정 보 보 호 학 회 지
제34권 제4호, 2024. 8

# ITU-T SG17(보안) 국제 표준화 회의 주요 결과 및 차기 연구회기(2025-2028) 추진 방향

고 재 남*, 오 흥 룡**, 염 흥 열*

요 약

국제전기통신연합(ITU)은 국제연합(UN) 산하 정보통신기술(ICT)에 대한 국제 표준화기구이다. 193개 회원국, 약 900개 기업 및 학계 멤버 등으로 구성되어 있으며, 산하에 전기통신표준화부문(ITU-T), 전기통신개발부문(ITU-D), 그리고 전파통신 부문(ITU-R) 등 3개의 부문으로 구성되어 있다[1]. ITU-T는 역할과 임무에 따라 11개의 연구반 (SG, Study Group)으로 구성되어 있으며, 각 업무에 맞는 선도 그룹(Lead Study Group)을 지정하여 국제 표준을 개발하고 있다. 정보보안 분야 국제 표준은 ITU-T SG17(보안)에서 담당한다[2]. ITU-T 국제 표준화 조직은 4년 주기의 연구회기(Study Period)로 연구반 구조조정, 의장단 선출 및 표준화 추진 방향을 WTSA(World Telecommunication Standardization Assembly) 총회에서 결정한다. 다음 총회는 올해 2024년 10월에 인도 뉴델리에서 열릴 예정이다.

본 논문에서는 지난 2023년 8/9월과 2024년 2/3월 진행된 ITU-T SG17 회의에서 한국이 주도적으로 수행한 정보보호 표준화 활동 결과를 알아보고, 차기 연구회기(2025-2028) ITU-T SG17 추진 방향에 대해 2024년 7월 진행된 ITU-T SG17 E-Plenary 참석 결과를 중심으로 살펴본다.

## Ⅰ. 서 론

ITU-T SG17(보안, 의장: 순천향대 염흥열 교수)은 ITU-T 내 정보보호 기술에 대한 국제 표준을 개발하는 연구반(Study Gruop)이다. 지난 2023년 8/9월 (2023. 8. 29~9. 8) 대한민국 고양시와 2024년 2/3월 (2024. 2. 20~3. 1) 스위스 제네바에서 개최된 SG17 회의에서는 다수의 국제 표준 최종 승인과 국제 표준 사전 채택, 신규 표준화 과제 승인이 있었다.

특히, 나날이 지능화·조직화 되고 있는 사이버 공격을 막기 위한 호환성 있는 대응 기법에 대한 사이버 보안 분야의 국제 표준 중요성은 매우 강조되고 있다.

본 논문 제2장에서는 2023년 8/9월 회의와 2024년 2/3월 진행된 ITU-T SG17 국제 표준화 활동의 결과를 중점적으로 살펴보고, 제3장에서는 차기 연구회기 (2025-2028)를 위한 ITU-T SG17 추진 방향에 대해 제시한다. 제4장은 본 논문의 결론과 향후 대응 방안을 제시한다.

## Ⅱ. ITU-T SG17 국제 표준화 활동 현황

### 2.1. 현 연구회기(2022-2024) SG17 의장단 명단

[표 1]은 현 연구회기 ITU-T SG17 의장단 명단이다. 이 의장단은 2022년 3월 WTSA-20에서 선출되었다.

〔표 1〕 SG17 의장단(연구회기 2022~2024)

| 이름 | 국가 | 직위 |
|---|---|---|
| 염흥열 | 대한민국 | 의장 |
| Samir Gaber ABDEL-GAWAD | 이집트 | 부의장 |
| Laialy A. ALMANSOURY | 쿠웨이트 | 부의장 |
| Afnan AL-ROMI | 사우디 아라비아 | 부의장 |
| Abdenour BOURENNANE | 알제리 | 부의장 |

본 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임.
[*No.2021-0-00112, 차세대보안 표준전문연구실, **No.2022-0-00009, ICT 국제공식표준화대응 및 국가표준 연구]
* 순천향대학교 정보보호학과/차세대보안 표준전문연구실 (책임연구원, jnko@sch.ac.kr, 교수, hyyoum@sch.ac.kr)
** 한국정보통신기술협회 표준화본부 (수석연구원, hroh@tta.or.kr)

| 이름 | 국가 | 직위 |
|---|---|---|
| Gökhan EVREN | 터키 | 부의장 |
| Yutaka MIYAKE | 일본 | 부의장 |
| Lía MOLINARI | 아르헨티나 | 부의장 |
| Kwadwo Gyamfi OSAFO-MAAFO | 가나 | 부의장 |
| Greg RATTA | 미국 | 부의장 |
| Pushpendra Kumar SINGH | 인도 | 부의장 |
| Arnaud TADDEI | 영국 | 부의장 |
| Wala TURKI LATROUS | 튀니지 | 부의장 |
| Liang WEI | 중국 | 부의장 |

## 2.2. 2023년 8/9월 ITU-T SG17 회의 주요 결과 [3]

본 절에서는 2023년 8/9월 대한민국 고양시에서 개최된 ITU-T SG17 국제 표준 회의에서 논의되었던 주요 결과에 대해 살펴본다.

### 2.2.1. 국제 표준 등 최종 승인 (3건)

[표 2]는 2023년 8/9월 SG17 국제회의에서 최종 승인된 국제표준, 국제표준 부속서, 기술보고서로 한국이 주도적으로 개발해 온 국제표준이다.

〔표 2〕 한국 주도 국제 표준 등 최종 승인

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.1333 Cor.1 | 인터넷 연계 제어시스템의 원격접속도구 사용 보안 지침 오류정정서 | 이건희 (ETRI부설연구소) |
| X.sup39 | 데이터 비식별화 보증 요건 | 강이석(KISA), 김순석(한라대), 염흥열(순천향대), 임형진(금융보안원) |
| TR. sgfdm | 머신러닝에서 동형암호기반 데이터결집을 위한 보안 가이드라인 | 조지훈(삼성SDS), 이동건(서울대), 나재훈(ETRI) |

- **인터넷 연계 제어시스템의 원격접속도구 사용 보안 지침 오류정정서 (ITU-T X.1333 Cor. 1)**

최근 스마트제조 및 신재생에너지 발전원 등의 산업제어시스템에 대한 관리 또는 관제를 위해 원격접속을 사용하는 사례가 늘고 있다. 이에 국내 보안 기준에 적합한 원격접속 보안대책과 해당 보안대책을 안전하게 구현하기 위한 가이드라인을 제시하고자 우리나라 주도로 ITU-T X.1333(인터넷 연계 제어시스템 내 원격 접속 도구 사용 보안 가이드라인, 2022.1월) 표준을 제정했다.

우리나라는 기 제정된 표준 내 일부 영문 오류로 인해 독자가 지침을 잘못 이해할 수 있는 부분이 있어 이를 바로잡고자 오류정정서(Corrigendum) 발간을 제안하여 이번 회의에서 각국의 동의하에 승인되었다[4].

- **데이터 비식별화 보증 요건 (ITU-T X.sup39)**

이 부속서는 데이터 비식별화 보증을 위한 일반 요구사항으로 데이터 자체, 데이터 이용환경, 데이터 이용 및 관리 관점을 제안하여 국제표준 부속서로 최종 승인되었다[5].

- **머신러닝에서 동형암호기반 데이터결집을 위한 보안 가이드라인 (ITU-T TR.sgfdm)**

이 기술보고서는 정보누출의 가능성과 그 원인을 제안하여 기고문에서 그 대책을 제시하였다, privacy 단어 사용의 이슈가 있어 데이터보호(data protection)으로 수정하였고 참고문헌 정보 업데이트 추가를 제안하여 기술보고서로 최종 승인되었다[6].

### 2.2.2. 국제 표준 사전 채택 (6건)

2023년 8/9월 SG17 국제회의에서는 [표 3]과 같이 6건의 국제표준이 사전 채택 되었다.

- **호스트 내 악성코드 공격으로부터 스토리지를 보호하기 위한 보안 프레임워크 (ITU-T X.1220)**

이 표준은 네트워크 보안영역과 엔드포인트 보안영역에서 막을 수 없는 랜섬웨어와 데이터탈취 멀웨어 공격을 예방할 수 있는 스토리지 보안 기술을 정의하

〔표 3〕 한국 주도 국제 표준 사전 채택

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.1220 | 호스트 내 악성코드 공격으로부터 스토리지를 보호하기 위한 보안 프레임워크 | 우종현(듀얼오스), 김봉찬(나무소프트), 신희준(이스톰), 김종현(ETRI), 박수정(TTA) |
| X.1236 | 표적형 이메일 공격 대응책 및 보안 요구사항 | 김충한(기원테크), 김종현(ETRI), 박수정(TTA) |
| X.1150 | 디지털 금융 서비스를 위한 보안 보증 프레임워크 | 염흥열, 박성채, 박준형(순천향대학교) |
| X.1280 | 모바일 기기를 이용한 대역 외 서버 인증을 위한 프레임워크 | 우종현(듀얼오스), 신희준, 정일진(이스톰), 박수정(TTA) |
| X.1095 | 텔레바이오인식 기반 반려동물 개체인증 서비스 | 김재성(KISA), 김태헌(파이리코) |
| X.1373 rev | 지능형통신시스템 소프트웨어 업데이트 보안 능력 개정 | 이상우(ETRI), 박승욱, 조아람(현대자동차) |

여 제안하였다. 또한 스토리지 보안 구조 및 주체별 기능 정의, 스토리지 보안 운영 절차를 제안하여 국제표준으로 사전 채택되었다[7].

• 표적형 이메일 공격 대응책 및 보안 요구사항 (ITU-T X.1236)

이 표준은 표적형 이메일 공격 보안 요구사항 및 대응방안에 대한 표준으로, 표적형 이메일 공격 유형 목차 순서 변경 및 정의 보완, 문법사항 수정 및 불명확한 내용 보완, 공격 유형 별 이를 위한 보안 기능 요구사항 및 대응책 본문 추가를 제안하여 사전채택 되었다[8].

• 디지털 금융 서비스를 위한 보안 보증 프레임워크 (ITU-T X.1150)

이 표준은 FIGI(Financial Inclusion Global Initiative)에서 디지털 금융보안을 위한 안전한 인증 기술 구현에 대한 결과물 산출과 ITU FIGI 담당자의 국제표준화 추진 필요성이 제기됨에 따라 FIGI 결과물을 신규 기술보고서 표준화 과제로 제안하여 사전 채택되었다[9].

• 모바일 기기를 이용한 대역 외 서버 인증을 위한 프레임워크 (ITU-T X.1280)

이 표준은 모바일 단말을 이용한 대역 외 서버 인증 프레임워크로 대역 외 서버 인증 프레임워크의 세부 구성 요소 및 역할을 제안하고, 서버 인증 절차 설명을 제안하여 사전 채택되었다〔10〕.

• 텔레바이오인식 기반 반려동물 개체인증 서비스 (ITU-T X.1095)

이 표준은 반려동물의 비문 및 안면 정의 추가, ROI(Region Of Interest) 정의 추가, 반려동물 플랫폼 활용사례 부록 추가를 제안하여 사전 채택되었다[11].

• 지능형통신시스템 소프트웨어 업데이트 보안 능력 개정 (ITU-T X.1373rev)

이 표준은 기존의 X.1373에서 다루지 않았던 차량 소프트웨어 업데이트를 위한 차내망 통신 메시지를 정의하기 위해 개정 작업을 추진하여 사전 채택되었다[12].

### 2.2.3. 신규 표준화 과제 승인 (9건)

한국은 [표 4]와 같이 정보보호관리체계, 인공지능 보안, ITS 보안 분야 등에 대한 신규 표준화 과제를 제안하여 총 9건의 표준이 채택되었으며, 향후 주도적인 표준 개발을 위해 에디터쉽을 확보하였다.

〔표 4〕 한국 주도 신규 준화 과제 승인

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.1053rev | 중소조직을 위한 정보보호 관리체계 개정 | 김창오(야놀자), 염흥열(순천향대) |
| X.sf-dtea | 표적형 이메일 공격 탐지를 위한 보안 프레임워크 | 신현민, 김충한(기원테크), 김종현(ETRI), 박수정(TTA) |
| X.sup-ekyc-dfs | X.1254 부속서: 디지털 금융 서비스 e-KYC 활용사례 | 염흥열, 박성채, 현다은(순천향대) |
| X.sup-sat-dfs | X.1254 부속서: 디지털 금융 보안에서 안전한 인증 기술의 구현 | 염흥열, 박성채, 박준형(순천향대) |

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.afotak | 분산원장기술을 이용한 일회성 인증키 기반 인증 프레임워크 | 고형승, 전승주, 장현주(FNSValue), 염홍열, 박성채 (순천향대) |
| X.af-sec | 자율주행차량에서의 얼굴 이미지를 이용한 익명화 기술의 평가 방법 | 이유식(순천향대), 이상우, 나재훈 (ETRI) |
| X.fod-sec | 커넥티드카 환경에서의 FoD 서비스 보안을 위한 가이드라인 | 정창훈, 한지용, 박승욱(현대자동차) |
| X.DLT-dgi | 상호운용성을 위한 DLT 게이트웨이 보안 요구사항 | 김영진(드림시큐리티), 박경철(케이포시큐리티), 황정연(성신여대) |
| X.sr-ai | 인공지능 시스템을 위한 보안 요구사항 | 염홍열, 박성채, 고재남, 현다은, 박준형(순천향대) |

• 중소조직을 위한 정보보호 관리체계 개정 (X.1053rev)

이 표준은 2017년 최초 제정 이후, 참조 표준인 X.1051가 2차례에 걸쳐 개정이 되었으며, 2023년 5월에 사전 승인됨에 따라, 정보보호 관리체계에 대한 국제적인 변화의 흐름을 반영하여 중소 조직을 위한 정보보호 관리체계의 개정을 제안해 채택되었다[13].

• 표적형 이메일 공격 탐지를 위한 보안 프레임워크 (X.sf-dtea)

이 표준은 표적형 이메일 공격 탐지를 위한 관련 시스템 정의와 수신 및 발신 표적형 이메일 공격 탐지를 위한 요소 및 기능 규정, 표적형 이메일 공격 탐지를 위한 보안 프레임워크 및 프레임워크의 워크플로우 규정을 제안해 채택되었다[14].

• X.1254 부속서: 디지털 금융 서비스 e-KYC 활용사례 (X.sup-ekyc-dfs)

이 표준은 DFS FIGI(Digital Financial Services Financial Inclusion Global Initiative)에서 연구한 산출물을 기반으로, 신규 기술보고서(TR) 개발을 제안하였고, 디지털 금융 서비스 내 e-KYC 사용 사례 식별, e-KYC 인증 과정 설명을 제안해 채택되었다[15].

• X.1254 부속서: 디지털 금융 보안에서 안전한 인증 기술의 구현 (X.sup-sat-dfs)

이 표준은 FIGI 결과물을 X.1254의 부속서로 신규 워크아이템 제안해 디지털 금융 서비스에서의 안전한 인증에 대한 필요성과 디지털 금융 서비스에서의 안전한 인증 사용 사례를 제안해 채택되었다[16].

• 분산원장기술을 이용한 일회성 인증키 기반 인증 프레임워크 (X.afotak)

이 표준은 분산원장기술 기반 하에 제3의 신뢰할 수 있는 인증서버를 통해 일회성 인증키를 생성하는 패스워드리스 디바이스 인증 프레임워크를 제안하였다[17].

• 자율주행차량에서의 얼굴 이미지를 이용한 익명화 기술의 평가 방법 (X.af-sec)

이 표준은 자율주행 자동차 환경에서 카메라를 이용한 기술을 도입할 때 불특정한 사람들을 촬영하게 되므로 개인정보 보호를 위해 익명화 기술이 필요하며, 이 때 익명화 정도를 평가할 수 있는 기준 및 방법을 제안해 채택되었다[18].

• 커넥티드카 환경에서의 FoD 서비스 보안을 위한 가이드라인 (X.fod-sec)

이 표준은 커넥티드카 환경에서 FoD 서비스의 생태계 정의, 해당 생태계를 기반으로 구독 유스케이스 정의, 해당 생태계와 유스케이스에서 발생 가능한 보안 위협을 분석, 보안 위협에 따른 보안 요구사항 정의를 제안해 채택되었다[19].

• 상호운용성을 위한 DLT 게이트웨이 보안 요구사항 (X.DLT-dgi)

이 표준은 이기종 DLT 시스템 간 상호운용성을 지원하기 위한 DLT 게이트웨이와 관련된 개념 및 보안 위협과 서로 다른 DLT 시스템 간의 안전한 상호운용성을 보장하기 위한 DLT 게이트웨이의 보안 요구 사항을 제안해 채택되었다[20].

• 인공지능 시스템을 위한 보안 요구사항 (X.sr-ai)

이 표준은 인공지능 시스템의 생명주기 및 모델을 제시, 각 생명주기 단계별 위협을 정의하고, 이를 기반으로 보안 요구사항을 제안해 채택되었다[21].

### 2.3. 2024년 2/3월 ITU-T SG17 회의 주요 결과

본 절에서는 2024년 2/3월 SG17 회의에서 논의되었던 주요 결과에 대해 살펴본다. 국제 표준 최종 승인 5건과 국제 표준안 사전채택 4건, 신규 표준화 과제 승인 9건의 주요 결과가 있었다.

#### 2.3.1. 국제 표준 등 최종 승인 (5건)

[표 5]는 2024년 2/3월 SG17 국제회의에서 최종 승인된 국제표준, 국제표준 부속서, 기술보고서로 한국이 주도적으로 개발해 온 국제표준이다.

〔표 5〕 한국 주도 국제 표준 등 최종 승인

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.1150 | 디지털 금융 서비스를 위한 보안 보증 프레임워크 | 염흥열, 박성채, 박준형(순천향대) |
| X.1280 | 모바일 단말을 이용한 대역 외 서버 인증 프레임워크 | 우종현(듀얼오스), 신희준(이스톰), 박수정(TTA) |
| X.1373 rev | 지능형교통시스템 통신 디바이스 소프트웨어 업데이트 보안 기능(개정) | 이상우(ETRI), 박승욱, 조아람 (현대자동차) |
| X.1352 Amd | 사물인터넷(IoT) 기기 및 게이트웨이의 보안 요구사항(개정) | 염흥열(순천향대) |
| X.suppl. uc-dcc | X.1152 부속서: 디지털 코로나19 인증서 사용 사례<br>* X.1152(제 3자 신뢰 기관(TTP)서비스의 종단간 데이터 통신 보안) | 염흥열, 현다은, 박성채(순천향대) |

• 디지털 금융 서비스를 위한 보안 보증 프레임워크 (X.1150)

이 표준은 디지털 금융 보안에서 안전한 인증 기술의 구현을 위해 안전한 사용자 인증에 대한 한국 주도의 국제표준화 추진을 제안해 채택되었다[22].

• 모바일 단말을 이용한 대역 외 서버 인증 프레임워크 (X.1280)

이 표준은 대역 외 물리적 접근 제어 시스템의 개요 및 절차, 시스템 프레임워크의 보안 위협 및 보안 요구사항, 시스템 적용 예시를 제안해 채택되었다[23].

• 지능형통신시스템 통신 디바이스 소프트웨어 업데이트 보안 기능 (X.1373 rev)

이 표준은 기존의 X.1373(지능형통신시스템 소프트웨어 보안 능력)에서 다루지 않았던 차량 소프트웨어 업데이트를 위한 차내망 통신 메시지를 정의하기 위해 개정 작업을 제안해 최종 승인되었다[24].

• 사물인터넷(IoT) 기기 및 게이트웨이의 보안 요구사항 (X.1352 Amd)

이 표준은 블루투스 공격에 대한 용어 정의 추가, 문서 전반에 걸친 수정 텍스트 제안하여 최종 승인되었다[25].

• X.1152 부속서: 디지털 COVID-19 인증서 사용 사례 (X.suppl.uc-dcc)

이 표준은 디지털 COVID-19 인증서 활용사례로 분산신원관리 등 용어 정의 추가, 한국 백신접종증명서 사례 제안 등을 반영하여 최종 채택되었다[26].

#### 2.3.2. 국제 표준 사전 채택 (4건)

2024년 2/3월 SG17 회의에서 사전 채택된 국제표준은 [표 6]과 같다.

• 차량용 에지 컴퓨팅 보안 요구사항 및 가이드라인 (X.1384)

이 표준은 차량 통신 환경에서 에지 컴퓨팅 환경이 고려됨에 따라, 차량 에지 컴퓨팅참조 구조 및 차량 데이터의 보안 위협 및 보안 요구사항 수정안을 제안해 사전 채택되었다[27].

〔표 6〕 국제 표준안 사전 채택

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.1384 | 차량용 에지 컴퓨팅 보안 요구사항 및 가이드라인 | 이상우 (ETRI) |
| X.1771 | 비식별화 처리된 데이터 결합을 위한 보안 가이드라인 | 염흥열, 박성채, 고재남 (순천향대) |
| X.1144rev | 확장 가능한 액세스 제어 마크업 언어(XACML 3.1) | 나재훈(ETRI), Duncan Sparrell (US ICP) |
| X.1455 | 스마트 주거 커뮤니티를 위한 보안 조치 | 나재훈(ETRI), Feng Gao, Junjie Xia (ChinaUnicom), Feng Zhang (ChinaMobile) |

▪ **비식별화 처리된 데이터 결합을 위한 보안 가이드라인 (X.1771)**

이 표준은 신뢰할 수 있는 제3자를 사용하여 비식별 데이터를 결합하기 위한 보안 지침을 제안하여 비식별 데이터, 결합 키등 용어 정의와 보안 통제 등을 제시하였고, 이번 회의에서 사전 채택되었다[28].

• 확장 가능한 액세스 제어 마크업 언어(XACML 3.1) (X.1144rev)

이 표준은 권고 ITU-T X.1144의 개정 표준으로, 2021년 4월 OASIS로부터 XACML 3.0에 대한 수정 버전을 반영하여 X.1144에 대한 개정을 제안해 사전 채택되었다[29].

• 스마트 주거 커뮤니티를 위한 보안 조치 (X.1455)

이 표준은 스마트 시티 거주자들을 위한 인프라, 플랫폼, 응용 및 외부 인터페이스에서 발생 가능한 위협 요인 식별, 정보보호 요구사항 분석을 통하여 정보보호 조치를 제안해 사전 채택되었다[30].

2.3.3. 신규 표준화 과제 승인 (9건)

한국은 2024년 2/3월 SG17 회의에서 [표 7]과 같이 인공지능 보안, ITS 보안, 양자통신 보안 등 신흥 보안 주제와 관련해 9건의 신규 표준화 과제를 제안하였으며 모두 채택되었다.

• 통신 네트워크를 위한 고수준의 제로트러스트 모델 및 보안 기능 (X.ztmc)

이 표준은 국내 실정을 반영한 제로트러스트 모델과 각 영역에 대한 공통 보안 능력 등을 중심으로 하는 신규 워크 아이템을 제안하여 최종 채택되었다[31].

• 첨단항공교통(AAM)의 분류된 데이터를 위한 보안 가이드라인 (X.aamcd-sec)

이 표준은 차세대 교통시스템으로 각광받는 첨단항공교통(Advanced Air Mobility, AAM) 환경에서, 안전한 데이터의 사용을 위하여 중요도에 따라 데이터들을 분류하고, 등급별로 접근 및 관리 방법을 제안하여 채택되었다[32].

• 비컨 기반 상호 인증을 이용한 대역 외 물리적 접근 제어 시스템 프레임워크 (X.oob-pacs)

이 표준은 비컨(beakon) 기반 상호인증으로 사용자와 물리적 접근 제어 시스템 간 이용한 대역 외 물리적 접근 제어 시스템 프레임워크를 제안해 채택되었다[33].

• 악성코드 공격으로부터 네트워크 스토리지 보호를 위한 보안 프레임워크 (X.nspam)

이 표준은 호스트 내 멀웨어 공격으로부터 네트워크 스토리지를 보호하기 위한 보안 프레임워크에 대해 표준화 아이템 개발을 제안해 채택되었다[34].

• 정보분할에 의한 원격생체인증 (X.tis)

이 표준은 생체정보보호를 위한 분할 기법 및 절차와 분할된 생체정보를 이용한 원격 생체인증을 제안해 신규 채택되었다[35].

〔표 7〕 신규 표준화 아이템 승인 및 에디터쉽 확보

| 표준 번호 | 표준 제목 | 에디터(소속) |
|---|---|---|
| X.ztmc | 통신 네트워크를 위한 고수준의 제로트러스트 모델 및 보안 기능 | 염흥열, 박성채, 박준형(순천향대) |
| X.aamcd-sec | 첨단항공교통(AAM)의 분류된 데이터를 위한 보안 가이드라인 | 박승욱, 정창훈(현대자동차), 이유식(순천향대), 이상우(ETRI) |
| X.oob-pacs | 비컨 기반 상호 인증을 이용한 대역 외 물리적 접근 제어 시스템 프레임워크 | 우종현(듀얼오스), 이태일(이스톰), 박수정(TTA), 이영주(서강대) |
| X.nspam | 악성코드 공격으로부터 네트워크 스토리지 보호를 위한 보안 프레임워크 | 우종현(듀얼오스), 김봉찬(나무소프트), 김종현(ETRI), 박수정(TTA) |
| X.tis | 정보분할에 의한 원격생체인증 | 전명근(충북대학교) |
| X.sr-dpts | 허가형 DLT 기반 분산 전력거래 시스템 보안 요구사항 | 이종혁(세종대학교) |
| TR.divs | 검증 가능한 데이터에 기반한 분산 신원 확인 시스템의 이론적 근거와 초기 접근 방식 | 염흥열, 박성채(순천향대) |
| TR.dw-lasf | 디지털 지갑 기술 보고서: 전자지갑의 현황 분석 및 지갑을 위한 보안 기능 | 오경희(티씨에이서비스), 최동빈, 박용범(단국대), 이영주(서강대) |
| X.1400Rev | X.1400(분산원장기술 용어 정의) 개정 | 염흥열, 박성채, 고재남(순천향대) |
| X.1058rev | 개인정보 보호를 위한 실무 준칙 | 염흥열, 박성채(순천향대), 김창오(야놀자) |

• 허가형 DLT 기반 분산 전력거래 시스템 보안 요구사항 (X.sr-dpts)

이 표준은 허가형 DLT 기반 분산 전력거래 시스템에 대한 보안 위협을 식별하고 보안 요구사항 명세를 제안해 신규 채택되었다[36].

• 검증 가능한 데이터에 기반한 분산 신원 확인 시스템의 이론적 근거와 초기 접근 방식 (TR.divs)

이 표준은 우리나라는 모바일 주민등록증, 모바일 운전면허증, 그리고 백신 접종 증명서 등 블록체인기반의 탈중앙 신원확인 서비스를 제공하고 있으며, 범위, 탈중앙 신원확인 방법 구조, 실용적 활용 사례, 편리성 고려사항 등 탈중앙 신원확인 솔루션에 대한 신규 워크 아이템을 제안해 채택되었다[37].

• 전자지갑의 현황 분석 및 지갑을 위한 보안 기능 (TR.dw-lasf)

이 기술보고서 표준은 전자지갑의 현황 분석 및 일반화된 지갑의 보안 기능을 제시하기 위한 기술보고서로 이번 회의에서 신규 아이템으로 채택되었다[38].

• X.1400(분산원장기술 용어 정의) 개정 (X.1400Rev)

이 표준은 2024년에 개정된 ISO 22739 표준의 개정 사항을 반영하고 분산 신원관리에 대한 용어 개정이 필요해 개정안을 제안하였으며, 분산식별자, 분산신원, 신원 등 개정 제안이 이의 없이 반영되어 신규 표준으로 채택되었다[39].

• 개인정보보호를 위한 실무 준칙 (X.1058rev)

이 표준은 개인정보보호와 관련된 위험 및 영향 평가에서 식별된 요구사항을 충족하기 위한 통제 목표, 통제 지침을 제공하고, 개인정보 처리 요구사항을 고려하여 ISO/IEC 27002(사이버보안 및 개인정보보호 - 정보보안 통제)를 기반으로 한 보안 지침을 제공하는 표준으로서 이번 회의에서 2017년도에 발표된 표준을 개정하기로 합의 했다[40].

## Ⅲ. 차기 연구회기 ITU-T SG17 추진 방향

### 3.1. 2024년 7월 SG17 E-Plenary 논의 결과 [41]

본 절에서는 차기 연구회기 ITU-T SG17 추진 방향

〔표 8〕 ITU-T SG17 현재 구조(왼쪽)와 제안된 구조(오른쪽) 비교표

| 현재 번호 | 현재 Question 제목 | 제안 번호 | 제안 Question 제목 |
|---|---|---|---|
| 1/17 | 보안 표준화 전략 및 조정 | 1/17 | 보안 표준화 전략, 인큐베이션 및 조정 |
| 2/17 | 보안 아키텍처 및 네트워크 보안 | 2/17 | 보안 아키텍처 및 네트워크 보안 |
| 3/17 | 정보통신 보안 관리 및 보안 서비스 | 3/17 | 정보통신 보안 관리 및 보안 서비스 |
| 4/17 | 사이버 보안 및 스팸 대응 | 4/17 | 사이버 보안 및 스팸 대응 |
| 6/17 | 통신 서비스 및 사물 인터넷 보안 | 6/17 | 통신 서비스, 사물 인터넷, 디지털 트윈 및 메타버스를 위한 보안 |
| 7/17 | 애플리케이션 서비스 보안 | 7/17 | 애플리케이션 서비스 보안 |
| 8/17 | 클라우드 컴퓨팅 및 빅 데이터 인프라 보안 | 8/17 | 클라우드 컴퓨팅 및 빅데이터 인프라 보안 |
| 10/17 | 신원 관리 및 텔레바이오메트릭스 아키텍처 및 메커니즘 | 10/17 | 신원 관리 및 텔레바이오메트릭스 아키텍처 및 메커니즘 |
| 11/17 | 보안 애플리케이션을 지원하는 일반 기술(예: 디렉터리, PKI, 공식 언어, 객체 식별자) | 11/17 | 보안 애플리케이션을 지원하는 일반 기술 |
| 13/17 | 지능형 교통 시스템(ITS) 보안 | 13/17 | 지능형 교통 시스템(ITS), 자율주행차 보안 |
| 14/17 | 분산 원장 기술(DLT) 보안 | 14/17 | 분산 원장 기술(DLT) 보안 |
| 15/17 | 양자 기반 보안을 포함한 새로운 기술을 위한/에 의한 보안 | 15/17 | 양자 기반 보안 |

으로 2024년 7월 SG17 E-Plenary 회의에서 논의되었던 주요 결과에 대해 살펴본다.

이번 회의에서 2건의 기고 제출되어 2건 모두 최종 반영되었다. 합의 내용을 정리하면 [표 8]과 같으며, 각 연구과제(Questions) 구조의 현재와 제안된 내용을 비교하였다. 이 제안은 9월 회의에서 논의가 된 후에 10월에 열릴 WTSA-24 총회에서 최종 확정 될 예정이다.

- **차기 연구회기를 위한 SG17 일반 연구영역에 대한 논의** (Suggested one item addition to “General areas of study” for the next study period (2025-2028))

SG17은 올해 3월부터 WTSA-24를 준비하기 위한 CG(임시 서면그룹) 를 운영해 왔다. CG는 6월 7일 8번째 원격회의를 통해 WTSA-24 파트 1(SG17 연구범위 및 임무)과 파트 2(각 연구과제의 구조 및 연구 범위)를 합의하였다. 인공지능은 인공지능시스템에 대한 자체적인 보안, 인공지능을 이용한 응용기술 측면에서의 보안 능력 향상이 있다. CG에서 합의한 두가지 측면에서의 인공지능 보안을 general area of study 항목에 추가하는 것을 제안하였으며, 이의 없이 반영되었다.

- **차기 연구회기를 위한 연구과제 구조 및 연구과제 텍스트 최종안 논의** (Proposed update to SG17 Questions for the next study period (2025-2028))

이 기고서는 WTSA-24 준비 CG 활동 결과를 기반으로 연구과제에서 제목변경과 Q6와 Q15의 연구범위에 대한 에디토리얼한 수정 사항을 제안했으며, 각 연구과제별 업데이트된 텍스트가 반영되었다.

## Ⅳ. 결 론

본 논문에서는 2023년 8/9월 대한민국 고양시에서 개최된 IUT-T SG17 회의와 2024년 2/3월 스위스 제네바 ITU-T SG17 회의에서 한국이 주도적으로 개발해 얻은 표준화 결과와 차기 연구회기(2025-2028)의 추진방향에 대해 살펴보았다.

이를 요약하면 2023년 8/9월 SG17 회의에서는 한국이 주도적으로 개발한 국제 표준 5건이 최종 채택되었으며, 6건의 국제 표준이 사전 채택되었고, 신규 표준화 과제로 9건이 승인되었다. 2024년 2/3월 SG17 회의에서는 한국이 주도적으로 개발한 국제 표준 5건이 최종 채택되었으며, 4건의 국제 표준 사전 채택되

었고, 신규 표준화 과제로 9건이 승인되었다.

또한 7월 개최된 ITU-T SG17 E-Plenary 참석 결과로 차기 연구회기(2025~2028)를 위한 SG17 연구반 구조 및 각 연구 과제별 연구범위들이 최종 합의 되었다. 차기 연구 회기에서는 국내 산·학·연 각계 전문가들이 인공지능, 제로트러스트 등 다양한 보안 기술을 국제표준으로 추진 할 수 있도록 발판을 마련하였다.

앞으로도 우리나라는 ITU-T SG17 국제 표준화 활동의 지속적인 주도권을 확보하기 위해서 SG17 연구반 의장을 중심으로 정부, 정보보호 산업체, 학계, 공공기관 전문가의 협업과 미국, 영국 등 주요국과의 협력을 추진할 예정이다. 이런 활동의 결과는 ITU-T 정보보호 국제 표준 활동을 선도할 수 있을 것으로 전망한다.

## 참 고 문 헌


[1] ITU-T 홈페이지, http://www.itu.int

[2] ITU-T SG17 홈페이지, https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/default.aspx

[3] 박수정, 염흥열, ITU-T SG17(정보보호, 2023년 8/9월) 국제회의 결과, TTA ICT Standard Weekly 제1166호, 2023. 10, http://weekly.tta.or.kr/weekly/files/20231026081049_weekly.pdf

[4] X.1333 Cor. 1, Security guidelines for use of remote access tools in Internet-connected control systems, https://www.itu.int/rec/T-REC-X.1333-202309-I!Cor1

[5] X.sup39, Supplement on requirements for data de-identification assurance, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17979

[6] TR.sgfdm, Fully Homomorphic Encryption (FHE) - based data aggregation in machine learning, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17999

[7] X.1220, Security framework for storage protection against malware attacks on hosts, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18345

[8] X.1236, Security requirements and countermeasures for targeted email attacks, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18346

[9] X.1150, Security assurance framework for digital financial services, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18035

[10] X.1280, Framework for out-of-band server authentication using mobile devices, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18036

[11] X.1095, Entity authentication service for pet animals using telebiometrics, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18003

[12] X.1373rev, Secure software update capability for intelligent transportation system communication devices, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17976

[13] X.1053rev, Information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19077

[14] X.sf-dtea, Security framework for detecting targeted email attacks, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19080

[15] X.sup-ekyc-dfs, Supplement to ITU-T X.1254: e-KYC use cases in digital financial services, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19105

[16] X.sup-sat-dfs, Supplement to ITU-T X.1254: Implementation of secure authentication technologies for digital financial services, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19106

[17] X.afotak, Authentication framework based on one-time authentication key using distributed ledger technology, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19104

[18] X.af-sec, Evaluation methodologies for anonymization techniques using face images in autonomous vehicles, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19113

[19] X.fod-sec, Security guidelines for a feature on demand (FoD) service in a connected vehicle environment, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19114

[20] X.DLT-dgi, Security requirements of DLT gateway for interoperabilit, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19111

[21] X.sr-ai, Security requirements for AI systems, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19051

[22] X.1150, Security assurance framework for digital financial services, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18035

[23] X.1280, Framework for out-of-band server authentication using mobile devices, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18036

[24] X.1373rev, Secure software update capability for intelligent transportation system communication devices https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17976

[25] X.1352 Amd, Amendment 1 to ITU-T X.1352: Security Requirements for Internet of things (IoT) devices and gateway, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19045

[26] X.suppl.uc-dcc, ITU-T X.1152 - Supplement on Use cases for digital COVID-19 certificates, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18350

[27] X.1384, Security requirements and guidelines for vehicular edge computing, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=17967

[28] X.1771, Security guidelines for combining de-identified data using trusted third party, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18022

[29] X.1144, eXtensible Access Control Markup Language (XACML) 3.1, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18020

[30] X.1455, Security Measure for Smart Residential Community, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=18001

[31] X.ztmc, Guidelines for Hhigh level Zero trust model and its security capabilities for in telecommunication networks, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19314

[32] X.aamcd-sec, Security guidelines for categorized data in advanced air mobility (AAM), https://www.itu.int/md/T22-SG17-C-0560/en

[33] X.oob-pacs, Framework for out-of-band physical access control systems using beacon-initiated mutual authentication, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19341

[34] X.nspam, Security framework for network storage protection against malware attacks, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19325

[35] X.tis, Telebiometric authentication based on information splitting, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19344

[36] X.sr-dpts, Security requirements for DLT data on permissioned DLT-based distributed power trading systems, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19338

[37] TR.divs, Technical Report: Rationale and initial vision of a decentralized identity verification system (DIVS) based on verifiable data, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19342

[38] TR.dw-lasf, Technical report: A landscape analysis and security features for a digital wallet, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19339

[39] X.1400Rev, Terms and definitions for distributed ledger technology, https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=19335

[40] ITU-T SG17 홈페이지, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=19323

[41] ITU-T SG17 홈페이지, https://www.itu.int/md/T22-SG17-240711-TD/en

## 〈저자소개〉

**고 재 남 (Jae Nam Ko)**

순천향대학교 정보보호학과 학사 졸업

순천향대학교 정보보호학과 석사 졸업

순천향대학교 정보보호학과 박사 과정

<관심분야> 개인정보보호, 네트워크 보안, 정보보안 국제 표준

**오 흥 룡 (Heung-Ryong Oh)**
종신회원

2002년 2월 : 순천향대학교 전자공학과 학사
2004년 2월 : 순천향대학교 정보보호학과 석사
2018년 2월 : 순천향대학교 정보보호학과 박사
2004년 2월~현재 : 한국정보통신기술협회 표준화본부 수석연구원
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
2011년~현재 : 한국정보보호학회 학회지 편집위원
2012년 8월~현재 : 국방부 국방정보기술표준(DITA) 자문위원
2017년 9월~현재 : 금융결제원 바이오인증 성능위원회 자문위원
2019년 4월~현재 : 용인시 지역정보화위원회 자문위원
2022년 9월~현재 : 개인정보보호위원회 개인정보기술포럼 표준화분과 간사 및 위원(1기, 2기)
<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 정보보호학과 정교수
2011년 1월~12월 : 한국정보보호학회 회장(역), 명예회장(현)
2009년~2016년 : ITU-T SG17 부의장
2009년~2016년 : ITU-T SG17 WP3 의장
2017년~현재 : ITU-T SG17 의장
2019년 8월~현재 : 분산신원관리 기술 및 표준화 포럼 의장
2020년 8월 5일~2023년 8월 4일 : 개인정보보호위원회 위원(역)
2022년 9월~현재 : 개인정보보호기술포럼 의장
<관심분야> 정보보호관리체계, 개인정보보호, IoT 보안, 네트워크 보안, 암호 프로토콜, 인공지능 보안과 프라이버시, 블록체인 보안, 5G/6G 보안