정 보 보 호 학 회 지
제24권 제6호, 2014. 12

# 클라우드 보안 표준화와 향상된 인증 방안*

김 태 경**, 나 재 훈***

요 약

클라우드 컴퓨팅은 인터넷 기술을 활용하여 IT 자원을 서비스로 제공하는 것으로 IT 자원(SW, 스토리지, 서버, 네트워크)을 필요한 만큼 빌려서 사용하고, 서비스 부하에 따라서 실시간 확장성을 지원받으며, 사용한 만큼의 비용을 지불하는 컴퓨팅 특성을 가지고 있다. 이러한 클라우드 컴퓨팅 서비스의 영역이 점차 확대되고 있으며 이를 제공하는 회사 및 사용자들도 증가하는 추세에 있어, 클라우드 서비스와 관련된 보안 및 표준화 활동의 중요성이 더욱 커지고 있다. 본 논문에서는 클라우드 보안 표준과 관련하여 ITU-T SG 17 및 ISO/IEC JTC1/SC27에서 추진 중인 국제 표준화 동향과 클라우드 보안 관련 기구들의 활동 그리고 국내 클라우드 보안 표준화에 대해서 살펴보았다. 또한 속성정보 기반의 인증 프로토콜(X.eaaa: Enhanced entity authentication based on aggregated attributes)에 대해서 정리하였다. X.eaaa는 인터넷 서비스에 강화된 인증을 제공할 수 있을 뿐만 아니라 다양한 클라우드 서비스에도 적용이 가능한 기술로 추후 클라우드 보안 기술에 속성정보 기반의 인증 프로토콜을 적용하는 방안에 대한 연구가 필요하다.

## Ⅰ. 서 론

클라우드 컴퓨팅 서비스는 사용자의 단말을 통해 언제 어디서나 편리하게 사용자의 요구에 따라 다양한 플랫폼, 응용 서비스, 네트워크, 하드웨어 등의 공유 컴퓨팅 자원을 임대해 활용 가능케 하는 정보통신 서비스이다. 국내외의 클라우드 서비스 제공자가 증가하고 있으며, 사용자의 스마트 단말기도 증가하고 있어 앞으로 클라우딩 컴퓨팅의 활용도는 더 높아질 전망이다[1].

클라우드 배치 모델 (deployment model)은 인프라, 플랫폼, 소프트웨어, 그리고 네트워크를 서비스로 제공하는 4 가지 서비스 모델을 갖는다. 그러나 클라우드 컴퓨팅 서비스의 확산에 가장 우려되는 것은 보안 위협과 클라우드 서비스 고객의 정보 통제권 상실 그리고 개인정보 유출 등의 프라이버시 이슈이다. 또한, 제3의 신뢰인증기관이 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[2].

클라우드 컴퓨팅 보안을 위한 국제 표준화 활동은 두 개의 공적 표준화기구인 ITU-T SG 17과 ISO/IEC JTC1/SC 27에서 수행되고 있으며 이외에도 여러 기관에서 클라우드 보안 관련 활동을 수행하고 있다.

본 논문의 구성은 다음과 같다. 제2장에서는 ITU-T SG17과 ISO/IEC JTC1/SC27에서 추진 중인 보안 연구과제, 클라우드 보안 관련 기구들의 활동 및 국내 클라우드 보안 표준화에 대해서 살펴보고, 3장에서 ITU-T SG17에서 신규 아이템으로 선정된 속성기반의 인증 프로토콜에 대해서 기술하였다. 마지막으로 4장에서 향후 추진 사항에 대한 내용으로 결론을 맺는다.

* 본 연구는 미래창조과학부의 지원을 받는 방송통신표준기술력향상사업의 일환으로 수행되었음.
** 서울신학대학교 교양학부 교수(tkkim@stu.ac.kr)
*** 한국전자통신연구원 사이버보안연구본부 전문위원(jhnah@etri.re.kr)

## Ⅱ. 국제 및 국내 클라우드 보안 표준화 활동

### 2.1. ITU-T의 클라우드 보안 표준화 활동

ITU-T SG17은 정보보호에 대한 국제 표준화를 담당하고 있으며, ITU-T SG13은 미래 네트워크에 대한 국제 표준을 맡고 있다[2]. ITU-T SG13 및 SG17에서 클라우드 컴퓨팅 표준과 관련된 조직은 다음의 [표 1]과 같다.

일반적으로 클라우드 컴퓨팅에 대한 보안 영역 식별, 보안 기능 세부 사항, 보안 구조 기본 개념, 기존/신규 보안 메커니즘, 보안 관리, 보안 모범 사례, 운영 보안 등은 SG17에서 담당하고 있으며, 보안 위협 식별, 보안 요구사항, 신뢰 모델 정의 등은 SG17이 주도하고 SG13과 공통으로 수행하는 프로젝트로 진행하기로 하였다.

ITU-T SG17에서 개발 중인 클라우드 컴퓨팅 보안 관련 표준 과제는 다음의 [표 2]와 같으며[3], 현재 대부분의 과제가 Q.8과 Q.3에서 수행되고 있다.

〔표 1〕 SG13, 17 클라우드 보안 연구과제

| Study Group | Question | 연구과제 제목 |
|---|---|---|
| SG13 | Q.17 | 클라우드 컴퓨팅 에코시스템, 일반 요구사항 |
| | Q.18 | 클라우드 기능구조, 인프라, 네트워킹 |
| SG17 | Q.3 | 통신망 정보보호관리체계 |
| | Q.8 | 클라우드 컴퓨팅 보안 |
| | Q.10 | ID 관리 구조 및 메커니즘 |

〔표 2〕 SG13, 17 클라우드 보안 연구과제

| 표준 아이템 | 제목 |
|---|---|
| X.cc-control | Information technology - Security techniques - Code of practice for information security controls for cloud computing services based on ISO/IEC 27002 |
| X.CSCDataSec | Guidelines for cloud service customer data security |
| X.goscc | Guidelines of operational security for cloud computing |
| X.sfcse | Security requirements for Software as a Service (SaaS) application environments |
| X.idmcc | Requirements of IdM in cloud computing |

### 2.2. JTC1 SC27 클라우드 보안 표준화 활동

ISO/IEC JTC1/SC27은 정보보안기술에 대한 국제표준화를 추진하고 있는 표준화 단체이다. SC27의 클라우드 컴퓨팅 보안 표준화는 작업그룹 1(WG, working group), 작업그룹 4, 작업 그룹 5에서 추진하고 있다[2]. ISO/IEC JTC1 SC27에서 개발 중인 클라우드 보안 표준과제는 다음의 [표 3]과 같다.

현재 JTC1 SC27에서 개발 중인 클라우드 보안 연구과제로는 클라우드 컴퓨팅 서비스 사업자를 위한 보안 통제 지침 국제 표준(ISO/IEC DIS 27017)과 클라우드 서비스 보안 가이드라인(ISO/IEC WD 27036-4)이 있다.

〔표 3〕 JTC1 SC27 클라우드 보안 연구과제

| 표준 아이템 | 제목 |
|---|---|
| ISO/IEC DIS 27017[4] | Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services |
| ISO/IEC WD 27036‐4[4] | Information technology ‐ Security techniques ‐ Information security for supplier relationships ‐ Part 4: Guidelines for security of cloud services |

### 2.3. 클라우드 보안 관련 기구 활동

#### 2.3.1. NIST(The National Institute of Standards and Technology)

NIST는 미국 정부 클라우드 컴퓨팅 기술 로드맵 볼륨Ⅰ, Ⅱ를 발간하였다. 로드맵은 연방정부의 클라우드 컴퓨팅 채택을 가속화시키는 전략에 초점을 맞춘 것으로, 세계 각 국에서 보내온 200개 이상의 코멘트를 반영하여 작성하였다[5].

- 볼륨Ⅰ(High-Priority Requirements to Further USG Agency Cloud Computing Adoption): 로드맵의 목적과 범위를 설명하였다. 보안, 상호운용성(시스템끼리 함께 작업할 수 있는 능력), 이식성(한 클라우드에서 다른 클라우드 시스템으로 이동할 수 있는 능력)의 3가지 우선순위에 초점을 맞췄다.
- 볼륨Ⅱ(Useful Information for Cloud Adopters): 개

념적인 모델로써 NIST 클라우드 컴퓨팅 참조 아키텍처 및 분류 그리고 미국 정부 클라우드 타겟 비즈니스 및 기술사용 사례를 소개하였다. 또한 볼륨Ⅱ는 현재 클라우드 모델에 적용되는 표준들을 조사하여, 신규 및 개정 표준이 필요한 우선순위를 다뤘다.

또한 GICTF(Global Inter-Cloud Technology Forum)에서는 보안전담 그룹은 없지만 재난상황 및 비상상황 발생 시 비즈니스 연속성 및 복구에 대해서 연구를 수행하고 있으며, OASIS(Identity in the Cloud TC)에서는 클라우드 환경에서의 아이덴티티(Identity) 기술 규격을 개발하고 있다. 이외에도 ENISA, CSA, DMTF 등에서 클라우드 보안 관련 활동을 수행하고 있다[1].

#### 2.3.2. ENISA(European Network and Information Security Agency) 클라우드 컴퓨팅

정보기술을 위한 이점, 위험 및 권고, 거버넌스 환경에서의 클라우드 보안 문서에 대한 개발을 수행하고 있다.

#### 2.3.3. CSA(Cloud Security Alliance)

클라우드 컴퓨팅 내에 보안 인증을 위한 성공 사례 구현을 목적으로 하고 있으며, 이를 위한 교육 등의 프로그램을 함께 제공하고 있다. 특히 13가지 도메인 내에 클라우드 보안 가이드라인을 제공하고 있다.

#### 2.3.4. DMTF(Distributed Management Task Force)

분산화 관리 환경을 고려한 공통 정보 모델 및 보안 모델을 규정하고 있다. 특히, 공통 정보 모델, 분산된 네트워크 보안, 정책 기반 보안관리를 위한 툴킷, 관리형 클라우드 화이트 페이퍼를 위한 구조, 클라우드 감사 데이터 연계 방법에 대한 연구를 수행하고 있다.

### 2.4. 클라우드 보안 관련 국내 표준

클라우드 보안과 관련하여 제정된 최근(2013년 이후)의 방송통신표준(KCS)은 다음과 같다.

- KCS.KO-10.2001: 클라우드 서비스 제공자의 개인정보 보호 지침
- KCS.KO-10.2000: 클라우드 서비스 제공자의 정보보호 지침
- KCS.KO-10.0619: 모바일 클라우드 기본 기능 및 요구 사항
- KCS.KO-10.0618: 모바일 클라우드 정의 및 단말 요구 사항

## Ⅲ. 속성기반의 강화된 인증 방안

2014년 9월에 개최된 ITU-T SG17 회의에서 속성정보 기반의 인증 프로토콜이 신규 아이템(X.eaaa: Enhanced entity authentication based on aggregated attributes)으로 승인되었다[6].

이 신규 아이템은 2013년 9월에 Q.7(안전한 응용 서비스), Q.10(IdM: 신원정보 관리)에서 1차로 논의되었으며, 2014년 1월에 2차로 논의되었다. 그리고 2014년 9월에 3차로 한국 제안으로 추진되었다. 이 신규 아이템은 여러 ID 제공자로부터 속성 정보들을 취합하고, 취합된 속성 정보들을 통해서 강화된 인증방식을 제공하는 것을 그 내용으로 하고 있다.

속성기반의 강화된 인증 방안의 개념은 다음과 같다. 많은 서비스 제공자들이 현재의 IdM(Identity Management) 관리구조의 IdP(Identity Provider)의 역할을 수행하고, 각각의 IdP는 자신의 서버에 각기 다른 사용자의 속성을 가지게 된다. 예를 들면 신용카드회사에 의해 운영되는 IdP의 경우에는 사용자의 신용카드 정보를 가지고 있게 되며, 대학교에 의해 운영되는 IdP의 경우에는 재학생이나 졸업생들에 대한 정보를 가지고 관련 증명서를 발급하게 된다. 즉, 서비스 이용자에 대한 강화된 인증을 제공하기 위해서는 개인에 대한 여러 속성값들이 필요하며, 서비스 이용자는 여러 IdP에 있는 자신의 속성값들을 결합하여 강화된 인증방식을 제공할 수 있게 된다[7].

향후 이 표준은 인터넷 서비스 영역 이외에 클라우드 서비스에 적용이 가능한 메커니즘으로, 사이버공간에서 이루어지는 다양한 서비스에 필수적인 표준으로 고려할 수 있다.

## Ⅳ. 결 론

클라우드 컴퓨팅 서비스는 사용자의 단말을 통해 언제 어디서나 편리하게 사용자의 요구에 따라 다양한 플랫폼, 응용 서비스, 네트워크, 하드웨어 등의 공유 컴퓨팅 자원을 임대해 활용 가능케 하는 정보통신 서비스이다. 클라우드 서비스를 제공하는 회사들이 증가하고 있으며, 이에 따라 서비스 이용자들도 증가하는 추세에 있어 클라우드 서비스에 대한 보안의 중요성은 더욱 증가하고 있다.

본 논문에서는 클라우드 보안 표준과 관련하여 ITU-T SG 17 및 ISO/IEC JTC1/SC27에서 추진 중인 국제 표준화 동향 그리고 클라우드 보안 관련 기구들의 활동 및 국내 클라우드 보안 표준화에 대해서 살펴보았다. 이외에도 2014년 9월 신규 아이템으로 선정된 속성정보 기반의 인증 프로토콜(X.eaaa: Enhanced entity authentication based on aggregated attributes)에 대해서도 알아보았다.

신규 아이템으로 선정된 X.eaaa는 인터넷 서비스에 강화된 인증을 제공할 수 있을 뿐만 아니라 다양한 클라우드 서비스에도 적용이 가능한 기술로, 클라우드 서비스 인증에 있어 속성정보 기반의 인증 프로토콜을 적용하는 방안에 대한 연구가 필요하다.

## 참 고 문 헌

[1] 오흥룡, 김영화, 진병문, "클라우드 컴퓨팅 보안 국제표준화 연구", 한국통신학회 2013년 하계종합학술발표회.

[2] 염흥열, 윤미연, "클라우드 컴퓨팅 보안 국제표준화 동향", 정보보호학회지 23권 3호 2013년 6월.

[3] http://www.itu.int/ITU-T/workprog/wp_search.aspx?isn_sp=1749&isn_sg=1759

[4] http://www.iso.org/iso/home/search.htm?qt=cloud&published=on&active_tab=standards&sort_by=rel

[5] 해외 ICT 표준화 동향 정보, TTA, 2014년 10월.

[6] 나재훈, "ITU-T SG17 웹 서비스 인증 강화 표준", TTA ICT Standard Weekly, 2014년 11월.

[7] Tae Kyung Kim and Jae Hoon Nah, "Analysis on the Attribute Binding based Enhanced User Authentication", International Journal of Security and Its Applications Vol.7, No.6, 2013.

## 〈저 자 소 개〉

**김 태 경 (KIM TAE KYUNG)**
종신회원

1997년 2월 : 단국대학교 수학교육과 졸업
2001년 8월 : 성균관대학교 정보통신공학과 공학석사
2005년 8월 : 성균관대학교 전기전자및컴퓨터공학과 공학박사
2006년 3월~2008년 2월 : 서일대학 정보전자과 교수
2008년 3월~현재 : 서울신학대학교 교양학부 교수
관심분야 : 네트워크보안, USN, 클라우드컴퓨팅, COP

**나 재 훈 (Jae Hoon Nah)**
종신회원

1985년 2월 : 중앙대학교 컴퓨터공학과 졸업
1987년 2월 : 중앙대학교 컴퓨터공학과 석사
2005년 2월 : 한국외국어대학교 전자정보공학과 박사
1987년~현재 : 한국전자통신연구원 사이버융합보안연구단 전문위원/책임연구원
2009년~현재 : ITU-T SG17 Q7 Rapporteur
2011년~현재 : 한국정보보호학회 학회지 편집위원장
관심분야 : IPv6/MIPv6, P2P, IPTV, 웹메시업 보안