클라우드 보안 인증 제도 현황 및 국제 표준 동향

김 형 구*

◈ 목 차 ◈

1. 서 론

지난 15년 3월 “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률이 제정 및 시행(‘15.09)됨에 따라 미래창조과학부에서는 제17차 경제관계장관회의(’15.09)에서 국정과제 및 경제혁신 3개년 계획의 핵심과제중 하나인 ’클라우드 컴퓨팅 산업 육성‘의 일환으로 ”클라우드 서비스 활성화를 위한 정보보호 대책“을 수립, 발표하였다. 클라우드 정보보호대책은 ① 클라우드 사업자 정보보호 수준향상 및 대응체계 구축, ② 클라우드 이용자 정보보호 기반 구축, ③ 클라우드 정보보호 전문기업 육성 등의 과제로 ‘19년까지 단계적으로 추진할 계획이다[1].

또한, K-ICT 클라우드컴퓨팅 활성화 계획(미래창조과학부, 15.11)을 통해 클라우드 컴퓨팅 발전 기본계획을 발표하면서, 클라우드 정보보호 수준 향상을 위해 국제 클라우드 보안표준 및 주요국의 보안인증기준을 고려하여 정보보호 기준을 마련하기로 하였으며, 이와 더불어 한국인터넷진흥원(KISA)에서는 K-FedRAMP 적용을 위한 ‘클라우드 보안등급별 인증기준개발 및 시범적용’ 사업을 시행하고 있다[2][3].

클라우드 서비스에 대한 보안 관련 기준으로는 일반적으로 비영리단체인 클라우드 보안 협회(Cloud Security Alliance, 이하 CSA)의 CCM(Clound Contorls Matrix, 이하 CCM) 등 가이드라인이나, 미국 정부의 클라우드 서비스 인증제도인 FedRAMP(Fedrral Risk and Authorization Management Program, 이하 FedRAMP)와 같은 규제 요구사항, ISO/IEC 27001:2013[2], PCI DSS[3], ISO/IEC 27018:2014[4] 등과 같은 국제 표준 등이 있다.

본 동향에서는 FedRAMP, CCM 등을 중심으로 클라우드 인증 현황을 분석하고, ISO/IEC 27017:2015와 ISO/IEC 27018:2014 표준 동향을 요약 제시하여, 국내 클라우드 보안 인증 제도 적용 방안에 대해 논의하고자 한다.

2. 클라우드 보안 인증 현황

2.1 FedRAMP

미국의 클라우드 정책은 미국 연방정보 CIO, Vivek Kundra가 기존 IT 환경 하에서 발생하는 예산 활용의 비효율성과 자원관리 시스템 취약성, 조달 프로세스의 복잡성 등을 개선하고자 2009년 5월 연방 CIO 협의회에서 클라우드 컴퓨팅 추진 전략을 발표하고, 미연방

* 현대그린푸드 IT실 전략기획파트

2) 정보보호관리체계에 대한 국제 표준으로 정보보호 경영 시스템 프레임워크를 제공한다. 정보보호 관리과정은 7개 필수 요구사항, 정보보호 통제과정은 14개 영역 114개 통제항목으로 구성되어 있다.

3) PCI DSS(Payment Card Industry Data Security Standard) : 가맹점 결제 대행 사업자가 취급하는 카드 회원의 신용카드 정보 및 거래 정보를 안전하게 보호하기 위해 국제 결제 브랜드 5개사가 공동으로 책정 한 신용업계 글로벌 보안 기준

4) 클라우드 프라이버스에 대한 국제 표준으로 클라우드 환경에서의 개인정보보호에 대한 지침

(표 1) FedRAMP Control

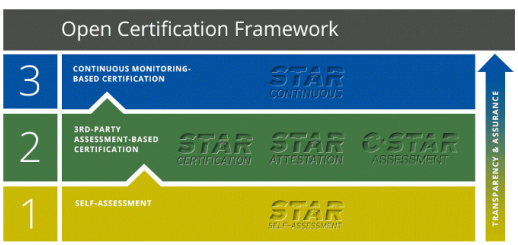
ID	Family	Low	Moderate
AC	Access Control	11	18(25)
AT	Awareness and Training	4	4(1)
AU	Audit and Accountability	10	11(8)
CA	Certification, Accrediation and Security Assessment	7(1)	8(7)
CM	Configuration Management	8	11(15)
CP	Contingency Planning	6	9(15)
IA	Identification and Authentication	7(8)	8(19)
IR	Incident Response	7	9(9)
MA	Maintenance	4	6(5)
MP	Media Protection	4	7(3)
PE	Physical and Environmental Protection	10	16(4)
PL	Planning	3	4(2)
PS	Personnel Security	8	8(1)
RA	Risk Assessment	4	4(6)
SA	System and Service Acquisition	6(1)	9(13)
SC	System and Communications Pretection	10	20(12)
SI	System and Information Integrity	6	12(16)
Totals (Controls and Enhancements)		**125**	**325**

조달청(General Service Administration : GSA)이 SaaS (Softwaare as a Service) / IaaS(Infrastructure as Service) 조달에 관한 RFI(Request for Inforamtion)를 발표하면서 시작되었다[4].

FedRAMP의 실행은 2012년 6월 GSA가 FedRAMP의 공식 실행을 발표하면서 인증 작업을 개시하였으며, 통제항목은 위의 (표1)과 같이 17개 통제 그룹에 325개의 통제항목으로 되어 있으며, NIST 800-53 기반으로 인증체계가 구성되어 있다[5].

2.2 CSA (BSI STAR)

CSA는 2008년 12월에 비영리 기관으로 설립되었다. CSA에서는 3단계의 Open Certification Framework 인증을 제시하고 있다.



(그림 1) Open Certification Framework[6]

1단계는 Self-Assessment로 CAIQ(Consensus Assessments Initiative Questionnaire, 이하 CAIQ) v3.0.1[7]과 CCM v3.0.1[8]를 이용한 자가 진단의 단계이다.

CAIQ는 클라우드 사용자나 감사자가 클라우드 제공자에게 요청할 수 있는 질문집이라고 할 수 있다. CAIQ는 CCM의 통제항목과 IaaS, PaaS, SaaS에서 제공하는 투명한 보안 통제를 기반으로 한 문서화의 방법 등을 포함한다. CAIQ는 각 질문에 대해 [표2]의 예시와 같이 "Yes or No"로 질의 응답하는 방식으로 자가진단을 할 수 있다.

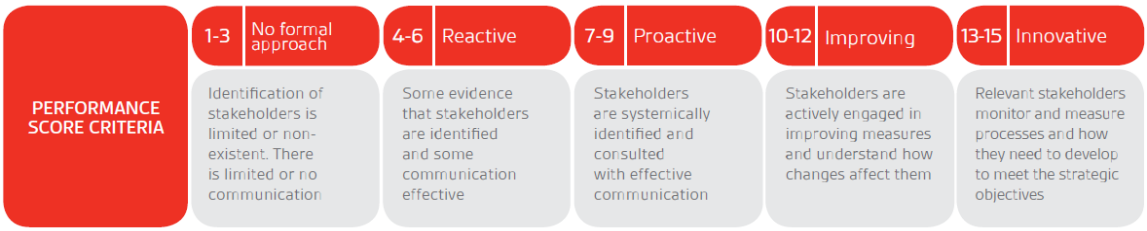
(표 2) CAIQ V3.0.1(2014.09) 예시

Control Group	Consensus Assessment Questions
Application & Interface Security	Are All requrements and trust levels for customer's access defined and documented?

CCM은 16개 도메인(Control Domain), 133개 통제항목(Control ID)으로 구성되어 있으며, CAIQ는 16개 통제그룹(Control Group), 133개 CGID(Control Group ID) 및 295개의 통제ID(Contorl ID)가 질문형식으로 구성되어 있는데, CAIQ와 CCM을 정리하면, 아래의 (표3)과 같다. CAIQ와 CCM은 서로 대응된다.

(표 3) CAIQ & CCM Control

Control Group (CAIQ) / Control Domain (CCM)	CGID (CAIQ) / Control ID(CCM)	CID (CAIQ) / -	Control Group (CAIQ) / Control Domain (CCM)	CGID (CAIQ) / Control ID(CCM)	CID (CAIQ) / -
Application & Interface Security (AIS)	4	9	Human Resources (HRS)	11	24
Audit Assurance & Compliance (AAC)	3	13	Identity & Access Management (IAM)	13	40
Business Continuity Management & Operational Resilience) (BCR)	11	22	Infrastructure & Virtualization Security (IVS)	13	33
Change Control & Configuration Management (CCC)	5	10	Interoperability & Portability (IPY)	5	8
Data Security & Information Lifecycle Management (DSI)	7	17	Mobile Security (MOS)	20	29
Datacenter Security (DCS)	9	11	Security Incident Management, E-Discovery & Cloud Forensics (SEF)	5	13
Encryption & Key Management (ERM)	4	14	Supply Chain Management, Transparency and Accountability (STA)	9	20
Governance and Risk Management (GRM)	11	22	Threat and Vulnerability Management (TVM)	3	10
Total				133	296



(그림 2) STAR 인증 성숙도 평가 모델(Maturity Model)[9]

2단계는 3rd-Party Assessments Based Certificaiton으로 앞서 1단계에서 살펴본 CAIQ는 자가진단인 반면 CSA CCM을 통합한 ISO/IEC 27001 기반의 제3자 평가의 개념(STAR 인증)이다. STAR 인증은 기존의 ISO 인증과 달리 성숙도 평가 모델(Maturity Model)을 적용한다. 성숙도 평가 모델은 Score에 따라 성숙도를 평가하고 점수를 부여하는데, 해당 Score는 위의 (그림2)와 같다.

3단계는 Continuous Monitoring-Based Certification으로 모니터링 기반 인증으로 지속적인 감사 증적 수집을 기반으로 소비자 요구사항을 충족하는지 여부를 거의 실시간 모니터링 하도록 구현하려는 개념이다.

2.3 해외 사례

일본 및 영국에서도 클라우드 서비스 인증제도가 실시되고 있는데, 일본은 재단법인 멀티미디어 진흥센터(Foundation for Multimedia Communications, FMCC)는 2008년 'ASP-SaaS 서비스 정보 공개 인증, 2012년 'IaaS-Pass 서비스 공개 인증', 2012년 '데이터 센터 서비스 정보 공개 인증'을 시행중인데, 이러한 3가지 서비스 영역 인증 제도를 '클라우드 서비스 안전·신뢰성에 관한 정보 공개 인증제도'라고 총칭하여 운영하고 있다.

일본의 인증심사 대상항목을 정리하면 아래의 (표 4)와 같다.

(표 4) 일본의 클라우드 인증심사 대상항목[10][11]

구분	유형	대상항목
사업자 안전·신뢰성 정보공개 항목	공통	사업설립/사업내용, 인적자원, 재정상황, 자본관계, 비즈니스 관계, 규정준수
서비스 안전·신뢰성 정보공개 항목	ASP-SaaS	기본특성, 응용프로그램, 플랫폼, 서버/스토리지, 네트워크, 보호(서버위치), 서비스 지원
	IaaS-PaaS	기본특성, 서비스운영(인프라, 보안), 네트워크, 보호(서버위치), 서비스지원
	데이터 센터	보호(시설장비), 보호(네트워크), 보호(서비스내용), 보호(서비스자원), IaaS-PaaS 지원시(서비스내용)

영국 정부는 미국 정부와 마찬가지로 공공 부문 IT 시스템 조달시 클라우드 서비스를 우선 고려해야 한

다는 내용의 '클라우드 퍼스트 정책(Cloud First Policy)'를 발표하였다. 2012년 발표된 보안 인증제도인 '지클라우드(G-Cloud)"는 서비스의 기밀성과 무결성 측면의 업무영향수준에 따라 "BIL(Business Impact Level)" 수준으로 구분된다. 이에 대한 자세한 사항은 아래 (표5)와 같다[11].

(표 5) G-Cloud BIL 평가 [11]

구분	내 용
BIL/BIL1	ISO/IEC 27001 인증 기반으로 이루어지며, 인증범위는 서비스 제공자와 범정부인가처(PGA) 협의로 결정
BIL2	서비스 제공자는 27001 인증서와 함께 RMADS(위험관리 인가문서)와 잔여 위험 및 미해결 이슈 등의 정보를 증적으로 제출
BIL3	영국 정부의 정보보증(IA) 표준 및 지침에 따르는지 점검하기 위하여 PGA가 직접 현장 실사를 수행함(국외도 해당)
BIL4	BIL4 이상의 기밀은 사설 클라우드 서비스로 구현되어야 한다.

3. 클라우드 국제 표준 동향

3.1 ISO/IEC 27018:2014

국제 표준화 기구(ISO)에서는 클라우드 서비스 제공자를 위한 데이터 보호 통제 지침을 2014년에 국제표준(ISO/IEC 27018:2014)을 채택하였다.

ISO/IEC 27018:2014는 일반적으로 공공 클라우드 컴퓨팅 환경에 대한 ISO/IEC 29100의 개인정보보호원칙에 따라 개인식별정보(PII)를 보호하기 위한 조치를 구현하기 위한 통제 목표, 통제 및 지침을 제공하고 있는데, 특히 ISO/IEC 27018:2014는 ISO/IEC 27002에 기초한 기준을 가지고 퍼블릭 클라우드 서비스 5)제공자의 정보 보안 위험 환경들의 맥락내에서 적용할 수 있는 PII의 보호 요건을 고려하고 있다[13].

ISO/IEC 27002와 ISO/IEC 27018의 통제 구현과 관련된 차이는 아래의 (표6)과 같은데, ISO/IEC 27002를 참고하지만, 부문별 구현 지침 및 기타 정보를 제공하고 있다.

(표 6) ISO/IEC 27018:2014 (통제별 ISO/IEC 27002 기반의 통제 시행을 위한 구현 지침과 기타 정보)[13]

Clause Number	Titile	Remark
5	정보보호정책	부분별 구현 지침 및 기타 정보 제공
6	정보보호조직	부분별 구현 지침 제공
7	인적보안	부분별 구현 지침 및 기타 정보 제공

5) 클라우드 서비스 제공자가 오픈된 인터넷망을 통해 불특정다수의 기업 또는 개인에게 컴퓨팅 자원(서버, 스토리지 등)을 빌려주는 형태의 서비스

Clause Number	Titile	Remark
8	자산관리	ISO 27002 준용
9	접근통제	부분별 구현 지침 제공 및 Annex A의 제어 상호 참조
10	암호화	부분별 구현 지침 제공
11	물리적보안	부분별 구현 지침 제공 및 Annex A의 제어 상호 참조
12	운영보안	부분별 구현 지침 제공
13	통신보안	부분별 구현 지침 제공 및 Annex A의 제어 상호 참조
14	시스템개발보안	ISO 27002 준용
15	공급망관리	ISO 27002 준용
16	정보보호사고 관리	부분별 구현 지침 제공
17	연속성관리	ISO 27002 준용
18	법적준거성	부분별 구현 지침 제공 및 Annex A의 제어 상호 참조

Annex A에서는 ISO/IEC 29100의 11개 개인정보보호원칙에 따라 분류하였다. 많은 통제 항목이 하나 이상의 개인정보보호원칙과 연관되어 있기 때문에 이 경우에는 가장 관련성이 높은 원칙에 분류하고 있다. Annex A 내용을 요약하면 (표7)과 같다.

(표 7) ISO/IEC 27018:2014 Annex A [13]

Clause Number	Control	Remark
A.1	동의 및 선택	올바른 개인 식별 정보 주체의 권리의 행사를 용이하도록 하여야 함 (Public PII 구현 안내)
A.2	목적의 정당성	목적외 이용 금지 및 명시적 동의없이 마케팅, 광고 금지 (Public PII 구현 안내)
A.3	수집 제한	ISO 29100 준용
A.4	데이터 최소화	임시 파일 및 문서는 지정된 기간내에 삭제 또는 파기 (Public PII 구현 안내)
A.5	사용, 보존 및 제공 제한	클라우드 서비스 제공자와 서비스 고객 사이 계약, 제3자에게 제공에 대해서는 제공된 내용을 포함하여 기록 (Public PII 구현 안내)
A.6	정확성 및 품질	ISO 29100 준용
A.7	개방성, 투명성 및 통지	위탁 공개 (Public PII 구현 안내)
A.8	개인의 참여 및 접근	ISO 29100 준용
A.9	책임	침해사고에 대한 통보, 보안정책과 지침 보존, 개인정보 반환/폐기(A.4 연계) (Public PII 구현 안내)
A.10	정보보안	비밀유지의무, 개인식별정보를 표시하는 HardCopy 생성 금지, 로깅 및 데이터 복원, 저장매체 보호, 암호화되지 않은 휴대용 저장매체 사용, 암호화 전송, 안전한 폐기, 고유한 사용자ID 사용, 사용자 기록 저장, ID관리, 계약 방법, 하부위탁계약 기준, 기존 데이터에 대한 액세스 (Public PII 구현 안내)
A.11	개인정보 보호 규정 준수	개인식별정보의 저장공간의 지리적 위치, 데이터 전송에 대한 적절한 제어 (Public PII 구현 안내)

3.2 ISO/IEC 27017:2015

국제 표준화 기구(ISO)에서는 클라우드 컴퓨팅 서비스 사업자를 위한 보안 통제 지침인 ISO/IEC 27017:2015은 2015년에 채택하였다.

ISO/IEC 27017:2015는 클라우드 서비스의 사용에 적용할 수 있는 정보보안 관리에 대한 지침을 제공하고 있는데, ISO/IEC 27002에 규정된 관련 컨트롤에 대해 추가 구현을 안내하고 있으며, 구체적으로 클라우드 서비스와 관련된 구현 지침을 통제항목으로 추가하였다. 또한, ITU-T와 공동으로 IT 보안 기술에 대해 동일하게 게시하였다. ITU-T X.1631 SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY (Cloud computing security – Cloud computing security design)

ISO/IEC 27017은 클라우드 서비스 제공자와 클라우스 서비스 고객 모두에 대한 제어 및 구현 지침을 제

(표 8) ISO/IEC 27017 in implementing controls in ISO/IEC 27002

Clause Number	Control	Remark
5	정보보호정책	부분별 구현 지침 및 기타 정보 제공(5.1.1) ISO/IEC 27002 Apply(5.1.2)
6	정보보호조직	부분별 구현 지침 및 기타 정보 제공(6.1.1, 6.1.3) ISO/IEC 27002 Apply(6.1.2, 6.1.4, 6.1.5, 6..2)
7	인적보안	부분별 구현 지침 및 기타 정보 제공(7.2.2) ISO/IEC 27002 Apply(7.1, 7.2.1, 7.2.3, 7.3)
8	자산관리	부분별 구현 지침 및 기타 정보 제공(8.1.1,8.1.2,8.2.2) ISO/IEC 27002 Apply(8.1.3,8.1.4,8.2.1,8.2.3,8.3)
9	접근통제	부분별 구현 지침 및 기타 정보 제공(9.1.2, 9.2.1, 9,2.2.,9.2.3,9.2.4,9.4.1,9.4.4) ISO/IEC 27002 Apply(9.1.1,9.2.5,9.2.6,9.3,9.42.,9.4.3,9.4.5)
10	암호화	부분별 구현 지침 및 기타 정보 제공(10.1)
11	물리적보안	부분별 구현 지침 및 기타 정보 제공(11.2.7) ISO/IEC 27002 Apply(11.2.7외)
12	운영보안	부분별 구현 지침 및 기타 정보 제공(12.1.2,12.1.3,12.3,12.4.1,12.4.3,12.4.4,12.6.1) ISO/IEC 27002 Apply(12.1.1,12.1.4,12.2,12.4.2,12.5,12.6.2,12.7)
13	통신보안	부분별 구현 지침 및 기타 정보 제공(13.1.3) ISO/IEC 27002 Apply(13.1.3외)
14	시스템개발보안	부분별 구현 지침 및 기타 정보 제공(14.1.1,14.2.1,14.2.9) ISO/IEC 27002 Apply(14.1.1,14.2.1,14.2.9외)
15	공급망관리	부분별 구현 지침 및 기타 정보 제공(15.1.1,15.1.2,15.1.3) ISO/IEC 27002 Apply(15.2)
16	정보보호사고 관리	부분별 구현 지침 및 기타 정보 제공(16.1.1,16.1.2,16.1.7) ISO/IEC 27002 Apply(16.1.1,16.1.2,16.1.7외)
17	연속성관리	ISO/IEC 27002 Apply
18	법적준거성	부분별 구현 지침 및 기타 정보 제공(18.1.1,18.1.2,18.1.3,18.1.5,18.2.1) ISO/IEC 27002 Apply(18.1.4,18.2.2,18.2.3)

공하고 있어, 각 항목별로 Cloud Service Customer와 Cloud Service Provider에 대한 구현 안내를 하고 있다. 이러한 ISO/IEC 27017의 통제항목별 기존의 ISO27002 준수와 부분별 구현 지침 및 기타 정보 제공한 통제 항목을 구분하면 (표8)과 같다[12].

또한, 클라우드 서비스와 관련된 Control Set을 추가한 Annex A 또한, Cloud Service Customer와 Cloud Serivice Provider를 구분하여 가이드라인을 제시하고 있다.

3.3 소 결

ISO/IEC 27017과 ISO/IEC 27018에서 ISO/IEC 27002를 기반으로 추가적인 구현 지침 및 기타 정보를 제공하고 있음에 따라, 클라우드에 적합한 사항에 대한 표준 제시는 적절한 것으로 보인다. 또한, ISO/IEC 27017은 클라우드 서비스 제공자 및 사용자 측면에서의 구현 지침 및 기타 정보를 상세히 제공하고 있고, ISO/IEC 27018은 데이터 측면, 즉 개인정보보호에서의 표준을 클라우드 환경에 맞게 제시하고 있다.

참고로, NIST의 SP 800-53 Rev 4에서도 Appendix J에서 Privacy Control Catalog를 제시하고 있으며, 이러한 각 통제항목이 FedRAMP 및 CSA CCM에 Mapping되어 운영되고 있고 있으며, NIST의 SP 800-53 Rev 4에서의 Privacy Controls은 8개분야, 26개로 구성되어 있으며, 각 Privacy Control은 기존의 Controls와 연계된다.

국내의 정보보호관리체계 또한 정보보안경영시스템에 대한 국제적인 표준인 ISO/IEC 27001과 정보보호 통제에 대한 실무 지침인 ISO/IEC 27002을 기반으로 통제항목을 국내 실정에 맞도록 재구성하고 있으므로, ISO/IEC 27017, ISO/IEC 27018을 참조하여 클라우드 환경을 반영한 정보보호관리체계 인증을 수립하거나, 별도의 K-FedRAMP 구성이 필요하다.

4. 결 론

클라우드 산업의 활성화를 위해 정보보호가 반영된 안전한 환경 구성에 대한 인증을 위해서는 미국의 FedRAMP나 CSA CCM을 기준으로 한 BSI STAR 인증과 같은 인증 기준 수립이 매우 중요한 시점이다. 또한, ISO 27018 표준 제정에 따라 아마존 및 마이크로소프트가 ISO 27018 인증을 취득하는 등 해외 사업자의 클라우드 보안 인증에 대한 대응이 매우 빠르게 진행되고 있다.

금번 동향에서는 FedRAMP, CSA CCM 및 ISO27002를 기준으로 ISO 27018과 ISO 27017의 변경 사항에 대해 요약 정리하였으나, ISO27002 대비 추가적으로 제시한 항목에 있어 상세한 분석이 필요하며, 국내의 개인정보보호법, 정보통신망법, 클라우드발전법 등의 컴플라이언스 측면을 고려한 추가적인 비교 분석이 필요하다.

향후에는 이러한 클라우드 환경에 따라 제시된 추가적인 항목과 국내의 정보보호관리체계(ISMS) 인증 간의 상세 항목 비교를 통해 정보보호관리체계(ISMS)에서의 클라우드보안 인증제 수용 가능 여부 및 정부에서 시행 예정인 K-FedRAMP에 대한 상세 비교가 이루어진다면 국내의 클라우드 산업의 발전과 클라우드 환경의 보안 강화에 일조할 것으로 보인다.

참 고 문 헌

[1] 관계부처 합동, “클라우드 서비스 활성화를 위한 정보보호 대책”, 2015.09.09

[2] 관계부처 합동, “K-ICT 클라우드컴퓨팅 활성화 계획(안)”, 2015.11.10.

[3] KISA, “클라우드 보안등급별 인증기준 개발 및 시범적용 용역”, 2015.06.23

[4] KISA, “미 연방정부 클라우드 서비스 보안인증제도(FedRAMP) 분석”, 정보통신사업진흥원 주간기술동향, 2013.05.22.

[5] FedRAMP, “http://www.fedramp.gov”

[6] CSA, “https://cloudsecurityalliance.org/star”

[7] CSA, “Consensus Assessment Initiative Questionnaire(CAIQ) V.3.0.1”, 2014.12

[8] CSA, “Cloud Control Matrix(CCM) V.3.0.1”, 2014.12

[9] CSA, “Auditing the Cloud Controls Matrix Release 2”, 2014.05

[10] CSA Korea(김정덕), “클라우드 보안 관련 국내외 표준/기준 동향”, CSA Korea Summit 발표회 발표자료, 2013

[11] 박영호, “해외 선진사례 분석을 통한 한국형 클라우드 인증제도 분석 및 제안”, 29~34쪽, 세종사이버대학교 정보보호대학원 정보보호학과 석사논문, 2015

[12] ISO/IEC, “ISO/IEC 27017:2015, Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, 2015.12

[13] ISO/IEC, “ISO/IEC 27018:2014, Information technology - Security techniques - Code of practice for protection of personally identifiable information(PII) in public clouds acting as PII processors”, 2014.08

◐ 저 자 소 개 ◑

김 형 구

2002년 동국대학교 컴퓨터멀티미디어학과 학사
2014년 ~ 현재 세종사이버대학교 정보보호대학원 정보보호학과 석사과정
2010년 ~ 현재 (사)한국정보시스템감사통제협회 정보보호거버넌스 간사
2015년 ~ 현재 한국정보보호심사원협회(KISCA) 이사
2002년 ~ 2014년 현대HCN 정보보호파트
2015년 ~ 현재 현대그린푸드 IT실 전략기획파트
관심분야 : 정보보호관리, 개인정보보호