# 1 보안 솔루션 종류

## 1 VPN(Virtual private network)

- 방화벽, 침입 탐지 시스템과 함께
  가장 일반적인 보안 솔루션 중 하나(Public + Private)

- VPN은 한 달에 3만 원이면 이용할 수 있는
  인터넷 회선을 전용선과 비슷한 용도로
  사용할 수 있게 해주는 솔루션

- 전용선과 비슷한 수준의 기밀성을 위해 암호화 필요

## 1 VPN(Virtual private network)

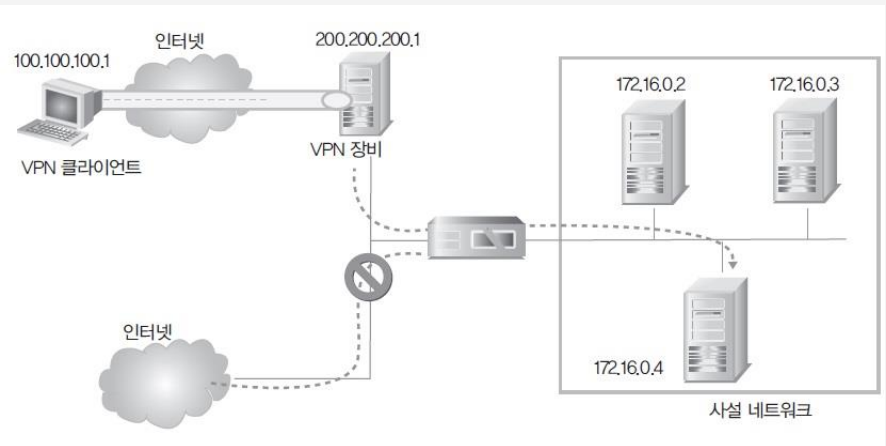
- VPN에 사용하는 암호화 프로토콜
  : PPTP, L2TF(2계층), IPSec(3계층), SSL(4계층) 등

- 현재 웹 브라우저의 인프라를 이용하는
  SSL VPN이 널리 사용되고 있음

## 2 VPN 이용 사례

- 해외에서 국내 온라인 게임 즐기기
- 집에서 회사 내부 시스템에 접근하기

[VPN을 이용하여
외부에서
내부 시스템에 접근]

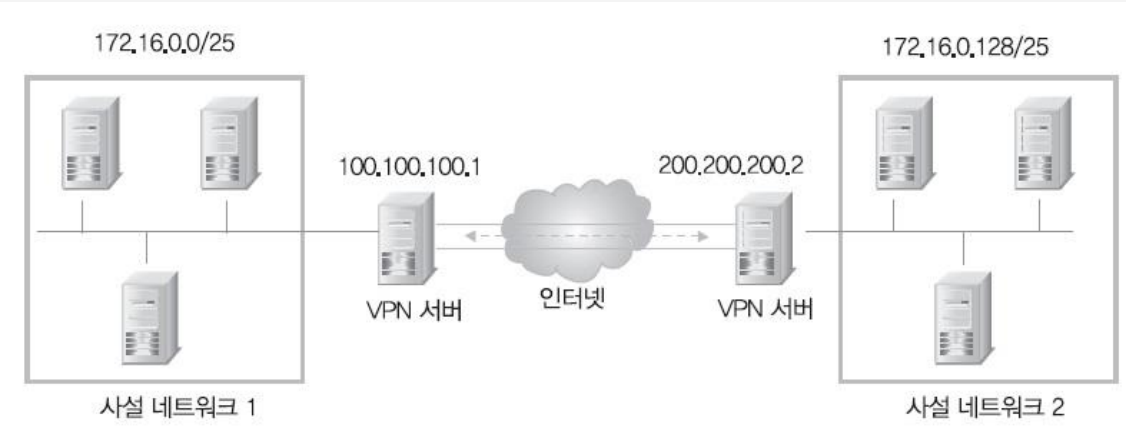



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 VPN 이용 사례

- 원격의 두 지점을 내부 네트워크처럼 이용하기(터널링)

[VPN을 이용한 터널링]




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 VPN

- 가상사설망(假想私設網) 또는 VPN(영어 : Virtual private network)은 공중 네트워크를 통해 한 회사나 몇몇 단체가 내용을 바깥 사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망(Public + Private)

- 가상 사설망에서 메시지는 인터넷과 같은 공공망 위에서 표준 프로토콜을 써서 전달되거나, 가상 사설망 서비스 제공자와 고객이 서비스 수준 계약(SLA)을 맺은 후 서비스 제공자의 사설망을 통해 전달

## 3 VPN

- 가상 사설망의 등장배경은 인터넷을 기반으로 한 기업 업무환경의 변화에 기인함, 즉 소규모 지역에서 문서만을 전달하던 업무처리 기반에서 하나의 건물 내의 네트워크를 이용한 업무로, 다시 본사와 다수의 지사 관계, 또한 지사는 국내 지사와 국외 지사로 확장(지사를 통한 업무 확장)

## 3 VPN

- 이들이 하나의 네트워크 구축을 위해 기존 전용선을 사용하는 방법에는 비용을 포함한 여러가지 한계를 가지며, 전용선을 이용해서 네트워크가 구성되었다고 하더라도 네트워크 운영을 자체적으로 하는 것과 새로운 기술들을 도입하는 것 역시 기업의 입장에서는 상당한 부담이 될 수 있음(비용 + 운영)

## 3 VPN

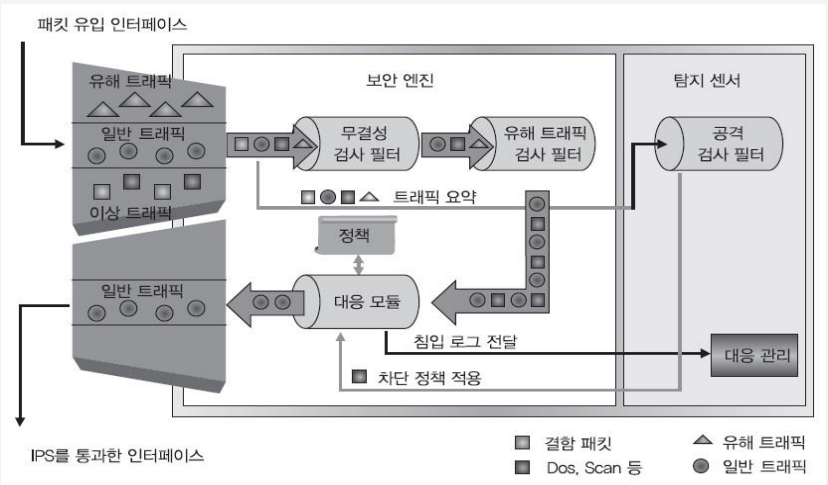
- 또한 기존의 공중 네트워크는 보안과 관련해서는
  서비스를 제공하지 않기 때문에 중요한 문서나
  데이터를 전달하기에는 부족한 점이 있었음(보안)

  이러한 복합적인 이유가
  가상 사설망이 등장한 계기가 됨

## 4 IPS(intrusion prevention system)

- 방화벽(Firewall)과 침입 탐지 시스템(IDS)의 한계로 대두된 보안 솔루션

[IPS의 동작 원리]

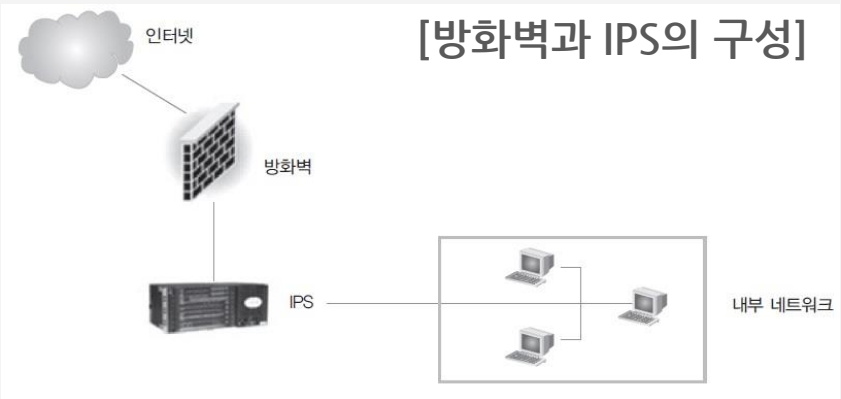



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 IPS(intrusion prevention system)

- 일반적으로 방화벽 다음에 설치
- 방화벽 없이 IPS를 설치할 경우
  높은 성능을 내기 위해 ASIC 이용(어플라이언스)

[방화벽과 IPS의 구성]




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 4 IPS(intrusion prevention system)

- 침입 차단 시스템(侵入遮斷 - , 영어: Intrusion Prevention Systems (IPS), Intrusion Detection and Prevention Systems (IDPS)) 또는 침입 방지 시스템은 외부 네트워크로부터 내부 네트워크로 침입하는 네트워크 패킷을 찾아 제어하는 기능을 가진 소프트웨어 또는 하드웨어임

## 4 IPS(intrusion prevention system)

- 일반적으로 내부 네트워크로 들어오는 모든 패킷이 지나가는 경로에 설치되며, 호스트의 IP주소, TCP/UDP의 포트번호, 사용자 인증에 기반을 두고 외부 침입을 차단하는 역할을 함, 허용되지 않는 사용자나 서비스에 대해 사용을 거부하여 내부 자원을 보호 함

## 5 스팸메일 차단 솔루션

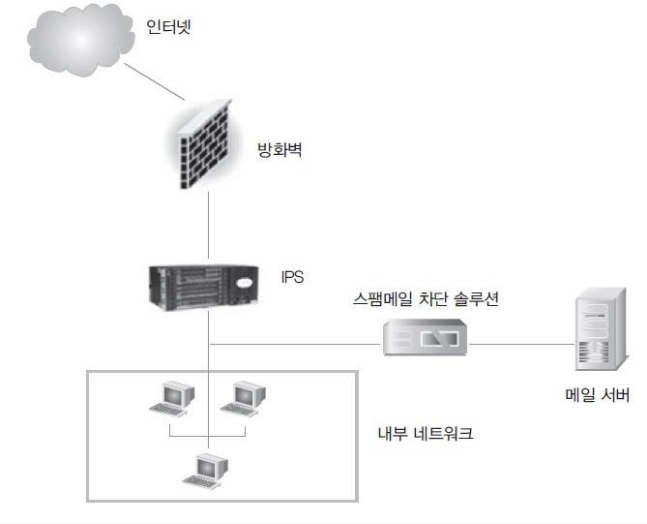
- 메일 서버 앞쪽에 위치하여
  프록시 메일 서버로 동작(Proxy)

- SMTP 프로토콜을 이용한 DoS 공격이나 폭탄 메일,
  스팸 메일 등을 차단(SMTP, POP3, IMAP)

- 최근에는 내부에서 외부로 보내는 메일의 본문 검색,
  첨부 파일 검색 등의 기능을 통해 내부 정보 유출 방지
  기능도 수행

## 5 스팸메일 차단 솔루션

### 스팸 메일 차단 솔루션의 구성




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 5 스팸메일 차단 솔루션

- 메일 헤더 필터링
  - 메일 헤더의 내용 중에서 아이디, 보낸 사람 이름, 도메인 등에 특정 내용이 포함되어 있는지 검사
  - 보낸 서버의 IP, 도메인, 반송 주소의 유효성과 이상 유무를 검사
  - 너무 많은 수신자가 포함되어 있는지, 혹은 존재하지 않는 수신자가 포함되어 있는지 검사

## 5 스팸메일 차단 솔루션

- 제목 필터링
  - 메일 제목에 '광고', '음란' 등의 문자열이 포함되어 있는지 검사
- 본문 필터링
  - 메일 본문에 특정 단어 또는 특정 문자가 포함되어 있는지 검사
  - 메일 본문 크기와 메일 전체 크기를 비교하여 유효성을 검사

## 5 스팸메일 차단 솔루션

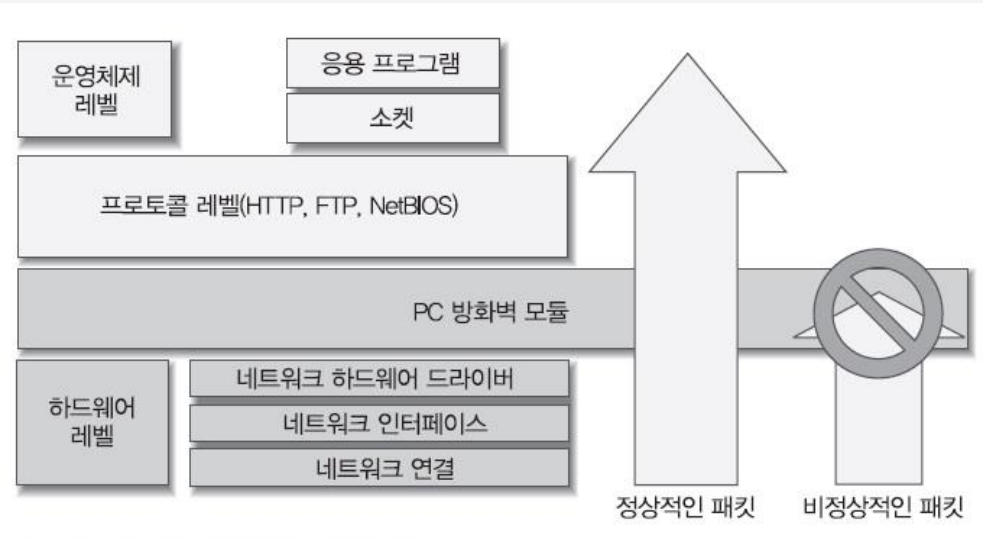
- 첨부 파일 필터링
  - 첨부 파일의 이름, 이름의 길이, 크기, 개수 등을 기준으로 필터링 수행
  - 특정 확장자의 첨부 파일만 메일을 통해 전송되도록 설정 (실행 파일 첨부 못함)

## 6 PC 방화벽

- 후킹(Hooking) : 방화벽 드라이버 설치
- 방화벽을 설치하면 일반적으로 PC 방화벽 모듈이 네트워크 하드웨어 드라이버와 프로토콜 레벨 사이에 배치됨(중간에 들어감)

## 6 PC 방화벽

### PC방화벽 동작방식




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

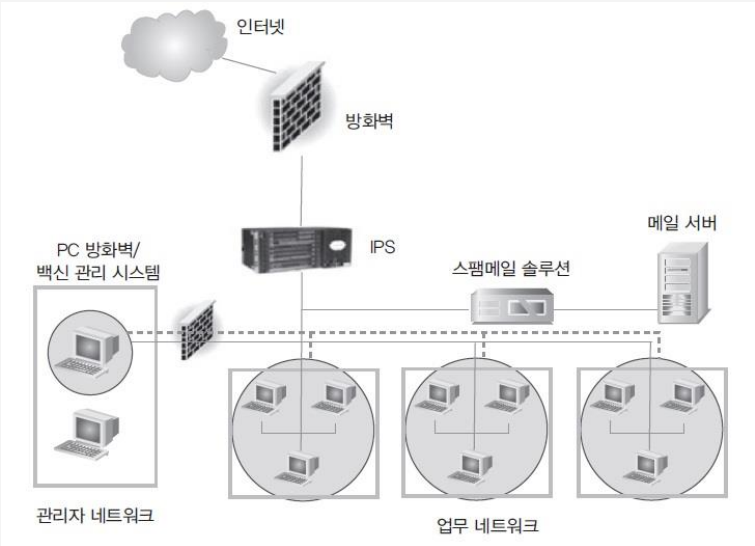
## 7 백신

- 시스템에 이미 바이러스가 침투했거나 USB 드라이브와 같은 외부 장치를 통해 시스템에 복사되거나 실행될 때 이를 실시간으로 검사(특정 문자열을 찾아냄)

- 가장 좋은 형태는 백신과 PC 방화벽을 함께 사용하여 서로의 약점이 보완되도록 하는 것

## 7 백신

### PC방화벽과 백신 솔루션의 구성




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 7 백신

- 바이러스 검사 소프트웨어(문화어 : 비루스 검사 소프트웨어, 비루스방역프로그람) 또는 안티바이러스 소프트웨어(영어 : Antivirus software) 은 악성 소프트웨어를 찾아내서 제거하는 기능을 갖춘 컴퓨터 프로그램(특정 문자열을 찾아냄)

- 대한민국에서는 이를 지칭하는데 백신 프로그램이라는 말이 일상용어로 사용되고 있음, 한국에서 백신이라는 용어는 V3의 초기 버전인 Vaccine(=V1), V2, V2PLUS로 인해 대중적인 용어가 되었음

## 7 백신

- 원래 목적은 바이러스만 잡는 것이었으나,
  현대에는 악성코드, 피싱 공격, 트로이 목마,
  웜 등도 검출함(피싱, 트로이목마, 웜)

  바이러스 검사 소프트웨어는 보통
  다음과 같은 두 가지 기술을 사용하여 이를 수행함

- 바이러스 데이터베이스의 정의와 일치하는
  바이러스를 확인하기 위해 파일의 내용을 살핌
  (첫번째)

## 7 백신

- 감염으로 표시될 가능성이 있는 컴퓨터 프로그램에서 의심이 가는 행동을 찾아냄, 이 기술은 발견적 분석이라고 부름, 이러한 분석은 자료 포착, 포트 감시 등의 방식을 포함할 수 있음(두번째)

- 보통 상용 바이러스 검사 소프트웨어는 이 두 가지 기능을 모두 사용

## 8 백신-역사

- 첫 백신 프로그램이 무엇인가는 확실하지 않음, 다만 처음으로 문서화된 컴퓨터 바이러스 제거 프로그램은 1987년 발표된 번트 픽스(Bernd Fix)인 것으로 알려져 있음

- 폴란드의 컴퓨터 바이러스 MKS vir를 제거하는 프로그램은 1987년 발표되었음, 닥터 솔로몬의 안티바이러스 툴킷, AIDSTEST와 AntiVir 등도 1988년 발표됨

## 8 백신-역사

- 한국에서도 안랩(前 안철수연구소)의 창립자 안철수 박사가 1988년 6월 10일 V1 (이후 보편화된 V3의 전신)이라는 백신 프로그램을 제작하여, 당시 맹위를 떨치던 바이러스 (c)Brain을 잡는데 큰 공헌을 하였음

- 1990년 후반 즈음에는,
  19개의 바이러스 검사 프로그램이 나타났으며,
  노턴 안티바이러스 등이 대표적인 예

  이 당시 컴퓨터 바이러스 연구를 한 사람들로는
  한국의 안철수 박사를 비롯해 프레드 코헨,
  존 맥아피 등이 있음

## 8 백신-역사

- 인터넷이 광범위하게 퍼지기 전에는,
  바이러스는 플로피 디스크를 통해 퍼져나갔음
  (플로피 → 하드)

  바이러스 검사 프로그램이 1980년대 후반에
  나타났으나, 업데이트는 비교적 느림(현재 전담팀)

  이 시기에 바이러스 검사 소프트웨어는 실행 파일과
  플로피 디스크, 하드 디스크의 부트 섹터를 검사하는
  것으로 되었음, 하지만, 인터넷 사용이 보편화되면서,
  바이러스는 인터넷을 통해 퍼지기 시작하였음
  (바이러스 → 웜)

## 8 백신-역사

- 마이크로소프트 워드 같은 워드 프로세서 프로그램의 매크로 기능 역시 위험을 증가시킴
- 바이러스 제작자들은 매크로를 사용해 문서에 바이러스를 첨부하기 시작
- 이것은 문서 파일의 숨겨진 매크로를 통해 바이러스에 감염될 수도 있다는 뜻 (누구나 쉽게 바이러스 제작)

## 8 백신-역사

- 이후 아웃룩 익스프레스 같은 전자 우편 프로그램도 전자 우편에 첨부된 바이러스의 위험에 노출됨

  현재는 전자우편을 여는 것만으로 감염되는 바이러스도 제작된 상태(XSS), 이로 인해 바이러스 검사자들은 더 다양한 종류의 프로그램을 체크해야 하게 됨, 그 결과 V3, 노턴 안티 바이러스, 알약 같은 다양한 백신 프로그램들은 라이브 업데이트라는 기능으로 실시간 업데이트를 지원하고 있음

## 8 백신-역사

- 하지만 바이러스에 대한 업데이트가 있기 전에 광범위하게 바이러스를 퍼뜨리는 제로데이 공격 등으로 인해 아직도 위험은 존재하는 상황임 (시간차 공격)

## 9 백신-접근 방식

- 사전 데이터베이스
  - 바이러스 검사 소프트웨어가 파일을 찾아내면, 바이러스 검사 프로그램을 만든 사람이 정의해 놓은 "알려진 바이러스"의 데이터베이스를 참조함 (특정 문자열)
  - 파일 안의 코드 일부가 데이터베이스의 바이러스와 일치하면, 바이러스 검사 프로그램은 다음의 과정 가운데 하나를 수행할 수 있음
  - 파일 안의 바이러스 자체를 제거하여 파일을 고치려고 시도함

## 9 백신-접근 방식

- 사전 데이터베이스
  - 파일을 차단함
  - 다른 프로그램이 해당 파일에 접근할 수 없으며, 바이러스는 퍼지지 않음
  - 감염된 파일을 삭제함

## 9 백신-접근 방식

- 의심스러운 동작
  - 의심스러운 동작이 접근한다고 하여 알려진 바이러스를 확인하려고 시도하지는 않지만, 모든 프로그램의 동작을 감시함(동작 감시)
  - 이를테면, 어느 프로그램이 실행 프로그램에 데이터를 기록하려고 한다면 바이러스 검사 소프트웨어는 이러한 의심스러운 동작을 사용자에게 알리고 무엇을 할 것인지 물어 봄

## 9 백신-접근 방식

- 의심스러운 동작
  - 사전 데이터베이스 접근과 달리, 의심스런 동작의 접근은 데이터베이스에 없는 새로운 바이러스에 대한 보호를 제공함
  - 그러나 수많은 오진이 일어날 수 있으며, 사용자는 모든 경고에 둔감해지게 됨, 사용자가 경고가 뜰 때마다 “허용”을 누르면 바이러스 검사 소프트웨어는 어떠한 작업도 수행하지 않음(오진)
  - 그러므로 현대에 나온 바이러스 검사 소프트웨어는 이 기술을 되도록 적게 사용함

## 9 백신-접근 방식

- 다른 접근
  - 어떠한 바이러스 검사 소프트웨어는 다른 종류의 발견적 분석을 사용함, 이를테면, 제어권을 어떠한 실행 파일에 이행하기 전에 시스템이 호출하는 새로운 실행 파일의 코드의 시작 부분을 가상으로 구현하려고 할 수 있음(발견적 분석)
  - 해당 프로그램이 자가 정정 코드를 사용한다거나 바이러스인 것처럼 보인다면 바이러스가 실행 파일을 감염시킬 가능성이 있다고 추측할 수 있음
  - 그러나 이러한 방식은 많은 오진을 낳을 수 있음(오진)

## 9 백신-접근 방식

- 다른 접근
  - 다른 감지 방식의 경우 샌드박스를 사용하여 수행함, 샌드박스는 운영 체제를 가상으로 구현하여 이 시뮬레이션 안에서 실행 파일을 실행, 프로그램을 종료한 다음, 소프트웨어는 샌드박스를 이용하여 바이러스로 보이는 변경 사항을 분석함(샌드박스)
  - 컴퓨터 성능 문제 때문에 이러한 종류의 검출은 사용자가 요청할 때에만 이루어짐, 또한 이러한 방식은 바이러스가 비결정적이며 실행시 다른 동작을 수행할 경우 실패할 가능성도 있음(비결정적)

## 10 통합 PC 보안 솔루션의 추가 기능

- 공유 자원 접근 제어
  - PC의 공유 자원을 중앙에서 관리하고 통제할 수 있게 하는 기능을 제공
- 패치 모니터링 및 설치
  - PMS와 같이 패치 모니터링과 설치 기능만 제공하는 제품이 별도로 출시되기도 함 (Patch Management System)

## 10 통합 PC 보안 솔루션의 추가 기능

- 파일 암호 및 복호화
  - 침입 사고에 의한 내부 자료 유출을 막기 위해 특정 데이터를 암호화(암호화)
- 주변 기기 매체 제어
  - 시스템에 USB 장치 등의 사용을 통제하는 기능

## 10 통합 PC 보안 솔루션의 추가 기능

- 자산 및 IP 관리
  - 중앙 관리 시스템의 인증을 거쳐야만 네트워크에 접속할 수 있게 하여 각 PC에 대한 정보 수집과 사용하는 IP 관리

- 모니터링
  - 내부자가 외부로 보내는 메일을 확인하거나 네트워크 트래픽을 감시함으로써 기밀 정보 유출을 막을 수 있는 기능

## 11 PC 방화벽 설치하고 사용하기

1. ZoneAlarm 사이트 방문
   - 사이트에서 <FREE DOWNLOAD>를 클릭하여 파일 내려 받기
   - https://www.zonealarm.com/software/free-firewall/

**[무료 PC 방화벽 다운로드 사이트]**


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

# 11 PC 방화벽 설치하고 사용하기

## 2 ZoneAlarm 설치

- 내려받은 파일을 실행하여 ZoneAlarm Firewall을 설치 후 실행

[ZoneAlarm Firewall 실행 화면]


※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

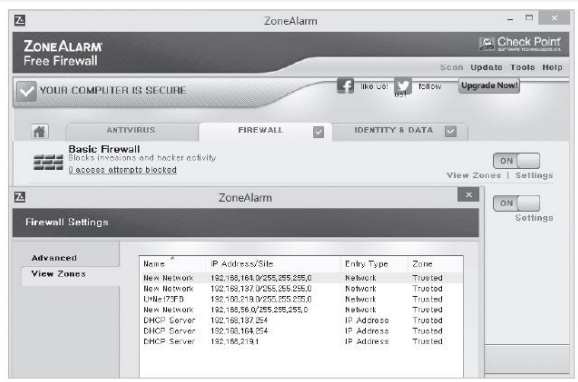
## 11 PC 방화벽 설치하고 사용하기

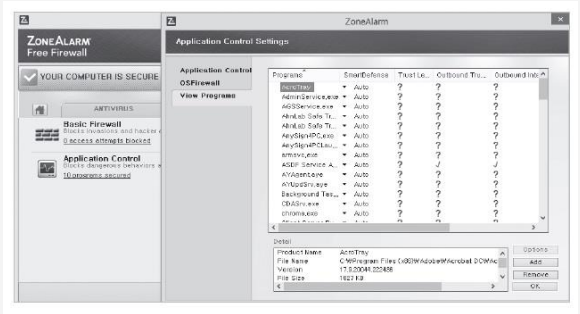
3 네트워크의 방화벽 규칙 확인

- <FIREWALL>을 누르면 실행 중인 프로그램에 대한 방화벽 규칙 확인 가능 (Header → Port, IP)
- 애플리케이션마다 신뢰할 수 있는 정도를 개별적으로 설정할 수도 있음

# 11 PC 방화벽 설치하고 사용하기

## 3 네트워크의 방화벽 규칙 확인




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 12 ZoneAlarm

- ZoneAlarm is an internet security software company that provides consumer antivirus and firewall products. ZoneAlarm was developed by Zone Labs, which was acquired in March 2004 by Check Point

- ZoneAlarm's firewall security products include an inbound intrusion detection system, as well as the ability to control which programs can create outbound connections

## 12 ZoneAlarm

- In August 2015, ZoneAlarm introduced a 100% virus-free guarantee with its Extreme Security product(100%는 없음)

# 2 보안 솔루션 기능

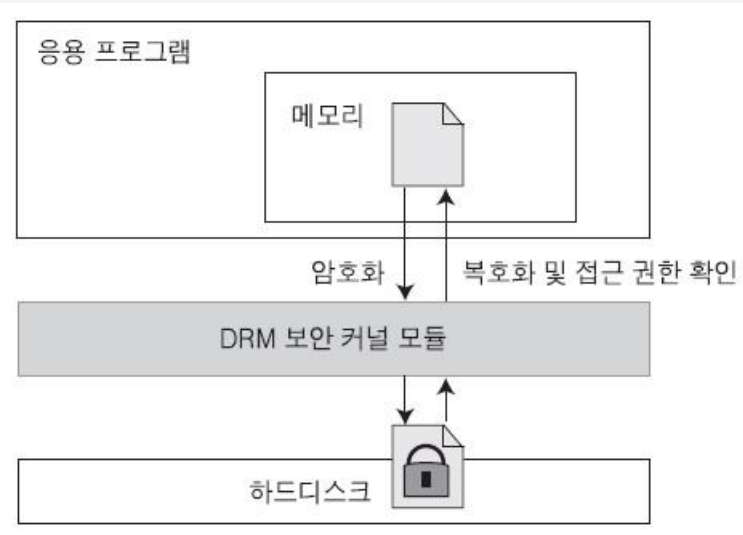
## 1 DRM(digital right management)

- 문서 보안에 초점을 맞춘 보안 기술로, 문서를 열람하고 편집하고 프린트하는 것까지 접근 권한을 설정하여 통제(암호화)

- MS 워드를 비롯해 HWP, TXT, PDF 파일 등 업무에 사용하는 대부분의 파일을 통제할 수 있음

## 1 DRM(digital right management)

### DRM 모듈의 역할




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 1 DRM(digital right management)

- 디지털 권리 관리(Digital rights management, DRM)는 출판자 또는 저작권자가 그들이 배포한 디지털 자료나 하드웨어의 사용을 제어하고 이를 의도한 용도로만 사용하도록 제한하는 데 사용되는 모든 기술들을 지칭하는 용어임

- 이는 종종 복사 방지, 기술 보호 장치와 혼동하기도 함(좁은 의미), 앞의 두 용어는 디지털 권한 관리 설계의 일부로, 이런 기술이 설치된 전자장치 상의 디지털 콘텐츠에 대해 사용을 제어하는 데 사용되는 기술을 지칭함(넓은 의미)

## 1 DRM(digital right management)

- 디지털 권리 관리는 논란의 여지가 있는 분야로 지지자들은 저작권 소유자가 저작물에 대한 불법복제를 막아 지속적인 수입원을 확보하는 데 필요하다고 말함(copyright vs. copyleft)
- 자유 소프트웨어 재단을 포함한 이 기술에 대한 비평가들은 "권리"라는 용어는 오해를 일으킬 수 있으므로 사용을 피하고, 더 정확한 용어인 디지털 제약 관리(Digital restrictions management)로 바꿀 것을 제안하고 있음

## 1 DRM(digital right management)

- 주로 기업의 기밀 사항을 담고 있는 내부 문서를 외부로 유출되지 않도록 관리하는 데 사용됨

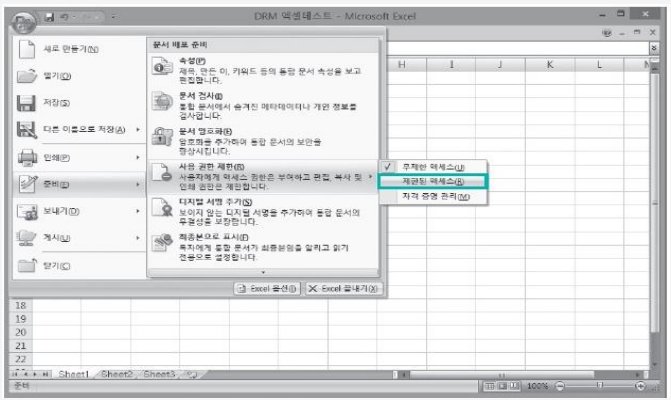
- 기존 CD나 DVD 등을 이용하여 오프라인 상에서 유통되던 많은 음악, 영화 등이 온라인 상에서 유통되고 정당한 금액을 지불하지 않는 불법적인 사용을 차단하기 위하여 인증된 사용자가 인증된 기간 동안만 사용가능 하도록 통제함으로써 불법적인 사용을 제한하고 있는데 이때 많이 사용되는 기술임(MP3 암호화)

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

### 1 MS Office 2007에서 IRM(정보 권한 관리) 이용하기

- 액셀 파일을 연 상태에서 MS Office 로고를 클릭한 후 [준비]-[사용 권한 제한]-[제한된 액세스] 선택

[엑셀 사용 권한 제한]



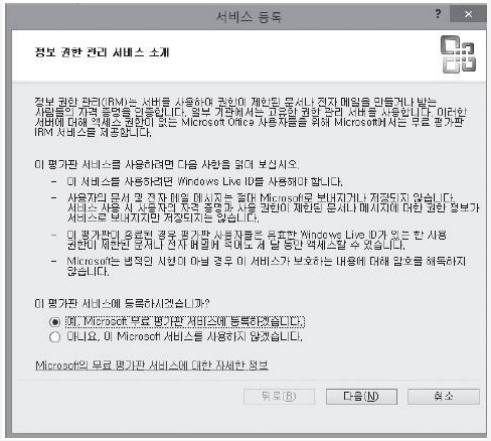

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

# 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

## 2 IRM(정보 권한 관리) 설치를 위한 마법사 실행

- IRM 서비스를 이용할 것인지 묻고, IRM 서비스를 이용할 Microsoft 계정이 있는지 확인

[정보 권한 관리 서비스 등록]



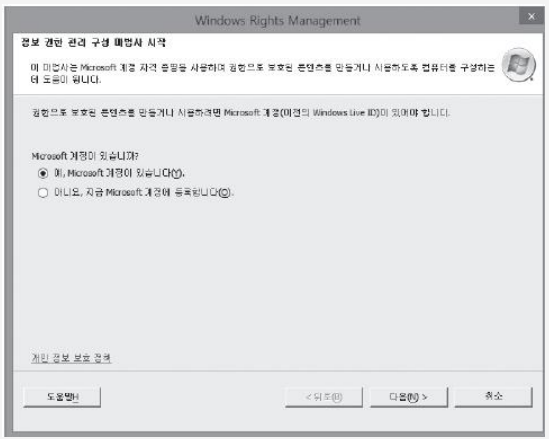

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

2 IRM(정보 권한 관리) 설치를 위한 마법사 실행

- IRM 서비스를 이용할 것인지 묻고, IRM 서비스를 이용할 Microsoft 계정이 있는지 확인

[Microsoft 계정 유무 확인]



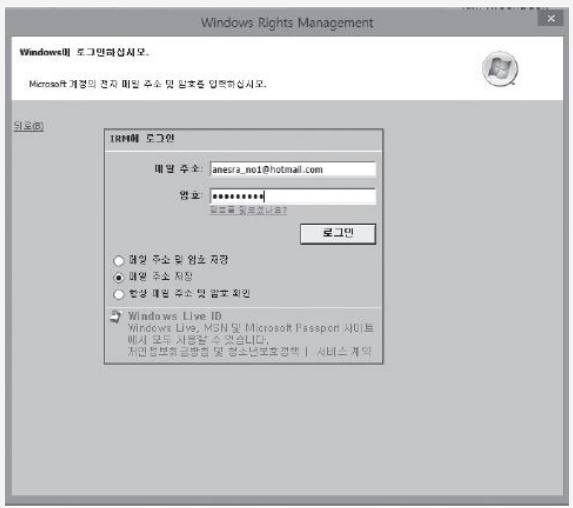

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

### 3 MS Office 계정으로 로그인

- MSN이나 Hotmail 계정이 없으면 새로운 계정을 만든 후 로그인

[윈도우 IRM 로그인 화면]



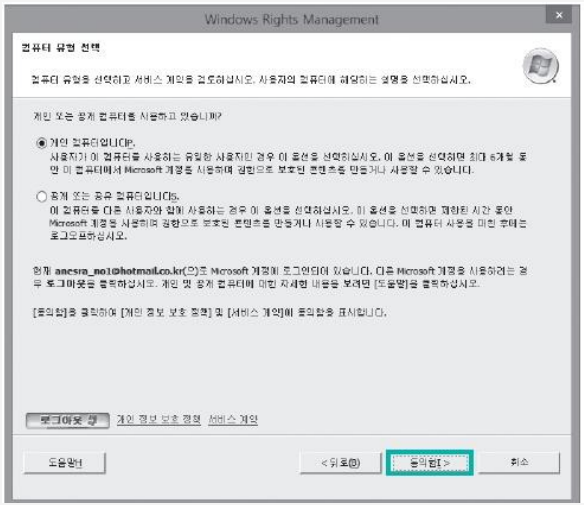

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

### 4 IRM(정보 권한 관리) 서비스 설치 완료

- 컴퓨터 유형을 선택한 후 IRM 서비스 설치 완료

[컴퓨터 유형 선택]



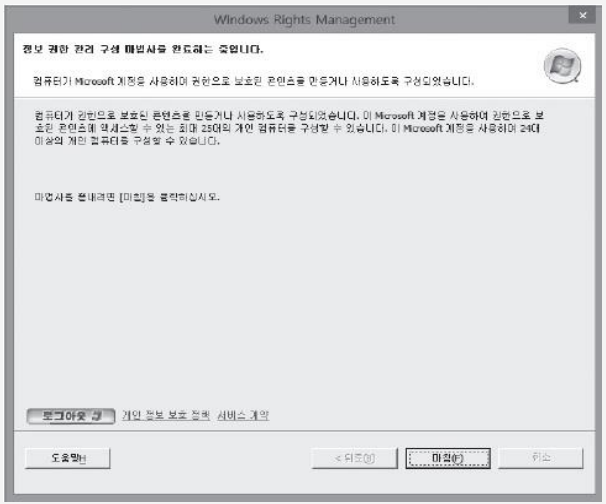

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

### 4 IRM(정보 권한 관리) 서비스 설치 완료

- 컴퓨터 유형을 선택한 후 IRM 서비스 설치 완료

[IRM 설치 마법사 끝내기]

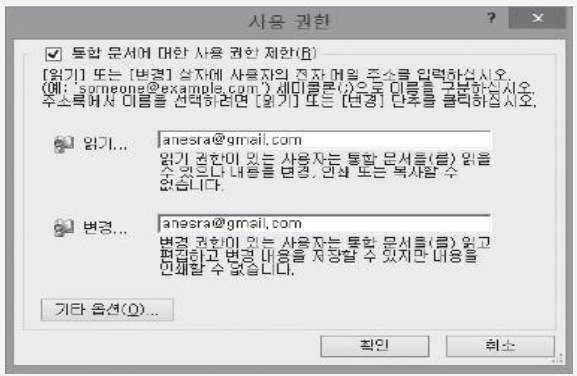



※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

5 IRM 기능을 활용한 사용 권한 설정

- '통합 문서에 대한 사용 권한 제한'에 체크 표시를 한 뒤 '읽기'와 '변경' 부분에 원하는 사용자 이메일 주소를 입력(이메일 주소)



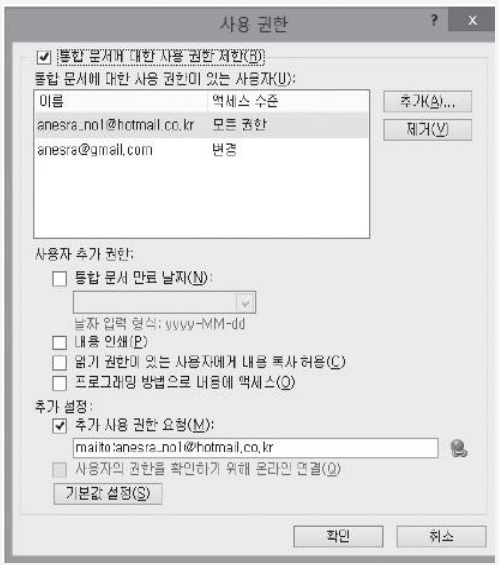

[사용 권한 설정]

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

### 5 IRM 기능을 활용한 사용 권한 설정(기타 옵션)

- '통합 문서에 대한 사용 권한 제한'에 체크 표시를 한 뒤 사용 권한 추가/제거



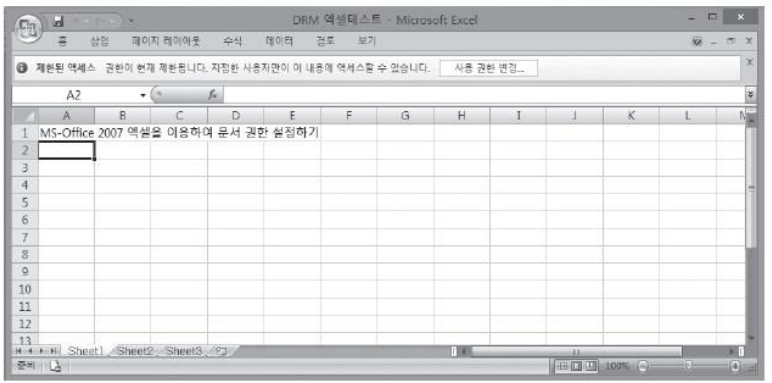

**[사용 권한 설정 : 기타 옵션]**

※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 2 MS Office 2007 엑셀을 이용하여 문서 권한 설정하기

6 사용 권한 설정 결과 확인

- 권한이 설정된 문서에는 화면 상단에 '제한된 엑세스' 창이 나타나고, 이 창에서 사용 권한 설정과 변경 요청을 할 수 있음




※ 출처 : 인터넷 해킹과 보안, 김경곤, 한빛아카데미, 2017

## 3 ESM(enterprise security management)

- 여러 종류의 보안 솔루션을 중앙 집중화된 구조로 모니터링하기 위해 만든 솔루션(Enterprise, 접근제어, 모니터링)

## 4 ESM의 종류

- 보안 또는 관리 정책에 따른
  사용자 및 접근 제어를 위한 ESM(첫번째, 접근제어)

- 최근 주류를 이루는 네트워크 및 시스템 취약점이나
  위험 요소 등을 분석하고 모니터링 하는 관리 도구의
  형태를 취하는 ESM(두번째, 모니터링)

## 5 SIEM(security information event management)

- IT 시스템 및 보안 시스템에서 발생하는 로그를 분석하여 이상 징후를 파악하고, 그 결과를 경영진에게 보고할 수 있도록 하는 시스템(Event)

## 5 SIEM(security information event management)

- In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware

## 5 SIEM(security information event management)

- Vendors sell SIEM as software, as appliances or as managed services; these products are also used to log security data and generate reports for compliance purposes

## 6 SIEM의 기능

- 실시간 위험 탐지 및 대응을 위해
  이벤트 로그 데이터를 실시간으로 수집하고 분석(로그)

- 침해 공격 로그에 대한 포렌식(디지털 증거)과
  컴플라이언스(보안에 대한 방향성 제시) 또는
  법적 조사를 위한 해당 데이터의 신속한 검색 및
  리포팅 기능