디지털로 여는 좋은 세상

2022-3호

D.gov 해외동향

Issue

영국 CDEI, 데이터와 인공지능(AI)에 대한 시민 인식 조사 결과 발표
영국 디지털규제협력포럼(DRCF), 인공지능 알고리즘 감사에 관한 보고서 발간
영국 국가사이버안전센터(NCSC), 앱스토어 사이버 보안 위협 사례 보고서 공개

News

EU, 디지털서비스법안 도입 확정 등 총 9건

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

CONTENTS

01 Issue

02 News

ISSUE ① 영국 CDEI, 데이터와 인공지능(AI)에 대한 시민 인식 조사 결과 발표

Reading Point

- 영국 데이터 윤리 혁신 센터(Centre for Data Ethics and Innovation, CDEI)는 데이터와 AI에 대한 시민 인식 조사를 실시하였으며 결과를 발표[1)]
- 디지털 기술에 관한 영국 시민의 전반적인 인식과 태도를 6개 주제로 구분하여 살펴보고, 정부 정책 설립에 참고할 수 있는 시사점 도출

Ⅰ 개요

❍ 영국 CDEI는 데이터와 AI에 관한 시민 인식 변화를 추적할 수 있는 설문조사(PADAI[2)])의 제1회 조사를 완료하고 결과보고서를 발간

- 영국 성인 4,257명을 대상으로 온라인 설문조사 실시('21.11 ~ '21.12)
- 디지털 소외계층 200명을 대상으로 전화 인터뷰 실시('21.12 ~ '22.1)
- 제1회 조사 결과는 시민 인식 변화를 추적하기 위한 향후 설문조사의 기준점으로 활용 예정

❍ 설문조사 결과를 6가지 주제별로 나눠 영국 시민의 전반적 인식·태도와 디지털 정보기술 친숙도[3)]에 따른 인식 차이를 제시

- 6가지 주제는 ①공익을 위한 개인정보 활용, ②개인정보 수집·이용에 대한 불신, ③ 데이터 제공·공유 의사, ④미디어와 데이터 활용에 대한 태도, ⑤AI에 대한 태도, ⑥코로나19의 영향

---

1) CDEI(2022.3), CDEI Public Attitudes to Data and AI Tracker Survey Wave 1 Final Report
2) PADAI는 'Public Attitudes to Data and AI'의 약자
3) Digital familiarity라는 표현을 의역하였으며, 응답자가 소셜미디어나 인터넷을 자주 활용하는지 또는 컴퓨터나 스마트폰과 같은 전자기기를 통해 온라인상의 활동을 할 때 자신이 있는지를 기반으로 4개 집단을 구분

〈 디지털정보기술 친숙도 집단별 주요 인구통계학적 특성〉

디지털정보기술 친숙도	응답자 수	평균연령	성별	사회경제적 배경
매우 낮음	200명*	71세	여성: 63% 남성: 36%	상위: 49% 하위: 52%
낮음	1,476명	61세	여성: 43% 남성: 56%	상위: 46% 하위: 54%
보통	1,697명	47세	여성: 51% 남성: 48%	상위: 46% 하위: 54%
높음	1,084명	36세	여성: 61% 남성: 39%	상위: 59% 하위: 41%

* 디지털 소외계층을 대상으로 실시된 전화 인터뷰에 참여한 응답자

❍ 온라인 설문조사로 파악할 수 있는 개인정보 제공·이용에 관한 주요 시민 인식 결과는 정부의 행정운영과 공공서비스 제공에 참고 가능

- **(개인정보 제공)** 정부의 공공서비스를 위해 자신의 개인정보를 제공하는 것에 대해 응답자 62%가 긍정적으로 인식
- **(데이터 활용 혜택·위협)** 응답자는 데이터를 활용하여 가장 큰 혜택을 실현할 수 있다고 판단되는 항목으로 코로나19 대응(19%)과 보건 분야(14%)를 선택했으며, 가장 큰 위협은 데이터가 안전하게 보관되지 않아 해킹되거나 탈취될 가능성(25%)
- **(데이터 수집 주체에 대한 신뢰)** 영국 국민건강보험(NHS, National Health Service)에 대한 응답자의 신뢰수준이 상당히 높았지만, 중앙정부와 소셜미디어에 대한 신뢰수준은 전반적으로 낮음

〈 데이터 수집 주체에 대한 신뢰수준 〉

	나의 이익을 고려할 거라 생각	데이터를 안전하게 보관할 거라 생각
중앙정부	39%	47%
NHS	89%	75%
소셜미디어	36%	33%
빅테크 기업	60%	49%

Ⅱ 주요 내용

1 공익을 위한 개인정보 활용

○ 대부분 일반 시민이 인터넷을 자주 활용한다고 응답했으나, 디지털 소외 집단의 인터넷 활용 수준은 제한적

- 온라인 설문조사에 참여한 일반 시민의 대다수가 인터넷을 매일 사용(84%)
- 반면, 전화 인터뷰에 참여한 디지털 소외 집단의 일부만 인터넷을 매일 사용(47%)

〈 집단별 인터넷 활용 수준 〉

	일반 시민 (온라인 설문조사 응답자)	디지털 소외 집단 (전화 인터뷰 응답자)
매일 인터넷 사용	84%	47%
자주 인터넷 사용	93%	63%

○ 대부분의 온라인 설문조사 응답자는 자신의 개인정보가 다양한 목적을 위해 활용되는 것에 대해 긍정적으로 생각

- 특히 새로운 치료법을 개발하기 위해 NHS에 개인정보를 제공에 대해 대다수가 긍정적으로 반응(81%)
- 정부의 공공서비스를 위한 개인정보 제공에 대해 절반 이상이 긍정적으로 인식(62%)
- 반면, 기업의 개인맞춤형 제품·서비스를 위한 개인정보 제공에 대해 긍정적으로 생각하는 응답자 비율은 오직 51%였으며, 특히 65세 이상 연령층의 비율은 더 낮음(40%)

○ 데이터 활용이 가장 시급하고 유용할 것으로 생각되는 분야로는 코로나19 대응(19%), 보건(14%), 그리고 경제(7%)를 지목

❍ 대다수 응답자가 데이터 활용이 자신에게 이득이 될 수 있다고 생각했지만(51%), 데이터 활용으로 인한 긍정적 사회적 영향(40%) 또는 균등한 이익 분배(31%)에 대해 불확실

〈 데이터 활용의 유용성에 대한 인식〉

	그렇다	중립적	아니다	모르겠음
데이터는 나에게 이득이 될 수 있는 제품·서비스 개발에 도움이 된다	51%	32%	14%	3%
데이터 수집·분석은 사회에 긍정적 영향을 미친다	40%	37%	20%	4%
모든 집단에 데이터 사용을 통한 이익이 균등하게 분배된다	31%	33%	31%	6%

❍ AI에 대해서도 많은 응답자가 긍정적인 영향을 기대

- AI가 정부, 대기업, 중소기업 중 특히 대기업에 긍정적인 영향을 미칠 것으로 생각(48%)
- 반면, AI가 소수집단에 미치는 영향이 부정적일 것으로 예상(28%)

〈 AI가 미치는 영향 〉

	긍정적	중립적	부정적	모르겠음
대기업에 미치는 영향	48%	27%	17%	9%
중소기업에 미치는 영향	36%	31%	24%	9%
정부에 미치는 영향	39%	27%	25%	9%
소수집단에 미치는 영향	26%	35%	28%	11%

2 개인정보 수집·이용에 대한 불신

❍ 대부분 응답자는 개인정보 수집·이용에 대한 제한적 지식만 보유

- 전체 응답자의 45% 정도만이 상당 수준 이상의 지식을 알고 있다고 응답
- 이용자의 나이와 개인정보 수집·이용 지식 간의 반비례 관계 관찰

〈 연령별 개인정보 수집·이용 지식수준 〉

연령	거의 없음	적음	상당함	매우 높음	모르겠음
18 - 24세	7%	26%	42%	19%	6%
25 - 35세	6%	30%	43%	18%	3%
35 - 44세	8%	35%	41%	13%	3%
45 - 54세	10%	44%	34%	9%	3%
55 - 64세	14%	50%	29%	4%	3%
65 - 74세	14%	51%	29%	2%	4%
75세 이상	18%	53%	24%	2%	3%
전체	11%	41%	35%	10%	3%

❍ 개인정보 수집·이용에 관한 안전성과 통제가능성에 대한 불신 존재

- 응답자의 연령대가 높을수록 자신의 정보 이용에 관한 통제 가능성이 없다고 생각
- 연령대가 높을수록 정부가 데이터 오남용에 대한 책임을 진다고 생각하는 비율도 감소

〈 기관·기업의 데이터 수집·이용에 대한 인식 〉

	그렇다	중립적	아니다	모르겠음
(투명성) 나의 데이터를 수집하는 기관·기업이 어떻게 데이터를 활용할지 알고 있다	40%	25%	33%	2%
(안전성) 나의 데이터를 가지고 있는 기관·기업은 데이터를 안전하게 보관하고 있을 것이다	32%	32%	31%	5%
(통제가능성) 나는 누가 어떻게 나의 데이터를 사용하는지 통제할 수 있다	33%	26%	38%	3%
(책임) 정부는 데이터 오남용에 대한 책임을 진다	40%	20%	35%	5%
(책임) 민간기업은 데이터 오남용에 대한 책임을 진다	45%	22%	28%	5%

❍ 많은 응답자가 데이터 보안에 대해 우려사항을 표현

- 특히 데이터 활용으로 인한 발생할 수 있는 가장 큰 사회적 위기로 데이터 보관 및 해킹·도난 위험(25%), 이용자 동의가 없는 데이터 판매(18%)를 지목

〈 데이터 관련 우려사항 〉

	선택 비율*
1. 데이터가 안전하게 보관되지 않고 해킹되거나 도난될 수 있다	25%
2. 기업은 나의 데이터로 이윤을 취득하기 위해 데이터를 다른 회사에 판매할 것이다	18%
3. 데이터가 (사회)감시를 위해 이용될 것이다	10%
4. 중요한 의사결정이 사람의 개입 없이 컴퓨터에 의해 결정될 것이다	9%
5. 사람들은 자신의 데이터가 공유될 때 충분한 선택권을 가지지 못할 것이다	8%
6. 일부 사람들이 서비스에 접근하지 못하고 배제될 것이다	8%
7. 새로운 기술이 사람들의 직업을 빼앗아 갈 것이다	6%
8. 새로운 기술은 편향되고 불공정한 결과를 초래할 것이다	5%
9. 모르겠음	9%
10. 기타	2%
합 계	100%

* 응답자는 10가지 선택사항 중 1가지를 선택

3 데이터 제공·공유 의사

❍ 응답자들은 정부·공공기관, 학계, 시민단체[4]에 대한 데이터 공유 의사가 가장 높음
- 다양한 데이터 수집·이용 기관, 개인정보 유형, 공유 목적 등을 조합한 시나리오를 응답자에게 제시한 결과, NHS가 데이터 수집·이용 기관으로 포함될 때 69%가 공유 의사를 표현
- 반면, 소셜미디어 기업이 포함될 때 36%만이 공유 의사를 표현*

* 응답자 인식과 행동 간의 차이가 있을 수 있으며, 실제 많은 사람이 소셜미디어 기업에 데이터를 제공

❍ 데이터 주체의 이익을 고려하는 기관·기업이 데이터를 잘 활용·보관할 것이라 인식
- 예를 들어, 응답자 대부분이 NHS가 자신의 이익을 고려한다고 생각했으며(89%), 데이터도 효과적이며 책임감 있게 사용한다고 생각(74%*)

* 표 내 '①~⑤ 평균' 수치 참고

- 예외적으로 지역 자영업자는 자신의 이익을 고려하지만(57%), 데이터 활용·보관이 미숙할 것으로 판단(49%)

〈 기관·기업별 데이터 수집·이용에 대한 신뢰도 〉

	대체로 나의 이익을 고려	① 상품·서비스 개선을 위해 효과적으로 데이터 사용	② 데이터를 안전하게 보관	③ 사회적 이익을 위한 데이터 이용	④ 데이터 활용정보를 투명하게 공개	⑤ 데이터 주인이 의사결정	①~⑤ 평균
NHS	89%	78%	75%	75%	73%	69%	74%
학계	76%	65%	63%	67%	62%	60%	63%
은행	71%	66%	69%	53%	60%	60%	62%
경찰	72%	58%	63%	57%	56%	52%	57%
공기업[5]	61%	55%	56%	48%	50%	48%	51%
지역정부[6]	57%	54%	53%	52%	50%	46%	51%
지역 자영업자	85%	55%	50%	46%	49%	47%	49%
빅테크 기업	60%	54%	49%	42%	43%	43%	46%
정부	39%	48%	47%	46%	41%	39%	44%
소셜미디어 기업	36%	36%	33%	30%	32%	34%	33%

4) Third sector organisations
5) Utilities provider로 우리나라 한국전력공사, 가스안전공사 등의 공기업에 해당
6) Local councils로 지역선거로 당선된 대표와 관련 관계자로 구성

4 미디어와 데이터 활용에 대한 태도

❍ 데이터에 관한 언론 기사를 회상할 때, 응답자들은 긍정적 기사보다 부정적 기사를 더 많이 언급

- 최근에 데이터 관련 뉴스를 접한 응답자의 37%가 데이터 활용에 대한 부정적 인상*을 기억

  * 긍정적 데이터 활용 기사를 기억하는 응답자는 24%였으며, 중립적 인상을 기억하는 응답자는 35%

  ※ 설문조사 실시 전, CDEI가 수행한 2021년 하반기 미디어 모니터링 조사에 따르면 공공·민간부문 조직의 데이터 침해와 유출에 관한 내용이 미디어에서 주로 다루어짐

❍ 응답자들의 부정적 이미지는 소셜미디어 기업의 개인 데이터 오용, 데이터 유출 등의 문제와 연관

※ 특히 페이스북 표적 광고와 같은 소셜미디어 기업의 개인정보 수집·판매와 관련된 이야기를 자주 회상

❍ 응답자들이 기억하는 긍정적인 기사는 코로나19와 연관된 데이터 활용이며, 주요 내용으로는 확산양상, 입원현황, 예방접종실적 등을 추적하여 대응 전략 설립하는 것이 지배적

〈 데이터 활용에 관한 언론 기사 이미지와 주요 내용 〉

부정적 이미지	긍정적 이미지
	

5 AI에 대한 태도

❍ 응답자들은 AI에 대한 자신의 지식이 제한적이라고 평가
- 응답자의 13%만이 AI에 대한 완전한 설명이 가능하다고 생각

※ AI에 대해 약간 설명할 수 있다고 생각한 응답자는 63%

❍ 성별, 사회경제적 배경, 그리고 디지털정보기술 친숙도에 따라 AI에 대한 자신의 지식 수준을 다르게 응답
- **(성별)** 대체로 남성이 여성보다 자신이 AI에 관해 설명할 수 있다고 응답

※ 남성: 70%, 여성: 56%

- **(사회경제적 배경)** 사회경제적 계층 높을수록 AI에 관해 설명할 수 있다고 생각

※ 상위: 68%, 하위: 56%

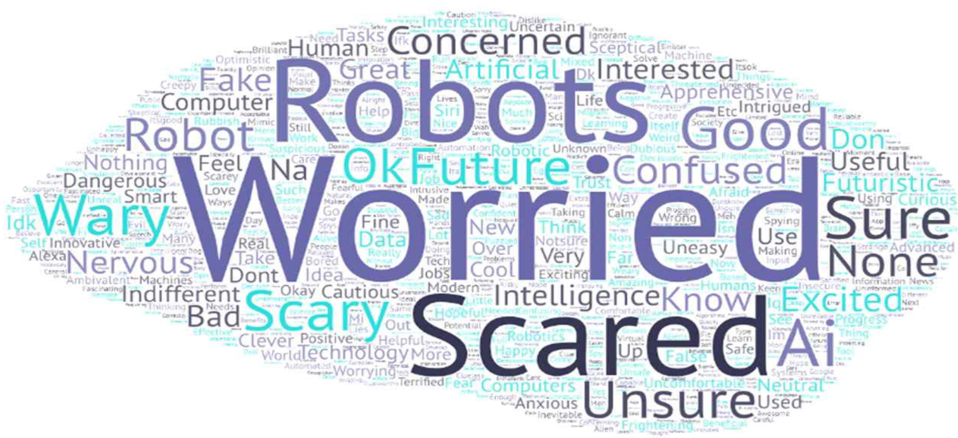
- **(디지털정보기술 친숙도)** 디지털정보기술에 대한 친숙도가 매우 낮은 집단은 대체로 자신의 AI 지식수준이 낮게 평가

※ 오직 34%가 AI에 대해 약간 또는 완전한 설명이 가능하다고 응답

○ AI에 대한 감정을 나타내는 단어로는 걱정(worried), 두려움(scared)과 같은 부정적 인식이 대부분이었지만, 흥분(excited)와 관심(interested) 같은 긍정적 단어도 표현

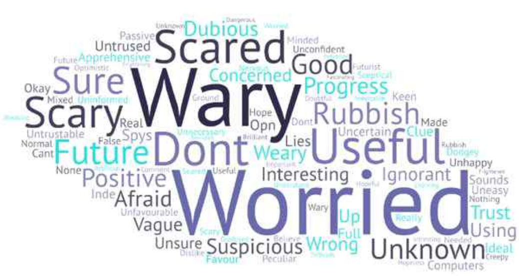
- 응답자들은 AI를 로봇, 컴퓨터와 강하게 연관시키면서 미래의 일부로 인식

〈 AI에 대한 감정 〉

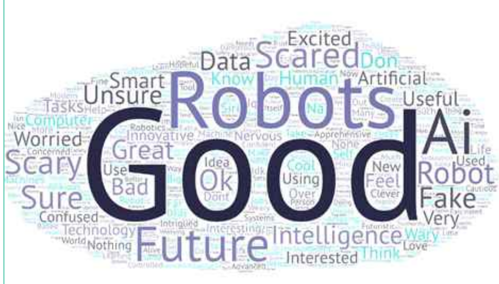


○ 대체로 디지털정보기술 친숙도가 높은 집단이 AI의 부정적 영향에 대해 우려하지 않는 양상을 관찰

〈 디지털정보기술 친숙도에 따른 AI에 대한 감정 〉



친숙도가 매우 낮은 집단



친숙도가 높은 집단

❍ 대부분 응답자는 웹페이지 추천(60%) 또는 암진단·치료(59%)를 위한 AI 기술 활용이 괜찮다고 생각했지만, 채용이나 재소자와 연관된 용도에 대해서는 부정적으로 인식*

* 과반수의 응답자가 채용(49%)과 재소자(55%)에 대한 의사결정에 AI를 적용하는 것이 불편하다고 응답

〈 AI 활용 용도·상황에 대한 인식 〉

가상사례(Scenario)	긍정적	부정적	모르겠음
(추천) 사람들이 구글과 같은 검색엔진을 사용할 때 웹페이지 추천을 위해 AI 활용하는 것은?	60%	32%	8%
(의료) 환자의 의료영상을 분석해 암 진단이나 치료 권유를 위해 AI를 활용하는 것은?	59%	34%	6%
(채용) 입사지원자의 이력서를 평가하고 면접 대상자를 선별할 때 AI를 활용하는 것은?	45%	49%	6%
(재소자) 재소자의 재범률이나 조기 석방을 판단하기 위해 AI를 활용하는 것은?	38%	55%	8%

❍ 디지털정보기술 친숙도가 높은 집단에 비해, 친숙도가 낮은 집단은 대부분 용도·상황에 AI를 활용하는 것에 대한 부담을 표현

〈 디지털정보기술 친숙도 집단별 AI 활용 용도·상황에 대한 인식 〉

가상사례(Scenario)	디지털정보기술 친숙도 집단별 각 사례에 대해 '괜찮다'라고 응답한 비율			
	매우 낮은 집단	낮은 집단	보통 집단	높은 집단
(추천) 사람들이 구글과 같은 검색엔진을 사용할 때 웹페이지 추천을 위해 AI 활용하는 것은?	36%	48%	63%	72%
(의료) 환자의 의료영상을 분석해 암 진단이나 치료 권유를 위해 AI를 활용하는 것은?	69%	56%	58%	64%
(채용) 입사지원자의 이력서를 평가하고 면접 대상자를 선별할 때 AI를 활용하는 것은?	32%	35%	47%	57%
(재소자) 재소자의 재범률이나 조기 석방을 판단하기 위해 AI를 활용하는 것은?	20%	29%	37%	50%

6 코로나19의 영향

❍ 코로나19 대응을 위한 영국 정부의 데이터 활용에 대한 엇갈린 견해가 존재

- 전체 응답자의 44%는 정부가 데이터를 실효성 있게 활용했다고 생각했지만, 43%는 부정적으로 평가

〈 코로나19 대응을 위한 정부의 데이터 사용 〉

	실효성 있음	실효성 없음	모르겠음
코로나19 대응을 위한 영국 정부의 데이터 활용	44%	43%	13%

❍ 코로나19 팬데믹 이후, 대부분 응답자는 영국 정부의 데이터 활용에 대한 신뢰도에 변화가 없다 대답(42%)

- 다만, 정부의 데이터 활용에 대한 신뢰도가 상승한 응답자(21%)보다 신뢰도가 감소한 응답자(32%)가 더 많음
- 디지털정보 친숙도가 높은 집단의 경우, 다른 집단보다 정부의 데이터 활용에 대한 신뢰도가 증가했다고 대답한 응답자 비율이 상당히 높음(34%)*

* 디지털정보기술 친숙도가 매우 낮거나(15%), 낮거나(14%), 보통(18%)인 집단과 비교할 때 통계적으로 유의미한 차이

〈 코로나19 팬데믹 이후 정부의 데이터 활용에 대한 신뢰도 〉

		감소	변화 없음	상승	모르겠음
전체		32%	42%	21%	6%
디지털 정보기술 친숙도	매우 낮음	37%	45%	15%	4%
	낮음	27%	51%	14%	8%
	보통	35%	41%	18%	6%
	높음	32%	29%	34%	5%

III 시사점

❍ **(공익을 위한 개인정보 활용)** 공익 개선을 위한 개인정보 활용 기회 포착
- 데이터와 AI에 관한 시민 인식 조사를 통해 새로운 치료법 개발, 공공서비스 개선, 맞춤형 제품·서비스 제공 등을 위한 데이터 제공에 대한 반감이 낮은 것으로 파악

❍ **(개인정보 수집·이용에 대한 불신)** 데이터 활용을 통해 얻을 수 있는 최대한의 효과를 누리기 위해 개인정보 수집·활용에 대한 시민의 불신과 우려사항을 해결할 필요성 존재
- 특히 데이터 보안과 개인정보보호를 담당하는 조직의 능력에 대한 신뢰를 향상하는 것이 급선무

❍ **(데이터 제공·공유 의사)** 대중의 데이터 제공·공유 의사를 높이기 위해서 강력한 개인정보 보호 거버넌스 체계를 마련하고 적극적 전파·홍보가 필요
- 업무 수행을 위해 데이터가 필요한 조직에 대한 시민의 신뢰수준 역시 데이터 공유 의사와 밀접한 관련성을 지녀 거버넌스 체계 마련에 참고 가능

❍ **(미디어와 데이터 활용에 대한 태도)** 데이터 활용에 대한 시민의 인식은 미디어와의 상호작용을 통해 형성
- 언론에서 부정적 보도를 주를 다루는 경향이 있으므로, 대처 방안 마련 필요

❍ **(AI에 대한 태도)** 디지털정보기술 친숙도와 AI에 대한 인식 간에 밀접한 상관관계 발견
- AI 기술의 사회적 채택과 활성화를 위해 시민 전반의 디지털정보 친숙도를 높이는 방안 마련도 고려 가능

❍ **(코로나19의 영향)** 전염병 극복을 위한 영국 정부의 데이터 활용의 실효성과 신뢰도에 대한 견해가 엇갈림
- 코로나19 팬데믹 이후, 정부의 데이터 활용에 대한 신뢰도가 증가한 응답자보다 감소한 응답자가 더 많았다는 점은 향후 정책 수행에 감안 필요

ISSUE ② 영국 디지털규제협력포럼(DRCF), 인공지능 알고리즘 감사에 관한 보고서 발간

Reading Point

- **영국 디지털규제협력포럼은 인공지능 알고리즘 감사에 관한 최신 동향, 정책, 그리고 미래 전망을 담은 보고서를 발간[7)]**
- **다양한 이해관계자가 참여하는 알고리즘 감사 생태계가 등장하고 있으며, 현재 식별된 문제와 바람직한 미래 감사 생태계 조성을 위한 정부 규제기관의 역할 제안**

Ⅰ 개요

❍ 알고리즘 감사는 자동화된 데이터 처리 시스템[8)]의 이점을 실현하기 위한 평가 방식
- 알고리즘은 디지털 제품과 온라인 서비스에 필수적 요소이며 다양한 이점과 단점[9)]을 지님
- 알고리즘 감사는 알고리즘의 긍정적 영향을 극대화하고 위험 발생 가능성을 최소화하기 위해 조직이 알고리즘을 통해 수행하는 작업과 알고리즘 시스템의 작동방식을 평가

❍ 현재 알고리즘 감사는 다양한 형태로 존재
- 조직이 임명한 외부 당사자 또는 자체적으로 시스템 감사를 수행하는 규제 기관, 연구원 또는 기타 당사자가 수행 가능
- 구체적 감사 방식으로는 알고리즘 시스템과 연관된 거버넌스 체계 문서자료 확인, 알고리즘 출력 결과 테스트, 내부 작동 검사 등을 포함

---

7) DRCF(2022.4.28.), Auditing algorithms: the existing landscape, role of regulators and future outlook
8) 보고서에서 활용된 '알고리즘'의 정의이며, 소비자 또는 사용자에게 직접적 영향을 미치는 의사결정이나 출력 결과(개인맞춤형 동영상 추천 등)를 도출하는 통계모형이나 머신러닝 모델을 포괄
9) 참고자료: DRCF(2022.4.28.), The benefits and harms of algorithms: a shared perspective from the four digital regulators

❍ 앞으로 정부, 학계 연구자, 민간기업 등의 다양한 이해관계자가 참여하는 알고리즘 감사 시장과 생태계 등장이 예상되며, 이에 대비하기 위한 일관된 감사 프레임워크와 표준이 필요

- 알고리즘 감사는 이미 명확하게 정의된 규정이 있는 전통적인 재무 감사와 다르며, 주요 감사 기준이나 접근법에 대한 합의 형성이 절실
- 알고리즘 감사 방식과 범위는 관련 위험의 성격·규모, 알고리즘이 배포되는 상황, 기존 규제 요구사항에 따라 조정 가능

❍ 디지털규제협력포럼은 규제기관이 알고리즘 시스템이 사용되는 맥락을 이해하고 관련 영향에 대한 일관된 평가 방식을 제시하기 위해 고려할 7가지 주요 질문을 제안

〈 알고리즘 감사에 관한 고려할 주요 질문 〉

• 알고리즘 감사를 수행할 때 참고할 프레임워크는 무엇인가?
• 어떤 기준·표준을 기반으로 알고리즘 시스템을 검토해야 하며, 규제 맥락에 따라 해당 기준·표준을 변경해야 하는가?
• 규제 준수와 관련하여, 알고리즘 감사는 어떤 역할을 해야 하는가?
• 관련 조직·기관은 누구*에게 어느 수준의 투명성을 보장해야 하는가? *예시: 소비자 또는 알고리즘 시스템의 영향을 받는 사람들
• 다양한 영역·맥락에서 어떤 유형의 알고리즘 감사가 적절한가?
• 알고리즘 감사 표준 개발을 누가 책임져야 하는가?
• 알고리즘 감사를 어떤 상황에 의무화해야 하는가?

II 주요 내용

1 알고리즘 감사의 역할

○ 알고리즘 감사는 다양한 이해관계자들 간의 신뢰를 구축하는 데 중요한 역할을 수행

- 알고리즘 시스템 개발자, 배포자, 규제자, 소비자 등의 이해관계자가 알고 있는 시스템 작동방식과 성능 정보가 일관되지 않아 시스템에 대한 불신 조장
- 알고리즘 감사는 특정 시스템의 작동방식과 영향에 대한 체계적 점검을 통해 시스템의 품질, 성능, 내외부 규정·규제의 준수 여부 등의 보장 수단으로 역할 가능

○ 현재 경쟁시장청(CMA), 금융감독청(FCA), 개인정보보호위원회(ICO) 등을 포함한 영국 규제기관들은 알고리즘 감사를 요구하거나 알고리즘 관련 정보를 요청할 권한을 보유

〈 알고리즘 감사 또는 정보 요청을 명령할 수 있는 규제기관〉

기관	규제 내용
경쟁시장청 (CMA, Competition and Markets Authority)	• 경쟁법 및 소비자 보호법에 따른 법적 정보 수집 권한을 사용하여 기업에 데이터 및 코드를 포함한 정보 요청 권한 보유하며, 특히 독점 금지 조사, 시장 조사, 합병 조사에 요청 가능 • 1998년 경쟁법(Competition Act 1998) 및 2002년 기업법(Enterprise Act 2002)에 따라 개인이 인터뷰에 참석하도록 강요 가능
금융감독청 (FCA, Financial Conduct Authority)	• 2000년 금융 서비스 및 시장법(Financial Services and Markets Act 2000)에 따라 광범위한 정보 수집 권한을 지녔으며, 기업의 데이터 및 코드 정보 요청 가능 • 특히 알고리즘 감사에서 사용될 수 있는 "숙련된 사람(skilled person)"에게 검토보고서 작성을 위임할 권한 보유하며, 협조의무를 지닌 면담, 현장 방문 등을 포함한 조사 실시 가능
개인정보보호 위원회 (ICO, Information Commissioner's Office)	• 영국 일반 개인정보보호법(UK General Data Protection Regulation)과 2018년 개인정보보호법(Data Protection Act 2018)[10]에 따라 외부 확인, 현장 테스트 및 면담을 수행하고 증거 복구·분석을 실시할 권한 보유 • 개인정보를 처리하는 조직·개인은 데이터 주체에게 방지·완화될 수 없는 심각한 영향을 미칠 가능성이 높은 개인정보를 처리하기 전에 의무적으로 개인정보영향평가(Data protection impact assessments)를 실시하고 ICO에 관련 자료를 제출 ※ 정부의 정보보호정책 개혁으로 인해, 영향평가 실시·보고 의무가 변경될 가능성 존재
방송통신규제 위원회(Ofcom)	• 현재 의회에서 검토 중인 온라인 안전법(Online Safety Bill)에 따라, 소셜미디어 플랫폼과 검색엔진 서비스에 관한 불법·유해 콘텐츠에 관한 조사 권한과 "숙련된 사람"에게 보고서 작성을 위임할 권한 등의 정보수집·조사 권한을 미래에 보유 가능

10) 참고자료: 개인정보보호위원회, 개인정보보호 국제협력센터, https://www.privacy.go.kr/pic/nation_england.do

❍ 표준은 알고리즘 감사에서 중요한 역할을 하며, 크게 개발·정보처리, 감사, 그리고 특성 평가와 연관

- **(개발·정보처리)** 편향된 결과 방지·완화 등을 위해 분석 대상 모집단을 대표할 수 있는 훈련 데이터를 사용해 알고리즘을 구축했는지 점검
- **(감사)** 감사 담당자가 알고리즘 편향성 등의 문제를 조사하기 위해 알고리즘 검사 방향* 설정

  * 예시: 새로운 데이터를 인공지능 모델에 입력하거나, 특정 인구통계학적 특성에 따른 결과값을 비교
- **(특성 평가)** 알고리즘 결과의 투명성, 설명가능성, 또는 편향성을 결정할 기준 제시

❍ 목적에 따라 인공지능 시스템과 연관된 표준을 개발하는 주체는 규제기관, 산업계 또는 시민단체를 포함

- 예시로, 영국 개인정보보호위원회(ICO)는 내부 조사팀이 인공지능 시스템의 규정·규제의 준수 여부를 평가할 때 사용할 프레임워크[11], AI와 데이터 보호에 대한 안내지침[12], 개인·조직의 자체 점검·감사를 위한 AI 및 데이터 보호 툴킷[13]을 공개
- IEEE[14], ISO[15], IEC[16]와 같은 국제 표준 협회·기관에서도 알고리즘 정보처리 표준을 개발하기 시작

❍ 적절한 표준체계가 자리 잡은 후, 인증체계 형성이 가능

※ 다만, 현재 알고리즘 감사 시장·생태계가 등장하는 초기 단계라서, 감사 담당자와 규제 기관의 역할 분담이 정립된 후 명확한 표준과 인증체계가 나타날 것으로 예상

❍ 알고리즘의 변동성으로 인해, 알고리즘 감사 결과의 유효성에 대한 제한사항 고려 필요

- 대다수의 머신러닝 알고리즘은 주기적으로 업데이트되지만, 알고리즘 감사가 특정 시점에 성능이나 결과만을 점검
- 그러므로 감사를 단일한 방식이 아닌 사례별 접근방식을 가지고 실시하는 것이 바람직

  ※ 비즈니스 모델, 알고리즘과 연관된 소비자·시민, 알고리즘 개발·배포 맥락에 대한 고려 필요

---

11) AI Auditing Framework, https://ico.org.uk/about-the-ico/media-centre/ai-auditing-framework/

12) Guidance on AI and data protection, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-artificial-intelligence-and-data-protection/

13) AI and data protection risk toolkit, https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/

14) Institute of Electrical and Electronics Engineers

15) International Organization for Standardization

16) International Electrotechnical Commission

2 알고리즘 감사 수준·범위

❍ 알고리즘 감사의 수준과 범위는 매우 다양하며, 크게 거버넌스 감사, 실증적 감사, 그리고 기능적 감사로 구분 가능

❍ 알고리즘 감사의 주요 결과는 흔히 감사 방법론과 평가 결과를 자세히 설명하는 보고서로 공개
- 규제기관이 명령·실시한 감사의 경우, 감사 결과는 집행 조치의 일부로 활용 가능
- 긍정적인 평가 결과는 감사 대상 시스템이 특정 표준, 품질 벤치마크, 또는 법적 프레임워크를 준수함을 입증·보증
- 반면, 부정적 결과는 시스템 개발자와 사용자 모두에 대한 관련 장애 및 위험에 대한 이해 향상

〈알고리즘 감사 유형〉

구분	주요 내용	감사 방법	예시
거버넌스 감사	적절한 알고리즘 거버넌스 정책·관행 준수 여부 평가	• 영향평가 • 준법·이행 감사 (compliance audit) ※ 투명성 감사 포함 • 적합성 평가	**(EU 인공지능 법안)** 고위험 인공지능 시스템에 대한 적합성 평가를 의무화
실증적 감사	입·출력값을 사용해 알고리즘의 영향을 분석	• 스크래핑 감사[17] • 미스터리 쇼퍼 감사[18]	**(프로퍼블리카 COMPAS 조사)** 미국 언론사 프로퍼블리카는 피고인의 예상 재범률 산출한 COMPAS 모델을 조사하기 위해 피고인의 인종 등을 임의로 변경하여 알고리즘 결과값을 비교
기능적 감사	알고리즘의 내부 데이터, 소스코드, 기타정보 등을 점검	• 시스템 입력값 검토[19] • 모델 개발과정 평가 • 위험 통제 조치 검토 • 스트레스 테스트[20] • (소스)코드 감사[21]	**(구글社 내부 개발과정)** 구글 동료 간에 서로가 개발한 코드를 검토하는 것이 흔한 관행

17) Scraping audit으로, 담당자가 감사를 위해 필요한 정보를 자동으로 수집하는 소프트웨어를 활용해 직접 감사대상 플랫폼에서 정보를 스크래핑하여 감사 실시
참고자료: https://www.adalovelaceinstitute.org/report/technical-methods-regulatory-inspection/

18) Mystery shopper audit는 인공지능 모델에 대한 접근권이 없을 때 활용되는 감사 방법이며, 감사를 위해 선별된 특성을 기반으로 사용자 계정을 생성해 일반 사용자와 같이 알고리즘 시스템을 사용하며 점검

19) 알고리즘(개발)에 활용된 데이터의 품질과 대표성 점검

20) 실험용 데이터세트와 시뮬레이션을 통해 알고리즘 모델의 작동방식을 시험

21) Code audit으로, 기술 전문가를 통해 알고리즘 모델의 (소스)코드를 직접 수기로 점검

3 현재 상황과 문제점

❍ 알고리즘 감사 생태계와 연관된 당사자는 정부, 표준화기관, 대형 IT 기업, 기존 및 신생 컨설팅 회사, 산·학계 연구원, 언론사, 그리고 시민단체를 포함하여 다양한 문제 존재

※ 학계, 산업계, 공공 부문, 그리고 시민단체에 소속된 알고리즘 기반 정보처리 시스템 전문가를 대상으로 실시한 인터뷰와 워크숍을 통해 현재 알고리즘 감사 생태계의 문제와 해결방안을 파악

① 알고리즘 감사 생태계 내 거버넌스 부재

- 의료건강 및 항공과 같이 분야를 제외하고 알고리즘 감사에 대한 규칙·표준이 없음
- 감사를 수행할 때 따라야 하는 표준이 불분명하며 합의된 표준이 없어 감사 결과는 조언을 제공하는 수준에 그침
- 부문·영역별 알고리즘 감사 원칙과 기준을 개발하여 문제 대응·극복 가능

② 알고리즘 접근권한 제한으로 인한 한계

- 감사 담당자가 인공지능 시스템의 알고리즘, 콘텐츠 조정·관리 정책, 관련 데이터 등에 대한 충분한 접근 권한을 얻지 못하는 경우 감사의 품질을 저하
- 알고리즘 시스템의 부정적 영향을 탐색하는 학계 연구진은 정보 스크랩핑[22]이나 허위계정 생성에 대한 법적 제재를 받을 위험에 노출
- 영국 경쟁시장청(CMA)은 인공지능 시스템에 대한 접근 권한 문제에 대응하기 위해 알고리즘이 수행하는 일부 기능에 대한 투명한 정보 공개 원칙을 제안

③ 이의제기·배상요구 기반이 부족

- 알고리즘 감사는 인공지능 시스템으로 인해 피해를 경험한 사람들이 활용할 수 있는 핵심 자원
- 하지만 현재 일반 대중이나 시민단체가 알고리즘으로 도출된 결정·결과에 이의를 제기하거나 시정을 요구할 수 있는 명확한 메커니즘이 부족
- 일부 사회단체는 EU 집행위원회가 제안한 인공지능 법안에 개인·집단구제 조항을 포함할 것을 촉구[23]

---

22) 각주 17번 참고

23) 참고자료: https://edri.org/wp-content/uploads/2021/12/Political-statement-on-AI-Act.pdf

④ 알고리즘 감사에 대한 일관성 부족

- 알고리즘 감사 간의 일관성 보장하기 어려우며, 특히 공정성(fairness)에 대한 합의된 정의가 없어 각 분야, 적용 기술·서비스, 사용 맥락에 따라 상이[24)]
- 알고리즘 감사 결과로 특정 시스템의 영향을 객관적으로 판단하기 위해, 산업 부문별 안내지침이나 표준이 필요

  ※ 또한, 감사의 독립성을 보장하고 감사 결과에 대한 공개적 보고도 요구 가능

⑤ 알고리즘 감사 담당자와 대상자 간의 이해관계 존재 가능성

- 일부 산업계 이해관계자는 감사 담당자와 대상자가 서로 경쟁업체*일 가능성을 우려

  * 감사 담당자를 고용한 회사가 감사 대상자의 경쟁업체일 가능성도 존재
- 따라서 알고리즘 감사를 위한 데이터 수집·활용에 대한 강력한 법적 보호가 필요

⑥ 알고리즘 감사 비용 부담 고려

- 알고리즘 감사 비용이 높으면, 규모가 작은 조직보다 큰 조직에게 유리하게 작용
- 관련 규제기관은 기업·조직 규모와 상관없이 기술혁신을 장려하기 위해 노력 필요

24) 참고자료: https://proceedings.mlr.press/v81/binns18a.html

4 현재 상황·문제 대응을 위한 정부 규제기관의 역할

❍ 알고리즘 감사 생태계의 문제점을 해결하기 위하여 산·학계 기관과 시민단체는 알고리즘 감사에 활용될 수 있는 기술 표준·도구를 개발할 수 있으며, 정부 규제기관은 5가지 주요 역할 수행 가능

① 알고리즘 감사 실시 시점 명시

- 알고리즘 시스템의 잠재적인 위험에 따라 감사를 언제 수행해야 하는지에 대한 안내지침 발표

② 표준 및 모범사례 수립

- 관련 기관·조직이 인공지능 시스템에 대한 정보를 누구에게 공개해야 하는지를 포함한 기준과 모범사례를 자체적으로 또는 공공기관·표준화기관과 함께 개발해 공개

③ 알고리즘 감사 기반조성 조력자로 역할

- 알고리즘 감사의 독립성, 투명성 보장을 위한 최소 요구사항, 알고리즘 감사 범위 등에 대한 기대치를 설정하는 표준을 만들거나 지원

※ 정부 규제기관은 감사 담당자·기관에게 라이선스를 부여·승인하고, 벌금 부과 또는 운영 금지를 명령하려 알고리즘 감사의 품질관리에 기여할 수 있음

④ 알고리즘 감사로 식별된 피해에 대한 조치·대응 확인

- 알고리즘 감사로 심각한 문제나 불법행위가 발견되었을 때, 적절한 조치가 이뤄지기 전까지 해당 알고리즘 시스템의 활용을 금지
- 추가로, 당사자가 정보를 제공하도록 인센티브를 제공하고 대중 및 기타 이해관계자가 피해를 보고하기 쉬운 환경 조성
- 새로운 감사 요구사항을 도입하는 이점과 기업에 대한 규제 비용 간에 균형이 이루어질 수 있도록 신중한 고려 필요

⑤ 오해 소지가 있는 주장 식별·해결

- 알고리즘 시스템과 관련된 잘못된 주장과 관행을 둘러싼 불만을 접수, 이해 및 대응

5 향후 계획

❍ 영국 디지털규제협력포럼은 알고리즘 감사 생태계에 정부 규제기관의 역할을 정의하기 위한 일련의 가설을 설립하고, 정부, 학계 연구자, 민간기업, 시민단체 이해관계자에 의견 요청

※ 각 가설의 장단점, 추가연구가 필요한 가설, 알고리즘 감사와 연관된 기타 고려사항 등에 대한 의견을 요청하고, 수렴된 의견을 요약자료로 정리해 공개 예정

〈 정부 규제기관의 잠재적 역할과 장단점 〉

규제기관의 역할	장점	단점
1. 알고리즘 개발·배포자가 외부 감사를 활용해 규정·규제 준수 여부를 입증할 수 있도록 명확한 감사 기준·조건 제시	• 규정 준수 여부를 입증할 수 있는 확실한 방안 확보 • 알고리즘 감사 수요 증가로 시장 경쟁 촉진	• 알고리즘 감사 방식의 혁신성과 유통성 감소 • 법원이 규정·규제 준수 여부를 결정하는 경우, 안내지침만 제공
2. 제3자가 알고리즘 감사를 수행하는 방법 그리고 규정 준수를 입증하기 위한 감사 결과물 작성 안내지침 개발·공개	• 특정 규정에 적합한 감사 유형을 안내해, 감사 비용 절감 • 시장 진입 장벽을 낮춰 제3자가 활발히 참여	• 기술발전에 따른 새로운 유해 사례에 맞춰 지침 조정 필요 • 개념화 수준이 높은 지침이 잘못 해석될 위험 존재
3. 규정·규제에 설명된 요구사항을 표준화기관이 알고리즘 감사를 통해 점검 가능한 기준·지표로 개발할 수 있도록 지원	• 제3자가 관련 규정·규제 준수 관련 이해 도모 • 시장의 진입 장벽을 낮춤	• 알고리즘 감사로 점검할 수 있는 기준·지표 개발이 바람직하지 않거나 불가능한 상황 존재
4. 내·외부 감사 담당자, 일반 대중, 시민단체와 새로운 피해에 관해 증거 축적을 돕기 위한 안전한 정보 공유 방안 마련	• 알고리즘의 영향과 연관된 규제적 한계 보완 • 적절한 경우, 수집한 정보로 공식적인 조사·조치에 착수	• 정보의 품질이나 불투명성과 연관된 문제 발생 가능
5. 감사 인증체계를 통해, 인증받은 조직·기관이 알고리즘 시스템의 준법성·적절성을 보증	• 공식적 준법감사 필요성과 비용 감소 • 알고리즘 시스템에 대한 신뢰와 활용을 향상	• 감사 인증체계가 이해관계자 또는 일반 대중을 대상으로 충분한 투명성을 보장하지 못하면, 관련 책임·책무성 회피방안으로 작용
6. 통제된 환경에서 알고리즘 시스템을 시험하기 위해 규제 샌드박스 확대	• 알고리즘 시스템 개발·배포자는 시스템이 규제 요구사항에 부합하는지 미리 파악 가능 • 시간을 절약하고 규제 준수 비용 감소	• 소수의 규제기관만 샌드박스에 참여한다면, 시스템 개발·배포자는 여러 기관을 개별적으로 연락해 준법사항 확인 필요

III 결론 및 시사점

○ **(알고리즘 감사 필요성)** 알고리즘 시스템이 의도한 방식으로 작동하고, 알려지지 않은 유해 결과 없이 작동하는지 확인하기 위해 독립적으로 또는 외부 제3자를 통해 감사 수행

○ **(알고리즘 감사 방법)** 알고리즘 감사는 크게 거버넌스, 기술 및 실증적 감사로 나뉠 수 있으며 다양한 주체가 주도

- 내부적으로 수행하는 자체 감사는 역동적인 시스템 점검·검사가 가능하며 규제 부담으로 인한 비용 절감 효과를 실현할 수 있지만, 외부 검사만큼 문제를 자주 발견하지 못함
- 규제기관, 학계 연구원, 제3자 감사조직, 시민단체, 언론사 등의 이해관계자는 다양한 방식으로 알고리즘 감사에 참여할 수 있으며, 알고리즘 정보처리 시스템의 감시·감독에 참여

○ **(현재 알고리즘 감사의 문제점)** 현재 형성되고 있는 알고리즘 감사 생태계에는 3가지 주요 문제점 존재

- 합의된 표준, 원칙, 기준 등을 기반으로 한 효과적인 거버넌스 체계가 부재
- 일부 알고리즘 감사 담당자는 알고리즘 시스템에 접근할 수 없어 난감
- 알고리즘 정보처리 피해자가 이의를 제기하고 배상을 요구할 수 있는 소통창구가 부족

○ **(미래 발전을 위한 규제기관의 역할)** 규제기관은 기업이 사회에 도움이 되는 시스템을 개발·배포하도록 장려하는 동시에 피해 위험을 최소화할 수 있도록 지원

- 특히 ①감사 시점 명시, ②표준·모범사례 수립, ③알고리즘 감사 시장 기반조성, ④식별된 피해에 대한 조치 확인·보장, ⑤알고리즘 시스템에 관한 오해 소지 식별·해결에 기여 가능

○ **(건전한 알고리즘 생태계 조성을 위한 논의)** 알고리즘이 사회에 미치는 영향력이 고려하여 적절한 알고리즘 감사 체계와 방안에 대한 사회적 논의 필요

- 알고리즘이 사회에 미치는 영향력이 고려하여 건전하고 투명한 알고리즘 생태계 조성을 위해 알고리즘 감사는 필수적
- 일률적인 감사 표준이나 승인 보다 규제기관, 학계 연구진, 산업계, 시민단체, 언론사 등의 이해관계자가 참여해 분야별 감사 범위와 방향성에 대한 논의와 합의 도출이 필요

ISSUE ③ 영국 국가사이버안전센터(NCSC), 앱스토어 사이버 보안 위협 사례 보고서 공개

Reading Point

- **영국 국가사이버안전센터(National Cyber Security Centre, NCSC)는 애플 앱스토어, 구글 플레이스토어, 삼성 갤럭시스토어와 같은 애플리케이션(앱) 장터의 사이버 보안 위협 사례를 정리해 보고서로 발간[25]**
- **다양한 위협 사례 정보를 기반으로 관련 정책 설립에 기여해 소비자와 기업 모두를 보호하는 앱 장터의 사이버 보안과 개인정보보호 개선에 도움이 될 것으로 기대**

Ⅰ 개요

❍ 지난 10년 동안 스마트폰과 스마트 기기의 사용이 빠르게 증가하였으며, 대부분 사용자는 추가 응용 프로그램 및 콘텐츠를 내려받을 수 있는 온라인 장터인 '앱스토어'를 활용

- 코로나19로 모든 전자기기*의 앱 수요가 더욱 증가하여 소비자와 기업을 위협하는 다양한 사이버 보안 문제가 발생

* 스마트폰, 태블릿PC 등의 전자기기 외에도 데스크톱·노트북 컴퓨터, 게임 콘솔, 웨어러블 기기, 스마트 TV·스피커, 또는 사물 인터넷 기기에도 앱 설치가 가능

❍ 영국 소비자가 앱 장터를 신뢰하며 응용 프로그램을 내려받을 수 있도록 보장하는 것이 중요

- 영국 국가사이버안전센터는 공식·비공식 앱 장터에서 발생하는 다양한 보안 위협 사례를 조사·분석해 사이버 보안과 개인정보보호 개선을 위한 기초 자료를 제공

※ 영국 국가사이버안전센터는 이미 사이버 보안 위협을 식별·방지할 수 있도록 사고 관리 지침[26], 기기 보안 지침[27], 사이버 인식 지침[28]을 포함한 안내지침을 제공

25) National Cyber Security Centre(2022.5.20), Threat report on application stores
26) Incident Management Guide, https://www.ncsc.gov.uk/section/about-ncsc/incident-management
27) Device Security Guidance, https://www.ncsc.gov.uk/collection/device-security-guidance
28) Cyber Aware Guidance, https://www.ncsc.gov.uk/cyberaware/home

Ⅱ 주요 내용

1 악성코드로 인한 사이버 공격

❍ 앱스토어에 인기가 높은 앱이 외부 사이버 공격으로 손상된 상태로 존재한다면, 수백만 명의 사용자가 잠재적인 피해에 노출되며 앱 제공업체 측에도 평판이 훼손될 가능성 존재

❍ 컴퓨터 시스템, 네트워크 또는 장치를 손상시킬 수 있는 모든 소프트웨어를 악성코드(malware)라 지칭하며, 악성코드는 다양한 방식으로 앱 장터를 침투하고 사이버 보안을 위협

- 사용자의 기기가 악성코드로 손상된 경우, 스파이웨어[29] 및 랜섬웨어[30]를 포함한 특정 유형의 악성코드로 인해 개인정보 유출이나 사기 피해 위협으로 이어질 가능성 존재
- 피해를 당한 사용자나 기관·조직은 중요한 데이터를 잃어버리거나, 데이터·시스템 접근 권한 상실, 금전적 손해, 또는 자사의 평판 손실 등의 영향을 받음

〈악성코드가 앱 장터를 침투하는 경로〉

경로 유형	설명
타사 앱스토어 내 앱 복사본	• 특정 앱이 공식 앱스토어에 삭제되었거나 특정 국가에 제공되지 않을 때, 사용자가 공식 앱스토어의 대안으로 존재하는 타사 앱스토어[31]에 있는 복사본을 내려받을 때 발생
앱 업데이트	• 이미 존재하는 앱의 업데이트 버전에 내부 개발자가 악성코드를 추가하거나 외부 공격으로 인해 업데이트 버전에 악성코드가 포함되었을 때
타사 소프트웨어 개발 키트	• 광고노출이나 기타 기능을 앱에 추가하기 위해 개발자가 타사 소프트웨어 개발 키트(Software Development Kit, SDK)를 사용하며, 해당 SDK에 악성코드가 있을 때
앱 개발자 변경	• 사용자가 많은 앱의 개발자 계정을 외부 공격자가 구매하고 악성코드가 포함된 업데이트 버전을 공개할 경우
앱 개발 도구	• 개발자가 앱을 개발할 때 활용하는 도구(빌더, 컴파일러)에 악성코드가 있을 때 발생

29) 사용자의 동의 없이 또는 사용자를 속여 설치되어 광고나 마케팅용 정보를 수집하거나 중요한 개인 정보를 빼가는 악의적 프로그램 (출처: TTA 정보통신용어사전)

30) 컴퓨터 사용자의 파일들을 암호화하여 금전을 요구하는 악성코드 (출처: TTA 정보통신용어사전)

31) 구글 안드로이드 플랫폼에서 활용할 수 있는 타사 앱스토어로, 사용자와 개발자가 자유롭게 앱을 올리고 내려받을 수 있지만, 만약 악성코드가 의도적으로 추가된 앱이 있을 때 큰 사용자 피해 발생 가능

2 앱스토어 유형별 사이버 보안 위협

❍ 모바일 기기에 앱 설치, 가상 음성 비서에 기능 추가, 스마트 기기에 앱 설치, 그리고 유·무료 게임 콘텐츠를 내려받기 등을 위한 다양한 앱스토어가 존재하며 사이버 보안을 위협

① 공식 모바일 앱스토어

- 안드로이드와 iOS 모바일 기기의 공식 앱스토어는 애플 앱스토어와 구글 플레이 스토어이며, 각각 430만 개와 290만 개의 앱을 제공('20년 11월 기준)
- 개발자가 앱스토어에 앱을 올리기 전, 악성 콘텐츠·코드가 있나 확인하는 심사 절차 존재
- 심사 절차가 있음에도 불구하고, 엄청난 사용자 수를 보유한 앱스토어에서 사이버 범죄자들은 자신의 수익을 극대화하기 위해 끊임없이 악성코드를 침투시키려 노력

〈 주요 보안 위협 사례 (공식 모바일 앱스토어) 〉

유형	설명
애플 앱스토어 'XcodeGhost'	• 2015년에 악성코드가 있는 소프트웨어 개발 키트(SDK) 'XcodeGhost'로 인해 대량의 개인정보 유출 • 중국에서 피해가 가장 컸는데, 당시 대용량 파일을 내려받을 때 인터넷 속도가 느려 대부분 개발자가 애플 iOS 앱 개발 도구인 'Xcode'의 타사 배포 버전을 활용했기 때문 • 메신저, 은행·주식 거래, 이동통신사 서비스, 지도, SNS, 게임 등을 비롯한 다양한 앱에 침투하여 대량의 개인정보 유출 • 애플社는 악성코드로 감염된 모든 응용 프로그램을 제거하고 모든 개발자가 애플에서 제공하는 Xcode로 응용 프로그램을 다시 컴파일하도록 요청
구글 플레이스토어 '조커'	• 2017년부터 2020년까지 '조커(Joker)'라는 악성코드가 포함된 PDF스캐너, 사진편집기 등의 유틸리티 앱을 많은 안드로이드 기기 사용자가 내려받고 사용 • 공격자는 악성코드를 사용해 피해자 핸드폰의 SMS 기능으로 프리미엄 또는 유료 서비스에 구독하고, 피해자 이동전화요금으로 비용을 청구해 금전적인 이득을 취득 • 구글社는 2017년부터 구글 플레이스토어에서 1,700개 이상의 악의적 앱을 제거했지만, 몇몇 악성코드 앱이 아직도 존재
마이크로소프트 스토어 'Torrenty'	• 2015년 마이크로소프트 스토어(Microsoft Store)에서 P2P 파일 교환 도구인 'Torrenty'라는 앱에 있는 악성코드로 사용자 기기의 브라우저에 팝업 광고 노출 • 앱에서 '업데이트 1개 보류 중'이란 알림 메시지가 표시되었으며, 일부 사용자가 알림창을 누르고 브라우저를 실행하면 원치 않는 광고에 노출 • 마이크로소프트社는 Torrenty를 즉시 제거

② 타사 모바일 앱스토어

- 애플 iOS와 달리 구글이 제공하는 안드로이드 플랫폼은 타사 앱스토어를 허용하는데[32], 심사 절차가 철저하지 않아 스파이웨어[33], 은행·금융정보 유출 또는 원치 않은 유료 서비스 구독을 시도하는 악성코드에 취약
- iOS 기기 이용자도 '탈옥(Jailbreak)'이라는 방식을 통해 타사 앱스토어를 사용할 수 있으며, 애플이 제공하는 보안 제어를 우회하게 되어 보안 위협에 더욱 취약

〈 주요 보안 위협 사례 (타사 모바일 앱스토어) 〉

유형	설명
안드로이드 타사 앱스토어 'PhantomLance'	• 2015년부터 'PhantomLance' 악성코드는 여러 안드로이드 기기용 타사 앱스토어에 발견되었으며, 은행·금융정보를 포함한 사용자의 개인정보를 훔치고 광고를 노출 • 'OpenGL 플러그인'이라는 앱에서도 발견되었으며, 대부분 앱스토어에 올려진 앱의 초기 버전이 아닌 업데이트 버전 등을 통해 악성코드에 감염
안드로이드 타사 앱스토어 'ANDROIDOS_ LIBSKIN.A'	• 2016년에 여러 안드로이드 기기용 앱스토어[34]에서 모바일 게임, 보안, 음악 스트리밍 등을 위한 앱으로 위장한 악성코드 'ANDROIDOS_LIBSKIN.A'를 발견 • 악성코드는 사용자의 기기를 루팅[35]한 후 사용자 데이터를 수집하고 원치 않는 앱을 내려받는 팝업 알림을 지속적으로 보냄
안드로이드 타사 앱스토어 'Triada'	• 2021년 4월, 많은 사용자가 활용하는 안드로이드 타사 앱스토어 'APKPure Store'에서 프리미엄 서비스에 구독하고 추가 악성코드를 내려받을 수 있는 악성코드 'Triada'를 발견 • APKPure측은 자사 앱을 빠르게 업데이트하여 대응
iOS 타사 앱스토어 'KeyRaider'	• 2015년에 iOS 기기 사용자가 '탈옥' 방식을 통해 앱을 올리고 내려받을 수 있는 타사 앱스토어 'Cydia'에서 'KeyRaider'라는 악성코드 발견 • KeyRaider는 총 225,000건 이상의 사용자 애플 계정정보를 탈취

32) 각주 31번 참고
33) 각주 29번 참고
34) Aptoide, Mobogenie, mobile9 and 9apps 등의 타사 앱스토어 포함
35) 안드로이드 기기의 운영 체제를 해킹해 관리자 권한을 얻는 행위 (출처: TTA 정보통신용어사전)

③ 음성 비서 (앱)스토어

- 아마존 에코(Echo)와 구글 네스트(Nest) 기기와 같은 다양한 사물 인터넷 기기로 가상 음성 비서 기능을 활용 가능
- 특히 아마존社는 모바일 앱스토어와 유사하게 다른 개발자들이 자사의 음성 비서인 알렉사(Alexa)의 기능을 확장할 수 있는 'Alexa Skills' 플랫폼을 제공[36)]
- 아마존 인공지능 스피커가 약 1억 대 이상 판매되었으며(2019년 1월 기준), Alexa Skills를 통해 악성코드를 배포해 사용자의 데이터 탈취와 도청 가능성 존재

※ 예시: 인공지능 스피커 마이크로 사용자가 모르게 오디오 녹음을 하는 앱을 설치해서 도청

〈 주요 보안 위협 사례 (음성 비서 스토어) 〉

사례
• 2021년 초, Alexa Skills 앱 심사 과정에 취약점을 발견 • 악의적 의도를 가진 외부 공격자는 신뢰할 만한 개발자의 이름으로 Alexa Skills 앱을 개발·공개한 후, 앱 버전 관리를 통해 악성코드를 추가해 사용자가 휴대폰 번호 등의 개인정보를 제공하게 유도 가능 • 아마존社는 발견된 취약점에 대한 대응방안을 마련하기 위해 노력 중

36) Alexa Skills Kit 홈페이지: https://developer.amazon.com/en-US/alexa/alexa-skills-kit

④ 스마트 기기 (앱)스토어

- 스마트 워치, 스마트 TV 등의 기기로도 앱을 내려받기 위한 다양한 스토어가 존재
- 해커가 모바일 앱스토어가 아닌 스마트 기기 (앱)스토어를 공격할 이유가 적으나, 악의적 의도로 활용될 가능성 존재

※ 예시: 스마트 워치로 사용자의 위치정보를 수집하거나 스마트 TV로 사물 인터넷 봇넷(Botnet)[37] 공격을 실시

〈 주요 보안 위협 사례 (스마트 기기 스토어) 〉

유형	설명
'Fitbit Gallery' 취약점	• 2020년 10월, 핏빗(Fitbit) 기기에 앱을 내려받을 수 있는 'Fitbit Gallery'의 취약점 발견 • 핏빗 사용자는 외부 개발자 앱을 내려받기 위한 전용 링크가 있다면, 공식 스토어인 Fitbit Gallery로 연결되는 설치화면에서 앱을 내려받고 사용 가능 ※ 사용자는 공식적인 설치화면을 보고 해당 앱이 안전하고 합법적이나 생각할 수 있음 • 만약 악의적 의도를 가진 해커가 악성코드가 있는 앱을 개발해 전용 링크로 배포한다면, 사용자 위치정보, 신체 데이터 등 다양한 정보를 훔칠 수 있음 • 핏빗社는 사용자에게 전용 링크로 앱을 내려받을 때 참고할 보안 경고 메시지를 공개하며 대응
삼성 '타이젠 (Tizen)' 취약점	• 2017년에 삼성 스마트 TV, 스마트 워치 및 모바일 기기를 위한 운영 체제인 '타이젠 (Tizen)'에서 40개의 취약점 발견 • 가장 심각한 취약점은 타이젠 앱스토어를 통해 원격으로 코드를 실행하며 기기를 조정해 스마트 TV와 같은 기기에 악성코드를 내려받는 것 • 삼성은 발견된 보안 취약점에 대응하기 위해 관련 연구자와 협력하겠다고 발표

37) 악성 프로그램에 감염되어 나중에 악의적인 의도로 사용될 수 있는 다수의 컴퓨터들이 네트워크로 연결된 형태를 말하며, 해커는 봇넷에 연결된 컴퓨터를 원격 조종해 개인 정보 유출, 스팸 메일 발송, 다른 시스템에 대한 공격 등 악성 행위를 할 수 있음 (출처: TTA 정보통신용어사전)

⑤ 게임 스토어

- 닌텐도, 엑스박스, 플레이스테이션과 같은 일부 콘솔 게임 회사는 전용 스토어를 제공[38)]
- PC게임을 위한 다양한 온라인 스토어도 있으며, 대부분 사람들은 '스팀(Steam)'[39)]을 가장 많이 활용
- 합법적인 게임 소프트웨어를 가장해 수많은 플랫폼에서 악성코드가 사이버 보안을 위협

〈 주요 보안 위협 사례 (게임 스토어) 〉

사례
• 유료 게임 콘텐츠의 접근 권한을 얻기 위해 사용자 계정정보 탈취하는 사건이 자주 발생 ※ 예시: 다크웹에 악성코드 'BloodySteaker'를 구매해 쉽게 계정정보 탈취 가능 • 2015년 'Octopus City Blues'라는 게임의 가짜 스팀(Steam) 페이지*에 악성코드가 있는 체험판을 발견하였으며, 스팀측은 페이지를 삭제하며 대응 * 실제 게임 예고편, 스크린샷 및 설명을 활용해 복사본을 만들었으며, 페이지를 관리자는 피해를 입은 사용자가 다른 사람들에게 남긴 경고 댓글까지 삭제

38) PlayStation Store, Xbox Store, Nintendo eShop 등이 존재

39) Steam 게임 스토어 홈페이지: https://store.steampowered.com/

Ⅲ 결론 및 시사점

❍ 사이버 범죄자는 사용자의 개인정보를 탈취하거나 금전적 이득을 취하기 위해 앱스토어에 악성코드를 침투시키려 노력

- 애플 앱스토어, 구글 플레이스토어와 같은 공식 앱스토어에는 악성코드를 식별하고 걸러내기 위한 심도있는 심사 절차가 존재
- 안드로이드 운영체계를 사용하는 기기의 경우, 여러 타사 앱스토어가 존재하는데 대부분이 유사한 심사 절차가 없어 보안 위협에 매우 취약

❍ 코로나19 팬데믹의 영향으로 게임용 앱을 포함한 다양한 온라인 앱의 수요가 크게 증가하며 악성코드로 인한 보안 위협이 증가

- 개별 사용자와 기관·조직은 공식 또는 타사 앱스토어를 통해 다양한 기기에 앱을 안전하게 내려받을 수 있도록 주의 필요
- 앱스토어 운영자는 영국 디지털문화미디어스포츠부[40]가 발표한 앱스토어 보안 및 사생활 보호 지침(안)[41]을 참고해 악성코드 심사 절차를 개선할 수 있음

40) Department for Digital Culture, Media & Sport(DCMS)

41) DCMS(2022.5.4.), App security and privacy interventions
('Proposed Code of Practice for App Store Operators and App Developers' 부분 참고)

NEWS 1 EU, 디지털서비스법안 도입 확정[42]

❍ 유럽의회[43]와 유럽이사회[44]는 디지털서비스법안[45]을 제정하기로 결정

❍ 구글, 애플, 메타(구 페이스북) 등의 온라인 플랫폼社에 불법 온라인 콘텐츠, 제품, 서비스를 삭제할 의무를 부여해 온라인 거래와 연관된 책임과 권리의 균형을 재정립할 것으로 기대

〈 디지털 서비스 법안의 주요 내용[46] 〉

A. 인터넷상 불법 제품, 서비스 및 콘텐츠에 대해 조치
• 사용자가 불법 콘텐츠를 쉽게 표시(flag)할 수 있도록 하며, 플랫폼이 신뢰할 수 있는 사용자와 협업 • 온라인 플랫폼·마켓 내 사업이용자의 추적가능성(신원 확인 등) 보장에 관한 의무 부여
B. 사용자와 사회의 권리·권한 확장을 위한 방안 마련
• 콘텐츠 삭제·접근차단 등의 콘텐츠 조정에 대한 불만 제기와 구제방안 마련 • 신뢰할 수 있는 연구자에게 주요 온라인 플랫폼의 핵심 데이터 제공, 시민단체에게 개방데이터 제공 • 추천 알고리즘을 비롯한 다양한 사안에 관한 투명성 요구
C. 위험성을 평가하고 경감시킬 방안 수립
• 대형 플랫폼社를 대상으로 시스템 오용을 방지하기 위해 위험관리를 수행할 의무를 부여하고, 자사의 위험관리체계에 대한 독립적 감사를 요구 • 모두의 보건안보에 영향을 미칠 수 있는 위기에 신속하고 효율적으로 대응할 수 있는 메커니즘 마련 • 미성년자를 보호하고 민감한 개인정보를 사용하는 표적 광고를 제한하기 위해 새로운 안전장치 마련

42) European Parliament(2022.4.23.), Digital Services Act: agreement for a transparent and safe online environment

43) European Parliament

44) European Council

45) Digital Services Act, DSA

46) European Commission(2022.4.23.), Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment
참고자료: 김현수·전성호(2020.12.21.), 유럽연합 디지털서비스법안(Digital Services Act)의 주요 내용 및 시사점, KISDI Premium Report
이재호(2021.3), EU 디지털서비스법과 국내 소비자법의 시사점, 소비자정책동향 제111호

NEWS 2 EU 집행위원회, 디지털 권리와 원칙 선언문 제안[47]

❍ EU 집행위원회는 유럽연합 내 디지털 전환 방향성을 담은 '디지털 권리 및 원칙 선언문[48]' 초안을 발표

※ 유럽의회[49]와 유럽이사회[50]는 초안을 검토 중이며, 세부 내용을 수정하여 서명·채택 예정[51]

〈 '디지털 권리 및 원칙 선언문' 주요 내용 〉

1. 인간중심의 디지털 전환
• 모든 유럽인들에게 기술을 통한 혜택을 제공 • 시민들의 기본권을 보장·존중하며, 개인이 이루고 싶은 꿈이나 욕구를 향해 갈 수 있도록 장려
2. 단결과 포용 장려
• (인터넷 접속) 소득수준과 거주지에 상관없이 모든 사람이 고속인터넷망에 접근하고 동일한 조건하에 온라인 콘텐츠, 서비스, 프로그램을 활용할 수 있도록 보장 • (디지털 교육) 모든 사람에게 디지털 교육, 훈련, 평생학습 권리를 보장하고 디지털 기술 역량을 습득할 수 하도록 지원 • (직업·업무 환경) 소득수준, 생활방식, 근로기간에 상관없이 모든 사람에게 평등하고 건강하며 안전한 디지털 업무 환경을 보장하며, 일과 삶의 균형 도모를 위해 디지털 연락 단절을 요구 • (온라인 공공서비스) 모든 사람은 유럽연합 내 제공되는 주요 공공서비스를 온라인 환경에서 접근할 수 있고, 필요 이상으로 개인정보를 제공해야 하지 않도록 온라인 공공서비스 제공
3. 선택의 자유 확보
• (알고리즘과 인공지능 시스템) 인공지능 기술과 연관된 다양한 위험과 악영향을 방지하며 사용자가 스스로 정보에 입각한 선택을 통해 혜택을 누릴 수 있도록 지원 • (공정성) 모든 사람이 객관적이고 신뢰할 수 있는 정보를 기반으로 온라인 서비스를 효율적으로 선택할 수 있고, 동시에 플랫폼社와 같은 서비스제공자 간의 공정한 경쟁·혁신을 장려할 수 있는 환경 조성

47) European Commission(2022.1.26.), European Declaration on Digital Rights and Principles for the Digital Decade

48) European Declaration on Digital Rights and Principles for the Digital Decade

49) European Parliament

50) European Council

51) Free Software Foundation Europe(2022.4.14.), EU Declaration of Digital Rights and Principles

4. 디지털 공공 공간에 관한 참여 보장
• 시민참여와 민주주의를 증진할 수 있는 디지털 기술 개발 지원 • 온라인 환경에서 지속적으로 기본권 및 표현의 자유를 보호 • 모든 형태의 불법 콘텐츠에 대해 조치 방안 수립 ※ 표현과 정보의 자유를 존중하며, 별도 모니터링 의무를 부과하지 않는 방안 필요 • 허위정보와 기타 유해 콘텐츠로부터 사람들이 보호받을 수 있는 온라인 환경 구축
5. 안전성, 보안성, 그리고 개인정보에 관한 권리 확립
• (안전성) 안전이 보장되며 개인정보를 보호할 수 있는 디지털 기술, 제품, 그리고 서비스 이용을 보장 • (개인정보 권리) 모든 사람들이 자신의 정보에 관한 권리와 통제권을 확보한 상태에서 디지털 서비스 간에 손쉬운 개인정보 공유·이전을 보증 • (아동·미성년 보호) 영유아를 비롯한 미성년층이 안전한 선택을 하고 온라인 환경에서 창의성을 표현할 수 있도록 안전한 디지털 환경을 형성하고 불법 온라인 콘텐츠, 착취, 남용 등의 디지털 범죄로부터 보호
6. 지속가능성 장려
• 최소의 환경·사회적 영향을 미치는 지속가능한 디지털 기술 개발을 지원 • 환경과 기후에 긍정적 영향을 미칠 수 있는 디지털 해결책 개발·사용

NEWS 3 미국 하원, 전자화폐 개발·시범적용 법안 발의[52]

❍ 미국 하원이 전자화폐 개발과 시범적용을 요구하는 '전자화폐 및 안전한 하드웨어 법안[53]'을 재무부에 제출

- 미국 중앙은행 연방준비제도이사회[54]가 연구하고 있는 중앙디지털 화폐(CBDC)와 별개인 디지털 달러 제안
- 재무부가 발행하는 이캐쉬의 배포와 시범 활용을 위한 법률적 근거를 제의
- 특히 전자화폐 혁신 프로그램[55]을 설립하여 이캐쉬와 관련된 일련의 시범 사업 관리 가능

❍ 미국 하원이 제안한 이캐쉬는 블록체인 기술을 기반으로 하지 않기 때문에 분산원장[56]이나 분산형 디지털 데이터베이스를 지니지 않는다는 점이 특징

- 분산원장 기반의 암호화폐에서 흔히 요구되는 거래 데이터 생성과 공동 기록·관리 절차를 최소화하고 이용자 간 직접적인 거래(peer-to-peer transfer)가 가능
- 은행이나 신용카드사 등의 민간 금융중재기관 없이 활용 가능
- 이캐쉬 거래 정보는 하드웨어 기기에 로컬 암호화와 같은 보안 기술을 활용해 저장·관리[57]

※ 연방정부, 이캐쉬 유통업체, 기타 제3자는 거래 정보를 수집, 모니터링 또는 보유할 수 없음[58]

❍ 법안이 통과될 경우, 4년 이내에 일반 시민을 대상으로 이캐쉬 배포 가능

- 재무부는 법안 통과일을 기준으로 90일 이내 시범 사업 착수

---

52) The Verge(2022.3.28.), A new bill would launch a large-scale test of digital dollars
53) Electronic Currency and Secure Hardcare Act, ECASH
54) Federal Reserve System
55) Electronic Currency Innovation Program
56) 분산 네트워크 참여자가 암호화 기술을 사용하여 거래 정보를 검증하고 합의한 원장(ledger)을 공동으로 분산관리 (출처: TTA 정보통신용어사전)
57) Electronic Currency and Secure Hardware Act p.6
58) Electronic Currency and Secure Hardware Act p.10

NEWS 4 브루킹스 연구소, 연방정부 내 인공지능 개발 권고사항 제안

❍ 브루킹스 연구소는 연방정부 내에서 책임감 있는 인공지능을 개발을 위해 지켜져야 할 원칙과 실천방안을 제시[59)]

〈 책임감 있는 인공지능 개발을 위한 권고사항 〉

구 분	내용
구체적 행동 강령 수립	• 모든 정부기관이 준수할 공통 행동 강령 마련 ※ 예시: 공정성, 투명성, 사생활 보호 • 개별 기관의 특성에 따라 세부 행동 강령 조정 ※ 예시: 교육 또는 보건의료 기관은 기록물의 정보보안과 기밀성에 관한 강령 필요
윤리 원칙을 장려하고 편견 방지	• 인공지능 기술을 기반으로 한 자동화된 의사결정에 대한 인간의 개입 가능성 고려 • 인간중심적이며 개별 정부기관에 적합한 알고리즘과 소프트웨어 개발·활용
명확한 평가기준 개발	• 알고리즘이 정부기관의 임무 수행에 도움이 되며 책임감 있는 인공지능 개발을 위한 행동 강령을 충족하는지 판단할 평가기준 마련 • 절차적 공정성(procedural fairness)과 실질적 공정성(substantive)을 구분한 기준 개발 • 데이터 공유 및 개방형 API을 통해 다양한 주체가 평가기준을 활용할 수 있도록 장려
문제 해결을 위한 기술 표준 사용	• 산·학계 전문가 간의 기술 표준이 등장하면 정부기관도 안전성, 사생활 보호, 공정성, 형평성 등에 관한 공통 표준 준수 가능 • 직·간접적으로 편견과 차별로 이어질 수 있는 인공지능 기술의 활용을 방지할 수 있는 기술 표준 마련 ※ 인종과 종교 등의 민간정보를 추정할 수 있는 대체변수(proxy) 악용 가능성도 고려 필요
시범 사업을 통한 위험관리	• 소규모 시범사업을 통해 많은 사람에게 피해를 미치지 않으며 소프트웨어 개발 가능 • 적법한 절차에 따른 시범 프로젝트의 진행과 각 사업단계에 관한 철저한 평가 필요
다양한 인력 혼용·양성	• 시스템 설계자뿐만 아니라 사회적, 윤리적 전문성을 가진 변호사, 사회 과학자, 정책 전문가, 윤리학자가 필요 • 직원들이 필요한 역량·지식을 습득할 수 있도록 자금지원 제공

59) Brookings Institution(2022.3.20.), Six Steps to Responsible AI in the Federal Government

NEWS 5 캐나다 정부, 인공지능(AI) 기반 지능형 농업 투자 활기

❍ 캐나다 농업농산식품부[60]는 국가 농업 지원정책[61]을 통해 Mojow Autonomous Solutions[62]社에 최대 41.9만 달러를 투자 예정[63]

- 투자금은 농장 운영에 활용될 수 있는 디지털 트윈 생성도구 'Eye-Box'를 개발하기 위해 활용될 예정
- Eye-Box는 여러 대의 카메라, GPS, 실시간 데이터 처리 기기 등을 탑재한 보급형 기술로 야외 환경에 적합한 소형 센서를 탑재한 종합 AI 기반 데이터 기록·분류 솔루션
  ※ 자동으로 이미지를 수집하고 각 픽셀을 분류하는 작업을 실행하여, 농업 활동 전반에 걸친 디지털 재현 가능
- 특히 컴퓨터 알고리즘을 활용해 농업현장 문제해결과정에 체계적 정보에 입각한 의사결정 지원

❍ 캐나다 정부의 지원을 받는 비영리기관 SCALE AI[64]는 5개의 혁신적 AI 사업을 지원하기 위해 2,400만 달러를 투자 예정[65]

- 농업 부문 프로젝트로, 식물 생장 측정 기술과 이미지 기반 데이터를 활용하여 농산물 생산량 최적화 플랫폼을 개발할 예정
  ※ 디지털 전환 자문 기관 Adastra와 농업 분야 선도 기업 Good Leaf Farms가 참여하며, 총 250만 달러 투자(SCALE AI 투자금 100만 달러 포함)

---

60) Agriculture and Agri-Food Canada

61) Canadian Agricultural Partnership
홈페이지: https://agriculture.canada.ca/en/about-our-department/key-departmental-initiatives/canadian-agricultural-partnership

62) Mojow Automonous Solutions

63) Government of Canada(2022.4.5.), Government of Canada invests in digitization of farming to strengthen sustainability of Canada's agriculture sector

64) 모든 산업 분야에 AI 기술을 적용하고, 다수의 산업 부문이 상호연결된 공급망을 형성하여 캐나다를 선도 수출국으로 만드는 것이 목표

65) SCALE AI(2022.4.6.), Accelerating the integration of artificial intelligence solutions: SCALE AI announces a $24-million investment in five new projects

〈 캐나다 SCALE AI 5대 AI 투자사업 〉

산업 분야	투자 목적	사업 내용
농업	농식품 생산량 최적화	• 옥내 재배 환경에서 LED 조명을 통해 연중 재배·수확이 가능한 수직 농업용 스마트플랫폼 고도화 • 식물 생장 측정 기술과 이미지 기반 데이터를 활용하여 농산물 생산량과 작물 품질 최적화
제조업 유통·판매	유통·판매 수요 예측	• 120개국에 있는 유통·판매업체에게 제품을 공급하는 캐나다 기업[66]의 수요 예측을 지원하기 위한 알고리즘 기술 개발 • 핵심 의사결정자와 공급망 이해관계자들을 위한 인사이트 제공을 목표
복지서비스	방문요양 서비스 제공 최적화	• 가정 방문 요양 서비스업체가 활용할 수 있는 경영·인력관리 AI 솔루션[67] 고도화 • 한정된 요양보호사의 개별 역량·전문성을 고려하여 최적의 경로와 일정을 예측할 수 있는 모델링 기술 개발
의약품 판매	의약품 공급·재고 관리	• AI 기반 데이터 분석을 통해 의약품 미판매 재고로 인한 손실과 공급 부족으로 인한 문제 방지 • 의약품 관리를 위해 현장에서 요구되는 노동집약적 수작업 감소
제조업 품질관리	강판 제조공정 생산성 향상	• 센서와 제품검사 시스템을 통해 제조과정에 발생할 수 있는 결함 존재 여부, 유형, 크기 등을 예측하는 품질관리 시스템 개발 • AI 모델을 기반으로 한 품질관리로 강판 공급망 전반에 걸쳐 폐기물을 감소하고 생산성 개선

66) 레저용 전문 차량 제조업체 BRP(Bombardier Recreational Products)

67) AyalaCare

NEWS 6 미·영국, 디지털 기술을 활용한 보안 이슈에 대응

❍ 미국 시민단체는 시민의 사생활과 디지털 권리를 침해하는 안면인식 기술에 대한 문제 제기를 지속적으로 해왔으며, 최근 AI 안면인식 업체 ClearView AI가 대부분 미국 기업에 소프트웨어를 판매하지 않기로 합의[68]

- 미국의 프라이버시 및 디지털 권리 옹호 단체는 안면인식 소프트웨어가 프라이버시 문제를 비롯하여 잠재한 실제적 위험을 내재하고 있다고 비판
- 이미 캐나다, 호주를 포함한 일부 국가는 ClearView AI의 소프트웨어를 불법으로 취급
- 2020년에 미국자유시민연합과 몇몇 비영리단체는 일리노이 주 법원에 ClearView AI가 생체정보보호법(BIPA)[69]을 위반했다며 소송을 제기
- ClearView AI는 정부기관을 제외한 대부분 기업에 자사의 소프트웨어를 판매하지 않기로 합의

❍ 영국 정부는 허위 소셜미디어 계정으로 기밀정보 유출을 유도하는 온라인 첩보요원에 대한 인지도를 높이기 위한 'Think Before You Link' 앱을 공개[70]

- 영국 정보기관 MI5은 약 1만 명의 영국 국민이 링크드인이나 페이스북에서 해외 첩보요원의 표적이 되는 것을 발견

  ※ 초기에 덜 민감한 정보를 요청하며 접근하며 관계 형성 시도

- 'Think Before You Link' 앱의 주요 사용자는 공무원이나 기밀정보를 다루는 산·학계 관계자이며, 민감한 정보 유출·공유를 요청하는 소셜미디어 계정 탐지에 기여

  ※ 앱상에서 접근한 사람이 허위 계정을 활용했을 가능성이 있는지, 수상한 메시지를 보냈는지 등의 질문을 제시하며, 사용자 답변을 기반으로 접근자의 위험도를 진단

- 앞으로 딥페이크 기술을 비롯한 인공지능 기술이 활발하게 활용되면서 온라인 신원의 진위 여부를 구분하는 것이 더욱 어려워질 것으로 예상

---

68) CNN(2022.5.9.), Clearview AI agrees to restrict US sales of facial recognition mostly to law enforcement

69) Biometric Information Privacy Act의 약자이며, 미국 일리노이 주에서 기업이 생체정보를 수집·사용하기 전에 사람들의 동의를 받도록 한 법

70) BBC(2022.5.17.), New app to help spot online spies

NEWS 7 인도, 국가 데이터 및 분석 플랫폼 개시[71]

❍ 인도 국가개혁위원회 NITI Aayog[72]에서 국가 데이터·분석 플랫폼[73](NDAP)을 개시

- 정부 기관의 공공데이터 개방을 목표로 상호 정보교환이 가능한 플랫폼을 구축
- 사용자는 플랫폼에 접속하여 다운로드·병합할 수 있는 데이터 세트와 추가적 분석·시각화 도구 활용 가능

〈 인도 국가 데이터·분석 플랫폼(NDAP)의 주요 내용 〉

구 분	내용
배경 및 목적	• 데이터와 디지털 기술의 확산으로 경제·사회가 급격히 변화하며 정부 업무 수행에 영향 • 정부의 공공데이터 접근성 증진을 위해 사용자가 편리하게 상호작용할 수 있는 플랫폼을 구축
특징	• 정부, 학계, 언론, 시민사회, 민간부문 사용자들의 요구에 맞춰 사용 사례 기반 접근법을 사용 • 농업, 에너지·자원, 교통, 부동산, 금융, 건강, 관광, 과학기술, 커뮤니케이션, 산업 등과 관련된 데이터 세트 구비 • 사용자가 쉽게 서로 다른 데이터 세트를 함께 활용할 수 있도록 상호 운용성 보장 • 데이터 세트를 자유롭게 다운로드 또는 병합할 수 있으며, 분석 및 시각화 도구도 제공
기대효과	• 정부가 데이터를 기반으로 한 정책적 의사결정을 할 수 있도록 보조 • 데이터 생태계 성장에 기여

71) OpenGov(2022.5.16.), India Launches National Data and Analytics Platform

72) National Institution of Transforming India의 약자로, 인도 정부의 주요 씽크탱크로 국가 개발 방향성과 정책적 조언을 제공

73) National Data and Analytics Platform
홈페이지: https://ndap.niti.gov.in/

NEWS 8 프랑스, 디지털 ID 보증 서비스 법안 공포[74]

❍ 프랑스 마크롱 대통령이 디지털 ID 보증 서비스 법안[75]에 서명('22.4.26)

- 프랑스 시민들은 앞으로 디지털 ID를 통해 다양한 정부 서비스를 안전하게 접근 가능

  ※ 디지털 ID로 1,000개 이상의 공공·민간 서비스 이용할 수 있는 FraceConnect 플랫폼[76] 접속해 활용

- 디지털 ID 보증 서비스(SGIN)는 프랑스 정부가 개발한 모바일 앱을 통해 제공될 예정

  ※ 근거리 무선 통신(NFC)을 지원하는 휴대폰에 물리적 신분증을 스캔하여 디지털 신분증으로 저장이 가능

- 인증받은 전자 신분증 사본 전송, 타 신분증 없이 연령대 확인 등의 기능도 제공 예정

❍ 프랑스 정부의 디지털 ID 보증 서비스 법안은 EU 집행위원회는 디지털 ID 도입 가이드라인[77]을 준수하기 위한 노력으로 파악되며, 유럽 주요국 전반에 디지털 ID에 대한 지원 확산 예상

- 룩셈부르크 정부는 2022년 4월에 모바일 ID 앱 'GouvID'를 개시하며 전자정부 포털[78]에 대한 안전하고 편리한 접근성을 제공

❍ 프랑스 극보수층은 디지털 ID가 사회적 감시를 조장한다는 비판 제기

※ 캐나다, 호주 등의 주요국 보수층도 유사한 비판 표현

- 디지털 ID 도입이 사회 신용 시스템의 기반을 제공함으로써 궁극적으로 국민 감시를 위해 활용될 수 있다는 우려가 제기되며 법안이 거센 반발에 부딪히고 있는 상황
- 프랑스 정부는 시민이 디지털 ID 보증 서비스(SGIN)에 의무적으로 참여할 필요가 없으며 자발적으로 참여하는 사람들에게 제공된다는 점을 강조

---

74) Mobile ID World(2022.5.3.), French President Signs New Digital ID Bill

75) Digital Identity Guarantee Service(SGIN) Degree
참고자료: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045667825

76) https://franceconnect.gouv.fr/

77) European Digital Identity Framework
참고자료: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

78) MyGuichet.lu
참고자료: https://guichet.public.lu/en/citoyens.html

NEWS 9 캐나다, 디지털 ID 활성화를 위한 국가디지털전략 개정 방안 검토[79)]

❍ 캐나다 정부가 디지털 ID에 중점을 둔 국가디지털전략* 개정 방안을 검토 중

* 2021년 6월에 수립된 캐나다 디지털 정부 전략(Digital Government Strategy)은 ▲주요 IT 시스템 교체·구축·관리 방식 첨단화, ▲언제 어디서나 제공 가능한 서비스, ▲부처 간 조율에 의한 디지털 운영, ▲제도 장벽 해소와 업무 혁신의 4개 영역으로 구성

❍ 앞으로 캐나다의 각 주·준주와 협력하여 디지털 ID 3계층(layers)에 대한 실행가능한 계획을 수립 예정

① 46개의 분산된 연방정부 서비스를 공통 단일 플랫폼으로 통합

② 데이터 관리 규칙을 설정하기 위한 '범캐나다 신뢰 프레임워크' 개발

③ 공공 부문 전반에 걸친 디지털 ID 호환성 확보를 위한 통합 계층 개발

※ 주·준주 디지털 ID로 모든 정부 서비스를 이용할 수 있고, 모든 서비스가 하나의 플랫폼으로 연동되도록 목표

❍ 캐나다는 연방정부가 제공하는 국가 디지털 ID가 없으며, 주 정부가 주축으로 디지털 ID 서비스를 제공 또는 개발하려 준비 중

〈 캐나다 주 정부의 디지털 ID 서비스 현황 〉

주(州)	주요 내용
온타리오주	• 올해 예정된 디지털 ID 출시 계획은 별도의 기한 없이 연기 • 온타리오주는 디지털 ID로 정부 자원·서비스 접근성 제고, 은행계좌 개설 등을 위한 신원 확인을 지원 예정
퀘벡주	• 2025년까지 건강보험증, 운전면허증, 출생증명서, 자동차보험 증빙서류* 등을 포괄한 디지털 ID 시스템을 개발·제공할 계획 * 민간기업이 발급한 서류도 디지털 ID 시스템에 포함될 수 있도록 지원 예정
브리티시 컬럼비아주	• 2002년부터 'BCeID' 디지털 ID를 운영 • 시민은 BCeID을 활용해 모든 주 정부 서비스에 접근 가능
앨버타주	• 2021년 1월부터 'My Alberta Digital ID' 서비스 제공 • 온라인상 신분 확인, 정부 서비스에 대한 접근성 제공 등에 활용 가능

79) Biometric Update(2022.5.19.), Canadian CIO outlines strategy with digital ID focus