보도자료 첨부용

대외공개

세계최고의 스마트 안심국가 실현을 위한

사물인터넷(IoT) 정보보호 로드맵

2014. 10. 31

미래창조과학부

목 차

Ⅰ 배 경

□ 사람, 사물, 공간, 데이터 등 **모든 것이 연결되는 超연결사회**가 도래함에 따라, 사물인터넷(IoT)이 미래의 **새로운 경제성장 동력**으로 부상

o IoT는 다양한 산업분야에 적용되고 있으며, 우리생활과 밀접한 홈·가전, 의료, 교통분야에서는 **본격적인 시장 활성화**가 진행 중

※ IoT로 창출되는 부가가치는 '20년까지 약 1조 9천억달러로 전망(가트너, '13년)

※ 글로벌 정보통신 전시회(CES, MWC, CeBIT 등)에서도 스마트홈, 웨어러블 헬스케어, 스마트카 등 IoT 기반 제품·서비스가 다수 출시

o 우리나라를 비롯해 세계 주요국*과 구글, 오라클, 시스코 등 글로벌 기업들이 **가장 적극적으로 투자·육성하고 있는 분야**

* 한국(사물인터넷 기본계획, '14.5월), 미국(리쇼어링 이니셔티브), 독일(인더스트리 4.0), 영국(British Innovation Gateway), 중국(감지중국(感知中國) 전략) 등

o 또한 IoT가 현실과 접목되어 발전·에너지 등 **주요 사회기반시설 인프라에 적용**되는 등 **사이버물리시스템*(CPS)의 중요성**이 부각

* 기존의 장치·설비(물리시스템) 등에 ICT 기술이 밀접하게 적용된 시스템

□ 그러나, IoT는 **활용분야가** 우리 실생활의 **모든 사물에 '직접 접목'**되기 때문에, 기존 사이버공간의 위험이 **현실세계로 전이(轉移)·확대***

* 기존 정보유출 및 금전탈취 등을 넘어 인간의 생명과 국가 기반시설까지 심각하게 위협하며, 이로 인한 경제적 피해는 '20년까지 17조 7천억원으로 전망(산업연구원)

o 또한, IoT 보안위협은 오동작·정지 등 **사람의 생명을 위협**할 만큼 **치명적**이며, 도입후에는 사후 보안조치가 **불가능**하거나 **高비용이 수반**

o IoT 보안은 선진국·글로벌 기업의 핵심 성장동력으로 추진, **보안이 적용되지 않은 IoT 제품·서비스**는 글로벌 시장에서 **경쟁력을 상실**

□ **누구나 안전하게** 사물인터넷의 **편리함을 누리고,** 이를 **창조경제 실현**을 위한 **미래 新성장동력으로 육성**하기 위해서는,

o **정보보호(Security)가 담보**된 **안전한 IoT 이용환경 조성**이 필수

참고 사물인터넷(IOT)과 사이버물리시스템(CPS) 개념

□ 개념

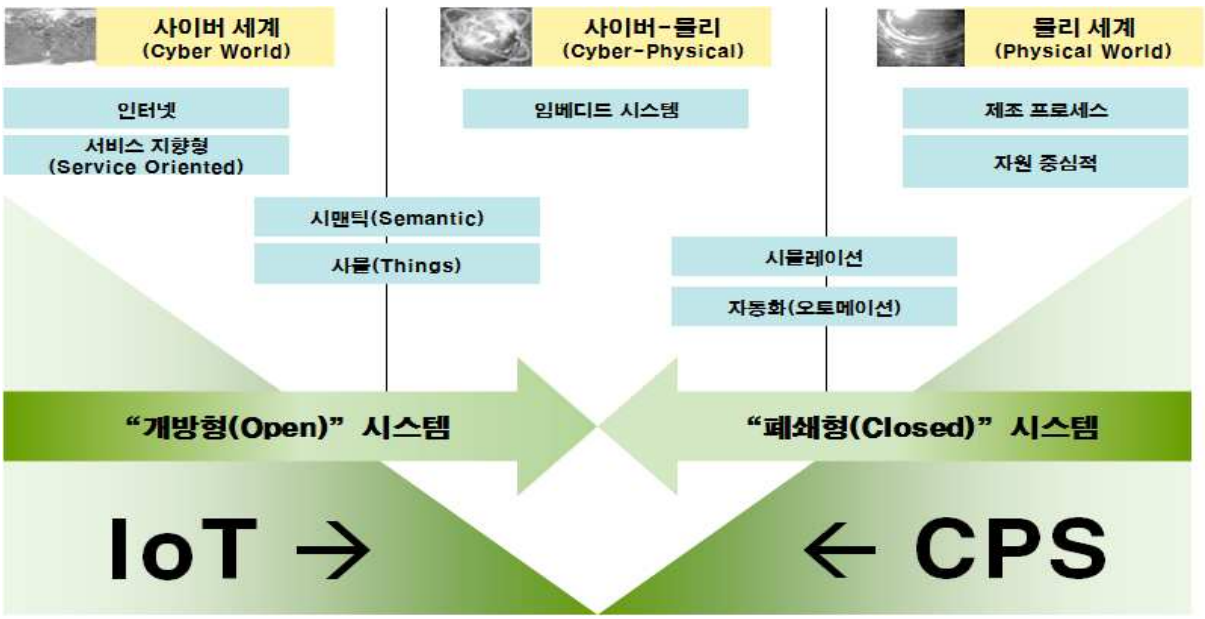
○ (IoT) 모든 사물에 태그, 센서 등을 부착하고 인터넷으로 연결하는 개념에서 사물 자체가 스마트 디바이스化되는 개념으로 진화

○ (CPS) 산업시설, 제조설비 등 물리시스템(Physical System)을 NW로 연결하고 센서, 엑추에이터 등을 활용하여 관리·통제하는 개념

⇨ **센서 등을 기반으로 각종 시설·디바이스를 네트워크로 연결하여 서비스하는 핵심개념과 주요 적용분야가 동일**

< IoT-CPS 비교 >

구분		IoT	CPS
등장		1999, Kevin Ashton, MIT	2006, Helen Gill, NSF
차이점	주된 관심 영역	스마트 디바이스, 네트워크, 주로 개방형 시스템	물리시스템, 임베디드 시스템, 주로 폐쇄형 시스템
	접근 방식	센서, 인터넷 등 기술을 융합하여 새로운 서비스를 개발	현존하는 물리시스템에 센서 등 ICT 기술을 접목하여 신뢰성 높은 시스템을 구현
공통점	핵심 개념	네트워크를 기반으로 구성요소(센서, 장치 등)를 연계	
	주요 적용 분야	- 농축수산·식품, 제조·유통, 교통·물류, 의료·복지, 문화관광·교육, 에너지·환경, 홈·도시, 국방 등 * 출처 : 사물인터넷 기본계획	- 스마트제조·생산, 교통, 에너지, 기반시설, 헬스케어, 빌딩 및 건설, 국방, 재난대응 등 ※ 출처 : Strategic RnD Opportunities for 21 Century Cyber-Physical Systems(NIST, 2013.01)



※ 출처 : Everything 4.0?-Drivers and Challenges of Cyber Physical Systems, Sabina Jeschke(2013.12)

Ⅱ IoT 동향 및 정보보호 패러다임 변화

1 IoT 시장전망 및 동향

□ **(시장)** IoT를 차세대 핵심 산업으로 인식, 세계 각국의 활성화 대책 수립·시행과 주요기업의 참여로 관련 시장의 급격한 성장 예상

< 2020년까지의 시장 전망 >

세계 시장 규모(단위 : 십억달러)	국내 시장 규모(단위 : 십억원)
 ※ 출처: Machina Research, STRACORP, 2013	 ※ 출처: STRACORP, 2013

o **(세계시장)** '13년 2천억불 → '20년 1조불, 연평균 26.21% 성장 전망

- 전세계 IoT 응용SW와 서비스의 시장성장률(~'20년)은 각각 89%와 122%로, IoT 기기(11.2%)에 비해 **응용SW, 서비스 중심으로 성장**할 것으로 예상

< 전세계 IoT 구성요소별 시장전망 >

(단위 : 십억 달러)

구 분	2013년	2014년	2015년	2016년	2017년	2018년	2019년	2020년	CAGR(%)
제품기기	1,887.98	2,140.43	2,486.63	2,785.50	3,093.25	3,355.67	3,713.07	3,970.44	11.20
통신망	95.17	109.91	139.06	181.21	225.14	268.29	308.43	355.50	20.72
응용SW	36.63	82.51	176.78	439.55	962.08	1,548.56	2,205.64	3,111.49	88.62
서비스	10.88	37.43	123.96	293.17	776.82	1,443.66	2,171.08	2,920.11	122.31
소 계	2,030.66	2,370.28	2,926.43	3,699.43	5,057.29	6,616.18	8,398.22	10,357.54	26.21

※ 출처: Machina Research, STRACORP, 2013

o **(국내시장)** '13년 2.3조원 → '20년 17.1조원, **연평균 32.8% 성장 전망**

※ 시장범위 : 제품기기(칩셋, 모듈 등) + 통신망(CDMA, LTE 등) + 응용SW + 서비스(텔레메틱스, 스마트그리드 등) 등

o **(정부)** EU, 미국, 중국 등 주요국에서는 범정부차원 계획 수립·추진

< 주요국 IoT 관련 정책 추진 현황 >

EU	미국	중국
IoT 활성화를 위해 기본적으로 추진해야할 실행과제를 명시한 '사물인터넷 액션플랜' 수립·추진('09년)	IoT/CPS를 국가 R&D 우선과제로 지정하고, 차세대 IoT 기술·과학·공학분야, 교육개발 등 150여개 프로젝트에 대한 연구투자 지원('09~'14년)	IoT 기반의 국가 핵심기술 개발, 산업화, 표준화 연구 등에 대한 추진방향을 제시한 '사물인터넷 12차 5개년 발전계획' 수립·추진('12년)

※ (독일) Industry 4.0 추진('12년), (영국) '25년까지 IoT 연구개발에 4,500만 파운드 투입('14년)

※ (미국) 국가정보위원회(NIC)는 '6대 파괴적 혁신 기술'로 사물인터넷을 선정하고 지원('08년)

o **(민간)** IBM, 구글, 삼성, SKT 국내·외 글로벌 기업은 자사의 경쟁력을 바탕으로 IoT 주도권을 확보하기 위한 합종연횡(合從連衡) 심화

< 주요기업 간 IoT 관련 인수·합병 현황 >

구 분	목 적
ARM + sensinode	- ARM은 모바일 저전력 프로세서를 이용하여 Sensinode의 IoT 애플리케이션을 기반으로 다양한 서비스 제공
Google + nest	- Google은 nest의 스마트홈 HW를 기반으로 독자적인 스마트홈 플랫폼 구축 추진
SAMSUNG + SmartThings	- 삼성은 SmartThings의 개방형 스마트홈 플랫폼을 활용하여 자사의 스마트홈 서비스를 강화

< IoT 기술 선점을 위한 Alliance 현황 >

구 분	설립 목적	회원사
OPEN INTERCONNECT CONSORTIUM (OIC 컨소시엄)	운영체제와 서비스 공급자가 달라도 기기 간 정보관리 및 무선공유가 가능하도록 업계 표준 기술에 기반을 둔 공통 운영체계 규정	(인텔, 브로드컴, 삼성, 델, 윈드리버, 아트멜 등)
THREAD GROUP (쓰레드 그룹)	스마트홈을 위한 새로운 IP기반 무선 네트워킹 프로토콜 스레드(Thread)를 개발해 일반 가정에 보급	7개 회원사 (네스트, 삼성, ARM, 프리스케일, 예일 등)
ALLSEEN ALLIANCE (올씬 얼라이언스)	기술 또는 통신 프로토콜과 관계없이 기기가 스스로 주변 제품을 발견해 상호 작용할 수 있도록 지원	80개 회원사 (퀄컴, LG, 샤프, MS, 소니, 보쉬, 파나소닉, 하이얼 등)

2 IoT 환경 도래에 따른 정보보호 패러다임 변화

□ 스마트홈, 스마트의료, 스마트카 등 IoT 서비스가 일상생활로 확산되면서 기존 **사이버세계의 위험이 현실세계로 전이(轉移)·확대**

□ 기존 PC, 모바일기기 중심의 사이버환경과 달리 IoT 환경은 보호대상, 주체, 방법 등에 있어 **새로운 정보보호 패러다임**으로 접근 필요

o 모든 사물간 상호연결이 심화되면서 이에 따른 보안위협 역시 크게 증가하므로, 제품·서비스의 **기획·설계단계부터 정보보호를 고려**

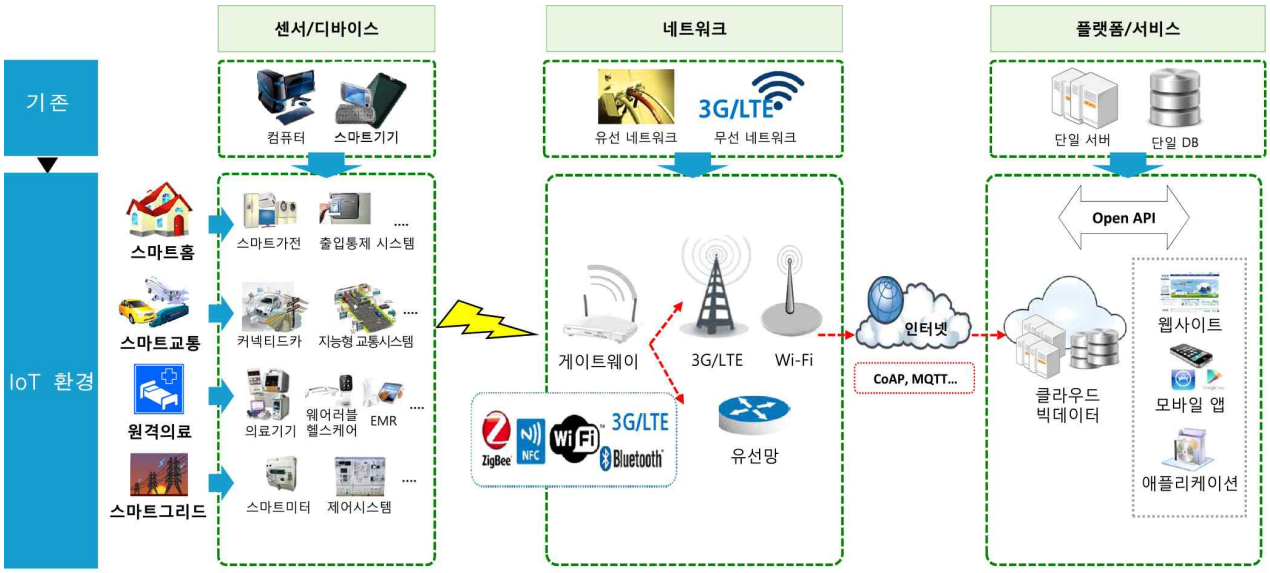
o 보호해야할 기기의 수가 우리 일상생활의 모든 사물로 확대되고, 그 특성도 다양화(경량·저전력, 초연결성 등) 되면서 **기존 보안기술 적용*에 한계**

* 경량 암호·인증 및 이기종 네트워크 보안관리, 프라이버시 보호 등 맞춤형 보안기술 요구

o 다양한 분야에 IoT 응용서비스가 도입·적용되면서, 기존 제조업·서비스업 등 **全산업분야에서 정보보호를 기본화**(基本化)할 필요

구 분	As-Is	To-Be
보호 대상	PC, 모바일 기기	**가전, 자동차, 의료기기 등 우리 주변 모든 사물(Things)**
대상의 특성	고성능, 고가용성을 가지는 운영환경	고성능, 고가용성 **+ 초경량, 저전력**
보안 주체	ISP, 보안 전문업체, 이용자	ISP, 보안 전문업체, 이용자 **+ 제조사, 서비스제공자**
보호 방법	별도의 보안장비, S/W 구현 및 연동	별도의 보안장비, S/W 구현 및 연동 **+ 설계단계부터 사물 내 보안 내재화**
피해 범위	정보유출, 금전피해	정보유출, 금전피해 **+ 시스템 정지, 생명위협**

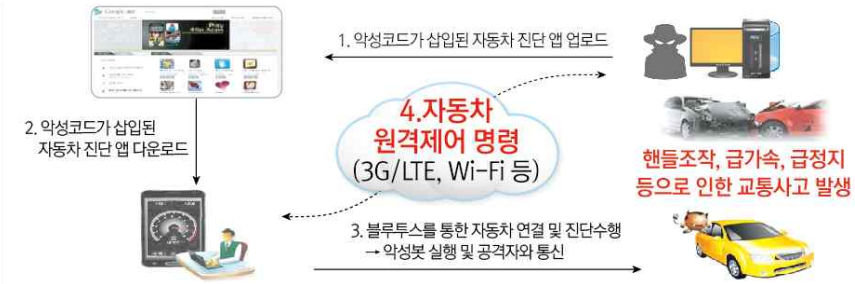
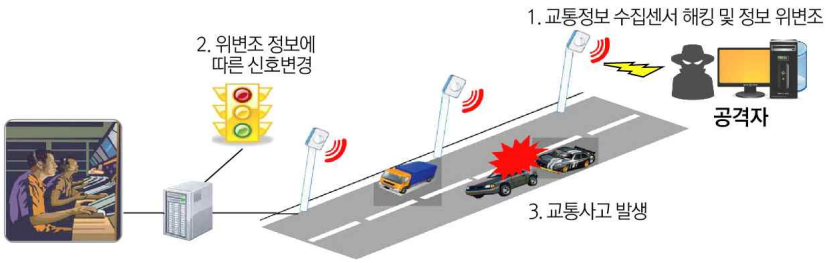
참고 IoT 적용에 따른 보안위협과 보안 요구사항



< 디바이스 > < 네트워크 > < 플랫폼/서비스 >

	< 디바이스 >	< 네트워크 >	< 플랫폼/서비스 >
기존	○**(PC, 모바일)** 네트워크에 연결된 PC, 모바일 제품에 대해 백신 등 개인 차원의 보안과 IPS 등 조직 차원의 보안 실행 ○**(폐쇄형 제품)** 가전제품, 의료기기, 자동차 등은 네트워크에 접속되지 않고, 개별적으로 사용	○**(네트워크 안전성)** PC 등은 유선 네트워크 사용하고, 무선 네트워크를 사용하는 모바일 스마트 기기 등은 상대적으로 안전한 3G/LTE 망 사용 ○**(네트워크 공격 예방□대응)** 악성코드에 감염된 좀비 PC들을 통한 DDoS(트래픽 폭증) 공격을 예방 · 대응하기 위해 좀비 PC 치료 체계, DDoS 대응장비 이용	○**(보안이 고려된 플랫폼 사용)** 인터넷 상에서 중요 정보는 암호화된 통신을 사용할 수 있도록 하고, 공인인증 등 인증 수단이 마련되어 있음 ○**(개인정보 관리)** 개인정보를 수집 관리하는 서비스제공자에게는 개인정보 관리 의무가 부여되고, 개인정보 노출 등에 대해 모니터링이 진행
IoT 이후 보안위협	⇨**(저사양 디바이스 해킹)** 디바이스들이 다양화되고, 종류가 늘어나면서 저사양 기기 사용이 늘어나고, 현재 보안 기술로는 저사양(메모리, CPU, 전력 등) 기기에 백신, 암호화, 인증 등 보안을 적용하기 곤란한 경우가 많음 ⇨**(디바이스 관리 취약점 증가)** 디바이스 수가 많아지고, 보안패치 적용 곤란, 통신 내용 모니터링 곤란에 따른 보안 취약성이 증가	⇨**(무선 네트워크 취약점)** Zigbee, Wi-fi, Bluetooth 등 이종 무선 네트워크간 상호연동이 되면서, 일정한 보안수준을 유지하기 어렵고, 디바이스간 통신이 지원되면서, 디바이스 인증이 제한적으로 지원 ⇨**(네트워크 트래픽 공격량 급증)** 클라우드 가상화 서비스를 통한 좀비 PC 대량 생산, 냉장고, 청소로봇, 의료기기 등 대규모 디바이스에 악성코드를 감염시켜 트래픽 폭증 공격 가능	⇨**(공개 플랫폼의 취약점)** 공개 플랫폼을 통한 기기-서비스간 허위 데이터 전송/오작동 등 공격 ⇨**(사용자 신원정보 유출/추적)** IoT 디바이스가 수집한 단편 정보의 중앙 집중 및 조합으로 사용자 신원정보 유출
보안요구사항	▷**(저사양 디바이스 보안기술)** 저사양 기기를 포함해 다양한 기기 특성을 반영한 경량 보안 기술(백신, 암호화, 인증 등) 개발 및 적용 ▷**(디바이스 관리 기술 개발)** 기기 운영 신뢰성 보장, 무결성 검증 등을 위해 센서/디바이스 보안패치 적용 기술 개발, 센서/디바이스 모니터링 체계 마련	▷**(네트워크 장비 모니터링)** 이중망 연동을 위한 프로토콜 상호운용성 기준 마련, 이기종 저사양 연결 통신 네트워크 환경에 적합한 보안기술 필요 ▷**(네트워크 장비 모니터링)** 대규모 기기 · 네트워크에 대한 보안 상태 모니터링 및 감시 필요	▷**(상호인증 키관리/신뢰관리)** 안전한 개방형 플랫폼 이용지침 마련, 디바이스/사용자 서비스 간 상호 인증 및 키관리, 신뢰 관리 필요 ▷**(개인정보 수집 제어)** 기기의 개인정보 수집/추적 방지 및 개인식별 정보 필터링 기술 필요

참고 IoT 서비스 환경에서 발생 가능한 보안위협 시나리오

시나리오		주요 내용
1	악성코드가 감염된 차량진단 앱을 통한 자동차 원격제어	
2	심박기 신호정보 위·변조를 통한 전류량 과잉공급	
3	홈서버 해킹을 통한 댁내 가스밸브 원격개방	
4	교통정보 수집 센서 해킹을 통한 신호제어	
5	기내 와이파이를 통한 악성코드 감염 및 항공기 제어시스템 오동작 유발	

Ⅲ IoT 정보보호 현황

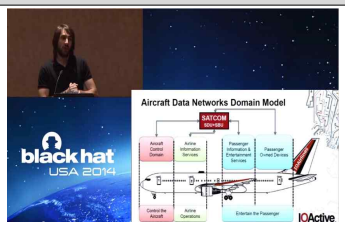
1 IoT 사업자 보안 동향

□ **(제조업)** 가전, 자동차 등 기존 제조업에 IoT가 적용되는 과정에서 **보안을 고려되지 않은 제품이 출시**되는 등 다양한 취약점이 노출

o 기업의 자체적인 보안인력 및 기술, 노력 등이 상대적으로 부족한 제조사는 IoT 제품·서비스 개발·보급에만 집중

※ 블랙햇(BlackHat) 2014에서는 IoT 기기(자동차, 항공기, 가전, 의료 등)에 대한 해킹 시연 및 취약점을 제시하고, IoT가 보안문제가 해결되지 않고는 이용 확산이 불가능함을 시사

< BlackHat 2014('14.8) 주요 해킹 시연 >

스마트카	스마트홈	항공기
		
자동차의 블루투스와 텔레매틱스, 차내 전화 애플리케이션 등 원격 네트워크의 취약점을 악용한 해킹 시연	네스트 스마트홈 디바이스의 보안 기능을 우회하여 댁내 주요설비의 원격제어 및 감시 시연	항공기의 위성통신시스템 해킹을 통한 항공기 네비게이션, 보안시스템 비인가 접근 해킹 시연

□ **(ICT 분야)** 보안기술을 탑재한 IoT 제품·서비스를 출시하거나, IoT에 특화된 보안 기술을 개발 중

구 분	내 용
삼성	미래기술육성사업으로 IoT 보안 연구과제(4개)를 선정하여 추진('14) · 선정과제 : IoT를 위한 안전한 게이트웨이, IoT 기반의 차량 보안, 신규 난제기반 경량 공개키 암호기술, 보안 및 개인정보보호를 위한 상황인지형 통합 IoT 플랫폼
Verizon	클라우드 기반의 IoT 기기 식별·인증, 통신 데이터 보호를 위한 보안솔루션 MCS(Managed Certificate Services) 개발
Cisco	IoE 환경에 필요한 인증, 권한관리 및 접근제어, 강제화된 네트워크 정책 등으로 구성된 보안 프레임워크 제안
WindRiver	모듈단위의 재구성이 가능한 IoT 전용 보안 운영체제 VxWorks 7 개발('14)

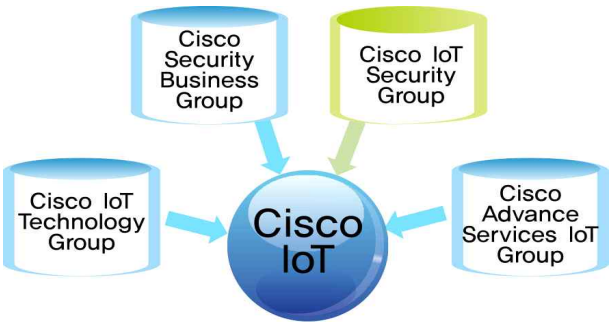
o 인텔, IBM, Cisco 등 글로벌 ICT 기업들은 IoT 보안 경쟁력 확보를 위하여 보안 전문업체 인수·합병을 경쟁적으로 추진

구 분	내 용
Cisco	셋톱박스 보안업체 NDS 인수('12), 차세대 네트워크 보안업체 SourceFire('13), 악성코드 분석업체 ThreatGrid('14)를 인수함으로써 IoT(디지털콘텐츠, 스마트홈 등) 사업의 보안역량 강화
인텔	맥아피(McAfee) 인수를 통해 IoT 게이트웨이에 기기의 신뢰성 및 무결성 보장, 데이터 보호를 수행하는 보안 솔루션 탑재('14)
IBM	클라우드 보안업체 라이트하우스, 크로스아이디어스를 연이어 인수함으로써 IoT 서비스 및 SW에서 보안 리더십 강화('14)
GE	사이버보안 전문회사 월드테크(Wurldtech)를 인수해 정유시설, 전력망, 의료기기 등에 대한 보안 강화('14)

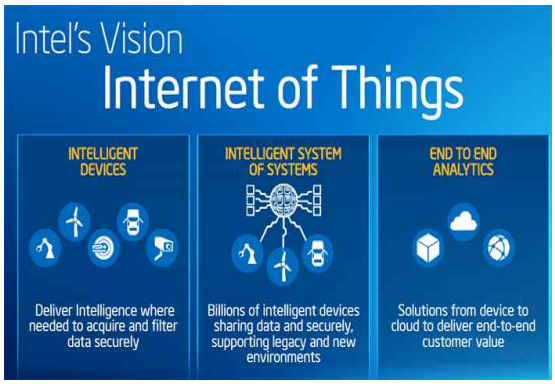
< Cisco의 IoT 보안 전담부서 >

o Cisco는 NDS 인수를 통해 자사의 IoT 보안 전담부서 SPVSS를 설립하였으며, IoT 디바이스, 소프트웨어, 시스템 보안 업무를 담당

o SPVSS는 IoT 디바이스 보호를 위한 개방형 IoT 보안플랫폼 개발을 진행 중



< Intel Security(McAfee)의 IoT 보안 >



< Intel의 IoT 전략 >

< Intel의 IoT Gateway Solutions >

2 주요국 IoT 보안 및 표준화 동향

□ (정부) 미국, 유럽 등 전세계적으로 IoT 보안정책 수립은 초기 단계

o 주요 선진국은 **IoT 산업진흥과 이용자 보호**를 함께 고려한 **균형잡힌 규제방안**을 정부 차원에서 검토 중

- IoT 기반의 다양한 서비스에 보안원칙 적용 및 지침 개발·보급 등 **시장 자율규제 중심**의 정보보호 정책·제도 수립
- 다만, **인간의 생명과 직결**되는 의료 등의 분야에서는 **의무적으로 보안을 적용**

구 분	내 용
유럽(EU)	시장 자율규제 중심(가이드, 권고 등)의 IoT 보안 정책 수립·이행 추진('13)
미국 (FTC)	TrendNet社 IP카메라 해킹으로 사생활 침해 우려가 고조됨에 따라, 관련 지침 마련을 위한 공공-민간 전문가 의견수렴('14.1)
미국 (FDA)	FDA가 제시한 보안지침을 준수하지 않는 의료기기들은 미국 내에서 판매 및 유통이 금지됨('13)

o IoT 인프라(CPS)에 대한 사이버공격으로 인한 셧다운, 오동작 등의 침해사고를 **선제적으로 예방·대응하기 위한 보안정책** 추진

※ 美 백악관은 주요 기반시설에 대한 사이버 공격으로 사회적·경제적 피해가 우려됨에 따라 CPS의 사이버보안 강화를 위한 대통령 행정명령 발동('13)

o 전세계적으로 IoT 보안기술의 주도권 확보를 위해 범국가적 차원의 IoT 보안기술 **R&D 및 시험·인증 환경**을 구축

구 분	내 용
유럽(EU)	IERC(European Research Cluster on the Internet of Things)의 AC(Activity Chain)5를 통해 FP7 프로젝트(인증·암호화 기술, 주요 위험요인 분석 등) IoT 보안의 연구과제를 수행(~'13)
미국 (NIST)	안전하고 신뢰할 수 있는 IoT 환경을 조성하기 위해 다양한 분야(교통, 에너지, 제조, 의료 등)의 IoT 기술, 테스트베드 연동시험을 위한 'Smart America Challenge' 프로젝트 진행('14)
중국	'IoT 발전의 10개 전문 행동계획('13~15)'을 통해 IoT 핵심 보안기술 개발, IoT 보안 테스트 평가 플랫폼 구축 등을 통한 보안능력 강화 추진('13)

□ **(표준화)** IoT 서비스 공통플랫폼 개발, 경량 인증·암호화 기술 표준화는 활발히 진행 중이며, **IoT 보안 요구사항에 대한 논의는 시작**되는 단계

o **(플랫폼)** 국내·외 표준기관 및 서비스 분야별 업체들을 중심으로 다양한 IoT 서비스 분야에 **공통으로 사용 가능한 플랫폼** 표준화 작업을 진행

구 분	내 용
oneM2M	자동차, 의료, 홈·가전, 전력 등 주요 IoT 서비스 간 호환성 확보를 위한 공통플랫폼 표준화를 추진 중이며, 인증, 암호화, 무결성 보장 등 보안 요구사항에 대한 논의도 함께 진행
ISO	IoT 작업반 ISO/IEC JTC1 WG7을 중심으로 IoT 구조 및 기기 플랫폼에 대한 표준화 진행 중

※ oneM2M : 韓·EU·美·日·中, 7개 표준기관, 267개 업체들을 중심으로 설립('12.7월)

o **(인증·암호화)** 전기·전자, 통신, 인터넷 등 다양한 분야의 표준화 단체는 IoT 환경에 적합한 **경량 인증·암호화 기술**에 대한 연구 추진

구 분	내 용
IETF	저전력·경량 기기를 위한 IoT 통신 프로토콜(CoAP) 및 보안 구조·모델 정의
ITU-T	IoT 보안 요구사항 및 경량 인증·암호화 기술을 IoT 통신 프로토콜(CoAP, MQTT 등)에 적용하는 방안 논의 중
ISO	IoT에 적용 가능한 경량암호 알고리즘(HIGHT, PRESENT)을 표준화
3GPP	SA3 그룹에서 이동통신 기반의 기기 간 안전한 통신을 위한 인증·암호화 표준화 작업 진행

※ CoAP(Constrained Application Protocol) : 저전력, 소형기기에 사용될 수 있는 경량형 웹 전송 프로토콜

※ MQTT(Message Queuing Telemetry Transport) : IBM에서 개발한 경량형 메시징 프로토콜로, OASIS에서 IoT 표준 프로토콜로 선정('13.4)

o **(IoT 보안 요구사항)** IoT 환경에서의 보안 요구사항을 정의하는 표준화 활동은 ITU-T, IETF 등 일부 표준화 단체를 중심으로 논의 중

구 분	내 용
ITU-T	IoT 표준 참조모델을 통해 각 구성요소(애플리케이션, 네트워크, 디바이스)에서 고려되어야 할 보안 요구사항들을 키워드로 제시
IETF	CoRE 워킹그룹에서 IP기반의 IoT 서비스들을 위험수준에 따라 분류하고, 각각의 분류체계별로 고려되어야할 보안 요구사항들을 논의 중

3 IoT 보안환경 현황

□ **(제품·서비스 보안원칙 부재)** IoT 제품 및 서비스를 개발하는 제조사가 적용할 수 있는 **IoT 보안원칙 및 지침**이 없음

o IoT 공통 보안원칙(프레임워크) 또는 서비스별 보안 지침이 개발되어 있지 않고, 일부 **제한적으로 보안 가이드를 제시**하는 수준

※ 일본: 자동차 분야, 미국: 스마트 홈 단말기 분야, 한국: 의료기기 시스템 분야 등

□ **(정보보호 대응체계 고도화 필요)** IoT 정보보호 체계가 마련되지 않아 제품 및 서비스의 안전한 도입·운영과 침해사고 대응에 어려움

o IoT 환경에서는 홈·가전, 의료, 교통 등 다양한 분야의 침해사고에 대하여 **신속한 정보공유 및 대응이 어려움**

※ EC 조사결과, 응답자의 약 74%가 다수의 이해관계자들로 구성된 별도의 IoT 거버넌스 추진체계(platform)가 있어야한다고 응답(Report on the Public Consultation on IoT Governance, '13.1)

□ **(제도적 측면 검토 필요)** 현행 정보보호 법·제도는 IoT 환경의 특성을 반영하는데 한계가 존재함에 따라 해석 및 적용에 있어 **다양한 이슈를 야기**할 우려

o IoT 제품의 사후관리(SW 업데이트 등*) 및 결함 발생에 따른 **손해배상과 이용자가 알아야 할 보안정보****의 공개 방안 등 정립 필요

* 새로운 공격기술 발전에 따른 기존 IoT 제품의 신규 보안위협 등장

** 신규 보안취약점 발생에 따라 이용자는 보안 업데이트를 어떻게 할 것인지 등

o 현행법상 사물이 주체*가 되는 IoT 환경은 침해사고 발생에 따른 제도적 측면 검토 필요

* 사물이 자동화·지능화되어 사람의 개입이 없이 스스로 판단하고 정보를 처리하는 행위

4 IoT 보안기술 동향

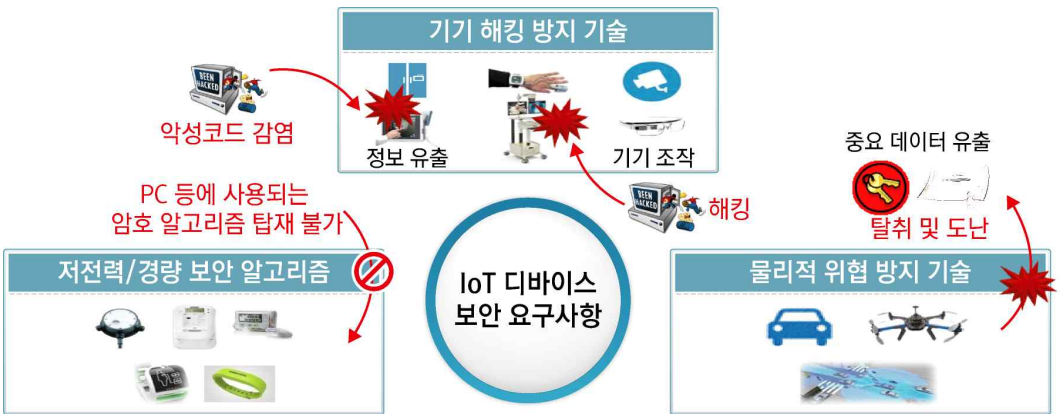
1 디바이스

□ **(보안 요구사항)** 드론, 센서 등 다양한 형태의 성능이 다른 IoT 기기별 **맞춤형 디바이스 보안기술** 필요

o CPU 성능, 메모리 크기, 소비전력 등의 제약을 갖는 IoT 기기에서는 기존 암호기술을 사용할 수 없으므로, 기기의 성능과 보안 강도를 고려한 **경량·저전력 암호기술** 필요

o 악성코드 감염 및 외부해킹으로 인한 **운영체제 위·변조 방지**와 디바이스 **정지·오작동을 방지**하는 기술 필요

o IoT 기기의 탈취·도난·해킹 등을 통한 **불법 복제 및 중요 데이터 유출을 방지**하기 위한 **하드웨어 보안 기술** 필요



□ **(현황·문제점)** 국외는 다양한 형태의 사물과 성능에 최적화된 IoT 디바이스 보안 기술이 개발되는 반면, 국내는 초기단계 수준

o 국내 LEA*, HIGHT**, 국외 PRESENT, KATAN 등의 경량형 암호가 개발되어 있으나 **부채널 공격*** 등 해킹에 취약**함

* LEA(Lightweight Encryption Algorithm) : '12년 국보연이 개발한 128비트 경량 블록암호

** HIGHT(HIGh security and light weigHT) : 64비트 저전력, 경량 블록암호 알고리즘

*** IoT 기기에서 발생하는 전자파와 전력소모량 등을 탐지·분석하여 암호키를 탈취

o Green-Hills 등에서는 가전, 금융 분야의 임베디드 운영체제를 개발하였으나, 경량암호 및 비인가 접근차단 등 **보안기능이 내재되어 있지 않음**

o 국외의 Silicon Labs, TI, Escrypt는 차량용 HW 보안모듈을 개발 중이며, 국내는 차량용 ECU간 암호통신 기술 개발 중

2 네트워크

□ **(보안 요구사항)** 이기종(異機種) 기기가 상호연결된 IoT 네트워크*를 대상으로 하는 해킹 및 악성코드 공격 등을 **탐지·차단하기 위한 네트워크 보안 기술** 필요

* 통신방식(ZigBee, Bluetooth, WiFi 등) 및 보안 특성(암호, 인증방식 등)이 서로 다른 기기·센서가 상호 연결된 네트워크

o 서로 다른기능을 수행하는 IoT 기기간 통합 네트워킹에 요구되는 단말 상호간 인증, 보안통신 및 접속제어 기능 필요

o IoT 네트워크에 접속한 기기와 보안기능이 상이한 게이트웨이로 구성된 IoT 서비스 환경에서 통합 해킹공격 탐지·대응

o 악성코드에 감염된 사물봇에 의한 트래픽 폭증 공격(DDoS)을 방지하기 위한 네트워크 모니터링·관리 기술 필요

※ 사물봇: 악성코드에 감염된 좀비 사물(냉장고, 토스터기 등)들의 집합

□ **(현황·문제점)** IoT 네트워크에 대한 침입차단, 안전한 연결성을 제공하기 위한 IoT 보안게이트웨이, 사물봇 공격방지 기술 등은 아직 연구 초기단계

o Intel, Freescale, Eurotech등에서 IoT 게이트웨이를 개발하였으나, IoT 네트워크 및 기기의 보안관리(실시간 보안 모니터링, 침입탐지 등) 기능은 미적용

o 자원 제약형 IoT 기기의 악성코드 감염 여부를 원격에서 검증하고 사물봇 공격을 탐지·대응하는 기술은 연구 초기 단계

3 플랫폼/서비스

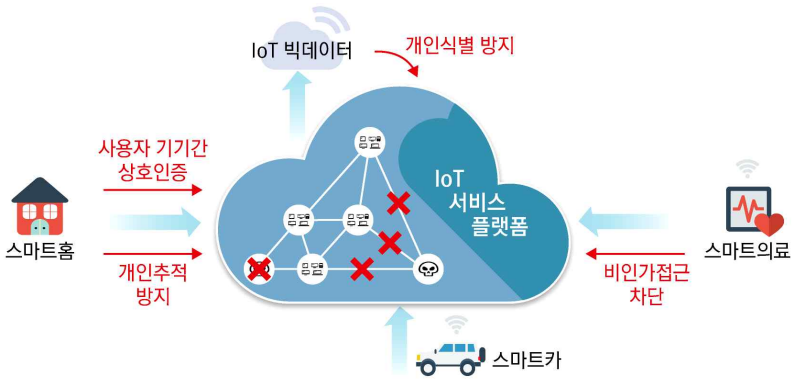
□ **(보안 요구사항)** IoT 서비스 구성 요소(기기, 사용자, 서비스)간 상호 인증, 접근제어 및 프라이버시(위치, ID, 데이터) 보호 기능 제공 필요

o 위장 사물, 기능이 변조된 사물 등의 서비스 비인가 접속을 차단하기 위한 기기 간 인증, 키 관리 및 접근제어 기능 필요

o IoT 환경에서 데이터 수집·분석에 의한 프라이버시 침해(개인식별, 추적)를 방지하기 위한 기술 필요

o IoT 서비스 특성(홈·가전, 의료, 교통 등)과 동작환경(임베디드, 웨어러블, 모바일 등)에 특화된 보안 플랫폼* 필요

* 여러 IoT 서비스가 혼재되어 동작(예: 자동차에서 홈·가전 및 의료서비스 접속)하는 경우, 비용 효율화를 위해 공통기능과 특화기능을 연계한 통합플랫폼 필요



□ **(현황·문제점)** 개방형 IoT 서비스 환경에서 기기인증, 부인방지 및 프라이버시 보호를 위한 국내 서비스보안 플랫폼의 기술수준 미흡

o 미국은 차량간무선통신(V2X)에서 차량간 인증 및 프라이버시(위치정보 등) 보호를 위한 VPKI(Vehicle Public-Key Infrastructure) 기술 개발

o 국내에서 토큰기반 기기 인증 및 접근제어 기능을 제공하는 수준의 IoT 사물 및 서비스 검색 플랫폼(Mobius) 개발

5 IoT/CPS 보안 산업 현황

□ **(보안업체)** IoT 보안 시장 선점을 위해 인증 및 암호화 등 보안제품 위주로 개발 중이며, 대기업보다는 중소·벤처기업이 적극 추진 중

구 분		내 용
국외	Symantec	IoT 디바이스의 임베디드OS 모니터링, 침입탐지·차단, 접근통제 기능 등을 제공하는 Critical System Protection(CSP) 개발
	Trend Micro	브로드컴(Broadcom)과 협력하여 사이버위협을 예방하고, 사용하기 쉬운 홈게이트웨이 보안솔루션(Home Gateway Security Solution) 제공 추진('14)
	Mocana	경량형 IoT 디바이스에서 동작하는 임베디드 보안 솔루션 NanoBoot 개발·보급
	Infinion Technology	스마트홈, 공장 등 기밀 데이터를 저장하고 교환하는 다양한 커넥티드 시스템에서의 인증, 암호화 등을 지원하는 OPTIGA Trust P 솔루션 출시('14.4)
국내	시큐아이	IoT를 통한 정보유출, 해킹을 차단하기 위한 하드웨어 모듈, 경량/고속 암호화 알고리즘 적용 소프트웨어 모듈, 이를 탑재한 게이트웨이 및 센서 등 개발
	SGA	IoT 디바이스를 위한 임베디드 시스템 악성코드 탐지 및 차단 솔루션, 보안 운영체제(Secure OS) 등 개발 추진
	KTB 솔루션	담뱃갑보다 작은 크기에 가벼운 무게로 휴대성이 용이한 '웨어러블 방화벽(Wearable Firewall)'을 개발('14)
	인포뱅크	AutoSAR 국제표준에 기반한 차량 내 ECU 소프트웨어 보안 플랫폼 구축을 위한 연구개발 추진('14)

□ **(융합보안 인력 양성체계 미흡)** 홈·가전, 의료, 자동차 등 다양한 산업분야의 전문지식과 보안지식을 갖춘 융합보안 인력 부족

o 체계적인 IoT 융합보안 인재 양성을 위한 **다학제간*(대학교), 산업분야별 현장 종사자**(재직자)** 대상의 정보보호 교육과정 필요

* 다학제(전공 간 융합) 예시 : 건축+IT+보안, 자동차+IT+보안, 조선+IT+보안 등

* 비ICT 분야의 제조업(운송, 조선, 건설 등) 재직자의 경우, 제품·서비스 개발 시 정보보호에 대한 전문지식이 없이 단순한 보안기능 또는 기초 솔루션을 도입·적용하는 수준

◀ 시 사 점 ▶

○ 全산업분야에 IoT 제품·서비스가 확산되면서 침해사고 발생에 따른 경제적 피해는 물론 국민의 생명까지 위협하고 있으나, 이에 대한 대응체계가 부재(不在)

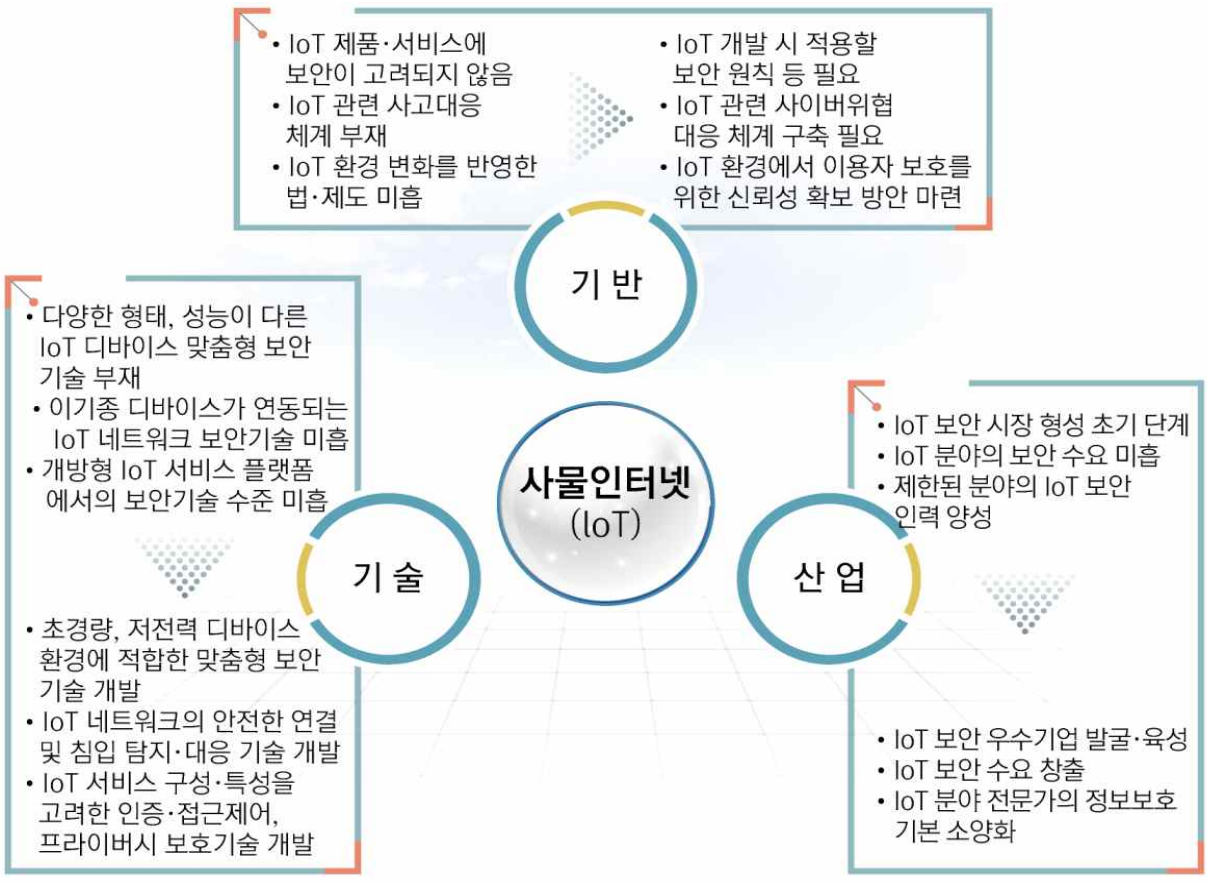
☞ **全산업분야에서 제품·서비스의 설계단계부터 보안을 내재화하고, 체계적인 사이버위협 대응체계 구축 등 IoT 보안 기반마련 필요**

○ 초경량·저전력 특성을 갖는 이기종기기간 상호연결이 심화되면서, 기존의 보안기술을 IoT 환경에 그대로 적용하기에는 어려움이 발생

⇒ **초경량·저전력 디바이스, 이기종 네트워크 연동 및 다중 사용자 이용 환경 등을 고려한 신규 IoT 보안기술 개발 필요**

○ 미국·EU 등 선진국과 글로벌 ICT 기업은 IoT 보안을 미래 성장을 위한 핵심 경쟁력으로 인식하고, R&D 투자 확대 및 전문인력 양성 등을 확대

⇒ **우수 IoT 보안 기업을 발굴·육성하여 글로벌 무대로 진출할 수 있도록 지원을 강화하고, 대학생 및 산업현장 종사자 등 IoT 보안 전문인력 양성 필요**

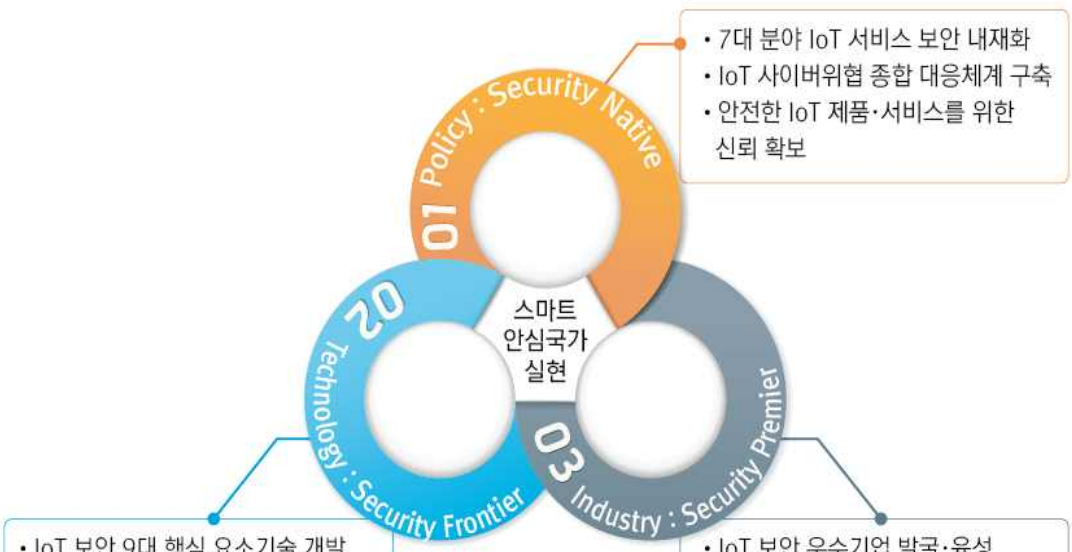


Ⅳ 비전 및 추진전략

비전	누구나 안전하게 사물인터넷의 편리함을 누리는 세계 최고의 스마트 안심국가 실현

추진전략			
	기반	Security Native	보안이 내재화된 IoT 기반 조성
	기술	Security Frontier	글로벌 IoT 보안 선도기술 개발
	산업	Security Premier	IoT 보안 산업경쟁력 강화

추진과제



Ⅴ 주요 추진과제

1 Security Native : 보안이 내재화된 IoT 기반 조성

◇ IoT 침해사고로 인해 **국민의 생명과 안전을 위협**할 수 있는 홈·가전, 의료, 자동차 등 **7대 산업분야에 보안 내재화(內在化) 추진**

1-1. 7대 분야 IoT 제품·서비스 보안 내재화

o **(Security-by-Design)** ICT와 융합되어 전 방위로 확산되는 산업분야별 IoT 서비스를 **홈·가전, 의료, 교통, 환경·재난, 제조, 건설, 에너지 등 7대 분야**로 분류하여 **공통 보안원칙**과 분야별 세부 **보안 고려사항 개발·보급**

< 7대 분야 보안 내재화 방안(예시) >

구 분		주요 내용
1단계 ('15년~)	홈·가전	홈게이트웨이, 공동주택단지서버, IoT 가전(로봇청소기, 지능형 냉장고 등)에 대한 외부비인가 접근 차단 및 오작동 방지 등
	의료 (식품)	심박기, 인슐린펌프 등 인간의 생명과 직결되는 의료기기의 비인가 원격제어 기능 차단 및 식료품 유통정보의 위·변조 방지기술 적용 등
	교통 (자동차·드론)	교통신호제어시스템(ITS), 철도제어시스템, 항공 제어시스템의 비인가 접근통제 및 데이터 위·변조 방지 등
2단계 ('16년~)	환경·재난*	산불감시, 홍수관리시스템, 문화재·재난관리시스템 등 오작동·중단 방지 및 데이터 보안
	제조(공장)	압력, 팬(fan) 기능 제어 등 산업제어시스템(ICS)에 탑재된 임베디드 S/W의 비인가접근 차단 및 데이터 위·변조 방지
	건설	IBS 빌딩의 엘리베이터, 전력공급, 출입문 개폐 등 제어시스템의 오작동·중단 방지 등
	에너지	스마트그리드 등 지능형 전력망 핵심요소의 데이터 위·변조 및 유출 방지

* 환경·재난 분야에 전자정부 관련 IoT 제품·서비스(안행부 별도 추진) 포함

- **(보안원칙 확립)** IoT 보안을 위한 **안전한 구조설계 및 개발, 공급망(Supply Chain) 안전 확보**를 위한 **3대 공통 보안원칙** 제시('15년~)

< 3대 IoT 보안원칙 >

① **(안전한 구조설계)** IoT 서비스의 지속적인 보안수준을 유지하고 침해사고 위험의 도미노적 전이·확산 방지를 위한 **보안 아키텍처(Secure Architecture)** 확립

- 보호되어야할 핵심자산과 위협을 식별하고, 현재의 보안수준을 평가하여 위협에 대응하기 위한 정책 수립, 보안시스템 구성·운영

※ 지능형건축물(IBS), 발전소 등 침해사고 발생 시 **시스템 중단 또는 오동작**에 의해 큰 피해가 예상되는 **제어·구동시설 및 다중이용 시설** 등에 우선 적용

② **(핵심요소의 안전한 개발)** IoT 서비스의 안정적인 운영을 위한 핵심요소(제어시스템, 구동·통신시스템 등)에 **보안기술 적용 및 보안품질 보증**

- IoT 소프트웨어 개발 과정에서 보안취약점 제거를 위해 **시큐어 코딩** 적용
- 소형화, 저전력의 IoT 디바이스, 네트워크 환경에 적합한 **경량 인증/암호화 기술** 적용
- IoT 시스템 운영 중에 발생할 수 있는 보안결함 및 해킹위협으로부터 시스템을 보호하기 위한 접근통제, 침입탐지 등 **임베디드 보안기술** 적용
- IoT H/W, S/W의 **보안품질 보증(Security Quality Assurance)** 적용

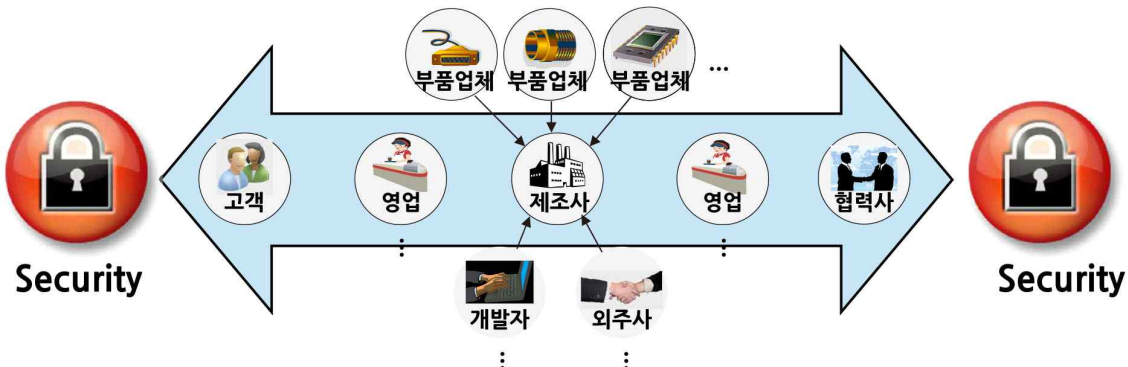
※ 개발 全 주기 내 보안 품질평가 프로세스(요구사항 정의 → 평가기준 마련 → 평가 → 피드백) 마련

※ 원자력, 수력, 화력 발전소, 자동차, 열차 등 24/7 무정지 상태를 유지해야하거나, 짧은 시간에 주변상황을 감지·처리하는 고가용성 디바이스 및 제어시스템에 우선 적용

③ **(공급망 안전 확보)** IoT 제품의 개발부터 유통·공급, 유지보수까지 **공급망(Supply Chain) 全 단계의 위험관리**를 위한 보안 관리체계 확립

- 제품의 무결성 보장, 유통이력의 식별·추적, 협력·공급업체·유지보수 업체관리 등

< 공급망 全단계 보안관리 >



- **(보안 고려사항)** 홈·가전, 의료, 교통 등 분야별 IoT 제품·서비스에 대한 최소한의 정보보호 요구사항을 제시하는 **보안 고려사항 개발·지원**('15년~)

※ 국민의 일상생활과 밀접하고 제품·서비스 출시 등 현재 상용화에 가장 앞선 3대 IoT 분야(홈·가전, 의료, 교통)에 우선 적용

< 3대 분야 서비스별 보안 고려사항(예시) >

서비스 유형		주요 내용
3대 분야	홈/가전	o 스마트홈/가전 기기는 출시전 보안취약점 점검을 의무적으로 실시하고, 출시 후에도 제조사는 지속적으로 보안패치 적용 및 배포 o 개인정보 저장·관리 또는 음성·영상 저장기능이 장착된 기기의 경우, 프라이버시 보호를 위한 사용자 인증 및 접근제어 기능 적용 o 원격제어 기능이 탑재된 스마트홈/가전 기기는 외부의 비인가 접근을 방지하기 위한 사용자 인증 및 암호화 통신 기능 적용 o 스마트홈 애플리케이션을 안전하게 사용할 수 있도록 지속적인 보안성 검증 및 업데이트 수행
	의료	o 개인정보, 질병정보를 저장·처리하는 의료장비 및 이와 연동되는 데이터 처리장치는 프라이버시 보호를 위한 인증 및 암호화 기능 적용 o 의료기기에 대해 정기적인 취약점 검증을 수행하고, 국제표준을 고려한 보안관리 체계 적용 o 의료기기 SW의 불법 위·변조 방지를 위해 유통망의 안전한 관리 o 스마트의료 서비스를 통해 수집·관리·공유되는 개인정보 보호방안 마련
	교통 (자동차)	o ABS, TPMS 등 자동차 주행 및 구동장치의 중단/오작동을 방지하기 위한 보안기능(데이터 암호화·복구, 비인가 접근통제 등)을 적용 o 전자제어시스템(ECU)과 연동된 각종 전자시스템은 정기적인 취약점 점검 및 보안패치 적용, SW 안전성 검사 수행 o 차량내부통신망(CAN)에 대한 암호화 통신 기능 적용 o 디지털 운행기록계(DTG, Digital Tachograph)를 통해 수집되는 정보의 안전한 저장·관리를 위해 ITS는 DB 보안기술 적용 o ITS의 차량검지센서 및 노변장치에서 전달되는 모든 교통 데이터는 암호화가 이루어져야 하며, 각 장치에 대한 인증기술 적용

1-2.「IoT 사이버위협 종합 대응체계」구축

o **(IoT 보안 협의체)** 정부와 IoT 제품·서비스 업체 및 보안업체 등이 참여하여, IoT 보안이슈 논의 및 기술자문 등을 수행하는 **민관 합동 「IoT 보안 협의체」** 구성·운영('15년~)

- IoT 보안 관련 법·제도 및 정책 논의, 이종 네트워크/플랫폼간 상호 호환성 및 기술표준 사항 협의 등

※ 상호 연결성이 심화된 사물인터넷 환경에서는 홈/가전, 의료, 교통 등 분야별 정보보호 관련 법·제도 및 정책, 규제, 표준사항 등이 서로 상이하므로 이를 통합적으로 논의하는 협의체가 필요

o **(IoT 인프라 보안강화)** IoT 서비스가 현실에서 **국가·사회경제 및 국민생활에** 밀접하게 접목된 **IoT 인프라***에 대한 **보호체계 강화**

* 열차집중제어장치, 홍수경보시스템, 전력계통운영시스템, 천연가스배관제어시스템 등

- 주요 IoT 인프라에 대한 침해사고 사전예방을 위한 **정기적 보안점검체계*** 마련('15년)

* 외부 보안전문가에 의한 정기적인 보안취약점 평가 및 모의해킹·훈련 실시 등

- 침해사고 발생시 **사회·경제적 파급력** 및 **국민생활 영향도** 등을 고려하여 주요 IoT 인프라를 **'주요정보통신기반시설'로 지정*** 추진('15년~)

*「정보통신기반보호법」 제8조에 따라 주요정보통신기반시설로 지정·보호

o **(IoT 취약점 분석·공유)** 홈/가전, 의료, 교통 등 분야별 IoT 제품·서비스 업체 및 보안업체, 관련부처 간 **보안취약점 공유·분석을** 위한 **'IoT-ISAC*' 구축**('15년~)

* 정보공유분석센터(Information Sharing Analysis Center)

- IoT 관련 보안위협 정보 및 침해사고 사례 등을 수집·분석하여 종합관리하고, 침해사고 발생시 **유관기관과 신속히 연계***

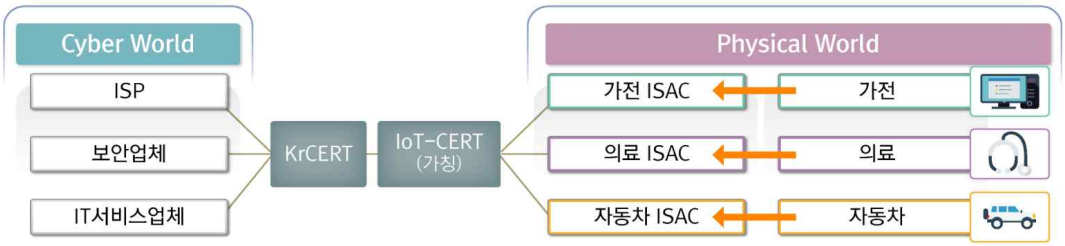
* 자동차 소유주 → 완성차 제조사/부품업체 → 자동차 ISAC(관계부처) → IoT-CERT

o **(사이버위협 종합대응 체계) 'IoT-ISAC'과 연계**하여 IoT 침해사고 예방·대응을 위한 「**IoT 사이버위협 종합 대응체계(IoT-CERT*)**」 단계적 구축·운영('16년~)

* 침해사고대응팀(Computer Emergency Response Team)

- 사이버세계 뿐만 아니라 IoT가 적용된 현실세계(스마트홈, 스마트의료, 스마트카 등)에서 발생 가능한 **보안위협 분석 및 모니터링, 침해사고 대응·복구 수행**

< IoT 사이버위협 종합대응 체계(안) >



1-3. 안전한 IoT 제품·서비스를 위한 신뢰성 확보

o **(IoT 제품·서비스 책임강화)** IoT 제품·서비스의 안전한 개발 및 유통·공급, 사후관리 등 **全단계에 걸쳐 책임성 확보**('16년~)

- IoT 제품·서비스의 **보안취약점** 및 이에 대한 **보호조치 사항**(SW 및 보안 업데이트 등)을 홈페이지 등을 통하여 **제품 사용자에게 공개 추진**

- IoT 제품·서비스 출시후 발견된 신규 보안취약점에 대해서는 **사후관리(보안업데이트) 등 지속적인 보안성 제공* 추진**

* IoT 제품·서비스는 특성상, 개발 또는 출시단계에서 예측하지 못한 신규 보안취약점이 발견될 수 있으므로, 제조사의 지속적인 사후관리가 필요

※ 미국은 '스마트홈 디바이스 보안가이드('13.7월)'에 IoT 제조사의 책임감 명시

<스마트홈 디바이스 보안가이드(美 US-CERT)>

1. **(지속적인 업그레이드 경로 마련)** 제조사는 제품의 패치 배포수단을 마련하고, 코드서명 기술을 적용하여 패치파일의 위·변조를 방지해야 한다.
2. **(IP 위·변조 검증)** 인터넷 연결기기는 외부로부터 유입되는 트래픽의 IP 출발지 주소가 위·변조되지 않도록 주소값 검증기술이 적용되어야 한다.
3. **(책임감) 제조사는 자사 제품의 보안문제에 대해 책임을 지고 이를 보완해야 한다.**

- 소비자가 IoT 제품·서비스 이용시 **결함에 따른 피해를 받은 경우**, 손해배상 등을 할 수 있는 **제도적 기반** 검토

o **(IoT 보안인증)** 소비자가 **안심하고 IoT 제품·서비스를 이용**할 수 있도록 보안성 검증·평가를 위한 **IoT 보안인증 도입** 검토·추진

- IoT 제조사 및 보안업계 등 **민간 주도의 IoT 보안인증**을 도입을 **적극 지원**하고 자율적인 **보안인증 활성화 기반*** 조성('15년~)

* 보안인증을 취득한 IoT 제품·서비스에 대하여 공공조달·구매 참여시 가점 부여 및 제조사에 대한 세제혜택 등 인센티브 부여 추진

- 향후, 시장성숙 단계에서 홈·가전, 의료, 교통 등 **각 부처 소관**으로 旣시행 중인 개별분야 **시험·평가·인증제도**에 **IoT 보안항목 및 기준 반영** 검토*('16년~)

* 각 분야별 IoT 제조사 및 보안업계, 관계부처와 공동으로 보안인증 방안을 마련하고, 시범운영을 거쳐 도입 추진

< 주요 산업분야별 인증제도 현황 >

< 3대 분야 보안 인증항목 적용 예시 >

o **홈/가전 분야 : '지능형 건축물 인증'**
- 홈게이트웨이 및 공동주택단지 서버를 통한 댁내망으로의 비인가 접근통제 및 사용자 인증, 승강기·도시가스·전력제어시스템의 정기적인 취약점 점검 등 보안 인증항목 신설

o **의료분야 : '보건제품 품질인증'**
- '전자의료기기 기준규격' 내 전자의료기기에서 발생 가능한 외부해킹 및 데이터 위·변조 방지, 보안패치 적용 등 기술적·관리적 보안항목 신설 등

o **자동차 분야 : '자동차 자기인증'**
- '자동차안전검사 세부기준'에 ECU 및 TPMS 등 전자제어시스템과 차량내부 통신 장비에 대한 비인가 접근통제 및 암호화 적용 항목 신설 등

- 인증기준이 없는 **새로운 유형의 IoT 제품·서비스**에 대해서는 신규 보안인증 항목 및 기준을 개발·적용한 **'IoT Security Verified 인증' 제도 시범운영**('17년~)

2 Security Frontier : 글로벌 IoT 보안 선도기술 개발

◇ IoT 제품·서비스를 안전하게 보호할 수 있는 **3계층**(디바이스, 네트워크, 서비스/플랫폼) **9대 핵심 원천기술 개발('시큐어Dome 프로젝트')**

2-1. 9대 IoT 보안 핵심기술 개발(시큐어Dome)

o **(디바이스Dome 기술)** IoT 기기(디바이스)의 크기(MCU, 메모리), CPU 성능, 전력상태 등을 고려한 경량·저전력 암호 모듈, HW 보안 SoC(System on Chip) 및 IoT 보안 운영체제 기술 개발

- 단기적으로 기존 암호기술을 **경량·저전력화**하고, 중·장기적으로 경량·저전력 신규 **암호 SW모듈**을 개발하여 IoT 기기 및 네트워크 플랫폼에 적용

※ 경량·저전력화를 위한 기존 암호는 AES, ARIA, SEED 등이고, 신규 개발 경량암호는 LEA, PRESENT 등

- **하드웨어(HW) 기반**의 경량·저전력 **암호 SW모듈을 개발**하여, 신체부착형 웨어러블 기기 및 초소형 센서 등에 대한 **위변조(ID) 및 부채널공격*을 방지**하는 **보안 SoC 개발**

* IoT 기기에서 발생하는 전자파와 전력소모량 등을 탐지·분석하여 암호키를 탈취

- 기기의 핵심 자원(운영체제, 개인정보 등)에 대한 비인가 접근차단 및 SW 위·변조 방지기능, 경량·저전력 암호모듈 등이 내재된 **보안 운영체제(Secure OS)** 개발*

  * 모듈형 보안 운영체제를 개발하여 스마트의료, 스마트카 등 인간의 안전과 직결되는 IoT 기기의 센서 및 게이트웨이 등에 재구성하여 우선 적용

o **(네크워크Dome 기술)** 이기종 기기가 상호 연결된 사물네트워크 환경에서 **실시간 이상징후를 탐지·대응**하는 보안기술 개발

- 신뢰/비신뢰 기기 및 이종 네트워크간 상호연결성(Bridge)과 보안 통신을 제공하는 **IoT 보안 게이트웨이*** 개발

  * IoT 서비스 분야(홈/가전, 의료, 교통 등) 별로 상이하게 요구되는 기기 간 연결 통신 방식(WAVE, IEEE11073, AllJoyn 등) 및 트래픽 특성을 고려한 보안 기능 제공

< 3대 분야 IoT 보안 게이트웨이(예시) >

o 스마트 홈/가전
- 이기종 홈기기간 상호연결 통신보안을 제공하고 사용자 프라이버시 보호를 위한 클라우드 연계형 홈 보안게이트웨이 개발

o 스마트의료 분야
- 해킹에 의한 의료기기의 오동작과 의료정보의 불법유출을 방지하는 침입방지시스템 및 텔레헬스케어 보안 게이트웨이 개발

o 스마트카 분야
- 스마트카의 내부 침입을 방지하는 임베디드 침입방지시스템 및 차량 내·외부의 V2X 통신 보안을 제공하는 보안 게이트웨이 개발

- IoT 기기와 네트워크의 물리적/행위적 이상징후를 탐지하여 실시간으로 대응하는 **클라우드 기반 IoT 침입탐지·대응 기술*** 개발

  * IoT 기기에 대한 공격과 오동작·결함을 클라우드에서 집중적으로 처리·분석·판단하여 동시 검출이 가능한 소프트웨어 정의 네트워크(SDN) 기반 동적 침입방지기술

- 무선기기의 보안상태를 원격 모니터링하여 보안SW, 규칙, 정책 등을 자동으로 업데이트(패치)하는 **IoT 원격 보안관리·관제 기술*** 개발

  * 빅데이터 분석 기반 대규모 악성 분산트래픽 공격을 탐지·대응하는 보안관제 기술

o **(서비스Dome 기술)** 웨어러블 등 IoT 서비스 환경에 적합한 인증·프라이버시 보호 및 IoT 서비스용 보안솔루션 개발

- 이용자의 생체 정보나 행위 패턴을 이용하여 사용자 인증과 기기의 접근 권한관리 기능을 제공하는 **스마트 인증 기술** 개발

※ IoT 네트워크 기기간 인증을 위한 확장성 있는 키분배 및 전통적인 PKI에서 벗어나 IoT 환경에 특화된 경량 PKI 기술 개발 필요

- 비정형 IoT 빅데이터를 실시간으로 분석하여 민감정보 노출 위험을 탐지·제거하는 **IoT 프라이버시 보호 기술** 개발

※ IoT 디바이스를 통한 이용자 위치 및 이용내역 추적을 방지하기 위해 익명화된 ID 기술을 적용하는 이용자 신원 및 위치정보 은닉 기술

- IoT 서비스 분야별 기술특성(프로토콜, 요구표준 등)을 고려한 적응형 **IoT 보안 솔루션*** 개발

* 스마트홈/가전 : 개인정보 및 프라이버시 보호를 위한 암호화, 스마트카 : 차량용 고속 보안통신, 스마트의료 : 고가용성·실시간성이 보장되는 접근제어 등

2-2. IoT R&D 오픈 이노베이션 구축

o **(IoT R&D 스피드 혁신)** 연구개발(R&D) 결과물의 성공적인 상용화를 위하여 홈/가전, 의료, 교통 등 7대 분야 IoT 실증사업을 통한 **R&D 결과물 시험·검증**

- 최종결과물 이전의 중간단계에서 R&D 결과물을 **실증사업에 적용**하여 **성능을 시험·검증**하고, 시장(Market)의 **요구사항을 재도출**한 후, **개발에 반영**하는 **R&D 스피드 체인*** **구축**('15년~)

* 기술개발 결과물 → 성능시험·검증(실증사업) → 시장 요구사항 재반영하는 'R&D 선순환 구조' 확립

- 경량·저전력 암호모듈 및 실시간 이상징후 탐지·대응, 스마트 인증 등 IoT 환경에서 **시급한 상용화가 요구되는 기술에 우선 적용**

< IoT R&D 스피드 체인 >

o **(IoT R&D 오디션 프로그램)** 빠르게 변화·진화하는 IoT 기술 및 시장 요구사항에 유연하게 대응하기 위한 **IoT R&D 오디션 프로그램** (경쟁형*/ 개방형**) 도입

* 동일 기술/주제로 다자간 연구개발 수행 후, 연차별 평가를 거쳐 한 곳을 선정하여 집중적인 연구개발 지원

** 연구개발 목표를 제시하여 先 연구개발 수행 후 결과물에 대한 평가를 거쳐 R&D 예산 지원

- 신규 경량·저전력 암호기술 등 **원천 기술개발 분야**를 대상으로 **'모험과제' 형식**으로 **우선적으로 추진**

o **(글로벌 R&D 역량 강화)** 미국, 유럽 등 IoT 보안 선도기술 및 실용화 기술 보유기관 등 **국제협력**을 통한 **IoT 보안 글로벌 R&D 역량** 강화

- 미국, 유럽 등 각국의 강점을 이용한 **국제공동연구 추진**('15년~)

※ 미국은 클라우드, 무선 센서네트워크 등 네트워크 보안 분야에서, 유럽은 제어시스템, 차량통신 등 산업보안 분야에서 강점을 보유

o **(IoT 보안 표준화)** 홈·가전, 교통, 의료 등 IoT 서비스 분야별 시장 수요와 기술 경쟁력을 고려하여 **IoT 보안기술의 국제 표준화**('15년~)

- 특히, IoT 기기간 인증, 경량·저전력, 보안통신 기술 등 **원천기술 개발**을 통한 **국제표준(IPR) 확보**(ISO, ITU-T, ETSI 등) 및 **표준화 연구과제(R&D) 기획·추진**

< IoT R&D 국제공동연구 후보기관 >

구 분	협력 기관	IoT 보안분야별 보유 기술
미국	퍼듀대	'98년 설립된 CERIAS(Center for Education and Research in Information Assurance and Security)를 중심으로 **CPS보안 및 무선 센서네트워크 보안 프로토콜** 연구 중
	로체스터공대	'13년 미국 내 전국 해킹방어대회 우승한 대학으로 해킹 테스트베드 센터 보유하고 있으며, **클라우드 기반 모바일 악성코드 분석 기술** 관련 강점 보유
	UCLA CENS	UCLA의 CENS(Center for Embedded Networked Sensing)에서는 **센서 원천기술 및 해양, 로봇, 오염도 측정, 지진 감지** 등 다양한 산업에 특화된 센서 기술에 대한 강점 보유
유럽	퀸즈대	영국 보안기술 플래그십 센터인 CSIT(Centre for Secure Information Technologies)을 중심으로 **제어시스템 및 IoT용 암호 엔지니어링 분야**의 연구를 수행 중임
	워릭대	영국 Warwick大의 산업기술연구센터로써, 영국내 차량 산업체와 공동연구를 진행하는 독보적인 차량-IT융합 연구기관임. 커넥티드 자동차가 주 연구분야이며, **차량통신보안 연구**에 강점 보유
	옥스포드대	업계, 연구기관 등과 함께 다양한 보안 프로젝트를 진행하고 있는 **Cyber Security Center**(Oxford대)는 홈네트워크, 스마트그리드, 클라우드 등 **산업보안 분야 연구**에 강점 보유

3 Security Premier : IoT 보안 산업경쟁력 강화

◇ 창의적 **아이디어 발굴·육성 및 실증사업**을 통해 **IoT 보안전문기업**을 육성하고, **다학제간 연계**를 통한 **융합보안 인력 양성** 추진

3-1. IoT 보안 우수기업 발굴 및 융합보안 실증 추진

o **(IoT 보안 Startup 기업 지원)** 창의적인 **보안 아이디어를 보유**한 개인과 기업을 **발굴·육성**하여 **창업 및 성장**을 적극 지원('15년~)

- 창의적인 보안기술 및 서비스 모델 발굴을 위한 **'IoT Security Innovation Contest'** 개최* 추진('15년~)

* IoT 제품·서비스의 취약점 해결을 위한 아이디어, 보안기술 및 서비스 등 발굴

- IoT 보안 중소·벤처기업 대상 창업지원 교육, 정보보호 전문심화 교육 등을 위한 **전문가 멘토링* 및 기업간 파트너십**** 제공

* 전문가 멘토링을 통한 IoT 제품·서비스 및 보안교육, 창업·투자 교육 등
** 국내외 보안업체 및 글로벌 IoT기업과의 파트너쉽 프로그램 운영·지원 등

- IoT 보안제품·서비스의 **성능검증 및 시험환경 제공**을 위한 홈/가전·교통·의료 등 분야별 **IoT 보안 테스트베드 구축**

o **(IoT 융합보안 실증사업)** IoT 보안제품·서비스의 **상용화 및 시장진출을 견인**하기 위한 「**IoT 융합보안 실증사업**」 **추진**('15년~)

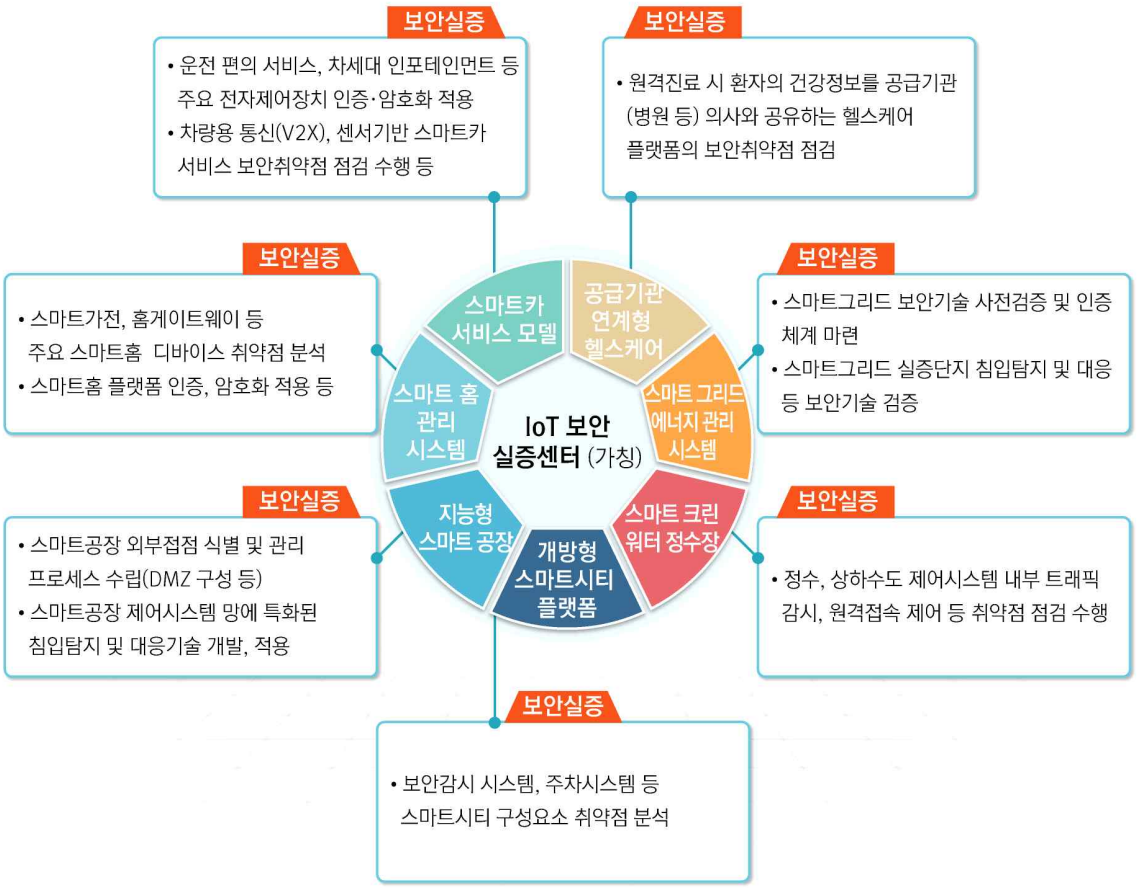
- 홈/가전, 의료, 교통 등 7대 IoT 분야의 주요 서비스(스마트홈, 스마트의료, 스마트카 등)에 대한 **취약점 점검 및 보안 컨설팅** 실시

- **부처별 IoT 실증사업**에 대한 정보보호 컨설팅 및 기술지원을 수행하는 **'IoT 보안 실증 지원센터*'** 구축·운영('15년~)

* IoT 실증사업 수행 시 보안컨설팅 및 보안제품·서비스 실제 적용 지원

- 홈/가전, 의료, 교통 등 IoT 제품·서비스 업체, 보안업체 및 정부가 **매칭펀드 방식**으로 **IoT 보안 시범사업** 추진('16년~)

< IoT 보안 실증 지원센터 구축안 >



3-2. IoT 보안제품·서비스 수요 창출

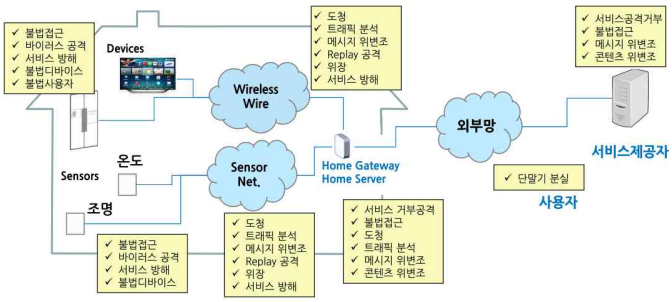
o **(IoT 보안취약점 발굴)** IoT 제품·서비스의 보안 취약점을 찾는 '解答 제시형 **버그바운티(취약점 신고포상제)' 도입**('15년~)

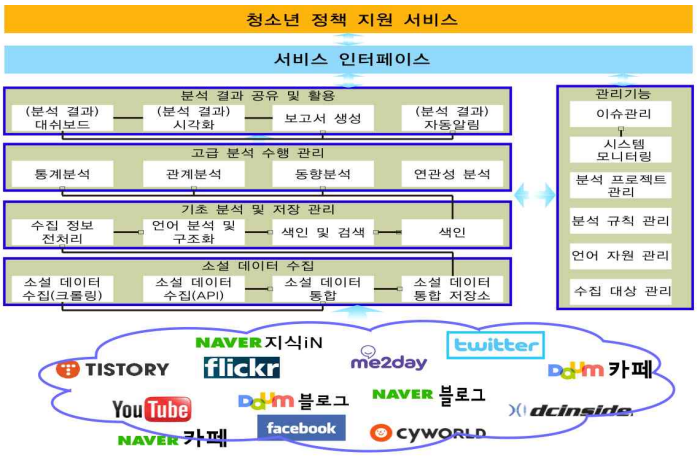
- 정부와 IoT 제품·서비스 업체의 공동 펀드방식으로 **취약점 신고자에게 포상금을 지급**하고, 우수내용은 **연구과제 기획을 통한 기술개발**까지 지원

o **(글로벌 IoT 보안수요 발굴)** **IoT 제조사(수요자)**와 **보안업체(공급자)간 기업매칭**을 지원하고, 보안 적용사례를 공유하는 **'IoT Security Networking Day'** 개최('15년~)

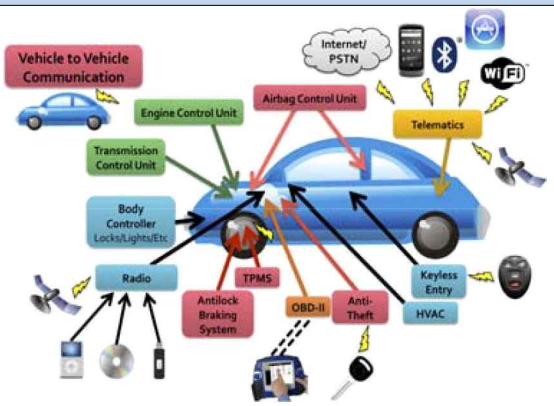
- **글로벌 전시회(CES, IFA 등) 참가 지원** 및 국제공동연구 참여 등을 통해 우수 IoT 보안업체의 **해외 보안수요 발굴 지원**('15년~)

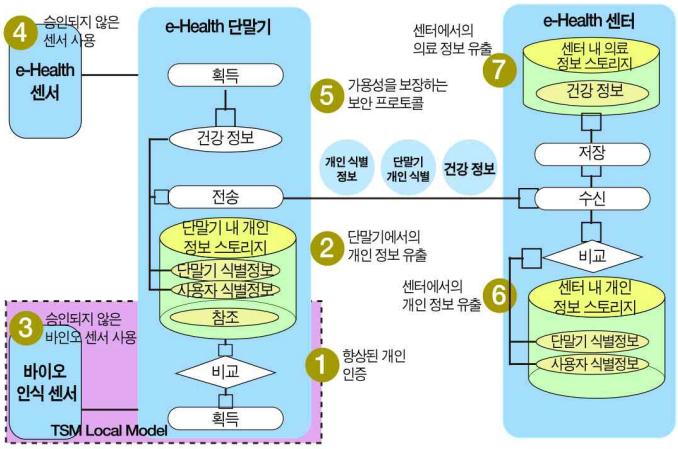
참고 IoT 실증사업별 보안위협 및 보안실증 예시

<table>
<tr><th colspan="2">주요내용</th><th>대응방안</th></tr>
<tr><td rowspan="2">(홈·가전)
1. 스마트 홈 관리 시스템</td><td> 

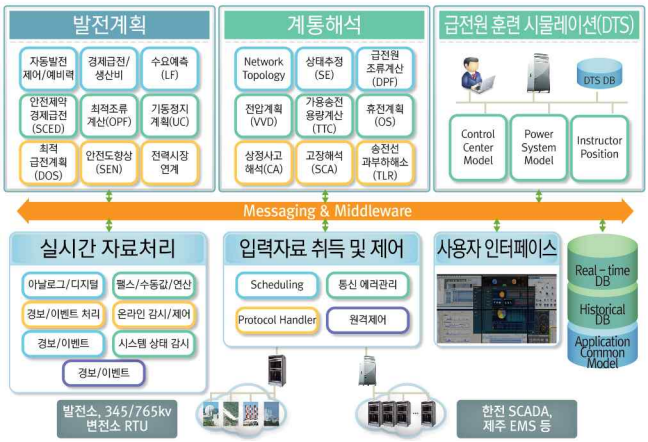
o 주요내용 : 홈센서 및 스마트 가전들이 유무선 네트워크로 연계된 스마트 홈 관리 시스템
o 보안위협 : 외부 인터넷과 연결된 스마트 가전의 취약점을 이용한 해킹 위협
- 카메라가 내장된 스마트 가전을 해킹하여 집 내부 감시 또는 온도 제어를 통한 물적·인적 피해 발생 가능</td><td>1) 온도, 습도 센서 등 저용량 디바이스에 대한 경량 암호화 기술 적용
2) 스마트 가전과 홈 게이트웨이 간 인증서 기반의 인증 체계 수립 및 적용
3) 스마트 가전에 대한 운영체제 업데이트 지침 수립
4) 스마트홈 네트워크 보안 및 인증 기술 개발을 통한 다중 보안 시스템 개발, 적용
5) 스마트홈 관리 시스템에 대한 내부 연결 네트워크 감시 체계 구축</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 다양한 스마트홈 기기 및 서비스 연동을 위한 개방형 관리 시스템 및 실증 환경을 구축하여, 3G/4G, Wi-Fi 기반의 통합형 스마트홈 관리 시스템 모의해킹, 내부 디바이스 접속을 통한 스마트 가전 제어 등 취약점 점검 수행</td></tr>
<tr><td rowspan="2">(교육)
1-1. 위기 청소년 예측 및 대응 시스템</td><td> 

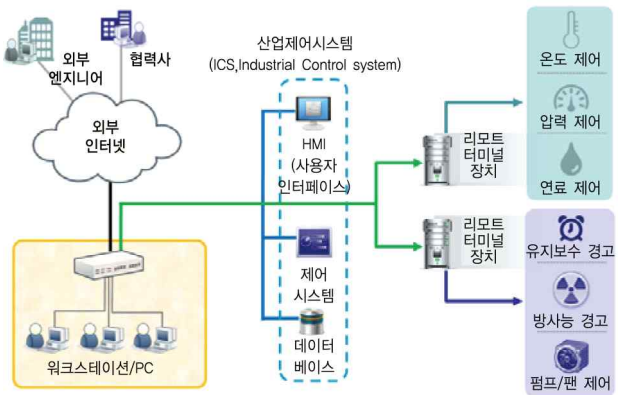
o 주요내용 : 위기 청소년 문제 발생의 실시간 대응을 위한 빅데이터 분석 기반 위기 청소년 예측 및 대응 시스템
o 보안위협 : 온라인으로 수집된 빅데이터 정보 유출
- 소셜 데이터 수집 및 저장 관리하는 DB의 접근 권한을 획득하여 위기 청소년에 대한 정보를 유출하거나 악의적으로 사용</td><td>1) 빅데이터 관리 DB에 대한 접근 통제 기술 개발 및 적용
2) 데이터 암호화 및 폐기에 대한 지침 마련 및 배포
3) 위기 청소년 예측 및 대응 시스템에 대한 외부 연결 네트워크 감시 체계 구축</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 소셜 데이터 수집 서버 및 빅데이터 분석시스템에 대한 보안 취약점 점검, 악의적인 쓰레기 정보 입력 필터링 여부 등 점검 수행</td></tr>
</table>

<table>
<tr><th colspan="2">주요내용</th><th>대응방안</th></tr>
<tr><td rowspan="2">(자동차)
2. 지능형 자동차 네트워크</td><td> 

o 주요내용 : 휴대용 기기의 무선통신을 통한 스마트카 제어 및 운행 효율성을 위한 지능형 자동차 네트워크
o 보안위협 : 다양한 컴퓨팅 시스템과 무선통신 인터페이스를 이용한 취약점 공격 위협
- 자동차에 연결된 휴대폰 등 디바이스, Bluetooth 통신 인터페이스 악용을 통해 차량 제어 및 조작 위협 가능</td><td>1) 스마트카 개발 단계에서의 보안 프로세스 수립 및 적용
2) 자동차에 적용되는 전자부품에 대한 자가인증제도 도입 및 운영
3) 운전자 식별정보, 주행정보 및 위치정보에 대한 보안 기술 개발 및 적용
4) 스마트카 디바이스 관리 통제 강화 지침 개발, 배포</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 차량용 통신(V2X) 및 스마트 센서 기반 스마트카 서비스 모델을 개발 및 실증하고, 차간거리·속도조절, 자율주행, 음성대화 등 운전편의 서비스 및 차세대 인포테인먼트 시스템 대상 인증우회, 데이터 위·변조로 인한 차량 오작동 등의 취약점 점검 수행</td></tr>
<tr><td rowspan="2">(의료)
3. 원격 의료시스템</td><td> 

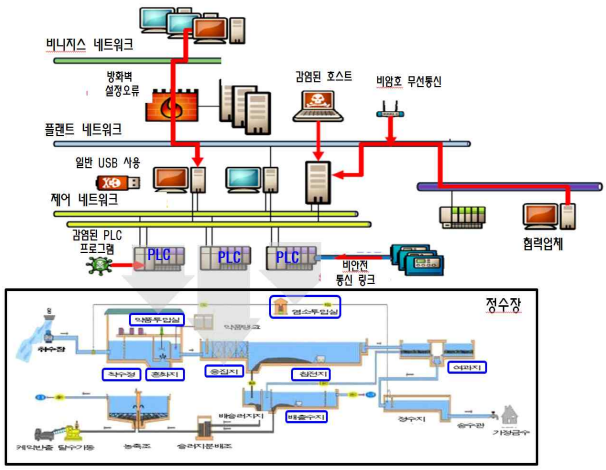
o 주요내용 : e-Health 센서, 유무선 네트워크를 활용하여 원격으로 질병 진단 및 치료가 가능한 원격의료시스템
o 보안위협 : 전자의료기기 및 네트워크 외부 침입 위협
- 스마트 의료 단말, 장비 및 바이오 센서 등과 연결된 서버에 대한 서비스 중단 또는 DB 정보유출 위협</td><td>1) 스마트 의료 센서에 대한 인증 표준 수립 및 적용
2) 전자의료기기 접속 인증 및 DB 암호화 프로토콜 개발 및 적용
3) 원격진료에 대한 위험평가 실시 및 의료기기 보안 시스템을 구축한 병원에 대한 지원 방안 마련
4) 의료 시스템 DB 접근 권한 통제 기술 개발
5) 환자 및 진료 데이터 암호화 및 폐기에 대한 지침 마련 및 배포</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 병원 등 수요기관과 의료기기업체 등 공급기관 연계형 헬스케어 실증단지를 조성하고, 원격의료시스템 및 환자 등의 건강정보를 수집·저장·분석하고 정보를 여러 병원의 의사와 공유하는 헬스케어 플랫폼의 민감 정보 유출 등 취약점 검증</td></tr>
</table>

<table>
<tr><th colspan="2">주요내용</th><th>대응방안</th></tr>
<tr><td rowspan="2">(에너지)
4. 에너지 관리시스템/ 스마트그리드</td><td> 

o 주요내용 : 지역별로 본사와 지사로 나뉘어 있는 에너지 인프라를 관리하기 위한 에너지 관리 시스템
o 보안위협 : 에너지 관리 시스템 네트워크와 외부 접점 취약점
- 기업 단위 서비스를 위해 에너지 관리 시스템에 대한 기업 비즈니스 네트워크 연결 및 확장시 외부 공격 및 대량 트래픽 위협 가능성 존재</td><td>1) 본사 지사간 접점구간에 대한 웜, 바이러스 탐지 강화
2) 지사별 네트워크 모니터링 체계 구축 및 정보보호 지침 마련 및 배포
3) 전력 제어망 확장, 재구축시 네트워크 부하 테스트 실시 지침 마련
4) 네트워크 트래픽 계측을 위한 기준수립 및 점검 근거를 마련
5) 내부 인프라와 외부망 사이의 방화벽 및 DMZ 구성 지침 수립</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 에너지 관리시스템을 포함한 스마트 그리드 구현, 보안기술 사전검증 및 인증체계를 마련하고, 스마트 그리드 실증단지의 침입탐지 및 대응, 암호화, 장비·시스템 위변조 방지, 접근통제 등 보안기술 검증</td></tr>
<tr><td rowspan="2">(공장)
5. 산업 제어시스템</td><td> 

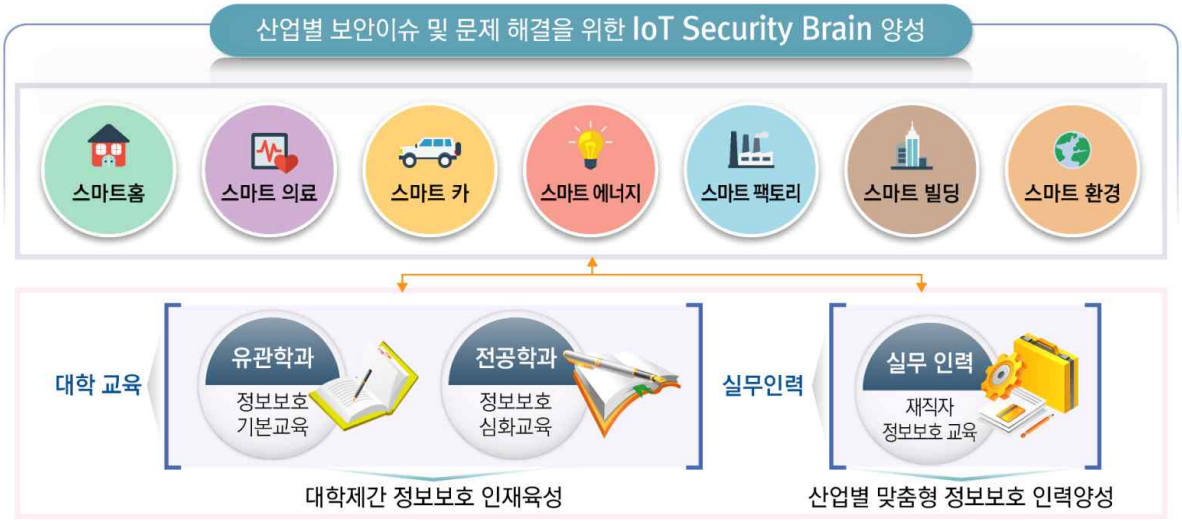
o 주요내용 : 국가 기반 시설 및 제품 생산 공장의 프로세스 및 설비 자동화를 위한 스마트 팩토리
o 보안위협 : 개방형 망구조 및 제어를 위한 무선 프로토콜 위협
- 자동화 시스템의 외부 원격제어를 통한 악의적인 오작동 유발 및 시스템 마비, 파괴를 통한 생산 중단</td><td>1) 스마트 팩토리의 외부 접점에 대한 식별 및 관리 프로세스 수립
2) 공장 업무망과 제어망 사이의 방화벽 및 DMZ 구성 지침 수립
3) 제어 시스템의 백도어로 사용될 수 있는 모든 매체에 대한 통제 지침 개발
4) 스마트 팩토리의 산업 제어 시스템 망에 특화된 이상징후 탐지 및 대응 기술 개발, 적용</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 원격 제어 및 생산이 가능한 미래 지능형 실증 공장을 구현하고, 산업 제어 시스템 및 빅데이터 기술을 이용한 생산/품질, 설비상태 점검 등을 수행하는 스마트 공장 플랫폼 대상 데이터 위·변조 등 취약점 점검</td></tr>
</table>

<table>
<tr><th colspan="2">주요내용</th><th>대응방안</th></tr>
<tr><td rowspan="2">(건설)
6. 건축물 e빌딩 케어 시스템</td><td> 

o 주요내용 : 건축물 점검, 생애이력 및 유지 관리의 자동화를 위한 건축물 e빌딩 케어 시스템
o 보안위협 : e빌딩 케어 시스템 접속 호스트에 대한 노출위협
- 모바일, PC 등 외부 관리 호스트에 대한 무단 접속을 통해 개인정보 탈취 및 건물 도면 유출, 설비 조작 가능성</td><td>1) 건축물 e빌딩 케어 시스템에 접속가능한 모든 매체에 대한 접근 통제 프로세스 수립
2) 건축물 e빌딩 케어 시스템 계정 및 데이터 접근에 대한 식별 기술 및 통제 기술 개발</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o IoT기반 개방형 스마트시티 플랫폼을 개발, 도시형 서비스 모델을 발굴 및 실증하고, 스마트 미터기, 건물 보안 감시 시스템, 주정차 지불시스템 등 스마트 시티 주요 구성 요소에 대한 취약점 분석</td></tr>
<tr><td rowspan="2">(환경)
7. 정수 및 상하수도 제어시스템</td><td> 

o 주요내용 : 오폐수 처리를 위한 정수 시설 및 수자원 공급의 설비 자동화를 위한 상하수도 제어 시스템
o 보안위협 : 정보수집 장치 연결지점을 통한 핵심 시스템 침입
- 비인가자에 의한 현장 정보수집 장치에 대한 네트워크 접속 통제 불가능으로 인한 오폐수 무단 방출 가능성</td><td>1) 산업용 방화벽 구축 및 단방향 데이터 전송 네트워크 및 내부 네트워크 트래픽 감시 프로세스 수립
2) 제어 명령 및 센서 전송값 유효성 검사 지침 개발
3) 정수 및 상하수도 제어 시스템 상태 감시 체계 구축</td></tr>
<tr><td colspan="2">※ 주요 보안 실증사업
o 수자원 공급 설비 및 공정 자동화된 상하수도 제어 시스템을 도입한 실증 정수장을 구현하고, 내부 트래픽 감시, 원격 시스템 접속 제어 등 스마트 크린 워터 기반 통합 정수장 대상 취약점 점검 수행</td></tr>
</table>

3-3. ICT와 Security가 결합된 맞춤형 「IoT Security Brain」 양성



o **(다학제간 융합보안 인재육성)** 기계공학, 건축공학, 에너지공학 등 7대 분야 관련학과에 각 분야별 보안이슈를 이해할 수 있도록 **정보보호 기본교육(素養化) 추진**('16년~)

<IoT 서비스 관련 학과 현황>

7대 분야	IoT 서비스	관련 학과
홈·가전	스마트TV, 냉장고, 에어컨 등 스마트홈	전자, 전산, 기계, 로봇
의료	바이오인식, 생체신호측정, 원격진료, 건강기록	의학, 전자, 기계, 전산
자동차	커넥티드카, 스마트 교통관제, 스마트 도로	전자, 기계, 도시공학, 물리
환경/재난	실시간 환경·생태 관측, 대기·수질 모니터링 및 예보	환경, 해양, 산림, 화학, 생물
제조(공장)	스마트 팩토리, 지능형 물류, 산업안전	기계, 전산, 전자, 수학
건설	인텔리전스 빌딩, 스마트 건축관리, 건물관제	건축, 토목, 전자, 전기, 기계
에너지	스마트 플러그, 지능형 에너지 수요관리	에너지, 자원, 전기, 전자

- IoT 환경의 각종 SW를 대상으로 하는 진화된(Invisible, untraceable) 공격에 대응하기 위해 **정보보호 전공학생 대상 심화교육** 추진('15년~)

※ 정보보호 학과를 보유한 대학을 중심으로 보안코딩, 임베디드 보안, 암호 등 IoT 정보보호관련 핵심 교육과정 개발 및 제공

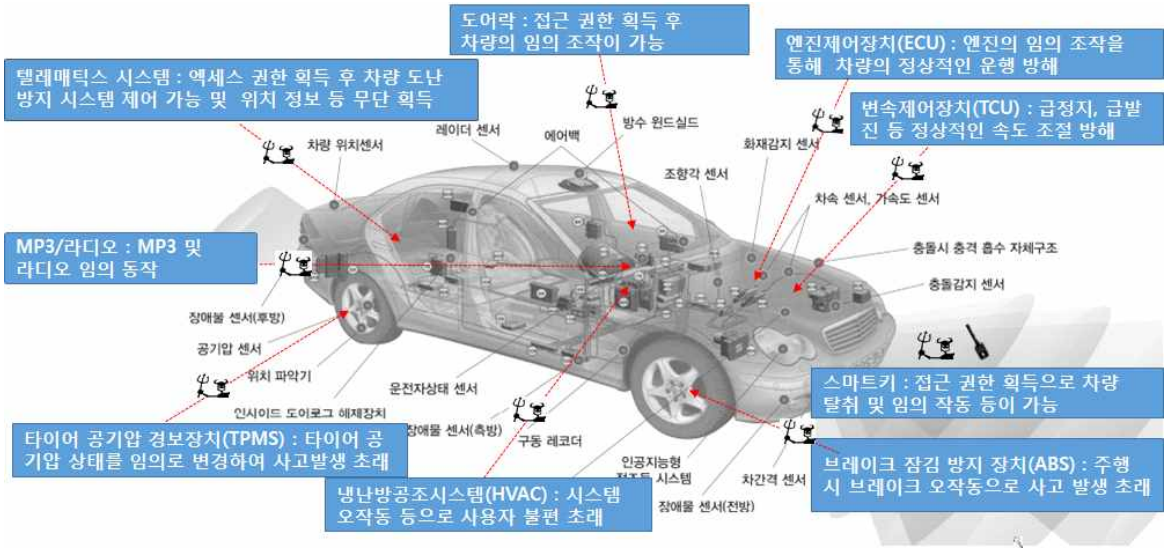
- 非 IT·정보보호 전공 학생의 **정보보호 부전공**을 지원하는 **다학제간 'IoT 정보보호 트랙(Track)' 과정** 신설 유도('16년~)

※ 주요 IoT 기업과 협약 체결 등을 통해 졸업생 인턴쉽 제공 및 취업시 서류전형 가점 부여 등 취업연계 추진

< 정보보호 기본 소양화(素養化) 추진 필요성 >

o 스마트카(기계공학, 자동차공학)

- 무인주행, 위험감지, 교통량 제어 등의 시스템에 대한 비인가 접근, 통신 채널 해킹 방지, 정보 위·변조 방지 등을 위해 **기존의 기계·전자·통신 학과 등에서도 정보보호 과정을 필수적으로 이수할 필요**



출처 : 2014년 IT산업 7대 메가트렌드(한국정보산업연합회) 인용 수정보완

o 스마트빌딩(건축공학, 에너지공학)

- 빌딩 관리 시스템(BMS)이 점차 지능화되고 상호 연결되면서 시스템 다운, 통신두절, 데이터 유출과 같은 보안위협을 예방하기 위해 **기존의 건축·토목·전자·전기 등 유관학과에 정보보호 과정을 필수적으로 이수할 필요**

출처 : CEMS technologies 인용 수정보완

o **(보안교육 인증제)** 산업계에서 필요로 하는 역량을 갖춘 정보보호 인력 배출을 위해 **'IoT 보안교육 인증제' 도입**('16년~)

- 정보보호 관련 대학 학과인증으로 교과목 구성의 적정성 및 교수진·교재·연구시설 등 **일정기준에 부합하는 학과 인증 추진**

※ 인증기준(안) : 교육목표, 학습성과, 전공별 정보보호 연계 교과수준, 실습·실무 연계 비율, 학생·교수진, 교육환경, 산학연계 계획 등을 평가

o **(ICT+Security 인력 양성)** 산업별 보안이슈 및 문제 해결을 위한 **ICT와 Security가 결합된 융합보안 인재** 양성('15년~)

- IoT 보안인력이 갖추어야 할 전문지식(Knowledge) 및 기술역량(Skill), 태도(Attitude) 등을 분석하여 주요 **산업분야별 보안 코디네이터*** **양성**

* 산업분야별 IoT가 적용된 제품·서비스 개발시, 기획·설계단계부터 ICT와 정보보호를 선도적으로 이끌어 나갈 수 있는 보안 전문인력

o **(7대 분야 재직자 정보보호 재교육)** 7대 IoT 산업분야 현장 종사자의 역량 강화를 위한 **IoT 정보보호 교육과정 운영**('16년~)

- **ICT가 접목**된 설계·제조·개발(제어 및 구동시스템 등)을 담당하는 **현장종사자의 정보보호 전문성 강화**를 위한 **'재직자 보안교육'** 실시

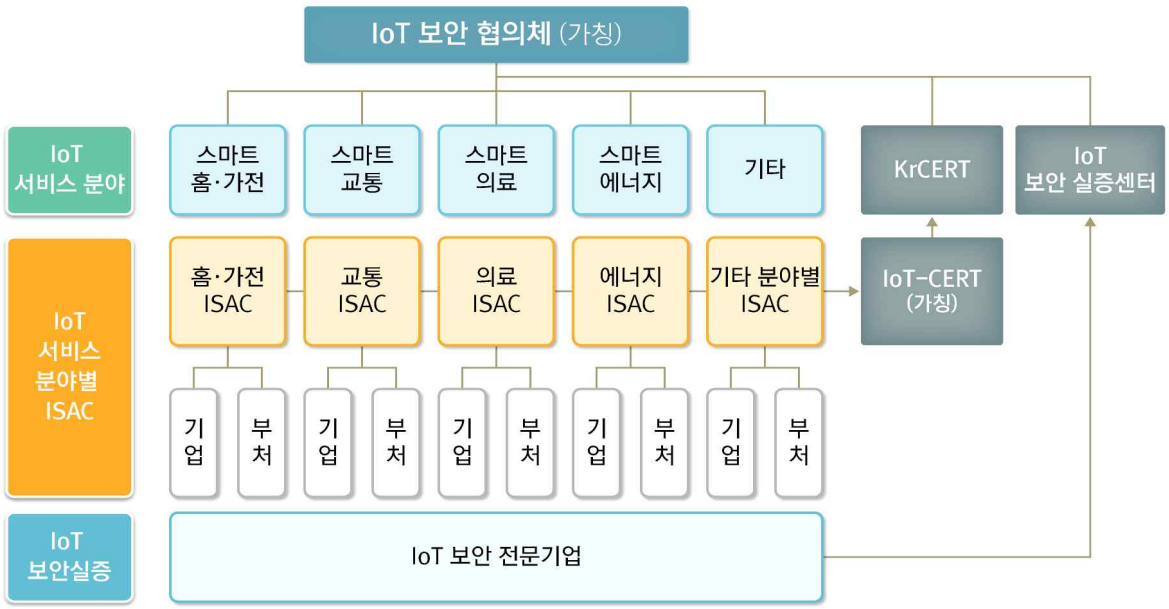
분야	재직자 교육 과정(예시)	추가 보안교육
홈·가전	3D전문인력 양성(산업부), SW현장전문인력양성(미래부)	o SW보안설계 - 임베디드 보안 - 시큐어코딩 - 경량 인증/암호화 o 보안 아키텍쳐 - 접근통제, 물리보안 - 다중체계 정보보안(DID) o 기타 산업별 보안원칙 등 정보보호 관련 교육 포함
의료	바이오전문인력양성(산업부), 보건산업핵심전문인재양성(복지부)	
자동차	자동차 및 정밀화학산업 인재양성(산업부)	
환경/재난	생태복원전문가 교육(미래부), 환경기술전문인력양성(환경부)	
제조(공장)	플랜트 설계인력 양성(산업부), 해외플랜트시공관리과정(국토부)	
건설	U-City전문인력양성, 미래 친환경 건축인력 양성(국토부)	
에너지	에너지 인력양성(산업부), 에너지 산업전문인력역량강화(산업부)	

-「**정보보호 지원센터**」를 통한 **지역 중소기업 재직자 보안교육** 및 **지방소재** IoT 제품·서비스 업체에 대한 **정보보호 기술 지원**

※ '17년까지 8개 지역에「정보보호 지원센터」를 구축하여 지방소재 중소기업의 IoT 보안교육 및 기술지원 등 정보보호 애로사항 해결

Ⅵ 추진체계 및 역할

□ 추진체계



구 분	주요 업무
IoT 보안 협의체(가칭)	- 기업, 부처 등이 참여하여 IoT 보안 최신기술·정책 동향 공유 및 IoT 보안이슈 발생 시 조정·해결
IoT 분야별 ISAC	- 홈·가전, 교통, 의료, 에너지 등 주요 IoT 서비스 분야별 보안위협 정보 수집·분석하여 'IoT-CERT'에 공유
IoT-CERT	- KrCERT, IoT 서비스 분야별 ISAC 등을 통해 수집한 IoT 취약점·침해사고 정보 등을 분석하고, 보안권고 및 기술지원 등 보호조치 이행
IoT 보안 실증센터	- 기업, 부처에서 수행하는 IoT 실증사업에 보안이 내재될 수 있도록 주요 실증사업과 보안 전문기업 매칭·관리 - IoT 보안 테스트베드를 구축·운영하여, IoT 보안 전문기업이 개발한 제품에 대한 보안 테스트 지원
IoT 보안 전문기업	- IoT 보안제품 및 서비스를 개발하고, IoT 보안 실증사업에 참여하여 상용화 준비를 위한 검증 수행
정부	- IoT 보안 강화를 위한 정책개발·추진 - IoT 보안 기술 연구·개발 지원 - IoT 소관 부처, 기업과의 협력체계 구축 - IoT 서비스 보안실증 지원(취약점 분석, 컨설팅 등)

Ⅶ 추진 일정

추진과제		'15	'16	'17	'18	소관부처
추진전략 1. 보안이 내재화된 IoT 기반 조성						
1-1. 7대 분야 IoT 제품·서비스 보안 내재화	공통 보안원칙 개발·보급	■				미래부
	7대 분야 보안 고려사항 개발·보급	■	■	■		범부처
1-2.. IoT 사이버위협 종합 대응체계 구축	IoT 보안 협의체 구성·운영	■	■	■		범부처
	IoT 인프라 보안 강화	■	■	■		범부처
	IoT 취약점 분석·공유(IoT-ISAC) 구축·운영	■	■	■		범부처
	사이버위협 종합대응 체계 구축·운영		■	■		범부처
1-3. 안전한 IoT 제품·서비스를 위한 신뢰성 확보	IoT 제품·서비스 책임 강화		■	■		미래부
	IoT 보안인증 도입 지원	■	■	■		범부처
전략 2. 글로벌 IoT 보안 선도기술 개발						
2-1. IoT 보안 핵심 원천기술 개발	경량·저전력 암호 기술 개발	■	■			미래부
	보안 SoC 및 보안 운영체제 개발	■	■	■		미래부
	실시간 이상징후 탐지·대응 기술 개발	■	■			미래부
	IoT 보안 게이트웨이 및 침입탐지 기술 개발	■	■	■		미래부
	스마트 인증 및 IoT 프라이버시 보호기술 개발	■	■			미래부
	IoT 보안 솔루션 개발	■	■			미래부
2-2. IoT R&D 오픈 이노베이션	IoT R&D 오디션 프로그램 도입	■	■	■		미래부
	IoT R&D 국제협력 및 표준화	■	■	■		미래부
전략 3. IoT 보안 산업경쟁력 강화						
3-1. IoT 보안 우수기업 발굴·육성	IoT 보안 Startup 기업 지원	■	■	■		미래부
	IoT 보안 테스트베드 구축 및 파트너십 제공		■	■		미래부
	IoT 융합보안 실증사업	■	■	■		범부처
3-2. IoT 제품·서비스 보안수요 확대	IoT 보안취약점(버그바운티) 발굴	■	■	■		미래부
	글로벌 IoT 보안수요 발굴	■	■	■		미래부
3-3.「IoT Security Brain」양성	다학제간 융합보안 인재 육성 및 보안교육 인증제 도입		■	■		미래부, 교육부,
	산업분야별 융합보안 인재(코디네이터)양성	■	■	■		범부처
	7대 분야 재직자 정보보호 교육		■	■		범부처

1. 개요 및 현황

□ 개념

○ **(개념)** 인간이 생활하고 거주하는 공간에 ICT를 융합하여 인간 중심적인 스마트 라이프를 실현하는 환경

- (협의) 스마트홈은 홈서버, 정보가전, 융합단말 및 이를 하나의 가상 홈으로 연결하기 위한 네트워크 환경구축과 홈서비스를 포함하는 개념

- (광의)건설 및 주택 인프라와 전자, 통신 기기 산업에서 융합된 서비스를 공급하는 홈 관련 산업 전반으로 정의

※ 출처 : 2013 스마트홈 산업현황 보고서(2014, 한국스마트홈산업협회)

< 스마트홈 구성도 >

※ 출처 : KEIT, 'IT R&D 발전전략 보고서'

□ 국내·외 동향

○ **(시장)** 글로벌 스마트홈 시장 규모는 '14년 480억 달러(약 49조원)에서 연평균 19%씩 성장하고, 국내는 '12년도 5조 4,067억 원에서 연평균 성장률(CAGR)은 27.6%로 전망 됨

※ 자료 출처: 2014 Strategy Analytics, 2013 스마트홈 산업현황 보고서(한국스마트홈산업협회)

○ **(해외 기업)** 스마트홈 관련 시장 진출 기업으로는 통신사업자, 정보가전 플랫폼 사업자, 건설사, 서비스 사업자 등 다양한 분야 기업들이 진출

종류	내 용
통신사	AT&T, Verizon 등 주요 통신사들은 스마트홈 서비스를 통합 콘텐츠 플랫폼으로 한 새로운 비즈니스 모델 창출 모색 중 * AT&T : 홈오토메이션과 보안을 결합한 Digital Life 상품 출시, 15개 도시('13년 4월) → 50개 도시('13년 말) * Verizon : 홈모니터링 & 컨트롤 서비스를 전국 확대(유선망, '12년 말)
서비스사업자	동작·음성인식 등 가전제품 제어기술과 스마트폰, 테이블릿 등 스마트 디바이스 간 N-스크린 서비스를 개발 중 * MS : 게임콘솔을 포함한 스마트 기기들의 콘텐츠와 프로토콜 통합 추진 * Apple : 자사제품들(iPhone, iPad, Apple TV 등)과 홈네트워크융합을 통한 N-스크린 서비스 추진
플랫폼 사업자	Apple, Google, 삼성전자 등이 각자의 얼라이언스 중심으로 플랫폼 전쟁 중 * Google : 안드로이드@홈을 통해 댁내의 가전을 위한 표준으로 안드로이드를 보급하고자 하였으나, 여의치 않자 네스트를 인수하여 제2의 안드로이드@홈 추진 * Apple : iOS7 iBeacon으로 플랫폼 연동 실내위치서비스 선도 사물 인터넷을 활용한 스마트홈 구현 플랫폼 '홈킷'을 개발 * 삼성전자 : IoT컨소시엄(쓰레드그룹, OIC컨소시업)에 참여 및 삼성 스마트홈 플랫폼 오픈, 스마트홈 플랫폼 회사인 Smart Things 인수 등을 통해 스마트홈에서의 주도권을 놓치지 않기 위한 노력 중
융합가전	미국의 GE, 독일의 지멘스, 일본의 SONY 등이 스마트그리드 기능, 스마트 제어 기능을 탑재하여 경쟁중 * GE, 월풀 : 냉장고, 세탁기, 의류건조기 등에 스마트그리드 기능을 적용하고 아이폰과 아이패드 앱을 통해 제어하는 기술 제품화 * 지멘스 : 에너지 절감 기술기반의 스마트 와트 시스템 개발 * 밀레 : 자사의 모든 가전을 스마트폰으로 제어하는 "InfoControl Plus" 제품을 개발하여 경쟁 중 * 도시바 : 자사 기기에 다운로드기반 업그레이드 기능을 적용

○ **(국내 기업)** 통신사업자, 기기 전문기업, 건설사, 서비스 사업자 등이 스마트 홈 인프라 및 서비스 개발 중

종류	내 용
통신사	· KT, SKB, LGU+ 등은 스마트 단말을 통한 부재 시 침입자 탐지와 원격 모니터링 등의 홈 보안 서비스를 제공 중 * KT(홈 지킴이), LGU+(홈 CCTV), SKB(해피뷰)
서비스 사업자	· IPTV, 홈엔터테인먼트 중심의 사업 전략에서, 최근 모바일서비스와 연계한 클라우드 서비스인 U-Cloud, T-Cloud를 스마트홈으로 확장 · 에스원, KT텔레캅 등 보안 전문업체에서는 스마트폰 기반으로 기존의 보안서비스에 원격제어 및 모니터링 등의 서비스를 확대 제공 * 에스원(세콤홈즈) : 센서와 제어기를 활용한 공동주택 개별세대 전용보안 시스템. {컨트롤러+전등제어+가스차단+영상+대기전력차단} + 스마트폰 * KT텔레캅(홈가드) : 센서 기반의 외부침입을 감시하는 홈 보안 서비스. {IP주장치+침입감지센서+SMS통보+원격제어+IP-CCTV} + 스마트폰
전문기기 사업자	· 홈 미디어 서버와 상호연동하는 홈네트워크 미들웨어개발에 주력하면서 실감·감성홈, 에너지 절감 등 미래를 대비한 기술개발 착수 * 삼성SDS : 침입자 감지·가스누출 경고·디지털 도어록 연동 기능이 가능한 이지온 월패드를 각 세대 및 공용구간, 관리사무소, 방재센터, 통신실 등과 인터넷으로 연계한 홈네트워크 서비스 공급 · 홈, 빌딩에너지를 위한 수동적인 관리에서 에너지 소비 모니터링 정보를 기반으로 소비절감을 지원하는 핵심기술 개발 중 * 하니웰, 삼성 SDS, (주)나라컨트롤, 현대산업개발 : 대기전력차단시스템, 빌딩 자동제어시스템을 개발하고 솔루션 구축 및 운용 사업 진행
건설사	· 신규아파트 중심의 홈오토메이션에서 호텔, 병원 등으로 사업영역 확장 및 u-City 연계된 스마트홈 사업 추진 * 신축 아파트의 빌트인 형태로 홈네트워크 구축을 추진하고 있으며, 향후 유비쿼터스 사회를 지향하는 종합건설서비스 회사로의 도약 추진
가전사	· 국내 업체들은 제품 개발과 함께 플랫폼 마련 위해 노력 중 * 삼성전자 : 스마트홈 플랫폼(SHP)을 오픈하고, 관련 가전 및 센서 사업자와의 연대를 통해 사업선점 추진 중 - 스마트홈 솔루션인 'Smart HomeNet'은 스마트폰, 무선인터넷(Wi-Fi), 클라우드 컴퓨팅 등 다양한 IT기술을 가전과 결합하여 특화된 콘텐츠와 서비스를 제공하는 사용자 중심의 스마트가전 전략 추진 * LG : 홈챗 솔루션을 통해 대화형 가전제어 서비스를 제공하고 있으며, 카카오톡, 라인 등과 같은 SNS서비스와 연계

○ **(정책)** 미래부 국가정보화기본계획, 정보통신 진흥 및 융합 활성화 기본계획, 사물인터넷 기본계획 등을 통해 스마트 홈 추진을 위한 추진전략 및 핵심과제 제시('13.12~'14.5)

○ **(표준화)** 스마트홈 미들웨어 상호연동(ISO/IEC JTC1), 댁내 미디어유통 및 홈엔터테인먼트 서비스(DLNA, UPnP 등) 국제 표준화 추진

- IEEE는 스마트 그리드 상호연동, ISO/IEC는 스마트홈 에너지 관리표준, AHAM 중심으로 북미 가전기기의 스마트그리드 연동기능 표준화 추진 중
- 국내는 스마트융합가전포럼 중심으로 스마트홈/가전의 융복합을 위한 IT서비스 접속규격 표준화 추진 중
- ESTI Smart M2M에서는 시맨틱 기능을 정보가전 플랫폼에 접목함으로써, 지능형 가전기기 간 에너지 관리를 위한 표준화 추진
- 서비스 반경이 넓고 주파수 혼잡도 낮은 WPAN 기술 표준화 활발

※ EEE802.15에서 WBAN, SUN, LECIM, TVWS-WPAN 무선 전송기술에 대한 표준이 완료되었으며, IETF에서 저속 WPAN을 이용한 IP 통신 표준화 진행 중

※ 국내는 TTA에서 RS-485와 SUN, LECIM 통신 표준 제정 완료, TVWS -WPAN 표준 진행 중

※ 국내는 유무선 홈네트워크 서비스 프로토콜(RS-485 및 IEEE 802.15.4 기반)과 홈게이트웨이, 월패드, 단지서버 규격(KS표준), SUN 통신 표준 제정이 완료됨

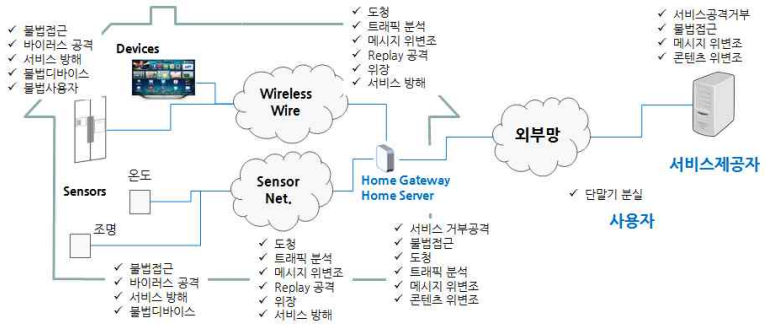
< 스마트홈 표준 현황 >

기구명	추진 목표	주요 참여기관
Allseen Alliance	IOT의 커넥티비티 표준화로 기기 간 및 플랫폼 간 연결호환성 확보	LG전자, 하이얼, 퀄컴, 마이크로소프트, 파나소닉, AT&T
OIC		삼성전자, 델, 인텔 등
Thread	Zigbee 기술단점을 보완한 보안 및 저전력 기술의 표준화	삼성전자, ARM, 프리스케일, 실리콘랩스
HomeKit	애플 생태계의 폐쇄적 IOT 표준화	Philips, Honeywell, Apple, Haier, TI
IIC(Industrial Internet, Consortium)	산업용 IOT 활성화를 위한 표준개발	Intel, IBM, AT&T, Microsoft, Cisco
스마트융합가전포럼	IOT 기반의 스마트홈 표준화	삼성전자, LG전자, 코웨이, 모뉴엘, 경동원

○ **(인증)** 국가기술표준원은 스마트홈 제품에 대한 적합성평가와 인증업무를 추진하기 위하여 한국제품인정제도(KAS: Korea Accreditation System)를 적용하기로 방침을 수립하고 수행기관으로 TTA를 선정

2. 보안위협과 사례

○ (보안 위협 요소) 스마트 홈은 가전제품들과 센서 등이 이종의 유무선 네트워크 및 프로토콜로 연결되고, 이를 위한 OS, S/W들이 혼재되어 있어 다양한 보안 취약성을 내재하고 있음



※ 출처 : 홈네트워크 보안기술 및 표준화 동향, ETRI, 2008

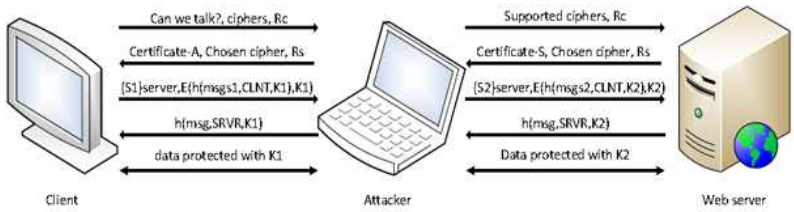
- 스마트 홈에 사용되는 스마트 디바이스는 컴퓨팅 능력, 네트워크 연결 등으로 기존 가전기기와 달리 다양한 보안 위협 존재

종류	특징	보안 위협
스마트TV	- 인터넷 연결 상에서 편의 기능 제공 - 예 : 멀티미디어 콘텐츠 재생, TV 전용 애플리케이션, 홈쇼핑, 웹서핑 등 - 리눅스 등 일반 OS 기반에서 작동 - PC 환경의 보안 위협을 내재	- 해킹 시, 공격자는 PC 환경에서의 거의 모든 악용 행위가 가능 - 예 : 금융정보 탈취, 스미싱 - 카메라/마이크 내장 시, 사생활 침해
로봇청소기	- 인공지능 프로그램으로 자가학습 및 개선된 청소 기능 구현 - 일반적으로 임베디드 리눅스 사용 - 카메라를 통한 장애물 인지·처리 - 인터넷 기능 내장으로, 해킹 위협 내재	- 알려진 OS 및 인터넷에 따른 해킹 위협 - 해킹 시, 공격자는 로봇청소기에 내장된 카메라를 통해 사용자 집 감시 가능 - 공격자는 로봇청소기를 원하는 위치로 이동시킬 수 있으므로 사생활 침해
인터넷 전화기	- 기존 전화보다 저렴한 요금으로 국내외 통화 가능 - 유선/무선 네트워크 디바이스 장착으로 항상 인터넷 연결 - 임베디드 환경과 유사하므로, 해킹 위협 존재	- 해킹 시, 치명적인 사생활 침해 - 회사에서 사용 시, 자산 노출 위험
가정용 CCTV	- 인터넷 전화기와 결합되는 경우가 많음 - 어느 곳이든 사용자 집을 볼 수 있음 - 인터넷 디바이스 내장으로, 카메라를 통한 사진/동영상 전송 SW가 구현됨 - 해커가 공격할 수 있는 attack point 존재	- 해킹 시, 공격자는 사진·동영상을 자신의 서버·이메일로 전송 가능 - 일반적으로 잘 보이는 곳에 설치되므로, 사생활 침해 우려 - 원격제어가 가능하므로, 공격자는 고정된 곳 외에 여러 곳을 훔쳐볼 수 있음

※ 출처 : 「임베디드 시스템 및 스마트가전 보안」 동향 분석 결과, 2013

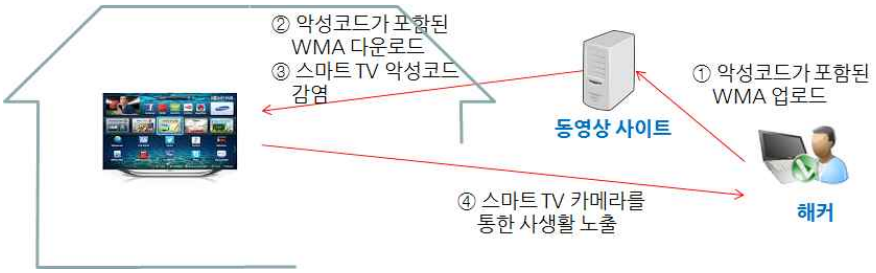
○ 보안위협 사례

- (사례 1 : 중간자 공격) 스마트 TV와 웹 서버간 SSL 통신 시, 침입자가 스마트 TV와 웹서버간에 중간자(Man-in-the-Middle attack)을 시도하여 전송 데이터에 접근하여 비인가 열람 및 위변조 가능



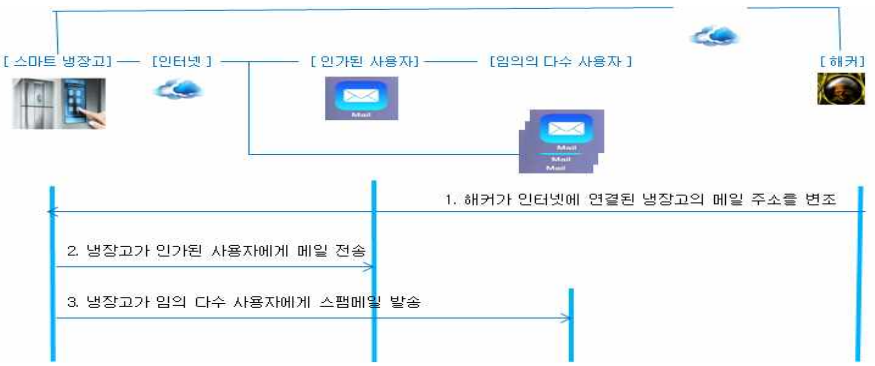
※ 출처 : Smart TV Hacking, University of Amsterdam, 2013

- (사례 2 : 악성코드) 악성코드가 포함된 동영상 파일을 통해 스마트 TV 등 카메라가 내장된 디바이스에 의한 사용자의 사생활 노출



※ 출처 : Demo: Using Malicious Media Files to Compromise the Security and Privacy of Smart TVs, 2014

- (사례 3 : 스팸) 침입자가 스마트 냉장고에 침입하여 저장된 메일 주소 또는 임의 메일 주소로 스팸메일을 대량 발송할 수 있음



※ 출처 : Demo: Using Malicious Media Files to Compromise the Security and Privacy of Smart TVs, 2014

○ (보안 기술 필요성) 스마트 홈의 안전성 확보와 산업의 활성화를 위해 보안 기술 적용 필요

1. 개요 및 현황

□ 스마트의료 개념

○ **(개념)** 센서, 유·무선 네트워킹 등의 융합기술을 활용하여 간단한 진료부터 원격진료, 맞춤형 의료기술에 이르기까지 언제 어디서나 질병을 예방·진단·치료·사후 관리를 하는 서비스를 의미

※ **유헬스(Ubiquitous-Health)** : IT기술을 의료서비스에 접목하여 환자 및 일반인이 언제, 어디서나 이용 가능한 원격의료 및 건강관리 서비스가 중심

※ **스마트 의료** : B2C, B2B, B2G등 의료정보 전체영역에서 의료정보처리 고도화, 시스템을 기반으로 라이프사이클과 관련, 향상되고 지능화된 기술을 접목하여 의료서비스를 종합적으로 개선하는 차세대형 의료의 **포괄적 의미**

○ **스마트 의료의 전체적인 아키텍처**는 전체적인 서비스 연계흐름 차원에서 기존 의료서비스기관들과 같은 이해관계자의 **로컬시스템, 국가인프라서비스, 온라인상의 서비스**로 구분

(출처: 지식경제부, 스마트의료정보 표준화 프레임워크 2012)

□ 국내·외 동향

○ **(시장)** IT, BT의 발전과 신기술 융합으로 **스마트 의료**와 같은 **예방중심의 맞춤형 서비스**가 가능해지면서 관련 시장 확대 추세

※ 향후 스마트 의료 분야에서 약 2조원 규모 시장 성장 및 연평균 약 13,000명 고용 창출 효과 예상(한국보건사회연구원)

	국내(억불, %)			국외(억불, %)		
	2011	2020	연성장률	2011	2020	연성장률
바이오 서비스	1	7	25.0%	447	3,328	25.0%
U-헬스케어	22	62	12.5%	129	2,310	37.8%

(출처: 차세대융합기술연구원, BBC Research)

- 스마트폰과 모바일 어플리케이션, 전용 단말기 등을 통한 헬스케어 시장이 성장하고 있음에 따라 전통적인 제조 중심의 전문기업 외에도 소규모 자본을 기반으로 하는 스타트업의 진출도 활발

구 분	업체명	주요 내용
미국	Fitbit, Jawbone, Misfit	- Fitbit, Jawbone, Misfit 등의 스타트업들이 웨어러블 건강정보 시장에 진출, 모바일 앱과 연동된 사용자의 신체 상태를 모니터링 및 활동을 체크하고 건강을 보조하는 기능을 제공
	Apple, Google	- Apple과 Google은 Healthkit 과 HomeKit, Google Fit 등의 서비스를 통해 건강 및 헬스케어 앱에서 생성된 건강정보를 받아 저장하는 중앙저장소 역할을 플랫폼 기반으로 처리할 수 있도록 제공 - 구글은 개인유전자 분석서비스 「23andMe」를 통해, 유전자 검사와 설문 조사를 기반으로 유전자와 신체특성에 관한 대규모 데이터베이스를 구축하고, 이 정보를 유상으로 의료기관에 제공 (현재는 FDA(미국 식약의약청)의 서비스 중지명령에 따라 '13.12 활동중단)
	Foundation Medicine	- 「Foundation One」 서비스도 의뢰받은 환자의 유전정보를 분석하여 의료진에게 제공, 차세대 시퀀싱 기술, 개인별 유전체 정보파악, 임상정보와 유전체 정보의 통합을 통한 개인중심의 맞춤형 서비스를 진행
	Sotera Wireless	- 맥박, 심전도, 산소포화도, 혈압, 호흡, 체온 등의 활력징후 상시 모니터링 가능한 손목 밴드형 모바일 장비를 출시, Cerner社의 병원정보시스템과 연동하여 입원환자 활력징후를 측정 방법을 혁신적으로 개선하는 기술을 제공
	Sloan -Kettering	- 암 연구센터 종양연구진의 암 치료 연구에 IBM의 인공지능 왓슨(Watson) 도입, 방대한 비정형 진료정보까지도 의료정보 연구 자료로 활용·분석하여 환자의 상태를 파악, 의심 질환들과 관련된 연구결과들을 실무적으로 제시하는 조수 역할 수행

- 국내 통신사와 글로벌 제조사 역시 보유한 기반을 이용하여 사업 영역 확장 진행 및 기존 의료기관과 연계한 신규 사업 추진

구 분	업체명	주요 내용
국내	SKT	- ICT기반의 스마트 의료 구축사업을 위한 다양한 모바일 솔루션 개발로 B2C 유형의 사업인 헬스온 서비스 모델화하고 2011년 서울대병원과 합작사 헬스커넥트 설립으로 예방, 진단, 치료, 관리를 연계한 차세대 의료서비스 모델개발을 추진
	KT	- U-Health 센터를 중심으로 독거노인, 만성질환자 관리등 공공 보건의료 서비스와 헬스 파크와 같은 주민건강증진 서비스를 제공하며 지자체별 특성(지역, 예산, 주민구성)에 맞는 차별화된 서비스 모델을 추진하고 2012년 연세대의료원과 함께 후헬스케어를 설립, 스마트 의료사업 추진
	삼성	- 5개 친환경 에너지 및 헬스케어 산업에 2020년 까지 23조 투자계획을 발표한바 있으며, 이에 따른 후속조치로 의료기기 분야를 신규사업으로 채택하여 축적해온 IT기반의 기술을 헬스케어 가치사슬 역량에 최대한 활용, 유헬스 분야에 집중 확장 - 또한 SAMI(Samsung Architecture Multimodal Interactions), IoT 및 웨어러블 컴퓨팅 기기에 적용될 소프트웨어 플랫폼 발표, 건강 데이터 중심의 수집, 상황인지, 맥락 분석, 음성인식, 안내기술을 포괄적으로 통합한 개방형 소프트웨어 플랫폼을 공개함

○ **(정책)** 주요국 정부는 ICT 기반의 헬스케어 활성화를 위한 다양한 진흥 정책을 마련하여 추진 중

구 분	주요 내용
미국	- 오바마 행정부는 경기 부양책인 경제재생법(American Recovery and Re-investment Act)의 일환으로,「경제 및 임상 의료를 위한 의료IT법」(HITECH Act)에 의거, 오마바케어 시행 - 2014년까지 미국 전체 의료기관에 대한 EHR시스템 활용 목표로 2009년부터 「국가 Health IT 전략계획 2011-2015」를 수립하여 Health IT 산업기술 및 건강관리시스템 혁신 등의 단계적 전략 제시하고 192억 달러의 예산을 배정하고 5년간 천억 달러 투자 - 기존 원격의료 시스템 네트워크를 기반으로 향상된 U-Health를 목표로 시행중이며, 보건성 산하 OAT에서 업무를 담당하고, OAT 산하의 6개의 원격의료 지원센터를 통해 법·제도 개선 및 서비스 제공·운영
EU	- 유럽연합, 전 회원국 간 협력을 기반으로 표준기반 EHR등 보건의료정보 교류 및 네트워크 구축을 위한「EU eHealth Action Plan 2012-2020」인 총괄적 추진계획을 수립·실행 - 6th Framework Program (TELEMED, AMON, RETAIN, ASFE21 등)에 국가간 협력을 통한 헬스케어 시스템 연구지원 내용이 포함, 광대역 및 협대역 GSM/ATM 종합통신망을 기반으로 영상, 의무기록을 교류하고 복합 착용형 의료기기를 통한 원격건강 모니터링 및 건강관리 프로젝트를 중장기 종합계획을 수립하여 추진
일본	- 선도화된 ICT기술을 바탕으로 의료정보분야를 5대 신성장동력으로 선정, 「국가 Brand Design의 Healthcare 정보화」정책의 일환으로 전략적인 관리 수행 - 전국민 대상 개인건강기록(PHR)시스템 운용시작 (2013년), 의료기관간 보건의료 정보 교류를 위한 EHR 구축완료(2015년) 등 스마트 정보기반 구축에 총력 - 원격 방사선 진단(Tele-radiology), 원격 병리진단(Tele-pathology), 협동의료, 원격가정간호 (Tele-Homecare)의 사업을 일본 후생성이 전국 지자체와 함께 사업을 진행, 서비스 확대 중 - 일본 로봇시장에 큰 비중을 차지하는 의료, 간병, 복지 부문(32.7%, 2014 TDB자료)의 Healthcare 로봇 시장 확대를 통해 저출산, 고령화 사회문제를 접근, 로봇 벤처기업 활성화 투자 지속

구 분	주요 내용
국내	- 박근혜 정부에서는 140대 국정과제 중 하나로 보건·고령친화산업을 미래성장 사업을 육성하기 위해 유헬스를 추진함으로 신 의료·융합서비스 발전을 위한 제도 및 정보화 기반을 조성 중 - 의료IT의 국제 경쟁력을 확보를 위한 전략 과제로 지식경제부는「2018년 의료기기 5대 선진강국으로 도약」하기 위한 추진 전략 및 장단기 추진과제로 디지털병원 수출, U-Healthcare 신사업 창출, 국제기준 적합화 지원, 임상시험지원 강화에 집중 - 공공전문 의료기관은 정부3.0 정책에 의거 정보공개를 원칙으로 병원, 약국 정보검색 서비스, 건강검진 결과 공유를 통한 운전면허 발급시, 신체검사 생략 서비스, 국민건강보험공단의 맞춤형 건강서비스 개발, 국민건강 주의예보 서비스 등 소비자중심 스마트 의료 서비스 형태로 구축하고 있음
	- 기술개발 측면에서는 2011년부터 WBS(World Best Software) 사업을 통해 글로벌 기준을 준수할 수 있는 의료정보프레임워크 개발과 지능형 영상진단 및 치료지원 시스템개발, 원천기술개발을 위해 디지털병원 정보시스템·의료기기 통합 프레임워크 개발 지원
	- 표준 확보 측면에서는 의료정보모델표준화, 의료정보 전송체계 표준화, 의료정보 보안표준, 의료정보시스템 인증제도 및 기준마련 등의 검토진행하고 K-Health 3.0 시범사업을 통해 진료정보교류를 위한 표준가이드라인 및 EMR/EHR 시스템의 기능성, 상호운용성, 보안성 인증기준 검증하고 있음
	- 스마트의료 서비스 영역에 있어서는 2011년부터 국가표준코디네이터 제도를 시행하여 국가표준프레임워크 개발하고 중장기적인 표준화 로드맵 전략을 수립하여 국가 R&D과제에 범·부처별로 진행되는 중복연구과제방지와 전략적 기술연계를 추진 중

□ 표준화 현황

○ 의료시장의 개방 및 국제화에 따라 점차 의료정보의 교환·공유 문제가 이슈화되는 추세

- 의료 표준화는 크게 콘텐츠와 기술영역으로 구분하여, 의료정보 체계를 객관적이고 공신력 있는 형태로 정의함으로써 의료산업과 관련된 모든 행위자들의 일관된 의료행위 처리가 가능하도록 함

○ 보건의료 표준화 관련 국제표준기관은 ISO/TC215, HL7, CEN/TC251 등이 대표적임

- 이들 기관은 표준개발에 관한 협력을 합의하고 ISO/TC215에 WG9하에 Standard Harmonization이라는 이름으로, 개발 중인 표준들 간의 상호 호환성 제고를 위해 노력 중

- 지난 '14년 10월, 국내에서 제안된 의료정보관련 표준안 3종이 국제 표준으로 채택됨에 따라, 공식 국제표준으로 발간 예정임

ISO/TC215에 제안된 한국형 의료정보 표준체계

의료정보 표준 체계	프로젝트 리더	진행 단계
의료정보모델의 질 평가 매트릭스 관련 표준안	안선주 국가기술표준원 국가표준코디네이터	국제표준으로 채택
개발도상국 위한 모바일 헬스 관련 표준안	김일곤 경북대 교수	
모바일 스마트 정보·의료기기 발전 표준안		
유전자 정보 관련 신규 표준안	신수용 서울아산병원 교수	국제표준으로 가치를 인정, 추후 논의
환자 중심의 진료정보교류 체계 표준안	이병기 삼성서울병원 수석	
뜸질 표현구조 관련 표준안	장현철 한의학연구원 책임연구원	
보건의료정보 보호 교육관련 표준안	이미정 단국대 교수	

자료:국가기술표준원

※ ISO/HL7의 CDA(Clinical Document Architecture, 진료문서교류)가 ISO의 국제표준이었으나, ASTM(American Society of Testing and Materials)의 CCR(Continuity of Care Record, 진료요약정보)이 산업계의 사실상의 표준으로 사용됨에 따라 현실을 반영하여 최근 CDA과 CCR를 합친 CCD(Continuity of Care Document)를 국제표준으로 제정하였음

○ 스마트 의료분야의 주요 표준화 현황은 PHR, 모바일헬스, 원격의료, 스마트데이터 및 의료정보보호 영역으로 구분 가능

스마트의료 영역	주요 표준 제안 및 추진 현황
평생건강관리 (PHR)	- ISO/TR 14292, Personal Health Record, 정의, 범위, 구조 표준 - ISO/DIS 16527 PHR System Functional Model R1, HL7 제안 - ISO/DIS 16527 PHR System Functional Model R2, HL7 진행 - ISO/IEEE 11073, 개인건강기기 표준프로토콜 및 PHR 연동표준
모바일헬스	- IHE, IHE-XDS(Cross-Enterprise Domain Sharing) 기술 제안 - IHE, MHD(Mobile Access to Health Document) 프로파일 제안 - HL7, 헬스케어 앱간의 정보공유 FHIR Framework 기술 제안
원격의료	- ISO/TR 16056, 원격의료 정의, 요구사항 표준 - ISO/TR 16058, 원격교육의 상호운영성 표준 제정 - ITU(국제전기통신연합회), 원격의료에 필요한 통신규격 연구
스마트데이터	- ISO 25720, 유전자 시퀀싱 Variation Markup Language 제정 - HL7, Domain Analysis Model: Clinical Genomics 제안
의료정보보호	- ISO/TS 2220, 사용자식별 - ISO/TS 22600, 사용자 인증 및 접근제어 - ISO/IEC 27799 정보보호 관련체계 - ISO/TS 25237 익명화

- 국내의 경우는 국가기술표준원으로부터 국가표준(KS) 개발, 관리 업무 활성화를 위해 표준개발협력기관(COSD, Co-operation Organization or Standards Development)을 지정하여 표준제정

국가산업표준 (KS)	표준 내용
ISO/TR 16056-X	원격의료 시스템 및 네트워크 상호운용성
KS X 21549-X	건강카드데이터
KS X 7502	진담검사의학과 결과보고서
KS X 7503	진담검사의학과 결과보고서 CDA
KS X ISO 11073	현장진료용 의료장비통신 관련표준들
KS X ISO 12052	의료분야 디지털 영상 및 통신(DICOM)
KS X ISO 12773	건강요약기록 비즈니스 요구사항 표준
KS X ISO 12967	보건의료정보 서비스 아키텍처 표준
KS X ISO 13606	평생전자건강진료기록 통신 관련 표준
KS X ISO 17115	보건의료정보 용어체계를 위한 용어표준
KS X ISO 18104	간호 참조용어 모델의 통합
KS X ISO 18232	메시지 및 통신
KS X ISO 18308	평생전자건간지료기록 아키텍처 요구사항
KS X ISO 18812	검사장비 및 검사정보 시스템간의 인터페이스
KS X ISO 20301	건강카드 일반특성
KS X ISO 20302	건강카드 발행식별 번호체계 및 등록절차
KS X ISO 21091	보안, 통신, 전문의료인 및 환자 식별 디렉토리서비스
KS X ISO 21298	기능적 및 구조적 역할
KS X ISO 21547	평생전자건강진료기록의 보관을 위한 보안요구
KS X ISO 21549	환자 건강카드 데이터
KS X ISO 21667	건강지표 개념 틀
KS X ISO 21731	HL7 버전3 - 참조정보모델
KS X ISO 22220	환자식별
KS X ISO 22857	개인건강정보의 국가간 통신을 위한 정보보호안내서
KS X ISO 25237	익명화
KS X ISO 25238	의료소프트웨어로 인한 안전위험의 분류
KS X ISO 27527	보건의료정보 의료제공자식별
KS X ISO 27789	평생전자건강진료기록을 위한 감사추적
KS X ISO 27951	공통용어서비스
KS X ISO HL7 10781	평생전자건강진료기록 시스탬 기능모델
KS X ISO HL7 27931	자료교환표준, HL7v2.6
KS X ISO TR 12309	용어 개발조직을 위한 가이드라인
KS X ISO TR 17119	보건의료정보 프로파일 프레임워크

□ 의료정보보호 기술 표준

○ 의료정보 기술 표준은 ISO/TC215, ASTM, HL7, DICOM 등과 같은 표준화 기구들의 활동을 통해 독자적, 상호 협력적으로 개발

※ HL7 : 병원정보시스템 및 의료 장비 접속에 관한 표준을 제정하는 표준기관
※ DICOM : 의료 디지털 영상과 부수적인 의료 통합 정보의 전송을 위한 표준 영상 신호 규약
※ ASTM : 미국의 제품 및 재료에 대한 용도 및 특성을 시험하고 제품의 품질을 규격화할 수 있도록 인증을 다루는 표준 기구
※ ISO/TC215 : 의료장비간 데이터의 상호연계성 및 호환성 확보, 의료기록의 디지털화에 필요한 표준 개발을 목표로 하는 의료정보기술위원회

○ 국내는 진료정보교류에 대한 표준 부재로 각 의료기관의 진료정보의 저장, 관리 및 보안체계 등이 상이하게 나타나고 있어, 향후 의료기관간 진료정보 교류에 문제 발생 예상

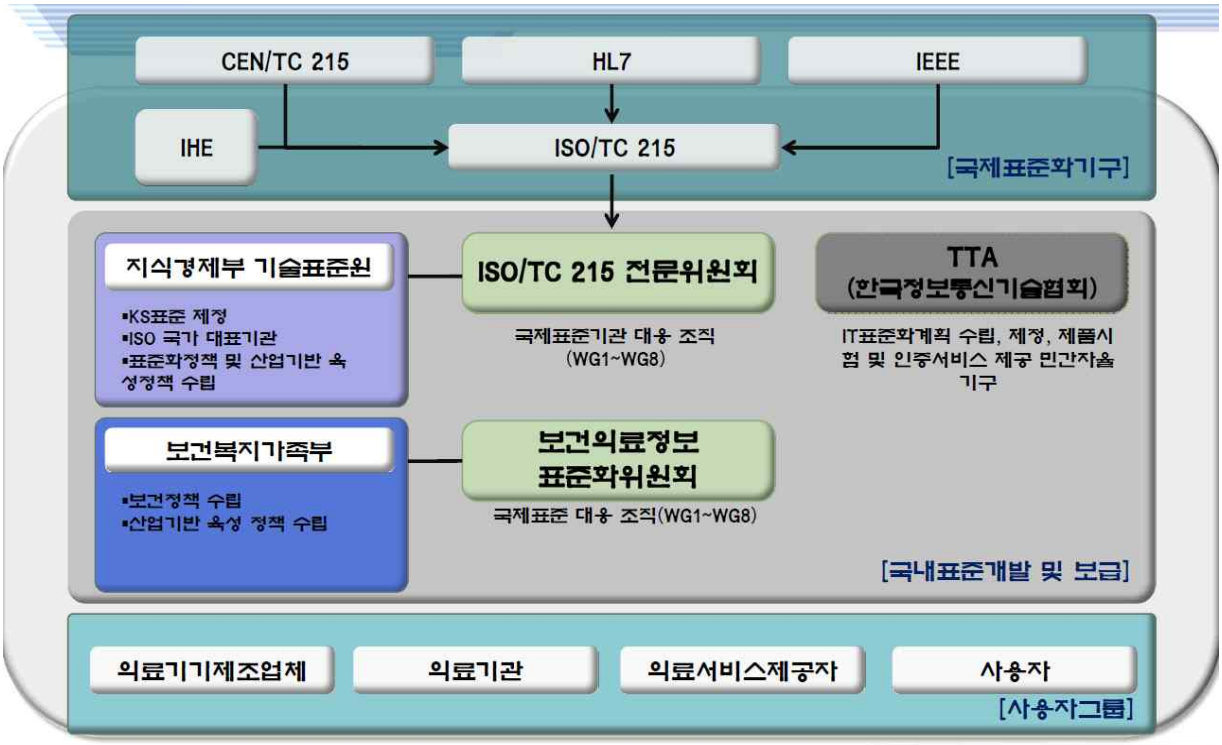
- IHE의 보안 및 프라이버시 통제 항목을 검토하여 종합병원, 병원 등의 규모를 반영한 국내 실정에 맞는 진료정보교류 보안체계 마련 필요

※ IHE(Integrating the Healthcare Enterprise) : 국제 의료정보표준

- ISO/IEC 27001 ISMS를 기반으로 한 의료분야 정보보호관리체계인 ISO/IEC 27799를 활용한 의료정보보호 표준화 작업 및 인증 체계 마련 필요

○ 이와 더불어, 병원정보 교류정보의 서식 및 용어 표준화 필요

- 국내의 진료정보교류 시스템은 상급종합병원을 중심으로 협력병원과 지역 병·의원 범위에서 독자적으로 구축되어 교류되고 있어 상호간 표준의 부재로 인해 시스템 인터페이스 문제가 발생
- 지역적·전국적인 진료정보 교류를 위해 교류항목, 용어, 서식, 인터페이스, 시스템의 표준화를 위해 대규모 구축사업 과정을 모니터링 및 조직화해야 하며 인적·물적 자원 관리체계 필요



국내 의료정보 표준화 추진체계도(TTA)

○ 의료 사이버보안 프레임워크 설계 및 구축 필요

- 환자, 의료진, 의료기기 제조업체, 병의원, 약국, 의료보험 관련기관, 정부 등을 망라한 이해당사자들이 활용 가능한 의료분야 보안 프레임워크 설계 및 구축이 시급

- 미국은 2013년 버락 오바마 대통령이 의료분야를 주요 사회기반시설로 정의하고, 사이버보안 개선을 위해 사이버보안 프레임워크 설계 및 구축을 추진

- 국내의 의료정보보호를 위해 환자, 의료진, 의료기기 제조업체, 병의원, 약국, 의료보험 관련기관, 정부 등을 망라한 이해당사자들이 활용 가능한 의료분야 보안 프레임워크 설계 및 구축이 시급

□ 인증 현황

○ 국내에는 의료기기법에 의거 의료기기의 안전성을 검증하고 품질을 심사하기 위해 의료기기의 등급을 분류하는 KFDA의「의료기기 품목허가(시고) 및 GMP 인증」이 존재

- 원격진료 환경을 마련을 위해 개인용 센싱 기술을 탑재한 신종 PHD(Personal Health Device)의 유형 증가로 관련 산업표준 정비 인증체계를 검증 진행

○ 의료정보시스템 인증제는 정보시스템 제품, 서비스, 표준화 규격의 부합성과 같은 사후관리제도를 위해 SW개발사의 정보화관리 등급, 제품의 기능성, 상호 운용성의 3가지 영역에서 인증범위를 검토함

- 국외 인증제도의 경우, 전자건강기록 인증프로그램으로 ANSI의 ONC (Office of the National Coordinator) 및 CCHIT(Certification Commission for Health Information Technology) 제도가 잘 되어 있는 것으로 평가

※ CCHIT는 전자건강기록 인증기준, 절차 및 보건의료정보 시스템간의 네트워크 인증기준을 개발하고 인증기준개발 대상 부문에서 외래, 입원, 네트워크를 구분해 기능성, 상호 운용성, 보안성 측면의 인증기준을 개발해서 활용하고 있음

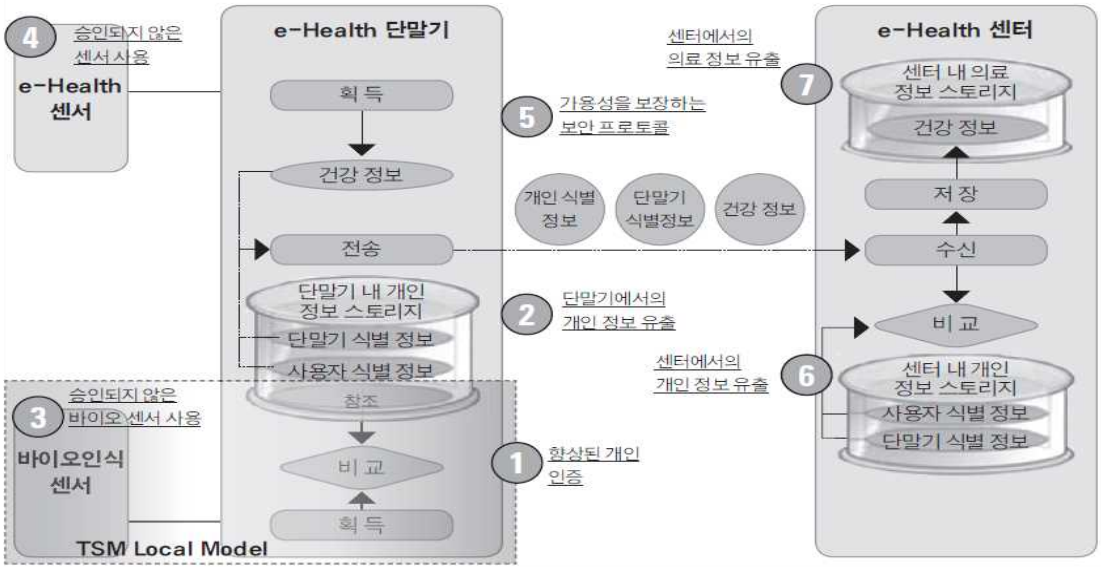
- 최근 국내에서는 의료정보 표준 보급을 위해 CCHIT의 인증 프로세스를 기본으로 우리의 실정에 맞도록 기능성, 상호운영성, 보안성 측면으로 변형한「EMR인증제」를 검토하는 단계임

2. 보안위협과 사례

□ 보안위협

○ 원격지 환자의 진단 및 치료를 위한 원격의료시스템은 환자의 신체 및 의료 정보를 공유함에 따라 개인정보침해의 위협이 존재

- (센서) 승인되지 않은 스마트 의료 센서/바이오인식 센서가 사용될 경우, 환자의 건강정보 노출 및 위변조 가능
- (단말기) 스마트 의료 단말기의 사용자 인증, 개인정보보호, 전송 데이터의 보안이 적절하게 이루어지지 않으면, 단말기를 통한 개인정보 유출 및 서비스 중단 등의 위협 존재
- (센터) 스마트 의료 센터 내 저장된 개인정보 및 의료정보의 접근제어, 암호화, 추적관리 등이 이루어지지 않으면 정보 노출 및 위변조의 가능



※ 출처 : 바이오인식기반 원격진료 보안기술 국제표준화 연구, TTA, 2012

※ ITU-T SG17 Q.9에서 추진 중인 e-Health 및 Worldwide 바이오 인식 데이터 및 개인정보 보호를 위한 통합 기반은 e-Health 모델을 센서, 단말기, 센터 구간으로 구분하여 정의

○ 전자의료기기와 유무선 네트워크가 결합된 스마트 의료 환경에서는 기존 TCP/IP 기반 보안 위협 및 신규 보안위협이 존재

- (서버에 대한 DoS 공격) 사용자 단말, 바이오 센서 등과 연결된 서버에 대한 DoS 공격으로 서비스를 적시에 사용할 수 없는 위협이 존재

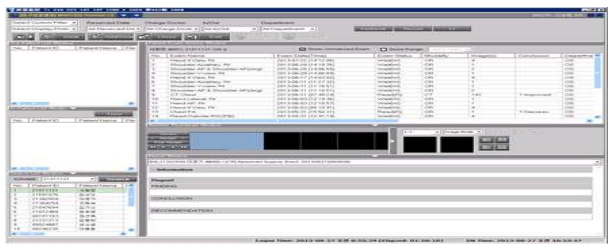
- (의료정보 도청/위변조 공격) 바이오 센서와 서버, 의료진 시스템과 서버, 사용자 단말과 서버간 전송되는 의료정보 및 개인정보의 도청 및 위변조

- (의료정보 공유에 따른 개인정보 노출) 환자 이동 또는 협진을 위한 환자 개인정보 및 의료정보 공유 시, 공유 범위, 열람 제한, 보안 감사, 생체정보 노출 시 인증 방안 등에 대한 보안대책 부재

□ 사례

○ 스마트 의료 산업이 발전함에 따라 의료기기 사이버 공격 위험성 증가로 국민의 생명과 안전에 직접적이고 심각한 영향 초래

- **국내**의 경우 해킹에 의해 의료정보 등의 유출 뿐만 아니라 병원 정보시스템을 장악하여 **생명을 해칠 수 있는 사건 발생**('13. 8)

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td>• Froedtert병원(미국)
– 직원 PC에 악성코드 삽입하여 권한을 획득하고, 환자 개인보험증서, 카드정보, 사회보장번호 등 환자 개인정보를 43,000여건 유출)
(February. 14. 2013. fox6now.com)</td>
<td>• 인슐린 펌프 원격공격 가능
– 해커가 인슐린 펌프를 사용하는 환자의 근처에 접근하여 인슐린 펌프 내부의 소형컴퓨터의 취약점 이용 인슐린의 양을 마음대로 조절하여 공급
(Barnaby Jack, 2012 RSA Conference, 미국)</td>
</tr>
<tr>
<td>  </td>
<td> 
</td>
</tr>
<tr>
<td colspan="2">• 국내 병원 내 각종 의료정보가 해외 서버에 수집
– 진료기록·처방목록·MRI 촬영 화면까지 담겼으며 병원 의료정보뿐 아니라 의약업체의 판매 현황 등
• 해커가 의료정보 유출에 그치지 않고 병원 내부 PC를 장악
– 다수의 의료기관 PC가 악성코드에 감염 (해당 서버가 최다 2000대의 PC를 동시 제어)
– 다수의 해커가 원격에서 병원 PC를 하여 처방전을 임의로 조작 가능
– 해커가 의료정보 유출에 그치지 않고 병원 내부 PC를 장악
※ “병원이 해킹에 노출되는 건 개인정보 유출 차원을 넘어 생명과 직결돼 매우 중대한 문제”</td>
</tr>
</table>

1. 개요 및 현황

□ 개념 및 이슈

○ **(개념)** 전통적인 자동차 기술에 차세대 전기·전자, 정보통신, 기능제어 기술을 접목하여 자동차의 내·외부 상황을 실시간 인식하고 고안전, 고편의 기능을 제공하는 인간 친화적 자동차

※ 출처: KIAT 2012

< 스마트카 개념도 >

○ **(주요 이슈)** 새로운 텔레매틱스 서비스의 발굴과 IoT 서비스의 접목으로 차량 내부와 외부 간의 통신이 증가함에 따라 사이버 보안위협이 도로안전을 위협하는 새로운 위험으로 등장

□ 국내·외 동향

○ **(기술)** OEM을 중심으로 차량과 스마트폰을 연동한 개방형 텔레매틱스 서비스가 출시 중이며, 최근 완성차와 IT 업체 간 협력을 통한 새로운 커넥티드 서비스 출현

< OEM과 모바일업체간 제휴를 통한 새로운 커넥티드 서비스 >

○ **(시장)** '15년까지 전세계 스마트카 시장은 연평균 8.4%, 국내 시장은 연평균 12.4% 성장 전망

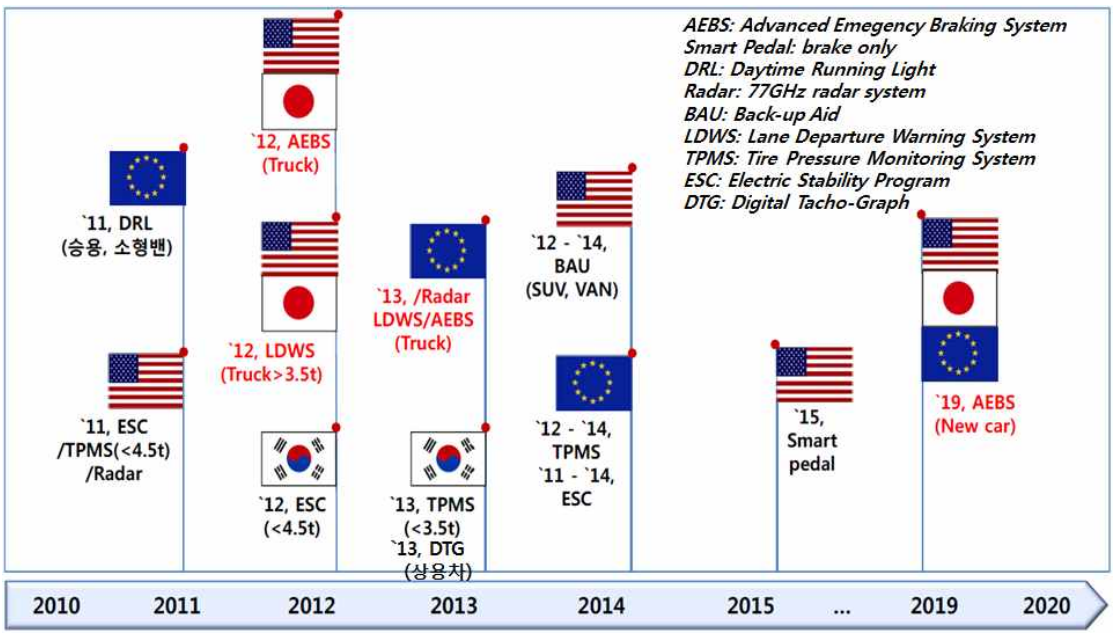
- '16년부터 다임러社가 차량 내부에 보안기능을 장착하기 시작하여 (전체 차량의 2%), '30년까지 99%가 장착될 것으로 예상

○ **(정책)** 주요 선진국들을 중심으로 차량 내 전자 안전장치 의무장착 추진

- 미국, 일본('12년), EU('13년)은 트럭을 대상으로 비상제동시스템(AEBS), 차선이탈경보장치(LDWS) 장착을 의무화하였으며 '19년까지 모든 신규 차량까지 확대 적용 예정

- 우리나라는 국토부에서 '13년 12월까지 상용차 대상 DTG 의무 장착 시행 및 교통안전공단에서 차량 주행정보를 수집 중

※ DTG(Digital TachoGraph) : 차량속도, RPM, 브레이크 사용기록, 위치정보, 운전시간 등 각종 차량 운행데이터를 초단위로 저장하는 디지털 운행기록계



< 주요국 차량 안전관련 의무 장착 현황 >

○ **(표준화)** ISO, GENIVI, CCC 등 글로벌 표준화 단체에서는 스마트카 및 관련 요소기술에 대한 다양한 표준화 활동 진행

- **(ISO)** TC22, TC204에서는 V2X 통신기술과 ITS 인프라 연동기술 표준화를 진행

- **(GENIVI)** 차량용 인포테인먼트 관련 플랫폼 표준화 진행

- **(CCC)** 차량과 스마트폰 연동기술 표준화 및 인증 등 수행

< 스마트카 표준 현황 >

표준단체	내 용
ISO TC22, TC204	스마트카 관련 국제 표준화는 ISO TC22와 TC204에서 주도하고 있으며 총 7개 SC, 42개 WG으로 구성 운영중. 특히 TC22는 자동차 부품에 대해 진행하고 TC204는 통신기술과 인프라관련 기술 표준 담당
GENIVI	Open Source기반의 차량 멀티미디어 표준 SW 플랫폼 표준화
CCC	미러링크 기술 표준화 및 미러링크 기술이 포함된 스마트폰, 헤드유닛, 애플리케이션은 모두 CCC에서 인증을 수행
AUTOSAR	자동차용 전자제어장치의 기능안전성과 상호호환성 향상을 목적으로 하며, 자동차 암호 서비스에 대한 스펙을 포함 ※ 개방형 자동차 표준 소프트웨어 구조로서, 주요 자동차 제조사와 자동차 전장부품 개발사들에 의해 개발
ISO 26262 (Functional Safety)	기능안전 국제표준(IEC 61508)을 자동차 전기/전자 시스템에 적용한 국제 표준으로 자동차에 탑재되는 소프트웨어의 오류로 인한 사고를 방지하기 위해 제정
WAVE (IEEE 1609)	자동차 전용 근거리 무선 통신 방식으로 차량간 통신 및 차량과 인프라간 통신 기술 표준화 ※ IEEE 1609.2에서는 지능형 자동차 네트워크의 보안 메시지 규격과 보안 통신을 위한 처리 절차를 기술

※ ISO TC22(Road Vehicles), ISO TC204(Intelligent Transport System), GENIVI(GENEVA In-Vehicle Infotainment) CCC(Car Connectivity Consortium), WAVE(Wireless Access in Vehicular Environments), AUTOSAR(AUTomotive Open System Architecture)

붙임 WAVE 표준의 종류 및 표준화 제정 현황

○ IEEE 1609.1 Resource Manager

- WAVE 자원 관리 애플리케이션의 서비스 및 인터페이스 정의
- WAVE 구조에서 제공되는 데이터 및 관리 서비스에 대해 기술하고, 명령어 메시지 및 그에 대응하는 응답 메시지의 포맷을 정의
- WAVE 규격 상의 개체 간 통신을 위한 애플리케이션의 데이터 저장 포맷 정의

○ IEEE 1609.2 Security Services for Applications and Management Messages

- 보안 메시지 규격과 보안 통신을 위한 처리 절차 기술
- 프라이버시 보호를 위한 익명 인증 메커니즘에 관한 표준화 진행중

○ IEEE 1609.3 Networking Services

- WAVE 데이터 교환을 위한 주소 체계 및 라우팅 방법을 포함하는 네트워크/전송 계층 서비스를 정의
- WAVE Short Message 프로토콜과 WAVE 프로토콜 스택을 위한 관리 정보(Management Information Base: MIB)를 기술

○ IEEE 1609.4 Multi-Channel Operation

- 제어 채널 및 서비스 채널로 구성되는 다중 채널을 지원하기 위한 MAC 계층 정의

< WAVE 표준화 현황 >

표준 번호	제 목
IEEE 1609.0	Architecture
IEEE 1609.1-2006	Resource Manager
IEEE 1609.2-2013	Security Services for Applications and Management Messages
IEEE 1609.3-2010	Networking Services
IEEE 1609.4-2010	Multi-Channel Operation
IEEE 1609.11-2010	Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation System (ITS)

2. 스마트카 주요 보안위협

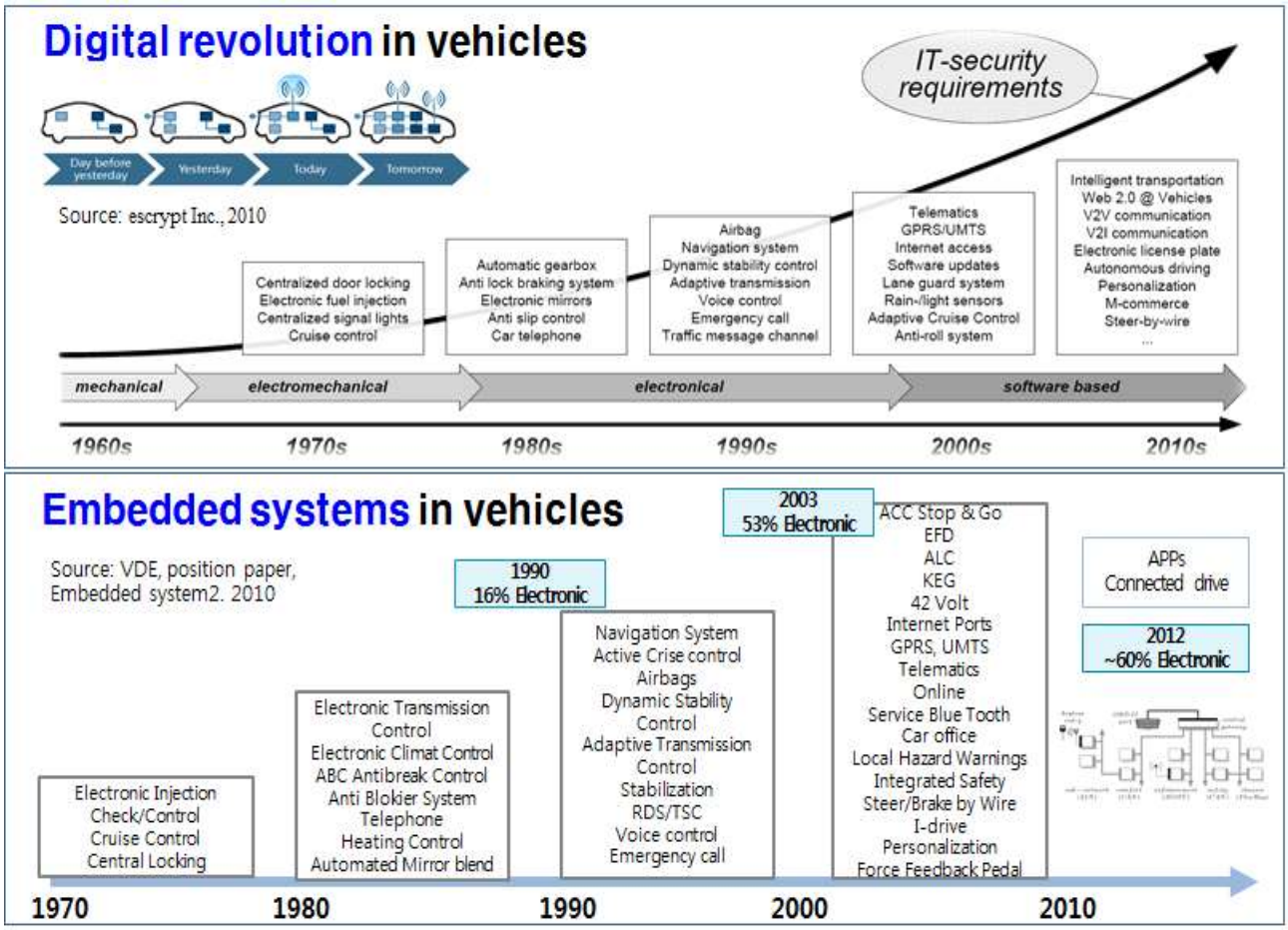
○ 기존 차량의 급격한 전자화 및 다양한 통신기능이 내장됨에 따라 발생할 수 있는 해킹, 오동작으로 인해 인간의 생명까지도 위협

- 차량 내부통신·처리 과정, OEM들이 제공하는 다양한 커넥티드 서비스에서의 정보유출 및 데이터 위·변조
- 정부의 교통 빅데이터 구축 시 프라이버시 침해, 해킹을 통한 도로 안전정보 위·변조에 따른 운전자 생명위협 등

○ 최근 차량의 주행거리계(Odometer) 조작이 경제적 손실이 가장 큰 보안위협으로 나타나는 추세

※ 미국에서는 한해 거래 중고차의 10~30%에 대해 주행거리가 조작

※ 독일의 경우 주행거리 조작으로 연간 60억유로, EU에서는 매년 96억유로의 손해 발생



< 스마트카의 발전에 따른 보안 위협 증대 >

< 스마트카 주요 보안위협 >

사용자 조작 미숙으로 인한 보안위협	
위 협	피 해
부적절한 세팅	사용자의 인포테인먼트 기능 사용시 의도하지 않은 서비스 제공자에게 개인 식별 정보 등이 전송되거나 통신 내용이 유출
바이러스 감염	인포테인먼트 디바이스 장치의 바이러스에 감염된 콘텐츠가 차량 내 LAN에 유포되어 차량에 탑재된 다른 기기를 감염

해커의 공격에 의한 보안위협	
위 협	피 해
인가되지 않은 사용	정비 공장 및 유지 보수 담당자 해킹 등을 통하여 외부 공격자가 차량의 전자기기에 접속하는 경우, 차량의 운행 조작이 가능
인가되지 않은 설정	장비의 패스워드나 암호화 설정 등이 취소되어 차량의 상태 정보가 해커에게 자동으로 전송되거나 ECU나 차량내 장비가 오작동
인가되지 않은 정보 접근	해커가 부적절한 세팅이나 취약점을 악용하여 차량내 프로그램, 콘텐츠, 운행 기록 등을 확인
스니핑	암호화되지 않고 평문으로 전송되는 TPMS 메시지 등은 타이어의 시리얼 번호 등을 포함하고 있어 자동차와 특정 개인을 연결가능하게 함에 따라, 운전자의 프라이버시를 침해할 수 있음
서비스 거부 공격	해커가 자동차의 텔레메틱스나 원격 제어와 관련된 포트에 대량의 패킷을 전송하여 자동차의 원격제어를 방해
메시지 변조	해커가 TPMS 메시지 등을 변조하여 이상알림 게기판의 조작이 가능한 경우, 자동차의 안정적인 운행에 침해 발생
로그 삭제	해커가 시스템 로그를 삭제하거나 변경하여 침입한 흔적을 삭제할 수 있으며, 로그가 기록되지 않도록 설정할 수 있음
무단 릴레이	스마트키 등을 위한 LF(Long Frequency) 주파수 대역에 해커가 침입하는 경우, 원격지에서 차량의 문을 개폐 가능

○ 미국, EU, 일본 등 주요 선진국에서는 스마트카 보안위협에 대응하기 위한 보안 요구사항 도출 및 관련 연구개발 수행

- **(EU)** 스마트카 보안사고로 경제적·사회적 파장이 클 것으로 예상하고 관련 보안 연구를 활발히 진행

  ※ 독일에서는 ECU용 보안(Light EVITA HSM), 차내 ECU간 통신 보안(Medium EVITA), 외부와 통신 보안(Full EVITA)으로 보안 기능을 정하고 4년동안 6백만유로의 연구비를 투입 → AUTOSAR 4.1.2에 반영하여 업체들이 적용하도록 권고

- **(미국)** 교통부(DoT)는 ITS 연구개발 중장기 전략(2010-2014)을 수립하고 ITS 보안강화를 위한 주요 과제들을 포함

- **(일본)** 미래성은 차량의 설계부터 폐차단계까지 사이버기록 관리 가이드라인을 마련

붙임 스마트카 보안위협 사례

구 분	내 용
CAN, 전장 ECU 해킹 시연 (2013)	데프콘에서 포드 이스케이프와 도요타 프리우스에 대해 CAN과 전장 ECU를 해킹한 코드를 공개 특히 포드 이스케이프는 미국 판매량 1위를 차지할 정도로 베스트셀링 차량이며 도요타 프리우스는 하이브리드카분야 전체계 판매량 1위(누적 300만대)를 차지한 차량이라는 점에서 보안 위협 발생 시 파급효과가 매우 클 것으로 예상 
고속도로 교통표시판 해킹 (2012)	미국의 고속도로 교통표시판(VMS)가 해킹되고 미국 주요 도시에 설치된 일부 교통제어시스템이 해킹에 노출 교통신호등의 경우 차량 검지를 위해 도로에 Sensys Networks社의 VDS240 매그네틱 센서에서 전달되는 교통상황 데이터에 대한 암호화 및 인증이 전혀 되어 있지 않은 것으로 나타남 ※ 미국은 '13년 NHTSA(도로교통국)산하에 보안위협관련 auto-safety regulator를 신설하고 차량과 ITS에 대한 사이버보안을 담당 
BMW 차량 300대 이상 도난 (2012)	해커들의 해킹 수법은 OBD-II의 보안 취약을 악용하여 BMW 차량 약 300대가 도난당했으며, 그 피해규모는 400억원으로 추정 최근 BMW, 아우디 등 고급차를 대상으로 GPS트래킹 등 사이버 보안 취약점을 악용한 신종 차량 절도 사고들이 지속적으로 발생