情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

# 망 분리기반의 정보보호에 대한 고찰

이 은 배*, 김 기 영**

요 약

정보 통신의 발전으로 인하여 모든 장소에서 인터넷, 인트라넷을 적용하여 외부와의 업무 연속성을 활용하고 있다. 그러나 이러한 환경은 계속적인 기업 내의 정보 유출에 대한 위험으로 내부 정보보호를 위해업무 영역과 개인 영역으로 구분된 환경을 조성하고 있다. 이를 위한 망 분리는 IT기술의 발전으로 물리적인 망 분리에서 가상화를 접목한 논리적 망 분리가 제시되고 있다. 업무 환경의 보호를 위한 망 분리에 대한 다양한 방안과 그 에 대한 장단점을 소개하도록 한다.

## Ⅰ. 서 론

정보 통신의 발전으로 인하여 먼 거리와의 업무 연락 및 비즈니스의 제한 폭이 점점 좁아지며, 특히 인터넷의 발전으로 그 속도는 가속화 되고 있다. 현재 IT 발전 방향의 추세는 기업, 관공서, 기타 모든 곳에서 인터넷, 인트라넷, 익스트라넷 등을 적용하여 외부와의 업무 연속성을 활용하는데 그 목적을 둔다. 이러한 목적은 기업 내 업무 환경의 효율성 증대의 취지에서 벗어나 다양한 정보 유출에 대한 위험성을 내재하고 있다. 인터넷 망이 연결된 내부망은 외부로부터의 해커나 악성 바이러스의 위험을 초래하고 있으며 내부에서는 산업 스파이나 악의적인 내부 사용자로부터 기업 내 중요 자료를 외부로 유출시키는 피해가 계속해서 발생하고 있다. 즉 외부로부터의 악의적 공격으로부터 안전한 환경을 조성하는 것과 더불어 내부 사용자로부터 기업 내 중요 자료를 보호해야하는 필요성은 계속해서 대두가 되고 있다. 기업 내 주요 정보를 보호하기 위한 방안으로 데이터 암호화, 문서 보안, 이메일 보안 및 내부 데이터 손실 방지와 같은 다양한 방안 및 솔루션이 제시되고 있으나 원천적인 내부 정보 보호를 위한 업무 영역과 외부 네트워크 분리의 필요성이 부각되었고 따라서 물리적 망 분리가 요구되어 왔다. 그러나 IT 기술의 발전으로 인하여 가상화 기술이 대두되었으며 이를 바탕으로 한 논리적 망 분리가 새롭게 제시되고 있다.

본 기고에서는 기업 내의 정보 유출 사례를 보고 이에 대한 주요 정보 보호 기법을 살피고 논리적 망 분리의 기반인 가상화 기술에 대한 고찰과 더불어 물리적 망 분리 방안과 논리적 망 분리 방안에 대한 장, 단점을 비교한다.

구성은 2장에서는 기업 내 내부 사용자에 대한 정보 유출 사례와 현재 주요 정보보호 솔루션을 제시하고 3장에서는 논리적 망 분리의 기반 기술인 가상화에 대한 종류 및 기법을 살피고 4장에서는 물리적 망 분리와 논리적 망 분리에 대한 각각의 종류와 장. 단점을 살펴보고 5장에서 결론을 짓는다.

## Ⅱ. 정보 보호 현황

### 2.1 기업 내 산업 유출 피해

최근 첨단산업의 핵심기술이 해외로 또는 경쟁 업체로 유출되는 사건들이 잇따르고 유명 사이트와 금융권 등에서도 개인 정보 유출 사고가 터지면서 내부 정보보호와 개인정보보호에 대한 중요성과 관심은 갈수록 증대되고 있다. 실제 기업들은 산업기술유출방지법, 전자금융거래법, 저작권법, 개인정보보호법 등 관련 법안 및 제도가 강화됨에 따른 발 빠르게 대비를 해야 하는 상황이다. 국가정보원 산업기밀 보호센터의 첨단 산업 기술동향(2007년 9월호)에 따르면, 2003년부터 2007년

* 현재 이니텍(주) 미래기술연구소
** 현재 이니텍(주) 개발본부

사이 적발된 기술 유출 사건만 124건에 이르며 그 피해액은 170초에 달하는 것으로 나타났다. 특히 이 같은 보안 사고의 80%이상이 외부인이 아닌 전, 현직 내부 직원에 의한 것(퇴직직원 65%, 현 직원 27%)으로 밝혀지면서 기업들은 내부정보유출방지 및 데이터 보안에 촉각을 세우고 있다.

기존 보안이 외부로부터 불법적인 침입에 대응하기 위한 것이었다면, 이제는 기업 내부 정보 보호에 초점을 맞춰야하기 때문이다. 보안 시장의 중심이 과거 해킹과 바이러스와 동시에 정보(데이터/콘텐츠) 보안을 강조하는 내부정보유출방지 및 데이터 관리 동시에 필요성이 강조된다.

## 2.2 정보 유출 방지를 위한 방안

### 2.2.1 DB 보안

DB 보안 솔루션은 데이터를 암호화하는 암호화 방식과 DBMS의 접근을 통제하는 접근 통제 방식으로 구분되며 암호화 방식은 원천 데이터에 대해 암호화를 하여 내부 사용자의 접근 시에도 원천데이터에 대한 유출을 방지하는데 목적을 두고 있으며 접근 통제 방식은 사용자별, 접근 방식 별 등의 접근 시 특정 권한을 두어 원천 데이터에 대한 접근을 제어하는 솔루션이다. 이러한 솔루션은 스니핑, 게이트웨이, 에이전트, 보안쉘에 대한 기술적인 지원뿐만 아니라 SQL 사전/사후 정보 저장을 제공하도록 하고 있다.

### 2.2.2 DRM

DRM(Digital Rights Management)이란 디지털 콘텐츠의 불법 유통과 복제를 방지하고, 적법한 사용자만이 데이터를 사용하게 하며, 저작권자의 권리 및 이익을 보호하는 시스템을 의미한다.

DRM 기술은 크게 사용자 허가와 데이터 유출 추적 기술로 나눌 수 있다. 사용자 허가 기술은 데이터를 정당한 권리를 가진 사용자에게만 안전하게 전송하고 허가된 사용범위 내에서 사용하게 제한하는 방법이다[12]. 데이터 유출 추적 기술은 불법적인 방법으로 데이터가 복제되고 유출될 경우, 해당 데이터의 저작권자가 누구인지 증명하고 어떤 경로를 통하여 불법 복제되고 유출되었는지를 추적하는 기능이다[13].

DRM 솔루션은 디지털 콘텐츠 및 문서의 사용 제한뿐만아니라 매체제어 기능과 결합하여 PC 정보 유출방지 솔루션으로 제공된다.

### 2.2.3 이메일 보안 솔루션

기업 내 주요 의사소통 수단 가운데 하나인 이메일을 통해 고의 또는 실수로 발생하는 개인정보, 기업 기밀 및 데이터 유출 사고를 방지하기 위해 이메일을 암호화하는 것이다. 또한 대량 광고 메일을 차단, 사기성 위장 메일을 통한 기업 및 개인정보 유출을 방지하는 기능을 제공하며 메일에 포함된 바이러스를 봉쇄하는 기능으로 발전하고 있다.

### 2.2.4 DLP

기존 내부 정보보호 솔루션의 대명사가 매체제어를 근간으로 한 PC보안과 접근제어를 근간으로 한 문서보안(DRM)이었다면 DLP(Data Loss Preventation)는 DRM, DB 보안, 스팸차단솔루션, 메신저 보안등을 포괄하는 새로운 개념의 종합 정보 유출 방지 솔루션이다.

DLP솔루션은
- 다양한 정보유출 경로를 모두 지원하고 실시간 차단 가능
- 개인 그룹별, 기능별, 정책별 관리 모두 지원
- 데이터 흐름 모니터링 및 유출 시도 시 로그 및 실시간 증거 수집
- 사내 기밀 자료가 변경되거나 포맷 변환되어도 지속적 보호기능 제공
- 내부사용자의 부적절한 자료 유출을 원천 차단

이러한 기능은 기업의 비즈니스 프로세스 상에 있는 정보를 지닌 컨텐츠가 유출되는 것을 막는 것이다. 이 솔루션은 정보유출을 네트워크 게이트 단에서 제어하는지, 호스트 단에서 제어하는지에 따라 네트워크기반 제품과 엔드포인트형 제품으로 구분된다.

### 2.2.5 서비스 분야

SI 기반 업체의 주도하에 기업의 정보유출 방지를 위한 서비스의 차별화된 특징을 제공하는데 다음과 같다.

- 기존의 IT 보안솔루션과 물리보안 솔루션의 유기적인 연계를 통한 다단계적인 보안 통제
- 하나의 관리시스템을 이용한 물리 및 IT 보안 영역에 대한 통합적인 보안정책 설정
- 보안 모니터링 - 실질적인 보안 사고를 유발하는 사람중심의 보안통제 및 관리

## Ⅲ. 가상화

### 3.1 가상화 정의

- 광의의 정의(사전적 의미)

실제로 있지 않거나 모호한 것에 대하여 마치 실제로 존재하는 사실이나 개체로 가정하여 취급하는 것

- 협의의 정의

물리적으로 다른 시스템을 논리적으로 통합하거나 하나의 시스템을 논리적으로 분할해 자원을 효율적으로 사용하게 하는 기술

- 여러 가지 기법으로 한정되어진 물리적 환경의 리소스를 하나의 서비스 또는 여러 개의 서비스 환경을 제공하는 기술
- Gartner

사용자에게 리소스의 물리적 속성이나 영역이 감춰진 채 제공되는 리소스의 모음

- Wikipedia

가상화는 컴퓨팅 리소스들의 논리적 그룹핑이나 하위 세트를 제공하여 원래 설정 보다 더 나은 혜택을 줄 수 있는 방식으로 액세스 될 수 있도록 하며, 이 새로운 가상 리소스는 구현, 지리적 위치, 기반 리소스의 물리적 설정에 제한되지 않는다.

- 한국정보통신기술협회(TTA)

컴퓨터 운용체제(OS)를 시스템 구조나 하드웨어에 영향 받지 않고 설치, 사용할 수 있도록 하는 기술

### 3.2 가상화 기술 유형

#### 3.2.1 하이퍼바이저

하이퍼바이저(hypervisor)는 호스트 컴퓨터에서 다수의 운영 체제(operating system)를 동시에 실행하기 위한 가상 플랫폼(platform)을 말한다. 가상 머신 모니터(virtual machine monitor, 줄여서 VMM)라고도 부르며 일반적으로 2가지로 나뉜다.

① **Type 1 (native 또는 bare-metal)**

운영 체제가 프로그램을 제어하듯이 하이퍼바이저가 해당 하드웨어에서 직접 실행되며 게스트 운영 체제는 하드웨어 위에서 2번째 수준로 실행된다. 이런 방식의 하이퍼바이저는 1960년대 IBM이 개발한 CP/CMS에서 시작되었으며 IBM의 z/VM으로 이어졌다. 최근에는 Xen, Citrix의 XenServer, VMware의 ESX Server, L4 마이크로커널, TRANGO, IBM의 POWER 하이퍼바이저(PR/SM), 마이크로소프트의 Hyper-V, 패러랠서버, Sun의 로지컬 도메인 하이퍼바이저 등이 있다. 또 히타치의 Virtage 하이퍼바이저같이 플랫폼의 펌웨어에 하이퍼바이저를 넣기도 하며 KVM은 하이퍼바이저 안에 완전한 리눅스 커널을 넣었는데 이것도 Type 1 이다.

② **Type 2 (hosted)**

하이퍼바이저는 일반 프로그램과 같이 운영 체제 안에서 실행되며 게스트 운영 체제는 하드웨어에서 3번째 수준으로 실행된다. VMware Server, VMware Workstation, VMware Fusion, QEMU, 마이크로소프트의 버추얼 PC와 버추얼 서버, InnoTek의 버추얼박스, SWsoft의 Parallels Workstation과 Parallels Desktop이 대표적이다.

하이퍼바이저란 System/370의 CP-67을 재작성한 CP-370에서 유래되었으며 1972년 VM/370으로 발표하였다. 하이퍼바이저 콜(hypervisor call), 곧 하이퍼콜(hypercall)이란 게스트 운영 체제가 (보다 높은 수준의) 제어 프로그램에서 직접 서비스에 접근할 수 있는 반가상화(paravirtualization) 인터페이스로 인용된다. - (같은 수준의) 운영 체제에서 감시자 호출(supervisor call)을 요청하는 것과 비슷하다. (슈퍼바이저란 IBM 메인프레임에서 감시 프로그램 상태로 실행되는 운영 체제 커널을 말한다.)

#### 3.2.2 서버 가상화

① 가상화의 분류

서버의 가상화는 자원의 가상화, 플랫폼기반 가상화, 프로세서 기반 가상화(Hypervisor기반 가상화), OS기

반 가상화 등으로 분류되며 일반적인 서버 가상화의 경우 가상머신(Virtual Machine) 이라는 중간계층을 통하여 물리적 서버를 복수의 가상서버로 분할하는 방식 등으로 OS상에서 하드웨어를 에뮬레이션 한다.

가상머신은 특히 윈도우(Window)등의 호스트 OS위에서 구동하는 OS, 즉 게스트 OS를 인스톨 할 수 있으며, 호스트 OS를 개입시켜 CPU, 하드디스크 등의 서버 자원을 사용한다.

② 서버 가상화 기술별 비교

- 플랫폼 기반 가상화 기술

컴퓨팅 자원(CPU, Memory)을 가상화하여 서비스 제공하고 컴퓨팅 자원간의 모든 통신을 가상화로 구현한다.

업무와 서버 하드웨어와의 분리하고, OS로부터 독립성을 확보하여 물리적인 서버 수 및 TCO 절감한다.

- 하이퍼바이저(Hypervisor) 가상화 기술

가장 널리 보급 되어 있는 가상화 솔루션으로 가상서버와 하드웨어 사이에 추상화 레이어(가상화 계층을 갖는 전용 커널)를 배치하는 구조이다.

CPU명령에 끼어들어 하드웨어, 컨트롤러와 주변기기로의 접근을 중개하며, 어떤 OS라도 수정하지 않고 가상 머신위에 바로 인스톨 가능하고 많은 종류의 게스트 OS를 지원하고 싶을 때, 혹은 소프트웨어 품질보증이나 테스트 실시 때 유용하다.

- OS기반 반 가상화 기술

프로세스 상의 부담을 주는 문제를 일부 해결하기 위한 수단으로 게스트 OS를 수정해 가상화 환경을 인식하도록 한 후 하이퍼바이저와 연계하여 가상화한다.

### 3.2.3 하드웨어 리소스 가상화

① 스토리지 하드웨어 기반 통합

기존에 분산되어 사용하고 있던 스토리지를 대용량 스토리지에 물리적으로 통합하여 스토리지를 SAN1)이나 NAS2) 형태로 통합하여 다수의 서버에서 스토리지 자원을 공유한다.

SAN과 NAS는 FC 또는 IP를 통하여 자원을 공유하는 형태이므로 넓은 의미의 스토리지 가상화 개념에 포함되기도 한다.

② 스토리지 가상화 기술

가상화 기능을 제공하는 소프트웨어 또는 별도의 하드웨어 장비 등을 통해 이기종 스토리지를 통합하는 기술로 스토리지 가상화는"물리적인 디스크 드라이브를 논리적 볼륨으로 연결하는 것"을 의미한다.

스토리지 가상화 기법은 가상화를 제공해 주는 자원의 위치에 따라 여러 가지 방식으로 분류된다.

### 3.2.4 데스크톱 가상화

사용자 PC 데스크톱에 대한 OS의 가상화이다. 가상화 환경은 서버와 하드웨어 리소스에 지원을 하였다. 사용자 PC 의 안정적인 환경을 위하여 서버 가상화 기술을 이용하여 일반 사용자 PC OS에 대한 가상화를 제공한다. 서버의 자원과 환경을 사용자가 공유하는 SBC (Server Based Computing), 서버 가상화를 기반으로 하여 사용자 PC thin 클라이언트를 이용하여 서버 가상화에 설정된 클라이언트 OS를 사용하는 서버 중앙형 방식의 데스크톱 가상화와 사용자 PC에서 OS 또는 별도의 인터페이스를 가상화하는 클라이언트 데스크톱 가상화로 나뉘어 질수 있다.

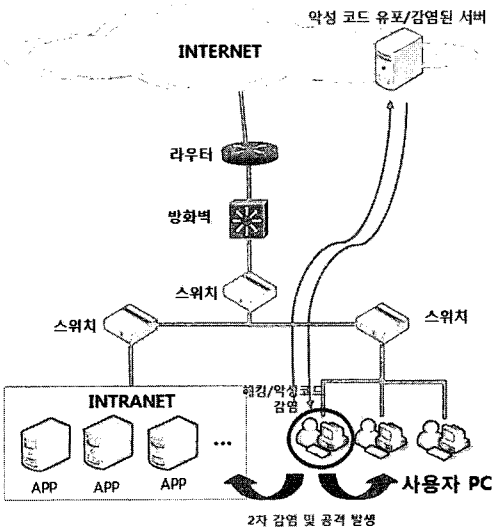
## Ⅳ. 망 분리 방안

### 4.1 목적

기업 내의 PC 환경에서는 외부로 연결되는 인터넷 망을 사용함으로 인하여 악성코드가 감염이 되고 이로 인하여 다른 사용자 PC의 악성 코드의 감염을 유도하게 된다. 이는 내부 서버를 감염시키거나 해킹으로부터 내부 정보 유출의 원인이 될 수 있다. 다음 그림과 같이 인터넷 망의 사용으로 인하여 악성 코드 또는 바이러스의 감염 그리고 외부 정보의 유출을 발생시킬 수 있다

기업 내의 PC 및 네트워크 환경을 업무 영역과 개인 영역을 분리하고 업무 영역은 내부 망을 사용하고 개인 영역은 인터넷 망으로 분리하여 다음과 같은 목적을 가진다.

1. 업무 망 내부의 불법 자료 유출 방지




〔그림 1〕 인터넷 망의 내부 위험

2. 업무 망 내부의 자료 불법 삭제, 변경 등의 해킹 방지
3. Virus, Spy-ware, Gray-ware 침투 원천 방지
4. 업무 효율성의 극대화
5. 자료 및 자원 활용의 실용성 증대

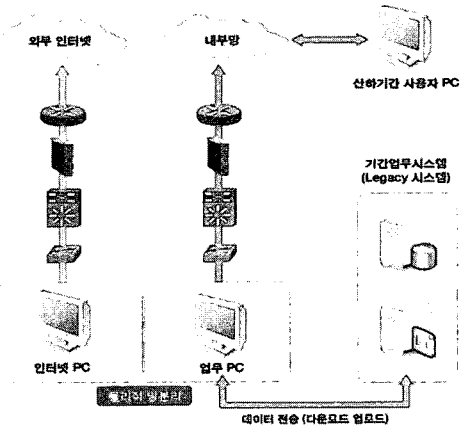
## 4.2 물리적 망 분리

물리적 망 분리는 말 그대로 물리적으로 네트워크를 분리, 외부의 네트워크와 내부의 네트워크를 별도로 구축하며 장점은 물리적으로 분리가 되어 있기 때문에 사용자 인식률이 높아 식별 가능하며 특별한 기술 불필요하다. 물리적인 추가 장치를 이용하여 망 분리를 구성한다. 일반적으로 2대의 PC를 이용한 망 분리와 네트워크 전환 장치를 이용한 망 분리가 있다. 이에 대한 구성 방식, 장점 및 단점을 제시한다.

### 4.2.1 PC 기반의 분리

① 방식

사용자 업무 환경에 업무용 PC와 인터넷용 PC, 2대의 PC로 구성하여 한대는 내부 망 용 다른 PC는 인터넷 망을 구성하여 네트워크를 물리적 분리한다.




〔그림 2〕 PC 기반의 망 분리

② 장점

물리적인 분리를 통한 가시성을 가지며 사용자의 인식률을 높일 수 있다.

③ 단점

사용자 당 2개의 PC가 필요하며 이에 따른 공간 확보와 네트워크 구축 및 추가적인 PC에 대한 비용이 발생하며 높은 전력 소비와 발열량으로 인하여 그린 IT에 역행하게 된다.

### 4.2.2 전환 장치를 이용한 분리

① 방식

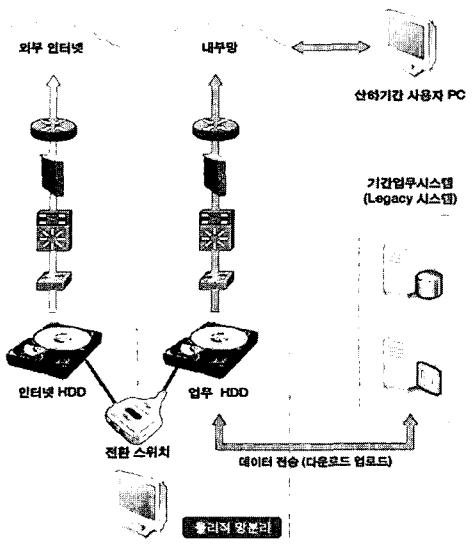
하드디스크, IP, 라우팅 정보 등의 비공유자원을 업무용과 인터넷용으로 분리하여 네트워크를 분리하고 PCI 카드형태의 전환 장치를 사용한다.

② 장점

전환 장치로 PC 2대를 사용하는 것과 유사한 방식을 제공한다.

③ 단점

망 분리를 위해 네트워크 구축 비용의 증가를 초래하며 사용자의 측면에서는 전환 장치를 통한 망 전환 시 사용자 PC 재 부팅으로 인하여 업무의 효율성을 저하 발생하며 인터넷을 통한 자료 수집에 대한 비효율성을 증대시킨다.




〔그림 3〕 전환 장치를 이용한 망분리

### 4.2.3 물리적 망 분리의 고찰

물리적 망 분리 적용 시 다음과 같은 위험을 고려해야 한다.

- 망 분리 이후 업무용 PC와 인터넷용 PC 사이 자료 이동 및 공유
- 업무PC의 인터넷 연결 시 유출 가능한 유통 경로 발생 가능성
- 업무 PC의 관리 소홀로 인한 정보 유출 가능성 및 고의적인 유출에 대한 가능성 존재
- 업무 데이터의 이력관리 방안이 미비, 사후 감사 및 유출 시 추적 자료 부재
- PC의 바이러스 감염이나 이동 저장 장치, 인쇄 캡쳐 등의 PC활용을 통한 유출 가능성 존재

물리적 망의 분리만을 통한 내부 정보 유출 및 악성코드 방지는 어려우며 추가적인 정보 유출 방지를 위한 솔루션 도입 또는 보호 방안을 마련해야 하며 업무 자료의 암호화 및 사용자 인증, 보안 정책관리에 대한 추가 적인 보호 방안이 마련되어야 한다.

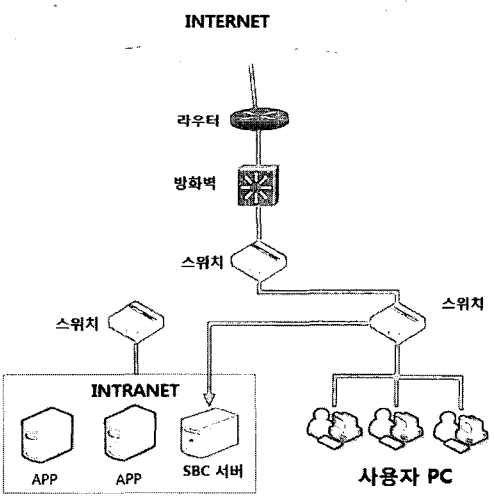
## 4.3 논리적 망 분리

논리적 망 분리는 주로 가상화 기술을 기반으로 하여 가상화 구성 방식에 의해 업무 영역과 개인 영역으로 구분되어 지며 가상화 영역의 망 분리를 통해 1 대의 PC에서 업무 영역의 분리와 네트워크 가상화를 이용하여 망 분리를 논리적으로 구성한다. 가상화 기반 기술은 사용자 인증을 통한 서버 접속 또는 보안영역 접속방법으로 문서가 생성, 조회되거나 다운로드 되는 일련의 과정이 중앙서버 또는 보안 영역을 벗어날 수 없어 정보 유출을 차단하고 사용자의 이벤트에 대한 이력 관리가 가능하며 기업의 보안 정책에 따라 데이터 및 사용자 관리가 가능하다.

### 4.3.1 SBC(Server Based Computing) 기반의 분리

① 방식

PC의 터미널을 이용하여 중앙에 가상 머신을 탑재한 서버에 접속하여 서버의 응용프로그램을 활용하고 데이터를 저장하는 등의 업무를 처리하는 방식




〔그림 4〕 SBC 기반의 망 분리

② 장점

사용자의 업무 수행 정보의 저장 및 작업을 서버에서 수행하여 서버의 중앙 집중 관리로 통제가 가능하다.

③ 단점

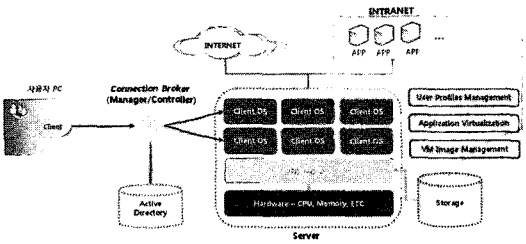
사용자 PC의 활용도가 없으며 한 서버에 여러 사용자의 사용으로 인한 타 사용자에게 데이터 공유 및 업무 환경의 침해가 발생할 수 있으며 사용자 별 응용프

로그램 설치에 제약을 받게 된다.

4.3.2 서버 중앙 방식 데스크톱 가상화 기반 의 분리

① 방식

중앙 서버의 하이퍼바이저에 사용자 별 클라이언트 OS를 가상화하여 연결된 사용자의 OS를 구동하여 사용자 PC에 설치된 클라이언트 연결 프로그램을 이용하여 서버에서 구동되는 가상화된 OS를 사용하는 방식이다.




〔그림 5〕 서버 중앙 방식의 가상화 기반의 망 분리

위의 그림을 보면 사용자 별 가상화된 클라이언트 OS는 사용자의 설정된 프로파일과 응용프로그램 정보를 이용하여 패키징을 하고 이를 서버 스토리지에 저장하여 사용자 PC에 설치된 클라이언트 프로그램을 실행시킬 때 Active Directory를 통해 사용자 인증 완료 후 해당 설정된 클라이언트 OS를 사용하게 된다. 서버의 네트워크 설정에 의해 인터넷 망 또는 내부 망 연결 및 업무 영역 또는 개인 영역으로 사용할 수 있다.

② 장점

사용자 PC 환경에 관계없이 클라이언트를 통해 서버에 설정된 가상 환경을 사용하기 때문에 중앙 통제가 원활하며 유지 보수 및 업그레이드가 수월하다

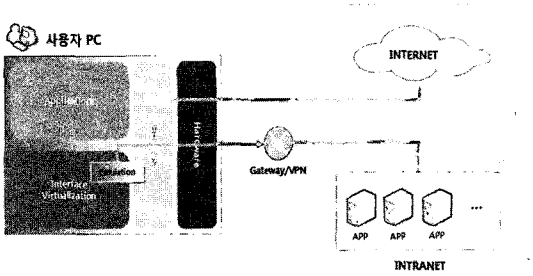
③ 단점

서버의 자원 및 환경에 종속되므로 인하여 사용자의 급증으로 인한 성능 저하 또는 추가적인 서버가 필요하다.

4.3.3 PC 데스크톱 가상화에 의한 분리

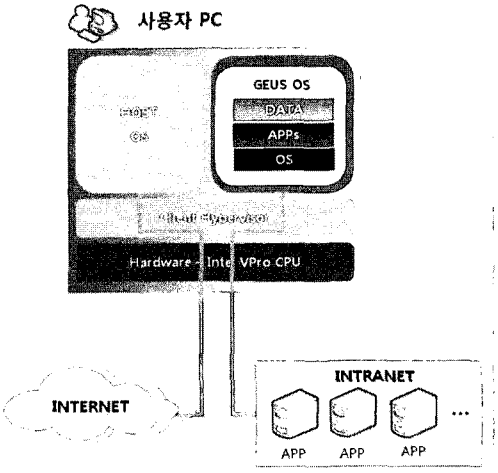
① 방식

PC 데스크톱 OS를 가상화하는 방식으로 Host OS와 Guest OS로 구성하여 각각의 영역에 대해 다른 네트워크 설정을 하여 망을 분리한다.




〔그림 6〕 PC 인터페이스 가상화에 의한 망 분리

위의 그림과 같이 가상화된 영역에 Host OS와 연결된 에뮬레이션 또는 가상 네트워크를 구성하여 연결하는 방식과 아래 그림과 같이 클라이언트 하이퍼바이저를 이용하여 두개 이상의 OS에 별도의 가상 네트워크를 사용하는 방식으로 구분된다




〔그림 7〕 클라이언트 하이퍼바이저에 의한 망분리

② 장점

추가 적인 서버 및 시스템 구축 없이 기존 사용자의 PC 환경을 사용하여 구축할 수 있다.

③ 단점

Host OS에 대한 인터페이스 가상화를 이용하는 경우 Host OS의 커널에 종속적이기 때문에 Host OS가 해킹 또는 바이러스에 감염되는 경우 가상화 영역도 악영향

을 받게 된다. 또한 클라이언트 하이퍼바이저를 이용한 방식은 CPU가 가상화를 지원하는 CPU이어야 하며 신규 설치에 가능함으로 기존의 OS환경을 모두 재구축해야 한다.

#### 4.3.4 논리적 망분리에 대한 고찰

가상화를 이용한 논리적 망분리 시 다음과 같은 사항을 점검 및 확인하여야 한다.

- 가상화 영역의 선정, 내부 망을 가상화 할 것인지 외부 망을 가상화 할 것인지 여부 결정
- 가상화 영역에 대한 응용 프로그램에 대한 호환성 여부 확인
- 가상화로 인한 소프트웨어 라이센스 변화 확인
- 가상화 기술 적용을 위해 기술적, 업무적, 서비스 및 프로세스, 제도적, 조직적 변화와 보안등에 대한 고려가 선행

## V. 결 론

기업 내에 축적된 정보의 보호는 기업이 유지하고 발전하는 기본 사항이다. 정보 유출에 대한 끊임없는 위협은 외부와 내부 모두에서 계속적으로 시도되고 있으며 이를 방지하기 위한 노력도 계속 될 것이다.

망 분리를 통한 폐쇄 망의 구조만으로 기업 내의 정보가 보호가 될 것으로 생각은 가장 큰 오판이 될 수 있다. 내부 사용자에 의한 정보 유출 및 해킹, 바이러스 유포는 오히려 더 큰 위험인 것이다.

내부 정보 보호를 위한 망 분리는 제시한 물리적 망분리와 논리적 망 분리에 대한 기업 내의 보유 자산과 비용적인 측면을 고려하여 망 분리의 모델을 선정해야 할 것이다.

## 참고문헌

[1] 국내 1000대 기업 대상 보안 조사, 대한상공회의소 2007.

[2] 최종현, 이병희, 김승주, 원동호, "DRM(Digital Rights Management)기술", 정보과학회지 제25권 제5호, 2007. 5, pp. 17~21.

[3] www.moazine.com.

[4] 김정은, 내부정보유출 방지 ,컴퓨터 월드 2009년 5월호.

[5] ko.wikipedia.org.

[6] IBM Corporation, Version 2 Release 1 (2005), publib.boulder.ibm.com description of basic concepts.

[7] 정보통신연구진흥원, 주간기술동향 제1802호'서버 가상화 기술 동향', 2007. 6. 2.

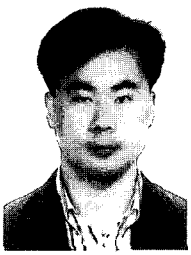
[8] 한국정보사회진흥원, "IT기반구조 및 운영방식 기술 트랜드", 2007.

[9] 한국정보사회 진흥원, "가상화 기술현황과 공공기관 적용 시사점" 2007.

[10] www.citrix.com.

[11] www.vmware.com.

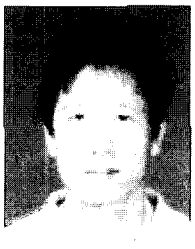
## 〈著者紹介〉



**김 기 영 (Kiyoung. Kim)**

정회원

1997년 2월: 한양대학교 전자공학과 졸업 (학사)
1997년 2월: 포스코
1998년 1월: 한국후지쯔
2000년 10월: 소프트포럼
2009년 10월: 이니텍 상무



**이 은 배 (Eunbae Lee)**

2000년 2월: 명지대학교 수학과졸업
2004년 8월: 숙명여자대학교 정보통신대학원 졸업(석사)
1999년 11월: 렌탈브레인
2004년 8월: 구름커뮤니케이션
2005년 9월: 이니텍