

해외 표준화기구 동향¹⁾

TTA 표준화본부 표준기획부



1. 국제표준화기구 최근 동향

1.1 국제전기통신연합(ITU)

1.1.1 ITU, 두바이 스마트시티 성능 보고서 발표[1]

2016년 12월 21일, ITU는 세계 첫 스마트시티를 구현한 두바이 사례의 스마트시티 성능 보고서²⁾를 발표하였다. 이번 보고서는 2015년 ITU와 두바이의 스마트시티 협력 체결에 따른 발간으로, 세부 내용으로는 도시 개발 문제의 해결책 등을 담고 있다.

1.2 ISO/IEC 합동기술위원회(ISO/IEC JTC1)

1.2.1 ISO/IEC JTC1, 발행자인증번호 표준 개정[2]

2016년 11월 21일, ISO/IEC JTC1는 발행자 인증 번호(IIN, Issuer Identification Number³⁾) 표준

(ISO/IEC 7812-1)을 개정하였다.

현재, 발행자 인증 번호(IIN)는 ISO/IEC 7812-1 SC17(카드 및 개인식별)에서 담당하고, 발행자인증 번호(IIN)에 대해 6자리 고정 길이 숫자로 정의하고 있으며, 8~19자리의 다양한 길이를 가진 카드 소유자 식별에 사용하는 주요 계좌 번호(PAN, Primary Account Number)⁴⁾를 정의하고 있다.

발행자인증번호 표준은 카드 발급사가 점차 증가함에 따라 IIN의 공급이 부족할 것을 예상하여, ISO/IEC 7812-1에서 IIN을 현재의 6자리에서 8자리로 확장한다는 내용과 PAN을 10~19자리로 범위를 확대한다는 내용을 설명하고 있다. 현재 표준초안이 ISO 회원의 승인을 득하였고, 2017년 초에 최종 발표될 예정이다.

1) TTA는 해외 표준화기구의 최신 동향을 조사하여 주간 및 월간으로 '해외 ICT 표준화 동향 정보'를 제공하며, 이 칼럼은 지난 2017년 1월부터 2월까지 게재한 정보 중에서 공유 필요가 있는 정보를 선정하여 제공하고자 합니다.

2) 보고서 원문: <http://www.itu.int/en/publications/Documents/tsb/2016-DubaiCase/index.html>

3) 발행자 인증 번호(IIN, Issuer Identification Number): 발행자 인증은 ISO가 1989년에 처음 제정한 국제 표준(ISO/IEC 7812)으로, 발행자 인증 번호(IIN)가 국가 간, 산업 간, 산업 내 교환에서 운영될 수 있도록 만든 카드 발행자 인증을 위한 숫자 매김 시스템으로, IIN 등록을 위한 절차를 밟음. ※출처: 위키백과

4) 주요 계좌 번호(PAN, Primary Account Number): 지불 또는 신용카드와 같이 돈을 지불하는 카드의 식별자로서 경우에 따라 은행 카드 번호라 함. 이는 단순히 카드를 식별하는 기능으로, 발행 회사가 카드를 식별하거나 카드 소유자를 식별하지 못함. ※출처: 위키백과

1.2.2 ISO/IEC JTC1, 사이버보안 지침(ISO/IEC 27004:2016)

제정[3]

2016년 12월 30일, ISO/IEC JTC1은 사이버보안 성능 표준(ISO/IEC 27004:2016)⁵⁾을 제정하였다. 이는 ‘정보기술-보안기술-정보보안관리-모니터링, 측정, 분석 및 평가(ISO/IEC 27004:2016)’ 표준으로, ISO/IEC 27001(정보보안 요구사항)⁶⁾의 성능 측정 방법에 대한 가이드라인을 제공하고 있다.

이번 표준은 53개국 참여와 DIN(독일표준협회)의 주최 하에 ISO/IEC JTC1의 정보기술 위원회(SC 27)에서 개발하였다. ISO/IEC 27001은 정보보안관리시스템(ISMS, information security management system)의 요구사항에 대한 것으로, ISO/IEC 27004 표준은 효과적 구현을 위하여 정보보안 측정 프로그램 구성방법과 측정방법의 선택 및 측정 프로세스 작동방법에 대하여 명시하고 있다.

이번 표준은 각 기관이 자체적으로 포괄적 복구 계획을 마련하는 데 이용하기 위함으로 사이버 공격 사건 처리 및 긴급사태 대책에 대해 추가하여 기존 NIST 사이버 공격 복구 가이드라인을 통합하였고, ‘사이버보안 프레임워크’라 불리는 핵심 인프라 사이버보안 개선을 위한 ‘복구’ 기능과 관련 추가 정보들을 제시하고 있다. 특히, 다양한 조치에 대한 포괄적 예시와 조치 평가 방법 등이 포함되어 있으며, 책임성 향상, 개선된 정보보안 성능과 ISMS 프로세스 및 적용이 가능한 법률, 규칙 및 규정과 ISO/IEC 27001의 요구사항에 대한 증거를 볼 수 있다.

2. 지역 및 국가별 표준화기구 최근 동향

2.1 유럽 표준화동향

2.1.1 ETSI, 콘텐츠 정보관리 산업규격그룹(ISG CIM) 신설[4]

2017년 1월 11일, ETSI는 스마트시티 응용프로그램에 대한 조치들을 위하여 콘텐츠 정보 관리(Context Information Management) 산업규격그룹(ISG CIM)을 신설하였다.

이번 콘텐츠 정보 관리(CIM) 시스템은 스마트 응용프로그램을 위해 관련 콘텐츠에 따라 계시, 발견, 감독 및 관리하는 역할을 수행한다. 신설된 산업규격그룹에서는 공동 콘텐츠 정보 관리 API, 데이터 계시 플랫폼(data publication platforms) 및 표준 데이터 모델에 대한 규격을 개발할 예정이다.

2.1.2 불가리아 · 프랑스 · 영국 · 미국, 오픈소스 정책 지지에 합의[5]

2016년 12월 9일, 미국, 불가리아, 프랑스, 영국 4개 회원국은 오픈소스 정책 지지에 합의하였다. 이는 제4회 세계정상회의에서 오픈정부협력(OGP, Open Goverment Partnership)의 결과물인 ‘파리 선언’의 오픈소스 정책⁷⁾에 대한 지지에 동의한 것으로, 특히 프랑스 정부는 오픈소스 정책에 대한 첫 지지 표명이었다.

2.2 미국 표준화동향

2.2.1. NIST, 사이버보안 ‘복구’ 가이드라인 발표[6]

2016년 12월 22일, NIST는 사고처리 및 비상 계획과 같은 기존 NIST 복구 가이드를 통합하여 사이버보안 문제 발생 시 시스템 회복을 위한 ‘사이버보안 문제의 복구 가이드(Guide for Cybersecurity Event Recovery)⁸⁾’를 발표하였다.

2015년 美 백악관 관리예산처에서 발간한 ‘사이

5) ISO/IEC 27004:2016 원본: http://www.iso.org/iso/catalogue_detail?csnumber=64120

6) ISO/IEC 27001 원본: <http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fIEC%27001%3a2013>

7) 정책 원문: <https://paris-declaration.ogpsummit.org/topic/5820e48c2fd812b46ab9facc>

8) 가이드라인 원문: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf>

버 보안 전략 및 정보 계획(CSIP, Cybersecurity Strategy and Information Plan⁹⁾)’에서는 美연방 정부의 일관성 없는 사이버보안 대응 능력을 지적하며 개선기관에 이를 요청하였다. 2016년 12월 카스퍼스키 보안 게시판(Kaspersky Security Bulletin)¹⁰⁾에 따르면, 해커가 대가를 지불할 때까지 기관 데이터를 인질로 잡고 있는 랜섬웨어가 발생한 회사가 2016년 1분기에서 3분기 사이에 3배나 증가함을 발표하였다.

CSIP는 사이버보안에 약해진 시스템을 완전히 회복하기 위한 계획, 프로세스, 절차를 개발하고 구현하는 것을 ‘복구(recover)’로 정의하며, 이 ‘복구’는 백업에서 데이터를 복원하는 것처럼 간단할 수 있지만 더 복잡하고, 시스템을 단계적으로 온라인으로 가져올 수 있음을 설명하였다. 그러나 복구는 위험 관리 프로세스에서 중요한 부분임에도 미 연방정부 정책이나 표준, 가이드 어디에도 복구 접근법에 대한 언급이 없었다.

이번 사이버 보안 복구 가이드는 연방 및 기타 조직들이 사이버보안 문제가 발생했을 때 미리 기관의 포괄적 복구 계획을 수립할 수 있는 프로세스를 제공하며 데이터 유출과 랜섬웨어의 처리가 가능한 예를 제공한다. 또한, 복구 계획의 개발, 테스트, 개선에 대한 전술과 전략적 가이드를 제공하며, 해당 기관이 발생 가능한 사이버 보안 문제의 시나리오를 마련할 것을 권고하고 있다.

2.2.2 미 상무부, 사물인터넷 녹서(Green Paper) 발표[7]

2017년 1월 12일, 미국 상무부(Department of Commerce)는 사물인터넷 녹서(Green paper)를 발표¹¹⁾하였다. 이는 미국의 사물인터넷 기술과 관

련한 정부의 공식적 첫 발을 내딛는 것으로, 이해관계자들의 의견을 반영하여 2016년 4월 ‘사물인터넷 장점과 문제점, 그리고 기술 촉진을 위한 정부의 역할’이라는 발간물을 최종 발표하였다.

2.2.3 미 상무부, IoT 보안표준 분류에 착수[8]

2017년 2월 6일, 미국 상무부의 국가전기통신정보관리국(NTIA, National Telecommunications and Information Administration)은 기존 보안표준 분류 작업에 착수하기로 결정하였다.

이번 분류 작업의 궁극적 목적은 IoT의 소비자 인식과 이해가 날로 높아짐에 따라 IoT 기기 보안과 관련 장치 및 시스템을 제공하기 위함으로, ‘IoT’와 ‘사이버보안’의 공개적인 의견수렴에 대한 대응적 차원으로 미국 상무부와 NTIA에 다양한 이해관계자와의 자발적 협력 프로세스를 통해서 IoT 보안 문제 해결을 요청하였다.

이에, NTIA WG1는 기존 IoT 보안표준과 이니셔티브를 대상으로 IoT 기기와 인프라의 보안 패치 및 업그레이드 가능성에 대하여 조사·검토하고 있으며, NIST, IEEE 사물인터넷, 사물인터넷 컨소시엄, ISO 및 IEC 간의 협력과 그 노력을 평가할 예정이다.

2.3 중국 표준화 동향

2.3.1 중국, 사이버보안 및 데이터 프라이버시 국가표준 초안 발표[9]

2016년 12월 22일, 중국 표준개발위원회인 국가정보보안표준기술위원회(NISSTC, China’s National Information Security Standardization Technical Committee)는 사이버보안 및 데이터 프

9) 백악관 관리예산처의 ‘사이버 보안 전략 및 정보 계획(CSIP)’ 원문: <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf>

10) 카스퍼스키 보안 게시판: <https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/>

11) 녹서 원문: https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

라이버시와 관련한 다음의 국가표준 초안 7개를 발표하였다.

- 정보 보안 기술 – 개인 정보 보안 규격
- 정보 보안 기술 – 사이버보안 분류 보호를 위한 구현 가이드
- 정보 보안 기술 – 빅데이터 서비스의 보안 기능 요구사항
- 정보 보안 기술 – 산업 제어 시스템의 보안 위험 평가 가이드
- 정보 보안 기술 – 산업적 제어 네트워크 모니터링을 위한 보안기술 요구사항 및 시험 평가 방법
- 정보 보안 기술 – 산업 제어 시스템 취약성 탐지를 위한 기술 요구사항 및 시험 평가 방법
- 정보 보안 기술 – 하드웨어 장치 보안의 테스트 및 평가 방법

3. 사실표준화기구의 최근 동향

3.1 IEEE, 인공지능 관련 윤리 지침 최초 발표[10]

2016년 12월 13일, IEEE는 최초로 윤리적 인공지능 시스템 개발 지침을 발표하였다.

이번 지침은 ‘윤리적 배열 설계: 인공지능과 자율시스템을 통해 인류 행복을 최우선으로 생각하는 비전(Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems)¹²⁾’이라는 제목으로, 기술자들이 자율적 창의성과 지능적 기술에 있어 윤리적 관점에 대해 생각하도록 권고하며, 추후 인공지능 제작에도 적용할 계획이다.

IEEE는 인공지능은 인류를 위한 ‘윤리적 설계’를 추구하여야 하나, 현재는 기술 산업에서 윤리의식 및 책임감의 부족으로 인권(human rights), 책임(responsibility), 투명성(transparency), 교육(education)에 관심을 기울여야 함을 주장하였다.

이번 지침은 인공지능이 인권을 보장하고, 투명하게 작동되며, 자동화된 결정이 어떻게 도출되는 것인지 설명할 수 있어야 한다는 원칙과 적절한 인간 규범과 가치의 시스템 내재화, 예상 가능한 차별 방지 및 신뢰성, 가치 판단 기준의 평가 등을 포함하고 있다. 또한, 알고리즘 동작을 감독하는 독립적 평가기관의 부족과 알고리즘 개발 시 블랙박스 컴포넌트를 사용하는 등 윤리적 인공지능에서 발생하는 문제점을 지적하였다.

3.2 IEEE, 지역 네트워크 연결 관련 IEEE 802.1Qbz™ 제정[11]

2016년 12월 1일, IEEE 및 IEEE-SA는 지역권 및 대도시권 지역망 표준인 IEEE 802.1Qbz™를 제정하였다. 이번 표준은 IEEE 802.11™의 미디어 연결 성 강화를 위하여 브리지 및 브리지 네트워크 수정(Bridges and Bridged Networks Amendment)에 대해 다루고 있다.

이번 신규 표준은 IEEE 802.11 미디어의 프로토콜과 세부 절차를 명시하고, 브리지 망 접근뿐만 아니라 브리지 망 내의 내부적 연결성 제공을 위한 IEEE 802.11 미디어의 목표 관리에 대해 기술하고 있다.

현재, 가정용 엔터테인먼트 시스템과 산업 제어 장비를 포함한 많은 신제품은 IEEE 802.11 무선 스테이션 성능과 유선 IEEE 802.3 이더넷 성능을 둘 다 지원하고 있다. 이에, IEEE 802.1Qbz은 네트워크 내부 매체와 네트워크 접근 제공 매체의 연결로서 다른 미디어를 동일 수준에서 지원하는 IEEE 802.11 미디어 통합에 대한 많은 수요를 반영하였다.

12) 원문 참조: http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf

3.3 국제가상현실협회(GVRA) 설립[12]

2016년 12월 8일, 삼성, 구글, HTC VIVE, 페이스북 Oculus, Acer Starbreeze, 소니인터렉티브엔터테인먼트는 국제 가상현실협회(GVRA, Global Virtual Reality Association)를 창설하였다. 해당 협회는 가상현실 산업의 성장을 촉진하기 위한 국제적 가상현실 헤드셋 관련 비영리기관으로, 세계 가상현실 이해관계자들과 산업적 노하우 공유를 지원할 계획이다.

3.4 Khronos 그룹, 가상현실(VR) 표준 이니셔티브 신설 [13]

2016년 11월 17일, Khronos 그룹은 가상현실(VR) 통합을 위한 표준화 협력체인 'Khronos VR 표준 이니셔티브(Khronos VR Standards initiative)'를 신설하였다.

가상현실(VR) 초기 단계에서는 동작(motion)과 제어(control)에 대한 다양한 콘텐츠와 표준 중에서 특정한 것을 선택해야 하는 많은 플랫폼, 솔루션들이 존재한다. 현재 스팀 VR(STEAM VR), 오클러스 리프트(Oculus Rift), OSVR, 데이드림(Daydream) 등 업체마다 각기 다른 VR 솔루션과 게임용 엔진 등의 다양한 API 사용으로 모든 VR 기기에 통합적으로 적용되는 단일 소프트웨어 개발이 어려운 상황으로, 이는 특정 VR 솔루션에 특화되어 개발되어야 하기 때문에 각각의 개발 비용이 발생하여 산업 성장을 제한하게 된다.

이에 크로노스(Khronos) 그룹은 다양한 VR기술의 표준화를 통해 호환이 가능한 가상현실 기기와 애플리케이션을 개발하는 'Khronos VR 표준 이니셔티브'를 신설하였고, 휴대용 VR 애플리케이션과 엔진들이 다른 하드웨어와 공급 장치 드라이버 간

인터페이스에 사용할 수 있게 하는 API 표준 개발을 위해 노력할 계획이다.

3.5 MICRON, 버스 인터페이스 표준 컨소시엄 (Xccela™) 발족[14]

2016년 12월 15일, 마이크론 테크놀로지(Micron Technology)¹³⁾는 Xccela 버스 인터페이스 표준 개발을 위한 Xccela™ 컨소시엄을 발족하였다.

Xccela™ 컨소시엄은 Xccela 버스 인터페이스를 휘발성 및 비휘발성 메모리와 기타 유형의 집적 회로(MCU, SoC, ADC 등)에 적합한 새로운 형식의 데이터 상호연결 및 데이터 통신 버스의 공개표준을 개발할 계획이다. 마이크론은 버스(Bus) 및 각종 지원 장치를 사용한 애플리케이션의 가속 성능 개선을 위하여 이전에 발표한 XTRMFlash™와 XTRMBus™의 명칭을 Xccela™ Flash와 Xccela™ Bus로 변경하였다.

이번 컨소시엄 창립멤버는 Micron, 윈본드(Winbond, 대만 전자기업), 기가디바이스(GigaDevice, 중국 플래시 메모리 제조업체), AP Memory Technology(대만 메모리 제조업체) 등으로, 현재 다른 회원사와 협력하여 Xccela 버스 호환 메모리, 컨트롤러, ASIC, SoC 및 다른 장치 개발에 노력할 것이다.

오늘날 스마트폰 등장으로 그래픽 사용자 인터페이스, 펌웨어, 소프트웨어 실행 등에 데이터 처리 및 저장을 위한 고성능 버스가 필요하다. 이에 Xccela은 현재의 버스 인터페이스가 고성능의 하이핀 카운트 병렬 인터페이스(high pin-count parallel interface) 또는 직렬 인터페이스의 작은 활성 신호 풋프린트(small active signal footprint of a serial interface)와 같이 성능과 풋 프린트 간의 절충이 요

13) 마이크론 테크놀로지(Micron Technology): 1978년 5월 미국 아이아호 보이시에 설립된 DRAM, NAND, NOR 플래시 등 첨단 반도체 메모리 시스템 개발 기업임.
※출처: www.micron.com

구되어 왔다.

Xccela 버스는 성능 개선과 작은 신호 카운트를 결합한 차세대 버스로, 첫 반복 작업에서 불과 11개 활성 버스 신호를 이용하여 최대 400MB/s(3.2Gbps)의 데이터 전송을 촉진하여 단순한 시스템 설계만으로도 빠른 데이터 전송을 가능케 한다.



[참고문헌]

- [1] <http://www.itu.int/en/mediacentre/Pages/2016-PR61.aspx>
- [2] http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref2146
- [3] https://www.ansi.org/news_publications/
- [4] <http://www.etsi.org/news-events/news/>
- [5] <https://joinup.ec.europa.eu/community/osor/news>
- [6] <https://www.nist.gov/news-events/news/2016/12/>
- [7] <http://www.theregister.co.uk/2017/01/13/>
- [8] https://www.ansi.org/news_publications/
- [9] <http://www.natlawreview.com/article/>
- [10] http://standards.ieee.org/news/2016/ethically_aligned_design.html
- [11] http://standards.ieee.org/news/2016/ieee_802.1qbz-2016.html
- [12] <http://www.cbronline.com/news/internet-of-things/>
- [13] <http://www.anandtech.com/show/10892/>
- [14] <https://globenewswire.com/news-release/2016/12/15/897990/en/>

[주요 용어 풀이]

• 랜섬웨어(ransomware): 미국에서 발견된 스파이웨어 등 신종 악성 프로그램. 컴퓨터 사용자의 문서를 복모로 잡고 돈을 요구한다고 해서 '랜섬(ransom)'이란 수식어가 붙었다. 인터넷 사용자의 컴퓨터에 잡입해 내부 문서나 스프레드 시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들거나 첨부된 이메일 주소로 접속해 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다면 금품을 요구하기도 한다.

• 자율시스템(Autonomous System): 동일 라우팅 정책으로 하나의 관리자에 의하여 운영 관리되는 라우터와 부분 통신망의 집합체로, 흔히 인터넷(internet)은 자율 시스템(AS)들의 집합체라고 볼 수 있다. 자율 시스템(AS)으로 네트워크를 분리하는 이유는 라우팅 정책의 독립성, 보안 유지, 운영관리의 국지화, 라우팅 트래픽량 최소화 등이다. 인터넷 회선 접속 사업자가 상호 접속해서 구성한 인터넷 기간 망에서는 자율 시스템(AS)끼리의 통신을 어떤 경로를 거쳐서 실현할 것인지를 결정할 필요가 있다. 각 AS에서는 AS 내부에서 발신하는 통신이나 약간 떨어진 곳의 AS가 발신한 통신을 인접한 AS를 거쳐서 실행하는 것을 경로 결정표에 기입해둔다.

• 크로노스 그룹(Khronos Group): 응용프로그래밍 인터페이스(API)의 표준을 제정하는 비영리 표준화 단체로, 3D 그래픽과 동영상, 이미지 등에 사용되는 멀티미디어 콘텐츠가 다양한 디지털 기기에서 구현될 수 있도록 로열티 제한이 없는 오픈 표준 API를 제공한다.

• 가상현실(Virtual Reality, VR): 인간의 상상에 따른 공간과 사물을 컴퓨터에서 가상으로 만들어, 시각, 청각, 촉각을 비롯한 인간 오감을 활용한 작용으로 현실 세계에서는 직접 경험하지 못하는 상황을 아바타를 통해 간접으로 체험할 수 있도록 하는 기술이다.