정 보 보 호 학 회 지
제27권 제5호, 2017. 10

# ITU-T SG17 Q2 국제표준화 동향

오 흥 룡*, 염 흥 열**

요 약

국제전기통신연합(ITU)은 UN 산하에 신설된 국제기구로써, 산하에 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R) 등 3개의 부문으로 구성되어 있다[1],[2]. ITU-T SG17 (Study Group 17) 은 보안을 선도하고 있는 그룹으로 산하에 총 14개의 연구과제(Question)를 구성하여 국제표준을 개발 및 연구하고 있다.

본 논문에서는 ITU-T SG17 내에 저자가 라포처로 활동하고 있는 연구과제 2 (Q2, 보안구조 및 프레임워크) 국제표준화 동향 및 향후 추진방향에 대해 살펴보고자 한다.

## Ⅰ. 서 론

정보통신기술(ICT)은 과거 단순히 컴퓨터 및 서버 환경을 탈피해서 점점 고도화되고 복잡하게 진화되고 있다. 특히, 네트워크 환경도 빅데이터 및 클라우드 형태의 환경으로 변화하였고, 통신에 참여하는 엔티티들도 사용자-서버, 사용자-사용자, 기기-기기 등 다양화되었고, 통신구조도 중앙집중화 (Centralization) 에서 분산화 (Decentralization) 된 방식으로 변화하였다. 또한 통신의 목적 및 서비스 조건에 따라 적용되는 응용 플랫폼(분산원장기술, SDN/NFV 등), 보안구조 및 응용 프로토콜 등이 다양하게 변화되고 있다.

따라서 다변화되고 있는 ICT 환경에서 새로운 보안 위협 분석과 사용자 및 자산을 보호하는 기술 개발은 매우 중요한 일이다. 또한, 정보보호 국내외 표준 개발을 통해 산업체에서 개발된 보안 제품들 간에 상호운용성 확보 및 최적의 운영환경을 위한 가이드라인을 제공하는 업무는 점점 중요성이 증가되고 있다.

본 논문에서는 ITU-T SG17 Q2(Question 2, 보안구조 및 프레임워크) 그룹 내에서 새로운 환경에 맞추어 보안구조 및 프레임워크 관련 최신 개발 완료된 표준 및 개발 중에 있는 국제표준을 분석하고, 향후 중점적으로 추진하고자하는 방향을 소개하고자 한다.

## Ⅱ. Q2(보안구조 및 프레임워크) 표준화 동향

ITU-T SG17 Q2는 개방형 시스템 환경을 위한 보안 국제표준(X.800 시리즈)을 중점적으로 개발하였다. 이 중에서도 가장 인용이 많이 되고 있는 대표 국제표준은 X.805(종단간 통신 제공 시스템을 위한 보안 구조, 2003.10.)이며, 이를 근거로 각각의 보안서비스 및 메커니즘(인증성, 접근통제, 부인방지, 기밀성, 무결성, 보안감사 등)을 표준들을 개발하였다.

현재 Q2에서는 새로운 네트워크 환경을 위한 보안구조 및 프레임워크 국제표준을 개발하고 있으며, 세부 표준화 아이템으로는 SDN/NFV(Software-Defined Networking/Network Function Virtualization) 보안구조, VoLTE 보안구조, 전자상거래 보안구조, 별정통신사업자 보안구조 등을 다루고 있다. 본 논문에서 최근 2년간에 표준화 활동 동향에 대해 중점적으로 분석하고자 한다[3],[4].

### 2.1. 개별 정보 서비스 보안 가이드라인(X.1033)

본 국제표준(X.1033)은 중국 차이나유니콤에서 제안해서 개발된 표준으로 통신사업자가 사용자에게 제공되는 다양한 정보들을 개별적으로 제공할 때 고려되어야 할 보안 가이드라인을 정의하고 있다. 즉, 개별 정보 서

본 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00069, 공식표준화기구(ITU/APT등) 표준화대응연구)
* 한국정보통신기술협회 표준화본부 (hroh@tta.or.kr)
** 순천향대학교 정보보호학과 (hyyoum@sch.ac.kr)

비스는 크게 통신서비스, 콘텐츠서비스, 정보화서비스로 분리된다. 통신서비스는 전화, 인터넷, 모바일, 디렉토리, 텔레매틱, 메시지, 비디오 등 유무선 및 위성망을 통해서 이용할 수 있는 서비스를 나타낸다. 콘텐츠서비스는 제3의 서비스 제공자(인터넷서비스제공자, 인터넷 콘텐츠제공자)가 사용자의 편의성을 목적으로 제공되는 웹서비스, 어플리케이션 스토어, 모바일 광고, 위치서비스, 소셜서비스 등을 의미한다. 마지막 정보화서비스는 IT기술을 이용하여 향상된 서비스를 지원하는 기술로 전자정부, 전자상거래, 디지털홈, 헬스케어 등 새로운 분야를 지원하는 서비스이다.

본 국제표준은 상기에 언급된 3가지 서비스 관점에서 기밀성, 데이터 무결성, 시스템 무결성, 가용성, 책임성, 복구성 및 관리성을 충족하기 위한 보안 요구사항과 보안 메커니즘을 통신사업자, 사용자 및 정부 규제 관점에서 가이드라인을 정의하고 있다[5].

### 2.2. ITU-T X.805 구현을 위한 기술적 보안 대응책 (X.1039)

ITU-T X.805 국제표준에서 정의하고 있는 상위 수준의 보안기능은 개발도상국이나 중소기업 관점에서 구현하기에 어려움이 존재하고 있다. 따라서 본 국제표준(X.1039)은 한국 미래부가 2014년에 발표한 정보보호 준비도를 근거로 ITU-T X.805를 구현하기 위한 보안 대응책을 정의한 국제표준화 성공 사례이다(에디터: 염흥열 교수, 순천향대).

본 국제표준은 접근통제, 인증성, 부인방지, 데이터 기밀성, 통신 보안성, 데이터 무결성, 가용성, 프라이버시를 만족하기 위한 보안 대응책 및 기술적 구현 지침을 제공하고 있다. 그리고 기관 운영관점에서의 구현 지침과 보안보증 레벨 분류 및 기준, 국제표준 적용 사례를 부록으로 정의하고 있다[6].

### 2.3. SDN/NFV 보안 표준화 동향

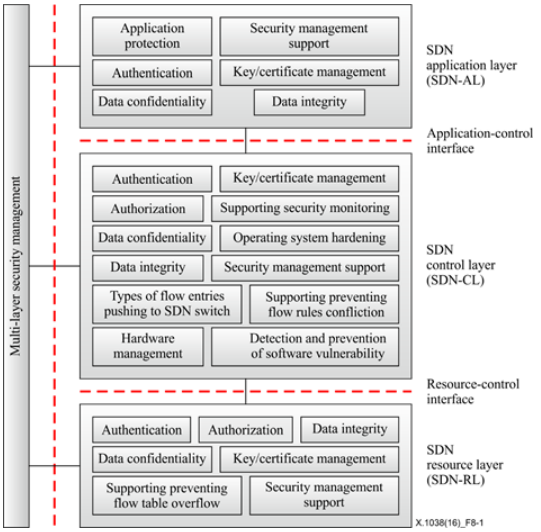
ITU-T SG17에서 SDN(Software-Defined Networking) 보안 표준화 작업은 2014년 1월, 한국 ETRI 제안으로 개발을 시작하였으며, 처음 논의 시작점은 SDN 자체에 대한 보안(Security of SDN)과 SDN을 이용한 보안(Security by SDN)으로 분리해서 표준화 작업을 시작하였다. 따라서 SG17에서는 Q2에서 SDN 자체에 대한 보안을 다루기로 하고 Q6에서 SDN을 이용한 보안을 나누어서 작업하였으나, 현재는 표준 개발 효율성을 위해 Q2에서 SDN 및 NFV(Network Functions Virtualization) 보안을 전담하기로 하였다[7],[8].

#### 2.3.1. SDN을 이용한 보안서비스(X.sdnsec-1)

본 국제표준 초안은 2014년 9월, 한국 제안으로 개발을 시작하였다(에디터: 박정수 책임/ETRI, 김형식 교수/성균관대). SG17에서 처음으로 개발하기 시작한 본 표준초안은 SDN 기반 보안서비스를 이용해서 네트워크 자원을 보호하기 위한 방법을 정의하고 있다. 네트워크 자원은 SDN 어플리케이션, SDN 컨트롤러, SDN 스위치, 보안 매니저로 구성되고, 이를 근거로 중앙집중형 방화벽 서비스, 중앙집중형 허니팟 서비스, 중앙집중형 DDoS 공격 대응서비스, 중앙집중형 불법 단말 관리서비스, 분산형 접근통제 관리서비스를 정의하고 있다. 예로 네트워크 환경에서 다수의 스위치를 통해 DDoS 공격 트래픽이 전달될 경우, 관리자 입장에서는 모든 스위치 장비를 하나나 점검 및 보안 패치를 해야 되는 상황이 발생할 수 있어 물리적 관점에서 대응시간이 늦어질 수 있다. 하지만 SDN 기술을 적용해서 소프트웨어 기반으로 DDoS 어플리케이션 관련 보안 패치를 SDN 컨트롤러를 통해 네트워크 내에 모든 스위치에 일괄적으로 보안 패치를 업그레이드 할 수 있다. 향후 본 국제표준 초안은 SDN을 이용한 보안서비스를 추가적으로 정의할 계획이고, 2018년 하반기에 국제표준 채택을 목표로 개발될 예정이다[9].

#### 2.3.2. SDN 레퍼런스 구조 및 보안 요구사항(X.1038)

본 국제표준은 중국 알카텔-루슨트-상하이, ZTE, 차이나유니콤 사업체에서 연합으로 제안하였으며, SDN 자체에 대한 보안을 다루기 위해 레퍼런스 구조 및 보안 요구사항을 정의하고 있다. 특히, 네트워크 자체에 대한 보안위협 분석과 SDN을 적용했을 때 발생할 수 있는 새로운 보안위협을 분석하였고, 이를 대응하기 위한 보안 요구사항 및 보안 대응책을 정의하였다. 또한, 부속서로 SDN 기술 적용에 따른 새로운 보안 위협에 대한 유즈케이스를 정의하였다.




〔그림 1〕 SDN을 위한 보안 레퍼런스 구조

ITU-T X.1038에서 정의하고 있는 SDN을 위한 보안 레퍼런스 구조는 그림 1과 같으며, 총 4개 계층을 기준으로 보안 요구사항 및 보안 메커니즘을 정의하였다[10].

#### 2.3.3. SDN 기반 서비스 기능 체인의 보안 가이드라인 (X.sdnsec-3)

본 국제표준 초안은 2017년 3월, 중국 차이나모바일, 차이나유니콤, 노키아-상하이가 공동으로 제안하여 표준 개발을 시작하였으며, 아직 초기단계에 있다. 본 표준초안의 주요 목적은 SDN 기반 서비스 기능 체인에 대한 보안위협을 분석하고, 이를 해결하기 위한 보안 가이드라인을 제시하는데 있다. 서비스 기능 체인은 네트워크 관리자가 효율적이고 편리하게 네트워크 정책을 분배하기 위해 사용되고, SDN 기능은 변화되는 요구사항에 따라 트래픽을 자동으로 조정하는 목적으로 사용된다. 따라서 이러한 두 가지 기능이 결합되었을 때, 네트워크 관리 입장에서는 더 효율적이고 더 강력한 기능 제공이 가능할 것으로 예상된다. 현재 표준초안은 초기 단계에 있어 많은 내용이 기술되어 있지 않지만, SDN 기반 서비스 기능 체인에 대한 보안구조를 정의하고, 이에 따른 보안위협 분석 및 보안 요구사항, 보안 대응책을 정의할 계획이다[11].

#### 2.3.4. 보안서비스 체인 구조(X.ssc)

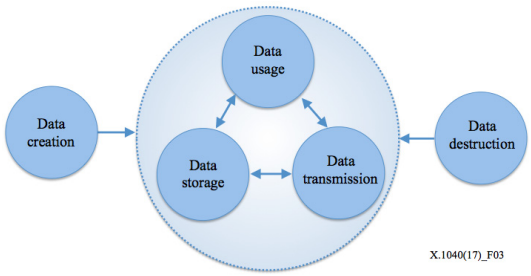
본 국제표준 초안은 2017년 9월, 중국 노키아-상하이, 차이나모바일, 차이나유니콤, MIIT(산업정보기술부)가 공동으로 제안하여 개발을 착수한 신규 표준화 아이템이다. 본 표준초안의 주요목적은 네트워크 및 어플리케이션을 위해 최적화되고 자동화된 보안서비스 제공이 가능한 서비스 체인구조를 정의하는데 있다. 전형적인 보안 어플라이언스(방화벽, 침입탐지시스템 등)는 하드웨어 기반의 미들박스로 구현되어 네트워크에 고정되어 구축된다. 따라서 대용량 네트워크 환경을 구축할 때 관리자 입장에서는 서로 다른 보안 요구사항을 고려한 다수의 하드웨어 기반 장비 설치 및 관리 메커니즘 적용은 매우 어려운 숙제로 남는다. 따라서 본 표준초안은 보안서비스 체인을 생성하는 방법 및 적용 시나리오를 정의할 계획이다[12].

#### 2.3.5. 네트워크 가상화 보안 요구사항(X.srnv)

본 국제표준 초안은 2017년 9월, 중국 차이나유니콤, 차이나모바일, MIIT(산업정보기술부)가 공동으로 제안하여 개발을 착수한 신규 표준화 아이템이다. 본 표준초안의 주요목적은 네트워크 가상화를 위한 보안 위협 및 문제점을 분석하고, 물리적 자원 계층, 가상화 자원 계층 및 LINP(Logically Isolated Network Partitions) 계층에서의 보안 요구사항 정의 및 구현 관점에서의 보안 이슈를 정의할 계획이다[13].

### 2.4. 전자상거래 비즈니스 데이터의 생명주기 관리를 위한 보안 레퍼런스 구조(X.salcm)

본 국제표준 초안은 2016년 3월, 중국 알리바바, 차이나모바일, 차이나유니콤, ZTE가 공동으로 제안하여 개발한 표준초안으로 2017년 9월, SG17 국제회의에서 표준초안 개발이 최종 마무리되어 9월 SG17 회의에서 사전 채택되었다. 향후 ITU 회원국 및 섹터멤버 간에 4주간 의견수렴 과정 후, 2017년 10월경에 ITU-T X.1040 국제표준으로 채택될 예정이다. 본 표준초안의 주요목적은 전자상거래 구조에서 발생할 수 있는 보안 위협 및 주요특징들을 분석하고, 전자상거래 과정에서 발생되는 비즈니스 데이터를 안전하게 관리할 수 있는 보안 레퍼런스 구조를 정의하는데 있다. 비즈니스 데이




〔그림 2〕 데이터 생명주기 관리

터를 안전하게 관리하기 위해 고려되고 있는 보안 기능은 기밀성, 무결성, 가용성, 인증서, 권한부여, 책임성을 적용하였다. 본 표준초안에서 정의한 전자상거래 비즈니스 데이터의 생명주기 관리는 그림 2와 같은 개념으로 정의하였다. 데이터가 생성되어, 일정기간 활용된 후, 데이터가 파기되지만, 필요에 따라 복구할 수 있는 개념으로 정의되었다[14].

### 2.5. VoLTE 네트워크 운영을 위한 보안 프레임워크 (X.voLTEsec-1)

본 국제표준 초안은 2016년 3월, 중국 차이나모바일, CAICT, ZTE가 공동으로 제안하여 개발하고 있는 표준으로 VoLTE 네트워크 운영을 위한 보안 프레임워크를 정의하고 있다. 즉, 네트워크 사업자가 VoLTE 서비스 제공할 때 발생할 수 있는 보안위협을 분석하고, 이를 해결하기 위한 기술적 관리적 대응책을 정의한다. 그리고 보안위협 및 대응책을 고려한 VoLTE 구축 및 운영을 위한 보안 프레임워크를 정의한다. 본 표준초안은 VoLTE 네트워크 보호를 위해 데이터 보안, 어플리케이션 보안, 네트워크 보안, 인프라구조 보안, 보안 정책 측면에서 보안위협 및 보안 요구사항, 보안 대응책 및 보안 레퍼런스 구조 등을 정의할 계획이고, 2018년 하반기에 국제표준 채택을 목표로 개발될 예정이다[15].

### 2.6. 모바일 가상 네트워크 운영자를 위한 보안 가이드라인(부속서, X.sup-sgmvno)

본 부속서(Supplement)는 2014년 9월, 중국 CATR, 차이나텔레콤, 쉐젠대학교에서 공동으로 제안하여 2017년 9월, SG17 국제회의에서 최종 승인된 부속서이다. 본 부속서는 모바일 네트워크 사업자의 망을 임대해서 사용하고 있는 모바일 가상 네트워크 운영자(별정통신사업자) 관점에서 보안 가이드라인을 정의하고 있다. 즉, ITU-T X.805 국제표준에서 정의하고 있는 상위 수준의 보안기능은 별정통신사업자 관점에서 모두 구현하기가 어려워 이를 고려한 부속서를 개발하게 되었다. 본 부속서의 주요내용은 네트워크 침입 탐지, 아이덴티티 및 권한부여 관리, 네트워크 접근통제, DDoS 및 악성코드 대응, 데이터베이스 보안, 웹 어플리케이션 보안, 데이터분실방지, 단말 보안, 보안 감사 및 데이터 복구에 대한 대응책을 정의하고 있다[16].

### 2.7. 양자 정보통신 표준화 동향

한국 KT에서 2017년 9월, SG17 국제회의에 양자암호 기반 안전한 통신기술에 대한 국제표준화가 필요하다는 기고서를 제안하였다. 양자 정보통신은 유럽표준화기구(ETSI QKD, QSC)에서 이미 활동을 하고 있지만, 통신 사업자 관점에서는 양자암호 기반의 보안 솔루션을 제공하기 위한 새로운 보안구조 및 프레임워크에 대한 국제표준이 필요하다고 제안하였다. 본 기고서를 근거로 향후 SG17에서 양자 정보통신을 어떻게 다룰지에 대한 다방면으로 검토가 이루어졌고, Q2 관점에서 본 이슈를 다루는 것으로 논의되었다. 차기 SG17 국제회의에서는 양자 정보통신에 대한 구체화된 표준화 아이템 발굴이 논의될 것으로 판단된다[17],[18].

## Ⅲ. 결 론

본 논문에서는 ITU-T SG17 Q2(보안구조 및 프레임워크)에서 논의되고 있는 국제표준화 활동 현황에 대해 간단히 분석하였다. 현재 Q2는 중국 통신사업자가 다수 국제표준을 개발하고 있으며, 미국, 영국, 캐나다 등이 다양한 관점에서 검토 의견을 개진하고 있다. 향후 Q2는 SDN/NFV 보안, VoLTE 보안, 양자 정보통신 기술을 중점적으로 다룰 것으로 예상된다.

## 참 고 문 헌

[1] ITU-T 홈페이지, http://www.itu.int
[2] 오흥룡, 김영화, 염흥열, “ITU-T SG17 국제표준화 동향 및 향후 전망”, 정보보호학회지, 제23권 제3호, 2013.06.

[3] 염흥열, 오흥룡, “정보보호 기술 및 국제표준화 동향(ITU-T SG17)”, 정보보호학회지, 제24권 제4호, 2014.08.
[4] 오흥룡, 염흥열, “ITU-T SG17(보안) 국제표준화 동향”, 정보보호학회지, 제26권 제4호, 2016.08
[5] ITU-T X.1033(X.gsiiso), “Guidelines on security of the individual information service provided by the operators”, 2016.04.
[6] ITU-T X.1039(X.tigsc), “Technical security measures for implementation of ITU-T X.805 security dimensions”, 2016.10.
[7] ITU-T SG17 C-212, “Security implication on Software-Defined Networking (SDN)”, 2014.01.
[8] ITU-T SG17 C-203, “Basic principles to study new security issues (e.g. security for ITS and SDN)”, 2014.01.
[9] ITU-T SG17 TD768, “Revision of the draft Recommendation X.sdnsec-1: Security services using the software-defined networking”, 2017.09.
[10] ITU-T X.1038(X.sdnsec-2), “Security requirements and reference architecture for software-defined networking”, 2016.10.
[11] ITU-T SG17 TD728, “Revised baseline text for X.sdnsec-3: Security guideline of Service Function Chain based on software defined network”, 2017.09.
[12] ITU-T SG17 TD668, “New work item template for ITU-T X.ssc: Security Service Chain Architecture”, 2017.09.
[13] ITU-T SG17 TD674, “New work item template for ITU-T X.srnv: Security requirements of Network Virtualization”, 2017.09.
[14] ITU-T SG17 TD672, “Draft X.salcm, Security reference architecture for lifecycle management of e-commerce business data (for consent)”, 2017.09.
[15] ITU-T SG17 TD743, “Revised baseline text for X.voltesec-1: Security framework for VoLTE network operation”, 2017.09.
[16] ITU-T SG17 TD667, “Agreement: Revised draft text of X.sup-sgmvno”, 2017.09.
[17] ITU-T SG17 C180/R2, “Proposal of new study on secure communication based on Quantum Cryptography”, 2017.09.
[18] ITU-T SG17 TD502/R3, “Meeting report of Q2/17”, 2017.09

## 〈저자소개〉

**오 흥 룡 (Heung-Ryong Oh)**
종신회원

2002년 2월 : 순천향대학교 전자공학과 졸업
2004년 2월 : 순천향대학교 정보보호학과 석사
2007년 6월 : 순천향대학교 정보보호학과 박사 수료
2004년 2월~현재 : 한국정보통신기술협회 표준화본부 책임연구원
2005년 3월~현재 : ITU-T SG17 국내 연구반 간사(역) 및 위원
2009년~2016년 : ITU-T SG17 Q2 Associate Rapporteur
2017년~현재 : ITU-T SG17 Q2 Co-Rapporteur
관심분야 : 보안프로토콜, 정보보호표준

**염 흥 열 (Heung-Youl 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
2009년~2016년 : ITU-T SG17 부의장, WP3 의장
2017년~현재 : ITU-T SG17 의장
2011년 1월~12월 : 한국정보보호학회 회장(역)
2012년 1월~현재 : 한국정보보호학회 명예회장
2016년 5월~현재 : 개인정보보호표준포럼 의장
관심분야 : 인터넷 보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜