

파운데이션 모델 생태계의 근본적 딜레마: 지속 가능한 AI 시대를 위한 새로운 제언

새로운 패러다임의 서막

인공지능(AI) 기술은 새로운 시대의 서막을 열고 있습니다. 그 중심에는 ‘파운데이션 모델(Foundation Model)’이 자리 잡고 있습니다. 스탠포드 인간 중심 AI 연구소(HAI)에 의해 명명된 파운데이션 모델은, 방대한 데이터로 훈련되어 광범위한 작업에 적용될 수 있는 대규모 범용 AI 모델을 의미합니다.¹ 이는 특정 작업에만 국한되던 기존 AI와 달리, 한번 구축되면 여러 애플리케이션의 기반 인프라로 재사용될 수 있는 패러다임의 전환을 의미합니다.³

이러한 모델의 등장은 AI 생태계의 폭발적인 성장을 견인했습니다. 2023 년에만 149 개의 새로운 파운데이션 모델이 발표되었는데, 이는 2022 년의 두 배가 넘는 수치입니다.⁴ 텍스트와 이미지를 넘어 비디오, 음성, 심지어 물리 세계를 시뮬레이션하는 월드 파운데이션 모델에 이르기까지 그 적용 범위는 무한히 확장되고 있습니다.⁴

그러나 이 눈부신 발전의 이면에는 ‘동질화(Homogenization)’라는 구조적 특징이 숨어 있습니다.² 소수의 거대 파운데이션 모델이 수많은 애플리케이션의 기반이 되는 현상은 효율성을 높이지만, 동시에 시스템 전체의 리스크를 한곳에 집중시키는 양날의 검과 같습니다. 이는 단순히 기술적 장애의 문제를 넘어섭니다. 만약 그 ‘기초(Foundation)’가 되는 모델 자체가 법적, 윤리적 결함을 안고 있다면, 그 위에 세워진 수천, 수만 개의 애플리케이션과 서비스 전체가 한순간에 붕괴할 수 있는 시스템적 취약성을 내포하게 됩니다. 현재 AI 생태계는 바로 이 불안정한 토대 위에 위태롭게 서 있으며, AHNIST 는 이 구조적 문제를 해결하고 지속 가능한 기술의 미래를 제시하고자 합니다.⁵

보이지 않는 AI의 건축 구조

AI 생태계의 문제를 이해하기 위해서는 먼저 그 기술적 구조를 파악해야 합니다. 일반적으로 AI 기술 스택(Tech Stack)은 네 가지 핵심 계층으로 구성됩니다.⁶

1. **인프라 계층 (Infrastructure Layer):** AI 모델의 연산을 처리하는 GPU와 같은 반도체 칩, 서버, 클라우드 등 물리적 하드웨어의 기반입니다.
2. **데이터 계층 (Data Layer):** 모델을 훈련시키기 위한 방대한 데이터를 수집, 저장, 관리하는 영역입니다.
3. **모델 계층 (Model Layer):** 데이터 계층의 정보를 바탕으로 훈련된 파운데이션 모델, LLM 등이 위치하는 AI의 지능의 핵심입니다.
4. **애플리케이션 계층 (Application Layer):** ChatGPT와 같이 최종 사용자가 직접 상호작용하는 서비스와 소프트웨어입니다.

이 계층들을 관통하며 ‘데이터 수집 → 모델 훈련 → 콘텐츠 생성 → 유통 → 수익화’라는 AI 워크플로우가 작동합니다.⁶ 하지만 현재의 기술 스택에는 결정적인 한 가지가 빠져 있습니다. 바로 생태계의 기본 규칙을 관장하는 ‘메타-인프라스트럭처(Meta-Infrastructure)’ 계층입니다.⁵

메타-인프라스트럭처는 데이터와 모델 계층 사이에 위치하며, 데이터의 출처(Provenance)를 검증하고, 콘텐츠의 진본성(Authenticity)을 증명하며, 지적 재산권(IP)을 추적하고, 가치 교환을 자동화하는 생태계의 등기소이자 신뢰 시스템의 역할을 수행해야 합니다. 이 계층의 부재는 현재 AI 생태계가 겪고 있는 모든 문제의 근본 원인입니다. AHNIST는 바로 이 비어있는 필수 계층을 구축하는 독점적인 솔루션을 제공합니다.⁵

표 1: AI 기술 스택과 부재하는 메타-인프라스트럭처 계층

계층	설명	주요 구성 요소	지배 원리
애플리케이션	최종 사용자가 상호작용하는 AI 서비스	ChatGPT, AI 편집기, 챗봇	사용자 경험
모델	데이터로부터 학습된 AI의 핵심 지능	파운데이션 모델, LLM, 미세조정 모델	예측 및 생성
메타-인프라 (AHNIST)	[부재하는 계층] 생태계의 규칙과 신뢰를 관장	콘텐츠 윌렛, 절대 식별자(AID), 콘텐츠 체인	출처, 진본성, 소유권 증명
데이터	AI 모델 훈련을 위한 데이터의 수집 및 관리	데이터베이스, 데이터 레이크, 웹 스크래핑	규모와 품질
인프라	AI 연산을 위한 물리적 기반	GPU, 클라우드 서버, 데이터 센터	컴퓨팅 파워

AI 생태계 중심의 삼중 딜레마 (Trilemma)

메타-인프라스트럭처의 부재는 해결 불가능해 보이는 세 가지 근본적인 딜레마, 즉 ‘트리레마’를 야기합니다. 이들은 별개의 문제가 아니라 서로 긴밀하게 연결된 하나의 복합적인 위기입니다.⁵

3.1 출처의 역설: 근원을 알 수 없는 토대 위에 세운 세상

파운데이션 모델은 그 성능을 위해 인터넷에서 무차별적으로 수집된, 출처가 불분명한 방대한 데이터를 학습합니다.¹ 이는 필연적으로 ‘데이터 프로버넌스(Data Provenance)’, 즉 데이터 출처 증명의 위기를 초래합니다.⁵

이 문제는 더 이상 이론에 머무르지 않습니다. 2023 년, 뉴욕타임스(NYT)는 OpenAI 와 마이크로소프트를 상대로 수백만 건의 기사에 대한 대규모 저작권 침해 소송을 제기했습니다.⁹ NYT 는 ChatGPT 가 자사의 기사를 거의 그대로 ‘암기(memorization)’하고 ‘역류(regurgitation)’시키는 사례를 100 가지 이상 제시하며, 이것이 단순 학습을 넘어선 명백한 저작권 침해라고 주장했습니다.⁹ 이 소송의 잠재적 손해 배상액은 최소 수십억 달러에서 최대 수천억 달러에 이를 수 있으며, 이는 AI 산업의 기반을 뒤흔들 수 있는 막대한 법적 리스크입니다.⁹

이러한 소송은 NYT 에 국한되지 않습니다. 작가, 예술가, 컴퓨터 프로그래머 등 수많은 창작자들이 자신의 저작물이 허락 없이 AI 훈련에 사용되었다며 소송을 제기하고 있으며, 이는 AI 산업 전반에 걸친 시스템적 문제입니다.¹² 게티이미지가 스태빌리티 AI 를 상대로 제기한 소송은, 일단 학습이 완료된 후에는 저작권 침해를 입증하는 것이 얼마나 어려운지를 보여주며, 사후 대응이 아닌 사전적인 출처 추적 시스템의 필요성을 역설합니다.¹⁴

3.2 진본성의 심연: 디지털 신뢰의 붕괴

AI 가 생성하는 콘텐츠의 품질이 비약적으로 향상되면서, 인간의 저작물과 AI 생성물을 구분하는 것이 거의 불가능해지고 있습니다.⁵ 이는 ‘콘텐츠 진본성(Content Authenticity)’의 붕괴로 이어져 디지털 세계 전체의 신뢰 기반을 무너뜨리고 있습니다.¹⁶

2023 년에만 최소 50 만 개의 딥페이크 영상 및 음성이 소셜 미디어에 공유되었으며¹⁶, 대중의 미디어에 대한 신뢰도는 역대 최저 수준으로 떨어졌습니다.¹⁷ 이 문제의 심각성은 단순한 가짜 뉴스 유포를 넘어섭니다. 바로 ‘거짓말쟁이의 배당금(Liar's Dividend)’이라는 두 번째 효과를 낳기 때문입니다.¹⁸ 이는 딥페이크 기술의 존재만으로도 악의적인 행위자가 불리한 ‘진짜’ 증거를 ‘가짜’라고 주장하며 빠져나갈 명분을 만들어주는 현상입니다.¹⁹ 결국, 진실과 거짓의 경계가 무너지면서 사회적 합의와 공적 담론의 기반 자체가 침식되는 ‘탈진실(post-truth)’ 환경이 고착화됩니다.¹⁷

3.3 가치의 공백: 지적 재산과 창작자 수익의 블랙홀

현재의 AI 생태계는 수백만 창작자들의 지적 노동을 가치 있는 자산이 아닌, 무료로 채굴 가능한 원자재처럼 취급합니다.⁵ AI 모델이 어떤 창작물로부터 가치를 학습했는지, 그 기여도를 추적하고 정당한 보상을 분배할 메커니즘이 전무하기 때문입니다.⁵

이는 ‘창작자 경제(Creator Economy)’의 역설을 낳습니다. 창작자 경제의 시장 규모는 2030년까지 약 5,000억 달러에 이를 것으로 전망될 만큼 거대하지만²⁰, 그 부는 창작자에게 거의 돌아가지 않습니다. 통계에 따르면, 전업 창작자 중 생계를 유지할 수 있는 수준(연 5만 달러 이상)의 수입을 올리는 비율은 4%에서 12%에 불과합니다.²¹

이러한 불공정한 분배 구조는 이미 음악 스트리밍 시장에서 현실화되었습니다. 플랫폼 기업들은 수십억 달러의 수익을 창출하지만, 아티스트에게 돌아가는 스트리밍당 수익은 1센트의 일부에 불과하며, 이마저도 수년간의 하락 끝에 겨우 안정화된 수치입니다.²³ 플랫폼이 유통망을 독점하고 수익의 대부분을 가져가는 구조(국내 음원 시장의 경우 유통사/제작사가 84% 차지)가 AI 생태계에서 그대로 재현되고 있는 것입니다.⁵

결론적으로, 이 세 가지 딜레마는 하나의 뿌리에서 파생됩니다. 데이터의 **출처**를 모르기 때문에 콘텐츠의 **진본성**을 보장할 수 없으며, 기여한 **가치**를 정당하게 분배할 수도 없는 것입니다. 이는 디지털 자산의 출생부터 모든 이력을 기록하고 증명할 신뢰할 수 있는 ‘등기 시스템’의 부재라는 단일한 위기이며, 이 문제를 해결하는 것이야말로 지속 가능한 AI 생태계 구축의 선결 과제입니다.

업계의 대응: 필요하지만 결함 있는 첫걸음

이러한 문제에 대응하기 위해 업계는 자발적으로 해결책을 모색하기 시작했습니다. 그 대표적인 사례가 바로 어도비(Adobe)가 주도하고 마이크로소프트, 구글 등 주요 기업들이 참여하는 ‘콘텐츠 출처 및 진본성을 위한 연합(C2PA, Coalition for Content Provenance and Authenticity)’입니다.²⁵

C2PA의 핵심 기술은 ‘콘텐츠 크리덴셜(Content Credentials)’이라는 표준입니다.²⁷ 이는 디지털 파일에 생성자, 편집 이력 등의 출처 정보(메타데이터)를 담은 ‘매니페스트(Manifest)’를 첨부하고, 이를 암호화 기술로 서명하여 위변조 여부를 확인할 수 있게 하는 방식입니다.²⁸ 이 기술은 콘텐츠의 투명성을 높이려는 중요한 시도이며, 그 자체로 의미가 있습니다.

그러나 C2PA는 근본적인 아킬레스건을 가지고 있습니다. 바로 그 보안성이 콘텐츠의 본질이 아닌, 파일에 ‘부착된 라벨’과 같은 메타데이터에 의존한다는 점입니다. 이 방식은 콘텐츠가 끊임없이 복제되고 변형되는 실제 인터넷 환경에서 치명적인 취약점을 드러냅니다.

- **메타데이터 제거(Stripping) 취약성:** C2PA의 콘텐츠 크리덴셜은 너무나 쉽게, 그리고 영구적으로 제거될 수 있습니다.
 - **파일 형식 변환:** 가장 흔한 작업 중 하나인 JPG 파일을 PNG로 변환하거나, 플랫폼에 업로드할 때 압축 및 재인코딩 과정을 거치면 C2PA 메타데이터가 손실될 수 있습니다.³⁰
 - **화면 캡처:** 인터넷에서 콘텐츠를 공유하는 가장 보편적인 방법인 스크린샷은 원본의 메타데이터가 전혀 없는 완전히 새로운 이미지 파일을 생성합니다. 이는 인터넷 전반의 콘텐츠를 추적하려는 시스템에게는 치명적인 결함입니다.³²
 - **플랫폼 비호환성:** 많은 소셜 미디어 플랫폼은 역사적으로 업로드 과정에서 불필요한 메타데이터를 제거해 왔으며, 이는 C2PA 정보의 유실로 이어집니다.³⁵

C2PA 스스로도 이 문제를 인지하고 있습니다. 공식 보안 문서에서는 ‘C2PA 매니페스트 제거(Stripping C2PA Manifests)’를 예방할 수 없는 위협으로 명시하고 있으며, 이에 대한 해결책으로 워터마크나 외부 데이터베이스를 연동하는 복잡한 ‘소프트 바인딩(Soft Binding)’ 기술을 제안하지만, 이는 완전한 해결책이 아닌 사후적 보완책에 불과합니다.²⁸

결국 C2PA의 근본적인 한계는 기술적 버그가 아닌, 철학적·구조적 문제입니다. 이는 혼란스러운 디지털 환경에 외부에서 ‘라벨’을 붙여 질서를 부여하려는 시도입니다. 하지만 콘텐츠의 복제와 변형이 일상인 환경에서 ‘라벨’에 의존하는 보안 시스템은 실패할 수밖에 없습니다. 진정으로 견고한 솔루션은 외부의 라벨이 아닌, 디지털 자산의 본질, 즉 ‘디지털 DNA’ 자체에 내재되어야 합니다.

새로운 토대: AHNIST 메타-인프라스트럭처 솔루션

AHNIST는 C2PA와 같은 메타데이터 기반 접근법의 한계를 근본적으로 극복하는 새로운 패러다임을 제시합니다. 이는 외부의 라벨이 아닌, 콘텐츠의 본질에 보안과 소유권을 각인시키는 ‘메타-인프라스트럭처’ 솔루션입니다.

5.1 불안정한 메타데이터에서 불변의 하드웨어로: 콘텐츠 월렛

AHNIST 기술의 핵심은 ‘콘텐츠 월렛(Content Wallet)’입니다. 이는 하드웨어 기반의 ‘디지털 데이터용 실물 지갑’이라는 혁신적인 개념입니다.⁵

핵심 원리는 간단하고 강력합니다. 원본 데이터와 그 진본성을 증명하는 인증서는 분리 불가능한 상태로, 물리적으로 안전한 전용 단말기 내부에서 생성되고 보관됩니다. 보안이 분리 가능한 ‘라벨’이 아닌, 자산의 출생 자체에 내재된 물리적 속성이 되는 것입니다.⁵ 이는 C2PA의 메타데이터 제거 문제를 원천적으로 해결합니다. 콘텐츠 월렛으로 관리되는 자산을 스크린샷으로 캡처하더라도, 그것은 원본의 가치를 지니지 않는 단순한 이미지일 뿐입니다. 거래 가능하고 법적 효력을 갖는 유일무이한 원본은 오직 소유자의 콘텐츠 월렛 안에 안전하게 남아있습니다.

5.2 현실에 뿌리내린 정체성: 절대 식별자(AID)와 민주적 OTP(D-OTP)

익명성에 기댄 저작권 침해와 책임 회피를 막기 위해, AHNIST는 기존 분산 ID(DID)의 허점을 보완한 새로운 신원 인증 체계를 제안합니다.⁵ 바로 ‘절대 식별자(Absolute Identifier, AID)’와 ‘민주적 OTP(Democratic OTP, D-OTP)’입니다.

이 시스템은 사용자가 소유한 두 개의 물리적 기기, 즉 ‘콘텐츠 월렛’과 스마트폰과 같은 ‘노드’ 사이의 암호화된 통신을 통해 신원을 증명합니다.⁵ 이를 통해 디지털 신원(AID)이 특정 개인의 물리적 소유권과 분리 불가능하게 연결됩니다. 이는 가짜 계정 생성을 원천 차단하고 모든 디지털 활동에 대한 명확한 법적 책임 소재를 부여함으로써, 신뢰할 수 있는 거래의 기반을 마련합니다.

5.3 휴먼 체인: 기술이 현실이 되는 시나리오

AHNIST의 기술이 어떻게 실제로 작동하는지, 가상의 시나리오를 통해 살펴보겠습니다.

- **1 단계 (창작과 증명):** 독립 뮤지션 ‘하나’는 새로운 곡을 완성합니다. 그녀는 자신의 ‘콘텐츠 월렛’을 통해 이 마스터 음원 파일을 ‘발행(minting)’합니다. 이 순간, 음원의 고유한 해시값이 생성되고 하나의 절대적인 원본으로 등록됩니다. 동시에 하나의 AID가 창작자로 기록되며, 이 곡의 ‘디지털 DNA’가 탄생합니다. 이 모든 정보는 위변조가 불가능한 ‘콘텐츠 체인’에 기록됩니다.⁵
- **2 단계 (유통과 거래):** 하나는 이 곡을 1,000장 한정판으로 판매하기로 결정하고, 가격과 사용 조건을 월렛 인터페이스에서 직접 설정합니다. 팬인 ‘진’이 이 곡을 구매하고자 P2P 거래를 시작합니다.
- **3 단계 (인증과 복제):** 진의 기기가 구매를 요청하면, 네트워크는 진의 신원(AID)과 결제 여부를 확인합니다. 모든 것이 확인되면, 하나의 콘텐츠 월렛은 진을 위한 합법적인 라이선스 복제본 생성을 승인하고 전송합니다. ‘하나가 진에게, 특정 시간에, 특정 가격으로 판매했다’는 거래 기록 역시 콘텐츠 체인에 남습니다.⁵
- **4 단계 (수익 분배):** 결제된 금액은 복잡한 중간 유통 과정이나 높은 플랫폼 수수료가 없이, 즉시 그리고 자동으로 하나의 계좌로 입금됩니다. 그녀는 자신이 창출한 가치의 대부분을 직접 소유하게 됩니다.

이 시나리오는 AHNIST의 시스템이 어떻게 트릴레마를 동시에 해결하는지 보여줍니다. 출처는 창작의 순간 하드웨어에 각인되고, 진본성은 물리적 기기로 보장되며, 가치는 체인 위에서 투명하게 추적되고 공정하게 분배됩니다.

표 2: 콘텐츠 진본성 솔루션 비교 분석

기능	AHNIST (특허 기반)	C2PA / CAI	Numbers Protocol	기타 DID 솔루션
핵심 원리	하드웨어 기반 원본 증명	파일 메타데이터 부착	NFT 기반 등록	디지털 신원 증명
원본 증명 방식	윌렛 내 불변의 원본 존재	파일 내/외부 메타데이터	블록체인 상 NFT 발행	해당 없음
메타데이터 제거 취약성	면역 (Immune)	높음 (High) - 스크린샷, 형식 변환 시 제거	중간 (Medium) - NFT와 자산 분리 가능	해당 없음
신원 책임성	물리적 기기 연동 AID	서명자 평판에 의존	NFT 소유자 주소	물리적 주체 부재, 익명 생성 가능
IP 추적 및 라이선싱	체인 기반 자동화	기능 부재 (수동/오프체인)	NFT 거래 내역으로 제한적 추적	기능 부재
창작자 수익 분배	P2P 직접 거래	플랫폼 중개 방식	NFT 거래 수수료	해당 없음
법적 집행력	강력함 - 명확한 증거 사슬	취약함 - 증거 사슬 단절 용이	중간 - 블록체인 로그 활용	취약함

출처: AHNIST IR 자료 ⁵ 및 C2PA 기술 분석 ³⁰ 기반 재구성

결론: 지속 가능하고 공정한 AI 미래를 향한 제언

현재 AI 생태계가 걷고 있는 길은 지속 가능하지 않습니다. 출처를 알 수 없는 데이터 위에 세워지고, 진실과 거짓의 경계가 무너지고 있으며, 창작자의 노동을 정당한 대가 없이 착취하는 현재의 패러다임은 법적으로, 사회적으로, 그리고 윤리적으로 거대한

위기를 내포하고 있습니다.

이제 우리는 선택의 기로에 서 있습니다. 이는 단순히 어떤 기술이나 제품을 선택하는 문제가 아닙니다. 혼돈과 착취로 점철된 미래와, 질서와 공정함에 기반한 미래 사이의 선택입니다.

AHNIST가 제안하는 것은 단순한 앱이나 서비스가 아닙니다. 이는 왜곡된 디지털 경제의 구조를 바로잡고, 기술의 혜택이 소수가 아닌 모두에게 돌아가야 한다는 확고한 철학에서 출발한 ‘사회 혁신 운동’입니다.⁵ AHNIST의 기술은 디지털 시대에 필수적인 새로운 사회적 인프라, 즉 신뢰할 수 있고 공정한 AI 생태계를 가능하게 하는 진정한 ‘메타-인프라스트럭처’를 제공합니다. 이 기술은 웹의 창시자들이 꿈꿨던 탈중앙화된 민주주의적 인터넷의 이상을 실현하고, 모든 창작자의 권리가 존중받는 새로운 시대를 여는 첫걸음이 될 것입니다.

참고 자료

1. Foundation model - Wikipedia, 7 월 14, 2025 에 액세스, https://en.wikipedia.org/wiki/Foundation_model
2. Reflections on Foundation Models | Stanford HAI, 7 월 14, 2025 에 액세스, <https://hai.stanford.edu/news/reflections-foundation-models>
3. What Are Foundation Models? - IBM, 7 월 14, 2025 에 액세스, <https://www.ibm.com/think/topics/foundation-models>
4. What Are Foundation Models? | NVIDIA Blogs, 7 월 14, 2025 에 액세스, <https://blogs.nvidia.com/blog/what-are-foundation-models/>
5. 사업계획서_통합버전_20250623.pdf
6. AI Tech Stack Solutions - Intel, 7 월 14, 2025 에 액세스, <https://www.intel.com/content/www/us/en/learn/ai-tech-stack.html>
7. The AI Tech Stack: A Business Guide to the Moving Parts of the AI Ecosystem, 7 월 14, 2025 에 액세스, <https://www.pymnts.com/news/artificial-intelligence/2025/ai-tech-stack-business-guide/>
8. AI Tech Stack: A Guide to Frameworks & Best Practices, 7 월 14, 2025 에 액세스, <https://www.spaceo.ai/blog/ai-tech-stack/>
9. The New York Times v. OpenAI: The Biggest IP Case Ever - Sunstein LLP, 7 월 14, 2025 에 액세스,

<https://www.sunsteinlaw.com/publications/the-new-york-times-v-openai-the-biggest-ip-case-ever>

10. The New York Times Case against OpenAI is Different. Here's Why. - Patent Docs, 7 월 14, 2025 에 액세스,
<https://www.patentdocs.org/2024/02/the-new-york-times-case-against-openai-is-different-heres-why.html>
11. NYT v. OpenAI: The Times's About-Face - Harvard Law Review, 7 월 14, 2025 에 액세스,
<https://harvardlawreview.org/blog/2024/04/nyt-v-openai-the-timess-about-face/>
12. AI and intellectual property rights - Dentons, 7 월 14, 2025 에 액세스,
<https://www.dentons.com/ru/insights/articles/2025/january/28/ai-and-intellectual-property-rights>
13. AI, Copyright, and the Law: The Ongoing Battle Over Intellectual Property Rights, 7 월 14, 2025 에 액세스,
<https://sites.usc.edu/ip/2025/02/04/ai-copyright-and-the-law-the-ongoing-battle-over-intellectual-property-rights/>
14. Getty Images v Stability AI: main copyright claims dropped - Pinsent Masons, 7 월 14, 2025 에 액세스,
<https://www.pinsentmasons.com/out-law/news/getty-images-stability-ai-copyright-claims-dropped>
15. Navigating representative actions: takeaways from Getty Images v Stability AI, 7 월 14, 2025 에 액세스,
<https://www.hsframer.com/notes/ip/2025-01/navigating-representative-actions-takeaways-from-getty-images-v-stability-ai>
16. How Do Deepfakes Affect Media Authenticity? - Identity.com, 7 월 14, 2025 에 액세스,
<https://www.identity.com/deepfake-ai-how-verified-credentials-enhance-media-authenticity/>
17. How Deepfakes Are Impacting Public Trust in Media - Pindrop Security, 7 월 14, 2025 에 액세스,
<https://www.pindrop.com/article/deepfakes-impacting-trust-media/>
18. Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions - PubMed Central, 7 월 14, 2025 에 액세스,
<https://pmc.ncbi.nlm.nih.gov/articles/PMC9453721/>

19. Understanding the Impact of AI-Generated Deepfakes on Public Opinion, Political Discourse, and Personal Security in Social Media - IEEE Computer Society, 7 월 14, 2025 에 액세스,
<https://www.computer.org/csdl/magazine/sp/2024/04/10552098/1XApkaTs5l6>
20. 32+ Creator Economy Statistics of 2025 (Market Size Data) - Demand Sage, 7 월 14, 2025 에 액세스,
<https://www.demandsage.com/creator-economy-statistics/>
21. Creator Economy Statistics 2024: Everything You Need to Know - Shanna Lindinger, 7 월 14, 2025 에 액세스,
<https://www.shannalindinger.com/articles/creator-economy-statistics>
22. 22 Eye-Opening Creator Economy Statistics (2025 Data) - Blogging Wizard, 7 월 14, 2025 에 액세스,
<https://bloggingwizard.com/creator-economy-statistics/>
23. Duetti's 2024 Music Economics Report Finds Industry-Wide Per Stream Rates for Independent Artists Are Finally Stabilizing Following Years of Decline - PR Newswire, 7 월 14, 2025 에 액세스,
<https://www.prnewswire.com/news-releases/duettis-2024-music-economics-report-finds-industry-wide-per-stream-rates-for-independent-artists-are-finally-stabilizing-following-years-of-decline-302358273.html>
24. Streaming Music Revenue Shows Sluggish Growth in 2024 as Industry Faces New Challenges - Vinyl Me, Please, 7 월 14, 2025 에 액세스,
<https://www.vinylmeplease.com/blogs/music-industry-news/streaming-music-revenue-shows-sluggish-growth-in-2024-as-industry-faces-new-challenges>
25. C2PA | Verifying Media Content Sources, 7 월 14, 2025 에 액세스,
<https://c2pa.org/>
26. The Content Authenticity Initiative - Transparency in the Age of AI - YouTube, 7 월 14, 2025 에 액세스, <https://www.youtube.com/watch?v=q2VpOuctSF4>
27. Content Credentials, 7 월 14, 2025 에 액세스, <https://contentcredentials.org/>
28. C2PA Specifications :: C2PA Specifications, 7 월 14, 2025 에 액세스,
<https://c2pa.org/specifications/specifications/2.2/index.html>
29. How it works - Content Authenticity Initiative, 7 월 14, 2025 에 액세스,
<https://contentauthenticity.org/how-it-works>
30. The Role of Blockchain in Securing Content Without C2PA Labels - Numbers Protocol, 7 월 14, 2025 에 액세스,
<https://www.numbersprotocol.io/blog/blockchain-secures-content-without-c2>

[pa](#)

31. Unable to apply Content Credentials - Adobe Support, 7 월 14, 2025 에 액세스,
<https://helpx.adobe.com/creative-cloud/help/cai/unable-to-apply-content-credentials.html>
32. How C2PA can safeguard the truth from digital manipulation - SC Media, 7 월 14, 2025 에 액세스,
<https://www.scworld.com/perspective/how-c2pa-can-safeguard-the-truth-from-digital-manipulation>
33. Research Integrity, Image Manipulation, Content Provenance and the C2PA, 7 월 14, 2025 에 액세스,
<https://scholarlykitchen.sspnet.org/2025/03/13/research-integrity-content-provenance-and-c2pa/>
34. Frequently-asked questions | Open-source tools for content authenticity and provenance, 7 월 14, 2025 에 액세스,
<https://opensource.contentauthenticity.org/docs/faqs/>
35. Do not strip C2PA manifests from EXIF of uploaded photos · Issue #35100 - GitHub, 7 월 14, 2025 에 액세스,
<https://github.com/mastodon/mastodon/issues/35100>
36. C2PA Security Considerations, 7 월 14, 2025 에 액세스,
https://c2pa.org/specifications/specifications/1.0/security/Security_Considerations.html
37. C2PA Security Considerations, 7 월 14, 2025 에 액세스,
https://c2pa.org/specifications/specifications/2.0/security/Security_Considerations.html