

ITU-T SG17(정보보호) 전자 국제회의의 결과

박수정 TTA 표준화본부 책임
 염흥열 ITU-T SG17 국제 의장, 순천향대 정보보호학과 교수

1. 머리말

ITU-T SG17(Study Group 17, 정보보호)은 고도화되는 사이버 위협에 대응하고, 4차 산업혁명 등 디지털 대전환에 따른 신규 융합 인프라에 대한 보안을 강화하기 위해 정보보호 분야의 국제표준을 개발하는 연구반이다. SG17 국제회의는 2021년 8월 24일부터 9월 3일까지 코로나19 확산 방지를 위해 온라인으로 개최되었다. 이번 SG17 국제회의에는 전 세계 28개국에서 223명이 참석하였으며, 한국에서는 염흥열 교수(순천향대, 수석대표) 등 38명의 국가대표단이 참가하였다.

우리나라는 5G 보안, 신원관리 및 인증 보안, 지능형차량통신 보안, 분산원장기술 보안, 양자 암호통신 등 차세대보안기술 표준화를 위해 국가기고서 28건을 제안하여, 총 3건의 국제표준 사전채택, 총 4건의 신규 표준화 아이템 승인 등 괄목할 만한 성과를 거두었다. 본고에서는 한국 주도로 개발하여 사전 채택된 국제표준과 새롭게 개발을 시작한 신규 표준화 아이템을 중점적으로 기술하고자 하며, 이번 SG17 국제회의에서 공유된 ITU/WHO 디지털 백신 접종 증명서 워크숍 관련 주요 논의 결과에 대해 소개하고자 한다.

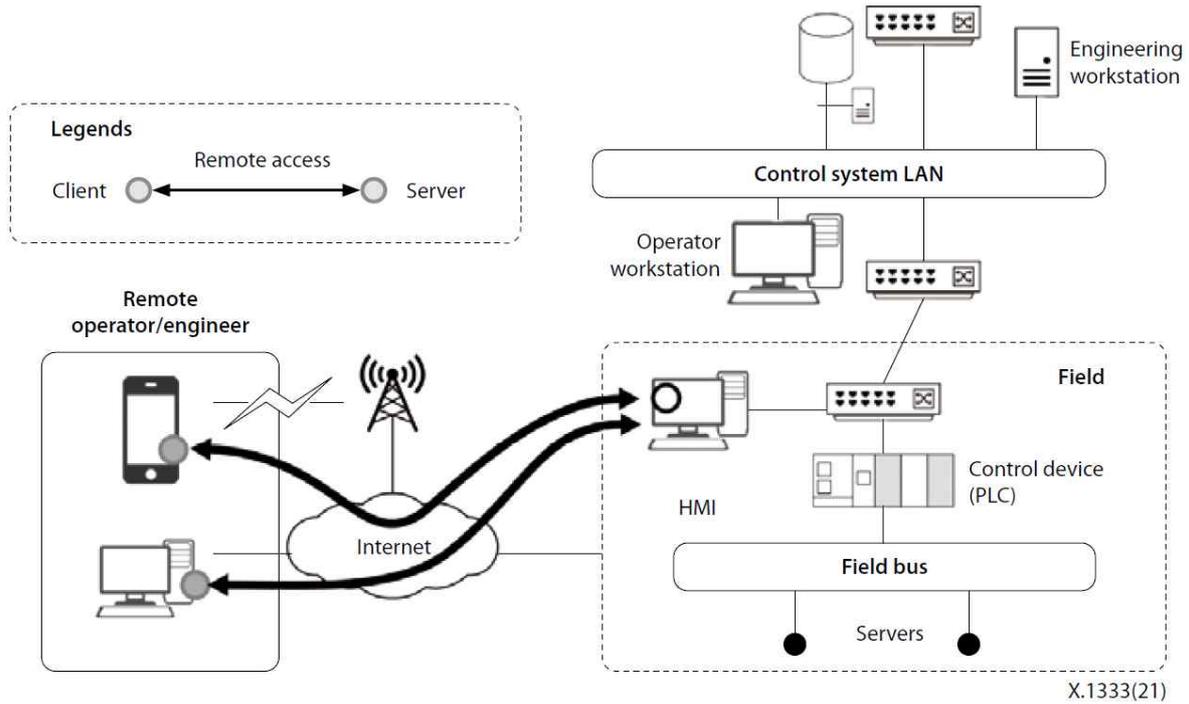
2. 주요 회의 내용

2.1 국제표준 사전채택

이번 SG17 국제회의에서는 산업제어시스템 보안, 사물인터넷 보안, 분산원장기술 보안 등 다양한 융합 서비스 분야에서 한국이 다년간 주도적으로 개발해온 국제표준 3건이 사전 채택되었다.

첫 번째 표준으로 '인터넷 연계 제어시스템 내 원격 접속 도구 사용 보안 가이드라인(X.1333)'은 산업제어시스템에서 시스템 관리 및 유지보수 등을 위해서 원격 접속 도구(RAT, Remote Access Tool)를 이용할 때 고려해야 하는 보안 요구사항을 RAT 서버, RAT 클라이언트, 서버와 클라이언트 간 통신 채널의 관점에서 제시한다. 그리고 이에 대한 보안 대책을 구현하기 위한 가이드라인을 제공하고, 예시로 신재생에너지 운영시스템의 원격제어를 위한 보안 구성을 제시한다. 이 표준은 2019년 8월 한국이 제안하여 신규 표준화 과제로 채택되었으며, 일본 등 각국의 의견을 반영하여 산업제어시스템의 구성은 다양할 수 있으므로, 표준의 대상을 인터넷 연계 제어시스템으로 국한하여 개발되었다. 이 표준은 에너지신산업 정책에 따라 증가하는 신재생 에너지 발전원에 대한 원격관리 보안 지침으로 참고 가능하며, 향후 글로벌 제조사

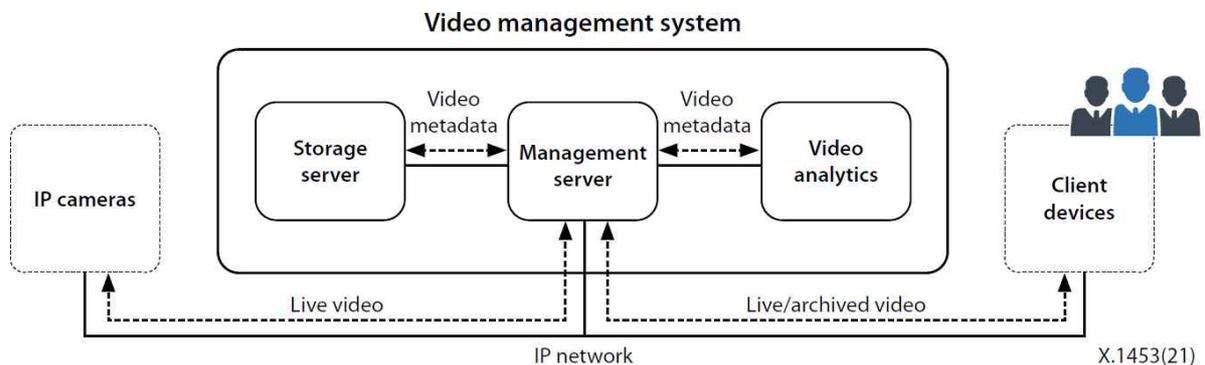
에게 보안 대책 수립을 요구할 수 있는 근거자료로도 활용 가능할 것으로 기대된다.



※출처: ITU-T X.133

[그림 1] 인터넷 연계 제어시스템에서 원격 접속 도구를 사용한 네트워크 구성 예시

두 번째 표준으로 '영상관리시스템을 위한 보안 위협 및 요구사항(X.1453)'은 공공 안전, 교통 모니터링 등에 사용되는 영상 관리 시스템(VMS, Video Management System) 구조를 IP 카메라, 저장 서버, 관리 서버, 영상 분석 서버, 클라이언트 단말의 5가지 구성요소로 분석한다. 그리고 각 구성요소 구간별 보안 위협을 식별하고, 각 구간의 보안 위협에 대응하기 위한 보안 요구사항을 제시한다. 이 표준은 2018년 3월 한국이 제안하여 신규 표준화 과제로 채택되었으며, 영국 등 일부 국가에서 영상감시 서비스에 대한 보안 표준화에 프라이버시 이슈 관련 의견을 제시하여, 영상감시 서비스 대신 영상 관리 시스템에 대한 보안 표준으로 수정하여 개발을 추진하였다.

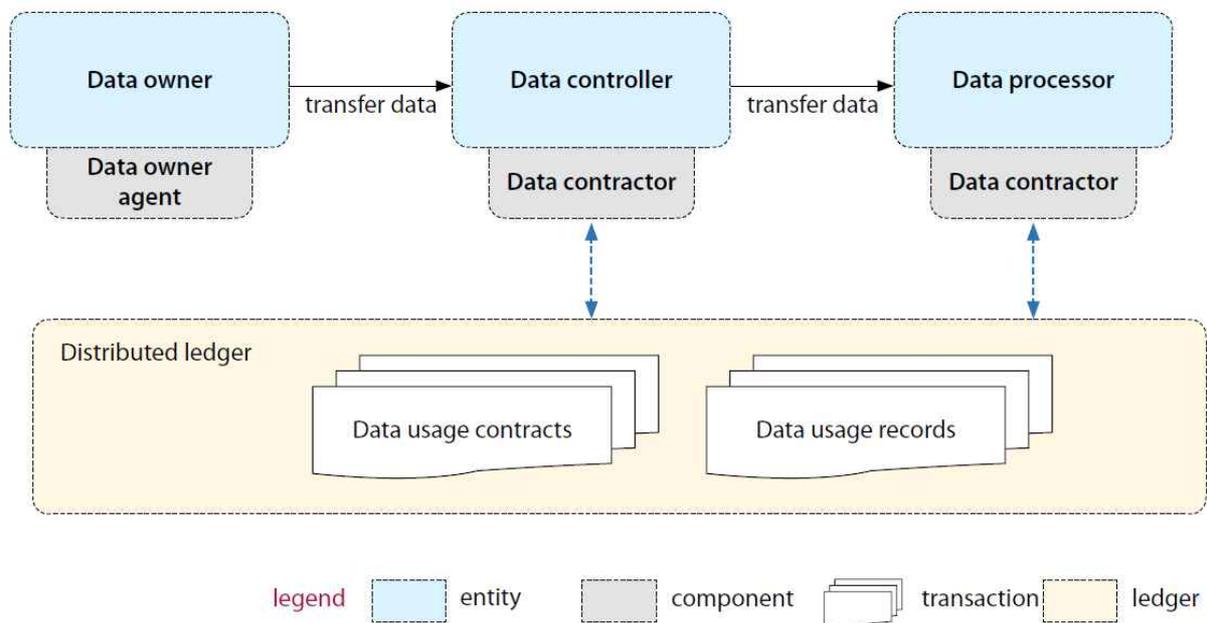


※출처: ITU-T X.1453

[그림 2] 영상 관리 시스템(VMS)의 기능적 구조

IP 기반으로 서비스를 제공하는 영상감시시스템의 특성을 노려 관련 서비스 및 인프라에 대한 다양한 사이버 위협이 증가하고 있는 현 시점에서, 이 표준은 CCTV 및 VMS 등 영상감시 제품의 보안 기능 개발 시 활용이 기대되며, 나아가 국내 산업의 글로벌 경쟁력 확보에 도움이 될 것으로 예상된다.

세 번째 표준인 '분산원장기술 기반 데이터 접근 및 공유를 위한 보안 위협 및 요구사항(X.1408)'은 분산원장기술(DLT, Distributed Ledger Technology)을 기반으로 하는 데이터 접근 및 공유 관리 시스템을 위한 보안 프레임워크, 참조모델을 제시한다. 그리고 DLT 기반의 데이터 접근 및 공유 관리 시스템의 개체를 데이터 소유자(data owner), 데이터 제어자(data controller), 데이터 처리자(data processor) 등으로 식별하고, 각 개체에 대한 보안 위협 및 이를 해결하기 위한 보안 요구사항을 설명한다.



※출처: ITU-T X.1408

[그림 3] DLT 기반 데이터 접근 및 공유를 위한 기본 모델

한국은 데이터의 투명성 및 변경 불가능성을 제공하는 분산원장기술을 이용하여 개인정보 데이터 이용을 추적 및 관리하고자 '18년 3월 SG17 국제회의에 신규 표준 개발을 제안하였으며, 영국 등에서 표준의 범위를 개인정보에 한정하기보다 일반적인 데이터 접근 및 공유 관리 시스템으로 확장 제안하여 수정 개발되었다. 이 표준은 데이터 활용 주체인 산업계 측면에서 분산원장기술 기반 데이터의 추적 및 공유 시스템 구축 및 활용 시에 데이터의 안전한 이동 및 관리를 위해 참고 가능하다. 정보 주체인 개인의 측면에서는 자신의 개인정보에 대한 통제성을 강화할 수 있을 것으로 기대된다.

사전채택된 국제표준은 일반적으로 TAP(Traditional Approval Process) 또는 AAP(Alternative Approval Process)의 승인 절차를 거쳐 채택된다. 표준에 정책 및 규제적 내용이 포함된 경우 TAP 승인 절차를, 일반적인 기술을 다루는 경우 AAP 승인 절차를 거쳐 국제표준으로 채택된

다. TAP로 사전 채택된 2건의 권고안(X.1333, X.1453)은 향후 3개월간의 국가별 의견 수렴과정을 추진하며, 반대하는 국가가 없을 경우, 2022년 1월 개최될 SG 17 특별 전자 총회에서 국제표준 채택 여부를 결정한다. AAP로 사전 채택된 1건의 권고안(X.1408)은 4주간의 의견 수렴 기간(LC, last call)을 거쳐 이견이 없으면 바로 국제표준으로 최종 채택될 예정이다.

<표 1> 한국 주도 국제표준 사전 채택

No.	표준 번호	표준 제목	에디터(소속)	비고(승인절차)
1	X.1333(X.sg-rat)	인터넷 연계 제어시스템 내 원격 접속 도구 사용 보안 가이드라인	이건희 (ETRI부설연구소)	TAP
2	X.1453(X.strvms)	영상관리시스템을 위한 보안 위협 및 요구사항	한종욱(ETRI) 임경수(ETRI) 김건우(ETRI)	TAP
3	X.1408(X.das-mgt)	분산원장기술 기반 데이터 접근 및 공유를 위한 보안 위협 및 요구사항	염홍열(순천향대) 김미연(NSHC) 박근덕(서울외대)	AAP

2.2 신규 표준화 아이템 승인

한국은 응용 서비스 보안, 신원 관리 및 인증분야 등에서 신규 표준화 아이템 4건을 제안하여 <표 2>와 같이 승인되었으며, 향후 주도적 표준 개발을 위해 에디터십을 확보하였다.

<표 2> 신규 표준화 아이템 승인 및 에디터십 확보

No.	표준 번호	표준 제목	에디터(소속)	비고(승인절차)
1	X.saf-dfs	디지털 금융 서비스를 위한 보안 보증 프레임워크	염홍열(순천향대) 김미연(NSHC)	AAP
2	X.oob-sa	모바일 단말을 이용한 대역 외 서버 인증 프레임워크	우종현(듀얼오스) 신희준(이스툼) 정일진(이스툼) 박수정(TTA)	TAP
3	X.srdidm	분산원장기술을 이용한 탈중앙화 신원 관리 시스템을 위한 보안 요구사항	박근덕(서울외대) 여기호(현대오토에버) 진병문(순천향대) 염홍열(순천향대)	AAP
	XSTP-5Gsec-RM	5G 보안 표준화 로드맵 (기술문서)	이건희 (ETRI부설연구소)	Agreement

첫 번째 신규 표준화 아이템은 '디지털 금융 서비스를 위한 보안 보증 프레임워크(X.saf-dfs)'이며, DFS FIGI의 산출물을 기반으로 순천향대와 NSHC가 공동으로 제안하였다. 이 표준은 디지털 금융서비스 비즈니스 모델, 에코시스템 구성요소를 식별하고, 디지털 금융서비스에서 발생 가능한 보안 위협 및 요구사항을 개발할 계획이다. 향후 디지털 금융 서비스 제공업체에서 유용하게 참고 가능할 것으로 기대된다.

두 번째 신규 표준화 아이템은 '모바일 단말을 이용한 대역 외 서버 인증 프레임워크'이며, 국내 중소기업의 상호 인증 보안 기술을 바탕으로 이스툼과 TTA가 제안하였다. 이 표준에서는 이용자가 모바일 단말을 이용하여 서비스 제공자를 확인하고, 이용자와 서비스 제공자 간 상호 인증을 가능하게 하기 위한 대역 외 서버 인증 프레임워크 및 인증 절차를 제시하고자 한

다. 또한 대역 외(Out-of-Band) 서버 인증모델의 보안 위협과 요구사항에 대해서도 개발할 계획이다. 이를 통해, 이용자는 피싱이나 파밍 등 검증되지 않은 서버에 대한 보안 위협에서 벗어나 안전한 인증 서비스를 제공 받을 수 있을 것으로 사료된다.

세 번째 신규 표준화 아이템은 '분산원장기술을 이용한 탈중앙화 신원 관리 시스템을 위한 보안 요구사항'으로, 서울외대, 현대오토에버, 순천향대에서 공동으로 제안하였다. 이 표준에서는 DLT 기반 탈중앙화 신원 관리 모델과 보증 수준 등을 정의하고, 비밀성·무결성·가용성에 근거하여 보안 위협을 식별하고, 이러한 위협을 완화하는 보안 요구사항을 개발할 계획이다. 또한 DLT 기반 탈중앙화 신원 관리 시스템의 활용사례 등을 예시로 제시하고자 한다. 이 표준이 제정되면 모바일 운전면허증, 공무원증과 같은 디지털 신분증, 디지털 백신접종 증명서 등 전 세계 다양한 DID 서비스들의 보안 수준을 높이는데 기여할 것으로 예상된다.

네 번째 신규 표준화 아이템은 '5G 보안 표준화 로드맵 (기술문서)'로 일본이 제안하였고, ETRI부설연구소가 에디터로 참여하게 되었다. 이 기술문서는 여러 표준화 기구에서 개발하고 있는 5G 보안 표준 목록을 정리하고, ITU-T에서 향후 개발할 필요가 있는 5G 보안 표준 분야를 식별하고자 각국의 요청에 따라 개발 시작되었다. 향후 5G 보안 표준화 로드맵에 한국의 기술 개발 방향을 지속적으로 반영함으로써, 국내 5G 보안 기술의 ITU-T 표준화를 위한 초석으로 활용할 수 있을 것으로 기대된다.

2.3 ITU/WHO 디지털 백신 접종 증명서 워크숍 결과 공유

국내에서도 코로나19의 신규 확진자가 연일 갱신되고 있으며, 전 세계적으로도 델타 변이 바이러스 등장 등으로 코로나19 확산세가 수그러들지 않는 추세이다. 그러나 영국 등 세계 각국에서 워드 코로나로 방역 정책을 전환하는 움직임이 있으며, 이에 따라 디지털 백신 접종 증명서에 대한 필요성이 증대되고 있다. 이러한 배경으로 ITU-T 산하 3개 연구반(SG17 정보보호, SG16 멀티미디어, SG20 IoT 및 스마트 시티)이 주도하여 WHO와 공동으로 디지털 백신 접종 증명서 워크숍을 지난 8월 11일에 개최하였다.

디지털 백신 접종 워크숍에서는 한국 질병관리청의 모바일 백신 인증서 앱(COOV)을 포함하여 각국의 디지털 백신 접종 증명서 활용사례 등을 공유하였으며, 다양한 표준화기구 및 백신 접종 관계기관 간 상호 협력 필요성을 공감하고, 향후 표준화 방향에 대한 논의를 진행하였다.

디지털 백신 접종 워크숍의 주요 결과는 크게 3가지이다. 첫 번째로 디지털 백신 접종 인증서 표준화를 위한 ITU-T 산하 포커스그룹(FG) 신설의 필요성을 합의하였다. 이러한 국제적인 합의를 바탕으로 한국은 10월에 개최될 ITU-T TSAG(전기통신표준자문반) 회의에 디지털 COVID-19 인증서 기반 서비스 포커스그룹의 신설을 제안할 예정이다. 두 번째로 디지털 백신 접종 증명서에 대한 2차 워크숍 개최를 추진하기로 하였다. 2차 워크숍은 올해 10~12월 사이에 진행 예정인 ITU Digital World 2021 기간에 연계하여 개최할 계획이다. 마지막으로 WHO에서 발간한 '디지털 COVID-19 증명서:백신 현황' 문서를 ITU에 공유하여 향후 ITU 표준화 추진 필요성에 대해 검토하기로 하였다. 워크숍의 주요 결과는 ITU-T TSAG에도 전달되어 관련 후속 논의를 추진할 것이다.

이번 SG17 국제회의에서는 위와 같은 디지털 백신 접종 워크숍의 주요 내용 및 결과를 참가

국에 공유하였으며, 디지털 COVID-19 인증서 기반 서비스 포커스 그룹 신설 및 디지털 백신 접종 관련 표준화에 대한 각국의 이해를 증진하고 지지를 도모하였다.

3. 맺음말

한국은 이번 SG17 국제회의의 성과로 소개한 분산원장기술 보안, 산업제어시스템 보안, DID 및 인증 보안, 5G 보안 분야 외에도 지능형 차량통신 시스템 보안, 사물인터넷(IoT) 보안, 바이오인식 보안 등 다양한 분야에 대한 지속적인 기고를 통해 왕성한 국제표준화 활동을 추진하고 있다. SG17의 체계적인 국제표준화 활동은 국내 SG17 연구반(반장:순천향대 염홍열 교수)을 중심으로 KT 등 통신회사, 현대자동차, 서울외대, 고려대, 한국전자통신연구원, 한국인터넷진흥원, 금융보안원 등 산학연 중심으로 수행되고 있으며, 이스툼, 맥데이터 등 우수한 기술을 보유한 국내 중소·중견기업이 TTA 표준기술 자문서비스를 통해 SG17 국제표준화를 추진함으로써 글로벌 시장에 진출할 수 있는 계기를 마련하였다. 특히 국내 중소 중견 기업의 SG17 표준화 작업 참여는 우리 기업의 고유 보안 기술을 국제표준으로 연결해 국내 보안 산업과 서비스 경쟁력 향상에 크게 기여할 것으로 기대된다. 향후에도 국내 SG17 연구반은 산학연 전문가들의 유기적 협력을 바탕으로 한국의 우수한 정보보호 기술을 국제표준에 반영하기 위해 적극적인 국제표준화 활동을 추진할 계획이다.

차기 SG17 국제회의는 2022년 1월 7일 특별전자 총회로써 온라인으로 개최될 예정이다. 해당 회의에서는 사전 채택된 국제표준인 인터넷 연계 제어시스템 내 원격 접속 도구 사용 보안가이드라인(X.1333), 영상관리시스템을 위한 보안 위협 및 요구사항(X.1453) 등에 대한 국제 표준 채택 여부를 최종 결정할 예정이다. 또한 WTSA20에 제출할 SG17 임무, 연구과제의 최종안을 확정할 예정이다. 이후 2022년 5-6월에 SG17 총회를 개최할 계획이며, 코로나19의 확산현황에 따라 온라인 혹은 대면으로 개최될 예정이다.

※ 본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2017-0-00069, 공식표준화기구(ITU/APT 등) 표준화 대응 연구)

[주요 용어 풀이]

- DFS FIGI(Digital Financial Services Financial Inclusion Global Initiative): ITU 지원으로 금융 서비스를 위한 디지털 ID, 전자 결제 승인, 보안 등에 대해 연구하는 그룹
- 대역 외(Out-of-Band) 인증기술 : 온라인 서비스 제공자 서버와 이용자가 별도의 통신 채널을 통해 인증정보를 제공하는 기술 (예. SMS, 푸시 알림, QR 코드 등)
- FG(Focus Group) : 특정 이슈에 대해 ITU-T 연구반의 활동을 돕고 외부 전문가 등의 참여를 장려하여 해당 기술 및 표준 사전연구 등을 위해 설립(한시적 운영, 약 9~12개월)
- TSAG(Telecommunication Standardization Advisory Group) : 전기통신표준자문반

※ 출처: TTA 저널 제197호

(코로나 이슈로 각 표준화기구의 표준화회의가 연기·취소됨에 따라 TTA 저널로 대체합니다)