OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2025 アニュアル レポート

openssf.org

目次

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

はじめに: オープンソースの未来を共に守ろう

Open Source Security Foundation (OpenSSF) アニュアルレポートへようこそ。より安全で回復力のあるオープンソースコミュニティを引き続き形成し続ける、進歩、創造性、そしてコラボレーションを、今年もみなさんと一緒にたたえたいと思います。

OpenSSFは、オープンソースソフトウェアの開発、保守、そして利用を持続的に安全に行えるようにするために存在します。私たちのコミュニティは、オープン性、包括性、そして透明性という共通の価値観に基づいています。これらの原則は、セキュリティは孤立して達成されるものではなく、共に学び、知識を共有し、分野、地域、経験の境界を越えて信頼を築くという、集団的な努力によって達成されることを私たちに思い出させます。単一のプルリクエストからグローバルな取り組みまで、あらゆる貢献が、私たちのコミュニティの成長を支える基盤を強化します。

2025年も、私たちの取り組みは引き続き戦略目標に沿ったものとなりました。それは、セキュア バイ デザイン開発を通じて変化の触媒となること、セキュリティ意識とスキルを養うリソースで現代の開発者を教育し、力を与えること、そして標準、ポリシーへの関与、オープンソースセキュリティの未来を形作るパートナーシップを通じてコミュニティ全体にリーダーシップを発揮することです。

これらの目標は、私たちの基本的な四本柱に反映されています。

- **教育:** 世界中のセキュアな開発の基準を高める、実践的でアクセスしやすい学習機会を拡大します。
- **コミュニティとイベント:** 貢献者同士を結びつけ、刺激を与える集会、ワークショップ、グローバルな会話を通じてコラボレーションを促進します。
- **ポリシーと公共部門の関与:** 政府や業界のリーダーと建設的に協力し、デジタルの信頼とソフトウェアのセキュリティに対するバランスのとれた証拠に基づくアプローチを推 進します。
- **プログラムとプロジェクト:** 安全なオープンソースソフトウェアのための実用的なツール、フレームワーク、ガイダンスを作成する技術的取り組みを通じてイノベーションを推進します。

このレポートでは、OpenSSFの影響と2025年を通じて達成された全体的な進捗状況の包括的な概要を示します。このアニュアルレポートは、オープンソースセキュリティにおける進化する課題への対応を軸に、マイルストーン、コミュニティの取り組み、そして技術的成果に焦点を当てています。読者の皆様に、リーダーシップとワーキンググループからの洞察、教育および政策イニシアチブの最新情報、そして主要な業界イベントやコラボレーションを通じたOpenSSFのグローバルなプレゼンスの拡大についてご紹介します。今年のアニュアルレポートをお読みいただき、皆様が共に歩んできた進歩に満ちた一年をお祝いできることを心待ちにしています。この一年は、私たちがどれほどの道のりを歩んできたかを示すものであり、オープンソースの未来を共に築くための、これからの共通の旅路を改めて思い起こさせるものとなるでしょう。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

数字で見る 2025年

オープンソースセキュリティを
推進する**112の組織**から
262人以上のアクティブな貢献者

10のワーキンググループと
32の技術的な取り組み
(プロジェクト、関連プロジェクト、SIGを含む)

ソウルからブリュッセル、
アトランタに至る世界中で
11のコミュニティイベントを開催

ORBIT ワーキンググループ

- **20,000以上のOSS repoをスキャン**
- **セキュリティ知見が前年比200%向上**

毎月500,000プロジェクト
に対して
重要度スコアを算出

Alpha-Omega

- 14の重要なオープンソースプロジェクトに対する**580万ドル**の投資
- **60件以上**の監査と参画を完了

OpenSSF の無料トレーニング
プログラム全体で
約20,000 件のコース登録、
5,700人以上の学習者が
Understanding the EU Cyber
Resilience Act (LFEL1001) に登録

16の業界（金融、クラウド、AI、
政府、学術機関など）、
40ヶ国以上にまたがる
117組織のメンバー

OpenSSFのコミュニティは
年間で**20件の**
外部イベントに
60本以上
スピーカー参加

上位5つのメディアハイライトだけで
月間685万以上のアクセス
（ZDNET、The New Stack、
Infosecurity Magazine、
diginomica、Help Net Security）

OpenSSF Technical Advisory Council
(TAC)はオープン ソース ソフトウェア
エコシステムのセキュリティと
回復力を強化するため
14の技術イニシアチブに
$663,248を提供

メンバー企業は
総額$50億を調達、
OpenSSF エコシステムの
規模と影響力を拡大

重要なプロジェクトの保全

- **60以上の重要なOSSプロジェクト**へ
  セキュリティ強化資金を直接提供
- **6つの新しい脅威モデル、52の脆弱性の修正、**
  5つのファジングフレームワークを実装

悪意あるパッケージ

- エコシステム全体にわたる悪意のある
  パッケージに関するデータの保存
  - **66,000 NPM**
  - **10,000 PyPi**
  - **1,000 RubyGems**
  - **1,000 NuGet**

General Managerより

OpenSSF コミュニティを定義するものが 1 つあるとすれば、それは回復力です。

今年は、私たちの強さは特定のプロジェクトや企業から生まれるものではないということを改めて認識させられました。それは、オープンソースをより安全で強固なものにするために日々尽力しているメンテナー、開発者、研究者、そしてアドボケートの方々、皆さん全員から生まれているのです。

変化を通して共に築く

多くのファウンデーションと同様に、私たちも今年、変化する環境を乗り越えてきました。エコシステムは優先順位の変化に直面しましたが、私たちのコミュニティは活動を遅らせるのではなく、この課題に立ち向かいました。

ワーキンググループはリソースを共有し、プロジェクトは共通の目標に沿って連携し、世界中の貢献者が勢いを維持しています。この協働の取組みが、OpenSSF を特別なものにしています。

みなで勝ち得た今年のハイライト

2025年は、教育、ツール、知識の共有が業界を前進させられるという信念に基づき、意義ある進展の年となりました。

力を与える教育： 開発者、マネージャー、そして政策立案者を対象とするコースを開設•拡充しました。ソフトウェア開発マネージャーのためのセキュリティ（LFD125）、EU サイバーレジリエンス法の理解（LFEL1001）、そして新設のセキュアAI/ML駆動型ソフトウェア開発（LFEL1012）は、チームがソフトウェア開発のあらゆるレイヤーにセキュリティを組み込むための支援を提供します。

情報提供のためのガイドとホワイトペーパー： OpenSSF は、依存関係の管理や AI セキュリティなどの複雑なトピックをよりわかりやすくする 2 つの新しいガイドと 2 つの新しいホワイトペーパーをリリースしました。

拡張可能なインフラストラクチャとツール: プロジェクト全体にわたって、貢献者は、依存関係データパイプラインの強化から開発者が日常的に使用するツールの進化まで、オープン ソース セキュリティ インフラストラクチャの改善を実現しました。

世界的なプレゼンスと政策への影響: OpenSSFは、特に EU サイバーレジリエンス法と世界的な AIxCC イニシアチブに関する取り組みを通じて、サイバーセキュリティに関して政府および公共部門との連携を継続しました。

OpenSSF の声は、北米だけでなく、ヨーロッパ、インド、日本、韓国の主要なイベントでも反響を呼び、地元のオープンソース コミュニティを集めてソリューションを共有し、連携を強化しました。

今後の展望

2026 年を迎えても、私たちの焦点は明確です。

私たちは、安全で持続可能なオープンソース エコシステムの基盤を構築し続けます。

私たちは教育、安全な開発を簡素化するツール、そしてこの仕事をスケールさせる世界的な関係性に対して投資を継続します。

最も重要なのは、私たちは人材への投資を継続していくということです。このコミュニティは単なるプロジェクトのネットワークではなく、信頼、寛大さ、そして共通の目的に基づくネットワークです。

あらゆる貢献、あらゆるレビュー、あらゆるフィードバックが、オープンソースをすべての人にとってより強力なものにします。

ご参加いただき、コラボレーションを信じていただき、一緒にオープンソース セキュリティを永続的な世界的利益にできることを証明していただき、ありがとうございます。

Best regards,
Steve Fernandez
General Manager
Open Source Security Foundation

OpenSSF について

Open Source Security Foundation (OpenSSF)について

Open Source Security Foundation (OpenSSF) は、世界中のソフトウェア開発者、セキュリティ エンジニア、組織が結集し、公共の利益のためにオープン ソースソフトウェアをセキュアに保つための Linux Foundation 傘下の業界横断的な取り組みです。

2020 年に設立されたOpenSSFは、オープンソースソフトウェアの信頼性、回復力、セキュリティを高めるためのコラボレーション、ベストプラクティス、ツールに重点を置いています。

参加や貢献する方法にについて詳しく知りたい方は、openssf.org をご覧ください。

参加するには

- **ワーキンググループに参加：**継続的なセキュリティ向上に貢献することができます。こちらから参加してください。
- **メンバーシップについて：**OpenSSFのメンバーになり、オープンソースセキュリティの未来を形作りましょう。メンバーシップについてはこちらをご覧ください。
- **ソーシャルメディアをフォローしてください：**LinkedIn、X、Bluesky、Mastodon 、YouTubeで私たちをフォローして、最新情報を入手してください。
- **ニュースレターを購読する：**最新情報をメールで直接お届けします。こちらからご購読ください。
- **OpenSSFに他の人の参加を促す：**私たちの目標は野心的でありながら重要であり、広く共感を呼ぶものだと信じています。ぜひ私たちと一緒に変化を起こしましょう。

コミュニティヘルパー - 支援してくれる人たち

ガイダンスが必要な場合、質問がある場合、または参加したい場合は、次のコミュニティ リーダーや代表者が連絡先として最適です。OpenSSF Slack で問い合わせることもできます: http://slack.openssf.org/

コミュニティリーダー

ZACH STEINDLER
OpenSSF TAC Chair and Principal Engineer, GitHub

BOB CALLOWAY
OpenSSF TAC Vice Chair & Head of Google's Open Source Security Team

ワーキンググループとプロジェクトチーム:

OpenSSFワーキンググループまたはプロジェクトチームのリーダーに直接質問することもできます。彼らは技術的な成果物やコミュニティの取り組みに深く関わっており、新しい貢献者をいつでも喜んでサポートしてくれます。

ゼネラルメンバー代表

TRACY RAGAN
CEO and Co-Founder, DeployHub (General Member Rep)

IAN DUNBAR-HALL
Chief Engineer, Lockheed Martin (General Mem Rep)

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari (General Mem Rep)

アソシエイトメンバー代表

REBECCA RUMBUL
Executive Director & CEO, Rust Foundation (Associate Mem Rep)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2025年メンバーの概要

OpenSSFのメンバーコミュニティは2025年も拡大と多様化を続けており、これはオープンソースセキュリティが共通の責任であるという世界的な認識の高まりを反映しています。クラウドプロバイダー、半導体大手、金融機関、政府機関、そしてオープンソースに注力するスタートアップ企業など、幅広いメンバーが加盟するOpenSSFは、ソフトウェアサプライチェーンのセキュリティに取り組む最も包括的なエコシステムの一つとなっています。

過去1年間、OpenSSFは新しいメンバー サクセス プログラムを通じて関与を強化し、政府および政策関係者との連携を拡大し、メンバーがAIセキュリティ戦略の形成、CRAの準備、および世界的な脆弱性開示フレームワークを行うための機会を作りました。

OpenSSFはまた、組織の成長と規模に合わせてメンバー構造を見直し、メンバーの知名度、影響力、およびインパクトを高めながら、主要な取り組みに対する持続的なサポートを確保しました。

penSSFは、この進化を通じて、中立的かつ信頼できるコラボレーションの拠点としての役割を果たし、オープンソースソフトウェアのセキュリティを強化するという使命に引き続き取り組んでいきます。

2025 年、OpenSSFは成長を続けるコミュニティへの新メンバー加入について何件かのアナウンスができたことを誇りに思っています。

ゼネラルメンバー

balena
Buildkite
Canonical
THREAD AI
TRACE MACHINA
TRIAM SECURITY

アソシエイトメンバー

ERLANG ECOSYSTEM FOUNDATION

メンバー紹介

プレミアメンバー

aws, Apple, Capital One, DATADOG, DELL Technologies, ERICSSON, GitHub, Google, HUAWEI, intel, IBM, JPMorgan Chase & Co., Microsoft, Morgan Stanley, Red Hat, sonatype

ゼネラルメンバー

ADALOGICS, aiven, Akamai, Alibaba, ANACONDA, apiiro, arm, AURISTOR, balena, block, Bloomberg Engineering, BOEING, boost security.io, Buildkite, Canonical, Chainguard, chainloop, cisco, citi, cloudsmith, code intelligence, COMCAST, controlplane, cybertrust, cybozu, Defense Unicorns, DeployHub, DTCC, docker, embraceableAI, ensignia, FOSSA, FUJITSU, FUTUREWEI Technologies, RESEARCH, GitLab, Goldman Sachs, GUIDEWIRE, hackerone, Hedera, herodevs, HITACHI, HONDA The Power of Dreams, JFrog, KEYFACTOR, kusari, LEGIT SECURITY, LOCKHEED MARTIN, NUTANIX, Patchstack OÜ, REEVO Cloud & Cyber Security, RENESAS, REVERSING LABS, root, RTX, salesforce, SAP, Scotiabank, SHEBASH, shopify, snyk, Socket, SPARKFABRIK, Spotify, stacklok, StepSecurity, SUSE, sysdig, Technology Innovation Institute, TESTIFYSEC, THREAD AI, TRACE MACHINA, TRAIL OF BITS, CleanStart, WNDRVR, AMD XILINX, ZTE

アソシエイトメンバー

Carnegie Mellon University, CAICT 中国信通院, ECLIPSE FOUNDATION, FS-ISAC, ERLANG ECOSYSTEM FOUNDATION, ISCAS 中国科学院软件研究所, ISC2, LISH Laboratory for Innovation Science at Harvard, NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE, OSB Open Source Business ALLIANCE, ofe OpenForum Europe, OpenUK, PURDUE UNIVERSITY, python SOFTWARE FOUNDATION, RTEMS www.rtems.org, Ruby Central, Inc., Rust Foundation, SAFECode, MITRE, TODO, Trifecta Tech Foundation

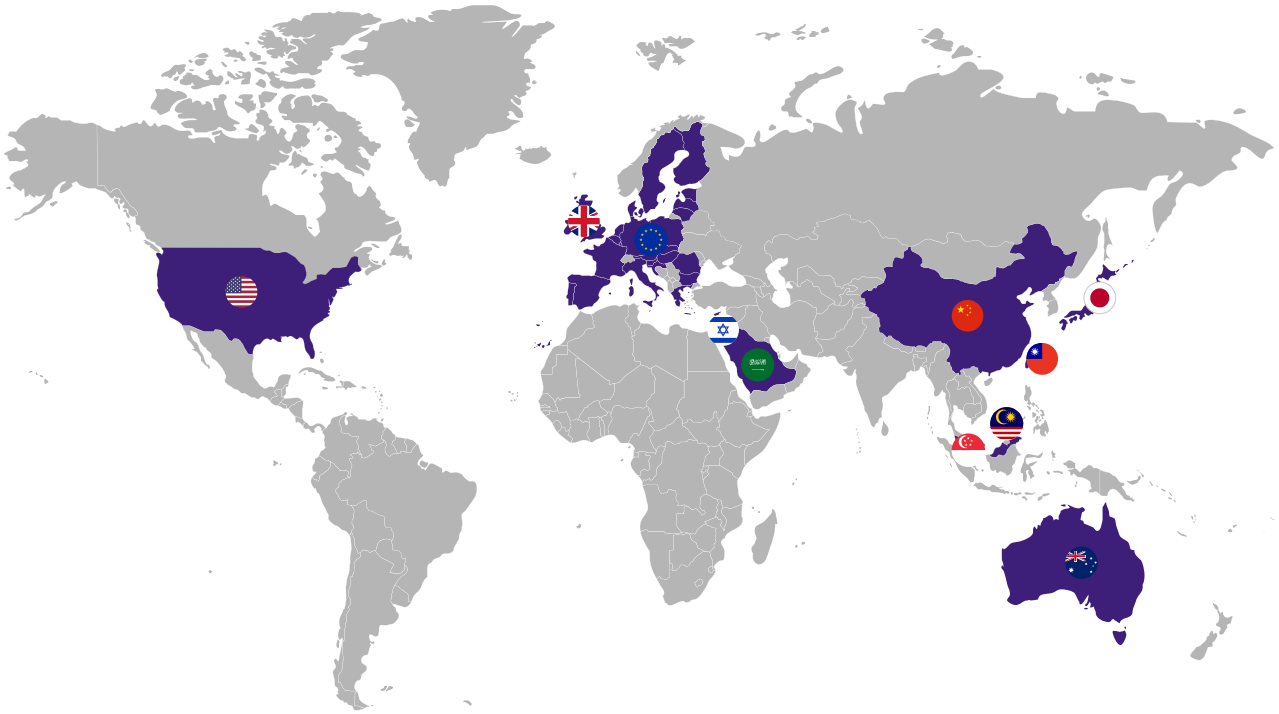
今すぐOpenSSFに参加しよう

OpenSSFはオープンソースセキュリティに関するグローバルな連携を推進し続けており、メンバーの役割はこれまで以上に重要になっています。クラウド、金融、政府、AI、製造業、オープンソース開発など、あらゆる分野の組織の皆様に、安全なソフトウェアの未来を形作るためにご参加いただくようお願いいたします。

メンバーシップにより、技術的方向性、ポリシーへの関与、世界的な支援活動に対して直接発言する権利が与えられ、同時にあなたのチームと、今日の最も緊急性の高いソフトウェア セキュリティの課題に対するソリューションを推進する一流の専門家とのつながりが生まれます。

OpenSSF コミュニティに参加し、デジタルの未来の基盤を守る共同の取り組みに参加しましょう。

メンバーの地理分布



メンバーの業界

Governing Boardメンバー

BRIAN FOX
CTO, Sonatype

EMILIO ESCOBAR
Chief Information Security Officer, Datadog

ERIC BREWER
VP of Infrastructure & Google Fellow, Google

GRAHAM HILL
Managing Director, Cybersecurity & Technology Controls at JPMorgan Chase & Co.

IAN DUNBAR-HALL
Chief Engineer, Lockheed Martin (General Mem Rep)

JAMIE THOMAS
Chief Client Innovation Officer and Enterprise Security Executive, IBM

JINGUO CUI
Executive Director of Open Source Security and Infrastructure, Huawei

JOHN ROESE
Global Chief Technology Officer Products and Operations, Dell Technologies

JUSTIN CAPPOS
Professor, New York University Tandon School of Engineering (SCIR)

KELLY ANN
Cloud Infrastructure Security Engineer, Apple

MARK RUSSINOVICH
OpenSSF Board Chair & Azure CTO and Technical Fellow, Microsoft

MARK RYLAND
Director, Office of the CISO AWS Security

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari (General Mem Rep)

MIKE LINKSVAYER
Vice President of Developer Policy, GitHub

PER BEMING
VP and Head of Standards & Industry Initiatives, Ericsson

REBECCA RUMBUL
Executive Director & CEO, Rust Foundation (Associate Mem Rep)

ROY CROWDER
Executive Director - Morgan Stanley

SCOTT SCHENKEIN
VP, Distinguished Engineer Cyber Security, Capital One

TRACY RAGAN
CEO and Co-Founder, DeployHub (General Member Rep)

VINCENT DANEN
Vice President of Product Security, Red Hat

Governing Board議長から

この一年間でオープンソースのセキュリティには大きな進展がみられ、グローバルなソフトウェア基盤の信頼性を強化するためのOpenSSFからの貢献には目を見張るものがありました。セキュア・バイ・デザインの概念は、様々な分野で具体的な基準としてますます導入が進んでいます。OpenSSFは今後も、開発者、企業、政府機関を結集し、この共通の目標を推進することに尽力していきます。

ソフトウェアセキュリティ基盤の強化

2024年はコミュニティが協調型セキュリティの有効性を証明した年でしたが、2025年はそれを拡大する年となりました。OpenSSFプロジェクトは、様々な業界において目に見える効果を発揮しています。例えば、SBOM管理ツールであるBomctlのLockheed Martinによる 実装、KaggleによるAIモデル署名のSigstoreへの追加、Defense UnicornsによるZarfとGUACの統合、Docker HubによるOpenSSFツールと標準の活用によるソースコードでのセキュリティ強化などです。これにより、組織は開発から本番環境に至るまでパイプラインを保護できるようになりました。ソフトウェア認証と検証可能なビルドでも進歩が遂げられており、コンフィデンシャル コンピューティングとハードウェアベースのセキュリティからの知見がオープンソース エコシステムの強化に活用されています。

変化する脅威の状況への対応

攻撃者はますます巧妙化しており、コードだけでなく、オープンソースを支える信頼のネットワークも標的にしています。2025年には、オープンソースコミュニティは大規模なサプライチェーン攻撃に見舞われました。攻撃者はメンテナーアカウントを乗っ取り、毎週数十億回ダウンロードされる人気パッケージに悪意のあるコードを注入しました。OpenSSFは、ベストプラクティスの更新、コミュニティガイダンス、そして公的機関やパッケージレジストリとのより強固なパートナーシップによってこれに対応しました。

AIセキュア開発の実現

AIは開発者のコード作成とリリース方法を変えました。同時に、新たなリスクも生み出しました。Secure AI/ML-Driven Software Developmentコース（LFEL1012）や、AI Cyber Challenge（AIxCC）を含むOpenSSFのAIセキュリティに関するより広範な取り組みは、セキュアな開発プラクティスの推進へのコミットメントを示す好例です。これらのリソースにより、開発者はAIツールの責任ある使い方を理解し、ソフトウェア開発ライフサイクル全体を通じてデータ、モデル、パイプラインを保護することができます。

今後、OpenSSF は、コンフィデンシャル コンピューティング、信頼可能な実行（TE）、プライバシー保護技術によってAIワークフローをさらに安全に保護する方法を継続的に模索していきます。

成長を続けるグローバルコミュニティ

私たちのコミュニティはかつてないほど強くなっています。今年は3大陸で5つのCommunity Daysを開催し、グローバルサイバーポリシーとOSPS Baselineに焦点を当てた新たなワーキンググループを立ち上げました。また、EU Cyber Resilience Act（CRA）や米国のSecure Software Development Framework（SSDF）などの進化する規制においてオープンソースの視点が反映されるよう、政府機関や国際標準化団体との連携を深めました。

これから楽しみなこと

オープンソースは現代のコンピューティングの基盤を形成し、そのセキュリティと持続可能性を確保する共同責任を伴います。私はこれまでのキャリアを通じて、クローズドソースソフトウェアとオープンソースソフトウェアの両方におけるサイバーセキュリティの推進に深く関わってきました。2019年のOpenSSFの共同設立、コンフィデンシャルコンピューティングのビジョンへの貢献、そして2018年のConfidential Computing Consortiumの立上げ支援を通して、セキュアソフトウェア開発の進化する状況を直接的に理解することができました。これらの経験に加え、マイクロソフトのSecure Supply Chain Consumption Framework（S2C2F）をOpenSSFで利用できるようにしたり、マイクロソフトのSecure Future Initiativeを主導したりするなどの取り組みは、業界の取り組みをオープンソース標準と整合させ、幅広いセキュリティ課題に対処するという、私の一貫したコミットメントを反映しています。

Chairとして、私はOpenSSFの使命である、業界の変化し続けるニーズへの対応を支援することに注力しています。OpenSSFは今後も、大企業から個々のプロジェクトメンテナーまで、誰もがセキュリティを基盤として設計されたソフトウェアを開発•利用できるよう、標準とツールを確立し、推進していきます。管理、リポジトリ管理、メンテナーの実践、ビルドパイプラインのベンチマークを設定することで、ソフトウェアの整合性をあらゆる段階で検証できる、明確で透明性が高い基準の構築を目指しています。これらの標準が確立されることで、開発ツールはソフトウェアの自動検証を支援し、手作業の負担を軽減し、エコシステムへの信頼を高めることができます。

さらに、OpenSSFは、コミュニティが重大なオープンソースの脆弱性に迅速かつ協調的に対応できるよう、ツールとシステムの構築に取り組んでいます。このアプローチは、レジリエンス（回復力）を強化するだけでなく、オープンソースエコシステム全体の信頼を育みます。パッケージマネージャーのための持続可能なインフラストラクチャを支援し、CRAなどの変化する規制に対応するために政府や標準化団体と緊密に連携することで、OpenSSFはオープンソースが革新的で安全であり、誰もがアクセス可能な状態を維持できるよう支援しています。

私にとって最も刺激的なのは、このコミュニティの献身と創意工夫です。私たちが共に成し遂げてきた進歩は、コラボレーションの力の証です。OpenSSFのミッションの実現に尽力してくださるすべての貢献者、メンバー、そしてパートナーの皆様に感謝申し上げます。

Mark Russinovich
OpenSSF Board Chair & Azure CTO and Technical Fellow,
Microsoft

TAC Chairより

OpenSSF コミュニティの皆さん、こんにちは!

2025年は浮き沈みの多い年でした。

公共部門では、オープンソースソフトウェアの多くのメンテナーや消費者が、欧州連合サイバーレジリエンス法（EU CRA）について疑問を抱いています。そのため、2025年に私たちは **ハイレベルのガイダンス** をまとめました。**EU CRAを理解するための無料コース**もあります。

また、**crates.io**、**npm**、**NuGet** のリリースなど、さまざまなセキュリティ機能に関して複数のパッケージリポジトリと協力しました。Trusted publishing は、**攻撃者の標的となっている** ビルドパイプラインからパスワードや長期間有効な API キーを取得するのに役立ちます。パッケージ リポジトリはオープンソースの中心であり、需要が増加しており、運用モデルの変更が必要になる可能性があります。これについては、**「Open Infrastructure is Not Free」**で概説しています。

今年は **SLSA v1.1** がリリースされました。ソフトウェア サプライチェーン セキュリティを理解する鍵として、アテステーションへの関心が高まっています。Sigstoreは、（長期間有効な鍵を管理することなく）アテステーションに署名するための非常に人気の高い方法であり、**Sigstoreのパブリック インスタンス透明性ログ** は、月間ユニーク ID 数が1 月の500 万～600 万から 9 月は 1,400 万～1,500 万へと爆発的に増加しました。

また、AI/ML セキュリティ ワーキンググループの **モデル署名仕様** に基づき、**NVIDIAのNGCカタログを含むAIモデルの署名に** Sigstoreが採用されていることも確認しました。LLM をはじめとする AI の進歩が、防御側が攻撃者に遅れずについていくためにどのように役立つかを示すサイバー推論システムを構築する **AIサイバーチャレンジの終了**など、AIにとって忙しい一年でした。

最後になりましたが、TAC は (スタッフと協力して) **OpenSSF 技術イニシアチブの資金調達プロセスを刷新** しました。2024 年には 5 件の提案に 10 万ドルの資金を提供し、2025 年には資金提供額を 14 件の提案に 663,248 ドルへと拡大しました。これらの提案は、セキュリティ監査、メンターシップ プログラム、テクニカル ライター、設計支援、開発作業にまで及び、OpenSSF の技術イニシアチブが時間の経過とともに成熟し、より広範なコミュニティに採用されるにつれてニーズが進化していることを示しています。

これから私たちはどこへ向かうのでしょうか？オープンソースのセキュリティ確保に関する問題はすべて解決したからといって、心配する必要はありません。2026年には多くのことが待ち受けており、やるべきことがまだたくさんあることは承知していますが、2025年の成果を忘れないようにしましょう。

2025年から得た教訓は、何よりもコミュニティの重要性です。オープンソースのセキュリティ確保という共通の目標に向かって、私たちが共に努力していなければ、世界中のセキュリティ機能はすべて無意味です。OpenSSFでは、カンファレンス、ビデオ通話、オンラインチャットなど、あらゆる場面で素晴らしいエネルギーが溢れています。2026年がどんな年になるのか、今から待ち遠しいです。

オンラインでお会いしましょう。

Zach Steindler
OpenSSF 2025 TAC Chair

Technical Advisory Council メンバー

Technical Advisory Council（TAC）は、OpenSSFの技術コミュニティ全体の技術ビジョンを策定し、監督を行います。その活動は以下のとおりです。

- 技術イニシアチブの承認、確立、構造化、組織化、およびアーカイブ化。
- 単一のプロジェクトの範囲外にあるコミュニティの規範、ワークフロー、またはポリシーの確立。
- 複数のプロジェクトに影響する技術的な問題の解決。
- プロジェクト横断の機会の調整。

ZACH STEINDLER
OpenSSF TAC Chair and Principal Engineer, GitHub

BOB CALLAWAY
OpenSSF TAC Vice Chair & Head of Google's Open Source Security Team

ARNAUD LE HORS
Senior Technical Staff Member - Open Technologies, IBM

GEORG KUNZ
Open Source Manager - Open Source Program Office - CTO Office, Ericsson

JAUTAU "JAY" WHITE
Open Source Software and Supply Chain Security Strategy, Microsoft

MARCELA MELARA
Research Scientist, Intel Labs

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari

MICHAEL SCOVETTA
Principal Security PM Manager, Microsoft

STEPHEN AUGUSTUS
Technical Architect — Office of the CTO, Bloomberg

OpenSSFスタッフ

STEVE FERNANDEZ
General Manager

ADRIANNE MARCUM
Chief of Staff

CHRISTOPHER ROBINSON (CROB)
Chief Technology Officer/Chief Security Architect

DAVID A. WHEELER
Director, Open Source Supply Chain Security

JEFF DIECKS
Technical Project Manager

KRIS BORCHERS
Technical Project Manager

STACEY POTTER
Manager of Community

MADALIN NEAG
EU Policy Advisor

OpenSSFサポート スタッフ

ANGELAH LIU
Associate Manager, Communications & Marketing

JOHN NIRO
Membership Solutions

KATE POWELL
Program Manager

NAOMI WASHINGTON
Program Manager

RAM IYENGAR
Community Engagement Lead, India

REDEN MARTINEZ
Project Coordinator

SALLY COOPER
Senior Manager, Communications & Marketing

SUSAN REMMERT
Project Marketer

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2025年の成果とハイライト

ファウンデーション全体の成果

2025年、OpenSSFは5周年を迎え、オープンソース セキュリティの向上において大きな前進を遂げました。主な成果としては、Cybersecurity Skills Framework や Open Source Project Security (OSPS) Baseline の立ち上げなどが挙げられます。新たなワーキンググループ（ORBIT、Global Cyber Policy）を結成し、OpenSSF Community DaysやOpen Source SecurityConといったグローバルイベントを主催しました。コミュニティは8人の新メンバーと1つのアップグレードによって成長し、OpenSSF Scorecardプロジェクトはセキュリティ監査を受けました。

教育面では、「Security for Software Development Managers (LFD125)」「Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)」「Secure AI/ML-Driven Software Development (LFEL1012)」といった新しいコースが追加され、gittuf や RSTUF などのプロジェクト向けのメンターシップ プログラムも拡充されました。

コミュニティの活動も活発化し、ウェブサイトのトラフィックは20%増加、LinkedInコミュニティは44%成長、YouTube登録者数は45%増加しました。OpenSSFはソーシャルメディアへの展開を拡大し、Blueskyにも参加するようになりました。また、オープンインフラへの持続的な投資を求める公開書簡を主導しました。

技術的には、OpenSSFは14件の技術イニシアチブに66万3000ドル以上の助成金を提供しました。モデル署名（OMS）の仕様や、AIコードアシスタント指示、SBOMデータ、セキュアMLOpsの可視化に関するホワイトペーパーなど、新たな研究と仕様が公開されました。これらの共同の取り組みは、成熟しつつあるコミュニティがオープンソース セキュリティに世界的な影響を与えていることを示しています。

教育

ソフトウェア セキュリティ教育

教育は、オープンソース ソフトウェア (OSS) のセキュリティを向上させるための実践的な戦略の重要な要素です。ソフトウェア開発者の実践的なセキュリティ知識を高めるための大規模かつスケーラブルな取り組みなしに、デジタル コモンズを守ることはできません。OpenSSFの教育イニシアチブは、この重要なニーズを満たすために設計されています。私たちの焦点はOSSですが、クローズド ソースのソフトウェア システムも大部分がOSSコンポーネントで構成されており、同じ種類の攻撃の対象となり、多くの場合は同じ人々によって開発されています。したがって、当社の教育資料のほとんどは、クローズド ソース ソフトウェアにも同様に適用されます。

2025年初頭、OpenSSFとLinux Foundationは、Cybersecurity Skills Framework を導入しました。組織や個人が、幅広い技術職やリーダーシップ職に不可欠なセキュリティ能力を評価し、強化するのを支援するためのフレームワークです。このフレームワークは、14の主要なIT職種を3つの熟練度レベルにマッピングし、DoD 8140、CISA NICE、ICT e-CFなどの国際標準に準拠しています。このフレームワークは現在、OpenSSFの教育プログラムを、世界的に認められたサイバーセキュリティ スキルと整合させるための基盤となり、将来のコース開発やアップデートのための構造としても機能しています。このフレームワークのリリース後に、ライブ ウェビナー が開催されました。何百人もの参加者に向けてフレームワークが紹介され、これが人材育成、コンプライアンス対応、オープンソース セキュリティの成熟度評価をどのようにサポートするかが説明されました。

今年は 3 つの新しいコースを作成してリリースしました。

- Security for Software Development Managers (LFD125)。このコースは、AI アシスタントを安全に使用してより安全なコードを作成し、より的確なレビューを提供することで専門的な価値を高めたいと考えているソフトウェア開発者とレビュー担当者を対象としています。
- Understanding the EU Cyber Resilience Act (CRA) (LFEL1001) 。このコースでは、開発者 (製造者および管理者を含む) が規制環境における重要な変化を理解し、コンプライアンスに対応して必要な制御を実装できるようにします。CRAは世界的な影響を及ぼしており、ソフトウェア開発に関わるすべての人がCRAを理解することが重要です。
- Secure AI/ML-Driven Software Development (LFEL1012) 。このコースは、AI アシスタントを安全に使用してより安全なコードを作成し、より的確なレビューを提供することで専門的な価値を高めたいと考えているソフトウェア開発者とレビュー担当者を対象としています。

これらは既存のコースに加えて提供されるものです。最も人気のあるコースは「Developing Secure Software」で、edX (LFD104xおよびLFD104-JPx) とLinux Foundationウェブサイト (LFD121およびLFD121-JP) の両方で、英語と日本語で受講可能です。今年度のみで見ると、受講登録者数上位のコース (2025年10月22日時点) は以下のとおりです。

- Developing Secure Software (英語と日本語、LFおよびedX)

- Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)

- Security for Software Development Managers (LFD125)

- Securing Projects with OpenSSF Scorecard (LFEL1006)

- Securing Your Software Supply Chain with Sigstore (LFS182)

***コースの詳細については、教育とトレーニングのセクションを参照してください。**

AIコースLFEL1012は2025年10月16日にリリースされ、2025年10月31日までにすでに335人の登録者を獲得していました。AI はソフトウェア開発を変革しつつありますが、ソフトウェア開発においてAI を安全に使用する方法に関する資料は比較的少ないため、この新しいコースには今後さらに登録者が増えると予想されます。

この膨大な登録者数は、私たちが何千人もの開発者の教育を向上し、さらにその先にいる何百万人ものソフトウェア ユーザーを支援していることを示しています。私たちは、サイバーセキュリティ スキル フレームワークへのサポートを強化するために、既存のコースを拡張することに加えて、少なくとも1つのコースを追加する予定です。

セキュリティガイドとホワイトペーパー

膨大な情報量に圧倒されてしまうのはよくあることです。そこで私たちは、成功へのシンプルな道筋を提供するための様々なガイドやホワイトペーパーを作成しました。ここでは、AI/ML、CRA/SBOM、一般的なセキュリティのベスト プラクティスの 3 つのカテゴリに分類された、重要なガイドとホワイト ペーパーを紹介します。

AI/ML

- 「Visualizing Secure MLOps (MLSecOps): A Practical Guide for Building Robust AI/ML Pipeline Security」：このホワイトペーパ ーでは、機械学習のライフサイクル全体にセキュリティを統合するためのレイヤー別のフレームワークを紹介しています。また、DevSecOps の実績ある戦略を AI/機械学習環境に適用し、SLSA、Sigstore、OpenSSF Scorecard といったオープンソースツールを活用する方法についても解説しています。

- 「Security-Focused Guide for AI Code Assistant Instructions」：このガイドは、AI アシスタントが生成するコードのセキュリティを高めるために、明確でセキュリティを重視したカスタムプロンプト（指示文）を作成する方法を解説しています。また、不十分または曖昧な入力によって生じうるリスクに対処する内容も含まれています。このガイドは Secure AI/ML-Driven Software Development（LFEL1012）コースの重要なサポートガイドであり、AI/ML ワーキング グループ と Best Practices ワーキング グループ によって共同開発されました。

CRA/SBOM

- 「Cyber Resilience Act (CRA) Brief Guide for OSS Developers」：この実践的なガイドは、オープンソース開発者とコントリビューターが、EUサイバーレジリエンス法がプロジェクトに与える影響を理解するのに役立ちます。このガイドは、Global Cyber Policy ワーキング グループ と Best Practices ワーキング グループによって共同で作成されました。
- 「Improving Risk Management Decisions with SBOM Data」：このドキュメントでは、ソフトウェア部品表 (SBOM) データを、「ただ作って終わり」ではなく、効果的に使用して具体的なリスク管理の意思決定を行う方法について、組織向けに解説します。

一般的なセキュリティ ベスト プラクティス

- 「Simplifying Software Component Updates」：コンポーネントの作成者と利用者向けの、アップデートを簡素化し、後方互換性の問題を回避するためのガイドです。このガイドは、DC Policy Summit 2025で提起された懸念事項や問題への対応として作成されました。

コミュニティとイベント

エコシステム パートナーシップとコミュニティ コラボレーション

BaselineとORBIT：オープンソース セキュリティの水準を引き上げる

2025年にOpenSSFは Open Source Project Security (OSPS) Baselineを立ち上げました。オープンソースプロジェクトがセキュリティ準備状況を評価•証明するのに役立つ、コミュニティが維持するフレームワークです。**2025年2月25日**にリリースされたこのベースラインは、**NIST Secure Software Development Framework（SSDF）**、**EUサイバーレジリエンス法（CRA）**、**ISO 27001**に準拠しており、グローバル標準にマッピングされた実用的で包括的なガイダンスを提供します。

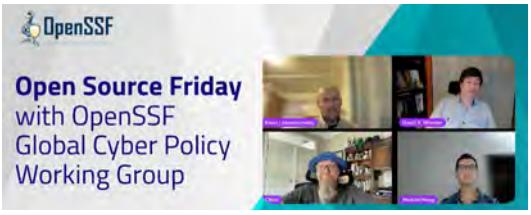
ベースラインは3つの成熟度レベルと8つの管理カテゴリーを定義し、認証、セキュアビルド、脆弱性管理に関する実用的な推奨事項を提供しています。Open Source Summit North America の基調講演と Tech Talk では、メンテナーや組織が標準に準拠し、日常のワークフローにセキュリティを統合するためにベースライン をどのように適用できるかが紹介されました。

The ORBIT ワーキング グループ は、セキュリティ インサイトや自動化統合などの関連プロジェクトを通じてベースラインを維持および拡張し、メンテナーがプロジェクトのセキュリティ データを公開し、長期にわたって改善を追跡できるようにします。Baseline と ORBIT を組み合わせることで、グローバル エコシステム全体にわたって測定可能で透明性のあるオープン ソース セキュリティの共通基盤が確立されます。

GitHub Secure Open Source Fundとの連携

OpenSSFは GitHub セキュアオープンソースファンドのエコシステムパートナーとして認められました。メンテナーへの直接的な資金提供と専門家によるガイダンスの 提供を通じて、オープンソースのセキュリティ強化に特化したプログラムです。OpenSSFは年間を通して、GitHubのSecure OSSコホートと定期的に連携し、セキュ リティのベストプラクティスを共有し、主要なOpenSSFプロジェクトを紹介し、メンテナーがコードベースのレジリエンスを向上できるよう支援しました。

このコラボレーションはGitHubのOpen Source Fridayスポットライトでも取り上げられ、OpenSSFグローバル サイバーポリシー ワーキング グループ がEUサイバーレジリエンス法（CRA）などのサイバーセキュリティ規制の変化について議論しました。セッションでは、OSPSベースラインやOpenSSFトレーニングコースといったコミュニティ主導のイニシアチブが、開発者、メンテナー、そして政策立案者にとって新たなコンプライアンス要件への対応にどのように役立っているかが強調されました。詳細については、当社のブログ「Open Source Friday with OpenSSF – Global Cyber Policy Working Group」をご覧ください。



イベントとグローバル展開

2025 年は OpenSSF のグローバル コミュニティの取り組みにとって節目の年となりました。大陸をまたいで活動範囲が拡大し、つながりが深まることで、私たちの存在感は大幅に高まりました。

主催イベント：世界規模のコミュニティ構築

私たちの主力イベントである**OpenSSF Community Days**は、**4大陸**にまたがる、真にグローバルなシリーズへと進化しました。セキュリティ実務家、オープンソースのメンテナー、そして業界リーダーが一 堂に会しました。**東京からデンバー、アムステルダムからハイデラバード、そしてソウル**に至るまで、これらの会合は、地域のオープンソース セキュリティ コミュニティにおける知識共有と関係構築のための重要な拠点として機能しました。

それぞれの Community Daysでは、その地域の独自の特徴が反映されるとともに、ソフトウェア サプライチェーンのセキュリティ保護の重要性、協力による防御の力、アクセスしやすいセキュリティ ツールとプラクティスの必要性、といった共通のテーマが強調されました。

この勢いに乗って、私たちは**アトランタ**で初の**Open Source SecurityCon North America**を共同主催しました。これはCloud Native Computing Foundation（CNCF）と共同で、KubeCon/CloudNativeConとの併催でした。この新しいカンファレンス は、オープンソース セキュリティとクラウドネイティブ エコシステム全体における、大規模なプロジェクト横断型のコラボレーションの進化を象徴しています。

私たちの声を広げる：業界との連携

OpenSSFのコミュニティは、主催イベント以外にも年間を通して**20以上の外部イベント**で、**60回以上の講演**を行いました。**Black Hat**や**DEF CON** 、地域ミートアップ、専門フォーラムなど、メンバーは多様な聴衆と知見、研究成果、実践的なガイダンスを共有しました。

また、Open Source in Finance ForumやベルギーでのLinux Foundation EU RoadshowのCRA in Practice sessionsなど、スポンサー付きトラックでのセッションを通じて、業界特有のコミュニティとの関わりを深めました。

地域の成長とコミュニティ間の連携

特に2025年は、OpenSSFが単なるグローバル展開ではなく、地域に根ざした存在感を重視していることが明確に示されました。アジア太平洋市場への進出、特に日本、インド、韓国における積極的な活動は、オープンソース開発の真の国際性と、ソフトウェア サプライチェーン セキュリティが直面する共通の課題を反映しています。また、Open Source Summit、KubeCon/CloudNativeCon、OpenSearchConにより、セキュリティを重視する実務者とより広範なオープンソース エコシステムの間で自然なコラボレーションとアイデアの相互交流が可能になり、開発ライフサイクル全体にセキュリティの考え方が組み込まれました。

2025年に築いた、継続的な地域との関わり、イベント形式の拡大、業界パートナーシップの深化を土台にして、OpenSSFはオープンソース セキュリティの真にグローバルな勢力として成長し続けることになります。

詳細なイベント情報については、「Community Engagement & Education: Events」セクションをご覧ください。

政策・公共部門との連携

サイバーレジリエンス法（CRA）：OpenSSFの役割と影響

世界各国の政府は、米国の「国家サイバーセキュリティ向上に関する大統領令」やEUの「サイバーレジリエンス法（CRA）」など、サイバーセキュリティ強化に向けた取り組みを加速しています。これらの取り組みはデジタルシステムの安全性向上を目指していますが、一部の対策は、オープンソースソフトウェア（OSS）の作成者や利用者にとって、意図せず負担を生み出す可能性があります。OpenSSF は政策立案者と協力し、サイバーセキュリティの進展が、オープンソース コミュニティを阻害するのではなく、支援するものとなるよう、理解を深めています。

2024年12月に開催された Open Source Software Stewards and Manufacturers Workshop を受け、OpenSSF は、新しいワーキング グループ「 Global Cyber Policy 」を立ち上げました。その目標はシンプルですが野心的です。サイバーレジリエンス法 (CRA) などの、世界的なサイバーセキュリティ規制と密接に連携し、その議論の場にオープンソースの声を確実に届けることです。

OpenSSF は、独自のイニシアチブとStandardization SIG と Awareness SIGの活動を通じて、実用的なポリシーと標準の策定を支援する専門家を集めています。開発者、企業、そして政府がセキュリティとコンプライアンスの目標を達成できるよう支援することに重点を置いています。これは、形式的な手続きを増やすのではなく、知識、ツール、そしてコラボレーションの機会を共有することで実現されます。グループの活動は、以下のいくつかの核となる考え方に基づいています。

- オープンソース コミュニティにおける教育と意識の向上
- 公共部門と直接関わり、意味のある政策形成に影響を与えること
- コンプライアンス遵守を容易にするツールの構築と改善
- オープンソースの成功の原動力であるコラボレーションとイノベーションを守りながら、国境や組織を越えた運用上のコラボレーションを促進すること

今年の重要な優先事項は、欧州の政策エコシステムとの強固な関係を構築することでした。最も大きな成果の一つは、ETSIとのパートナーシップを深め、参加と影響力の新たな道を切り開いたことです。

- IETSI 内では、OpenSSF が直接的な代表権を持ち、オープンソース ソフトウェアに関連するいくつかの標準づくりに貢献しています。
- ETSI と CEN/CENELEC のMode 4協力を通じて、これまでほとんどのコミュニティ グループが参加できなかった追加の欧州標準化活動にアクセスできるようになりました。

この取り組みにより、OpenSSFはメンバーに対し、CRA関連の標準の最新情報や関連する取り組みの進捗状況について周知の徹底を図ることができました。これらの取り組みに関連して、OpenSSFはType C組織として認定された3つの財団の1つであり、**European Commission's CRA Expert Group** に積極的に参加しています。このグループは**CRA's Article 26** の法的義務を満たし、「欧州委員会とステークホルダー間の協力と情報交換を促進する」ために設立されました。

さらに、OpenSSFはBSI（ドイツ連邦情報セキュリティ局）との非公式なパートナーシップを強化し続けています。BSIの関連研究をレビューし、そのフレームワークを活用してベースラインツールを強化してきました。このパートナーシップはまさに双方向のものであり、それに応じて、OpenSSFのガイドラインや成果物が BSI の出版物全体で参照されています。

OpenSSFコミュニティは、CRAに関わる特定のステークホルダーへの対応を支援する、高く評価されている成果物を提供してきました。最初のものは、CRAの様々な用語、関係者、そして要件を分かりやすく説明するために作成された「**Understanding the EU Cyber Resilience Act (LFEL1001)**」というクラスです。このクラスはすぐに最も人気のある無料クラスとなり、提供開始から 1 週間以内に何千人もの参加者が登録してクラスを受講しました。この傾向は年間を通じて続いています。

次に注目すべき点は、OSS 開発者向けの簡易ガイド「**Brief Guide for OSS Developers for the CRA**」も作成されたことです。この簡潔な文書は、オープンソース開発者向けに法律を解説し、施行が近づくにつれて開発者がどのようなことを期待できるかについて、明確で簡潔かつ実践的なアドバイスを提供しています。OpenSSFは、オープンソース開発者、オープンソース管理者、そして製造者が今後の期限に備えられるよう、様々な支援成果物の作成に積極的に取り組んでいます。

グループは月例会議を開催し、様々なCRAのコンセプトについて深く議論したり、開発者、管理者、製造者がそれぞれの義務を果たす上で役立つツールを紹介したりしてきました。これらの取り組みは、欧州標準化コミュニティとの緊密な関係によって支えられています。

OSSはグローバルな活動であるため、ヨーロッパも重要ですが、他の政策関連の取り組みも行ってきました。2025年初頭、OpenSSFはワシントンD.C.で政策サミットを開催しました。このフォーラムで提起され議論された問題に基づき、新しい OpenSSFガイド（「Simplifying Software Component Updates」）が作成されました。また、国連で開催されたOpen Source Week（特に Digital Resilience and Sovereignty トラック）にも参加しました。これらに加えて、以下でさらに説明するように、世界中のコミュニティへの働

きかけも続けています。

OpenSSFは今後1年間、サイバーセキュリティと標準化政策の策定における役割をさらに強化する予定です。CEN/CENELECとのリエゾン組織となるための申請を既に提出しており、ENISA、ECSO、ITUとの連携を模索し、世界規模での協力体制の拡大を目指しています。

OpenSSFは、ポリシーと標準化以外にも、Open Source Congress、OpenSSF Community Day 、European Open Source Security Forum など、複数の注目度の高いイベントに積極的に参加しています。これらの参加を通じて、EU 関係者、OSS コミュニティのリーダー、メーカー、その他の関係者との直接の交流や意見共有が促進されました。

私たちの目標は変わりません。それは、ヨーロッパや世界各地のサイバーセキュリティ ポリシーの開発において、オープンソースが強力で、情報に基づいた、信頼できる発言力を持つことを保証することです。

人工知能サイバーチャレンジ(AIxCC)

人工知能サイバーチャレンジ (AIxCC)は、国防高等研究計画局 (DARPA) が主導ARPA-Hと共同で、AIを活用したオープンソースソフトウェアのセキュリティ確保を目指した取り組みです。AIxCCの参加者は、重要な公共サービスで使用されるオープンソース ソフトウェアのサイバーセキュリティの脆弱性を自動的に検出し、修正するAIシステムを開発しました。8月のDef Conで閉幕したこのコンテストの決勝戦では、各チームのシステムが5,400万行に及ぶコード全体にわたる人工的な脆弱性を特定し、パッチを生成 するという課題に挑戦しました。決勝戦の70の課題において、参加者のシステムは合計54件の人工的な脆弱性を発見し、そのうち43件にパッチを適用しました。また、18件の人工的ではない実際の脆弱性を発見し、そのうち11件に対してパッチ生成に成功しました。OpenSSFは、オープンソース プロジェクトへの責任ある情報開示とパッチ提出を支援しています。

OpenSSFはAIxCCのチャレンジアドバイザーを務め、コンテストがオープンソース文化とコミュニティに有益なソリューションを提供するよう努めました。ファイナリストの7チームのシステムはオープンソースとして公開されました。コンテストで使用されたインフラストラクチャとデータも、進行中の研究活動を支援するためにオープンソースとして公開されました。

OpenSSFの AI / ML Security Working Group は、IxCC参加者による継続的なコラボレーションと、オープンソース ソフトウェアのセキュリティを向上させる自律システムのさらなる開発をサポートするために、Cyber Reasoning Systems Special Interest Groupを結成しました。

プログラムとプロジェクト

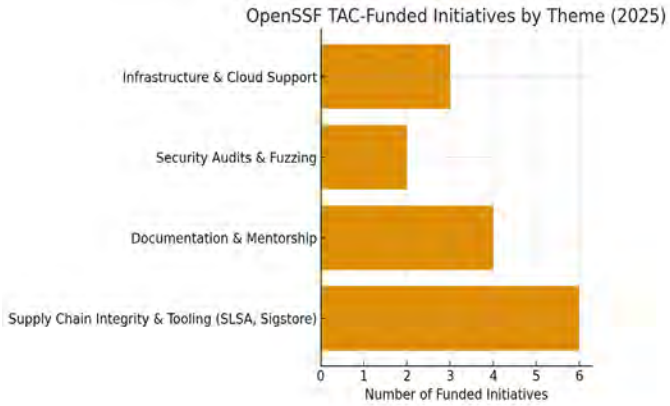
TI資金提供プロジェクトとその影響

過去1年間、OpenSSF技術諮問委員会（TAC）は、オープンソースソフトウェア エコシステムのセキュリティとレジリエンスを強化する14の技術イニシアチブに総額663,248ドルを提供しました。これらのプロジェクトは、監査、仕様策定、インフラストラクチャ、そしてコミュニティ開発にまで及び、オープンソースソフトウェアの安全性と持続可能性を高めるというOpenSSFの使命を推進しています。

主要な投資分野は、オープンソース ソフトウェア サイクル全体の信頼性を確保するためのサプライチェーンの整合性とツールです。資金提供を受けた14のTIのうち6つは、Supply-Chain Levels for Software Artifacts（SLSA）フレームワークに関連する作業に重点を置いていました。その他の投資は、コード署名インフラストラクチャにおける異常を検出することを目的とした新しいログ監視ウェブサイトの開発など、Sigstoreエコシステムを支援しました。

さらに、TACはOpenSSFの夏季メンターシッププログラムに資金を提供しました。4名のメンティーがメンターシップを無事に修了し、gittufおよびRSTUFプロジェクトに多大な貢献を果たしました。この取り組みは2026年夏にも継続される予定です。

グラフに示すように、今年の TI のほとんどはサプライ チェーンの整合性とツールに集中しており、続いてドキュメント、インフラストラクチャ、監査関連の作業が続きました。これらの取り組みは、世界のオープンソース インフラストラクチャのセキュリティを確保する実用的かつ協調的なソリューションに対する OpenSSF の取り組みを反映しています。



OSSインフラストラクチャとツールの改善

OpenSSFは **共同公開書簡** を通じて、オープンインフラへの持続可能な投資の必要性を強調し、広くメディアで取り上げられました。また、2025年を通して、様々な手段を通じて、OSSのインフラストラクチャとツール（OpenSSFが開発するツールを含む）の改善に取り組んできました。主な成果は以下のとおりです（詳細はOpenSSF TACの技術イニシアチブ **レポート** をご覧ください）。

重要なプロジェクトへの投資（Alpha-Omega）

Alpha-Omega プロジェクトは、2024 年の成功の勢いに乗って、戦略的投資モデルを拡大しました。2025年第1四半期および第3四半期を通じて、このプロジェクトは世界で最も重要なオープンソースプロジェクトに対し、数百万ドル規模の助成金とセキュリティサービスを提供し続けました。主要なインフラ整備の取り組みには、Python Software FoundationやRubyGemsといった主要なエコシステム内にセキュリティ担当者を配置することが含まれており、ボランティアによって維持されていることが多いプロジェクトの継続的なセキュリティ確保に役立っています。助成金により、専用のセキュリティ監査と高度なセキュリティ対策の実装を通じて、LinuxカーネルやHomebrewパッケージマネージャーなどのコアインフラ コンポーネントの強化に成功しました。これらの取り組みにより、OSS の重要な基盤部分の安全

参照：

- https://github.com/ossf/tac/issues/379
- https://github.com/ossf/tac/issues/414
- https://github.com/ossf/tac/issues/417
- https://github.com/ossf/tac/issues/451
- https://github.com/ossf/tac/issues/470
- https://github.com/ossf/tac/issues/472
- https://github.com/ossf/tac/issues/474
- https://github.com/ossf/tac/issues/475
- https://github.com/ossf/tac/issues/493
- https://github.com/ossf/tac/issues/494
- https://github.com/ossf/tac/issues/511
- https://github.com/ossf/tac/issues/538
- https://github.com/ossf/tac/issues/537
- https://github.com/ossf/tac/issues/536
- https://github.com/ossf/tac/issues/531

性が大幅に向上しています。Alpha-Omegaは最近、OSTIFを通じて主要なオープンソースプロジェクトに対する6 件の大規模監査と 20 件の迅速監査 の実施に資金提供を 承認 しました。また、Eclipse Foundation の OpenVSX に対しては、API 認証などの改善を通じて ecosyste.ms のセキュリティ態勢を強化するための支援 を行いました。さらに、OpenRefactory を通じて、Apache Airflow をパートナーとしてVEX 自動化ツールの構築を進めるための資金提供も行われています。

サプライチェーン ツールの成熟

2025年の主な焦点は、サプライチェーン セキュリティの基盤となるツールの成熟と普及でした。Sigstoreプロジェクトは、開発者が暗号署名されたソフトウェア成果物を容易に作成•検証できるようにするための取り組みを続けています。透明性ログはRekor on Tiles（別名「Rekor v2」）に 移行 し、バックエンドを最新のタイルベースの透明性ログ実装に移行することで、メンテナンスの簡素化と運用コストの削減を実現しました。タイルは保存コストが低く、キャッシュも簡単で、サービスのフットプリントも小さいため、導入の複雑さを軽減できます。

Supply Chain Integrity Working Groupは、SLSA 1.2 RC1（source trackの新規追加を含む）が リリース され、多くのコメントを受けて現在対応中です。S2C2Fは「SLSA Dependency Track」としてSLSAに統合され、重複を排除したうえで提供されます。GUAC（Graph for Understanding Artifact Composition）プロジェクトは、バージョン1.0のリリースにより、より広範な本番環境での使用が可能となり、安定性という大きなマイルストーンを達成しました。このインフラ ストラクチャの改善により、組織は複雑なソフトウェアサプライチェーンのメタデータを効率的に分析できるようになります。さらにOpenSSFは Trustifyの貢献を歓迎しました。Trustify は、サプライチェーン知識グラフを構築・活用するための統合的な中央ハブとして機能することを意図したツールであり、共同インフラストラクチャや開発者向けのセキュリティ分析ツールを直接強化するものです。

さらに、新しい AI モデル署名ライブラリに対する ファジング の資金提供も行われ、この取り組みの中で修正すべき問題が発見されました。

リポジトリの強化

Securing Software Repositories Working Groupは、Principles for Package Repository Securityを基に、パッケージ レジストリ (npm や PyPI など) 向けの ガイダンス の開発や実装の整備において大きな進歩を遂げました。例えば：

- Rust Crates、npm、および NuGet は、PyPI に続いて Trusted Publishing をサポートするようになりました。Trusted Publishing により、CI/CD パイプラインから公開する際にシークレットを埋め込む必要がなくなるため、デプロイが簡素化され、これまで起こっていた 危険なサプライチェーン攻撃の可能性が完全に排除 されます。
- パッケージ削除ポリシー を改良してリリースしました。パッケージレジストリが 2016 年の left-pad 事件のような問題に対処できるようにします。
- ソフトウェアリポジトリにおけるアテステーションのUI/UXサポートに関する研究に資金提供し、Style Guide for Attestations UI/UX を公開しました。一般的なユーザーはアテステーションに馴染みがないですが、意味が伝わり、信頼性が高く、既存のインターフェースと統合された方法で提示する必要があるため、人間にとって難しい問題となっています。私たちは、すべてのソフトウェアが依存する配布インフラ ストラクチャ全体のレジリエンスを強化するために引き続き取り組んでいきます。

私たちは、すべてのソフトウェアが依存する配布インフラ ストラクチャ全体のレジリエンスを強化するために引き続き取り組んでいきます。

参照：

- https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-Repos-WG.md
- https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-Repos-WG.md
- https://github.com/ossf/tac/pull/539/files
- https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-ST-WG.md
- https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-SCP-WG.md
- https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q3-SCP-WG.md
- https://github.com/ossf/tac/blob/main/TI-reports/2025/2025-Q1-Sigstore.md

メディアハイライト

ZDNET（月間閲覧数6,079,719回）
2025年に受講できる最高の無料AIコースと認定資格 - すべて試してみた
OpenSSFの「セキュアAI/ML駆動型ソフトウェア開発」コースが、無料AIコースとリソースのベストセレクションに選出されました。このコースは、セキュアAIコードのベストプラクティスを学ぶための良い出発点として評価されています。

The New Stack（月間閲覧数589,793回）
EUのサイバー法が孤独なオープンソース開発者に課す負担
OpenSSFのChristopher “CRob” RobinsonがThe New Stack Agentsポッドキャストに出演。Open Source Summit EU の出席中に、サイバーレジリエンス法について議論しました。

Infosecurity Magazine（月間閲覧数115,265回）
対談：Black HatとDEF CON後のCISOの学び
OpenSFFのチーフセキュリティアーキテクトであるChristopher “CRob” Robinsonが、Black Hat USA 2025とDEF CON 2025の後で考えを語ります。この記事には、OpenSSFのTrail of Bits、Canoncial、OSTIF も参加しています。

diginomica（月間視聴者数43,854人）
メンテナーを燃やすのではなく、橋を架ける - CRA がオープンソース関係をどのように再構築するか
OpenSSF の Christopher “CRob” Robinson は、Open Source Summit EU の会場で、CRA に関連する今後の機会と課題について diginomica のインタビューを受けました。

Help Net Security（月間閲覧数18,700回）
MLSecOpsの導入で企業が直面する6つの課題
OpenSFF のチーフ セキュリティ アーキテクトである Christopher “CRob” Robinson が、MLSecOps プログラムを確立または成熟させる際に IT リーダーが直面する 6 つの主要な課題について、Help Net Securityで詳しく説明します。

その他の報道

- **Tech.eu**、Linux Foundation Europe and OpenSSF launch initiative for EU Cyber Resilience Act compliance、2025年1月31日
- **ADT Magazine**、Linux Foundation and OpenSSF to Help Developers Navigate EU Cyber Resilience Act、2025年2月12日
- **Dark Reading**、OpenSSF Sets Minimum Security Baselines for Open Source Projects、2025年2月26日
- **SecurityWeek**、OpenSSF Releases Security Baseline for Open Source Projects、2025年2月26日
- **Infosecurity Magazine**、OpenSSF Releases Security Baseline for Open Source Projects、2025年2月27日
- **Help Net Security**、OSPS Baseline: Practical security best practices for open source software projects、2025年2月28日
- **DevOps.com**、OpenSSF Defines Baseline for Securing Open Source Software、2025年3月3日
- **InfoQ**、OpenSSF Publishes Security Baseline for Open-Source Projects、2025年3月5日
- **SD Times**、OpenSSF creates Project Security Baseline、2025年3月10日
- **I-Programmer**、Why OpenSSF's Baseline Security For Open Source Projects Is Important、2025年4月21日
- **ITOps Times**、Linux Foundation and OpenSSF launch Cybersecurity Skills Framework、2025年5月14日
- **SiliconANGLE**、Linux Foundation debuts Cybersecurity Skills Framework to address enterprise talent gaps、2025年5月14日
- **SC Media**、New Cybersecurity Skills Framework seeks to bolster enterprise talent readiness、2025年5月15日
- **Help Net Security**、Cybersecurity Skills Framework connects the dots between IT job roles and the practical skills needed、2025年5月16日
- **Security Boulevard**、Linux Foundation Shares Framework for Building Effective Cybersecurity Teams、2025年5月16日
- **ITdaily**、Linux Foundation Launches Global Cybersecurity Skills Framework、2025年5月19日
- **Linux Insider**、Is a Security Baseline Enough for Open-Source Software?、2025年6月13日
- **theCUBE**、CRob Robinson, OpenSSF | Open Source Summit 2025、2025年6月24日
- **Infosecurity Magazine**、NSA and CISA Urge Adoption of Memory Safe Languages for Safety、2025年6月25日
- **SiliconANGLE**、How open-source developers can meet global cybersecurity laws — before it's too late、2025年6月26日
- **SiliconANGLE**、Code, community and the future: 13 takeaways from Open Source Summit NA、2025年6月28日
- **Techstrong.ai**、Techstrong TV June 30, 2025、2025年6月30日
- **Techstrong.ai**、Navigating Software Supply Chain Security Challenges with Christopher (CRob) Robinson | Open Source Summit NA 2025、2025年7月3日

- **Help Net Security**、The 6 challenges your business will face in implementing MLSecOps、2025年8月20日
- **The New Stack**、What the EU's Cyber Resilience Act Means for Open Source、2025年8月21日
- **Infosecurity Magazine**、CISA Seeks Biden Era's SBOM Minimum Requirements Guideline Change、2025年8月25日
- **Tech.eu**、The World of Open Source Europe report 2025: mapping trends, challenges, and the push for digital sovereignty、2025年8月25日
- **Dutch IT Channel**、OpenSSF honors achievements in open source security and AI、2025年8月27日
- **Dutch IT Leaders**、OpenSSF honors achievements in open source security and AI、2025年8月27日
- **ITPro Today**、New Research Debunks Open Source Business Model Myths、2025年8月27日
- **diginomica**、Building bridges, not burning maintainers - how the CRA is reshaping open source relations、
  2025年8月27日
- **The New Stack**、The Cyber Resilience Act: Fear, Confusion — And Reassurance、2025年8月28日
- **The New Stack**、TNS Daily | August 29,、2025年8月29日
- **diginomica**、Enterprise hits and misses - services firms have an AI market meltdown, but why? Tech earnings roll in, as NVIDIA gets an Alibaba heads up、2025年9月2日
- **ITdaily**、Europe's turn: the opportunities and challenges of open source、2025年9月4日
- **Data Center Insider**、Digital sovereignty is moving to the center of open source strategies、2025年9月5日
- **Cybersecurity Dive**、How AI and politics hampered the secure open-source software movement、2025年9月9日
- **Data Center Insider**、Christopher Robinson on MLSecOps and the Cyber Resilience Act,、
  2025年9月10日
- **Infosecurity Magazine**、対談：Black HatとDEF CON後のCISOの学び、2025年9月10日
- **The New Stack**、How the EU's Cyber Act Burdens Lone Open Source Developers、2025年9月11日
- **The New Stack**、SBOMs Get a Needed Update for New Threats、2025年9月10日
- **InfoWorld**、More money for open source security won't work、2025年9月22日
- **Reversing Labs**、The call for funding of open-source platforms、2025年10月1日
- **ZDNET**、The best free AI courses and certificates right now、2025年10月23日

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

ワーキンググループとプロジェクトの最新情報

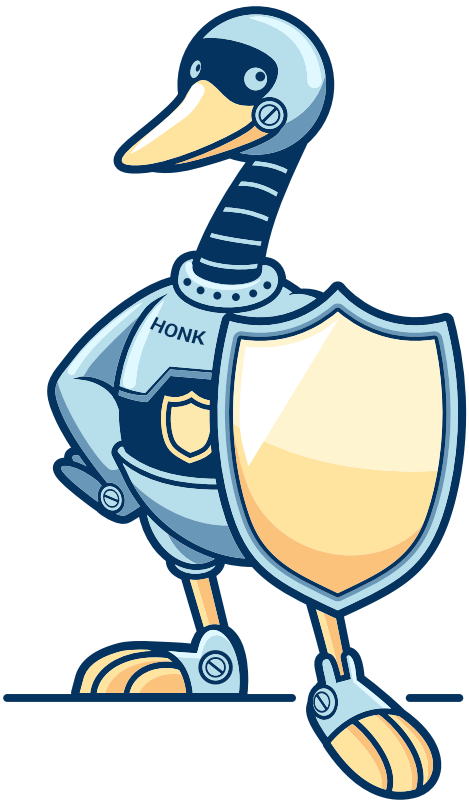
Open Source Security Foundation（OpenSSF）は、私たち全員が依存するソフトウェアのセキュリティ確保のため、オープンソース エコシステム全体にわたるコラボレーションを推進しています。ワーキンググループとプロジェクトは、このミッションの技術的バックボーンを形成し、脆弱性開示やサプライチェーンの整合性から、AI/MLの安全性やグローバルなポリシーへの関与に至るまで、オープンソース セキュリティにおける具体的な課題の解決に取り組んでいます。

2025年も、これらの取り組みは目に見える進歩を続け、新たな仕様の発表、Foundation間の連携の推進、教育リソースの公開、そして世界中でオープンセキュリティツールの普及拡大を実現しました。これらは、OpenSSFコミュニティを特徴づける、集合的な技術革新、コミュニティのリーダーシップ、そして共有責任を体現しています。

OpenSSF Technical Advisory Council (TAC)は、すべての技術イニシアチブ (TI) を監督し、ホストされているプロジェクトのプロジェクト ライフサイクルを維持します。

OpenSSF の技術的取り組みとホストされているプロジェクトの詳細については、プロジェクト ページ Projects pageをご覧ください。

OpenSSF GitHub リポジトリ: github.com/ossf



ワーキンググループ

AI / ML Security

AI/ML ワークロードのオープンソース ソフトウェア セキュリティの解決に焦点を当てたインキュベーティング ワーキング グループ

ワーキンググループ リーダー	コントリビューターの定常人数
Jay White, Mihai Maruseac	10〜20

GitHubリポジトリ

ossf/ai-ml-security

2025年のハイライト

- model-signing 1.0および1.1の立ち上げ
  - » OMSモデル署名フォーマット仕様の立ち上げ
- Visualizing Secure ML Ops ホワイトペーパー
- 「Secure AI/ML-Driven Software development」(LFEL 1012) course
- 4つの異なるSIG：
  - » Model signing
  - » AI Economics for OSS
  - » Safe MCP
  - » Cyber Reasoning Systems

影響

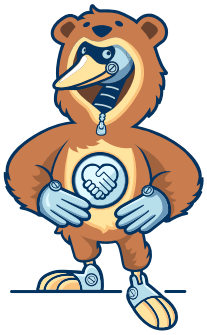
- 「AIのためのセキュリティ」（安全なMCP、モデル署名、エージェントカードの署名）と「セキュリティのためのAI」（推論システム、DARPA AIxCC、AIエコノミクスSIG）に取り組んでいます。
- OSSエコシステム全体におけるAIとセキュリティに関するあらゆる情報の中心的な場所。OpenSSF（BEST、サプライチェーンセキュリティ）、Linux Foundation（LF AI & Data Cybersecurity Compliance）、外部（Coalition for Secure AIなど）の他のワーキンググループとの連携
- Coaliation for Secure AIのホワイトペーパーでは、MLサプライチェーンのセキュリティ確保の第一歩としてmodel-signingアプローチを推奨しています。

次は何か（2026年）

- モデル署名のための統合を強化します。モデルハブがデフォルトで署名をサポートするようにし、最先端のラボがOSSのLLMに署名できるようにします。
- モデル署名、Atlasプロジェクト (Intel)、Sentryプロジェクト (Purdue) を基盤として、署名モデル、データセット、エージェントカードなどをカバーする AI/ML サプライ チェーン セキュリティの統合インフラストラクチャを構築し、すべての ML 成果物の来歴を生成します。

ワーキンググループ

Belonging, Empowerment, Allyship, and Representation



代表性を高め、サイバーセキュリティ人材の有効性を高める

ワーキンググループ リーダー	コントリビューターの定常人数
Jay White, Marcela Melara, Yesenia Yser	5〜8

GitHubリポジトリ
ossf/wg-dei

2025年のハイライト

- Ejiro Oghenekome、Sal Kimmich が オープンソース入門に関する3 部構成のblogシリーズをリリースし、2つが公開されました。
  - » 初心者からビルダーへ: 最初のコード貢献 – Open Source Security Foundation
  - » 初心者からビルダーへ: OpenSSFを理解するコミュニティとワーキンググループ – Open Source Security Foundation
- BEARワーキンググループは、OpenSSF Community Day NAでランチ・ミートアップをホストし、Open Source Summit NAでのOpenSFブースでの影響を共有しました。
- BEARワーキンググループは、2025年夏のLinux Foundation Mentorship プログラムで、メンティーの資金を獲得しました。4人のメンティーが今年のメンターシッププログラムを修了しました。
  - » 4人のメンティーを紹介するオフィスアワー https://youtu.be/_U-A7AD_Qks?si=6y6NPL30z8bbGsAb
- 2025年には、1月から10月まで合計9回のオフィスアワーが開催され、様々な種類のオフィスアワーが開催されました。

影響

- 新しい貢献者を OpenSSF に導くための初心者向けのブログ シリーズを公開しました。これにはトピックに重点を置いたオフィス アワーやマーケティングの配信も含まれます。
- Ijeomaの参加によるPython Ghanaや、OpenSSF Community Day NA や OSS Summit NA でのミートアップやブースの開催など世界各地のさまざまなオープンソースサミットにおいて、BEARを世界的に代表しました。
- Funded & mentored four mentees via Linux Foundation's 2025 summer program.
- 2025 年 1 月から 10 月にかけて、メンティー ショーケース セッション、AI/ML 開発コースのリリース、初心者向けブログ シリーズなど、9 回のオフィス アワーを開催しました。

次は何か（2026年）

- Prince Oforh Asiedu、Seth Mensah、Aaron Will Djadaの運営により、ソフトウェア開発、オープンソース、セキュリティに重点を置いたミートアップをアフリカで実施します。
- PyCon Africaの講演者や、ガーナおよびアフリカ全域で開催される PyConにおいて、The Linux Foundationへの可能性のあるブーススポンサーの支援を行います。
- オフィスアワーを継続します。
- DevRel グループと協力して、新しい貢献者の認識、ガイダンス、ワーキング グループの調整を支援する方法を戦略化します。
- オープンソース プロジェクトに対する追加のメンターシップのサポートを提供します。

ワーキンググループ

Best Practices for Open Source Developers

オープンソース開発者にベストプラクティスの推奨事項とアクセス可能なリソースを提供します

ワーキンググループ リーダー	コントリビューターの定常人数
Georg Kunz, Avishay Balter	8 ～ 9

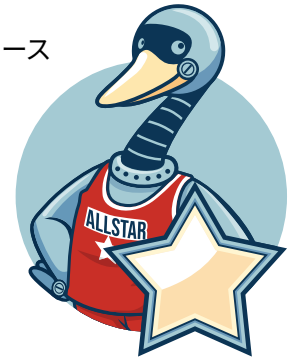
GitHubリポジトリ

ossf/wg-best-practices-os-developers

2025年のハイライト

- トレーニングコース
  - » Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)
  - » Security for Software Development Managers (LFD125)
  - » Secure AI/ML-Driven Software Development (LFEL1012)
  - » Japanese translation of LFD121
- 簡潔なガイド
  - » Security Focused Guide for AI Code Assistant Instructions
  - » Cyber Resilience Act (CRA) Brief Guide for Open Source Software (OSS) Developers
  - » Simplifying Software Component Updates
  - » Security Web Application Guidelines
- OpenSSFスコアカード
  - » OpenSSF Scorecard v5.3.0のリリース

  - » Allstar v.4.5 のリリース



- メモリセーフティSIG
  - » Memory Safety Continuum

影響

- ワーキンググループはLF Education主催の複数のトレーニングコースを公開しました。コースは非常に好評で、多数の受講生が参加しています。
- ワーキンググループは、ガイドや教育資料を共同で開発することにより、AI/MLワーキンググループおよびグローバルサイバーポリシーWGの両方と非常に効果的に協力しました。

次は何か（2026年）

- Python セキュア コーディング ガイドを開発しているチームは、2026 年初頭の最初のリリースに向けて取り組んでいます。
- C/C++ コンパイラ注釈ガイドは、既存の C/C++ コンパイラ オプション ガイドを補完するものとして、2026 年初頭に最初のリリースが予定されています。
- 教育SIGは、さらなる教育コースと教材に取り組んでいます。

ワーキンググループ

Global Cyber Policy

国際的な規制と立法、およびサイバーセキュリティフレームワークの適用に対する多分野にわたるアプローチ

ワーキンググループリーダー	コントリビューターの定常人数
Dan Appelquist, Roman Zhukov	19

GitHubリポジトリ
ossf/wg-global-cyber-policy

2025年のハイライト

- このグループは、2024年12月にアムステルダムで開催された「管理者と製造業者」に関するLinux Foundationのワークショップのあとに2025年1月に結成されました。このグループの形態は、このワークショップでの合意に基づいて決定されました。グループの目的は、オープンソースプロジェクトとその利用者による規制要件への適合を促進する、グローバルなサイバーセキュリティ関連の法規制、フレームワーク、標準について、メンバーとより広範なコミュニティが協力するためのフォーラムを提供することです。私たちは隔週で電話会議を開催しています。 私たちには2つのアクティブなSIGがあります。それはAwarenessとStandardsです。グループは、欧州サイバーレジリエンス法（CRA）に注力しており、他の法域の活動を監視する時間も確保しています。また、連絡担当者リストも作成しました。これは外部の連携する必要があると思われる liaisons list です。
- このグループは成果文書を作成し、アウトリーチ手段として機能し、規制の状況とそれが業界および OSS エコシステムに与える影響についてコミュニティのメンバー間で議論し情報を共有する場としても機能しました。
- ワーキンググループの共同リーダーは Daniel Appelquist | Samsung と Roman Zhukov | Redhat の2名です。Mike Bursell | Confidential Compute Consortium は、2025年10月まで最初のリーダーとして活躍しました。 CRob, Jeff Diecks, Madalin Neag そして David A. Wheelerを含むOpenSSFスタッフのサポートを受けています。
- また、私たちは「EU CRA Monthly Tech Talk」（旧称「CRA Tech Bi-weekly」）を運営しており、その議題は Awareness SIG によって管理されています。
- AwarenessおよびStandards SIGの定期的な会議に加え、主要なワーキンググループの会議 も開催しています。ツール関連の問題については、ORBITワーキンググループと協力しています。また、（FOSDEMおよびOSS NAといった他の対面式会議に加えて）Open Source Summit Europeにおいて、ワーキンググループの特別な対面式ハイブリッド会議を開催しました。この会議の焦点は、2つの異なる組織からCRA準備の取り組みと計画について意見を聞くこと、そしてCISAが最近発表した 2025年SBOMの最小要素に関する意見募集について意見を聞くことでした。
- LF Europe Roadshowーでワークショップを開催しました。昨年アムステルダムでこのワーキンググループを立ち上げたワークショップの形式を反映し、インタラクティブなディスカッションのために 10 月 29 日にゲントに集まりました。

影響

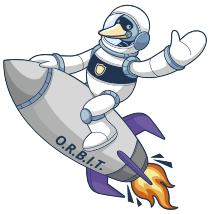
- CRAとその製造業者および開発業者への影響について、世界的な認知度向上に貢献しました。CRAに関する CRAに関する無料のLFトレーニング の立ち上げにも貢献しました。フィードバックや意見を提供することで、これまでに5500人以上の登録者を獲得しています。 6月の技術講演の要約 や 私は製造者か管理者か などのいくつかのブログ記事や CRA概要ガイドを公開しました。また、Linux Foundation 内のオープンソース管理に関するいくつかの OpenSSF ドキュメントに対するフィードバックも提供しました。

次は何か（2026年）

- 10月29日にゲントで開催されたLF Europe Roadshowでのワークショップの成果を活用して、2026年の実施プログラムを策定する予定です。2026年の焦点は、メーカー、保守担当者、管理者に対してより実用的なガイダンスを提供することになるでしょう。検討すべきトピックには、セキュリティデューデリジェンスの定義、「メーカー向けベースライン」の必要性の有無、メーカーが小規模なロングテールの上流プロジェクトにどのように関与できるか、ETSIやその他の標準化団体での活動、米国およびその他の規制体制との連携、「compliance.md」の定義、CRA関連ツールの現状把握などについてが含まれます。また、来年のFOSDEMでDevRoomの設置を提案しています。

ワーキンググループ

Open Resources for Baselines, Interoperability, and Tooling



国際的なベストプラクティスと規制に基づいて実装および評価するためのベースラインカタログとサポートツールに焦点を当てています

ワーキンググループ リーダー	コントリビューターの定常人数
Eddie Knight, TSC Chair. TSC members: Ben Cotton, John Kjell, Jennifer Power, Travis Truman	コールあたり平均10人の参加者

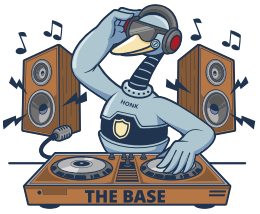
GitHubリポジトリ

ossf/wg-orbit

2025年のハイライト

影響

- LFXでOSPS Baselineのロールアウトを実施し、現在は2万個のリポジトリをスキャンしています。



- FINOSはGemaraを使用して3つのGRC関連プロジェクトをリンクできるようになりました
- FINOS TOCは、成熟度レベルに結びついたプロジェクトヘルスチェックの今後の改訂版にOSPSベースライン要件を含めました
- CNCF Security SlamとLFXの連携により、今年のSecurity Insightsの採用は200%増加しました

次は何か（2026年）

- OSPS BaselineとSecurity Insightsの継続的なメンテナンスと改善
- その他のプロジェクトやツールの継続的な開発

ワーキンググループ

Securing Critical Projects

重要なオープンソースプロジェクトを保護するためのリソースの特定と割り当てを行う

ワーキンググループ リーダー	コントリビューターの定常人数
Amir Montazery, Jeff Mendoza	4〜6

GitHubリポジトリ

ossf/wg-securing-critical-projects

2025年のハイライト

- 重要プロジェクトのセキュリティ確保ワーキンググループ（WG）では、エコシステム全体で広く利用されているオープンソースコンポーネントのセキュリティ体制を強化するため、複数の大規模な取り組みを推進しました。このグループの活動は、協調的なセキュリティ監査、対象を絞った修復、そしてエコシステム全体にわたる連携を通じて、測定可能な改善を推進することに重点を置きました。Malicious Packages は、Package Analysisから分離したスタンドアロンのプロジェクトとなりました。
- **セキュリティ監査と改善**
  - » Open Source Technology Improvement Fund(OSTIF) などのコミュニティ パートナーと連携した取り組みを含む、影響力の大きいオープン ソース プロジェクトに対して多数のセキュリティ監査と改善を実施しました。
  - » RSTUF を含むいくつかの OpenSSF プロジェクトの監査を完了しました (RSTUF Audit Complete!) およびセキュリティ スコアカード (OpenSSF Scorecard Audit is Complete!)。
  - » 発見事項を確実に修復し、脅威モデル、テスト インフラストラクチャ、ファジング機能を改善することで、長期的な持続可能性をサポートしました。
- **AIと重要インフラの取り組み**
  - » オープンソースAIインフラのレジリエンス向上に向けた実装活動を支援するOpenSSFとWGパートナーと、DARPAのAIxCC Challengeとの協力を継続していきます。2025年半ばに開始されたもので、2026年も継続されます。
- **Alpha-Omega エンゲージメント**
  - » Alpha-Omegaプログラムを通じて、WGは重要なOSSコンポーネントのセキュリティ強化活動に資金を提供し、監督しました。
  - » 25のオープンソースAIライブラリに関するセキュリティ調査（2025年第4四半期に公開予定）
  - » 重要な暗号化ライブラリのセキュリティ監査（2025年第4四半期〜2026年第1四半期に発行予定）
  - » セキュリティ強化プログラム: 60以上の重要なオープンソースプロジェクトが評価と修復作業を実施中
  - » Rubyエコシステムプログラム: セキュリティ監査とAlpha-Omegaと外部財団間の費用分担を通じて調整されたファズテストの改善
- **共同セキュリティエンゲージメント**
  - » ワーキンググループは、オープンソース技術改善基金（OSTIF）(ostif.org)を含むエコシステム全体とのパートナーシップを強化しました。重要なプロジェクトのセキュリティに関する連携を深めるため、2025 年にOSTIFのGeneral Memberに昇格しました。
- Malicious Packages
  - » これは包括的で高品質のオープンソースの、オープンソース パッケージリポジトリに公開された悪意のあるパッケージのレポートのデータベースです。.
  - » Package Analysisから分離し、スタンドアロンのプロジェクトに移行しました。

  - » エコシステム全体にわたる悪意のあるパッケージに関するデータの保存
    - – 66,000 NPM
    - – 10,000 PyPi
    - – 1,000 RubyGems
    - – 1,000 NuGet
  - » Go、Crates、Gitリポジトリ、Mavenレポートもサポートしています。
  - » 新しい **ステータスページ**
- **Criticality Score**
  - » このプロジェクトは、プロジェクトの影響と重要性を推定するための定量的なアプローチを実装しています
  - » 50万件のプロジェクトのスコアを毎月計算

影響

- 2025 年のセキュリティ活動の結果:
  - » **6つ**の脅威モデルが新たに追加もしくは更新されました
  - » **52**件の問題、発見事項、または強化の推奨事項に対処しました
  - » **5つ**のテストおよびファジングフレームワークを実装または強化
- これらの成果は、世界で最も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向上させるという WG の使命に向けた具体的な進歩を示しています。

次は何か（2026年）

- ワーキンググループは、持続可能な修復、エコシステムの拡張性、そして測定可能な成果を重視し、直接的なセキュリティ支援を必要とするより多くのプロジェクトを支援することに、エンゲージメントパイプラインを拡大します。2025年の勢いに乗って、すでに100近くのオープンソースプロジェクトがセキュリティ介入のターゲットとしての恩恵を受けており、2026年にはさらに多くのプロジェクトがこれに続く予定です。

ワーキンググループ

Securing Software Repositories

ソフトウェアリポジトリを強化し、保護する新しいツールとテクノロジーを導入します

ワーキンググループ リーダー	コントリビューターの定常人数
Dustin Ingram, Zach Steindler	-

GitHubリポジトリ

ossf/wg-securing-software-repos

2025年のハイライト

- ビルドパイプラインからAPIトークンを取得するためのセキュリティ機能であるTrusted Publishingが crates.io、npm、そして NuGet 向けにリリースされました。
- RSTUFはv1.0をリリースしました。これは、リポジトリがパッケージインデックスの整合性を保護できるようにするものです。
- デザイナーと協力して リポジトリ内のアテステーションを表示するためのUI/UXガイダンスを作成しました。
- The working group released guidance on パッケージ削除ポリシーを作成するためのガイダンスをリリースしました。

影響

- ワーキンググループは、2025年に6つのパッケージリポジトリに展開される8つのセキュリティ機能を促進/サポートしました。特に、前述のcrates.io,、 npm,、そして NuGet 向けのTrusted Publishingに加えて、Maven Central や Bazel Central の来歴(provenance)の検証サポートです。
- 私たちは、ソフトウェア リポジトリに対するさまざまなサプライチェーン攻撃の後に多くの議論をホストしました。

次は何か（2026年）

- 過去2年間の教訓を踏まえた パッケージリポジトリのセキュリティに関する原則 の更新
- リポジトリを集めて、ギャップ、ロードマップ、そして資金調達全般に関する議論
- リポジトリのマルウェア検出、対処、通知についての議論

ワーキンググループ

Security Tooling

オープンソース開発者向けのセキュリティツールを提供し、誰でもアクセスできるようにします

ワーキンググループリーダー	コントリビューターの定常人数
Ryan Ware	8〜12人のアクティブなコントリビューター

GitHubリポジトリ

ossf/wg-security-tooling

2025年のハイライト

- Security Tooling WGは今年、オープン ソース ソフトウェア セキュリティ エコシステムを強化するためにいくつかの重要な取り組みを進めました。
- OpenBao はLF EdgeからWGプロジェクトとして承認され、サンドボックス 要件を満たし、インキュベーションプロセスを開始しました。v2.3.0では、Namespace（テナンシー）、UI 2.0、外部キー管理などの新機能が導入され、スケーラビリティと信頼性のさらなる向上が計画されています。

- このグループは、バイナリ分析を改善し、脆弱性評価を強化するためにコンパイラツールチェーンにメタデータを埋め込むために、Reliable Software Decomposition SIG（DARPA E-BOSS プログラムから派生）を立ち上げました。
- SBOMit はインキュベーションに向けて進歩を続けており、検証可能な SBOM を生成するための in-toto 認証と自動化に焦点を当てた最初のワークショップをワシントン DC で開催しました。

- Minder は自動化と修復の機能を成熟させ、コンテキスト処理の拡張、ルール作成の改良、他の OpenSSF ツールとの相互運用性の向上を実現しました。

- 隔週で定期的に開催されるコミュニティコールでは、GitLab、Intel、Lockheed Martin、Target、Oracle、NYUなどのコントリビューターを含むエコシステム全体からの積極的な参加が維持され、複数のサブプロジェクト間で優先順位を調整するのに役立ちました。
- CVE-Bin-Tool はOpenSSF TACによって新しいプロジェクトとして承認され、コンパイルされたバイナリ内の脆弱な依存関係を開発者が特定する能力を強化します。

影響

- WGは、OpenSSF ツール プロジェクトと外部エコシステムの相互運用性を強化し、導入の障壁が下がり、オープンソース ソフトウェアのセキュリティに対する開発者の信頼を高めました。OpenBao、Minder、CVE-Bin-Tool、SBOMitといったイニシアチブを単一のフレームワークに統合することで、WGはソフトウェアサプライチェーンのあらゆる段階に対応する、より統合性の高いオープンツールスイートの構築に貢献しました。Reliable Software Decomposition SIGを通じた連携により、学術•研究コミュニティとの連携が拡大し、コンパイラレベルのセキュリティ計測におけるイノベーションが促進されました。

次は何か（2026年）

- 来年、WGは以下のことを計画しています。
  - » SBOMit をインキュベーションに向けて前進させ、サプライチェーンの認証用の SBOM ツールを拡張します。
  - » OpenBaoの卒業記念の節目をサポートし、他のOpenSSF プロジェクトとの統合を深めます。
  - » WG プロジェクト全体でドキュメントと成熟度の追跡を統合します。
  - » Reliable Software Decomposition SIG とクロスファウンデーション パートナーシップの拡大を継続します。
  - » AI/ML セキュリティ WG を含む WG 間の連携を強化し、進化するオープンソース セキュリティ環境全体にわたる取り組みを調整します。

ワーキンググループ

Supply Chain Integrity

個人がコードの由来を理解し、情報に基づいた意思決定を行えるように支援します。これにはGUAC、SLSA、gittufのようなプロジェクトが含まれます。

ワーキンググループ リーダー	コントリビューターの定常人数
Isaac Hepworth, Jay White	-

GitHubリポジトリ

ossf/wg-supply-chain-integrity

2025年のハイライト

- 新しいSLSAトラック
- GUAC傘下のTrustify寄付
- GUAC 1.0.0 リリース

影響

- 共有機能をサポートするためにプロジェクトを統合します。
  - » ZARFとGUAC統合

次は何か（2026年）

- SCI WGは目標と重点分野を刷新しています。
  - » コラボレーションを促進し、実用的なリソースを提供するための役割と主要な目標を特定します。

ワーキンググループ

Vulnerability Disclosures

脆弱性報告とコミュニケーションを促進するオープンソースセキュリティを強化します

ワーキンググループ リーダー	コントリビューターの定常人数
Madison Oliver, CRob	2025年に2回以上会議に出席したコントリビュータ19名

GitHubリポジトリ

ossf/wg-vulnerability-disclosures

2025年のハイライト

- OSV スキーマの拡張が新しいエコシステム (Kubernetes、MinimOS、Bellsoft Alpaquita、Hardened Containers、Echo、Julia) にまで広がり、数百万の OSS ユーザーとパッケージの脆弱性カバレッジが向上しました。
- OSV Linter はパッケージ/バージョンを追加して強化されました存在チェックとupstream/aliasesの検証により、OSV レコードのデータ品質と使いやすさが向上します。
- マルチステークホルダーの脆弱性対応プラットフォームである OpenSSF のもとで、Advise (旧称 VINCE) のオープンソース化に向けて議論されました。
- OpenSSFメンバー/プロジェクトが著名な代表として VulnCon 2025 へ参加しました
- AI-generated/slop security reports について、メンテナーと報告者への潜在的なガイダンスについて議論しました。「セキュリティ業務は特別なもの」というパラダイムの転換、持続可能で包括的なセキュリティ報告モデルの促進について検討しました。
- CISA ソフトウェア取得ガイドで強調されている product-first vulnerability disclosure report (VDR) specification の必要性について議論しました。
- CVE プログラムの資金リスクに対応して CVE プログラムの持続可能性と緊急時対応計画について継続的に議論し、OSV as potentially a global vulnerability databaseなどの代替手段を通じて OSS の回復力を確保します。

影響

- VulnCon などの業界カンファレンスにおけるOpenSSF の存在感と影響力を高め、CVE プログラムや PURL プロジェクトなどの業界パートナーとの協業を強化しました。
- 低品質の AI 生成セキュリティ レポートが大量に生成されることによる課題に対処し、高品質のレポートの促進に取り組みました。
- 断片化を回避し、既存の取り組みを活用するため、OWASP CycloneDX など既存の標準化団体との協業を視野に入れた VDR 開発の戦略的再評価を実施しました。
- 消費者向けに緩和と修復を重視した、消費者向けの実用的な脆弱性情報の作成に注力しました。

次は何か（2026年）

- OpenSSFプロジェクトとしてAdviseの開発と採用を継続します。
- CVD Guide for OSS Consumers の完成と普及を推進します。
- 標準化された製品中心の VDR に関する継続的な議論や潜在的なコラボレーションに参加します。
- AI によって生成されたセキュリティ レポートを評価および処理するためのガイダンスを開発します。
- ワーキンググループ会議への世界的な参加を促進します。

OPENSSFプロジェクトおよび関連プロジェクト

Sigstore

ソフトウェアサプライチェーンにおける信頼性を向上させるための署名、検証、透明性ツールを提供します

ワーキンググループリーダー	コントリビューターの定常人数
TSC (Bob Callaway, Luke Hinds, Trevor Rosen, Santiago Torres-Arias, Priya Wadhwa), Community Chair (Hayden Blauzvern)	55

GitHubリポジトリ
sigstore

2025年のハイライト

- Sigstore署名のMaven Central がサポートを発表しました。
- Sigstore を使用する Go アプリケーション用の最小限の API を提供し、他の Sigstore SDK に準拠した sigstore-go v1.0 がリリースされました。
- 標準化された 署名バンドル形式 をサポートし、OCI Image v1.1参照アーティファクトとしてアテステーションを保存する Cosign v3 がリリースされました。
- メンテナンスを簡素化し運用コストが削減するため再設計され近代化された署名の透明性ログである Launched Rekor v2 がリリースされました。
- オープンソースでのサインインを調査する研究者向けのBigQueryデータセットである Sigstore Transparency Log research dataset が公開されました。
- OpenSSF、NVIDIA、HiddenLayerと共同で、透明な署名を介してMLモデルを改ざん不可能にする model-transparency v1.0 を発表しました。
- NVIDIA announced signed models がNGCカタログの署名済みモデルを発表しました。

影響

- AIが現代の開発の基盤となるにつれ、SigstoreはMLサプライチェーンのセキュリティパイプラインに信頼性と整合性を提供します。OpenSSFはSigstoreとモデルの透明性を活用したMLモデルのセキュリティに関する ホワイトペーパー を、CoSAIはSigstoreとモデルの透明性に関する ホワイトペーパー を公開しました。また、ICMLでは、on ML model security with Sigstore and model-transparency, and a MLモデルのサプライチェーンセキュリティに関する研究論文 とSigstoreがモデル署名の透明性をどのように実現するかに関する研究論文が発表されました。

次は何か（2026年）

- OSSパッケージマネージャとの連携を継続し、署名と検証を簡素化します。
- ポスト量子署名 に関する研究と実験を支援します。
- 公開ログオペレータの多様性を高め、ログを public witness network に統合します。

OPENSSFプロジェクトおよび関連プロジェクト

Core Toolchain Infrastructure

Core Toolchain Infrastructure (CTI) プロジェクトの使命は、安全なサプライ チェーンにおける信頼できる基盤となるためのコミュニティの開発努力をサポートするために必要な、安全なインフラストラクチャと最先端のサービスによって GNU ツールチェーン コミュニティをサポートすることです。

ワーキンググループ リーダー	Webサイト
Carlos O'Donell, David Edelsohn	https://cti.coretoolchain.dev/

GitHubリポジトリ
https://git.coretoolchain.dev/

2025 HIGHLIGHTS

- CTI TAC と glibc プロジェクトは、glibc と GNU ツールチェーンの SSDLC 記述に取り組み、2025/2026 年に持続可能かつ安全なインフラストラクチャを備えた GNU ツールチェーンの前進をサポートしました。
- CCTI TAC は、glibc ソース リポジトリ (gitolite) に対する透過的かつ監査可能なアクセス制御の使用に関する提案をガイドしました。

次は何か（2026年）

- CTI は、SSDLC を通じて、GNU ツールチェーンの持続可能かつ安全な開発インフラストラクチャのサポートを継続します。

OPENSSFプロジェクトおよび関連プロジェクト

Alpha-Omega

2025年も、Alpha-Omegaは、効果が高く持続可能な投資を通じてオープンソースのセキュリティを強化するという使命を継続しました。14の重要なオープンソースプロジェクトに580万ドル以上が投入され、対象を絞ったエンジニアリング活動と、より広範なエコシステムの改善の両方を支援しました。

α → Leverage

Ω → Scale

Citiは5月に一般会員として参加し、資金とエンジニアリングサポートの両方を提供しました。Alpha-Omegaは、Open Source Summit North Americaで第2回年次対面式ラウンドテーブルを主催したほか、ワシントンD.C.で開催された2025 Policy Summitや国連Open Source WeekのMaintain-a-Thonといった主要イベントにも参加し、エコシステムへの関与を深めました。

プロジェクトの重要なマイルストーンとしては、RustのTrusted Publishingのローンチ とCVE認証、 ApacheのTrusted Releaseパイプラインのパイロット、そしてPython、Node.js、Ruby、Eclipse Foundation、FreeBSDのセキュリティアップグレードなどが挙げられます。Alpha-OmegaはOSTIFとのパートナーシップの下、数多くのオープンソースプロジェクトの監査への投資を継続しました。これらの監査は、多くのプロジェクトにとってセキュリティ強化の道のりの始まりとなります。

セキュリティ対策への支援を求めるオープンソースプロジェクトは、助成金申請を提出することをお勧めします。詳細については、Alpha-Omega website と GitHub リポジトリ をご覧ください。アニュアルレポートの全文は、2026 年初頭にここに公開される予定です。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

コミュニティ エンゲージメントと教育

Chair, Marketing Advisory Councilより

過去1年間、OpenSSFコミュニティはその影響力と野心を拡大し続けており、マーケティング諮問委員会（MAC）はその勢いをさらに推進する一翼を担えたことを光栄に思います。私たちの役割は、OpenSSF全体で行われている重要な取り組みを加速させ、貢献者、メンテナー、政策立案者、そして企業のリーダーたちが、オープンソースのセキュリティ確保がなぜ重要なのか、そしてどのように行動を起こすことができるのかを明確に理解できるようにすることです。

後、2026 年以降に向けた当社の重点は明確です。

2026年に向けた共通のマーケティングビジョン

私たちは、会員の協力を促す、統一された年間マーケティングテーマを開発しています。年間を通してストーリーを共有する機会を設けることで、会員の皆様はOpenSSFの優先事項に沿って活動を進め、共に私たちの使命を推進することができます。

長期的な向上成功事例

Mila Zhou, Chair, Marketing Advisory Council OpenSSF

私たちのセキュリティ対策の多くは、その効果が完全に発揮されるまでに時間がかかり、時には何年もかかることもあります。2026年には、こうした長期的な成果に関するストーリーテリングをさら

に強化します。意義のある成果を追跡し、強調することで、メンバーの皆様が取り組みの成果を実証できるよう支援し、オープンソース セキュリティへの投資と組織内での継続的なサポートを確保します。

教育と意識の拡大

セキュリティは、知識へのアクセスが容易になることで向上します。MACは、プログラム、コンテンツ、キャンペーンを通じて、オープンソースセキュリティの重要性だけでなく、それを実践的に導入する方法についても、世界中の人々に理解を深めていただけるよう支援していきます。LFD121のような

広く普及しているコース、プロジェクトスポットライト、あるいは新たなペルソナレベルのコミュニケーションなどを通じて、チームが自信を持って次のステップに踏み出せるよう支援していきます。

私たちの財団としての成功は、メンバー、貢献者、そしてより大規模なコミュニティの協力によって強化され、OpenSSFのツールとベスト プラクティスを世界中の開発者に提供し続けています。

安全なソフトウェアの未来を築く中で、マーケティングは単なるプロモーションではありません。それは、支援、教育、そしてエンパワーメントです。このコミュニティの情熱と創造性に感謝し、OpenSSFの影響力の拡大を共に語り合いながら、共に歩んでいくことを楽しみにしています。

感謝を込めて

Mila Zhou
Chair, Marketing Advisory Council
OpenSSF

OpenSSF DevRel アクティビティ 2024年後半以降

Katherine Druckman
Independent

Stacey Potter
Manager of Community, OpenSSF

ミッションと戦略的基盤

OpenSSF DevRelコミュニティは、OpenSSFの使命と活動を広く伝えることを目的としています。重要なオープンソースプロジェクトにおけるツールの採用を促進し、エンドユーザーとオープンソースコミュニティ全体とのより強 固な関係を築くことを目指しています。

コンテンツ制作とグローバルイベントへの参加

コミュニティは、「What's in the SOSS?」ポッドキャストや、FOSDEM、VulnCon、OpenSSF Community Days、世界中の Open Source Summits などのイベントへのカンファレンス参加を通じて、強力なグローバルプレゼンスを維持しました。コミュニティはブーススペースを担当し、オフィスアワーを主催し、セキュリティツールの導入から EU サイバーレジリエンス法の遵守まで、さまざまなトピックに関するセッションを発表しました。

専門性の向上と将来の方向性

DevRelコミュニティの活動は、**開発者リレーション** の設立によって強化されました。2025年 8 月に Linux Foundation 傘下の OpenSSF DevRel Foundation が設立され、DevRel プラクティスの向上と標準化されたメトリクスの確立に重点を置いた、より大規模な専門的ムー ブメントの中に OpenSSF DevRel が位置付けられるようになりました。

DevRelコミュニティは今後も、OpenSSFセキュリティツールの採用拡大、エンドユーザーおよびメンテナーとの関係強化、そしてコンプライアンス重視の姿勢よりもコラボレーションと教育を重視する人間中心のアプローチを通じて、より安全なオープンソース・エコシステムへのコミットメント強化に尽力していきます。現在、持続可能なエンゲージメントのためのインフラの構築、新規参入者向けの文脈に沿った資料の開発、イベント戦略フレームワークの確立、そして貢献者向けオンランプの強化に注力しています。

イベント

Policy Summit DC

2025年3月4日 | ワシントンD.C.

OPEN SOURCE SECURITY FOUNDATION
POLICY SUMMIT

OPEN SOURCE SECURITY FOUNDATION
POLICY SUMMIT

ワシントン D.C.
2025年3月4日

#SOSSPOLICY

イベント開催報告

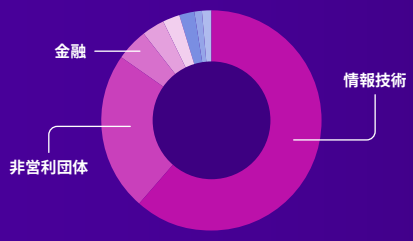
88 参加者の登録人数

70 参加者の出席人数

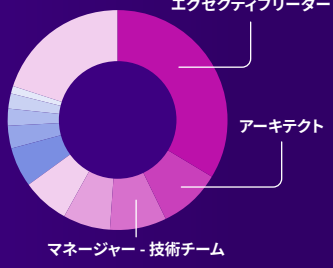
62 組織の総数

バージニア州: 16.25%
ニューヨーク州/カリフォルニア州: 13.75%
コロンビア特別区: 11.25%
テキサス州: 6.25%
メリーランド州 / マサチューセッツ州 / コロラド州: 5.00%

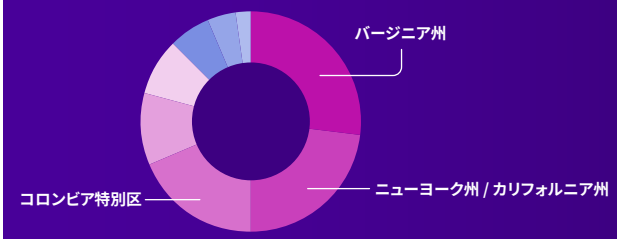
23 SPEAKERS
35% 女性スピーカー
4 ブレイクアウト
5 パネルセッション
5 基調講演

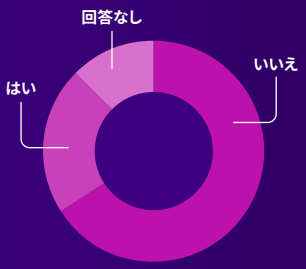


産業
- 情報技術 62%
- 非営利団体 23%
- 金融 5%
- 工業 3%
- ヘルスケア 2%
- 通信 2%
- コンシューマ製品 1%
- 無回答 1%



職務内容
- エグゼクティブリーダー 34%
- アーキテクト 9%
- マネージャー - 技術チーム 8%
- 法務 / コンプライアンス 7%
- マネージャー - その他 7%
- マネージャー - OSPO 6%
- マーケティング 3%
- 製品 / ビジネス開発 2%
- 教授 / 学術 2%
- アプリケーション開発者（フロントエンド / バックエンド / モバイル / フルスタック）2%
- その他 20%





OpenSSF イベントは初めてですか？
- いいえ 66%
- はい 22%
- 無回答 13%

OpenSSF Community Day Japan

2025年6月18日 | 東京、KUBECONと共催

OpenSSF Community Day
JAPAN

OpenSSF Community Day
JAPAN

東京、日本 2025

#OpenSSFCommunity

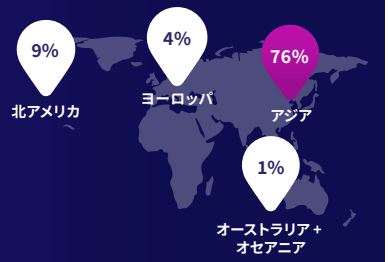
イベント開催報告

67 参加者の登録人数

271 参加者の出席人数

182 組織の総数

地域別参加者数



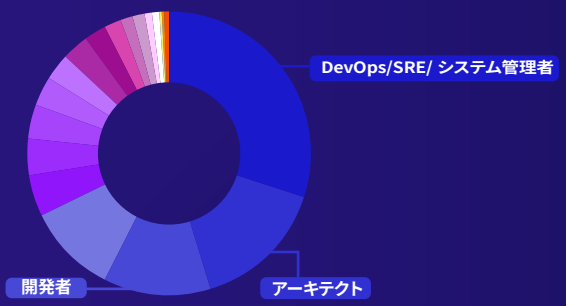
24 CFPへの応募

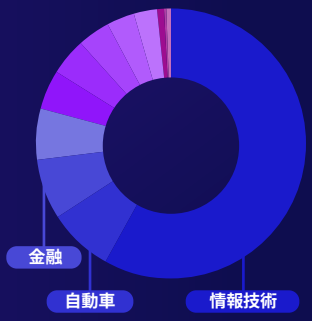
3 基調講演

16 スピーカー

19% ジェンダーマイノリティのスピーカー

57% POCスピーカー





職務内容

DevOps/SRE/ システム管理者	30.26%	マネージャー - OSPO	2.58%
アーキテクト	15.13%	カーネル / オペレーティングシステム開発者	1.85%
開発者	12.18%	IT オペレーション	1.48%
その他	10.33%	マネージャー - 技術チーム	1.48%
エグゼクティブリーダー	4.80%	教授 / 学術	0.74%
マーケティング	4.06%	学生	0.74%
製品 / ビジネス開発	4.06%	法務 / コンプライアンス	0.37%
アプリケーション開発者（フロントエンド / バックエンド / モバイル / フルスタック）	3.32%	その他マネージャー	0.37%
		メディア / アナリスト	0.37%
ビジネスオペレーション	2.95%		
システム / 組み込み開発者	2.95%		

業界

情報技術	58.30%
自動車	7.75%
金融	7.01%
通信	6.27%
プロフェッショナルサービス	4.80%
工業	4.43%
非営利団体	3.69%
コンシューマ製品	3.32%
無回答	2.95%
エネルギー	0.74%
ヘルスケア	0.37%
素材	0.37%

OpenSSF Community Day North America

2025年6月26日 | デンバー、オープンソースサミットと同時開催

北米

OpenSSF Community Day
NORTH AMERICA 2025

OpenSSF Community Day
NORTH AMERICA

コロラド州デンバー 2025

#OpenSSFCommunity

イベント開催報告

149 参加者の登録人数

164 参加者の出席人数

108 組織の総数

地域別参加者数

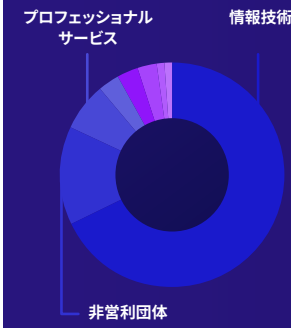
72 CFPへの応募

29 セッション

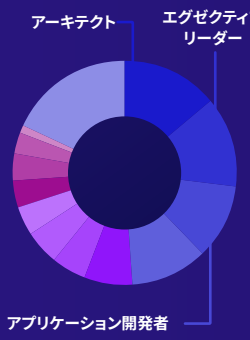
42 セッション

10% ジェンダーマイノリティのスピーカー

5% POCスピーカー



Industry
- 情報技術 68%
- 非営利団体 14%
- プロフェッショナルサービス 7%
- コンシューマ製品 3%
- 金融 3%
- 工業 3%
- 自動車 1%
- 通信 1%



職務内容
- アーキテクト 14%
- エグゼクティブリーダー 13%
- アプリケーション開発者（フロントエンド / バックエンド / モバイル / フルスタック）11%
- マネージャー - 技術チーム 11%
- マネージャー - その他 7%
- マーケティング 5%
- DevOps/SRE 5%
- マネージャー - OSPO 4%
- 学生 4%
- 製品 / ビジネス開発 4%
- 法務 / コンプライアンス 3%
- 教授 / 学術 1%
- その他 18%

スポンサーの皆様に感謝申し上げます

Defense Unicorns

kusari

DELL Technologies

OpenSSF Community Day India

2025年8月4日 | ハイデラバード、KUBECON+クラウドネイティブコン インド と共同開催

OpenSSF Community Day
INDIA

OpenSSF Community Day
INDIA

August 4, 2025

ハイデラバード、インド

#OpenSSFCommunity

イベント開催報告

209 参加者の登録人数

232 参加者の出席人数

138 組織の総数

地域別参加者数

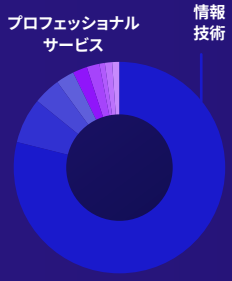
55 CFP提出

17 セッション

18 スピーカー

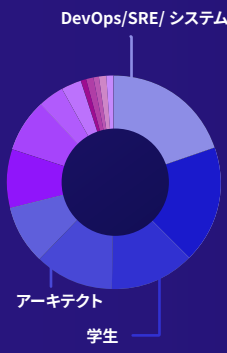
11% ジェンダーマイノリティのスピーカー

10 POCスピーカー



業界

- 情報技術 79%
- プロフェッショナルサービス 7%
- 非営利団体 4%
- 通信 3%
- 自動車 2%
- 工業 2%
- ヘルスケア 1%
- エネルギー 1%
- 金融 1%



職務内容

- DevOps/SRE/ システム管理 20%
- アプリケーション開発者（フロントエンド / バックエンド / モバイル / フルスタック）18%
- 学生 13%
- アーキテクト 12%
- カーネル / オペレーティングシステム開発者 9%
- その他 8%
- エグゼクティブリーダー 8%
- システム / 組み込み開発者 4%
- マネージャー - その他 3%
- マネージャー - OSPO 1%
- マネージャー - 技術チーム 1%
- 製品 / ビジネス開発 1%
- マーケティング 1%
- 教授 / 学術 1%

OpenSSF Community Day Europe

2025年8月28日 | アムステルダム
OPEN SOURCE SUMMIT EUROPE併設

OpenSSF Community Day
EUROPE 2025

OpenSSF Community Day
EUROPE

アムステルダム, オランダ 2025

#OpenSSFCommunity

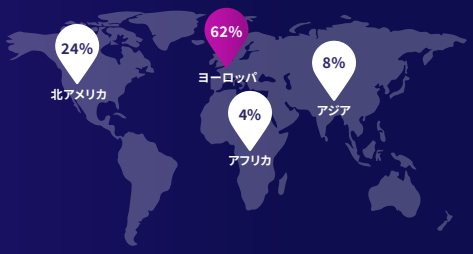
イベント開催報告

144 参加者の登録人数

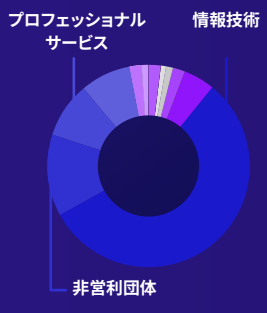
165 参加者の出席人数

118 組織の総数

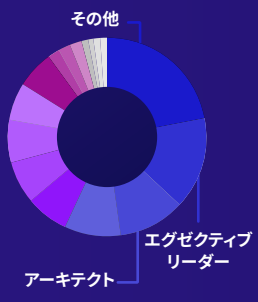
地域別参加者数



91	27	33	18%	3%
CFP提出	セッション	スピーカー	ジェンダーマイノリティのスピーカー	POCスピーカー



業界
- 情報技術 56%
- 非営利団体 13%
- プロフェッショナルサービス 9%
- 通信 8%
- 製造業 5%
- ヘルスケア 2%
- 自動車 2%
- コンシューマ製品 2%
- エネルギー 1%
- 金融 1%
- 材料 1%



職務内容
- その他 23%
- エグゼクティブリーダー 15%
- アーキテクト 12%
- マネージャー - その他 9%
- システム / 組み込み 開発者 - その他 7%
- アプリケーション開発者（フロントエンド / バックエンド / モバイル / フルスタック）7%
- マネージャー - 技術チーム 7%
- DevOps/SRE/ システム管理者 6%
- マネージャー - OSPO 5%
- カーネル / オペレーティングシステム開発者 2%
- 法務 / コンプライアンス 2%
- マーケティング 2%
- メディア / アナリスト 1%
- 教授 / 学術 1%
- 製品 / ビジネス開発 1%

スポンサーの皆様に感謝申し上げます

BREAKS
kusari

RECEPTION
Red Hat

European Open Source Security Forum
2025年10月30日

European Open Source Security Forum 2025

ブリュッセル、ベルギー

#OSSecurityForum

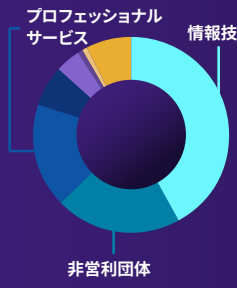
イベント開催報告

81 参加者の登録人数

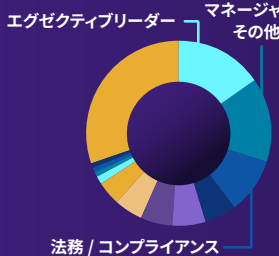
125 参加者の出席人数

100 組織の総数

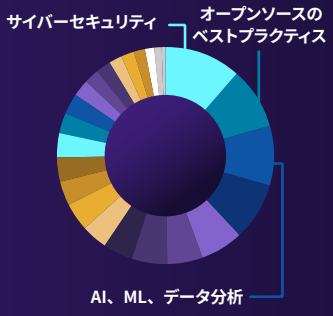
3	7	21	5	2
基調講演	ブレイクアウトセッション	スピーカー	ジェンダーマイノリティのスピーカー	POCスピーカー



業界
- 情報技術 41%
- 非営利団体 20%
- プロフェッショナルサービス 17%
- 通信 7%
- 金融 4%
- 自動車 1%
- エネルギー 1%
- その他 9%



職務内容
- エグゼクティブリーダー 15%
- マネージャー - その他 15%
- 法務 / コンプライアンス 10%
- マネージャー - OSPO 5%
- マネージャー - 技術チーム 5%
- 教授 / 学術 7%
- アーキテクト 5%
- メディア / アナリスト 4%
- DevOps/SRE/ システム管理者 1%
- アプリケーション開発者 (フロントエンド / バックエンド / モバイル / フルスタック) 1%
- システム / 組み込み開発者 1%
- その他 30%



関心領域
- サイバーセキュリティ 12%
- オープンソースのベストプラクティス 9%
- AI、ML、データ分析 9%
- プライバシーとセキュリティ 8%
- クラウド、コンテナ、仮想化 6%
- リーダーシップとコミュニティ 5%
- OSPO 5%
- サプライチェーン 4%
- IoT と組み込み 4%
- セーフティクリティカルシステム 4%
- クロステクノロジー 4%
- ネットワーキングとエッジ 4%
- DevOps、CI/CD、サイト信頼性 3%
- 持続可能性 3%
- 多様性、公平性、包括性 2%
- Linux カーネル 2%
- オープンハードウェア 2%
- システムエンジニアリング 2%
- システム管理 2%
- Web およびアプリケーション開発 2%
- 視覚効果 1%
- セキュリティ 1%

OpenSSF Community Day Korea

2025年11月4日 | ソウル
OPEN SOURCE SUMMIT KOREA併設

OpenSSF Community Day
KOREA

OpenSSF Community Day
KOREA

2025 November 4

ソウル、韓国

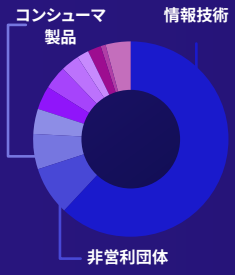
#OpenSSFCommunity

イベント開催報告

207 参加者の登録人数

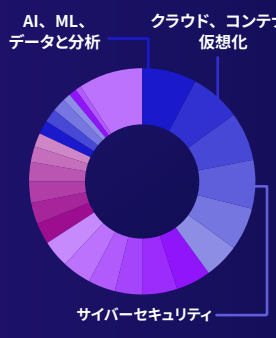
165 組織の総数

28	13	3	2	8	3
CFP提出	スピーカー	ジェンダーマイノリティのスピーカー	POCスピーカー	ブレークアウトセッション	基調講演



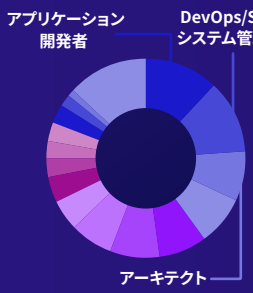
業界

- 情報技術 62%
- 非営利団体 8%
- Consumer Goods 6%
- 自動車 4%
- プロフェッショナルサービス 4%
- 通信 4%
- 金融 3%
- ヘルスケア 2%
- 工業 2%
- エネルギー 1%
- その他 4%



関心領域

- AI、ML、データと分析 8%
- クラウド、コンテナと仮想化 7%
- サイバーセキュリティ 7%
- オープンソースのベストプラクティス 7%
- DevOps、CI/CD、サイト信頼性 6%
- Linux カーネル 5%
- プライバシーとセキュリティ 5%
- Web とアプリケーション開発 5%
- IoT と組み込み 4%
- ネットワーキングとエッジ 4%
- サプライチェーン 4%
- システムエンジニア 4%
- リーダーシップとコミュニティ 3%
- オープンハードウェア 3%
- OSPO 3%
- システム管理 3%
- ブロックチェーンと分散型アイデンティティ 2%
- クロステクノロジー 2%
- 多様性、公平性、包括性 2%
- セーフティクリティカルシステム 2%
- 持続可能性 2%
- ブロックチェーン 1%
- セキュリティ 1%
- 視覚効果 1%
- 無回答 9%



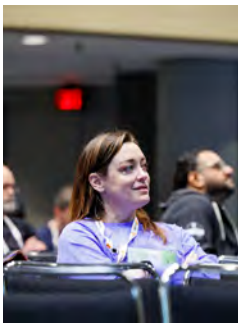
職務内容

- アプリケーション開発者（フロントエンド / バックエンド / モバイル / フルスタック）12%
- DevOps/SRE/ システム管理者 12%
- アーキテクト 8%
- エグゼクティブリーダー 8%
- マネージャ - 技術チーム 8%
- 学生 8%
- カーネル / オペレーティングシステム開発者 7%
- システム / 組み込み開発者 5%
- マーケティング 4%
- 法務 / コンプライアンス 3%
- マネージャー - OSPO 3%
- マネージャー - その他 3%
- 教授 / 学術 3%
- 製品 / ビジネス開発 2%
- メディア / アナリスト 1%
- その他 13%

Open Source SecurityCon North America

2025年11月10日 | アトランタ、KUBECON+CLOUDNATIVECON NORTH AMERICA併設

OPEN SOURCE SecurityCon



OPEN SOURCE SecurityCon

ジョージア州アトランタ

#securitycon

イベント開催報告

152	35	46	38%	40
提出された提案	セッション	スピーカー	女性またはノンバイナリー	代表企業

スポンサーシップ

ダイヤモンドスポンサー

Chainguard　docker　Red Hat

プラチナスポンサー

minimus　SEAL SECURITY

ゴールドスポンサー

DELL Technologies

教育とトレーニング

*これらの数値は2025年11月4日現在のものです。

Developing Secure Software (LFD121)
2025年受講者数：6,127
総受講者数: 27,254

Security for Software Development Managers (LFD125)
2025年受講者数: 372
総受講者数: 3,706

Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)
2025年受講者数: 5,571
総受講者数: 5,571

Security Self-Assessments for Open Source Projects (LFEL1005)
2025年受講者数: 705
総受講者数: 1,909

Securing Projects with OpenSSF Scorecard (LFEL1006)
2025年受講者数: 851
総受講者数: 2,186

Automating Supply Chain Security: SBOMs and Signatures (LFEL1007)
2025年受講者数: 922
総受講者数: 3,367

Secure AI/ML-Driven Software Development (LFEL1012)
2025年受講者数: 363
総受講者数: 363

Securing Your Software Supply Chain with Sigstore (LFS182)
2025年受講者数: 597
総受講者数: 1,200

Secure Software Development: Requirements, Design, and Reuse (LFD104x)
2025年受講者数: 1,012
総受講者数: 8,178

Secure Software Development: Implementation (LFD105x)
2025年受講者数: 538
総受講者数: 4,208

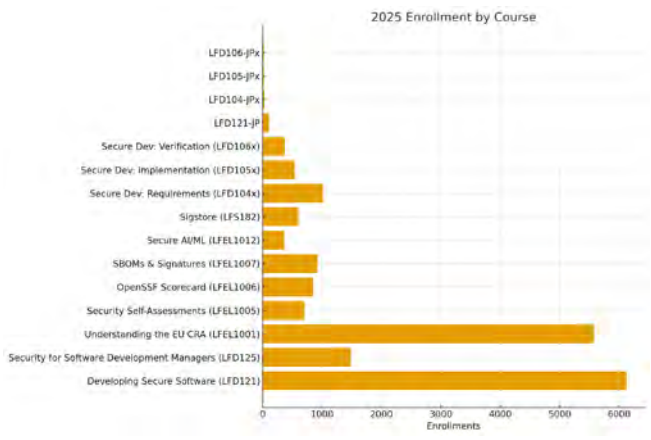
Secure Software Development: Verification and More Specialized Topics (LFD106x)
2025年受講者数: 372
総受講者数: 3,706

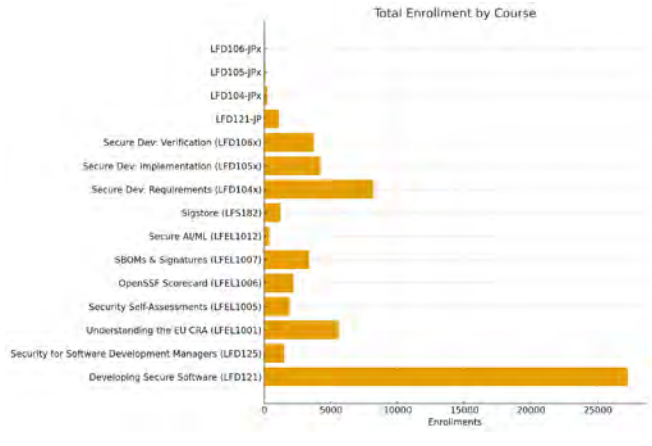
Developing Secure Software - Japanese (LFD121-JP)
2025年受講者数: 108
総受講者数: 1,098

Secure Software Development: Requirements, Design, and Reuse - Japanese (LFD104-JPx)
2025年受講者数: 26
総受講者数: 217

Secure Software Development: Implementation (LFD105-JPx)
2025年受講者数: 21
総受講者数: 92

Secure Software Development: Verification and More Specialized Topics (LFD106-JPx)
2025年受講者数: 21
総受講者数: 54





ポッドキャスト

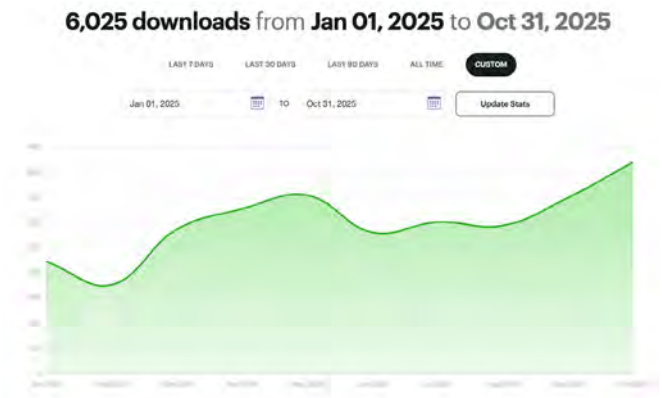
2025年、OpenSSFは「What's in the SOSS?」シーズン2を開始しました。これは**OpenSSFのチーフ セキュリティアーキテクトであるChristopher Robinson（別名「CRob」）**がホストを務める隔週ポッドキャストで、新たに **Microsoftシニア セキュリティ プログラムマネージャーのYesenia Yser氏**を共同ホストとして迎えました。本番組はそのリーチと影響力を拡大し続け、OSSセキュリティの未来を牽引する以下のトピックについて、深く掘り下げた議論をお届けしています。

- **サイバーレジリエンス法**とグローバルポリシーフレームワーク
- **AI/ML セキュリティとMLSecOps**
- 持続可能な管理と**OSSメンテナーの幸福**
- **信頼できる公開**と安全なソフトウェア配信の実践
- **SBOM**、脆弱性開示、サプライチェーン基準
- 重要なオープンソースインフラストラクチャにおけるコミュニティコラボレーション

エピソードでは現在、**メンバーを特集した対話**や**イノベーションの紹介**が定期的に取り上げられ、組織がセキュア開発への投資によって得た実際の成果を共有するプラットフォームを提供しています。

ポッドキャスト配信プラットフォームで累計1万ダウンロードを突破

2025年には6,025件のダウンロード



ダウンロードに最も人気のあるアプリケーション

Apple Podcasts	24%	2,724
Buzzsprout Embed Player	23%	2,640
Spotify	15%	1,708
Antenna Pod	8%	907
Overcast	7%	805

2025年の最も人気のあるエピソード

KUSARI'S MICHAEL LIEBERMAN TALKS GUAC, SLSA AND SECURING THE OPEN SOURCE SUPPLY CHAIN

2025年1月7日公開
309 ダウンロード

RACING AGAINST QUANTUM: THE URGENT MIGRATION TO POST-QUANTUM CRYPTOGRAPHY WITH KEYFACTOR'S CRYPTO EXPERTS

2025年9月9日公開
239 ダウンロード

Cybersecurity Framework Launch

2025年5月20日公開
220 ダウンロード

ブログ

2025年、OpenSSFブログはオープンソース セキュリティに関する洞察の中心的ハブであり続けました。オリジナル記事、ゲスト寄稿、パートナーやメンバー組織からのクロスポストなどが掲載されました。私たちの発信するナリッジ リーダーシップは、AI/MLセキュリティ、SBOM、サプライチェーンの完全性から、グローバルなポリシー エンゲージメントやコミュニティイベントまで、幅広いトピックを網羅しました。これらのストーリー記事は、OpenSSFコミュニティを特徴づける幅広いコラボレーション、技術革新、そして知識の共有学習を反映しています。

1. SBOMs in the Era of the CRA: Toward a Unified and Actionable Framework
2. A New Course on Secure AI/ML-Driven Software Development
3. Announcing the Sigstore Transparency Log Research Dataset
4. OpenSSF Scorecard Audit is Complete!
5. Building Security in Open Source for Financial Services: OpenSSF at Open Source in Finance Forum (OSFF)
6. KubeCon + CloudNativeCon North America 2025 Co-Located Event Deep Dive: Open Source SecurityCon
7. Recap: OpenSSF Tech Talk on Securing the AI Lifecycle
8. Open Infrastructure is Not Free: A Joint Statement on Sustainable Stewardship
9. From Beginner to Builder: Your First Code Contribution
10. From Ghent to Brussels: OpenSSF's Week of Policy and Security in Europe
11. Improving Risk Management Decisions with SBOM Data: A New Whitepaper from the OpenSSF SBOM Everywhere SIG
12. New OpenSSF Guidance on AI Code Assistant Instructions
13. Celebrating the Community: OpenSSF at Open Source Summit and OpenSSF Community Day Europe Recap
14. Open Source Friday with OpenSSF – Global Cyber Policy Working Group
15. Recap: OpenSSF Community Day India 2025
16. OpenSSF Community Day Korea 2025 Agenda Live!
17. OpenSSF Celebrates Global Momentum, AI/ML Security Initiatives and Golden Egg Award Winners at Community Day Europe
18. Trustify joins GUAC
19. What Not to Miss at Open Source Summit & OpenSSF Community Day Europe
20. Case Study: How LFX Insights and OSPS Baseline Validated GUAC's Security in Under an Hour
21. OpenSSF at Black Hat USA 2025 & DEF CON 33: AIxCC Highlights, Big Wins, and the Future of Securing Open Source
22. Securing AI: The Next Cybersecurity Battleground
23. From Beginner to Builder: Understanding OpenSSF Community and Working Groups
24. OpenSSF at DEF CON 33: AI Cyber Challenge (AIxCC), MLSecOps, and Securing Critical Infrastructure
25. Visualizing Secure MLOps (MLSecOps): A Practical Guide for Building Robust AI/ML Pipeline Security
26. Celebrating Five Years of OpenSSF: A Journey Through Open Source Security
27. Speaking, Volunteering, Parenting, and Exploring Nature — My Week at OSS Summit NA 2025
28. Case Study: Google Secures Machine Learning Models with sigstore
29. Building India's Open Source Security Community: Join Us in Hyderabad!
30. New: Cyber Resilience Act (CRA) Brief Guide for OSS Developers
31. Recap: OpenSSF Community Day North America 2025

32. Recap: OpenSSF Community Day Japan 2025
33. On-Demand Webinar: Cybersecurity Skills, Simplified
34. OpenSSF at UN Open Source Week 2025: Securing the Supply Chain Through Global Collaboration
35. OpenSSF Welcomes New Members and Presents Golden Egg Award
36. An Introduction to the OpenSSF Model Signing (OMS) Specification: Model Signing for Secure and Trusted AI Supply Chains
37. Member Spotlight: Datadog – Powering Open Source Security with Tools, Standards, and Community Leadership
38. OpenBao Joins the OpenSSF to Advance Secure Secrets Management in Open Source
39. Tech Talk Recap | CRA-Ready: How Open Source Projects Can Prepare for the EU Cyber Resilience Act
40. Case Study: OSTIF Improves Security Posture of Critical Open Source Projects Through OpenSSF Membership
41. GUAC 1.0 is Now Available
42. Maintainers' Guide: Securing CI/CD Pipelines After the tj-actions and reviewdog Supply Chain Attacks
43. From Sandbox to Incubating: gittuf's Next Step in Open Source Security
44. Choosing an SBOM Generation Tool
45. OSS and the CRA: am I a Manufacturer or a Steward?
46. Member Spotlight: Trail of Bits – Driving Open Source Security Through Standards, Prototypes, and Policy
47. Call for Proposals Now Open for Open Source SecurityCon 2025
48. Case Study: Ericsson's C/C++ Compiler Options Hardening Guide and OpenSSF Collaboration
49. Call for Proposals for OpenSSF Community Day Europe Open Through 26 May, 2025
50. Announcing the Summer 2025 OpenSSF Mentorship Program
51. New Guide on Simplifying Software Component Updates
52. OpenSSF Tech Talk Recap: Using the OSPS Baseline to Navigate Standards and Regulations
53. Recognizing Academic Excellence in Open Source and Secure Software Education
54. OpenSSF Launches Free Course to Prepare Developers for the EU Cyber Resilience Act
55. Announcing the Release of "The Memory Safety Continuum"
56. Repository Service for The Update Framework (RSTUF) Reaches New Security Milestone with Successful Audit
57. Vulnerability Enumeration Conundrum – an Open Source Perspective on CVE and CWE
58. NEW FREE COURSE: Understanding the EU Cyber Resilience Act (CRA) (LFEL1001)
59. Key Takeaways from VulnCon 2025: Insights from the OpenSSF Community
60. Tech Talk Preview: Strengthening Open Source Through Security Standards and Global Policy
61. OpenSSF Community Day NA 2025 Agenda Live!
62. Launch of Model Signing v1.0: OpenSSF AI/ML Working Group Secures the Machine Learning Supply Chain
63. GuardDog: Strengthening Open Source Security Against Supply Chain Attacks
64. Beyond the Software Bill of Materials (SBOM): Ensuring Integrity with Attestations – Event Recap
65. What will my business need to do for the EU CRA?
66. Linux Foundation Research Reports Reveal Wide Spectrum for Cyber Resilience Act Readiness and

Compliance

67. CNCF & OpenSSF Announce Open Source SecurityCon 2025
68. OpenSSF Policy Summit DC 2025 Recap
69. OpenSSF Hosts 2025 Policy Summit in Washington, D.C. to Tackle Open Source Security Challenges
70. NEW FREE COURSE: Security for Software Development Managers (LFD125)
71. 2025 OpenSSF Content Themes: Strengthening Open Source Security Throughout the Year
72. FOSDEM 2025: OpenSSF Community Wrap Up
73. OpenSSF Announces Initial Release of the Open Source Project Security Baseline
74. Does the EU CRA affect my business?
75. Securing Public Sector Supply Chains is a Team Sport
76. Linux Foundation Europe and OpenSSF Launch Initiative to Prepare Maintainers, Manufacturers, and Open Source Stewards for Global Cybersecurity Legislation
77. Alpha-Omega 2024 Annual Report
78. OpenSSF Community Day NA 2025: Call for Proposals Now Open!
79. Predictions for Open Source Security in 2025: AI, State Actors, and Supply Chains
80. Accelerating OpenSSF Adoption: Unlocking Scorecard Insights with a Centralized Dashboard
81. SOSS Community Day India 2024: Wrap Up
82. CRA Stewards and Manufacturers Workshop: Key Takeaways and Next Steps
83. Staying OSS Safe During the Holidays
84. SigstoreCon 2024: Advancing Software Supply Chain Security
85. Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 1
86. Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 2
87. In the Face of Mounting Regulatory Oversight, Honda and Guidewire Join Industry Leaders Securing Software Development at the Open Source Security Foundation (OpenSSF)
88. The OpenSSF 2024 Annual Report Is Live!
89. Open Source Usage Trends and Security Challenges Revealed in New Study
90. Shaping the Future of Generative AI: A Focus on Security
91. The OpenSSF Armored Goose "Honk": Advancing Open Source Security
92. How We Can Learn from Open Source Software to Address the Challenges of AI
93. Red Hat's Collaboration with the OpenSSF and OSV.dev Yields Results: Red Hat Security Data Now Available in the OSV Format

トップブログ

[Open Infrastructure is Not Free: A Joint Statement on Sustainable Stewardship]

9,383 ビュー

[Predictions for Open Source Security in 2025: AI, State Actors, and Supply Chains]

1,877ビュー

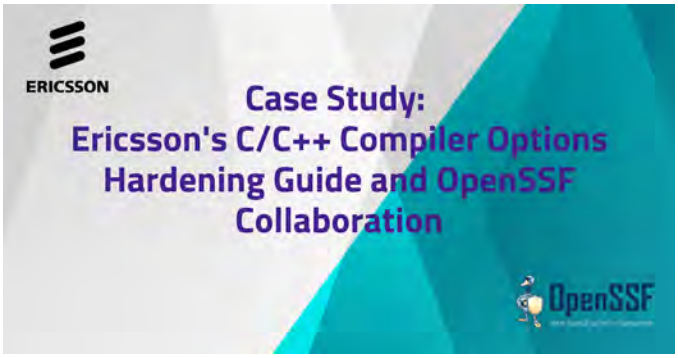
[Launch of Model Signing v1.0: OpenSSF AI/ML Working Group Secures the Machine Learning Supply Chain]

1,496ビュー

ケーススタディ

2025年、OpenSSFメンバーは、オープンソースのセキュリティツールとベストプラクティスがソフトウェアエコシステムをどのように強化するかについて、強調した共同ケーススタディを通じて、実社会への影響を示しました。Ericssonのコンパイラ強化作業、OSTIFのプロジェクト監査、GoogleのSigstoreを利用したセキュア モデル署名、GUACのOSPSベースラインを用いた迅速な検証など、これらの事例は、共同セキュリティイノベーションの具体的なメリットを実証しています。

[Case Study: Ericsson's C/C++ Compiler Options Hardening Guide and OpenSSF Collaboration]



[Case Study: OSTIF Improves Security Posture of Critical Open Source Projects Through OpenSSF Membership]

[Case Study: Google Secures Machine Learning Models with sigstore]

[Case Study: How LFX Insights and OSPS Baseline Validated GUAC's Security in Under an Hour]

テックトーク

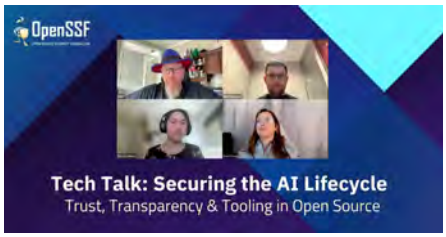
2025年、OpenSSFは教育とコミュニティへのアウトリーチ活動をさらに拡大し、新たなvバーチャル テックトークシリーズを開始しました。これらのセッションは、 オープンソースソフトウェアのセキュリティを強化するOpenSSFのツール、フレームワーク、そして取り組みへの理解を深めることを目的としています。各テックトークでは、プロジェクトのメンテナー、技術貢献者、そしてセキュリティ実務者が一堂に会し、エコシステム全体における実践的な応用とそこから得られた教訓について議論します。

すべてのテックトークの録画は OpenSSF YouTube チャネルでご覧いただけます。プレゼンテーション デッキは、OpenSSF テックトークページからアクセスできます。以下に例をいくつか挙げます。

Simplifying DevSecOps in Air-Gapped Environments with Zarf

2025年11月6日
このセッションでは、エアギャップ環境や半接続環境におけるソフトウェア配信を簡素化する OpenSSFプロジェクトであるZarfが紹介されました。参加者は、Zarfの宣言的パッケージング戦略が、インターネットアクセスがない場合でもKubernetesやクラウドネイティブ ワークロードを安全かつ運用可能な状態を維持する上でどのように役立つか学びました。

Securing the AI Lifecycle: Trust, Transparency & Tooling in Open Source

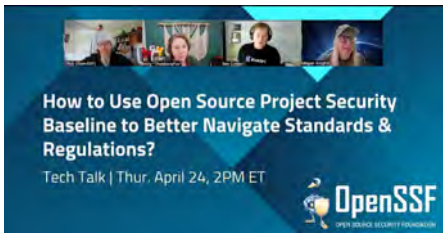


2025年9月24日
この50分間のテックトークでは、オープンソースプロジェクトとそのコントリビューターがAI/MLサプライチェーンへの信頼をどのように構築しているかについて、具体的には、モデル署名、再現性、メタデータ、そしてセキュアな開発手法に焦点が当てられました。議論では、オープンなコラボレーションが責任ある透明性の高いAIをいかに支えているかが強調されました。

CRA-Ready: How to Prepare Your Open Source Project for EU Cybersecurity Regulations

2025年6月12日
今年初め、EUサイバーレジリエンス法（CRA）の施行が迫る中、このセッションでは、オープンソースプロジェクトが新たなサイバーセキュリティ要件に積極的に対応していく方法について参加者に 解説しました。講演者は、コンプライアンスを維持し、早期にレジリエンスを構築するためのベストプラクティスとリソースを共有しました。

How to Use the Open Source Project Security Baseline to Better Navigate Standards & Regulations

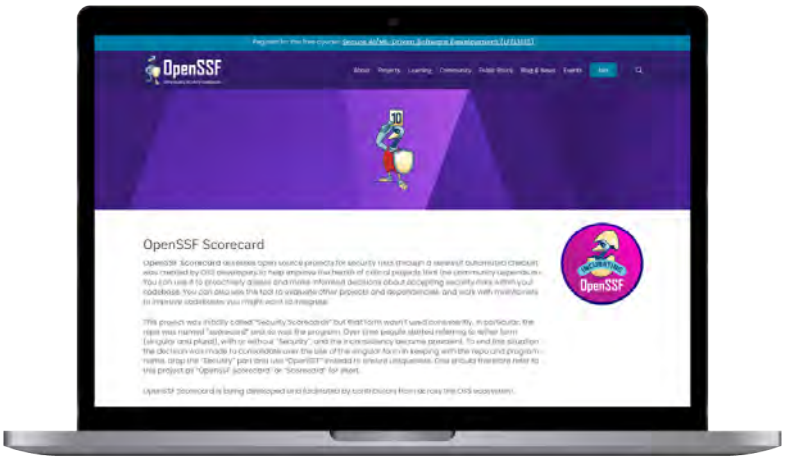


2025年4月24日
このテックトークでは、Open Source Project Security Baseline (OSPS Baseline)を適用して、プロジェクトのセキュリティ体制を強化し、新たな標準へのコンプライアンスを容易にする方法を実演しました。参加者は、このベースラインをワークフローに統合することで、より安全で持続可能なオープンソース開発を支えるために、このベースラインを自らのワークフローに統合するための実践的な洞察を得ました。

ソーシャルメディアとウェブサイトの指標

***これらの数字は2025年10月31日現在のものです。**

Webサイト



360,536 PAGE VIEWS
(Sources) (20% YoY Growth)

Top 3 pages of the year and numbers	
OpenSSF Scorecard	14,113
OpenSSF Education	11,828
Open Infrastructure is Not Free: A Joint Statement on Sustainable Stewardship Blog	9,175

ニュースレター

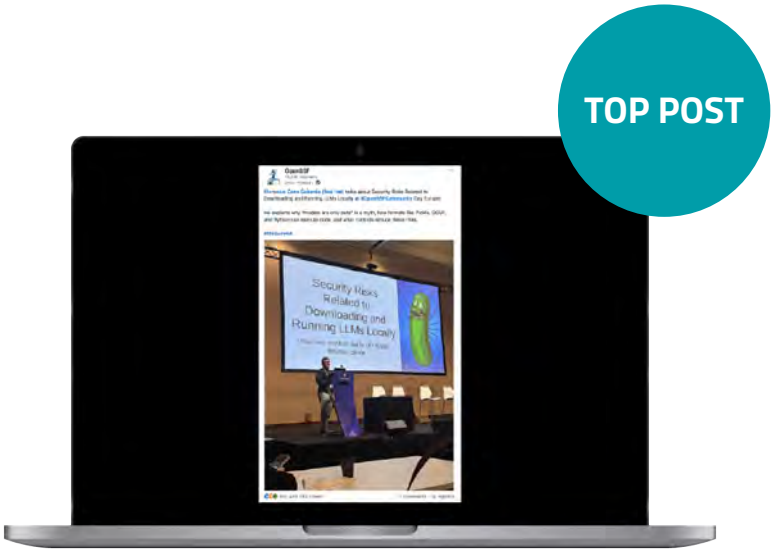
11,453
購読者

39.33%
平均開封率

7.15 %
平均クリック
スルー率

47,007
総閲覧数

LinkedIn



トップポスト: LLMのダウンロードと実行に関連するセキュリティリスク ヨーロッパの#OpenSSFCommunity Day Europeで現地開催

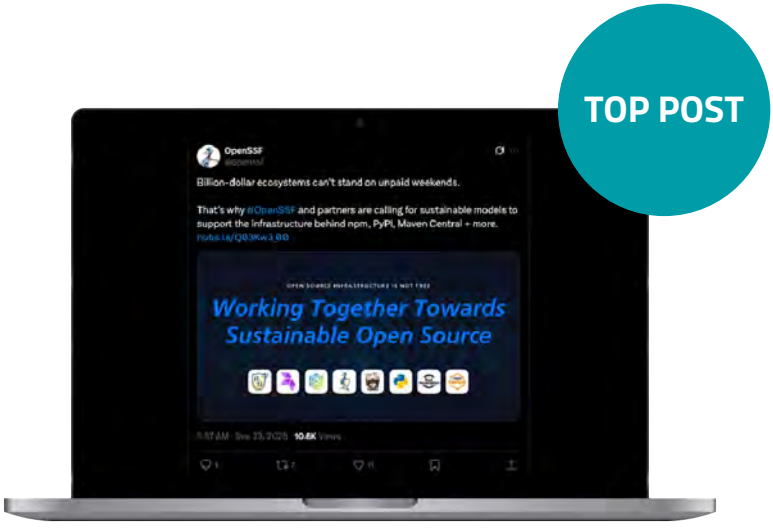
フォロワー数**12,212人**
(前年比44.4%増)

365 件の投稿

575,779 インプレッション

エンゲージメント率**6.2%**

X

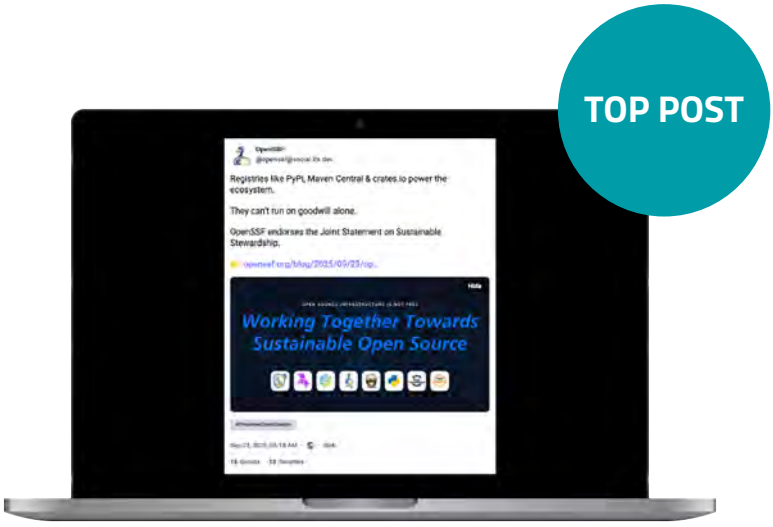


フォロワー数**5,705人**
(前年比2.4%増)

336件の投稿

1,482件のインタラクション

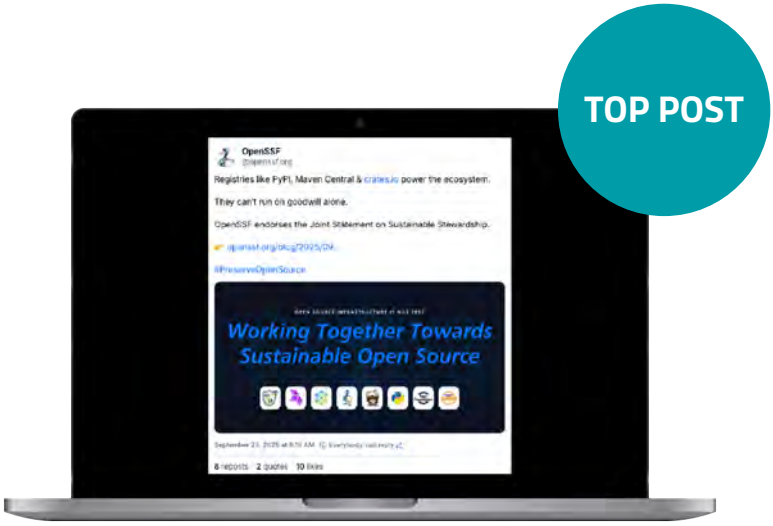
Mastodon



フォロワー数**1,200人**
(前年比 34.08% 増加)

397件の投稿

Bluesky



フォロワー数**1,783人**

218 件の投稿

YouTube

YOUTUBEチャンネルの総視聴回数
97,563

最も視聴された動画 374 回視聴
OpenSSF Tech Talk: How to use the OSPS Baseline to Better Navigate Standards and Regulations

1,940 人の購読者
（前年比44.78%増）

244 VIDEOS

GitHub

212 件の解決した問題
81 レポ
24 のプロジェクト
88 チーム
149 人
472 人のアクティブなコントリビューター
200 のアクティブな組織
1146 件のプルリクエスト

Slack

4,865 ユーザー

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2026年に向けて

2025 年は OpenSSF にとって重要な一年でした。活動が5 年という節目を迎え、グローバルな協調、そして成熟度の向上など成果が実感できた年でした。

とりわけ 2025 年の主要な成果としてTechnical Initiative（TI）資金による具体的なインパクトが挙げられます。Technical Advisory Council は 14 件のイニシアチブに対して合計 66 万ドル以上を提供しました。これらの投資により、サプライチェーンの完全性が強化され、Sigstore のような透明性ツールの高度化、Model Signing などの新たな仕様の支援、そしてAlpha-Omega を通じたコミュニティ主導のセキュリティ監査が可能となりました。

2026 年に向けて、OpenSSF は次の 3 つの核となる目標に注力します。

1. 導入の拡大と成果の測定

私たちは、OpenSSF のツール、フレームワーク、トレーニングの活用範囲と相互運用性をさらに広げ、日々の開発の中にセキュリティを組み込み、その取り組みがエコシステム全体にどのような成果をもたらしているかを把握していきます。

2. 技術投資の強化

私たちは、TI（Technical Initiative）資金モデルを今後も拡充・発展させ、イノベーションをさらに加速し、ファウンデーション間の連携を広げ、そして世界中で最も広く使われているソフトウェアを支えているメンテナーを支援していきます。

3. グローバルな連携と準備の推進

政府機関、標準化団体、コミュニティパートナーとの継続的な連携を通じて、EU サイバー・レジリエンス法（CRA）をはじめとする新たなサイバーセキュリティ フレームワークがオープンソースとうまく調和して機能するよう取り組んでいきます。

今後の取り組みには、OpenSSF 創設当初から大切にしてきた透明性、創造性、そして役割を分かち合う姿勢が引き続き求められます。私たちはメンバー、コントリビューター、パートナーとともに、世界を支えるソフトウェアの信頼性と強靭性をさらに高めていきます。

OpenSSF の使命は変わりません。世界中のすべての人が、安心してオープンソースを利用できるようにすることです。

参加するには

- **ワーキンググループに参加する**：進行中のセキュリティ関連の取り組みに貢献しましょう。こちらからご参加ください。
- **メンバーシップを検討する**: OpenSSFのメンバーになり、オープンソースセキュリティの未来を形作りましょう。**メンバーシップの詳細をご覧ください。**
- **ソーシャルメディアでフォローする**: LinkedIn、X、Bluesky、Mastodon、Youtubeで我々をフォローして最新情報を入手しましょう。
- **ニュースレターを購読する**：最新情報をメールで直接お届けします。こちらからご購読ください。
- **周囲の人へOpenSSFへの 参加を促す** :私たちの目標は大きく、そして欠かせないものです。多くの方に共感いただける内容だと私たちは信じています。一緒に未来をより良い方向へ動かしていきましょう。

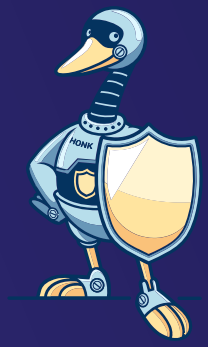
謝辞

OpenSSF 2025アニュアルレポートは、コミュニティ全体による真にグローバルな取り組みの成果です。**ワーキンググループやプロジェクトリーダー、Technical Advisory Council、Governing Board**の皆様のリーダーシップ、卓越した技術力、そしてオープンソース ソフトウェア エコシステムを守る継続的な貢献に心から感謝申し上げます。

また、40 か国以上にわたる**メンバーやコントリビューターの皆さま**にも特別な謝意を表します。本レポートで紹介した数々の成果は、皆さま一人ひとりの献身によって支えられています。

また、これらの成果を形にするうえで欠かせない**Marketing Advisory Council、Developer Relations Community**、そして **OpenSSF スタッフの皆さん**の、創造性、調整力、透明性のあるコミュニケーションに感謝いたします。さらに、本レポートの企画・デザイン・制作にあたり連携いただいた **Linux Foundation の Creative Services、Marketing & PR、Program Management、Event チーム**にも深く感謝申し上げます。

最後に、イベントを企画された方、スポンサーとして支えてくださった方、コントリビューターを支援したメンターの皆さん、リソースを作成された方、そして今年 OpenSSF のミッションを後押ししてくださったすべての皆さんに感謝いたします。皆さん一人ひとりの取り組みが、私たち全員にとって欠かせないオープンソースのセキュリティ向上につながっています。ここにまとめた成果は、すべて皆さんのものです。



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

安全で強靭なオープンソースのエコシステムを共に築いていきましょう。今すぐOpenSSF に参加して、2026 年をこれまでで最も大きな成果の年にする取り組みに力をお貸しください!

openssf.org/getinvolved

この資料は、OpenSSF 発行の「2025 OpenSSF Annual Report」を、OpenSSF Japan Chapter の有志メンバーで日本語に翻訳したものです。

日本語版翻訳協力：OpenSSF Japan Chapter 翻訳チーム

- 清海 佑太（本田技研工業）
- 川名 のん（日立製作所）
- 下沢 拓（日立製作所）
- 余保 東（ルネサスエレクトロニクス）
- 池田 宗広（サイバートラスト）

openssf.org