# [정보보호] SG 17 블록체인(DLT) 보안 신규 연구과제 수립

ITU-T는 블록체인이 분산장부기술(distributed ledger technology, DLT)의 일부라고 보고 DLT라는 용어를 사용하기로 결정하였다. 2017년 8월 ITU-T SG 17에서는 DLT 보안 측면에 관한 신규 연구과제(Question)가 수립되었다. 본고에서는 이번 회의에서 통과된 DLT 보안에 관한 신규 표준화 아이템과 연구과제 수립의 과정을 소개한다.

## 1. 신규 연구과제 수립 제안 및 논의의 진행

ITU-T SG 17(정보보호)은 2017년 3월 세미나의 후속작업으로 FG-DLT(Focus group on application of DLT)를 TSAG에 제안한 후, 8월 회의에서는 DLT의 보안 측면을 다루는 신규 연구과제(Q14, Security aspects for DLT)를 수립하고 7개의 신규 표준화 아이템을 개시하였다.

신규 연구과제 수립에 대해서는 3월 회의부터 제안되었으나 캐나다, 미국, 영국 등에서 논의 자체를 반대하는 등의 어려움이 있었다. 이번 회의에서는 신규 연구과제 수립 제안 외에도 한국, 미국, 중국 및 러시아에서 총 11개의 DLT 보안 관련 신규 표준화 아이템이 제안되면서 DLT 보안이 중요한 현안으로 떠올랐다.

신규 연구과제 검토를 위한 특별 세션에서는 DLT 관련 표준화 아이템을 처리하는 방법으로 기존의 한 연구과제에서 논의하는 방안, 기존 연구과제 중 관련 연구과제의 공동 회의를 통해 논의하는 방안, 그리고 새로운 연구과제를 수립하여 논의하는 방안이 제시되었다. 소규모 대표단을 가진 유럽 및 아메리카 대륙 국가들을 중심으로 신규 연구과제 수립에는 반대하지만 공동회의 대신 한 연구과제에서 집중하여 처리하기를 원하는 그룹과 한국 및 중국을 중심으로 신규 연구과제를 수립하기를 원하는 그룹으로 찬반이 분명하게 나뉘었다.

이에 대한 타협안으로 DLT 관련 신규 표준화 아이템(NWIP)을 한 곳에서 전담하여 검토하고 그 결과에 기초하여 신규 연구과제 수립을 논의하는 방안이 제시되었다. 전담 검토 그룹의 리더로 한국의 TCA서비스 오경희 대표가 지명되었고 이어진 전담반 회의를 통해 11개 제안을 검토하여, 한국에서 제안한 3개 표준화 아이템을 포함, 7개의 신규 표준화 아이템을 추진하기로 결정되었다.

## 2. 블록체인 보안 신규 표준화 항목

통과된 7개의 신규 표준화 아이템 목록 및 각각의 범위는 다음과 같다.

가. X.stadlt 'DLT 보안 아키텍처'는 DLT 보안 기능을 위한 아키텍처 프레임워크를 정의한다. 이를 통해 DLT 응용 및 서비스 제공자가 DLT 응용 및 서비스 구현에 있어 필요한 보안 기능을 체계적으로 통합시킴으로써 보안 위험을 감소시키기 위한 것이다. 본 과제는 러시아와 중국의 알리바바 그룹이 각각 제안하였으며 양국의 제안자들이 협의하여 하나로 재구성하여 통과되었다.

나. X.sct-dlt 'DLT 보안 능력 및 위협'은 DLT가 원천적으로 제공하는 보안 능력과 도입 모델 및 서비스에 따라 달라질 수 있는 한계와 보안 위협을 서술한다. 이를 통해 DLT를 개발, 운영 및 사용하는 데 있어서 필요한 보안 분석을 제공함으로써 DLT 기반 플랫폼 및 서비스 시스템의 보안 평가를 지원한다. (차이나 모바일 제안, 에디터)

다. X.sadlt 'DLT 보안 보증'은 데이터 무결성, 기밀성, 통신 보안 및 크리덴셜 관리의 측면에서 DLT를 위한 보안 보증 수준에 대한 지침과 보안 보증 프레임워크를 위한 모델을 제공한다. (한국의 순천향대학교 제안, 에디터)

라. X.dltsec 'DLT 데이터를 이용한 ID 관리에서의 개인정보보호 및 보안 고려사항'은 DLT 기반으로 신원 속성 및 신원 정보를 교환하는 연합형 모델에서의 신뢰를 제공하기 위하여, 신원관리에서 DLT 데이터를 사용함에 따라 발생하는 프라이버시 및 보안 고려사항을 서술한다. (미국의 Aenta 제안, 에디터)

마. X.strdlt 'DLT 기반의 전자지불 서비스에 대한 보안 위협 및 요구사항'은 디지털 금융 서비스 중에서도 특히 지불 시스템을 중심으로 DLT 활용 사례와 서비스 모델을 서술하고 이에 대한 보안 위협 및 챌린지를 분석하여 이에 대응하기 위한 보안 요구사항을 정의한다. (한국의 TCA서비스 제안, 에디터)

바. X.stov 'DLT를 이용한 온라인 투표의 보안 위협'은 DLT 기반의 온라인 투표 시스템 활용 사례를 분석하여 공통 모델을 서술하고 이에 기반하여 온라인 투표 시스템에 대한 보안 위협을 분석한다. (한국의 KSEL 제안, 에디터)

사. X.ss-dlt 'DLT 기반 보안 서비스'는 DLT에 기반한 보안 서비스에 대한 활용사례를 제공한다. PKI 기반의 인증서를 DLT를 이용하여 공유하는 시스템이 하나의 예가 될 수 있다. (차이나 모바일 제안, 에디터)

ID 관리에 대해서는 미국의 Aetna가 3개의 신규 표준화 항목을 제안하였으나, 용어(terminology)와 활용 사례(Use cases)의 경우 보안 특성을 다루는 SG 17보다는 DLT 전반에 관한 사항을 다루는 FG-DLT에서 다루는 것이 더 적절하다는 합의에 따라 FG-DLT로 이관하기로 결정하였다.

이 외 한국의 서강대학교에서 'DLT 기반의 IoT 장비/자원 검색 프레임워크'에 대한 기술보고서(Technical report)를 제안하여 통과되었으나, 에디터의 지속 참여가 어려워 진행하지 않기로

하였다. 서강대학교의 지속적 참여를 기대한다.

**3. 신규 Qustion 14(DLT 보안측면)의 수립과 향후의 일정**

이러한 7개의 표준화 아이템을 기존의 연구과제에서 소화하기에는 어려움이 있으며, 대부분의 국가는 DLT 보안에 관한 표준화 아이템들을 여러 연구과제에 분산하여 논의하는 것을 선호하지 않음에 따라 신규 연구과제를 수립하게 되었다.

다만, 지난 회의에 수립된 ITS 보안 연구과제에 이어 연속으로 신규 연구과제를 수립하게 되었기 때문에 새로운 현안이 발생할 때마다 지속적으로 연구과제를 수립할 수는 없다는 주장이 강하게 제기되었다. 이에 따라 SG 17의 전반적인 구조 조정이 신규 연구과제 수립의 조건으로 제시되었고 이를 위한 통신 그룹이 만들어졌다. SG 17의 구조 조정안이 합의될 때까지 Q14는 어떤 WP에도 속하지 않고 SG 17에 직접 보고하게 되었다.

한편, 일부 국가는 자신이 관할하고 있는 연구과제에서 DLT 보안 관련 표준화 아이템을 처리하고자 하였으나 여의치 않게 되자 신규 연구과제의 라포처십을 강력히 요구하였다. 많은 논의를 거쳐 Q14(DLT 보안)는 한국의 오경희 대표와 일본의 유키 카도바야시(NAIST 교수)가 공동으로 라포처를 맡게 되었으며, 부라포처 2인이 중국에서 추가로 임명되었다. Q14는 1차 라포처 회의를 11월 말 한국에서, 2차 라포처 회의를 2018년 1월 중국에서 개최할 예정이다.

DLT 보안 관련 표준을 실제 환경에 유용하게 개발하기 위하여 SG 17은 DLT 응용 전반을 다루는 FG-DLT 등 관련 FG, ITU-T 내 관련 SG 뿐만 아니라 TC 307과의 연락체계(liaison relationship)를 통하여 긴밀하게 협력할 예정이다. 이를 위하여 한국의 오경희 대표를 TC 307과 FG-DLT에 대한 연락담당관(liaison officer)으로 임명하였다.

블록체인(DLT)은 기술적 발전에 힘입어 2017년 들어 본격적으로 표준화가 진행되고 있는 분야이다. 본 신규 연구과제 수립으로 국내 기술을 반영한 블록체인 보안 연구 및 표준화가 더욱 활발하고 광범위하게 진행될 것을 기대한다.

오경희(TCA서비스 대표, khoh@tcaservices.kr)