디지털로 여는 좋은 세상

2023-1호

D.gov 해외동향

Issue

WEF, 2023년 글로벌 사이버보안 전망 보고서 발간

미국-EU 간 신뢰할 수 있는 AI 개발을 둘러싼 협력 현황 분석

News

미국, 제5차 열린정부 국민행동계획 발표 등 총 9건

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

CONTENTS

01 Issue

02 News

ISSUE ① WEF, 2023년 글로벌 사이버보안 전망 보고서 발간

Reading Point

- 세계경제포럼(World, Economic Forum, WEF)은 사이버보안에 관한 보고서를 발간[1]하였으며, 보안 이슈, 전문인력 현황, 사이버보안 거버넌스 격차 등의 주요 현황과 이슈를 도출
- 본 보고서는 최고경영진과 사이버보안 전문가를 대상으로 실시한 설문조사 결과[2]를 중심으로 요약하여 기술·규정에 대한 주요 인식 변화를 정리

Ⅰ 개요

❍ 세계경제포럼(WEF)은 2022년부터 '글로벌 사이버보안 전망(Global Cybersecurity Outlook 2023)' 보고서를 발간하며, 올해도 32개국 및 22개 산업부문에 있는 최고경영진과 사이버보안 전문가 117명이 참여

❍ 전년 대비 최고경영진과 사이버보안 전문가 간의 인식 차이가 높여졌음을 확인하였으며 지속적인 노력을 통해 지정학적 불안전성과 인재 부족 문제에 대한 대응방안 마련이 필요

- 우크라이나-러시아 전쟁은 많은 기업·조직의 사이버보안 전략에 큰 영향을 미침
- 개인정보보호법과 사이버보안 규제에 대한 인식은 전년 대비 크게 변화
- 사이버보안 노동시장에 대한 최고경영진과 사이버보안 전문가 간의 인식 격차가 감소

---

1) 2023년 1월에 사이보보안과 연관된 2건의 보고서를 발간
① WEF(2023.1), Global Cybersecurity Outlook 2023 - Insight Report
② WEF(2023.1), State of the Connected World 2023 Edition - Insight Report

2) WEF(2023.1), Global Cybersecurity Outlook 2023 - Insight Report
참고자료: WEF(2022.1), Global Cybersecurity Outlook 2022
https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

Ⅱ 주요 내용

1 지정학적 불안정성이 사이버보안에 미치는 영향

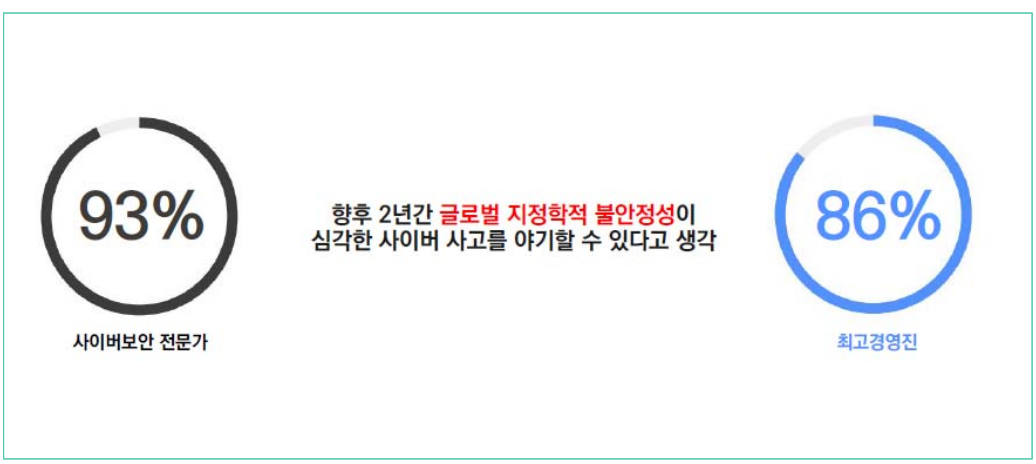
○ 최고경영진 및 사이버보안 전문가는 지정학적 불안정성(geopolitical instability)으로 향후 2년간 심각한 사이버보안 사건이 발생할 가능성이 있다고 응답

- 최고경영진 86%[3], 사이버보안 전문가 93%[4]가 치명적 사건이 발생할 것이라 생각

○ 대부분 응답자는 이미 지정학적 불안정성이 기업·조직의 사이버보안 전략에 다양한 영향을 미친다고 생각

- 기업·조직의 서비스 중단 또는 평판 훼손 등의 목적으로 한 사이버 위협을 위주로 사이버보안 전략을 수립

〈 지정학적 불안정성의 영향에 관한 조사 결과 〉



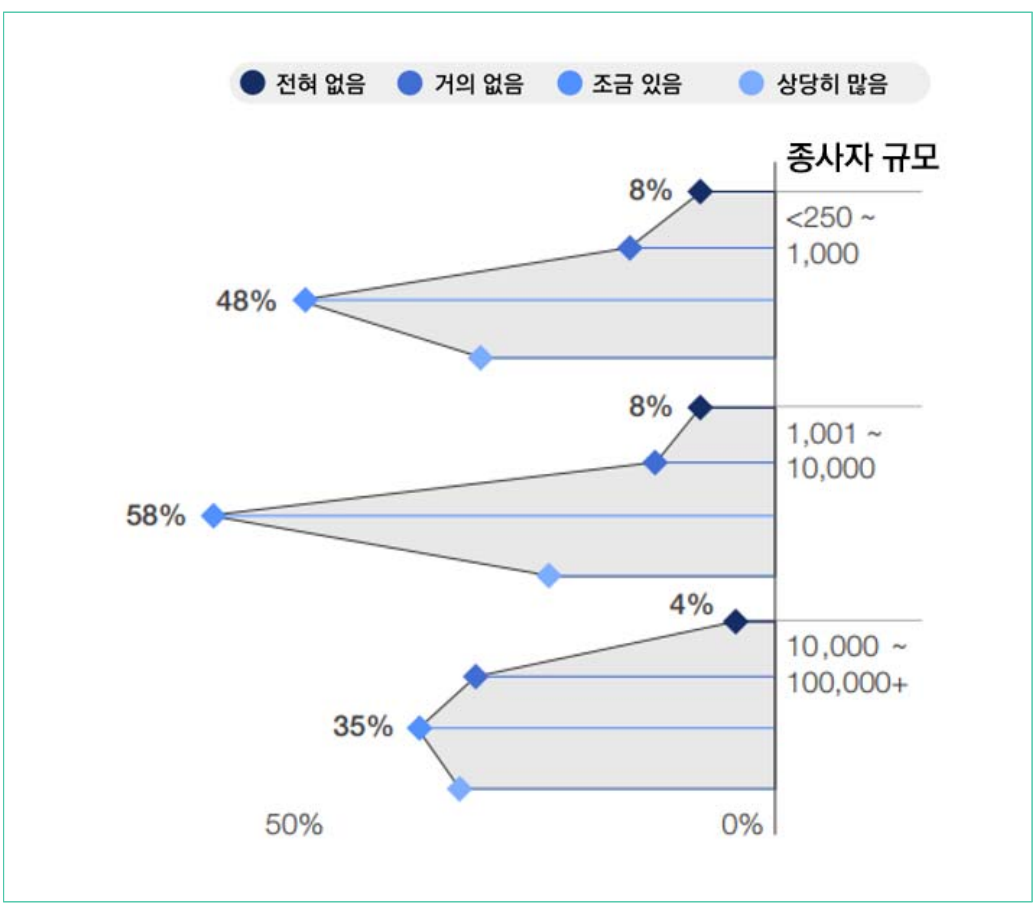
3) 최고경영진 중 치명적인 사건이 발생할 가능성이 '매우 높다'라고 생각하는 응답자는 45%, '어느 정도 있다'라고 생각하는 응답자는 41%

4) 사이버보안 전문가 중 치명적인 사건이 발생할 가능성이 '매우 높다'라고 생각하는 응답자는 46%, '어느 정도 있다'라고 생각하는 응답자는 47%

❍ 조직의 규모에 상관없이, 대부분 응답자는 지정학적 불안정성이 기업·조직의 사이버보안 전략에 영향을 미칠 것으로 예상

- 사이버보안 전략의 성공적인 변화가 있었다고 말한 응답자들은 사이버보안 전문가와 최고경영진 간의 의사소통을 지원하는 조직 구조를 갖추고 있다 대답
- 특히 조직 구조를 통해 최고경영진 활동 전반에 걸쳐 디지털 회복탄력성을 강화하기 위한 협업을 장려

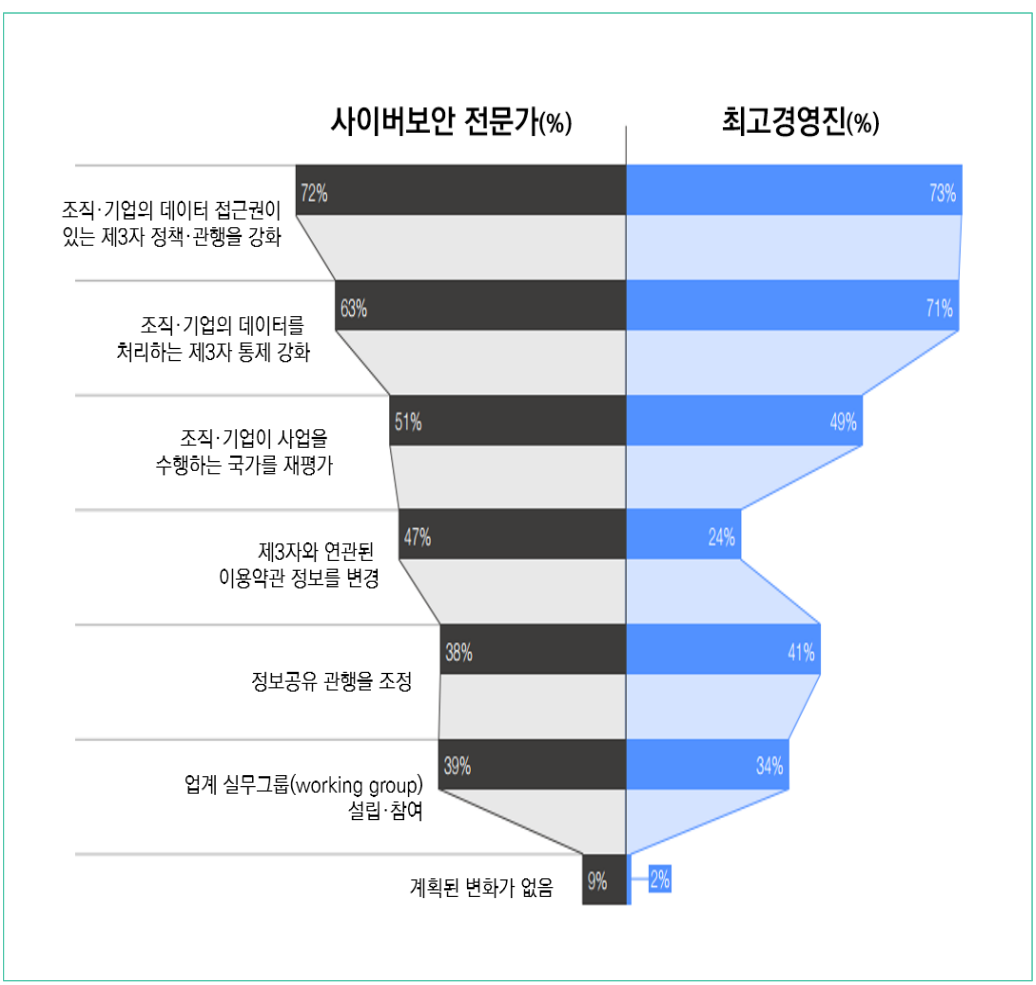
〈 지정학적 불안정성이 사이버보안 전략에 영향을 미칠 가능성 〉



❍ 지정학적 위험에 대응하는 방법으로는, 사이버보안 전문가와 최고경영진 모두 협력 업체 또는 협력 국가에 관한 전략을 재조정하는 것을 우선순위로 생각

- 특히 ① 데이터에 관한 직접적 접근권이 있는 제3자와 연관된 정책·관행을 강화, ② 데이터를 처리하는 제3자에 관한 통제권 강화, ③ 조직·기업이 사업을 수행하는 국가를 재평가하겠다고 응답
- 우크라이나-러시아 전쟁은 전 세계의 사이버 전략 및 전술적 사이버보안에 상당한 영향을 미쳤으며, 특히 내부 정책·프로세스를 강화하고 제3자에 대한 사이버보안 통제권을 높이기 위한 노력으로 이어짐
- 사이버 위협에 대한 조직적 대응은 장기적으로 긍정적인 영향을 미칠 것으로 예상

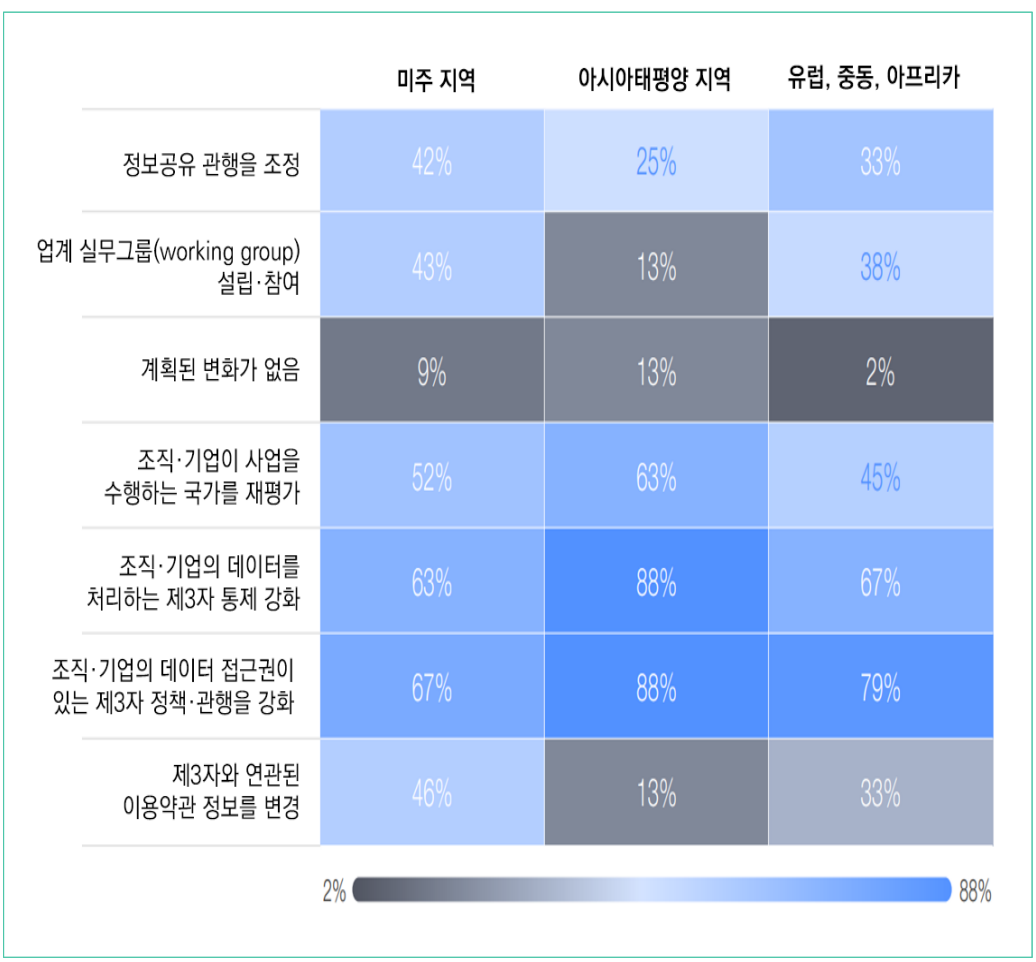
〈 지정학적 위험(risk)에 대응하는 방법 〉



❍ 지정학적 위험에 대응하는 방법은 지역에 따라 우선순위는 동일하나 응답 비율은 다소 상이

- 지정학적 불안정성은 더욱더 다양한 사이버보안 위협을 발생시킬 수 있음
- 멜웨어[5] 유형, 공격자가 목표로 삼는 자산 유형 또는 가치 창출 과정의 변화함에 따라 조직·기업 내부 사이버보안 관행에 대해 전략적으로 판단이 더 어려워짐
- 사이버보안 환경의 변화를 파악하는 데 더 많은 시간과 자원을 투자해야 하며, 공격자의 의도에 따른 공격 대상·방식을 예상할 필요성이 증가

〈지역별 지정학적 위험(risk)에 대응하는 방법 〉



5) 악의적인 목적을 위해 작성된 실행 가능한 코드로 악성 코드(Malicious Code) 또는 악성 프로그램(Malicious Program) 등으로도 불림 (TTA 정보통신용어사전)

2 보안 규제에 대한 인식

❍ 대부분 최고경영진과 사이버보안 전문가는 사이버보안 및 개인정보보호 규제가 기업·조직이 당면한 사이버 위협을 줄이는 데 효과적이라고 인식

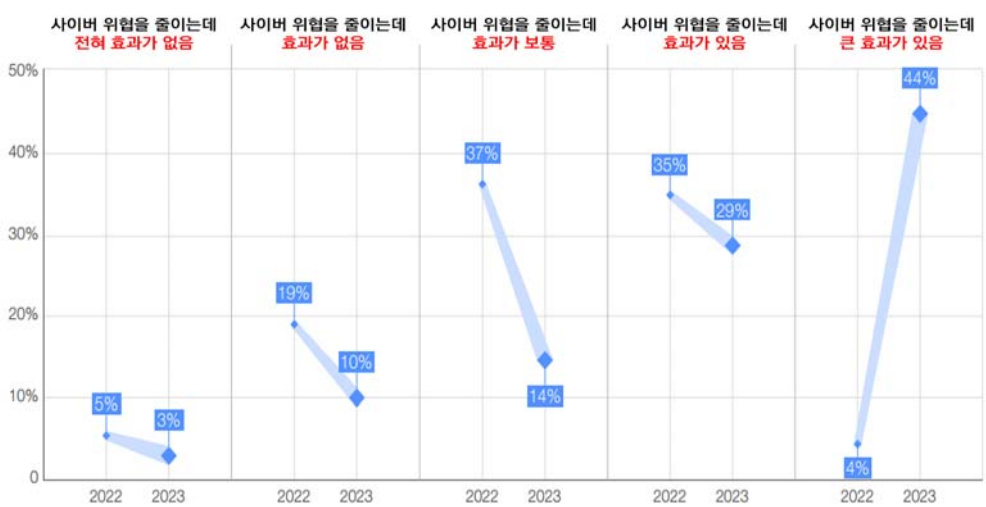
- 작년 대비 사이버보안 및 개인정보보호 규제에 대한 인식이 크게 변화

  ※ 2022년 설문조사 응답자 절반 이상은 규제가 효과적이라고 생각하지 않았으나, 2023년 조사에는 73%[6]가 효과적이라고 인식

- 하지만 일부 사이버보안 규제의 중복성으로 인한 한계가 여전히 존재

  ※ 2개 이상의 국가에서 활동하는 기업·조직은 중복된 규정을 준수하기 위해 시간과 자원을 투자하며, 실질적인 영향을 미칠 수 있는 핵심 사이버보안 업무에 소홀해질 수 있음

〈 사이버보안 및 개인정보보호 규정이 미치는 영향(2022년과 2023년 결과 비교)[7] 〉



※ 위 그래프는 최고경영진과 사이버보안 전문가의 응답을 종합한 결과

---

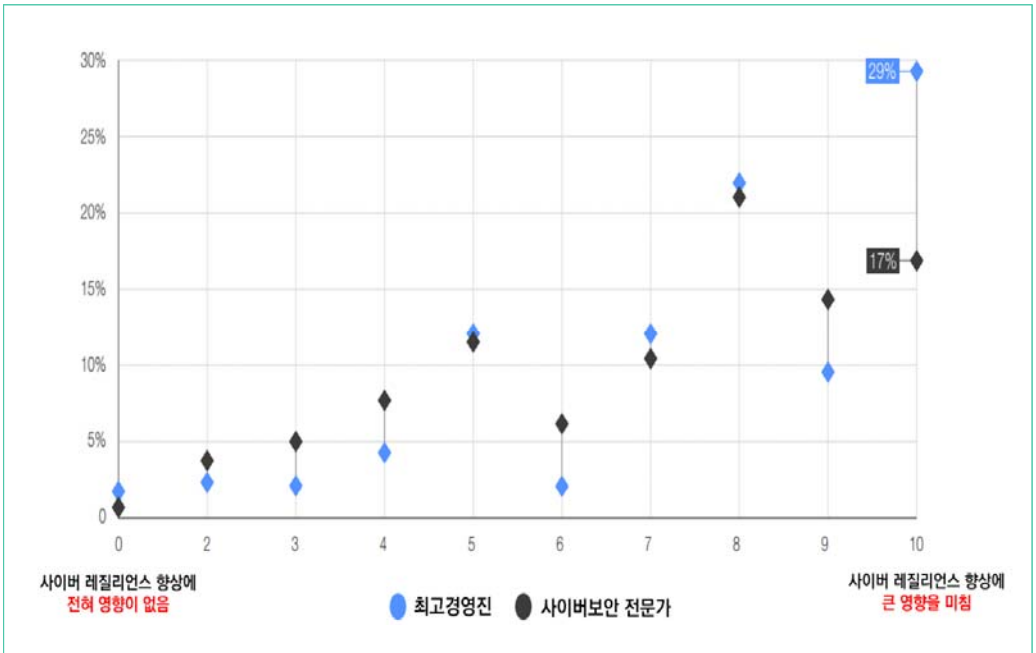
6) 사이버보안 및 개인정보보호 규정이 자사의 사이버 위협을 줄이는 데 '효과가 있다'라고 생각한 응답자는 29%, '큰 효과가 있다'라고 생각한 응답자는 44%

7) 응답자는 "사이버보안 및 개인정보보호 규정이 나의 기업·조직의 사이버 위협을 줄이는 데 효과적이다"라는 질문에 "전혀 그렇지 않다(Strongly disagree)", "그렇지 않다(Disagree)", "보통이다(Neither agree nor disagree)", "그렇다(Agree)", 또는 "매우 그렇다(Strongly agree)"라고 답변함. 본 고에서는 "전혀 그렇지 않다(Strongly disagree)"를 "전혀 효과가 없음", "그렇지 않다(Disagree)"를 "효과가 없음, "보통이다"를 "효과가 보통", "그렇다"를 "효과가 있음", 그리고 "매우 그렇다"를 "큰 효과가 있음"으로 의역

❍ 산업 전반의 규제 집행 노력이 사이버 레질리언스[8]에 미치는 영향에 대한 최고경영진과 사이버보안 전문가의 의견은 다소 엇갈림

- 응답자 중 최고경영진 29%는 산업 전반의 규제 집행이 확실히 사이버 레질리언스 향상에 기여할 것으로 생각했지만, 사이버보안 전문가 중 17%뿐만 그렇다고 답변
- 즉, 최고경영진에 비해 사이버보안 전문가가 규제 집행을 다소 부정적으로 인식
- 대부분 응답자는 지속적으로 변화하는 규제에 적응하기 어려울 것이라 생각하며, 일부 인터뷰 대상자는 "규제가 사이버보안 조치를 장려하지만, 조직 내 사이버 레질리언스로 직접 이어지지는 않는다"고 언급

〈 산업 전반의 규제 집행이 사이버 레질리언스에 미치는 영향[9] 〉



8) 사이버 레질리언스(cyber resilience)는 사업 연속성, 정보 시스템 보안, 조직의 복원성을 결합한 개념이며, 사이버 공격, 자연재해 또는 경기 침체와 같은 상황에서도 의도한 결과를 계속 제공할 수 있는 능력을 의미 (출처: https://www.ibm.com/kr-ko/topics/cyber-resilience)

9) 응답자는 "산업 분야(sector) 전반에 더 효과적인 규제·규정 집행은 나의 기업·조직의 사이버 레질리언스를 향상할 것이다"라는 질문에 "전혀 그렇지 않다(Strongly disagree)"부터 "매우 그렇다(Strongly agree)"까지의 답변을 선택. 본 고에서는 "전혀 그렇지 않다"를 "전혀 영향이 없음", "매우 그렇다"를 "큰 영향을 미침"으로 의역

3 사이버보안을 위한 기업·조직의 접근 방식

❍ 기업·조직의 사이버보안에 가장 긍정적인 영향을 미칠 요인은 ▲클라우드 기반 서비스, ▲디지털 전환[10] 정책, ▲사이버보안 위협에 대한 직원 인식 제고 등을 포함

- 사이버보안 전문가는 향후 12개월 동안 클라우드 기반 서비스 사용 증가가 가장 큰 영향을 미칠 것으로 생각하였으며, 그다음으로 디지털 전환 정책과 직원 인식 제고를 선택
- 반면, 최고경영진은 직원 인식 제고를 1순위로 여겼으며, 클라우드 기반 서비스 사용 증가는 3순위, 디지털 전환 정책은 6순위로 응답
- 디지털 대전환을 위해 기존 IT 시스템에 신기술을 도입하면 새로운 보안 위협이 발생할 수 있기 때문에, 조직을 이끄는 경영진과 사이버보안 전문가는 신기술의 가치와 조직이 감당할 수 있는 위험 간의 균형을 유지하기 위한 노력이 필요

〈 기업·조직의 사이버보안에 가장 긍정적인 영향을 미칠 요인 〉

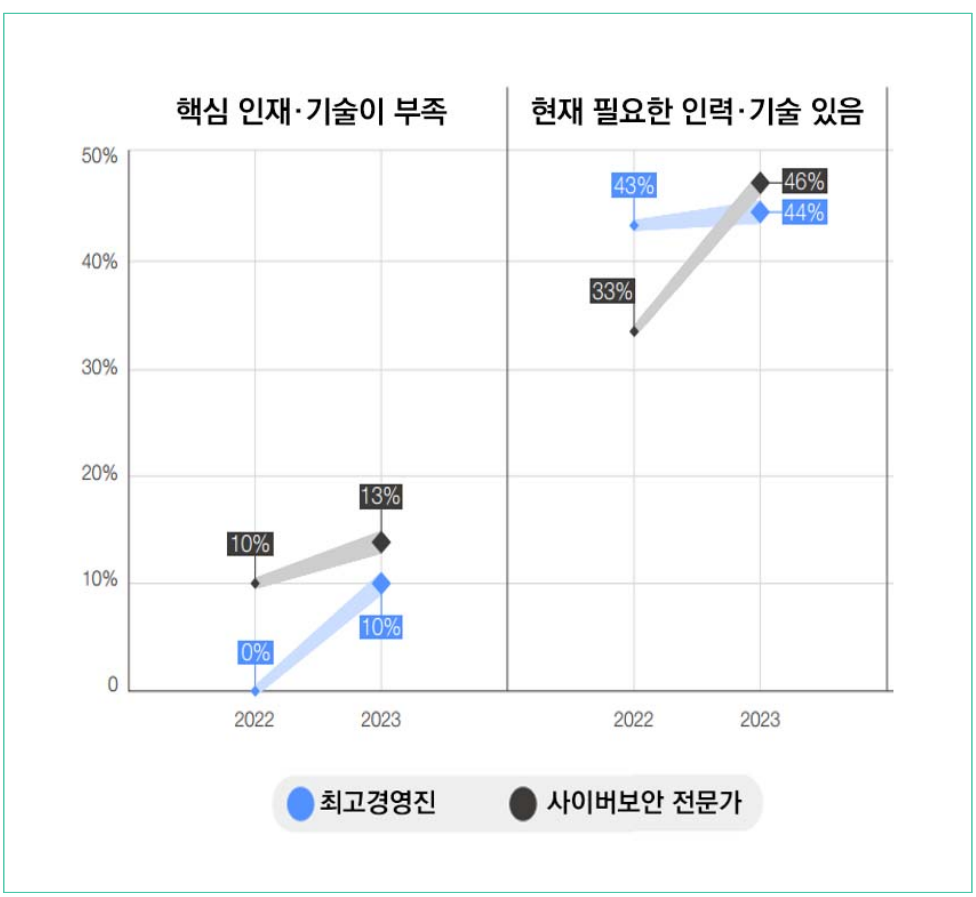
10) 디지털 전환(Digital Transformation)은 디지털 기술을 사회 전반에 적용하여 전통적인 사회 구조를 혁신시키는 것. 일반적으로 기업에서 사물 인터넷(IoT), 클라우드 컴퓨팅, 인공지능(AI), 빅데이터 솔루션 등 정보통신기술을 플랫폼으로 구축·활용하여 기존 전통적인 운영 방식과 서비스 등을 혁신하는 것을 의미(TTA 정보통신용어사전)

4 사이버보안 인재 현황에 대한 인식

❍ 사이버 인재 채용·관리는 모든 조직에서 계속해서 상당한 장애물로 작용

- 그러나 작년 대비 올해 최고경영진과 사이버보안 전문가 간의 인식 격차가 크게 줄어들어 사이버보안 노동시장에 대한 두 집단의 생각이 점차 유사하게 변화함을 확인
- 2022년에 사이버보안 전문가 중 10%가 사이버 공격 대처에 필요한 인력·기술이 부족하다 응답했지만, 최고경영진은 아무도(0%) 인력·기술이 부족하다 대답하지 않음
- 2023년에 사이버 공격 대처에 필요한 인력·기술이 부족하다고 응답한 최고경영진은 10%로 크게 늘어났으며, 사이버보안 전문가는 13%로 증가
- 즉, 인력·기술 문제가 실질적으로 악화된 것이 아니라, 두 집단 모두 노동시장 현황에 대한 이해도가 높아졌음을 나타냄

〈 사이버보안 노동시장에 대한 인식 〉



❍ 정보기술 서비스를 제공하거나 관련 서비스를 활발히 사용하는 산업[11]에 속한 응답자 중 절반 이상이 현재 필요한 인력·기술을 보유하고 있다고 응답

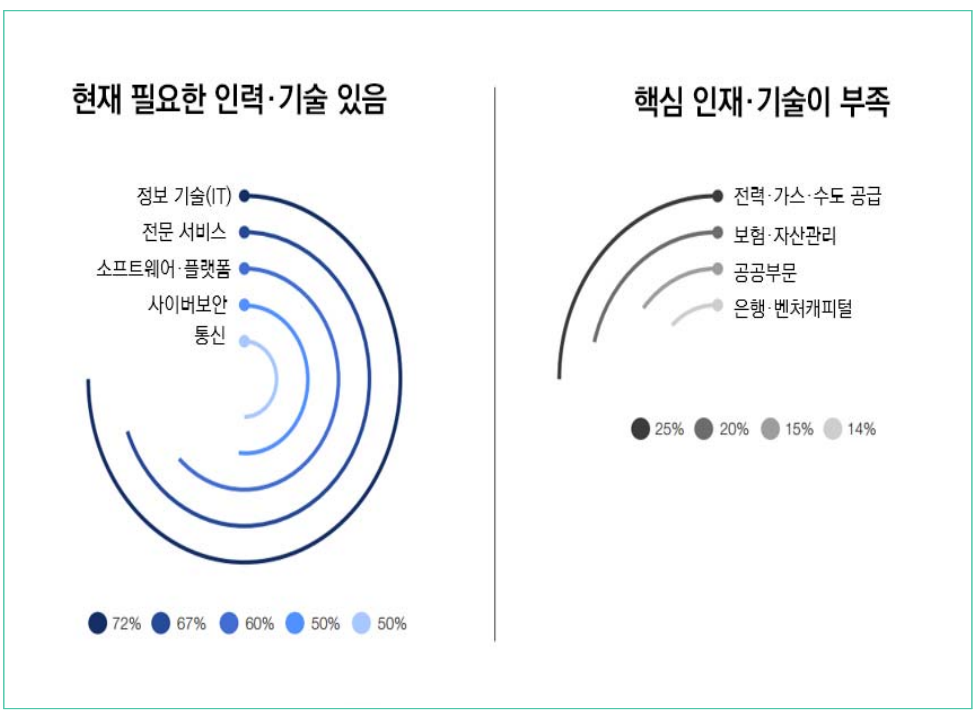
※ 정보 기술(IT) 산업은 72%, 전문 서비스 산업은 67%, 소프트웨어·플랫폼 산업은 60% 등 대부분 응답자가 이미 필요한 인력 및 기술을 보유하고 있다고 생각

- 반면, 전력·가스·수도 공급업을 포함한 주요 인프라 산업과 공공부문은 핵심 인력 및 기술이 부족하다고 응답

※ 특히 전력·가스·수도 공급업은 25%, 보험·자산관리 분야는 20%가 핵심 인재 및 기술이 부족하다고 인식

- 많은 기업이 자체적으로 인력·기술 부족 문제를 해결하기는 어려울 것이며, 다른 기업과의 협력이 필요

〈 산업별 사이버보안 인력·기술 격차 〉



11) 정보 기술 및 통신 산업을 포함

Ⅲ 결론

❍ 작년 대비 사이버보안 전문가와 최고경영진은 점점 더 체계적으로 의사소통하며, 대부분 인식 격차가 감소하는 추세를 관찰

- 지정학적 불안정성이 사이버보안에 미치는 영향, 사이버보안 및 개인정보보호 규제가 미치는 영향, 노동시장에 대한 생각 등 다양한 질문에 유사하게 응답
- 사이버보안 전문가 중 56%가 매월 또는 더 자주 기업·조직의 이사회와 만난다고 말함
- 이미 많은 인식 격차가 줄어들었지만, 최고경영진과 사이버보안 팀 간의 이해를 촉진하기 위해 더 많은 노력이 필요

❍ 효과적인 사이버보안 위험관리를 위해서 보안 위협에 대해 적극적으로 소통하는 조직 구조상의 변화가 필요

- 사이버보안 전문가는 기업·조직 이사회가 이해하고 조치를 취할 수 있는 형태로 보안 문제를 설명해야 함
- 최고경영진은 조직 전반의 사이버보안 역량 강화를 위해서 요구되는 규제 또는 정책에 대한 책임을 직접 짊어져야 함

❍ 사이버보안 인재 채용·관리는 사이버 레질리언스를 위한 핵심 과제

- 한정된 인재풀을 확대하기 위해 타전공자, 전통적인 교육제도에 속하지 않은 인재, 취약계층 등도 재교육을 통해 사이버보안 업무에 참여할 수 있도록 유도할 수 있음
- '코딩하는 소녀들'[12]과 같은 시민사회 조직과 관계를 구축하고 협력하는 것이 필요
- 4년제 학위보다 기술과 경험에 더 집중하여 채용 프로세스를 여는 것도 가능

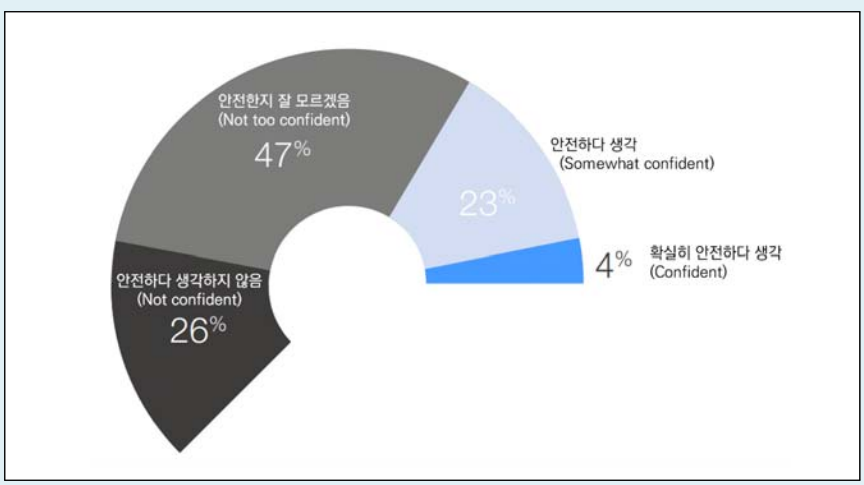
12) Girls Who Code (홈페이지: https://girlswhocode.com/)

〈 참고: 사물의인터넷(IoT) 기술에 관한 사이버보안 거버넌스 격차 현황[13] 〉

❍ 세계경제포럼(WEF)은 사물인터넷 기술에 대한 거버넌스 격차 현황을 조사하기 위해 공공·민간 분야 IoT 전문가 271명을 대상으로 설문조사, 25명을 대상으로 인터뷰를 실시

- 조사 결과, 코로나19 및 사물인터넷 기술혁신 등으로 인해 윤리, 사이버보안, 기술 접근권 등에 관한 'IoT 거버넌스 격차'가 존재함을 발견
- '거버넌스 격차(governance gap)'는 기술이 야기하는 잠재적 위험과 이러한 위험을 방지·대응하려는 사회적 노력 간의 차이
- 특히 사이버보안과 관련된 거버넌스 격차는 조직의 재정적, 생산적 손실을 야기하므로 격차를 줄이기 위한 노력이 필요

❍ **(사이버보안 거버넌스 격차 현황)** 대부분 응답자는 IoT 연결장치 또는 기술을 이용하는 사용자가 사이버 범죄·공격으로부터 안전한지 잘 모르거나(47%), 안전하다 생각하지 않는다고(26%) 응답[14]



13) 출처: WEF(2023.1), State of the Connected World 2023 Edition - Insight Report
사물인터넷(IoT) 및 주변 기술에 대한 거버넌스 격차 현황을 조사하기 위해 설문조사 및 인터뷰 결과를 요약한 보고서이며, 본 보고서에서는 사이버보안에 관한 주요 내용을 요약

14) "IoT 연결장치·기술을 이용하는 사용자가 사이버 범죄·공격으로부터 안전하다 믿음"이라는 질문에 응답자는 "확실히 안전하다 생각(confident)", "안전하다 생각(Somewhat confident)", "안전한지 잘 모르겠음(Not too confident)", 그리고 "안전하다 생각하지 않음(Not confident)" 중에 선택

❍ **(사물인터넷 기술로 인한 보안상 취약점)** 사물인터넷 기술로 연결된 장치·기술에 대한 의존도가 높아짐에 따라 조직, 정부 및 개인 사용자가 사이버 위협에 점점 더 취약해졌으며[15], 개인과 기업에 상당한 결과를 초래할 가능성을 지님[16]

- 웨어러블 장치, 스마트 홈, 센서, 온도 조절 장치 및 기타 IoT 관련 기술의 활용은 전체 시스템을 손상할 수 있는 많은 취약점을 제공
- 사용자가 취약한 암호를 사용하거나 피싱 이메일을 식별할 수 없는 것과 같은 열악한 보안 관행, 시장의 전반적인 투명성 부족으로 인한 보안상 취약점 인식 부족 등의 위험에 노출
- 보안 고려 사항이 설계·프로토타이핑 단계 후반에 포함되는 경향이 있어, 악의적인 행위자가 시스템과 연결과 장치를 침입하는 결과를 초래

❍ **(사이버보안 거버넌스 격차의 영향)** 현재 사물인터넷 기술의 사이보보안 수준과 위험 관리와 관련된 관행으로 다양한 부정적 영향이 발생

① 조직, 정부 및 개인 사용자에게 심각한 재정적 손실을 초래할 수 있음

※ 글로벌 사이버 범죄는 향후 5년 동안 매년 15%씩 성장하여 2025년까지 10조 5천억 달러에 이를 것으로 예상됨

② 사이버범죄자들은 점점 주유소 등의 주요 인프라를 공격해 물리적 피해를 유발

※ 미국의 콜로니얼 파이프라인 시스템을 해킹하여 주유소의 기름을 고갈시켜 패닉바잉(Panic Buying)을 야기했으며, 유럽에서는 해킹으로 수십 개의 병원이 시스템이 마비된 적이 있음

③ 기업은 보안취약점으로 은행 계좌 정보, 주민등록번호, 신용카드 번호 등 고객의 개인 정보 유출로 고객의 신뢰를 잃으며 기업 평판에 손상을 초래

※ Forbes Insight 보고서에 따르면, 조직의 46%가 데이터 유출로 인한 평판 손상 및 19%는 제3자 보안 침해로 인한 평판 및 브랜드 손상을 겪음

④ 사이버 공격이 발생하면 해당 IT 직원은 원인 식별, 취약성 수정, 보안 조치 강화를 조치를 수행하게 되며, 생산성이 저하됨

15) 2021년 상반기 전 세계적으로 15억 건의 IoT 표적 공격이 기록되었고, 데이터 유출은 전년 대비 15.1% 증가함
16) 랜섬웨어 공격의 재정적 영향은 2022년 전 세계적으로 7조 달러의 비용이 들 것으로 예상

❍ **(사이버보안 취약점 극복을 위한 인식 변화)** 사물인터넷 기술이 야기하는 잠재적 위험을 사회적으로 인식하고 방지·대응하려면 다양한 노력이 필요

- 사용자 인식 변화를 위한 캠페인[17]을 통해 개인과 운영자에게 필요한 교육을 하며 장치 제조업체는 사용자에게 교육 및 경고를 제공해야 함
- 즉, 모든 장치에 대한 2차인증, 비밀번호 및 암호 변경, 생체인식 또는 보안키와 같은 암호 대안 등을 제시하는 것이 바람직함

❍ **(사이버보안 취약점 극복을 위한 표준·관행)** 정부와 산업계는 사물인터넷 기술을 더 안전하게 설계하기 위해 표준과 관행을 마련해야 함

- 국가 또는 산업 부문별 사이버보안 관행에 관한 공통된 공유 표준[18]을 마련하고 적용하는 것이 중요
- 보안 위협에 대한 대응이 아닌, 기술 설계·개발 과정의 기본적으로 사이보보안을 고려하는 것이 필요

※ 대다수 조직·기업은 여전히 사이버보안에 사후에 대응하며 기존 피해 관리에 목표를 두고 있으나 제품 설계 단계부터 강력한 사이버 보안 인프라를 구축하는 데 집중해야 하며 사용자가 장치 및 시스템 내의 취약성으로 보호되도록 기본값을 강화해야 함

❍ **(사이버보안 취약점 극복을 위한 정책·규제)** 정부는 규제 균형을 목표로 정책 개발에 적극적이고 지속적으로 참여하기 위해 노력

- 특히 정책을 설립할 때 관련 기술 전문가와 함께 적응하고 협력해야 함

※ EU 데이터 보호 규정은 과소 규제와 과잉 규제 사이의 균형을 유지하며 시장을 촉진하기 위한 지침을 제공

17) 2021년 5월 미국 정부는 국가의 사이버 보안을 개선하기 위한 행정 명령을 발표하여, 미국 국립표준기술연구소는 IoT 소비자 장치와 소프트웨어의 사이버 보안 기능에 대한 라벨링 프로그램을 개발하여 소비자를 교육하고 보호하도록 함

18) California Security of Connected Devices Law이며, 캘리포니아주 내의 모든 연결된 장치가 인증을 위한 보안 조치를 포함해야 한다는 표준을 설정하도록 함

ISSUE ② 미국-EU 간 신뢰할 수 있는 AI 개발을 둘러싼 협력 현황 분석

Reading Point

- **미국과 EU는 2021년 9월 무역기술위원회(TTC)를 발족하며 주요 의제로 인공지능(AI)을 채택하여 신뢰할 수 있는 AI 시스템의 개발과 응용 촉진에 협력할 것을 천명**
- **이후 양측은 'AI 신뢰성 및 위험 관리를 위한 평가 및 측정에 관한 공동 로드맵('22.5.)' 공동 개발 및 '공익을 위한 AI 행정협정('23.1.)'을 추진하며 AI 분야에서 구체적이고 포괄적인 협력을 강화**

Ⅰ 개요

❍ 인공지능 일상화 정책 관련 부작용을 최소화하기 위한 규제를 포괄하는 국제적 AI 거버넌스에 대한 관심이 부각되는 가운데, 미국과 EU의 협력이 매우 활발하게 진행

- 미국-EU 간 AI 거버넌스 협력은 2021년 9월에 출범된 무역기술위원회(TTC)[19]가 주요 단초가 되어 보편적 인권과 민주주의 가치를 존중하고 민간산업을 보호·육성할 수 있도록 AI 협력을 도모하는 데 양측이 합의
- 무역기술위원회(TTC)의 2차 회의가 개최된 2022년 5월에는 1차 회의의 후속 조치로써 신뢰할 수 있는 AI 추진과 관련된 로드맵의 공동 개발에 합의
- 2차 회의 결과에 따라 2022년 12월 무역기술위원회(TTC)는 AI 신뢰성 및 위험 관리를 위한 평가 및 측정에 관한 공동 로드맵[20]을 발간

19) U.S.-E.U. Trade and Technology Council
참고자료: https://digital-strategy.ec.europa.eu/en/policies/trade-and-technology-council
https://ustr.gov/useuttc

20) The White House(2022.5.16.), FACT SHEET: U.S.-EU Trade and Technology Council Establishes Economic and Technology Policies & Initiatives

❍ 미국과 EU는 사회 문제 해결과 공익 증진을 위해 2023년 1월, AI 기술 응용을 위한 연구협력을 장려하는 '공익을 위한 인공지능(AI) 행정협정[21]'을 체결

❍ 본 보고서는 최근 미국-EU 간에 이뤄지고 있는 AI 협력 경과에 대한 무역기술위원회 조직·활동, 미국 국무부-EU집행위원회 정보통신총국(DG CONNECT) 간의 협정 분석 등 양측 간 일련의 협력이 지니는 시사점을 살펴보고자 함

〈 미국-EU 간 인공지능(AI) 분야 공동 대응 경과 〉

주체	협력 내용	주요 내용
미국-EU 간 무역기술위원회 (TTC)	미국-EU 간 무역·투자 공조 강화를 위해 TTC 출범 (2021.9)	• 5개 의제 중 하나로 AI 시스템 개발·응용을 채택 • 보편적 인권과 민주주의 가치를 존중하고 민간산업을 보호·육성할 수 있도록 AI 협력을 도모
	신뢰할 수 있는 AI를 위한 로드맵 개발과 공조 선언 (2022.5.)	• 무역기술위원회 제2차 회의를 통해 신뢰할 수 있는 AI를 위한 공동 로드맵을 구축하기로 합의 • 용어, 신뢰할 수 있는 AI 표준, AI 위험 모니터링 시스템 등에 관한 3개 전문가그룹을 구성해 국제 표준을 개발하기 위해 노력
	AI 신뢰성 및 위험 관리를 위한 평가 및 측정에 관한 공동 로드맵 (2022.12.)	• AI 위험 관리 및 신뢰할 수 있는 AI 도구·방법론·접근방식 개발 가이드 제공 • 국제표준화 공동 대응을 위한 실행 계획 제시
미국 국무부, EU집행위원회 정보통신총국 (DG CONNECT)	공익을 위한 AI 행정협정 발표 (2023.1.)	• 사회 문제 해결과 공익 증진을 위한 AI 연구 협력을 장려하는 행정협정에 미국과 EU 대표가 서약

21) Administrative Arrangement on Artificial Intelligence for the Public Good
참고자료: European Commission(2023.1.17.), The European Union and the United States of America strengthen cooperation on research in Artificial Intelligence and computing for the Public Good
https://www.state.gov/under-secretary-fernandez-signs-administrative-arrangement-with-european-commissions-directorate-general-for-communications-networks-content-and-technology-dg-cnect-on-artificial-intellig/

Ⅱ 무역기술위원회(TTC)가 주도한 미국-EU 간의 AI 협력

1 무역기술위원회, 5대 의제 중 신뢰성 있는 AI 채택[22]

○ 미국과 EU는 무역·기술 분야의 협력 촉진을 위해 무역기술위원회 출범에 합의('21.9)

- 무역기술위원회는 중국의 경제부상을 견제하기 위해 출범했다는 분석이 있으며[23], 반도체 공급망 안정화, 수출 통제, 인공지능을 포함한 기술 표준 설정 등의 5대 의제를 설정

※ 5대 의제 추진을 위한 하위 10개 작업반은 ① 기술표준, ② 기술변화와 청정기술, ③ 안전한 공급망, ④ 정보통신기술 서비스 보호와 경쟁, ⑤ 데이터 관리와 기술 플랫폼, ⑥ 안보와 인권 위협 기술의 오남용, ⑦ 수출통제, ⑧ 투자심사, ⑨ 중소기업의 디지털 기술 접근성·사용 촉진, ⑩ 글로벌 무역 현안 등으로 구성[24]

〈 미국-EU 무역기술위원회 5대 주요 의제[25] 〉

의제	주요 내용
비시장 요소[26] 및 무역 장벽 해소	• 글로벌 무역에서 비시장적 관행, 강제노동이나 아동노동 등 노동권 위반 행위 등 글로벌 무역을 왜곡시키는 관행을 해소해 경쟁력과 기술 주도권을 강화
반도체 공급망 강화	• 반도체 공급망의 회복력 강화를 위해 국내 R&D와 공급 생태계를 강화
투자심사 체계 강화	• 안보, 산업 트렌드, 투자 원천, 거래 방식 등을 포괄하는 투자 정보와 민감한 기술과 데이터 관련 투자 리스크도 고려한 투자심사 체계 구축
수출 통제	• 상업용과 군사용의 이중용도(Dual-use)로 활용되는 품목 거래에 대한 수출통제 협력의 강화
신뢰할 수 있는 AI	• 신뢰할 수 있는 AI 시스템의 개발과 응용 촉진

22) EC(2021.9.30.), Trade and Technology Council: Inaugural meeting agrees on important deliverables and outlines areas for future EU-US cooperation

23) 산업통상자원부(2021.12), '미국 ·EU, 중국 포위 겨냥한 무역기술위원회(TTC) 출범', 통하는 세상 VOL.115 https://tongsangnews.kr/webzine/2112/sub2_2.html

24) 각주 23 참고

25) 산업통상자원부(2021.2) 자료 재구성

26) 미국 상무부(The Department of Commerce)는 대중국 무역 수지 적자 문제 해소의 일환으로 중국을 비시장경제(non-market economy)로 지정하며 별도의 덤핑 마진 산출방식을 적용 중. 비시장적 요소는 정부의 개입에 의해 제품이나 서비스의 가격과 비용을 조정하는 행위 등이 포함

❍ 인공지능과 관련해서, 미국과 EU는 ▲AI를 포함한 핵심 및 신기술 분야의 조정·협력을 위한 접근법을 개발하고, ▲미국-EU의 핵심 가치 보호를 위한 기술 표준 개발을 지원하며, ▲신기술 분야의 시민 사회 조직, 스타트업, 중소기업을 위한 표준화 단체 참여 촉진 등에 합의

❍ 미국과 EU는 무역기술위원회를 통해 반도체와 같은 전략 물품의 공급망 안정화와 신뢰할 수 있는 AI 기술의 표준화를 기반으로 한 원활한 디지털 무역체계 구축을 위한 양측 간 공조 방향성을 제시

❍ 무역기술위원회(TTC)의 출범은 미국-EU 주도의 디지털 경제 질서 체계 구축뿐만 아니라 나아가 기술 패권 시대에 중국의 글로벌 기술 영향력 확산을 제어하고 압박하기 위한 전략적 공동 대응 체계로서의 의미도 함께 내포

2 AI 신뢰성 및 위험 관리를 위한 평가 및 측정에 관한 공동 로드맵[27]

○ 무역기술위원회(TTC)는 2022년 5월에 개최된 2차 회의에서 신뢰할 수 있는 AI 마련을 위한 로드맵을 개발하기로 예고했으며, 이후 2022년 12월에 로드맵[28]을 공개

- 양측은 로드맵을 토대로 한 국제 AI 기술 표준 설정을 위해 노력
- 동 로드맵에서는 경제협력개발기구(OECD) AI 권고안[29]에 제시된 주요국 공동체의 약속을 지키기 위한 실질적인 조치들을 담고 있음

※ OECD 권고안은 신뢰할 수 있는 AI 기술의 책임감 있는 보급을 위해 다음의 5개 원칙을 제시

① AI 시스템은 포용 성장, 지속가능한 개발, 웰빙을 통해 인간과 지구에 혜택을 주어야 함
② AI 시스템은 법제와 인권, 민주적 가치와 다양성을 존중하는 방식으로 설계되어야 함
③ AI 시스템에 대한 투명성·책임성 있는 공개가 이루어져 결과물을 시험할 수 있어야 함
④ AI 시스템은 잠재적인 위험이 지속적으로 평가 관리되어야 함
⑤ AI 시스템을 개발, 보급, 운영하는 기관과 개인은 상기 원칙들에 부합하도록 책임을 져야 함

○ **(위험 기반 접근법)** 미국과 EU는 AI 시스템의 긍정적인 영향과 이점을 극대화하기 위해 개인, 문화, 경제, 사회 및 지구에 미치는 부정적인 영향을 최소화해야 한다는 데 로드맵의 대원칙을 확인

- 양측은 신뢰할 수 있는 AI를 발전시키기 위해 사회적 요인과 기술적 요인을 복합적으로 고려한 위험 기반 접근 방식 적용을 강화하기로 했으며, 현재 AI 분야의 정책 및 법률 제정 활동을 통해 다양한 조치를 실행 중
- 공동 로드맵에서는 미국과 EU의 접근 방식과 관련하여 과학, 국제표준, 공유 용어, 검증된 지표 및 방법론의 중요성을 부각해서 강조
- 이에 따라, 양측의 각 규제, 정책 및 입법 이니셔티브와 양립할 수 있는 활동을 제안

---

27) The White House(2022.5.16.), FACT SHEET: U.S.-EU Trade and Technology Council Establishes Economic and Technology Policies & Initiatives

28) European Commission(2022.12.10.), TTC Joint Roadmap for Trustworthy AI and Risk Management https://ec.europa.eu/newsroom/dae/redirection/document/92123

29) OECD(2019.5.21.), Recommendation of the Council on Artificial Intelligence

〈 AI 위험 기반 접근법 관련 미국과 EU의 법률·정책 〉

국가	법률/정책	주요 내용
미국	국립표준기술원(NIST) AI 위험 관리 프레임워크 초안[30]	• AI와 관련된 위험을 구성하는 방법에 대해 논의 • 신뢰할 수 있는 AI 시스템의 특성과 조직이 실제로 AI 시스템의 위험을 해결하는 데 도움이 되는 4가지 특정 기능(거버넌스, 매핑, 측정, 관리)에 관해 기술
	과학기술정책국(OSTP) AI 권리장전 청사진[31]	• ① 안전하고 효과적인 시스템 구축, ② 알고리즘을 통한 차별 방지 ③ 데이터 관련 사생활 보호, ④ 자동화 시스템의 활용에 대한 고지와 설명, ⑤ 인간 대안 마련 등 5가지 원칙 제시
EU	EU AI Act(초안)[32]	• 민주적 가치 보호, 신뢰할 수 있는 AI 시스템 정착 등을 위한 엄격한 기준을 적용한 규범을 담은 법안으로, 위험의 정도에 따라 차등화된 규제를 적용 • **(금지 AI 시스템)** EU의 가치를 침해하고 사람들의 안전·생계·권리에 명백한 위협이 되는 시스템으로, ▲인간의 행동을 조작하는 AI 시스템, ▲정부의 사회평가 시스템, ▲실시간 원격 생체 신원확인 시스템 등을 규정했으며, 이후 수정 법안에서 ▲'예측적 치안'[33]이 새롭게 추가 • **(고위험 AI 시스템)** 사람들의 건강·안전·기본권에 부정적인 영향을 끼칠 수 있는 시스템으로, ▲생체인식 시스템, ▲주요기반시설의 관리 및 운용, ▲교육 및 직업훈련, ▲고용, 근로자 관리 및 자영업, ▲필수 공공·민간 서비스, ▲기본권을 간섭할 수 있는 법 집행, ▲이민·망명·국경관리 등을 규정
	AI 고위전문가그룹(HLEG) 신뢰할 수 있는 AI 윤리 가이드라인[34]	• '시민 복지'라는 인간중심의 윤리적 목적을 달성하면서 신뢰할 수 있는 기술 발달 기준을 구체적으로 제시 • 특히 신뢰할 수 있는 AI는 기본권을 보호하고 윤리적 목적 달성과 공익 강화에 기여해야 함

30) National Institute of Science and Technology(2023.1.), AI Risk Management Framework https://www.nist.gov/itl/ai-risk-management-framework

31) Office of Science and Technology Policy(2022.10.), Blueprint for an AI Bill of Rights

32) European Commission(2022.4.), The Artificial Intelligence Act

33) Predictive Policing으로, 치안 구역 범위 내의 범죄, 인구통계 데이터셋을 기반으로 지역, 시간대, 범죄 유형 등을 예측하는 방법

34) EC High-Level Expert Group(HLEG)(2019.4.), Ethics Guidelines for Trustworthy AI

○ **(로드맵 활동)** 로드맵 추진을 위한 양측의 실행 사항은 ① 공통 용어 및 분류법 개선, ② 국제 기술 표준·도구 개발 활동을 위한 리더십 및 협력, ③ 기존 및 새로운 AI 위험 상황에 대한 모니터링·측정의 3대 영역을 중심으로 추진

〈 미국-EU AI 공동 로드맵: 주요 활동 〉

3대 영역		주요 내용
공통 용어 및 분류법 개선		• 기본 용어에 대한 이해를 공유함으로써 표준 개발과 책임, 관행·정책 확인 시 상호 공동으로 활용할 수 있는 분류 체계를 확보 • 국제 표준화기구(ISO), 경제협력개발기구(OECD), 전기전자공학회(IEEE) 등의 기존 글로벌 표준 수용 • 미국과 EU 양측의 현행 규제 및 법률 고려
국제 기술 표준 및 도구 개발 리더십과 협력	국제 기술 표준	• 미국과 EU는 각자의 법률 시스템의 특수성, 요구사항을 침해하지 않고 WTO 기술장벽(TBT) 원칙[35]*을 준수 • 양측의 이해관계자 및 관련 조직들과의 협력 체계 내에서 기존 국제 AI 표준 개발 활동의 주요 미비점 확인 • 다양한 이해관계자가 지속적으로 AI 표준 개발 작업에 참여하도록 장려 • 개방적이고 투명하며, 기술적으로 건전하고, 성과 중심적이며 공공·민간 부문에서 사용하기에 적합한 국제 AI 표준 개발 및 자발적 활용을 촉진
	AI 위험 관리 도구	• AI 신뢰성, 위험 관리 방법 및 관련 도구를 측정하기 위한 지표 및 방법론에 대한 공통 지식 기반(허브 또는 저장소) 구축에 협력 • 상호운용 가능한 위험 관리 전략, 평가 및 측정 도구 개발 및 이와 관련된 연구 활동 지원
AI 위험 모니터링 및 측정	AI 위험 범주 추적 체계	• 맥락·상황, 활용 사례 및 AI 사고(incidents)·영향·피해에 대한 경험 데이터를 기반으로 기존 및 새로운 위험, 위험 범주 추적 체계(tracker)를 개발 • AI 시스템 개발 및 활용과정에서 다양하게 발생하는 신규 및 잠재적 위험 요소에 대한 이해 제고, 다수의 시스템 간 상호작용으로 인한 복합적 위험, 또는 새로운 AI 방법이나 활용 맥락에서 발생할 수 있는 예측 가능한 위험 등을 추적 대상으로 함
	AI 위험 테스트 및 평가	• 평가 시 AI 시스템의 정확도뿐만 아니라 동작 환경을 고려하여 피해와 이점을 평가 • 최신 기술, 다양한 AI 시스템 아키텍처, 대규모 딥러닝 시스템 동작 프로세스 등 성능 측면의 신뢰성도 함께 평가

35) Technical Barriers to Trade의 약자로 기술 규정, 표준, 적합성 평가 절차 등이 국가 간의 교역에 불필요한 장애요인을 형성하는 것을 포괄적으로 지칭

❍ **(실행 계획)** 로드맵은 ▲포괄적인 협력 채널 구축 공유 용어, ▲분류 체계 고도화, ▲AI 표준, ▲도구 개발, ▲기존 및 새로운 AI 위험 모니터링 및 측정 등의 4개 분야에 걸쳐 단기와 장기로 구분하여 목표 달성 메커니즘을 구성

〈 미국-EU AI 공동 로드맵: 실행 계획 〉

구분	단기	장기
포괄적인 협력 채널 구축	• ① AI 용어 및 분류법, ② 신뢰할 수 있는 AI 및 위험 관리를 위한 AI 표준 및 도구, ③ 기존 및 새로운 AI 위험 모니터링 및 측정 등 3개의 전문가 실무 그룹(working groups)을 구성 및 작업 계획 개발	• 전문가 워크숍 실시 • 로드맵 업데이트 및 추진 경과 공유
분류 체계 고도화	• 주요 EU·미국 문서 및 국제 표준의 용어 및 분류 체계 매핑	• 용어 및 분류에 대한 공통의 체계 개발 및 수정
AI 표준	• EU나 미국의 이해관계에 부합하는 국제표준 현황 분석 수행과 국제표준 개발에 대한 각 당사자의 참여 및 기여 수준 평가 • 미국-EU 간 공통의 국제표준 관심 영역 식별	• 세부 주제별 국제표준화 포럼을 통한 협력 체계 조직
도구 개발	• 도구의 선택, 포함 및 수정 프로세스 수립 • 신뢰할 수 있는 AI 도구에 대한 평가 기준을 설정	• 공유 허브/저장소에 추가할 지표와 방법론 확인 • 공유 허브/저장소를 업데이트하고 유지 및 관리
AI 위험 모니터링 및 측정	• AI 활용 사례 및 사고 보고에 기반한 기존 AI 위험을 추적하기 위한 목표 및 방법론 수립 • 새로운 AI 위험에 대한 테스트 및 평가를 위한 연구 방법론을 발굴	• AI 사고에 대한 경험적 연구를 통해 확보한 AI 위험 벤치마크 및 평가 툴 생성 • 이론 및 분석에 기반한 위험 예측

Ⅲ 미국-EU 간 공익을 위한 AI 행정협정[36]

❍ 2023년 1월, 미국 국무부(DoS)[37]와 EU 집행위원회는 AI 응용과 연구 역량 강화를 도모하기 위해 '공익을 위한 인공지능(AI) 행정협정'을 체결

- 미 국무부(DoS)의 호세 페르난데스(Jose W. Fernandez) 경제성장·에너지·환경 담당 차관과 EU 집행위원회의 로베르토 비올라(Roberto Viola) 정보통신총국(DG CONNECT) 국장 간에 체결
- '인터넷의 미래를 위한 선언(Declaration for the Future of the Internet)'*에 명시된 원칙과 글로벌 과제 해결을 목표로 새로운 디지털 기술을 사용하는 것에 대한 공동의 이익과 가치 실현에 중점을 두고 작성

  * 인터넷과 디지털 기술의 낙관적 미래로 나아가기 위해 2022년 4월 미국 국무부(DoS) 주도하에 60여 개국이 참여하여 작성한 선언문으로, ▲인권 보호, ▲국가 간 정보의 자유로운 이동, ▲디지털 경제의 포용성 강화, ▲디지털 생태계 내 프라이버시 보호를 포함한 신뢰, ▲다양한 이해당사자들의 이익 보장 등을 주요 기치로 삼고 있음[38]

- 즉, 공통의 가치를 공유함과 동시에 관련 역량이 부족한 국제 파트너들과 연구 결과, 자원을 공유하여 현재와 같은 비상 상황과 도전을 관리하는 데 기여할 것을 도모

❍ EU 집행위원회에 따르면, AI 행정협정이 ▲기후 변화, ▲자연재해, ▲보건 및 의료, ▲전력망 최적화, ▲농업 등 5대 분야를 중심으로 광범위한 사회적 혜택을 창출할 수 있는 AI 연구 결과를 공유하며, 발전시키는 데 기여할 것

- 전 세계적으로 홍수나 화재와 같은 기상이변과 자연재해가 점점 더 빈번해지고 파괴력도 커짐에 따라, AI는 재난 대비와 비상 대응에 도움이 되는 예측 및 시뮬레이션에 더욱 중요한 역할을 하게 될 것
- AI 연구 및 컴퓨팅은 토양 및 대기 조건, 조류·곤충 동향, 식재, 관개, 살충제 및 비료 사용, 수확 주기 등의 자연조건을 분석하고 모델링하여 농작물 수확량, 효율성 및 지속

---

36) European Commission(2023.1.17.), The European Union and the United States of America strengthen cooperation on research in Artificial Intelligence and computing for the Public Good

37) The U.S. Department of State

38) https://www.state.gov/declaration-for-the-future-of-the-internet

가능성을 크게 향상시킬 수 있는 잠재력을 보유

- AI는 이미 의료 연구, 진단 및 치료를 강화하고 있으며, 최근 팬데믹으로 인해 범세계적인 접근 방식의 필요성이 강조되고 있지만 동시에 국가 간 격차 문제도 크게 부각

❍ 미 국무부(DoS) 측은 이번 협정이 전 세계 과학계 내의 공동 과학 및 기술 연구 기회를 제공하고 투명성, 공정성, 개인정보보호 등의 민주적 가치 수호 하에 AI 활용의 비전을 제시한다고 언급

- 이와 관련하여, 최근 미국은 연방 부처들을 중심으로 신뢰할 수 있는 AI 개발 및 AI의 부작용 대응을 위해 다양한 규정 및 전략 개발 노력을 강화

❍ 이 행정협정은 양측 간 구체적 협력 실행 계획을 담고 있지는 않으나 AI 분야의 응용과 연구개발을 위한 포괄적 협력에 공조키로 했다는 점에서 의의를 지니며, 향후 동 협정에 따른 다양한 후속 조치들이 이어질 것으로 예상

〈 미국 연방정부가 추진 중인 AI 규제 및 정책 대응 〉

연방 부처	시점	AI 규제 및 정책
연방거래위원회 (FTC)	2021.4.	• (FTC 블로그 입장문[39]) 연방거래위원회법(FTC Act)의 위반 가능성을 줄이고 FTC의 규정을 준수하기 위해 다음의 사항을 고려할 것을 언급 - 데이터셋 구축 시 편향성 최소화 방안 마련 - 왜곡된 AI 결과 도출 여부 확인 - 투명성과 독립성 유지 - 알고리즘과 비편향적 결과에 대한 과신 금물 - 법적 테두리 내에서 학습데이터 활용 - 알고리즘과 결과물에 대한 설명가능성 확보
연방거래위원회 (FTC)	2021년 가을	• (규칙제정 절차 착수[40]) FTC 법 제18절 하에서 개인정보 남용 제약, AI 차별, 사기 및 관련 데이터 오용 문제에 대해 FTC의 재량 하에 처리하는 규정 제정 검토 착수
주택도시개발부 (HUD)	2021.6.	• (주택 관련 알고리즘 규제 복원[41]) 트럼프 행정부 당시 대출 시 은행이나 보험사가 유색 인종 차별을 위한 편향적 알고리즘을 활용하는 것에 대해 고소를 불가능하게 하는 규정을 제정

연방 부처	시점	AI 규제 및 정책
주택도시개발부 (HUD)	2021.6.	했으나, 2021년 6월 바이든 정부 이후 편향적 알고리즘에 대한 고소를 허용하는 규정을 재차 복원
평등고용기회위원회 (EEOS)	2021.10.	• (공정 알고리즘[42]) 채용 AI 시스템 알고리즘의 공정성을 담보하기 위한 이니셔티브에 착수
연준을 비롯한 5개 금융기관	2021.3.	• (AI 관행 조사[43]) 연방준비제도이사회를 비롯한 5개 금융 규제기관[44]은 위험 관리, 공정한 대출 및 신용도에 영향을 미칠 수 있는 금융기관의 AI 관행에 대한 조사에 착수
국립표준기술연구 (NIST)	2023.1.	• (AI 위험 프레임워크[45]) 개인, 조직 및 사회가 직면할 수 있는 AI 관련 위험 관리 프레임워크(ver. 1.0) 개발

39) FTC Business Blog(2021.4.19.), Aiming for truth, fairness, and equity in your company's use of AI
40) Reginfo.gov(2021 Fall), Trade Regulation Rule on Commercial Surveillance
41) Federal Register(2021.6.25.), Reinstatement of HUD's Discriminatory Effects Standard
42) EEOC(2021.10.28.), EEOC Launches Initiative on Artificial Intelligence and Algorithmic Fairnes
43) CFPB(2021.3.29.), Agencies Seek Wide Range of Views on Financial Institutions' Use of Artificial Intelligence
44) 연방준비제도(FRB, (FRB: Federal Reserve Board), 소비자금융보호국(CFPB, Consumer Financial Protection Bureau), 연방예금보험공사(FDIC, Federal Deposit Insurance Corporation), 전국신용조합감독청(NCUA, National Credit Union Administration), 통화감독청(OCC, Office of the Comptroller of the Currency)
45) NIST(2023.1.26.), NIST AI Risk Management Framework (AI RMF 1.0) Launch

Ⅳ 평가 및 시사점

❍ 미국-EU는 실행 단위에서의 다양한 AI 정책에 공조를 구체화할 뿐만 아니라 최근의 AI 행정협정을 통해 협력의 범위도 확장

- TTC 출범을 계기로 본격화된 미국-영국 간의 AI 기술 분야의 공조는 신뢰할 수 있는 AI 개발을 위한 공동 로드맵 개발을 거쳐 최근의 공익을 위한 AI 행정협정에 이르기까지 선언적 협력의 구체적 실천과 함께 그 범위도 포괄적으로 확산되는 양상으로 전개

❍ 미국은 AI 규제 및 정책 개발에 속도를 내며 EU와의 공조 환경이 점차 개선

- AI 규제 논의가 상대적으로 EU에 비해 뒤처진 미국은 바이든 정부 이후 AI 편향성 극복을 위한 규정 개발과 함께 주요 부처 단위에서 공정한 알고리즘 적용 정책과 이니셔티브를 다양하게 발표하는 등 EU의 AI 규제 전략과 적극적으로 보조를 맞춰가고 있는 것으로 관찰
- 2023년 1월에 공개된 AI 위험 관리 프레임워크(v.1.0)는 신뢰할 수 있는 AI 시스템 개발과 관련된 구체적인 가이드를 제공함으로써 '금지 AI 시스템'과 '고위험 AI 시스템' 등 AI 시스템에 따른 차등적 규제를 주요 내용으로 담고 있는 EU의 AI 법안에 준하는 유사한 관리 접근법을 제시
- 미국 상원에서는 2023년 1월 플랫폼 책임 및 투명성 법안[46]을 발의하는 등 의회 차원에서 AI뿐만 아니라 소셜 미디어 전반에 걸친 플랫폼에 대한 사업자들의 의무 준수를 요구하는 등 의회 차원의 입법 노력도 활발하게 이뤄지고 있음

❍ 미국-EU 간 AI 분야의 공조는 기술 발전 촉진과 글로벌 표준 주도권의 우위를 선점

- 대서양 양안의 거대 경제권인 미국과 EU 간의 신뢰성 기반 AI 개발을 둘러싼 협력은 양측 간 공조에 의한 AI 학습 촉진을 통해 AI 시스템의 성능 향상에 기여
- 또한, AI 연구 생태계 내 신뢰할 수 있는 안전한 AI 시스템 개발을 독려하며 이와 관련된 글로벌 기준점을 제시하게 될 것

---

46) GovTrack(2023.1.26.), S. 111: Providing Accountability Through Transparency Act of 2023

❍ 국내에서는 2021년 5월 관계부처 합동에 의해 '신뢰할 수 있는 인공지능 실현 전략(안)'을 마련한 바 있으며, 이 같은 정책 수립 노력은 최근 주요국 중심으로 강조되고 있는 AI 전략과 일관된 움직임으로 평가

- 향후 해당 전략 개정 시에는 EU와 미국 및 EU-미국 간 공조를 통해 개발이 추진되고 있는 신뢰할 수 있는 AI와 관련된 정부 가이드라인과 규정, 법률 제정 및 표준 수립 동향을 면밀히 파악하여 이와 보조를 맞춘 정책 및 입법 대응 요청
- 특히 고위험 AI 시스템의 정의와 범위, AI 영향 평가 항목 등의 경우 미국과 EU가 추진 중인 정책 및 기술 문서와의 일관성 검토를 통해 보다 효과적인 추진이 가능할 것

NEWS 1 미국, 제5차 열린정부 국민행동계획 발표[47)]

❍ 미국 백악관이 보다 포괄적이고, 대응적이며, 책임감 있는 정부로 도약하기 위한 범정부 차원의 '제5차 열린정부 국민행동계획'을 발표

※ 2011년 오바마 정부에서 제1차 '열린정부 국민행동계획'이 공개됐으며, 이번 계획은 바이든-해리슨 정부에 접어들어 최초로 제시된 전략

❍ 이번 계획에서는 소외, 배제, 차별을 겪는 공동체의 포용성 촉진을 강조

- 제5차 열린정부 국민행동계획은 5대 영역*에 걸쳐 정부의 목표를 제시

* ① 정부 데이터, 연구 및 정보에 대한 접근성 개선, ② 시민 참여를 위한 시민 공간 확대 ③ 정부 서비스 제공 혁신, ④ 부패 대응 및 국민에 대한 정부의 성실성과 책임성 보장, ⑤ 법 아래서 평등한 정의 보장

❍ 제5차 열린정부 국민행동계획에서는 특히 데이터 공유 환경 개선과 연방 부처 보유 데이터 개방의 중요성이 부각

- 국민 구성원이 자유롭게 데이터를 요청하고 접근할 수 있는 피드백 메커니즘을 구축함으로써, 연방·주정부·지자체, 지역사회 기반 조직 및 연구자들과의 파트너십·협업을 통해 공정성(equity) 향상을 위한 정부의 책임 강화
- 공공 데이터 이용자와 연방 데이터 관리자 간 피드백 루프 개선, 국민 참여, 투명성·책임을 강화하여 효과적이고 공정한 데이터 관행 개발

※ 국가과학기술위원회(NSTC)[48)] 공정데이터소위원회(Subcommittee on Equitable Data)를 통해 정부 부처 정보·소식 전파 및 토론 등을 위한 ▲메일링 리스트(listserv) 운영, ▲사용법 가이드와 같은 안내자료 제공, ▲부처 간 경험 공유 웨비나 등으로 실무 커뮤니티 조성

---

47) The White House(2022.12.28.), White House Releases Fifth Open Government National Action Plan to Advance a More Inclusive, Responsive, and Accountable Government

48) National Science and Technology Council. 백악관 직속 조직으로 국가 과학기술 정책 총괄 역할을 담당

NEWS 2 튀르키예, 블록체인 기반 디지털 ID 적용 계획 발표[49]

❍ 튀르키예 푸아트 옥타이(Fuat Oktay) 부통령은 온라인 공공서비스 로그인 절차에 블록체인 기술을 활용한 디지털 ID를 활용할 계획을 발표

- 옥타이 부통령은 블록체인 기반 애플리케이션이 전자정부 혁신의 일환으로 개발됐으며 정부의 디지털 서비스 안전성과 접근성 향상을 기대한다고 언급
- 이번에 개발된 블록체인 기술은 디지털지갑 애플리케이션과 함께 개인의 정보를 휴대폰상에 저장할 수 있도록 설계
- 앞서 튀르키예 중앙은행은 2022년 12월 말 중앙은행 디지털화폐(CBDC)[50] 파일럿 시험에서 결제 거래에 성공하였으며, 디지털 ID의 필요성을 시사[51]한 바 있어, 향후 튀르키예 디지털 ID 보급이 탄력을 입게 될 것으로 관측

❍ 한편, 튀르키예는 과거 수년간 다수의 블록체인 프로젝트를 추진했으나, 현재 실제 적용까지 이어진 사례는 거의 없었던 상황

- 튀르키예는 2019년부터 국가 블록체인 인프라 구축 계획에 착수했으나, 몇몇 개념검증(PoC) 프로젝트와 수차례의 지연 끝에 실행된 중앙은행 디지털화폐 테스트 외에는 블록체인 프로젝트의 후속 사업이 미진
- 2020년 1월 당시 튀르키예의 문화 중심지인 콘야(Konya)에서 시민들의 공공서비스 비용 지불에 사용할 수 있는 '시티 코인(City Coin)' 프로젝트를 착수했으나, 최근 2년간 프로젝트 관련 업데이트 사항은 공개되지 않고 있는 실정

49) CoinTelegraph(2023.1.2.), Turkey to use blockchain-based digital identity for online public services
50) Central Bank Digital Currency
51) Ledger Insights(2023.1.3.), Turkey launches CBDC pilot, introduces blockchain digital ID

NEWS 3 EU 집행위원회, '2030 Digital Decade'[52] 목표 달성을 위한 협력 개시[53]

❍ EU 집행위원회는 '2030 Digital Decade' 정책 프로그램 목표 달성을 위해 유럽의회와 회원국과 협력하여 4가지 핵심 영역*에서 구체적 공동목표를 설정하고 주기적인 협력 과정을 구축하기 위한 절차를 개시

* ① 디지털 기술, ② 연결 인프라, ③ 기업 디지털화 및 ④ 온라인 공공서비스 등

❍ 회원국은 9개월 이내로 각 국가별 전략 로드맵을 작성할 예정

※ 목표와 목표 달성을 위해 국가 차원에서 계획한 정책, 조치 및 행동 등을 기술

〈 '2030 Digital Decade' 목표 달성을 위한 협력 및 모니터링 프로세스 〉

시기	계획내용
2023년 상반기	• 디지털경제사회지수(DESI)를 활용하여 각 목표를 달성하기 위한 과정을 추적하는 데 사용될 핵심성과지표(KPI)를 개발
2023년 6월	• 첫 번째 연례 추진현황 보고서('State of the Digital Decade') 발간 예정 • 현 진행 상황을 검토하고, 평가 및 권고사항을 제공
2023년 10월	• 각 회원국에서 첫 번째 국가별 전략 로드맵을 제출 • EU 집행위원회는 각 로드맵을 지원하기 위한 안내자료를 출간

❍ EU 집행위원회, 유럽의회, 그리고 EU 회원국의 협력은 '디지털 권리와 원칙에 관한 기관 간 선언('22.1.26.)[54]을 기반하여 추진

---

52) EU가 디지털 대전환을 위해 향후 10년 동안 추진할 디지털 원칙과 2030년까지 달성할 정책 목표 등을 제시

53) European Commission(2023.1.9.), First cooperation and monitoring cycle to reach EU 2030 Digital Decade targets kicks off

54) Declaration on Digital Rights and Principles이며, ①사람을 중심으로 한 디지털 변혁과 ②결속 및 포용을 지지하고 ③온라인 선택에 대한 자유를 보장하며, ④디지털 공공 공간에의 참여를 장려하고 ⑤개인의 안전 및 보안과 권한을 강화하고 ⑥디지털 미래의 지속가능성을 촉진하는 등을 강조
참고자료: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

NEWS 4 미국 CISA, 사이버 위협 식별을 위한 데이터 분석 플랫폼 구축[55]

❍ 미국 사이버보안 및 사회기반시설 보안국(CISA)[56]은 국토안보부[57] 산하 과학기술국[58]과 함께 사이버 위협에 대한 통찰력을 제공·공유하기 위해 기계학습 기술을 활용한 데이터 분석 플랫폼 'CAP-M'[59]을 개발 중

❍ 사이버보안 및 사회기반시설 보안국의 CAP-M를 온프레미스[60] 및 멀티 클라우드[61] 시나리오 모두에서 사용할 계획

- CAP-M에서 이루어진 다양한 실험을 통해 도출된 데이터 및 이들의 상관관계를 분석하게 될 것이며, 실험에 활용되는 데이터의 프라이버시도 보장할 것
- 실험 데이터는 학술기관, 기업을 포함한 민간부문과 타 정부 부처에도 제공되어 모든 조직이 사이버 보안 위협으로부터 자신을 보호할 수 있도록 지원할 예정

※ 국토안보부는 CAP-M 처음에는 사이버 임무 지원 역할을 할 것이지만, 이후 다른 기반시설의 보안 임무를 위한 데이터 세트, 도구 및 협업을 지원하는 등으로 확장할 것으로 기대

❍ 인공지능 및 기계학습 기술의 사이버 위협 분석 능력에 대한 기대가 존재하나, 아직 CAP-M에 관한 구체적인 내용과 일정은 제공되어 있지 않은 상황

- 사이버보안 전문가들은 대체로 사이버 위협을 방지·감소하는 데 도움이 되는 도구로

---

55) TechRadar(2023.1.10.) The US government is building an AI sandbox to tackle cybercrime
56) Cybersecurity and Infrastructure Security Agency (CISA)는 미국 국토안보부 산하기관으로, 사이버 및 물리적 인프라에 대한 위험을 이해 증진 및 위험관리에 기여 (https://www.cisa.gov/about-cisa)
57) Department of Homeland Security (DHS)
58) Science and Technology Directorate (S&T)
59) CAP-M (CISA's Advanced Analytics Platform for Machine Learning)
60) 온-프레미스 컴퓨팅은 기업이나 조직이 하드웨어, 소프트웨어 등 모든 컴퓨팅 환경을 자체적으로 구축하고, 운영·유지·관리하는 것을 말하며, 클라우드 컴퓨팅 기술을 사용하지 않는 전통적인 서버나 데이터 센터를 의미 (출처: TTA 정보통신용어사전)
61) 두 개 이상의 독립적인 클라우드 서비스 제공자가 제공하는 복수의 공용 클라우드 서비스들을 연계하여 사용하는 클라우드 컴퓨팅 환경 (출처: TTA 정보통신용어사전)

활용될 것을 기대

- 하지만 기계학습 모델의 일반화로 인한 부작용, 대중 또는 다른 국가의 악의적 이용 등을 우려하는 전문가도 존재

〈 AI 샌드박스에 대한 전문가들의 반응 〉

구 분	내용
비밀번호 관리 솔루션업체 'Keeper Security' CTO Craig Lurey	• 미국 연방정부의 연구개발(R&D) 사업은 민간부문 사이버 보안업체가 개별적으로 수행하는 R&D를 지원·촉진하는 데에 도움이 될 것 • 사이버보안은 국가안보와 연결되어 있으며, 정부의 지원이 필요
보안취약점 식별 솔루션업체 'Contrast Security' 부사장 Tom Kellermann	• CAP-M이 TTP* 정보 공유를 개선하고 미국의 사이버공간에 대한 상황인식을 향상할 중요한 프로젝트라고 평가 *TTPs: tactics(전술), techniques(기술), procedures(절차)
모의해킹(Pentest) 플랫폼 'Horizon3.ai' 이사 Monti Konde	• 사이버보안 전문가와 실무자는 너무 많은 허위 해킹·보안 신고로 '경고 피로(alert fatigue)'를 경험하고 있음 • CAP-M을 통해 실시된 실험은 현실의 복잡성과 노이즈를 완전히 반영할 수 없다는 한계를 가지지만, 일단 긍정적인 영향을 미칠 것으로 기대 • CAP-M 인공지능 모델 훈련을 위해, 모의해킹 공격을 자동으로 실행해 실제 보안 위협을 식별하는 데 활용할 수 있음
사이보보안업체 'Cerberus Sentinel'[62] 생체인식 전문가 Sami Elhin	• 기계학습을 활용한 데이터 분석으로 사이버보안 공격에 대한 깊은 이해를 끌어낼 수 있을 것으로 기대 • 하지만 기계학습 모델의 일반화로 인해, 상대적으로 작은 표적에 대한 위협이 필터링되고 모니터링·식별 대상에서 배제될 수 있음 • 인공지능 또는 기계학습 모델이 대중에게 노출되면, 악용될 가능성도 증가하며 다른 국가가 CAP-M를 표적으로 삼아 데이터 분석을 방해할 가능성이 존재

62) CISO Global로 회사명칭을 변경 중 (https://www.ciso.inc/)

NEWS 5 영국, 미성년자 주류 구매 방지 등을 위한 시범사업 실시[63]

❍ 영국 내무부(Home Office)와 제품안전기준국(OPSS)[64]은 2022년에 주류를 판매하는 매장에서 구매자의 나이를 추정·확인하기 위한 9개 시범사업[65]을 실시

- 각 시범사업은 디지털 ID 생성, 얼굴인식 알고리즘, 손가락 정맥 생체정보 등록 등의 다양한 기술을 활용해 미성년자의 주류 구매 방지에 기여

  ※ 각 시범사업이 활용한 기술, 기술을 도입한 장소, 사업 기간 등이 다르지만, 시범사업의 목적은 동일하며 영국 제품안전기준국에서 관리

- 더 나아가 매장 직원을 향한 공격적 언사·행동, 행사장 밖 긴 대기 줄로 인한 혼잡 등이 감소하여, 매장 직원들의 만족도가 향상

❍ 시범사업에 대한 전반적 반응은 긍정적이나, 나이 추정·확인 기술이 도입된 장소와 방식에 따라 평가가 다소 엇갈림

- 매장 내 셀프계산대 등에 얼굴인식 기술이 활용된 경우, 대체로 긍정적으로 반응
- 디지털 ID 애플리케이션을 설치하는 시범사업의 경우, 활용 수준은 낮음
- 클럽이나 술집을 대상으로 한 시범사업에 대한 평가는 불명확
- 영국 내무부는 2022년 동안 시행한 시범사업에 대한 최종보고서를 발표하지 않았으며, 요약 사례[66]만 내무부 홈페이지를 통해 간단히 소개

---

63) BiometricUpdate.com(2023.1.11.), Success of age estimation, digital ID trials in UK lead to pressure for changes to the law

64) The Office for Product Safety and Standards. 사업·에너지·산업전략부(Department for Business, Energy and Industrial Strategy) 내 영국 유통 제품에 대한 안전과 무결성과 관련된 규제를 담당하는 조직

65) Home Office & OPSS(2022.12.30.), Form- Details of the trials
https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox/details-of-the-trials

66) 각주 65번 참고

❍ 영국 소매업계 대표 단체인 '영국소매컨소시엄(BRC)[67]'은 내무부의 성공적 시범사업 결과에 따라, 주류 구매 나이 인증에 관한 법 개정을 요구

- 현행 인허가법(Licensing Act 2003) 하에서는 주류 구매가 18세부터 허용이 되며, 판매자는 18세 미만으로 추정되는 청소년에게 반드시 유효한 신분증을 요구해야 함
- 특히 주류 구매를 위해 요구되는 신분증은 물리적인 ID여야 하며 자외선이나 홀로그래픽 요소를 반드시 갖출 것을 의무화
- 영국소매컨소시엄에 따르면, 디지털 나이 추정·확인 기술을 활용해 주류 판매장의 안정성을 높이고, 고객 응대 시간 단축, 직원에 대한 폭력 감소가 가능

  ※ 영국소매컨소시엄의 자체 조사에 따르면 소매 판매장 직원들은 매일 1,300건 이상의 폭력과 학대에 노출되며, 이중 가장 빈번한 사례가 주류 구매자 나이 확인 중 발생
- 이미 담배, 칼, 의약품과 제품을 구매할 때 디지털 솔루션을 통해 나이 확인이 가능해, 영국소매컨소시엄은 이를 주류 판매 분야로 확장해야 한다고 주장

〈 영국 내무부 연령 추정 시범사업 사례: 요티(Yoti) 〉

- **(개요)** 영국 정부의 디지털 ID 솔루션 공급사인 요티(Yoti)는 슈퍼마켓 체인인 아스다(Asda), 모리슨(Morrison), 더코업(The Co-op) 등의 매장을 대상으로 시범사업을 실시
- **(배경)** 영국의 대부분 슈퍼마켓과 의류 상점에서는 무인 계산대를 설치하고 있어, 구매 연령 제한 제품을 스캔하려면 직원이 해당 계산대에 와서 고객의 나이를 확인하고 구매 허용 코드를 입력
  - 일부 매장에는 체크아웃 매대 위에 카메라를 설치하여 원격 모니터링을 통해 구매자 나이를 확인하고 있어, 고객 불만이 커지고 있으며, 심지어 불매운동으로 이어짐
- **(연령 추정 절차)** 시범사업에 참여하는 매장에서는 고객들이 계산대에 연결된 카메라를 들여다보며 연령 추정을 위한 이미지를 제공 → 카메라를 통해 캡처된 이미지에 대해 요티(Yoti)는 얼굴 분석을 실행하여 판매 여부를 판단 → 수집 이미지 삭제
  - **분석 결과에 오류가 발생할 경우,** 매장 체크아웃 화면에 요티 앱이나 요티가 제공하는 우체국 EasyID 앱에서 제공하는 QR 코드를 스캔하여 나이를 인증
  - 앱을 활용할 수 없다면, 기존과 같이 직원에게 연령 확인을 요청

67) The British Retail Consortium

NEWS 6 웨일스, 임신·출산 통합시스템 구축 예정[68]

❍ 웨일스(Wales) 정부는 산모와 태아가 받는 서비스를 개선하기 위해 700만 파운드 투자해 통합 디지털 시스템을 구축할 예정

- 현재 일부 보건기구는 디지털 시스템으로 서류를 처리하고, 일부 기구는 종이로 처리
- 보건기구가 활용하는 시스템이 혼재한 상황이며, 임신·출산 서비스 관리를 위한 통합 시스템 구축이 필요
- 특히 통합시스템을 구축하면 의료전문가들이 신속히 다른 전문가들과 산모의 건강정보를 공유할 수 있어, 잠재적인 합병증 위험을 줄이고 안전하고 효과적인 관리가 가능

❍ 새로운 시스템은 건강한 임신·출산을 지원하기 위해 임산부에게 적시에 메시지를 전달하고 자신의 건강정보 기록을 편리하게 볼 수 있도록 설계 예정

〈 구축 예정 통합시스템의 주요 기능 〉

기능	내용
건강정보 공유	• 산모와 태아에 대한 건강정보를 신속하게 공유
앱 또는 웹사이트 활용	• 산모가 NHS 웨일스 앱 또는 웹사이트를 통해 직접 자신의 기록을 볼 수 있도록 설계[69]
상담 및 알림 기능	• 건강상담, 독감예방주사 등의 알림, 중요한 개별 의료 메시지 등을 받을 수 있는 기능 추가 예정

68) Digital Health(2023.1.17.), Welsh government to create unified digital system for maternity services

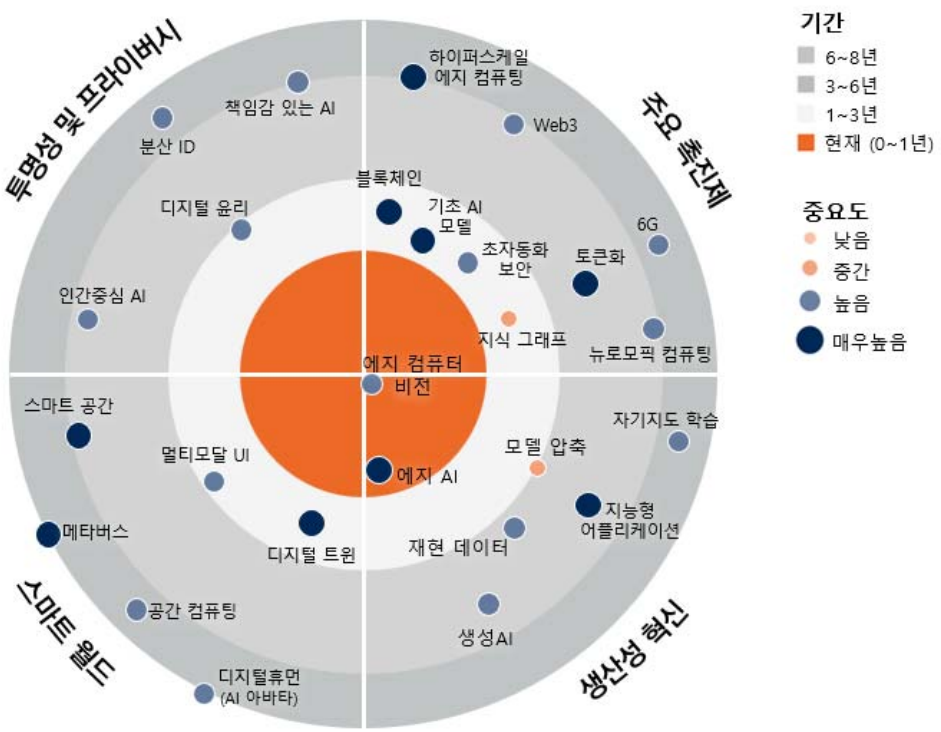
69) 현재 산모 1,000명을 대상으로 베타 테스트를 진행하고 있음

NEWS 7 가트너, 2023년 신기술 및 트렌드 소개[70]

❍ 글로벌컨설팅社 가트너(Gartner)는 새로운 기술의 성숙도, 성장 가능성, 그리고 영향력을 나타내는 'Impact Radar'를 통해 26개의 기술을 4가지 영역*으로 구분하여 소개

* ① 스마트 월드[71], ②생산성 혁신[72], ③ 투명성 및 개인정보 보호[73], ④ 주요 촉진제(enabler)[74]

〈 주요 신기술 및 트렌드의 영향력 〉



70) Gartner(2023.1.19), 4 Emerging Technologies You Need to Know About
71) 스마트 월드 영역은 물리적 경험과 디지털 경험이 융합·확장하는 기술을 포함
72) 생산성 혁신 영역은 다양한 작업의 생산성을 가속화할 수 있는 인공지능 기술을 포함
73) 투명성 및 프라이버시 영역은 기업과 개인 정보 수집이 기하급수적으로 증가하면서 등장한 주요 기술 및 주제를 포함
74) 주요 기술 촉진제는 새로운 비즈니스와 수익 창출 기회를 확보하는 데 기여하는 기술을 포함

❍ 가트너는 26개 신기술 중 3년~8년 사이에 일상에 활발하게 활용될 4가지 기술에 주목해야 한다고 강조

① 뉴로모픽 컴퓨팅[75]은 뇌의 작동방식을 훨씬 더 정교하게 모델링할 수 있는 주요 기술

- 뉴로모픽 컴퓨팅 기술을 AI 시스템 개발에 적용하면, 현실 세계의 불확실성에 더 잘 대응할 수 있는 제품 개발이 가능
- 인간의 뇌와 같이, 실시간으로 발생하는 이벤트와 정보에 빠르게 반응하는 자율성을 지닌 시스템을 만들어 다수의 AI 기반 제품의 기반을 형성할 것으로 전망
- 또한 현재 AI 기술로는 달성할 수 없는 전력 절감 효과와 성능을 실현할 것으로 전망

② 자기지도 학습[76]은 자동으로 데이터에 주석을 달거나 라벨링을 하는 접근법을 사용해 생산성을 높이며 상황·맥락의 선후 관계, 단어 간 연관성 등의 관계를 학습

- 컴퓨터 비전과 자연어처리(NLP)와 같이, 라벨링 된 데이터를 다루는 AI 활용 분야와 가장 두드러지게 관련
- 대규모 데이터를 다루기 어려운 기업이 기계학습을 활용할 가능성을 열어줄 수 있어 잠재적인 영향력과 이점이 큼

③ 메타버스[77]는 광대한 디지털 환경을 제공함으로써 물리적 세계와 디지털 세계의 융합·확장을 촉진하고, 분산화하며 상호운용성을 지닌 디지털 콘텐츠를 현실 세계와 연결

- 메타버스는 특히 독립적인 트렌드와 기술들이 서로 상호작용하며 다른 새로운 트렌드로 발전하는 '복합 트렌드'[78]의 예시
- 새롭게 부상 중인 기술과 트렌드(ETT)[79]는 공간 컴퓨팅 및 웹, 디지털 지속성[80], 멀티엔티티(multientity) 환경, 분산화 기술, 초고속 네트워크, 센서 기술, AI 응용 프로그램 등을 포함
- 메타버스의 이점과 기회를 바로 실현할 수 없지만, 잠재적인 활용 사례를 보여주며 메타버스로의 전환이 아날로그에서 디지털로의 전환만큼 중요할 것으로 전망

---

75) Neuromorphic computing
76) Self-supervised learning
77) Metaverse
78) combinational trend
79) Emerging, supporting technologies and trends
80) Digital persistence

④ 인간중심 AI(HCAI)[81]는 투명성과 프라이버시를 향상하고 사람과 사회에 이익을 줄 수 있도록 기술을 설계·개발하는 일반적인 AI 원칙

- 인공지능 기술을 설계·개발할 때, 사람들과 인공지능이 함께 협력하는 파트너십 모델을 가정

  ※ 학습, 의사결정 및 새로운 경험 등을 함께 수행

- 인간의 상식과 개입으로 인공지능 시스템의 단점을 보완하며, 기업이 위험을 관리하고 자동화를 통해 윤리적이고 책임감 있고 효율적으로 운영되도록 도움

- 기술 중심의 설계·개발 방식으로 인한 수많은 부정적인 영향으로 인해 다수의 기업이 AI 제품에 관한 전략을 재검토하고 있으며, 이미 많은 기업이 책임감 있는 인간중심 접근 방식으로 전환

81) Human-centered AI

NEWS 8 스웨덴, 공공부문 디지털 전환을 지원하는 4개년 계획 발표[82]

❍ 스웨덴 정부는 공공행정, 경제 및 사회 분야의 디지털 전환과 자본 투자 촉진을 위한 4개년 계획인 '디지털 전환 기반시설 계획[83]'에 착수

※ 약 10억 유로 상당의 규모

- 교육, 교통, 의료, 국가안보를 포함한 정부 및 공공서비스 디지털 전환 가속화를 목표
- 스웨덴 디지털 정부청[84]과의 협업을 통해 실시되며, 디지털 정부청에게 디지털 기반시설 프로젝트를 감독할 권한을 부여
- 스웨덴 정부의 정책은 민간 이해관계자로부터도 지지를 얻고 있음

※ 스웨덴 IT 기업 연합회[85]에 따르면 디지털化가 필연적인 현실에서 정부의 로드맵은 환영하며, 디지털 전환이 지속가능한 경제의 구성요소가 될 수 있도록 관련 기술을 개발할 것을 강조

❍ 스웨덴 IT 기업 연합회[86]는 스웨덴이 2024년까지 디지털화 계획을 확립하고 이행하기 위해 7만~10만 명의 직원을 추가로 고용해야 할 것으로 추산

- 현재 디지털 역량과 인재가 부족한 상황이며, 스웨덴 기업의 성장에 큰 걸림돌로 작용
- 정보통신 산업부문[87]은 스웨덴의 경제개발, 고용, 기후 적응 및 번영을 위해 점점 더 큰 역할을 할 것으로 기대
- 성장 잠재력의 실현 극대화를 위해서는 디지털 인재의 확보가 관건임을 지적

---

82) ComputerWeekly(2023.1.19.) Swedish government launches accelerated digitisation plan

83) Digital Transformation Infrastructure Plan (DTIP): 작년 9월 스웨덴 총선을 앞두고 중도 정당이 제안한 기술 주도 자본 투자 제안에 기초하며 총선 이후 연정 협상 과정을 거치면서 전 정부의 지지를 받음

84) The Agency for Digital Government (ADG/Myndigheten för Digital Förvaltning): 스웨덴의 공공행정의 디지털화를 조정·지원하는 국가기관이며, 지방행정과 공공서비스의 디지털 전환을 우선순위로 상정하고 공통의 전국적인 디지털 기반시설 도입에 초점
참고자료: https://www.digg.se/en/management-and-coordination

85) TechSverige, 1,400여 개의 스웨덴 IT 기업들이 회원사임

86) 각주 85번 참고

87) 과거의 IT, 통신 산업에 더하여 컴퓨터 게임, 헬스케어, 핀테크 및 에드테크 회사들이 포함됨

❍ 스웨덴 디지털 정부청[88]은 '디지털 전환 기반시설 계획'으로 마련한 자금을 활용해 더 안전하고 효율적인 정보 전송을 위한 디지털 기반시설을 구축하기 위해 노력

- 우선, 기본 데이터[89] 공유·교환을 위한 국가 프레임워크를 개발 중
- 디지털 정부청 조사에 따르면, 국가 디지털 기반시설 개발을 통한 비용 절감 효과가 10년간 총 100억 스웨덴 크로나(8억 9,000만 유로)에 달할 것으로 예측

❍ '디지털 전환 기반시설 계획'이 다루는 핵심 디지털 전환 이니셔티브의 상당수는 12개 스웨덴 주 정부[90]와 협업하며 디지털 정부청이 운영하는 'ENA' 프로젝트[91]에 포함

- ENA의 주된 역할은 국가의 공공행정 시스템을 위한 새로운 공동 디지털 솔루션 개발
- ENA를 활용해 민관 구분 없이 누구나 디지털 기반시설에 접근할 수 있음

❍ 또한, '디지털 전환 기반시설 계획' 지원금을 활용해 디지털 정부청의 고부가가치 연구 활동을 가속화하여 지방 정부가 디지털 기반시설로부터 얻을 수 있는 최적의 조건을 분석할 계획

- 주요 목표 중 하나는 2026년까지 스웨덴의 공공복지 시스템·서비스의 디지털화

❍ 스웨덴 디지털 정부청은 민간기업과 및 사회 전반이 "디지털 사회"에 참여하는 수준을 측정·분석할 수 있는 '디지털 대시보드 연구 툴'을 출시(2022.12.)

- 현재 무료 베타버전을 통해 디지털 사회에 대한 참여 수준을 계산하고 분석이 가능
- '디지털 대시보드 연구 툴'을 활용해 대량의 데이터에 접근해 유용하기 활용할 수 있고, 메타데이터를 활용해 연구 및 기업 간 파트너십 형성에도 활용할 수 있음

  ※ 특히 공공부문, 교육기관 및 언론에게 도움이 될 것으로 예상

---

88) 각주 84번 참고

89) Basic data라고 표기하였으며, 조직·기관 간에 교환된 데이터의 진위 확인을 위한 이름, 성별 등의 정보로 추정
참고자료: https://www.digg.se/en/management-and-coordination,
https://www.lawinsider.com/dictionary/basic-data

90) 고용, 기업, 법원, 세무, 교통, 통계, e-보건은 물론 보험 토지 측량 및 국립기록원 등이 해당

91) https://www.digg.se/ledning-och-samordning/ena---sveriges-digitala-infrastruktur

NEWS 9 포브스, 공공부문 기술 활용방안 제안[92]

❍ 미국 경제잡지 포브스(Forbes)는 정부의 클라우드, 블록체인 및 분산원장(DLT)[93] 등의 기술 활용으로 안전한 데이터 관리·공유 및 업무 효율성 향상이 가능하다고 강조

〈 정부 생산성·기능 향상을 위한 기술 활용방안 요약 〉

활용방안		주요 내용
1	클라우드 기술을 통한 정보 수집·보안	• 클라우드 기술을 활용해 정부와 각 기관 간 안전하게 데이터 공유
2	레거시 시스템[94]을 클라우드와 연결	• 효율성 증진을 위해 현대화된 시스템으로 전환 • 버티컬 클라우드[95] 방식을 통해 진행
3	블록체인 및 DLT으로 효율성 증대	• 어렵고 비용이 많이 드는 공공데이터 유지·관리 작업을 단순화
4	민감한 정보의 보안 향상	• 인공지능 기술 활용, 2차 인증, 사이버보안 교육 등의 다양한 조치를 취해 정보 보안 수준 향상
5	공공행정 업무 처리방식 변화	• 자동화 기술을 점진적으로 활용해 공공부문 업무 처리방식의 효율성 증대

92) Forbes(2023.1.24.), Exploring The Future Of Government Technology And Its Global Impact

93) 분산원장기술(distributed ledger technology, DLT); 분산 네트워크 참여자가 암호화 기술을 사용하여 거래 정보를 검증하고 합의한 원장(ledger)을 공동으로 분산·관리하는 기술 (출처: TTA 정보통신용어사전)

94) 레거시(기존) 시스템은 구형 컴퓨터나 서버와 같은 하드웨어부터, 현재 운영 중인 컴퓨터 운영 체제, 프로그래밍 소스 코드, 데이터베이스 등 소프트웨어 자산까지 모두 포함하는 개념이며, 일부에서는 기존 시스템을 노후화된 하드웨어, 복잡하고 비대해진 애플리케이션, 특정 공급 업체에 의존도가 높은 시스템 등과 같이, 보수 또는 교체가 불가피한 시스템이라는 의미로도 사용 (출처: TTA 정보통신용어사전)

95) Vertical cloud이며, 특정 산업이나 수익모델을 위한 클라우드컴퓨팅 서비스를 통합한 것
참고자료: https://www.techtarget.com/searchcloudcomputing/definition/vertical-cloud
Forbes(2021.3.30.), The Future Of Cloud Is Vertical
Digital Today(2022.6.13), 빅클라우드 틈바구니 속 버티컬 클라우드 약진...다양한 분야서 거점 확대

❍ **(클라우드 기술)** 정부는 클라우드 기술을 통해 정부와 각 기관 간 안전하게 데이터 공유와 관리가 가능

- 정부가 보유·관리하는 정보가 완전히 연결되고 상호운용성을 지닐 경우, 공공부문 업무 부담이 약 60% 감소할 것으로 추정[96]

❍ **(레거시 시스템 통합[97])** 클라우드 기반 애플리케이션을 레거시 시스템[98]과 연결하여 더 빠르고 쉽게 데이터를 접근·활용하고 모든 시스템 간의 연계·동기화가 가능하도록 지원

- API, 데이터베이스 커넥터 등을 통해 레거시 시스템 통합을 수행할 수 있음
- 특히 정부의 요구사항을 구분한 다음, 해결책을 제공하는 버티컬 클라우드 방식[99]으로 진행

❍ **(블록체인 및 분산원장[100])** 현재 공공데이터 유지·관리가 어렵고 비용이 많이 들지만, 블록체인 및 분산원장 기술을 활용해 무단 활동 및 정보 유출 등 방지가 가능

- 블록체인 기술의 장점은 투명성이며, 정부는 계약, 금융 거래 및 신원정보 관리 등에 적용할 수 있음
- 정부는 블록체인 기술을 활용해 금융 거래의 투명성 향상, 사기 등 부정행위 방지·감소, 의료 및 신원정보의 보안 향상, 거래 수수료 감소 등을 실현할 수 있음
- 또한 공급망을 가시적으로 드러내고 관련 정보를 실시간으로 제공이 가능
- 다만 블록체인 및 분산원장 기술을 본격적으로 활용하기 전, 기술적 통찰력과 문화적 변화가 필요하며 소규모 프로토타입을 시범적으로 도입하고 기관의 요구사항을 충족하는지 확인이 필요

---

96) 참고자료: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/government-data-management-for-the-digital-age
https://www.normenkontrollrat.bund.de/resource/blob/300864/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf

97) Legacy system integration

98) 각주 94번 참고

99) 각주 95번 참고

100) 각주 93번 참고

❍ **(인공지능 및 정보보안 전략)** 인공지능과 같은 신기술을 활용해 민감한 데이터를 보호하기 위한 정보보안 증진이 필요

- 인공지능 기술은 보안 위협 정보를 학습해 민감한 데이터를 표적으로 삼는 해킹 공격을 대처하는 데 효과적인 방법 중 하나
- 데이터에서 패턴을 추정하고 실시간으로 이상징후를 탐지하는 등 유용하게 활용 가능
- 인공지능 기술 외에도 사이버보안을 강화하기 위해 다양한 조치*가 필요

  * ▲강력한 규칙과 보안 정책을 개발, ▲상시 감사 및 보안 테스트 진행, ▲민감한 데이터에 대해 2차 인증 및 암호화 기술 도입, ▲사이버보안 이슈 대응에 대한 교육 제공, ▲재택근무자의 네트워크 보안 모니터링 등을 포함

❍ **(업무방식 변화)** 기술을 통해 저가치(low-value) 활동을 제거 또는 자동화함으로써 정부 운영 및 업무방식 개선이 가능

- 공무원과 공공부문 종사자가 수행하는 업무 중 일부에 서서히 기술을 도입해 필요한 인력 및 업무량을 감소하고, 투자이익률 및 생산성 향상, 작업 품질 유지, 탄소발자국 감소 등의 효과를 실현할 수 있음
- 효율적인 디지털 거버넌스를 실현하기 위해 재정 자원 절약, 인력 최적화, 국민에게 원활한 경험 제공 등을 기준으로 다양한 기능을 평가하는 것이 중요