해외 표준화기구 동향

TTA 표준화본부 표준기획단

1. 지역 및 국가별 표준화기구 동향

1.1 유럽

1.1.1 ETSI NFV ISG, 5G에서의 ETSI NFV 역할 강조[1]

2019년 7월 1일, ETSI ISG(Industry Specificaton Group, 산업 규격 그룹) NFV(Network Functions Virtualization, 네트워크 기능 가상화)는 5G 시스템에서 실행될 다양한 응용 프로그램을 처리하는 데 있어 NFV의 역할을 강조하였다.

* 2012년 초부터 ETSI는 ISG NFV를 통해 NFV의 표준 작업에 상당한 진전을 이루었으며, 5G 구축을 위한 과정이 진행됨에 따라 NFV 시스템의 네트워크 관리 측면에서 3GPP SA5 워킹그룹과의 협력은 매우 중요해지고 있다.

5G NFV Release 3는 5G와 밀접한 관련이 있다. 또한, ETSI ISG NFV는 5G 네트워크를 지원하기 위한 새로운 기능을 설계하고 시스템을 강화시켰다.

'NFV에서의 네트워크 슬라이싱 지원(GS NFV-IFA 024)', '다중 관리 도메인에 대한 관리(GS NFV-IFA 030)' 및 '다중 사이트 네트워크 연결(GS NFV-IFA 032)'과 같은 기능은 5G 시스템에서 실행될 다양한 응용 프로그램을 처리하는 데 필수적이다. 또한, 위 기능은 3GPP 관리 시스템이 가상화된 5G 네트워크의 리소스 관리를 위한 NFV MANO(Management and Orchestration) 시스템과 상호 작용하도록 돕고 있다.

1.1.2 EU, 자율주행 통신관련 WAVE 표준 도입 방안 최종 부결[2]

2019년 7월 8일, 유럽의 V2X(Vehicle to Everything, 차량·사물 통신) 표준으로 IEEE 802.11p 기반 WAVE 표준 도입 법안이 최종 부결됨을 공식적으로 발표하였다.

* TTA는 해외 표준화기구의 최신 동향을 조사하여 주간/월간으로 '해외 ICT 표준화 동향 정보'를 제공하고 있습니다. 본 원고는 2019년 5월 말부터 2019년 7월 초까지 게재한 정보를 요약 정리하였습니다.

유럽에서는 비면허대역 5.9GHz 주파수 관련 자율 주행차에 적용할 기술에 있어서 어느 기술이 더 적합하고 안전한지에 대해 5G 기반 C-V2X 진영과 IEEE 802.11p Wi-Fi 기반 WAVE 진영 간의 논쟁이 있어 왔다.

2019년 4월 EU(European Union, 유럽연합)는 앞서 C-ITS(Cooperative Intelligence Transport System, 차세대 지능형교통체계) 표준 기술로 WAVE를 택한 EU 최종결정을 2개월 보류하기로 했으며, 2019년 7월 4일 있었던 투표를 통하여 본회의 결정을 뒤집으며 결과적으로 WAVE 표준 도입 법안이 최종 부결되었다.

자율주행 통신 기술로 5G를 지지했던 5GAA(5G Automotive Association, 5G 자동차협회)의 Maxime Flament는 'EU 이사회의 투표 결과는 기술 중립성의 중요성을 강조한 EC(European Commission, 유럽위원회)에 보내는 강력한 메시지'라고 언급하였다.

1.1.3 ETSI 오픈소스 표준 Rel 6(Open Source MANO OSM Rel 6) 발표[3]

2019년 6월 20일, ETSI OSG(Open Source Group) OSM(Open Source MANO)은 OSM Rel 6를 발표하였다.

2016년 2월 22일, ETSI는 MWC(Mobile World Congress, 세계 이동통신 산업 전시회)에서 오픈소스그룹(OSG)인 Open Source MANO(OSM) 신설을 발표하였다.

OSM은 오픈소스를 기반으로 하여 NFV(Network Function Virtualization, 네트워크 기능 가상화) MANO(Management and Orchestration)의 구현을 위해 ETSI에서 지원하는 프로젝트이며 NFV-MANO는 NFV의 자원을 생성 및 관리, VNF(Virtualized network functions, 가상화 네트워크 기능) 관리 등을 수행한다.

OSM Rel 6는 HetNet(heterogeneous networks, 이종 네트워크) 및 클라우드 기술 전반에 걸쳐 엔드-투-엔드 오케스트레이션(Orchestration)을 제공할 수 있는 새로운 기능을 제공한다.

Rel6는 네트워크 서비스의 확장된 기능과 SA(Service Assurance, 서비스보증) 프레임워크의 확장으로 인해 복잡한 서비스 관리가 이전보다 수월해졌으며, OSM이 지원하는 기본 기술 범위를 더욱 넓혔다. 또한, FOG05 Edge Cloud, TAPI 기반 전송 네트워크, VMware의 vCloud Director 9.5 및 공용 클라우드를 위한 새로운 커넥터를 개발하였으며, 지원을 개선하기 위해 추가적인 EPA(Enhanced Platform Awareness) 속성을 지원하고, 멀티 세그먼트 네트워크를 추가함으로써 이전 릴리스에서 이용 가능한 커넥터에 여러 가지 개선 사항이 추가되었다.

1.1.4 CEN/CENELEC, 제15차 연례회의에서 유럽표준의 청사진 논의[4]

2019년 6월 5일부터 6일까지, CEN과 CENELEC은 루마니아 부쿠레슈티(Bucharest)에서 열린 제 15차 연례회의에서 유럽 표준의 지금까지의 성과를 평가하고 미래 나아가야 할 방향과 우선순위를 논의하였다.

2019년 6월 6일은 CEN과 CENELEC 회원국들은 각각 따로 만나 구체적인 조직적, 절차적 요소를 논의한 뒤 공동 이익에 관한 문제를 논의하기 위한 공동 세션을 개최하였으며, 공동

세션에서 CEN과 CENELEC 담당자는 유럽 표준화와 관련된 주요 전략, 정책 및 기술적 문제에 대해 보고하였다. CEN과 CENELEC 총회는 미래 발전을 위한 다음의 몇 가지 중요한 조치와 결정을 승인하였다.

첫째, 유럽 위원회와의 협력 강화를 위한 노력의 일환으로, 일치된 표준 개발 과정의 성과에 대한 적절한 모니터링을 위해 공동 KPI가 제안되었다.

둘째, 국제적인 맥락에서 유럽 시스템의 강점을 고려하기 위해 'Strategy beyond 2020'에 대한 논의를 계속하기로 결정하였고, 2019년 7월 17일부터 18일까지 'Strategy beyond 2020' 특별 워크숍을 개최할 예정이다.

셋째, CEN과 CENELEC의 디지털 전환 전략(Digital Transformation Strategy)의 일부인 IT 프로젝트와 시범사업 등의 포괄적이고 효율적인 관리를 위해 새로운 DITSAG(Strategic Advisory Group on Digital and Information Technology, 디지털 정보 기술의 전략자문그룹)을 설립하였다. 이를 통해 CEN과 CENELEC은 ETSI와의 협력을 더욱 강화하고자 하는 목표를 확인하였다.

넷째, 사이버보안과 표준화에 대한 심도 깊은 논의도 진행되었는데 사이버보안 인증 프레임워크에서, CEN과 CENELEC은 사이버보안이 비즈니스, 정책결정자에게 도움이 되는 사이버보안과 표준화에 대한 논의와 과제를 심층적으로 분석하였으며, 안전하고 접근 가능하며 신뢰할 수 있는 새로운 기술을 만들기 위해 표준화가 기여할 수 있는 몇 가지 방법을 제안하였다. 사이버 보안과 관련하여 EU는 2018년 말 ICT 제품, 시스템 및 서비스에 대한 유럽의 공통 사이버 보안 인증 프레임워크를 구축하여 사이버 공격에 효과적으로 대응할 수 있는 능력 확보를 목표로 자체적인 「사이버 보안법」을 제안한 바 있다.

1.1.5 ETSI, IoT 상호 운용성 향상을 위한 IP 비디오 감시 표준 발표[5]

2019년 6월 13일, ETSI TC ATTM(Access, Terminals, Transmission and Multiplexing)은 이더넷과 IP 영상 감시에 대한 PoC(Power over Coax, 동축케이블) 솔루션을 제공하기 위한 TS 105 176-2 기술 표준을 발표하였다.

ETSI TC ATTM은 접근, 터미널, 전송, 멀티플렉싱의 표준화를 담당하며, 이는 배선(cabling), 설치, 신호 전송 및 물리층의 특정 기술, 장비, 설치 및 규정 측면에 초점을 맞춘 개인 및 공공 영역에서의 디지털화까지의 신호처리를 포함한다.

이 표준은 동축케이블 인프라에서 IP 데이터를 전송함으로써 기존의 아날로그 비디오 감시 시스템에서 IP 비디오 감시 시스템으로 에너지를 효율적이면서 지속 가능한 전환을 가능하게 하여 안전하고 신뢰할 수 있는 전력 공급을 보장하기 위해 개발되었다.

ETSI TS 105 176-2 구현은 IP 카메라, IP 스위치, 비디오 인터콤 시스템, 디스플레이 등과 같은 통신 기기 간의 상호 운용성을 보장한다. 또한, 헤드 엔드(head-end) 기기에서 새로운 프론트 엔드(front-end) 기기로 새 케이블을 배치하지 않고도 추가 IP 카메라 또는 기기로 비디오 감시 동축 네트워크를 확장하는 기능을 제공하며 동축 케이블 인프라의 장거리에서 전력 및 IP 데이터 기기 간의 상호 운용 전송을

가능하게 하여 견고하고 관리가 용이하며 상호 운용 가능한 인프라를 제공한다.

2. 사실표준화 기구 동향

2.1 FIDO Alliance, 2개의 새로운 WG 신설 발표[6]

2019년 6월 26일, FIDO Alliance는 IoT(Internet Of Things, 사물인터넷)와 본인 인증에 관한 표준 기술 규격 및 시험인증 프로그램 개발 준비를 위해 다음과 같은 두 개의 워킹그룹의 신설을 발표하였다.

- **IoT TWG:** IoT 기술 워킹 그룹, IoT Technical Working Group
- **IDWG:** 본인 인증 및 바인딩 워킹그룹, Identity Verification and Binding Working Group

IoT TWG는 2020년 약 200억 개 이상의 사물이 연결될 것으로 예측되는 사물인터넷 시장에 종합적인 인증 프레임워크를 제공하여 부족한 사물인터넷 보안 표준 그리고 이들이 운영되는 네트워크와 프로세스 상에서 야기될 수 있는 대규모 해킹공격에 대한 우려를 해결하고자 한다.

IDWG는 원격 신원 확인 기준을 정의하고 시험인증 프로그램과 교육 자료를 개발해 FIDO 인증장치를 분실하거나 도난당한 경우 계정 복구 프로세스가 사용자 계정의 무결성을 유지하도록 하는 역할을 할 예정이다.

Fido Alliance는 신규로 신설된 두 개의 WG을 통하여 해당 분야의 가이드라인과 시험인증 기준을 세워 본인 증명 강화를 통해 계정 복구 프로세스를 개선하고자 하며 또한, IoT 환경에서 비밀번호 사용을 제거하기 위해 온보딩(Onboarding)을 자동화하고자 하는 목표를 두고 있다.

2.2 FIDO Alliance, '암호없는 FIDO2 인증방식을 적용한 마이크로소프트의 공개 프리뷰' 소개[7]

2019년 7월 9일, 마이크로소프트사는 로그인 시에 암호를 제거하여 암호 없는 인증 기능을 사용자에게 제공하기 위해 Azure AD(Azure Active Directory)의 FIDO2 보안 키에 대한 공개 프리뷰를 발표하였다.

FIDO2 보안 키는 모든 폼 팩터에서 발생할 수 있는 암호 없는 인증 표준 기반 방법이며 개방형 표준인데 FIDO2 보안 키와 덕분에 Azure AD 사용자는 암호를 입력하지 않고도 로그인이 가능해졌다.

마이크로소프트 365팀은 '이러한 강력한 인증 요인은 생체 인식(지문 또는 안면 인식) 또는 PIN으로 보호되는 공용 키/개인 키 암호화 표준 및 프로토콜을 기반으로 한다'고 언급하였다.

사용자는 생체인식 팩터나 PIN을 적용하여 기기에 안전하게 저장된 개인키를 잠금 해제하고, 그 다음 키는 사용자와 장치가 서비스에 누구인지를 증명하는 데 사용된다.

FIDO2 암호 없는 로그인 지원과 마찬가지로 Microsoft 365 사용자는 7월 9일부터 일주일 동안 새로운 공개 미리보기 기능에 액세스할 수 있다.

[참고문헌]

[1] https://www.etsi.org/newsroom/press-releases/1622-2019-07-etsi-nfv-announces-new-features-to-its-architecture-to-support-5g

[2] https://www.reuters.com/article/us-eu-autos-tech/eu-opens-road-to-5g-connected-cars-in-boost-to-bmw-qualcomm-idUSKCN1TZ11F

[3] https://www.etsi.org/newsroom/press-releases/1616-etsi-osm-release-six-enhances-edge-support-and-lets-your-network-service-fly

[4] https://www.cencenelec.eu/News/Press_Releases/Pages/PR-2019-05.aspx

[5] https://www.etsi.org/newsroom/press-releases/1613-2019-06-etsi-releases-specification-for-energy-efficient-ip-video-surveillance-enabling-further-iot-interoperability

[6] https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/

[7] https://fidoalliance.org/bleepingcomputer-microsoft-azure-ad-fido2-passwordless-sign-in-in-public-preview/

[주요 용어 풀이]

- NFV(Network Function Virtualization, 네트워크 기능 가상화): 네트워크의 방화벽, 트래픽 부하 제어 관리, 라우터 등과 같은 하드웨어 장비의 기능과 처리 기능을 서버단에서 소프트웨어로 구현하는 기술. 네트워크 기능 가상화(NFV) 프레임워크는 크게 VNF(Virtualized network functions), NFVI(NFV infrastructure), NFV-MANO 아키텍처 프레임워크(NFV management and orchestration architectural framework)로 구성된다. VNF는 여러 응용 프로그램을 지원하는 네트워크 기능들의 집합이며, NFVI는 컴퓨터 프로세싱, 스토리지, 네트워킹 자원을 가상화하고 VNF 실행을 지원한다.
- 오케스트레이션(orchestration): 일부 유용한 기능을 구현하기 위해 한 웹서비스가 다른 웹서비스를 호출하는 순서와 조건을 정의한다.