IoT 서비스 인프라를 위한 보안 플랫폼 기술

제로 트러스트 아키텍처를 위한 IoT 동적 경계망 기술

2022.04.20

소프트플로우 소범석 팀장

SOFTFLOW

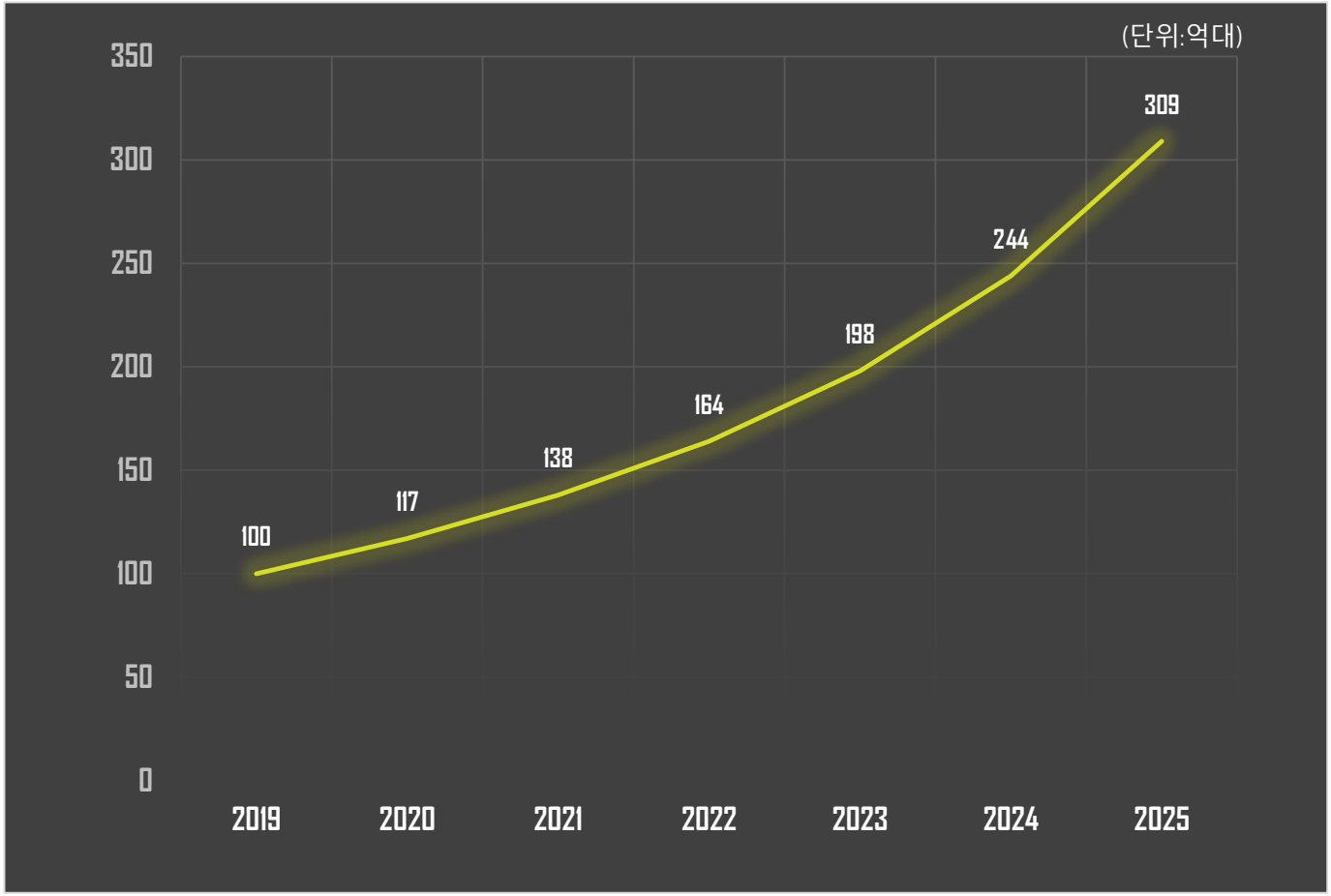
IoT 서비스의 확장

- **(IoT+Network+AI) + 산업시장 = 새로운 융합산업 및 서비스 창출**
  - Ex> 스마트홈, 스마트팩토리, 스마트시티, 자율주행차, 스마트의료, 스마트국방 등

IoT 서비스 인프라

IoT 산업의 발전

- **IoT 서비스는 다양한 분야에서 폭발적으로 성장 중**
  - 이에 따른 IoT 기기 대상 사이버 공격 시도 또한 증가할 것으로 전망



IoT 산업의 핵심 기술

• IoT 기술의 발전과 핵심기술

	연결형IoT	지능형IoT	자율형IoT	
IoT 플랫폼	데이터 관제/유통	온디바이스/엣지	디지털지능트윈	지능/자율
	관리/제어, 커먼즈, 공유, 마켓	엣지, 포그, 실시간, AI	가상화, 시뮬레이션, 예지보전	학습, 추론, 협업, 중재, 조정
IoT 디바이스	센싱/엑츄에이터	부품	초소형	지능/자율
	스마트센서, 보정, 고신뢰	안테나, 베터리, RFID, AP	수mm이하, 저전력, 오케스트레이션	상황인지, 강화학습, 분산협업
IoT 서비스	데이터 모델링	도메인 특화		매쉬업
	데이터 전처리, 데이터 생성, 일반화	홈, 건강, 안전, 제조, 농축수산, 에너지 등		서비스 조합/융합, 크로스 도메인
IoT 네트워킹	저전력/근거리	저전력/광역	고신뢰/저지연	지능/자율
	Near Range, IEEE802.15.4	Long Range, LPWAN, Massive	URLLC, mMTC, TSN, High reliability	AI Driven, 제로터치 Predictive

• IoT 핵심기술 분류

분류	요소기술	기술의 범위
IoT플랫폼	데이터/관제 IoT 플랫폼 기술, 온디바이스/엣지 IoT 플랫폼 기술, 공유·유통 IoT 플랫폼 기술, 디지털 트윈 IoT 플랫폼 기술, 지능/자율 IoT 플랫폼 기술	사물/공간/사람을 유기적으로 연결하고 상황을 분석/예측/판단해 지능화된 서비스를 제공하는 공통 플랫폼 기술
IoT디바이스	IoT 센싱 및 액츄에이팅 기술, IoT 부품 및 반도체 기술, 초소형 IoT 디바이스 기술, 지능/자율형 IoT 디바이스 기술	IoT 환경을 구성하는 사물로서 센싱 및 액츄에이팅 기술 수행
IoT서비스	도메인 데이터 모델링 기술, 서비스 도메인 특화 기술, 매시업 IoT 서비스 기술	IoT 기반 개인/공공/산업별 다양한 서비스 제공을 위한 기술
IoT네트워킹	저전력/근거리 IoT 네트워크 기술, 저전력/광역 IoT 네트워크 기술, 고신뢰/저지연 IoT 네트워크 기술, 지능형/자율형 IoT 네트워크 기술	IoT 사물 간, 사물-플랫폼 간 연결을 위한 유무선 통신 기술

* IITP "ICT R&D 기술로드맵 2025" 참고

IoT 산업 성장전망 - 분야별

- **대표적인 IoT 활용 분야**
  - "정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령" 제36조의2(별표1의3)

분야	정보통신망 연결기기 등
가전 분야	스마트 홈네트워크에 연결되는 멀티미디어 제품, 주방가전 제품 또는 생활가전 제품 등의 가전제품 또는 그 제품에 사용되는 기기・설비・장비
성장률 3위 교통 분야	다음 각 목의 제품 등에 사용되는 기기・설비・장비 가.「국가통합교통체계효율화법」 제2조제16호에 따른 지능형교통체계 나.「드론 활용의 촉진 및 기반조성에 관한 법률」 제2조제1호에 따른 드론 다.「자동차관리법」 제2조제1호에 따른 자동차 라.「선박법」 제1조의2제1항에 따른 선박
금융 분야	「전자금융거래법」 제2조제8호에 따른 전자적 장치
스마트도시 분야	「스마트도시 조성 및 산업진흥 등에 관한 법률」 제2조제2호에 따른 스마트도시서비스에 사용되는 기기・설비・장비
의료 분야	「의료기기법」 제2조제1항에 따른 의료기기 중 통신기능을 보유한 기기・설비・장비
성장률 2위 제조·생산 분야	제품의 제조・생산 또는 용역을 관리하기 위하여 제어・점검・측정・탐지 등의 용도로 사용되는 기기・설비・장비
성장률 1위 주택 분야	「건축법」 제2조제1항제4호에 따른 건축설비 중 지능형 홈네트워크에 연결되는 기기・설비・장비
통신 분야	「전파법」 제2조제16호에 따른 방송통신기자재 중 무선 또는 유선으로 통신이 가능한 방송통신기자재

• 국내 사물인터넷 시장 규모 및 분야별 시장 규모

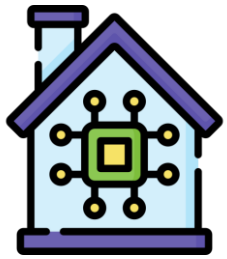
헬스케어/의료/복지		에너지
• 지정인 활동상태 관리·분석 • 보호자 모니터링·알림 • 심리 안정 디스플레이 콘텐츠		• 시스템 소비전력 모니터링·절감 • 배터리 현황 모니터링 • 에너지 데이터 시각
제조 (시장규모 2위)		스마트홈
• 반복 업무 자동화 • 산업 환경 실시간 모니터링 • 장비 가동 효율 증대	325,455 백만원	• 원격 홈 관리 • 홈 보안 향상 • 다세대 주거지 공용 공간 시스템화
금융		교육
• 결제 간소화 • 생체 인증 보안		• 자동 출결 시스템 • 전자 도서관 • 온라인 수업
국방		농림/축산/수산
• 무인이동체, 네트워크 등 무인체계 • 감시·정찰 기술 고도화		• 산업 환경 데이터 수집 • 원격 모니터링/관리 • 빅데이터 활용한 생산 효율 증대
자동차/교통/항공/우주/조선 (시장규모 3위)		관광/스포츠
• AI 도입 영상 분석 시스템 • 주차장 자동 통합 관리 • 실시간 교통상황 중계	325,455 백만원	• 맞춤형 관광 상품 패키지 추천 • 사용자 위치 기반 여행 경로 추천 • 맞춤형 운동 추천과 활동 데이터 구축
소매/물류		건설·시설물 관리/안전/환경 (시장규모 1위)
• 물류 창고 관리 시스템 • 운송·장비가동 효율 증대 • 무인택배함 운용		• 건물, 네트워크 보안 • 건물 상태 원격 모니터링 • 건물 에너지 관리 효율 증대

1,092,797 백만원

- 테크월드 "IoT 서비스 산업별 특화 기술과 적용 사례" 참고
- 과학기술정보통신부(2020) – 국내 사물인터넷 시장 규모 및 서비스 활용 분야별 시장 규모

IoT 서비스 공격 사례

- **주요 IoT 서비스 분야별 사이버 공격 사례**



Smart Home

- **아파트 월패드 해킹** : 사생활 침해 및 도어락 개방 / 보일러 가동 등 기기 임의 조작
  - 2021년 전국 700여 단지가 해킹 당한 대규모 피해 발생

Smart Factory

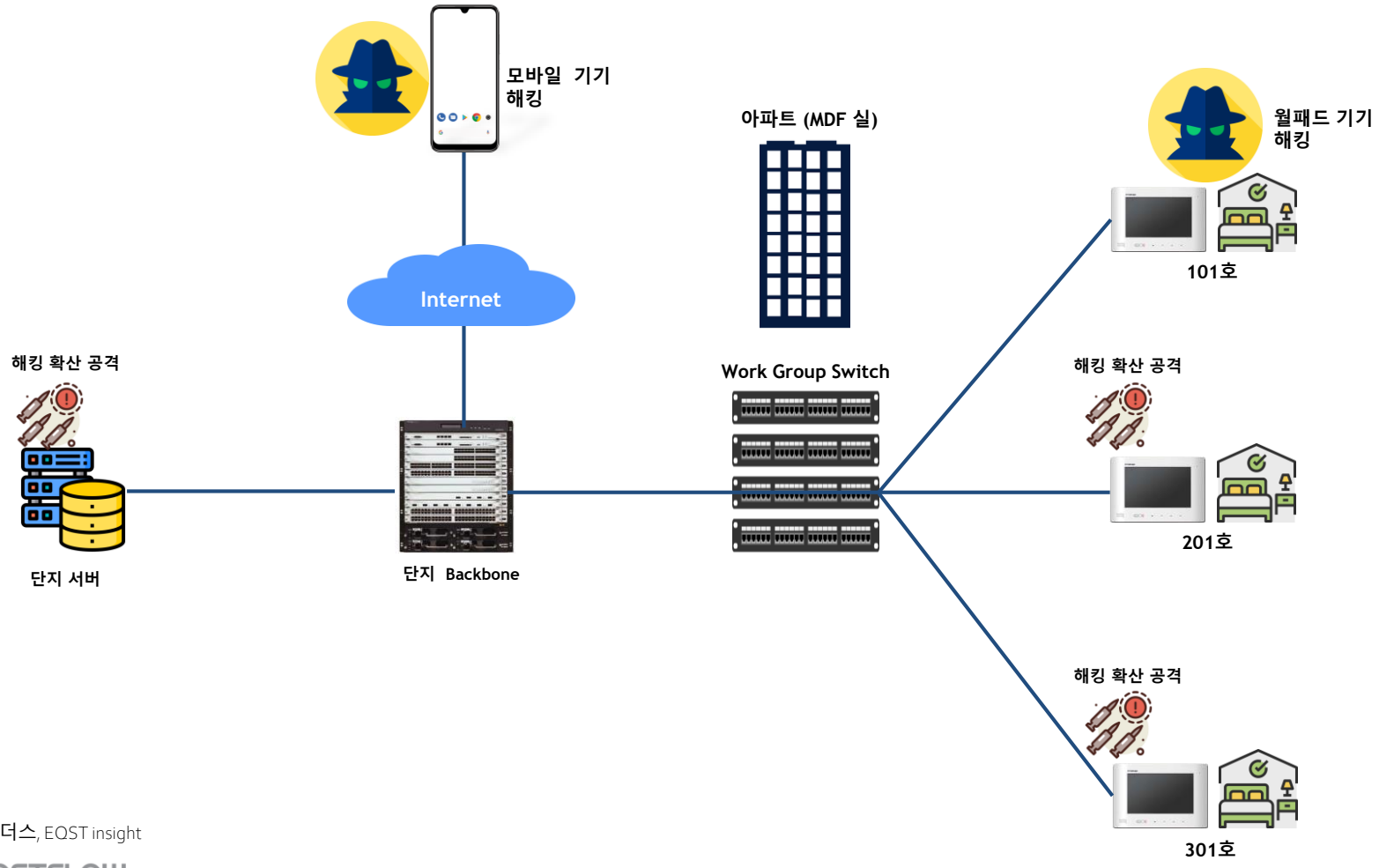
- **산업 제어 시스템 공격** : 산업 시설 가동 중단 / 중요 데이터 유출
  - 한국수력원자력 / 한국철도공사 등 주요 기반 시설에 대한 공격 발생

Smart Car

- **스마트카 해킹** : 자동차 주행 기능 임의 조작에 따른 인명 피해 발생 가능
  - 실제 해킹 사례는 없으나 보안 전문가들의 해킹 시연으로 증명

IoT 서비스의 해킹 사고 사례 분석

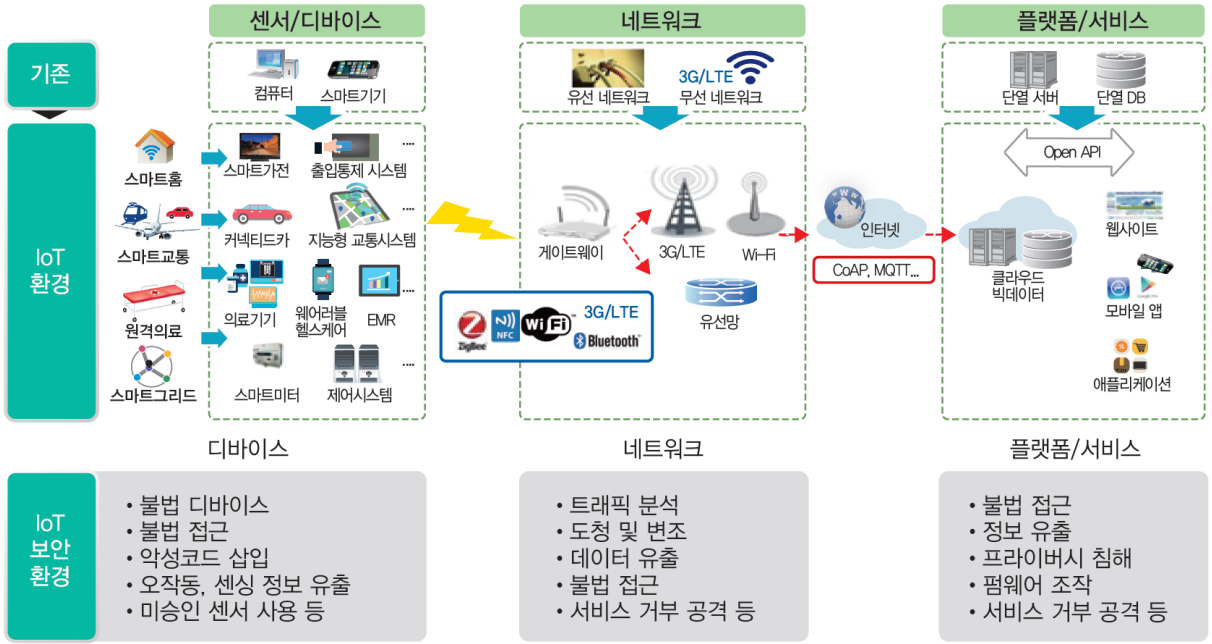
- **스마트 홈 해킹 사례로 보는 IoT 기기 보호의 중요성**
  - IoT 기기 한대의 해킹을 통하여 전체 서비스로 확산 공격이 이루어 지는 사례 발생
    - 중간자 공격, 관리자PC 악성코드 감염, 원격제어 프로그램, 공급망(제조사)공격을 통한 접근



- SK쉴더스, EQST insight

IoT 서비스의 사이버 공격 추세

- **특징 1 : IoT 환경에서의 사이버 공격 목표 변화**
  - 서비스 운영 시스템 침해 방식에서 해킹이 더 용이한 사용자 기기를 목표로 한 위협이 증가
- **특징 2 : 점차 다양한 IoT 기기 및 서비스의 등장으로 IoT 환경이 복잡해짐**
  - IoT 환경의 관리 복잡성의 증가는 보안 취약점 발생으로 이어짐
- **특징 3 : 일상을 파고드는 사이버 위협**
  - 기업 등 일부 한정된 범위 ➔ 우리의 안전까지 위협하는 형태로 진화, 다크 웹 판매



<IoT 환경에서의 보안위협, 한국인터넷진흥원>

IoT 산업의 핵심 기술? 보안

- **IoT 기술의 발전과 핵심기술? ➔ 보안**

	연결형IoT	지능형IoT	자율형IoT	
IoT 플랫폼	데이터 관제/유통	온디바이스/엣지	디지털지능트윈	지능/자율
	관리/제어, 커먼즈, 공유, 마켓	엣지, 포그, 실시간, AI	가상화, 시뮬레이션, 예지보전	학습, 추론, 협업, 중재, 조정
IoT 디바이스	센싱/엑츄에이터	부품	초소형	지능/자율
	스마트센서, 보정, 고신뢰	안테나, 베터리, RFID, AP	수mm이하, 저전력, 오케스트레이션	상황인지, 강화학습, 분산협업
IoT 서비스	데이터 모델링	도메인 특화		매쉬업
	데이터 전처리, 데이터 생성, 일반화	홈, 건강, 안전, 제조, 농축수산, 에너지 등		서비스 조합/융합, 크로스 도메인
IoT 네트워킹	저전력/근거리	저전력/광역	고신뢰/저지연	지능/자율
	Near Range, IEEE802.15.4	Long Range, LPWAN, Massive	URLLC, mMTC, TSN, High reliability	AI Driven, 제로터치 Predictive

IoT 산업과 서비스를 위한 IoT 보안 플랫폼 기술 필요

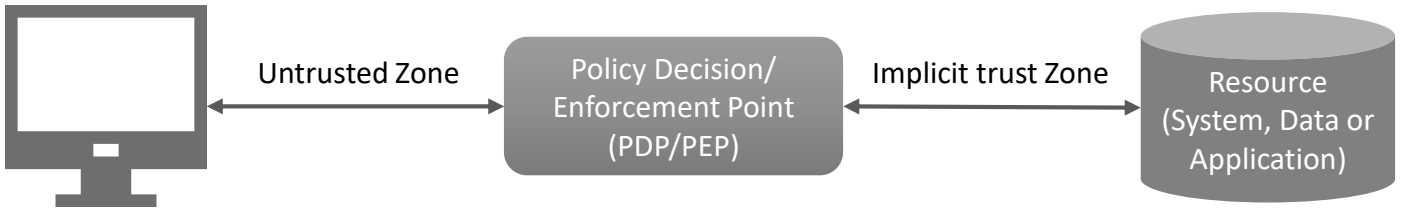
IoT 서비스 사이버 공격 대응 방향

- **방송정보통신망연결기기등 정보보호인증기준**
  - 인증기관: 한국인터넷진흥원(KISA) IoT 보안인증 서비스(IoT-SAP)
  - 시험대행기관: 한국기계전기전자시험연구원(KTC), 한국정보통신기술협회(TTA)
  - IoT 제품 및 연동 어플리케이션에 대한 일정 수준의 보안을 갖추었는지 인증

분 류	평가내용
식별 및 인증	안전한 인증정보 사용, 사용자 인증 및 권한 관리, 비인가 상호인증 제한, 반복된 인증시도 제한, 정보노출 방지, 안전한 세션 관리
데이터 보호	전송·저장 데이터 보호, 중요정보 저장 영역 보호강화, 개인정보 법적 준거성, 중요정보 완전삭제
암호	안전한 암호 알고리즘 사용, 안전한 암호키 생성, 안전한 암호키 관리, 안전한 난수 생성
소프트웨어 보안	시큐어코딩, 소스코드 난독화, 소프트웨어 보안기능 시험, 알려진 취약점 조치, 불필요한 기능 및 코드 제거, 안전한 소프트웨어 적용, 감사기록
업데이트 및 기술지원	모델명 및 제품정보 확인, 안전한 업데이트 수행, 업데이트 파일의 안전성 보장, 업데이트 실패 시 복구, 업데이트 기술 지원, 업데이트 정보 제공, 자동업데이트 기능 제공
운영체제 및 네트워크 보안	안전한 운영체제 적용, 불필요한 계정·서비스·포트 통제, 불필요한 네트워크 인터페이스 비활성화, 실행코드 및 설정파일 무결성 검증, 장애 시 시스템 복원, 서비스 거부 공격 대응, 운영체제 기능 보호, 접근권한 최소화, 비인가 소프트웨어 설치·실행차단, 원격접속·네트워크 트래픽 통제
하드웨어 보안	안전한 부팅 및 자체시험, 자체시험 실패 시 대응, 하드웨어 장애 대응, 무단 훼손 방어, 부채널·메모리 공격 대응, 비휘발성 메모리 보호, 외·내부 인터페이스 보호

IoT 서비스를 위한 제로 트러스트 아키텍처

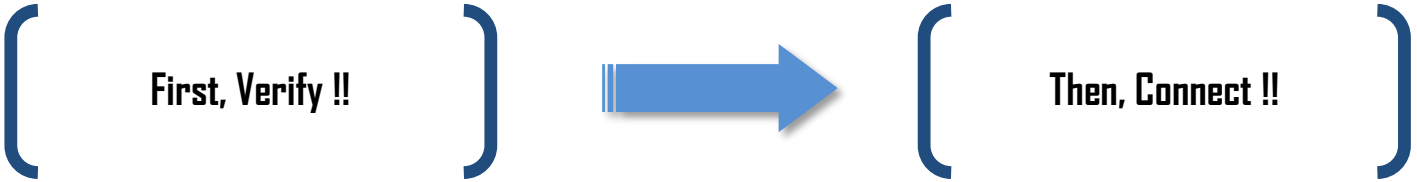
- **Zero Trust**
  - 네트워크가 침해 당한 경우라도, 정보 시스템이나 서비스에 있어서 각 리퀘스트를 정확하고 최소한의 권한이 되도록 엑세스를 판단할 때의 불확실성을 최소화하기 위해 설계된 개념과 아이디어의 집합체
- **Zero Trust Architect**
  - Zero Trust 원칙 기반으로, 데이터 침해를 방지하고, 내부 이동을 제한하도록 설계된 엔터프라이즈 사이버 보안 아키텍처
  - 보안 상태를 개선할 수 있는 워크플로우, 시스템 설계, 운영에 대한 가이드라인 모음
- **Zero Trust Architecture 접근법**
  - ZTA Using Enhanced Identity Governance
  - ZTA Using Micro-Segmentation
  - ZTA Using Network Infrastructure and Software Defined Perimeters



- NIST.SP.800-207 Zero Trust Architecture • PDP : Policy Decision Point • PEP : Policy Enforcement Point

SOFLO.IoT - Zero Trust Architecture의 동적 경계망 및 구성

- **Zero Trust Architecture 동적 경계망이란?**
  - Zero Trust 정책 기반으로 동작하는 별도 Controller의 인증 후 End Point간 연결
  - End Point 별로 Controller의 정책 List에 따라 동적 연결 프로비저닝 진행 구조

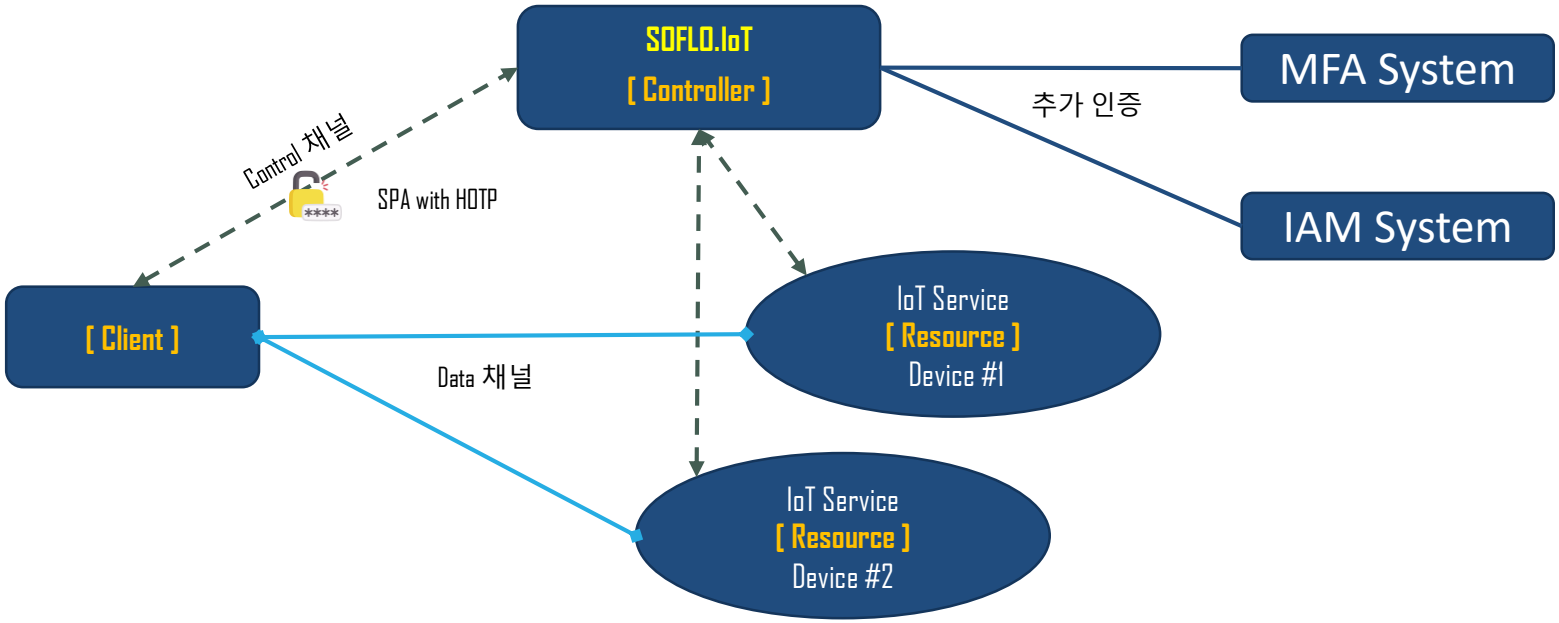


- **구성 1) Controller**
  - 별도의 Server에 구축되어 동작하는 어플라이언스 장비로 정책 List 정보를 관리
  - 연결 시도 및 처리 결과에 대한 모니터링 기능 제공

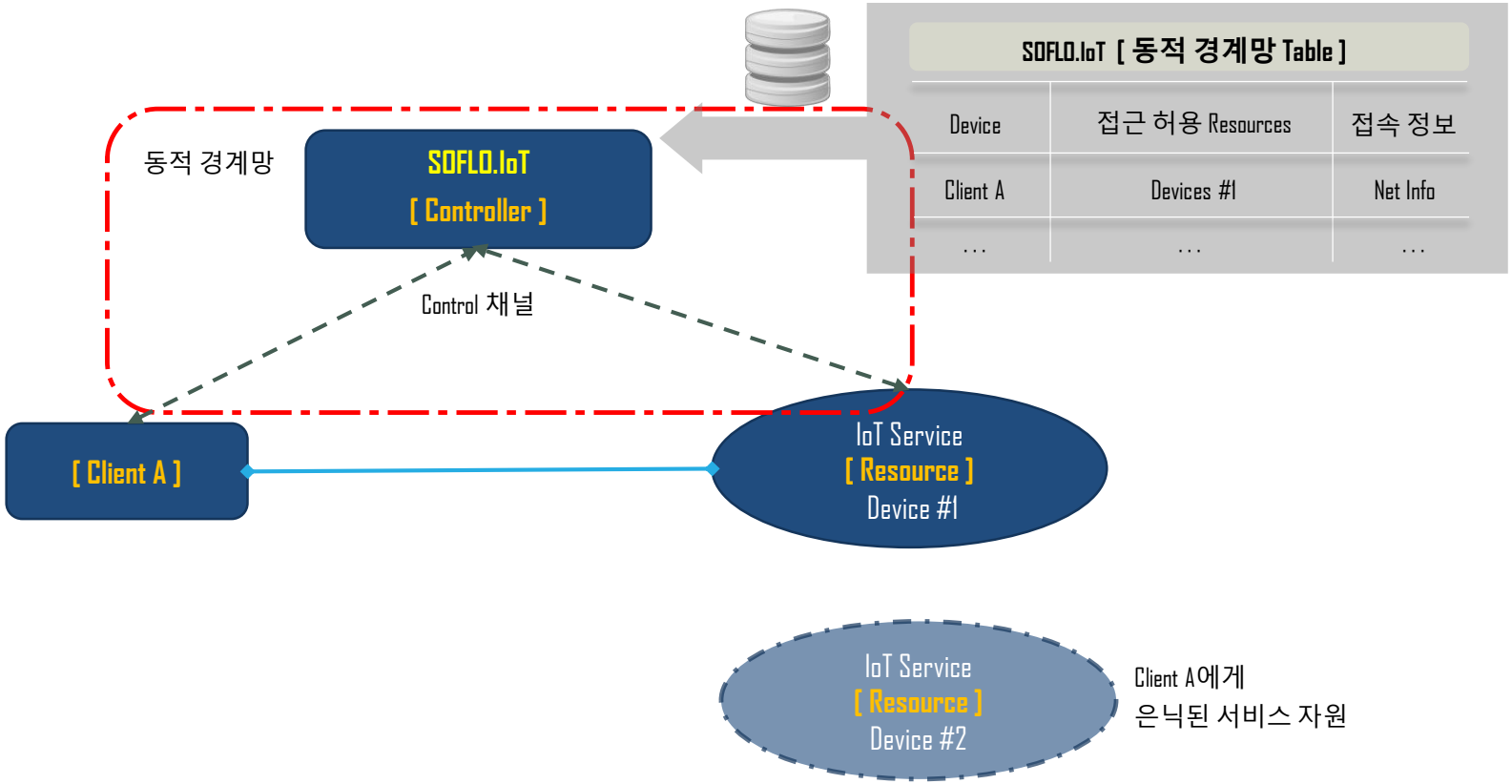
- **구성 2) End Points**
  - End Points는 Client Devices / IoT Devices / Edge Computing / Application Servers를 지칭
  - End Points에는 SOFLO.IoT Client SDK가 제공되어 Controller와 연결 동작

SOFLO.IoT - 기기 및 사용자 인증 기술

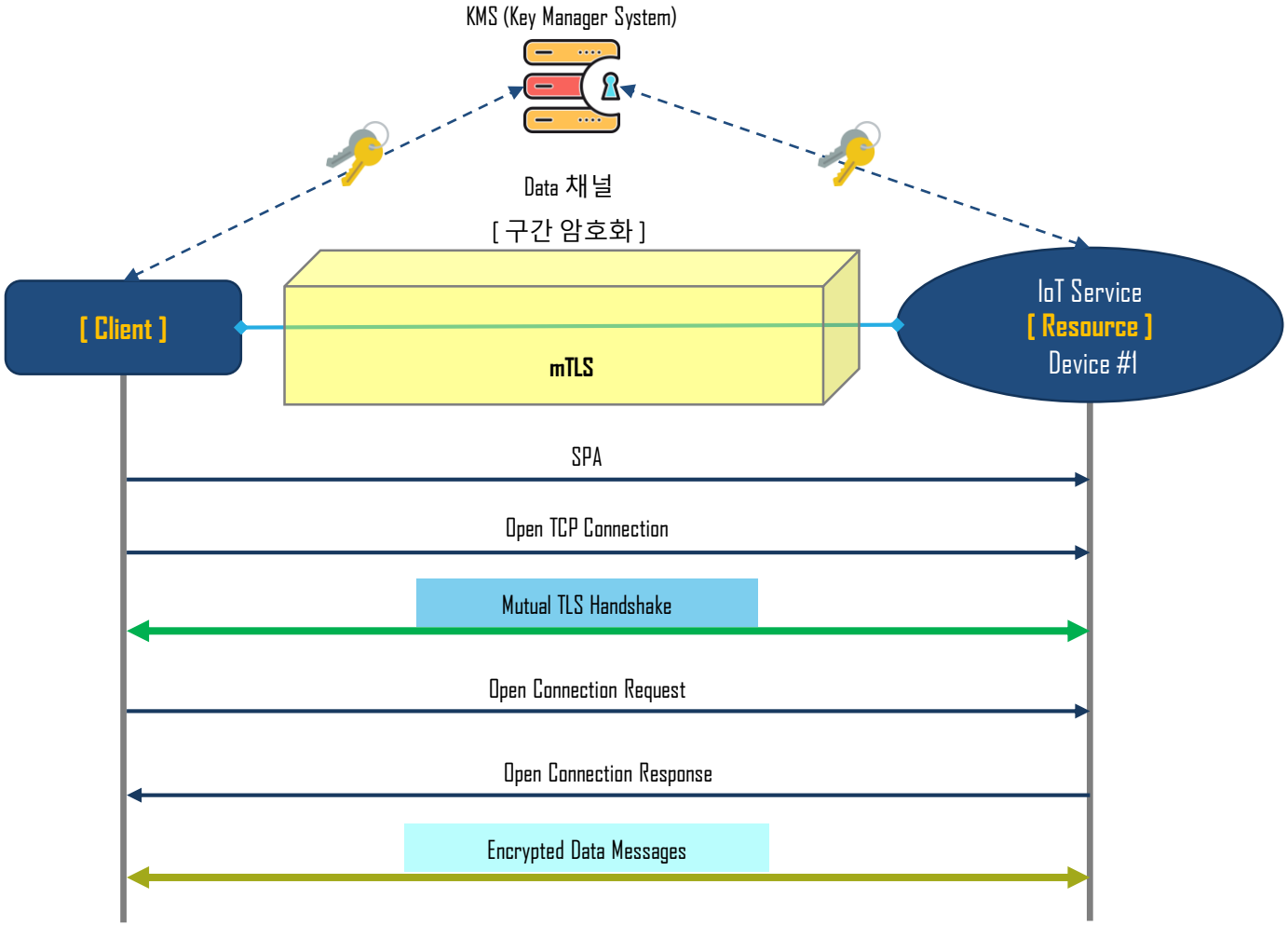
- **Controller는 End Point들과 신뢰 연결을 위한 SPA (Single Packet Authorization) 구현**
  - End Point는 고유의 비밀 시드 값으로 HOTP (HMAC One Time Password)를 생성 후 Controller에 전달
  - Controller는 받은 HOTP를 검증 후 신뢰된 End 기기인 경우 Control 채널 연결
- **Controller는 End Point간 Data 채널 연결 전 추가 인증 (MFA, IAM) 연동 수행**
  - MFA (Multi-factor Authentication) : OTP / Device Fingerprint 등 기기 인증
  - IAM (Identity and Access Management) : PKI / LDAP 등 사용자 인증



- **Controller는 End Points 신원을 기반으로 기기간 접속 정보 통제**
  - 예) Client A는 Resource #1에만 접근 허용되며, 타 Resources 접속 정보는 Blind 상태
- **Controller는 Control 채널 연결 프로비저닝을 위한 동적 경계망 Table 보유**



- End Point간 연결되는 Control 채널은 기본적으로 mTLS 연결을 통해 보호
- TLS Encryption Keys & Certificates의 경우 KMS을 통한 Lifecycle 관리 추천



- **"지능형 홈네트워크 설비 설치 및 기술 기준" 홈네트워크 보안 관련 개정**
  - 홈네트워크 장비에 대한 보안요구사항 (제14조의 2 제1항 관련) 신설

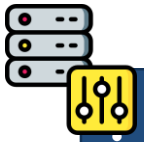
구 분	보안 요구사항
데이터 기밀성	이용자 식별정보, 인증정보, 개인정보 등에 대해 "**암호 알고리즘, 암호키 생성·관리 등 암호화 기술**"과 "**민감한 데이터의 접근제어 관리기술**" 적용으로 "**기밀성을 구현**" (※ 데이터의 처리(생성, 읽기, 쓰기, 변경, 삭제, 저장 등)가 아닌 단순 전송 등을 담당하는 워크그룹 스위치 등은 적용 제외)
데이터 무결성	이용자 식별정보, 인증정보, 개인정보 등에 대해 "**해쉬함수, 전자서명 등 기술**" 적용으로 **"위·변조 여부 확인 및 방지"** 조치 (※ 데이터의 처리(생성, 읽기, 쓰기, 변경, 삭제, 저장 등)가 아닌 단순 전송 등을 담당하는 워크그룹 스위치 등은 적용 제외)
인증	사용자 확인을 위하여 "**전자서명, 아이디/비밀번호, 일회용비밀번호(OTP) 등**"을 통해 **"신원확인 및 인증 기능을 구현"**
접근통제	**"자산·사용자 식별, IP관리, 단말인증 등 기술"**을 적용하여 사용자 유형 분류, 접근권한 부여·제한 기능 구현을 통해 **"인가된 사용자 이외에 비인가된 접근을 통제"**
전송데이터 보안	승인된 홈네트워크장비 간에 전송되는 데이터가 유출 또는 탈취되거나 흐름의 전환 등이 발생하지 않도록 **"전송데이터 보안 기능을 구현"**

※ 국토교통부 고시 제 2021-1533호 (고시일 : 21년 12월 31일 / 시행일 : 22년 7월 1일)

- **보안 요구 사항 충족을 위한 최적의 솔루션을 적용하여 목표 구현**

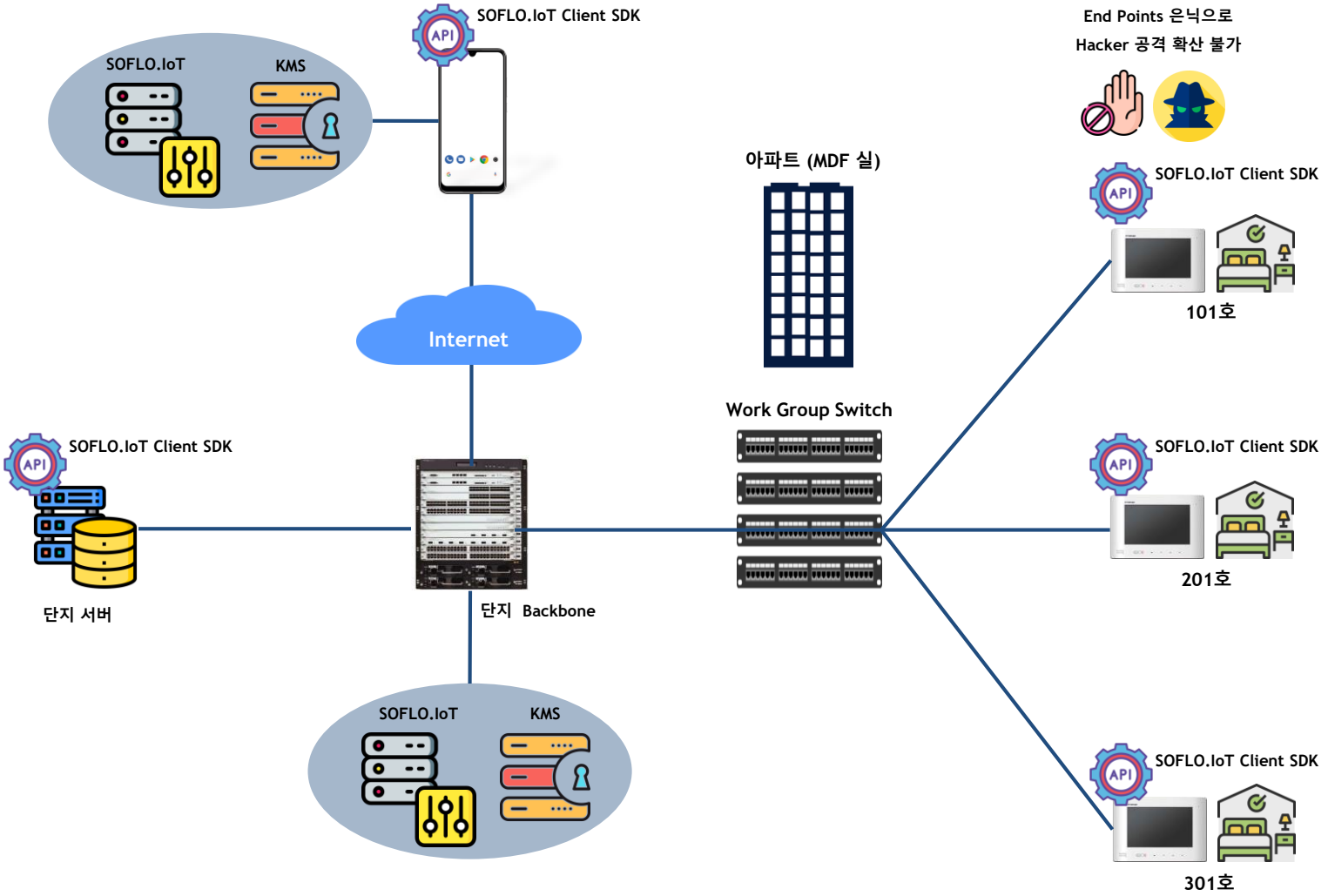
No	구 분	구현 목표	적용 솔루션
1	데이터 기밀성	암호키 Lifecycle 관리	Neo KeyManger
2	데이터 무결성	인증서 Lifecycle 관리	Neo KeyManager (with 사설 PKI)
3	인증	SPA 매커니즘 및 추가 인증 시스템 연동	SOFLO.IoT (with MFA & IAM)
4	접근통제	Zero Trust 기반 동적 경계망 구현	SOFLO.IoT (with 정책 Controller)
5	전송데이터 보안	데이터 전송 구간 암호화	SOFLO.IoT (with mTLS)
6	망분리	동적 가상 경계망 기반 논리적 망분리	SOFLO.IoT (with 정책 Controller)

- 솔루션 || Neo KeyManager
- 개발사 || 한컴인텔리전스



- 솔루션 || SOFLO.IoT
- 개발사 || 소프트플로우

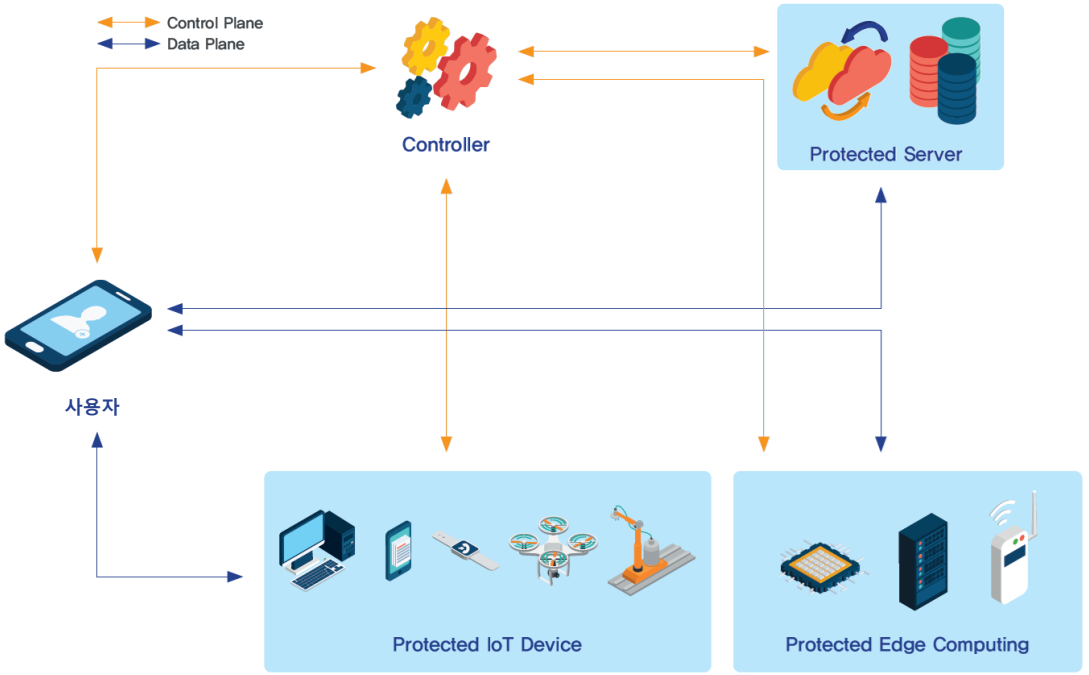
- **스마트홈 End Points 보호를 위한 동적 가상 경계망 적용**



결론

부스: N65

- **다양한 산업 분야 + IoT 서비스 = 새로운 산업 / 서비스**
- **"IoT 보안 기술은 향후 IoT 서비스 및 활성화를 위한 최대 걸림돌", 중소기업기술정보진흥원**
- **<u>IoT 보안 플랫폼 기술의 발전 및 확보 필요</u>**
  - 사용자(기기)별 동적-보안 경계망
  - 사용자(기기)의 네트워크 접속 정보 / 서비스 은닉
  - 공격 표면 최소화를 통한 보안 위험 감소
  - 해킹된 디바이스로부터 인프라 보호
  - ...



Thank you!

SOFTFLOW

소프트플로우㈜

연락처 : (Tel) 070-7724-2752 / (E-mail) info@softflow.io

주 소 : (13449) 경기도 성남시 수정구 대왕판교로 815, 8층 807호