해외 표준화기구 동향

TTA 표준화본부 표준기획단

1. 국제 및 국가별 표준화기구

1.1 ISO, 정보 보안 거버넌스 관련 표준 개정[1]

시스템과 도구, 인력 문제로 데이터 침해와 해킹에 맞서 회사의 정보를 보호하는 일은 매우 복잡하다. ISO는 이에 따라 국제적으로 합의된 정보 보안 거버넌스의 표준을 12월 16일 개정했다.

ISO/IEC 27014, 정보 보안, 사이버 보안 및 프라이버시 보호, 즉 정보 보안 거버넌스는 조직이 ISO/IEC 27001을 기반으로 정보 보안 관리 시스템(ISMS)을 평가·지시·모니터링·전달할 수 있도록 개념, 목표 및 프로세스에 대한 지침을 제공한다.

이번 ISO/IEC 27014 개정판은 ISMS의 범위와 전체 조직에서 정보 보안 거버넌스에 대한 핵심 정보를 제공한다. 또한 구조를 명확히 표현하도록 개선했으며 기타 신규 정보를 포함했다. 특히 ISO/IEC 27001, 정보 기술 - 보안 기술 - 정보 보안 관리 시스템 요구사항과 연계돼 조직의 광범위한 거버넌스 정보를 포함한다.

ISO/IEC 27014는 현재 개발됐거나 개발 중인 정보 보안에 대한 몇 가지 다른 표준과 함께 사용될 예정이며, 해당 목록은 아래와 같다.

- ISO/IEC 27002, 정보 기술 - 보안 기술 - 정보 보안 제어에 대한 실천 강령
- ISO/IEC TS 27110, 정보 기술, 사이버 보안 및 개인 정보 보호 - 사이버 보안 프레임워크 개발 지침
- ISO/IEC TS 27100, 정보 기술 - 사이버 보안 - 개요 및 개념
- ISO/IEC 27005, 정보 기술 - 보안 기술 - 정보 보안 위험 관리

1.2 ITU, 자율 네트워크 신규 공개 연구 그룹 출범[2]

디지털 보건 및 지능형 교통 시스템 분야에서 고도화된 상호작용 통신을 경험하도록 진보함에 따라 네트워크의 복잡성도 증가하고 있다. 이에 따라 IMT-2020/5G와 미래 네트워크는 매우

TTA는 해외 표준화기구의 최신 동향을 조사해 주간·월간으로 '해외 ICT 표준화 동향 정보'를 제공합니다. 본고는 2020년 12월 1주부터 2021년 1월 1주까지 게재한 주요 정보를 정리했습니다.

다양한 ICT 애플리케이션의 요구사항을 충족할 수 있을 것이다. IMT-2020/5G와 미래 네트워크의 다재다능성은 클라우드 컴퓨팅 및 네트워크 가상화를 발전하게 하지만 동시에 네트워크 복잡성도 크게 증가시킨다.

인공지능(AI)과 기계학습은 이런 복잡성을 관리하는 데 중요한 역할을 할 것이다. 특히 관련 요구사항은 미리 정의된 자동화 프로세스뿐만 아니라 인간의 능력을 초과하기 때문에 네트워크 관리 및 제어에 대한 새로운 요구를 충족시킬 것으로 예상된다. 최신 네트워크 아키텍처가 복잡해 자율 네트워크가 필요해졌다. 동시에 복잡한 아키텍처 때문에 5G와 미래 네트워크에 '창조적 인텔리전스' 기법을 통합하는 데 필요한 요구사항이 생겨났다.

자율 네트워크는 스스로를 감시·운영·복구·치유·보호·최적화·재구성하는 능력인 '자체'속성을 표시할 것이다. 이런 네트워크는 자율적으로 적응하며 관리와 제어까지 개선할 수 있다. 그뿐만 아니라 제어기와 제어기 계층을 더 적합하게 구성하도록 온라인 실험을 통해 자체 진화할 수도 있을 것이다.

ITU는 12월 23일 효율적이고 자율적으로 행동을 제어할 수 있는 ICT 네트워크의 개발을 지원하고자 신규 포커스 그룹을 출범했다. 해당 그룹은 공개 그룹으로 관련된 모든 이해 당사자가 참가할 수 있다.

자율 네트워크 ITU 포커스 그룹은 ITU 표준이 어떻게 자율 네트워크를 실현하고 향후 자율 네트워크가 진보할 때 어떻게 지원할 것인지 결정하는 탐색적 '사전 표준화(prestandardization)' 연구를 주도할 것이다. 또한 온라인 실험실을 활용해 창조적 인텔리전스 기법을 연구함으로써 '탐색적 진화', '비상적 행동', '실시간 대응 실험'과 같은 기초 개념을 상세히 설명할 예정이다. 다음으로 자율 네트워크의 의미와 특성을 연구하고 자율 네트워크의 창의성을 뒷받침하는 개념을 명확히 하고자 용어를 정의할 것이다.

미래 ICT 환경 및 이용 사례에 대한 네트워크의 동적 적응을 지원하기 위해서는 자율 네트워크가 진보하는 데 필요한 기술적 활성화 장치를 제안할 예정이다. 특히 실시간 응답 실험을 통해 더 높은 수준의 자율성을 가능하게 하는 아키텍처 개념을 입증하고 관련 지침을 개발할 계획을 발표했다. 본 포커스 그룹은 표준화 및 오픈소스 커뮤니티가 협력하는 개방형 플랫폼과 현장에서 활동 중인 모든 산업 참가자와 학계의 협력을 통해 자율적 네트워크를 향한 혁신에 기여할 것이다.

1.3 DIN, 'AI, Made in Germany' 인공지능 표준화 로드맵 발표[3]

독일 표준화기구(DIN), 독일 전기규격위원회(DKE) 및 독일연방경제에너지부(BMWi)는 지난해 11월 30일 독일연방정부의 디지털 서밋에서 AI 표준화 로드맵을 대중에 발표했다. 200페이지가 넘는 로드맵은 인공지능을 모든 측면에서 표준화하기 위한 행동 권고사항을 제시한다. AI 표준화 로드맵을 통해 독일 연방정부는 AI 전략에 대한 필수적 조치를 시행할 예정이다. 독일 연방경제부 장관은 규범과 표준이 AI 시스템에 대한 원활한 협력과 신뢰를 보장하기 위한 'AI-Made in Germany'의 발판을 마련했다고 강조했다.

해당 로드맵은 2019년 10월부터 기업·과학·공공부문·시민사회 전문가 300여 명이 개발에 참여해 1년여에 걸친 작업한 결과이다. 본 로드맵의 목적은 독일 산업의 국제 경쟁력을 뒷받침하

고, 유럽적 가치를 국제 수준으로 끌어올릴 표준화를 위한 기반 작업을 조기에 개발하는 것이다. 독일 AI 표준화 로드맵에는 기본 주제, 윤리/책임 AI, 품질, 적합성 평가 및 인증, AI 시스템의 IT 보안(및 안전), 산업자동화, 모빌리티 및 물류, 의학 분야 AI를 비롯해 7가지 주요 주제에 대한 현황과 요구사항, 과제에 대한 종합적 개요를 제공한다.

로드맵에는 70개 이상의 확인된 표준화 요구사항이 포함돼 있다. 이와 더불어 AI 시스템 상호운용성을 위한 데이터 참조 모델 구현, 수평 AI 기본 보안 표준 구축, AI 시스템의 실질적인 초기 중요도 검사 설계, 유럽 품질 인프라 강화를 위한 국가 이행 프로그램 「신뢰할 수 있는 AI」의 개시 및 시행, 표준화 요구에 대한 사용 사례 분석 및 평가라는 5가지 핵심 조치 권고안을 설명한다.

1.4 ETSI, 에지 앱 개발자용 MEC 샌드박스 발표[4]

ETSI는 지난 1월 6일 ETSI MEC(Multi-access Edge Computing) 샌드박스를 출시했다. 해당 샌드박스는 애플리케이션 개발자가 ETSI MEC API 구현을 경험하고 상호작용하며 애플리케이션을 테스트할 수 있도록 설계됐다. 또한 사용자가 ETSI MEC 서비스 API를 배우고 실험할 수 있는 인터랙티브 환경을 제공한다. 이런 표준화된 RESTful API는 MEC 애플리케이션 개발자에게 네트워크 및 컨텍스트 정보(고정 또는 모바일)에 실시간으로 접근할 수 있게 한다. 이와 더불어 인프라 및 사용자 장비에 대한 위치 정보를 포함해 MEC가 제공하는 부가가치 서비스를 제공한다. API를 개발하기 위한 설계 원칙은 http 메소드, 템플릿, 규약 및 패턴과 함께 ETSI GS MEC 009에도 명시돼 있다. MEC 서비스 API는 OpenAPI-compliant descriptions을 통해 제공되는 https://forge.etsi.org에서 YAML 및 JSON 형식으로 제공된다.

ETSI MEC 구축 및 ECO 시스템 개발(DECODE) 워킹그룹(WG) 의장은 "샌드박스를 사용하면 기존 애플리케이션을 사용하는 개발자가 자체 테스트 환경에서 실행되는 라이브 MEC API에 액세스하고 사용하도록 구성할 수 있다. 본 API는 이런 애플리케이션에 필수이며 MEC 샌드박스는 표준을 채택할 수 있는 새로운 기술을 개척함으로써 시장을 가속화하고 개발자가 시장에 진출할 수 있도록 지원할 것"이라고 강조했다.

MEC 샌드박스는 사용자에게 다양한 네트워크 기술(4G, 5G, Wi-Fi)과 차량, 보행자, 연결된 물체 등 단말 장비를 결합한 시나리오를 제공한다. 이러한 시뮬레이션된 자산을 지리 위치 환경에서 결합하여 사용자는 위치(MEC013), 무선 네트워크 정보(MEC012) 및 WLAN 정보(MEC028) 서비스 API 등의 동작과 기능에 대한 실제 경험을 얻을 수 있다. 또한 이런 정보는 에지 기반 MEC 애플리케이션에 뛰어난 차등 성능을 제공할 수 있을 것이다.

MEC Wiki에서 개발자들은 ETSI ISG DECODE WG의 작업과 관련된 정보를 주로 제공하는 에코시스템 페이지를 탐색할 수 있도록 지원될 예정이다. 이 섹션에는 제3자가 이용할 수 있는 MEC 애플리케이션 및 솔루션 목록을 포함하며, 다른 부분은 API 적합성 테스트 스위트와 MEC 개념 증명 활동을 통한 MEC 테스트로 구성된다.

2. 사실표준화 기구 동향

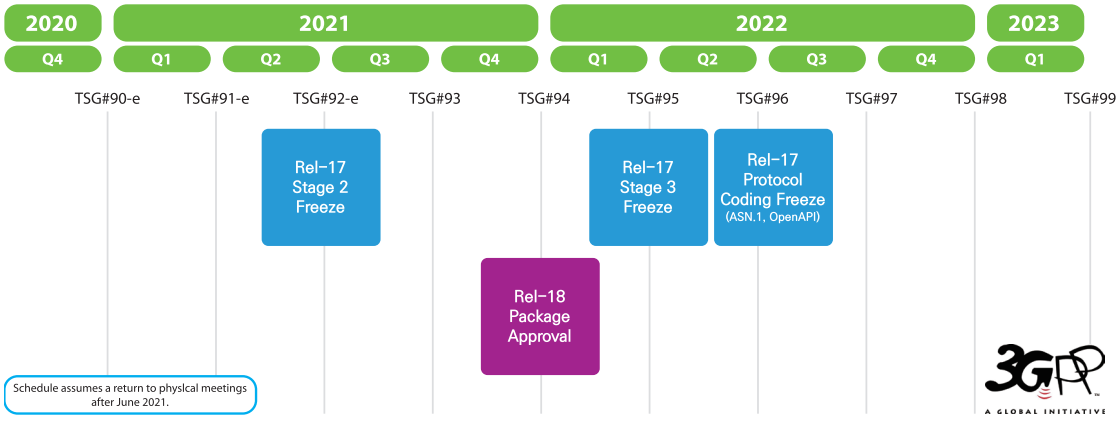
2.1 3GPP, 릴리스 17 향후 일정 공동 승인 및 공개[5]

3GPP TSG(기술규격그룹)는 지난해 12월 둘째 주 본회의에서 릴리스 17의 향후 일정에 대해 공동 승인했다. TSGs#90-e는 2020년 계획한 대면 회의가 취소되고 원격 회의로 대체된 결과를 감안해 해당 일정을 발표했다. 2021년 6월까지 원격 작업이 확정됨에 따라, 워킹그룹 의장 및 3명의 TSG 의장의 지침으로 원격 회의와 토론에 참여하는 이해관계자들이 작업 결과를 정확하게 통합하는 시간이 더 필요하다는 의견이 고려됐다. 본 회의에서 TSG RAN, TSG SA 및 TSG CT 의장은 2021년 하반기에 3GPP 대면 회의가 재개된다는 가정하에 릴리스 17 작업을 완료하기 위한 새로운 일정을 공동 제안했고 다음과 같이 발표했다.

릴리스 17의 작업 일정만 변경됐으며 내용은 2019년 12월 TSG#86 회의에서 승인된 내용으로 유지된다. 이번에 발표된 일정으로 기업의 네트워크 롤아웃과 신제품 개발에 계획을 진전하는 데 크게 기여할 것이다. 또한 일정이 조정됨에 따라 3GPP는 릴리스 16 규격을 유지보수하는 데 시간을 투자할 예정이며 동시에 릴리스 17 기능의 우선순위를 결정할 계획이다.

이와 더불어 다양한 핵심 분야의 연구가 이미 진행 중이다. 여기에는 커버리지 및 포지셔닝 향상, NR 및 슬라이싱 QoE 작업, 신규 주파수 범위 추가, 축소된 NR 기능 장치, 향상된 비공개 네트워크 지원, 무인 항공 시스템 지원, 5GC 에지 컴퓨팅 지원, 5GS 근접 기반 서비스, 5G의 네트워크 자동화(2단계) 및 트래픽 스티어링 접근, 전환 및 분할(ATSSS)이 포함된다.

릴리스 17은 NR을 통한 산업용 IoT에 대한 새로운 작업과 향상된 기능을 포함할 것이다. 여기에는 NR을 통한 산업용 IoT, 비지상파 네트워크를 통한 NR 지원, MIMO, 통합 액세스 및 백홀(IAB), MBS 포지셔닝, NR 멀티캐스트 및 방송 서비스, RAN 슬라이싱 NR, NR 사이드링크, 다중 RAT 듀얼 연결, LTE/NR 다중 SIM 장치 지원, 비활성 상태의 NR 소량 데이터 전송 및 멀



- 2021년 6월, TSGs#92-e, Rel-17 2단계 Functional Freeze
- 2022년 3월, TSGs#95, Rel-17 3단계 Protocol Freeze
- 2022년 6월, TSGs#96, Rel-17 Protocol coding Freeze(ASN.1, OpenAPI)

[그림 1] 릴리스 17 작업 완료 일정

티미디어 우선순위 서비스 등이 포함된다. 2021년 3월 예정된 TSG#91 원격 회의에서는 논의를 통해 2021년 하반기에 물리적 미팅을 재개할 수 있을지 평가할 계획이다. 대면 회의는 빠르면 2021년 6월 TSG 원격 회의 이후가 될 예정이다.

2.2 OASIS, 사이버 위협 정보 표현 STIX 버전 2.1 검토 [6]

OASIS Cyber Threat Intelligence(CTI) TC는 STIX(Structured Threat Information eXpression, 구조화된 사이버 위협 정보 표현) 버전 2.1 위원회 규격 초안을 1월 4일 발표하여 검토 의견을 공개적으로 구했다.

STIX는 사이버 위협 인텔리전스를 교환하는 데 사용하는 언어 및 직렬화 형식이다. 이를 통해 조직과 도구는 협업 위협 분석, 자동화된 위협 교환, 자동화된 탐지 및 대응 같은 다양한 기능을 개선하는 방식으로 위협 인텔리전스를 이해관계자 간 공유할 수 있다. STIX 2.1은 지난 버전 2.0 구현 경험을 기반으로 새로운 객체와 개념을 추가했으며 향상된 기능을 통합해 제공한다. 통합된 추가 객체 및 기능은 CTI를 공유하기 위한 기본 소비자 및 생산자 요건을 충족하는 반복적인 접근방식을 제시한다. STIX 버전 2.1에 포함되지 않은, 향후 커뮤니티에서 필요하다고 간주하는 개체 및 속성은 차기 릴리스에 포함될 예정이다.

참고문헌

[1] https://www.iso.org/news/ref2604.html

[2] https://www.itu.int/en/mediacentre/Pages/pr31-2020-open-research-group-autonomous-networks.aspx

[3] https://www.din.de/de/din-und-seine-partner/presse/mitteilungen/-ki-made-in-germany-etablieren-772680

[4] https://www.etsi.org/newsroom/press-releases/1864-2020-12-etsi-releases-middlebox-security-protocols-framework-specification

[5] https://www.3gpp.org/news-events/2145-rel-17_newtimeline

[6] https://www.oasis-open.org/2021/01/04/invitation-to-comment-on-stix-v2-1/

주요 용어 풀이

- **RESTful API**: RESTful API는 REST원리를 준수해 만들어진 API를 말한다. REST(Representational State Transfer)는 월드 와이드 웹과 같은 분산 하이퍼미디어 시스템을 위한 소프트웨어 아키텍처의 한 형식이다. 이 용어는 로이 필딩(Roy Fielding)의 2000년 박사학위 논문에서 소개됐다. 그는 하이퍼텍스트 전송 프로토콜(HTTP)의 주요 저자들 가운데 한 사람이다.
- **NR**(New Radio, 엔알): 5세대(5G) 이동 통신에서 단말과 기지국 사이의 무선 접속(Radio Access 또는 무선 인터페이스) 기술. 이동 통신 국제 표준화 단체 3GPP에서 만든 공식 명칭이다. 2016년 12월 비엔나에서 개최된 3GPP 제74차 기술 총회(TSG: Technical Specification Group)는 5G 무선 접속 기술의 이름으로 엔알(NR, New Radio)을 채택했다.
- **STIX**(Structured Threat Information eXpression, 구조화된 사이버 위협 정보 표현): 사이버 위협 정보를 구조화하는 표현 규격. 조직별로 수집하여 보유한 비표준 형태의 사이버 위협 정보(CTI, Cyber Threat Intelligence)를 누구나 분석, 해석해 활용할 수 있도록 체계화된 구조로 표준화한 것으로, 사이버 보안 위협 시 신속하고 효율적으로 대응할 수 있도록 한다. 주로 정보공유분석센터(ISAC)와 침해사고대응팀(CERT)과 같은 사이버 테러나 정보 침해 등에 공동으로 대응하는 정보보호 기관에서 사용한다.
  STIX는 소스 코드가 공개되며 누구나 자유롭게 사용할 수 있다.