Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.1, Feb. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.1.123

제로 트러스트(Zero-Trust) 기반의 스마트시티 공급망 보안모델 연구*

이 현 진,[1†] 손 경 호[2‡]
[1,2]강원대학교(대학원생, 교수)

A Study on a Smart City Supply Chain Security Model Based on Zero-Trust*

Hyun-jin Lee,[1†] Kyung-ho Son[2‡]
[1,2]Kangwon National University(Graduate Student, Professor)

요 약

최근 다양한 도시문제로 세계적으로 국가와 기업에서 스마트시티 개념을 도입한 문제 해결 연구가 진행 중이다. 스마트시티는 도시의 ICT를 융합하고 도시의 모든 구성요소를 네트워크로 연결하여 데이터를 수집·전달하며, 다양한 IoT 제품이나 서비스로 구성된 공급망으로 이뤄져 있다. 스마트시티의 여러 사이버 보안 위협 및 공급망(Supply-Chain) 위협 증가는 불가피하며, 이에 대응하기 위해 공급망 보안 정책 등 프레임워크 수립과 더불어, 제로 트러스트(Zero-Trust) 관점에서 데이터 연계에 따른 각 데이터 제공자·서비스 등의 인증과 적절한 접속통제가 필요하다. 이를 위해 국내에서도 스마트시티 보안 위협을 위한 스마트시티 보안모델이 개발되었으나, 공급망 보안과 제로 트러스트와 관련된 보안 요구사항은 부족한 실정이다. 본 논문에서는 해외 스마트시티 보안 동향을 살펴보고, 정보보호 및 개인정보보호 관리체계(ISMS-P)와 국제표준으로 등록된 ICT 공급망 보안에 대한 보안 요구사항을 비롯해, Zero-Trust 관련 기술을 국내 스마트시티 보안모델에 적용하기 위한 보안 요구사항을 제시하고자 한다.

ABSTRACT

Recently, research on solving problems that have introduced the concept of smart city in countries and companies around the world is in progress due to various urban problems. A smart city converges the city's ICT, connects all the city's components with a network, collects and delivers data, and consists of a supply chain composed of various IoT products and services. The increase in various cyber security threats and supply chain threats in smart cities is inevitable, in addition to establishing a framework such as supply chain security policy, authentication of each data provider and service according to data linkage and appropriate access control are required in a Zero-Trust point of view. To this end, a smart city security model has been developed for smart city security threats in Korea, but security requirements related to supply chain security and zero trust are insufficient. This paper examines overseas smart city security trends, presents international standard security requirements related to ISMS-P and supply chain security, as well as security requirements for applying zero trust related technologies to domestic smart city security models.

Keywords: SmartCity Security, Supply Chain, Zero Trust

Received(11. 26. 2021), Modified(12. 28. 2021), Accepted(01. 06. 2022)

* 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2020-0-00185, 공급망 장비에 대한 하드웨어 보안 및 신뢰성 검증 기술 개발). 이 논문은 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(No.2021-0-00613, 언택트 시대의 기업망 보호를 위한 제로 트러스트 기반 접근제어 및 이상징후 분석기술 개발).

† 주저자, lee@kangwon.ac.kr
‡ 교신저자, khson@kangwon.ac.kr(Corresponding author)

I. 서 론

최근 도시의 노후화, 교통체증, 환경오염, 인구집중 등의 다양한 도시문제가 발생하고 있어, 다양한 국가와 기업에서는 ICT 기술을 이용해 도시 생활에서 발생하는 문제를 스마트시티(Smart City) 개념을 도입하여 위와 같은 문제를 해결하려 하고 있다. 스마트시티는 ICT를 도시에 적용하여 도시와 시민들의 삶의 질을 높이는 목적을 두고 있다. 4차산업혁명 시대가 도래함에 따라, IoT, 5G, 빅데이터, AI 등과 같은 기술을 활용하여 교통, 에너지, 헬스케어, 교육, 환경, 안전, 생활 분야에 이런 기술들을 적용하고 각 분야에서 발생하는 데이터를 상호 연계하거나 결합하는 형태로 스마트시티가 변화되고 있다.

스마트시티는 도시의 모든 구성요소를 네트워크에 연결하여 데이터를 수집하고, 수집된 데이터를 활용하여 다양한 서비스를 제공하고 있으므로 기존의 ICT 환경에서 발생하는 해킹, 개인정보 유출 등의 보안 문제들이 스마트시티 환경에도 그대로 전이되고 있으며, 생활 속에 다양한 사이버 보안 위협이 존재한다. 최근, 스마트시티의 헬스케어 서비스를 대상으로 랜섬웨어, 하드웨어 트로이 같은 사이버 공격은 치명적이다. 2017년에는 미국의 한 지역의 CCTV가 랜섬웨어에 의해 오작동하였고, 2018년 3월에 애틀랜타시는 랜섬웨어 공격을 받아 수백 개의 온라인 서비스와 경찰의 카메라 녹음, 법률 기록 등이 분실되었다. 2018년 7월에는 싱가폴의 SingHealth DB가 해커의 공격을 당해 150만 명의 병원의 환자의 건강 데이터가 유출되는 사고가 발생하였다. 2019년 1월에는 빌딩의 자동화 시스템의 취약점이 발표되어, 11,000대 이상의 기기가 취약점에 노출되는 등 스마트시티의 발전과 비례하여 사이버 보안 문제가 증가하고 있다.

이에 대응하기 위해 미국, EU를 비롯해 우리나라에서도 안전한 스마트시티를 구축하기 위한 보안 프레임워크(체계), 보안요구사항 등을 개발해 제시하고 있다.

특히, 미국 NIST(미국 표준기술연구소)에서는 글로벌 스마트시티 협업을 위한 GCTC(Global City Teams Challenge) 프로그램을 시작하여 스마트시티 관련 솔루션 개발 및 구현을 위한 모범 사례와 기술 지침을 제공하기 위해 NIST SCCF(Smart Cities and Communities Framework)를 제공하고 있으며, 특히, CPAC (Cybersecurity and Privacy Advisory Committee)에서 스마트시티의 사이버 보안과 프라이버시를 위한 위험 관리 가이드북을 개발해 제공하고 있다[1].

일본에서는 스마트시티가 지역마다 다른 기준으로 설계되므로 구성요소를 정형화하는 것이 어려워 일본의 내각부에서는 “Smart City Reference Architecture”를 정의하였다. 보안과 관련해서는 이 문서를 기반으로 스마트시티의 주체별 IoT 디바이스, 데이터 활용 인프라, 서비스, 데이터 공유 등에 대한 보안대책 수립을 위해 총무성에서 “Smart City Security Guideline ver 2.0”을 발표하였다[3].

국내에서도 한국인터넷진흥원(KISA)에서 ‘스마트시티 보안모델’을 개발해 스마트시티의 핵심 역할을 수행하는 스마트시티 통합플랫폼의 보안요구사항을 정의하고, 이를 점검할 수 있는 체계를 구축하기 위한 보안모델을 제시하고 있다[12].

스마트시티 설계에 있어 기본적인 사이버 보안 관리 외에도 공급망(Supply-Chain) 보안 관리 부재가 발생할 경우, 스마트시티 내 시스템, IoT 기기 등을 이용하기 위한 아웃소싱 위탁기업에서 악의적인 목적 또는 보안에 취약하여 악성코드에 감염되었을 때, 데이터 유출을 비롯하여 많은 스마트시티 이해관계자의 피해를 초래할 수 있다. 또한, 데이터 연계와 원격 접속이 활발히 이루어지는 스마트시티에서 네트워크 접속과 관련되어 한계점이 분명히 존재하는 네트워크 망분리 접근통제만으로는 고도화되는 사이버 위협에 취약하다. 이러한 보안 문제 해결을 위해 스마트시티에 공급망 체계가 갖춰져야 하는 보안 요구사항이 필수적이며, 나아가 데이터 연계 시 확실한 보안을 위해 네트워크 망분리를 통해서만 데이터 연계를 진행하고 있는 현재 스마트시티 보안모델을 제로트러스트 기술을 기반으로 스마트시티를 설계할 수 있어야한다. 그러나 국내 보안모델은 공급망 리스크에 대한 문제와 스마트시티에 참여하는 여러 서비스에 산재하는 데이터를 연계하여 분야·조직을 초월한 데이터 활용과 서비스 제공을 가능케 하기 위한 데이터 연계 시의 데이터의 근원지 파악과 객체의 접근권한 제어 등의 보안문제 해결을 담고 있지는 않다.

본 논문에서는 스마트시티 보안과 관련되어 국내 및 해외 스마트시티 보안모델과 안전한 보안 관리를 위한 ISMS-P 인증기준 비교 분석을 진행하고, 공급망에서의 일정 수준 이상을 보안을 담보하기 위한 요구사항, 데이터 연계 시 신뢰할 수 있는 네트워크

를 위한 적절한 인가 없이는 아무것도 신뢰하지 않는 제로 트러스트(Zero - Trust) 관점에서의 보안모델과 요구사항을 제시하고자 한다.

II. 국내 스마트시티 보안모델

국내에서 스마트시티와 관련해 도시 성장의 단계별 접근, 도시 가치를 높이는 사람 중심의 맞춤형 기술 도입 및 주체별 역할 강화인 세 가지 전략을 토대로 적극적인 스마트시티 플랫폼을 추진하여 2023년까지 전국적으로 스마트시티 통합플랫폼을 구축할 계획이다.

안전한 스마트시티 구축을 위해 한국인터넷진흥원(KISA)에서는 스마트시티 플랫폼 구축에 있어 효과적인 보안을 위해 국내 및 해외의 스마트시티 서비스 동향 분석과 스마트시티 서비스 보안모델, 해당 보안모델의 검증 방법 등을 제공하고 있다[12]. KISA의 스마트시티 보안모델에서는 세계적으로 시행 또는 개발하고 있는 보안 프레임워크와 스마트시티의 보안 위협을 도출하고, 그에 맞는 스마트시티 보안모델을 제안하면서 국내 스마트시티 플랫폼 구축을 위해 필요한 보안요구사항 및 보안대책을 제시하고 있다. 스마트시티와 관련된 국내외 표준과 기술 동향은 살펴보고, 스마트시티를 인프라 분야, 플랫폼 분야, 서비스 분야로 나누어 각 분야의 표준화 개발 기구와 표준화 추진 상황을 설명하고 있다.

또한, 스마트시티 서비스 보안모델을 제안하기 위해 스마트시티 서비스 내 위협을 분석할 때, 스마트시티 서비스는 크게 U-City 통합플랫폼 기반 서비스와 스마트시티 통합플랫폼 기반 서비스의 두 가지로 나눈다. U-City 통합플랫폼을 기반으로 한 서비스 내 위협 분석을 위해 해당 서비스의 현황분석을 진행하여 서비스 구성에 따른 인프라, 디바이스, 연계망 등 침투 가능한 영역과 외부자, 내부자, 내·외부 연계 관점별로 침투 포인트를 식별한 이후, 침투 포인트를 활용한 시나리오 수립을 통해 상세한 침투 시나리오를 고려하고 있다.

스마트시티 통합플랫폼 기반 서비스에는 플랫폼과 플랫폼 및 서비스 간 연계와 플랫폼과 디바이스 간 연계 두 가지로 나누어 현황을 분석하고 위협을 도출하고 있다. 플랫폼 간 및 서비스 간 연계에서 각 플랫폼과 데이터 연계 단계에서 API 연동 시 인증 우회, 비인가 접근 등의 위협 시나리오와 그에 대응하는 방안을 도출한다. 또한, 망 연계 단계에서 자료전송 시 정보 노출, 암호키 등 위협 시나리오와 대응방안을 도출하여 보안 위협에 따른 보안 요구사항을 설명한다. 플랫폼과 디바이스 간 연계에서는 각 플랫폼과 사용자, 서비스 활용기관별 서비스 흐름을 분석하고 흐름에 따라 총 4가지로 구분하여 공격 시나리오를 수립한다. 시나리오 기반 도출 위협은 크게 정보보호 고려사항인 무결성, 기밀성, 가용성, 프라이버시, 인증 등으로 보고 세부 위협에 대한 내용을 설명한다.

이처럼 KISA의 스마트시티 보안모델은 보안 가이드 동향에서 제시하는 접근통제, 물리적·소프트웨어 보안 등의 요구사항과 U-City 통합플랫폼 기반 서비스, 플랫폼 및 서비스 간 연계, 스마트시티 관련 사고사례의 요구사항 공통점을 매핑하여 정리하고 있으며, 이를 통해, 스마트시티 보안모델의 세부 요소를 규정할 수 있으며, 스마트시티의 구성요소를 고려하여 보안모델을 수립해야 함을 기술하고 있다.

또한, 스마트시티와 관련된 국내외 표준, 기술, 보안 프레임워크, 보안 가이드 등을 고려하여 Fig 1과 같이 스마트시티 보안모델 개념을 정의하고 있다.

정의한 스마트시티 보안모델에서 보안 관리, 서비스, 디바이스, 통합플랫폼 등 영역별 보안 요구사항을 기준, 세부 질의 항목, 세부 설명으로 나누어 제시한다. 해당 보안모델을 적용할 때, 스마트시티 보안 점검을 통해 각 지방자치단체에서 운영하거나 운영 예정인 스마트시티와 제시한 보안모델과의 차이가 발생하는지 조사하고 조치한다. 보안 점검 절차는 대상 식별, 항목 조정 및 점검, 대책 수립 및 조치 순이다. 먼저, 보안모델 적용을 위해 위 모델에 제시된 영역별 대상을 식별한다. 대상 식별 이후 보안모델에

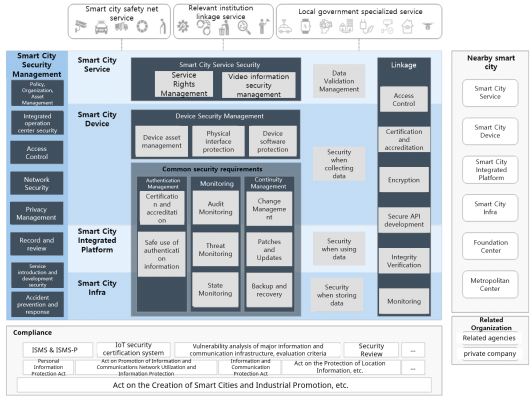

Fig. 1. Concept of Smart City Security Measures

서 제시하는 스마트시티 구성요소와 차이가 발생하는 유형과 항목을 찾아 조정한다. 제시한 보안모델 영역 중 스마트시티 인프라에 해당하는 세부 유형은 서버, 통합 DB, 네트워크 장비 등이 있다. 스마트시티 보안모델을 검증하는 방법으로 각 영역에 대한 분야와 해당 분야의 항목에 대해 상세 내용을 제시하고 있으며, 내용에 대한 이행 지침이 존재하여 스마트시티를 구축하고자 할 때 적용할 수 있도록 제시하고 있다.

해당 보안모델의 요구사항은 스마트시티의 서비스, 디바이스, 네트워크 등 전반적인 보안 요구사항을 포괄하고 있으나, 공급망 관련 요구사항이 외부자 관리나 소프트웨어 변경이력 관리에만 국한되어 있어, 공급망 보안 요구사항이 부족한 것을 확인할 수 있다.

III. 해외 스마트시티 보안 가이드(지침)

본 장에서는 미국의 스마트시티 보안 프레임워크인 '스마트시티의 사이버 보안 및 프라이버시에 대한 위험 관리 접근 방식'과 일본의 '스마트시티 보안지침'을 중심으로 분석하고자 한다.

2.1 미국 스마트시티 보안 가이드

미국 NIST에서는 2014년부터 글로벌 스마트시티 커뮤니티의 협업을 위해 GCTC(Global City Teams Challenge) 프로그램을 시작했다. GCTC는 IoT와 CPS를 사용하는 상호 운용 가능한 표준 솔루션 육성과 구축하여, 지속 가능한 모델을 만드는 것을 목표로 하고 있으며, 세부 워킹그룹인 SC3(Secure Cities and Communities Challenge)의 사이버 보안과 관련된 가이드인 'A Risk Management Approach to Smart City Cybersecurity and Privacy'을 살펴보고자 한다. 이 문서는 스마트시티 사이버 보안과 개인정보보호 위험 관리에 대한 접근 방식을 제시하고, 핵심 고려사항을 제공한다[1].

본 가이드는 NIST의 위험 관리 프레임워크(RMF, Risk Management Framework)에 기초해, 스마트시티 특유의 사이버 보안과 위험 관리에서의 고려사항을 제공하고 있으며, 실제 상황에서 이를 적용하기 위한 방법론을 제시하고 있다.

기본적으로 스마트시티와 IT의 사이버 보안과 개인정보보호 관련 취약점과 위협은 상당히 비슷하다.

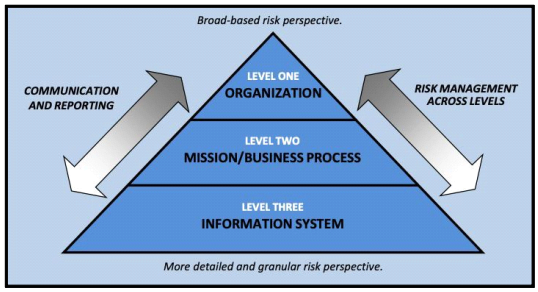

Fig. 2. NIST's Approach to Organizational Risk Management

기본적인 위험 관리 프로세스로 NIST RMF에서는 (1)조직 수준, (2)임무/업무 프로세스 수준, (3)정보 시스템 또는 시스템 구성요소 수준의 3단계 접근법을 사용한다.

조직은 위험 관리 전략을 수립하고, 위험 관리 지침을 전달하며, 임무와 비즈니스 프로세스를 파악하고, 조직의 위험태세를 감독한다. 전략적 수준에서 개발된 위험지침은 낮은 전술적 수준(예: 정보 시스템 및 시스템 구성요소 수준)에서 수행되는 위험 관리 활동을 결정한다. 정보 시스템 수준에서 궁극적으로 구현되는 보안 및 프라이버시 위험 관리 관행은 조직이 정의한 위험 관리 원칙을 직접 반영한다. 조직 수준까지의 시스템 위험 보고는 조직 전체의 위험에 대한 총체적인 뷰를 제공함으로써 조직이 원하는 위험을 조정하고 달성할 수 있도록 하기 위한 것이다.

이를 위해 스마트시티의 사이버 보안과 개인정보보호를 위해 아래와 같은 RMF 문서의 7단계 위험 관리 프로세스를 준용하고 있다.

- 0단계: Prepare(모든 조직에서 위험 관리 준비)
- 1단계: Categorize(정보 및 정보 시스템 분류)
- 2단계: Select(보안 및 개인정보 통제 선택)
- 3단계: Implement(보안 및 개인정보 통제 구현)
- 4단계: Assess(적절하고 의도된 구현, 운영 및 위험 결과에 대한 평가)
- 5단계: Authorize(시스템 작업 승인)
- 6단계: Monitor 시스템 및 환경 변화에 적응하고 조직의 위험 상태에 대한 인식을 유지하기 위해 모니터링(계속)

스마트시티의 주요 위험 관리 고려사항으로 아래와 같이 20개 세부 사항을 기술하고 있으며, 이를

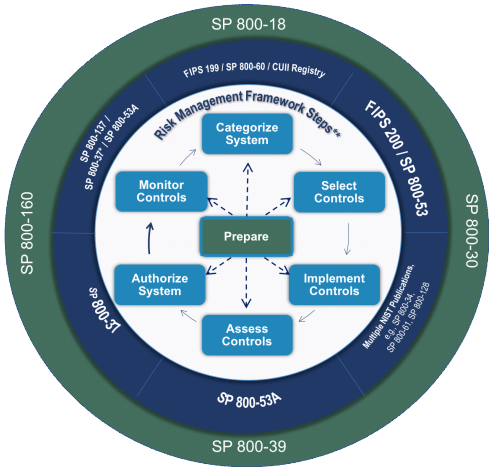

Fig. 3. NIST's RMF and Corresponding NIST Guidelines

적용한 활용 사례를 제시하고 있다.

- 전략적 고려사항(3개): 스마트시티 구현자로서의 위험 관리, 기존의 IT 기업을 능가하는 관점을 채택, 상호의존성 확인 및 이해 및 평가
- 조정 및 커뮤니케이션 고려사항(3개): 정부 내 조정 및 협업, 공공-민간과 범정부 코디네이션, 위험관리 전략 및 정책의 외부 커뮤니케이션
- 자원 계획 고려사항(3개): 사이버 보안 및 개인정보 보호의 비용과 이점을 사전에 평가, 능력 유지 및 성숙을 위한 자원 설명 및 제공, 기존 IT/시스템 평가 및 감사 기능 활용
- 조달, 계약 및 공급망 고려사항(5개): 위험 관리 기능에 대해 인소싱과 아웃소싱을 모두 고려, 획득 및 조달 메커니즘 활용, 공급망을 이해해 위험 프로파일을 결정, 외부 서비스와 시스템 및 제품의 위험 관리, 상용 제품 공급업체의 취약성 알림 요구
- 기술 및 IoT 관련 고려 사항(3개): 기술적 다양성과 한계, 일반적인 제어 문제 및 기회, 역동적인 스마트 환경에서 지속적인 모니터링
- 법적 및 책임 고려 사항(3개): 신규 및 추가 규제 노출 이해, 사이버 보안 보험을 통한 위험 완화, 비공개 계약의 신중한 사용

2.2 일본 스마트시티 보안지침

일본에서는 스마트시티를 구축할 때 지역별 스마트시티 인프라가 달라 지역 간 데이터와 서비스를 교

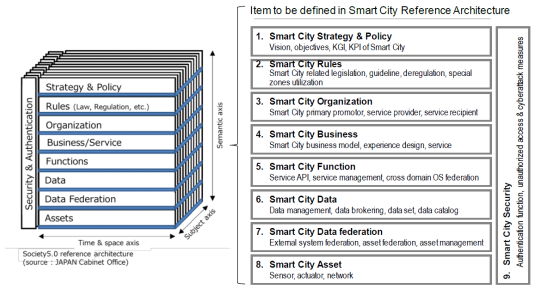

Fig. 4. Items to be Defined in Smart City Reference Architecture

환할 때 호환성이 부족함을 해결하기 위해, 2020년 일본 과학 혁신 협의회가 주도하는 R&D 프로그램인 SIP(Strategic Innovation Promotion Program)에서 Smart City Reference Architecture를 발간하였다[2]. 해당 백서는 시스템 측면에서 스마트시티를 구축하는데 필요한 구성요소를 제시하고, 스마트시티의 기본 메커니즘인 City Operating System을 정의해 지역 간 스마트시티 데이터 이동권을 효율적으로 할 방안을 제시하고 있다.

SIP의 스마트시티 참조 아키텍처에서는 스마트시티 이해관계자가 참조할 구조를 정의하고 다음과 같이 각 계층 구성요소를 지정한다.

또한, 다음과 같은 네 가지 기본 개념을 정의한다.

- User-Centricity Principle : 스마트시티 참여자들은 서비스 이용자들을 항상 인지해야 함
- Role of City Management : 스마트시티의 지속 가능한 경영을 위해 도시 전체의 거버넌스와 관리 메커니즘 필요
- Role of City OS: City OS를 통해 스마트시티 서비스를 제공해 서비스에 장애가 없어야 함
- Importance of Interoperability : 스마트시티의 효율적 구현을 위해 다른 지역과 시스템과 상호 운용성을 확보

네 가지 기본 원칙 중 User-Centricity Principle은 스마트시티의 지역 및 분야와 관계없이 스마트시티 이용자가 편리하게 경제활동을 수행할 수 있어야 하므로 사용 방법에 대한 지시나 어려운 사용자 인터페이스 등의 서비스가 존재해서는 안 되며, 상대적으로 이용자가 적더라도 완벽하게 구현되어있

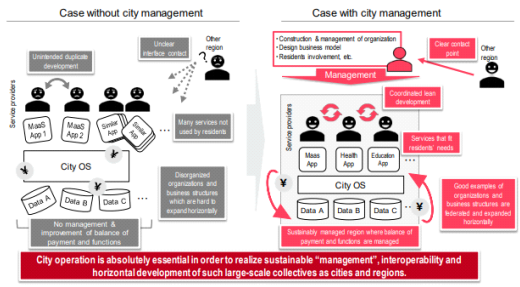

Fig. 5. Illustrated Role of City Management

어야 한다. Role of City Management는 스마트시티가 지속 가능하고 안정적인 서비스를 제공하기 위해 스마트시티 관리가 통일되어있어야 한다는 원칙을 제시한다. 아래 Fig 5와 같이 스마트시티가 종합적으로 관리·구현되지 않아 발생하는 의도치 않은 중복 개발, 인식 부족, 비즈니스 모델을 고려하지 않은 비용 부담 등을 방지하려는 것이 Role of City Management 원칙이다.

City OS의 역할은 서비스와 데이터가 원활하고 능률적으로 공유되고 연합되어야 하는 것으로 City OS가 활발히 운영되지 않을 경우, 스마트시티 전체의 IT 시스템이 분할되어 데이터 공유의 장애로 서비스가 확장되기 어렵게 된다. 스마트시티는 전국적으로 통합되기 전에 각 지역의 특성에 맞게 구축되는 서비스로 지자체별로 진행될 때, 각 지역의 새로운 데이터나 운영 중인 서비스를 사용 가능토록 공통 API와 같은 체계적인 상호운용성 메커니즘이 존재해야 한다.

위 같은 기본 개념과 스마트시티 구성요소 간의 관계를 고려하여 일본에서는 스마트시티 이니셔티브를 진행하도록 하고 있다 Fig 6는 스마트시티 참조 아키텍처의 전체 개요를 보여준다.

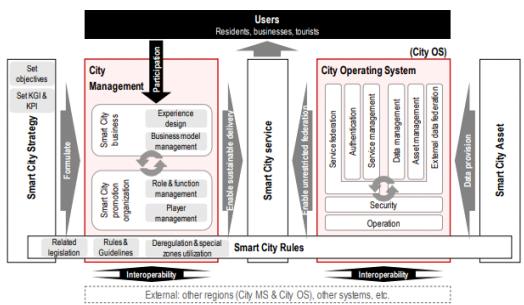

Fig. 6. Overall Picture of Smart City Reference Architecture

스마트시티 참조 아키텍처에서 Smart City Strategy는 각 지역의 스마트시티가 목표를 달성하는 방법에 대한 전략으로 로드맵을 설명한다. 전략을 수립함으로써 서비스, 조직, 시스템 등 스마트시티 전체를 구조적이고 효율적으로 구축할 수 있다. 전략을 수립하기 위한 프레임워크는 크게 핵심 구성요소인 목표와 목표 달성 수준의 정량적 표현인 KGI(Key Goal Indicator), KPI(Key Performance Indicator)로 분류된다. 각 지역의 이슈를 반영하여 주요 목표를 정하고 목표 계층 구조를 하위 목표까지 구성한다. Fig 7은 전략 구조와 전략 수립 과정을 보여준다.

Extract central issues 과정에서는 스마트시티가 달성하고자 하는 목표 결정 전, 해당 지역의 이슈와 배경 및 다양한 자산을 이해하고 스마트시티를 통해 해결해야 할 핵심 이슈를 선정하는 것이 필요하다. 핵심 이슈가 결정되면 Major goals 단계에서 어떤 목적을 달성하고 무엇이 필요한지에 대한 정의가 필요하다. 스마트시티 이해관계자들의 원활한 이해를 통해 목표를 점진적으로 구체화하는 것이 통일된 스마트시티 전략 확보 관점에서 중요한 단계이다. 결정된 주요 목표를 누구나 연관성 있고 논리적으로 이해할 수 있도록 주요 목표를 계층적 방식으로 구성한다. Mid goals 단계는 주요 목표와 하위 목표 사이의 연관성을 위한 레이어(층)로 볼 수 있다. Sub goals는 주요 목표가 특정 목표로 세분화될 수 있도록 모든 목표 마지막 레이어에 배치된다. KGI와 KPI인 중요 목표 달성 지표와 핵심 성과 지표는 주요 목표 및 기타 목표 측정 값에 대해 설정되어야 하며, 측정이 가능한 정략적 요소를 정의하는 기준이라 볼 수 있다.

스마트시티 규칙은 주제에 따라 스마트시티 계획

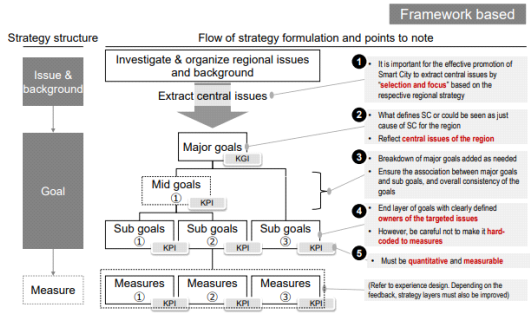

Fig. 7. Strategy Formulation Process and Points to Note

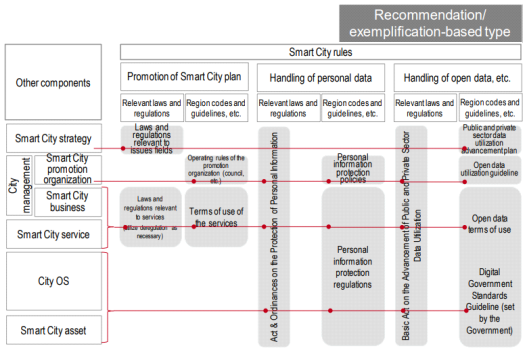

Fig. 8. Relationship Between the Classification of Smart City Rules and Other Components

추진 규칙과 데이터 처리 규칙으로 구분 가능하며, 데이터 처리 규칙은 개인 데이터 및 오픈 데이터의 처리로 분류된다. Fig 8은 스마트시티 규칙 분류와 앞서 설명한 기타 구성요소와의 관계를 매핑하여 나타낸다.

그리고, 일본 총무성에서는 안전한 스마트시티 구축·활용을 위해서 스마트시티 참조 레퍼런스를 준용해 'Smart City Security Guideline ver 2.0'을 발간하였다[3]. 해당 가이드라인은 주체별 고려해야 할 보안 개념을 정의하고, 발생 가능한 문제점과 안전한 스마트시티 구축을 위한 대책을 설명한다. 또한, Fig 9과 같이 스마트시티 참조 아키텍처의 8개의 계층을 정의하고 각 계층을 스마트시티 운영에 있어 전체적인 보안 검토를 위해 거버넌스, 서비스, 도시 운영, 자산 4가지의 카테고리로 분류한다. 각 카테고리의 운용에 따른 보안의 개념과 상정되는 보안 위협 설명, 보안 위협에 맞는 보안 정책 수립, 사고 대응, 감사 및 관리, 위험평가 등 보안대책을 제시하고 있다.

스마트시티 보안체계 수립과 관련해 첫 번째 특이점은 공급망 위험 해소를 위해 공급망 보안을 주요 이슈로 제시하고 있다는 점이다. 이는 스마트시티는

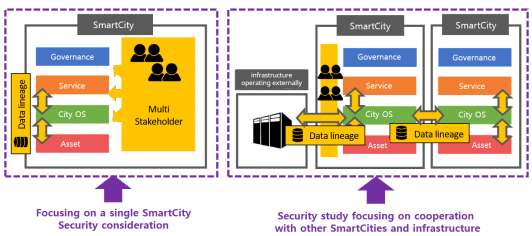

Fig. 9. Security Review of the Entire Smart City

여러 주체가 참여하는 만큼 고도의 네트워크 및 공급망이 존재함으로 주체에 대한 보안대책만으로는 스마트시티 전체의 보안을 확보하는 데 한계가 있다. 가이드라인에서는 각 카테고리에 대한 보안대책을 제시하는 것 이외의 스마트시티 특유의 보안 개념과 대책을 공급망 관리를 통한 신뢰성 확보, 사고 발생에 대한 대응, 데이터 연계 시 보안 3가지 관점으로 실시하여 전반적인 스마트시티의 보안대책을 수립하는 것을 중요하게 여긴다.

스마트시티 내 공급망 확대에 따른 사이버 공격이나 피해를 최소화하기 위해 스마트시티 이해관계자와 관련된 공급망 전체를 관리하고 파악해야 한다. 이를 위해 공급망 보안 관리 체제를 평가하여 일정 수준 이상 보안을 유지해야 한다. 스마트시티 내 특정 컴포넌트에서 보안 문제가 발생했을 경우 피해가 확대되어 스마트시티 전체에 미칠 수 있어 사전 스마트시티 이해관계자들이 책임 범위를 명확히 하여 보안사고 대응 체제를 구축해야 하며 공유를 통한 적절한 공급망 관리로 취약성 파악과 대처가 필요하다.

또한, 스마트시티를 운용할 때 정보 누출이나 서비스가 정지하는 등의 보안 사건·사고가 발생했을 경우, 신속한 원인의 규명과 적절한 대응이 어려우면 2차 피해가 확산될 위험이 존재한다. 특히 스마트시티는 많은 이해관계자가 관련되어 있으므로 사고 대응의 어려움이 있다. 보안 관점에서 구체적인 대응체계를 구축하고 정기적인 보안사고 훈련, 명확한 책임 범위 등을 통하여 사고 대응 대책을 수립할 수 있어야 한다.

스마트시티 보안체계 수립과 관련해 두 번째 특이점으로 스마트시티는 데이터를 소유하는 여러 주체가 데이터 활용과 서비스 제공을 위해 데이터 연계 기반 구현이 필수적이다. 이는 스마트시티 내, 스마트시티 간, 스마트시티와 일반 도시 등의 데이터 연계 시 미비한 보안으로 인한 데이터 변조나 소실이나 데이터 접근 권한의 문제 등의 발생을 통해 데이터의 신뢰를 잃고 서비스의 어려움이 발생할 수 있다. 이러한 데이터 연계에 있어 정보를 공유하기 위한 API 보안 확보, 데이터 연계자와 연계처의 보증 확보, 데이터 연계 보안체계 수립, 암호화 등 신뢰성을 확보해야 한다. 데이터에 대한 적절한 접근 제어와 추적 가능성 확보, 또한, 데이터 이용의 투명성 보장 및 데이터를 보증할 수 있도록 해야한다.

일본 스마트시티 가이드라인은 스마트시티를 구축하고 운용할 때 공급망을 포함한 스마트시티 추진,

Table. 1. Japan SmartCity Guideline Security Measures

	Governance	Service	Asset	City Os	Supply Chain	Incident Response	Data Lineage
Security Measures	Establish Security Policy	Risk Assessment by Service	Asset Monitoring and Management	Security Measures for External Attacks	Risk Management of the Entire Supply Chain	Scope of Responsibilities	Data Linkage Security System Evaluation
	Policies for Multi-Stakeholder	Security Measures for External Attacks	Security Measures for Assets	Security Measures to Prevent Security Accidents	Outsourced Security Management Evaluation	Establishment of Security Incident Response System	Data Provider Authentication and Access Control
	Countermeasures to Maintain Governance	Security Measures to Prevent Security Accidents		Security Measures for Accidents	Identify And Respond to Vulnerabilities	Multi-Stakeholder Sharing	Ensure Data Traceability and Data Transparency
		Security Measures for Accidents		Use of Appropriate Cloud Services		Response to Multi-Stakeholder Incidents	Data Source Assurance and Data Reliability
						Regular Security Incident Response Training	

운영과 관련된 주체에서 발생할 수 있는 보안 위협 시나리오를 제시하고 해당 위험에 맞는 보안대책을 제시한다. Table 1은 해당 가이드라인에서 분류한 카테고리와 공급망 보안, 사고 대응, 데이터 연계 3가지 관점을 포함한 보안대책 항목으로 보안 정책 수립, 위험 관리, 이해관계자 관리 등 항목별로 필요한 전반적인 보안대책을 보여준다.

특히, 본 지침에서는 보안대책을 서술함과 동시에 스마트시티와 관련된 보안 위험 목록과 보안대책 목록 및 스마트시티 보안 도입 체크리스트를 제시한다. 체크리스트에는 예상 보안 문제, 위협 및 취약성, 대책 요구사항 코드로 매핑하여 제시하고, 보안 목록에 대해서는 보안 카테고리, 요구사항 코드, 요구사항 내용, 참조 아키텍처로 매핑하고 있다.

해당 보안 체크리스트를 통해 스마트시티를 추진하는 데 있어 예상되는 보안 목록을 정리하고 보안대책을 검토하는 데 활용할 수 있다.

IV. 공급망(Supply-Chain) 보안

ICT 공급망(Supply-Chain)은 ICT 제품 및 서비스가 설계되고 개발되어 사용자가 사용하기까지에 이르는 전체 프로세스에서 하나의 기업이 모든 업무를 담당하는 것이 아닌, 제품 및 서비스를 외부에 위탁하고 공급, 취득하는 과정을 일컫는다. 공급망은 최근 IT 기술 확대 및 기업의 글로벌화로 인해 더욱

다양화되어가고 있다. 이러한 공급망의 다양화와 더불어 위탁과 공급과정에서의 사이버 공격 문제가 더욱 대두되고 있다. 이러한 공급망 공격은 공급망과 관련된 이해관계자 모두의 제품 또는 서비스를 감염시켜 무력화시키거나 데이터를 유출시키는 등의 행위가 가능해진다[17].

공급망 보안과 관련된 국제표준인 ISO/IEC: 27036(Information Security for Supplier Relationships)에서는 공급망을 '획득자, 공급자 또는 각각이 구매 주문, 계약 또는 공식적인 소싱 계약을 체결할 때 설정된 연속적인 관계를 형성하기 위한 연결된 자원 및 프로세스의 조직적인 집합'으로 정의하고 있으며, 취득자와 공급자 관계에서 정보 및 정보 시스템을 보호하기 위해 정의한 국제표준이며, 공급망 유형을 분류하고 이에 따른 위협과 개선 방안, 보안대책 등 접근방법을 제시한다. 해당 국제표준은 Part를 4개로 나누어 각 공급 관계에 대한 체계, 제품 및 서비스의 요구사항 정의, 공급망 보안지침, 클라우드 서비스 관점의 보안지침을 정의한다[6][7][8][9].

ISO/IEC 27036에서는 최종 사용자에게까지 가는 공급망 관계를 Fig 10과 같이 나타내며 공급자와 관련된 Tier1과 Tier2에 대한 범위를 지정하고 설명한다. 악의적인 목적으로 감염되거나 위조된 제품의 위험을 감소시키기 위한 무결성 공급망 보안 국제표준인 ISO/IEC 20243(O-TTPS)는 Part1인 제품의 생명주기 동안 감염 또는 위조 위협에 노출된 제품을 보증하기 위한 요구사항이다. Part2는 Part1에 포함된 요구사항에 대한 적합성을 입증하는 평가절차로 구성되어 있다[10][11].

국제표준 외에 미국 NIST에서 개발한 공급망 보안기준 및 정책 중 본 논문에서 제시하고자 하는 스마트시티 내용과 가장 밀접하게 관련된 것이 NIST

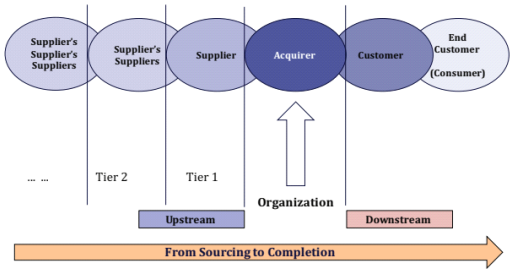

Fig. 10. ISO/IEC 27036 Supply Chain Relationship

SP800-161이다. SP800-161에서는 제품과 부품의 다양화에 따라 공급망 복잡화로 공급망 생명주기를 상세히 파악하는 것이 어려워진 것을 이용해 공급망 공격의 위협에 대응하기 위한 관리대책을 설명한다. 해당 대책에서는 위험 발생 확률과 영향을 평가하여 공급망 대책을 실행하며 조직 전체에 대한 통합 위험관리 수행을 위한 계층적 접근법을 채택하여 전략적으로 위험을 통합 관리하는 목표를 가지고 있다[5].

영국의 NSCS(National Cyber Security Centre)에서는 공급망 보안을 위한 위험 인지, 통제권 수립, 준비사항, 지속적인 개선 4단계로 총 12개의 원칙을 정의했다. 영국 내각부는 공급망에서 발생하는 위험을 8가지 주요 항목을 통해 위험평가를 분석하여 기업에 대한 공급망 위협을 효과적으로 식별·관리하고자 SAF(Supplier Assurance Framework)를 발표했다[4].

이 외에도 EU에서는 사이버 보안 인증 프레임워크(Cybersecurity Certification Framework) 수립 및 사이버 보안 대응(NIS Direcive)를 구현하여 공급망 보안기준을 확립하려는 연구가 활발히 진행 중이다[13]. 이처럼 전 세계적으로 공급망 보안은 필수 요소로 여겨지고 있으며, 스마트시티의 경우 IoT 장비와 센서를 더불어 수많은 기기에 네트워크를 통한 공급망 플랫폼으로 이루어져 있으므로, 스마트시티를 설계할 때 공급망 보안에 해당하는 요구사항이 존재하지 않는 경우 공급망 공격의 예방이나 사고 시 대응체계가 부족한 문제가 생길 수 있다. 안전한 스마트시티를 설계하기 위해 공급망 보안 요구사항은 필수 요소로 여러 스마트시티 공급망 보안을 도출하여 국내 실정에 적절히 맞추어 추가되어야 할 것으로 보인다.

V. 제로 트러스트(Zero-Trust) 보안

Zero-Trust는 2010년 포레스트 리서치의 존 킨더버그가 최초로 언급하면서 시작된 개념으로 아무것도 신뢰하지 않고 모든 것을 검증하고 일관된 제어를 유지하는 것을 본질로 가지고 있다. Zero-Trust는 발송지가 네트워크 내부, 외부든 상관없이 커뮤니케이션이 이루어지기 전에 동일한 수준의 인증과 권한 확인 과정을 거쳐야 하며, 신뢰할 수 있음을 입증하지 못하면 아무것에도 액세스할 수 없다는 것이다.

최근 COVID-19 감염병 예방 및 차단을 위해 집이나 공공장소 등 원격지 어느 곳이든 일할 수 있는

WFA(Work From Anywhere)가 받아들여지면서 대면 업무와 유사한 환경으로 비대면 업무를 조성하고 있다. COVID-19 이후에도 재택근무 비율이나, 스마트시티 내 원격 접속 및 기술이 증가할 것으로 예상되나, 현재의 환경은 사이버 침해에 무방비한 상태이다. 이를 위한 대책으로 인터넷망과 업무망을 분리하는 망 분리를 시행하고 있으나, 4차 산업혁명과 같은 초연결 시대에서 망 분리는 오픈소스나 클라우드 및 모바일 환경 증가에 따른 보안 경계 수립이 어려워 걸림돌로 작용한다. 또한, 망 분리를 위한 비용 문제나 개인 PC의 감염으로 인한 보안 문제를 해결하기는 어렵다.

망 분리가 완화되며 레거시 환경에서 새로운 통합 보안 접근전략을 위해 제로 트러스트 전략을 도입하게 되면, 언택트 시대에 맞게 업무망과 인터넷망의 물리적 분리 없어도 상호 접근을 불가능하게 분리하는 기술을 가지게 되며, 사용자의 위치, 시간 등 환경에 구애 없이 안전한 본인 확인과 수시 인증 처리가 가능하다. 또한, 사용자의 이상 행위나 행위 로그, 시스템 자원의 정보에 따라 위험을 감지하여 자원의 접근을 제한하기 위한 사용자 추가 인증도 가능하게 된다.

제로 트러스트 모델은 다음과 같은 5가지의 적용 절차를 가지게 된다.

- 악성 데이터 확인 및 분류
- 악성 트래픽 경로 파악
- 제로 트러스트 네트워크 설계
- 지능형 정책 생성
- 제로 트러스트 에코시스템 모니터링

미국 국립 표준기술연구소(NIST)는 이러한 망 분리 환경의 한계점을 인식하고 제로 트러스트의 개념을 수용하여, 'Zero Trust Architecture(SP 800-207)' 문서를 제시하고 있다[14]. SP 800-207에서는 제로 트러스트에 대한 개념과 적용 환경, 보안 요구사항을 제시하고 이를 운영할 수 있는 제로 트러스트의 아키텍처 유형, 레거시 환경과의 연동 방법을 제시한다. 모든 기업의 네트워크는 신뢰 영역으로 간주하지 않고 항상 공격자가 있다고 가정하고, 신뢰할 수 있는 자원 또한 없어 모든 장치에 대해 보안 상태 평가가 요구되며, 이는 기업 네트워크를 이용하는 동안 유지해야 한다고 설명한다. 원격 접속 시도 시 모든 트래픽이 모니터링되고 수정될 가능성이 존재하므로, 모든 연결 요청은 인증 및 승인

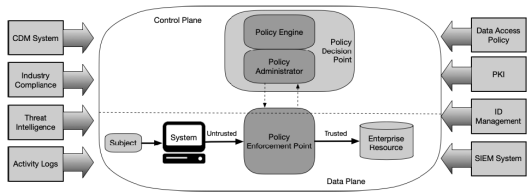

Fig. 11. NIST SP 800-207, Core Zero Trust Logical Components

되어야 하고, 가장 안전한 환경 유지가 필요하다고 강조한다.

NIST SP 800-207에서 설명하는 제로 트러스트 핵심 구성요소는 다음 Fig. 11와 같다.

핵심 구성요소는 정책 엔진(PE), 정책 관리자(PA), 정책 시행 시점(PEP)으로 구성된다. 정책 엔진은 엔터프라이즈 정책뿐만 아니라 CDM 시스템, 위협 인텔리전스 서비스 등 외부 소스의 입력을 신뢰 알고리즘 기반으로 액세스 권한을 부여한다. 정책 관리자는 사용자가 리소스에 액세스하는데 사용하는 세션별 인증 및 인증 토큰 또는 자격 증명을 생성한다. 정책 시행 지점은 사용자가 리소스에 액세스하는데 사용하는 인증 정보, 키 또는 토큰을 통해 세션을 관리한다.

Zero Trust의 Trust Algorithm(TA)은 궁극적으로 리소스에 대한 액세스를 허용하거나 거부하는데 정책 엔진이 사용하는 프로세스로 볼 수 있다. 다음 Fig 12은 Trust Algorithm에 제공하는 입력을 기반으로 범주를 나눈 것이다.

Access Request는 실제 요청으로, 요청된 리소스가 기본 정보로 요청자에 대한 정보도 사용되며, OS 버전, 사용된 소프트웨어 등이 포함된다. 해당

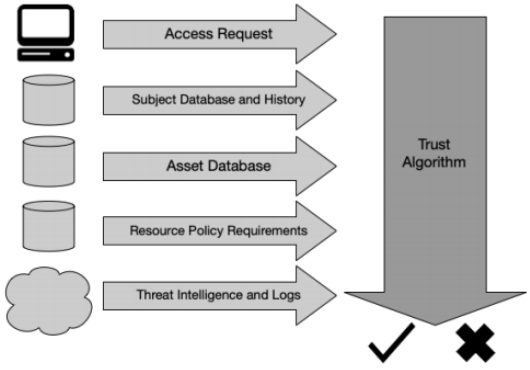

Fig. 12. Trust Algorithm Input

정보들과 자산 보안 상태에 따라 액세스가 제한될 수 있다. Subject Database는 리소스에 대한 액세스를 요청하는 사용자에 대한 것으로, 할당된 속성 및 권한의 모음이며, 이를 통해 리소스 액세스를 위한 정책의 기초를 형성한다. 사용자 ID에는 논리적 ID(계정 ID 등)와 PEP를 통한 인증 검사 결과를 합쳐 나타낼 수 있다. 신뢰 수준을 도출하는 데 고려할 수 있는 속성에는 시간과 지리적 위치를 포함할 수 있다. Asset Database에는 각 기업의 소유 자산의 상태를 나타내는 데이터베이스로, 소프트웨어의 무결성 및 위치 등 자산 액세스 요청 기업의 자산 상태에 따라 액세스가 제한될 수 있다. Resource Policy는 정책 집합으로 사용자 ID 및 속성 데이터베이스를 보완하고 리소스 액세스에 대한 최소 요구사항을 정의한다. 요구사항에는 MFA, 데이터 민감도, 보증 수준 등을 포함한다. Threat Intelligence는 인터넷에서 작동할 수 있는 일반적인 위협 및 멀웨어에 대한 정보 피드로 의심스러운 장치에서 나타나는 특징 정보 등을 포함한다. TA를 구현할 때 위의 각 데이터 소스에 대한 중요도의 가중치는 구현하는 사람과 기업에 따라 다르며, 점수 또는 신뢰 수준에 대한 가중치 평가 혹은 각 장치에 대한 요청에 따른 독립적인 처리 평가를 수행할 수도 있다.

NIST SP 800-207에서는 단일 기업의 로컬 네트워크 연결, 로컬 네트워크를 가지면서 여러 클라우드를 활용하는 기업, 기업과 계약한 서비스 제공자를 포함하는 기업, 기업 간 프로젝트를 진행하는 기업, 공공 기업 혹은 고객 대면 서비스를 제공하는 기업과 같이 Zero Trust 구축을 위한 몇 가지 시나리오를 제시하며, 각 시나리오 별 리소스 액세스에 대한 제한 조치를 설명하고 있다.

Zero Trust는 레거시 혼재망을 대체할 전략으로 기업에 초점을 맞추어 대두되고 있지만, 장비와 장비 간, 장비와 사람 간 등 원격접속과 데이터 연계로 이루어지는 스마트시티 플랫폼에서 신뢰할 수 있는 접속 및 데이터 연계를 위한 Zero Trust 전략의 도입이 필요할 것으로 보인다.

VI. ISMS-P 인증심사 기준

ISMS-P(Personal information & Information

Table. 2. ISMS-P Certification Audit Criteria

Certification		Category	Number of certification criteria by field	
ISMS-P (102)	ISMS (80)	1. Establishment and operation of management system (16)	1.1 Establishment of management system foundation (6)	1.2 Risk Management (4)
			1.3 Management system operation (3)	1.4 Management system inspection and improvement
		2. Protection requirements (64)	2.1 Policy, Organization, and Asset Management(3)	2.2 Human Security (6)
			2.3 Outsider Security(4)	2.4 Physical Security(7)
			2.5 Authentication and Rights Management (6)	2.6 Access Control (7)
			2.7 Encryption Enforcement (2)	2.8 Information system introduction and development security (6)
			2.9 System and service operation management (7)	2.10 System and service security management (9)
			2.11 Accident Prevention and Response (5)	2.12 Disaster Recovery (2)
	-	3. Requirements for each stage of processing personal information (22)	3.1 Protection measures when collecting personal information (7)	3.2 Protection measures for retention and use of personal information (5)
			3.3 Protection measures when providing personal information (3)	3.4 Protection measures when personal information is destroyed (4)
			3.5 Protection of data subject rights (3)	

Security Management System) 인증제도는 2001년, 기업 또는 조직의 정보보호 관리체계가 요구사항(인증기준)에 적합한지를 독립적이고 객관적인 입장에 있는 제3의 인증기관이 평가하여 인증을 부여하기 위해 2001년에「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조에 따라 국내에 도입되었으며, 2013년 일정 규모 이상의 주요정보통신서비스 제공자 등이 ISMS 인증 의무대상자로 지정되었다. 2016년에는 매출액 또는 세입 1,500억 원 이상인 상급종합병원과 재학생 수 1만 명 이상의 대학교 등 비영리 분야로 의무대상자가 확대되었다. 2018년도에는 정보보호와 개인정보보호의 연계 필요성이 제기되어 2018년 정보보호 관리체계(ISMS)와 별도로 운영되던 개인정보보호 관리체계(PIMS, Personal Information Management System)를 통합하여 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증 등에 관한 고시를 개정하고 통합인증제도를 시행하고 있다.

ISMS-P 인증은 관리체계 수립 및 운영(16개)과 보호대책 요구사항(64개)으로 구성되어 있으며, ISMS-P 인증기준은 ISMS 인증 기준(80개)과 개인정보 처리 단계별 요구사항(22개)으로 구성되어 있다.

크게, 관리체계 수립 및 운영, 보호대책 요구사항, 개인정보 처리단계별 요구사항 항목 3가지로 나누어져 있다. 관리체계 수립 및 운영은 16개, 세부항목 42개, 보호대책 요구사항은 64개, 세부항목 192개, 개인정보 처리단계별 요구사항은 22개, 세부항목 91개로 기업이 정보를 처리하기 위한 요구사항 항목이 제시되어 있으며, 각 카테고리와 세부 내용을 번호로

Table. 3. Comparison of Domestic and Overseas Smart City Security Model Summary

	NIST GCTC	Japan Guideline	Kisa Security Model
Policy	Policy Establishment, Risk Management of Smart City Implementers, Confirmation and Understanding and Evaluation of Interdependence	Policy Establishment	Policy Establishment
Communication	Coordination and Collaboration Within Government, Public-Private and Whole-Government Coordination, Communication Outside Risk Management Strategies And Policies	Security Training and Education, Records Management, Incident Response	Security Training and Education, Records Management, Incident Response
Asset Management	Information Security Cost Assessment, Asset Description, Audit Function	Responsibilities Based on Asset Priorities, Audit Function, Asset Record	Asset Records, Continuous Monitoring
Technology and System Security	Technology Diversity, Access Control, Continuous Monitoring	Technology Diversity, Access Control, Continuous Monitoring	Technology Diversity, Access Control, Continuous Monitoring, Service Introduction and Development Security
Law and Responsibilities	Understanding New and Additional Regulations, Cybersecurity Insurance, Discreet Non disclosure Agreements	Designation of Security Management Officer, Data Protection According to Law	Designation of The Person In Charge of Security Management, Identification of Important Personnel
Supply Chain Management	Consider Insourcing and Outsourcing, Leveraging Acquisition and Procurement Mechanisms, Managing External Services and Systems and Products Risk, and Alerting Vendors of Commercial Products to Vulnerabilities	Consider Insourcing and Outsourcing, Leveraging Acquisition and Procurement Mechanisms, Risk Management of External Services and Systems and Products, Alerting Vendors of Commercial Product Vulnerabilities, Incident Response	Outsider Contract Security

지정하여 제공하고 있다[15][16].

VII. 제로 트러스트 기반 스마트시티 보안 요구사항 제안

본 장에서는 앞서 설명한 국내 '스마트시티 보안모델'과 일본의 '스마트시티 가이드라인'에서 제시하는 보안 요구사항, 미국 NIST의 스마트시티 보안 관리 고려사항, 보안관리를 위한 'ISMS-P 인증기준 세부 점검항목'을 매핑해 비교분석하였으며, 최근 보안분야에 이슈가 되고 있는 '공급망 보안' 문제와 데이터 연계 등을 위한 '제로 트러스트' 보안 요구사항을 추가해, 추가적인 스마트시티 보안모델과 보안 요구사항을 제안하고자 한다.

다음 Table 3은 앞서 분석한 해외 및 국내의 스마트시티 보안 지침의 구성 특성을 비교 분석한 표로, 각 보안모델에서 요구하고자 하는 내용을 정책, 커뮤니케이션, 자산 관리, 기술 및 시스템 보안, 법률 및 책임, 공급망 관리로 나누어 요약하고 기술했다.

Table 3에서 나타낸 스마트시티 보안 지침과 더불어 ISMS-P 인증제도 요구사항 항목을 비교 분석하여 국내 스마트시티를 구축할 때 필요한 요구사항을 아래 Table 4와 같이 제안하고자 한다.

미국 NIST의 GCTC 스마트시티 프레임워크에서는 조직이 스마트시티를 구현하고자 할 때 전체적인 보안 프로세스를 단계별로 기술하고 있으며, 커뮤니케이션에 중점을 두어 위험 전략을 수립하고 있다. 또한, 정책과 관련된 내용 및 공급망 위험 관리에 대한 보안 프레임워크를 잘 나타내고 있어 전반적인 스마트시티 정책, 공급망 위험 관리 요구사항을 참조할 수 있다.

일본 스마트시티 보안 가이드라인에서는 스마트시티 전체에 필요한 보안 관련 요구사항을 코드별로 제시하고, 거버넌스, 자산, 도시 OS, 서비스에 맞게 매핑하여 제공하고 있다. 또한, 스마트시티를 운용하고자 할 때 보안 위험과 관련하여 접근통제, 인적·자원 관리, 사고대응 등 구체적으로 명시되어 있으며 특히, 공급망 위험 관리에 대한 요구사항이 인·아웃소싱, 외부자, 교육 등 전체적인 공급망 보안 프로세스를 나타내고 있다.

KISA의 스마트시티 보안모델은 보안 관리, 통합 플랫폼, 서비스, 인프라, 디바이스를 크게 분류하고 각각에 해당하는 보안 요구사항을 제시하고 있으며, 분류된 각 항목에 대해 악성기능 관리, 암호화, 연속성 관리, 데이터 관리 등 기술적인 요구사항을 구체적으로 제시하고 있어, 본 논문에서 제안하는 보안 운영 관리와 데이터 흐름 관리 항목 요구사항을 도출할 수 있었다.

마지막으로 스마트시티는 국가 및 기업에서 진행하며, 사용자는 개인이므로 제안하는 요구사항에 국내 실정에 맞는 개인정보 및 정보보호 인증제도인 ISMS-P에서 요구하는 항목을 추가하여 매핑하였다. ISMS-P와 일본 가이드라인은 실제 문서에서 제공하는 번호 및 코드로 매핑하였으며, KISA에서 제공하는 요구사항의 경우 코드로 정해져 있지 않으므로, 보안 관리는 SM, 통합 플랫폼은 IP, 서비스는 Ser, 인프라는 Inf, 디바이스는 Dev로 나누어 각 항목에 맞게 정리하였다.

다만, 미국 GCTC 스마트시티 프레임워크는 NIST의 사이버보안 프레임워크(CSF, Cybersecurity Framework)에 따른 위험관리 프레임워크(RMF, Risk Management Framework)의 사이버보안 요구사항을 도출하는 방식으로, 직접적인 스마트시티 모델(사례)과 범위가 도출되고, 이에 대한 세부 보안 요구사항을 도출하는 방식이라, 매핑에서 제외하였다.

도출된 제로 트러스트 기반 스마트시티 보안 요구사항에서 볼 수 있듯이 데이터 연계를 위한 요구사항과 공급망 보안의 보안요구사항을 도출하고 있다. KISA의 스마트시티 보안 요구사항에서 공급망과 관련된 요구사항은 외부자 관리(보안관리1.3)인 보안정책 및 유지보수 사항을 계약서에 반영하는 것을 일부 포함하고 있으나, 그 외 공급망 보안 내용은 찾아볼 수 없어 미흡한 것을 확인할 수 있다. 일본 스마트시티의 공급망 관련 요구사항의 경우 계약 내용뿐만 아니라, 공급망에 연결된 모든 조직의 역할을 식별하며, 외부자 및 외부자와 관련된 서비스에 대해 보안 감사가 주기적으로 이루어져야 하며, 보안 감사 결과에 따른 대응 및 계약 만료 시 보안과 관련된 절차가 마련되고 시행될 수 있어야 한다고 명시되어 있다. 그 외에도 공급망 정책과 프로세스에 대한 요구사항을 정확히 명시하고 있어, 스마트시티 설계·운영 시 공급망 위험에 대해 주기적인 평가 및 대응이 적절히 이루어질 것으로 보인다. 공급망 보안과 관련된 요구사항 부족으로 생기는 보안 문제는 스마트시티 플랫폼을 더불어 스마트시티 이해관계자의 전반적인 위협으로 이어질 수 있어, 스마트시티 보안모델을 설

Table. 4. Smart City Security Requirements Proposal and Mapping Table

Category			ISMS-P	KISA Security Model	Japan Guideline
Information Security Governance	Information Protection Policy Management	Establishment and Operation of Security Policies	1.1.5	SM.1.1	BE-2
		Security Policy Review and Revision	1.1.5	SM.1.1	BE-2
	Human Security Management	Management of Main Employees	2.2.1	SM.1.2	AM-7, BR-2
		Security Policy Compliance Pledge	2.2.3	SM.1.2	GV-1
		Specialized Training for Main Employees	2.2.4	SM.1.2	AT-2, AT-3
	Supply Chain Management	Supply Chain Contract Security	2.3.2	SM.1.3	RP-2, SC-1
		Supply Chain Status Management	2.3.1	SM.1.3	BE-1, SC-5
		Supply Chain Security Implementation Management	2.3.3, 2.3.4	N/A	RM-2, SC-2, SC-3, SC-4, SC-6, SC-7, SC-8, SC-9, SC-10, SC-11
	Risk Management	Information System Asset Management	1.2.1, 2.1.3	SM.1.4	AM-1, AM-2, AM-6
		Risk Assessment	1.2.3	N/A	GV-4, RA-4, RA-5, RM-2
		Establish an Information Protection Plan	1.2.4	N/A	RA-6
	Protection Measures Management	Implementation of Protection Measures And Management of Current Status	1.3.1	N/A	RA-7
		Legal Compliance Review	1.3.3	N/A	GV-2, GV-3
		Protective Measures Audit and Improvement	1.4.1	SM.8.1	IM-1
Physical Security Management	Access Control	Operation Center Protection Zone Designation and Access Control	2.4.1	SM.2.1	AC-2
		Operation Center Access Record Review	2.3.2	SM.2.2	CM-2
		Control of Import and Export Equipment	2.4.6	SM.2.2	N/A
	Facility Security	Protection Equipment Operation	2.4.4	SM.2.3	IP-5
		Operation Of Image Information Processing Equipment	3.1.6	Ser.1.2	N/A
Information Flow Management	Information Status Management	Service Flow Analysis	1.2.2	N/A	AM-4
		Information Identification	2.6.4	N/A	N/A
	Security Management at Each Stage of Information Processing	Protective Measures When Collecting Information	3.1.1	SM.5.1, Dev.5.1	N/A
		Protection Measures When Transmitting and Storing Information	2.7.1	SM.4.1, SM.5.1, Inf.4.1,	DS-2, DS-3, DS-4, DS-5
		Protective Measures When Providing and Linking Information	2.10.5	N/A	DS-1
		Protective Measures when Using Information	3.2.3, 3.2.5	SM.5.1, SM.5.2, IP.4.1	IP-6

Category			ISMS-P	KISA Security Model	Japan Guideline
		Information Validity Management	N/A	Ser.2.1	CM-4, DS-11, DS-14
Authentication and Permission Management	Account and Permission Management	Creating Individual Accounts and Granting Different Privileges	2.5.1, 2.5.2, 2.5.5	SM.3.1, SM.3.2, Dev.1.1	AC-1
		Review Account and Authority	2.5.6	SM.3.1	IP-9
	User Authentication	Password Management	2.5.4	SM.3.2, Dev.1.2, IP.1.2, Inf.1.2	IP-1
		Authentication Function Management	2.5.3	Dev.1.1, IP.1.1, Inf.1.1	AC-3, AC-4, AC-6
Access Control	Network Access Control	Separation and Control of Network Areas	2.6.1	SM.4.1	AC-7, AE-1, CM-1, CO-1
		External Remote Access Control	2.6.6	N/A	CM-1, MA-2
		Internet Access Control	2.6.7	N/A	CM-1, DS-9
		Wireless Network Security	2.6.5	N/A	CM-1
	Information System Access Control	Operating System Access Control	2.6.2	SM.3.3	AC-8, IP-1, PT-2
		Web Server Security	2.10.3	SM.4.1	IP-1
		Application Access Control	2.6.3	SM.3.3	AC-6, AC-9
		Database Access Control	2.6.4	N/A	IP-1
		Device Security	N/A	Dev.1.1 Dev.1.2, Dev.2.1, Dev.3.2, Dev.4.2, Dev.4.3	AC-3, AC-4, DS-8, DS-10, DS-12, DS-13, DS-15, IP-1, PT-2, PT-3
Introduction and Development Security	Information System Introduction and Development Standards	Defining Security Requirements	2.8.1	SM.7.1, Dev.4.3	IP-3
		Confirmation And Testing of Security Requirements	2.8.2	SM.7.2, Dev.4.3	IP-3
	Service Software Environment Security	Separation of Test and Operating Environment	2.8.3	SM.7.3	IP-3
		Operational Data Security	2.8.4	SM.7.4,	IP-3
		Source Program Management	2.8.5	SM.7.5	IP-3
		Software Operating Environment Transfer Control	2.8.6	SM.7.6	IP-3
Security Operation Management	Log Management	Log Creation and Preservation	2.9.4	SM.6.1	PT-1
		Log Review	2.9.5	SM.6.2, Dev.2.1, IP.2.1, Inf.2.1	PT-1
	Service Continuity Management	Change Management	2.9.1	Dev.3.1, IP.3.1, Inf.3.1	AM-3, AM-5, IP-2
		Device Installation and Operation Check	N/A	Dev.4.1	CM-6
		Performance Management	2.9.2	Dev.2.3,	DS-7

Category			ISMS-P	KISA Security Model	Japan Guideline
				IP.2.3, Inf.2.3	
		Disability Management	2.9.2	N/A	DS-7
		Backup and Recovery Management	2.9.3	Dev.3.3, IP.3.3, Inf.3.3	IP-4
		Disaster Recovery Management	2.12.1 2.12.2	Dev.3.3, IP.3.3, Inf.3.3	BE-3, CO-2, CO-3, IM-2, RP-3
	Vulnerability Management	Patch Management	2.10.3	Dev.3.2, IP.3.2, Inf.3.2	MA-1, MA-3
		Malware Control	N/A	Dev.2.2, IP.2.2, Inf.2.2	DM-3
		Vulnerability Check and Action	2.11.2	SM.8.1, Dev.2.2, IP.2.2, Inf.2.2	CM-7, IP-10, RA-1, RA-2
	Prevention and Response to Infringement Accidents	Cyber Threat Detection and First Response	2.11.2 2.11.3	SM.8.1	AE-2, AE-3, AE-4, AE-5, AN-1, AN-3, CM-5, DS-6, MI-1, RP-1
		Incident Response and Recovery	2.11.5	N/A	DP-1, DP-2, RA-3, RP-4
		Incident Response Training	2.11.4	SM.8.2	AT-1, DP-3, DP4

계할 때 일본 스마트시티 가이드라인과 공급망 보안 국제표준인 ISO/IEC 27036 및 20243등 관련된 가이드라인을 국내 실정에 맞게 스마트시티 보안 요구사항에 추가하여 안전한 공급망 관리체계를 마련할 수 있어야 한다. 본 논문에서 제안하는 스마트시티 보안모델에서는 기존 KISA 국내 보안모델에서 제시되지 않았던 공급망 위험 관리 항목 중 'Supply Chain Security Implementation Management'를 추가하여 위탁업체의 관계자의 보안관리·교육과 인증 및 권한을 통한 접근통제, 보안 감사 등을 통해 협업을 진행 중일 때뿐만 아니라 계약이 종료된 이후에도 접근권한 회수, 비밀확약서 등을 통한 공급망 보안 관리를 진행할 수 있도록 한다.

또한, 데이터 연계로 운영되는 스마트시티에서 네트워크 접근제어 및 데이터 연계 시 보안 요구사항이 국내 스마트시티 보안모델에서 부족하여 본 논문에서는 데이터 연계 시 보안 요구사항인 'Protective measures when providing and linking information' 항목과 내·외부 및 데이터베이스 접근통제 항목을 추가하여 스마트시티의 전체적인 보안관리 뿐만 아니라 인프라 내 악의적인 내부자 모니터링, 안전하지 않은 디바이스 인증과 권한에 따른 접근통제 등 Zero-Trust 개념을 토대로 스마트시티 통합플랫폼 주요 직무자를 비롯하여 일반 사용자까지 신뢰하지 않도록 하고, 접근하는 IoT, BYOD, 원격접속 등 모든 기기의 내부, 외부 인증 및 계정 권한 관리를 통해 신뢰할 수 있는 스마트시티의 데이터 연계가 필요할 것으로 보인다.

또한, 스마트시티에서는 국가, 지방공공단체, 민간 등에서 산재하는 데이터를 연계하여 분야·조직을 초월한 데이터 활용과 서비스 제공을 가능하게 하기 위해 데이터 분산 방식으로 대표되는 데이터 연계 기반의 구현이 필요하다. 따라서 데이터 연계 시, 데이터 등을 다른 서비스나 어플리케이션에서 호출하여 이용하기 위한 연계 기술인 API에서의 보안 확보뿐 아니라, 데이터 연계 시의 데이터 연계원, 연계처의 보

안 체제를 평가하는 등 연계처의 신뢰성을 확보하면서, 데이터에 대한 적절한 접근 제어와 데이터 추적 가능성 확보를 통한 데이터 이용의 투명성 보장, 데이터 원본성 보증에 의한 데이터 연계 대책 등 연계처의 신뢰성을 확보하는 것이 필요할 것이다.

VIII. 결 론

스마트시티는 여러 기기 및 IoT 장비를 네트워크를 통해 하나로 결합하여 스마트시티 이해관계자에게 데이터를 연계하며 시민의 질을 높이고자 하는 데 목적을 두고 있는 스마트한 도시이다. 이는 많은 기기를 통해 데이터가 사용되는 만큼 사이버 보안에 취약하며 각별한 주의가 필요하다. 실제로 구축된 스마트시티에서 데이터가 유출되는 사고들이 발생하고 있는 만큼 설계 시 보안 요구사항과 사고 대책이 구체적으로 명시되어 있어야 한다. 스마트시티는 각 나라 및 지역, 설계하고자 하는 특성마다 다르므로, 세부적인 보안 요구사항은 상이할 수 있으나, 기존의 다양한 ICT 서비스에서 발생하는 보안문제에 대응하기 위한 요구사항이 추가되어야 할 것이다. 특히, 최근에 원격근무, 원격관리, 데이터 연계 등의 보안문제로 제기되는 '제로 트러스트(Zero-Trust)문제나 다양한 디바이스, 서비스 연결로 인한, 공급망 보안문제를 해결하는 것이 필수적일 것이다.

이에, 본 논문에서는 미국, 일본 등 주요국가의 스마트시티와 관련된 프레임워크, 가이드라인, 보안 요구사항 동향을 알아보고 ISMS-P와 일본 스마트시티 보안 요구사항, 현재 국내 KISA에서 제시한 스마트시티 보안 요구사항을 참고하여 국내 스마트시티 보안 요구사항에 필요한 내용과 참고한 문서들의 공통 요구사항을 표로 매핑하여 제시하였다. 앞서 설명한 바와 같이, 국내의 스마트시티 구축 방향성과 특성이 다르므로 제로 트러스트나 공급망 보안 요구사항을 제시할 때, 국내 기업 공급망 실정에 맞는 요구사항이 필요할 것으로 보인다. 특히, 데이터 연계 시, 안전한 데이터에 연계 및 결합에 대한 '개인정보보호법' 등의 규정이 상이해 이에 따른 보안 요구사항 도출이 필요할 것이다.

또한, 현재 모든 스마트시티의 네트워크 보안은 망 분리에 대한 네트워크 보안 요구사항만 존재한다. 하지만, 최근 스마트시티에서 기기 간 또는 기기와 사람의 장비 간 원격 접속을 통한 데이터 연계의 경우도 다수 생겨났다. 이는 원격 접속에 대한 위험 또한 존재하는 것을 의미한다. 따라서 보안 요구사항에 네트워크망 분리의 요구사항만 필요한 것이 아닌 본 논문에서 제시한 제로 트러스트 개념을 이용하여, 망 분리의 한계점을 넘어서 스마트시티의 안전한 보안 아키텍처를 확립하여 스마트시티 플랫폼에 도입할 수 있도록 추후 연구를 진행할 예정이다.

References

[1] National Institute of Standards and Technology, "GCTC SC3 Cybersecurity and Privacy Advisory Committee Guidebook", Jul. 2019

[2] Japan cabinet office, " SIP Second Phase, Smart City Architecture White Paper", Mar. 2020

[3] Ministry of Internal Affairs and Communications, "Smart City Security Guideline 2.0", Jun. 2021

[4] The National Cyber Security Centre, "nscs supply chain security", https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security, Nov.19.2021

[5] National Institute of Standards and Technology," Supply Chain Risk Management Practices for Federal Information Systems and Organizations" Special Publication 800-161, Apr. 2015

[6] International Standard, "Information security for supplier relationships – Part 1: Overview and concepts", ISO/IEC 27036-1, Apr. 2014

[7] International Standard, "Information security for supplier relationships – Part 2: Requirements", ISO/IEC 27036-2, Aug. 2014

[8] International Standard, "Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security", ISO/IEC 27036-3, Nov. 2013

[9] International Standard, "Information security for supplier relationships – Part 4: Guidelines for security of cloud services", ISO/IEC 27036-4, Oct. 2016
[10] International Standard, "Information technology – (O-TTPS) – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations", ISO/IEC 20243-1, Feb. 2016
[11] International Standard, "Information technology – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018", ISO/IEC 20243-2, Jan. 2018
[12] KISA, "Smart City Security Model", Dec. 2020
[13] European Cyber Security Organisation, "Overview of existing Cybersecurity standards and certification schemes v2", Dec. 2017
[14] National Institute of Standards and Technology, "Zero Trust Architecture", Special Publication 800-207, Aug. 2020
[15] International Standars, "Information Security Management", ISO/IEC 27001, 2013
[16] KISA, "ISMS-P Certification Guideline", Jul.2021
[17] Seong-hyun Min, Kyung-ho Son, "Comparative Analysis on ICT Supply Chain Security Standards and Framework", Journal of the Korea Institute of Information Security & Cryptology, 30(6), pp. 1189-1206, Dec. 2020

〈저자소개〉

이 현 진 (Hyun-jin Lee) 학생회원
2021년 2월: 강원대학교 컴퓨터정보통신공학과 졸업
2021년 3월~현재: 강원대학교 융합보안학과 석사과정
〈관심분야〉 공급망 보안, 보안성 시험·인증, 개인정보 비식별&Mydata 활용, 제로 트러스트 보안

손 경 호 (Kyung-ho Son) 종신회원
2015년 8월: 성균관대학교 컴퓨터공학과 박사졸업
2001년 1월~2018년 8월: 한국인터넷진흥원 팀장/단장/센터장
2018년 9월~현재: 강원대학교 교수
〈관심분야〉 IoT/CPS보안, 보안성 시험·인증, 개인정보 비식별& Mydata 활용