OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024 アニュアル レポート

openssf.org

目次

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

数字で見る2024

OpenSSFプロジェクト全体で
2,239の
技術コントリビューター
8つのワーキング グループ　37個の技術的な取り組み

15の地域と19の独創的な業界から
126のメンバーが参加し、ゼネラル
メンバー数を10%増やすという
私たちの目標を上回り、
現在の増加率は15%です。

OpenSSFベスト プラクティス バッジには7,680の参加プロジェクトがあり、少なくとも1,544のプロジェクトがバッジを獲得しています。

OpenSSFは、開発者のセキュアなソフトウェア開発を支援します

今年、8,200人以上が
LFD121に登録しており、
累計登録者数は20,000人を
超えています。

(LF104xと日本語翻訳版も含めると、
登録者数は28,000人を超えています)

22人の常連コントリビューターにより、Sigstoreでは2023年以降コミット数が289.06%増加しました。

62,618の独創的なGitHubプロジェクトがSigstoreを使用してアーティファクトとアテステーションに署名していました。一般公開（GA）後に1億4400万の署名が記録されました。

現在、500以上の様々な組織やユーザー アカウントでインストールされ、42,361のリポジトリを保護しています。

OpenSSF Scorecard：バージョン5.0.0をリリースし、Structured ResultsとMaintainer Annotationsが追加されました。これにより、既存の18のチェックが47のプローブに拡大され、より詳細なカスタマイズが可能になりました。

スコアカード アクションのインストール数は7,600、READMEにOpenSSF Scorecardバッジを表示しているレポジトリ数は3,400に上ります。

悪意のあるパッケージ：悪意のあるパッケージを検索するために、以下を含む約25,000件のデータ ポイントを取得します。

- 15,000 npmパッケージ
- 8,000 pypiパッケージ
- 1,000 rubygems
- 1,000 nugetパッケージ

Alpha-Omega

2024年に25件の助成金総額500万ドルを授与し、創業以来15以上のオープンソースプロジェクトに900万ドル以上を出資

General Manager より

OpenSSFコミュニティの皆様

今年を締めくくるにあたり、OpenSSFコミュニティの素晴らしい功績を称えたいと思います。この1年は、進歩とコラボレーションの年でした。オープンソース ソフトウェアのセキュリティ確保という重要なミッションにコミットしてくださったコミュニティの皆様一人ひとりに、深く感謝いたします。世界中の政府が規制への取り組みを強化する中、私たちの団結した対応こそが、世界中の開発者がソフトウェアのサプライチェーンをセキュアに保つことを可能にするでしょう。

運営委員会、ワーキング グループのメンバー、プロジェクト リーダーたちと協業することで、私たちの取り組みの強さを実感することができました。私たちのイニシアチブは、多様な才能と視点を結集することで、私たちが達成できることを示しています。各コントリビューションは、私たちのコミュニティを豊かにし、私たちの目標を強化します。

今年、私たちのメンバー数は15カ国、126にまで拡大しました。これは、私たちの活動が世界に広がり、影響力を増していることを示しています。セキュアなソフトウェア開発を推進するために、これほど多様な組織が結集していることは、非常に心強いことです。教育分野では、12,000人もの人々が当社のOpenSSFトレーニングコースを受講しており、セキュアなソフトウェア教育に対する需要が高まっています。当社のプロジェクトは14件に増加し、さらに24件の技術イニシアチブが進行中です。コミュニティ全体のコントリビューター数は28%増加しました。そして最も重要なこととして、当社のプロジェクトは、SBOMの作成と移植の複雑さを軽減し (protobom、bomctl)、セキュアな開発を簡単に導入できるツールを提供することで (Minder)、開発者に大きな影響を与えています。7,500を超えるプロジェクトが、Linuxカーネル、Kubernetes、Zephyr、CIP、node.jsなど、当社のベスト プラクティスを採用しています。

チーム内、公共部門のパートナー、コミュニティのメンバーでの会話は、私たちの未来を形成する上で非常に貴重な見識をもたらしました。DARPA（国防高等研究計画局）との「Artificial Intelligence Cybersecurity Challenge (AIxCC)」への参加には特に期待しています。このプロジェクトでは、オープンソース プロジェクトの脆弱性に対処するためのツールを開発しています。

今後についてですが、アメリカには多くのチャンスがあると考えています。私たちの仕事は重要であり、共にオープンソースと世界をよりセキュアにすることができます。来年、共に達成できることを楽しみにしています。

どうぞよろしくお願いいたします。

Todd Moore
Interim General Manager of OpenSSF, SVP of The Linux Foundation Operations

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF について

OpenSSF のミッション

The Open Source Security Foundation (OpenSSF) は、私たちが依存しているオープンソース ソフトウェア（OSS）の開発、メンテナンス、リリース、利用を、持続可能性のある形でよりセキュアなものにすることを目指しています。これには、OpenSSF内外でのコラボレーションの促進、ベスト プラクティスの確立、革新的なソリューションの開発などが含まれます。

OpenSSF のビジョン

OSSはデジタル公共財であり、業界としては、私たちはコミュニティとともにセキュリティ上の懸念に対処する義務があります。私たちは、OSSが広く信頼され、セキュアで信頼性の高いものとなる未来を思い描いています。OSSのすべてのスキルレベルのプロデューサーは、負担の少ないツールの自動化、教育、明確で実行可能なガイダンスを通じて、既存のセキュリティ脅威や新たに発生するセキュリティ脅威の両方に、事前及び事後対処することができます。このコラボレーションのビジョンにより、グローバル エコシステムにおける有意義なコントリビューションができます。OSSコミュニティの利点を自信をもって活用し、有意義なコントリビューションができます。

OpenSSF の価値観

OpenSSFは、関連するオープンソース ファウンデーションやプロジェクトの信頼できるパートナーとして、設計によるセキュリティ確保とデフォルトによるセキュリティ確保を推奨する貴重なガイダンスや成果物を提供しています。OpenSSFのイニシアチブは、オープンソースのメンテナーやコントリビューターにとって、セキュリティをより容易なものにするはずです。OSSの利用者は、OpenSSFのアウトプットを活用することで、OSSコンテンツのセキュリティ プロファイルをよりよく理解するための明確で一貫性があり信頼できるシグナルを得ることができます。

OpenSSFは、ファウンデーションと技術イニシアチブ(TIs)に、関心のあるすべての関係者の参加を促すことにコミットしています。OpenSSFは、相互に有益な外部取り組みの有力な支持者であり、方針決定者の教育者として認識されています。

多様性、公平性、受容（DEI）グループへの支援にとどまらず、OpenSSFは、あらゆる視点、あらゆる背景、そしてグローバルな指導と教育の公平な機会を直接的に促進する環境づくりに引き続きコミットしています。OpenSSFは、より包括的で多様なソフトウェア セキュリティ教育を実現するための取り組みを継続的に進化させることに引き続きコミットしています。OpenSSFは、関係者がOpenSSF TIsから価値を受け取るためのオープンで透過的な機会を提供します。

OpenSSF の戦略

OpenSSFの戦略は、セキュアな開発を容易にするツールやプロセスの開発、ベスト プラクティスのより深い理解の促進、革新的な技術イニシアチブへのサポートの提供を通じて、OSSのセキュリティを拡張することを目的とした一連の目標です。憲章はOpenSSFの真実を語る資料であり、この戦略は憲章に基づいています。目標は、一貫性、完全性、およびリスク評価を確保し、OSSエコシステムの全体的なセキュリティを強化するツールとプロセスに焦点を当てています。

この焦点は、OSSのセキュリティ技術イニシアチブを加速させるツール、プロセス、教材の開発を行うことでコミュニティをサポートしています。これらの目標を達成することで、OSSのすべてのスキルレベルのメンテナーやコントリビューターは、既存のセキュリティ脅威や新たに発生するセキュリティ脅威に、事前及び事後対処できるようになります。

OpenSSFの戦略は、3つの主要分野で構成されています。

- **変化の引き金：** OpenSSFは、オープンソース ソフトウェアのプロデューサーと協力し、「セキュア バイ デザイン/デフォルト」の改善を促す引き金としての役割を果たしています。技術的な取り組みを推進し、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ために、セキュリティ基盤の導入障壁を取り除く統合ツールを作成します。
- **現代の開発者の教育とエンパワメント：** 現在および将来のOSS 開発者が、十分なセキュアな開発スキルを習得し、維持できるようにするためのベストプラクティス ガイドおよび教材を作成し、維持します。OSSの利用者は、サプライチェーンで取得したオープンソースコンテンツのセキュリティ状況をよりよく理解するために、明確で一貫性があり、統合が容易な信頼性の高いシグナルを活用することができます。
- **エコシステム リーダー：** 影響力のある提唱者となり、パートナー、OSSコミュニティ、セキュリティ専門家、業界とコラボレートするための思想的リーダーシップのフォーラムを提供します。オープンソース ソフトウェアのセキュリティとサプライチェーンにとって重要な事項の関係者です。OSSのセキュリティに影響を与えるスタンダード、フレームワーク、パブリックポリシーに積極的に参画します。必要に応じて政府、業界団体、その他の関連組織とオープンソース ソフトウェアのセキュリティに関する高度な技術的側面について協力します。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024 年メンバー数の増加とエンゲージメント

OpenSSF は、コミュニティの関与と戦略的イニシアチブを通じて、オープンソース ソフトウェアのセキュリティと回復力を強化することに専念しています。メンバーは、OpenSSF の技術イニシアチブやプロジェクトに積極的にコントリビュートし、オープンソースのセキュリティをコラボレートしながら向上させています。

2024 年には、OpenSSF のメンバー数は大幅に増加し、ゼネラル メンバー数を 10% 増加させるという当初の目標を上回る 15% の増加となりました。また、ヨーロッパでも順調に前進しており、地域メンバー数を 20% 増やすという目標の 82% を達成しています。主な新加入メンバー：

プレミア メンバー

DATADOG

ゼネラル メンバー

ADALOGICS　arm　BOEING　chainloop

Defense Unicorns　embraceableAI　FUJITSU　KEYFACTOR

RESEARCH　GUIDEWIRE　Hedera　herodevs

アソシエイト メンバー

Trifecta Tech Foundation

HONDA The Power of Dreams　PROTECT AI　SIGHUP　StepSecurity

OpenSSF の 現在のメンバーのカテゴリー別リスト は、メンバーレベル（プレミア メンバー、ゼネラル メンバー、アソシエイト メンバー）別に分類されています。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

メンバーリスト

プレミア メンバー

aws, Apple, Capital One, cisco, citi, 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, Airbyte, aiven, Akamai, Alibaba, ANACONDA, apiiro, arm, ATLASSIAN, AURISTOR, BLOCK, Bloomberg Engineering, BOEING, boost security.io, Chainguard, chainloop, Checkmarx, cloudsmith, code intelligence, CodeThink, COMCAST, controlplane, cybertrust, cybozu, cycode, Defense Unicorns, DeployHub, DTCC, docker, embraceableAI, ENDOR LABS, ensignia, f5, Fidelity, FOSSA, FUJITSU, FUTUREWEI, GitLab, Goldman Sachs, GUIDEWIRE, hackerone, Hedera, herodevs, HITACHI, HONDA The Power of Dreams, JFrog, KASTEN by Veeam, KEYFACTOR, kusari, LEGIT SECURITY, LOCKHEED MARTIN, mend.io, NUTANIX, OSCHINA, patchstack, PROTECT AI, RENESAS, REVERSING LABS, RTX, salesforce, SAP, Scotiabank, SHESHASH, shopify, SIGHUP, SlimAI, snyk, Socket, SPARKFABRIK, Spotify, stacklok, StepSecurity, sysdig, TII Technology Innovation Institute, tenable, TESTIFYSEC, TIDELIFT, timesys, TRAIL OF BITS, RESEARCH, VicOne, vmware by Broadcom, WNDRVR, AMD XILINX, ZTE

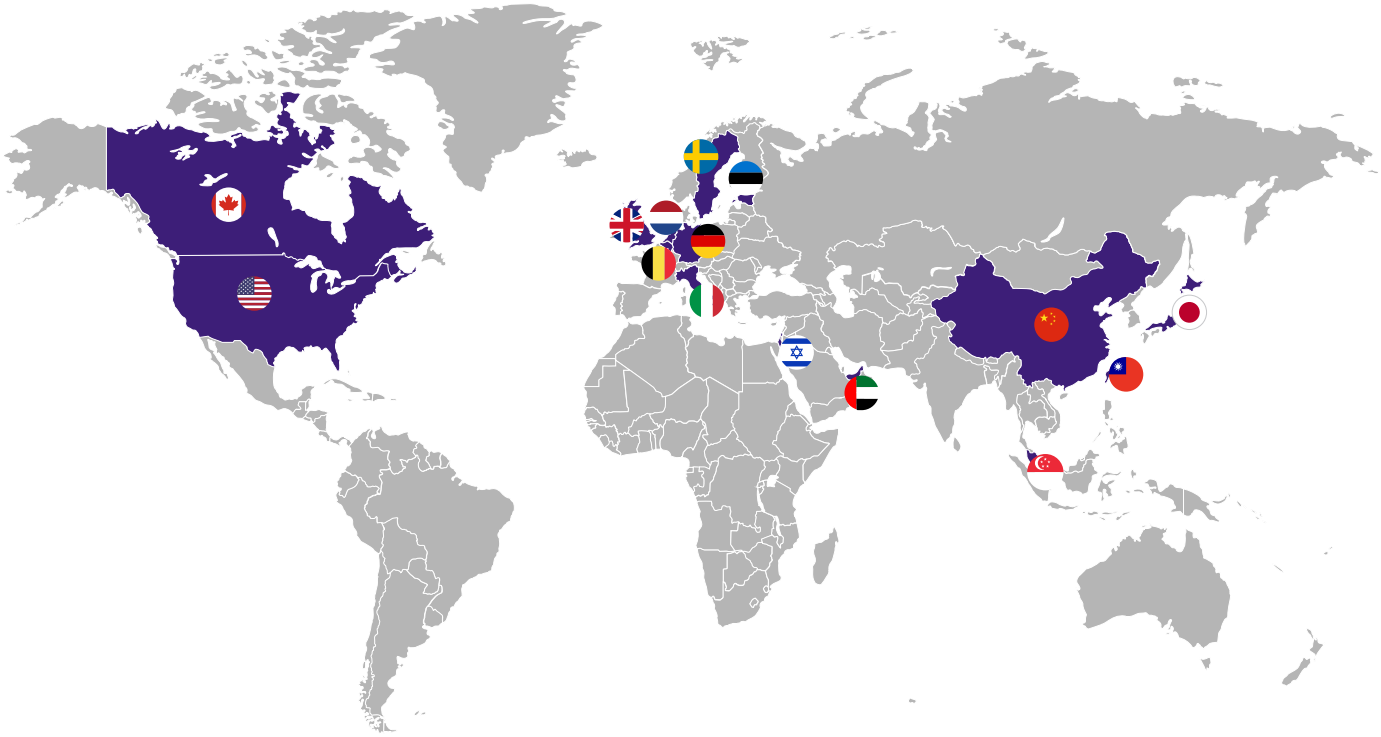
アソシエイト メンバー

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

今すぐ OpenSSF に参加しよう

OpenSSF の公式メンバーになって、主要なセキュリティ イニシアチブを活用し、影響を与え、サポートしましょう。参加するには登録ページにアクセスしてください : [OpenSSF メンバーの登録]

メンバーの地理分布



メンバーの業界

Governing Board Members

ARUN GUPTA (2024 BOARD CHAIR)
Vice President and General Manager, Open Ecosystem Initiatives, Intel Corporation

BRIAN FOX
CTO, Sonatype

ZACH STEINDLER
Acting OpenSSF TAC Chair & Principal Engineer, GitHub

CHRISTOPHER "CROB" ROBINSON
Former OpenSSF TAC Chair & Chief Security Architect, OpenSSF

DAVID DESANTO
Chief Product Officer, GitLab (General Mem Rep)

DECLAN O'DONOVAN
VP, Security Architecture, IAM and Application Security, Morgan Stanley

EMILIO ESCOBAR
Chief Information Security Officer, Datadog

ERIC BREWER
VP of Infrastructure & Google Fellow, Google

GRAHAM HILL
Managing Director, Cybersecurity & Technology Controls, JPMorgan Chase

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

JAMIE THOMAS
GM, Technology Lifecycle Services, and IBM Enterprise Security Executive

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

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

JONATHAN MEADOWS
Head of Cloud Cyber-security Engineering and Software Supply Chain Security, Citibank

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

KELLY ANN
Cloud Infrastructure Security Engineer, Apple

MARK RUSSINOVICH
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 BENJAMIN
Cyber Chief Technology Officer, Capital One

MIKE HANLEY
Chief Security Officer, GitHub

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

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

STEPHEN AUGUSTUS
Head of Open Source, Cisco

VINCENT DANEN
Vice President of Product Security, Red Hat

Governing Board Chair より

世界の技術インフラは、オープンソース ソフトウェア（OSS）に大きく依存しています。しかし、このエコシステムをセキュアに保つことは複雑な課題です。OpenSSF は、コミュニティ、業界、ガバナンスを統合し、OSS をよりセキュアなものにするという課題に取り組んでいます。

理事会はオープンソースセキュリティの重要な課題に取り組んでいます。

- **依存関係の脆弱性：**多くの組織は、Log4shell で確認されたように、時代遅れまたはセキュアでない依存関係の問題に今も直面しています。OpenSSF の **GUAC** プロジェクトは、開発者および利用者が依存関係と関連リスクを追跡するための視覚的なツールを提供しています。
- **タイポスクワッティングと悪意のあるパッケージ**：攻撃者は、人気パッケージを装った悪意のあるコードをアップロードしてソフトウェア レジストリを標的にすることが多く、データ盗難やマルウェアにつながります。OpenSSF は CISA と提携して**「パッケージ リポジトリ セキュリティの原則**をリリースし、OSV プロジェクトでは、これらの脅威に対抗するために 26,000 以上の悪意のあるパッケージを追跡しています。
- **ソーシャル エンジニアリング攻撃**：XZ Utils バックドア (**CVE-2024-3094**) は、ソーシャル エンジニアリングのリスクを浮き彫りにしました。OpenSSF と OpenJS ファウンデーションは、オープンソース プロジェクトがこのような脅威を防ぐための **注意喚起**を行いました。
- **サプライチェーン攻撃**：これらの攻撃は、相互接続されたソフトウェア システムの脆弱性を悪用します。政府は、サプライチェーンのリスクを管理し、透過性を向上させるために、ソフトウェア部品表（SBOM）の導入を推進しています。 OpenSSF は、**protobom** と **bomctl** プロジェクトの追加により、SBOM の作成と移植性を簡素化しています。
- **規制圧力**：EU サイバー レジリエンス法（CRA）やアメリカのような新たな規制。CRA がサイバーセキュリティを拡張する一方で、その実装は、中小企業、オープンソース コミュニティ、イノベーションに想定外の影響をもたらすでしょう。OpenSSF は、オープンソースをサポートするバランスの取れた実装を確保するために、EU と協力しています。

進歩とコラボレーションの 1 年

資金調達モデル：今年、私たちはリソースの割り当てをよりスムーズにし、OpenSSF プロジェクトの影響力を高めるために、テクニカル イニシアチブのための **新しい資金調達構造**を導入しました。

机上演習 : **北米**、**ヨーロッパ**、**日本**における SOSS Community Days では、架空の脆弱性発生をシミュレーションするハンズオン シミュレーションを開催し、参加者は非常にポジティブなフィードバックを受けました

社会をよくするための OSPO: 私たちは国連と協力し、オープンソース ソフトウェアをクリティカルなデジタル公共財として強調し、そのセキュリティと持続可能性を提唱しました。

AI の採用が拡大するにつれ、AI とオープンソースをよりセキュアにするツールを OpenSSF がさらに開発し、AI を活用してセキュリティを拡張していくことを期待しています。私はオープンソース セキュリティの認知度を高め、コミュニティとつながり、アイデアを交換し、オープンソース セキュリティの限界を押し広げたいと考えています。

OpenSSF のスタッフや他の理事とのパートナーシップは強固であり、ファウンデーションは有望な道を歩んでいます。オープンソース エコシステムの取り組みをよりセキュアなものにするために、**私たちに加わりませんか**。

Arun Gupta

2024 年 OpenSSF Governing Board Chair

Intel 社 Vice President、Developer Programs General Manager

TAC Chair より

技術諮問委員会（TAC）は、よく「ファウンデーションの心臓部」と称されます。理事会の利益を促進する上で重要な役割を果たすとともに、技術メンバーのサポートとモチベーションの向上も図っています。TAC は、アメリカの技術的取り組みを導く原動力となり、団結して主要な課題に取り組むことを支援しています。

2024 年には、当ファウンデーションの技術イニシアチブ（TIs）が、コミュニティにとって顕著な成果を達成しました。TIs とは、ワーキング グループ（WG）、特別関心グループ（SIG）、プロジェクト内の技術的なコラボレーションを指します。このレポートの後半で、当社の TIs の仕様書について詳しく説明しますが、ここではいくつかの主な成果を紹介したいと思います。今年、OpenSSF は 4 つの新しいソフトウェア プロジェクト（Protobom、Bomctl、Zarf、RSTUF、Minder）を採用し、最も重要なプロジェクトのいくつかは、大幅な成長とエコシステムへの影響を示しました。特筆すべきは、Sigstore がフル プロジェクトに移行し、Scorecard が Incubating ステータスに達したことです。また、さまざまな技術ガイドやトレーニング教材を共同で発行し、業界全体でオープンソース ソフトウェアのセキュリティ対策を向上させるために協力してきました。

TAC は今年、選出および任命されたメンバーの多様な組み合わせにより、9 席に拡大されました。私たちのコミュニティをサポートするプロセスを合理化し、簡素化するために多くの作業が行われてきました。私たちは、TIs のサポートと資金調達に向けた取り組みを首尾よく立ち上げ、これにより、メンバーは私たちのミッションを推進する力を得ることができました。私は、TAC の同僚たちが示したコミットメントと努力を誇りに思います。彼らの努力が、アメリカの技術的ビジョン達成とコミュニティへの貢献につながりました。

本レポートでは、当社の TIs が成し遂げた素晴らしい業績についてお読みいただけます。どうぞお楽しみください。メンテナーが活用できるよりシンプルなセキュリティ ソリューションを提供し、同時に、日々の業務やプロジェクトで使用するオープンソース ソフトウェアを評価する際に、末端の利用者に対してシグナルを発信する、私たちの取り組みに、ぜひご賛同いただき、ご参加いただければ幸いです。より良い世界を実現するために、日々私たちをサポートしてくださるコミュニティの皆様、ボランティアの皆様、エコシステム パートナーの皆様に心より感謝申し上げます。

Christopher “CRob” Robinson
2023 年、2024 年 TAC Chair
OpenSSF

Technical Advisory Council Members

TAC は、コミュニティを導くためにボランティアで参加する 9 人のメンバーで構成されています。これは、地域社会で選出された個人と理事会が任命した人物の集まりです。TAC は、ファウンデーションの「業務」である運営委員会と技術イニシアチブの間に位置し、両者と調整を図ります。

TAC メンバーは 2 年任期で、OpenSSF のワーキング グループ、SIG、プロジェクトに直接関与します。

ARNAUD LE HORS
OpenSSF TAC Vice Chair & Senior Technical Staff Member - Open Technologies, IBM

BOB CALLAWAY
Tech Lead & Manager, Google Open Source Security Team

CHRISTOPHER "CROB" ROBINSON
Former OpenSSF TAC Chair & Chief Security Architect, OpenSSF

DAN APPELQUIST
Open Source Strategist, Samsung

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

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari

MARCELA MELARA
Research Scientist, Intel Labs

SARAH EVANS
Security Research Technologist, Dell Technologies

ZACH STEINDLER
Acting OpenSSF TAC Chair & Principal Engineer, GitHub

OpenSSF Staff

TODD MOORE
Interim General Manager of OpenSSF, SVP of The Linux Foundation Operations

ADRIANNE MARCUM
Chief of Staff

CHRISTOPHER ROBINSON (CROB)
Chief Security Architect

DAVID A. WHEELER
Director, Open Source Supply Chain Security

JEFF DIECKS
Technical Project Manager

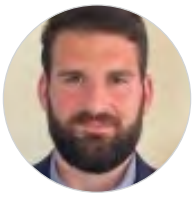
KHAHIL WHITE
Technical Program Manager

CHRISTIAN HORCHERT (FUKAMI)
EU Policy Advisor for OpenSSF

KRIS BORCHERS
Technical Project Manager

OpenSSF Support Staff

ANGELAH LIU
Communications & Marketing Manager



JOHN NIRO
Membership Solutions

NAOMI WASHINGTON
Program Manager

RAM IYENGAR
Community Engagement Lead, India

RANDI ARMOUR
Membership Solutions

REDEN MARTINEZ
Project Coordinator

RIAAN KLEINHANS
Program Manager

SALLY COOPER
Communications & Marketing Manager

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2024年のハイライト

ソフトウェア セキュリティ教育

私たちは、無料コース「Developing Secure Software (LFD121)」と、その edX コースを拡張し、インタラクティブなラボを追加しました。現時点では、主要要素をカバーする 16 のラボ セクションがあり、ウェブ ブラウザーからアクセスできます。ソフトウェアのインストールは不要です。

LFD121 のマーケティングへの取り組みは成功しています。2024 年 11 月中旬の時点で、登録者数は 8,000 人を突破しました。これは、2023 年の総数（6,658 人）を上回るだけでなく、20% 成長という私たちの目標（7,990 人）も上回っています。

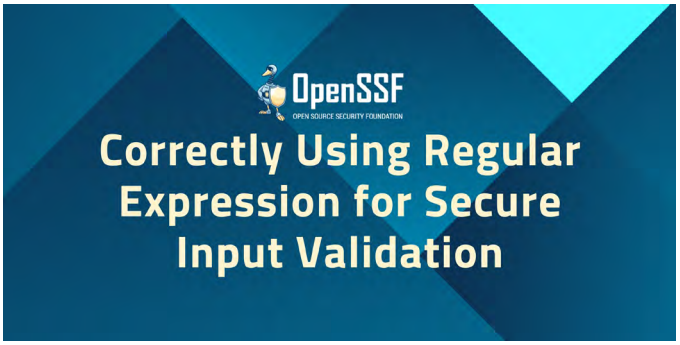
ILF Research とコラボレーションして、OpenSSF は「セキュア ソフトウェア開発教育 2024 年調査」を実施し、貴重な洞察が明らかになりました。注目すべきことに、プロフェッショナルの 53% はセキュアなソフトウェア開発に関するコースを受講したことがなく、44% は優れたコースの認知度が低いことを理由に挙げています。 さらに、経験 1 年以下のソフトウェア開発者の 75% は、セキュアなソフトウェア開発についてよく知りませんでした。

私たちは、ポスト量子暗号や正規表現の適切な使用に関する新しいコンテンツの追加など、LFD121 の改良を続けています。また、2024 年に完成、立ち上げ予定の新しいコース「Security for Software Development」も現在開発中です。

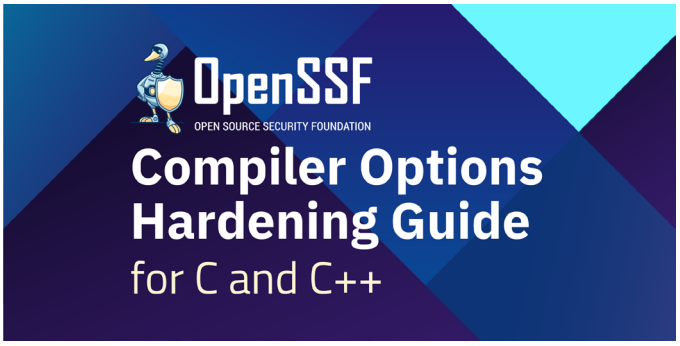
セキュリティ ガイド

- 私たちは Principles for Package Repository Security を策定し、OSS リポジトリと協力してその実装に取り組んでいます。

- 私たちは、よく使用されるものの、誤用されることが多い一般的なセキュリティ メカニズムのための新しいガイド「Correctly Using Regular Expressions for Secure Input Validation」を 開発しました。



- 既存のガイド、例えば「Compiler Options Hardening Guide for C and C++」などを更新しました。



- Python ガイドの草案「Secure Coding One Stop Shop for Python」の作成を開始しました。
- 私たちは、長期間有効なトークンや認証情報への依存を減らすことを目的とした仕様書「Trusted Publishers for All Package Repositories」を開発しました。

OSS インフラストラクチャーとツールの改善

私たちは引き続き、OpenSSF ベスト プラクティス バッジを維持し、法的保護を目的とした LLC を正式に設立し、この種のデータをより適切に扱うために CDLA-Permissive-2.0 ライセンスに移行しました。OpenSSF Scorecard プロジェクトもメンテナンスされ、今年度は Incubating ステータスを獲得しました。さらに、Allstar プロジェクトは、調整を合理化するために OpenSSF Scorecard に統合されました。Sigstore は、その採用と独自の専用カンファレンスの開催の両面で、成長を続ける技術イニシアチブであり続けています。メンテナーは 2025 年もイベントを継続して開催したいと考えています。

公共部門との関わり

2024 年を通して、OpenSSF はアメリカおよびヨーロッパの公共部門とアクティブに関わってきました。以下は、当社の業績の一部です。

アメリカ

OpenSSF は、米国サイバーセキュリティ インフラ保護庁（CISA）が発行した「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software（サイバー セキュリティ リスクのバランスを変える：セキュア バイ デザイン ソフトウェアのための原則とアプローチ）」に関する情報提供依頼（RFI）に 正式な回答 を提出し、CISA Open Source Software (OSS) Security Summit にも参加しました。

OpenSSF は CISA と協力し 、パッケージ リポジトリ セキュリティの原則 の開発と普及に努めました。多くのリポジトリが、その推奨事項の 実装 を開始しています。

OpenSSF は、脆弱性を発見し修正するツールを開発し、オープンソース ソフトウェアとしてリリースする大会である、DARPA の 人工知能サイバーチャレンジ (AIxCC) と ARPA-H をアクティブにサポートしています。私たちは、今後の進め方について助言し、OSS プロジェクトが競合を理解できるよう支援し、OSS が技術移行の強力なサポートとなり得ることを公に説明してきました。

OpenSSF は、CISA および国土安全保障省（DHS）科学技術局（S&T）とコラボレーションし、オープンソースのサプライチェーン ツールである protobom を 立ち上げました。このツールは、ソフトウェア部品表（SBOM）やファイルデータを読み込み、生成するほか、このデータを標準的な業界 SBOM フォーマットに変換することも可能です。

ヨーロッパ

イベントとワークショップ

2024 年 3 月、OpenSSF はブリュッセルで EU 政策サミットを首尾よく開催し、その存在感を強化するとともに、EU 機関および加盟国とサイバー レジリエンス法（CRA）に関するコラボレーションを開始しました。それ以来、OpenSSF はさまざまなイベントに積極的に参加し、欧州のスタンダード化とオープンソースの協力においてブリュッセルの主要なプレーヤーとしての地位を確立しました。さらに、FSFE Youth Hackathon のスポンサーとなったことで、開発者コミュニティの次世代の才能ある人々に OpenSSF を紹介することができました。

コンサルテーション

OpenSSF は、NIS2 実装法に関するパブリック コンサルテーションにコントリビュートし、オープンソースとそのサプライヤーに関する NIS2 と CRA の相違する見解を強調する共同回答にコラボレートし、オープンソース エコシステムへの影響を緩和することを目指しました。このことがきっかけとなり、欧州委員会とのフォロー アップ会議が開催され、今後の CRA 関連業務の洞察が得られました。

OpenSSF と標準化

OpenSSF は、CRA の実装に関する LF の作業に深く関与しています。ブリュッセルで最もアクティブな技術系ファウンデーションのひとつである OpenSSF は、技術的な議論をサポートするために、ツール、ガイダンス、コラボレーションをコントリビュートしています。OpenSSF は LF Research と CRA 準拠でも協力しており、LF Europe と共同で CRA ワークショップの開催を計画しています。

他の関係者とのコラボレーション

ブリュッセルにおける OpenSSF の活動は、主に規制当局の利害関係者を CRA の議論に関与させ、OpenSSF のメンバー、および他のオープンソース グループにはあまり関与していないより幅広い関係者を巻き込むことを目的としています。技術的な専門知識と実用的なコントリビューションで知られる OpenSSF は、CRA の実装を超えた知識共有を促進しています。OpenSSF は、欧州委員会の CRA に関する専門家グループに 170 の組織のひとつとして参加しました。

課題

CRA の取り組みには主に 2 つの課題があります。1 つ目は、実質的な成果を得るために適切な関係者間の協議を調整すること、2 つ目は、ヨーロッパのメンバーと地域社会への働きかけを強化することです。OpenSSF の影響力は拡大していますが、強固なヨーロッパの参加者およびメンバー基盤を構築するには、ターゲットを絞ったメディア戦略およびアウトリーチ戦略が必要です。

OpenSSFのイベント

今年、OpenSSF Community Day program はインドにも拡大し、北アメリカ、ヨーロッパ、日本での年次カンファレンスに加わりました。OpenSSF はブリュッセルで初の European Policy Summit を開催し、米国政策サミットの開催に向けた計画が進行中です。また、今年は独立した OpenSSF イベントとして SOSS Fusion も開催しました。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

ワーキンググループ

ワーキング グループ

AI / ML

このワーキング グループは現在、初期のライフサイクル段階にあり、AI/ML のワークロードにおける
オープンソース ソフトウェアのセキュリティ対応に重点的に取り組んでいます。

GitHub リポジトリ	リーダー	定常コントリビューターの人数
ossf/ai-ml-security	**Jay White, Mihai Maurseac**	**約 10 人**

2024 年のハイライト

- モデル署名のための別プロジェクトを立ち上げ、Sigstore を使用した model signing のプロトタイプを開発しました。安定版リリースは間もなく予定されています。
- AI セキュリティ分野におけるさまざまなワーキング グループとコラボレートし、関係者全員に効果的に情報を発信する取り組みを開始しました。

次に行うこと

- model signing ライブラリの安定したリリースを目指し、Sigstore と独自 PKI ソリューションの両方と互換性があり、複数の ML フレームワークとモデル ハブに統合することを目指しています。
- ML のメタデータを署名に組み込むサポートと、ML のワーク ストリームにおける SLSA の一貫したハッシュ化手法の採用を計画しており、取り組みは来年から開始されます。

ワーキング グループ

オープンソース開発者のためのベスト プラクティス

このグループは、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、それらを学習し適用するためのアクセス可能なリソースを提供しています。

ワーキング グループのリーダー	定常コントリビューターの人数
Christopher Robinson (Former Chair), Co-chair: Avishay Balter, Georg Kunz	20 人

GitHub リポジトリ

ossf/wg-best-practices-os-developers

2024 年のハイライト

- Secure Development Fundamentals Course（LFD121）にラボを追加しました。
- Secure Developer Training と LFD121 コースに関する認知度向上キャンペーンを立ち上げました。
- C/C++ コンパイラーのオプション ガイド、OpenSSF Scorecard、ベスト プラクティス バッジなどのトピックをカバーする多数のカンファレンス講演を実施しました。
- SOSS タスク フォースを通じて教育に従事しました。
- OpenSSF Security Baseline の採用を推進しました。
- W3C とウェブ開発者のためのベスト プラクティスについてコラボレートしました
- Intel 社から「Security for Software Development Managers」コースの寄付を受けました。
- CNCF との学術認定プログラムを開始しました。
- OSS-NA および SOSS-Fusion カンファレンスの前に、OpenSSF Scorecard のコントリビューター向けワークショップを開催しました。
- C/C++ コンパイラーの強化オプション ガイドを拡張しました。
- Ericsson 社から寄贈された新しいプロジェクト「Secure Coding One Stop Shop for Python guidelines」を開始しました。
- 正規表現の正しい使い方に関する新しいガイダンス ドキュメントをリリースしました。
- OpenSSF Scorecard は、Structured Results（probe）と Maintainer Annotations を特徴とする v5 をリリース しました。これは、OpenSSF Incubating プロジェクトとして申請され、OpenSSF Scorecard Monitor である Allstar と、OpenSSF Scorecard API Visualizer が採用されています。

影響

- LFD121 の在籍者数が増加しました。今年、Secure Software Development (LFD121) コースには、2024 年 11 月 27 日時点で 8,415 人以上が登録しており、2024 年の登録者数 7,990 人という私たちのゴールを上回っています。理事会メンバーやその他の人々は、私たちの教材を共有し、彼らの組織にこの無料コースの利用を勧めてくれました。
- メンバーは多くのカンファレンスに参加し、当社の教材やプロジェクトについて講演を行いました。イベントには、OSS-NA、OSS-EU、Blackhat、RSA、VulnCon、FOSDEM、SBOM-o-rama、NordicCON、SOSS Fusion が含まれていました。

次に行うこと

- 開発マネージャー向けのセキュリティ コースを新しく公開します。
- セキュリティ アーキテクチャー コースを開発します。
- OpenSSF ツール（Best Practices Badge, OpenSSF Scorecard, Security Insights, LFX portal）への統合を含む、OpenSSF セキュリティ ベースラインを展開します。
- 「Secure Coding One Stop Shop for Python guidelines」の提供と発表をします。 - Q125。
- Kubecon にて、OpenSSF + CNCF Academic Accreditation program を発表、オープンします。
- OpenSSF セキュリティ ベースラインを公開します（パイロット版 OpenSSF、CNCF、および OpenJS プロジェクトからの採用を含む）。OpenSSF のツールと手法が開発者と利用者がコンプライアンス体制に対応する上で役立つことを示すための、規制コンプライアンス マトリックスを作成します。

ワーキング グループ

多様性、公平性、包括性

このグループは、サイバーセキュリティ人材のリプレゼンテーションを拡大し、その全体的な有効性を高めることを目的としています。

ワーキング グループのリーダー	定常コントリビューターの人数
Marcela Melara, Yesenia Yser, Jay White	約 5 人

GitHub リポジトリ

ossf/wg-dei

2024 年のハイライト

- SOSS Community Day NA '24 でパネル ディスカッションを主催し、OpenSSF コミュニティにおける包括性と公平性の重要性を訴えました。**録画を見る**
- 2024 年 7 月に開始した、毎月開催のコミュニティ オフィス アワーでは、OSS とサイバー セキュリティにおける新規参入者や少数派グループに関連するトピックについて議論する専門家スピーカーを特集しています。
- 9 月のオフィス アワーは、「OSS とサイバーセキュリティにおけるメンターとコミュニティの探し方」に焦点を当てました。**録画を見る**
- 2024 年の全スケジュールはこちらから閲覧可能です。**こちら**。

影響

ワーキング グループはまだ勢いを得ている最中ですが、取り組みはコミュニティの構築とアウトリーチに集中しています。パネル ディスカッションは、OpenSSF コミュニティ全体の認知度向上に役立ちました。通常、オフィス アワーには世界中で 10 ～ 20 人の参加者が集まり、OSS とサイバーセキュリティに関するアドバイスや機会を求めています。

次に行うこと

- OpenSSF コミュニティ メンバーによるキャリアのヒントをブログやソーシャル メディアで紹介する「Tip of the Month」投稿を立ち上げます。
- LFX メンターシップの機会を作り、新規参加者が進行中の OpenSSF プロジェクトに影響ののあるコントリビュートができるよう促します。
- OpenSSF プロジェクトのための、包括的で新規参加者にもやさしいコントリビューション ガイドラインのベストプラクティスを確立します。

ワーキング グループ

クリティカル プロジェクトのセキュリティ確保

このグループは、私たちの信頼にとって不可欠なクリティカルなオープンソースプロジェクトを特定し、リソースを割り当てることに重点を置いています。

ワーキング グループのリーダー	定常コントリビューターの人数
Amir Montazery, Jeff Mendoza	5-10 人

GitHub リポジトリ

ossf/wg-securing-critical-projects

2024 年のハイライト

- クリティカル プロジェクト セットの導入と利用性を高めるため、最小実用セキュリティ要件（MVSR）フレームワークを採用しました。
- クリティカルなプロジェクトを特定するための選択プロセスを提示しました。
- Reversing Labs の Malicious Packages 向けパッケージのフィードを統合しました。
- データの品質とソフトウェア識別に関する問題の改善に取り組みました。
- Criticality Score の構造を拡張し、一貫した実行とカバレッジの向上を実現します。
- 国勢調査第 3 号の調査結果をリリースしました。

影響

- **悪意のあるパッケージ：**約 25,000 件のデータポイントを取得します。
  - » 15,000 npm パッケージ
  - » 8,000 の pypi パッケージ
  - » 1,000 rubygems
  - » 1,000 の nuget パッケージ
- **Criticality Score：毎月のスコア計算は 50 万のプロジェクトを対象としています。**

次に行うこと

- MVSR に基づく戦略とロードマップの開発を継続し、クリティカル プロジェクト セットを拡張します。
- 悪意のあるパッケージ リポジトリの「悪意のある」の定義を明確化します。

ワーキング グループ

セキュアなソフトウェア リポジトリ

このグループは、ソフトウェアのリポジトリを強化し、セキュアにする新しいツールやテクノロジーを紹介するためにコラボレートしています。現在進行中のプロジェクトは、TUF のリポジトリ サービスです。ぜひご参加いただき、詳細をご覧ください!

ワーキング グループのリーダー	定常コントリビューターの人数
Dustin Ingram, Zach Steindler	N/A

GitHub リポジトリ

ossf/wg-securing-software-repos

2024 年のハイライト

- オープンソース パッケージ リポジトリがセキュリティ ロードマップを策定するのを支援するため、米国 CISA と共同で「Principles for Package Repository Security」を発行しました。
- RSTUF で大きな進展がありました。実験的なシステムから、本番環境への展開に適した MVP リリースへと進化し、パッケージ リポジトリ インデックスの保護を目指しています。
- プラットフォーム間のパイプライン構築における機密管理の拡張を目的とした、実装ガイドライン「全てのパッケージ リポジトリにおける信頼された発行者」を公開しました。

影響

- 「Principles of Package Repository Security」というドキュメントに触発され、CISA は Open Source Software Security Summit を開催しました。
- Homebrew のビルドの出所に関する作業は、昨年のグループの提案がきっかけでした。
- RSTUF のプロトタイプは、RubyGems と PyPI と連携して、パッケージ インデックスを保護します。
- NuGet の信頼された発行者仕様は、その基盤として全てのパッケージ リポジトリにおける信頼された発行者として引用されています。
- Crates.io における信頼されたパブリッシング サポートに関する RFC が公開されました。

次に行うこと

- オープンソース パッケージ リポジトリの新興トピックに関する実装ガイドラインの公開を継続します。
- オープンソース コミュニティと関わり、米国公共部門とコラボレートする可能性のあるベスト プラクティスを公開します。
- RSTUF v1.0 をリリースし、RubyGems と PyPI への本番環境の展開を促進します。

ワーキング グループ

セキュリティ ツール

このグループは、オープンソース開発者向けに最高のセキュリティ ツールを提供することに重点を置いており、それらのツールが誰でもアクセスできるようにすることを目指しています。

ワーキング グループのリーダー	定常コントリビューターの人数
Ryan Ware	5-10

GitHub リポジトリ
ossf/wg-security-tooling

2024 年のハイライト

- Protobom は最近、OpenSSF 内のサンドボックス プロジェクトとして承認されました。このフォーマットに依存しないツールは、組織が使用および開発するソフトウェアのソフトウェア部品表（SBOM）のインポートと作成の両方を可能にします。

- bomctl プロジェクトはサンドボックス プロジェクトとして受け入れられました。Protobom は多くのユースケースに効果的に対応しますが、特定のニーズには独自のソリューションが必要です。それを受けて、チームはこれらの要件に対応するために、Protobom エンジンをベースとした bomctl を開発しました。
- SBOM-Everywhere プロジェクトは、SBOM ツールのカタログ作成 と、SBOM の使用開始に役立つベスト プラクティスのドキュメント化に重点的に取り組んでいます。

- 技術諮問委員会（TAC）は、OpenSSF に寄贈されたオープンソース プロジェクトである Minder のサンドボックス アプリケーションを認可しました。Minder は、オープンソース開発者リポジトリのセキュア化を支援することで、OpenSSF ソリューション スイートに追加されます。これには、長期的なセキュリティを確保するためのポリシーの実装も含まれます。
- ファジング コラボレーション グループは、ファジング ソリューションをプロジェクトに統合する方法について、オープンソースのメンテナーに教育を行う取り組みを継続しています。

影響

- OpenSSF の SBOM に関する取り組みは、イノベーションの最前線にあります。SBOM-A-Rama 2024 への参加からもわかるように、メンバーは、メンテナーや組織の SBOM ニーズをサポートできる新たな分野を特定し続けています。これらの取り組みにより、エコシステム全体で SBOM の導入が促進されています。
- ファジングも、開発者が取り組みを始めるのに苦労することが多い分野です。ファジング コラボレーション グループは、OSS-Fuzz のようなファジング ソリューションを導入するオープンソース プロジェクトを支援し続けています。

次に行うこと

- 私たちは、SBOM によって OpenSSF がエコシステムを支援できる分野をさらに広げていきます。さらに、Minder のような SBOM 以外のツールにも焦点を当て、OpenSSF ソリューションのポートフォリオを拡張するとともに、重複する部分については他の OpenSSF ツールとクローズにコラボレートしていきます。

ワーキング グループ

サプライチェーンの統合

このグループは、メンテナー、プロデューサー、ユーザーが、GUAC、SLSA、gittuf などのプロジェクトを含め、自身が使用するコードの由来を理解し、情報に基づいた決定を行うことを支援します。

ワーキング グループのリーダー	定常コントリビューターの人数
Isaac Hepworth, Jay White	25-50 人

GitHub リポジトリ

ossf/wg-supply-chain-integrity

2024 年のハイライト

- **プロジェクトの追加 :** サプライチェーンの完全性に関するワーキング グループに GUAC,、Zarf,、Security Insights を正式に歓迎しました。

- SLSA: 仕様書 v1.1 は最終草案に近づいています。変更には、アップデートされた脅威モデルと VSA の検証手順が含まれます。ソース トラックは草案中です。ハードウェア認証トラックは定義中です。依存関係トラックは S2C2F からブートストラップ中です。

- S2C2F: C コア S2C2F 仕様書の継続的な改良。SLSA の依存関係トラックとコラボレートしています。AI/ML セキュリティ WG と提携し、S2C2F を AI ユースケース（HuggingFace からのモデル利用など）に拡張する新しいワークストリームを開始しました。

- gittuf: 実世界のパイロット版へのアクティブな取り組み、およびアプリ ホスティングのための資金調達を模索中です。

- GUAC: 3 月に OpenSSF に参加し、それ以来、恒久的なデータベースのサポートや明確に定義されたライセンス情報など、15 のアップデートをリリースしました。13 人の新しいコントリビューターを迎え入れ、コントリビューターの階層で 2 つの昇進がありました。

- Zarf: OpenSSF へのオンボーディングと、2024 年第 4 四半期リリースのリリース候補版 1.0 の準備をしました。

影響

- SLSA は、オープンなサプライチェーン セキュリティ フレームワークとして、引き続き注目と認知度を高めています。そのユーティリティと価値を拡張するために、多数の新しいトラックを開発しています。
- GUAC のコントリビューションには、Guidewire からのケース スタディが含まれています。

次に行うこと

- SLSA v1.1 およびソース トラック、ハードウェア認証トラック、依存関係トラック。
- GUAC は 1.0 リリースの実現に向けて作業を進めており、データベースのパフォーマンス チューニングに重点的に取り組んでいます。
- Zarf v1.0 をリリースします。

ワーキング グループ

脆弱性に関する情報公開

このグループは、脆弱性報告とコミュニケーションの改善を通じて、オープンソース エコシステムのセキュリティ全体を拡張することを目的としています。彼らは、VEX ドキュメントの発行、脆弱性レポートの整理と影響内容の伝達という負担を軽減し、VEX フィードを可能にすることで、これらのプロセスを合理化する OSSM メンテナーを支援しています。

ワーキング グループのリーダー	定常コントリビューターの人数
Madison Oliver, Christopher Robinson (Former Chair)	10 人

GitHub リポジトリ

ossf/wg-vulnerability-disclosures

2024 年のハイライト

- TTX（テーブルトップ エクササイズ）用の資料を発行しました。
- OSS-NA と OSS-EU の TTX を実施しました。OSS-JP はまもなく実施予定です。
- SIREN 脅威インテリジェンス メーリングリストをローンチしました。
- OSV と OpenVEX に関するアップデートを提供しました。

影響

- このグループは、2024 VulnCon vulnerability ecosystem conference に多数参加し、カンファレンスでは 40 のセッションで 11 人のメンバーが発表を行い、CVD、オープンソース脆弱性メタデータ、VEX/SBOM に関する議論が行われました。OpenSSF がカンファレンスのスポンサーを務め、その成功に貢献しました。
- LF イベントでの TTX セッションは、サイバーインシデント プロセスのドキュメント化と演習に関するコミュニティの認知度を高めました。
- SIREN メーリングリストは、エコシステムでアクティブに悪用されているセキュリティ問題や脆弱性に関する情報を共有するためのプラットフォームとなっています。
- 今年度の OSV エコシステムの導入：
  - » Ubuntu
  - » Malicious Packages
  - » Mageia
  - » Chainguard + Wolfi
  - » SUSE/openSUSE
  - » Red Hat

次に行うこと

- 2025 年の VulnCon の論文募集は 10 月中旬にオープンします。
- オープンソース利用者向けの協調的脆弱性開示ガイドの作成と公開します。
- CVE および CNA プログラムにおけるエコシステムと継続的にコラボレーションします。
- SBoM と VEX におけるエコシステムと継続的にコラボレーションします。
- 机上演習（TTX）資料および、カンファレンス演習の更に拡大します。

プロジェクト

Sigstore

ワーキング グループのリーダー	定常コントリビューターの人数
TSC (Bob Callaway, Luke Hinds, Trevor Rosen, Santiago Torres-Arias, Priya Wadhwa), Community Chair (Hayden Blauzvern)	22 人

GitHub リポジトリ
sigstore

2024 年のハイライト

- Sigstore は OpenSSF 内のプロジェクトとしては正式に卒業し、ソフトウェアの作成とディストリビューションの信頼性を拡張する、その成熟と採用における重要なマイルストーンを達成しました。
- 11 月に開催された SigstoreCon は、Kubecon と同時開催され、サプライチェーン セキュリティ コミュニティを統合し、Sigstore と関連 SSCI プロジェクトについて議論しました。
- アクティブな開発には、sigstore-python、sigstore-java、sigstore-go、sigstore-ruby のメジャー リリースと、ML モデル署名のためのモデル透過性の導入が含まれます。

影響

- Sigstore は、複数のパッケージ エコシステムで広く採用されています。以下はその例です。
  - » npm による採用。Sigstore 署名付き SLSA の証明をサポート。
  - » GitHub Artifact Attestations は、ワークフロー実行時の署名付き証明書として Sigstore を利用しています。
  - » Homebrew では、homebrew-core 内のすべてのボトルについて Sigstore 署名付きの証明書を作成し、Alpha-Omega の資金提供を元に、brew インストール でそれらを検証しています。
  - » PEP 740 は、Sigstore 署名付き証明書のインデックス サポートのために PyPI によって承認され、導入されました。
  - » Maven Central は、Sigstore 署名バンドルをサポートします。
  - » PEP 761 は、CPython リリースにおける PGP 署名を廃止し、Sigstore 署名を推奨します。

次に行うこと

- OSS パッケージ マネージャーを Sigstore 導入の主要な経路として引き続きサポートします。
- Sigstore の透過ログである Rekor を再設計し、パブリックおよびプライベートな展開の両方において、管理を簡素化し、運用コストを削減します。
- アカデミック コミュニティとコラボレートして、信頼保証とプライバシー保証を拡張します。
- sigstore-go、sigstore-ruby、sigstore-rs のメジャー リリースが間近に迫っています。
- 暗号化の機敏性を可能にし、量子コンピューター以降の署名をサポートします。

プロジェクト

Alpha-Omega

Alpha-Omega

Alpha-Omega は、2022 年 2 月に設立された OpenSSF の関連プロジェクトであり、Microsoft 社、Google 社、Amazon 社からの資金提供を受け、最もクリティカルなオープンソース ソフトウェア プロジェクトおよびエコシステムに持続可能なセキュリティ改善を促すことで社会を保護することをミッションとしています。Alpha-Omega は、世界中の何百万人ものエンドユーザーのセキュリティを改善するために、最も重要なオープンソース ファウンデーションおよび組織と協力しています。

α → Leverage

Ω → Scale

Alpha-Omega は、大きな影響力と効果をもたらす集中的な取り組み（Alpha）と、数十万のプロジェクトに対応するスケーラブルなアプローチの両方を対象としています。例えば、Python Software Foundation は、Python エコシステム初のセキュリティ エンジニア イン レジデンスとして Seth Larson 氏を雇用するために、Alpha-Omega の助成金を利用しました。同氏の仕事は、より広範な Python コミュニティ全体で活用されています。また、Alpha-Omega の助成金は、Airflow プロジェクトの 700 を超える依存関係の監査に対するスケーラブルなアプローチにも重点的に活用されています。

2024 年までに、Alpha-Omega は総額 500 万ドルを超える 25 件の助成金を提供しました。プロジェクトの設立以来、15 以上の異なる **オープンソース プロジェクトおよび組織** に 900 万ドルを超える助成金が提供されました。これらの助成金は、ショベルレディであり、エンジニアリング リソースがすぐにでも対応できる案件を優先しています。これらの案件は、4 つの戦略的カテゴリーのいずれかに分類されます。s:

Alpha-Omega の年次レポートおよびプロジェクトごとのステータス アップデートは、**Alpha-Omega ウェブサイト** および **GitHub レポジトリ** で閲覧可能です。

Projects は、クリティカルなオープンソース ソフトウェアをセキュアにするセキュリティ ツールとベスト プラクティスの革新的な提供をサポートする OpenSSF の技術イニシアチブです。

The OpenSSF **Technical Advisory Council** は、さまざまな技術イニシアチブ（TI）の監督責任を負い、ホストされているプロジェクトのプロジェクト ライフサイクルを管理しています。**プロジェクトのホストに興味がありますか?**

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

地域社会との関わり

DevRel & Marketing Advisory Council

DevRel コミュニティは、OpenSSF のミッションと業務を広めること、およびエンドユーザーやオープンソースのメンテナー、コントリビューターを中心とした強力なコミュニティの構築を目的として、Marketing Advisory Council と提携し、同委員会が管理しています。

このコミュニティの主なゴールは、クリティカルな OSS プロジェクトにおけるツールの導入を促進すること、より幅広いエンドユーザーおよびオープンソース コミュニティとの関係を構築し維持すること、そして、コントリビューターが参加しやすい環境やコントリビューター主導のプロジェクト イベントを通じて「OpenSSF コントリビューターコミュニティ」を創出することです。

2024 年、OpenSSF DevRel コミュニティは、そのミッションの定義、強固なコミュニティ基盤の構築、そしてソフトウェアのサプライチェーンをセキュアに保つために不可欠なオープンソース プロジェクトのポートフォリオを拡大する上で、Developer Relations の役割を強調することにおいて、大きな進歩を遂げました。今年初め、Tracy Ragan と Kathrine Druckman は、このコミュニティを形成するための取り組みをローンチし、コミュニティ ブログ プログラムのガイドライン作成から始めました。それ以来、OpenSSF は、オープンソース ソフトウェアの使用とセキュリティに関する議論を広げるセキュリティ トピックに関する多数の投稿を受け取っています。私たちは、カンファレンスでの講演やオープン オフィス アワーを通じて、コミュニティ メンバーが OpenSSF ツールやベスト プラクティスを各自のオープンソース コミュニティに持ち帰ることを奨励し、サポートを提供することに重点的に取り組んできました。


Katherine Druckman (Intel)


Tracy Ragan (DeployHub)

2025 年に向けて、DevRel コミュニティはアウトリーチ活動の拡大に重点的に取り組んでいます。私たちのゴールは、世界中のコントリビューターの取り組みを通じて開発された OpenSSF のセキュリティツールのグローバルな導入を推進し、よりセキュアなオープンソース エコシステムへのコミットメントを強化することです。

DevRel and Marketing Advisory Council Co-Chair:

Katherine Druckman (Intel Corporation)
Tracy Ragan (DeployHub)

イベント

SOSS Community Day North America

2024 年 4 月 15 日｜ワシントン州シアトル

SOSS Community Day
NORTH AMERICA

SOSS Community Day
NORTH AMERICA

ワシントン州シアトル
#SOSSCOMMUNITY

イベント終了報告

49% 技術職の役職者

340 出席者の参加人数

345 代表される組織の総数

595 出席者の登録人数

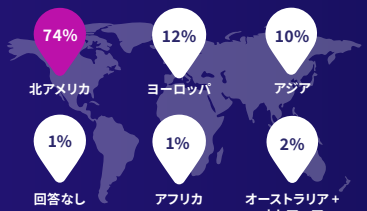
61 CFPへの応募

3 基調講演

22 パネル ディスカッション＋講演

33% ジェンダー マイノリティ スピーカー

地域別参加者数

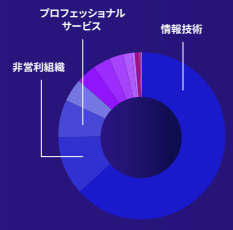


ジョブ機能トップ3：

エグゼクティブ リーダー

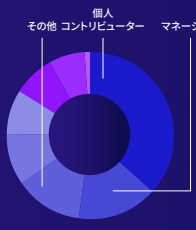
テクニカル チーム マネージャー

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）



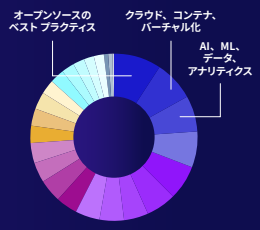
業界

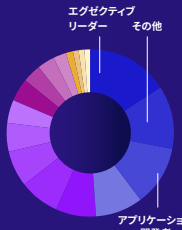
- 情報技術 64%
- 非営利組織 11%
- プロフェッショナル サービス 7%
- 電気通信 4%
- 産業 4%
- 金融 3%
- 一般消費財 3%
- 自動車 2%
- 値なし 0.7%
- ヘルスケア 0.7%
- 材料 0.3%
- エネルギー 0.2%



ジョブ レベル

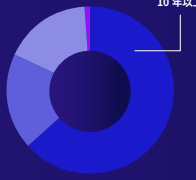
- 個人コントリビューター 37%
- ディレクター 16%
- マネージャー 13%
- その他 10%
- CXO / ED 9%
- 研究者 8%
- VP / SVP / GM 7%
- 無回答 1%





職務内容

- エグゼクティブ リーダー 13%
- その他 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）10%
- システム / 組み込み開発者 10%
- マネージャー - テクニカル チーム 9%
- マネージャー - OSPO 8%
- 設計者 8%
- マネージャー - その他 4%
- 法務 / コンプライアンス 4%
- カーネル / オペレーティング システム開発者 4%
- DevOps / SRE 3%
- マーケティング 3%
- 製品 / 事業開発 3%
- 教授 / 研究者 3%
- 学生 2%
- メディア / アナリスト 1%
- 無回答 1%



IT 業界での経験年数

- 10 年以上 63%
- 0-4 年 19%
- 5-9 年 17%
- 無回答 1%

関心領域

- オープンソース ベスト プラクティス 9%
- クラウド、コンテナ、バーチャル化 8%
- AI、ML、データ、アナリティクス 7%
- DevOps、CI / CD、サイト信頼性 7%
- サイバーセキュリティ 7%
- プライバシー、セキュリティ 6%
- サプライチェーン 5%
- Linux カーネル 5%
- IoT、組み込み 5%
- システム エンジニアリング 4%
- オープンソース プログラム オフィス 4%
- ウェブ / アプリケーション開発 4%
- リーダーシップ、コミュニティ 4%
- ネットワーク、エッジ 4%
- クロス テクノロジー 3%
- オープン ハードウェア 3%
- 多様性、公平性、包括性 3%
- セーフティ クリティカルシステム 3%
- セキュリティ 3%
- ブロックチェーン 2%
- サステナビリティ 2%
- システム管理 2%
- 視覚効果 1%
- コンプライアンス 1%
- 無回答 0.1%

SOSS Community Day Europe

2024 年 9 月 19 日｜ウィーン、オーストリア

SOSS Community Day
EUROPE

SOSS Community Day
EUROPE

ウィーン、オーストリア

イベント終了報告

42% 技術職の役職者

397 出席者の登録人数

234 代表される組織の総数

307 出席者の参加人数

85 CFPへの応募

29 実施されたセッション

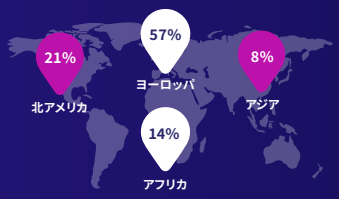
6 基調講演

23 ブレイクアウト

35 スピーカー

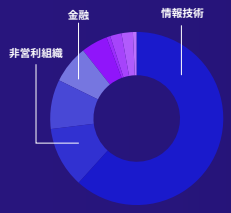
25% ジェンダー マイノリティ スピーカー

地域別参加者数



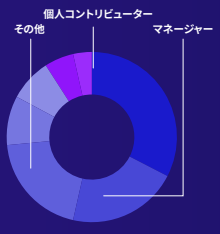
ジョブ機能 トップ3:

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)
エグゼクティブ リーダー
設計者



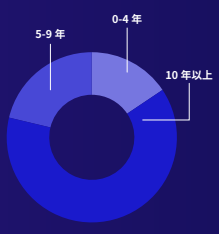
業界

- 情報技術 59%
- 非営利組織 13%
- 電気通信 8%
- 金融 6%
- プロフェッショナル サービス 5%
- 自動車 3%
- 一般消費財 3%
- 産業 3%
- エネルギー 1%
- ヘルスケア 1%



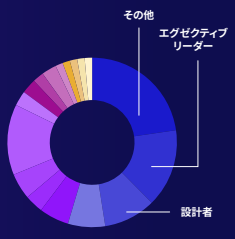
ジョブ レベル

- 個人コントリビューター 33%
- マネージャー 21%
- その他 20%
- ディレクター 9%
- CXO / ED 8%
- 研究者 6%
- VP / SVP / GM 4%



IT 業界での経験年数

- 10 年以上 65%
- 5-9 年 19%
- 0-4 年 16%



職務内容

- その他 18%
- エグゼクティブ リーダー 14%
- 設計者 12%
- マネージャー - その他 9%
- マネージャー - テクニカル チーム 7%
- システム / 組み込み開発者 6%
- DevOps/SRE 6%
- 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) 6%
- マネージャー - OSPO 6%
- マーケティング 4%
- 学生 4%
- カーネル / オペレーティング システム開発者 3%
- 教授 / 研究者 2%
- DevOps/SRE/Sysadmin 1%
- 法務 / コンプライアンス 1%
- 製品 / 事業開発 1%
- メディア / アナリスト 1%

SOSS FUSION/24

SOSS FUSION

10 月 22 日～ 23 日｜ジョージア州、アトランタ

SOSS FUSION/24

2024年10月22日～23日｜ジョージア州、アトランタ
#SOSSFusion

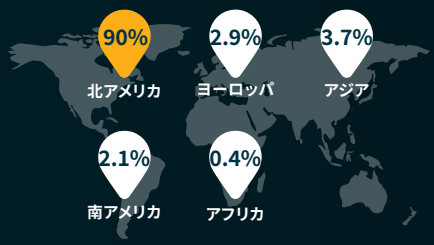
イベント終了報告

241 出席者の登録人数

191 出席者の参加人数

155 代表される組織の総数

地域別参加者数



198 CFPへの応募

1 同時開催イベント

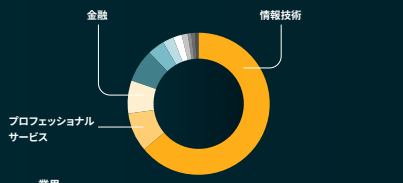
11 基調講演

35 ブレイクアウト

8 ライトニング トーク

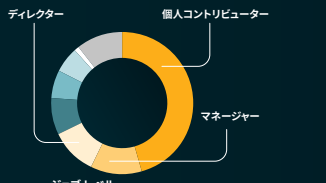
59 スピーカーの数

17% ジェンダー マイノリティ スピーカー



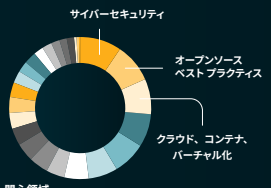
業界

- 情報技術 63.90%
- プロフェッショナル サービス 9.13%
- 金融 7.47%
- 非営利組織 7.47%
- ヘルスケア 3.73%
- 電気通信 2.49%
- 産業 2.07%
- 自動車 1.24%
- 一般消費財 0.83%
- エネルギー 0.83%
- 値なし 0.83%



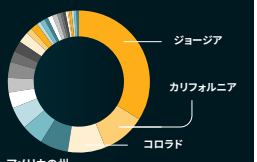
ジョブ レベル

- 個人コントリビューター 45.64%
- マネージャー 11.62%
- ディレクター 10.79%
- CXO / ED 8.30%
- 研究者 6.22%
- VP / SVP / GM 5.81%
- 値なし 1.24%
- その他 10.37%



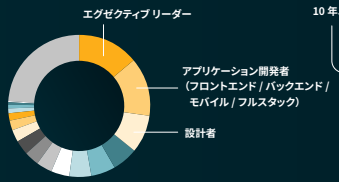
関心領域

- サイバーセキュリティ 65.98%
- オープンソース ベスト プラクティス 62.66%
- クラウド、コンテナ、バーチャル化 54.77%
- AI、ML、データ、アナリティクス 53.53%
- DevOps、CI/CD、サイト信頼性 51.45%
- プライバシー、セキュリティ 46.47%
- サプライチェーン 37.34%
- オープンソース プログラム オフィス（OSPO）30.71%
- リーダーシップ、コミュニティ 29.88%
- システム エンジニアリング 29.88%
- Linux カーネル 26.14%
- ネットワーク、エッジ 25.73%
- ウェブ / アプリケーション開発 24.90%
- IoT、組み込み 21.99%
- 多様性、公平性、包括性 19.09%
- クロス テクノロジー 18.67%
- システム管理 18.67%
- セーフティ クリティカル システム 16.18%
- オープン ハードウェア 15.77%
- サステナビリティ 12.86%
- ブロックチェーン 12.03%
- セキュリティ 10.37%
- 視覚効果 4.98%
- コンプライアンス 2.90%
- 値なし 1.24%



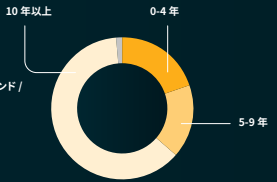
アメリカの州

- ジョージア 34%
- カリフォルニア 10%
- コロラド 8.5%
- テキサス 6.5%
- ニューヨーク 5%
- ワシントン 5%
- フロリダ 3.5%
- ノースカロライナ 3.5%
- バージニア 3.5%
- マサチューセッツ 2.5%
- ペンシルバニア 2.5%
- テネシー 2.5%
- イリノイ 1.5%
- オレゴン 1.5%
- アラバマ 1%
- アリゾナ 1%
- メリーランド 1%
- ミシガン 1%
- ミネソタ 1%
- サウスカロライナ 1%
- アーカンソー 0.5%
- デラウェア 0.5%
- コロンビア特別区 0.5%
- ケンタッキー 0.5%
- ニューハンプシャー 0.5%
- ニュージャージー 0.5%
- オハイオ 0.5%
- オクラホマ 0.5%



職務内容

- エグゼクティブ リーダー 14.11%
- 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）13.28%
- 設計者 8.71%
- マネージャー - その他 5.81%
- 製品 / 事業開発 5.39%
- DevOps/SRE 4.98%
- マネージャー - テクニカル チーム 4.15%
- 学生 3.73%
- マーケティング 3.32%
- システム / 組み込み開発者 3.32%
- マネージャー - OSPO 2.90%
- 教授 / 研究者 2.07%
- DevOps/SRE/Sysadmin 1.66%
- 値なし 1.24%
- カーネル / オペレーティング システム開発者 0.83%
- 法務 / コンプライアンス 0.41%
- メディア / アナリスト 0.41%
- その他 23.65%



IT 業界での経験年数

- 0-4 年 19.92%
- 5-9 年 16.60%
- 10 年以上 62.24%
- 値なし 1.24%

SOSS Community Day JAPAN

SOSS Community Day Japan

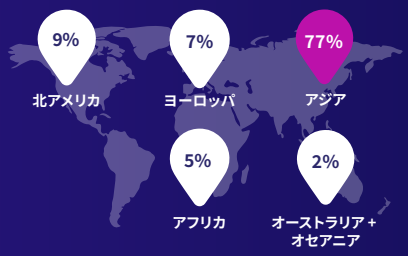
2024 年 10 月 30 日｜日本、東京

SOSS Community Day
JAPAN

日本、東京

イベント終了報告

地域別参加者数



203 出席者の登録人数

171 出席者の参加人数

57% 技術職の役職者

22 CFPへの応募

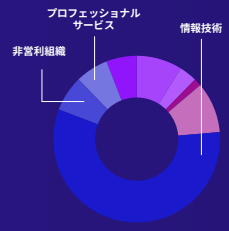
3 基調講演

16 セッション

21 スピーカー

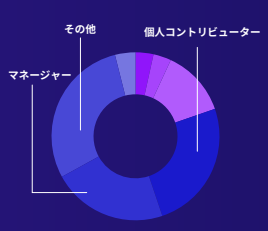
10% ジェンダー マイノリティ スピーカー

60 代表される組織の総数



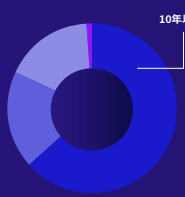
業界

- 情報技術 57%
- 産業 10%
- 自動車 9%
- 非営利組織 7%
- プロフェッショナル サービス 6%
- 電気通信6%
- 一般消費財 3%
- 金融 1%



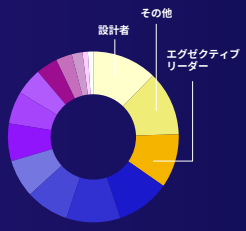
ジョブ レベル

- 個人コントリビューター 25%
- マネージャー 22%
- ディレクター 13%
- VP / SVP / GM 4%
- 研究者 3%
- CXO / ED 3%
- その他 29%



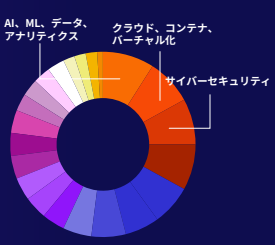
IT業界での経験年数

- 10年以上 15%
- 0-4年 21%
- 5-9 年 17%



職務内容

- 設計者 12%
- その他 12%
- エグゼクティブ リーダー 10%
- マネージャー - テクニカルチーム 10%
- システム / 組み込み開発者 10%
- アプリケーション開発者 8%
  (フロントエンド / バックエンド / モバイル / フルスタック)
- カーネル / オペレーティング システム開発 7%
- マネージャー - その他 7%
- 製品 / 事業開発 6%
- マネージャー - OSPO 5%
- DevOps/SRE 4%
- メディア / アナリスト 3%
- マーケティング 2%
- DevOps/SRE/Sysadmin 1%
- 法律/コンプライアンス 1%



関心領域

- AI、ML、データ、アナリティクス 9%
- クラウド、コンテナ、バーチャル化 8%
- サイバーセキュリティ 8%
- オープンソース ベスト プラクティス 8%
- DevOps、CI/CD、サイト信頼性 7%
- IoT、組み込み 6%
- Linuxカーネル 6%
- ネットワーク、エッジ 5%
- オープンソース プログラム オフィス 4%
- プライバシー、セキュリティ 4%
- セーフティ クリティカル システム 4%
- セキュリティ 4%
- サプライチェーン 4%
- システム エンジニアリング 4%
- クロス テクノロジー 3%
- リーダーシップ、コミュニティ 3%
- オープン ハードウェア 3%
- ウェブ、アプリケーション開発3%
- ブロックチェーン 2%
- サステナビリティ 2%
- システム管理 2%
- 多様性、公平性、包括性 1%

SOSS Community Day India

2024 年 12 月 10 日｜インド、デリー

SOSS Community Day India は、OpenSSF が新たな地域に拡大するにあたり、エキサイティングなマイルストーンとなります。これはインドで開催される初の Community Day イベントで、2024 年 12 月 10 日にデリーで開催されました。

このイベントでは、コラボレーションを促進し、オープンソース ソフトウェアのセキュリティ確保に関する進捗を共有するための魅力的なセッションが予定されています。

セッションのハイライト

Welcome & Opening Remarks – Arun Gupta, Vice President and General Manager, Developer Programs, Intel

- Cooking up Secure OCI Artifacts with SLSA – Harsh Thakur, Civo & Saiyam Pathak, Loft Labs
- Building a Security-First Open Source Project: Tools and Best Practices – Abhinav Sharma, KodeKloud
- Towards a Quantum-Proof Software Supply Chain with Post-Quantum Cryptographic Algorithms – Anitha Natarajan & Savita Ashture, Red Hat
- Who Guards the Guards? – Arnab Chatterjee, Nomura
- Patch It Up: Real-Time Vulnerability Management with Kyverno and KubeArmor – Barun Acharya & Ramakant Sharma, AccuKnox Inc.
- AI-Driven Policy Automation with Kyverno – Sonali Srivastava & Pavan N G, InfraCloud
- Securing CI/CD: Complexity & Inspiration from Runtime Security – Abhimanyu Dhamija, KoalaLab
- From CVE Chaos to Control: Building a “0 CVE” Strategy – Rakshit Gondwal, BuildSafe & Harsh Thakur, Civo
- Lightning Talk – What Do We Do With All These SBOMs? – Nikhita Raghunath, Broadcom

SOSS Community Day INDIA

- Connecting the Dots: SBOM and VEX in Software Security – Rajan Ravi, Red Hat India Pvt. Ltd.
- Case Study on Adversarial Emulation Using MITRE Caldera for Kubernetes – Rudraksh Pareek, AccuKnox
- From Bloat to Secure: Rethinking Container Base Images for the Modern Security Landscape – Abhishek Anand, KoalaLab
- How to Resolve Top 3 Security and Risk Challenges for Enterprises Consuming Open Source – Nitish Tyagi, Gartner
- Automating Container Security: Docker Scout in CI/CD for Safer Software Supply Chains – Pradumna V Saraf, Independent
- CERT.in Guidelines on Software Bill of Materials (SBOM) – Biju Nair, Legalitech
- Adversarial Resilience in Open Source LLMs: A Comprehensive Approach to Security and Robustness – Padmajeet Mhaske, JP Morgan Chase
- Quarantining and Locking Down Your Cloud Infrastructure – Prerit Munjal, KubeCloud
- Closing Remarks – Ram Iyengar, Community Engagement Lead - India, OpenSSF

SOSS COMMUNITY DAYS について

Secure Open Source Software (SOSS) Community Days は、セキュリティとオープンソース エコシステム全体からメンバーが集まり、オープンソース ソフトウェア（OSS）の開発、メンテナンス、利用を継続的にセキュアに保つためのアイデアを共有し、能力を向上させることを目的としています。イベントの詳細は こちら をご覧ください。

「What's in the SOSS?」— OpenSSF ポッドキャスト

4 月には、OpenSSF は「What's in the SOSS?」をローンチしました。これは、OpenSSF の Chief Security Architect である Christopher Robinson（通称「CRob」）と、元 OpenSSF の GM である Omkhar Arasaratnam がホストを務める隔週のポッドキャストです。わずか 7 ヶ月で、「What's in the SOSS?」はセキュアなオープンソース ソフトウェアに関する洞察のコンテンツハブとして定着しました。このポッドキャストは、より幅広いオープンソース コミュニティの構築と、OpenSSF メンバーとの関係強化に貢献しています。

「SOSS の中身」には、Google、OpenAI、GitHub、Dell、Intel、Red Hat、CISA、Rust ファウンデーションなど、世界で最も知名度の高いテクノロジー企業や組織からゲストが集まりました。現在、業界をリードするベンダーや業界組織からゲスト招待の依頼が寄せられており、これはこのプログラムの影響力とポジティブなビジビリティの証です。

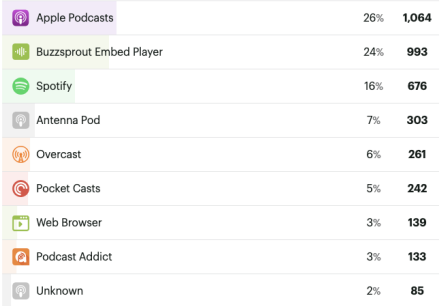
購読者（APPLE と SPOTIFY のみが購読者統計を共有）

- 合計 : 230
- Apple 製品 : 100
- Spotify: 130

年初来のダウンロード数

最も人気のダウンロード アプリケーション

- Apple 製品 : ダウンロードの 26%、合計 1064 件
- Buzzsprout Embed Player (OpenSSF サイト): ダウンロードの 24%、合計 993 件
- Spotify: ダウンロードの 16%、合計 676 件
- Antenna Pod: ダウンロード数 7%、合計 303 件
- Overcast: ダウンロードの 6%、合計 261 件



最も人気の高いエピソード

WHAT’S IN THE SOSS? PODCAST #13 – GITHUB’S MIKE HANLEY AND TRANSFORMING THE “DEPT. OF NO” INTO THE DEPT. OF “YES AND…”

2024 年 9 月 3 日公開
337 件のダウンロード

WHAT’S IN THE SOSS? PODCAST #11 – GOOGLE’S ANDREW POLLOCK AND ADDRESSING OPEN SOURCE VULNERABILITIES

2024 年 8 月 13 日公開
281 件のダウンロード

WHAT’S IN THE SOSS? PODCAST #9 – SONATYPE’S BRIAN FOX AND THE PERPLEXING PHENOMENON OF DOWNLOADING KNOWN VULNERABILITIES

2024 年 7 月 16 日公開
279 件のダウンロード

ブログ、リソース

OpenSSF ブログでは、クリティカルなサイバーセキュリティ ツールや課題への対応に向けたコミュニティのアクティブなコントリビューションに焦点を当てています。ブログ、ゲストブログ、ケーススタディを通じて、セキュアなソフトウェア開発とオープンソース セキュリティの進歩を促す多様な洞察とソリューションを共有してきました。

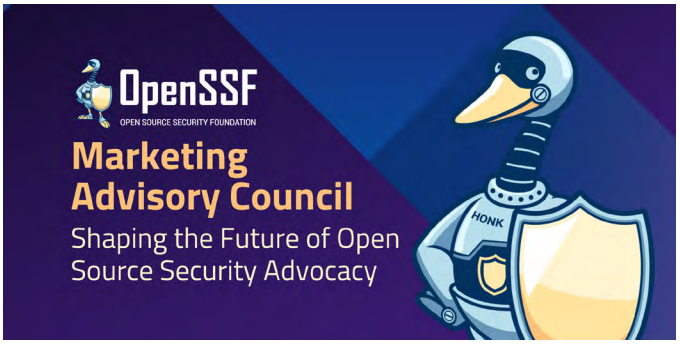
共有したいアイデアをお持ちですか？ブログの提案を提出 して、2025 年のサイバーセキュリティの未来を形作ることにコントリビュートしましょう！

OpenSSF ブログ

OpenSSF ブログは、サイバーセキュリティの主要な問題に関する専門家の洞察、詳細な分析、コミュニティのアップデートを提供する重要なリソースです。年間を通じて、当ブログでは、セキュアなソフトウェア開発とオープンソース セキュリティの最新動向を探る多様なコンテンツを掲載しています。これには、主要な業界イベントへの参加のハイライトも含まれています。

- Understanding the CRA: OpenSSF's Role in the Cyber Resilience Act Implementation – Part 1
- The OpenSSF Armored Goose "Honk": Advancing Open Source Security
- How We Can Learn from Open Source Software to Address the Challenges of AI
- OpenSSF Welcomes New Members and Introduces New Initiatives at SOSS Community Day Japan
- OpenSSF Expands Secure Development Course with Interactive Labs
- Cybersecurity Awareness Month 2024: Stay Secure, Stay Informed
- OpenSSF SOSS Fusion Conference Kicks off with Talks from Google and Cisco Executives
- Developer Relations: The Human Connection Driving Open Source Security
- OpenSSF Education Tech Talk Highlights & Future Opportunities
- Recap on SOSS Community Day EU
- OpenSSF at Grace Hopper Celebration 2024: Advancing Diversity and Security in Open Source
- Join Us at the OSS Security Meetup in Tokyo, Japan
- Must-Attend Sessions at SOSS Community Day EU and Open Source Summit Europe 2024
- Prioritizing Security: Key Findings from the OpenSSF Survey for Financial Institutions
- AIxCC Semifinals at DEF CON Showcase AI's Potential in Securing Critical OSS Projects
- A Bird's-Eye View of LFD 121 (Developing Secure Software) — and Why Every Developer Should Take It
- GUAC v0.8.0 Released
- Announcing SigstoreCon: Supply Chain Day!
- Mitigating Attack Vectors in GitHub Workflows
- Call for Proposals: SOSS Community Day Japan 2024
- What's Next for Open Source? Workshop Highlights and Calls to Action to Inspire Progress for Global Sustainability
- OSS Security Adventure: Recap of Recent Security-Focused Events Featuring OpenSSF
- SOSS Community Day EU Agenda Now Live!
- SOSS Fusion 2024 CFP Results: A Look at Our Diverse and Engaging Program
- Celebrating Excellence: An Interview with Golden Egg Award Winner Christopher "CRob" Robinson
- Recognizing Excellence in OSS Community: Golden Egg Award Nominations Are Now Open!
- AI Cyber Challenge (AIxCC) and the Needle Linux Kernel Vulnerability – Part 1

- AI Cyber Challenge (AIxCC) and the Needle Linux Kernel Vulnerability – Part 2
- Learn How To Develop Secure Software!
- Why are Organizations Struggling to Implement Secure Software Development?
- A Deep Dive into SBOMit and Attestations
- Know Your Regular Expressions: Securing Input Validation Across Languages
- July in NYC: Join Us at the United Nations' (UN's) OSPOs for Good 2024 Conference & the "What's Next for Open Source?" Event
- OpenSSF GUAC Tech Talk Highlights
- Final Call: Submit your Technical Initiatives (TI) Funding Request by June 7th, 2024
- The OSS Security Adventure: Exploring the Frontlines of OSS Security through SOSS Policy Summit, RSA Conference, and Japan Meetup
- Beyond the OpenSSF: An Introduction to Other Security Efforts Across the Linux Foundation
- The Opportunity for DEI Participation in the Security Industry (And OpenSSF)
- OpenSSF Joins Open Source Consortium To Define E.U. CRA Security Specifications
- Join Our Upcoming OpenSSF Tech Talk: Proactive Supply Chain Security with GUAC
- Call for Proposals: Submit to Speak at SOSS Community Day Europe
- Unlock the Keys to Improved Software Security
- Recap of SOSS Community Day North America 2024
- Join Us at the OSS Security Meetup in Tokyo, Japan With General Manager Omkhar + SOSS Community Day North America Event Report
- Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects
- Unveiling the Golden Egg Award Winners: Celebrating Excellence in Open Source Security
- Sessions You Won't Want to Miss at SOSS Community Day NA and Open Source Summit North America 2024
- "What's in the SOSS?" Podcast is Now Live
- Join us for a TTX: Securing OSS & Empowering Maintainers
- xz Backdoor CVE-2024-3094
- VulnCon 2024 Wrap-up: Securing the Ecosystem through Global Cooperation
- How Intel Uses OpenSSF Scorecard To Better Secure Its Software Portfolio
- Empowering Women in Tech: An Interview on Angela Jeffrey's Journey to Cybersecurity
- OpenSSF Scorecard Tech Talk Highlights
- Driving Change Together: The OpenSSF Takes On VulnCon
- Sigstore Graduates: A Monumental Step Towards Secure Software Supply Chains
- Join OpenSSF for our First Tabletop Exercise (TTX) at SOSS Community Day North America
- How OpenSSF Technical Initiatives Can Receive Strategic Funding
- OpenSSF Releases Plan for Improving Software Developer Security Education



- The India Initiative: An OpenSSF Awareness Program for a Secure Future
- OpenSSF Marketing Advisory Council Aims to Shape the Future of Open Source Security Advocacy
- Participate in Our Survey on Secure Software Development Education!
- OpenSSF and CISA Join Forces to Secure Open Source Software
- Graph for Understanding Artifact Composition (GUAC): Joins OpenSSF as Incubating Project
- OpenSSF Scorecard: Evaluating and Improving the Health of Critical OSS Projects
- Come to First OpenSSF Tech Talk of the Year on Scorecard
- Golden Egg Award: Celebrating Exceptional Contributions in the OpenSSF Community
- SOSS Community Day North America (NA) Agenda Live
- OpenSSF Supports White House's Efforts to Build More Secure and Measurable Software
- Submit to Speak at SOSS Fusion 2024
- OpenSSF Responds to US CISA RFI on Cybersecurity Risk and Secure by Design Software
- Scaling Up Supply Chain Security: Implementing Sigstore for Seamless Container Image Signing
- Alpha-Omega 2023 Annual Report
- Linux Kernel Achieves CVE Numbering Authority Status
- Announcing the First Ever SOSS Fusion Conference: How You Can Get Involved
- OpenSSF Participates in Department of Commerce Consortium Dedicated to AI Safety
- OpenSSF Securing Software Repositories Working Group Releases Principles for Package Repository Security
- Time is of the Essence to Mitigate Vulnerabilities like Leaky Vessels
- Post-Quantum Cryptography Alliance Launch
- CVE-2023-6246 Root Access Vulnerability in glibc
- OpenSSF Champions a More Secure Future in Collaboration with Public Sector
- Maintainer Motivations, Challenges, and Best Practices on Open Source Software Security
- OSS Security Sessions & FOSDEM Survival Guide
- Introducing gittuf: A Security Layer for Git Repositories
- Submit to Speak at SOSS Community Day North America 2024
- OpenSSF Election Results for Technical Advisory Council and Representatives to the Governing Board

ゲストブログ

ゲストブログは、OpenSSF コミュニティの重要な一部であり、メンバーが自身の声や専門知識をコントリビュートするためのプラットフォームを提供しています。これらのブログでは、プロジェクトの最新情報、新しいイノベーション、オープンソース セキュリティの最前線でアクティブに活動する人々の個人的な視点が紹介されています。コミュニティメンバーに自身のストーリーや洞察を共有してもらうことで、オープンソース ソフトウェアのセキュリティに関する対話をより豊かなものにし、今日のサイバーセキュリティの課題に取り組む上でコラボレーションが持つ力を強調しています。

- Red Hat's Collaboration with the OpenSSF and OSV.dev Yields Results: Red Hat Security Data Now Available in the OSV Format
- OpenSSF Adds Minder as a Sandbox Project to Simplify the Integration and Use of Open Source Security Tools
- New Guide for Package Repositories to Adopt Trusted Publishers
- Neo Malware: Malicious Open Source Packages
- How to Make Programming Language Package Repositories More Secure
- Chainguard Enhances Security With OSV Advisory Feed
- Improving OpenSSF Scorecard Scores: StepSecurity Automation for Four Key Checks
- An Open Source Approach to Threat Mitigation in AWS
- Ubuntu Security Notices Now Available in OSV
- Introducing Artifact Attestations—Now in Public Beta
- Enhancing Open Source Security: Introducing Siren by OpenSSF
- Where Does Your Software (Really) Come From?
- DruBOM: An SBOM for Drupal
- Spotlight on the OpenSSF AI/ML Working Group
- Beyond Scores with OpenSSF Scorecard: Granular Structured Results for Custom Policy Enforcement
- Static Binary Analysis: A Final Exam for Software Supply Chain Protection

ケーススタディ

ケーススタディは、組織が OpenSSF のツールやテクノロジーを導入し、サイバーセキュリティ対策を拡張することに成功した事例を強力に裏付けるものです。これらの実例は、OpenSSF エコシステムに参加することの具体的な利点を示し、コラボレートしオープンソース ソリューションを使用することで、ソフトウェア セキュリティの大幅な向上につながることを示しています。

- Case Study: Kusari's Implementation of OpenSSF Tools and Services
- Innovative Supply Chain Security for Enterprise Cloud Platform Service
- OpenSSF Case Study: Enhancing Open Source Security with Sigstore at Stacklok
- Introducing Artifact Attestations—Now in Public Beta
- How Intel Uses OpenSSF Scorecard To Better Secure Its Software Portfolio
- Scaling Up Supply Chain Security: Implementing Sigstore for Seamless Container Image Signing

技術講演会

OpenSSF Tech Talks は、コミュニティがプロジェクト、ツール、イノベーションを紹介し、コラボレートし、オープンソース セキュリティにおけるリーダーシップを発揮するためのプラットフォームを提供します。今年の講演からインスピレーションを得て、アイデアを提出 し、OpenSSF コミュニティ内であなたの作品を共有し、議論を活性化させましょう!

JUMPSTART YOUR JOURNEY: MASTERING OSS SECURITY DEVELOPMENT WITH THE LINUX FOUNDATION EDUCATION (2024-10-10)

オンデマンドビデオが 利用可能 です。

PROACTIVE SUPPLY CHAIN SECURITY WITH GUAC (2024-06-06)

オンデマンドビデオが 利用可能 です。

BUILDING A STRONGER OPEN SOURCE ECOSYSTEM: OPENSSF SCORECARD (2024-03-13)

オンデマンドビデオが 利用可能 です。

インド イニシアチブ

今年、OpenSSF は、ライブストリーム、ミートアップ、プネーでの Security Samvad、CNCF Meetups、IndiaFOSS 2024 などのイベントを通じて、インドのオープンソース コミュニティとの関わりを深めました。これらの活動を通じて、オープンソース セキュリティに関する実践的な洞察が得られ、地域全体の開発者やコントリビューターとつながることができました。今後、OpenSSF はインドでの活動を拡大し、コラボレートしながら、共にセキュアなオープンソース エコシステムを構築していくことを楽しみにしています。

ライブ配信

3 月

- Let's Chat Open Source Security
- How To Secure Open Source Code

4 月

- Techniques & Tools: PINNY
- Tools & Techniques: BOLT

5 月

- Supply Chain Security: Fundamentals and more...
- Building A Culture Of Security

6 月

- SLSA, A Security Paradigm For Your Builds
- Tips, Tricks, and Techniques to Ace Supply Chain Security

対面ミーティング

5 月

- 5 月 4 日 Security Samvad in Pune（OpenSSF Scorecard に焦点をあてた）

7 月

- 7 月 25 日 Accel Cybersecurity Summit

8 月

- 7 月 25 日 CNCF Aug Meetup: Security Theme (GUAC に焦点を当てた)

10 月

- 10 月 19 日 CNCF New Delhi Meetup: Secret to Cloud Native Security
- 10 月 26 日 Observability Marathon By-Two Edition - AWS UG Bengaluru x New Relic Oct meet-up

講演

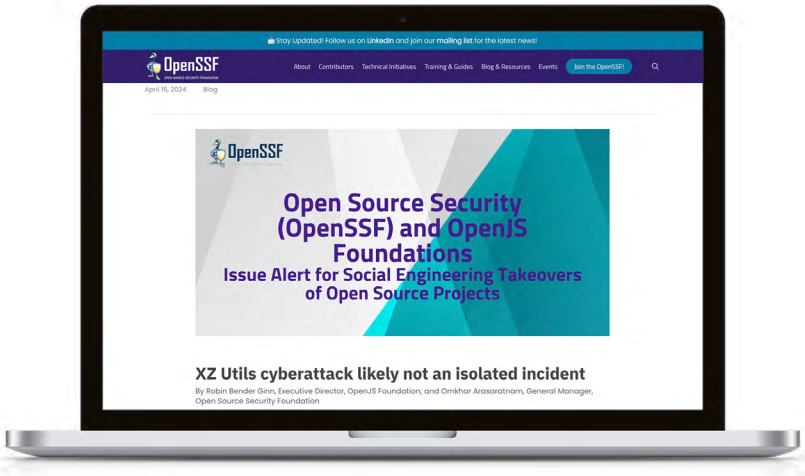
- Is What You See, What You Deploy? AllDayDevOps conference
- Scorecard: Assessments Made Easy KubeCon Hong Kong
- Security: Shift Left, or Swipe Left? DevOpsDays Kerala

その他のイベント

- IndiaFoss 2024 (2024 年 9 月 7 日～ 8 日、ベンガルール)

ウェブサイト

トップ ウェブ ページ
Secure Software Development Fundamentals Courses



人気ブログ記事
Open Source Security (OpenSSF) and OpenJS Foundations Issue Alert for Social Engineering Takeovers of Open Source Projects

ニュースレター

8,833 人の
購読者

19.85%
平均開封率

14.93%
平均クリック率

215,671 回
総再生回数

YouTube

最も視聴された動画
Open Source Security Foundation (OpenSSF) - Who We Are

1.34 万人の登録者
(前年比 49.22% 増)

988 本の動画

X

5,574 人のフォロワー
(前年比 49.22% 増)

551 投稿

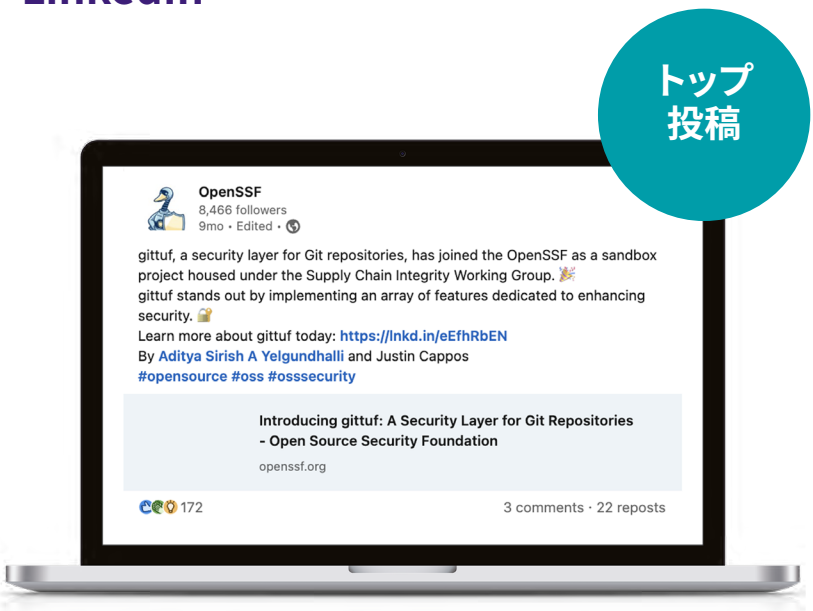
2,180 インタラクション

Mastodon

895 人のフォロワー

375 件の投稿

LinkedIn



8,459 人のフォロワー
(前年比 98.38% 増)

523 件の投稿

500,861 インプレッション

10,067 インタラクション

65 のレポジトリと
1398 人のアクティブな
コントリビューター

GitHub

1,300 のフォロワー
(前年比 52.42% 増)

1,398 人のコントリビューター

65 のリポジトリ

18 のプロジェクト

77 チーム

133 人

180 の課題

420 のプル リクエスト

Slack

3,822 のユーザー

トレーニングと教育 ー LF 教育

ヨルダンのサイバーセキュリティ分野を目指す女性をサポートする奨学金

今年、OpenSSF、Linux Foundation Education、Cloud Native Computing Foundation (CNCF) は、アメリカ ホワイトハウスの国家安全保障会議（NSC）と提携し、ヨルダンの女性を対象に、Kubernetes やクラウド ネイティブ セキュリティの専門認定を含む 250 の無料セキュリティ コースと認定を提供するパイロット プログラムをローンチしました。

OpenSSF と LF T&C がスポンサーを務めるこのイニシアチブは、オープンソース セキュリティの向上、サイバーセキュリティにおける多様性、公平性、包括性の推進、そしてヨルダンの女性に価値ある補完的な認定資格を与えることで労働力の課題に対処するというコミットメントを強調するものです。

このイニシアチブについてさらに詳しく : OpenSSF, Linux Foundation Training & Certification, and CNCF Announce Scholarships to Support Women in Jordan Entering the Cybersecurity Field in Collaboration with US White House National Security Council

2024 年 セキュアなソフトウェア開発コースの受講登録

私たちは、よりセキュアなソフトウェアの作成方法を学ぶ人々を支援する素晴らしい 1 年を過ごしました。「Developing Secure Software」（LFD121）の無料コースへの登録者数は、昨年と比較して 20% 増（7,990 人）という当初の目標をはるかに上回りました。さらに、edX の同等のコース（LFD104x、LFD105x、および LFD106x）を受講した人数も増えました。また、「Sigstore」と「OpenSSF Scorecard」のコースを受講した人数は 1,000 人を超えました。

Developing Secure Software - LFD121
2024 年 ー 入学者数：8,186 人
2022 ー 2024 年入学者数：19,980 人

Securing Your Software Supply Chain with Sigstore - LFS182x
2024 年 ー 入学者数：91 人
2022 ー 2024 年入学者数：1,551 人

Securing Projects with OpenSSF Scorecard - LFEL1006
2024 年 ー 入学者数：852 人
2023 ー 2024 年入学者数：1,254 人

Secure Software Development: Requirements, Design, and Reuse - LFD104x
2024 年 ー 入学者数：1,213 人
2020 年 ー 2024 年の入学者数：7,031 人

Secure Software Development: Implementation - LFD105x
2024 年 ー 入学者数：605 人
2020 年 ー 2024 年の入学者数：3,592 人

Secure Software Development: Verification and More Specialized Topics - LFD106x
2024 年 ー 入学者数：477 人
2020 年 ー 2024 年の入学者数：3,279 人

* これらの数字は 2024 年 11 月 18 日時点でアップデートされています。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

注目記事

過去数年にわたり、OpenSSF はオープンソース セキュリティの原則におけるベスト プラクティスとガイダンスの信頼できるリソースとして、技術コミュニティ内で確固たる評価を築いてきました。2024 年の私たちのミッションは、この影響力のレガシーを基盤としつつ、より権威があり、より多くの読者を持つ出版物へのリーチを拡大することです。

今年、私たちは OpenSSF ブランド、および OpenSSF プロジェクト、プログラム、メンバー、コラボレーションのビジビリティを劇的に向上させました。私たちは、この組織を専門知識のリソースとして確立し、技術的なトピックだけでなく、AI などの公共政策や世界的なトレンドに関するリソースとしても活用しています。組織のプロジェクト、研究、コンテンツについて、多くの本質的な発言を目にしています。

以下のメディアのハイライトは、OpenSSF が今年達成した幅広い報道とリーチを紹介します。私たちは、このような掲載の機会を得るごとに、オープンソースのセキュリティを推進するというミッションをさらに高め、業界全体および世界中にその影響を広げています。

成功指標

110%

2024年のわずか9か月間で、
報道量が2倍以上に
増加（110%増）

215%

わずか9か月で
OpenSSFプロジェクトのカバー範囲を
3倍以上に拡大（215%増）

2,000万以上

2,000万人以上の
潜在的な読者を持つ出版物に
12件のメディア掲載

5,000万以上

5,000万人以上の
潜在的な読者を持つ出版物に
6件のメディア掲載

10000

OpenSSFについて言及した記事の
ソーシャル共有が約10,000件

11

11のプレスリリースで、
新しいプロジェクト、メンバー、
コラボレーション、マイルストーンを発表

トップ キャンペーン

XZ Utils、OpenSSH、PyPi などの主要な脆弱性やサイバーセキュリティ インシデントに関するリーダーシップ。

OpenSSF が業界初の OSS インテリジェンス リソース **Siren** をローンチします。

LF と OpenSSF は、セキュアなソフトウェア開発教育に関する研究を発表しています。

OpenSSF は、DARPA AI Cyber Challenge に参加します。

OpenSSF、DHS および CISA と提携し、Global Software Supply Chain Project をローンチします。

OpenSSF は、LFD 121 にインタラクティブなラボを追加します。

主要なメディア報道

Washington Post（月間 1 億 3,890 万ビュー）
[Hackers race to win millions in contest to thwart cyberattacks with AI]
OpenSSF の創設者である Brian Behlendorf 氏は、DARPA AI Cyber Challenge に関する大規模なストーリーの一部として、オープンソース セキュリティの重要性を論じました。

NPR
[The Hack that Almost Broke the Internet]
元 OpenSSF の GM である Omkhar Arasaratnam 氏は、NPR の取材に対し、XZ Utils のバックドア脆弱性について、「これは、オープンソースを社会が消費してきた方法の失敗例のひとつでしょう。このような問題に対処しなければならないという負担は、耐え難いものになる可能性があります」と語りました。

Politico（月間 5,200 万ビュー）
[Hacking The Gender Gap]
国家安全保障会議と OpenSSF および Linux Foundation との提携について、ヨルダンの女性たちに 250 の無料サイバーセキュリティ コースと認定資格を提供していることについて、サイバーおよび新技術担当の国家安全保障顧問代理である Anne Neuberger 氏は、「これはヨルダンの女性たちに重要なスキルを身につけさせ、国家の安全保障に貢献するでしょう」と述べています。

Reuters（月間 8,400 万ビュー）
[Open source groups say more software projects may have been targeted for sabotage]
OpenSSF と OpenJS は、XZ Utils に秘密のバックドアを挿入しようとした試みは孤立した事件ではなく、また、複数の JavaScript プロジェクトも標的とされていたことを示す声明を発表しました。

Fortune（月間 3,630 万ビュー）
[After a failed Linux backdoor attempt grabs headlines, open source leaders warn of more attacks]
OpenSSF と OpenJS は、XZ Utils とそれに続く攻撃について次のように引用しています。「これらのソーシャル エンジニアリング攻撃は、メンテナーがプロジェクトやコミュニティに対して抱いている義務感を悪用し、彼らを操ろうとするものです。あなた自身がどのように感じているかに目を向けてください。自己不信、劣等感、プロジェクトに十分貢献できていないのではないかといった感情を生み出す人とのかかわりは、ソーシャル エンジニアリング攻撃の一部である可能性があります。」

Gizmodo（月間 1,680 万ビュー）
[Open source Cybersecurity Is a Ticking Time Bomb]
OpenSSF と OpenJS は、XZ Utils とそれに続く攻撃について次のように引用しています。「これらのソーシャル エンジニアリング攻撃は、メンテナーがプロジェクトやコミュニティに対して抱いている義務感を悪用し、彼らを操ろうとするものです。あなた自身がどのように感じているかに目を向けてください。自己不信、劣等感、プロジェクトに十分貢献できていないのではないかといった感情を生み出す人とのかかわりは、ソーシャル エンジニアリング攻撃の一部である可能性があります。」

その他のレポート

The Economist、Why is so much of the internet's infrastructure run by volunteers?、(April 23, 2024)

Axios、1 big thing: Open source developers face a potential crisis、(April 19, 2024)

Quartz、Open source cybersecurity could derail the internet as we know it、(May 10, 2024)

The Register、OpenSSF sings a Siren song to steer developers away from buggy FOSS、(May 20, 2024)

The Hacker News、New OpenSSH Vulnerability Could Lead to RCE as Root on Linux Systems、(July 1, 2024)

TechTarget、Linux group announces Post-Quantum Cryptography Alliance、(Feb. 6, 2024)

CSO、Keeping up with AI: OWASP LLM AI Cybersecurity and Governance Checklist、(March 14, 2024)

Dark Reading、Under-Resourced Maintainers Pose Risk to Africa's Open Source Push、(July 22, 2024)

The New Stack、There Is Just One Way To Do Open Source Security: Together、(October 23, 2024)

ZDNet、Technologist Bruce Schneier on security, society and why we need 'public AI' models、(October 24, 2024)

SC Magazine、Crowdstrike: The Aftermath – PSW #836、(July 27, 2024)

TechStrong、Securing Open Source as Critical Infrastructure with Omkhar Arasaratnam at OSS Seattle 2024、(April 19, 2024)

SiliconANGLE、Enhancing open source security: Collaborative strategies from OpenSSF、(March 21, 2024)

InfoSecurity Magazine、RSAC: Three Strategies to Boost Open source Security、(May 8, 2024)

Help Net Security、One-third of dev professionals unfamiliar with secure coding practices、(July 19, 2024)

InfoQ、Sigstore: Secure and Scalable Infrastructure for Signing and Verifying Software、(Feb 29. 2024)

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2025 年に向けて

2025年に歩み出すにあたり、私たちのコミュニティが達成したすべてのことに感謝の意を表したいと思います。オープンソース ソフトウェア（OSS）はグローバルなイノベーションの基盤であり、そのセキュア化は私たち全員が共有する責任です。皆さま一人ひとりの献身と努力が、より安全でセキュアな未来の構築に役立っていることに深く感謝しています。私たちは共に、コードを一行ずつ書き加えることで、世界をより良い場所に変えていきます！

今後、コラボレーション、つながり、イノベーションの機会をさらに増やし、この勢いを継続していくことを楽しみにしています。OpenSSFのミッションの核心は、このコミュニティにあります。私たちは、皆様の声を大きくし、皆様のコントリビューションが今後も末永く影響を与え続けるよう尽力してまいります。

コラボレーションの促進

私たちは、OpenSSF Community Days、meetups、Tech Talks、spacesなどを通じて、メンテナーと組織を結びつけ、有意義な議論と、私たちが直面するセキュリティ上の課題に対する真の解決策を見出す場を提供し続けていきます。

コミュニティ主導の取り組みの拡大

2025年には、ベストプラクティス バッジの改善、Sigstoreの進展、コンパイラー オプションの強化ガイドのようなリソースの改良といった主要プロジェクトに、皆様が関与できる機会を拡大していきます。大小かかわらず、皆様のコントリビューションが、私たちを前進させてくれます。.

共に成長

誰もが参加し、学び、成長しやすいイニシアチブへの投資も継続していきます。例えば、「セキュアなソフトウェア開発」コースやマネージャー向けの新しいリソースなどです。皆さまの継続的なサポートにより、より強固でセキュアなオープンソース エコシステムを構築し続けていきます。

あなたにもできること

- **ワーキンググループに参加**: 進行中のセキュリティイニシアチブにコントリビュートする。こちら から参加してください。
- **エクスプローラー メンバー**: OpenSSFのメンバーになって、オープンソースセキュリティの未来を形作っていきましょう。メンバーになる機会について詳しく見る。
- **私たちのソーシャル メディアをフォロー**: LinkedIn、X、Bluesky、Mastodon で私たちをフォローして、最新ニュースを入手しましょう。
- **ニュースレターを購読**: 最新のアップデートを直接受信トレイにお届けします。こちら から購読してください。
- **OpenSSFへの参加を 他の人にも呼びかけましょう** : 私たちのゴールは野心的でありながらも重要であり、広く共感を得られるものと信じています。私たちと一緒に違いを生み出しましょう。

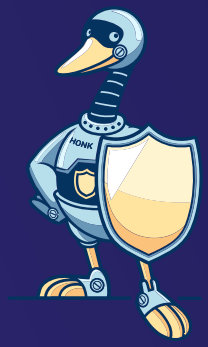
一緒にセキュアで強靭なオープンソース エコシステムを構築しましょう。今すぐ参加して、2025年をこれまでにないほどインパクトのある年にしましょう!

— The OpenSSF Team

本訳文について

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

翻訳協力：富田明男・富田佑実



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

一緒にセキュアで強靭なオープンソース エコシステムを構築しましょう。 今すぐ参加して、2025 年をこれまでにないほどインパクトのある年にしましょう！

openssf.org/getinvolved

openssf.org