KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

IoT 보안 개요 및 인증

2020.07.17.

융합보안단 이용필 단장

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Content

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

1 IoT 보안 개요

1 IoT 현황

Communication : 사물-사물(자동), 사물-사람

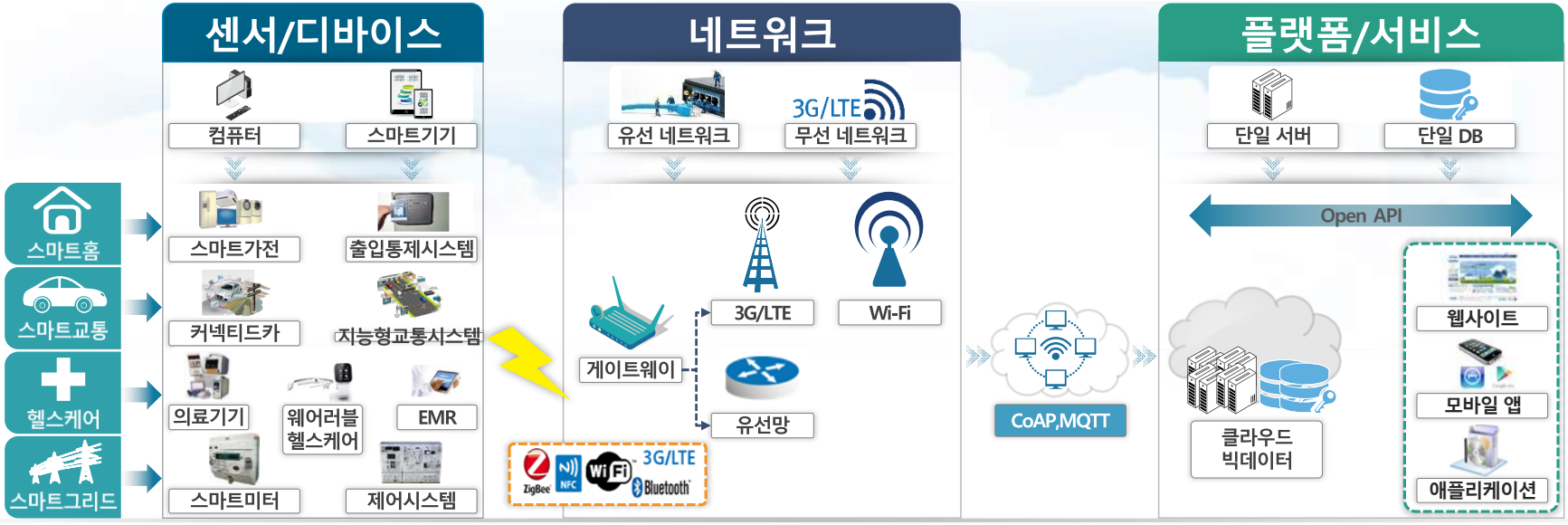
- IoT 플랫폼 시장 규모는 전년 대비 19.5% 증가한 7,540억원까지 증가할 전망이며, 23년까지 16.1%의 연평균성장률을 보이며 1조 3,308억원이 이를 것으로 예상함(IDC, 20년)

23년 전세계 연결 기기, 149억 개로 전망

- 전세계 네트워크 연결 기기 중 IoT 애플리케이션을 지원하는 M2M 연결은 149억 개에 달하며, 23년에는 전세계 인구 1인당 3.6개의 네트워크 연결 기기를 보유하며, 가구당 10개의 네트워크 연결 기기를 보유할 것으로 예상함(Cisco, 20년)

Objects are heterogeneous

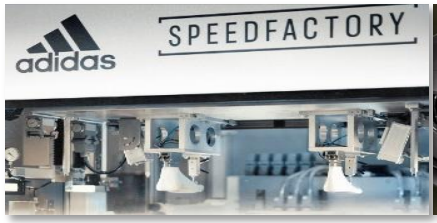
- 다양한 종류의 디바이스 및 프로토콜 혼재



2 IoT 보안의 중요성

- IoT 도입 후에는 사후 보안조치가 불가능하거나, 高비용이 수반
- IoT 제품 및 서비스 개발 全주기에 걸쳐 'Security'가 고려되도록 보안 내재화(內在化)가 요구

스마트 공장	자율주행차	디지털 헬스케어	스마트 시티



•"사이버 보안 빠진 스마트공장 육성 '잠재적 재앙"

- 노르웨이, 알루미늄 공장 랜섬웨어 감염('19)
- 대만 반도체공장(TSMC) 바이러스 감염('18)

•"자율주행차량 조작해 사회혼란 야기 가능"

- 독일 BMW 차량 원격 접근 가능 14개 취약점 발견('18)
- ICS-CERT, 자동차 CAN 버스 표준 취약점 발견('17)

•"헬스케어 기기 해킹 시 사용자의 생명 위협"

- ICS-CERT, 심장박동기에 대한 취약점 발견('19)
- 미국 FDA, 해킹 조작 위험 우려로 심장박동기 50만대 리콜('17)

•"스마트시티 해킹 시 사회적 혼란 야기 가능"

- 미국 애틀랜타 시행정 시스템 랜섬웨어 감염('18)
- 미국 텍사스 주의 경보시스템이 해킹당해 비상 사이렌 작동('17)

'24년에 사이버 공격으로 인해 약 1조4천억 달러 시장이 위협 받음

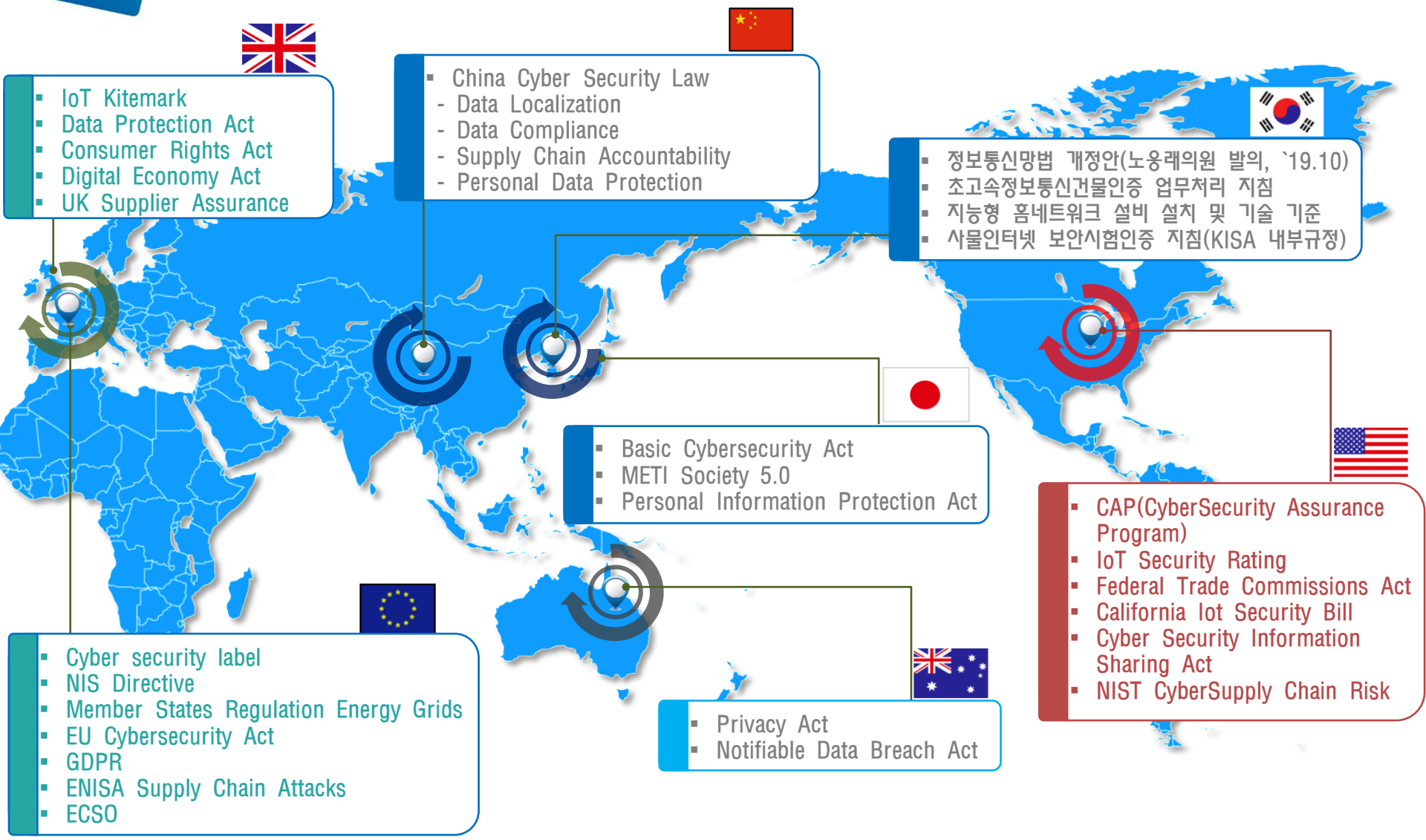
* 스마트 공장 : 2,448억, 스마트 교통 : 2,192억 , 디지털헬스케어 : 3,047억, 스마트시티 : 7,172억 (24년/Markets and Markets)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2 해외 IoT 보안인증 제도

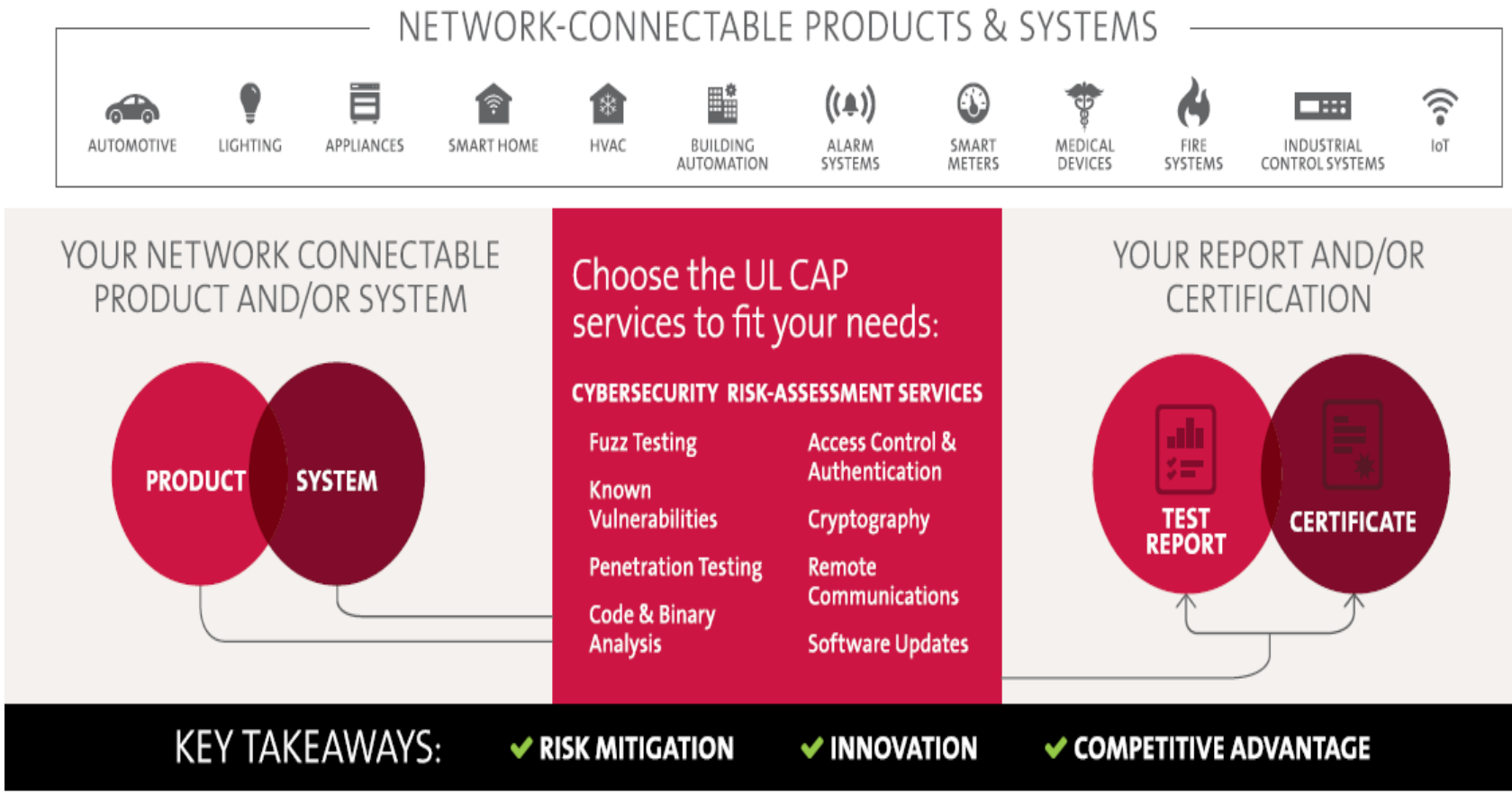
1 국내외 IoT 사이버보안 관련 규제

해외 IoT 보안인증 제도

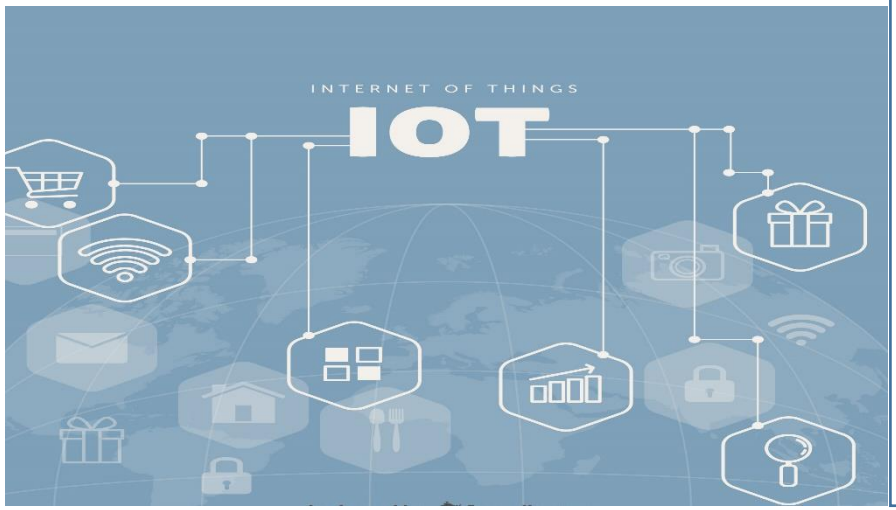


- UL CAP (CyberSecurity Assurance Program)
- UL IoT Security Rating
- BSI IoT Kitemark
- Finland Cyber Security Label
- EUROSMART IoT 인증

UL CAP(Cybersecurity Assurance Program)



2 해외 인증제 : 미국 UL IoT Security Rateing 해외 IoT 보안인증 제도



· **UL의 IoT 보안 등급**은 IoT 산업에서 '보안 기준'을 만들기 위해 **일반적인 공격 방법 및 알려진 IoT 취약성**에 대해 **스마트 제품의 중요 보안 측면을 평가하는 프로세스**임

· 2019년 5월 런칭 후 CES 2020에서 인증마크 발표

시장	사용자
· Energy metering · IoT Device (components of PCB) · Connectivity (eUICC*, network products) · Access control · Smart home 등.	· Application Developers · Device Makers · Service Providers · Product vendors 등.

* eUICC : embedded universal integrated circuit card

제 품	업체명	유효 날짜	등급	비고
· GE ™ · GE Profile ™ · Café ™ · Monogram ™ · Haier ™	GE Appliances	2020.03.10 (유효 1년)	Security Capabilities Verified GOLD	가정에 연결된 모든 GE 제품

출처 : https://www.verify.ul.com/ (2020.04.09 기준, **인증 총 1건**)

출처 : A Cartography of Security Certification Schemes/Standards for IOT (2019.6~9)

The BSI Kitemark™ for
The Internet of Things

Generate trust in your brand
with the BSI Kitemark

bsi.
Functional Safety
E/E/PE Systems
KITEMARK™

bsi.

...making excellence a habit.™

- BSI IoT Kitemark Certification

- BSI Kitemark 인증은 표준이 시간의 경과에 따라 변경되지 않도록 장치의 기능, 상호운용성 및 보안에 대한 테스트를 거쳤음을 보장하는 의미.

- IoT장치에 대한 Kitemark 인증 받는 방법

- 효과적인 품질 관리 시스템을 갖추고 있음을 증명.
  (예: ISO 9001)

※ 통과해야 될 시험

1. 기능 - 관련 제품 성능 안전 시험
2. 상호운용성 - 장치와 인터넷 시험
3. 보안 - 취약점 및 보안 결함을 탐지하는 침투 시험

※ 지속적, 정기적으로 모니터링 평가

1. 기능 / 상호운용성 시험
2. 침투 시험
3. 제품 시험 및 품질 관리 시스템 검토가 포함된 Kitemark 연례 평가

출처 : BSI

2 해외 인증제 : 핀란드 Cyber Security Label 해외 IoT 보안인증 제도

- 핀란드 교통&통신기관인 Traficom은 2019년 11월에 ETSI EN 303 645 Cyber Security for Consumer Internet of Things v2.0.0 초안 문서를 기반으로 인증 수행
  - 사이버보안 레이블의 적극적인 개발은 2018년 말에 시작
  - Cozify Oy, DNA Plc 및 Polar Electro Oy와 공동으로 NCSC-FI(National Cyber Security Center Finland)가 이끄는 파일럿 프로젝트에서 개발
  - 장치가 EN 303 645에 기반한 인증 기준을 충족하는 경우, 사이버 보안 레이블을 네트워킹 스마트 장치에 부여
- 2019년 11월 유럽 처음으로 사이버보안 라벨 부여
  - 대상 제품 : 스마트 홈에 대한 Cozify Hub, DNA의 Wattinen 스마트 난방시스템, Polar Ignite 피트니스 스마트워치 제품

Cozify Hub
Cozify는 사용하기 쉬운 무선 핀란드 스마트 홈 솔루션입니다.

Polar Ignite Fitness 시계
Polar Ignite는 차세대 피트니스 시계입니다.

와트 - älytermostaattipalvelu
지능형 아파트 난방 컨트롤러.

2 해외 인증제 : EUROSMART IoT 인증

- EUROSMART(스마트 보안 산업 협회)는 유럽 사이버보안 인증프레임워크(European Cybersecurity Certification Framework)를 완벽하게 준수하도록 2019년 1월부터 유로스마트 IoT 보안인증 스킴인 e-IoT-SCS (Eurosmart IoT device certification scheme at the level "substantial") 개발 → 파일럿 프로젝트 시작

- 목적
  - IoT 장치의 설계가 잘못되어 일반적으로 존재하지 않거나 비효율적인 보안통제로 인해 소비자와 공급업체에 심각한 결과를 초래하는 공격 성공의 위험을 최소화
  - IoT 장치는 처음부터 보안 설계 및 검증된 보안 기능을 갖추어야 함
- 범위
  - 사이버 보안법에 정의된 실질적인 보안 보증 수준에 중점을 둔 IoT 장치
- 예상되는 인증소요 기간 : 12~27 Man/Days

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

3 국내 IoT 보안 정책

IoT 보안정책 추진 경과

- **2009.10** 사물지능통신 기반구축 기본계획발표
- **2013.6** 인터넷 신산업 육성방안 발표
- **2014.5** 초연결 디지털 혁명의 선도국가 실현을 위한 IoT기본계획발표
- **2014.10** IoT정보보호 로드맵수립
- **2015.6** IoT공통보안 원칙발표
- **2016** K-ICT 융합보안 발전전략 발표 IoT 공통보안 가이드개발
- **2017~2019** IoT 보안인증 서비스 시행 분야별 IoT 보안 가이드개발

IoT 보안테스트베드 구축

IoT 7대 핵심분야 보안 내재화 : 보안원칙, 서비스 가이드 개발 · 보급

1단계(15년~)
IoT 공통 보안원칙

2단계(16년~)
IoT 공통보안 가이드

IoT 공통 보안원칙

01 정보보호와 프라이버시 강화를 고려한 IoT 제품·서비스 설계
02 안전한 소프트웨어 및 하드웨어 개발기술 적용 및 검증
03 안전한 초기 보안 설정 방안 제공
04 보안 프로토콜 준수 및 안전한 파라미터 설정
05 IoT 제품, 서비스의 취약점 보안패치 및 업데이트 지속 이행
06 안전한 운영관리를 위한 정보보호 및 프라이버시 관리체계 마련
07 IoT 침해사고 대응체계 및 책임추적성 확보 방안 마련

IoT 제품 · 서비스 생산 全 단계(설계/개발/운영) 보안 내재화

공통보안가이드 및 서비스별 보안가이드

IoT 공통보안가이드 개발 및 서비스 분야별 가이드 개발 지원

3단계(17년~)
IoT 서비스분야별 (홈가전, 의료, 자동차, 공장, 안전재난환경, 에너지) 보안 가이드 제시

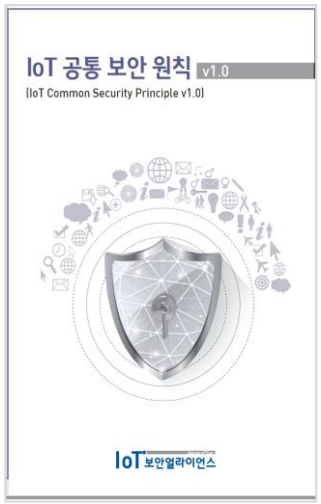
4단계(18년~)
IoT 보안인증 서비스 시행

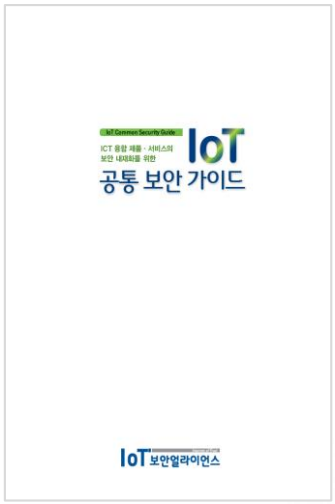
핵심 서비스 분야 보안내재화 : 보안원칙, 서비스 분야별 보안가이드 개발 · 보급

1단계(15년~)
IoT 공통 보안원칙

2단계(16년~)
IoT 공통 보안가이드

3단계(17년~)
서비스 분야별 보안 가이드





IoT 제품·서비스의 보안 수준을 자체 검증 및 보완할 수 있는 IoT 보안테스트베드 운영

IoT 제품 · 서비스 보안내재화 확산”

IoT 보안테스트베드

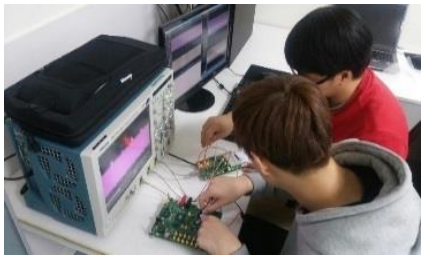
- 홈가전
- 에너지
- 스마트카
- 스마트팩토리
- 스마트의료
- …

IoT 융합 제품/서비스 보안컨설팅	IoT 보안 교육 프로그램 운영	IoT 보안테스트베드 견학 프로그램 운영	IoT 융합 제품/서비스 보안 테스트 환경 구축

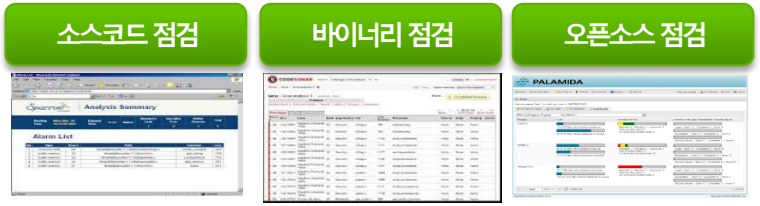
IoT 보안취약점 분석 및 보안컨설팅

- IoT 보안 시험 도구를 활용한 IoT 보안취약점 분석, 보안컨설팅 등 기술 지원

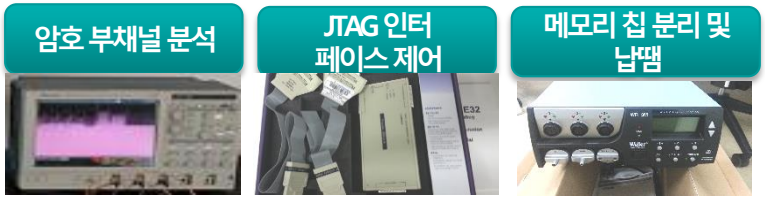





- 소스코드 점검 도구



- 펌웨어 추출 및 취약점 분석 도구



- 통신 프로토콜 취약점 점검 도구

IoT 융합서비스별 보안 테스트 및 해킹 시연 환경 구축·운영

홈/가전, 에너지('15)

자동차, 공장('16)

의료('17)

안전/재난, 환경('18)

건설('19)

홈네트워크건물인증 서비스 개요

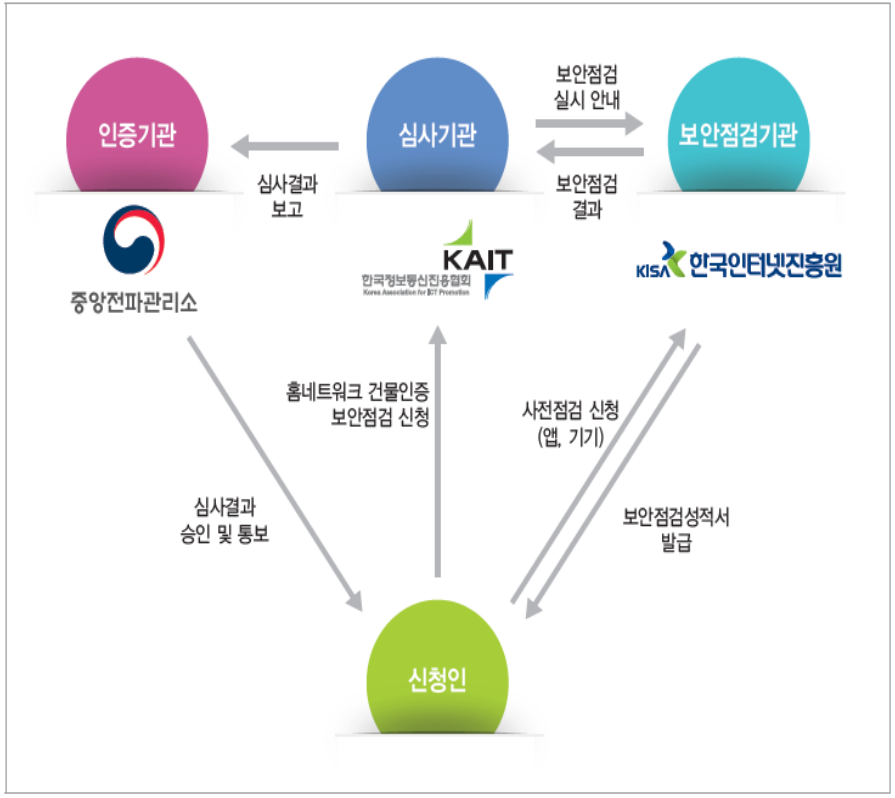
- 건설사 및 IoT 제조사 등에서 개발 및 구축한 인프라와 IoT 기기 등에서 발생할 수 있는 취약점을 사전 점검하는 서비스
- 인증 대상 : 홈IoT기기, 홈IoT 앱, 정보보안장비, 네트워크 장비, 서버
- 점검 및 인증기관 : (점검)한국인터넷진흥원, (심사)한국정보통신진흥협회, (인증)중앙전파관리소
- 인증 수수료 : 없음

< AAA(홈IoT) 인증 마크 >

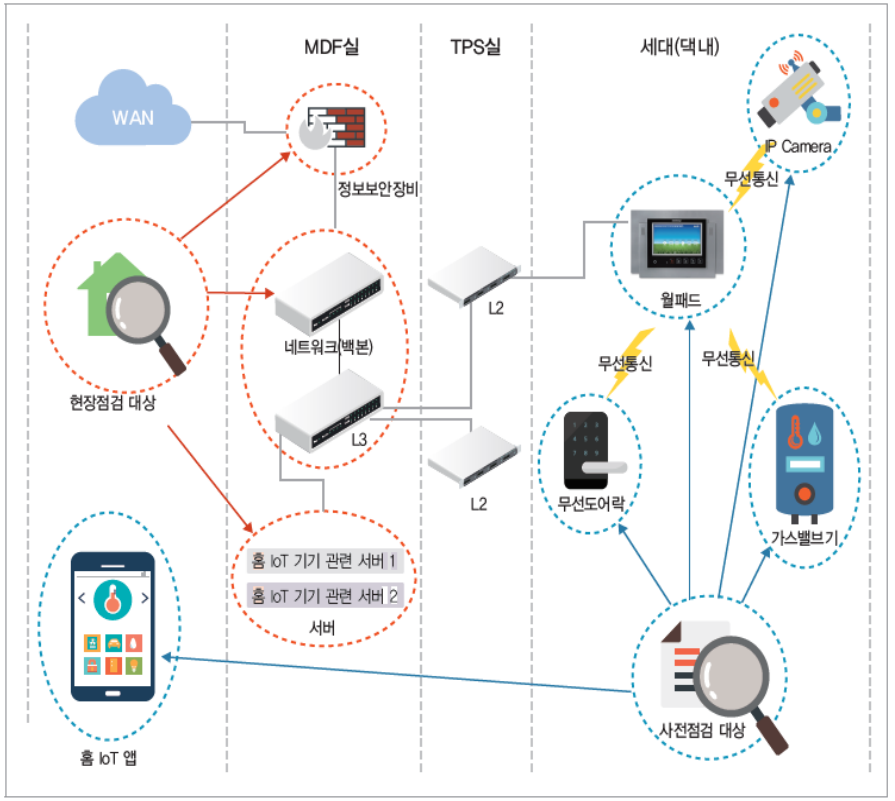
홈네트워크건물인증 보안점검 기준

구 분	점검 항목	
사전점검 기준	앱 보안(5개 항목)	난독화, 불필요한 권한 설정, 패스워드 정책, 중요정보 저장·전송시 암호화, 악성행위 기능 존재
	기기 보안(7개 항목)	고유한 식별자 이용, 관리자 페이지 대상 세션인증, 무선으로 전송시 중요정보 암호화, 검증된 알고리즘 사용, 중요정보 저장, 보안 및 펌웨어 업데이트, 외부 인터페이스를 통한 접근
현장점검 기준	네트워크 보안(2개 항목)	불필요한 서비스, 비인가 IP 원격 접속
	서버 보안(3개 항목)	사용자 인증 정책, 불필요한 서비스, 소프트웨어 패치
	정보보안장비 보안(2개 항목)	취약한 패스워드, 원격 접근통제

추진 체계


인증기관
심사기관
보안점검기관
보안점검
실시 안내
심사결과
보고
보안점검
결과
중앙전파관리소
KAIT
한국정보통신진흥협회
KISA 한국인터넷진흥원
홈네트워크 건물인증
보안점검 신청
사전점검 신청
(앱, 기기)
심사결과
승인 및 통보
보안점검성적서
발급
신청인

점검 범위


MDF실
TPS실
세대(댁내)
WAN
정보보안장비
IP Camera
무선통신
현장점검 대상
네트워크(백본)
L3
L2
L2
월패드
무선통신
무선통신
무선도어락
가스밸브기
홈 IoT 기기 관련 서버 1
홈 IoT 기기 관련 서버 2
서버
홈 IoT 앱
사전점검 대상

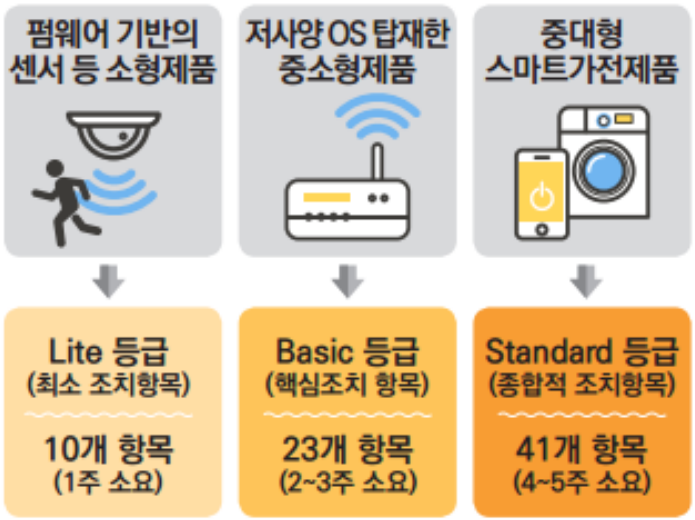
KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

4 국내 IoT 보안인증 제도

IoT 보안 시험·인증 서비스 개요

- IoT 제품 및 연동 모바일 앱에 대해 일정 수준의 보안을 갖추었는지 시험하여 기준 충족 시 인증서를 발급해주는 서비스
- 인증 대상 : IoT 제품 및 연동 모바일 앱 ※유효기간 3년(2년 연장 가능)
- 시험 및 인증기관 : 한국인터넷진흥원
- 인증 수수료 : 초기 인증 수요 창출, 업계 부담 완화 등을 위해 무료 시행 중
- 점검사항 : 인증, 암호, 데이터 보호, 플랫폼 보호, 물리적 보호

IoT 보안 시험·인증 서비스 대상 및 등급



IoT 보안 인증서 발급


KISA
사물인터넷 기기 보안
인 증 서
인증유형 LITE 등급
인 증 번 호 : KISA-IOTSAP-2018-1-0
업 체 명 :
대 표 자 : 조진수
주 소 : 경기도 성남시 수정구 대왕판교로 815, 814호
인 증 대 상 : IoT센서노드(m2m002 버전 2.0)
유 효 기 간 : 2018. 4. 27. ~ 2021. 4. 26.
상기 제품은 한국인터넷진흥원의 사물인터넷(IoT) 기기 보안 인증 기준에 적합함으로 판명되었기에 인증서를 발급합니다.
2018 년 4 월 27 일
KISA 한국인터넷진흥원장

IoT 보안 시험·인증 서비스 절차

IoT 보안 인증서 및 혜택

IoT 보안 시험·인증 혜택

신뢰성 향상
신뢰있는 전문기관 (KISA)으로부터 제품 인증·평가

제품 홍보
온라인 홍보
다나와, KISA누리집 등
오프라인 홍보
전시회 부스 홍보 등

무료 제공
정보보호컨설팅, 테스트도구·환경 인증수수료無

* 인증받은 제품에 대해 **인증마크**, **복제방지용 홀로그램** 제공

IoT 보안 시험·인증 서비스 기대효과

IoT 제품의 자율적 보안강화 유도

국내 IoT기업 보안역량 강화 및 해외시장 진출 활성화 기여

IoT 제품에 대한 국민의 불안감 해소

보안 항목			주요 내용	L	B	S
인증	사용자 인증	AU1-1	▪ 처음 제품을 사용할 때 인증정보를 설정하도록 요구하거나, 초기 인증정보를 변경하도록 요구해야 한다.	○	○	○
		AU1-2	▪ 관리서비스 및 중요정보 접근 시 사용자 신원을 검증하기 위해 식별 및 인증이 선행되어야 한다.	○	○	○
		AU1-3	▪ 잘못된 인증정보를 통한 반복된 인증 시도를 제한해야 한다.	-	○	○
		AU1-4	▪ 기기의 초기 인증정보는 유일한 값으로 설정되어야 한다.	-	-	○
		AU1-5	▪ 제품에서 사용되는 사용자 계정 및 권한에 대한 관리 기능을 제공해야 한다.	-	-	○
		AU1-6	▪ 모든 사용자 계정에 대해 최소 권한의 원칙을 적용해야 한다.	-	-	○
		AU1-7	▪ 관리자 계정에 대해서는 동시 접속을 제한해야 한다.	-	-	○
		AU1-8	▪ 길이, 주기, 복잡성을 고려한 안전한 비밀번호로 설정되도록 해야 한다.	-	-	○
	인증정보의 안전한 사용	AU2-1	▪ 인증정보는 하드코딩 되거나 평문으로 저장되지 않아야 한다.	-	○	○
		AU2-2	▪ 인증을 위한 비밀번호 입력 시 화면에 노출되지 않도록 마스킹 처리해야 한다.	-	○	○
		AU2-3	▪ 인증 실패 시 실패 사유에 대한 피드백 정보를 제공하지 않아야 한다.	-	○	○
	기기 인증	AU3-1	▪ 하드웨어 제품은 각각의 고유 식별정보를 보유해야 한다.	○	○	○
		AU3-2	▪ 제품 간 중요정보 전송 시 혹은 제품 제어를 위한 상호연결 수행 시 상호인증이 선행되어야 한다.	-	-	○
암호	안전한 암호 알고리즘 사용	CR1-1	▪ 중요정보 전송 또는 저장 시 안전한 암호 알고리즘을 사용해야 한다.	○	○	○
		CR2-1	▪ 암호키는 안전성이 검증된 방법으로 생성·갱신·분배·사용·저장·파기되어야 한다.	-	-	○
		CR3-1	▪ 난수 생성 시 난수성이 검증된 알고리즘을 이용해야 한다.	-	-	○
데이터 보호	전송 데이터 보호	DP1-1	▪ 제품 간 전송되는 중요정보는 암호화해야 한다.	○	○	○
		DP1-2	▪ 알려진 프로토콜 기반으로 통신 채널 생성시 안전한 보안 모드를 사용해야 한다.	-	○	○
	저장 데이터 보호	DP2-1	▪ 제품에 저장되는 중요정보는 암호화해야 한다.	○	○	○
		DP2-2	▪ 사용자 필요에 의해 기기에 저장된 중요한 정보를 삭제한 경우, 복원이 어렵도록 해야 한다.	-	-	○
	정보흐름통제	DP3-1	▪ 허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	-	-	○

보안 항목			주요 내용	L	B	S
데이터 보안	정보흐름통제	DP3-1	▪ 허가되지 않은 네트워크 트래픽 차단 기능을 제공해야 한다.	-	-	○
	안전한 세션관리	DP4-1	▪ 세션 연결 후 일정 시간동안 미사용 시, 세션을 잠그거나 종료시켜야 한다.	-	○	○
		DP4-2	▪ 세션 ID는 예측할 수 없는 값이어야 한다.	-	-	○
	개인정보 보호	DP5-1	▪ 제품에 저장되는 중요정보는 암호화해야 한다.	-	-	○
플랫폼 보안	소프트웨어 보안	PL1-1	▪ 보안약점이 존재하지 않도록 시큐어코딩을 적용해야 한다.	-	○	○
		PL1-2	▪ 알려진 보안취약점 존재여부를 확인하고 제거하여야 한다.	○	○	○
		PL1-3	▪ 소스코드 분석 방지를 위해 난독화를 적용해야 한다.	○	○	○
		PL1-4	▪ 주요 설정 값 및 실행코드에 대한 무결성 검증 기능을 지원해야 한다.	-	-	○
	안전한 업데이트	PL2-1	▪ 업데이트 수행 전 인가된 사용자 여부를 확인해야 한다.	○	○	○
		PL2-2	▪ 업데이트 실패 시 롤백 기능을 지원해야 한다.	-	○	○
		PL2-3	▪ 업데이트 수행 전 무결성 검사를 수행해야 한다.	-	-	○
	보안관리	PL3-1	▪ 불필요한 서비스는 제거하거나 비활성화해야 한다.	-	○	○
		PL3-2	▪ 원격관리는 신뢰할 수 있는 환경에서 수행되어야 한다.	-	○	○
		PL3-3	▪ 3rd party 라이브러리 사용 시 최신 보안패치가 적용된 버전을 사용해야 한다.	-	○	○
		PL3-4	▪ 하드웨어 및 소프트웨어의 자체 시험 기능을 제공해야 한다.	-	-	○
	감사기록	PL4-1	▪ 보안과 관련된 이벤트는 감사기록을 생성해야 한다.	-	○	○
		PL4-2	▪ 감사기록에 대한 보호 기능을 제공해야 한다.	-	-	○
	타임스탬프	PL5-1	▪ 신뢰할 수 있는 타임스탬프 기능을 지원해야 한다.	-	-	○
물리적 보호	물리적 인터페이스 보호	PH1-1	▪ 불필요한 외부 인터페이스는 비활성화하고, 필요 시 접근통제 기능을 지원해야 한다.	-	○	○
		PH1-2	▪ 비인가자의 내부 포트 접근을 방지해야 한다.	○	○	○
	무단조작 방어	PH2-1	▪ 비인가자의 무단 조작을 탐지하여 대응할 수 있는 기능을 지원해야 한다.	-	-	○

‘18년 4건, ’19년 24건, ’20년 9건 등 총 37건 인증 (Lite 24건, Basic 13건)

※ 20.5.30.기준

연도	#	제품군	제품명	제조사	등급
‘18년	1	기기	IoT 센서노드 (m2sn002)	엠투클라우드	Basic
	2	기기	실내 공기질 측정기	케이웨더	Basic
	3	기기	공기질측정 스마트센서	알엠테크	Basic
	4	기기	Smart IoT 침수 감지 단말기	현진 ICT	Basic
‘19년	5	앱	IoT@Home 앱	LG 유플러스	Lite
	6	앱	하이브리드 전기보일러 앱	한에너지시스템	Basic
	7	앱	HioT Smart Home 앱	현대오토에버	Lite
	8	기기	보행신호 음성안내 보조장치	삼성티엔지	Basic
	9	앱	T-sign 앱	케이스마텍	Basic
	10	기기	전기자동차 충전 콘센트	클린일렉스	Basic
	11	기기	전기자동차 충전 전력분배 게이트웨이	클린일렉스	Basic
	12	기기	무선 온습도 센서	유타렉스	Lite
	13	기기	스마트홈월패드	삼성 SDS	Lite
	14	기기	디지털도어록	삼성 SDS	Lite
	15	앱	sHome 앱	삼성 SDS	Lite
	16	기기	IoT 센서노드 (m2sn003)	엠투클라우드	Lite
	17	기기	NB-IoT 플러그	에이나인	Lite
	18	기기	스마트 GPS 리피터	㈜텔에이스	Basic
	19	앱	GIGA Genie 홈 IoT 앱	KT	Lite
	20	기기	IoT 삼상 전력 측정기	다원디엔에스	Lite
	21	기기	NB-IoT 스마트 플러그	다원디엔에스	Lite
	22	기기	도어센서	코맥스	Lite
	23	기기	온습도센서	코맥스	Lite
	24	기기	보안 미디어 컨버터 모듈 (IP 카메라)	케이씨에스	Lite
	25	기기	보안 미디어 컨버터 모듈 (Wall Pad)	케이씨에스	Lite
	26	기기	보안 미디어 컨버터 모듈(Smart Enerygy)	케이씨에스	Lite
	27	기기	실외공기질측정기	케이웨더	Lite
	28	기기	온습도센서	코맥스	Lite

‘18년 4건, ’19년 24건, ’20년 9건 등 총 37건 인증 (Lite 24건, Basic 13건)

연도	#	제품군	제품명	제조사	등급
’20년	29	기기	IoT스마트허브	코맥스	BASIC
	30	기기	조도조절형 LED센서조명기구	텔트론	LITE
	31	기기	Zigbee RCU	오성전자	LITE
	32	기기	미로티 블루투스 2세대	미로	LITE
	33	기기	분기전력측정기	서준전기	LITE
	34	기기	에너지미터	서준전기	LITE
	35	기기	IoT 지적-기준점(가속도&지진센서)	알엠테크	LITE
	36	기기	DANA Diabecare R(인슐린주입기)	수일개발	BASIC
	37	기기	DANA Diabecare R(remotecontroller)	수일개발	BASIC

제품 활용 사례

IoT 공기측정기, 어린이집 744곳 1500여대 납품

디지털 도어락, 고덕동 아파트(5000세대) 납품

협력 강화

o IoT 제품을 대량으로 도입하는 기관과 업무협력 강화

※ MoU : 서울시('18.6), KT('19.6), LH공사('19.9), SH공사('19.11), 식품의약품안전평가원('20.5)

- AI 스피커 제조 · 운영자인 통신사 등과 업무협력 확대 추진('20.7월)

시험 환경 구축

o 중소 IoT 제조·개발사가 자율적인 시험·점검할 수 있는 테스트 점검도구 확대

※IoT보안 테스트베드를 구축·운영 중이며, '20년에 스마트홈 무선점검 도구(7종) 추가 구축

국제 표준화 추진

o IoT보안 시험·인증 기준과 관련한 국제표준이 없어, 우리의 기준을 국제 표준으로 추진

※Standard 등급 41개 기준(ITU-T X.iotsec-4)을 ITU에 제안('18.8월), 아이템 채택('19.8월)

법적 근거 마련

o 정보통신망 연결기기 등 자율인증제도 근거 신설

※ 정보통신망법 개정안(노웅래 의원, '19.10.28) 국회 통과('20.5.20)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

5 정보통신망법 개정

추진 배경

○ 초연결을 가속화하는 5G 상용화, ICT 융합 등으로 융합 서비스, 융합 제품의 보안 문제가 중요해짐에 따라 변화에 부응하는 법제도 준비

- IP카메라, 지능형CCTV, 스마트홈, 자율주행차 등 융합서비스·제품에 대한 보안위협은 국민의 신체·재산 피해와 사회적 혼란을 야기 할 수 있어 선제적 대응 필요

- "테슬라 GPS 내비게이션, 외부 사이버 공격에 취약" 지적(매일뉴스, '19.06.21.)
- 안방CCTV를 누군가 훔쳐본다… 스마트홈 파고드는 'IoT 해킹'(동아일보, '19.07.31.)
- 구멍 뚫린 스마트홈…현관문이 저절로 열려(매일경제, '19.07.21)
- "사생활이 위험하다"…웹캠·IP카메라 해킹 영상 '수두룩'(NEWSIS, '19.02.05.)
- 병원 MRI·X-레이에 악성코드 발견…국내 피해 우려(news1, '18.04.29.)
- AI 스피커, 고주파로 해킹돼… (조선비즈, '18.9.5.)
- 스마트TV, 해킹에 취약…삼성·中TCL 등 영향(연합뉴스, '18.2.8.)
- 자동차 블루투스 보안 2분 만에 무력화(보안뉴스, '18.6.14.)
- 자율주행 전기차, 해킹에 '원격조종' 당했다(경향신문, '16.9.21.)

주요 경과

- 『K-ICT 융합보안 발전전략』('16.5) 수립 시 법제 개선 필요성 제시
- 융합보안 강화를 위한 법제 개선 TF 운영('18~'19)
- 노웅래의원실, 정보통신망법 개정안 발의('19.10.29)
- 개정안 심사소위원회 통과('20.5.6), 법사위 및 국회 본회의 통과('20.5.20)
- 하위법령 개정을 위한 『법제 워킹그룹』 1차~3차 회의('20.5~6)

추진 현황

ㅇ 융합보안강화를 위한 정보통신망법 개정안 국회통과('20.5.20)

< 법 개정 주요내용 >

① **정보보호지침**(고시) **규율대상 확대**('정보통신망 연결기기' 제조·수입업자 추가) 및 **개별법상 시험·인증 기준** 등에 **정보보호지침 반영** 근거 마련

② **정보통신망연결기기** 등에 대한 침해사고 발생시 **원인분석** 및 관계중앙행정기관장에 **조치를 요청**할 수 있도록 규정

※ 침해사고가 발생한 정보통신망 연결기기 제조·수입업자에 취약점 개선 및 재발방지 조치 권고 조항도 신설

③ **정보통신망 연결기기**(IoT 등)에 대한 '**정보보호인증**' 제도 신설

ㅇ 하위법령 마련을 위한 '법제 실무반' 구성하여 개정안 마련 중('20.5.27~)

- (시행령) 정보통신망 연결기기등의 범위, 대통령령으로 정하는 전문기관, 정보보호인증의 절차 및 수수료, 인증시험대행기관 지정기준 및 절차 등을 신설
- (고시) 정보통신망 연결기기 등의 정보보호지침 개정안, 정보보호인증의 인증기준 고시 제정안 등

국회 본회의 통과한 정보통신망법 개정안, 핵심은 '융합보안' 기반 조성

정보통신망의 안전성·신뢰성 확보...안전한 융합서비스 이용환경 제공

| 입력 : 2020-05-21 15:10

[보안뉴스 권 준 기자] 과학기술정보통신부(장관 최기영, 이하 과기정통부)는 국민이 안심하고 정보통신망을 이용할 수 있는 환경조성을 위한 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)' 일부 개정안이 이번 제378회 국회(임시회) 본회의를 통과했다고 밝혔다.

둘째, 정보통신기술(ICT) 융합 기기·제품·서비스에 대한 보안사고 예방 및 피해 최소화를 위해 법 적용 대상 확대 및 최소한의 보안기준을 마련하여 준수하도록 권고했다. 기존 정보통신서비스 제공자에 적용되던 정보보호지침의 규율대상에 '정보통신망 연결기기 등'을 제조·수입하는 자를 추가하고, 정보보호지침에 정보통신망 연결기기 등의 안전한 이용을 위한 정보보호를 고려한 기술적 보호조치를 추가하여 준수하도록 권고했다.

셋째, 산업별 개별법상의 기준에 정보보호지침 반영 요청 근거를 마련했다. 생명·신체 등 피해우려가 있는 일부 기기의 경우, 과기정통부장관이 개별법에 따른 시험, 인증 등 기준에 정보보호지침이 반영될 수 있도록 소관부처에 요청할 수 있는 근거를 마련했다. 개별법에 따른 기준 반영 시, 정보보호지침을 의무화하지 않더라도 실질적인 규제 효과가 발생할 수 있다.

넷째, 융합보안 사고 원인분석 체계를 마련했다. 과기정통부가 관계부처와 협력하여 정보통신망에 연결되어 있는 기기 등에 사고가 발생할 경우 사고 원인분석을 할 수 있는 근거 및 관계부처와 제조·수입업자에게 피해확산 방지조치를 요청할 수 있는 근거를 마련했다.

마지막으로 사물인터넷(IoT) 제품 등의 보안인증 제도를 도입해 기업의 자발적인 보안수준 향상을 유도하고 이용자의 선택권을 보장하는 내용이다. 정보통신망 연결기기 등에 대하여 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 자율인증제도 실시 근거를 마련했다.

2 정보통신망법 개정안에 따른 변경 사항정보통신망법 개정

변경 사항

	<현행>	<개정안>
1. 적용대상	• 정보통신서비스제공자	• 정보통신서비스제공자 • **정보통신망 연결기기등 제조·수입자**
2. 규율내용	• 정보통신망의 안정성·신뢰성 확보를 위한 **정보보호지침 준수(권고사항)**	• 정보보호지침에 **'정보통신망 연결기기등의 안전한 이용을 위한 기술적 보호조치' 추가(권고사항)**
3. 지침 반영	• 없음	• 산업별 개별법상 기준에 **정보보호지침 반영 요청** 근거 마련
4. 융합보안 사고분석	• 없음	• **정보통신망연결기기등 침해사고 원인분석** 체계 마련
5. 사업 지원근거	• 없음	• 정보보호지침 마련 및 시험검사인증 등 기준 개선 등 **연구 수행 지원 근거 마련**
6. 보안인증제도	• 법적 근거 없이 IoT 보안인증제도 운영	• 정보통신망연결기기등에 대한 **보안인증제도 운영 근거 마련**

개정안 주요내용

○ (개정) 제45조(정보통신망의 안전성 확보)
- (제1~3항 개정) 정보보호규율대상을 정보통신망 연결기기등을 제조·수집하는 자로 확대 및 기술적 보호조치 추가
- (제4항 신설) 개별법 상 시험·인증 등 기준에 정보보호지침 반영 근거 마련

○ (신설) 제48조의5(정보통신망 연결기기 등 관련 침해사고의 대응 등)
- (제1항) 융합제품 관련 침해사고 발생시 과기정통부장관이 관계부처와 협력하여 융합제품 관련 침해사고 원인분석 권한
- (제2항) 관계부처에 대한 ① 취약점 점검, 기술 지원 ② 피해확산방지 조치 ③ 정보보호제도 개선 요청 권한
- (제3항) 제조·수입업자에 대한 취약점 개선조치 등 권고 권한
- (제4항) KISA등 전문기관에 대한 정보보호지침 마련 및 시험·검사·인증기준 개선 연구를 위한 비용지원 근거

○ (신설) 제48조의6(정보통신망 연결기기등에 관한 인증)
- (제1항, 제3항) 융합제품에 대한 정보보호인증 및 취소 근거
- (제2항) 정보보호인증 기준 고시를 위한 근거
- (제4~5항) 인증시험대행기관 지정 및 취소 근거
- (제6항) 정보보호인증 및 취소 업무의 KISA 위탁 근거
- (제7항) 정보보호인증 및 취소 절차, 인증시험대행기관 지정 및 취소 절차 등 시행령을 위한 근거

○ (신설) 제64조의4(청문) (제5호) 정보보호인증 취소, 인증시험대행기관 지정 취소

정보통신망 개정안 통과에 따라, 하위법령 개정을 위한 법제 워킹그룹 운영 등 추진

※산・학・법조 전문가와 협력하여, 시험・인증 유사제도 법률 검토를 통해 시행령, 고시 등 하위법령 개정안 마련

(하위법령 개정) 정보통신망 연결기기등에 관한 하위법령 개정

< 위임사항 >

	개정사항	위임 조항
시행령	o **(신설) 대통령령으로 정하는 정보통신망 연결기기등의 범위** - 정보통신망에 연결되어 정보를 송·수신할 수 있는 기기·설비·장비 중 정보보호지침 적용 범위에 포함할 대상	안 제45조제1항제2호
	o **(신설) 대통령령으로 정하는 전문기관** - 정보통신망 연결기기 등 관련 정보보호지침 마련 및 시험·검사·인증 등의 기준 개선을 위한 연구 사업을 수행하는 전문기관	안 제48조의5제4항
	o **(신설)** 정보통신망 연결기기등에 관한 **인증(정보보호인증)의 절차** 및 그 취소 절차	안 제48조의6제7항
	o **(신설) 인증시험대행기관의 지정**기준, 지정 및 지정취소에 관한 사항	안 제48조의6제4항·제7항
고시	o **(개정)** 정보통신망 연결기기등의 **정보보호지침 고시** - 정보통신망 연결기기등의 정보보호를 위한 기술적 보호조치	안 제45조제3항
	o **(신설)** 정보보호인증의 **인증기준 고시**	안 제48조의6제2항

< 기타 원활한 시행을 위하여 필요한 사항 >

	시행령 개정사항	근거 조항
시행령	o **(신설)** 정보보호인증의 **수수료에 관한 사항**	안 제48조의6

향후 일정(안)

○(운영계획) 법제 워킹그룹 착수 회의(5월말) 및 하위법령(시행령, 고시) 개정 지원(6~12월)

- (6~8월) 하위법령 개정안 마련, 부처협의
- (8~9월) 입법예고 및 공청회
- (10~11월) 규제·법제 심사
- (12월) 차관·국무회의 및 관보 게재

기대 효과

○정보통신망의 안전성과 신뢰성 확보는 물론 국민과 기업에 안전한 융합서비스 이용환경 제공과 이를 통한 융합산업의 경쟁력 강화

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

감사합니다

Thank You For Listening