15차시. 스마트시티와 사어버 보안(2)

01. 각국의 스마트시티 추진

스마트시티 추진

- 전 세계적으로 전례 없는 빠른 속도로 인구가 도시로 집중하고 있다. 고용기회의 확대, 건강과 교육 기회의 확대, 그리고 오락, 문화 및 예술 기회의 확대 등 도시가 주는 혜택으로 도시화가 진행되고 있다. 현재 전 세계 도시는 지리적으로 2%의 면적을 차지하지만 전체 에너지의 66%, 식수의 60%를 도시에서 소비하고 있으며 이산화탄소 배출량은 전체의 70%를 차지하고 있고 전 세계 GDP의 50% 가량이 600여 개 도시에서 생산되고 있는 것이다.
  도시화의 진전으로 도시인구는 지속적으로 증가하여 2050년이면 전 세계의 인구는 약 95억 명에 도달하는데 그 중 약 67%가 도시에서 거주하게 될 전망이다. 단기적으로는 향후 10년 내에 7억 명의 도시인구가 증가하고, 금세기 중반까지는 약 30억 명의 추가적인 도시인구가 수용될 것으로 전망하고 있다. 치근 UN 보고서에 따르면 세계적으로 4만 개의 새로운 도시가 필요하다고 내다보고 있다.
  따라서 현재 인구 규모의 일부분을 수용하도록 건설된 도시 인프라는 도시화가 진행되면서 커다란 압박을 받고 있어 대규모의 업그레이드가 필요한 것이다. 2013년 the America Society of Civil Engineers의 조사에 따르면 미국의 도시 인프라는 D+로 평가되었다. 한편 개발도상국 대부분의 도시 경우에는 없거나 불충분한 도시 인프라로 대규모의 확장이 필요한 시점이다. 한 예로 2012년 인디아의 정전으로 6억 명에게 전기가 공급 중단된 사고가 발생하였는데 이는 증가하는 전기 수요를 채워주지 못하는 불충분한 전력 공급 인프라가 그 원인으로 판명되었다. McKinsey & Company에서도 도시에 대한 매년 자본투자가 현재 10조 달러에서 2025년에는 20조 달러로 증가할 것으로 추산하고 있다. 이와 같은 배경으로 선진국은 물론 개발도상국가에서는 그 국가의 도시환경에 맞는 목적을 달성하기 위하여 스마트시티 건설에 많은 노력을 기울이고 있는 것이다.

스마트시티 발전과정

- 스마트시티는 1990년대 중반 미국에서 '디지털시티'의 개념이 등장하면서 지난 20년간 3단계의 진화과정을 거치면서 발전을 하였다.

  - 태동기(1996 ~ 2002): 1990년대 중반 디지털시티 확산을 계기로 태동하여 1993년 암스테르담 디지털시티, 1996년 헬싱키Arena 2000, 1998년 쿄토 등 실제 스마트시티는 도시 혁신을 주도한 Eco-City 또는 sustainable City 등 도시 지속성장 프로젝트가 해당된다.

  - 성장기(2003 ~ 2011): 2003년 한국 u-City를 기점으로 기술주도형 스마트시티 태동하였고 전략의 중심이 부분적 정보기술 활용에서 전반적 도시 정보화로 이동하였다. 2008년 IBM의 smarter Planet을 계기로 CISCO 등 글로벌 기업이 스마트시티에 참여하기 시작하였다. 유럽과 미국에서는 Open Innovation과 연계되면서 Living Lab으로 발전하였다.

  - 확산 및 고도화기(2012 ~ 현재): 2012년 중국이 스마트시티 구축을 공식화하면서 세계적으로 급속히 확산되었다. 2012년 구글의 딥러닝 기술발전 등으로 스마트시티 고도화 빨라지고 있으며 2015년 인도 모디총리가 스마트시티 구축전략을 발표하면서 스마트시티가 개도국에도 확실히 정착되는 계기가 되었다.

해외 주요국의 스마트시티 추진

- 일본의 닛케이(Nikkei) BP가 추산한 전체 608건의 세계 스마트시티 프로젝트 가운데 중국, 미국, 일본, 유럽, 우리나라 등 5개 국가의 프로젝트 비중이 84%가 넘는다. 특히, 선진국은 주로 기존 도시에 새로운 활력을 넣기 위한 도시 재개발을 통한 스마트시티 전략을 접근하는 것에 반해 신흥 국가는 새로운 도시를 건설하는 전략을 선택하고 있다. 즉 해외의 대표적 스마트 시티 정책을 살펴보면 중국 및 인도를 비롯한 신흥국의 경우에는 급속한 도시화 문제를 해결하기 위한 대책으로 스마트시티를 추진하고 있으며 유럽 및 북미 선진국의 경우에는 도시의 노후화 또는 기후의 변화에 대응하기 위하여 스마트시티를 추진하는 도시경쟁력 제고를 위한 방안인 것이다.
  미국 연방정부는 에너지·의료 분야 외에는 별다른 스마트시티 이니셔티브를 제안하지 않고 스마트시티 구축을 주 정부나 지자체, 그리고 민간 기업들에게 위임하고 있다.
  유럽에서는 유럽집행위원회(EC)가 EU차원에서 에너지와 교통에 주안점을 둔 스마트시티 도입 촉진 정책을 총괄하고, 구체적인 프로젝트는 각 국가 또는 도시에서 개별적으로 추진하고 있다. 닛케이에 따르면 독일이 20건, 영국 13건, 프랑스 10건, 덴마크 9건, 스웨덴 8건으로 나타나고 있다. 유럽에서는 스페인의 바르셀로나와 비엔나가 가장 대표적인 스마트시티 정책 추진으로 주목을 받고 있다. 두 도시는 각각 시스코와 지멘스의 협력으로 프로젝트를 진행하고 있다.

네덜란드 암스테르담의 사례

네덜란드의 암스테르담시 사례는 주목할 만하다. 지난 2004년 'I amsterdam'라는 브랜드를 설정하고 스마트시티 사업을 지속적으로 추진해 왔는데, 생활(living), 근로(working), 교통, 공공시설, 데이터 개방이라는 5가지 테마를 중심으로 총 3개 지역에서 무료 WiFi, 스마트 가로등, 연료전지, 헬스, 스마트그리드, 스마트 주차, 교통 트래픽 관리, 스마트홈 등 40개 이상의 개별 프로젝트를 진행 중이다. 또한 덴마크의 코펜하겐시 역시 스마트시티 프로젝트를 추진하는 대표적인 도시로 편리하고(convenient), 창의적이며(creative), 효율적(efficient)이고, 재미있는(fun) 도시를 목표로 하고 있다. 특히 2005~2015년에 걸쳐 이산화탄소 배출량을 20% 줄이고, 2025년에는 탄소 배출량을 'zero'로 만들겠다는 목표(carbon netural)를 세우고 있다. 이로 인해 Siemens는 자체적으로 산정하는 녹색도시지표(green city index)에서 유럽 지역의 1위 도시 로 코펜하겐을 선정한 바 있다.

영국 런던의 사례

영국의 런던 역시 급격한 인구 증가와 이로 인해 발생하는 사회, 건강, 교육 문제 등을 새로운 기술을 활용하여 효율적으로 해결하기 위해 2013년 12월 "스마트 런던 플랜(Smart London Plan)"을 발표했다. '스마트 런던 플랜"은 협력 및 참여, 기술 혁신, 정보 공개 및 투명성, 효율적인 자원 관리를 통해 런던 시민의 삶의 질을 향상시키는 데에 그 주요 목적이 있으며, 이를 위해 '시민 중심의 계획' '공공 데이터 개방' '연구, 기술, 창조성 연계' 등 7개의 정책 방향을 제시하고 있다.

영국의 Milton Keynes시의 Data Hub 프로젝트는 스마트시티를 통해 발생되는 데이터의 가치를 제고한 사례로 구체적으로 알아 본다. 스마트시티 서비스를 효율적으로 지원하기 위해 Milton Keynes시 당국은 Open University, BT가 함께 데이터 공유 플랫폼을 구축하였다. 제공되는 데이터는 ① 중앙과 지방의 공개 데이터, ② 에너지, 교통, 수자원 등 주요 도시 인프라에서 생성되는 데이터, ③ 인공위성과 각종 센서로부터 제공되는 데이터, ④ 각종 소셜 매체에서 생성되는 crowdsourced data 등 도시 와 관련된 모든 데이터를 망라하고 있으며 점차 대상을 확대할 계획이다. 제공되는 데이터 형태는 ① file data, ② 특정 장소, 조직 등 각종 대상을 모아놓은 Entity API, ③ 실시간으로 제공되는 Feed API, ④ 공간정보 데이터이며, 데이터를 기계적으로 모아서 제공하는 것이 아니라 스마트시티 서비스에 맞게 연관된 데이터를 모으고 다듬은 다음 이를 분석할 수 있는 도구와 교육 등 전문적 지원서비스를 묶어서 함께 제공하고 있는 것이다.

- **일본의 사례**
  일본은 2010년부터 추진 중인 '일본 신성장전략'의 일환으로 '그린 이노베이션에 의한 환경, 에너지 대국전략'을 추진 중이며, 스마트 시티는 이 전략에 포함되어 있다. 일본 경제산업성은 해당 사업을 통해 자국 내의 스마트시티 건설뿐 아니라 해외 시장에 관련 기술을 수출하는 것을 목표로 삼고 있는데, 2020년까지 3조 2천억 엔의 경제효과와 6만 명 이상의 고용창출 효과를 기대하고 있다. 여러 스마트시티 프로젝트 가운데 내각부의 환경미래도시 구상, 경제산업성의 스마트 커뮤니티 구상, 총무성의 ICT 스마트 타운 구상 등 3가지가 가장 대표적이다.

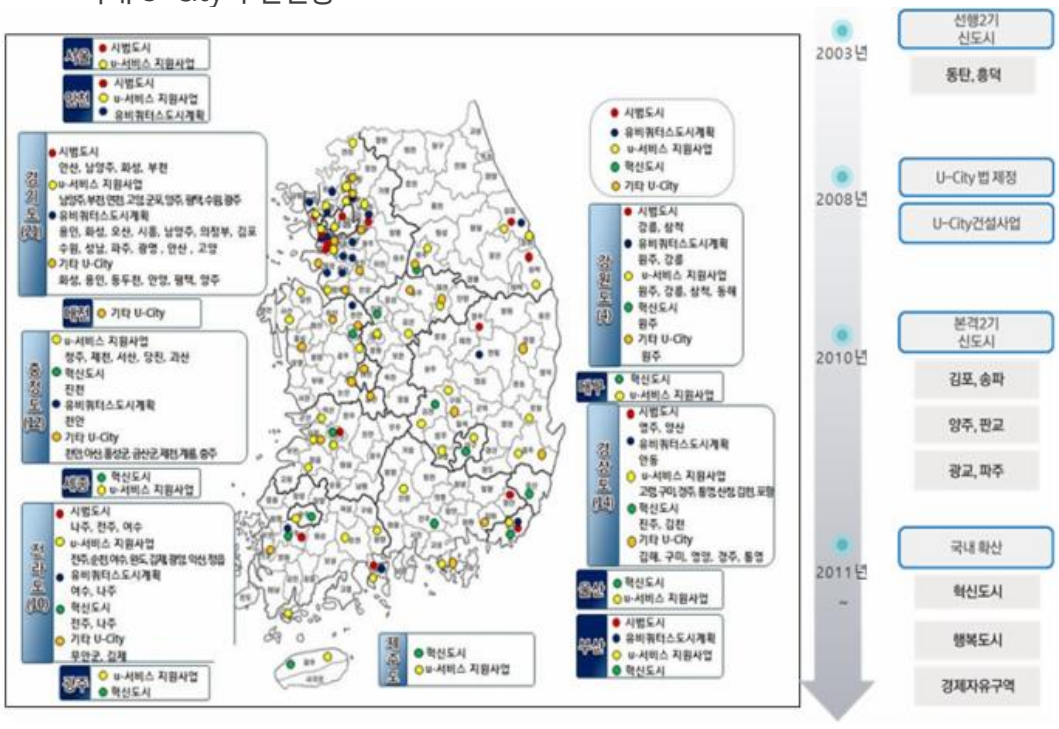
- **중국의 사례**
  중국 정부는 2015년까지 320개 스마트시티 구축 계획 발표했으며, 2025년까지 2조 위안 (3,330억 불)을 투자할 계획이다. 중국의 스마트시티 사업은 도시의 특징에 맞추어 다르게 진행하고 있다. 예를 들어 베이징은 실시간 인구정보 시스템과 스마트 미터기, 도시 보안 감시 시스템, 주정차 지불시스템 등을 추진해왔다. 상하이는 초고속 네트워크에 집중 투자하고 있다. 또한 선전(深圳)는 스마트그리드, 창수(常熟)는 지역 경쟁 활성화에 초점을 맞추고 있다. 이 외에도 분산된 도시들을 연계해 지역 특성에 맞는 스마트시티 클러스터를 구축하고 있다.

- **인도의 사례**
  2014년 6월, 인도의 나렌드라 모디 수상은 100 개의 스마트시티를 구축하겠다는 계획을 발표했다. 2015년 모디 총리의 Smart City Mission 발표로 국가정책으로 공식화하였고, 구도시형(Brownfield)과 신 도시형(Greenfield)으로 구분하여 추진하는 계획을 가지고 있다. 선진국에서 말하는 스마트시티와 달리 외국자본 투자를 유도할 수 있을 정도의 현대적 도시 구축을 의미하는 구도시형은 2015년 100개 도시를 선정하여 20개 도시를 먼저 착수하고 나머 지 80개 도시는 2016년부터 40개씩 2차에 걸쳐 순차적으로 추진하고 있다. 신도시형은 2009년부터 준비해 온 신도시 개발계획을 이어받아 추진하며 Dholera 지역 등이 유명하며 개발기간은 구도시형이 1~5년, 신도시형은 10~30년이 소요될 것으로 예상하고 있다.

한국의 스마트시티 추진

- 1994년 서울 아현동 지하철 공사장 도시가스폭발사고와 1995년 대구지하철 공사장 가스폭발사고 등의 지하 시설물 관련 사고가 잇달아 발생하면서 국가적으로 지리정보 기반 조성의 필요성이 커지면서 1995년 국가지리정보체계 구축사업을 시작하였다.
  공간정보의 유통 및 활용에 중점두면서 각 지자체별로 공간정보 DB 및 시스템을 구축하여 지자체의 관련 업무에 활용하도록 하였다.
  2000년 구축된 국가지리정보체계를 기반으로 효율적 관리에 대한 수요가 발생하면서 도시를 시스템적으로 관리하기 위한 도시정보시스템 구축 사업을 추진하게 되었다.
  도시에 존재하는 전기, 가스, 통신 등 지하 시설물의 위치를 파악하여 배관 파손 등으로 인한 화재, 폭발, 가스누출 등의 사고를 미연에 예방하는 것이 목적이었다.

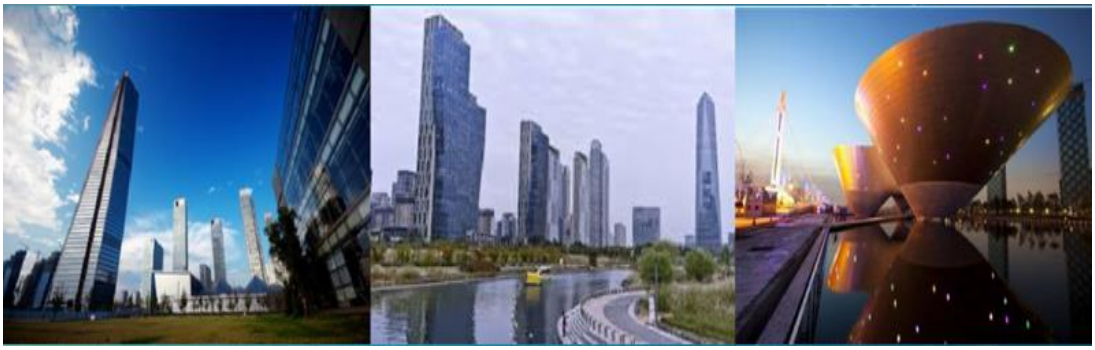
- 2004년 ITS 839 전략을 수립하는데 이 전략은 IT가 일상생활에 스며들어 사회를 변화시키고 새로운 부가 가치를 창출하는 국가 차원의 IT 미래비전이었다. 이에 따라 국내 스마트시티의 전신인 유비쿼터스 도시(u-City) 개념을 적극적으로 도입하면서 2008년 '유비쿼터스도시의 건설 등에 관한 법률(u-City 법)'을 제정하게 된다. 일명 u-City 법에는
  - u-City구축을 위한 종합계획의 수립,
  - 지자체 유비쿼터스 도시 계획의 수립 및 승인,
  - 시범도시의 지정 등 u-City구축을 위한 제도적 기반 마련
  - 신도시 지역에 u-City법에 의거한 기반시설(통신망, 지능화된 기반시설, 도시통합운영센터로 법에 규정을 법으로 규정) 등의 내용을 포함하고 있었다.
  - 국내 U-city 추진현황



- u-City법으로 인해 신도시지역의 u-City구축의 확산 및 지원에는 성공하였지만 기존 시가지까지 확산은 불가능하였고 u-City 기반시설 구축에만 집중하여 효율적 관리 운영이 미흡하는 등 여러 가지 한계를 지니고 있었다. 따라서 u-City법은 도시 범위를 기존 시가지까지 확대할 수 있도록 「스마트도시 조성 및 산업진흥 등에 관한 법률(스마트도시법)」(일명 스마트도시법)으로 전면 개정되어 지난 2017년 3월 2일 국회 본회의 통과하고 9월 22일자로 시행되었다.

- 스마트 도시법에서는 사업 지원대상이 165만㎡ 이상의 대규모 신도시에서 30만㎡로 축소되어 신도시 건설이 아닌 도시재생에 초점을 맞추었고 사물인터넷(IoT) 및 빅데이터 등을 활용하여 교통, 쓰레기 수거, 방범 등 도시 문제를 해결하는 경우 인센티브를 제공하도록 하였다. 또한 사업시행자로 민간 사업자를 추가하여 건설사나 통신사 등이 지방자치단체 사업에 참여할 수 있는 범위를 확대하였으며 스마트시티 서비스 지원 기관 업무에 스마트시티 기술의 수출 지원을 추가하여 국내 업체가 해외 진출에 나설 수 있는 발판을 마련하였다.

  - 사례 1: 인천 송도 신도시
    . 최첨단 ICT를 거주지, 비즈니스, 공공부문, 산업단지 등 도시의 모든 분야에 접목해 정보화 미래형 도시를 구축
    . 차세대 지능형 방법 서비스와 스마트 스페이스 서비스 등을 구축한 선도적 신도시



  - 사례 2: 세종시
    . 버스운행, 교통체증 상황부터 대기농도까지 도시 모든 정보를 수집하는 정보센터 운영
    . 도시토탈 솔루션을 제공하여 교통, 안전, 도시관리, 에너지 등에 대한 시범단지 구성

02. 4차 산업혁명과 보안(종합)

4차 산업혁명의 서비스에 대한 보안 요구사항

- 보안 요구사항은 운자가 사용자에게 서비스를 제공하기 위해 보안 부분에 있어서 반드시 지켜야 할 사항을 말한다. 보안 요구사항은 안전한 서비스를 제공하기 위한 보안요건들이 갖춰졌을 때 충족된다. 다시 말해 보안 요구사항을 충족하기 위해서는 그에 상응하는 보안기술이 갖춰져야 함을 의미한다.
  보안 요구사항은 기본적으로 6가지 요소로 이뤄져 있다. 그리고 이 보안 요구 사항은 모든 서비스에 공통적으로 적용되는 기본요소라고 할 수 있다. 6가지 기본 요구사항 외에 4차 산업혁명 서비스로 인해 추가적으로 지켜야 할 4가지 사항들이 더 있다. 결과적으로 4차 산업혁명 시대에 제공되는 스마트 서비스가 지켜야할 보안 요구사항은 총 10가지로 정리된다. 이 10가지를 기준으로 안전한 서비스 제공이 가능한지 판별해야 한다.

- **공통 보안 요구사항 – 기밀성**
  기밀성은 권한이 없는 사용자는 정보를 읽지 못하도록 정보를 암호화하여 정보유출을 막도록 하는 것이다. 가령 사용자의 전력정보를 측정하는 스마트 미터기의 해킹을 방지하기 위해 전력정보를 암호화 하여 유출을 방지하도록 하는 요구사항인 것이다.

- **공통 보안 요구사항 - 무결성**
  무결성은 송신자가 전송한 원래의 메시지 내용이 위변조 되지 않도록 하는 보안요구 사항이다. 예를 들어 사용자가 은행에 돈을 입금할 때 돈을 입금 받는 계좌정보를 해커계좌로 위변조 할 수 있으며, 스마트카의 경우 스마트카에서 주고받는 명령체계를 위변조할 수 있다. 스마트카 탑승자는 최종 도착지를 A지역으로 명령했지만, 해커는 위변조로 B를 목적지를 바꿀 수 있다. 혹은 A로 가는 동안 명령체계를 마음대로 위변조해 탑승객의 안전을 위협할 수 있다. 무결성은 이러한 위변조를 방지 하도록 한다.

- **공통 보안 요구사항 - 가용성**
  가용성은 권한이 부여된 사용자가 서비스 접근을 보장하는 것이다. 가용성을 위협하는 대표적인 공격은 '서비스거부공격'이다. 이러한 공격의 대표적인 사례로는 '7.7 서비스분산거부공격'이 있다. 이 공격은 해커가 2009년 7월 7일을 기점으로 대한민국과 미국의 주요 정부기관, 포털 사이트, 은행 사이트 등이 서비스를 제공하지 못하도록 서버에 서비스거부공격을 한 사건이다.

- **공통 보안 요구사항 - 인증**
  인증은 사용자 및 기기들이 서비스 접근에 인증되었는지 여부를 판단하도록 하는 요구사항이다. 인증은 비권한자가 서비스에 함부로 접근하지 못하도록 하는 것으로 대표적으로 '로그인' 기능을 들 수 있다. 로그인은 아이디와 비밀 번호를 아는 권한자만 서비스에 접근 할 수 있다. 그러나 로그인이 해킹되었을 경우 인증 요구사항은 무너진 것이다. 또한 중요정보인 로그인정보가 유출 되었고 서비스의 중요 정보들에도 접근할 수 있기 때문에 '기밀성'도 무너졌다고 할 수 있다.

- **공통 보안 요구사항 – 부인방지**
  부인방지 요구사항은 전자서명이나 공개키 등을 이용해 송수신 사실을 부인 할 수 없도록 하는 것이다. 서비스를 제공받았음에도 제공받지 않았다고 부인할 수 없게 하는 요구사항인 셈이다. 해커가 사이버공격을 통해 은행으로부터 돈을 받았음에도 불구하고 받지 않았다고 부인할 수 있는데, 부인방지는 이러한 사기유형을 방지해준다.

- **공통 보안 요구사항 - 접근제어**
  접근제어는 사용자와 기기의 특성에 따라 서비스 접근가능성을 차등 부여해서 사이버공격으로부터의 위험을 막는 것이다. 접근제어는 내부정보유출과 APT공격 위협을 경감시키는 요구사항이다.

- **새로운 보안 요구사항 - 추적 불가능**
  추적불가능은 현재 얻은 정보로 과거정보를 추적하는 것을 방지하는 요구 사항이다. 이는 특히 사물인터넷 센서에 요구되는 사항이다. 해커가 센서의 통신 정보를 낚아채 사용자 정보가 노출된다면 보안 요구사항 중 '기밀성'이 깨지게 된다. 뿐만 아니라 해커가 낚아챈 정보를 이용해 정보의 근원지와 과거정보까지 유출해낸다면, 정보유출 피해가 더욱 심각해진다. 이러한 피해를 방지하는데 필요한 요구사항이 바로 추적불가능이다.

- **새로운 보안 요구사항 - 확장성**
  확장성은 ICBM(IoT, Cloud, Big data, Mobile) 서비스에 해당되는 요구사항이다. 서버가 센서로부터 전달되는 정보를 처리하기 위해서는 센서가 보낸 정보를 서버가 읽기 위한 인증이 필요하다. 그때 서버는 인증을 위한 정보가 필요한데, 센서만 그 정보를 가지고 있으면 서버는 읽지 못한다. 그래서 센서 뿐만 아니라 서버도 인증정보를 가지고 있어야 하며, 이를 확장성이라고 한다.

- **새로운 보안 요구사항 - 익명성**
  익명성은 정보 기밀성 중 사용자 정보와 관련된 사항이다. '기밀성' 혹은 '추적불가능'과 비슷한 내용 같지만 차이점을 가지고 있다. 기밀성은 통신 내부에 포함되어 있는 정보자체를 보호하는 것이고 익명성은 정보를 보낸 주체자의 정보를 보호하는 것이다. 그래서 익명성은 데이터 암호화 같은 것이 아니라, 보낸 사람 이름의 일부를 마스킹 처리하는 형태의 보호법이다. 4차 산업혁명에서는 스마트그리드, 스마트홈, 스마트헬스 등 개인과 밀접하게 관련된 정보들을 다루며 사생활 보호를 위해 서비스를 제공받는 주체의 정보가 공개 되어서는 안 된다. 때문에 '익명성'이 매우 중요하다.

- **새로운 보안 요구사항 - 실시간성**
  4차 산업혁명에서는 보안기능도 중요하지만 실시간 정보를 제공하기 위한 신뢰성 있고 안정성 있는 서비스도 필요하다. 실제로 보안작업은 트래픽을 모니터링하기 때문에 네트워크 속도를 저하시킨다. 그러나 실시간성을 요구하는 스마트 서비스에서 보안 때문에 서비스 속도가 느려진다면 피해가 발생할 수 있다. 예를 들어 스마트카를 운전하는 도중에 GPS 수신이 늦어져서 스마트카 시스템 내에 결함이 생긴다면 탑승객 생명에 큰 위협을 될 수도 있다. 비슷한 예로 기관에 들어가는 방화벽 장비들 중 제공되는 보안 기능은 많으나 네트워크 속도를 저하시켜서 오히려 제공기능을 끄고 사용하는 경우도 있다. 이는 보안기능이 아무리 훌륭하더라도 실시간으로 서비스를 제공하지 않는다면 의미가 없음을 보여주는 단적인 예이다.

- 안전한 보안서비스를 위해서는 위에서 설명한 10가지 요구사항을 만족해야 한다. 참고로 각각의 보안 요구사항 요소는 완전히 독립적인 것은 아니며 상호 연관성을 주기도 한다. 가령 보안을 위한 인증이 지켜지지 않으면 기밀성은 자동으로 무너지며 익명성이 지켜지지 않으면 추적불가능성도 당연히 만족되지 않는다. 결국 10가지 보안 요구사항을 개별 사항으로 생각하고 일부만을 만족시키기 위해 노력하는 것이 아니라 전체를 하나의 유기적인 시스템으로 바라보고 이를 지킬 필요가 있다. 끝으로 10가지 보안 요구사항을 만족하기 위해서 보완하는 방법을 학습한다.

ICBM (IoT, Cloud, Big data, Mobile) 보안 대응방안

- **함호화 통신 복호화**
  사이버 보안 전문 회사인, 지스케일러에 따르면 사이버공격의 54%가 암호화 트래픽을 사용한다고 한다. 암호화통신은 네트워크와 통신을 할 때 통신하는 내용을 보지 못하게 통신을 암호화시켜 놓은 것을 말한다. 암호화 통신을 보기 위해서는 상호 인증한 키가 있어야 해당 정보를 열람할 수 있다.
  암호화 통신에 멀웨어를 숨겨서 보낼 시 방화벽, 침입탐지시스템 등 보안 장비들이 멀웨어를 탐지할 방법이 없다. 2015년도에는 암호화 통신으로 삼성 스마트냉장고를 해킹한 시연이 있었다. 스마트냉장고에는 이메일 기능이 있었는데, 암호화 통신을 이용해 이메일 전달시 보안탐지를 피해서 공격한 것이다. 이처럼 4차 산업혁명 시대에는 암호화 통신을 활용해 공격하는 경향이 늘어날 것이며, 실제로 보안 산업에서 중요한 이슈로 부각되고 있다.
  여기서 요구되는 것이 암호화 통신의 복호화기능이다. 암호화 통신을 복호화 할 경우 네트워크 보안장비들은 암호화 통신에 숨겨진 멀웨어를 탐지하고 차단시킬 수 있다. 네트워크 보안장비인 방화벽에 이러한 기능을 탑재해 판매하는 경우가 많은데 실제로는 복호화기능을 사용하지 않는 경우가 많다고 한다. 그 이유는 보안장비의 기존기능 외에 실제 복호화까지 이루어진다면 보안에 소요되는 시간이 길어지고 실시간성이 떨어지기 때문이다. 증가하는 암호화 트래픽에 대응하기 위해서는 복호화 성능에 대한 이슈를 해결할 실질적인 제공이 필요하다.

- **보안 게이트웨이**

  센서 및 모바일들은 성능이 낮기 때문에 멀웨어에 감염되기 쉽다. 낮은 성능을 보안하기 위한 방법은 통합게이트웨이를 활용하는 것이다. 통합 게이트웨이는 센서들의 정보를 모아서 중앙서버에 전달하거나 중앙서버에서 받은 명령을 모바일에 제공하는 역할을 한다. 또한 게이트웨이에 보안기능을 추가해 센서들을 대신하여 악성감염여부를 체크 할 수도 있다. 이러한 방법은 보안게이트웨이가 원격으로 악성감염여부를 검사할 수 있게 하며, 비정상적 인 행위가 발생했을 때 해당 관리자에게 증후를 알려 센서 및 모바일의 사이버 공격을 최소화 시킬 수 있다.

- **통합보안플랫폼**

  클라우드 기술을 통해 중앙시스템에서는 수많은 센서와 모바일 통신이 가능 하다. 이로 인해서 중앙시스템은 게이트웨이 혹은 센서, 모바일들의 현황을 실시간으로 관리해야 한다. 보안도 마찬가지 이다. 지역마다 기능마다 개별적 인 관리가 이루어진다면 관리 화면도 늘어나게 되고 복잡도도 증가해 업무의 효율성이 떨어질 것이다. 그렇게 되면 보안 관리자들은 관리가 필요한 부분들 을 놓치게 되므로 보안은 취약해질 것이다. 이를 예방하기 위해서 통합보안 플랫폼이 필요하다.

  통합보안플랫폼은 중앙시스템과 연계된 모든 기기들의 보안현황을 보여주고 빅데이터를 활용해 이상여부를 자동적으로 판별하거나 우선순위화 해 중요한 이슈들을 먼저 보여줘 보안관리자들의 보안 관리를 돕게 한다. 그렇게 되면 신속한 대응이 가능해져서 보안침해를 빠르게 인지하며 보안 피해를 최소화 할 수 있다.

- **모바일 '인증' 보호기능 강화**

  4차 산업혁명시대에는 우리가 상호작용하고 있는 기기(혹은 모바일)들의 사용접근을 인증할 때 아날로그 방식이 아닌 디지털 방식을 이용하게 될 것이다. 예를 들어 자동차의 경우 열쇠로 문을 열었다면, 요즘은 지문인증 방식으로 문을 열고 닫을 수 있다. 이처럼 모바일 인증기능이 디지털화 되고 있다. 편리 한 만큼 이로 인해 새롭게 발생할 사이버위협 문제를 생각해 보아야 한다.

  자동차를 열쇠로 열고 닫는 것은 단지 열쇠의 모양만 가능했다. 그러나 지문의 경우 사용자의 지문을 인식하기 위해서는 특정 하드디스크에 지문이 저장돼야 한다. 이때 자동차가 네트워크로 연결된다면 해커는 지문이 저장된 하드디스크에 접근해 지문정보를 탈취해 갈 수 있다. 그렇게 되면 자동차를 도난 할 수 있을 뿐만 아니라 지문 인증방식을 사용하는 다양한 곳에 악용될 수 있다.

  이러한 문제점을 해결하기 위해서는 지문정보에 접근하지 못하게 하는 보안시스템이 적용돼야 한다. 그리고 지문정보가 탈취 되더라도 제3자가 열어 볼 수 없게 지문정보를 암호화해야 한다. 그리고 모바일 인증을 이중으로 강화해서 지문이 탈취되더라도 추가피해를 방지할 수 있게 해야 한다. 가령 자동차 문을 열 때 지문만으로 인증하는 것이 아니라 간단한 숫자 암호버튼을 눌러 본인임을 인증하게 한다. 그렇게 하면 해커가 지문정보와 암호번호를 탈취하더라도, 사용자가 다른 곳에 다른 번호로 암호를 설정 해뒀다면 해커는 불법적으로 서비스에 쉽게 접근할 수 없게 된다.

- **클라우드 기반의 실시간성 업데이트**
  4차 산업혁명 시대에는 모든 정보가 클라우드를 기반으로 공유된다. 사이버 보안도 마찬가지다. 보안솔루션 회사들은 클라우드를 기반으로 보안서비스를 제공할 수 있다. 클라우드 기반의 보안솔루션이 세계에서는 큰 인기를 끌며 클라우드 기반 보안서비스 전문 업체인 지스케일러가 큰 주목을 받고 있는 것도 이 때문이다. 지스케일러는 현재 구글에서 8,000억 원을 투자 받았다.
  클라우드는 공급자와 사용자 입장에서 운용 효율성을 증대시켜 비용을 절감시켜준다는 장점이 있다. 이외에도 클라우드 서비스를 이용하면 보안 탐지력을 더욱 강화시켜 준다. 예를 들어 전 세계가 클라우드로 보안서비스를 제공하면, 악성코드 및 보안사건 사고들이 중앙서버인 클라우드에 모이게 되고 그렇게 되면 악성코드, 침해사고 탐지의 정확성을 올려주기 때문에 사이버 공격 탐지가 용이하다.

- **사후대응기술**
  완벽한 것이 없듯이, 보안에도 완벽함은 없다. 하지만 사이버공격을 방지 하기 위해 최대한의 노력을 기울여야 하는 것은 당연하다. 그러나 이러한 노력에도 불구하고 예상치 못한 보안취약점으로 보안이 뚫릴 수 있다. 그 때를 대비해서 사후대응 기술이 필요하다. 어떠한 보안공격이 발생했을 시 미래 발생할 유사한 보안공격에 쉽게 대응하기 위해 공격방법, 공격근원지 등을 파악한 뒤 대응체계를 마련해야 한다. 해외는 이러한 체계가 잘 잡혀있지만, 국내는 아직 많이 부족하다. 4차 산업혁명 시대에는 효과적인 사이버공격 대처가 필요하다. 그래서 해킹공격이 발생 했을 때 이를 분석하고, 취약점을 강화시키는 체계가 마련돼야 한다.

- **물리공격 대응**
  해커는 네트워크가 아닌 센서에 직접 멀웨어를 주입할 수 있다. 이를 인젝션 공격이라고 한다. 사물인터넷으로 수많은 센서들이 설치될 것으로 전망된다. 그리고 센서들은 사람의 눈에 쉽게 띄기 때문에, 그 만큼 인젝션 공격에 노출 되기 쉽다. 하지만 의외로 인젝션 공격방지는 간단하다. 해커가 센서에 직접 접근하지 못하게 하면 된다. 그래서 센서가 있는 장소에 문을 잠그거나 눈에 잘 뛰지 않는 곳에 둬서, 기본적인 공격으로부터 예방할 필요가 있다.