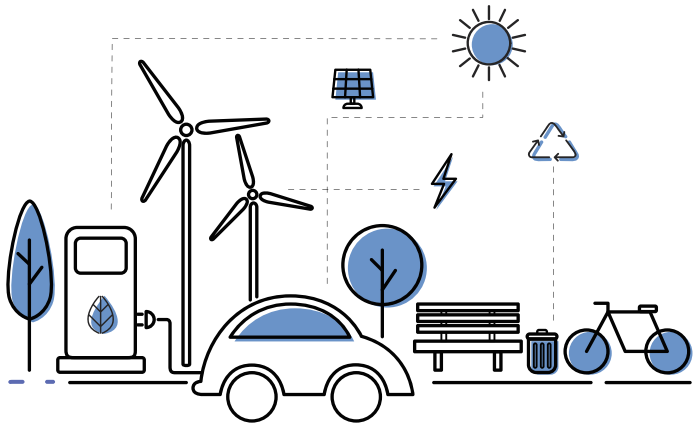
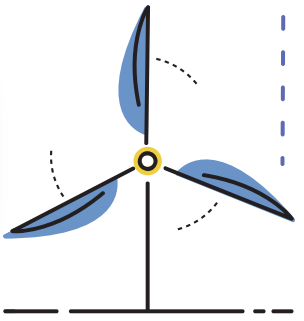
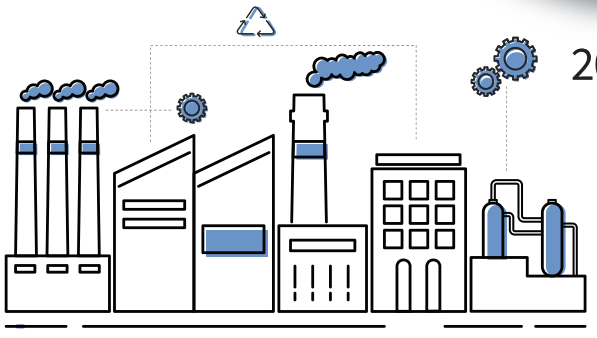
요약본



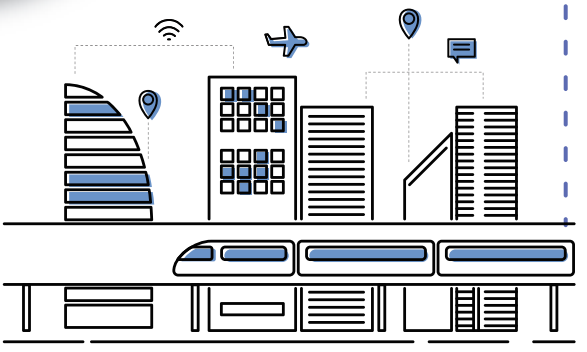
스마트시티 보안모델

PART Ⅰ : 스마트시티 및 서비스





2021. 12



과학기술정보통신부
Ministry of Science and ICT

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

제 1 장

배경 및 목적

세계는 급격하게 증가하는 도시화로 인한 다양한 문제에 직면해있다. 이러한 도시화 문제를 해결하기 위한 다양한 노력들이 진행되고 있으며 스마트시티도 그 중 하나의 방안이다.

스마트시티는 기존 도시의 양적, 경제적 성장을 초월하여 도시의 경쟁력과 삶의 질의 향상을 위해 다양한 기술을 융합 또는 복합적으로 적용하고 다양한 도시 서비스를 제공하는 지속가능한 도시를 목표로 하고 있다.

하지만 스마트시티는 정보통신기술이 매우 집약적으로 적용됨에 따른 사이버 공격에 노출되기 쉽다. 이러한 사이버 공격은 결국 스마트시티의 다양한 서비스를 무력화하고 도시 기능을 마비시킬 수 있으며 심각한 경우 시민의 생명에도 위협을 가할 수 있다. 따라서 스마트시티의 구축과 운영 시 확인되어야 할 보안 요구사항을 정의하기 위하여『스마트시티 보안모델』을 2020년 최초 개발하였다.

금번 개정 스마트시티 보안모델은 스마트서비스 보안 모델과 기존 사이버보안 가이드 · 지침 등과 관계와 지자체 등에서 스마트시티 사업의 추진 시점에 따라 즉시 적용 가능하도록 개정하였다.

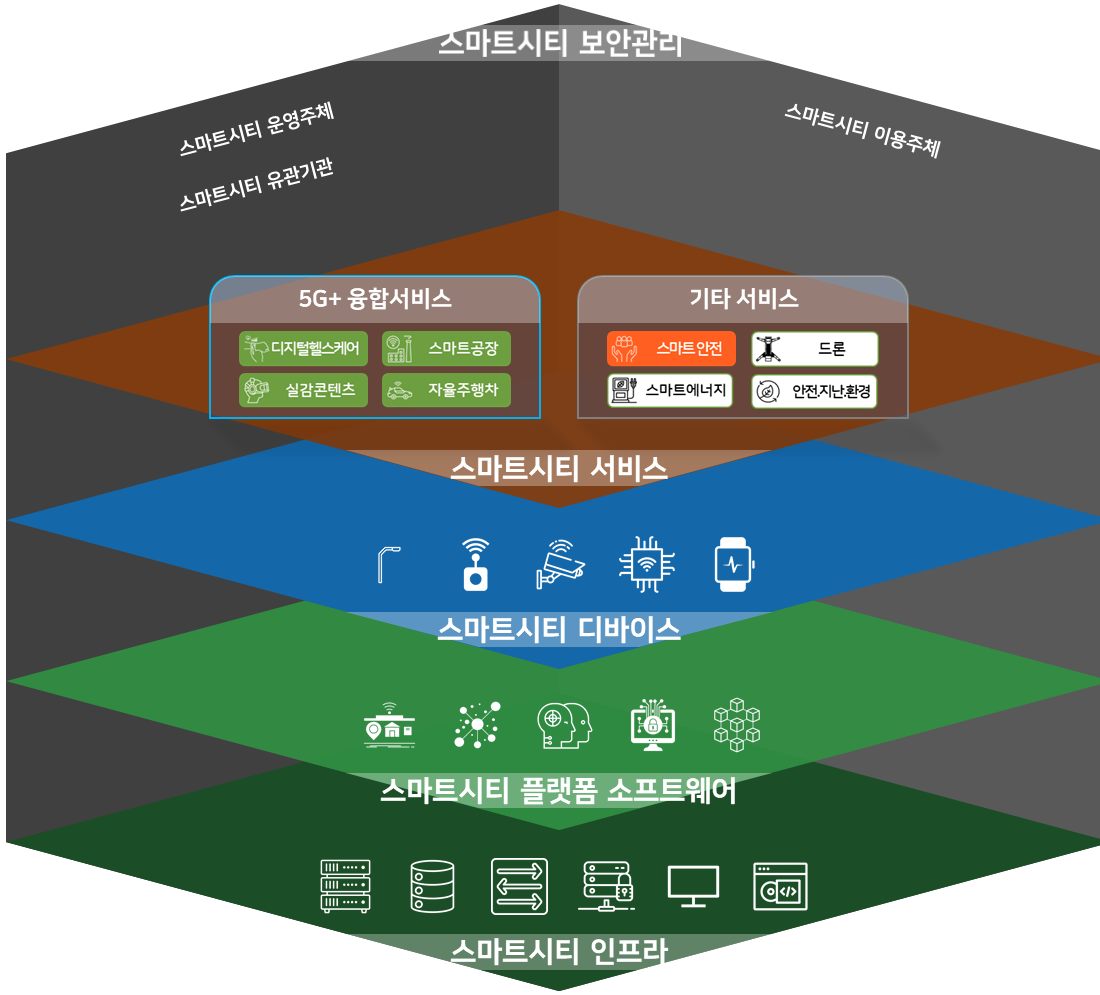
스마트시티의 구축을 계획하거나 추진 및 운영하는 지방자치단체, 스마트시티 서비스 제공을 위하여 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스 등을 개발 및 납품하는 민간기업 등에서 활용하여 보다 안전한 스마트시티로 발전하는데 이바지할 수 있기를 바란다.

제 2 장

스마트시티 구성요소

1 스마트시티 구성요소

그림 1 스마트시티 구성요소



스마트시티 이용주체

이용주체는 서비스를 이용하는 스마트시티의 시민 또는 스마트시티를 방문한 타 도시의 시민, 외국인 등이다. 그들은 스마트시티 서비스를 단순히 이용하는 것이므로 이용주체가 서비스를 이용함에 따른 보안 기능을 제공할 수는 있으나 보안요구사항은 제시할 수 없다.

※ 리빙랩, 규제 샌드박스 등에서는 시민이 직접 참여하게 되므로 '운영주체'로 볼 수 있으나, 그들이 이용하는 공간 / 절차 / 시설 등에 정보보호 통제를 적용하고 이행하도록 할 수 있으므로 보안 통제의 대상은 되지 않는다.

스마트시티 운영주체

운영주체는 스마트시티 서비스를 구상하고 시민과 방문객이 이용할 수 있도록 서비스를 제공하는 주체이다. 이들은, 더 안전한 스마트시티 서비스를 운영할 책임이 있으며 이에 따라 여러 가지 보안요구사항을 만족하여야 한다.

지방자치단체는 스마트시티를 기획·구축·운영하는 핵심 운영주체이다. 지방자치단체는 스마트시티 서비스를 운영하기 위하여 통합운영센터를 구축하고 관련 정보시스템을 이용하여 서비스가 시민과 방문객이 이용 가능하게 한다. 따라서 이들은 스마트시티 서비스의 기획 단계에서부터 정보보호 요구사항을 식별하고 서비스를 개발하여 정보보호가 적용된 정보시스템이나 디바이스를 활용한 서비스를 운영하여야 한다. 또한 통합운영센터는 모든 스마트시티 데이터가 집중되고 처리되는 곳이므로 각별한 보안 측면에서의 요구사항을 만족할 수 있어야 한다.

서비스 제공자는 지방자치단체이거나 지방자치단체가 선정한 스마트시티 서비스 운영자(SPC라 한다.)로 스마트시티 서비스를 구축 및 운영함에 있어 지방자치단체와 같은 지위를 갖는다. 따라서 지방자치단체와 같은 보안 측면에서의 요구사항을 만족할 수 있어야 한다.

※ SPC : 특수목적법인(Special Purpose Company)으로 스마트시티 서비스의 구축 및 운영을 목적으로 스마트시티가 선정하여 운영하는 민간부문 사업자이다.

스마트시티 유관기관

기타 관련 기관은 도시 관련 데이터를 제공하는 데이터 제공기관과 연계 서비스를 제공하는 연계기관으로 구분할 수 있다. 데이터 제공기관은 GIS·BIM 등을 제공하여 도시의 가상화(디지털트윈 등)를 지원하며, 연계기관은 시민의 응급상황에 대응하여 경찰 / 소방 / 병원 등에서 서비스를 제공하는 기관을 의미한다. 이러한 관련 기관은 서비스에 따라 직접적인 보안요구사항이 제시될 수 있으나 대부분 데이터 연계 / 연동

시 보안요구사항을 이행하거나 전달받은 정보의 안전한 관리가 주요한 보안요구사항이며 이러한 사항은 각 기관 자체적인 관리체계에서 그 요구사항을 충족해야 하므로 본 문서에서는 다루지 않는다.

※ GIS(Geographic Information System)는 지리정보시스템을 의미BIM(Building Information Modeling)은 건물(빌딩)정보모델링이라 불리며 다차원 가상공간에 가상으로 시설물을 모델링하는 과정을 의미한다.

스마트시티 인프라

스마트시티 인프라는 스마트시티 서비스를 구성하는 가장 기본적이며 고전적인 영역이다. 서버, 데이터베이스, 네트워크 장비, 보안장비, 관리PC 등 서비스 운영에 필요한 데이터의 수집 / 저장 / 이동 등의 역할을 담당한다. 특히 스마트시티 인프라는 지방자치단체가 운영하는 경우가 대부분이므로 주요정보통신기반시설과 동일한 보호체계가 요구된다.

스마트시티 플랫폼 소프트웨어

스마트시티 플랫폼 소프트웨어는 스마트시티 인프라와 더불어 스마트시티 서비스의 기본적인 영역에 속한다. 서비스 웹, 모바일 앱, 운영 소프트웨어, 스마트시티 플랫폼(데이터허브 플랫폼, IoT 플랫폼, 사이버보안 플랫폼, 디지털 트윈)이 포함되며 수집한 데이터를 처리하거나 이용주체가 요구한 서비스의 결과를 제공하기 위하여 데이터를 가공 후 정보를 제공하는 역할을 한다.

스마트시티 디바이스

센서, 사물인터넷, IoT 등의 디바이스는 스마트시티 서비스에서 데이터의 수집 역할을 담당한다. 정확한 데이터를 수집하여야 스마트시티 플랫폼 소프트웨어에서 처리하고 계획한 서비스를 제공할 수 있다. 또한 스마트시티 디바이스는 시민과 가장 가까이 위치하여 이용주체가 정상적으로 이용하는 것이 일반적이나 이용주체의 실수나 악의적인 의도를 가진 공격자에게 쉽게 노출될 수 있다. 이러한 장비적 특성에 따라 도난, 분실의 상황에서도 스마트시티 서비스에 주는 영향을 최소화할 수 있는 보안 설정이 필요하다. 이러한 보안 설정은 스마트시티 디바이스의 특성이 명확히 반영되어 있어야 하므로 「IoT 제품 대상 IoT 보안인증 적용 기준」을 보안요구사항 적용이 요구된다.

스마트시티 서비스

스마트시티 서비스는 스마트시티에서 제공되는 다양한 서비스 자체를 의미한다. 분류하는 기준에 따라 호칭도는 용어는 다를 수 있으나 스마트 교통, 스마트 헬스케어, 스마트 교육, 스마트 에너지, 스마트 환경, 스마트 안전, 스마트 생활, 스마트 공장, 실감콘텐츠, 자율주행차 등이 서비스될 수 있다.

스마트시티 보안관리

스마트시티 보안관리는 스마트시티 서비스를 운영하는 모든 구성요소를 관리하는 영역이다. 스마트시티 보안관리를 위해서는 운영 조직, 물리적 공간, 업무 절차, 업무처리용 정보시스템 및 업무시스템 등을 갖추어야 하며 이를 이용하여 스마트시티 서비스를 제공하는 업무를 수행하여야 한다. 이러한 업무에서 발생할 수 있는 각종 위험들은 다양하여 관리 · 물리 · 기술적 관점에서 포괄적인 보안요구사항이 적용 되어야 한다.

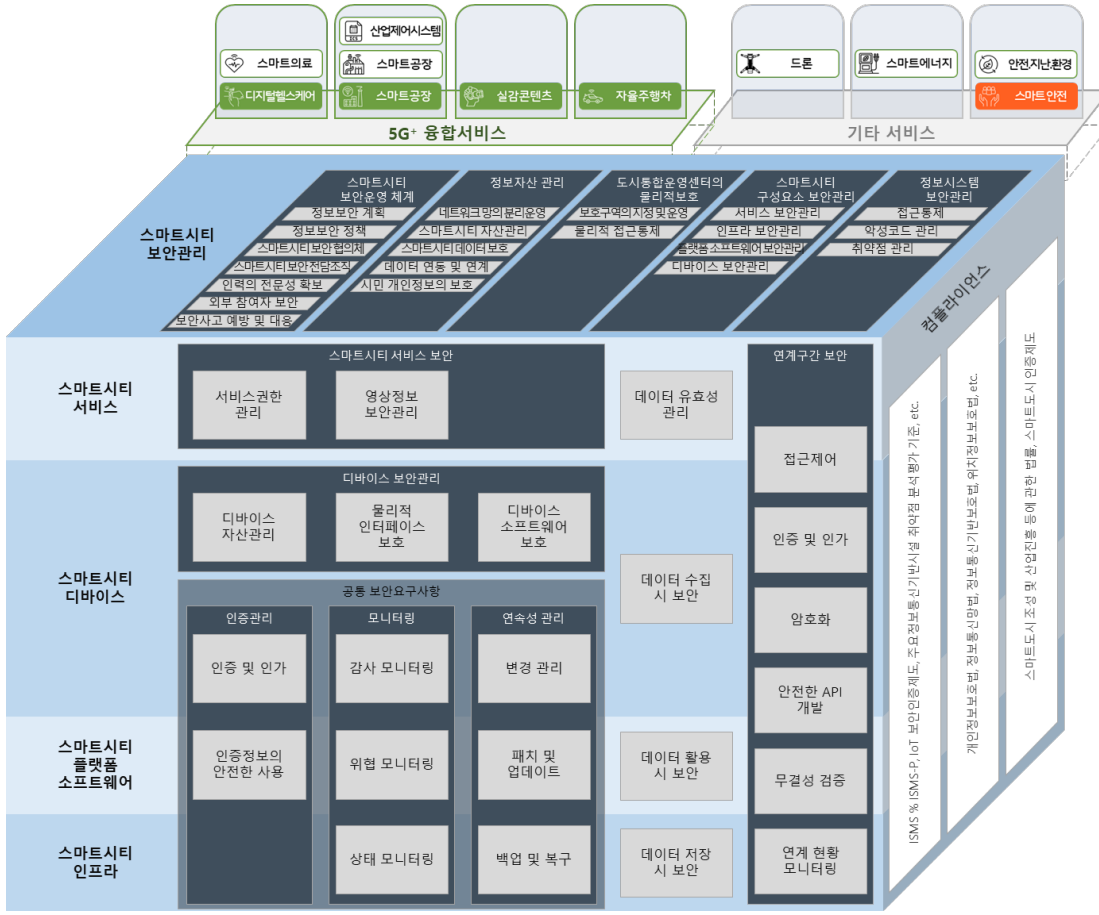
제 3 장

스마트시티 보안 모델

1 스마트시티 보안아키텍처

스마트시티를 구성하는 각 요소를 구조화하고, 보안요구사항을 반영하면 다음과 같다.

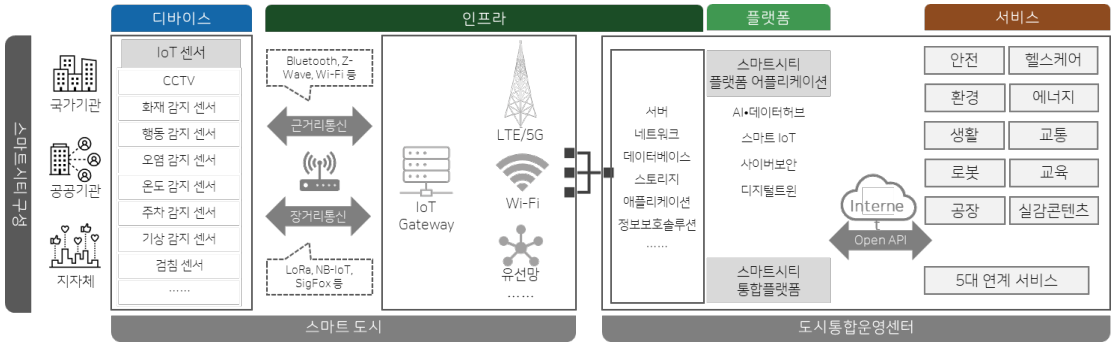
그림 2 스마트시티 보안아키텍처



2 스마트시티 보안 위협

스마트시티의 보안 위협은 스마트시티 구성요소 별 발생 가능한 공격의 가능성을 살펴보았다. 스마트시티 구성요소는 다음과 같이 다시 설명할 수 있다.

그림 3 서비스 흐름 중심의 스마트시티 구성도



위의 구성도에 따라 발생 가능한 보안 위협은 다음과 같이 정리할 수 있다.

그림 4 스마트시티 보안위협

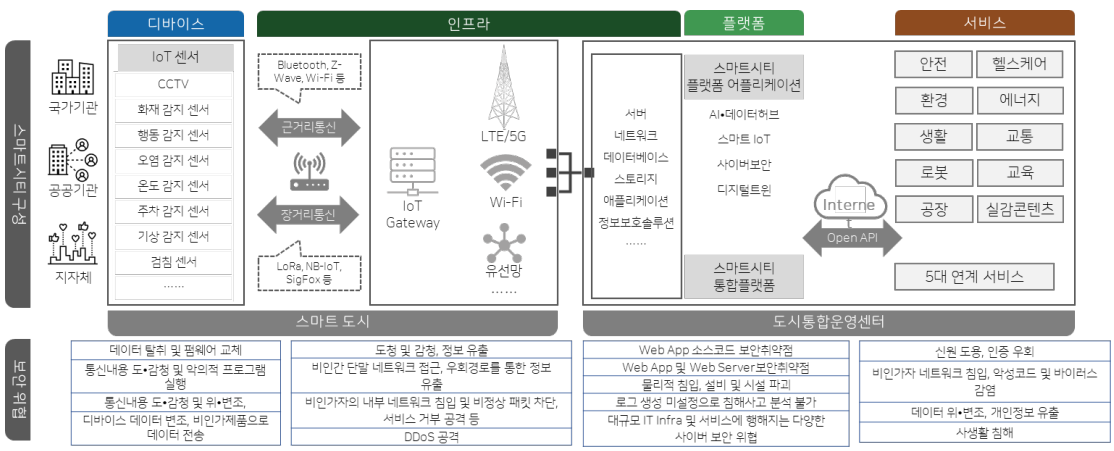


표 4 스마트시티 보안위협 상세설명

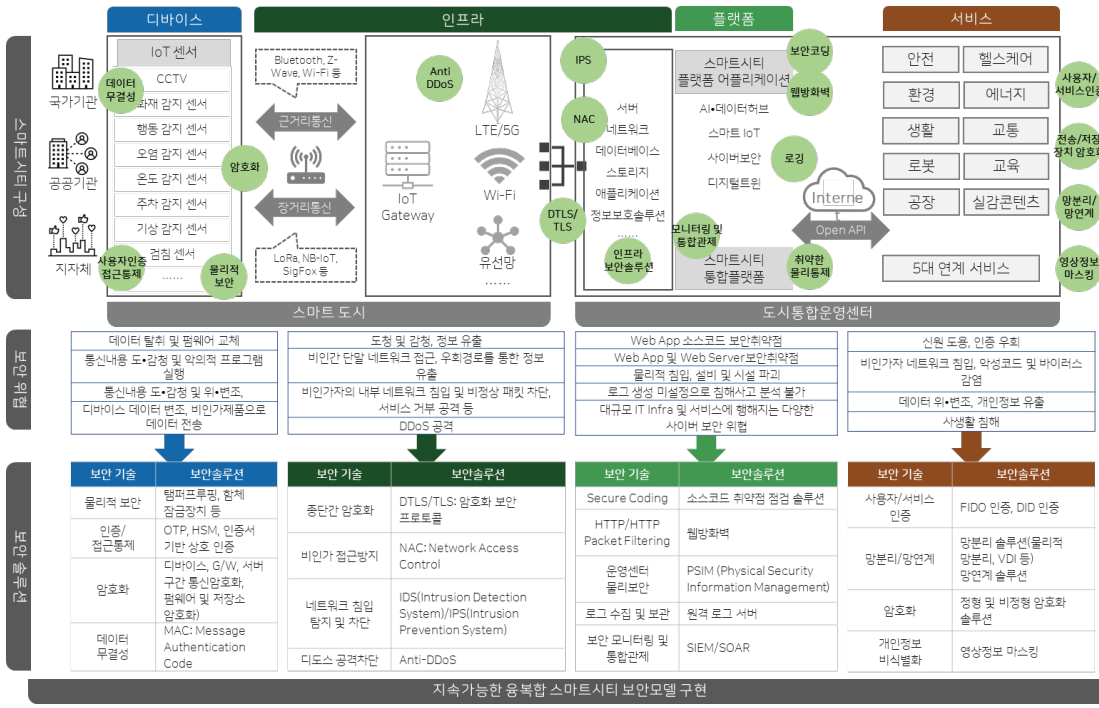
구분		내용
스마트시티 디바이스	특성	• 서비스 개방형으로 다수의 디바이스와 주변 환경이 상호연동 및 통합 • 디바이스간 성능의 차이 존재 (전력, 메모리, CPU, 사용기간 등) • 실감, 지능, 융합형 서비스 제공
	예시	• 통신기술(WiFi, 블루투스, LTE, IoT G/W, 등)을 이용한 영상기기(CCTV), 구동기기(IoT 센서, 드론, RF 자동차·헬기 등) 같은 다양한 단말 / 제어기기
	보안위협 / 취약점	• 가용성의 손상 • DoS 공격으로 인한 통신 방해 및 서비스 중지 • 악성코드 전이 • 악의적 프로그램 실행을 통한 디바이스 간 악성코드 전이 • 부적절한 암호사용 • 암호키 노출, 취약한 암호화로 인한 부적절한 암호사용 • 개인정보 변조, 유출 • 펌웨어 위변조에 의한 개인정보 변조, 유출
스마트시티 인프라 (네트워크)	특성	• 초연결 네트워크 (HW 자원, 통신방식, 보안구조 상이) • 저전력 통신망 • 멀티홉 라우팅 통신 • 트래픽 폭증
	예시	• 유선 LAN 부터 WIFI, LTE/5G, ZigGee와 같은 무선통신, 저전력 광대역 네트워크 LPWA와 무선 데이터를 주고받는 NFC 기술을 통해 디바이스와 플랫폼을 연결해주는 역할
	보안위협 / 취약점	• 도청 및 감청 • 관리자 인가없이 설치된 액세스 포인트 • 비인가 접근 • 무선랜에 연결하여 스나이핑 프로그램을 심어 금융정보를 가로챔 • 서비스 거부공격 • 사용자 수를 초과하여 접속함으로서 정상적인 사용자의 접속 자체를 방해 • Rouge AP • 통신 시스템 사이를 불법적으로 엿듣고 세션ID를 캡쳐 하는 등 개인정보를 갈취

구분		내용
스마트시티 인프라 / 스마트시티 플랫폼 소프트웨어	특성	• 멀티 도메인 서비스 플랫폼 • IP 기반 경량 서비스 플랫폼 • 생산된 데이터의 시민 공유와 활용 지원 • 도시핵심 데이터의 연계, 저장, 분석과 데이터 중심 협업 환경을 제공
	예시	• 디바이스, IoT 게이트웨이 등 암호화 통신 기능이 기반이 된 IoT 통합 플랫폼 구축 • 웹 개발 포탈, 응용 서비스 기능, 공공 데이터 연계, 스트리밍 기능 같은 하드웨어를 응용한 응용 플랫폼과 openAPI, 공통 서비스 기능, 디바이스 프로토콜과 같이 데이터를 공유해 타 플랫폼과 상호 연계를 진행하는 공통 플랫폼이 있음
	보안위협 / 취약점	• 잘못된 설계 구현 • 플랫폼 설계 과정의 부적절한 업데이트 프로세스, 소프트웨어 버그 등 취약한 부분의 보안 위협 • 중간자 공격 • 세션 하이재킹, 스니핑 등 통신하는 두 당사자 사이에 끼어들어 들키지 않고 통신 내용을 변경 • 부적절한 접근 통제 • 네트워크의 서버, 주요정보 등에 비인가 불법 접근 • 부적절한 물리적 통제 • 하드웨어, USB 포트 등 물리적방법을 통해 서버에 무단접근해 플랫폼 데이터 손상
스마트시티 서비스	특성	• OPEN API 기반 IoT 서비스 • 개방형 플랫폼을 기반으로 상호작용을 통해 도시 문제를 해결
	예시	• 스마트시티 플랫폼과 연계된 다양한 실질적 지원 서비스
	보안위협 / 취약점	• 데이터 손실 • 서비스 데이터 위변조를 통한 연계망 서비스 데이터 손실 • 미흡한 권한 관리 • 미흡한 사용자 권한 관리에 따른 개인정보, 인증정보, GIS, 위치 정보의 노출 • 부적절한 인적행위 • 사용자 부주의로 인한 부적절한 인적 행위 • 사생활 침해 • 센서, 통합시스템, 빅데이터, 개인정보를 기반으로 융합 도시가 만들어지는 스마트시티의 개인 사생활 침해 우려

3 스마트시티 보안 솔루션

스마트시티 구성도에서 보안위협은 다양한 위치에서 발생할 수 있다. 하지만 스마트시티 구성요소에 발생 가능한 보안위협을 예측, 예방, 대응 및 조치 가능한 보안 솔루션이 존재하므로 스마트시티에 적용할 수 있다.

그림 5 스마트시티에 적용 가능한 보안솔루션



위의 구성도에 따라 발생 가능한 보안 위협은 다음과 같이 정리할 수 있다.

표 6 스마트시티에 적용 가능한 보안솔루션 현황

스마트시티 디바이스			
보안기술	보안솔루션 예시	사용 목적	관리 가능한 보안위협
물리적보안	탬퍼프루핑, 함체 잠금장치 등	디바이스의 물리적 보안 강화	데이터 탈취 및 펌웨어 교체
인증/접근통제	OTP, HSM, 인증서 기반 상호 인증	수집데이터의 위변조 탈취, 삭제를 막기 위한 인증 솔루션 도입	통신내용 도·감청 및 악의적 프로그램 실행
암호화	디바이스, G/W, 서버 구간 통신암호화, 펌웨어 및 저장소 암호화	펌웨어 보안을 위한 암호화	통신내용 도·감청 및 위·변조,
데이터 무결성	MAC: Message Authentication Code	데이터에 메시지 인증 코드를 첨부하고, 서버에서 이를 검증	디바이스 데이터 변조, 비인가제품으로 데이터 전송

스마트시티 인프라			
보안기술	보안솔루션 예시	사용 목적	관리 가능한 보안위협
종단간 암호화	DTLS/TLS: 암호화 보안 프로토콜	패킷 도청 및 감청을 막는 데이터 암호화 기능 지원	도청 및 감청, 정보 유출
비인가 접근방지	NAC: Network Access Control	네트워크에 접근 기기를 검사해 네트워크 무결성을 유지	비인간 단말 네트워크 접근, 우회경로를 통한 정보 유출
네트워크 침입 탐지 및 차단	IDS(Intrusion Detection System)/IPS(Intrusion Prevention System)	내부 네트워크로 유입되는 패킷의 이상행위 탐지 및 차단	비인가자의 내부 네트워크 침입 및 비정상 패킷 차단, 서비스 거부 공격 등
디도스 공격차단	Anti-DDoS	DDoS 공격 발생 시 네트워크 임계치를 기준으로 네트워크 유입량을 조절	DDoS 공격

스마트시티 플랫폼 소프트웨어			
보안기술	보안솔루션 예시	사용 목적	관리 가능한 보안위협
Secure Coding	소스코드 취약점 점검 솔루션	소스코드에 존재하는 잠재적 보안취약점 제거	Web App 소스코드 보안취약점
HTTP Packet Filtering	웹방화벽	Web App 기반의 공격 패킷 탐지 및 차단	Web App 및 Web Server 보안취약점
운영센터 물리보안	PSIM	물리보안 통합 관리 플랫폼	물리적 침입, 설비 및 시설 파괴
로그 수집 및 보관	원격 로그 서버	하드웨어에 접근하는 사용자의 이력 통제 및 기록	로그 생성 미설정으로 침해사고 분석 불가
보안 모니터링 및 통합관제	SIEM/SOAR	사이버 공격에 대비한 실시간 모니터링, 이상행위 및 공격 탐지, 위협 대응	대규모 IT Infra 및 서비스에 행해지는 다양한 사이버 보안 위협

스마트시티 서비스			
보안기술	보안솔루션 예시	사용 목적	관리 가능한 보안위협
사용자/서비스 인증	FIDO 인증, DID 인증	사용자 및 서비스 보안을 위한 본인 인증 방식	신원 도용, 인증 우회
망분리/망연계	망분리 솔루션 (물리적 망분리, VDI 등) 망연계 솔루션	업무망과 인터넷망을 분리하는 망분리 솔루션	비인가자 네트워크 침입, 악성코드 및 바이러스 감염
암호화	정형 및 비정형 암호화 솔루션	DB 데이터 암호화 및 영상, 음성, 이미지 등 개인정보 암호화	데이터 위·변조, 개인정보 유출
개인정보 비식별화	영상정보 마스킹	민감 개인정보보호를 위한 자동 마스킹 기능	사생활 침해

제 4 장

스마트시티 보안요구사항

1 스마트시티 보안관리

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.1 스마트 시티 보안 운영 체계	1.1.1 정보 보안 계획	· 스마트 도시를 향한 발전계획에는 정보보안과 관련한 위협을 식별하고 이를 개선할 수 있는 정보보안 계획이 포함되어야 한다.	기획 단계	· 스마트시티 추진 계획에 정보보안 관련 계획을 수립한다.	· 스마트 도시 발전계획에 정보보안과 관련한 구체적인 계획을 수립하고 있으며, 해당 정보보안 계획이 스마트시티 구축 및 운영 전 단계에 걸쳐 누락 없이 이행되고 있는지 확인한다.	· 스마트도시 발전 및 정보보안에 대한 계획을 수립하고 계획의 이행 여부를 연 단위로 확인하여야 한다.
			운영 단계	· 스마트시티 관련 정보보안 정책을 기반으로 구체적인 스마트시티 정보보안 추진 계획을 수립 및 적용한다.		
			발전 단계	· 스마트시티 정보보안 계획을 완료하기 전 시민과 스마트시티 보안 협의체의 의견을 수렴하여 계획을 이행한다.		
	1.1.2 정보 보안 정책	· 스마트시티는 운영 주체와 관련 민간업체 등에 적용 가능한 정보보안 정책을 수립 후 운영하여야 한다.	기획 단계	· 스마트시티는 운영 주체와 관련 민간업체 등에 적용 가능한 정보보안 정책을 수립 후 운영하여야 한다.	· 스마트시티에서 적용 가능한 별도의 정보보안 정책을 수립하여야 하며, 시민 및 관련기관 등 이해관계자와의 지속적인 거버넌스를 통해 갱신되고 있는지 확인한다.	· 스마트시티에 적용 가능한 보안정책을 수립하고 주기적으로 대내외 환경 변화에 따라 제개정을 수행하여야 한다.
			운영 단계	· 스마트시티 서비스를 대상으로 한 별도의 정보보안 정책을 수립하고 운영해야 한다.		
			발전 단계	· 스마트시티 전체를 그 범위로 하는 정보보안 정책은 참여자들이 접근하여 의사소통할 수 있다.		

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.1 스마트 시티 보안 운영 체계	1.1.3 스마트 시티 보안 협의체	· 스마트시티 보안 협의체는 스마트시티 내 발생 가능한 위험에 대한 분석, 검토, 이행계획의 수립 및 승인 등을 수행할 수 있어야 한다.	기획 단계	· 운영 주체의 정보보안 협의체 등 스마트시티 보안 협의체를 자체적으로 구성한다.	· 스마트시티 보안 협의체를 지자체, 관련기관, 참여업체, 외부 보안 전문가, 시민 등으로 구성하고 구체적인 의사결정 권한 및 절차에 따라 운영하는지 확인한다.	· 스마트시티 보안 협의체를 구성하고 운영하여야 한다.
			운영 단계	· 스마트시티 보안 협의체를 운영하며, 외부 전문가를 일부 포함한다.		
			발전 단계	· 스마트시티 외부 전문가, 시민 등을 포함하며, 구체적인 의사결정 권한 및 절차가 명시된 스마트시티 보안 협의체를 구성 및 운영한다.		
	1.1.4 스마트 시티 보안 전담 조직	· 스마트시티 서비스의 운영, 관리를 위한 전담 인력을 지정하고 운영하여야 한다.	기획 단계	· 스마트시티 보안을 위한 전담 조직은 없으나, 자체 정보보안 조직이 그 역할을 대신한다.	· 스마트시티의 보안을 위하여 스마트시티 보안 관련 전문적인 지식을 보유한 인력으로 전담 조직을 구성하여 운영하며, 부족한 지식을 보완하기 위하여 외부 전문가 등과 협의하고 있는지 확인한다.	· 보안에 대한 전문적인 지식이 있는 인력을 뽑아 보안 전담 조직을 구성하고 운영하여야 한다.
			운영 단계	· 스마트시티 보안을 위한 전담 조직을 구성하여 운영한다.		
			발전 단계	· 스마트시티 보안과 관련한 전문적 지식을 보유한 전담 조직을 운영하며, 외부 전문기관 등과 협업한다.		
	1.1.5 인력의 전문성 확보	· 전담 인력은 스마트시티 및 스마트시티 보안에 관한 전문적 지식을 지속적으로 습득하여 활용 가능하도록 교육하여야 한다.	기획 단계	· 기본적인 정보보안 교육을 이수한다.	· 스마트시티 보안 전담 조직의 구성원을 대상으로 스마트시티 보안모델 및 보안기술에 관한 정기적인 교육 프로그램을 수립하여 운영하는지 확인한다.	· 스마트시티 보안 전담 조직의 구성원을 대상으로 교육 계획을 수립하고 이행하여야 한다
			운영 단계	· 스마트시티 관련 보안모델, 보안기술을 학습한다.		
			발전 단계	· 정기적인 교육 프로그램에 따라 스마트시티 정보보안 관련 지식을 습득한다.		
	1.1.6 외부 참여자 보안	· 스마트시티 운영 및 서비스에 참여하는 모든 외부자는 보안 요구사항을 계약서에 명시하고 보안 서비스수준(보안 SLA) 협약을 이행하여야 한다.	기획 단계	· 스마트시티 운영 및 서비스 제공과 관련한 모든 외부자는 계약서에 보안과 관련한 사항을 명시한다.	· 스마트시티 운영 및 서비스에 참여하는 외주업체, SPC, 보안 전문가 등과의 협업 시 보안 서비스수준(보안 SLA)을 계약서에 명시하고 확인해야 한다.	· 스마트시티 서비스와 관련된 외부 업체 및 인력 계약 시 스마트시티 보안정책에 따른 보안 요구사항을 명시하여 계약을 진행하여야 한다.

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.1 스마트시티 보안 운영 체계	1.1.6 외부 참여자 보안		운영 단계	· 계약서 또는 협약서에 구체적인 연계 항목, 방법, 절차를 명시하여 계약한다.		
			스마트시티 보안운영 체계	· 스마트시티 보안 협의체 또는 거버넌스를 통해 확정된 보안활동이 외부자에게 전달되고 즉시 이행할 수 있는 체계가 운영된다.		
	1.1.7 보안 사고 예방 및 대응	· 스마트시티의 지속가능한 서비스 제공을 위하여 보안 사고 예방 및 대응방안을 수립하고 운영하여야 한다.	기획 단계	· 보안사고의 대응을 위한 탐지, 대응, 분석, 공유 활동이 포함된 보안 사고대응 계획을 수립한다.	· 스마트시티에서 발생 가능한 보안 사고에 대한 탐지, 대응, 분석, 공유 등의 활동이 가능한 보안사고대응 계획을 수립하고 해당 계획에 이행하며, 사이버 보안 플랫폼 등 스마트시티 플랫폼을 활용한 체계를 운영하는지 확인한다.	· 보안사고대응 계획을 수립하여 적용하고 매년 계획의 검토를 통해 적절성을 확인하여야 한다.
			운영 단계	· 보안사고대응 계획에 따른 지속적인 훈련을 실시하고, 실시간 모니터링을 수행하여 사고발생에 따른 즉각적인 대응이 가능하다.		
			발전 단계	· 스마트시티 플랫폼을 이용하여 위협의 모니터링 및 초기대응이 가능하다.		
1.2 정보자산 관리	1.2.1 네트워크 망의 분리 운영	· 스마트시티 플랫폼 및 서비스의 운영을 위한 네트워크, 데이터 허브 등 공유 네트워크, 서비스 네트워크 등은 그 특성에 맞게 물리적 또는 논리적으로 분리되어야 한다.(법적 요구사항 존재시)	기획 단계	· 스마트시티 도시통합 운영센터 운영을 위한 독립적인 망 분리계획을 수립한다.(법적 요구사항 존재시)	· 스마트시티 서비스 운영을 위한 인프라, 플랫폼 소프트웨어, 디바이스는 중요도 또는 법적 요구사항에 따라 물리적 또는 논리적으로 분리하여 운영한다.	· 스마트시티 서비스 운영에 필요한 네트워크는 중요도 및 법적 요구사항에 따라 망분리를 수행하여야 한다.(법적 요구사항 존재시)
			운영 단계	· 스마트시티 서비스에 필요한 구성요소를 분리된 망에서 운영하며, 서비스 운영에서 반드시 필요한 기관과 연계한다.(법적 요구사항 존재시)		
			발전 단계	· 스마트시티 내 데이터 공유체계를 수립하여 분리된 망과 연계영역을 식별하고 데이터 연계를 적용한다.(법적 요구사항 존재시)		

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.2 정보 자산 관리	1.2.2 스마트 시티 자산 관리	· 스마트시티 서비스와 관련한 모든 자산은 항상 그 현황이 유지되고 운영 및 관리의 범주 내에 있어야 한다.	기획 단계	· 스마트시티 서비스 구축 시 자산식별 후 목록화하여 유지하고 있다.	· 스마트시티 서비스와 관련된 모든 자산들의 현황을 최신으로 유지하고 운영 및 관리한다.	· 스마트시티 서비스와 관련된 모든 자산을 식별하여 자산 리스트를 만들고 주기적으로 업데이트하여 최신으로 유지해야 한다.
			운영 단계	· 스마트시티 서비스와 관련한 모든 자산을 식별 후 목록화하고 지속적으로 갱신하고 있다.		
			발전 단계	· 스마트시티 서비스 관련 자산의 목록화 이후 자산식별 및 관리 시스템을 이용하여 자동화하여 관리한다.		
	1.2.3 스마트 시티 데이터 보호	· 스마트시티 내에서 공개 불가능한 중요 데이터를 식별 후 비인가자가 처리할 수 없도록 안전하게 보호하여야 한다.	기획 단계	· 스마트시티에 수집되는 데이터는 관계기관에만 공유되며, 행정망 등 폐쇄적 환경에서만 사용한다.	· 공개가 불가능한 중요 데이터는 식별 후 비인가자가 처리할 수 없도록 안전하게 보호한다.	· 중요 데이터를 식별하여 목록화하고 식별된 데이터는 접근 통제 정책을 적용하는 등 비인가자가 접근, 처리할 수 없도록 대책을 적용하여야 한다.(암호화)
			운영 단계	· 공개 불가능한 데이터를 식별하고 데이터 암호화, 망연계 등 기술적 보완방안을 적용한다.		
			발전 단계	· 모든 데이터를 공개 가능한 형태 및 내용으로 변환하고 데이터 연동 및 연계 체계에 따라 공유한다.		
	1.2.4 스마트 시티 데이터 연동 및 연계	· 스마트시티 플랫폼, 서비스, 유관 기관, 운영업체 등과의 데이터 연계 및 연동에 관한 기준을 수립하고 연계 구간에서의 위협을 미연에 방지하여야 한다.	기획 단계	· 스마트시티 플랫폼, 서비스, 유관 기관, 운영업체 등과의 데이터 연계 및 연동 기준을 수립한다.	· 스마트시티 데이터 연동 및 연계에 대한 기준을 수립한다. · 데이터 연동 및 연계 구간에 위협이 발생하지 않도록 암호화 등과 같은 통제 정책을 적용한다.	· 스마트시티 데이터 연동 및 연계에 대한 기준 및 접근 통제 정책을 수립하여 적용한다. (인증/접근통제, 망분리/망연계)
			운영 단계	· 데이터 연동 API, 전송구간 데이터 무결성, 데이터 기밀성을 고려하여 사전 승인된 기관에서만 활용하도록 통제한다.		
			발전 단계	· 스마트시티 데이터를 공개 가능하도록 식별 및 변환하고 연동 및 연계되는 데이터 무결성을 모니터링하여 사고 발생 전 조치한다.		

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.2 정보 자산 관리	1.2.5 시민 개인 정보의 보호	· 시민의 개인정보는 안전하게 법률에 따라 처리되어야 한다.	기획 단계	· 스마트시티 서비스를 통해 처리되는 시민의 개인정보를 식별하고 보안통제를 적용한다.	· 시민의 개인정보는 관련 법률에 의거하여 안전하게 처리한다.	· 시민이 스마트시티 서비스를 이용하기 전 개인식별정보, 개인영상정보, 개인위치정보 등 개인정보는 관련 법률에 따라 각종 동의를 득하고, 개인정보의 수집, 전송, 저장에 따라 각각에 알맞은 암호화를 적용하여야 한다.(암호화, 개인정보 비식별화)
			운영 단계	· 스마트시티 보안협의체의 승인과 운영주체의 개인정보 내부관리지침에 따라 보안통제를 적용 후 처리한다.		
			발전 단계	· 거버넌스를 활용하여 스마트시티 서비스 내 정보주체의 개인정보 선택권을 보장한다.		
1.3 도시 통합 운영 센터의 물리적 보호	1.3.1 보호 구역의 지정 및 운영	· 스마트시티 서비스를 구성하는 인프라, 디바이스, 설비 등을 보관하는 장소를 보호구역으로 지정하고 안전하게 관리하여야 한다.	기획 단계	· 전산실, 통합운영센터를 보호구역으로 지정하고 관리한다.	· 스마트시티 서비스를 구성하는 인프라, 디바이스, 설비 등이 설치, 보관된 장소는 보호구역으로 지정한다. · 보호구역 내 설비들은 안전하게 관리한다.	· 스마트시티 서비스를 구성하는 인프라, 디바이스, 설비 등을 보호가기 위하여 통제구역, 제한구역, 접견구역등 물리적 보호 구역 지정기준을 수립/이행하고 구역별 보호대책을 수립/이행하여야 한다.(운영센터 물리보안)
			운영 단계	· 도시 내 설치된 디바이스의 물리적 보호를 위한 설비를 구축한다.		
			발전 단계	· 전산실, 통합운영센터, 도시 내 디바이스 등 스마트시티 서비스와 관련된 모든 물리공간을 식별하고 필요한 보호구역을 지정하여 운영한다.		
	1.3.2 물리적 접근 통제	· 통합운영센터, 센터 내 인프라 및 어플리케이션에 접근 가능한 인력은 사전에 식별되고 제한적으로 허용되어야 한다.	기획 단계	· 출입 대장, 접근현황이 문서로 관리된다.	· 통합운영센터, 센터 내 인프라 및 어플리케이션에 접근 가능한 인력을 식별하여 접근통제를 적용한다.	· 통합운영센터, 센터 내 인프라 및 어플리케이션에 접근 가능한 인력을 식별하여 출입권한을 부여하고, 출입 기록 및 권한에 대한 주기적인 검토를 수행하여야 한다.(물리적 보안, 운영센터 물리보안)
			운영 단계	· 출입 및 접근에 관한 사항이 관련 시스템에서 관리된다.		
			발전 단계	· 출입 및 접근뿐 아니라 접근의 적절성이 시스템에서 관리된다.		
1.4 스마트 시티 구성 요소 보안 관리	1.4.1 스마트 시티 서비스 보안 관리	· 운영되는 스마트시티 서비스의 보안관련 문제점은 지속적으로 검토하여 개선하여야 한다.	기획 단계	· 스마트시티 서비스 내 보안 문제점의 지속적 검토 및 개선을 위한 구체적인 계획을 수립한다.	· 스마트시티 서비스의 보안 관련 문제점은 지속적으로 식별하고 검토하여 개선한다.	· 스마트시티 서비스의 보안 관련 문제점을 지속적인 점검을 통해 확인하고 검토하여 개선방안을 적용하여야 한다.(개발보안 및 Secure Coding)

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.4 스마트 시티 구성 요소 보안 관리	1.4.1 스마트 시티 서비스 보안 관리		운영 단계	· 스마트시티 서비스별 보안 문제점의 지속적 검토 및 개선이 수행된다.		
			발전 단계	· 스마트시티 서비스별 보안 문제점의 지속적 검토 및 개선과 더불어 서비스 간 문제점 및 개선방안이 공유되고 통합 운영된다.		
	1.4.2 스마트 시티 인프라 보안 관리	· 스마트시티 인프라는 스마트시티 서비스의 가용성 보장을 위하여 정상 동작 여부가 지속적으로 모니터링되어야 하며, 즉각적인 복구가 가능하여야 한다.	기획 단계	· 스마트시티 인프라의 정상 동작 기준을 정의하고 이에 따른 운영체계, 절차 및 설비의 구축 및 운영방안을 수립한다.	· 스마트시티 인프라는 가용성 보장을 위해 정상적인 동작 여부를 지속적으로 모니터링 한다. · 스마트 인프라에 문제가 발생한 경우 즉시 복구할 수 있는 대책 등을 마련해야 한다.	· 스마트시티 인프라의 동작 여부를 지속적으로 확인 및 모니터링하고 문제가 발견될 경우 즉시 복구할 수 있는 보안 절차를 마련해 적용하여야 한다. · 보안 모니터링 및 통합관제
			운영 단계	· 스마트시티 인프라의 운영체계, 절차, 설비를 정상 동작 기준에 따라 구축하고 운영한다.		
			발전 단계	· 스마트시티 인프라의 비정상 동작을 실시간 모니터링 하여 정상 동작 기준에 따라 비상대응체계를 운영한다.		
	1.4.3 스마트 시티 플랫폼 소프트웨어 보안 관리	· 스마트시티 플랫폼 소프트웨어는 개발 전단계에 보안 내재화(Security by design)가 적용되어야 한다.	기획 단계	· 스마트시티 플랫폼 소프트웨어의 개발 및 구축에 필요한 보안 요구사항을 사전에 정의하고 개발 및 구축 단계별 보안 내재화 방안을 수립한다.	· 스마트시티 플랫폼 소프트웨어는 개발 전 보안 내재화를 적용한다.	· 스마트시티 플랫폼 소프트웨어를 개발하기 전 전체적인 영역에 대한 보안 요구사항을 식별해 적용하여야 한다. (Secure Coding)
			운영 단계	· 스마트시티 플랫폼 소프트웨어의 보안 내재화 방안에 따라 개발 및 구축한다.		
			발전 단계	· 스마트시티 플랫폼 소프트웨어의 보안 내재화 적용할 수 있는 리빙랩 등 시험환경을 조성하고 운영한다.		

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.4 스마트시티 구성요소 보안 관리	1.4.4 스마트시티 디바이스 보안 관리	· 스마트시티 디바이스 자체의 보호와 디바이스에서 수행되는 정보 전송은 안전하게 보호되어야 한다.	기획 단계	· 스마트시티 디바이스를 물리적으로 보호하며, 디바이스에서 전송하거나 디바이스에 전송되는 정보를 보호하는 구체적인 방안을 수립한다.	· 스마트시티 디바이스와 디바이스를 통해 송수신되는 데이터들은 접근통제, 암호화 등의 방식으로 안전하게 보호한다.	· 스마트시티 서비스 내 통신망 및 네트워크를 이용하여 전송되는 모든 구간은 암호화 기술(SSL 인증서, 암호화 응용프로그램 설치, VPN 등)을 적용하여 보호하여야 한다.(물리적보안, 인증/접근통제, 암호화, 데이터 무결성)
			운영 단계	· 스마트시티 디바이스의 물리적 보호 및 정보 전송 구간에 대한 보안 대책을 적용한다.		
			발전 단계	· 디바이스에서 발생하는 물리적 위협, 전송구간의 위협을 모니터링하여 즉각 확인 및 조치한다.		
1.5 정보시스템 보안 관리	1.5.1 접근통제	· 비정상적인 접근을 제어할 수 있는 접근통제 정책을 수립하고 모든 스마트시티 구성요소에 적용하여야 한다.	기획 단계	· 스마트시티의 모든 구성요소 별 접근통제 정책을 수립한다.	· 스마트시티 구성요소에 이루어지는 비정상적인 접근을 통제할 수 있도록 접근통제 정책을 수립한다.	· 스마트시티 서비스 관련 시스템 및 중요정보에 대한 비인가 접근을 통제하기 위해 공식적인 계정 및 접근권한 등록, 해지, 변경, 삭제 절차를 수립/이행하고 주기적으로 검토하여야 한다. (인증/접근통제, 네트워크 침입 탐지 및 차단, 망분리/망연계)
			운영 단계	· 스마트시티 구성요소에 필요한 접근통제 정책을 적용한다.		
			발전 단계	· 스마트시티 접근통제 정책에 따라 비정상 접근을 실시간 모니터링하고 즉각 차단한다.		
	1.5.2 악성코드 관리	· 스마트시티에 악성코드가 감염되는 것을 고려하여 방지, 식별, 조치하는 절차가 운영되어야 한다.	기획 단계	· 악성코드로부터 스마트시티 구성요소 및 데이터의 보호를 위한 예방, 탐지, 대응 등이 포함된 보호 대책을 수립한다.	· 악성코드 감염에 대응할 수 있는 대응 절차를 수립하여 운영한다.	· 악성코드 대응을 위해 대응 절차(조치 방법, 신고 안내 등)를 수립/이행하여야 한다.(비인가 접근 방지, 보안 모니터링 및 통합관제)
			운영 단계	· 악성코드의 예방, 탐지, 대응 솔루션을 운영한다.		
			발전 단계	· 악성코드의 보호 대책을 이행할 수 있는 체계, 솔루션을 운영한다.		

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
1.5 정보 시스템 보안 관리	1.5.3 취약점 관리	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스의 취약점 정보를 지속적으로 확인하고 점검 후 조치하여야 한다.	기획 단계	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스의 취약점 정보를 지속적으로 확인하고 점검 후 조치할 수 있는 체계를 수립한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 주기적인 취약점 점검을 통해 취약점 정보를 확인한다. · 점검으로 발견된 취약점은 즉시 후속 조치를 수행한다.	· 스마트시티 서비스 내 모든 인프라, 플랫폼 소프트웨어, 디바이스는 주기적으로 취약점 분석을 수행하며, 발견되는 취약점은 조치를 취해야 한다. (보안 모니터링 및 통합관제)
			운영 단계	· 스마트시티 구축 시 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스의 취약점을 점검하고 조치한다.		
			발전 단계	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스의 취약점을 지속적으로 점검하고 조치하는 절차를 이행한다.		

2 스마트시티 인프라

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
2.1 인증 관리	2.1.1 인증 및 인가	· 스마트시티 인프라에 접근하려는 경우 인증 및 인가 절차에 따라 부여된 권한에 한하여 접근하도록 통제하여야 한다.	· 접근통제 정책에 따라 스마트시티 서비스의 모든 인프라에 접근 시 인증을 거쳐 접근하여야 한다.	· 스마트시티 서비스 접근통제 정책에 따라 모든 인프라에 대한 접근 시 인증을 거쳐 접근하고 있는지 확인한다.	· 스마트시티 서비스의 모든 시스템에 접근 시 사용자 인증, 로그인 횟수 제한, 불법 로그인 경고 등 안전한 사용자 인증 절차에 의해 접근하고, 1인 1계정 부여 및 목적에 따른 권한을 차등부여하여야 한다.(인증/접근통제)
	2.1.2 인증 정보의 안전한 사용	· 인증 및 인가에 사용되는 인증정보는 안전하게 관리되어야 한다.	· 인증 및 인가에 사용되는 인증정보를 안전하게 관리하는 절차가 수립/이행되어야 한다.	· 인증에 사용하는 인증정보(ID/PW, 인증키, 토큰 등)를 안전하게 관리하는 절차를 운영한다.	· 인증정보(ID/PW, 인증키, 토큰 등)의 안전한 관리를 위해 관리절차를 수립하고 적용하여야 한다.(암호화)
2.2 모니터링	2.2.1 감사 모니터링	· 스마트시티 서비스 내에서 수행되는 사용자 및 관리자의 행위 기록을 기반으로 모니터링이 수행되어야 한다.	· 스마트시티 서비스 내 시스템에 접근하는 사용자 및 관리자의 이상행위를 모니터링하여야 한다.	· 스마트시티 디바이스에 접근하는 사용자 및 관리자는 정상적인 행위가 아닌 경우를 모니터링한다.	· 스마트시티 서비스 내 인프라, 플랫폼 소프트웨어, 디바이스에 접근하는 사용자 및 관리자의 행위를 모니터링 하여 이상행위 여부를 모니터링하여야 한다.(로그 수집 및 보관)

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
2.2 모니터링	2.2.2 위협 모니터링	· 스마트시티 서비스의 위협을 고려하여 취약점 및 악성코드가 지속적으로 감시되고 반영되어야 한다.	· 스마트시티 서비스 내 관련 취약점에 대한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인하고 점검하여야 한다.	· 스마트시티 디바이스 관련 취약점에 관한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인한다.	· 스마트시티 서비스 내 인프라, 플랫폼 소프트웨어, 디바이스와 관련된 취약점에 관한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인하고, 취약점 정보에 대한 내부 적용 여부를 검토하여 적용하여야 한다.(보안 모니터링 및 통합관제)
	2.2.3 상태 모니터링	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정상적인 동작 여부를 실시간으로 알 수 있어야 한다.	· 스마트시티 인프라의 상태 값에 대해 모니터링해야 한다.	· 스마트시티 인프라는 정상 동작뿐 아니라 상태 값을 주기적으로 확인하고 있다.	· 스마트시티 인프라의 각 장비 별 성능, 용량 등을 지속적으로 모니터링하여야 한다. (보안 모니터링 및 통합관제)
2.3 연속성 관리	2.3.1 변경 관리	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정, 세부 현황의 변경이 기록되고 검토되어야 한다.	· 스마트시티 관련 모든 정책, 설정값 등 모든 변경사항은 기록/관리되어야 한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정값, 현황 등의 모든 변경사항을 기록한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정값 등 모든 변경사항이 기록되고 관리되어야 한다.
	2.3.2 보안 패치 및 업데이트	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용되어야 할 보안 패치를 지속적으로 확인하여 적용에 따른 영향도를 고려하여 지체없이 적용하여야 한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용해야 할 보안 패치 및 업데이트를 모니터링해야 한다.	· 스마트시티 인프라에 적용되어야 할 패치 및 업데이트를 지속적으로 모니터링 한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용되어야 할 보안 패치 및 업데이트 정보를 지속적으로 확인 및 모니터링 하여야 한다.
	2.3.3 백업 및 복구	· 스마트시티 서비스의 가용성 확보를 위하여 데이터, 설정값등의 백업과 백업본을 이용한 복구계획이 수립 및 운영되어야 한다.	· 스마트시티 서비스의 모든 데이터 및 설정값에 대한 백업 계획에 따라 백업을 수행해야 한다.	· 스마트시티 인프라의 가용성, 데이터 무결성 등을 확보하기 위하여 모든 데이터 및 설정값에 대한 백업 계획에 따라 백업을 수행한다.	· 스마트시티 인프라의 가용성, 데이터 무결성 등을 확보하기 위해 모든 데이터 및 설정값에 대한 백업 및 복구 계획을 수립하고 계획에 따라 수행하여야 한다.
2.4 데이터 흐름 관리	2.4.1 데이터 저장 시 보안	· 스마트시티 서비스 중 저장되는 데이터 중 암호화가 필요한 데이터는 안전한 암호 알고리즘으로 암호화하여야 한다.	· 스마트시티 인프라에 저장되는 데이터 중 암호화 대상을 식별하고 식별된 데이터는 암호화하여 저장해야 한다.	· 스마트시티 인프라에 저장하는 데이터 중 암호화의 대상을 식별하여 암호화 후 저장한다.	· 스마트시티 인프라에 저장하는 데이터 중 암호화 적용 대상을 식별하고 식별된 데이터는 암호화를 적용해 저장하여야 한다.(암호화)

3 스마트시티 플랫폼 소프트웨어

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
3.1 인증 관리	3.1.1 인증 및 인가	· 스마트시티 서비스에 접근하려는 경우 인증 및 인가 절차에 따라 부여된 권한에 한하여 접근하도록 통제하여야 한다.	· 접근통제 정책에 따라 스마트시티 서비스의 모든 인프라, 플랫폼 소프트웨어, 디바이스, 네트워크 등에 접근 시 인증을 거쳐 접근하여야 한다.	· 스마트시티 서비스 접근통제 정책에 따라 플랫폼 소프트웨어에 대한 접근 시 인증을 거쳐 접근한다.	· 스마트시티 서비스의 모든 시스템에 접근 시 사용자 인증, 로그인 횟수 제한, 불법 로그인 경고 등 안전한 사용자 인증 절차에 의해 접근하고, 1인 1계정 부여 및 목적에 따른 권한을 차등 부여하여야 한다. (사용자/서비스 인증)
	3.1.2 인증 정보의 안전한 사용	· 인증 및 인가에 사용되는 인증정보는 안전하게 관리되어야 한다.	· 인증 및 인가에 사용되는 인증정보를 안전하게 관리하는 절차가 수립/이행되어야 한다.	· 인증에 사용하는 인증정보(ID/PW, 인증키, 토큰 등)를 안전하게 관리하는 절차를 운영한다.	· 인증정보(ID/PW, 인증키, 토큰 등)의 안전한 관리를 위해 관리절차를 수립하고 적용하여야 한다.(암호화)
3.2 모니터링	3.2.1 감사 모니터링	· 스마트시티 서비스 내에서 수행되는 사용자 및 관리자의 행위 기록을 기반으로 모니터링이 수행되어야 한다.	· 스마트시티 서비스 내 시스템에 접근하는 사용자 및 관리자의 이상행위를 모니터링하여야 한다.	· 스마트시티 플랫폼 소프트웨어에 접근하는 사용자 및 관리자는 정상적인 행위가 아닌 경우를 모니터링 한다.	· 스마트시티 서비스 내 인프라, 플랫폼 소프트웨어, 디바이스에 접근하는 사용자 및 관리자의 행위를 모니터링하여 이상행위 여부를 모니터링하여야 한다.(로그 수집 및 보관)
	3.2.2 위협 모니터링	· 스마트시티 서비스의 위협을 고려하여 취약점 및 악성코드가 지속적으로 감시되고 반영되어야 한다.	· 스마트시티 서비스 내 관련 취약점에 대한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인하고 점검해야 한다.	· 스마트시티 플랫폼 소프트웨어 관련 취약점에 관한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인한다.	· 스마트시티 서비스 내 인프라, 플랫폼 소프트웨어, 디바이스와 관련된 취약점에 관한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인하고, 취약점 정보에 대한 내부 적용 여부를 검토하여 적용하여야 한다.(보안 모니터링 및 통합관제)
	3.2.3 상태 모니터링	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정상적인 동작 여부를 실시간으로 알 수 있어야 한다.	· 스마트시티 플랫폼 소프트웨어의 이상 행위 발생 시 즉시 확인 및 대응이 가능하도록 알람기능이 설정되어 운영해야 한다.	· 스마트시티 플랫폼 소프트웨어의 비정상적인 상태 발견 즉시 확인 가능하도록 알람기능을 설정하여 운영한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스 등 각 장비 별 성능, 용량 등을 지속적으로 모니터링하여야 한다.(보안 모니터링 및 통합관제)
3.3 연속성 관리	3.3.1 변경 관리	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정, 세부 현황의 변경이 기록되고 검토되어야 한다.	· 스마트시티 관련 모든 정책, 설정값 등 모든 변경사항은 기록/관리되어야 한다.	· 스마트시티 플랫폼 소프트웨어는 정책, 설정값, 현황 등의 모든 변경사항을 기록한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정값 등 보든 변경사항이 기록되고 관리되어야 한다.
	3.3.2 보안 패치 및 업데이트	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용되어야 할 보안 패치를 지속적으로 확인하여 적용에 따른 영향도를 고려하여 지체없이 적용하여야 한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용해야 할 보안 패치 및 업데이트를 모니터링해야 한다.	· 스마트시티 플랫폼 소프트웨어에 적용되어야 할 패치 및 업데이트를 지속적으로 모니터링 한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용되어야 할 보안 패치 및 업데이트 정보를 지속적으로 확인 및 모니터링 하여야 한다.

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
3.3 연속성 관리	3.3.3 백업 및 복구	· 스마트시티 서비스의 가용성 확보를 위하여 데이터, 설정값 등의 백업과 백업본을 이용한 복구계획이 수립 및 운영되어야 한다.	· 스마트시티 서비스의 모든 데이터 및 설정값에 대한 백업 계획에 따라 백업을 수행해야 한다.	· 스마트시티 플랫폼 소프트웨어의 가용성, 데이터 무결성 등을 확보하기 위하여 모든 데이터 및 설값에 대한 백업 계획에 따라 백업을 수행한다.	· 스마트시티 서비스의 가용성, 데이터 무결성 등을 확보하기 위해 모든 데이터 및 설정값에 대한 백업 및 복구 계획을 수립하고 계획에 따라 수행하여야 한다.
3.4 데이터 흐름 관리	3.4.1 데이터 활용 시 보안	· 스마트시티 서비스 내 데이터를 활용 시 제공되는 데이터의 범위와 사용자를 식별하여 최소한의 데이터만 활용되도록 통제하여야 한다.	· 외부 기관에 제공하는 정보는 해당 기관 및 기관에 포함된 인력에 의해 무단 활용되지 않도록 통제하고 있으며, 스마트시티에서 사용되는 도시 데이터는 공개 범위를 식별하여 공개해야 한다.	· 외부 기관에 제공되는 정보는 해당 기관 및 해당 기관에 포함된 인력에 의한 무단 활용되지 않도록 통제하며, 스마트시티에서 사용되는 도시 데이터는 공개 범위를 식별하여 공개한다.	· 외부 기관에 제공되는 정보는 해당 기관 및 해당 기관에 포함된 인력에 의한 무단 활용이 되지 않도록 통제하고, 정보의 정확성과 신뢰성을 위해 모든 시스템은 표준시각으로 동기화하고, 주기적으로 시각 동기화가 정상적으로 이루어지는 점검하여야 한다.

4 스마트시티 디바이스

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
4.1 인증 관리	4.1.1 인증 및 인가	· 스마트시티 서비스에 접근하려는 경우 인증 및 인가 절차에 따라 부여된 권한에 한하여 접근하도록 통제하여야 한다.	· 접근통제 정책에 따라 스마트시티 서비스의 모든 인프라, 플랫폼 소프트웨어, 디바이스, 네트워크 등에 접근 시 인증을 거쳐 접근해야 한다.	· 스마트시티 서비스 접근통제 정책에 따라 모든 인프라에 대한 접근 시 인증을 거쳐 접근한다.	· 스마트시티 서비스의 모든 시스템에 접근 시 사용자 인증, 로그인 횟수 제한, 불법 로그인 경고 등 안전한 사용자 인증 절차에 의해 접근하고, 1인 1계정 부여 및 목적에 따른 권한을 차등부여하여야 한다.(사용자/서비스 인증)
	4.1.2 인증정보의 안전한 사용	· 인증 및 인가에 사용되는 인증정보는 안전하게 관리되어야 한다.	· 인증 및 인가에 사용되는 인증정보를 안전하게 관리하는 절차가 수립/이행되어야 한다.	· 인증에 사용하는 인증정보(ID/PW, 인증키, 토큰 등)를 안전하게 관리하는 절차를 운영한다.	· 인증정보(ID/PW, 인증키, 토큰 등)의 안전한 관리를 위해 관리절차를 수립하고 적용하여야 한다.(암호화)
4.2 모니터링	4.2.1 감사 모니터링	· 스마트시티 서비스 내에서 수행되는 사용자 및 관리자의 행위 기록을 기반으로 모니터링이 수행되어야 한다	· 스마트시티 서비스 내 시스템에 접근하는 사용자 및 관리자의 이상행위를 모니터링해야 한다.	· 스마트시티 디바이스에 접근하는 사용자 및 관리자는 정상적인 행위가 아닌 경우를 모니터링 한다.	· 스마트시티 서비스 내 인프라, 플랫폼 소프트웨어, 디바이스에 접근하는 사용자 및 관리자의 행위를 모니터링 하여 이상행위 여부를 모니터링하여야 한다.

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
4.2 모니터링	4.2.2 위협 모니터링	· 스마트시티 서비스의 위협을 고려하여 취약점 및 악성코드가 지속적으로 감시되고 반영되어야 한다.	· 스마트시티 서비스 내 관련 취약점에 대한 정보를 외부 전문 기관 등을 이용하여 지속적으로 확인하고 점검해야 한다.	· 스마트시티 디바이스 관련 취약점에 관한 정보를 외부 전문 기관 등을 이용하여 지속적으로 확인한다.	· 스마트시티 서비스 내 인프라, 플랫폼 소프트웨어, 디바이스와 관련된 취약점에 관한 정보를 외부 전문기관 등을 이용하여 지속적으로 확인하고, 취약점 정보에 대한 내부 적용 여부를 검토하여 적용하여야 한다.(보안 모니터링 및 통합관제)
	4.2.3 상태 모니터링	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정상적인 동작 여부를 실시간으로 알 수 있어야 한다.	· 스마트시티 인프라의 장비별 용량 한계점을 설정하고, 한계점 이상에 대비한 개선 계획이 수립/적용되어야 한다.	· 디바이스의 성능 및 용량의 한계점을 설정하고 한계점 이상에 대비한 개선 계획을 적용한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스 등 각 장비 별 성능, 용량 등을 지속적으로 모니터링하여야 한다.(보안 모니터링 및 통합관제)
4.3 연속성 관리	4.3.1 변경 관리	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정, 세부 현황의 변경이 기록되고 검토되어야 한다.	· 스마트시티 관련 모든 정책, 설정값 등 모든 변경사항은 기록/관리해야 한다.	· 스마트시티 디바이스는 정책, 설정값, 현황 등의 모든 변경사항을 기록한다.	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스는 정책, 설정값 등 보든 변경사항이 기록되고 관리되어야 한다.
	4.3.2 보안 패치 및 업데이트	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용되어야 할 보안 패치를 지속적으로 확인하여 적용에 따른 영향도를 고려하여 지체 없이 적용하여야 한	· 스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용해야 할 보안 패치 및 업데이트를 모니터링해야 한다.	· 스마트시티 디바이스에 적용되어야 할 패치 및 업데이트를 지속적으로 모니터링 한다.	스마트시티 인프라, 플랫폼 소프트웨어, 디바이스에 적용되어야 할 보안 패치 및 업데이트 정보를 지속적으로 확인 및 모니터링 하여야 한다.
	4.3.3 백업 및 복구	· 스마트시티 서비스의 가용성 확보를 위하여 데이터, 설정값 등의 백업과 백업본을 이용한 복구계획이 수립 및 운영되어야 한다.	· 스마트시티 서비스의 모든 데이터 및 설정값에 대한 백업 계획에 따라 백업을 수행해야 한다.	· 스마트시티 디바이스의 가용성, 데이터 무결성 등을 확보하기 위하여 모든 데이터 및 설값에 대한 백업 계획에 따라 백업을 수행한다.	· 스마트시티 서비스의 가용성, 데이터 무결성 등을 확보하기 위해 모든 데이터 및 설정값에 대한 백업 및 복구 계획을 수립하고 계획에 따라 수행하여야 한다.
4.4 디바이스 보안 관리	4.4.1 디바이스 자산 관리	· 스마트시티 도시 공간에 산재되어 있는 디바이스는 일반 자산과 별도로 세부 현황까지 관리되어야 하며 추가적인 물리적 보호통제를 적용하여야 한다.	· 스마트시티 디바이스는 공간적 위치(GIS)를 포함하여 자산으로 관리해야 한다.	· 스마트시티 디바이스는 공간적 위치(GIS)를 포함하여 자산 관리한다.	· 스마트시티 디바이스의 공간적 위치(GIS)는 자산으로 포함하여 관리하여야 한다.
	4.4.2 물리적 인터페이스 보호	· 스마트시티 디바이스의 물리적 인터페이스를 관리용도로 한정하여 접근이 허용되어야 한다.	· 디바이스 내 디버깅 용도의 인터페이스는 물리적으로 제거 후 사용해야 한다.	· 디바이스에서 디버깅 용도로 사용하는 인터페이스를 물리적으로 제거하고 사용한다.	· 디바이스에 디버깅 용도로 사용되는 인터페이스는 물리적으로 제거 또는 사용이 불가능하도록 조치후 사용하여야 한다.(물리적보안)
	4.4.3 디바이스 소프트웨어 보호	· 디바이스에 설치되는 소프트웨어는 안전하게 개발하고 역분석이 되지 않도록 통제하여야 한다.	· 디바이스 소프트웨어 개발 시 시큐어코딩을 적용하고 주기적으로 보안 취약점을 점검해야 한다.	· 디바이스 소프트웨어는 개발 시 시큐어코딩을 적용하며, 주기적으로 보안 취약점 존재여부를 점검하고 조치한다.	· 디바이스 소프트웨어의 개발 시 안전한 시큐어코딩 방법에 적용하여 개발하여야 하며, 디바이스 소프트웨어에 발생 가능한 보안 취약점의 존재 여부를 주기적으로 점검하고 보안 취약점 발견 시 즉치 조치를 취하여야 한다.(Secure Coding)

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
4.5 데이터 흐름 관리	4.5.1 데이터 수집 시 보안	· 스마트시티 서비스에서 수집하는 데이터는 서비스의 목적 내에서 수집되어야 한다.	· 수집하는 데이터는 서비스 목적에 따른 데이터 이외에는 수집하지 않아야 한다.	· 디바이스에서 수집하는 데이터는 서비스 목적에 따른 데이터 이외에는 수집하지 않는다.	· 디바이스에서 수집하는 데이터는 서비스 목적에 따라 수집되어야 하며, 목적 이외에 데이터는 수집하지 않아야 한다.

5 스마트시티 서비스

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
5.1 스마트시티 서비스 보안	5.1.1 서비스 권한 관리	· 스마트시티 서비스를 이용하는 외부기관은 외부기관의 서비스 접근 목적에 맞는 권한을 부여받고 사용하여야 한다.	· 스마트시티 서비스 내 외부기관의 권한은 업무 및 사용 목적과 용도에 맞는 필요 최소한의 권한으로 관리한다.	· 스마트시티 서비스를 이용하는 외부 기관이 부여받은 권한 외에 사용할 수 없도록 통제하는지 확인한다. · 스마트시티 서비스 제공 목적 이외에 서비스 기능 이용을 통제하는지 확인한다. · 스마트시티 서비스 중 CCTV 제어 기능은 외부 기관에 제공하지 않고 있는지 확인한다.	· 외부기관에 제공하는 스마스티시 서비스와 관련된 모든 권한의 적절성을 주기적으로 점검하고 권한을 우회할 수 있는 기능 또는 절차가 존재하는지 확인하여 조치한다.(사용자 권한관리)
	5.1.2 영상정보 보안 관리	· 스마트시티 서비스를 이용하는 외부기관에게 제공되는 영상정보는 안전하게 보호되어야 한다.	· 영상정보는 외부기관에 연계 / 중계의 경우를 제외하고 승인없이 제공되어서는 안되며, 무단 복제하지 않아야 하고 가용성 보장을 위한 이중화를 수행하여 안전하게 관리하고 기록하여야 한다.	· 사전에 목적지로 등록되지 않은 외부 기관에 영상정보가 전송되는지 확인한다. · 외부기관에 제공되는 영상정보의 무단 복제가 가능한지 확인한다. · 영상정보의 연계, 중계, 반출을 위한 장비가 이중화 되어 있는지 확인한다. · 영상정보의 연계, 중계, 반출 시 해당 기록을 모두 유지하는지 확인한다.	· 스마트시티에서 수집되는 영상정보는 시민의 얼굴을 포함하므로 개인영상정보에 해당한다. 따라서 개인영상정보를 서비스 연계에 따라 외부기관과 공유하는 경우에는 반드시 사전 계획되고 승인된 절차 및 방법에 따라야 한다. · 외부기관에 제공되는 영상정보는 사전에 필요한 영상이 무엇인지 식별하고 해당 영상만 전달되도록 한다. · 영상정보가 전달되는 경우 영상 파일을 전달하는 것이 아닌 영상을 스트리밍 방식으로 전달하여 조회만 가능하도록 통제한다. · 영상정보를 활용하는 스마트시티 서비스는 시민의 안전에 직결되므로 장비의 문제로 영상정보가 전달되지 않는 상황을 조성하지 않아야 하므로, 단일 경로로 전달되지 않고 복수 경로로 전달되도록 설계하고, 내부 영상정보의 저장 및 처리를 위

분야	항목	상세내용	보안요구사항		점검 방법	보안 대응 방안
5.1 스마트 시티 서비스 보안	5.1.2 영상 정보 보안 관리					한 정보시스템을 이중화한다. (권고) · 영상정보의 연계, 중계가 아닌 요청에 의한 반출인 경우는 반드시 반출 요청 및 반출 여부를 기록으로 유지한다.
5.2 데이터 흐름 관리	5.2.1 데이터 유효성 관리	· 스마트시티 서비스에 사용되는 데이터는 최신화되어야 하며 변조되지 않도록 관리하여야 한다. · 스마트시티 서비스에 사용되는 데이터는 최신화되어야 하며 변조되지 않도록 관리하여야 한다. · 스마트시티 서비스에 사용되는 데이터는 최신화되어야 하며 변조되지 않도록 관리하여야 한다.	기획 단계	· 스마트시티 서비스에 사용되는 데이터 유효성 확보 방안을 수립한다.	· 제공 받은 도시 데이터는 주기적으로 확인하여 최신의 상태로 유지한다. · 스마트시티 서비스 내에서 송수신되는 모든 데이터는 변조되지 않았는지 확인한다. · API를 이용한 연계 시 메시지 무결성을 검증하는 기능을 적용한다. · 제공 받은 도시 데이터는 주기적으로 확인하여 최신의 상태로 유지한다. · 스마트시티 서비스 내에서 송수신되는 모든 데이터는 변조되지 않았는지 확인한다. · API를 이용한 연계 시 메시지 무결성을 검증하는 기능을 적용한다. · 제공 받은 도시 데이터는 주기적으로 확인하여 최신의 상태로 유지한다. · 스마트시티 서비스 내에서 송수신되는 모든 데이터는 변조되지 않았는지 확인한다. · API를 이용한 연계 시 메시지 무결성을 검증하는 기능을 적용한다.	· 제공 받은 도시 데이터는 주기적으로 확인하여 데이터를 최신 상태로 유지하고, 송수신 되는 모든 데이터가 위/변조 되지 않았는지 점검 및 확인하여야 한다. (데이터 무결성) · 제공 받은 도시 데이터는 주기적으로 확인하여 데이터를 최신 상태로 유지하고, 송수신 되는 모든 데이터가 위/변조 되지 않았는지 점검 및 확인하여야 한다. (데이터 무결성) · 제공 받은 도시 데이터는 주기적으로 확인하여 데이터를 최신 상태로 유지하고, 송수신 되는 모든 데이터가 위/변조 되지 않았는지 점검 및 확인하여야 한다. (데이터 무결성)
			운영 단계	· 제공 받은 도시 데이터는 주기적으로 검토하여 최신의 상태로 유지한다		
			발전 단계	· 제공 받은 도시 데이터의 최신성 및 무결성 확보방안을 수립하고 이행한다.		

6 연계구간

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
6.1 연계 구간 보안	6.1.1 접근 제어	· 플랫폼 및 서비스의 연계는 필요한 범위를 식별하고 범위에 따른 접근제어 방식에 따라 연계되어야 한다.	· 연계가 필요한 구간을 명확하게 식별하고 범위를 정의해야 한다.	· 연계가 필요한 구간을 명확하게 식별하여 범위를 정의한다.	· 플랫폼 및 서비스의 연계가 필요한 구간을 명확하게 실별하고 연계 범위를 정의하고, 접근통제 영역, 접근통제 범위, 접근통제 규칙 등이 포함된 접근제어 정책을 수립/운영하여야 한다.(망분리/망연계)

분야	항목	상세내용	보안요구사항	점검 방법	보안 대응 방안
6.1 연계 구간 보안	6.1.1 접근 제어	· 플랫폼 및 서비스의 연계는 필요한 범위를 식별하고 범위에 따른 접근제어 방식에 따라 연계되어야 한다.	· 연계가 필요한 구간을 명확하게 식별하고 범위를 정의해야 한다.	· 연계가 필요한 구간을 명확하게 식별하여 범위를 정의한다.	· 플랫폼 및 서비스의 연계가 필요한 구간을 명확하게 실별하고 연계 범위를 정의하고, 접근통제 영역, 접근통제 범위, 접근통제 규칙 등이 포함된 접근제어 정책을 수립/운영하여야 한다.(망분리/망연계)
	6.1.2 인증 및 인가	· 플랫폼 및 서비스의 연계 시에도 연계 방식에 따른 안전한 인증 및 인가 절차를 적용하여야 한다.	· API 연계 시 안전한 API 인증방식을 적용해야 한다. 또는 망연계 솔루션 사용 시 등록된 사용자만 이용가능하도록 통제하여야 한다.	· API 연계에 따른 안전한 API 인증방식을 적용한다. · 망연계 솔루션을 사용하는 경우 사전에 등록된 사용자만 이용가능하도록 통제한다.	· 플랫폼 및 서비스의 연계 중 API 연계에 따른 안전한 API 인증방식(토큰사용, 암호화 및 서명 사용, API게이트웨이 사용 등)을 적용하여야 한다.(망분리/망연계)
	6.1.3 암호화	· 플랫폼 및 서비스의 연계 시에도 데이터의 송수신 시에는 관련 법령에 따라 암호화 등 안전한 방식으로 송수신하여야 한다.	· 데이터 연계 시 관련 법률에 따라 송수신, 저장 시 암호화를 위한 암호화 정책을 수립/이행해야 한다.	· 데이터를 연계하는 경우 관련 법률에 따라 송수신 및 저장 시 암호화를 위한 암호화 정책을 수립하여 운영한다. · 데이터 송수신 시 암호화 통신을 적용한다. · 데이터 수신 후 저장 시에는 안전한 암호 알고리즘으로 암호화하여 저장한다.– 암호키 관리 정책을 수립하여 암호키를 안전하게 관리한다.	· 플랫폼 및 서비스 연계 시 데이터의 송수신 및 저장 시 관련 법률에 따라 암호화를 위한 암호화 정책(암호화 대상, 암호 알고리즘, 암호화 방식 등)을 수립/이행하여야 한다.(암호화)
	6.1.4 안전한 API 개발	· 데이터 연계에 필요한 API를 개발하는 경우 개발 보안 절차에 따라 안전하게 개발된 API를 사용하여야 한다.	· API 개발 시 소프트웨어 개발 보안 절차에 따라 개발하고, 개발 후 API 개발 후 구현 단계로 이관 전 취약점 점검실시 및 조치 후 이관해야 한다.	· API 개발 시 소프트웨어 개발 보안 절차에 따라 개발하고, API 개발 후 구현 단계로 이관 전 취약점 점검을 실시하고 조치 후 이관한다.	· 데이터 연계에 필요하거나 API를 개발하는 경우 소프트웨어 개발 보안절차에 따라 개발을 수행하고 구현 단계로 이관 전 취약점 점검을 실시하여 발견된 취약점을 조치 및 확인 후 이관을 수행하여야 한다.(Secure Coding)
	6.1.5 무결성 검증	· 연계되는 모든 데이터는 중간에 변조되지 않고 전달되도록 무결성이 확보되어야 한다.	· API를 이용한 데이터 연계 시 송수신되는 메시지의 무결성을 검증해야 한다.	· API를 이용한 데이터 연계 시 송수신되는 메시지의 무결성을 검증한다.	· API를 이용한 데이터 연계 시 송수신되는 메시지의 무결성을 검증(메시지에 대한 Signature를 생성하여 메시지와 같이 전송 후 검증 등)을 하여야 한다.(데이터 무결성)
	6.1.6 연계 현황 모니터링	· 데이터 연계 현황을 모니터링 할 수 있는 계획에 따라 모니터링하고 데이터 흐름의 사후 추적성을 확보하여야 한다.	· 데이터 연계에 따른 모니터링 계획의 수립/이행해야 한다.	· 데이터 연계에 따라 모니터링 계획을 수립하여 이행한다. · 망 간 데이터 흐름의 기록을 로그 형식으로 기록한다. · 망 간 데이터 흐름의 기록을 주기적으로 검토하여 이상징후를 확인한다.	· 각 데이터 연계에 따른 데이터 연계 현황을 모니터링하도록 모니터링 계획을 수립/이행하고, 망간 데이터의 흐름은 로그 형식으로 기록하여 주기적으로 검토하여야 한다.(보안 모니터링 및 통합관제)