학 사 학 위 논 문

파일 불법 송수신 대응에 대한 연구

지 도 교 수
유승재 교수님

중부대학교 정보보호학과

마상준

2015

◆◆목　　차◆◆

연구요약

본 논문은 파일 불법 송수신에 대응하기 위한 연구이다.

서문에서는 산업기술 유출과 개인정보 유출에 대해 사례를 바탕으로 이에 대해 문제성을 제기하여 내부에서 외부로의 파일 불법 송수신에 대한 방지를 위한 대응을 목표를 기술하였다.

2장 관련연구에서는 파일 송수신시 파일적 특성과 송수신에 대한 특성에 따라 크게 파일, 포트, 패킷으로 총 3개의 장으로 구성하였으며, 각 장은 각 성질에 따른 특징을 바탕으로 다양한 가능성을 시작으로 차단기법을 연구하였다.

각 절은 가능성에 대해 각각의 결과를 도출하고 이해를 중점으로 전개하였다.

첫 장은 파일의 특성에 따른 파일의 크기, 이동과 복제, 확장자, 접근권한에 대해 제시하였으며, 다음 장인 포트에서는 다양한 가능성을 원초적으로 차단할 수 있는 방식을 연구하였고, 마지막 패킷의 장에서는 파일을 불법으로 송수신시 패킷을 감지할 수 있다는 것을 인지시키도록 연구하였다.

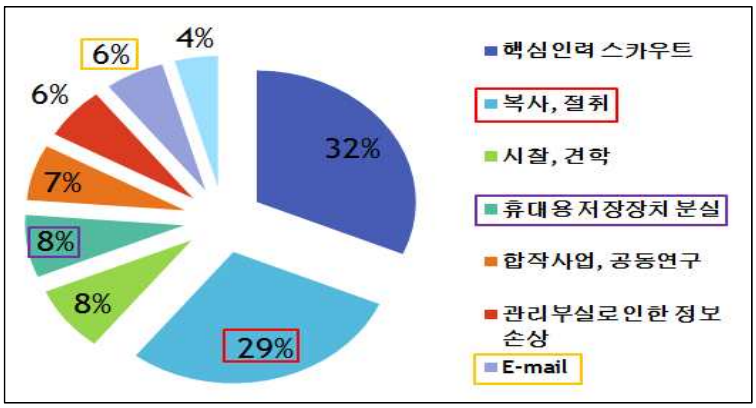
3장 본론에서는 앞의 관련연구로부터 연구한 차단기법을 통해 이것에 따른 OS자체에서 지원하는 서비스에 의한 차단방법을 제시하였다. 크게 Windows8와 Solaris10를 예시로 하였다.

마지막으로 4장 결론으로 이번 연구를 하게 된 목적에 대해서 다시 상기시키며, 이 논문을 토대로 전달하고자 하는 말로 마무리하였다.

1장 서론

현재 우리나라 전국에는 약 360만 사업체가 존재하며, 산업기술 유출 피해가 10년간 약 500조에 달한다. 이는 천문학적 비용이 든 기술들이 해외로 유출되면서 기술격차를 단숨에 추월 당할 뿐만 아니라, 방위산업, 전략물자 기술 유출은 국가안보에 위협이 되고 있다.

지식경제부에서는 산업기술의 유출을 방지하기 위하여 「산업 기술의 유출방지 및 보호를 관한 법률 제5조 [종합계획의 수립·시행] ①지식경제부장관은 산업기술의 유출방지 및 보호에 관한 종합계획을 수립·시행하여야한다」에 따라 3년마다 종합계획을 수립·시행하고 있어, 이에 산업기술 보호에 따른 산업기술 보호에 대한 기본적 보호체계가 정립되어 가고 있다[1]. 그러나 국가 핵심기술 보유기관 실태조사결과 대기업 및 공공연구기관의 보호역량은 상대적으로 양호하나 중소기업은 위험수준이라고 판단했으며, 기술유출은 온라인 보안 망 침입 등의 물리적 방법보다 내부자를 통한 유출이 다수라고 보고하였다[2][3].



< 그림1. 산업기술 유출수단 >

근래에 들어 시간이 흐를수록 개인 정보에 대한 중요성이 증대하고 있다. 웹사이트 해킹에 따른 개인정보 유출과 대기업 및 중소기업에서의 비밀리에 개인정보를 판매에 의한 유출 사건들이 연속적으로 벌어짐에 따라 대형 유출사건들이 이슈화됨으로서 개인정보보호에 대한 관심과 중요성이 증대되고 있으며, 또한 개인정보의 무분별한 사용을 자제하기 위해 정부차원에서 여러 가지 정책적

대안들이 제시되는 등 많은 노력들이 이루어지고 있다.

개인정보 침해가 이루어지는 범위는 크게 5가지로 개인정보 유출, 개인정보 매매, 개인정보 오·남용, 홈페이지 노출, 허술한 관리/방치들로 나뉘며 이에 따른 손실은 다음 <표1>과 같다[4].

< 표1. 개인정보침해에 따른 손실 >

구분	손실
개인	정신적 피해 및 명의도용, 보이스피싱에 의한 금전적 손해, 유괴 등 각 범죄에 노출
기업	기업의 이미지 실추, 소비자단체 등의 불매운동, 다수 피해자에 대한 집단적 손해배상시 기업경영에 큰 타격
국가	프라이버시 라운드의 대두에 따른 IT산업의 수출애로, 전자정부의 신뢰성 하락, 국가브랜드 하락

이처럼 개인정보 침해에 따른 손실은 많은 피해를 이루며 실제 보도된 유출사례들이 수없이 많으며, 또한 이들은 USB 등 다른 저장매체에 의한 유출, E-Mail을 이용한 개인정보의 송신, 해킹으로 인한 개인정보 데이터의 송신 등으로 발생하며 개인정보 유출은 개인의 도덕성과 보안의식 수준에 따른 문제야기이며, 직접적인 유출 경로에 대한 방지가 필요하다.

2. 관련연구 (특성 및 차단기법)

오늘날 정보화시대에 들어 모든 개인정보 및 사업, 기밀 정보들이 데이터화 되어 파일로서 저장된다. 이전은 문서로 기록하여 저장했지만 현재는 우리 주변에서 컴퓨터라는 기기가 우리 생활에 스며들어 모든 것을 처리하는 도구로 쓰여지고, 문서 또한 컴퓨터에 의해 파일로서 기록된다. 이로 인하여 우리는 컴퓨터 속의 파일에 대해서 보호할 조치가 필요해졌으며, 이를 보호하기 위해 유출에 따른 차단방식에 대해 연구 및 방법을 알리고자 한다.

파일이 유출되는 경로는 개인 컴퓨터에서 외부, 크게 하나의 사업체의 내부 네트워크에서 외부 네트워크로 유출되는 경우로 볼 수 있다. 따라서 내부 네트워크에서 외부 네트워크로의 송수신이 발생할 수 있는 경우에 대해서 연구하였다.

파일의 특성으로는 먼저 파일이란 '하나의 단위로서 처리되는 서로 관련 있는 레코드의 집합'이다. 이는 집합으로서의 크기를 지녔다는 것이다. 두 번째로 컴퓨터에서 파일은 각 파일의 용도와 성격에 따라서 확장자라는 것을 지니고 있다. 이는 컴퓨터가 인식하기 편한 다른 응용프로그램으로부터의 호환을 위한 구분자로 쓰인다. 따라서 파일의 특성으로 인한 방법에 대해서는 파일크기와 확장자에 대한 유출 송수신의 확인을 연구해보고자 한다.

다음으로는 네트워크의 특성이다. 네트워크에서 다른 네트워크와 연결될 시에 이는 하나의 연결된 구멍 즉 포트라는 것을 이용하여, 다양한 정보들을 주고받는다. 두 번째 특성으로는 네트워크에서는 데이터 전송 즉 상호간의 연결 사이에서 신호를 패킷이라는 하나의 단위로 된 집합체를 전송하며 이루어진다. 이 패킷은 다양한 종류가 있으며, 또한 이 패킷 안에는 다양한 정보와 송수신 될 데이터가 들어있다. 따라서 우리는 네트워크에 특성으로 인한 방법으로 포트라는 연결구멍에 대한 연구와 패킷이라는 데이터의 특성에 따른 연구를 해보고자 한다.

또한 위와 같은 연구를 통하여 각 차단을 할 수 있는 방식을 연구하고, 그 방법에 따른 대응방법을 강구할 것이다.

2.1 파일

파일은 다양한 특성을 지닌다. 보조기억장치에 저장된 데이터 모임으로서 확장자를 통한 응용프로그램에 의해 우리에게 접해지는 문서, 소리, 영상, 그림 파일들이 대표적인 것으로 이를 토대로 다른 네트워크 간의 이동, 복사가 가능하며, 자체적으로 읽기, 쓰기, 실행 등이 가능해지며 크기를 지녔다.

2.1.1 기초이론

⑴ 파일(File)

데이터의 모임으로서 보조기억 장치에 저장된 것을 말한다. 즉 문서, 소리, 그림, 동화상 등의 자료를 모아놓은 것이다.

파일은 컴퓨터의 하드디스크나 플로피디스크의 보조기억장치에 일정한 형식을 가지고 저장되며, 문자나 숫자 등으로 이루어진 파일인 텍스트파일과 프로그램 파일인 이진파일들이 있다. 또한 파일은 각각마다 이름이 있고, 확장자로 그 종류를 구분한다.

⑵ 파일크기

파일크기는 컴퓨터 파일의 크기를 측정한다. 보통 바이트로 측정된다. 파일을 저장할 때 쓰이는 디스크 공간의 실제 범위는 파일 시스템에 따라 다르다. 최대 파일 크기는 크기 정보를 저장하기 위해 남겨진 비트의 수에 따라 달라진다. 이를테면, FAT32의 경우 파일 한 개의 크기가 4 기가바이트를 초과할 수 없다.

< 표2. 파일 사이즈 단위 >

이름	기호	2진 측정값	10진 측정값	바이트 수	같은 값
킬로바이트	KB	2^{10}	10^{3}	1,024	1,024 Byte
메가바이트	MB	2^{20}	10^{6}	1,048,576	1,024 KB

기가바이트	GB	2^{30}	10^{9}	1,073,741,824	1,024 MB
테라바이트	TB	2^{40}	10^{12}	1,099,511,627,776	1,024 GB
페타바이트	PB	2^{50}	10^{15}	1,125,899,906,842,624	1,024 TB
엑사바이트	EB	2^{60}	10^{18}	1,152,921,504,606,846,976	1,024 PB
제타바이트	ZB	2^{70}	10^{21}	1,180,591,620,717,411,303,424	1,024 EB
요타바이트	YB	2^{80}	10^{24}	1,208,925,819,614,629,174,706,176	1,024 ZB

⑶ 파일확장자

파일 확장자는 컴퓨터 파일의 이름에서 파일의 종류와 그 역할을 표시하기 위해 사용하는 부부분이다. 간단히 확장자라고도 한다. 많은 운영체제들은 파일 이름에서 마지막 점(.) 뒤에 나타나는 부분을 확장자로 인식한다. VMS, CP/M과 그로부터 파생된 도스 등의 운영체제에서는 확장자가 실제로는 파일 이름과 분리되어 있으며, 확장자를 실행 파일을 나타내는 등의 특수한 용도로 사용한다. 반면 유닉스 계열 운영체제들은 확장자가 파일 이름의 일부분일 뿐으로, 도스 등의 운영체제보다는 확장자에 덜 의존한다.

마이크로소프트 윈도, OS X, 그놈, KDE 등의 여러 그래픽 사용자 인터페이스(GUI)에서는 파일 확장자를 단순히 종류를 나타내는 것뿐만이 아니라 인터페이스 상에서 파일의 아이콘이나 그에 연관된 작업들을 결정하는 데 사용한다. 예를 들어서 특정한 파일을 열었을 때, .txt 확장자는 텍스트 편집기를 .htm이나 .html 확장자는 웹 브라우저를, .png, .gif 등의 확장자는 그래픽 편집기를, .doc, .odt 등의 확장자는 워드 프로세서를 실행하는 등의 동작을 지정할 수 있다. 특히 마이크로소프트 도스와 윈도 운영체제에서는 .exe, .com, .bat, .cmd 등의 확장자를 가진 파일을 실행 파일로 인식한다. 이런 특성 때문에 파일 확장자는 일종의 메타데이터로 볼 수 있다.

2.1.2 차단방식기법

먼저 파일간의 송수신 될 수 있는 환경에 대해서 논하고자 한다. 여기서 연구하자 하는 것은 인트라넷과 인터넷, 인터넷과 인터넷간의 차단에 대해서 연구하려 한다. 인트라넷만 사용되어지는 네트워크상에서는 내부간의 자료교환이기에 유출에 대해서 신경 쓸 필요가 없다. 따라서 인트라넷과 인터넷이 공동으로 쓰여지는 단절되지 않은 네트워크와 인트라넷이 사용되어지지 않은 인터넷을 이용하는 네트워크를 논하고자 한다.

파일의 크기는 아무것도 쓰여지지 않은 빈 파일 0 Byte부터 FAT32방식 경우의 4 GB까지 파일크기가 측정된다. 텍스트 파일의 경우는 숫자, 영문자, 특수문자는 글자 수당 1 Byte로 측정되며, 한글의 경우에는 2 Byte로 측정된다. 이를 토대로 내부 네트워크에서 외부 네트워크로 유출시 파일 크기 x Byte가 전송될시 파일을 차단하는 방식이다.

파일은 각 파일의 특성에 따라서 위의 텍스트 파일과 같은 형식으로 크기가 측정되는데 이 크기란 것은 어떠한 정보가 들어 있다는 가정 하에 혹은 암호로 되어있다 가정 하에 평균 최소 문자열인 한 단어가 되어있을 때 abcd 4Byte에 대한 차단을 요하려 한다. 또한 한 수 더 나아가 지능적으로 이를 피하기 위해서 한 문자씩 여러 차례에 걸쳐 전송한다고 가정하였을 때 1 Byte씩 송신될 가능성이 존재한다. 또한 2진 단위인 bit 단위로 송신될 경우도 존재한다.

이 파일에 대한 크기를 지닌다는 특성으로 원초적인 차단을 하는 방법에 대해서 강구해 보면 파일이란 크기를 지녔고 이것은 보조기억장치에 저장된다. 이 기억장치는 크기 즉 용량을 지녔으며, 파일 또한 용량을 지녔다. 따라서 용량의 변동사항에 대한 차단을 연구하였다.

파일은 기억장치에서 이동할 수 있는 방식은 이동과 복제가 존재한다.

먼저 이동은 말 그대로 파일을 이동시키는 경우로 파일이 보조기억장치에 들어있을 때에서 외부로 나갔을 시 즉 이동이 되었을 때 크기가 줄게 되어있다. 따라서 데이터 장치의 크기가 변동사항이 있을 시 이는 유출 되었다라고 판별할

수 있다.

복제의 경우는 파일을 있는 그대로 복제하여 똑같은 파일을 만드는 경우이다. 이는 용량의 변화가 없기에 유출 유무를 판단할 수 없지만 파일의 크기와 상관없이 유출경우는 판단내릴 수 있다. 이는 물리적 데이터 전송매체인 USB, 플로피 디스크 경우에는 물리적인 인터페이스를 다루는 것과 내부 혹은 외부간의 네트워크상에서도 복제를 하는 경우도 확인할 수 있으며, 이는 2.3.2 패킷의 차단방식 연구에서 다루며, 추가적으로 파일의 크기와 패킷의 크기는 각각 파일은 0 Byte부터 최대 FAT32 경우 4 GB까지 크기를 지녔으며, 이를 네트워크간의 이동시에 패킷을 통해 이동하게 되는데, 패킷의 최대 크기는 6.5 KB 이다.

다만 6.5 KB 이상은 패킷이 아니라 데이터 파일이라고 할 것이라 생각하기 쉽지만 데이터 이동은 우리가 보기에는 인터페이스상 한번에 그 파일이 이동되는 것으로 보이지만 실제로는 패킷을 통해 파일이 여러 데이터로 분할되어 나뉘고, 이는 여러 번 전송이 되어 다시 하나의 파일이 완성되는 것이다. 이를 바탕으로 파일 전송 시작 전 패킷의 크기부터 완료시까지의 패킷의 크기의 합으로 유출되었다라고 판단될 수 있으나 이는 파일전송이 시작되는 순간부터 패킷을 감지했기에 이는 해당사항이 되지 않는다.

다음으로는 파일은 확장자를 지닌다는 특성에 대한 연구이다. 각 파일은 특성에 따라 각각의 확장자를 지니고, 유출될 가능성 즉 정보를 가지고 있는 파일들의 특성들이 지니고 있는 확장자를 제한해보는 것에 대해 연구해보려 한다.

먼저 업무에 있어서 사용되는 것은 주로 문서이다. 또한 데이터들이 보고되고 저장되는 것은 문서이다. 일반적으로 업무상 사용 되어지는 것은 다음의 서식 파일들이다. 첫 째로 한국에서 제일 많이 쓰이는 .hwp 한글문서이다. 국내에 국한되는 텍스트 편집기로 한글에 대한 다양한 표현을 이루며, 텍스트 및 표 등 문서작성에 있어서 한글에 맞춰 특성화된 텍스트 편집기이다. .doc, doc, odf 등 다양한 파일 형식과 호환을 지원하나 주로 .hwp로 사용되어짐에 따라 한글파일인 .hwp이 주된 문서 확장자이다.

두 번째는 MS오피스의 지원되는 확장자들이다. MS 오피스는 Window에서 주

로 쓰일 여러 특성의 편집기를 지원하며, 간단하게 설명하자면 한글과 같이 문서 편집기로 주로 쓰이는 MS-WORD는 .doc, .docx의 확장자를 지닌다. 또한 숫자형식의 계산식 도표 등에 특성화된 MS-EXCEL이 있으며 이는 .xls, .xlsx이 대표적으로 쓰인다. 그리고 MS-PowerPoint는 프리젠테이션에 특성화된 서식파일로 .ppt, .pptx의 확장자로 쓰인다.
그 외 Publisher, Access, OneDrive, OneNote, Outlook 등 다양한 서식환경을 제공하지만 주로 쓰이는 것은 위의 3가지 Word, Excel, PowerPoint이다.

세 번째는 어도비시스템즈에서 만든 PDF 파일이다. PDF는 문서파일 형태로 윈도우, 맥, 유닉스, 안드로이드 등 거의 모든 운영체제에서 읽거나 인쇄할 수 있으며 원본 문서의 글꼴, 이미지, 그래픽, 문서 형태등이 그대로 유지되는 디지털 문서의 표준이 되는 파일이다. 보안성이 높아 공공기관, 구소 등에서 자료 배포용으로 쓰이며, 인쇄업에서도 주로 쓰이는 형식이다. pdf 파일은 .pdf의 확장자를 지닌다.

위 와 같이 3가지의 특성의 형식 파일들이 주로 쓰이며 이 확장자라는 특성을 가지고 차단하려 하고, OS 자체적으로 지원하는 서비스에는 차단할 수 있는 방법은 없다. 다만 이를 추가적인 소프트웨어적으로 차단을 하던가 혹은 응용단에 첨부형식으로 차단이 가능하다.

확장자에 따른 차단방식은 큰 문제점이 있다. 먼저 확장자라는 것은 파일의 특성에 따른 응용프로그램으로 실행이 가능하도록 구분지어 놓은 것이다. 이는 즉 확장자가 변경되어도 파일은 유지 된다는 것이다. 이것이 무엇을 의미하는지는 다음과 같다.

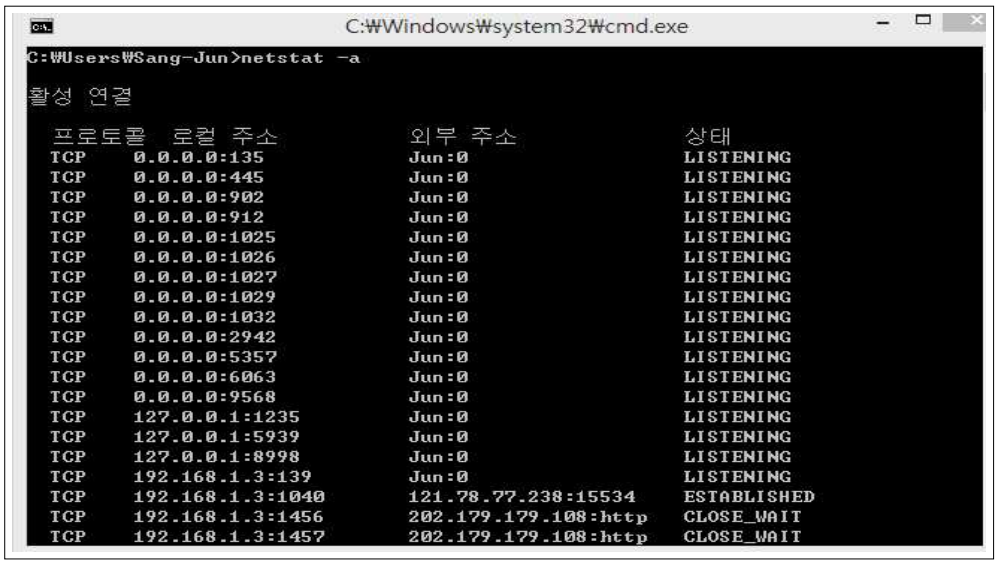
먼저 여러OS에서는 파일의 확장자를 볼 수 있도록 되어있다. 또한 파일명 변경시 확장자 또한 변경이 가능하게 되어있다. 이는 즉 예를들면 확장자가 .hwp인 파일을 .hwpp로 변경한다면 이는 실행시 파일이 한글 파일로 열리지 않으며 실행가능 한 응용프로그램을 찾지 못하고 나오지만, 파일자체가 존재한다는 것이다. 또한 이는 파일이 일부 확장자 변경으로 인하여 변경 과정에 내용이 손실되는 부분이 있지만 대부분 내용은 그대로 보존되어 있으며, hwpp를 다시 .hwp로 변경하여 파일을 실행한다면 한글파일로 처음 그대로 내용이 보존된

채 열람이 가능하다. 따라서 파일 확장자로 차단할 시에는 이 차단이 되어있는 확장자를 제외한 그 외의 확장자로 변경하여 이동이나 복제가 가능하다는 점이다. 따라서 이 확장자의 경우는 특정의 확장자와 추가적으로 불특정 인식되지 않은 확장자에 대한 차단을 취하여야 한다는 것이 전제이며 결론적으로 이는 모든 확장자에 대해서 차단하지 않을 확장자에 대해서만 실행 권한을 주어주며, 그 외는 차단하는 방식이 합당하다고 여겨진다.

2.2 포트

네트워크상에서 파일이 유출되는 경로는 반드시 연결 통로인 포트를 통하여 PC에서 외부 장치로 나가게 된다. 이 포트란 것은 컴퓨터의 주변 장치를 접속하기 위해 사용되는 연결 부분에 해당되며 또한 직접전 연결이 아닌 다른 네트워크 간의 연결되는 연결 통로이다.

활성화된 포트를 확인하는 방법은 커맨드(cmd) 창에 'netstat -a' 명령어를 입력하면 활성화된 네트워크 연결정보를 볼 수 있다.



< 그림2. 활성화된 네트워크정보 >

여기서 로컬 주소와 외부 주소를 보면 x.x.x.x:xxxx 로 되어있는 부분이 보일

것이다. 여기서 이 앞의 x.x.x.x 는 주소에 해당되는 네트워크 IP 주소이며, 그 뒷부분 :xxxx가 해당 포트 번호이다. 또한 상태에 Listening 은 포트가 열려있단 것을 의미하며, Close_wait은 포트가 끊어진 상태로 대기 중이라는 것이며, Established 는 연결 중 상태를 의미한다.

2.2.1 기초이론

⑴ 포트(Port)

컴퓨터에서 포트는 크게 두 가지 의미를 지닌다. 첫째는 컴퓨터의 주변장치를 접속하기 위해 사용되는 연결 부분을 의미한다. 대게 소켓이나 플러그 등의 형태로 되어 있다. 정보가 드나드는 출입구로, 주로 프린터를 접속하기 위한 센트로닉스 등의 병렬포트와 기타 주변장치를 접속하기 위한 RS-232C 등의 직렬포트가 있다.

둘째, 프로그래밍에서는 논리적인 접속장소를 뜻한다. 특히 TCP/IP를 사용할 때에는 클라이언트 프로그램이 네트워크상의 특정 서버 프로그램을 지정하는 방법으로 사용된다. TCP/IP의 상위 프로토콜을 사용하는 응용프로그램에서는 인터넷번호 할당 허가위원회(IANA)에 의해 미리 지정된 포트번호들을 가지고 있다. 이런 포트번호들은 '잘 알려진 포트들'이라고 불린다. 다른 응용프로그램 프로세스들은 접속할 때마다 포트번호가 새로 부여된다. 포트번호는 0부터 65535까지이며, 0부터 1023까지는 어떤 특권을 가진 서비스에 의해 사용될 수 있도록 예약되어 있다. HTTP서비스를 위해서는 대개 80번 포트가 지정된다.

포트번호는 잘 알려진 포트(Well known ports): 0~1023, 등록된 포트(Registered ports): 1024~49151, 동적 포트(Dynamic or Private ports): 49152~65535 으로 지정되어 있다.

⑵ 잘 알려진 포트(Well known ports)

잘 알려진 포트는 특정한 쓰임새를 위해서 IANA에서 할당한 TCP 및 UDP 포트 번호의 일부이다. 이 포트 번호는 강제적으로 지정된 것은 아니며, IANA의 권고안 일 뿐이다. 가끔 각 포트 번호를 그대로 사용하지 않고 다른 용도로 사

용하는 경우도 있다. 예시로 트로이 목마와 같은 악의적인 목적의 프로그램들이 포트를 변경하여 사용하는 경우도 있다.

< 표3. 잘 알려진 포트 번호 >

포트	TCP	UDP	설명	상태
7	✓	✓	ECHO 프로토콜	공식
9	✓	✓	DISCARD 프로토콜	공식
13	✓	✓	DAYTIME 프로토콜	공식
20	✓		FTP(파일 전송 프로토콜) - 데이터 포트	공식
21	✓		FTP - 제어포트	공식
22	✓		SSH(Secure Shell) - ssh scp, sftp 같은 프로토콜 및 포트 포워딩	공식
23	✓		텔넷 프로토콜 - 암호화되지 않은 텍스트 통신	공식
25	✓		SMTP(Simple Mail Transfer Protocol) - 이메일 전송에 사용	공식
53	✓	✓	DNS(Domain Name System)	공식
69		✓	TFTP	공식
80	✓	✓	HTTP(HyperText Transfer Protocol) - 웹 페이지 전송	공식
109	✓		POP2(Post Office Protocol version 2) - 전자우편 가져오기에 사용	공식
110	✓		POP3(Post Office Protocol version 3) - 전자우편 가져오기에 사용	공식
123		✓	NTP(Network Time Protocol) - 시간동기화	공식
143	✓		IMAP4(인터넷 메시지 접근 프로토콜 4) - 이메일 가져오기에 사용	공식
161		✓	SNMP(Simple Network Management Protocol)	공식
194	✓		IRC(Internet Relay Chat)	공식
443	✓		HTTPS - HTTP over SSL (암호화 전송)	공식
465	✓		SSL 위의 SMTP - Cisco 프로토콜과 충돌	비공식
514		✓	syslog 프로토콜 - 시스템 로그 작성	공식
515	✓		LPD 프로토콜 - 라인 프린터 데몬 서비스	공식
587	✓		email message submission (SMTP) (RFC 2476)	공식
591	✓		파일메이커 6.0 Web Sharing (HTTP Alternate, see port 80)	공식
636	✓		SSL 위의 LDAP (암호화된 전송)	공식
993	✓		SSL 위의 IMAP4 (암호화 전송)	공식
995	✓		SSL 위의 POP3 (암호화 전송)	공식

2.2.2 차단기법연구

네트워크상에서의 포트를 차단하는 방식에 대해 연구하고자 한다. 위의 이론부에서 설명하였듯이 사용 되어지는 포트들이 지정되어 있다. 대표적으로 잘 알려진 포트가 존재하며, 그 외에는 프로그램마다 특정 포트를 이용하여 서로간의 송수신을 한다.
대표적으로 파일 전송 프로토콜인 FTP는 20번 데이터포트를 통해 파일을 송수신하게 된다. 이 부분에 대해서는 한정적 제한을 두려고 한다. 한정적 제한이라는 것은 다른 포트의 경우 데이터를 송수신하는 경우에 데이터 즉 파일 송수신 포트를 임의로 설정이 가능하게 되어있다. 따라서 대표적인 파일 송수신 포트이기에 임의의 포트를 설정하는 것이 아닌 20번 포트만을 한정적 이용하기 때문에 이를 한정적 제한이라는 표현을 사용하였고, 단순히 차단하는 방식으로 파일의 유출 위험성을 차단할 수가 있다. (또한 추가적으로 25번 포트 SMTP 메일에 의한 첨부 기능을 차단하는 것 또한 이와 동일하다.)
이렇게 잘 알려진 포트번호는 위와 같이 그 해당 번호만 단순히 차단을 시키면 된다. 문제는 그 외의 포트의 경우이다. 프로그램 마다 사용되어지는 포트번호는 다르며, 이를 사용하는 경우에만 알 수 있기 때문에 추가적인 프로세스에 대한 포트번호는 추가 조사가 필요하다. 또한 파일송수신 포트는 임의로 변경이 가능하다는 점이다.

대표적인 예시로 아래 <그림3>은 한 메신저의 네트워크 연결 설정의 사진이다.

< 그림3. 메신저의 네트워크 연결설정 예시[5] >

위의 사진과 같이 연결 포트를 임의로 설정이 가능하게 되어있으며, 결과적으로 임의의 포트를 알아내서 차단하는 방식은 그 특정 프로그램의 포트를 일일이 알아내야 한다는 단점에 이어서 위와 같이 포트설정이 임의로 설정이 가능하기 때문에 특정 포트를 막는 것을 통해 파일 유출을 방지한다는 것은 불가능하다. 따라서 잘 알려진 포트 중에서 파일 송수신이 가능한 포트를 제외한 나머지 포트를 허용하고 그 외의 나머지 포트는 차단하면 된다.

1) 잘 알려진 포트 중에서 FTP, SMTP 포트 각 20, 25번 포트를 제외한 포트만 허용한다.
2) 결론적으로 FTP, SMTP 포트와 불특정한 알려지지 않은 포트에 대해서 모든 포트를 차단한다.
* 추가적으로 필요한 포트가 생기는 경우에는 그 해당 포트만 추가하여 허용하면 된다.

2.3 패킷

패킷은 네트워크상에서 데이터가 오갈 때 쓰이는 집합체로, 이는 데이터를 포함하며, 이번 연구의 목표인 파일 송수신시에 생성되는 패킷에 대해 연구할 것이며, 이론부에는 구체적인 이론이 아닌 연구에 필요한 간단한 이해를 요하는 부분에 대해서 간략히 기술하였다. 예를 들면 다음 설명할 1-2의 TCP, UDP 부분에서 헤더부분에 대한 설명은 생략하였으며, 전송과정의 특징에 대해서만 간략히 기술하였다.

2.3.1 기초이론

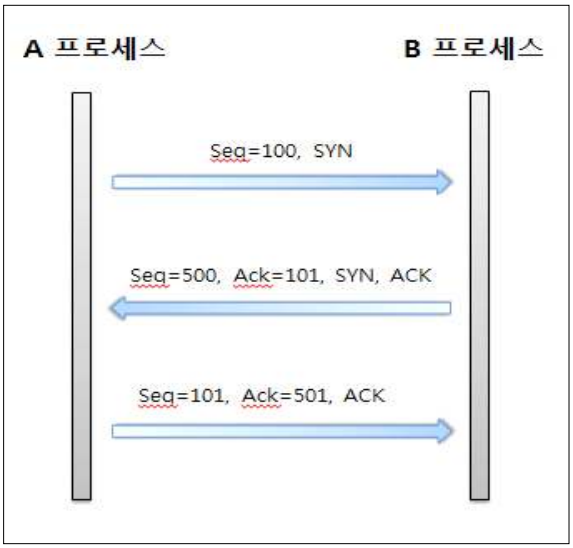
⑴ 패킷(Packet)

패킷은 소포를 뜻하는 용어로, 소화물을 뜻하는 패키지(Package)와 덩어리를 뜻하는 버킷(Bucket)의 합성어로, 우체국에서는 화물을 정당한 덩어리로 나눠 행선지를 표시하는 꼬리표를 붙이는데, 이러한 방식을 데이터통신에 접목한 것이며, 데이터 전송에서 송신측과 수신측에 의하여 하나의 단위로 취급되어 전송되는 집합체를 의미한다.

파일은 전송시 분할하여 패킷의 데이터에 붙어 전송되고 수신하는 곳에서는 원래의 파일로 다시 재조립하는 과정을 거치며, 패킷은 헤더와 데이터·테레일러로 이루어져있는데, 헤더에는 데이터가 전달될 주소와 순서 등이 기록되고, 테레일러에는 에러 정보가 기록된다. 보통 2계층으로 내려가기 전까지 3·4계층의 데이터 단위는 패킷이라 하고, 1·2계층의 데이터단위는 프레임이라고 한다.

⑵ TCP / UDP

TCP와 UDP는 전송계층에 해당하며 통신 노드간의 연결을 제어하고, 자료의 송수신을 담당하는 프로토콜이다. 먼저 TCP는 스트림 전달 방식으로 버퍼를 이용해 패킷을 전달한다. 수신측에서 버퍼의 패킷순서를 검사하여 오류를 검사하며, 패킷 전송이 끝나면 프로세스 메시지를 전달하는 과정을 갖는 연결지향형 프로토콜로 신뢰성과 순서를 보장하며, 에러 및 흐름제어가 가능하다. 또한 3-way handshaking이라는 3단계 설정을 통해 연결을 한다.



< 그림4. TCP 3-way handshaking 과정[6] >

위 <그림 4>에서 나타난 것과 같이 3-way handshaking과정은 먼저 1단계는 A 프로세스는 TCP헤더에 SYN 플래그를 지정한 세그먼트를 전송하여 연결 설정을 요구하고, 2단계는 B 프로세스가 연결을 수락하려면 SYN 세그먼트의 순서번호에 1을 더해 ACK 플래그를 지정하며, 다시 SYN 플래그에 임의의 세그

먼트를 지정하여 A 프로세스에게 전송한다. 그러면 3단계로 이를 받은 A 프로세스는 이 연결수락 세그먼트를 잘 받았다는 세그먼트를 앞의 과정과 같이 전송하며, 만일 전송 데이터가 있을 시에 이를 포함하여 전송하게 된다.

다음으로 UDP는 세그먼트를 단순히 전달해주는 역할을 하는 비연결지향형 전송프로토콜로 신뢰도가 없으며, 주로 프로세스에서 사용되어 진다. 또한 UDP는 분실 오류를 복구하는 기능을 수행하지 않으며, 데이터 순서번호 기능을 제공하지 않은 단순한 송수신만 지원하기 때문에 이를 해결하기 위해서는 추가적으로 이를 사용하는 응용프로그램 내부에 구현된 기능을 이용하여야 한다.

⑶ NDIS Filter Driver

NDIS Filter Driver는 윈도우에서 지원하는 NDIS 윈도우 운용 시스템에서 지원하는 데이터 필터링 드라이버이다. 이는 보안 또는 다른 목적을 위한 데이터 필터링과 네트워크 데이터 통계를 모니터링하고 수집하는 용도로 이용되어지는데 이를 통해 패킷감지를 할 수 있다[9].
NDIS는 Network Device Interface Specification으로 NIC로부터 생성된 모든 트래픽 즉 패킷을 제2의 가상드라이버를 생성하여 이를 수신하며, 이 트래픽을 제어하기 위해 NDIS의 가상드라이버에 미니포트를 생성하여 운용하는 윈도우 운용 시스템 드라이버이다. 흔히 패킷 캡쳐에 사용되는 winpcap, wireshark 등의 소프트웨어들이 이를 이용한다. 이 NDIS Filter Driver는 윈도우에서 지원하지만 자체적으로 설치되어 있지 않으며, 이를 이용하기 위해서는 따로 설치가 필요하다.

2.3.2 차단기법연구

먼저 차단기법연구는 패킷을 통해 어떻게 차단할 것인가가 아닌 상황에 따른 패킷의 생성과 이를 파일 송수신인지 확인 가능한가에 대해 의의를 두었으며, 패킷을 통해 어떻게 하는가에 따른 패킷 분석 후 해당 부분을 조정하기에 앞서, 패킷이 생성된 순간 이를 감지 후 송수신을 막기 위함이다. 또한 이는 OS 자체적으로 지원되는 서비스는 없으며 추가적인 소프트웨어를 요구하기에 원리와 인식에 대해 연구하였다. 따라서 이론부에 NIC에서 생성되는 패킷을 감청이 가능한 점을 인식시키기 위해 NDIS에 대해 설명을 하였고, 이를 토대로 파일

송수신시의 패킷의 특징에 대해서 연구하였다.

1) 물리적 기억장치간의 데이터 이동
이는 파일의 이동에 대한 특성에 따른 차단방식에서 간략히 넘어간 부분이다. 물리적 기억장치로는 흔히 USB를 이용하는데 이에 대해 설명할 것이다. USB에서의 데이터 전송은 단일 호스트가 복수의 타깃 디바이스를 처리하고, 처리된 타깃이 응답하는 형태로 실행되며 이는 파이프를 통하여 데이터 전송이 진행되고, 전송모드는 4가지이며, 이는 엔드포인트의 설정에 의해 지정된다. 보통 리얼타임의 음성이 아닌 파일 송수신의 경우 패킷 당 최대 데이터 전송 크기는 64 바이트이다.

< 표4. USB 전송모드 >

항목	동시성 전송	벌크 전송	인터럽트 전송	컨트롤전송
주된 용도	음성 등의 리얼타임 전송	부정기적인 대용량 데이터 전송	정기적인 소용량 데이터 전송	셋업 데이터 전송
전송속도	12 Mbps	12Mbps	1.5Mbps /512 Mbps	1.5Mbps /12Mbps
데이터 전송 주기	1 ms(프레임)	부정	Nms(N=1~255)	부정
1패킷당 전송량	1~1023 바이트	8/16/32/64 바이트	1~64바이트 (풀) 1~8바이트 (로)	1~64바이트 (풀) 1~8바이트 (로)
데이터 에러시 재요구	없음	있음	있음	있음

USB의 패킷은 SOF(Start Of Frame) 패킷, 토큰 패킷, 데이터 패킷, 핸드셰이크 패킷으로 이루어 져있는데, 이들 패킷을 감청하여 캡쳐시 프로토콜은 USB로 잡히며, 각 세부 항목에 전송방식이 표기되고, 데이터들을 확인할 수 있다.

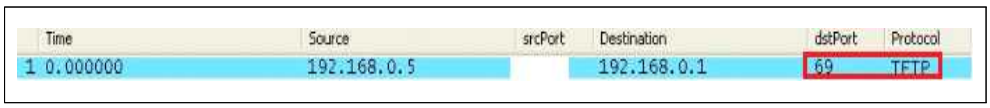
2) 네트워크상의 파일 송수신
네트워크상에서 파일 송수신에는 크게 두 가지가 있다. 먼저 잘 알려진 포트를 사용하는 FTP와 TFTP가 있으며, 두 번째로는 알려지지 않은 포트를 사용하는 다른 파일 송수신 프로그램을 이용하는 경우이다. 여기서 문제를 야기할 부분

은 후자의 알려지지 않은 포트를 이용하는 경우인데, 이 경우에 패킷을 감청 시 파일 송수신인지 알 수 있는가에 대한 부분이지만 이는 실제로 포트번호만 다를뿐 송수신 프로토콜은 동일하다. 또한 추가적으로 고려할 부분은 FTP 프로토콜이 감청되는 순간 이는 파일 송수신이 시작되는 것이 아닌가에 대한 것인데, 이는 TCP 포트번호 중 20번 포트인 FTP 데이터 포트인 경우 이미 파일 송수신이 진행이 되는 중이며, 21번 포트의 경우는 연결 대화 상자이다. 하지만 FTP의 경우 FTP 프로토콜 이전에 연결을 위해 TCP 프로토콜 패킷이 먼저 이루어지기 때문에 파일 송수신이 진행되기 전에 이를 감지할 수 있고, 또한 TCP 패킷 안에 FTP가 명시되어있다.

< 그림5. FTP 패킷 송신 전 TCP 패킷 >

위처럼 FTP 클라이언트의 명령어 패킷은 TCP 헤더 뒤에 존재하며 이를 토대로 FTP 파일 송수신전에 TCP 패킷으로 확인이 가능하다.

다음은 UDP 전송프로토콜을 이용하는 TFTP의 경우이다. TFTP는 잘 알려진 포트로 69번 포트를 이용하는데, 이는 패킷 감청 시 프로토콜에 TFTP로 확인이 가능하다.



< 그림6. TFTP 패킷의 포트와 프로토콜 감지 >

TFTP는 FTP처럼 시작 전 다른 프로토콜에 의해 파일 송수신을 미리 확인할 수는 없다. 하지만 TFTP는 UDP의 데이터의 신뢰성과 순서 제어 등의 오류와 관련된 기능을 지원하지 않기 때문에 TFTP 자체에 이 문제를 해결하기 위해 하나의 DATA 메시지에 대해 ACK 메시지 처리가 순차적으로 완료되게 설계되어 데이터 블록 전송을 하나씩 처리하는 흐름 제어 방식을 사용하고, 이 DATA와 ACK 메시지를 서로 송수신하기 전에 세션 연결을 위해 파일 이름과

모드 정보가 담긴 RRQ 메시지를 전송하는데, 이를 토대로 TFTP 프로토콜의 패킷을 캡쳐시 Info에 RRQ 정보가 담겨있으면 이를 토대로 해당 포트를 닫아버리면 된다.

결론적으로 패킷에 따른 차단 방법은 다음과 같다.
1. 파일 송수신에 해당되는 프로토콜의 바로 전단계의 프토토콜을 감지한다.
2. 정보를 확인하여 송수신이 확인되면 포트번호를 확인한다.
3. 해당 포트를 차단한다.

위와 같이 패킷 자체를 차단하는 것이 아닌, 해당 패킷을 통해 파일 송수신을 감지하고 포트를 차단하는 방식으로 이루어진다.

3장 파일 불법 송수신 차단방법

여기에서는 차단 방식에 따른 차단 방법에 대해서는 추가적인 소프트웨어나 프로그램에 의한 차단 방법이 아닌 PC 자체의 내장된 OS단의 차단 방법에 대해 언급하였다.

3.1 파일기반의 차단

3.1.1 파일크기에 따른 이동과 복사

보조기억장치 혹은 물리적인 장치의 크기 변동을 제한하는 것에는 큰 문제가 있다. 이는 장치의 내부에는 PC가 작동하면서 수많은 데이터들이 오가며 값이 주어지기 때문에 크기는 항상 변한다. 예를들면 PC를 키게 되면 PC에서는 OS를 띄운 후 사용자 시작시 각 사용자에 따라 시작프로그램이 구동된다. 이 시작 프로그램은 업데이트 혹은 작업에 따라서 그 파일의 크기가 변동되게 되는데, 이 는 그 장치의 크기 변동에 잠금을 걸어버리면 실시간으로 변경되는 아주 작은 단위의 값의 용량이 변하는 것을 막아버리고 결국 장비를 멈춘다는 것과 같다. 결국은 장치의 크기변동 자체를 차단하는 것은 사용하지 않는다와 상통 된다.

3.1.2 접근권한설정

파일이란 것은 각 OS의 파일시스템의 접근권한에 따라 파일을 이동, 복제가 불가능하게 설정이 가능하다.

접근권한이라는 것은 파일 시스템에서 사용자들이 널리 파일을 공유할 수 있도록 유연한 도구를 제공하고, 또한 이 파일의 보안을 위해 접근 방법을 제어할 수 있도록 다양한 선택사항을 제공한다.

접근권한은 크게 다음과 같은 그룹으로 나누어 접근권한을 설정한다.
- 특정 사용자(Specific user): 사용자 ID로 지명받은 개별 사용자들
- 사용자 그룹(User groups):개인적으로 지명받지 않은 사용자 단체. 이 경우

시스템은 각 사용자 그룹이 어떤 구성원들을 포함하고 있는지 알아낼 수 있어야 한다.

- 모든 사용자(All): 시스템에 접근할 수 있는 모든 사용자. 이는 공용 파일에 해당된다.

다음 <표5>은 각 특정 파일에 대한 특정 사용자에게 부여될 수 있는 대표적 접근권한이다.

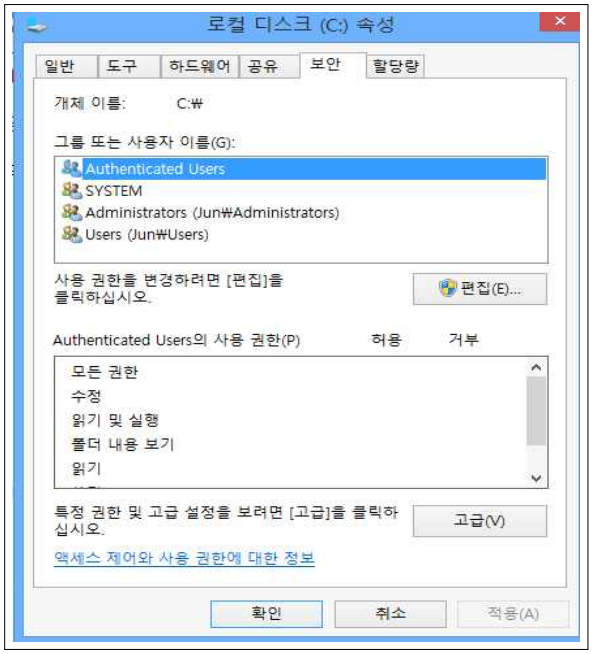
< 표5. 파일시스템의 대표적 접근권한[7] >

접근권한	설명
없음(None)	파일에 접근하지 못하며, 파일의 존재조차 알지 못할 수도 있다. 이런 제약을 설정하기 위해, 해당 파일을 포함하고 있는 디렉토리를 읽지 못하게 할 수도 있다.
인지(Knowledge)	파일이 존재한다는 것과 그 소유자가 누구인지 알 수 있어, 소유자에게 부가적인 접근권한을 요청할 수 있다.
실행(Execution)	프로그램을 적재하여 실행시킬 수 있지만 복사는 할 수 없다. 대개 개인소유 프로그램들에 대해 이와 같은 접근권한이 설정된다.
읽기(Reading)	어떤 목적(복사, 실행 등)으로든 파일을 읽을 수 있다. 어떤 시스템에서는 내용보기와 복사를 구분하는데, 이 경우 파일 내용을 볼 수 있지만 복사할 수는 없다.
첨가(Appending)	파일에 데이터를 첨가할 수 있는데, 종종 끝 부분에만 첨가할 수 있을 뿐, 파일 내용을 수정하거나 삭제할 수는 없다. 이 권한은 여러 출처로부터 데이터를 수집할 때 유용하다.
갱신(Updating)	파일 데이터를 수정·삭제·추가할 수 있다. 여기에는 파일에 대한 초기 쓰기나 완전 혹은 부분 되쓰기, 데이터 전부나 일부의 제거 등이 포함된다. 어떤 시스템에서는 갱신의 수준을 구분하고 있다.
권한변경(Changing protection)	접근권한을 변경하여 다른 사용자에게 부여할 수 있는 권한으로, 일반적으로 파일 소유자만 가진다. 어떤 시스템에서는 소유자가 이 권한을 다른 사람들에게 확대시킬 수 있다. 일반적으로 이 기법의 남용을 막이 위해, 이 권한의 보유자가 어떤 권한을 변경할 수 있는지 파일 소유자가 명시할 수 있을 것이다.
삭제(Deletion)	파일시스템으로부터 파일을 삭제할 수 있다.

여기서 주목해야 할 부분은 읽기 부분이다. 어떤 목적(복사, 실행 등)으로 파일을 읽을 수 있지만 어떤 시스템에는 내용보기와 복사를 구분하는 가운데, 파일 내용을 볼 수 있지만 복사할 수는 없다.

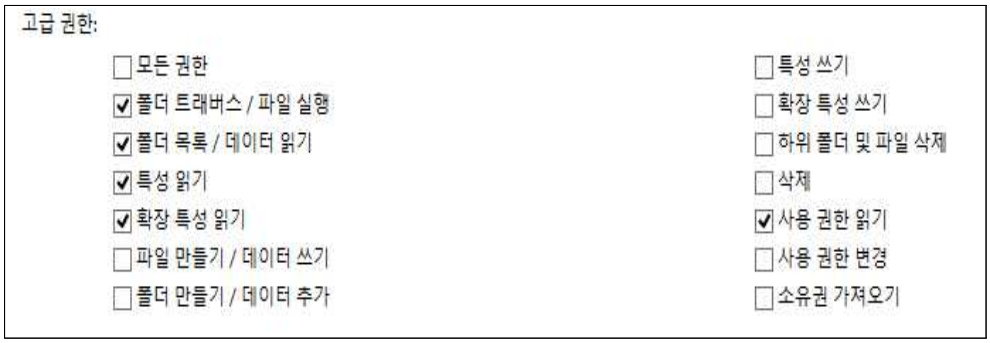
이것으로 접근권한제어를 통해 위의 파일 크기에 따른 이동 및 복사는 불가능하지만 이를 통해 OS 단에서 차단 할 수 있다.

A. 마이크로소프트 윈도우에서는 접근권한 설정 방법이다.(Windows 8)
내 컴퓨터에서 해당 로컬 디스크의 마우스 우측버튼 클릭 후 속성을 들어간 후 보안 탭을 들어가면 다음 <그림7>과 같은 권한설정이 나온다.



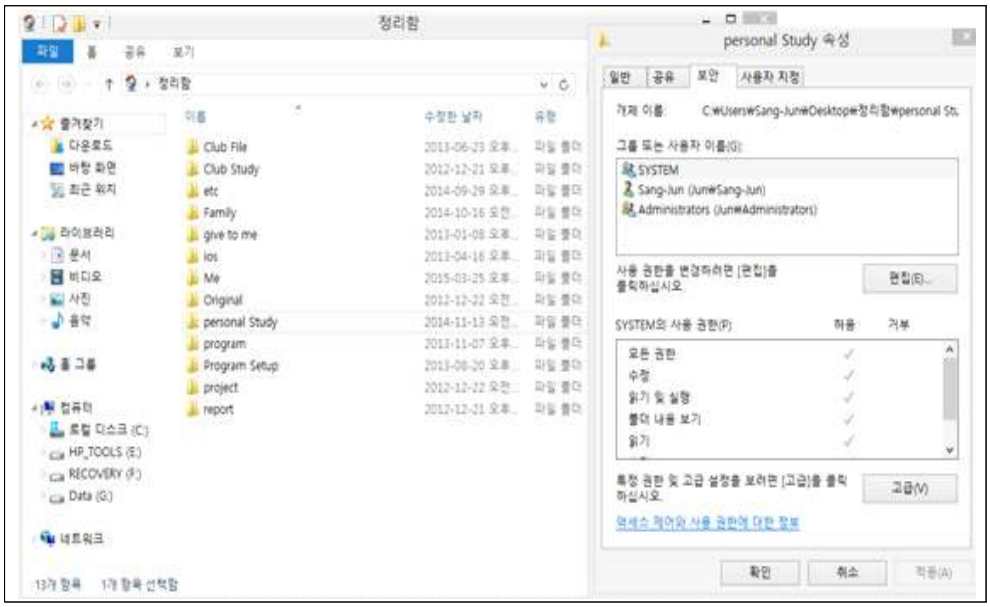
< 그림7. 속성 보안탭 >

이처럼 각 그룹, 계정에 따라 모든 권한, 수정, 읽기 및 실행 등 권한 설정이 가능하며 추가적으로 고급을 클릭하면 아래와 같은 특별한 권한설정이 가능하다.



< 그림8. 고급 권한 >

또한 위와 같은 권한설정은 디스크뿐 아니라 폴더 및 파일에서도 설정이 가능하다.



< 그림9. 폴더 권한설정 >

B. Linux / Unix의 파일 접근권한 설정이다.(Solaris 10)

Linux와 Unix 계열에서는 파일 허가권이란 것이 존재한다. 이는 즉 파일의 접근권한을 부여하는 것을 의미한다.

< 그림10. 솔라리스에서의 그룹 >

위 그림은 솔라리스의 그룹을 나타내며 이는 그룹이름::넘버::해당그룹의 이용자를 의미한다.

다음은 파일 즉 디렉토리들의 파일 허가권을 알아보자.
파일의 허가권 확인은 'ls -l' 명령어 입력을 통해 확인할 수 있다.

< 그림11. 솔라리스의 파일허가권 >

위 그림 <11>을 보면 맨 앞줄에 drwxr-xr-x 라는 것이 보이는데 이는 즉 파일 허가권을 의미한다.

-	rwx	r-x	r-x
File type	User	그룹	Others

* 여기서 나타내는 User란 파일을 생성한 자를 의미한다.
각 r, w, x에 대한 권한은 다음 <표6>과 같다.

< 표6. 파일의 권한 >

Permission	Sysbol	File	Directory
Read	r(4)	피일 읽기 및 copy 가능	ls 명령어로 디렉토리 리스트를 확인가능
Write	w(2)	파일의 내용을 수정 가능	디렉토리에 파일을 추가 또는 삭제 가능
Execute	x(1)	실행 가능한 파일을 실행가능	cd 명령어로 디렉토리에 접근가능

위에서 확인한 허가권을 변경하기 위해서는 'chmod 권한 파일명'이라는 명령어를 통해 변경이 가능하며, 권한설정은 두 가지 방법있다.

1) 첫 번째는 chmod ugo+rwx test를 입력하여 모든권한을 주도록 변경한 모습이다.

< 그림12. 파일허가권변경1 >

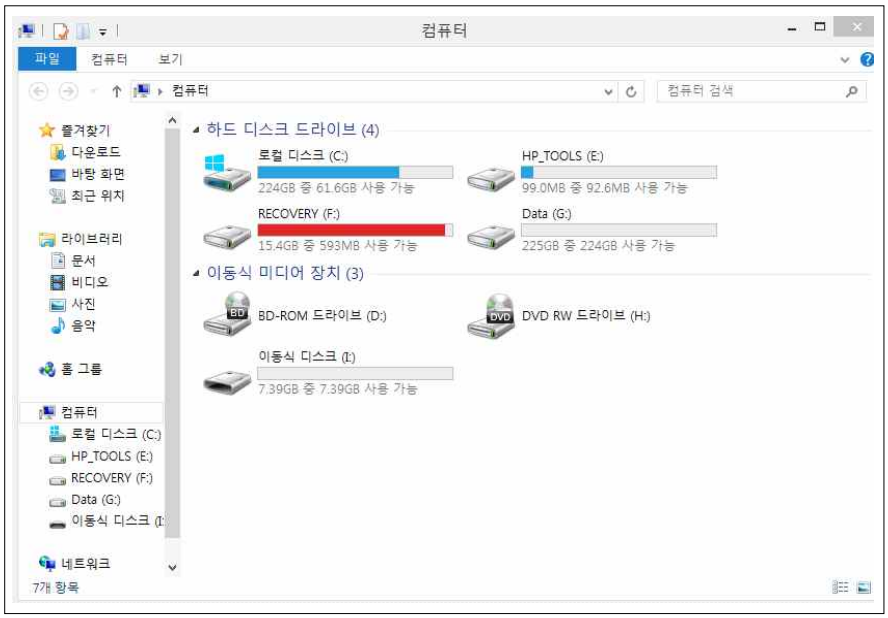
- ugo 란 User(소유자), Group(그룹), Others(그 외 이용자)를 의미한다.
- +rwx에서 +는 허가권추가, rwx는 Read, Write, eXecute를 의미하며, 추가적으로 +는 허가권 추가 -는 허가권 삭제를 의미한다.

2) 두 번째는 chmod 777 test를 입력하여 모든 권한을 주도록 변경한 모습이다.

< 그림13. 파일허가권변경2 >

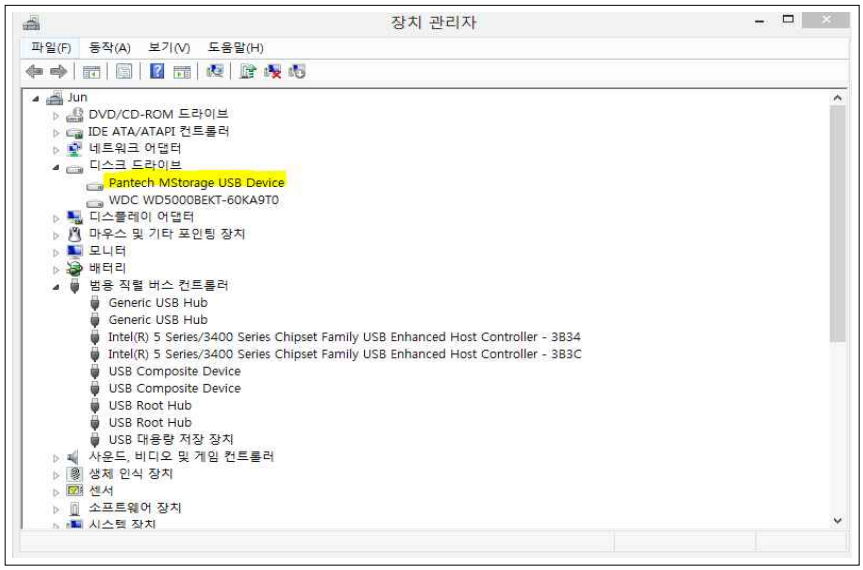
- 777이란 각 r, w, x에 대한 심볼릭 넘버 4, 2, 1을 합산한 값이다.
- 위와 같은 파일 허가권 설정으로 Linux, Unix 계열에서 접근제한을 할 수 있다.

참고적으로 앞의 2.1.2 파일에서 설명하였던 물리적 기억 장치에 해당되는 USB에 대해 추가적으로 기술하자면, 이 물리적 기억 장치는 온라인 즉 네트워크상이 아닌 PC에 물리적으로 물리는(연결되는) 것이기 때문에 위의 파일의 특성에서의 접근권한 설정과 같다. 이는 즉 물리장치이기 때문에 하나의 디스크로 인식된다는 것이다.

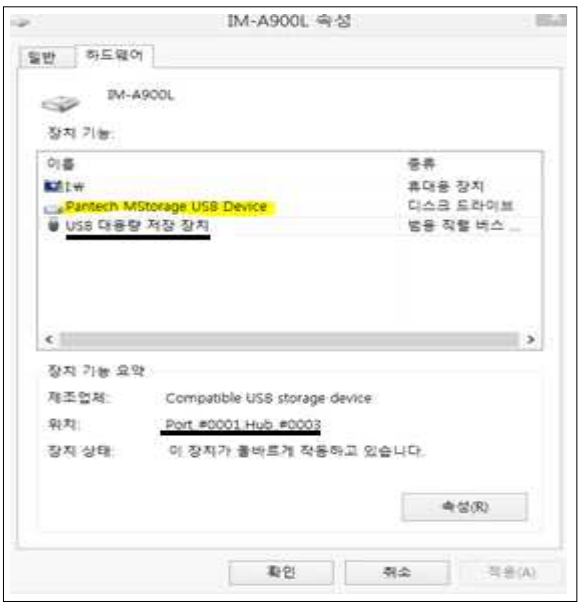


< 그림14. 물리적 기억장치의 연결(USB) >

위의 <그림14>처럼 이동식 디스크(I:)라는 디스크로 인식이 된다. 따라서 접근 권한 설정이 가능하다. 또한 연결된 장치를 확인하는 방법은 아래의 <그림15>와 같으며, 제어판의 장치관리자에 들어가서 확인이 가능하다.



< 그림15. 물리적 기억장치 확인1 >



< 그림16. 물리적 기억장치 확인2 >

위의 예시는 윈도우 7에서의 예시였으며, 리눅스 및 유닉스 계열에서는 USB장치는 /dev에서 추가된 장치를 확인할 수 있으며, 위의 파일의 특성에 의한 접근권한 차단 방법과 동일하다.

3.1.3 파일확장자

이는 소프트웨어 적인 방법이 주로 해당되며, OS에서 지원하는 서비스 기능으로는 확장자로 차단할 수 있는 방법은 없다. 하지만 외부로 나가는 즉 다른 네트워크간의 파일 유출을 확장자로 차단할 수 있는 방법이 있으며, 실질적으로 확장자에 의존한 차단 방법이라고 하기 보다는 데이터가 이동되는 것을 차단시키는 것으로 확장자에 차단이라고 볼 수 없다.

하지만 물리적 장비 자체의 내장된 프로그램 또는 웹 서버, 메일 등의 업로드에 의한 유출 시에는 자체의 구동된 프로그램 내부에 의해 일부 확장자를 차단할 수 있다. 예를 들면 메일 혹은 웹 서버 업로드 시 프로그램의 소스코드에 확장자를 구분 짓게 해놓는 것이다.

- 다음 <그림17>은 Gmail의 예시이다.

< 그림17. G-mail 편지쓰기 - 파일첨부 DS_NTFS.exe[8] >

위 <그림17>과 같이 exe파일은 보안상의 이유로 차단되었다고 나온다. 이에 대해서 자세히 살펴보면 다음과 같다.

< 그림18. G-mail - 첨부파일 문제형식[8] >

먼저 위와 같이 잠재적인 바이러스를 막기 위해서 실행파일에 해당되는 메일은 첨부가 불가능하게 제한되어있다. 또한 아래의 .zip, .tar등 압축파일도 차단되어 있는데 이것은 보안상 메일 자체에서 압축된 파일을 압축을 풀어 내부의 파일들에 실행 파일들이 들어있는지 확인이 불가능하기에 잠재적인 바이러스 방지를 위해 차단해놓은 것이다.

결론적으로 물리적 장치간의 OS단의 차단 방법은 없지만 네트워크 단에서는 파일 확장자에 따른 차단이 가능하다.

3.1.4 암호화

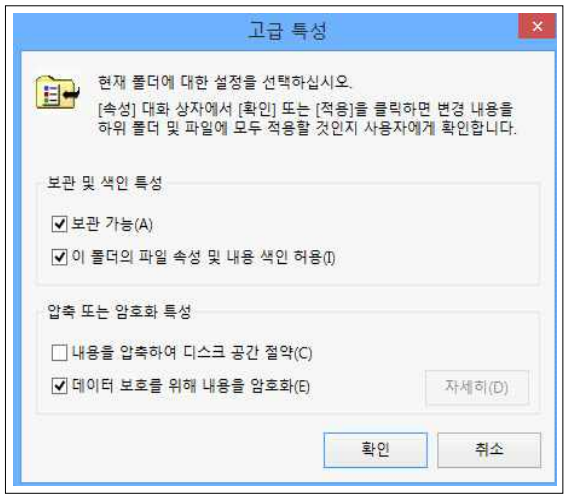
파일의 유출을 방지하기 위해 암호화라는 기능이 존재한다. 이는 파일에 암호를 걸어 패스워드를 입력해야만 파일을 열어볼 수 있도록 하여, 외부로부터 유출되었을 때 내용을 알아볼 수 없도록 제한을 거는 것이다. 이 부분은 문제점은 타인에 의한 유출일 시 에는 효과가 있지만 내부에 의한 유출일 겨우는 효용이 없으므로 명심해야 한다.

암호화의 장점은 암호를 알고만 있는 사람만이 유일하게 그 파일에 대한 접근이 가능하다는 점이 가장 뛰어나며, 또한 암호를 모르는 사람이 존재한다 하여도 암호의 길이, 암호의 종류에 따라서 파일에 대한 암호추측이 어렵다는 점에 있다.

암호화를 하는 방법은 다양하다. 우선적으로 여러 가지 소프트웨어를 통해서 파일을 암호화 하는 경우가 가능하다. 이는 해제할 시에 암호화 했던 소프트웨어가 있어야만 해제가 가능하다는 점에서 불편함을 요하지만 장점으로는 해당 PC에서만 사용 가능하도록 소프트웨어를 통해 설정하면 외부로 유출이 되어도 풀 수 없도록 되어있다.

A. 파일 암호화 (Windows 8)

파일을 암호화 하기 위해서는 해당 파일(혹은 폴더)의 속성탭을 들어간 뒤에 고급탭을 들어가게 되면 아래 그림과 같이 암호화 기능이 존재한다.



< 그림19. 파일암호화 >

B. 드라이브 암호화 BitLocker (Window 8)

추가적으로 윈도우7 이후부터는 윈도우 자체에 BitLocker 이라는 기능을 지원한다.

- 이는 드라이브에 암호를 걸어서 잠금을 하는 기능이다. 제어판 - BitLocker 드라이브 암호화를 클릭하면 아래와 같은 드라이브에 따른 잠금을 할 수가 있다.

< 그림20. 드라이브암호화 >

이 기능은 부팅 시에 필요한 운영체제 OS정보가 들어있는 드라이브를 잠가 버리는 기능으로 부팅 시 암호화된 킷값을 요구하며, 이 킷값이 없으면 부팅이 되지 않는다.

- 이것은 파일의 특성에 따른 암호화라고 하기보다는 OS 자체를 암호화를 한다고 표현하는 것이 맞는 것이다. 이 기능이 이용되어지는 경우는 두 개의 하드디스크에 각 OS를 저장해놓고 하나는 작업용, 다른 하나는 공용으로 사용할 때 사용하는 용도로 주로 사용된다.

3.1.5 그 외의 방법

위의 방법 외에 다양한 방법이 있을 것이다. 대표적으로 다룰 수 있는 가능성이 있는 부분에 대해서 연구한 것이고, 무한한 다양한 가능성이 존재한다. 예를 들면 해당 파일이 사용하는 일시 파일이 실행 중이기에 이동 복사가 불가능하다는 점을 이용해 볼 수도 있다. 이는 파일을 계속 사용 중인 상태로 열어두는 상태로 작업하는 것이며, 종료를 하지 않는 점에서 프로세스 낭비가 심하다. 하지만 이 낭비를 신경 안 쓸 수 있다던가 혹은 이와 관련된 시스템이 갖춰진다면 충분이 이 또한 차단방법이 될 수 있는 것이다.

위의 차단 방법은 추가적인 소프트웨어나 프로그램을 이용한 방법이 아닌 운영체제 자체에 내장된 기능을 이용하여 할 수 있는 방법 이였다. 따라서 소프트웨어나 프로그램을 이용한 방법은 시중에 나와 있는 것이 많기에 온라인으로 구할 수 있다. 대표적으로 하나의 서버에서 접근권한을 설정하여 각 PC에서 서버에 있는 데이터를 읽기, 수정, 실행 권한만 주어지며 이를 이동 복사는 불가능하게 설정되고 관리 할 수 있는 시스템이 있다.

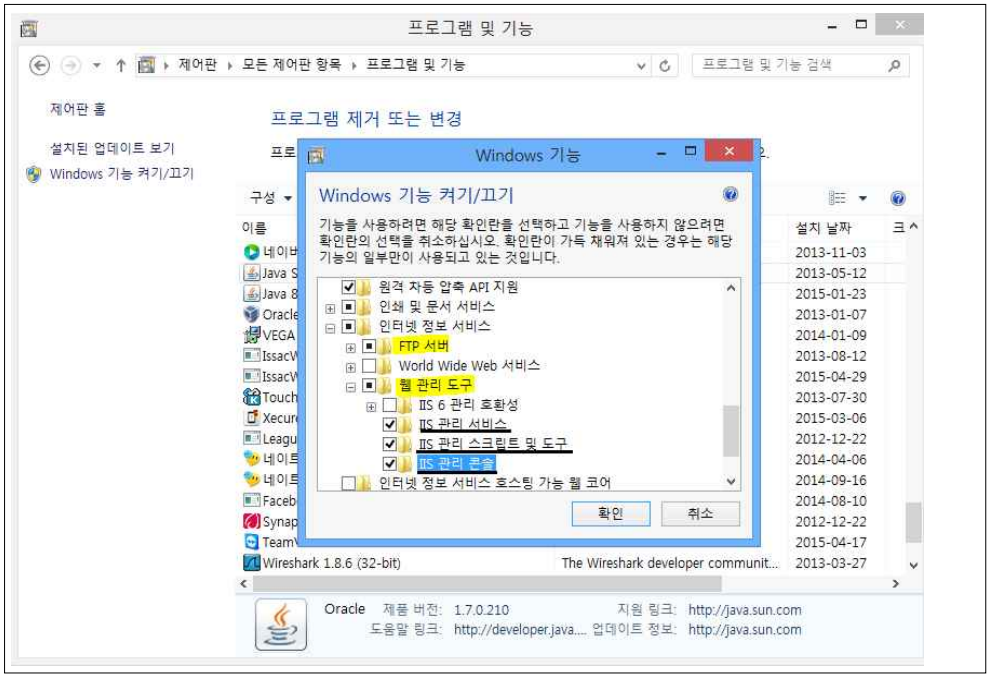
위와 같이 다양한 방식과 방법이 있지만, 가장 큰 문제점은 본인 당사자가 파일을 생성하여 그 파일을 송신하는 경우에는 파일 특성에 의한 방법으로는 방지할 수 없다는 점이다. 즉 타인에 대한 유출을 차단하기 위한 방법이다.

3.2 포트기반의 차단

먼저 잘 알려진 포트의 경우 포트 자체를 막는 경우를 제외하고 사용자의 권한 설정에 따른 접근권한 설정으로 유출을 막는 경우가 있다. 이는 파일특성에서 말한 것과 같이 파일을 생성한 본인이 유출하는 경우 즉 PC의 최고권한을 지닌 자에 대해서는 차단할 수 없는 방법으로, 타인에 의한 차단 방법이다.

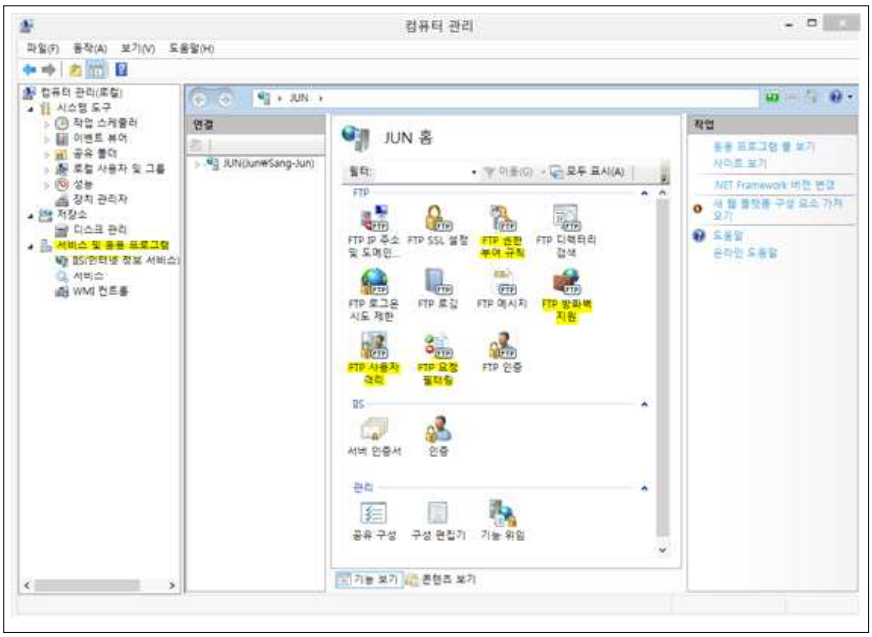
1) 먼저 OS에 내장된 서비스를 이용한 차단방법이며, 그 중 FTP 서비스에 대한 예시이다.

A. Window 8



< 그림21. FTP, IIS 서비스기능 On >

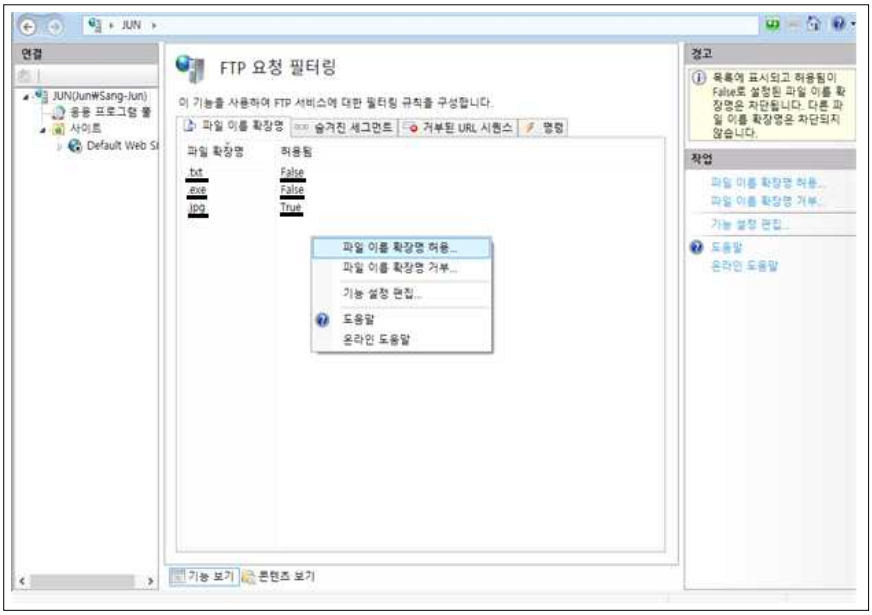
먼저 윈도우의 제어판에서 프로그램 및 기능에 들어가 Windows 기능의 항목 중 위의 그림과 같이 FTP 서버와, 웹 관리 도구를 체크해 줘야한다. 이는 Windows 자체에서 지원하는 FTP서비스이며, 추가적으로 IIS 인터넷 정보 서비스 관리를 체크하게 되면 FTP 서비스를 쉽게 관리 및 설정이 가능하다.



< 그림22. IIS 서비스를 이용한 FTP 설정 >

위의 그림은 앞서말한 IIS를 통한 FTP 서비스 설정관리이며, 내 컴퓨터에서 우측클릭 후 컴퓨터 관리에 들어간 그림이다. 여기서 유심히 볼 부분은 FTP 권한부여 규칙, 방화벽지원, 사용자 격리, 요청 필터링에 해당하는 보안 부분이다.

- 권한 부여규칙, 사용자 격리는 접근권한 지정(제어)로 파일 접근권한 방식과 동일하다.
- 방화벽 지원은 방화벽에서 규칙을 설정하여 제어하는 방식으로 다음 전체적인 포트 차단 방법에 대해서 기술할 것이다.

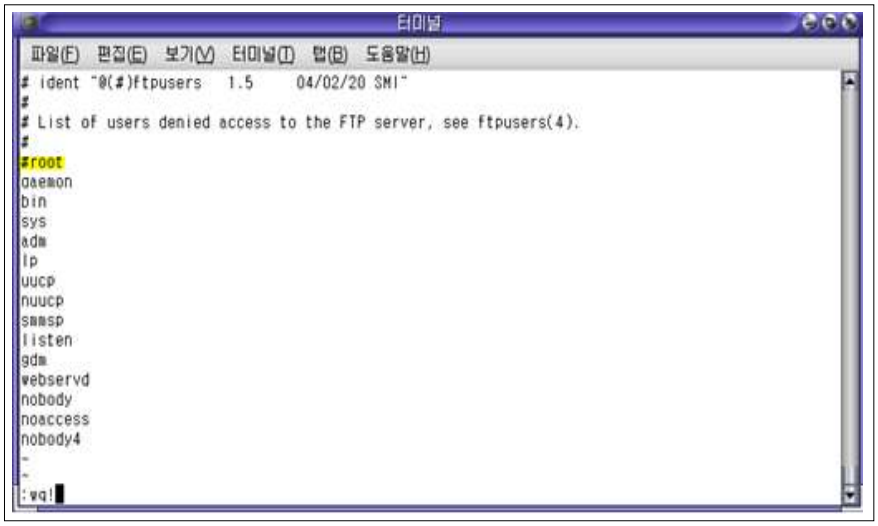


< 그림23. FTP 요청 필터링 >

위의 그림은 FTP 요청필터링에 해당하는 부분으로 파일 이름 확장명 허용, 거부를 통해서 특정 확장자에 대한 파일 송수신을 차단할 수 있도록 지원한다.

B. Linux 및 Unix (Solaris 10)
먼저 FTP 서비스 상태를 확인한 후에 작동되지 않았을 시에 작동해주며, 다음과 같은 명령어를 통해 확인할 수 있다.
svcs -a | grep ftp << ftp 작동 확인
svcadm enable ftp << ftp 작동하기

다음으로 FTP 접속 차단 사용자 목록을 수정해준다.
vi /etc/ftpd/ftpusers << ftp 차단된 사용자 목록이 담긴 곳이다.

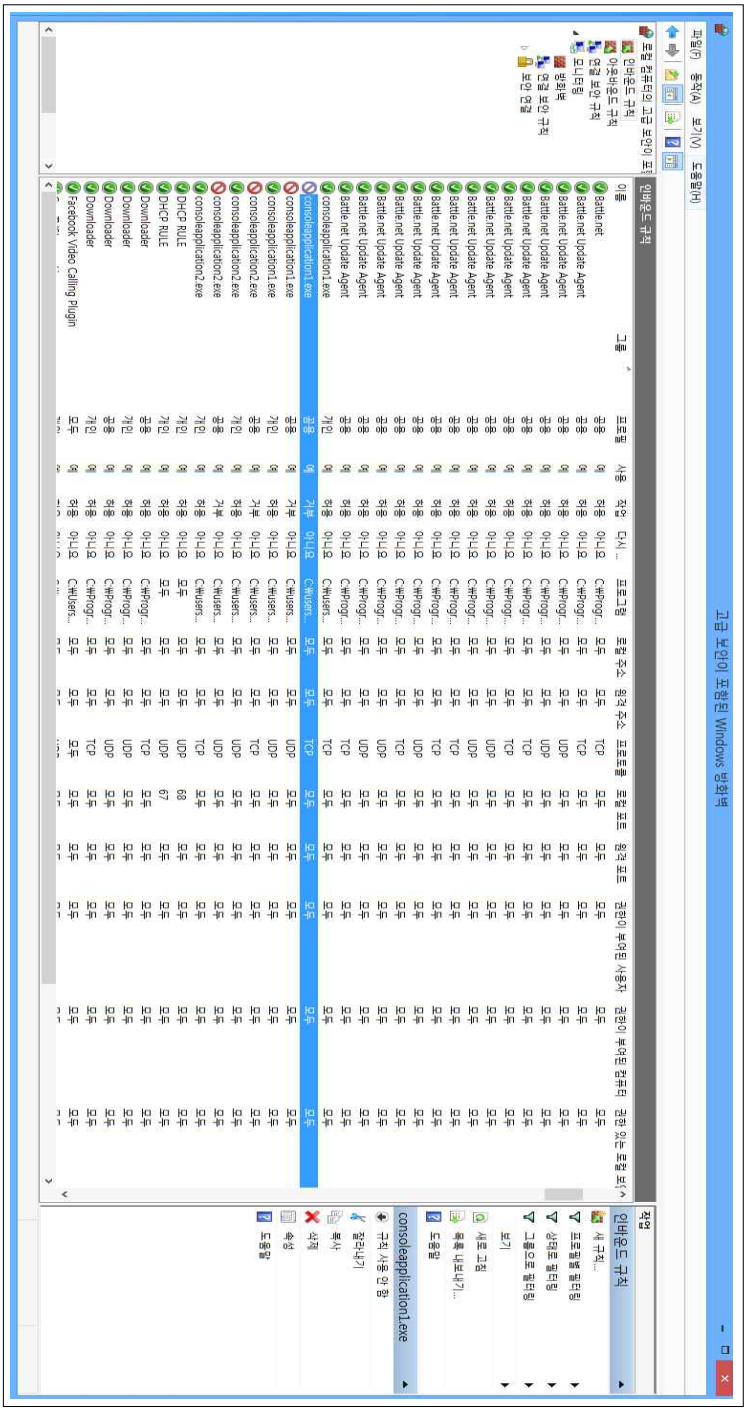


< 그림24. FTP에 차단된 사용자목록 >

초기에는 root(관리자) 또한 차단목록에 들어가 있다. 위에처럼 #을 앞에 추가하여 주석처리를 한다. 이처럼 Unix 계열 또한 FTP 서비스 자체에서 접근권한을 설정할 수 있도록 되어있다.

2) 다음으로는 포트를 통한 차단 방법이다. 위에서 연구한 바와 같이 해당 포트가 아닌 잘 알려진 포트만 허용하고 그 외의 포트의 경우에는 차단하는 것이 관리하기 편한 합리적인 방법이다. OS단에는 방화벽을 통해서 포트들을 관리할 수 있다.

A. Window 8의 경우
제어판의 방화벽 설정을 들어가면 다음과 같은 그림이 나오며, 다양한 규칙들이 나오며, 그 규칙들을 통해 보안설정이 되어있다.



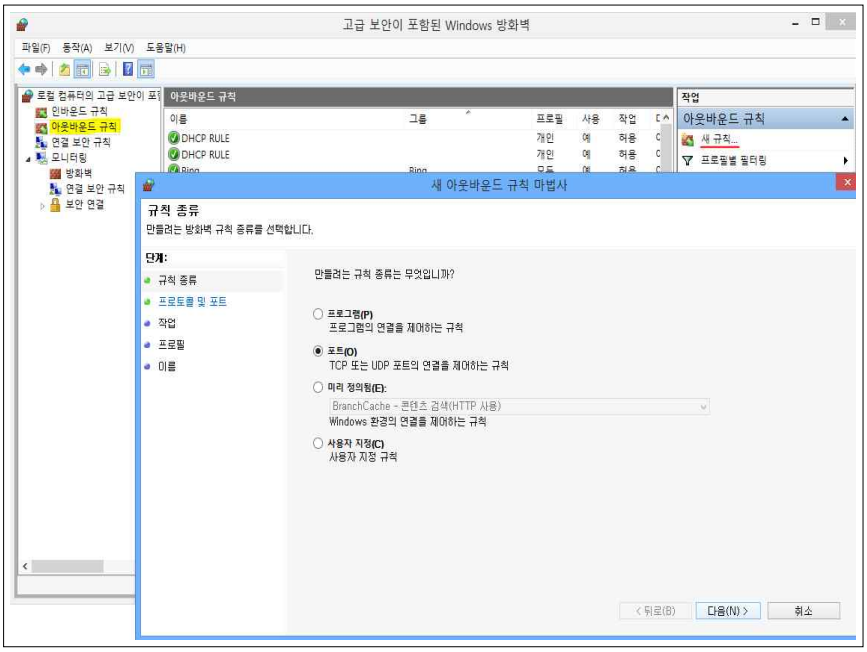
< 그림25. Windows 방화벽 >

그림을 보면 인바운드 규칙과 언바운드 규칙이 존재하는데 이는 다음과 같다.

- 인바운드 규칙 : 외부 네트워크에서 내부 네트워크로 들어오는 것을 의미한다.
- 아웃바운드 규칙 : 내부 네트워크에서 외부 네트워크로 나가는 것을 의미한다.

여기서 연구하며 차단방법을 기술하는 부분은 외부로의 유출을 방지하기 위해 내부 네트워크에서 외부 네트워크로 나가는 차단방법에 대한 방법임으로 기술될 부분은 아웃바운드에 해당된다. 또한 앞서 차단방식 연구에서 기술한 것과 같이 모든 포트를 차단 후 그 외의 포트는 예외처리 하고자한다. 다음은 이제 대한 설정을 하는 과정으로 간략히 순서화 하였다.

1. 아웃바운드에 새 규칙 마법사를 통해 설정해준다.



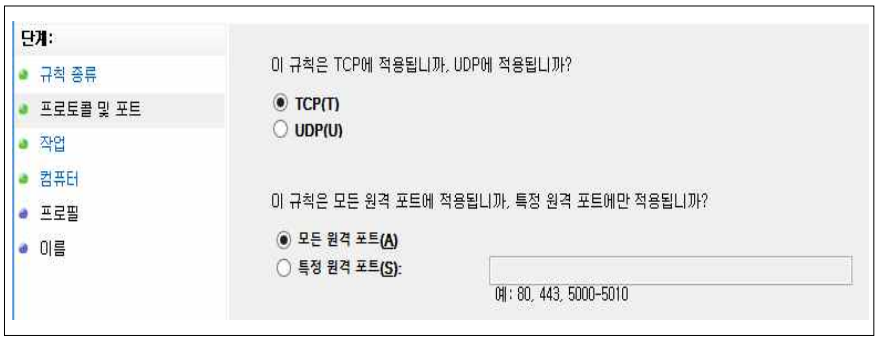
< 그림26. 방화벽 규칙설정1 >

2. 포트에 의한 차단 방법이기에 규칙종류에서 포트를 선택해 준다.

※ 위 <그림26> 참조

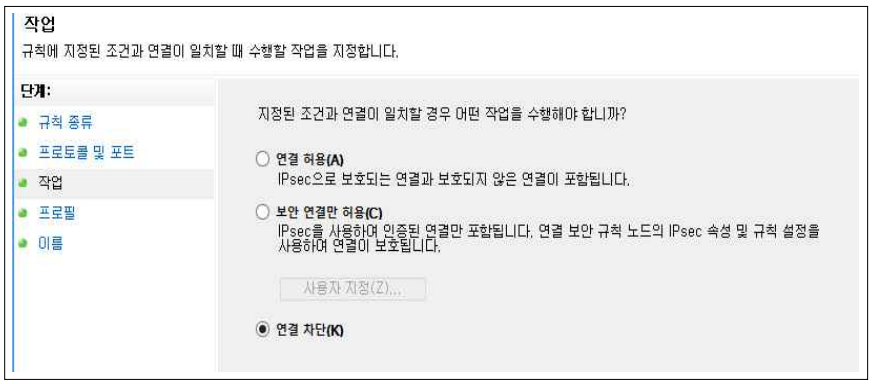
3. TCP/UDP 구분에 따른 2번의 설정과 4. 작업설정에서의 2번 설정 총 4번의 규칙설정을 요한다. (각 3-1, 4-1의 모든 원격포트 차단 1회 / 3-2, 4-2 차단규칙 예외 설정을 해줄 것이다.)

3-1. 프로토콜 및 포트에 대한 부분은 TCP와 UDP를 구분하여 모든 포트를 차단해준다.
※ 처음 제안한 방법으로 차단할 것이기에 모든 포트를 차단한다. 작업 창에서 예외 설정이 가능하다.



< 그림27. 방화벽 규칙설정2 >

4-1. 연결 차단을 한다.

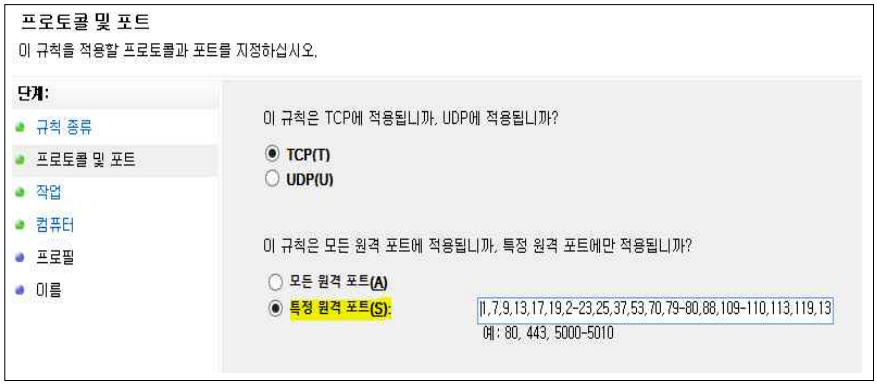


< 그림28. 방화벽 규칙설정3 >

> 이렇게 해서 모든 TCP, UDP 포트에 대하여 차단설정이 완료되었다. 이제는

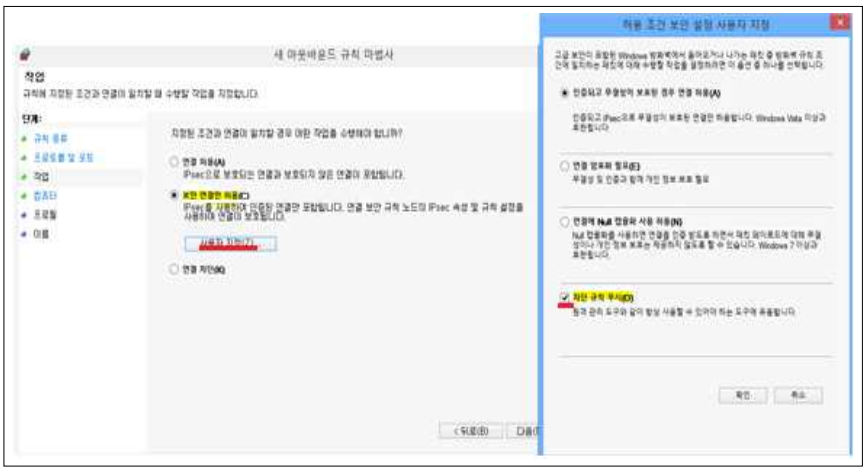
차단 규칙에 대한 예외 설정을 해준다.

3-2 특정 원격 포트 값을 입력해준다.
※ 잘 알려진 포트 번호를 넣는다. (단, FTP 20번과 SMTP 25번은 제외한다.)



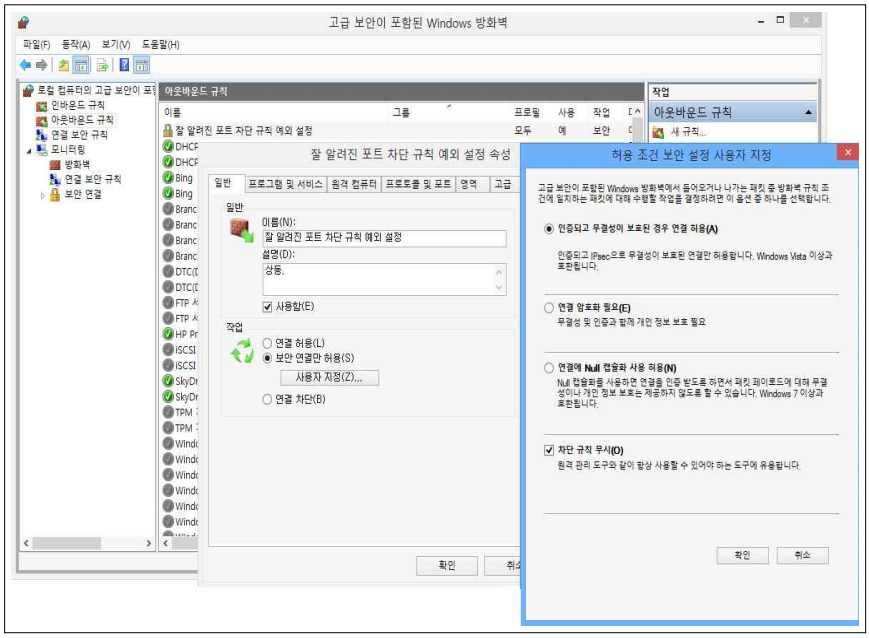
< 그림29. 방화벽 규칙설정4 >

4-2 보안 연결만 허용 - 사용자 지정에서 차단 규칙 무시를 선택해준다.



< 그림30. 방화벽 규칙설정5 >

※ 위처럼 차례대로 진행하게 되면 모든 방화벽 규칙 설정이 완료되고 아래와 같이 아웃바운드 규칙이 생성된 것을 확인할 수 있다.



< 그림31. 방화벽 규칙설정6 >

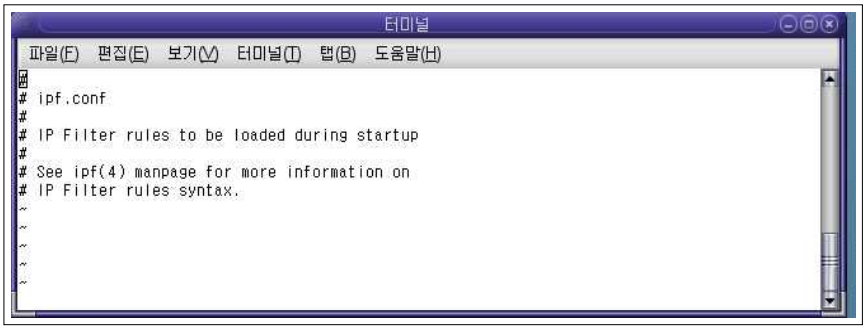
B. Linux 및 Unix의 경우(Solaris 10)

Solaris 10의 경우에는 방화벽 역할을 하는 ipfilter라는 서비스가 있다. 이를 이용한 포트 차단하는 방법에 대해서 기술하였다.

먼저 'svcs -a' 명령어 입력을 통해 실행중인 서비스 목록을 확인하고 차단설정을 할 데몬들을 종료해 준다.

두 번째로 ipfilter 방화벽 규칙을 설정해 준다. 'vi /etc/ipf/ipf.conf' 명령어를 입력해주면 다음과 같이 나온다.

※ 어떤 경우에는 /etc/opt/ipf/ipf.conf인 경우도 있다.



< 그림32. ipfilter rule >

이곳에 규칙을 작성하면 되고 규칙은 다음과 문법을 지녔다.

- block : 패킷을 차단
- in : 인바운드 패킷
- all : 모든 패킷
- out : 아웃바운드 패킷

위와 같이 4가지를 이용하며, 문장으로 예시를 들자면 아래와 같다.
pass out on hme0 proto tcp form any to any keep state
pass out - 나가는 패킷에 대해서
on hme0 - hme0 인터페이스는
※ quck 도 존재하는데 이는 이에 해당되는 모든 룰에 대해 적용시키는것이며, 이에 해당되는 추가된 아래의 룰에 대해서는 무시한다.

proto tcp - tcp 프로토콜의
form any - 모든 곳에서
to any - 모든 곳으로 가는 것은
keep stat - 상태를 유지한다. 라는 의미다
즉, hme0 인터페이스는 아웃바운드에 대해서 tcp 프로토콜의 모든 것을 허용한다는 것이다.

차단 방식에는 quick이라는 것이 존재하여 이를 잘 이용해야 한다.
[pass out quick on pcn0 proto icmp from any to any keep state]이란 룰 에서 붉은색 글자는 동작방식을, 파란색 글자는 패킷의 조건을 나타낸다. 파

란색 글자의 내용과 일치하는 패킷에 대해 붉은색 글자로 된 내용을 수행한다.

윈도우에서의 방화벽은 모든패킷을 차단시킨 후 허용할 잘 알려진 포트에 대해서 예외처리 하였지만, ipfilter 룰에서는 quick이란 규칙을 사용함으로서 그 아래의 규칙은 무시하기 때문에 먼저 TCP, UDP 패킷 중 잘 알려진 포트에 대해서 통과시키며, 그 룰은 아래와 같다.
Pass out on pcn0 proto tcp from any to any port=포트번호 keep state

위에서 잘 알려진 포트를 먼저 허용시켰고 이제는 그 외의 모든 패킷을 차단하는 룰이다.
Block out quick on pcn0 all

> 결론적으로 첫줄에서 알려진 포트는 통과되고 그 다음 quick 룰이 적용된 부분부터 모든 패킷에 대해 차단함으로써, 모든 패킷을 차단하되 첫줄의 알려진 포트를 예외한다 라는 것이다.

3.3 패킷

패킷을 차단하는 방법은 OS에서 자체적으로 지원되는 서비스는 없으며, 위 3.2의 포트의 차단방법에 해당되는 방화벽에서 포트와 관련하여 패킷을 차단할 수 있게 되어있는 것이 전부이다. 따라서 패킷을 차단하기 위해서는 추가적인 소프트웨어를 요구하며, 이번 연구에서는 2.3.2 관련연구 패킷 차단기법연구에서 패킷을 사전에 인지가 가능하다는 점을 이야기함으로서 마무리 하였다.

4. 결론

이번 연구는 내부자료가 외부로 유출됨으로 인하여 산업기술과 개인정보 유출이 근래에 들어 이슈화 되고 있음을 알리며 많은 피해를 방지하기 위한 연구로, 현재 국재에는 추가적인 소프트웨어를 설치하여 유출을 차단할 수 있는 방법이 존재한다. 하지만 이에 의하여 방지하는 개인 혹은 업체에 있어서 OS 자체에서 지원하는 서비스로도 일부 방지가 가능하다는 점을 알리며, 파일이 유출되는 원리와 특성 등을 연구하고 이에 대한 다양한 가능성을 인식하게 하여, 이를 토대로 사전에 방비하기 위한 노력을 요구하도록 파일 불법 유출에 대한 보안의식을 고취시키고자 하여 시작된 연구이다.

본 연구에 제시된 다양한 가능성은 파일 송수신이 갖는 원초적인 원리와 그에 따른 특성을 바탕으로 제시 및 유추하였으며, 제시된 사실과 유추에 따른 추론은 실제로 공시된 자료를 토대로 근거시 하여 연구하여 기술하였다.

파일 유출이라는 것은 생각보다 간단히 발생하며, 기술적인 문제보다 사람에 의한 문제가 가장 큰 원인을 차지하며, 이 연구에 기술된 내용에서 자주 언급되는 것 또한 이에 대한 문제점이다. 따라서 이 연구의 주된 기술적인 측면보다는 각 개인 및 기업에서의 보안의식에 대한 교양이 필수적이며, 자체적인 자원·인적관리가 항시 이루어 져야한다.

또한 유출로 인한 피해는 큰 심각성이 부여되고, 상대적으로 양호하다고는 하나 상대적인 것은 가치의 높낮이를 평함에 있어서 기준차에 불과하다. 국가적인 차원에서 종합계획을 수립하고 지원함에 따라 많은 개인 및 기업이 관심을 두고 정보공유 등을 통한 피해를 줄여나가길 바란다.

결론적으로 이번 연구논문을 통해 많은 사람들이 문제가 증가하여 발생함에 따른 인지가 아닌 이를 방지하기 위한 노력과 인식이 필요하다고 여겨지고, 이를 방지하기 위해 노력하였으면 한다.

◆◆ 표/그림 목차 ◆◆

◆◆ 참고문헌 ◆◆

[1] 지식경제부, 산업기술 유출방지 및 보호에 관한 종합계획, pp.5,2013.3
[2] 중소기업청, 중소기업 기술유출 실태 및 기술보호 정책, pp.3-8,2013.2
[3] 중소기업청, 제3차 중소기업 기술혁신촉진계획(안), pp.8,2014.7
[4] 개인정보보호 종합포털, www.privacy.go.kr
[5] 네이트, Nateon5 헬프데스크, www.nateonwep.nate.com
[6] 황석훈, 보안관리자가 알아야 할 네트워크 이론과 해킹 기법, 도서출판 혜지원, pp.113-120
[7] 운영체제 내부구조 및 설계원리 제5판, 도서출판 그린, pp.592-602
[8] 구글, G-Mail 도움말, https://support.google.com/mail
[9] Microsoft, Windows 하드웨어 개발자센터, NDIS 필터 드라이버, http://msdn.microsoft.com/en-us/library/windows/hardware/ff565501(v=vs.85).aspx