http://dx.doi.org/10.14400/JDPM.2014.12.1.405

클라우드 서비스 평가 프로그램과 ISO/IEC 27001:2013의 비교 연구

최주영*, 최은정**, 김명주*
서울여자대학교 정보보호학과*, 서울여자대학교 교양학부**

A Comparison Study between Cloud Service Assessment Programs and ISO/IEC 27001:2013

Ju-Young Choi*, Eun-Jung Choi, Myuhng-Joo Kim***
Dept. of Information Security, Seoul Women's University*
Dept. of General Education, Seoul Women's University**

요 약 IT 자원의 동적 확장과 비용절감이라는 클라우드 서비스의 장점은 IT 사용자의 관심이다. 그러나 클라우드 서비스의 신뢰성은 클라우드 서비스를 적극적으로 사용하는데 걸림돌이 되고 있다. 기존 클라우드 서비스의 평가 프로그램은 ISO/IEC 27001:2005을 참고하여 정보보호 평가 항목을 도출하고 클라우드 서비스 특징을 추가하는 방법으로 연구가 이루어지고 있다. 본 논문은 최근 발표된 ISO/IEC 27001:2013의 추가와 삭제 그리고 변경된 통제영역 및 통제 항목을 살펴본다. ISO/IEC 27001:2013의 통제 항목과 클라우드 서비스 평가 프로그램인 CSA CCM v.3, FedRAMP의 통제 항목을 비교 분석하여 정보보호관리체계에서 클라우드 서비스와 관련된 평가 항목을 제시한다. 도출한 통제 항목은 클라우드 서비스 기반의 정보보호관리체계를 운영하는 기업의 보안 정책에 참고 지표가 될 것이다.

주제어 : 클라우드 서비스 평가, ISO/IEC 27001:2013, 정보보호관리체계, CSA CCM v.3, FedRAMP

Abstract It is very important to IT users that the Cloud service provides dynamic extension of IT resources and cost-saving. However, the reliability for Cloud service hinders utilizing Cloud service actively. Existing studies on assessment program for Cloud Service are executed by extracting information security assessment articles and adding features of cloud services by referencing ISO/IEC 27001:2005. This paper will review the recently released ISO/IEC 27001:2013 for the addition, reduction, and changing of articles for Controls and Control objectives. Comparative analysis for the Controls of ISO/IEC 27001:2013 with those of CSA CCMv.3, FedRAMP which is an assessment program for Cloud service will suggest Control Objects of Information Security Management System for related Cloud service. The suggestion of Controls will be an important reference index for the security policy of companies which manage the information security management system based on Cloud service.

Key Words : Cloud Service Assessment, ISO/IEC 27001:2013, Information Security Management System, CSA CCM v.3, FedRAMP

* 이 논문은 2013학년도 서울여자대학교 교내학술특별연구비의 지원을 받았음.
Received 1 December 2013, Revised 7 January 2014
Accepted 20 January 2014
Corresponding Author: Myuhng-Joo Kim (Seoul Women's University)
Email: mjkim@swu.ac.kr

ISSN: 1738-1916

1. 서론

클라우드 컴퓨팅은 가상화와 분산처리 기술을 기반으로 인터넷을 통해 대규모 IT자원을 임대하고 사용한 만큼의 요금을 지불하는 컴퓨팅 환경을 말한다[1]. 이를 기반으로 주문형 아웃 소싱 IT 서비스를 제공하는 클라우드 서비스의 관심이 높아지고 있다.

시장 조사 전문기관인 IDC(International Data Corporation)는 전 세계 퍼블릭 IT 클라우드 서비스에 대한 지출 규모가 2013년 474억 달러에 달하고 2017년에는 1,080억 달러에 이를 것으로 전망하고 있다[2]. 이는 2013년부터 2017년까지 퍼블릭 IT 클라우드 서비스가 연평균 23.5%로 성장할 것으로 예상한 것이다. 국내 시장규모는 2012년 2억3천만 달러에서 2014년 4억6천만 달러로 증가하며 연평균 47.6%의 성장률을 기록할 것으로 예상한다[3].

클라우드 서비스 사용자는 서비스를 도입하길 원하지만 클라우드 서비스의 신뢰성(보안 및 프라이버시, 가용성 및 업무연속성, 컴플라이언스, 시스템 간 통합의 어려움, 공급자 관리 등)에 대한 불안으로 결정하지 못하고 있다. 또한 클라우드 서비스 공급자는 시장 확보를 위하여 공인된 평가 시스템을 요구하고 있으며 이와 관련된 클라우드 서비스 평가 프로그램 연구가 진행 중에 있다.

클라우드 서비스 평가 프로그램은 기존 감사 프로그램 ISO/IEC(International Organization for Standardization and International Electrotechnical Commission) 27001[4], AICPA(American Institute of CPAs) SOC(Service Organization Control)[5], PCI(Payment Card Industry)-DSS(Data Security Standard)[6], ISACA(Information Systems Audit and Control Association) Cloud IT Audit [9]에 클라우드 컴퓨팅 분야의 평가 항목을 추가한 평가 프로그램과 클라우드 컴퓨팅을 특화한 서비스 평가 프로그램으로 FedRAMP(Federal Risk and Authorization Management Program)[7], CSA OCF(Cloud Security Alliance Open Certification Framework Vision Statement) [8], KCSA(Korea Cloud Service Alliance) 클라우드 서비스 인증[10] 등이 있다.

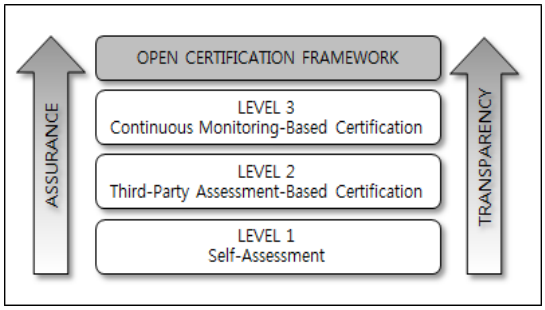
최근 정보보호관리체계의 국제 표준 ISO/IEC 27001은 ISO/IEC 27001:2005 문서의 구조, 요구사항, 통제 영역, 통제 목적 그리고 통제 항목의 내용이 일부 삭제 및 수정 보완하여 2013년 10월 발표되었다. 발표된 ISO/IEC 27001:2013은 ISO/IEC 27001:2005 발표 이후 8년 만에 제정된 것으로 IT 시장의 변화가 어느 정도 반영된 정보보호관리체계 일 것으로 예상된다. 또한 정보보호관리체계 표준을 따른 기존 정보보호 분야의 감사 프로그램 변화에 큰 영향이 미칠 것으로 예상된다.

본 논문은 기존 클라우드 서비스 평가 프로그램 가운데 CSA OCF와 FedRAMP을 살펴보고 발표된 ISO/IEC 27001:2013의 추가와 삭제 그리고 변경된 통제영역 및 통제 항목을 분석했다. 클라우드 서비스 평가 프로그램인 CSA CCM(Cloud Controls Matrix)v.3 문서를 기준으로 ISO/IEC 2701:2005와 ISO/IEC 27001:2013을 비교 연구하여 클라우드 환경이 정보보호관리체계에 어느 정보 반영되었는지 확인하였다. 그리고 ISO/IEC 27001:2013를 기준으로 클라우드 서비스 평가 프로그램 두 개를 비교 분석하여 정보보호관리체계 가운데에서 클라우드 서비스와 관련된 평가 항목의 발전방향에 대하여 제안한다.

2. 기존 클라우드 서비스 평가 프로그램

2.1 CSA OCF(Open Certification Framework)

비영리단체인 클라우드 보안 협회(CSA, Cloud Security Alliance)에서 제정한 클라우드 보안 제어 프레임워크이다[Fig. 1]. CSA OCF는 3단계의 신뢰를 기반으로 구축되어 있으며, 각 단계는 클라우드 서비스 제공자의 운영에 대한 점진적인 가시성과 투명성 수준을 제공하고 클라우드 소비자에게 더 높은 수준의 보장을 제공한다.



[Fig. 1] CSA Open Certification Framework

1단계. 자체 평가 : 클라우드 제공자는 CSA 최적실무

(best practice)에 따른 컴플라이언스 상태를 보여주는 CAIQ(The Consensus Assessments Initiative Questionnaire)와 CCM 보고서를 제출한다.

2단계. 인증(제3자 평가) : CSA와 CCM을 통합한 ISO/IEC 27001이 인증을 한다. ISO/IEC 27001의 CCM에 명시된 기준을 기반으로 평가자가 장기적인 지속 가능성과 위험에 대비한 조직의 수행능력을 수치로 점수화하고 매년 개선 상황을 정량적으로 평가한다. CCM에 포함된 관리 원칙과 통제를 적용하여, 평가는 조직이 기존의 업무 관리체계를 향상시키고 업무 최적실무를 도입하는데 집중할 수 있도록 핵심 수행능력 개선의 기회를 제공하는데 중점을 두었다.

3단계. 지속적인 모니터링 기반 인증 : 현재 개발이 진행 중이며 지속적인 감사 증적 수집을 기반으로 소비자 요구사항을 충족하는지 여부를 거의 실시간으로 모니터링 하도록 구현하는 개념이다.

2.1.1 CSA CCM v.3 통제 영역

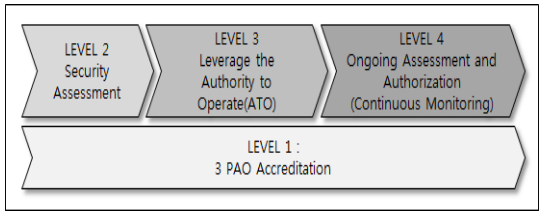
CSA OCF 2단계 중, '제3 기관에 의한 평가'에서 사용하는 평가 항목이다. 16개 통제 영역(Control Domain), 136개 통제 항목(Items)으로 구성된다<Table 1>. CSA CCM v.3은 Cobit, PCI-DSS, FedRAMP 등 국제 표준의 통제 항목 간의 대응 관계 정보를 제공한다.

〈Table 1〉 Control Domain of CSA CCM v.3

Control Domain (Symbol)	Items
1. Application & Interface Security (AIS)	4
2. Audit Assurance & Compliance (AAC)	3
3. Business Continuity Management & Operational Resilience (BCR)	12
4. Change Control & Configuration Management (CCC)	5
5. Data Security & Information Lifecycle Management (DSI)	8
6. Datacenter Security (DCS)	9
7. Encryption & Key Management (EKM)	4
8. Governance and Risk Management (GRM)	12
9. Human Resources (HRS)	12
10. Identity & Access Management (IAM)	13
11. Infrastructure & Virtualization Security (IVS)	12
12. Interoperability & Portability (IPY)	5
13. Mobile Security (MOS)	20
14. Security Incident Management E-Discovery & Cloud Forensics (SEF)	5
15. Supply Chain Management, Transparency and Accountability (STA)	9
16. Threat and Vulnerability Management (TVM)	3

2.2 FedRAMP

FedRAMP는 미국 연방정부에서 'Cloud First' 정책 실현을 위해 클라우드 서비스 인증을 간소화하고 서비스를 효율적으로 조달하려는 목적으로 운영하는 클라우드 서비스 평가 프로그램이다. 또한 3 PAO(Third Party Audit Organization) 외부 전문 평가 기관을 선정하여 일관성 있는 보안 평가 및 인증을 수행하고, 사후 관리에 관련된 모든 사항을 체계화하여 미 정부기관에 안전한 클라우드 서비스를 도입하기 위한 프로그램이다. FedRAMP 보안 평가 프로세스는 다음[Fig. 2]과 같다.



[Fig. 2] FedRAMP Security Assessment Process

1단계. 3 PAO 인가 : 클라우드 서비스 제공자에 대한 보안 평가를 위하여 미국 정부에서 공식 인증한 민간업체로 구성된 제3의 평가기관을 인증하는 단계이다. 3 PAO는 독립성, 고유의 방법론, 그리고 독립성을 가지고 있는지 자격요건을 평가하고 전문가검토위원회(ERB, Expert Review Board)에 의해 승인된다.

2단계. 보안 평가 : 미국 연방정부 기관에 클라우드 서비스를 제공하기 원하는 클라우드 서비스 제공자가 공동인가위원회(JAB, Join Authorization Board)에 FedRAMP 승인을 요구하는 단계이다. FedRAMP의 요구사항 및 통제 항목을 기준으로 3 PAO를 통해 보안 평가를 수행하고 보안 평가 보고서 및 관련 자료를 제출한다. 클라우드 서비스 제공자가 승인을 받게 되면 FedRAMP 보안 데이터베이스(Security Repository Database)에 클라우드 서비스 제공자 정보와 평가 결과를 업로드 한다.

3단계. 운영 권한 등급 : 미국 연방정부 기관에서 도입할 클라우드 서비스를 선정하는 단계이다. FedRAMP 보안 데이터베이스에서 클라우드 서비스 제공자 정보를 확인 및 검토하여 추가적인 요구사항의 경우 SLA를 통하여 클라우드 서비스 제공자를 선정한다.

4단계. 지속적인 평가 및 인증 : 승인 된 클라우드 서비스 제공자는 최소 연 1회 3 PAO를 통해 재평가를 받아

야 하는 지속적인 모니터링을 수행하는 단계이다. 클라우드 서비스에 변경사항이나 사고가 발생했을 경우 FedRAMP와 정부기관에 보고해야 한다.

2.2.1 FedRAMP 보호 통제 영역

FedRAMP 보안 평가 프로세스 2단계에서 사용한 평가 기준은 NIST(National Institute of Standards and Technology) 800-53 revision 3[11]의 중-하(Moderate-Low Level)급의 영향을 미치는 시스템상의 클라우드 서비스 통제 항목을 제시하였다.

FedRAMP 보호 통제 항목은 연방정보보안관리법(FISMA, Federal Information Security Management Act)에 따라 NIST가 개발한 연방 정보시스템 보안통제 장치 권고 문서 NIST 800-53 version 3에 기초한다. 또한 NIST 800-53 revision 3의 중-하(Moderate-Low Level)급 통제 항목 가운데 클라우드와 관계없는 부분은 배제하고 추가적으로 클라우드에서 필요한 부분들을 추가하여 제시하였다. 17개의 통제 영역(Control Domain), 168개의 통제 항목(Items)으로 구성된다<Table 2>.

〈Table 2〉 Control Domain of FedRAMP

Control Domain (Symbol)	Items
1. Access Control (AC)	17
2. Awareness and Training (AT)	4
3. Audit and Accountability (AU)	12
4. Security Assessment and Authorization (CA)	6
5. Configuration Management (CM)	9
6. Contingency Planning (CP)	9
7. Identification and Authentication (IA)	8
8. Incident Response (IR)	8
9. Maintenance (MA)	6
10. Media Protection (MP)	6
11. Physical and Environmental Protection (PE)	18
12. Planing (PL)	5
13. Personnel Security (PS)	8
14. Risk Assessment (RA)	4
15. System and Services Acquisition (SA)	12
16. System and Communication Protection (SC)	24
17. System and Inforation Integrity (SI)	12

3. ISO/IEC 27001:2013

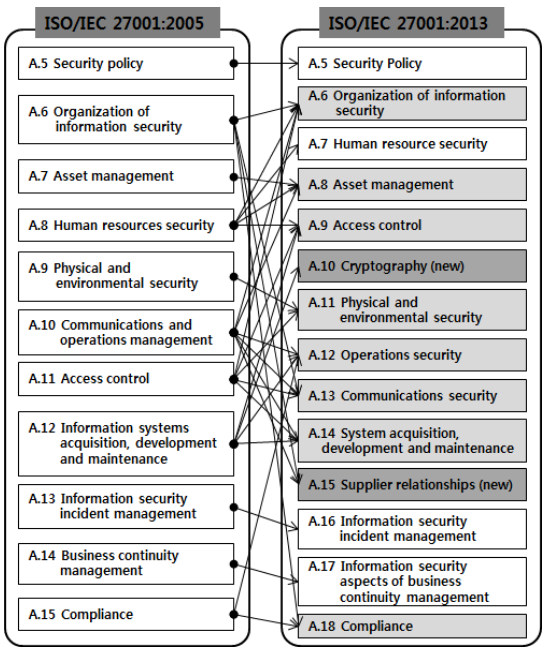
3.1 ISO/IEC 27001:2013 개요

ISO/IEC 27001은 조직의 정보보호를 위해 '무엇'을 해야 하는가를 정의하는데 목적을 갖는다. 또한 조직 내 정보 자산을 기준으로 자산 평가, 위협 평가, 취약성 평가를 산정하고 수용 가능한 위험 수준인 위험을 정의한다. ISO/IEC 27001:2005는 정보보호를 위한 위험 관리 방법에 '계획-실행-점검-개선(PDCA, Plan-Do-Check-Act) 모델'을 적용한다. 그러나 ISO/IEC 27001:2013은 ISO/IEC 31000 위험 관리 프로세스 기반에 '위험분석-평가-관리-모니터링 모델'을 적용하여 시나리오 기반의 위험관리를 정하였다.

ISO/IEC 27001:2013은 조직의 구조 변화 (예를 들면, 클라우드 컴퓨팅을 적용한 조직)을 고려하여 통제 영역과 통제 항목에 변화가 생겼다. 기존 11개 통제 영역(Domains)에서 14개 통제 영역으로 3개가 추가되었고, 기존 133개 통제 항목(Controls)에서 114개 통제 항목으로 19개가 삭제되었다.

3.2 ISO/IEC 27001:2013 통제 영역

다음 [Fig. 3]은 ISO/IEC 27001:2005와 ISO/IEC 27001:2013의 통제 영역의 연계 정보를 나타낸다.



[Fig. 3] Mapping table between ISO/IEC 27001:2005 and ISO/IEC 27001:2013

기존 통제 영역과 항목을 유지한 부분은 '2013 A.5 정보보호 정책', '2013 A.7 인적자원 보호', '2013 A.16 정보보호 사고관리', '2013 A.17 업무연속성 관리'이며 신규 통제 영역과 재구성된 통제 영역은 다음의 3.2.1 그리고 3.2.2 문항과 같다.

3.2.1 신규 통제 영역

'2013 A.10 암호화'와 '2013 A.15 위탁 관리'가 새로운 영역으로 추가되었다. 그 중 '2013 A.10 암호화' 통제 영역은 '2005 A.12.3 암호화 통제' 항목을 신규 통제 영역으로 발표하였으며 '2013 A.15 위탁 관리' 통제 영역은 '2005 A.6.2 외부 조직' 통제 항목과 '2005 A.10.2 제3자 서비스 전달 관리' 통제 항목으로 구성하고 신규 '2013 A.15.1.1 위탁 관리 정책'과 '2013 A.15.1.3 위탁 기술'에 대한 통제 항목을 구성했다.

3.2.2 재구성된 통제 영역

IT환경의 변화는 정보시스템 조직의 변화와 나아가 정보보호관리체계의 통제 항목의 재구성을 요구하였다. 그리고 이를 반영하여 기존 통제 영역의 통제 항목을 분석하고 통제 영역에 재배치하였다.

- '2013 A.6 정보보호 조직' : 내부 조직의 '2005 A.6.1 정보보호의 책임'과 운영 관리의 '2005 A.10.1.3 책임 범위 및 의무', 그리고 '2005 A.11.7 무선 디바이스의 정책과 통신' 통제 항목이 재구성되었다.
- '2013 A.8 자산 관리' : '2005 A.7 자산 관리' 통제 영역은 그대로 유지하고 '2005 A.8.3 자산 회수' 통제 항목과 '2005 A.10.7 미디어 관리와 물리적 미디어 변경' 통제 항목을 포함했다.
- '2013 A.9 접근 통제' : '2005 A.11 접근 통제'의 접근 통제 정책, 네트워크 서비스 정책, 사용자 접근 관리, 사용자 패스워드, 정보 접근 제한, 패스워드 관리 항목을 유지하면서 '2005 A.12.4.3 프로그램 소스 코드 접근 통제'와 '2005 A.8.3.3 접근 권한의 회수' 통제 항목을 추가했다.
- '2013 A.11 물리적 및 환경 정보보호' : '2005 A.9 물리적 및 환경 정보보호' 통제 영역을 유지하면서 '2005 A.11.3 사용자 기기 삭제' 통제 항목을 포함했다.
- '2013 A.12 운영 정보보호' : '2005 A.10 통신 및 운영 관리' 통제 영역의 운영 관리 부분과 '2005 A.12 정보시스템 도입, 개발, 유지보수' 통제영역의 소프트웨어 운영 통제와 취약점 통제 부분이 재구성되었다. '2005 A.15 준거성' 통제영역의 정보시스템 감사 통제 부분이 추가되었다.
- '2013 A.13 통신보호' : '2005 A.6 정보보호 조직'의 기밀규약의 통제 영역을 포함하고 '2005 A.10.6 네트워크 정보보호 관리'와 '2005 A.10.8 정보 변경' 그리고 '2005 A.11.4.5 네트워크 분리'의 통제 영역을 추가했다.
- '2013 A.14 정보시스템 도입, 개발, 유지보수' : '2005 A.12 정보시스템 도입, 개발, 유지보수' 통제 영역에서 5개의 항목을 삭제하고 '2005 A.10.9 전자상거래 서비스'의 통제 영역과 '2005 A.10.3 정보시스템 인수'의 통제 영역을 포함했다.
- '2013 A.18 준거성' : '2005 A.15 준거성'의 통제 항목을 유지하면서 '2005 A.6.1.8 정보보호의 의존성' 통제 항목을 포함했다.

3.3 ISO/IEC 27001:2013 통제 목적

ISO/IEC 27001:2005 통제 목적은 20개의 통제 항목이 삭제(Deleted 필드의 음영)<Table 3> 되고, 11개 신규 통제 항목이 추가(New 필드의 음영)<Table 4>되었다. 통제 항목 '정보시스템 도입, 개발, 유지보수'는 추가('2013 A.14') 및 삭제('2005 A.12')가 발생한 것으로 IT 환경의 변화에 민감한 영향을 받았음을 확인 할 수 있다. 통제 항목 '접근 통제'는 네트워크 접근 통제의 물리적 항목에 대한 삭제('2005 A.11.4')가 많았다.

클라우드 컴퓨팅 환경에 따른 정보보호관리체계의 변화로 볼 수 있는 통제 항목 '위탁 관리'는 공급자 관계에 대한 정보보호 정책('2013 A.15.1.1')과 정보 및 통신 서비스의 공급망 규약('2013 A.15.1.3')에 대한 부분이 추가되었다. 정보보호 조직 내 프로젝트 유형에 관계없이 정보보호 처리에 대한 통제 영역('2013 A.6')과 정보보호 사고 판단에 대한 문서화('2013 A.16.1.4')와 정보보호 사고 대응에 대한 처리('2013 A.16.1.5')에 대한 통제 항목이 추가되었다. 또한 소프트웨어 설치 상의 제약('2013 A.12.6.2')와 업무의 연속성에 대한 처리 절차('2013 A.17.2.1')가 새로운 항목이 되었다.

〈Table 3〉 Control Objects of ISO/IEC 27001: 2005

Control identification # : Control Objects (Items)	Deleted
A.5.1: Information security policy (2)	
A.6.1: Internal organization (8)	3
A.6.2: External parties (3)	2
A.7.1: Responsibility for assets (3)	
A.7.2: Information classification (2)	
A.8.1: Prior to employment (3)	
A.8.2: During employment (3)	
A.8.3: Termination or change of employment (3)	
A.9.1: Secure areas (6)	
A.9.2: Equipment security (7)	
A.10.1: Operational procedures and responsibilities (4)	
A.10.2: Third party service delivery management (3)	
A.10.3: System planning and acceptance (2)	
A.10.4: Protection against malicious and mobile code (2)	
A.10.5: Back-up (1)	
A.10.6: Network security management (2)	
A.10.7: Media handling (4)	1
A.10.8: Exchange of information (5)	1
A.10.9: Electronic commerce services (3)	
A.10.10: Monitoring (6)	
A.11.1: Business requirement for access control (1)	
A.11.2: User access management (4)	
A.11.3: User responsibilities (3)	
A.11.4: Network access control (7)	5
A.11.5: Operating system access control (6)	
A.11.6: Application and information access control (2)	1
A.11.7: Mobile computing and teleworking (2)	
A.12.1: Security requirements of information systems (1)	
A.12.2: Correct processing in applications (4)	4
A.12.3: Cryptographic controls (2)	
A.12.4: Security of system files (3)	
A.12.5: Security in development and support processes (5)	1
A.12.6: Technical Vulnerability Management (1)	
A.13.1: Reporting information security events and weaknesses (2)	
A.13.2: Management of information security incidents and improvements (3)	
A.14.1: Information security aspects of business continuity management (5)	
A.15.1: Compliance with legal requirements (6)	1
A.15.2: Compliance with security policies and standards, and technical compliance (2)	
A.15.3: Information systems audit considerations (2)	1

〈Table 4〉 Control Objects of ISO/IEC 27001: 2013

Control identification # : Control Objects (Items)	New
A.5.1: Management direction for information security (2)	
A.6.1: Internal organization (5)	1
A.6.2: Mobile devices and teleworking (2)	
A.7.1: Prior to employment (2)	
A.7.2: During employment (3)	
A.7.3: Termination and change of employment (1)	
A.8.1: Responsibility for assets (4)	
A.8.2: Information classification (3)	
A.8.3: Media handling (3)	
A.9.1: Business requirements of access control (2)	
A.9.2: User access management (6)	
A.9.3: User responsibilities (1)	
A.9.4: System and application access control (5)	
A.10.1: Cryptographic controls (2)	
A.11.1: Secure areas (6)	
A.11.2: Equipment (9)	
A.12.1: Operational procedures and responsibilities (4)	
A.12.2: Protection from malware (1)	
A.12.3: Backup (1)	
A.12.4: Logging and monitoring (4)	
A.12.5: Control of operational software (1)	
A.12.6: Technical vulnerability management (2)	1
A.12.7: Information systems audit considerations (1)	
A.13.1: Network security management (3)	
A.13.2: Information transfer (4)	
A.14.1: Security requirements of information systems (3)	
A.14.2: Security in development and support processes (9)	4
A.14.3: Test data (1)	
A.15.1: Information security in supplier relationships (3)	2
A.15.2: Supplier service delivery management (2)	
A.16.1: Management of information security incidents and improvements (7)	2
A.17.1: Information security continuity (3)	
A.17.2: Redundancies (1)	1
A.18.1: Compliance with legal and contractual requirements (5)	
A.18.2: Information security reviews (3)	

4. 클라우드 서비스 평가 프로그램과 ISO/IEC 27001:2013 비교 연구

4.1 ISO/IEC 27001와 클라우드 서비스 비교 연구

클라우드 서비스 환경 이전의 표준 규격('2005')과 이후의 표준 규격('2013') 차이점을 살펴봄으로써 발표된 IS

〈Table 5〉 Comparison table for ISO/IEC 27001:2005 and CSA CCM v.3

Control identification # of ISO/IEC 27001:2005	CSA CCM v.3															
	1 AIS	2 AAC	3 BCR	4 CCC	5 DSI	6 DCS	7 EKM	8 GRM	9 HRS	10 IAM	11 IVS	12 IPY	13 MOS	14 SEF	15 STA	16 TVM
A.5.1								3								
A.6.1		1	1	3	1			2	4					2		
A.6.2	1			2				3		1					3	
A.7.1					1	1			2		1					
A.7.2		1			3			1	1							
A.8.1									3							
A.8.2			1					3	3					2		
A.8.3									2	3						
A.9.1			1		1	4			1							
A.9.2			5		1	2					1					
A.10.1			1	4	1	1		1		1	1					
A.10.2				1				1							2	
A.10.3				2							2					
A.10.4				1												2
A.10.5			1													
A.10.6					2		1			1	2				2	
A.10.7			2		2		1		1							
A.10.8	1				1		1		1		1				1	
A.10.9					1		1				1					
A.10.10	1										4					
A.11.1	2									5	1					
A.11.2								1		6	2					
A.11.3									2							
A.11.4	1					1				4	3				1	
A.11.5	1			1						4	1					
A.11.6	2			1						2	2				1	
A.11.7									1							
A.12.1				3				1								
A.12.2	2			2												1
A.12.3	1						2				1				1	
A.12.4				4	1					1						
A.12.5	2			5	2			2			1				1	1
A.12.6	1			2				3								1
A.13.1				2							1			2		
A.13.2											1			4		
A.14.1			4					3								
A.15.1	1	1		1	2		2	3	1	1	3			1		
A.15.2	2			2				6			1					
A.15.3		1								1						

〈Table 6〉 Comparison table for ISO/IEC 27001:2013 and CSA CCM v.3

Control identification # of ISO/IEC 27001:2013	CSA CCM v.3															
	1 AIS	2 AAC	3 BCR	4 CCC	5 DSI	6 DCS	7 EKM	8 GRM	9 HRS	10 IAM	11 IVS	12 IPY	13 MOS	14 SEF	15 STA	16 TVM
A.5.1								3								
A.6.1			1	2	1			1	2	1				2		
A.6.2									1							
A.7.1									2							
A.7.2			1					3	3					2		
A.7.3									1							
A.8.1					2	1			2		1					
A.8.2		1	1		3		1		1							
A.8.3					2		1		1		1					
A.9.1	2									6	2					
A.9.2								1		5	2					
A.9.3									2							
A.9.4	2			4						6	2				1	
A.10.1	1						2				1				1	
A.11.1			1			4			1							
A.11.2			5		1	2			2		1					
A.12.1			1	3	1	1		1			2					
A.12.2				1												2
A.12.3			1													
A.12.4											4					
A.12.5				4												
A.12.6	2			2				3								1
A.12.7		1														
A.13.1					2		1			1	3				2	
A.13.2	1				1		1	1	2		1				1	
A.14.1	1			2	1		1	1			1					
A.14.2	1			5	1			2			1					1
A.14.3				4												
A.15.1				1											3	
A.15.2				1				1							1	
A.16.1				2							1			4		
A.17.1			4					3								
A.17.2																
A.18.1	1	1		1	2		2	3	1	1	3			1		
A.18.2	2	1		3				7			1					

O/IEC 27001:2013에 클라우드 서비스가 어떠한 영향을 주었는지 살펴보고자 한다. 이를 위하여 2.1절에서 살펴본 클라우드 서비스 평가 프로그램 중 하나인 CSA CCM v.3 통제 영역<Table 1>을 기준으로 클라우드 서비스 환경 전후의 통제 영역을 비교하였다. 1단계, ISO/IEC 27001:2005의 통제 목적<Table 3>을 비교 연구<Table 5>하고 2단계, CSA CCM v.3 통제 영역<Table 1>과 ISO/IEC 27001:2013<Table 4>의 통제 목적을 비교 연구<Table 6>하여 도출된 통제 영역의 특징은 다음과 같다.

첫째, 전반적으로 ISO/IEC 27001:2013의 통제 항목이 고르게 분포되어 특정 통제 영역에 편중되었던 ISO/IEC 27001:2005의 통제 항목과는 달리 통제 영역 및 통제 항목 재구성이 잘 되었음을 알 수 있다.

둘째, 클라우드 '접근 통제' 보안 요소[12]는 '통제 변경, 식별자 및 접근 관리'에 대하여 적극적으로 통제 항목

〈Table 7〉 Comparison table for ISO/IEC 27001:2013 and Cloud Service Assessment Programs

Control Domain of FedRAMP																	Control # of ISO/IEC 27001:2013	Control Domain of CSA CCM v.3														
SI	SC	SA	RA	PS	PL	PE	MP	MA	IR	IA	CP	CM	CA	AU	AT	AC		AIS	AAC	BCR	CCC	DSI	DCS	EKM	GRM	HRS	IAM	IVS	IPY	MOS	SEF	STA	TVM
										×							A.5.1								×								
×		×		×								×	×	×		×	A.6.1			×	×	×			×	×	×				×		
							×									×	A.6.2									×							
				×													A.7.1.									×							
×		×		×			×		×			×		×	×		A.7.2			×					×	×					×		
				×													A.7.3									×							
		×										×				×	A.8.1					×	×			×		×					
	×	×	×				×				×	×		×		×	A.8.2		×	×		×		×		×							
	×						×									×	A.8.3					×		×		×		×					
	×							×		×			×			×	A.9.1	×									×	×					
×	×									×			×	×	×	×	A.9.2								×		×	×					
							×									×	A.9.3									×							
×	×	×								×		×		×		×	A.9.4	×			×						×	×			×		
	×	×														×	A.10.1	×						×				×			×		
						×	×										A.11.1			×			×			×							
	×					×	×	×			×					×	A.11.2			×		×	×			×		×					
×		×										×	×				A.12.1			×	×	×	×		×			×					
×												×					A.12.2				×												×
											×						A.12.3			×													
×	×													×			A.12.4										×						
×		×														×	A.12.5				×												
×	×	×	×									×	×				A.12.6	×			×				×								×
													×				A.12.7		×														
	×							×			×					×	A.13.1					×		×			×	×				×		
×	×			×			×									×	A.13.2	×				×		×	×	×		×				×		
×	×															×	A.14.1	×			×	×		×	×			×						
×	×	×	×														A.14.2	×			×	×			×			×						×
		×															A.14.3				×													
	×	×					×				×						A.15.1				×											×		
	×	×															A.15.2				×				×							×		
×		×							×			×		×			A.16.1				×							×			×		
×			×								×		×				A.17.1			×					×								
																	A.17.2																
	×	×					×		×					×		×	A.18.1	×	×		×	×		×	×	×	×	×			×		
×		×	×									×	×	×	×		A.18.2	×	×		×				×			×					

('2013 A.9')이 추가되었다.

셋째, 클라우드 '서비스 장애' 보안 요소[13]는 '통제 변경, 공급망 관리'에 대하여 기존 외부 정책 통제 항목('2013 A.15.1')을 재구성하고 SLA에 대한 중요성을 강조하였다.

마지막으로 클라우드 '인프라 및 가상화 보안'와 '데이터 센터 보안' 보안 요소 측면에서 특별한 변화를 보이지 않으므로 인프라 계층의 통제 항목은 기존 ISO/IEC 27001:2005 통제 항목을 유지하였으나 플랫폼 및 어플리케이션 계층의 정보보호 통제 항목에 집중하였음을 알 수 있다.

4.2 ISO/IEC 27001:2013과 클라우드 서비스 평가 프로그램 비교 연구

클라우드 서비스 평가 프로그램을 대표하는 FedRAMP 평가 영역<Table 2>과 CSA CCM v.3의 평가 영역<Table 1>을 정보보호관리체계 표준인 ISO/IEC 27001:2013의 평가 목적<Table 4>과 비교 연구한 결과는 <Table 7>이다. 결과를 통해 정보보호관리체계 표준인 ISO/IEC 27001:2013을 기준으로 클라우드 서비스 평가 프로그램간의 차이점은 다음과 같다.

첫째, 클라우드 서비스 평가 프로그램간의 통제 영역

분류의 차이가 있음을 알 수 있다. FedRAMP는 ISO/IEC 27001:2013 관계에서 6개의 평가 항목(접근통제-AC, 형상관리-CM, 미디어 정보보호-MP, 시스템 및 서비스 조달-SA, 시스템 및 통신 정보보호-SC, 시스템 및 정보 무결성-SI)에 중점적으로 연관되어 있고, CSA CCM v.3은 5개의 평가 항목(통제 변경 및 형상관리-CCC, 데이터 보안 및 정보 라이프사이클 관리-DSI, 운영 및 위험 관리-GRM, 인프라 및 가상 보안-IVS)에 중점적으로 연관되어 있음을 알 수 있다. 이러한 현상은 클라우드 서비스 평가 프로그램의 제정한 관점의 차이라 볼 수 있다. FedRAMP의 통제 항목은 미국 연방정보보호법에 의해 보안 통제 항목을 구성한 기본 항목에 클라우드 기술의 일부 통제 항목을 포함하여 G-Cloud 정책(미 정부기관의 평가 인증된 클라우드 서비스 적극적으로 도입)에 맞는 '시스템 및 서비스 조달-SA', '접근통제-AC', '시스템 및 통신 정보보호-SC'에 특별히 집중되어 있다. CSA CCM 연구는 클라우드 컴퓨팅 환경의 신뢰성을 목표로 클라우드 보안 위협에 관한 연구를 주도적으로 이끌었고 이점은 기존 정보보호관리체계 통제 항목보다 클라우드 특성화된 '인프라 및 가상 보안-IVS' 통제 항목의 관계에서 확인 할 수 있었다.

둘째, FedRMP의 '정보보호계획(PL)'와 CSA CCM v.3의 '모바일 보안' 및 '상호운용 및 이식성' 통제 항목은 적용되는 통제 항목이 없는 것으로 확인되었다. 이것은 ISO/IEC 27001:2013 정보보호관리체계의 표준 규격이므로 클라우드 서비스에 맞는 특성화된 평가 프로그램의 지속적인 개발이 필요함을 보여준다.

5. 결론

ISO/IEC 27001 문서는 그 시대의 IT 환경을 반영한 정보보호관리체계의 통제 항목이다. 기존 클라우드 서비스 평가 프로그램들은 ISO/IEC 27001 문서를 근거로 통제 항목을 개발하고 있다.

본 논문은 최근 발표된 ISO/IEC 27001:2013 문서와 클라우드 서비스 평가 프로그램의 비교 연구를 위해 두 가지 측면으로 연구하였다. 첫째, 클라우드 서비스 환경이 정보보호관리체계에 어떠한 영향을 미쳤는지 살펴보았다. 이를 위해 클라우드 서비스 이전에 발표된 ISO/IEC 27001:2005와 클라우드 서비스 이후에 발표된 ISO/IEC 27001:2013을 비교 연구하였고 '접근 통제', '서비스 공급망 관리', '인프라 및 가상화 보안' 통제 목적에서 클라우드 서비스 환경이 반영되었음을 알 수 있었다. 둘째, 발표된 ISO/IEC 27001:2013 문서가 클라우드 서비스에 특화된 평가 프로그램의 통제 영역을 어느 정도 반영되었는지 확인하였다. ISO/IEC 27001:2013 문서의 통제 목적과 CSA CCM v.3 및 FedRAMP의 통제 영역을 각각 비교 연구하여 클라우드 서비스 평가 프로그램간의 통제 영역 분류의 차이가 있음을 알 수 있었다.

본 논문을 통해 클라우드 서비스 평가 기관에게 변화하고 있는 정보보호관리체계의 평가 항목을 제안하고 클라우드 서비스 공급자에게 클라우드 서비스 평가 지표를 제시하였다. 최근 정부차원으로 진행되고 있는 기업의 정보보호관리체계인증 의무화 시행은 기업의 보안 정책에 중요성을 강조하고 있다. 기업의 일부 시스템을 클라우드 서비스로 사용할 경우 본 논문의 비교 연구된 평가 항목은 클라우드 서비스 이용자 조직의 보안 정책 수립에 참고 지표가 될 것이다.

ACKNOWLEDGMENTS

This work was supported by a special research grant from Seoul Women's University(2013)

REFERENCES

[1] Telecommunications Technology Association, http://word.tta.or.kr/terms/terms.jsp

[2] IDC, WorldWide and Regional Public IT Cloud Services 2013-2017 Forecast

[3] W. Y. Kang, Market Views and Policy Trends for Foreign Cloud, Internet & Security Issue, pp. 10, Jun. 2012.

[4] ISO/IEC FDIS 27001 Information technology - Security techniques - Information security management systems - Requirements, ISO/IEC, 2013, http://www.iso.org

[5] Cloud Security Alliance, CSA Position Paper on AICPA Service Organization Control Reports, Feb. 2013.
[6] PCI-DSS, Information Supplement: PCI DSS Cloud Computing Guidelines Version 2.0, Feb. 2013.
[7] FedRAMP: The Federal Risk and Authorization Management Program, FedRAMP CONOPS Version 1.2, Jul. 2012.
[8] Cloud Security Alliance, Open Certification Framework Vision Statement, Rev. 1, Aug. 2013.
[9] ISACA, Cloud Computing Management Audit/Assurance Program, 2010.
[10] KCSA, Assessment Criteria of Cloud Service, Feb. 2012.
[11] NIST Computer Security Division, "Recommended Security Control for Federal Information Systems and Organizations", NIST SP 800-53 Revision 3, Feb, 2010.
[12] Kchul Kim, Ok Heo, Seungjoo 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.
[13] Kyoung-a Shin, Sang-jin Lee, Information Security Management System on Cloud Computing Service, Journal of The Korea Institute of Information Security & Cryptology, Vol. 22, No. 1, pp. 156-167. 2013.

최 주 영(Choi, Ju Young)

- 1999년 2월 : 서울여자대학교 컴퓨터학과 이학사
- 2003년 2월 : 서울여자대학교 컴퓨터학과 이학석사
- 2012년 2월 : 서울여자대학교 컴퓨터학과 이학박사
- 2011년 3월 ~ 현재 : 서울여자대학교 정보보호학과 초빙강의교수

- 관심분야 : 클라우드컴퓨팅, 정보보호관리체계, 정보보안
- E-Mail : jychoi@swu.ac.kr

최 은 정(Choi, Eun-Jung)

- 1997년 2월 : 서울여자대학교 전산과학과 이학사
- 2000년 2월 : 서울여자대학교 컴퓨터학과 이학석사
- 2005년 8월 : 서울여자대학교 컴퓨터학과 이학박사
- 2006년 3월 ~ 현재 : 서울여자대학교 교양학부 조교수

- 관심분야 : 정보보안, 클라우드컴퓨팅, 빅데이터
- E-Mail : chej@swu.ac.kr

김 명 주(Kim, Myuhng-Joo)

- 1986년 2월 : 서울대학교 컴퓨터공학과 공학사
- 1988년 2월 : 서울대학교 컴퓨터공학과 공학석사
- 1993년 8월 : 서울대학교 컴퓨터공학과 공학박사
- 1993년 9월 ~ 1995년 8월 : 서울대학교 컴퓨터 신기술 공동연구소 특별연구원

- 2003년, 2010년 : 미국 펜실베이니아대학교(UPenn) 객원 연구원
- 1995년 ~ 현재 : 서울여자대학교 정보보호학과 교수
- 관심분야 : 소프트웨어보안, 악성코드, 웹보안, 창의성과 윤리
- E-Mail : mjkim@swu.ac.kr