2024 결산

오픈소스 이슈

10분 안에 모아보기

아! 그때 들었던 것 같은데? 하던 소식들 요약해드립니다.

Open Source Program Office 이서연

주의

지극히 주관적인 기준으로 한 해 동안의 이슈를 되돌아보았습니다.
오픈소스를 매일 쓰는 개발자의 상식을 넓히는 목적으로 작성했습니다.
개인의 견해일 뿐, 회사의 견해가 아닙니다.

AI와 오픈소스의 상관 관계

깃허브에 있는 AI는 다 오픈소스 아니에요?

2024년에는 GitHub에서 생성 AI 프로젝트에 기여하는 수가 59% 급증했고, 전체 프로젝트 수는 98% 증가했습니다. (Octoverse 2024)

이렇게나 많은 AI 프로젝트가 쏟아지고 있는데요.
과연 이것들을 모두 "자유 오픈소스 소프트웨어" 로 볼 수 있을까요?

뭔가 'Open' 이라는 단어가 붙은 명칭도 쉽게 찾아볼 수 있고, 스스로를 오픈소스라 칭하는 것들도 많습니다. 하지만 OSPO팀에서 조사한 결과, 개별적으로 까다로운 조건이 많거나 라이선스 해석이 모호한 경우가 대부분이었습니다.

요약

생성AI의 급격한 발전

'Open' 이라는 이름도 많고, 공개된 파일도 많다.

그러나 이를 모두 오픈소스라고 부를 수는 없다.

개별적으로 까다로운 조건이 많으니 주의가 필요!

AI

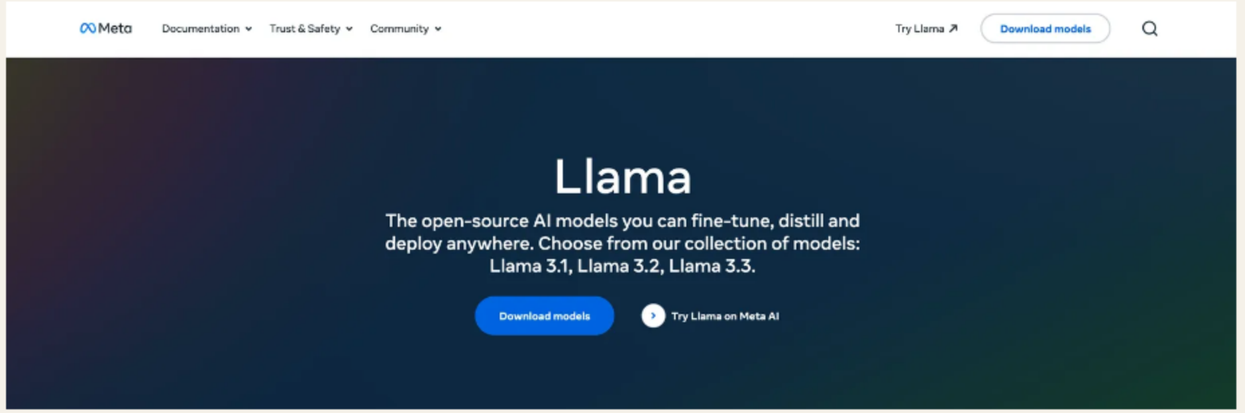
AI와 오픈소스의 상관 관계

사례 1. Meta

Meta는 Llama라는 AI 모델을 공개하며 AI 기술을 선도하고 있습니다.
Llama 에 적용하는 이용 약관을 들여다보면 오픈소스의 원칙을 다수 위배하고 있는 것을 알 수 있습니다.
(Llama 3 Community License Agreement 기준)

- 다른 대규모 언어 모델을 향상시킬 목적으로 이용 불가 (1.v. / 연구의 제한, 이용 목적에 따른 차별)
- 7억 명 이상의 Monthly Active Users가 있는 경우 Meta와 별도의 계약을 체결해야 함 (2 / 이용자의 차별)

뿐만 아니라 Meta에 의해 언제든지 통보 없이 바뀔 수 있는 추가 제약까지 두어, 불확실성을 더하고 있습니다.
이러한 이유로 오픈소스 전문가들은 Llama를 '오픈소스' 라고 부를 수 없다는 주장을 하고 있습니다.

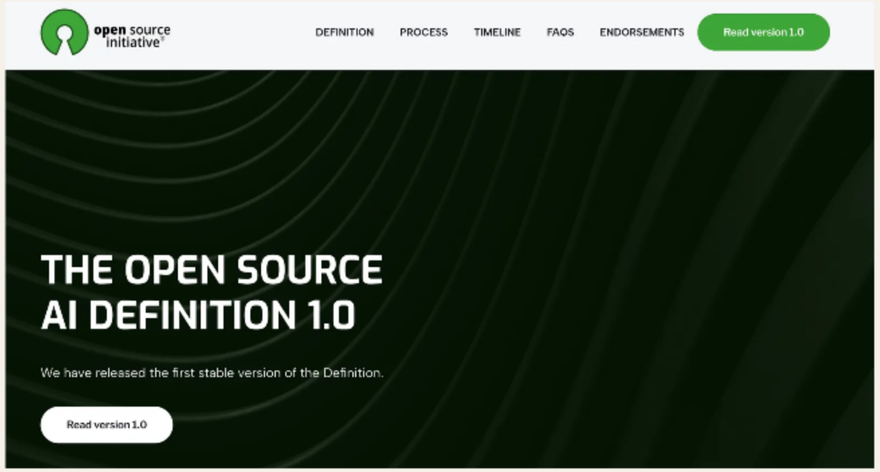


AI와 오픈소스의 상관 관계

사례 2. Open Source AI 정의 제정

그렇다면, 오픈소스 전문가들은 어떤 기준으로 AI를 오픈소스와 오픈소스가 아닌 것으로 구분을 하고 있을까요?
아직 명확한 기준은 없지만, 2024년에는 이를 위한 첫 발을 떼었습니다.

기존의 Open Source Definition(이하 OSD)을 기준으로, Open Source AI의 정의를 내린 것인데요.
업계에서는 OSD에 부합하는 라이선스를 인증하는 제도를 운용했던 Open Source Initiative에서 Open Source AI에 대해서도 인증 제도를 시행할 것인지에 대해 주목하고 있습니다.



SECURITY

XZ Utils 백도어 사건

정말 이 세상에 믿을 사람 하나 없나요?

오픈소스 개발은 외롭습니다.

2014년, 개발/보안 업계를 발칵 뒤집었던 OpenSSL의 Heartbleed 취약점이 발견되었습니다. OpenSSL을 안 쓰는 곳은 없었지만, OpenSSL의 운영/개발자는 단 두 명이었다는 사실이 알려진지 꼭 10년이 되었습니다.

리눅스 및 MacOS에서 널리 사용되는 압축 라이브러리인 XZ Utils에서 치명적인 보안 취약점이 발견되었습니다. 사람의 실수에 의해 어쩔 수 없이 발생하는 취약점이 아닌, 처음부터 악의를 가지고 몇 년에 걸쳐 이런 일을 가능케 했던 것으로 드러나 업계를 충격에 빠트렸습니다.

아아.. 오픈소스 개발은 외롭습니다. 관심이 많이 필요합니다.

```
SYNOPSIS
        xz [option...]  [file...]
```

요약

소수의 사람에 의해
유지되는 오픈소스

10년 전이나 지금이나 똑같다.

일 뒤에는 사람이 있다.

그 어떤 것도
저절로 굴러가는 일은 없다.

SECURITY

XZ Utils 백도어 사건

사건 요약

백도어란?
프로그램을 우회하여 접근할 수 있도록 하는 기능입니다. 백도어를 이용하면 시스템에 원격으로 접근하여 민감한 데이터를 훔치거나 악성 소프트웨어를 설치할 수 있습니다.

XZ Utiils는 아주 널리 사용되는 라이브러리이지만, 개발자 한 명이 유지하던 작은 프로젝트였습니다. 오픈소스 메인테이너는 부담과 과로에 시달리는 경우가 많습니다.

이런 환경에서 공격자는 2년 이상 XZ Utils에 부지런하고 효과적인 기여자로 활동하는 치밀함을 보였습니다. 개발자의 부담을 덜어주는 노력을 하며 파트너로서 성장합니다. 신뢰를 얻은 공격자는 결국 프로젝트의 관리자 권한을 얻게 됩니다.

이후 공격자는 더욱 치밀하게 개발을 이어가며, 일부 바이너리 테스트 파일 내부에 잘 숨겨진 백도어 바이너리 코드를 병합합니다.

과연 누가 이 함정에서 빠져나올 수 있을까요?

SECURITY

XZ Utils 백도어 사건

시사점

사람이 활동하는 공간에는 먼지가 생깁니다. 물론 머리카락도 떨어집니다.
그런데 사람이 없는 빈 집은 먼지나 머리카락이 떨어지지 않는데도, 더욱 빠르게 낡는 현상이 있습니다.
이 현상은 인간의 활동과 유지 보수가 건물의 자연적인 노화 과정을 늦추는 데 큰 역할을 한다는 점을 보여줍니다.

오픈소스도 집처럼 사람의 손이 닿지 않으면 빠르게 바스러지는 것 중 하나입니다.

저는 오픈소스 생태계의 지속가능성에 대해 언제나 고민해야 하는 위치에 있습니다. 오픈소스를 유지하는 사람은 정말 소수라는 점을 알고 있지만, 이런 판도를 바꿀만한 큰 활동을 하지는 못했다고 부끄러워하곤 했습니다. 그렇기에 이번 사건이 정말 충격적으로 다가왔습니다.
(앗, 그렇습니다. 저는 F입니다!)

그동안 이렇게까지 잔인하게 심리전을 펼친 오픈소스 보안 취약점은 없었던 것 같습니다.

오픈소스는 사람의 손길을 필요로 한다는 점을 기억해야 합니다.
그 어떤 것도 저절로 지속되는 것은 없습니다.

저는 제 위치에서 계속 고민하고, 관심을 가지고, 활동하는 전문가가 되고 싶습니다.

라이선스 정책의 변경 경향

그동안 우리 좋았는데...

2024년은 오픈소스 라이선스와 관련한 소식이 끊임없이 들려오는 한 해였습니다.

마음 놓고 의존해오던 오픈소스가 더 이상 오픈소스가 아니게 된 것, 혹은 더 이상 같은 조건으로는 사용할 수 없게 된 것 등 많은 변화가 있었습니다.

제 예상보다 더욱 빠르게 커뮤니티는 이런 변화에 반응했고, Fork 버전이 생겨나는 등 다양한 움직임이 있었습니다.

특히 LINE 개발자가 많이 의존하는 오픈소스의 변화, 그리고 이런 경향의 배경에 대해 요약합니다.

- Redis vs Valkey
- 돌아온 Elastic

요약

라이선스 변경이 많았다.

갈아타야할 것도 있다.

경향을 지켜보자.

오픈소스 비즈니스란
결코 쉽지 않았다.

LICENSE

라이선스 정책의 변경 경향

Redis vs Valkey

3월 20일, Redis는 기존의 BSD 라이선스에서 벗어나 Redis 7.4부터 Redis Source Abailable License와 SSPL의 듀얼 라이선스 정책으로 변경한다고 발표하였습니다. 이 두 라이선스는 모두 오픈소스의 원칙에 부합하지 않습니다.

불과 일주일 만에, 리눅스 재단은 BSD 라이선스의 Redis를 Fork한 Valkey라는 프로젝트의 런칭을 알렸습니다.

Fork가 꼭 성공하는 것은 아닙니다. 그럼에도 불구하고 Valkey가 우위를 차지하고 있다는 것을 시사하는 많은 글들이 발표되었습니다. 그 이유는 대표적으로 아래와 같습니다.

- Redis의 메인테이너 2/3가 이미 Valkey로 옮겨갔습니다.
- 리눅스 재단의 후원 아래 AWS, Googld Cloud, Oracle이 Valkey를 지원합니다.

Redis는 개인이 시작한 프로젝트로, 프로젝트의 후원과 오너십이 여러 차례 변화를 겪었습니다. 2020년에 결국 창시자가 프로젝트 관리자 자리에서 물러나면서 더더욱 프로젝트 운영에는 여러 가지 혼란이 발생한 것으로 보입니다.

Redis를 쓰고 계시는 여러분, 2025년에는 Valkey를 주목할 필요가 있습니다.

LICENSE

라이선스 정책의 변경 경향

돌아온 Elastic

지난 8월, Elastic 사의 Elasticsearch와 Kibana가 Apache License 2.0을 적용하는 오픈소스에서 벗어난 지 3년 반 만에, 다시 오픈소스로 돌아온다는 소식이 있었습니다.

라이선스 변경을 요약하자면 다음과 같습니다.
Apache License 2.0 ➡ (변경 1) Elastic License | SSPL ➡ (변경 2) Elastic License | SSPL | AGPL

Elastic은 변경 1의 시점에서 많은 것을 잃었다는 평을 얻었습니다.

- Elasticsearch와 Kibana를 오픈소스로 이용하던 대다수의 고객이 Opensearch를 선택했습니다.
- 더 이상 오픈소스라고 부를 수 없는 라이선스를 적용하며 코드 기여에 관한 저작권 문제에 휘말렸습니다. 이로 인해 기존 기여자들로부터 신뢰를 잃었습니다.

이에 Elastic은 다시 오픈소스 커뮤니티와의 관계 회복을 위해 이번과 같은 결정을 내린 것으로 해석됩니다.

전문가들은 이러한 변화가 Elastic 커뮤니티에 어떤 영향을 가지고 올지 지켜보고 있습니다.

라이선스 정책의 변경 경향

시사점

2023년에는 Terraform 또한 라이선스 변경을 결정한 바 있습니다.
Elastic에서도 보다시피 Opensearch를 맛본 사람들은 이런 라이선스 변화가 결코 유리하지 않다는 것을 경험했습니다. 커뮤니티와 멀어지고, 대체제에 밀리는 현상을 직접 봤습니다.

그런데도 왜, 그들은 이런 결정을 하는 것일까요?

전문가들은 오픈소스를 운영하는 회사의 존속에 집중하고 있습니다.
어떤 것을 만들기 위해서는 투자자가 필요합니다. 그러나 오픈소스 비즈니스의 투자자는 오픈소스의 작동 원리에 대해서 깊이 이해하지 못하는 경우도 많다고 합니다. 수익 극대화에 집중하거나, 회사를 매각하면서 가치를 올리기 위해 이런 결정을 하는 경우가 대부분입니다.

그렇다면 우리들은 이런 변화에 어떻게 대응해야 할까요?

개발자로서, 사용 중인 오픈소스에 더욱 관심을 가지고 **변화가 없는지 주기적으로 확인**해야 합니다. 또한, 어떤 변화가 감지되지만 스스로 판단하기 어려운 경우, 회사 안에서의 **전문가에게 도움을 요청**합시다.

저는 담당자로서 물론 계속해서 모니터링을 할 예정입니다.
하지만 오픈소스가 더 이상 오픈소스가 아니게 되는 선택보다는, 커뮤니티와 관계를 강화하는 선택을 하는 일이 늘어나기 위해서는 **오픈소스를 사용하는 기업들의 역할이 중요**다고 생각합니다.
이러한 지속가능성을 위해 계속 노력하는 오픈소스 전문가가 되고 싶습니다.

경청해주셔서 감사합니다!

참고 자료

- https://github.blog/news-insights/octoverse/octoverse-2024/
- https://opensource.org/ai/open-source-ai-definition
- https://boehs.org/node/everything-i-know-about-the-xz-backdoor
- https://research.swtch.com/xz-timeline
- https://redis.io/blog/redis-adopts-dual-source-available-licensing/
- https://www.linuxfoundation.org/press/linux-foundation-launches-open-source-valkey-community
- https://thenewstack.io/valkey-is-a-different-kind-of-fork/

1. https://www.gomomento.com/blog/rip-redis-how-garantia-data-pulled-off-the-biggest-heist-in-open-source-history/

- https://www.elastic.co/blog/elasticsearch-is-open-source-again
- https://openchain-project.github.io/OpenChain-KWG/blog/2024/09/06/%EB%98%90-%EB%8B%A4%EC%8B%9C-elasticsearch-%EB%9D%BC%EC%9D%B4%EC%84%A0%EC%8A%A4-%EB%B3%80%EA%B2%BD-%EA%B8%B0%EC%97%85%EC%9D%98-%EB%8C%80%EC%9D%91-%EB%B0%A9%EC%95%88%EC%9D%80/