

# 클라우드 컴퓨팅 보안 표준화 동향

박 대하 고려사이버대학교 정보관리보안학과 교수



## 1. 머리말

클라우드 컴퓨팅은 IT 자원의 비용 절감과 협업의 기회를 도모하고 다양한 장치를 통한 접근성과 유연성 확보가 가능하므로 개인과 기업 등 클라우드 사용자의 호응이 높아지고 있다[1]. 하지만 다수의 사용자는 클라우드 컴퓨팅의 도입에 보안이 가장 큰 이슈로 지적하고 있으며, 클라우드 서비스의 가장 큰 우려 사항으로 서비스 제공자의 보안대책에 대한 정보 부족을 들고 있다[2].

클라우드 컴퓨팅 환경에서 제공하는 다양한 서비스의 등장에 발맞추어 국내외의 다양한 표준화 기구(ISO/IEC, ITU, IETF, ETSI, KATS, TTA 등)에서는 전문가 활동을 통해 클라우드 서비스의 보안 이슈를 해결할 수 있는 표준 문서를 지속적으로 개발하고 있다. 본고에서는 정보기술 분야의 대표적인 국제표준화 기관인 ISO/IEC JTC 1과 ITU-T, 그리고 국내 산업표준인 KS를 제정하는 국가기술표준원(KATS) 및 국내 정보통신 분야의 표준을 개발하는 TTA에서 최근 표준 문건으로 개발하였거나 개발 중인 클라우드 컴퓨팅 또는 클라우드 서비스의 정보보호 표준화 작업에 대해서 살펴보고자 한다.

## 2. 국제 표준화 동향

### 2.1 ISO/IEC JTC 1/SC 27 표준화 동향

대표적인 공적 표준화 기관인 ISO와 IEC는 정보기술 전반에 대한 국제표준을 개발하기 위하여 공동으로 표준화 절차와 규정을 제정하여 ISO/IEC JTC 1을 중심으로 긴밀하게 협력하고 있으며, 소위원회(SC, Sub-committee) 중 하나인 SC 27은 정보보호 관리 및 기술 표준화를 담당하는 5개 작업그룹(WG, Working Group)으로 구성되어 있다[3].

이 중에서 정보보호관리체계(ISMS, Information Security Management System)에 관련된 표준을 개발하고 있는 WG 1은 2015년에 클라우드 컴퓨팅 서비스의 정보보호 통제를 위한 최적 실무를 ISO/IEC 27017로 신규 제정하고[4], 아이디 관리와 프라이버시 기술, 프라이버시 연관 바이오인식 기술에 대한 표준을 개발하고 있는 WG 5와 함께 2클라우드 환경에 특화된 프라이버시를 보장하기 위한 데이터 보호 통제의 최적 실무를 2014년에 ISO/IEC 27018로 신규 제정하였다[5]. 또한, 보안 통제 목적과 통제의 구현을 지원하기 위한 서비스와 애플리케이션에 대한 표준 및 지침을 개발하고 있는 WG 4에서는

IT 아웃소싱이나 클라우드 서비스 등에 대한 정보보호를 공급망 관리 측면에서 다루기 위하여 ISO/IEC 27036을 제정하였으며, 그중에서 제4부(Part 4)에서 클라우드 서비스의 보안에 대해 다루고 있다[6].

### 2.1.1 ISO/IEC 27017

ISO/IEC 27017 ‘Code of practice for information security controls based on ISO/IEC 27002 for cloud services(클라우드 서비스를 위한 ISO/IEC 27002 기반의 정보보호 통제 실무 준칙)’은 정보보호관리체계를 구축하기 위한 범용 정보보호 통제인 ISO/IEC 27002(2013년도 개정판)를 기반으로 클라우드 서비스 고객과 클라우드 서비스 제공자 측면에서 모두 적용할 수 있는 보안 통제항목 및 구현지침을 명시하고 있다. ISO/IEC 27002의 114개 통제항목 중에서 35개 정도의 통제항목에 클라우드 서비스에 적합한 새로운 구현지침을 추가하고, 클라우드 서비스에 특화된 확장 통제항목으로 7개가 추가하였다. 새로운 구현지침이 명시된 대표적인 통제 분야에는 정보보호 정책, 인적자원 보안, 접근통제, 암호화, 운영보안, 공급자 관계, 정보보호 사고관리, 준거성 등이 있다. 확장 통제항목으로는 클라우드 서비스 환경의 책임 공유, 서비스 고객의 자산 제거, 가상 컴퓨팅 환경의 분리, 가상머신 보안 강화, 관리자 운영 보안, 클라우드 서비스 모니터링, 가상망과 물리망의 일관성 유지 등을 포함하고 있다.

### 2.1.2 ISO/IEC 27018

ISO/IEC 27018 ‘Code of practice for protection of personally identifiable information(PII) in public clouds acting as PII processors(개인정보보호를 위한 실무 준칙)’은 2013년도 개정판인 ISO/IEC 27002를 기반으로 클라우드 서비스 제공자가 개인정보취급자(표준에서는 ‘공공 클라우드 개인정보

처리자’로 명시)의 역할을 맡아서 수행해야 하는 정보보호 통제에 대해 주로 명시하고 있다. ISO/IEC 27002의 통제항목 중에서 16개의 통제항목에 클라우드 서비스에 적합한 새로운 개인정보보호 구현지침을 추가하고, 개인정보 생명주기의 관리에 대한 내용을 중심으로 25개의 확장 통제항목을 추가하였다. 새로운 개인정보보호 구현지침이 명시된 대표적인 통제 분야에는 정보보호 정책, 접근통제, 암호화, 운영보안, 정보보호 사고관리, 준거성 등을 포함하고 있으며, 확장 통제항목에는 정보주체 권리에 대한 상호협력 의무, 개인정보처리 목적, 개인정보의 상업적 사용 제한, 임시 파일의 안전한 삭제, 하위 계약 처리의 공개, 위반사항 공지, 개인정보 반환과 이전 및 폐기, 개인정보의 지리적 위치 등을 포함하고 있다.

### 2.1.3 ISO/IEC 27036-4

ISO/IEC 27036-4 ‘Information security for supplier relationships - Part 4: Guidelines for security of cloud services(공급망 관계의 정보보호 · 제4부: 클라우드 서비스 보안을 위한 지침)’는 공급망 관계에서 클라우드 서비스 고객과 클라우드 서비스 제공자 간 또는 클라우드 서비스 제공자와 하위 제공자 간의 정보보호 위험을 가시화하고 관리하기 위한 방법을 주로 명시하고 있다. ISO/IEC 27002의 보안 통제를 지원하면서 ISO/IEC 15288과 ISO/IEC 12207에서 명시한 클라우드 기반 제품 및 서비스 생명주기 프로세스에 따라 정보보호 프로세스와 실무를 통합하였다. 클라우드 서비스를 사용하는 조직에서 발생하는 보안 영향을 고려하여 서비스의 도입 및 제공에 따른 위험에 대응하는 방법을 제공하지만 클라우드 서비스와 관련된 업무연속성 관리 및 복구 이슈는 ISO/IEC 27031 ‘ICT Readiness for Business Continuity(업무연속성을 위한 정보통신 준비도)’에서 다루므로 여기서는 제외하고 있다. 2015년 3월

현재 ISO/IEC 27036-4는 DIS 상태이며, 2017년 5월 제정을 목표로 작업이 진행 중이다.

## 2.2 ITU-T SG 17 표준화동향

ITU-T SG 17은 정보통신 기술의 안전한 사용을 위한 네트워크, 서비스, 애플리케이션 정보보호에 대한 국제 표준화를 추진하고 있으며, Q.8(Cloud computing security)을 중심으로 클라우드 컴퓨팅 보안에 대한 연구 과제를 진행하고 있다[7]. 클라우드 컴퓨팅 환경에서 보안을 제공하는 최적 실무와 지침을 개발하고, 클라우드 컴퓨팅 생태계의 참가자와 관련 역할에 대한 책임 명시 및 보안 요구사항 정의, 보안 아키텍처, 보안 관리 및 감사 기술 등을 표준화 대상으로 한다.

2016년 3월 현재, 클라우드 컴퓨팅 보안에 대한 전반적인 위협과 이슈를 분석하여 보안 기능을 매핑할 수 있는 프레임워크로 X.1601[8]이 제정되었고, ISO/IEC 27017과 동일한 내용을 가진 공통 표준으로 X.1631[9]이 개발되었다. 또한, SaaS 애플리케이션 환경의 보안 요구사항을 명시한 X.1602[10]와 클라우드 컴퓨팅의 운영 보안에 필요한 지침을 명시한 X.1642[11]가 조만간 제정될 예정이다. 그 외에도 현재 작업 초안 상태이지만 클라우드 서비스 고객의 데이터 보안에 대한 지침을 제공하는 X.CSCDataSec[12]과 클라우드 컴퓨팅 서비스의 모니터링을 위한 데이터 보안 요구사항을 X.dsms[13]로 제정하고 있는 중이다.

### 2.2.1 ITU-T X.1601

ITU-T X.1601 ‘Security framework for cloud computing(클라우드 컴퓨팅 보안 프레임워크)’은 클라우드 컴퓨팅 환경에서의 보안 위협과 이슈를 분석하고 이를 해결하기 위한 보안 기능을 명시하며, 2015년 10월에 제정되었다. 보안 위협과 보안 이슈는 각각 클라우드 서비스 고객, 클라우드 서비-

스 제공자, 클라우드 서비스 파트너의 측면에서 제시하고 있으며, 신뢰 모델과 식별 및 권한 관리 등을 포함한 14가지의 클라우드 컴퓨팅 보안 기능을 명시하고 있다. 특정한 서비스 환경에서 클라우드 컴퓨팅에 보안 위협 및 이슈를 분석하기 위한 보안 프레임워크를 예제와 함께 제시하고 있으며, 부록에서는 보안 위협 및 이슈와 대응하는 보안 기능을 매핑한 표를 제공하고 있어서 활용도를 높였다.

### 2.2.2 ITU-T X.1602

ITU-T X.1602 ‘Security requirements for software as a service application environment(SaaS 애플리케이션 환경의 보안 요구사항)’은 SaaS 애플리케이션의 성숙도 수준을 분석하고 안전한 서비스 실행 환경을 제공하는 보안 요구사항을 제공한다. SaaS 애플리케이션에 대한 성숙도 수준은 4가지 단계로 구분하며, SaaS 애플리케이션 환경에 대한 보안 요구사항은 공통 요구사항과 클라우드 서비스 제공자의 요구사항 및 클라우드 서비스 파트너의 요구사항으로 제시하고 있다.

### 2.2.3 ITU-T X.1642 등

ITU-T X.1642 ‘Guidelines for the operational security of cloud computing(클라우드 컴퓨팅을 위한 운영 보안 지침)’은 클라우드 서비스 제공자 관점에서 클라우드 서비스에 대한 일반적인 운영 보안 지침을 명시한다. 클라우드 컴퓨팅 운영을 위한 보안 요구사항과 보안 척도를 분석하고, 세부적인 보안 활동(접근통제, 모니터링, 재해복구, 내부감사 등)을 명시하여 클라우드 서비스 제공자에서 발생 할 수 있는 보안 위험에 대처할 수 있도록 지침을 제공하고자 한다. 전기통신 사업자나 인터넷 서비스 사업자)에게 필요한 클라우드 컴퓨팅 인프라의 보안 척도를 제시하여 클라우드 서비스 제공자 측에서 발생할 수 있는 운영 위험을 감소시킬 수 있으며,

특히 보안 조항을 포함한 표준화된 클라우드 SLA의 작성에 도움을 주려는 목적으로 2016년 3월 제정을 목표로 하고 있다.

X.CSCDataSec ‘Guidelines for cloud service customer data security(클라우드 서비스 고객 데이터 보안 지침)’는 클라우드 서비스별로 적용 시나리오와 데이터 생명주기에 따라 요구가 달라지는 서비스 데이터의 보안 통제를 명시하며, 2016년 9월 제정을 목표로 하고 있다. X.dsms ‘Data security requirements for the monitoring service of cloud computing(클라우드 컴퓨팅의 모니터링 서비스를 위한 데이터 보안 요구사항)’은 모니터링 데이터의 범위와 생명주기, 모니터링 데이터 획득 및 보관 등 클라우드 컴퓨팅의 모니터링 서비스에 필요한 데이터 보안 요구사항을 명시하며, 2017년 10월 제정을 목표로 하고 있다.

### 3. 국내 표준화 동향

#### 3.1 KATS 표준화 동향

국내에서는 2014년에 국립전파연구원의 방송통신 표준(KCS)으로 클라우드 서비스 환경의 정보보호 지침(KCS.KO-10.2000[14])과 개인정보보호 지침(KCS.KO-10.2001[15])이 제정된 후 현재는 국가 기술표준원(KATS)이 관리하는 산업표준(KS)으로 통합되었다.

##### 3.1.1 KCS.KO-10.2000

KCS.KO-10.2000 ‘클라우드 서비스 제공자의 정보보호 지침’은 클라우드 서비스 제공자가 안전한 클라우드 서비스를 제공하기 위해 고려할 관리적·기술적 정보보호 지침을 정의하고 있다. 클라우드 서비스 제공자의 정보보호 프레임워크를 거버넌스, 관리 프로세스, 기술 프로세스 영역으로 구분하여 정의하고 있으며, 영역별로 안전한 클라우드 서비-

스를 제공하기 위해 클라우드 서비스 제공자가 고려해야 하는 정보보호 지침을 제공한다.

##### 3.1.2 KCS.KO-10.2001

KCS.KO-10.2001 ‘클라우드 서비스 제공자의 개인정보보호 지침’은 클라우드 서비스 제공자가 클라우드 서비스 사용자의 개인정보를 안전하게 수집, 저장, 관리, 이용할 수 있도록 개인정보보호 관리와 개인정보 생명주기 관리를 중심으로 클라우드 서비스를 위한 개인정보보호 프레임워크를 제시하고 이를 기반으로 고려해야 할 지침을 제공한다. 개인정보보호 관리를 위한 8개의 영역(정책, 조직, 인력, 자산분류, 접근통제, 사후관리, 공급망 위험관리, 법적 및 계약적 요구사항 준수)과 개인정보 생명주기 관리를 위한 4개의 영역(개인정보 수집, 저장 및 관리, 이용 및 제공, 파기)으로 구분하여 프레임워크를 설정하고 있다.

#### 3.2 TTA 표준화 동향

TTA는 정보통신단체표준(TTAS)로 클라우드 서비스 도입을 위한 자가진단 지침(TTAK.KO-10.0893[16]), ITU-T X.1601의 한글판인 클라우드 컴퓨팅을 위한 보안 프레임워크(TTAE.IT-X.1601[17]), 퍼스널 클라우드 개인정보보호 참조모델(TTAK.KO-10.0616[18]), 퍼스널 클라우드 보안 프레임워크(TTAK.KO-10.0533[19]), 공공 클라우드 컴퓨팅의 보안 및 프라이버시 보호 지침(TTAE.OT-12.0015[20]) 등을 제정하였다. 최근에는 ICT 표준화 포럼에 대한 지원 사업을 기반으로 ‘클라우드 컴퓨팅 표준화 포럼’ 등에서 자체적인 포럼 표준의 개발을 유도하고 있다.

## 4. 맷음말

본고에서는 ISO/IEC JTC 1/SC 27과 ITU-T SG 17을 중심으로 클라우드 컴퓨팅 환경의 최신 국제 보안 표준화 동향과 KATS 및 TTA를 중심으로 하는 국내 보안 표준화 동향을 정리하여 안전한 클라우드 서비스의 제공과 사용에 대한 기준을 설정하는 데 도움을 주고자 하였다. 특히 최근 국제적으로 클라우드 서비스의 보안성 평가 및 인증을 위한 ISMS, FedRAMP 등의 제도가 글로벌 또는 로컬 표준을 기반으로 진행되고 있는 점을 감안할 때, 국내에서도 국제 표준의 수용 및 지역화를 위한 노력이 수반되어야 한다.

클라우드 산업의 활성화를 위한 국가적인 차원의 노력(예: 2009년 ‘범정부 클라우드 컴퓨팅 활성화 종합계획’ 발표)이 성과를 거두기 위하여 단순히 표준화 작업에만 그치지 않도록 표준의 활용을 장려하는 법 제도의 지원이 함께 이루어지는 것이 바람직하다. 

## [참고문헌]

- [1] Christopher Barnatt, ‘A brief guide to cloud computing’, Constable & Robinson, pp. 22-28, 2010.
- [2] Nakao Koji, ‘The art of information security technology for introducing cloud’, Network Security Forum 2011, Tokyo, 2011.
- [3] 김정덕, ‘정보보호관리 국제표준화 동향’, 정보보호학회지, 21(2), pp.19-22, 2011.
- [4] ISO/IEC 27017:2015, ‘Code of practice for information security controls based on ISO/IEC 27002 for cloud services’, 2015.
- [5] ISO/IEC 27018:2014, ‘Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors’, 2014.
- [6] ISO/IEC DIS 27036-4, ‘Information security for supplier relationships - Part 4: Guidelines for security of cloud services’, 2016.
- [7] 염홍열, 윤미연, ‘클라우드 컴퓨팅 보안 국제 표준화 동향’, 정보보호학회지, 23(3), pp.14-18, 2013.
- [8] ITU-T X.1601, ‘Security framework for cloud computing’, 2015.

- [9] ITU-T X.1631, ‘Code of practice for information security controls based on ISO/IEC 27002 for cloud services’, 2015.
- [10] ITU-T X.1602 (X.sfcse), ‘Security requirements for software as a service application environment’, 2015.
- [11] ITU-T X.1642 (X.goscc), ‘Guidelines for the operational security of cloud computing’, 2015.
- [12] ITU-T X.CSCDataSec, ‘Guidelines for cloud service customer data security’, 2015.
- [13] ITU-T X.dsms, ‘Data security requirements for the monitoring service of cloud computing’, 2015.
- [14] 방송통신표준 KCS.KO-10.2000, ‘클라우드 서비스 제공자의 정보 보호 지침’, 2014.
- [15] 방송통신표준 KCS.KO-10.2001, ‘클라우드 서비스 제공자의 개인정보 보호 지침’, 2014.
- [16] 정보통신단체표준 TTAK.KO-10.0893, ‘클라우드 서비스 도입을 위한 보안 자가진단 지침’, 2015.
- [17] 정보통신단체표준 TTAE.IT-X.1601, ‘클라우드 컴퓨팅을 위한 보안 프레임워크’, 2014.
- [18] 정보통신단체표준 TTAK.KO-10.0616, ‘퍼스널 클라우드 개인정보 보호 참조모델’, 2012.
- [19] 정보통신단체표준 TTAK.KO-10.0533, ‘퍼스널 클라우드 보안 프레임워크’, 2011.
- [20] 정보통신단체표준 TTAE.OT-12.0015, ‘공공 클라우드 컴퓨팅의 보안 및 프라이버시 보호 지침’, 2011.