기업 시스템 관리를 위한 클라우드 환경에서의 연구

박현진*, 이신재**
*고려대학교 컴퓨터정보통신대학원 소프트웨어공학과
**고려대학교 컴퓨터공학과
e-mail : noisygene@gmail.com *
shinjae01@gmail.com **

A Study of the Management for Enterprise Systems on Cloud Environment

Hyun jin Park*, Sin jae Lee**
* Graduate School of Computer & Information Technology, Korea University
** Dept. of Computer Science and Engineering , Korea University

요 약

IT 기술의 발전과 변화에 따라 기업에서는 기업용 시스템 관리를 위하여 가상화 컴퓨팅 시스템을 도입을 추진 중이며 비용 절감 및 보안 이슈들을 검토하기를 앞다투고 있다. 따라서 본 논문에서는 가상화 기술의 종류 및 방법들을 연구하여 보고 사례 분석 등을 통하여 기업 시스템 관리를 위한 폐쇄적 가상화 컴퓨팅 시스템 기술의 방법을 제시해보며 효과 분석을 도출해본다.

1. 서론

최근 IT 기술의 집약적인 발전과 변화에 따라 대용량 컴퓨팅의 관심이 증폭 발전 되어가고 있다. 인터넷과 더불어 컴퓨팅 자원을 기반으로 하는 다양한 형태의 정보를 제공하는 서비스의 요구들이 강력하게 나타났다. 기존의 기술 중심의 메인 프레임 및 클라이언트-서버 환경의 비즈니스 컴퓨팅 환경에서 소프트웨어, 플랫폼, 인프라 등 모든 컴퓨팅 자원의 서비스를 제공하는 클라우드 컴퓨팅으로 발전 되어가고 있다.

<표 1> 클라우드 컴퓨팅 서비스 유형별 모델

SaaS (Software as a Service)	- 애플리케이션의 기능을 네트워크를 경유해 이용할 수 있는 서비스 - 다양한 애플리케이션을 다중 임대 방식을 통해 On-demand 형태로 제공 - 기업 직원들과 같은 다수의 사용자에게 공통으로 필요한 소프트웨어를 서버에서 서비스 소프트웨어를 배포하고 관리하여 품질과 사후 관리를 제공
PaaS (Platform as a Service)	- 애플리케이션을 서비스하는 플랫폼 기능을 네트워크를 경유해 이용할 수 있는 빌드형 서비스 - 클라우드 서비스 사업자는 PaaS 를 통해 서비스 구성 컴포넌트, 호환성 제공 서비스를 제공 - 클라우드 컴퓨팅 기술이 제공하는 이점을 활용 하여 어플리케이션 서비스를 직접 배치 구동 관리할 수 있도록, 소프트웨어 개발 도구와 자동화된 클라우드 서비스 사이클 관리 기술 탑재
IaaS (Infrastructure as a Service)	- 서버, 스토리지, 네트워크를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있게 서비스를 제공하는 호스트 서비스 방식 - 서버, 클라이언트, 소프트웨어, 스토리지 공간, 네트워크 장비 등을 서비스 형태로 필요한 컴퓨팅 자산의 일부 또는 전체를 빌려 쓰는 방식

클라우드 컴퓨팅은 네트워크 상의 데이터 서버에 프로그램을 두고 단말기와 휴대용 단말장치 등에서 네트워크에 기반한 소프트웨어 서비스를 사용자들이 인프라 구조에 대한 전문 지식이 없이도 사용할 수 있는 큰 장점이 있지만 최근 기업에서 최근 빈번히 일어나는 보안 사고들을 심각하게 고려해야 한다. 정부의 “정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령” 법률에 따라 금융사업자와 다수의 개인정보를 다루는 기업은 의무적으로 가상화와 망 분리를 시행하도록 법이 개정되었다. 그래서 다수의 금융권 회사들이 망 분리 및 가상화 시스템 구축 사업을 도입하고 있으며 몇몇 기업에서는 이미 도입이 된 사례가 많이 나타나고 있다.

이에 본 논문은 보안도가 높은 폐쇄형 기반의 업무 시스템 에서 적용 할만한 가상화 컴퓨팅 기술과 네트워크 방법들을 적용 해보고 보안 취약점을 보완하는 방법들을 연구 또는 제시해본다.

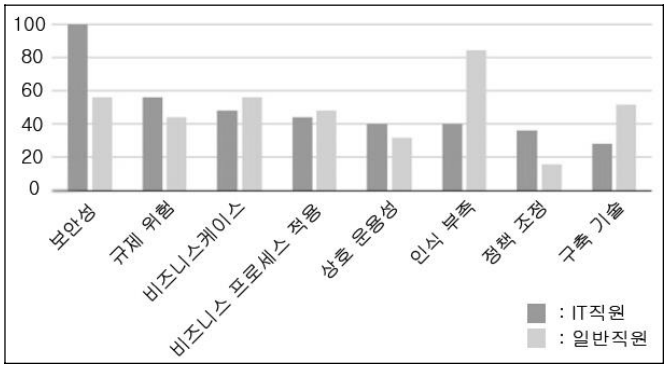
2. 연구방법

본 연구는 보안이 높은 기업 업무용 인터페이스 환경을 구현하기 위해서 적합한 가상화 컴퓨팅 서비스 방법을 찾아 적용하고, 효과적인 가상화 컴퓨팅 방법을 찾기 위해 진행 되었다. 외부 유출이 통제된 망

분리가 된 폐쇄적 업무 시스템에서 보안 향상을 위해 서버의 가상화 방법과 단말장치의 가상화를 통한 기업형 인터페이스 모형을 찾고자 하였다. 거기에 망 분리 방법을 연구하여 가상화와 망 분리가 함께 적용된 업무시스템을 연구하였고 또한 구축된 사례와 해외 도입 사례 들을 분석하여 효율적인 가상화 컴퓨팅 시스템 도입 방법들에 관한 연구를 진행한다.

2.1 가상화 시스템 도입의 문제점

우선 기업에서의 클라우드 컴퓨팅 기술 적용의 장애물 요소 조사 결과는 아래의 그림과 같은 결과를 나타냈다.



(그림 1) 클라우드 기술의 장애물 조사

IT 직원들은 보안성에 중점을 많이 두었으며 일반 직원들은 가상화 시스템의 생소함에 무게를 많이 실었다. 일반적인 클라우드 컴퓨팅 가상화 기법을 도입하여 위의 조사 결과와 같은 보안 위험도를 낮추고 일반 직원들에게 가상화 시스템의 효과적인 인식 확립과 쉬운 운용성을 제공하는 방법을 선택 하여야 한다.

2.2 가상화의 종류

서버 가상화의 종류로는 하이퍼바이져 형과 호스트 형으로 크게 나뉘어진다. 물리적 하드웨어에서 직접 동작하느냐 가상 머신 모니터에서 동작하느냐로 나뉘며 서버 가상화를 통해 하드웨어적 물리 자원에 얽매이지 않고 분리적으로 시스템을 활용할 수 있게 된다. 서버의 활용도가 높아지며 운용체계를 하드웨어와 분리하여 구동함으로 다양한 애플리케이션과 기업 업무용 프로그램 자원들을 활용할 수 있게 된다.

<표 2> 서버의 가상화 유형별 모델

하이퍼바이져 형 – Type 1	호스트 형 – Type 2
- 물리 컴퓨터의 하드웨어에서 직접 동작 - 오버헤드 적고 리소스 관리가 유연 - 별도 관리콘솔 필요	- 가상화 머신 모니터(VMM)에서 동작 - 오버헤드가 크지만 대부분의 OS 에서 동작

하이퍼바이져 형 가상화는 가상화 머신 모니터를 하드웨어상에 직접동작 시켜 호스트 OS 가 필요 없다. 또한 호스트 형 가상화는 물리적 컴퓨터 상의 호스트 OS 위에 가상화 머신 모니터를 설치해 이 가상화 머신 모니터 위에 게스트 OS 를 동작시키는 방법이다. 일반적 상용화 된 많은 가상화 소프트웨어 들이 이러한 형태를 나타내고 있으며

데스크톱 가상화는 VDI(Virtual Desktop Infrastructure) 서버에 클라이언트 OS 환경을 통째로 설치하여 이를 원격의 단말을 통해 활용하는 방법이다. 서버 가상화와 같이 여러 개의 가상 단말을 만들어 사용자는 별다른 OS 설치 없이 자신의 PC 를 사용하듯 사용하게 된다.

2.3 가상화 시스템의 효과

가상화 시스템의 도입 효과에 관련된 많은 수의 보고서에서는 기업들의 많은 시스템이 가상화로 이루어질 경우 다수의 직원들이 혜택을 받는 것으로 나타내고 있다. 비용 절감, 보안 강화 등의 장점은 확실하지만 직원들의 업무 효율성 및 시스템 인식을 가장 크게 고려하지 않는다면 실패된 시스템으로 전락될 수 있다. 사용자들의 업무 소통과 가상화 시스템의 장점을 결합하여 정교한 업무시스템 제어와 지속적인 비용절감(장비 및 License 등) 효과를 기대할 수 있다.

가상화 시스템을 도입하려면 고객들과 직원들의 도입 초기 업무 시스템 적응과 인식이 쉽지 않다. 또한 도입 비용이 비싼 등의 단점이 있다. 기업에서는 가상화 클라우드 컴퓨팅을 보안에 취약하고 외부에 노출이 된다고 여기고 있어 도입을 꺼려하거나 주저하고 있다고 한다. 하지만 폐쇄적 기업용 업무시스템에서 기업 업무용 가상화 인프라 시스템을 구축하여 사용한다면 업무 효율 및 자원의 활용도가 높아지고 불필요한 서버 및 자원을 줄이고 애플리케이션을 하나로 통합하면 비용 절감에도 큰 기대를 가질 수 있게 된다. 이러한 효과로 국내와 해외에 진입 장벽이 쉬운 클라이언트 기반의 손쉬운 솔루션 업체들이 많이 생겨나고 있다.

<표 4> 해외에서의 클라우드 컴퓨팅 도입 사례

구분	내 용
A 사	하둡 기반 데이터 분석 클라우드 시스템 도입
B 사	전 세계 직원용 클라우드 기반 업무시스템 도입
C 사	사내 개별적 시스템 클라우드 컴퓨팅 기반 통합
D 사	각 계열사 통합 클라우드 기반 인증서비스 도입
E 사	모바일뱅킹 및 리테일뱅킹 지원 앱클라우드 구축
F 사	정보계 업무 전반 금융 클라우드 회사에 아웃소싱
G 사	인트라넷, 정보계 빅데이터 클라우드 시스템 도입

2.4 망 분리 방식의 종류

망 분리 방식의 종류는 크게 물리적, 논리적으로 나눌 수 있다.

<표 3> 망 분리 방식 종류

구분	물리적 망 분리	논리적 망 분리	
		PC 기반	서버기반
운영방법	업무/개인용 2 대	PC 내 선택	외부망
도입비용	높음	낮음	보통
추가장비	추가 PC 1 대	게이트웨이	서버구축
보안	매우 높음	낮음	높음
장점	위협 원천 차단	도입 간편	보안성 우수
단점	비용 증가	성능 저하	복잡한 구성

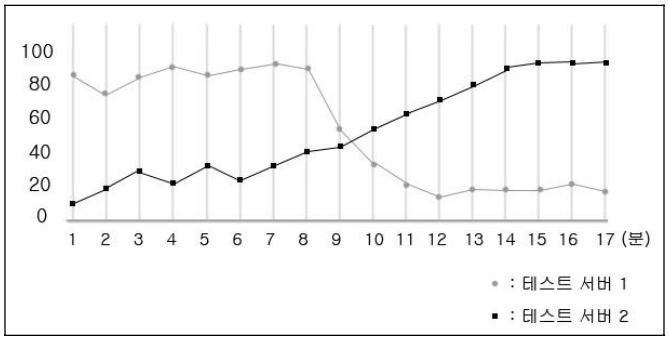
물리적 망 분리는 네트워크 장비와 통신 네트워크를 별도로 이원화 하여 업무 망과 인터넷 망을 분리하여 PC 를 2 대 이상 사용해야 한다. 네트워크가 분리 되어 있으므로 보안성은 높지만 별도의 망을 구축해야 하기에 제반 시설 및 인프라 구축 비용이 많이 든다.

논리적 망 분리는 물리적으론 같은 네트워크를 사용하나 가상화 방법을 통하여 각각의 네트워크를 접근할 수 없도록 구성한다. 서버기반의 논리적 망 분리 방식과 PC 기반의 논리적 망 분리 방식이 있다. 추가되는 장비는 적고 도입이 간편해 보안성은 높지만 성능저하 및 복잡성 증가로 높은 기술력을 필요로 한다.

3. 연구 제안 및 결과

선행 조사 내역들과 같이 가상화 기술 방법 파악 및 사례 분석 결과를 토대로 고려할 때 기업이 가상화 업무 시스템을 도입 효과를 최대화 하기 위해서는 아래와 같은 방법 모델들을 적용하길 연구 제안한다.

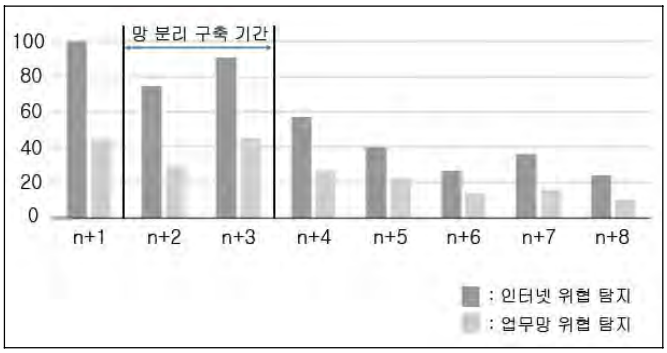
업무 시스템 서버의 가상화는 분석에 따라 효율성을 최대화 한 모델인 하이퍼바이져 형 기반의 상용 전가상화 모델 프로그램을 선택하여 서버 테스트를 진행하였다. 가상화의 장점을 통해 유연하게 여러 대의 서버를 설치할 수 있었으며 CPU 및 I/O 리소스 사용률을 분석하였다.



(그림 2) 가상화 서버 리소스 사용률 추이 시뮬레이션 결과

각각의 테스트 서버에서 CPU 연산과 대용량 I/O 를 수행하였으며 테스트 서버 1 과 서버 2 를 교대로 가상화 서버를 활용해보았다. 여러 개의 가상의 단말들에 가상화 머신 모니터 프로그램을 설치하여 다중 연산 시뮬레이션을 수행 하였다. 리소스를 효율적으로 로드밸런스 하여 자원이 최대한 활용될 수 있어 자원 사용의 효율성을 확인할 수 있었다. 하지만 두 대의 서버 모두 CPU 와 I/O 중 하나로 몰리는 업무 시스템의 경우 별도의 독립적 어플리케이션 서버를 두는 편이 좋다. 또한 하나의 물리적 서버로 운영이 되어 열 및 전력 리소스가 절감되어 여러 대의 서버를 운영하는 기업의 경우 비용 절감 효과도 기대해 볼 수 있다.

위와 같은 시스템 가상화와 함께 기업의 업무 데이터 유출을 줄이고 보안을 증대 시키고자 이중으로 물리적 망 분리를 함께 구성한다. 사용자 단말의 망 분리는 망 전환 장치를 사용하여 물리적으로 저장공간을 각각 분리한다. 하지만 저장 장치 이외의 하드웨어 자원을 함께 사용함으로 자원 활용도를 높이고 비용을 절감한다. 또한 가상화 서비스의 데이터 유출을 강력하게 막아주게 된다.



(그림 3) 보안 위협 탐지 추이 시뮬레이션 결과

보안 위협 탐지 시뮬레이션은 망 분리 전의 위협 시뮬레이션과 망 분리 후의 시뮬레이션을 순차적으로 수행하였다. 가상의 업무용 단말 클라이언트에 기업용 업무 프로그램을 설치하고 가상의 위협 상황을 만들어서 위협을 시도하고 보안 프로그램의 위협 탐지 결과 값을 분석하였다. 그 결과 망 분리 후 인터넷을 통한 업무 시스템으로의 보안 프로그램의 위협 탐지 수치는 망 분리로 인해 70% 이상 줄었고 업무 망에서의 위협 탐지 수치 또한 하락하였다. 데이터 유출 등의 보안 사고 위험을 줄이기 위해 네트워크 탐지 활동과 암호화 등의 기술을 적절히 사용한다. 그리고 가상화 시스템의 단점일수 있는 데이터 소실 위험을 줄여서 무결성에 위배되지 않아야 한다.

그 결과 상호 보안성 향상과 효율성 및 운용성이 높아지고 기업은 비용 절감으로 인한 이익 창출도 기대된다.

4. 결론 및 향후 과제

최근 기업에서는 IT 인프라 투자의 효율성을 끌어

올리기 위한 수많은 노력을 기울이고 있다. 반복적으로 빈번히 나타나는 보안 사고들을 대비하고 원천 차단하기 위해서는 기업용 업무시스템을 폐쇄적인 가상화 시스템 인프라 도입을 검토하는 것도 하나의 방법이 될 수 있을 것이다. 운영하는 자원을 가상화 된 독립적 환경으로 구축하고 가상화 사용자 영역을 제공함으로 보안 인프라도 구축 되게 되고 내부적 시스템 결함이나 장애 발생시 빠르게 대응할 수 있게 되므로 이익 창출이 목표인 기업에서는 효율성을 기대해봐도 좋다. 이에 따라 현재 관련 연구들이 많이 진행 되고 있으며 더 많은 사례들이 앞으로 나오게 된다.

본 논문은 기업에서의 시스템 관리를 위한 가상화 컴퓨팅 시스템을 위한 제반 기술 및 도입 방법들을 다루었으나 추후 진행되는 연구에는 독립적 가상화 시스템 내에서의 네트워크 보안 방법들을 추후 연구하여 기업의 가상화 시스템 운영에 관한 사례들과 운영 현황들을 연구할 예정이며 보안 위협에 관한 사례 및 개선 방법들의 연구가 진행 될 예정이다.

참고문헌

[1] J. Szefer, and R. B. Lee, “Architectural Support for Hypervisor-Secure Virtualization,” In Proc. of ASPLOS XVII, pp. 437-450, 2012.

[2] Cloud Security Alliance, “The Notorious Nine Cloud Computing Top Threats in 2013”, Jan. 2013.

[3] 김인혁, 김정한, 엄영익 "안전한 클라우드 컴퓨팅 환경을 위한 중첩 가상화 기법" 한국컴퓨터정보학회 하계 학술대회 논문집 제 21 권 제 2 호

[4] 방송통신위원회, “정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령”, pp.5, 08.2014

[5] 장승재, 손경호, 이용필 “클라우드 서비스 환경에서 데이터 보호를 위한 정보보호 고려사항” 정보보호학회지 2014.12

[6] 강승석, 손예진, 문은지 “클라우드 컴퓨팅 서비스 구현을 위한 네트워크 가상화 연구” 한국지역정보회학회지 제 13 권 3 호 2010.09

[7] 이향진, 손경호, 이재일 “클라우드 서비스 기반의 기업 정보보호 강화 방안” 정보보호학회지 제 23 권 4 호 2013.08

[8] 주헌식 “클라우드 컴퓨팅 기술동향과 관점” 한국인터넷정보학회 2010.12

[9] 서정준, 신영상, 정현철 “클라우드 컴퓨팅 환경 기반의 가상화 기술 및 네트워크 분석기법 관련 동향” 정보보호학회지 2012.11