情 報 保 護 學 會 誌
第23卷 第3號, 2013. 6

클라우드 컴퓨팅 보안 국제 표준화 동향

염 흥 열*, 윤 미 연**

요 약

클라우드 컴퓨팅 서비스는 클라우드 서비스 고객에게 편리하면서도 온디맨드 (on-demand) 방식으로 풀 형태로 준비되어 있는 공유 자원 (네트워크, 서버, 메모리, 어플리케이션, 그리고 서비스) 을 제공한다. 클라우드 컴퓨팅 서비스의 확산을 위해서 가장 우려되는 것은 보안 위협과 클라우드 서비스 고객의 정보 통제권 상실과 개인정보 유출 등의 프라이버시 이슈이다. 클라우드 컴퓨팅 보안을 위한 국제 표준화 활동은 두 개의 공적 표준화 기구인 국제전기통신연합-전기통신표준화부문 연구반 17 (ITU-T SG 17) [1]과 국제표준화기구/국제전기표준화위원회 합동기술위원회 1 연구그룹 27(ISO/IEC JTC 1/SC 27) [3] 에서 주로 수행되고 있다. 본 논문에서는 클라우드 컴퓨팅 보안을 위해 양대 공적 국제 표준화 기구에서 추진 중인 동향을 제시하고, 이를 근거로 향후 표준화 추진 방향을 제시하고자 한다.

Ⅰ. 서 론

클라우드 컴퓨팅 서비스는 클라우드 서비스 고객에게 편리하면서도 온디맨드 (on-demand) 방식으로 풀형태로 준비되어 있는 공유 자원 (네트워크, 서버, 메모리, 어플리케이션, 그리고 서비스) 을 제공한다. 클라우드 서비스 고객은 별도의 자신만을 위한 정보자산을 구입하여 운영하는 대신에, 이를 사업자로부터 임대해 사용함으로써, 비즈니스 경제성을 확보할 수 있다. 클라우드 배치 모델 (deployment model)은 인프라, 플래폼, 소프트웨어, 그리고 네트워크를 서비스로 제공하는 4 가지 서비스 모델을 갖는다. 그러나, 클라우드 컴퓨팅 서비스의 확산을 위해서 가장 우려되는 것은 보안 위협과 클라우드 서비스 고객의 정보 통제권 상실과 개인정보 유출 등의 프라이버시 이슈이다. 또한, 제3의 신뢰 인증기관이 클라우드 서비스 사업자가 필요한 보호대책을 적절히 준비하고 운영하는지를 검사하여 사업자를 인증하기 위한 인증기준은 국가나 지역 차원이 아닌 글로벌 차원에서 합의되어야 한다. 대표적인 클라이언트 컴퓨팅 서비스 고객에 미치는 위협은 고객의 데이터의 손실이나 유출, 비인가된 사용자에 의한 고객 클라우드 서비스로의 불법 접근, 그리고 클라우드 서비스 이용자 내부자에 의해 초래되는 여러 가지 위협 등이 존재하며, 이러한 위협을 막기 위한 다양한 보호대책들이 식별되어야 한다. 클라우드 컴퓨팅 보안을 위한 국제 표준화 활동은 두 개의 공적 표준화기구인 국제전기통신연합-전기통신표준화부문 연구반 17 (ITU-T SG 17) [1]과 국제표준화기구/국제전기표준화위원회 합동기술위원회 1 연구그룹 27(ISO/IEC JTC 1/SC 27) [3] 에서 수행되고 있다.

그러나, 클라우드 컴퓨팅 서비스의 확산을 위해서 가장 우려되는 것은 보안 위협과 개인정보 유출 등의 프라이버시 이슈이다. 대표적으로 현재 다양한 형태로 제공되고 있는 클라우드 컴퓨팅 서비스의 상호운용성을 제공하기 위해서는 국제 표준의 개발이 요구된다. 대표적인 클라이언트 컴퓨팅 서비스 고객에 미치는 위협은 고객의 데이터의 손실이나 유출, 비인가된 사용자에 의한 클라우드 고객 서비스 불법 접근, 그리고 클라우드 서비스 이용자 내부자에 의한 위협이 존재한다.

클라우드 컴퓨팅 보안을 위한 국제 표준화 활동은 두 개의 공적 표준화기구인 ITU-T SG 17과 ISO/IEC JTC 1/SC 27에서 수행되고 있다.

본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 연구결과로 수행되었음(개인정보보호관리체계(PIMS) 국제 표준 개발, No. 2013-PK10-19).
* 순천향대학교 정보보호학과 교수, 정보보안산업표준포럼 의장 (hyyoum@sch.ac.kr)
** 한국인터넷진흥원 책임연구원 (myyoon@kisa.or.kr)

〔표 1〕 연구반 17에서 클라우드 컴퓨팅 보안 연구과제

번호	연구과제 제목	주요 표준화 내용
Q.8/17	클라우드 컴퓨팅 보안	보안 요구사항, 보안 구조, 모범 사례, 클라우드 컴퓨팅 보안 관리 지침 등
Q.3/17	통신망 정보보호관리 체계	통신망 정보보호관리체계 지침, 개인정보보호관리체계 지침 등
Q.10/17	ID 관리 구조 및 메카니즘	ID 관리 구조, 요구사항, 보안 능력 등

본 논문의 구성은 다음과 같다. 제2장에서는 ITU-T에서 추진 중인 국제 표준화 동향을 제시하고, 제3장에서는 ISO/IEC JTC 1/SC 27에서 추진 중인 국제 표준화 동향을 살펴본다. 그리고 4장에서는 향후 추진 사항으로 결론을 맺는다.

Ⅱ. ITU-T 국제 표준화 동향

2.1 ITU-T SG 17

ITU-T SG 17 은 정보보호에 대한 국제 표준화를 추진하고 있는 ITU-T 내의 연구반이다[1]. 연구반 17에서 클라우드 컴퓨팅 보안에 대한 표준화를 추진하는 표준화 그룹은 [표 1[과 같이 연구과제 3, 8, 10 이며, 주도하는 연구과제(Question)는 Q.8/17 이다. Q.8/17은 논문 작성 당시에 [표 2]와 같이 5개의 국제 표준을 개발하고 있다. 이와 더불어 연구과제 3(통신망 정보보호관리체계)과 연구과제 10(ID 관리 구조 및 메카니즘)도 클라우드 컴퓨팅 보안 국제 표준 개발을 지원 또는 추진하고 있다. 특히 연구과제 3은 클라우드 서비스 이용을 위한 보안 통제에 대한 국제 표준 개발을 ISO/IEC JTC 1/WG 1과 협력해 지원하고 있고, 연구과제 10은 클라우드 컴퓨팅 환경에서 ID 관리 표준을 개발하고 있다. 이를 정리하면 [표 2]와 같다.

2.2 ITU-T SG 13

ITU-T SG13 (미래 네트워크)은 ITU-T 내에서 미래 네트워크에 대한 국제 표준을 개발하는 연구반이다. 또한, SG13은 클라우드 컴퓨팅 국제 표준화 추진을 위한 조정 활동을 수행하는 조인트 조정 활동 (JCA, joint coordination activity) 의 부모 연구반(parent study group)이기도 하다[2]. 이번 연구회기(2013-2016)동안 클라우드 컴퓨팅 국제 표준화를 위해 3개의 연구과제를 [표 3]과 같이 신설해 보안이 아닌 부문을 중심으로 클라우드 컴퓨팅 국제 표준을 개발하고 있다.

2.3 SG13과 SG17간의 업무 조정

클라우드 컴퓨팅 보안 국제 표준은 연구반 17이 중심이 되어야 하나, 클라우드 기능 구조 등과 연관된 경우, 연구반 13과 긴밀한 협력 하에 일관성을 유지하는 국제 표준화 추진이 요구되었다. 이에 따라 2012년 ITU 두바이 세계정보통신표준총회 (WTSA-12) 에서는 ITU-T

〔표 3〕 연구반 13 클라우드 컴퓨팅 관련 연구과제

번호	연구과제 제목
Q.17/13	클라우드 컴퓨팅 에코시스템, 일반 요구사항, 능력
Q.18/13	클라우드 기능구조, 인프라, 네트워킹
Q.18/13	종단간 서비스 및 자원할당

〔표 2〕 ITU-T SG17에서 개발중인 클라우드 컴퓨팅 보안 국제 표준

표준화 기구	국제 표준	제목	개발주체
ITU-T SG 17	ITU-T X.ccsec	High-level security framework for cloud computing [4]	Q.8/17
	ITU-T X.fsspvn	Framework for a secure service platform for virtual network [5]	Q.8/17
	ITU-T X.goscc	Guidelines of operational security for cloud computing [6]	Q.8/17
	ITU-T X.sfcse	Security functional requirements for Software as a Service (SaaS) application environment [7]	Q.8/17
	ITU-T X.cc-control	ITU-T X.cc-control/ISO/IEC 27017 – Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 [8]	Q.8/17
	ITU-T X.idm-cc	Requirement of IdM in cloud computing [9]	Q.10/17

SG 17과 SG 13에게 클라우드 컴퓨팅 국제 표준 추진을 위한 업무 할당 영역을 식별하고 그 결과를 2013년 6월 정보통신표준자문반(TSAG) 회의에 보고하도록 요청했고, 6월 TSAG 회의에서 두 연구반 간 업무 조종 및 할당을 최종 결정할 것을 합의한 바 있었다.

이에 따라, 2013년 2월에 ITU-T SG 13 회의에서는 이 이슈에 대한 논의를 진행한 바 있으며, 이 회의에서는 역할 할당을 위해 14 가지 태스크를 식별하고 그 중 보안 위협 할당, 보안 요구사항, 보안 기능 할당, 신뢰 관리 등의 4가지 태스크를 두 SG가 공동으로 추진할 공통 프로젝트(common project)로 할당했고, 더불어 이용 사례 등 2가지 태스크는 SG 13 업무로 할당했고, 나머지 대부분의 태스크는 SG 17에 할당했으나, 몇 가지 미해결 이슈가 존재했다.

또한, 2013년 4월 SG 17 회의에서는 5번의 특별 세션 (좌장: 염흥열) 을 개최했고 이에 대한 타협안을 마련하는데 성공했다. 2013년 4월 SG17 회의에서 두 SG 간의 업무 할당을 위한 주요 국가의 입장은 다양했다. 먼저, 러시아는 SG 17이 ITU-T에서 보안 리드 SG이므로 대부분의 태스크를 SG 17에 할당해야 한다고 주장했고, 영국은 SG 13이 클라우드 컴퓨팅을 책임지는 리드 SG이므로 4가지 공통 프로젝트를 SG 13 주도로 할당을 주장했으며, 미국은 특별한 의견을 제시하지 않고 전문가의 토론을 지켜보고 나서 입장을 결정하겠다고 했으며, 중국은 SG 17 내에 Q.8/17 (클라우드 컴퓨팅 보안) 라포처를 맡고 있어 SG 17 주도 국제 표준화를 지지하는 입장이었다. 한국은 SG 13 및 SG 17 국내 연구반 간에 사전 입장 조율에 따라 별도의 의견 개진 없이 중립의 입장을 견지했다.

이번 회의에서 중점적으로 다뤄진 논쟁사항은 두 SG 간에 공통으로 개발할 공통 프로젝트(common project)에 대한 정의에 집중되었고, 공통 프로젝트는 두 SG가 공동으로 개발할 권고로써, 이 공통 프로젝트마다 주도 연구반 (principal study group) 을 할당해, 이 주도 연구반이 신규 권고를 신설하고 권고 채택을 최종적으로

〔표 4〕 SG13과 SG17 간의 클라우드 컴퓨팅 보안 태스크 할당

태스크	할당
클라우드 컴퓨팅 보안 유스케이스	SG13
기능 구조	SG13
보안 위협 식별	SG17 주도 공통 프로젝트
일반 보안 요구사항	SG13 주도 공통 프로젝트
보안 요구사항	SG17 주도 공통 프로젝트
보안 영역 식별	SG17
보안 기능의 기능 구조 할당	SG13 주도 공통 프로젝트
보안 기능 세부 사항	SG17
보안 구조 기본 개념	SG17
신뢰 모델 정의	SG17 주도 공통 프로젝트
기존 보안 메카니즘	SG17
신규 보안 메카니즘	SG17
보안 관리	SG17
보안 모범 사례	SG17
운영 보안	SG17

〔표 5〕 클라우드 컴퓨팅 보안 관련 작업그룹(SC 27)

번호	작업그룹 제목
WG 1/27	정보보호관리체계
WG 4/27	보안 통제 및 서비스
WG 5/27	아이덴티티 관리 및 프라이버시 기술

〔표 6〕 JTC 1/SC 27에서 개발 중인 클라우드 컴퓨팅 보안 관련 국제 표준

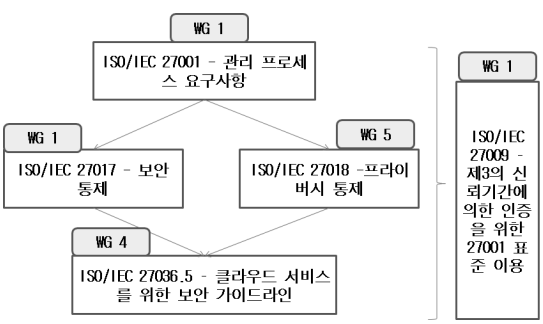
표준화 기구	국제 표준 상태	제목	개발주체
ISO/IEC JTC 1/SC 27	ISO/IEC WD 27017	ISO/IEC 27017 - Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 [13]	SC 27/ WG 1
	ISO/IEC CD 27018	ISO/IEC 27018 - Information security management - Code of practice for data protection controls for public cloud Computing [14]	SC 27/ WG 5
	ISO/IEC WD 27036-4	Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services [15]	SC 27/ WG 4
	ISO/IEC WD 27036-4	Information technology - Security techniques - The use and application of ISO/IEC 27001 for sector/service-specific Third-Party accredited certifications[12]	SC 27/ WG 1

승인하며, 대외적으로 연락 창구로 활동하게 한다는 것에 합의했다. 최종적으로 합의된 두 연구반간의 클라우드 보안 관련 태스크 할당은 [표 4]와 같다[10]. 이와 더불어 현재 Q.8/17와 Q.10/17에서 개발 중에 있는 6개의 기존 권고는 현재 연구과제에서 수행하도록 합의했다. 이번 연구반 17 회의에서 합의된 업무 조정안은 연락문서를 통해 6월 TSAG 회의에 전달되었으며, 최종 결정은 6월 TSAG 회의에서 결정될 것이다.

Ⅲ. ISO/IEC JTC 1 국제 표준화 동향

3.1 JTC 1/SC 27

ISO/IEC JTC 1/SC 27은 정보보안기술에 대한 국제 표준화를 추진하고 있는 공적 표준화 연구그룹이다[3]. 연구그룹 27의 클라우드 컴퓨팅 보안 표준화는 [표 5]와 같이 SC 27산하의 작업그룹 1(WG, working group), 작업그룹 4, 작업 그룹 5에서 추진하고 있다. JTC 1/SC 27 산하 3개의 작업그룹에서 논문작성 시점에 개발하고 있는 국제 표준은 [표 6]과 같이 “클라우드 컴퓨팅 서비스 사업자를 위한 보안 통제 지침” 국제 표준(ISO/IEC WD 27017), “클라우드 사업자를 위한 데이터 보호 통제 지침” 국제 표준(ISO/IEC CD 27018), 그리고 클라우드 서비스 보안 가이드라인(ISO/IEC WD 27036-4) 등이다. 이에 더해 클라우드 컴퓨팅 서비스 제공자에 대해 보안 측면에서 제3의 인증기관에 의해 평가하여 인증서를 부여하기 위한 국제 표준 구성요소는 [그림 1]과 같이 보안 관리 프로세스를 위한 국제 표준(ISO/IEC 27001[11]), 인증을 부여하기 위해 각 표준과의 관계와 세부 요구사항을 표준화할 국제표준(ISO/IEC 27009[12]), 클라우드 서비스 사업자에 특화된 요구사항 등을 다룰 국제표준(ISO/IEC 27036.4), 클라우드 서비스 제공자를 위한 보안 통제 지침 국제표준(ISO/IEC 27017), 클라우드 서비스 제공자를 위한 데이터 보호 통제 지침 국제표준(ISO/IEC 27018) 등으로 구성되어야 한다. 특히 ISO/IEC 27009는 한국이 제안한 개인정보관리체계 국제 표준화 추진을 위한 부산물로 나타난 국제표준으로 이를 이용하면, 클라우드 서비스 제공자를 포함해 개인정보관리체계, 에너지 그리드 사업자를 위한 보안관리체계, 금융부문을 위한 보안관리체계, 통신부문 보안관리체계, 의료부문 보안관리체계에 대한 인증에 ISO/IEC 27001 국제 표준이 어떻게 활용될 수 있는지를 제시하는 국제표준이 될 것으로 기대된다.



〔그림 1〕 클라우드 컴퓨팅 보안 인증을 위한 국제 표준 구성요소

Ⅵ. 결 론

클라우드 컴퓨팅 서비스의 활성화의 저해 요소는 보안 이슈와 프라이버시 이슈이다. 현재 양대 국제 공적 표준화 기구에서는 클라우드 컴퓨팅 보안을 위한 국제 표준화를 진행하고 있다.

본 논문에서는 클라우드 컴퓨팅 보안을 위한 양대 공적 국제 표준화 기구에서 추진 중인 국제 표준화 동향을 제시했다. 본 논문은 향후 클라우드 컴퓨팅 보안 국제 표준 추진을 위한 많은 전문가에게 유익하게 활용될 수 있기를 기대한다.

참고문헌

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

[2] ITU-T SG 13 website, http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx

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

[4] ITU-T X.ccsec, High-level security framework for cloud computing, ITU-T SG17, TD 0251 Rev.2, 2013.4

[5] ITU-T X.fsspvn, Framework for a secure service platform for virtual network, ITU-T SG17

[6] ITU-T X.goscc, Guidelines of operational security for cloud computing, ITU-T SG17, TD 0284 Rev.1, 2013.4

[7] ITU-T X.sfcse, Security functional requirements for Software as a Service (SaaS) application environment, ITU-T SG17, TD 0237 Rev.1, 2013.4
[8] ITU-T X.cc-control/ISO/IEC 27017 – Information security management – Guidelines on information security controls for the use of cloud computing ser vices based on ISO/IEC 27002
[9] ITU-T X.idm-cc, Requirement of IdM in cloud computing, ITU-T SG17, TD 0322 Rev.1, 2013.4
[10] Heung Youl Youm, Report of the special sessions on cloud computing security separation between SG17 and SG13 (18, 19, and 24 April 2013), ITU-T SG17, TD 0144 Rev.3, 2013.4
[11] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements
[12] ISO/IEC NP 27009, The use and application of ISO/IEC 27001 for sector/service-specific Third-Party accredited certifications
[13] ISO/IEC 27017 – Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002
[14] ISO/IEC 27018, ISO/IEC 27018 – Information security management – Code of practice for data protection controls for public cloud Computing
[15] ISO/IEC 27036-4, Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services

〈著者紹介〉

염 흥 열 (HeungYoul YOUM)
종신회원

한양대학교 전자공학과 학사 졸업
한양대학교 대학원 전자공학과 석사 졸업
한양대학교 대학원 전자공학과 박사 졸업
1982년 12월~1990년 9월 : 한국전자통신연구소 선임연구원
1990년 9월~현재 : 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월 : 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 : 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재 : 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사, 논문지편집위원 위원장, 수석부회장(역), 명예회장(현)
2005년~2008년 : ITU-T SG17 Q.9 Rapporteur(역)
2006년 11월~2009년 2월 (구) 정통부 정보보호 PM/, 정보통신연구진흥원 정보보호전문위원
2011년 1월~12월 : 한국정보보호학회 회장(역)
2008년 7월~현재 : 방송통신위원회 자체평가위원회
2008년 7월 ~2013년 2월 : 행정안전부 정책자문위원회
2013년 5월~현재 : 미래창조과학부 자체평가위원회
2009년 5월~현재 : 국정원 암호검증위원회 위원
2009년~현재 : ITU-T SG17 부의장 /SG17 WP3 의장
2012년 6월~현재 : 정보보안산업표준 포럼 의장
<관심분야> 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜

윤 미 연 (Miyeon YOON)
가톨릭대학교 수/컴퓨터학과 학사 졸업
숭실대학교 일반대학원 컴퓨터공학과 석사 졸업
숭실대학교 대학원 컴퓨터공학과 박사 졸업
2005년 6월~2009년 7월 : 한국정보보호진흥원 선임연구원
2009년 7월~현재 : 한국인터넷진흥원 책임연구원
<관심분야> 인터넷 보안, USN 보안, 멀티캐스트/IPTV 보안, 모바일 보안, 스마트그리드 보안, 클라우드 보안