클라우드 컴퓨팅의 보안 전략

김아용 · 박성현 · 하의륜 · 저순 · 박만섭 · 김종문 · 정회경

배재대학교 컴퓨터공학과

Security Strategy in the Cloud Computing

A-yong Kim · Sung-Hyun Park · HE YILUN · CHU XUN · Man-Seub Park · Jong-Moon Kim · Hoe-kyung Jung

Department of Computer Engineering, PaiChai University

E-mail : janlssary@puc.ac.kr, {enoid00, mrheyilun}@gmail.com, 846045855@qq.com, ceo@egluon.com, elcomtech@elcomtech.co.kr,hkjung@puc.ac.kr

요 약

스마트 기기의 보급화로 인해 IT 생태계는 변하고 있으며, 이로 인해 기업들로 하여금 클라우드 컴퓨팅 분야가 이슈화 되고 있다. 클라우드 컴퓨팅은 IT 비용을 절감하며, 친환경적인 그린 IT를 지향한다. 또한, 모든 IT 기기를 지원하여 이동시에도 실시간으로 업무를 처리할 수 있다. 이러한 장점으로 인해 많은 기업들은 클라우드 컴퓨팅 서비스를 도입 및 검토 중에 있으며, 클라우드 도입시 저해되는 요인은 보안이다.

이에 본 논문에서는 클라우드가 갖고 있는 보안 문제점을 분석하고, 올바른 가이드라인을 제시한다. 이는 클라우드 컴퓨팅 시스템 및 서비스의 제공분야에 활용될 것으로 사료된다.

ABSTRACT

IT ecosystem is changing with the spread of smart devices and thus, cloud computing fields have been issued to companies. Cloud computing reduces IT costs and aims for eco-friendly Green IT. It also supports all kinds of IT equipment so you can conduct business in real time when moving. With these advantages, many corporations are considering cloud computing but there are security issues when implementing cloud.

In this paper, we analyze security problems of clouding service and present the appropriate guidelines. This will be utilized in the fields of cloud computing and service delivery.

키워드

가상화, 가이드라인, 보안, 클라우드

Ⅰ. 서 론

클라우드 서비스는 IT 자원을 인터넷 기반으로 서비스하는 것을 의미하며, 사용자는 별도의 지식이나 관리자의 개입 없이 IT 자원을 공간과 시간의 제약 없이 사용할 수 있게 한다. 최근 스마트폰이나 태블릿 PC 등 한 사용자가 여러대의 기기를 사용하는 것을 흔하게 볼 수 있다.

사용자는 여러 기기의 정보를 서로 공유하기 위해서 클라우드 서비스를 활용한다. 또한, 휴대성이 편리한 기기의 하드웨어 성능보다 더 높은 사양을 요구하는 작업을 클라우드 IT 자원을 통하여 처리할 수 있다. 이것은 기존에 이루어지기 힘들었던 여러 일들이 일상화되어 생활 및 업무에 많은 변화를 주게 되었다. 이러한 장점을 가진 클라우드 서비스는 사용자와 기업들이 가장 저해되는 요인으로 보는 것이 보안 취약성이다. 특히, 주요 데이터 유실 및 유출이 주된 요인이다. 또

한, 클라우드는 복잡한 가상화 방식을 사용하여 또 다른 보안 취약성을 갖는다.

이에 따라 오픈 소스 단체나 정부에서 보안 표준화를 연구하고 있으며, 각 상용 업체에서는 통합 보안을 통하여 고객들에게 신뢰를 얻고자 한다.

본 논문에서는 클라우드가 갖고 있는 보안 취약성과 보안 기술과 인증제도를 분석하여, 향후 보안 전략에 관해 연구한다.

Ⅱ. 클라우드 컴퓨팅 보안

2.1 클라우드 컴퓨팅 보안 요소 기술

케빈스 테크놀러지 컨설팅의 설립자이자 CTO인 마이크 캐비스는 “보안 요구 조건은 실제로 똑같지만, SaaS에서 PaaS나 IaaS로 옮겨가면, 확보하고 있는 보안 제어 수준이 달라진다”며, “논리적인 관점에서 보면, 아무것도 없지만, 물리적으로 어떻게 하는지가 극적으로 바뀐다”라고 강조했다[1].

보안 요소 기술은 기밀성과 데이터 암호화, 사용자 인증 및 접근 제어, 데이터 무결성, 가용성 및 복구, 가상화 보호, 네트워크 및 웹 보안, 공격 모델 및 시뮬레이션으로 구성되어 있다.

2.2 인증 제도

클라우드 보안 인증 제도는 클라우드 시장을 활성화 하기 위해서 클라우드 서비스 제공업체가 서비스의 수준을 보장하기 위해 필요한 서비스 체계를 구축하였는지 점검하고, 일정 수준 이상의 클라우드 서비스에 인증을 부여하는 제도를 도입하여 클라우드 서비스 산업 전반에 대한 불안감을 해소하고, 서비스의 품질을 향상시켜 클라우드 서비스를 더 활성하고자 하는 제도이다.

2012년 1월 방송통신위원회에서 클라우드 서비스 인증제를 발표하였으며, 서비스 사업자로는 KT사가 최초로 클라우드 서비스 인증을 획득하였다. 국내 클라우드 관련 인증 제도로는 ASP 인증제도, GS 인증제도, 녹색 인증제도가 있으며, 클라우드 서비스 협회(KCSA)에서 클라우드 서비스의 품질, 보호, 기반 제공 분야를 심사하여 우수 클라우드 서비스를 인증한다. 다음 표 1은 KCSA에서 심사하는 영역이다.

표 1. KCSA - 7개의 심사영역

측정 목적	측정 항목
서비스 품질	- 가용성(Availability) - 성능(Performance) - 확장성(Scalability)
서비스 정보 보호	- 데이터 관리 (Data Management) - 보안(Security)
서비스 기반	- 서비스 지속성 (Continuity) - 서비스 지원(Support)

2.3 클라우드 컴퓨팅 보안 전략

2.3.1 신뢰할 수 있는 클라우드 구축 전략

기업과 사용자에게 신뢰를 얻으려면 클라우드 서비스는 안정적이고 투명하게 운영할 수 있는 환경을 갖추어야 한다. 또한, 개인 정보 법적 문제에 어긋나지 않으려면 신뢰성 요구사항인 규정 준수, 거버넌스, 위험 요소 관리, 가용성, 무결성, 기밀 유지 및 개인 정보 보호를 충족해야 한다[2].

2.3.2 효과적인 보안 관리 방안

효과적인 클라우드 보안 관리를 하려면 컴플라이언스(Compliance)는 비즈니스 활동에 있어서 최우선으로 고려해야 한다. 효과적인 컴플라이언스를 하기 위해서는 지속적이고 일관성을 고려한 정보보호 전략을 수립해야 하고, 최고의 경영층의 정보보호활동에 의지 반영 및 참여를 유도하며, 전사적 자원을 체계적으로 종합하여 정보보호 관리 이행 및 실천한다.

효과적인 컴플라이언스를 하기 위해서는 자사 정보보호 전략 및 프레임워크를 수립하고, 능등적 위험관리 기반의 정보보호 시스템을 구축하며, 효율적인 프로세스의 재정립 및 시스템화한다. 또한, 모니터링 강화 및 임직원에게 교육을 통해 인식을 제고한다[3].

Ⅲ. 클라우드 도입 가이드 라인

3.1 클라우드 도입시 고려사항

클라우드 서비스를 도입하기 전에 활용 방안 및 ROI(Retrun on Investment)를 고려하여 기업의 현황 분석을 통하여 클라우드 서비스의 필요성 여부를 검토할 필요가 있다. 클라우드 컴퓨팅은 도입이 일차적인 목적이 아니며, 경제성을 바탕으로 분석하여 도입시 무리하게 진행하지 않도록 한다.

또한, 클라우드의 구축여부 및 클라우드 제공업체를 통해 서비스를 제공 받는 여부는 기업 현황에 맞게 분석하여 선택해야 한다. 클라우드를 직접 구축할 경우 보안 측면에서는 향상되지만 초기 투자 비용이 필요하며, 지속적인 유지보수가 필요하며, 전문적인 인력이 필요하다.

전문적인 인력은 직접 양성 및 채용으로 분류되며, 양성은 IT에 관련된 직원을 교육해야 하고, 채용시에는 인성검사와 체계적인 면접 프로그램을 통하여 신뢰적인 인재를 채용해야 한다. 제공업체를 통해 도입하면 초기 투자 비용 및 유지보수가 절감되지만 보안 측면에서는 효율성이 낮아 회사 기밀 업무에는 자제해야 한다.

3.2 운영 방안

사설 클라우드는 기업 내부에서만 인트라넷을

통해 서비스하는 형태로 공용 클라우드를 사용할 때에 비해 보안, 정보 통제, 기밀 업무 유출 등을 우려하는 기업의 요구 조건을 충족 시켜 준다. 사설 클라우드는 공용 클라우드에 비해 보안 측면은 우수하지만, 보안 사고를 대비하여 업무의 내용을 보안 등급으로 차등하여 기밀 업무일 경우, 2단계 보안 인증과 OTP(One-Time Password)를 통해 보안을 이중화 한다.

공용 클라우드는 프로토 타입형 개발과 테스트, 트레이닝 서버, 고객용 웹 사이트 등에 적용하면 좋다. 또한, 공용 클라우드는 한 업체만 이용하지 말고 여러 업체를 이용하여 위험을 분산해야 하며, 모니터링을 구축하여 실시간으로 확인해야 한다.

3.3 보안 교육 및 문서 관리

클라우드 보안은 시스템에만 해당되는 것이 아니며, 관리자와 사용자의 취약점을 이용하여 사회공학적 해킹을 시도한다. 이러한 것을 예방하기 위해서는 주기적인 보안 교육을 실시하여 보안 의식 수준을 높이고, 위기 대처 방안 교육을 통하여 대처 능력을 향상할 수 있도록 한다.

기밀 문서의 경우 사설 클라우드 내에서만 이용할 수 있게 하며, 각 문서에 보안 등급을 부여하여 해당 권한을 가진 사람들에 한하여 문서를 열람 할 수 있도록 한다. 파트너사와 협업 등을 위해 부득이한 외부 공유의 필요시, 외부 공유에 대한 보안 규칙에 맞는 관리가 필요하다.

Ⅳ. 결 론

클라우드 컴퓨팅은 기존의 IT 환경에서 할 수 없었던 일을 실현시켜주는 차세대 기술이다. 올해 가트너(Gartner)에서는 2013년 10대 전략 기술에 퍼스널 클라우드, 하이브리드IT & 클라우드 컴퓨팅이 포함되어 있으며, 또 다른 전략 기술인 전략적 빅데이터, 모바일 앱 등을 지원하기 때문에 각 분야에 활용될 수 있는 효과적인 기술이다.

이러한 장점에 주목받아 기업 및 정부에서는 클라우드에 대한 연구가 활발히 진행되고 있다. 하지만 보안에 관한 취약점이 존재하여 시스템 도입시 고려해야하는 사항이다.

본 논문에서는 클라우드 컴퓨팅의 문제점인 보안 위협 요소와 보안기술, 인증제도를 살펴보고, 보안 전략을 분석하였다. 또한 클라우드 도입 가이드라인을 제시하였다.

향후 연구과제로는 클라우드 서비스의 표준화 동향 및 발전 방향에 대해 좀 더 세밀하게 분석하여 오픈 소스를 활용한 클라우드 보안 기술 시스템의 설계 및 구현에 관한 연구가 필요하다.

감사의 글

본 논문은 중소기업청에서 시행한 산학연 공동기술개발사업의 결과입니다.

참고 문헌

[1] 최재규, 노봉남, “클라우드 컴퓨팅 환경에서의 보안 평가 요소,” 보안공학연구논문지, Vol8, No3, pp.371-384, 2011.6

[2] 신경아, 이상진, “클라우드 컴퓨팅 서비스에 관한 정보호호관리체계,” 정보보호학회논문지, Vol22, No1, pp.155-167, 2012.2

[3] 김진섭, “위험관리 기반 침해사고 조기 대응체계 구축 사례,” 정보보호학회지, Vol20, No6, pp.73-87, 2010.12