



저작권 이슈 브리프

SUMMARY

산업/기업

기술

기업 시댄스 2.5 사례로 본 생성 후 차단 방식의 성과와 저작물 학습 문제

▶ 중국 IT 기업 바이트댄스의 AI 영상 생성 모델 시댄스 2.0이 저작물을 그대로 재현한 영상을 대량 생성하자, 미국영화협회는 바이트댄스에 침해 중단을 요구하는 서한을 보냈다. 이후 출시된 시댄스 2.5를 VN.ai가 검증한 결과, 저작물이 포함된 영상을 요구한 프롬프트의 약 80%가 차단돼 이전 모델보다 일관된 성능이 확인되었다. 다만 이 차단은 모델이 영상을 우선 생성한 뒤 저작물을 인식해 제공하지 않는 생성 후 차단 방식으로, 저작물을 학습 데이터로 활용했을 가능성을 보여주며 명칭을 피한 프롬프트로 우회될 수 있다는 한계도 드러났다. 바이트댄스는 2026년 8월 미국영화협회와 저작권 안전장치를 강화하는 첫 협약을 체결했으나, 학습 단계의 저작물 이용 문제와 외부 검증을 통한 안전장치 확인은 과제로 남아 있다.

기업 애플뮤직 사례로 본 AI 생성 음원의 태그 기반 표시 확대

▶ AI 음악 생성 서비스가 확산되면서 음원의 AI 사용 여부를 표기하라는 요구가 커지고 있으나, 생성 단계에서 식별 신호를 삽입하는 방식은 아직 널리 보급되지 않았다. 이런 가운데 애플뮤직은 2026년 3월 도입 후 이용자에게 공개하지 않았던 AI 투명성 태그를 연내 ‘메이드 위드 AI’ 라벨로 표시하고, 태그 제출도 권고에서 필수 요건으로 전환하기로 했다. 이 방식은 별도의 탐지 기술 없이 음원과 작곡, 아트워크, 뮤직비디오 단위까지 AI 사용 여부를 표시할 수 있다는 이점이 있다. 다만 애플뮤직이 AI 생성 음원을 직접 탐지하지 않아 태그가 제출되지 않은 음원은 라벨 없이 유통될 수 있다. 이에 따라 표기 체계의 신뢰도는 태그 제출의 이행과 생성 단계 마킹 기술의 보급에 달려 있다.

기업 클라우드플레이어의 페이 퍼 유즈 도입에서 나타난 AI 크롤러 보상 기준의 전환

▶ AI 크롤러가 콘텐츠를 대량으로 수집하자 클라우드플레이어는 2025년부터 이를 기본 차단하고, 크롤 건당 요금을 부과하는 ‘페이 퍼 크롤’을 제시했다. 그러나 크롤러 접근의 절반 이상이 갱신되지 않은 정보를 반복 수집하는 것으로 나타나, 크롤 횟수만으로는 콘텐츠의 실제 사용량을 파악하기 어려웠다. 이에 클라우드플레이어는 2026년 7월 콘텐츠가 AI 답변에 사용됐는지를 기준으로 보상하는 ‘페이 퍼 유즈’로 방향을 전환하고, 사용 여부를 확인하는 대시보드도 공개했다. 다만 참여 사업자 밖에서 이뤄지는 사용은 확인하기 어렵고, 신원을 숨긴 크롤링도 정확한 계측을 제약한다. 이에 따라 보상 체계의 정착 여부는 크롤러의 용도 구분과 콘텐츠 사용량의 정확한 계측에 달려 있다.



저작권 이슈 브리프

SUMMARY

산업/기업

기술

산업 아소보 신작 레조넌스 PC 버전 유출, 출시 전 복제 방지 공백

▶ 2026년 들어 주요 게임이 예정된 출시일 전에 온라인으로 유출되는 사례가 이어지고 있다. 이런 가운데 아소보 스튜디오의 레조넌스는 PC 버전에 복제 방지 기술 데누보를 적용하지 않았으며, 스팀의 기본 DRM만 적용된 빌드는 등장 직후 우회돼 공식 출시일보다 7일 먼저 유통됐다. 복제본은 온라인 커뮤니티를 통해 확산됐고, 유출본을 실행한 이용자들의 성능 평가까지 정식 판매 전에 공개됐다. 그러나 이미 배포된 파일을 회수할 수단이 없어 개발사와 유통사는 확산에 제대로 대응하지 못했으며, 매출 영향도 게임과 이용자층에 따라 달라 단정하기 어려운 상태다. 이 사례는 보호 수단의 적용 여부를 비용과 성능 부담만으로 판단하기 어렵고, 출시 전 배포되는 프리로드의 보안을 스팀의 기본 보호와 별도로 확보해야 함을 보여준다.

산업 닌텐도의 저장소 대량 삭제 사례로 본 오픈소스 코드의 잔존

▶ 닌텐도는 2026년 8월 17일 깃허브에 우회 방지 통지 7건을 제출해 스위치 에뮬레이터 코드 저장소 400여 개를 하루 만에 삭제했다. 규모가 가장 큰 통지는 에뮬레이터 수유를 대상으로 했으며, 삭제 대상 네트워크가 100개를 넘어 이 한 건에서만 311개가 삭제됐다. 반면 상위 저장소 한 곳만 대상으로 삼은 통지도 있어 건별 삭제 범위의 차이가 컸다. 삭제 대상에는 2023년 개발이 중단된 스카이라인처럼 오래전 멈춘 프로젝트의 코드까지 포함돼, 한 차례의 조치로 대응이 끝나지 않음을 보여준다. 통지가 새로운 포크와 복제본의 등장 속도를 따라가지 못하는 만큼, 저장소를 삭제하는 일보다 코드의 재확산을 막는 일이 더 큰 과제로 남았다.

기술 주간 기술 동향

▶ AI가 생성한 음성이 사람의 목소리와 구분하기 어려워지면서, 유통 중인 음성이 어떤 모델에서 만들어졌는지 확인할 기술적 수단이 요구되고 있다. 기존 워터마킹은 완성된 음성을 변형해 표식을 삽입하거나 생성 모델을 재학습해야 해 음질 저하와 학습 비용 문제를 피하기 어려웠다. 오디오노이즈프린츠는 음성 생성이 무작위 잡음에서 시작된다는 점에 주목한다. 완성된 음성에 출발점이 된 잡음의 특성이 남는 성질을 이용해, 미리 정한 잡음을 표식으로 삼고 유사도 계산만으로 생성 모델을 판별하는 방식이다. 모델을 다시 학습시키거나 완성된 음성을 변형할 필요도 없다. 실험에서는 재생 속도나 길이를 바꾼 음성에서도 기존 방식보다 높은 판별 성능을 보였다.



저작권 이슈 브리프

SUMMARY

산업/기업

기술

시댄스 2.5 사례로 본 생성 후 차단 방식의 성과와 저작물 학습 문제

시댄스 2.0의 저작물 무단 재현 논란과 후속 모델의 외부 검증

• 저작물 무단 재현 영상의 대량 생성 문제

- 중국 IT 기업 바이트댄스(ByteDance)의 AI 영상 생성 모델 시댄스(Seedance) 2.0이 저작물을 그대로 재현한 영상을 대량 생성하면서 논란이 불거짐. 할리우드 배우 톰 크루즈(Tom Cruise)와 브래드 피트(Brad Pitt)가 싸우는 영상이 널리 확산된 사례가 대표적임
- 이에 미국 영화 및 TV 산업 단체 미국영화협회(Motion Picture Association, MPA)는 2026년 2월 바이트댄스에 저작물의 무단 이용 중단을 요구하는 서한을 보냄¹⁾
- 이는 미국영화협회가 주요 AI 기업에 이러한 공식 서한을 보낸 첫 사례로, 개별 침해 논란이 권리자 단체 차원의 공식 대응으로 확대됨
- 바이트댄스는 안전장치를 강화하겠다는 입장을 밝혔으나, 이후 자사 이미지 생성 모델 시드림(Seedream) 5.0의 외부 검증에서 프롬프트(prompt)*를 변형한 우회 생성이 가능한 것으로 확인됨. 이에 따라 안전장치가 실제로 개선됐는지 확인할 필요성이 커짐

* 프롬프트(prompt): 이용자가 AI 모델에 원하는 결과물을 지시하기 위해 입력하는 명령 문장

• 후속 모델 시댄스 2.5 출시와 외부 검증의 진행

- 이러한 논란 속에서 바이트댄스는 2026년 7월 말 시댄스 2.0의 후속 영상 생성 모델 시댄스 2.5를 출시함²⁾. 침해 논란과 개선 약속 이후 선보인 모델인 만큼, 안전장치 강화가 실제로 반영됐는지가 곧바로 검증 대상이 됨
- 실제로 생성형 AI 도구의 저작물 무단 이용 여부를 검증하는 기술 스타트업 VN.ai가 시댄스 2.5의 저작물 차단 성능을 검증했으며, 미국 연예 전문 매체 데드라인(Deadline)이 그 결과를 단독 보도함²⁾

검증으로 드러난 생성 후 차단 방식의 성과와 한계

• 일관된 수준으로 확인된 저작물 차단 성과

- VN.ai의 검증 결과에 따르면, 시댄스 2.5는 저작물이 포함된 영상을 요구한 프롬프트 중 약 80%에 대해 결과물을 이용자에게 제공하지 않는 것으로 나타남. 이러한 차단 성능은 시댄스 2.0과 시드림 5.0 등 바이트댄스의 이전 모델보다 훨씬 일관된 수준으로 평가됨²⁾

1) Wendy Lee, "Hollywood strikes first AI copyright truce with ByteDance", Los Angeles Times, 2026.08.17., <https://www.latimes.com/entertainment-arts/business/story/2026-08-17/motion-picture-association-reaches-agreement-with-bytedance-over-ai-guardrails>

2) Jake Kanter, "After Chaos Of Cruise Vs Pitt AI Deepfakes, Seedance 2.5 Is Now Blocking Hollywood Rip-Offs", Deadline, 2026.08.12., <https://deadline.com/2026/08/seedance-blocking-hollywood-ripoff-cruise-pitt-ai-deepfakes-1237031665/>

- 특히 검증 과정에서 저작물 이미지를 입력해 영상을 생성하려 한 시도는 시덴스 2.5가 모두 차단한 것으로 확인됨. 이로써 기존 이미지를 바탕으로 저작물을 재현하는 경로는 사실상 막힌 것으로 평가됨

• 생성된 영상을 인식해 제공을 거부하는 방식이 드러낸 저작물 학습 가능성

- 다만 VN.ai에 따르면 이러한 차단은 시덴스 2.5가 프롬프트 입력 단계에서 요청을 거부하는 방식이 아님. 검증 과정에서 모델은 요청된 영상을 우선 생성한 뒤, 결과물에 포함된 저작물을 스스로 인식하면 제공을 거부하는 방식으로 작동함
- VN.ai는 이 같은 차단을 모델 능력에 따른 부수적 결과로 설명함. 모델이 저작물을 정확히 재현할 수 있고, 생성된 영상에서도 이를 인식할 수 있기 때문에 침해 영상의 제공을 차단한다는 것임
- 이처럼 검증에서 확인된 저작물 재현 능력은 시덴스 2.5가 저작물을 학습 데이터로 활용했을 가능성을 보여줌. 따라서 결과물 제공 차단과 별개로, 학습 단계에서의 저작물 이용은 권리자에게 여전히 문제로 남을 수 있음

• 우회 생성의 한계와 미국영화협회와의 협약 체결

- 아울러 검증에서는 생성 후 차단이 모든 우회 시도를 막지는 못한다는 점도 드러남. VN.ai가 작품명과 캐릭터명을 쓰지 않고 영화 샤크 테일(Shark Tale)의 캐릭터 오스카(Oscar)를 묘사한 프롬프트를 입력하자 시덴스 2.5가 영상을 제공해, 명칭을 피한 프롬프트로 차단을 우회할 수 있음이 확인됨³⁾
- 이러한 검증 결과에 대해 바이트댄스 대변인은 저작물의 무단 이용을 방지하는 안전장치를 갖춰 모델을 출시하고 있으며, 창작 업계와 협력해 이를 지속적으로 강화하겠다고 밝힘
- 이후 바이트댄스와 미국영화협회는 2026년 8월 17일 시덴스와 시드림 모델의 저작물 보호 안전장치를 강화하기 위한 협약을 체결함⁴⁾. 이는 미국영화협회가 AI 기업과 맺은 첫 협약으로, 양측은 AI 기술 발전에 맞춰 안전장치 협력을 지속하겠다고 발표함

생성 후 차단 방식이 남긴 학습 문제와 검증 과제

• 생성 후 차단만으로 해소되지 않는 학습 단계의 저작물 이용 문제

- 이번 검증은 생성 후 차단이 침해 영상의 제공을 상당 부분 막을 수 있음을 보여주는 동시에, 그 차단 능력이 저작물 학습에서 비롯됐을 가능성도 드러냄. 이에 따라 침해 영상의 제공을 차단하는 문제와 학습 단계에서 저작물을 이용하는 문제는 별개의 쟁점으로 남게 됨
- 권리자들은 AI 모델이 허락이나 보상 없이 저작물을 학습에 이용하는 데 지속적으로 우려를 제기해 옴. 제공 차단의 성과와 별개로, 학습 데이터 이용을 둘러싼 논의는 계속될 것으로 보임

• 외부 검증과 권리자 협력을 통한 안전장치 보완의 필요성

- 한편 AI 기업들이 고객 확보 경쟁 속에서 안전장치를 충분히 갖추지 않은 채 제품을 서둘러 출시하는 사례가 있음. 이러한 상황에서 출시 이후 실제 성능을 확인하는 외부 검증은 개선을 이끄는 수단이 될 수 있음

3) Jake Kanter, "After Chaos Of Cruise Vs Pitt AI Deepfakes, Seedance 2.5 Is Now Blocking Hollywood Rip-Offs", Deadline, 2026.08.12., <https://deadline.com/2026/08/seedance-blocking-hollywood-ripoff-cruise-pitt-ai-deepfakes-1237031665/>

4) Reuters, "ByteDance signs AI copyright pact with Hollywood trade group", Reuters, 2026.08.17., <https://www.reuters.com/legal/litigation/bytedance-signs-ai-copyright-pact-with-hollywood-trade-group-2026-08-17/>

- 또한 이번 협약에 따른 구체적인 안전장치가 공개되지 않은 만큼, 이행 여부도 이번 사례와 같은 외부 검증을 통해 확인할 필요가 있음. 양측이 지속적인 협력을 약속한 가운데, 안전장치 보완이 사업자 단독 대응을 넘어 권리자와의 협력으로 이어질지가 향후 과제로 남음

참고문헌

- Jake Kanter, "After Chaos Of Cruise Vs Pitt AI Deepfakes, Seedance 2.5 Is Now Blocking Hollywood Rip-Offs", Deadline, 2026.08.12., <https://deadline.com/2026/08/seedance-blocking-hollywood-rip-off-cruise-pitt-ai-deepfakes-1237031665/>
- Wendy Lee, "Hollywood strikes first AI copyright truce with ByteDance", Los Angeles Times, 2026.08.17., <https://www.latimes.com/entertainment-arts/business/story/2026-08-17/motion-picture-association-reaches-agreement-with-bytedance-over-ai-guardrails>
- Reuters, "ByteDance signs AI copyright pact with Hollywood trade group", Reuters, 2026.08.17., <https://www.reuters.com/legal/litigation/bytedance-signs-ai-copyright-pact-with-hollywood-trade-group-2026-08-17/>



저작권 이슈 브리프

SUMMARY

산업/기업

기술

애플뮤직 사례로 본 AI 생성 음원의 태그 기반 표시 확대

AI 생성 음원의 확산과 판별 수단의 미비

• AI 음악 생성 서비스의 확산에 따른 음원 표시 요구의 대두

- AI 음악 생성 서비스 수노(Suno)와 유디오(Udio)가 확산되면서, 음반사와 스트리밍 업체는 최근 3년간 소송 제기과 라이선스 계약 체결 등으로 대응해 옴. 다만 이용자가 음원 제작에 AI가 사용됐는지 확인할 수단은 충분치 않아 별도의 표시가 필요하다는 요구가 제기됨
- 이에 미국 음반산업협회(Recording Industry Association of America, RIAA)를 비롯한 음악 산업 단체들은 2026년 7월 주요 스트리밍 서비스에 AI 생성 음원의 표시 체계를 도입할 것을 공동으로 요구함¹⁾. 이를 계기로 관련 표시가 개별 서비스의 선택을 넘어 업계 공통 과제로 논의되기 시작함

• 생성 단계의 식별 기술 도입 지연과 유통 단계 표시의 시작

- AI 사용 여부를 표시하려면 먼저 이를 판별할 수 있어야 하나, 생성 단계에서 식별 신호를 삽입하는 기술은 아직 널리 보급되지 않음. 수노의 경우 2026년 8월 6일 오디오 워터마킹(audio watermarking)*과 오디오 핑거프린팅(audio fingerprinting)**을 도입하겠다고 예고한 단계임²⁾
- 유통 단계에서는 스트리밍 서비스들이 자체 기준에 따라 AI 생성 음원을 표시하기 시작함. 미국의 정보기술 기업 애플(Apple)의 음악 스트리밍 서비스 애플뮤직(Apple Music)도 2026년 8월 20일 '메이드 워드 AI(Made With AI)' 라벨 도입 계획을 업계 파트너에게 알림²⁾

* 오디오 워터마킹(audio watermarking): 음원에 사람이 알아채기 어려운 식별 신호를 삽입하는 기술

** 오디오 핑거프린팅(audio fingerprinting): 음원의 소리 특징을 추출해 동일한 음원을 찾아내는 기술

애플뮤직의 태그 기반 표시 방식과 이점 및 제약

• AI 투명성 태그를 이용자 화면의 라벨로 확대 적용

- 애플뮤직은 2026년 3월 음반사와 유통사가 음원을 납품할 때 AI 사용 여부를 표시하도록 AI 투명성 태그(AI Transparency Tags)*를 도입함. 그동안 이 태그는 이용자에게 공개되지 않았으나, 연내 '메이드 워드 AI' 라벨로 이용자 화면에 표시될 예정임

1) Variety, "Apple Music to Label AI-Made Tracks", 2026.08.20., <https://variety.com/2026/music/news/apple-music-to-label-ai-made-tracks-1236839371/>

2) Tim Ingham, "Apple Music to slap AI labels on Suno tracks - but pushes the onus onto record companies", Music Business Worldwide, 2026.08.20., <https://www.musicbusinessworldwide.com/apple-music-to-slap-on-suno/>

- 이용자에게 공개되는 정보의 범위가 넓어지는 동시에 태그 제출의 성격도 달라짐. 2026년 3월에는 AI로 상당 부분 생성한 콘텐츠에 태그를 제출하도록 권고하는 수준이었으나, 8월에는 음반사와 유통사가 태그를 제출하도록 의무화됨
- 태그 적용 대상도 구체화됨. 애플은 'AI 플랫폼 생성 콘텐츠(AI-platform-generated content)'를 생성형 AI 서비스에서 주로 파생된 콘텐츠로 정의하고, 해당 서비스로 생성한 음원을 태그 제출 대상에 포함함

* AI 투명성 태그(AI Transparency Tags): 음반사와 유통사가 콘텐츠 납품 시 AI 사용 여부를 표시하는 메타데이터

• 음반사와 유통사의 태그 제출을 표시 근거로 활용

- 애플은 음반사와 유통사가 콘텐츠의 제작 과정을 가장 잘 파악할 수 있는 주체라는 점을 이러한 방식의 근거로 제시함. 유통 이후 AI 사용 여부를 별도로 판별하기보다 제작 단계에서 확보한 정보를 표시에 활용하는 방식임
- 별도의 탐지 기술을 구축하지 않고 기존 태그를 그대로 활용할 수 있다는 점도 이점임. 또한 태그가 음원과 작곡, 아트워크(artwork), 뮤직비디오(music video) 단위로 구분돼 있어 콘텐츠의 어느 부분에 AI가 사용됐는지까지 표시할 수 있음

• 태그 제출 여부에 따라 달라지는 표시 범위

- 반면 애플뮤직은 라벨을 부착하기 위해 AI 생성 음원을 직접 탐지하지 않으므로, 태그가 제출되지 않은 음원은 라벨 없이 유통될 수 있음. 이에 따라 실제 표시 범위가 음반사와 유통사의 태그 제출 여부에 좌우되는 한계가 있음
- 이는 자체 판별 절차를 병행하는 다른 음악 스트리밍 서비스와 구별되는 지점임. 스포티파이(Spotify)는 제작 주체의 신고뿐 아니라 프로필을 직접 검토해 AI 여부를 판단하며, 디저(Deezer)는 자체 기술로 AI 생성이 의심되는 음원을 탐지해 표시함

[표 1] 주요 음악 스트리밍 서비스의 AI 생성 음원 표시 방식

구분	애플뮤직	스포티파이	디저
표시 대상	음원, 작곡, 아트워크, 뮤직비디오	아티스트 프로필, 음원 크레딧	AI 생성이 의심되는 음원
판별 방식	음반사와 유통사의 태그 제출	프로필은 자체 검토, 음원은 제작 주체의 크레딧 기재	자체 기술 탐지
이용자 표시	연내 메이드 위드 AI 라벨 표시 예정	프로필 배지 및 곡 크레딧 표시	음원에 AI 생성 의심 표시

출처: Tim Ingham, "Apple Music to slap AI labels on Suno tracks - but pushes the onus onto record companies", Music Business Worldwide, 2026.08.20., <https://www.musicbusinessworldwide.com/apple-music-to-slap-on-suno/>

시사점: 표시 범위 확대와 생성 단계 식별 기술의 연계 과제

• 라벨이 없는 음원에 대한 이용자 안내 기준 마련 필요

- 애플뮤직의 라벨은 음반사와 유통사가 제공한 정보를 바탕으로 표시되므로, 라벨이 없다는 이유만으로 AI를 사용하지 않은 음원이라고 판단하기는 어려움. 이용자가 라벨 부재를 AI가 사용되지 않았다는 의미로 받아들이지 않도록 명확한 안내 기준을 마련할 필요가 있음

- AI 사용 여부를 표시하는 라벨과 AI를 사용하지 않았음을 나타내는 라벨은 전달하는 정보가 서로 다를 수 있음. 이에 따라 이용자가 각 표시의 의미를 쉽게 구분할 수 있도록 적용 기준과 범위를 명확히 제시할 필요가 있음

• 생성 단계의 식별 정보와 유통 단계 메타데이터의 연계 필요

- 오디오 워터마킹과 같은 생성 단계 식별 기술이 보급되면, 음반사와 유통사가 AI 사용 여부를 판별할 때 참고할 수 있는 추가 근거가 마련될 수 있음. 이는 음반사와 유통사의 정보 입력에 의존하는 현행 방식을 보완하는 수단이 될 수 있음
- 장기적으로는 생성 단계에서 확보한 식별 정보를 유통 단계의 메타데이터(metadata)와 연계하는 체계를 마련할 필요가 있음. AI 음악 생성 서비스와 스트리밍 서비스의 정보 체계가 긴밀하게 연결될수록 AI 사용 여부를 이용자에게 전달하는 과정의 신뢰성도 높아질 것으로 보임

참고문헌

- Tim Ingham, "Apple Music to slap AI labels on Suno tracks - but pushes the onus onto record companies", Music Business Worldwide, 2026.08.20., <https://www.musicbusinessworldwide.com/apple-music-to-slap-on-suno/>
- Variety, "Apple Music to Label AI-Made Tracks", 2026.08.20., <https://variety.com/2026/music/news/apple-music-to-label-ai-made-tracks-1236839371/>



저작권 이슈 브리프

SUMMARY

산업/기업

기술

클라우드플레어의 페이 퍼 유즈 도입에서 나타난 AI 크롤러 보상 기준의 전환

AI 크롤링 확산과 크롤 횟수 기준 보상 방식의 한계

• 봇 트래픽 증가에 따른 AI 크롤러 기본 차단 확산

- AI 서비스가 답변 생성에 웹사이트 콘텐츠를 수집 및 활용하면서도 이에 대한 보상이 이뤄지지 않는 문제가 제기됨. 이에 사이트 운영자들은 검색과 AI 서비스에서의 노출은 유지하되 무단 활용은 제한하고, 콘텐츠 이용에 대한 통제권과 보상 체계를 확보할 필요성이 커짐
- 전 세계 웹사이트 약 20%에 서비스를 제공하는 웹 보안 및 인프라 기업 클라우드플레어(Cloudflare)는 2025년부터 사이트 운영자가 별도로 허용하지 않는 한 AI 크롤러(AI crawler)*를 기본 차단하는 조치를 시행함
- 이에 더해, 봇 트래픽(bot traffic)**이 사람의 접속량을 넘어서자 클라우드플레어는 차단 범위를 확대함. 클라우드플레어는 지속 가능한 이용 환경이 자리 잡기 위해 대응을 앞당겨야 한다고 밝힘

* AI 크롤러(AI crawler): AI 서비스의 학습이나 답변 생성에 사용할 콘텐츠를 웹사이트에서 자동으로 수집하는 프로그램

** 봇 트래픽(bot traffic): 사람이 아닌 자동 프로그램이 웹사이트에 접속해 발생하는 트래픽

• 크롤 횟수를 기준으로 한 보상 방식의 한계

- AI 크롤러의 기본 차단은 콘텐츠 이용 계약에 관한 논의로 이어짐
- 클라우드플레어는 AI 크롤러의 접근 여부를 확인할 수 있어 예측이 쉽다는 점을 고려해, 우선 사이트 운영자가 허용한 크롤러에 크롤 횟수에 따라 요금을 부과하는 콘텐츠 보상 방식 '페이 퍼 크롤(Pay Per Crawl)'을 제시함¹⁾
- 그러나 클라우드플레어의 자체 데이터를 분석한 결과, AI 크롤러가 접근한 정보 중 절반 이상은 직전 접근 이후 갱신되지 않은 것으로 나타남. 이에 따라 크롤 횟수만으로 콘텐츠의 실제 사용 정도를 판단하기 어렵다는 한계가 확인됨¹⁾

1) Charlotte Tobitt, "Cloudflare says bot blocking is fuelling publisher AI deals", Press Gazette, 2026.08.17., <https://pressgazette.co.uk/platforms/cloudflare-says-bot-blocking-is-fueling-publisher-ai-deals/>

AI 콘텐츠 보상 기준의 전환과 사용 계측 수단의 확대

• AI 답변에서의 실제 사용으로 이동하는 보상 기준

- 클라우드플레어는 2026년 7월 1일 콘텐츠가 AI 답변 등에 실제로 사용돼 직접적인 가치를 창출한 경우를 기준으로 사이트 운영자에게 보상하도록 페이 퍼 크롤을 '페이 퍼 유즈(Pay Per Use)'로 발전시키겠다는 구상을 제시함
- 초기 실험은 AI 검색 서비스 세라믹AI(Ceramic.ai)와 기업용 AI 검색 서비스 유닷컴(You.com)을 대상으로 진행됨. 사이트 운영자가 페이 퍼 유즈 적용을 선택하면 세라믹AI의 검색 결과에 해당 콘텐츠가 사용되거나 유닷컴이 유료 콘텐츠에 접근할 때 보상이 이뤄지는 방식임
- 콘텐츠 사용 여부를 계측하기 위한 수단도 함께 제공됨. 클라우드플레어는 AI 가시성 대시보드(AI visibility dashboard)*를 공개해 사이트 운영자가 자사 콘텐츠가 챗GPT(ChatGPT)와 클로드(Claude) 등 AI 서비스의 답변에 얼마나 자주 등장하는지 확인할 수 있도록 함

*AI 가시성 대시보드(AI visibility dashboard): 사이트 운영자가 자사 콘텐츠가 AI 서비스의 답변에 얼마나 등장하는지 확인할 수 있는 도구

[표 1] 페이 퍼 크롤과 페이 퍼 유즈의 보상 기준 비교

구분	페이 퍼 크롤	페이 퍼 유즈
보상 기준	크롤러의 콘텐츠 접근	AI 답변 등에서의 실제 사용
계측 방식	크롤 요청 발생 여부	콘텐츠 사용과 가치 창출 여부
운영 단계	비공개 베타	일부 AI 사업자와 초기 실험
주요 한계	크롤과 실제 사용이 불일치	참여 사업자 밖의 이용은 확인하기 어려움

출처: Sarah Perez, "Cloudflare's new policy pushes AI companies to pay for publishers' content", TechCrunch, 2026.07.01., <https://techcrunch.com/2026/07/01/cloudflares-new-policy-pushes-ai-companies-to-pay-for-publishers-content/>

• 신원을 위장하는 크롤링에 따른 사용 계측의 제약

- 한편 보상의 전제가 되는 AI 크롤러 식별에는 여전히 제약이 있음. 봇 트래픽 분석 기업 톨빗(TollBit)의 보고서에 따르면, 일부 AI 크롤러가 다른 사업자로 위장하거나 IP 주소를 변경하고 주거용 프록시(residential proxy)*를 활용하는 사례가 관측됨²⁾
- 클라우드플레어도 AI 검색 서비스 퍼플렉시티(Perplexity)가 네트워크 차단을 우회하는 과정에서 AI 크롤러 신원을 위장하는 것으로 보인다고 밝힌 바 있음. 이에 브라우저 내 이용자 세션을 분석해 일반 이용자로 위장한 접근을 식별하는 봇 관리 제품 프리커서(Precursor)**를 지속해서 개선하고 있음

* 주거용 프록시(residential proxy): 가정용 인터넷 회선의 주소를 거쳐 접속해 일반 이용자의 접속처럼 보이게 하는 우회 경로

** 프리커서(Precursor): 웹 브라우저 안에서 작동해 이용자 세션을 지속적으로 확인하고 사람처럼 행동하는 봇을 걸러내는 봇 관리 제품

²⁾ Charlotte Tobitt, "Cloudflare says bot blocking is fuelling publisher AI deals", Press Gazette, 2026.08.17., <https://pressgazette.co.uk/platforms/cloudflare-says-bot-blocking-is-fueling-publisher-ai-deals/>

계측 범위 확보와 크롤러 용도 구분의 과제

• 참여 서비스와 콘텐츠 유통 경로에 따라 달라지는 계측 범위

- 다만 페이 퍼 유즈는 참여 AI 사업자와 연계된 사례를 중심으로 콘텐츠 사용 여부를 계측하는 방식이므로, 비참여 사업자의 서비스에서 콘텐츠가 사용되는 경우까지 포괄하기 어려움. 초기 실험 단계라는 점도 보상 대상과 계측 범위를 제한하는 요인임
- 콘텐츠가 유통되는 경로 역시 계측 범위를 좌우함. 클라우드플레어는 자사 사이트에서 AI 크롤러를 차단하더라도 콘텐츠가 제3자 웹사이트를 통해 재유통될 수 있으므로, 사이트 운영자가 자사 콘텐츠의 실제 노출 경로를 별도로 확인할 필요가 있다고 지적함

• 크롤러 용도 구분과 사용 기반 계측 체계의 정착 필요성

- 사용 기반의 보상 방식이 제대로 작동하려면 AI 크롤러가 콘텐츠에 접근하는 목적부터 구분할 수 있어야 함
- 클라우드플레어는 2026년 9월 15일부터 광고 페이지에 접근하는 AI 크롤러 가운데 검색용은 허용하되, AI 학습용과 에이전트용, 혼합 용도 크롤러는 기본 차단할 예정임
- AI 크롤러가 용도별로 구분되면 사이트 운영자는 접근 목적에 따라 허용 여부를 정할 수 있음. 클라우드플레어는 이러한 구분이 정착되면 장기적으로 크롤 횟수와 실제 콘텐츠 사용 간 격차도 줄어들 것으로 전망함

참고문헌

- Sarah Perez, "Cloudflare's new policy pushes AI companies to pay for publishers' content", TechCrunch, 2026.07.01., <https://techcrunch.com/2026/07/01/cloudflares-new-policy-pushes-ai-companies-to-pay-for-publishers-content/>
- Charlotte Tobitt, "Cloudflare says bot blocking is fuelling publisher AI deals", Press Gazette, 2026.08.17., <https://pressgazette.co.uk/platforms/cloudflare-says-bot-blocking-is-fueling-publisher-ai-deals/>



저작권 이슈 브리프

SUMMARY

산업/기업

기술

아소보 신작 레조넌스 PC 버전 유출, 출시 전 복제 방지의 공백

게임 출시 전 유출과 데누보 미적용 사례 증가

• 2026년 주요 게임에서 출시 전 유출 사례 잇달아 발생

- 2026년에는 주요 게임의 파일과 영상이 예정된 출시일 전에 온라인으로 유출되는 사례가 이어지고 있음. 여러 대형 게임에서 유사한 사고가 반복되면서 개별 게임의 문제를 넘어 출시 전 배포 과정 전반의 취약점으로 지적됨
- 실제로 2026년 5월 ‘포르자 호라이즌 6(Forza Horizon 6)’는 155GB에 달하는 전체 프리로드(preload)* 파일이 암호화되지 않은 채 배포됐으며, ‘레고 배트맨(Lego Batman)’도 가정용 비디오 게임기 엑스박스(Xbox)의 이용자에게 출시 전에 유출됨
- 유출의 형태는 게임 파일에 국한되지 않음. ‘007 퍼스트 라이트(007 First Light)’는 초반부 영상이, ‘그랜드 테프트 오토 6(Grand Theft Auto 6)’는 무단 플레이 영상이 출시 전에 확산됨
- 유출 시점도 상업적으로 가장 중요한 출시 직전에 집중되고 있음. 특히 2026년 3분기에는 보호되지 않은 프리로드 파일이 유출로 이어질 수 있다는 점이 반복해서 확인됨¹⁾

* 프리로드(preload): 출시일 전에 이용자에게 미리 배포되는 게임 설치 파일

• 성능 저하 및 비용 부담으로 데누보 미적용 확대

- 이러한 유출에 대응해 업계가 활용해 온 수단은 복제 방지 기술 데누보(Denuvo)*임. 데누보는 출시 초기에 복제 방지 기술이 우회되는 것을 막아 판매가 집중되는 첫 주 동안 불법 복제를 억제하는 역할을 해 왔으나, 적용 시 게임 성능이 저하된다는 이용자들의 비판도 제기돼 옴
- 이에 개발사들이 라이선스 비용과 성능 부담, 유출 위험을 함께 고려해 데누보를 적용하지 않는 사례가 늘고 있음. 프랑스 게임 개발사 아소보 스튜디오(Asobo Studio)의 액션 게임 ‘레조넌스: 플레그 테일 레저시(Resonance: A Plague Tale Legacy, 이하 레조넌스)’도 PC 버전에 데누보를 적용하지 않음
- 대신 레조넌스 PC 버전은 PC 게임 유통 플랫폼 스팀(Steam)의 기본 디지털 권한 관리(Digital Rights Management, 이하 DRM)**만으로 보호됨. 그 결과 공식 출시일인 2026년 8월 27일보다 일주일 앞선 8월 20일 불법 파일 공유 사이트에 복제본이 유통된 것이 확인되면서 보호 공백이 드러남

* 데누보(Denuvo): 게임 파일의 변조와 보호 우회를 막기 위해 적용하는 안티탐퍼(anti-tamper) 방식의 복제 방지 기술

** 디지털 권한 관리(Digital Rights Management, DRM): 디지털 콘텐츠의 복제와 이용을 제한하는 저작권 관리 기술

1) Anton Kratiuk, "Resonance: A Plague Tale Legacy cracked a week before launch as DRM-free PC release backfires", Gagadget, 2026.08.20., <https://gagadget.com/en/722884-resonance-a-plague-tale-legacy-cracked-a-week-before-launch-as-drm-free-pc-release-backfires/>

레조넌스 PC 버전에서 확인된 보호 우회와 복제본 확산

• 스팀 기본 DRM만 적용된 PC 버전의 신속한 보호 우회

- 스팀의 기본 DRM만 적용된 레조넌스 PC 버전은 출시일을 일주일 앞두고 보호가 우회됨. 이에 따라 데누보와 같은 추가 수단 없이 기본 DRM만으로는 보호 우회 시점을 늦추기 어렵다는 점이 드러남
- 우회 속도와 별개로 파일이 유출된 경위도 확인되지 않음. 레조넌스는 유료 선행 플레이(paid early access)를 제공하지 않아 출시일 전까지 게임이 잠금 해제되지 않았는데도 전체 게임 파일이 불법 파일 공유 사이트에 업로드됨

• 커뮤니티를 통한 복제본 확산과 성능 평가의 사전 노출

- 보호 우회와 복제본 유통 소식은 온라인 커뮤니티 레딧(Reddit)*의 해당 게임 게시판에 처음 올라온 뒤 게임 로딩 화면 이미지가 공유되고, 다른 불법 복제 관련 게시판으로도 퍼지며 유출 사실이 정식 출시 전에 널리 알려짐
- 확산 과정에서 일부 이용자가 게임을 미리 실행했다고 밝히자 다른 이용자들은 스포일러(spoiler)**를 피해 커뮤니티 접속을 중단하면서, 출시 전 유출이 구매를 기다리던 이용자의 커뮤니티 이용까지 제약함
- 아울러 미리 실행한 이용자들이 게임의 작동 상태에 관한 평가를 공유하면서, 정식 판매 전에 게임의 완성도에 관한 정보가 불법 복제 경로를 통해 먼저 알려짐

* 레딧(Reddit): 관심사별로 모인 커뮤니티 게시판들이 모여 있는 미국의 초대형 온라인 소셜 뉴스 및 토론 사이트

** 스포일러(spoiler): 창작물의 줄거리, 반전 요소, 결말 등 중요 사항을 유출하여 이야기를 감상하는 재미와 흥미를 저하시키는 행위를 총칭

• 복제본 회수 수단의 부재와 영향 판단의 공백

- 유출이 확인된 후에도 아소보 스튜디오와 유통사 포커스 엔터테인먼트(Focus Entertainment)는 이미 유통된 복제본을 회수할 수 없었음
- 아소보 스튜디오는 유출에 대해 공식 입장을 내놓지 않았으며, 포커스 엔터테인먼트도 이번 사태가 매출에 어떤 영향을 미칠지에 대해 언급하지 않음
- 유출에 따른 피해 규모도 확정하기 어려움. 2024년 실시된 한 연구에서는 데누보를 적용하지 않은 게임이 불법 복제로 출시 첫 주 매출의 15~20%를 잃을 수 있는 것으로 나타났으나, 실제 손실 규모는 게임과 이용자층에 따라 편차가 큼²⁾

시사점: 복제 방지 기술 선택과 출시 전 배포 관리의 과제

• 게임별 조건을 반영한 복제 방지 기술 선택 기준의 필요성

- 이번 사례는 라이선스 비용과 성능 부담을 이유로 별도의 복제 방지 기술을 적용하지 않을 경우, 판매가 집중되는 출시 첫 주가 불법 복제 위협에 그대로 노출될 수 있음을 보여줌
- 다만 손실 규모가 게임과 이용자층에 따라 크게 달라 데누보 적용 여부를 일률적으로 결정하기는 어려움. 따라서 비용과 성능 부담뿐 아니라 게임별 판매 구조와 예상 수요, 유출 위험을 함께 비교할 수 있는 판단 기준이 필요함

2) Anton Kratiuk, "Resonance: A Plague Tale Legacy cracked a week before launch as DRM-free PC release backfires", gadget, 2026.08.20., <https://gadget.com/en/722884-resonance-a-plague-tale-legacy-cracked-a-week-before-launch-as-drm-free-pc-release-backfires/>

• 사후 대응을 넘어서 출시 전 배포 관리의 필요성

- 유출된 파일은 확산이 시작되면 개발사와 유통사의 사후 대응으로 되돌리기 어려움. 이에 따라 대응 시점을 파일이 외부로 유출되기 전으로 앞당기는 일이 핵심 과제로 남음
- 특히 출시 전에 미리 배포되는 설치 파일이 암호화되지 않은 채 유통된 사례도 확인된 만큼, 복제 방지 기술의 적용 여부와 함께 출시 전 배포 파일의 보안 및 관리 체계도 점검할 필요가 있음

참고문헌

- Ethan Gach, "Pirates Have Resonance: A Plague Tale Legacy A Week Before Release As Games Keep Leaking On PC", Kotaku, 2026.08.20., <https://kotaku.com/pirates-have-resonance-a-plague-tale-legacy-a-week-before-release-as-games-keep-leaking-on-pc-2000726279>
- Hennadiy Chemeris, "Resonance: A Plague Tale Legacy Cracked and Leaked Online a Week Before Official Release", VGTimes, 2026.08.20., https://vgtimes.com/gaming-news/164849-resonance-a-plague-tale-legacy-cracked-and-leaked-online-a-week-before-official-release.html#google_vignette
- Anton kratiuk, "Resonance: A Plague Tale Legacy cracked a week before launch as DRM-free PC release backfires", Gagadget, 2026.08.20., <https://gagadget.com/en/722884-resonance-a-plague-tale-legacy-cracked-a-week-before-launch-as-drm-free-pc-release-backfires/>



저작권 이슈 브리프

SUMMARY

산업/기업

기술

닌텐도의 저장소 대량 삭제 사례로 본 오픈소스 코드의 잔존

반복되는 저장소 대량 삭제와 그 배경

• 하루 7건 통지로 저장소 400개 이상 삭제

- 일본 게임 기업 닌텐도(Nintendo)는 2026년 8월 17일 자사 게임기 스위치(Switch)용 비공식 에뮬레이터(emulator)* 저장소(repository)** 400여 개의 삭제를 요청하는 통지를 코드 공유 플랫폼 깃허브(GitHub)에 제출함¹⁾
- 이에 따라 깃허브는 닌텐도가 제출한 7건의 디지털 밀레니엄 저작권법(Digital Millennium Copyright Act, 이하 DMCA)*** 우회 방지 통지(anti-circumvention notice)****를 근거로 해당 저장소를 삭제함
- 닌텐도의 대규모 저장소 삭제 통지는 이번이 처음이 아님. 2024년 5월에는 DMCA 우회 방지 통지를 통해 오픈소스(open source) 스위치 에뮬레이터 유주(Yuzu)의 저장소 8,535개가 삭제됐으며, 2026년 2월에도 유주를 포함해 13개의 에뮬레이터를 대상으로 동일한 저장소 삭제 통지를 제출함²⁾

* 에뮬레이터(emulator): 특정 게임기용으로 만들어진 게임을 다른 기기에서 실행할 수 있게 하는 프로그램

** 저장소(repository): 소프트웨어 개발에서 소스 코드, 데이터, 관련 파일들을 모아두고 버전 관리(수정 이력 기록)를 하는 디지털 보관소

*** 디지털 밀레니엄 저작권법(Digital Millennium Copyright Act, DMCA): 저작권 보유자가 포털·플랫폼 등 서비스 제공자 측에 저작권 침해 소명하면 확인 절차를 거쳐 문제의 자료를 삭제하도록 규정한 법

**** 우회 방지 통지(anti-circumvention notice): 게임의 기술적 보호 조치를 우회하는 도구라는 이유로 해당 코드의 삭제를 요청하는 통지

• 프로젝트 종료 이후에도 온라인에 남은 코드

- 저장소 삭제가 반복되는 것은 개발이 중단된 뒤에도 코드가 온라인에 남기 때문임. 유주는 2024년 소송 합의에 따라 개발을 중단했으며, 또 다른 에뮬레이터 류진엑스(Ryujinx)도 같은 해 10월 개발을 중단함. 그러나 두 프로젝트의 코드는 온라인에서 완전히 사라지지 않음
- 오픈소스로 공개된 코드는 포크(fork)*나 복제를 거쳐 다른 저장소에 남고, 이렇게 남은 코드가 다시 삭제 대상이 되면서 개발이 중단된 프로젝트의 저장소 삭제가 반복됨

* 포크(fork): 공개된 원본 코드를 복사해 별도의 저장소에서 독립적으로 이어 개발하는 것

1) Ernesto Van der Sar, "Nintendo Wipes Out 400+ Switch Emulator Repos in Single-Day GitHub Sweep", TorrentFreak, 2026.08.21., <https://torrentfreak.com/nintendo-wipes-out-400-switch-emulator-repos-in-single-day-github-sweep/>

2) Chris Scullion, "Nintendo wipes out 400 more Switch emulator repositories on GitHub as it continues its fight on piracy", VGC, 2026.08.21., <https://www.videogameschronicle.com/news/nintendo-wipes-out-400-more-switch-emulator-repositories-on-github-as-it-continues-its-fight-on-piracy/>

네트워크 단위 처리로 확대된 삭제 범위와 삭제 이후의 상태

• 저장소 네트워크 단위 적용으로 확대된 삭제 규모

- 유주의 개발 중단 이후 주목받은 후속 프로젝트 수유(Suyu)의 경우 삭제 대상 저장소 네트워크(repository network)*에 100개가 넘는 저장소가 포함됨. 깃허브는 통지 1건을 네트워크 전체에 적용해 저장소 311개를 한꺼번에 삭제했으며³⁾, 나머지 6건은 하나의 저장소부터 수십 개까지 처리 규모가 다양함
- 전체 7건 가운데 4건은 깃허브가 처리한 네트워크의 저장소 수가 공개됐으나, 나머지 3건은 네트워크 정보가 공개되지 않아 통지에 명시된 저장소만 확인할 수 있음. 이 가운데 일부 저장소는 명칭도 비공개로 처리됨

* 저장소 네트워크(repository network): 하나의 상위 저장소와 이를 포크한 저장소를 묶어 깃허브가 함께 관리하는 단위

[표 1] DMCA 우회 방지 통지 7건의 대상 프로젝트별 저장소 수

상위 저장소	프로젝트	대상 저장소 수
vstyler96/suyu	수유(유주 후속)	311개(네트워크 전체)
skyline-emu/skyline	스카이라인(안드로이드, 독립형)	29개(네트워크 전체)
NicolasArvani/yuzu	유주 포크	14개(네트워크 전체)
liushuyu/yuzu-android	유주 안드로이드 이식판	8개(네트워크 전체)
exverge-0/yuzu-EA4176	유주 얼리 액세스 빌드 4176	21개(통지에 명시된 포크)
irlbunny-archive/MonoNX	모노NX(C#* 기반)	17개(통지에 명시된 포크)
lpwnedU/yuzu-master	유주 포크	상위 저장소만

출처: Ernesto Van der Sar, "Nintendo Wipes Out 400+ Switch Emulator Repos in Single-Day GitHub Sweep", TorrentFreak, 2026.08.21., <https://torrentfreak.com/nintendo-wipes-out-400-switch-emulator-repos-in-single-day-github-sweep/>

* C#: 소프트웨어 즉, 응용 프로그램을 만들기 위한 프로그래밍 언어

• 개발 중단된 프로젝트까지 삭제 대상에 포함

- 삭제 대상에는 이미 개발이 중단된 프로젝트의 코드도 포함됨. 안드로이드용 에뮬레이터 스카이라인(Skyline)은 유주 계열이 아닌 독립 프로젝트로 2023년 개발을 중단했으나, 오픈소스 코드가 온라인에 남아 있어 이번에 관련 저장소 29개가 함께 삭제됨⁴⁾
- 더욱이 삭제 대상에는 유주에서 파생된 포크와 독립 에뮬레이터도 함께 포함됨. 유주의 안드로이드 이식판(Android Port)*과 얼리 액세스 빌드(Early Access Build)**가 삭제됐으며, 모노NX (MonoNX)도 같은 날 삭제 대상에 포함됨

* 안드로이드 이식판(Android Port): 원래 다른 기기용으로 먼저 개발되었던 소프트웨어나 게임을 안드로이드 운영체제(OS)에서 작동할 수 있도록 수정하여 출시한 버전

** 얼리 액세스 빌드(Early Access Build): 게임이나 소프트웨어가 정식 출시되기 전, 개발 도중의 버전을 유저들에게 미리 공개하고 판매하는 정식 개발 단계의 결과물

3) Chris Scullion, "Nintendo wipes out 400 more Switch emulator repositories on GitHub as it continues its fight on piracy", VGC, 2026.08.21., <https://www.videogameschronicle.com/news/nintendo-wipes-out-400-more-switch-emulator-repositories-on-github-as-it-continues-its-fight-on-piracy/>

4) Ernesto Van der Sar, "Nintendo Wipes Out 400+ Switch Emulator Repos in Single-Day GitHub Sweep", TorrentFreak, 2026.08.21., <https://torrentfreak.com/nintendo-wipes-out-400-switch-emulator-repos-in-single-day-github-sweep/>

• 삭제 이후에도 남는 코드의 재확산 가능성

- 삭제 이후 저장소에 표시되는 상태는 일률적이지 않음. 대부분은 삭제 안내문과 관련 통지 링크가 표시되지만, 일부는 404 오류(404 error)*로 연결돼 개발자가 통지를 받은 뒤 저장소를 직접 삭제한 것으로 추정됨
- 이러한 조치에도 코드가 완전히 사라지는 것은 아님. 개별 저장소를 삭제하는 것보다 복제본을 온라인에서 지속적으로 제거하는 일이 더 어려우며, 통지에 따라 포크가 삭제되는 속도보다 새로운 복제본이 나타나는 속도가 빠를 수 있음

* 404 오류(404 error): 클라이언트가 서버와 통신할 수는 있지만 서버가 요청한 바를 찾을 수 없다는 것을 가리키는 HTTP 표준 응답 코드

시사점: 코드 확산 속도를 고려한 지속적인 대응 필요

• 대량 삭제와 코드 잔존 사이의 간극 및 향후 과제

- 저장소 네트워크 단위의 적용으로 한 번에 삭제되는 규모는 커졌지만, 이번 7건 가운데 상위 저장소 한 곳만 대상으로 삼은 통지도 있어 건별 삭제 범위에는 상당한 차이가 나타남
- 개발이 중단된 코드까지 삭제 대상에 포함된 것은 한 차례의 조치만으로 대응이 끝나지 않음을 보여줌. 스카이라인처럼 수년 전 개발이 중단된 프로젝트도 다시 삭제 대상이 된 만큼, 저장소 삭제는 일회성 정리보다 지속적인 대응에 가까움
- 대응의 실효성은 최초 삭제 시점보다 이후 코드의 재확산을 얼마나 억제하는지에 따라 달라짐. 저장소를 삭제하더라도 통지가 새로운 포크와 복제본의 등장 속도를 따라가지 못하면 코드는 온라인에 계속 남을 수 있음
- 따라서 이번 조치의 효과를 삭제된 저장소 수만으로 판단하기는 어려움. 대규모 삭제가 여러 차례 반복된 만큼, 저장소를 삭제하는 것보다 동일한 코드가 다른 경로로 재확산되는 것을 막는 일이 더 큰 과제로 남음

참고문헌

- Ernesto Van der Sar, "Nintendo Wipes Out 400+ Switch Emulator Repos in Single-Day GitHub Sweep", TorrentFreak, 2026.08.21., <https://torrentfreak.com/nintendo-wipes-out-400-switch-emulator-repos-in-single-day-github-sweep/>
- Chris Scullion, "Nintendo wipes out 400 more Switch emulator repositories on GitHub as it continues its fight on piracy", VGC, 2026.08.21., <https://www.videogameschronicle.com/news/nintendo-wipes-out-400-more-switch-emulator-repositories-on-github-as-it-continues-its-fight-on-piracy/>
- Liam Doolan, "Nintendo Wipes Out Hundreds Of Switch Emulator Repositories", Nintendo Life, 2026.08.22., <https://www.nintendolife.com/news/2026/08/nintendo-wipes-out-hundreds-of-switch-emulator-repositories>



저작권 이슈 브리프

SUMMARY

산업/기업

기술

주간 기술 동향

생성 노이즈
상관관계를 활용한
음성 워터마킹 기술
AudioNoisePrints

• AI 음성 복제에 대한 권리 보호 강화와 합성 음성 추적 기술의 필요성

사람이 직접 녹음하던 음성 콘텐츠 영역에 AI로 생성한 음성이 확산되고 있다. 특정 인물의 목소리를 복제한 AI 음성이 만들어지면서, 성우와 유명인의 목소리가 무단 복제 되는 일이 발생하고 있다. 실제로 일본에서는 한 성우가 자신의 목소리를 복제한 영상이 수익을 발생시켰다며 해당 플랫폼 운영사를 상대로 민사 소송을 제기한 사례도 확인되었다. 그러나 분쟁이 벌어져도 문제가 된 음성이 사람의 녹음인지 AI 생성물인지, AI라면 어떤 서비스에서 나왔는지 확인할 방법은 마땅치 않다.

2026년 8월, 일본 법무성은 동의 없이 특정인의 목소리를 흉내 낸 AI 음성을 상업적으로 이용하는 행위가 퍼블리시티권을 침해한다는 가이드라인을 확정했다.¹⁾ 판단의 기준은 음성이 AI로 만들어졌는지가 아니라 본인의 동의가 있었는지에 있으며, 이 기준은 기업과 개인 이용자 모두에게 적용된다. 다만 목소리는 얼굴보다 특정 인물에게 귀속시키기 어렵기 때문에, 가이드라인은 단순한 유사성만이 아니라 해당 음성을 실존 인물과 연결하는 정황 정보를 함께 따지도록 규정하고 있다.

이를 위해 음성에 사람이 들을 수 없는 표식을 심어 두는 워터마킹 기술이 쓰이고 있으며, 크게 두 가지 방식으로 나뉜다. 첫 번째는 이미 만들어진 음성에 별도의 프로그램으로 표식을 덧입히는 방식으로, 음성을 만든 뒤 한 번 더 처리해야 하므로 시간과 연산이 추가로 든다. 또한 표식을 뚜렷하게 심을수록 지워지지는 않지만 음질이 나빠지는 상충 관계가 있고, 공개된 프로그램을 쓰는 경우 공격자가 같은 프로그램으로 표식을 덮어쓸 수 있다. 두 번째는 음성을 만드는 AI 자체를 다시 학습시켜 워터마크를 삽입하는 방식인데, 학습 비용이 클 뿐만 아니라 그 과정에서 음성 품질이 떨어질 수 있다.

이러한 배경에서 AI가 음성을 만드는 원리 자체를 표식으로 활용하는 접근이 제시되고 있다. 최근의 음성 생성 AI는 아무 의미 없는 잡음에서 출발해 이를 조금씩 다듬어 음성으로 바꾼다. 이미지 생성 모델에서는 완성된 결과물이 출발점이 된 잡음과 뚜렷하게 닮는다는 성질이 앞서 확인되었으나, 음성에서도 같은 성질이 나타나는지는 검증되지 않았다. 본 보고서에서는 이 성질을 이용해 AI를 다시 학습시키거나 음성을 변형하지 않고도 표식을 남기는 오디오노이즈프린트(Audio NoisePrints, 이하 ANP) 기술을 중심으로, 해당 방식이 기존 워터마킹의 한계를 어떻게 우회했는지 분석한다.

1) Earl Bensen, "Japan Rules AI Voice Cloning Requires Consent: Developers Face Civil Liability", TechTimes, 2026.08.08., <https://www.techtimes.com/articles/323616/20260808/japan-rules-ai-voice-cloning-requires-consent-developers-face-civil-liability.htm>

[사례] 생성 노이즈 상관관계를 활용한 모델 프리 오디오 워터마킹

• 기존 오디오 워터마킹 방식의 구조적 한계

- 오디오 워터마킹(audio watermarking)은 사람이 인지하지 못하면서도 기계는 안정적으로 검출할 수 있는 정보를 음성 파일에 삽입하는 기술로, 현재 사용되는 방식은 사후 삽입과 모델 내부 삽입의 두 갈래로 나뉨
- 사후 삽입 방식은 이미 만들어진 음성을 별도의 워터마킹 모델로 변형해 표식을 심는 방식으로, 기존 생성 과정에 그대로 붙일 수 있으나 음성을 만든 뒤 한 번 더 처리해야 하므로 추가 연산과 지연이 발생함. 또한 음성을 크게 변형할수록 공격에는 강해지지만 음질은 나빠지는 상충 관계를 피할 수 없음
- 공개된 워터마킹 모델을 사용하는 경우, 공격자가 어떤 모델이 적용되었는지 식별한 뒤 동일한 모델로 자신의 워터마크를 덮어쓰는 덮어쓰기 공격에 취약함
- 모델 내부 삽입 방식은 생성 모델 자체를 재학습해 워터마크를 내재화하는 방식으로 추가 연산과 덮어쓰기 문제를 피할 수 있으나, 학습에 필요한 계산 자원이 크고 재학습 이후 생성 품질이 저하될 수 있음

• 초기 잡음과 생성 결과 간 공간적 상관관계

- 최근의 음성 합성 모델은 무작위 잡음에서 출발해 여러 단계에 걸쳐 이를 조금씩 다듬어 나가며 음성을 만들어 냄. 각 단계마다 잡음을 목표 음성 쪽으로 밀어주는 계산이 반복 적용되며, 어떤 잡음에서 시작했는지에 따라 최종 결과물도 달라짐
- 완성된 음성은 출발점이 된 잡음과 뚜렷하게 닮아 있음. 같은 음성을 무작위로 새로 뽑은 잡음들과 하나씩 비교해 보면 유사도 차이가 크게 벌어지는데, 이는 출발 잡음이 지닌 패턴이 다듬어지는 과정에서 사라지지 않고 결과물에 남는다는 의미임
- 이러한 성질은 이미지 생성 모델에서 먼저 확인되어 워터마킹에 활용된 바 있으나, 음성 합성 모델에서도 같은 성질이 재현될지는 검증되지 않았음

• 모델 프리 판별 방식의 작동 원리

- ANP는 미리 정해진 특정 잡음을 출발점으로 삼아 음성을 생성하고, 그 잡음 자체를 표식으로 활용하는 방식임. ANP는 모델의 재학습이나 별도의 판별 모델이 필요 없기 때문에 모델 프리(model free) 방식으로 분류되며, 완성된 음성엔 손을 대지 않아 음질 저하도 없음
- 검증 단계에서는 의심스러운 음성을 멜 스펙트로그램(mel-spectrogram)*으로 변환한 뒤, 지정해 둔 잡음과 얼마나 닮았는지를 코사인 유사도(cosine similarity)**로 계산해 워터마크 여부를 판별함
- 이미지 영역의 선행 기법은 모델 내부의 압축된 표현끼리 거리를 계산했으나, ANP는 이를 오디오나 멜 스펙트로그램에서 직접 계산하도록 절차를 변경함
- 판정에는 고정된 기준값 대신 경험적 p값(empirical p-value)***을 사용함. 검증 대상 음성을 무작위 잡음 여러 개와 비교해 유사도 분포를 만든 뒤, 지정 잡음의 유사도가 그 분포에서 얼마나 드문 값인지를 따져 우연으로 보기 어려울 때만 워터마크가 있다고 판정함
- 두 값의 거리를 재는 방식에는 여러 가지가 있어 네 종류를 함께 검토했으며, 이 가운데 코사인 유사도와 내적만 판별에 쓸 만한 성능을 보임. 코사인 유사도가 근소하게 우수해 이후 실험의 기준으로 채택됨

* 멜 스펙트로그램(mel-spectrogram): 음성을 시간에 따른 주파수 분포로 변환한 뒤, 사람의 청각이 소리 높낮이를 인식하는 방식에 맞추어 주파수 축을 조정된 표현

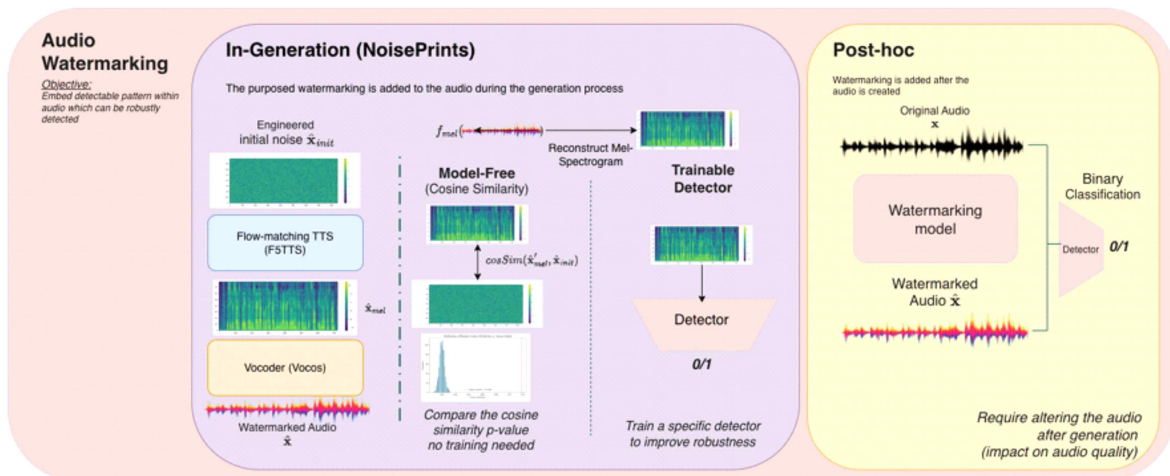
** 코사인 유사도(cosine similarity): 두 데이터를 각각 방향 값으로 보고, 두 방향이 이루는 각도를 통해 서로 얼마나 닮았는지를 재는 계산 방식

*** 경험적 p값(empirical p-value): p값은 관측된 결과가 우연히 나타날 확률을 뜻하며, 값이 작을수록 우연으로 보기 어렵다는 의미임. 경험적 p값은 이론적으로 계산된 확률 대신 실제 비교 데이터를 직접 만들어 산출한 p값을 가리킴

• 탐지기 확장 구조

- 유사도 계산에 의존하는 판별 방식은 주파수 영역에서의 공격에 취약할 뿐 아니라, 음성 길이가 고정되어 있지 않은 탓에 일부가 잘리거나 재생 속도가 바뀌면 지정 잡음과 맞춰 볼 구간 자체를 찾기 어려워 복원 절차가 크게 복잡해지는 문제를 안고 있음
- 이에 지정 잡음에서 만들어진 음성과 무작위 잡음에서 만들어진 음성을 학습시킨 뒤 그 둘을 구분해 내는 합성곱 신경망(convolutional neural network)* 탐지기를 판별 단계에 별도로 도입함
- 탐지기 학습에는 두 종류의 음성을 대량으로 생성해 함께 넣되 압축처럼 실제 유통 과정에서 흔히 발생하는 변형을 미리 가하고, 음성 일부만 잘려 나가는 공격에 대비해서는 지정 잡음을 일정 길이 단위로 나눈 뒤 음성 전체를 덮을 때까지 반복해서 배치하는 방식을 사용함
- 탐지기는 추가 학습을 요구하지만 음성을 만들어내는 모델 자체는 그대로 두므로, 모델 프리 방식의 이점이 유지되며, 품질 저하 없이 추론 속도를 높이고 판별 절차를 단순화함

[그림 1] ANP의 워터마크 삽입 및 판별 구조와 사후 삽입 방식의 비교



출처: Timothy Tin-Long Tse 외 3인, "AudioNoisePrints: Model-free audio watermarking using spatial correlation in flow matching TTS", arXiv, 2026.08.23., <https://arxiv.org/html/2608.22186v1>

• 실험 설계 및 성능 평가

- 서로 다른 구조를 가진 두 개의 음성 합성 모델을 대상으로 실험이 진행되었으며, 비교 기준으로는 사후 삽입 방식의 대표 모델인 오디오씰(AudioSeal)을 사용함
- ANP의 판별 최고 정확도는 97~98% 수준으로 오디오씰의 100%에 다소 못 미쳤으나, 잡음 추가나 주파수 여과처럼 강한 변형이 가해진 조건에서는 ANP가 뚜렷하게 앞섰고, 특히 재생 속도를 1%만 바꾸어도 오디오씰은 판별에 완전히 실패함
- 다만 음성에 울림을 더하는 에코 변형에서는 ANP의 정확도가 0.5 부근에 머물러 사실상 판별이 어려웠는데, 이는 비교 대상 모델이 해당 변형을 미리 학습한 것과 달리 ANP는 학습하지 않았기 때문임
- 오디오씰이 4,500시간 분량의 음성으로 학습된 반면 ANP는 그보다 훨씬 적은 데이터만 사용했으며, 구조가 다른 음성 생성 모델에서도 같은 상관관계가 확인되어 적용 범위를 더 넓힐 수 있을 것으로 평가됨

결론 및 시사점

• 기술적 의의 및 산업적 활용 가능성

- ANP는 생성 모델을 재학습하지 않고 완성된 음성에도 손대지 않아, 워터마크를 뚜렷하게 심을수록 음질이 나빠지던 기존 방식의 상충 관계를 피할 수 있음
- 기존 생성 절차를 그대로 둔 채 출발 잡음만 지정하면 되어 도입 부담이 작으며, 4,500시간 분량의 음성으로 학습된 기존 모델과 비교해도 훨씬 적은 자원으로 구현되어 계산과 데이터 양쪽에서 효율적인 방식으로 평가됨
- 실험에 사용된 두 모델뿐 아니라 구조가 다른 음성 생성 모델에서도 잡음과 결과물 사이의 상관관계가 동일하게 확인되었으며, 이는 앞으로 등장할 여러 음성 합성 모델과 보코더(vocoder)*에도 같은 방식을 적용할 여지가 있음을 시사함
- 다만 학습하지 않은 변형에는 취약해 에코가 더해진 음성에서는 판별이 이루어지지 않았고 변형이 없는 조건에서의 정확도도 기존 모델에 미치지 못해, 실제 유통 환경에서 나타나는 다양한 변형까지 포괄하는 학습 설계가 앞으로의 과제로 남아 있음

* 보코더(Vocoder): 사람의 목소리를 분석해 그 주파수 특성을 악기 소리에 입혀 로봇 같은 독특한 음성 효과를 내는 음향 장치이자 신시사이저의 일종

참고문헌

- Timothy Tin-Long Tse 외 3인, "AudioNoisePrints: Model-free audio watermarking using spatial correlation in flow matching TTS", arXiv, 2026.08.23., <https://arxiv.org/html/2608.22186v1>
- Earl Bensen, "Japan Rules AI Voice Cloning Requires Consent: Developers Face Civil Liability", TechTimes, 2026.08.08., <https://www.techtimes.com/articles/323616/20260808/japan-rules-ai-voice-cloning-requires-consent-developers-face-civil-liability.htm>