JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 21, No. 2, pp. 395-403, Feb. 2020

Check for updates

클라우드 환경에서 기술유출 최소화를 위한 보안관리체계 설계연구

박 원 효[1] · 장 항 배[2*]
[1]중앙대학교 융합보안학과 석사과정
[2]중앙대학교 산업보안학과 교수

Security Management System for Minimizing Technology Leakage in Cloud Environment

Won-hyo Park[1] · Hangbae Chang[2*]
[1]Master's Course, Department of Security Convergence, Chung-Ang University, Seoul, Korea
[2]Professor, Department of Industrial Security, Chung-Ang University, Seoul, Korea

[요 약]

클라우드컴퓨팅 기술의 여러 장점으로 인하여 전 세계의 다양한 산업군에서 클라우드 서비스 도입이 빠르게 확산되고 있다. 그러나 자원공유, 가상화 등의 특성으로 인한 정보 유출, 서비스 장애 등 여러 보안 위협들이 내재되어 있어, 국내의 경우 클라우드 서비스 도입에 따른 보안 우려로 많은 기업들의 클라우드 서비스 도입이 다소 미진한 실정이다. 이에 본 연구에서는 기업이 클라우드 환경으로의 전환 시 안전한 클라우드 서비스 환경의 구축하면서, 보안 관점에서 기술유출 최소화를 위한 관리체계를 제시하였다.

[Abstract]

The advantages of cloud computing technology have led to rapid adoption of cloud services in various industrial groups around the world. However, many companies are slow to adopt cloud services due to security concerns stemming from the introduction of cloud services, as there are many security threats inherent in the nature of resource sharing, virtualization, and so on. Therefore, this study seeks to present a security management system to minimize technology leakage from the perspective of security and the establishment of a secure cloud service environment for enterprises as they move to the cloud.

색인어 : 클라우드서비스, 산업보안, 기술유출, 보안관리체계, 보안관리항목

Key word : Cloud Service, Industrial Security, Technology Leakage, Security Management System, Security Management Control

http://dx.doi.org/10.9728/dcs.2020.21.2.395

Received 07 January 2020; **Revised** 20 January 2020
Accepted 25 February 2020

***Corresponding Author; Hangbae Chang**

Tel: ※ 개인정보 표시제한
E-mail: hbchang@cau.ac.kr

Ⅰ. 서 론

초 연결(Hyper-Connectivity)로 인하여 연결된 모든 물체가 실시간으로 데이터를 상호 공유하고 수집됨으로써 데이터 규모가 확대되어 그 종류는 예측하기 어려울 정도로 다양해졌다. 이러한 데이터수집 규모의 확대와 종류의 다양화는 사물인터넷, 빅데이터, 인공지능 등 초 지능(Super Intelligence) 정보통신기술을 발전시켜 제4차 산업혁명 시대의 도래를 가속화하고 있다.

빅데이터는 과거 데이터에 비하면 그 규모가 방대하고 새로운 종류가 끊임없이 나타나며 그 생명주기 또한 짧다. 수치 데이터뿐만 아니라 문자와 위치 데이터, 영상 데이터 등을 포함하는 다양한 형태의 데이터는 각 산업의 가치와 비즈니스 확장성에 있어서 중요한 역할을 한다[1]. 그러나 기존의 온-프레미스(On-Premise) 환경에서는 데이터 보관 및 관리에 어려움이 있어, 전 세계적 흐름은 데이터와 관련된 정보통신자원을 “소유”하는 것에서 벗어나 자원이 필요할 때마다 빌려 쓰는 “활용”의 형태로 변하고 있다[2].

안전성이 보장된 컴퓨팅 환경에서의 데이터 활용을 위해 세계 각국의 정부와 기업들은 초 연결 환경구축을 위한 오프-프레미스(Off-Premise) 형태의 “클라우드컴퓨팅”기술을 주목하고 있으며, 정보통신자원의 유연한 사용을 가능하게 하는 “클라우드컴퓨팅(Cloud Computing)”기술은 첨단 정보통신기술과 융합하여 데이터 수집과 분석, 데이터 가용성 확보, 데이터 공유와 활용 극대화 등을 위한 투입비용 대비 효율적인 서비스 제공을 가능하게 하였다.

이러한 클라우드컴퓨팅의 다양한 특징과 장점들로 인하여 전 세계의 다양한 산업군에서 클라우드 서비스 도입이 빠르게 확산되고 있다. 국내의 경우에도 세계 최초로 클라우드 법을 제정하고, 인증제도 시행, 가이드라인 개발 등 국내 클라우드 산업 육성과 경쟁력 강화를 위해 다방면으로 노력을 하고 있다[3]. 그러나 이러한 노력에도 불구하고 국내 클라우드 서비스 도입 사례는 매우 저조한 실정이다.

클라우드 서비스 도입 확산에 따른 사이버 공간의 활용성 증대와 취약성 또한 증대되고 있어, 사이버 상의 기술유출 역시 증가할 전망이다[4]-[5]. 또한, 정보통신산업진흥원의 클라우드 산업 실태조사 요약보고서 자료에 따르면 국내 클라우드 산업 활성화 저해요인으로 보안 문제가 가장 높게 나타났으며, 아직 국내에는 클라우드 도입에 따른 안정성 및 신뢰성에 대한 보안 우려가 큰 상황이다[6]. 이처럼 국내 클라우드 산업의 활성화와 보안 문제에 따른 신뢰성 해결이 시급한 실정이다.

Ⅱ. 본 론

2-1 클라우드컴퓨팅과 서비스

1) 클라우드컴퓨팅 개념

「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조(정의)에 의하면 클라우드컴퓨팅(Cloud Computing)이란 “집적·공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계”를 말한다.

기존 공급자 중심의 호스팅·아웃소싱 방식과 다르게 클라우드컴퓨팅 환경은 사용자 중심이자 자동화 제공방식을 채택하였다는 점에서 차별성을 갖는다[7]. 기존 레거시시스템(Legacy System)인 온-프레미스(On-Premise) 방식은 조직의 IT거버넌스를 위해 자체 데이터센터를 보유하여 시스템 구축부터 운영까지를 모두 수행하는 방식이며, 시스템을 구축하는데 수개월 이상의 시간과 비용부담이 큰 단점이 있다[8].

반면, 클라우드컴퓨팅 환경은 운영 및 비용 효율화의 장점을 가지고 있으며, 필요시 다양한 종류의 서비스를 즉시 제공하고 플랫폼의 선택적용이 가능하다는 점에서 민첩성이 뛰어나다[9]. 또한, 클라우드 서비스 제공사(CSP)에 의해 모니터링과 관제 서비스 등을 제공하고 분야별 전문인력을 지원하여 사고발생 시 빠른 업무지원과 대응을 통해 개발·운영에 대한 인력비용을 절감할 수 있다[10].

2) 클라우드컴퓨팅 환경에서의 서비스

클라우드컴퓨팅 환경의 영역별 구성방법은 크게 3가지로 분류되며 퍼블릭(Public), 프라이빗(Private), 하이브리드(Hybrid) 클라우드 서비스로 나뉜다. 퍼블릭 클라우드는 이용대상을 제한하지 않으며, 인터넷에 접속 가능한 모든 불특정 다수의 사용자를 위해 개방적인 형태로 제공되는 클라우드 서비스이다[11]. 적은 비용으로도 다양한 서비스 이용이 가능하다는 특징이 있다. 프라이빗 클라우드는 특정 기업이나 특정 이용자를 대상으로 그 이용자에게만 폐쇄적으로 제공되는 서비스로 초기 투자비용이 많이 소요되고 확장성이 떨어지는 단점이 있지만, 보안을 우선시하는 경우 많이 이용된다[12]. 하이브리드 클라우드는 퍼블릭 클라우드와 프라이빗 방식이 결합된 서비스이다[13].

단일 환경은 동일한 클라우드 서비스 제공사(CSP)에서 퍼블릭과 프라이빗 중 1개의 제공형태를 선택하여 이용하는 유형이다. 하나의 클라우드 서비스 제공사(CSP)를 사용할 경우 단일 인터페이스만 사용하므로 보안 시스템이나 데이터베이스 등 이기종 환경의 복잡성 우려가 적어지고, 클라우드 서비스들이 함께 동작하는 것도 매끄럽다. 그러나 단일 환경의 클라우드컴퓨팅 구성은 클라우드 서비스 제공사(CSP)의 갑작스러운 가격 인상이나 일방적인 유지보수지원 종료통보 등과 같은 부당한 상황과 서비스 장애 및 보안사고 문제 등의 업체 종속성이 높아질 수 있는 위험이 존재한다[14]. 또한, 서비스 장애 발생 시 복구될 때까지 서비스가 중단되어 최악의 경우 비즈니스에 직접적인 영향을 미치게 된다. 이러한 단일 클라우드의 문제점들로 대부분의 기업들이 가용성과 안정성을 높여주는 멀티 클라우

드 방법을 활용하고 있다.

멀티 클라우드란 퍼블릭 클라우드 서비스 또는 프라이빗 클라우드 서비스를 다중으로 구성하는 형태이며, 이때 각각의 클라우드컴퓨팅 환경은 동일 클라우드 서비스 제공사(CSP)이거나 다른 업체일 수 있다. 이러한 클라우드 서비스 구성방법은 동일 기종의 상이한 서비스를 제공하는 하이브리드 클라우드 서비스와는 차별점이 존재하며, 멀티 클라우드는 특정 클라우드 서비스 제공사(CSP)에 얽매이지 않고, 유연한 비즈니스 계획을 짤 수 있다[15]. 단순히 리스크를 보완하는 것뿐만 아니라 데이터 관리·분석의 효율성 극대화와 금전적·시간적 비용 최적화에도 장점이 있다[16].

3) 클라우드 서비스 유형 및 특성

클라우드 서비스는 정보통신 자원의 서비스 종류에 따라 IT 인프라(서버, 스토리지 등) 서비스를 제공하는 IaaS(Infrastructure-as-a-Service)와 SW개발환경(플랫폼) 서비스를 제공하는 PaaS(Platform-as-a-Service), 응용SW 서비스를 제공하는 SaaS(Software-as-a-Service)로 나눌 수 있다[17].

IaaS는 이용자에게 서버, 스토리지 등 하드웨어 자원을 임대 및 제공하는 방식이다. 이용자는 CPU, 하드디스크, 메모리 등 필요 정보통신 자원의 사양과 성능을 주문하고 클라우드 서비스 제공사(CSP)는 요구사항에 맞게 가상화된 하드웨어를 구성 및 제공한다[18]. PaaS는 운영체제, 데이터베이스, 웹서버 등 이용자에게 필요한 서비스를 개발할 때 필요한 플랫폼을 제공하는 방식이다. 클라우드 서비스 제공사(CSP)는 운영체제, 데이터베이스 등을 제공하고, 이용자는 이를 이용하여 응용프로그램을 개발할 수 있다. SaaS는 오피스, ERP 등의 소프트웨어를 임대 및 제공하는 방식이다. SaaS 클라우드 모델에서는 서비스 제공자가 모든 인프라와 소프트웨어 제품을 제공하며, 사용자는 클라우드에서 제공하는 제품을 자신의 컴퓨터에서 사용할 수 있다[19].

클라우드 서비스가 가지는 특성은 경제성, 유연성, 효율성, 이용편의성, 신속성 등 다양한 장점을 지니고 있으며, 기업에서는 주로 경제성, 유연성, 효율성의 측면에서 클라우드 서비스를 이용한다[2]. 이 중 가장 두드러지는 특성은 사용량에 비례한 과금 체계의 특성인 “경제성”과 접속자 수 증가 및 트래픽 폭주 등의 갑작스러운 이용량 증가에 대응하는 “유연성”이다. 데이터나 네트워크 트래픽을 여러 서버에 나누어 분산처리 하는 “효율성” 또한 클라우드의 큰 특성이자 장점이다. 인터넷에 접속된 이용자 단말에 상관없이 언제 어디서나 클라우드 서비스에 접속할 수 있는 “이용편의성”은 업무효율을 높이는 특성을 갖는다. 자체적인 시스템 구축시간을 단축할 수 있어 결과적으로 신속한 사업개시가 가능하다[17].

클라우드 서비스는 앞서 열거된 특성들 이외에도 다양한 특성들을 기반으로 방대한 양의 데이터 관리와 분석을 진행하면서 부가적으로 사물인터넷, 인공지능 등과 같은 신기술 적용에 따른 서비스 장애 등의 위험을 최소화 하도록 설계되어 있다[20].

2-2 클라우드컴퓨팅 도입 사례분석

1) 해외 클라우드 서비스 현황 및 사례

해외 선도국들은 클라우드 서비스 시장을 선점하기 위해 클라우드컴퓨팅 산업을 적극적으로 육성하고 있다. 공공부문에 클라우드를 선제적으로 도입하여 안정성을 검증한 후 검증된 클라우드 서비스를 민간으로 확산시키는 정책을 펼치고 있다. 또한, 정부 차원에서 직접적인 기술개발 투자와 클라우드 컴퓨팅 기업을 적극 지원 중이다[19]

2017년 미국 트럼프 대통령의 클라우드 온리(Cloud Only) 행정 명령으로 모든 정보화 시스템의 보안과 효율의 개선을 위해 공공기관 민간 클라우드 전환을 의무화하도록 했다[2]. 또한, 미국 정부는 공공에서 민간 클라우드 도입 시에 보안 문제 해결을 위해 FedRAMP를 구축했다. 영국의 경우 데이터 보안 분류 체계를 6단계에서 3단계(일급기밀, 중요기밀, 공공데이터)로 간소화했고, 공공부문 클라우드 서비스 도입을 위해 G-Cloud 전략을 수립하여 클라우드 유통체계를 마련했다[21]. 일본은 가스미가세키 프로젝트를 통해 13개 중앙부처의 서버를 통합하여 지방자치단체의 클라우드 도입을 추진했다[22]. 중국 국가발전개혁위원회는 국무원의 신흥 산업 육성 전략의 일환으로 ‘클라우드컴퓨팅 혁신발전을 위한 시범사업’을 추진하였고, 중앙정부의 시범사업 외에도 각 지방정부가 자체적으로 클라우드 지원 사업을 추진하였다[22].

2) 국내 클라우드 서비스 현황 및 사례

2015년 정부는 세계 최초로 클라우드 법 제정과 1차 범정부 기본계획 수립 등 국내의 클라우드 산업 육성을 위해 많은 노력을 기울여 왔다. 또한, 공공기관의 민간 클라우드 이용을 지원하기 위해 정보보호 기준 고시 및 인증제도 시행, 가이드라인 등을 마련함으로써 정부 차원에서 국내 클라우드 서비스 활성화를 위해 다양한 노력을 하였다[23].

그러나 이러한 정부의 노력에도 불구하고 국내의 클라우드컴퓨팅 사용률은 여전히 낮은 실정이다. OECD의 조사 자료에 따르면 한국 기업들의 클라우드 사용률은 OECD 국가 중 최하위 수준이며, 그리스, 폴란드, 터키, 멕시코와 함께 가장 사용률이 낮은 국가에 포함된다[24]. 또한, 정보통신기획평가원의 ‘2018 ICT 기술수준조사 보고서’ 자료에 따르면 한국의 클라우드컴퓨팅 기술 수준은 84%로 경쟁국들과 비교 했을 때 가장 낮은 것으로 평가되었다. 최고기술국(미국) 대비 국가별 기술 수준 격차는 유럽 10.7%, 중국 15%, 일본 15.8% 순이며, 한국은 16%의 가장 큰 기술수준 격차를 보이고 있다[25].

아직 국내 클라우드 산업은 해외 주요국에 비해 매력적인 사례들이 부족하다. 그러나 정부는 국내 클라우드 산업의 활성화와 산업 경쟁력 강화를 위해 공공부문의 선제적인 도입과 혁신 사례 창출을 통한 민간으로의 확대를 위해 다차원적인 노력을 하고 있다.

2-3 클라우드 서비스 보안위험 분석

1) 클라우드 서비스 보안위협

클라우드 서비스는 구성 요소와 방법이 다양하고 자원의 공유, 가상화, 정보 외부위탁 등의 특성으로 인하여 정보 유출, 서비스 장애 등 여러 보안위협이 발생할 수 있다. 한국인터넷진흥원의 자료에 따르면 클라우드 서비스 핵심 보안위협을 다음과 같이 정리하였다. ① 가상화 취약점(악성코드 및 서비스 가용성 침해) ② 정보위탁(소유와 관리 분리)에 따른 정보 유출 위협, ③ 자원 공유 및 집중화에 따른 서비스 장애, ④ 단말 다양성에 따른 정보 유출, ⑤ 분산 처리에 따른 보안 적용의 어려움, ⑥ 법규 및 규제의 문제 총 6가지로 분류하고 있다[26]-[27].

소프트웨어정책연구소(2017)는 클라우드 서비스 핵심 보안위협 요소 6가지를 기술적 문제와 기술외적 문제로 분류했다. 기술적 문제로는 가상화 취약점, 정보위탁에 따른 정보 유출 위협, 자원 공유 및 집중화에 따른 서비스 장애로 구분했고, 기술외적인 문제로는 단말 다양성에 따른 정보 유출, 분산 처리에 따른 보안 적용의 어려움, 법규 및 규제의 문제로 구분했다.

CSA(2019)의 가장 최근 발표 자료에 따르면 클라우드 보안위협요소는 시스템 취약성, 분산 서비스 공격 등 기술적 문제보다 내부자의 도덕적 해이, 불충분한 관리와 부주의 등 기술외적인(사람) 문제와 관련된 것들이 매우 중요한 요소임을 지적했다. 이는 곧 기술적 위협대응책이 있어도 결국 내부 인력에 의한 의도된 위협은 막기 어렵고, 내부자들에 대한 보안 인식 교육이 클라우드 서비스 보안을 위해 매우 중요한 요소임을 말한다[28]-[29].

2) 클라우드 서비스 보안체계

클라우드 환경은 기존의 온-프레미스(On-Premise) 환경과 동일한 보안 업무를 수행하는 부분도 존재하나, 기업이 클라우드 서비스 도입에 따른 변화에 효율적이고 안정적으로 대응하기 위해서는 자산 식별 및 통제, 서비스 연속성 관리, 가상화 보안 등 클라우드 서비스 환경 특성에 따른 새로운 보안관리체계를 갖춰야 할 필요가 있다[30]. 한국인터넷진흥원의 클라우드 정보보호 안내서(2017)에서 클라우드 인프라를 안정하게 운영함에 있어 필요한 보안 사항들을 요약한 내용은 다음과 같다.

표 1. 클라우드 운영 보안
Table 1. Cloud Operation Security

Type	Description
Cloud Information Protection Policy Establishment	procedures for technical and administrative protection of information systems and assets
Security Organization and Personnel Security	organizations and personnel whose responsibilities, authorities and relationships are defined in order to carry out information protection activities
Identifying Assets and Controlling	identify physical assets (information systems, etc.) and information assets, management responsibility and control measures
Infringement Accident Management	report and handling process in case of infringement incident
Service Continuity Management	process in case of service use problems such as service failure
Standard Management	legal obligations such as in-house security regulations, privacy laws, and information and communication network laws
Virtualization and Server Security	anti-malware measures, managing virtual resources (modify, move, delete, copy) and applying technical security measures to cloud servers
Access Control Security	establish access control policies, manage and restrict access to users and administrators, divide user and administrator accounts, and minimize authority
Network Security	manage network partitioning or redundancy, establish network security systems, secure network availability
Data Protection and Backup	usage of safe encrypted algorithm and management on encryption keys for classifying critical data, establishing data ownership and data protection
System Development and Implementation Security	establishing merging policies including design and implementation which reflects security requirements in system development, safety testing when system is introduced, etc.

Ⅲ. 제 3 장 연구방법론과 보안관리항목 설계

3-1 연구방법론 설계

본 연구는 첫째, 클라우드컴퓨팅 서비스에 대한 이론적 고찰을 한다. 둘째, 이찬우(2017)의 '산업기술보호 수준진단 참조모델'을 차용하고, 선행연구 및 문헌조사를 통해 클라우드 환경 특성과 보안 고려사항을 도출하여 클라우드 환경에서 기술유출 최소화를 위한 보안관리항목을 설계한다[31]. 셋째, 선행연구 및 문헌조사를 통해 설계된 보안관리항목들에 대한 검증을 진행한다. 넷째, 검증을 통해 최종 설계된 보안관리체계의 상대적 우선순위 도출한다. 마지막으로 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계의 설계를 한다.

3-2 클라우드 서비스 보안관리항목 설계

다음 표 2는 클라우드 환경에서 기술유출 최소화를 위한 보안관리항목 설계의 선행연구 및 문헌조사 목록이다.

표 2. 선행연구 및 문헌조사 목록
Table 2. List of Precedent Research and Literature Surveys

List
Information Security Management System on Cloud Computing Service (2012)
The Important Factors in Security for Introducing the Cloud Services (2012)
Key Issues and Countermeasures in Cloud Security (2017)
Conceptual SLA Framework for Cloud Computing (2010)

Proposal for establishing cloud adoption criteria in the public sector (2015)
Cloud Computing Understanding and Financial Use Cases (2017)
Economic Evaluation of Cloud Computing Investment Alternatives (2011)
A Study on the Significant Factors Affecting the Adoption of Enterprise Cloud Computing (2012)
A Study of Factors Affecting the Adoption of Cloud Computing (2012)
Flexible Crypto System for IoT and Cloud Service (2016)
Private Cloud Implementation Practices (2012)
Outsourced Cloud Computing (2012)
A Guide to the Use of Cloud Computing Services in the Financial Field (2019)
Financial Cloud Services Status and Implications (2019)
2018 Kubecon Cleanup and Cloud Implication on Native (2019)

Ⅳ. 제 4 장 연구결과

4-1 클라우드 환경에서 기술유출 최소화를 위한 보안관리 항목 검증

1) 검증 절차

본 연구를 통해 도출된 클라우드 환경에서 기술유출 최소화를 위한 보안관리항목 검증을 위해 설문조사를 실시하였다. 클라우드와 산업보안에 대한 관련 지식이 있는 교수, IT보안 전문가 및 관련 전문가 50명을 대상으로 진행하여 총 44명의 데이터를 최종 확보하였다. 설문조사는 2019년 11월 4일부터 11월 24일까지 진행하였고, 연구를 통해 설계된 보안관리항목들에 대한 검증을 5점 리커트 척도로 응답하게 하였다. 조사 방법은 이메일을 통한 자기기입식 조사와 현장에서 직접 설문을 제공하는 오프라인 방식을 병행하였다.

2) 검증 결과

본 연구를 통해 도출된 보안관리항목들의 검증 결과 19, 20, 26, 27번 항목의 경우 3.5 이하로 부적절한 결과값이 나왔으며, 이외의 항목들에 대한 평균값은 모두 3.5 이상으로 보안관리항목에 적합함이 검증되었다.

표 3. 보안관리항목 검증 결과
Table 3. Security Management Category Verification Result

No	Category	Average	Standard Deviation
1	regulations for the legal requirements of the industry to which the company belongs(Compliance)	4.27	0.69
2	executive participation in security education	4.09	0.80
3	executive support on security organization	4.14	0.73
4	improving security awareness for enterprise-wide technology protection and eliminating vague security concerns due to the introduction of cloud technology (IT Rent Service)	4.07	0.76
5	the level of cooperation of employees regarding the security activities designed by security manager	4.02	0.85
6	the degree of discomfort to employees regarding altered task procedure due to consideration of security(security receptivity)	3.77	0.77
7	establish standards for Service Level Agreements(SLA) from a security perspective by quantifying a service levels with Cloud Service Providers (CSP)	4.05	0.86
8	assignment of security personnel (or establishment of security departments)	3.93	0.85
9	the degree of security management for employees(security pledge and security education for new employees, retained employees, retiree employees, etc.)	4.14	0.88
10	size of investment in technology protection(security personnel + security education + security consulting + security system introduction and operation, etc.)	4.30	0.79
11	decisions on cloudification	4.34	0.81
12	settings on relocation for cloudification(Public, Private, Hybrid, Multi, etc.)	4.32	0.74
13	improve research environment for researchers (making researchers permanent, compensation system for job invention, etc.)	3.82	0.81
14	identification and importance evaluation of developed research results	4.05	0.81
15	establish and evaluate on cloud relocation targets due to technology information rating identification and importance assessment	3.95	0.78
16	security management for research assets(research security pledge, research content security management, etc.)	3.95	0.79
17	joint (commissioned) research security management (co-ordinating/ consignment security contracts, security activities inspection, etc.)	3.95	0.81
18	performance Management of Research Results (Technical Rights, Technology Implementation) Security activities for technology transfer, etc.)	3.89	0.78
19	setting up and managing security zones (equipment)	3.39	0.62
20	introduction and utilization of security systems (ingress control + intrusion alert + image detection, etc.)	3.45	0.63
21	identification on objectified domestic and international security certifications for selection of cloud service providers (CC certification, ISO27001, CSA STARs, etc.)	3.93	0.79
22	personal computer security level (user authentication, updated version), SecuritySW introduction and operation, etc.)	3.91	0.80
23	server security level (user authentication, (shared folder)access Management, up-to-date versions, security, introduction and operation of SW, Etc.)	3.68	0.80
24	database security level (user authentication, up-to-date version), security SW introduction and operation, Etc.)	3.80	0.79

25	computer network security level (user authentication, up-to-date version, security SW introduction and operation, etc.)	3.84	0.81
26	establishment and implementation of supply chain security	3.48	0.63
27	the degree of production process security guidelines and implementation (prevent disruptions and information)	3.45	0.63
28	the degree of internal security audit activities (conduct security policy management standards)	3.86	0.77
29	the degree of efforts to improve the security system through the analysis on external best security practices	3.66	0.81
30	obtain an security certification objectified by a third party(ISO27001 certification, K-ISMS certification, etc.)	3.61	0.75
31	system failure response activities (business continuity planning, system redundancy and backup, shared responsibilities, etc.)	3.82	0.90
32	countermeasures for technology leakage incidents (plan forincident response, measures to prevent recurrence of accidents, cause analysis on incident, etc.)	3.68	0.86

4-2 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계

이찬우(2017)의 '산업기술보호 수준진단 참조모델'을 차용하여 선행연구 및 문헌조사를 통해 설계한 보안관리체계 항목들의 검증 결과 최종 도출된 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계는 다음과 같다.

표 4. 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계
Table 4. Security Management System for Minimizing Technology Leakage in Cloud Environment

Technology Protection Level Diagnosis Area		Technology Protection Level Diagnosis Item
1	External Environment for Technology Protection	
1-1	Legislation for Technology Protection	regulations for the legal requirements of the industry to which the company belongs(compliance)
2	Cultural Environment for Technology Protection	
2-1	Will to Promote Technology Protection(Executives)	executive participation in security education
		executive support on security organization
2-2	Security Trust(Mutual) for Technology Protection	improving security awareness for enterprise-wide technology protection and eliminating vague security concerns due to the introduction of cloud technology (it rent service)
		the level of cooperation of employees regarding the security activities designed by security manager
		the degree of discomfort to employees regarding altered task procedure due to consideration of security(security receptivity)
		establish standards for service level agreements(SLA) from a security perspective by quantifying a service levels with cloud service providers (CSP)
3	Support for Technology Protection	
3-1	Workforce Deployment for Technology Protection	assignment of security personnel(or establishment of security departments)
		the degree of security management for employees(security pledge and security education for new employees, retirees , etc.)
3-2	Investment on Technology Protection	size of investment in technology protection(security personnel + security education + security consulting + security system introduction and operation, etc.)
3-3	Analysis and Design on Economic Efficiency	decisions on cloudification
		settings on relocation for cloudification(public, private, hybrid, multi, etc.)
4	Operation Management for Technology Protection	
4-1	Identification/Classification of the Importance of Technology Development and Output	improve research environment for researchers(making researchers permanent, compensation system for job invention, etc.)
		identification and importance evaluation of developed research results
		establish and evaluate on cloud relocation targets due to technology information rating identification and importance assessment
		security management for research assets(research security pledge, research content security management, etc.)
		joint(commissioned) research security management (co-ordinating/ consignment security contracts, security activities inspection, etc.)
		performance management of research results(technical rights, technology implementation) security activities for technology transfer, Etc.)
4-2	Electronic Technology Protection System	identification on objectified domestic and international security certifications for selection of cloud Service providers(cc certification, iso27001, csa star, etc.)
		personal computer security level(user authentication, updated version) , security sw introduction and operation, etc.)
		server security level(user authentication, (shared folder)access management, up-to-date versions, security, introduction and operation of sw, etc.)
		database security level (user authentication, up-to-date version), security sw introduction and operation, etc.)
		computer network security level (user authentication, up-to-date version, security sw introduction and operation, etc.)
5	Change Management for Technology Protection	
5-1	Technology Protection Measurement and Improvement Activity	the degree of internal security audit activities (conduct security policy management standards)
		the degree of efforts to improve the security system through the analysis on external best security practices
		obtain an security certification objectified by a third party(iso27001 certification, k-isms certification, etc.)
5-2	Incident Response for Technology Protection (Restore)	system failure response activities (business continuity planning, system redundancy and backup, shared responsibilities, etc.)
		countermeasures for technology leakage incidents(plan for incident response, measures to prevent recurrence of accidents, cause analysis on incident, etc.)

4-3 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계 우선순위 도출

AHP 분석은 클라우드와 보안에 대한 경험과 전문지식을 보유하고 있는 총 14명의 전문가들을 대상으로 하였다. 조사도구는 자기기입식 설문지로써 1~9점의 쌍대비교 척도를 활용하여 설문을 진행하였다.

본 연구를 통해 설계된 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계 항목들의 중요 우선순위를 결정하기 위해 복합가중치를 계산하였다. 복합가중치는 상위계층, 중간계층, 하위계층의 가중치를 곱하여 계산하였다. 복합가중치 계산에 의한 보안관리체계 전체 항목들의 우선순위는 다음 표 5와 같다.

표 5. 복합가중치를 이용한 전체 항목의 우선순위
Table 5. Priority of All Category Using Composite Weight

Category	Rank	Composite Weight
regulations for the legal requirements of the industry to which the company belongs(Compliance)	1	0.259
decisions on cloudification	2	0.1293
settings on relocation for cloudification(Public, Private, Hybrid, Multi, etc.)	3	0.0925
size of investment in technology protection(security personnel + security education + security consulting + security system introduction and operation, etc.)	4	0.0865
identification on objectified domestic and international security certifications for selection of cloud service providers (CC certification, ISO27001, CSA STARs, etc.)	5	0.0837
improving security awareness for enterprise-wide technology protection and eliminating vague security concerns due to the introduction of cloud technology (IT Rent Service)	6	0.0408
executive's support on security organization	7	0.0343
identification and importance evaluation of developed research results	8	0.0315
the degree of internal security audit activities (conduct security policy management standards)	9	0.0299
establish and evaluate on cloud relocation targets due to technology information rating identification and importance assessment	10	0.0228
system failure response activities (business continuity planning, system redundancy and backup, shared responsibilities, etc.)	11	0.0194
assignment of security personnel (or establishment of security departments)	12	0.0174
identification on objectified domestic and international security certifications for selection of cloud service providers (CC certification, ISO27001, CSA STARs, etc.)	13	0.0166
security management for research assets(research security pledge, research content security management, etc.)	14	0.0149
the level of cooperation of employees regarding the security activities designed by security manager	15	0.0135
the degree of security management for employees(security pledge and security education for new employees, retained employees, retiree employees, etc.)	16	0.0134
the degree of efforts to improve the security system through the analysis on external best security practices	17	0.0129
personal computer security level (user authentication, updated version) , security sw introduction and operation, etc.)	18	0.0106
the degree of discomfort to employees regarding altered task procedure due to consideration of security(security receptivity)	19	0.0104
executive participation in security education	20	0.0103
joint (commissioned) research security management (co-ordinating/ consignment security contracts, security activities inspection, etc.)	21	0.0101
countermeasures for technology leakage incidents (plan for incident response, measures to prevent recurrence of accidents, cause analysis on incident, etc.)	22	0.0084
obtain an security certification objectified by a third party(iso27001 certification, k-isms certification, etc.)	23	0.0073
improve research environment for researchers(making researchers permanent, compensation system for job invention, etc.)	24	0.0064
database security level(user authentication, up-to-date version), security sw introduction and operation, etc.)	25	0.006
performance management of research results(technical rights, technology implementation) security activities for technology transfer, etc.)	26	0.0056
computer network security level (user authentication, up-to-date version, security sw introduction and operation, etc.)	27	0.004
server security level (user authentication, (shared folder)access Management, up-to-date versions, security, introduction and operation of sw, etc.)	28	0.0023

V. 결 론

클라우드컴퓨팅 기술은 4차 산업혁명의 주요 핵심 요소기술인 사물인터넷, 빅데이터, 인공지능 등의 플랫폼 역할을 수행하며, 4차 산업혁명을 이끌 핵심 기반기술로서 각 기술 분야에 연결성 및 데이터 수집, 분석 등을 지원하고 있다.

이러한 클라우드컴퓨팅 기술의 다양한 장점들로 인하여 전 세계의 다양한 산업군에서 클라우드컴퓨팅 서비스 도입이 빠르게 확산되고 있다. 그러나 클라우드컴퓨팅 서비스는 자원공유, 가상화 등의 특성으로 인하여 정보유출, 서비스 장애 등 여

러 보안 위협들이 내재되어 있다. 또한, 국내의 경우 클라우드 컴퓨팅 서비스 도입에 따른 안전성 및 신뢰성 등에 대한 보안 우려로 인하여 많은 기업들이 클라우드컴퓨팅 서비스 도입이 저조한 실정이다.

이에 본 연구는 기업이 기존 온-프레미스(On-Premise) 방식에서 클라우드컴퓨팅 서비스 환경으로의 구축 시 안전한 클라우드컴퓨팅 서비스 환경 구축을 위한 보안관리체계의 설계를 목적으로 실시되었다.

구체적으로는 이찬우(2017)의 '산업기술보호 수준진단 참조모델'을 차용하여 선행연구 및 문헌조사를 통해 클라우드 환경 특성과 보안 고려사항들을 도출하여 보안관리항목들을 설계하였다. 도출된 보안관리항목들에 대한 검증과 상대적 우선순위를 도출하였고, 최종적으로 클라우드 환경에서 기술유출 최소화를 위한 보안관리체계를 제시하였다.

본 연구는 기존 온-프레미스(On-Premise) 환경에서 클라우드컴퓨팅 서비스 환경으로의 구축 시 보안 관점에서 필요한 항목들에 대한 전체적인 설계는 하였으나 세부 항목들에 대한 추가적인 연구가 부족하였다. 그러나 실무적 관점에서 기업이 클라우드컴퓨팅 환경으로의 구축 시 기업이 스스로 안전한 클라우드 환경을 구축하고 서비스 품질 향상을 위해 역량을 집중하고자 할 때, 이를 판단하기 위한 기준으로 본 연구의 내용이 참고자료로써 활용될 수 있을 것으로 기대한다.

참고문헌

[1] M. J. Lee : Internet & Information Security:Big Data and the Utilization of Public Data, KISA, Seoul, ISSN 2093-9612, PP. 47~64, 2011

[2] S. W. Ahn : Policy and directions for revitalizing domestic cloud computing, Software Policy&Research Institute, Seongnam, 2018-009, pp. 1~87, 2019

[3] How to extend the use of the cloud in the financial sector, FSC, Seoul, pp. 1~22, 2018

[4] D. H. Bae, "Definition and Characteristics of Cyberspace-Focused on Some Examples -", *The Association of Korean Cultural and Historical Geographers*, Vol. 27, No. 1, pp. 129-243, April 2015.

[5] Wang, T., Zhou, J., Huang, M., Bhuiyan, M. Z. A., Liu, A., Xu, W., & Xie, M, "Fog-based storage technology to fight with cyber threat", *Future Generation Computer Systems,* Vol. 83, pp. 208-218, June 2018.

[6] 2018 Cloud Industry Survey Summary Report, NIPA, Seoul, pp. 1~52, 2018

[7] A Study on the Application Rental Service (ASP) Industry, KISDI, Jincheon, pp. 1~154, 2001

[8] Bibi, S., Katsaros, D., & Bozanis, P, "Business application acquisition: On-premise or SaaS-based solutions?", *IEEE software,* Vol. 29, No. 3, pp. 86-93, June 2012.

[9] D. H. Kim, J. H. Lee, & Y. P. Park, "A Study of Factors Affecting the Adoption of Cloud Computing", *Society for e-Business Studies*, Vol. 17, No. 1, pp. 111-136, February 2012.

[10] SW·Computing Cloud Computing, TTA, PP. 67~151, 2019

[11] Hofmann, P., & Woods, D, "Cloud computing: the limits of public clouds for business applications", *IEEE Internet Computing*, Vol. 14, No. 6, pp. 90-93, Nov.-Dec. 2010.

[12] 2014 KISTI Future Hope Technology 10: Cloud-Based Security, KISTI, pp. 1~76, 2014

[13] Cloud Computing Execution (ACT) Strategy for the Fourth Industrial Revolution, MSIT, pp. 1~37, 2018

[14] Cloud Computing Challenges, KFTC, pp. 33~54, 2011

[15] Cloud Strategy and Choice Criteria in the Multi-Cloud Era, IDG, pp. 1~18, 2017

[16] Multicloud Management Market, INNOPOLIS, pp. 1~9, 2017

[17] Cloud Information Protection Guide, KISA, pp. 1~66, 2017

[18] Key Infrastructure in the Spread of Artificial Intelligence,Cloud Industry Trends Analysis and Implications, NIPA, pp. 1~11, 2019

[19] Analyze the status of cloud services in the financial sector, FSEC, pp. 34~57, 2015

[20] Cloud and Financial Transformation, FSC, pp. 1~22, 2019

[21] A Case Study on the Cloud Specialized Distribution System in the U.K. and its Implications, NIA, pp. 1~10, 2018

[22] Cloud Computing Industry Status and Policy Implications in China, NIPA, pp. 1~12, 2012

[23] Cloud Computing Challenges, NARS, Seoul, ISSN 2005-3215, pp. 1~79, 2017

[24] M. S. Gang : Cloud Computing Market Trends and Prospects, KDB, Seoul, pp. 54~71, 2019

[25] ICTTechnical Level Survey Report, IITP, pp. 54~71, 2018

[26] Cloud Services Information Protection Guide, KISA, pp. 1~98, 2011

[27] Cloud Computing Issues and Status, KEIT, PP. 1~48, 2011

[28] Bishop, M, "Education in information security", *IEEE Concurrency*, Vol. 8, No. 4, pp. 4-8, Oct-Dec 2000.

[29] S. J. JUNG & Y. M. BAE, "Trend analysis of Threats and Technologies for Cloud Securit", *Journal of Security Engineering*, Vol. 10, No. 2, pp. 199-212, April 2013

[30] Höfer, C. N., & Karagiannis, "G. Cloud computing services taxonomy and comparison", J*ournal of Internet Services and Applications,* Vol. 2, No. 2, pp. 81-94, June 2011

[31] C. W. LEE, J. W. KIM, H. B. CHANG, "A Study on Design for Measurement of Industrial Technology Security Level Based on Digital Information Analysis", *Korea*

Intelligent Information Systems Society, Vol. 11, pp. 1-3, 2017

박원효(Won-Hyo Park)

2018년~현재: 중앙대학교 대학원 (융합보안학석사)

2018년～현재: 중앙대학교 일반대학원 융합보안학과 산업보안전공 석사과정
※관심분야: 클라우드, 산업보안, 방첩

장항배(Hang-Bae CHANG)

2006년: 연세대학교 정보시스템 박사

2014년~현재: 중앙대학교 산업보안학과 교수
※관심분야: 클라우드 서비스, 정보보호, 산업보안