THE LINUX FOUNDATION | Research

共通の課題に立ち向かう

2023年 Open Source Congress レポート

Anthony Williams, President and co-founder, DEEP Centre
序文 Yue Chen, Chris Xie, Futurewei Technologies, Inc

2023年 12月

Sponsored by
FUTUREWEI Technologies

共通の課題に立ち向かう

オープンソースは透明性、包括性、そしてコミュニティドリブンを**基本原則とし、**人類の集合知の基盤として**繁栄します。**

オープンソースのレジリエンスを維持するためには、サイバー セキュリティ、人工知能（AI）、テクノ ナショナリズムなど共通の課題に取り組むために、コミュニティ全体のコミットメントが求められます。

オープンソース ソフトウェア（OSS）のセキュリティは、**潤沢なサイバーセキュリティ専門人材とのつながり**や、メンテナーを惹きつけ、維持することができるインセンティブの構造に密接に関係します。

オープンソース コミュニティはアプリケーション設計の基盤にセキュリティを据えた**「セキュリティ バイデフォルト」**モデルを受け入れる必要があります。

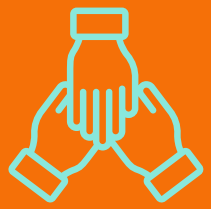
OSSの採用が増加するにつれ、規制に対する監視の目が厳しくなります。新たな規制をオープンソースの原則と実践に適合させるためには、政策提言と教育が不可欠です。

オープンソース ファウンデーションは、法的な洞察力、コミュニケーション能力、コミュニティの関係性を深める能力を駆使して、**政策の場で効果的な主張**を行わなければなりません。

デジタル主権重視が断片化を増加させ、規制の調和を阻害する可能性があります。しかし、技術的な自律性を促進する各国の取り組みが、オープンソースの採用拡大につながっています。

ファウンデーションは、コミュニティへの貢献を管理し、国境を越えた知識や技術の流れを維持するための中立的なプロトコルを確立することで、**地政学的な緊張を緩和することができます。**

コミュニティは、**ダイバーシティ & インクルージョンにコミットし**、行動規範を利用して共通の基準を推進することで、新たな人材を惹きつけ、社会的インパクトを最大化することができます。



説明できることとその成り立ちは、AIシステムの信頼性を高め、ライセンス、セキュリティ、ガバナンスの懸念に対処する上で極めて重要です。

透明性とオープンであることは、ますます強力になり普及するAIシステムに関する、新たなリスクと倫理的な配慮を管理する上で中心的な要素です。

より大きなコラボレーションのためのモデルとして、オープンソースを管理する新しいグローバルな事務局や、OSSコミュニティのリーダーたちのピア ツー ピアのネットワークなどがあります。

目次

序文

急速に進化するデジタル時代において、人類の集合知の基盤としてのオープンソースは、希望と進歩の道標として存在しています。透明性、包括性、コミュニティ ドリブンの開発という基本原則に根ざしたオープンソースは、国境や文化を超えたコラボレーションによる協力を象徴しています。2023 年の Open Source Congress から知見を得ることで、オープンソースの強さはそのコードだけでなく、それを育むグローバルコミュニティにあることが明らかになりました。

オープンソースの回復力は、私たちの共通のコミットメントの証です。サイバー セキュリティ、人工知能（AI）、そしてテクノ ナショナリズムの出現という複雑な問題を乗り越えるには、オープンソース ソフトウェア（OSS）のセキュリティを確保することが不可欠です。相互接続された世界において最も重要な関心事であるセキュリティは、時折必要となるソフトウェアの修正やパッチ以上のものが求められます。真のオープンソース セキュリティには、体系的かつ全体的なアプローチが必要であり、脆弱性の症状と根本原因に対処する必要があります。オープンソース インフラストラクチャのサービス プロバイダや実際の業務に携わる者にとって、「セキュリティ バイ デフォルト」の原則を守ることは、緊急で対応しなければならないことなのです。簡単にアクセスできるセキュリティ ツール、堅牢な基準、プロトコル、ベスト プラクティスは、開発者による創作活動を基礎から支える力を与えます。

OSSの導入が進むにつれ、規制に関する検査が強化されたことで、OSSは重要な岐路に立たされています。規制に対する監視の目が強くなると、政策の提言と教育に対する積極的なアプローチが必要になります。誤った情報に基づく規制は、オープンソースの基本的な価値を損なう恐れがあります。オープンソースの本質に対する理解不足から生じるこのような措置は、イノベーションを阻害し、コラボレーションに障壁を築き、グローバルなオープンソース コミュニティを分断する危険性があります。法律に関する専門知識、コミュニケーション能力、およびコミュニティの関係性を深める能力を備えたオープンソース ファウンデーションは、規制がオープンソースの原則に適合することを確実にするため、政策分野において提言できる独自の立場にあります。

AI が私たちの生活のあらゆる面に浸透し続けるにつれて、オープンソースの原則はさらに重要になります。オープン性と透明性は、AI の安全性という課題に対処するための中心的な要素です。AI の開発にオープンソースの原則を採用することで、AI システムは強力になるだけでなく、倫理的で説明責任を果たし、安全なものになるでしょう。

将来を見据えて、多様性（ダイバーシティ）、包括性（インクルージョン）、および行動基準の共有は、オープンソースの成長と影響力の基礎として機能し続けるでしょう。グローバルな事務局を通じてであれ、ピア ツーピアのネットワークを通じてであれ、グローバルなオープンソース コミュニティのための統一戦線のモデルは、オープンソースが人類の集合知であり続けることを保証するのに役立ちます。私たちの希望は、私たちが共に立ち上がり、共有する課題に取り組み、より明るく、よりオープンな未来を形作る準備ができることです。

オープンソースと共に。

Yue Chen, Head of Technology Strategy Chris Xie, Head of Open Source Strategy Futurewei Technologies, Inc.

はじめに

1980 年代以降、オープンソースは草の根運動から技術革新と社会革新の重要な原動力へと成長しました。ソフトウェアのソースコードを誰でも自由に閲覧、修正、配布できるようにするという考え方は、世界のソフトウェア産業を包括的に変革しました。しかし、これは他の領域におけるコラボレーションとイノベーションのための強力な新しいモデルとしても機能しました。

今世紀に入る頃には、ソフトウェア開発への共有のアプローチが、オープン スタンダード、オープン ハードウェア、オープン データ[1] を中心とした大規模な共同で実施する取り組みを生み出しました。その結果、今日使用されているデジタル ツールやアプリケーションの中で、オープン ソース コードを組み込んでいないもの、あるいは開発者がオープン ソースの手法に大きな影響を受けていないものはほとんどありません。

透明性、包括性、コミュニティ主導の開発という原則は、私たちがどのように革新し、知識を共有し、デジタル時代の複雑な問題を解決するかを形作り続けています。テクノロジーやソフトウェア開発の世界にとどまらず、オープンなコラボレーションは、オープン ガバメント、オープン サイエンス、オープン エデュケーションの台頭など、制度面での大きな変革を促しています。また、オープンソース ソフトウェア（OSS）の協力性、透明性、コスト効率の高さは、気候変動への対応や難病の治療など、世界的な取り組みに欠かせないものとなっています。

オープンソース コミュニティにとってかつてない挑戦の時代

数十年にわたる持続的な進歩を経て、オープンソース コミュニティは今日、かつてない挑戦の時代に直面しています。たとえば、強力なオープンソースのアプローチは画期的な進歩をもたらす可能性がある一方で、同時に攻撃者によりオープンソースが悪用される可能性もあります。プロプライエタリなソフトウェア製品が悪者によって侵害される可能性があるのと同様に、オープンソースが非常にオープンであるため、オープンソース プロジェクトに脆弱性やバックドアを持ち込むサイバー犯罪者やその他の攻撃者による悪用に対して脆弱になっています。高度な OSS サプライ チェーン攻撃が増加しており、サイバー セキュリティの体制強化に対する緊急の必要性を OSS コミュニティに警告しています。[2]

同時に、OSS の普及が進むにつれて、規制による監視も強化されています。過去 2 年間だけでも、米国の CISA Open Source Security Roadmap[3] と欧州の製造物責任指令(Product Liability Directive)およびサイバーレジリエンス法(Cyber Resilience Act (CRA)) は製品の安全性に対する責任を強化する措置を導入し、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ています。

残念なことに、このような善意の規制に関するイニシアチブの一部は、オープンソース コミュニティ独自の開発、商業化、およびライセンシング モデルへの影響に対する微妙な理解が欠けているものもあります。その結果、これらの規制は、コンプライアンス上の重大な問題を引き起こしています。新たな規制は、Linux、Apache Web サーバー、Mozilla Firefox、その他多くのデジタルインフラの基礎となる重要な部分を生み出したオープンソースの開発モデルを破壊しかねないと主張する人もいます。規制上の課題が積み重なるにつれ、OSS ファウンデーションは、開発者が新たな規制に準拠するのを支援し、デジタル分野における新たな法律の形成に、より早く、より積極的に関与するよう求められています。

オープンソースが繁栄してきたのは、オープン性、コラボレーション、国境を越えた自由な情報の流れに対するコミュニティの揺るぎないコミットメントのおかげです。ここでもまた、コミュニティは国境を越えた協力に対する新たな障壁に直面しています。世界的な貿易摩擦、地政学的対立、デジタル主権重視の高まりは、デジタル技術に関する国際協力の真の障害となっています。例えば、いわゆるテクノ ナショナリズムの高まりにより、米国や中国をはじめとする国々は、半導体やその他さまざまな重要技術について厳格な輸出規制を導入しています。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、コミュニティ内の多様性の促進やより多様な人材を育成する取り組みが阻害されることを懸念しています。

最後に、ソフトウェア開発において人工知能システムの導入が加速していることも、OSS コミュニティに困難をもたらします。AI 対応のコードジェネレーターは、自然言語によるプロンプトを数秒のうちに完全にコード化された関数に変えることができます。ソフトウェア産業やそれ以外の分野でも、生産性向上の潜在的なメリットは否定できません。しかし、AI モデルによって生成されるコードに関連する不確かな出所により、専有コードやライセンスコードの不用意な誤用につながる可能性があり、潜在的な侵害問題や、ライセンスやサイバー セキュリティに関連するその他の懸念につながります。

より広く言えば、今日の AI への大規模な投資は、医療、交通、行政、金融、教育への画期的な応用を含む、急速な進歩を約束しています。同時に、AI の影響力の増大により、偏見、透明性、プライバシー、雇用の喪失、人類に対する長期的な脅威などに関連する、新たなリスクや倫理的考慮事項が生じています。新世代の AI 技術を導入と収益化を競う企業は、主に秘密主義と独自の開発モデルを主張してきました。一方、オープンソース コミュニティは、AI に対する真にオープンなアプローチが、AI システムが人間の価値観と一致し、人権を保護し、社会全体の幸福を促進するためのより良い道を提供することを証明しようとしています。

2023 年 Open Source Congress ジュネーブ

今日のオープンソースの影響力は世界的なものであり、世界的な広がりと影響力には深い責任が伴います。規制、テクノ ナショナリズム、AI、およびサイバー セキュリティは、オープンソースの状況を一変させ、集団として行動する必要性がでてきました。オープンソース コミュニティの多くのステークホルダーは、コミュニティ メンバーがこれらの共通の課題に団結できるようにするために、OSS プロジェクトとそれをサポートするファウンデーションの間で連携を強化することが急務であると認識しています。

OSSファウンデーションは、エコシステムにおいて異なる使命、構成員、役割を担っています。過去には、理念や考え方の相違が協力の妨げになったこともありました。しかし、共通の課題を踏まえ、グローバルなOSSコミュニティのリーダーたちは最近、エコシステムの継続的な成功を確実にするために、これらの相違を脇に置き、新たな提携を結びました。

2023年7月、37の組織を代表する53人のオープンソースリーダーが、スイスのジュネーブに集まり、Open Source Congressを開催しました。この会議の任務は、共有する価値を特定し、主要なステークホルダー間の関係を構築し、オープンソースの活力、回復力、および完全性を維持するための計画を策定することでした。

ジュネーブを会議の開催地として選んだことは象徴的でした。有名なジュネーブ条約発祥の地であるジュネーブは、長い間中立地であり、各国が意見の相違を解決し、共通点を見つける場所でした。主権国家の指導者らは、国際関係の指針となるルールを策定するために頻繁にジュネーブに集まっており、その取り組みは人類の福祉を増進するという共通の取り組みに基づいていました。

同様の精神で、会議に参加したオープンソースのリーダーたちは、地域的な隔たり、イデオロギーの違い、そして現代の地政学的な情勢を乗り越えるよう求められました。参加者は、オープンソースがさまざまな分野を超えた集合的な善であり、国際な協力とエコシステムの優れた管理体制に依存していることを広く認識しています。オープンソース リーダーにとっての課題は、オープン性、包括性、コミュニティ主導の開発というコミュニティの基本原則に忠実であることを保証するために、相互のコミットメントと行動計画を策定することでした。

具体的には、ジュネーブ会議の参加者に課された目標は以下の通りです。

- オープンソース コミュニティが直面する**重要な課題を調査し、議論すること。**
- 共通の価値観を維持するための仕組みや、共通の課題に取り組むための戦略など、財団間の協力関係を強化するための**道筋を探ること。**
- 今後行われる関連する協議のための**新たなチャンネルを確立し、**ジュネーブで結ばれた合意を支援するために必要となる特定の活動を支援すること。

参加者は、オープンソースがさまざまな分野を超えた集合的な善であり、国際的な協力とエコシステムの優れた管理体制に依存していることを広く認識しています。

2023 年 7 月 27 日午前、会議の参加者は、オープンソース コミュニティにとって喫緊の 4 つの課題を中心に構成された一連のパネルディスカッションに参加しました。

- **オープンソースのセキュリティを読み解く：**セキュリティの脆弱性に対処し、重要な OSS インフラを維持することで、OSS ソリューションの信頼と信用を促進することに焦点を当てた議論
- **分散型組織における技術的な政策の影響：**OSS の開発および導入に影響を与える可能性のある新たな規制に関するを活動を受け入れ、協調的な対応の構築に関するラウンドテーブル
- **グローバル、オープン、包括的なコラボレーションの維持:**データ、半導体、その他の必須技術に関連する輸出規制やデジタル主権に関する動きを含む、コラボレーションに対する地政学的障壁について批評的な観点から考察
- **AI はすべてを変えるか:**ライセンス違反、著作権侵害、人的資本、ソーシャル グッドなど、AI が OSS エコシステムにもたらす潜在的リスクの検証

午後は、オープンソース コミュニティの最も緊急な課題に対処するために、主要なステークホルダーでつながりを持つ方法に焦点が当てられました。会議の参加者は、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設立や、オープンソース ファウンデーションの取り組みが相互に協調できるようにするための軽量なピア ツー ピア ネットワークの構築などのオプションを含め、コラボレーションを強化するためのさまざまなメカニズムを検討しました。ジュネーブでの議論は、OSS ファウンデーションのリーダーを定期的に招集し、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に共同で取り組むことに多大な価値があるという強いコンセンサスを持って終了しました。本レポートの残りの部分では、2023 年 Open Source Congress の議事録をまとめ、この記念すべき日の主要な論点と結論に焦点を当てます。

オープンソースのセキュリティを読み解く

他のカテゴリのソフトウェアと同様、OSS もセキュリティの脆弱性の影響を受けないわけではありません。コードには欠陥が存在する可能性があり、それが発見されると、悪意のある攻撃者によって悪用される可能性があります。これらの脆弱性は、コーディング エラー、アップデートの欠如、または不十分なセキュリティ レビューによって発生する可能性があります。最近、攻撃者はソフトウェア サプライ チェーンを標的にし、広く使用されているオープン ソース ライブラリやコンポーネントに悪意のあるコードを挿入しています。これらの攻撃は、ライブラリに依存する多数のアプリケーションを侵害し、OSS を利用する組織に壊滅的な障害や侵害を引き起こす可能性があります。

このような状況を考えると、この日の最初のパネルにオープンソース コミュニティのリーダーが集まり、OSSのセキュリティとその回復力を強化する戦略に関する重要な問題について議論したのは驚くべきことではありません。重要なオープンソース インフラストラクチャのセキュリティを高め保護することが、OSSエコシステムにおけるコラボレーションの注目すべきポイントとなっています。会議の参加者は、OSSに対する信頼と信用を構築し、重要なオープンソース インフラストラクチャの継続的なメンテナンスをサポートすることが緊急の課題であるという前提から出発しました。議論の鍵となったのは、これらの目的を達成するためにOSSコミュニティをどのように組織化するのが最善であるかという点でした。

オープンソースのセキュリティには、メンテナーコミュニティと協力するための新しいパラダイムが必要です

分散型イノベーションにより、素晴らしいコンポーネントが紡ぎあげられています。それらのオープンソース コンポーネントは、デジタル経済をサポートするために広く展開されています。会議の参加者が説明したように、これらのコンポーネントは、送電網、配送、輸送から電子商取引や金融に至るまで、世界的な商取引の基盤を提供する多数の重要なインフラストラクチャに組み込まれています。どのコンポーネントが最も広く使用されており、悪用に対して最も脆弱かを理解することは、オープンソース エコシステムとより広範なデジタル経済の健全性を継続するために非常に重要です。ある参加者が指摘したように、そうすることは、日常のインターネット ユーザーに安全なインフラストラクチャを提供するためにも不可欠です。

ジュネーブのオープンソースのリーダーたちは、現在使用されている様々な OSS コンポーネントを維持することは複雑な課題であり、透明性と調整されたアプローチ、そしてオープンソース インフラストラクチャを活用し主に利益を得ている組織から、より大規模な資金とリソースの投入が必要であると認識しました。より具体的には、会議参加者は相互に関連するいくつかの課題を指摘しました。

1 つ目の課題は、OSS が増加する状況を追跡し、潜在的な脆弱性を監視することです。サプライ チェーン全体の実稼働アプリケーションには何十万もの OSS パッケージが存在するため、どの OSS コンポーネントが最も広く使用されているかを正確に理解することは簡単な作業ではありません。セキュリティ インシデントが発生した場合、品質とメンテナンスを保証する中央当局が存在しないため、潜在的な脆弱性を調整して開示し、問題を修正する責任を割り当てることは困難になります。オープンソースのエコシステムによって、共通のプロセスと統一されたベストプラクティスを適用できる必要があります。

2 つ目の課題は、現在使用されている膨大な数の重要な OSS コンポーネントを維持することです。会議の参加者らは、ほとんどの場合、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に、公式なリソース割り当てがなく、正式な要件や基準がほとんどないことを指摘しました。Linux などの注目度の高いプロジェクトには活発なコミュニティがあり、定期的に注目を集めていますが、他のプロジェクトに頻繁な更新はなく、その状況を把握する人もほとんどいません。

何名かの参加者は、メンテナンス担当者、特に定期的な更新やメンテナンスを実行するための時間とリソースが不足している担当者に対し、セキュリティに重点を置くための補償を提供することを提案しました。補償とは、必ずしも追加の財源を投入することを必要とするわけではありません。EleutherAI などの OSS プロジェクトは、主要なライブラリのコードや学術研究論文で引用したデータに対し、すばらしい貢献をし

た方の名前を追加することで、貢献やメンテナンス活動を奨励してきました。

会議の参加者はまた、2021 年に資金提供プロジェクトとなった Open Source Security Foundation（OpenSSF）の取り組みを歓迎しました。OpenSSF は、公共部門、民間部門、コミュニティの間で OSS を保護する取り組みを調整する上で重要な役割を果たしています。その重要な役割とは、サポートされていない領域またはリソースが不足している領域にリソースを振り向けることです。課題の規模を考慮し、会議参加者はセキュリティの脆弱性を根本的かつ大規模に解決するために、より持続可能な資金源を求めました。

こうした課題がありますが、会議の参加者は、OSS がプロプライエタリ ソフトウェアよりも本質的に安全性が低いわけではないことを熱心に指摘しました。実際、オープンソースには、透明（誰でもコードをレビューできる）、脆弱性が発見されたときのコミュニティからの迅速な対応、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て強化する機能など、セキュリティ上の利点があります。

デジタル対応の製品やサービス全体でサイバー攻撃やデータ侵害が急増しておりサイバー セキュリティの重要性に対する意識が高まっています。

OSS エコシステムは、セキュリティ上の課題に対処するためのタレントとの関係構築を助ける必要があります

前述したように、多くのオープンソース プロジェクトは、資金や人材など限られたリソースで運営されています。人材の不足は、プロジェクトのセキュリティ監査の実施、脆弱性への対応、またはタイムリーなサポートの提供に影響を与える可能性があります。しかし、会議の参加者らは、関連するもう一つのシステム上の課題、つまり業界全体のサイバー セキュリティ専門家の不足を指摘しました。

デジタル対応の製品やサービス全体でサイバー攻撃やデータ侵害が急増しており、サイバー セキュリティの重要性に対する意識が高まっています。脅威がより巧妙になるにつれて、それらを防御するための熟練した専門家の需要が大幅に増加しています。さらに、クラウド コンピューティング、モノのインターネット、モバイル デバイスの成長に伴い、攻撃対象領域が大幅に拡大し、システムとデータのセキュリティを確保する上で新たな課題が生じています。サイバー セキュリティは、ネットワーク セキュリティ、アプリケーション セキュリティ、侵入テスト、インシデント対応、法規制順守など、さまざまな専門分野を持つ幅広い分野でもあります。大企業は、人材獲得の競争が激化する世界市場で、適切な専門分野を備えた専門家を見つけるのに苦労しており、そのことがオープンソース プロジェクトの課題をさらに厳しいものにしています。

これらの課題を考慮して、会議の参加者は OSS コミュニティに検討すべき一連の質問を提起しました。セキュリティをより迅速に進めるために、コミュニティにどのようなツールやトレーニングを提供できるか？セキュリティの専門家であることの意味を再定義することはできるか？開発者の多様性を高めて、新しい才能をエコシステムに引き付けることはできるか？コンピュータ サイエンス プログラムにおけるサイバー セキュリティへの注目を高めることに貢献できるか？

サイバー セキュリティの人材不足に対する将来的な解決策としては、サイバー セキュリティのトレーニング プログラムや認定コース、最新のサイバー セキュリティ カリキュラムを作成するための大学との提携、人材

の不足を埋めるための DEI の取り組みなどが挙げられます。会議参加者は、OSS ファウンデーションがこれらの優先事項についてさらなる議論と行動を追求すべきであることに同意しました。

最後に、関連する見解として、会議の参加者は、多くの中小企業が OSS に依存しているものの、IT セキュリティを管理するための社内リソースが限られていると指摘しました。ある参加者は、中小企業の 95% にはソフトウェア セキュリティを管理する人材がいないと推定しています。IT セキュリティを管理するためのリソースが不足しているため、OSS コミュニティのタイムリーなサポートに中小企業コミュニティは特に依存しています。

セキュリティ バイ デフォルトとは、最初らセキュリティを第一に考えてソフトウェア アプリケーションを設計・開発し、セキュリティを後回しにするのではなく、デフォルトの状態にすることです。

OSS コミュニティではセキュリティ バイ デフォルトを優先する必要があります

サイバー セキュリティに関する議論の締めくくりとして、会議の参加者は、OSS コミュニティが「セキュリティ バイ デフォルト」モデルに移行する必要性について語りました。セキュリティ バイ デフォルトとは、最初からセキュリティを第一に考えてソフトウェア アプリケーションを設計・開発し、セキュリティを後回しにするのではなく、デフォルトの状態にすることです。ジュネーブに集まったオープンソースのセキュリティ リーダーによると、重要なステップには、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、ソフトウェアがデプロイされ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。

会議の参加者は、セキュリティ バイ デフォルト モデルを採用し、セキュリティ テストと保守のプロセスを自動化することで、OSS アプリケーションのセキュリティ侵害や脆弱性の可能性を大幅に低減できることに同意しました。また、開発者や保守担当者をエコシステムにおける他の重要な作業に解放することができます。ある参加者は、「セキュリティ バイ デフォルトを実現すればするほど、より高次の問題に集中できるようになる」と述べています。

分散型組織における技術的な政策の影響：課題と機会

サイバー セキュリティをめぐる議論は、OSS エコシステムの継続的な成功と回復力にとって、優れたガバナンスと政策への関与がますます重要になっている理由を浮き彫りにしました。しかし、サイバー セキュリティ以外にも、オープンソース ソリューションのユーザーや開発者に大きな課題と機会をもたらすインターネットに関連する政策の問題は数多くあります。たとえば、知的財産権、プライバシー、製造物責任法、独占禁止法などの重要な問題において、オープンソース コミュニティは、技術的な政策の対話において必要なほどの影響力や主張力を持たず、その結果、オープンソース モデルを危険にさらす規制に関する活動につながったという見解が広く共有されています。同時に、OSS は、現代の極めて重要な政策的な課題の多くに対処するソリューションを提供しています。しかし、政策グループにおけるコミュニティの知名度の低さは、コミュニティの社会経済的貢献が過小評価されがちであることを意味します。

オープンソースのリーダーたちがジュネーブに集まり、最近の規制措置がオープンソースのエコシステムに及ぼす影響、OSS のユニークな特性と方法論について世界の政策コミュニティを教育する必要性、効果的な政策への関与と主張のために OSS ファウンデーションがコラボレーションと能力開発を強化することを優先する必要性などについて、自然に議論が行われました。

OSS の普及により規制は避けられないものに

オープンソース ソフトウェアは、今日の技術状況の基本的かつ広範な要素となっています。さまざまな領域のイノベーションを支え、開発者や組織間のコラボレーションを促進し、強力なソフトウェア ツールやソリューションへのアクセスが一般化する中で、その影響力は拡大し続けています。ウェブ開発や機械学習から、クラウド コンピューティング、データ サイエンス、科学研究まで、さまざまなアプリケーションを含む最新のソフトウェアソリューションの 70 ～ 90% は、オープンソース コンポーネントによって支えられているという試算もあります。[4]

OSS の普及に伴い、規制当局による監視も強化されています。例えば、サーバーやクラウドコンピューティング市場における Linux オペレーティングシステムの優位性は、競争や独占禁止法上の問題に対する懸念を引き起こしています。ヨーロッパの General Data Protection Regulation（GDPR）のようなデータ プライバシー規制は、データ処理と保存のための OSS パッケージがデータ保護の法律に準拠しているかどうかに注目しています。Log4Shell の後、規制当局は、組織がオープンソース コンポーネントを適切に管理し、セキュリティの脆弱性に対処しているかどうかを調査しています。より広範には、サイバー セキュリティと重要なインフラとしての懸念から、国や企業のサイバー セキュリティ戦略におけるオープンソース ソリューションの役割が評価されています。

会議の参加者は、欧州は技術的な政策にとって極めて重要な「戦場」であるとし、欧州は技術的な政策においてしばしば先手を打つ一方、米国は様子見の姿勢を取りがちであると指摘しました。実際、欧州の規制当局は、データ プライバシーの保護、競争の促進、サイバー セキュリティの確保、新興技術がもたらす社会経済的課題への対応など、他のどの地域よりも迅速に動いています。過去 5 年間だけでも、欧州はデータ保護とプライバシーの基準を定める GDPR、大規模なデジタル プラットフォームを規制し、反競争的行為を防止するデジタル市場法（Digital Markets Act）、違法コンテンツと闘い、オンラインサービスの透明性を高めるデジタルサービス法（Digital Services Act）、AI の開発と利用を規制する AI 法（AI Act）を導入しました。最近では、欧州がデジタル要素を含む製品のサイバー セキュリティ要件を強化するために CRA を提案し、製造物責任指令（Product Liability Directive）をデジタル時代向けに更新しました。

OSS がデジタル経済において重要な役割を担っているにもかかわらず、欧州の技術的な政策や規制当局が立法プロセスにおいて批判的であること。政策コミュニティとの関わりの欠如は、OSS エコシステムのユニークなニーズや視点、その方法論、OSS ソリューションの社会経済的影響に対する配慮の欠如につながります。会議の参加者は、CRA のような規制は、デフォルトとしてプロプライエタリなソフトウェア開発を前

提としており、その開発やライセンスモデルを含む OSS の明確な特性を適切に理解または説明していないと主張しました出席した欧州の OSS リーダーたちは、CRA の文書化、認証、および責任に関する規定は、OSS 開発に冷ややかな影響を与える可能性があると予測しています。[5] 一方、OSS の開発と配布のユニークなダイナミクスを考慮した、より包括的な規制プロセスは、サイバー セキュリティを強化し、オープンソースのエコシステムに利益をもたらす可能性があります。

オープンソース エコシステムの継続的な成功には、政策提言と教育が不可欠です。

会議の参加者が最も恐れているのは、政策立案者がオープンソースのエコシステムがどのように運営されているかを理解しておらず、コミュニティを成功に導くコラボレーション モデルを故意または無意識のうちに壊すリスクのある規制や政策を導入していることです。何人かのファウンデーションのリーダーは、政策立案者は規制するすべてのことに必ずしも深い専門家ではないため、業界内部の人々の専門知識に依存していると指摘しています。主要な技術的な政策問題に対するオープンソースの協調的な対応の欠如が空白を生み、最終的に、より大きな、より優れたリソースを持つ団体に支配される可能性を残しているケースもあります。

一般的に、OSS ファウンデーションは専任の政府関係組織を運営する資金的余裕はありません。それでも、OSS ファウンデーションは、主要な政策課題に対して積極的に取り組んできました。何人かのファウンデーションのリーダーは、Log4Shell のセキュリティ インシデントをきっかけに、政策立案者にオープンソース コンポーネントについて何時間も何時間も啓蒙活動を行ったと回想していますが、そのような努力は表面的なものに過ぎないと指摘しています。OSS ファウンデーションは、オープン スタンダードとオープン ソースの利点について政策コミュニティの教育にもっと投資すべきだという声が数多く聞かれました。

会議の参加者は、政策立案者が教育を必要としているいくつかの重要な問題を特定しました。例えば、オープン スタンダードとは何か？オープンソースの収益モデルはどのように機能するのか？ OSS はソフトウェア市場における競争と選択にどのような影響を与えるのか？また、インターネット セキュリティ、製造物責任、知的財産（いくつか例を挙げます）をめぐる政策は、オープンソースの製造および配布モデルにどのような影響を与えるのか？などです。

ジュネーブに集まったオープンソースのリーダーたちは、政策立案者や規制当局と友好的でお互いにメリットのある関係を築くことを広く支持していました。しかし、会議の参加者は、OSS コミュニティは標準規格が武器化される可能性を警戒しなければならないとも警告しました。ある参加者は、標準規格は長い間、国家経済戦略の要素として利用されており、技術的優位性のある領域で標準規格を整える取り組みは、国家競争上の優位性を与えることができると指摘しました。そのため、一部の当事者は、オープンスタンダードの開発を進める代わりに、国益や 技術のリーダーシップを促進する目的として、標準化プロセスを採用する危険性があります。国の当事者が地政学的な意図を推進するために OSS を武器化する可能性があるという現実は、コミュニティメンバーが力を合わせて OSS の中立性を守り、全人類の集合知としての OSS の重要な役割を強調する必要性を裏付けています。

効果的な政策活動には、専門的なスキルと OSS ファウンデーション間の連携強化が必要です

ジュネーブでのディスカッションで繰り返し議論されたのは、政策提言活動は OSS 開発作業とは大きく異なり、専門的なスキルセットとコミュニティの協力体制の強化が必要であるという考え方でした。会議の参加者の何人かは、ソフトウェアに携わるエンジニアと、欧州委員会のような規制機関で働く政策担当者との間には、しばしば隔たりがあると指摘しました。そのため、OSS ファウンデーションには、規制機関がどのように政策を作成するかについての微妙な理解を含め、政策審議に関与するために必要なスキルセットと知識を習得する責任があります。その他の重要な能力としては、法律的な洞察力や規制の状況に精通していること、複雑な技術的概念を非技術的な聴衆に伝える能力、特定の技術的な政策に対する認識を高め、支持を集めるための提言や公の場でのスピーチ、コミュニティとの連携するスキルなどが挙げられます。

会議の参加者は、オープンソース エコシステムに利益をもたらす政策変更に影響を与えるには単に能力構築への長期的なコミットメントだけでなく、政策コミュニティとの関係構築への投資も必要であることに同意しました。何人かの参加者は、政策に影響を与えるには長いプロセスが必要であり、多くの場合、粘り強さと長期的な政策目標に向かって努力する能力が必要であると主張しました。また、ジュネーブに参加した OSS ファウンデーションの多くは、政策活動に必要な人材が不足していると指摘しました。OSS ファウンデーションの中には、専門のロビイストを雇っているところもありますが、会員企業の多くが大規模で潤沢な資金を持つ政府広報活動から、さらなる支援を得ることができるのではないかという意見もありました。ある参加者は、「政策関係者の関与のレベルは高まっていますが、関係構築のためにはより多くのリソースと持続的な努力が必要です」と述べています。

最終的に、OSS ファウンデーションのリーダーたちは、コミュニティが政策アジェンダに影響を与えることを成功させるためには、政策に関するコミュニティ全体の協力が不可欠であることに同意しました。一般的な意見としては、OSS ファウンデーションは、ソフトウェア開発に関するコラボレーションには優れているが、政策やガバナンスに関するコラボレーションに関しては劣っているということでした。多くのファウンデーションは、サイバー セキュリティ、AI、プライバシー、知的財産、その他の関連事項に関する新しい政策を提案するために、オープンソースのファウンデーションが協力することを望んでいます。会議の参加者はまた、様々な政策チーム間のつながりを構築し、コミュニティ全体で政策提言の能力を高め、政策問題に関してファウンデーション横断的な協力体制を確立するためには、より多くの議論が必要であるとの意見で一致しました。ある参加者は、「私たちは、ファウンデーションとしての取り組みをよりよく調整できるように、規約やメンバーの関心事、政策に影響を与えるための取り組みなど、互いをよりよく理解する必要があります」と述べています。

政策審議に関与するために必要なスキルセットと知識を習得する責任があります。

コラボレーションをグローバルに、オープンに、包括的に：輸出規制、デジタル主権、DEI の影響の検証

何十年もの間、OSS 開発における自由なグローバルコラボレーションは、オープンソースプロジェクトに貢献する有能な開発者の数を増やしてきました。2022 年には、200 カ国以上から 8,300 万人以上の開発者が GitHub のオープンソースプロジェクトに貢献しました。重要なのは、GitHub のグローバルユーザーの約 74% が米国以外に居住しており、アジア、中南米、東欧を拠点とする開発者の割合が大幅に増加していることです。一方、画期的な OSS のイノベーションは、日本（Ruby）、フィンランド（Linux）、南アフリカ（Ubuntu）などから生まれています。

オープンソースがかつてないグローバルな成功を収めている一方で、ジュネーブに集まったコミュニティのリーダーたちは、世界的な貿易摩擦、地政学的対立、デジタル主権への注目の高まりが、オープンで包括的なコラボレーションに真の障害をもたらすという懸念を表明しました。例えば、テクノナショナリズムの高まりは、米国、中国、その他の国々に対して、半導体、無人航空機、全地球測位システム、さまざまな軍事用電子機器やソフトウェアシステムなどの重要技術に対する輸出規制の強化を促しています。コミュニティのリーダーたちは、テクノナショナリズムの政策が OSS の開発を地域のサイロに分断し、より大きなインクルージョンを育み、コミュニティの人材の層を厚くする努力を挫折させるのではないかと議論しました。

このようなリスクを踏まえ、会議の参加者は、国境を越えた知識と技術の自由な流れを維持するための様々な選択肢について検討しました。会議の参加者はまた、オープンソースプロジェクトリーダーが多様な参加者を統合し、オープンソースの行動基準、倫理、ベストプラクティスの普及を成功させるための方策についても議論しました。

デジタル主権がオープンソースにチャンスと課題をもたらす

デジタル主権は、ジュネーブにおける主要な議論のトピックであり、デジタル技術やデータの流れに対する国の管理を強化する取り組みが、どの程度オープンソース運動を促進するのか、あるいは阻害するのかなどについて議論されました。デジタル主権とは、外国政府や企業から不当な影響を受けることなく、自国のデジタル技術、データ、情報の流れを国境内で管理する国の能力のことです。デジタル主権とは、国家が自国の価値観、利益、安全保障上の懸念に沿った形で、デジタルインフラ、政策、規制に関する決定を下す権限を持つべきだという考え方を包括するものです。

近年、さまざまな国がデジタル主権を導入していますが、その背景には、データ プライバシー、国家安全保障、経済成長、外国のテクノロジープロバイダーへの依存を減らしたいという懸念があります。例えば、ロシアと中国は、データの国内での利用を義務付ける法律を導入し、データを国内で保存、管理するための独自のクラウドインフラの構築に投資しています。一方、欧州は、国民のデータ保護とプライバシー保護を強化するため、先駆けて 2018 年に GDPR を施行しました。GDPR に続いて、デジタル市場法（Digital Markets Act）、デジタルサービス法（Digital Services Act）、欧州半導体法（European Chips Act）が施行され、目前に迫った EU の AI 法（E.U. AI Act）と合わせて、デジタル主権に関する取り組みが一斉に開始されました。これらの新法の目的は、デジタル空間における欧州市民の権利を守るだけでなく、米国の大手ハイテク企業との競争に打ち勝つために欧州企業の競争力を高めることにあります。[6]

デジタル主権は、各国が自国のデジタル環境をよりコントロールできるようにすることを目的としていますが、インターネットの断片化、国境を越えたデータの流れの障壁、国際規範との軋轢、ソフトウェア開発者やテクノロジー企業にとっての規制遵守の負担増といった課題にもつながりかねません。ジュネーブに集まったコミュニティのリーダーたちは、デジタル主権は規制の調和という目標としばしば対立するものであると主張しました。オープンソース ファウンデーションは、さまざまな国や文化が技術的な政策問題に取り組む方法には常に違いがあることを理解しています。しかし、新たな規制の急増はコンプライアンスにかかるコストを増加させ、リーダーたちは、リソース不足の OSS ファウンデーションが世界中の技術的な政策と足並みをそろえることは困難であると指摘しました。ある参加者は、「オープンソースは、ソフトウェア産業全体を規制しようと急ぐあまり、巻き添えを食う危険性がある」と述べています。

一方、オープンソース会議の参加者の中には、デジタル主権の取り組みがオープンソース コミュニティに利益をもたらす可能性を示唆する者もいました。例えば、デジタル主権を追求するために、一部の国はプロプライエタリな技術への依存を減らすために OSS を採用しています。その一例として、会議の参加者の一人は、欧州はオープンソースとオープン スタンダードを活用しなければ、より大きな技術的自律性を達成することはできないと主張しました。これは欧州のユーザーがベンダー ロックインを避け、テクノロジー スタックに対するコントロールを得ることになります。言い換えれば、オープンソース ソリューションの構築と使用における欧州のリーダーシップが同様に強力な救済策を提供するのであれば、欧州の人々はデジタルにおける自律性を拡大するために必ずしもソースコードを所有する必要はないということです。

テクノ ナショナリズムの政策がオープンソースコミュニティの分裂とサイロ化を引き起こしています

デジタル主権とは、主に、国家が決定した要請に沿った形で、デジタルインフラ、政策、規制を管理する上で、国家政府の自主性を高めたいという願望に関するものです。しかし、会議の参加者は、デジタル主権の追求が地政学的な対立に巻き込まれ、不信感を増大させる雰囲気、あるいは一部のアナリストがテクノ ナショナリズムと呼ぶ雰囲気を醸成している場合があると警告しています。

シンガポール国立大学の Alex Capri 氏は、テクノ ナショナリズムを「国家の技術的能力と企業を、国家の安全保障、経済的繁栄、社会的安定の問題と結びつける重商主義的な行動」[7] と定義しています。一例として、Capri は「ハードウェア関連技術の輸出規制が目に見える形で着実に進み、次いでデータへのアクセスや利用が制限され、そして最近では、人的資本の自由な移動と発展を妨げる新たな規制が始まっている」と述べています。

テクノナショナリズムは、国家の自治を強化するだけでなく、ロボット工学や AI から産業インターネットや高度通信ネットワークに至るまで、21 世紀を支配すると考えられている技術論理分野でトップに君臨するためのより積極的な対策を含んでいます。世界有数の経済大国間で国家技術の優位性をめぐる競争は熾烈を極めており、エコシステムのリーダーらは、地政学的な緊張とそれに伴う政策介入が技術の進歩を遅らせ、OSS コミュニティが依存している国際協力を損なう可能性があると懸念しています。[8]

何十年もの間、テクノロジーは相互関係を強化し、グローバルなコラボレーションを推進してきました。OSS はその好例です。会議の参加者は、かつては何の問題もなかったオープンソース カンファレンスの開催地に関する決定も含め、今日の環境ではグローバルなコラボレーションが政治的な危険にさらされていると指摘しました。欧米諸国に本社を置く企業が、法的な不確実性や国内での政策の反発のリスクを理由に、地政学的にライバル関係にある企業が参加する国際的なオープンソース プロジェクトに参加したがらないケースもあります。また、国際的な紛争や制裁によって、さまざまな国籍の貢献者がオープンソース コミュニティから排除されるケースもあります。[9]

参加者は、テクノ ナショナリストの政策や傾向が、オープンソースのエコシステムにおける参加とコミュニティ管理の力学に与える影響について、いくつかの批判的な質問を投げかけました。例えば、「エンティティリスト」（米国の国家安全保障や外交政策上の利益を脅かす活動に関与する組織に対して、特定の機密技術やコンポーネントの輸出を制限するために米国商務省が管理する外国人や組織のリスト）に掲載されている企業と、どのようにオープンに協力するのか？信頼に値しないと疑われる様々な国からの貢献者に対して、私たちはどのように安全保障政策に取り組むべきなのでしょうか？ロシアのウクライナ侵攻を受け、貢献者がその国籍ゆえに嫌がらせを受けている場合、ファウンデーションとしてどのように介入すべきでしょうか？

ジュネーブでの話し合いは、地政学上の緊張の高まりによってもたらされた厄介な問題のいくつかを解決するには至りませんでした。しかし、会議の参加者はいくつかの方針で合意しました。

1. オープンソース ファウンデーションは、コミュニティとその主要なプラットフォームが地政学的な境界線に沿って分断されることに反対し、国境を越えた知識、技術、コラボレーションの自由な流れを維持することを提唱しなければならないという点で意見が一致しました。
2. オープンソースのリーダーたちは、誰が、どのような条件で、どのような目的でオープンソース コミュニティに参加するかという技術的な決定が、政治的な配慮によって支配されるような状況を避けたいと考えています。
3. 会議の参加者は、政治的に中立な姿勢と、コミュニティへの貢献を管理するための透明性質を持つプロトコルが、オープンソース プロジェクトが地政学的な緊張に左右されることなく運営され、才能ある開発者といつどのように関わるかを確実にする鍵であると指摘しました。
4. Open Source Congress を毎年開催することで、国際的な対話が促進され、世界のさまざまな地域を代表する OSS ファウンデーション間でベストプラクティスが共有されるという点で、幅広い合意が得られました。
5. また、オープンソースのリーダーたちは、政治家や規制当局と関わる際、OSS ファウンデーションは、国境でコラボレーションを閉鎖する国は、グローバルな協力とその利点を受け入れる国よりも成功しないというメッセージを広めるべきだという点でも意見が一致しました。

かつては何の問題もなかったオープンソース カンファレンスの開催地に関する決定も含め、今日の環境ではグローバルなコラボレーションが政治的な危険にさらされている

ダイバーシティ（多様性）とインクルージョン（包括性）は、オープンなコラボレーションにおけるこれからの景色と対話において不可欠な要素です

かつては米国と西ヨーロッパに強固に根ざしていたオープンソース コミュニティも、今日ではますますグローバルで国際的なものとなっています。例えば、中国はオープンソース テクノロジーの主要な利用者で、貢献者でもあります。中国企業の 90% 近くがオープンソース テクノロジーを使用しているだけでなく、中国のユーザーは GitHub で米国のユーザーに次いで 2 番目に多いグループです。[10] しかし、中国だけではありません。インド、ロシア、韓国、ウクライナなど、多くの新興経済国にはオープンソース開発者の大規模なコミュニティがあります。中低所得国にとって、オープンソース コミュニティとの関わりは新たな起業を生み出し、経済発展のペースを加速させています。

オープンソースが世界的に繁栄している一方で、ジュネーブに集まったオープンソースのリーダーたちは、言語、文化、そして欧米中心の制度の伝統が、才能ある開発者の参加を最大限に引き出すための障害となっていると警告しています。オープンソース コミュニティはますます国際的になっていますが、会議の参加者の何人かは、ほとんどのオープンソース プロジェクトを形成する上で、米国に本社を置く組織が圧倒的な影響力を持っていると主張しました。北米の参加者の優位性は、世界の他の地域で生まれたオープンソース プロジェクトに影を落とす可能性があります。

会議の参加者は、ダイバーシティとインクルージョンの問題への取り組みの失敗が、グローバルな OSS エコシステムの才能と独創性へのアクセスを抑制し、それによってイノベーション、アクセス、社会的インパクトを最大化する能力が損なわれることを懸念しています。ある参加者は、「歓迎されていないと感じる人々は、他の方法でテクノロジーを構築するでしょう。残念ながら、それは優秀な人材が無償で貢献する時間やリソースがないため、プロプライエタリな技術を構築してしまうことを意味します。

異なる言語や文化をオープンソース コミュニティに統合するという課題は新しい問題ではなく、グローバルなインクルージョンを促進するエコシステムの能力に相当の信頼が寄せられています。しかし、会議の参加者は、コミュニティがグローバルなインクルージョンを促進するためにもっとできることがあるとの意見で一致しました。例えば、参加者の中には、プロジェクト コミュニケーションのための迅速な機械翻訳機能に投資する必要性を強調する人もいました。英語はソフトウェア世界の共通語かもしれませんが、OSS のリーダーたちは、プロジェクトコミュニケーションをローカライズすることで、北米以外の開発者の参加を促進することができると主張しています。

会議の参加者はまた、オープンソースの行動基準を普及させ、業界の男らしい「仲間」文化を手なずけ、コミュニティの対話と意思決定においてプロフェッショナリズムを育成することの重要性についても議論しました。何人かの参加者は、行動規範はコミュニティの行動基準を確立し、多様な参加を促進し、包括的な環境を作り出すための重要なツールであると指摘しました。しかし、自分たちの自由と自治を非常に大切にすることで知られている、オープンソース コミュニティでは、行動規範がしばしば物議を醸してきました。コントリビューターのコミュニティから反発を受けることもあり、コミュニティの行動基準や行動規範の実施は、微妙なバランスの上に成り立っています。何人かのファウンデーション スタッフは、行動規範の執行をめぐって嫌がらせを受けたと報告しています。ジュネーブでは、OSS ファウンデーションは、コミュニティにおける多様性と包摂を促進する行動規範を作成し、実施するための協調的なアプローチに取り組むべきだということで、幅広い合意が得られました。

AI はすべてを変えるのか？オープンとは何か？責任、倫理、価値観

人工知能（AI）とは、知覚、学習、推論、複雑な問題解決、意思決定など、これまで人間の知性を必要としていたタスクをコンピュータが実行する能力と定義できます。機械学習、自然言語処理、コンピュータビジョン、ロボット工学、エキスパート システムなど、幅広い技術やアプローチを包含する幅広い分野です。

近年、AIは私たちの日常生活にますます溶け込んでいます。ジェネレーティブAI、音声アシスタント、レコメンデーション システム、パーソナライズされた広告（パーソナライズされた看板さえも）など、AIを活用したアプリケーションやサービスは一般的なものとなりました。しかし、私たちのデジタル体験の変革はまだ始まったばかりです。ロボット手術から自律走行車、画期的なバイオテクノロジー研究からCTスキャンの読み取りまで、ますます賢くなっていく機器のアプリケーションは、医療、法律、金融サービス、輸送、建設、農業、製造など、多岐にわたります。

現在、グーグル、フェイスブック、マイクロソフト、IBM、テンセント、アリババ、AWS、そして膨大なデータセットとコンピューティング パワーを利用できるほとんどの大手企業など、多くの企業がAIの取り組みを開始しています。International Data Corporation（IDC）は、当面のAI支出の平均成長率を26%と予測しています。10年間維持されれば、この雪だるま式投資は10倍以上の増加をもたらすでしょう。ソフトウェア企業だけではありません。2023年半ばには、JPモルガンの全募集ポジションの約40%がAI関連で、データ エンジニアやクオンツ アナリストのほか、倫理やガバナンスの役割もありました。

OSS コミュニティにとって、AI はさまざまな機会と課題をもたらします。ジュネーブに集まったコミュニティのリーダーたちは、オープンな AI の定義について一致させる必要性や、AI 対応のコードジェネレータがライセンス、セキュリティ、知的財産権にもたらす課題について議論しました。最後に、会議の参加者は、AI のより広範な社会的影響と、偏見、プライバシー、人類への存続的脅威などの問題に対処するためのオープンソース コミュニティの役割についても考察しました。

AI におけるオープン性はソースコードへのアクセスだけではない

AI におけるオープン性の本質とそれが持つ意味に関する議論は、AI における責任ある開発に関する議論の焦点となりました。会議の参加者は、関連する一連の質問と格闘しました。責任ある AI に対して私たちが期待することは何か？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？

OSS では、オープン性の定義は確立されています。オープンソースの定義によると、OSS とは、誰でも検査、拡張、配布できるソースコードを持つソフトウェアのことです。[11] さらに、OSS の使用、変更、配布に関して、開発者の権利とユーザーの権利を規定するフレームワーク、ライセンス、法的な理解もあります。

同じ OSS のプロトコルや定義が AI システムにシームレスに適用されるわけではありません。Stefano Maffulli が最近のブログ記事で書いているように、「（OSS のコードで）バグを見つけたとき、あなたは誰を責めるべきか、どこに報告すべきか、そしてどのように修正すべきかを知っています。しかし、AI に関しては、バグやエラー、偏りを修正するために何をすべきかを同じように理解しているでしょうか？」[12]Maffulli やジュネーブの会議の参加者によれば、その答えは明白な「ノー」でした。

AI の分野は主に、データを処理・分析し、パターンを学習し、プログラムされたルールや統計モデルに基づいて、あるいは単にデータその

ものから連想や思考を導き出して意思決定を行うことができるシステムを作り出すことに焦点を当てています。ニューラル ネットワークの意思決定プロセスは、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おり、人間の理解の範疇を超えているため、基礎となるモデルはブラック ボックスと表現されます。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できないことを認めています。[13]

ジュネーブの会議の参加者は、説明能力を高めるとは、AI システムが特定の決定、推奨、予測に至った理由を表現する能力を向上させることだと主張しました。説明可能性が重要なのは、病気の診断や誰がクレジットにアクセスできるかの決定など、人生を左右する決定をますます形作るシステムの信頼性、安全性、説明責任を高めるためです。ジュネーブの会議の参加者は、説明能力を高めるとは、AI システムが特定の決定、推奨、予測に至った理由を表現する能力を向上させることだと主張しました。説明可能性が重要なのは、病気の診断やクレジット利用者の決定など、人生を左右する決定をますます形作るシステムの信頼性、安全性、説明責任を高めるためです。ルイビル大学のコンピューターサイエンス教授である Roman V. Yampolskiy 氏が最近の論文で説明しているように、「もし我々が持っているものが “ブラックボックス “だけであれば、故障の原因を理解し、システムの安全性を向上させることは不可能です」。さらに Yampolskiy は、説明のない AI の答えを信頼することは、AI をオラクルシステムとして扱うことと同じだと主張します。危険なのは「（AI システムが）間違った答えや操作的な答えを出し始めたとしても、それを見分けることができなくなる」ことであると、Yampolskiy は言います。[14]

会議の参加者によると、AI の説明可能性を高めるには、モデル内のさまざまな変数に適用される重み、訓練に使用されるデータの種類など、モデル アーキテクチャを理解する必要があるとのこと。残念ながら、AI システムが洗練されればされるほど、特定の見解を導き出した方法を正確に特定することは難しくなります。実際、AI の専門家の中には、AI の性能と解釈可能性の間にはトレードオフがあると主張する人もいます。[15] 言い換えれば、AI モデルを説明可能にすることは、モデルの複雑さを軽減し（例えば、ディープ ニューラル ネットワークではなく、決定木や線形回帰を使用する）、より小さく、より精選されたデータ セットでモデルを訓練する必要性を意味するため、AI の効果を低下させる可能性があります。

AI の透明性を高める点において、もう 1 つの頭を悩ませる要因は、AI システムの動作規模です。Maffulli が説明するように、「AI によって消費および生成されるデータの量は、テラ バイトやペタ バイト単位で測定されます。つまり、このサイズのデータ セットに対して高速な計算を実行するには、特別なハードウェアが必要になります…残念ながら、これらの大きな AI モデルを構築して実行するために必要なハードウェアは独自のもので高価であり、セットアップには特別な知識が必要です。」[16] 要するに、モデルの実行に必要な膨大なコンピューティング パワーは、第三者機関がその出力を調査することを困難にしているのです。したがって、AI の限界や偏りを表面化させる答えは、部分的には、グーグルやメタなどの企業が自社のモデルやシステムを外部の監査や信頼性テストに提出することにあるのかもしれません。

AI によって生成されたコードは、オープンソースのライセンス、セキュリティ、規制に課題をもたらすでしょう

ジュネーブでのもう 1 つの重要な論点は、ソフトウェア開発の世界で AI を利用したコードジェネレータの存在感が高まっていることです。ここ数年、GitHub の Copilot や OpenAI の Codex のような新しいツールは、自然言語のプロンプトに基づいて、単純な数行のコードだけでなく、完全なコードの関数を生成する能力で開発者を驚かせています。これまで何時間も、あるいは何日もかかっていたコーディング作業が、数秒で完了するようになったのです。GitHub は、AI コーディングが 2030 年までに世界の GDP を 1.5 兆ドル押し上げると予測しています。[17]

他の大規模な言語モデルと同様に、AI コード ジェネレータは、GitHub や他のプラットフォームでホストされている膨大なオープンソース コード ライブラリを含む、大規模なデータ セットで訓練されています。オー

プンソースのリポジトリには、世界中の開発者によって書かれた多様なコードが豊富に含まれています。これらのリポジトリは、膨大なプログラミング言語、プログラミング パラダイム、アプリケーション ドメインを包含しており、AI モデルをトレーニングするための実世界のコードの豊富で網羅的な源泉となっています。要するに、世界中の開発者コミュニティの経験と集合知を反映しているのです。

会議の参加者が指摘したように、欠点は、AI コードジェネレータの使用の増加は、ライセンス、セキュリティ、および規制遵守に関連する一連の課題を生み出すということです。これらの課題は、AI モデルによって生成されたコードに関連する出所の欠如に起因しています。例えば、OpenAI の Codex には、生成されたコードスニペットに影響を与えた元のコードを管理するライセンス スキームに関する情報は含まれていません。その結果、生成されたコードがプロプライエタリなのか、オープンソースなのか、あるいは他のライセンス スキームに該当するのかを確認するのは困難です。この不透明性により、プロプライエタリなコードやライセンスされたコードが不注意で誤用されるリスクが生じ、潜在的な侵害問題につながります。同様の懸念は、AI コードジェネレータが、学習させたコードベースに存在したバグやセキュリティ上の欠陥を再現しているかどうかという点についても提起されています。[18]

AI のコード ジェネレーターは、膨大な量のオープンソース コードで訓練されているため、AI が生成するコードの使用により、作成する新しいソフトウェア アプリケーションがオープンソース ライセンスによって管理されるべきかどうかについても問題を提起しています。[19] 言い換えると、AI が生成したコードは、オープンソースのコードベースの「派生物」とみなされるべきなのでしょうか？

ジュネーブでの議論では、これらの難問を最終的に解決することはできませんでした。しかし、参加者は、AI は今後ソフトウェア開発において常に存在するツールになる可能性が高いため、OSS ファウンデーションが AI が生成したコードを扱うための新たなフレームワークについて協力すべきだという点で意見が一致しました。

AI がもたらすシステムのリスクには、早急な、オープンソースによる対応が必要

AI開発への大規模な投資は、AIシステムがますます複雑な課題に取り組み、人間生活の様々な側面にプラスの影響を与えることを可能にし、急速な進歩を約束します。同時に、会議の参加者は、AIの影響力の増大が、偏見、透明性、プライバシー、雇用の喪失、人類への存亡の危機などに関連する新たなリスクや倫理的配慮を生じさせたと警告しています。

偏見と差別に注目してみましょう。人工知能システムは、訓練されたデータに存在するバイアスを受け継いだり、増幅したりする可能性があります。学習データに偏ったパターンや差別的なパターンが含まれている場合、AI システムはこれらのバイアスを強化し、さらには悪化させ、雇用、融資、刑事司法などの分野で不公平な結果を招く可能性があります。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、差別的な融資慣行を永続させる可能性があり、その結果、社会から疎外されたグループのクレジットやローンへのアクセスが不平等になる可能性があります。AI アルゴリズムを使って犯罪の多発地域を特定し、警察のリソースを割り当てる予測取り締まりシステムは、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して批判されています。

人工知能が作り出した差別は、そのモデルが学習されたデータに本質的に組み込まれたものであるため、発見が困難であり、その対策はさらに困難となる可能性があります。前述したように、AI モデルがどのように機能するかについて透明性が欠如している現状では、AI システムがどのように結論や予測に至るかを理解することは不可能です。意思決定のロジックや基礎となるデータの山が、解き明かしたりリバースエンジニアリングしたりすることがほとんど不可能な場合、どのようにして潜在的なバイアスを特定し、対処することができるのでしょうか？

偏見や差別は、ほとんどの場合、社会の偏見や権力構造を反映したデータを AI に学習させることによって、意図せずに生じるものです。しかし、AI のような強力なテクノロジーは、その能力を悪意のある目的のため

に意図的に悪用することは避けられません。実際、AIAAIC（AI, Algorithmic, and Automation Incidents and Controversies）レポジトリは、このような悪用がすでに日常化していることを示唆しています。同団体の最新報告書によると、新たに報告された AI の事件や論争の数は、2021 年には 2012 年の 26 倍に上ったとのこと。著者らは、「報告された事件の増加は、AI が現実世界に入り込む度合いが高まっていることと、AI が倫理的に悪用される可能性があるという認識が高まっていることの両方の証拠であろう」と結論づけています。[20] 2022 年には、ウクライナの Volodymyr Zelenskyy 大統領がロシアとの戦いに降伏するよう自軍に呼びかけるディープフェイク動画や、選挙からニュースの議題、ソーシャルメディアに至るまで、あらゆるものを操作する「ボット」の使用がかつてないほど増加するなど、注目すべき事件が発生しました。近い将来のリスクとしては、重要インフラへの身代金要求、自動運転車の事故、商用ドローンのミサイル化など、悪意ある人物がサイバーフィジカル システムを破壊的な目的のために利用する可能性があります。[21]

偏見、不正行為、雇用の喪失、AIを利用した犯罪やテロリズムなど、リスクは枚挙にいとまがありません。しかし、究極の本質的な問題は、魔神が瓶から取り出された今、人類がAIをコントロールできるかどうかということなのかもしれません。AIの専門家の多くは、AIシステムは最終的に超知能のレベルに達すると予測しています。超知能が実現する時期については、さまざまな憶測や議論があります。しかし、それが実現すれば、AIシステムは自らの目標を優先し、人類にとって有害な行動をとる可能性があります。

危機的な状況を踏まえ、ジュネーブの OSS リーダーたちは、AI 技術の課題をよりよく理解し、責任ある開発と導入を確保するために行われている様々な取り組みを歓迎しました。最も注目すべきは、2023 年 3 月 29 日、AI コミュニティーの 5,000 人以上が、リスクが適切に調査され軽減されるまで、GPT-4 のような大規模言語モデルの開発を少なくとも 6 ヶ月間停止することを求める公開書簡に署名したことです。著名な署名者には、OpenAI を共同設立した Elon Musk、ロンドンに拠点を置く Stability AI を設立した Emad Mostaque、Apple の共同設立者である Steve Wozniak、Amazon、DeepMind、Google、Meta、Microsoft などのエンジニアが含まれています。[22] 公開書簡では、「新しく優れた規制当局」、「強固な監査と認証のエコシステム」、AI が引き起こす可能性のある「劇的な経済的・政治的混乱に対処するための十分なリソースを備えた機関」の必要性を訴えています。さらに、「強力な AI システムは、その効果がポジティブなものであり、そのリスクが管理可能なものであると確信できる場合にのみ開発されるべきです。」と、付け加えています。[23]

この公開書簡は、AI コミュニティの関心の高さを象徴するものです。しかし、この一時停止措置の案は、一時停止措置に強制力があるのかどうかなど、答えと同じくらい多くの疑問を投げかけています。実際、まもなく数兆ドル規模になるであろうこの産業の競争において、どの政府や企業も、AI 技術のリーダーたちに一方的に開発の一時停止を強制し、ライバルに大きな優位性を譲り渡すリスクを冒すことはなさそうです。[24]

ジュネーブに集まった OSS のリーダーたちにとって、AI の責任ある開発と展開の鍵は、必ずしも一時停止ではなく、むしろオープンと透明性の向上へのコミットメントです。AI システムの最大手開発者の多くが AI モデルをクローズドに保つことを主張している一方で、会議の参加者の何人かは、AI モデルをオープンに開発することには利点があると主張しました。これらの利点には、コードを監視する目を増やし、AI システムの信頼性を確保するために必要な透明性を生み出すことが含まれます。

要するに、ジュネーブでの議論から得られたコンセンサスは、AI におけるオープン化は、AI の弱点や課題に対処するためのより良い道筋を提供するということです。テック企業はシステムを非常に迅速に導入し、発

見されたバイアスやその他の問題に対処すると主張しているとの指摘もありました。オープンソースのリーダーたちは、AI コミュニティはより高い基準の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、AI システムを多様なデータセットでトレーニングすること、そして倫理、安全性、アルゴリズムの透明性を、後付けではなく最初から AI モデルに組み込むことです。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手法も含まれます。ある参加者は次のように述べています。「AI 開発者が大規模な言語モデルの出力を説明できないという考え方は、もはや受け入れられません。出力を透明化し、説明可能にするために、技術的な限界に挑戦する必要があります」。

基礎となる技術が成熟するにつれ、AI は学習、推論、問題解決、知覚、意思決定など、今日では人間の知性を必要とするさまざまなタスクを実行するようになるでしょう。医療、交通、行政、金融、教育、エンターテインメントなどの領域における画期的なアプリケーションは、大きな社会的・経済的利益をもたらすと同時に、大きなリスクももたらすでしょう。企業が新世代の AI 技術の導入と収益化を競い合う中、AI 開発に携わるすべての利害関係者が、透明性、説明責任、公平性、AI 技術の責任ある利用を促進し、AI システムが人間の価値観と社会の幸福に合致することを保証する、AI 開発の倫理的ガイドラインや原則にコミットすることが賢明でしょう。とりわけ、オープンソースアプローチへのコミットメントは、AI が人間の価値観に合致し、人権を保護し、社会全体の幸福を促進する方法で展開されることを保証するでしょう。

医療、交通、行政、金融、教育、エンターテインメントなどの領域における画期的なアプリケーションは、大きな社会的・経済的利益をもたらすと同時に、大きなリスクももたらすでしょう。企業が新世代の AI 技術の導入と収益化を競い合う中、AI 開発に携わるすべての利害関係者が、透明性、説明責任、意思決定を促進する AI 開発の倫理的ガイドラインまたは原則にコミットすることが賢明です。

オープンソース コラボレーションの必要性

午前中にジュネーブで行われたオープンソースのリーダーたちによるディスカッションでは、オープンソースのエコシステムが直面するいくつかの重要な課題について掘り下げられました。ある参加者は、これらの課題を、オープンソース コラボレーションに対する 4 つの本質的な脅威として多彩に表現しました：サイバー セキュリティと重要インフラの回復力。オープンソースモデルを脅かす新たな規制の取り組み。テクノナショナリズムの高まりとオープンソース プロジェクトへの多様な参加の促進。そして、オープンソースのライセンス、セキュリティ、知的財産に対する AI の影響、です。

これらの各領域を横断する包括的なテーマは、OSS ファウンデーションとグローバルなオープンソース エコシステムにおける他の主要な利害関係者間のコラボレーションを強化する必要性でした。午後は、オープンソース コミュニティが直面する緊急の課題に対処するために、主要な利害関係者をどのように引き合わせるかに焦点が当てられました。

オープンソース エコシステムに対する共通の優先事項の特定

協力の潜在的な仕組みに取り組む前に、会議の参加者は、より大きな協力が必要とされる核となる問題を再確認しました。

- **オープンソース インフラストラクチャの保護。**会議の参加者は、OSS ファウンデーションがサイバー セキュリティの懸念を管理するエコシステムのアプローチを洗練させるために協力することを望んでいます。主な優先事項には、重要な OSS インフラストラクチャの保守により多くのリソースを割くこと、サイバー セキュリティの専門家の人材層を厚くすること、自動テスト、パッチ適用、監査の機能を強化したセキュリティ バイ デフォルトモデルに移行することなどがあります。ある参加者は、「この問題を解決しなければ、規制当局による監視がますます厳しくなるでしょう」と述べています。
- **オープンソース開発モデルを保護するための政策協力の強化。**規制当局による監視が強化される中、オープンソースのリーダーたちは、OSS ファウンデーションが政策への関与に積極的な姿勢を示し、政策審議プロセスのより早い段階から関与するよう求めました。会議の参加者は、OSS ファウンデーションに対し、経験豊富な政策戦略家を採用し、重要な問題に関してより緊密な連携を図るよう求めました。「私たちは、コラボレーションを通じて脅威に立ち向かう必要があります。」と述べました。「オープンソースの背後にあるより大きな軍隊は、私たちの価値観と要請を前進させるのに役立つでしょう。」
- **政策への関与の拡大。**オープンソースのリーダーたちは、OSS ファウンデーションが、多くの政策コラボレーションからほとんど取り残されている大規模な有権者をより包括的に取り込むことも望んでいます。参加者は、米国やヨーロッパの組織間では多くの政策コラボレーションが行われている一方で、中国、インド、ブラジルなどでは、コントリビューターの数は非常に多いが、政策決定にはほとんど関与していないことを指摘しました。参加者の一人は、「私たちは、国を超えて架け橋を築き、他の国々の声を会話に取り入れなければなりません」と述べています。
- **地域の分断を防ぐ。**会議の参加者は、デジタル主権を強化するための各国の取り組みに概ね共感的でした。各国が自国のデータとデジタルインフラをより大きく管理できるようにする上で、OSS が実質的な役割を果たすと考える人もいます。しかし、オープンソースのリーダーたちは、世界的な貿易摩擦や地政学的対立がオープンで包括的なコラボレーションに真の障害をもたらすことを懸念しており、OSS ファウンデーションが協力してオープンソース プロジェクトにおける地域的な分断やサイロ化を避けることを望んでいます。

- **オープンソース コミュニティの行動規範の調整によるインクルージョンの促進。**会議の参加者は、コミュニティ全体で行動規範の内容を統一することで、OSS プロジェクトに対する期待や規範を共有することができると提案しました。また、行動規範の問題の解決を支援するために、中立的な仲間からなるコミュニティを招集するなど、外部からの実施支援を求める声もありました。また、OSS ファウンデーションのための共通の行動規範テンプレートを支持する意見もありましたが、参加者の中には、地域や文化の違いに対応できる柔軟性が必要だと指摘する人もいました。[25]

- **AI の機会と課題の管理。**他の多くの取り組み分野と同様に、AI はソフトウェア開発に大きな変化をもたらしています。会議の参加者は、AI は開発者がオープンソース　コードを生成する方法のすべてを変えるため、OSS コミュニティは AI への集団的アプローチが必要であることに同意しました。コラボレーションの分野には、大規模な言語モデルをトレーニングするためのデータ コモンズの創設や、ライセンスや知的財産に対する AI の影響の調査などがあります。会議の参加者はまた、コミュニティがオープン AI をどのように定義するかについて、足並みをそろえたいと考えています。これは、ますます強力になる AI システムに関連する社会経済的リスクと課題を管理するためのより良い道筋を示すものであることに多くの人が同意しています。

オープンソース モデルに対する脅威に注意を集中することは当然であり、最終的には不可欠なことですが、会議の参加者は、オープンソース コミュニティが生み出してきた公共の利益ーインターネットの本質的な基盤から、あらゆるもののための強力なソフトウェア ソリューションである広大なクラウドまで、ビジネス運営から、人類の最も緊急な課題への取り組みまでーについて、もっと声を大にする必要性も認識しました。会議の参加者は、OSS ファウンデーションが結束して、世界中の開発者が数え切れないほどの時間を費やして築き上げてきたテクノロジー コモンズを保護し、強化するよう求めました。ある参加者は、「コミュニティとして、私たちが目指しているのは、単に費用対効果の高いソフトウェアではなく、ソフトウェアとコンピューティングをコントロールすることです。私たちは、その方向性と影響力においてグローバルである必要があるのです。」

効果的なコラボレーションのための仕組みとプロセスの構築

世界のオープンソース コミュニティが共有する優先事項を特定した後、会議の参加者は、コラボレーションを可能にするメカニズムに注目しました。選択肢を検討する中で、オープンソースのリーダーは、コラボレーションのための 2 つの潜在的なモデルを提起しました。

- **オープンソースのためのグローバル事務局。** 会議の参加者の何人かは、新しいグローバルな事務局、あるいはオープンソース コミュニティのための国連と表現されるものを主張しました。新しいグローバルな組織を支持する人は、ほとんどの業界では、多数が良いと考える事を、その会員を代表してロビー活動を行う国際的な団体があると指摘しました。一方、オープンソース コミュニティには、地域、セクター、プロジェクトなど、多様で大規模なファウンデーションが存在し、それぞれのニーズに対応しています。しかし、エコシステムには、コミュニティが共有する利益を促進するための包括的な構造や組織が欠けています。ある参加者は、今日のファウンデーション間のコラボレーションに対する場当たり的なアプローチは、OSS コミュニティが規制や政策に対するアプローチにおいて専門的でなく、組織化されていないように見えると示唆しました。

  会議の参加者は、コミュニティを代表して既存の組織をグローバルな管理者の役割に割り当てることが可能かどうか議論しました。何人かが指摘したように、確立された OSS ファウンデーションは、そのメンバー組織によって特定された優先事項を実現するための明確な責務とリソースを持っています。そのため、エコシステム全体のために、より大きなグローバルな調整やアドボカシーの役割を果たすための設備や資金は必ずしも整っていません。しかし、何人かの参加者は、Open Source Initiative が、Open Policy Alliance を通じて、OSS に関連する公共政策の決定、コンテンツ、研究、および教育について知らせるために、すでにパートナーの連携を行っていることを指摘しました。[26] ある参加者は「真にグローバルで代表的なものが必要です。リソース、政策に関する深い専門知識、中立的な立場、そしてエコシステム全体への奉仕を使命とする事務局があれば良いと考えています。」と説明しました。

新たなグローバル事務局の設置に賛成する意見からは、既存の OSS ファウンデーションがエコシステム全体の課題に取り組むための受け止められる容量が限られていることへの懸念が示されました。エコシステム全体のコラボレーションを深める必要性については、善意の表明に事欠かない一方で、ファウンデーション間の協力が、既存の職務を遂行するための日々の忙しさによって疎かになることを懸念する声もありました。一般的に、OSS ファウンデーション間の協力のための資金は限られています。ある参加者が主張したように、「誰かの仕事でなければ、それは実現しない」のです。

- **コラボレーションのための軽量でピア ツー ピアのネットワーク。** 議論の反対側には、OSS ファウンデーションのエグゼクティブ ディレクターのネットワーク一場合によっては、ポリシー リードのピア グループーで、エコシステムの重要なニーズの多くを達成するのに十分であると主張する人々がいました。エコシステム コラボレーションへのライトウェイト アプローチに賛成する会議の参加者は、人とインフラに多大な投資を必要とする新しいグローバル組織の設立の利点に懐疑的でした。彼らは、エコシステムにはすでにいくつかのメタ組織があると指摘。さらに彼らは、既存の OSS ファウンデーションのリーダーたちが定期的に集まり、共通の優先事項を特定し、協力的な取り組みを管理する責任を分担する能力を信頼していました。

ジュネーブでの話し合いが終了した時点で、エコシステム全体の協力体制を構築するための最善の道を定めるためには、さらなる話し合いが必要であることは明らかでした。どのようなメカニズムにせよ、ジュネーブで始まった話し合いを継続することに、幅広い支持が集まりました。短期的には、会議の参加者は、勢いを持続させることが重要だと述べました。何人かは、コラボレーションのためのシンプルなツールを備えた一連のファウンデーション間ワーキング グループが、サイバー セキュリティ、規制、オープン AI などの問題で進展をもたらす可能性があると提案しました。

年次 Open Source Congress の開催にも強い支持があり、OSS ファウンデーションのリーダーやその他の関係者を定期的に招集することに大きな価値を見出すという点で、会議の参加者の意見が一致しました。ある参加者は、「今日、私たちは組織として分断されていますが、私たちが団結することで、より強力になることができます。

今後は、オープンソース ガバナンスにおけるインクルージョンの拡大が最も重要であるというコンセンサスが得られました。ヨーロッパと北米以外からの参加者は、今日のオープンソースの集まりの多くが西洋中心であることを確認しました。彼らは、リアルタイムの地域化を含む包括的なプロセスを望んでいます。また、毎年開催される Open Source Congress を、伝統的に参加者の少ない世界各地域で持ち回りで開催することについても、幅広い支持を得ました。

会議の参加者はまた、既存の OSS ファウンデーションのコミュニティが、新興のファウンデーションにより多くのサポートを提供することを望んでいます。例えば、アジア、アフリカ、ラテンアメリカでは、広範な開発者コミュニティと多くのアドホックなユーザーグループがありますが、正式なファウンデーションはほとんどありません。ガバナンスや政策への参画を促進するためには、これらの構成員を代表する、より地域に特化したファウンデーションが必要かもしれません。新しいファウンデーションのためのオンボーディング プロセスは、成熟したファウンデーションから新興の OSS 組織への知識の移転に役立つのではないかという意見が何人かの参加者から出されました。ピア ネットワークや ファウンデーションの一覧表があれば、新しいファウンデーション リーダーもエコシステムとのつながりを感じやすくなるでしょう。

最後に

最終的に、会議の参加者は、ジュネーブに集まるために費やされた時間とリソースが十分に投資されたことに同意しました。世界中から集まったオープンソースのリーダーたちは、親密な雰囲気の中で会う機会を得て、その多くは初めてお互いを知ることになりました。各分野の専門家たちは、パネル ディスカッションで重要な問題を洗い出しました。共通の優先事項が特定され、議論されました。エコシステム全体の協力を深めるための選択肢が提案され、議論されました。そして何よりも、参加者は今後も対話を続け、協力を深めていく決意を固めました。

究極のプリンの証明は、もちろん食べることにあります。現在、オープンソース コミュニティの重要な活動において協力し継続するという急を要する課題に対し団結するかどうかは、エコシステムのリーダーにかかっています。高まるテクノナショナリズム、新たな規制、そして新たなサイバーセキュリティの脅威が課題となるでしょう。より団結し、協力的なオープンソース コミュニティは、それらを解決する上でより成功するでしょう。ジュネーブに集結したOSSファウンデーションのリーダーたちは、その先頭に立つことを約束し、さらに多くの人々が参加することでしょう。ある参加者が見事にこう言いました。「私たちがここで行っているコラボレーションは、何十億ドルものソフトウェアを生産し、その過程で世界を変えている何十万人もの開発者を支援することです。」

謝辞

筆者は、ジュネーブに集い、その洞察と解説によって本レポートにインスピレーションを与えてくれた 53 名のオープンソース コミュニティのリーダーの貢献に感謝します。また、Futurewei の Chris Xie 氏のリーダーシップと貢献により、Open Source Congress が実現したこと、そして、刺激的なイベントを主催し、このレポートを発行してくれた Linux Foundation チームに感謝します。Jerry Michalski 氏には、会議のための知識面の土台作りと、ジュネーブでのコミュニティの会話を盛り上げるためのチームワークに感謝します。また、Omkhar Arasaratnam 氏、Stella Biderman 氏、Mirko Boehm 氏、Jory Burson 氏、Thierry Carrez 氏、Stefano Maffulli 氏、Mike Milinkovich 氏、Deb Nicholson 氏、Rebecca Rumbul 氏など、初期の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くださった方々にも感謝の意を表したいと思います。

著者について

Anthony は DEEP Centre の創設者兼代表であり、ビジネスと社会におけるデジタル革命、イノベーション、創造性の分野で国際的権威。世界的ベストセラー『Wikinomics』とその続編『Macrowikinomics: New Solutions for a Connected Planet』の共著者（Don Tapscott との共著）。

その他の役割として、Anthony は **Blockchain Research Institute** のリサーチ ディレクターであり、**Markle Foundation** の Initiative for America’s Economic Future のエキスパート アドバイザー、ブリュッセルの **Lisbon Council** のシニア フェローを務めています。Anthony は最近、National Research Council の Committee on **Science for the EPA’s Future** の委員、トロント大学 **Munk School of Global Affairs** の客員研究員、ブラジルの Free Education Project のチーフ アドバイザーを務めました。テクノロジーとイノベーションに関する彼の研究は、Harvard BusinessReview、Huffington Post、Globe and Mail などの出版物で紹介されています。

このレポートは、以下の文書の参考訳です。
Standing Together on Shared Challanges
翻訳協力：松本央

参考資料

1 https://academic.oup.com/book/44727/chapter/378967711

2 https://linuxfoundation.eu/newsroom/the-rising-threat-of-software-supply-chain-attacks-managing-dependencies-of-open-source-projects

3 https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap

4 https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on#:~:text=Introduction,and%20non%2Dtech%20companies%20alike.

5 https://newsroom.eclipse.org/news/announcements/open-letter-european-commission-cyber-resilience-act

6 https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

7 https://thediplomat.com/2020/09/us-china-techno-nationalism-and-the-decoupling-of-innovation/

8 https://www.channelnewsasia.com/business/risc-v-group-says-restrictions-open-technology-would-slow-innovation-3833631

9 https://www.computer.org/publications/tech-news/community-voices/on-the-weaponization-of-open-source

10 https://merics.org/en/short-analysis/china-bets-open-source-technologies-boost-domestic-innovation

11 https://opensource.com/resources/what-open-source

12 https://opensource.com/article/22/10/defining-open-source-ai

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

14 https://philarchive.org/archive/YAMUAI

15 https://www.linkedin.com/pulse/interpretability-vs-performance-trade-off-balancing-model-shirsat

16 https://opensource.com/article/22/10/defining-open-source-ai

17 https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/

18 https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/

19 https://www.lexology.com/library/detail.aspx?g=4d3d8be3-abeb-430b-a7ab-bae434d3e014

20 https://aiindex.stanford.edu/report/

21 https://www.cam.ac.uk/Malicious-AI-Report

22 https://www.theguardian.com/technology/2023/mar/29/elon-musk-joins-call-for-pause-in-creation-of-giant-ai-digital-minds

23 https://www.bloomberg.com/opinion/articles/2023-04-05/an-ai-pause-would-be-a-disaster-for-innovation

24 https://www.brookings.edu/blog/techtank/2023/04/11/the-problems-with-a-moratorium-on-training-large-ai-systems/

25 Potential models for a shared code of conduct template include:
OpenSSF: https://openssf.org/community/code-of-conduct/
CC: https://opensource.creativecommons.org/community/code-of-conduct/
Meta: https://opensource.fb.com/code-of-conduct/
Amazon: https://aws.github.io/code-of-conduct

26 https://opensource.org/programs/open-policy-alliance/

THE LINUX FOUNDATION | Research

2021 年に設立された **Linux Foundation 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、新たな技術トレンド、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洞察を提供しています。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・定性的手法の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洞察を得るための最適なライブラリを構築しています。

この著作物を参照するには、以下のように引用してください。
Anthony Williams,“ Standing Together on Shared Challenges: Report on the 2023 Open Source Congress,” foreword by Yue Chen and Chris Xie, The Linux Foundation, December 2023.