AI와 사회적 감지 기반의 재난 정보 공유 체계 구축을 위한 데이터 윤리

장 요 한*

Abstract

AI와 사회적 감지(Social Sensing) 기반 재난 정보 공유 체계는 재난 대응의 속도와 정밀도를 높일 수 있으나, 예측의 정확도만으로는 그 효용성을 정당화하기 어렵다. 특히, 민원이나 제보 등은 개인의 경험과 맥락에 기반한 신호로, 원문 그대로 다루면 프라이버시(Privacy)와 활용 제한 문제가 커지고, 지나치게 단순화하면 품질과 대표성의 문제가 발생한다. 따라서 핵심은 민원을 "원문"이 아닌 "신호"로 변환 및 집계하여 활용하고, 평시와 위기 단계에 따라 범위를 확장 및 종료하는 운영 규칙을 마련하는 데 있다. 또한 민관 결합 환경에서는 역할과 책임, 데이터의 접근권한, 기록·감사 체계 등을 문서로 규정하고, 실시간성 요구와 절차의 충돌을 줄이는 규칙 기반 프로토콜(Rule-based Protocol)을 구축할 필요가 있다. 결국 데이터 윤리(Data Ethics)는 대응을 늦추는 장치가 아니라, 빠른 대응이 신뢰를 잃지 않도록 하는 최소 운영 조건이다. 본 원고는 이러한 맥락을 바탕으로 AI와 사회적 감지 기반의 재난 정보 공유 체계 구축을 위해 살펴보아야 할 요소들을 데이터 윤리의 관점에서 논하였다.

I. 서 론

“오늘 당신이 사용하는 AI가 당신이 평생 사용할 AI 중 최악의 모델임을 기억하라[1]”「듀얼 브레인(Co-Intelligence)」으로 널리 알려진 이선 몰릭(Ethan Mollick)의 저서에 있는 문장이다. 만약, 생성형 인공지능(Artificial Intelligence, AI)이 대중화되기 이전인 2019년 무렵에 우리가 이러한 문구를 접했다면 다소 과장처럼 느껴졌을 수 있다. 하지만, 각종 AI

* 국토연구원 국토인프라·공간정보연구본부 부연구위원, ycanns@krihs.re.kr

1) 원문: Whatever AI you are using right now is going to be the worst AI you will ever use(Ethan Mollick, 2024)

관련 서비스들이 봇물 터지듯 쏟아지는 요즘에는 AI의 발전 속도가 우리의 체화 속도를 이미 벗어나고 있음을 깨닫는다. 우리가 PC나 휴대전화 따위에 견주어 기억하는 AI – 이를테면 점진적으로 축적되고 시기에 따라 업그레이드되는 기계 – 가 이제는 그 틀을 완전히 벗어나 상시적인 업그레이드 사이클로 고도화되기 시작했다.

이러한 전환은 특히 에이전트형(Agentic) AI의 부상을 통해 선명하게 확인된다. 실지로 지난 2025년 11월 공개된 오픈소스 자율형 AI 에이전트인 오픈클로(OpenClaw)[2)3)4)]는 사용자가 명시적으로 지시하지 않은 오래된 온라인상의 이메일이나 온오프라인 파일 정리, 사용자에게 시기적으로 필요한 뉴스 및 영상 콘텐츠의 선별 및 취합, 이메일 답장 등 구체적 작업을 스스로 계획하고 실행하는 등 자율적 워크플로우(Workflow) 능력으로 세상을 놀라게 했다. 이는 AI의 능력이 챗지피티(ChatGPT)로 기억되는 기존의 응답 생성 중심의 도구 기능에서 벗어나, 실제 시스템과 데이터에 접속해 일련의 의사결정 과정을 통해 과업을 통제하는 실행 주체로 변화하고 있음을 시사한다.

실행 주체로서의 AI는 필연적으로 더 넓은 데이터 접근 범위와 더 강한 실행 권한을 전제한다 해도 과언이 아니다. 결국, 핵심 쟁점은 "무엇을, 어느 수준까지, 어떤 근거로 수집·처리·공유할 것인가"라는 AI 데이터 윤리(AI Data Ethics)와 데이터 거버넌스(Data Governance)로 수렴하게 된다. 우리의 일상에서 AI의 발전을 감탄하는 과정에서는 이 쟁점은 유의미하게 다가오지 않을 수 있다. 하지만, 개인 환경을 넘어 재난 예측과 대응, 감염병 확산 분석, 기후 위험 조기경보 등 공공 안전 영역에서 긴급성과 사회적 파급효과를 수반하게 될 때 신중함을 요구하게 된다. 더 나아가 재난 상황에서 관련 정보 공유는 공공데이터뿐만 아니라 기관과 민관 간 데이터의 결합 및 실시간 공유 등이 필수적으로 요구되는 경우가 많기 때문에, 통신 기반 위치정보, 소셜 미디어 정보, 교통 및 의료 등 이질적 데이터가 통합 및 분석되는 과정에서 이를테면 프라이버시 보호와 책임성 및 투명성 등과 충돌 가능성이 구조적으로 커지게 마련이다.

그렇다면 재난 대응이라는 공공적 맥락에서 개인정보나 민감정보의 공유는 어떤 조건에서 어느 범위까지 정당화될 수 있을까? 예측 정확도 제고를 위한 데이터 확장의 필요성과 프라이버시 보호 간의 다양한 상충관계(Trade-Off)는 어떤 기준과 절차로 조정되어야 할

2) 오픈클로 깃허브 웹페이지(https://github.com/openclaw/openclaw, 2026년 2월 20일 접속)

3) 오픈클로 공식 웹페이지(https://openclaw.ai/, 2026년 2월 20일 접속)

4) 오픈클로는 대규모 언어모델(Large Language Model, LLM)로 동작하는 개인형 AI 에이전트로, 사용자의 개인 PC나 클라우드 환경에 설치한 뒤, 텔레그램(Telegram) 등의 개인용 메신저를 통해 대화하며 인터넷 검색, 이메일 관리, 파일 정리 등의 작업을 수행한다(저자 각주).

까? 또한 이러한 기준을 단순히 논의 수준에 머물지 않고 권한 설계에서부터 접근 통제, 책임 소재 등 운영 가능한 규칙으로 전환하기 위한 거버넌스 아키텍처는 어떻게 구성되어야 하는 것일까? 나아가 민원이나 신고와 같은 사회적 감지(Social Sensing) 신호를 재난 대응에 활용할 때, 이를 "신호"로 변환 및 집계하여 활용하는 기준은 어떻게 설정되어야 하는가?

본 원고는 이러한 문제의식에서 출발한다. 특히 센서 기반 관측의 공백을 메우기 위해 신고나 민원과 같은 사회적 감지 신호가 재난 정보 공유 체계에 포함되는 상황에서는, 데이터의 활용이 기술적 가능성만이 아니라 정당성의 조건과 통제 방식 자체를 함께 묻게 된다. 이에 공공 안전을 위해 AI를 활용하는 재난 정보 공유 체계에서 요구되는 데이터 윤리의 개념과 원칙을 정립하고, 국내외 사례 분석을 통해 정책적 쟁점을 도출한다. 이를 바탕으로 한국형 재난 AI 데이터 거버넌스 모델의 설계 방향과 정책 옵션을 제시하고자 한다. 나아가 2장에서는 AI 데이터 윤리의 개념과 원칙 및 관련 규범을 정리하고, 3장에서는 재난 정보 공유 체계의 현황과 과제를 진단한다. 4장에서는 국내외 사례를 비교 분석하며, 5장에서는 정책적 쟁점과 개선 방향을 도출한 뒤, 6장에서 결론 및 정책 제언을 제시한다. 특히 국내 주요 사례로 민원 데이터를 사회적 감지(Social Sensing)로 활용한 사례인 「AI 기반 재해 초단기 예측을 위한 나우캐스트 연구: 방법론 정립을 중심으로」를 중심축으로 삼아, 민원 기반 사회적 감지 데이터의 활용 가능성과 개인정보 보호와 데이터 연계 거버넌스의 설계 요건 등을 검토한다.

Ⅱ. AI 데이터 윤리의 개념과 원칙

AI를 활용한 재난 대응은 단순히 "모델 성능"만으로 정당화될 수 없다. 특히 재난 예측이 경보나 대응 같은 의사결정과 맞물리는 순간, AI는 단순 분석 도구를 넘어 공공 안전을 좌우하는 일종의 운영 인프라(Operational Infrastructure)로 작동하게 된다. 때문에, 이때부터 데이터 처리와 공유의 정당성, 책무성 등은 더 이상 "있으면 좋은 조건"이 아니라 시스템 신뢰를 좌우하는 핵심 성과지표(Key Performance Indicators, KPIs)에 가까워진다.

(1) AI 기반의 재난 정보 공유와 데이터 윤리

통상적으로 우리가 이해하고 있는 AI의 구동 원리는 과거로부터 방대한 양의 데이터를

학습하여 모호한 현상이나 가까운 미래 예측에 대해 가장 근사한 답을 유추해 내는 것 정도로 이해되고 있다. 때문에, 많은 데이터가 학습될수록 AI의 예측력 또한 더욱 좋아질 것이라는 기대가 자연스럽게 뒤따른다. 이러한 이해 방식이 AI를 이용한 재난 대응에도 크게 다르지 않게 적용되어, 가능한 데이터가 많을수록 공공의 안전을 위한 각종 예측이 정교해질 것이라는 기대가 자연스럽게 수반된다. 하지만 AI의 활용 이전에, 재난 상황에서 공유되는 다양한 공공 및 민간 데이터는 단순한 정보의 공유 수준을 넘어 하나의 행위가 될 수 있다는 점을 염두에 두어야 한다. 즉, 누구의 데이터를 어떤 근거로 수집하고, 어떤 방식으로 결합하며, 어디까지 공공에 또는 차등적으로 공유할 것인지가 곧 시민의 일상과 권리에 직결되기 때문이다. 더구나 예측이 경보나 순차적 대응 프로토콜 등으로 이어지는 순간, AI를 위한 데이터 활용은 단순한 시뮬레이션 수준을 넘어 공공서비스의 일부가 되고, 그 결과에 대해서도 사회적 책임이 필요하다.

그림 1 스트라바(Strava) 히트맵 사건

(a) (b)

주: (a) 아프가니스탄(Afghanistan) 군 부대 주변 조깅 히트맵; (b) 미국 해군부대 기지 중 하나인 Area-51 주변의 사이클링 코스 히트맵

자료: 스트라바 히트맵 자료를 The Guardian에서 재인용

특히 다른 데이터와 결합하면 의도하지 않았던 정보까지 노출될 수 있는, 이를테면 위치 정보나 민원 정보처럼, 맥락이 풍부한 데이터는 시간과 정황과 같은 정보와 결합되는 순간부터 원래 의도하지 않은 정보까지 드러낼 수 있다. 실지로 지난 2018년 발생한 스트라바(Strava) 보안 유출 사건[5]에서, GPS 기반 운동 기록 앱인 스트라바가 전 세계 사용자의 운동 경로 10억 개(약 3조 개의 GPS 좌표)를 시각화한 "글로벌 히트맵"을 공개한 바 있다.

물론 개별 사용자의 이름의 삭제된 비식별·집계(Aggregated) 데이터였고, 전 세계에서 가장 인기 있는 러닝과 사이클링 코스를 보여주며 사용자들에게 동기를 부여하려는 목적이었으나, 문제는 군사 기지 근처에서 군인들이 조깅하며 남긴 GPS 데이터가 히트맵으로 공개되어, 기지 내의 이동 경로, 경비 초소 위치, 기지 내부 구조가 의도치 않게 전 세계에 노출된 사례가 있다. 이런 환경에서는 "정확도를 높이기 위한" 목표가 "데이터를 어디까지 수집하고 활용해도 되는가"라는 질문과 충돌하게 된다. 결국 재난 정보 공유에서 데이터 윤리는, 기술의 가능성을 부정하려는 장치라기 보다는 "필요한 만큼만, 납득할 수 있는 방식으로" 활용하기 위한 최소한의 안전장치에 가깝다.

(2) 데이터 윤리와 AI 윤리

데이터 윤리(Data Ethics)는 간단하게 말하자면, 데이터를 다루는 전 과정에서 "무엇이 정당한가"를 묻는 규범 체계라 할 수 있다(Ekmekci et al., 2025). 기존의 데이터 활용 과정에서 주요 논의가 "무엇이 맞고 논리적인가"에 그 무게를 두었다면, 데이터 윤리에서 주요 논의는 "그렇게 해도 윤리적으로 문제가 되지 않는가"를 함께 고려해야 한다는 점이 구별되는 부분이다. 물론 데이터 활용 과정에서 법적 준수(Compliance)는 중요한 출발점이지만, 데이터의 활용 경험이 부족하거나 새로운 경우에는, 법을 통해 모든 상황을 미리 규정하기란 여간 쉽지 않다. 때문에, 데이터 윤리는 사회적 수용성과 권리 보호, 공정성, 책임 배분까지 포함하는 더 넓은 판단 기준으로 확장될 필요가 있다(NIST, 2022; 류현숙, 2025).

한편, AI 윤리(AI Ethics)는 AI가 만들어내는 사회와 경제, 그리고 안전 리스크 전반을 포괄할 수 있다(Pappu, 2024). 그중에서도 AI에 필수적으로 사용되는 데이터는 완성도 높은 AI의 출발점이자 연료이기 때문에, 데이터 윤리는 AI 윤리의 핵심 하위 축으로 기능한다 해도 과언이 아니다(NIST, 2022; Pappu, 2024). 재난 대응에서는 이 관계가 더욱 선명해지는데, 예측 결과가 경보 발령이나 자원 배분, 대피 안내처럼 사람과 재원의 실행으로 이어지는 순간, 핵심 쟁점은 "모델의 옳고 그름"만이 아니라 프로토콜 즉, "어떤 데이터가 어떤 방식과 권한 아래에서 생산되고 실행되는가"로 이동하게 된다(Wood, 2025; 류현숙, 2025). 이때 데이터 윤리는 권한과 책임 및 통제를 포괄하는 거버넌스 설계의 출발점이 된다.

---

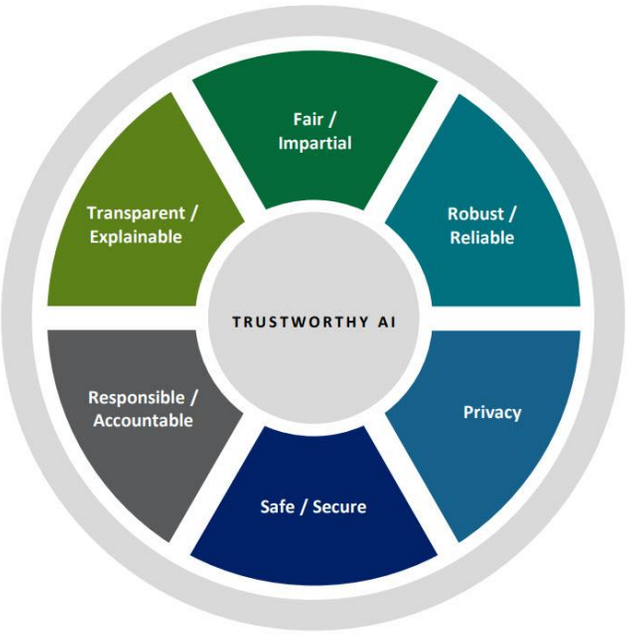
5) The Guardian, 「Fitness tracking app Strava gives away location of secret US army bases」, 2018. 1. 28. (https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, 2026년 2월 20일 접속)

(3) 재난 정보 공유를 위한 핵심 원칙

국제적으로는 OECD의 AI 원칙, UNESCO 권고, NIST의 AI 위험관리 프레임워크(Risk Management Framework, RMF) 등에서 공통적으로 "신뢰할 수 있는 AI(Trustworthy AI)"를 만들기 위한 기준을 제시해 왔다(Ekmekci et al., 2025; NIST, 2023; OECD, 2019; Pappu, 2024). 각 표현과 강조점은 조금씩 다르지만, 재난 정보 공유 체계라는 관점에서 메시지는 비교적 분명하게 수렴된다. 즉, 데이터가 커지고, 그 결과가 현실의 경보와 대응으로 이어질수록, 단순히 성능만으로는 사회적 정당성을 확보하기 어렵다는 점이다. 이를 재난 정보 공유 체계에 적용 가능한 원칙으로 정리하면 다음 여섯 가지로 압축된다.

첫 번째로, 투명성(Transparency, 또는 설명가능성 Explainability)은 "무엇을 왜 쓰는지"와 "결과를 어떻게 이해해야 하는지"를 설명할 수 있어야 한다는 요구라 할 수 있다(NIST, 2023; OECD, 2019). 시민에게는 어떤 정보가 누구에게 어떤 목적을 위해 쓰이는지, 어디까지 활용되는지가 이해할 수 있는 논리로 제시되어야 한다(Pappu, 2024; Wood, 2025). 한편, 현장의 의사결정자에게는 예측의 불확실성과 오류 가능성이 함께 전달되어야 한다. 설명이 부족한 예측은 맹목적으로 과신하게 되거나, 반대로 신뢰를 잃을 수 있어, 어느 쪽이든 재난 대응에서는 위험하다(NIST, 2023; Wood, 2025).

그림 2 신뢰할 수 있는 AI(Trustworthy AI) 개념도 예시



자료: 캘리포니아 주립대학교 샌프란시스코 웹페이지(https://ai.ucsf.edu/trustworthy, 2026년 2월 20일 접속)

둘째로, 책임성(Accountability, 또는 추적가능성 Traceability)은 문제가 생겼을 때 원인을 되짚고 개선할 수 있는 구조가 있어야 한다는 원칙이다(OECD, 2019; Pappu, 2024). 어떤 데이터가 어떤 경로로 결합하였고, 어떤 근거로 일련의 판단이 이루어졌는지 그 과정을 추적할 수 있어야 한다(OECD, 2019). 특히, 복수 이상의 기관이 결합하여 다수의 정보가 혼재하는 환경에서는 명확한 책임이 모호해지는 순간 오류가 반복되기 쉽다. 책임성은 "누구 탓인가"를 가리기 위한 장치라기보다, "어떻게 고칠 것인가"를 가능하게 하는 설계 조건에 가깝다(NIST, 2023; 류현숙, 2025).

셋째로, 공정성(Fairness, 또는 비차별 Non-Discrimination)은 AI가 특정 집단이나 지역에 불리하거나 유리하게 작동하지 않도록 편향을 관리해야 한다는 원칙이다(NIST, 2023; OECD, 2019). 재난 대응에서 공정성은 결국 "누구에게 이 예측 결과가 집중되는가"라는 질문으로 구체화된다. 데이터가 풍부한 곳은 더 정교해지고, 반대로 데이터가 부족한 곳은 투박해지는 경향이 생길 수 있는데, 이 격차가 재난 위기 상황에서는 결국 경보와 자원 배분의 격차로 이어질 수 있다(Wood, 2025). 특히 민원이나 주민 신고처럼 사람의 행동이 수반되는 데이터는 사회적 조건의 차이를 반영하기 때문에, 상황에 따라서는 취약지역 및 취약계층을 기준으로 성능과 영향을 점검하는 방식이 필요하다(NIST, 2022; 장요한 외, 2024; 장요한 외, 2025; Wood, 2025; Yuan et al., 2025).

넷째로, 프라이버시(Privacy, 또는 데이터 보호 Data Protection)는 개인(및 민감정보)의 식별 및 추적 위험을 낮추고 목적 외 이용을 통제해야 한다는 원칙이다(NIST, 2023; Pappu, 2024). 재난이라는 공익 목적이 존재하더라도, 그것이 무제한 수집의 근거가 될 수는 없다(Ekmekci et al., 2025; 장요한 외, 2024). 앞서 언급한 사례처럼 위치정보나 의료정보, 민원 텍스트처럼 맥락이 풍부한 데이터는 결합과 추론을 통해 재식별 위험이 커질 수 있다(Pati et al., 2024; Yuan et al., 2025). 결국 "정말 필요한 범위와 기간"을 먼저 정하고, 접근과 활용을 통제하며, 그 과정이 기록으로 남도록 관리하는 방식이 핵심이 된다(OECD, 2019; Wood, 2025).

다섯 번째로, 안전·보안(Safety & Security, 또는 견고성 Robustness)은 오류나 공격, 환경 변화에서도 시스템이 안정적으로 작동해야 한다는 원칙이다(NIST, 2023; OECD, 2019). 특히 재난 상황에서는 센서 고장과 통신 불안정, 그리고 그에 따른 데이터 결측과 같은 문제들이 동시 다발적으로 발생할 수 있고, 때에 따라서는 허위 정보나 조작 정보가 유입될 가능성도 커진다(Yuan et al., 2025; 류현숙, 2025). 이런 환경에서 모델이 취약하면 경보 체계 전체로 전이될 공산이 높으며, 그 비용은 결국 행정비용으로 남게 된다. 때문

에 데이터 무결성, 품질 관리, 이상 징후 대응은 기술적 과제이면서 동시에 윤리적 과제가 될 수 있다.

마지막으로, 공익성(Public Interest, 또는 목적 적합성 Purpose Fit)은 재난 데이터 활용의 공익적 정당성이 크더라도 그것이 면죄부가 되지 않는다는 점을 분명히 한다는 원칙이다(Ekmekci et al., 2025). 재난 대응을 명분으로 모인 데이터는 그 목적이 조금만 확장되거나 모호하게 해석해도 치안 단속이나 상업적 활용으로 오용될 수 있고, 이는 시스템 신뢰의 실패로 이어질 수 있다(류현숙, 2025). 결국 목적 적합성은 "재난 예측과 대응에 필요한가"라는 질문을 반복해서 던지게 만들고, 목적이 바뀌는 순간을 엄격히 다루도록 요구한다(OECD, 2019; Ekmekci et al., 2025).

(4) 통제와 개인정보 보호 기술(Privacy-Enhancing Technologies, PETs)

재난 정보 공유 체계에서 원칙은 스스로 실행되지 않는다. 때문에 원칙을 운영 요건(Requirements)으로 구체화하고, 이를 제도·프로세스·기술 통제(Controls)로 내재화하는 과정이 필요하다(NIST, 2022; NIST, 2023; OECD, 2019). 예를 들면, "최소 수집"은 수집 항목을 줄이자는 의미라기 보다는, 수집 단계에서 필요성과 대체가능성, 비례성 등을 점검하고 그 목적이 바뀌면 처음부터 재심사하는 규칙 등으로 정착되어야 함을 의미한다고 할 수 있다(NIST, 2023). "책임성" 역시 단순히 책임자를 지정하는 데서 멈추지 않고, 데이터 접근 기록과 모델 변경 이력, 검증 자료와 관련 의사결정 근거 등을 남겨 사후 점검이 가능하게 만드는 구조로 이어져야 함을 의미하고(NIST, 2022; OECD, 2019), "투명성"도 단순 공개가 아니라, 무엇을 언제 어떤 방식으로 알릴지의 기준을 정하고, 설명이 가능한 문서화와 기록을 운영 습관으로 만드는 데서 힘을 얻는다(NIST, 2022; NIST, 2023).

이 과정에서 개인정보 보호 기술(Privacy-Enhancing Technologies, PETs)은 프라이버시를 사후 대응이 아니라 사전 단계인 설계 요건으로 앞당기는 수단이라 할 수 있다(NIST, 2023). PETs는 "데이터를 덜 수집하는 것"과 "필요한 데이터를 안전하게 활용하는 것"을 동시에 달성하기 위한 정책적·기술적 지렛대로 이해할 수 있다.

(5) 국내외 규범 및 표준

국내외 규범과 표준은 대체로 원칙(Principles)-의무(Obligations)-구현(Implementation Tools)의 3층 구조로 이해할 수 있다(NIST, 2023; OECD, 2019). OECD와 UNESCO는 신뢰할 수 있는 AI를 위한 가치와 원칙을 제시하며 정책 설계의 준거를(Ekmekci et al.,

2025; OECD, 2019; 이상욱, 2021), GDPR과 EU AI Act는 데이터 처리 원칙과 위험 기반 규제 체계를 통해 준수해야 할 의무를 구체화하며(European Parliament, 2025; Truong et al., 2021), NIST AI RMF와 ISO/IEC 계열 표준은 조직이 위험을 식별하고 관리하며 지속적으로 개선하기 위한 절차와 운영 틀을 제공한다(NIST, 2023).

한국의 맥락에서는 개인정보보호법과 가명정보 관련 지침, 재난 및 안전관리 기본법 체계, 그리고 AI 관련 기본법·윤리 기준 등이 함께 작동한다. 중요한 것은 어느 하나의 문서만으로 답을 찾기 어렵다는 사실이다(류현숙, 2025). 재난 정보 공유는 긴급성과 공익성, 데이터 결합, 의사결정으로 연결 등의 특성을 동시에 갖기 때문에, 원칙-의무-구현을 일관되게 묶어 운영 규칙과 통제 장치로 전환할 때 비로소 지속 가능해진다(Ekmekci et al., 2025; 류현숙, 2025).

Ⅲ. 재난 정보 공유 체계의 현황과 과제

재난이 발생하면 시민이 마주하는 정보는 휴대전화 재난문자, 방송 자막, 지자체 안내 등 대체로 한 줄의 짤막한 경보로 요약된다. 하지만, 그 한 줄이 만들어지기까지는 관측과 신고, 행정과 민간의 데이터가 서로 다른 속도와 형태로 뒤섞이고, 기관 간 판단과 책임이 다양하게 겹치는 경로를 거치게 된다(Ekmekci et al., 2025; Ise et al., 2022). 재난 정보 공유 체계가 어렵게 느껴지는 까닭은, 단지 데이터 부족이나 결핍에서 기인한 현상이 아니다. 데이터가 모이고 결합되는 방식 자체가 복잡하며, 재난이라는 시간 압박 속에서는 그 복잡함이 그대로 운영상의 과제로 남게 되기 때문이다.

(1) 재난 정보가 만들어지는 경로

국내 재난 정보는 하나의 통로에서 일괄적으로 생산되지 않는다. 대체로 관측 및 감시 데이터, 신고 및 민원 데이터, 행정 및 인프라 데이터, 그리고 민간 운영 데이터가 각각의 경로에서 모이고, 상황에 따라 필요한 방식으로 가공 및 결합되어 경보와 대응 판단으로 이어진다(Ise et al., 2022; 장요한 외, 2025).

관측 및 감시 데이터는 기상, 지진, 산불 등 센서 기반 데이터로, 비교적 표준화된 형식을 갖고 시계열에 따라 축적된다(Ise et al., 2022). 그러나 관측망이 촘촘하지 못한 영역에서는 공백이 생기고, 싱크홀이나 산불처럼 변화가 빠른 긴급상황에서는 관측 주기 사이

의 공백이 곧 "정보의 공백"으로 드러나기 쉽다(장요한 외, 2025). 119 등 신고, 주민 제보, 민원, 현장 보고 등 데이터는 이러한 공백을 메우는 신호가 될 수 있다. 다만 신고는 본질적으로 사람의 행동과 판단이 섞인 데이터이기 때문에, 중복이나 과장, 시간차 오류 등이 복합적으로 발생할 수 있고, 지역과 계층에 따라 제보 양상 자체가 달라질 수도 있다(장요한 외, 2024; 장요한 외, 2025). 그럼에도 불구하고 재난 대응에서는 현장의 변화를 빠르게 감지해야 하므로, 이 신호를 완전히 배제하기 어렵다.

한편 인구 분포, 취약계층 현황, 대피시설 위치, 의료·교통·기반시설 정보 등 행정 및 인프라 데이터는 예측 결과를 "실제 대응"으로 연결하는 데 결정적인 자료 역할을 한다(Ise et al., 2022; Wood, 2025). 같은 위험 신호라도 어디에 먼저 자원을 투입할지, 대피를 어디로 안내할지 같은 결정은 결국 이 행정 및 인프라 데이터에 기대게 된다. 문제는 이 데이터가 지역과 항목에 따라 기관별로 관리되고, 갱신 주기와 형식이 달라 재난 상황처럼 일촉을 다투는 국면에서는 즉각적인 결합을 기대하기 어렵다는 점이다(Ise et al., 2022; WHO, 2022). 이 때문에 현장에서는 "당장 파악이 가능한 데이터"나 "의사결정 그룹의 경험" 위주로 판단이 기울어지기 쉬운데, 그 과정에서 취약지역이나 취약계층이 차순위로 밀려날 위험도 함께 커진다.

마지막으로 통신이나 내비게이션 등과 같은 민간 운영 데이터는 "현재성(Real-Time)"의 특징이 강한 데이터라고 할 수 있다(WHO, 2022; 이승환, 2025). 재난은 시간 단위로 상황이 바뀌고, 실제 이동과 혼잡, 통제 구간, 우회 경로 같은 정보는 공공 인프라보다 민간 인프라가 상대적으로 빠르게 파악하는 경우가 많기 때문이다. 다만 이 데이터는 공공이 직접 생산하거나 관리하지 않는 만큼, 수집되는 형식과 범위가 제각각이고 계약이나 협약 조건에 따라 제공 수준과 범위가 달라질 수 있다(장요한 외, 2024; 장요한 외, 2025). 결과적으로 재난 정보는 하나의 데이터로부터 완벽한 성과물로 이어진다기보다, 서로 다른 이종(異種, Hybrid) 데이터가 "상황에 따라 가능한 방식"으로 결합되어 생성된 결과로 보는 편이 정확하다.

(2) 이종(異種, Hybrid) 데이터 결합

민관 데이터 결합은 대개 공공 데이터만으로 속도와 세밀함을 동시에 확보하기 어려운 지점에서 요구된다(장요한 외, 2025). 문제는 결합의 필요가 곧바로 결합의 방식으로 이어지지 않는다는 점이다. 실제 현장에서는 민간 데이터가 원천 데이터 형태로 제공되는 경우도 있지만, 처음부터 집계 지표 형태로 제공되거나, 일정 조건을 충족한 경우에만 제공되거

나, 분석 결과만 가공되어 전달되는 형태 등으로 제공되는 경우도 적지 않다(장요한 외, 2025). 어떤 방식이 선택되는지는 기술의 문제라기보다는 제공 조건과 위험 부담, 그리고 책임 경계 설정의 문제로 귀결된다(Pati et al., 2024; 장요한 외, 2025).

여기서 가장 자주 발생하는 이슈는 "실시간성"과 "절차"의 충돌이다(Ekmekci et al., 2025). 일촉을 다투는 재난 상황에서는 빠르게 판단해야 하는 압력이 높고, 자칫 늦어진 판단은 현실의 피해로 직결될 수 있다. 반면 민간 데이터는 제공 과정에서 목적과 범위, 보관, 재제공 등의 조건이 확인되어야 하고, 제공 형태가 바뀌면 해석 방식도 달라진다(Truong et al., 2021). 이때 경우의 수는 크게 두 방향으로 나뉜다. 하나는 위급한 상황에서 데이터 제공 조건에 대한 해석 범위를 넓히거나 관련 절차를 생략하는 방향이고, 다른 하나는 법적 절차를 지나치게 앞세워 현장 대응의 속도를 잃는 방향이다(Ekmekci et al., 2025). 어느 쪽이든 재난 정보 공유 체계에서는 비용이 발생한다.

또 다른 어려움은 "신호의 성격"에서 비롯된다. 민원이나 제보 등은 수집되는 신호가 그 자체로 직관적인 현상을 의미하지 않을 수 있다(장요한 외, 2024; 장요한 외, 2025). 현장의 이상 징후를 빠르게 반영할 수 있는 장점이 있는 반면, 허위 정보나 과장된 신호가 섞이거나 특정 지역이나 주제의 목소리만 과대 반영될 가능성도 있다[6]. 따라서 민관 데이터 결합은 단순히 많은 데이터를 확보하는 문제가 아니라, 확보된 데이터를 어디까지 신뢰하고 어떤 적법 절차 및 방식으로 판단에 반영할지까지 포함한 운영 문제로 이해될 필요가 있다.

(3) 의사결정을 위한 데이터 품질과 책임의 간격

재난 상황에서 실시간으로 유입되는 데이터는 대체로 온전하지 않거나 시차가 발생하는 등 불완전한 경우가 많다(WHO, 2022). 데이터에 결측이 발생하고, 동일 사건에 대해서도 여러 경로로 중복되어 취합되며, 시각과 위치(국내의 경우 서로 다른 GIS 좌표계가 혼재하는 경우)도 어긋나기 쉽다. 특히 현장의 신고나 민원 데이터는 문장 형태로 기록되어 같은 현상을 서로 다른 언어로 기술하는 일이 비일비재(非一非再)하다(장요한 외, 2024; 장요한 외, 2025). 이때 문제가 되는 것은 "완벽한 데이터를 확보하지 못했다"는 사실 자체보다, 불완전함을 전제로 한 의사결정이 어떤 근거 위에서 이루어졌는지를 남기기 어렵다는 점이다(Ekmekci et al., 2025; 류현숙, 2025).

---

6) 장요한 외(2025)는 민원 데이터를 활용한 싱크홀 이상 징후 검지의 활용 가능성을 제시한 바 있으나, 장요한 외(2024)는 반복 민원과 이첩 과정에서 민원의 구체성이 약화되거나 특정 주제의 목소리가 과대 해석될 수 있음을 지적한다.

책임 추적이 어려운 이유는 구조적이다[7]. 데이터는 여러 기관과 시스템을 거치며 가공되고, 판단은 상황실과 현장 지휘 체계, 협업 기관 사이에서 동시에 이루어진다(Ise et al., 2022; 류현숙, 2025). 이 과정에서 어떤 데이터가 어떤 형태로 결합되었는지, 어느 시점의 정보가 최종 판단에 반영되었는지, 판단의 근거가 무엇이었는지가 일관된 방식으로 남지 않으면 사후에는 "왜 그렇게 판단했는지"를 설명하기가 어렵다(Yuan et al., 2025; 류현숙, 2025). 설명이 어려우면 개선도 어렵고, 개선이 어렵다면 같은 문제가 반복될 가능성도 높아진다.

Ⅳ. 국내외 주요 적용 사례

재난 정보 공유 체계는 머리로 이해하는 것보다, 실제로 어떤 방식으로 운영되는지를 보고 나면 훨씬 선명해진다. 어떤 경우는 데이터 처리의 기준을 문서로 먼저 고정하고, 어떤 경우는 여러 기관이 같은 화면을 보도록 만드는 일에 집중하며, 또 어떤 경우에는 빠른 대응을 앞세운 나머지 불필요한 정보까지 함께 흘러가기도 한다(European Commission, 2026; Ise et al., 2022).

(1) 해외 사례

먼저 EU의 사례는 "재난 대응이라 해도 데이터 처리는 예외가 아니다"라는 점을 비교적 정돈된 형태로 보여준다. 예컨대 코페르니쿠스 긴급관리 서비스(Copernicus Emergency Management Service, CEMS)는 재난 대응을 지원하는 공공서비스이지만, 개인정보 처리에 대해서도 별도의 개인정보 명시(Privacy Statement)를 통해 처리 목적, 법적 근거, 보관 기간, 접근 권한, 권리 행사 창구 등을 문서로 제시한다(European Commission, 2026). 특히 이 문서는 접근 권한을 "필요한 사람만(Need to Know)"으로 제한한다는 점을 명시하고, 자동화된 의사결정(Automated Decision-Making)이나 프로파일링(Profiling)에 사용하지 않는다는 점도 분명히 하고 있다. 재난 대응이라는 공익 목적이 데이터 활용의 강한 동기가 되더라도, 운영 규칙과 책임 구조를 문서화하여 먼저 고정해 두지 않으면 이

7) 장요한 외(2025)에 따르면 전국에서 집계되는 각종 신고나 민원은 관할 지역이나 해당 공공기관으로 접수된 뒤, 데이터 소유권과 개인정보 이슈 등으로 인해 통합 집계 체계를 거치게 되는데, 그사이에 빈번한 민원 이첩(移牒)이나 반복 민원이 발생하면 의사결정 체계에 장애로 작동할 우려가 있다.

후의 논쟁은 “왜 그랬는지”가 아니라 “어디까지였는지”부터 다시 묻게 된다는 점에서, 이 사례의 의미는 간과할 수 없다(European Commission, 2026).

일본의 사례는 기술보다 “연결”이 중요하다는 사실을 강조한다(Ise et al., 2022). 대규모 재난은 영향을 받은 지역의 지방정부만으로 대응하기 어렵고, 중앙정부와 비피해 지역의 지원이 동시에 들어오는데, 이때 정보 공유가 원활하지 않으면 지원은 들어와도 효과적인 활동이 어렵다고 지적된다. 일본에서는 재난 정보 공유를 위한 플랫폼으로 SIP4D(Shared Information Platform for Disaster Management)가 논의·운영되어 왔고, 현장에서 공통 상황 인식(Common Operational Picture)을 만들기 위한 정보 파이프라인을 구축하려는 시도가 이어지고 있다. NIED는 SIP4D 개발과 함께 ISUT(Information Support Team)와 같은 현장 지원 체계를 언급하며, “현장에서 들어오는 정보”를 모아 공통 그림을 만드는 것이 재난 대응에서 중요하다고 설명한다(Ise et al., 2022). 결국 이 사례가 보여주는 핵심은, 데이터가 많아도 연결이 되지 않으면 공유가 성립하지 않고, 공유가 성립하지 않으면 협업은 기대만큼 작동하지 않는다는 점이다.

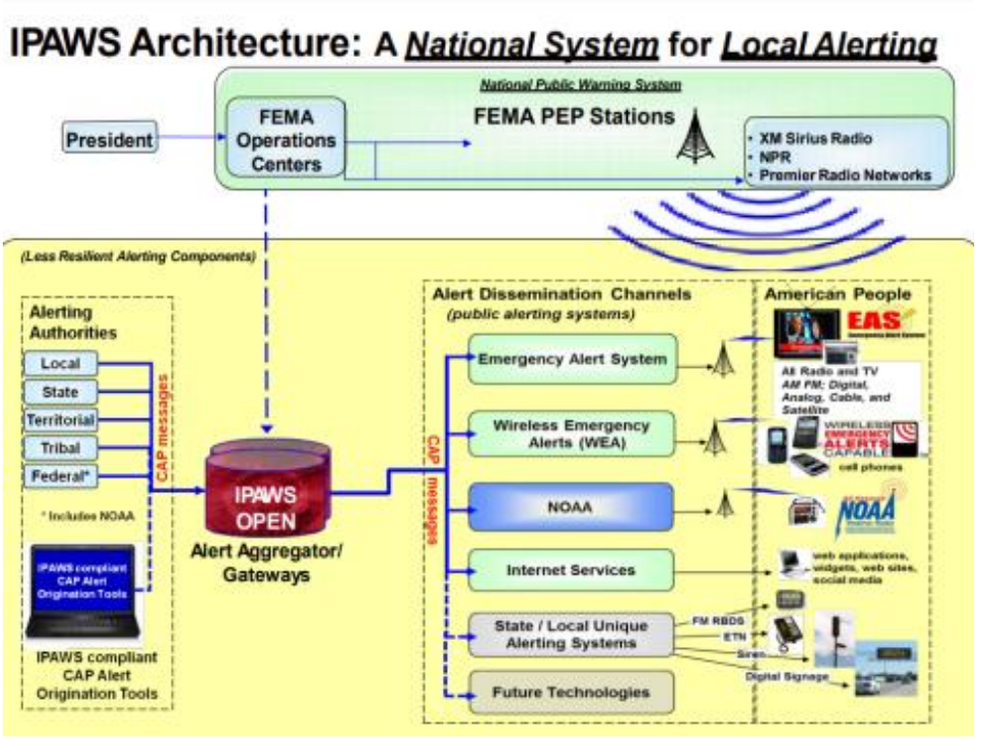
그림 3 일본의 SIP4D

자료: SIP4D 웹페이지(https://www.sip4d.jp/, 2026년 2월 20일 접속)

미국의 사례는 경보·전파 체계의 표준화가 무엇을 가능하게 하는지 보여주는 한편, “불필요한 데이터가 함께 흘러갈 때” 어떤 일이 벌어지는지도 동시에 보여준다. IPAWS(Integrated Public Alert and Warning System)처럼 경보를 다중 채널로 전달하는 체계에서는 메시지의 표준화가 중요한데, FEMA는 CAP(Common Alerting Protocol)과 IPAWS 프로파일을 채택해 경보 메시지의 교환·전달을 표준화하는 방향을 설명한다(FEMA, 2019; Peskin, 2026). 이는 재난 상황에서 경보를 더 빠르고 일관되게 전달하는 데 기여할 수 있다.

다만 재난 대응 과정에서 개인정보를 포함한 데이터가 개입되는 순간, 표준화만으로는 충분하지 않다. DHS OIG 보고서는 FEMA가 재난 생존자 지원 프로그램(Transitional Sheltering Assistance, TSA) 운영 과정에서 계약자에게 "필요 이상의 민감한 개인정보"를 제공했고, 그 결과 개인정보 보호 측면의 취약점이 발생했음을 지적한다. 재난 대응에서는 속도가 우선되기 쉽지만, 그 속도가 "데이터 범위의 관성적 확대"로 이어질 때 위험은 오히려 커진다는 점을 보여주는 사례다(DHS OIG, 2019; Ekmekci et al., 2025).

그림 4 미국의 IPAWS 아키텍처 예시



자료: Peskin(2026) p.7

(2) 국내 사례

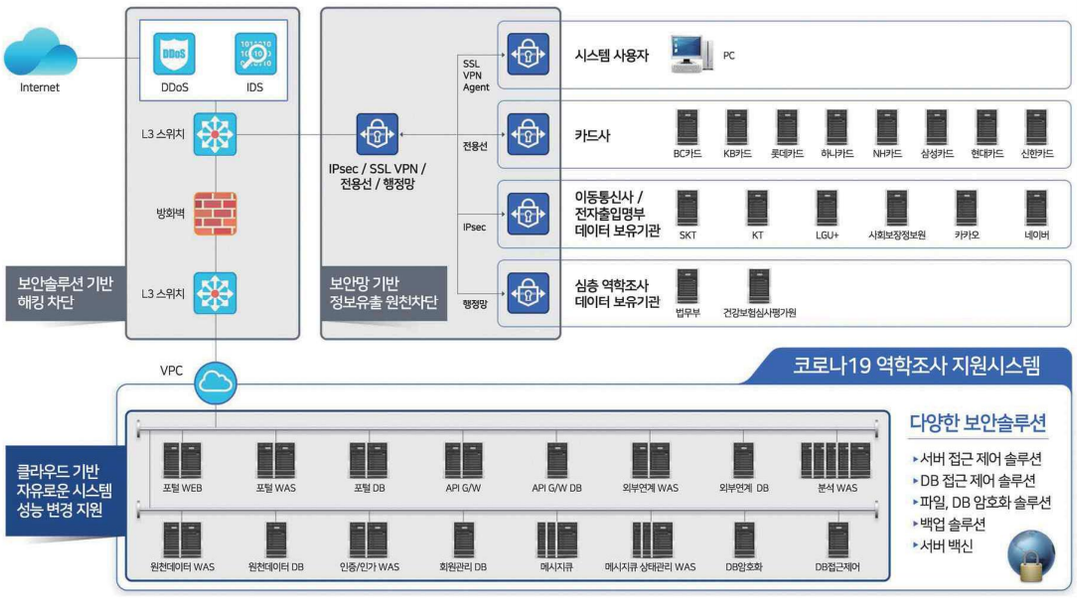
국내에서 데이터 활용의 정당성과 한계를 사회가 집단적으로 경험한 대표 사례는 코로나19 대응 과정이다(Jung et al., 2020). 특히 역학조사 지원 시스템(Epidemiological Investigation Support System, EISS)은 확진자 동선 파악과 접촉자 추적의 속도를 높이기 위해 도시 데이터 허브 등과 결합된 형태로 운영되었고, 관련 소개 자료에서는 역학조사 시간이 크게 단축되었다고 설명한다(국토교통과학진흥기술원, 2023; 질병관리청, 2022). "빠른 추적"이 공공 안전에 기여할 수 있다는 점은 분명했지만, 그 과정에서 위치정보, 카드

이용 내역, CCTV 등 민감한 정보의 활용 근거와 범위, 그리고 공개 방식은 곧바로 사회적 논쟁의 대상이 되었다(Jung et al., 2020; 질병관리청, 2022).

또한 실제 공개된 동선 정보가 개인의 일상과 사회적 관계를 추론 가능하게 만들 수 있다는 점을 분석한 연구는, 공익과 프라이버시가 단순히 추상적 원칙의 충돌이 아니라 "어떤 정보를 어디까지 공개했는가"라는 매우 구체적인 운영의 문제로 나타난다는 사실을 보여준다(Jung et al., 2020).

이 사례는 재난 정보 공유 체계에도 직접적인 시사점을 준다. 재난이 "긴급" 해질수록 데이터 활용의 범위가 넓어지기 쉽고, 그 과정에서 시민이 납득할 수 있는 설명의 언어는 오히려 빈약해지기 때문이다. 특히 법적 근거가 존재하더라도, 실제 운영에서 데이터가 어느 단계에서 어떤 단위로 사용되었는지, 공개는 어떤 기준으로 제한되었는지, 문제가 생겼을 때 어떤 방식으로 정정되었는지까지 설명되지 않으면, 신뢰는 결과보다 과정에서 먼저 흔들릴 수 있다(Ekmekci et al., 2025; Jung et al., 2020).

그림 5 한국의 EISS 인프라 구조



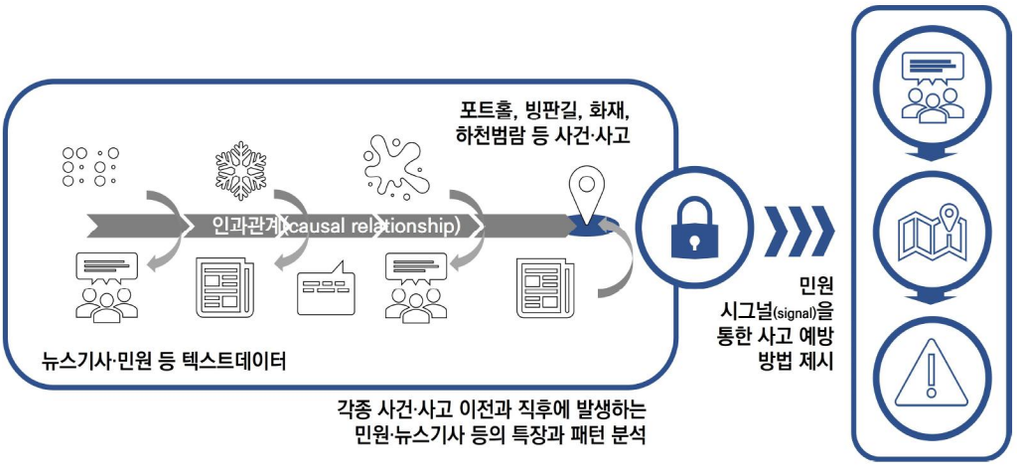
자료: 국토교통과학진흥기술원(2023) p.75

(3) 국내의 민원 활용 사례: 사회적 감지 기반 재난 정보 활용

본 원고의 핵심 사례로서, 국내의 민원을 활용한 재난·재해의 초단기 예측을 시도한 연구인 「AI 기반 재해 초단기 예측을 위한 나우캐스트 연구: 방법론 정립을 중심으로」는, 재

난 정보 공유 체계에서 데이터가 부족해 보이는 지점을 어떤 방식으로 보완할 수 있는지를 보여준다. 장요한 외(2025)에 따르면 이 연구는 민원 데이터와 외생적 공간 및 환경 정보를 결합해 재해의 이상징후(Signal)를 조기 감지하고, 초단기 예측이 가능한 AI 기반 나우캐스트(Nowcast) 모델의 프레임워크(가칭 AI-raDar)를 제안한다. 특히 민원DB에서 재해 관련 민원을 추출하고, 싱크홀·화재·홍수 등 실제 발생 기록과 결합하며, 위험징후 키워드를 추출한 뒤, 각종 정보를 1km 격자 단위로 배분하여 AI 학습과 예측으로 이어지는 일련의 단계가 제시된다. 민원이 단순한 불만의 기록이 아니라, 현장의 변화가 먼저 드러나는 사회적 감지(Social Sensing) 신호가 될 수 있다는 점을 방법론 수준에서 정리했다는 점에서 의미가 있다.

그림 6 **민원 등 사회적 감지(Social Sensing) 신호를 활용한 나우캐스트(Nowcast) 사례**



자료: 장요한 외(2025) p.6

다만 이 연구가 던지는 질문은 "가능하다"에서 끝나지 않는다. 민원 데이터는 사람의 행동이 개입된 데이터이기 때문에 대표성과 편향 문제가 발생할 수 있고, 반복 민원이나 이첩 과정이 많아질수록 민원의 맥락이 흐려지거나 특정 주제가 과대 반영될 우려도 생긴다. 또한 비정형 텍스트는 정형 데이터보다 재식별 가능성이 다른 방식으로 발생할 수 있어, 무엇을 추출하고 무엇을 남길지에 대한 기준이 필요하다고 설명한다(장요한 외, 2025). 이는 민원 기반 나우캐스트가 단순한 모델 개발을 넘어, 데이터 접근과 연계의 조건을 함께 설계해야만 운영 가능한 형태가 된다는 점을 시사한다.

(4) 소결

국내외 사례는 서로 다른 맥락을 갖지만, 공통으로 세 가지 사실을 반복해서 보여준다. 첫째, 재난 대응에서 데이터 활용은 언제든지 "범위"의 문제로 돌아온다(DHS OIG, 2019; European Commission, 2026; Jung et al., 2020). 둘째, 여러 기관과 민간이 결합하는 순간 정보는 풍부해지지만, 그만큼 책임과 설명의 경로는 복잡해진다(Ise et al., 2022; 류현숙, 2025). 셋째, 기술의 성능이 좋아지는 것과 별개로, 운영 규칙과 접근 권한, 기록의 체계가 함께 갖춰지지 않으면 신뢰는 쉽게 약해진다(NIST, 2023; Pappu, 2024; 류현숙, 2025). 지속가능한 재난 정보 공유 체계 구축을 위해서 선행되어야 하는 것들은 기술적인 비중도 크게 작용하겠지만, 결국에는 표준화와 적법한 절차에 있음을 확인할 수 있다.

Ⅴ. 정책적 쟁점과 개선 방향[8)]

앞선 장에서 확인했듯이, 재난 정보 공유는 "어느 정도의 데이터를 사용할 수 있는가"의 문제로만 설명되기 어렵다. 재난 상황에서는 센서 기반 관측만으로는 포착하기 어려운 변화가 빠르게 발생하고, 그 공백을 신고·제보·민원과 같은 사회적 감지(Social Sensing) 신호가 메우는 경우가 많다(장요한 외, 2025). 다만 사회적 감지 신호는 현장을 빠르게 비추는 대신, 그 자체가 곧바로 사실을 의미하지 않을 수 있고, 데이터가 결합되는 순간부터 책임과 설명의 경로가 복잡해진다. 결국 "유용하기 때문에 지향해야 한다"는 결론만으로는 운영이 지속되기 어렵고, "위험하기 때문에 지양해야 한다"는 결론만으로는 재난 대응에 요구되는 시간과는 그 호흡의 결이 갈린다.

(1) 데이터 수집·활용 범위 설정

사회적 감지 기반 체계에서 가장 먼저 정리되어야 할 것은 "어디까지를 데이터로 볼 것인가"이다. 특히 민원·신고 데이터는 맥락이 풍부한 만큼, 원문을 그대로 쥐고 있으면 활용의 여지가 넓어지는 동시에 위험도 커진다. 그래서 범위 설정은 단순히 항목을 줄이는 문제가 아니라, 사회적 감지 데이터를 "원문 데이터"가 아니라 "신호 데이터"로 다루는 방식으로 전환하는 문제에 가깝다. 예컨대 원문 텍스트를 그대로 공유하는 대신, 위험 징후 키워드나

8) 본 장은 장요한 외.(2024)와 장요한 외.(2025)의 연구 내용을 종합하여 재구성함

분류 결과, 발생 가능성을 나타내는 지표로 변환하고, 공간·시간 단위를 격자나 구간 단위로 올려(상향 집계) 활용하는 방식이 기본값으로 자리 잡아야 한다. 민원이라는 "개별 경험"을 그대로 옮기는 것이 아니라, 재난 대응에 필요한 "집단적 신호"만 뽑아내는 설계가 선행되어야 한다.

또 하나의 핵심은 범위를 "상시"로 고정하기보다 "단계"로 운영하는 것이다. 평시에는 낮은 정밀도의 집계 신호만 활용하고, 특정 조건이 충족될 때에만(경보 단계 상향, 특정 지역의 급격한 신호 증가, 관측 데이터와의 교차 검증 결과 등) 더 정밀한 데이터 접근을 허용하는 방식이 현실적이다. 이때 확장 조건과 종료 조건이 문서로 고정되지 않으면, 긴급성은 곧바로 관행적 확장의 근거가 되기 쉽다. 사회적 감지 기반 체계에서 "범위 설정"은 결국 기술의 선택이 아니라, 확대와 축소가 모두 가능한 운영 규칙의 선택이다(Ekmekci et al., 2025; 류현숙, 2025).

(2) 법·제도 정합성

사회적 감지 기반 정보 공유는 공익 목적이 분명한 영역에 속하지만, 그 사실이 곧바로 모든 데이터 활용을 정당화하지는 않는다(Ekmekci et al., 2025; Yuan et al., 2025). 특히 민원·신고·위치 기반 신호는 기관이 다르고 경로가 다르며, 민관 협력이 개입되면 제공자·처리자·운영자의 책임이 분리되기 쉽다. 이때 법·제도 정비의 방향은 "가능하면 쓰자"를 넓히는 데만 있지 않고, "어떤 조건에서 어디까지 쓸 수 있는가"를 문서와 절차로 고정하는 데에 있어야 한다. 목적 제한, 보관 기간, 재제공 금지, 접근 권한, 사후 점검의 요구사항이 한 패키지로 묶이지 않으면, 운영은 빠르게 확장되고 설명은 뒤늦게 따라가게 된다(European Commission, 2026; Truong et al., 2021).

또한 사회적 감지 신호는 재난 대응과 밀접하지만, 목적이 조금만 확장되면 곧바로 다른 영역(단속·감시·상업적 활용)으로 전이될 수 있다는 점에서 경계 설정이 중요하다(류현숙, 2025). 따라서 목적 변경은 단순한 운영상의 선택이 아니라, 별도의 승인과 기록을 요구하는 "거버넌스 이벤트"로 취급되어야 한다. 역할 측면에서는 데이터 관리자(Controller)와 처리자(Processor), 제공자(Provider), 운영자(Deployer)의 책임 경계가 사전에 정리되어야 하며, 협약은 선언적 협약이 아니라 접근·보관·재위탁·기록·감사까지 포함하는 운영 규칙의 형태를 갖추어야 한다(Truong et al., 2021; 류현숙, 2025). 그래야만 사고가 발생했을 때 "누가 무엇을 했는지"가 남고, 개선이 가능한 지점도 특정될 수 있다(GLOPID-R, 2018; 류현숙, 2025).

(3) 거버넌스와 운영 통제

재난 정보 공유에서 가장 반복적으로 발생하는 마찰은 실시간성 요구와 절차의 충돌이다(Ekmekci et al., 2025). 위기 상황에서는 판단이 늦어질수록 피해가 커질 수 있고, 그 압박은 데이터 범위를 넓히거나 확인 절차를 생략하는 방향으로 작동하기 쉽다. 반대로 절차만을 앞세우면 현장 대응의 속도가 무너질 수 있다. 이 충돌을 줄이기 위해서는 "위기 시에 절차를 만들지 않도록" 평시에 운영 규칙과 예외 조건을 사전에 정의할 필요가 있다. 어떤 신호가 어느 수준에 도달하면 어떤 범위의 데이터를 원문이나 지표 및 분석 결과 등 어떤 형태로 활용할 수 있는지, 승인권자는 누구인지, 기록은 무엇을 남겨야 하는지가 사전에 마련되어야 한다.

운영 통제의 관점에서는 접근과 활용을 분리해 설계하는 방식이 유효하다. 즉, 원천 데이터에 대한 접근은 최소화하되, 필요한 분석은 통제된 환경에서 수행하고, 결과물만 공유하는 구조를 기본으로 두는 것이다(Pati et al., 2024; Truong et al., 2021). 이 과정에서 개인정보 보호 기술(PETs)은 선택지가 될 수 있지만, 핵심은 기술의 도입 자체가 아니라 "접근이 최소화되었는지, 변경 이력이 남는지, 사후 감사가 가능한지"가 운영 습관으로 정착되는 데 있다(Truong et al., 2021; Zendata, 2024). 특히 사회적 감지 신호는 노이즈(Noise)가 많고 재가공이 필수적이므로, 데이터 전처리 기준과 모델 버전, 지표 생성 방식이 기록으로 남지 않으면 동일한 결과라도 설명이 어렵고, 이는 신뢰를 저해하는 요인이 된다.

(4) 품질·편향·불확실성 관리

사회적 감지 신호는 빠르지만 불완전하다(WHO, 2022). 신고와 민원은 중복·지연·누락이 함께 발생할 수 있고, 지역과 계층의 특성이 신호의 강도를 좌우할 수 있다. 따라서 품질 관리는 "완벽한 데이터만 쓰자"는 목표로 접근하기보다, 불완전함을 전제로 판단의 안전성을 확보하는 방향으로 구성되어야 한다. 예컨대 사회적 감지 신호는 단독 근거로 쓰기보다 관측 데이터나 행정 데이터와 교차 검증하는 방식으로 운영하고, 신호가 단기간 급증하는 경우에도 일정 기준 이상은 "참고"로 분류해 추가 확인을 거치도록 설계할 필요가 있다. 사회적 감지 기반 체계는 결국 "어떤 신호를 경보로 전환할 것인가"라는 임곗값(Threshold)의 문제를 피할 수 없고, 이 임곗값을 어떻게 정하고 어떻게 수정하는지가 곧 정책의 문제로 이어진다(WHO, 2022).

또한 편향과 대표성 문제는 시스템이 커질수록 더 중요해진다(NIST, 2022; Wood, 2025). 특정 지역에서 민원이 많다고 해서 위험이 항상 큰 것은 아니며, 반대로 민원이 적다고 해서 위험이 낮다고 단정할 수도 없다. 따라서 운영 단계에서는 지역·계층별 신호의 분포를 지속적으로 점검하고, 실제 발생 기록과 비교하며, 성능과 오류를 기록하는 최소한의 모니터링 체계를 갖춰야 한다. 사회적 감지 기반 재난 정보 공유가 지속 가능하려면, "예측이 맞았는가"만이 아니라 "어떤 근거로 그렇게 판단했는가"가 계속 설명될 수 있어야 한다(Yuan et al., 2025; 류현숙, 2025).

(5) 대국민 소통과 단계적 구축

사회적 감지 기반 체계는 시민이 생산한 신호를 활용한다는 점에서, 다른 재난 데이터보다 신뢰의 기반이 더 취약할 수 있다(류현숙, 2025). 시민이 느끼기에 그 체계가 "공공 안전을 위한 참여"로 보이지 않고 "일상에 대한 감시"로 보이는 순간, 데이터 활용의 정당성은 급격히 약해진다(Yuan et al., 2025; 류현숙, 2025). 따라서 소통은 홍보가 아니라 운영의 일부가 되어야 한다. 어떤 종류의 신호를 어떤 단위로 집계해 쓰는지, 원문은 어느 단계에서 어떤 방식으로 처리되는지, 결과물은 어떤 기준으로 공유되는지, 오류가 발생했을 때 어떻게 정정하고 책임을 점검하는지와 같은 기본 정보가 평시에 정리되어 있어야 한다(Jung et al., 2020; Yuan et al., 2025). 또한 예측 기반 정보는 불확실성을 포함하므로, 경보와 안내에서 "확정"처럼 표현하는 습관을 줄이고, 어느 수준의 불확실성이 있는지를 시민이 이해할 수 있는 언어로 전달하는 방식도 필요할 것이다.

구축 전략의 측면에서는 한 번에 완성형으로 가기보다 단계적 접근이 현실적이다(류현숙, 2025). 먼저 특정 유형(예: 도심 싱크홀, 국지성 호우, 산불 등)과 특정 지역을 대상으로 집계 신호 중심의 시범 운영을 수행하고, 운영 중에 발생하는 품질 문제와 편향 문제, 설명과 기록의 공백을 먼저 정리한 뒤 확장하는 방식이 바람직하다. 사회적 감지 기반 재난 정보 공유 체계는 기술적 가능성만으로 확장되지 않는다. 범위의 절제, 절차의 명확화, 기록의 습관, 그리고 시민의 이해와 동의라는 조건이 함께 갖춰질 때만 비로소 "구축"이라는 단어가 실질적 의미를 갖게 된다(Ekmekci et al., 2025; 류현숙, 2025).

Ⅵ. 결론 및 정책 제언

재난 대응에서 데이터는 단순한 참고자료가 아니라, 경보와 대응을 움직이는 기반이 된다. 특히 센서 기반 관측만으로는 포착하기 어려운 변화가 빠르게 발생하는 상황에서는, 신고나 민원과 같은 사회적 감지(Social Sensing) 신호가 공공 인프라의 공백을 메우는 중요한 단서가 될 수 있다. 다만 사회적 감지 신호는 "현장을 빠르게 비춘다"는 장점과 함께, 그 신호가 언제나 사실을 의미하지는 않는다는 한계도 동시에 지닌다. 결국 AI와 사회적 감지 기반의 재난 정보 공유 체계를 구축한다는 일은, 데이터를 더 모으는 기술적 확장만을 뜻하지 않는다. 어떤 신호를 어떤 범위에서 어떤 방식으로 결합·가공·공유할지에 대한 운영 규칙을 먼저 만들고, 그 규칙을 흔들리지 않게 유지할 책임 구조와 기록 체계를 함께 갖추는 일에 가깝다.

본 원고가 반복해서 확인한 사실은 단순하다. 재난 정보 공유는 "예측의 정확도"만으로 정당화되기 어렵고, 데이터가 결합되는 순간부터 정당성과 책무성, 설명 가능성의 문제가 함께 발생한다. 특히 사회적 감지 기반 데이터는 때에 따라서 개인의 경험과 행동이 섞인 신호이기 때문에, 그 신호를 원문 그대로 다루는 순간에는 프라이버시와 목적 제한의 문제가 커지고, 신호를 지나치게 단순화하는 순간에는 데이터로써 품질과 대표성의 문제가 커진다. 따라서 사회적 감지 기반 체계는 "더 많이 모으자"가 아니라 "어떤 형태의 신호로 바꾸어 재난 대응에 사용할 것인가"라는 질문에서 출발해야 한다. 결국 어떤 데이터를 어떤 단위로 가공 및 결합했는지, 그리고 그 과정이 어떤 권한과 기록 체계 아래에서 이루어졌는지가 AI가 내놓는 판단의 성격과 한계를 좌우한다.

다음은 AI와 사회적 감지 기반의 재난 정보 공유 체계 구축을 위해 다루어야 할 몇 가지 요소들을 종합한 내용이다.

첫째, 사회적 감지 데이터는 가능한 한 "원문"이 아니라 "신호"로 다루는 것이 기본값이 되어야 한다. 재난 대응에 필요한 것은 개별 민원의 서사가 아니라, 특정 위험 징후가 어느 지역에서 어느 시간대에 증가하는지와 같은 집단적 패턴이다(장요한 외, 2024; 장요한 외, 2025). 따라서 텍스트 원문을 그대로 공유하는 방식보다, 위험 징후 분류·키워드 지표·공간 격자(Grid) 등으로 변환한 뒤 공유하는 방식이 우선되어야 할 필요가 있다. 원문 접근은 예외적 필요가 입증되는 경우에만 제한적으로 허용되고, 그 또한 목적과 기간이 명확히 고정되어야 한다(GLOPID-R, 2018; Truong et al., 2021).

둘째, 데이터 범위는 상시로 고정하기보다 단계적으로 운영될 필요가 있다. 평시에는 낮

은 정밀도의 집계 신호를 중심으로 운영하고, 일정 조건이 충족될 때만 범위를 확장하는 방식이 현실적이다. 중요한 것은 확장 조건뿐 아니라 종료 조건까지 함께 마련하는 것이다. 재난의 긴급성은 범위를 넓히는 방향으로만 작동하기 쉬우므로, 종료 조건이 없으면 확대는 관행이 된다(Ekmekci et al., 2025; Jung et al., 2020; 장요한 외, 2024; 장요한 외, 2025).

셋째, 민관 결합에서는 역할과 책임을 문서로 먼저 고정해야 한다. 데이터 제공자(Provider), 관리자(Controller), 처리자(Processor), 운영자(Deployer)가 분리되는 구조에서 책임 경계가 흐려지면, 문제는 사후에 되풀이된다(Truong et al., 2021; 류현숙, 2025). 특히 목적, 범위, 보관 기간, 재제공 금지, 접근 권한, 기록·감사 방식이 한 세트로 정리되지 않으면, 위기 시에는 범위가 넓어지고 사후에는 책임이 분산되기 쉽다(European Commission, 2026; GLOPID-R, 2018; Truong et al., 2021).

넷째, 실시간성 요구와 절차의 충돌을 줄이기 위한 규칙 기반 프로토콜을 만들어야 한다. 재난의 유형과 국면이 다양해질수록, 위기 시에는 절차가 느슨해지거나 반대로 절차가 과도하게 작동하는 극단이 반복되기 쉽다(Ekmekci et al., 2025). 어떤 신호가 어느 수준에 도달하면 어떤 데이터가 어떤 형태로 사용되는지, 승인권자는 누구인지, 무엇을 기록으로 남겨야 하는지가 사전에 마련되어야할 필요가 있다. 개인정보 보호 기술(PETs)은 이러한 규칙 기반 프로토콜을 구현하는 선택지가 될 수 있으나, 핵심은 기술 도입 자체가 아니라 접근 최소화와 기록·감사가 운영 습관으로 정착되는 데 있다(Pati et al., 2024; Truong et al., 2021).

다섯째, 사회적 감지 기반 예측은 "정확도"뿐 아니라 "판단의 안전성"으로 평가되어야 한다. 사회적 감지 신호는 노이즈와 편향 가능성을 내포하므로, 관측 데이터나 행정·인프라 데이터와의 교차 검증이 기본 운영 방식이 되어야 한다(Wood, 2025; Yuan et al., 2025; 장요한 외, 2025). 또한 지역 · 계층별 신호 편차가 경보와 자원 배분으로 전이되지 않도록, 최소한의 모니터링과 성능 점검이 상시적으로 필요하다. 불확실성을 숨기는 체계는 빠르게 확장될 수는 있어도, 오래 지속되기는 어렵다(Ekmekci et al., 2025; 류현숙, 2025).

AI와 사회적 감지 기반 재난 정보 공유 체계는 기술적으로는 매력적인 가능성을 보여준다. 그러나 재난 대응에서 진정한 성과는 "AI를 활용한 예측 모델이 적중했다"는 순간에만 존재하지 않는다. 필요한 데이터를 필요한 만큼만 쓰고, 그 과정이 사후에 설명될 수 있으며, 시민이 그 운영을 납득할 수 있을 때 비로소 체계는 지속 가능해진다. 결국 데이터 윤리는 재난 대응을 늦추기 위한 장치가 아니라, 재난 대응이 빠르게 움직이면서도 신뢰를

잃지 않게 하기 위한 최소한의 운영 조건이며, 사회적 감지 기반 체계 구축은 그 조건을 선명하게 요구하는 영역이라고 할 수 있다.

참고문헌

국토교통과학진흥기술원. 2023. 스마트시티 혁신성장동력 프로젝트 사업단 보고서.(테크니컬리포트) [1부 1권 별책1] 코로나19 역학조사지원시스템 PoC. 한국전자기술연구원.

류현숙. 2025. 재난안전 정책의 효과적 의사결정을 위한 AI 활용방안 연구. KIPA 연구보고서 2025-03. 한국행정연구원.

이승환. 2025. “AI와 가상융합 기반 재난재해 대응 방안.” 국가미래전략 Insight 120호. 국회미래연구원.

이상욱. 2021. “유네스코 인공지능(AI) 윤리 권고 해설서 인공지능 윤리 이해하기.” 서울: 유네스코한국위원회.

오픈클로 깃허브 웹페이지(https://github.com/openclaw/openclaw, 2026년 2월 20일 접속)

오픈클로 공식 웹페이지(https://openclaw.ai/, 2026년 2월 20일 접속)

장요한, 손재선, 최혜림(2024). 민생현안 모니터링을 위한 민원지도 개선방안 연구, 세종: 국토연구원.

장요한, 손재선, 최혜림(2025). AI기반 재해 초단기 예측을 위한 나우캐스트 연구: 방법론 정립을 중심으로, 세종: 국토연구원.

질병관리청. 2022. 코로나19 역학조사지원시스템 운영 결과.

캘리포니아 주립대학교 샌프란시스코 웹페이지(https://ai.ucsf.edu/trustworthy, 2026년 2월 20일 접속).

DHS OIG(Department of Homeland Security Office of Inspector General). 2019. Management Alert - FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information. OIG-19-32. Washington, DC: DHS OIG.

Ekmekci, Perihan Elif, Lili Zhang, and Francis P. Crawley. 2025. “Ethics Underpinning Data Policy in Crisis Situations.” Data Science Journal 24(4): 1-9. https://doi.org/10.5334/dsj-2025-004.

European Commission. 2026. “The European approach to artificial intelligence.” https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.

European Parliament. 2025. “EU AI Act: first regulation on artificial intelligence.”

FEMA(Federal Emergency Management Agency). 2019. Integrated Public Alert and Warning System(IPAWS).

GLOPID-R. 2018. Global Research Collaboration for Infectious Disease Preparedness.

Ise, T., et al. 2022. "Approach About Wide Area Cooperation of Disaster Information Using SIP4D." Journal of Disaster Research 17(6): 978-984.

Jung, Gyuwon, Hyunsoo Lee, Auk Kim, and Uichin Lee. 2020. "Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With COVID-19 in South Korea." Frontiers in Public Health 8: 305. https://doi.org/10.3389/fpubh.2020.00305.

Mollick, Ethan. 2024. Co-intelligence: Living and working with AI. Penguin,

NIST(National Institute of Standards and Technology). 2022. Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. NIST Special Publication 1270. https://doi.org/10.6028/NIST.SP.1270.

NIST(National Institute of Standards and Technology). 2023. Artificial Intelligence Risk Management Framework(AI RMF 1.0). NIST AI 100-1. https://doi.org/10.6028/NIST.AI.100-1.

OECD(Organisation for Economic Co-operation and Development). 2019. AI principles. https://oecd.ai/en/ai-principles.

Pappu, Narayana. 2024. "AI Ethics 101: Comparing IEEE, EU, and OECD Guidelines." Zendata. May 20, 2024.

Pati, S., et al. 2024. "Privacy preservation in federated learning and medical imaging." (Review).

Peskin, Amanda H. 2026. "The Integrated Public Alert and Warning System(IPAWS): Primer and Issues for Congress." Congressional Research Service. R48363. Updated January 15, 2026. https://crsreports.congress.gov/product/pdf/R/R48363.

SIP4D 웹페이지(https://www.sip4d.jp/, 2026년 2월 20일 접속)

The Guardian, 「Fitness tracking app Strava gives away location of secret US army bases」, 2018. 1. 28. (https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases, 2026년 2월 20일 접속).

Truong, Nguyen, Kai Sun, Siyao Wang, Florian Guitton, and YiKe Guo. 2021. "Privacy preservation in federated learning: An insightful survey from the GDPR perspective." Computers & Security 110: 102402. https://doi.org/10.1016/j.cose.2021.102402.

WHO(World Health Organization). 2022. Health Emergency and Disaster Risk Management Framework.

Wood, Erik Xavier. 2025. "AI and big data in disaster response: Ethical and practical challenges." Journal of Dynamic Disasters 1: 100041.

Yuan, Xiaojun, Qingyue Guo, Yvonne Appiah Dadson, et al. 2025. "A Review of Ethical Challenges in AI for Emergency Management." Knowledge 5: 21. https://doi.org/10.3390/knowledge5030021.