 서버를 통해 등록될 수 있고 특정한 파일의 목록을 전달할 수 있다. 그 다음에 해커는 특정 파일에 대한 검색을 수행한다. 그리고 일치될 때, 감염된 시스템을 식별할 수 있다. 어떤 파일을 위한 요구 사항은 특별한 해킹 작업을 수행하도록 하기 위해 감염된 시스템에 신호를 보낸다. 이를테면 스크린 화면처럼, 정보의 수집과 시스템의 제어는 방화벽을 우회하고 해커의 익명성을 보증하는 방법으로 수행된다.

또한 악의적인 소프트웨어는 기존의 P2P 클라이언트의 구성을 쉽게 변경할 수 있다. 예를 들면, 트로이 목마는 접속을 위해 연결되는 특정한 디렉토리를 대신 하기 위하여 구성을 수정할 수 있다. C:\My Music처럼, 전체의 하드 드라이브는 검색과 다운로드를 위해 개방되어진다[4~6].

따라서 P2P 환경에서 이러한 불법적인 공격에 대한 주요 위협은 다음과 같다[7].

3.1 기밀성

기밀성에서는 정보의 유출을 방지하기 위해서 불법적인 접근에 관한 취약성이 있다. P2P 소프트웨어를 이용하는 PC에 있는 파일에 대해서 각각의 기밀성을 설정하지 않고, 또 기밀성에 대응해서 파일마다 접근 제어를 소홀히 하면, 악의적인 P2P 소프트웨어의 이용자로부터 파일을 불법적으로 유출하거나, 수정하는 불법적인 접근의 위협을 받게된다. 더구나 사용 정보에 대한 로그관리를 소홀히 하면, 언제, 누가, 어떤 파일을 접근하고, 정보를 유출, 수정했는지 나중에 추적할 수 없게 된다.

이러한 불법적인 접근에 대한 취약성에는 기밀성에 의한 PC 파일의 미비, 누구에게 어떤 파일의 이용을 허가할 것인가 하는 접근제어의 미비, 사용정보를 알기 위한 로그관리 미비 등이다

3.2 무결성

P2P 소프트웨어의 도입에 의해, 정보의 무결성을 저해하는 위협으로서 트래픽의 증가에 의한 네트워크의 정지, 바이러스의 침투, 신뢰성이 낮은 정보의 유통 등이 있다.

3.2.1 네트워크의 정지

P2P 소프트웨어를 여러 명이 동시에 사용하면, 네트워크의 트래픽이 증가하여 다른 시스템에 지장을 주는 경우가 있다.

오레곤 주립대학을 시작으로 전 미국에서 70% 이상의 대학이 트래픽의 증가에 의해 다른 시스템에 지장을 초래한다고 하는 이유 때문에 학교 내의 PC에서 냅스터의 사용을 금지했다.

또, P2P 소프트웨어 자체의 통신이 중단됨으로서 검색결과와 송신결과가 불충분하게 되는 경우도 있다.

그누텔라는 이용자의 증가로 네트워크 트래픽이 증가해 그누텔라 시스템 전체가 정지하는 사태가 발생했다. 그누텔라와 같은 모델에서는 시스템으로의 참가자가 증가하면 지수급수적으로 트래픽이 증대하기 위해, 어느 계층까지 문의할 것인가를 제한하는 기관이 필요하게 된다.

이 취약성에서는 트래픽 제어의 미비나 네트워크의 대역폭의 부족 등이 있다.

3.2.2 바이러스의 침입

P2P 소프트웨어에서는 PC 자원을 직접 공유하기 때문에 공유하고자 하는 PC에 바이러스가 감염된 파일이 있으면 그 파일을 공유한 PC은 연쇄적으로 감염된다. 이러한 이유로 기존의 통신 형태보다도 바이러스에 감염되기가 쉽다.

기존의 바이러스 감염경로는, 플로피디스크나 CD-ROM등에 의해 감염되는 경우와 감염된 파일을 전자메일에 첨부해 보내진 경우가 대부분이었다. 이와 같이 P2P는 기존의 바이러스의 감염경로에 추가해서 새로운 감염 경로를 가지게 된다.

이에 대한 취약성에는 백신소프트웨어의 미도입, 파일의 비동기가 있다.

3.2.3 신뢰성이 낮은 정보의 유통

정보의 발신지가 신뢰 가능한 형태로 인증되지 않는 경우, 이러한 정보의 신뢰성에 대한 판단은 어렵다. 예를 들면, SETI@home에서는, 참가자의 인센티브로서 작업의 공헌도에 대해 랭킹을 발표하고 있다. 그러나 결과를 속이거나 완료한 작업을 많이 게시하여 랭킹차트의 순위를 올리려고 하는 사용자에 대한 연산 결과의 확인작업에 많은 비용이 든다고 한다. P2P를 통해 인터넷에서 협력작업을 할 경우, 이러한 작업은 간단하게 가능하지만 이곳에서 공유하는 정보의 신뢰성이 낮으면 결과에 대한 적정한 판단이 되지 않는다. 이러한 정보의 신뢰성에 대한 문제가 취약성이 된다.

3.3 가용성

가용성에 관한 위협에는, 하드웨어의 고장, 서버의 정지, 시스템의 사용 불능이 있다.

3.3.1 하드웨어의 고장

일반적으로, PC은 24시간 365일 동안 사용하지 않기 때문에 그 내구성은 서버에 비해서 낮다. 장시간동안 연속해서 이용하면 I/O(Input/Output)에 관련된 하드디스크나 네트워크보드에 장해가 많이 발생한다. 이것 때문에, 중요한 데이터가 소실되거나, PC를 이용할 수 없는 상태가 되기도 한다.

3.3.2 서버의 정지

P2P에서는, 현재 어떤 PC가 통신 가능한지를 알 필요가 있다. 냅스터와 같은 모델에서는 서버가 그 중개기능을 담당하고 있다. 그 때문에 그누텔라와 같은 모델보다 가용성이 높은 시스템을 구축할 수 있다. 다만, 서버가 정지하면 중개기능을 이용할 수 없기 때문에, 냅스터 모델에서는 전체의 서버가 정지하게 된다. 이 취약성에는 처리량에 대한 서버의 내구성과 소프트웨어의 설계에 대한 문제가 있다.

3.3.3 시스템의 사용 불능

기관의 정보시스템 환경에 따라, P2P 소프트웨어를 사용할 수 없는 경우도 있다. 현재 인터넷통신은 IPv4를 사용하고 있다. 이 IP 주소는 4,294,967,296개이지만, 인터넷이 급속히 보급됨으로 인해 IP 주소 고갈 문제가 심각해지고 있다. 대책으로서, 한정된 IP 주소를 효율적으로 사용하기 위해 일반적으로 기관내의 네트워크에서는 기관이 임의로 결정한 로컬 IP 주소를 이용해, 외부와 통신하는 경우, 방화벽 등에서 여러 개의 광역 IP 주소에 NAT(Network Address Translation)변환한다.

그러나 NAT 변환된 IP 주소에서는 외부로부터 그 기관의 PC는 모두 여러 개의 공통 광역 IP 주소로 인식되기 때문에, 실제의 통신상대와 대응하는 것이 어렵게 된다. 따라서 이에 대한 대책이 필요하다.

현재의 냅스터나 그누텔라에서는 송수신자가 방화벽에서 NAT하고 있는 경우에 그 시스템을 이용할 수 없다.

3.4 준법성

준법성에 관한 위협에는 불법 복사, 공동 저작물 등에 관한 권리 침해, 개인정보유출이 있다.

3.4.1 불법 복사

저작물을 디지털화하면, 저작물을 원본과 다름없는 사본을 저렴한 비용으로 간단히 복사할 수 있다. 더구나 냅스터나 그누텔라 같은 P2P 소프트웨어를 사용하면, 그 저작물을 전 세계에서 공유하는 것이 가능하게 된다. 그 때문에 기관은 담당자의 고의 또는, 무지나 부주의로 인한 취약성에 의해, 타인의 저작물을 무단으로 사용하거나 공유하고, 타 기관의 저작권을 침해할 위험이 있다. 또 반대로, 타 기관이 자신의 기관 저작물을 침해할 수 있는 위협도 있다.

3.4.2 공동저작물등에 관한 권리침해

현재는 디지털 저작물의 작성자의 정보를 파일에 입력하는 기관이 서서히 일반화 되어가고 있지만, 디지털저작물을 공동으로 작성한 경우, 누구의 아이디어로 어느 부분을 작성했는지를 기록에 남기는 기술이 아직 일반적이지 않다. 이것은 기존의 저작물을 편집 가공하는 것에서 새로이 저작권이 발생하는 편집 저작물에 대해서도 마찬가지이다. 또 권리범위를 계약에 명기하고 있지 않기 때문에, 뒤에 이것이 문제가 되는 경우도 있다.

이렇게 공동저작물 등에 관한 권리침해에서는 디지털저작권보호기술의 미비나 계약의 미비가 취약성이 된다.

3.4.3 개인정보유출

모바일·인텔리전스·에이젠트의 P2P 소프트웨어에서는 사용자가 사전에 자신이 원하는 정보의 조건에 대해 등록하면, 여러 기관이 필요할 때 관련된 정보를 제공하는 것이 가능하게 된다. 그러나 이것은 사용자의 취미·기호 등의 정보를 기관 측에 제공하는 것이 전제가 된다. 이러한 정보를 기관은 외부로 유출되지 않도록 해야 한다. 그러나 고장 혹은 규정의 미비나 교육의 불충분이라고 하는 취약성 때문에 고객정보가 유출되는 위험이 있다.

IV. P2P 환경에서 요구되는 정보보호 서비스

기관은 어느 시점에서 누구에 대해 어떤 정보를 공개하고 공유할 것인지, 또 PC 자원의 이용을 허가할 것인가에 대한 정보보호 정책을 명확히 하지 않으면 안 된다. 그래서 부서 내, 부서간이나 기관간, 사용자나 타 기관간 등에서 어느 P2P 소프트웨어를 이용하는가에 대해, P2P의 기술동향이나 타 기관의 도입 상황을 파악하고, 검사할 필요가 있다.

위에서 설명한 것과 같이 새로운 기술인 P2P라고 해도 그 기술은 기존의 TCP/IP를 시작으로 하는 여러 가지 인터넷기술을 선택해서 구성하고, 거기에 새로운 기능을 추가하는 것으로 이루어진다. 따라서, 현재의 인터넷의 정보보호 대책을 P2P의 특성에 맞춰서 검토하는 것이 중요하다.

P2P의 취약성에 대한 구체적인 정보보호 서비스는 표2와 같다. 정보보호 서비스는 정보보호 관련 기술에 의한 기술적 대책, 건물과 같은 구조물에 대

한 물리적 대책, 실제로 작업하는 사람이나 제도에 관한 기관·제도적 대책 등이 있다.

각각의 P2P 소프트웨어에 대해 다음의 모든 대책을 실시할 필요는 없지만 그 소프트웨어의 특성에 따라서 대책을 마련하고 실시해야만 한다[7].

4.1 기밀성

P2P에서는 파일 접근 제어, 파일의 암호화, 접근 로그 관리의 기능을 어떻게 PC에서 구현할 것인지가 배포의 한 조건이 된다. P2P 소프트웨어는 상황에 따라 사용자를 제한할 수 있어야 한다. 현재의 PC의 기본소프트웨어에는, 이러한 기능이 없거나 또는 불충분하기 때문에 차후에 이에 대한 개선이 필요하다. 또 P2P 소프트웨어의 도입을 검토하는 경우, 그 소프트웨어에 위에서 언급한 기능이 존재하는가를 검토해야 한다. 그 외에 방화벽이나 스팸메일 대책 등도 PC 기반에서 고려해야만 한다.

P2P의 사용 환경이 PC이기 때문에 서버와 같이 별도의 전산실을 두어 관리하는 것은 어렵다. 그러나 기밀성을 향상시키기 위해서는 P2P에서 이용하는 PC의 위치를 제한하는 등의 물리적 대책이 필요하다.

기관·제도적 대책으로는 각 PC의 파일에 대한 기밀성에 의한 분류, 전자인증시스템에 의한 기관 외부 사용자의 신분 사전 확인, 사용자의 제한, 정보보호 의무와 손해 배상에 대해서의 계약 체결 등을 실시해야한다.

4.2 무결성

P2P에서는 정보의 무결성을 확보하기 위해, 네트워크의 트래픽의 증가 제어, 바이러스 침입 방지, 정보의 신뢰성 향상 등이 과제가 된다.

4.2.1 트래픽의 제어

트래픽을 제어하기 위해, 업무에 불필요한 P2P 소프트웨어의 사용을 제한하는 규정과 기술적 대책이 고려되어야 한다.

광대역의 네트워크를 정비하는 것도 대책의 하나이지만, 네트워크가 정지하여 다시 파일을 송수신할 때, 도중부터 재 전송되는 기능을 P2P 소프트웨어에 적용해야만 한다. 또 네트워크 장비에 대해서 QoS(Quality of Service)에 의한 프로토콜마다 트래픽을 제한하거나, 우선순위를 변경하는 것도 가능해야 한다. 이 기능을 사용하여 기관 내에서 P2P 소프트웨어 사용을 금지하거나 우선적인 네트워크 자원을 할당할 수 있다.

4.2.2 바이러스의 침입

PC의 수가 증가하면서 서버로부터 프로그램을 자동적으로 다운로드해서 PC의 프로그램을 갱신하지 않는 경우, 모든 PC의 프로그램이 갱신되지 않아 동기를 맞출 수 없는 경우도 있다. 그러나, P2P에서는 상호 프로그램 파일의 버전을 순차적으로 검사하면서 동기를 맞출 수 있다.

4.2.3 정보의 신뢰성향상

정보의 신뢰성을 향상시키기 위해, 정보를 이중으로 검사하는 것이 필요하게 된다. SETI@home에서는 같은 데이터에 의한 계산을 이중으로 실시하고 그 사이에 차이가 있는지를 검사해서 정보의 신뢰성을 확보하고 있다.

4.3 가용성

기존의 기관들은 시스템의 가용성을 향상시키기 위해서 서버나 네트워크의 정지를 방지하고 신속하게 복구시키는 대책을 강구해왔다.

예를 들면, 하드디스크 등의 이중화, 데이터의 백업이 대표적이다. 더구나 P2P에서는 활성 정보의 공유, IPv6의 보급 등이 가용성을 향상시키기 위해 필요하게 된다.

4.3.1 하드디스크 등의 이중화

P2P에서 중요한 처리를 담당하고 있는 PC는 서버와 같이 높은 가용성 부품을 사용해야만 한다. 하드디스크 등의 이중화는 분산 저장 공유가 하나의 해결책이 된다. 이것은 여러 개의 PC의 하드디스크에 분산해서 파일을 공유하는 것으로, 시스템 전체로서 하드디스크를 이중화하는 구조이다.

4.3.2 데이터의 백업

클라이언트/서버 시스템은 파일을 서버에 저장하는 것이 가능하기 때문에 서버에서 일괄적으로 백업을 하는 것이 가능하다. 그러나 P2P에서는 파일이 각 PC에 분산되어있기 때문에 일괄적인 백업은 할 수 가 없다. 분산 저장 공유는 데이터의 백업으로

사용이 가능하지만, PC 자체의 가용성은 서버에 비해 낮기 때문에 중요한 데이터의 백업은 각자 처리해야만 한다.

4.3.3 활성 정보의 공유

활성 정보를 관리하는 서버가 정지하면, 냅스터 모델은 처리할 수 없기 때문에, 시스템 전체를 다중화하기 위해서 서버를 여러 곳에 분산배치하지 않으면 안 된다.

4.3.4 IPv6의 보급

P2P에서는 통신 상대를 확정하기 위해서 각 PC에 고정의 광역 IP 주소를 설정하는 것이 바람직하다. IP 주소 고갈 문제를 해소하기 위해서는 약 3.4×10^{38}의 주소를 가진 새로운 IPv6의 보급이 기대되어진다. 또 IPv6에서는 종래의 IPv4와는 달리 데이터 통신의 암호화를 적용해야하고, 기밀성의 관점에서도 도입이 바람직하다.

4.4 준법성

준법성에 관한 기술적 대책에는, 전자투명, 전자인증 시스템, 전자 지불 시스템, 불법적인 복사 탐지용 웜 등이 있다.

4.4.1 전자투명

디지털저작물에 저작권자의 정보를 넣는 기술이다.

4.4.2 전자인증시스템

저작권자와 사용자의 신분 증명과 전자 투명을 이용해 정보가 수정되었는지를 검사할 수 있다.

〔표 2〕 P2P의 정보보호 서비스와 대책

기밀성	기술적 대책	· 파일 접근 제어 · 파일의 암호화 · 접근 로그 관리 · 개인 방화벽 · 스팸메일 방지 · 전자 인증 시스템
	물리적 대책	· P2P를 이용하는 PC의 설치 위치를 제한
	기관·제도적 대책	· 파일의 기밀성에 따른 분류 · 사용자(기관내·외)의 제한 · 기관 내부 사용자의 신분 확인 · 사용자의 정보보호의무와 손해 배상 청구 계약의 체결
무결성	기술적 대책	· 프로토콜에 대한 트래픽 제어 · 광대역 네트워크의 정비 · 소프트웨어의 재 전송 기능의 적용 · 데이터의 순차적 갱신 · 바이러스 대책
	기관·제도적 대책	· 사용제한에 대한 규정 · 복수처리에 의한 계산 결과의 확인
가용성	기술적 대책	· 높은 가용성을 가진 부품의 사용 · 하드웨어의 이중화 · 데이터 백업 · 분산 병렬 처리 · IPv6의 적용
	기관·제도적 대책	· 허가되지 않은 소프트웨어의 사용금지
준법성	기술적 대책	· 전자 투명 · 전자 인증 시스템 · 전자 지불시스템 · 불법적인 복사 탐지용 웜
	기관·제도적 대책	· 저작권에 대한 교육 · 공동 저작권의 권리 계약 체결 · 과금 제도의 정비

4.4.3 전자 지불 시스템

디지털저작물의 이용에 대한 과금 시스템이며, 컴퓨터를 통해 소액의 금액을 지불하는 시스템이다.

4.4.4 불법적인 복사 탐지용 웜

타인의 PC에서 불법 복사한 파일이 있는지를 검사하는 바이러스의 한 종류이다.

그러나 위의 대부분은 실험단계에 있으며 표준화 작업 중이기 때문에 실용화가 늦어지고 있다. 따라서, 준법성에 대한 사용 가능한 정보보호기술의 실용화를 위해 그 취약성을 기관·제도적 대책에 따라 보호하지 않으면 안 된다. 저작권이나 개인 정보보호에 대한 직원 교육, 공동 저작물의 권리 범위나 과금 제도 등이 있다.

V. 결 론

P2P 서비스를 사용하기 위해 연결되는 가상의 공유 시스템은 개방 시스템이기 때문에 근본적으로 정보보호의 문제점을 안고 있다. 그래서 적절한 정보보호 수준을 유지하기가 쉽지 않다. 그러므로 정보보호와 개인정보 노출, 컴퓨터 바이러스 확산, 비공유 영역에 대한 침해(일종의 해킹)와 같은 부당한 침해에 대한 문제점이 심각하게 대두될 수 있다. 현재 각 업체에서는 P2P프로그램을 이용해 파일을 공유할 때 해킹 위험으로부터 사용자의 컴퓨터를 보호해 주는 프로그램이 대해 연구를 하고 있지만 아직 공격 방법이나 바이러스의 유형 그리고 정보보호 환경에 대한 정보보호모델 및 대응방법에 대한 연구는 진행되고 있지 않아 정보보호 서비스 기능이 부족하고 위협에 대해 불안전하다.

따라서 본 연구에서는 이러한 연구를 위한 기반 기술로서 P2P 환경에서의 정보보호 위협요소와 정보보호 서비스에 대해 고찰하였다. 향후의 연구 과제로서, 이러한 정보보호 서비스를 설계할 수 있는 P2P 정보보호 환경과 플랫폼에 대한 연구가 필요하다.

참고문헌

[1] 전현성 역, *"차세대 인터넷 P2P"*, 한빛미디어, 2001

[2] 한성수, 조재완, 김천식, "P2P(Peer-to-Peer) 비즈니스 모델에 관한 연구", 한국경영정보학회, *2001년도 정영정보 계열 공동 국제학술대회*, 2001.

[3] Dreamtech Software Team, *"Peer to peer Application Development: Cracking the Code"* John Wiley & Sons, 2001

[4] Paulson, L.D., "New viruses target P2P systems", *Computer*, vol.34, no.11, November , 2001.

[5] Hurwicz, Michael, "Peer pressure: Securing P2P networking", *Network Magazine*, vol.17, no.2, February, 2002.

[6] Simon Kilvington, "The dangers of P2P networks", *Computer Weekly*, Sept 20, 2001.

[7] Idota, Hiroki, "The Issues for Information Security of Peer-to-Peer", *Osaka Economic Papers*, vol.51, no.3, December 2001.

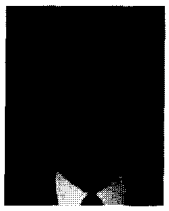
〈著者紹介〉

김 봉 한 (Bong-han Kim)
정회원

1994년 2월 : 청주대학교 전자계산학과 졸업
1996년 2월 : 한남대학교 전자계산공학과 석사
2000년 2월 : 한남대학교 컴퓨터공학과 박사
2001년 3월~현재 : 청주대학교 컴퓨터정보공학과 전임강사
관심분야 : 컴퓨터네트워크, 멀티캐스트, 정보보호

임 명 현 (Myung-hyun Lim)

2000년 : 조선대학교 전자계산학과(이학사)
2002년 : 조선대학교 전자계산학과(이학석사)
2002년 1월~현재 : 한국정보보진흥원 해킹·바이러스상담지원센터 연구원
관심분야 : 컴퓨터 해킹·바이러스, 바이오인포매틱스, 유전자알고리즘



임 재 명 (Jae-myung Lim)
1981년 : 한양대학교 전자공학과 (학사)
1983년 : 한양대학교 전자공학과 (석사)
1991년 : 한양대학교 전자공학과 (박사과정수료)
2000년~현재 : 한국정보보호진흥원 해킹·바이러스상담지원센터 센터장
관심분야 : BIOS, 인터넷 네트워크 트래픽, QOS, RTOS, 컴퓨터 해킹·바이러스

이 재 광 (Jae-kwang Lee)
종신회원
1984년 : 광운대학교 전자계산학과 졸업
1986년 : 광운대학교 대학원 전자계산학과 석사
1993년 : 광운대학교 대학원 전자계산학과 박사
2002년~현재 : 한남대학교 컴퓨터공학과 정교수
관심분야 : 컴퓨터 네트워크, 정보통신 정보보호