클라우드컴퓨팅 시스템 환경의 효과적 위험분석평가 방법에 관한 연구

[1] 이정림, [2*]장항배

A Study on effective risk analysis and evaluation method of cloud computing system environment

[1]Junglimg Lee, [2*]Hangbae Chang

요 약

정보보안에 있어서 온-프레미스의 환경에서 위험분석평가에 대한 많은 연구가 진행되었지만, 클라우드컴퓨팅 시스템에 대한 위험분석평가의 효과적인 방법론에 대한 연구는 많이 부족한 실정이다. 2015년 클라우드컴퓨팅 발전법이 제정되어 클라우드컴퓨팅 도입 촉진 계기가 되었다, 그러나 클라우드컴퓨팅 시스템의 보안사고 증가 등의 이유로 활성화가 미진한 상황이다. 또한, 클라우드컴퓨팅 시스템을 도입하려는 관련 담당자의 클라우드컴퓨팅 시스템 기술 이해의 어려움 때문에 적극적으로 도입이 이루어지고 있지 않은 상황이다. 이에 관하여 이 연구는 클라우드컴퓨팅 시스템이 가진 특성과 개념, 그리고 모델을 살펴보고 이러한 특성이 위험분석평가에 어떻게 영향을 미치는지를 분석하여 효과적인 위험분석평가 방법을 제시하였다.

Abstract

Although many studies have been conducted on risk analysis and evaluation in the on-premises environment in information security, studies on effective methodologies of risk analysis and evaluation for cloud computing systems are lacking. In 2015, the Cloud Computing Development Act was enacted, which served as an opportunity to promote the introduction of cloud computing. However, due to the increase in security incidents in the cloud computing system, activation is insufficient. In addition, the cloud computing system is not being actively introduced because of the difficulty in understanding the cloud computing system technology of the person in charge who intends to introduce the cloud computing system. In this regard, this study presented an effective risk analysis and evaluation method by examining the characteristics, concepts, and models of cloud computing systems and analyzing how these characteristics affect risk analysis and evaluation.

Keywords: *Cloud computing, risk analysis and evaluation, CVE, CCE, CWE, CVSS, CWSS, OWASP*

[1] *중앙대학교 대학원 융합보안학과 석사과정 (junglimg@gmail.com)*
[2*] *교신저자 중앙대학교 산업보안학과 교수 (hbchang@cau.ac.kr)*

Received: May. 04, 2021, Revised: Jun. 01, 2021, Accepted: Jun. 24, 2021

I. 서론

1.1 연구 배경 및 목적

융합보안, 산업보안 등 모든 보안 영역에서 떼어 놓을 수 없는 공통적인 부분으로 ICT 기술을 사용과 ICT 환경에서 클라우드컴퓨팅 시스템 환경으로 급속하게 이전이 일어나고 있는 것을 들 수 있다. 클라우드컴퓨팅 시스템 도입의 촉진과 제도적 지원을 위해서 2015 년 '클라우드컴퓨팅 발전 및 이용자 보호에 관한 법' 이 제정되면서 각종 가이드 및 지원에 관한 법률이 제정되어 모든 기업에서 물리보안, 정보보안 등 ICT 와 관련된 시스템이 클라우드컴퓨팅 시스템으로 빠르게 이전되고 있다[1].

'정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 47 조에 따라 일정한 기준과 조건에 해당하는 기업은 의무적으로 정보보호 관리체계 인증을 받아야 하며 인증을 취득하기 위해서는 인증기준에서 요구하는 위험분석·평가를 반드시 수행하여야 한다. 또한, 국제표준화기구의 ISO27001 인증을 획득하기 위해서 통제항목 기준 8.1 과 8.3 에 따른 위험평가와 위험처리 절차를 수행해야 하며, '정보통신기반보호법' 에서 요구하는 '주요정보통신기반시설 보호대책' 수립 시에도 위험분석·평가를 수행해야 한다. 이처럼 일반기업, 공공기관 등은 인증체계를 획득하거나 효과적인 보안대책을 수립을 위해서 반드시 위험분석·평가를 수행해야 한다.

조직의 대부분 시스템은 온-프레미스(On-Premise) 환경으로 기업 내부에서 관리하는 방식이었다. 그러나 최근에 클라우드컴퓨팅 시스템의 확산으로 조직의 ICT 시스템을 클라우드컴퓨팅 시스템을 제공하는 기업이 운영하는 방식으로 변경되고 있다. 이렇게 클라우드컴퓨팅 시스템 환경으로 변경되면서 클라우드컴퓨팅의 기술 특징인 가상서버, 프로비저닝 기술, 하이파이저(Hypervisor) 기술, 컨테이너 기술 등으로 물리적 형태의 시스템 자산이 논리적 가상 형태의 시스템 자산으로 변화되고 있다. 따라서 온-프레미스 환경에서 물리적 행태의 시스템 자산을 식별하여 위험을 평가하는 방식을 클라우드컴퓨팅 환경에서는 논리적인 시스템 자산을 파악하여 위험을 평가하는 방식으로 전환하는 것이 필요하다. 그런데, 클라우드컴퓨팅 환경에서 시스템 서버는 여러 개의 논리적인 가상 서버로 구성되어 있고, 또한 클라우드컴퓨팅의 자동 확장 리스너 기술을 통해 가상 서버가 탄력적으로 확장, 축소되어 시스템 자산을 유일하게 식별하는 것이 어려워 효과적인 위험분석·평가에 이슈가 발생하고 있는 상황이다[2].

조직의 ICT 시스템 변화에 따라 사이버 환경에서 발생하는 위험으로부터 조직을 보호하는 일의 중요성은 더욱 커지고 있다. 기업 조직의 사이버 공간에 대한 침해 사고 가능성이 커지고 있어 자산에 대한 보안관리 활동을 체계적으로 수행하지 않을 경우 기업은 막대한 손실을 볼 수 있다. 따라서 이 연구는 클라우드컴퓨팅 시스템을 도입함으로써 시스템 자산을 식별하는 방식의 변화에 따라 위험분석·평가를 효과적으로 수행할 방법을 연구한다.

1.2 연구 배경 및 목적

이 연구의 목적 달성을 위해 클라우드컴퓨팅 시스템 개념 및 특성, 클라우드컴퓨팅 관련 기술, 메커니즘과 아키텍처, 관련 법률 등의 문헌고찰과 선행연구를 분석을 수행한다. 조직 또는 특정 분야에서 정보보안을 위한 위험분석·평가의 일반적인 방법론에 대한 이론적 개념과 특징을 살펴보고 위험분석·평가 방법론이 융합보안이나 산업보안 분야에 다르게 적용될 수 있는 특화된 방법론이 있는지를 검토하여 방법론의 특성을 고찰해 본다. 또한 클라우드컴퓨팅 시스템 위험분석·평가와 관련하여 취약점 진단을 위한 여러 기준의 프로비저닝 관련 사항을 분석하여 위험분석·평가 수행방법을 제시한다. 그리고 국내 정보보호 전문 기업의 전문가를 대상으로 인터뷰를 통한 검증을 수행하며, 위험분석·평가에 대한 효과적인 방법에 대한 결과 및 시사점을 도출한다.

이 연구는 클라우드컴퓨팅 시스템을 도입하려는 기업과 기관 등에 조직의 경쟁 도구로써 더욱더 빠르게 확산하고 정착될 수 있도록 전략적 방향을 제시한다. 또한 추가로 클라우드컴퓨팅 시스템에 영향을 미치는 특성 요소들을 분석하여 효과적인 위험관리를 제시하는 데 연구의 의의가 있을 것이다.

II. 이론적 배경 및 선행연구

2.1 클라우드컴퓨팅 시스템 개념 및 특성

클라우드컴퓨팅 시스템은 확장할 수 있고 탄력적인 IT 기능이 컴퓨터 통신망을 통해서 사용자에게 제공되는 컴퓨팅 방식으로 정보통신망을 통해 시스템을 사용한 만큼 과금 되고 셀프 서비스하는 방식으로 제공되는 표준화된 시스템 기능이다. 컴퓨팅의 정보처리가 기업이 보유한 시스템에서 이루어지는 것이 아니라 클라우드컴퓨팅을 제공하는 기업의 시스템에서 이루어지기도 한다. 또한, 클라우드컴퓨팅은 시스템 자원에 시간과 장소에 제약 없이 필요에 따라 편리하게 정보통신망을 통해 접근이 가능한 기능을 제공한다. 클라우드컴퓨팅 시스템은 컴퓨팅 시스템을 효과적으로 사용할 수 있도록 신속한 프로비저닝 특성이 있으며 5 가지 기본 특성과 4 가지 배포 모델, 3 가지 서비스 형태가 있다[3].

클라우드컴퓨팅은 다음과 같이 5 가지 기본 특성을 갖는다. 첫째, 주문형 셀프서비스(On Demand Self Service) 형태이다. 컴퓨팅 시스템이 필요한 경우 시스템 관리자의 관여 없이 사용자가 시스템을 즉시 사용할 수 있는 특성이 있다. 둘째, 광역 네트워크 액세스(Broad Network Access) 형태이다. 클라우드컴퓨팅 시스템 사용자는 정보통신망을 기반으로 어디서나 시스템에 접속할 수 있으며, 사용자는 다양한 클라이언트 플랫폼에서 시스템에 접근할 수 있는 특성이 있다. 셋째, 빠른 탄력성(Rapid Elasticity) 이다. 클라우드컴퓨팅 시스템 사용자는 자원을 원하는 대로 확장할 수 있으며, 요구하는 만큼의 수준으로 축소도 할 수 있다. 또한, 이러한 확장과 축소의 작업이 실시간으로 이루어지는 특성이 있다. 넷째, 자원의 공동관리(Resource Pooling) 형태이다. 물리적인 시스템이나 가상화된 시스템을 풀(Pool)로 관리할 수 있으며 사용자의 요청으로 사용자에게 할당되거나 다시 풀(Pool)로 반환된다. 사용자는 시스템이 위치한 물리적인 장소나 크기를 알지 못하며 시스템이 논리적으로 추상화되어 운영되는 특성이다. 다섯째, 측정 가능한 서비스(Measured Service) 형태이다. 클라우드컴퓨팅 시스템을 제공하는 서비스 제공자는 시스템의 사용량을 실시간으로 수집하고 모니터링 할 수 있어 사용한 양에 따라서 사용요금을 부과할 수 있으며, 모니터링에 따라 자원이 부족한 경우 자원을 추가하여 제공할 수 있는 특성이 있다.

클라우드컴퓨팅은 4 가지 배포 모델 형태가 있다. 큰 규모의 기업이나 기관 또는 스타트 기업과 같은 중소기업에 컴퓨팅 시스템을 제공해 주는 퍼블릭 클라우드(Public Cloud) 모델이 있다. 보안 강화를 목적으로 기업이 자체적으로 운영하거나 클라우드컴퓨팅 시스템 제공자가 한 기업이나 기관만을 위해 강화된 방화벽을 구성하여 독립적인 네트워크를 운영하는 형태인 프라이빗 클라우드(Private Cloud) 모델이 있다. 커뮤니티 클라우드 모델(Community Cloud)은 공동의 목적을 가진 커뮤니티를 위하여 운영되는 모델 형태이다. 공공 클라우드와 사설 클라우드 중에서 개인정보 등 중요하게 보안 활동을 해야 부분은 프라이빗 클라우드 시스템으로 구축을 하고 상대적으로 중요성이 낮은 부분은 퍼블릭 클라우드를 이용하는 형태의 모델이 하이브리드 클라우드(Hybrid Cloud) 이다[2, 4, 5, 6, 7].

시스템을 어느 범위까지 클라우드컴퓨팅 시스템으로 사용하는지에 따라서 서비스 형태를 그림 2 와 같이 3 가지의 서비스 형태로 구분한다. IaaS(Infra as a Service) 모델은 서버나 스토리지 등 필요한 물리적인 인프라 시스템을 사용하는 형태이다. PaaS(Platform as a Service) 모델은 소프트웨어 개발에 필요한 개발 프로그램 및 운영체제와 같은 플랫폼을 개발자에게 제공하여 개발의 효율성을 높이는 컴퓨팅 시스템을 사용하는 형태이다. SaaS(Software as a Service) 모델은 소프트웨어 및 애플리케이션을 정보통신망을 통해서 사용할 수 있게 해주는 형태로 이렇게 세 가지로 구분된다[2, 8].

2.2 클라우드컴퓨팅 법률

클라우드컴퓨팅 도입의 촉진을 위해서 2015 년 클라우드컴퓨팅 발전법을 제정하여 시행하고 있다. 클라우드컴퓨팅 발전법 제정을 계기로 그간 정체되어 있던 기업 및 공공부문 등의 시장에 클라우드컴퓨팅 시스템 도입을 촉진하는 계기가 되었다. 클라우드컴퓨팅 발전법에 “침해사고 등의 통지 등” 조항에서 “침해사고가 발생한 때” 그리고 “이용자의 정보가 유출된 때”

유출된 사실을 서비스를 이용하고 있는 이용자 등에게 알려야 하고 이용자 대한 정보가 저장된 국가를 알려줄 것을 요구하고 있어 클라우드 컴퓨팅 서비스를 이용 시 발생되는 개인정보에 대한 보호조치에 관해서 규정하고 있다[2, 3].

클라우드컴퓨팅 발전법 제정으로 클라우드컴퓨팅 도입을 확산하고 발전 기반을 만들어 클라우드컴퓨팅 이용을 활성화하고자 하였으나 현재 기업 및 기관이 클라우드컴퓨팅 시스템 구축을 빠르게 진행하지 못하고 있다. 클라우드컴퓨팅 시스템 도입으로 클라우드컴퓨팅 시스템 제공자의 데이터센터 리전에 따른 이슈, 시스템 관리에 대한 책임과 권한의 범위에 대한 이슈 등 문제점이 제기되고 있어 쉽게 클라우드컴퓨팅 시스템의 활성화가 이루어지고 있지 못한 실정이다. 또한, 클라우드컴퓨팅의 기술적 특징인 가상화, 분산화의 기술이 적용되기 때문이며 위험관리에 어려움이 발생하며 이러한 부분이 시스템을 활성화하는 데 장애 요소로 작용하고 있다[9].

개인정보의 국외이전 시 개인정보보호법에서 규정한 내용을 준수해야 한다. 따라서 개인정보를 국내 리전에만 저장하도록 클라우드 관리콘솔에서 설정 등을 반영하여 계약을 체결할 수 있다. 그러나 클라우드의 분산화 기술, 가상화 기술, 가용성 확보 기술에 따라 데이터가 제 3 국으로의 이동의 가능성이 있는 아키텍처를 갖고 있다. 이러한 기술적 구조 때문에 전문기술자들조차 물리적 데이터 저장의 위치를 정확하게 파악할 수 없다고 한다.

금융기업의 경우 전자금융감독규정에 따라 클라우드컴퓨팅 서비스 이용 절차와 규정을 준수해야 한다. 이에 따라 개인신용정보에 대한 보호와 데이터 저장 위치 관련하여 재해복구센터 및 정보처리시스템이 국내에 설치된 클라우드컴퓨팅 시스템을 이용해야 한다. 이 또한 분산된 기술로 시스템의 자산 위치를 정확하게 파악하는 것이 현실적으로 어려울 수 있는 상황이다. 이러한 상황으로 기업이 비즈니스 목적으로 달성하기 위해 ICT 시스템을 클라우드컴퓨팅 시스템 형태로 이용 시 정보보호관리체계 인증 등을 취득하기 위하여 위험분석·평가를 수행할 경우 시스템 자산을 정확하게 식별하지 못하여 결국, 위험을 평가하는 데 어려움이 발생하고 있다.

2.3 위험분석 방법론

2.3.1 위험분석 방법론 고찰

위험관리는 정보자산의 중요성 평가 및 위협과 취약점에 대한 분석을 하여 정보자산에 발생할 수 있는 위험 수준을 검토하고, 이에 대한 보안 대책과 통제를 하여 자산의 위험을 허용 가능한 수준(DoA: Degree of Assurance) 이하로 감소시키기 위한 관리활동을 하는 것을 말한다[10].

위험의 관리 절차 및 단계는 첫째, 현황분석 단계로 보유 자산에 대한 파악 및 분석 시점에서의 정보보호 활동을 분석하는 단계, 둘째, 조직의 자산에 대한 관리 · 운영상의 위험 수준을 평가하는 단계, 셋째, 정보자산의 위험 수준을 평가하기 위하여 취약점을 진단하는 단계, 넷째, 분석 시점의 정보보호 수준 및 향후 통제 수준을 고려하여 DoA, 즉 허용 가능한 위험 수준을 산정하고 이에 따른 High Risk 를 제시하는 단계, 다섯째, 정보자산에 대한 High Risk 의 취약점을 처리하기 위해 통제 정책을 수립하고 상세 통제사항을 정의하는 단계, 여섯째, 조직 전체의 보안 통제를 적용하기 위하여 정보보호 정책 및 절차, 업무절차 등을 재조정하는 단계, 일곱째, 수립된 통제 정책을 정책과 지침, 절차에 따라 조직의 프로세스 환경에 적용하고 위험 수준을 감소시키는 단계, 여덟째, 통제적용 후 남아있는 잔존 위험에 대하여 수용관리 및 지속적인 위험관리를 통하여 잔여 위험을 모니터링하는 단계로 구성되어 있다[11].

위험분석평가는 위험관리 프로세스의 한 단계로 기업 자산에 대한 손상으로 사업에 영향을 미치는 상황과 보호 대상 자산에 영향을 줄 수 있는 위협과 취약점을 분석하여 위협이 발생할 경우 자산에 미치는 잠재적 영향을 산출하는 관리 프로세스이다. 위험평가 요소로 자산, 취약점, 위협이 있으며 자산은 조직 또는 기업이 비즈니스 목적을 달성하고 생존하기 위해서 보호가 필요한 대상, 즉, 정보보호 관점에서 자산은 정보자산과 정보의 효율적인 활용을 위한 관련 자산으로 정의한다. 취약점은 조직의 내부와 외부의 공격에 쉽게 노출되고 손상될 수 있는 자산에 내재된 약점이며, 위협은 자산의 속성이 가지고 있는 취약점 때문에 기업의 손실 등을 발생시킬 수 있는 외부의 요인 또는 사건으로 정의한다[12].

위협이 발생하여 기업에 손실이 발생하려면 위협과 연결된 취약점이 있어야 가능하다. 따라서 “위험=자산 × 위협 × 취약점” 식으로 위험도를 산출할 수 있다. 또한 위협은 발생 가능성으로 표현되며 취약점으로 인해 자산에 미치는 영향은 손실의 크기로 표현할 수 있다. 따라서 “위험= 위협의 발생 가능성 × 자산에 미치는 영향(손실 크기)” 식으로 나타낸다[12]. 이러한 위험분석평가에 대한 방식이 일반적으로 위험을 평가하는 방법으로 적용될 수 있는 표준화된 방법론이다.

위험 분석 · 평가 방법론은 위험 분석 · 평가의 수행기준 및 접근방법에 따라 표 1 과 같이 기준선 접근법, 상세위험 접근법, 비정형 접근법인 전문가 판단법, 기준선 접근법과 상세위험 접근법을 혼합하여 사용하는 복합접근법을 기준으로 시스템에 대한 위험분석평가를 수행한다[12].

Table 1. Risk analysis and assessment approach
표 1. 위험·분석평가 접근법

Application method	Description
Baseline Approach	- Define the security level for all information assets and establish a series of protection measures to achieve security goals - It is possible to establish the necessary security measures for the organization without investing a lot of resources such as time and money - Because the environmental characteristics of the organization are not reflected, security controls are applied at a level higher or lower than the ability of the organization
Detailed Approach	- Determine the size of risk by measuring the importance of information assets and examining vulnerabilities of information assets and threats using them - It is possible to establish a security level that can be applied according to the characteristics of the organizational environment - It requires a lot of time and money as it is performed by experts who are skilled in risk analysis and evaluation
Expert Decision	- Conduct risk analysis with the knowledge and judgment of experts who are experienced in risk assessment without applying standardized methods - Because there is no systematic analysis and evaluation method, it may be difficult to accurately assess risks, and it may be difficult to rationally select security measures and derive appropriate costs. - Limits exist as an evaluation method for continuously repeated security audits or follow-up management
Compounded Approach	- First, identify high risk targets in the organizational process, apply the detailed risk approach to high-risk targets, and use intuitive methods such as the baseline approach for low risk targets - It is possible to quickly establish security control measures and efficiently use the resources invested in risk analysis and evaluation - Failure to accurately distinguish between high risk and low risk may result in wastage of resources

온-프레미스 환경에서 위험평가를 수행하기 위해서 시스템 자산을 표 2 와 같이 시스템 장비, 네트워크 장비, 보안장비 등으로 식별한다[12].

클라우드컴퓨팅 시스템 환경의 경우 앞서 선행 연구를 고찰한 위험분석평가를 방법론을 그대로 적용할 수 있을 것인가에 대한 문제를 제기할 수 있다. 클라우드컴퓨팅 기술의 특성으로 시스템 자산을 온-프레미스 환경과 같이 개별적으로 물리적 고정형태의 시스템 자산을 식별할 수 없기 때문에 “위험=자산 × 위협 × 취약성” 공식을 그대로 적용할 수 없는 문제점이 발생하게 된다. 그렇다면, 클라우드컴퓨팅 환경에서 일반적이고 통용적으로 사용하는 위험분석 방법론이 아닌 다르게 적용할 수 있는 방법론이 있을지에 대한 논의가 필요하게 된다.

정보보안에 대해서 컨설팅을 수행하는 기업의 방법론과 융합보안 또는 산업보안에서 위험평가를 위한 다른 방법론을 적용하고 있는지 비교 검토를 통해서 방법론이 차이를 고찰해 본다.

Table 2. System asset classification criteria
표 2. 시스템 자산 분류 기준

Asset type	Description	Examples of such assets
system equipment	Infrastructure systems such as servers required to perform corporate services and tasks	- Data Server, Data Historian, Input/Output(IO) Server - DNS, DB server, public server (Web, Mail), file server, management server (NMS, SMS), application server, log server, etc. [※O/S, web server, WAS server, database, etc.]
network equipment	Routers, switches, etc. installed in networks to connect information and communications networks	- Router, L3 switch, L2 switch, L4 switch
security equipment	Firewall for information protection, intrusion prevention system, etc.	- DDoS equipment, firewall, IPSec VPN, IPS, VPN
DBMS	DBMS for service and business	- Administrative and academic affairs DB, public member DB, system management data storage
Backup and storage	Device for data backup	- Storage, SAN switch, etc.
PC	business PC	- PC for management console, distribution PC

2.3.2 위험분석 방법론 비교

위험분석 방법론과 관련하여 정보보호 전문서비스 기업이 가진 정보보안 컨설팅 방법론에서 위험분석평가 방법론에서 개념을 찾아볼 수 있다. 정보보안 컨설팅 결과물을 도출하기 위해서 위험분석평가 대상 식별하고 현상을 관찰하여 문제점을 찾아서 그 대책 마련하는 절차, 규칙 등의 집합체로 핵심 내용을 구성하고 있다. 국내에서 대표적인 보안 전문업체 A 사의 보안컨설팅 방법론이나 최근에 보안 전문업체로 지정된 H사의 보안컨설팅 방법론을 보면 절차 및 단계에 따라서 사용하는 용어를 달리 사용하고 있을 뿐 개념적으로 보면 동일하다.

정보보호 전문서비스 기업인 A 사는 2004 년 한국소프트웨어 기술대상을 받은 ASEM 방법론을 제시하고 있다. 방법론을 보면 “정보보호 전문 컨설턴트가 보안 진단을 통해 위협을 분석하고 대책을 수립하여 최적의 정보보호 시스템 구축을 위한 체계적이고 과학적인 방법”이라고 설명하고 있다. 또한, 특징으로 “PC 통합보안에서부터 네트워크 Appliance, 인터넷 보안에 이르기까지 기반기술과 개발 요소기술을 바탕으로 고객 요구에 최적으로 만족하는 컨설팅 서비스를 제공”함을 설명한다[13].

위험분석 방법의 핵심적인 구조는 위험분석 평가를 수행하면서 PDSC(Plan-Do-See-Check) 접근 방식으로 단계별 세부적인 활동 내용으로 구성되어 있다. PDSC(Plan-Do-See-Check) 기법을 근간으로 정의된 절차에 따라 정보보안 컨설팅을 수행함으로써 정보보호의 궁극적인 목적인 기밀성, 무결성, 가용성을 달성하는 것을 핵심내용으로 하여 첫째, 계획수립 과정, 둘째, 위험분석 과정, 셋째, 대책수립 과정, 넷째, 구현관리 과정의 4 단계의 핵심 과정을 설명한다. 각 단계에는 정보보안 컨설팅수행을 위해 적용할 수 있는 프로세스와 표준 템플릿을 제시하며 원활한 프로젝트 관리와 품질을 위해서 프로젝트 수행 시 발생할 수 있는 위험을 최소화하고 높은 품질 서비스를 제공하기 위해서 5 단계에서 품질보증 프로세스를 적용한다.

2020 년 하반기에 ‘정보보호 전문서비스 기업’으로 신규 지정된 H 사의 방법론은 보면 4 단계로 구성된 환경분석, 취약점분석, 위험분석 및 대책수립, 인증지원 절차로 구성되어 있다. H 사의 방법론은 단계별로 구조화하여 특징적 핵심 내용을 설명하고 있을 뿐 A 사의 방법론과 비교해 보면 차이가 없이 대동소이함을 알 수 있다. 즉, 조직의 현황을 분석해서 위협과 취약점을 진단하고 위험을 평가하여 보호대책을 제시하는 핵심 절차나 과정의 맥락이 동일함을 알 수 있으며 다만 사용하는 용어, 표현, 절차의 순서가 다를 뿐이다[14].

한국산업기술보호협회(KAIT)의 주요사업 분야에 ‘산업보안 진단 컨설팅’ 비즈니스가 있다. “기술유출사고 예방 및 산업보안 의식강화, 중장기 보안대책 마련 등을 통해 기업의 보안수준

제고와 대외 신뢰도 향상을 위해 보안전문가가 현장을 방문하여 보안영역별 취약점을 점검함으로써 보안관리 문제점을 찾아내고 보호대책과 개선방안 등을 제시해 주는 서비스”로 설명하고 있다.[18] 한국산업기술보호협회(KAIT)는 산업보안 컨설팅 수행방법을 “기업 현황파악, 임직원 보안의식 조사, 자산분류 및 중요도 평가, 보안영역별 취약점 점검, 위험식별 및 분석, 평가, 수용가능한 위험수준(DoA) 선정, 보안영역별 대응방안 제시, 보안전문분야 상담 및 보안교육, 보안규정 및 지침, 절차 제ㆍ개정, 최종결과 보고” 단계로 제시하고 있다[18]. 본 컨설팅 방법론의 특징은 A 사의 방법론과 H 사의 방법론의 절차를 세부적으로 구분해서 설명하고 있을 뿐 내용상의 차이는 없다[15].

산업보안을 위한 위험분석 방법이나 정보보안을 위험분석 방법에 있어서 보안의 대상에 차이가 있을 뿐 위험분석을 통해서 조직의 위험을 보호하고자 하는 목적이 동일하다. 위험분석평가를 하고자 하는 기업은 핵심업무를 파악하고 업무를 지원하는 자산을 가장 우선적으로 식별하여 자산을 목록화하고 이에 대해서 위험분석평가와 연관된 정보인프라의 취약점을 분석하여 기업의 비즈니스 목적 달성을 위해 안전성과 신뢰성을 위한 정보보안의 대책방안을 제시하는 방법은 동일하다.

2.3.3 위험분석 취약점 점검 기준

위험평가를 위해서 시스템에 대한 자산을 우선 식별해야 한다. 다음으로는 시스템 자산에 대해서 취약점을 식별해야 한다. 취약점은 시스템 또는 소프트웨어에 존재하는 보안 약점을 말한다. 시스템의 장애 또는 데이터의 분실, 도난, 유출, 변조 또는 훼손이 발생하는 취약점을 평가하기 위한 기준으로 CVE, CCE, CWE, CVSS, CWSS, OWASP 가 있다.

CVE(Common Vulnerabilities and Exposures)는 웹서비스, 시스템 OS 에서 발견된 취약점에 대해서 고유의 식별번호를 부여하여 전 세계적 공통으로 인식할 수 있는 취약점 목록을 제시한다. CVE 의 식별번호는 “CVE - (연도) - (발생순서)” 규칙으로 번호를 부여며, MITRE 라는 기관에서 CVE 를 관리하고 있다[16].

CCE(Common Configuration Enumeration)는 OS 시스템에 있어서 접근권한 이상의 동작을 허용 또는 범위 이상의 정보를 열람하거나 변조 또는 유출을 가능하게 하는 시스템 취약점 목록을 정의한다. 시스템 자산의 취약점을 점검할 경우 통상적으로 CCE 에 대한 기준으로 진단을 하며, 우리나라의 경우 ‘정보통신기반보호법’에서 정의하고 있는 취약점을 수행하기 위해서 ‘주요정보통신기반시설 취약점 분석평가 가이드’에서 서버, 네트워크, 보안장비 등의 취약점 목록으로 공개하고 있다[17].

CWE(Common Weakness Enumeration)은 프로그래밍 언어인 C, C++, Java 및 아키텍처, 설계, 코딩 등에서 발생하는 취약점 목록을 정의한다. 국내에는 프로그램 개발 시 안전한 소스 코드 작성을 위해 한국인터넷진흥원에서 ‘시큐어 코딩 가이드’를 공개하고 있다[18].

CVSS(Common Vulnerability Scoring System)는 하드웨어와 소프트웨어 플랫폼 전체에 걸쳐서 취약점을 등급으로 나누어 점수화하는 방식을 제공하고 있다. 이 취약점 기준은 시간과 환경에 제약을 받지 않는 특성이 있는 시스템의 기본 영역과 시간의 변화에 따라 취약점 변경이 나타나는 시간 영역 그리고 특정 상황에 따라 변화가 나타나는 환경 영역이 있다. 기본 영역은 공격의 장소(Access Vector), 공격 형태의 복잡성(Access Complexity), 인증의 필요성(Authentication)에 대해서 기밀성, 무결성, 가용성에 대한 Impact 를 측정한다. 시간 영역은 공격 가능성(Exploit ability), 취약점 복구 수준(Remediation Level), 보고 신뢰성(Report Confidence)에 대한 진단을 수행하며, 환경 영역에서는 이차적 피해 가능성(Collateral Damage Potential), 공격 목표의 분포(Target Distribution)에 대해서 기밀성, 가용성, 무결성에 대한 보안 사항을 평가한다. 이렇게 미리 정의된 개별 항목들의 결과 값을 선정하여 기본 영역을 기초로 하고 시간 영역 및 환경 영역은 상황에 따라 선택하는 방식을 이용하여 0 부터 10 점까지의 점수를 도출하여 위험도를 정량적으로 평가하는 방식이다[26]. 이러한 취약점 기준은 클라우드컴퓨팅 시스템에서 적용할 수 있는 부분과 적용을 할 수 없는 부분이 존재한다. 클라우드컴퓨팅 서비스 제공자인 A 사의 클라우드 EC2 서비스의 경우 표 3 과 같이 기존의 점검 목록과는 다른 항목으로 취약점 점검을 수행해야 한다[19].

Table 3. Cloud common part check items
표 3. 클라우드 공통부문 점검 항목

Domain	Item name	Importance
EC2 Common Area Account Security	key pair	High
	AWS Access Password Settings	High
	Multi Factor Certification	Middle
	access key	High
	Identity-Based Policy (IAM) Account Security	Low
	Identity-Based Policy (IAM) Security Policy Settings (EC2/ECS/ECR)	High
EC2 Common Area Network Security	Security Group	Middle
	ACL	Middle
	NAT Gateway	Low
	Internet Gateway	Low
	Routing Tables	Middle
	Elastic IP	Low
RDS common area	Manage RDS Resource Access Permissions	Middle
	Authorize RDS API operations	Middle
	Subnet Availability Zones	Low
	Identity-Based Policy (IAM) Security Policy Settings (RDS)	High
RDS Options Policy	RDS parameter management area setting	Low
	MariaDB/MySQL Audit Plugin Settings	Low
	Oracle APEX Listener Settings	Middle
	Oracle Basic Network Encryption (NNE) Settings	Low
	Oracle SSL Settings	Low
	Oracle Enterprise Manager (OEM) Setup	Middle
	Oracle UTL MAIL Setup	Low
RDS logging	MariaDB/MySQL Security Log Settings	Low
	MSSQL Security Log Settings	Low
	Oracle Security Log Settings	Low
	PostgreSQL Security Log Settings	Low
S3 Data Security	Bucket Access Security	Middle
	Default encryption settings	High
	Log file collection and permission settings	Middle
	Identity-Based Policy (IAM) Security Policy Settings (S3)	High

OWASP 평가항목은 표 4 와 같이 웹서비스에 대한 취약점에 대해서 비인가자들로부터 공격 성공 확률 (Likelihood)을 평가하는 항목, 공격이 이루어져 조직에 미치는 영향 (Impact)을 평가하는 항목으로 분류된다[20].

공격 성공 확률 평가는 위협원으로부터 공격 성공 가능성을 추정하는 위협요소(Threat Agent)와 특정 취약점 도출 그리고 공격의 가능성을 추정할 수 있는 취약점(Vulnerability)으로 이루어진다. 위협요소는 위협원이 기술적으로 숙련되어 있는지에 대한 수준(Skill Level), 위협원의 집단이 취약점을 찾아 공격의 목적을 달성하기 위한 동기(Motive), 위협원의 집단이 취약점을 도출하고 공격하는데 필요한 자원과 기회(Opportunity), 위협원의 집단 크기(Size)를 평가하도록 구분된다. 취약점은 쉽게 도출할 수 있는가(Ease of Discovery), 쉽게 취약점을 공격할 수 있는가(Ease of Exploit), 취약점이 외부에 공개되어 있는가(Awareness), 취약점을 공격할 때 탐지가 가능한가(Intrusion Detection)에 대해서 진단을 할 수 있게 되어 있다.

공격이 실행되어 성공하게 되면 기업에 미칠 수 있는 영향을 평가하는 항목은 취약점이 도출되어 공격을 받게 되었을 때 시스템에 미치는 기술측면의 영향(Technical Impact)을 평가하는 것과 사업 목적에 영향을 미치는 정도(Business Impact)를 분석하는 항목으로 구분된다[21].

Table 4. OWASP Risk Assessment Method Assessment Items
표 4. OWASP 위험평가 방법 평가항목

OWASP Risk Rating Methodology		
Likelihood	Threat Agent	Skill Level
		Motive
		Opportunity
		Size
	Vulnerability	Ease of Discovery
		Ease of Exploit
		Awareness
		Intrusion Detection
Impact	Technical Impact	Loss of Confidentiality
		Loss of Integrity
		Loss of Availability
		Loss of Accountability
	Business Impact	Financial Damage
		Reputation Damage
		Non-Compliance
		Privacy Violation

앞의 이론적 배경과 선행연구를 통해 시스템 자산에 대한 위험분석평가는 자산 식별과 이러한 자산에 대한 취약점을 진단하여 위험을 산정하는 것에 대해서 공통으로 적용할 수 있는 방법론을 살펴보았다. 또한 위험분석평가는 범위에 포함되는 대상을 식별하여 특성과 환경 부분을 함께 고려해야만 일관적이고 효과적인 평가를 수행할 수 있는 점을 검토했다.

최근 클라우드컴퓨팅 기술을 적용한 다양한 방식의 시스템 환경이 등장하고 있지만 클라우드 환경의 위험분석평가를 정성적, 정량적으로 위험 값을 산출하는 연구가 없기 때문에 클라우드컴퓨팅에 대한 사이버 공격을 대응하기 위한 위험분석평가 방법론의 연구는 시스템의 안전성을 확보하는 데 효과적일 것이다.

일반으로 보안을 위한 위험분석평가의 취약점 평가 방법론인 CVSS, CWSS, OWASP 등의 평가 항목은 온-프레미스의 시스템 또는 소프트웨어 등의 레거시 인프라 환경 특성과 상태를 고려하여 구성되어 있어 효과적인 위험평가를 수행할 수 있도록 한다. 그러나 클라우드컴퓨팅 시스템 관점의 다양한 취약점 대상을 고려하지 않고 제시된 항목이므로 클라우드컴퓨팅 시스템의 효과적인 위험분석평가를 위해서 클라우드컴퓨팅 시스템 자산에 대한 식별 문제와 클라우드컴퓨팅이 갖는 특성의 취약점 진단 항목과 평가방식을 제시함으로써 정성적이고 정량적인 위험분석평가에 대한 효과적인 방법론을 제시할 수 있다.

III. 클라우드컴퓨팅 시스템의 효과적 위험분석평가 방법 설계

3.1 클라우드컴퓨팅 시스템 자산 식별

클라우드컴퓨팅 시스템의 자산은 온-프레미스에서 식별하는 자산 분류와는 다른 체계를 적용해야 한다. 클라우드컴퓨팅 시스템 모델인 IaaS, PaaS, SaaS 에 따라 클라우드컴퓨팅 시스템 제공자가(CSP) 책임을 지는 영역과 클라우드컴퓨팅 소비자가 책임을 지는 영역을 구분해서 자산을 파악해야 한다.

IaaS 기준에서 CSP 가 책임을 지는 영역에 대한 시스템 자산 식별은 Physical Network, Storage, Server, Hypervisor 를 기준으로 시스템 자산에 대해 식별을 해야 한다. Hypervisor 는 논리적인 가상 서버를 통제하는 프로그램으로 위험평가를 위해서 식별을 명확히 해야 하는 부분이다. 클라우드컴퓨팅 기술의 특징으로 서버는 물리적 형태가 아닌 가상화된 형태로 존재하기 때문에 가상서버에 대한 현황을 파악해야 한다. 가상서버는 탄력적 확장 및 축소를 통해서 시간 및 상황에 따라 변동성을 가질 수 있어 가상화 이미지를 대상으로 자산을 파악한다. 백업 스토리지 시스템 또한 서버와 같은 방식으로 가상화가 되므로 Storage 이지를 대상으로 자산을 파악해야 한다. 네트워크의 영역에서는 물리적 네트워크를 할당받게 되는데 이 부분은 온-프레미스 방식과 동일하게 식별하여 위험분석평가에 반영한다. PaaS 의 경우 IaaS 시스템 자산에

추가하여 CSP 가 관리하는 영역이 Runtime, Middleware, Operating System, Virtual Network 까지 확대된다. 이 부분에서도 각 부문에 있어서 자산을 식별해야 하며 각 단계에서 가상화된 시스템을 이미지 형태로 자산을 파악하여 위험분석평가에 반영해야 한다. SaaS 의 경우에는 PaaS 시스템 자산에 추가하여 CSP 가 관리하는 영역이 Application 까지 확대된다[22].

응용프로그램의 시스템 자산은 서비스의 URL 형식으로 자산을 파악한다. 이처럼 시스템 제공 형태에 따라 소비자의 관리 관할 영역이 다르게 되며 자산의 소유권이 CSP 에 있게 되면 자산의 통제권한이 소비자 영역 밖에 존재하게 된다. 시스템 자산의 권한이 소비자에게 있지 않고 CSP 에 있게 되면 위험분석평가를 수행하는 주체가 달라 된다. 그러나 시스템 자산의 권한이 소비자의 영역 밖에 존재한다고 하여 위험분석평가를 수행하지 않아도 될 수 있다고 여길 수 있으나 기업의 보안대책을 수립하거나 ISMS 인증을 취득하기 위해서는 위험분석평가가 소비자 관점에서 이루어져야 한다. 소비자는 클라우드컴퓨팅 시스템을 사용하고 있는 자산에 대한 명확한 목록를 작성하고 관리를 해야 위험평가에 자산을 누락하여 위험을 초래하는 상황을 제거할 수 있다.

3.2 클라우드컴퓨팅 관리적 위험평가 항목

취약점에 기준에 대한 고찰을 통해서 살펴본 항목들은 기술적 요소 부문만을 언급했다 그러나 클라우드컴퓨팅의 위험분석평가는 관리적 취약점 항목도 고려해야만 한다. 관리적 취약 항목으로 클라우드컴퓨팅 서비스의 안전성에 관한 요소를 제시한다. “금융분야 클라우드 컴퓨팅 서비스 이용 가이드”에서 명시된 안전성 점검 기준을 적용할 수 있으며 인적보안, 자산관리, 서비스 위탁 업무 관리, 침해사고 관리, 서비스 연속성 관리, 암호화 및 데이터 보호, 접근통제, 네트워크 보안, 시스템 운영관리 9 개 분야에 대해서 세부 점검항목을 조직 특성에 맞게 적용하여 취약점의 형태를 5 점 척도로 위험분석평가를 수행한다. 취약점에 대한 양호 판단의 정도를 VH(Very High, 5 점), H(Hing, 4 점), M(Middle, 3 점), L(Low, 2 점), VL(Very Low, 1 점)으로 구분하여 위험분석 산식에 반영하여 위험을 계산한다. 관리적 위험평가 항목을 표 5 와 같이 제시한다.

3.3 클라우드컴퓨팅 기술적 위험평가 항목

온-프레미스 환경에서의 기술적 항목은 선행연구 고찰에서 검토한 CWE 항목 기준에서 보면 서버는 계정관리, 시스템 및 서비스 관리, 파일관리, 접근통제, 감사 및 패치관리 부문에서 취약점 도출과 위험평가를 수행하며, WEB/WAS 는 계정관리, 보안설정, 취약점 관리, 보안패치 부문, DBMS 는 계정관리, 로그관리, 보안설정, 접근통제, 감사 및 패치관리, 네트워크는 계정관리, 로그관리, 보안설정, 접근통제 기준을 적용을 한다. 클라우드컴퓨팅은 환경에는 특화된 콘솔 취약점 점검 항목을 통해서 위험분석평가를 수행해야 한다. 이에 따른 취약점 점검 분야는 계정/사용자 관리, 데이터보호, 키관리, 네트워크 설정, 로깅 및 모니터링, 서비스 관리 6 개 영역으로 구분한다. 계정/사용자 관리 영역은 Account 와 IAM 서비스를 통한 사용자 및 정책관리를 평가하며, 데이터보호 영역은 서비스에 대한 저장/통신 시 암호화, 키관리 영역은 KMS 또는 타 솔루션을 통한 암호화 키 보호, 네트워크 설정 영역은 Cloud 환경 고유의 네트워크 서비스 접근통제, 로깅 및 모니터링 영역은 CloudTrail, CloudWatch 등을 통해 로그 설정 및 모니터링, 그리고 서비스 관리영역은 S3, RDS, EC2 등 서비스에 특화된 관리 영역을 평가한다. 각 기술적 평가항목에 대해서는 노출위험도를 산정하며 노출위험도의 방식은 3 점 척도를 기준으로 한다. 노출위험이 가장 높은 경우 상(3 점), 보통인 경우 중(2 점), 낮은 경우 (1 점)으로 점수를 반영하여 위험을 계산한다.

Table 5. Cloud system management evaluation items
표 5. 클라우드 시스템 관리평가 항목

No	Domain(9)	Classification	Number of items
1	Human security	Cloud Computing System Service Operation Organization	2
		Separation of duties	1
		Job change management	2
		Implementation and review of cloud computing system service security training	2
2	Asset management	Virtual resource status management	2
		Importance rating	1
		Setback checking	2
3	Service consignment management	Cloud computing system service contract management	3
		Cloud computing system service provider and self-evaluation	2
4	Incident management	Establishment of processes and systems for responding to incidents	3
		Intrusion incident response test and inspection for prevention	2
5	Service Continuity Management	Establishment of business continuity plan	4
		Disaster recovery simulation training	3
		Service availability management	2
		Data backup	3
		Redundancy of information processing system	1
6	Access control	Establishment and application of access control policy	1
		Access record management	3
		Register user account and grant access	3
		Administrator and special privilege management	3
		User identification and authentication	3
		Management of insider password change, etc. for employees, etc.	1
7	Network security	Network security policy establishment	1
		Network information protection system operation	2
		network encryption	1
		Network Physical and Logical Zone Separation	2
8	Data protection and encryption	Encryption of sensitive information and data such as personal information	2
		Encryption program and encryption/decryption key management	2
9	System operation management	Malware Control	5
		Information processing system operation procedure and manual preparation	1
		Information processing system regular maintenance management and patching	1
		Public web server access control	2
		Malware Control	3
Sum			70

3.4 클라우드컴퓨팅 위험분석평가 방법 개발

위험분석평가 방법으로 사용하는 “위험= 자산 × 취약성 × 위협”의 방법을 모든 분야에 같이 적용할 수 있다. 그러나 클라우드컴퓨팅의 환경적 기술적 특성으로 일반적으로 적용되는 위험평가 방식을 사용하는 것보다 클라우드컴퓨팅 환경 내 시스템과 관리 콘솔에 영향을 주는 기밀성, 무결성, 가용성의 특성을 반영하여 위험을 평가하는 방법이 위험에 대응하는 최적화된 방법이 된다.

자산에 대한 중요도를 평가하여 반영하며, 자산의 중요도는 앞서 제시된 클라우드컴퓨팅 가상서버에 대한 자산을 대상으로 상, 중, 하(3 점 적도)를 반영한다. 자산의 중요도는 자산을 책임지고 있는 책임자 또는 관리자가 수행한다.

취약성은 기술적 취약점에 대한 평가 점수와 관리적 취약점에 대한 평가 점수를 반영하여 위험을 산출하는 방법을 적용한다. 자산에 대한 자체적인 취약점 항목에 따라 존재하는 취약점수를 반영하는 것은 기존 온-프레미스의 방식과 동일하나 관리적 취약점 항목에 대한 점수를 반영하게 되면 위험을 더 정확하게 파악할 수 있는 결과를 도출하게 된다. 관리적 취약점을 반영하는 방식은 분야별 항목에 대해서 세부평가 항목 수를 가중한 평균 점수를 사용하여

각각의 자산에 반영하여 위험을 평가한다. 위협은 클라우드컴퓨팅 시스템을 사용함에 따라서 발생하게 되는 일반 위협을 반영하여 위험을 산출하는 방식을 적용한다. 클라우드컴퓨팅 시스템의 위험분석평가 방법의 산출식은 아래와 같이 나타난다.

노출위험값 = (잠재성 위험 값 – (잠재성 위험 값 X 관리평가 값)) X 임의의 값(3)

잠재위험 값은 기술취약점이 가진 위험의 정도를 3 점 척도로 점수 반영한다. 관리평가 값은 관리적 평가 항목에 대한 평균 값으로 0 ~ 1 범위의 값으로 0 점은 취약, 1 점은 양호로 판단한다. 임의의 값은 수용가능한 위험수준을 조정하기 위한 임의의 값으로 3 점을 적용하게 될 경우 최소 수용가능한 위험수준이 3 이 된다.

위험분석을 수행하기 위하여 식별된 자산의 중요도를 상, 중, 하 값으로 3 점 척도로 반영하고, 계산된 노출위험값을 산식에 반영하여 위험도를 산출하는 방식을 아래와 같이 적용하여 위험분석평가를 수행한다.

위험도 = 자산 중요도 + 노출위험값

이러한 방법을 통해서 시스템에 대한 위험분석평가 방법을 적용하면 직관적으로 위험을 관리할 수 있는 효과적인 방법이 된다.

IV. 위험분석평가 타당성 검토

4.1 클라우드컴퓨팅 시스템 자산 식별

이 연구에서 위험분석평가 방법에 대한 타당성을 검증하기 위해 전문가 인터뷰 방법을 실시하였다. 전문가 그룹 인터뷰는 어떤 특정 사항에 대해서, 소수의 그룹을 대상으로 하는 인터뷰 방식이며, 연구자가 진행하여 인터뷰 대상과 함께 토론하는 방식으로 수행되는 연구 방법이다[23].

이 연구는 제안된 위험분석평가 방법의 중요성과 수행 가능성을 검증하기 위하여 리커트 5 점 척도를 기준으로 하여 타당성 검토를 수행하였다. Cabrera et al. (2008) 의 연구에서 중요성과 실행 가능성에 대해서 측정을 수행하여 문제 해결을 위한 우선순위를 부여하는 방식을 사용하였다. 따라서 위험분석평가 방법에 대한 중요성과 실현가능성에 대한 조작적 정의를 하여 중요도와 실행가능성이 전체 2.5 점 이상이면 채택을 하고 두개 항목 모두가 2.5 점 미만인 경우에는 기각하는 방식으로 결과를 도출하였다[24].

Table 6. Metrics for materiality and feasibility
표 6. 중요성과 실현가능성에 대한 측정 지표

Standard	Operational definition	Source
Importance	The degree of importance of the developed method in the security risk assessment method	Ozdemir, Miu(2009), Cabrera et. al. (2008),
Feasibility	The degree of practicability of the proposed risk assessment method	Ozdemir, Miu(2009), Cabrera et. al. (2008),

4.2 전문가 인터뷰 대상자

이 연구에서는 위험분석평가 방법에 관하여 전문가 인터뷰를 위하여, 정보보안 활동 수행 경험 10 년 이상의 경력을 보유하고 있는 3 명의 전문가를 대상으로 구성하였다. 또한, 인터뷰 대상의 참여자는 보안 위험관리에 관하여 실무 경험이 있는 컨설턴트 및 보안담당자로 위험분석평가 방법을 검토할 수 있는 실무 수석급 이상의 직급 담당자로 구성하였다.

Table 7. Expert interviewees
표 7. 전문가 인터뷰 대상자

No.	subject	experience	position	Duty	Participant characteristics
1	Consultant A	more than 10 years	head of department	Security Consulting	Security Risk Management
2	Consultant B	more than 10 years	head of department	Security Consulting	Security Risk Management
3	Security Officer A	more than 10 years	head of department	Security Management	Information Protection Officer

4.3 전문가 인터뷰 절차

이 연구는 위험분석평가에 대한 클라우드컴퓨팅 시스템에 적용할 수 있는 방법을 설명하고 중요성과 실현 가능성에 대한 평가를 위해 1 회 인터뷰를 진행하였다. 전문가 그룹 인터뷰에서 클라우드컴퓨팅 시스템의 특성에 대한 선행연구를 통해 위험평가 수행 시 이슈가 되는 부분을 설명하고 온-프레미스 환경에서의 자산식별과 클라우드컴퓨팅 환경에서의 자산식별 그리고 취약점에 대한 다양한 사항을 검토하고 개발된 위험분석평가 방법에 관해서 토론을 진행하였다. 전문가 그룹 인터뷰에 참여자는 위험분석평가에 대한 방법을 직관적으로 인식하고 실무적으로 적용할 수 있고 활용성이 높은 방안에 대해 심층 토론하고 검토된 보안 위험분석평가 방법에 대한 중요성과 실현가능성에 대해서 리커트(Likert) 5 점 척도로 평가를 수행하였다.

4.4 타당성 검토 결과

4.4.1 전문가 그룹 인터뷰 결과

보안 위험분석평가 방법에 대한 전문가 그룹 인터뷰 결과, 공통으로 위험분석평가에 고려해야 하는 측정 요소와 클라우드컴퓨팅 시스템에 관한 선행연구에서 분석 내용에 관련한 문제점을 크게 벗어나지 않았다. 클라우드컴퓨팅 시스템의 위험분석평가 경우 기존 선행연구와 마찬가지로 자산을 식별하는 어려움과 취약점 항목에 대한 다른 방식의 적용에 대해서 같은 특징을 파악할 수 있었다.

측정 내용에 대한 지표의 척도를 '매우 그렇다, 그렇다, 보통이다, 그렇지 않다, 매우 그렇지 않다.' 방식으로 1 점에서 5 점까지의 리커트 척도로 하여 검토를 수행하였다. 이는 각 평가 항목의 점수가 높을수록 위험분석평가 방식에 대해 합리적 견해를 제시하는 유형을 나타낸다.

보안 컨설턴트 인터뷰 그룹의 참여자는 모두 중요성과 실현가능성에 4 점 이상으로 평가를 하였고, 보안 담당자만 중요성에서 중립적 평가를 제시하였다. 중요성 측면의 평가 점수 평균을 보면 3.7 로 실현가능성보다 상대적으로 낮게 나타났다. 이는 위험분석평가 방법이 새로운 방식으로 제시되었으나 위험을 측정하는 다양한 방식이 있어 상대적으로 중요성이 떨어지는 것으로 나타났다고 볼 수 있다.

Table 8. Risk analysis evaluation feasibility review result
표 8. 위험분석평가 타당성 검토 결과

	Importance	Feasibility	Average
Consultant A	4	5	4.5
Consultant B	4	5	4.5
Security Officer A	3	4	3.5
Average	3.7	4.7	4.2

4.4.2 전문가 그룹 결과 분석 및 시서점

앞서 전문가 그룹 인터뷰를 하여 도출된 위험분석평가 방법에 대해서 타당성을 결과 전체 평균 점수가 4.2 로 수용에 타당한 것으로 검토되었다. 그러나 보안담당자와 컨설턴트가 평가한

점수에 1 점의 평균 점수 차이가 벌어진 점에서 위험분석평가 자체에 대한 필요성에 대해서 다른 견해를 가진 것으로 볼 수 있다. 보안담당자는 조직의 보안을 위해서 위험분석평가 업무의 수행 비중을 낮게 보고 있는 것으로 보인다.

현재 클라우드컴퓨팅 환경의 위험분석평가에 관한 연구가 미흡하고 부족한 실정이다. 따라서 해당 분야에서 10 년 이상 근무한 전문가들로 구성된 전문가 그룹 인터뷰를 통해 위험평가에 대한 새로운 방법의 타당성을 검토하였다. 중요성과 실행가능성에 대한 기준을 검토한 결과 위험분석평가 방법은 모두 타당성이 검증되어 의미가 있으며, 실무 수행이 가능하다는 결론을 도출하였다.

V. 결론

5.1 연구 요약 및 결론

클라우드컴퓨팅 서비스의 주요 특징인 탄력적 시스템의 확장과 가용성 확보 등에 대한 기술 특징과 관련하여 위험분석평가의 효과적인 방법에 대한 연구를 진행하였다.

이 연구에서는 기업의 비즈니스를 반영한 전사 위험관리의 계획 수립과 수용 가능한 위험수준을 설정하는 데 효과적인 평가 방법이 될 수 있는 산식을 도출하였다. 4 차 산업혁명으로 디지털 트랜스포메이션이 되어 나아 감에 따라 클라우드컴퓨팅의 확산은 더욱 가속화될 것이며, 이에 따라 다양한 위험이 지속해서 증가할 것으로 예상된다. 따라서 조직은 기존 IT 자산기반의 보안 위험관리에서 벗어나 다양한 환경의 위험관리 접근방식을 수용할 필요가 있다.

이 연구는 선행연구에서 다루지 못한 클라우드 환경에서의 위험분석 평가의 효과적인 방법에 관한 연구를 제시한 것이 이전의 이전 연구와 차별점이 될 것이다. 위험분석에 관한 연구는 다수 진행이 되었으나 클라우드 환경의 특수성을 고려한 연구는 진행이 되지 않아 학술적 의의를 가진다. 또한, 이연구는 향후 위험분석에 관하여 더 깊이 있는 연구가 지속될 수 있는 단초를 제공한 의의를 있을 것이다.

기업에게는 클라우드컴퓨팅 시스템 환경에서 효과적인 위험평가를 수행할 수 있는 방법론을 제시함으로써 실무자들에게 다양한 위험평가를 수행할 방안을 제시하는 데 공헌 점을 들 수 있다. 또한 이 연구의 결과는 클라우드컴퓨팅 시스템의 정보보호 강화 요인뿐만 아니라 클라우드컴퓨팅 시스템 도입 촉진을 이루는 데 장해가 되는 위험 요인을 제거하는 데 공헌하게 될 것이다[5, 9].

5.2 연구의 한계 및 향후 제안

이 연구의 한계점으로 다음과 같이 사항을 제시할 수 있다. 첫째, 이 연구는 클라우드컴퓨팅 시스템의 위험분석평가에 대한 깊이 있는 연구가 수행된 사례가 없어서 소수의 전문가만을 대상으로 인터뷰하여 타당성을 측정하였기 때문에 일반화에 대한 어려움이 존재한다. 그러므로, 추후 여러 평가 방식의 요소 등에 관하여 정략적으로 연구를 수행하는 것이 필요하다. 둘째, 제안된 위험분석평가 항목은 관리적 관점에서 제시되어 기술적인 요소들에 대한 세부적인 추가 연구가 필요하다. 셋째는 제시된 위험분석평가 방법에 관한 실증적인 연구가 더 필요하다. 제안된 위험분석평가 방법을 더 세분화하여 구체적으로 수행할 수 있는 위험평가 방법에 관한 체계의 실증연구가 진행될 필요가 있다.

기업의 위험을 효과적으로 관리하기 위해서 실효성 있고 효과적인 위험관리가 수행될 경우, 기업의 목적인 이익창출을 더 효과적으로 얻을 수 있으며, 또한 기업의 신뢰도가 높아질 수 있다. 이 연구의 결과는 위험관리 활동의 기본적인 사항이지만 실질적으로 기업에서 제대로 수행하지 못하고 있는 위험분석평가에 대한 보안관리 활동의 중요성을 인식하는 데 중요한 시사점을 제시할 것으로 기대한다.

VI. 참고문헌

[1] Eunjoo Kim. “Public sector cloud application examples and performance analysis”. Journal of Korean Communication Sciences (Information and Communication), 36 (2), 23-27. 2019.

[2] Thomas Erl, Zaigham Mahmood and Ricardo Puttini, “Cloud Computing: Concepts, Technology & Architecture”

[3] Dongho Kim, Junghoon Lee, and Yangpyo Park, "A Study on the Factors of Cloud Computing Characteristics Influencing Enterprise's Intention to Adopt Cloud Computing Services," The Jounal of Society for e-Business Studies, vol. 17, no. 1, pp. 111-136, 2012.

[4] S. Kim and H. Park, "The Relationship between Vender Dependency and Expected Benefits of Cloud Computing: The Moderating Effects of Vendor Trust and Organizational Supports," korean management review, vol. 47, no. 5, pp. 1021-1047, 2018, doi: 10.17287/kmr. 2018. 47.5.1021.

[5] Saeha Jeon, Narae Park, and Jung Jung Lee, "Study on the Factors Affecting the Intention to Adopt Public Cloud Computing Service," Entrue Journal of Information Technology, vol. 10, no. 2, pp. 97-112, 2011.

[6] Woojin Jeon and Kiwoong Park, "Container-friendly File System Event Detection System for PaaS Cloud Computing," The Korea Next Generation Computing Society, vol. 15, no. 1, pp. 86-98, 2019.

[7] Ilhoon Jung, Junghun Oh, Jungheum Park, and Sangjin Lee, "A Digital Forensic Study on IaaS Type Cloud Computing Services," Journal of the Korea Institute of Information Security & Cryptology, vol. 21, no. 9, pp. 55-65, 2011.

[8] Sangyong Choi and Kimoon Jung, "Security Architecture for a Secure Cloud Computing Environment," Journal of the Korea Society of Computer and Information, vol. 23, no. 12, pp. 81-87, 2018, doi: 10.9708/jksci. 2018.23.12.081.

[9] Roh Hyun-suk, “A Study on the Concept of Moving Personal Information Overseas in Cloud Service” Ancient Law No. 79 2015.

[10] Changjae Lee, “A Study on the Risk Assessment Plan for Persons Handling Personal Information,” Dongguk University Master's Thesis, 2016.

[11] Lee Myung-ryul, “A Study on Information Security Risk Analysis Method Reflecting Information Security Governance and External Threats” Master's Thesis, Soongsil University, 2017.

[12] Lee Cheong-hee, “Information Flow-Based Risk Analysis Methodology _ Focusing on Photomask Process Flow” Master's Thesis, Kyungwon University, 2009.

[13] http://www.ahnlab.com

[14] https://www.hangrp.com/consulting/consulting_03_01.php

[15] http://www.kaits.or.kr/sub/?p=sub14

[16] https://cve.mitre.org/cve/update_cve_records.html

[17] http://www.zinion.co.kr/index.php?mid=service04

[18] http://cwe.mitre.org,

[19] https://nvd.nist.gov/vuln-metrics/cvss

[20] https://owasp.org/

[21] http://aws,amazon.com/ko/agreement/, Security Handoff Point

[22] Shin Kyung-ah and Lee Sang-jin, "Information Security Management System for Cloud Computing Services," Journal of the Korea Institute of Information Security & Cryptology 21(6), vol. 22, no. 1, pp. 155-167, 2012.

[23] Morgan, D. L. (1996). Focus groups as qualitative research (Vol. 16). Sage publications.

[24] Cabrera, D., Mandel, J. T., Andras, J. P., & Nydam, M. L. (2008). What is the crisis? Defining and prioritizing the world's most pressing problems. Frontiers in Ecology and the Environment, 6(9), 469-475.

저자 소개

이정림(*Junglim Lee*)

2021 년 6 월 중앙대학교 대학원 융합보안학과 석사과정

관심분야 : 클라우드, 정보보호, 산업보안

장항배(*Hangbae Jang*)

2006 년 연세대학교 대학원 정보시스템관리 박사
2014 년 ~ 현재 중앙대학교 산업보안학과 교수

관심분야 : 산업보안, 기업보안, 인수합병, 정보유출