편집위원 : 김정녀(ETRI)

클라우드 컴퓨팅 보안 국제표준화 동향

문종호, 김지예, 원동호
성균관대학교

요 약

클라우드 컴퓨팅은 IT 자원(스토리지, 서버, 소프트웨어, 네트워크 등)을 인터넷 기술을 이용하여 서비스 형태로 제공하는 기술이다. 최근 클라우드 컴퓨팅 서비스의 영역이 지속적으로 확대되고 있으며 특히 사물인터넷 (Internet of Things) 등의 IT 기술 발전에 따라 가정, 의료 등에 클라우드 컴퓨팅을 접목하여 활용할 수 있는 방법이 활발히 연구되고 있다. 그러나 클라우드 컴퓨팅 서비스의 확산과 더불어 알려지지 않은 새로운 보안 위협, 클라우드 서비스 고객의 자기정보 통제권 상실, 개인정보 유출로 인해 발생하는 프라이버시 침해 또한 이슈가 되고 있다. 본 논문에서는 클라우드 보안을 위한 국제 표준화 기구와 해당 기구에서 추진 중인 국제 표준화 현황에 대해 살펴본다.

Ⅰ. 서 론

클라우드 컴퓨팅 서비스는 사용자의 위치에 관계없이 언제 어디서나 사용자의 단말기를 통해 다양한 플랫폼, 네트워크, 어플리케이션 서비스, 하드웨어 등의 자원을 필요한 만큼 임대해서 사용할 수 있는 서비스이다[1]. 클라우드 서비스 제공자는 별도의 정보 자산을 구입하여 직접 운영하는 대신 클라우드 사업자로부터 이를 임대하여 운영함으로써 비용을 절약할 수 있다. 이러한 장점 때문에 국내외의 클라우드 서비스 제공자가 지속적으로 증가하고 있으며 서비스의 영역 또한 점차 확대되고 있다.

클라우드 컴퓨팅의 기본 개념은 2006년부터 등장하였으나 표준화 관점에서 보면 2007년부터 일부 사실(de facto) 표준화 기구들이 클라우드 관련 작업을 시작하였으며 본격적으로 국제 표준화 추진이 시작된 것은 2011년 이후라고 할 수 있다[1][2][3]. 그러나 표준화 진행 속도에 비해 실질적인 서비스 개발 및 보급이 더 먼저 이루어져 왔다. 이로 인해 알려지지 않은 새로운 보안 위협, 클라우드 서비스 고객의 자기정보 통제권 상실, 개인정보 유출로 인한 프라이버시 침해 등의 문제가 야기될 것으로 예상되며 클라우드 서비스 고객의 데이터 손실이나 유출, 비인가된 사용자에 대한 불법적인 접근 등의 잠재적인 위협 또한 이슈가 되고 있다. 이러한 위협으로부터 고객의 정보나 데이터를 보호하기 위한 다양한 보안 대책들이 수립되어야 하며 클라우드 서비스를 안전하게 제공하기 위한 표준화 작업도 시급하게 요구된다.

클라우드 컴퓨팅 보안을 위한 국제 표준화 활동은 두 개의 공적(de jeure) 표준화기구인 국제전기통신연합-전기통신표준화부문 연구반 17(ITU-T SG17) [4]과 국제표준화기구/국제전기표준화위원회 합동기술위원회 1 연구그룹 27(ISO/IEC JTC 1/SC 27) [5] 에서 진행되고 있다.

본 논문의 구성은 다음과 같다. 제 2장에서는 ITU-T SG13 및 SG17에서 추진 중인 클라우드 보안 국제 표준화 동향을 제시하고, 제 3장에서는 ISO/IEC JTC 1/SC 27에서 추진 중인 국제 표준화 동향을 살펴본다. 제 4장에서는 클라우드 표준화 관련 사실 기구들의 주요 활동에 대해 살펴보고 마지막으로 제 5장에서 향후 추진 사항에 대한 내용으로 결론을 맺는다.

Ⅱ. ITU-T 국제 표준화 동향

국제전기통신연합(ITU, International Telecommunication Union)은 1865년에 설립된 국제전신연합으로 가장 오래된 국제기구이다. ITU-T는 전기통신기술, 운용, 요금과 관련된 사항에 대해 연구를 진행하고 있으며 연구반(SG, Study Group)을 설립하여 연구과제(Question) 수행을 통해 새로운 통신 기반 설비 체계 및 서비스 등에 관한 표준을 수립하고 있다. 특히 ITU-T SG17은 정보보호에 대한 국제 표준화를 담당하고 있으며 ITU-T SG13은 미래 네트워크에 대한 국제 표준의 개발을 맡고 있다[2]. ITU-T SG13 및 SG17에서 진행되고 있는 클라우드 컴퓨팅 보안에 대한 표준화 연구과제[4][6]는 다음의 〈표 1〉과 같다.

2013년 2월, ITU-T SG 13 회의에서는 클라우드 보안 연구에 대한 역할 할당을 위해 14개의 태스크를 식별하였으며 클라

표 1. SG13/SG17 Cloud Security Question

Study Group	Question	Title
13	17	Requirements, Ecosystem, and General Capabilities for Cloud Computing and Big Data
	18	Cloud Functional Architecture, Infrastructure and Networking
	19	End-to-end Cloud Computing Management and Security
17	3	Telecommunication Information Security Management
	8	Cloud Computing Security
	10	Identity Management Architecture and Mechanisms

표 2. SG13 Cloud Security Standard

Question	Standard	Title
17	Y.3501-ed2	Cloud Computing Framework and High-Level Requirements-Edition 2
	Y.3600 (ex Y.BigData-reqts)	Requirements and Capabilities for Cloud Computing based Big Data
18	Y.3510-ed2	Cloud Computing Infrastructure Requirements
	Y.CCIC-arch	Cloud Computing – Functional Architecture of Inter-Cloud Computing
	Y.CCNaaS-arch	Cloud Computing – Functional Architecture of Network as a Service
19	M.rcsm	Requirements for Cloud Service Management
	Y.3520 Rev.1 (ex Y.3520 ed2)	Cloud Computing Framework for End-to-end Resource Management
	Y.cctic	Cloud Computing Trusted Inter-Cloud
	Y.e2ecslm-Req	End-to-end Cloud Service Lifecycle Management
	Y.inter-cloud-sec	Security Aspects of Inter-Cloud Computing
	Y.oe2eccm/ M.oe2eccm (ex Y.e2ecm; Y.e2ecmrgb)	Overview of e2eCloud Computing Management

표 3. SG17 Cloud Security Standard

Question	Standard	Title
3	X.1051rev	Information Technology – Security Techniques – Code of Practice for Information Security Controls based on ISO/IEC 27002 for Telecommunications Organizations
	X.gpim	Information Technology – Security Techniques – Code of Practice for Personally Identifiable Information Protection
	X.sgsm	Information Security Management Guidelines for Small and Medium Telecommunication Organizations
	X.sup-gpim	Supplement to ITU-T X.gpim Code of Practice for Personally Identifiable Information Protection based on ITU-T X.gpim for Telecommunications Organizations
8	X.1601	Security Framework for Cloud Computing
	X.CSCDataSec	Guidelines for Cloud Service Customer Data Security
	X.goscc	Guidelines of Operational Security for Cloud Computing
	X.sfcse	Security Requirements for SaaS Application Environments
10	X.1255sup	Supplement to Recommendation ITU-T X.1255, Proposed Conceptual Models based on ITU-T X.1255 Frameworks
	X.authi	Guidelines and Framework for Sharing Network Authentication Results with Service Applications
	X.eaaa	Enhanced Entity Authentication based on Aggregated Attributes
	X.iamt	Identity and Access Management Taxonomy

표 4. SG13/SG17 Security Tasks Collaboration

Task	Group
Example Cloud Security Use Cases	SG13
Functional Architecture	
Identify the Security Threats (Identify Cloud Computing Security for Service Categories and Deployment Models)	Common Project
Generic Security Requirements based on Threats Analysis and Use Cases	
Allocation of Security Functions to Cloud Computing Architecture Layers and Functional Blocks	
Defining Trust Models	
Identity Areas where is a Lack of Security Capabilities and Mechanisms	SG17
Detailed Description of Security Functions	
Fundamental Concepts for Security Architectures	
Existing/New Security Mechanism (Applicable to Cloud Computing Service Categories and Deployment Models)	
Security Management (ISMS Family: working with JTC 1/SC 27)	
Security Best Practices & Operational Security	

표 5. Cloud Computing Security Working Group

Working Group	Title
1	Information Security Management Systems
4	Security Controls and Services
5	Identity Management and Privacy Technologies

우드 컴퓨팅의 보안 구조에 대한 기본 개념 관리, 기능 세부 사항, 운영 등은 SG17에서 담당하고 보안 위협 식별, 보안 요구사항, 보안기능 할당, 신뢰모델 정의 등의 4가지 태스크를 SG17이 주도하고 SG13과 공통으로 수행하는 프로젝트를 통해 진행하는 것으로 합의하였다.

공통 프로젝트(Common Project)는 SG13 및 SG17의 두 연구반이 공동으로 개발하는 권고로써, 이 공통 프로젝트마다 주도 연구반(Principal Study Group)을 할당해 신규 권고를 신설하고 권고 채택을 최종적으로 승인하도록 하고 있다.

ITU-T SG13 및 SG17에서 현재 진행되고 있는 클라우드 컴퓨팅 보안관련 표준은 〈표 2〉, 〈표 3〉과 같으며, 최종적으로 합의된 두 연구반 간의 클라우드 보안 관련 태스크 할당은 〈표 4〉와 같다.

현재 대부분의 표준 연구가 SG17의 Q.3 및 Q.8에서 수행되고 있다.

Ⅲ. ISO/IEC JTC 1 국제 표준화 동향

ISO/IEC JTC 1/SC 27은 정보보안기술에 대한 국제 표준화를 추진하고 있는 공적 표준화 연구그룹이다[5]. 연구그룹 27의 클라우드 컴퓨팅 보안 표준화는 〈표 5〉와 같이 SC 27 산하에 있는 작업그룹(WG, Working Group) 1, 4, 5에서 추진하고 있다.

ISO/IEC JTC 1/SC 27은 2010년 10월 베를린 회의에서 일본의 제안에 의해 클라우드 컴퓨팅 보안에 대한 국제 표준화 작업을 착수하게 되었으며[7] 작업그룹 1에서는 클라우드 컴퓨팅 보안 관리 기술 측면, 작업그룹 4에서는 클라우드 컴퓨팅 보안 서비스 측면, 작업그룹 5에서는 클라우드 컴퓨팅 보안 프라이버시 측면에서 각 표준 초안 개발 및 신규 표준화 아이템 발굴을 위한 연구를 활발히 진행하고 있다.

ISO/IEC JTC 1/SC 27 산하 3개의 작업그룹에서 현재 개발하고 있는 국제 표준은 〈표 6〉과 같이 SLA(Service Level Agreement) 프레임워크 및 기술(ISO/IEC 19086-4), 클라우드 컴퓨팅 서비스 사업자를 위한 보안 통제 지침(ISO/IEC 27017), 클라우드 사업자를 위한 데이터 보호 통제 지침 (ISO/IEC 27018), 그리고 클라우드 서비스 보안 가이드라인(ISO/IEC 27036-4) 등이다.

ISO/IEC JTC 1/SC 27은 정보 보호를 위한 일반적인 방법에 대한 표준화, 보안 서비스를 위한 요구사항 명세, 암호화 알고리즘의 표준화, 보안 기술 및 메커니즘 개발, 문서 및 표준화를

표 6. JTC 1/SC 27 Standard

No	Title
ISO/IEC 19086-4	Information technology – Cloud computing – Service level agreement (SLA) Framework and Technology – Part 4: Security and Privacy
ISO/IEC 27017	Information Technology – Security Techniques – Code of Practice for Information Security Controls based on ISO/IEC 27002 for Cloud Services
ISO/IEC 27018	Information Technology – Security Techniques – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors
ISO/IEC 27036-4	Information Technology – Information Security for Supplier Relationships – Part 4: Guidelines for Security of Cloud Services

표 7. Security Guidance for Critical Areas Focus in Cloud Computing

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

지원하는 관리 개발을 주로 수행하고 있다.

Ⅳ. 클라우드 보안 관련 기구 활동

클라우드 컴퓨팅 국제 표준화는 초기부터 주로 사실(de facto) 표준화 기구 중심으로 진행되어 왔으며 NIST, ENISA, CSA, DMTF, OASIS, GICTF 등의 기구들을 통해서 다양한 표준화 시도가 진행되고 있다.

하지만 일부 사실표준화 기구를 제외한 대부분의 활동들이 분산된 이해 집단을 통해 추진되고 있으며 최근에는 오픈 스택(OpenStack)과 같은 오픈 소스 기반의 클라우드 플랫폼이 기업을 중심으로 활용 가치를 높이면서 사실상의 표준으로 대두되고 있는 추세이다.

1. NIST[8][9]

NIST(The National Institute of Standards and Technology)는 최근 미국 정부 클라우드 컴퓨팅 기술 로드맵 I, II를 발간하였다. 해당 로드맵은 연방정부의 클라우드 컴퓨팅 채택을 가속화시키는 전략에 초점을 맞춘 것으로 세계 각국에서 보내온 200개 이상의 코멘트를 반영하여 작성되었다.

- **볼륨 I(High-Priority Requirements to Further USG Agency Cloud Computing Adoption)**: 로드맵의 목적과 범위를 설명한다. 보안, 상호 운용성(시스템끼리 함께 작업할 수 있는 능력), 이식성(한 클라우드에서 다른 클라우드 시스템으로 이동할 수 있는 능력)의 3가지 우선순위에 초점을 맞췄다.
- **볼륨 II(Useful Information for Cloud Adopters)**: 개념적인 모델로써 NIST 클라우드 컴퓨팅 참조 아키텍처 및 분류, 그리고 미국 정부 클라우드 타켓 비즈니스 및 기술 사례를 소개한다. 또한 볼륨 II는 현재 클라우드 모델에 적용되는 표준들을 조사하여, 신규 및 개정 표준이 필요한 우선순위를 다뤘다.

2. ENISA[10]

유럽연합(EU, European Union)의 사이버 보안 담당 기관인

ENISA(European Network and Information Security Agency)는 유럽연합 회원국 정부 및 공공기관의 클라우드 서비스 도입을 위한 프레임워크를 개발 및 보급하고 있다. 특히, ENISA가 발간한 '정부 클라우드를 위한 보안 프레임워크'는 정부의 클라우드 서비스 조달 및 보안을 위한 단계적 가이드를 상세하게 기술하고 있다. 정부의 클라우드 도입 시 공통적으로 필요한 보안 프레임워크를 기술하였으며 에스토니아, 그리스, 스페인, 영국 등 4개 회원국의 정부 클라우드 도입 사례 연구를 바탕으로 작성되었다. 해당 프레임워크는 PDCA(Plan-Do-Check-Act) 라이프사이클에 따라 9개의 보안 행동(Security Activity) 및 14개의 보안 단계(Security Steps)로 구성되어 있다.

3. CSA[11]

2008년 11월 20일에 개최된 보안 실무자 컨퍼런스인 ISSA(Information Systems Security Association) Forum에서 탄생한 CSA(Cloud Security Alliance)는 클라우드 컴퓨팅의 안전성 증진과 보안 인증을 위한 성공 사례 구현, 사용자 교육 등을 목적으로 만든 비영리 기관이다. CSA는 클라우드 도입에 있어 필요한 가이드라인을 〈표 7〉과 같이 크게 3개 영역으로 구분하고 14가지 세부 항목으로 제시하고 있다.

4. DMTF[12]

DMTF(Distributed Management Task Force)는 기업 및 분산 네트워크 환경을 대상으로 오픈 클라우드 표준 인큐베이터(Open Cloud Standards Incubator)를 통하여 공공 클라우드(Public Cloud)와 개인 클라우드(Private Cloud)간 상호 호환에 대한 표준을 개발하고 있다. 특히 공공 정보 모델, 정책 기반 보안관리를 위한 툴킷, 분산 네트워크 보안, 관리형 클라우드 화이트 페이퍼를 위한 구조, 클라우드 감사 데이터 연계 방법에 대한 연구를 주로 수행하고 있다.

5. OASIS[13]

OASIS(Identity in the Cloud TC)에서는 클라우드 환경에서의 식별자(Identity) 기술 규격을 개발하고 있다.

6. GICTF[14]

NTT, 히타치제작소 등 일본 기업들과 민간 전문가들로 구성된 GICTF(Global Inter-Cloud Technology Forum)은 보안 전담그룹은 없지만 재난상황이나 비상상황이 발생했을 경우 클라우드 서비스의 비즈니스 연속성 및 복구에 대한 연구를 진행하고 있다. 특히 제 2차 ITU-T Focus Group Cloud 회의에서는 GICTF에서 정의한 클라우드 간 서비스 사용 방법이 표준 문서에 포함되었다.

7. CCIF[15]

CCIF(Cloud Computing Interoperability Forum)는 글로벌 형태의 클라우드 컴퓨팅 생태계(Ecosystem)를 목표로 설립된 기구로서 단일화된 인터페이스(UCI, Unified Cloud Interface)로 정보를 교환하는 하나 이상의 클라우드 플랫폼을 위한 프레임워크와 온톨로지 개발을 목표로 하고 있다. CCIF는 UCI 프로젝트 추진을 통해 다양한 클라우드 API(Application Programming Interface)를 통합하여 표준화되고 개방된 클라우드 인터페이스를 개발하고 있다.

8. SNIA[16]

모든 공급업체를 위한 포괄적인 무역협회인 SNIA(Storage Networking Industry Association)는 스토리지 관련 표준, 기술, 포괄적인 교육 서비스 등을 지원하는 비영리 단체로서 미래의 스토리지 산업 표준 주도를 목표로 하고 있다. SNIA는 CSI(Cloud Storage Initiative) 구성을 선언하고 성공적인 클라우드 스토리지 시장 확대를 위해 클라우드 상에서 데이터를 저장하는 표준과 인터페이스 표준 등을 개발하고 있다.

Ⅴ. 결 론

본 논문에서는 클라우드 컴퓨팅 보안에 대한 국제 표준화 기구과 활동 동향에 대해 분석하였다. 클라우드 컴퓨팅 서비스는 사용자의 단말을 통하여 사용자의 위치에 관계없이 언제 어디서나 편리하게 사용자의 요구에 따라 다양한 플랫폼, 네트워크, 어플리케이션 서비스, 하드웨어 등의 자원을 필요한 만큼 임대해서 사용할 수 있는 서비스이다. 국내에서도 오픈스택 등을 활용하여 클라우드 서비스를 제공하는 기업들이 증가하고 있으며 이에 따라 클라우드 서비스에 대한 보안의 중요성은 더욱 증가하고 있다.

클라우드 컴퓨팅에 대한 표준화는 2010년 이전에는 사실 표준화 기구를 중심으로 연구가 진행되어 왔고, 2010년이 되어서야 국제 공식 표준화 기구를 통해 표준화 작업이 시작되었다. 국제 표준화 기구인 ITU-T SG13 및 SG17과 ISO/IEC JTC 1/SC 27에서는 지속적인 논의와 회의를 통해 각종 표준들을 신설하고 통합, 수정하여 클라우드 컴퓨팅의 국제 표준화를 선도하고 있으며, 사실 표준화 기구에서도 다양한 관점에서 표준을 정의하고 개발하고 있다. 국내에서도 클라우드 컴퓨팅 관련 기업 및 기관을 중심으로 국제 표준화 추진 및 협력, 보안성 강화 방안 마련을 위한 전략 수립 및 개발이 필요할 것으로 보인다.

본 논문에서 제공하고 있는 클라우드 컴퓨팅 보안에 대한 국제 표준화 현황 분석이 향후 클라우드 컴퓨팅 서비스를 제공하려는 서비스 제공자나 표준화 기관 등에 유용하게 활용될 수 있기를 기대한다.

참 고 문 헌

[1] 이강찬, 이승윤. "클라우드 컴퓨팅 표준화 동향 및 전략." 전자통신동향분석, pp. 90-99

[2] 염흥렬, 윤미연. "클라우드 컴퓨팅 보안 국제 표준화 동향", 정보보호학회지, pp. 14-18

[3] 김태경, 나재훈. "클라우드 보안 표준화와 향상된 인증 방안", 정보보호학회지, pp. 21-24

[4] ITU-T SG 17 website, http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx

[5] ISO/IEC JTC 1/SC 27 website, http://www.iso.org/iso/iso_technical_committee?commid=45306

[6] ITU-T SG 13 website, http://www.itu.int/en/ITU-T/studygroups/2013-2016/13/Pages/default.aspx

[7] 오홍룡, 김영화, 진병문. "클라우드 컴퓨팅 보안 국제 표준화 연구", 한국통신학회 종합 학술 발표회 논문집(하계) 2013, pp. 1027-1028

[8] NIST Cloud Computing Standards Roadmap, http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

[9] TTA. "해외 ICT 표준화 동향", 2014.10

[10] ENISA, https://www.enisa.europa.eu/

[11] CSA Security Guidance Version 3, https://cloudsecurityalliance.org/group/security-guidance/

[12] DMTF, http://www.dmtf.org

[13] OASIS, https://www.oasis-open.org/committees/id-cloud/

[14] GICTF, http:// http://www.gictf.jp/

[15] CCIF, http://www.cloudforum.org/

[16] SNIA, http://www.snia.org

약 력

문 종 호

2012년 성균관대학교 공학사
2014년 성균관대학교 공학석사
2015년~현재 성균관대학교 전자전기컴퓨터공학과 박사과정
2014년~2015년 ㈜시큐아이 보안서비스개발팀
관심분야: 사용자 인증, 암호학, 키관리 등

김 지 예

1999년 성균관대학교 공학사
2007년 이화여자대학교 컴퓨터교육학석사
2013년~현재 성균관대학교 전자전기컴퓨터공학과 박사과정
1999년~2013년 ㈜팬택 소프트웨어 개발그룹
관심분야: 사용자 인증, 암호학, 키관리 등

원 동 호

1976년 성균관대학교 공학사
1978년 성균관대학교 공학석사
1988년 성균관대학교 공학박사
1982년~2015년 성균관대학교 교수
2015년~현재 성균관대학교 행단석좌교수
관심분야: 암호이론, 정보시스템 보안 등