

[정보보호] 클라우드 컴퓨팅 보안, ITU-T에서 본격 추진 진용 마련

국제전기통신연합-정보통신부문 SG 17(ITU-T Study Group 17) 회의가 2013년 4월 17일부터 4월 26일까지 스위스 제네바에서 열렸다. 이번 회의에서 클라우드 컴퓨팅 보안 국제 표준화를 위해 ITU-T SG 17 (보안)과 SG 13 (미래 네트워크) 간의 업무 할당 및 조정에 대한 윤곽이 마련되었다. 본 고에서는 이번 회의에서 다뤄진 주요 이슈에 대한 논쟁사항과 합의 사항을 중심으로 기술한다.

주요 이슈 및 논쟁사항

이번 SG 17 회의에서는 SG 17과 SG 13 간의 클라우드 컴퓨팅 보안 태스크 할당 이슈와 각 연구과제마다 디폴트 승인 과정에 대한 배정이 주요 이슈로 다뤄졌다.

첫 번째 이슈의 경우, 2012년 두바이 세계정보통신표준총회(WTSA-12)에서 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. 본 이슈를 다루기 위해 이번 SG 17 회의에서는 5번의 특별 세션(좌장: 영흥열, 한국)을 개최했고 타협안을 마련하는데 성공했다.

2013년 2월에 SG 13 회의에서도 이 이슈를 다루기 위해 논의가 진행된 바 있으며, 이 회의에서는 역할 할당을 위해 14가지 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.

이번 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 공동으로 개발할 공통 프로젝트(common project)에 대한 정의에 집중되었고, 공통 프로젝트는 두 SG가 공동으로 개발할 권고로서, 이 공통 프로젝트마다 주도 연구반(principal SG)을 할당해, 이 주도 연구반이 신규 권고를 신설하고 권고 채택을 최종적으로 승인하며, 대외적으로 연락 창구로 활동하게 한다는 것에 합의했다. 5번의 세션을 통해 다음과 같은 최종적으로 다음과 같은 태스크 할당에 합의했다.

- SG 13: 활용사례, 기능 블록 (2가지)

- SG 17: 보안 영역 식별, 상세 보안 기능, 보안 구조 기본 개념, 기존 보안 메커니즘, 신규 메커니즘, 보안 관리, 모범사례, 운영보안 (8가지)
- SG 13/SG 17 공통 태스크 (5가지)
 - SG13 주도 공통: 위협분석 및 활용사례 기반 일반적인 보안 요구사항, 클라우드 컴퓨팅 기능 구조 및 기능 블록에 대한 보안기능 할당 (2가지)
 - SG17 주도 공통: 보안위협 식별, 일반적인 보안 요구사항을 고려한 위협분석/활용사례 기반 클라우드 컴퓨팅 보안 솔루션 및 메커니즘에 대한 보안 요구사항, 신뢰모델 정의 (3가지)

이와 더불어 현재 Q.8/17와 Q.10/17에서 개발 중에 있는 6개의 기존 권고는 현재 연구과제에서 수행하도록 합의했다. 이번 SG 17 회의에서 합의된 업무 조정안은 연락문서를 통해 6월 TSAG 회의에 전달될 예정이다.

<표 1> 국제 공식 표준화기구에서 현재 개발 중인 국제 표준 목록

표준화 기구	개발 중인 국제 표준	제목	개발주체
ITU-T SG 17	ITU-T X.ccsec	High-level security framework for cloud computing	Q.8/17
	ITU-T X.fsspv	Framework for a secure service platform for virtual network	Q.8/17
	ITU-T X.goscc	Guidelines of operational security for cloud computing	Q.8/17
	ITU-T X.sfcse	Security functional requirements for Software as a Service (SaaS) application environment	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	Q.8/17
	ITU-T X.idm-cc	Requirement of IdM in cloud computing	Q.10/17
ISO/IEC JTC 1/SC 27	ISO/IEC 27017	ISO/IEC 27017 – Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	SC 27/WG 1
	ISO/IEC 27018	ISO/IEC 27018 – Information security management – Code of practice for data protection controls for public cloud Computing	SC 27/WG 5
	ISO/IEC 27036-4	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services	SC 27/WG 4

두 번째 이슈는 각 연구과제마다 디폴트 승인 절차를 정하는 이슈였다. 한국은 국가 기고서 제출을 통해 12개의 연구과제(Question)마다 디폴트승인절차를 제안한 바 있다. 디폴트승인절차는 각 연구과제가 권고를 개발할 때 별도의 의의가 없으면 적용되는 권고에 대한

승인과정이다. ITU-T에서는 대체승인절차(AAP, alternative approval process)와 전통승인절차(TAP, traditional approval process)의 두 가지 권고승인과정이 존재하며, AAP는 기술적인 권고에 적용되는 승인 과정으로 국제회의 종료 후 4주간 국가별 의견수렴(LC)에서 의견이 없을 경우 자동 채택하는 방식이며, TAP는 규제 또는 정책과 연관되는 권고에 적용되는 승인과정으로 국제회의 종료 후 회람 문서(Circular letter)로 공지하여 각 회원국의 투표에 의해 다음 SG 회의에서 채택 여부를 위임케 하며, 해당 SG 회의에서 권고 채택 여부를 최종 결정하는 방식이다. 한국은 통신서비스 보안의 연구과제 6과 응용 서비스 보안의 연구과제 7의 디폴트 승인 절차로 대체승인절차(AAP, alternative approval process)를 제안한 바 있다. 대부분의 연구과제에 대한 디폴트 승인 과정은 한국 제안대로 반영되었으나, Q.6/17의 디폴트 승인과정은 특별 세션에서 한국의 제안과는 달리 TAP로 결정되어 한국은 SG 17 프리너리(Closing Plenary)에서 다시 이 이슈를 제기하였다. 한국은 현재 Q.6/17의 디폴트 승인과정이 AAP이고, 지금까지 승인과정에서 문제가 없었으며, Q.6/17에서 개발 중인 권고가 기술적인 사항을 대부분 다루고 있으며, 지금까지 대부분의 권고가 AAP로 승인되었었으며, 산업체와 연관되어 산업체가 빠른 승인절차를 요구하고 있다는 주장하면서 AAP가 되어야 한다고 주장했다. 이에 반해 독일 등은 규제적 성격의 권고 가능성이 있다는 이유로 TAP를 주장했다. 이러한 한국의 주장에, 중국 등 5개국이 적극 찬성한 반면, 독일 등 4개국이 반대했다. 약 1시간 넘은 공방이 이어졌고, 최종적으로 연구과제 6의 디폴트 승인과정을 AAP를 유지기로 결정했다.

향후 추진 전망

이번 회의에서 합의된 클라우드 컴퓨팅 보안 태스크 할당 조정 결과는 6월 TSAG 회의에 전달될 예정이며, 2013년 6월 TSAG 회의에서 최종안이 결정될 예정이다. 또한, 이번 SG 17 회의 결과에 따라 향후 SG17에서 클라우드 컴퓨팅 보안 국제표준 개발에 대한 확고한 기반이 될 것으로 예측된다. 국내 클라우드 컴퓨팅 보안 서비스 관련 산업체와 표준 개발 주체는 향후 TSAG 논의 결과를 면밀히 관찰할 필요가 있다.

염흥열 (순천향대 교수, ITU-T SG17 부의장, SG 17 WP 3 의장, hyyoum@sch.ac.kr)