KISA 한국인터넷진흥원

지능정보사회,
보안 패러다임의 변화

2017.4. 27. PRESENTATION

손경호
한국인터넷진흥원

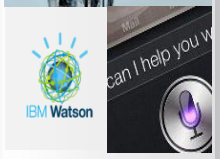
순서

지능정보사회의 정의와 개념

KISA Korea Internet & Security Agency

신기술의 등장 → **산업의 혁신** → **다양한 경제·사회적 변화 수반**

지능정보기술의 등장



생산성 향상, 근로시간 감소


제조


교통

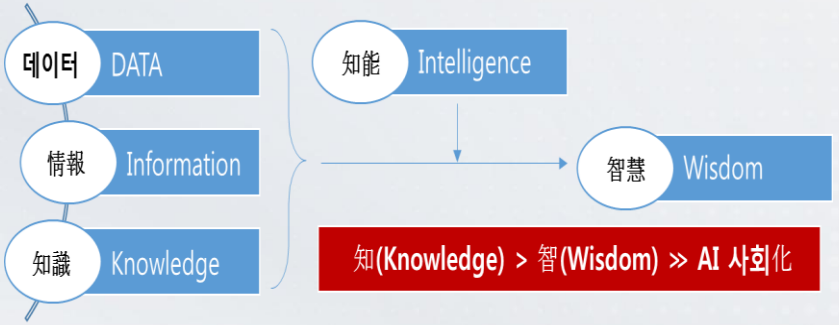
서비스

삶의 질 향상 및 새로운 사회문제 발생

삶의 편의성 증가 안전한 생활환경 맞춤형 서비스

일자리 감소 빈부격차 심화

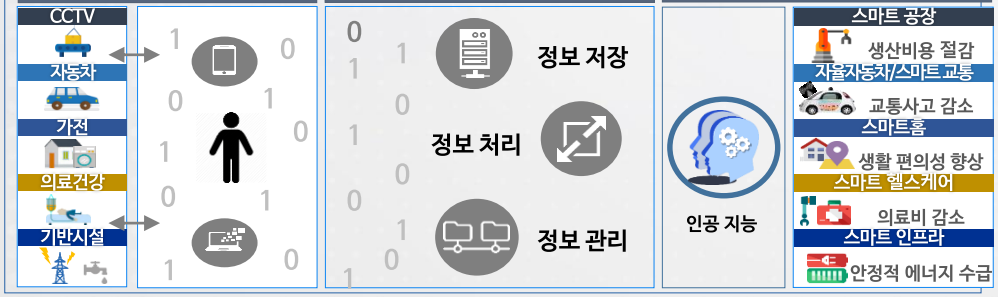
인공지능, ICT 등 지능정보기술이 촉발하는 제4차 산업혁명은 사회 전반을 변화시킬 것입니다.



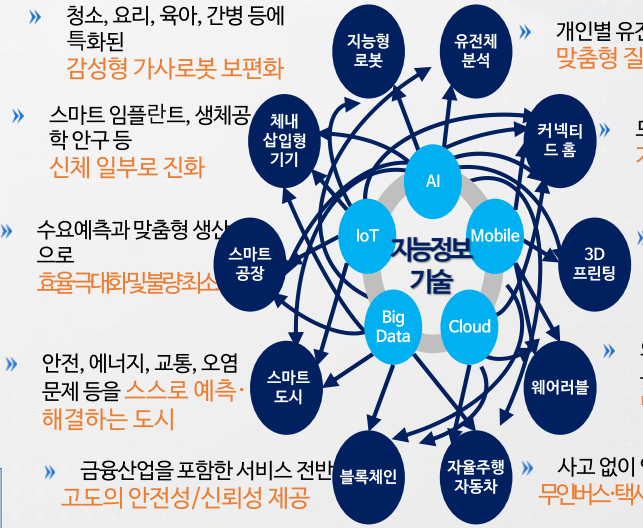
- 데이터(Data) : 단편적인 사실, 수치, 문자
- 정보(Information) : 데이터를 조합해 의미를 부여한 것
- 지식(Knowledge) : 데이터와 정보를 체계적으로 집적
- 지능(Intelligence) : 데이터·정보·지식을 해석해 새로운 데이터·정보·지식을 창조하는 기능
- 지혜(Wisdom) : 데이터·정보·지식에 기반해 지능을 활용해서 사물에 대처하는 인간의 능력

개념

IoT	Mobile	Cloud & Big Data	A.I.	새로운 가치
모든 기계·인간으로부터 데이터 수집		정보처리능력 고도화로 데이터 축적·분석 강화	기계가 데이터를 빠르게 학습하여 새로운 지능정보가치 창출	



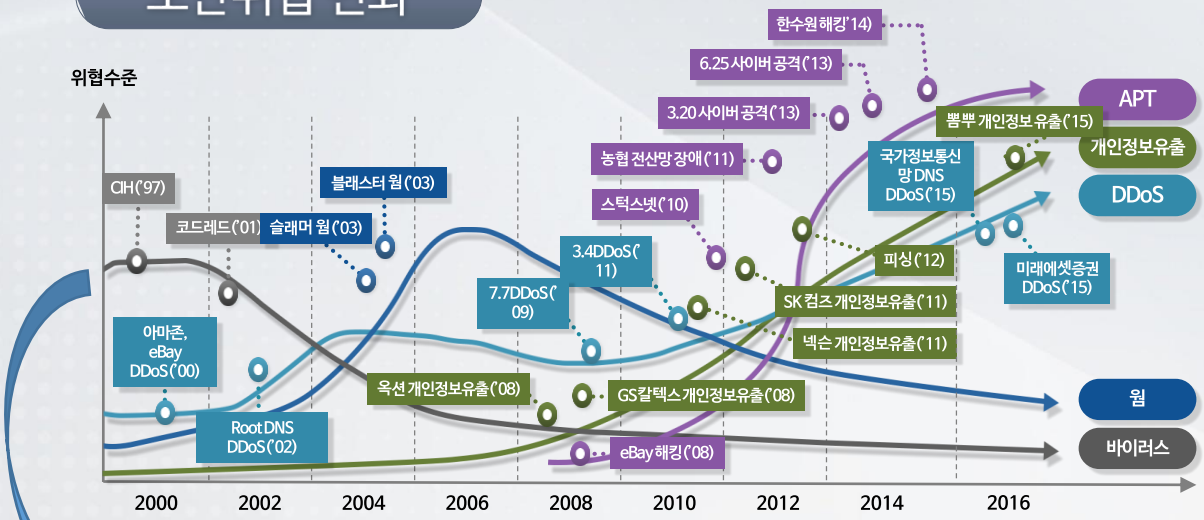
특징 : 만물의데이터화 | 실시간반응 | 자율진화 | 무인의사결정



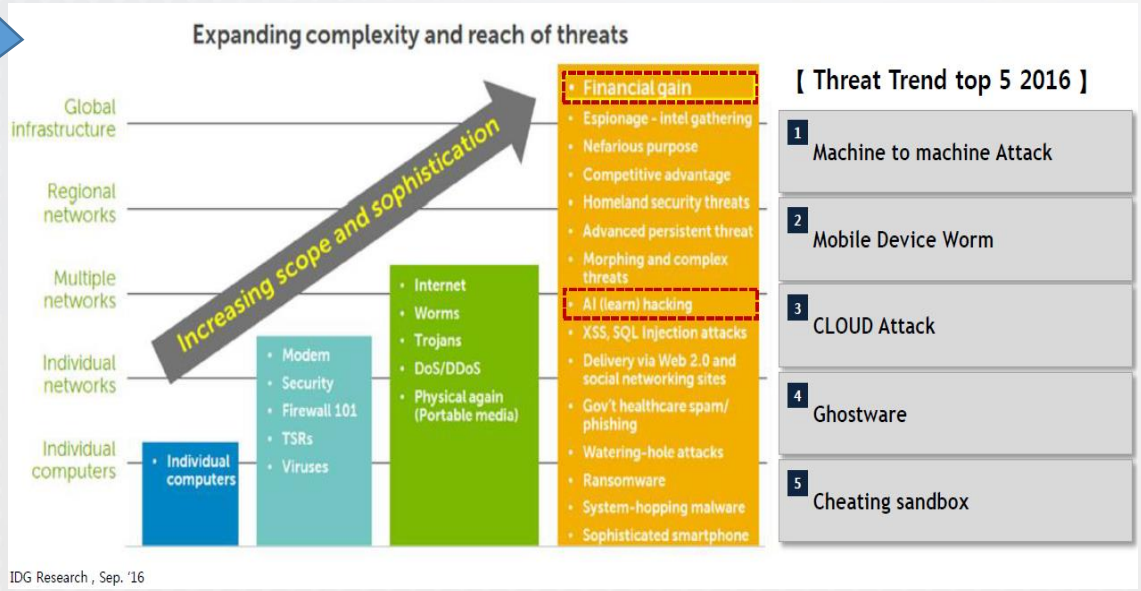
- 청소, 요리, 육아, 간병 등에 특화된 감성형 가사로봇 보편화
- 스마트 임플란트, 생체공학 안구 등 신체 일부로 진화
- 수요예측과 맞춤형 생산으로 효율극대화및불량최소화
- 안전, 에너지, 교통, 오염 문제 등을 스스로 예측·해결하는 도시
- 금융산업을 포함한 서비스 전반 고도의 안전성/신뢰성 제공
- 개인별 유전자 특성을 분석하여 맞춤형 질병 치료
- 모든 전자제품의 자율제어로 가사노동에서 해방
- 누구나 원하는 제품을 만드는 1인 제조시대
- 의류 일체형 웨어러블 기술 등을 통해 초현실가상체험 및증강인간구현
- 사고 없이 안전하게 운행하는 무인버스·택시및무인물류상용화

보안위협 변화

보안위협 변화



2020년에는?



RSA 2017 주요 KeyNote

- 마이클 맥콜 미 국토안보위원장은 사이버위협 대응을 위해 각 국가들의 사이버 위협정보 공유 중요성 강조
- DEFCON에서 진행된 DARPA의 Cyber Grand Challenge 이후 AI에 의한 자동화된 공격, 방어에 대한 관심 확인
- 구글(알파벳) 슈미츠 회장은 AI는 보안에 중요한 보조기술이 될 것으로 전망하며, 더 많은 관심과 연구를 요구
- MS-CLO, 브렌드 스미스는 날로 급증하는 국가차원 해킹 대응을 위해 '디지털 제네바 협약' 제안

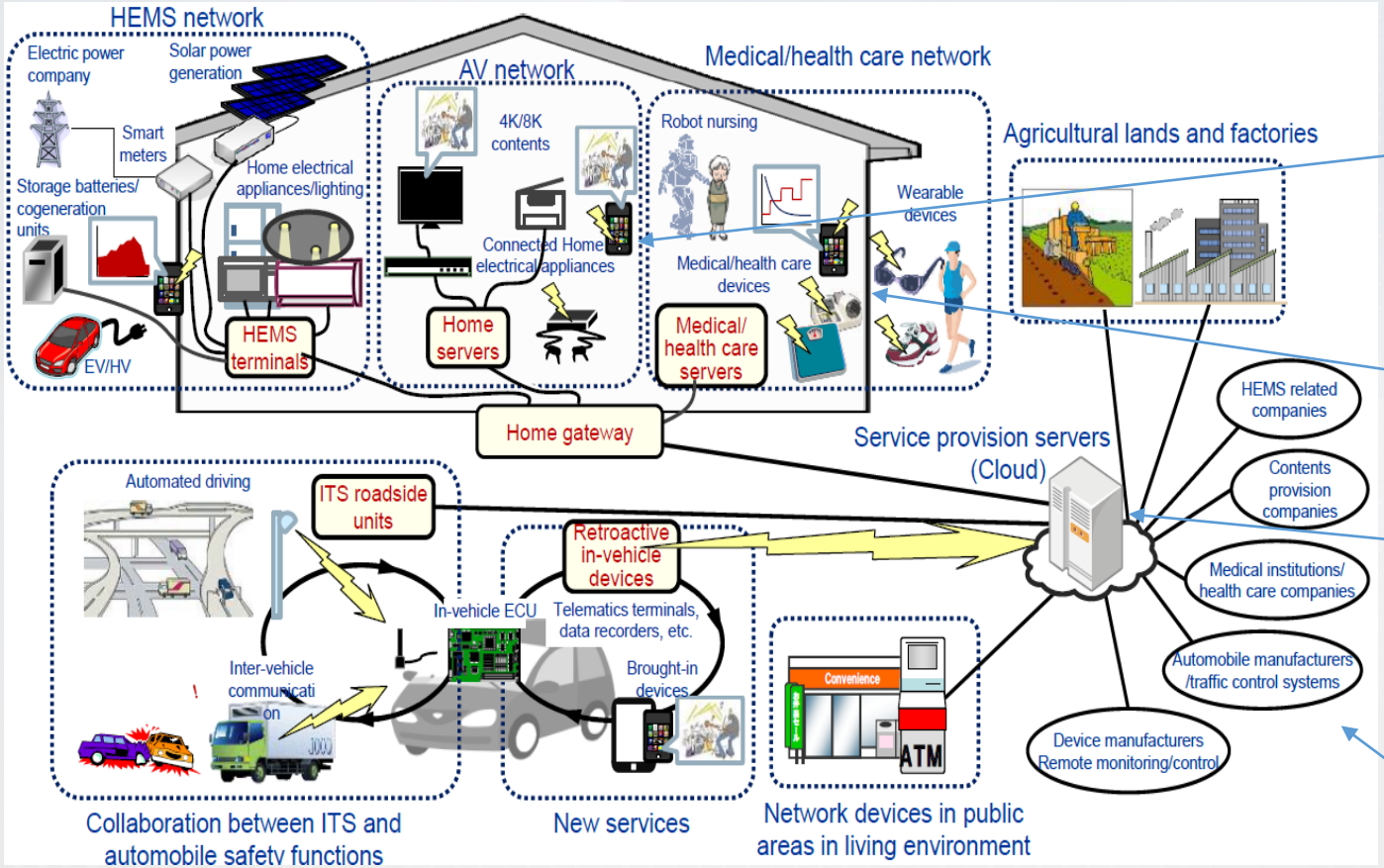
實 생활에 보안위협

KISA Korea Internet & Security Agency

Smart Life Security

무엇이 연결되어 있는지 모름
= 취약한 생활 기기가 공격의 포인트

인간이 관여된 "공격자-방어자" 개념에서 AI와 로봇에 의한 자동화된 공격과 방어형태로 진화



Society5.0

다양한 네트워크 연결성 증가
= 다른 분야의 생활 기기의 예상치 못한 동작

기기와 모바일 장치가 연결
= 모바일 장치가 보안위협 전파하는 매개체

많은 생활 기기가 서버와 통신
= 개인에 관한 정보의 유출 및 변조의 위험

생활 기기를 원격으로 모니터하고 조작하는 서비스가 증가
= 원격 서버에서 정보를 탈취해 생활 기기에 대한 공격도 가능

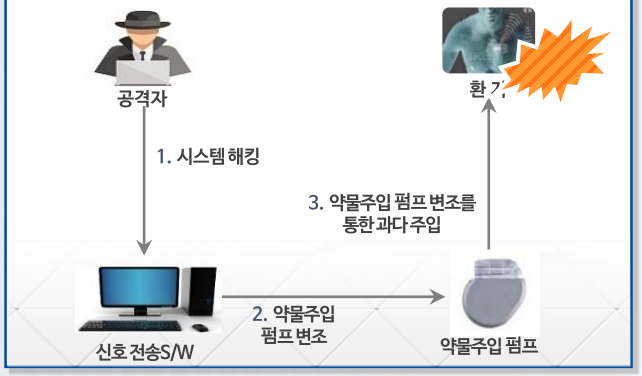
악의의 사람·사물이 네트워크에 연결되어 거짓정보(데이터) 등을 제공 시, 이를 신뢰하는 사람·사물은 예기치 못한 피해발생이 가능하여 사회의 안전 저해, 국민의 생명·재산 위협 우려

출처: 일본 CCDS 재편집

實 생활에 보안위협

實 사례

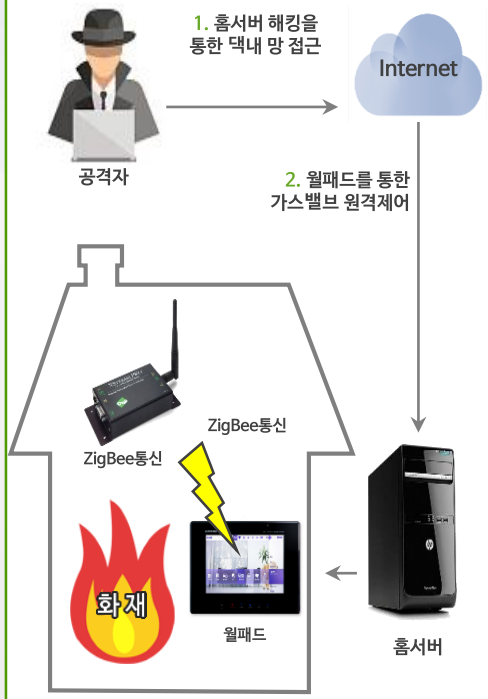
약물주입 펌프 변조를 통한 심박 약물주입 펌프 변조(미국)



악성코드가 감염된 차량진단 앱을 통한 자동차 원격제어(미국)

해킹을 통한 공장 제어시스템 파괴로 제품생산 마비(독일)

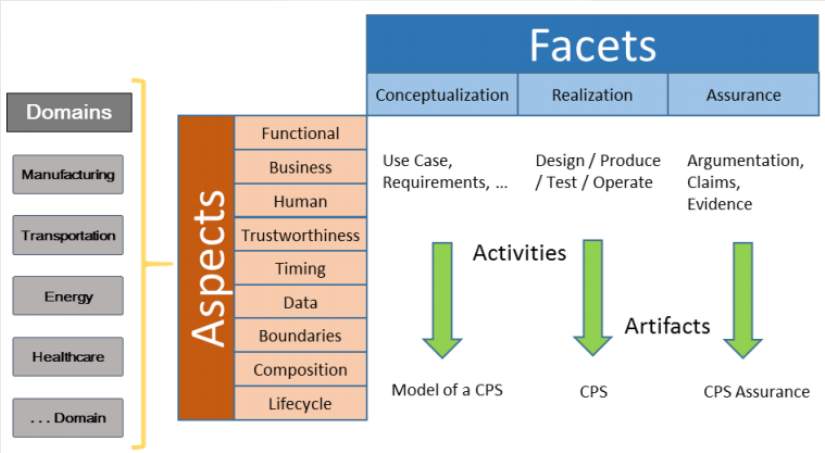
홈서버 해킹을 통한 댁내 가스밸브 원격개방(미국)

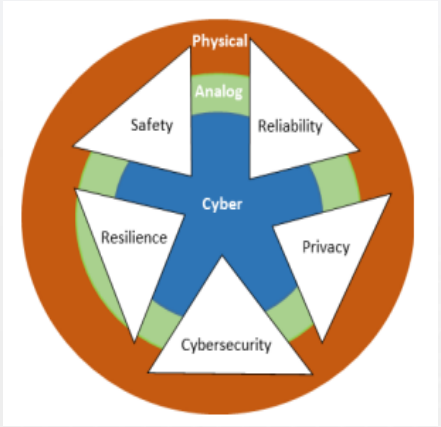


보안 속성변화

CPS Security 속성 변화

NIST, CPS Framework – Domains, Facets, Aspects





- **Cybersecurity** : 가용성에 대한 위험에도 불구하고 중요한 기능을 수행하기 위해 시스템을 가능하게 하는 방법의 확립과 보호 대책을 유지하는 것
- **Privacy** : 내부 시스템 간 또는 물리적 환경을 조작하여 자신의 개인 정보를 처리할 때 발생하는 위험을 완화시키기 위한 방법의 확립하는 것

- **Safety** : 물리적 손상이나 사람들의 건강에 피해를 허용 할 수 없는 위험에 대해 직접 또는 간접적으로 치명적인 영향이 없도록 하는 것
- **Reliability** : 사용자 또는 적절한 서비스의 연속성과 종료하는 서비스 일관성 수준을 제공하는 능력
- **Resilience** : 상황의 변화에 적응하고 공격 사고에서 빠르게 회복하는 능력

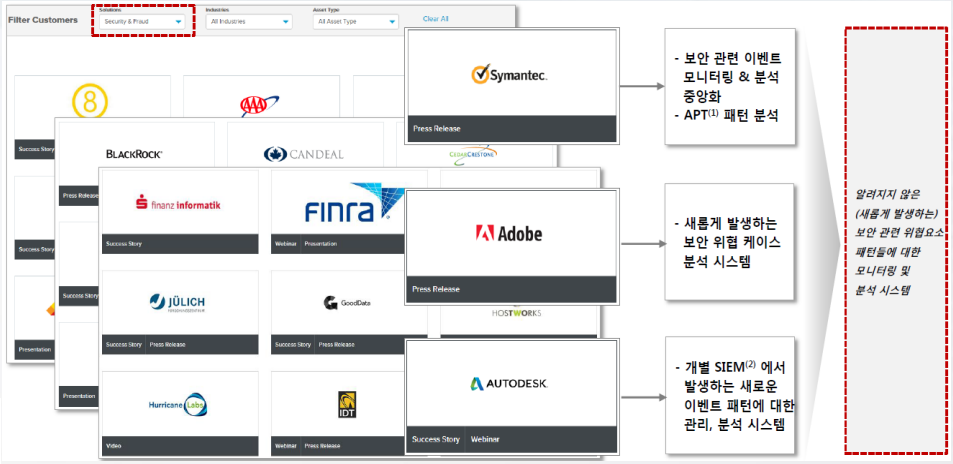
AI기술 >> 보안시스템에 적용 사례

- 현재, 각종 보안이벤트 정보를 자동 수집·분석해 보안 위협을 확인하는 수준에서 → 클라우드컴퓨팅 연산자원 활용 및 보안특화 알고리즘 개발을 통해 각종 공격이 어떤 방식으로 들어오는지를 학습하고, 이를 통해 적절한 대응방법을 적용하는 기술로 발달

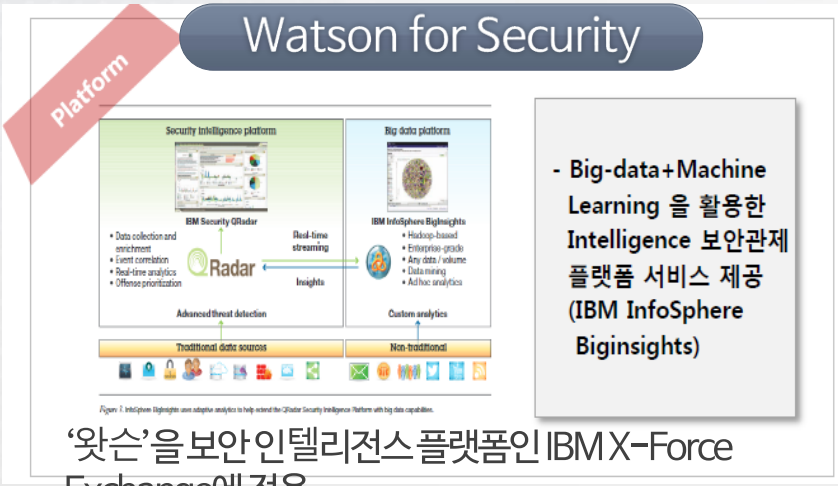
Caspida- Machine Learning 적용

각종 장비로부터 수집되는 정상적인 Event의 자동 인식으로 99.99%의 탐지 Event 감소

Splunk Enterprise Security



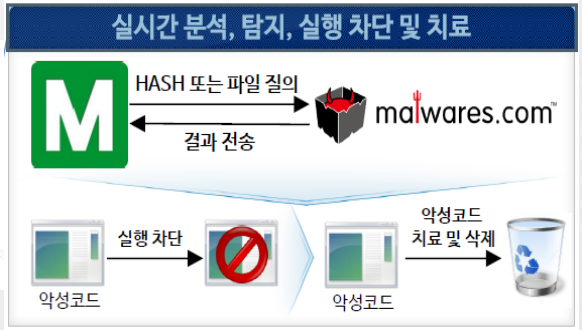
Watson for Security



- Big-data+Machine Learning 을 활용한 Intelligence 보안관제 플랫폼 서비스 제공 (IBM InfoSphere Biginsights)

'왓슨'을 보안 인텔리전스 플랫폼인 IBM X-Force Exchange에 적용

Cylance Protect & MAX



AI 기술 활용 가속화(CGC)

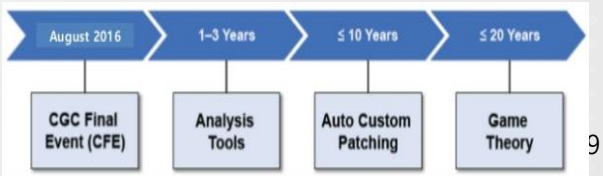
- '16년 10월, 미 백악관에서는 「인공지능의 미래를 위한 준비(Preparing for the Future of Artificial Intelligence)」란 보고서에서 AI와 사이버보안과 관련해서 중요 내용으로 CGC가 사이버 위협을 사전에 탐지하고 평가하며 소프트웨어 취약점에 대한 패치 작업을 할 수 있는 **고급 자동화 시스템 개발을 독려하고 가속화하기 위해 기획된 경연 대회임을 밝힘**

CGC(Cyber Grand Challenge)

목표 : 기계가 제로데이를 찾아내고 그것을 해결하는 패치를 만드는 전 과정을 자동화는 기술 확립. 몇 분 이내(소프트웨어의 리버스 엔지니어링, 취약점 발견 및 검증 패치 작성, 적용까지 모든 공정을 완전 자동)에 이 문제를 자동으로 해결하는 것이 목적. CGC 프로그램 관리자인 DARPA 마이크 워커는 "우리는 보안 라이프 사이클 전체를 자동화 할 수 있다는 것을 증명하려 한다."고 말했다. 보안 모니터링을 자동화하고 더 강한 네트워크를 만들기 위한 10년 계획의 첫 번째 단계라고 말함.

- ✓ DARPA는 우승상금으로 200만달러(약 22억)와 CGC 경기환경 준비·구축비로 3년 동안 5,500만달러 (약 629억원)의 자금 투자
- ✓ 자동화 시스템의 핵심인 "자동 추론"(Automated Reasoning) 기술을 활용해 CGC는 보안 대책의 자동화라는 단기 목표의 실현뿐만 아니라 인공 지능의 고도화라는 장기 테마로 중요한 역할 담당
- ✓ DARPA는 이번 경기의 대상이 된 기술을 "CRS (Cyber Reasoning System = 기계 학습 등을 이용하여 고급 추론하는 시스템)라고 부르며, AI기술과는 구별하고 있지만, 보안 AI화도 시작에 들어 가 있다고 말함.
- ✓ 자동운전 자동차 경주가 실용화 가능성이 보일 때 까지 약 10년이 걸렸지만 보안자동화 시스템은 3년~5년 이내 상용화 가능

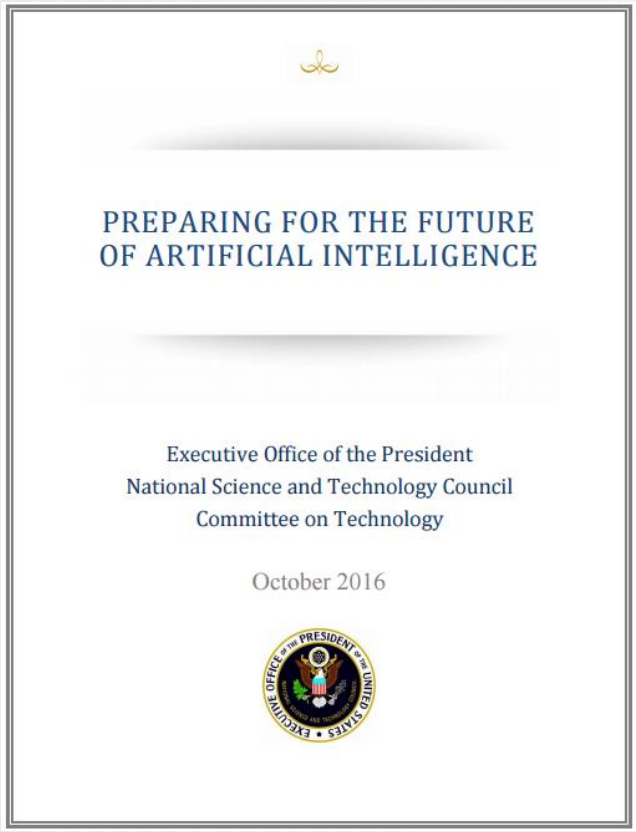
- ✓ 3년 내 해킹으로 악용될 가능성이 있는 취약점을 자동으로 찾아주는 프로그램 개발
- ✓ 10년 내 자동 보안 패치 프로그램 개발
- ✓ 20년 내 완전 자동화된 인공지능 네트워크 방어 프로그램 개발 추진



미국의 전략

AI 기술 적용 및 AI시스템 보안 강화

미국 국가과학기술위원회(National Science and Technology Council, NSTC)는 2016년 10월 인공지능(AI) 의 향후 방향성을 검토하는 보고서 「인공지능의 미래를 위한 준비(Preparing for the Future of Artificial Intelligence)」를 발표함


PREPARING FOR THE FUTURE
OF ARTIFICIAL INTELLIGENCE

Executive Office of the President
National Science and Technology Council
Committee on Technology

October 2016

- ✓ 보고서는 사회에 여러 가지 혜택을 제공하는 AI를 더 긍정적인 방향으로 유도한다는 관점을 제시
- ✓ 이를 위해, △도입 부문에서 AI의 개념·현황·역사를 요약한 후 △공공의 이익을 위한 AI의 활용 △미 연방정부에서의 AI △AI와 규제 △연구 및 관련 인력 양성 △AI와 자동화가 경제에 미치는 영향 △공정성, 안전, 거버넌스의 문제 △글로벌 상황에 대한 고려와 보안 관련 내용을 검토
- ✓ 좁은 인공지능(Narrow AI)은 사이버보안 분야에서 매우 중요하게 활용되고 있으며, 방어형 보안(defensive 혹은 reactive)과 공격형 보안(offensive 혹은 proactive) 등 영역 모두에서 역할이 점점 더 확대될 것으로 전망됨
- ✓ 미래의 AI 시스템은 **예측 분석(predictive analytics)을 통해 사이버공격을 미리 예상**할 수 있을 것으로 기대 – 이 같은 기능은 막대한 데이터를 통해 다양한 동적 위협 모델(dynamic threat model)을 구축함으로써 가능함
- ✓ **AI시스템 및 구동되는 애플리케이션들은 △데이터와 기능(functionality)의 무결성을 보장하고 △프라이버시와 기밀을 보호하며 △항상 이용 가능한 상태를 유지하기 위해 건전한 사이버 보안 통제가 요구**

일본의 전략

AI 네트워크화에 따른 검토 보고서

총무성 정보통신정책연구소는 AI기반의 산업의 급격한 발전에 따라 AI 개발 피해방지 및 글로벌 AI 개발 주도권 확보를 위해 AI 개발 원칙 마련('17.1).

구분	주요내용
투명성의 원칙	AI 네트워크 시스템의 동작검증 가능성 및 설명 가능성을 확보할 것
제어가능성의 원칙	AI 네트워크 시스템의 제어 가능성을 확보할 것
보안 확보의 원칙	AI 네트워크 시스템의 견고성과 신뢰성을 확보할 것
안전 보호의 원칙	AI 네트워크 시스템이 이용자 및 제3자의 생명·신체의 안전에 위해를 미치지 않도록 배려할 것
개인정보보호 원칙	AI 네트워크 시스템이 이용자 및 제3자의 프라이버시를 침해하지 않도록 배려할 것
윤리의 원칙	AI 네트워크 시스템의 연구 개발에 있어서 인간의 존엄성과 개인의 자율을 존중할 것
이용자 지원의 원칙	AI 네트워크 시스템이 이용자를 지원하고 이용자에게 선택의 기회를 적절히 제공하도록 배려할 것

✓ AI 보안 리스크 평가, 보안 중심 설계, 지속적인 취약점 점검 등 포함

✓ 개발 원칙의 실효성 확보를 위한 장치

– 공공 조달의 대상으로 하는 AI 및 공적 연구비의 교부 대상으로 하는 AI에 관해 개발 원칙에 입각하여 조건을 설정

– 시장의 기능을 활용하여 개발 원칙을 준수하는 AI가 시장에서 경쟁력에 우위를 가질 수 있도록 환경을 정비

① 개발자가 제공하는 정보에 근거하여 제3의 기관이 해당 AI가 개발 원칙을 준수하고 있는지 평가하여 인증하는 제도 운용 검토

② 배상책임제도의 수정: ①의 인증을 받은 AI의 이용으로 인하여 이용자가 제3자에게 손해를 입힌 경우, 해당 이용자의 법률상 책임 등을 감면하는 제도 운용

지능정보사회 중장기 종합대책 추진방향(1/2)

KISA Korea Internet & Security Agency

- '16년.12.15일에 범정부「제4차 산업혁명에 대응한 지능정보사회 중장기 종합대책」을 확정

① 기술

» 글로벌 수준 기술기반 확보

01 미래 경쟁력 원천인 데이터 자원의 가치 창출

02 지능정보기술 기반 확보

03 데이터·서비스 중심의 초연결 네트워크 환경 구축

② 산업

» 全 산업 지능정보화 촉진

04 국가 근간 서비스에 선제적 지능정보기술 활용

05 산업생태계 조성으로 민간혁신 파트너 역할 수행

06 지능형 의료서비스를 통한 혁신가치 창출

07 제조업의 디지털 혁신

③ 사회

» 사회정책 개선 및 제도정비

08 지능정보사회 대비 교육혁신

09 자동화 및 고용형태 다변화에 적극적 대응

10 지능정보사회에 대응한 사회안전망 강화

11 지능정보사회 대비 법제 정비 및 윤리 정립

12 사이버위협, AI 오작동 등 역기능 대응

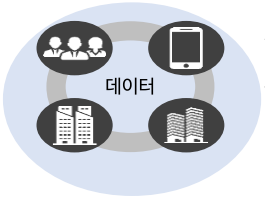
02 보안 내재화된 고신뢰 네트워크 구축

- 해킹 원천 차단 양자암호통신 단계적 도입 추진

1단계('20년)	2단계('25년)	3단계('30년)
전용회선 구간 (국가핵심시설, 데이터센터)	공용망 (국방·재난·행정·금융망, 클라우드 등)	양자인터넷 핵심기술 개발 및 인프라 구축

- 재난망에 AI 기반 고신뢰 네트워크 적용

기계 학습이 가능한 데이터 기반 구축



- 공공데이터 포맷 전환·개방
  - ✓ 공공 빅데이터 확대('18 20개→'25 320개)
  - ✓ 의료·특허·언어 등 데이터셋 구축·제공
- 데이터 보유기관의 클라우드 도입
  - ✓ 클라우드 규제 개선 및 선도 프로젝트 추진
- 데이터 보유-분석기업 컨소시엄 지원

안전한 데이터 유통·활용 촉진

일반정보

비식별정보

개인정보

- 개방형 플랫폼 데이터 거래소 구축
  - ✓ 가치에 기반해 거래되는 데이터 시장 조성
- 데이터 프리존 운영
  - ✓ 데이터 비식별화 지원 및 데이터 결합을 자유롭게 시험
- K-MyData 프로그램 도입
  - ✓ 개인 동의 기반 개인정보 활용 지원

지능정보사회 중장기 종합대책 추진방향(2/2)

해킹·오작동 등 기술적 위협에 효과적으로 대비하여 사회 불안감 해소

지능형 자율 방어체계 실현

- **사이버보안 빅데이터 센터 구축**

AI 기반 제품, 비정형 데이터까지 탐지

- **개인 맞춤형 지능 보안 시스템**

✓ 개인용 AI 기기·서비스의 보안 취약점 자동 관리

사람+사물 지능형 통합 인증

- 사물 식별·인증체계 개발

✓ 다양한 AI기기로 인증대상 확대

경량화된 사물인증 기술 개발

- 인공지능 기반 자동인증 및 이상 징후시스템과 자동 연계

이상징후감지 + 실시간 대응 시스템

지능정보SW 안전성 평가

- 全산업 SW안전성 인증

✓ 적합한 데이터 사용, 오작동 탐지

자동차, 의료기기, 정보통신 분야 등

- 보안성 평가체계 마련

✓ 설계시부터 SW안전성 및 보안성이 확보될 수 있도록 평가체계 마련

AI 기기·시스템 설계 ~ 활용 全 단계

주요 선진국과 첨단기술 공동연구 확대
사이버 위협 정보 공유 강화 및 대응 공조 체계 구축

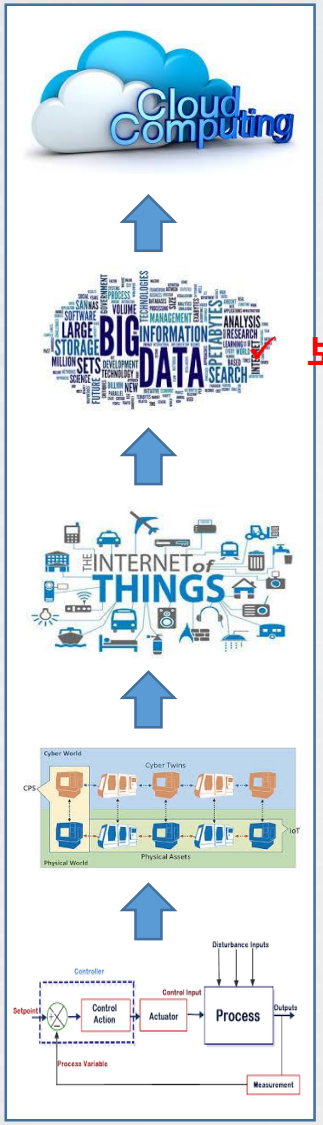
4차 산업혁명시대의 新 보안 패러다임

- IoT·CPS 확산에 따라 정보의 처리에서 → 사물을 제어하는 방향으로 기술이 변화됨에 따라 인명 등 Safety에 관련된 위협 도래
- 특히, 자동차, 의료, 플랜트 등의 분야에서는 Safety와 Security 각각의 분석방법을 통합 고려해 공통된 개념을 정리하고 통합하는 가이드라인 마련 필요

환경 변화	새로운 위협	보안 대책
기술의 변화 "정보"의 처리 -〉 "사물"의 제어	인명 등의 안전에 관한 위협 확대	안전 및 보안의 통합적인 대책 구축
비즈니스 모델의 변화 "제품" → "서비스" →공유・이코노미 → 제로・한계 비용 사회	다양한 사용자의 보안 인식과 지식 차이	취약점을 자동 관리하고 필요에 따라 자동으로 업데이트하는 기반 정비 (자가 치유형 보안)
프로세스 혁신 공급망 다양화	공급망 리스크의 확대 (조달 부품의 백도어, 악성 기능의 삽입 위험)	공급망 위험 관리
제품 혁신 드론, 자동 운전, 간호 로봇, 감시 카메라 등 새로운 기기의 등장	제조사의 보안 고려 불충분	분야·영역별 취약점 정보 공유 기반, 보안 코딩 확보
기타 혁신 경제혁신 물류혁신	기술 정보 유출 및 개인 정보보호 유출 위험	데이터 분석의 보안성 확보 (익명화, 안전한 다자간계산 등)

- ✓ 국가 전체 측면에서 Risk 경감 방안 고려
  - Economic of Security 고려
- ✓ 정부규제 신중한 고려, 기업·시장의 역할 강화
  - Negative 규제
  - 규제와 진흥의 조화
- ✓ 주력산업 글로벌 경쟁력강화
  - 스마트가전 수출대비 등
- ✓ 사후대응 → 능동적, 공세적 방어 대응
- ✓ 산업 측면 국제공조 필수
  - 글로벌 공동기준 마련 등

영역·Layer별 고려사항



IoT

CPS

ICS

⑥ Functions and data move to cloud

✓ 보안플랫폼 부재

⑨ Big Data causes confidentiality problems

⑦ Need for trusted identities and trustworthy infrastructure

⑧ Security by Design to cope with complexity

③ Core services are outsourced

⑤ Loss of perimeter control

① Hacking cyber-physical systems

② No air gap, everything connected

④ Shared ownership of machines

✓ 산업별 전문가 협력 부족

✓ 산업별 보안가이드 부족

✓ 보안기술 개발자 부족

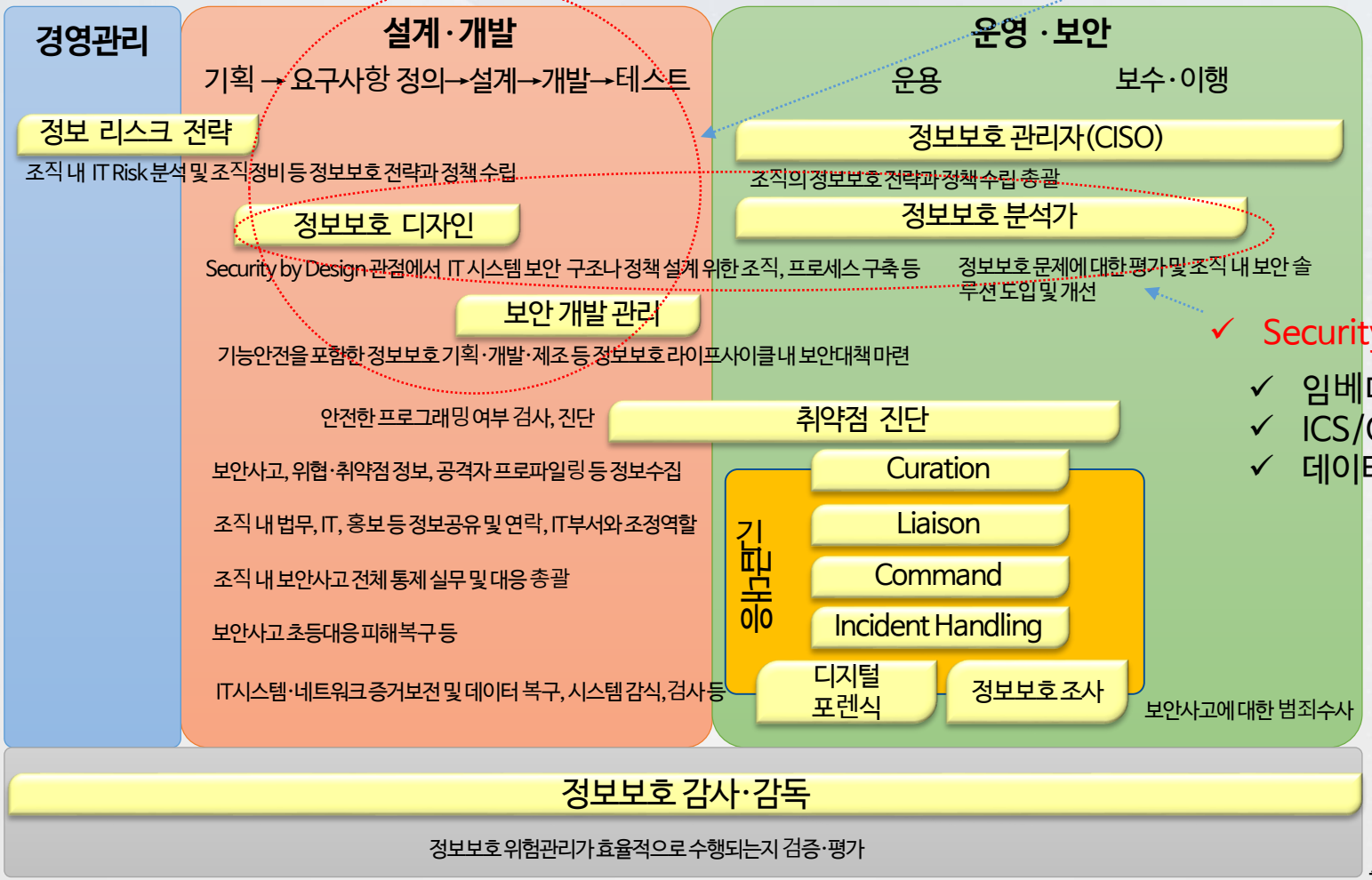
✓ Embedded Security 기술 부족

✓ 접근 어려움

① 인력은?

보안 엔지니어 & Security Architecture

✓ 보안 엔지니어(기술개발)



✓ Security Architecture

✓ 임베디드 보안전문가
✓ ICS/CPS 보안전문가
✓ 데이터 분석가

출처: 일본 IPA재편집

② 산업은?

산업별 보안전문기업 & AI기술 적용 가속화

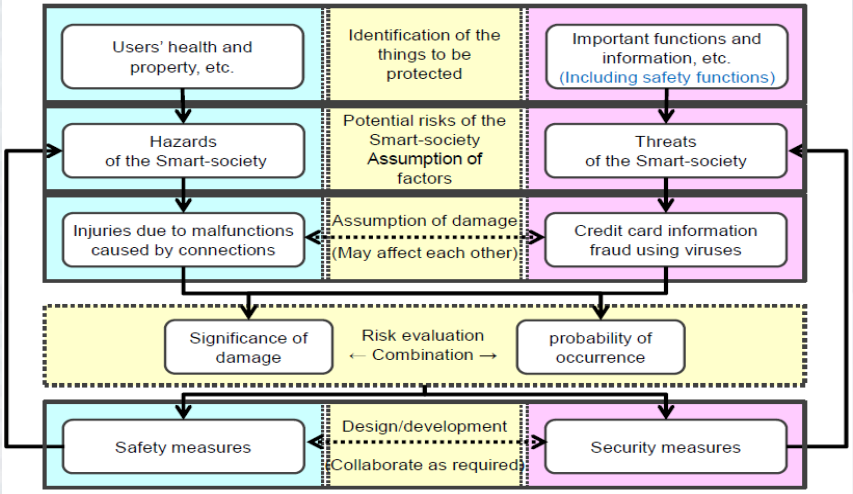
- **기존 보안기업 → 산업별 전문보안기업으로(주력산업·제품에 보안기능 내재화)**
  - ☞ No – Box, Secaas(클라우드 기반 보안서비스) 전문기업, ex) 자동차 보안 전문기업

- **AI(머신러닝, 딥러닝 등)기술을 활용한 보안위협 전단계(취약점↔공격↔방어↔패치) 자동화**
  - ☞ 머신러닝 기반 Anti-Malware, 인지·학습·추론을 통한 침입탐지·차단 솔루션 등 각종 보안이벤트 정보를 자동 수집·분석해 보안 위협을 확인하는 수준에서 → 클라우드컴퓨팅 연산자원 활용 및 보안특화 알고리즘 개발을 통해 각종 공격이 어떤 방식으로 들어오는지를 학습하고, 이를 통해 적절한 대응방법을 적용

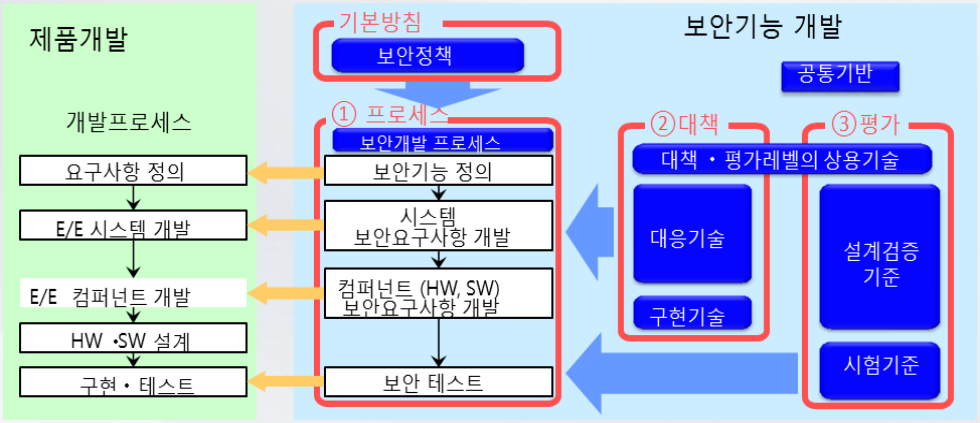
- **Unified(통합)을 넘어선 → Fabric(직물 구조)을 통한 보안관리 서비스 전문기업으로**
  - ☞ 클라우드, 사물인터넷(IoT)로 분산된 네트워크에서 각각 다뤄지던 보안을 네트워크 인프라 중심부에서 통합
  - ☞ 인텔리전스 전문 서비스 기업 육성

③ 기술개발은?

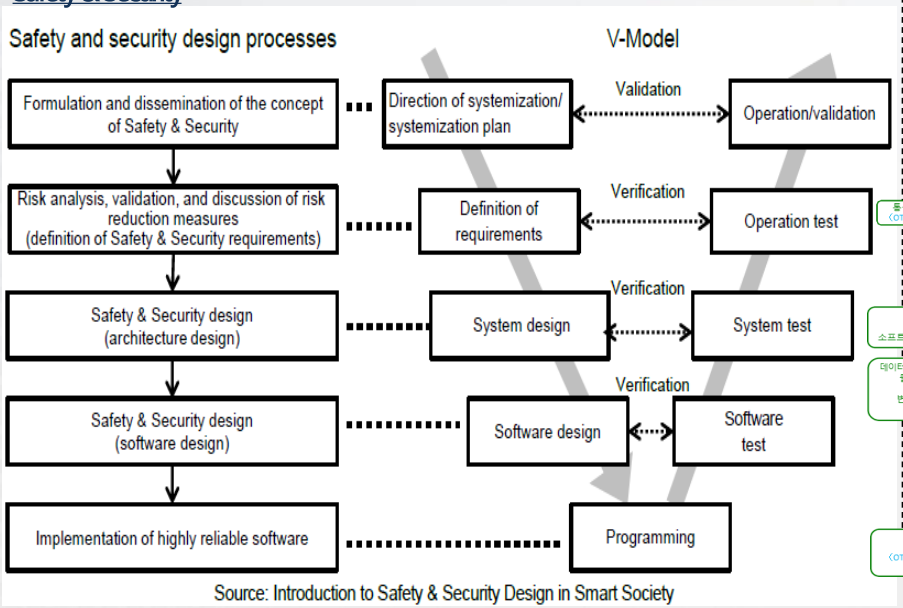
Risk Analysis



Security by Design

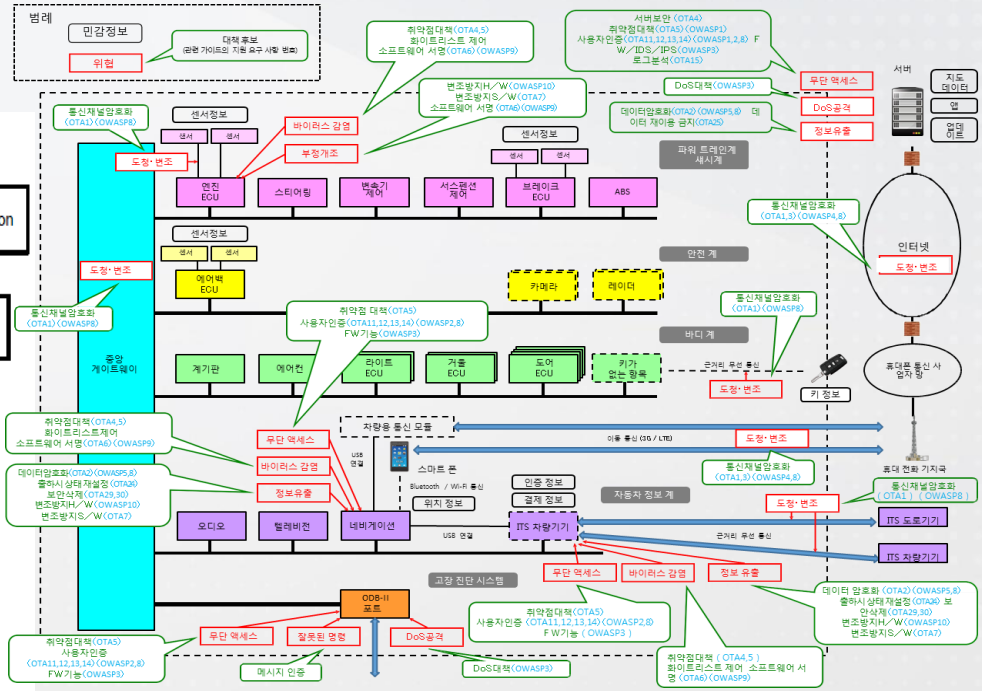


Safety & Security



Source: Introduction to Safety & Security Design in Smart Society

Threat Modeling



출처: SAE, IPA, DENSO 재편집

④ 정부는?

공유· 협업 체계 강화

침해대응 : 능동적 탐지·대응(Offensive Security) 체계 마련

☞ AI기반 네트워크 관제·대응 : CTI, 다크웹 분석, K-Shodan 구축·운영

☞ 자율 학습형 면역시스템 및 자가방어 체계 구축 : 자가변이·치유, 전송경로 변경 등

정보공유 활성화 & 제품 취약점관리 체계 마련

☞ 국가 취약점 관리 체계 구축 : 국내 제품, 서비스 등 CVE/CPE/CVSS + STIX/TAXII 체계 구축

☞ 사이버 위협 빅 데이터 센터 구축 : 이기종 기기/비정형 데이터 수집 → 인공지능 훈련·시험용 공공데이터 공유 환경 조성

善 자율 後 책임 원칙의 개인정보보호 강화

☞ 규제 중심의 수동적 보호를 탈피 하여 기업, 기관의 책임을 강화하는 先 자율 後 자율 책임 원칙 확산

AI 연구 개발 지침, 역기능 대응을 위한 민·관 공동 협의체 마련·운영

☞ 정부기관들의 각종 계획과 전략들은 사이버 보안에 대한 AI의 영향 고려

☞ 보안 위협에 대한 AI 시스템과 생태계의 안전성과 회복력을 보장할 방안을 강구

☞ AI를 효과적이고 효율적인 사이버보안 활동에 적용할 수 있는 혁신적 방안들을 강구

결언

01 1, 2, 3차 산업혁명과 달리 4차 혁명의 시대로 빠르게 진입 중
또한, 지능정보사회를 선도하기 위해서는 사이버보안이 필수불가결한 전제조건

02 공공과 민간 모든 이해관계자가 머리를 맞대고 사이버보안 기술개발과
이를 뒷받침할 정책을 마련하는 등 각고의 노력을 경주해야 함

03 제4차 산업혁명에 따라 산업 全 분야에 보안내재화 등 보안인력, 산업구조 변화가
예상됨에 따라, 민간과 공공, 각 산업영역별 구분 없이, 횡단적인 보안정책 수립 필요

04 지능정보사회 보안을 위한 전담기관 마련 등 지능정보사회의 모든 혜택을 향유할 수
있도록 학계, 업계, 정부 등과 함께 적극 협력 필요