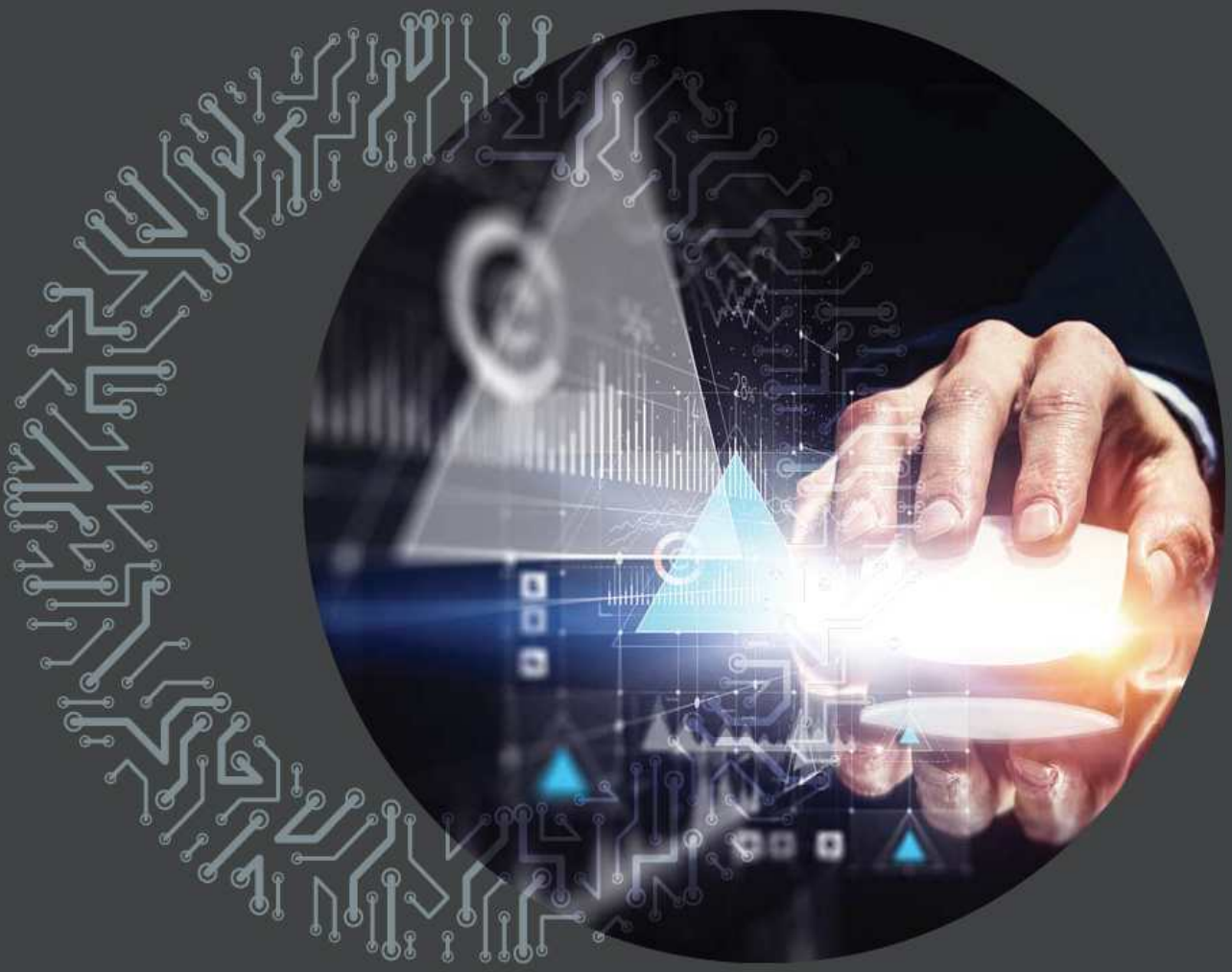
ETRI Insight

Insight Report 2017-40

기술경제연구본부/미래기술연구본부
정지형 · 안창원 · 이지형 · 석왕헌 ·
허필선 · 조영환

Insight Report

공공수요형 IDX 추진을 위한 산업환경 및 생태계 분석



ETRI Electronics and Telecommunications Research Institute

※ 본 보고서의 내용은 필자의 개인적인 견해이며, 한국전자통신연구원의 공식 견해가 아님을 알려드립니다.

본 문서에서 음영처리된 부분은 ( ) 정보공개법 제9조의 비공개대상정보와 저작권법 및 그 밖의 다른 법령에서 보호하고 있는 제3자의 권리가 포함된 저작물로 공개대상에서 제외되었습니다.

CONTENTS

요 약

국방 IDX 전략

국방기술력의 현황과 문제점

- 국방기술품질원의 국방기술력 수준 조사에 따르면 종합적인 국내 국방기술 수준은 주요 16개국 중 9위이며 감시정찰, 항공우주, 화력 등은 상대적 약세
  - 국내 방위산업체 기술력은 4개 무기체계 분야 12개 주요 방위산업 완제품과 46개 핵심기술에서 세계 최고수준의 71.0 수준
- 국내 국방기술 기획이 정밀타격, 무인전투, 감시정찰, 항공우주 등의 세계적인 국방기술투자 추세를 따르고 있다고 볼 수 있으나 실제 확보가능한 기술수준이 전력 우위를 담보한다고 판단하기는 어려움
  - 미국 등 주요 군사 강국들은 감시정찰, 정밀타격, 항공우주, 무인전투 등을 중심으로 국방과학기술 투자를 추진, 국방 역량 첨단화에 매진 중
- 국내 민·군기술협력은 무기체계 적용을 위한 추격형 개발사업에 치중하고 있어 민간 부문의 최신 기술혁신 성과의 국방 도입을 위한 장기적·체계적 접근으로서는 한계가 있는 것으로 판단됨
  - 주요국들은 국방력 강화를 위해 AI, 3D 프린팅, IoT 등 민간에서 촉발된 기술혁신 결과물을 국방과학기술에 적극적으로 접목하는 중

미래 국방 전망

- 정보화 시대를 지나 AI, 로봇, 4차 산업혁명의 시대로 접어들고 있는 현재 새로운 기술들이 전쟁과 평화의 방법론을 데이터, 네트워크, 지능, 인간·기계 복합체계에 기반한 것으로 변화시키는 중
- 정보화 시대의 전쟁이 인식·정보의 중요성을 강조한다면 빅데이터, AI, IoT 등 지능화 기술이 본격적으로 활용될 미래전은 전황 분석 및 무기체계 운용에 적용될 기계화된 지능의 중요성이 부각될 것으로 전망
  - 미래전에 나타날 기술적 선택지들은 무한히 다양할 수 있으나 군사 전문가들은 로봇, 사이버전, 에너지 무기와 AI, 무인경계, BCI(Brain-Computer Interface), 우주 기반 전투기술 등을 주요 기술로 제시
  - 무기체계 첨단화와 고성능화에 따른 비용 증가, ICT를 중심으로 이루어지고 있는 첨단 기술의 세계적 균등화로 인해 저비용·비주류 국방 기술에 기반한 미래전 또한 발생가능한 미래

- 발전된 기술의 국방 적용은 미래 전투가 보다 넓은 전장에서, 혁신기술이 적용된 무기를 동원하여, 실시간 정보공유·의사결정을 통해 진행되도록 변화시킬 것으로 예측됨
  - (전장공간) 인지·정보 능력과 지능화된 무기체계가 전쟁 승리에 미치는 영향이 증가하면서 지상, 해양, 공중 등 전통적 전장공간 외에 사이버 및 우주라는 새로운 전장 영역이 추가
  - (전투수단) 장거리 정밀타격력, 무인전투체계, 비전통적 무기체계의 활용이 증가하면서 국가의 전반적인 과학기술력이 군사적 타격능력에 직결
  - (전투형태) 전장공간의 확장, 신기술 기반 전투수단의 등장으로 인해 전략적 중심 마비의 스마트 전투, 네트워크 중심 전투, 운용 중심의 전투가 미래전의 전개 양상이 될 것으로 전망

국방 IDX의 정의

- 국방 IDX는 ICT 및 관련 융합기술의 국방 부문 도입을 통해 미래전쟁 양상 변화에 대비하고 국방 무기체계와 국방 지원 부문의 효율성과 효과성을 제고하기 위한 국방기술혁신 전략
  - 전투 공간의 확장, 무기의 정밀화·무인화, 전투 수행의 유연화·스마트화 등의 미래전 변화에 대응하기 위해 ICT 및 관련 융합기술 부문의 신기술을 개발·활용
  - ICT 및 관련 융합기술 부문에서 기확보된 기술역량을 국방 부문에 적용하고 군의 소요 충족을 위해 기초·원천·응용 기술을 연구개발

국방 IDX를 통한 미래 국방 변화상

- 초연결 데이터 중심전
  - 운용 중심 전투 실현을 위해 5차원 전장 공간의 초연결로 획득한 정보를 식별·탐지한 데이터의 실시간 공유·분석으로 결심권자의 신속한 지휘 가능으로 초연결 데이터 중심전(HCDcN)의 미래상을 구현할 것으로 기대
- 공세적 사이버 중심전
  - 5차원 전투 공간 및 지휘통신의 초연결로 이루어지는 사이버상에서, AI 기반의 능동적 방호 체계와 공세적 사이버 방호로 전·후방, 전·평시에 무관한 안전한 국방망 실현을 기대

◐ 실시간 무인감시정찰 체계

- 드론, 경계 로봇, 스마트 센서, 무인 감시정 등에 지능을 탑재하여 실시간 정밀 분석을 하는 무인 지능적 감시정찰 체계로 기존 인간의 오감기반 경계·감시를 대신하여 무인 국방이 실현될 것으로 기대

◐ 지능 중심전

- 국방 데이터 지능형 정밀분석 기술이 전투병·전투무기체계·전투지원체계와 작전지휘 의사결정 분야에 도입되어 인적·물적 손실피해 최소화 전장 운영을 가능하게 하며 전투력 자율 증강 등을 기대

◐ 실 가상화 지능 훈련체계

- 시뮬레이션 기구, 가상현실, 워 게임 등이 통합된 실 가상화 지능 훈련체계 도입을 통해 무인전투체계, AI 기반 전장분석 및 지휘결심보조 등 새로운 전투환경에 투입될 지휘관·병사의 능력을 최고수준으로 연마

행정 IDX 전략

행정 IDX 개념 정립

- 행정 IDX(Intelligent Digital Transformation) 정의 : 중앙정부 또는 지방자치 단체의 목적을 실현하기 위한 사람과 물자를 관리하는 운영과정이나 정책결 정과 집행을 중심으로 하는 정책과정에서 운영의 효율을 높이고 조직 성과를 향상시키기 위해 행정 시스템을 디지털로 전환하고, 유기적으로 통합하여 지능형으로 발전시키는 과정 또는 플랫폼

행정 분야 생태계 분석

- **행정 데이터 수집 Player들**
  - 각 행정업무 담당자
  - 지자체 IoT 인프라 관계자
  - 지자체 정책 수집 관계자
  - 국가 공공데이터 수집 관계자

- **행정 서비스 앱 개발자들**
  - 사회, 경제, 복지 전문가들 : 대학교수, 사회복지사, 시민사회운동단체,
  - 데이터 분석가 : 경제학자, 사회학자, 통계학자, 빅데이터전문가
  - 공공앱 개발자 : 정부가 직접 앱을 개발·운영하는 방식을 탈피, 필요한 공공서비스 기능을 '정부가 제안'하고 정부는 원천 데이터를 제공하고 '민간이 개발·운영'하는 민간앱 개발 공모전도 개최하여 창업 활성화 지원

- **행정 서비스 사용자**
  - 지자체 정책결정 공무원 : 환경복지, 도시건축, 경제 일자리, 안전 등 지자체 공무원

행정 IDX 추진 포인트 도출

- Data 융합연계 Platform (디지털 트윈의 실세계 데이터 반영을 통한 높은 정확도)
- 통합/복합 모델링 프레임워크 (ABM의 미시적인 모델을 통한 높은 정확도와 컴퓨팅 환경의 급격한 성능 향상)
- 다차원 시뮬레이션 엔진 (실제 도시 정책 데이터와 실시간 현실 데이터를 정합한 실환경 반영으로 정확도 향상)

행정 IDX 미래상

- **정책과정 혁신 (Policy-Making Excellence)**
  - **데이터 기반 정책 수립** : 정부가 확보한 수많은 데이터를 기반으로 재난, 범죄, 서비스 수요을 예측해 최적의 대책을 수립할 수 있는 인공지능과 빅데이터가 결합된 인지·예측 기반 지능행정 기술이 구현될 것
  - **AR/VR 기반 원격 행정** : 미래에는 VR 시스템이 구축된 가상 회의실에서 회의를 하는 것이 당연해지는 시대가 될 것
- **운영과정 혁신 (Operational Excellence)**
  - **AI 기반 실시간 여론조사** : 정치 및 정책 결정권자가 연설이나 토론을 할 때 인공지능 컴퓨터가 공적 발언의 사실 여부를 실시간으로 판별해 알려주어 사실에 기초한 검증된 토론이 가능해질 것
  - **직접 민주주의로 새로운 정치질서** : 얼굴 인식, 생체 인식, 블록체인 기술 등을 활용한 인터넷 투표로 디지털 직접민주주의가 확대될 것

교육 IDX 전략

교육 IDX 개요

- **(개념)** 교육에 고도화된 IT기술이 적용이 본격화되어 교육시스템이 지능화, 실감화가 가능하게 변화함에 따라 개인별 맞춤 교육을 효과적으로 지원하는 교육 패러다임 및 환경을 의미
- **(범위)** 교육이 일어나는 공간을 중심으로 교육 IDX의 범위를 한정해 교육현장, 가정 공간, 산업 응용 및 온오프 연계로 설정

교육 문제점 및 IDX 수요 도출

- **(교육현장)** 교육의 효율성·지속성·형평성 문제를 해결하기 위해 개인별 인공지능 교사를 두게 함으로써 불필요한 사교육 근절 및 교육의 효율성을 극대화
- **(가정공간)** 사회변화로 인한 가정, 장애아, 고령화 문제가 지속적으로 발생하는 문제를 해결하기 위해 가정용 로봇을 도입해 가정교사로 활용
- **(산업응용)** 직업교육의 장비의 고비용성, 난이도, 부상 등의 문제를 해결하기 위해 가상증강현실 기술을 활용한 실감 및 체험형 학습시뮬레이터 개발·보급
- **(온오프 연계)** 물리적·환경적 제약으로 인하 현장학습의 한계점을 가상증강현실 기술을 이용해 극복

교육 IDX R&D 전략 방향

- **(프로젝트형 R&BD 추진)** 플래그쉽 프로젝트를 구성하고 그에 맞는 R&BD 추진 필요
- **(사회문제 해결을 위한 R&D)** 현재 발생 및 진행 중인 교육관련 사회문제를 해결하기 위한 다양한 R&D가 필요
- **(원천/응용기술 R&D)** 전자·정보·통신의 원천기술 개발과 함께 교육과 관련된 응용기술을 개발하는 형태를 취할 필요

Cybersecurity IDX 전략

Cybersecurity 분야 생태계 분석

- 최근에는 ICT 산업은 물론 비ICT 산업 등 모든 산업이 기존 아날로그 방식을 탈피하여 디지털로 전환되는 디지털 트랜스포메이션 (Digital transformation)이 일반적인 추세

  * 예를 들어 항공기의 전자부품 비중이 2005년 10% 에서 2013년 30%로, 의료기기 중 전자의료의 기기 비중이 2005년 10% 에서 2013년 45%로, 자동차의 전자 부품 비중이 2005년 23%에서 2013년 60%로 가파르게 상승하고 있음

- 향후에는 국가 전반에 걸쳐 모든 산업 분야를 포함한 거시적 및 미시적 경제시스템의 디지털 포메이션이 한층 가속화 될 것임. 경제시스템은 크게 3가지의 하위 시스템으로 구성되고 있으며, ① 생산시스템 ② 소비시스템 ③ 생산과 소비를 연결하는 제 3의 시스템 등임. 이들 각각이 디지털 트랜스포메이션화 될 것이며, 이들이 상호 연동 되어 운영될 것임. 특히 생산과 소비를 연결하는 제 3의 시스템은 CPS 및 IIoT가 주요 구성요소로 자리 잡을 것임. 또한 CPS 와 IIoT가 전방에 있는 생산시스템과 후방에 있는 소비시스템을 연결하는 가교 역할을 할 것임

- Cybersecurity 생태계는 CPS 및 IIoT를 중심으로 하여, 관련 제품 및 솔루션, 산업 분야, 리스크 관리, 설치 유형, 서비스 포트폴리오, 보안 유형, 설치 플랫폼, 거버넌스, 보안 작업, 보안 공학, 프레임워크, 표준 및 규제 프레임워크, 경력 개발, 위협 지능, 사용자 교육 등을 포함하는 매우 범위가 넓은 도메인으로 구성됨

IDX 추진 포인트 도출

- IDX 플랫폼 상에서의 가치 창출 네트워크는 IDX 플랫폼에 연결되어 있는 사람, 기계 및 시스템, 환경 간의 네트워킹을 추진하고, 기업 IT 및 인터넷과의 밀접한 연결을 견인할 것임. 외부 공격으로 부터의 보호 및 내부 침입자의 조작에 대한 보호는 IDX 플랫폼으로 부터의 다양한 요구사항을 충족시켜야 할 것임
- (기본적인 보호해야 할 대상) IDX 플랫폼과 연결된 생산 영역 내에서 보호할 대상은 다음과 같음. : ① 가용성, ②무결성, 및 ③기밀성의 보호 등임. 추가적으로 ① 확실성, ② 시간의 무결성(특히 기업 범주를 벗어난 가치 네트워크와 관련), ③ 추적가능성, ④ 법적 보안 등
- (IDX를 위한 보안 설계 (security by design)) IDX 플랫폼을 구현하기 위해서, 정보 보안을 위한 조치를 신속성 있게 고려해야 함. 보안을 위한 기술적 메커니즘을 소급 통합하는 것 보다는 IDX 플랫폼과 연결되어 있는 제품 개발 및 프로세스와 관련한 통합적 접근방법은 시스템 및 인프라의 보호를 위해서 요구
- (가치 네트워크의 동적 구성 가능성) 효과적인 가치 네트워크는 IDX 플랫폼의 동적 형상/재형상을 요구함. 보안 관리는 IDX 플랫폼의 동적 성격을 지원해야 함. IDX 플랫폼 상의 구성요소의 보안 특성(보안 프로파일)이 표준화된 언어 (보안 시맨틱)로 설명되는 것이 필수적이며, 한편으로는 이는 통신 인터페이스/프로토콜과 이들의 보안 특성을 명확하게 설명해야 함

Part 1

국방 IDX 전략

Ⅰ 국방 분야의 개요 및 연구범위

국방의 개념

- 국방(國防)은 국가가 국민과 영토, 영해, 영공 등 자국 영역의 안전을 내외부 위협으로부터 지키며, 경우에 따라서 이들의 보존과 안정을 위하여 국가가 지닌 모든 권력과 수단을 동원하는 행위 및 제도라 할 수 있음
  - 국방은 안보, 안전보장 등의 명칭으로 불리기도 하며 극단적인 상황에서는 국가가 동원할 수 있는 폭력 수단을 타국가, 조직, 개인에게 사용하는 전쟁과 전투를 통하여 국민과 자국 영역을 보호
- 합법적인 폭력집단인 국가는 국방을 위한 무기체계와 이를 운용하기 위한 인력으로 구성된 군대를 보유, 관리함으로써 국방 역량을 유지
  - 1928년 체결된 파리부전조약 체결 이후, 국제법 상으로 방위전쟁 외의 침략전쟁은 금지되었으나 세계 각지에서 내전, 국지전 등은 지속적으로 발생하고 있어 적정한 국방력은 국가 유지에 필수적

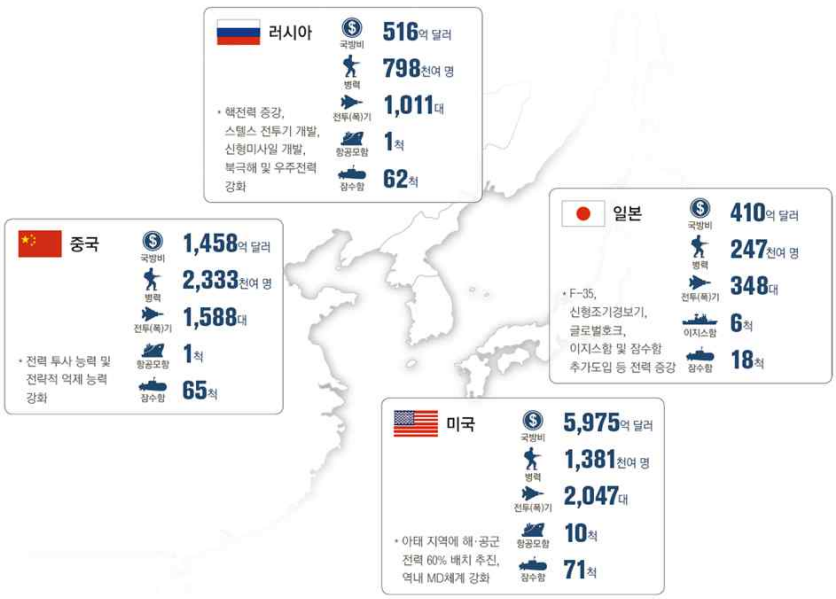
국방과 국방 산업

- 세계 국방 산업 시장은 1조 달러를 상회하는 큰 시장을 형성하고 있으나 본 보고서에서는 국방의 산업적 측면보다는 국가의 자주성과 정치외교적 영향력 확보를 위한 국방의 의미에 집중
  - 2016년 국방 예산 규모 측면에서 1~10위를 보인 10개국의 국방 예산 합계액은 1조 2천 억 달러를 상회하고 있어 국방 산업의 세계 시장 규모는 천문학적 규모
    * 2016년 국방 예산 규모 측면에서 1위인 미국은 6,171억 달러, 10위인 대한민국은 335억 달러 규모의 국방 예산을 집행
  - 분단 상황에서 군사적 긴장이 상존해있는 대한민국의 특성 상 산업으로서의 국방이 아니라 적정한 국방력 확보를 통한 국가 자주성 및 안정성 확보가 보다 중요

Ⅱ 국방 분야 현황 및 문제점

세계 및 한반도 주변의 국방기술력 현황

- 세계적 군사 대국이 견제·대립하는 지정학적 요지인 한반도는 최근 북한의 핵개발, ICBM 시험발사 등으로 인해 군사적 긴장감이 급격히 고조된 상황
  - 미국, 중국, 러시아, 일본 등 한반도 주변국들은 세계적 군사 강국들로서 정치·외교·경제적 이익을 위해 군사적으로 상호 견제와 대립 중
  - 최근 북한의 핵개발 및 ICBM 시험발사, 한반도 내 THAAD 배치 등의 이슈로 인해 미국, 중국, 러시아, 일본의 군사적·정치적 긴장감이 한층 더 상승



[그림 1-1] 한반도 주변 4국의 군사력[1)]

- 국방 기술력 측면에서 미국이 여전히 세계 최강국이지만 최근 중국의 기술추격세가 두드러지고 전통적 군사강국인 러시아의 기술력 또한 위협적
  - 국방기술력 측면에서 6위로 평가받는 중국은 사이버무기, 수상함, 잠수함, 우주무기, 방공무기 등의 부문에서 국방기술력을 강화하고 있으며 특히 ICBM 탑재 원자력 잠수함 개발을 추진함으로써 세계적 군사 대국으로 발돋움 중

1) 2016 국방백서, 국방부, 2016.12.31.

- 러시아는 냉전 시대부터 축적된 국방 역량을 바탕으로 무기체계 전반에 있어서 세계 최고 수준의 국방기술력을 갖추고 있는 것으로 평가받음
- 일본은 평화헌법 등으로 인해 국방력 강화에 제한이 있는 상황에서도 감시정찰, 항공우주 등 첨단무기체계 확보를 위한 연구개발을 꾸준히 진행 중

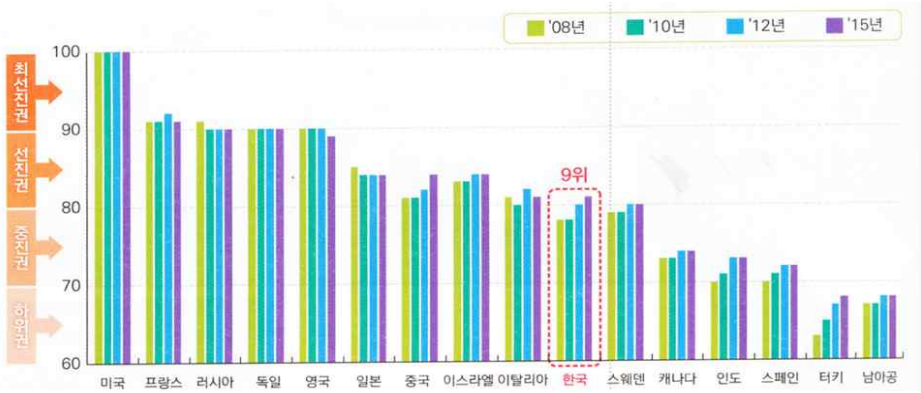
[표 1-1] 세계 주요국의 국방기술력 현황[2)3)]

국가	국방기술수준	주요 현황
미국	1위, 100%	•무기체계 전 분야에서 세계 최고의 기술력 보유 •레이더, 고정익기, 잠수함, 유도무기 등에서 독보적 기술력 보유
프랑스	2위, 91%	•회전익 분야의 신개념 Blue Edge 기술 개발 •유도무기 부문에서 대공미사일 Aster 30 Block Ⅱ 개발
러시아	3위, 90%	•항공기용 AESA 레이더 등 최첨단 기술 보유
독일	3위, 90%	•기동, 화력 분야에 강점 있으며 무기 수출, 레이저무기, 요격어뢰 등 신개념 무기체계 개발 중
영국	5위, 89%	•NATO 회원국 중 국방예산이 최대규모였으나 최근 삭감 추세
중국	6위, 84%	•2010년 81%, 2012년 82%에서 지속적으로 국방기술력 성장 중 •사이버전, 수상함, 잠수함, 우주무기, 방공무기 등 우수 •미국 방어체계 무력화를 위한 사이버 공격무기 독자 개발 •장거리정밀탄도탄, 사이버무기, 항공모함, 스텔스기 등 개발 추진 중 •ICBM 탑재 원자력 잠수함 개발, 초공동 신형잠수함 개발 추진 중 •대함탄도탄 등 장거리 정밀타격 유도무기 독자모델 개발 지속 •우주무기 체계는 90% 수준의 기술력 확보 •전술통신, 전자전, 지상무인, 개인전투, M&S 분야가 약세
일본	6위, 84%	•무기체계 전 분야에서 고른 우수 기술력 보유 •수상함, 잠수함, EO/IR, 항공우주 등에 강점 •항공모함으로 개조가능한 함정 개발에 관심 •3000톤급 이상 잠수함 설계건조에 강점 보유 •원자력 잠수함 건조 기술 보유 •EO/IR 부문에서 민간기술을 방산에 접목함으로써 기술력 강화 •항공우주 부문에서 제트엔진, 로켓발사체 등에서 강점 •개인전투, 화포, 탄약, 화생방, 국방M&S 등에서 상대적 약세
이스라엘	6위, 84%	•무인기, 우주, 미사일 방어 부문 등에 집중적인 투자 •첨단 레이더, 전자기술을 기본으로 핵심 시스템·부품 중심 개발
이탈리아	9위, 81%	•대부분의 무기체계 자체개발 보유 •재정 위기 영향으로 국방비 감소 추세

2) 2016 국방과학기술조사서(요약본), 국방기술품질원, 2016.12
3) 질적 성장 추진과 함께 기력력 세계 9위에 오르다, 국방홍보원, 2016.01.05.

국내 국방기술력 수준 현황

- 국방기술품질원의 국방기술력 수준 조사에 따르면 종합적인 국내 국방기술수준은 주요 16개국 중 9위이며 감시정찰, 항공우주, 화력 등은 상대적 약세[4)]
  - 2008년 이래 전반적인 국방기술력이 점차 향상되고 있고 기술수준 순위는 2008년 세계 11위에서 2016년 세계 9위로 상승



[그림 1-2] 주요 16개국 국방기술수준 종합 순위[5)]

- 국방기술분야별 기술 수준 비교에서 국내 국방기술이 감시정찰, 항공우주, 화력 등 부문에서 상대적 약세를 보이는 것으로 평가

  * 분야별 국내 국방기술력 수준은 지휘통제·통신 9위, 기동 8위, 함정 9위, 방호 9위, 감시정찰 11위, 항공우주 10위, 화력 10위, 기타부문 11위로 평가받음

[그림 1-3] 8대 국방기술부문별 국내 국방기술수준 순위[6)]

4) 2016 국방과학기술조사서(요약본), 국방기술품질원, 2016.12.
5) 2016 국방과학기술조사서(요약본) (국방기술품질원, 2016.12)

● 산업연구원의 조사에 따르면 국내 방위산업체 기술력은 4개 무기체계 분야 12개 주요 방위산업 완제품과 46개 핵심기술에서 세계 최고수준의 70%에 미치지 못하는 기술분야가 과반수[7)]

- (항공 분야) 2016년 현재 국내 방위산업체의 전투기·훈련기 부문의 기술력 수준은 보라매(KFX) 전투기 AESA 레이더의 경우 세계 최고수준(=100) 대비 57.1으로 평가되었으며 5년 후에는 76.1까지 성장할 것으로 전망

  * 5년 후 기술력 전망이 낙관적인 이유는 2016년 현재 관련 기술에 대한 국내 연구개발이 진행 중이며 해외 방산업체와의 기술협력 등을 통해서 경쟁력 제고가 예상되기 때문

- (항공 분야) 전투기·훈련기의 항공전자·엔진·무장·적외선추적장비(IRST)·전자전·재머(Jammer)·체계통합(SI) 분야 핵심기술들의 상대적 기술력은 60~64.9 수준으로 평가되어 전반적으로 저조하며 5년 후에는 70점 대로 향상될 것으로 전망

  * 전투기·훈련기의 핵심기술인 엔진 기술은 5년 후에도 세계 최고기술력 대비 68.9 수준에 머무를 것으로 평가되어 첨단 기술 획득에 애로가 있는 것으로 판단됨

- (항공 분야) 군용헬기 부문의 2016년 현재 국내 방위산업체 기술력은 최고수준 대비 56.1~69.2로 평가되었으며 무장분야 기술력이 가장 저조해 소형 무장헬기(LAH) 개발, 헬기탑재 미사일 다양화에 따른 무장체계종합기술 등 기술력 확보가 시급함을 시사

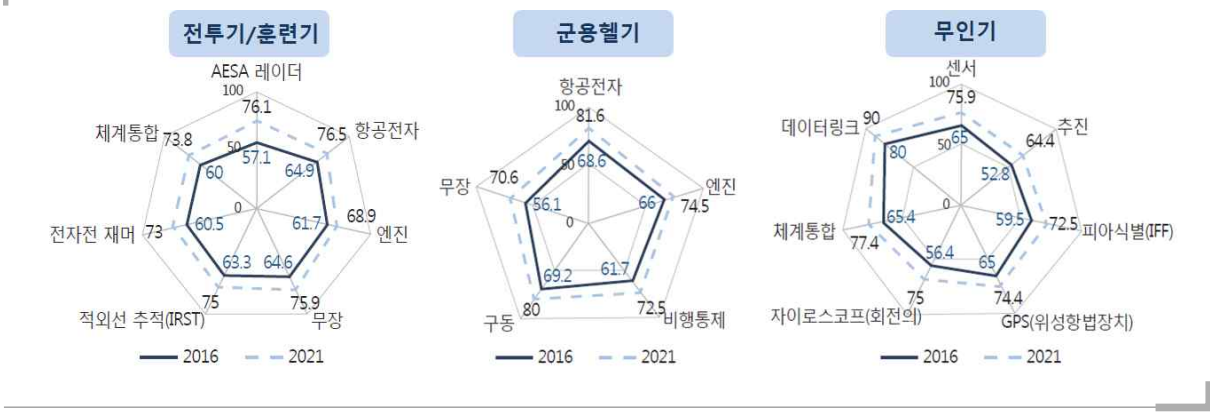
- (항공 분야) 군용헬기 부문의 5년 후의 기술경쟁력은 현재 진행 중인 군겸용헬기(LAH/LCH) 사업과 수리온 개발과 공공·소방 등 파생제품 개조개발에 따라 세계 최고수준 대비 70.6~81.6까지 향상될 것으로 전망

  * 군용 헬기의 무장 기술은 5년 이후에도 세계 최고수준 대비 70.6 수준일 것으로 전망

- (항공 분야) 무인기 부문의 2016년 현재 국내 방위산업체 기술력은 세계 최고수준 대비 52.8~80.0으로 큰 편차를 보였는데 추진 (52.8), 자이로스코프 (56.4), 피아식별장치 (59.5) 등의 기술력이 상대적으로 부족한 것으로 평가

- (항공 분야) 무인기 부문의 5년 후 국내 방위산업체 기술력은 최고수준 대비 64.4~90.0으로 향상될 것이지만, 피아식별장치 등의 기술력은 여전히 부족할 것으로 예측

6) 2016 국방과학기술조사서(요약본), 국방기술품질원, 2016.12.
7) 주요 방산제품의 핵심기술 경쟁력 분석과 향후 과제, KIET 산업경제, 2017.



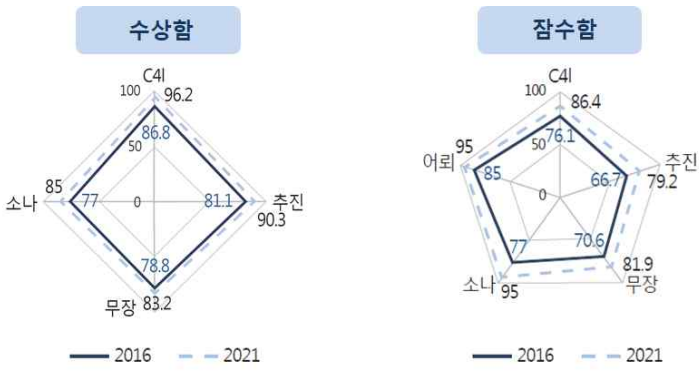
[그림 1-4] 국내 방위산업체의 항공 분야 핵심기술 경쟁력[8)]

- (함정 분야) 수상함 부문의 국내 방위산업체 경쟁력은 일부 부문을 제외하고는 글로벌 경쟁력을 갖춘 것으로 보여지는데 2016년 현재 국내 방위산업체의 기술력이 세계 최고수준 대비 77~86.8로 평가되었고 소나 (77), 무장 (78.8) 등의 부문이 가장 저조
- (함정 분야) 수상함 부문의 5년 후 국내 방위산업체 기술력은 83.2~96.2까지 향상될 것으로 전망되었으며 소나와 무장은 각각 85.0, 83.2으로 전망
- (함정 분야) 잠수함 부문의 국내 방위산업체 경쟁력은 세계 최고수준 대비 66.7~85.0으로 평가되며 추진 분야의 기술력 수준이 66.7으로 가장 저조

  * 잠수함 디젤엔진이 독일 MTU사와의 기술협력을 통해 생산되고 있고 잠수함 배터리에서 나타나고 있는 빈번한 고장으로 인해 잠수함 추진 분야의 기술력 평가 점수가 저조

- (함정 분야) 잠수함 부문의 5년 후 국내 방위산업체 기술력은 잠수함 C4I[9)], 소나, 어뢰 부문의 기술수준이 최고수준 대비 86.4~95.0에 이를 것으로 전망되었으나 추진과 무장 분야는 각각 79.2, 81.9로 여전히 저조

8) 주요 방산제품의 핵심기술 경쟁력 분석과 향후 과제, KIET 산업경제, 2017.
9) C4I는 국방 지휘 통신체계의 핵심요소를 가리키는 용어로서 Command, Control, Communication, Computer and Intelligence의 약자

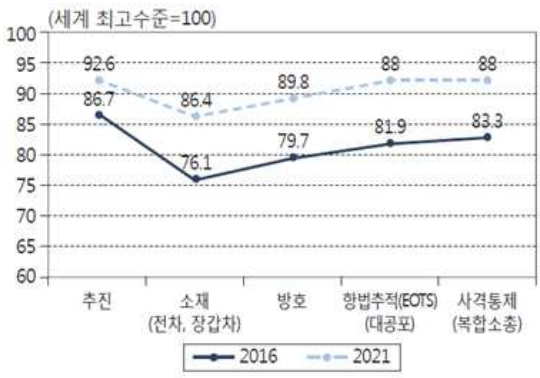


[그림 1-5] 국내 방위산업체의 함정 분야 핵심기술 경쟁력[10)]

- (기동·화력·방호) 전차·장갑차 부문의 국내 방위산업체 핵심기술 경쟁력은 세계 최고수준 대비 추진 86.7, 소재 76.1, 방호 79.7 수준으로 각각 평가되었고 대공포의 항법추적장치(EOTS)는 81.9, 복합소총의 사격통제장비는 83.3 수준인 것으로 나타났음

  * 추진분야 핵심기술력은 파워팩(powerpack) 국산화 및 양산화로 인해 향상되었지만 미국 등 선진국들이 아프가니스탄 전쟁 등을 겪으며 소재, 방호능력 향상 요구가 증가하였음에도 불구하고 우리나라의 관련 기술력은 80.0에도 못미쳐 보완이 필요한 것으로 보임

- (기동·화력·방호) 전차·장갑차, 대공포, 복합소총 등의 5년 후 국내 방위산업체 기술력은 최고수준 대비 85~92.6까지 향상될 것으로 전망되며 전차·장갑차 소재 분야의 상대적 기술수준이 86.4로 전망되어 가장 낮을 것으로 예측



[그림 1-6] 국내 방위산업체의 기동·화력·방호 분야 핵심기술 경쟁력[11)]

10) 주요 방산제품의 핵심기술 경쟁력 분석과 향후 과제, KIET 산업경제, 2017.
11) 주요 방산제품의 핵심기술 경쟁력 분석과 향후 과제, KIET 산업경제, 2017.

- (유도 분야) 장거리 유도무기 부문의 국내 방위산업체 경쟁력은 세계 최고수준 대비 60.0~90.0으로 평가되었는데 피아식별 분야 (60.0), 항법장치 (66.0) 등이 가장 낮은 기술력을 가진 것으로 인식

  * 최근 사드(Thaad) 배치 관련 논란이 일었던 장거리 유도무기 부문은 미국의 사드, 이스라엘의 애로우(Arrow), 러시아의 S-400 등 주요 선진국들이 정밀타격능력 확보와 적 미사일 위협 대응 차원에서 전략·비닉 무기에 대한 연구개발 투자를 집중하고 있는 핵심 전략무기 분야

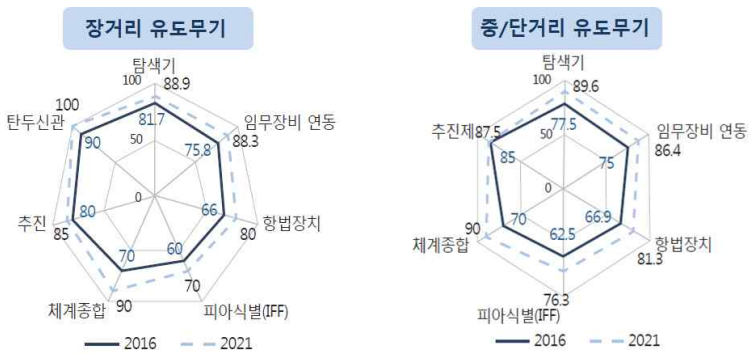
  * 미국 트럼프 대통령 또한 2017년 1월 취임식에서 6대 국정기조를 발표하면서 국방 분야에서는 최첨단 미사일방어시스템 개발을 적극 추진하겠다는 공약을 제시한 바 있음

- (유도 분야) 장거리 유도무기 부문의 5년 후 국내 방위산업체 경쟁력은 체계종합과 탄두신관 분야 핵심기술력이 최고수준 대비 각각 90, 100으로 제고될 것으로 예측되는 반면 피아식별(IFF) 분야의 기술력 향상은 선진국 대비 70 수준에 머물 것으로 전망

  * 체계종합 기술력의 향상에 대한 낙관적 전망은 최근 장거리 공대공 미사일 도입 및 전투기 탑재에 따른 선진국과의 기술협력이 진행 중이라는 점과 2020년 대 중반으로 예정된 L-SAM 개발사업이 추진되고 있다는 점 등에 기인한 것으로 판단됨

- (유도 분야) 중·단거리 유도무기 부문의 국내 방위산업체 기술력은 세계 최고수준 대비 62.5~85.0 수준으로 평가되었으며 장거리 유도무기 분야와 유사하게 피아식별 (62.5), 항법장치 (66.9), 체계종합 (70.0) 등 분야가 저조한 것으로 파악

- (유도 분야) 중·단거리 유도무기 부문의 5년 후 국내 방위산업체 기술력은 일부를 제외하고는 최고수준 대비 86.4~90.0 수준을 확보할 것으로 전망되었으나 피아식별 (76.3), 항법장치 (81.3) 부문의 기술력은 여전히 낮을 것으로 예측

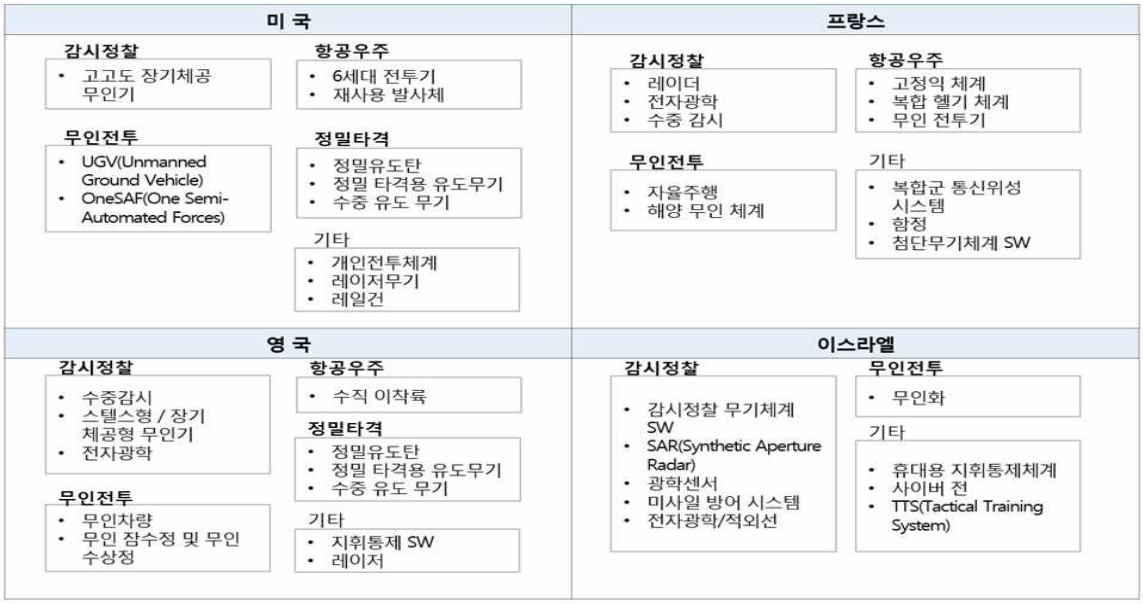


[그림 1-7] 국내 방위산업체의 유도 무기 분야 핵심기술 경쟁력[12)]

12) 주요 방산제품의 핵심기술 경쟁력 분석과 향후 과제, KIET 산업경제, 2017.

세계 주요국의 국방과학기술 주요투자 부문

- 미국 등 주요 군사 강국들은 감시정찰, 정밀타격, 항공우주, 무인전투 등을 중심으로 국방과학기술 투자를 추진, 국방 역량 첨단화에 매진 중
  - 국방역량 전반에서 세계 최고 수준을 유지하고 있는 것으로 평가받는 미국은 무인전투, 항공우주, 정밀타격, 감시정찰 등에 집중적인 기술 투자 진행 중
  - 독자적인 전투기와 유도무기 관련 기술력을 보유하고 있는 프랑스 또한 무인전투, 항공우주, 감시정찰 등의 부문에서 국방기술력 강화를 위해 노력 중
  - 무기체계 내 핵심 시스템·부품 부문에서 강점을 가진 이스라엘은 감시정찰, 미사일 방어시스템, 무인전투 부문에 기술 투자가 활발



[그림 1-8] 주요국의 국방과학기술 중점 투자 부문

- 세계 1위의 국방역량을 보유한 미국은 3차에 걸친 상쇄전략(1st-2nd-3rd Offset Strategy) 전개를 통해 인간·기계 협력 중심의 새로운 국방 전략을 제시
  - 미국의 상쇄전략은 과학기술력을 바탕으로 군사적 경쟁국과의 격차를 유지하려는 국방부의 국방기술력 확보 전략으로서 핵무기, 스텔스 비행기, 인터넷, GPS 등의 전략적 무기 체계 마련의 근간으로 작용
  - 2014년 이후 추진되고 있는 3차 상쇄전략은 빅데이터, AI, 로봇 등의 ICT 기술혁신의 국방 도입을 통해 인간·기계 합동 작전 수행역량 확보를 추구

[표 1-2] 미국의 1, 2, 3차 상쇄전략(Offset Strategy) 개요

	제1차 상쇄전략	제2차 상쇄전략	제3차 상쇄전략
시기	1950년대 말	1970년대 중반	2014년~
발안자	아이젠하워 대통령	해롤드 국방장관	헤이글 국방장관
목적	•공산주의 침략 저지 •경제 성장 지속	•국방과학기술력 측면에서 소련과의 격차 확보	•국방과학기술력 측면에서 압도적 우위 확보
이슈	•소련 군사력이 수 적으로 우위	•바르샤바 조약 국가들의 무기가 수 적으로 우세	•러시아, 중국의 국방과학기술력 및군사력 성장
전략 내용	•핵무기의 전략·전술적 활용 •미국이 원하는 장소, 시간에 전략적 비대칭성 확보	•정보감시정찰(ISR) 및 전장 관리체계 강화 •정밀타격 체계 확보 •스텔스 비행기 전력화 •우주자산의 전술적 활용	•인간+기계 전투력 확보 (1) 학습 기계 (2) 인간-기계 협동 (3) 기계보조 인간 활동 (4) 인간-기계 전투 조합 (5) 자율무기 등 •전세계 감시타격체계 확보 (1) 무인장비 운용력 (2) 장거리 정찰 비행과 타격 체제 (3) 스텔스 무기 (4) 해저작전수행력 (5) 체계공학 및 체계 통합능력
성과물	•수소폭탄 •전폭기,ICBM •인터넷	•위상배열레이더 •조기경보통제기 •순항미사일 •무인기, 무인고공정찰기 •정찰인공위성, GPS	N/A

국내 국방과학기술 주요 투자 부문

- 국방기술품질원의 국방 핵심기술기획[13]에 따르면 최근 무인전투, 정밀타격, 감시정찰 등의 부문에 대한 투자가 증가 혹은 꾸준히 이루어지고 있는 것으로 판단

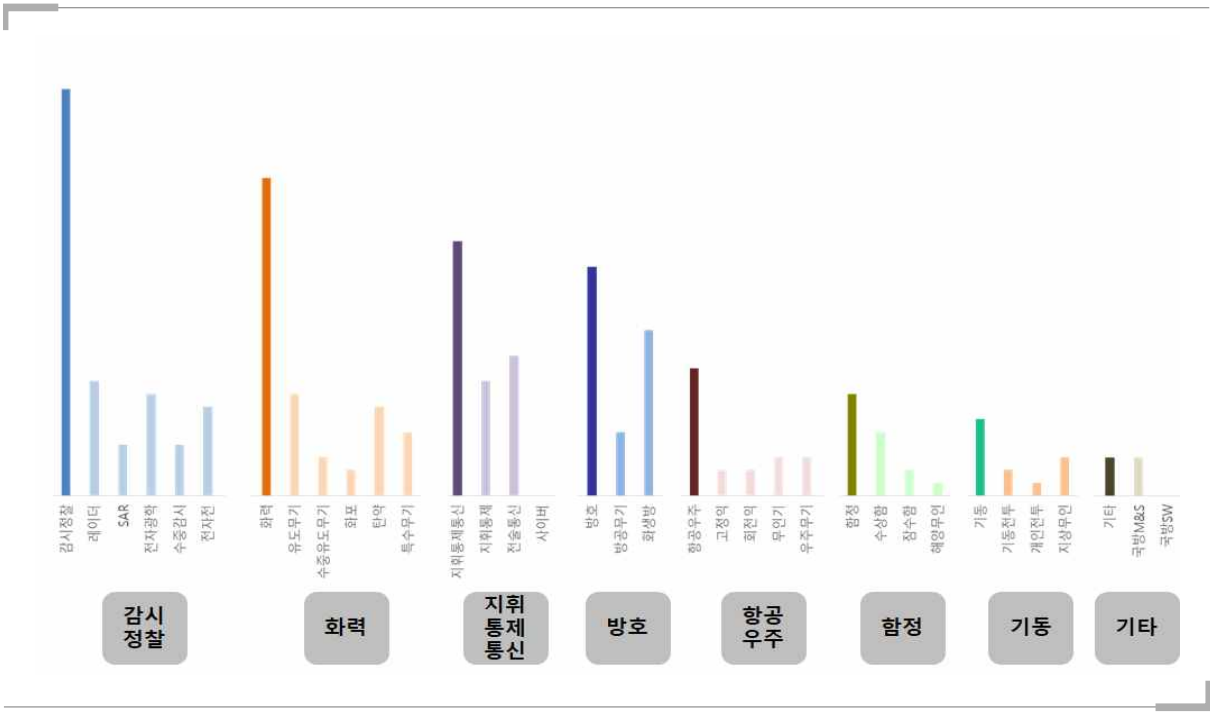
  - 국방기술품질원의 국방 관련 핵심기술기획은 국내 국방기술확보의 중심적 기획이라 할 수 있으며 핵심기술 선정·기획에 있어서 무기체계 선택·집중 측면과 특정 무기체계 누락곤란 측면을 동시에 고려한 Two-Track의 핵심기술 기획을 추진

    * 국방 관련 핵심기술기획의 Two-Track은 '중점기획 대상 무기체계 핵심기술'과 '일반기획 대상 무기체계 핵심기술'로 구분

13) '17~'31 핵심기술기획서 일반본, 국방기술품질원, 2016.

- 국방 관련 핵심기술기획에 포함된 '일반기획 대상 무기체계 핵심기술'은 군 소요 무기체계의 기술기획 누락 최소화 관점에서 선택된 기술들로서 2016년 말 현재 122개 기술이 선정

  * 122개 일반기획 대상 무기체계를 27개 대표 무기체계별로 분류하고 공통핵심기술 기반으로 대표 무기체계별 핵심기술로드맵을 수립



[그림 1-9] 국내 일반기획 대상 무기체계 핵심기술[14)]

- '일반기획 대상 무기체계 핵심기술'에 포함된 122개 기술을 8대 무기체계별로 나누어보면 감시정찰, 화력, 지휘통제통신 등에 다수의 기술기획이 포진되어 있고 항공우주, 함정, 기동, 국방M&S 등은 상대적으로 적은 수의 기술기획 진행

- 국방 관련 핵심기술기획에 포함된 '중점기획 대상 무기체계 핵심기술'은 선택과 집중의 기술기획 관점에서 선택된 기술들로서 로봇·무인전투체계, 에너지 등 특수무기, 공통적용기술, 사이버전, 적중심파괴 분야에서 17개의 무기체계와 유사전력 8개 등 총 25개가 선정됨

  * 로봇/무인전투체계 5개, 에너지 등 특수무기 5개, 공통적용기술 4개, 사이버전 1개, 적중심파괴 2개 등 17개

  * 최초 17개의 핵심기술 개발 중에 추가 확보가능한 유사전력 8개를 추가로 선정하여 최종적으로 25개의 중점기획 대상 무기체계 핵심기술이 선정되었음

14) '17~'31 핵심기술기획서 일반본 (국방기술품질원, 2016.) 참고하여 자체 작성

* '중점기획 대상 무기체계 핵심기술'에 포함된 적중심파괴 분야 기술의 내용은 비공개 상태지만 원거리 정밀타격 능력 등에 관련된 기술 기획으로 추정됨

- '일반기획' 내 무인기 · 해상무인 · 지상무인 등의 무인전력 체계 관련 기술기획이 상대적으로 적지만 '중점기획'에 로봇 · 무인전투체계 기술이 포함되어 있어 현재 무인전력 체계 마련을 위한 투자가 진행 중인 것으로 판단
- 세계 주요국의 국방기술투자가 활발하게 이루어지는 정찰감시 부문은 '일반기획' 내 가장 주요한 기술기획이 이루어지고 있는 부문으로 지속적인 기술투자와 개발이 진행 중인 것으로 사료됨
- 정밀타격과 관련된 것으로 추정되는 적중심파괴 분야 기술이 '중점기획'에 포함되어 있고 '일반기획'에서도 유도무기, 수중유도무기 등에 기술기획이 적지 않아 정밀타격 부문에 대한 국내 기술개발 노력이 상당하다고 볼 수 있음
- 항공우주 관련 기술기획은 '일반기획'에서 상대적으로 적게 나타나고 있고 '중점기획'에서는 표면적으로 드러난 것이 없어 국내 기술개발 노력이 활발하다고 보기는 어려움

● 국내 국방기술 기획이 정밀타격, 무인전투, 감시정찰, 항공우주 등의 세계적인 국방기술투자 추세를 따르고 있다고 볼 수 있으나 실제 확보가능한 기술수준이 전력 우위를 담보한다고 판단하기는 어려움

- 앞서 살펴본 국내 방위산업체의 상대적 기술력은 유도무기, 무인기, 전투기 엔진, 전투기 레이더 등의 부문에서 세계 최고수준에 대비할 때 적지 않은 격차로 뒤떨어져 있는 것이 현실
- 따라서 2016년 현재 '중점기획', '일반기획'에 포함된 무인전력, 정찰감시, 정밀타격, 항공우주 등 부문의 국방기술기획이 실제 군전력의 상대적 수준을 어느 정도 향상시킬 지에 대해서는 신중한 접근이 필요

주요국 국방 부문의 민간 기술력 도입 현황

- 주요국들은 국방력 강화를 위해 AI, 3D 프린팅, IoT 등 민간에서 촉발된 기술 혁신 결과물을 국방과학기술에 적극적으로 접목하는 중
  - 민간 기술력을 국방 부문에 빠르게 도입하기 위한 제도적 장치 마련과 더불어 군수산업체를 중심으로 3D프린팅, IoT 등의 제조 기술을 도입하려는 시도가 활발
  - AI, 무인이동체 등의 ICT 부문에서 확보된 민간 기술력을 지휘통제 및 무기체계에 직접 도입하여 국방 역량을 일신하려는 노력 또한 주요한 움직임

미 국	영 국
• 비전통적 신기술 도입을 위해 국방혁신실(DIUX: Defense Innovation Unit-Experimental) 실리콘 밸리에 설치 (2015.08) • Alphabet 회장인 Eric Schmidt를 국방부 혁신자문위원회 위원장에 영입 (2016.03) • Boost Aerospace, Lockheed Matin Digital Tapestry, Airbus Amx 등 다양한 시도를 통해 IoT, 3D 프린팅 등 민간기술혁신을 무기체계와 방위산업에 적극적으로 도입 중	• (Rolls Royce) 디지털 트윈에 기반해 항공기·군함 가스터빈 부품의 설계, 개발을 연계하는 DA-VINCI 추진 • (Meggitt) 시뮬레이션과 데이터 분석에 기반해 무인기, 항공전자장비 생산, 유지보수의 효율성을 제고하는 M4 추진(Meggitt Modular Modifiable Manufacturing) • (BAE systems) 로봇 적용을 통해 항공기 생산성을 제고하는 Robot Counter Sinking Cell 체계 적용
중 국	**일본**
• 제조업 강화 국가 전략인 Made in China 2025이 국방에 직접적인 연관을 가진 로봇, 정보통신, 우주항공, 조선을 강조 • Made in China 2025와 함께 방위산업 부문에서도 공급망 혁신, 자동화 강화, 3D 프린팅 및 AI 역량 강화 등을 추진 중 • Siemens와 협력으로 추진 중인 Cloud manufacturing을 통해 방위산업의 제조 역량 강화 추진	• 평화헌법 하에 있는 일본은 경단련 등 민간 기업을 중심으로 방위 산업 활성화, 우주개발 활성화 등이 추진 • 세계 100대 방산기업 중 일본 기업이 총 6개 포함되어 있어 민간 부문에서 세계적 국방 기술력 확보 • 2015년 신설된 방위장비청(ATLA)는 대학, 공공연구소, 기업 등의 군사응용가능 기술 개발을 지원

[그림 1-10] 주요국의 국방 부문 민간 기술력 도입 현황

- 미국 국방부는 민간기술 도입에 적극적으로 나서 국방혁신실(DIUX: Defense Innovation Unit-Experimental) 등 제도적 장치를 선도적으로 마련
  - 미 국방부는 실리콘 밸리의 ICT 혁신역량을 국방에 도입하기 위해 2015년 8월 국방혁신실(DIUX: Defense Innovation Unit-Experimental)을 실리콘 밸리에 설치
    * 민간 기술의 국방 도입을 맡고 있는 국방혁신실은 2017년 2월 기계학습 기반 위성사진 분석업체인 Orbital Insight에 투자했으며 2017년 3월에는 소형 레이더위성 군집운영기술 업체인 Capella Space와 계약을 체결하는 등 활발히 활동 중
  - 국방 부문의 폐쇄성을 타파하기 위해 2016년 3월 Alphabet社 회장인 Eric Schmidt를 국방부 혁신자문위원회 위원장으로 영입

- 군수업체인 Lockheed Matin社는 Digital Tapestry, Airbus社는 AMX 등의 전략을 각각 추진함으로써 IoT, 3D 프린팅 등 민간기술혁신 성과를 빠르게 도입

  * Digital Tapestry는 빅데이터, 3D 프린팅, VR 등의 ICT 기술혁신을 통해 설계, 생산, 유지보수에 이르는 제품 전주기를 연결하고자하는 전략

  * Airbus社의 AMX는 적층형 생산방식과 생물체 모방 설계를 통해 항공기 경량화를 추구

◐ 일본은 민간 주도의 국방기술력 확보가 이루어져 왔으나 2015년 방위장비청(ATLA)을 신설하며 공공 부문의 국방기술 개발을 본격적으로 추진 시작

- 일본 방위산업계는 경단련을 중심으로 자국 방위 산업의 수출 활성화, 국제공동개발 및 생산체계 참여, 우주개발 분야의 산업경쟁력 강화 등을 주장해왔음
- 2015년 일본 방위장비청(ATLA)을 신설하여 무기에 대한 연구·개발·도입을 통한 독자적 방위력 강화, 무기 수출 및 외국과의 공동개발 등을 추진

  * 일본 방위장비청은 2015년 10월 아베정권이 통과시킨 방위성설치법 개정안에 따라 설립 근거가 마련됐으며 2015년 현재 5조엔 규모인 일본 방위예산의 3분의 1 정도를 관할

- 일본은 평화헌법 등 독특한 정치적 환경으로 인해 민간-국방의 협업이 강화된 상태

◐ 영국은 주요 군수업체들이 IoT, 로봇, 빅데이터 등의 ICT 기술혁신 성과물을 적극적으로 도입함으로써 무기체계 설계, 개발의 효율성 제고를 추진

- Rolls Royce社는 디지털 트윈에 기반해 항공기·군함 가스터빈 부품의 설계, 개발을 연계하는 DA-VINCI 프로젝트를 추진
- Meggitt社는 시뮬레이션과 데이터 분석에 기반한 M4(Meggitt Modular Modifiable Manufacturing) 프로젝트를 통해 무인기·항공전자장비의 생산·유지보수 효율성을 제고
- BAE systems社는 로봇 적용을 통해 항공기 생산성을 제고하는 Robot Counter Sinking Cell 체계를 적용

◐ 중국은 제조업 강화 국가 전략인 Made in China 2025를 통해 국방 관련 산업과 기술 진흥을 강조

- Made in China 2025은 국방에 직접적 연관을 가진 로봇, 정보통신, 우주항공, 조선 등의 부문을 강조하고 있으며 이와 더불어 방위산업 부문에서도 공급망 혁신, 자동화 강화, 3D 프린팅 및 AI 역량 강화 등을 추진 중
- Siemens와 협력으로 추진 중인 Cloud Manufacturing을 통해 방위산업의 제조 역량 강화를 추진

국내 국방 부문의 민간 기술력 도입 현황

- 국내에서도 국방·민간기술 융합을 통한 국방력과 산업경쟁력 강화를 위하여 민·군기술협력 활성화 노력을 기울여 왔고 소기의 성공 사례도 존재
  - 국방부, 산업통상자원부, 과학기술정보통신부 등의 협업으로 추진되는 민·군기술협력사업은 '민·군기술협력사업 촉진법[15]'에 의거하여 추진되어 왔으며 관련 예산은 2013년 416억 원에서 2016년 677억 원으로 증액된 바 있음
    * 민·군기술협력사업은 민과 군이 공통적으로 활용할 수 있는 기술·소재 등을 개발하는 민·군기술개발사업, 민과 군이 보유하고 있는 기술을 상호 이전하여 실용화 가능성을 연구하는 민·군기술이전사업, 민수규격과 국방규격을 통일하고 표준화하는 민·군규격 표준화 사업, 민과 군의 기술정보를 교류하는 민·군기술정보교류 사업 등으로 구성
    * 민·군기술협력 산업 활성화를 위해 국방부는 2014년 국방과학연구소 내 민·군기술협력사업 전담기구인 민·군협력진흥원과 방산업체의 무기체계 연구개발 사업에 대한 기술지원을 담당하는 방위산업기술 지원센터 등을 설립
  - 민·군기술협력사업의 대표적 사례로 수리온 헬기에 적용된 보조동력장치, 해군 고속함의 중소형 워터젯 시스템, KF-16 전투기 착륙장치의 브레이크 디스크에 적용된 탄소·탄소복합재, T-50 고등훈련기의 공기흡입구 구성품 성형기술 등
- 소기의 성공사례에도 불구하고 국내 민·군기술협력은 무기체계 적용을 위한 추격형 개발사업에 치중하고 있어 민간 부문의 최신 기술혁신 성과의 국방 도입을 위한 장기적·체계적 접근으로서는 한계가 있는 것으로 판단됨
  - 지난 40여 년간 국방 R&D는 국방과학기술 전담 연구기관이 주도하고 민간은 시제품 생산만을 담당해왔던 관행과 개발 후 성과물의 상업적 활용을 불가능하게 하는 관련 정책은 민간의 국방 R&D 투자·활동을 유도하지 못하는 것이 현실[16]
  - 국방기초연구 분야의 혁신성 강화를 위해 국방과학연구원 내 국방고등기술원을 설립하여 혁신적 무기체계개발을 위한 국방관련 기초·원천 R&D를 포함한 산학연 협업을 추진한다는 시도 또한 국방 R&D 연구환경의 경직성으로 인해 한계 봉착
    * 2017년 국방과학연구원의 무인기 시험 비행 중 발생한 사고에 대해 연구자 개인의 배상책임이 논의되는 현실은 무기체계의 빠른 개발에 집중해온 국방 R&D 환경의 경직성을 보여주는 하나의 사례

15) 1998년 4월에 제정한 산업통상자원부와 국방부의 공동소관 법률
16) 국방 연구개발 실태 및 개선방안, 과학기술정책연구원, 2015.12.

- 기초연구부터 무기개발에 이르는 국방 R&D 대부분을 국방과학기술 전담 연구기관에 의존하는 연구 체계와 조기전력화를 강조해온 국방 정책은 민간 또는 타 정부출연연의 기술 혁신 역량의 국방 적용을 위한 실험적 접근을 차단

시사점

- 미국, 중국 등 한반도를 둘러싼 군사대국들의 국방력 강화 경쟁과 더불어 북한의 핵 개발 사태 및 이에 맞물린 일본의 평화헌법 개정 시도 등은 한반도 평화에 심각한 위협
  - 중국은 자국의 지정학적 영향권에 대한 접근거부력 강화를 위해 우주항공, 수상함 및 잠수함 등 부문에 대한 기술력을 강화
  - 일본 아베정권은 방위장비청을 신설하는 등 자국의 국방기술력 강화를 위한 본격적인 움직임을 보이고 있는 한편 평화헌법 개정을 통한 본격적 군사강국으로의 발돋움을 끊임없이 시도 중
  - 최근 정치적·군사적 경쟁국들의 국방기술력 성장에 자극받은 미국은 제3차 상쇄전략(3rd Offset Strategy) 하에 국방과학기술 R&D를 강화
  - 트럼프 정부의 자국 우선주의 정책으로 인해 한미 군사동맹력 약화에 대한 우려가 존재하며 첨단무기부문에서 대미 의존도가 높은 국내 국방력은 미국 정책 변화에 민감
- 무기체계 전반에 걸친 다양한 국방 기술 투자가 이루어지고 있는 것으로 보이지만 세계 최고수준 대비 낮은 국내 국방기술력은 미래전 대비를 위한 국방기술 확보를 위한 새로운 접근법을 요구
  - 전반적인 국방기술력이 세계 9위 수준으로 평가되고 미국 등 주요 군사강국들이 주목하고 있는 정찰감시, 정밀타격, 무인전투, 항공우주 등의 부문에 대해 국내에서도 국방 R&D 투자 노력이 이루어지고 있다는 점은 긍정적인 현상
  - 그러나 정찰감시, 정밀타격, 무인전투, 항공우주 등의 부문에서 기 확보된 국내 국방기술력은 세계 최고수준 대비 낮게 나타나고 있어 향후 안정적 국방력 확보 전망을 긍정적으로 평가하기 어렵게 함
  - 세계 주요국들이 ICT를 중심으로 한 민간 부문의 기술혁신 성과를 국방에 도입하기 위해 적극적인 움직임을 보이는데 비해 국내 국방 R&D 체계는 민·군의 협력과 교류에 장애요인으로 작용하는 것으로 판단됨
  - 보다 유연하고 개방적인 국방 기술 연구개발 환경 조성 등의 새로운 접근법을 통해 미래전력 체계를 준비하는 시도가 필요

Ⅲ 미래 국방 전망

현대전의 주요 변화 트렌드

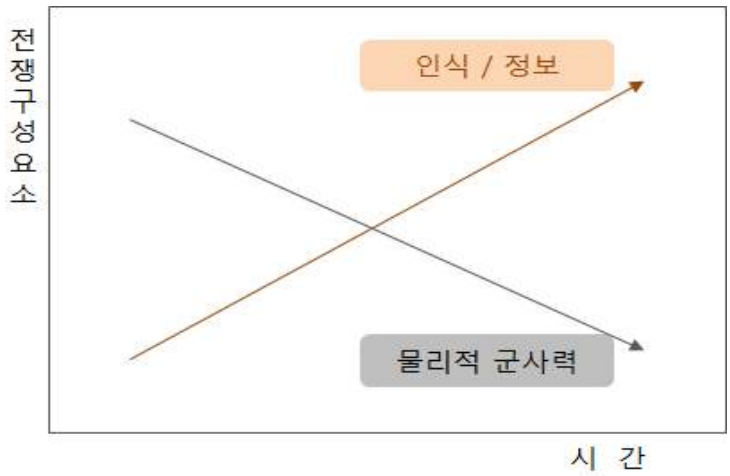
- 정보화 시대를 거치면서 원거리 감시정찰, 원거리 정밀타격 무기체계를 활용해 공격 목표만을 빠르고 효율적으로 타격하는 전쟁이 벌어지고 있음
  - 전투 수행 방식이 전장 내 피아격돌에서 벌어지는 대량살상·파괴에서 벗어나 원거리 정밀유도무기에 의해 정해진 목표물만을 파괴하는 방식으로 변화
    * 최근 전쟁에서의 정밀유도무기 사용 비율은 걸프전(1991년) 8% 수준, 코소보전(1999년) 35% 수준, 이라크전(2003년) 80% 수준으로 점차 상향되는 추세[17)]
  - 전문화된 소수의 엘리트 병력 및 첨단 무기체계에 의해 전쟁의 시작과 종결이 빠르게 이루어지는 추세
    * 걸프전의 경우 1991년 1월 17일 '사막의 폭풍작전'이 시작된 지 43일 만인 1991년 2월 28일 전쟁 종식이 선언되었고 코소보전은 1999년 3월 23일 NATO군에 의한 세르비아·코소보 공습 시작 이래 79일 후인 1999년 6월 10일 코소보 평화안이 합의되면서 전쟁이 끝났으며 이라크전은 2000년 3월 20일 '이라크의 자유 작전'이 시작되어 26일 후인 2003년 4월 14일 미군이 티크리트에 진입하면서 전쟁이 종식
  - 정밀감시 체계와 원거리 유도 무기, 공중·지상 합동작전을 통해 전후방의 구분이 불분명한 상태로 분산 전개되는 전투
    * 1, 2차 세계대전은 전선과 후방이 구분된 상태에서 전선에서 피아 간 전진과 후퇴가 반복되는 전쟁이었으나 걸프전, 코소보전, 이라크전 등 최근 전쟁은 우주·공중 감시정찰 시스템이 제공하는 정보에 따라 전·후방 구분없이 적국의 주요 군사시설을 동시에 타격하는 방식으로 전개

전쟁 패러다임의 전환

- 정보화 시대를 지나 AI, 로봇, 4차 산업혁명의 시대로 접어들고 있는 현재 새로운 기술들이 전쟁과 평화의 방법론을 데이터, 네트워크, 지능, 인간·기계복합체계에 기반한 것으로 변화시키는 중
  - 미래학자 Alvin Toffler는 부를 창출하는 산업·경제 패러다임의 변화가 전쟁

17) 2013 군사과학기술 동향, 국방기술품질원, 2013.6.30.

의 방식을 바꾸어왔고 바뀐 전쟁 방식은 평화 유지 방법 또한 변화시키고 있음을 지적[18)]



[그림 1-11] 전쟁에서의 인식·정보 및 무력의 비중 변화[19)]

- 제3의 물결을 낳은 정보화 기술은 전쟁에 있어서 정보와 인식의 중요성을 제고했고 이에 따라 평화 유지를 위한 방식 또한 정보화 기술에 기반해야 한다는 것이 Toffler의 주장

  * 18세기 후반 시작된 산업혁명에 의한 대량생산 능력은 전시에 동원되는 병력과 무기를 대규모화 했고 20세기 전반에 이루어진 철도, 자동차, 항공기 등의 대중화는 탱크, 군함, 전투기 등 기계화 무기를 전쟁의 주역으로 변화

- 컴퓨터와 디지털 네트워크가 산업과 일상생활에 깊숙이 뿌리내린 현재와 미래의 전쟁에서는 무력에 앞서 정보와 인식의 중요성이 부각될 것으로 예상

● 정보화 시대의 전쟁이 인식·정보의 중요성을 강조한다면 빅데이터, AI, IoT 등 지능화 기술이 본격적으로 활용될 미래전은 전황 분석 및 무기체계 운용에 적용될 기계화된 지능의 중요성이 부각될 것으로 전망

- 전장과 무기체계 전반에 걸친 작동하는 인식·정보망이 생산하는 데이터를 적시에 효과적으로 활용하는 기계화된 지능은 유사한 수준의 인식·정보능력과 타격능력을 갖춘 세력 간 전투에서 승패를 결정하는 새로운 요소가 될 것으로 예상

- 하지만 원거리 정밀무기 등 타격능력의 향상과 우주와 사이버공간을 포함한 전장공간에 대한 인식·정보능력의 확장에 대한 경쟁은 지속될 것으로 전망

18) 전쟁 반전쟁, 앨빈 토플러, 2011.4.7.
19) 2013 군사과학기술 동향, 국방기술품질원, 2013.6.30.

[표 1-3] 문명 패러다임의 전환과 전쟁의 변화

사회변화	농업사회	산업사회	정보사회	초지능사회
전쟁 양상	육체·백병전	기계·화학전	정보·지식전	**데이터·지능화전**
전쟁 공간	1차원: 지상	3차원: 지상, 해상, 공중	5차원: 지상, 해상, 공중, 우주, 사이버	**5차원: 지상, 해상, 공중, 우주, CPS공간**
지휘 구조	장수 중심 구조	수직적 계층 구조	수평적 네트워크 구조	**초공간 네트워크 구조**
전력 구조	병력 집약형	자산 집약형	정보 집약형	**지능 집약형**
전투 형태	선형	선형·비선형 (대부대, 집중)	비선형 (소부대, 분산)	**비선형·불규칙형 (소부대, 개인, 무인화 무기, 분산)**
파괴·피해	노획, 포로	대량 파괴, 대량살상	정밀 파괴, 소량 피해	**정밀 파괴, 마비, 소량·무 피해**

- 지능화 기술 외에 로봇, 3D 프린팅 등 제4차 산업혁명의 동력이 될 신기술들이 빠르게 발전, 확산됨에 따라 군사 전력 측면에서 새로운 기술 경쟁이 벌어질 것으로 예상
  - 지능화 기술이 데이터 분석·해석하는 인간의 지적 역량을 보완한다면 로봇, 3D 프린팅 등은 인간 노동력, 전통적 제조기술을 대체·보완하는 기술들
  - 로봇, 3D 프린팅 등 신기술은 인간 병력의 기능을 부분적으로 대체하고 무기체계 제조 측면에서 새로운 대안을 제시하면서 미래전에 영향을 미칠 것으로 전망

미래전에 나타날 주요 무기체계 변화 양상

- 미래전에 나타날 기술적 선택지들은 무한히 다양할 수 있으나 군사 전문가들은 로봇, 사이버전, 에너지 무기와 AI, 무인경계, BCI(Brain-Computer Interface), 우주 기반 전투기술 등을 주요 기술로 제시[20)]
  - 2015년 미 육군에 의해 열린 '전술적 지상전의 미래' 워크샵에서 군사 및 미

20) Visualizing the tactical ground battlefield in the year 2050: Workshop report, US Army Research Laboratory, 2015.06.

래기술 전문가 집단은 로봇, 사이버전, 에너지 무기와 AI, 무인경계, BCI(Brain-Computer Interface), 우주 기반 전투기술 등을 미래 주요 군사기술 이슈로 제기

- 스마트 센서와 인공지능으로 무장한 전투로봇이 미래 전투 수행 주체로 제기되었고 인간 병력은 로봇 외골격, 첨단무기, 근력·감각강화 유전공학기술에 의해 수퍼휴먼화 될 것으로 전망
- 정보 탈취와 오염을 위한 해킹 기술이 고도화되고 AI 해킹이 일반화되면서 물리적 공격에 앞서 적국의 기간시설, 무기시스템을 교란하는 사이버전이 전쟁의 주요한 부분이 될 것이라는 시각이 제기
- 레이저, 고출력 마이크로파, 입자빔, X선 등을 이용한 에너지 무기와 피아식별, 피해범위 계산, 공격 정밀도 향상이 가능한 AI가 결합되어 목표물만을 정밀파괴하는 경제적 전투가 벌어질 것으로 예측
- 국경, 전투지역을 경계·감시하던 인간의 오감을 대신하여 드론, 경계로봇, AI 감시센서, 무인 감시정 등 무인 경계 시스템이 보편화되면서 경계의 효율성과 정밀성이 향상될 것으로 전망
- 인간의 두뇌와 컴퓨터 시스템을 연계하는 BCI(Brain-Computer Interface) 기술로 인해 인간의 무기제어능력이 강화시킴으로써 AI 기반 무기체계를 보완할 것으로 전망
- 우주를 포함한 공중을 지배하는 국가·집단이 전쟁의 승기를 쥘 것이므로 레이저, 투하형 무기 등이 위성에 탑재되고 우주에서 운용 가능한 전투기가 등장할 것으로 예상

◐ 무기체계 첨단화와 고성능화에 따른 비용 증가, ICT를 중심으로 이루어지고 있는 첨단 기술의 세계적 균등화로 인해 저비용·비주류 국방 기술에 기반한 미래전 대비 또한 필요하다는 전문가 의견이 존재[21)]

- 우주에 대한 접근능력이 고도화되고 보편화됨에 따라 정찰감시, 항법의 기반이 되는 위성체계 파괴 가능성이 높으므로 이에 대비하기 위하여 분산형, 저비용 위성群 기술이 등장할 수 있음
- GPS 등 항법안내시스템의 도움없이 위치·속도·시간을 정밀하게 계측할 수 있는 양자센서, 저온원자간섭계 등이 적용된 무인전투 기계 및 유도무기 기술이 등장할 것으로 전망
- 해킹 대비 자기방어능력 향상을 위해 원격제어 등에 제한을 두거나 정보시스

21) 2030년 군사우위를 위한 기술 혁신 전략, 국방기술품질원, 2014.5.30.

템 전체를 무결한 표준시스템으로 초기화할 수 있는 동력망, 군사 네트워크 등이 등장 가능

- 3D 프린팅 등을 통해 제작된 저비용 미사일 등의 무기는 정밀타격 능력은 다소 낮더라도 목표물 파괴 및 감시정찰·방어 체계 혼란에 있어서 비용효율적인 대안으로 부각될 수 있음

미래전 수행의 주요 변화 양상

- 발전된 기술의 국방 적용은 미래 전투가 보다 넓은 전장에서, 혁신기술이 적용된 무기를 동원하여, 실시간 정보공유·의사결정을 통해 진행되도록 변화시킬 것으로 예측됨

  - 미래전의 승리는 국방기술의 기능적 우수성 뿐만 아니라 적의 기술 수준 및 기술 운용 방식에 대한 대응 전략에 크게 의존하므로 국방에 적용가능한 미래 기술에 대한 예측과 주요 신기술 확보에 의해 보장된다고 할 수 없음

  - 하지만 기술 변화 및 국방 적용의 추세로 볼 때 전장공간의 확장, 전투수단에 대한 신기술 적용, 전투수행 방식에서의 실시간 정보공유·의사결정의 중요성 증가는 비교적 확실한 미래전의 변화 방향으로 판단됨

- (전장공간) 인지·정보 능력과 지능화된 무기체계가 전쟁 승리에 미치는 영향이 증가하면서 지상, 해양, 공중 등 전통적 전장공간 외에 사이버 및 우주라는 새로운 전장 영역이 추가

  - (사이버 전장) 감시정찰, 정밀타격, 무인전투 등의 유기적 결합·운용에 근간이 되는 정보체계의 우수성이 결정적 승리 요인이 됨에 따라 아군의 정보체계를 보호하고 적 정보체계를 파괴·마비시키기 위한 사이버전이 주요한 군사작전에 포함

    * 사이버전은 군사용 정보시스템 뿐만 아니라 민간통신망, 동력망, 상하수도 관리망 등의 비군사적 정보설비까지 공격 대상으로 삼을 수 있으며 해킹, 물리적 공격, 정보오염·심리전 등 다양한 수단을 통해 치루어 질 것으로 전망

  - (우주 전장) 지상·해상·공중전 수행에 있어서 인공위성 등 우주 자원의 영향력이 증가함에 따라 위성공격, 위성 간 공격 등 우주 공간 자체가 새로운 전장으로 변모

  - (전장공간의 확대) 사이버·우주 공간이 전장에 새롭게 편입되고 전·후방에 위치한 군사기지 및 정보시설에 대한 동시 타격의 중요성이 증가하면서 전장은 광역화되고 입체화

* 전통적 군사작전이 특정한 국가, 지역이라는 평면적·지리적 영역에 대한 무력 장악을 목표로 이루어졌다면 미래전이 치루어지는 우주공간은 특정 국가의 영공을 벗어나고 사이버전은 지리적 좌표가 무의미한 전장에서 이루어짐

● (전투수단) 장거리 정밀타격력, 무인전투체계, 비전통적 무기체계의 활용이 증가하면서 국가의 전반적인 과학기술력이 군사적 타격능력에 직결

- (장거리 정밀타격) 인공위성, 고고도 정찰체계 등에 의해 원거리 감시정찰 능력이 향상됨에 따라 전방·후방에 위치한 적 전력 및 군사시설을 타격할 수 있는 장거리 정밀타격 역량이 국가의 군사 공격능력의 척도가 될 것으로 전망
- (무인전투체계) 무인기, 무인장갑차, 무인잠수정 등의 무인전투체계는 인명 희생을 최소화하면서도 고위험·고난도 작전의 수행을 가능하게 할 것으로 전망

* 무인전투체계는 로봇공학과 AI 기술 발전에도 불구하고 운용의 유연성 등에서 약점을 가질 것이지만 대량생산을 통한 저비용 전력요소이자 소모가능한 전력요소라는 특성으로 인해 미래전의 주요 전력이 될 수 있음

- (비전통적 무기체계) EMP(Electro Magnetic Pulse) 무기, 고출력마이크로파 무기, 레이저 무기 등은 파괴력 조절의 용이성, 전자전·사이버전 대응성 등의 특성으로 인해 미래 무기로 각광받을 것으로 예상

* EMP(Electro Magnetic Pulse) 무기는 강력한 전자기 펄스로 전자장비를 파괴 또는 무력화시키는 무기이며 고출력마이크로파 무기는 전자파를 방사해 전자장비를 파괴함

* 레이저 무기는 레이저광을 조사함으로써 미사일, 지상표적, 항공기 등을 공격

● (전투형태) 전장공간의 확장, 신기술 기반 전투수단의 등장으로 인해 전략적 중심 마비의 스마트 전투, 네트워크 중심 전투, 운용 중심의 전투가 미래전의 전개 양상이 될 것으로 예상

- (전략적 중심 마비) 광역 전장에 대한 정밀한 파악, 정보의 실시간 공유, 장거리 정밀타격 수단의 확산으로 인해 대량파괴·대량살상을 수반하지 않는 전략적 중심을 효과적으로 파괴하는 스마트 전투가 치루어질 것으로 예측

* 독립적으로 전투를 수행하는 소규모 전투부대들에 의해 전·후방에 걸친 광범위한 지역에서 치열한 전투가 단기간에 벌어지는 것이 미래전의 진행 방식

- (네트워크 중심 전투) 전장 정보를 공유함으로써 분산 배치된 무기와 전력을 통합적으로 운용하고 이를 통해 적 공격에 대한 생존성을 향상시키고 적에게는 최대한의 피해를 입히는 것이 미래 네트워크 중심 전투

* 전통적인 플랫폼 중심 전투가 함대, 기계화 부대 등 미리 정의된 상호보완적 역할을 가

진 전력요소들의 구성을 강조했다면 네트워크 중심 전투는 정보·지식의 공유와 신속한 의사결정에 기반해 분산된 전력요소의 유연한 운용을 강조

- (운영 중심 전투) 복잡한 전장 상황의 실시간 파악과 신속한 의사결정이 가능해짐에 따라 첩보·감시정찰에 의거해 미리 수립된 작전계획의 완수를 강조하던 계획 중심 전투가 아니라 계획의 실시간 수정·조정을 강조하는 운영 중심 전투가 실현

시사점

- 전쟁양상의 변화 배경에는 과학기술의 발전에 따른 무기체계와 관련 설비의 변화가 있어왔는데 미래전 핵심적 기술은 디지털 네트워크, 센서, AI, 로봇 등 ICT 및 관련 융합기술로 사료됨
  - 세계 주요국들이 정보화 시대를 거치고 걸프전 등 현대전을 직·간접적으로 겪으면서 전쟁에서의 인지·정보 관련 능력의 중요성을 인지했다고 볼 수 있음
  - 인지·정보 능력에 관련된 기술이 다양한 유무선 통신기술 뿐만 아니라 센서, AI, 로봇, 3D 프린팅으로까지 확장되는 것이 현실이며 이에 따라 미래전의 주요 기술 또한 변화할 것으로 예상
  - 감시정찰체계, 무기체계, 전투병 등으로부터 수집되는 전장 정보를 실시간으로 분석하고 의사결정을 내리기 위해서는 AI 등의 최신 ICT 기술의 국방 적용이 필수적
  - 인간의 희생을 최소화하는 효과적 전투 수행을 위해 드론, 로봇, 자율주행차 등에서 등장하고 있는 신기술이 지상·해상·공중전의 다양한 무인무기체계에 적용될 것으로 전망
  - 3D 프린팅은 저비용 무기체계 제조를 가능하게 함으로써 무기체계 운용의 유연성을 향상시킬 수 있는 기술적 대안으로 점쳐지고 있음
- 미래전에서 ICT 및 관련 융합기술이 무기화됨에 따라 이들에 대한 공격·방어 기술 또한 주요한 미래 전력 요소로 편입될 것으로 전망
  - EMP 무기, 고출력마이크로파 무기 등은 전자장비, 통신망 등을 파괴하기 위한 목적으로 개발되는 무기들로서 이에 대한 대응책 또한 마련되어야 할 것임
  - 사이버전은 ICT 및 관련 융합기술이 만들어 낸 새로운 전장공간, 전투수단, 전투형태이며 현재 민간·상용 ICT 기술의 군사적 활용에 있어서 반드시 대비책을 마련해야 할 부문

Ⅳ 국방 IDX와 미래 국방

국방 IDX의 개요

- 국방 IDX는 ICT 및 관련 융합기술의 국방 부문 도입을 통해 미래전쟁 양상 변화에 대비하고 국방 무기체계와 국방 지원 부문의 효율성과 효과성을 제고하기 위한 국방기술혁신 전략
  - 전투 공간의 확장, 무기의 정밀화·무인화, 전투 수행의 유연화·스마트화 등의 미래전 변화에 대응하기 위해 ICT 및 관련 융합기술 부문의 신기술을 개발·활용
  - ICT 및 관련 융합기술 부문에서 기확보된 기술역량을 국방 부문에 적용하고 군의 소요 충족을 위해 기초·원천·응용 기술을 연구개발

국방 IDX 추진의 방향성

- 전투 공간의 확장, 무기의 정밀화·무인화, 전투 수행의 유연화·스마트화 등의 미래전 변화와 현재 활발하게 진행되고 있는 AI, 빅데이터, IoT, 등 ICT 혁신 상황을 연계하는 것이 국방 IDX의 기본 전개 방향
  - 무장, 추진, 레이더 등 군사 부문에 특화된 기술 영역 또한 미래전 대응에 주요 요소이나 인식·정보의 중요성이 증가하고 있는 전쟁 패러다임의 변화 추세는 ICT 및 관련 융합기술 부문의 혁신 중요성을 부각
  - 민간 기업, 학계, 정부출연연 등이 기확보한 풍부한 ICT 기술 역량과 경험을 국방 부문에서 활용할 수 있다는 점 또한 ICT 혁신기술의 국방 도입을 강조하는 국방 IDX의 효과성을 제고
- 미래전 변화 전망에 기반한다면 국방 IDX 추진의 효율·효과를 크게 제고할 수 있는 부분은 '5차원 전투공간 대응 국방', '정밀 무인형 국방', '新 전력요소 포괄형 국방' 등
  - (5차원 전투공간 대응 국방) 사이버 공간과 우주 공간까지 확장될 전투 공간에 대한 효과적 장악과 전투 지휘를 위한 초연결 데이터망 기술, 사이버전 대응 기술 등을 통해 광범위한 전장 인지·파악, 안전한 국방망 실현에 기여
  - (정밀 무인형 국방) 실시간 정밀 감시정찰 체계와 지능중심전 실현 기술을 적용하여 지능적 무인 감시정찰과 국방 빅 데이터에 대한 실시간 지능분석 기반으로 적확하고 신속한 지휘결심을 실현

- (新 전력요소 포괄형 국방) 데이터 기반 전투, AI 기반 전술·전략 의사결정, 무인전투체계 등으로 이루어진 새로운 전투 환경에 최고의 능력을 발휘할 수 있는 지휘관과 병사 양성을 위한 무인초실감 가상화 지능훈련 체계를 수립

[그림 1-12] 미래전 대비를 위한 국방 IDX 추진 방향성

미래전 대응을 위한 국방 IDX 추진 내용의 개요

- 5차원 전장공간 정보의 실시간 수집·분석·지휘결심을 위한 초연결 데이터 중심 전쟁(HcDcW: Hyper-connected and Data centric Warfare) 역량 확보
  - 운용 중심의 전투 실현을 위해 5차원 전장공간에서 초연결로 획득한 정보의 실시간 분석으로 결심권자의 신속한 지휘 지원
- 사이버 공간에서 공세적 사이버 중심 전쟁(A-CcW: Aggressive Cyber centric Warfare)
  - 5차원 전장공간 및 지휘통신의 초연결로 이루어지는 사이버상에서, AI 기반 능동적 방호 체계와 공세적 사이버 방호로 전·후방 및 전·평시에 무관한 안전한 국방망 실현
- 드론, 감시정 등 무인 감시정찰 이동체, 경계로봇, 스마트 감시 센서 기반의 실시간 정밀 무인 감시정찰 체계(UISRS: Unmanned Intelligent Surveillance and Reconnaissance System)
  - 기존 인간의 오감기반 경계·감시를 대신하여 드론, 경계로봇, 스마트 센서, 무인 감시정 등에 지능을 탑재하여 실시간 정밀 분석을 하는 지능적 무인 감시정찰체계
- 정밀 타격의 자율 무기, 무인화 무기 등을 위한 지능 중심 전쟁(AI-cW: AI

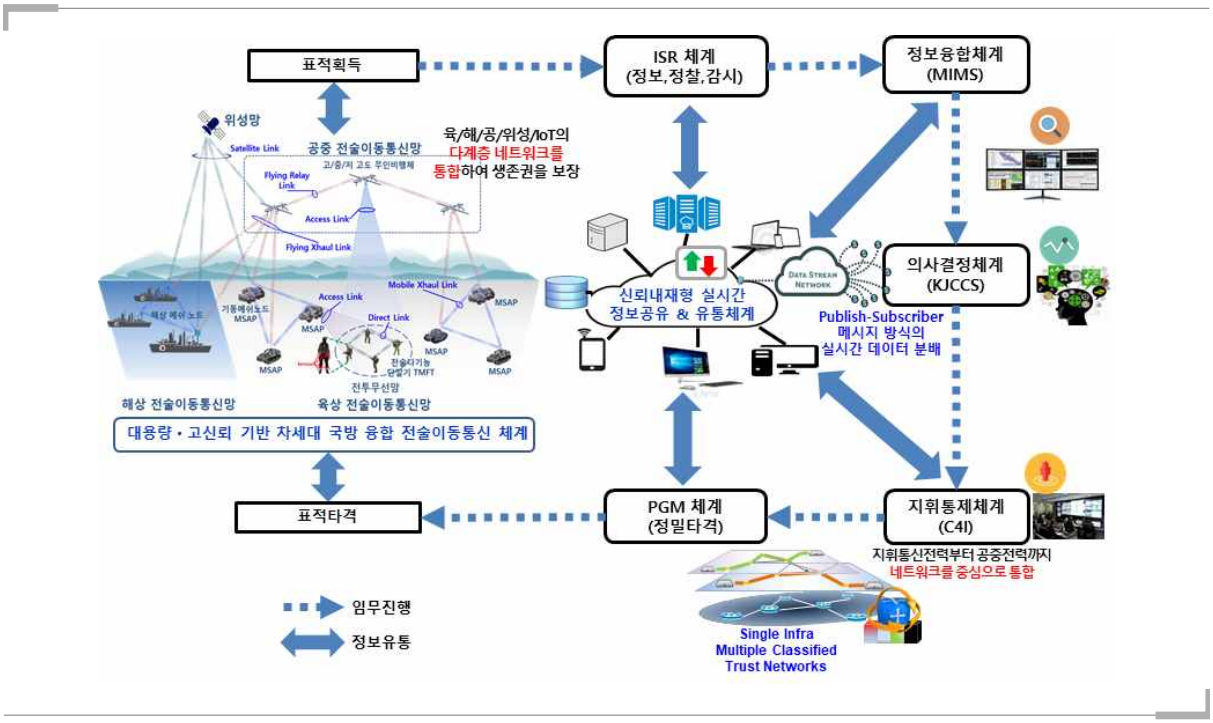
centric Warfare)

- 인적 손실피해 최소화 전장운영을 위한 전투병/전투무기/전투지원체계 지능화와 이들간의 데이터 실시간 지능형 분석기반 작전지휘 의사결정을 기반으로 하는 지능 중심 전쟁

● 스마트 전투병력 양성 등을 위한 초연결기반 초실감 가상화 지능 훈련 체계 (I-LVC: Intelligent Live-Virtual-Construction System)

초연결 데이터 중심전

- 운용 중심 전투 실현을 위해 5차원 전장 공간의 초연결로 획득한 정보를 식별·탐지한 데이터의 실시간 공유·분석으로 결심권자의 신속한 지휘 가능으로 초연결 데이터 중심전(HCDcN)의 미래상을 구현할 것으로 기대
  - 신뢰성 있는 LTE 망을 통해 사람과 사물을 잇는 NB-IoT 통신기술을 M-IoT에 활용한 전투원-자원 국방관리체계 적용으로 NCW에 필요한 전투원과 사물, 사물과 사물간의 통신으로 전장에서의 유기적 작전수행 기대
  - 대용량·고신뢰·고효율의 차세대 이동통신 기반 다계층 통합형 육·해·공·위성·IoT의 다계층 네트워크를 통합하여 네트워크의 생존성을 보장
  - 실시간 네트워크 장애·이상 징후 분석 및 선 대응 시스템 기술로 NCW 맞춤형 전장 상황 지능화 및 가시화 가능
  - 미션 크리티컬 임무 수행시 네트워크 강건성(Robustness) 및 초저지연 통신 보장이 가능한 이동형 전술 클라우드 플랫폼 구축 가능
  - 체계 비종속형 고신뢰 정보유통 및 공유기술 기반체계 통합망 구축과 정보유통 및 정보공유를 통한 체계통합 효과 발휘로 무기체계 플랫폼 간의 상호운용성 확보



[그림 1-13] 초연결 데이터 중심전(HCDcN) 개념도

공세적 사이버 중심전

- 5차원 전투 공간 및 지휘통신의 초연결로 이루어지는 사이버상에서, AI 기반의 능동적 방호 체계와 공세적 사이버 방호로 전·후방, 전·평시에 무관한 안전한 국방망 실현을 기대

  - 인공지능(AI) 기반 능동적 방호 체계가 '국방 사이버보안' 부분에 효과적으로 적용됨으로써 기존의 알려진 공격에 대한 대응 위주의 보안체계에서 신종 악성코드 등에 대응 가능한 예방 중심의 사이버 방호가 가능하게 되어, 국방 사이버 보안의 효율성을 크게 향상시킬 수 있게 되고, 이를 통해 전·후방과 전·평시에 무관한 안전한 국방망 실현이라는 기대효과를 예상해 볼 수 있음

    * 5차원 전장공간 및 지휘 통신의 초연결로 이루어진 사이버 상에서 인공지능(AI) 기반의 지휘 의사결정 지원과 침입자의 탐지 및 대응이 효율적으로 수행

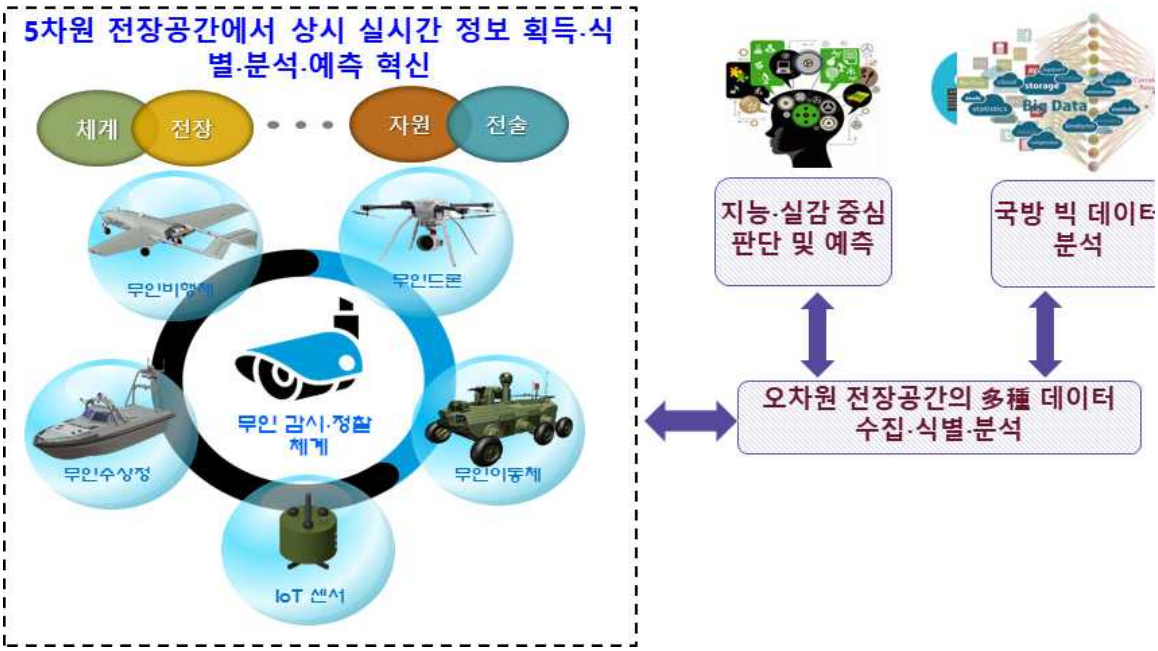
  - 공세적 사이버 방호 기술이 '국방 사이버보안' 부분에 효과적으로 적용됨으로써 평시에도 사이버 상에서 이루어지는 악의적인 사이버 공격에 대응해 침입자에 대한 역추적 및 대응이 가능하게 되어 적절한 사이버 자위권을 수행 가능

    * 초연결로 이루어진 사이버 상에서 침입자에 대한 역추적 및 대응, 각종 물리적 무기체계의 임베디드 보안으로 체계적인 사이버 자위권 수행

[그림 1-14] 공세적 사이버 중심전 개념도

실시간 무인감시정찰 체계

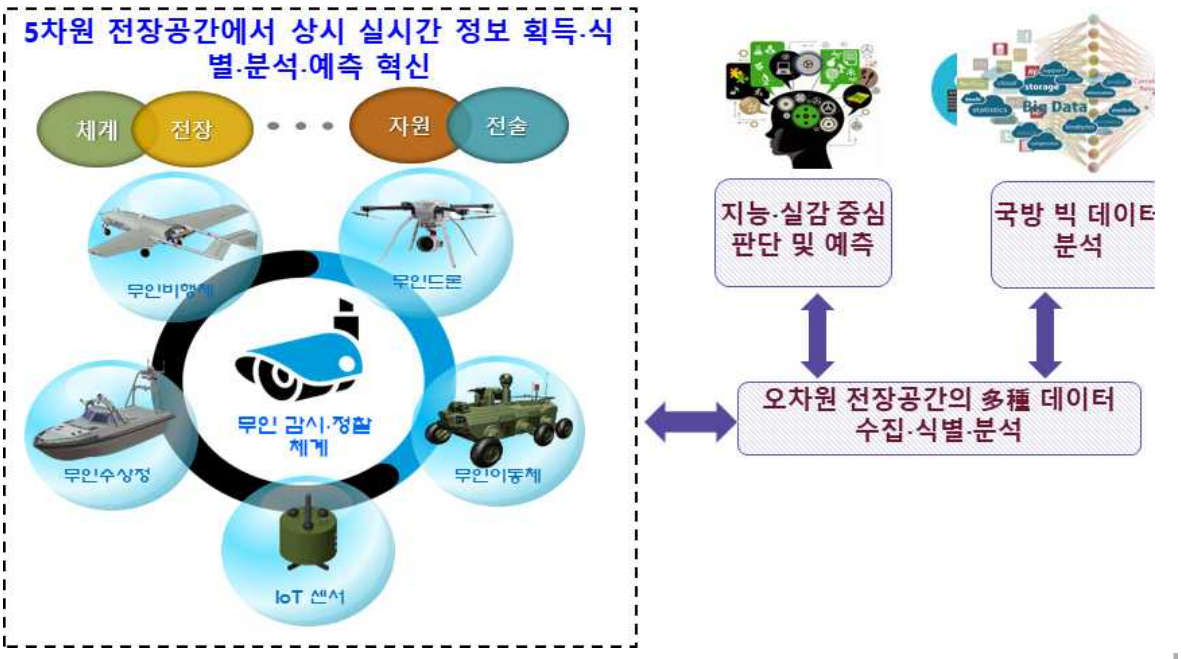
- (5차원 전장공간에서 상시 실시간 정보 획득·식별·분석·예측 혁신) 드론, 경계 로봇, 스마트 센서, 무인 감시정 등에 지능을 탑재하여 실시간 정밀 분석을 하는 무인 지능적 감시정찰 체계로 기존 인간의 오감기반 경계·감시를 대신하여 무인 국방 실현에 기여
  - 오감에 의존한 감시정찰을 지능적 분석을 통한 판단·예측으로 바꾸어 효율적인 국방 경계 감시 실현
  - 줄어드는 병력 자원에 대응하여 효율적인 국방 경계 감시 역할을 수행
  - 삼면이 바다로 둘러싸인 우리의 영해내 수중에서 24시간 상시 실시간 감시·정찰할 수 있는 수중 광 케이블 기반 감시정찰로 안전한 바다 실현에 기여



[그림 1-15] 실시간 무인감시정찰 체계 개념도

지능 중심전

- 국방 데이터 지능형 정밀분석 기술이 전투병·전투무기체계·전투지원체계와 작전지휘 의사결정 분야에 도입되어 인적·물적 손실피해 최소화 전장 운영을 가능하게 하며 전투력 자율 증강 등을 기대
  - (전투무기체계 지능화) 전투 무기체계에 탑재되는 공격 표적 탐지 및 추적기에 인공지능 기술을 도입하여 공격 표적 인식을 가능하게 하여 정밀 타격을 가능하게 하며 나아가 자율 전투 등의 기대효과 예상
  - (전투병 지능화) 전투병의 전투력 증강을 위해 지능형 웨어러블 전투장비를 통해 공격 표적을 실시간 정밀 식별 및 인식하고 전투 경험의 실시간 학습을 통한 전투력 증강 등의 기대효과 예상
  - (전투지원체계 지능화) 전투병, 전투무기체계, 전투지원체계 자원의 수요와 공급을 적재 적소에 공급할 수 있도록 관련 데이터를 학습하여 정밀 수요 예측을 가능하게 할 것으로 예상
  - (지휘통제체계 지능화) 실제 전투 및 훈련에 관련된 누적 데이터 또는 실시간 수집 데이터의 딥러닝을 통해 작전 및 지휘 의사 결정 자동화를 가능하게 할 것으로 예상



[그림 1-16] 지능 중심전 개념도

실 가상화 지능 훈련체계

- 시뮬레이션 기구, 가상현실, 워 게임 등이 통합된 실 가상화 지능 훈련체계 도입을 통해 무인전투체계, AI 기반 전장분석 및 지휘결심보조 등 새로운 전투환경에 투입될 지휘관·병사의 능력을 최고수준으로 연마

  - 무인전투체계, AI 등이 전력체계에 편입되면서 발생할 미래전의 다양한 전략·전술적 상황 대비를 위해 가상현실, 시뮬레이터 등을 활용한 새로운 훈련체계의 광범위한 도입이 요구

  - 실 가상화 지능 훈련체계는 전투기, 장갑차 등의 무기체계에 대한 시뮬레이션 기기, 전장 환경에 대한 가상현실, 실제 전투와 유사한 동적 전투 시나리오를 제공하는 가상 전투 시뮬레이션 SW체계 등을 연계하는 훈련 환경

  - 합성환경(Synthetic Environment), 합성전장(Synthetic Battlefield) 또는 실제 전투공간을 제공하고 L(Live)-V(Virtual)-C(Constructive) 훈련자산과 전투지휘체계를 연결함으로써 통합적 훈련환경을 제공

    * Live는 실 병력이 실제 지형 하에서 직접 기동하면서 훈련을 하는 것을 의미하고, Virtual은 전투장비 시뮬레이터 또는 가상현실을 활용하여 훈련하는 것을 나타내며, Constructive는 가상 상황 하에서 가상 병력을 운용하는 훈련을 의미

  - 실 가상화 지능 훈련체계를 통해 원격에 위치한 특수부대원 등이 가상 작전지역에 대해서 실전과 같은 다대다 전술훈련을 수행할 수 있는 이기종 특수전 가상훈련 시스템 등의 구성이 가능할 것으로 예상

[그림 1-17] 실 가상화 지능 훈련체계 개념도

Part 2

행정 IDX 전략

I 행정 분야 IDX 추진 배경

행정 분야 정의

행정이란?

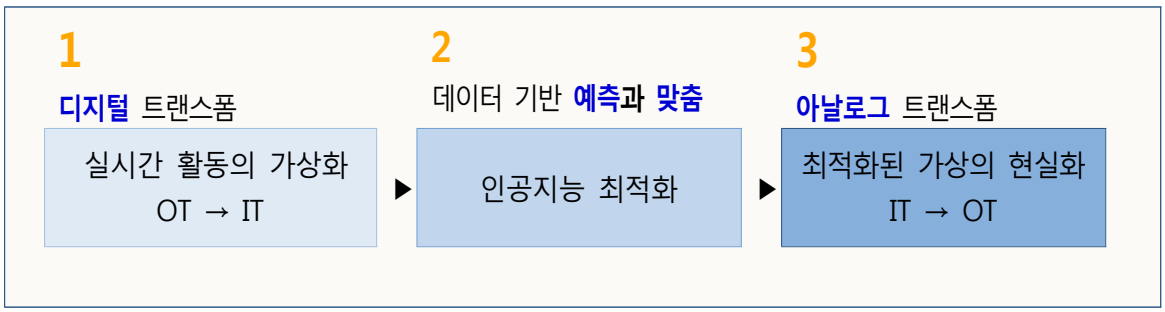
- 행정이란 “공익 목적을 달성하기 위한 공공문제의 해결 및 공공서비스의 생산과 분배와 관련된 정부의 제반 활동과 상호작용”
  - 넓은 의미의 행정은 조직 일반에 적용할 수 있는 인간 협동의 측면에 초점을 맞추는 개념으로 "고도의 합리성을 수반한 협동적 인간 노력의 한 형태"로 정의
  - 좁은 의미의 행정은 정부 관료제 관점에서 행정부의 구조와 공무원의 활동을 포함하는 개념으로, 국가 목적을 실현하기 위한 사람과 물자의 관리로 보거나, 정책결정과 집행을 중심으로 하는 정치 과정의 일부
- 행정은 국가 목적을 실현하기 위한 사람과 물자를 관리하는 운영과정, 정책결정과 집행을 중심으로 하는 정책과정으로 구성

IDX(Intelligent DX)란?

- IDX = Digital Transformation + Intelligence
- 디지털 역량을 바탕으로 기존 산업의 제품·서비스 및 프로세스 전반을 혁신하는 DX의 마지막 단계
- ICT DNA가 ICT가 아닌 다른 산업으로 스며들면서 산업 자체의 생태계를 근본적으로 파괴하고 변화시키는 제 4차 산업혁명의 실체적인 과정
- 기존의 DX에서 한 걸음 더 나아가 국가사회·경제 시스템의 지능형 디지털 유기체화를 통해 제4차 산업혁명 시대를 선도하고 미래 성장 동력을 선점하기 위한 중·장기적인 빅 푸시 전략 (Big Push Strategy)

  ※ Big Push Strategy : 성장이 정체되는 시점에서 기존 사회·경제 시스템 전방에 변화를 가져올 수 있는 혁신 또는 과감하고 도전적인 시도
- 유사개념 : 산업인터넷
  - 산업 요소와 프로세스 연결망[22] → 산업 커넥토믹스 (Industry Connectomics)
  - 제품진단 소프트웨어와 분석 솔루션을 결합해 기계와 기계, 기계와 사람, 기계와 비즈니스 운영을 서로 연결시켜 기존 설비나 운영체계를 최적화하는 차세대 기술[23]

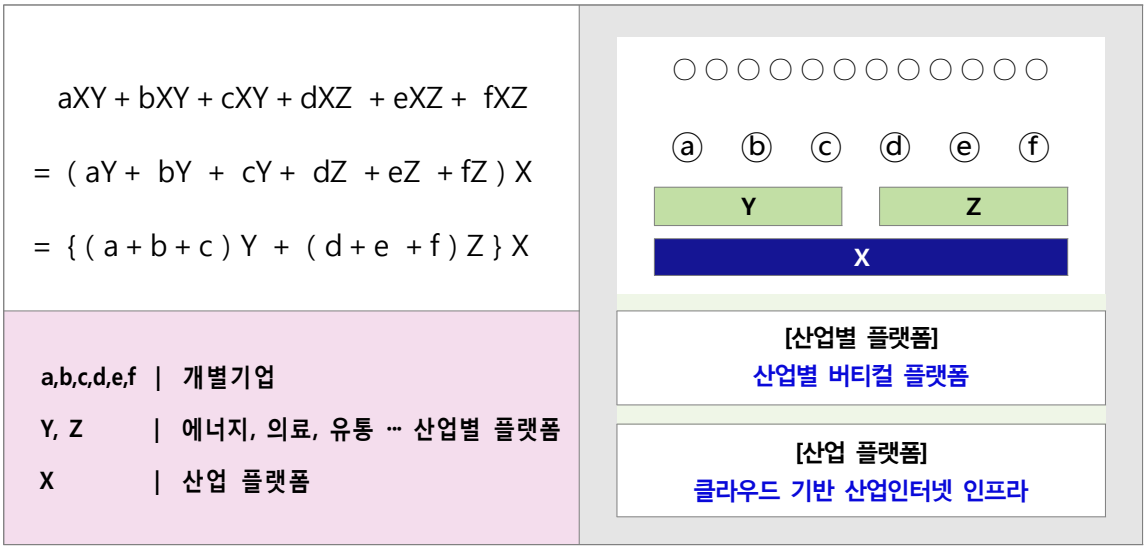
22) KCERN, 2017



자료 : KCERN, 2017, 웨어러블 로봇 플랫폼 워크숍, 2017

[그림 2-1] 산업인터넷 3단계 프로세스

• 산업 플랫폼 아키텍처 : 다중 계층 구조



자료 : KCERN, 2017, 웨어러블 로봇 플랫폼 워크숍, 2017

[그림 2-2] 산업 플랫폼 구조

행정 IDX 개요

행정 IDX란?

- 중앙정부 또는 지방자치단체의 목적을 실현하기 위한 사람과 물자를 관리하는 운영 과정이나 정책결정과 집행을 중심으로 하는 정책과정에서 운영의 효율을 높이고 조직성과를 향상시키기 위해 행정 시스템을 디지털로 전환하고, 유기적으로 통합하여 지능형으로 발전시키는 과정 또는 플랫폼

23) GE

행정 IDX 도입 필요성

- 저출산 고령화로 인한 인구구조 및 규모의 급격한 변화 등에 대비하여 시민행복 증진과 삶의 질 향상을 위해, 과학기술의 사회적 역할 강화와 실용적 적용이 절실
  - 일상생활에서 발생하는 사회경제 문제를 입체적으로 분석하고 구조적인 사회 변화를 적시에 인지하고 능동적, 선제적으로 대응하여 건강·안전·편의 등 지속적인 삶의 질 향상 도모
- 내외부 환경 변화에 대응한 정부 정책실패로 인한 사회적 비용이 증가하고 있어, 정부정책에 대한 신뢰도 하락과 정책의 실효성 저하 심각
  - 저출산·고령화 시대의 도시문제 해결을 위해 도시가 직면한 다양한 문제를 분석하고, 미래변화 모습을 이해하고 새로운 기회와 위험을 포착하여, 근원적 해결책 제시 필요
- 한편 전 세계적으로 도시인구의 유입증가 및 신흥국의 경제성장으로 인해 세계 도시화 추세가 가속화 될 전망
  - 급속한 도시화 추세는 새로운 시장을 형성한다는 측면에서 바람직한 현상으로 받아들여지나 환경오염, 범죄율 증가, 혼잡성 등 다양한 문제를 야기

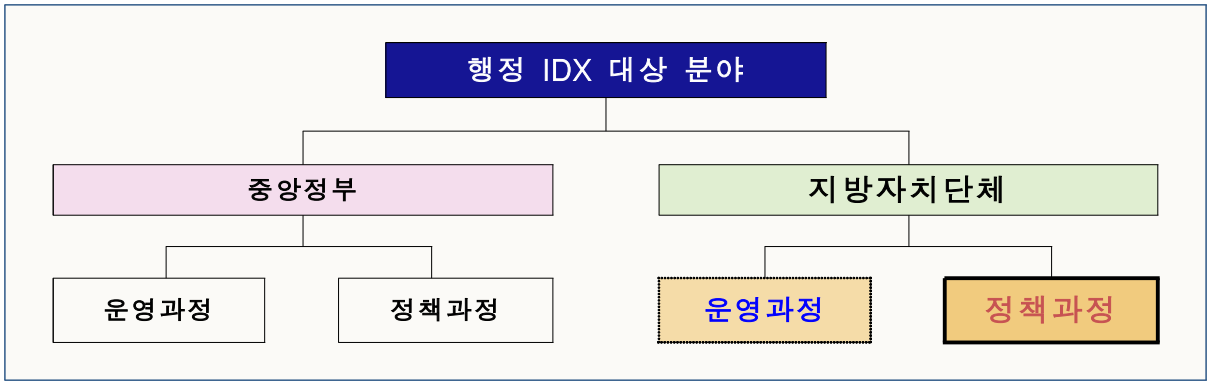
정책과정 요구사항 변화 추세

- **대량화** : 다루어야 할 정책문제의 수가 점차 많아지는 추세
- **복잡화** : 문제와 문제가 얽혀있어 훨씬 복잡해지는 추세
- **다양화** : 내용 또한 매우 다양해지는 추세
- **신속성 및 전문성** : 해결의 신속성/전문성을 점차 중요해지는 추세

[그림 2-3] 정책과정 (Policy Process) 요구사항

행정 IDX 우선 추진 분야

- 행정 분야에서 운영과정은 전자정부에서 주요 의제로 삼고 있는 분야로 이미 세계적인 수준까지 실현되고 있음
- 동적인 환경 변화에 대해 대응하지 못하고 있는 정책과정(Policy Process)을 혁신하여 지방정부에 적용하는 것을 우선 추진하고자 함
- 최근 대두된 분산원장기술(Distributed Ledger Tech.)을 적용하여 시민사회 중심 분산자율 "운영과정 혁신(Operational Excellence)"은 차후 추가하고자 함
- 따라서 본 보고서에서는 이를 구체적으로 실현할 수 있는 시스템을 가칭 **도시행정 디지털트윈 시스템**으로 칭하고 지방자치단체의 정책과정을 대상으로 구체적으로 발전시키고자 함

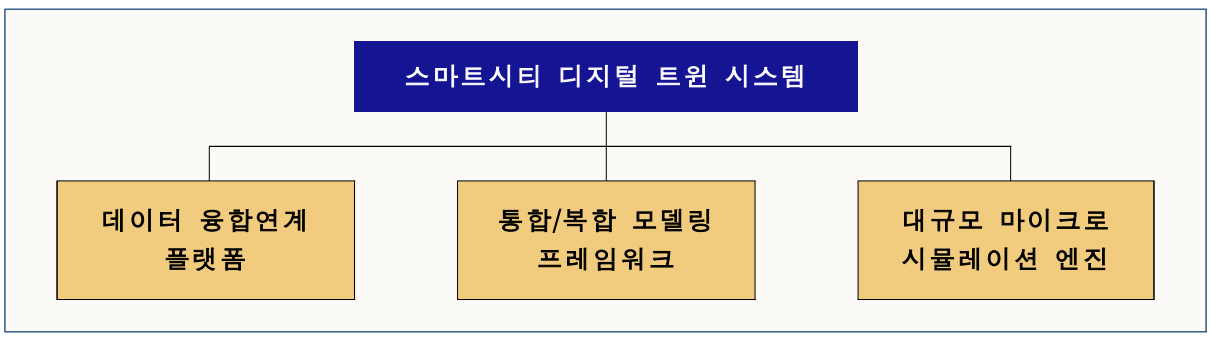


자료출처 : ETRI, 2017

[그림 2-4] 행정 IDX 우선 추진 분야

◐ 도시행정 디지털트윈 시스템 주요 구성 요소

- **데이터 융합연계 플랫폼**
  - 디지털 트윈의 실세계 데이터 반영을 통한 높은 정확도
- **통합/복합 모델링 프레임워크**
  - ABM의 미시적 모델을 통한 높은 정확도와 컴퓨팅 환경의 급격한 성능향상
- **다차원 시뮬레이션 엔진**
  - 정량적인 분석 모델인 ABM의 한계를 디지털트윈 사용자와 시각화 및 인터랙션을 통해 정성적 정책 수립 가능
  - ABM의 미시적 모델을 고성능 컴퓨팅 기반 시뮬레이션으로 높은 정확도의 Massive ABM 시뮬레이션 실현
  - 컴퓨터 전문가가 아닌 사람도 쉽게 사용이 가능하고, 데이터에 의해 진화가 가능한 모델 및 인터랙티브 시각화 기술
  - 실제 도시정책 데이터와 실시간 현실 데이터를 정합한 실환경 반영으로 정확도 향상



자료 : ETRI, 2017

[그림 2-5] 도시행정 디지털트윈 시스템 구성

● 도시행정 디지털트윈 시스템 도입 필요성

- 스마트씨티 디지털 트윈을 도입함으로써 지방자치단체는 공익 목적을 달성하기 위한 공공문제의 해결 및 공공서비스의 생산과 분배의 행정실패 가능성을 대폭 줄임으로써 비용 점감 및 신속한 의사결정을 가능케 하여 생산성 향상 효과를 기대할 수 있음

II 행정 분야 IDX 추진 포인트

행정 분야 생태계 분석

지방자치단체 행정 분야 업무영역

[표 2-1] 행정 분야 업무영역

순번	업무영역	순번	업무영역	순번	업무영역
1	자치행정	2	복지여성	3	문화체육관광
5	산림	6	기획	7	의회
9	복무관리	10	보건위생	11	경제통상
13	교통	14	도로	15	건축주택
17	축산	18	수산	19	공보
21	물품관리	22	차량관리		

자료 : 행정안전부 지방행정정보화, 2017.

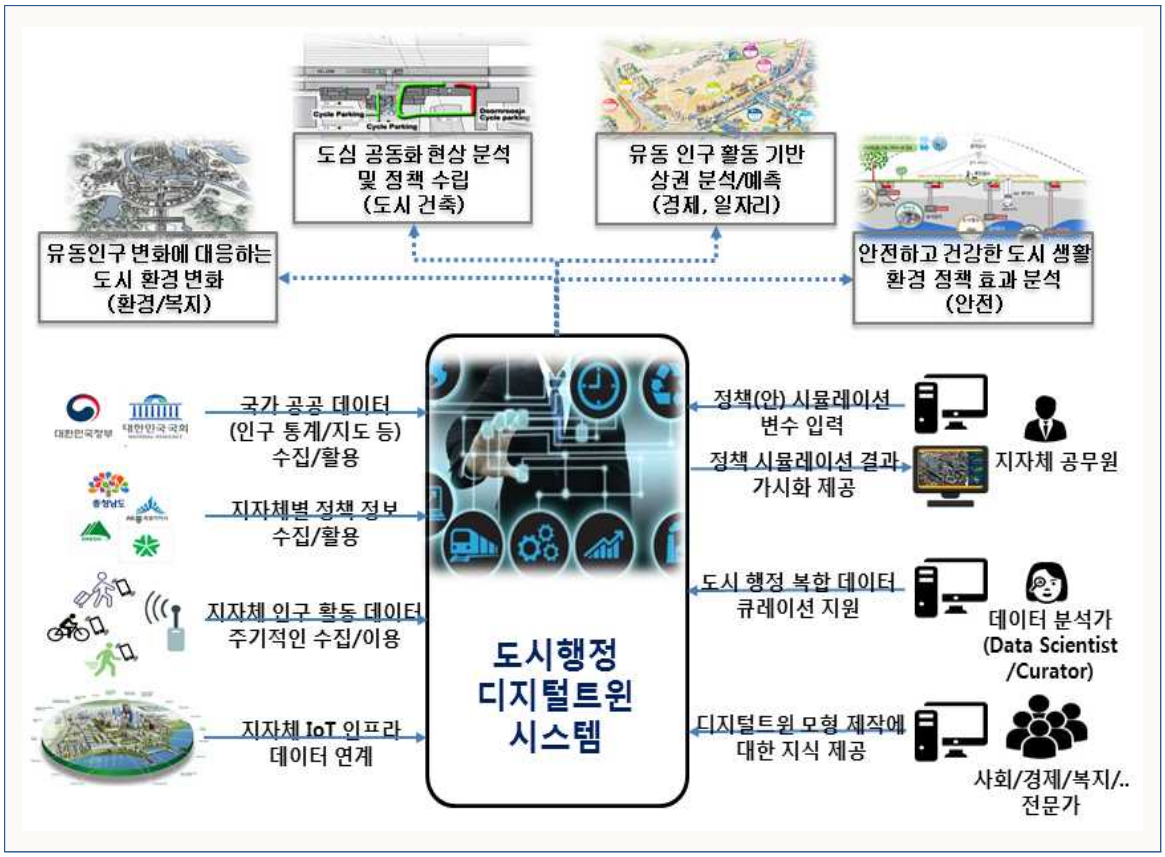
지방자치단체 정책과정 (Policy Process)

(1) 정책의제 발굴
→ (2) 관련 정책 현황 파악 및 정책 이해관계자 맵 도출
→ (3) 정책 방향성 수립
→ (4) 정책 대안 도출
→ (5) 정책 형성 (최고결정자/최고정책결정기구)
→ (6) 정책 집행 및 사후관리

자료 : 고경훈, 지방자치단체 정책형성 요인에 관한 연구, 한국정책연구 2010 재구성
[그림 2-6] 정책과정 (Policy Process)

● 행정 IDX 기반 정책과정 (Policy Process) 업무 흐름

- 자료수집 과정
  - 국가공공데이터 (인구통계, 지도 등 수집 활동)
  - 지자체별 정책 정보 수집 및 활용
  - 지자체 인구 활동 데이터 주기적인 수집 및 이용
  - 지자체 IoT 인프라 데이터 연계
- 자료분석 과정
  - 정책안 시뮬레이션 변수 입력 (지자체 공무원)
  - 도시행정 복합 데이터 큐레이션 지원 (데이터 분석가)
  - 디지털트윈 모형 제작에 대한 지식 제공 (사회, 경제, 복지 전문가)
- 시뮬레이션 결과 제공 과정
  - 지자체 공무원이 정책결정에 활용



자료 : ETRI, 2017

[그림 2-7] 도시행정 흐름도

행정 IDX와 주요 Player와의 유기적 연결고리

- **행정 데이터 수집 Player들**
  - 각 행정업무 담당자
  - 지자체 IoT 인프라 관계자
  - 지자체 정책 수집 관계자
  - 국가 공공데이터 수집 관계자
- **행정 서비스 앱 개발자들**
  - 사회, 경제, 복지 전문가들 : 대학교수, 사회복지사, 시민사회운동단체,
  - 데이터 분석가 : 경제학자, 사회학자, 통계학자, 빅데이터전문가
  - 공공앱 개발자 : 정부가 직접 앱을 개발·운영하는 방식을 탈피, 필요한 공공서비스 기능을 '정부가 제안'하고 정부는 원천 데이터를 제공하고 '민간이 개발·운영'하는 민간앱 개발 공모전도 개최하여 창업 활성화를 지원
- **행정 서비스 사용자**

  · 지자체 정책결정 공무원 : 환경복지, 도시건축, 경제 일자리, 안전 등 지자체 공무원

자료 : 대전광역시 조직도, 2017

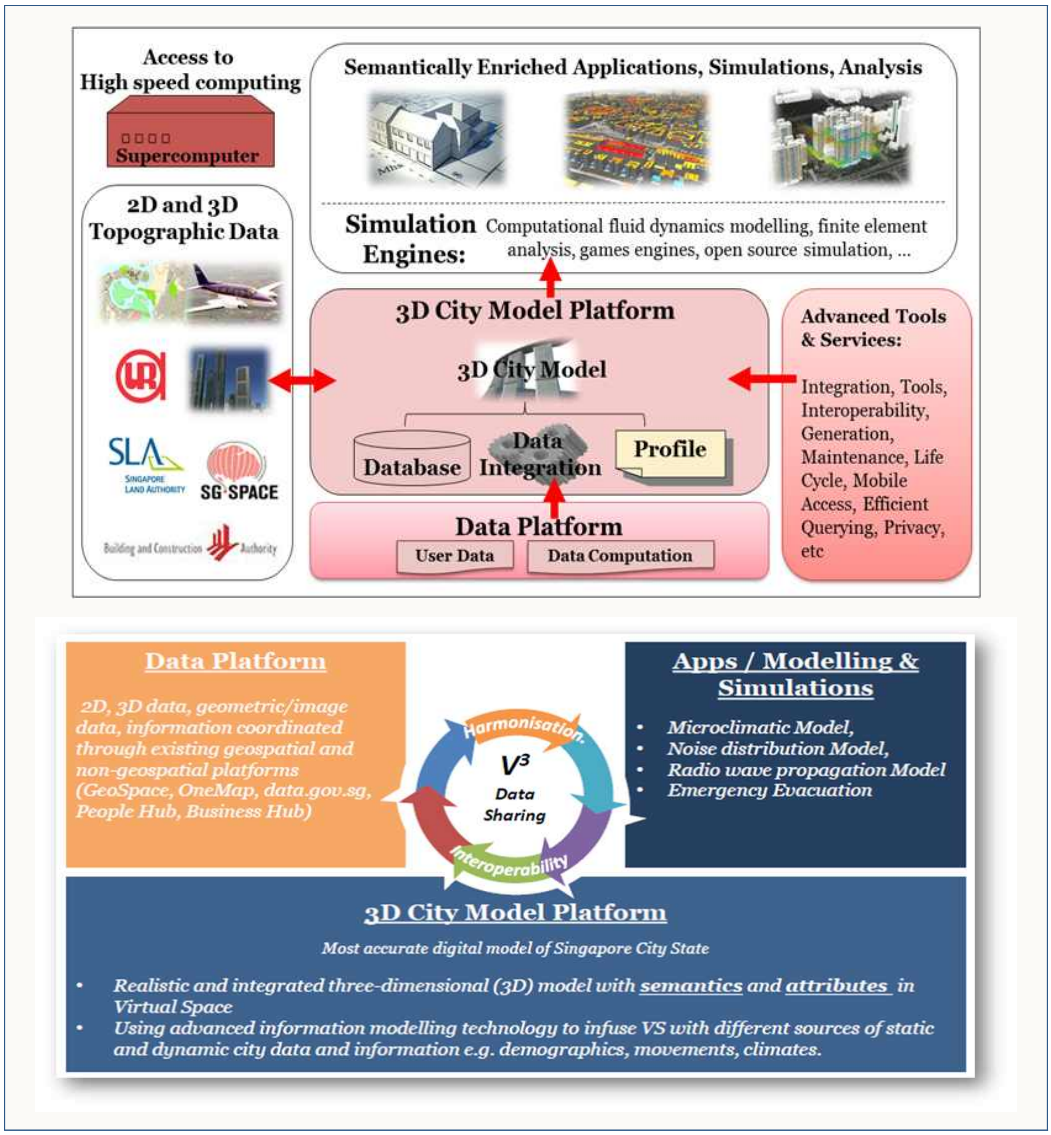
[그림 2-8] 지방정부(대전광역시) 조직도

행정 분야 IDX 기술개발 동향

행정 IDX Benchmark : 싱가포르 “Virtual Singapore”

- 프로젝트 개요

- 도시국가 싱가포르는 건물, 인프라, 녹지를 비롯해 도시의 모든 측면을 가상화하고, 그 결과를 상호작용이 가능한 3D 모델로 구현하려는 대규모 프로젝트[24)]



자료 : Virtual Singapore Project

[그림 2-9] Virtual Singapore Platform

24) 3DEXPERIENCity, 다쏘시스템코리아, 2015

· 시뮬레이션을 통해 다양한 도시 문제를 분석하고, 해결 방안을 탐색

· "가상 싱가포르"를 통해 도시에서 움직이는 모든 것을 포착하고 도시에서 일어나는 모든 일을 실시간으로 파악하고자 함

· "가상 싱가포르"는 인구증가, 새로운 건축 및 주요 행사, 사건에 따라 싱가포르가 어떻게 발전 및 진화해 나가는지를 3D로 가시화 해볼 수 있음

• 싱가포르 국립연구재단(National Research Foundation Singapore)이 싱가포르 국토청(Singapore Land Authority, SLA), 싱가포르 정보개발청(Infocomm Development Authority of Singapore, IDA)과 공동으로 추진

· 점진적으로 개발하여 2018년 완성을 목표로 함

· 인구성장 및 자원관리에서 공공 행사 및 건물 패턴에 이르는 모든 구성 요소를 대상으로 다양한 현상을 시뮬레이션하여, 가장 안전하고 긍정적인 결과 도출

- **주요 활용 분야**

• **SENSg 프로젝트**

· 싱가포르 국립연구재단과 교육부가 싱가포르 기술 및 설계 대학교, 싱가포르 과학센터, A*STAR와 공동으로 조직한 프로젝트

· 300명 이상의 싱가포르 학생들이 SENSg 라는 간단한 기기를 지니고 온도, 습도, 소음 수준 같은 데이터를 실시간으로 수집

· 수집된 정보는 무선으로 중앙 컴퓨터 서버에 전송되며, 학생들은 자신이 수집한 데이터(자신의 걸음 수, 외부에서 보낸 시간, 이동 패턴 등)을 확인할 수 있음

• **공공 데이터/지식 공유**

· 가상 싱가포르 개념에는 빅데이터, 사물인터넷, 3D 모델링, 예측 분석 같은 여러 가지 첨단 기술 트렌드가 결합

· Virtual Singapore 모형은 정부 기관에 정보를 제공하고, 시민은 제한된 데이터에 접근할 수 있는 플랫폼으로 활용 가능

· 기업 역시 공공 데이터를 활용하여 고객에게 맞춤형 서비스를 제공할 수 있으며, 연구자들은 새로운 기술과 서비스를 창조하는 방법을 연구

• **시뮬레이션 기반 의사결정 플랫폼**

· 사고에 대비하여, 3차원 인텔리전트 모델링을 통해 사람들이 흩어지는 모습과 사람들이 취할 행동을 미리 시뮬레이션하여 예측, 대피 계획 수립

· 문제를 해결하기 위하여, 관련된 모든 기관이 동일한 플랫폼에서 문제를 확인하고 협력을 통해 문제를 통합적으로 해결 할 수 있을 것으로 기대

• **과학기술 개발을 위한 기회 제공**

· 과학, 기술, 엔지니어링, 수학(STEM)을 실제 세계에 응용해볼 기회를 제공하는 것과 환경 데이터를 수집해 가상 싱가포르에 활용

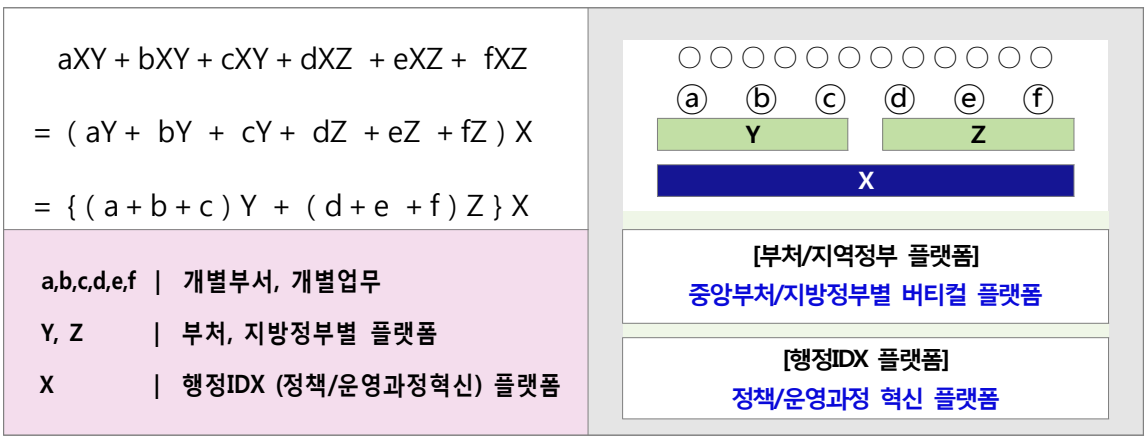
자료 : Virtual Singapore media briefing, 2014

[그림 2-10] Virtual Singapore 활용 예시

행정 분야 IDX 추진 포인트 도출

정책과정 혁신 - 디지털트윈 (Digital Twin)

- 행정 분야에서 IDX 추진을 통해 효율성을 가장 크게 제고할 수 있는 부분은 가치사슬 상 '**정책수립**' 부분과 '**정책평가**' 부분
- 정책과정 분야는 IoT, 빅데이터, 인공지능 기술 등을 적용하여 정책의 효과와 효율 향상시켜 정책 실패로 인한 사회적 비용을 획기적으로 절감 가능

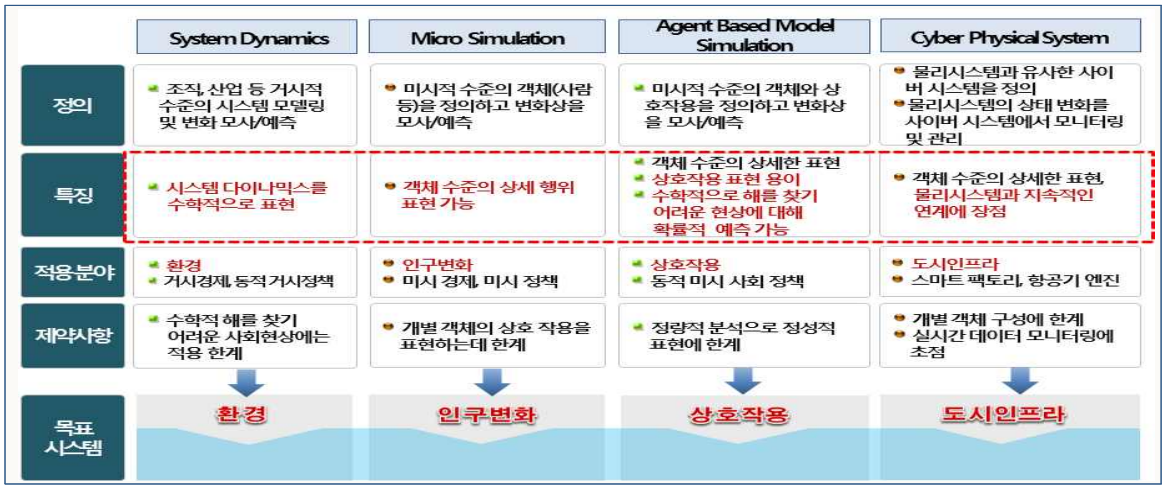


자료 : ETRI, 2017

[그림 2-11] 행정 IDX 정책과정 혁신 플랫폼 구조

도시행정 디지털트윈에 활용 가능한 기술 비교

- 기존 정책 시뮬레이션에서 사용하던 매크로 시뮬레이션, 마이크로 시뮬레이션과 시스템 공학에서 사용하던 ABMS(Agent Based Model Simulation), CPS(Cyber Physical System) 기술을 비교한 것임

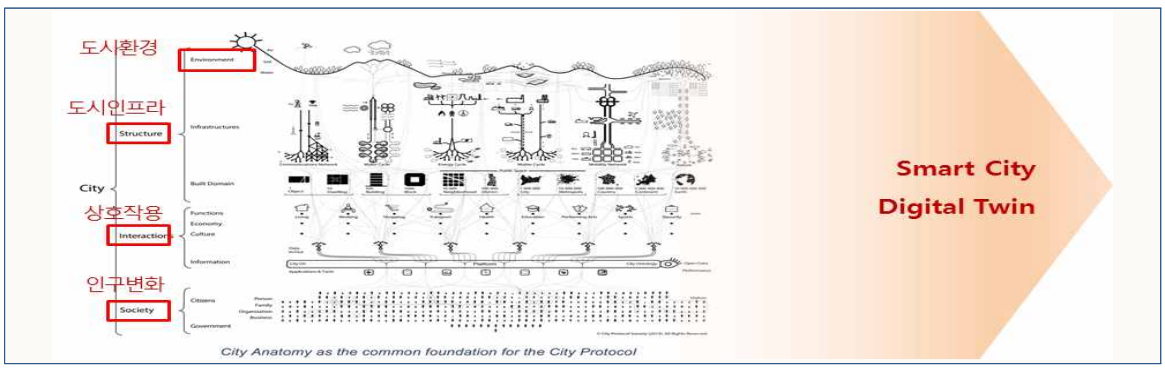


자료 : ETRI, 2017

[그림 2-12] 도시행정 디지털트윈 활용 기술 비교

활용 가능 기술 비교 분석 결과

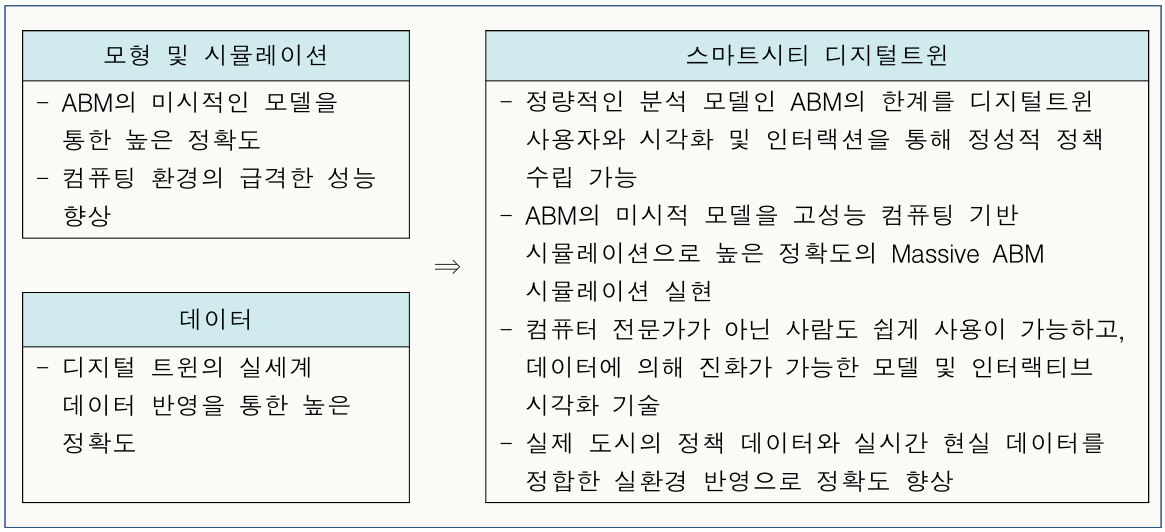
- 개별적인 행위의 분석을 통하여, 거시적인 시스템 관점에서 정성적, 정량적 분석이 가능하고 실시간 데이터를 통해 정확도를 높이기 위해서는 **대규모 ABMS** (Massive Agent based Model Simulation) 방법론 채택
- 도시 공간에 존재하는 미시적 수준의 객체를 정의하고 상호작용을 모두 표현할 수 있는 인공 사회(Artificial Society)를 구축하고, 물리적인 도시의 현실 데이터와 연계하여 현황에 대한 입체적인 분석과 도시 미래 예측, 정책 실험 및 검증



자료 : ETRI 재작성, 2017

[그림 2-13] 도시행정 디지털트윈 해부도

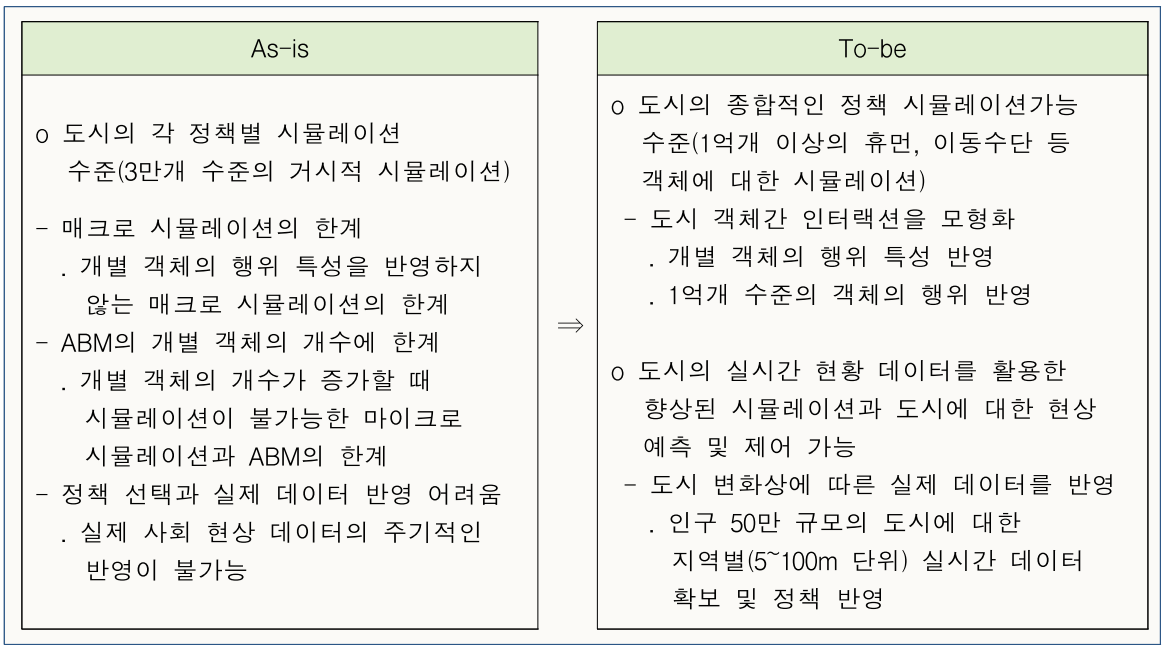
- 도시 규모를 미시적 수준에서 통합 시뮬레이션이 가능하도록 대규모 ABM, 고성능 컴퓨팅, 실시간 마이크로 데이터 연계를 해결 방안으로 채택



자료 : ETRI, 2017

[그림 2-14] 미시적 수준 통합 시뮬레이션

- 입체적/동적 데이터 플랫폼과 1억 개 수준의 도시 객체 모델링/시뮬레이션을 통한 도시 커넥토믹스 기반 디지털 트윈 실현



자료 : ETRI, 2017

[그림 2-15] 도시 커넥토믹스 기반 디지털 트윈 실현

행정 분야 IDX 미래상

정책과정 혁신 (Policy-Making Excellence)

- **(데이터 기반 정책 수립)** 정부가 확보한 수많은 데이터를 기반으로 재난, 범죄, 서비스 수요을 예측해 최적의 대책을 수립할 수 있는 인공지능과 빅데이터가 결합된 인지·예측 기반 지능행정 기술이 구현될 것
  - 예를 들면 지방자치단체의 결혼 인구, 노령 인구 등과 같은 행정 빅데이터를 과학적으로 분석하여 미래 인구 정책 등에 활용할 것
  - 인공지능이 모든 정책 데이터를 분석해 상황에 맞는 최적의 정책적 처방을 제시해주는 한편, 새로운 정책을 개발하는 데에도 활용될 수 있을 것
  - 모든 정책 정보가 빅데이터와 클라우드로 공유되면서 중앙 정부와 지방 정부간, 부처간, 부서간 정책의 미스캐치나 중복 추진이 발생할 경우 인공지능이 경고를 보내주어 정부 예산의 효율적 사용이 가능해질 것

자료 : ETRI, 2017

[그림 2-16] 데이터 기반 정책 수립과정

- **(AR/VR 기반 원격 행정)** 미래에는 VR 시스템이 구축된 가상 회의실에서 회의를 하는 것이 당연해지는 시대가 될 것
  - 현재의 회의 문화가 가상현실 회의로 대체되는 것
  - VR 기술과 홀로그램 기술이 더욱 발전되어 회의실이나 온라인상에서 진행되는 회의를 가상공간에서 진행할 수 있게 될 것
  - 이에 따라 공무원의 재택근무가 가능해지고, 홀로그램이나 VR을 이용해 현장 상황을 같이 보면서 정책 결정을 할 수 있기 때문에 탁상공론이나 탁상행정에서 벗

어날 수 있게 될 것

- 국민들에게도 현장감을 높인 행정 서비스 제공이 가능해져 행정 서비스에 대한 만족도와 활용률이 증가할 것
- 한편 자동 통역 기능이 내장된 원격 회의 시스템 덕분에 다른 국가의 정책 담당자와도 수시로 회의가 가능해지고 정확한 정책을 추진할 수 있게 될 것

운영과정 혁신 (Operational Excellence)

- **(AI 기반 실시간 여론조사)** 정치 및 정책 결정권자가 연설이나 토론을 할 때 인공지능 컴퓨터가 공적 발언의 사실 여부를 실시간으로 판별해 알려주어 사실에 기초한 검증된 토론이 가능해질 것
  - 이에 따라 유언비어나 근거 없는 악성 루머를 방지하고 국민 여론을 실시간으로 수렴하여 정책에 반영할 수 있게 될 것
  - 또한 신빙성 없는 각종 여론조사에 현혹되지 않을 수 있고, SNS 등에 연결된 국민들의 성향을 인공지능이 실시간으로 분석하여 연설이나 통론에 대한 정확한 반응과 예측이 가능해질 것
  - 개인이 정치, 경제, 외교, 교육, 복지 등 갖공 이슈에 관한 입장을 선택하면 인공지능이 자신과 비슷한 경해와 관심사를 가진 사람들을 인터넷에서 연결해주는 것이 가능해지고 온라인상에서 논의되는 내용을 인공지능을 통해 정책에 반영할 수도 있을 것
- **(직접 민주주의로 새로운 정치질서)** 얼굴 인식, 생체 인식, 블록체인 기술 등을 활용한 인터넷 투표로 디지털 직접민주주의가 확대될 것
  - 시민이 직접 정책 입안 과정에 참여하여 정치의 계급구조가 사라지고 수평구조가 정착될 것
  - 이러한 시스템상에서 시민들은 동등하게 의안 논의에 참여하고, 이를 바탕으로 의사결정까지 할 수 있게 될 것
  - 디지털 직접 민주주의가 확대됨에 따라 문제를 겪고 있는 사랑들이 직접 문제해결에 나설 수 있게 되어 사회적 문제 해결이 보다 수월해질 것
  - 또한 온라인 정당이 활성화되면 집단지성을 통한 당원의 의견 수렴을 통해 국민 의사가 실시간으로 반영되어, 인물 중심의 정치 질서가 정책중심의 정치 질서로 재편될 것
  - 앞으로 정당 안에서 폐쇄적으로 결정되어 온 의제, 후보 지정, 투표 방식 등 선거의 전반적 과정이 온라인을 통해 투명하게 공개되고 설정될 것
  - 이에 따라 로비 세력이나 정치자금 규모가 아닌, 유권자의 뜻을 보다 잘 따른 후보가 선출될 것

Part 3

교육 IDX 전략

Ⅰ 개요

【1】 개념 및 범위

교육이란?

- 교육은 지식, 기술을 가르치고 배우는 활동으로 정의되고 그 시대 및 사회가 요구하는 인재상에 따라 적합한 학습법이 등장

- 과거 농경사회에서 실용적 기술을 익히기 위해 도제식 교육법이 중요했고, 산업혁명으로 인해 대량생산체계 하에서 학문적 지식을 익히기 위해 국가가 보편적 의무교육을 추진하였으며 정보화 혁명 이후 개인의 평생학습이 강조

[표 3-1] 교육 패러다임 변화

구분	1세대 : 도제식 교육	2세대 : 보편적/의무교육	3세대 : 평생학습
책임의 주체	부모	국가	개인과 부모
목표	사회적 재생산	대량 생산	개인의 선택 존중
교육의 내용	실용적 기술	학문적 지식	자기학습
페다고지	도제식	주입식	상호작용

자료 : Collins&Halmerson(2009)를 재인용

디지털 교육 패러다임 변화

- 4차 산업혁명의 대두로 미래 일자리 변화, 그에 따른 새로운 인재상이 요구됨에 따라 교육 분야의 중요성과 변화가 자연스럽게 부각 중

- **(일자리 변화)** 세계경제포럼(WEF), 마틴스쿨(옥스포드) 등에서 사회변화와 그에 따른 고용, 새로운 인재상*에 대한 이슈를 제기

  * 크게 ①기초기술(문해, 수해, 과학문해, ICT문해, 재정문해, 문화 및 시민문해), ②역량(비판적사고/문제해결, 창의성, 의사소통, 협력), ③인성자질(창의성, 주도성, 일관성/도전정신, 적응력, 리더쉽, 과학 및 문화)을 21세기에서 요구할 미래상으로 제시(WEF, 2015)

  ※ 세계경제포럼(WEF:World Economic Forum)은 '제4차 산업혁명의 이해'를 핵심 의제로 채택하고 "과학기술과 디지털화가 모든 것을 완전히 바꾸는 파괴적 변화와 혁신의 시대"가 될 것으로 예측(2016)

  ※ 마틴스쿨의 '고용의 미래'보고서에서 기술에 의한 자동화로 향후 20년 내에 미국 내 현재 직업의 47%가 도태 가능성을 제시

- **(새로운 인재 역량)** 예측 불가능한 사회 변화에 대응하기 위한 인재상으로 창의

성, 복잡한 문제해결 능력, 도전정신 등을 가져야하며 사회적 기술 및 시스템 기술*이 이를 뒷받침 할 것으로 전망

* 인공지능, 빅데이터, 클라우드, 로봇, 3D 프린팅, VR/AR 등이 제4차 산업혁명을 주도할 IT 기술로 부각 중

- **(교수법의 다변화)** 전통적인 주입식 교육과 차별화되며, IT 기술을 접목한 다양한 새로운 개념의 학습모델이 새롭게 부상 중

※ 최근 부상 중인 MOOC(Massive Open Online Course)는 새로운 학습모델로써 웹 기반 대규모 참여가 가능한 상호작용형 교육 시스템

● 교육환경의 변화는 크게 교육 대상, 교육시간 및 장소, 교육의 방법, 학습 개념 등 전반에 걸쳐 나타남

- **(대상)** 학생뿐만 아니라 성인까지 확대되어 평생학습이 활성화 중
- **(시간 및 장소)** 시공간 제약이 사라져 실시간으로 어디서든 교육과 학습이 이루어질 수 있도록 교육환경이 변화(집합식 교실수업→Cyber 자기주도 학습)
- **(방법)** 교육자(교수) 중심에서 학생 중심으로 변화됨에 따라 이에 맞는 다양한 학습 콘텐츠나 교수법이 출현 중
- **(개념)** 학습개념이 주입식(Training)에서 과제해결형(Learning)으로 변화

[그림 3-1] 교육+IT 융합으로 인한 교육환경 변화

- ICT 기술 발달로 디지털 교육은 이러닝→유러닝→스마트러닝으로 학습방법의 변화가 나타나고 있으며, 방향성은 개인 맞춤형 학습 콘텐츠를 지능화하는 형태로 진행 중
  - 초기 ICT 활용 교육은 다양한 멀티미디어 및 기기를 활용하여 개개인이 필요로 하는 미디어형 교육자료를 수동적으로 제공하는 형태
  - 최근에는 스마트러닝을 에듀테크(edutech: education+technology)와 유사 개념으로 제시하고 있으며 주요 선진국들은 에듀테크의 활성화 및 생태계 형성을 위해 다양한 정책, 기술개발 등을 추진 중

[표 3-2] 디지털 교육(학습)의 진화

	ICT활용교육	이러닝	유러닝	스마트러닝
학습형태	컴퓨터보조수업(CAI) 인터넷활용교육(WBI)	학습관리(LMS)	이동학습 (m-Learning)	지능형맞춤형식 (Intelligent, Adapted)
주요 서비스	문자통신, 미디어 학습, EBS위성방송	인터넷기업직무교육 수능인터넷강의 인터넷공무원교육	모바일 콘텐츠 증강현실 콘텐츠	지능형진단평가 앱서비스, SNS활용
주요기기	데스크탑 PC	인터넷PC	모바일 노트북, PDA, PMP	스마트폰, 스마트TV
시기	1996년 ~	2002년 ~	2005년 ~	2010년 ~

출처 : 한국이러닝산업협회(2016)

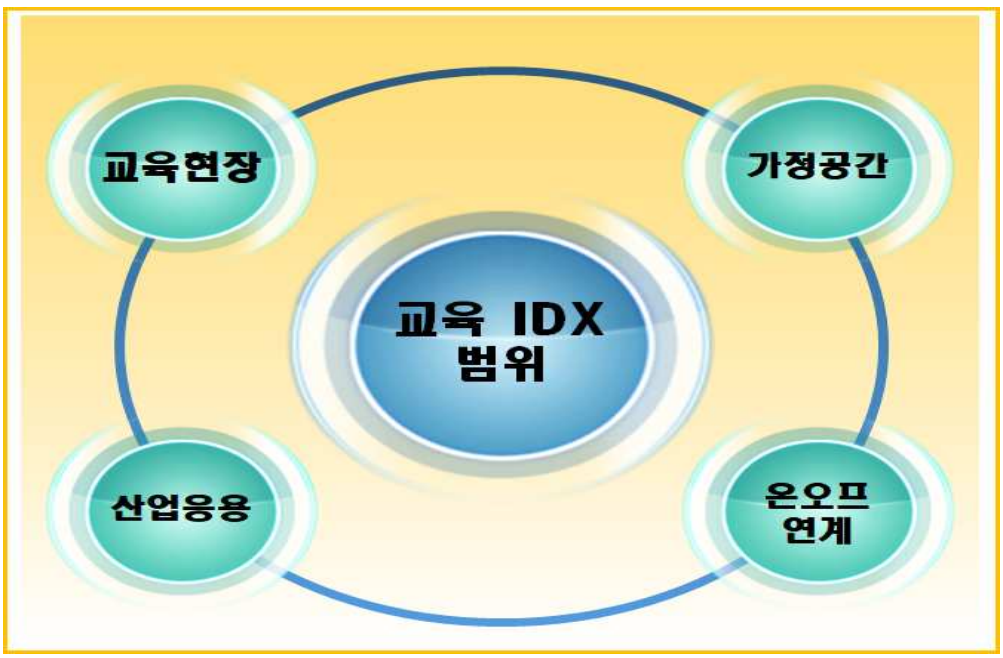
교육 IDX 개념 및 범위

- **(개념)** 교육에 고도화된 IT기술이 적용이 본격화되어 교육시스템이 지능화, 실감화가 가능하게 변화함에 따라 개인별 맞춤 교육을 효과적으로 지원하는 교육 패러다임 및 환경을 의미
  - 디지털 환경의 변화에 따라 교육의 DX 현상이 이미 진행 중이고, 그로 인해 과거 단순 ICT 활용교육에서 점차 발전하여 에듀테크로 진화 중이며 그 연장선상에서 나타날 결과물이 교육 IDX일 것으로 예상
    * DX(Digital Transformation)는 인간 사회의 모든 분야에서 디지털 기술의 적용과 관련된 변화로 정의(Erik S. & Anna C., 2004)

- 따라서 본고에서는 에듀테크를 중심으로 동향을 살펴보고, 교육 문제점과 그로 인한 교육 IDX 이슈(해결방안), 미래상, 정책 및 R&D 방향 등을 모색해 보고자함

● **(범위)** 교육이 일어나는 공간을 중심으로 교육 현장, 가정 공간, 산업 응용 및 온오프 연계의 4가지 영역으로 설정

- **(교육현장)** 일반적인 교육과 학습은 학교라는 교육현장에서 발생
  ※ 초등, 중등, 고등학교와 대학교를 일반적인 교육현장으로 다루며 관련 사교육도 포함. 다만 본고에서는 정규교육과정 및 공교육 관점에서 기술
- **(가정공간)** 흔히 가정교육으로 불리며 가정공간 상에서 이루어짐
- **(산업응용)** 산업현장에서 일어나는 직업교육은 다양한 산업 내에 존재함에 따라 명칭은 산업응용으로 설정
  ※ 산업응용 분야는 제조업뿐만 아니라 물류(항공, 교통 등), 개인서비스, 스포츠, 국방, 금융 등 다양한 영역에서 직업훈련 실감콘텐츠 제공이 가능
- **(온오프연계)** 전통적인 현장학습은 이론 교육 장소 밖에서 이루어지나 온오프 연계는 이런 장소의 구분 없이 교육을 어떤 장소에서건 할 수 있는 형태이며, 교육에서의 새로운 영역에 해당



[그림 3-2] 교육 IDX 범위

【2】 관련 산업 현황

에듀테크 산업 개요

- **(개념)** 학습 알고리즘, 데이터 기반 평가 및 분석, 참여자간 상호작용, 가상 및 증강현실 등의 ICT 기술을 이용해 교육 및 학습 서비스 제공하는 개념으로 교육(education) + 기술(Technology)의 합성어

  * 에듀테크(Education Technology) : 교육과 기술의 합성어로 전통적인 교육에, 미디어, 디자인, 소프트웨어, VR, AR, 3D 등 ICT 기술이 결합

- **(특징)** 국가별 교육정책에 따라 형성된 교육방법에 진화된 ICT 기술을 접목함으로써 새로운 교육시스템으로 거듭나는 것이 특징

- 모바일 러닝 분야의 성장과 함께 게임형태의 학습시스템 등장
- 대형 출판사에서부터 기술기반 스타트업까지 적응교육을 이용한 개인 맞춤형 학습 시스템을 형성하는 중
- 학습관리는 웹, 앱 및 소셜 기반 오픈소스 소프트웨어가 새롭게 부상 중
- 개인, 사업체에 대한 평생학습 및 훈련에 대한 수요가 점차 증가하고 있으며 복잡한 문제를 해결하기 위해 다양한 ICT기술을 활용하는 추세

- **(산업구조)** 크게 에듀테크 콘텐츠를 중심으로 교육이론, 인터넷, 모바일 등 후방산업과 초중교, 대학, 산업체 등이 전방산업으로 존재하는 형태

- 후방산업의 기술적 인프라 수준에 따라 관련 서비스 및 콘텐츠의 양적 및 질적 차이가 존재
- 전방산업은 초중고 온라인학습, 전문강의, 언어/취미 등의 평생교육, 직무교육 등의 분야가 존재

- 최근 인공지능, VR/AR 등의 ICT 기술 발달로 교육 분야에 적용성이 확대 중이며, 그로 인해 상호작용 및 실감형 콘텐츠, 학습환경 및 학습자관리 등의 교육과 ICT가 융합된 새로운 콘텐츠가 출현 중

- 이러닝이 에듀테크로의 변화에 있어 최근 ICT 기술 발달은 큰 기여를 하고 있으며 교육뿐만 아니라 다양한 산업영역에까지 응용영역이 확대 중
- 창의적인 인재 양성을 위해 적응학습, 개인화 학습, 플립러닝, 소셜러닝 등 다양한 교수법이 등장하고 있고 이를 뒷받침하기 위한 교육 콘텐츠 개발이 확대되는 추세

에듀테크 기술 분류

- **(에듀테크)** 콘텐츠 개발 중심으로 필요한 기술을 구성하고 있으며, 크게 실감교육, 맞춤형 학습, 코딩교육으로 구분(중소기업청, 2016)
  - (실감교육) 가상증강현실 기술을 중심으로 다양한 체험형 콘텐츠를 통해 학습할 수 있도록 하는 교육서비스
  - (맞춤형 학습) 학습분석기술, MOOC 학습 데이터 분석 기술, 학습 에이전트 기술, 소셜러닝 콘텐츠 분류 및 검색 기술 등
  - (코딩교육) 네이티브 프로그래밍 기술

[표 3-3] 에듀테크 제품 중심 기술 분류

구분		세부기술
실감교육	공간인식 기반 체험형 가상증강현실	- 가상증강현실 구현 기술, 공간인식 기술, 인터렉티브 콘텐츠 제작 기술
맞춤형 학습	학습 분석 기술	- 학습자 평가 및 채점 기술, 학습자 모델링 및 학습 능력 진단 기술, 학습자 성적 예측 기술
	학습 에이전트 기술	- 맞춤 학습 콘텐츠 추천 기술, 학습 콘텐츠 제공 플랫폼 기술, 맞춤형 학습 스케줄 생성 기술, 개인별 학습 코칭 기술
	MOOC학습 데이터 분석 기술	- 스텔스 시험 기술, 학습 데이터 기반 도메인 지식 추출 기술, 데이터 마이닝 기술
코딩교육	네이티브 프로그래밍 기술	- 저작도구 기술, 프로그램 클래스 블록화 엔진 기술, 2D/3D 엔진

출처 : 중소기업청(2016)

[참고 1] 이러닝 기술분류 및 내용

◐ **(이러닝)** 국제표준화기구(ISO)에서 이러닝 분야의 교육기술을 ITLET*로 정의하고 세부기술별로 표준화 추진 중

* Information Technology for Learning, Education and Traning

- **(콘텐츠)** 온라인 콘텐츠 표현 및 전달 기술, 교육용 전자책 표현 기술, 실감형 콘텐츠 제작/표현/상호작용 기술, 교육기술 접근성
- **(평가)** 문제은행 및 온라인 평가 기술
- **(학습환경)** 스마트 학습환경, 서드파티 학습용 소프트웨어 연동 기술
- **(학습자관리)** 프로파일 및 e-포트폴리오 관리 기술, 학습 분석 기술

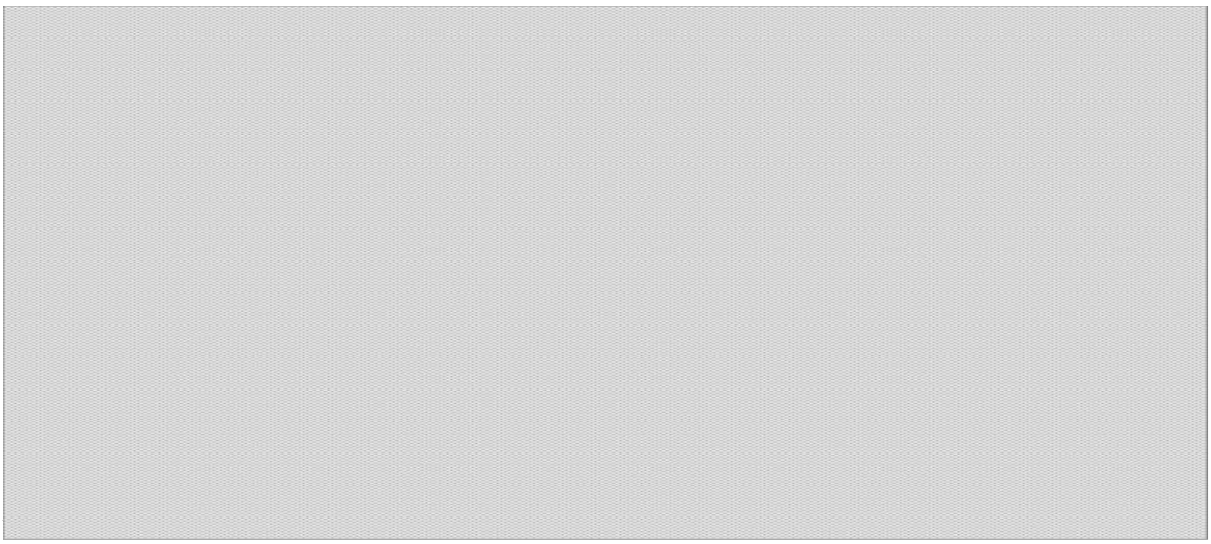
< 이러닝 기술 내용 >

구분		기술내용
콘텐츠	온라인콘텐츠 표현 및 전달 기술	-웹 페이지, 학습용 SW 호출, 온라인 포럼, 온라인 평가 등의 기능을 모듈 단위로 연계
	교육용 전자책 표현 기술	-HTML5와 CSS3 등 새로운 웹 기술을 이용한 상호작용 콘텐츠 표현 -메모, 하이라이트, 사용자 주석처리 등 사용자 데이터를 저장/관리 -전자책에 온라인 평가, 학습용 SW호출 등 이러닝 지원을 연계
	실감형 콘텐츠 제작, 표현 및 상호작용 기술	-VR/AR기술을 활용한 실감교육 콘텐츠 제작 가이드 -HMD와 NUI기술을 활용한 학습자와 교육 콘텐츠 상호작용, 교육 주체간 커뮤니케이션 가이드 -실감형 콘텐츠를 학습관리시스템에 탑재 및 전달키 위한 패키징 기술
	교육기술 접근성	-사용자의 요구 및 선호도를 기술하는 공통의 정보모델을 이용해 메타데이터를 매칭하는 방식의 접근 기술
평가	문제은행 및 온라인 평가 기술	-평가시스템에서 시험자의 응시부터 결과제출단계까지의 프로세스를 생명주기 관점에서 표현할 수 있도록 설계
학습 환경	스마트 학습환경	-사물인터넷과 클라우드 서비스, 로봇 활용 등 첨단 기술과 미디어를 활용하여 개별화된 학습 경험과 매체 활용 상호작용을 통한 학습 효과 증진을 위한 교실 및 학습 환경을 구성하는 요소 기술
	서드파티 학습용 소프트웨어 연동 기술	-학습 플랫폼 내부 및 외부에 존재하는 학습용 SW를 호출하고 데이터를 상호운용할 수 있는 표준
학습자 관리	학습자 프로파일, e-포트폴리오 관리 기술	-학습자의 이력, 목표, 성취도 기록 및 관리, 역량 개발 이력 및 관리, 학습분석에 따른 학습 경험 유도, 학습자의 학습 기회 파악 등을 표현
	학습분석기술	-학습 활동으로 생성되는 정형 또는 비정형 데이터를 체계 적으로 수집·분석·가공·시각화하는 워크플로우에 대한 참조 모델과 시스템 요구사항

출처 : 국가기술표준원(2017)

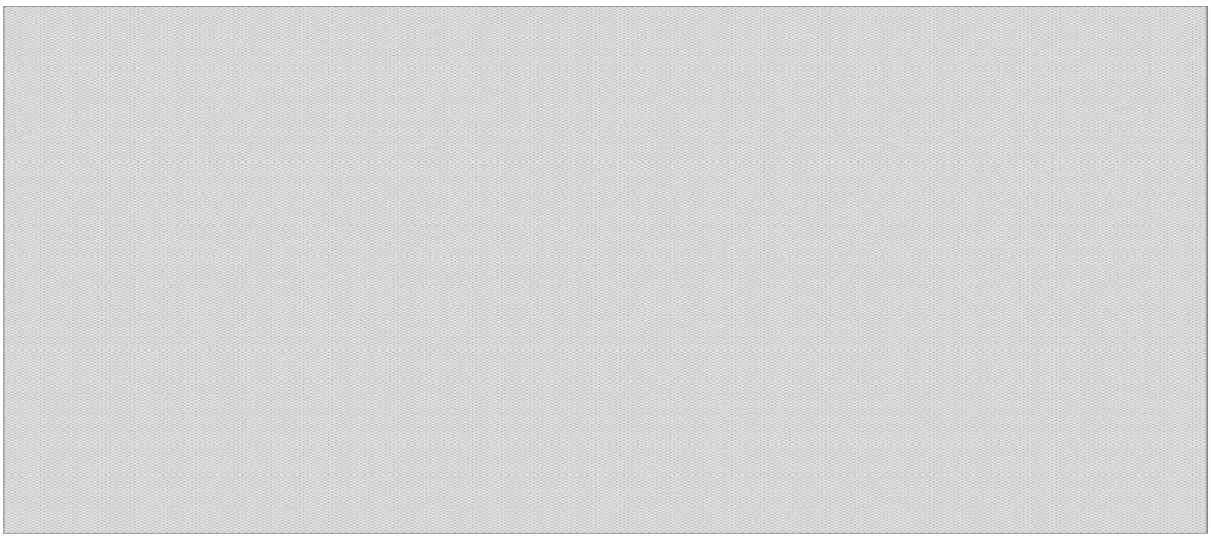
시장 현황 및 전망

- **(해외)** 세계 시장은 '15년 450억파운드(593억$)에서 '20년에는 1,290억파운드(1,699억$)로 성장 전망(런던앤파트너스, 에듀테크UK, 2015)
  - 기술개발 관련 투자는 '12년 9.6억 달러 규모에서 '16년 23.4억달러 규모로 급격히 성장 중*
    * 국가별로 에듀테크 펀딩비중은 미국이 68%로 압도적인 1위로 나타나며 중국 20%, 인도 3%로 편중이 매우 심함
  - 관련 시장으로 세계 이러닝 시장은 '15년 1,273억달러에서 '22년에는 2,415억 달러의 규모로 성장할 예정(GIA, '16년)
  - 미국, 영국 등 교육기술 선진국을 중심으로 교육과 첨단 기술을 접목하고 있으며 에듀테크(Edutech)에 대한 논의가 활발히 진행 중



[그림 3-3] 세계 에듀테크 투자현황(단위: 백만달러, %)

- **(국내)** 국내 시장은 아직 형성단계이며 이제 투자가 진행되는 상황
  - 국내의 에듀테크 관련 총 투자규모는 '10년~'16년까지 총 900억원에 이르며 ST&COMPANY, SMART STUDY, Knowre 등에 투자비가 집중화되는 현상이 나타남
  - 투자분야는 대부분 외국어, 수학 등 사교육 분야에 편중
  - '16년 이후 기술에 대한 투자는 머신러닝, 빅데이터분석, 소셜네트워크, IoT, 클라우드, 프로그램개발 등으로 변화*
    * 종전까지는 3D그래픽/애니메이션, 검색, 게임개발, 이미지/영상제작 등은 투자가 활발히 나타남(https://bruch.co.kr)



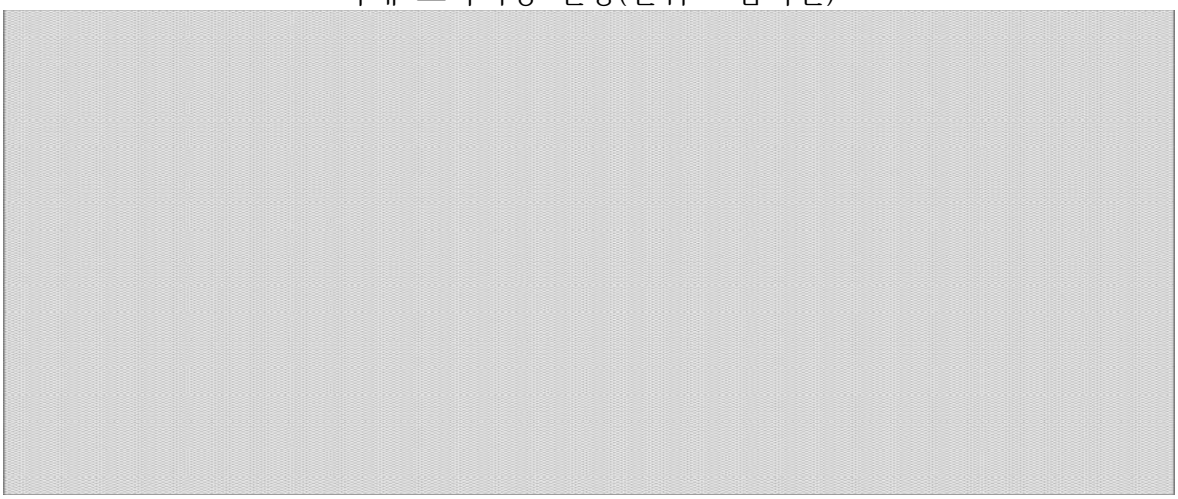
[그림 3-4] 국내 에듀테크 투자현황(단위: 억원)

[참고 2] 가계교육지출비 vs 이러닝 매출액 (국내)

◐ 가계교육지출비는 ’11년 2.4조원으로 연평균 9.2%로 고성장하여 ’15년 3.5조원에 도달

- 교육 지출 대비 이러닝 매출액 비중은 ’11년 5.7%에서 ’15년 8.8%로 점차 증대되고 있으며 교육을 위한 학습방법 중 하나로써 중요성이 증가하고 있는 상황
- 국내의 가계교육지출비가 평균 40.8조원(’11년~’15년)인 점을 감안 했을 때 국내 이러닝 매출액은 가계교육비 대비 평균 7.3% 수준

< 국내 교육시장 현황(단위 : 십억원) >



주) 민간분야 자료만 사용하였으며 정부지출, 기업부문까지 고려되면 실제 국내 교육서비스 시장은 상기 자료수치보다 더 클 것으로 예상

자료 : 통계청(부문별 가계지출), 산업통상자원부(2015년 이러닝 산업 실태조사)를 이용해 작성

주요 업체 현황

- **(해외)** 크게 학습 에이전트 기술, 학습데이터분석 및 맞춤형 서비스기술, 공간인식기반 체험형 증강현실 기술 등과 관련해 주요업체가 활동 중
  - **(학습에이전트기술)** Blackboard, Moodle, edmode 등이 활동 중
    ※ Blackboard : 설치형 LMS(Learning Management System) 기업이며 오픈소스 기반 CourseSite 개설을 통해 시장지배력을 공고히 확보하고 있는 중
    ※ Moodle : 오픈 소스 기반 LMS를 제공하고 있으며 국내외 대학기관들이 Moodle을 이용해 LMS 시스템 구축을 완료
    ※ edmode : 최근 MOOCs의 이슈로 만들어진 Social LMS로 구글, 애플 등과 같이 LMS 플랫폼을 제공하고 생태계를 구축해 앱수수료, 광고 등을 통한 수익모델을 구축하고 있음
  - **(학습데이터분석 및 맞춤형서비스기술)** NoRedInk, MCGRAW-HILL Education 등이 학습데이터분석 및 맞춤형서비스를 제공 중
    ※ NoRedInk : 온라인 웹기반의 언어학습 플렛폼 제공 중이며 개인별 학습데이터를 분석해 숙련도를 추적하여 맞춤형 학습을 할 수 있도록 유도 중
    ※ MCGRAW-HILL : 해외 주요 출판사인 MCGRAW-HILL은 스마트북을 공개하고 전자책 형태의 플랫폼 내에서 맞춤형 학습서비스를 제공 중
  - **(공간인식기반 체험형 증강현실기술)** Relentless, SCE Japan Studio 등이 관련 시스템 기술을 보유 중
    ※ Relentless : 증강 현실 기반 인터랙티브 TV 프로그램인 Kinet Nat Geo TV를 지원 중
    ※ SCE Japan Studio : The Playroom 인터랙션 게임을 제공 중
- **(국내)** 에듀테크 기술관련 시스템 및 서비스 보유 업체로 클래스팅 유비온, 테크빌, 클루빌, 디지털대성 등이 있음
  - **(클래스팅)** 학급 운영과 학습 자료 공유에 특화된 Social LMS인 “Classting”을 개발
    * ’15년 8월 기준 총 20만개의 클래스가 개설되었고 총 180만명 이상의 사용자를 확보, 일본시장 진출 등의 성과가 나타남
  - **(테크빌)** ‘샘빌’은 플립 러닝 지원 플랫폼으로 SNS 연동, 교육과정관리, 수강관리 등의 기능을 지원
  - **(유비온)** ’13년 모바일 기반 오픈소스 학습 플랫폼인 코스모스를 개발하여 1서울대, 카이스트, 이화여대 등 국내 대학에 보급
  - **(클루빌)** 가상 아바타를 이용한 영어학습시스템을 청담러닝, NCSoft 등에 제공 중
  - **(디지털대성)** 중학교 수학 교육 콘텐츠인 “마하S”를 제공 중이며 틀린 문제의 숫자를 바꾸어 다시 풀게 하는 맞춤학습을 제공

[표 3-4] 기술 분류별 국내외 주요업체 현황

구분	내용		
기술분류	공간 인식 기반 체험형 증강현실	학습분석	학습에이전트
주요서비스 및 기술	몰입형 영어학습 서비스, 인터렉티브 TV 프로그램 및 체험형 학습게임, 공간/객체의 인식/변형/정합 기술, See-through HMD	학습자 맞춤형 분석 기술, 에튜테인먼트 기술, 학습 콘텐츠	통합 교육 플랫폼, 오픈소스/Social LMS, 빅데이터분석기술, 플립러닝기술
해외 기업	Relentless, SCE, Japan Studio, EonVision, Microsoft	NoRedInk, MCGRAW-HILL Education, Smart Sparrow, DouLingo, Enome, Course Hero, Knowre	BlackBoard, Desire2Learn, edmode, LORE, Class Twist, Skillsoft, Cornerstone onDemand, Interactyx
국내 기업	MAXST, 클루빌, 다림비젼	MPDA Math, 노리, 디지털대성	클래스팅, 유비온, 테크빌

출처 : 중소기업청(2016)

주요 국가별 정책 현황

- 주요 국가들은 교육제도에 ICT 기술 및 인프라 접목에 대한 정책적 기조가 확연히 나타나는 중
  - 대부분의 주요 국가들은 교육 IT 서비스 및 콘텐츠를 도입 준비를 위해 학교 시설의 환경 정비를 우선적으로 실행 중
  - 유럽을 중심으로 코딩교육을 초등학교에서부터 실시하는 교육 과정을 신설 중이며 국내에서도 '18년부터 도입 예정
  - 중국은 국가 교육 개혁을 위한 장기적이며 체계적인 정책기조를 수립하고 추진 중

국가별 세부 정책 동향

- (미국) 미래지향적 교육기술 기반환경 조성을 위해 「10년 국가 교육기술계획인 'National Education Technology Plan (NETP 2010)」발표 이후 지속적인 관련 정책을 마련 및 추진 중

- 그밖에 공교육 강화 법안, 산업단지 육성, 각종 프로그램 운영 등의 다양한 정책을 시행 중이며 다양한 펀딩이 발현 중
- 「아동낙오방지법(No Child Left Behind)」을 만들고 스마트 기기를 이용해 교육할 수 있는 환경 마련을 진행 중
- 로스엔젤레스, 시카고, 뉴욕 등 주요 도시에 교육 관련 산업단지를 육성 중이며, 모바일 기반 교육용 게임 개발이 지속적으로 성장 중
- GCSP(Grand Challenge Scholars Program), 칸랩스쿨(Khan Lab School), 알트스쿨(Alt School), 미네르바 스쿨 등 다양한 프로그램이 운영 중

[표 3-5] 미국 각주별 다양한 교육 프로젝트 활동현황

구분	현황
조지아 텍사스 버지니아	• BYOD 성공적인 운영 - 안정적인 네트워크 기반 구축 - 기기활용 가이드라인 확립 - 학생 및 학부모에게 정확한 정보전달
유타	• 학생 성취도 백팩(Student Achievement Backpack) 프로그램 추진
플로리다	• MOOC를 통한 온라인 학습 옵션 확대
켄터키	• 2013-2018 켄터키 교육 테크놀로지 시스템 마스터플랜(KETS) 발표
텍사스	• 클라인 독립 학구 - '06년부터 1:1 학습 프로그램 시행 - 최근 학습 성과 파악을 위한 전담팀 마련 - 새로운 1:1 모델을 찾기 위한 교육자 커뮤니티 신설

출처 : 한국이러닝산업협회(2015)

◐ (EU) EU소속 국가들은 주로 SW 개발 교육을 정규과정으로 채택하는 형태로 IT와 교육의 융합을 준비하는 중

- EC(European Commission)는 “유럽 코드 주간(EU Code Week)”를 운영을 통해 학생들의 프로그램언어를 이용한 코딩 능력 개발을 장려*

  * 유러피안 스쿨넷(European Schoolnet) 코딩 캠프 개최, 코딩 워크숍의 세션 운영, 코딩자원 소개 등 유럽 학생들의 코딩 학습을 지원 중

- 코딩교육이 초등학교 교육과정에 의무화*하거나 선택적 도입** 국가로 나뉘는 상황이며, 대부분의 유럽국가는 학교 교과과정에 코딩교육을 도입하는 방안에 지지 입장을 표명

  * 코딩교육 의무 국가 : 영국, 불가리아, 사이프러스, 체코, 그리스, 폴란드, 포르투갈 등

  ** 선택적 코딩교육 국가 : 덴마크, 에스토니아, 아일랜드, 이태리, 리투아니아, 독일 등

- EU code week('14년 10월 11일~17일)기간 중 European Coding Initiative의 일환으로, 초등학교에서의 코딩교육 의무화를 촉구('14년 10월)

◐ (영국) 과학혁신분야 성장계획을 통해 융합인재양성 정책을 다양하게 실행 중

- ’11년 12월 “21세기 학교 프로그램(21st Century School Programme)”을 발표하고 학교시설의 현대화를 시작으로 교육에 기술을 융합하는 정책을 추진 중
  * 세계 최초로 초중등 과정에서 코딩 교육을 의무화하고 관련 과목을 개설하여 정규 과목으로 편성 및 운용 중
- 관련 분야에 29억 파운드를 투자 중이며, 8대 주요기술 선정 등 구체적인 정책 가이드라인을 제공
- 공학교육 혁신을 위한 보고서, 기능인력 양성을 위한 5개 국립대학 신설, 산업견습생 프로그램, 에듀테크UK 협의체 마련, 유소년 코딩교육 체계 마련 등 다양하게 진행 중

◐ (일본) 문무과학성 중심으로 「교육의 IT화를 위한 환경정비 4개년 계획」을 발표하고 다양한 정책과제를 발굴*추진 중

  * IT 교육 환경 구축을 위해 교육용 컴퓨터, 전자칠판, 실물투영기, 인터넷 서비스 지원 등의 교육용 IT 인프라 구축과 학습용 소프트웨어 구비, ICT 지원인력 배치 등을 추진 중

- 3년(2014~2016년)에 걸쳐 100곳의 지역거점학교를 선정하고 디지털교과서를 활용한 수업을 실시
- 규제개혁회의에서 ’13년 디지털교과서를 교과용으로 인정하는 방침을 세우고 ’14년까지 디지털교과서의 지위 확립 및 검정 제도와 관련해 정리를 마침
- ’19년까지 전국 모든 학교에 무선랜 설치에 총 100억엔을 투입

◐ (중국) ’11년 「국가 중장기 교육 개혁과 발전계획」과 「교육 정보화 10년 발전계획」 등을 마련하고 장기적 관점에서 교육 IT 환경을 구축 중

- 교육수요*에 의해 시장규모나 투자가 급격하게 늘고 있는 상황
  * 최근 1가구 1자녀 정책이 폐지되고 1가구 2자녀까지 허용함에 따라 시장에서 교육수요가 급격하게 증가할 전망(2016)

  ※ 중국 온라인 교육시장은 전 세계 에듀테크 투자의 40% 수준에 달함(중소기업청, 2016)
- 중국 온라인 교육 서비스는 주요 인터넷 서비스 업체(바이두, 알리바바, 텐센트 등)에 의해 주도되고 있는 상황
- 중국의 「교육 정보화 10년 발전 계획」은 2개의 구조로 구성
  ① 2011~2015년 : 교육 정보 기초 설비(시설)의 전면 구축과 교육 정보화 자원 전면 이용 실현
  ② 2015~2020년 : 교육 정보화 수준을 선진국 수준으로 도약시키며 정보기술과 교육의 전면적이고 심층적인 융합을 실현

[표 3-6] 교육 정보화 10년 발전 세부계획

분 류	2020년 목표
기초교육	• 전국 초·중·고등학교 인터넷 설비와 학생 6명당 컴퓨터 한 대를 보급하고 교사 개인 컴퓨터 보급 실현 • 모든 미취학 아동 교육시설에 멀티미디어 교실 배치와 관리·제어 가능한 안전하고 친환경적인 디지털 교정 건설
직업교육	• 전국 각지의 각종 직업학교에 인터넷 설비를 보급해 학습 전반에 활용하고, 멀티미디어 교실 및 IT관리 프로그램을 보급 • 모든 핵심 과목의 디지털 교육 자료를 개발해 시뮬레이션과 인터넷 직업교육 시스템을 전면 보급하며, 교수들의 IT 활용 교육을 참여를 의무화 함.
고등교육	• 대학과 대학원 내 인터넷 설비를 보강하며 모든 교실에 지능형 단말장치를 배치 • 전국 대학과 대학원에 인터넷 수업을 개설해 80%의 과목에 온라인과 오프라인을 혼합한 교육을 실시 • 매 교육 기관은 전자 교무시스템을 건립하고 교내 전문 정보화 관리 부서를 설립해 전체 교직원 수의 4%의 인원을 배치
평생교육 (성인교육)	• 전국 평생교육 기구의 자료와 서비스 시스템을 구축하며, 온라인 과목의 강의 평가 기준을 도입해 강의 품질을 제고 • 세계 일류의 개방대학(방송과 통신을 주매체(主媒體)로 삼는 고등교육 기관. 가정에서, 또는 직장생활을 하면서 일반대학교와 같은 수준과 내용을 교육하는 기관) 건설과 인터넷-위성 연동률 90% 달성
교육관리	• 데이터 연동을 통한 총괄 데이터 정보 관리 실현. 교육 관리 업무 프로세스 전산화 비율을 90%까지 제고

출처 : 중화인민공화국 교육부

◐ (국내) '06년부터 장기적 관점에서 이러닝산업발전을 위한 기본계획안을 마련하고 정부주도하(교육부, 산업부, 미래부 등) 추진 중

- 이러닝 주요 내용으로는 이러닝산업 생태계 개선, 기술혁신 역량강화와 창의적 인재양성, 이러닝 활용 촉진, 이러닝산업 해외진출 확대 등으로 구성
- 적극적인 정책 추진으로 인한 주요 성과로 시장규모의 확대, 이러닝 이용률 상승, 제도마련, 교육지원 등을 꼽음(이러닝산업협회, 2016)
- 최근 인공지능이나 가상현실 등 첨단 IT 기술을 접목*해 새로운 시장창출을 위한 산업으로 육성키 위한 내용을 중심으로 하는 3차 기본계획을 발표

  * 이러닝 유망 분야로 맞춤형 교육(빅데티어 이용한 개인 맞춤형 이러닝 서비스), 실감형 학습(VR/AR 기술 활용), 소셜 러닝(소셜미디어 활용) 등을 예시로 제시

Ⅱ 교육 IDX 수요 및 파급효과 분석

【1】 문제점 및 IDX 수요 도출

교육 현장 : '개인 맞춤형 학습 환경' 제공

- (문제점) 개인별로 상이한 학습 수준과 그에 따른 학습목표를 맞춤형으로 진행해야할 필요성 제기
  - 여전히 교사와 학생 간 비율차이가 존재함에 따라 1:1 학습이 어려운 상황*
    * '00년부터 꾸준히 비율차이가 줄어 '17년에는 초중고의 교원1인당 학생수가 14.5명(초등), 12.7명(중등), 12.4명(고등)에 이르나 평균 학급당 학생 수는 '15년 기준 전기중등교육이 30명 이상, 초등교육이 20명 이상으로 나타남
  - 현재 수준별 학습을 위해서는 이동수업을 할 수 밖에 없는 상황
    * 교과교실제라는 이름으로 여전히 중·고등학교에서 수준별 이동수업을 실시 중이며, 성적으로 반을 배치함에 따라 학생들간 위화감 조성 및 차별 문제를 야기 중
  - 평생학습 관점에서 나이, 학력 등에 관계없이 교육을 받기 위한 방법이 필요
    ※ 맞춤형 평생교육 컨설팅 결과보고서에 따르면 인력확보, 관리시스템, 물리적 운용 등에 관한 문제점(교육자의 재능기부요구, 평생교육기관 간 연계시스템 미흡, 프로그램 간 학습 활동의 연속성 부재 등)을 제시(인천평생교육진흥원, 2016)

- (IDX 수요 도출) 개인별 맞춤형 학습 지원 AI 조교 서비스 제공
  - 학습자의 학습수준 분석·수준별 콘텐츠 추천 등 개별화된 학습과정 제공
    ※ 교원 확보, 수준별 이동학습, 평생학습 인력확보 등에 대한 문제를 해결할 수 있으며, 가구별 교육비를 절감할 수 있을 것으로 전망
  - 맞춤형 학습의 전단계로써 디지털교과서 제작 과목(영어, 사회, 과학)과 시범학교 선정* 및 확산** 중
    * 2018년부터 초중고에 디지털교과서 전면도입 계획안 발표(교육부, 2016 개정 교육과정에 따른 초·중등학교 디지털교과서 국·검정안)
    ** 교과부의 교내 인프라 환경 구축사업 및 디지털교과서 제작 일정과 연계해 적용 지역, 대상학년 확대, 타 교과서 적용 추진 등

가정 공간 : '지능형·적응형 로봇 기반 학습 및 보호 환경' 제공

◐ (문제점) 가구 내 소득주체의 다양화로 인한 교육 문제(맞벌이), 장애아 교육, 노령인구관리 등과 같은 사회적 문제의 지속적 대두

- 부부 맞벌이로 인해 자녀를 낳고 교육하거나 유대관계를 형성하는 절대적 시간의 부재로 다양한 사회문제가 출현·증가되는 상황*

  * 촉법소년의 중범죄화(경찰청, 2014), 가출청소년 증가(경찰청, 2010), 학교 부적응으로 인한 학업중단(교육부, 2014) 등 다양한 문제가 대두되며 이에 대한 원인을 가정환경, 사회환경, 학교환경, 자기절제 등의 요인으로 설명(이동임, 2012)

  ※ 부모의 무관심과 부모와 자식 간의 갈등이 많을수록 가출할 가능성이 높고, 가출 후에는 생계를 위해 범죄에 가담할 확률이 높아짐(임지영, 2011)

- 님비 현상으로 인해 특수학교 수를 충분히 확보하지 못하고 있으며 자폐아, 서번트증후근 등 장애아에 대한 전문 교육이 실시되기 어려운 상황

- 최근 인구의 고령화로 인한 사회적 문제가 대두되고 있으며 이를 IT 기술을 이용해 해결하는 방안들이 나타나는 중*

  * 치매, 우울증, 성인병 등 고령화로 인한 의료비 및 인력확보 문제를 해결하기 위해 로봇이 대안으로 제기되고 있으며 일본은 이미 파로(노인 심리치료로봇)를 출시해 보급 중

  ※ 그밖에 가정용 로봇을 통해 고독사 예방, 평생교육 추진 등의 활용성이 부각 중

◐ (IDX 수요 도출) 가정용 교육 서비스 로봇(가정교사 로봇) 개발 및 도입

- 생애주기별 가정교사로봇 개발보급하여 부모의 역할을 일부 나누어 수행함으로써 일과 가정을 병행하더라도 사회문제를 최적화할 수 있는 방안 마련

  ※ 맞벌이로 인해 발생하는 가정교육의 시간적 부족 문제를 해결할 수 있으며, 갈등 발생 시 중간자 역할도 가능

- 공교육의 기능 감소현상에 있어* 국가의 역할이 집체교육에서 개인별 교육 관리로 변화할 필요가 있으며 로봇을 통해 진행 가능

  * 「더퓨처리스트」에 따르면 '30년에 사라질 10가지 중 하나로 교실, 교사 등 공교육 시스템을 꼽고 있으며 집단교육이 사라지고 개인화된 교육이 될 것으로 예측(세계미래학회, 2013)

  ※ 신체적·정신적 장애가 있더라도 가정 내에서 교육/관리를 가능케하는 역할도 도모

- 가정용 로봇은 개인·독신화로 인한 독거인을 보호·관리하는 역할도 수행

  ※ 개인의 고질병을 관리하고 필요시 병원, 경찰, 소방 등에 즉각적인 연락을 취할 수 있는 형태

산업 현장 : '현장 수요 기반 체험형 학습 및 훈련 환경' 제공

- (문제점) 산업현장에서의 교육훈련은 기술 및 인력수요의 불일치, 재직자 숙련도 격차로 인한 교육과정 상 문제, 훈련성과부실, 부정수급의 문제, 실습생에 대한 처우 문제 등 여러 문제가 상존
  - 직업훈련에 가장 큰 걸림돌은 비용*과 난이도** 문제이며 이를 해결하기 위한 다양한 정책이 진행 중이나 그 성과는 미비한 상황
    * 정부의 고용보험기금을 재원으로 매년 1조원 이상의 직업교육(실업자, 재직자 모두 포함)을 실시하고 있으나 계좌제 방식의 부작용이 나타남
      ① 훈련 수요와 기업 수요의 불일치 및 불필요한 계좌발급 : 훈련생의 수용와 기업의 구인수요 간의 불일치, 취업의사 없는 비경제활동 인구에 계좌발급 등
      ② 훈련 품질 저하 : 훈련기관의 영세화, 불확실성으로 인한 품질하락, 훈련교사의 질적 저하, 형식적인 훈련상담 및 관리 등
    ** 재직자 및 실업자에 대한 참가율은 증가중이고 최근 사무직과 서비스분야 중심으로 대상 훈련이 확대됨에 따라 전문성을 높이는 고급과정의 편성이 낮음
  - 현장실습생(미성년자)과 같은 사회적 약자들은 산업현장노동착취, 산업재해 등에 노출되어 있으며 이는 학교 내에서 관련 교육을 제공해주지 못하는 것에 기인함에 따라 이를 보완할 교육과정 개설이 필요
- (IDX 수요 도출) 실감 콘텐츠 개발을 통해 체험형 전문 교육 시뮬레이터 공급
  - 고위험·고숙련 인재가 필요한 분야(원전, 선반, 전기, 설계 등)에 현장 실무 경험을 가상으로 체험 가능하도록 시나리오 기반의 실습실 제작, 설치·운영
    ※ 반복실수 교정지도 및 돌발 상황 시나리오를 추가해 훈련 효과성 극대화
  - 특정 실내공간 내에 대화면, HMD, 스마트글래스 등의 장비와 다양한 훈련 콘텐츠를 이용해 시뮬레이터를 구성
  - 가상 및 증강현실 기술을 활용해 시뮬레이션 기능을 이미 스포츠 훈련(미식축구, 농구, 야구 등)에 적용 중*
    * 사이버 스포츠 레슨, 러닝 시뮬레이터, 사이버 휘트니스, 체력진단 시뮬레이션 등
  - 부상, 산업재해 등으로 인한 재활교육도 시뮬레이터를 통해 지원 가능

온오프 연계 : '가상증강 실감교육 환경' 제공

◐ (문제점) 야외수업에 있어 장소섭외, 현장학습 관련 정보수집, 결과보고서 작성 등 부수적 업무의 가중화로 인한 문제

- 생물, 지구과학 등의 과목은 야외에서 자연환경 자체의 관찰을 수행함으로써 자발적 학습동기, 관찰력 등 학습효과를 제고한다고 보는 견해*가 다수
  * 이상교(1985), 서승조(1990), 송시태(2003) 등에 의하면 초·중등 및 대학 등 대상에 따라 지질, 지구과학, 생물의 분야에서 수준별 현장학습이 중요하다고 주장
- 야외학습 프로그램 구성에 있어 교사의 역할이 중요하며 연구절차상 적합한 구성을 하였는가에 대한 기준이 모호한 문제*가 존재
  ※ 연구절차는 준비단계, 야외학습단계, 요약단계로 구분되며 보다 세부적으로는 교육과정 분석→교육과정 상에서 야외학습을 실시할 개념 및 자세한 학습내용 파악→야외학습장소의 선정→야외학습경로 지정→교수학습보조물 개발 등의 과정을 거침
  * 교사 1인이 야외수업을 위해 필요한 전 과정을 소화해야하며 시간적·물리적(장소 접근성) 한계성으로 인해 다양한 야외수업을 할 수 없는 문제
- 학교 내의 문제*와 학교외 환경 문제**로 인해 야외학습에 어려움이 존재하고 있으며 이를 해결하기 위한 방안이 필요한 실정
  * 다인수의 학급, 실험실습기구의 부족, 교수·학습자료의 부족, 성적향상에 몰두하는 경향성 등의 학교 내 열악한 환경과 성적우선에 대한 고정관념의 문제 등
  ** 최근 미세먼지와 같은 환경적 요인 등을 이유로 실외수업 단축 및 금지하는 등 외부 환경요인에 종속되는 경향성 존재

◐ (IDX 수요 도출) 가상·증강 기술을 이용한 온오프라인 연계 시스템 보급

- 현장학습이 필요하나 환경적·물리적으로 어려운 경우 가상·증강 기술을 활용해 교실 내에서도 유사학습이 이루어질 수 있도록 하는 시스템 개발 및 보급
- 현장학습의 질적 제고 및 교사 자료준비의 부담감 완화 위해 현장학습 시 스마트 글래스나 HMD, 스마트폰 등의 기기를 통해 관련 정보를 바로 제공
- 다양한 현장학습 환경 마련으로 학생 및 교사의 학습 만족도 제고 가능

【2】 교육 IDX 파급효과 분석

종합

- 사교육 가중화로 인한 교육비 부담, 학습자의 수준차이 발생, 산업훈련 시 고비용, 숙련도, 사고위험 등의 문제점을 IT 기술을 통해 해결 가능
  - **(교육현장)** 특별히 사교육을 하지 않더라도 공교육 차원에서 개인별 수준 맞춤 학습을 통해 학습수준을 제고시킬 전망
  - **(가정공간)** 교육용 로봇뿐만 아니라 작업현장에서 로봇이 사용됨에 따라 가구당 가정내에서 기거하는 시간이 늘어남에 따라 촉법소년을 비롯한 비행청소년을 줄이는 효과를 통해 사회적 문제 해결 가능
  - **(산업응용)** 산업현장에서 난이도와 개인수준에 맞춘 훈련을 실가상 통합운용을 통해 비용과 시간을 절약하고 고난의도 기술자 양성에 기여 가능
- 여러 학습도구의 발생으로 교육 기회의 다양성 확보
  - 현재 교실내에서 이루어지는 1대 다수의 수업방식이 보편화되어 있으나 향후 교실 안팎 및 가정 내에서 다양한 수업방식이 나타날 것으로 기대
  - 최근에 이미 이런 경향성이 반영된 다양한 교수법이 나타나는 상황이며, 다양한 교수법의 등장으로 현재 교육체계가 변화될 가능성 농후

※ 적응학습, 개인화 학습, 혼합학습, 플립러닝, 프로젝트 기반 학습, 소셜러닝, 대규모 온라인 학습(MOOC) 등 IT 기술을 접목한 다양한 새로운 개념의 학습모델이 부상 중

- 새로운 성장동력으로써 교육산업의 역할이 점차 증대될 전망
  - 다양한 스마트 기기와 교육용 로봇의 보급, 신규 교육 서비스 등장 등으로 교육산업은 과거 인적네트워크 기반에서 자본네트워크 기반으로 이동하고 여러 시장 형성 요소를 근간으로 한 산업으로 재편 가능성 확대

개인 맞춤형 학습 환경 : 교육현장

- 교육대상 확대, 교육격차 완화, 사교육비 절감 등의 사회적 문제를 해소뿐만 아니라 관련 HW 및 SW 시장성장도 가능
  - 공교육이 점차 개인화 학습으로 1대 1의 형태의 수업방식 변화로 교육격차 완화나 사교육비*를 절감시킬 수 있는 파급효과를 예상

    * 사교육비 총액은 약 18조 1천억원, 학생 1인당 월평균 사교육비는 25만 6천원 수준에 달하며 국영수 과목이 19만 1천원으로 대부분의 사교육비를 차지
  - 학교 부적응의 대부분은 학습수준 차이에 따른 관심부족에 기인하며 이에 대해 공

교육이 해결할 수 있는 가능성 발생

- 디지털 교과서 및 칠판, 교육용 프로젝터, 무선랜 등 네트워크 장비, 클라우드 서비스 등 다양한 IT 영역과 관련된 제품 및 서비스가 발생 가능

	파급효과
	. 학습력 제고 . 사교육비 감소 . 시간과 공간의 제약 사라짐 . 콘텐츠/소프트웨어 및 장비산업 육성

[그림 3-5] 교육에서의 ICT 기반 해결 과제 및 방안 : 교육현장

지능형·적응형 교육 로봇 : 가정

- 가정교육 기능 강화 및 새로운 산업으로써 육성기회 확보
  - 촉법소년 및 비행청소년 등의 가정내 불화에 기인해 발생하는 문제를 완화 가능하며 학교외 수업을 가정내에서 수용 가능
  - 장애우 뿐만 아니라 독거인들을 관리 및 치료교육을 가정내에서 가능케 함에 따라 장애학교설립, 고독사, 치매 등의 사회문제를 해결 가능
  - 다양한 가정교사 로봇 및 서비스가 등장함에 따라 새로운 교육산업으로써 성장할 기회 제공

	파급효과
	. 취약자(아이, 노인) 돌봄 기능 제공 . 질병 장애를 가정내에서 치료 및 교육이 가능 . 로봇을 비롯해 관련 소프트웨어 장비 등의 산업 활성화 가능

[그림 3-6] 교육에서의 ICT 기반 해결 과제 및 방안 : 가정공간

현장 수요 기반 체험형 학습 : 산업현장

- 우수한 기술인력 확보 및 관련 파생 교육 산업 육성
  - 교육기회가 기업의 규모와 비용에 비례했던 과거에 비해 저렴한 비용과 교육시간활용의 극대화로 비교적 짧은 시간 내에 우수한 기술인력 확보 가능
  - 기존의 수동적이며 교육기회가 적은 체험 교육이 적극적이고 다양한 가상 체험기회를 가질 수 있도록 변화가 예상
  - 제조업뿐만 아니라 서비스업에서 요구하는 직업훈련을 뒷받침하기 위해 여러 가지 훈련 콘텐츠가 발생 가능

	파급효과
	. 숙련자 확보 교육이 용이해짐 - 고위험, 고비용, 긴 교육시간 등의 제약조건을 해결 가능 . 서비스 분야에도 적용 가능 - 항공, 물류, 차량정비 등

[그림 3-7] 교육에서의 ICT 기반 해결 과제 및 방안 : 산업응용

증강교육 : 온오프 연계

- 다양한 온오프 연계교육 등장으로 교육의 다양성 및 질적 향상 제고
  - 온오프 연계교육의 초기 서비스는 초중고 학생을 대상으로 개발하고 추후 산업현장으로 확대함으로써 영역의 다양성 확보 가능
  - 실가상 통합 현장교육 콘텐츠 양성을 통해 새로운 교육법 발굴 및 교육 산업 관련 제품 및 서비스 경쟁력을 고취

	파급효과
	. 가상현실로 시공간을 초월한 인문학 교육 가능 . 증강현실로 현장 정보를 실시간 확보함으로써 교육 효율성 제고

[그림 3-8] 교육에서의 ICT 기반 해결 과제 및 방안 : 온오프 연계

Ⅲ IDX 추진의 가능 미래상

종합

- 4차산업 혁명을 위한 IDX 추진은 교육뿐만 아니라 다양한 산업영역에서도 발생하므로 미래의 교육방향성은 현재와는 다른 양상으로 전개될 가능성 존재
  - IT 기술의 진보와 여러 산업영역과의 융합으로 실제 관련 지식을 보유 하지 않더라도 주변 기술 및 제품/서비스 등을 활용하여 누구나 창조물(제품 및 서비스)을 만들어내는 환경으로의 변화가 나타날 수 있음
  - 즉, 인간은 여러 가지 툴이 있는 가운데 문제 해결을 위해 어떤 툴을 조합하여 해결할 것인가에 대해 고민하는 형태가 됨에 따라 관련 교육이 그에 적합한 형태로 변화할 것으로 예상

    ※ 최근 컴퓨터 프로그램의 코딩교육으로 관련 지식이 축적되고 미래 인공지능, 로봇 등의 기술과 융합함에 따라 코딩교육을 받지 않더라도 특정 키워드를 주면 알아서 프로그램이 만들어지는 미래상을 그려볼 때 현재 필요한 교육과정이 미래에는 사라질 수 있음
  - 먼 미래로 이어지는 과도기적 상황인 지금 향후 10년 내에 변화될 교육 시스템의 미래상을 그려봄으로써 대응방향 모색 가능

교육 IDX 분야별 미래상

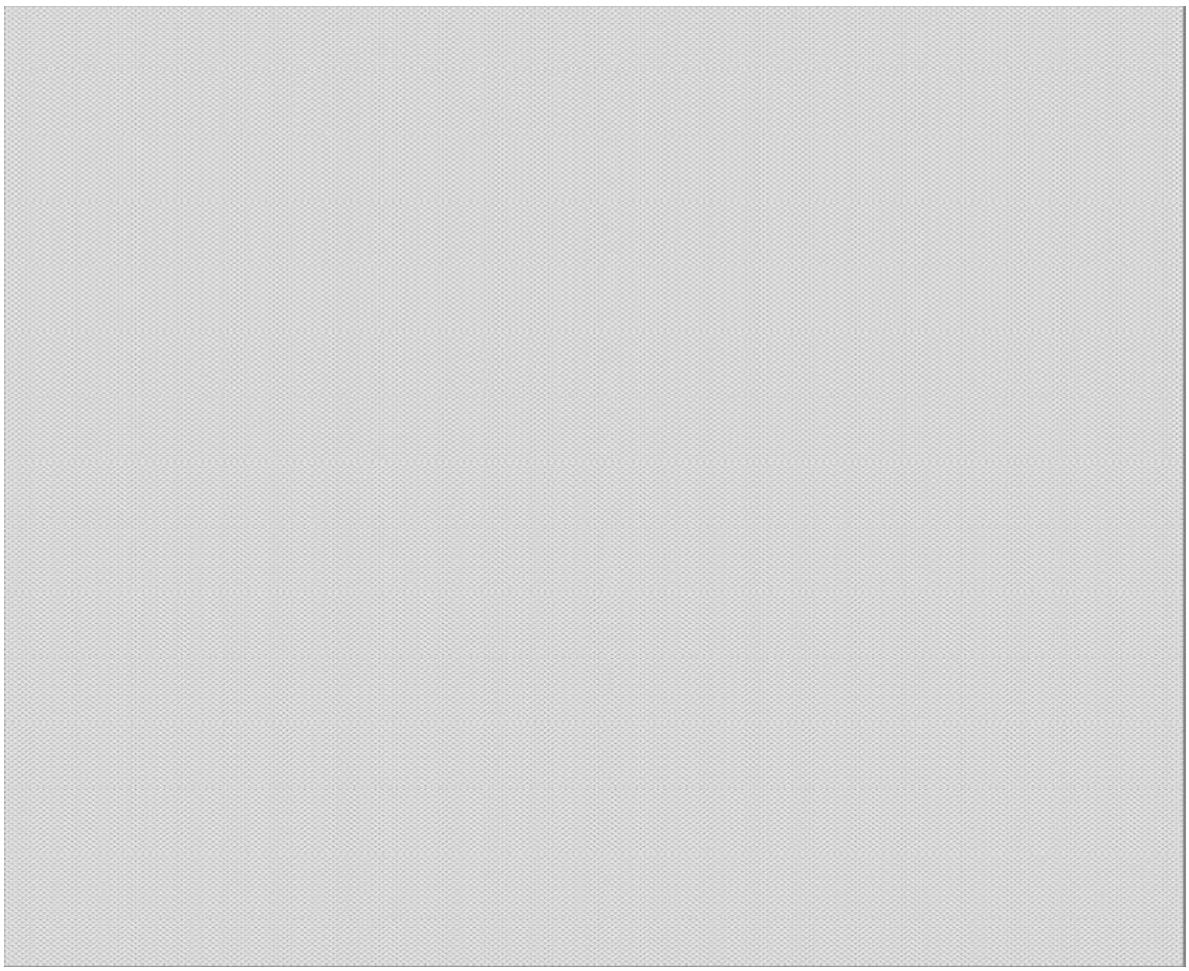
- (교육 현장) 단기에는 교육 IT 인프라 형성에 주력할 것으로 보이며, 장기로 가면 개인 맞춤형 학습이 주요 교육서비스로 자리 잡을 전망
  - **(단기)** 교육IDX를 위한 디지털교과서 및 디지털칠판 등의 교보재 보급, 무선랜 및 클라우드 서버 구축 등이 주요 IT 인프라로 형성되고 다양한 교육 관련 데이터가 축적되는 시기
  - **(중기)** 교실 내 다양한 센서가 구축되고 인지능력이 발달됨에 따라 학습자의 태도를 분석하고 피드백 하는 기능이 제공될 것으로 기대
  - **(장기)** 인공지능 기술의 발달과 클라우드 서비스가 일반화됨에 따라 시공간을 초월해 교육과 학습을 할 수 있는 환경으로 변화할 전망
- (가정 공간) 인공지능로봇의 보급으로 가정 내에서 다양한 기능을 처리할 것으로 예상
  - **(단기)** 서비스용 로봇이 가정 내 점차 도입될 것으로 보이며, 교육적 내용을 포함한 게임형태의 흥미유발형 콘텐츠가 주를 이룰 것으로 예상
  - **(중기)** 이동형 소형로봇이 보급되고 개인비서 형태로 사용자가 원하는 일반적

인 정보를 제공하는 수준으로 변화할 것으로 예상

- **(장기)** 로봇 및 인공지능 기술 발달로 가정 및 개인교사, 장애치료, 노인관리 등 다양한 기능을 가정 내에서도 실현 가능

● (산업 현장 및 온오프 연계) 실감 콘텐츠를 이용해 직업훈련 및 교육을 실현함으로써 다양한 산업영역을 비롯해 현장학습 등에 활용

- **(단기)** 교육용 실감 콘텐츠를 개발하기 위해 다양한 교육현장을 모델링 하여 데이터 형태로 구축
- **(중기)** 성숙화된 가상증강기술과 모델링 자료를 활용해 풍부한 실감 교육콘텐츠 보급
- **(장기)** 교육현장에서 산업현장으로의 이동하여 다양한 실감 콘텐츠를 활용한 교육 및 훈련을 실시



[그림 3-9] 교육IDX 분야별 미래상

Ⅳ 정책 및 R&D 전략 방향

【1】 교육 IDX 정책 방향

종합적인 교육 IDX 추진계획 마련

- 미래 인재상에 걸맞는 교육 실현을 위해 장기적이고 종합적이며 구체적인 교육 IDX 기본계획(안) 마련이 필요
  - 미래 인재상에 걸맞게 교육체계 및 시스템 변화를 유도해야하므로 이에 대해 장기적 관점에서 정책 수립을 마련할 필요성 제기
  - 교육의 변화로 영향을 받을 수 있는 각계·각층의 대표단을 구성하고 범정부 차원에서 거대 거버넌스를 구축하여 토론, 의견 수렴 등의 절차를 거쳐 종합적인 정책 수립 추진
  - 교육 IDX로 인해 변화될 미래상을 도출하고 각 시나리오별로 그에 걸맞는 구체적인 정책 가이드라인이 필요

교육 IDX 인프라 구축 및 콘텐츠 개발 환경 조성

- 인프라 구축을 단계적으로 시행하며 관련 제품, 서비스, 콘텐츠를 지속적으로 제공될 수 있도록 하는 계획이 필요
  - 교육 인프라는 초기 전자책과 전자칠판을 통해 다양한 멀티미디어를 이용하는 형태로 진행되겠지만 미래에는 각 학습자별 교육정보를 활용하는 서비스가 제공되어야 하므로 이를 위한 장기 인프라 구축 플랜이 필요
  - 즉, 교육정보를 저장, 분석하고 예측하기 위해 어떤 ICT 인프라 형태가 가장 적합하고 효율적인지 확인 및 분석하는 작업 필요

※ 지능형 클라우드 서비스, 가상 무선랜 서비스 활용, 보안설계 등 가용한 ICT 기술 및 서비스를 대상으로 인프라 형성에 고려해야할 사항을 나열해보고 이를 적시에 적용할 수 있도록 설계

  - 인프라가 형성되는 과정에서도 지능형 교육 서비스나 콘텐츠도 국내 환경에 맞게 개발 및 보급될 수 있도록 하는 단계별 R&BD 수립도 필요

체계적인 교육 IDX R&D 방향 수립

- 교육 IDX 종합계획에 근거해 관련 원천 및 응용 기술 R&D를 체계적으로 추진할 필요
  - 주요 ICT 원천 기술 개발 뿐만 아니라 교육 목적용 시스템 개발을 위한 응용 기술 개발도 중요
  - 응용기술 개발은 항상 R&D를 통해 서비스나 비즈니스화 될 수 있도록 하여 최대한 빠르게 적용될 수 있도록 고려할 필요
  - 오픈소스 형태의 기술개발로 누구나 참여하여 제품화 할 수 있도록 환경을 조성

교육 IDX 관련 생태계 조기 형성

- 학교에서 요구하는 교육법에 맞는 시스템 구축과 콘텐츠개발을 진행하고 그에 따라 관련 기업이 참여해 성장할 수 있는 계기를 만들 필요
  - 산학연관 네트워크를 구성하고 다양한 기업들이 지능형 교육 시스템 구현에 참가할 수 있도록 하여 관련 기술 및 콘텐츠 개발 역량 확보에 기여할 필요
  - 시범서비스 학교를 우선적으로 확대하는 한편 직능교육에 실감콘텐츠를 이용할 수 있도록 지원책 마련

[그림 3-10] 교육 IDX 정책 방향

【2】 교육 IDX R&D 전략 방향

교육 IDX를 위한 주요기술

- (교육 IDX 주요기술) '15년 교육과 관련된 IT기술의 하이프사이클(Hype Cycle)을 발표하며, 장기적 관점에서 교육에 영향을 미칠 기술들을 제공
  - 가장 직접적으로 향후 2년 이내에 영향을 미칠 중요한 기술로는 클라우드 고성능 컴퓨팅(HighPerformance Computing ; HPC), 가상세계, BYOD 등을 선정
  - 2~5년 내 학습분석기술이 가장 큰 영향을 미칠 것으로 예측하고 있으며 세부적으로는 기관/학생/졸업생 CRM 등의 분석기술과 적응적 전자교과서/학습플랫폼, 게임화(Gamification)기술의 파급력이 클 것으로 전망
  - 10년 내에는 역량기반의 교육 플랫폼과 학습자 정보 상호운용 표준, 개방형 마이크로 크리덴셜, 빅데이터 등의 기술이 시장에 큰 영향을 미칠 것으로 전망

[표 3-7] 교육에 영향을 미치는 주요 기술

	2년 미만	2~5년	5~10년	10년 이상
변혁적 영향		적응형 학습	-인지컴퓨팅 -교육 애플리케이션 -데브옵스 -디지털작업장그래프	-개인분석 기술
큰 영향	-클라우드 HPC/Caas -IT인프라 유틸리티 -소셜학습플랫폼	-적응형 E-교과서 -졸업생 및 학생 CRM BPO, -시민개발자 -클라우드 오피스 -연구자료디지털보유 -게임, -HVD -학습분석기술 -UC	-빅데이터 -능력기반교육플랫폼 -디지털 평가기술 -기업 아키텍쳐 -이수자 데이터 관리 -MOOC 기능 기술 -개방형 작은 학위 -SaaS SIS -SIS 국제 데이터 상호운용성 표준	-퀀텀 컴퓨팅
중간 정도 영향	-BYOD 전략 -강의 캡처기술 -오픈소스 -기업서비스 Bus -SaaS 관리앱	-EA 프레임워크 -교육용 태블릿 -기업 모바일 앱스토어 -E-교과서 -모바일 학습 스마트폰 -가상현실 -Waas	-감성컴퓨팅 -ITIL -오픈소스 SIS	-교실 3D 프린팅 -COBIT -Tin Can API
작은 영향	-80211ac Vave1			

자료 : Gartner(2015), 정보통신정책연구원(2015)를 참고

● **(주요 기술의 활용)** 빅데이터 및 인공지능 기술, 가상증강기술 MOOC 플랫폼* 등의 발전이 교육 부문에서의 변화를 촉발할 것으로 전망

- **(빅데이터)** 개인별 학습시간 및 학습자 패턴 등을 데이터화하여 분석함으로써 개인 맞춤형 학습에 활용
- **(게임화)** 게임 공학 및 설계 기법을 적용해 콘텐츠를 개발하고 보다 재미있는 학습이 될 수 있도록 함으로써 학습동기 부여와 학습효과 제고
- **(인공지능)** 빅데이터와 함께 학습자의 개인별 패턴을 효과적으로 분석하여 개인 교사, 가정교사 등의 역할을 수행 가능
- **(가상증강 학습)** 가상증강기술 운용이 가능한 스마트디바이스 및 HMD형 디바이스를 활용해 실감적인 교육 및 훈련 콘텐츠 제공
- **(MOOC)** 현재는 대학생을 대상으로 하는 각 대학별 교과과정을 제공하고 있으며, 그 대상을 향후 기업이나 조직 등으로 범위를 확장시키고 훈련까지 가능하도록 환경이 변화할 것으로 예상

[표 3-8] 주요기술 활용내용

구분	활용내용
빅데이터	• 에듀테크의 양적인 증가로 인하여 데이터 처리 중요성 부각 - 수업 달성 시간, 달성률 등 통계는 학습 과정에 대한 이해 상향 - 학습자 및 그룹의 패턴 분석 - 개인차를 고려하여 개별적 강의 제공 가능 - 학습자의 학습 시간 분석을 통해 난이도 평가
게임화	• 게임 공학과 게임 설계 기법을 적용하여 학습자 동기부여 - 게임을 통하여 학습에 직접 참여함으로써 기억 향상
인공지능	• 인공지능 기반의 에듀테크 기술을 통해 교실 밖에서도 언제든 학습 관련한 도움 가능 - 인공지능을 활용하여 채점과 같은 기본적 교육활동 자동화 가능 - 학생 수준별 진도학습 및 교육과정 자체 맞춤형으로 진행 - 학습과정에서 학생이 이해하지 못하는 부분에 대한 진단 및 피드백 가능 - 인공지능을 활용하면 학생의 정보자원에 대한 접근성 상승
가상증강 학습	• 환경이 학습자에게 적응하는 On-demand 학습으로 이해도를 높임 - QR code hunting, Oculus Rift 개발된 강의, GPS 기반 실생활과 결합한 활동, 애플워치 및 구글 글래스 앱 활용
MOOC 플랫폼	• 대학의 공급 강의를 전세계 학생들과 공유하는 온라인 공개 강의 - 대학에서 개인/기업/조직으로 범위가 확장되어 개인 및 조직원 훈련, 수요에 맞도록 미래 교육 훈련, 브랜드 인지도 및 지식 공유

출처 : 융합연구정책센터(2017)

● **(교육 IDX 기술매칭 및 격차)** 에듀테크 주요기술에 해당하는 국가전략기술*을 매칭 결과 대부분 세계 최고국에 비해 기술수준 및 격차가 존재

* 국가전략기술은 한국과학기술기획평가원에서 발표한 자료를 토대로 교육 IDX 주요기술과 매칭하였고 '전자·정보·통신 분야'가 대부분을 차지

- 국가전략기술은 핵심기술로써 원전기술의 성격이 강함으로 다양한 응용 영역별로 활용을 위해서라도 필요
- 각 영역별로 기술최고 국가인 미국에 비해 길게는 3.5년, 짧게는 1.0년의 격차가 존재하므로 교육 IDX를 위한 기술개발 및 서비스 도입시기가 늦어지는 문제가 발생할 소지 농후
- 주도권 확보를 위해서 국가전략기술의 R&D를 비롯해 교육 IDX를 위한 응용기술의 R&D를 수행할 필요

[표 3-9] 교육 IDX 주요기술과 국가전략기술 간 매칭 및 수준격차 현황

교육IDX 필요기술	관련 국가전략기술	기술수준		기술격차	
		최고국	현수준	최고국	현수준
빅데이터	지식기반 빅데이터 활용기술	미국	77.3	미국	3.3
	데이터분산처리 시스템기술	미국	79.9	미국	2.5
	차세대 유무선통신 네트워크 기술	미국	85.1	미국	1.9
	지식정보보안기술	미국	81.5	미국	2.7
게임화	지능형 인터렉티브기술	미국	78.5	미국	3.5
	감성공학적 디자인기술	미국	81.8	미국	2.9
인공지능	신개념 컴퓨팅 기술	미국	80.8	미국	2.1
	감성인지 및 처리기술	미국	83.3	미국	2.4
가상/증강 학습	가상증강현실기술	미국	79.9	미국	2.0
	실감형 감성 콘텐츠기술	미국	84.0	미국	1.7
	융합서비스 플랫폼기술	미국	80.7	미국	2.3
	인간친화형 디스플레이기술	미국	93.3	미국	1.0
MOOC 플랫폼	신개념 사용자 경험기술	미국	84.6	미국	2.1
	방송통신융합서비스	미국	86.4	미국	1.8
	차세대 유무선통신 네트워크 기술	미국	85.1	미국	1.9
	융합서비스 플랫폼기술	미국	80.7	미국	2.3

자료 : 한국과학기술기획평가원(2017)

교육 IDX R&D 전략 방향

- **(프로젝트형 R&BD 추진)** 플래그쉽 프로젝트를 구성하고 그에 맞는 R&BD 추진 필요
  - 교육현장, 가정공간, 산업응용, 온오프연계 등 4가지 측면에서 꼭 필요한 서비스를 고려해보고 그에 해당하는 플래그쉽 프로젝트를 선정하여 추진
  - 플래그쉽 선정을 위해 각 정부부처, 산업계, 교육계, 각 현장별 대표단 등의 거버넌스를 구축하고 관련 논의를 추진
  - 개발이 완료된 시점에 서비스나 제품이 제공될 수 있도록 설계 단계에서부터 교육서비스 및 비즈니스 모델을 고려할 필요
- **(사회문제 해결형 R&D 추진)** 현재 발생 및 진행 중인 교육관련 사회문제를 해결하기 위한 다양한 R&D가 필요
  - **(교육현장)** 지역별 교사불균형, 학교부적응, 수준별 교육 등 교육현장에서 발생하는 문제를 해결하기 위한 개인별 맞춤 교사 R&D 필요
  - **(가정공간)** 인구구조 및 사회의 다변화로 파생되는 문제(촉법소년, 고독사, 장애아 교육, 건강관리 등)를 1차적으로 가정공간에서 해결할 수 있는 방안을 모색하기 위한 일환으로 가정교사와 로봇을 연계하는 R&D가 필요
  - **(산업응용)** 직업교육 시 발생하는 위험요인을 안전하게 처리할 수 있는 교육방안 마련하기 위한 훈련 체험형 시뮬레이터 및 콘텐츠에 관한 R&D가 필요
- **(원천/응용기술 R&D 추진)** 교육 IDX에 원천이 되는 기술의 대부분은 전자·정보·통신에 해당되며 기술수준과 격차가 선진국과 차이가 나므로 이에 대한 원천/응용기술에 대한 R&D가 필요
  - 각 영역별로 기술최고 국가인 미국에 비해 기술수준 및 격차가 존재하므로 향후 교육 IDX관련 서비스 시기가 늦어질 수 있다는 점에서 주도권을 빼길 수 있는 문제가 발생할 가능성 농후
  - 개인교사나 가정 내에 보급될 로봇 등 교육 IDX와 관련된 다양한 기능을 제공하기 위해 인공지능 및 빅데이터 등에서 응용기술 개발도 필요

Part 4

Cybersecurity IDX 전략

I Cybersecurity 분야 IDX 추진 배경

Cybersecurity 분야 정의

Cybersecurity 개요

- 위키피디아에 의하면, Cybersecurity는 컴퓨터 시스템을 하드웨어, 소프트웨어 또는 정보의 도난 및 손상으로부터 보호하는 것이며 또한 컴퓨터 시스템이 제공하는 서비스의 중단 또는 오용으로부터 보호하는 것으로 정의[25]하고 있음
  - Cybersecurity는 하드웨어 및 플랫폼 등에서 중요성이 높아지고 있음. 클라우드 기술의 성장, 기업에서의 BYOD (bring your own devices) 채택, 5G 등 무선 기술의 확산, 스마트 IoT (internet of things)의 사용 등은 사이버 위협을 가중시키고 있음
  - Cybersecurity의 유형은 네트워크 안전, 엔드포인트 안전, 앱 안전, 클라우드 시스템 안전, 콘텐츠 안전, 게이트웨이 안전, 산업 통제 시스템 안전, 및 기타 다양한 안전의 형태를 가짐. 해커들은 위에서 언급한 여러 행태의 안전을 위협하여 과도한 이득을 얻기 위해서 컴퓨터 시스템을 파괴시키는 새로운 방법을 지속적으로 찾고 있음
  - Cybersecurity는 기업의 네트워크로부터 정부의 네트워크로 범위를 확장하고 있음. 공공 부문을 포함하는 정부 IT 도메인에서의 Cybersecurity는 최근에 매우 복잡해지고 있으며, 부담해야할 비용도 증가하고 있음

Cybersecurity 범위

- cybersecurity의 공격과 방어의 관점 및 사이버 보안 시장의 관점에서 본 cybersecurity 유형은 다음과 같이 나누어 설명할 수 있음. ① 네트워크 보안 ② 엔드포인트 보안 ③ 응용프로그램 보안 ④ 산업통제시스템 보안 ⑤ 클라우드 보안 ⑥ 무선 보안 ⑦ 콘텐츠 보안 ⑧ 게이트웨이 보안 ⑨ 최근에 부상하고 있는 IOT 보안 등이 있음.
- (**네트워크 보안**) : 컴퓨터 네트워크 및 네트워크로 액세스 할 수 있는 자원에 무인가 액세스, 남용, 수정 및 거절을 예방하거나 모니터 하기 위해서 채택되는 정책 및 관행으로 구성됨.
- (**엔드포인트 보안**) : 클라이언트 디바이스에 원격으로 연결된 컴퓨터의 네트워

25) Gasser, Morris (1988). Building a Secure Computer System. Van Nostrand Reinhold. P.3. ISBN 0-442-23022-2. Retrieved 6 September 2015.

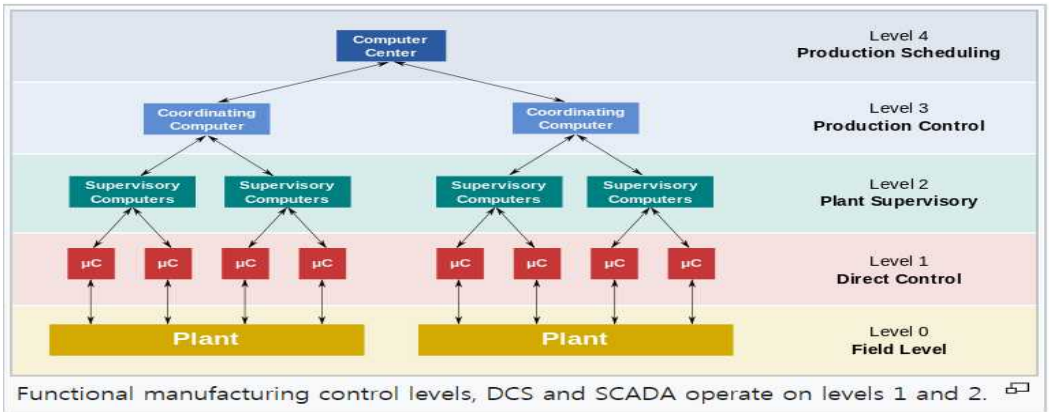
크의 보호를 위한 접근방법임. 랩탑, 태블릿, 모바일 폰 기타 무선 디바이스가 기업 네트워크에 연결하는 것은 보안 위협을 위한 공격 대상이 됨. 엔드포인트 보안은 이러한 디바이스들이 표준에 대한 명확한 수준을 준수하는지 확인하려고 시도함.

- (**응용프로그램 보안**) : 보안의 취약점을 찾고, 수정하고 예방함으로써 어떤 응용프로그램의 보안을 개선시키기 위한 조치들을 포함함. 응용프로그램의 라이프사이클, 예를 들어 설계, 개발, 설치, 업그레이드 또는 유지보수 등의 각각의 단계에서 보안 취약점을 알아차리기 위해 여러 가지 기법이 사용되고 있음.

[표 4-1] 사이버 보안의 위협과 공격 유형

Category	Threats / Attacks
인풋 검증 (유효성 조사)	Buffer overflow; cross-site scripting; SQL injection; canonicalization
소프트웨어 변조	Attacker modifies an existing application's runtime behavior to perform unauthorized actions; exploited via binary patching, code substitution, or code extension
인증	Network eavesdropping ; Brute force attack; dictionary attacks; cookie replay; credential theft
권한 부여	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
형상 관리	Unauthorized access to administration interfaces; unauthorized access to configuration stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
민감한 정보	Access sensitive code or data in storage; network eavesdropping; code/data tampering
세션 관리	Session hijacking; session replay; man in the middle
암호화	Poor key generation or key management; weak or custom encryption
패러미터 조작	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
예외 관리	Information disclosure; denial of service

- (**산업 통제 시스템 보안**) : 산업의 프로세스 통제를 위해 사용되는 여러 유형의 통제 시스템 및 관련 도구 포함함. 산업 통제 시스템 보안은 산업 자동화 및 통제 시스템의 적절한 운영에 의도적 또는 비의도적 인터페이스 하는 것을 예방하는 것임.



[그림 4-1] 산업 통제 시스템 보안의 예시

- (**클라우드 보안**) : 클라우드 컴퓨팅의 데이터, 응용프로그램, 및 관련 인프라를 보호하기 위해서 전개되는 다양한 정책, 기술 및 통제를 말함. 클라우드 컴퓨팅과 관련한 보안 이슈는 크게 두가지로 분류될 수 있음. 클라우드 서비스 제공자가 직면할 보안 이슈와 클라우드 사용자가 직면할 보안 이슈 등임. 제공자는 인프라가 안전하고 클라이언트 데이터 및 응용프로그램이 보호되고 있음을 보장해야 하며, 반면에 사용자는 이러한 적용을 강화하고 강력한 패스워드 및 인증 수단를 사용하기 위한 조치를 취해야 함. 어떤 조직이 데이터를 보관하고 공공 클라우드에 응용프로그램을 호스트 한다면, 이는 정보를 호스팅 하는 서버에 물리적으로 액세스 할 수 있는 능력을 상실하게 될 것이고, 결과적으로 잠재적인 민감 데이터는 내부 공격으로 부터의 위험한 상태에 놓이게 됨. 최근의 클라우드 보안 협회 보고에 따르면 내부 공격은 클라우드 컴퓨팅에 있어서 6번째의 위협이 되고 있음[26]. 따라서 클라우드 서비스 제공자는 데이터 센터에 있는 서버에 물리적으로 액세스하는 종업원을 대상으로 철저한 백그라운드 체크가 이루어지고 있음을 보장해야 함. 이에 추가하여, 데이터 센터는 종종 수상한 행동에 대해 모니터 해야 함. 자원을 보존하고, 비용을 절감하고, 효율성을 유지하기 위해서, 클라우드 서비스 제공자는 종종 동일한 서버에 하나 이상의 고객의 데이터를 저장함. 그 결과, 한 사용자의 사적 데이터가 다른 사용자에 의해서 보여 질 수 있는 기회가 있을 수 있음. 이러한 민감한 상황을 처리하기 위해서, 클라우드 서비스 제공자는 적합한 데이터 분리 및 논리적 스토리지 분리를 보장해야 함. 클라우드 인프라를 구현함에 있어서

26) “Top threats to cloud computing v1.0” Cloud Security Alliance. Retrieved 2014-10-20. 위협의 유형은 다음과 같음. ① 클라우드 컴퓨팅의 남용 및 극악한 사용 ② 보안되지 않는 인터페이스 및 API ③ 악의적 내부자 ④ 공유된 기술 이슈 ⑤ 데이터 손실 또는 누출 ⑥ 계정 또는 서비스 하이잭킹 ⑦ 알려지지 않는 리스크 프로파일 등임.

가상화의 포괄적인 사용은 공공 클라우드 서비스의 사용자에게 보안에 관한 우려를 가져올 수 있음. 가상화는 OS 와 이에 기반하는 하드웨어의 관계를 변화시키며, 이는 컴퓨팅, 스토리지 또는 네트워킹에도 다 적용됨. 이것은 추가적인 레이어즉 가상화를 도입하는 것으로 스스로 형상화되고, 관리되고, 보안되는 것임. 특정한 우려는 가상화 소프트웨어를 손상시키는 잠재력을 포함함. 이러한 우려는 매우 이론적이기는 하지만, 존재하고 있음. 예를 들어 가상화 소프트웨어의 관리 소프트웨어로 관리자 워크스테이션에 침해를 가하는 것은 모든 데이터센터가 작동을 멈추거나 공격자의 의도대로 재형상될 수 있게함

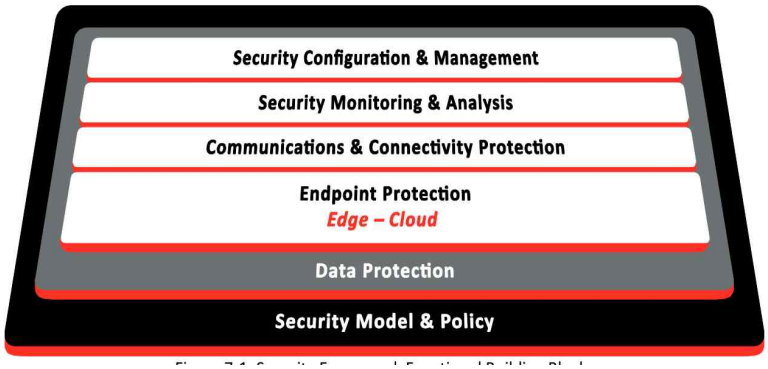
- (**무선 보안**) : 무선 보안 : 무선 네트워크를 사용하는 컴퓨터에 무단 액세스 또는 손상을 가하는 것을 예방하는 것임. 무선 액세스의 형태는 다음과 같음. ① Accidental association ② Malicious assoiciation ③ 임시 네트워크 ④ 비전통적인 네트워크 ⑤ ID 도용 (MAC spoofing) ⑥ Man-in-the-middle attacks ⑦ DoS ⑧ Network injection ⑧ Caffe Latte attack 등임

- (**콘텐츠 보안**) : 신뢰받고 있는 웹 페이지 컨텍스트에서 악의적 콘텐츠의 실행으로 말미암는 cross-site scripting[27], clickjacking, 기타 코드 주입을 예방하기 도입되는 컴퓨터 보안 표준임

- (**IIOT 보안**) : IIOT 보안 프레임워크의 기능상의 관점은 6개의 빌딩 블록으로 이루어지며, 이 6개는 다시 3개의 계층을 구성함. 상층 계층은 네 개의 핵심 보안 기능을 포함함. ① 엔드포인트 보호 ② 통신 및 연결 보호 ③ 보안 모니터링 및 분석 ④ 보안 형상 관리 등임. 이 네 개의 기능은 데이터 보호 계층 및 시스템 전반의 보안 모형 및 정책 계층에 의해 지원됨. 이 3개의 계층은 산업 인터넷 보안 프레임워크의 기능적 관점을 포함하고 있음
  - 엔드포인트 보호는 에지와 클라우드에 있는 디바이스에 방어적 능력을 구현함. 최우선적인 관심사는 물리적 보안 기능, 사이버 보안 기법 및 권한을 가진 ID를 포함함. 엔드포인트가 상호간에 통신을 하며, 그리고 통신이 취약점의 원인을 제공할 수 있기 때문에 엔드포인트 보호만으로는 충분하지 않음.

27) 크로스 사이트 스크립팅은 웹 응용프로그램에서 전형적으로 발견되는 컴퓨터 보안 취약성의 하나의 유형임. XSS는 다른 사용자에 의해 보여지는 웹사이트에 클라이언트 스크립을 주입시키는 것을 가능하게 함.

- 통신 및 연결 보호는 트래픽의 인증 및 권한 부여를 구현하기 위해서 엔드포인트 보호로부터 권한있는 ID 역량을 사용함. 정보 흐름의 통제 뿐만 아니라 무결성 및 기밀성을 확보하기 위한 암호 기술은 통신 및 연결을 보호함.
- 일단 엔드포인트가 보호되고 통신이 보안되면, 시스템의 상태는 시스템의 모든 구성 요소를 위해서 보안 모니터링 및 분석 기능과 통제된 보안 형상 관리에 의해 운영 라이프 전반에 걸쳐 보존되어야 함.
- 이들 네가지의 빌딩 블록은 엔드포인트에 머물러 있는 데이터로부터 통신을 하면서 움직이는 데이터로 확장하고 있는 공통의 데이터 보안 기능에 의해 지원됨. 이것은 또한 모니터링 및 분석 기능의 일부로서 모아진 모든 데이터와 그리고 시스템 형상 및 관리 데이터를 포함함.
- 시스템 모형 및 정책은 보안이 어떻게 실현되는 가를 관리하며, 라이프 사이클 전반에 걸쳐 시스템의 기밀성, 무결성 및 사용가능성을 보장하는 정책을 관리함. 이는 융합적인 종단간 보안을 실현시키기 위해서 모든 기능적인 요소들이 어떻게 상호간에 작동하는 것을 조율함.



[그림 4-2] IIOT 보안 프레임워크 개요

Cybersecurity 분야 현황 및 문제점

Cybersecurity 시장

- Cybersecurity 시장은 최종 제품, 솔루션, 및 관련 서비스를 포함하여 2017년 1,205.6 억 달러에서, 2022년 2,059.1 억 달러로 성장할 것으로 예측 되며, 연평균 11.3 %의 고속 성장시장으로 보여짐. (Mind commerce 사 예측)
  - **(제품 및 솔루션 : 서비스 시장)** Cybersecurity 제품 및 솔루션 시장은 2017년 1,085.0 억달러 시장에서 2022년 1,850 억달러 시장으로 성장하고 서비스 시장은 2017년 120.6 억달러에서 2022년 205.9 억달러로 성장할 것으로 예측 됨.

제품 및 솔루션 시장이 전체의 90 %를 차지하고, 나머지 10 %를 서비스 시장이 차지하고 있음.

- (**제품 및 솔루션 시장**) 2022년에, 제품 및 솔루션 시장 규모는 1,850 억달러이며, 이중에서 방화벽 솔루션 시장이 315억 달러이며, ID 및 액서스 관리, 리스크 및 규정 준수 관리 시장이 각각 200~300억 달러 시장이며, 암호화 솔루션, 엔드포인트 보호 관리, 보안 정보 및 이벤트 관리 소프트웨어 시장이 각각 100~200억 달러시장임. 위 6개의 제품 및 솔루션 시장이 제품 및 솔루션 시장의 63 %를 차지하고 있음.
- (**서비스 시장**) 2022년에, 서비스 시장 규모는 205.9억 달러 이며, 이중에서 전문 서비스 및 관리서비스가 각각 78%, 22%를 차지하고 있음.

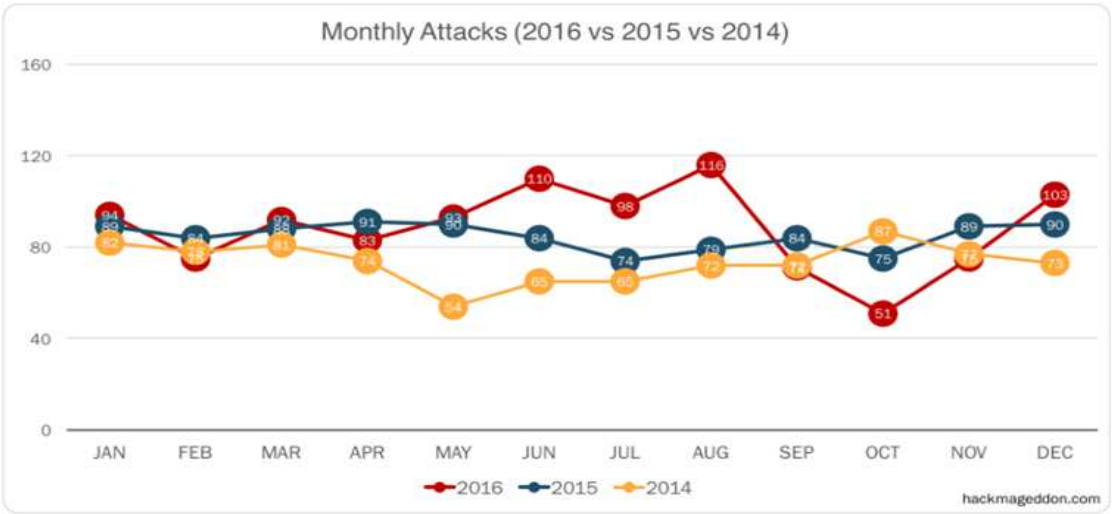
  * 2022년에, 전문 서비스 시장 중에서 유지·보수 서비스 시장 및 컨설팅 시장이 각각 33.7억 달러, 30.5억 달러 이며, 리스크 평가 서비스 시장, 훈련 서비스 시장은 각각 20억~30억 달러 규모임. 상기한 4개의 전문 서비스 시장이 전문 서비스 시장의 55%를 차지하고 있음.
- (**보안 유형별 시장**) 2022년에, 보안 유형별로 구분하여 살펴보면, 네트워크 보안 시장이 514.8억 달러 규모이며, 엔드포인트 보안 시장이 400억~500억 달러 규모, 응용 프로그램 보안 시장이 300억~400억 달러 규모, 산업 통제 시스템 보안 시장이 200억~300억 달러 규모, 클라우드 보안 및 무선 보안 시장이 각각 100~200억 달러 규모임. 상기한 6개의 시장이 사이버 시장 전체의 91 %를 차지하고 있음.

◐ Cybersecurity 관련 사건의 최근 동향 (2014~2016)

- 1988년 로버트 모리스 및 최초의 컴퓨터 웜 (Robert morris and the first computer worm) 이후로 발생한 사이버 공격 및 침해 중 대표적인 것은 다음과 같음.
  - 1994년의 rome laboratory case, 2007년의 TJX customer credit card case, 2013년의 stuxnet attack, global surveillance disclosure, 2013~2014년의 target and Home Depot breaches, 2015년의 personal management data breathes, 2015년의 Ashkey Madison breach, 2016년의 Russian meddling of US election 등임.

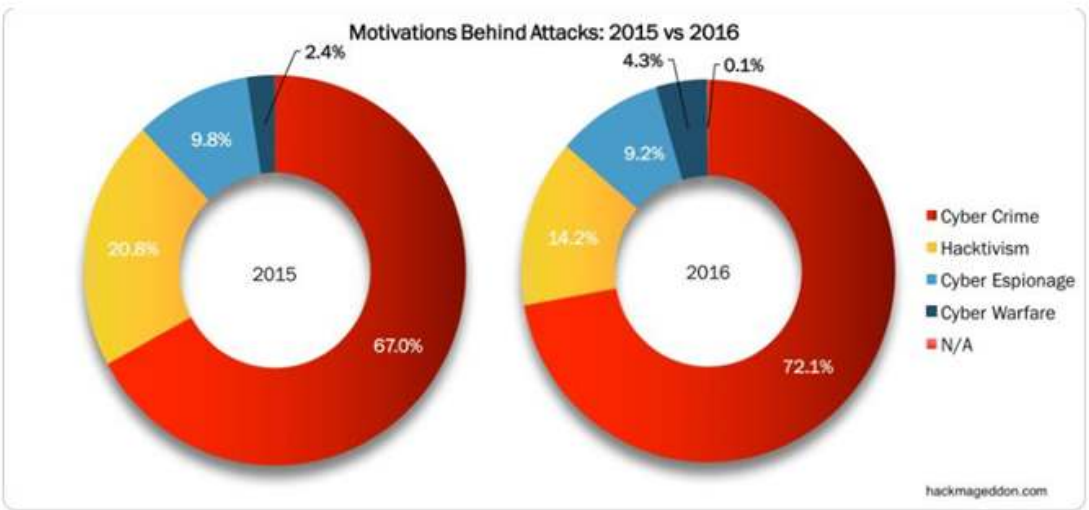
- Cybersecurity는 컴퓨터 사용 이후로 일상적인 관심에 머물러 있었으나, 최근 3년 동안에 관심이 커지고 있음.

• 최근 3년 동안의 사이버 공격은 해가 거듭될수록 증가하는 추세를 보임. 이 기간 동안에 월별 데이터를 보더라도 비슷한 추세를 보이고 있음.



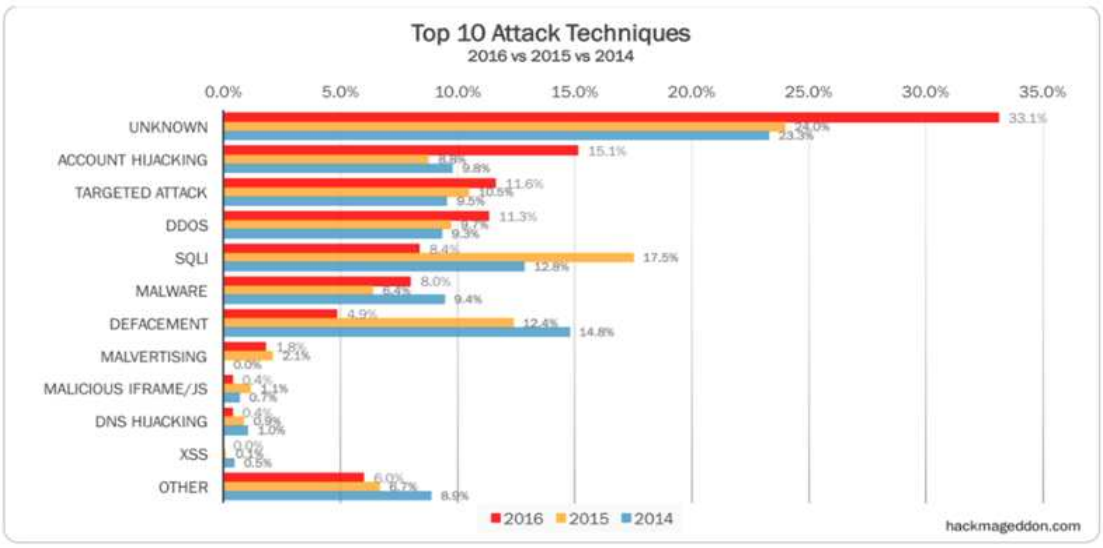
[그림 4-3] 사이버 공격 월별 트렌드 비교 (2014~2016)

• 동 기간의 사이버 공격 배후의 동기(motivation)를 조사할 때, 상기한 추세와 비슷한 추세를 보이고 있음. 사이버 범죄의 비율이 2015년 67 % 에서 2016년 72 %로 증가하였음. 해킹, 사이버 간첩첩, 사이버 전쟁을 포함한 기타 동기(motivation)들도 혼합 추세를 보였음. 다음의 그래프는 사이버 공격 배후의 동기를 비교한 것임.



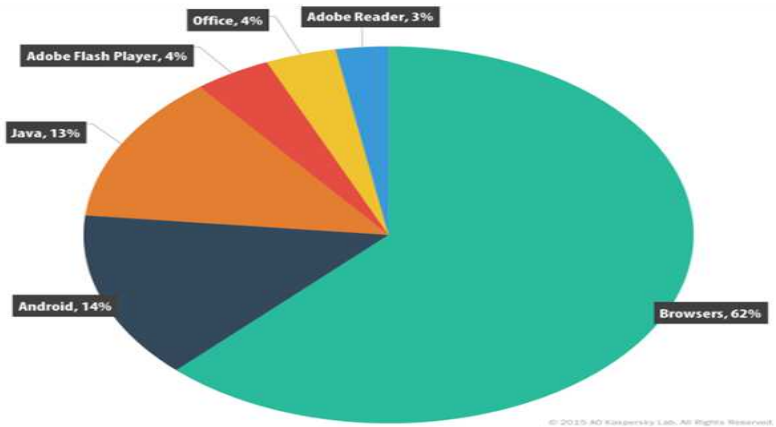
[그림 4-4] 사이버 공격의 동기 분석(2015~2016)

• 사이버 공격 기술은 동 기간에 유사한 트렌드를 보임. 10개의 공격 기술 중에서 알려지지 않는 이유 (unknown reason)가 2014년에 비하여 10% 포인트 상승하여 2016년에는 33%를 차지하고 있음.



[그림 4-5] 상위 10대 기술 사이버 공격 기술 비교 (2014~2016)

• 아도브 플래시 플레이어가 사이버범죄자들에 사용되어지고 있는 해킹의 가장 취약한 소스 중의 하나임. 그러나 브라우저 앱이 사이버공격의 주요 소스로서 사용되고 있으며 자바 및 안드로이드 악용이 2015년 이후 기하급수적으로 증가하였음. 다음의 그래프는 2015년에 사이버 해킹에 사용된 앱의 비율을 보이고 있음.



[그림 4-6] 사이버 보안의 대상이 되는 응용프로그램 (2015)

- 동시에, 방어 체계는 강화되었으며, 취약점이 제로인 날의 수가 또한 증가하였음. 예를 들어 취약점이 제로인 날이 2015년에 매주에 발생하였음.
  * 날수로는 2014년에 24일에서 2015년에 54일로 증가하였으며, 또 다른 추세는 모든 사건들이 그 해에 보고되지 않음이 밝혀졌음.
  * 기록된 데이터는 거의 5천만명의 개인 기록이 2015년에 도난 당했다고 밝히고 있음.
  * 패치받지 못한 취약성을 가지고 있는 웹사이트의 75%가 위험스러운 사건을 증가시켰음. 스피어 피싱이 또한 2015년에 55% 증가하였음.

Cybersecurity 분야 규제 프레임워크

Cybersecurity 규제 프레임워크 : 국제 동향

- Cybersecurity 규제 프레임워크는 조직체의 크기 및 산업체 분야와는 관계없이 모든 조직체에 산업 표준, 국가 규정, 국제 이니시어티브를 통합시킴
  - 포괄적인 보안 관리 및 규제 가이드라인의 필요성은 업계 전반에 걸쳐 강력함.
  - 어떤 산업 표준들은 소매업 분야에서는 ISAC[28] 이니시어티브, 통신 및 인터넷 산업 분야에서는 중국의 개인 정보 보호 규칙, 디지털 미디어 산업 분야에서는 DMCA (Digital Millenium Copyright Act), 지불 카드 산업에서는 데이터 보안 표준을, 의료 산업 분야에서는 건강 보험 이식성 및 책임 규칙, 스포츠 산업에서는 스포츠 ISAO (Information sharing and analysis organization) 이니시어티브를 포함하고 있음
  - 몇가지의 예시로는 미국 금융산업의 Gramm Leach-Biely Act, the Bank Secrecy Act and Sasbanes-Oxley Act, 미국의 연방정보보안관리법, EU의 일반 데이터 보호 규정, EU의 CSIRTs TERENA 태스크포스 TF-CSIRT, 캐나다의 사이버 보안 전략, 중국의 국가 보안 및 장기 발전 및 조정 이니시어티브, 독일의 국가 사이버-방어 이니시어티브, 인도의 2013년도 국가 사이버 보안 정책, 한국의 2017년에 5,000 명의 신규 사이버보안 전문가를 고용하는 정부 이니시어티브, 미국의 컴퓨터 사기 및 남용법, AT&T, IBM, 팔토 알토 네트워크, 시맨텍, 및 Trustonic 중심의 사이버보안 연합 등이 있음
  - 몇가지의 국제 활동으로는 FIRST (The Forum of Incident Response and Security Teams), MAAWG (The council of Europoe for cybercrime,

28) ISAC (Information Sharing and Analysis Center)는 주요 기반 시설의 사이버 위협에 관한 정보를 모으고, 사적 및 공공 부문 간에 정보 공유를 제공하기 위한 주된 자원을 공급하는 비영리기관임.

Managing Anti-Abuse Working Group (MAAWG), ENISA European Network and Information Security Agency) 등이 있음. 선두에 서 있는 기업들로는 AT&T, 애플, 시스코, MaCfee, 마이크로소프트, 프랑스 텔레콤, 패북, 스프린드 등이 있으며, 이들이 각각 다른 국제 포럼 및 이니시어티브에 활동하고 있음

Cybersecurity 규제 프레임워크 : 국내 동향

- 우리나라 정보화에 관한 최초 법률은 1986년에 제정된 「전산망 보급 촉진에 관한 법률」(시행 1987.1.1.) 임. 이는 전기통신설비와 전자계산조직 및 전자계산조직의 이용기술을 활용하여 정보를 처리·보관하거나 전송하는 조직망을 보호하기 위한 사항을 규정하고 있음
  - 정부(체신부장관)은 국가기관, 지방자치단체, 정부투자기관이 업무의 전산화를 촉진하기 위하여 추진하는 국가기간전산망의 의 구축의 법적근거를 마련
  - 2001년에 「정보통신 이용촉진 및 정보보호에 관한 법률」(시행 2001.7.1.)로 전면 수정하고, 2003년에 발생한 1.25 인터넷 대란을 계기로 전자침해사고 대응 관련 규정을 보완하였으며, 2004년에 정보보호 관련 규정들을 정비하였음
    * ① 정보보호산업[29]을 정의하고 있으며, ② 인터넷 정보보호를 강화하기 위하여 전국적으로 정보통신망 접속서비스를 제공하는 자 등에 대하여 정보보호지침[30]의 준수 의무화, ③ 매년 정보보호 안전진단을 받으며, ④ 정보통신부 장관은 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 이를 권고할 수 있으며, ⑤ 주요 정보통신서비스제공자는 정보통신망에 중대한 침해사고가 발생하여 정보통신망 등에 심각한 장애가 발생할 가능성이 높은 경우에는 이용자에게 보호조치를 요청할 수 있게 함
  - 2012년에 일부 수정을 통하여 정보보호 안전진단제도를 폐지하고 기업의 정보보호를 체계적으로 관리·지원할 수 있는 정보보호 관리체계 인증제도로 일원화하며, 정보보호 사전점검 제도에 대한 법적 근거를 마련하였음

- 1995년에, 우리나라 정보화를 체계적으로 정립한 「정보화 촉진 기본법」을 제정하여 (시행 1996년 1월 1일), 정보화[31] 및 정보보호[32]를 최초로 정의하고

29) "정보보호산업"이라 함은 정보보호제품을 개발·생산 또는 유통하거나 정보보호에 관한 컨설팅 등과 관련된 사업을 말함.

30) 정보보호지침에 반드시 포함되어야 할 사항으로는 ① 정당한 권한 없는 자의 정보통신망에의 접근과 침입을 방지하거나 대응하기 위한 정보보호시스템의 설치 운영 및 기술적·물리적 보호조치, ② 정보의 불법 유출·변조·삭제 등을 방지하기 위한 기술적 보호조치, ③ 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리적 보호조치, ④ 정보통신망의 안정 및 정보보호를 위한 인력 조직 경비의 확보 및 관련 계획 수립 등 관리적 보호조치, ⑤ 그 밖에 정보통신부 장관이 정보통신망의 안정 및 정보보호에 필요하다고 인정하는 사항 등임

하였으며, 정보화 촉진을 통하여 우리나라 수출주력산업으로 부상한 정보통신산업의 기반을 조성하여 국민경제의 발전에 이바지하기 위한 사항을 규정

- 1999년에, 일부 개정을 통하여 정보보호와 관련하여 정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 강구할 의무가 있음을 규정하고 있으며, 한국정보보호센터 설립, 정보보호시스템에 관한 기준 고시, 정보시스템에 대한 감리 등을 규정하고 있음
- 2009년에, 정보화 촉진 기본법을 전부 개정하여 국가정보화기본법을 공포하였음. 동법 제4장 제2절(정보이용의 안전성 및 신뢰성 보장) 제37조에서 국가기관과 지방자치단체는 정보를 처리하는 과정에서 정보의 안전한 유통을 위하여 정보보호를 위한 시책을 마련하며, 정부는 암호기술의 개발과 이용을 촉진하고 암호기술을 이용하여 정보통신서비스의 안전을 도모할 수 있는 조치를 마련해야 함
  * 정보보호시스템의 보완과 관련하여 동법 시행령에서는 과학기술부장관은 정보보호시스템의 성능과 신뢰도에 관한 기준을 정하거나, 그 기준에 맞는지의 여부를 평가 또는 인증하는 업무에 관한 세부 사항을 정할 때에는 관계기관의 장과 미리 협의하여야 하며, 과학기술정보통신부장관은 정보보호시스템을 제조하거나 수입하는 자가 그 시스템이 상기한 기준에 합치되는지의 확인을 요청한 경우에는 한국인터넷진흥원의 장 또는 관계국제협약에서 정한 기준에 맞는 기관의 장에게 그 시스템을 조사 또는 시험·평가하게 할 수 있으며, 상기한 조사 또는 시험평가를 요청하는 자는 과학기술정보통신부장관이 정하여 고시하는 기준에 따라 한국인터넷진흥원의 장과 및 관계 국제협약에서 정한 기준에 맞는 기관의 장이 정한 수수료를 내야 한다고 규정하고 있음
- 2013년에, 인터넷 중독의 예방에 필요한 조치를 한 정보통신서비스에 대한 인증제도를 도입하고, 장애인고령자 등의 정보 접근 및 이용 편의를 증진하기 위하여 웹사이트를 통하여 제공되는 정보통신서비스의 접근성에 대한 인증 제도를 도입하였음
- 2015년에, 정부는 다수의 정보통신기반을 일정한 공간에 집적시켜 통합 운영 관리하는 시설인 데이터센터의 안정적인 운영과 효율적인 제공등을 위하여 데이터센터의 구축 및 운영 활성화에 대한 시택을 수립 시행할 수 있도록 하고 있음

- 1999년에, 개인 및 기업의 정보유통과 중요정보를 보호하기 위하여 「전자서명법」을 제정하였는 데, 이는 전자문서[33]의 안정성과 신뢰성을 확보하고 그

31) “정보화”라 함은 정보를 생산·유통 또는 활용하여 사회 각 분야의 활동을 가능하게 하거나 효율화를 도모하는 것을 말함.

32) “정보보호”라 함은 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단(이하 "정보보호시스템"이라 한다)을 강구하는 것을 말함.

이용을 활성화하기 위해서 전자서명[34]에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 하고 있음

- 2002년에, 전자서명을 위한 기술을 "전자서명키" 등 특정기술로 한정하고 있었으므로, 앞으로의 전자서명 및 인증기술의 발전추세에 대비하여, 보다 다양한 기술을 수용할 수 있도록 전자서명의 개념을 새로이 정이하고 국제화 시대를 맞이하여 날로 확대되는 국제거래 상의 전자서명 인증문제를 명확하게 규정하였음. 따라서 전자서명의 정의를 서명자를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는 데 이용하기 위하여 당해 전자문서에 첨부하거나 논리적으로 결합된 전자적 형태의 정보를 말하는 것으로 수정하였음

* 한편 공인인증[35]기관의 안정성 확보를 위하여 공인인증업무와 관련된 시설에 대하여 보호조치를 취하도록 하고, 이의 안전운용 여부의 점검을 의무화하도록 하고 있으며, 정부는 전자서명의 안전성과 신뢰성의 확보 및 이용 활성화를 위한 기본정책의 수립 시행 등에 관한 시책을 강구할 의무가 있음

- 2001년에, 정보화의 진전에 따라 주요사회기반시설의 정보통신시스템에 대한 의존도가 심화되면서 해킹·컴퓨터 바이러스 등을 이용한 전자적 침해 행위[36]가 지식기반국가의 건설을 저해하고 국가 안보를 위협하는 새로운 요소로 대두됨에 따라 전자적 침해행위에 대비하여 주요정보통신기반시설[37]을 보호하기 위한 체계적이고 종합적인 대응체계를 구축하기 위해서 「정보통신기반보호법」을 제정하였음 (시행 2001.7.1.)

  - 주요정보통신기반시설이라 함은 중앙행정기관이 소관분야의 정보통신기반시설 중 다음 각호의 사항을 고려하여 전자적 침해행위로부터 보호가 필요하다고 인정되는 정보통신기반시설을 말함. 고려사항[38]은 다음과 같음

---

33) "전자문서"라 함은 컴퓨터 등 정보처리능력을 가진 장치에 전자적 형태로 작성, 송·수신 또는 저장된 정보를 말함. 이후 2002년 4월 1일에 정보처리시스템에 의하여 전자적 형태롤 작성되어 송신 또는 수신되거나 저장된 정보를 말하는 것으로 수정됨.

34) "전자서명"이라 함은 전자문서를 작성한 자의 신원과 전자문서의 변경여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명생성키로 생성한 정보로서 당해 전자문서에 고유한 것을 말함. "전자서명생성키"라 함은 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말함. "전자서명검증키"라 함은 전자서명을 검증하기 위하여 이용하는 전자적 정보를 말함. "전자서명키"라 함은 전자서명생성키와 이와 합치되는 전자서명검증키를 말함.

35) "인증"이라 함은 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위를 말함.

36) "전자적 침해행위"라 함은 정보통신기반시설을 대상으로 해킹, 컴퓨터바이러스,논리·메일폭탄,서비스거부 또는 고출력 전자기파 등에 의하여 정보통신기반시설을 공격하는 행위를 말함.

37) "정보통신기반시설"이라 함은 국가안전보장 행정 국방 치안 금융 통신 운송 에너지 등의 업무와 관련된 전자적 제어 관리 시스템 및 정보통신망이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 제1호의 규정에 의한 정보통신망을 말함.

* 이밖에도 국무총리 소속하에 정보통신기반보호위원회 설치, 주 요정보통신기반시설 관리기관장의 소관 시설에 대한 취약점 분석 평가, 국가 안전보장에 중대한 영향을 미치는 도로·지하철·공 항· 전력시설 등 주요정보통신기반시설의 관리기관장은 국가안보 업무를 수행하는 기관의 장에게 우선적으로 기술지원 요청, 단 금 융정보통신기반시설 및 그 밖의 정보통신기반시설에 대하여는 대 통령령이 정하는 국가기관의 장 또는 전문기관의 장에게 기술적 지원 요청, 주요정보통신기반시설을 관리하는 기관의 장은 소관 시설이 침해 사고로 인해 교란·미비 또는 파괴된 사실을 인지한 때에는 이를 관계기관 등에 통지하고 피해복구 및 피해확산 방지 를 위한 조치를 취해야 함

- 2002년에는 일부 개정하여 정보보호전문업체를 정보보호컨설팅전문업체로 변경하였으며, 2008년에는 주요정보통신기반시설을 신속하고 효과적으로 보호하기 위하여 정보통신부장관과 국가보안업무를 수행하는 기관의 장 등 대통령이 정하는 국가기관의 장이 중앙행정기관에 주요정보통신기반시설의 지정을 권고하고 주요정보통신기반시설 보호대책의 이행여부를 확인할 수 있도록 하였음
- 2015년 7월에는 관계중앙행정기관의 장은 소관분야에 대한 주요정보통신기반시설에 관한 보호계획을 수립 시행할 때 현행 시설중심의 대책을 확대하여 관리 정보의 침해사고에 대한 예방, 백업, 복구 등 데이터중심의 관리대책을 포함시켰음. 동년 12월에는 전문분야별 기반시설의 특성에 따른 사이버위협 분석 및 정보제공 등을 위해 구축·운영할 수 있는 정보공유·분석 센터를 현재 정보통신, 금융 및 행정분야에서 보건의료, 에너지, 교육 등 다양한 분야로 확산 장려하기 위해 인센티브 제공 근거를 마련하고 정보공유·분석 센터 구축시 불필요한 행정적·절차적 부담을 완화하였음
- 한편, 2005년에 국가안보를 위협하는 해킹, 바이러스 등 사이버 공격[39]으로부터 국가정보통신망[40]을 보호하기 위하여 사이버 안전[41]에 관한 조직 및 운영에 대한 사항을 체계적으로 정립한 「국가사이버안전관리규정」이 대통령 훈령으로 발령되었음. 동 훈령의 적용대상은 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망이며, 상위법인 정보통신기반보호법 제8조의 규정에 의하여 지정된 주요정보통

38) 고려사항은 ① 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성, ② 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도, ③ 다른 정보통신기반시설의 상호연계성, ④ 침해사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위, ⑤침해사고의 가능성 및 그 복구의 용이성 등임.

39) "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말함.

40) "정보통신망"이라 함은 전기통신법 제2조 제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말함.

41) "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지시키는 상태를 말함.

신기반시설은 제외하였음. 그리고 사이버 공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가사이버안전센터[42]를 설립을 규정하고 있음

* 2010년에는 사이버 공격을 탐지하여 차단하고 사이버 공격 발생시 범정부 차원에서 효율적으로 대응하기 위한 국가 사이버위기[43] 종합대책의 이행을 위하여 중앙행정기관의 장은 보안관제센터를 설치 ·운영하고, 국가정보원장은 주의 수준 이상의 경보 발령시에는 범정부적 차원에서 대책본부를 구성 운영할 수 있도록 하고 있음
* 2012년에는 국가기관 홈페이지에 대한 디도스 공격 등 다양한 사이버공격으로 사회·경제적 혼란이 발생함에 따라, 국가정보원장은 사이버안전 정책을 효율적·체계적으로 수행하기 위하여 사이버안전계획을 수립 시행하도록 하고 있으며, 사이버위협에 대한 국가 차원의 종합판단·상황관제, 위협요인 분석 및 합동조사 등을 하기 위하여 국가정보원 사이버안전센터에 민·관·군 합동대응반을 설치·운영토록 함

- 2015년에, 국내 정보보호 시장의 확대, 정보보호 전문가 양성, 세계 최고 수준의 정보보호 제품개발을 위하여 수요확충과 신시장 창출, 정보보호 전문인력의 체계적 양성 관리 및 세계적 정보보호 기업 육성 지원 등의 법적 근거를 마련하고, 정보보호산업의 기반 구축과 경쟁력을 강화함으로써 국민생활의 향상과 국민경제의 건전한 발전에 기여하고자 「정보보호산업의 진흥에 관한 법률」을 제정
  • 동 법 제2조 (정의)에서 정보보호[44], 정보보호산업[45], 정보보호기업[46] 및 이용자[47]에 대하여 규정하고 있다.

---

42) 국가정보원장 소속하에 국가사이버안전센터를 두며, 사이버안전센터의 주요 업무는 다음과 같음. ①국가 사이버안전정책의 수립 ② 전략회의 및 대책회의의 운영에 대한 지원 ③ 사이버위협 관련 정보의 수집·분석·전파 ④ 국가정보통신망의 안전성 확인 ⑤ 국가사이버안전메뉴얼의 작성배포 ⑥ 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원 ⑦ 외국과의 사이버위협 관련 정보의 협력

43) "사이버위기"란 사이버공격으로부터 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시설의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 말함.

44) 정보보호산업의 진흥에 관한 법률 제2조 (정의)에서 "정보보호"란 다음 각 목의 활동을 위한 관리적·기술적·물리적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다. 가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것 나. 암호 인증 인식 감시 등의 보안기술을 활용하여 재난 재해 범죄 등에 대응하거나 관련 장비 시설을 안전하게 운영하는 것

45) 정보보호산업의 진흥에 관한 법률 제2조 (정의)에서 "정보보호산업"이란 정보보호를 위한 기술(이하 "정보보호기술"이라 한다) 및 정보보호기술이 적용된 제품(이하 "정보보호제품"이라 한다)을 개발·생산 또는 유통하거나 이에 관련한 서비스(이하 "정보보호서비스"라 한다)를 제공하는 산업을 말한다.

46) 정보보호산업의 진흥에 관한 법률 제2조 (정의)에서 "정보보호기업"이란 정보보호산업과 관련된 경제활동(이하 "정보보호사업"이라 한다)을 영위하는 자를 말한다.

47) 정보보호산업의 진흥에 관한 법률 제2조 (정의)에서 "이용자"란 정보보호기업이 제공하는 정보보호기술, 정보보호제품 및 정보보호서비스 (이하 "정보보호기술등"이라 한다)를 이용하는 자를 말한다.

- 과학기술정보통신부장관은 정보보호산업의 진흥에 관한 정책목표 및 방향을 설정하기 위하여 진흥계획을 수립·시행하도록 하고 있으며, 정보보호와 관련한 공공 수요를 촉진하기 위하여 국가기관 등으로 하여금 정보보호제품, 정보보호서비스 등에 대한 구매수요정보를 과학기술정보통신부장관에게 제출하도록 하고, 공공기관은 정보보호시스템의 품질보장을 위한 적정 수준의 대가 지급을 위해 노력해야 하며, 과학기술정보통신부장관은 부당한 발주행위가 일어나지 않도록 조치하도록 하고 있다. 또한 공공기관의 장은 정보보호를 위한 관리적·물리적·기술적 방안을 마련하여야 하며, 정부는 공공기관의 정보보호 현황을 조사하여 정보보호를 위한 조치를 취할 수 있도록 하고 있다.
- 과학기술정보통신부장관은 정보보호산업과 그 밖의 산업 간의 융합을 촉진하기 위한 사업을 할 수 있으며, 정보보호기술의 개발, 투자 촉진 및 표준화 추진을 위한 사업을 할 수 있다.
- 과학기술부정보통신장관은 정보통신서비스 이용자의 안전을 위하여 정보보호준비도 평가를 수행하는 기관에 필요한 기술적 재정적 지원을 할 수 있도록 하고 있으며, 정보보호 시스템 수요 확대 및 정보통신서비스 이용자의 안전한 인터넷이용을 위하여 정보통신서비스제공자로 하여금 정보보호현황을 대통령령으로 정하는 바에 따라 공개할 수 있도록 하고 있으며, 정보보호제품의 품질확보·유통촉진·이용자 보호· 융합산업 활성화 들을 위하여 성능평가를 실시할 수 있도록 하고 있으며, 정보보호기업이 자율적으로 준수할 수 있는 이용자 보호지침을 정할 수 있도록 하고 있다.
- 과학기술정보통신부장관은 정보보호 전문인력을 육성하기 위한 시책을 수립 시행할 수 있고, 미래인재 및 해외 우수인력의 발굴 육성 사업과 학점이수 인턴제도를 추진할 수 있도록 하고 있다.
- 과학기술정보통신부장관은 주요정보통신기반시설의 취약점 분석·평가, 보호대책의 수립 업무 등을 안전하고 신뢰성 있게 수행할 수 있는 자를 정보보호 전문서비스 기업으로 지정·관리할 수 있다.
- 한편, 정보보호제품 및 정보보호서비스의 개발 이용 등에 관한 분쟁을 조정하기 위하여 정보보호산업 분쟁조정위원회를 설치하고, 정보보호산업과 관련된 사업을 경영하는 자가 과학기술정보통신장관의 인가를 받아 한국정보보호산업협회를 설립할 수 있도록 하고 있다.

Cybersecurity 분야 기술, 솔루션 및 인프라

Cybersecurity 기술 및 인프라

- Cybersecurity 시장은 플랫폼 및 솔루션 범주 전반에 걸쳐 본질적으로 다양화되고 있음. 주요 시장으로 부상하고 있는 IoT 패러다임은 또한 본질적으로 다양화를 촉진시켰음
  - 다양화된 분류는 하드웨어, 네트워크, 앱, 엔드포인트 노드, 산업 시스템, 클라우드 네트워크 시스템, 무선 시스템, 콘텐츠, 네트워크 게이트웨이 등을 포함하고 있음. 이 모든 것들은 구내에 또는 클라우드 플랫폼 상에 설치되고 있음

- 모든 분류들은 더욱 다양한 사이버보안 제품 및 솔루션을 창출하기 위해 범위를 개방하고 있음. 최초의 중요한 제품 및 솔루션 분류는 PRISAP (Prognostic-Receptive-Inspective-Supervisive-Analytical- Protective)의 범주 안에 묶일 수 있음
  - 예후 솔루션 : 예후 솔루션은 위협 및 공격의 사후예방적 평가를 나타내며, 사이버보안 솔루션의 기초로서 고려되고 있음. 이에 해당하는 사이버보안 제품 및 솔루션은 다음과 같은 것을 포함하고 있음. ① 통합된 위협 관리 ② 보안 및 취약성 관리 ③ 보안 사고 관리 ④ 게이트웨이 보안 관리 ⑤ 웹 필터링 관리 ⑥ 침투 테스트 솔루션 ⑦ 보안 형상 관리 ⑧ 액서스 거버넌스 ⑨ 정적 응용 프로그램 보안 테스트 ⑩ 동적 응용 프로그램 보안 테스트 ⑪ 상호작용 응용 프로그램 보안 테스트 ⑫ 위협 정보 ⑬ 보안 인식 ⑭ 사칭 방지
  - 수용성 솔루션 : 수용성 솔루션은 사고의 조사를 나타내는 것으로 필요한 변화를 하거나 보안 설계 및 모형을 변화시킴. 이에 해당하는 솔루션은 다음과 같음. ① 재해 복구 관리 ② 데이터 손실 방지 ③ 사고 관리/대응 ④ IT 서비스 관리 ⑤ 법의학 도구
  - 조사 솔루션 : 조사 솔루션은 사고의 우선순위를 나타냄. 이에 해당하는 솔루션은 다음과 같음. ① 보안 정보 및 이벤트 관리 소프트웨어 ② 리스크 평가 서비스 ③ 로그 관리 ④ 데이터 누출 방지 ⑤ 엔드포인트 탐지 및 대응 ⑥ 사기/거래 모니터링 ⑦ 속임수 도구
  - 감독 솔루션 : 감독 솔루션은 전체 시스템을 모니터하고 가이드하는 것을 나타내며, 보안 지식을 시스템에 주입시킴. 이에 해당하는 솔루션은 다음과 같음. ① 리스크 및 규정 준수 관리 ② 소셜 미디어 통제 ③ 관리 서비스[48] 솔루션

48) managed services는 사전예방적 차원에서 운영을 개선시키고 비용을 절감시키기 위해 관리책임, 기능, 및 전략적 방법 등을 아웃소싱시키는 행위를 말함.

④ IT 리스크 관리 ⑤ 위협 및 취약점 관리 ⑥ 보안 오케스트레이션 ⑦ 네트워크 보안 정책 관리 ⑧ 보안 운영, 분석, 레포팅 임.

- 분석 솔루션 : 분석 솔루션은 과거 사건의 분석, 상관 패턴의 분석, 및 보안 통찰력을 나타냄. 이에 해당하는 솔루션은 다음과 같음. ① 보안 분석 ② 사용자 및 법인체의 행위 분석
- 보호 솔루션 : 보호 솔루션은 감염 및 시스템을 격리시키고 공격방향을 전환시키는 작용을 함. ① 방어벽 솔루션 ② ID 및 액세스 관리 ③ 암호화 솔루션 ④ 엔드포인트 보호 관리 ⑤ 침투 탐지 시스템/침투 예방 시스템 ⑥ 앤티 바이러스/ 앤티 말웨어 제품 ⑦ 분산된 서비스 거부 완화 ⑧ 보안 시스템 통합 ⑨ 보안/매스킹 ⑩ 가상사설망 ⑪ 클라우드 액세스 보안 브로커 ⑫ 反 지능형 지속 공격 ⑬ 격리 ⑭ 기업 모바일 관리

◐ 기업의 Cybersecurity 인프라

- 기업, 산업 및 정부는 자신의 디지털 및 물리적 자산 그리고 정보 시스템을 위한 보안 정책을 채택할 필요가 있음. 보안 정책은 사이버보안의 잠재적 위험을 완화시키고, 손상을 통제하고, 생산성을 유지하고, 책임을 최소화하고, 조직의 재산권을 보호하고, 무결성 및 신뢰성을 강화시키기는 것을 목적으로 하고 있음
  - 보안 정책은 보안 아키텍처[49]를 정의하고 패스워드 변경, 컴퓨터 소프트웨어 사용, 앤티바이러스 사용 등과 같이 정보 또는 자산의 사용에 대하여 필요한 통제를 함. 보안 아키텍처를 정의하고 설계하는 것은 기업에게 가장 중요한 과업 중의 하나임

    ① 사용자 및 하드웨어 보호 시스템 예를 들어 고급 암호화 표준, 가상 사설망, 신뢰받을 수 있는 플랫폼 모듈, 컴퓨터 케이스 침투 탐지, 드라이브 록, USB 포트 비활성화, 모바일 지원 디바이스의 액서스 통제 등을 위한 컴퓨터 액서스 통제를 위한 가이드라인

    ② 바이러스 백신 소프트웨어 보안 코딩, 보안 설계 및 보안 OS를 포함하는 보안 응용 프로그램

    ③ 기업의 데이터 센터, 기계장치, 응용프로그램, 기타 소프트웨어 통제 자산 또는 시스템을 사용하기 위한 ID 인증 및 권한 개발

    ④ 데이터 중심의 보안 정책 개발

49) 보안 아키텍처 (security architecture)는 어떤 시나리오 또는 환경과 관련하여 위험의 잠재성을 해결하기 위한 통합화된 보안 설계를 말함. 이는 또한 보안 통제를 언제 그리고 어디에 적용할 것을 정함. 설계 과정은 일반적을 재생산이 가능함.

⑤ 네트워크 방어벽, 심층 패킷 조사, 화이트리스트, 무국적 방화벽, 액서스 통제 리스트, DDoS 완화, 데이터 누출 방지, 기타 시스템

⑥ 시스템 내의 비무장지대[50]를 포함한 프록시 서버 사용

⑦ 호스트 기반의 침투 탐지 시스템, 보안 운영 센터 등과 같은 침투, 탐지 및 예방 시스템 사용,

⑧ 편차, 서명, 및 샌드박싱[51], 송신자 정책 프레임워크, 도메인 키 식별 메일 등의 탐지,

⑨ 보안 정보 및 이벤트 관리 행위, 빅데이터 분석, APTs 활동, 시스템 로그, 공통 이벤트 형식[52], 보안 콘텐츠 자동화 프로토콜을 다루기 위한 보안 운영 센터 구축

⑩ 보안 침해에 대한 대응 시스템 개발 예를 들어 취약성 관리, 취약성 스캐너, 컴퓨터 웜, DNA 테스트, 법의학, 네트워크 관리자 등을 포함함.

⑪ 안전한 모바일 및 IoT의 엔드포인트 및 게이트웨이

- (내부 및 외부 위협) 내부 및 외부의 위협으로부터 보호하는 것은 조직에 있어서 동등하게 중요함. 사이버 위협의 대부분은 외부에서 발생되고 있음이 밝혀졌음. 예를 들어 영국 대기업의 2/3가 동일한 것을 2016년에 경험하였고, 영국 정부는 대기업이 설치할 수 있도록 사이버 필수 계획 (CES, Cyber Essentials Scheme)를 개발하였음

50) 컴퓨터 보안에서의 비무장지대는 조직의 내부 네트워크와 외부 네트워크 (일반적으로 인터넷) 사이에 위치한 서브넷을 말함. 내부 네트워크와 외부 네트워크가 DMZ로 연결할 수 있도록 허용하면서도, DMZ내의 컴퓨터는 오직 외부 네트워크에만 연결할 수 있도록 하고 있음.

51) sandbox는 외부로부터 들어온 프로그램이 보호된 영역에서만 동작해 시스템이 부정하게 조작되는 것을 막는 보안 형태임.

52) common log format은 서버의 로그 파일을 생성할 때, 웹 서버에 의해 사용도는 표준화된 텍스트 파일 포맷을 말함.

[표 4-2] 영국의 사이버 필수 계획

Cyber Essentials scheme
- Cyber Essentials scheme 는 영국 정부와 산업체 공동개발 한 것으로, 두가지의 기능을 수행하기 위함. - 이는 정부의 사이버 보안의 10단계 라는 상황하에서 공통의 인터넷 기반 위협으로의 위험을 감소시키기 위해서 모든 조직체가 구현해야할 기본적으로 통제해야 할 것을 명확하게 정리하고 있음. - 그리고, Assurance Framework를 통하여, 이는 조직체들이 고객, 투자자, 보험회사에게 그들이 이러한 필수적인 예방조치를 취하고 있었음을 알리는 메카니즘을 제공함.
사이버 보안의 10 단계
- 2012년에 발표되었으며, FTSE350 소속 기업의 2/3에 의해서 사용되고 있음. - 정보 리스크 관리 체계를 중심으로 하여 ① 네트워크 보안 ② 사용자 교육 및 인식 ③ 홈 및 모바일 워킹 ④ 안전한 형상, ⑤ 이동식 미디어 통제 ⑥ 사용자 권한 관리 ⑦ 사고 관리 ⑧ 모니터링 ⑨ 말웨어 예방 등임.
보증 프레임워크 (Assurance Framework)
- 보증 프레임워크는 저렴한 비용으로 실현가능하기 위해서 중소기업과 협의를 거쳐 설계되었음. - 두가지 옵션이 있으며, 이는 중소기업이 얻고자 하는 보증의 수준과 이것을 하기 위한 비용을 기준으로 선택할 수 있게 함. - 인증은 어느 시점에 기업의 사이버 보안 프랙티스의 스냅샷 만을 제공하고, 다른 한편으로 견고한 사이버 보안 상태를 유지하는 것은 추가적인 조치 예를 들어 견고한 리스크 관리 접근방법 등을 요구하고 있음을 인식하는 것이 중요함.

- (위협 정보 및 정보 공유) 실시간 위협 정보 및 상황 위협의 인식을 개발하는 것은 기업들이 사이버 위협을 탐지, 대응, 완화시키는 위해서 매우 중요함. 사업 동료, 산업 그룹, 및 정부 기관간에 정보를 공유하는 것은 위협 및 방어 메카니즘의 새로운 유형을 아는 데 도움이 되고 있음

- (지정학적 위협) 지정학적 위협은 국가의 지원을 받는 해커들이 기업 및 정부의 자원에 부당하게 액서스 하는 글로벌 조직들을 위한 새로운 도전적인 패러다임임
  - 조직체들은 각각 다른 툴로서 예를 들어 실시간 모니터링, 분석, 위협 탐지, ID 관리 등을 가지고 방어 메카니즘을 보호할 수 있음

- (운영 효율성) 운영의 효율성을 개발하는 것은 서비스 지속성 및 고객 신뢰를 위하여 매우 중요함. 조직체들은 사이버 위협 및 방어 이슈를 다루기 숙련된 전문가를 고용할 수 있음

- (경쟁우위로서의 사이버 보안) 조직체들은 위에서 언급한 견고한 사이버 보안 솔루션을 설치하여 경쟁 우위를 얻을 수 있음. 이 솔루션은 잠재적 위협 및 데이터 침해로부터 사전예방적으로 기업 데이터 및 정보를 보호할 것임
  - 궁극적으로 내부 및 외부 고객들은 기업의 제품 및 솔루션에서 신뢰를 얻고, 기업들은 경쟁우위를 얻음

Cybersecurity 분야 문제점

Cyber 위협의 패턴 및 데이터 유출

- 사이버 위협은 CVE (common vulnerability or exposure)에서 기록되는 시스템 취약점 및 흠집 들을 표현함
  - 컴퓨터 데이터베이스를 안전하게 하기 위해서, 여러 유형의 사이버 위협의 패턴을 아는 것이 중요함. 사이버 공격을 분류하는 것 중에는 암호시스템을 이용한 백도어 또는 알고리즘; DDoS; 소프트웨어 웜, 키로거, 은밀한 청취 장치, 무선 마우스, 디스 암호 및 신뢰할 수 있는 플랫폼 모듈과 같은 직접적인 액서스 공격; carnivore, naruslnsight, 및 TEMPEST와 같은 프로그램을 사용하는 도청; 스푸핑, 조작, 권한 에스컬레이션, 피싱, 클릭재킹, 거짓 CEO 이메일을 회계 및 금융 부서에 보내는 사회적 공학 등임

- 인터넷의 발전은 가장 큰 혁명 중의 하나임. 인터넷 사용의 증가로 사이버 안전에 대한 여러 유형의 취약점을 노출시킴. FBI는 사이버 사기의 비용이 2014~2015년에 미국 기업에 약 20억 불에 해당한다고 발표하였음. 사이버 위협의 유형은 다음과 같음
  - Malware : 말웨어는 악의적 의도가 주입된 코드로서, 주로 데이터를 훔치거나 다른 사람의 컴퓨터의 콘텐츠를 파괴하기 위해서 사용됨. 말웨어는 일반적으로 이메일에 첨부되어 들어오거나 소프트웨어 다운로드에 의해서 들어옴
  - Phishing : 최근에, 피싱 공격은 크게 증가하고 있음. 하나의 링크가 이메일을 통하여 보내지고, 사용자들은 그 링크를 열고 그들의 개인적인 정보를 입력하라고 요구받음. 이후에 개인적인 정보가 그들의 계좌에서 돈을 인출하거나 기타 금융적인 활동을 하도록 사용됨
  - Password attacks : 패스워드 공격은 사용자의 패스워드를 해독하여 사용자의 계좌에 접근하는 권한을 얻는 것에 관한 것임. 이러한 공격을 하기 위해서 악성 코드 또는 소프트웨어를 만들 필요가 없음. 그러나 해커들은 코드를 해독하기 위해서 소프트웨어를 사용할 수 있음

- Denial-Of-Service Attacks : Dos 공격은 서비스를 방해하기 위해서 상당한 양의 데이터를 네트워크에 주입시킴. 이러한 유형의 공격에서, 해커들은 네트워크에 과부화를 주는 데이터를 보내기 위해서 다양한 시스템을 사용함. 이는 네트웨어 오류 또는 네트워크의 오작동을 발생시킴. 가장 일반적인 유형의 DoS 공격은 분산화된 DDoS임
- Man in the Middle (MITM) : MITM은 어느 사용자가 WAP (Wireless Application Protocol), WPA (Wi-Fi Protected Access) 그리고 WPA2 등과 같은 안전 조치의 사용 없이 암호화되지 않은 무선 액서스 포인트에 접근 하려고 할 때 발생함
- Drive-By Downloads : 이러한 공격은 시스템에 다운로드 되는 동안에 사용자의 허가를 요구하지 않음. 이러한 파일들은 웹사이트에 첨부되어 있어서 사용자가가 이 사이트를 방문할 때, 이것이 사용자의 시스템에 자동적으로 다운로드 될 것임. 이러한 코드는 사용자의 운영 시스템에 영향을 미치며 시스템에 설치된 다양한 프로그램의 오작동을 유발시킴
- Malvertising : 이런 유형의 공격은 사용자가 광고에 클릭 할 때에 주로 발생함. 해커가 감염된 파일을 추가하거나 임시 네트워크의 도움으로 웹사이트에 광고를 보임. 이러한 광고는 광고 기준에 합치되는 다른 웹사이트에 배포됨. 광고에 클릭 함으로써, 말웨어는 시스템에 다운로드 되며, 연이어 시스템의 프로그램과 데이터에 영향을 미침
- Rogue software : 이러한 공격은 팝업의 도움으로 사용자의 스크린에 각각 다른 안전에 관한 경고문을 사용함으로써 시작됨. 사용자가 엡데이트에 동의하거나 프로그램이 다운로드 될 것을 허락한다면, 공격 받을 확률이 있음. 이 다운로드된 소프트웨어 시스템의 작동에 영향을 미칠 수 있음. 이러한 유형의 공격은 파이어월의 도움으로 최소화 될 수 있음

- 데이터 유출은 여러 방법으로 발생할 수 있음. 이는 랩탑 또는 휴대용 저장장치를 도난당하거나, 또는 외부자가 비밀의 정보에 접근하기 위하여 시스템을 침입하는 시도, 종업원이 실수로 내부 침입자에게 정보를 제공하는 종업원 과실 등의 경우임
  - 데이터 유출을 발생시키는 여러 이유 중에서, 해킹과 말웨어가 가장 일반적이며 빠르게 성장하는 이유로 밝혀져 왔음. 예를 들어 2014년에, 재정적 이득을 빼앗으려는 악의적 해커들이 사이버 범죄 중 가장 높은 비율을 차지하고 있으며, 이는 데이터 유출의 60%에 해당하며, 그 다음으로 지적재산권을 훔치는 의도를 가진 해커가 따르고 있음

• 데이터 유출의 수가 증가하고 있으며, 다른 한편으로는 데이터 유출의 비용도 또한 최근에 상승하고 있음. 2014년에 데이터 유출로 인해 발생한 비용이 평균적으로 15 % 상승하였으며, 이는 한 조직에 350 만 달러의 비용을 추가적으로 부담하게 하였음. 재정적인 비용 뿐만 아니라 기업들은 브랜드 및 평판에도 손상을 입게 되었으며, 이들의 고객 신뢰 및 브랜드 이미지를 회복하기 위하여 수백만 달러를 지출해야 함

[표 4-3] 데이터 유출의 비용

데이터 유출의 비용
- 사이버 범죄는 적대적인 국가의 지원을 받은 공격으로 2017~2022 년 사이에 누적치로 6조 달러 이상의 손실을 입히고 있음. - 이 예측치에는 데이터의 손상 및 파괴, 도난 당한 돈, 생산성 저하, 지적재산권 절도, 개인 및 금융 데이터의 절도, 도용, 사기, 비즈니스의 정상적인 과정에 공격후 중단, 법의학적 조사, 해킹 당한 데이터 및 시스템의 회복 및 폐기, 평판의 위험 등이 포함됨. - 데이터 유출의 60% 이상이 북미에서 발생하고 있으며 평균비용은 2022년 까지 1.5억 달러로 추산되고 있음.

• 민감한 데이터를 보호하고 공격의 복잡성을 방지하기 위해서, 조직들은 암호화를 채택하고 있음. 암호화는 해킹, 말웨어, 도둑, 등으로부터 데이터 유출을 방지하기 위한 단순하면서도 강력한 솔루션을 제공함. 암호화는 사이버 공격을 최소화하는 매우 효과적인 안전 메카니즘이라는 것을 증명하였음

• 지금까지 발생한 데이터 유출 중 주목할 것들은 Home Depot, ebay, Michaels Stores, JP Morgan Chase, 한국의 은행들 (KB 금융지주회사, 농협금융 지주회사, 롯데 그룹), Community Health Systems 등이 공격을 받았음

산업에서의 사이버 위협

- 대부분의 산업 부문들이 지난 2~3년 사이에 사이버 공격에 대해 영향을 받고 있음. 10명의 사이버 보안 담당 중의 8명이 자신들의 회사가 업계 전반에 걸쳐 지난 24개월 사이에 사이버 공격에 의해 피해를 받았다고 응답하였음
  • 산업별로는 소매업의 89%, 자동차산업의 85%, 은행업의 76% 가 피해를 입었다고 발표되었음. 그러나 사이버 솔루션의 지출 측면에서 보면, 금융, 정부 및 공익기관, 통신 및 IT, 항공 및 국방, 의료 부문으로 나타났음

- 모든 기업들이 사이버 보안에 투자하고 있지 않은 것으로 보여짐. 단지 49%

만이 2016년 사이버 보안에 투자하였음. 업종별로는 2016년에 자동차 기업의 32% 만이 투자하였으며, 금융이 66%, 통신 및 IT 부문에서 62%가 투자하였음

- 또한 모든 기업들이 사이버 보안 이슈를 해결하기 위해서 인적 자원을 투입하는 것이 아니고, 단지 69% 만이 인적 자원을 투입하고 있음. 금융업의 85%, 자동차산업의 45%가 사이버 보안에 대처하기 위해서 인적 자원을 투입하였음

- 금융 시스템이 사이버 공격을 받기 쉬운 영역으로서, 신용 카드, 은행 계좌, ATM 부스, PIN, 및 외환 등이 공격의 대상이 되고 있음. 산업 장비 및 유틸리티가 사이버 공격을 받기 쉬운 영역으로서, 파워 그리드, 원자력 발전소, 연결된 기계류, 스마트 미터, 연결된 네트워크가 공격의 대상임. 유사한 것들이 항공, 소비자 디바이스, 대기업, 자동차, 정부, IoT 디바이스 및 네트워크, 의료 부문에서 나타나고 있음
  - 2017년에 금융 부문이 사이버 공격 및 사이버 지출의 선두를 달리고 있음. 2015년에 Kaspersky 랩 솔루션이 온라인 뱅킹 영역에서의 200만건 컴퓨터 공격을 봉쇄하였는 데, 이는 2014년에 비해 2.8%가 증가한 것임. 금융 부문에서 사이버 공격을 받은 사용자의 비율을 상위에 있는 국가별로 보면 다음과 같음. ① 싱가폴 (11.6 %), ② 오스트리아 (10.6 %) ③ 스위스 (10.6 %) ④ 호주 (10.1 %), ⑤ 뉴질랜드 (10.0 %), ⑥ 브라질 (9.8 %), ⑦ 나미비아 (9.3 %), ⑧ 홍콩 (9.0 %), ⑨ 남아프리카공화국 (8.2 %), ⑩ 레바논 (6.6 %) 임

Cybercrime의 증가

- 디지틀 기술이 비즈니스와 서비스를 지속적으로 변혁시키고 있으며, 사이버 범죄가 산업 분야에서 급증하고 있음. 2016년에, 사이버 범죄가 사이버 위협 중에서 2번째로 많은 경제적 피해를 입혔다고 보고되고 있음
  - 사이버 위반은 모든 비즈니스와 서비스 사업자를 해치는 것을 시작함. 사이버 범죄로부터 보호하는 것은 비즈니스와 조직의 경쟁 우위를 확보하는 데 매우 중요
  - 한 조사연구는 조직의 32%가 사이버 범죄에 의해 영향을 받았으며, 매해 1억불 이상의 비용을 부담하고 있음을 밝히고 있음. 이들 중에서 56%는 위협의 강도를 알지도 못한 채로, 손실을 입었음. 2016년에 전체적으로 사이버 범죄가 53% 증가
  - 2017년에, 사이버 범죄는 34% 이상의 조직을 대상으로 하여 더욱 증가할 것으로 추산되고 있음. 방어 측면에서, 대부분의 조직들은 사이버 범죄에 대비가

되어 있지 못하며, 37%의 조직만이 실제적으로 잠재적 사이버 범죄에 대응할 확고한 계획을 가지고 있을 뿐임

- 사이버 범죄는 IT 문제만이 아니고 비즈니스에 모든 국면에 영향에 미치는 것임

사이버 위협을 초래하는 BYOD (Bring your own device)

- Mind Commerce사는 2020년 까지 작업장에서 20억개 이상의 BYOD 디바이스가 연결될 것이라고 예측하고 있음. 이는 기업의 생태계를 말웨어 및 사이버 위협에 더욱 취약하게 할 것임. 세계적으로 71% 기업들이 BYOD를 채택하면서 데이터 보안 이슈를 고려하고 있음. 한편으로는 다른 유형의 보안 이슈를 고려하지 않고 있음
  - 대부분의 경우에, BYOD는 기업을 위한 필수품으로 되었음. 기업들이 개인 디바이스로 기업 정보 또는 데이터의 사용을 제한시키는 정책을 사용하지만, BYOD는 기업의 디바이스 및 네트워크 생태계를 사이버 공격에 더욱 취약한 것으로 만들고 있으며 효과적인 보안 정책의 실현을 매우 어렵게 하고 있음.

랜섬웨어 증가

- 램섬웨어는 최근에 부당한 이득을 얻기 위해서 사이버 범죄, 랜섬웨어에 인질된 사용자들의 PC 또는 인터넷에 연결된 디바이스을 대상으로 크게 증가하고 있음. 이는 디바이스 데이터를 무단으로 수정하거나 컴퓨터의 정상 작동을 봉쇄하여 궁극적으로는 컴퓨터 또는 연결된 디바이스가 작동하지 못하도록 하고 있음
  - 암호화는 PC, 스마트폰, 리눅스 시스템 및 IoT 디바이스 플랫폼을 포함하는 모든 플랫폼에 침투하여, 랜섬웨어 공격을 시도하는 방법임. 암호화는 침투받는 자들로부터 파일을 해독하거나 컴퓨터가 말웨어로부터 차단되어 있는 것을 해제하기 위하여 돈 또는 다른 중요한 것을 요구함
    * 랜섬웨어는 2015년에 전년도에 비해 35 % 증가하였음. 좋은 예시 중의 하나는 14,000 암호화 키를 탐지하는 네덜란드 경찰에 의해 코인볼트 말웨어(CoinVault malware)에 대한 용의자 2명을 체포한 것을 포함함. 2015년에, 텔스라크립트 (TeslaCrypt)의 발생은 그래픽 인터페이스를 사용한 암호화로서 주요한 사건중의 하나임. 트로이 목마 랜섬 말웨어가 또한 2015년에 급격하게 증가하였음. Kaspersky Lab은 약 800만개의 트로이 목마 랜섬 말웨어에 감염된 컴퓨터를 탐지하였음

* 암호해독기 수정은 2015년에 2배로 증가하였음. 2014년에 3064건에서 2015년 6835 건으로 증가하였음
* 트로이 목마 암호화 말웨어에 의해 공격 받은 사용자의 수도 2015년에 급격히 증가하였으며, 2014년에 12,084 명에서 2015년 179,209 명 이었음

• 이스트소프트가 발표한 '2016년 랜섬웨어 동향 결산'에 따르면, 2016년 랜섬웨어 공격은 총 397만 4,658건으로 해마다 증가하고 있으며 사이버보안 위협도 점차 높아지고 있음. 2013년 강력한 암호와 알로리즘 기술을 적용한 랜섬웨어 '크립토락커 (CryptoLocker)'가 등장하면서 관련 피해가 급증하고 있는 추세임. (참조 : 2010년대의 해킹)

• 랜섬웨어 피해 규모는 2015년 3억 2,500만 달러에서 2017년 50억 달러로 2년 동안에 15배 증가했으며, 보안 회사들은 특히 의료기관에 대한 랜섬웨어 공격이 2020년 까지 4배 늘어날 것으로 예상하고 있음

[표 4-4] 2016년 랜섬웨어로 인한 피해 사례

2016년 랜섬웨어로 인한 피해 사례
- 2016년 초, 리눅스 웹서버 및 백업 서버 153대를 감염시킨 에레버스(Erebus) 랜섬웨어 공격으로 웹호스팅업체 '인터넷나야나'의 고객사 웹사이트 3,400여개가 일시에 마비되었음. - 이 업체는 해커들에게 13억원의 거액의 보상금을 주기로 합의하였는데, 이 금액은 랜섬웨어에 대한 사상 최고 보상금으로 기록되고 있음. 이로 인해 한국에 대한 해커들의 랜섬웨어에 대한 공격이 거세질 것으로 우려되고 있음.

◐ 사이버 전쟁 및 사이버 테러

- 각국 정부는 최근에 발생되는 사이버 전쟁 및 사이버 테러를 매우 우려하고 있음. 사이버 전쟁 및 사이버 테러는 새로운 전쟁의 개념으로 자금을 지원 받은 범죄자들이 지구 반대편에서 클릭 마우스로 전쟁을 일으키는 것을 말함
  • 첫 번째 동기는 무기화되고 있는 컴퓨터 프로그램을 파괴하는 것이고 또는 주요 기반 산업 예를 들어 운송, 통신 및 에너지 산업을 파괴시키는 것임. 이는 군의 네트워크가 군대, 제트기, 명령 및 전함의 통제를 불가능하게 할 수 있음

◐ 다크넷[53] 및 Cybersecurity

- 다크넷은 사이버 범죄 및 사이버 보안과 밀접한 관계를 가짐. 다크넷은 보이지 않는

53) 다크넷 (darknet)은 비표준화된 통신프로토콜 및 포트를 주로 사용하면서, 특정한 소프트웨어, 형상, 권한만을 가지고 액서스할 수 있는 오버레이 네트워크를 말함.

웹으로서, 보호되는 데이터 베이스, 웹사이트, 국가 및 주정부 기록, 인트라넷, 게시판, 웹사이트 아카이브, 포럼, 분류된 광과 및 온라인 도서관 캐털로그를 포함함

- 사이버 범죄자들은 다크넷 재산을 훔치기 위해서 새로운 방법들을 찾아내고 있음. 이러한 재산을 보호하는 것은 기업, 정부 및 다른 법인체 들에게 매우 중요

IoT 도메인에서의 Cybersecurity

- 연결된 IoT 디바이스는 사이버 범죄에 새로운 힘을 견인시키고 있는 데, 물리적 개체 또는 디바이스 또는 시스템을 보호하는 것으로부터 연결된 디바이스, 개체 또는 사물들을 통제하기 위하여 IoT 네트웨크 또는 도메인 상의 가상 앱들로 초점을 이동시키고 있음
  - 이는 또한 IoT 보안에 관한 지출을 견인하여, 사이버 보안 시장을 17% 까지 증가시켰음

* IoT 영역에서의 사이버 보안 지출은 200억불에서 2022년에 350억불로 증가하였음
* 미라이 사기단 (Mirai Exploits)에 의한 독일텔레콤의 IoT 라우터가 해킹 당한 것은 IoT 침투의 패턴을 보여주신 예시임. 통신사업자들은 IoT 도메인에는 안전한 백도어가 없을 때에는 크게 고민할 필요가 있음

산업차원에서의 Cybersecurity 및 IoT

- 산업차원의 IoT가 IT 환경과 OT 환경을 융합시킴에 따라 Cybersecurity는 산업 공간에서 더욱 중요하게 됨
  - IoT는 산업 인프라를 디지털화 과정으로 가져오게 함. 이는 외부 위협에 범위를 확장시키는 결과를 초래함. 심지어 난방 시스템 환기, 공조 시스템/설비, 전력 조절, 비디오 시스템, 소방 안전 시스템 및 기타 유사 시스템은 산업의 데이터센터에 무단으로 액세스 하기 위해서 안전의 취약점일 수 있음
  - 사이버 공격은 종업원 과실 또는 의도적 손상을 통하여 발생할 수 있음. 따라서 각각의 연결된 시스템 내에서의 위협 가능성을 주의 깊게 평가하는 작업은 매우 중요함

Cybersecurity 분야 IDX 추진 필요성

IDX 추진 필요성 : Cybersecurity 패러다임 변화의 관점

- 지난 40년간 각 산업 분야의 효율성을 높이기 위한 보조적인 수단으로서, 무어의 법칙에 기반을 둔 반도체 칩 기술진화에 따른 컴퓨팅 파워에 힘입어, 디

지털화가 진행되었음. 최근에는 ICT 산업은 물론 비ICT 산업 등 모든 산업이 기존 아날로그 방식을 탈피하여 디지털로 전환되는 디지털 트랜스포메이션(Digital transformation)이 일반적인 추세임

- 예를 들어 항공기의 전자부품 비중이 2005년 10 % 에서 2013년 30 %로, 의료기기 중 전자의료의 기기 비중이 2005년 10 % 에서 2013년 45 %로, 자동차의 전자 부품 비중이 2005년 23 %에서 2013년 60 %로 가파르게 상승하고 있음이 디지털 트랜스포메이션이 급격하에 추진되고 있음을 증거하고 있음.

- 향후에는 국가 전반에 걸쳐 모든 산업 분야를 포함한 거시적 및 미시적 경제 시스템의 디지털 포메이션이 한층 가속화 될 것임. 경제시스템은 크게 3가지의 하위 시스템으로 구성되고 있으며, ① 생산시스템 ② 소비 시스템 ③ 생산과 소비를 연결하는 제 3의 시스템 등임. 이들 각각이 디지털 트랜스포메이션화 될 것이며, 이들이 상호 연동 되어 운영될 것임. 특히 생산과 소비를 연결하는 제 3의 시스템은 CPS 및 IoT가 주요 구성요소로 자리 잡을 것임. 또한 CPS 와 IoT가 전방에 있는 생산시스템과 후방에 있는 소비시스템을 연결하는 가교의 역할을 할 것임

  - 그러나, 이렇게 추진되는 디지털 트랜스포메이션은 사이버 보안의 패러다임을 크게 변화시킬 것임. 지금까지 현재의 획일화된, 개별 솔루션 중심에서 향후에는 경제 전반에 걸쳐 지속적으로 전개되고 있는 디지털 트랜스포메이션에 기반을 둔 디지털 비즈니스 형태에 적합한 맞춤형 보안으로 변화해야 할 것임.

[표 4-5] 디지털 트랜스포메이션 환경하에서의 사이버 보안의 관점의 변화

구분	AS-IS	To-be
보안 대상	PC, 모바일 기기, 저장된 데이터	IoT 센서, 스마트 기기, 지속적으로 생산 되는 데이터, 사회 기반 시설, 사람, 환경 등
보안 아키텍처	내부망과 외부망 사이의 경계에 보안 솔루션을 다수 설치하는 형태	단말, 플랫폼, 그리고 최종적으로 이를 이용하는 사용자 (기업 및 가정 등)를 통합하는 보안 정책
보안 기술 개발 방식	선 하드웨어 제작 및 후 보안 기술 개발	하드웨어 또는 소프트웨어의 설계 시점부터 보안 기술 개발 : 예시, Security by Design의 고도화

◐ IDX 추진 필요성 : Cybersecurity 도전과제 관점

- (**기업 자산- 서비스 중심**) IDX 플랫폼 상에서 더 큰 범위의 위협을 탐지하기 위해서, 기업에 가치가 있는 것은 반드시 고려되어야 함. 보안의 관점에서 시스템, 시스템의 구성요소 뿐만 아니라 서비스가 기업의 핵심 자산으로서 고려되어져야 함
  - 따라서 지금까지는 제품을 만드는 생산시스템의 가용성이 초점이었다면 IDX 플랫폼 상에서는 기밀성이 중요하게 되고 있음. 서비스 형태를 갖춘 추가 자산은 제품에 도입되거나 통합되는 새로운 트렌드와 새로운 기술로 인해 존재
  - 이러한 추가 자산은 IT 시스템들이며, 과거에는 중심 역할을 하지 못하였거나, 존재하지도 않았으며, 또는 고립된 영역에서 운영되었음. 이들의 예시로는 제품 및 구성요소의 디지털 ID 또는 전자적으로 협상된 계약서의 법적 안정성 이슈 및 관리 등임

- (**가용성 및 신뢰성**) IDX 플랫폼 상에서는 기업의 프로세스가 시스템, 기계 및 IT 시스템들에 더 많이 지원될 것이며, 조직간 의사소통 및 동적인 성향이 증가한 운영 시스템을 위해 인터페이스가 더욱 늘어날 것임. 이들 시스템 및 인터페이스를 사용할 수 없다면, 이는 기업 프로세스, 가치 창출 및 재정적인 측면에 적지 않은 영향을 미칠 것임
  - 제품 및 기타 서비스에 미치는 중대한 혼란은 기업적인 직접적인 위협이 될 것이며, 예를 들어 물리적 침해를 막기 위한 조치를 취해야 하는 과정에서의 추

가적인 위협이 가능하게 됨

- DDoS 공격은 외부적으로 접속가능한 모든 인터페이스에 리스크를 가하고, 공격에 대응하여 안전성을 확보하는 어렵게 하고 있음. IDX 플랫폼 상에서는 이러한 DDoS를 위한 공격에 추가적인 지점을 제공하면서 시간요소가 중요한 역할을 하는 프로세스 및 서비스가 다수 존재함
- SCADA (supervisory control and data acquisition) 시스템은 각각 다른 시스템으로 부여 받은 각각 다른 프로세스 데이터를 계산하여 자동화 시켜 통제 명령을 포워드 시키고 있는 데, 이때 통제 명령을 산출하기 위해 요구되는 데이터에 영향을 미치는 통신 에러는 IDX 플랫폼 상에서는 매우 큰 도전과제가 될 것임

- (**가용성에 대한 비간접적 공격 및 안전 기능에 대한 공격**) 어느 기업 내에서 네트워킹 및 자원의 집단적 사용의 빈도가 많아짐에 따라, 안전을 위한 구성요소에도 동일한 현상이 발생할 수 있음. 그 결과 안전을 위한 구성요소가 공통 네트워르 내에서 기타 시스템과 묶여서 운영되고 있음. 이는 안전을 위한 구성요소가 기타 구성요소와 마찬가지로 네트워크를 통하여 공격을 받고 있음을 의미함. 동시에 안전 기능에 관한 공격 및 가용성에 관한 비간접적인 공격이 가능하게 되고 있음

가용성에 대한 비간접적 공격
- 안전 기능에 대한 공격은 IDX 플랫폼 상의 시스템 및 기계장치의 긴급정지의 위협을 가함. - 이것은 예를 들어, 구성요소에 수많은 요구를 통하여 과부화가 걸리게 하거나, 사용 중인 네트워크에 과부화를 걸리게 하거나, 지정된 안전 기능을 활성케 하는 구성 요소에 소프트웨어 에러 등에 의해서 발생할 수 있음. - 안전 구성요소의 실제 기능은 이러한 경우에 손상되지 않고 그대로 남아있고, 사람 또는 환경에는 위험이 없으나, 예를 들어 IDX 플랫폼에 연결되어 있는 생산 프로세스에는 손상이 있을 수 있음.
안전 기능에 대한 공격
- 최악의 시나리오로서, 안전 기능을 가진 구성 요소의 취약성을 악용하는 것은 기능을 조작하게 함. 예를 들어 임계값의 수정 등임. 이것은 기능상의 안전 및 보안이 이미 확보될 수 가 없게 함. 이러한 경우에, 사람이나 환경에 대한 피해는 단지 추가적인 보호조치에 의해서만 보장될 수 있음. 관련 보호 기능이 법적 지침에 따라 규정되면서 (예를 들어 Machine Directive), 안전에 관한 요구사항을 충족시키기 위해 보안 요구를 통합하는 것은 표준화 위원회 등에서 이미 해결되고 있음.

- (**무결성**) IDX 플랫폼상에 연결되어 있는 생산시스템의 생산을 위한 데이터와 기록되어 있는 데이터의 무결성이 매우 중요해 지고 있음
  - 생산을 위해 사용된 데이터에 대한 공격은 제품에 품질에 부정적인 영향을 미칠 것임. 극단적인 경우에서는, 안전과 관련이 있는 제품의 특성이 변경되어 사람 또는 재산에 상당한 피해를 줄 수 있을 것임
  - 생산 프로세스를 추적하는 기록의 무결성 역시 중요함. 이는 제약 산업에서와 마찬가지로 책임 문제 또는 규제 지침 때문임
  - 상기한 이유로 인해, 거의 모든 산업 부문에서 암묵적으로 신뢰성이 관련 이해당사자 사이에서 가장 중요한 것으로 인지되는 경우에는 무결성을 우선시하고 있음
  - IDX 플랫폼과 연결된 조직간의 가치 네트워크에서는 무결성이 확실성의 문제와 추가적으로 연결되어 보완되고 있음. 특히 정확한 동시성이 프로세스 조정을 위해 요구되고 있기 때문에, 시간의 무결성은 매우 중요한 요소가 되고 있음

- (**기밀성**) 대부분의 경우에 시간이 제한되어 있는 정보는 기밀성 유지를 위한 취급을 해야함. 이는 설계 데이터 또는 통제 프로그램을 포함함. 이러한 데이터는 이것을 얻기 위해서 지출되는 자원 및 지식으로 인해 기업에게는 상당한 가치를 갖는 자산임.
  - “데이터 도용”은 정보의 바람직하지 않는 방향으로의 흘러가는 데 사용되는 것임. 그러나, 이 데이터는 원본 데이터는 그대로 남겨둔 채로 복사된 상태이므로 정확성은 떨어질 수 있음. “데이터 도용”을 둘러싼 중요한 도전은 이것이 쉽사리 주시되지 않는 다는 것임
  - 데이터 도용 또는 데이터의 무단 액세스에서의 특정한 문제는 프로세스를 원상으로 돌리거나 보호조치를 취하는 등의 옵션이 부족함. 데이터 손실의 첫 번째 경우로부터, 기업은 무단 액세스가 연이어 이어지는 경우에 대하여 완전한 통제권을 잃게 하고 있음. 안전의 경우에서처럼 후퇴라는 것이 없음. 따라서 기획단계에서 관련 조치를 고려하는 것이 추천되고 있음. 이를 통하여 기업에 중요성이 있는 데이터가 중요도에 따라 표시가 되고 이러한 데이트 적절한 취급이 공식화되는 것이 보장되어야 함
  - 지금까지는, 기업이 스스로가 도난 당하거나 밖으로 알려지는 못하도록 하는 책임을 지고 있었음. IDX 플랫폼 상에서는 이러한 책임이 관련된 기업으로 확장되어 갈것임. 따라서 중요 정보가 기밀성을 유지하면서 취급되는 것을 보장하기 위해서, 레벨링, 취급 및 책임에 대하여 적합한 규칙을 정의하는 것이 중요함. 데이터를 분류할 경우에, IDX 플랫폼 상에 연결된 스마트 팩토리가 있는

경우에, 최종 제품, 또는 기계에 관한 데이터는 기업의 통제 범위를 넘어선 것으로 고려되어져야 함. 최종 제품의 차원은 경쟁자에 의해서 결정될 수 있음. 이러한 경우에 공개에 앞서 기밀성이 특히 중요하나, 나중에 제품을 기반으로 한 재구축은 매우 쉽게 됨

- (**ID 도용**) 신뢰에 기반한 관계는 안전 조치와 관련하여 중요한 역할을 함. : 예를 들어 웹사이트를 방문하면, 사용자는 전송된 주소가 그를 해로운 웹사이트로 이동시키지 않을 것을 신뢰함. 이는 나쁜 목적으로 조작될 여지는 있음. 또한 웹서비스를 로그하고 있는 사용자가 자신이 누구인가를 밝히는 것을 신뢰함. 이렇게 신뢰에 기반한 관계는 사적 거래와 기업간 거래에도 적용되고 일반적으로 안전 조치에 의해서 지원되고 있음
  - ID 도용의 위험은 공격자가 전혀 다른 사람이라는 것을 밝히고, 이 사람의 합법적인 액서스 권리를 받은 경우에 발생함. 액서스 프로토콜에서의 인증은 공격자를 실질적이며 합법적인 사용자로부터 구별할 수가 없음. 위험을 줄이는 방법이 있음. 실제 사용자가 시스템에 로그인 할 때, 그가 잠재적인 보안 침해자인가를 알려주며, 이것을 확인하거나 부인할 수 있음. 다양한 경우에, 해당 인물과의 상호작용이 확인을 위해서 요구됨. 피드백을 받은 후에, 확인 과정이 개선될 수 있으며 어떤 지점에서는 완전 자동화 될 수 있음
  - IDX 플랫폼 상에서, ID 도용은 시스템의 가용성과 정보의 기밀성에 심각한 위협을 줄 수 있음

    * 사람, 서비스, 시스템 및 관련된 센서의 자리들은 동태적으로 변화될 수 있음. 이는 수많은 ID 및 수많은 공격 가능한 벡터가 있음을 의미함. 또한, 기계는 의사결정을 하는 데 있어서 융통성이 있을 수가 없음. 이는 보안 조치를 인식하고 개선하고 자동화하는 것을 어렵게 함. 여기서의 문제는 머신-머신의 식별과는 거의 관련성이 없으며, 공격자가 기계라고 주장하는 것과 깊이 관련성이 있음. ID 요소 예를 들어 로그인 데이터, 통신 행위 또는 데이터 볼륨 등의 범위를 기록하고, 조사를 위해 잠재적인 신원 도용과 관련된 사례를 전달할 중앙집중적인 감시 체계가 요구되고 있음

◐ IDX 추진의 필요성 : K-ICT 시큐리티 발전 전략 관점

- 2015년 「정보보호산업 진흥에 관한 법률」을 제정 공포하면서, 미래창조과학부는 「K-ICT 발전 전략」을 발표하였음. 이는 우리나라 정보보호 산업이 선진국 대비 산업기반, 전문인력 및 연구개발 등 기초체력이 부족하고, 국내 정

보보호업체 대부분이 영세· 중소기업 이라는 실정을 바탕으로 하면서, 기존 산업과 ICT가 융합되어 디지털 트랜스포메이션 시대가 급속하게 도래하여 사이버위협이 개인정보 유출이나 단순한 금전 탈취 등을 넘어 국가 사회적 혼란을 유발하고, 국가 안보를 위협하는 수준으로 진화하고 있는 현실적 인식을 바탕으로 하고 있음

- 이 발전 전략은 사이버 보안 복원력 제고를 투자 확대에 중점을 두고 있으며, 전략적 추진 과제로서 사전 예방 중심의 사이버 보안 대응 체계 (Secure Dome)을 구축하고, 정보보호 사각지대 없는 민간 주도의 사이버 보안을 강화하겠다는 의지를 표명한 바 있음.

[표 4-6] K-security 전략

전략과제	세부내용
사전 예방 중심의 사이버보안 대응 체계 구축	- 민간분야 주요시설 (ISP, 기반시설 등) 및 다중이용서비스 (CDN·웹하드·공유기 등의 보안 강화를 위한 사이버안전 대진단 실 ('15년 : 400개) - 사이버 공격의 신속한 탐지 및 대응범위 확대를 위한 '사이버 심층 탐지 체계 (DID : Detection In-depth)' 확충 - 해커 유인용 '사이버트랩' 구축 (10만개)을 통한 전자금융사기 탐지·예방 강화 및 스마트폰· 공유기· CCTV 등 '생활기기' 보안 강화 추진 - 위협정보· 침해사고 대응 등 실시간 정보공유를 위하여 정부와 주요 기업 (이통사, 포털) '정보보호 최고책임자 핫라인(3,000 명) 구축 (15년~)
정보보호 사각지대 없는 민간 주도의 사이버 보안 강화	- 민간 주요통신기반시설 외부 관리인력 및 위탁 용역, 구매 조달 등 공급망 전단계에 대한 보안 강화 ('16~'17) - 산업제어시스템 등 주요 기반시설 지정 확대 ('17년, 400개, 정보공유 분석센터 확대 (4개-> 7개) 구축 지원 ('15~'17년) ● 현재 통신, 금융, 증권, 지자체 -> 에너지, 의료, 교육 분야로 확대 구축 - 정보보호 사각지대 해소를 위한 중소 영세 기업에 대한 정보보호 지원을 위한 '전국 118 정보보호 지원 체계' 구축 ('15년) - 기업간 정보보호 격차해소를 위하여 보안 취약점 바우처 프로그램 추진 ('16년~)

- IDX 추진의 필요성 : IDX 추진의 핵심 구성요소인 CPS (Cyber-Physical systems) 관점

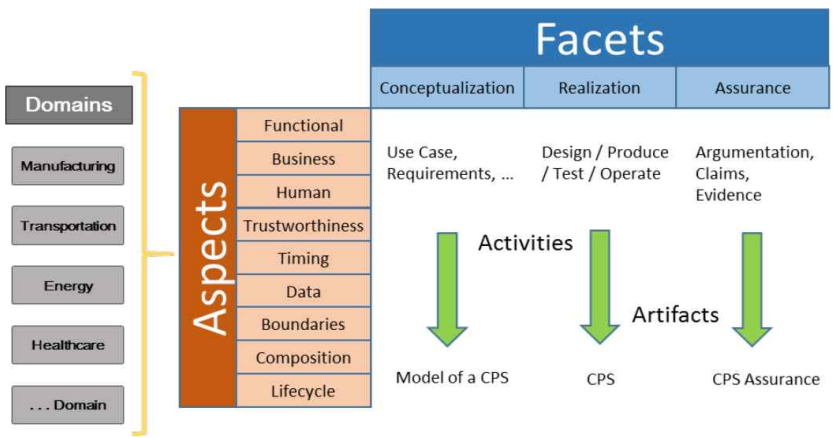
  - CPS는 인터넷과 사용자가 밀접하게 통합된 메카니즘으로, 컴퓨터 기반의 알고리즘에 의해 통제되거나 모니터 되는 것임. CPS에서는 물리적 및 소프트웨어 구성요소가 깊숙하게 얽혀 있으면서, 각각 다른 공간 및 시간 내에서 운용되며, 다양하고 독특한 행동양식을 보이고, 상황과 함께 변화하는 방법으로 상호 작용하고 있음[54)]

    • 지금까지 운영되고 있는 CPS로서는 스마트 그리드, 자율 자동차 시스템, 의료 장치 모니터링, 프로세스 통제 시스템, 로봇 시스템 및 자동 조정 항공 전자공학 등이 있음

  - CPS는 사이버너틱스, 메가트로닉스, 설계 및 프로세스 과학을 융합시켜, 다분야 접근법을 활용하고 있음. CPS는 IoT와 기본적인 아키텍처를 공유하고 있어서 IoT와 유사한 점이 있으나, CPS는 IoT와 비교하여 물리적 및 사이버 구성 요소 간에 통합 및 조정이 더욱 긴밀하게 이루어지고 있음

    • CPS 계열로서 이전에 운영되는 것은 항공, 자동차, 화학 프로세스, 토목, 에너지, 의료, 제조, 운송, 및 소비자 가전기기 등의 분야 등에서 발견되었음

  - NIST는 2017년에 CPS 프레임워크를 발표하였음. CPS 프레임워크의 주요 요소는 다음 그림과 같음



[그림 4-7] NIST CPS 프레임워크

54) "US National Science Foundation, Cyber-Physical Systems (CPS)

- 도메인은 CPS를 적용하는 분야를 가리키며, 예를 들어, 제조업, 운송, 에너지, 의료 등등의 분야를 포함함.
- Aspects은 개념적으로 Concerns과 동일하거나 관련된 것임. Concerns은 이해당사자가 개별적 또는 집단적으로 가지는 관점으로 표현되는 것으로서 CPS 프레임워크 방법론을 이끌어가는 원천적인 개념임. Aspects는 에 의해서 표현 기능적, 비즈니스적, 인간적, 신뢰, 타이밍, 데이터, 바운더리, 컴포지션, 및 라이프싸이클 등으로 분류되고 있음. 이중 Cybersecurity와 직접적으로 관련되는 신뢰는 다음과 같이 Concerns으로 세분류하고 있으며, CPS 내에서 Security를 보장할 수 있는 조치를 찾고 있음을 알 수 있음.

[표 4-7] CPS의 security의 예시

Aspect	Concern	설명
Trustworthiness	privacy	CPS가 개체 (사람, 기계)가 CPS 안에 저장되거나 CPS 에 의해 만들어지는 데이터에 액세스하지 못하도록 방지할 수 있는 능력에 관련된 우려를 말함. 따라서 개인들이나 그룹이 자신 또는 자신에 관한 정보를 시킬 수 숨길 수 없게 됨. 프라이버시는 시스템 내부 및 시스템 간에 또는 물리적 환경의 조작을 통하여 개인 정보를 프로세싱으로 인한 개인의 리스크를 완화시키는 것을 지원하는 일련의 방법들의 구축 및 유지에 이르는 조건임
Trustworthiness	reliability	CPS가 기대되는 조건 내에서 안정적이고 예측가능한 성능을 줄 수 있는 능력에 관련된 우려를 말함
Trustworthiness	resilience	CPS가 불안정성, 기대되지 않는 조건을 제거하면서 예측가능하지만 성능을 저하될 수 있도록 하는 능력에 관련된 우려를 말함
Trustworthiness	safety	CPS가 이해당사자의 생명, 건강, 자산 또는 데이터와 그리고 물리적 환경에 대하여 격변적인 결과가 없음을 보장하는 능력에 관련된 우려를 말함
Trustworthiness	security	CPS가 물리적 및 가상적인 프로세스 및 메카니즘, 그리고 서비스가 비의도적이며 무단의 액세스, 변화, 피해, 파기로부터 내부 및 외부적으로 보호될 수 있음을 보장하는 능력에 관련된 우려를 말함 - 기밀성 : 액세스 및 공개에 대한 허가 된 제한을 유지하는 것 - 무결성 : 시스템의 부적절한 수정 또는 파기로부터 보호하는 것, 그리고 부인(否認) 방지 및 신뢰성을 보장하는 것을 포함함 - 가용성 : 시스템에 대한 신속하고 신뢰할 수 있는 액세스 및 사용

II cybersecurity 분야 IDX 추진 포인트

Cybersecurity 분야 생태계 분석

Cybersecurity의 생태계

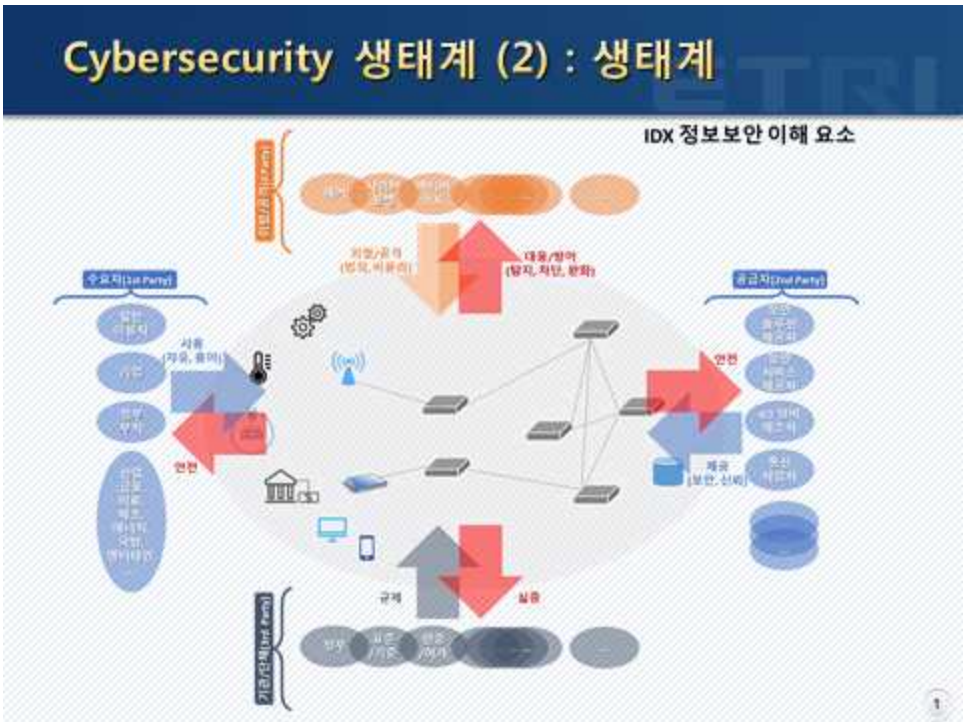
- Cybersecurity 생태계는 제품 및 솔루션, 산업 분야, 리스크 관리, 설치 유형, 서비스 포트폴리오, 보안 유형, 설치 플랫폼, 거버넌스, 보안 작업, 보안 공학, 프레임워크, 표준 및 규제 프레임워크, 경력 개발, 위협 지능, 사용자 교육 등을 포함하는 매우 범위가 넓은 도메인을 말함. 다음의 표는 cybersecurity 생태계와 관련한 도메인 및 각 분류별 세부항목을 설명하고 있음.

[표 4-8] Cybersecurity 도메인

분류	세부 항목
제품 및 솔루션	방어벽 솔루션 (FS) ID 및 액서스 관리 (IAM) 위험 및 규정 준수 관리 (RCM) 암호 솔루션 (ES) 엔드 포인트 보호 솔루션 (EPM) 보안 정보 및 이벤트 관리 소프트웨어 (SIEMS) 게이트웨어 보안 관리 (EPM) 침투 탐지 시스템/ 침투 방지 시스템 (IDS/IPS) 데이터 손실 방지 (DLP) 통합 위협 관리 (UTM) 앤티 바이러스/앤티 말웨어 제품 (AP) 보안 및 취약점 관리 (SVM) DDoS 완화 (DDoSM) 웹 필더링 관리 (WFM) 재해 복구 관리 (DRM) 보안 사고 관리 (SIM) 소셜 미디어 제어(SMC)
산업	은행/정부 및 공공기관/통신 및 IT/항공 및 국방/의료/소매/ 제조 (로보틱 포함)/보험/에너지 및 전력/운송 및 물류/자동차/건축 자동화 /농업/감시 및 보안/비은행 금융기관/미디어 및 광고
리스트 관리	취약점 스캔 제 3자/ 제 4자 리스크 데이터 중심 리스크 평가 :데이터 플로우 맵 침투 테스트 : 사회적 공학, 인프라 및 앱, 화이트박스 및 블랙박스

설치 유형	구내 (on-premise) 클라우드 기반
서비스 포트폴리오	관리 서비스 (magaged service) 전문적 서비스 : 유지 보수, 컨설팅, 리스크 관리, 훈련, 설계, 시스템 통합, 보안 분석
보안 유형	네트워크 보안/ 엔트포인트 보안/ 앱 보안/ 산업 통제 시스템 보안/ 클라우드 보안/ 무선 보안/ 콘텐츠 보안/ 케이트웨이 보안
설치 플랫폼	웹 특화/ 모바일 특화/ IoT 특화/ 크로스 특화
거버넌스	회계/ 법 및 규제 – 산업 또는 국제 또는 국가별/ 최고 경영자 관여/ 기업의 감독 절차 : 정책, 절차, 표준 가이드라인, 준수 및 집행
보안 작업	탐지 및 방어/ 복구/ 예방/ SIEM/SOC/ 사고 대응 : 침해 공지, 봉쇄, 근절, 조사/ 취약점 관리/ 데이터 유출
보안 공학	액서스 통제 : ID 관리 – PAM/IAM/ 데이터 보호/ 네트워크 설계/ 클라우드 보안/ 앱 개발/ 시스템 통합/ 보안 아키텍처/ 암호법
프레임워크, 표준 및 규제 프레임워크	NIST/ ISO/IEC/ SANA/CSC/ 지불카드데이터보안표준/ HIPPA/ 연방 정보보안 관리법/ Gramme-Leach-Billey Act/ Sabanes-Oxiey Act
경력 개발	훈련 및 자격/ 회의/ 피어 그룹/ 셀프 스터디/ 풀 타임 잡
위협 지능	국제 공유/ 콘텍트튜얼/ IOCs/ 내부/ 외부
사용자 교육	훈련 (새로운 스킬)/ 인지 (강화)

- Cybersecurity의 생태계를 그림으로 표현하면 다음과 같음



[그림 4-8] cybersecurity 생태계 - IDX 정보보안이해요소

[그림 4-9] cybersecurity 생태계 - IDX 정보보안요구활동

- 여기서 악한 침입자들은 개인, 범죄 회사, 및 국가 들이며, 이들은 개인 또는 금융 정보, 또는 자산, 지적재산권, 기업 비밀 또는 국가 비밀을 빼내는 것을 목표로 하여, IT 시스템에 침해를 가하는 것을 시도함
- 악한 침입자들은 재정적 또는 국가 안보 이득을 얻기 위하여 시스템을 침해하기 위한 자금 지원이 막강하고 높은 유인이 제공되고, 높은 기술로 무장되어 있음
- 다양한 위협의 범주는 지능형 지속 위협 (Advanced persistent threat, APT)을 구성함. 악한 침입자는 네트워크 시스템 또는 정보 시스템에서 취약점을 악용하기 위하여 말웨어라고 불리워지는 막성 소프트웨어를 사용함. 이들은 말웨어를 주입시키거나, 속이는 방법을 사용하여 사용자들로 하여금 소프트웨어를 이들의 디바이스 또는 시스템에 설치하게 함. 이러한 실제적인 전쟁은 악한 침해자들과 취약점 사이에서 발생함. 이들 취약점들은 보안 업데이트에서 수정되거나 패치되고 있기는 함
- 공격이 없는 날일지라도, 사이버 위협은 감지되지 못하며 매우 위험스러운 상황에서 발생함. 말웨어는 그 목적에 따라 스파이웨어, 애드웨어 및 웜, 바이러스 또는 트로이 목마 등과 같이 불리워지고 있음. 악한 침입자 들은 스펨 이메일, 피싱, 스피어 피싱, 공격 백터, 다중 흐름 공격 또는 다운로드를 통한 드라이브와 같은 말웨어를 퍼지게 하기 위하여 각각 다른 방법을 사용함

◐ Cybersecurity 서비스 모형

- 모든 기업들이 개별 부서를 만들어서 사이버 위협에 대처할 여력이 있는 것이 아니며, 이 이슈를 다룰 방법을 이해하고 있는 것도 아님
  - 이러한 것들이 사이버 보안 관리 서비스 및 전문 서비스 시장을 만들게 되는 요인이 되고 있음. 관리 서비스는 데이터, 정보 및 네트워크를 위해 맞추어진 제품, 솔루션 및 보안 서비스를 제공하는 것을 포함함. 서비스 시장의 22% 차지하는 것으며 주로 중소기업이 고객이 되고 있음
  - 다른 한편으로 전문 서비스 시장은 서비스 시장의 78%를 차지하고 있으며, 여러 유형의 서비스 예를 들면 유지 보수 서비스, 컨설팅 서비스, 리스크 평가 서비스, 교육 및 훈련, 보안 아키텍처 설계 서비스, 시스템 통합 서비스, 및 보안 분석 서비스 들을 포함하고 있음. 대규업 들은 사이버 보안을 위한 각각 다른 유형의 전문 서비스에 의존도가 높아지고 있음

Cybersecurity 분야 IDX 추진 포인트 도출

- IDX 플랫폼 상에서의 가치 창출 흐름은 기계 및 시스템의 네트워킹을 추진하고, 기업 IT 및 인터넷과의 밀접한 연결을 견인할 것임. 외부 공격으로 부터의 보호 및 내부 침입자의 조작에 대한 보호는 IDX 플랫폼으로 부터의 다양한 요구사항을 고려해야 할 것임
  - IDX 플랫폼 상에서 산업 차원의 보안 (제품 측면에서의 보안) 및 IT 보안 (오피스) 간의 긴밀한 협력이 근본적인 필수조건임. 이 둘의 상호작용이 공통의 안전하며 표준화된 IT 인프라를 목표로 구성되어져야 함.

- (**기본적인 보호해야 할 대상**) IDX 플랫폼과 연결된 생산 영역 내에서 보호할 대상은 다음과 같음. : ① 가용성, ②무결성, 및 ③기밀성의 보호 등임. 추가적으로 ① 확실성, ② 시간의 무결성, 특히 기업 범주를 벗어난 가치 네트워크와 관련한 것임. ③ 추적가능성 ④ 법적 보안 등임
  - 확실성은 특히 통신이 기업의 범주를 넘어서는 경우에는 가치 네트워크에서 필수적인 특성임. 또한 추적가능성은 종업원 또는 고객 등의 개인 데이터가 프로세스 될 때, 데이터 보호 요구사항으로부터 발생함. 보안 메커니즘에서 프라이버시/데이터 보호에 관한 기술적 사항은 중요한 역할을 함.
  - 이들 보호할 대상들은 운영 기능, 감시 기능 및 보호 기능에 동일하게 적용함. 시스템을 위한 안전 (기능상의 안전)는 적절한 기능을 취함으로써, 기계 또는

설비의 기능이 사람 또는 환경에는 위험을 끼치지 않음을 보장하는 것을 의미함. 이러한 관점에서, 보안의 소급효과로 부터의 자유는 모든 특별한 프로파일에서 보장되어야 함.

- **(IDX를 위한 보안 설계 (security by design))** [55] IDX 플랫폼을 구현하기 위해서, 정보 보안을 위한 조치를 신속하게 고려하는 것은 피할 수 없음. 보안을 위한 기술적 메커니즘을 소급 통합하는 것 보다는 IDX 플랫폼과 연결되어 있는 제품 개발 및 프로세스와 관련한 통합적 접근방법은 시스템 및 인프라의 보호를 위해서 요구되고 있음
  - 이와 관련하여, 기존 개발 프로세스가 수정되어져야 함. 보안 요구사항을 효과적으로 적용하기 위해서, 제품 생산 관련 응용 프로그램을 특별하게 고려하는 위협 및 리스크 분석이 요구되고 있음. 어떤 제품의 보안 조치를 위한 보호 목표들은 보호를 요구하는 제조자의 자산, 통합자, 운영자 그리고 정부 당국의 규제 지침 예를 들어 주요 기반 시설과 관련된 시나리오 등에 기반을 두고 있음
  - 보안 설계는 IDX 플랫폼과 연결되어 있는 생산 시스템의 라이프 사이클을 고려해야 함. 대개 10~15년을 내다보아야 함
  - 보호를 요구하는 자산을 인식 한 후에, 위협 및 위기 분석이 이루어짐. 가능성이 있는 보안 조치는 확인된 위험을 기반으로 하여 선택됨. 이러한 관점에서 경제적 측면이 중요한 역할을 함. 보안 조치들은 이들이 목표 아키텍처의 비즈니스 모델과 합치하고, 관련된 재정적 지출이 관리할 수 있을 경우에만 시장에서 받아들여짐
  - 암호화 구성요소를 선택할 때, 수출 가이드라인 및 관련 프로세스가 고려되어져야 함. 이는 데이터의 암호화를 위한 특별한 기능과 관련되어 있음; 이 경우에 전용 인증 또는 무결성 메카니즘은 그리 중요하지 않게 됨
  - 현재의 보안 분석은 주로 방화벽, VPNs (Virtual private networks), 네트워크의 원격 접속 등과 같은 네트워크 보안과 관련한 기능에 중점을 두고 있음. 향후의 보안 분석은 IDX 플랫폼과 관련하여서는 변화할 것임. : 복잡하면서도 분산화된 응용프로그램이 보안 설계와 함께 선험적인 보안 조치 (a priori security measures) 를 포함해야 함. 보안 프로파일은 민첩해야 함. 예를 들어 보안 프로파일을 동적으로 적응하고 협상하는 것이 반드시 가능해야 함. 빠

55) 보안 설계는 지속적인 테스팅, 인증 안전 장치, 및 최고의 프로그래밍 방식을 준수하는 조치들을 통하여 시스템들이 취약성으로부터 자유로우며 공격에 침투당하지 않도록 하는 소프트웨어 및 하드웨어 개발 접근방법임.

른 (재)형상은 포용적인 보안을 허용해야 함

- 전통적인 품질 조치들이 전형적인 보안 조치들에 맞추어 보완되어져야 함. 아래의 것들이 포함됨. : ① 취약성 테스트, 침투 테스트, ② 특히 보호 프로토콜 및 암호 기능과 관련하여 생산 프로세스의 무결성 보장 ③ 의도된 보안 수준에 의존하여, 특정한 경우에 시간 집중적인 노력 및 상당한 추가적인 비용을 초래하는 인증서의 요구 등임
- 절차상의 수준에서 명백한 보안 기능의 관리에 추가하여, 소프트웨어 기반의 응용프로그램의 안전한 구현이 또한 보장되어야 함. 관련 소프트웨어 엔지니어에 의한 훈련 및 취약점의 전략적 품질 테스트가 지속적인 구현을 위해 필요함. 품질 테스트로부터 발생한 정보는 설계 프로세스에서 분석되고 통합되어져야 함

- (**ID 관리**) IDX 플랫폼의 가치 네트워크에 있는 참여자 (사용자, 기계, 제품 및 서비스) 의 필수적인 특성은 위조에 강하고 디지털 인증서로 대표되는 명확한 ID 임. 인증 코드에 추가하여 디지털 인증서는 암호화 및 해독을 위해 필요한 정보를 포함함
  - 신뢰할 수 있는 저장 매체가 보안과 관련성이 있는 기록 정보를 위해 요구됨. 통합된 보안 기능을 가진 보안 프로토콜 및 응용프로그램은 요구되고 있는 로그인 데이터와 함께 제공되어져야 함. 이에 대한 전제조건은 참여자의 ID의 모호하지 않으면서 일관된 식별 및 속성을 보장하고, 인증과 ID에 기반하여 권한을 부여하는 것을 지원하는 가치 네트워크를 따라가는 ID 인프라 (복잡도에 따라 하나 또는 두 개의 예시들) 임
  - 신뢰할 만한 인증기관이 IDX 플랫폼 상의 가치 네트워크에 모든 참여자들의 디지털 인증서를 위한 관리기관으로서 요구되고 있음
  - 효과적인 ID 관리를 보장하기 위해서, 참여자를 보안 로그인 데이터/코드는 안전한 ID로 개인화되거나 디바이스와 쌍을 이루어야 함

- (**가치 네트워크의 동적 구성 가능성**) 효과적인 가치 네트워크는 IDX 플랫폼의 동적 형상/재형상을 요구함. 보안 관리는 IDX 플랫폼의 동적 성격을 지원해야 함. IDX 플랫폼 상의 구성요소의 보안 특성(보안 프로파일)이 표준화된 언어 (보안 시맨틱)로 설명되는 것이 필수적이며, 한편으로는 이는 통신 인터페이스/프로토콜과 이들의 보안 특성을 명확하게 설명하고 있음
  - IDX 플랫폼 구성요소가 어떠한 보안 역량을 가지고 있으며, 요구된 보안 수준

은 어떤 방법을 성취할 수 있는 가를 강조하며 설명되어져야 함

- 일반적으로 IDX 플랫폼 구성요소의 보안 기능은 가치 네트워크의 현재의 요구사항을 수용하기 위하여 각각 다른 보안 수준을 지원해야 함. 이러한 전제조건은 IDX 플랫폼의 보안 프로파일의 통합을 통하여 IDX 플랫폼의 보안 수준을 평가하는 것을 가능하게 함
- 보안 프로파일은 적절한 보호 기능을 가지면서 동적으로 변화하고 있는 가치 네트워크로부터 요구되는 융통성을 지원할 수 있어야만 함. 이는 IDX 플랫폼 상의 이질적 시스템을 위한 실질적인 표준화 요구사항으로 이어짐. (예를 들어 IT 보안을 위한 표준화 로드맵 등임)
- 결론적으로 말해, 고전적 분석 (통신 및 네트워크 중심의 보안)은 응용 레벨을 위해서 복잡한 보안 아키텍처로 넘어갈 것임

- (**가상 머신을 위한 보안**) IDX 플랫폼에 연결되어 있는 생산 시스템의 가상 머신은 IDX 플랫폼과 관련하여 매우 중요한 역할을 함. 보안 요구사항의 물리적 구현에 추가하여, 가상 머신을 위한 적합한 보안이 동시에 요구되고 있음
  - 독일의 제조업의 제 4차 산업혁명인 Industrie 4.0를 살펴보면, 논리적인 관점에서, Industrie 4.0의 구성요소는 하나 또는 두 개의 객체와 관리 셀을 포함하고 있으며, 이 관리 셀은 가상적 표현을 위한 데이터 및 기술적 기능을 포함
  - 클라우드 상에서의 가상 머신의 분포에 따라, 각각 다른 보안 프레임워크 조건들이 물리적 구현을 위해서 보다 더 많이 발생할 수 있음. 물론, 물리적 레벨에서의 상호작용은 안전하고 추적가능 할 수 있도록 설계되어져야 함. 따라서 복잡한 보안 아키텍처[56]는 응용 레벨에서 요구되고 있음. 전문 기술 보호 및 무결성특히 중요한 요구사항임. 보안을 위한 고전적인 도메인 경계는 가상 모형에서는 단순하게 묘사되지 못함. 종단간 보안이 중요한 측면이 될 것임. 복구 기능과 관련한 가상 머신은 보안 아키텍처를 구현하는 데 적극적으로 기여할 수 있음. 이는 가상 머신이 보안 사고를 후에 물리적 환경을 복구하기 위하여 요구되는 모든 정보를 포함해야 하기 때문

56) Security architecture 는 어떤 시나리오 또는 환경과 관련된 가상의 위험을 해결하는 보안 설계임. 이는 보안 통제를 언제 그리고 어디에서 적용할 것을 지정하고 있음.

- (**예방 및 대응**)

예방 및 대응은 동등하게 필요함 :
- IDX 플랫폼 솔루션은 추가적인 활동이 반드시 동반되어야 함. - 공격자의 전문지식 및 장비는 지속적으로 발전함. 그 결과 공격 방향도 지속적으로 변화하며, 효과적인 대응조치를 위한 지속적인 개발을 요구할 수 있음. - 예방적인 보호 조치에 추가하여, 대응 메카니즘이 매우 필요함. (모니터링 및 이벤트 처리, 사고 관리) - 룰 기반의 분석을 가진 보안 메시지를 위한 표준화된 세마틱은 능동적인 대응 관리를 위한 전제조건을 만들 수 있음. - 상시의 보안 운영 센터의 번들링 활동은 모든 보안 측면의 집중된 문서, 분석, 평가를 위한 운영상의 전제조건을 제공함.
보안은 일회성의 주제가 아님. :
- 보안은 단 한 번에 행동을 하여 달성 될 수 있는 것이 아님.; 위협 상황는 잠재적 공격자의 새로운 기술적 가능성 또는 표준화된 제품 및 구성요소의 취약성의 발견 및 공개로 인해 지속적으로 변화하고 있음. IDX 플랫폼 과 연결되어 있는 제조업자 및 경영자는 패치 및 엡데이트와 함께 이것들에 대응해함. 보안을 위한 비용은 제조업자 및 경영자들에게는 상당함.; 따라서 모든 프로세스에서 오버 엔지니어링을 예방하기 위해 헌신된 노력을 기울여야 함. - 포괄적인 보안 아키텍처의 구현이 우선시 되고 있음. 동시에, 전체적인 아키텍처 및 모든 프로세스들이 표준화, 개발, 생산 및 관리과 관련하여 반드시 고려되어져야 함. - 보안은 대부분이 프로세스 상의 주제이지 개인의 보안 칩에 의해 보증되지 않음. - 생산 환경의 특별한 프레임워크 조건을 고려하면서, IT 구조의 적응을 추구해야 함.

- (**인식, 훈련 및 추가 교육**) 조직적인 조치가 중요한 역할을 함. 보안 조치의 인식 및 이들의 필요성을 높이기 위해 사람을 훈련시키는 것이 모든 관련 조직에서 반드시 이루어져야 함. 이는 조치들의 이해도를 높이며 구현상의 품질을 높임
  - 인프라 및 인적자원은 보안 관리 기능 및 프로세스에 관련된 훈련을 받고 제공되어져야 함. 제품 및 솔루션의 제조업자에 의해 제공되는 사용자 가이드라인은 프로세스 상에서 통합되어져야 함. 이는 패스워드, 데이터, 데이터 저장 디바이스, 정규적인 데이터 백업을 취급하는 것을 포함

- (**유지·보수**) 상세한 사전 지식이 없어도 산업의 보안 기능을 운영하는 것이 가능해야 함. 이는 유지 및 기타 서비스와 관련하여 문제를 해결하는 것에 적용함. 특히 플러그 및 운영인 보안 솔루션을 위해서 추구되어져야 함

- (**표준 및 지침**) “산업 통제 시스템을 위한 IT 보안 - 네트워크 및 시스템 보호”에 관한 국제표준은 4단계의 보안 레벨에 기반하여 산업 보안을 위한 평가 기준을 가진 프레임워크를 창출함. 이는 향후에 인증을 위해 사용될 수 있을 것임
  - 어떤 시스템에 구성 요소를 통합할 때, 구성 요소의 보안 역량은 요구되는 보안 레벨에 따라 고려되어져야 함. 동시에, 프로세스는 요구되고 있는 보안 수준을 달성하기 위해서 설계되어져야 함
  - 조직이 보안 프로세스를 구축하고 구현할 수 있는 능력은 적절한 벤치마크와 함께 결정될 수 있을 것임
  - 상기한 동적 형상은 유효한 규제 및 규범적인 지침과는 독립적이며, 유효한 규제 및 규범적인 지침은 변화의 국면에서는 인증서/운영 라이센스를 잃을 수가 있을 것임. 그래서, 동적인 것을 설명하는 일련의 규칙이 요구되고 있음. 소급 효과로부터 자유로운 보안 메카니즘에 참여하는 모든 참여자들에 의한 일관성 있는 자가 보호가 전제조건임

※ 참고문헌

Part 1. 국방 IDX 전략

'17~'31 핵심기술기획서 일반본, 국방기술품질원, 2016.

2013 군사과학기술 동향, 국방기술품질원, 2013.6.30.

2016 국방과학기술조사서(요약본), 국방기술품질원, 2016.12

2016 국방백서, 국방부, 2016.12.31.

국방 연구개발 실태 및 개선방안, 과학기술정책연구원, 2015.12.

전쟁 반전쟁, 앨빈 토플러, 2011.4.7.

주요 방산제품의 핵심기술 경쟁력 분석과 향후 과제, KIET 산업경제, 2017.

질적 성장 추진과 함께 기술력 세계 9위에 오르다, 국방홍보원, 2016.1.5.

Visualizing the tactical ground battlefield in the year 2050: Workshop report, US Army Research Laboratory, 2015.06.

Part 2. 행정 IDX 전략

국가과학기술심의회 (2013), 과학기술 기반 사회문제해결 종합실천계획(안), 관계부처합동

국정기획자문위원회 (2017), 문재인정부 국정운영 5개년 계획

국토교통부 (2016), 한국형 스마트시티 해외진출에 총력 기울인다. 도시경제과 보도자료

미래창조과학부 (2016), 대한민국 미래 책임질 9대 국가전략 프로젝트 선정, 과학기술혁신팀 보도자료

보건복지부 (2017), 국민건강증진을 위한 보건의료 빅데이터 추진전략, 관계부처 합동

안창원 외 (2016), 빅데이터 기반 모사현실 기술동향, 전자통신동향분석 제31권 제5호, p120~130.

장병탁, 여무송 (2012), Cognitive Computing I: Multisensory Perceptual Intelligence - 실세계 지각행동 지능, 정보과학회지 2012.1, p.75~87.

장병탁, 여무송 (2012,. Cognitive Computing II: Machine Vision-Language Learning - 실생활 시각언어 학습, 정보과학회지 2012.1, p.88~100.

장병탁, 김현수 (2012), Cognitive Computing III: Deep Dynamic Prediction – 실시간 예측결정 추론, 정보과학회지 2012.1, p.101~111.

행정자치부 (2016), 전자정부 2020 기본계획.

행정자치부 (2017), 데이터기반행정 활성화에 관한 법률안

행정자치부 (2017), 데이터기반행정 활성화에 관한 법률 제정계획(안)

황종성 (2016), 스마트시티 발전전망과 한국의 경쟁력, IT & Future Strategy, 제6호, NIA

Alessandro Zanni (2015), Cyber-physical systems and smart cities, IBM developerWorks, IBM.

Ashish R. Jagdale (2014), Data Mining and Data Pre-processing for Big Data. Int. Journal of Scientific & Engineering Research, Vol. 5, Issue 7, 1156-1161.

Boon Siong Neo & Geraldine Chen (2007), Dynamic Governance, World Scientific Publishing.

Christos G. Cassandras (2016), Smart Cities as Cyber-Physical Social Systems, Engineering 2, p.156-158, Elservier.

City Protocol Society, http://cityprotocol.org

Claude Sammut, Geoffery Webb (2011), Encyclopedia of Machine Learning, Springer.

Henry Markram, et al (2012). The Human Brain Project: A Report to the European Commission, The HBP-PS Consortium.

IBM (2017), IBM Reveals Five Innovations that will Help Change our Lives within Five Years, http://www.research.ibm.com/5-in-5/macroscopes/

Ikbal Taleb (2015), Big Data Pre-Processing: A Quality Framework. Big Data Congress 2015.

John Holdren, Eric Lander (2016), Report to the President: Technology and the Future of Cities, President's Council of Advisors on Science and Technology.

Josep M. Pujol (2006), Structure in Artificial Societies, Ph.D. Thesis Dissertation, UPC.

Joshua M. Epstein & Robert L. Axtell (1996), Growing Artificial Societies: Social

Science From the Botttop Up (Complex Adaptive Systems), Brookings Institution Press & MIT Press.

Juergen Branke (2011), Artificial Societies, Encyclopedia of Machine Learning, Springer.

Michele Goetz (2016), Vendor Landscape: Data Preparation Tools, Data Self-Service Breaks Down Barriers in Systems of Insight. Forrester.

Nigel Gilbert, Jim Doran (1994), Simulating Societies: Computer Simulation of Social Phenomena, Univ Coll Londo.

NIST (2016), Smart Cities/CPS budget sheet at NIST, http://www.nist.gov/

Pauline Tay (2015), Innovation Clusters - a National Strategy to Build Technology Capabilities in Singapore, 18th TCI Global Conference

Peter Kogge, et al (2009), ExaScale Computing Study: Technology Challenges in Achieving Exascale Systems, DARPA IPTO.

Peter Tyson (1997), Rewriting Life: Artificial Societies, MIT Technology Review.

Rob Dubbledeman, Stephen Ward (2015), Smart Cities: How rapid advances in technology are reshaping our economy and society, Deloitte GOV LAB.

Robert Gao (2015), A Cyber-Physical Infrastructure for the “Smart City”, https://cps-vo.org/node/23817

Ron Bekkerman (2008), Data Weaving Scaling Up the State-Of-The-Art in Data Clustering. ACM CIKM (Conference in Information & Knowledge Management).

Soon Chun (2017), Big Data driven Megacity Insights Platform, CUNY College of Staten Island

FuturICT project (2012).

Part 3. 교육 IDX 전략

국가기술표준원(2017), '교육 기술 전망과 표준화 동향', KATS 기술보고서.

국가평생교육진흥원(2016), '4차 산업혁명의 시대에서 묻는 교육의 미래', 글로벌평생교육동향.

박윤수, 강창희, 김진영, 김창환(2017), '4차 산업형명에 대비한 교육개혁 방향', 2016년 국가중장기 전략 수립을 위한 작업반 운영, 결과자료.

미래창조과학부(2017), '미래 사회 변화 대응 과학기술인재 육성 방안 연구'.

심진보, 하영욱, 최병철, 노유나(2016), '제4차 산업혁명과 ICT', ETRI Insight Report.

이러닝진흥위원회(2017), '제3차 이러닝산업 발전 및 이러닝 활용 촉진 기본계획'.

정보통신산업진흥원(2015), '2015년 이러닝산업 실태조사'.

중소기업청(2017), '중소·중견기업 기술로드맵', 콘텐츠분야.

통계청(2017), '2016년 초·중·고 사교육비조사 결과'.

한국교육학술정보원(2017), '교육정보화 글로벌 동향', 2017년 6월 2호.

한국이러닝산업협회(2015), '효율적인 이러닝 활용을 위한 국제표준 및 정책동향 연구조사 보고서'.

한국인터넷진흥원(2016), Power Review, KISA Report, 2016년 5월.

Gartner (2015. 6). "Hype Cycle for Education, 2015".

Gartner (2015. 7). "Hype Cycle for education, 2015".

Part 4. Cybersecurity IDX 전략

ETRI, 새로운 미래를 위한 전략과 통찰, IDX, 대한민국 제4차 산업혁명, 심진보, 최병철, 노유나, 하영욱, 콘텐츠 하다

ETRI, 훤히 보이는 정보보호, 정교일, 이병천, 진승현, 전자신문사

이경주, 4차 산업 혁명 : 앞으로 5년, 마리북스,

김은 et al, Industrie 4.0. 클라우드 나인, 2017

KT 경제경영연구소, 한국형 4차 산업 혁명의 미래, 한스미디어,

서울대 법경제연구센터, 데이터 이코노미, 한스미디어

acatech, “Recommendations for implementing the strategic initiative INDUSTRI4.0”, 2013.April

bitkom, VDMA, ZVEI, “Implementation Strategy Industrie 4.0”, 2016. Janunary

NIST, “Framwork for CPS: Volume 1, Overview”, Jun 2017

W.Colombo외, “Industrial Cyberphysical System”, IEEE industrial Electronics Magazine, Mar 2017

Wollschilaeger외, “The Future of Industrial Communication”, IEEE industrial Electronics Magazine, Mar 2017

industrial internet consortium, Industrial Internet of things , volumn G4 :security framework 2016.

Gartner. (2017). Predicts 2017 : Information security management

NSTC. (2016). Federal cybersecurity research and development strategic plan

저자소개

정지형 ETRI 미래전략연구소 기술경제연구본부 산업전략연구그룹 선임연구원
e-mail: jhc123@etri.re.kr Tel. 042-860-5643

안창원 ETRI 미래전략연구소 미래기술연구본부 전문위원
e-mail: ahn@etri.re.kr Tel. 042-860-1239

이지형 ETRI 미래전략연구소 기술경제연구본부 기술경제연구그룹 책임연구원
e-mail: leejeehy@etri.re.kr Tel. 042-860-5124

석왕헌 ETRI 미래전략연구소 기술경제연구본부 산업전략연구그룹 선임연구원
e-mail: whseok@etri.re.kr Tel. 042-860-6208

허필선 ETRI 미래전략연구소 기술경제연구본부 산업전략연구그룹 선임연구원
e-mail: f3style@etri.re.kr Tel. 042-860-5396

조영환 ETRI 미래전략연구소 기술경제연구본부 책임급 전문계약직원
e-mail: ywcho@etri.re.kr Tel. 042-860-6012

공공수요형 IDX 추진을 위한 산업환경 및 생태계 분석

발 행 인 : 한 성 수

발 행 처 : 한국전자통신연구원 미래전략연구소 기술경제연구본부

발 행 일 : 2017년 12월 31일

ETRI 한국전자통신연구원
미 래 전 략 연 구 소

(34129) 대전광역시 유성구 가정로 218
전화 : (042) 860-3874, 팩스 : (042) 860-6504

ETRI 미래전략연구소 www.etri.re.kr