



해외 ICT 표준화 동향

2018년 5월

(2018.5.1.~2018.5.31.)

* 게시물 보기

TTA 홈페이지 ▷ 자료마당 ▷ TTA 간행물 ▷ 표준화 이슈 및 해외 동향

목차

I. 국제 표준화 기구

1. ITU, ITU PP-18 회의 개최 예정
2. ITU, ICT CBS-2018(정보통신기술 능력배양 심포지엄) 개최

II. 지역 표준화 기구

1. 미국

- 1.1 NIST, 사이버 보안 프레임워크(CSF) 1.1 버전 발표
- 1.2 ATIS-OCF 상업용 IoT 표준향상을 위한 MoU 체결
- 1.3 ISO/IEC JTC1, AIDC 애플리케이션 표준 개발을 위한 WG 8 발표
- 1.4 EU 개인정보보호규정(GDPR) 관련 국제표준 소개

2. 중국

- 1.1 중국, 국가표준 프로젝트 검토 회의 개최
- 1.2 중국, 블록체인 국가표준 2019년 말 공식화 예정

III. 기타 사실 표준화 기구

1. IEEE, 분산 전원(DERs)의 상호 연결과 상호 운용에 대한 표준 개정
2. IEEE, 중국의 고대역폭 무선 LAN 용량 증가를 위한 표준 개정
3. 미 국방부, 공급망 내 사이버 보안을 위한 새로운 지침 발표
4. 2018 산업용 사물인터넷(IIOT) 기술 혁신 협약 개최
5. NIST, 위험 관리 프레임워크(RMF) 개선을 위한 초안 발표
6. 3GPP CVD(Coordinated Vulnerability Disclosure)프로세스 시작 발표
7. Wi-Fi Alliance, EasyMesh™ 프로그램 개시

I. 국제 표준화 기구

1. ISO/IEC JTC1

1.1 ITU, ITU PP-18 회의 개최 예정

ITU(International Telecommunication Union, 국제전기통신연합) PP-18(Plenipotentiary Conference 2018, 전권위원회), 두바이에서 10월 29일부터 11월 16일까지 개최될 예정이다. 또한, 4년마다 열리는 이 회의는 ITU 회원국인 193개국이 모여 2020-2023 로드맵을 수립할 예정이다.

※ 참고: <http://www.pp18dubai.ae/>

<https://www.itu.int/en/mediacentre/Pages/2018-CM08.aspx>

1.2 ITU, ICT CBS-2018(정보통신기술 능력배양 심포지엄) 개최

2018년 6월 18일부터 20일까지, ITU(International Telecommunication Union, 국제 전기 통신 연합)는 ICT 능력배양 심포지엄(Capacity Building Symposium, CBS-2018)을 개최할 예정이다.

이 심포지엄에서는 다음과 같은 주제를 다룰 예정이다.

- 유엔의 지속가능발전목표(Sustainable Development Goals, SDGs)를 달성하기 위해 ICT 사용에 있어서 요구되는 기술 요구 사항
- 디지털 경제에 적합한 인력 준비를 위한 학술 기관의 역할
- 인공 지능, 로봇 및 기계 학습, 사물의 인터넷, 클라우드 컴퓨팅 및 빅 데이터 분석을 비롯한 글로벌 디지털 변환을 고려한 디지털 기술

<https://www.itu.int/en/mediacentre/Pages/2018-MA11.aspx>

II. 지역 표준화 기구

1. 미국

1.1 NIST, 사이버 보안 프레임워크(CSF) 1.1 버전 발표

2018년 4월 16일, 미 상무부의 국립 표준 기술 연구소(National Institute of Standards and Technology, NIST)는 사이버보안 인프라의 중요한 개선을 위한 프레임워크(Framework for Improving Critical Infrastructure Cybersecurity)의 1.1버전¹⁾을 발표하였다.

사이버보안 프레임워크 1.0 버전은 2014년 2월에 발표되었고 NIST의 프레임워크는 사이버보안 문제와 관련된 이해관계자, 정부, 산업계 및 학계의 피드백을 토대로 개발하였다.

업데이트된 사이버보안 프레임워크 버전 1.1은 현재 사용되는 표준, 지침 및 관행을 정리하여 사이버보안의 여러 접근법에 대한 공통의 조직 구조를 제공한다.

사이버보안 프레임워크 1.1 버전의 업데이트된 주요 내용은 다음과 같다.

- 인증 및 아이덴티티(authentication and identity)
- 사이버보안 위험 자체 평가(self-assessing cybersecurity risk)
- 공급망 내의 사이버보안 관리(managing cybersecurity within the supply chain)
- 취약점 공개(vulnerability disclosure)

☞ https://www.ansi.org/news_publications/news_story?menuid=7&articleid=f5

1.2 ATIS-OCF 상업용 IoT 표준향상을 위한 MoU 체결

2018년 3월 6일, ATIS(Alliance for Telecommunications Industry Solutions)와 OCF(Open Connectivity Foundation)는 OCF와 IoT(Internet of Things)표준 간의 기술적인 연계를 촉진하기 위한 MoU(Memorandum of Understanding)를 체결하였다.

MoU에 따라 ATIS와 OCF의 회원사는 협력하여 oneM2M 글로벌 표준을 사용하여 상용 제품의 광범위한 사물인터넷(IoT) 서비스에 대한 원활한 사용자 액세스를 지원하는 중추적인 단계로 인터 워킹 프록시의 오픈소스 구현을 개발할 예정이다.


ATIS-OCF 공동 작업의 시작점은 ATIS의 OS2-IoT 오픈소스 구현인 oneM2M 표준에 기반을 두고 있다. OS-IoT는 스마트 장치 및 기타 임베디드 경량 응용 프로그램에 대한 oneM2M 채택을 향상시키는 데 도움이 되는 중요한 리소스이다.

또한, ATIS는 개발자에게 oneM2M 기능에 액세스할 수 있는 툴킷(Toolkit)을 제공하는 OS-IoT

1)참고: <https://www.khronos.org/registry/vulkan/specs/1.1/html/vkspec.html>

소프트웨어 라이브러리를 출시하였다

ATIS CEO인 수잔 밀러(Susan Miller)는 OCF와의 MoU는 사물인터넷(IoT)을 발전시키는 표준에 대한 ATIS의 약속을 반영하며 표준화와 상호운용성은 원격 의료, 자동차 분야, 가정 자동화 등에 이르는 분야에서 IoT 솔루션의 성공과 보안을 보장하는데 필수적이라고 언급하였다.

 <https://sites.atis.org/insights/atis-open-connectivity-foundation-collaboration-advances-iot-standards-for-commercial-applications/>

1.3 ISO/IEC JTC1, AIDC 애플리케이션 표준 개발을 위한 WG 8 발표

ISO/IEC JTC1 SC 31(자동식별 데이터 캡처 기술, Automatic identification and data capture techniques)²⁾은 AIDC(자동 식별 데이터 캡처, Automatic Identification and Data Capture) 애플리케이션 표준 개발을 위한 워킹그룹(WG 8)을 신설하였다.

ISO/IEC JTC1 SC 31은 바코드 기호(바코드 작성 및 읽기 방법), RFID 에어 인터 페이스 프로토콜(RFID 태그 인식 방법), 실시간 위치 시스템, 고유 ID 및 데이터 콘텐츠를 제공한다.

AIDC는 전 세계적으로 수십억 개 품목에 대한 정보를 식별, 기록 및 저장하는데 사용되는 기술 패밀리이며 소비재는 AIDC(예 : 바코드, RFID)를 사용하여 태그가 지정되고 AIDC는 일반적으로 선형 바코드 또는 2차원 DataMatrix³⁾ 형태를 취한다.

WG 8은 AIDC 표준을 적용할 수 있도록 다른 표준위원회를 지원하고, AIDC 응용 표준을 개발할 예정이다.

 https://www.ansi.org/news_publications/news_story?menuid=7&articleid=67fb73b7-2f1d-4fb1-9898-437625b91c0b

1.4 EU 개인정보보호규정(GDPR) 관련 국제표준 소개

2018년 5월 25일, 유럽연합(European Union, EU)이 제정한 개인정보보호 규정(General Data Protection Regulation, GDPR)이 발효되었다.

2)참고: http://www.iec.ch/dyn/www/f?p=103:7:0:::FSP_ORG_ID:3405

3)참고: http://www.barcode.center/data.html?type=view&code1=A&code2=AB&code3=&code4=&code5=&gd_no=2068

GDPR은 1995년부터 유럽연합이 운영해 온 '유럽연합 정보보호법'을 강화한 규정이며 2016년 4월 14일 유럽연합 의회의 승인을 얻어 5월 25일부터 발효되었다.

GDPR은 유럽 전역의 데이터 개인정보보호법을 조화시키고 모든 유럽연합 시민의 데이터 개인 정보를 보호하고 권한을 부여하며 지역의 조직이 데이터 개인정보에 접근하는 방식을 재구성하도록 고안되었으며 특히 기관이 GDPR(개인정보보호규정)을 적절하게 준수하도록 마련한 국제표준은 다음과 같다.⁴⁾

- ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements : 정보 보안 관리 시스템을 수립, 구현, 유지 및 지속적으로 개선하기 위한 요구 사항을 규정함

- ISO/IEC 27018:2014 - Information technology - Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors : 공개 클라우드 컴퓨팅 환경에 대한 ISO/IEC 29100의 개인정보보호 원칙에 따라 개인식별정보(Personally Identifiable Information, PII) 보호를 위해 일반적으로 수용되는 통제 목표, 통제 및 지침을 수립

- BS 10012:2017 - Data protection. Specification for a personal information management system (British Standard) : 데이터 보호 요구사항을 준수 및 개선하기 위한 프레임워크인 개인정보경영시스템(Personal information management system, PIMS)의 올바른 구축과 적용을 위한 표준

☞ https://www.ansi.org/news_publications/news_story?menuid=7&articleid=9edde569-2ae5-41ec-bb82-a04c54f8907f

2. 중국

1.1 중국, 국가표준 프로젝트 검토 회의 개최

2018년 4월 19일 중국국가표준연구소(China National Institute of Standardization), CNIS)와 국가표준기술검토센터(National Standard Technology Review Center)는 베이징에서 국가표준(권고표준) 프로젝트 검토 회의를 개최하였다.

이번 검토회의에서는 총 311 개의 국가표준 프로젝트 승인이 있었으며, 대부분 비철금속,

4)참고: <https://blog.ansi.org/2018/04/general-data-protection-regulation-gdpr-27001/>

금속, 전자, 에너지 및 전기의 주요 경제 및 사회 개발 분야와 관련하여 회의가 진행되었다.

※ 참고: http://www.cnis.gov.cn/xwdt/bzhdt/201804/t20180423_24035.shtml

☞ <http://www.cspress.com.cn/xinwenzhongxin/zonghexinwen/46004.html>

1.2 중국, 블록체인 국가표준 2019년 말 공식화 예정

2018년 5월 10일, 중국 정부가 블록체인 기술에 대한 국가표준을 마련하고, 2019년까지 중국 블록체인 산업 육성을 위한 정층설계(頂層設界)에 나선다고 밝혔다.

정층설계란 정부가 관련 분야의 발전 전략을 수립하여 방향을 제시하는 전략이며 블록체인 분야에 대한 정층설계는 중국 정부가 나서 이 산업을 발전시키겠다는 의미를 내포하고 있다.

중국 정부는 이러한 목표를 달성하기 위해 '분산원장기술 표준화 위원회'를 설립하고 2019년까지 공식적인 국가표준을 공개할 것이라고 밝혔으며 해당 위원회는 블록체인 기술의 기술적, 사업적 호환성과 보안성 등의 부분을 검토할 예정이다.

현재 탈 중앙 방식을 적용할 수 있는 다양한 분야에 블록체인 기술을 도입하기 위해 국가적 차원의 표준을 개발하고 있으며 기본적인 부분부터 사업·응용프로그램, 프로세스, 정보보안 등 구체적인 부분까지 상호 운용이 가능하고 신뢰성 높은 산업 표준을 제시할 예정이다.

중국 정부 관계자는 '보안'을 블록체인 기술에서 가장 중요한 요소로 보고 표준을 설정하는 데 핵심적인 검토 사항이 될 것이라고 밝혔다.

현재 중국은 ISO TC 307(Blockchain and distributed ledger technologies)에서 블록체인 표준 개발을 위해 참여하고 있다.

☞ http://big5.xinhuanet.com/gate/big5/www.cs.com.cn/xwzx/201805/t20180510_5798199_1.html

Ⅲ. 기타 사실 표준화 기구

1. IEEE, 분산 전원(DERs)의 상호 연결과 상호 운용에 대한 표준 개정

2018년 4월 26일, IEEE는 공공전력 시스템(EPSS)과 분산 전원(DERs, Distributed Energy Resources) 간의 상호 연결 및 상호 운용성에 대한 표준(IEEE 표준 1547-2018)을 개정하였다.⁵⁾

IEEE 표준 1547-2018은 성능, 작동, 테스트, 안전 고려 사항 및 상호 연결 유지와 관련된 요구 사항을 제공한다.

- 비정상적인 상황에 대한 대응, 전력 품질, 고립 상태, 테스트 규격 및 설계, 생산, 설치 평가, 커미셔닝, 및 주기적 테스트와 일반적인 요구사항을 제공하고 분산 전원 규격의 모든 유형과 크기에 대한 적합성을 보장함

분산 전원의 상호 연결에 대한 IEEE 1547 요구사항에는 대부분의 설비에 일반적으로 적용되는 동기식 기계, 유도 장치 또는 전원 인버터/변환기용 요구 사항이 포함된다.

- 방사형 1차 및 2차 배전 시스템에 분산 전원을 설치하는 것은 IEEE 표준 1547-2018의 주된 강조점임

☞ http://standards.ieee.org/news/2018/ieee_1547-2018_standard_revision.html

2. IEEE, 중국의 고대역폭 무선 LAN 용량 증가를 위한 표준 개정

2018년 5월 3일, IEEE는 IEEE 802.11aj 표준을 개정하였다.

IEEE 802.11aj-2018은 IEEE 802.11-2016의 개정안으로 중국에서 증가하는 고속 무선 LAN 수요량을 충족시키기 위해 60GHz 및 45GHz 주변의 중국 밀리미터파주파수 대역에서 작동할 수 있도록 물리적(Physical, PHY) 계층과 매체 액세스제어(Medium Access Control, MAC) 계층에 대한 개정을 포함한다.

- 60GHz 대역에서 네 개의 1.08GHz 채널을 지정하여 데이터 전송률이 높고 적용 범위가 넓은 저 전력 장치를 지원하고 최대 15Gb/s의 데이터 전송 속도로 45GHz 대역의 새로운 5GHz 대역폭에 대한 액세스를 제공함

5)참고: <https://standards.ieee.org/findstds/standard/1547-2018.html>

- 중국의 인구 밀집 도시와 모바일 장치의 유비쿼터스 사용과 관련하여 IEEE 802.11aj는 장치 간섭을 완화하고 즉각적인 전력 요구 사항을 낮추고 소형 안테나가 있는 소형 폼팩터 배터리 구동 장치의 경우 적용 범위를 늘리는 강력한 솔루션을 제공함

개정 표준에는 향상된 네트워크 성능과 IEEE 802.11a™ 표준과의 역 호환성을 위한 MAC 메커니즘이 포함되어 있다. 또한, IEEE 802.11aj는 더 높은 네트워크 성능을 위해 다중 입력 다중 출력 (multiple-input multiple-output, MIMO)¹⁾ 기술을 통합하여 중국의 45GHz 대역에 할당된 최대 5GHz의 비 면허 대역폭에서 작동할 수 있다.

☞ http://standards.ieee.org/news/2018/standard_increased_high_bandwidth_wlan_china.html

3. 미 국방부, 공급망 내 사이버 보안을 위한 새로운 지침 발표

2018년 4월 24일, 미 국방부(Department of Defense, DoD)는 NIST SP 800-171에 규정된 새로운 보안 규칙을 준수하지 않은 사업체를 제재하는 방법에 대한 새로운 가이드를 발표하였다.

향후 미 국방부에 제품과 서비스를 제공하는 회사는 NIST SP 800-171에 명시된 110가지 보안 요구 사항을 충족해야한다.

☞ <https://www.csoonline.com/article/3269526/data-protection/dod-releases-new-guidance-to-protect-data-within-the-supply-chain.html>

4. 2018 산업용 사물인터넷(IIOT) 기술 혁신 협약 개최

2018년 5월 24일부터 26일까지 2018 산업용 사물인터넷 기술혁신 컨벤션(Industrial Internet of Things Innovation Convention 2018)이 베이징에서 개최될 예정이다.

기술 연구, 5개 산업 분야의 선도적인 우수 사례, 활발한 대화 형 토론 및 피어 투 피어(peer to peer, P2P) 네트워킹으로부터 얻은 사례 연구에 대한 포괄적인 시각을 제공하기 위해 고안되었다.

☞ http://www.szwgroup.com/industrial-internet-of-things-innovation-convention-2018-en/news_detail.aspx?id=131256

5. NIST, 위험 관리 프레임워크(RMF) 개선을 위한 초안 발표

2018년 5월, NIST는 개인의 사생활 보호뿐만 아니라 사이버 보안 위협으로부터 국가의 중요 자산을 보호하기 위한 노력을 강화하여 위험 관리 프레임워크(RMF, Risk Management Framework)를 개선하기 위한 초안(Draft NIST Special Publication(SP) 800-37 Revision 2)1)을 발표하였다.

NIST (SP) 800-37 Revision 2 초안의 주요 내용은 다음과 같음

- 조직의 최고책임자(C-suite) 수준에서 위험 관리 프로세스와 활동 간의 긴밀한 연계 및 의사소통을 제공하며 조직의 시스템 및 운영 수준에서 개인, 프로세스 및 활동 간의 긴밀한 연계와 의사소통을 제공함
- 보다 효과적이고 비용 효율적인 위험 관리 프레임워크 실행을 촉진하기 위해 중요한 조직 차원의 위험 관리 준비 활동을 제도화함
- 사이버 보안 프레임워크가 위험 관리 프레임워크와 어떻게 연계되고 기존의 NIST 위험 관리 프로세스를 사용하여 구현 될 수 있는지 보여줌
- 개인 정보 위험 관리 개념과 원칙을 위험 관리 프레임워크에 통합하고 통합된 보안 및 개인 정보 제어 카탈로그의 사용을 NIST SP 800-53 Revision 5(Security and Privacy Controls for Information Systems and Organizations)에서 지원함
- NIST SP 800-160(Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems)의 수명주기 기반 시스템 엔지니어링 프로세스를 위험 관리 프레임워크의 단계와 일치시켜 신뢰할 수 있는 안전한 소프트웨어 및 시스템 개발을 촉진
- SDLC 전반에 걸쳐 신뢰할 수 없는 공급업체, 위조품 삽입, 변조, 무단 생산, 도용, 악성 코드 삽입, 제조 및 개발 관행의 취약성으로부터 보호하기 위해 SCRM(Supply Chain Risk Management) 개념을 위험 관리 프레임워크(RMF)에 통합함
- 기존의 기본 제어 선택 접근방법을 보완하기 위해 조직에서 생성한 대체 제어 접근방법을 제공함

NIST는 2018년 6월 22일까지 RMF 초안에 대한 의견을 수렴하고 최종 버전은 2018년 10월에 발행할 예정이다.

☞ <https://www.nist.gov/news-events/news/2018/05/nist-updates-risk-management-framework-incorporate-privacy-considerations>

6. 3GPP CVD(Coordinated Vulnerability Disclosure)프로세스 시작 발표

3GPP 사무국은 CVD(Coordinated Vulnerability Disclosure, 협정 취약성 공개) 프로세스를 시작하였음을 공표하였다.

CVD는 기술 규격의 오류, 누락 또는 모호함으로 인해 의심되거나 입증된 취약성을 보고받아 3GPP 담당 그룹으로 신속하게 전달함으로써 문제를 분석하고 해결하도록 하는 절차이다/

개인이나 기관이 3GPP 발간물과 관련된 취약점에 대한 정보를 제공할 수 있는 공식화된 프로세스를 최초로 마련하였다.

☞ http://www.3gpp.org/news-events/3gpp-news/1958-cvd_news

7. Wi-Fi Alliance, EasyMesh™ 프로그램 개시

2018년 5월 14일, Wi-Fi Alliance는 일련의 통일된 Wi-Fi 서비스를 제공하는 효율적인 자가 조직(Self-organizing) 네트워크를 가능케 하는 Wi-Fi CERTIFIED EasyMesh™ 프로그램을 개시하였다.

- Wi-Fi Certified EasyMesh™ 프로그램은 멀티AP 솔루션으로 액세스 포인트에 중점을 둔 프로그램이며 EasyMesh 기술은 서로 다른 유무선 AP(Access Point, 액세스 포인트)를 조합해 Wi-Fi 신호를 끌어올리는 메시(Mesh) 네트워크 프로그램으로 EasyMesh와 호환되는 유무선 AP는 제조사에 관계없이 서로 정보를 주고 받으며 Wi-Fi에 최적화된 신호를 전달할 수 있다.

Wi-Fi CERTIFIED EasyMesh™ 는 다음의 2가지 주요 구성을 가진다.

- 에이전트(Agents) : 네트워크 및 클라이언트 성능을 모니터링한 뒤 네트워크 기기에서 작동하는 컨트롤러에 보고함

- 컨트롤러(Controller) : 네트워크 트래픽을 관리하고 AP에 클라이언트를 할당해 네트워크 성능과 효율성을 극대화함

Wi-Fi CERTIFIED EasyMesh™의 주요 기능은 다음과 같다.

- 유연한 디자인(Flexible design) : 확장된 커버리지를 제공하는 여러 개의 AP를 최적으로 배치할 수 있음
- 손쉬운 설정(Easy setup) : 자동화 기기 온보딩(onboarding) 및 구성 제공
- 네트워크 인텔리전스(Network intelligence) : 자체 구성 및 자체 최적화 네트워크는 정보를 수집하고 네트워크 상황에 대응하여 성능을 극대화함
- 효율적인 로드 밸런싱(Effective load balancing) : 장치가 최상의 접속을 찾고 간섭을 회피할 수 있도록 가이드
- 확장성(Scalability) : Wi-Fi EasyMesh AP가 다양한 제조업체에 고착되지 않도록 함

Wi-Fi Alliance는 EasyMesh 표준이 하드웨어뿐만 아니라 라우터의 인텔리전스에 대한 혁신을 이끌어 갈 것으로 예상함

☞ <https://www.wi-fi.org/news-events/newsroom/wi-fi-certified-easymesh-delivers-intelligent-wi-fi-networks>