사물인터넷(IoT) 정보보호 로드맵 3개년 시행계획

2015. 6.

정보보호정책관
정보보호지원과

순 서

Ⅰ 추진배경

□ **사물인터넷**(IoT)은 홈 · 가전, 의료, 교통 등 다양한 산업분야에 적용되고 있으며, **본격적인 시장 활성화**가 **진행 중**

※ 세계적으로 '20년까지 인터넷에 연결되는 사물의 수는 약 260억개, IoT로 창출되는 부가가치는 약 1조 9천억 달러로 전망(가트너, '13)

○ 그러나, IoT는 **활용분야**가 우리 실생활의 **모든 사물**에 '**직접 접목**'되기 때문에, 기존 사이버공간의 **위험이 현실세계로 전이·확대**

- 때문에, **IoT 제품 · 서비스**의 **보안위협**에 대한 **우려가 점증**

< IoT 제품 · 서비스의 보안에 대한 우려들 >

- IoT 디바이스(기기)의 70%가 암호화되지 않은 네트워크를 통해 데이터를 전송하는 것으로 조사(HP, '14)
- 보안전문가 391명 대상 설문조사 결과, 2/3가 IoT 보안에 대해 우려하고 있다고 답변(SANS Institute, '13)
- 22%의 기업이 IoT로 인해 새로운 위협에 직면할 것이라 경고(가트너, '14)

○ 한편, IoT 디바이스는 생산 · 판매 이후에 유지보수, 보안 업데이트 적용 등 **사후 보안조치가 불가능**하거나 **高비용이 수반**

※ IoT 등 융합보안 침해사고에 따른 피해규모는 '15년 약 13조 4천억원에서 '30년 약 26조 7천억원에 이를 것으로 전망(산업연구원, '14.2)

□ 미래부는 IoT 제품 · 서비스의 취약한 보안 현실을 체계적으로 개선해 나가기 위해 「**사물인터넷(IoT) 정보보호 로드맵**」 **수립**('14.10)

○ 로드맵 과제를 체계적으로 추진하여, **IoT 보안**을 **창조경제 먹거리 산업화**하기 위해, **시행계획 마련** 필요

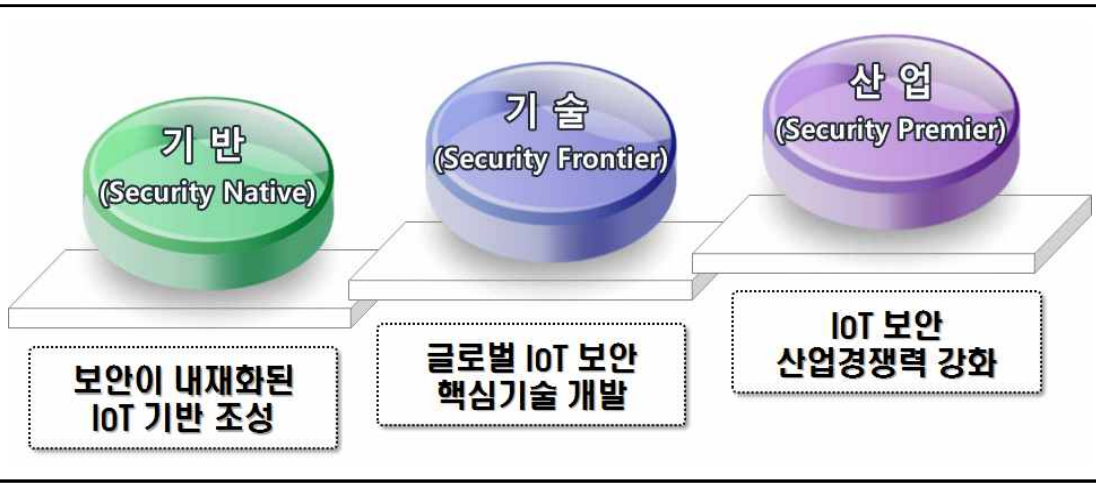
「사물인터넷(IoT) 정보보호 로드맵 3개년 시행계획」의 수립 · 이행을 통해 세계최고의 스마트 안심국가 실현을 본격추진

Ⅱ 비전 및 추진과제

비전

누구나 안전하게 사물인터넷의 편리함을 누리는 세계 최고의 스마트 안심국가 실현

추진 전략



추진 과제

1. Security Native : 보안이 내재화된 IoT 기반 조성
1-1. 7대 분야 IoT 제품 · 서비스 보안 내재화
1-2.「IoT 사이버위협 종합 대응체계」구축
1-3. 안전한 IoT 제품 · 서비스를 위한 신뢰성 확보
2. Security Frontier : 글로벌 IoT 보안 선도기술 개발
2-1. IoT 보안 9대 핵심 원천기술 개발
2-2. IoT R&D 오픈 이노베이션 체계 구축
3. Security Premier : IoT 보안 산업경쟁력 강화
3-1. IoT 보안 우수기업 발굴·육성
3-2. IoT 보안 제품 · 서비스 수요 창출
3-3. ICT와 Security가 결합된 맞춤형「IoT Security Brain」 양성

Ⅲ 세부 시행계획

1. 보안이 내재화된 IoT 기반 조성

1-1. 7대 분야 IoT 제품·서비스 보안 내재화

□ 추진배경

○ IoT 제품 생산, 서비스 제공시 활용 가능한 보안 고려사항 개발 및 민간 자율적용 유도를 통해 **IoT 제품·서비스의 보안 내재화** 촉진

- IoT 제품 · 서비스 **개발 초기**에 **안전성**을 **확보**하여, 국민피해 예방

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) 홈 · 가전, 의료, 교통(스마트 카 · ITS), 환경 · 재난, 제조, 건설, 에너지 등 **7대 IoT 분야**의 **공통 보안원칙**과 **분야별 보안 고려사항** 개발

① IoT 관련 사업자가 제품 생산, 서비스 제공시 **보안성 확보**를 위해 **기본적**으로 **고려할 사항**인 **'공통 보안원칙' 개발 · 보급**

○ IoT 제품 · 서비스 **생산단계**(설계-개발-운영)를 **고려**하여 마련('15)

* 산 · 학 · 연 전문가 자문단에서 심층검토 후 확정 · 공표

○ **스마트챌린지** 사업에 **시범적용***하여 **실효성 검증** 및 **개선**('15~)

* (대상) 글로벌 스마트시티 실증단지, 수요연계형 Daily-Healthcare 실증단지 등

< IoT 공통 보안원칙 항목(예시) >

설계	1. **정보보호**와 **프라이버시 강화**를 **고려**한 IoT 제품·서비스 설계 2. **안전한** 소프트웨어 및 하드웨어 **개발 기술 적용** 및 **검증**
운영	3. **사용자 편의 중심**의 **보안 설정/구성 기술** 제공 4. **표준화된 보안 프로토콜 준수** 및 안전한 파라미터 설정
관리	5. IoT 제품의 취약점 **보안패치 및 업데이트 지속 이행** 6. 안전한 운영·관리를 위한 **정보보호 및 프라이버시 관리체계 마련** 7. IoT **침해사고 대응체계** 및 책임추적성 확보 방안 마련

② 7대 IoT 분야별 **'보안가이드'**(세부 보안 고려사항) **개발** 기술지원('16~)

○ 보안가이드 개발을 위한 사전 작업으로써 **IoT 보안 관련 산업 실태파악** 및 **'공통 보안 요구사항*'** **도출**('15)

* IoT 제품 및 서비스 보안성 강화방안 연구 추진 중('15.4~)

○ '공통 보안 요구사항'을 기초로 7대 IoT 분야에 공통적으로 활용 가능한 **'공통보안 가이드' 마련**('16)

○ 관계부처, 관련 제조업계 등과 협업하여 **'7대 IoT 분야별 보안 가이드'** 개발 가능하도록 **기술지원**('17~)

< 공통 보안원칙 및 보안가이드 관계 >

공통 보안원칙	▶	공통 보안가이드	▶	분야별 보안가이드
IoT가 **기본적**으로 갖추어야할 **보안원칙**		IoT에 **공통적으로 요구**되는 **보안사항** (공통 보안원칙 구체화)		**각 IoT 서비스별로 특화**된 **보안 요구사항**

< 공통 보안원칙, 공통 보안가이드 및 서비스별 보안가이드 주요내용(예시) >

<table>
<tr><th>구분</th><th>주요내용(예시)</th></tr>
<tr><td>공통보안 원칙 (설계)</td><td>1. 정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계
2. 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증</td></tr>
<tr><td>공통보안 가이드 (설계)</td><td>< ① 정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계 >
- Privacy by Design" 및 "Security by Design" 기본 원칙 준수
<table>
<tr><th>기본 원칙</th><th>Privacy by Design</th><th>Security By Design</th></tr>
<tr><td>지속적인 선제 방어 (Proactive not Reactive)</td><td>침해(위협) 후 대응이 아닌 침해 발생 전 프라이버시 위협 방어 고민 및 예측</td><td>설계 시작부터 서비스의 종료까지를 고려하여, 보안이 지속(proactive) 구현 될 수 있도록 다양한 방법론 활용</td></tr>
<tr><td>기본 설정 (Default Setting)</td><td>사용할 ICT 시스템이나 사업 관행에 프라이버시 보호 방법론을 기본 포함</td><td>최소 권한 설정, 지식 한정, 최소 신용, 접근제어 필수, 의무(권한) 분리 등을 포함한 기본 보안 정책의 구현</td></tr>
</table>
</td></tr>
</table>

설계 단계에 포함 (Embedded into Design)	ICT 시스템 구조와 사업 구조의 설계에 프라이버시 보호 고려 사항 포함	소프트웨어 보안 보증 항목들을 적용하고, TPM과 같은 하드웨어 기술 적용 고려
포지티브 섬 (Positive Sum)	제로섬을 고려한 트레이드 오프의 관점에서 모든 구성 요소 및 구성원이 상호 이득을 볼 수 있는 구조 설계	제로섬을 고려한 트레이드 오프의 관점에서 모든 구성 요소 및 구성원이 상호 이득을 볼 수 있는 구조 설계
종단 간 보안 (end-to-end Security)	정보의 전주기 및 실행 주체 간의 종단 간 보호	종단 간의 관점에서 구성 요소 및 구성원의 정보 보호
가시화와 투명성 (Visibility and Transparency)	ICT 시스템과 사업 수행의 구성 요소들을 사용자 및 서비스 제공자에게 가시화하고 투명성 보장	잘 알려져 있는 기능과 외부 검증이 수행되어진 공개 표준 기반의 보안 기술 활용
사용자 중심 (Respect for the User)	개개인의 정보 및 자원 보호에서 사용자 중심 우선 고려	개인 및 기업을 모두 고려한 수요자 중심 보호 기술

< ② 안전한 소프트웨어 및 하드웨어 개발 기술 적용 및 검증 >

- 시큐어 코딩, 오픈소스 보안성 검증 및 시큐어 하드웨어 장치 활용

< C/C++ 시큐어 코딩 가이드 구성 >

유 형	내 용
입력 데이터 검증 및 표현	프로그램 입력값에 대한 검증 누락 또는 부적절한 검증, 데이터의 잘못된 형식지정으로 인해 발생할 수 있는 보안약점
보안 기능	보안기능(인증, 접근제어, 기밀성, 암호화, 권한관리 등)을 적절하지 않게 구현시 발생할 수 있는 보안약점
시간 및 상태	동시 또는 거의 동시 수행을 지원하는 병렬 시스템, 하나 이상의 프로세스가 동작하는 환경에서 시간 및 상태를 부적절하게 관리하여 발생할 수 있는 보안약점
에러 처리	에러를 처리하지 않거나, 불충분하게 처리하여 에러정보에 중요정보(시스템 등)가 포함될 때 발생할 수 있는 보안약점

코드 오류	타입 변환 오류, 자원(메모리 등)의 부적절한 반환 등과 같이 개발자가 범할 수 있는 코딩오류로 인해 유발되는 보안약점
캡슐화	중요한 데이터 또는 기능성을 불충분하게 캡슐화 하였을 때, 인가되지 않는 사용자에게 데이터 누출이 가능해지는 보안약점
API 오용	의도된 사용에 반하는 방법으로 API를 사용하거나, 보안에 취약한 API를 사용하여 발생할 수 있는 보안약점

< 오픈소스 취약점 점검 내용 >

유 형	내 용
의존S/W 열거	사용한 상용・오픈소스 S/W를 포함하여 의존성을 가지는 모든 S/W 열거하고 찾아야 함
취약점 검색	열거된 의존 S/W에 대한 취약점을 모두 검색 필요
취약점/ 대응방법 열거	S/W 별로 알려진 취약점을 모두 열거
대응방법 반영	알려진 취약점에 대한 대응절차에 따라 오픈소스 S/W에 반영하여 보완해야 함

< 시큐어 하드웨어 장치 활용 >

IoT 디바이스는 응용 서비스 종류에 따라 다양한 수준의 보안 강도를 필요로 한다. IoT 디바이스는 공격자에게 쉽게 노출될 수 있는 환경에 주로 설치되기 때문에 부채널 공격이나 펌웨어 코드 추출, 키 값 추출 등 다양한 하드웨어 보안 취약성을 갖는다. 이 때문에 하드웨어 보안성을 강화하기 위해, TPM(Trusted Platform Module)이나 HSM(Hardware Security Module), Trust Zone, JTAG 보안, 펌웨어/코드 암호화, 실행코드 영역제어, 역공학 방지 기법 등 다양한 하드웨어 보안 기법이 존재하며 이를 디바이스 서비스 응용 환경에 따라 적절히 적용할 필요가 있다.

분야별 보안가이드

< 홈·가전 >

- o 스마트홈·가전 디바이스는 출시전 보안취약점 점검을 의무적으로 실시하고, 출시 후에도 제조사는 지속적으로 보안패치 적용 및 배포
- o 개인정보의 저장·관리, 음성·영상 저장기능이 장착된 디바이스의 경우, 프라이버시 보호를 위한 사용자 인증 및 접근제어 기능 적용
- o 원격제어 기능이 탑재된 스마트 홈·가전 디바이스는 외부 비인가 접근을 방지하기 위한 사용자 인증 및 암호화 통신 기능 적용

	< 의료 > o 개인 · 질병정보를 저장·처리하는 의료장비 및 이와 연동되는 데이터 처리장치는 프라이버시 보호를 위한 인증 및 암호화 기능 적용 o 의료 디바이스에 대해 정기적인 취약점 검증을 수행하고, 국제 표준을 고려한 보안관리 체계 적용 o 스마트의료 서비스로 수집·관리·공유되는 개인정보 보호방안 마련 < 교통 > o ABS, TPMS 등 자동차 주행, 구동장치의 중단/오작동을 방지하기 위한 보안기능(데이터 암호화·복구, 비인가 접근통제 등)을 적용 o 전자제어시스템(ECU)과 연동된 각종 전자시스템은 정기적 취약점 점검 및 보안패치 적용, SW 안전성 검사 수행 o 디지털 운행기록계(Digital Tachograph)를 통해 수집되는 정보의 안전한 저장·관리를 위해 ITS는 DB 보안기술 적용 o ITS의 차량검지센서, 노변장치에서 전달되는 모든 교통 데이터는 암호화가 이루어져야 하며 각 장치에 대한 인증기술 적용

□ 주요 추진일정

추진내용	추진일정					
	'15년				'16	'17
	1/4	2/4	3/4	4/4		
① IoT 제품·서비스 '공통 보안원칙' 개발·보급						
- IoT 공통 보안원칙 마련		○				
- 스마트챌린지 사업 시범적용		○	○	○	○	○
② 7대 IoT 분야별 '보안가이드' 개발 기술지원						
- IoT 정보보호 실태 파악 및 공통보안 요구사항 도출			○	○		
- IoT 공통 보안가이드 마련					○	
- IoT 서비스 분야별 보안가이드 개발 지원						○

1-2. 「IoT 보안 위협 종합 대응체계」 구축

□ 추진배경

○ **IoT 보안위협**에 대비하기 위한 공동 대응체계 확립 및 IoT 핵심 인프라의 보안 강화를 통해 **피해예방 및 최소화**

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) IoT 제조·보안업체 등이 참여하는 **보안 협의체 구성**, IoT 인프라의 **보호 강화**, **IoT 보안 위협 대응체계 구축**

① IoT 보안 협의체 구성

○ IoT 보안정책 수립 등을 위한 이슈 논의와 기술·정책 자문을 위해 **'IoT 보안 얼라이언스*'**를 **구성·운영**('15~)

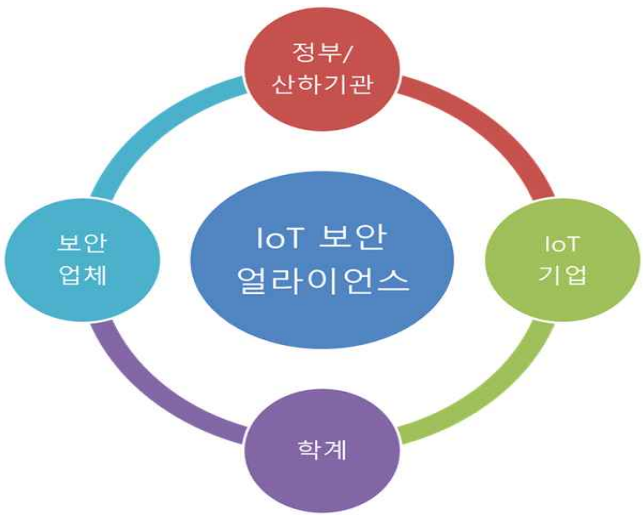
* 정부/산하기관, IoT 제조업체, 보안업체, 학계 등 총 50여개 기관으로 구성

※ IoT 분야는 얼라이언스를 중심으로 표준 및 시장 주도권 확보를 위해 노력하는 것이 국내외 트랜드

- **연 2회 정기적인 회의**을 통해 IoT 보안 관련 **제도개선 방안** 논의, 보안 가이드 개발 지원, **보안 인증제도 관련 검토** 등을 실시

※ 금년 상반기('15.6) 발대식 개최 예정

< IoT 보안 얼라이언스 구성 >



< IoT 보안 얼라이언스 주요 기능(예) >

o IoT 공통 보안원칙에 기반한 **공통 보안 가이드 개발**
o IoT 보안 **인증제도** 평가항목 및 기준, 운영지침 검토
o IoT 보안 **취약요소**에 따른 **보호조치 적용방안** 협의
o IoT 보안 관련 **제도 및 정책** 논의
o 이종 네트워크, 플랫폼간 상호 호환성 및 기술 **표준사항** 등 협의
o IoT **기업**과 **보안업체**간 **신제품·서비스 수요 발굴** 등을 위한 협업 지원

② IoT 인프라 보안 강화

○ 침해사고 발생시 국민생활 등에 큰 영향을 끼치는 IoT 인프라에 대해 **'주요정보통신기반시설*' 신규 지정** 및 **보호체계 강화**('15~)

* 정보통신기반시설중 중요성, 침해시 피해규모 및 범위 등을 고려하여 전자적 침해행위로부터의 보호가 필요하다고 지정되는 시설

- 에너지, 제조, 의료분야에 대해 **주요정보통신기반시설 신규지정**을 위한 **실태조사**(서면, 현장조사 등) 및 **평가** 수행('15)

< 실태조사 추진계획 >

대상시설 파악 및 **조사항목 마련**	→	**서면조사** (약 80개 시설)	→	**현장조사** (약 60개 시설)	→	지정평가반 구성 및 **평가** (약 30개 시설)

- 실태조사, 평가 및 심의결과 등을 다각도로 검토하여 **'주요정보통신기반시설' 신규지정 추진**('16~)

< 주요정보통신기반시설 지정절차 >

1단계		2단계		3단계		4단계		5단계
지정 기준 수립	→	평가반 구성 및 평가 수행	→	평가 결과 심사	→	지정여부 심의	→	저정시설 고시
중앙행정기관		대상 기관		중앙행정기관		정보통신기반 보호위원회		중앙행정기관

- 신규 주요정보통신기반시설에 대한 **취약점분석, 이행점검** 실시('16~)

※「정보통신기반보호법」에 따라 주요정보통신기반시설로서 보호·점검

○ 전체 **주요정보통신기반시설 중 IoT 인프라를 보유한 시설**에 대해 IoT 보안 관련 **모의해킹 훈련** 등 대응역량 점검 추진('17)

③ ‘IoT 보안위협 대응체계’ 구축 추진

○ 정보통신, 금융, 지자체 등 **기 설립된 ISAC***에서 각 분야의 **IoT 보안관련 취약점 공유·분석** 등의 기능수행 추진('15~)

* 정보공유분석센터(Information Sharing Analysis Center)

< 국내 ISAC 현황 >

구 분	설 립	운영주체	회원사
정보통신ISAC	'13. 02	한국정보통신진흥협회	기간통신사업자
금융ISAC	'15. 04	금융보안원	국내금융기관
지자체 ISAC	'13. 02	지역정보개발원	지방자치단체

○ ISAC 설립 필요성이 높고, IoT 디바이스 활용도가 높은 **에너지, 의료, 교육** 분야 등에 대한 신규 **ISAC 설립 필요성*** 검토('16~)

○ 기 설립된 **분야별 ISAC**을 위한 **총괄체계 구축** 검토('17~)

□ 주요 추진일정

추진내용	추진일정					
	‘15년				‘16	‘17
	1/4	2/4	3/4	4/4		
① IoT 보안 협의체 구성						
- 발대식 및 제1회 정책 세미나 개최		○				
- 주요 IoT 보안이슈 검토 등 정기적 회합			○	○	○	○
② IoT 인프라 보안 강화						
- 주요정보통시기반시설 신규지정을 위한 실태조사				○	○	○
- 주요정보통신기반시설 지정 및 보안체계 강화					○	○
③ ‘IoT 보안위협 대응체계’ 구축 추진						
- 기 설립된 ISAC의 IoT 보안관련 기능 수행 추진 검토				○	○	○
- 에너지, 의료, 교육 분야 ISAC 설립 필요성 검토					○	○
- 분야별 ISAC 총괄 관리체계 설립 등 검토						○

1-3. 안전한 IoT 제품·서비스를 위한 신뢰성 확보

□ 추진배경

○ IoT 제품 및 서비스 사업자의 책임강화와 디바이스 인증 등을 통해 **IoT 제품·서비스**의 **안전한 개발, 유통, 관리** 도모

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) **IoT 제품·서비스**에 대한 **제조사**의 **책임성**을 **확보**하고, **보안인증 도입**을 **검토** 등

① IoT 제품·서비스 사업자에 대한 책임성 확보

○ IoT 제품·서비스의 **설계단계**부터 **보안적용, 사후관리**(보안패치, S/W 업데이트) 등 전 단계에 걸쳐 **책임성 확보**를 위한 **연구*** **추진**('15)

* IoT 제품·서비스 책임강화 방안 연구('15.4~10월, 4,000만원)

※ IoT 환경은 각각 다른 종류·제조사의 센서·디바이스가 상호 연결되므로 보안문제 발생 시, 기술적·제도적 책임규명이 어려운 상황

- 국내외 기업의 IoT 제품·서비스의 불충분한 보안 조치로 사용자에게 손해 발생시의 **피해구제 방안** 등을 **검토**

○ **IoT 제품·서비스 사업자**의 **책임성 확보방안 마련** 추진('16~)

- IoT 제품 및 서비스의 **보안취약점**과 **보호조치 사항**(S/W 및 보안 업데이트 등)을 홈페이지 등을 통하여 **제품 사용자에게 공개** 추진

- IoT 제품 및 서비스 출시후 발견된 **신규 보안취약점**에 대해서는 **사후관리**(보안업데이트) 등 지속적인 **보안 강화방안 제공*** 추진

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

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

② 'IoT 디바이스 보안 인증' 제도 추진

○ 7대 IoT 분야 디바이스에 공통 적용이 가능한 기술적·관리적 보안 **인증항목 도출** 및 **인증제도 도입방안 사전연구*** **수행**('15)

* IoT 디바이스 보안인증 기반 연구('15.4~10월, 4,000만원)

○ 'IoT 보안 얼라이언스'에 **'IoT 디바이스 보안인증 분과'**를 **설치**하여 글로벌 표준에 부합한 보안인증 항목* 공통 규격화 추진('16)

* 프로토콜 적합성, 상호운용성, 보안기능·성능 검증 등

※ 자동차, 의료 등 분야별 디바이스 인증시 인증요건과 충돌되지 않도록 추진

○ 공통 인증규격을 기반으로 **'민간 자율의 7대 IoT 분야별 디바이스 보안인증 방안'**을 **마련**하고, 시범운영 후 인증제 도입 추진('16~)

- 인증기준이 없는 신규 IoT 제품·서비스에 대해서는 신규 항목 및 기준을 개발·적용한 **'IoT Security Verified*'** 제도 운영검토('17~)

* Verified : 자체적으로 정한 기준에 따라 시험 후 통과하면 인증마크 부여

□ 주요 추진일정

추진내용	추진일정					
	'15년				'16	'17
	1/4	2/4	3/4	4/4		
① IoT 제품·서비스 사업자에 대한 책임성 확보						
- IoT 보안이슈에 따른 책임성 확보 사전연구			○	○		
- IoT 책임성 확보 관련 의견수렴				○		
- IoT 책임강화를 위한 관련 제도 개선					○	○
② IoT 디바이스 보안 인증 제도 추진						
- IoT 보안인증 항목 개발 및 도입 방안 연구		○	○	○		
- 인증기관 대상 IoT 보안인증 항목 공통 규격화					○	
- 7대 IoT 서비스 분야 인증제도 시행					○	○
- IoT Security Verified 제도 시범운영						○

2. 글로벌 IoT 보안 선도기술 개발

2-1. IoT 보안 핵심 원천기술 개발

□ 추진배경

○ IoT 3계층(디바이스, 네트워크, 서비스/플랫폼)의 보안관련 9대 핵심 원천기술을 개발하여 **IoT 제품·서비스의 안전성 강화**

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) IoT 디바이스, 네트워크, 서비스 환경과 관련된 **9대 IoT 보안 핵심 원천기술 개발**

① (**IoT 디바이스**) CPU 성능, 전력상태 등을 고려한 **경량·저전력 암호기술, 보안 콘트롤러 칩**(SoC) 및 **보안 운영체제** 개발 추진

○ **암호기술**을 IoT 서비스에 적용할 수 있도록 **경량·저전력화**하되, 특정 IoT 분야에 국한되지 않도록 **개방형**으로 개발

* 다양한 IoT 서비스 개발을 위한 경량암호/인증 보안 라이브러리 개발 ('15~'16, '15년 4억)

- 향후, 신규 개발된 **경량·저전력 암호를 탑재하기 위한 SW 모듈**을 **개발**하여 IoT 디바이스 및 네트워크 플랫폼에 적용

○ 웨어러블 디바이스, 초소형 센서 등에 대한 **위변조, 부채널공격***을 **방지**하는 **보안 콘트롤러 칩**(SoC) **개발****('15~)

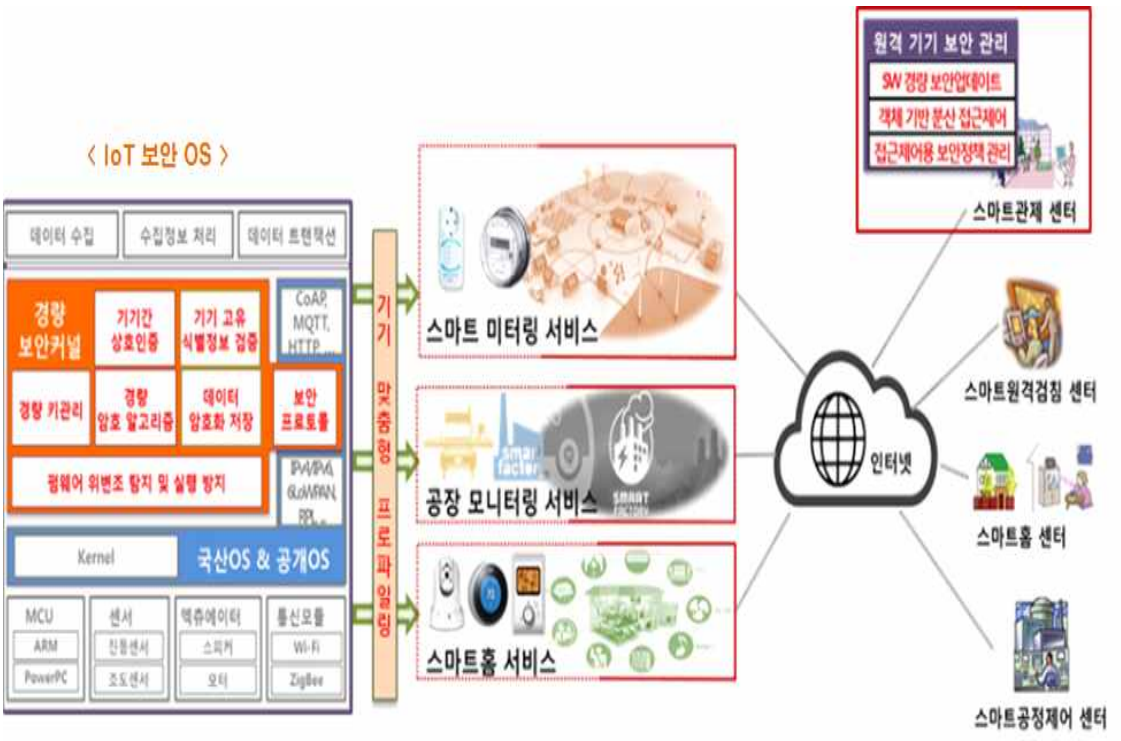
* IoT 디바이스에서 발생한 전자파, 전력소모량 등을 탐지·분석하여 암호키 탈취
** IoT 디바이스 보안을 위한 콘트롤러 칩(SoC)세트 개발('15~'16, '15년 9.5억)

○ 디바이스 핵심자원(OS, 개인정보 등)에 대한 **비인가 접근차단, 위·변조 방지** 기능 등이 내재된 **보안 운영체제**(Secure OS) **개발***('15~)

* 스마트 경량 IoT 디바이스용 운영체제 보안 핵심 기술개발('15~'17, '15년 27억)

- 펌웨어 위변조 탐지, 디바이스 고유 식별정보 검증 등 IoT 보안 OS의 핵심인 **경량 보안커널 기술**을 포함하여 개발

< IoT 보안 운영체제 >



② **(IoT 네트워크)** 이종 네트워크 간 안전한 통신을 위한 IoT **보안 게이트웨이, 침입 탐지·대응 기술**과 **원격 보안 관리·관제 기술** 개발

○ 신뢰/비신뢰 디바이스, 이종 네트워크 간 상호연결성과 보안통신을 제공하는 **IoT 보안 게이트웨이*** **개발 추진**('16~)

* IoT 서비스 분야별로 달리 요구되는 디바이스 간 연결 통신 방식(WAVE, AllJoyn 등), 트래픽 특성 등을 고려한 보안기능 제공

- 7대 IoT 분야별로 네트워크 보안 특성을 반영하여 순차적으로 개발하되, **3대 IoT 분야***에 대해 **우선 개발** 추진

* 홈·가전(디바이스 상호연결 통신보안, 사용자 프라이버시 보호 등), 의료(침입방지시스템 등), 자동차(침입방지시스템, 차량 내외부간 통신보안 등)

○ IoT 디바이스, 네트워크의 물리적/행위적 이상징후를 탐지하여 실시간 대응하는 **클라우드 기반 IoT 침입탐지·대응 기술*** 개발('16~)

* IoT 디바이스 공격과 오동작 등을 클라우드에서 집중 처리·분석·판단하여 실시간 공격탐지가 가능한 '소프트웨어 정의 네트워크' 기반의 동적 침입방지기술

○ 무선기기의 보안상태를 모니터링하여 보안SW, 규칙, 정책 등을 자동으로 업데이트하는 **IoT 원격 보안관리 · 관제 기술 개발**('16~)

③ **(IoT 서비스환경)** 각종 IoT 서비스 환경에 적합한 스마트 인증, IoT 프라이버시 보호기술 및 **IoT 보안솔루션 기술 개발**

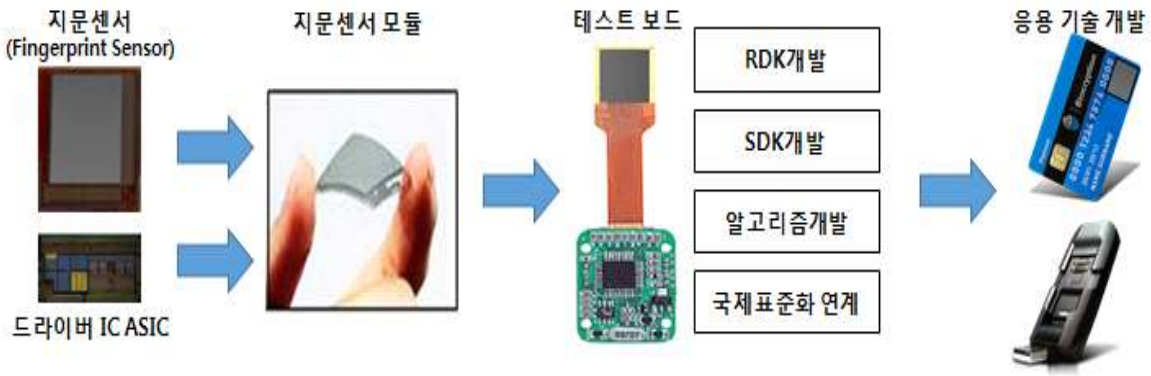
○ 생체정보를 이용하여 사용자 인증과 디바이스 접근권한 관리 기능을 제공하는 **스마트 디바이스용 인증기술*** **개발****('15~)

* 전통적인 PKI 인증 기술 등에서 벗어난 IoT 환경에 특화된 경량 PKI 인증 기술개발 등 필요

** 스마트 디바이스용 박막 타입 지문센서 모듈 및 프라이버시 보호 응용 소프트웨어 기술 개발('15~'17, 7.4억)

- 필름 형태의 초음파식 **박막형 센서**와 **저전력 H/W 모듈** 및 IC카드 기반의 프라이버시 **보호형 모바일 지문인식** 기술 활용

< 스마트 디바이스용 인증기술(예시) >



○ IoT 서비스 분야별 기술특성(프로토콜, 요구표준 등)을 고려하여 최적화된 **IoT 보안 솔루션*** **개발**('16~)

* (홈 · 가전) 개인정보 · 프라이버시 보호를 위한 암호화, (교통) 차량용 고속 보안통신, (의료) 고가용성 · 실시간성이 보장되는 접근제어 등

○ 비정형 IoT 빅데이터를 실시간으로 분석하여 민감정보 노출 위험을 탐지 · 제거하는 **프라이버시 보호기술 기술 개발**('17~)

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

□ 주요 추진일정

추진내용	추진일정					
	‘15년				‘16	‘17
	1/4	2/4	3/4	4/4		
① **IoT 디바이스 관련 보안기술 개발**						
- 경량·저전력 암호 기술개발		○	○	○	○	
- 디바이스 위변조 방지용 보안 SoC 개발		○	○	○	○	
- IoT 보안 운영체제 개발		○	○	○	○	○
② **IoT 네트워크 관련 보안기술 개발**						
- IoT 보안 게이트웨이 개발					○	○
- IoT 침입탐지·대응기술 개발					○	○
- IoT 원격 보안관리·관제기술 개발					○	○
③ **IoT 서비스환경 관련 보안기술 개발**						
- 스마트 인증기술		○	○	○	○	○
- IoT 보안솔루션 개발					○	○
- IoT 프라이버시 보호 기술						○

2-2. IoT R&D 오픈 이노베이션 구축

□ 추진배경

○ 빠르게 변화하는 IoT 보안기술 시장에 대한 **R&D 적시성 강화** 및 보안 선도국가와의 국제공동연구를 통해 **글로벌 역량 강화**

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) IoT **R&D 오디션 프로그램** 도입, IoT 보안 R&D **국제협력** 및 **표준화** 추진

① IoT R&D 오디션 프로그램 도입

○ IoT 기술 및 시장 요구사항에 유연한 대응을 위해 **경쟁형*** **IoT R&D 오디션 프로그램** 도입('15~)

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

- '다양한 IoT 서비스 개발을 위한 경량 암호/인증 보안 라이브러리 개발 사업' R&D 과제에 대해 우선 추진

* 2개 사업자를 선정하여 금년에는 사업자별로 2억원씩 지원한 후, 평가를 거쳐 1개 사업자를 선정하여 '16년에 4억원으로 확대 지원

② IoT R&D 국제협력 및 표준화

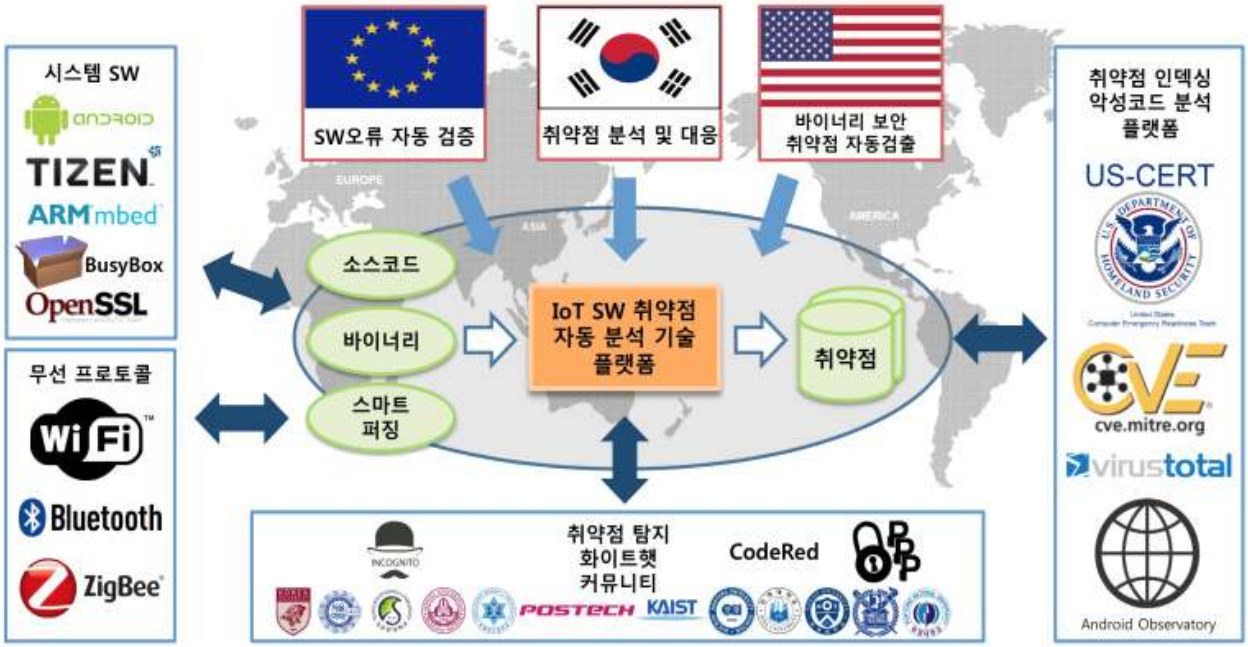
○ 미국, 유럽 등 IoT 보안 선도기술 및 실용화 기술 보유기관 등과 **국제협력**을 통해 R&D IoT 보안분야 글로벌 역량 강화('15~)

- IoT 디바이스의 시스템 SW와 **무선 프로토콜**의 **보안 취약점 자동 분석 기술** 및 통합플랫폼 개발을 위한 **한·미·EU 공동연구** 추진

※ 고려대 · KISA(한국), 카네기멜론大(미국), 옥스퍼드大(영국), ETH(스위스) 등

- IoT 디바이스를 외부 서비스 거부 공격으로부터 방어하기 위한 **시큐어 하드웨어 컨테이너 기술 개발**을 위한 **한·미 공동연구 추진**

※ ETRI(한국), UC 버클리, 조지 메이슨大(미국) 등



○ 홈·가전, 교통, 의료 등 IoT 분야별 시장수요와 기술 경쟁력을 고려하여 **IoT 보안기술의 국제 표준화**('16~)를 추진

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

□ 주요 추진일정

추진내용	추진일정					
	'15년				'16	'17
	1/4	2/4	3/4	4/4		
① IoT R&D 오디션 프로그램 도입						
- 경쟁형 IoT R&D 오디션 프로그램 추진		○	○	○	○	○
② IoT R&D 국제협력 및 표준화						
- IoT R&D 국제협력		○	○	○	○	
- IoT 보안기술 국제 표준화					○	○

3. IoT 보안 산업경쟁력 강화

3-1. IoT 보안 우수기업 발굴·육성

□ 추진배경

○ IoT 보안기술을 보유한 스타트업 기업의 육성을 지원하고, 보안 기술의 테스트 환경을 구축하여 **IoT 보안산업 활성화의 기반 마련**

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) IoT **보안 스타트업** 기업 지원, IoT **시큐리티 센터** 구축 및 IoT·**융합보안 시범사업** 추진

① IoT 보안 스타트업(Startup) 지원

○ 기 추진중인 **스타트업 프로그램**內에 **IoT 보안분야**를 **추가**하여 기획·개발·테스트·투자유치·해외진출 등을 원스톱 지원('15)

- **'K-글로벌 스타트업' 등과 연계***하여 **IoT 보안 스타트업**(5개 내외) **선정** 및 전문가 멘토링, 개발 인프라 제공, 창업화 교육 등 지원

※ K-글로벌 스타트업 및 K-글로벌 IoT 스타트업 챌린지와 연계

< IoT 보안 스타트업 주요 추진일정 >

4월	▶	5월	▶	~10월	▶	11월
모집 공고		대상 선정		개발, 사업화 지원		결과물 심사, 시상

< '15년 정보보호 스타트업 발굴·육성 팀 수 >

단계유형	대상	연계 프로그램	선발팀 수	추진시기
발굴·육성	예비 창업자	ㅇ K-글로벌 : 스타트업	5개팀 내외	3월~9월
		ㅇ K-글로벌 : IoT 스타트업 챌린지	5개팀 내외	5월~11월

- **IoT 보안분야**에 특화된 **스타트업 지원 프로그램** 개발 추진('16~)

○ 스타트업 선정 팀 대상으로 창의적인 보안기술 및 서비스 모델 발굴을 위한 **'IoT Security Innovation Contest*'** 개최 추진('16~)

* 우수 IoT 보안 스타트업 제품 또는 서비스의 취약점을 해결하기 위한 **아이디어, 보안기술** 등을 **심사**하여 **예산 또는 해외진출 지원**

② IoT 시큐리티 센터 구축

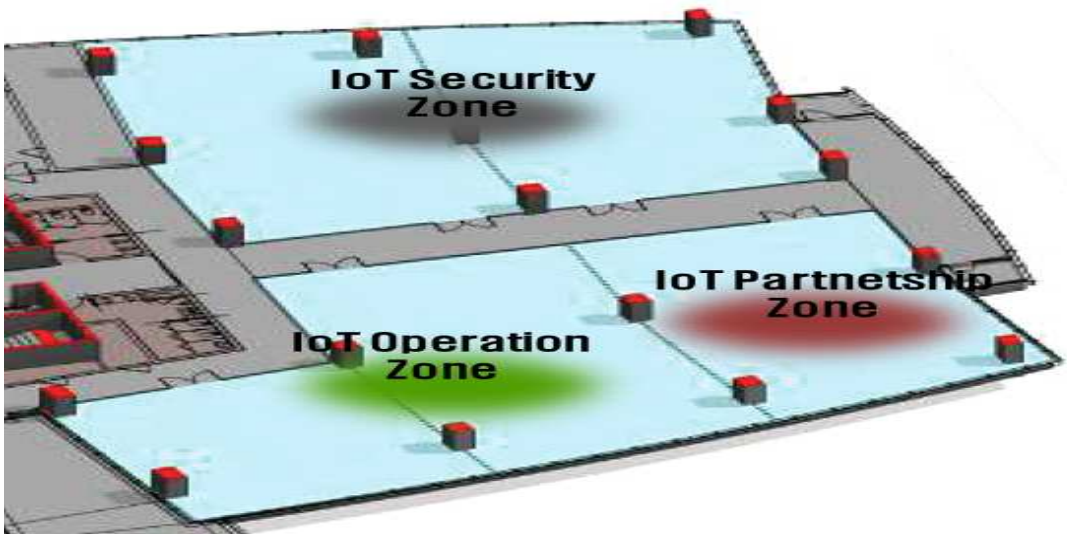
○ 보안 스타트업 육성, IoT 보안 실증사업에 대한 컨설팅, 기술지원 등 **IoT 보안 관련 기업 지원업무**를 위한 **'IoT 시큐리티 센터*' 구축**('15)

* IoT 혁신센터와 연계하여 구축하고 '16년 중 산학연 R&D센터(판교) 이전 예정

○ IoT 제품의 공통 적용되는 보안사항의 검증, 시험 등을 위한 **'IoT 보안 테스트베드'**를 **'IoT 시큐리티 센터' 內 구축**('15)

- 7대 IoT 분야별 보안특성을 반영한 보안성능 검증 및 시험환경 제공을 위해 **IoT 보안 테스트베드 확대 설치 추진**('16~)

< IoT 보안 테스트베드 배치계획(안) >



< IoT 보안 테스트베드 구축 필요성 >

o 많은 IoT 디바이스들에 어떤 보안기능을 탑재해야 하는지 몰라 보안을 고려하지 않고 출시되고 있으며, 보안기능을 탑재하더라도 적합성 여부를 판단할 수 있는 인프라 부재

- HP社에서 수행한 IoT 제품 보안수준 점검 결과('14)

* 70%의 IoT 디바이스는 통신과정에서 암호화를 수행하지 않음

* 80%의 디바이스 및 이와 연동된 애플리케이션에서 취약한 패스워드 인증방식 사용

* 90%의 IoT 디바이스, 클라우드 및 모바일 앱에서 최소 1가지 이상 개인정보 수집

③ IoT 보안 실증사업 추진

○ **스마트챌린지** 사업 등 IoT 실증사업의 보안 취약점 점검 및 보호대책 결과를 기반으로 **IoT 보안실증 사업을 추진**('15~)

- **스마트챌린지** 실증단지(스마트시티, 헬스케어 등) 대상 **보안취약점 점검** 및 **컨설팅 수행***을 통한 보안대책 수립 지원

  * 스마트시티, 헬스케어 등 IoT 서비스 취약점 점검 및 보안 컨설팅 지원 용역('15.5~12월, 3,000만원)

- **IoT 실증사업**에서 마련한 보안대책 **결과 분석**을 통하여 필요한 보안기술 등 **신규 사업 아이템 발굴**

  * IoT 등 융합보안 동향 조사·분석 및 전문가 의견수렴(인터뷰 등)도 추진

□ 주요 추진일정

추진내용	추진일정					
	'15년				'16	'17
	1/4	2/4	3/4	4/4		
① IoT 보안 Startup 기업 지원						
- IoT 보안 스타트업 기업 선정 및 인큐베이팅 지원		○	○	○		
- 원스톱 IoT 보안 스타트업 지원 프로그램 운영					○	○
② IoT 시큐리티 센터 구축						
- IoT 공통 보안 테스트베드 구축		○	○	○		
- IoT 보안 테스트베드 확대 구축·운영					○	○
③ IoT 보안 실증사업 추진						
- IoT 보안실증 추진		○	○	○	○	○
- 신규사업 아이템 발굴					○	○

3-2. IoT 보안제품·서비스 수요 창출

□ 추진배경

○ IoT 보안 제품·서비스 개발 및 글로벌 IoT 보안수요 발굴을 추진하여 **IoT 보안산업 활성화** 도모

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) IoT 보안취약점(**버그바운티**) 발굴, **글로벌 IoT 보안수요** 발굴

① IoT 보안취약점 발굴

○ **취약점 신고포상제**(버그바운티) 대상 분야를 S/W, ActiveX 이외에 **IoT**와 관련된 **분야**로 **확대**하고 시범운영('15)

< 취약점 신고포상제 >

o 소프트웨어의 취약점 발견자에게 포상금을 지급하는 제도로, 취약점을 악용한 침해사고를 사전에 예방하고 취약점 발굴 기여자에 대한 보상체계 마련을 위해 '12.10월부터 실시 중

- IoT 환경에 이용되는 **네트워크 장비**(공유기, 홈라우터 등) 및 **오픈소스 S/W**를 대상으로 시작하여 **점진적으로 확대 추진**

  * 공유기 취약점 신고 포상제 운영 실시('15.4~)

○ IoT 보안취약점을 조기에 발굴하고 이에 대한 대응방안 마련을 위해 **'글로벌 IoT 보안취약점 발굴 대회'**를 개최('15)

- IoT 디바이스*를 놓고 참여자들이 실제 해킹을 시도하는 **공격자 관점**에서의 **취약점 발견**과 **대응책 마련**을 추진

  * 라우터, 공유기, 스마트워치, 스마트TV 분야 등 검토

- **입상자**에게는 **포상금**을 **지급**하고, 우수내용에 대해서는 **연구과제**의 **기획**에서 **기술개발**까지 다각도의 **지원** 추진

② 글로벌 IoT 보안수요 발굴

○ 국내외 IoT 제조사와 국내 보안업체간 **기업매칭**을 **지원**하고, 보안 적용사례를 공유하는 **'IoT Security Networking Day'** 개최('15~)

* 용이한 파트너쉽 구축을 위해 IoT 보안 얼라이언스와 연계

○ **IoT 보안** 관련 **전시회 참가*** 및 **선진시장**과의 **교류**를 통한 동향 조사, 최신 기술파악 등 추진('15)

* 일본 IST 2015, 중국 CPSE 2015 등

○ IoT 보안분야의 **해외진출 유망기업**을 **선정***하여 **전시회, 컨설팅 참가** 등 **해외진출 지원**을 통한 해외 레퍼런스 확보('16)

* 정보보호 해외진출 유망기업 선정 시 IoT 보안 기업도 함께 선정

※ 미국 RSA, ISC West, 영국 K-Tech 등 참가 지원

○ 관련 해외전시회, 컨설팅에 물리·정보보안 기업과 **공동관 구성 참가** 등을 통한 **해외시장 다변화** 및 **진출지역 확대** 추진('17)

□ 주요 추진일정

추진내용	추진일정					
	'15년				'16	'17
	1/4	2/4	3/4	4/4		
① **IoT 보안취약점 발굴**						
- 취약점 신고포상제 IoT 분야 확대 시범운영			○	○		
- 글로벌 IoT 보안취약점 발굴 대회 개최				○	○	○
② **글로벌 IoT 보안수요 발굴**						
- IoT 보안 트렌드 및 관련기술 확보	○	○	○	○	○	
- IoT 해외진출유망 기업 발굴					○	○
- 정보보호 전시회 및 비즈니스상담회 참가					○	○

3-3. 「IoT Security Brain」 양성

□ 추진배경

○ IoT 등 융합산업 발전으로 기존 **'침해 대응'** 뿐만 아니라 **'개발·영업'**까지 **비즈니스 全단계**에 관련 **전문인력**의 **수요**가 **증대**

※ '17년까지 정보보호 인력이 약 22,500명 부족 예상(정보보호인력 실태조사, '14)

○ 수요 증대에 적기에 대응할 수 있는 인재양성 체계를 마련하여 IoT 등 **관련 산업의 안정적 발전** 도모

□ 주요내용 및 추진계획

◎ (**로드맵 요지**) **IoT 등 융합보안 인재 육성** 및 **보안교육 인증제** 도입, 7대 IoT 분야 **재직자 교육** 등

① **'정보보호 전공생' 융합보안 교육** 실시 및 **보안교육 인증제** 도입

○ IoT 보안 등 **융합보안 심화교육** 실시

- **정보보호 특성화 대학*** 운영시 **융합보안 관련 전공과목**을 **개설**·운영하여 융합보안 관련 전문성 강화를 도모('15~)

* ('15년) 보안코딩, 임베디드 보안, 암호기술 등 교과과정 개발 및 장비 구축, ('16년~) 학생 선발 및 운영

○ 업계 수요에 대응하는 인력양성을 위해 **기업 및 민간교육기관** 등 **정보보호 관련 교육 운영단체** 대상 **'교육 인증체계'** 구축('15~)

- 인증체계 구축을 위한 **정책연구** 실시('15), **인증체계**(안) **마련** 및 시범적용('16), 최종확정·시행('17) 등 순차 추진

② **K-Shield**(최정예 사이버보안인력) **인증생*** **대상 IoT 보안교육 실시**

* 국가 사이버공격 및 대응 관련 이론 및 실전 훈련(200시간) 수료 인력

○ 임베디드 SW, 제어 프로토콜(UART 등), 무선 프로토콜(Bluetooth 등) 관련 **보안취약점** 이론 등 **'IoT 보안 기본교육'** 실시('15, 1~2기)

○ ‘IoT 보안 테스트베드’를 활용하여 **게이트웨이 · 무선 네트워크 분야** 등에 대해 **‘IoT 보안취약점 분석교육’** 실시(‘16, 1~3기)

○ **스마트홈 분야** 사이버공격 **예방 · 대응교육** 실시(‘17, 1~4기)

③ ‘7대 IoT 분야 재직자’ 정보보호 재교육

○ IoT 분야 종사자의 IoT **보안인식 제고**, 동향파악, 디바이스 **보안취약점 실습** 등 **‘IoT 정보보호 기본과정’** 운영(‘15, 4회 120명)

○ IoT **공통 보안원칙** 및 IoT 보안 관련 **정책, 기술 소개** 등 **‘IoT 정보보호 전문성 강화과정’** 운영(‘16, 5회 150명)

○ IoT 디바이스(SW, HW)별로 **IoT 디바이스 개발자** 및 **기업**의 **관리자 대상** 맞춤형 **교육 프로그램***(콘텐츠, 커리큘럼 등) 개발(‘17)

* 디바이스 해킹 방지, 물리적 위협 방지, 초경량 저전력 보안 알고리즘 등

□ 주요 추진일정

추진내용	추진일정					
	‘15년				‘16	‘17
	1/4	2/4	3/4	4/4		
① **‘정보보호 전공생’ 융합보안 교육 및 보안교육 인증제**						
- 정보보호 특성화 대학 선정 및 지원		○	○	○	○	○
- 정보보호 교육 인증체계 구축 추진		○	○	○	○	○
② **K-Shield 인증생 대상 IoT 보안교육 실시**						
- IoT 보안 기본교육 실시			○	○	○	○
- IoT 보안 취약점교육 실시					○	○
- 스마트 홈 분야 IoT 보안교육						○
③ **7대 IoT 분야 재직자 정보보호 재교육**						
- ‘IoT 정보보호 기본과정’ 운영		○	○	○		
- ‘IoT 정보보호 전문성 강화과정’ 운영					○	
- 7대 분야 개발자/관리자 대상 맞춤형 프로그램 개발						○

Ⅳ 추진체계

○ IoT 보안관련 **의견수렴, 인증제도 관리, IoT 보안기업 지원 관리** 등을 위한 **체계를 구성**하여 효과적으로 정책을 추진

< IoT 보안관련 추진체계 >

분야	구분	주요업무
의견수렴 · 인증제도	**IoT 보안 얼라이언스**	- IoT 보안 관련 최신기술 및 정책 동향을 공유하고, IoT 보안이슈 발생 시 논의 - IoT 디바이스 보안 인증절차, 인증항목 검토 등
IoT 보안 기업 지원 관리	**IoT 시큐리티 센터**	- IoT 보안 관련 주요 실증사업 및 기업지원 관리 등 - IoT 보안 테스트베드를 구축·운영하여, IoT 보안 제품에 대한 보안 테스트 지원