

해외 ICT 표준화 동향

2016. 4

3rd Week

목 차

■ 본문

1. ITU, 2016년도 ICT 규제보고서 발간
2. NIST, 암호화 관련 표준 및 지침 개발 절차 표준 제정

한국정보통신기술협회
Telecommunications Technology Association

게시물 보기 : TTA 홈페이지 ▷ 자료마당 ▷ TTA간행물 ▷ 표준화 이슈 및 해외 동향

1. ITU, 2016년도 ICT 규제보고서 발간

(Trends in Telecommunication Reform 2016: new edition of ITU's flagship ICT regulatory report)

보도날짜 2016.04.05.

출 처 ITU

사 이 트 http://www.itu.int/net/pressoffice/press_releases/2016/12.aspx#.VwdDbqSLSUI

- 2016년 4월, ITU가 매년 발간하는 ICT 규제보고서(2016년 정보통신개혁 동향:Trends in Telecommunication Reform 2016)가 발간됨

- 이번 보고서는 5G 모바일에서부터 사물인터넷(IoT)에 이르는 차세대 데이터 집약 기술의 기반을 위한 네트워크 운영자들의 준비 및 서비스 확산, 융합 플랫폼에 대한 ICT 규제자들이 당면한 문제에 대해 분석함



<출처: ITU 홈페이지>

- 본 보고서는 경쟁과 혁신에 필수적인 '공평한 경쟁의 장'을 위한 규제문제를 강조하고 있음

- '디지털 기회 획득을 위한 규제 인센티브 검토(exploring regulatory incentives to achieve digital opportunities)'라는 주제로, 시장성장 촉진과 동시에 소비자 권리 보호와 신흥 업체를 격려하는 유연하고 기술 중립적인 규제 원칙을 강조함

- 2016년 보고서의 주요 내용 요약

① 광대역 투자(Broadband investment)

- 2014년~2019년까지 섬유 인프라에 대한 설비 투자가 1,442억 달러 이상 예상
- 전세계 40여개 사업자가 LTE-A 구축을 시작했거나 준비 중임(이 중 선진국 88%)
- 소비자 데이터 소비의 증가가 Wi-Fi 투자를 촉진할 것임
- 점점 더 많은 現운영자와 新경쟁자, 그리고 금융업자는 광대역 네트워크 투자를 위한 대체 자금 조달을 위해 노력 중
- 통신 인프라에 투자하지 않는 헤지펀드 또는 법인 조차 광대역 인프라에 투자

② 네트워크 공유(Network Sharing)

- 네트워크 범위의 경쟁 차별화가 심화되면, 운영자들은 네트워크 공유를 통해 인프라 투자 전환 및 혁신적 서비스 개발을 위한 네트워크 통합이 필요함
- 정부는 현재 전용회선(dedicated basis) 기준으로 스펙트럼을 할당하며, 新

DSA(동적 스펙트럼 접속) 기술은 기기가 특정 지리적 영역 및 특정 시간대에 사용되지 못했던 곳의 스펙트럼을 사용할 수 있게 함

- 네트워크 공유는 경쟁 강도 감소, 가격 담합 및 정보 공유 가능성, 서비스 기반 경쟁자의 선택권 감소와 같은 위험도 함께 지니고 있음

③ 사물인터넷(IoT)

- 모바일 산업협회(GSMA)는 M2M 연결이 2020년까지 10~20억개가 될 것으로 예측하며, 이는 2019년까지 세계 경제에 1조 7천 달러 가치에 달한 것임
- 간단한 IoT 기술(수동형 RFID 태깅)은 이미 판매가 시작되었고, NFC(근거리통신)도 신형 스마트폰에 포함되어 무선 결제 애플리케이션 등을 가능케 함
- IoT 표준은 다양한 목적과 요구를 가진 여러 이해관계자 및 애플리케이션에 사용되고 있어, 서로 다른 표준 프레임워크의 통합이 요구됨
- IoT가 유비쿼터스 기술이 되기 위해서는 태그, 센서, 통신 시스템의 비용 감소 필요가 있고, 접근이 쉬워야 함
- 수천 개의 센서, 기기, 리더기를 포함하는 대규모 시스템에 있어 높은 수준의 신뢰도와 보안이 요구됨

④ 상호운용성(Interoperability)

- "상호운용성"이라는 개념은 기술, 데이터, 사람, 기관의 4개 주요 수준을 함축한 것으로, 시스템들은 기술의 상호연결을 위한 기회 제공, 상호연결이 가능한 시스템과 서비스 유형의 개방 향상, 다양한 데이터 지원, 상호연결 활용의 용이성 향상을 통해 상호운용성을 향상시킬 수 있음
- 상호운용성은 시스템 개발 기회를 증가시키는데, 접속지점이 많은 시스템은 더 많은 종류의 시스템을 연결시킬 수 있고 제한없이 데이터를 처리할 수 있으며, 잠재적 공격 벡터(vector)를 증가시키고, 바이러스 등이 데이터를 이용하거나 불량 코드를 삽입하기 쉽게 만드는 등 점점 더 많은 상호운용성 단계가 사용자의 선택 및 자율성을 강화함
- 상호운용성은 그 자체가 끝이 아니며 반드시 극대화할 필요는 없고, 대신 민간 사업자 및 규제자는 그들의 목표를 달성하기 위해 필요한 상호운용성 수준을 최적화해야 함

2. NIST, 암호화 관련 표준 및 지침 개발 절차 표준 제정

(NIST Releases New Document on its Cryptographic Standards and Guidelines Process)

보도날짜 2016.03.31

출 처 NIST

사 이 트 <http://www.nist.gov/itl/csd/nist-releases-new-document-on-its-cryptographic-standards-and-guidelines-process.cfm>

- 2016년 3월 31일, 미국 연방표준기술국(NIST)은 '암호화 표준 및 지침 개발 방법(NIST Cryptographic Standards and Guidelines Development Process, NISTIR 7977)' 제정을 발표함
 - 본 표준은 암호화 개발 절차에 폭넓은 참여와 이해를 높이기 위한 NIST의 노력으로써, 특정 형태의 데이터를 저장하고 전송할 수 있는 기술을 통해 의도된 수신인만이 데이터를 읽거나 진행할 수 있음
 - 2013년 11월, 암호화 표준과 지침 개발에 대한 프로세스를 검토하였으며, 2014년 2월, 공개 의견수렴을 통한 표준 초안이 제정되었고, 검토 전문가 독자 패널(조사위원회, independent panel)이 소집되었음
 - * 2014년 7월 패널 보고서 발표, 2015년 1월 공개 의견수렴을 통한 최종 표준을 NIST 홈페이지 확인 가능 (<http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf>)
 - NIST 사이버보안 최고 감독관이자 사이버보안 관련 정보 기술 연구소 소장인 도나 도슨(Donna Dodson)은 NIST의 목표는 널리 수용되고 신뢰가는 효과적 암호화 표준 및 지침을 개발하는 것으로, 해당 표준 작업은 공공 및 민간 부문을 모두 아우르는 국제적 접근이 될 것이라 언급함
- 해당 표준은 투명성, 개방성, 균형, 기술 장점 및 글로벌 수용 등을 포함한 강력한 암호화를 위한 NIST 노력 지침의 9개 원칙을 포함함
 - 9개 원칙 중 '글로벌 수용(global acceptability)'은 오늘날 상거래의 글로벌적 성격과 대중의 의견을 반영하여 추가되었음
 - 또한, 해당 표준은 NIST가 발행한 다른 형태의 암호화 간행물에 대해 설명하고, 그러한 간행물들이 대중 의견을 받아들이는 방법, 간행물의 생명주기 관리 방법 등을 설명함

- NISTIR 7977은 또한, NIST가 최신 암호화 전문 지식에 관한 접근성을 갖는 것의 중요성을 강조하고 있을 뿐만 아니라 내부 능력을 강력하고 효과적으로 보장하고, 다양한 암호화 연구 단체와의 협력을 위해 노력하고 있음을 강조함
- NIST는 이번 표준의 주 사용자가 연방정부 및 공급업체라고 언급했지만, 암호화 표준, 지침, 도구, 매트릭스의 사용자 단체는 더욱 포괄적임
- NIST는 “강력한 암호화 사용을 공포하기 위한 NIST의 사명과 법 집행기관 및 기타 기관의 국가 안보 임무 사이의 의견충돌”이 있을 수 있으며, NIST는 독립적 결정 및 개방적이고 투명한 프로세스 사용을 위해 최선을 다 할 것임을 밝힘