

디지털 대전환(DX·AX)과 ‘디지털 위험 관리’의 중요성

디지털 대전환(DX·AX)과 ‘디지털 위험 관리’의 중요성

목 차

I. DX·AX 시대의 디지털 위험 관리 _ 3

II. 디지털 위험 요인과 패러다임의 변화 _ 9

III. 새로운 디지털 위험 관리 방안 _ 15



GDX(Grand Digital Transformation) 보고서는
국가사회 디지털 대전환(GDX)에 따른 주요 이슈와 사회적 현안을
파악해 선제적으로 정책 대안을 제시하는 보고서입니다.

NIA의 승인 없이 본 보고서의 무단전재나 복제를 금하며, 인용하실 때는 반드시
NIA, 「GDX 보고서」라고 밝혀주시기 바랍니다.

▶ 보고서 작성

- 한국지능정보사회진흥원(NIA) 인공지능(AI)정책본부 미래전략팀
이정아 (leeja@nia.or.kr)

▶ 보고서 온라인 서비스

- www.nia.or.kr

세계 최고의 인공지능(AI) 활용기관 NIA

1. 본 보고서는 방송통신발전기금으로 수행한 정보통신방송 연구지원 사업의 결과물이므로, 보고서 내용을 발표할 때 반드시 '과학기술정보통신부 정보통신방송 연구지원 사업'의 연구 결과임을 밝혀야 합니다.
2. 본 보고서를 가공인용할 때는 출처에 「한국지능정보사회진흥원(NIA)」이라고 밝혀주시기 바랍니다.
3. 본 보고서의 내용은 한국지능정보사회진흥원(NIA)의 공식적인 견해가 아닙니다.

I. DX·AX 시대의 디지털 위험 관리

1. 디지털·AI 전환(DX·AX)¹⁾ 가속화와 디지털 위험²⁾ 증가

■ ‘DX’는 기업 디지털 전략 측면에서 거론됐지만, 본래 디지털 사회혁신의 개념

- ▶ 디지털 전환(DX)의 본래 정의는 기업 비즈니스나 산업분야 혁신에 한정되는 것이 아닌, ‘디지털 기술이 인간 삶의 모든 측면에 일으키는 변화’를 총체적으로 일컫는 의미
 - DX는 주로 기업의 가치 창출과 혁신, 신사업 발굴, 레거시 비즈니스를 디지털 비즈니스로 전면 변환시키는 디지털화가 확대되면서 기업 디지털 전략과 변화의 의미로 사용했으나,
 - 근본적으로는 디지털 기술을 폭넓게 활용해 삶의 질을 향상시키고, 진화하는 디지털 기술로 삶을 풍요롭게 하는 것, 기존 가치관·틀을 근본적으로 파괴해 혁신을 가져오는 것을 의미
 - DX라는 용어를 처음 정의한 논문³⁾에서는 ‘디지털 기술이 인간 삶의 모든 측면에 영향을 미쳐서 나타나는 변화’라고 광의로 정의⁴⁾
- ▶ 우리나라는 기술적 의미가 강한 ‘IT·ICT·디지털화’, 디지털 기술이 가져오는 경제산업의 변화를 의미한 ‘4차 산업혁명’ 이후, 국가사회 전반의 디지털화라는 의미에서 DX를 정책적 용어로 활용
 - 국가사회 모든 분야에 디지털 기술을 적용해 편리성·생산성·효율성을 향상시키고, 혁신과 변혁을 일으켜 국가경쟁력과 국민 삶의 질을 제고시킨다는 정책적 의지를 반영한 의미

[NIA가 정의한 디지털 전환(DX)]

DX란, 디지털 기술(IT·ICT 포함)의 발전으로 국가사회 전반의 시스템(국민생활 포함)과 인프라의 디지털화가 급진전 되고 온오프라인 융합이 사회적 변화를 수반해 디지털이 국민 삶에 미치는 영향이 커지는 상태. 더 나아가 이런 현상이 진전되어 AX까지 포함한 디지털 기반이 SoC가 된 상태를 ‘디지털 대전환(GDX)’으로 칭함

1) ‘Digital Transformation’의 이니셜은 ‘DT’지만 영어권에서는 접두사 ‘Trans’를 ‘X’로 쓰는 관습이 있고, ‘Trans’에는 ‘~를 가로지른다’는 의미가 있어 동어 ‘Cross’를 생략할 때 사용하는 ‘X’를 약칭으로 사용해 ‘DX’로 표기, AX는 ‘AI Transformation’.

2) 본 보고서에서 의미하는 디지털 위험은 ‘DX·AX로 인해 기술비즈니스·자연사회적으로 발생 가능한 포괄적·광범위한 위험’까지 포함

3) 스웨덴 우메오대학(Umeå Universit), Erik Stolterman & Anna Croon Fors, 「Information Technology(IT) And The Good Life」에서 처음 정의 (Stolterman은 '04년 당시 우메오대학 교수였고, 현재는 美 인디애나대학 부학부장)

4) “The digital transformation can be understood as the changes that the digital technology causes or influences in all aspects of human life.”

■ ‘AX’는 생성AI 출현 이후 급속히 발전하는 AI 기술이 가져올 획기적 변혁을 의미

- ▶ DX 측면에서 AI는 DX 추진의 필수적이고 효과적인 수단이지만 AI를 활용한다고 해서 반드시 DX를 추진할 수 있는 것은 아니며, 하나의 기술로 작용(‘AI=DX가 아닌 AI=DX 도구이며 무기’)
 - AI는 데이터 분석, 자동화, 고객 경험의 개인화 등의 측면에서 DX 목표 달성을 효과적으로 지원할 수 있으며 프로세스 효율화, 의사결정의 신속화, 새로운 가치 창출의 원천으로 작용
 - 기존 IT 시스템 등과 마찬가지로 AI를 활용하면 반드시 효과가 있는 것이 아니라, 유효한 분야와 효과성을 충분히 파악한 후 AI 기술을 적용해야 DX로 연계되고 혁신이 가능
 - 따라서 AI는 DX를 더욱 빠르고 효과적, 효율적으로 촉진시키는 핵심 기술의 하나로, AI 기술로 인해 나타나는 현상인 AX도 DX 과정의 일부로 보는 것이 일반적
- ▶ 그러나 한편으로 생성AI가 미치는 영향력·파급력이 높아지고, 글로벌 각국과 기업이 AI를 강력한 변혁의 도구로 활용하면서 생성AI에 의한 AX를 DX 이후 새로운 패러다임으로 인식
 - 인터넷, 모바일, DX 등 과거의 파괴 사이클과는 비교가 되지 않게 변화의 속도가 현저하게 빠르고, 전례가 없을 정도의 생산성 향상과 경쟁 우위성을 가진 생성AI가 주도하는 AX가 DX보다 더 비약적인 발전을 가져올 것으로 전망

■ 국가기업의 전략적 변혁 의지와 관계없이 디지털 기술 진보로 DX·AX는 진행 중

- ▶ DX·AX가 미치는 것은 단순한 변화가 아닌, 디지털 기술에 의한 파괴적 혁신을 의미하는 ‘디지털 파괴(Disruption)’, 즉 기존의 가치관과 틀을 근본적으로 바꾸는 혁신
- ▶ 디지털 기술의 발전으로 인공지능(AI)·클라우드·IoT 등의 신기술을 이용한 솔루션과 서비스가 일상화되면서 국가사회 DX·AX는 더욱 가속화되고, 디지털 대전환(GDX)으로 급속히 확대
- ▶ 특히, AI기술의 발전에 따른 생성AI의 출현은 민간이나 공공부문의 DX·AX 추진에 큰 영향을 미칠 것으로 예상되며 이에 따른 예측 불가능한 위험성 대비, 안전성 확보 등이 주요 현안으로 부상

【참 고 1】 DX(Digital Transformation)의 새로운 정의 (2022)

■ 사회의 디지털 전환(DX)

DX는 인간 삶의 모든 측면에 영향을 미치며, 단순한 기술적 발전이 아니라 사회를 구성하는 우리가 현실(Real)과 디지털 공간이 융합되어 고도로 복잡하고 변화하는 세계에 어떻게 관여하고 접하는지에 영향을 주는 넓고 깊은 변화. DX는 더 스마트한 사회와, 개개인이 건강하고 문화적인 더 좋은 생활(Good Life)을 보낼 수 있는 지속가능한 미래를 실현

(DX influences all aspects of human life. DX is not solely a technical development, it is a broad and deep change merging the real and digital space in a way that influences how we as a society approach and deal with a highly complex and changing world. DX has the potential to improve and lead to standards of wholesome and cultured living and a sustainable future with a smarter society and a good life for each individual.)

■ 공공(행정)의 디지털 전환(DX) (중앙정부와 지자체)

DX는 모든 조직·분야에서 스마트 행정서비스 개발과 혁신적 가치 창출을 지원. 또한, 안전·안심·쾌적·지속가능한 사회 실현 방안을 제공해 국민(주민)이 더 행복하며 풍요롭고 열정적인 삶을 누릴 수 있도록 해서 지역의 가치 향상을 가능하게 함. DX는 기존 체계와 절차에 도전하고 협력적 방식으로 국민 중심의 혁신적 해결책을 강구하도록 촉구. DX를 위해서는 조직 본연의 방식과 문화를 혁신적이고 민첩하며 협력적으로 변혁하고, 최고관리자 주도하에 모든 이해관계자가 참여하는 것이 필요

(DX makes it possible to develop smart government services in every organization and category and to assist innovative value creation. DX also makes it possible to improve the value of areas and regions by enabling happier, richer, and more passionate conditions for resident by creating solutions that can make residents more safe and secure and lead to a comfortable and sustainable society. DX encourages everyone to challenge existing structures and procedures and in a collaborative way think about innovative solutions that are more resident-oriented. DX requires transforming the attitude and culture of the public sector to become innovative, agile, and collaborative. DX requires all stakeholders to participate in the transformation while being initiated and led by top management.)

■ 민간(기업)의 디지털 전환(DX)

DX는 기업이 비즈니스 목표·비전 달성을 위해 그 가치·제품·서비스 제공 체계를 변혁시키는 것. DX는 고객에게 더 높은 가치를 제공해 기업 전체의 가치 향상도 가능. DX를 위해서는 전략과 조직행동·구조·문화와 교육·거버넌스·절차 등 조직의 모든 요소를 변혁하고, 디지털 기술 활용에 기반한 최적의 생태계 구축, 최고경영자 주도하에 전 직원이 혁신에 참여하는 것이 중요

(DX can empower industries to transform the delivery of their value, products, and services, to accomplish their business goals and visions. DX also makes it possible to improve the overall value of a company in the industry by changing the delivery method to offer a higher value to their customers. DX requires organizations in the industry to redesign all elements of the organization, including strategy, organizational behavior, organizational structure, organizational culture, education, governance, and procedures to create an optimized ecosystem based on the use of digital technology. DX requires all employees to participate in the transformation while being initiated and led by top management.)

출처 : Erik Stolterman & The Digital Transformation Lab in Japan (<https://www.dxlabs.jp/>)

2. AX를 촉진하는 생성AI 출현과 AI 안전성 대두

■ 인공지능(AI)은 DX·AX의 핵심 기술이지만, '생성AI'는 예측 불가능한 위험도 수반

- ▶ AI 투자와 활용이 가속화되면서 역사상 다른 어떤 기술 발전보다 더 빠르게 미래 노동 시장과 경제를 변화시킬 것으로 예상
- ▶ 챗GPT 등을 포함한 생성AI 출현으로 AX가 급속히 진전되고 업무 효율화나 생산성 향상에도 영향을 미치고 있지만, 데이터 보안의 문제 등 생성AI 활용에 따른 다양한 위험성도 부상
 - 운영 리스크와 함께 사이버 범죄, 기밀정보 유출, 대중 선동, 저작권 침해 등의 심각한 사고가 발생하면 영향이 커질 가능성이 높아 일부에서는 생성AI 사용을 제한하기 시작
 - 생성AI 등장과 급속한 보급·이용 확대로 지금까지의 기술 측면의 분류·추측·인식형 AI와는 다른 측면에서 윤리적·법적·사회적 과제(ELSI)*도 논의

* ELSI(Ethical·Legal·Social Issues) : 책임성, 안전성과 보안, 프라이버시, 투명성과 설명가능성, 공정성과 비차별성, 전문가의 책임성과 윤리, 인간적인 가치의 촉진, 글로벌 협력과 거버넌스 강화 등

- ▶ AI가 인간에게 미칠 영향을 우려하는 각계각층 의견이나 제언이 계속되면서 악용이나 오남용 예방, 책임 있는 활용을 위한 대책 마련과 함께 AI 안전*도 중요한 이슈로 부각

* AI로 인한 피해의 이해·예방과 완화. 피해는 고의적·우발적일 수 있으며 개인·그룹·조직·국가, 또는 전 세계적으로 발생하면 신체적·정신적·사회적·경제적 피해와 함께 이에 국한되지 않는 다양한 유형의 피해 발생⁵⁾

■ 생성AI는 막대한 기회뿐만 아니라 현재·미래에 심각한 피해를 제공(NIST)⁶⁾

- ▶ AI 발전은 우리 사회와 삶을 변화시킬 수 있는 잠재력을 가지고 있지만, 이는 AI를 책임감 있게 개발·배포하지 않았을 때 나타나는 AI 위험 완화를 위해 열심히 노력하는 경우에만 가능
- ▶ 인류와 지구에 도움이 되는 AI 잠재력을 미래에 최대한 실현하기 위해서는 위험을 완화하면서 AI 기술의 혁신을 촉진하는 것이 중요
 - 안전한 AI 혁신을 달성·유지하는 데 있어 주요 과제 중 하나는 AI 안전의 과학적 연구로, 국가 안보·공공 안전·개인 권리를 포함한 다양한 위험에 걸쳐 AI 안전 과학을 발전시키는 것
- ▶ AI 모델과 시스템의 기능·위험을 정확하게 평가하고 완화 및 보호 장치의 효과를 평가하려면 신뢰할 수 있고 재현이 가능한 AI 안전 과학이 시급하게 필요

“AI가 전혀 다른 세상을 만들고 있다. 그리고 모든 새로운 기술을 적용할 때와 마찬가지로 우리는 그 기능·한계·영향을 측정하는 방법을 알아야 한다. 이것이 NIST가 업계·학계·시민사회·정부 대표자들의 협력을 모아 국가적으로 중요한 과제를 해결하기 위해 함께 모이는 이유이다.”

(AI 안전 전담 최초 컨소시엄 발표 언론 브리핑 中(NIST 디렉터 Laurie E. Locascio('24.2.8))

5) <https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute>

6) <https://www.commerce.gov/news/press-releases/2024/05/us-secretary-commerce-gina-raimondo-releases-strategic-vision-ai-safety>

■ 영·미·일 등 주요국은 ‘AI안전연구소’를 설립, 글로벌 협력을 통해 AI 위험에 대응

- ▶ 영국은 AI 안전과 책임감 있는 개발·제공의 국제적 논의 주도를 위해 공익을 위한 첨단 AI 안전에 중점을 둔 최초 국가 지원 기관으로 과학혁신기술부 산하에 AI안전연구소(AISI) 설립('23.11)⁷⁾
- ▶ 미국은 바이든 대통령 행정명령에 따라 국립표준기술연구소(NIST)⁸⁾ 산하에 미국 AI안전연구소(U.S.AISI: Artificial Intelligence Safety Institute) 설립('24.2)
 - AI 안전·보안 강화를 위한 AI 기술과 시스템 설계·개발·사용, 거버넌스 신뢰 향상이 목표이며, 평가 및 데이터를 포함한 측정 과학, 기술, 표준과 관련 도구를 개선하는 데 중점
 - ※ 이 기관의 AI 목표와 활동은 법적 명령, 대통령 행정 명령과 정책, 그리고 미국 업계, 글로벌 연구 커뮤니티, 기타 연방 기관과 시민 사회 요구 사항에 따라 수행
 - 안전·신뢰할 수 있는 AI 개발과 제공을 위해 AI 개발자·사용자·학계·정부(주·지방)·산업계 연구원·시민사회 단체로 구성된 미국 AI안전연구소 컨소시엄(AISIC) 창설⁹⁾(‘24.2)
 - ※ 컨소시엄은 AI안전연구소(USAISI) 산하에 속하며 레드팀 구성, 역량 평가, 위험관리, 안전과 보안, 합성 콘텐츠 워터마킹을 위한 지침 개발을 포함해 바이든 대통령의 행정 명령에 설명된 우선 조치에 기여
- ▶ 일본은 안전·안심·신뢰할 수 있는 AI 실현을 위해 AI 안전성 평가 방법과 기준 검토·추진을 위한 AI안전연구소(Japan AISI) 설립('24.2)
 - ※ AI 전략회의에서 AI안전연구소 설립 표명, IPA(Information-technology Promotion Agency)에 사무국 설치

■ 생성AI 기술 특성에 맞춰 기업·국가는 글로벌 차원의 디지털 위험 대응 필요

- ▶ AI기술로 비즈니스나 업무 프로세스 혁신을 도모하는 기업이 증가하고 있지만, 본격적으로 AX를 추진하려는 기업·조직은 생성AI 위험 요인을 충분히 식별해 대책을 마련하는 것이 중요
- ▶ 생성AI는 예측할 수 없는 디지털 위험을 현실화시키고, 글로벌 문제로 확장시킬 수 있으므로 기술적 대책과 함께 글로벌 규범과 위험성 대책을 위한 가이드라인 마련 필요

〈 그림 1 〉 AI 기술의 특징에서 기인하는 위험(Risk)



출처 : 딜로이트, 'AI 거버넌스 - 생성AI 시대에 요구되는 신뢰할 수 있는 AI 실현의 길'

7) <https://www.aisi.gov.uk/>

8) National Institute of Standards and Technology(NIST)

9) <https://www.nist.gov/news-events/news/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated-ai>

3. 디지털 위험 증가와 대응의 중요성

■ 디지털 기술의 발전과 함께 팬데믹에 의한 급속한 DX로 새로운 디지털 위험 발생

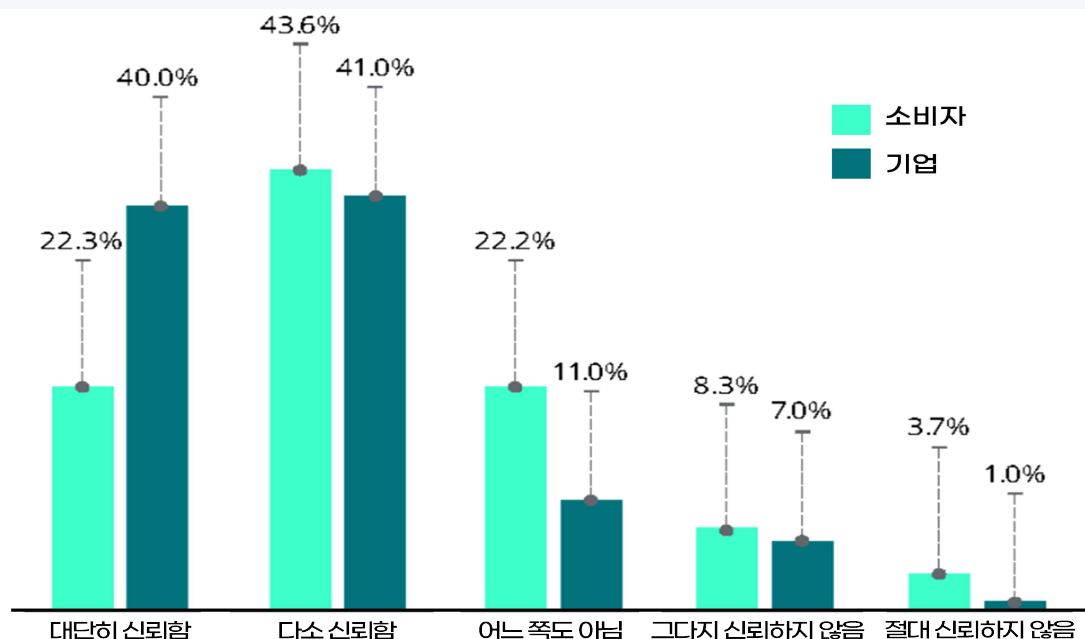
- ▶ AI·클라우드·IoT 등 디지털 신기술을 이용한 솔루션과 서비스 보급은 보편화되고 있으며, 공공서비스뿐만 아니라 민간 비즈니스나 서비스 분야의 DX도 촉진
- ▶ 특히, 코로나19로 인한 글로벌 팬데믹을 겪으면서 사회적 거리두기, 도시 락다운 등에 따라 사회적 서비스, 기업의 일하는 방식을 온라인으로 혁신하기 위해 DX는 불가역적으로 가속화
- ▶ 팬데믹과 함께 진행된 공공·기업의 디지털 신기술 도입과 국가사회 급속한 DX는 국민 생활과 사회 환경을 크게 변화시키는 전환기를 마련했고, 디지털 위험의 발생 가능성 또한 증가

※ 인류사에서 다양한 사회 환경의 패러다임슈프트가 일어나는데, 예를 들어 19세기 팬데믹을 일으킨 콜레라가 100만 명 이상의 사상자를 내면서, 식수 소독과 상하수도 인프라 정비가 이루어져 현대적인 공중위생을 확립하는 계기 마련

■ DX·AX 시대 국민(소비자) 신뢰 확보는 안전·안심할 수 있는 디지털 서비스에서 시작

- ▶ 고도화되고 있는 사이버 공격의 피해를 당하는 기업은 해마다 증가하고 있으며, 대기업뿐만 아니라 공공기관을 포함한 중소 규모 조직도 사이버 공격의 표적이 되어 DX·AX 추진을 위협
- ▶ DX·AX로 기업 활동이나 공공서비스 시스템은 기업간·조직간 전반에 네트워크화되어 디지털 위험으로 인한 문제 발생 시, 국소적 피해로 그치지 않고 연계된 모든 시스템에 연쇄적 파급
- ▶ 디지털 기술 활용도가 높을수록 디지털 위험에 대비하지 않으면, 문제 발생 시 업무 중단·정지로 국민 불편과 경제적 피해 발생, 기관기업 이미지 훼손, 서비스 신뢰 상실 등 큰 손실 초래
- DX·AX 시대에 국민 신뢰를 얻기 위해서는 국가기업의 안전·안심한 디지털 서비스 제공과 함께 상시적 디지털 위험에 신속히 대응해 회복탄력성(Resilience)을 높이는 체계 마련이 중요

〈 그림 2 〉 디지털 기술의 안전·정보·안·지속가능성에 대한 신뢰성 차이 (소비자 vs. 비즈니스 리더)



출처 : 딜로이트, 'Global Digital Risk Survey 2022'(file:///C:/Users/user/Downloads/jp-or-global-digital-risk-survey-2022.pdf)

【참고 2】 주요국(영·미·일) ‘AI안전연구소’ 주요 현황과 역할

□ 영국 AI안전연구소(AISI : AI Safety Institute)

- AISI는 첨단 AI시스템의 기능과 위험을 이해하고, AI 규제 프레임워크를 알려줌으로써 AI를 안전하고 책임감 있게 개발·제공하도록 보장하기 위해 설립
- AI 안전 관련 국제적 협력 주도를 위해 ‘Frontier AI Taskforce’ 출범시켰고 세계 최초로 ‘AI Safety Summit’을 주최했으며, 이를 발전시켜 AISI 설립

[주요 기능과 역할]

- ▶ **AI 시스템 평가 개발수행** (평가 우선순위 : 이중용도 기능, 사회적 영향, 시스템 안전보안, 통제력 상실)
 - AI 오용 관련 기능, 조작설득, 편향된 결과추론 등 사회적 피해를 악화시킬 수 있는 기능
 - 시스템 보호 조치 효율성과 한계, 사이버 보안 조치의 적절성 이해 등 시스템 안전·보안
 - 자율적 복제 등 통제력 상실로 이어질 수 있는 능력·경향
- ▶ **(학계나 업계 등이 추진할 수 없거나 추진하지 않는) 기초 AI 안전 연구 추진**
 - 편향, 또는 속성과 관련된 훈련 데이터를 분석하는 기술 등 AI 거버넌스를 위한 도구 개발
 - 측정하기 어려운 효과를 측정하기 위한 다학제적 사회기술적 평가를 개발하기 위해 노력
 - AI 시스템에서 생성된 데이터에 대한 인간 큐레이션, 합성 데이터 및 교육의 효과 연구 등
- ▶ **정보 교환 촉진** : 정책 입안자·규제기관·민간기업·글로벌 파트너·대중과 연구 결과 공유
- ▶ **파트너십** : 글로벌 파트너, 민간기업, 학계·시민사회, 국방·국가 안보 커뮤니티 전문 지식 등

□ 미국 AI안전연구소(U.S. AISI)

- 세 가지 주요 목표 : ❶ AI 안전 과학을 발전, ❷ AI 안전 관행을 명확히 설명·시연·전파, ❸ AI 안전 관련 기관·커뮤니티·조정 지원 (AI 서울 서밋에 맞춰 미국 AISI의 전략적 비전 발표(‘24.5.21))
- AI 안전을 위한 측정 과학과 연구 추진, 모델·시스템의 안전성 평가 수행, 콘텐츠 인증 및 합성 콘텐츠 감지를 포함한 평가와 AI 위험 완화를 위한 지침 개발 등
- 다양한 커뮤니티와 긴밀히 협력해 기술의 현재와 새로운 기능·한계·실세계(real-world)에 미치는 영향에 대한 이해를 얻고 AI 안전 관련 규범·네트워크·기관 육성
- AI 안전 과학에 관한 국제 협력을 위한 서울 의향서를 토대로 AI안전연구소 국제 네트워크를 출범, 각국의 AISI와 협력을 강화확장

□ 일본 AI안전연구소(Japan AISI)

- 영국·미국 등의 관련 기관과 협력해 AI 개발·제공·이용의 안전성 향상에 기여하는 기준·가이드라인 등 검토, AI 안전성 평가 방법 등 조사, AI 안전성 기술·사례 조사 등 추진
- ❶ 안전성 평가 조사기준 등 검토 : 안전 관련 표준, 체크 톨, 가짜 정보 대책 기술, AI와 사이버 보안 조사, 안전성에 관한 기준, 지침 등의 검토와 AI 테스트 환경 검토
- ❷ 안전성 평가 방법 검토 : 산학과의 의견 교환, AI 안전성 평가 운용 검토 등
- ❸ 관계기관(영·미 AISI 등)과의 협력, 관련 기초 조사 추진

출처 : 각국 AI안전연구소(AISI) 누리집, 관련 기사 등

Ⅱ. 디지털 위험 요인과 패러다임의 변화

1. 디지털 위험 요인(Risk Factors)의 다양화·복잡화

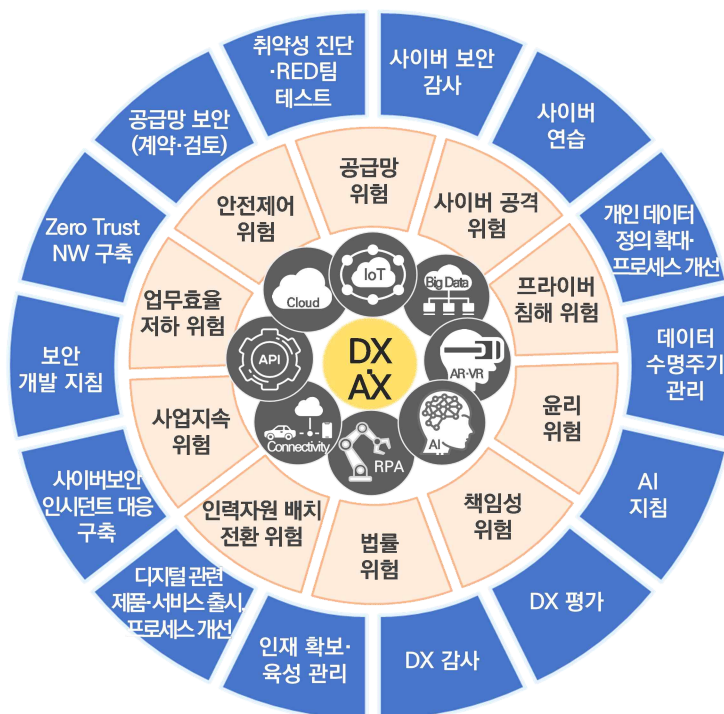
■ 국가사회 운영 시스템과 국민생활·경제활동, 기업 비즈니스의 디지털 의존도 상승

- ▶ 전력·가스·교통 등 대규모 사회기반시설 운영과 관리, 금융·유통·물류·무역 거래, 각종 서비스 등 비즈니스 전반의 디지털 전환 가속화로 디지털 기반이 사회간접자본(SOC) 수준으로 확대
- ▶ 사회·경제활동의 범위가 오프라인에서 온라인으로 확장되어 온오프라인의 경계가 사라지고, 온라인 공간이 일상생활의 보편적 영역으로 자리매김
- ▶ AI 등 지능화 기술의 발전과 고도화, 국가사회·경제산업의 전방위적인 디지털 대전환과 혁신으로 기술 의존성과 결합도, 영향력 심화

■ 공공기업의 DX·AX 추진으로 사회비즈니스 생태계 전반에 디지털 위험 요인 다변화

- ▶ 사람·프로세스·데이터·사물 등 모든 것이 네트워크화되면서 디지털 위험 요인은 다양화·복잡화
- ▶ 새롭게 발생하는 위험관리를 위해서는 신규 도입 기술에 따라 고려해야 할 위험 관점이나 부정 예방을 위한 접근도 다르므로 기술 특성에 따른 위험을 진단·판별하는 것이 필요

〈 그림 3 〉 공공기업에서 대응해야 할 디지털 위험 요소 (예시)



출처 : NEWTON CONSULTING, 'AI/DX/디지털 리스크 관리 서비스' (<https://www.newton-consulting.co.jp/solution/dx/index.html>)

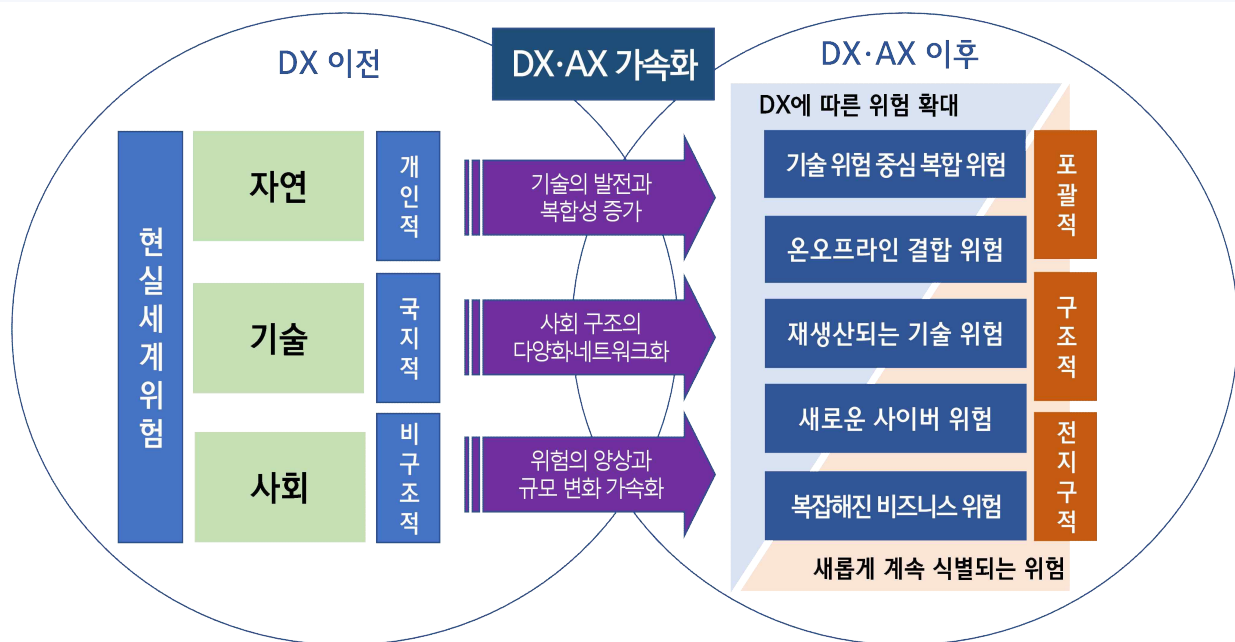
2. 디지털 위험 관리 패러다임과 구조의 변화

■ DX·AX 본격화 이전과 이후의 디지털 위험 패러다임이 변화

- ▶ 개인적·국지적·비구조적이었던 위험 요인이, DX·AX에 따라 기술이 사회의 구조적 기반을 이루면서 도처에 편재되어 확산
- ▶ 디지털 전환 사회에서 위험은 포괄적·전지구적·구조적 성격을 띠며 언제든지 역동적으로 예기치 못한 위기를 초래하고, 재난을 유발하므로 가능성 예측과 대응이 무엇보다 중요

위험(Risk) 요인 발생 → 위기(Crisis) 초래 → 재난(Disaster) 유발
 ↳ 미래에 관한 것으로 아직 닥치지 않은 많은 가능성

〈 그림 4 〉 디지털 전환(DX)과 디지털 위험 관리 패러다임의 변화



■ 디지털 위험의 요인과 특징을 다양한 관점에서 분석하고 대응해야 할 시대 도래

- ▶ DX·AX로 국가사회·조직을 변화시키기 위해서는 디지털 기술의 위험 관리가 중요 과제 중 하나이며, 디지털 위험 다변화로 기존 위험관리 방법과는 다른 접근법 필요

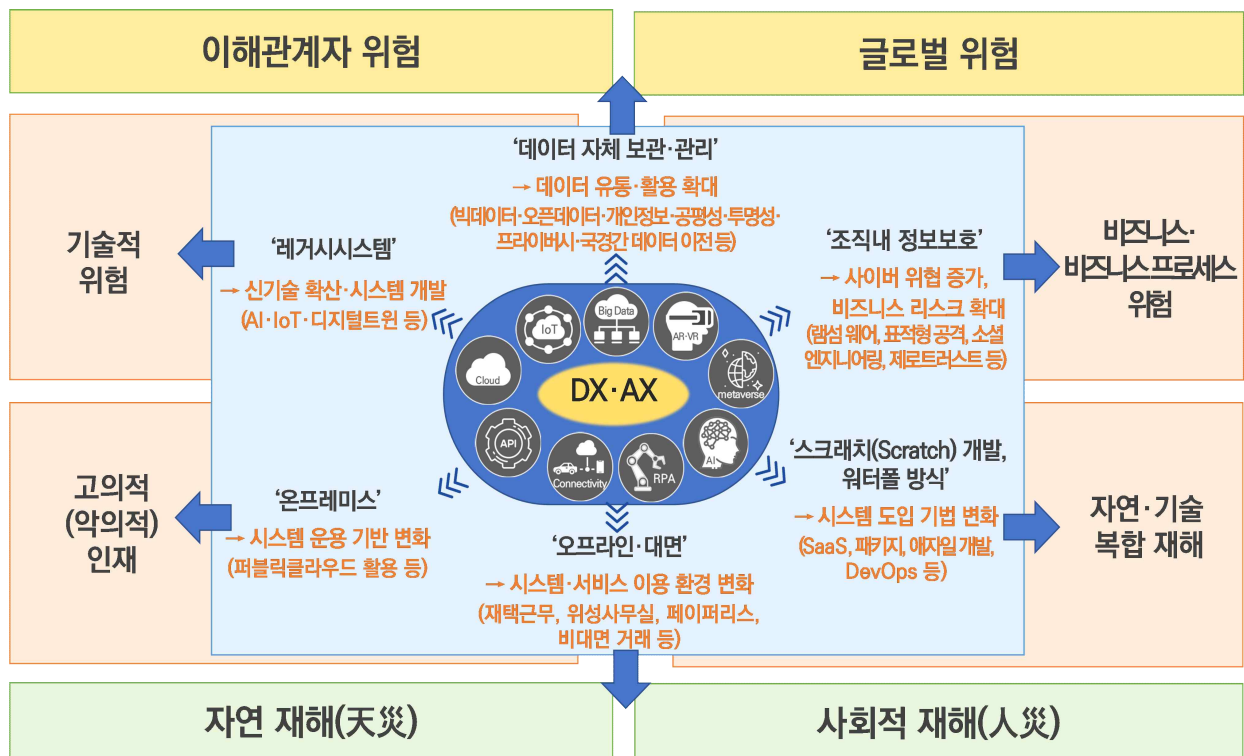
※ 예를 들어, 텍스트 생성AI 활용 시 정보보안의 검증 항목 대부분은 기존의 정보시스템이나 AI시스템과 유사하지만, 생성AI의 고유한 특징에서 기인하는 위험도 존재하므로 일반적으로 논의하기는 어려움

신규 비즈니스 창출 위험	업무·프로세스·조직·문화·환경을 넘어선 비즈니스 변혁·개혁으로 생기는 새로운 위험 (신제품·신서비스의 법규제 저촉 문제 등)
디지털 신기술 도입 위험	AI·클라우드 서비스 등 신기술 도입으로 발생 가능한 투명성(결과의 책임·검증)과 공정성(인종차별·인권침해), 프라이버시 등의 위험
데이터 활용·데이터 보호 위험	다종다양·대량 데이터 활용 관련 개인 데이터 취급, 외부 위탁처의 데이터 관리 미비에 의한 정보 유출, 퍼블릭 클라우드 추진에 수반하는 개인정보 취급 위험
사이버 보안 위험	랜섬웨어 등 사이버 공격의 고도화로 인한 위험

▶ 디지털 신기술과 DX·AX로 발생하는 디지털 위험의 다양한 요인과 특징을 고려해 대응 방안 마련

- ❶ (자연재해) 인간 의도가 포함되지 않은 자연현상으로 발생
- ❷ (사회적 재해) 사회적 피해를 동반하는 일정 규모 이상의 특정 사고
- ❸ (자연-기술 복합 재난) 자연 재난이 기술 재난으로 이어지는 경우
- ❹ (고의적 인재) 인간의 의도적·악의적 행위로 발생
- ❺ (기술적 위험) 기기 장애나 오작동, 누군가의 잘못이나 실수로 인해 유발
- ❻ (비즈니스-비즈니스 프로세스 위험) 기업 활동이 기업간·조직간·고객과의 네트워크와 디지털 기술·서비스에 의존하면서 발생
- ❼ (이해관계자 위험) 비즈니스 이해관계자와의 다양한 거래에서 발생
- ❽ (글로벌 위험) 국경을 초월한 시스템·데이터 관리, 무역 갈등으로 발생

〈 그림 5 〉 다양화복잡화 되는 디지털 위험 요인



출처 : MIZUHO 리서치&테크놀로지, 'DX 실현을 위한 디지털 리스크 관리'('22.3.)에 내용을 추가해 재구성

3. 디지털 위험 관리 거버넌스 변화 요구

■ 디지털 위험 패러다임 변화에 맞춰 획기적이고 체계적인 위험 관리가 필요

- ▶ 기술에서 파생된 위험이 다양한 사회경제 시스템과 상호작용하면서 확대되고, 일상화되고, 전면화되는 형태로 디지털 위험의 구조가 변화

새로운 디지털 위험의 복잡성 증대

↳ 사회문화적·인적·의사결정·사건·기술적·상호작용의 복잡성 등

- ▶ 데이터와 서비스가 네트워크화된 DX·AX 사회에서 디지털 재난은 국가사회 전체의 ‘디지털 블랙아웃(Digital Blackout)’*으로 확대될 가능성

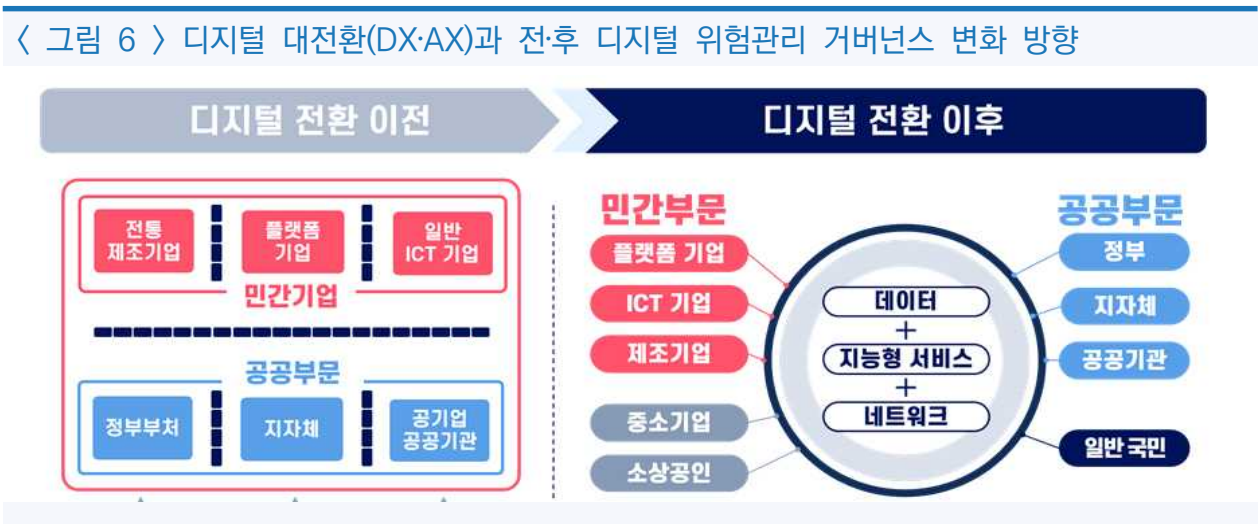
* 디지털 시스템 작동 중단으로 통신이 불가능한 상태. 단순한 ‘정전(Blackout)’과 달리 국민 안전·생업·생존에 직접적인 손해를 끼치고, 인명피해와 사회적 혼란 야기

〈 표 2 | 디지털 블랙아웃 발생 유형과 피해 (예시) 〉

발생 유형	피해 사례
• 자연재난으로 인한 통신시설의 피해 • 화재·폭발 등으로 인한 통신시설 피해 • 정전으로 통신시설 전력공급 차단 • 오류·고장 등으로 통신서비스 장애 • 트래픽 폭주로 통신서비스 마비 • 핵심 시설 마비로 통신망 단절 등	• 사고 발생 시 신고 불가 • 보안 시스템 문제로 치안 유지 불가 • 국가 안보 위험성 증가 • 결제시스템 이용 불가로 영업손실 • 모바일 결제와 송금 불가로 경제활동 불가 • 교통·전력·에너지·금융·통신 등 SoC 마비 • 사이버 전쟁으로 군사통신, 항공관제, 궤도위성 통제 불가 등

- ▶ 기존의 개별기업·부처·기관 등 사일로 형태의 디지털 위험 관리를 범국가적으로 체계화해 신속하고 동일한 수준의 대응이 되도록 관리 필요

※ 주요국은 디지털 블랙아웃을 새로운 사회적 재난으로 규정하고 국가 차원에서 관리(미국: National Security/Emergency Preparedness 프로그램 운영, 일본: 초고속 무선통신 네트워크인 ‘디펜더블 에어’ 운영으로 비상 상황에서도 통신 가능)



〈 표 3 | 디지털 위험 발생 요인 (예시) 〉

구분	주요 위험 요인
자연 재난 (천재(天災))	태풍, 홍수, 산불, 호우, 강풍, 풍랑, 해일, 대설, 한파, 낙뢰, 가뭄, 폭염, 지진, 황사, 조류 대발생, 조수, 화산활동 등
사회적 재난 (인재(人災))	화재, 붕괴, 폭발, 교통사고, 항공사고, 해상사고, 화생방 사고, 화학물질 유출, 환경오염 사고, 감염병, 미세먼지 피해 등
자연-기술 복합 재난 (Natech disaster, Techna disaster)	폭우로 전기 누전, 지구 온난화, 기후변화, 데이터센터 온실가스 배출 문제, 통신 기지국 전자파 문제, 정보 과부하에 따른 사회적 갈등, 승자 독식 경제, 정보시스템 오작동에 따른 자연재해(댐관리 시스템 오작동에 의한 홍수, 폐기물처리 제어시스템으로 폐기물 무단 방출, 가솔린 유출, 원자력발전소 폭발 등)
고의적 인재	전쟁·테러·파업·파산·해킹(네트워크·애플리케이션·웹·시스템), 크래커, 화이트해커, 사이버 공격, 개인정보 문제(유출·판매·침해·부정이용 등), 회계부정, 부정결제, 정보 유출, 온라인 계정 탈취, 데이터 위변조, 사이버폭력·사기, 시스템 개발기간 단축 등
기술적 위험	에너지 공급 중단, 전력 문제(블랙아웃), 전자파, 자기장, 설계문제(시스템·구조물 등), 정보시스템 장애·고장·오작동·정자·보안 문제, 클라우드 시스템 서비스·개인정보 유출, AI 윤리·인권 문제, 오픈소스나 클라우드 기술 문제, 기술 시스템 실패나 시스템 설계의 관리방식 문제, 정보기술의 오류와 네트워크 위험 등
비즈니스 위험	개인정보 유출, 데이터 위변조, 정보보안, 안전성·신뢰성 낮은 서비스, (악의적) 사이트 정보 변경, SNS상의 기업 브랜드 훼손 평판(평가) 피해, 종업원 IT리터러시 격차, IT인재 부족, 인재(기술자) 유출, IT기기 인식 부족, 정보시스템 운영·관리(신규 도입, 렌트·리스, 유지보수, 재해대책 등) 비용 상승, 법적 문제(법률 위반 비즈니스 설계), 윤리 문제(인권침해·설명책임 불이행), 노동자원 배치 전환, 몬스터 인플루언서 문제, 우수 IT인재 유지·채용의 어려움, 조직원의 정보시스템 활용 능력 부족 등
비즈니스 프로세스 위험	표적형 공격에 따른 정보 유출, 내부 부정에 의한 피해(정보유출, 업무정지 등), 랜섬웨어 피해(정보소실, 금전 피해), 메일 오송신과 오배신, 정보기기나 사원증 등의 분실·파손에 따른 정보 유출, 퇴직자·전직자의 재임시 이용했던 정보 이용, 기업 이메일 침해(BEC: Business Email Compromise), 이메일 계정 침해(EAC, Email Account Compromise)에 의한 서비스 침해, 자사 웹서비스에 리스크형 계정 해킹, 사이버 공격에 따른 조업 정지와 공급망 피해(자동차선박 등), 개인 정보를 활용한 상품과 서비스 유통, 소셜 미디어의 평판 모니터링 등
이해관계자 위험	공급망 리스크, 컨택트 리스크(광의의 준법 훼손 위험, 금융 업계에서 '고객 보호', '시장 건전성', '유효한 경쟁'에 부정적 영향을 미치는 행위가 발생할 위험), 타사(공급업체·서비스 제공업체·대행사·계약 직원·JV(Joint Venture)·상담원 등) 위험(데이터 유출 등의 정보보안 위험, 불안정한 재무 상황, 공급망 붕괴, 환경 보호 및 사회적 책임(직원 인권·건강 안전, 아동 노동 등)의 문제, 규제·컴플라이언스 우려, 뇌물수수·부정·부패 등), 직원 노동 위험(장시간 노동, 과로, 인재 유출 등) 등
글로벌 위험	공급망 변동성(물품 적기납품 어려움), 유가 변동성, 부품 가격 변동성, 금융위기, 글로벌 경제위기, 국제 은행 간 금융정보통신망(SWIFT) 마비, 해외 클라우드 서버 마비, 반도체 공급망 교란, 국가간 사이버테러, 무역 갈등(저작권데이터 활용 문제 등) 등

출처 : 워터저널, 「특집」 II. 자연-기술 복합 재난에 대한 이해와 대비」(‘22.7) 등을 참고로 내용을 추가, 재정리

【참고 3】 디지털 재해와 디지털 장애의 개념

□ 법률적 의미에서 재난과 재해 개념

- **재난** : 국민의 생명·신체, 재산과 국가에 피해를 주거나 줄 수 있는 것
- **재해** : 재난으로 인하여 발생하는 피해

※ 재해를 뜻하는 영어의 'disaster'는 우리말의 재해와 재난을 통칭하고 있으며, 실제로 재해와 재난은 흔히 혼용

[재난 및 안전관리 기본법 제3조]

1. “재난”이란 국민의 생명·신체·재산과 국가에 피해를 주거나 줄 수 있는 것으로서 다음 각 목의 것을 말한다.
 - 가. 자연재난 : 태풍, 홍수, 호우(豪雨), 강풍, 풍랑, 해일(海溢), 대설, 한파, 낙뢰, 가뭄, 폭염, 지진, 황사(黃砂), 조류(藻類) 대발생, 조수(潮水), 화산활동, 소행성·유성체 등 자연우주물체의 추락·충돌, 그 밖에 이에 준하는 자연현상으로 인하여 발생하는 재해
 - 나. 사회재난 : 화재·붕괴·폭발·교통사고(항공사고 및 해상사고를 포함한다)·화생방 사고·환경오염 사고 등으로 인하여 발생하는 대통령령으로 정하는 규모 이상의 피해와 국가 핵심기반의 마비, 「감염병의 예방 및 관리에 관한 법률」에 따른 감염병 또는 「가축전염병예방법」에 따른 가축전염병의 확산, 「미세먼지 저감 및 관리에 관한 특별법」에 따른 미세먼지 등으로 인한 피해

□ 디지털 재해와 디지털 장애의 개념

- **재해(Disaster)** : 정보기술 외부로부터 기인하여 예방 및 통제가 불가능한 사건으로 인해 정보기술 서비스가 중단되거나, 정보시스템 장애 발생 후로부터 예상 복구 소요 시간이 허용 가능한 범위를 초과해 정상적인 업무 수행에 지장을 초래하는 피해
- **장애(Incident)** : 통제 불가능한 재해(자연재해와 인적재해)를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 인적장애, 시스템 장애, 기반구조 장애(운영 장애, 설비 장애 등 포함) 등과 같은 통제 가능한 요인들에 의한 정보시스템의 기능 저하, 오류, 고장
 - ※ 협의의 장애 개념에서는 광의의 개념에서 포함한 자연재해를 제외하고 직접적으로 정보시스템에 영향을 미치는 요인들, 즉 시스템 장애와 기반구조 장애(혹은, 운영 장애와 설비 장애 등)와 같은 요인만을 포함
- 장애라고 할지라도 이로 인한 정보시스템 서비스의 중단시간이 허용 가능한 시간(예를 들어 24시간)을 초과하는 경우에는 재해로 볼 수 있음

□ 디지털 재해와 장애의 비교

구분	재해	장애
원인의 발생 위치	정보기술 기반 외부	정보기술 기반 내부
예방 및 통제	불가능	가능
정보기술 기반의 손상 규모	Site 전체	Site 내에서 부분적
대응조직의 수준	전사적 수준	정보시스템 관리 부서 수준
시스템 복원 예상소요시간	수일 이상	수시간(최대 24시간)

출처 : 「재난 및 안전관리 기본법」, 「자연재해대책법」 등

Ⅲ. 새로운 디지털 위험 대응 방안

1 디지털 대전환(DX·AX) 진행에 맞춰 디지털 위험 관리 상시화체계화

- ▶ 국가사회 운영 인프라와 시스템 전반이 디지털 기술로 초연결되어 효율화되고, 생산성·편리성 제고로 국민 삶의 질이 향상되었지만, 예측이나 예상이 어려운 디지털 위험도 상존
 - 디지털 위험 요인들은 디지털 장애와 재해를 유발해 경제적 손실을 초래하면서 국민 생활 전반과 국가경쟁력에 미치는 영향력도 지대하며, 사회적 혼란을 가중
- ▶ DX·AX에 따른 디지털 위험은 기존의 사이버 보안이나 개인정보 유출 등의 장애·사고를 넘어 광범위하게 발생하는 파급력 높은 위험으로, 사회 기능을 마비시키는 재난을 초래
 - 특히, 플랫폼 기업에 장애나 재해가 발생하면 메신저·결제·금융·교통·인증·공공서비스 등 많은 국민이 사용하는 핵심 서비스가 중단되어 단순한 불편을 넘어 대규모 ‘연계된 재난’ 발생
- ▶ 디지털 장애·재해가 국가사회 전체를 마비시키는 ‘디지털 블랙아웃’으로 확대되지 않도록 DX·AX 시대 디지털 위험 대응을 위한 정책적 관심, 제도적 개선, 체계적·구체적 실행 과제 마련 필요
 - 화재·전쟁·팬데믹·지진 등 위험 유형별, 시나리오별로 디지털 장애·재해 대비 운영 기술과 경험을 쌓기 위해 BCP(업무 연속성 계획)을 수립하고 정기적이고 지속적으로 모의훈련 실시

2 디지털 위험 관리와 대비를 위한 국민 의식 전환 노력과 국민 공감대 형성

- ▶ 디지털 위험으로 발생할 수 있는 새로운 형태의 재난·재해 예측과 신속한 대응, 회복탄력성을 높이는 방안을 체계적으로 마련해 교육하고 상시적으로 디지털 재난·재해 대응 훈련과 점검
- ▶ 급속히 변화하는 디지털 환경에 익숙해진 국민이 디지털 위험의 중요성을 새롭게 인지하고, 예상할 수 없는 디지털 위험에 노출되었을 때 대응할 수 있도록 지속적인 교육과 대책 마련
- ▶ 국가 안보나 테러, 자연 재난이나 사회적 재난 대응 수준으로 디지털 재난에 대응할 수 있도록 대국민용 디지털 위험 대응 매뉴얼 마련 필요

3 AX 촉진에 따른 새로운 디지털 위험 발생 가능성에 집중적으로 대비

- ▶ AI는 시스템 장애나 보안 사고를 일으키는 것을 넘어 무책임한 권력을 소수에게 집중시키거나, 사회적 신뢰 훼손, 공공 안전·신뢰와 안보 침식, 국제 안보 위협에 악의적으로 사용 가능(영국 AISI)
- ▶ 이러한 위험 중 일부는 이미 사람들에게 해를 끼치는 것으로 나타나고 있으며, AI 발전과 함께 AI 위험의 논쟁 또한 양극화되고 있어 안전·신뢰 가능한 AI 제공에 집중해야 할 상황
- ▶ AI는 우리에게 일어나고 있는 자연적 현상이 아니라 우리가 관리하고 지시할 수 있는 인간의 창조물이라는 것을 염두에 두고, 향후 수년간 안전에 기반한 AI 활용을 강구(영국 AISI)

4 세계 도처에서 동시다발적으로 발생하는 예측 불가능한 디지털 위험에 대응

- ▶ 새로운 유형의 디지털 위험은 일부 시스템이나 조직에 국소적인 불편이나 손실을 주기도 하지만, AI나 클라우드 서비스 이용이 일반화되면서 글로벌하게 전방위적인 재난을 초래

※ 러시아 해킹단체 레빌(Revil)이 플로리다 업체 카세야(Kaseya)를 공격, 이 랜섬웨어 공격으로 8천 킬로 떨어진 스웨덴 대형마트 쿵(COOP)의 전자결제시스템이 마비, 플로리다에서 시작된 해킹 공격이 대서양 넘어 스웨덴까지 파급('21.7)

- ▶ 디지털 플랫폼·시스템·데이터·서비스 등이 글로벌하게 산재되고 연계돼 있어 디지털 재해는 전세계를 대상으로 발생하므로 디지털 위험 대응 방안도 국제적 대응을 상정해서 마련하는 것이 필요

- ▶ 특히 AI 개발이나 이용에 있어서 안전성·신뢰성을 확보하기 위한 글로벌 룰 형성의 필요성이 요구되고, 공감대가 형성되고 있어 AI 안전과 관련한 글로벌 협력에 빠른 참여 필요

※ 미국과 영국은 이러한 국제적 룰 형성을 주도하기 위해 AI 안전성 확보를 위한 협력 각서를 체결('24.4). 특히 미국은 '자국 내 AI 정책이나 지침, 룰 등이 세계적인 행동 모델이 되는 것을 목표'로 추진

5 디지털 위험에 대응하는 범국가적 통합 거버넌스 마련

- ▶ 디지털 공공서비스 제공 기관, DX·AX 시대에 국민(소비자) 신뢰 확보가 필요한 디지털 서비스 개발·제공 기업, 디지털 서비스 이용자 등 분야 횡단 간에 디지털 위험 대응 거버넌스 구축

- ▶ 대기업·스타트업·학계·시민사회·중앙정부·지자체 등 산학연관이 협력해 디지털 전환 시대 새로운 위험 대응 방안을 마련하고, 국민은 디지털의 혜택과 권리를 누릴 수 있도록 위험 대응에 참여

- ▶ DX·AX 사회에서는 더 이상 기업이 디지털 서비스를 비즈니스적 관점에서만 바라보지 않도록, 각 기업에 국가 기간 서비스 제공자 수준의 디지털 위험 대응 매뉴얼을 요구하는 것이 필요

※ 맥킨지 등 컨설팅 기업은 디지털 전환 시대에 디지털 위험 관리를 필수적인 활동으로 인식하고 각 기업은 적극적으로 대응할 필요가 있다고 지적

“디지털 혁명이 가져오는 큰 이점이 유해 행동이나 콘텐츠로 손상될 수 있다는 것을 우리는 용납할 수 없다. 일부 기업은 플랫폼상에서 안전성 제고 조치를 강구하고 있지만, 전체적으로 진행이 너무 느리고, 일관성이 부족하다”(Online Harms White Paper(2020), 영국 정부)

【 참고 자료 】

(모든 관련 웹사이트 Accessed(2024-5~6))

- [1] Erik Stolterman, Anna Croon Fors(Umeå Universit), 'INFORMATION TECHNOLOGY AND THE GOOD LIFE', 2004. (https://link.springer.com/content/pdf/10.1007/1-4020-8095-6_45.pdf)
- [2] 딜로이트, 'See the Unseen, Global Digital Risk Survey 2022'
- [3] <file:///C:/Users/user/Downloads/jp-or-global-digital-risk-survey-2022.pdf>
- [4] https://data.wingarc.com/all_about_dx_by_erik-stolterman-35507
- [5] <https://www.sbbit.jp/article/cont1/100265>
- [6] https://monstar-lab.com/dx/about/digital_transformation/
- [7] <https://monstar-lab.com/dx/about/dx-it/>
- [8] <https://www2.deloitte.com/uk/en/pages/risk/articles/global-digital-risk-survey.html>
- [9] https://www.undp.org/sites/g/files/zskgke326/files/2022-09/DDRRMM%20White%20Paper%20Version%204.0%20%28FINAL%29_1%20September%202022.pdf
- [10] <https://www.upguard.com/blog/digital-risk>
- [11] <https://www.cloud-for-all.com/azure/blog/what-is-digital-risk-management>
- [12] <https://www.mizuho-rt.co.jp/publication/column/2022/0324.html>
- [13] <https://www.reliefsign.co.jp/column/230201>
- [14] https://www.brainpad.co.jp/doors/cp/dx_pyramid.html
- [15] https://www.brainpad.co.jp/doors/contents/dx_it/
- [16] <https://www.newton-consulting.co.jp/solution/dx/index.html>
- [17] <https://www2.deloitte.com/jp/ja/pages/deloitte-analytics/articles/ai-governance.html>
- [18] <https://www.dxlabs.jp/what> (DX 정의의 변천)
- [19] <https://www.otsuka-shokai.co.jp/erprnavi/topics/dx-mikata/archive/why-dx.html>
- [20] https://www.ntt.com/business/sdpf/knowledge/archive_16.html
- [21] https://www.ntt.com/business/sdpf/knowledge/archive_27.html
- [22] <https://www.smbc.co.jp/hojin/magazine/planning/about-dx.html>
- [23] https://www.softbank.jp/sbnews/entry/20221027_01
- [24] https://www.soumu.go.jp/denshijiti/index_00001.html
- [25] <https://www.sbbit.jp/article/cont1/100265>

- [26] <https://www.dxlabs.jp/what>
- [27] <https://www.dxlabs.jp/new-dx>(DX 재정의)
- [28] <https://www.stoltermanbergqvist.com/post/a-new-definition-of-digital-transformation-together-with-the-digital-transformation-lab-ltd>(A new definition of Digital Transformation together with the Digital Transformation Lab, Ltd)
- [29] <https://www.nist.gov/aisi> (미국 인공지능안전연구소)
- [30] <https://www.jetro.go.jp/biznews/2024/04/6c98249beee45a0a.html>
- [31] <https://www.nist.gov/news-events/news/2024/05/us-secretary-commerce-gina-raimondo-releases-strategic-vision-ai-safety>
- [32] <https://www.gov.uk/government/publications/ai-safety-institute-overview/introducing-the-ai-safety-institute>
- [33] <https://www.aisi.gov.uk/>

디지털 대전환(DX·AX)과 ‘디지털 위험 관리’의 중요성



‘세계 최고의 인공지능(AI) 활용기관’

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY