OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2023 アニュアル レポート

openssf.org

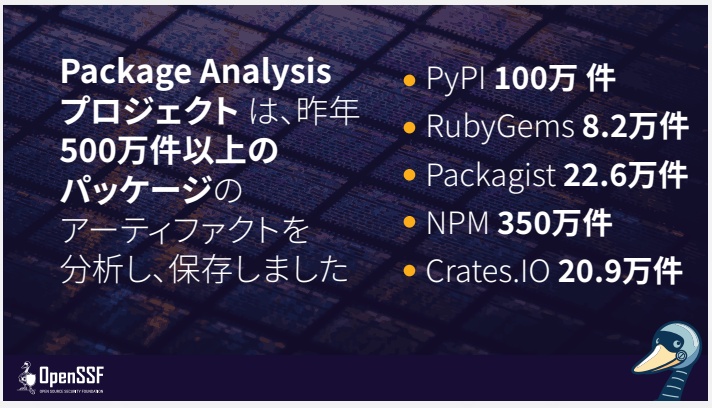
目次

この文書は、2023 OpenSSF Annual Report の参考訳です。
原文のレポートは以下のページからダウンロードできます。
https://openssf.org/download-the-2023-openssf-annual-report/

翻訳協力：辻村幸弘

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

数字で見る 2023



数字で見る 2023

悪意のあるパッケージ
リポジトリには
クロスエコシステムから
報告された悪意のある
パッケージのデータ
16,000 点が
含まれています

- npm **9000件**
- pypi **6500件**
- その他
  rubygemsと
  crates.ioからも

OpenSSFには、**25業界**から
120人のメンバーが参加しており
時価総額は**13.5兆ドル**です

OpenSSFスコアカード プロジェクトは
GitHubで**3,776個のスター**を持ち
100万件を超える OSSプロジェクトの
ソフトウェア セキュリティ基準に照らした
自動評価スキャンを
毎週実行しています

OpenSSFは、よりセキュアなコードを
書くための開発者の育成を支援しています

登録者22,771名
安全なソフトウェアの
開発コース

登録者1,263名
Sigstoreによるソフトウェ
ア サプライチェーンの
セキュリティ確保

Alpha-Omega

2023年に**オープンソースの**
セキュリティ確保に向けて**490万**
ドル以上の助成金を獲得しました

ゼネラル マネージャーより

2023 年の年次報告書を発表できることを嬉しく思います。この年次報告書には、OpenSSF コミュニティが今年達成した多くの活動や成果が記載されています。5 月、私はゼネラル マネージャーとして OpenSSF に参加し、理事会、ワーキング グループ、プロジェクト リーダー、そしてコミュニティと密接に協力し、私たちの活動をどのようにサポートし、公共の利益のためにオープンソースを確保するために前進させるのが最善かを検討し続けてきました。

2023 年の間に、OpenSSF のメンバーは、北米（77 名）、ヨーロッパ（13 名）、アジア（15 名）、中東（1 名）にまたがり、100 名を超えるまでになりました。私たちは、さまざまな業界や対象分野にまたがる企業や非営利団体を含む、すべてのメンバーからの支援に依存しています。すべてのメンバーは、公共の利益のために安全なオープンソース ソフトウェアを維持するという共通の目標を持って集まっています。

私たちは今年、公共部門のパートナーとの協力で素晴らしい進歩を遂げました。8 月には、OpenSSF が国防高等研究計画局（DARPA）の人工知能サイバーセキュリティ チャレンジ（AIxCC）に助言することを発表しました。また、9 月には、国家安全保障会議（NSC）、国家サイバー長官室（ONCD）、サイバーセキュリティ・社会基盤安全保証庁（CISA）などのパートナーとともに、セキュア・オープンソース・ソフトウェア（SOSS）サミットを開催しました。私たちは、オープンソースのエコシステムとポリシーが健全で、信頼性が高く、私たちコミュニティ全員のために機能することを保証するために、公共部門との継続的な関与が重要な役割を果たすと信じています。

オープンソースのセキュリティは、公共部門、民間部門、およびコミュニティの間で説明責任を共有することです。2024 年、私たちは、技術的な取り組みを継続し、私たち全員が依存するオープンソース ソフトウェアのセキュリティ確保とサポートに関心のあるすべてのステークホルダーと関わっていくことを楽しみにしています。

Regards,

Omkhar Arasaratnam
General Manager
OpenSSF

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF について

ミッション

オープンソース セキュリティ財団（OpenSSF）は、私たち全員が依存しているオープンソース ソフトウェア（OSS）の開発、保守、使用を持続的な安全の確保を容易にすることを目指しています。これには、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。

ビジョン

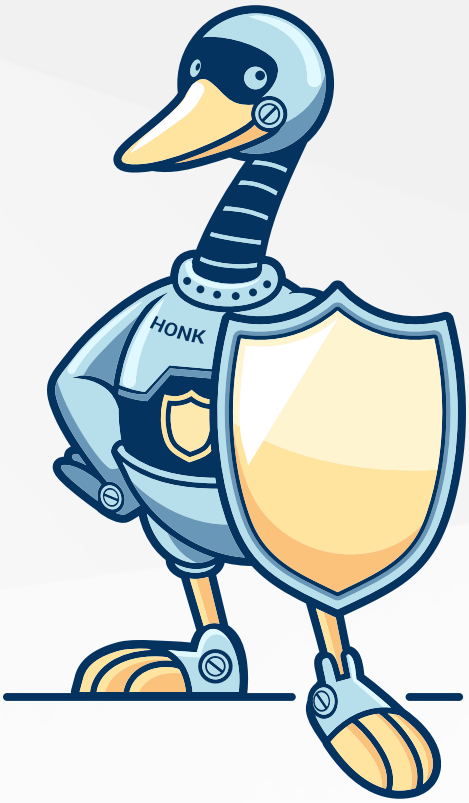
OSS はデジタル公共財であり、業界として、私たちはコミュニティとともにセキュリティの懸念に対処する義務があります。私たちは、OSS が普遍的に信頼され、安全で、信頼できる未来を描いています。この協力的なビジョンにより、グローバルなエコシステムにおける個人や組織が自信を持ってその恩恵を活用し、OSS コミュニティに有意義に貢献できるようになります。

価値観

OpenSSF は、関連するオープンソース財団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やデフォルトによるセキュリティを奨励するプロジェクトや財団に、「セキュア ソフトウェア開発の指針」トップ 10 のような価値あるガイダンスやアーティファクトを提供しています。OpenSSF の取り組みは、オープンソースのメンテナーや貢献者にとって、セキュリティをより容易にするものでなければなりません。OSS の利用者は、OpenSSF のアウトプットを活用することで、OSS の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、関心のあるすべての利害関係者が財団とその技術的取り組み（TI）に参加することを奨励することを約束します。OpenSSF は、相互に価値のある情報の外部への発信者であり、政策決定者の教育者であるとみなされています。OpenSSF は、多様性、公平性、包括性（DEI）グループへの支援にとどまらず、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ための公平な機会を提供する環境を直接促進することを約束します。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もたらし、ステークホルダーが OpenSSF の技術的な取り組みに参加し、そこから価値を受け取る機会を共有できるようにするために、これらの取り組みを継続的に進化させることを約束し続けます。



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を開発し、ベスト プラクティスの理解を深め、革新的な技術的取り組みをサポートすることで、OSS のセキュリティを強化することを目的とした一連の目標です。憲章は OpenSSF の真実の源であり、この戦略は憲章に基づいています。

目標は、OSS エコシステム全体のセキュリティを強化する一貫性、完全性、リスク評価を確実にするために設計されたツールとプロセスに焦点を当てています。これにより、OSS セキュリティに関する技術的取り組みを加速するツール、プロセス、教育資産を開発するコミュニティを支援します。これらの目標を達成することで、あらゆるスキル レベルの OSS のメンテナーや貢献者に、既存のセキュリティ脅威と新たに発生するセキュリティ脅威の両方に、事前または事後的に対処する能力を提供します。

OpenSSF の戦略は、5 つの重要な分野で概説されています：

教育と対象を絞ったコミュニケーション：ベスト プラクティス、ガイドライン、教育リソースを開発・推進し、エコシステム内のオープンソース ソフトウェア セキュリティに対する意識と専門知識を高めます。OpenSSF は、OSS エコシステム内のターゲットとなるペルソナ（メンテナー、貢献者、利用者を含む）に対して、デフォルトのセキュリティ態勢を改善するよう提唱し、その状態を達成するための摩擦を低減または排除するための取り組みを促進します。

コラボレーションの促進：OSS コミュニティ、セキュリティ専門家、業界の利害関係者の間で、協力と包括の文化を醸成し、オープンソース ソフトウェアのセキュリティ課題に透明性のある運用とガバナンスによって効果的に持続的に対処できるようにします。

持続可能な技術革新とデリバリーの強化：既存のセキュリティ機能に対するツールとプロセスの強化を支援します。脆弱性検出、インシデント対応、セキュアなコーディング プラクティス、実用的な標準など、新たなセキュリ ティ機能をオープンソース エコシステムに提供します。

提唱と政策：政府、業界団体、その他の関連組織と連携して、OSS セキュリティを促進する政策と実践を提唱します。

コミュニティとの連携：イベント、カンファレンス、ワークショップ、オンライン プラットフォームを通じて OSS コミュニティと積極的に関わり、対話、コラボレーション、知識交換を促進します。

プレミア メンバー

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

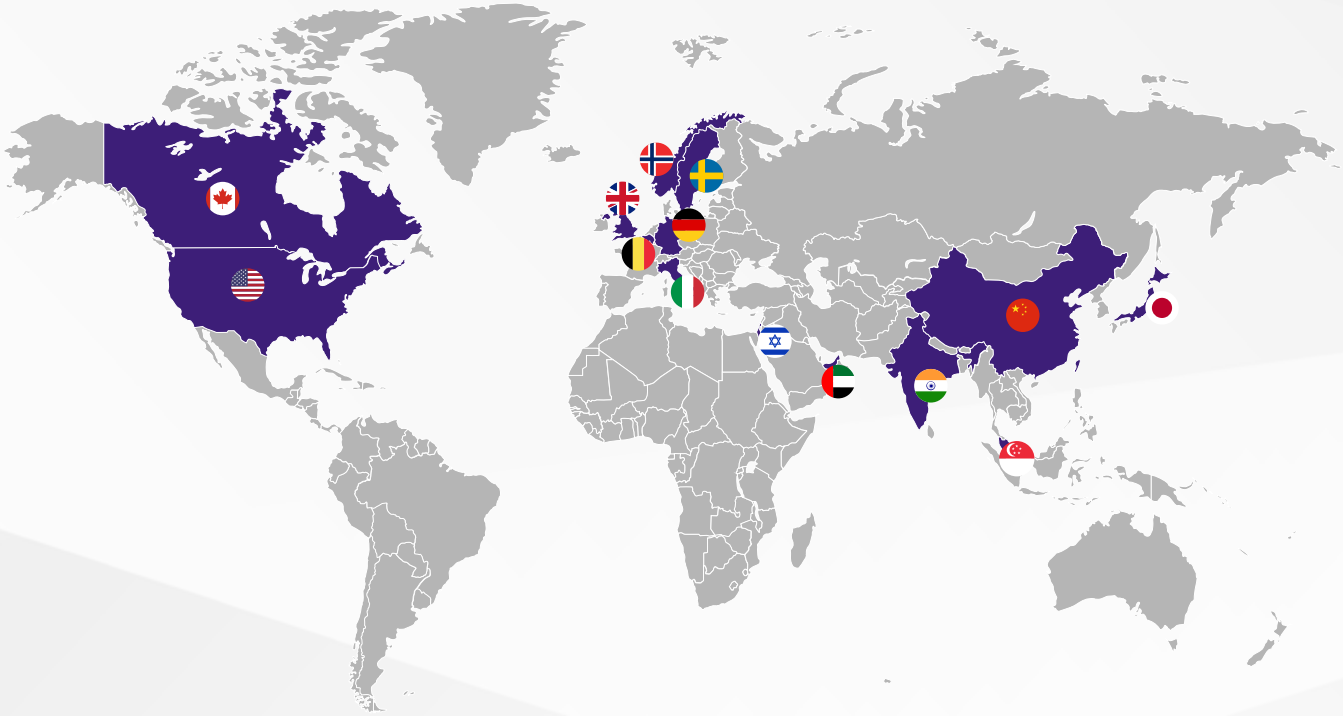
ゼネラル メンバー

ACCUKNOX, Airbyte, aiven, Akamai, Alibaba, amesto Fortytwo, ANACONDA, anchore, apiiro, arnica, ATLASSIAN, AURISTOR, BLOCK, Bloomberg Engineering, boost security.io, CHAINGUARD, Checkmarx, cloudsmith, code intelligence, CodeThink, coinbase, COMCAST, controlplane, cybertrust, cycode, DeployHub, DTCC, docker, ENDOR LABS, ensignia, f5, Fidelity INVESTMENTS, FOSSA, FUTUREWEI Technologies, GitLab, Goldman Sachs, hackerone, HITACHI, JFrog, KASTEN by Veeam, KUSARI, LEGIT, LOCKHEED MARTIN, mend.io, NUTANIX, patchstack, privado, RENESAS, REVERSING LABS, salesforce, SAP, SCANTIST, Scotiabank, SECTREND, SHEBASH, shopify, SlimAI, snyk, Socket, SPARKFABRIK, Spotify, STACKHAWK, stacklok, SUSE, SUZUKI, sysdig, TII Technology Innovation Institute, tenable, Tencent 腾讯, TESTIFYSEC, TIDELIFT, timesys, TRAIL of BITS, VicOne, 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, OpenUK, PURDUE UNIVERSITY, python SOFTWARE FOUNDATION, Rust Foundation, SAFECode, TODO

メンバーの地理的分布



メンバーの産業分野

ガバニング ボード メンバー

ANDREW VAN DER STOCK
Executive Director, OWASP Foundation

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

BRIAN FOX
CTO, Sonatype

CHRISTOPHER "CROB" ROBINSON
OpenSSF TAC Chair & Director of Security Communications, Intel

CLYDE RODRIGUEZ
Vice President of Engineering, Meta

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

ERIC BREWER
VP of Infrastructure & Google Fellow, Google

JAMIE THOMAS (2023 BOARD CHAIR)
GM, Technology Lifecycle Services, and IBM Enterprise Security Executive

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

JOHN HEIMANN
Vice President, Security Programs, Oracle

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

KELLY ANN
Cloud Infrastructure Security Engineer, Apple

KIT COLBERT
Chief Technology Officer, VMware

LUKE HINDS
Independent, Security Community Individual Representative

MARK RUSSINOVICH
Azure CTO and Technical Fellow, Microsoft

MARK RYLAND
Director, Office of the CISO AWS Security

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

RAO LAKKAKULA
Executive Director, JPMorgan Chase

STEPHEN AUGUSTUS
Head of Open Source, Cisco

STEPHEN CHIN
VP of Developer Relations, JFrog

SUBHA TATAVARTI
CTO, Wipro

VINCENT DANEN
Vice President of Product Security, Red Hat

2023 年 ガバニング ボード メンバー 代表のことば

オープンソースのエコシステムそのものがそうであるように、OpenSSF は多忙な 2023 年に成長し、進化してきました。今日、誰もがオープンソース ソフトウェアに依存していることは、もはや議論の余地がありません。最大のオープン ソフトウェア リポジトリからの調査によると、オープンソース ソフトウェアは、現代のソフトウェア サプライ チェーンのほとんどすべてを支えています。

2023 年を通して、技術エコシステムにおけるより広範な課題にもかかわらず、OpenSSF は重要なマイルストーンを達成し、認知度を高め、オープンソース ソフトウェア エコシステム全体のセキュリティを向上させながら、勢いをつけてきました。私たちの取り組みの中心にあるのは、常にオープンソース ソフトウェアの開発者を念頭に置くことです。彼らをサポートし、彼らのワークフローにセキュリティを組み込むことを容易にする革新的な方法を見つけなければなりません。

この分野を前進させるには、明確な考え、適切なレベルのリソース、そして決意が必要です。私たち全員が自分の役割を果たす必要があり、特に 2023 年の間、惜しみなく貢献してくれた人材、ブランド支援、財源に対するオープンソース セキュリティ財団の各メンバーに感謝したいです。

2023 年のハイライトをいくつか紹介させてください。

- **ソフトウェアセキュリティ教育とセキュリティガイドライン：**2023 年 8 月現在、20,000 人以上の開発者が、安全なソフトウェア開発の基礎に関する OpenSSF のコースを受講しています。また、私たちのコミュニティは、より安全なソフトウェア開発を支援するベスト プラクティスの改善を支援するために、開発者、利用者、セキュリティ コミュニティ向けのさまざまなガイドを共同で作成しています。
- **オープンソース ソフトウェアの評価と基盤の改善：**オープンソース ソフトウェア（OSS）のセキュリティを利用者やメンテナーがより効率的に評価できるように、オープンソース ソフトウェア パッケージに関するセキュリティ情報の入手を簡素化しました。以下に 3 つの例を示します：
  - **OpenSSF スコアカード**—OSS プロジェクトを様々なソフトウェア セキュリティ基準に照らして自動的に評価します。OSS の利用者が OSS のセキュリティを推定するのに役立つスコアが作成され、スコアを向上させる目標を与えることでメンテナーを支援します。最近の改良点として、GitHub に加えて GitLab にも対応しました。
  - **ソフトウェア アーティファクトのためのサプライ チェーン レベル（SLSA）**—SLSA は、改ざんを防ぎ、完全性を向上させ、パッケージとインフラを安全にするためのフレームワークです。SLSA バージョン 1.0 は今年 4 月にリリースされ、ソフトウェアのビルド プロセスの保護に焦点を当てています。
  - **Sigstore**—Sigstore は、ソフトウェアのサプライ チェーン セキュリティを向上させるオープンソース プロジェクトです。Sigstore フレームワークとツールは、ソフトウェア開発者と利用者がリリース ファイル、コンテナ イメージ、バイナリ、ソフトウェア部品表（SBOM）などのソフトウェア アーティファクトに安全に署名し検証できるようにします。

2023 年 ガバニング ボード メンバー 代表のことば

- さらに、ソフトウェア リポジトリのセキュリティ向上、脆弱性の発見と報告の強化、セキュリティ監査への資金提供、OS のセキュリティ研究などの分野でも成果を上げています。

また、この 9 月にワシントン D.C. で主要政府機関の代表者とのフォローアップ会合を開催し、大成功を収めました。国家安全保障会議（NSC）、国家サイバー長官室（ONCD）、サイバーセキュリティ社会基盤安全保障庁（CISA）などの米国政府関係者が、民間企業のリーダーたちとともに出席し、前回の会合以降の進捗状況を確認しました。

オープンソースソフトウェアは、民間部門と公共部門の両者で利用される、かけがえのないデジタル公共財であるという新たなコンセンサスを聞くことができ、非常に勇気づけられました。また、オープンソース ソフトウェアから恩恵を受ける人々は、オープンソース エコシステムを積極的に直接支援する必要があること、または支援する他者から OS ソフトウェアを入手する必要があることでも意見が一致しました。私たちは、世界中の主要な政府機関と引き続き協力し、それぞれの政府機関独自の視点に配慮しつつ、共通の懸念事項を理解してもらうよう努めます。

2024 年に向けて、人工知能（AI）、機械学習（ML）、そしてオープンソース役割が利用される機会や課題が前面に出てくるようになってきました。この分野もまた、コミュニティ間の協力が鍵となる分野です。特に、OpenSSF のメンバーが Linux Foundation の姉妹組織である LF AI&Data と協力し、知識を共有し、より安全な未来を提供するためにサブジェクト マター エキスパート（SME）[JB1] を集めようとしていることに勇気づけられています。これもまた、官民の幅広い協力が不可欠な分野です。

個人的なことですが、理事長として 2 年目の任期を終えることになりました。OpenSSF の創設期にゼネラル マネージャーを務めた Brian Behlendorf 氏に感謝するとともに、今年半ばにこのイニシアチブを次のレベルに引き上げるために就任した Omkhar Arasaratnam 氏を再びゼネラル マネージャーとして迎えたいと思います。この 2 年間、OpenSSF の理事長を務めさせていただき、大変光栄に思っております。そして、2024 年にはさらに大きな成果を上げる音を楽しみにしています。まだメンバーでない方は、ぜひご入会ください。

敬具

Jamie Thomas
Chair of the OpenSSF Governing Board
GM, Technology Lifecycle Services, and IBM Enterprise Security Executive

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2023 年のハイライト


OpenSSF Day Europe

ソフトウェアセキュリティ教育

- 22,000 人を超えるソフトウェア開発者が安全なソフトウェア開発の基礎に関するコースに登録し、1,000 人以上が Sigstore を使用したソフトウェア サプライ チェーンの保護に関するコースに登録しています。
- DEI Special Interest Group は、OSS セキュリティの新人を指導するための「オフィス アワー」プログラムを開始し、ワーキング グループになりました。
- サイバーセキュリティ トレーニングの深さと範囲を拡大するために、Linux Foundation Training and Certification、ISC2、および OpenSSF のコラボレーションを発表しました。

セキュリティガイド

複数のガイドがリリースまたは更新され、開発者、利用者、セキュリティ コミュニティのセキュリティ対策の強化に役立ちました。

- より安全なソフトウェアを開発するための簡潔なガイド
- オープンソース ソフトウェアを評価するための簡潔なガイド
- ソースコード管理プラットフォーム構成のベスト プラクティス
- オープンソース プロジェクトとして CVE 番号付け機関になるためのガイド
- C および C++ のコンパイラ オプション強化ガイド

OSS セキュリティ評価

- OpenSSF スコアカードは、さまざまなソフトウェア セキュリティ基準に照らして OSS プロジェクトを自動的に評価し、現在では 100 万を超える OSS プロジェクトに対して毎週スコアカード スキャンを実行しています。最近では（GitHub に加えて）GitLab のサポートを追加しました。
- Allstar は、開発中の組織またはプロジェクト内でスコアカードの使用を合理化するのに役立つ補完的な取り組みです。
- OpenSSF ベスト プラクティス バッジは、OSS プロジェクトが取り組みをより深く評価するために使用できるセキュリティと維持の基準を示します。今年は 6,300 を超える参加プロジェクトがあり、新しい領域に移行しました。

- Supply-chain Levels for Software Artifacts（SLSA）は、改ざんを防止し、整合性を向上させ、パッケージとインフラストラクチャを保護するためのフレームワークです。ビルド プロセスの保護に重点を置いた SLSA バージョン 1.0 を 2023 年 4 月にリリースしました。SLSA はその後、パッケージの整合性を確保するために npm によって採用されました。
- セキュリティ レビューコレクション。私たちは、OSS の一連の既知のセキュリティ評価を収集し、他の人がこの情報をすぐに見つけて確認できるようにしました。
- セキュリティ インサイトの仕様。私たちは、メンテナンス担当者がプロジェクトのセキュリティ プロセスを機械処理する方法を提供するため、新しい仕様の v1.0 をリリースしました。

改良された OSS インフラとツール

- Sigstore は、アーティファクトのデジタル署名と検証を提供します。Sigstore は、CPython、Kubernetes のアーティファクトのリリースの署名に使用され、npm パッケージのプロベナンスの一部として使用されています。Sigstore の使い方に関する無料講座もあります。Sigstore のパブリック署名の透明性ログ内の署名には、5,200 万件を超えるエントリが記録されており、その範囲は Kubernetes、CPython、LLVM、KNative、Istio、ArgoCD を含む 22,000 を超えるユニークな OSS プロジェクトに及びます。
- **安全なソフトウェア リポジトリ。**私たちはパッケージ マネージャーのセキュリティ ランドスケープ調査を実施してセキュリティ機能を比較しました。そしてそれをもとに、リポジトリ全体の改善を促進するために、すべてのパッケージ レジストリのビルド プロベナンスに関するガイダンスを開発しました。
- **より優れたツール。**OpenSSF は、SBOM の取り扱いを改善するために spdx/tools-python に資金を拠出し、これが Python SPDX-Tools パッケージの 0.7.0 リリースにつながりました。Fuzz Introspector は、攻撃者が脆弱性を見つける前に検出できるようファズ テストとファズ テスト ツールを改善するために設計され、C、C++、Java、Python を統合サポートするようになりました。
- 悪意のあるパッケージに関するリポジトリは、悪意のあるパッケージのクロスエコシステム レポートを収集および公開するためのオープンソース システムです。

脆弱性の発見と報告

- Alpha-Omega。アマゾン ウェブ サービス、マイクロソフト、グーグルから 1,320 万ドル以上が提供された Alpha-Omega プロジェクトは、最も重要なオープンソース プロジェクトとエコシステム内で持続可能なセキュリティの向上を促進するために活動しています。Alpha-Omega は、重要で広く使用されているオープンソース プロジェクトである Python Software 財団（Python security ディベロッパーインレジデンスへの資金提供を含む）、Node.js、jQuery、Eclipse 財団、Homebrew、および Rust 財団と緊密に連携してします。
- **セキュリティ監査。**私たちは、Alpha-Omega や OSTIF とのパートナーシップを通じて、広く使用されている OSS の詳細なセキュリティ監査をサポートしてきました。これらの監査には、OpenSSL 3.1.0 およびさまざまな Eclipse プロジェクト（p2、Mosquitto、Jetty、jKube）が含まれます。また、Alpha-Omega を通じて、OpenRefactory などの組織と協力して、何百ものオープンソース プロジェクトにわたる脆弱性を特定して修正してきました。

- オープンソース脆弱性（OSV）スキーマは、脆弱性とオープンソース パッケージのバージョンまたはコミット ハッシュとの正確なマッピング情報を機械が読める形式にしたもので、現在 18 のエコシステムで使用されており、最近追加された AlmaLinux、Rocky Linux、および Haskell プログラミング言語も含まれます。

研究と出版物

- OpenSSF ソフトウェアのセキュリティ意識調査で LF Research と提携し、一連の重要な OSS プロジェクトの改良を続けています。
- LF Energy との共同ホワイトペーパーを発行しました：エネルギーインフラにおけるサイバーセキュリティ：オープンソースソフトウェアの価値

公共部門への参画

- OpenSSF は、DARPA AI サイバー チャレンジ（AIxCC）のチャレンジ アドバイザーを務めており、重要なインフラやソフトウェア サプライ チェーンのセキュリティなど、重要なサイバーセキュリティ問題に対処できる AI システムの構築においてチームを指導しています。
- 9 月のセキュア オープンソース ソフトウェア サミットに、国家安全保障会議（NSC）、国家サイバー長官室（ONCD）、およびサイバーセキュリティ・社会基盤安全保障庁（CISA）の米国政府関係者と業界リーダーを集め、重要インフラの安全性の確保について協力しました。
- 米国ホワイトハウスの国家サイバー長官室（ONCD）とオープンソース ソフトウェア セキュリティ イニシアチブ（OS3I）のパートナーからの、オープンソース ソフトウェア（OSS）のセキュリティとメモリ セーフ プログラミング言語に関する情報提供要請（RFI）に回答しました。

コミュニティ構築と支援

- カナダのバンクーバーで OpenSSF Day North America、スペインのビルバオで OpenSSF Day Europe、そして東京で OpenSSF Day Japan を開催しました。これらのイベントには、オープンソースのメンテナー、作成者、利用者からなるグローバル コミュニティが集まり、OSS サプライ チェーンのセキュリティ確保における課題、大局的な解決策、進行中の作業、成功事例について話し合いました。
- OpenSSF リソースの使用を促進するために、グローバル OSS コミュニティでローカル ミートアップを開催しました。
- 数多くの OpenSSF の取り組みが、ニュース記事、ウェビナー、ポッドキャスト、業界カンファレンスで取り上げられています。
- 新しいセキュリティ求人掲示板を立ち上げました。


OpenSSF Day North America

テクニカル アドバイザリー カウンシル（TAC）代表のことば

2023 年という素晴らしい一年を終えることができました!

技術諮問委員会（Technical Advisory Council：TAC）としての私たちの役割は、OpenSSF の全体的な技術ビジョンを開発し、すべての技術的取り組みを通じたコラボレーションを構築し、促進することです。今年も、活発なワーキング グループやプロジェクトから、数多くの素晴らしい成果や取り組みが生まれました。リストは長くなりますが、ハイライトをいくつか挙げてみましょう：

- 22,000 人以上の開発者が安全なソフトウェア開発教育コースに登録しました
- いくつかのベスト プラクティス ガイドを公開および更新しました
- OpenSSF スコアカードなどの既存の取り組みを改善しました
- ソフトウェア部品表（SBOM）の普及と使いやすさを向上させるためのツールに資金を提供しました

これらの取り組みには共通点が 1 つあります。それは、オープンソース コミュニティのメンバーに利益をもたらし、メンバーの参加を促すように設計されているということです。すべてのワーキング グループは、どんなに技術的なものであっても、自分の経験に基づいた意見を持っている人なら誰でも参加できます。私たちの取り組みはソフトウェアを構築するだけではなく、オープンソース エコシステムの状態を理解し、デフォルトでコードの安全性を容易に構築することができるガイドラインとプロセスを開発することにも努めています。

今年の 4 月に私たちは TAC のメンバーを決め、欠員が生じた場合には年間を通じて新しいメンバーを任命しました。これまでのサポートに対する Aeva Black と Dan Lorenc の両名に感謝するとともに、OpenSSF とコミュニティへの貢献に対して新たに加わった Michael Leiberman と Daniel Appelquist に感謝します。また、プロジェクト、ワーキング グループ、その他の OpenSSF の取り組みでのすべての作業を通じて、エコシステムのセキュリティを毎日確保するのに貢献してくださっている素晴らしいメンバーと参加者の皆様にも感謝します!

2024 年にはさらに多くの取り組みが行われ、これらの取り組みがさらに強化されることを楽しみにしています!

Christopher “CRob” Robinson
TAC Chair
OpenSSF

TAC メンバー

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
Directory of Security Communications, Intel

DAN APPELQUIST
Open Source & Open Standards Strategy Director, Snyk

DUSTIN INGRAM
Staff Software Engineer at Google Open Source Security Team

MICHAEL LIEBERMAN
Co-Founder & CTO, Kusari

ZACH STEINDLER
Principal Engineer, GitHub

Linux Foundation Member Summit

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

この育成中のワーキング グループは、人工知能／機械学習（AI ／ ML）とセキュリティが両立する OSS のセキュリティ問題に対処するために取り組んでいます。

これには、OSS、メンテナー、コミュニティ、およびその採用者に対する AI ／ ML 技術のセキュリティ上の影響への対処や、OSS プロジェクトが大規模言語モデル（LLM）を含む AI ／ ML をどのように安全に、あるいは効果的に活用してセキュリティ体制を向上させることができるかも含まれます。

公正さ、正確さ、知的財産の観点から AI を「保護」する必要があります。これらは通常のセキュリティの範囲外ではあるものの、極めて重要です。

また、（LLM を含む）AI ／ ML の興奮の中で、人々は安全な慣習を（もし持っていたとしても）捨て去ろうとしているようにも思います。警戒心を捨て去ると安全なシステムが構築できるとは思えません。

GitHub リポジトリ	ワーキング グループ リーダー	定期貢献者の数
github.com/ossf/ai-ml-security	Jay White Mihai Maurseac	5-15

2023 年のハイライト

- 今年は自己研鑽の年であり、テクノロジー業界の急速に変化する部分に対応するアプローチを検討した年でした。

次のステップ

- グループとして何を達成できるかをさらに掘り下げます。私たちは現在手始めとして、AI ／ ML に対するセキュリティ体制について企業と選択的かつ直接的に協力することを計画しています。

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 プラクティスに関する推奨事項と、それを学習して適用する簡単な方法を提供するために活動しています。

ワーキング グループ リーダー	定期貢献者の数
CRob	20-30

GitHub リポジトリ
github.com/ossf/wg-best-practices-os-developers

2023 年のハイライト

- ブログにソース コード管理ベスト プラクティス ガイドの作成
- C/C++ コンパイラ強化オプション ガイドの作成
- ベスト プラクティス バッジ プロジェクト のバッジの新しい URL とロゴ、および、Web 用のワーキング グループ資料のプレゼンテーションの改善
- スコアカード 4.12 リリース—アップデートに加え、要望の多かった GitLab 統合も追加!—ブログ
- 安全なソフトウェア開発指導原則 1.0 リリース
- Sterling Toolchain の概念を推進するために Security Toolbelt SIG を採用。これには、安全なオープンソースの作成者と利用者が使用できる一連の望ましい機能のセット、およびオープンソースの制作、構成、配信、使用がどのように攻撃されるかを詳細に説明する一連の脅威モデルの開発（それらのリスクを管理する方法に関するガイダンス付き）とともに、財団全体で使用するための標準的なペルソナの開発も含まれます。
- OSS-NA および OSS-EU で実施した、メンテナーとプロジェクトがベスト プラクティス バッジとスコアカードを統合および採用する方法に関するプレゼンテーション
- 多様性、公平性、包括性（DEI）SIG は、オープンソース開発／サイバーセキュリティに携わろうとしている新しい専門家と交流するために、毎月のオフィス アワーの開催を開始しました。これは最終的に独自のワーキング グループに昇格しました。
- OpenSSF 動員計画の書き換え ストリーム 1—教育
- OpenSSF 動員計画の書き換え ストリーム 4—メモリの安全性

インパクト

BEST WG は、OpenSSF 内で最も星の数が多いリポジトリの 1 つであり（トップ 5!）、コミュニティだけでなくより広範なエコシステムにも非常に広いリーチを持っています。私たちは業界、最終利用者、公共部門、学術機関と協力して、開発者が日常業務に組み込むためのベスト プラクティスやテクニックを厳選して紹介しています。

次のステップ

- なぜ開発ライフサイクル全体を通じてアプリケーション セキュリティの実践とツールを使用する必要があるかという点に着目した開発者マネージャー トレーニング クラスをリリース
- プロジェクトがさまざまな OpenSSF プロジェクトを統合するのに役立つ OpenSSF プロジェクトのトレーニング資料とドキュメントの作成
- 財団全体の取り組みを紹介するためのポッドキャストの作成
- 他の財団のプロジェクトとの連携によるベスト プラクティスのドキュメントやガイダンスとの整合性の確保。そして、ベスト プラクティス バッジなどをプロジェクトのポートフォリオに統合
- それ以外にもいろいろ!

ワーキング グループ

エンドユーザー

このグループは、オープンソースを生産するのではなく、主にオープンソースを利用する官民の組織の利益を代表しています。

ワーキング グループ リーダー	定期貢献者の数
Jonathan Meadows Jacques Chester	8-15

GitHub リポジトリ
github.com/ossf/wg-endusers

2023 年のハイライト

- OSS 利用者向けの脅威モデルを構築するための SIG を立ち上げ、モデルの開発を着実に進めています
- オープンソース消費マニフェストを採用し、取り組みました
- 新しいメンバーを募集するために積極的に連絡を取って、さらに多くのメンバーを見つけようとしています

次のステップ

- すべての主要な業種および地域に確実に参加してもらうため、エンド ユーザーを継続的に採用
- 脅威分類の最終化と OpenSSF による標準としての受け入れ
- 消費アーキテクチャの最終決定と OpenSSF による受け入れ

インパクト

エンド ユーザー WG は、主にオープン ソースを利用する組織の声が確実に反映されるようにします。エンド ユーザーのニーズや問題は、オープンソースの再パッケージ化やオープンソースへ貢献しているオープンソースのメンテナーやベンダーのニーズや問題とは異なる場合があります。

次のステップ

私たちは今後も脅威モデルの開発に取り組み、コミュニティをさらに成長させたいと考えています!

OpenSSF Day North America

ワーキング グループ

メトリクスとメタデータ

このグループは、関連するメトリクスとメタデータを収集、整理、伝達することにより、情報に基づいた OSS のセキュリティの信頼性を実現します。

ワーキング グループ リーダー	定期貢献者の数
Michael Scovetta Luigi Gubello	5-10

GitHub リポジトリ
github.com/ossf/wg-identifying-security-threats

2023 年のハイライト

- リスク ダッシュボードは、OpenSSF スコアカード、OpenSSF ベスト プラクティス バッジ、貢献データ、脆弱性データ、その他の情報からのデータを集約することにより、オープンソースの利用者がリスクを理解できるように関連するメトリクスを提供します。近日中に製品デモを公開する予定です。
- Security Insights は、OSS メンテナーが、プロジェクト内で実施されているセキュリティ体制と実践に関する情報を、人が読める形式と機械が読める形式（YAML）の両方で表現する方法を提供します。リリース v.1.0.0 は 2023 年 10 月に発表されました。
- ドキュメント「オープンソース エコシステムにおける脅威、リスク、および軽減策」で、オープンソース エコシステムのセキュリティ リスク状況についての共通理解を確立しています。2023 年にアップデートをリリースすることに取り組んできました。
- ブログ：OpenSSF による Security Insights 仕様書 1.0 の紹介を公開

インパクト

OSS プロジェクト／パッケージのリスクを人間が理解するためにどのようなメトリクスが重要であるかについての参加と議論が増え、データ駆動型の評価を行うための知識、文書、ツールが提供されます。

次のステップ

- 2024 年にリスク ダッシュボードの最初のバージョンをリリース予定。
- Security Insights1.1 がロードマップにあります。
- 他の WG と協力して、オープンソース エコシステムの脅威に関する、より包括的かつ網羅的な文書をリリース。
- 潜在的な新しいプロジェクトについて定期的に議論。ぜひ会話に参加してください!

OpenSSF Day Europe

ワーキング グループ

重要なプロジェクトの保護

このグループは、私たち全員が依存している重要なオープンソース プロジェクトの安全を保つためのリソースを確保するため特定および支援するために活動しています。

ワーキング グループ リーダー	定期貢献者の数
Amir Montazery Jeff Mendoza	5-10

GitHub リポジトリ
github.com/ossf/wg-securing-critical-projects

2023 年のハイライト

- 私たちは一連の重要なオープンソース プロジェクトの最新のイテレーションを完了しました。リストはこのリンクからご覧いただけます。これをまとめるには、作業グループ内での分析、調査、および議論が必要でした。私たちは、criticality_score や Census II プログラムのデータ、OSTIF の管理する監査プログラムの結果など、さまざまなデータやツールに基づきパッケージをランク付けしました。
- 悪意のあるパッケージのクロスエコシステム レポートを収集および公開するための初のオープンソース システムである、悪意のあるパッケージ リポジトリを立ち上げました。（ブログ投稿）
  - » Checkmarx、Google オープンソース セキュリティ チームからの寄稿。GHSA からのマルウェア レポートも取り込んでいます。
- Package Analysis はアーカイブ目的でパッケージのアーティファクトを保存するようになりました。

インパクト

- Allstar は現在、427 を超える GitHub 組織／インストールにおいて 36,600 のリポジトリを保護しています
- 悪意のあるパッケージ リポジトリには、以下を含む 16,000 のデータ ポイントが含まれています。
  - » npm から 9,000 例、pypi からの 6,500 例、および rubygems と crates.io からのいくつかの例が含まれています
- Package Analysis プロジェクトは昨年 500 万件以上のパッケージを分析しました
  - » PyPI：100 万件
  - » RubyGems：82,000 件
  - » Packagist：226,000 件
  - » NPM：350 万件
  - » Crates.IO：209,000 件

次のステップ

- 私たちは、これらの重要なプロジェクトの普及と、これらの重要なプロジェクトをサポートすることの影響をよりよく理解できるように、OpenSSF およびより大きなオープンソース コミュニティ内の一連の重要なプロジェクトのユースケースを調査しています。たとえば、10,000 個のパッケージのリストでは Alpha-Omega との連携が緊密になります。
- また、一連の重要なオープンソース プロジェクトを情報収集、取り込み、保守するためのシステムの開発も開始しています。その意図は、より自動化され、ワーキング グループによる維持管理が少なくて済む方法で、一連のプロジェクトを継続的に精選し更新できるシステムを開発することです。
- 悪意のあるパッケージ リポジトリの今後の改善点は次のとおり。
  - » OSV レポートに含めることができるメタデータの仕様を拡張
  - » サンプルを OSV レポートに関連付けてダウンロードする機能
  - » 新しい情報源と利用者を探索
- Package Analysis
  - » HTTP/HTTPS 動的分析コレクションを完了
  - » GCS と BigQuery による静的解析データを収集して提供
  - » ファイルシステムのスナップショットをサポート
  - » 動的解析のための Windows 環境のシミュレーション
- 重要度スコアについては、GitHub Search API の問題を回避して、定期的に再実行できるようにします。
- ハーバード大学と協力して Census II を更新し、広く使用されている OS を定量的に特定する「Census III」を作成します。

ワーキング グループ

ソフトウェア リポジトリのセキュリティ保護

このグループは、ソフトウェア リポジトリを強化および保護するための新しいツールとテクノロジの導入について、協調するための環境を提供します。

ワーキング グループ リーダー	定期貢献者の数
Dustin Ingram Zach Steindler	20 - 30

GitHub リポジトリ
github.com/ossf/wg-securing-software-repos

2023 年のハイライト

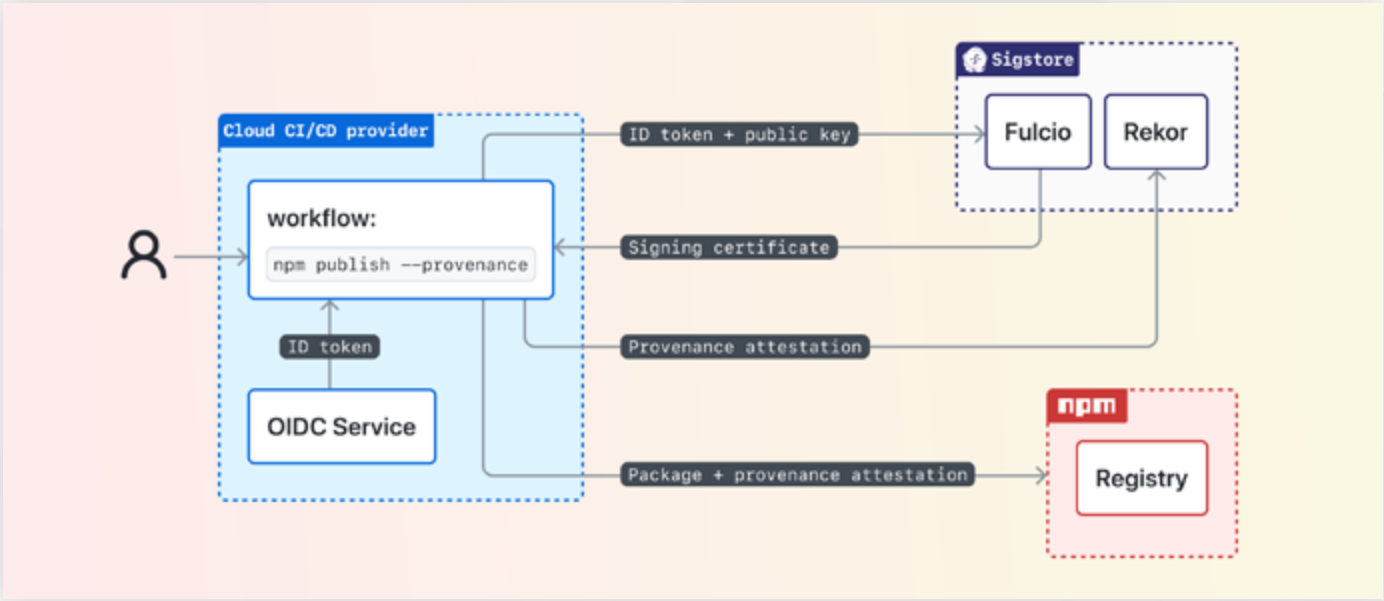
- すべてのパッケージ レジストリのビルド プロベナンスを公開し、ビルド プロベナンス採用を促進することで、オープンソースの利用者がパッケージの生成にどのようなソース コードとビルド手順が使用されたかを正確に知ることができるようになりました。
- Homebrew がプロベナンスとコード署名を構築するための資金を獲得できるよう支援しています。
- パッケージ マネージャーの管理者がセキュリティ機能に関するベスト プラクティスやアドバイスを交換するためのフォーラムを提供し続けました。

インパクト

- 現在、約 4,000 の npm パッケージが SLSA ビルド プロベナンスとともに公開されています。

次のステップ

- パッケージ マネージャーのセキュリティ ロードマップをブレインストーミングから公開まで進める
- 関心のあるパッケージ管理者が、セキュリティ ロードマップを前進させるためにフルタイムのセキュリティ ロールの資金を獲得できるように支援する（現在 RubyGems と協力しています）
- TUF のリポジトリ サービスの開発をサポートし、パッケージ マネージャー全体での導入を促進することで、オープンソース パッケージの利用者がキーを信頼してパッケージの署名を検証できるようにします。



ワーキング グループ

セキュリティ ツール

このグループの使命は、オープンソース開発者に最高のセキュリティ ツールを提供し、誰でもアクセスできるようにすることです。

ワーキング グループ リーダー	定期貢献者の数
Ryan Ware	12

GitHub リポジトリ
github.com/ossf/wg-security-tooling

2023 年のハイライト

- SBOM Everywhere は、コミュニティがすでに SBOM で行っていることを調査し、より多くのプロジェクトが SBOM を組み込むのを支援するための適切なハンドブックを作成することに継続的に焦点を当てます。
- SBOMit はサンドボックス プロジェクトとして WG に導入されました。
- Ryan Ware が新しい WG 議長になりました。

方向性

ワーキング グループは、次の分野に焦点を当てて憲章を改訂するプロセスを進めています。

- オープンソース コミュニティが苦戦を続けているセキュリティ標準化の分野に合意をもたらすことに引き続き注力する。SBOM Everywhere はこの取り組みの好例であり、私たちはオープンソース コミュニティからの需要に応じてこの分野での取り組みを拡大し続けます。
- オープンソース コミュニティと開発者の両者に、一定のセキュリティ対策が必要な理由を理解し、それらを現在の開発パイプラインに簡単に組み込むためのツールとガイダンスをもたらすためのリソースを提供します。
- 他の WG が目標達成のために必要なツールを作成する際に「実際にキーボードを操作」して、必要に応じてサポートします。

アクティブなプロジェクト

- Fuzz Introspector：OSS-Fuzz は現在、合計 1186 件のオープンソース プロジェクトを継続的にファジングしています。プロジェクトはコード カバレッジ分析と Fuzz Introspector ツールによって分析され、これらのいずれかのビルドが成功したデータのみが表示されます。
- SBOM Everywhere：Istio、Snyk、EVE-OS、Yocto などの組織による実際の SBOM の使用状況をレビューします。オープンソース プロジェクトと直接連携して、セキュリティのための SBOM ユースケースを計画します。
- SBOMit：追加の検証情報を使用してコンポーネントを証明するための、SBOM 形式に依存しない方法。これらの証明書は、サプライ チェーンの生成時に生成されます。

ワーキング グループ

サプライ チェーンの完全性

このグループは、人々が維持、作成、使用するコードの出所を理解し、意思決定できるよう支援しています。

ワーキング グループ リーダー	定期貢献者の数
Isaac Hepworth Jay White	30

GitHub リポジトリ
github.com/ossf/wg-supply-chain-integrity

2023 年のハイライト

- SLSA v1.0 仕様の発表
- npm がプロベナンスに SLSA を採用
- gittuf がプロジェクトとして追加
- GUAC がプロジェクトとして追加
- コンテナベースの SLSA3 ビルダー
- ワーキング グループによるサプライ チェーン インテグリティのビジョン、優先順位、方向性の採択
- S2C2F1.0 の受け入れと採用が増加。Intel、Dell によってレビューされており、安全なオープンソースの使用と依存関係の管理を評価するためにさまざまなコンサルタントによって使用されています。
- S2C2F は、オープンソース コンポーネントの安全な使用を確保するための共通フレームワークとして NIST と CISA に認められました

インパクト

- SLSA は、ソフトウェア サプライ チェーンの出所とビルドの整合性を示す事実上の標準になりつつあります
- S2C2F は、オープンソースの利用と依存関係を安全に管理するための標準になりつつあります

次のステップ

- 更なる SLSA の追跡：ソース、依存関係…
  - » SCI での私たちの目標（ssci.io/sci-future を参照）は、「キーとなる機能領域をカバーする実用的なサプライ チェーン セキュリティ フレームワーク」を「構築、証明、依存関係、ソース ... の高度な問題空間を人間工学的に分解」して作成することです。
  - » 2023 年、SLSA　v1.0 を立ち上げ、レベル 1 ～ 3 のビルド トラックを導入しました。
  - » 2024 年に向けて、ビジョンに沿って、問題領域をより完全にカバーするために SLSA を拡張する予定です。現在追跡中です：
    - ソースの追跡
    - 依存関係の追跡
    - ハードウェア認証済みプラットフォームの拡張
    - ビルドプラットフォーム操作の拡張
  - » 方向性としては、SLSA の仕様は時間の経過とともに拡張され、サプライ チェーンの完全性に関する懸念のある主要な機能領域をすべてカバーする予定です
- ポリシーの実装例
- サプライ チェーン コントロール プレーンのデモンストレーション ssci.io/control-plane

ワーキング グループ

脆弱性の開示

このグループは、脆弱性の報告とコミュニケーションの推進を支援することで、OSS エコシステムの全体的なセキュリティを向上させています。

ワーキング グループ リーダー	定期貢献者の数
CRob	15-20

GitHub リポジトリ
github.com/ossf/wg-vulnerability-disclosures

2023 年のハイライト

- OSV は、OSS の脆弱性に関する情報のための標準化された機械処理可能な構造と、いくつかの参照ツールを提供します。このスキーマとツールは、GitHub セキュリティ アドバイザリ、PyPI セキュリティ アドバイザリ（Python 用）、Go、Rust など、少なくとも 16 の組織／プロジェクトによって脆弱性情報を共有するために使用されています。
- OpenVEX SIG は、OpenVEX 仕様、Go ライブラリ、およびツールの保守と維持管理をサポートするとともに、より広範な業界の CISA SBOM ／ VEX の取り組みと協力して、上流プロジェクトによる VEX の利用を推進し、下流の利用者が取り込んで評価できるように、悪用可能性情報をオープンソース サプライ チェーンに注入します。
- OSS- 北米でのプレゼンテーション—ワーキング グループの代表が「オープンソースにおける脆弱性開示の調整の簡素化」を発表しました。
- OSS- 欧州—ワーキンググループのメンバーはが 2 つのセッションを発表しました。1 つは OSV について、もう 1 つは OpenVEX についてでした。
- ワーキング グループ メンバーの Python Software 財団（PSF）セキュリティ デベロッパ イン レジデンスである Seth 氏は、PSF で同じことを行った経験に基づいて、OSS プロジェクトが CNA になるためのガイドを作成しました。
- OpenSSF アウトバウンド脆弱性開示ポリシーの起草と作成およびあらゆるオープンソース プロジェクトのためのモデルの作成
- OpenSSF 動員計画の書き換え ストリーム 1— オープンソース インシデント対策チーム
- それ以外にもいろいろ!

インパクト

ワーキング グループのプロジェクトと取り組みをめぐる努力は、業界全体で数多く採用され浸透しています。OSV スキーマは、オープンソース プロジェクトが一貫した脆弱性データをシームレスに共有し、CVE などの主要な業界標準と相互運用できる重要な方法となっています。より広範な CISA SBOM および VEX の取り組みに参加する OpenVEX SIG の活動は、オープンソース コミュニティの重要な声をワーキング グループに提供するのに役立ち、ソフトウェアが脆弱性によってどのように影響を受けるかを共有するこの新しい方法を定義し、普及するのに役立ちました。Alpha-Omega セキュリティ デベロッパ イン レジデンスである Seth Larson 氏とのワーキング グループの継続的な協力は、Python コミュニティにリソースを提供するのに役立ち、独自の CNA になって脆弱性管理プロセスをコントロールすることに関心のあるオープンソース プロジェクトのロードマップを開発するのに役立ちました。

次のステップ

- OSS 利用者向け CVD ガイド
- 2024 年 VulnCon への参加
- CVD ガイドのトレーニングを作成

プロジェクト

Alpha-Omega

Alpha-Omega

チーム
Bob Callaway, Henri Yandell, Michael Scovetta, Michael Winser, Michelle Martineau, and Naomi Washington.

Web サイト
alpha-omega.dev

Alpha-Omega は、Microsoft、Google、AWS の資金提供を受けて 2022 年 2 月に設立された OpenSSF の関連プロジェクトです。そのミッションは、最も重要なオープンソース ソフトウェア プロジェクトとエコシステムに対する持続可能なセキュリティの向上を促進することで社会を保護し、重要なオープンソース プロジェクトが安全で、セキュリティの脆弱性が迅速に発見され修正される世界の構築を目指しています。

Alpha-Omega は、2023 年にオープンソースのセキュリティを向上させるために 490 万ドルを超える助成金を発行しました。これらの助成金はオープンソースのセキュリティに大きな影響を与え、Python Software 財団、Eclipse 財団、Rust 財団、Node.js など、最も利用されているオープンソースの言語、エコシステム、プロジェクトを代表する組織のセキュリティ チームの人員確保に貢献しました。これらの助成金は、これらの組織が長年のセキュリティ課題に取り組み、セキュリティ プロセスを改善し、攻撃に対するインフラを強化するのに役立ちました。最も重要なことは、それぞれのコミュニティ内で持続可能なセキュリティ文化を確立するために取り組んできたことです。Alpha-Omega もまた、jQuery、RustTLS、Linux カーネル、Homebrew などのような重要なプロジェクトにおけるセキュリティ監査、バグ修正、限定的な開発作業にも直接資金を提供しています。

Alpha-Omega の助成金と受給者のエネルギー、リーダーシップ、コミットメントの組み合わせは、2024 年においても繰り返し、拡大する価値のある、成功の方程式です。

プロジェクト

Sigstore

Sigstore の使命は、ソフトウェア サプライ チェーン内で使用されるすべてのアーティファクトとメタデータが検証可能で透明性のある整合性とプロベナンスを確保し、利用者が明確な信頼性の決定を行えるようにすることです。

リード	定期貢献者の数
Sigstore TSC (Luke Hinds, Bob Callaway, Trevor Rosen, Priya Wadhwa, Santiago Torres-Arias), Hayden Blauzvern (community chair)	30

GitHub レポジトリ
www.sigstore.dev

2023 年のハイライト S

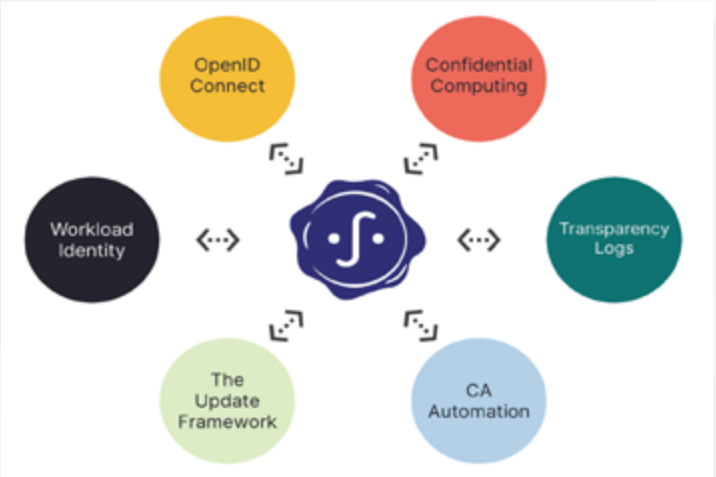
- 2022 年 10 月に公共財サービスとして Sigstore が一般提供
- 一般提供後に 5,200 万件の署名が記録
- 22,000 のユニークな GitHub プロジェクトがアーティファクトと証明書への署名に Sigstore を使用
- npm での Sigstore のサポートは、4 月のパブリックベータ版と 10 月の一般提供版の両方で開始され、ソースとバイナリ アーティファクトをリンクする Sigstore 署名付き SLSA 証明書が可能になった
- GitHub Actions、GitLab、BuildKite、クラウド プロバイダー（AWS、GCP、Azure）、Kubernetes サービス アカウントの Workload Identity サポート
- マルチベンダーによる 24 時間 365 日のオンコール ローテーションにより 99.5% の SLO を維持
- コミュニティ ロードマップの公開

インパクト

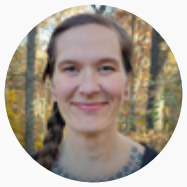
- Sigstore は、OSS ソフトウェア アーティファクトとメタデータの署名と検証の両方において事実上の標準になりつつあります
- Sigstore は npm パッケージ マネージャーの信頼基盤を提供し、より多くのパッケージ マネージャー統合が計画されており、自動署名を利用して Sigstore 署名付き SLSA 証明書をソースとバイナリ アーティファクトにリンクできるようになります
- Sigstore は、Linux Foundation 傘下で最大かつ急速に成長しているオープンソース コミュニティのトップ 25 の 1 つに成長しました

次のステップ

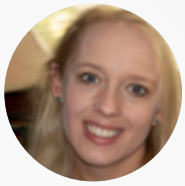
- OSS エコシステムにおける Sigstore 導入の主要なパスとして OSS パッケージ マネージャーに焦点を当てます
- オープン スタンダードを追求します—IETF を介した API、署名認証フォーマットの批准を追跡します
- Sigstore インフラ サービスを公共事業者と民間事業者の両方にとって運用しやすくします
- 学術コミュニティと協力して、より強力な信頼保証とプライバシー保証を提供します
- 検証が署名と同様にシームレスであることを保証します
- より詳細については、Sigstore のコミュニティ ロードマップを確認してください
- Alpha-Omega は Homebrew に資金を提供し、SLSA ビルド プロベナンスと Sigstore コード署名のサポートを追加しました



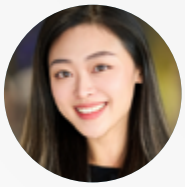
スタッフ



ADRIANNE MARCUM
Technical Program Manager



AMANDA MARTIN
Director of Program Management



ANGELAH LIU
Communications and Marketing Manager

BENNETT PURSELL
Ecosystem Strategist

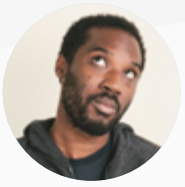
CHEUK TING HO
Community Manager

DANA WANG
Chief Architect

DAVID A. WHEELER
Director of Open Source Supply Chain Security

HARRY TOOR
Chief of Staff

JENNIFER BLY
Senior Marketing & Communications Manager



KHAHIL WHITE
Program Manager

OMKHAR ARASARATNAM
General Manager

RANDI ARMOUR
Membership Solutions

REDEN MARTINEZ
Project Coordinator

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

コミュニティへの参加

SOSS Summit 2023

セキュア オープンソース ソフトウェア（SOSS）サミット 2023

2023 年 9 月 12 ～ 13 日 | ワシントン D.C.

OpenSSF は、セキュア オープンソース ソフトウェア（SOSS）サミット 2023 において、国家安全保障会議（NSC）、国家サイバー長官室（ONCD）、サイバーセキュリティ・社会基盤安全保障庁（CISA）などの米国政府（USG）職員をはじめとする業界リーダーを一堂に集めました。サミットの参加者は、重要インフラ分野およびその他の分野における OSS の利用に関するセキュリティ上の課題について議論し、重要インフラにおける OSS の回復力を確保するために必要な共有責任を強調しました。プレスリリースをご覧ください。

OpenSSF Day イベント

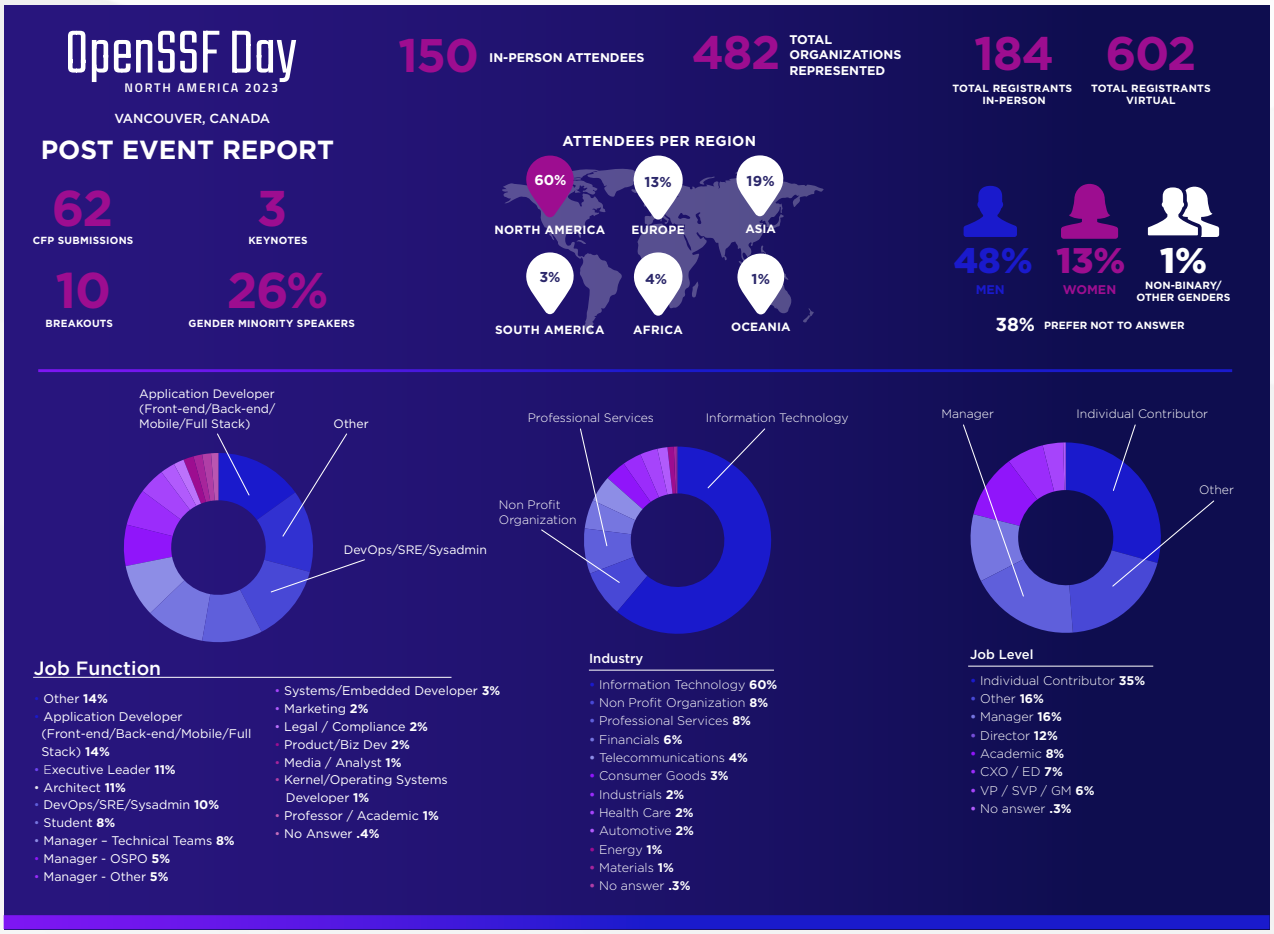
OpenSSF Day では、オープンソース コミュニティが集まり、オープンソース ソフトウェア（OSS）サプライ チェーンのセキュリティを確保するための課題、大局的な解決策、進行中の作業、成功体験について話し合いました。OpenSSF の貢献者や思想的リーダーによる基調講演が行われました。セッションでは、セキュリティのベスト プラクティス、脆弱性の発見、重要なプロジェクトの保護、OSS セキュリティの将来などのテーマに関するプレゼンテーション、パネル、雑談が行われました。

OpenSSF Day
NORTH AMERICA

OpenSSF Day North America

2023 年 5 月 10 日 | カナダ、バンクーバー

イベントの概要と議題のハイライトを表示

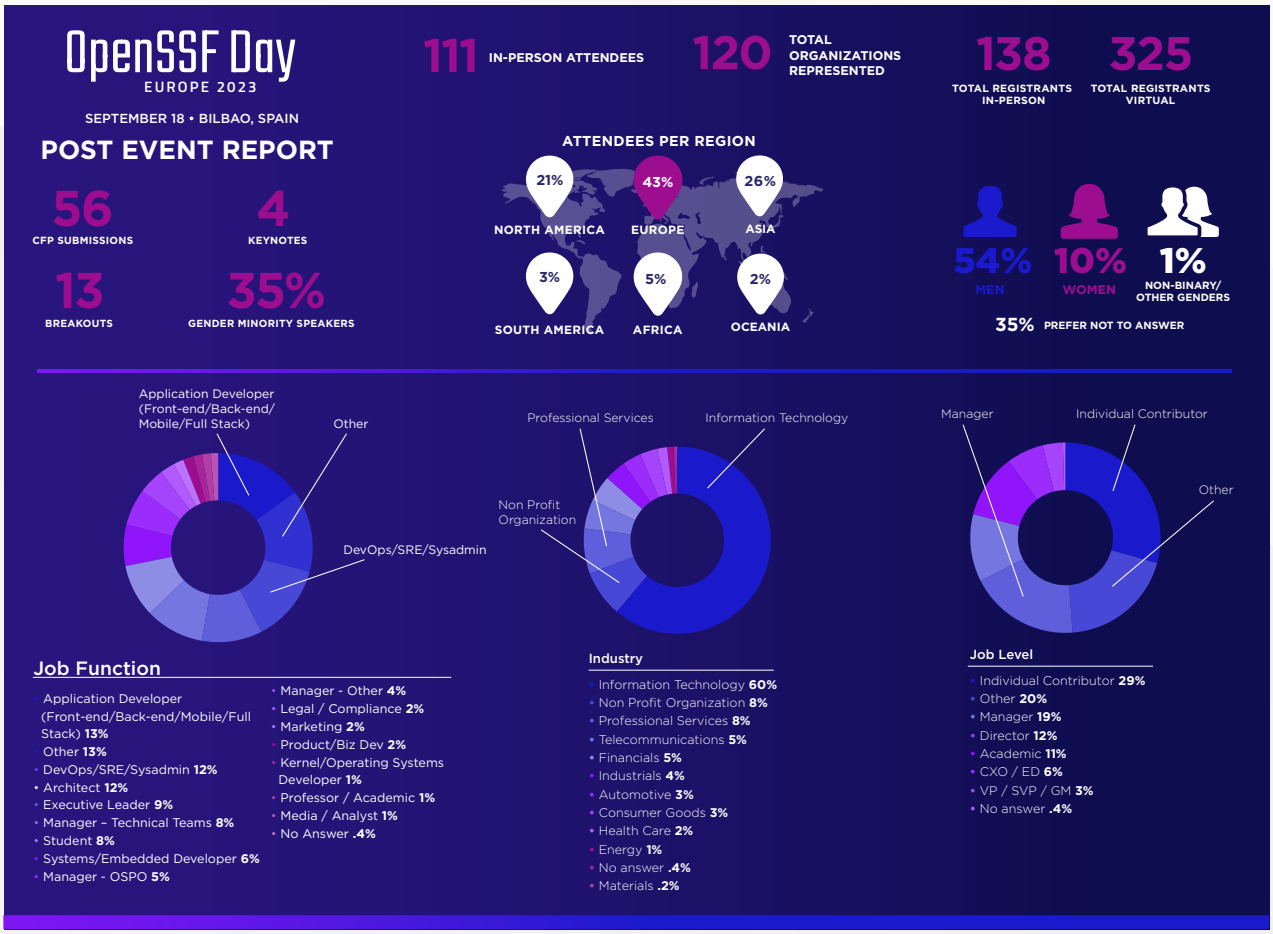


OpenSSF Day
EUROPE 2023

OpenSSF Day Europe

9 月 18 日 | スペイン、ビルバオ

イベントの概要と議題のハイライトを表示



OpenSSF Day
JAPAN

OpenSSF Day Japan

12 月 4 日 | 東京

イベントの概要と議題のハイライトを表示

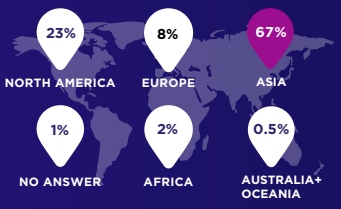
OpenSSF Day
JAPAN 2023
TOKYO, JAPAN

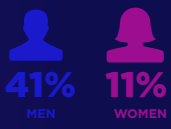
POST EVENT REPORT

20 CFP SUBMISSIONS
2 KEYNOTES
13 PANBELS+TALKS
20% GENDER MINORITY SPEAKERS

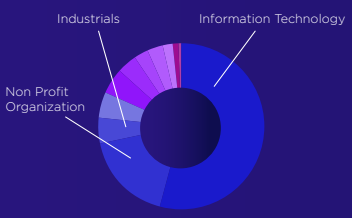
207 IN-PERSON ATTENDEES
185 TOTAL ORGANIZATIONS REPRESENTED
58% OF ATTENDEES IN TECHNICAL POSITIONS

ATTENDEES PER REGION



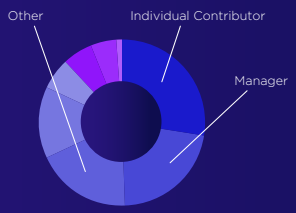


48% PREFER NOT TO ANSWER



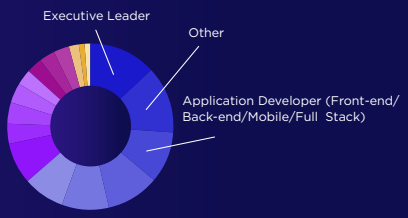
Industry

- Information Technology **55%**
- Non Profit Organization **18%**
- Industrials **5%**
- Automotive **5%**
- Professional Services **5%**
- Telecommunications **4%**
- Consumer Goods **3%**
- Financials **3%**
- No answer **2%**
- Energy **1%**
- Health Care **0.5%**



Job Level

- Individual Contributor **28%**
- Manager **22%**
- Other **19%**
- Director **14%**
- CXO / ED **6%**
- VP / SVP / GM **6%**
- Academic **5%**
- No answer **1%**



Job Function

- Executive Leader **13%**
- Other **13%**
- Application Developer (Front-end/Back-end/Mobile/Full Stack) **10%**
- Systems/Embedded Developer **10%**
- Manager - Technical Teams **9%**
- Manager - OSPO **8%**
- Architect **8%**
- Manager - Other **4%**
- Legal / Compliance **4%**
- Kernel/Operating Systems Developer **4%**
- DevOps/SRE **3%**
- Marketing **3%**
- Product/Biz Dev **3%**
- Professor / Academic **3%**
- Student **2%**
- Media / Analyst **1%**
- No Answer **1%**

ミートアップ

私たちは次の場所でグループを設立しました：ロンドン、バンガロール、シンガポール、ソウル、香港、台北、シドニー、ジャカルタ

DevRel コミュニティ

DevRel コミュニティは、マーケティング委員会の下にある特別な作業グループであり、アウトリーチとコミュニティ構築に焦点を当てています。8 月に開始して以来、指定された Slack チャンネルには 27 人のメンバーがおり、18 人のメンバーが月例定例会に参加しています。

イベント参加

1 月

- SBOM とサイバーセキュリティ
- SchmooCon
- ソフトウェアとサプライチェーン保証フォーラム（SSCA）
- OSPology.live 共有して学ぶ｜オランダ
- OpenI 開発者カンファレンス

2 月

- CloudNativeSecurityCon
- EU オープンソース ポリシー サミット 2023
- FOSDEM
- State of OpenCon
- NIST サイバーセキュリティ フレームワーク（CSF）2.0 ワーキング セッション
- 大西洋評議会ワークショップ
- Big Fix

3 月

- 香港ミートアップ
- オープンソース コンプライアンスとアート ミートアップ
- OpenSSF タウンホール
- 国防総省防衛産業基地 クォータリー サイバー サミット
- エンタープライズ オープンソースのリスク ガバナンス実践サミット
- ソフトウェア サプライチェーンのリーダーシップ シリーズ：Come SLSA with us! ウェビナー
- OSPO サミット

4 月

- ボストン アプリケーション セキュリティ カンファレンス（BASC）
- Devnexus


OpenSSF Day Japan

CloudNatveSecurityCon のブース


Linux Foundation メンバー サミット

コミュニティへの参加

- FOSSASIA
- SoFlo DevCon 南フロリダテックハブ
- RSAC
- AWS Dev Day 香港

5 月

- Devguild Open Source
- オープンソース サミット北米
- OpenSSF Day
- MIT Sloan CIO シンポジウム
- グローバル オープンソース テクノロジー カンファレンス

6 月

- 日本 OSS ミートアップ
- シンガポール OSS ミートアップ
- COPU サミット

7 月

- サプライ チェーン セキュリティ ワークショップ
- SGTech—セキュア パス：DevSecOps 変革プログラム
- オープンソース会議

8 月

- BlackHat
- DEF CON
- EuroSciPy
- ウェブ サマー キャンプ

9 月

- セキュア オープンソース ソフトウェア（SOSS）サミット
- GovTech シンガポール CISO イベント
- オープンソース サミット欧州
- OpenSSF Day Europe
- グレース ホッパー祝賀会
- Secure the Web Forward
- PyCon エストニア
- PyData アムステルダム
- PyCon インド

10 月

- SLSA テックトーク
- Ospology.live ドイツ
- LF メンバー サミット
- PyCon スペイン
- Django Con US
- PyCon APAC

11 月

- 金融フォーラムにおけるオープンソース
- KubeCon+CloudNativeCon 北米
- ACM SCORED
- PyCon 香港

12 月

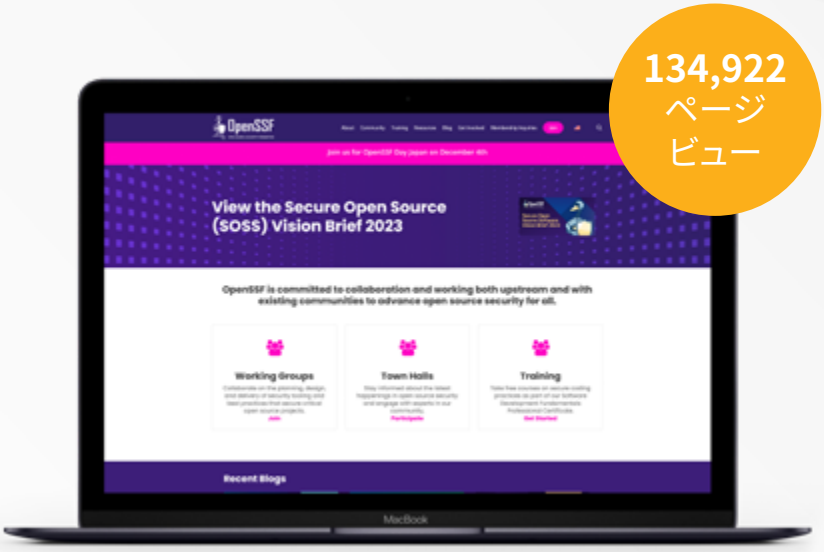
- OpenSSF Day Japan
- オープンソース サミット ジャパン
- Sciwork

OpenSSF Day Europe


Linux Foundation メンバー サミット


Devnexus

Web サイト



134,922 ページビュー

トップ ページ
セキュア ソフトウェア開発基礎コース

トップ プレスリリース

SLSA バージョン 1.0 リリース

トップ ブログ投稿
オープンソース消費マニュフェストを採用しよう

ニュースレター

9,288 登録者
（前年比 +469%）

27.8% 平均開封率

4% 平均クリック率

148,203 総閲覧回数

YouTube

3 月 Town Hall 最多視聴

898 登録者
（前年比 +44%）

9,346 回の視聴

649 時間の視聴

X

トップ記事

4,673 フォロワー
(前年比 +31%)

413 投稿

535,800 インプレッション

2,501 インタラクション

Mastodon

トップ記事

432 フォロワー

193 投稿

LinkedIn

トップ記事

OpenSSF
4,259 followers
1mo ·

"Since OpenSSF hosted the Open Source Software Security Summit II in May 2022, we have seen tangible outputs such as sigstore, which enables secure validation of software, and Alpha-Omega, which finds and fixes vulnerabilities in the most commonly used open source software. There is more to be done in improving integrated tooling to address software supply chain attacks and we look forward to continuing our support of these important initiatives as a founding member of OpenSSF. Securing the open source ecosystem is critical for securing a large enterprise like JPMorgan Chase on behalf of our clients, customers, and the global financial system." - Pat Opet, CISO, JPMorgan Chase & Co.

4,264 フォロワー
(+139% YoY GROWTH)

334 投稿

223,000 インプレッション

5,749 インタラクション

GitHub

853 フォロワー
66 リポジトリ
15 プロジェクト
72 チーム
136 人
3,199 プル リクエスト
726 イシュー

Slack

2,802 ユーザー

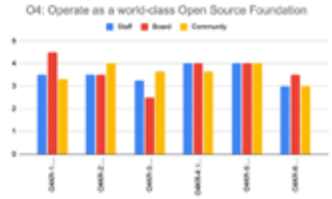
トレーニング

[安全なソフトウェア開発](#) コース
登録者 **22,771** 名

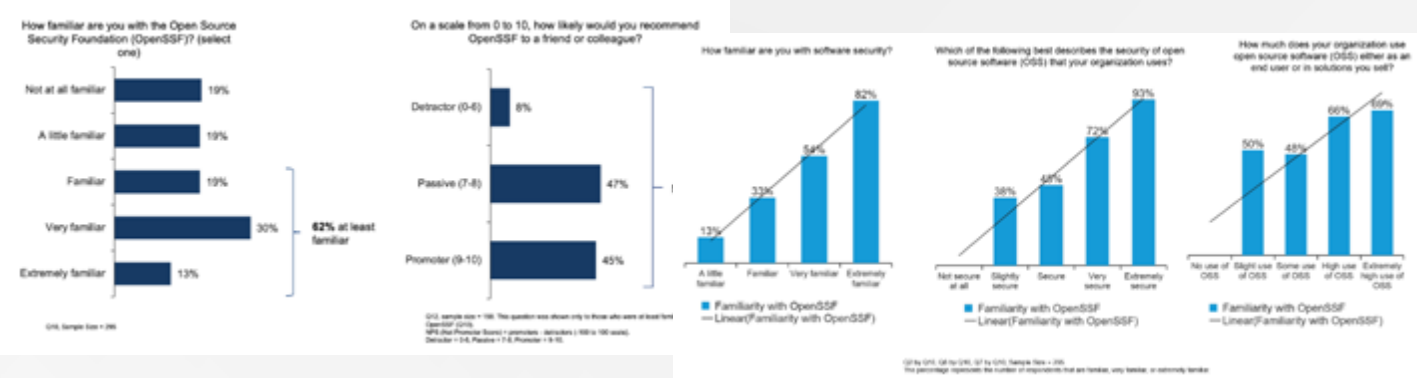
[Sigstore によるソフトウェア サプライ チェーンのセキュリティ確保](#) コース
登録者 **1,263** 名

OKR スナップショット結果

O4: Operate as a world-class Open Source Foundation	
O4KR-1: Governing Board, TAC, and Committees are well-operated, pre-reads provided early, and programmatic support to elevate members' efficiency.	3.7 (+12.1%)
O4KR-2: Events we attend and organize are planned according to a well-defined process driven by the Marketing Committee and leveraging many member organizations.	3.7 (+12.1%)
O4KR-3: Marketing processes are outcome-oriented, understood, and easy to utilize.	3.2 (+14.3%)
O4KR-4: Intellectual property rights are well-managed for visibility, throughput, and defense of contributors, members, and users.	3.9 (+14.7%)
O4KR-5: Brand identity is clear, published, and upheld. Existing materials that do not reflect new guidelines are updated.	4.0 (+8.1%)
O4KR-6: The process for creating a new OpenSSF project or SIG (whether or not it's based on existing work) is clearly documented and applied as documented.	3.1 (+24.0%)



OpenSSF の認知度、認識度、親しみやすさ



メディア ハイライト

OpenSSF はすでにセキュリティや開発者コミュニティの間で高く評価されていますが、この 1 年を通して、影響力を拡大し、組織の隅々まで、また私たちの活動に影響を与える政府基幹からも信頼されるリソースとなるよう努めました。サイバーセキュリティの重要性が経営幹部から開発の最前線に至るまで高まる中、OpenSSF は、メディアを通じてリーチを拡大するためたゆまぬ努力を続けてきました。

これらのメディア ハイライトは、画期的なプロジェクトや重要なコラボレーション、重要なマイルストーンについて、私たちがどのように認知度を高めることに成功したかを紹介しています。私たちは、ポッドキャスト、ビデオ インタビュー、会議やイベントでの現場でのディスカッション、記者会見、従来のニュース チャンネルなど、多面的なアプローチを採用しました。

オープンソース セキュリティの実践を向上させる我々の能力は、すべての人のためにオープンソース セキュリティを推進するという我々のミッションの証です。

OPENSSF、そのプログラム、パートナーシップについての全体的な認識の向上

9

新プロジェクト、コラボレーション、マイルストーンに関するプレス リリース

15%

記事全体における OpenSSF のメンションの増加

25%

サイバー セキュリティや政府協力に関する記事での OpenSSF に関するメンションが増加

25%

OpenSSF ツールとプログラムのメンションが増加

さまざまな視聴者への認知拡大

- ☑ 経営幹部
- ☑ サイバーセキュリティ専門家
- ☑ 開発者やメンテナー
- ☑ 教育機関や学生
- ☑ 企業
- ☑ 政府および規制機関
- ☑ オープンソース ユーザーや愛好家
- ☑ 研究者

ニュースのハイライト

SiliconANGLE New repository aims to illuminate open-source package vulnerabilities and malicious code (2023 年 10 月 12 日)

Cyberscoop Long-awaited curl vulnerability flops (2023 年 10 月 11 日)

The Wall Street Journal White House Calls for Stronger Open-Source Security (2023 年 9 月 13 日)

The Washington Post The Biden administration wants to put AI to the test for cybersecurity (2023年8月10日)

CNBC Hackers to compete for nearly $20 million in prizes by using A.I. for cybersecurity, Biden administration announces (2023 年 8 月 9 日)

TechCrunch DARPA launches two-year competition to build AI-powered cyber defenses (2023 年 8 月 9 日)

Security Boulevard How to trust open source software: A conversation with OpenSSF's Naveen Srinivasan (2023 年 6 月 14 日)

Techstrong TV Chris Robinson, Intel | OSS North America 2023 (2023 年 5 月 29 日)

Forbes The Hidden Risk Lurking In The Software Supply Chain: Transitive Open-Source Dependencies (2023 年 5 月 26 日)

The Register Python Package Index had one person on-call to hold back weekend malware rush (2023 年 5 月 22 日)

The New Stack Tracy Ragan: My Favorite Open Source Security Projects (2023 年 5 月 22 日)

Silicon ANGLE OpenSSF: Making SBOMs more dynamic to reduce software security risks (2023 年 5 月 15 日)

The Register EU's Cyber Resilience Act contains a poison pill for open source developers (2023 年 5 月 12 日)

SecurityWeek OpenSSF Receives $5 Million for Open Source Software Security Project (2023 年 5 月 11 日)

Dark Reading OpenSSF adds software supply chain tracks to SLSA Framework (2023 年 4 月 20 日)

CSO Magazine OpenSSF releases SLSA v1.0, adds software supply chain-specific tracks (2023 年 4 月 19 日)

SDxCentral How OpenSSF Aims to Make Log4j-Like Incidents Rare (2023 年 3 月 9 日)

SiliconANGLE AI threats and open-source vulnerabilities top host of security issues facing cloud-native community (2023 年 2 月 4 日)

TechTarget OpenSSF GM talks funding, legal software supply chain issues (2023 年 1 月 25 日)

VentureBeat Don't forget open source software (OSS) when assessing cloud app security (2023 年 1 月 15 日)

注目すべき発言

THE WALL STREET JOURNAL

ホワイトハウスがオープンソースのセキュリティ強化を呼びかけ
[Anne Neuberger 米国国家安全保障副大統領補佐官] 前回の会議以降に作成された内容の進歩を指摘した。その中には、安全な開発を支援する非営利団体である Open Source Security 財団によるソフトウェアのデジタル証明書の開発も含まれている。同氏によると、証明書は現在 17,000 以上のプロジェクトをカバーしており、これによりランサムウェアやネットワーク バックドアなどの悪意のある修正のオープンソース プログラムへの追加を阻止するのにされるのを阻止することができている。

DARK Reading

MOVEit の侵害は SQL インジェクションが依然としてアキレス腱であることを示した
「開発者とセキュリティ チーム両者にとって『構築における安全性』が非常に重要で、それには教育が必要です。私たちはよく『シフトレフト（対策の前倒し）』について話しますが、最も対策を前倒しできる方法は（OpenSSF の安全なソフトウェア開発の基礎コースなどの）教育です。」

THENEWSTACK

Tracy Ragan：私のお気に入りのオープンソース セキュリティ プロジェクト
「私たちは誰もが超能力を持っています。あなたの超能力をこれらのグループのいずれかに適用してください。なぜなら私たちは本当に本当にあなたを必要としているから。」と基調講演で Open Source Security 財団（OpenSSF）の取り組みとその背後にある勤勉な推進者と変革者を賞賛したラガン氏は述べた。

CSO FROM IDG

GitHub 上の最も人気のある生成 AI プロジェクトは最も安全性が低い
研究者は OpenSSF スコアカードを使用して、最も人気のある 50 の GitHub 上にある生成 AI 大規模言語モデル プロジェクトのセキュリティを測定しています。

TheDefensePost

OpenSSF は次世代 AI サイバーセキュリティ ツールを求めて DARPA プログラムに参加
「オープンソース ソフトウェアは、我が国の重要なインフラの不可欠かつ中核的な部分です。」と OpenSSF ゼネラル マネージャーの Omkhar Arasaratnam 氏は説明した。「構築においてオープンソース ソフトウェア サプライ チェーンの安全性を確保する新しくて革新的な方法を探すことは全員の最も関心のあることです。

The Register

Python Package Index では、週末のマルウェアの急増を抑えるために 1 人の問い合わせ担当者を配置
Durbin 氏は、いくつか良いニュースがあると述べた。OpenSSF と Linux Foundation からの資金提供のおかげで、間もなく Python Software 財団（PSF）に 1 年間セキュリティ ディベロッパ イン レジデンスが参加する。

CYBERSCOOP

待望の curl の脆弱性がざわつかせる
「脆弱性は今後も出てきます。来週には新しいものが出る予定です。また来年には新しいものがあるでしょう。」と Linux Foundation の Open Source Security 財団ゼネラル マネージャーの Omkhar Arasaratnam 氏は述べています。「私がすべての組織にお勧めしたいのは、脆弱性が出現したときに、その情報を受け取り、優先順位を付け、それに対して対処できるように訓練することです。これは驚くべきことではないでしょう。脆弱性が現れるたびに慌てふためき多忙になるべきではありません。」

DARK Reading

OpenSSF が SLSA フレームワークにソフトウェア サプライ チェーン トラックを追加
Open Source Security 財団の SLSA v1.0 リリースは、ソフトウェア サプライ チェーンのセキュリティの向上と、ソフトウェア保護のために組織が必要とするツール提供における重要なマイルストーンです。

2024 年 ガバニング ボード メンバー 代表のことば

2024 年の OpenSSF 理事長を務めることができて光栄に思います。ジェイミー・トーマスの過去 2 期にわたる理事長としての功績、過去 1 年間に達成したすべての成果に感謝します。今日、まさに、OSS が世界中で最も重要なインフラを動かしていることはこれまで以上に明らかであり、それに依存する我々にとってオープンソース ソフトウェアのセキュリティを確保することは基本的かつ重要なことです。オープンソース ソフトウェアのセキュリティ確保は OpenSSF のミッションの最重要事項であり、それを実現するには、世界中の多様な官民のステークホルダーとのコラボレーションを促進し、オープンソース セキュリティの取り組みの成長と持続可能性に貢献する必要があります。私たちだけではこれを成し遂げることはできません。これをみんなのために機能させるためにあなたの助けが必要です。

来年、私たちは OpenSSF のミッションを前進させるためにいくつかの主要分野に焦点を当てます。私たちは、あらゆる背景を持つ貢献者が協力し、知識を共有し、セキュリティ課題にみんなで取り組むことができる、活気に満ちた包括的なコミュニティの育成に取り組んでいきます。連邦政府、民間企業、学術界、その他の場所を通じてオープンソースのセキュリティを強化する取り組みが行われています。私たちはオープンソース ソフトウェアのセキュリティを強化する取り組みのため、他の組織との提携を積極的に模索していきます。私たちはまた、財団の運営における透明性を維持し、私たちのリソースがより広範なオープンソース セキュリティ エコシステムに利益をもたらすために効果的に使用されることを保証することに全力を尽くします。

来年、私たちは OpenSSF ののミッションを前進させるためにいくつかの主要分野に焦点を当てます。私たちは、あらゆる背景を持つ貢献者が協力し、知識を共有し、セキュリティ課題にみんなで取り組むことができる、活気に満ちた包括的なコミュニティの育成に取り組んでいきます。連邦政府、民間企業、学術界、その他の場所を通じてオープンソースのセキュリティを強化する取り組みが行われています。私たちはオープンソース ソフトウェアのセキュリティを強化する取り組みのため、他の組織との提携を積極的に模索していきます。私たちはまた、財団の運営における透明性を維持し、私たちのリソースがより広範なオープンソース セキュリティ エコシステムに利益をもたらすために効果的に使用されることを保証することに全力を尽くします。

Regards,

Aruna Gupta
2024 Chair of the OpenSSF Governing Board
VP & GM, Open Ecosystem Initiatives, Intel Corporation

素晴らしい一年をありがとうございました!
2024 年とその先のオープンソース エコシステム
の安全確保に参加しましょう

openssf.org/getinvolved