



Open Source Congress 2024

AI、セキュリティ、デジタル公共財における
コラボレーションの未来を切り開く

2024年12月

Anthony Williams, President 兼 Co-founder, DEEP Centre

序文 : Chris Xie および Yue Chen, Futurewei Technologies, Inc.

Open Source Congress 2024

Open Source Congressは、オピニオンリーダー、実務家、コミュニティリーダーが一堂に会し、**オープンソース技術の未来を切り開く**ための年次集会です。



OpenHarmonyやOpenEulerに代表されるオープンソースへの中国の貢献は、**グローバルなコラボレーションやデジタル主権を強化**するという中国のコミットメントの象徴です。



世界各国政府からの規制圧力は、**コミュニティ主導の積極的な政策提言**が必要であることを物語っています。



オープンソースAIにより、強力なAIツールへのアクセスが民主化され、世界中の開発者、研究者、企業が既存のモデルを実験、共有、改良できるようになりました。

責任あるAIは、多様なデータセットでAIシステムの訓練がされており、**倫理、安全性、透明性**を付加的な要素としてではなく、最初から**AIモデルに組み込む**必要があります。



オープンソースソフトウェアのコピケータス化により、**サイバーセキュリティ**は、世界のグローバル デジタルインフラの**安全性、信頼性、信憑性を確保**する上でますます重要になっています。



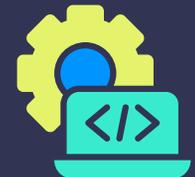
総会では、適切な制限や基準、実績の追跡、高品質なトレーニングデータの共有リポジトリなど、**AI特有のセキュリティフレームワーク**の必要性に焦点が当たりました。



オープンソースは、ブロックチェーンのような**分散型テクノロジー**を支える原動力であり、ユーザーは自分のデータ、資産、アイデンティティ、デジタル インタラクションをコントロールすることができます。



オープンソース ソフトウェアやオープン データのような**デジタル公共財**は、教育、医療、気候変動におけるグローバルでの発展のために不可欠なツールとなっています。



総会の参加者は、サイバーセキュリティ、サステナビリティ、コンプライアンスといったエコシステムの課題に取り組むためには、**継続的な対話と協力**が不可欠であることに賛同しました。



オープンソース コラボレーションを強化するための提案として、年次総会の継続、ピアツーピアの人脈形成、グローバル事務局の設置などが挙げられました。



Open Source Congressは、ポジション ペーパーの作成、参加者の拡大、ブリュッセルでの2025年イベントの計画など、**コラボレーションのため**に一年を通して活動する**プラットフォーム**へと進化しています。

目次

序文	4
2024 年 Open Source Congress : コラボレーションの継続	5
現状認識 : 進化するオープンソース ソフトウェアの役割とインパクト	7
オープンソース人工知能 : イノベーションと責任のバランス	9
オープンソース サイバーセキュリティ : コラボレーションによるセキュリティ強化	14
より広い視点 : 分散型インフラからデジタル公共財へ	19
オープンソース組織間のコラボレーション : 持続可能な未来の構築	23
結論 : 進むべき道を示す	27
謝辞	29
著者について	29
付録 : Open Source Congress 2025 参加団体リスト	30

序文

Open Source Congress (OSC) 2024 は、グローバルなオープンソースエコシステムの進化における重要な節目となり、多くの参加と組織にとって目覚ましい進歩を得ることができました。中国の北京で開催され、OpenAtom Foundation のプロフェッショナルな管理の下、世界中から多様な声が集まり、様々なディスカッションが行われたこのカンファレンスは、オープンソース コラボレーションの礎として極めて高い評価を得ることができました。OpenAtom 財団の揺るぎないサポートと綿密な運営は、カンファレンスを新たな高みへと昇華させ、今後のイベントのベンチマークとなりました。

OSC2024 は、グローバルでのオープンソース ムーブメントが直面する重要な問題に対するコミュニティの意識の高まりを示すものでした。コラボレーションの促進から新たな課題への取り組みに至るまで、参加者は思慮深く対話を行い、オープンソースの価値を守り促進するための実行性のある取り組みを始めました。重要な進展として、Eclipse Foundation が OSC 2025 の組織化と開催にコミットしました。これは OSC のミッションに専心する組織のネットワークが拡大していることの証でもあります。

しかし、特に OSC 自体の将来を考えると依然として前途多難です。財団の枠を超えた世界的なマルチ ステークホルダー組織を公式に継続する意志が OSC コミュニティに十分にあるのだろうか？という疑問が残ります。このような統一的な取り組みは、国連の OSPO for Good や OpenForum Europe のヨーロッパにおける政策提言の活動など、他の重要な取り組みと連携することで、OSC の総合的な影響力を増幅させることができるでしょう。これらの取り組みは共通の目標を掲げているものの、優先順位には違いがあることが多く、まとまりのあるグローバル戦略が必要であることが浮き彫りとなっています。

私たちは、ビジョンを共有し志を同じくする組織が力を合わせ、真のグローバル イニシアチブを構築することを願っています。そのような取り組みは、オープンソースの原則を守るだけでなく、オープンソースを普遍的な知識ベースとして高め、全人類に恩恵をもたらすでしょう。この活動を、統一された影響力ある活動の出発点としましょう。

Chris Xie および Yue Chen
Futurewei Technologies, Inc.

2024 年 Open Source Congress :

コラボレーションの継続

北京で開催された [Open Source Congress \(OSC\) 2024](#) は、オープンソース技術の未来を切り開くために、コミュニティで最も優秀な頭脳を結集しました。OpenAtom Foundation が主催するこの第 2 回大会は、エコシステムが直面する重要な課題と、地域や業界を超えたオープンソース ソリューションの影響力の高まりにハイライトし、率直な対話による親密な関係づくりの場となりました。オープンソースの人工知能 (AI)、サイバーセキュリティ、分散型インフラ、グローバル コラボレーションに焦点を当てた北京での活発な意見交換は、スイスのジュネーブで開催された第 1 回 2023 年イベントで始まったコミュニティの対話をさらに広げ、深めました。

ジュネーブの振り返り

ジュネーブで開催された Open Source Congress 2023 は、重要な時期に開催された精力的なイベントでした。オープンソース ソフトウェア (OSS) のユビキタス化が進むにつれ、規制当局の監視が強化され、オープンソース インフラの安全確保が急務となっていました。同時に、コミュニティのリーダーたちは、地政学的な対立やテクノナショナリズムの脅威の高まりが技術の進歩を遅らせ、OSS コミュニティが依存する国際的な協力関係が損なわれることを懸念していました。

2023 年総会の前の 2 年間のうちに、米国は CISA オープンソース セキュリティ ロードマップを導入し、欧州連合は製造物責任指令とサイバー レジリエンス法 (CRA) を開始しました。これらの規制の取り組みは、製品の安全性に対する責任を高める措置を導入し、セキュリティ脆弱性のよりタイムリーな開示とパッチ適用を要求しました。残念ながら、これらの規制の取り組みの中には、OSS コミュニティ独自の開発、商業化、ライセンス モデルの影響について、微妙に理解が欠けているものもあります。その結果、これらの取り組みによりコンプライアンス上の重大な問題が引き起こされ、コミュニティからの早急な対策が求められています。

一方、世界的な貿易摩擦、地政学的対立、デジタル主権意識の高まりは、近年、デジタル テクノロジーにおける国際協力の真の阻害要因として浮上してきました。例えば、2022 年、米国と中国は、国境を越えた重要技術の流出を制限するため、半導体やその他の戦略的資産に対する厳格な輸出規制を導入しました。オープンソース コミュニティの多くは、技術貿易の抑制が OSS 開発の地域的な分断につながり、コミュニティ内の包括性を促進したり、より多様な人材を育成したりする取り組みが疎外されることを懸念していました。

最後に、Log4Shell や XZutils のような有名なサイバーセキュリティ事件は、重要なオープンソース インフラの保護や、コミュニティのリーダーたちが保護のための取り組みに焦点を当てるきっかけとなりました。悪質な人物がプロ

プライベートなソフトウェア製品に危害を加えることができるのと同様に、サイバー犯罪者はオープンソースのオープン性を悪用して、オープンソースプロジェクトに脆弱性やバックドアを導入することができます。洗練されたOSSのサプライチェーンに対する攻撃は増加の一途をたどっており、OSSコミュニティはサイバーセキュリティ態勢を早急に強化する必要があると認識し始めています。

つまり、規制、テクノナショナリズム、サイバーセキュリティの課題により、オープンソースの環境は大きく変化し、集団行動が求められるようになりました。多くのコミュニティのステークホルダーは、OSSプロジェクトとそれを支援する財団がより強固な協力体制を早急に整備し、コミュニティメンバーはこれらの共通課題に共に立ち向かっていく必要があると認識しました。コミュニティの大原則であるオープン性、包括性、協力、コミュニティ主導の開発を忠実に保証するため、オープンソースのリーダーたちに対し、相互のコミットメントと行動計画を策定することが呼びかけられました。

コラボレーションの継続は北京で

ジュネーブでの議論では、OSS財団のリーダーが定期的集まり、グローバルなオープンソースエコシステムを管理するための集団的な取り組みを行うことが大きな価値につながるというコンセンサスが得られ、締めくくられました。また、この年1回の集まりを、定期的に、世界各国の代表者の少ない地域で持ち回りで開催することについても、幅広い支持を集めました。そこで、このコラボレーションを継続するため、OpenAtom Foundationは2024年のOpen Source Congressを北京で開催することを快諾しました。本レポートの残りは、2024年のOpen Source Congressの議事録であり、この重要なイベントから得られた主要な論点と結論に焦点を当てます。

現状認識： 進化するオープンソース ソフトウェアの役割とインパクト

オープンソース ソフトウェアは、ビジネスや社会におけるイノベーション、コラボレーション、包括性を推進し、現代テクノロジーのベースとなっています。過去数十年にわたり、OSS はソフトウェアの開発と共有の方法を変革し、個人の開発者からグローバル企業まで、誰もが共有デジタル インフラに貢献し、そこから利益を得ることができるようにしてきました。ソースコードを一般に公開し、開発者がそれを改変して配布できるようにすることで、OSS はイノベーション、透明性、自由、継続的改善の文化を育てています。

オープンソースは、クラウド コンピューティング、モバイル アプリケーション、そしてインターネットそのものといった重要なシステムにパワーを注入し、産業に革命をもたらしました。オープンソースは、最先端技術へのアクセスを民主化し、中小企業や新興企業が大手ハイテク企業と同じ土俵で競争できるようにしました。大手企業、財団、非営利団体は、スケーラブルなソリューションを構築するためにオープンソースプラットフォームを採用しています。同時に、政府や教育機関も、行政から科学研究まで、あらゆる分野で OSS を利用しています。オープンソースの柔軟性とコスト効率により、スタートアップ企業、フリーランス開発者、技術系起業家の成長の道が開かれ、オープン インフラをベースに構築されたイノベーションやビジネス モデルにも新たな道が切り開かれています。

重要な課題と新たなコラボレーションの必要性

その大きな成功の一方で、OSS コミュニティはいくつかの課題に直面しています。多くのオープンソース プロジェクトはボランティアによる貢献に依存しており、システムの維持と拡張にはより多くの財政的支援が必要であるため、持続可能性と資金調達には依然として大きな懸念事項となっています。オープンソースの透明性により、厳密なコード レビュー

ができるようになった一方で、適切に管理されなければならない悪用される可能性のあるリスクのある脆弱性が、悪意ある人物にもさらされるようになりました。さらに、オープンソース コミュニティのガバナンスは複雑であり、多くのメリットがある一方で、分散型のリーダーシップモデルは、ときとして断片化、プロジェクト管理の難しさ、重要な問題への対応の遅れなどにつながります。このような課題を考えると、オープンソース組織間の協力が最も重要です。組織はリソースをプールし、ベストプラクティスを共有し、協力することでより持続可能なエコシステムを構築することができます。また、コミュニティが互いの成功事例をベースとして、重複した取り組みを避けることができるため、コラボレーションがより迅速なイノベーションを生み出します。さらに、世界中の政府からの規制圧力により、オープンソース組織は政策議論においてまとまった発言力を持つことが不可欠となっています。集団行動を通じて、OSS コミュニティは、セキュリティ、サステナビリティ、政策といった共通の課題によりよい対策が可能となり、オープンソース技術が社会的・経済的進歩の原動力として繁栄し続けることを保証します。

オープンソース ソフトウェアのグローバル展開

北京で開催されたオープンソース総会において、OSS がまさにグローバルな現象となったことが示され、その影響力は今や北米での初期の取り組みから想像できないほど広がっています。デジタル インフラが経済発展の中心的存在となるにつれ、世界中の政府や組織は、その透明性、柔軟性、コスト効率のために OSS をますます活用するようになっています。ヨーロッパ、アジア、アフリカなどの地域では、オープンソース ソリューションが、医療、教育、行政における重要なイノベーションを支えています。これらの地域では、OSS を採用し、エコシステムへの実質的な貢献者となり、重要なプロジェクトを推進し、地域のニーズに対応するツールを開発しています。たとえば、ヨーロッパのいくつか

の国では、公共政策の枠組みやデジタル主権の取り組みにオープンソース技術を活用し、デジタル インフラが安全にアクセス可能な状態を維持しています。

グローバルで大多数の人々にとって、OSS の国際的なインパクトは非常に大きく、オープンソース ソリューションではデジタル インクルージョンが進んでいます。多くの新興国では、OSS がデジタル格差の是正のために利用されており、現地の開発者がプロプライエタリなソフトウェアの経済的負担を負うことなく、スケーラブル テクノロジーを構築できるようになっています。また、オープンソースのツールは、現地の起業家や新興企業にも活用され、彼らがイノベーションを起こし、グローバル競争に参入できるようにしています。サハラ以南のアフリカにおけるスマート農業から東南アジアにおけるデジタル政府プラットフォームまで、オープンソース プロジェクトは経済発展を促進しながら、地域固有の課題に取り組んでいます。

オープンソースの進歩における中国の役割

2024 年 Open Source Congress の開催に際して OpenAtom Foundation が主導したことは、新興技術においても国際協力の取り組みが進んでいるという、もう一つの重要な側面を示しています。中国は、グローバルなオープンソース コミュニティにおいて強力な勢力として台頭し、OSS のイノベーションと普及を推進する上で極めて重要な役割を果たしています

デジタル インフラにおけるリーダーを目指す中国の政府と民間セクターは、オープンソース テクノロジーに多大な投資を行っています。中国は、主要な国際プロジェクトへの貢献度を高めており、開発者はグローバルなオープンソース コミュニティに積極的に参加しています。OpenHarmony や OpenEuler のような国内プラットフォームは、プロプライエタリなシステムに代わる国産のオープンソースを提供し、人気を博しています。これらの取り組みは、デジタル主権を強化する中国の幅広い戦略を反映したものです。

世界の OSS 環境全体において中国の影響力は、ソフトウェア開発にとどまりません。また、ICANN や国連のさまざまな作業部会への参画から、デジタル シルクロード構想やアフリカおよび中東全域にわたるデジタル インフラ投資まで、オープンソース ガバナンス、サイバーセキュリティ、デジタル公共財に関する重要な国際協議にも参加しています。¹ オープンソース総会を主催することで、OpenAtom Foundation は、グローバル オープンソース エコシステムのための協力の推進とスタンダードの設立への献身的な取り組み姿勢を示しました。中国がオープンソースの取り組みの拡大を続けることで、その貢献によりグローバル オープンソースの採用が加速され、業界全体の OSS の影響力を高めることにつながるでしょう。

¹ <https://usali.org/usali-perspectives-blog/understanding-chinas-growing-influence-in-global-data-governance>

オープンソース人工知能： イノベーションと責任のバランス

過去 10 年間、人工知能 (AI) は大きな進化を遂げ、業界を変革し、デジタル環境を再構築してきました。最も影響力のある発展のひとつに挙げられるのは、膨大な量のデータを分析してパターンを特定し、予測を行うことができるニューラル ネットワークを搭載したディープ ラーニングの台頭です。ディープ ラーニングは、コンピュータ ビジョン、自然言語処理 (NLP)、音声認識においてブレークスルーをもたらし、自律走行車、バーチャル アシスタント、リアルタイム言語翻訳などの技術を可能にしました。変換モデル、特に GPT と BERT の開発は、機械が人間のようなテキストを理解し生成できるようにすることで NLP に革命をもたらし、チャットボット、コンテンツ生成、そして最近では GPT-4 のような大規模言語モデル (LLM) への応用に拍車をかけています。

こうした進歩により、AI は分野横断的な変革を進める推進力としての役割を確固たるものとし、次世代インテリジェント システムへの道を切り開きました。ヘルスケア分野では、機械学習アルゴリズムが診断を改善し、治療計画をパーソナライズし、創薬を加速しており、最近ではグーグルの AlphaFold がタンパク質構造予測で画期的な成果を上げています。金融分野では、AI アルゴリズムが取引システムを自動化し、不正検知を改善し、パーソナライズされたファイナンシャル プランニングやロボ アドバイザーを通じて顧客サービスを強化しています。交通機関では、AI が自律走行車の基幹となり、自動車が複雑な環境をナビゲートし、リアルタイムで意思決定を行い、事故を減少させています。AI は製造業にも革命をもたらし、予知保全やインテリジェント オートメーションシステムによって生産ラインが最適化され、ダウンタイムが最小限に抑えられ、全体的な業務効率が向上しています。小売業では、AI は推奨システム、ダイナミックプライシング、需要予測を通じて顧客体験を向上させ、農業では、精密農業、作物モニタリング、収量増加のための資源利用の最適化に AI を活用しています。AI は業界を大きく変えるも

のであり、オープンソース コミュニティはその発展において重要な役割を果たしています。TensorFlow や PyTorch のようなオープンソース プラットフォームは、強力な AI ツールへのアクセスを民主化し、それにより世界中の開発者、研究者、企業が既存のモデルを実験、共有、改良できるようになりました。このような集団行動により AI 研究の進歩が加速され、開発者たちはオープンソースの手法を使用して、トランスフォーマー モデルやディープ ラーニング アーキテクチャのような重要なブレークスルーを実現しています。

もちろん、AI の画期的な可能性には大きな責任が伴います。OSC2024 では、オープンソースの AI と、さまざまなリスクや倫理的配慮に対処しながらイノベーションを推進する取り組みが重要なテーマとなりました。AI システムにおける最大手の開発者の多くは、AI モデルをクローズドにしています。しかし、総会参加者は、オープンな AI モデルの開発にはメリットがあると主張しました。オープンソースであれば、開発者はセキュリティ、公平性、倫理的な懸念に対処するために AI アルゴリズムを監視し、改良することができるため、より綿密な精査と信頼獲得が可能になります。参入障壁を低くし、貢献者のグローバルなコミュニティを奨励することで、オープンソース AI は、より多様で堅牢な AI システムに進化することができ、業界全体の広範な採用を促進することができます。

オープン性と AI の安全性や説明のしやすさの必要性

AI におけるオープン性の本質と意味について、総会参加者が一連の関連する質問の対応の中で、議論の焦点となりました。責任ある AI に期待されるものは何か？ソースコードにアクセスできることはオープンであると言えるのか？ AI モデルやツールの開発者にとって、どの程度の透明性が妥当なのか？マーケットのリーダーが人材、インフラ、データに巨

額の投資をしていることを考慮した場合にオープンソースの AI はプロプライエタリなソリューションに対抗できるのか？

責任ある AI に向けた期待として、オープンソースのリーダーたちは、AI コミュニティがより高い基準を設定し、責任ある開発に取り組むべきだと主張しました。責任ある開発とは、多様なデータセットで AI システムを訓練すること、倫理、安全性、アルゴリズムの透明性を、付加的な要素として扱うのではなく、最初から AI モデルに組み込むことなどが含まれます。さらに、データ収集のガイドライン、厳格なテストプロトコル、偏見や差別を緩和するための監査プラクティスなども含まれています。

また、総会参加者は AI システムの説明のしやすさを高めることが重要であると主張しました。説明のしやすさとは、AI システムが特定の重みを持つ理由や、特定の決定、推奨、予測を行った理由を表現する能力を向上させることです。説明のしやすさは、病気の診断やクレジット利用者の決定など、今後ますます人生を左右する意思決定を下す機会が増えるシステムの信頼性、安全性、説明責任を高めるため、不可欠です。

AI の安全性、説明のしやすさ、公平性を高めるには、モデルアーキテクチャやモデルの訓練データなど、ほとんどの AI 企業が機密事項としている要素も含めて、よりオープンにする必要があります。データのサプライチェーンを考えてみましょう。アルゴリズムによる意思決定の中で発生する偏見や差別は、社会の偏見や権力構造を反映したデータを使って AI システムを訓練することで生れた予期せぬ結果であり、雇用、融資、刑事司法における偏見や差別的なパターンもそのひとつです。例えば、過去の融資データに基づいて訓練された人工知能システムは、差別的な融資を続けてしまう可能性があり、その結果、社会から疎外された人々のクレジットやローンが不平等になります。同様に、社会正義を擁護する人たちは、AI アルゴリズムを使って犯罪のホットスポットを特定し、警察のリソースを割り当てる予測警察システムが、マイノリティのコミュニティを不当に標的にしていると批判しています。

透明性のあるデータ サプライチェーンがあれば、アルゴリズムの意思決定において偏った結果を生み出すリスクを大幅に減らすことができます。透明性を確保することで、トレーニング データの出所、品質、取り扱いがきちんと文書化され、追跡可能になります。トレーサビリティが確保されれば、差別的なパターンや不公正な表現がないかデータを監査するなど、より綿密な監視が可能になります。また、データ収集や準備の初期段階でデータの偏りを特定し、緩和することができれば、モデル開発者が多様で代表的なデータセットを探し出し、利用を促すことができます。

モデルアーキテクチャに関して、現在使用されているほとんどの LLM はブラックボックスであると言われています。ニューラルネットワークは、何兆ものデータポイントから推測される統計的確率に基づいて予測を行うため、人間の理解の範疇を超えています。AI のソースコードを見るだけでは、AI システムがなぜそのような出力を生成するのかを説明したり解明したりすることはできません。AI 開発者でさえ、開発中の AI システムの出力を容易に説明することはできません。²

モデルの動作は、学習データやそのデータに適用される変換レイヤーに依存するため、ソースコードを見るだけでは解読できません。これらのソースコード以外の要素は、コード自体から得られる情報よりもはるかに複雑です。実際、AI システムが洗練されればされるほど、その内部的な意思決定プロセス（例えば、ディープニューラルネットワーク）が不透明となり、説明が困難になるため、AI システムがどのように判断しているのかを正確に特定することが難しくなります。

まとめると、AI の説明のしやすさや出力モデルの解釈のしやすさは、オープンソースで解決しようとしている現在研究中のテーマです。オープンソースであることで、世界中の研究者や開発者が説明のしやすさに関する技術について協力し、洞察を共有し、互いの進化を積み重ねることが可能です。例えば、AI モデルやアルゴリズムにオープンにアクセスすることで、コミュニティはシステムの内部構造を精査し、説明が難しい原因となっているパターンや欠陥を明らかにすることができます。

² <https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works>

また、説明ツール（SHAP、LIME、顕著性マップなど）を開発し共有することで、オープンソース コミュニティは、AI の出力を説明するための、より標準化された利便性の高い開発環境の整備に貢献することができます。

オープン AI の定義

AI の安全性と説明のしやすさに関する議論では、何がオープンソース AI として適格であるかを明確に定義することが重要であると示されました。総会参加者は、この課題に取り組むための 2 つの著名な取り組み、Linux Foundation の Model Openness Framework (MOF) と Open Source Initiative のオープンソース AI 定義 (OSAID) について議論しました。

Model Openness Framework は、機械学習モデルの完全性とオープン性を客観的に評価・分類するための Linux Foundation の包括的なフレームワークです。³

LF の AI & Data チームが説明しているように、MOF は、完全なモデルリリースのために必要な 16 の要素を特定し、これらの要素を基にして、モデルのオープン性を 3 つの段階に分けて定義しています。

- **クラス III - オープンモデル** : コア モデル（アーキテクチャ、パラメータ、必須ドキュメント）をオープン ライセンスで公開すること
- **クラス II - オープンツール** : モデルのトレーニング、評価、実行に使用されるコード一式と主要なデータセットが含まれていること
- **クラス I - オープンサイエンス** : 生のトレーニング データ セット、モデル開発プロセスを詳述した研究論文、ログ ファイルなど、エンドツーエンドの開発パイプラインにおけるすべての成果物を公開すること

モデルの製作者と利用者は、このフレームワークを AI システムのさまざまなコンポーネントに対して適用することで、一般的に認知が進んでいるオープンソース ライセンスの考え方に準拠しているかどうかを評価することができます。このフレームワークがオープン AI の道標となること

で、オープン コラボレーションのメリットを生かしながら、オープンで信頼感があり、すべての人にとって有益な AI システムを開発することができる実践的なロードマップを示すことができます。

Model Openness Framework に関する LF の取り組みに加え、Open Source Initiative のオープン AI を定義する取り組みの中で大きな進展がありました。2 年にわたる協議の結果、オープンソース AI 定義のバージョン 1.0 が確立され、ベースとなる 4 つの自由を提示しました。⁴

- **使用** : どのような目的でも、許可を得ることなくシステムを使用することができる。
- **研究** : システムの仕組みを研究し、構成要素を調査することができる。
- **変更** : 出力の変更を含め、あらゆる目的でシステムを変更することができる。
- **共有** : 変更の有無にかかわらず、いかなる目的であれ、他者が使用できるようにシステムを共有することができる。

オープンソース AI 定義は、オープン AI システムに必要な構成要素についても概説しています：

- **オープン コード** : システムの学習と実行に使用されるすべてのコード
- **オープン ウェイト** : オープンソース ライセンスで利用可能なモデルパラメータと重み
- **オープン データ情報** : 学習に使用されたデータ セットに関する詳細情報。他者による同様のシステム再現ができるための情報

MOF とオープンソース AI 定義は、既存の AI システムがオープンソースの原則にどの程度合致しているかを評価するため、強固なフレームワークを提供しています。数名の参加者によると、フロンティア モデルの開発者は、AI の開発や商業化において独自のアプローチを追求すること

³ <https://lfaidata.foundation/blog/2024/04/17/introducing-the-model-openness-framework-promoting-completeness-and-openness-for-reproducibility-transparency-and-usability-in-ai/>

⁴ <https://opensource.org/ai>

ができるような、大きな力と自由度があると指摘しました。また、OSS コミュニティに対して、実用的なオープン性を達成できるようにするため、妥当性のある目標を設定するよう警告しました。ある講演者はこう説明しています。「すべてのデータにアクセスしないかもしれませんが、価値ある一部の構成要素はオープンにできるかもしれません。」

最も重要なことは、これらのフレームワークが、継続的な開発と社会的課題への取り組みのロードマップを示していることです。オープン AI のメリットを推進し、明確な基準を設けたこれらのフレームワークにより AI 開発者はアクセス、変更、監査が可能なモデルやデータソースを構築することができますようになります。透明性を高め、オープンなコラボレーションを促進することで、関係者は AI 導入時に、倫理的・社会的な影響への対策を行うことができ、これにより倫理基準に合致し、社会的利益を促進できる AI 技術を開発・導入することができるようになります。

コミュニティ主導型 AI の拡大

総会でのオープン AI に関する議論は、プロプライエタリなソリューションに対抗するためのオープンソースの利用拡大を行う際の課題へと進みました。一番の課題はコストです。生成 AI モデルの開発と実行は、膨大な計算能力とインフラを必要とするコストのかかる取り組みです。これらのモデルのトレーニングには、強力な GPU や特殊なハードウェアを使用して、多くの場合、数十億から数兆のパラメータを持つ膨大なデータセットを処理する必要があります。開発者はモデルとデータを管理するために、大規模なクラウド インフラとストレージを必要とします。また、大規模な AI モデルの学習と実行のためのエネルギー消費も非常に大きく、運用コストがかさみます。

もうひとつの重要な課題は、こうした複雑なシステムを開発・維持するための専門知識です。一流の AI 研究者やエンジニアは、そのスキルに高い需要があり、高い給与を得ています。これらの知識が活用される分野では動きが激しいため、開発者は金融、医療、物流、その他の領域において AI のさまざまな応用に対応するため、モデル、データ ソース、

インフラを常に微調整しなければなりません。結集された計算能力の要求や大規模なデータ処理と相まって、これらを進歩させるための人材確保が必要であるために、生成 AI の分野は大量のリソースとコストがかかる状態となっています。

参入障壁の高さは、重大な問題を投げかけています：どうすれば OSS コミュニティはその価値提案を差別化し、世界で最も資金力のある AI 企業と歩調を合わせることができるのか？総会参加者はいくつかの提案を行いました。

その一つは、大規模な言語モデルやその他の複雑なシステムに必要なとされる大規模なスケールやリソースを必要としないニッチなユースケースに対応するために、より小規模で専門的なモデルに焦点を当てることです。小規模なモデルは、その性質上、学習や実行に必要な計算能力やリソースが少なく済むため、予算が限られている開発者や組織にとって、より利用しやすいものとなります。多くの状況において、より小さくドメインに特化したモデルは、汎用的な膨大なデータを使う必要がほとんどありません。また、OSS コミュニティは、ヘルスケア診断、法的文書処理、金融分析などの、特定のドメインで非常に優れた性能を発揮するように、特化したモデルとなるよう微調整することもできます。焦点を絞ることで、これらのモデルはそれぞれの分野において汎用的な AI システムを凌駕し、より高い精度とより適切な出力を提供することができます。

もう1つの提案は、高品質で標準化されたデータにアクセスしやすくし、モデルのトレーニングに関連するコストを削減するために、オープンデータ コモンズを構築することでした。例えば、医療、環境のサステナビリティ、農業、自然言語処理などの重要な分野において、学術機関や研究機関のグローバル ネットワークから提供を募り、分野別のリポジトリを構築することができます。開発者たちは、特定の問題や業界に特化したデータセットをカスタマイズすることができ、AI ソリューションの訓練や開発が容易になります。データ コモンズという提案は原理的には魅力的ですが、Meta、Google、Microsoft のような AI 大手に継続的に新しいデータを供給する巨大なデータ収集プラットフォーム

ムと対抗した場合に、オープンソースコミュニティは分が悪いと、複数の講演者が語りました。

最後に、オープンソースのイニシアチブは、大学、研究機関、慈善財団、政府プログラムから支援を受けることが多くあります。総会参加者は、公的資金やパートナーシップによって開発コストを相殺し、オープン AI プロジェクトが、より著名なプロプライエタリ事業者と対抗するために必要なコンピューティング インフラを利用できるようにすることを提示しました。これらのパートナーシップは財政的な支援を提供し、多様な視点や専門知識をもたらすことで、オープンな AI イノベーションのための協力体制を育成します。

専門化されたモデル、管理されたデータ コモンズ、公的パートナーシップという補完的な戦術が提供されることで、OSS コミュニティは最先端のオープンソース AI アプリケーションの構築力を高めることが可能になります。これらのメリットを活用することで、オープンソース AI の取り組みは競争力を維持し、プロプライエタリな AI ソリューションに代わる柔軟で透明性の高い、コミュニティ主導の選択肢を提供することができるでしょう。

オープンソース サイバーセキュリティ： コラボレーションによるセキュリティ強化

サイバーセキュリティはオープンソース コミュニティにおいて依然として重要な関心事であり、OSC2024 ではサイバーセキュリティ フレームワークの必要性が高まっていることが示されました。AI の台頭に伴い、AI アプリケーション特有の脆弱性への対策のため AI 固有のセキュリティ プロトコルの必要性が高まっています。AI が高度化するにつれて、リスクも高まっています。特に、AI の出力が安全で信頼性が高く、悪意のある攻撃の影響を受けないことを保証しなければなりません。

同時に、オープンソース ソフトウェアは現代のデジタル インフラのバックボーンを形成し続けており、セキュリティは重要な関心事です。オープンソース プロジェクトは、クラウド サービスのパワーアップから、医療、金融、政府で必須のツールの実現まで、世界中で複数の極めて重要なシステムを支えています。しかし、OSS のイノベーションを促進するオープン性は、サプライチェーン攻撃のリスク、古くなった依存関係、コードの貢献に対する不十分な監視など、独自の脆弱性をもたらしています。オープンソース インフラのセキュリティは、頻繁で巧妙なサイバー攻撃からグローバル デジタル エコシステムの完全性と信頼性を守る上で不可欠なものとなっていると、総会参加者からの警鐘がなされました。

AI における安全性とサイバーセキュリティ

OSC2024 の初日には、パネリストが一堂に会し、今後より多くの企業や組織が AI を重要なシステムに統合していく中で、新たに生じているセキュリティ上の課題を探りました。AI を利用した攻撃に対する OSS の安全性を確保するためのベストプラクティスや、AI の安全性を高めるためのオープンソース コミュニティの役割に議論が集まりました。パネル ディスカッションでは、AI モデルに対する適切な制限や基準、出所追跡のためのツール、偏りやその他の欠陥のないオープンソースの AI アプリケーションを構築するための高品質なトレーニング データの共有

リポジトリなど、AI 特有のセキュリティ フレームワークの必要性も示されました。

パネリストたちは、ディスカッションの背景を説明するために、4 つの重大リスクに焦点を当てました：

- 1. 有害な目的のために AI を導入する悪意ある人物。** AI モデルがますます強力になるにつれて、こうした悪意ある人物が AI システムを武器にして情報を操作し、経済を混乱させ、社会の安定を損なうリスクが生じます。例えば、現在、多くの人は AI を搭載したシステムを使うことで、ディープ フェイクや誤解を招くようなコンテンツを作成し、世論に影響を与えたり、メディアや民主的プロセスに対して信頼を損なう行為を行ったりすることができます。経済的には、AI モデルにより高度な詐欺スキームや市場操作を実現でき、大規模な金融損失を引き起こす可能性があります。また、AI モデルにより不平等を助長させる可能性もあります。例えば、企業が AI を利用して仕事を自動化し、労働者には適切な支援システムを導入せず、置き換えてしまう可能性があります。また、偏った AI システムは、既存の社会的不平等を増幅させ、差別的な雇用、融資、法執行をもたらす可能性もあります。講演者は、AI の能力が高まるにつれ、有害な目的への悪用を防ぐための強固な倫理指針、ガバナンス、セキュリティ対策の必要性が高まっていると警告しました。
- 2. AI によるサイバーセキュリティ リスクの加速。** AI 能力の急速な加速により、開発者がより洗練された AI システムを重要インフラ、金融システム、消費者技術に統合するにつれて、セキュリティ脅威の潜在する範囲が大幅に拡大しています。AI がより強力で自律的になるにつれて、悪意のあるディープ フェイク、自律的ハッキングツールの開発、AI 搭載システムの脆弱性の悪用など、悪用の可能性も高まっています。膨大な量のデータを処理し、タスクを自動化

する AI の能力は、データ操作や AI 主導のマルウェアなど、サイバー犯罪者にとって新たな攻撃の手段を提供することにもなります。さらに、最新の AI モデルが複雑であったり、特に従来のセキュリティ対策よりも速く進化したりするため、より問題は複雑化し、こうした脅威を検知して緩和することが困難になっています。総会参加者からは、OSS コミュニティに対し、AI を攻撃に利用する可能性のある人物に対抗するためのインフラの強化策を早急に調査するよう呼びかけられました。具体的には、より強固な AI ガバナンスの枠組みや、増大するリスクから保護するための AI 特有のサイバーセキュリティ プロトコルの改善など、より強力な対策の早急な整備の必要性について講演者から呼びかけられました。

3. **悪質なコードの拡散。**プログラミング作業を自動化するための強力なツールである AI コード ジェネレーターは、いくつかの理由で、不注意により有害なコードを拡散させてしまう可能性があります。その 1 つは、これらのシステムは既存のコードの膨大なデータセットに依存することが多く、そのデータセットには、旧来の、安全性が保証されなかったり安全性が低かったりする実装事例が含まれている可能性があるためです。AI モデルがこうした欠陥のあるパターンに基づいてコードを生成すると、適切な監視なしにエラーや脆弱性、非効率性が伝播する可能性があります。

AI コード ジェネレーターには、人間の開発者が持つような文脈の理解が不足しているため、表面的な機能性は満たしていても、パフォーマンス、セキュリティ、スケーラビリティのベストプラクティスを遵守していないコードが生成される可能性があります。経験の浅い開発者も含め、多くの開発者が AI が生成したコードを使用するようになると、このようなお粗末なコードがオープンソース プロジェクトや商用ソフトウェアに広まり、ソフトウェアのバグやセキュ

リティのリスクが高まる危険性があります。講演者は、AI が生成したコードは、徹底的なレビューとテストを行わなければ、これらの問題を悪化させる可能性があるとして指摘しました。また、AI 支援開発は、十分なコード検証プロセスと人による監視が必要であることも強調しました。

4. **AI の非決定的動作。**講演者は、AI の非決定的動作を問題点として指摘しました。AI システムが意思決定を行う際に、非決定的動作により予測が不可能になり透明性が欠如するからです。非決定的 AI モデルは、同じ入力を与えられた場合でも異なる出力を生成する可能性があり、システムの意思決定プロセスを完全に理解し、信頼することが難しくなります。予測や説明可能な意思決定が極めて重要で、正確性、説明責任、公平性が求められる医療、金融、法律システムなどの重要なアプリケーションにおいてこの一貫性のなさが問題となる場合があります。また、非決定的動作は、特定の出力に至った経緯を追跡することが難しいため、AI システムのデバッグや監査にも課題となります。

こうした AI の安全やセキュリティ リスクに対応するため、総会参加者は、制限や基準、実績追跡、厳格なテスト、その他の対策を含む AI 特有のセキュリティ フレームワークが必要であると指摘しました。

- **AI に特化したガバナンスの枠組みを確立すること。**フレームワークにより AI システムの安全な開発、展開、監視のためのガイドラインを提供することができます。フレームワークの中に、データの出所、モデルの説明責任、透明性に関する基準を設けることで、AI システムがそのライフサイクルを通じて監査や追跡が可能であることを保証できます。EU の AI 法などの法整備でも、開発者がモデルの使用に責任を持つことや、特に AI 開発においてセキュリティや透明性が重要であることを指摘しています。⁵

5 <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

- **制限や基準の導入。**モデルを有害な活動に利用することができないようにするための、コントロールや保護のための AI の制限や基準を確立することが重要で、これにより悪意ある目的での AI 使用を防止することができます。制限や基準には、AI モデルの開発、展開、利用方法を管理する倫理的ガイドライン、組み込みの制約、監視システムなどが含まれます。例えば、モデルが処理できる入力と生成できる出力の種類に境界を設定することで、偽情報やディープフェイクのような不適切、有害、または誤解を招くコンテンツを AI が生成することを制限することができます。
- **AI システムへの出所追跡の組み込み。**出所追跡、つまり AI が生成したコンテンツの出所を検証することは、データがどのように処理され、どのようなモデルを使用し、どのように出力を生成するかを明らかにすることで、AI システムの透明性と信頼性を高めることができます。このプロセスにより、ユーザー、規制当局、開発者は、AI が生成したコンテンツの経路を追跡することができ、それが倫理的に作成され、操作されていないことを確認することができます。コンテンツの生成に関与したデータソースとアルゴリズムに対し、検証可能な記録を残すことで、出所追跡により誤情報、偏った出力、悪意のある改変のリスクを軽減するのに活用することができます。
- **高品質で吟味されたデータで AI モデルをトレーニング。**AI モデルの精度、公平性、信頼性は、主に開発者がトレーニングに使用するデータに依存するため、高品質なトレーニングデータを用いることは、偏りやその他の欠陥を排除するための基本です。トレーニングデータが多様で、偏りなく、よくキュレーションされていれば、AI システムが異なる属性、ユースケース、環境であっても公平で正確な結果を出すことが保証できるでしょう。トレーニングデータセットを慎重に選択し、クリーニングすることで、AI 開発者はアルゴリズムのバイアスを軽減し、より堅牢で信頼性の高い AI アプリケーションを開発できると講演者は指摘しました。
- **AI が生成したコードの厳密なテストや検証。**AI が生成したコードがセキュリティ、パフォーマンス、機能性についての基準を満たし

ていることを保証するために、徹底したテストが不可欠です。開発者は、自動化されたセキュリティスキャナーやコードレビュープロセスを用いて、AI が生成したコードの潜在的な脆弱性や非効率性をデプロイする前に検出する必要があります。また、コードジェネレータを高品質のコードライブラリでトレーニングすることで、AI モデルが複製する可能性のある、安全でない、または欠陥のあるコーディングパターンの伝播を防ぐことができます。

- **依然として人が監視することが AI の安全性やセキュリティの確保において重要。**定期的な監査や人による監視により、AI の動作を継続的に評価することで、AI モデルが倫理的または法的な範囲を超えた動作をした場合に対処することができます。言い換えると、経験豊富な開発者が、AI の生成したコードをレビューして欠陥を発見し、ベストプラクティスを遵守していることを確認し、内容に応じて判断する必要があります。

最後に、2024 年総会では、知識とツールを共有し、AI セキュリティ、特に防御の強化や新たな脅威の特定と対処について、より統一的かつ積極的なアプローチを実施するための協力した取り組みが必要であると指摘されました。コミュニティが協力することで、安全な AI システムを開発、展開、監視するための AI 特有のガバナンスフレームワークを開発し、実施することができます。これらのフレームワークには、データの出所、透明性、説明責任に関する基準が含まれており、AI の偏見、誤報、悪意のある利用などのリスクを軽減するのに役立つでしょう。知識やリソースが共有されることで、倫理的ガイドラインやセキュリティ管理などの制限・基準や実績追跡も恩恵を受けることができ、悪質な人物によるオープンソースプロジェクトに対する AI モデルの悪用からの防衛線を張ることができるようになります。

オープンソース AI アプリケーションの開発を促進するための、高品質なトレーニングデータのリポジトリを構築するためには、コラボレーションが特に重要です。十分にキュレーションされたデータセットにより、AI システムが多様で、偏りなく、正確な情報に基づいて訓練されることを保証し、その正確性、信頼性、公平性を向上させることができ

ます。これらのデータセットをオープンに利用できるようにすることで、オープンソース コミュニティは参入障壁を下げることもでき、より多くの開発者や組織が、高額なデータ収集や準備のコストを費やすことなく、堅牢な AI ソリューションを作成できるようになります。

今後もオープンソースコミュニティは、新たな脅威と解決策に関する知識を共有するために協力し続けなければなりません。コミュニティが AI システムを保護し、すべての人の利益のために責任を持って AI を開発・導入できるようにするためには、集団行動が必要であり、それにより積極的で統一したアプローチを維持することができます。

オープンソース インフラの保護

他のソフトウェアと同様に、OSS もセキュリティの脆弱性から逃れることはできません。コードには欠陥が含まれる可能性があり、悪意のある人物がそれを発見した場合には悪用することができてしまいます。このような脆弱性は、コーディング ミス、アップデートの不足、不十分なセキュリティ レビューなどが原因です。一方、オープンソースは、透明性（誰でもコードをレビューできる）があったり、誰かが脆弱性を発見したときのコミュニティからの迅速な対応ができたり、特定のセキュリティ ニーズに合わせてソフトウェアをカスタマイズし、強化することができたりするなど、セキュリティにとってのメリットもあります。

OSC2024 の 2 日目では、オープンソース ソフトウェアが業界全体へ普及したことで、セキュリティ侵害の攻撃対象が潜在的に拡大していることが指摘されました。攻撃者が最近ソフトウェアのサプライチェーンを標的にしており、多くのソフトウェアで使用されているオープンソースのライブラリやコンポーネントに悪意のあるコードが注入されていることを講演者が指摘しました。これらの攻撃は、ターゲットとなるライブラリに依存して動作する多数のソフトウェア、いわゆるダウンストリームアプリケーションも危険にさらす可能性があり、OSS に依存する組織にとって致命的な障害や侵害を引き起こす可能性があります。

Synposys のサイバーセキュリティ リサーチ センターの分析によると、OSS リポジトリの 84% に少なくとも 1 つは脆弱性が含まれており、特にモノのインターネット (IoT) や自動車産業などの重要なセクターで高

リスクの脆弱性が蔓延していることが判明しました。⁶ この傾向は、事態が深刻であり、セキュリティ対策の強化が急務であることを物語っています。また、多くの企業が脆弱性の定期的なアップデートやパッチ適用を行わず、オープンソース ソフトウェアを使い続けているため、プロジェクトで複数の古いバージョンの OSS を使用することがセキュリティをさらに複雑にしていると分析しています。

こうしたリスクと闘うために、総会では次のことを求めました：

- **OSS セキュリティ監視の強化。** サプライチェーン全体で何十万もの OSS パッケージが生産適用されているため、OSS の開発者とユーザーは、潜在的な脆弱性を開示し、問題を修正する責任者を明確にするための、より良い仕組みが必要です。オープンソース セキュリティ財団 (OpenSSF) の取り組みは、OSS のセキュリティ確保の取り組みの調整役として重要な役割を果たしており、サポートされていない分野やリソースが不足している分野にリソースを誘導しており、このような活動を総会参加者は歓迎しました。
- **ソフトウェア部品表 (SBOM) の採用拡大。** SBOM の普及により、ソフトウェア開発の透明性とトレーサビリティが向上し、オープンソース コンポーネントの追跡と安全確保が容易になります。
- **OSS プロジェクトにおけるセキュリティ ガバナンスの改善。** 総会の参加者の多くは、重要なオープンソース コードのセキュリティを維持するための正式な要件や標準がほとんどなく、対策のために公式にリソースが割り当てられることもないと指摘しました。ソフトウェアのサプライチェーンにおける脆弱性を軽減するためのベストプラクティスには、ソフトウェア設計段階の早い段階でセキュリティ要件を定義すること、製造段階で定期的なセキュリティ レビューを実施すること、エンドユーザーがソフトウェアをデプロイした時点でセキュリティ テスト、パッチ適用、コンプライアンス監査を自動化することなどが含まれます。
- **共同セキュリティ対策への資金と参加の増加。** 現在使用されているようなそれぞれの OSS コンポーネントを維持するためには、オープンソース インフラの主要な受益者、特に世界最大級のテクノロ

⁶ <https://www.csoonline.com/article/574607/at-least-one-open-source-vulnerability-found-in-84-of-code-bases-report.html>

ジー企業からの、より多くの資金とリソースの投入が必要です。総会参加者は、重要な OSS インフラを維持し、既知の脆弱性に対処するために、OSS や広範な技術コミュニティ内で責任を共有することを求めました。

デジタルの未来を守る

OSC2024 での議論では、AI システムおよび広範な OSS エコシステムの安全性、信頼性、信憑性を確保する上で、サイバーセキュリティが果たす重要な役割が示されました。OSS は、医療、金融、運輸、公共部門に至るまで、重要なセクターを長く支えており、グローバルにおいてデジタル インフラの不可欠な要素となっています。しかし、このような普及に伴い、OSS は進化する脅威に対して安全かつ強靱であり続けることを保証する責任が高まっています。

強固なセキュリティ ガバナンスは、デジタルの未来を守るために極めて重要です。それにより、OSS 財団やその他のステークホルダーが、オープンソース プロジェクトで発生する脆弱性に対処するための明確で透明性の高い構造の採用を保証することができます。明確に定義されたガバナンス体制がなければ、多くのオープンソース プロジェクトの膨大な規模と非中央集権的な性質によって、重要な OSS コンポーネントの維持が難しくなり、セキュリティ上の欠陥が放置されたり、ソフトウェアのサプライチェーンが脆弱になったりする可能性があります。プロアクティブなリスク管理も同様に極めて重要であり、潜在的なセキュリティ リスクを予測し、新たな脅威に迅速に対応し、悪意のある人物からソフトウェアのサプライチェーンを守ることができます。ガバナンスとリスク管理に投資することで、オープンソース コミュニティは、グローバル インフラにおける重要な役割を維持し、私たちの世界を動かすデジタルツールの継続的な信頼と安全を確保することができます。

より広い視点：分散型インフラからデジタル公共財へ

オープンソース総会が2日間の会期で開催されることになったメリットの1つは、アジェンダの幅を広げ、オープンソースコミュニティにとって重要な新しいトレンドや事象に焦点を当てることができたことです。代表的な例として、デジタル公共財に関するセッションと、分散型インフラに関するプレゼンテーションやパネルディスカッションが挙げられます。

- **分散型インフラ**。ブロックチェーンや Web3 のような分散型テクノロジーの分野で、より安全で透明性が高く、ユーザーが制御できるシステムを実現するためのデジタルエコシステムにおいて、中央集権的な制御から分散型にシフトしていることにより分散型インフラが台頭してきています。イノベーションの促進、プライバシーの強化、大規模で中央集権的な技術プラットフォームへの依存の低減を探求するためのプラットフォームが分散型インフラにより提供されています。
- **デジタル公共財**。社会的・経済的發展を世界的に促進する自由に利用できるオープンソースの技術やデータのことで、総会では、デジタル公共財による、不平等や気候変動などの世界的課題への対処や必要不可欠なサービスへのアクセスについて取り上げ、オープンソースソリューションの役割が示されました。

両セッションでは、オープンソース総会がどれほど将来に向けたアイデアの促進に貢献しているか、世界の最前線であり続ける組織にとってエコシステムの存在が社会と技術革新の融合にどれだけ貢献しているかという点について示されました。

デジタル公共財：オープンソースによる環境維持と社会貢献

気候変動、貧困、不平等といったますます複雑化する課題に対する世

界的な取り組みが進む中、デジタル公共財は世界の進歩に不可欠なツールとなっています。オープンソースのソフトウェア、データ、デジタルインフラのような、自由に利用できるツールは、世界中でグローバルな課題に取り組む際の、間口を広げ、より大きなイノベーションを促すことにつながっています。気候変動監視システムを動かすオープンソースプラットフォームから、十分なサービスを受けていない地域の教育や医療へのアクセスを改善するツールに至るまで、多くの人がこれらのデジタルリソースを、国連の定義する持続可能な開発目標 (SDGs) の達成に不可欠なものと考えています。

オープンソースと環境のサステナビリティ

気候変動をはじめとする環境問題との戦いの中で、オープンソースソフトウェアは、資源消費の削減、エネルギー効率の向上、環境モニタリングの改善に役立つソリューションの提供に貢献しており、環境のサステナビリティを促進する上での重要な役割を果たしています。例えば、オープンソースのエネルギー管理システムは、データセンター、スマートグリッド、家庭での電力使用を最適化し、エネルギーの無駄を大幅に削減します。農業分野では、オープンソースのプラットフォームが、化学薬品の使用を最小限に抑え、水を節約し、作物の収穫量を増やす精密農業を可能にします。

オープンソースのソリューションは、汚染、森林伐採、気候変動の影響を追跡するリアルタイムの環境モニタリングシステムにも力を発揮しています。政府や環境保護団体は、このようなデータ駆動型の分析結果を活用して、投資決定や政策に情報を提供し、サステナビリティの取り組みを加速させています。各例に共通する重要なポイントは、オープンソースにより強力な技術が広範に利用可能となり、サステナビリティと環境保護を支援するデジタル公共財へのアクセスを民主化しているということです。

社会的利益のためのオープンソース

環境問題にとどまらず、身近で利用しやすい OSS 技術は、社会から取り残されたコミュニティがデジタル経済に参加し、重要なサービスにアクセスしたり、教育を向上したりする原動力となってきました。例えば、オープンソースのプラットフォームは、恵まれない地域に質の高い教育ツールをもたらし、以前は手の届かなかったインタラクティブな学習教材やリソースへのアクセスを提供しています。

医療分野におけるデジタル公共財により、研究者や公衆衛生担当者の医療データの活用方法を変革することで、グローバルでの医療アクセスや治療成果の改善につながっています。例えば、DHIS2 (District Health Information Software 2) のようなオープンソースの医療情報システムは、政府や組織において、資源へのアクセスの限られた環境でも公衆衛生データを追跡・管理することを可能にしています。⁷ オープンソースのソリューションや遠隔医療プラットフォームも、遠隔地における近代的な医療サービスへのアクセスを拡大しています。

デジタル公共財へのアクセス拡大に向けたグローバル コラボレーションの活用

OSC2024 の議論からデジタル公共財に関して最終的に得られた答えは、オープンソースの理念が、社会的・環境的課題の解決に向けたグローバルな協力のための理想的な手段であるということです。オープンソース プロジェクトでは、世界中の開発者、組織、コミュニティが革新的な解決策を実現し、互いにその恩恵を受けることで、集団的な問題解決ができています。このコラボレーションの精神は、気候変動、貧困、不平等などのグローバルで統一的な対応が必要とされる分野での取り組みに適しています。

デジタル公共財は、次のステップとして、オープンソースのイノベーションを必要としている分野全体に拡大するための強固な人材と資金プールを構築することが必要です。実際、OSS コミュニティがその潜在能力を十分に発揮するためには、オープンソースの手法に長け、グローバ

ルな課題の解決に先進技術を応用できる開発者、研究者、政策立案者の人材パイプラインを育成する必要があります。エコシステムには、新しいソリューションの開発、展開、維持をサポートするための、公的、民間、慈善団体を含む資金調達メカニズムも必要です。人的資本や財源などの必要なインフラを構築することで、デジタル公共財のアクセス性と利用効果を最大化することができます。幸いなことに、オープンソース総会は、オープンソース コミュニティが、すべての人にとって、より公平でサステナブルな未来にどのように貢献できるかについて、認識を高めることができました。

分散型インフラ：デジタル自治への道を開く

北京で開催されたオープンソース総会では、少数の大企業や機関の手にコントロールが集中する従来の中央集権型システムから、個人やコミュニティが力を持つ分散型インフラへシフトするというデジタル環境の重要な変革期において、オープンソースがいかに中心的な役割を果たすかを議論するユニークなフォーラムとなりました。説得力のある基調講演とパネル ディスカッションを通して、分散型システムを用いてデジタル体験の基本的アーキテクチャをどのように変え、ブロックチェーン、暗号通貨、ピアツーピア ネットワークのような分散型技術を生み出し、ユーザーが自分のデータ、資産、アイデンティティ、デジタルインタラクションをよりコントロールできるようにしているのかが語られました。

また、オープンソースがいかに Web3 のビジョンの中核となる分散型技術の推進力となってきたかについても語られました。例えば、世界中のオープンソース開発者は、スマート コントラクト、分散型台帳、分散型金融 (DeFi) のイノベーションを促進するために、分散型アプリケーション (dApps) やプロトコルを構築し、実験しています。より広く言えば、透明性、自律性、分散所有権という Web3 の理念は、より公平で安全なデジタル エコシステムを追求するオープンソースのコミットメントと共鳴しています。

⁷ <https://dhis2.org/>

インターネットは間違った方向に進んでしまったのか？

OSC2024 のディスカッションでは、現在のデジタル体験におけるいくつかの体系的課題が、ユーザーの信頼を損ない、社会問題の一因となっていることが指摘されました。センセーショナルで感情的なコンテンツを優先することによりユーザーとのエンゲージメントを最大化する中毒性のあるアルゴリズムの使用は、大きな懸念事項の一つです。こうしたアルゴリズムはユーザーを夢中にさせる一方で、不健康な習慣を助長し、偏向を高め、極端な思考を助長する可能性もあります。さらに、インターネット通信負荷の 46% 近くを占めるポットの急増は、誤った情報を増幅し、議論を操作し、論争の的となっているトピックについてコンセンサスがあるかのように錯覚させることで、この問題を悪化させています。

他には、個人データの大量収集の問題があり、プラットフォームは広告のターゲットや行動に影響を与えるために膨大な量のユーザー情報を収集しています。このようなデータ収集は深刻なプライバシーの問題を引き起こし、ユーザーをデータ漏洩やデータ操作の危険にさらします。また、ソーシャルメディアでは、フィルターバブルを生み出しやすく、プラットフォームによりユーザーの今までの思想に沿ったコンテンツを提供し続けることで、現実認識を歪め、偏見を強化し、社会的分裂を深めています。このような環境では、誤報やフェイクニュースが拡散し、信頼できる情報と虚偽の作り話を区別することが難しくなり、国民の理解がさらに歪められます。これらの問題は、現実をゆがめ、信頼を損ない、言論を分断するデジタル環境の一因となっています。

Web3 とともに前進する

Web3 は、現在のソーシャルメディアプラットフォームに存在する深い社会的課題、たとえば中毒性のある行動、偏向、誤った情報の拡散などを完全に解決することはできないかもしれません。しかし、オープンソース技術を活用することで、ユーザーにより良いデジタル体験を提供できる可能性はあります。その一例が LF Decentralized Trust であり、ブロックチェーンや台帳、アイデンティティ、相互運用性、暗号、およびそれらの関連技術の成長するエコシステム全体のコラボレーションと

イノベーションを促進する新しい統括組織です。2024 年 9 月に発足したこの取り組みには、分散型 ID ソリューションからデータトークナイゼーションプラットフォームまで、より透明で安全、かつ包括的なデジタルの未来を実現する何百ものプロジェクトが集結しています。⁸

LF Decentralized Trust と他の Web3 イニシアティブは、制御を分散化し、ユーザーにデータとデジタル ID の所有権を与えることで、より強力なプライバシー、セキュリティ、自律性を約束します。ユーザーは自分のデータがどのように共有され、使用されるかを選択することができます。個人情報の大量採取を減らし、より倫理的なデータプラクティスを実現します。また、分散型プラットフォームは利益のためにコンテンツを操作する中央集権的なアルゴリズムの力を弱め、操作や搾取よりも倫理的基準を優先する、より安全で透明性の高い、ユーザー中心のインターネットの基盤を作ることができます。

Web3 のビジョンを実現するために、OSC2024 では、分散化とユーザーコントロールの原則を体現する強力なデジタルプライバシーソリューションである Tor プロジェクト (The Onion Router) の概要も紹介されました。Tor は、ノードと呼ばれるボランティアが運営するサーバーのネットワークを経由してトラフィックをルーティングすることで、ユーザーの IP アドレスと所在地を隠蔽し、ユーザーが匿名でインターネットを閲覧することを可能にします。このシステムは、政府、インターネットサービスプロバイダー、ハッカーなどの第三者がユーザーのオンライン活動を追跡したり、物理的な位置を特定したりすることを防ぐことで、根本的なプライバシーとセキュリティを提供しています。

分散型ネットワークとして、Tor は中央当局なしで運営されており、単一の団体がトラフィックやユーザーデータの流れを制御することはありません。このような構成により、検閲や監視に対する耐性が非常に高くなっています。これは、抑圧的な体制が敷かれている地域や、追跡や監視からの保護を必要とするユーザーにとって非常に重要です。

また、Tor はトラフィックが複数回暗号化され、一連のランダムなノードを経由して送信されるオニオンルーティングの特徴があり、仲介者

⁸ <https://www.prnewswire.com/news-releases/linux-foundation-decentralized-trust-launches-with-17-projects-100-founding-members-302248504.html>

がユーザーの活動を完全に把握できないようにしています。Tor はプライバシーを保護し、安全な通信を可能にすることで、Web3 ビジョンの礎としての地位を確立しました。そのユースケースは、個人のプライバシーの保護から、ジャーナリスト、活動家、内部告発者などの安全が脅かされる環境にいる人物が自由で安全なコミュニケーションを可能にすることまで、多岐にわたります。要するに、Tor は、よりオープンでセキュアで検閲に強いインターネットを促進しながら、Web3 テクノロジーがいかにユーザーにデジタル ライフをコントロールする力となるかを示しているのです。

Web3 の更なる進化

Web3 の更なる進化として、ユーザーが自分のデジタル ID や資産を管理できるようにする分散型アプリケーションの台頭が予想されます。分散型デジタル ウォレットは、中央集権的な仲介機関に依存することなく、個人が暗号通貨、NFT、トークンなどさまざまなデジタル資産を安全に保管・管理できる重要なツールとして台頭しています。また、これらのウォレットは自己主権的なデジタル アイデンティティを実現し、

ユーザーは健康記録や財務データなどの個人情報へのアクセスを制御し、その共有方法や共有相手を決定することができます。

ヘルスケア分野では、分散型プラットフォームによって患者は自分の健康データをコントロールできるようになり、プライバシーとセキュリティを維持しながら医療提供者と記録を共有できるようになります。金融分野では、分散型資産管理プラットフォームによって、ユーザーは銀行やブローカーを介さずに投資やローン、その他の金融活動を管理できるようになり、金融の未来に対する透明性、安全性、自律性が強化されます。これらの新たなアプリケーションは、Web3 の分散型インフラを用いることで、よりユーザー中心のデジタル エコシステムへシフトすることが示唆されています。

オープンソース組織間のコラボレーション： 持続可能な未来の構築

2024年総会のクロージングセッションでは、持続可能なオープンソースエコシステムを構築する上で、コラボレーションが重要な役割を果たすことが改めて指摘されました。コミュニティの長期的な継続や回復力を得るために、オープンソース組織間の継続的な対話と協力の必要性が議論できたことは大きな収穫です。エコシステム全体のコラボレーションを組織化するためのこれまでの取り組みは、やや場当たりのものでした。それに対し、特に新たな規制に対応するために、構造化された積極的なコラボレーションを強く求める声がありました。



規制

政策展開のモニタリング
規制の影響に関する分析の共有
提言メッセージの調整



組織力の向上

ベストプラクティス
知識の共有
人脈形成
トレーニング ワークショップ



OSS セキュリティ

脆弱性情報の共有
改善の取り組みの調整
セキュリティ専門家の育成



オープンソース AI

AI モデルのコンプライアンスに対する
インプットの提供
データ コモンズへの寄付を募る

図 1：財団間での協力における優先事項を考える

欧州連合 (EU) が提案したサイバーレジリエンス (CRA) 法に対するオープンソースコミュニティの対応は、その一例です。複数の参加者

は、Open Forum Europe に OSS コミュニティが結集し、懸念事項への対策のために提案された規制を修正するよう欧州委員会に働きかけたことを称賛しました。しかし、ある講演者は、「私たちはもっとスクランブルをかけなければならなかった。何とかやり遂げることはできたが後手に回ってしまった。あのような経験を繰り返さないように、コミュニティとしてもっと積極的に活動する必要がある。」と語りました。重要なのは、危機が起きなくてもコミュニティが団結できるようにすることです。

様々な組織のリーダーが、規制の問題点に対策するための協力体制を制度化することの重要性について議論しており、CRA 以外にも、OSS コミュニティに影響を与える新たな規制の取り組みが今後も現れるだろうと指摘しました。また、財政のサステナビリティ、労働力不足、プロジェクトガバナンスなど、他の共通の課題についても協力が求められました。例えば、参加者からは、共有インフラを開発し、ベストプラクティスを普及させるためには、グローバルでの協力が必要であるという意見が挙がりました。

2023 年にもあったコラボレーションの議論と同様に、OSS コミュニティからは、弱点である複雑な取り組みにおけるプロジェクトマネジメントの改善を求める意見が挙がりました。豊富な経験を持つ組織が、才能とベストプラクティスを共有することによってエコシステムの能力を高めることは極めて重要です。また、熟練した人材を抱える企業は、開発者がオープンソースプロジェクトに貢献する時間を増やすために協力することもできます。共通する優先事項を特定し、コラボレーションに注力することで、OSS コミュニティはイノベーションを推進するためのより良い体制を整えることができるでしょう。これらの実現に向けて、ベストプラクティスを明確にし、標準化を推進するため、Open Regulatory Compliance ワーキンググループに数名のオープンソースのメンバーが参加しました。ある講演者が語ったように、コミュニティは技術を生み出す新しいモデルの一部であり、集団行動により、システムやソフトウェアの構築方法を変革し、社会に大きく貢献する可能性を秘めています。

コラボレーションモデル

多くのコラボレーションが有益であるという点ではグローバルでの合意が得られたものの、エコシステム全体で協力を促進するための方策については、ほとんど意見が一致しませんでした。議論は、ジュネーブでの総会を彷彿とさせるものでした。参加者は、年次総会、ライトなピアツーピアネットワーク、グローバル事務局という3つの中心的な提案について議論しました。



図2：コラボレーション モデルの具体例

年次総会。 OSS コミュニティの一部のリーダーにとっては、年次開催される総会は、財団のリーダーたちが知識の共有や戦略的な取り組みの計画をするための専用のプラットフォームであり、エコシステムにおける重要なコラボレーションのニーズを満たすことができます。ジュネーブと北京で開催されたイベントでは、サステナビリティ、サイバーセキュリティ、技術政策、オープンソース AI の将来像などの重要な問題について活発な議論が行われました。年次総会は、団結感や集団的な目的意識の構築、共通の目標に向かって多様な組織を調整するのに大きく貢献しました。また、総会では人脈の形成や同業者のつながりを促進し、パートナーシップを構築することで、より強固で強靱なエコシステムを育成しています。

こうしたメリットはあるものの、参加者の多くは、コミュニティ間で共有された目標や課題に取り組む場合には、年1回のイベントでは限界があると認識しています。プロジェクト管理、サイバーセキュリティ、政策提言といった重要な問題には、継続的な監視とタイムリーな対応が必要な場合が多く、年1回の開催ではそれができません。総会と総会の間隔が空くと、重要な取り組みの勢いを維持することが難しかったり、意思決定や重要な成果物の進捗の実質的な遅れにつながる可能性があります。加えて、オープンソースの開発は素早く、新たな課題やチャンスが頻繁に発生するため、継続的な対話と調整が必要です。定期的な連携がなければ、コミュニティは突発的な問題に対処したり、進化するベストプラクティスを共有したり、協力的なイノベーションを活用したりするのも苦労するかもしれません。効果的な協力関係を維持するために、総会参加者の多くは、コミュニティの足並みを揃え、重要な課題に取り組む姿勢を維持するために、より頻繁な連携と継続的なプロセスの必要性を訴えました。

ライトなピアツーピア ネットワーク。 総会参加者の中には、総会と次の総会の間、勢いを持続させたいという強い思いから、OSS 財団のエグゼクティブ ディレクターの人脈や、場合によっては、政策リーダーのピアグループにおいて、コラボレーションを強化することが、高頻度な連携を促進するのに重要であると考えた人もいました。エコシステムのコラボレーションのためのライトなアプローチを推進する OSS リーダーたちは、人材とインフラへの多大な投資を必要とする新しいグローバル組織の設立には懐疑的でした。彼らからは、エコシステムにはすでにいくつかの中核組織があるという意見があがりました。さらに、既存の OSS 財団のリーダーたちが定期的集まることで、共通の優先課題の特定や、ワーキンググループの設立により、共同作業の管理責任を分担することができるかと指摘しました。

ピアツーピア モデルを疑問視する人々からは、既存の任務を遂行するために日々奔走しており、財団間の協力が進まない可能性があるという意見も挙がりました。連携を深めたいという意欲は十分であっても、協力した取り組みに対して資金や経営陣の能力が不足した場合に、エコシステム全体での共通の課題への取り組みの進展が遅れたり、阻害されたりする可能性があるかと指摘しました。

オープンソースのためのグローバル事務局。ジュネーブ総会と同様、複数の総会参加者からは、オープンソース コミュニティのための新しいグローバル事務局の必要性が訴えられました。新しいグローバル組織の提案者からは、多くの業界に関連する商品群を生産したり、関連するメンバを代表し政策提言したりするための国際的な団体があると指摘がありました。一方、オープンソース コミュニティには、地域密着型、セクター密着型、プロジェクト密着型など、多種多様な財団があり、それぞれのニーズに対応しています。その結果、参加者からは、コミュニティからエコシステムに展開された成果を推進するための包括的な構造や組織が必要だという意見が挙がりました。例えば、ある参加者は、現在の場当たりのアプローチでは、多くの現場の課題や疑問を解決することができないと語りました。また、共有プロジェクトを成功させるために誰が必要なリソースを確保し、配置するのか？新たな規制の取り組みに意見を表明するとき、どの組織が政策立案者の窓口となるべきなのか？という質問を投げかけました。

2023年、総会参加者は、既存の組織をコミュニティを代表するグローバルな資産管理組織と位置付けることが可能かどうか議論されました。しかし、既存のOSS財団は、その傘下の組織によって明らかにされた課題を解決するという明確な任務とそのためのリソースしかありません。そのため、既存のOSS組織は、エコシステム全体のために、より大きなグローバルでの調整や政策提言の役割を果たすための設備や資金を備えておらず、また、そうした義務も負っていないと結論づけられました。

2024年、複数の講演者は、エコシステム全体に奉仕することを使命とする新しいグローバル事務局を創設するという代替案を提示しました。彼らは、深い政策的専門知識と中立的な立場を持つ、真にグローバルで代表となる組織をイメージしました。ITU、GSMA、IEEEのような国際機関が、特定の国の構成メンバーに支配されたり、吸収されたりすることがないのと同様に、OSSコミュニティのための新しいグローバル事務局が、既存組織の資金を乗っ取ったり、孤立させたりはしないだろうと主張しました。「私たちには成長マインドセットが必要だ。」「新しい組織を作ったからといって、既存の組織のリソースを減らすことに

はならない。」という反対意見もあり、スタッフの時間確保やその他のリソースにおける多大なコストなどの課題が伴うものの、財団間の協力は、他の重要な優先項目を犠牲にしたとしても財団内で吸収すべきだという意見もありました。

また、何人かの参加者からは、協働や合意形成がエコシステムの課題に取り組む最善策となる場合もあるとの意見が挙がりました。ある講演者は、「協力がミッションクリティカルである部分と、多様なアプローチや場合によっては競争も奨励されている部分があり、より具体的な説明が必要である」と述べました。協力や協調は、独立性を放棄しているわけではありません。すべてにおいて同意する必要はありません。私たちは多様性から得られるメリットもあります。

北京での討議が終了した時点で、エコシステム全体の協力体制を構築するための最良の道筋を明確にするためには、さらなる話し合いが必要であることが明らかになりました。短期的には、勢いを持続させることが重要であると、総会の参加者は述べています。サイバーセキュリティ、規制、オープンソースAIなどの問題については、簡単なツールを備えた一連の財団間ワーキンググループを設置することで、進展を図ることができるのではないかと意見もありました。

オープンソース総会の未来

OSC2024の閉幕段階におけるもうひとつの中心テーマは、総会そのものの将来についてでした。パネリストと参加者は、OSCは年1回のイベントから、年間を通じてグローバルな協力を促進する継続的でプロセス主導の取り組みへと進化しなければならないという点で意見が一致しました。総会参加者の中には、政策立案者や規制当局に提示するポジションペーパーを作成し承認するために、総会を利用することを提案する人もいました。また、この総会は、安全な環境の中で、形式にとらわれない会話、非公式な人脈形成、同業者同士の関わり、多様な視点を披露する貴重な機会を提供していると言う参加者もいました。

また、OSCは環境のサステナビリティ、オープンソースAI、組織ガバナンス、OSSプロジェクトや組織を維持するための組織的なリーダー

シップ、コラボレーション、資金調達必要性など、将来において注目されるかもしれないピックについても検討しました。総会参加者は、率直な会話を奨励するため、チャタムハウスルールを維持することを望んでいます。また、今後のオープンソース総会の開催において、新たなメンバーを招き、参加者の幅を広げることについても支持されました。

総会のサステナビリティを強化するための提案として、中立的で透明性のある組織を設立し、毎年開催されるイベントを運営し、議論や取り組みが会合の間の期間に勢いを維持できるようにすることなどが盛り込まれました。一方、Eclipse Foundation は、2025 年総会をブリュッセルで開催することを提案し、オープンソースコミュニティにとって極めて重要なプラットフォームである総会での更なる結束を呼びかけました。

結論：進むべき道を示す

Open Source Congress 2024 は、オープンソース エコシステムにおける重要な課題と機会について取り上げた画期的なイベントでした。AI の急速な台頭から、より良いセキュリティ フレームワークの必要性、デジタル公共財や分散型インフラの公約に至るまで、総会は、コラボレーション、イノベーション、グローバルな包括性を促進するための他にはない連携の場となりました。主な収穫は以下の通りです：

- **OSC2024 では、オープンソース AI が AI ソリューションを展開する際に、どれほどイノベーションと責任のバランスを取るのに役立つかを示しました。**オープンソース プラットフォームは、AI ツールへのアクセスを民主化し、医療、金融、輸送などの分野におけるイノベーションを促進しています。しかし、総会の参加者は、倫理的なプラクティスを実行し、AI システムにおける偏りのリスクを低減するために、透明性、公平性、説明性に焦点を当て、責任ある AI 開発の必要性を示しました。Linux Foundation の Model Openness Framework (MOF) や Open Source Initiative のオープンソース AI 定義などのオープン AI フレームワークは、責任ある AI の実践を定義し推進する上で極めて重要です。
- **OSC2024 は、オープンソース AI を拡大するために重要となる課題と機会を明確にしました。**オープンソース AI プロジェクトは、特に高いコストと専門的な専門知識が必要とされる状況を考慮すると、プロプライエタリ モデルとの競合が大きな課題となっています。これらの障壁を克服するための提案として、ニッチなユースケースに対応する小規模で専門的なモデルに焦点を当てること、アクセス可能で高品質なデータを提供するオープンデータ コモンズを構築すること、オープン AI プロジェクトを支援するための公的資金やパートナーシップを活用することなどが挙げられます。これらの戦略は、オープンソース コミュニティが競争力を維持し、コミュニティ主導の AI イノベーションを促進するのに活用できます。
- **OSC2024 は、OSS セキュリティ対策の強化が急務であることを示しました。**オープンソース リポジトリとソフトウェア サプライ

チェーンにおける脆弱性は、壊滅的な侵害につながる可能性があります。より良いセキュリティ ガバナンス、継続的なメンテナンス、脆弱性監視が必要であることは明らかです。これらのリスクに対処するため、総会では、監視の改善、透明性確保のためのソフトウェア部品表 (SBOM) の採用、OSS プロジェクトにおけるより強固なセキュリティ ガバナンス、OSS インフラを保護するための大手テクノロジー企業やエンドユーザー組織からの資金提供や協力の強化など、セキュリティ対策の強化を求めました。これらの取り組みは、OSS を活用したグローバルにおけるデジタル インフラを保護する上で極めて重要です。

- **OSC2024 では、分散型インフラとデジタル公共財により、オープンソース イノベーションを拡大するための価値あるチャンスが生まれる理由が紹介されました。**分散型インフラや Web3 技術を、オープンソース ソリューションを活用して導入することで、中央集権型プラットフォームへの依存を減らし、ユーザーがデータ、プライバシー、デジタル インタラクションをよりコントロールできるようになり、デジタル環境を再構築しています。また、オープンソースは十分なサービスを受けられていない地域において、医療や教育へのアクセスを改善し、気候変動や金融包摂などの世界的な課題に取り組むデジタル公共財にとっても不可欠です。OSC2024 は、分散型テクノロジーとデジタル公共財が、オープンソース ソリューションの影響を拡大し、より公平でサステナブルな未来に向けた進化を加速させる大きな可能性を秘めていると結論づけています。この可能性を最大化するため、次のステップとして、人材パイプラインの構築、資金の確保、OSS 組織間の協力関係の促進などが重要です。
- **OSC2024 は、コラボレーションの制度化の必要性について、コミュニティのコンセンサスを固めました。**オープンソース コミュニティは、規制の遵守、サイバーセキュリティ、財政のサステナビリティといった共通の課題に対処するために、エコシステムの知識とリソー

スをプールすることが重要であると考えています。欧州連合のサイバーレジリエンス法に対するコミュニティの対応のような場当たりの協力は、最終的には効果的であったものの、エコシステムが回復力を確保し長期継続するためには、より体系的なアプローチが必要であることを浮き彫りにしました。

- **OSC2024 は、コミュニティ全体の適切な協力モデルについて継続的に議論が必要であることを示しました。**オープンソースコミュニティ内では、コラボレーションをどのように制度化するのが最善か議論が続いています。年次総会の継続、ピアツーピアネットワークの確立、恒久的なグローバル事務局の設立などの提案がありました。どのモデルにも支持者がおり課題があります。しかし、OSC2024 では対策を一つに絞ることができませんでした。コミュ

ニティのリーダーの間でさらなる対話が必要です。

オープンソースコミュニティが成長し多様化する中、OSC2024 から得られたこれらの教訓は、オープンソース技術がデジタル世界におけるイノベーションの包括的で、安全かつサステナブルな原動力であり続けるために、今後の取り組みを方向づけるものとなるでしょう。

謝辞

北京に集まり、洞察や解説により本レポートのインスピレーションを与えてくれたオープンソース コミュニティのリーダーたちの貢献に感謝します。オープンソース総会を実現させた Futurewei の Chris Xie のリーダーシップと貢献、刺激的なイベントを主催した Open Atom チーム、そして本レポートを出版した Linux Foundation に感謝します。また、初期草稿のレビューに時間を割いてくださり、貴重なアドバイスや洞察を提供して下さった Gael Blondelle、Deborah Bryant、Hilary Carter、Stefano Maffulli、Enzo Ribagnac に特に感謝を捧げたいと思います。

著者について

Anthony は DEEP Centre の founder 兼 president であり、ビジネスと社会におけるデジタル革命、イノベーション、創造性についての国際的権威です。画期的なベストセラー『Wikinomics』とその続編『Macrowikinomics: New Solutions for a Connected Planet.』の共著者（Don Tapscott との共著）です。

Anthony は、[ブロックチェーン研究所](#)の research director、[Markie Foundation](#) の「アメリカの今後の経済のためのイニシアチブ」の expert advisor、ブリュッセルの[リスボン評議会](#)の senior fellow などを務めています。Anthony は最近、全米研究評議会の「[EPA の未来のための科学委員会](#)」の委員、トロント大学の [Munk School of Global Affairs](#) の visiting fellow、ブラジルの「Free Education Project」の chief advisor を務めました。テクノロジーとイノベーションに関する彼の研究は、Harvard Business Review、Huffington Post、Globe and Mail などの出版物で紹介されています。

付録：Open Source Congress 2025 参加団体リスト

CCF ODC

China Academy of Information and Communications Technology
(CAICT)

DEEP Centre

Digital Asia Hub

Digital Public Goods Alliance

Eclipse Foundation

KAIYUANSHE

Linaro Limited

Linux Foundation

Linux Foundation AI & Data

Linux Foundation Research

Open Infrastructure Foundation

Open Invention Network

Open Source Initiative

OpenAtom Foundation

OpenChain

OpenDigger Community

OpenWallet Foundation

OWASP

Rust Foundation

Shanghai Opensource Information Technology Association

Software Heritage Foundation

The Tor Project

Web3Infra Foundation



Futurewei は、世界中の先進的な企業との継続的で綿密なコラボレーションを維持しています。オープン イノベーション モデルを採用し、技術コミュニティとアイデアや知識を共有し、新たなビジネス チャンスを生み出す取り組みを行うことで、研究開発におけるオープン性を追求しています。

私たちのビジョンは、完全に接続されたインテリジェントな世界に向けて未来を形作ることです。私たちの使命は、オープンソース、標準化、エコシステム内のコラボレーションを通じて、インテリジェントなデジタル社会に利益をもたらすイノベーションを開発することです。

私たちは過去 20 年間、標準化プログラムに積極的に取り組んできました。この取り組みを通じて、次世代ワイヤレス技術やネットワークの開発、ICT システムのオープン アプリケーション プラットフォームによるオープン エコシステムの構築に参加しています。

www.futurewei.com



2021 年に設立された [Linux Foundation Research](https://www.linuxfoundation.org/research) は、拡大するオープンソース コラボレーションを調査し、新たな技術動向、ベストプラクティス、オープンソース プロジェクトのグローバルな影響に関する分析を行っています。プロジェクトのデータベースやネットワークを活用し、定量的・定性的なベストプラクティスに取り組むことで、Linux Foundation Research は、世界中の組織にとって有益なオープンソースの見識を得るための最適なライブラリを構築しています。

本訳文について

この日本語文書は、[Open Source Congress 2024](https://www.linuxfoundation.org/congress-2024) の参考訳として、The Linux Foundation Japan が便宜上提供するものです。英語版と翻訳版の間で齟齬または矛盾がある場合（翻訳版の提供の遅滞による場合を含むがこれに限らない）、英語版が優先されます。

翻訳協力：辻村幸弘



Copyright © 2024 The Linux Foundation

本レポートは [Creative Commons Attribution-NonCommercial 4.0 International Public License](https://creativecommons.org/licenses/by-nc/4.0/) の下でライセンスされています。

この著作物を参照するには、次のように引用してください。Anthony Williams, "Open Source Congress 2024: Shaping the Future of Collaboration in AI, Security, and Digital Public Goods," foreword by Chris Xie and Yue Chen, The Linux Foundation, December 2024

 twitter.com/linuxfoundation

 facebook.com/TheLinuxFoundation

 linkedin.com/company/the-linux-foundation

 youtube.com/user/TheLinuxFoundation

 github.com/LF-Engineering