Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.23, NO.6, Dec. 2013 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2013.23.6.1231

국내 클라우드서비스 인증에서 보안 강화방안 연구

이 강 신[†‡]
김·장 법률사무소

Strengthening Security on the Internal Cloud Service Certification

Gangshin Lee[†‡]
KIM & CHANG

요 약

클라우드서비스에 대한 수요가 급증하고 있는 환경에서 보안 및 개인정보 침해를 우려하고 있다는 사실은 자칫 산업 활성화를 저해할 가능성이 있다. 따라서 클라우드서비스의 이용 신뢰성을 보장하는 것은 매우 중요하다. 본 논문에서는 클라우드서비스의 신뢰성을 보장하기 위한 CSA 인증, FedRAMP 인증, 한국클라우드서비스협회의 인증 등 국내외의 제도들을 비교함으로써 국내의 클라우드서비스 인증에는 보안 통제사항이 부족하다는 결론에 도달한다. 이에 따라 보안을 강화하기 위하여 국제표준인 ISO/IEC 27017, 한국인터넷진흥원(KISA)의 정보보호관리체계(ISMS) 인증에서의 보안 통제사항을 참고하여 제도 운용의 용이성, 전문성 등을 고려한 적절한 발전방향을 제시하였다.

ABSTRACT

In the background of rapidly increasing domestic cloud service demand, worries about security and privacy incidents can hinder the promotion of cloud service industry. Thus, it is crucial that the independent 3rd party assures the reliability for using the cloud service. This paper compares several external and internal cloud service certification cases, for example CSA certification, FedRAMP certification, KCSA certification, and concludes that insufficient security and privacy controls are prevailing. As a consequence, several enhanced countermeasures by using ISO/IEC 27017, KISA's ISMS considering manageability and expertise are proposed in the cloud service certification system.

Keywords: Cloud, Certification, Security, Control

I. 서 론

클라우드서비스(cloud service)는 IT분야에서 모바일 환경으로 전환되면서 전세계적으로 가장 빠른 성장세를 보이고 있다. 2013년 시만텍 조사에 의하면 2012년에 전세계의 기업 중 90% 이상이 클라우드서비스를 도입할 예정이라고 하였다[1]. 또한 2012년 시스코에서 발간한 보고서에 의하면 전 세계 클라우드 트래픽은 2011년부터 연평균 44% 성장하여 2016년에는 전 세계 데이터센터 트래픽의 60% 이상을 차지할 것이라고 전망하고 있다[2].

이와 같이 각국에서는 클라우드서비스의 활성화가 곧 국가산업의 경쟁력이라는 판단하에 앞다투어 도입에 사활을 걸고 추진해오고 있으나, 미국의 IT 솔루션 전문업체인 CDW가 2013년에 설문조사한 결과[3]에 의하면 클라우드서비스 도입 시 우려하는 가장 큰 위험요인으로 데이터 보안과 안정성을 지목하고 있다.

2013년 2월에 전 세계 5천만명의 사용자를 확보하고 있는 클라우드 기반의 메모장 서비스인 에버노트가 해킹을 당해 사용자 정보가 유출되었으며, 2012년 크리스마스 이브에는 아마존 클라우드서비스 내부 직원이 적절하지 못하게 데이터를 삭제하여 발생한 장애 때문에 고객사인 징가, 넷플릭스 등 주요 인터넷서비

접수일(2013년 10월 22일), 게제확정일(2013년 12월 4일)
† 주저자, gangshin.lee@kimchang.com
‡ 교신저자, gangshin.lee@kimchang.com(Corresponding author)

Table 1. Structure of Security Guidance

Section	Domain
Cloud Architecture	1: Cloud Computing Architectural Framework
Governing in the Cloud	2: Governance and Enterprise Risk Management
	3: Legal Issues: Contracts and Electronic Discovery
	4: Compliance and Audit Management
	5: Information Management and Data Security
	6: Interoperability and Portability
Operating in the Cloud	7: Traditional Security, Business Continuity, and Disaster Recovery
	8: Data Center Operations
	9: Incident Response
	10: Application Security
	11: Encryption and Key Management
	12: Identity, Entitlement, and Access Management
	13: Virtualization
	14: Security as a Service

스업체들이 최대 12시간 동안 서비스를 받지 못한 결과를 초래하기도 하였다.

이처럼 보안위협이 클라우드서비스 산업 활성화에 가장 큰 위협으로 작용하고 있음에도 불구하고 IT 강국인 한국은 위협에 제대로 대처하지 못함에 따라 클라우드 경쟁력은 상당히 저조한 수준에 머물고 있다.

BSA(The Software Alliance)가 2013년에 클라우드 국가 경쟁력 지수를 발표[4]하였는데, 세계 ICT시장의 80%를 차지하고 있는 24개국을 대상으로

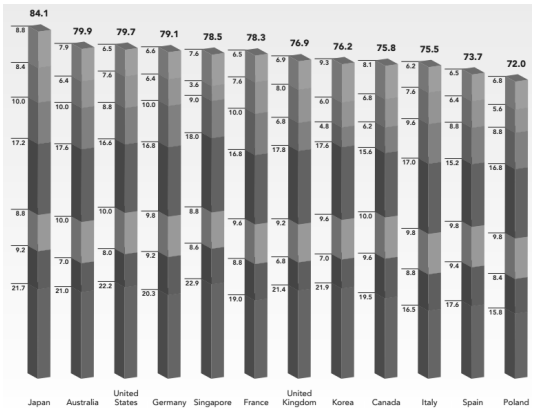

Fig.1. 2013 BSA Global Cloud Computing Scorecard

Fig.1의 위에서 부터 개인정보보호 (10점), 보안 (10점), 사이버범죄 예방 (10점), 지적재산권 보호 (20점), 산업의 독립성 및 국제적 조율 (10점), 국제정보 교류정책 (10점), 광대역통신망(30점) 이라는 7개 항목으로 구성된 지수 결과에서 한국은 8위라는 저조한 성적을 기록하였으며 이중에서도 보안, 사이버범죄 예방, 국제정보 교류정책이라는 3개 부문에서 특히 평균을 밑돌고 있었다.

따라서 본 논문에서는 클라우드서비스의 활성화에 가장 핵심적으로 고려하여야 하는 보안에 대하여 체계적으로 접근하고 있는 각 국가들의 모델과 모델을 토대로 한 인증제도에 대하여 분석하고 국내에서 도입하고 있는 모델, 가이드라인과 이를 토대로 하는 인증제도에 대하여 비교 분석함으로써 국내의 클라우드서비스의 인증이 어떤 모습이 되어야 할 것인지를 제안하고자 한다.

본 논문의 제2장에서는 클라우드 선진국들의 클라우드서비스 보안 모델, 프레임워크 등을 분석하고 제3장에서는 국내의 경우에 대해서 조사하여 비교 분석하며 제4장에서는 분석된 내용을 토대로 우리나라에서 클라우드서비스 인증을 위해 보안분야를 어떻게 강화시킬 것인지를 제시하고 제5장에서 결론을 맺는다.

II. 인증관련 국외현황

2.1 CSA(Cloud Security Alliance)

2008년 12월에 비영리 기관으로 클라우드 보안을 위해 창립된 CSA는 전 세계적으로 가장 활발하게 클라우드서비스 보안을 위해 노력하고 있다. 이러한 노력의 일환으로 아래 Fig.2와 같이 3단계의 인증 프레

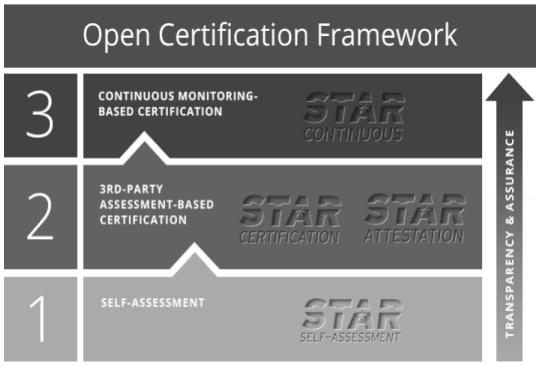

Fig.2. CSA's Open Certification Framework

임워크를 제시하고 있다. 1단계로는 2011년 9월 1일에 릴리즈한 Consensus Assessment Initiative Questionnaire (CAIQ) v1.1[5]과 2013년 9월 26일 릴리즈한 Cloud Control Matrix (CCM) v3.0[6]를 이용하여 자체평가를 할 수 있도록 하는 것이고, 2단계는 클라우드서비스가 CCM, ISO27001, AICPA SOC2를 만족하는지 제3자가 인증하는 것이며, 3단계는 클라우드서비스가 compliance, security, privacy, integrity, and operational security 를 준수하는지 증거를 확인해 볼 수 있도록 Cloud Trust Protocol(CTP)를 제공하고 있으면 잘 운영되고 있음을 보증하는 것이다[7].

1단계에서 활용하는 CAIQ, CCM은 모두 2009년 4월에 발간하여 2011년에 v3.0으로 릴리즈된 Security Guidance for Critical Areas of Focus Cloud Computing(일명 "Security Guidance")[8]을 토대로 만들어졌다.

Security Guidance는 아래 Table 1과 같이 총 14개 도메인(domain)으로 구성되었고 각 도메인별로 상세하게 내용을 포함하고 있다.

그리고 11개 분야 100개 통제그룹(control group)에 197개의 통제사항이 질문형식으로 구성된 CAIQ는 Security Guidance를 가지고 도출해 낸 것이며, 16개 통제 도메인(control domain)으로 구성된 CCM도 Security Guidance를 가지고 재 분류한 것이다. 즉, CAIQ와 CCM의 내용은 대부분이 Security Guidance 내용과 규모와 상세함에 있어서 유사하다고 할 수 있으며 이는 곧 보안의 전 분야뿐만 아니라 상세하게 내용을 다루고 있다는 점에서 신뢰성을 보증할 수 있는 프레임워크라 할 수 있다.

2단계 인증을 받기 위해서는 CCM과 ISO27001 또는 SOC2를 만족하여야 하는데 이는 영국표준원(British Standardization Institute, BSI)과 협력하여 인증하기 때문에 반영된 것이다. 보안 전반에 대하여 상세하게 확인하고 보증해 준다는 점을 알 수 있다. 더불어 SOC2를 만족하도록 한 것은 클라우드서비스가 SOX법에 따른 IT 및 정보보안 감사에서도 만족할 수 있어야 한다는 의미이기도 하기 때문에 매우 강력한 보안 인증 서비스를 제공한다고 할 수 있다.

2.2 ENISA (European Network and Information Security Agency)

유럽연합(EU)에서 보안에 관하여 각 국가들의 게이트웨이 역할을 하면서 총괄적인 역할을 하고 있는 ENISA도 2009년 11월에 Cloud Computing Benefits, risks and recommendations for information security(일명, Cloud Computing Risk Assessment)을 발간[9]하게 되었고 이를 토대로 유럽 연합에서는 클라우드서비스에 적용하기 시작하였다. ENISA는 동 지침을 토대로 동일 시점에 Cloud Computing Information Assurance Framework를 발간하여 민간기업에 대한 지배구조의 틀을 제시하게 되었다. 그리고 민간기업들이 서비스수준협약(Service Level Agreement)을 할 수 있도록 41개 질문으로 구성된 Survey and analysis of security parameters in cloud SLAs across the European public sector를 2011년 12월에 발간하였다.

이 중 가장 근원인 Cloud Computing Risk Assessment는 리스크(위협)를 정책과 조직위험(policy and organizational risks) 7개, 기술적 위험(technical risks) 13개, 법률적 위험(legal risks) 4개, 클라우드에 특화되지는 않으나 일반적인 보안위험 11개 등 총 35개로 분류하고, 취약점도 전체 53개로 분류하여 제시하고 있다. 동 가이드는 클라우드서비스 사업자들이 인증을 받기 위한 하나의 수단으로 사용할 수 있도록 발간된 것이다.

이상과 같이 ENISA에서 발간한 자료에서도 보안에 대한 위험과 취약점 목록을 제시함으로써 자산에 대한 위험을 평가할 시에 충분히 검토할 수 있을 정도의 내용을 반영하고 있다고 할 수 있다.

2.3 FedRAMP (Federal Risk and Authorization Management Program)

미 예산관리처(Office of Management and Budget)에서는 2010년 12월 9일에 Federal Risk and Authorization Management Program에서 Cloud First Policy를 발표하였다. 동 정책에서는 정부서비스가 안전성(secure), 신뢰성(reliable), 비용효과적(cost-effective)이기 위해서 클라우드서비스를 사용하도록 강력하게 권고하고 있어 미국 정부기관들이 클라우드서비스를 사용할 수 있는 근거로 삼을 수 있게 되었다. 다만 민간이 제공하는 클라우드서비스는 국가에서 지정하는 제3자(3PAO, Third-Party Assessor Organization)로부터 평

가를 받고 클라우드서비스를 이용하려는 기관에서는 동 평가 결과를 토대로 이용을 할 것인지 결정을 하는 방식으로 2012년 6월부터 시행에 들어갔다.

FedRAMP라는 동 인증체계는 미 전자정부법인 FISMA에서 정부기관이 준수하여야 할 가이드라인인 NIST 800-53A을 대통령 직속의 CIO Council에서 정부기관용으로 2010년 11월 2일에 발간한 Proposed Security Assessment & Authorization for U.S. Government Cloud Computing을 FedRAMP Security Controls Baseline v1.0으로 받아들여 사용하고 있다. 현재는 NIST 800-53A Revision 4까지 나와 있다.

동 FedRAMP Security Controls Baseline은 17개분야 185개의 보안 통제사항으로 아래 Table 2와 같이 구성되어 있어 매우 광범위하면서도 상세하다는 것이 특징이다. 그 만큼 클라우드서비스의 경우 신뢰성을 보장하기 위해서는 보안이 핵심적이라는 철학을 그대로 반영하고 있다.

Table 2. Structure of FedRAMP security controls baseline

분야	통제 사항 수
1. Access Control	22
2. Awareness and Training	4
3. Audit and Accountability	12
4. Assessment and Authorization	7
5. Configuration Management	9
6. Contingency Planning	10
7. Identification and Authentication	8
8. Incident Response	8
9. Maintenance	6
10. Media Protection	6
11. Physical and Environment Protection	18
12. Planning	6
13. Personnel Security	8
14. Risk Assessment	5
15. System and Services Acquisition	12
16. System and Communications Protection	32
17. System and Information Integrity	12
계	185

2.4 일본

총무성에서는 SaaS의 안전신뢰성 보장을 위하여 2008년 4월부터 클라우드서비스 인증제를 도입하게 되었는데 산하의 FMMC(Foundation for Multi-Media Communication)가 인증기관의 역할을 수행하고 있다. 심사 항목으로는 주로 로그관리, 바이러스 체크, 사용자 및 관리자의 인증, 서비스 일시 정지 사전 통지 등으로 구성되어 있다. 2011년 3월 기준으로 127건의 인증서가 발급이 되었다.

동 인증은 보안만으로 국한하지 않고 기업의 경영상태 등 전반에 대하여 심사를 하는데 보안 분야의 경우는 10여개 항목 수준으로 상당히 부족한 실정이다[11].

2.5 ISO/IEC WD 27017.4

ISO/IEC에서는 클라우드서비스 보안을 위해 ISO/IEC 27002를 기본으로 클라우드서비스 관련된 내용을 추가한 ISO/IEC WD 27017[12]을 작업문서(working draft)로 2012년 12월에 발간하게 되었다. 따라서 전체적으로 14분야에 걸쳐 117개의 통제사항으로 구성되어 있다. 이는 기존의 정보보호를 위한 통제사항 집합인 ISO/IEC 27002를 모두 적용함과 동시에 클라우드 특성이 있는 통제사항은 동 틀 내에서 반영하고 있는 구조이다.

III. 국내인증과 문제점 분석

3.1 한국인터넷진흥원(KISA)의 클라우드 서비스 보안관리 가이드

KISA에서는 2010년 11월에 시큐베이스의 위탁연구를 통하여 "클라우드 서비스 보안관리 가이드라인"을 발간하였다. 동 보고서는 국내의 정보보호관리체계(ISMS)의 통제사항을 기본으로 총 30분야 288개 통제사항을 체크리스트화하여 아래 Table 3과 같이 클라우드서비스 보안을 제시하였다[13].

클라우드서비스에 대한 보안을 위해 제시된 통제사항은 어느 다른 가이드보다도 광범위하면서도 상세하게 제시되어 있다. 그러나 동 연구 결과를 토대로 아직 제도적으로 반영되지는 않았다.

3.2 한국클라우드서비스협회(KCSA)의 인증제도

국내에서는 한국클라우드서비스협회가 2012년 4월부터 인증을 시작하였으며 에스케이텔레콤㈜의 T cloud biz와 주식회사 케이티의 ucloud biz가 동시

Table 3. Structure of Security Controls in [4]

분야	통제사항 수
정보보호정책	5
보안조직 운영	15
인력보안	9
자산에 대한 책임	8
정보자산분류	5
정보보안 이벤트와 취약성 보고	7
정보보안사고 및 개선방안 관리	9
위험분석 수행 및 복구대책 수립	8
서비스연속성	10
감사	11
정보시스템 정보보안 요구사항	3
암호통제	6
시스템파일 보안	11
네트워크 및 시스템 보안	4
어플리케이션 보안	14
컴플라이언스	30
보안구역	23
장비보안	20
운영절차 및 책임	12
시스템 계획수립 및 인수	6
악성코드 및 모바일코드에 대한 보호	7
백업	3
네트워크 보안관리	4
응용시스템의 정보보안	14
개발 및 지원 프로세스 보안	18
기술적 취약성 관리	4
정보보안 이벤트와 취약성 보고	7
정보보안 사고 및 개선방안 관리	9
데이터 및 스토리지 보안	3
식별 및 접근관리	3
계	288

에 인증을 받았다.

동 인증심사를 위한 항목을 살펴보면 크게 품질, 정보보호, 서비스기반 등 3개 부분에 걸쳐 가용성, 확장성, 성능, 데이터관리, 보안, 서비스지속성, 서비스 지원 등 7개 영역에서 105개의 세부 통제항목으로 구성되어 있다. 인증을 받기 위해서는 필수항목은 반드시 통과하여야 하며 전체의 70%를 통과할 경우 인증을 받을 수 있도록 되어 있다. 그리고 문서와 실사를 할 수 있는데 17개 항목에 대해서만 실사를 할 수 있고 필수는 39개에 불과한 실정이다. 99.5%의 가용성, 글로벌 수준의 손해배상 기준 명시, ISMS 인증을 획득한 경우에는 Fig.3처럼 우수SLA인증을 추가로 부여하고 있다.

Fig.3. KCSA's Cloud Service Certification Symbol

동 인증심사항목에서 보안분야는 105개의 약20% 정도를 차지하는 아래 Table 4에 있는 22개 통제항목을 차지하고 있으나 10개만이 필수항목으로 되어 있으며 실사는 4개만 하면 되는 것으로 되어 있어 보안분야에 대해서 매우 미약한 실정이다. 또한 가장 중요한 위협 중의 하나인 프라이버시의 침해 가능성 등이 상존하고 있음에도 불구하고 개인정보보호에 대한 법률적인 항목은 전혀 없는 실정이다.

Table 4. Structure of Security Controls in KCSA

NO	측정항목	심사방법		필수 여부
		문서	실사	
5.1	정보보호 정책수립	O	X	필수
		O	X	일반
		O	X	필수
5.2	조직 및 책임설정	O	X	일반
		O	X	필수
		O	X	일반
5.3	정보자산 관리	O	O	일반
5.4	인증 및 접근관리	O	X	필수
		O	O	필수
		O	X	필수
		O	X	일반
5.5	정보보호 교육	O	X	필수
		O	X	일반
5.6	내/외부인력 보안	O	X	일반
		O	X	일반
		O	X	필수
		O	X	일반
5.7	물리적 접근통제	O	X	필수
		O	X	일반
5.8	시스템 개발보안	O	O	일반
5.9	가상화 보안	O	O	일반
5.10	보안사고 관리	O	X	필수

3.5 국내 클라우드 인증제에서의 보안 문제점

상기에서 살펴 보았듯이 우리나라의 경우 현재 운영중인 클라우드서비스 인증제에서 보안분야가 매우 미흡하다. 국내의 인증제도가 미흡한 이유는 IT 강국임에도 불구하고 클라우드 산업의 출발이 늦었다는 이유로 인증의 목적성으로 서비스의 품질, 기업경영성을 중심으로 구성하였기 때문이다. 그러나 서론에서 살펴본 것처럼 클라우드서비스의 도입에 대하여 가장 우려하고 있는 이유는 보안 및 프라이버시 문제이다. 즉, 현재의 인증심사를 위한 항목으로서는 서비스 이용자들에게 신뢰성을 제공할 수 없기 때문에 클라우드서비스 산업을 활성화하기 어렵다는 결론에 도달한다.

Table 5. Comparison of Internal and External Cloud Service Security Guidelines

ISO27017 (14분야 117개 통제사항)	KISA의 ISMS (13분야 92개 통제사항)	CSA 가이드라인 (14 domain)	FedRAMP Security Controls Baseline (17분야 185개 통제사항)	KCSA 인증심사 기준 (10분야 22개 통제사항)
정보보호정책 (Security Policies)	정보보호정책	Governance and Enterprise Risk Management	Assessment and Authorization Planning Risk Assessment	정보보호 정책수립
정보보호 조직 (Organization of Information security)	정보보호 조직			조직 및 책임설정
인적보안 (Human resource security)	외부자보안 인적보안 정보보호교육	Traditional Security, Business Continuity and Disaster Recovery	Awareness and Training	정보보호 교육 내/외부인력 보안
자산관리 (asset management)	정보자산분류	Governance and Enterprise Risk Management	Risk Assessment	정보자산 관리
접근통제 (access control)	접근통제	Identity and Access Management	Access Control Identification and Authentication	인증 및 접근관리
암호 (cryptography)	암호통제	Encryption and Key Management		
물리 및 환경보안 (physical and environmental security)	물리적 보안	Traditional Security, Business Continuity and Disaster Recovery	Physical and Environmental Protection	물리적 접근통제
운영보안 (operations security)	운영보안	Data Center Operations	Audit and Accountability Media Protection System and Information Integrity	
통신보안 (communications security)			System and Communication Protection	
시스템 획득, 개발, 유지보수 (system acquisition, development and maintenance)	시스템 개발보안	Information Management and Data Security Application Security	Configuration Management Maintenance System and Services Acquisition	시스템 개발보안
공급자관계성 (supplier relationship)		Security as a Service		
보안사고관리 (Information security incident management)	침해사고관리	Incident Response, Notification and Remediation	Incident Response	보안사고 관리
업무연속성관리 (Information security aspects of business continuity management)	IT재해복구	Traditional Security, Business Continuity and Disaster Recovery	Contingency Planning	
법률준거성 (compliance)		Compliance and Audit Legal Issues: Contracts and Electronic Discovery		
		Portability and Interoperbility		
			Personal Security	
				가상화 보안

클라우드서비스 관련 국제표준인 ISO27005의 통제사항을 기준으로 한국인터넷진흥원(KISA)의 정보보호관리체계 인증심사 기준, CSA의 가이드라인, FedRAMP에서 사용하는 NIST 800-53A Revision 3, 한국클라우드서비스협회의 인증심사기준을 비교하면 다음 Table 5와 같다.

타 클라우드서비스 보안 관련한 가이드라인에 비하여 KCSA의 인증심사 기준의 통제사항 개수는 총 22개로 5%~10% 수준에 불과하다. 또한 22개 중에서도 선택을 제외할 경우 필수는 10개에 불과한 수준이다. 이는 타 가이드라인의 통제사항 대비 5% 미만일 정도로 매우 저조한 실정이다. 또한 일부 가장 중요한 암호화, 운영보안 등 도메인도 없다.

이와 같은 미흡한 보안 통제사항으로 서비스 이용자에게 신뢰감을 주기는 매우 어려우며, 이 때문에 국내의 클라우드서비스의 활성화는 다른 국가들에 비하여 발전속도가 더딜 수 밖에 없는 이유가 될 수 있다.

따라서 국내의 클라우드서비스에 대한 신뢰성을 확보하기 위해서 현재의 통제사항을 대폭 보강을 하여야 할 것이다. 보강을 위해서 현재의 제도에 포함을 하거나 정보보호 분야만을 별도로 전문적으로 인증하는 제도를 도입하는 것이 클라우드서비스 산업의 경쟁력을 확보하기 위해서 시급한 실정이다. 그러면 신뢰성을 보장하는 제도의 발전을 위한 몇 가지 방안을 고찰하도록 한다.

IV. 개선제안

제도의 개선을 위해서는 국내에서 클라우드서비스의 신뢰성을 확보하기 위하여 KCSA가 도입한 인증은 심사항목을 대폭 보강하여 추진하는 방법, 정보보호전문기관에서 보안분야만을 인증하는 제도를 도입하는 방법, 자체선언을 하는 방법을 생각해 볼 수 있다.

KCSA의 인증을 개선하기 위해서는 심사항목을 대폭 보강하되 ISO/IEC의 표준을 준용하는 방법,

KISA의 정보보호관리체계 인증심사 항목을 적용하는 방법 등을 고려할 수 있다. 또한 심사원의 전문성을 확보하여야 하며, 심사를 위한 기간도 충분히 가질 필요가 있다. 현재 정보보호관리체계 인증을 위해 투입하는 전문심사원과 시간, 인력을 유사하거나 복잡성 등을 고려하여 그 이상으로 투입하는 것이 타당하다.

정보보호전문기관이 수행할 경우는 법적인 근거를 마련하거나 기존의 제도를 활용하여 심사항목을 보완하는 방법이 있다. ISO/IEC 27017을 참고하여 기존의 통제항목에 반영하는 방법이 있다. 물론 CSA등 다른 기관의 가이드라인을 참고하여 국내실정에 적합한지에 대한 검토가 이루어져야 한다.

산업의 활성화에 따른 파급효과를 고려하여 이처럼 제도를 강화하거나 도입함으로써 조속히 신뢰할 수 있는 수준으로 클라우드서비스의 보안을 보증할 수 있어야 한다.

V. 결 론

클라우드서비스는 비용효과성과 이동성의 장점으로 인하여 전 세계적으로 수요가 급증하고 있으며 이로 인하여 산업의 성장성이 높은 분야이다. 이러한 블루오션인 클라우드서비스에 대하여 이용자들은 신뢰하기 어렵기 때문에 더 이상 성장하기 어려운 구조가 될 수 있다는 것이 각종 국내외 유명 리서치에서 나타나고 있다.

이러한 이유 때문에 선진국에서는 신뢰성을 확보하기 위하여 인증제도를 도입하고 있고 국내의 경우도 도입을 하였으나 신뢰할 수준까지는 갈길이 먼 상태이다. 그래서 타 국가의 클라우드서비스의 인증제도와 비교를 통하여 우리나라의 인증제도를 보안 특성에 맞게 신규로 도입을 하거나 대폭적으로 보안 통제사항을 보강하여야 한다는 결론을 얻을 수 있었다.

향후에 타 국가의 인증심사 항목 등에 대해서 국내의 임증심사 항목과 보다 구체적으로 비교 분석함으로써 실질적인 통제사항들을 도출하는 연구가 진행이 되어야 한다.

References

[1] Symantec, "Avoiding the hidden costs of the cloud," pp. 4, 2013.

[2] CISCO, "Cisco Global Cloud Index: Forecast and Methodology, 2011-2016," pp. 3, 2012.

[3] CDW, "2013 State of The Cloud Report," pp. 3, Feb. 2013.

[4] BSA, "2013 BSA Global Cloud Computing Scorecard", pp. 10-11, 2012.

[5] CSA, "Consensus Assessment Initiative Questionnaire (CAIQ) v1.1," Sep. 2011.

[6] CSA, "Cloud Control Matrix (CCM) v3.0", Sep. 2013.

[7] https://cloudsecurityalliance.org/

[8] CSA, "Security Guidance for Critical Areas of Focus Cloud Computing v3.0", 2011.

[9] ENISA, "Cloud Computing Benefits, risks and recommendations for information security," Nov. 2009.

[10] FMMC, http://www.fmmc.or.jp/asp-nintei/data/shinsa.pdf

[11] FMCC, "ASP･SaaS安全･信頼性に係る情報開示認定制度 審査對象項目： 事業者", pp. 1-2, 2013.

[12] ISO/IEC, "ISO/IEC WD 27017.4, Information technology - Security techniques - Code of practice for information security controls for cloud computing services," Dec. 2012.

[13] KISA, "A Guide of Security Management for Cloud Computing Services," pp. 103-130, Nov. 2010.

〈저 자 소 개〉

이 강 신 (GangShin Lee) 종신회원
1989년 8월: 한양대학교 수학과 석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
1990년 7월~1992년 6월: ㈜데이콤 종합연구소 연구원
1992년 7월~2000년 8월: 한국정보화진흥원 부장
2000년 9월~2011년10월: 한국인터넷진흥원 단장
2011년11월~현재: 김·장 법률사무소 전문위원
2006년 9월~현재: 건국대학교 정보통신대학원 겸임교수
〈관심분야〉 정보보호관리, 네트워크보안, 개인정보보호