



2020년 10월 다섯째주

해외 ICT 표준화 동향

목차

본문 20.10.20 EU, 디지털 운영 탄력성 규제 제안

20.09.26 가나 NITA, ICT 표준과 가이드라인 논의 포럼 개최

20.10.16 StandICT.Eu, 유럽중소기업표준(SBS)과 양해각서(MoU) 체결

단신

20.10.20 미국 CSC, 신뢰할 수 있는 ICT 공급망 구축 전략 제안

20.10.23 미국 NIST, 핵심 인프라 보호를 위한 사이버보안 지침 공개

※ 게시물 보기

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

1. EU, 디지털 운영 탄력성 규제 제안

The EU proposed digital operational resilience regulation

보도날짜 : 20.10.20.

출 처 : <https://www.lexology.com/library/detail.aspx?g=93ef55a8-db8f-4fc1-880c-2a903b4b9fab>

- EC(유럽연합집행위원회)는 EU의 금융 서비스 부문 내에서 디지털 운영 회복성에 관한 규정안을 발표. 이를 통해 ICT 및 보안 리스크 관리와 관련한 기존 지침을 대체·조정하고, 주요 ICT 서비스 사업자를 유럽 감독 당국의 감독 범위에 직접 포함시킬 계획
- EC는 2020년 9월 24일, 디지털 금융의 개발을 촉진하고 리스크를 완화하기 위해 광범위한 디지털 금융 전략 패키지의 일환으로 디지털 운용 탄력성(DORA: Digital Operational Resilience Act) 규정 초안을 발행
 - '디지털 운용 탄력성'이란, 서드파티 ICT 서비스 제공자를 통해 금융회사의 금융서비스에 대한 지속적인 제공과 품질을 지원하는 정보시스템을 제공함으로써 네트워크 보안에 필요한 ICT 관련 역량을 직접 또는 간접적으로 보장하여 기술적 관점에서 운용 무결성을 구축, 보장, 검토할 수 있는 역량을 의미
 - 기존 금융 서비스 분야의 ICT 리스크 관리와 관련된 현재 EU 요구사항은 다양한 금융 서비스 법률(예: CRD IV, PSD2, Solvency II, EMIR 및 MIFID)과 유럽 은행 당국(EBA), 유럽 보험 및 직업 연금 기관(EIOPA) 및 유럽 증권 시장 당국(ESMA)에서 별도로 발행한 가이드라인에 산재되어 있음. 따라서 해당하는 요구사항은 재무 하위 항목마다 상이함. 특히 은행 서비스 및 보험 내의 기업들은 이미 외부 서비스 제공업체 및 ICT 위험 관리와 관련된 요구사항에 직면해 있는 반면, 감사 회사 및 무역 저장소와 같은 기업들은 현재 디지털 운영 리스크를 부분적으로 포착하는 광범위한 위험 관리 요구사항만 적용받고 있는 상황임
 - 발표된 EC의 규제 제안은 기존의 법률을 수정하고 EU 금융 시스템 전체에 걸쳐 높은 공통 기준을 설정하기 위해 의무 규정을 무시하는 단일 세트를 제시. 이 규칙은 시스템 유지 보수, 복원력 테스트, 비즈니스 연속성 및 재해 복구, 사고 보고 및 타사 위험 보고와 같은 디지털 운영 탄력성과 관련된 다양한 측면을 다룸
 - 본 규정의 핵심은 EBA, EIOPA 및 ESMA의 감독 및 감독 범위 내에서 "중요하다"고 간주되는 주요 기술의 서비스 제공업체를 EU 금융 시스템에 파견할 것을 제안한다는 점임. DORA 규정으로 인해 당국은 광범위한 조사 권한을 갖게 될 것이며, 서비스 제공업체가 당국의 요청에 따르지 않을 경우 중징계를 부과할 수 있음
- DORA는 유럽 사이버보안청(ENISA)과 협의하여 ESA에 적절한 보안 정책이나 프로토콜, ICT 비즈니스 연속성/재해 복구 계획의 구성요소를 명시하는 등 ICT 리스크 관리를 목적으로 하는 여러 규제 기술 표준을 개발할 것을 의무화
- 곧 유럽 의회와 EU 이사회가 입법안을 검토할 예정이며, 본문의 최종본은 입법 절차가 끝날 때쯤 현재의 제안과 차이가 있을 수 있음

1. 20.09.26. 가나 NITA, ICT 표준과 가이드라인 논의 포럼 개최

- ▷ 원문제목 : NITA To Hold Virtual ICT Stakeholders Conference On Standards
- ▷ 원문링크 : <https://www.peacefmonline.com/pages/local/news/202009/428228.php>
- 가나 NITA(국가정보기술국)는 9월 28일, 정보통신기술(ICT) 분야내 이해관계자들을 대상으로 온라인 포럼을 개최하여 그동안 개발한 ICT 표준과 가이드라인에 대해 논의
 - 가나 부처 및 기관의 ICT 전문가와 민간 부문 ICT 전문가가 참석한 본 컨퍼런스는 "성공적인 디지털화 의제를 위한 규제 준수 심화"를 주제로 진행
- NITA는 ICT 표준 및 정책 지침을 세부적으로 조정하기 위한 의견과 아이디어를 요청하기 위해 이번 컨퍼런스를 개최하였다고 밝혔으며, 이번 컨퍼런스가 규제 이니셔티브의 진도 및 다양한 이슈에 관한 정보를 이해관계자와 대중에게 전파하는 매개체 역할을 하였다고 발표
- NITA는 현재 가나의 공공 부문과 민간 부문 모두에서 ICT의 도입, 구축, 구성 및 구현에 있어 표준의 적용에 관한 노력을 이행중

2. 20.10.16. StandICT.Eu, 유럽중소기업표준(SBS)과 양해각서(MoU) 체결

- ▷ 원문제목 : SBS and StandICT.eu 2023 sign a Memorandum of Understanding (MoU) to strengthen SME presence in the international standardisation landscape for ICT
- ▷ 원문링크 : <https://cordis.europa.eu/article/id/422536-sbs-and-standict-eu-2023-sign-a-memorandum-of-understanding-mou-to-strengthen-sme-presence-in>
- 유럽의 디지털 단일 시장(DSM, Digital Single Market)은 주요 ICT 분야의 광범위한 산업 및 서비스 분야에서 유럽의 경쟁력을 높이는 것을 목표로 하고 있으며, 이러한 목표를 수행하기 위해서는 ICT 표준화에 대한 지원과 유럽 중소기업(SME)의 표준 입안에 기여할 수 있는 올바른 도구를 제공하는 것이 필요
- 유럽의 ICT 표준화 전문가 지원기구 StandICT.Eu 2023은 유럽중소기업표준(SBS)과 함께 보다 효과적인 표준의 시장진출을 목표로하는 양해각서(MoU)를 체결
 - StandICT.eu 2023의 목표는 두 가지이며, 첫 번째 목표는 5G 및 고정 네트워크, IoT, 사이버 보안, 데이터, 클라우드 컴퓨팅, 양자 기술, AI, 블록체인, Industry 4.0 ITS/자동 운전, 핀테크/금융 서비스 및 eHealth 등과 같은 주제를 다루는 국제 표준화 개발 조직 워킹 그룹에 참여하기 위한 일련의 open calls를 통해 유럽 ICT 전문가에게 자금을 지원하는 것임.

두 번째 목표는 유럽 ICT 표준화 전망대 내에 표준화 생태계를 조성하여 유럽의 경쟁력을 높이는 것임. 궁극적으로 이 프로젝트는 교육 이니셔티브와 훈련을 통해 "차세대 유럽 표준 전문가"를 형성하는 데 기여할 것으로 예상

- SBS는 21개 중소기업 회원사를 통해 1,200만 이상의 중소기업을 대표하고 있음. 중소기업간 표준의 중요성에 대한 경각심을 높이고 표준화 과정에 대한 이해를 대변하는 것을 목적으로 함. 유럽 및 국제 수준에서 서로 다른 기술 위원회의 SME 전문가를 임명하여 이러한 목적을 수행하며, 또한 SBS는 소규모 및 중소기업의 요구를 고려하여 보다 많은 SME 호환 표준을 개발하기 위한 표준 제조업체를 지원하기 위해 최근 표준에 대한 SME 호환성 테스트를 개시
- 두 기관의 MoU의 서명은 글로벌 수준에서 ICT 영역의 표준화에 대한 유럽 중소기업들의 이해관계를 보다 강력하게 대변하는 데 도움이 될 것으로 예상

3. 20.10.20. 미국 CSC, 신뢰할 수 있는 ICT 공급망 구축 전략 제안

- ▷ 원문제목 : Cyberspace Solarium Commission Proposes Strategy to Create Trusted ICT Supply Chains
- ▷ 원문링크 : <https://www.govconwire.com/2020/10/cyberspace-solarium-commission-proposes-strategy-to-create-trusted-ict-supply-chains/>

- 미국 사이버스페이스 솔라리움 위원회(CSC, Cyberspace Solarium Commission)는 중대한 결과를 초래하는 사이버 공격으로부터 사이버 공간에서 미국을 방어하기 위한 전략적 접근방식에 대한 합의를 개발하기 위해 2019년 국방수권법에 설립. 완성된 보고서는 2020년 3월 11일에 대중에 공개됨
- CSC는 10월 20일 중요한 정보통신 기술에 대한 신뢰할 수 있는 공급망을 구축하기 위한 5개 핵심 전략을 제시하는 백서를 발표
 - 이 전략은 미국이 민관 협력과 정부 평가를 통해 핵심 기술과 장비를 파악하고, 가능한 최소의 제조 능력을 보장하며, 정보 공유, 제품 테스트 및 더 나은 인텔리전스를 통해 공급망을 위협으로부터 보호하고, 국내 시장을 활성화 및 글로벌 경쟁력 보장을 요구
 - 본 문서는 ICT 공급망 확보를 위한 5가지 핵심 권고안을 제시하며, 첫 번째 권고안은 집행부가 ICT 산업 기반 전략을 수립하고 이행하도록 의회가 지시할 것을 요구
 - 본 문서는 대통령이 선도기관을 지정해 정부와 민간 공급망 관리 이니셔티브를 조정하고 국가전략으로 통합할 것을 권고

- 의회는 국방, 국무, 상무부와 협력하여 국토안보부에 정부 검토와 산업 협의를 통해 ICT 및 관련 자료를 파악하도록 명령하고, 경제 클러스터링에 적합한 지역성에 대한 실행가능성 연구를 상무부에 지시할 예정
- 연방통신위원회는 5G 인프라 투자를 상호운용 가능한 개방형 표준과 연계하고 미국방부(DoD) 및 National Telecommunications and Information Agency와 협력하여 더 많은 중간 대역 주파수의 출시를 촉진하여 견고한 국내 통신 시장을 구축할 수 있도록 지원할 예정

4. 20.10.23. 미국 NIST, 핵심 인프라 보호를 위한 사이버보안 지침 공개

- ▷ 원문제목 : Safeguarding Critical Infrastructure: NIST Releases Draft Cybersecurity Guidance, Develops GPS-Free Backup for Timing Systems
- ▷ 원문링크 : <https://www.nist.gov/news-events/news/2020/10/safeguarding-critical-infrastructure-nist-releases-draft-cybersecurity>

- 미국 국립표준기술연구소(NIST)는 국가의 핵심 인프라 보호를 위해 종합위성항법(PNT, Positioning, Navigation and Timing) 데이터를 사용하는 위성 위치 확인 시스템(GPS)과 같은 핵심 기술에 사이버 보안 프레임워크를 적용하기 위한 지침 초안을 작성. 이러한 사이버 보안 지침은 PNT 데이터에 의존하는 시스템을 보호하기 위한 최근 행정명령을 구현하기 위한 NIST의 노력의 일환으로 시작되었으며 GPS와 독립적인 탄력적인 시간 계측 신호를 제공하고 테스트하기 위해 개발됨
- NIST의 새로운 사이버 보안 프로파일은 현대적인 금융, 운송, 에너지 및 기타 중요한 인프라를 뒷받침하는 시스템을 포함하여 종합위성항법(PNT) 데이터를 사용하는 시스템에 대한 리스크를 완화하도록 설계됨. 지상 또는 공간 기반 PNT 소스 신호 생성기와 제공자(위성 등)가 포함되지 않지만, 여전히 광범위한 기술을 다룸
- "PNT(Positioning, Navigation and Timing) 서비스의 책임 있는 사용을 위한 사이버 보안 프로파일"(NISTIR 8323)으로 공식 명명된 본 신규 지침은 금융, 운송, 에너지 및 기타 경제 부문을 뒷받침하는 시스템을 포함한 국가 및 경제 보안에 중요한 시스템을 위협에 빠뜨릴 수 있는 사이버 보안 위험을 완화하기 위해 고안됨
- 해당 프로파일은 조직이 다음 4가지 작업을 수행하는데 기여
 - PNT 데이터를 사용하거나 소스 신호를 기반으로 데이터를 전파하는 시스템 식별
 - GPS 신호와 같은 PNT 데이터 소스 식별
 - PNT 서비스를 사용하는 시스템의 교란 및 조작 탐지
 - PNT 서비스의 책임 있는 사용 및 발생하는 리스크 관리