

지능형 원격검침 인프라용 IoT 기기 보안 기술

Summary

Lab 소개

- 시스템보안연구그룹
 - 시스템보안연구그룹은 초연결 사회로의 진화 과정에서 심각한 보안 위협을 방지하고 안전성을 강화하기 위해 CPS 인프라 보안 분야의 연구개발을 수행

기술 소개

- 본 기술은 해킹에 의한 기기 위·변조를 방지하고 비인가 접근을 차단하여 안전한 지능형 AMI 서비스를 위한 스마트 원격검침용 ECC 인증서 기반의 인증 인프라 및 표준 규격 기반 안전한 Key 분배 기술
 - 펌웨어 위·변조 방지, 표준 기반 보안프로토콜
 - 경량 암호 및 안전저장 등의 경량 보안 커널 기술
 - 다양한 기기 사양에 맞춤형 보안을 적용하기 위한 보안 커널 재구성기술
 - 안전한 기기관리 및 운영을 위한 기기식별 및 기기인증
 - 접근제어 기술 등의 보안정책 기반 원격 기기 보안관리 기술

기술 경쟁력

- 세계최초 ECC 인증서 기반 상호 인증 및 Key 분배 기능 제공
- 표준 규격인 PANA(RFC5191), EAP(RFC3748), TLS(RFC5246) 준수 및 Cortex-M3 기반 개발
- 다양한 통신 환경(ZigBee, LTE, Wi-Fi 등)에서 기기 인증 및 Key 분배 적용 가능
- 우수한 처리 성능에 따른 경량 기기 보안 강화 가능
- KCMVP 인증 시험에 대응할 수 있는 다양한 암호 알고리즘 지원
- 국산암호(ARIA/SEED) 및 경량암호(HIGHT/LEA) 지원

진입 시장

- 목표시장 : 지능형 전력계량 정보제공 서비스
- 응용시장 : 스마트 홈/빌딩 IoT 보안 솔루션

시장 동향

- 시장규모
 - 세계 AMI 시장규모는 2011년 약 136억 달러로 추정되고 2020년에는 250억 달러로 2016년 대비 약 1.8배 증가 예상
 - 국내의 경우 2013년부터 2020년까지 8년간 저압 AMI를 2,194만대 보급할 계획
 - 2015년 전세계 스마트 홈 시장규모는 575억 달러 규모이며, 연평균 18.34%씩 성장하여 2020년에는 1,335억 달러에 이를 전망
 - 사물인터넷 기반 스마트팩토리 세계시장 규모는 2014년 1,796억 달러 규모였으며, 매년 6.8% 성장하여 2018년 2,461억 달러 규모로 성장전망




비즈니스 아이디어

- 지능형 전력계량(AMI)보안 서비스
 - AMI 운영 System 보안 (MDMS, AMI 운영시스템)
 - 지능형 계량기간 보안 (스마트 미터, 통신 설비)
- 스마트 홈/빌딩 IoT 보안 솔루션
 - 지능형 가전/사무 기기 IoT 보안
 - 지능형 IoT 플랫폼 보안

개요

기술 소개

- 해킹에 의한 기기 위·변조를 방지하고 비인가 접근을 차단하여 안전한 지능형 AMI 서비스를 위한 **[스마트 원격검침용 ECC 인증서 기반의 인증 인프라 및 표준 규격 기반 안전한 Key 분배 기술]**

<p>맞춤형 보안커널 재구성 기술</p> <ul style="list-style-type: none"> 커널 재구성을 위한 보안 기능별 모듈화 기술 재구성 가능한 보안 프로파일링 기술 	<p>기기 맞춤형 경량 보안커널 기술</p> <ul style="list-style-type: none"> 펌웨어 위변조 탐지 및 실행 방지 기술 키관리 및 암호 알고리즘 구현 기술 네트워크 보안프로토콜 기술 암호화 저장 기술 기기 고유 식별정보 검증 기술 자율형 기기간 상호 인증 기술 	<p>보안정책 기반 원격 기기 보안관리 기술</p> <ul style="list-style-type: none"> 상호인증기반 SW 경량보안업데이트 기술 객체 구성 지원 분산접근제어 기술 기기간 분산접근제어용 보안정책 관리 기술 사용자 권한관리, 접근제어, 프로세스관리 기술 
<p>펌웨어 위변조 방지, 보안프로토콜 맞춤형 보안커널 재구성</p>	<p>경량 암호 및 경량 보안커널 기기식별 및 기기인증</p>	

비즈니스 아이디어

지능형 전력계량(AMI)보안 서비스



AMI 운영 System 보안 (MDMS, AMI 운영시스템)



지능형 계량기기간 보안 (스마트 미터, 통신 설비)

스마트 홈/빌딩 IoT 보안 솔루션



지능형 가전/사무기기 IoT 보안



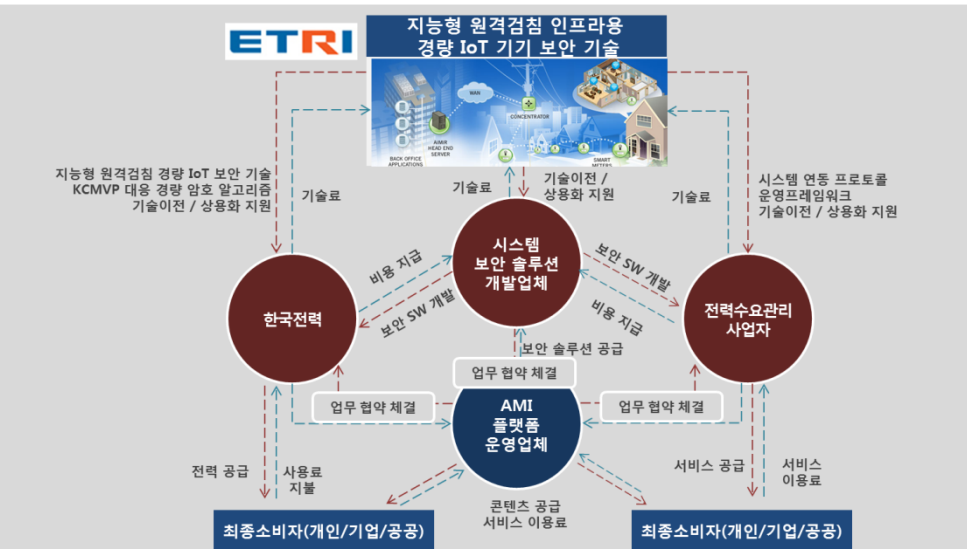
지능형 IoT 플랫폼 보안

진입 시장

- 1차 시장: 지능형 전력계량 보안 서비스
- 2차 시장: 스마트 홈/빌딩 IoT 보안 솔루션

 <p>지능형 전력계량 보안</p>	 <p>스마트 홈/빌딩 IoT 보안</p>	 <p>헬스케어/의료 보안</p>
<ul style="list-style-type: none"> 스마트미터 통신설비 지능형 전력정보관리시스템 AMI 운영시스템 	<ul style="list-style-type: none"> IoT 보안 게이트웨이 IoT 보안 서버 IoT 암호화 	<ul style="list-style-type: none"> 헬스케어/의료 디바이스 헬스케어/의료 플랫폼 의료정보처리 시스템 보안

예상 수익 구조



문의

ETRI 시스템보안연구그룹 김정녀 : 042-860-4884 / jnkim@etri.re.kr

지능형 원격검침 인프라용

IoT 기기 보안 기술

Lab 소개 05

기술소개 06

- 기술필요성
- 기술의 간략한 소개
- 기술의 특징
- 기존 기술대비 우위성
- 기술완성도(TRL)
- 기술이전 내용 및 지식재산권 현황

환경분석 12

- 기술동향
- 정책동향
- 기술사업화 진입시장
- 시장동향
- 시장참여자 현황

사업화전략 21

- SWOT 분석
- 시장진입 전략
- 기술도입 필요성(NABC)

비즈니스 모델 24

- 비즈니스 아이디어
- 예상 수익구조
- 기술사업화 시나리오
- 사업화 프로세스

Lab 소개

시스템보안연구그룹

- 시스템보안연구그룹은 초연결 사회로의 진화 과정에서 심각한 보안 위협을 방지하고 안전성을 강화하기 위해 CPS 인프라 보안 분야의 연구개발을 수행

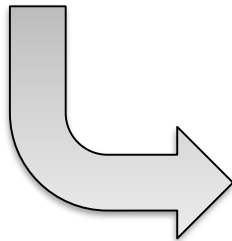
경량 IoT 기기
보호를 위한 핵심
보안 기술

사이버-물리시스템에서
물리적 단방향 보안
게이트웨이 기술

자율주행
자동차 보안 기술

선박/해양 안전을 위한
보안 기술

세부 연구 분야



- 펌웨어 위·변조 방지, 표준 기반 보안프로토콜
- 경량 암호 및 안전저장 등의 경량 보안 커널 기술
- 다양한 기기 사양에 맞춤형 보안을 적용하기 위한 보안 커널 재구성기술
- 안전한 기기관리 및 운영을 위한 기기식별 및 기기인증
- 접근제어 기술 등의 보안정책 기반 원격 기기 보안관리 기술

기술 필요성

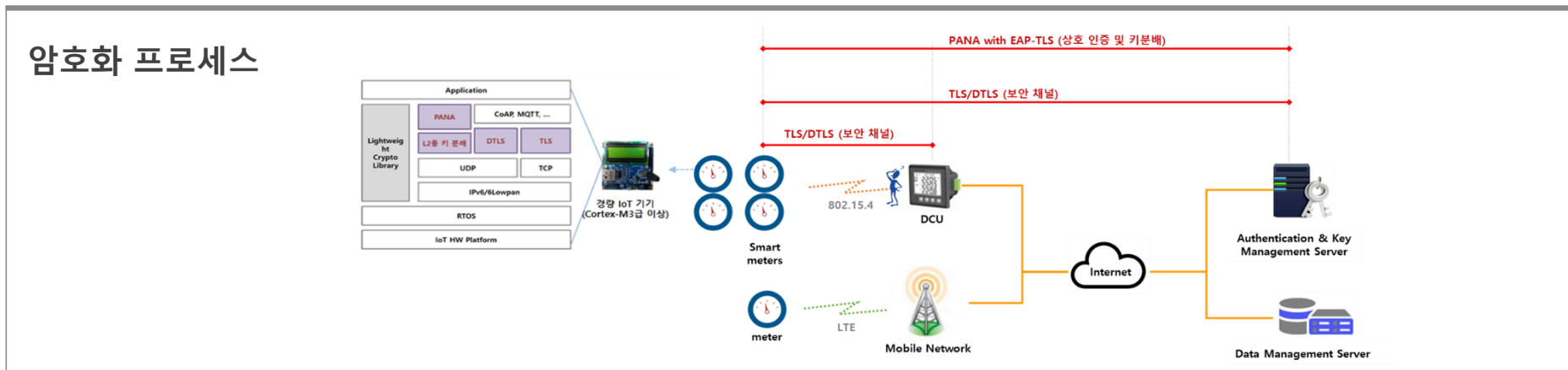
지능형 원격검침 인프라용 IoT 기기 산업 Needs

- 지능형 원격검침 인프라용 IoT에 경량화된 무결성 검증 및 기기인증서 기반의 보안 강화 인증 기술 필요
- 안전한 원격검침 IoT 서비스를 위해서는 해킹에 의한 IoT 기기의 위·변조 방지, 비인가 접근차단, 오작동 방지 등의 보안 기능을 내재하는 스마트 경량 IoT 기기용 운영체제 보안 기술 필요
- 지능형 원격검침 IoT 기기용 운영체제의 핵심 보안 기술 개발을 위해서는 기존보다 강화된 암호 알고리즘 필요



기술의 간략한 소개

- 해킹에 의한 기기 위·변조를 방지하고 비인가 접근을 차단하여 안전한 지능형 AMI 서비스를 위한 스마트 원격검침용 ECC 인증서 기반의 인증 인프라 및 **[표준 규격 기반 안전한 Key 분배 기술]**



주요기능 / 효과

경량 암호 및 해킹 대응 보안 커널 기술

→ 안전한 지능형 AMI 서비스 제공

맞춤형 보안커널 재구성 기술

→ 다양한 IoT 운영시스템에 적용

정부 보안정책과 부합하는 원격 디바이스 운영기술

→ 공공 인프라 원격 IoT 서비스 연계

기술의 특징

펌웨어 위·변조 방지, 표준 기반 보안프로토콜

경량 암호 및 안전저장 등의 경량 보안커널

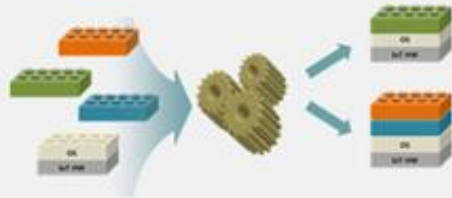
다양한 기기 사양에 맞춤형 보안커널 재구성

안전한 기기관리 및 운영을 위한 기기식별 및 기기인증

세부 제공 기술

맞춤형 보안커널 재구성 기술

- 커널 재구성을 위한 보안 기능별 모듈화 기술
- 재구성 가능한 보안 프로파일링 기술



기기 맞춤형 경량 보안커널 기술

- 펌웨어 위변조 탐지 및 실행 방지 기술
- 키관리 및 암호 알고리즘 구현 기술
- 네트워크 보안프로토콜 기술
- 암호화 저장 기술
- 기기 고유 식별정보 검증 기술
- 자율형 기기간 상호인증 기술



보안정책 기반 원격 기기 보안관리 기술

- 상호인증기반 SW 경량보안업데이트 기술
- 객체 구성 지원 분산접근제어 기술
- 기기간 분산접근제어용 보안정책 관리 기술
- 사용자 권한관리, 접근제어, 프로세스 관리 기술



기존 기술대비 우수성

기존기술 한계

- 최근 IoT 환경에 적용 가능한 경량 암호 알고리즘 자체에 대한 연구가 진행 중에 있지만, 실제 구현된 사례가 많지 않으며, 기존의 국내 보안 시스템과 연동하기에는 어려움이 있음
- IoT(Internet of Things) 디바이스는 전원 및 리소스의 제약으로 인해 기존 PC(Personal Computer)나 서버에서 사용되는 보안 기술을 그대로 적용할 수 없음
- 기존 지능형 IoT 서비스는 범용성이 낮은 경량화된 보안 기법을 개발하여 적용하거나, 최소한의 보안 기능만을 적용하여 운영되는 것이 대부분

본 기술의 우수성

- 세계최초 ECC 인증서 기반 상호 인증 및 Key 분배 기능 제공
- 표준 규격(RFC5191(PANA), RFC3748(EAP), RFC5246(TLS)) 준수 Cortex-M3 기반 개발
- 다양한 통신 환경(ZigBee, LTE, Wi-Fi 등)에서 기기 인증 및 Key분배 적용 가능
- 우수한 처리 성능에 따른 Cortex-M3급 경량 기기 보안 강화 가능
- KCMVP 인증 시험에 대응할 수 있는 다양한 암호 알고리즘 지원
- 국산 암호 (ARIA/SEED) 및 경량 암호 (HIGHT/LEA) 지원

세계최초 국제표준기반 경량형 PANA 프로토콜 구현 및 경량 기기용 KCMVP 대응 고성능 암호 알고리즘 구현

기술완성도(TRL)

TRL 5단계

TRL 9	사업화	<ul style="list-style-type: none"> 본격적인 양산 및 사업화 단계
TRL 8	시작품 인증/표준화	<ul style="list-style-type: none"> 일부 시제품의 인증 및 인허가 취득 단계 - 조선 기자재의 경우 선급기관 인증, 의약품의 경우 식약청의 품목 허가 등
TRL 7	Pilot 단계 시작품 신뢰성 평가	<ul style="list-style-type: none"> 시작품의 신뢰성 평가 실제 환경(수요기업)에서 성능 검증이 이루어지는 단계
TRL 6	Pilot 단계 시작품 성능 평가	<ul style="list-style-type: none"> 경제성(생산성)을 고려한, 파일럿 규모의 시작품 제작 및 평가 시작품 성능평가
TRL 5	시제품 제작/성능평가	<ul style="list-style-type: none"> 개발한 부품/시스템의 시작품(Prototype) 제작 및 성능 평가 경제성(생산성)을 고려하지 않고, 우수한 시작품을 1개~수개 미만으로 개발
TRL 4	연구실 규모의 부품/시스템 성능평가	<ul style="list-style-type: none"> 연구실 규모의 부품/시스템 성능 평가가 완료된 단계 실용화를 위한 핵심요소기술 확보
TRL 3	연구실 규모의 성능 검증	<ul style="list-style-type: none"> 연구실/시험실 규모의 환경에서 기본 성능이 검증될 수 있는 단계 개발하려는 시스템/부품의 기본 설계도면을 확보하는 단계 모델링/설계기술 확보
TRL 2	실용 목적의 아이디어/특허 등 개념 정립	<ul style="list-style-type: none"> 실용 목적의 아이디어, 특허 등 개념 정립
TRL 1	기초 이론/실험	<ul style="list-style-type: none"> 연구과제 탐색 및 기회 발굴 단계

기술이전 내용 및 지식재산권 현황

기술이전 범위

No.	구분	기술자산 보유 내역
1	소프트웨어	<ul style="list-style-type: none"> 지능형 원격검침 인프라용 PANA(with EAP-TLS) 프로토콜 구현 및 운영 프레임워크 지능형 원격검침 인프라용 TLS/DTLS 프로토콜 구현 및 운영 프레임워크 KCMVP 대응 경량 암호 알고리즘 IoT 기기용 블록암호 알고리즘 소프트웨어 버전 1.0 등 프로그램 3건
2	기술문서	<ul style="list-style-type: none"> 스마트 경량 IoT 기기용 운영체제 보안 요구사항 정의서(v1.0) 등 기술문서 8건

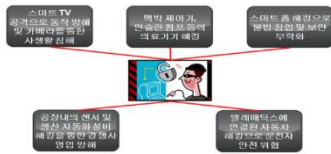
❖ 기술이전 내용 및 상세 범위는 기술 수요자와 협의를 통해 결정

지식재산권 현황

No.	특허번호	특허명	특허상태
1	10-2016-0025945	IoT 디바이스를 위한 보안 장치 및 방법	출원(공개)
2	10-2016-0040025	사물 인터넷 중계 장치, 그를 포함한 시스템 및 그 방법	출원(공개)
3	10-2016-0056362	펌웨어 업데이트 장치 및 방법, 그리고 펌웨어 업데이트 시스템	출원(공개)

기술동향

IoT 보안 기술



- IoT 기기들의 상호 운용성을 위해서는 범용 표준 마련이 우선적으로 필요한 상황임에도 불구하고 현재 IoT 기술을 주도하는 글로벌 표준이 없기 때문에 다양한 표준화 기구들이 각자의 특징점을 바탕으로 연구개발을 진행하고 있음
- 사물인터넷 보안 기술의 2010~2016 간 특허 출원동향을 살펴보면 지속적으로 IoT 보안 관련 기술 개발이 활발한 것으로 나타남
- 해외 선진 IoT 보안업체는 IoT 장치를 보다 쉽고 빠르게 개발할 수 있는 오픈소스 솔루션에 주력
- 국내 보안 업체는 원천기술 확보 부족으로 사물인터넷 보안 기술 및 산업 주도가 쉽지 않은 상황에 놓여 있음

AMI System (지능형계량시스템) 기술



- AMI 기반의 소비자 서비스를 제공하는 기업으로는 Opower, SDG&E, ENNET, Bidgely, PG&E, ComEd 등이 있으며 에너지 컨설팅 또는 다양한 요금과 고지 서비스 제공
- 일본 회사인 Ennet社는 인터넷 회원에게 시각화된 전력소비량 정보를 제공하여 절전을 유도하는 서비스로서 30분 간격으로 전력소비량 정보를 제공하며, 과소비 시 알람 기능 제공
- Bidgely社는 플러그에 센서를 장착하지 않고 AMI 빅데이터만을 분석·활용하여 고객에게 가전제품별 소비량과 전기요금을 제공
- ComEd社는 AMI 전력데이터 및 정산서비스 플랫폼을 활용, 고객에게 전기요금 고지서를 제공하고 있으며, 각 기기 별 전력 사용량 및 이에 따른 예상 전기요금, 스마트 온도제어장치를 통한 전력 사용을 제어함

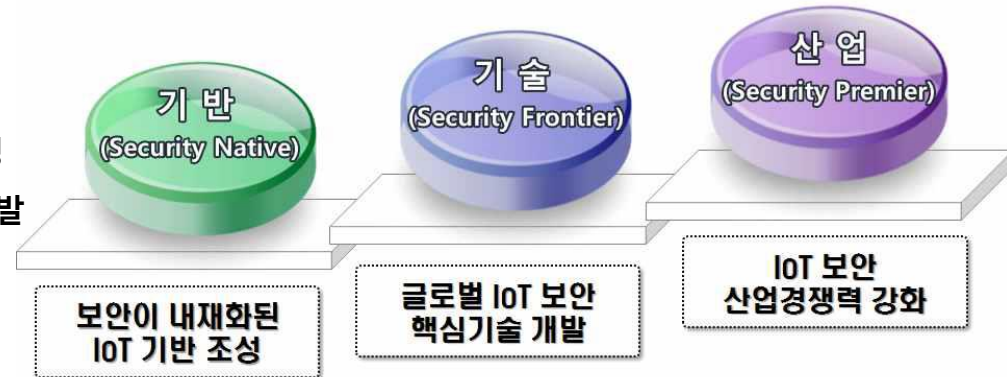
정책동향

IoT 보안 정책 현황

- 미래창조과학부는 IoT 제품·서비스의 취약한 보안 현실을 체계적으로 개선해 나가기 위해 2015년 6월 '사물인터넷(IoT) 정보보호 로드맵 3개년 시행계획'을 발표하였으며, 이는 보안이 내재화된 IoT 기반 조성, 글로벌 IoT 보안 선도기술 개발 및 IoT 보안 산업경쟁력 강화를 목표로 함

IoT 정보보호 로드맵 3개년 시행계획 핵심 추진과제

1. Security Native : 보안이 내재화된 IoT 기반 조성
2. Security Frontier : 글로벌 IoT 보안 선도기술 개발
3. Security Premier : IoT 보안 산업경쟁력 강화



IoT 제품 서비스의 취약한 보안 현실을 체계적으로 개선해 나가기 위해 정부차원의 보안 시책 강화

기술사업화 진입시장

- 1차 시장 : 지능형 전력계량 보안 서비스
- 2차 시장 : 스마트 홈/빌딩 IoT 보안 솔루션



지능형 전력계량 보안 서비스

- 스마트미터
- 통신설비
- 지능형 전력정보관리시스템(MDMS)
- AMI 운영시스템

B2B

B2C

B2G

주력 거래유형



스마트 홈/빌딩 IoT 보안

- IoT 보안 게이트웨이
- IoT 보안 서버
- IoT 암호화

B2B

B2C

B2G



헬스케어/의료 보안

- 헬스케어/의료 디바이스
- 헬스케어/의료 플랫폼
- 의료정보처리 시스템 보안

B2B

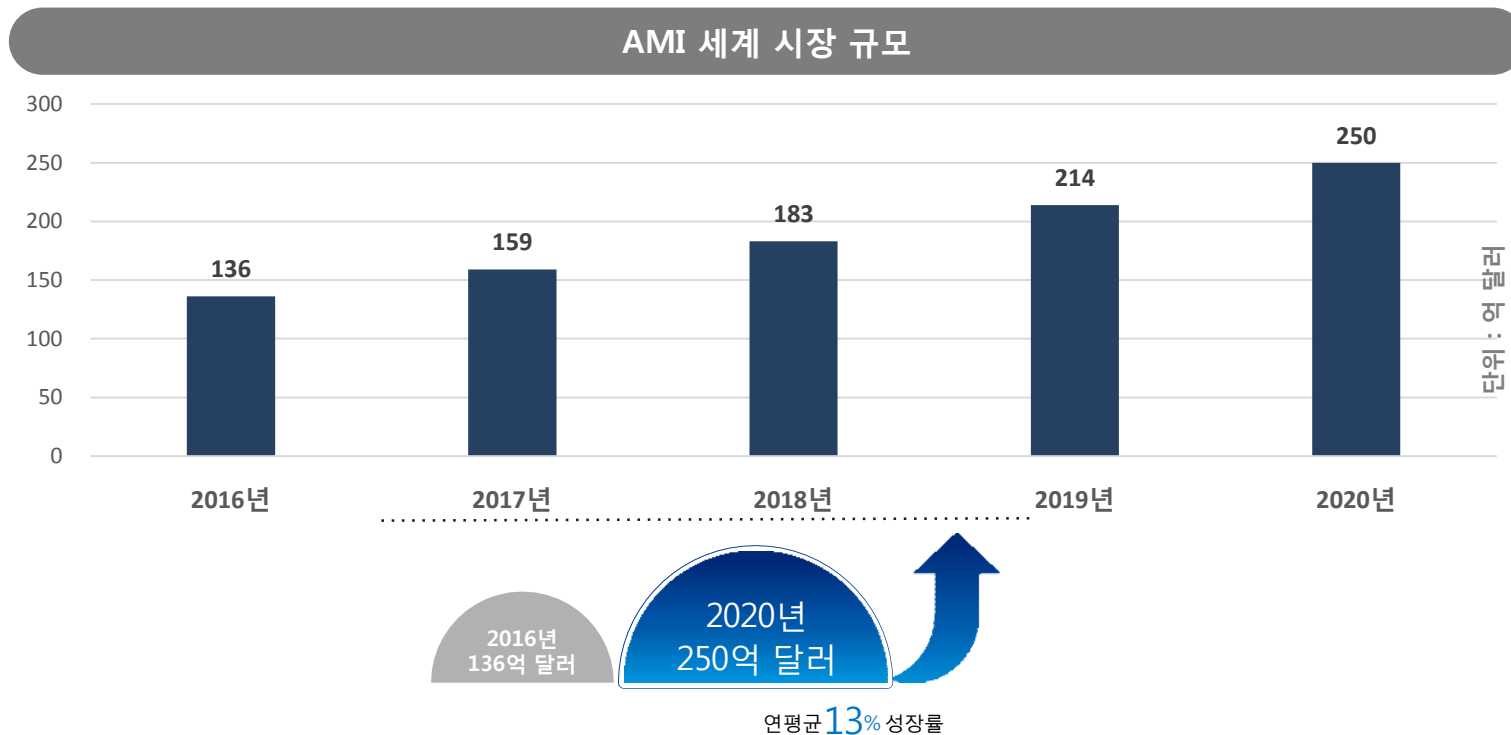
B2C

B2G

실시간 전력계량 정보제공 서비스(AMI) 세계 시장 동향

세계 AMI 시장규모는 2016년 약 136억 달러로 추정되고 2020년에는 250억 달러로 2016년 대비 약 1.8배 증가할 것으로 예상

※ 출처 : 중소기업청, 에너지산업, 중소기업기술로드맵, 2017-2019,, 2016. 재구성



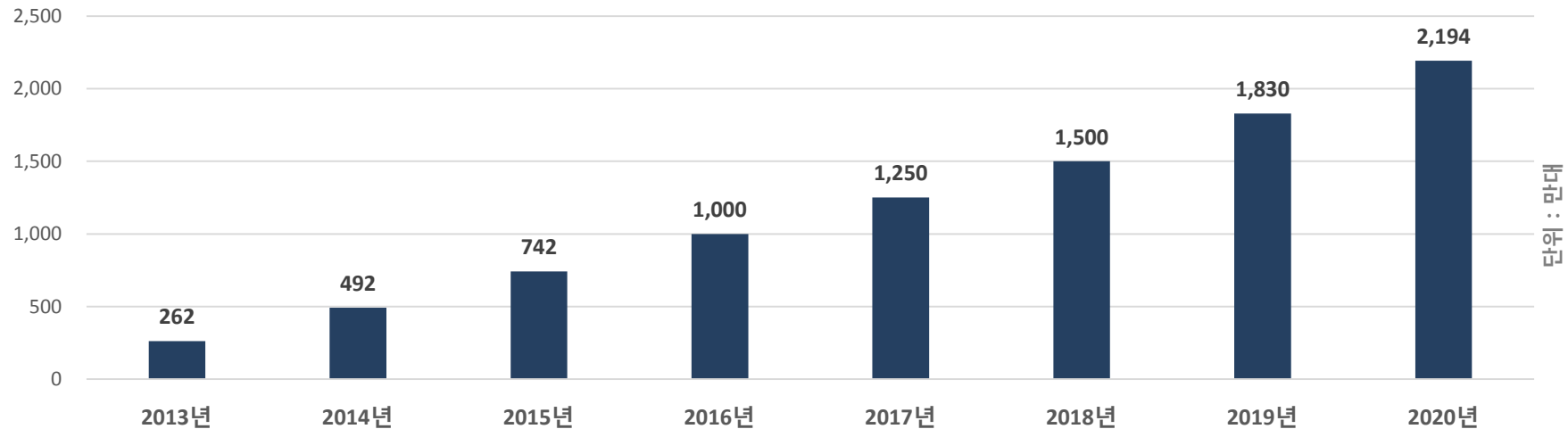
현재 시장은 초기단계이며, 향후 성장가능성이 높은 분야로서 AMI를 통해 새로운 생활 패턴 및 전력 소비 문화의 변화 진행

실시간 전력계량 정보제공 서비스(AMI) 국내 시장 동향

국내의 경우 전력수급 안정과 전력소비 감축을 위한 지능형 전력 솔루션 시장은 연평균 61.4%의 높은 성장률을 보이며 2020년 약 1,568억 원 시장 규모 예측

※ 출처 : 중소기업청, 에너지산업, 중소기업기술로드맵, 2017-2019,, 2016. 재구성

➤ 2013년부터 2020년까지 8년간 저압 AMI를 2,194만대 보급할 계획



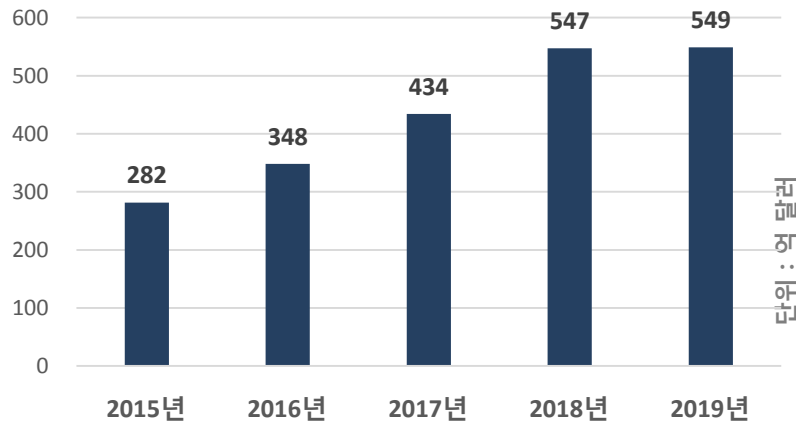
사업효과가 큰 일반용·산업용·밀집 주거지역 위주로 우선 보급하여,
AMI를 활용한 지능형 전력서비스 제공 추진

IoT 보안 분야 시장동향

2015년 IoT 보안 시장규모는 282억 달러 규모이며, 연평균 14%씩 성장하여 2019년에는 549억 달러에 이를 전망

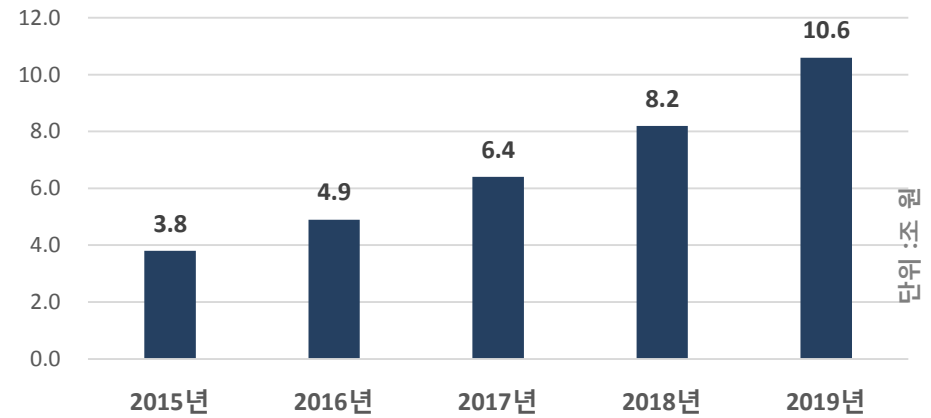
※ 출처 : 중소기업청, 정보보안, 중소기업기술로드맵, 2017-2019,, 2016. 재구성

IoT 보안 분야 세계 시장규모



연평균 14% 성장률

IoT 보안 분야 국내 시장규모



연평균 23% 성장률

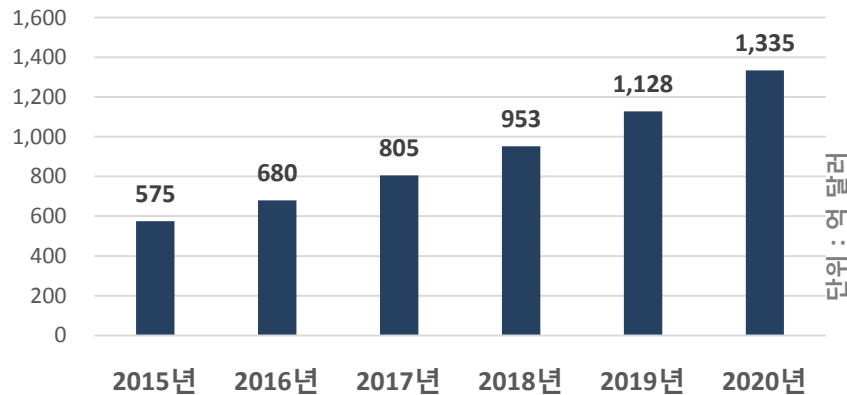
사물인터넷 보안 분야에 대한 지출은 기술력 향상, 조직 변화 및 확장 가능한 서비스 옵션이 늘어남에 따라 빠른 속도로 증가 예상

스마트 홈 시장동향

2015년 전세계 스마트 홈 시장규모는 575억 달러 규모이며, 연평균 18.34%씩 성장하여 2020년에는 1,335억 달러에 이를 전망

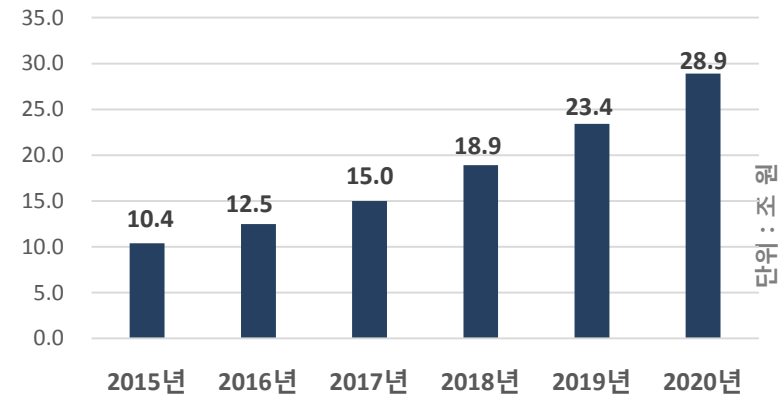
※ 출처 : 출처 한국스마트홈산업협회,(2014)

스마트 홈 세계 시장규모



연평균 18.34% 성장률

스마트 홈 국내 시장규모



연평균 23.7% 성장률

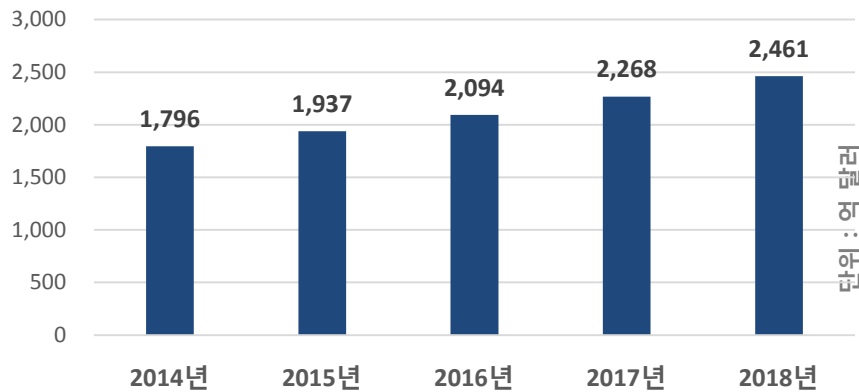
편리하면서도 안전하고, 즐거움이 있는 세련된 주거 생활에 대한 욕구가 강해지면서, 스마트 홈/빌딩의 공급 제품과 서비스에 대한 수요 증가

스마트팩토리 시장동향

사물인터넷 기반 스마트팩토리 세계시장 규모는 2014년 1,796억 달러 규모였으며, 매년 6.8% 성장하여 2018년 2,461억 달러 규모로 성장전망

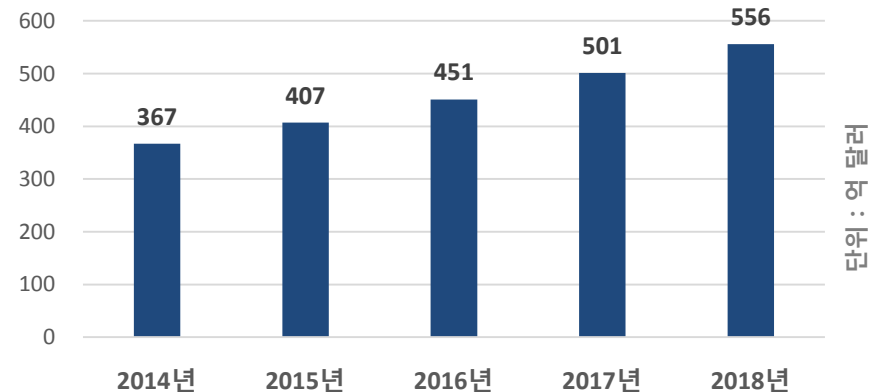
※ 출처 : MarketsandMarkets Analysis, 2013.1

스마트팩토리 세계시장 규모



연평균 6.8% 성장률

스마트팩토리 아시아 시장 규모



연평균 8.7% 성장률

제조업과 ICT 융합이 생산 방식의 혁명을 일으키면서
스마트팩토리가 제조업 위기의 돌파구로 주목 받고 있음

시장참여자 현황

- 전력수요관리사업자
- IoT 보안 솔루션 개발업체

전력수요관리사업자

기업명	대표자	업체 동향
아이디알서비스(IDRS)	강혜정	<ul style="list-style-type: none"> • 수요자원시장, 연구개발, 신재생 에너지 실시간 모니터링 서비스 제공 • 중,대형 산업고객의 수요관리 업무 및 소,중형 사용고객의 자동화된 수요관리 업무 수행 • 신재생 에너지 실시간 계측 시스템 및 실시간 예측 시스템 개발 및 공급 • 새로운 전력사업 비즈니스 모델 개발 위한 지능형 전력사업모델 제시 및 TEST BED 구현
그리드 위즈	김구환	<ul style="list-style-type: none"> • 자동수요반응서버(OpenADR2.0) 이용, 실시간 전력분석시스템 기술(미터링, RRMSE, CBL 분석, 정산) 보유, 에너지 빅데이터를 활용한 분석, 예측, 리스크 관리(미국 AutoGrid사 제휴)
에너지코리아 (ENERNOC)	김형민	<ul style="list-style-type: none"> • 전기 사업자들에게 클라우드 컴퓨팅 기반의 EIS(Energy Intelligence Software: 에너지 인텔리 전스 소프트웨어)와 관련 서비스 제공
포스코ICT	최두환	<ul style="list-style-type: none"> • 신재생에너지 발전에서부터 에너지 수요/공급 최적화, 소비 효율화, 전기차 운영 인프라에 이르기까지 효율적인 에너지 사용을 위한 Total 서비스 제공

IoT 보안 솔루션

기업명	대표자	업체 동향
SK인포섹	안희철	<ul style="list-style-type: none"> • IoT 기기 보안성을 강화하는 솔루션을 제공하고 있으며, 초경량 보안게이트웨이 개발 출시
LG이노텍	박중석	<ul style="list-style-type: none"> • LG이노텍은 무선통신기술과 제품을 융합한 보안 분야 IoT 제품 출시하고 있으며, 통신계열인 LG유플러스와 LG CNS 와 연계하여 IoT 솔루션 및 서비스 IoT 플랫폼 서비스 제공
씨제이엔스(CIS)	박세철	<ul style="list-style-type: none"> • DDoS 공격의 원인이 되는 좀비 PC를 가장 효과적으로 탐지/치료하는 TMS 솔루션과 가상화, 클라우드 환경에서 적용 가능한 업계 최초, 최고의 보안 솔루션을 제공
(주)티엔젠	심상국	<ul style="list-style-type: none"> • 사물인터넷에서 유통되는 각종 데이터를 검증 암호로 기밀성과 무결성을 제공하는 제품 및 솔루션 공급
(주)드림시큐리티	범진규	<ul style="list-style-type: none"> • PKI기반의 보안·인증솔루션 및 서비스를 제공하는 IT 인증 보안 전문기업으로 IT 환경, 스마트환경, 클라우드 등 빠르고 다양하게 변화하는 IT 환경의 보안 솔루션 및 서비스 제공업체
시큐리티플랫폼	황수익	<ul style="list-style-type: none"> • 사물인터넷 기기의 보안성을 높일 수 있는 칩 기반의 가상 사설망(VPN) 솔루션 '엑시오-VPN(AXIO-VPN)'을 개발 출시

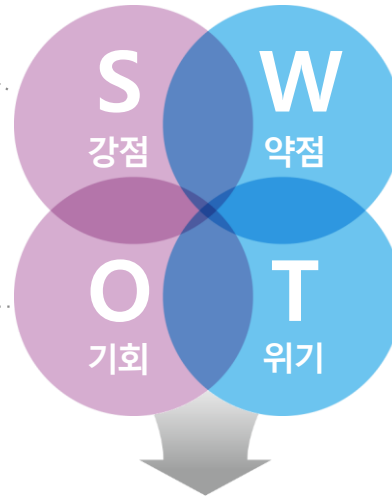
SWOT 분석

세계최초 국제표준기반 경량형 PANA 프로토콜 구현 및
경량 기기용 KCMVP 대응 고성능 암호알고리즘 기술

IoT는 다양한 산업분야에 적용되고 있으며,
홈·가전/스마트그리드/의료· 헬스케어/교통분야 시장
활성화에 따른 보안 수요 증대

정부정책차원에서 연구개발 및 시장 활성화 위한
적극적인 지원 시책들을 제공하고 있음

다양한 IoT 서비스가 가능하며, 시장 확대에 의한 보안
시장도 활성화되고 있음



스마트그리드 산업은 대규모 시스템 구축으로
독자적 사업이 어려우며, 신규비즈니스 영역으로
수익성 실현 난해

IoT 보안 기술 전문 인력 부족으로 원천기술
확보가 어려움

스마트그리드 등 기간산업 분야 IoT 서비스는 대규모
실증이 요구되어 상업화 되기까지는 시간이 다수
소요될 수 있음

글로벌 선진기업의 국내 진출이 가속화되고 있으며,
대기업 위주의 시장 생태계 구축

SO 전략(우선수행)

- 다양한 산업에 범용으로 사용가능 한 경량 IoT 보안 기술 활용
- 특화된 사업화 모델 개발 통한 시장 선점과 대기업과의 협력 통한 시장 진출

WO 전략(우선보완)

- 민관 공동 R&D 통해 기존IoT 보안 기술과 결합한 차별화된 전력 계량 정보제공 솔루션 확보
- IoT 보안 하드웨어 및 보안 소프트웨어 솔루션 원천기술 도입 통한 신속한 시장 진입 필요

ST 전략(RISK 해결)

- IoT 서비스에 요구되는 보안성/안정성/확장성이 검증된 실용화단계에 있는 검증된 IoT 보안기술 적용
- 대규모보안 시스템 구축사업은 정부와한전을 중심으로 한대기업이 진행하므로, 이들의 기술 수요를 반영한 보안 솔루션 개발

WT 전략(장기보완)

- 공동 R&D를 통해 기존IoT 보안 기술과 결합한 차별화된 실시간 전력계량 정보제공 서비스 구축
- 정부지원 사업의 적극 활용 통한 신속한 IoT 제품/ 서비스 상용 체계 구축

시장진입전략

진입시장

지능형 전력계량 정보제공 서비스

스마트 홈/빌딩 IoT 보안

헬스케어/의료 보안

목표고객

- 시스템 솔루션 개발 업체
- 전력수요관리사업자
- 한국전력

- 시스템 솔루션 개발 업체
- 스마트 가전기기 생산업체
- 지능형 보안 솔루션 공급업체

- IoT SW 개발 업체
- 의료기기 생산업체
- 웨어러블 디바이스 제조 업체

진입전략

지능형 AMI 상용서비스
효율적 에너지 관리/통제

스마트 홈 전자기기 보안 관리
지능형 보안 서비스 제공

의료기기/ 시스템 서버 등의
물리적 장치 보안
웨어러블 디바이스간 IoT 보안

Smart Grid

- 고성능 계량 IoT 보안
 - 주기적 데이터 계량 수집
 - 실시간 모니터링
 - 전력소비제어
 - 시간대별 차등요금제 운영
 - 계통 연계 조정

IoT THINGS

- 홈/빌딩 자동화 보안
 - 홈/빌딩 자동화 기기
 - 홈/빌딩 게이트웨이/월 패드
 - 아파트/빌딩 관리 서비스
- 홈/빌딩 시큐리티 관리
 - 가정 재난/보안 관리서비스
- 지능형 홈/빌딩 서비스
 - 홈 클라우드 서비스
 - 비상 상황 인지서비스
 - 홈 로봇 서비스
- 의료 정보 시스템 보안
- 헬스케어 플랫폼 보안
- IoT 디바이스 보안

기술도입 필요성(NABC)

Needs(시장수요)

- IoT 보안기능 부재는 사물인터넷 산업 성장을 저해하는 요인으로 작용되고 경량 IoT 기기에 적합한 보안 기술이 필요하며, 보안 접근방법 및 적용 범위의 확장 필요
- 하드웨어 및 서비스의 설계 단계부터 높은 보안성이 요구되며 디바이스 간 접속 및 정보전송에 강력한 인증 및 암호화 기술 필요
- 지능형 원격검침 IoT 기기용 운영체제의 핵심 보안 기술 개발을 위해서는 기존보다 강화된 암호 알고리즘 필요

Approach(해결방법)

- IoT 서비스는 다양한 사물 및 서비스 간 상호 운영이 중요하므로 이의 통신방법/보안체계의 표준화된 기술 사용
- 다양한 통신 환경(ZigBee, LTE, Wi-Fi 등)에서 기기 인증 및 Key분배 적용 가능한 기술 활용
- 우수한 처리 성능에 따른 Cortex-M3급 경량 기기 보안 강화 및 KCMVP 인증 시험에 대응할 수 있는 다양한 암호 알고리즘 적용

Benefit(기대효과)

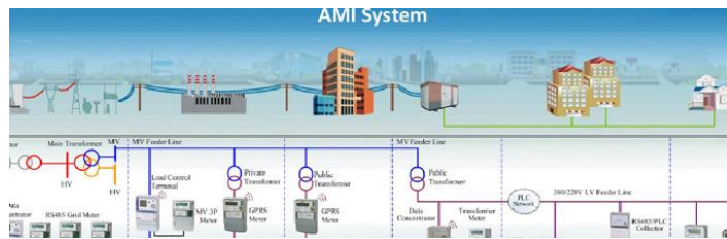
- 전력, 가스, 수도 및 교통시스템과 같은 국가주요 기반시설이나 산업분야에서 원거리에 산재된 시스템의 효과적인 보안 및 제어
- 해킹에 의한 기기 위변조를 방지하고 비인가 접근을 차단하여 안전한 지능형 AMI 서비스 제공
- IoT 기기의 위변조 방지, 비인가 접근차단, 오작동 방지 등 보안성이 우수한 스마트 경량 IoT 운영서비스 가능

Competition(경쟁현황)

- 국내 스마트 IoT 보안기술은 폐쇄적인 구조, 독점적인 통신 프로토콜, 제한된 연결성의 특징으로 IoT 서비스 보안 문제를 공극(Air-Gap) 정책으로 접근함으로써, 외부경계 보호에만 치중하는 실정
- AMI를 기반으로 한 비즈니스모델이 다양하지는 않지만 다양한 산업분야와 연계하여 비즈니스 영역이 확대될 가능성이 있음
- 스마트 홈/빌딩 보안 산업의 경우엔 과점 형태의 산업 구조에서 다양한 기술 기반의 경쟁 구조로 변화가 일어나고 있음

비즈니스 아이디어

지능형 전력계량(AMI)보안 서비스



AMI 운영 System 보안 (MDMS, AMI 운영시스템)

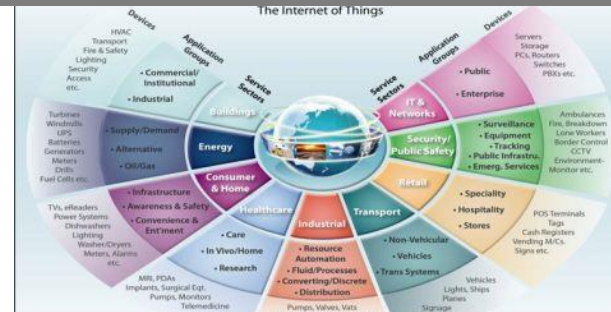


지능형 계량기간 보안 (스마트 미터, 통신 설비)

스마트 홈/빌딩 IoT 보안 솔루션



지능형 가전/사무 기기 IoT 보안

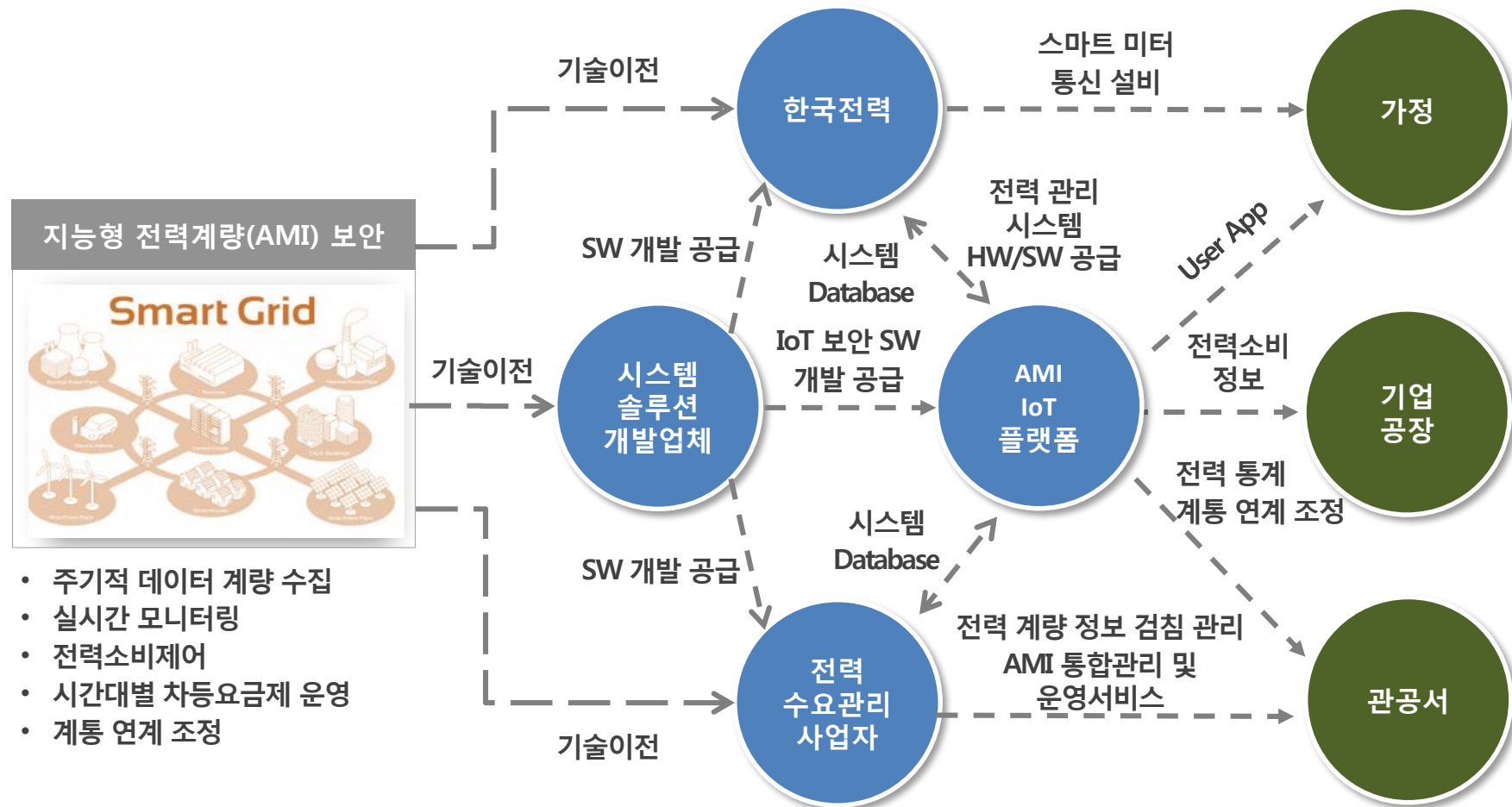


지능형 IoT 플랫폼 보안

지능형 IoT 서비스의 취약한 보안 문제를 해결하는
고성능 경량 IoT 보안 메커니즘을 적용한 지능형 보안 서비스 및 솔루션 공급

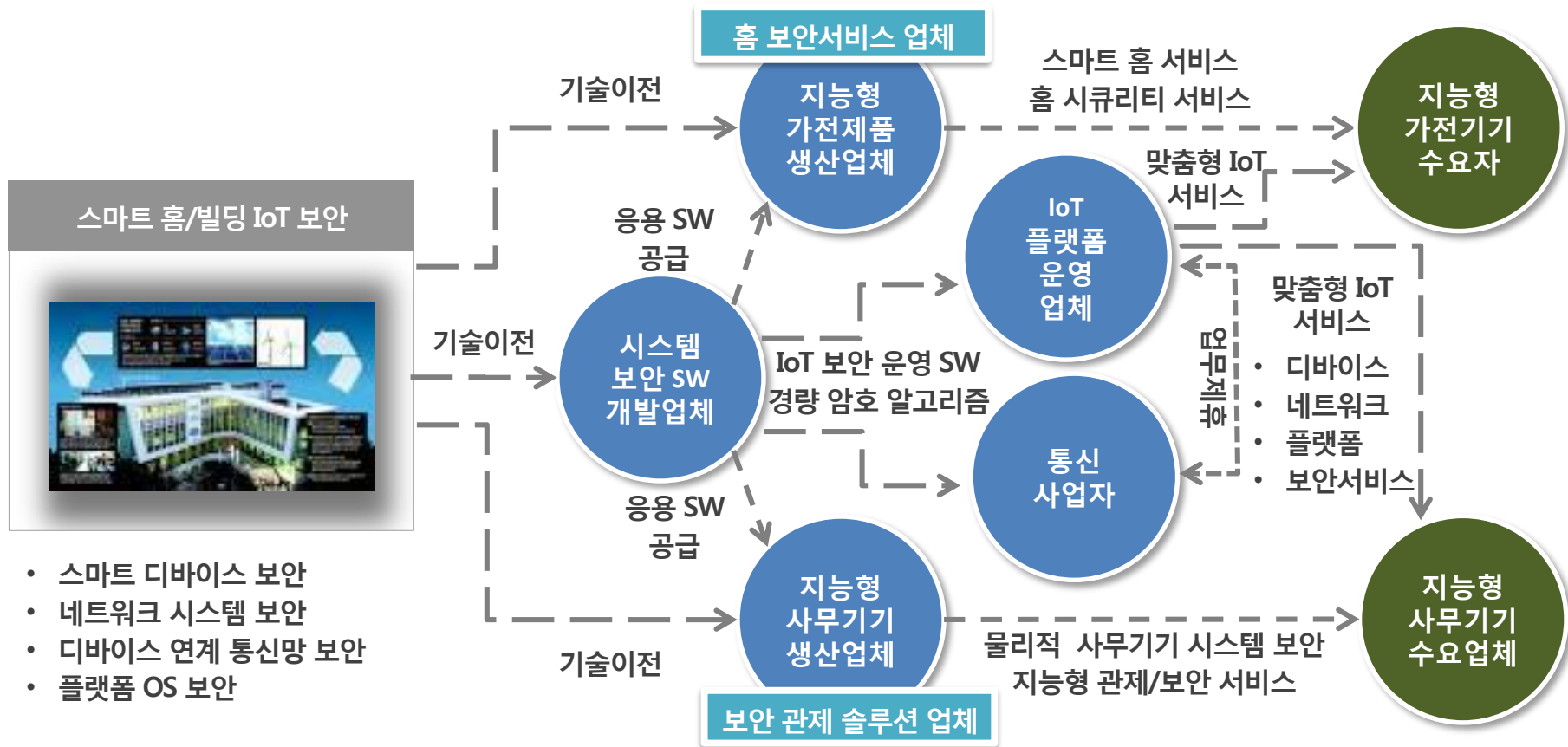
비즈니스 아이디어(1) : 지능형 전력계량 통합 보안 솔루션

- 지능형 전력계량(AMI) IoT 보안 SW 개발 공급
- AMI IoT 인증/보안 업데이트 등 응용 SW 기술지원



비즈니스 아이디어(2) : 스마트 홈/빌딩 IoT 보안 솔루션

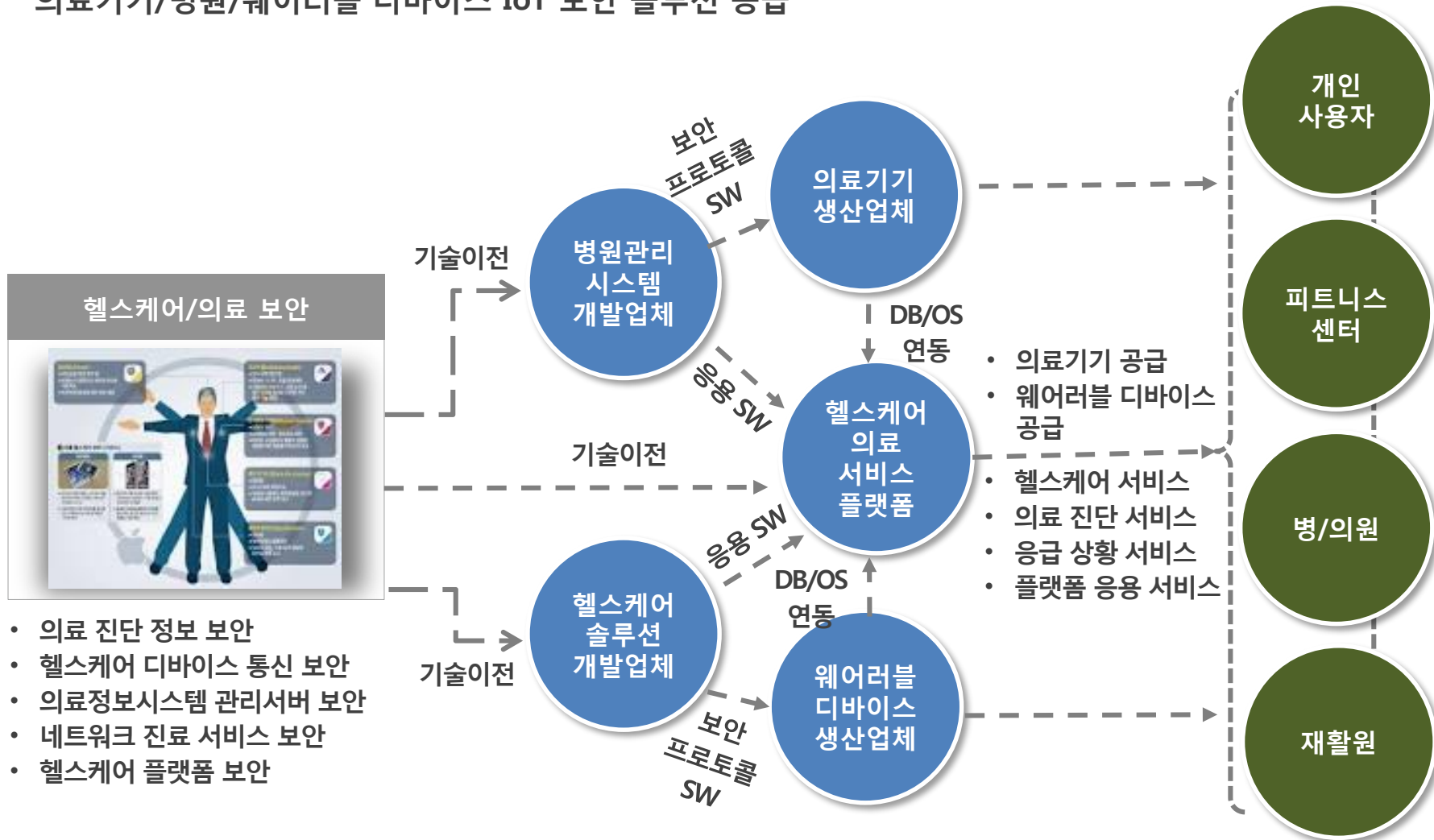
- 스마트 홈/빌딩 플랫폼의 안정적 보안서비스 통한 사용자 편의성 증대
- 사용자 관점의 맞춤형 킬러 서비스 공급



- 스마트 디바이스 보안
- 네트워크 시스템 보안
- 디바이스 연계 통신망 보안
- 플랫폼 OS 보안

비즈니스 아이디어(3) : 헬스케어/의료 보안 솔루션

- 의료기기/병원/웨어러블 디바이스 IoT 보안 솔루션 공급



비즈니스 아이디어 예상 수익구조

기술/서비스 흐름



수익 흐름



지능형 원격검침 인프라용 경량 IoT 기기 보안 기술



지능형 원격검침 경량 IoT 보안 기술
KCMVP 대응 경량 암호 알고리즘
기술이전 / 상용화 지원

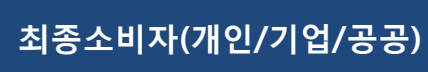
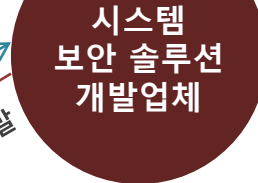
기술료

기술료

기술이전 / 상용화 지원

기술료

시스템 연동 프로토콜
운영프레임워크
기술이전 / 상용화 지원



비용 지급

보안 SW 개발

보안 SW 개발

비용 지급

보안 솔루션 공급

업무 협약 체결

업무 협약 체결

전력 공급

사용료 지불

서비스 공급

서비스 이용료

콘텐츠 공급
서비스 이용료

기술사업화 시나리오

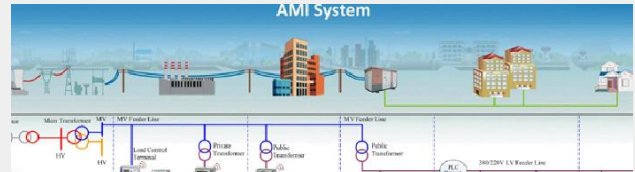
비즈니스
아이디어

목표시장
/고객

고객
기대효과

시기별
실행계획

지능형 전력계량 통합 보안 솔루션



AMI시스템 통합관리 및 다양한 MDMS(Meter Data Management System) 서비스를 제공하는 경량 IoT 보안 라이브러리

- ### AMI 보안 솔루션/플랫폼
- 시스템 솔루션 개발 업체
 - 전력수요관리사업자
 - 한국전력
 - 개인 가정
 - 산업체

원격 전력수요 검침
전력에너지 절약

전력 데이터 수집/관리
전력 데이터 통합관리

스마트 홈/빌딩 IoT 보안 솔루션



스마트 홈/빌딩 IoT 서비스의 최적화 보안기술 제공 통한 다양한 비즈니스 모델 생산 및 사용자 편의성 증대

- ### 스마트 홈
- 스마트 가전기기 생산
 - 홈 시큐리티 서비스
 - 웨어러블 디바이스 생산 업체

- ### 스마트 빌딩
- 사무기기 생산업체
 - 빌딩 관리 업체
 - 보안/관제시스템 운영업체

사용자 편의성과
안전성 확보

다양한 이종 디바이스
운영/연계서비스 확대

	1년차 (기술이전)	2년차 (사업화)
기술협력	기술지도, 관련 기술 전수	상용화 테스트 지원
기업 필요자금	착수기본료: 협의 매출정률사용료: 1.25%~5%	기술지도 비용(협의)
기타 지원사항	기술문서 제공 (지능형 원격검침 인프라용 운영 프로그램)	테스트 인력 지원

ETRI 개발기술 도입 통한 사업화 프로세스



ETRI 기업지원 프로그램



시장 수요 중심의 기술 기획

시장 가치 중심의 성과 확산

기술사업화 정부지원 사업

BM 기획

No.	사업명	발주기관	사업내용	과제당 사업비
1	Tech-BM Workshop 운영 사업	연구성과실용화진흥원	사업화 목적에 최적화된 사업성 분석, 시나리오 분석 등의 BM타당성 검증과제 지원	10백만원
2	연구소기업 설립 사전 기획	연구개발특구진흥재단	연구소기업 설립에 필요한 비즈니스 모델 수립 등 기획 지원	15백만원

기술업그레이드

No.	사업명	발주기관	사업내용	과제당 사업비
1	중대형 복합 기술사업화 지원	연구성과실용화진흥원	신시장·신산업 창출을 위한 신제품·서비스 상용화 공동R&D 자금 지원	7.5억 원
2	기술업그레이드 R&D	연구성과실용화진흥원	시제품 제작, 성능개량 및 향상 등 사업화에 필요한 추가연구개발 지원	2억 원
3	R&D 재발견 프로젝트	한국산업기술진흥원	공공연구 보유 기술을 중소·중견기업에 이전하고, 사업화 위한 기업과 공공연구의 추가 상용화 개발 지원	4억 원

기술사업화

No.	사업명	발주기관	사업내용	과제당 사업비
1	기술이전사업화 (R&BD과제)	연구개발특구진흥재단	공공기술을 이전(출자, 연구소기업) 받은 기업의 사업화(R&BD) 과제 지원	제품혁신형: 2억 원 시장창출형: 4억 원 글로벌도약형: 10억 원 연구소기업: 3억 원
2	사업화연계기술개발사업	한국산업기술진흥원	사업화 유망기술에 대한 제품화개발, 시제품제작, 성능평가 및 인증, 디자인 등 사업화 지원	투자유도형: 8억 원 BI연계형: 3억 원

기술이전 문의



ETRI 사업화협력실

042-860-1804 / hominkim@etri.re.kr