https://doi.org/10.33778/kcsa.2022.22.5.037

스마트시티(그리드, 빌딩, 교통 중심)보안 동향 분석★

김 점 구*

요 약

도시집중 현상이 가속화되고 도시 자원 및 인프라 부족, 교통 혼잡, 에너지 문제 등 이러한 도시 문제를 해결하고 4차 산업 혁명에 선제적으로 대응하기 위해 스마트 시티의 필요성이 전 세계적으로 대두 되고 있는 상황에서 전 세계 스마트시티 기술의 보안이 위험한 상태라는 분석이 지배적이다. 이에 본 논문에서는 스마트시티에 대한 주요 보안 이슈를 대표적인 서비스인 스마트 그리드, 스마트 빌딩, 스마트 교통 부분에 국한하여 기술 및 보안 위협 및 대응에 대해 분석하였다. 향후 스마트시티 구축의 다양한 기술에 대한 분석 및 사이버보안에 대한 연구가 활발히 진행됨에 있어 본 논문이 해결방안 마련의 시작이 될 것으로 기대한다.

Analysis of Security Trends in Smart Cities(A focus on grids, buildings, and transportation)

Jeom-goo, Kim*

ABSTRACT

The need for smart city is emerging all over the world to solve these urban problems such as urban resource and infrastructure shortage, traffic congestion, energy problems and to preemptively respond to the fourth industrial revolution. The analysis that the security of smart city technology is dangerous is dominant all over the world. In this paper, we analyze the technology, security threats and responses of smart city, which are the main security issues of smart city, limited to smart grid, smart building, and smart traffic. In the future, the analysis of various technologies of smart city construction and the research on cyber security are actively progressing, and this paper is expected to be the beginning of the solution plan.

Key-words: Smart City, Security, Analytics, Smart Grid, Smart Transportation

접수일(2022년 11월 30일), 수정일(1차 : 2022년 12월 11일, 2차 : 2022년 12월 14일), 게재확정일(2022년 12월 26일)

* 남서울대학교 컴퓨터소프트웨어학과 교수

★ 본 논문은 2022학년도 남서울대학교 교내연구비 지원에 의해서 연구 되었음

1. 서 론

전 세계 인구는 2050 년 약 100 억 명이 될 것으로 전망되고 있는 가운데 인구의 증가와 기술의 발전으로 인해 도시화율도 꾸준히 증가할 것으로 예상되며, 이에 도시집중 현상이 가속화되고 도시 자원 및 인프라 부족, 교통 혼잡, 에너지 문제 등 이러한 도시 문제를 해결하고 4 차 산업혁명에 선제적으로 대응하기 위해 스마트 시티의 필요성이 전 세계적으로 대두 되었다. 국내에서는 문재인 정부 취임 이후 스마트시티를 신성장동력의 핵심 플랫폼으로 선정하고, 4 차 산업혁명 대응을 선도할 범부처 혁신성장동력 중 하나로써 그 중요성을 강조하고 있으며, 국외에서는 매년 미국 라스베이거스에서 개최되는 CES 의 '18 년 공식 표어는 '스마트시티의 미래(The Future of Smart Cites)'로 교통시스템, 스마트에너지, 스마트 홈 제품 등 미래 도시의 다양한 모습을 예측함에 따라 스마트시티에 대한 관심이 높아지고 있다[1][2].

이에 정부에서는 국가스마트도시위원회 의결을 거쳐, 시범도시 입지 선정('18.1) 및 사업지별 비전과 목표, 주요 콘텐츠를 담은 기본구상 발표('18.7) 등으로 스마트시티는 정부가 아세안 국가들에 적극 자랑하고 있는 핵심사업 중 하나이다[4].

신재생에너지를 통한 에너지 공급, 에너지 관리 시스템을 활용한 수요관리 등 스마트에너지 기술 개발 확대를 위해 스마트시티 국가시범도시로 세종, 부산 등의 경우 유휴 공간, 도로 표면에 태양광 패널을 설치하여 전기를 생산할 예정이며, 전력피크 시 도시의 안정적인 전력 운용을 위해 전력을 저장(Energy Storage System)하고, 에너지를 관리(Energy Management System)할 수 있는 기술 적용을 위해 스마트시티 국가시범도시의 경우 IoT 가전 보급을 통해 피크시간대의 에너지 가동률을 제어하는 기술 적용을 예정하고 있다[5][6]. 또한 수요 자원 거래를 위해 소규모 신재생에너지 설비 증가 및 도시에서 발생한 잉여전력의 효율적인 분배를 위해 전력거래시장 및 기술 적용을 위해 도시 토큰(Token) 발행을 통한 VPP(Virtual Power Plant) 서비스를 적용하여 거주자 간 전력거래를 적용 할 예정에 있다[3][4][7].

미국은 미국 연방정부 스마트시티 정책을 기반으로 스마트 그리드, 의료화 정보화를 위해 에너지・의료 분야 외에는 각 주 정부는 자체적인 스마트 시티 프로젝트를 추진하고 민간 기업에 위임하고 있다. 미 국토교통부(DOT)는 스마트시티, 자율주행차, 드론 등 7 대 산업을 선정하고, 유비쿼터스 도시법에서 스마트시티 도시법을 확대 개편하는 한편 정부주도로 전국 49 개 지자체가 U-City 추진하고 있다[6]. 민간 기업을 중심으로 전개되는 미국 스마트 시장은 IBM, 시스코 등 기업이 스마트시티 솔루션을 구축해 세계 각국 주요 도시를 대상으로 서비스를 제공하고 있다. 특히, IBM 은 스마트시티 분야에서 가장 선진 기업으로 평가되고 있으며 스마트시티 컨설팅, 소프트웨어 구축 및 유지관리 등 솔루션 제공 중심의 사업기반을 구축하고 있다[13][14].

이러한 스마트시티 구축을 위한 기술 개발에 있어 다양한 IoT 기기들이 스마트한 서비스를 위해 필수기능 이외에 추가 기능 모듈이 제공되고 있으나, 보안이 취약한 부분을 통해 다양한 사이버 공격이 야기 되고 있으며, 개인의 프라이버시를 넘어서 사회의 안전에 치명적 영향을 미칠 수 있는 사례들이 지속적으로 발생하고 있고, 그 위협에 대해 많은 논의가 되어 지고 있다[16][17].

따라서 본 논문의 2 장에서는 스마트시티의 기본 개념을 소개하고, 3 장에서는 스마트시티 관련 주요 기술에 대해 기술한다. 4 장에서는 스마트시티와 관련된 보안 위협 및 대응방안에 대해 제시하고, 5 장에서 결론을 맺는다.

2. 스마트시티

2.1 스마트시티 개념

국내・외에 정의된 '스마트시티'에 대한 개념은 명확하게 규정된 것은 없지만, 도시 시설과 공간이 인터넷과 실시간 연결되는 IoT 와 ICT 가 접목되어 이용자들에게 실시간 도시서비스를 제공할 수 있는 도시상태로 정의 되고 있다.

스마트시티 개념은 2017 년 3 월 스마트도시 조성 및 산업진흥 등에 관한 법률(이하 스마트도시법)이 개정되면서 기존의 유비쿼터스 도시(u-시티)를 대체하는 단어로 통용되고 있다. 스마트시티의 정의는 매우 광범위하나 주로 "도시에 디지털 기기, 정보통신기술 등을 활용한 다양한 콘텐츠와 함께 유무선 네트워크, 사물인터넷(IoT) 기술, 5 세대 이동통신(5G), 블록체인 등의 기술들이 접목하여 각종 도시문제를 해결하고 삶의 질을 개선할 수 있는 도시"를 의미한다[1].

이와 유사한 개념으로 "스마트시티(Smart city) 또는 스마트 도시는 다양한 유형의 전자 데이터 수집 센서를 사용하여 자산과 자원을 효율적으로 관리하는 데 필요한 정보를 제공하는 도시 지역이다.24)" 그리고, "도시 운영 및 서비스의 효율성을 최적화하고 시민들과의 연결을 위해 네트워크에 연결된 다양한 물리적 장치인 사물 인터넷과 정보통신기술의 통합이다[17]."로 정의하고 있다. 또한 국외에서 정의하고 있는 스마트시티에 대한 개념은 <표 1>과 같다[4][7][9].

<표 1> 국외 스마트시티 개념

구분	개념
EU	디지털 기술을 활용하여 시민을 위해 더 낳은 공공서비스를 제공, 자원을 효율적으로 사용, 환경에 미치는 영향을 최소화하여 시민의 삶의 질 개선 및 도시
Birmingham City Council (영국)	인적자원과 사회 인프라, 교통수단, 그리고 첨단 정보통신기술(ICT) 등에 투자하여 지속적인 경제발전과 삶의 질 향상을 이룰 수 있는 도시
인도	상하수도, 위생, 보거 등 도시의 공공서비스를 제공할 수 있어야 하며, 투자를 유인할 수 있어야 하고, 행정의 투명성이 높고 비즈니스 하기 쉬우며, 시민이 안전하고 행복하게 느끼는 도시

이외 Gartner 는 "다양한 서브시스템 간 지능형 정보교류를 기반으로 하여 스마트 거버넌스 운영 프레임워크를 기반으로 지속적인 정보 교환을 수해하는 도시"로 정의하고 있으며, Forrester Research[24]에서는 스마트도시는 "주요 인프라 구성요소 및 도시서비스를 만들기 위해 스마트 컴퓨팅 기술을 사용하여 좀 더 지능적이고 상호 연결 되어 있으며 효율적인 도시 관리, 교육, 의료, 공공안전, 부동산 및 유틸리티를 포함 하는 것"으로 개념을 제시하고 있다[18][19].

2.2 스마트시티 주요 분야

스마트시티 구성 분야별 정의에 대해 알아본다. Forest&sullivan 에서는 스마트시티는 산업 구성은 스마트 기반시설, 스마트 거버넌스, 스마트 에너지, 스마트 교통, 스마트 빌딩, 스마트 보안, 스마트 헬스케어로 구분하여 정의하고 있다. 도시문제 해결을 위해 IT 기술 그리고 타 산업과의 융합을 통해 구성되며, 구성 분야별 요소로 다음 <표 2>에서 정의한다[9][10].

Navigant Research 에서는 스마트시티 관련 기술은 스마트 에너지, 스마트 물 관리, 스마트 교통,

스마트 빌딩, 스마트 정부 등 산업별로 구분하여 정의하고 있다. 스마트 에너지의 주요 기술은 스마트 미터, 홈 에너지 관리, 배전 자동화, 그리드 분석, 수요 반응 시스템, 에너지 저장 등이며, 스마트 교통의 경우 지능형 교통시스템, 도로 요금 시스템, 센서 네트워크, 주차 모니터링&관리, 예측분석, 오픈데이터플랫폼 등으로 구성된다[11].

스마트 빌딩은 빌딩에너지 관리시스템, 빌딩자동화시스템, 에너지성능관리, 그리드 통합 등이 있으며, 스마트 정부의 경우 센서 네트워크, 클라우드 컴퓨팅서비스, 데이터분석, 오픈데이터플랫폼, 긴급대응시스템 등을 주요 기술로 분류하고 있다.

앞서 기술한 바와 같이 스마트시티는 매우 다양한 구성 요소를 적용하고 있으며, 국내의 경우 에너지 분야에서 스마트 그리드, 스마트 빌딩, 스마트 교통 등을 주요 대상으로 스마트시티를 적용하고 있는 상황이다. 이에 본 논문에서는 국내 스마트시티의 중점 분야에 대한 기술 및 보안요소를 분석한다[12].

<표 2> 스마트시티 주요 구성 분야별 요소

분야	정의
스마트 에너지	지능형 통합 전송 및 전력 분배에 대한 수요 대응을 위해 첨단 미터 인프라(AMI), 배전관리 및 고전압 전송 시스템을 위해 디지털 기술을 사용
스마트 빌딩	조명, 온도, 보안 및 에너지 소비를 독립적으로 또는 최소한의 사람 개입으로 제어 및 관리하는 첨단 자동화 인프라로 친환경적, 에너지 효율적 시스템
스마트 이동성	저공해 자동차 및 다양한 운송 시스템과 같은 혁신적이고 통합된 기술 및 솔루션을 사용한 지능형 이동성
스마트 기술	스마트 그리드 시스템, 스마트 홈 솔루션, 고속광대역 연결 및 4G 기술 등으로 집, 사무실, 휴대폰 및 자동차를 단일 무선 IT 플랫폼에 연결
스마트 헬스 케어	e-health 및 m-health 시스템과 지능형 연결 의료기기를 사용, 건강 모니터링 및 진단은 물론 시민들의 건강, 웰니스, 웰빙을 장려하는 정책 시행
스마트 기반 시설	에너지 그리드 , 운송 네트워크, 수자원 및 폐기물 관리 시스템, 통신과 같은 다양한 유형의 지능형 인프라를 관리, 통신 및 통합하는 지능형 및 자동화 시스템
스마트 정부& 교육	인센티브, 보조금 또는 기타 홍보를 통한 친환경 및 지능형 솔루션 채택을 지원하는 정부 정책 및 디지털 서비스
스마트 보안	사람, 재산 및 정보를 보호하도록 설계된 비디오 감시, 공공 안전 및 관리 보안 서비스와 같은 기술 및 솔루션 포함
스마트 시민	일상적인 활동에서 스마트하고 친환경적인 솔루션을 채택하는데 관심을 가지고 있는 시민

3. 스마트시티 주요 기술

3.1 스마트 그리드

스마트 그리드는 기존 전력망에 ICT 를 접목하여 전력공급자와 소비자가 양방향으로 실시간 정보를 교환, 에너지효율을 최적화 하는 차세대 전력

망이다. DOE(Department of Energy)에 따른 핵심 기술 부문은 통합된 양방향 통신, 고급 구성요소(초전도성, 결함 공차, 과도한 전기 저장, 스마트 기기 및 진단장치), 고급제어방식, 감지 및 측정기술(스마트 그리드 안전성, 상태 및 보안 기능 지원), 향상된 인터페이스 및 결정지원 기술 및 유비쿼터스 방식 제공으로 분류하고 있다[20][22].

<표 3> 스마트 그리드분야별 주요 기술

기술 영역	시스템&소프트웨어
광역 모니터링 및 제어	· 감시제어 및 데이터수집(SCADA) · 광역 모니터링 시스템(WAMS) · 광역 적응 보호, 제어 및 자동화 (WAAPCA) · 광역 상황인식 시스템(WASA)
정보통신 기술통합	· 전사적 자원관리(ERP) 소프트웨어 · 고객정보시스템(CIS)
재생에너지 및 분산발전 통합	· 에너지 관리 시스템(EMS) · 배전 관리 시스템(DMS) · 감시제어 및 데이터수집(SCADA) · 지리 정보 시스템(GIS)
송전망 고도화	· 네트워크 안정성 분석 · 자동복구시스템
배전망 관리	· 지리 정보 시스템(GIS) · 배전 관리 시스템(DMS) · 정전 관리 시스템(OMS) · 인력 관리 시스템(WMS)
원격검침 인프라 (AMI)	· 계량데이터 관리 시스템(MDMS)
전기 자동차 충전 인프라	· 에너지 비용청구 · 스마트 G2V 충전 및 V2G 방전
고객측 시스템	· 에너지 대시보드 · 에너지 관리 시스템 · 스마트폰과 태블릿용 에너지 관리 앱

IEA(International Energy Agency)의 주요 기술은 광역 모니터링 및 제어, 정보통신기술 통합, 재생에너지 및 분산발전 통합, 송전망 고도화, 배전망 관리, AMI, 전기자동차 충전 인프라, 고객 측 시스템 등으로 영역을 분류한다[23]. <표 3>은 스마트 그리드 기술 분야별 주요 기술 중 시스템과 소프트웨어 부분에 대해 정리한다[8].

3.2 스마트 빌딩

<표 4> 스마트빌딩 주요 구현 서비스[25]

구분	기술 분류	구현 서비스
빌딩 에너지관리 시스템	빌딩전용 플랫폼	조명 · 공기조화 · CCTV 통합 관리 플랫폼, 제로에너지 빌딩(ZEB) 기술 개발
	전력 에너지	무선통신으로 소비전력을 통제하는 네트워크 스위치
	기타 에너지	방축열을 이용한 인공지능 냉방 시스템, 빌딩 탄소 제어 시스템
빌딩 보안 / 관리	보안 시스템	실시간 CCTV 이미지 분석을 통한 보안
	관리 시스템	빌딩 주차장 무인관리 시스템

Deloitte 에서 정의한 스마트 빌딩은 “기본적으로 최적화된 빌딩 및 운영 자동화와 지능형 공간 관리를 결합하여 사용자 경험을 향상시키고, 생산성을 높이며, 비용을 절감하고, 물리적 및 사이버 보안 위험을 완화하는 디지털 연결 건축물”을 의미한다[20][21].

또한, 스마트빌딩은 “건물에너지관리 시스템(Building Energy Management System)으로 빌딩 내 에너지 관리 설비의 다양한 정보를 실시간 수집·분석하여 에너지 사용 효율을 개선하는 시스템 기술로서 스마트시티에 적용 가능한 응용 기술”로 정의하고 있다. 스마트 빌딩에 적용되는 주요 기술은 스마트 빌딩 자동화 시스템, 사무자동화, 정보통신, 시스템 통합 등의 기술이 적용된다.

스마트 빌딩 자동화 시스템은 다목적(주거 및 비주거)의 빌딩에서 전통적인 제어(HVAC (Heating, Ventilating and Air Conditioning) 포함)를 위한 BAS(Building Automation System)와 시설 및 설비 제어를 위한 BMS(Building Management System)뿐만 아니라 에너지 효율적인 관리를 위한 EMS(Energy Management System) 또는 BEMS (Building EMS)를 포함하고 있다.

스마트 빌딩은 가장 많은 수의 IoT(Internet of things) 기기가 적용됨에 따라 스마트 빌딩의 주요 설비 및 위에에 IoT 센서를 적용하여 상황을 모니터링 하고 이를 기반으로 지능적인 최적의 운영을 지원하게 된다. 다음 <표 4>에서 스마트 빌딩의 주요 구현 서비스 기술을 정리 한다[15].

3.3 스마트 교통

스마트 교통은 도시의 핵심 문제인 교통체증 문제의 해결을 위하여 스마트시티 구축을 위해서 AI (Artificial Intelligence)기술과 빅데이터 분석 기술 등을 활용하여 스마트 교통 서비스를 제공하고 있다. 스마트 교통에서는 접근성의 향상, 안전한 교통 그리고 효율적이고 지능적인 교통시스템을 특징을 가지고 있으며, 스마트 교통은 도시 내 자율주행차량의 운행을 위한 교통 인프라와 효율적인 교통 정보 체계 중심의 기술 개발을 통한 스마트 교통을 구현하고 있다.

지능형 교통 체계를 실현을 위해 교통 인프라를 통해 수집된 자료를 활용하여 자율주행차량의 안전하고 효율적인 주행을 지원하기 위해 차세대 첨단교통체계(C-ITS : Cooperative Intelligent Transport System) 기술이 적용된다. 앞서 기술한 바와 같이, 스마트시티에서 교통은 ICT, IoT, Big Data,인공지능 등을 활용하여 타 분야와 연계되고 통합된 교통시스템, 스마트하고 지능화된 교통시스템, 시민이 참여하는 교통시스템, 편리한 교통시스템이 되어야 한다.

현재 국내에서는 스마트 하이웨이 사업(여주)과 C-ITS 시범사업(대전-세종 간)을 추진하였으며 한국교통연구원은 공공의 관측교통량 자료와 민간 네비게이션 데이터를 융합하여 교통량을 측정하는 ‘View T 1.0’ 기술을 개발하여 활용할 예정이다[26].

스마트 교통의 통신제어 부분의 핵심기술은 V2X(Vehicl to Everything)로 각광 받고 있다. 차량이 주행하면서 도로 인프라 및 다른 차량과의 지속적인 상호통신을 통해 각종 정보의 교환 및 공유를 지원하는 V2X 기술은 차량간 통신(Vehicle to Vehicle Communication)과 차량과 노변 기지국 간 통신(Vehicle to Infrastructure Communication)을 축약한 단어로 미국과 유럽에서 C-ITS(Cooperative Intelligent Transport Systems) 서비스 구현을 위한 통신기술 표준인 WAVE(Wireless Access in Vehicular Environment)의 기본 통신 기술을 적용한다.

4. 스마트시티 보안 위협 분석

4.1 스마트 그리드 보안 위협 및 대응

스마트 그리드에 대한 사이버 공격을 가능하게 하는 보안위협 요소는 크게 4 가지로 정의할 수 있다. 첫째, 스마트 미터, 전력공급업체, 관리업체 사이에 양방향 통신기술을 사용하여 침투경로로 활용되어 보안 위협이 증가되는 점이다. 둘째, 스마트 그리드는 상용 하드웨어와 소프트웨어 사용 증가로 인한 위협 요소이다. 이는 개방형 아키텍처를 도입하여 시스템 정보 및 취약점이 외부에 노출되는 상용 기술을 많이 사용하기 때문으로 분석된다. 셋째, 소비자단에서 스마트 그리드 시스템으로 수천만 대의 스마트 미터, DCU 등이 전력망에 연결할 수 있어 접근 가능한 지점의 증가로 인한 위협이 증대된다. 넷째, 스마트 미터, 배전 FIED 등의 스마트 그리드 장비가 광범위한 지역에 물리적 분산되어 보안 관제 측면의 문제점의 보안 위협이 존재한다. 이러한 위협으로 인해 발생할 수 있는 대표적인 스마트 그리드 보안 이슈는 다음 <표 5>와 같이 분류할 수 있다. 또한, 국내 스마트 그리드 보안 위협 및 대응에 대한 표준화는 TTA 의 “스마트 그리드 보안 요구 사항”으로 제공되고 있다.

기존의 다양한 연구 분석 결과와 같이, 스마트 그리드 기술의 경우 AMI, 네트워크, DB 등 여러 기기들로 구성되어 있기 때문에, 공격에 대한 경로가 매우 다양하다. 결과적으로 스마트그리드 보안 요소에 따라 우선 중요 위험유형에 대해 대응 방안을 적용하여 중점적으로 관리할 필요가 있다.

스마트 그리드 전력망에 사이버테러가 발생 하는 경우 사회적, 경제적인 혼란과 피해는 기존 전력망을 운영하는 경우 보다 확대되어 나타날 수 있어 적극적인 대응이 필요하며, 스마트 그리드 보안 요구사항을 파악하기 위해서 신규 네트워크 구축, 서비스 개발, 시스템 및 기기 운용 등 ICT 기술 융합과정에서 발생할 수 있는 보안위협 요인에 대한 다각적인 분석이 필요할 것이며, 다양한 운영 도메인 및 도메인 간 연계구간, 스마트 그리드기기 배치, 다양한 시스템 및 기기의 조합 등으로 인한 보안위협 요인에 대한 분석이 요구된다.

<표 5> 스마트 그리드 보안 이슈

항목	보안 이슈
전력공급 중단	· 해커의 공격으로 인한 전력 공급 중단 발생 가능 · 전력 사용을 필요로 하는 산업의 대규모 피해 발생 · 전력 차단은 다양한 사회 인프라 공격으로 확대 가능 · 예비 전력을 공급받을 수 있는 대체 수단 필요
개인정보 유출	· 전력 공급자와 사용자간의 양방향 통신을 사용 · 해킹으로 인한 개인정보 유출 가능(소유 가전제품, 세입자의 전력 사용량, 개인행동 패턴, 실시간 감시)
전력사용 통제권 상실	· 해커의 개별 전자제품의 전력공급 제어 가능 · 비정상적인 외부 통제에 의해 소비자가 전력을 자유롭게 사용하지 못한다는 위협 발생 · 사용자의 통제권 상실로 인한 문제(냉난방기구, 생명유지장치, 경쟁회사 전력시스템 공격)
스턱스넷	· 악성코드를 통한 전력망 제어시스템 공격

4.2 스마트빌딩 보안 위협 및 대응

스마트빌딩에 대한 보안의 경우 정부청사 공시생 침입사건, 인천공항 밀입국 사건 등의 발생 이후 빌딩보안에 대한 관심이 높아지고 있으며, 전통적인 빌딩 보안 시스템은 별도의 하드웨어와 소프트웨어, 설치, 감시, 서비스, 유지보수 등이 개별적으로 구비 되어 있으며, 현대적인 빌딩에 내장된 웹 기반 지능형 기기 대다수는 자체 보안 기능을 갖추고 있지 않아 건물 운영을 저해하고 안전상의 위험을 가할 수 있는 공격에 무방비로 노출되어 있다. 이처럼 제대로 된 보호를 받지 못하는 스마트 빌딩 관리 시스템은 악의를 가진 공격자가 기업의 경영 시스템에 침투할 수 있는 새로운 수단을 제공할 수 있다.

이러한 취약점은 '14 년 미국 타겟(Target)에서 발생했던 막대한 규모의 데이터 절도와 같이 누군가에 의해 타겟의 '난방, 환기, 공기조화(Heating, Ventilation and Air Conditioning)' 시스템을 관리하고 있는 업체의 접속인증 데이터가 도용되어 발생한 것이다. 이러한 문제는 보편적으로 발생할 수 있는 문제이며, 스마트빌딩에 통합된 기기의 대부분은 현재 자체 보안 기능이 내장되어 있지 않으며, IT 영역과 보안에 대한 고려되고 있지 않은 업체로부터 공급받고 있기 때문에 발생되는 문제이기도 하다.

빌딩 자동화 네트워크가 위협에 노출된 가능성이 확대됨에 따라 시스템에 대한 하나의 취약점은 모든 빌딩 시스템과 네트워크에 대한 심각한 사이버보안 사고가 야기 된다. 이러한 사이버보안 사고에 대응하기 위해 정보보안 및 사이버보안 관리 프로세스 관리 영역을 빌딩 관리시스템으로 확대하여 관리해야만 한다. 모든 스마트빌딩 시스템은 네트워크 분리, 강력한 인증 및 네트워크 모니터링을 등을 고려하고 빌딩과 관련된 시스템을 체계적이고 지능화하여 상호 연결을 통한 통합 보안의 형태로 진화되어야 한다.

이러한 문제 인식은 Honeywell, AXIS, 하이크비전 등 세계 보안업체들은 방문객 얼굴 인식 및 동선 추적 및 멀티팩터인증(MFA) 기반 출입통제 시스템, 지능형 CCTV 솔루션 개발을 지속 추진하고 있다. 지능형 CCTV 솔루션은 침입, 배회, 유기, 쓰러짐, 피플카운팅, 연기감지, 얼굴인식 기반 추적 등 이 있으며 정확도를 증가 시키는 것을 관건으로 하고 있으며, 중앙통제센터에서 모니터링에 대한 지능화를 통해 무인 경비 등의 인력 절감을 통한 효율적 운영을 도모해야한다.

4.3 스마트 교통 보안 위협 및 대응

한국인터넷진흥원(KISA)이 발표한 "스마트교통 사이버보안 가이드"에서는 스마트교통의 주요 보안위협을 물리적 위협, 모바일 기기조작, 펌웨어 조작, 메시지 위·변조, 중계공격, Dos 공격, 미숙한 서비스 관리, 사용자 부주의 등으로 정의하고 있다.

본 논문에서는 스마트 교통 보안 위협 중 통신 제어 부분에 대한 보안 위협에 대해 기술한다. 스마트 교통에서 차량의 구성요소와 외부와의 연결을 제어하는 텔레매틱스 서비스, V2X 통신의 서비스 등 다양한 연결 서비스를 제공하게 된다.

본 논문 3.2 에서 기술한 바와 같이 네트워크를 위해 차량 간, 차량 대 기반 통신 등 V2X 서비스에는 DSRC(Dedicated Short Range Communications) 방식의 WAVE(Wireless Access in Vehicluar Environments) 통신 등이 사용되고 있으며, L

TE, 5G 등 셀룰러 통신이 사용될 수 있다. 또한, 블루투스, Wi-Fi, USB 등을 통해 차량 내에서 외부 기기와 연결이 가능하다. 이처럼 스마트 교통은 스마트 교통은 유·무선 네트워크 환경을 기반으로 하고 있기 때문에 사이버보안 침해사고 위협 중 통신제어의 취약점에 대해 우선적인 고려가 필요하다. 차량 내·외부 데이터, 소프트웨어, 펌웨어의 업데이트의 경우 인증, 무결성, 접근 제어 정책, 암호화에 대한 고려, 각 통신구간에 대한 비정상적인 통신 탐지 및 이에 대한 대응, 비정상적인 출처 및 경로를 통해 유입되는 데이터 등에 대한 신속한 대응이 가능한 사이버 보안 대책이 적용되어야 할 것이다.

5. 결론

스마트시티 구축에 대한 다양한 추진 방식, 다양한 비즈니스 모델 분석·개발에 대한 연구가 활발히 진행되어야 할 것이다. 그러나 무엇보다 선행되어야 할 과제는 스마트시티 구축에 대한 보안 적용이며, 광범위적인 논의를 통해 정책적인 절차와 전략이 뒷받침되어야 사이버보안 사고에 대응 할 수 있다. 국내는 국외에 비해 스마트시티 보안에 대한 고려와 적용이 매우 낮으며, 현재 체계적인 보안에 대한 기술 분석 및 대응 방안에 대한 연구가 미흡한 실정이다.

이에 본 논문에서는 스마트시티에 대한 주요 보안 이슈를 대표적인 서비스인 스마트 그리드, 스마트 빌딩, 스마트 교통 부분에 국한하여 기술 및 보안 위협 및 대응에 대해 기술하였다. 향후 스마트시티 구축의 다양한 기술에 대한 분석 및 사이버보안에 대한 연구가 활발히 진행되어야 할 것이다.

참고문헌

[1] 국토교통부 홈페이지, https://www.molit.go.kr/USR/WPGE0201/m_36673/DTL.jsp

[2] 갈수록 똑똑해지는 스마트 빌딩, DIGIECO, 2017.

[3] 교통 분야 ICT 융합 제품·서비스의 보안 내재화를 위한 스마트교통 사이버보안 가이드. KISA. 2018.

[4] 국가건축정책위원회, Smart City 경쟁력 강화를 위한 정책방안 연구, 2019.12.

[5] 국내 스마트조명 추진을 위한 국내·외 스마트시티 개념과 스마트시티와 U-City 비교, 박창용 외, 한국조명전기설비학회 학술대회논문집, 2018.

[6] 도시 빅데이터를 활용한 스마트시티의 교통 예측 모델, 장선영 외, 한국BIM학회논문집, Vol. 8, No. 3, 2018.

[7] 미국의 스마트시티 지원 정책 및 시사점, 김규연, 산은조사월보, 2019.

[8] 세계 스마트그리드 시장 생태계 분석, Weekly KDB Report, 2018.

[9] 세계 스마트그리드 시장 생태계 분석, 김혜진, 산업기술리서치센터. 2018.

[10] 스마트그리드 보안기술 동향분석 및 대응방안, 유성민 외, 한국통신학회지, Vol. 31, No. 5, 2019.

[11] 스마트시티 ICT·SW 핵심, 플랫폼, 신명숙 외, NIPA, 2019.

[12] 스마트시티 국제표준화 동향, 한국전자통신연구원, 2018.

[13] 스마트시티 보안 관련 보고서 발표, 월간 디지털정부 최신 해외 정책·기술 동향, 2017.

[14] 스마트시티 상호운용성 검증 및 시험인증 동향, 한국정보통신기술협회, 2018.

[15] 스마트시티 이슈 해결을 위한 정책프레임워크 개발방향에 관한 연구, 장환영, 한국산학기술학회논문지, Vol. 19, No, 5, 2018.

[16] 스마트시티 플랫폼, 한국기업데이터(주), 2019.

[17] 스마트시티의 보안을 위한 사이버보안위협정보 활용 연구, 김현진 외, 디지털콘텐츠학회논문지, Vol. 20, No. 6, 2019.

[18] 위키피디아. https://ko.wikipedia.org/wiki/%EC%8A%A4%EB%A7%88%ED%8A%B8_%EC%8B%9C%ED%8B%B0

[19] 제3차 스마트도시 종합계획(2019~2023), 국토교통부, 2019.

[20] 지능형전력망 제2차 기본계획(2017~2021) 수립을 위한 사전연구 최종보고서, 한국스마트그리드사업단, 2017.

[21] A survey on smart grid technologies and applications. Elsevier. vol. 146, pp. 2589-2625. 2020.

[22] For information, contact Deloitte Anjin LLC, 2019.

[23] IEA, "Smart Grids Technology Roadmap", 2019.

[24] IoT 오픈 플랫폼 기반 제품서비스 개발을 위한 IoT와 oneM2M의 이해, NIPA, 2017.

[25] Matt Hamblen, Just what IS a smart city?, computerworld.com, Oct 1, 2015.

[26] Strategic Opportunity Analysis of the Global Smart City Market, Frost&Sullivan. 2013.

[27] 2018 전자정부기술트렌드, 한국정보화진흥원, 2018.

[28] 4차 산업혁명시대의 스마트시티 현황과 전망, 김기봉 외, 한국융합학회논문지, Vol. 9, No. 9, 2018.

〔저자소개〕

김 점 구 (Jeom Goo Kim)
1990년 2월 광운대학교
전자계산학과 이학사
1997년 8월 광운대학교
전자계산학과 석사
2000년 8월 한남대학교
컴퓨터공학 박사
1999년 3월~ 현재
남서울대학교
컴퓨터소프트웨어학과
교수
email : jgoo@nsu.ac.kr