

ITU-T SG17 회의

나재훈 TTA 응용보안 및 평가인증 PG 의장,
ETRI 인프라보호연구팀 팀장



1. 머리말

2010년 12월 8(수)~17(금)일, 스위스 제네바에서 개최된 ITU-T SG17(정보보호) 회의는 ITU 회원국 28개 국가에서 총 142명이 참석했으며, 그 중 한국에서는 31명이(국가대표 25명, ETRI 6명) 참가했다.

이번 회의에서 한국 주도로 개발된 4개의 표준 문건이 (X.1209: Capabilities and their context scenarios for cybersecurity information sharing and exchange - 한국과 일본 공동 개발, X.1205: Supplement 8 : Best practices against botnet threats - 한국과 일본 공동 개발, X.1245: Framework for countering spam in IP-based multimedia applications, X.1275: Guideline on protection for personally identifiable information in RFID applications) 최종 제정되었다. 그리고 한국 주도의 개발된 표준초안 5건이(X.1034, X.iptvse-5, X.usnsec-1, X.usnsec-2, X.sap-3) 승인을 위한 Consent에 들어갔고, 신규로 3건의(Information

Security Management Reference Model for Small and Medium Telecommunication Organizations, X.bhsm : Telebiometric authentication framework using biometric hardware security module, X.sip-cyber : Security Guideline for countering cyber attacks in SIP-based services) 표준초안이 작업 아 이템으로 만들어 졌다.

2. 주요 회의 내용

ITU-T SG17 회의에서는 최근 두 개의 주요 흐름이 있다. 하나는 CyberSecurity이고 또 하나는 IdM(Identity Management) 이다. 이 두 가지가 흐름의 축을 이루고 있으며, 다른 표준활동에 많은 영향을 미치고 있다.

2.1 Cybersecurity

2009년 9월 회의에서, 글로벌 Cybersecurity에 관련하여 중요한 사안들이 있었으며, Cybersecurity

정보 교환(CYBEX: Cybersecurity Information Exchange) 기술 이니셔티브의 채택되었다. 이것은 지난 수년 동안 정부와 산업계에서 지속적으로 개발해 왔던 20여 종의 표준들의 결과로 나타났으며, 이러한 표준들은 취약성을 최소화하기 위해 온라인 시스템을 걸어 잠금, 또 네트워크 장애 사고 발생 시에 사고에 대한 정보분석을 위한 일관된 방법에 대한 논의 지속적으로 이루어져 왔다.

2010년 12월 회의에서는 주요 표준안들이(X.1500: Cybersecurity information exchange techniques, X.1520: Common vulnerabilities and exposures, X.1521: Common vulnerability scoring system) TAP(Traditional Approval Procedure) 승인 절차에 들어갔고, 15개월간의 CYBEX 산업계의 전문가들의 작업이 일단락되었다.

또한 표준 개발 중인 X.1209(Capabilities and their context scenarios for cybersecurity information sharing and exchange)와 X.1205에 대한 추가문서 8도(Supplement 8 to Recommendation: ITU-T X.1205-Supplement on best practices against botnet threats) 이번 회의에서 승인절차에 들어 갔다.

그리고 현재 Q.4에서 11개의 CYBEX 문서가 개발 중에 있으며, 또한 다음과 같은 주제로 개발 중에 있다.

- Botnets: best practices against botnets and a framework for botnet detection and response
- Abnormal traffic detection and control guideline for telecommunication network
- Malware: guideline on preventing malicious code spreading
- Policy Distribution: Mechanism and procedure for distributing policies for network security
- Attacks: framework for countering cyber attacks in SIP-based services
- Traceback: capabilities and mechanisms

- A possible cybersecurity index
- Preventing web-based attacks

2.2 IdM

SG17 내에서의 IdM은 그 영역을 확장하려고 적극적인 활동을 하고 있다. IdM은 인증서, 식별자, 그에 따르는 속성에 대한 생명주기인 생성, 유지, 이용, 폐지에 따르는 관리를 목적으로 한다.

그러나 담당 연구과제인 Q10은 IdM의 ToR을 새로 개발을 하고자 하는 의도를 보이고 있다. 즉 인식자의 생성, 이용, 폐지에 대한 표준개발을 넘어서, 도메인 간의 신뢰정보의 전달 및 판단을 위한 인증 영역의 표준 개발을 하고 있으며, 더 나아가 CYBEX와의 연계를 꾀하고 있어, SG17의 전반적인 역할분담을 깨트리고 있는 상황이다.

현재 개발 중인 표준문서 X.eaa(Information technology-Security techniques-Entity authentication assurance)는 ISO/IEC와 공동으로 개발하고 있으며, 이 표준은 엔티티의 인증보증을 관리하는 프레임워크를 제공함을 목표로 하고 있다. 그 주요 내용으로는 엔티티 인증보증의 네 가지 수준, 네 가지 수준에 대한 기준 및 가이드라인, 다른 인증보증 스킴과의 연계를 위한 가이드, 및 위협을 약화시키기 위한 통제를 위한 가이드를 포함한다.

2.3 IPTV

IPTV 정보보호 관련 표준문건은 6개의 표준초안이 개발 중에 있으며, 이번 회의에서는 X.iptvsec-5(X.1195: Service and content protection(SCP) interoperability scheme) 문서가 승인(Consent) 절차에 들어 갔다. 2011년 차기 회의에는 X.iptvsec-2(Functional requirements and mechanisms for secure transcodable scheme of IPTV), X.iptvsec-3(Key management framework for secure IPTV services), X.iptvsec-4(Algorithm selection

scheme for service and content protection(SCP descrambling)와 같은 3건의 표준초안에 대하여 승인절차에 들어갈 예정에 있다.

IPTV 정보보호 표준초안에 대하여 지난 7월 임시회의에서부터 독일이 관심을 표명하였으며, 이번 회의에서는 X.iptvsec-3 표준초안에 대하여서 관련 기고서를 제안하였다. 기고내용은 X.iptvsec-3 표준초안에 TA(Trusted Authority) 기능을 추가하는 내용을 제안했다. 그러나 X.iptvsec-3는 키관리 메커니즘에 집중하고, 모바일 단말의 이동성 보장을 위한 프레임워크와 그에 따르는 TA 기능 제공에 대하여는 추후 논의를 하는 것으로 회의에서 결론을 내렸다.

2.4 Cybersecurity Index

X.csi(Guidelines for cybersecurity index) 표준초안은 사이버공간에서 정보보호 안전성을 평가하는 지수 개발을 목표로 하며 이번 회의에서는 총 27개의 지표가 제안되어 표준문서에 반영되었다. 즉 기관이나 국가의 사이버공간의 보안지수를 측정하기 위한 지표와 방법을 제시하는 것이며 향후 사이버 공간의 안전성을 평가하는 주요 지수가 될 수 있기 때문에 각국 간의 이해가 집중되는 표준초안이 된다. 본 문건에 대하여는 한국의 염홍열 교수가 에디터로 활동하고 있다.

2.5 JCA SEC

2010년 2월 TSAG에서는 SG17에 JCA-SEC(JCA on Security) 설립에 대한 고려를 요청하여, 한국의 염홍

열 교수가 JCA-SEC의 설립 필요성에 대하여 발표를 하였다. 이 문건에 대하여 ITU-T SG17에서는 지난 4월 제네바 회의에서, 후속 토론이 있었다. JCA-SEC의 설립은 모든 SG간에 정보보호 작업을 조정하고, 작업에 대한 중복투자를 피할 수 있도록 단일 창구를 두고, 작업에 방해가 되는 요소를 해소하기 위한 상호협력력을 목적으로 두고 있다.

그러나 SG17 4월 회의에서는 이에 대한 이해 부족과 몇몇 국가의 반대 입장으로 인하여 설립이 추진되지 못하였으나, 2010년 12월 SG17회의에서 재 거론되어 설립이 가결되었다. 앞으로 이 회의를 통하여 SG17은 정보보호 표준개발에 있어서 조정기구로서의 역할을 수행하고 이를 바탕으로 정보보호 표준 개발에 있어서 생산성과 효율성에 지대한 영향력을 행사할 것으로 사료된다.

3. 맺음말

ITU-T SG17 회의에서 한국, 일본, 중국은 표준 기고서 제안이 왕성한 국가들이다. 수년 동안의 투자와 노력에 의하여 SG17에서의 한중일의 역할은 매우 중요한 위치에 이르렀고, 또한 한중일의 협력도 상당히 좋은 분위기에 올라와 있다. 매년 1회에 걸친 CJK-SWIS 워크숍을 통한 삼국 간의 결속이 ITU-T SG17 회의장에서 협력으로 나타나고 있다. 이러한 분위기를 기반으로 표준에서 최종 목표가 되는 표준특허 개발에 집중을 할 수 있는 여건이 무르익어 가고 있다고 사료된다. **TTA**