OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2022 アニュアルレポート

openssf.org

目次

ゼネラルマネージャーのことば

Open Source Security Foundation (OpenSSF) は、オープンソース ソフトウェア エコシステムのセキュリティ レベルを全体的に向上させ、グローバルなソフトウェア サプライチェーンの弱点に対処するために、セキュリティ専門家のコミュニティとセキュリティに焦点を当てた組織を結集するグローバル コラボレーションです。2022 年は、既存のイニシアチブを強化し、新しいイニシアチブと関与分野の基盤を構築する印象的な 1 年でした。私たちは、2023 年にオープンソース コミュニティに利益をもたらすために、私たちの成功を積み上げ、さらに多くの成果をあげていきたいと考えています。

OpenSSF は、活発で多様なノンストップ コミュニティです。30 を超える様々なアクティブなソフトウェア プロジェクトと技術的イニシアチブを通して、グローバルなソフトウェア セキュリティの課題に対応するために必要となる影響力とその及ぼす範囲を持つことができてきていましたが、これらの課題はますます深刻化しコストが増大するばかりとなっています。

今年は、重要なインフラの信頼性を確保する一環として、オープンソース ソフトウェアのセキュリティを検討し、それを取り入れ、それに投資する必要性に、国家が目覚めた年です。このコミュニティは、そのような認識に応え、業界を超えた取り組みに必要な大まかな合意形成と実行コードを提供するために立ち上がりました。

2022 年の間に、OpenSSF の会員数は、あらゆる種類の 100 を超える組織にまで増加しました。600 人以上のさまざまな個人が、私たちの技術的なイニシアチブに貢献しました。

「OpenSSFは、すべての人のためのオープンソース セキュリティを推進するために、アップストリームと既存のコミュニティの両方とのコラボレーションと作業に取り組んでいます。」

この年次報告書では、Governing Board (GB) とTechnical Advisory Council (TAC) の議長から話を聞き、2022年のハイライトをいくつか紹介し、Working Group (WG) とAssociated Projectsを紹介し、OSS Summit IIで米国ホワイトハウスと共同で発表したOpen Source Software (OSS) Security Mobilization Plan（オープンソース ソフトウェア セキュリティ動員プラン）をレビューし、OpenSSFが1年を通してもたらした影響について議論します。

Sincerely,
Brian Behlendorf
General Manager
The Open Source Security Foundation

OpenSSF メンバー

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

ガバニング ボード メンバー 代表のことば

OpenSSF Foundation は、2022 年に非常に多忙な時期を経験しました。これは、ソフトウェア サプライチェーンのセキュリティが、世界中の企業組織および政府内で真剣に議論されるようになったためです。2021 年末に発表された log4j の脆弱性をきっかけに、技術部門と商業部門の垣根を越えた業界連携が急務となりました。その目的のために、OpenSSF は、ツールチェーンの自動化、教育、脆弱性の修復、透明性といった基本的なことに焦点を当て、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ことができる行動指針を推奨する影響力のある立場にありました。2022 年の間の OpenSSF の各メンバーの警戒、貢献、および努力に感謝します。

今年の OpenSSF のハイライトをいくつかご紹介しましょう。今年の初めに、White House はいくつかのミーティングを開催し、Linux Foundation と OpenSSF の両方がオープンソース開発者と商用エコシステムを代表して課題について議論しました。特に、参加者はオープンソース サプライチェーンのリスクを軽減し、回復力を向上させるためのアイデアの共有に焦点を当てました。今年の春にワシントン DC で開催された Open Source Software Security Summit II で、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ための 10 項目の計画を発表しました。OpenSSF は、官民を越えて政権と協力する意思を明確にし、重要な画期的なパートナーシップとなりました。

また、今春に OpenSSF と Linux Foundation から 2 年間の認定を受けた学習者を対象とした、安全なソフトウェア開発のための無料オンライン トレーニング コースを公開したコミュニティに感謝します。これは、私たちの教育活動に大きく貢献するものです。さらに、ツール チェーン強化の重要な要素である、オープンソース プロジェクト向けの無料のデジタル コード署名技術である Sigstore の一般向け提供も発表しました。これらの成果はいずれも、10 項目の計画に対して行われた重要な活動例です。

コラボレーションは年間を通じて継続され、今年はテキサス州オースティン、アイルランドのダブリン、および、日本の横浜で最初の OpenSSF Days が開催されました。このような重要な課題を解決するためには、パンデミック後に対面でコラボレーションする経験に勝るものはありません。私たちのコミュニティから新しい機能、ベストプラクティス、助成金、および優先事項に関する発表を聞くことができ、とてもうれしく思いました。

ご覧のように、まだやるべきことがたくさんあり、セキュリティは開発者ひとりひとりの責任であり、他人事ではないことを理解するためには、コミュニティの考え方が必要です。私たちのセキュリティの優先事項に関する取り組みを維持するために、コミュニティにエネルギーを注入することの重要性はいくら強調してもしすぎることはありません。この 1 年間、Open Source Security Foundation の理事会の議長を務めることができ大変光栄でした。2023 年の素晴らしい成果を楽しみにしています。

Sincerely,
Jamie Thomas
Chair of the Board of Directors

ガバニング ボード メンバー

STEPHEN AUGUSTUS
Head of Open Source, Cisco

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

ERIC BREWER
VP of Infrastructure & Google Fellow, Google

BOB CALLAWAY (TAC CHAIR)
Tech Lead & Manager, Google Open Source Security Team

STEPHEN CHIN
VP of Developer Relations, JFrog

KIT COLBERT
Chief Technology Officer, VMware

IAN COLDWATER
Security Community Individual Representative

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

JENNIFER FERNICK
SVP & Global Head of Research, NCC Group

BRIAN FOX
CTO, Sonatype

ARUN GUPTA
Vice President and General Manager, Open Ecosystem Initiatives, Intel Corporation

MIKE HANLEY
Chief Security Officer, GitHub

JOHN HEIMANN
Vice President, Security Programs, Oracle

RAO LAKKAKULA
Executive Director, JPMorgan Chase

ADRIAN LUDWIG
Chief Trust Officer, Atlassian

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

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

TRACY RAGAN
CEO and Co-Founder, DeployHub

SCOTT ROBERTS
Cloud CISO, Coinbase

CLYDE RODRIGUEZ
Vice President of Engineering, Meta

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

GARETH RUSHGROVE
VP of Product, Snyk

MARK RUSSINOVICH
Azure CTO and Technical Fellow, Microsoft

MARK RYLAND
Director, Office of the CISO AWS Security

SUBHA TATAVARTI
CTO, Wipro

JAMIE THOMAS (BOARD CHAIR)
Enterprise Security Executive, IBM

ANDREW VAN DER STOCK
Executive Director, OWASP Foundation

CHRIS WRIGHT
Senior Vice President and Chief Technology Officer, Red Hat

2022年のハイライト

2022 年 1 月、米国ホワイトハウスは、多くの米国連邦機関のリーダーや専門家とともに、オープン ソース開発者と商用エコシステムの重要な部門を招集し、OSS サプライチェーンの課題を特定し、リスクを低減し、回復力を高める方法について、アイデアを共有しました。このミーティングには、Linux Foundation と OpenSSF の両方が参加しました。フォローアップとして、OpenSSF は 5 月に Open Source Software Security Summit II を主催し、37 企業の 90 人以上のエグゼクティブと米国連邦政府のリーダーが一堂に会し、OSS エコシステムの回復力とセキュリティを向上させるための重要なアクションについて合意に達しました。

Summit II において、OpenSSF は Open Source Software Security Mobilization Plan をリリースし、OSS セキュリティを向上するための 3000 万ドルの誓約を発表した。この Mobilization Plan は、世界中の OSS セキュリティを直ちに改善し、より安全な未来のための強固な基盤を構築するために、十分に検証されたソリューションを迅速に進める 10 の投資の流れを概説しています。この計画の包括的な目標には、OSS 本番環境の保護、脆弱性の検出と修復の改善、およびエコシステムのパッチ適用の応答時間の短縮が含まれます。2022 年を通じて、OpenSSF コミュニティはこの Mobilization Plan に従って行動しており、2023 年以降も継続して行動する予定です。

2022 年 2 月、OpenSSF は、オープンソース ソフトウェアのセキュリティ体制を改善する取り組みである、Alpha-Omega Project を立ち上げました。初期投資額は 500 万ドルでした。

このプロジェクトの「Alpha」部分は、最も重要なオープンソース プロジェクトのメンテナーと協力し、セキュリティ脆弱性の特定と修正を支援することで、グローバルな OSS サプライチェーンの安全性を向上させます。「Omega」部分は、OSS プロジェクトのロングテールに焦点を当てており、広くデプロイされている少なくとも 10,000 のオープンソース プロジェクトの脆弱性を体系的に見つけて修正する事を支援します。2022 年、Alpha-Omega は、Node.js と jQuery、Eclipse Foundation、Python Software Foundation(PSF)、および Rust Foundation をサポートするために、OpenJS Foundation に累計 200 万ドル以上の助成を行いました。

Sigstore は、2022 年 10 月に初の冠イベントである SigstoreCon North America で一般公開されました。ソフトウェアの署名、検証、保護を容易にする Sigstore は、ソフトウェア サプライチェーンの整合性を向上させ、開発者が日常業務でセキュリティを実装する際に直面する摩擦を軽減するために、大規模な貢献と採用を続けています。2022 年 6 月には、ソフトウェア開発者、DevOps エンジニア、セキュリティ エンジニア、およびソフトウェア メンテナーが、Sigstore によるソフトウェア サプライチェーンの保護に関する新しい無料のコース（Securing Your Software Supply Chain with Sigstore）を受講できるようになりました。

OpenSSF Technical Advisory Council は、重要なオープンソース プロジェクトの開発者が多要素認証 (MFA) のより広範な採用を促進することを追求する中で、さまざまな組織での MFA の使用を増やすための多様な取り組みを強い言葉で公に支援しました。作業部会はまた、2021-2022 年に、「Great MFA Distribution」として知られる、無料の MFA トークンの初期プロトタイプバージョンを、最も重要な 100 のオープンソース プロジェクトの開発者に提供しました。

Best Practices Working Group は、著名なオープン ソース リポジトリ内の悪意のあるパッケージを特定するという課題に対処する Package Analysis Project の初期プロトタイプ バージョンを導入しました。

Best Practices for Open Source Developers WG は、無料のトレーニング コース「Developing Secure Software」の改善を通じて、セキュリティのベストプラクティスに対する認識と教育を向上させました。これは現在、Linux Foundation Training & Certification プラットフォームである edX およびさまざまな組織の Learning Management Systems で利用可能であり、8,000 人以上が登録しています。このコースは今年更新され、最近顕著になった攻撃 (CWE Top 25 および OWASP Top 10 による) に対処するとともに、機械学習を使用するシステムの保護などのトピックをカバーする資料が追加されました。ワーキング グループはまた、Concise Guides on Developing More Secure Software and Evaluating Open Source Software をリリースし、一般的な npm パッケージ マネージャーを使用する人向けに npm Best Practices Guide を提供しました。OpenSSF Best Practices Badge Program には現在、5,000 を超える参加プロジェクトと 850 を超える合格プロジェクトがあります。

Best Practices WG は、GitHub Action や REST API などの新しいスコアカード機能をリリースし、セキュリティ チェック、オープンソース エコシステムのスケールアップ スキャン、バッジを追加しました。1,600 を超えるリポジトリがスコアカードを使用して、継続的改善のためにソフトウェア開発ライフサイクルにベストプラクティスを組み込んでいます。

Vulnerability Disclosures with Open Source Software Projects を使用して、セキュリティ研究者または Finder ペルソナに焦点を当てた新しいガイドを作成することによって、脆弱性開示のオープンソース コーディネーションを改善する次の進化を明らかにしました。

Mobilization Plan の重要なコンポーネントは、SBOM Everywhere として知られるオープンソース エコシステムのセキュリティ体制を改善するための基本的なビルディングブロックとして、ソフトウェア部品表 (SBOM) を使用することです。SBOM Everywhere Special Interest Group(SIG) は Security Tooling WG の下で生まれました。その最初の取り組みは、SBOM の作成と処理をサポートする SPDX Python ライブラリの開発に資金を提供することでした。

2022 年 6 月、Security Tooling WG は Fuzz Introspector もリリースしました。多数の開発ワークフローは、クラッシュやその他の問題を意図的に引き起こし、ソフトウェアに予期しない入力を供給することによりバグを見つけるための自動化された技術であるファジングに依存するようになりました。ファジングは、脆弱性の発見において重要な役割を果たします。しかし、今日のファジングは、一部のコード領域の効果的なファジングを妨げる障害（「ブロッカー」）にたびたび遭遇します。Fuzz Introspector は、(1) ファジングを使用するプロジェクトを改善すること、および (2)（ツール開発者が現在の問題を理解するのを支援することによって）ファジング自体を改善すること、を目的として、開発者がファジング カバレッジ ブロッカーを特定して解決できるようにするための実用的な見識を提供します。

OpenSSF Supply Chain Integrity Working Group は、Supply chain Levels for Software Artifact (SLSA)（"salsa" と発音する）の改良作業を続けています。これは、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標準とコントロールのチェックリストです。ドラフトはすでに公開されており、"Version 1.0" リリースに向けて改良作業が続けられています。作業グループはまた、S2C2F ガイドをさらに発展させ、継続的に改善するために、補完的な Secure Supply Chain Consumption Framework (S2C2F) の作業を開始しました。このガイドでは、開発者のワークフローに OSS 依存関係を安全に使う方法の概要と定義を示します。

OpenSSF は、2 つの新しいワーキング グループ（WG）を追加しました。Securing Software Repositories WG 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およびテクノロジーの導入を調整するためのコラボレーション環境を提供します。End Users WG は、オープンソースを生成するのではなく、主に使用する公的および民間部門の組織の利益を代表します。

私たちはオースティン、ダブリン、横浜で開催された、Open Source Summit North America/Europe/Japan で、OpenSSF Day を主催しました。また、OpenSSF Summit China を深圳で開催し、オープンソース コミュニティが一堂に会して、OSS サプライチェーンの保護における課題、全体像のソリューション、進行中の作業、および成功について議論しました。

2022 年 5 月、OpenSSF の GM である Brian Behlendorf は、米国下院の科学・宇宙・技術委員会で、オープンソース ソフトウェアのセキュリティと信頼性を向上させるために OpenSSF とより広範な OSS コミュニティで行われている作業について証言しました。

2022 年 6 月、Linux Foundation のエグゼクティブディレクターである Jim Zemlin は、政府や民間セクターのリーダーと共に White House Cyber Workforce and Education Summit に参加し、OSS エコシステムに役立つサイバーセキュリティ教育の開発方法について議論しました。2022 年 12 月、Open Source Supply Chain Security のディレクターである David A. heeler は、欧州委員会が主催した、信頼できる安全な OSS に関するワークショップのパネリストでした。

OSSセキュリティのための動員プラン

(Open Source Software Security Mobilization Plan)

オープンソース コミュニティは、ソフトウェア サプライチェーンに対する新しい種類の攻撃に対して脆弱になっており、これらの課題に対処するための多くの取り組みが行われています。これらの取り組みには、導入を促進するための新しいプロセス、新しいツール、および新しいイニシアチブが必要です。特に各国政府の関心が高まったことで、オープンソース コミュニティは、いくつかのセキュリティ ゴールを達成するための動員プランを打ち出しました。

2022 年 5 月 12-13 日にワシントン DC で開催された Open Source Software Security Summit II において、The Linux Foundation と OpenSSF は、オープンソース ソフトウェアの回復力とセキュリティを向上させるために取るべき、影響の大きい行動について合意に達するために、オープンソース開発者や商用エコシステムの代表者、主要な米連邦政府機関のリーダーや専門家を集めました。オープンソースおよびソフトウェア サプライチェーンのセキュリティに幅広く対応する初めての計画では、オープンソース ソフトウェアのセキュリティが直面する 10 の主要な問題に対して十分に吟味されたソリューションを迅速に推進するために、2 年間で約 150M の資金を提供します。これらのステップは、迅速な改善を実現し、より安全な未来のための強固な基盤を構築するための具体的な行動の概要を示しています。

報告書より

「OSS の開発、再統合、分散、および展開の方法を体系的に強化し、高度に再利用される特定の「重要な」部分への賢い投資は、すべてのダウンストリーム ユーザーのリスクを軽減するための影響力が大きく、費用対効果の高い方法です。これには、OSS を組み込んだ多数の独自仕様およびカスタム ソフトウェア ソリューションが含まれます。」

OSSセキュリティのための動員プラン

この計画は、3 つの包括的な目標に焦点を当てています。

- **セキュアな OSS の作成：**コードおよびオープンソース パッケージのセキュリティ上の欠陥と脆弱性を最初から防ぐことに重点を置く
- **脆弱性の検出と修復方法の強化：**欠陥を見つけて修正するプロセスを改善する
- **エコシステムでのパッチ適用応答時間の短縮：**修正の配布と実装の応答時間を短縮する

この計画では、10 の投資の流れが示されています。

1. ベースラインの安全なソフトウェア開発教育
2. OSS のリスク アセスメント ダッシュボード
3. 信頼性向上のためのデジタル署名
4. メモリセーフでない言語の置き換え
5. オープンソース セキュリティ インシデント対応チーム
6. 新しい脆弱性の検出と修復を迅速化
7. サードパーティによる監査 / コードのレビューと修復
8. 重要なプロジェクトを決定するためのデータ共有
9. あらゆる場所での SBOM: セキュリティ ユース ケース、ツール
10. 構築システム、パッケージ マネージャー、および配布システム

テクニカル アドバイザリー カウンシル(TAC)代表のことば

Open Source Security Foundation (OpenSSF) は、オープンソース エコシステムの全体的なセキュリティの向上に取り組むオープンソース ソフトウェア コントリビューターとユーザーのコミュニティです。ソフトウェア プロジェクトとサービス、教材、および仕様に関するコラボレーションを通じて、OpenSSF は規範的なガイダンスとツールを提供します。それらは、消費者が使用するソフトウェアに関してより多くの情報に基づいた決定を下すのを支援するとともに、製造者がより安全なソフトウェアを作成して維持することを支援します。

Open Source Security Foundation (OpenSSF) は、オープンソース エコシステムの全体的なセキュリティの向上に取り組むオープンソース ソフトウェア コントリビューターとユーザーのコミュニティです。ソフトウェア プロジェクトとサービス、教材、および仕様に関するコラボレーションを通じて、OpenSSF は規範的なガイダンスとツールを提供します。それらは、消費者が使用するソフトウェアに関してより多くの情報に基づいた決定を下すのを支援するとともに、製造者がより安全なソフトウェアを作成して維持することを支援します。

2022 年に、OpenSSF Technical Advisory Council(TAC) は、2 つの新しい作業グループの作成を承認しました。Securing Software Repositories Working Group は、さまざまなプログラミング言語エコシステムの技術リーダーを集めて、消費者にソフトウェアパッケージを配布する最後の 1 マイルに存在する課題について議論し、革新していきます。このユニークなフォーラムでは、セキュリティ問題に対するさまざまなアプローチを比較対照した調査がすでに行われており、共通のサービスと仕様への投資がすべての関係者に大きな利益をもたらす可能性のある分野が特定されています。

End Users Working Group は、OpenSSF 内のさまざまなプロジェクトおよび作業グループ内の消費者の声を広げる支援をします。コミュニティの成果に関するタイムリーなフィードバックが提供されることを保証するだけでなく、作業グループは、消費者中心の推奨事項およびベストプラクティス ガイドを作成できる場所としても機能します。

TAC はまた、OpenSSF の一部であるソフトウェア プロジェクトについて、手続きを明確にし、メリットと期待を列挙することを目的としたプロジェクト ライフサイクル プロセスの作成を承認しました。TAC は、このプロセスが、エコシステムの将来に対する私たちの使命とビジョンに沿った追加プロジェクトの作成および / または基盤への導入を促進することを期待しています。

最後に、私たちは、SBOM の採用、インシデント対応、教育などの優先度の高いトピックに焦点を当てた新しい分科会 (SIG) が最近結成されたことをうれしく思います。私たちは、2022 年のすべてのコミュニティ メンバーの貢献に心から感謝し、2023 年以降もオープンソース エコシステム内に存在するより広範なセキュリティ課題を解決するためのイノベーションを継続することを楽しみにしています。

Sincerely,
Bob Callaway, PhD
Chair, OpenSSF Technical Advisory Council

TAC メンバー

ABHISHEK ARYA
Principal Engineer and Manager, Google Open Source Security Team

AEVA BLACK (TAC VICE CHAIR)
Open Source Hacker, Microsoft Azure Office of the CTO

JOSH BRESSERS
VP of Security, Anchore

BOB CALLAWAY (TAC CHAIR)
Tech Lead & Manager, Google Open Source Security Team

LUKE HINDS
Security Engineering Lead, OCTO, Red Hat

DAN LORENC
CEO, Chainguard

CHRISTOPHER “CROB” ROBINSON
Directory of Security Communications, Intel

Critical Infrastructure Security Summit

OpenSSF
OPEN SOURCE SECURITY FOUNDATIO

ワーキング グループ

ワーキング グループ

Best Practices for Open Source Developers

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を提供し、それらを学び、適用するための簡便な方法を提供するために活動しています。

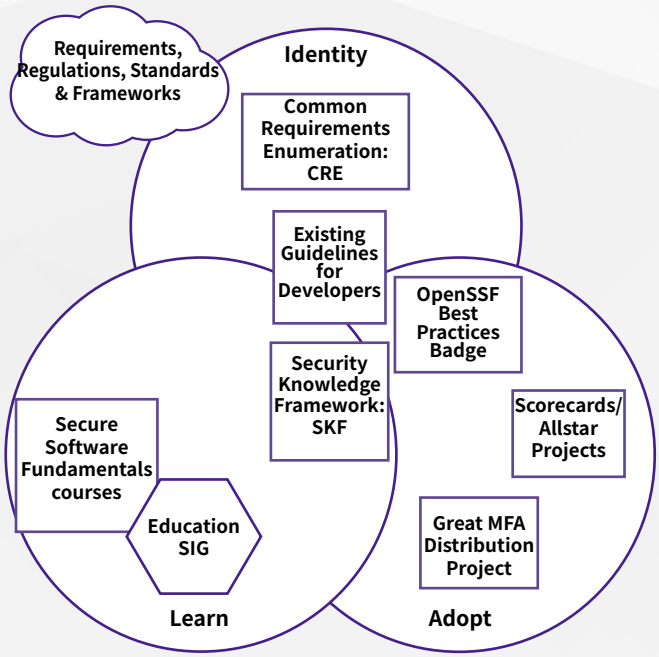
Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-best-practices-os-developers	Christopher “CRob” Robinson, Intel and Xavier René-Corail, GitHub	18 レギュラー参加者 20+ 断続的参加者

2022 年のハイライト

- コンサイスガイドの公開
- OSS-EU OpenSSF プレゼンテーション “BEST Practices makes Perfect”
- EDU.SIG

次のステップ

- EDU.SIG プランの公開
- 資金の確保
- エコシステム教育に着手
- C/C++ コンパイラー ベストプラクティス ガイド



ワーキング グループ

End Users

このグループは、オープンソースを作成するのではなく、主に消費する公的および民間部門の組織の利益を代表しています。

Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-endusers	Jonathan Meadows, Citi Andrew Aitken, Wipro	代表参加 15+ (銀行、運輸、小売などのオープンソースのエンドユーザーと、オープンソースの一部の作成者の強力な組み合わせによる)

私たちのミッション

End Users Working Group のミッションは、OpenSSF の技術的ビジョンの開発と提供において、エンドユーザーの明確で影響力のある声を確実に聞くことです。

私たちの目標

- ソフトウェア サプライチェーンを保護するための、より効率的で効果的な戦略、プロセス、ツール、ベストプラクティス、およびソリューションを開発および実装するためにエンドユーザーが必要とするリソースを提供します。
- エンドユーザーがオープンソース ソフトウェアを使用するためのユースケースが理解され、OpenSSF プログラムに含まれていることを保証します。
- 仲間の経験と知見から学ぶためのフォーラムを提供します。
- 主要な民間産業、公共部門、および複数の地理的地域からの広範な代表者を含みます。
- TAC とガバニング ボードの両方において、OpenSSF ワーキング グループとリーダーシップにおけるユーザーのリプレゼンテーションと積極的な参加を確立します。

2022 年のハイライト

- 10 以上の組織が積極的に参加し、ワーキング グループを立ち上げました。
- エンドユーザーの脅威分類を定義し、サプライチェーンとオープンソース ソフトウェアのリスクを特定して軽減するために、複数の機能と関連プロジェクトを連携させる方法を示しました。
- アプリケーションやモバイル アプリからコンテナ技術やオペレーティング システムに至るまで、ソフトウェア スタックのすべてのレイヤにわたって、商用およびオープンソースのサードパーティ ソフトウェアを利用するためのドラフト アーキテクチャを作成しました。
- 新たなイニシアチブが提案される際に、消費者の声が取り入れられることを確保するための、関連する各 OpenSSF 作業部会へのメンバーの参加。

次のステップ

- すべての主要な業界および地域をリプレゼントするエンドユーザーの採用の継続。
- 脅威分類の最終化と OpenSSF による標準としての承認。
- 消費アーキテクチャの最終化と OpenSSF による承認。

ワーキング グループ

Identifying Security Threats in Open Source Projects

このグループは、関連するメトリックとメタデータを収集、整理、および伝えることによって、OSS のセキュリティに対する情報に裏打ちされた信頼性を確保することができます。

Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-identifying-security-threats	Michael Scovetta, Microsoft	10-15 メンバー

目的

利害関係者がオープンソース プロジェクトのセキュリティに対して情報に裏打ちされた信頼を持てるようにすること。私たちは、オープンソース プロジェクトとその一部であるエコシステムから関連するメトリックとメタデータを収集し、整理し、伝えることによってこれを実現します。

ワーキング グループに参加し、未来の創造に貢献しましょう。OpenSSF の公開カレンダーを参照してください。

2022 年のハイライト

- Metrics Dashboard は、オープンソース ソフトウェア (OSS) パッケージ / プロジェクトに関する情報を提供し、ユーザーおよび潜在的なユーザーがリスクを評価するのを支援します。私たちはプロトタイプを開発しており、その経験に基づく充実したダッシュボードを構築する初期段階にあります。そのダッシュボードは、OpenSSF Scorecard、OpenSSF Best Practices バッジ、脆弱性データ（他のデータソースも含む）を基に構築されることが期待されています。
- Security Reviews は、OSS に対して実行されたセキュリティ レビューを収集および整理して、この情報を簡単に検索できるようにします。2022 年には 104 の新しいレビューを公開しました。
- Office Hours は、メンテナーがどんな (セキュリティ関連の) トピックについてでもセキュリティの専門家と話せるフォーラムを提供します。初めてのセッションには専門家以外の登録者がいませんでしたこれは、より長い準備期間と潜在的な要求者を対象とした広報活動が必要であることを示唆しています。
- 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の体制と実践に関する情報を、人間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。

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なのか、参加と議論が高まっています。

次のステップ

- Virtual Maintainer Summit が 2023 年 1 月に開催される予定です。
- Metrics Dashboard SIG（分科会）は、シナリオとモックアップの作成に取り組んでいます。
- 2023 年初頭には追加の Office Hours を計画しており、準備期間をより長くとり、潜在的な登録者を対象とした広報活動を行う予定です。
- 私たちは新しいプロジェクトの可能性について定期的に議論しています。話し合いに参加してください!

ワーキング グループ

Securing Critical Projects

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 プロジェクトを保護するためのリソースを特定し、割り当てるのを支援するために存在します。

Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-securing-critical-projects	Amir Montazery, OSTIF Jeff Mendoza, Google	平均 8-15 人のメンバーがミーティングに参加

2022 年のハイライト

- 100 の重要なオープンソース プロジェクトのセットからなる第一カット。
  - 「現在、このセットの管理と優先順位付けのプロセスを改良している。
- セキュリティ監査に推奨される 50 プロジェクトのセット。
  - Open Source Technology Improvement Fund によるさらなる分析が加えられた 100 の第一カットセットに基づく。
- 数々のプロジェクトに貢献：
  - Criticality Score
  - Allstar
- OpenSSF と GOSST からの資金提供のおかげで、Strategic Partner Open Source Technology Improvement Fund (OSTIF) は 2022 年に以下を達成しました。

22

脆弱性および CVEの 発見・解決

9

重大/高度 (CVSS > 7.0) な 問題の発見・解決

94

セキュリティの 改善

20

セキュリティ ファザーの構築と改善による継続的なオープンソース プロジェクトのモニタリング

8

セキュリティ エンゲージメントの 完了または進行

ワーキング グループ

Securing Software Repositories

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およびテクノロジーの導入を調整するための共同作業環境を提供します。

Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-securing-software-repos	Dustin Ingram, Google	20 - 40 regular contributors

私たちのミッション

“Securing Software Repositories” Working Group は、システム、言語、プラグイン、拡張、コンテナ システムを含むさまざまなレベルで、ソフトウェア リポジトリ、ソフトウェア レジストリ、およびそれらに依存するツールのメンテナーのためのものであり、彼らに焦点を当てています。経験を共有し、共有された問題、リスク、脅威について議論するためのフォーラムを提供します。WG には 20 ～ 40 人のレギュラー コントリビューターがおり、OpenSSF Slack には 250 人以上のメンバーがいます。

2022年のハイライト

2022 年に、同 WG は、潜在的なセキュリティ ギャップや改善の余地を含む、主要なソフトウェア リポジトリの既存の機能に関する「ランドスケープ」調査を実施し、その結果を共有しました。WG はまた、Sigstore を含む主要な OpenSSF 技術の採用に関する RFC と提案の指導と議論に広く貢献しました。WG はまた、ソフトウェア リポジトリによって増大するセキュリティ対策の負担を軽減するための「共有ヘルプデスク」の提案を作成し、共有しました。

その結果、多くのリポジトリが、すでに実装されているリポジトリのサポートを受けて新しいベストプラクティスを実装し (たとえば、npm の以前の経験から学んび、PyPI に 2 FA が必須となったこと)、新しい OpenSSF テクノロジーを採用しています (たとえば、Sigstore と署名付き証明書を使用するために npm が RFC を採用したこと)。

次のステップ

2023 年、同 WG は、重要なソフトウェア リポジトリにおける OpenSSF の主要技術とベストプラクティスの採用を、技術指導、議論、そして場合によっては OpenSSF の資金調達についても指導し、包括的かつ統一的にさらに支援することを目指します。

ワーキング グループ

Security Tooling

このグループのミッションは、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、それらを普遍的にアクセス可能にすることです。

Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-security-tooling	Josh Bressers, Anchore	SBOM Everywhereグループから15人の常時参加者

2022年のハイライト

OSS Security Mobilization Plan の重要なコンポーネントは、SBOM Everywhere と呼ばれるオープンソース エコシステム全体のセキュリティ体制を向上させるための基本的なビルディング ブロックとして、ソフトウェア部品表（SBOM）を使用することです。SBOM Everywhere は、その名前が示すように、SBOM をすべてのオープンソースに無停止で提供することに取り組んでいます。今年、私たちは SBOM Everywhere Special Interest Group (SIG) を導入し、まだ始めたばかりです。

SBOM Everywhere プロジェクトの最初の取り組みは、OpenSSF が SPDX Python ライブラリの開発に資金を提供できるようにする計画を作成することでした。この計画が承認され、9 月 1 日に作業が開始されたことをお知らせします。

SPDX は、ソフトウェアの部品表を記述するための標準です。これは、ソフトウェアの材料リストのようなものです。SPDX 仕様は、ISO/IEC 5962:2021 として知られる国際標準です。SPDX は SBOM の外観を記述する標準の 1 つですが、SPDX プロジェクトには、SPDX SBOM データを作成して解析するためのツールやライブラリなど、多くの技術プロジェクトも含まれています。これらのライブラリに関する作業は、長年にわたってコミュニティのボランティアによって行われてきました。SPDX Python ライブラリは、SPDX の最新バージョンに合わせて更新する必要があり、コミュニティが貢献しづらくならないよう、コードをメンテナンスしやすいものにする必要があることは、以前から知られていました。SPDX Python ライブラリには、作業を完了するための適切なスキルや資金を持つボランティアがいませんでした。ところが、OpenSSF には、これを遂行するための資金がありました。

SBOM は非常に重要になってきています。規制、法律、標準、さらには正式な要件にさえも登場しています。SBOM を簡単に使用して消費できるようにすることは容易ではないと理解していますが、非常に重要です。SBOM の作成、使用、保存、および配布が容易にならなければ、業界全体で使用される可能性は低くなります。

次のステップ

オープンソースを保護することに興味をお持ちの方は、ぜひご参加ください。オープンソースは、最近ではあらゆるものに含まれています。あなたがソフトウェアを作成するなら、あなたはオープンソース コミュニティの一員です。OpenSSF はコントリビューターからなる多様なコミュニティであり、やるべきことはたくさんあります。ぜひ皆さんに参加していただきたいと思います。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

ワーキング グループ

Supply Chain Integrity

このグループは、保守、生産、使用するコードの出所について、人々が理解し、意思決定できるよう支援しています。

Supply Chain Integrity WGは、個人や組織がオープンソース ソフトウェアのエンドツーエンド サプライチェーンのセキュリティを評価し、改善するために協力するためのコミュニティです。WGは、情報共有やプレゼンテーションの場として、また、いくつかのプロジェクトの拠点として活用されています。現在、このワーキング グループがスポンサーとなっているプロジェクトには、SLSA、FRSCA、および S2C2Fがあります。

Working Group Git リポ	Working Group リーダー
github.com/ossf/wg-supply-chain-integrity	Kim Lewandowski, Chainguard Dan Lorenc, Chainguard

Working Group メンバーシップ

通常、定期ミーティングに20-30人が参加者

プロジェクトに関連する数字

Supply Chain Integrity：Slackで460
SLSA (メイン・チャネル)：Slackで382、コントリビューター 30人
FRSCA：90人、コントリビューター 16人
S2C2F：コントリビューター 4人

その他のハイライト

OSS Compromise dataset | Verizon SLSA case study | CNCF CRI-O project security audit included a SLSA compliance report Eclipse Foundation projects are reporting their SLSA level on their project management pages | Flatcar Linux have adopted SLSA and made their build process SLSA level 3 compliant

Supply chain Levels for Software Artifacts (SLSA)

SLSA (「salsa」と発音する) はセキュリティフレームワークであり、プロジェクト、ビジネス、または企業における改ざんを防止し、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標準とコントロールのチェックリストです。これは、チェーン内の任意のリンクで、安全な状態から可能な限り回復力のある状態にする方法です。

2022年のハイライト

- SLSA 1.0ドラフト
- SLSAサーベイ
- 成功のためのSLSA:NISTのSSSDFを達成するためにSLSAを使用する
- GitHub Actions用SLSA3 Generic Generatorの一般提供
- GitHub Actions用のSLSA 3 Goネイティブ ビルダーの一般提供
- SBOM + SLSA：SLSAの支援によりSBOMの成功を加速

次のステップ

- SLSA 1.0リリース
- 適合プログラム
- 研修プログラム

Factory for Repeatable Secure Creation of Artifacts (FRSCA)

FRSCA(「フレスカ」と発音する) は、ビルド パイプラインを保護することによってサプライチェーンの安全確保に貢献することをを目的います。2022 年初頭に WG に採用されました。これは、CD Foundation、CNCF、OpenSSF などの LF グループ間の作業の統合です。

2022年のハイライト

- SLSA FRSCA Recipe For Secure Supply Chain (Parth Patel & Michael Lieberman)
- Putting the Supply Chain Pieces Together: A Deep Dive into the Secure Software (Michael Lieberman)

Secure Supply Chain Consumption Framework(S2C2F)

脅威ベースのリスク削減アプローチを使用して、オープンソース ソフトウェア (OSS) における現実世界の脅威を軽減する、消費に重点を置いたフレームワークで、同 WG において最近採用された最新の SIG です。ブログ投稿はこちら。

ワーキング グループ

Vulnerability Disclosures

このグループは、脆弱性の報告とコミュニケーションを促進することによって、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。

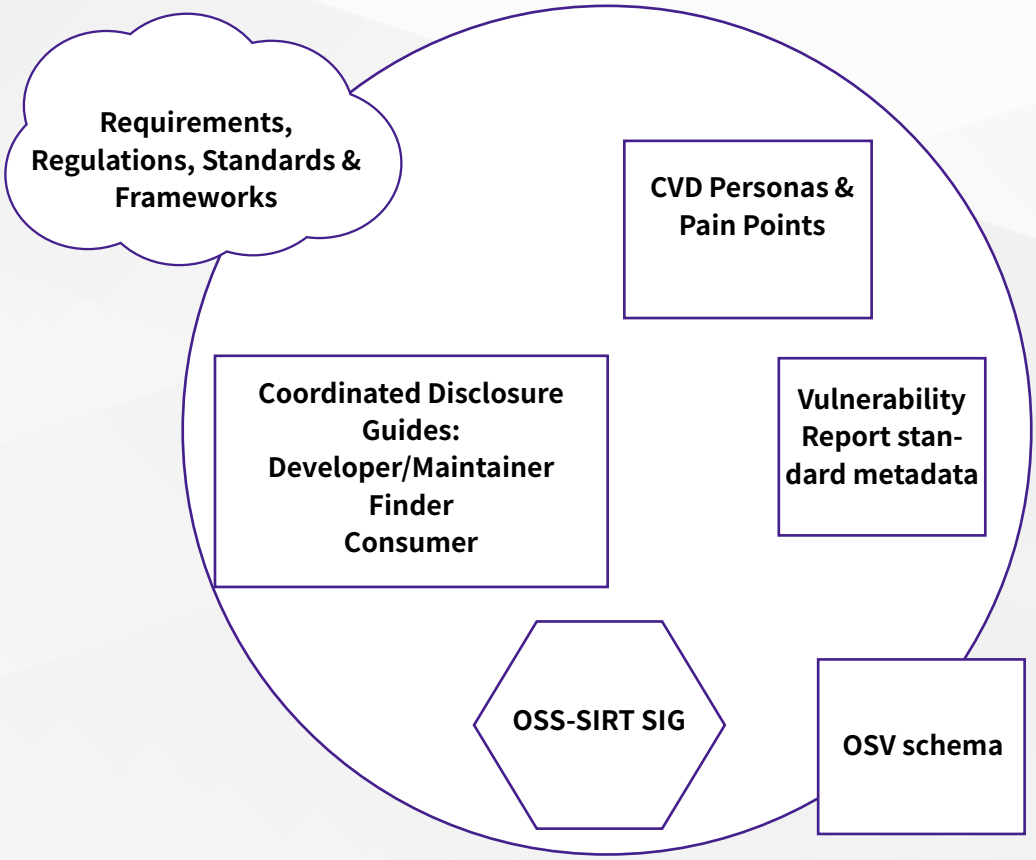
Working Group Git リポジトリ	Working Group リーダー	Working Group メンバーシップ
github.com/ossf/wg-vulnerability-disclosures	Christopher “CRob” Robinson, Intel	16人の常時参加者 15人以上の不定期参加者

2022年のハイライト

OSSプロジェクトに報告するCVD Guide for Findersの発行、OSS-NAプレゼンテーション ”0-Day Preppers” および ”Securing Open Source at Scale”、OSS-SIRT SIG。

次のステップ

OSS-SIRT 計画を発行し、資金を確保し、OSSの脆弱性開示、”CVD Guide for OSS Consumers” (End Users WG と協力)、”Incident Playbooks for Maintainers and OSS Projects” (メンテナーおよび OSS プロジェクト向けインシデント プレイブック) の調整を支援するチームの作成作業を開始します。



関連プロジェクト

Alpha-Omega

Alpha-Omega

Alpha-Omega は OpenSSF プロジェクトであり、メンテナーの直接的な関与と専門家の分析を通じてオープンソース 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 を通じて、私たちはいくつかの最も重要なオープンソース プロジェクトのセキュリティ作業に資金を提供しています。Omega を通じて、私たちはソフトウェア エンジニアリングとセキュリティ研究を適用し、広く使用されているプロジェクトのより広範なセットにわたってセキュリティを特定しています。

Alpha-Omega は、2022 年 2 月に Google と Microsoft が共同出資した 500 万ドルで設立されました。2022 年 6 月には、Google の Secure Open Source Rewards プログラムが私たちのへの参加を表明し、2022 年 12 月初旬には、Amazon Web Services が Alpha-Omega に 250 万ドルを寄付すると発表しました。

今年、Alpha-Omega は、Node.js プロジェクト、Rust Foundation、Eclipse Foundation、Python Software Foundation、および jQuery プロジェクトを含む 5 つの組織に対して、合計 200 万ドル強の資金を提供しました。この資金は、各組織内でセキュリティを直接改善するために使用され、合計で何百万人ものエンドユーザーに影響を与えます。私たちは、これらの財団のパートナーに感謝しながら、安全保障の成果を向上させるために最も効果的に資金を活用する方法を学んでいます。

これらの最初のいくつかの取り組みから得られた2つのおもなハイライトを次に示します。

- Node Security ワーキング グループが再活性化され、Node.jsの脅威モデルを構築しています。このグループはNode モジュールのための実験的な許可モデル、セキュリティ ベストプラクティス ガイドを発表し、継続的統合システムにセキュリティ チェックを加え始めました。彼らは、20以上の脆弱性報告のトリアージと修正を行い、複数のセキュリティ リリースを行いました。
- Eclipse Foundationは、Eclipse Foundation傘下のすべてのプロジェクトに対してセキュリティ スコアカードを実施しました。そして、その結果を分析し、ビルド インフラの強化やセキュリティ ツールの有効化を含む、最良かつ最も広範囲に改善するために注力すべき活動の優先順位リストを作成しました。Eclipse のプロジェクトが SLSA準拠レベルを宣言可能になり、HTTPS の使用を強制するようになりました。

> 「ソフトウェア セキュリティは終わりのないプロセスです。今回の資金援助は旅の第一歩です。Alpha-Omega プロジェクトの支援に感謝し、有効に活用することを約束します。」
>
> —MIKE MILINKOVICH, EXECUTIVE DIRECTOR, ECLIPSE FOUNDATION

Omega を通じて、オープンソース パッケージを対象としたオープンソース分析ツールチェーンをリリースし、このツールチェーンを使用して、重要なオープンソース プロジェクトにおける複数の脆弱性を特定しました。

「私は、オープンソース ソフトウェアの戦略的プロジェクトとして、Alpha-Omega プロジェクトを強く支持しています。このプロジェクトは、コミュニティとの提携によってオープンソース エコシステムのセキュリティを直接向上させ、すべてのユーザーに成果をもたらします。」

— JONATHAN MEADOWS, CITI

2023 年には、重要なオープンソース プロジェクトへの投資レベルを向上させると同時に、より長期的なプロジェクトで重要なセキュリティ脆弱性の特定と対処を支援するために、直接的な行動に引き続き重点を置く予定です。さらに、次のことを計画しています。

- 主要なプロジェクトや財団の予算において、セキュリティを第一級市民にすることを支援します。
- 私たちが注目しているプロジェクトに対するセキュリティの改善を通じて、測定可能な影響を実証します。
- Omega を拡張して、脆弱性の検出、トリアージ、通信 / レポート、および修復に対するスケーラブルなアプローチを提供します。
- 重要なプロジェクトのセットが大きく異なる可能性のある追加の分野（医療、自動車、金融サービスなど）をカバーするように、Alpha-Omega を拡張します。

私たちはコミュニティの関与と参加を歓迎します。私たちに連絡するか、私たちの毎月の公開会議の 1 つに参加してください。

Alpha-Omega Core チームには、Michael Scovetta (Microsoft)、Michael Winser (Google)、Yesenia Yser、Jonathan Leitschh、および Annapurna Veeramachaneni (Citi) が含まれています。Linux Foundation からの多大なサポートに感謝します。

Alpha-Omega の詳細については、こちら のアニュアル レポートをご覧ください。

Sigstore

Sigstore は、ソフトウェアの署名、検証、保護のための新しい標準です。

Sigstore を使用すると、開発者は、使用しているソフトウェアが、暗号化デジタル署名および透過ログ技術を使用していると主張されているものと正確に一致することを検証できます。Sigstore は、ソフトウェア アーティファクトに署名するための Cosign、Fulcio 認証局、Rekor 透過ログ、および Git コミットに署名するための Gitsign を含む一連の技術を提供しています。これらのツールは、独立して使用することも、1 つのプロセスとして使用することも可能で、オープンソースのセキュリティに対する全体的なアプローチを実現します。

オープンソースおよびソフトウェア サプライチェーンのセキュリティに対処するために、OpenSSF は 10 項目の動員プランの概要を示しました。そのゴールの 1 つは、上位 200 のプロジェクトのうち 50 のプロジェクトが、Sigstore によるソフトウェア署名に相互運用可能なアプローチを採用することです。

SIGSTORE の特長

2022 年は Sigstore プロジェクトにとって素晴らしい年であり、多くの重要なマイルストーンが達成されました。

450+
コントリビューター

9.4 million+
REKOR 署名

70+
団体

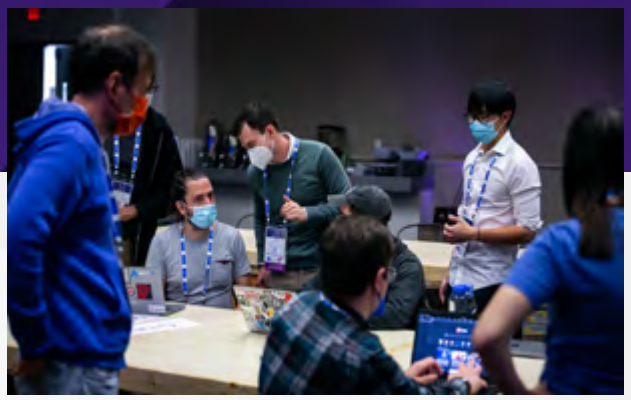
一般提供

Sigstore は、Rekor 透過ログと Fulcio 認証局の公益サービスの一般提供 (GA) を発表しました！コミュニティはこのマイルストーンを達成するために年間を通じて努力してきました。そしてオープンソース コミュニティが、アーティファクト署名と検証のためのプロダクション グレードの安定したサービスを Sigstore に自信を持って託すことができるようになったことに、私たちは感激しています。

SigstoreCon

コミュニティは、KubeCon + CloudNativeCon North America と同会場で、初めての Sigstore イベントである SigstoreCon を主催しました。

OpenSSF
OPEN SOURCE SECURITY FOUNDATION



このイベントでは、私たちの成長するエコシステムのあらゆる側面を示す 17 の素晴らしい講演が行われました。コミュニティは最初の授賞式を主催し、以下の 3 つの Sigstore Award を授与しました。
- Best User Adopter: SLSA GitHub Generators
- Best Evangelist:
  Batuhan (developer-guy) Batuhan Apaydın
- Most Valuable Contributor: Asra Ali

Sigstore の採用

その使いやすさのおかげで、オープンソース プロジェクトでは Sigstore の採用が急加速し始めました。5 月、Kubernetes のエコシステムが Sigstore を採用したのは、Kubernetes 1.24 のリリースに伴う画期的な動きでした。数か月後、Python コミュニティは CPython リリースの署名に Sigstore を採用しました。さらに、npm は最近、Sigstore の統合に積極的に取り組んでいると発表しました。これにより、すべての npm パッケージがソースコードとビルド命令に確実にリンクできます。Java の世界では、Maven は Maven セントラル プラットフォームの一部として Sigstore を採用する意向も発表しました。

Sigstoreは、史上最速で採用されたオープンソース プロジェクトのようです。さまざまなエコシステムでのSigstoreの採用を容易にするために、Python、Java、Javascript、Rust、およびRuby用のSigstore言語クライアントが開発中です。Sigstoreの状況は、成長するエコシステムを浮き彫りにしています。

> 「@projectsigstoreは超イケてると言うしかない。これこそが現代のソフトウェア署名と検証の姿だ。」
>
> —KELSEY HIGHTOWER

その他のハイライト

- “Sigstore: Software Signing For Everybody” が ACM Computer & Communications Security Conferenceの議事録に掲載されています。
- OpenSSFは、Sigstoreを使用してソフトウェア サプライチェーンの整合性とセキュリティを向上させるための新しい無料のオンライン トレーニングコースを発表しました。今すぐ登録してください。
- Sigstoreは、組織が現在Sigstoreをどのように使用しているかを強調するために、4つのエンドユーザーのケーススタディ を公開しています。

コミュニティの関与

Open Source Security Summit II

2022年5月12日ワシントンDC

The Linux Foundation と Open Source Software Security Foundation (OpenSSF) は、NSC、ONCD、CISA、NIST、DOE、および OMB から、37 社のエグゼクティブと政府リーダーを 90 名以上集め、オープンソース ソフトウェアの耐障害性とセキュリティを向上するために取るべき主要な行動について合意に達しました。

Open Source Software Security Summit II は、2022 年 1 月 13 日にホワイトハウスの国家安全保障会議が主導して開催された最初のサミットのフォローアップです。この会議は、バイデン大統領による「国家のサイバーセキュリティの改善に関する大統領令」の制定から 1 年後に開催されました。会議で、オープンソースとソフトウェア サプライチェーンのセキュリティに幅広く対応するための世界初の動員プランを発表しました。

プレスリリースはこちら。

Open Source Security Summit in Japan

2022年8月23日東京

米国のホワイトハウスと共に開催されたサミットに続いて、OpenSSF と Linux Foundation Japan が Open Source Security Summit Japan を開催しました。私たちは、日立、富士通、LINE、NEC、NTT データ、トヨタ、スズキ、東芝、SBI、OpenSSF のメンバーであるルネサス、サイバートラスト、サイボウズを含む 20 社以上の日本の大手企業のサイバーセキュリティ担当上級代表と、日本の経済産業省、AIST、IPA、JP-CERT の上級代表に参加してもらいました。

このサミットでは、世界中の政府や業界が OSS セキュリティに集中して協力することへの関心と優先順位が高まっていることが示されました。

要約はこちら

OpenSSF Day イベント

OpenSSF Days はオープンソース コミュニティを集めて、オープンソース ソフトウェア (OSS) のサプライチェーンを保護する上での課題、全体像のソリューション、進行中の作業、および成果について議論しました。彼らはOpenSSF のコントリビューターや思想的リーダーからの基調講演を特集しました。セッションには、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、および OSS セキュリティの将来などに関するプレゼンテーション、パネル、およびトーク イベントがありました。

OpenSSF Day North America

June 20 | Austin, TX, USA

- 11セッション、18講演者
- 登録参加者：861
  （対面：361、リモート：500）
- ハイライトはこちら

OpenSSF Day Europe

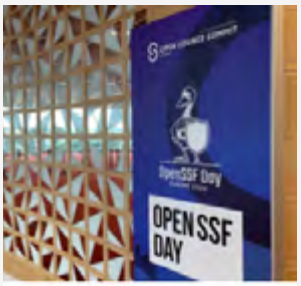
September 13 | Dublin, Ireland

- 11セッション、13講演者
- 登録参加者：510
  （対面：224、リモート：286）
- ハイライトはこちら

OpenSSF Day Japan

December 5 | Yokohama, Japan

- 7セッション、7講演者
- 登録参加者：283
  （対面：170、リモート：113）
- ハイライトはこちら



イベントへの参加

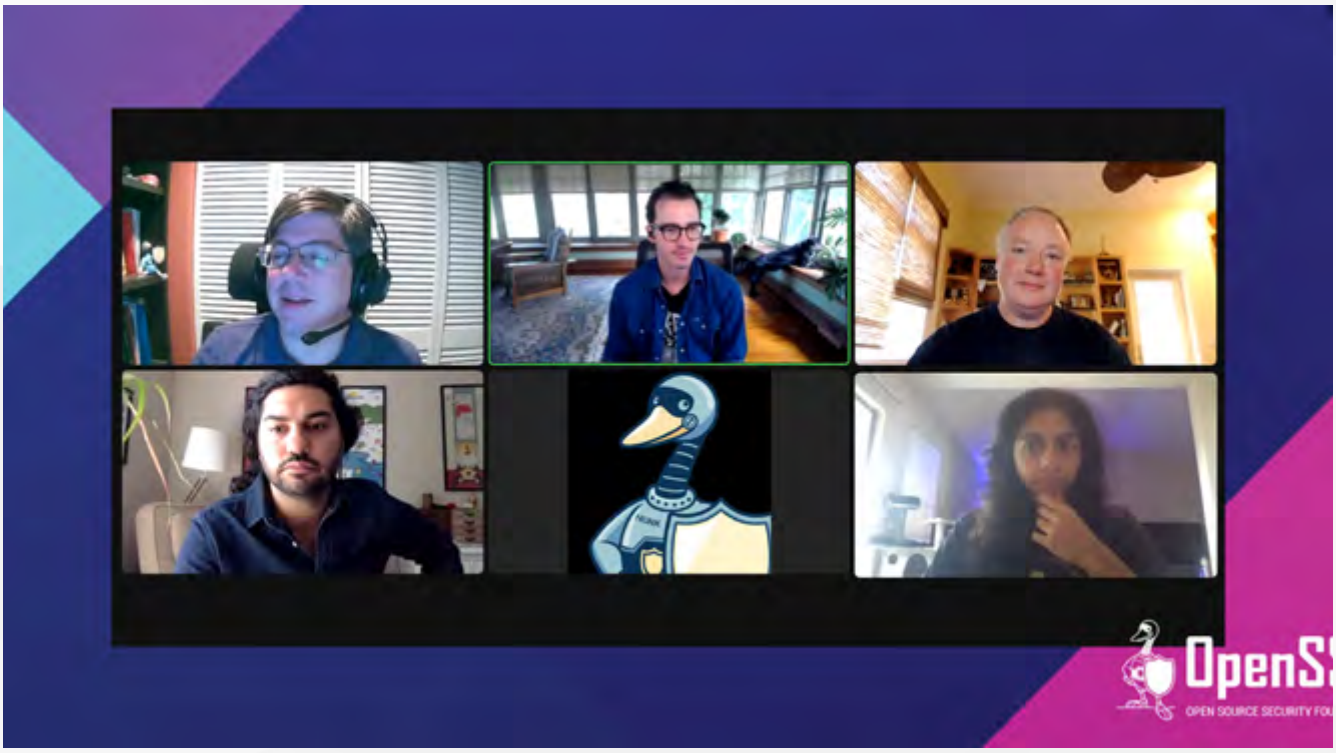
イベント
White House Summit on Software Security, Washington, D.C. (1/13)
Security Unhappy Hour, Virtual (2/14)
OpenSSF Town Hall, Virtual (2/23)
LF Webinar: Census II of Open Source Software Application Libraries the World Depends On, Virtual (3/2)
OpenSSF in APAC: How OpenSSF is Combatting Key Software Supply Chain Security Challenges, Virtual (3/24)
FOSSASIA Summit 2022, Virtual (4/8)
Future Compute, Cambridge, MA (5/3)
Testimony to the US House Committee on Science and Technology, Washington, D.C. (5/11)
Open Source Security Summit II, Washington, D.C. (5/13)
OpenJS World, Austin, TX (6/8)
OpenSSF Day at Open Source Summit North America, Austin, TX (6/20)
CSO's Future of Cybersecurity Summit, Virtual (7/19–7/20)
White House Cyber Workforce and Education Summit, Washington, D.C. (7/19)
Summer of Open Source Security, Virtual (7/20)
Fintech Festival India, Hybrid, New Delhi (7/20–7/22)
Open Source China Open Source World Summit, by COPU, Virtual (7/21–7/22)
OpenSSF Meetup in India, Bangalore (7/28)
ApacheCon Asia, Virtual, (7/29–7/31)
In the Nic of Time Podcast, Virtual (8/2)
BlackHat, Las Vegas, NV (8/6–8/11)
DEF CON, Las Vegas, NV (8/11–8/1)
OpenSSF Town Hall, Virtual (8/15)
OpenSSF & Scantist Community Events, Singapore (8/18–8/19)
Open Source Software Security Summit Japan, Tokyo, Japan (8/23)

イベント
VMware Explore, San Francisco, CA (8/29–9/1)
OpenSSF Day at Open Source Summit Europe, Dublin, Ireland (9/13)
Grace Hopper Celebration, Orlando, FL (9/20 - 9/23)
Open MainFrame Summit, Philadelphia, PA (9/21–9/22)
Critical Infrastructure Security Summit, Washington, D.C. (9/28 –9/29)
Black Bear Securities event: 'Application Development Best Practices' – Philippines, Virtual (9/30)
AWS ASEAN Security Forum, Singapore (10/4)
Snyk & OpenSSF in APAC: Cybersecurity Challenges in Open Source Software, Virtual (10/5)
ASIFMA Tech & Ops Conference 2022, Hybrid, Singapore (10/5–10/6)
OpenUK's Open Source Software: Infrastructure, Curation and Security Day, London, UK (10/17)
DevOps Enterprise Summit, Las Vegas, NV (10/18)
OSPOlogy.live Workshop, Stockholm, Sweden (10/19 –10/20)
CSDN "The Programmer Festival", China (10/22–24)
JAPAN Security Summit 2022, Japan (10/24)
KubeCon + CloudNativeCon North America 2022, Detroit, MI (10/24 –10/28)
Singapore Fintech Festival, Singapore (11/2–11/4)
NTU-Scantist DevSecOps event, Singapore (11/2)
IOSF and OpenSSF Summit China, Shenzhen, China (11/7)
ACM CCS 2022, Los Angeles, CA (11/7–11/11)
LF Member Summit, Lake Tahoe, CA (11/8–11/10)
DevOps Experience – DevOps Everywhere, Virtual, (11/16)
Internetdagarna, Virtual (11/22—11/22)
SWForum Event, Brussels (12/02)
OpenSSF Day at Open Source Summit Japan, Yokahama (12/05)


Supply Chain

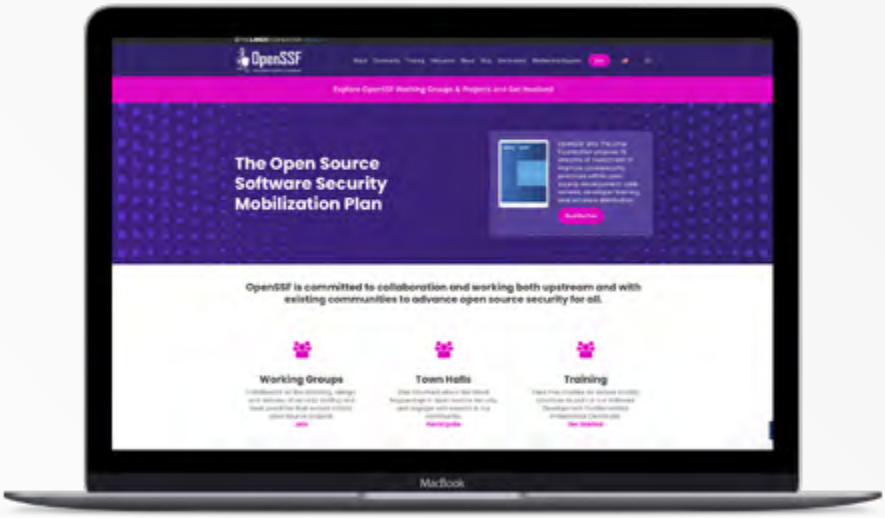
タウンホール（対話集会）

私たちは2022年2月と8月に2つのタウンホールを開催しました。これは、オープンソース ソフトウェアのメンテナー、コントリビューター、ソフトウェア開発者、およびOpenSSFのワーキング グループやプロジェクトにまだ参加していないOSSユーザーを対象としています。私たちは参加者にOpenSSFを紹介し、何が起こっているかをレビューし、次に何が起こるかについて共有しましたOpenSSFのエキサイティングな活動に初めて参加される方を支援するために、いくつかの主要な取り組みを詳しく紹介しました。



コミュニティの関与ハイライト

11月30日現在



ニュースレター メーリング リスト

メーリング リスト	購読者	ニュースレター オープン レート	クリック レート
Oct	1,254	40.17%	2.75%
Nov	1,489	31.60%	2.91%
Dec	1,631	33.19%	1.69%

Webサイト プレビュー: 192,998

月	ページビュー
Jan	17,024
Feb	21,187
March	14,308
April	13,694
May	35,667
June	18,579
July	13,394
Aug	15,052
Sept	15,939
Oct	14,862
Nov	13,292
合計:	**192,998**

Mobilization Plan: ダウンロード:4,009 | ブログ 投稿:51 | Slack 参加者:1,725

YouTube

- 登録者数:623
- 動画視聴数:45,896
- 視聴時間:2,100時間
- 投稿された動画数:377
- トップ動画:

トレーニング

Developing Secure Software コース:

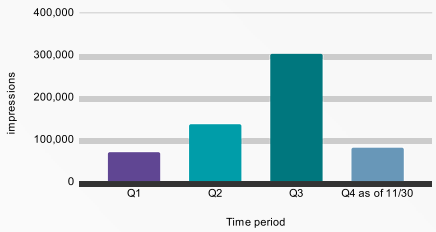
- 登録者数:8,412

Securing Your Software Supply Chain with Sigstore コース:

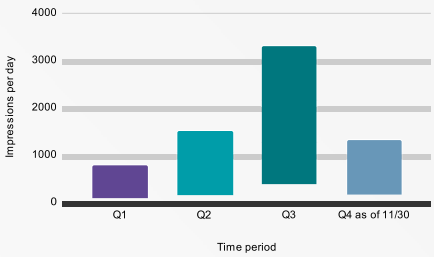
- 登録者数:741

Twitter @theopenssf

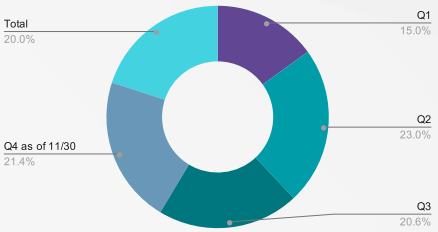
インプレッション:587,900



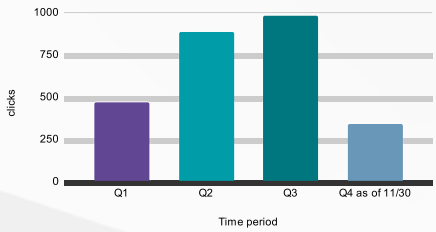
1日あたりのインプレッション:6,875



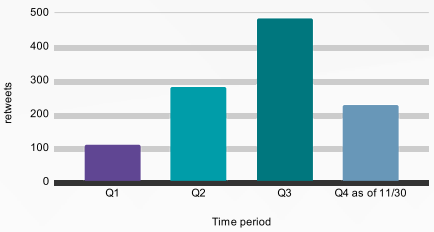
エンゲージメント率 %



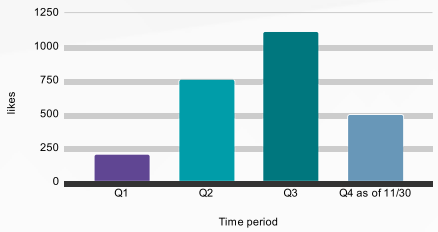
クリック数:2,667



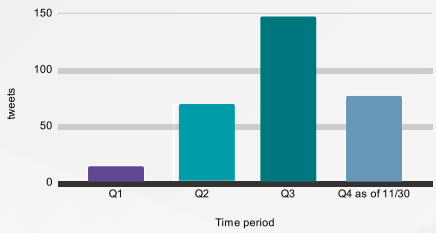
リツイート数:1,091



いいね!数:2,535

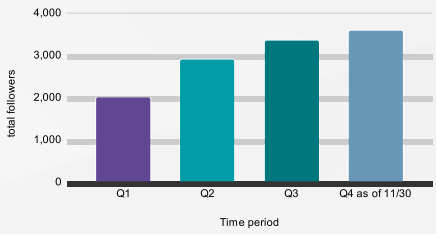


ツイート数:305



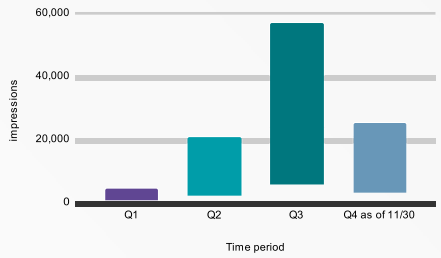
トップ ツイート:

フォロワー総数:3,577

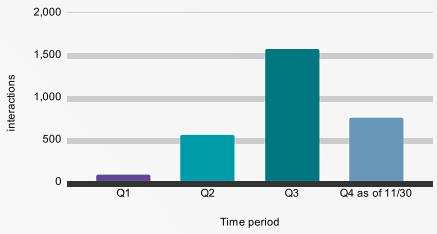


LinkedIn OpenSSF

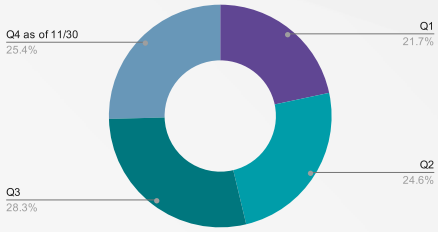
インプレッション：106,476



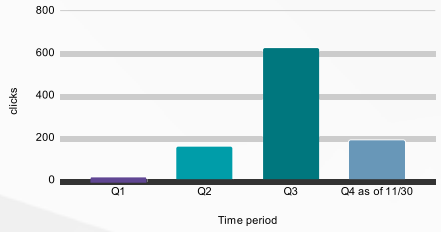
インタラクション：2,937



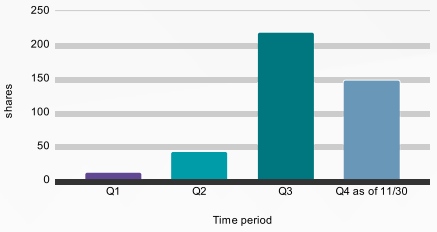
エンゲージメント率 %



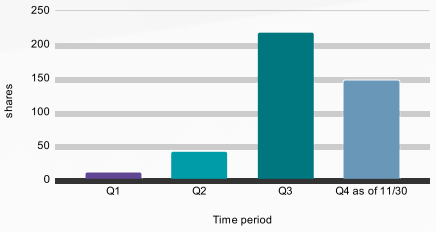
クリック数：972



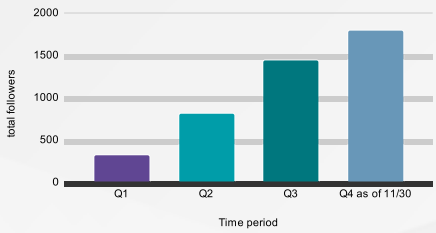
シェア数：414



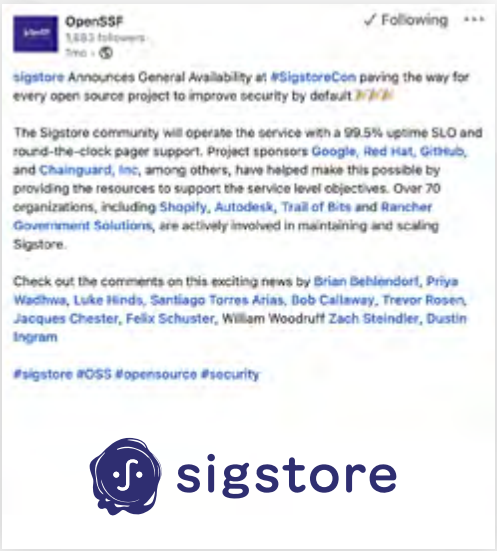
投稿数：240



フォロワー総数：1,783

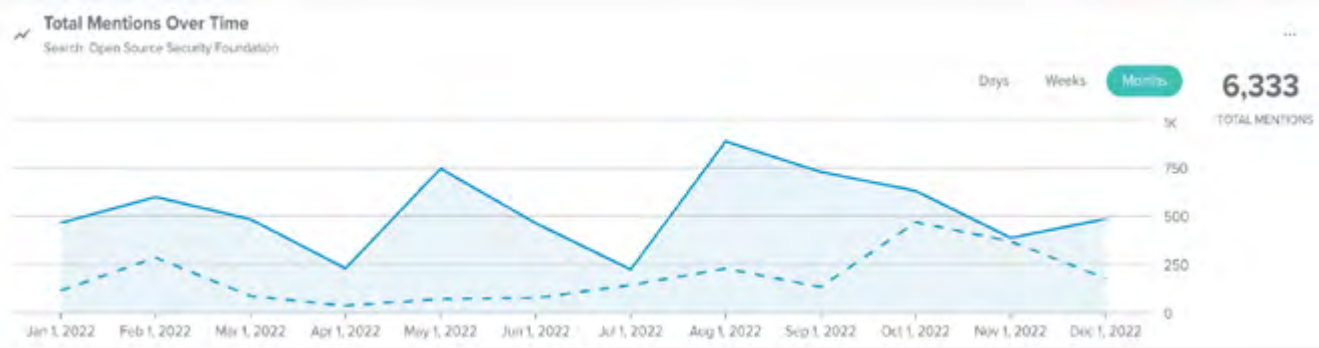


トップ記事：



報道ハイライト

プレスリリース発行：10
オンラインニュースやブログでの年間言及数：6,333 件（現時点）



OpenSSF
OPEN SOURCE SECURITY FOUNDATION

素晴らしい1年をありがとうございました!
2023年以降のオープンソース エコシステムの
保護にご参加ください。

openssf.org/getinvolved