14차시. 스마트시티와 사이버보안(1)

01. 사물인터넷과 사이버 보안

사물인터넷 사이버 보안의 이해

- 스마트홈, 스마트의료, 스마트카, Industry 4.0 등 사물인터넷 서비스가 일상과 생활 속으로 확산되면서 인터넷 기반으로 기존의 사이버 공간에서의 위협이 그대로 전이되고 확산될 우려가 높다. 특히 PC나 모바일기기 중심의 사이버환경과 달리 사물인터넷 환경은 보호대상, 주체, 방법 등에 있어 새로운 정보보호 방식으로 접근할 필요가 있다.
  - 보호대상: 기존의 PC나 모바일 기기를 넘어 가전, 자동차, 의료기기 등 주변의 모든 사물이 보호 대상
  - 보호 대상의 특성: 기존 기기가 보유한 고성능 및 고가용성의 환경 보다는 초경량 및 저전력 특성의 기기가 포함되기 때문에 기존의 백신이나 암호화 모듈 들이 탑재 되기어려운 특성을 지님
  - 보호 방법: 기존의 장비의 경우 별도의 보안 장비나 S/W와 연동하여 보호를 하였지만 실제 사물인터넷 환경에서는 컴퓨팅 자원의 한계로 인해 사물인터넷 제품의 설계 단계에서부터 보안을 내재화힐 필요가 있음
  - 피해 범위: 기존의 사이버 환경에서는 정보유출이나 금전피해에 그쳤지만 사물인터넷 환경에서는 시스템이 정지한다든지 생명에 까지 위험을 끼치는 피해가 발생할 수 있음

- 따라서 모든 사물 간의 상호연결이 확대되면서 보안위협도 확산되어 사물인터넷 제품 및 서비스의 기획 및 설계단계부터 정보보호를 고려해야만 한다. 또한 경량 암호 및 인증, 이기종 네트워크 보안관리, 프라이버시 보호 등 맞춤형 보안기술이 필요한 것이다.

사물인터넷의 보안 위협 및 사례

- 사실 IoT에 적용된 기술들은 아주 생소한 것들은 아니다. 네크워크 및 서버 보안은 이미 반복된 침해사고로 인해 보호대책에 관한 법/제도가 있으며 보안장비가 활발히 도입되고 있다. 하지만 사용자와 가장 밀접한 사물인터넷 기기는 아직 보안대책에 관한 어떠한 제도도 도입되지 않았다. 먼저 사물인터넷에서 발생한 위협 사례를 학습해보자.
  - CCTV를 통한 사생활 침해: 2016년 2월 전 세계 약 7만 3000여개의 CCTV가 해킹되어 인세캠이라는 사이트에 실시간으로 방송되는 사건이 발생. 인세캠은 직장, 학원, 헬스장, 음식점, 옷가게 등에 설치된 웹캠 영상을 해킹해 카메라 관리자나 촬영 대상자의 동의 없이 인터넷 상에 실시간 공개.

- 스마트 가전기기의 해킹 공격: 미국 보안서비스업체 '프루프포인트'에 따르면 2013년 12월 23일부터 2014년 1월 6일까지 하루에 3차례씩 10만 건 단위로 악성 이메일이 발송됐으며 공격 대상은 기업과 개인이었다. 그런데 이 사이버공격을 통해 발송된 악성 이메일 중 25%이상이 홈 네트워킹용 라우터, 인터넷에 연결된 멀티미디어센터, 스마트TV, 스마트 냉장고 등의 스마트 가전 제품이었다고 한다. TV와 냉장고 같은 가전제품이 대규모 스팸과 피싱 메일을 보낸 첫 사례로서 해커들이 인터넷에 연결된 가정의 스마트 제품들을 해킹하여 '좀비 가전'으로 만든 뒤 스팸 메일과 피싱 메일을 발송한 것이다.

IoT를 통한 해킹

- 스마트 자동차의 안전 위협: 텐센트 산하 보안 연구소인 킨시큐리티랩(Keen Security Lab)이 테슬라모터스의 전기자동차인 모델 S를 해킹하는데 성공했다. 원격에서 도어 잠금을 해제하거나 선루프를 열고 비상등을 점등하거나 전동시트를 원격으로 조작했다. 심지어 주행 중 트렁크를 열고 차선을 변경하고 급제동을 거는데 성공했다. 또한 2015년 7월 피아트-크라이슬러는 미국에서 판매한 차량 140만대를 리콜 했는데, 이는 해킹 위험 노출로 자동차 업체가 리콜을 실시한 첫 사례로 꼽히고 있다.

위의 사물인터넷 보안 위협 사례를 종합하여 보면 다음과 같이 사물인터넷에서의 보안 위협의 형태를 정리할 수 있다.

- 제조사의 이익 및 지적재산권 침해: 제조사가 심혈을 기울여 출시한 IoT 제품을 비용의 지불 없이 복제, 유통함으로써 제조사의 매출에 악영향을 끼치며 제품/제조사의 이미지 하락 유발. IoT 제품에 탑재된 펌웨어를 추출 및 분석으로 제조사의 지적 재산권까지 침해
- 서비스 무단 이용에 따른 비용 증가: 사물인터넷 제품의 위조를 통해 고객 대상 유상 서비스를 무단으로 사용함으로써, 제조사의 서비스 인프라 구축 및 운영 비용이 증가
- 인명사고 유발: 고객과 상호 작용을 하거나 안전을 제공하는 사물인터넷 제품의 경우, 오동작, 악의적 조작을 통해 고객에게 신체적/정신적인 피해를 유발할 수 있음. 인명 사고 발생 시 제조사의 대한 책임 문제 발생으로 이미지 하락과 함께 배상 및 보상 비용의 발생이 추가됨. 예를 들어 심박기를 원격으로 조정하여 심박기 신호정보 위·변조를 통한 전류량 과잉공급으로 환자를 사망에 이르게 할 수 있다.

- 프라이버시 침해: 사물인터넷 제품의 통신을 도청하거나 악성 코드를 이용하여 사물인터넷 제품이 수집한 민감한 정보를 몰래 탈취함으로써, 고객의 프라이버시를 침해. 개인정보 탈취사고 발생 시에는 제조사 책임에 따른 이미지 하락과 함께 배상 및 보상 비용이 발생

- 다른 공격의 경유지로 악용: 사물인터넷 제품의 보안 취약점을 이용한 제어권을 탈취하여 악성 코드 삽입 등을 통한 DDoS 등 다른 공격의 경유지로 악용. 이 경우 대규모 공격 경유지 이용에 대한 제조사 책임문제로 분쟁이 발생할 소지가 있음

사물인터넷 보안 대응 및 기술

사물인터넷 보안 대응정책

최근 사물인터넷 제품 및 서비스의 보안 문제에 대한 중요성이 급부상함에 따라 국내외 다수 국가기관 및 기업 얼라이언스에서 사물인터넷 보안 가이드를 개발하고 있다. 2016년에는 일본의 정보처리기구인 IPA, 국제이동통신사업자협회인 GSMA, 국제 웹보안표준 단체인 OWASP, 국제 클라우드 보안협의체인 CSA 등에서 사물인터넷 기기의 보안 설계 및 개발, 안전한 서비스 운영 등을 위한 가이드를 발표하였다.

보안가이드를 개발하는 기관 및 단체의 특성에 따라 보안 취약점, 사물인터넷 기기의 생명주기, 사물인터넷 서비스의 구성요소(단말, 네트워크, 서비스) 등 각기 서로 다른 관점으로 보안가이드를 제시하고 있으나 보안 요구사항에 있어서는 많은 부분이 유사하다고 할 수 있다. 국내의 경우도 2016년에 “IoT 공통보안 가이드”를 발표했으며 “산업별 가이드”를 거쳐 가장먼저 확산이 예상되는 홈, 자동차 분야의 인증제도 도입을 준비하고 있다. IoT 공통 보안 가이드에서는 IoT 제품 및 서비스의 설계 개발 단계, 배포·설치·구성 단계, 운영·관리·폐기 단계별로 아래와 같은 내용의 공통 보안 요구사항을 제시하였다.

- 정보보호와 프라이버시 강화를 고려한 IoT 제품 및 서비스 설계
- 안전한 소프트웨어 및 하드웨어 개발기술 적용 및 검증
- 안전한 초기 보안 설정 방안 제공
- 보안 프로토콜 준수 및 안전한 파라메터 설정
- IoT 제품 및 서비스의 취약점 보안 패치 및 업데이트 지속 이행
- 안전한 운영 및 관리를 위한 정보보호 및 프라이버시 관리체계 마련
- IoT 침해사고 대응체계 및 책임 추적성 확보방안 마련

사물인터넷 보안기술

사물인터넷 제품은 기존의 단독으로 구동하는 제품과 달리, 제품을 관리하고 서비스를 제공하는 서버가 존재하며, 제품과 서버는 인터넷을 통하여 상호간 통신을 수행한다. 이를 감안하여 전체 사물인터넷 서비스 구조를 제품(디바이스 및 게이트웨이), 네트워크, 서비스(서버)로 구분할 수 있으며 각 구간의 특성에 맞는 보안 기술을 필요로 한다. 네트워크와 서비스(서버) 구간의 경우는 기존의 인터넷 환경에서의 정보보안에 적용되는 기술이 그대로 적용되는 구간이기 때문에 우리는 상대적으로 보안이 취약한 사물인터넷 디바이스에 대한 보안을 집중적으로 학습한다.

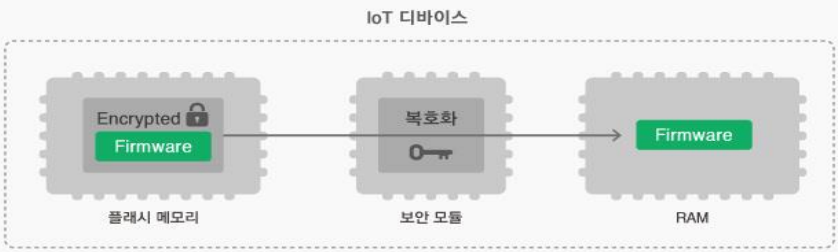
사물인터넷의 제품군에 속하는 디바이스 및 게이트웨이에 대한 보안은 용도와 기능에 따라 다양한 하드웨어 및 소프트웨어 사양을 가지고 있으며, 필요한 보안 기능도 다르다. 사물인터넷 제품을 능력에 따라 등급 0에서 등급2로 나누고 적용할 수 있는 필요한 보안 기능은 펌웨어 암호화, 보안 업데이트, 저장소 암호화, 프로세스 권한 제어, 상호 인증, 통신 암호화등으로 아래의 표와 같이 표현할 수 있다.

디바이스 등급 분류 및 등급별 적용 보안 기술

[등급 0]	[등급 1]	[등급 2]	[등급 3]
- 연산/통신 능력 제약 - 안전한 통신이 불가한 장치	- IoT 전용 프로토콜 사용 가능장치	- 통신/연산 제약이 크지 않은 장치(게이트웨이 등)	- 등급 2보다 강력한 성능의 장치(예: PC)
			
- 주기적으로 Keep alive 메시지 전송 및 기기 상태 전송 - 데이터 무결성 검증	- 통신 암호화 - 인증서 기반 상호인증 - 저장소 암호화 - 보안 업데이트 - 프로세스 권한 제어 - 사용자 로그인 - 사용자 PW 관리	- Tamper resistance - 펌웨어 암호화 - 보안 모니터링/관리 - 보안 부팅 - 기기고유식별정보 검증	- 안티 바이러스 - 폐쇄형 방화벽 - 보안정책 설정/관리 - 사용자/시스템/보안 - 이벤트 로그 생성

- 펌웨어 암호화

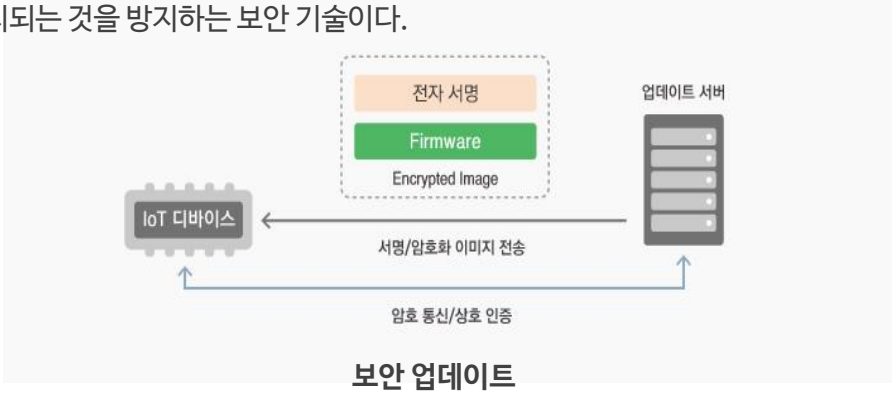
펌웨어 암호화(Firmware Encryption)는 사물인터넷 제품에 탑재되는 펌웨어를 암호화하고, 제품을 구동할 때 이를 복호화 함으로써, 제품에서 플래시 메모리나 디스크를 추출하여 펌웨어를 분석하는 행위를 차단하는 보안 기술이다. 사물인터넷 제품에 하드웨어 보안 모듈을 장착하거나 보안 기능을 제공하는 MCU를 사용하면, 각각의 사물인터넷 IoT 제품마다 다른 암복호화 키를 갖도록 할 수 있으며, 이를 통하여 제품의 복제를 방지하는 효과도 얻을 수 있다.



펌웨어 암호화

- 보안 업데이트

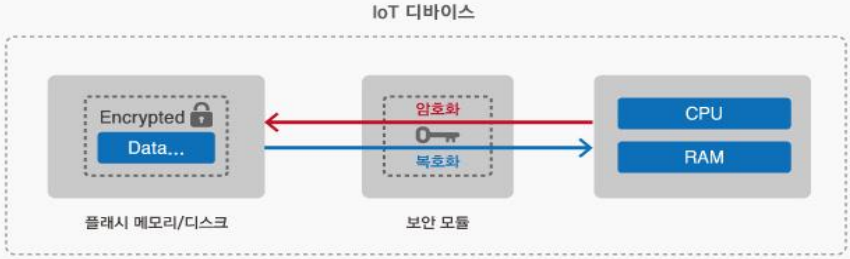
소프트웨어에는 개발 당시에 찾아내지 못한 오류나 보안 취약점이 존재할 수 있으며, 사물인터넷 제품의 펌웨어도 예외는 아니다. 사물인터넷 제품에서 오류나 보안 취약점이 발견되면 제조사는 이를 해결하기 위한 펌웨어를 배포하게 되며, 배포되는 펌웨어는 중간에서 제3자가 가로채 변조하거나 위조할 수 없도록 보호 조치를 취해야 한다. 따라서 보안 업데이트(Secure Update)는 업데이트 펌웨어를 보호하기 위한 기술로, 업데이트 수행 시 업데이트 서버와 제품 간의 상호 인증을 수행하고, 암호 통신 및 업데이트 이미지 암호화를 통하여 업데이트 이미지를 탈취당하거나, 위변조된 업데이트 이미지가 제품에 설치되는 것을 방지하는 보안 기술이다.



보안 업데이트

- 저장소 암호화(Storage Encryption)

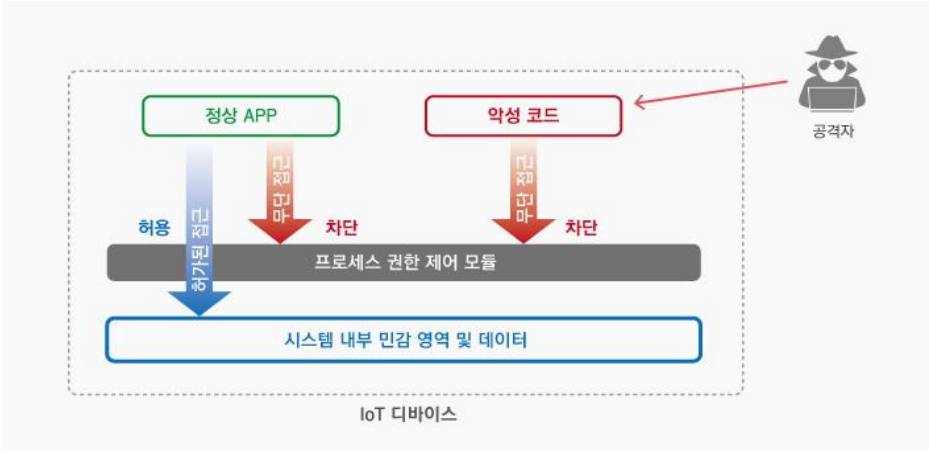
사물인터넷 제품이 내부적으로 저장하는 데이터에는 제품의 설정이나 사용자의 정보 등, 중요한 데이터가 포함되어 있을 수 있으며, 이를 분석하여 서비스에 접근하기 위한 중요 정보를 무단으로 취득하거나, 도난당한 제품에서 원 사용자의 중요한 정보를 취득하는 경우를 생각해 볼 수 있다. 저장소 암호화는 플래시 메모리나 디스크에 데이터를 저장할 때 자동으로 데이터를 암호화함으로써 저장된 데이터의 안전을 보장하는 보안 기술이다.



저장소 암호화

- 프로세스 권한 제어(Process Mandatory Access Control)

사물인터넷 제품의 펌웨어에 보안 취약점이 존재하는 경우, 이를 이용하여 제3자가 악성코드를 제품에 삽입하여 구동함으로써 제어 권한의 무단 획득, 중요 데이터 유출, DDoS와 같은 다른 공격의 경유지로 사용할 수 있다. 프로세스 권한 제어 기능은 제품 내에서 구동되는 프로세스가 시스템 자원(메모리, 파일 등)에 접근하는 권한을 제어하는 기능으로, 중요한 자원에 접근 가능한 프로세스를 최소한으로 제어함으로써 악성 코드가 삽입되더라도 정상적으로 동작할 수 없도록 한다.



프로세스 권한 제어

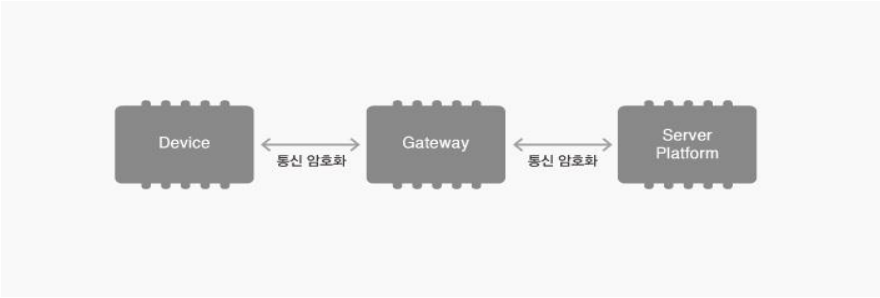
- 상호 인증(Mutual Authentication)

사물인터넷 디바이스와 게이트웨이, 서비스를 제공하는 서버가 상호간 통신을 수행할 때, 악의적인 목적을 가진 제3자가 정상적인 사물인터넷 제품 또는 서버인 것처럼 위장하여 중요 데이터를 탈취하거나 고의로 잘못된 데이터를 전송하여 통신을 수행하는 대상의 오동작을 유발하는 등의 공격이 발생할 수 있다. 상호 인증은 통신을 수행하는 상대방의 신원을 확인함으로써, 사물인터넷 제품과 서버를 제3자로부터 보호하는 보안 기술이다. 통신 데이터 암호화를 위하여 암호 키를 교환할 때도 잘못된 상대와 암호 통신 채널을 수립하는 것을 방지하기 위하여 상호 인증이 활용된다.

상호 인증

- 통신 데이터 암호화(Encrypted Data Transfer)

사물인터넷 디바이스와 게이트웨이, 서비스를 제공하는 서버가 상호간 통신을 수행할 때, 악의적인 목적을 가진 제3자가 통신 구간 중간에서 중요 데이터를 도청하거나, 통신 내용을 위변조하는 공격이 발생할 수 있다. 통신 데이터 암호화는 통신을 수행하는 양자간에 키 교환(key exchange)을 통하여 수립한 세션 키(session key)를 가지고 데이터를 암호화하여 전송함으로써, 제3자로부터 통신 데이터를 보호하는 보안 기술이다.



통신 데이터 암호화

본격적인 IoT 시대가 열리고 있다. 스마트 홈의 경우 얼리어뎁터만 이용하던 시대를 지나 2017년에는 100만 이상의 실 사용자가 비용을 지불하고 IoT기기를 구매 할 것으로 예상된다. 초 연결사회가 도래하고 있지만 기기간의 연결은 악의적 공격자에게 시장을 확대해 주는 절호의 기회이기도 하다. 따라서 공개SW포럼을 이용하는 개발자/솔루션 제조사의 입장에서 보안은 전문회사의 전유물에서 H/W 및 Embedded 개발관계자를 포함한 IoT산업 생태계 전반을 아우르는 필수 학습사항으로 자리 잡아야 할 것이다. “IoT” 용어의 창시자인 케빈 에쉬튼은 “IoT는 기술의 진보처럼 보이지만 결국 인간의 삶을 풍요롭게 하고 살찌우는 도구가 되야 한다”라고 말했다. 그의 말처럼 보안도 적용하면 불편한 기술이 아니라 이용자에게 편안하고 든든한 느낌을 제공해야 한다.

02. 스마트시티의 이해

최근 저출산, 고령화 및 환경오염 등과 같은 사회문제가 도시문제로 이어지면서 도시문제 해결 및 도시경쟁력 제고를 위한 대책이 필요한 시점이다. 과거 급속한 도시화로 인해 팽창한 도시에 최근 저출산, 고령화로 인해 도시인구가 급감하면서 빈집 문제 등 도시문제를 양산하고 있고 도시중심부의 교통량 집중으로 인한 대기오염 문제 및 에너지 수급 문제 등 도시문제가 심각해지면서 도시의 경쟁력이 퇴화되기도 한다.

따라서 도시경쟁력의 제고를 위한 방안으로 ‘스마트시티’가 4차 산업혁명 시대를 맞아 각광을 받고 있다. ‘스마트시티’는 사물인터넷과 빅데이터와 같은 ICT 기술을 기반으로 도시 인프라의 초연결성을 바탕으로 에너지 효율화, 데이터 개방, 도시 관리 효율화, 시민참여를 통한 혁신 등이 가능한 4차 산업혁명 시대의 축소판이기 때문이다. 이에, 4차 산업혁명 시대에 ‘스마트시티’가 도시문제를 해결하고 도시경쟁력 및 삶의 질을 향상시킬 수 있는 지속가능한 새로운 도시모델로 각광을 받고 있고 우리나라를 비롯한 세계 여러 나라에서도 각국의 상황에 맞게 ‘스마트시티’의 구축에 집중하고 있다.

우리나라는 사회적 경제적 파급력이 높아 신속하고 집중적인 지원이 필요한 '9대 국가 전략 프로젝트' 중 하나로 성장동력 확보를 위해 '스마트시티'를 선정하고 기존의 법(u-City법)을 스마트도시법으로 개정하는 등 적극적 지원하고 있다. 중국 및 인도를 비롯한 신흥국에서는 급속한 도시화 문제를 해결하기 위한 대책으로, 유럽 및 북미 선진국에서는 도시노후화 및 기후변화 대응방안으로 '스마트시티'를 채택하고 있다.

스마트시티의 개념

스마트시티는 물리적 도시시설 및 공간이 인터넷과 실시간 연결되는 사물인터넷(IoT)와 ICT가 접목되어 이용자들에게 실시간 도시서비스를 제공할 수 있는 도시상태를 의미한다고 일반적으로 정의하지만 2014년 세계전기통신 기구인 ITU가 조사한 바에 따르면 스마트시티(smart sustainable cities)에 대한 정의가 116개에 이르고 있고 개념 정의에 사용된 키워드 분포도 아래의 표에서 제시된 바와 같이 환경, 지속 성장, ICT, 지능 등 매우 다양하게 나타났다.

스마트시티 개념 정의에 사용된 키워드 분포

유형	빈도
생활과 생활의 질(Quality of life and lifestyle)	6%
인프라와 서비스(Infrastructure and services)	17%
ICT, 통신, 지능 ,정보(ICT, communication, intelligence, information)	26%
사람, 시민, 사회(People, citizens, society)	12%
환경과 지속성장(Environment and sustainability)	17%
거버넌스, 관리와 행정(Governance, management and administration)	10%
경제와 재정(Economy and Finance)	8%
이동성(Mobility)	4%

즉, 국가와 도시의 처한 환경에 따라서 스마트시티는 그 모습이 매우 다르게 나타날 수 있음을 의미하는 것이다. 예를 들어 유럽연합(EU)의 경우에는 '디지털 기술을 활용하여 시민을 위해 더 나은 공공서비스를 제공하고, 자원을 효율적으로 사용하며, 환경에 미치는 영향을 최소화하여 시민의 삶의 질 개선 및 도시 지속가능성을 높이는 도시'라고 정의하면서 시민중심과 노후 인프라 개선에 환경 관점을 중요시한 개념으로 스마트시티를 정의하고 있다.

반면 인도의 경우에는 '상하수도, 위생, 보건 등 도시의 공공서비스를 제공할 수 있어야 하며, 투자를 유인할 수 있어야 하고, 행정의 투명성이 높고 비즈니스하기 쉬우며, 시민이 안전하고 행복하게 느끼는 도시'로 스마트시티를 정의하면서 스마트시티의 초점을 '부족하거나 없는 도시 인프라 건설'과 '외부 투자유치'에 두고 있는 것이다.

하지만 기술관점에서 보면 스마트시티는 인프라, 데이터, 서비스로 구성된 하나의 커다란 플래폼으로 인식된다. 인프라는 도시, ICT기술, 공간정보 인프라를 포함한 물리적, 기술적 인프라를 의미하며, 데이터는 사물인터넷(IoT 기술)을 기반으로 도시 내 모든 인프라와 사물에서 발생하는 데이터로 자유로운 공유 및 활용이 가능함을 의미하며 서비스는 수집된 데이터를 바탕으로 실제 활용 가능한 품질 및 지능서비스를 개발하여 시민이 주도적으로 활용 가능한 환경을 조성하는 것을 의미한다.

왜 스마트시티?

스마트시티가 가져올 변화는 크게 비용 측면과 편익 측면에서 살펴볼 수 있다. 우선 비용측면에서 보면 대도시와 전통도시들이 그동안 증가된 비효율과 고비용 구조를 개선하여 지속성장을 할 수 있도록 하기 위해 추진하는 비용절감형 스마트시티를 생각할 수 있다. 유럽의 많은 선진국의 대도시 경우에는 오랜 기간 축적된 도시의 자원 낭비형의 도시구조 개선이 목표가 될 것이고, 중국의 베이징과 같은 개도국의 대도시 경우에는 급증하는 인구유입을 수용하기 위해 저비용의 도시를 구축하는 것을 지향하면서 스마트시티를 추진하게 된다.

편익 측면에서는 중소도시와 신도시들이 작은 도시규모에도 불구하고 대도시 못지않은 효율성과 매력도를 갖기 위해 추진하는 기회 창출형 스마트시티를 생각할 수 있다. 한국의 판교 테크노밸리와 같은 선진국의 중소도시 같은 경우에 경제활동, 의료서비스, 사회관계 등 제반 측면에서 대도시와 격차 극복하기 위해 스마트시티를 추진하며, 선진국 등의 신도시(예, 인천 송도)에서는 새로운 도시브랜드와 투자 가치 위해 스마트시티를 추진하며 개도국의 신도시는 도시현대화를 추진하여 해외투자 확대를 도모하기 위해 추진하는 경우이다.

하지만 스마트시티를 추진하면서 기대되는 중요한 변화는 생산성 향상과 경제 지표 개선에 있다. Georg Graetz와 Guy Michaels의 연구에 따르면 로봇의 생산성과 GDP기여도를 17개국을 대상으로 분석한 결과 1993~2007년 기간 동안 생산성과 GDP를 각각 0.36%p과 0.37%p를 증가시켰는데 이 기간 동안 연구대상의 17개국의 연평균 생산성 증가율은 2.17%로 로봇은 생산성을 20% 가량 증가시키는 효과를 수반하는 것으로 나타났다. 이것은 로봇과 같은 지능기술 기반의 스마트시티는 기존 도시에 비해 생산성을 최소 20% 이상을 증가시킬 수 있는 것으로 추정되는 근거가 되기 때문에 대부분의 많은 도시에서는 스마트시티추진을 통해서 생산성 향상과 경제지표 개선을 도모하는 것이다.

도시의 생산성 향상과 경제지표 개선은 그 도시에 거주하는 시민이나 그 도시에 거주하고자 하는 시민에 대하여 거주적합성 향상, 근무 적합성 향상 그리고 지속 가능성으로 대표될 수 있다.

- 거주적합성(Livability) 향상: 도시 거주자의 삶의 질을 향상을 의미하는 것으로 저렴한 에너지, 편리한 대중, 좋은 학교, 빠른 응급조치, 깨끗한 물과 공기, 낮은 범죄율 그리고 다양한 즐길 거리와 문화 혜택에 접근 등이 포함된다. 이를 위해서 도시에서는 원격 가정 서비스, 경보 시스템, 원격 환자 관찰 시스템에 접속 서비스하는 e-Health 혜택을 제공하는데 대표적인 예로 타이페이의 "Telecare"나 멕시코시티의 "A help button"를 들 수 있다. 또한 멕시코시티의 PICE(the Comprehensive School Connectivity Programme)나 프랑스의 Limoges Digital School Plan과 같은 e-러닝 프로그램들을 개발하여 시민에게 제공하는 사례가 많다.

- 근무 적합성(Workability) 향상: 더 많은 일자리, 더 좋은 일자리, 지역 GDP 향상을 의미하며 그 도시의 스마트시티 시민에게 세계 경제에서 경쟁할 수 있는 기초적인 인프라 서비스에 접속할 기회를 부여하고 광대역 연결성, 깨끗하고 싸고 신뢰성 있는 에너지, 교육 기회, 주거 및 상업 공간 확보 그리고 효율적인 운송 체계가 포함된다. 즉, 도시로 재능 있는 인재를 유치하고 보유하는 계획들을 개발하는 것으로 스페인 바르셀로나의 "Do it in Barcelona", 스페인 빌바오시의 "Plan for the Promotion of Creative Industries", 그리고 타이페이의 "Programme to boost R&D&i in SMEs" 등이 대표적인 사례이다.

- 지속 가능성: 자원을 고갈시키거나 영구히 손상을 가하지 않도록 자원을 사용하는 방법을 의미하며 환경과 경제적 현실을 고려하여 스마트시티는 자연, 인간 그리고 경제적 자원을 효율적으로 이용하여 긴축 시기에도 비용절감을 촉진하여 세금 납부자의 돈을 잘 관리하는 것을 포함한다.