情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

한국형 클라우드를 위한 정보보호 관리체계 평가 기준*

김 기 철,[1†] 허 옥,[2] 김 승 주[3‡]
[1]금융결제원, [2]고려대학교 정보보호대학원, [3]고려대학교 사이버국방학과/정보보호대학원

A Security Evaluation Criteria for Korean Cloud Computing Service*

Kichul Kim,[1†] Ok Heo,[2] Seungjoo Kim[3‡]
[1]Korea Financial Telecommunications and Clearings Institute,
[2]Center for Information Security Technologies(CIST), Korea University
[3]Department of Cyber Defense/Center for Information Security Technologies(CIST), Korea University

요 약

IT자원을 공유하여 서비스 형태로 제공하는 클라우드 컴퓨팅은 정보보호 이슈가 해결되지 않으면 활성화될 수 없다. 기업은 클라우드 컴퓨팅 서비스를 도입하여 정보통신 자원의 효율성을 극대화하고자 한다. 하지만 미국, 일본 등에 비해 국내에서 클라우드 컴퓨팅 서비스가 아직 활성화되지 못한 가장 큰 이유는 정보보호에 대한 신뢰가 부족하기 때문이다. 본 논문은 국내·외 클라우드 인증제도 및 가이드라인과 정보보호 관리체계 통제 항목을 비교 분석하여 한국형 클라우드를 위한 핵심 평가 기준 및 기존 정보보호 관리체계 통제 항목과의 중복성을 제거한 추가적인 평가 기준을 제안한다. 정보보호 관리체계 인증을 받은 클라우드 서비스 제공자는 추가 평가 기준만으로 중복되고 불필요한 인증 평가 작업을 최소화할 수 있다.

ABSTRACT

Cloud computing provided as a service type by sharing IT resources cannot be activated unless the issue of information security is solved. The enterprise attempts to maximize the efficiency of information and communication resources by introducing cloud computing services. In comparison to the United States and Japan, however, cloud computing service in korea has not been activated because of a lack of confidence in the security. This paper suggests core evaluation criteria and added evaluation criteria which is removed the redundancy of the security controls from existing ISMS for Korean cloud computing through a comparative analysis between domestic and foreign security controls of cloud certification scheme and guidelines and information security management system. A cloud service provider certified ISMS can minimize redundant and unnecessary certification assessment work by considering added evaluation criteria.

Keywords: Information Security Management System(ISMS), Information Assurance, Security Evaluation, Cloud Computing

접수일(2012년 11월 28일), 수정일(2013년 1월 21일), 게재확정일(2013년 3월 15일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2013-H0301-13-1003)
† 주저자, jeterkim@kftc.or.kr
‡ 교신저자, skim71@korea.ac.kr

I. 서 론

클라우드 컴퓨팅이란 네트워크, 서버, 스토리지, 애플리케이션, 서비스 등의 컴퓨팅 자원을 공유함으로써 언제 어디서나 편리하게 주문형(on-demand) 방식으로 네트워크 접속을 가능하게 해주는 모델이다[1]. 또한 유연성 및 확장성을 지닌 IT자원을 인터넷 기술을 통해 외부 고객에게 서비스(as a service)로 제공하는 컴퓨팅 방식으로 정의하기도 한다[2]. IT자원을 공유하여 서비스 형태로 제공하는 클라우드 컴퓨팅은 정보보호 이슈가 해결되지 않으면 활성화될 수 없다. 국내에서 클라우드 컴퓨팅 서비스는 IT관련 사업뿐 아니라 국가경쟁력을 좌우하는 산업으로 인식되어 클라우드 컴퓨팅 시장 규모를 키우고 세계시장 점유율을 확대하는 등 핵심 기술 개발을 본격 추진하고 있으나[3] 미국, 일본 등에 비해 아직 활성화되지 못한 가장 큰 이유는 정보보호에 대한 신뢰가 부족하기 때문이다[4][5]. 가트너에 따르면 클라우드 컴퓨팅은 무결성, 복구, 프라이버시 등의 위험 관리 영역과 e-디스커버리, 규정 준수, 감사 등 법적 쟁점 영역의 평가가 요구되어진다[6]. 따라서 클라우드를 위한 정보보호 평가 기준이 마련되어 클라우드 서비스 제공자 및 서비스를 평가한다면 클라우드 고객은 클라우드 컴퓨팅 서비스에 신뢰를 가지게 될 것이다. 미국 테크아메리카 재단의 Cloud^2 위원회는 오바마 정부 차원의 클라우드 도입 전략인 'Cloud First 정책' 을 더욱 발전시키기 위한 14개 권고사항이 담긴 보고서를 발표하였는데 가장 첫 번째 권고사항이 신뢰를 위한 보안 및 보증 프레임워크이다[7]. 보안 및 보증 프레임워크를 위한 모범 규준으로 클라우드 서비스 제공자는 NIST(National Institute of Standards and Technology) 및 관련 제도와의 협업을 권고하고 있으며 관련 제도로 연방정부의 클라우드 서비스에 대한 보안 평가 및 인증&인가 제도인 FedRAMP(Federal Risk and Authorization Management Program)외에 국제 표준 정보보호 관리체계 인증제도인 ISO27001, 미국 연방정보보안관리법(FISMA)에 따라 연방정부 및 연방정부에 도입되는 시스템의 보안 통제 항목으로 권고되는 NIST SP800-53, 신용카드 정보보호 표준인 PCI DSS(Payment Card Industry Data Security Standard) 등을 예시하고 있다. 국내에서는 정보보호 관리를 위한 정보보호관리체계(K-ISMS) 인증제도 및 프라이버시 준수를 위한 개인정보보호관리체계(PIMS) 인증제도가 본격적으로 시행 되고 있다. 하지만 정보통신 사업자 등 일반 기업에 적용되는 K-ISMS, PIMS로는 클라우드 서비스의 신뢰성 및 안전성을 모두 보증하기가 어려우며, ISO27001과 NIST 표준 및 지침 또한 클라우드 컴퓨팅의 정보보호 영역을 모두 커버하기에는 한계가 있다. 예를 들어 서비스 제공자와 고객 사이 멀티-테넌시(Multi-tenancy)의 자산 공유 위험이 고려되지 않고 있으며[8]. 가상화로 인한 보안 이슈를 커버하기엔 한계가 존재한다[9]. 이러한 이유로 미국 연방정부의 FedRAMP 외에도 가트너, NIST, CSA(Cloud Security Alliance), ENISA (European Network and Information Security Agency) 등에서 클라우드 컴퓨팅과 관련된 위협 및 보안 통제 항목들을 제시하고 있다. 국내에서는 방송통신위원회·한국인터넷진흥원(KISA)에서 개발한 정보보호 안내서를 통해 클라우드 서비스 제공자 및 이용자의 정보보호 체크리스트를 제공하고 있다.

본 논문은 K-ISMS, PIMS 등 국내에서 시행 중인 대표적인 정보보호 관리체계 평가·인증 제도와 클라우드 컴퓨팅을 위한 국내·외 인증제도, 표준, 가이드라인을 비교 분석함으로써 중복되지 않은 통제 항목을 도출한다. 도출된 통제 항목을 평가 기준 후보군으로 놓고 국내 환경에 처한 위협을 통해 한국형 클라우드를 위한 평가 기준을 최종 도출한다. 본 논문의 목적은 도출된 최종 평가 기준이 국내에서 시행 중인 정보보호 관리체계의 평가 기준과 중복되지 않기 때문에 인증제도 도입 시 중복되고 불필요한 인증 평가 작업을 최소화할 수 있어 효율성이 높음을 보이는데 있다. 외국 클라우드 서비스 제공자가 국내 클라우드 서비스에 진출하고자 할 경우 국내 환경에 맞는 정보보호 관리체계 인증을 받아야 국내 고객의 신뢰성과 안전성을 보증할 수 있으므로 본 논문의 한국형 클라우드는 국내 환경, 취약점, 위협을 반영한 클라우드 컴퓨팅 서비스라고 정의할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 국내·외 대표적인 정보보호 관리체계를 살펴보고, 3장에서는 클라우드를 위한 국내외 평가·인증 체계 및 표준, 가이드라인을 살펴본다. 4장에서는 각 제도의 통제 항목을 비교·분석하고 5장에서 비교·분석 결과로 도출된 클라우드 평가 기준 후보 항목들을 제시한다. 6장에서는 한국형 클라우드를 위한 평가 기준을 최종 도출하고 7장에서 결론을 맺는다.

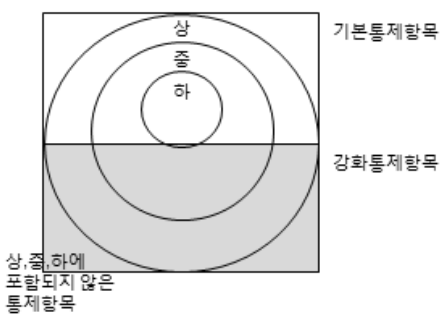
II. 배경

2.1 ISO27001

ISO27001은 정보보호를 계획-실행-검토-조치 단계의 PDCA(Plan-Do-Check-Act) 사이클에 의해 관리한다. 3개(일반, 문서통제, 기록통제)의 문서화 요구사항 및 11개 분야, 39개 통제 목적, 133개 보안 통제 항목을 적용한 국제 표준의 정보보호 관리체계이다. ISO27001는 정보보호 관리체계를 비즈니스, 조직, 장소, 자산과 기술적 특성을 고려하여 수립하고 목적 및 범위를 정의한다. 또한 정보보호 정책과 목적에 부합하도록 위험을 수용 가능한 수준으로 감소시키기 위해 위험분석 및 평가에 의거 위험처리, 위험수용, 위험회피, 위험전가 등의 전략을 설정하고 기준에서 제시하는 통제 항목을 선택한다.

2.2 NIST SP800-53

미국 국립표준기술원(NIST)에서 연방정보보호법(FISMA)에 의해 특별 간행물(Special Publication)로 개발한 SP800-53(r3)은 보안 통제 항목을 관리, 운영, 기술의 3개 클래스, 18개의 패밀리 그리고 198개(총 205개의 통제 항목 가운데 7개는 취소)의 통제 항목으로 분류하여 선택할 수 있도록 하는 미연방 정보시스템 및 조직을 위한 권고수준의 표준 가이드라인이다. 기본 통제 항목과 강화 통제 항목(Control enhancements)으로 구성되어 상(High-impact), 중(Moderate-impact), 하(Low-impact)의 세 가지 통제 항목 기준선(Control Baselines)을 제공한다. 각각 115개, 251개, 328개의 통제 항목으로 구성되며 통제 항목 수가 많을수록 보증 수준이 높아진다.



〔그림 1〕 SP800-53 통제 항목

2.3 국내 ISMS

2.3.1 K-ISMS

K-ISMS는 관리과정(정보보호 정책수립, 관리체계 범위설정, 위험관리, 구현, 사후관리의 5단계) 및 문서화, 정보보호 대책의 3가지 통제 분야와 23개의 통제 내용, 137개의 통제 항목과 446개의 세부 통제 항목으로 구성되어 있다. 이 가운데 관리과정과 문서화를 제외한 정보보호 대책의 통제 내용은 15개, 통제 항목은 120개로 정보보호 정책, 정보보호 조직으로부터 업무 연속성 관리 까지 대부분 ISO27001을 포함하고 있으나 전자거래 보안, 암호 통제, 외부자 보안 등이 국내 환경에 맞게 강화한 부분이다.

2.3.2 PIMS

PIMS는 관리과정(정책수립, 범위설정, 위험관리, 구현, 사후관리의 5단계) 및 보호대책, 생명주기의 3가지 통제 분야와 17개의 통제 내용, 42개의 통제 목적, 118개의 통제 항목, 325개의 점검항목으로 구성된다. 보호대책은 9개의 통제 내용으로 구성되어 있으며 개인정보 수립, 이용 및 제공, 관리 및 파기에 이르는 생명주기 통제분야가 존재하는 것이 특징이다. 기존 K-ISMS의 정보보호 대책 통제 항목과 많은 부분이 유사하여 K-ISMS와 국내 개인정보보호법을 포함한 정보보호 관리체계라고 볼 수 있다.

III. 클라우드 보안 인증, 가이드라인

3.1 국외

3.1.1 가트너 보고서

2008년 가트너에서 발표한 보고서[10]에서는 클라우드 컴퓨팅을 위한 7가지 보안 통제 항목을 제시하였다.

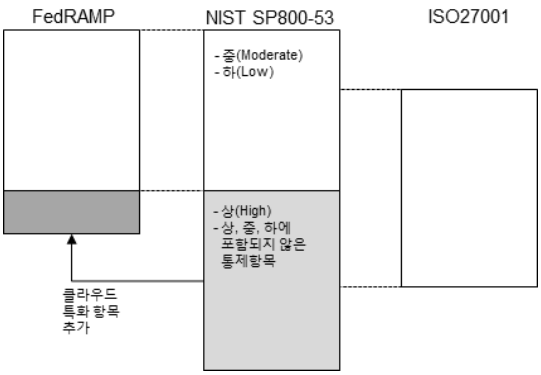
1. 권한 사용자 접근(Privileged User Access)
2. 규정 준수(Regulatory Compliance)
3. 데이터 위치(Data Location)
4. 데이터 분리(Data Segregation)
5. 복구(Recovery)
6. 조사지원(Investigative Support)
7. 장기간 생존성(Long-term Viability)

3.1.2 FedRAMP (미 연방 인증&인가제도)

미국 연방정부에 도입되는 클라우드 제품 및 서비스에 대한 보안성 평가·인증 제도인 FedRAMP[11]는 기존 정부기관별로 수행하던 IT 시스템에 대한 보안성 평가를 클라우드에 한해 FedRAMP로 통합하였다[12]. FedRAMP의 통제 항목은 NIST의 SP-800-53에서 제공하는 상(High), 중(Moderate), 하(Low)의 기준선 가운데 중, 하 등급의 통제 항목을 준용하고 클라우드에 특화된 일부 항목을 추가하였다. NIST SP800-53에서 제시하고 있는 252개의 중급 항목 가운데 클라우드 인증을 위해 45개 항목을 추가하였고 하급 항목은 1개 항목을 추가하였다〔표 1〕. 총 46개의 추가된 항목은 〔그림 2〕와 같이 SP800-53의 상 등급 또는 상, 중, 하에서 제외된 통제 항목에서 도출되었다.

〔표 1〕 FedRAMP 항목 비교

등급	NIST 항목 (SP800-53)	FedRAMP 추가 항목	계
하	115	1	116
중	252	45	297



〔그림 2〕 FedRAMP 추가 항목 도출

3.1.3 CSA 가이드라인, CSA-CCM

비영리조직 클라우드 보안 협회인 CSA에서는 클라우드 보안 가이드라인[13] 및 CSA-CCM(Cloud Controls Matrix)을 제공한다. 가이드라인은 클라우드 구조, 클라우드 거버닝(Governing), 클라우드 운영의 3개 섹션과 14개 도메인으로 구성된다. CSA-CCM은 98개 클라우드 통제 항목으로 구성되어 있다. 통제 항목은 CSA의 인증 프레임워크의 3단계 인증 단계(1단계:클라우드 서비스 제공자의 자기 평가, 2단계:제3기관에 의한 평가, 3단계:지속적인 모니터링 기반의 평가) 가운데 2단계에서 사용하게 된다. CSA-CCM은 FedRAMP 및 국제 표준의 통제 항목 간의 대응 관계를 매트릭스를 통해 제시한다[14].

〔표 2〕 CSA-CCM 통제 항목

통제 영역		개수
CO	컴플라이언스	6
DG	데이터 통제	8
FS	보안 설비	8
HR	인적 관리	3
IS	정보 보안	34
LG	법규 준수	2
OP	운영 관리	4
RI	위험 관리	5
RM	공표 관리	5
RS	사고 복구	8
SA	보안 아키텍쳐	15
계		98

3.1.4 ENISA(유럽 가이드라인)

유럽 ENISA에서 발간한 가이드라인은 클라우드 위험을 정책·조직의 위험, 기술적인 위험, 법규 위험, 클라우드에 특화되지 않은 위험의 4가지 영역 및 35개 항목으로 구분하고 적용 사례 시나리오 및 위험 평가 절차를 제시한다. 또한 클라우드에 특화된 취약점 및 자산을 분류하고 12개의 정보보증 요구사항을 다음과 같이 제시한다[15].

1. 인적 보안
2. 공급망(Supply-chain) 보증
3. 운영 보안
4. 식별 및 접근 관리
5. 자산 관리
6. 데이터와 서비스 이식성
7. 업무 연속성 관리
8. 물리적 보안
9. 환경 통제
10. 법규 요구사항
11. 법규 권고사항
12. 유럽 위원회에 법규 권고사항

3.2 국내

3.2.1 클라우드 서비스 인증

2012년 2월 방송통신위원회 산하 한국클라우드서비스협회(KCSA)는 클라우드 업체가 제공하는 서비스를 평가하여 일정수준 이상의 체계나 절차를 확보하고 있는 경우 인증을 부여하는 '클라우드 서비스 인증제'를 본격 시행하였다. 2011년 5월 관계부처 합동으로 발표한 "클라우드 컴퓨팅 확산 및 경쟁력 강화 전략"의 일환으로 마련된 제도로 클라우드 서비스 인증의 심사기준은 크게 가용성, 확장성, 성능, 데이터 관리, 보안, 서비스 지속성, 서비스 지원의 7개 항목으로 구성되어 있다[16]. 세부 측정내용은 〔표 3〕와 같다. 하지만 클라우드 서비스 인증 수요가 미미한 수준으로 향후 인증 등급을 부여하거나 정부 인증으로 격상하는 방안도 검토하고 있다. 추가적으로 클라우드 인증을 획득한 서비스 중 99.5% 이상의 가용성을 이용약관이나 서비스수준협약(SLA)을 통해 보장하며, 이와 관련하여 글로벌 주요 기업 수준의 손해배상액을 제시하고 정보보호관리체계(ISMS) 인증을 받는 조건을 모두 만족하는 서비스에 한해 부여하는 우수 SLA인증을 시행하고 있다.

〔표 3〕 클라우드 서비스 인증 측정항목

측정 목적	측정내용	측정 수	점검 수
가용성	신청기관은 클라우드 서비스를 약정된 내용에 따라 상시적으로 제공하기 위해 제반 조치를 하여야 한다.	5	14
확장성	클라우드 서비스 제공자는 클라우드 서비스 수요에 유연하게 자원을 확장하여 제공할 수 있도록 필요한 정책, 인적 물적 자원 등을 갖추어야 한다.	5	12
성능	클라우드 서비스 제공자는 서비스의 품질(속도)을 보장하기 위해 적절한 성능을 유지하여야 한다. 이를 위해 필요한 정책, 인적 물적 자원 등을 갖추어야 한다.	6	13
데이터 관리	클라우드 서비스 제공자는 클라우드 서비스 이용자의 데이터를 안전하게 보호/관리하기 위해 필요한 정책 및 인적/물적 자원 등을 갖추어야 한다.	5	15
보안	조직의 보안을 효과적으로 구현하기 위해 관리체계를 수립하여야 한다. 또한 조직의 물리적 시설 및 설비를 보호하기 위해 물리적 보호 방안이 마련되어야 한다. 또한 다양한 취약성을 분석하고 그에 대한 적절한 대책을 마련하고 적용하여야 한다.	10	22
서비스 지속성	이용자가 믿고 클라우드 서비스를 이용할 수 있도록 사업자는 인적·물적 기반을 확보하고 이를 관리하여야 한다.	4	13
서비스 지원	클라우드 서비스 제공자는 이용자의 서비스 만족도를 제고하기 위해 각종 기술지원, 제공방식의 다양성, 수준의 보장 등 지원 체계를 갖추어야 한다.	5	16
계		40	105

클라우드 서비스 정보보호 안내서(방통위·KISA)

동 안내서는 클라우드 서비스 모델, 주요 기능을 소개하며 예상되는 신규 보안 위협 및 보안 취약점 등을 분석하고 클라우드 서비스 제공자와 이용자를 대상으로 보안 이슈 및 정보보호 고려사항 등을 제시한다. 부록으로 제공되고 있는 클라우드 서비스 제공자 및 이용자의 정보보호 체크리스트 점검 항목은 〔표 4〕와 같다[17].

〔표 4〕 클라우드 서비스 정보보호 안내서 점검항목

점검분야	점검항목	항목수
클라우드서비스 보안정책	정보보호정책	2
보안조직 운영 및 인력보안	보안조직 운영	6
	인력보안	5
자산분류와 통제	자산보호	3
	자산분류	2
클라우드 서비스 사고 관리절차 수립	보안이슈보고	2
	보안사고 대응관리	3
서비스 연속성	서비스 연속성	3
컴플라이언스	컴플라이언스	7
물리적 보안	보안통제	5
	장비보안	6
통신 및 운영	운영관리	2
	시스템 관리	1
	악성코드 대응	2
	백업	1
	네트워크 보안관리	1
	감사	6
	보안 요구사항	1
	정보시스템 보안	1
	응용시스템 보안	3
	암호통제	2
	시스템 파일 보안	3
	개발관리	5
	취약성 관리	1
기술적 보안	시스템 보안	1
	정보보호	2
	보안 테스트	1
	접근 관리	1
계		77

IV. 비교 분석

4.1 정보보호 관리체계 비교 분석

4.1.1 ISO27001, NIST SP800-53

SP800-53의 부록(Appendix H)은 ISO27001의 부록(Annex A)에서 제시하는 통제 항목과 매핑한 테이블을 제공한다. ISO27001에 존재하지만 NIST SP800-53 (R3)에 존재하지 않는 통제 항목은 「A.11.5.6 연결시간 제한」, 「A.11.6.2 중요시스템 분리」, 「A.12.2.4 출력 데이터 검증」으로 3개 항목에 불과하지만 반대로 NIST SP800-53 (R3)에 존재하지만 ISO27001에 존재하지 않는 통제 항목은 「AC-22 공개적으로 접근가능한 내용」 등 38개 항목으로 그 수가 상대적으로 많다.

4.1.2 K-ISMS, PIMS

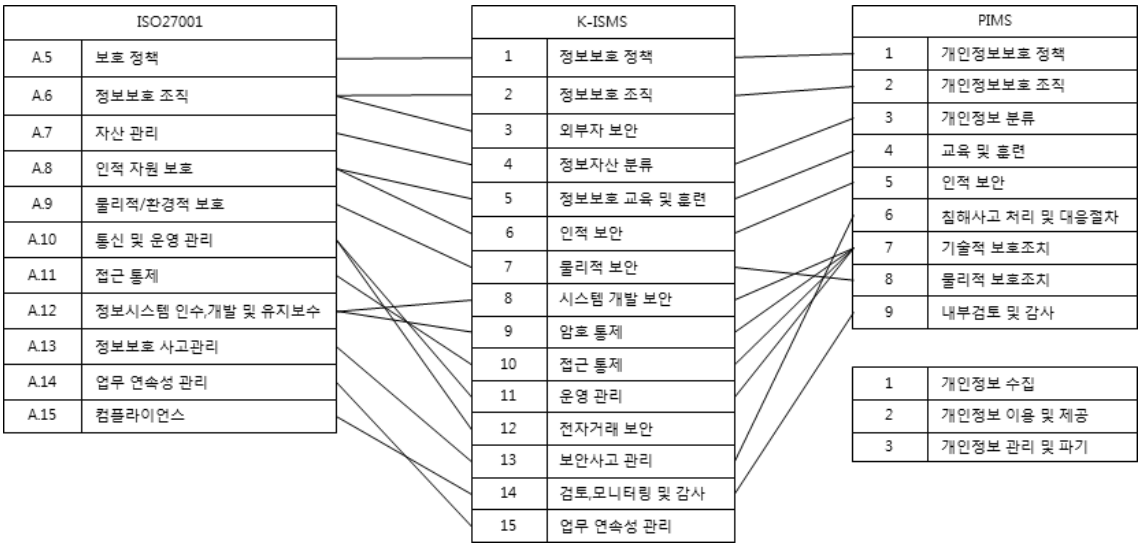
K-ISMS에는 존재하지만 PIMS에는 존재하지 않는 통제 항목은 〔그림 3〕의 정보보호 관리체계 매핑도를 통해서 확인한 결과 3.외부자 보안, 12. 전자거래 보안, 15.업무 연속성 관리 등 다수이다. 하지만 PIMS에만 존재하는 항목은 생명주기(1.개인정보 수집, 2.개인정보 이용및제공, 3.개인정보 관리및파기)의 28개 통제 항목이다. 세부 통제 항목을 자세히 매핑해본 결과 PIMS의 7.5.2 출력, 복사 시 기록 및 승인, 7.6.1 개인정보 마스킹, 9.3.1 개인정보 처리 활동 모니터링, 9.3.2 개인정보 열람기록 검토 및 오남용방지, 9.3.3 개인정보 처리 기록 검토 및 위변조 방지의 5개 보안대책 통제 항목이 K-ISMS와 매핑되지 않았다.

4.1.3 ISO27001, K-ISMS

K-ISMS는 ISO27001 국제 표준을 모두 포함하고 있으며, 국내 상황에 맞게 침해사고 예방, 암호화, 전자거래 등의 보안요건을 강화하였다. 따라서 ISMS 인증을 받게 되면 ISO27001 인증에서 요구하는 기준을 모두 만족하면서 국내 정보보호 환경에 맞는 정보보호 관리체계가 수립되었음을 보증할 수 있다[18]. 침해사고 예방, 암호화, 전자거래 등의 통제 항목이 K-ISMS에서 강화된 항목이다〔그림 3〕.

4.2 정보보호 관리체계, 클라우드 제도 비교 분석

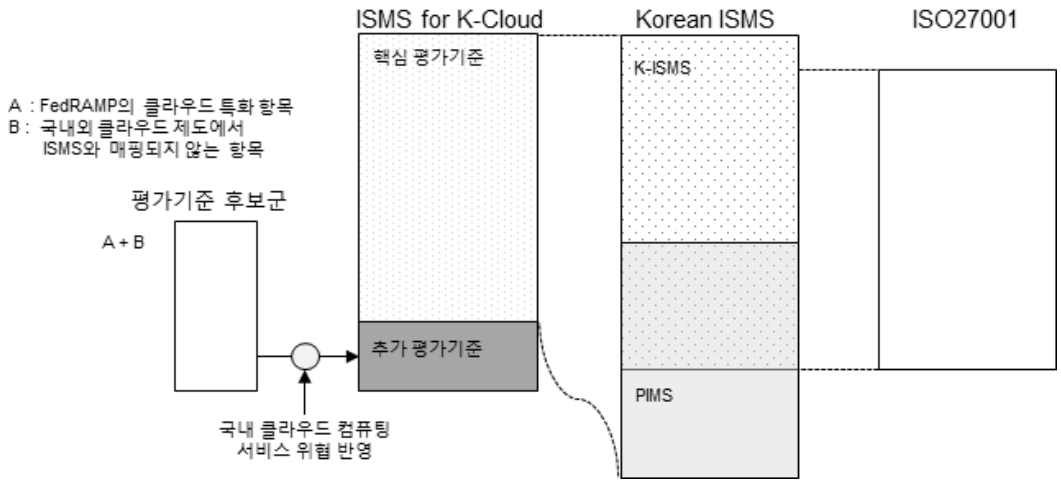
K-ISMS는 ISO27001을 모두 포함하는 정보보호 관리체계이므로 클라우드 통제 항목과 비교는 K-ISMS를 대상으로 한다. 또한 K-ISMS에 포함되지 않은 PIMS 통제 항목을 추가한다. 18개의 통제 항목과 3장에서 소개한 가트너, CSA-CCM, ENISA 및 한국 클라우드 인증, KISA 안내서에서 요구하는 보안 요구사항의 항목을 비교 분석한 결과는 〔표 5〕와 같다.



〔그림 3〕 정보보호 관리체계 매핑도

〔표 5〕 정보보호 관리체계와 클라우드 인증, 가이드라인 비교

분류	통제 항목	정보보호 관리체계		
		ISO27001	K-ISMS	PIMS
가트너	권한 사용자 접근	접근통제	접근통제	기술적 보호조치
	규정 준수	컴플라이언스	검토,모니터링및감사	생명주기 준거 요구사항
	데이터 위치	-	-	-
	데이터 분리	통신및운영관리	암호통제	기술적 보호조치
	복구	물리적/환경적 보호 업무연속성관리	물리적 보안 업무연속성관리	물리적 보호조치
	조사지원	-	-	-
	장기간 생존성	-	-	-
CSA-CCM	컴플라이언스	컴플라이언스	검토,모니터링및감사	생명주기 준거 요구사항
	데이터 통제	통신및운영관리	운영관리	기술적 보호조치
	보안 설비	물리적/환경적 보호	물리적 보안	물리적 보호조치
	인적 관리	인적자원보호	외부자보안 인적보안	인적보안
	정보 보안	통신및운영관리 접근통제 정보보호 사고관리	운영관리 접근통제 보안사고 관리	기술적 보호조치
	법규 준수	보호 정책	정보보호 정책	개인정보보호 정책
	운영 관리	통신및운영관리	운영관리	기술적 보호조치
	위험 관리	접근통제 시스템 인수,개발및유지보수	접근통제 시스템개발보안	기술적 보호조치
	공표 관리	시스템 인수,개발및유지보수	시스템개발보안	기술적 보호조치
	사고 복구	물리적/환경적 보호 업무연속성관리	물리적 보안 업무연속성관리	물리적 보호조치
	보안 아키텍처	통신및운영관리 접근통제 시스템 인수,개발및유지보수	운영관리 시스템개발보안 접근통제	기술적 보호조치
ENISA	인적 보안	인적자원보호	인적보안	인적보안
	공급망 보증	보호정책 통신및운영관리	외부자보안	-
	운영 보안	통신및운영관리	운영관리	기술적 보호조치
	식별 및 접근 관리	접근통제	접근통제	기술적 보호조치
	자산 관리	자산관리	정보자산 분류	개인정보 분류
	데이터와 서비스 이식성	-	-	-
	업무 연속성 관리	업무연속성관리	업무연속성관리	-
	물리적 보안	물리적/환경적 보호	물리적 보안	물리적 보호조치
	환경 통제	물리적/환경적 보호	물리적 보안	물리적 보호조치
	법규 요구사항	컴플라이언스	검토,모니터링및감사	생명주기 준거 요구사항
	법규 권고사항	컴플라이언스	검토,모니터링및감사	생명주기 준거 요구사항
	유럽 위원회에 법규 권고사항	-	-	-
한국 클라우드 인증	가용성	-	-	-
	확장성	-	-	-
	성능	-	-	-
	데이터 관리	자산관리 통신및운영관리	정보자산 분류 운영관리	개인정보 분류 기술적 보호조치
	보안	전 항목	전 항목	생명주기 준거 요구사항 제외한 전 항목
	서비스 지속성	시스템 인수,개발및유지보수	시스템개발보안	-
	서비스 지원	통신및운영관리	운영관리	기술적 보호조치
KISA 안내서	서비스 보안정책	보호정책	정보보호 정책	개인정보보호 정책
	보안조직 운영 및 인력보안	정보보호조직 인적자원보호	정보보호 조직 외부자보안 인적보안	개인정보보호 조직 인적보안
	자산분류와 통제	자산관리	정보자산 분류	개인정보 분류
	서비스 사고 관리절차 수립	정보보호 사고관리	보안사고 관리	침해사고 처리및대응절차
	서비스 연속성	업무연속성관리	업무연속성관리	-
	컴플라이언스	컴플라이언스	검토,모니터링및감사	생명주기 준거 요구사항
	물리적 보안	물리적/환경적 보호	물리적 보안	물리적 보호조치
	통신 및 운영	시스템 인수,개발및유지보수 통신및운영관리	시스템개발보안 암호통제, 운영관리 전자거래보안	기술적 보호조치
	기술적 보안	접근통제	접근통제	기술적 보호조치



〔그림 4〕 평가 기준 도출 방법

V. 평가 기준 도출

5.1 방법론

평가 기준을 도출하는 방법은 두 가지로 요약된다.

첫 번째 3.1.2 장에서 소개한 바와 같이 Fed-RAMP의 통제 항목 도출 시 적용하였던 미국의 방법론을 이용한다. FedRAMP에서 준용한 SP800-53과 같은 역할을 하는 통제 항목 리스트가 국내에서는 K-ISMS와 PIMS로 볼 수 있다. 추가적으로 클라우드에 특화된 통제 항목을 도출하기 위해서 Fed-RAMP의 클라우드 특화 항목(그림 4의 A)과 국내·외 클라우드 제도에서 정보보호 관리체계 통제 항목과 매핑되지 않은 항목(그림 4의 B)을 합하여 클라우드에 특화된 추가 평가 기준 후보군으로 도출할 수 있다. 이러한 방법론을 통해 한국형 클라우드 평가 기준에 적용할 핵심 평가 기준과 추가 평가 기준 후보군을 도출한다.

두 번째 추가 평가 기준 후보군에 다시 국내 클라우드 컴퓨팅 서비스 위협을 반영하여 최종 추가 평가 기준을 도출하게 된다[19]. 최종 추가 평가 기준 도출 방법론은 추가 평가 기준 후보군을 국제 공통평가기준(CC) 2, 3부(ISO/IEC 15408-2, 3)제공하는 보안 기능 요구사항 및 보증 요구사항으로 보아 보호 프로파일(PP) 개발 방법론을 적용할 수 있다[20].

5.2 핵심 평가 기준

핵심 평가 기준은 K-ISMS의 15가지 항목과 PIMS의 생명주기 준거 요구사항 3가지 항목(개인정보 수집, 개인정보 이용 및 제공, 개인정보 관리 및 파기)을 모두 선정한다. 국내에서는 2013년 2월부터 K-ISMS 인증제도가 의무화되었기 때문에 K-ISMS 인증을 받은 기업의 경우 추가적인 평가 기준만을 고려할 수 있도록 개발하기 위해서라도 K-ISMS의 15개 항목을 우선 핵심 평가 기준으로 선정하고 추가적으로 PIMS인증을 받은 기업을 고려하기 위하여 K-ISMS와 중복되지 않은 생명주기 준거 요구사항 3가지 항목을 추가적으로 핵심 평가 기준으로 선정하여 총 18가지 항목이 핵심 평가 기준이 된다.

5.3 추가 평가 기준 후보군

FedRAMP의 클라우드 특화 항목 46개 가운데 ISO27001과 항목이 중복되는 요소를 제외한 41개의 항목으로 재분류하였다. 추가적으로 국내·외 클라우드 관련 표준 및 가이드라인에 존재하는 통제 항목 가운데 정보보호 관리체계 통제 항목과 중복되는 요소를 제외한 항목을 합쳐 한국형 클라우드를 위한 정보보호 관리체계 평가 기준 후보군으로 놓는다〔표 6〕.

〔표 6〕 한국형 클라우드를 위한 추가 평가 기준 후보군

분야	평가 기준	내용	비고
접근 통제 강화	접근 권한 강화	역할(Role) 기반 접근 통제(RBAC)를 통해 권한 할당을 수행한다.	AC-2(7), AC-3(3)
	무선 접근 모니터링	비인가된 무선 연결을 통한 시스템 접근을 모니터링하고 적절한 조치를 취한다.	AC-18(2)
	세션 잠금	시스템을 일정 시간 미 사용시 세션 잠금 매커니즘을 사용하여 화면을 대체해야 한다.	AC-11(1)
	접근 제한의 자동화 매커니즘	자동화 매커니즘을 통해 개발자 등이 H/W, S/W, F/W를 직접적으로 변경하는 권한을 제한해야 한다.	CM-5(1), CM-5(5)
	미인가 디바이스 접근시 자동화 매커니즘을 통한 탐지	자동화 매커니즘을 통해 비인가된 컴포넌트/디바이스를 시스템에 추가, 접근시 탐지해야 한다.	CM-8(3)
감사 및 백업 강화	감사 기록, 분석, 백업 강화	의심 행위에 대한 조사 등을 지원하기 위하여 감사 기록의 분석 시 연관관계를 분석하고 다른 매체에 감사 기록을 백업한다.	AU-6(1), AU-6(3), AU-9(2)
	백업 복사본 저장	운영체제, 주요시스템 S/W등의 백업 복사본을 저장한다.	CP-9(3)
인증 및 식별 관리 강화	부인 방지 강화	이메일 SaaS를 포함한 서비스 주문을 위해 클라우드 서비스 제공자는 검증된 전자서명을 구현한다.	AU-10(5)
	식별자 관리	유일하게 사용자를 구별하기 위하여 사용자 식별자를 관리한다.	IA-4(4)
	인증자 관리	접근된 정보의 민감도 분류에 따라 인증자를 보호해야 한다.	IA-5(6), IA(7)
암호 통제 강화	스토리지 정보 암호화	스토리지내 정보를 암호화하여 보호해야 한다.	MP-4(1)
	검증된암호사용및관리	검증된 암호를 사용하여 데이터를 보호한다.	SC-12(2,5), SC-13(1)
취약점 평가 및 관리	취약점 분석 평가	취약점 제거를 위하여 모의해킹 등 취약점 분석·평가 계획 및 수행한다.	CA-7(2)
	취약점 점검 관리	자동화된 도구를 이용하여 신규 취약점을 식별하고 관리한다.	RA-5(2,3,5,6,9)
	개발자 보안 테스팅	개발자에게 코드 분석 도구를 사용하여 취약점을 진단하고 분석된 결과를 문서화할 것을 요구한다.	SA-11(1)
프로그램 관리	승인받은 프로그램 리스트 유지	공인된 인가 프로그램 리스트를 정의하고 유지한다.	CM-2(5)
	관리 프로그램	ISMP(Information Security Management Program)가 개발, 문서화, 승인, 구현되어야 한다.	CSA-CCM IS-01
데이터 관리	매체 분류 강화	중요 정보를 저장하고 있는 매체를 분류한다.	MP-6(4)
	자원 우선순위	우선 순위에 따라 자원 사용을 제한한다.	SC-6
운영 관리 강화	경계 보안	내부 통신 트래픽 및 외부 네트워크는 공인되어야 한다.	SC-7(8,12,13,18)
	신뢰 경로	사용자와 보안 가능 간에 신뢰된 통신 경로를 구성한다.	SC-11
	시스템 인수	CC제품을 도입하고 없는 경우 보안성 검토 등을 수행하여 한정된 기간 운영한다.	SA-4(7)
	아웃소싱 또는 인수 전 위험 평가 수행	시스템을 아웃소싱하거나 시스템을 인수하기 전에 위험 평가를 수행한다.	SA-9(1)
가상화 보안	가상화 기술	서로 다른 컴포넌트, 구성이 다른 컴포넌트에 대해 가상화 기술을 사용한다.	SC-30
	확장성	클라우드 서비스 제공자는 클라우드 서비스 수요에 유연하게 자원을 확장하여 제공해야 한다.	한국 클라우드서비스인증
	구성 설정의 자동화 매커니즘	자동화 매커니즘을 통해 구성 설정을 관리, 적용, 검증해야 한다.	CM-6(1)
비상 대응	비상 시 필요한 용량 계획 수행	비상 운영 시 정보 프로세싱, 통신, 환경 지원을 위하여 용량 계획을 수행한다.	CP-2(2)
	침해사고 대응을 위한 조직 구성	침해사고 대응을 위한 조직, 체계를 수립하고 외부의 서비스 제공자와 비상연락망을 유지한다.	IR-7(2)
법규 준수	데이터 위치	클라우드 고객 데이터가 저장된 국가, 위치 등을 파악하여 계약서 상에 명시하여 법적 문제 발생 시 재판 관할권 등에 따른 불이익을 최소화해야 한다.	가트너
	조사 지원	다수 고객의 데이터, 로그가 공존하므로 e-디스커버리, 포렌식 조사를 지원한다.	가트너
가용성	장기간 생존성	클라우드 서비스 제공자가 폐업, 인수·합병 시 고객 데이터의 가용성을 보장해야 한다.	가트너
	데이터와 서비스 이식성	데이터를 이식하기 위한 API, API인터페이스, 절차는 표준을 준수하여 문서화,구현,테스트되어야 한다.	ENISA
	가용성	클라우드 서비스 제공자는 약정된 내용의 가용성을 보장해야 한다. (예, 99.99% 가동율)	한국 클라우드서비스인증
성능	서비스의 품질	클라우드 서비스 제공자는 서비스의 품질(속도)을 보장하기 위해 적절한 성능을 유지해야 한다.	한국 클라우드서비스인증

VI. 평가 기준 제안

본 장에서는 5장에서 도출한 평가 기준 후보군에 국내 클라우드 업무 환경을 적용하여 한국형 클라우드를 위한 평가 기준을 제안한다. 제안 절차는 정보보호 시스템 공통평가기준(Common Criteria)을 통해 보호 프로파일(Protection Profile) 개발 시 보안 요구사항을 도출하는 방법론을 준용한다.

6.1 자산 식별

클라우드 컴퓨팅의 NIST 정의 표준(SP800-145)에서는 클라우드 서비스를 3가지로 모델로 구분한다. 소프트웨어(SaaS ,Software as a Service), 플랫폼(PaaS, Platform as a Service), 인프라(IaaS, Infrastructure as a Service) 서비스 모델로 각 모델에 따라 클라우드의 자산 구성이 달라질 수 있다. 클라우드 서비스 제공자는 고객이 소유한 IT 자원을 효율적으로 이용할 수 있도록 데이터 유출·노출을 방지하기 위해 자산을 정확히 파악해야 한다. 본 논문에서는 한국형 클라우드 컴퓨팅 환경의 자산을 방통위·KISA의 클라우드 서비스 정보보호 안내서를 토대로 〔표 7〕와 같이 분류하였다.

〔표 7〕 국내 클라우드 자산

구분	자산 영역
SaaS	응용 S/W, 게스트 운영체제, S/W 개발 플랫폼, API, 데이터베이스, 물리적 공간 및 설비, 네트워크 인프라 및 보안장치, 서버 시스템
PaaS	게스트 운영체제, S/W 개발 플랫폼, API, 데이터베이스, 물리적 공간 및 설비, 네트워크 인프라 및 보안장치, 서버 시스템
IaaS	물리적 공간 및 설비, 네트워크 인프라 및 보안장치, 서버 시스템

6.2 보안 위협 도출

클라우드 서비스의 보안위협은 주체와 관점에 따라 다양한 방법으로 분류되고 있다. KISA 가이드라인은 가트너, NIST, CSA 등에서 제시하는 대표적인 보안 위협 분석사례에서 클라우드 서비스의 핵심 보안위협 6개를 도출하였다. 핵심 보안위협은 ①가상화 취약점(악성코드 및 서비스 가용성 침해),②정보위탁(소유와 관리분리)에 따른 정보 유출 위협, ③자원 공유 및 집중화에 따른 서비스 장애, ④단말 다양성에 따른 정보 유출, ⑤분산 처리에 따른 보안 적용의 어려움, ⑥법규 및 규제의 문제 이다. 마찬가지로 금융부문 클라우드 보안 가이드라인[21]에서는 가트너, RSA, CSA, ENISA 등에서 제시하는 대표적 보안 위협 사례를 통해 3개의 대분류와 10개의 위협항목을 도출하였다. 위협항목은 ①데이터 손실 및 유출 위협, ②데이터 변조위협, ③인증 및 권한관련 위협, ④시스템 및 네트워크 보안위협, ⑤시스템 악용위협, ⑥가상머신 보안위협, ⑦보안수준 보장 및 사고대응의 어려움, ⑧서비스 장애위험, ⑨통합정책 관리의 어려움, ⑩법령 및 규정의 준수 이다. 신경아(2012)는 클라우드의 4가지 근원적 위협을 위탁/제공, 적용기술, 자원공유, 데이

〔표 8〕 국내 클라우드 위협

국내 클라우드 보안 위협			ISMS
정보보호 안내서(KISA)	금융부문 가이드라인	신경아 (2012)	
가상화 취약점	가상머신 보안위협	데이터 센터의 위치(가상화 기술로 인한 위협)	×
정보위탁(소유와 관리분리)에 따른 정보 유출 위협	보안수준 보장 및 사고대응의 어려움 데이터 손실 및 유출 위협	SLA/계약 분쟁 위협 데이터 보안 위협	△
자원 공유 및 집중화에 따른 서비스 장애	서비스 장애위험	자원 공유 가용성 침해 위협	△
분산 처리에 따른 보안 적용의 어려움	통합정책 관리의 어려움 인증 및 권한관련 위협	접근 통제 우회 위협	△
법규 및 규제의 문제	법령 및 규정의 준수	법 규제의 이탈 위협	△
단말 다양성에 따른 정보 유출			△
	시스템 및 네트워크 보안위협		○
	시스템 악용위협		○
	데이터 변조위협		○
		웹 인터페이스 위협	○
		관리적 보안위협	○

○ 충족, △ 부분충족, × 미충족

터센터의 배치로 분류하고 근원적 위협에서 파생된 9가지 위협을 분류하였다[22]. 9가지 위협소분류는 ①데이터 보안위협, ②관리적 보안위협, ③SLA/계약 분쟁 위협, ④가용성 침해 위협, ⑤자원 공유, ⑥데이터센터의 위치, ⑦웹 인터페이스 위협, ⑧접근 통제 우회 위협, ⑨법 규제의 이탈 위협 이다.

이 외에도 김지연(2009)[23], 최주영(2010)[24], 김정훈(2010)[25], 장은영(2011)[26]의 연구에서 제시하고 있는 클라우드 환경에서의 보안 위협을 참고하였다.

본 논문에서 도출하여야 할 위협은 K-ISMS, ISO27001, PIMS의 정보보호 관리체계에서 커버하지 못했던 위협을 국내 환경에 맞게 분류하는 것이다. 클라우드 서비스의 취약점 및 사고발생 사례를 통해 국내 환경에 맞는 위협을 도출해야 하지만 구글, 마이크로소프트, 아마존, 애플 등의 외국 클라우드 서비스 제공자의 장애, 알려지지 않은 사고, 법적 분쟁 사례 외에 국내 클라우드 서비스 제공자의 취약점 및 사고 사례는 경미한 수준이다. 아직 국내 클라우드 서비스 시장이 활성화되지 못한 것에 기인한다. 따라서 3가지의 국내에서 적용이 가능한 보안 위협 분류의 중복 항목을 제거하고 정보보호 관리체계의 통제 항목에 충족되지 않거나, 부분 충족되는 항목([표 8]의 ×, △)들을 분류하여 이를 기반으로 기존 정보보호 관리체계에서 대응할 수 없는 위협 영역을 [표 9]과 같이 도출하였다.

[표 9] 보안 위협 도출

위협	내용
가상화 보안 위협	악성코드 감염 및 상속 위협 하이퍼바이저 감염 시 게스트OS로 상속
데이터 보안 위협	정보의 소유/관리 분리로 인한 정보 유출 사용 단말의 다양화에 따른 정보 유출
법 규제 문제	데이터의 위치에 따른 책임 소재 외국에 서버를 둔 경우 재판 관할권에 따른 법규 상이
접근 통제 정책 관리 위협	분산 환경으로 인한 보안 적용 오류 자원 공유로 접근 통제 우회 위협
서비스 장애	서비스 복구가 서비스 제공자에 의존 자원의 집중화로 인한 디도스 공격 등 위협

6.3 보안 목적 정의

클라우드 자산에 대한 보안 목적은 정보보호 관리체계 인증을 받은 클라우드 서비스 제공자가 기존 정보보호 관리체계의 관리 영역을 벗어난 보안 위협에 대응하기 위한 보안적인 목적으로 [표 10]과 같이 분류되어 정의된다. [표 11]에서는 보안 목적과 보안 위협의 대응 관계를 통해 도출된 보안 목적의 타당성에 대한 이론적 근거를 제시한다.

[표 10] 위협을 해결하기 위한 보안 목적

보안 목적	내용
가용성	클라우드 자산은 장애 또는 공격 발생 시 최소한의 보안 기능을 유지하여 정상적인 서비스를 제공해야 한다.
식별 및 인증	클라우드 자산은 접근을 허용하기 전 사용자를 유일하게 식별 및 인증해야 한다.
조사 지원	클라우드 자산의 법적 책임 문제 발생 시 법, 규정에 맞게 조사를 지원해야 한다.
관리	클라우드 자산은 인가된 관리자가 고객의 정보를 효율적으로 안전하게 관리할 수 있는 수단을 제공해야 한다.
저장 데이터 보호	클라우드 자산에 저장된 정보를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.
가상화 보안	클라우드 자산은 가상화 기술 적용에 따라 취약점이 상속되지 않도록 취약점을 제거하고 점검해야 한다.

[표 11] 위협과 보안목적의 대응

위협 \ 보안목적	가용성	식별 및 인증	조사 지원	관리	저장 데이터 보호	가상화 보안
가상화 보안 위협						×
데이터 보안 위협					×	
법 규제 문제			×			
접근 통제 정책 관리		×		×		
서비스 장애	×					

6.4 보안 요구사항 도출

보안 요구사항은 기술 영역의 보안기능 요구사항과 운영·관리 영역의 환경적 요구사항으로 나누어진다. 5장에서 도출한 추가 평가 기준 후보군은 기술, 운영, 관리의 3개의 클래스로 구분되어 이 가운데 기술 클래스는 보안 기능 요구사항으로 운영과 관리 클래스는

〔표 12〕 보안 요구사항 도출

구분	분야	평가 기준	클래스
보안 기능 요구 사항	접근 통제 강화	접근 권한 강화	기술
		무선 접근 모니터링	
		세션 잠금	
		접근 제한의 자동화 매커니즘	
		미인가 디바이스 접근시 자동화 매커니즘을 통한 탐지	
	감사 및 백업 강화	감사 기록, 분석, 백업 강화	
		백업 복사본 저장	
	가상화 보안	가상화 기술	
		확장성	
		구성 설정의 자동화 매커니즘	
환경적 요구 사항	취약점 분석 및 관리	취약점 분석 평가	관리
		취약점 점검 관리	
		개발자 보안 테스팅	
	프로그램 관리	승인받은 프로그램 리스트 유지	
		관리 프로그램	
	데이터 관리	매체 분류 강화	
		자원 우선순위	
	법규 준수	데이터 위치	
		조사 지원	
	가용성	장기간 생존성	운영
		데이터와 서비스 이식성	
		가용성	

보안기능 요구사항으로 나눌 수 있다. 이와 같은 과정을 통해 22개의 보안 요구사항이 도출되었다. 〔표 12〕은 보안 요구사항을 제시하고 있으며 〔표 13〕은 〔표 12〕에서 도출한 보안 요구사항이 보안목적을 충족하는지 이론적 근거를 제시한다.

6.5 최종 추가 평가 기준 도출

6.4장에서 도출된 22개의 보안 요구사항 가운데 기존 정보보호 관리체계 평가 기준의 항목으로 통합될 수 있는 항목이 존재하므로 유사 항목을 재분류하여 최종 추가 평가 기준을 도출하였다. 도출된 평가 기준은 클라우드 서비스 제공자가 K-ISMS, ISO27001, PIMS 등의 기존 정보보호 관리체계 인증 기업이더라도 추가적으로 고려해야 할 평가 기준이 된다.

본 논문은 추가로 도출된 "가상화 보안, 취약점 분석 및 관리, 가용성" 의 3개 분야와 기존 K-ISMS의 15개 통제 분야 가운데 "접근 통제, 검토,모니터링 및 감사" 의 2개 분야에 세부 항목을 추가하여 한국형 클라우드를 위한 정보보호 관리체계 최종 평가 기준을 〔표 14〕와 같이 제안한다.

〔표 13〕 보안 요구사항의 이론적 근거

보안 요구사항 \ 보안 목적	가용성	식별 및 인증	조사 지원	관리	저장 데이터 보호	가상화 보안
접근 통제 강화		×				
감사 및 백업 강화			×			
가상화 보안						×
취약점 평가 및 관리						×
프로그램 관리				×		
데이터 관리					×	
법규 준수			×	×		
가용성	×					

VII. 결 론

본 논문은 클라우드 컴퓨팅 서비스 활성화 및 보안 및 신뢰를 보증하기 위하여 국내·외에서 시행중인 인증제도 및 가이드라인을 비교 분석하여 국내에서 적용이 가능한 평가 기준을 도출하였다. 방송통신위원회에서 도입한 클라우드 서비스 인증 및 안전행정부를 중심으로 추진 중인 공공부문의 클라우드 제도는 국내에서도 이미 클라우드 서비스 활성화를 위해 보안과 신뢰 향상을 위해 본격적으로 정보보증체계를 마련하고 있음을 반영한다. 국내에서는 K-ISMS가 의무화되어 국내 많은 기업이 정보보호 관리체계 인증을 받게될 것이다. 하지만 클라우드 서비스 제공자가 고객을 대상으로 높은 수준의 신뢰를 주기 위해서는 K-ISMS 이상의 보증 수준이 필요하다. 미국은 인증&인가 제도인 FedRAMP를 통해 정보보증 수준을 높이고 연방정부의 클라우드 서비스 활성화를 촉진시키고 있다. 본 논문을 통해 도출한 평가 기준으로 고객의 정보보호에 대한 신뢰수준을 높여 클라우드 서비스 활성화에 기여할 수 있기를 기대한다.

〔표 14〕 한국형 클라우드를 위한 정보보호 관리체계 평가 기준

핵심 평가 기준	1. 정보보호 정책, 2. 정보보호 조직, 3. 외부자 보안, 4. 정보자산 분류, 5. 정보보호 교육 및 훈련, 6. 인적 보안, 7. 물리적 보안, 8. 시스템 개발 보안, 9. 암호 통제			
	10	접근 통제	접근 권한 강화	역할(Role) 기반 접근 통제(RBAC)를 통해 권한 할당을 수행한다.
			무선 접근 모니터링	비인가된 무선 연결을 통한 시스템 접근을 모니터링하고 적절한 조치를 취한다.
			세션 잠금	시스템을 일정 시간 미 사용시 세션 잠금 매커니즘을 사용하여 화면을 대체해야 한다.
			접근 제한의 자동화 매커니즘	자동화 매커니즘을 통해 개발자 등이 H/W, S/W, F/W를 직접적으로 변경하는 권한을 제한해야 한다.
			미인가 디바이스 접근 시 자동화 매커니즘을 통한 탐지	자동화 매커니즘을 통해 비인가된 컴포넌트/디바이스를 시스템에 추가, 접근시 탐지해야 한다.
	11. 운영 관리, 12. 전자거래 보안, 13.보안사고 관리			
	14	검토,모니터링 및 감사	감사 기록, 분석, 백업 강화	의심 행위에 대한 조사 등을 지원하기 위하여 감사 기록의 분석 시 연관관계를 분석하고 다른 매체에 감사 기록을 백업한다.
			백업 복사본 저장	운영체제, 주요시스템 S/W등의 백업 복사본을 저장한다.
			데이터 위치	클라우드 고객 데이터가 저장된 국가, 위치 등을 파악하여 계약서 상에 명시하여 법적 문제 발생 시 재판 관할권 등에 따른 불이익을 최소화해야 한다.
			조사 지원	다수 고객의 데이터, 로그가 공존하므로 e-디스커버리, 포렌식 조사를 지원한다.
	15. 업무 연속성 관리			
	16. 개인정보 수집, 17. 개인정보 이용 및 제공, 18 개인정보 관리 및 파기			
추가 평가 기준	19	가상화 보안	가상화 기술	서로 다른 컴포넌트, 구성이 다른 컴포넌트에 대해 가상화 기술을 사용한다.
			확장성	클라우드 서비스 제공자는 클라우드 서비스 수요에 유연하게 자원을 확장하여 제공해야 한다.
			구성 설정의 자동화 매커니즘	자동화 매커니즘을 통해 구성 설정을 관리, 적용, 검증해야 한다.
	20	취약점 분석 및 관리	취약점 분석 평가	취약점 제거를 위하여 모의해킹 등 취약점 분석·평가 계획 및 수행한다.
			취약점 점검 관리	자동화된 도구를 이용하여 신규 취약점을 식별하고 관리한다.
			개발자 보안 테스팅	개발자에게 코드 분석 도구를 사용하여 취약점을 진단하고 분석된 결과를 문서화할 것을 요구한다.
	21	가용성	장기간 생존성	클라우드 서비스 제공자가 폐업, 인수·합병 시 고객 데이터의 가용성을 보장해야 한다.
			데이터와 서비스 이식성	데이터를 이식하기 위한 API, API인터페이스, 절차는 표준을 준수하여 문서화,구현,테스트되어야 한다.
			가용성	클라우드 서비스 제공자는 약정된 내용의 가용성을 보장해야 한다. (예. 99.99% 가동율)

참고문헌

〔1〕 Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," NIST SP800-145, Sep 2011.

〔2〕 Daryl C. Plummer, Thomas J. Bittman, Tom Austin, David W. Cearley, and David Mitchell Smith, "Cloud Computing: Defining and Describing an Emerging Phenomenon," Gartner, Jun 2008.

〔3〕 유우영, 임종인, "클라우드 컴퓨팅 서비스 제공자의 개인정보보호 조치방안에 대한 연구," 정보보학회 논문지, 제22권 제2호, pp.337~346, 2012년 4월

〔4〕 서광규, "클라우드 서비스 인증제도 수립을 위한 프레임워크," 정보화정책 제18권 제1호, pp.24-44, 2011년 봄호.

〔5〕 유수상, "클라우드 컴퓨팅 현황과 활성화 과제," 금융결제원 지급결제와 정보기술 제43호, pp.31-54, 2011년 1월.

〔6〕 Jon Brodkin, "Gartner:Seven Cloud-computing security risks," Network world, Jul 2008.

〔7〕 TechAmerica Foundation, "Cloud First, Cloud Fast: Recommendations for Innovation, Leadership and Job Creation," Cloud^2 Commission Report ,Jul 2011.

〔8〕 M. Almorsy, J. Grundy, and A. S. Ibrahim, "Collaboration-based cloud computing security management framework," Proceedings - 2011 IEEE 4th International Conference on Cloud Computing (CLOUD), pp364-371, 2011.

〔9〕 S Ristov, M Gusev, and M Kostoska, "A New Methodology for Security Evaluation in Cloud Computing," MIPRO, 2012 Proceedings of the 35th International Convention, pp.1484-1489, 2012.

〔10〕 Jay heiser and Mark Nicolett, "Assessing the Security Risks of Cloud Computing," Gartner Report, June 2008.

〔11〕 FedRAMP(The Federal Risk and Authorization Management Program), http://www.gsa.gov/portal/category/102371

〔12〕 신종회, "클라우드 보안 인증 스킴과 해결과제," 정보보호학회지, 제22권 제6호, pp29-33, 2012년 10월

〔13〕 CSA(cloud security alliance), "Security guidance for critical areas of focus in cloud computing v3.0," https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf, 2011.

〔14〕 CSA_CCM(v.1.3) https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v1.3.xlsx 2012.

〔15〕 ENISA, "Benefits, Risks and Recommendations for Information Security," Cloud Computing, Nov 2009.

〔16〕 한국 클라우드서비스협회 클라우드서비스 인증사무국, http://www.excellent-cloud.or.kr/

〔17〕 방통통신위원회, 한국인터넷진흥원, "클라우드 서비스 정보보호 안내서," KISA 안내.해설 제2011-8호, 2011년 10월.

〔18〕 한국인터넷진흥원, "정보보호관리체계 안내서," KISA 안내·해설 제2010-21호, 2010년 1월.

〔19〕 김기철, 김승주, "K-ISMS기반의 한국형 스마트그리드 정보보호 관리체계 평가 기준 제안," 정보보호학회논문지, 제22권 제6호, pp.1375-1392, 2012년 12월.

〔20〕 CCMB-2009-07-001~003, "정보보호시스템 공통평가기준," 개정3판, 2009년 7월.

〔21〕 금융보안연구원, 금융부문 클라우드컴퓨팅 보안가이드, 금보원 2010-11, 2010년 12월.

〔22〕 신경아, 이상진, "클라우드 컴퓨팅 서비스에 관한 정보보호 관리체계," 정보보호학회논문지, 제22권 제1호, pp.155-167, 2012년 2월.

〔23〕 김지연, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 환경의 가상화 기술 취약점 분석 연구," 정보보호학회지, 제19권 제4호, pp.72-77, 2009년 8월.

〔24〕 최주영, 김형종, 박춘식, 김명주, "클라우드 컴퓨팅 가상화 환경의 공격기법 분석," 정보과학화지, pp.75-81, 2010년 12월.

〔25〕 김정훈, 황용석, 김성현, 조시행, "클라우드 컴퓨팅 기반의 악성코드 대응 방법 및 사례," 정보보호학회지, 제20권 제2호, pp.51-55, 2010년 4월.

〔26〕 장은영, 김형종, 박춘식, 김주영, 이재일, "모바일 클라우드 서비스의 보안위협 대응 방안 연구," 정보보호학회논문지, 제21권 제1호, pp.177-186, 2011년 2월.

〈著者紹介〉

김 기 철 (Kichul Kim) 학생회원
2001년 2월: 동국대학교 컴퓨터공학과 학사
2013년 2월: 고려대학교 정보보호대학원 석사
2002년 4월~현재: 금융결제원 재직 중
〈관심분야〉 금융보안, 디지털 포렌식, 정보보호관리체계, 보안성 평가

허 옥 (Ok Heo) 학생회원
2007년 8월: 단국대학교 경영학과 학사
2010년 1월~현재: 엔씨소프트 재직 중
2011년 2월~현재: 고려대학교 정보보호대학원 정보보호학과 석사과정
〈관심분야〉 IT감사, 개인정보보호, 정보보호관리체계, 보안성 평가

김 승 주 (Seungjoo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년: KISA(舊한국정보보호진흥원) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2011년~현재: 고려대학교 정보보호대학원 정교수
2002년~현재: 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년~현재: 한국정보보호학회 이사
2005년~2006년: 교육인적자원부 유해정보차단 자문위원
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2007년~현재: 대검찰청 디지털수사 자문위원
2007년~2009년: 전자정부 서비스 보안위원회 사이버 침해사고대응 실무위원회 위원
2010년~현재: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: SK커뮤니케이션즈 보안강화 특별자문위원
2012년: 중앙선거관리위원회와 서울시장후보 홈페이지 사이버테러 특별검사 자문위원
〈관심분야〉 보안공학, 암호이론, 정보보증, 정보보호제품 보안성 평가, Usable Security