해외 ICT 표준화 동향

2017. 01

3st week

목차

* 게시물 보기

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

TTA 한국정보통신기술협회 Telecommunications Technology Association

1. IEEE, 자율 시스템(AS) 투명성 표준 프로젝트 착수

(IEEE Announces Standards Development Project to Address Transparency of Autonomous Systems)

보도날짜 2016.12.15.

출 처 IEEE

사 이 트 http://standards.ieee.org/news/2016/ieee_p7001.html
* 참고: https://standards.ieee.org/develop/project/7001.html

■ 2016년 12월 15일, IEEE와 IEEE-SA는 자율시스템(AS, autonomous systems)[1] 설계 및 개발의 투명성 보장 프로젝트(IEEE P7001™) 착수 발표

- IEEE P7001는 지능 기술과 자율성 개발에 있어 도덕적 우선순위 고려에 대한 최근 IEEE 발간물인 "윤리적 디자인: 인공지능과 지율시스템에서 인간 행복을 최우선으로 하는 비전"*에 따라 착수되었음

  * Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems (출처:http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html)

- 위 발간물과 IEEE P7001은 인공지능과 자율시스템의 윤리적 고려사항을 위한 IEEE 국제적 이니셔티브의 작업에서 부터 시작되었으며, IEEE P7001은 공공 안전보장과 신뢰 구축을 목표로 자율시스템의 책임성과 진행 추적성(traceability)을 제공함

■ 자율 시스템의 투명성과 투명성 보장의 이유는 다음과 같음[2]

- '투명성'이란 시스템이 무엇을 하고 왜 해야 하는지 사용자가 이해하는 방식을 간략히 제공함으로써 시스템에 대한 신뢰감을 구축토록 함. 예로 케어 로봇의 투명성이란 사용자가 다른 상황에서 로봇이 무엇을 할지 빨리 이해할 수 있는 것을 의미하며, 반면에 로봇이 예상치 못한 무슨 행동을 해야 한다면 사용자는 로봇에게 '왜 그랬는가?'라고 물어볼 수 있어야 함

- AS 투명성 검증과 승인을 위해서는 시스템 프로세스를 정밀하게 조사해야 하며, 사고 발생 시 AS는 사고 조사관에게 사고로 이어지는 내부과정을 추적할 수 있을 정도로 투명해야 함

---

1) 자율시스템(Autonomous System): 동일한 라우팅 정책으로 하나의 관리자에 의하여 운용 관리되는 라우터와 부분 통신망의 집합체임. 흔히 인터넷(internet)은 자율 시스템(AS)들의 집합체라고 볼수 있다. 자율 시스템(AS)으로 네트워크를 분리하는 이유는 라우팅 정책의 독립성, 보안 유지, 운용관리의 국지화, 라우팅 트래픽량의 최소화 등이다. 인터넷 회선 접속 사업자가 상호 접속해서 구성한 인터넷 기간망에서는 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 기입해 둔다. (출처: 정보통신용어사전, http://terms.tta.or.kr)

2) P7001 Working Group(작업반) 홈페이지: https://standards.ieee.org/develop/project/7001.html

- 증거를 요구할 수 있는 변호사 또는 다른 전문 증인들은 그들의 증거를 논증하기 위해 투명성을 필요로 하며, 운전자 없는 자동차와 같은 파괴적인 기술의 경우, 기술에 대한 대중의 신뢰를 구축하기 위해서 사회에서 폭넓게 받아들일 수 있는 일정 수준의 투명성이 필요함

■ 이번 IEEE P7001 표준은 메커니즘 개발 중 자체적인 투명성 평가에 대한 가이드를 제공하고, 설계자를 위하여 항공 데이터 기록장치, 블랙박스와 같은 센서 및 내부 상태 데이터의 안전한 저장을 필요로 하는 메커니즘에 더욱 개선된 투명성을 제안함

- 이번 표준은 자율시스템이 객관적으로 평가하고 준수 수준을 스스로 결정할 수 있도록 하기 위하여, 측정 가능하고 테스트 가능한 수준의 투명성을 설명하고 있으며, 달성 가능한 최고 수준까지의 최소 범위를 정하는 투명성 수준을 정의함

■ IEEE-SA 사무국장 콘스탄티노스 카라챌리오스(Konstantinos Karachalios)는 다음과 같이 언급함

- 이번 IEEE P7001의 작업은 자율시스템 운영이 다양한 이해관계자들에게 투명하게 이루어지도록 보장하는 표준을 개발하는 것으로, 투명성은 자율시스템의 성공적 구현의 핵심적인 부분으로 이번 IEEE P7001은 자율시스템이 대중의 신뢰를 얻고 추적성 제고에 도움이 될 것으로, 설계자가 개발 프로세스 초기에 투명성 개선과 자체적으로 평가 할 수 있도록 지원할 것임

2. NIST, 사이버보안 '복구'에 대한 가이드라인 발표

(NIST Guide Provides Way to Tackle Cybersecurity Incidents with Recovery Plan, Playbook

보도날짜 2016.12.22.

출 처 NIST

사 이 트 https://www.nist.gov/news-events/news/2016/12/nist-guide-provides-way-tackle-cybersecurity-incidents-recovery-plan

■ 2016년 12월 22일, NIST는 사이버 보안 문제 발생 시 시스템 회복을 위한 '사이버 보안 문제 복구 가이드(Guide for Cybersecurity Event Recovery)*'를 발표함

* http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

- NIST는 사고 처리 및 비상 계획과 같은 기존 NIST 복구 가이드를 통합하여 '사이버 보안 문제 복구 가이드'를 마련함

■ 2015년 美백악관 관리 예산처에서 발간한 '사이버 보안 전략 및 정보 계획(CSIP, Cybersecurity Strategy and Information Plan)[1]'에서는 美연방정부에서 일관성 없는 사이버보안 대응 능력을 지적하며 이를 개선할 기관을 요청함

- 2016년 12월 카스퍼스키 보안 게시판(Kaspersky Security Bulletin)[2]에 따르면, 해커가 대가 지불까지 기관 데이터를 인질로 잡고 있는 랜섬웨어[3] 사건이 발생한 회사만 '16년 1분기에서 3분기 사이에 3배나 증가함

- CSIP는 사이버보안 사건 내 약해진 시스템을 완전히 회복하기 위한 계획, 프로세스, 절차를 개발하고 구현하는 것을 "복구(recover)"로 정의하며, 복구는 백업에서 데이터를 복원하는 것처럼 간단할 수 있지만 일반적으로 더 복잡하고, 시스템을 단계적으로 온라인으로 가져올 수 있음

- 복구는 위험 관리 프로세스에서 중요한 부분이나 아직 美연방정부의 정책이나 표준 및 가이드 어디에도 복구 접근법에 대한 언급이 없음

---

1) 백악관 관리예산처
: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

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

3) 랜섬웨어(ransomware) : 미국에서 발견된 스파이웨어 등의 신종 악성 프로그램. 컴퓨터 사용자의 문서를 볼모로 잡고 돈을 요구한다고 해서 '랜섬(ransom)'이란 수식어가 붙었다. 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레드 시트, 그림 파일 등을 제멋대로 암호화해 열지 못하도록 만들거나 첨부된 이메일 주소로 접촉해 돈을 보내 주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하기도 한다.
(출처: 정보통신용어사전, http://terms.tta.or.kr)

■ 이번 사이버 보안 복구 가이드는 연방 및 기타 조직이 사이버보안 문제가 발생했을 때 미리 기관 소유의 포괄적인 복구 계획을 수립할 수 있는 프로세스를 제공하며 데이터 유출과 랜섬웨어의 처리가 가능한 각본의 예를 제공함

- 또한, 해당 기관이 복구 계획의 개발, 테스트, 개선에 대한 전술과 전략적 가이드를 제공하며, 발생 가능한 사이버 보안 문제의 시나리오를 마련할 것을 요청함

기타 소식

국제가상현실협회(GVRA) 설립

▶ 출처 : http://www.cbronline.com/news/internet-of-things/smart-technology/global-virtual-reality-association-vr-standards/ (2016.12.8)

○ 2016월 12월 8일, 삼성, 구글, HTC VIVE, 페이스북 Oculus, Acer Starbreeze, 소니인터렉티브엔터테인먼트는 국제 가상현실협회(GVRA, Global Virtual Reality Association)를 창설함

- 해당 협회는 가상현실 산업의 성장 촉진을 위한 국제적 가상현실 헤드셋 관련 비영리기관으로, 세계 가상현실 이해관계자들과 산업적 노하우 공유를 지원할 것임

중국, 사이버보안 및 데이터 개인 국가표준 초안

▶ 출처 : http://www.natlawreview.com/article/china-seeks-comment-seven-draft-cybersecurity-and-data-privacy-national-standards (2016.12.22)

○ 2016년 12월 22일, 중국 표준개발위원회인 국가정보보안표준기술위원회(NISSTC, China's National Information Security Standardization Technical Committee)는 사이버보안 및 데이터 프라이버시와 관련한 다음의 국가표준 7개 초안을 발표함

* 정보 보안 기술 – 개인 정보 보안 규격
* 정보 보안 기술 – 사이버 보안 분류 보호를 위한 구현 가이드
* 정보 보안 기술 – 빅 데이터 서비스의 보안 기능 요구사항
* 정보 보안 기술 – 산업 제어 시스템의 보안위험 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 – 하드카피 장치보안의 테스트 및 평가 방법