http://dx.doi.org/10.14400/JDC.2015.13.8.43

국내 클라우드 보안 인증스킴 개발에 관한 연구

정진우*, 김정덕**, 송명균*, 진철구*
중앙대학교 융합보안학과 박사과정*, 중앙대학교 산업보안학과 교수**

A study on Development of Certification Schemes for Cloud Security

Jin-Woo Jung*, Jungduk Kim, Myeong-Gyun Song*, Chul-Gu Jin***
Dept. of Convergence Security, The Graduate School of Chung-Ang Univ.*
Dept. of Industrial Security, The College of Business & Economics of Chung-Ang Univ.**

요 약 대표적인 융복합 ICT 서비스라고 할 수 있는 클라우드 컴퓨팅 서비스에 대한 법안이 2015년 3월에 통과되면서 많은 업체나 기관에서 다시금 클라우드 서비스 도입을 고려하고 있으나 보안에 대한 염려 때문에 서비스 도입을 주저하고 있다. 이러한 문제를 해결하기 위해서는 클라우드 서비스 보안에 대한 객관적이고 공정한 평가와 인증을 수행할 수 있는 클라우드 보안 인증체계의 도입이 요구된다. 현재 클라우드 보안 인증체계에 관한 연구가 활발히 진행되고 있지만 인증스킴에 대한 연구는 미흡하다. 따라서 본 연구는 국외 클라우드 보안 인증체계와 클라우드 서비스 제공자에 대한 평가 제도를 분석하여 국내 클라우드 보안 인증 도입시 고려되어야 할 요소들을 분석하였다. 이를 기반으로 국내 실정에 맞는 3가지 인증스킴을 제시하였고, 포커스 그룹 인터뷰를 통하여 인증스킴별 장단점을 도출하여 상황에 적절한 인증스킴을 제시하였다.

주제어 : 융복합 클라우드 서비스, 클라우드 보안 인증체계, 클라우드 보안 인증스킴, 포커스 그룹 인터뷰, 클라우드 보안 정책

Abstract As the cloud computing law was passed in March, 2015, many private companies and public organizations give consideration to introduce cloud computing services. However, most of them are still concerned about the security issues in cloud computing services. To solve the problem, a certification system of cloud security is necessary as an enabler for adoption of the trusted cloud services. There have been a number of studies about certification systems for cloud security, but only few studies exist about certification scheme of cloud security. Therefore, in this study, foreign certification systems for cloud security are analyzed to draw requirements for developing a domestic certification scheme for cloud security. Based on the result of analysis, this study proposes the three certification schemes of cloud security, which have been reviewed by the focus group interview method to draw advantages and disadvantages of each scheme.

Key Words : convergence cloud service, cloud security certification system, cloud security scheme, focus group interview, cloud security policy

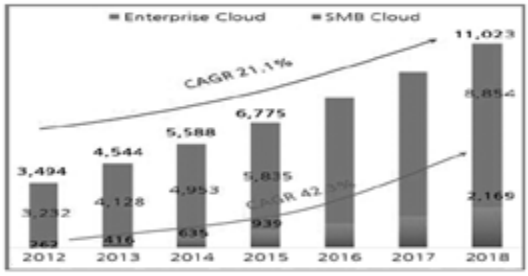
* "본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-H8501-15-1018)
Received 7 June 2015, Revised 17 July 2015
Accepted 20 August 2015
Corresponding Author: Jungduk Kim(Chung-Ang University)
Email: jdkimsac@cau.ac.kr

ISSN: 1738-1916

1. 서론

빅데이터, 사물인터넷(IoT) 등 융복합 ICT 기술의 출현은 클라우드 컴퓨팅을 기반으로 운영되고 있으므로 클라우드 컴퓨팅의 중요성이 점증하고 있다. 이는 클라우드 컴퓨팅이 더 이상 하나의 신 기술이 아닌 융복합 ICT 기술의 핵심 요소가 되어가고 있음을 의미한다. 현재 국내에는 네이버, 다음, 더존 비즈온 등 민간기업 중심의 클라우드 서비스가 제공이 되고 있으며, KRG의 2015년 IT 시장백서에 따르면, 국내 클라우드 컴퓨팅 시장규모는 2014년, 전년대비 23% 성장한 5,558억 원의 시장규모를 형성하였으며, 2015년에는 21% 성장한 6,775억 원 규모가 될 것으로 예상하고 있다. ([Fig. 1] 참조)[1]. 클라우드 컴퓨팅은 고효율, 저비용, 관리의 전문성, 접근성, 등의 장점으로 유럽, 미국 등 세계 여라 국가에서는 이미 오래 전부터 관심을 갖고 노력을 기울이고 있는 분야이다. 한국도 이러한 변화의 흐름에 합류하기 위해 “클라우드 발전 및 이용자 보호에 관한 법률”(이하 ”클라우드 컴퓨팅 발전법“이라 한다.)을 2015년 3월 27일 법률 제13234호로 제정하여 2015년 9월 28일 시행을 앞두고 있으며 클라우드컴퓨팅 발전 기반의 조성, 클라우드컴퓨팅 서비스의 이용 촉진, 클라우드컴퓨팅 서비스의 신뢰성 향상 및 이용자 보호 등 총 37개의 조문으로 제정되어있다[2]. 이처럼 국가 차원에서 법을 제정하여 클라우드를 활성화 시키고 시장규모를 키우는데 힘쓰고 있지만 가상화 취약점, 정보위탁에 따른 정보유출 위협, 다양한 단말로부터의 접속으로 인한 정보유출 위협 등 클라우드 보안에 대한 신뢰도가 부족하기 때문에 아직도 많은 기업이나 기관들은 클라우드 서비스의 이용을 꺼려하고 있다[3]. 이러한 특징으로 인해 클라우드는 기존의 IT환경에 비해 더 높은 수준의 보안 프로세스가 요구되고 있고 이를 위한 초석으로 국내 환경에 적합한 클라우드 보안 인증체계의 도입은 시급한 문제이다.

본 연구는 미국의 FedRAMP(Federal Risk and Authorization Management Program), 영국의 G-Cloud 그리고 CSA(Cloud Security Alliance)의 OCF(Open Certification Framework)등 국외 클라우드 보안 인증체계를 분석하였고, AICPA/CICA Trust Services Examination, ENISA의 클라우드 컴퓨팅 보안 보증 프레임워크 등의 클라우드 서비스 제공자를 대상으로 하는 평가 제도를 분석하였다. 이를 기반으로 국내 클라우드 보안 인증체계 도입시 필요한 요구사항을 도출하였고, 조직구조에 일반적 이용되는 3가지 속성(분권형, 중앙집중형, 하이브리드형)을 기반으로 클라우드 보안 인증스킴을 제안하였다[4]. 제안된 3가지 인증스킴은 포커스 그룹 인터뷰를 통해 각각의 장단점을 도출하였다.



[Fig. 1] A market trend of cloud computing

2. 관련 연구

2.1 미국의 FedRAMP 인증체계

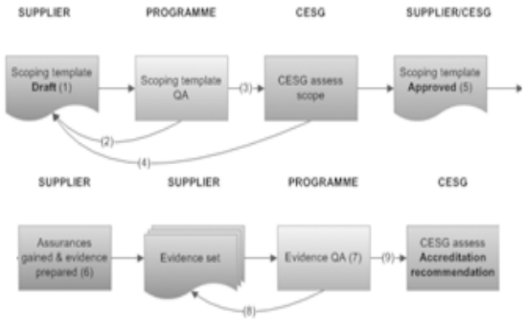
FedRAMP(Federation Risk & Authorization Management Program)는 미국 정부기관 공통의 클라우드 서비스·제품 인증심사 제도로 각각의 연방기관 간 중복을 최소화하기 위해 클라우드 제품 및 서비스를 위한 대한 보안성 인증심사를 통합적으로 수행하는 제도이다. General Services Administration(행정 관리청)은 클라우드 서비스·제품 보안성 인증심사 방식을 표준화하여 전체 미국 정부기관이 클라우드 서비스·제품 도입 시 공통적으로 적용할 수 있는 FedRAMP을 시행함으로써 개발업체의 인증심사 중복신청을 피하고 이로 인해 비용절감 효과를 가져 올 것이며 궁극적으로 미국 정부기관의 클라우드 서비스 및 제품 도입을 가속화시킬 것으로 기대되고 있다. FedRAMP의 인증체계는 3PAO인가, 임시인증 활용으로 구분되며 지속적인 모니터링 역량에 대한 평가도 포함되고 있다[6].

2.2 영국 G-Cloud 서비스 보안 인증체계

영국 정부가 운영하는 보안 인증제도인 G-Cloud는 클라우드 기반의 IT 서비스를 공공기관에 조달할 수 있

는 방법으로 제안되었으며, CloudStore라는 웹 서비스를 통해 2013년 기준으로 약 7,000 개 이상의 제공자가 서비스를 제공하고 있다. 또한 G-Cloud 시스템이 일부기관의 50%이상의 비용절감을 이루어 냈다고 설명하였다[15]. CloudStore의 서비스는 영국 통신 보안그룹의 범정부인가서비스(Pan Government Accreditation Service)에 의해 정보보안에 관련 항목을 포함하여 공공기관의 업무영향수준(BIL; Business Impact Level)에 적합한지 인가를 받을 수 있다[7,9].

G-Cloud의 인가는 서비스의 무결성 기밀성 측면의 업무 영향수준에 따라 3 BIL 수준으로 구분된다. 전체적인 G-Cloud 인가 프로세스는 다음과 같다.



[Fig. 2] Processes of G-Cloud

2.3 CSA의 STAR 인증체계

CSA(Cloud Security Alliance)의 OCF(Open Certification Framework)는 비영리단체인 CSA에서 제정한 클라우드 보안 통제 프레임워크이며, CSA의 보안 지침과 통제 목적에 따라 유연성 있고 점진적인 다중 계층 클라우드 제공자 인증을 위한 프로그램을 제공하며, 중복되는 시간과 비용을 피하기 위해 공인회계 분야에서 개발한 제3자 평가 및 증명서를 결합하였다. OCF는 3 단계의 신뢰를 기반으로 [Fig. 3]와 같이 구성되어 있다. 각 단계는 클라우드 소비자에게 높은 수준의 보장을 제공하며, 클라우드 서비스 제공자의 운영에 대한 가시성과 투명성에 대한 수준을 제공한다[8].

[fig. 3] Processes of OCF

2.4 클라우드 서비스 제공자에 대한 평가제도

현재 클라우드 서비스 제공자에 대한 대표적인 평가제도로는 AICPA/CICA Trust Services, ENISA 클라우드 컴퓨팅 보안 보증 프레임워크, Jericho Forum 자가진단 등이 있다. 먼저 AICPA/CICA는 미국 회계감사 표준을 기반으로 하는 독립적인 제3자 조사기관이며 2011년부터 시작되었다. 제공되는 클라우드 서비스의 시스템에 대한 통제가 보안성, 프라이버시, 기밀성, 무결성, 가용성을 만족하는지를 평가한다[14]. ENISA의 클라우드 컴퓨팅 보안 보증 프레임워크는 클라우드 위험관리를 기반으로 역할 정의, 운영 보안, 공급망 보장, 자산관리 등의 세부적인 지침을 제공한다[13]. Jericho Forum 자가진단은 서비스 벤더가 제공할 클라우드 서비스에 대한 자가진단에 중점을 둔 보안 프레임워크이다[9].

2.5 국내 클라우드 서비스 인증체계

앞서 설명한 것과 같이 국외에는 다양한 클라우드 서비스 보안 인증제도가 존재한다. 하지만 국내의 클라우드 인증제도는 한국 클라우드 서비스협회(KSCA)에서 제공하는 서비스 인증이 유일하며, 보안과 관련된 항목이 일부 포함되어 있다. 인증은 서비스, 정보보호, 품질의 대분류로 구분되며 확장성, 성능, 보안, 서비스 지속성, 서비스 지원, 가용성, 데이터관리 등 7개 영역과 105개의 세부 통제로 구성되어있다. 그리고 필수항목을 포함하여 70% 이상을 통과할 경우 인증을 받을 수 있다. 반면, 105개의 세부 통제항목 중 보안분야는 22개의 항목이 존재하며, 10개의 필수항목을 만족해야 한다. 하지만 이러한 항목들은 클라우드 서비스 보안의 가장 중요한 이슈 중 하나인 개인정보보호에 대한 어떠한 항목도 없는 등 국외의 클라우드 서비스 보안 인증제와 비교하였을 때 부족한 수준이라고 할 수 있다[16]. 따라서 국내의 안전한 클라우드 서비스 제공을 위한 보안 요구사항을 식별하고

이를 지속적으로 운영하기 위한 인증 스킴에 대한 연구가 필요하다.

3. 클라우드 보안 인증스킴 개발

3.1 클라우드 보안 인증체계 요구사항

일반적으로 인증체계는 다음과 같이 정의 한다. ISO/IEC 17000:2004에서 정의한 인증이란 적합성 평가를 지원하기위한 활동이며, 적합성 평가란 제품, 서비스, 프로세스, 시스템 및 조직의 구조가 요구사항(법, 표준)을 충족하는지 평가하는 것이다[11]. NIST SP 800-37에서 정의된 인증은 관리, 운영, 기술 보안의 관점에서 정보시스템을 평가하여 통제가 의도한대로 정확하게 구현되는지 여부를 판단하여 보안 인가를 지원하는 활동이며, 인가는 허용된 보안 통제 집합의 구현을 기반으로 정보시스템의 운영을 승인하고 조직의 운영, 자산, 개인에 대한 위험을 수용하기 위한 경영진의 활동을 의미한다[5]. 일반적인 인증체계와 마찬가지로 클라우드 보안 인증체계는 인증, 인정과정이 모두 포함되어야 하며, 모든 분야에 적용할 수 있어야한다.

일반적으로 인증 프로세스는 제공하는 제품 혹은 서비스가 일정 수준의 위험관리 기준을 만족하고 있음을 보장하는 인증(Certification)과 고객이 인증된 서비스를 사용하도록 허용하는 인가(Accreditation) 단계로 구분할 수 있다.

3.2 클라우드 보안 인증스킴 요소

국외 클라우드 보안 인증체제와 클라우드 서비스 제공자를 위한 평가 체계를 분석한 결과, 국내 환경에 적합한 클라우드 인증스킴 개발을 위해서 고려되어야 할 구성요소는 다음과 같다.

- 서비스 적용 대상에 대한 정의 (공공기관, 민간기관 혹은 모두 포함)
- 평가 대상에 대한 정의 (클라우드 서비스 제공자, 서비스 자체, 서비스 사용자)
- 평가 수행 주체 (인증기관, 별도의 평가기관)
- 감독 기관(인정기관)의 정의 (제공자 관점의 정부부처{예: 미래창조과학부}, 사용자 관점의 정부부처{예: 안전행정부})
- 인증 기관의 정의 (공공기관, 민간 인증기관)
- 인가 기관의 정의 (하나의 기관이 모두 수행, 부처별로 수행, 고객이 자체적으로 수행)
- 보증수준 인증 정의 (Pass/Fail, 성숙도 기반의 등급제, 업무 위험도 기반의 등급제)
- 이 밖에도 FedRAMP, G-Cloud등 국외 클라우드 보안 인증 결과의 인정여부, 인증제도의 지속 가능성, 사후 모니터링 체계의 구축, 등이 추가적으로 고려되어야 함

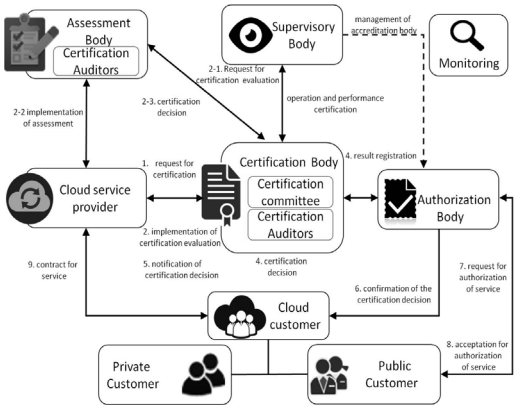
3.3 클라우드 보안 인증스킴

본 연구는 클라우드 보안 인증스킴 개발을 위하여 조직 내 의사결정 구조의 일반적 속성인 분권형, 중앙 집중형. 하이브리드형의 3가지 인증스킴을 제안하였다[4].

인증스킴은 평가기관, 감독기관, 인증기관, 인가기관 클라우드 서비스 제공자, 클라우드 서비스 이용 고객으로 구성되어 있으며 고객은 정부기관, 공기업 등의 공공기관과 대기업 및 중소기업으로 구성된 민간기업 및 개인고객으로 구성되어있다.

3.3.1 분권형 인증스킴

분권형 인증스킴은 공공기관 고객의 부처별로 인가기관을 지정하고, 인가기관에 인증심사 결과 및 인가 현황을 등록하고 조회하며, 고객 기관의 특성에 따른 추가적인 심사는 불가능하다. 분권형 인증스킴의 인증절차는 다음과 같다.



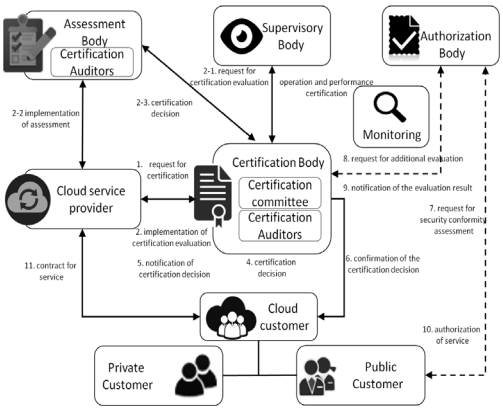
[Fig .4] Decentralized certification scheme

클라우드 서비스 제공자는 인증기관에 인증을 신청한다. 인증기관은 평가기관에 이에 대한 인증심사를 요청하며 인증기관은 인가기관에 심사 결과를 등록한다. 고객은 인가기관을 통하여 인증심사 결과를 조회할 수 있으며 공공 고객에 대한 서비스 사용 업무 또한 인가기관에서 담당한다.

3.3.2 중앙 집중형 인증스킴

중앙 집중형 인증스킴은 공공기관 고객에 대한 통합 인가기관을 지정하고, 인증기관에 인증심사 결과 및 인가 현황을 등록하고 조회하며, 필요에 따라 인증기관이 추가적인 심사가 가능하다. 중앙 집중형 인증스킴의 인증절차는 다음과 같다.

클라우드 서비스 제공자는 인증기관에 인증을 신청한다. 인증기관은 평가기관을 통하여 인증심사를 진행하며 클라우드 고객은 인증심사 결과를 인증기관으로부터 조회할 수 있으며 인가기관은 공공고객을 대상으로 서비스 사용 업무를 담당한다.

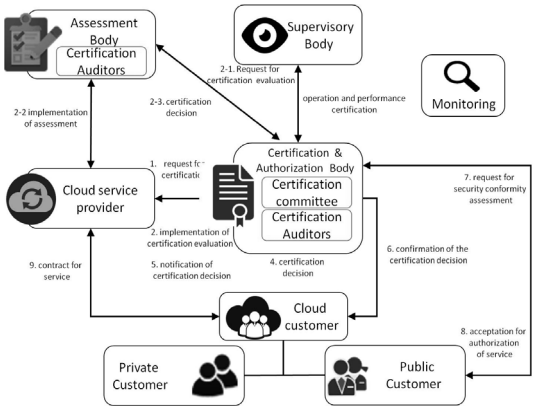


[Fig. 5] Centralized certification scheme

3.3.3 하이브리드형 인증스킴

하이브리드형 인증스킴은 인증기관이 인가기관의 역할까지 수행하며, 인증기관에 인증심사 결과 및 인가 현황을 등록하고 조회하며, 고객의 요청에 따라 인증기관의 추가적인 심사가 가능하다. 하이브리드형 인증스킴의 인증절차는 다음과 같다.

클라우드 제공자는 인가기관의 역할을 포함한 인증기관에 인정을 신청한다. 인증기관은 평가기관을 통하여 인증심사를 진행하며 클라우드 고객은 인증심사 결과를 인증기관으로부터 조회할 수 있다. 또한 공공고객은 보안 적합성 심사, 서비스 사용 인가 업무 또한 인증기관에서 담당한다.



[Fig. 6] Hybrid certification scheme

4. 연구 분석 및 결과

4.1 분석 방법

본 연구에서는 국내 환경에 적합한 클라우드 보안 인증체계 도입을 위해 3가지 인증스킴(중앙 집중형, 분권형, 하이브리드형)을 제시하였고 제시된 인증스킴의 실효성 평가를 위해 포커스 그룹 인터뷰 방식을 채택하였다. 그 이유로는 현재 국내 클라우드 보안 인증체계가 존재하지 않는 상황이기 때문에 정확한 비교 사례를 찾는 것이 어렵고, 클라우드 보안 인증의 통제 항목을 제시하는 연구는 많지만 이처럼 인증스킴을 제시하는 연구는 미비하기 때문이다. 포커스 그룹 인터뷰는 집단 간의 시각 차이를 파악할 때, 의견, 행동, 동기에 영향을 미치는 요인들을 조사할 때, 아이디어, 계획 또는 정책을 미리 시험해보고자 할 때 사용하기 때문에 본 연구에 적합한 방법이라고 사려 된다[12]. 본 연구에서는 진행된 포커스 그룹 인터뷰(2015. 3)에는 국내 클라우드 업체 이사, 정보보호 평가 및 인증 심사원, 대학 교수 등 8명의 자문 위원단을 구성하여 각 인증스킴별 장단점을 도출에 중점을 두고 토론을 진행하였다.

4.2 연구 결과

포커스 그룹 인터뷰를 통하여 전문가들의 의견을 수렴하였고, 각 인증스킴의 장단점과 실현가능성에 대하여 토론하였다. 대부분의 전문가들은 기업이나 기관에 특성에 맞게 3가지 인증스킴 모두 사용가능 할 것이라고 판단하였고, 아직 클라우드 보안인증 체계가 수립되지 않은 상황에 적절한 논제라고 대답하였다. 포커스 그룹 인터뷰를 통한 각 인증스킴의 장단점은 아래와 같다.

분권형 인증스킴은 개별 공공기관 고객의 보안 전문성이 요구되지 않으며 인가 업무의 분산 및 부처별 인가 조건의 설정이 가능하다. 또한 인증기관의 업무 부하를 절감할 수 있는 장점을 가지고 있다. 반면 부처별 인가 조건이 상이한 경우 제공자의 부담이 가중되고, 타 부처 고객의 인가에 필요한 정보의 공유가 어렵고 인가기관의 활동에 대한 추가적인 관리가 필요하다는 단점이 존재한다는 의견이 제시되었다.

중앙 집중형 인증스킴은 개별 공공기관 고객의 보안 전문성이 요구되지 않으며 일관된 인가 조건을 수립하고 고객 간 정보 공유에 효율적이고, 추가 심사를 통해 고객에 특화된 보안 요구사항의 반영이 가능하다는 장점이 제시되었다. 반면에, 인증기관 및 인가기관의 업무 부담과 책임성이 가중되며, 부처별 특성에 맞는 인가 조건이 설정이 어렵고, 인가기관과 인증기관 간의 신뢰도 유지가 어렵다는 의견이 단점으로 제시되었다.

하이브리드형 인증스킴은 일관된 인가 조건을 수립하고 고객 간 정보 공유에 효율적이며, 추가적인 심사를 통해 고객에 특화된 보안 요구사항의 반영이 가능하다. 또한 공공기관 고객에 대한 독립적인 평가체계의 유지가 가능하다는 장점이 제시되었다. 반면에 인증·인가기관의 업무 부담과 책임성이 가중되며, 부처별 특성에 맞는 인가 조건의 설정과 개별 고객의 보안 전문성 확보가 어렵다는 단점이 존재한다는 의견이 제시되었다.

포커스 그룹 인터뷰에 참여한 전문가들은 중앙 집중형과 하이브리드형 인증스킴이 공공기관에 적합하다고 판단하였고 민간기업은 기업 규모에 따라 분권형 혹은 하이브리드형 인증스킴을 수정해서 적용할 것을 권장하였다. 하지만 실직적인 선택은 기업 또는 기관의 클라우드 전문가들의 역할이라고 하였으며 그들이 속한 기업이나 기관의 특성에 맞는 보안 인증스킴을 선택해야 한다는 의견이 제시되었다.

5. 결론 및 향후 연구 과제

본 연구는 국외 클라우드 보안 인증제도와 클라우드 서비스 제공자 인증 평가를 분석하여 국내 클라우드 보안 인증체계 도입 시 고려되어야 할 사항을 식별하였다. 이를 통해 국내 환경에 적합한 클라우드 보안 인증체계를 위한 3가지 인증스킴을 개발하였고, 각 스킴은 포커스 그룹 인터뷰 방식을 통하여 장단점을 도출하였다. 클라우드 발전법의 통과로 공공기관 및 민간기업의 클라우드 서비스 도입이 구체화, 가속화 되고 있는 이 시점에 본 연구는 다음과 같은 의의를 갖는다.

첫째, 향후 실제 인증제도가 도입 될 시 본 연구에서 제안한 인증스킴을 참조하여 효율적인 인증체계 구축에 도움이 될 것으로 사려 된다. 둘째, 본 연구의 결과인 3가지 인증스킴은 상황별 적절한 인증스킴을 선택할 수 있는 기준이 될 수 있다.

하지만 본 연구는 국내 클라우드 전문가를 대상으로 인증스킴에 대한 장 단점 그리고 실현 가능성을 검토하였으나, 연구결과를 일반화가 어렵다는 한계가 있다. 따라서 향후 연구에서는 본 연구에서 제시한 클라우드 인증스킴에 따른 시범사업을 통해 개별 스킴의 실제 적용상의 문제점을 미리 파악할 필요가 있다.

ACKNOWLEDGMENTS

"This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2015-H8501-15-1018) supervised by the IITP(Institute for Information & communications Technology Promotion)"

REFERENCES

[1] DOI: http://blog.lgcns.com/770, April 28.
[2] M. S. Jung, Study on the main content of cloud computing Development Act, Korea Entertainment Industry Association, Vol. 5, pp. 163-167, 2015.

[3] K. C. Kim, O. Heo, S. J. Kim, A Security Evaluation Criteria for Korean Cloud Computing Service, Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 2, pp 251-265, 2013.
[4] C. V. Brown, S. L. Magill, Alignment of the IS functions with the enterprise: toward a model of antecedents, Journal of MIS Quarterly, Vol. 18, No. 4, pp 371-403, 1994.
[5] NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information System, 2010.
[6] S. J. Jang, The Analysis of FedRAMP, Weekly Technology Trend, 2013.
[7] Y. H. Park, Korean cloud certification system through foreign case of analysis and suggestions, Master's dissertation in Sejong Cyber University, 2015.
[8] J. Y. Choi, E. J. Choi, M. J. Kim, A Comparison Study between Cloud Service Assessment Programs and ISO/IEC 27001:2013, Journal of Digital Convergence, Vol. 12, No. 1, pp 405-414, 2013.
[9] Korean Standards Association, R&D Road map based on Standard, 2014.
[10] CSA: Open Certification Framework rev1, 2013.
[11] ISO/IEC 17000 : 2004: Conformity assessment - vocabulary and general principles, 2004.
[12] R. A. Krueger, M. A. Casey, Focus Groups: A practical guide for applied research 4th edition, sega publication(CA), London, 2008.
[13] ENISA: Cloud computing information assurance framework, 2010.
[14] ISACA: IT control objectives for could computing, 2011.
[15] KISA: Public data system restructuring in the UK government, 2014
[16] G. S. Lee, Strengthening Security on the Internal Cloud Service Certification, Journal of The Korea Institute of Information Security & Cryptology, Vol. 23, No. 6, pp,1231-1238, 2013

정 진 우(Jung, Jin Woo)

- 2009년 2월 : 광운대학교 소프트웨어학과(학사)
- 2014년 9월 : RHUL Univ. of London, 정보보호(석사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과(박사과정)
- 관심분야 : 개인정보보호, 클라우드 보안, 사회공학, 휴먼해킹
- E-Mail : zinuojung@gmail.com

김 정 덕(Kim, Jungduk)

- 1979년 2월 : 연세대학교 정치외교학과(학사)
- 1981년 8월 : 연세대학교 경제학과 대학원(석사)
- 1986년 8월 : Univ. of S. Carolina, MBA
- 1990년 12월 : Texas A&M Unv., Ph. D. in MIS
- 1995년 3월 ~ 현재 : 중앙대학교 산업보안학과 교수
- 관심분야 : 정보보호 거버넌스, 정보보호 관리, 디지털 비즈니스 보안
- E-Mail : jdkimsac@cau.ac.kr

송 명 균(Song Myeong Gyun)

- 2009년 2월 : 중앙대학교 정보시스템학과(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과(석사과정)
- 관심분야 : 개인정보보호, 보안문화, 정보보호 거버넌스
- E-Mail : a50692911@gmail.com

진 철 구(Jin Chul Gu)

- 2009년 2월 : 중앙대학교 정보시스템학과(학사)
- 2015년 3월 ~ 현재 : 중앙대학교 융합보안학과(석사과정)
- 관심분야 : 개인정보보호, 클라우드 보안, 정보보호 거버넌스
- E-Mail : raminez69@gmail.com