OpenSSF
OPEN SOURCE SECURITY FOUNDATION

2025年 セキュア オープンソース ソフトウェア ビジョン 概要

openssf.org

The Open Source Security Foundation（OpenSSF）は、Linux Foundationのイニシアチブで、オープンソースソフトウェア（OSS）のセキュリティを共同で改善するための業界横断的なフォーラムとして2020年に設立されました。多くの脆弱性がクローズドソースのソフトウェアで発見されてきました。しかし、OSS（オープンソースソフトウェア）コンポーネントであるlog4jのLog4Shell脆弱性や、xz utilsに悪意のあるコードが仕掛けられるなどの事件により、多くの組織がOSSのセキュリティにも大きく依存していることを認識するようになりました。これにより、OSSのセキュリティをさらに向上させる必要性への関心が高まっています。

アイデアを行動に移すことは困難に直面してきました。なぜなら、オープンソース コミュニティが直面する社会経済的な現実があるためです。このコミュニティには、日常の業務とは別に、より広い公共の利益のためにOSS（オープンソース ソフトウェア）を作成するメンテナーや貢献者が多く含まれています。

OpenSSF は、OSS のセキュリティ向上に向けて前進しています（例：2024年12月の年次報告書に記載された活動を基にした取り組み）。私たちの2024年の成果には以下が含まれます。

1. **公共セクターとの関わり。** 2024 年を通して、OpenSSFはアメリカやヨーロッパの公共セクターと積極的に関わってきました。その成果の一部をご紹介します。

   » **米国。** OpenSSFは、米国サイバーセキュリティ・イン フラセキュリティ庁（CISA）が発行した「サイバーセキュリティ・リスクのバランスをシフトする：セキュア・バイ・デザイン・ソフトウェアの原則とアプローチ」に関する情報提供要請（RFI）に対する正式な回答を提出するとともに、CISAのオープンソースソフトウェア（OSS）セキュリティ・サミットに参加しました。

   » OpenSSFはCISAと協力して「パッケージ・リポジトリのセキュリティのための原則」を開発し、その採用を促進した。多くのリポジトリがその勧告の実装を開始しています。

   » OpenSSFは、DARPAとARPA-Hによる人工知能サイ バーチャレンジ（AIxCC）を積極的にサポートしています。これは、脆弱性を発見し修正するツールを開発し、そのツールをオープンソースソフトウェアとしてリリースするコンペティションです。また、OSSプロジェクトがコンペティションについて理解する手助けをし、OSSが技術移行の強力なサポートとなることを公に説明しています。

   » OpenSSFは、CISAおよび国土安全保障省 (DHS) 科学技術局 (S&T) と協力して、ソフトウェア部品表 (SBOM) とファイルデータを読み取って生成し、標準的な業界SBOM形式にデータを変換するOSSサプライチェーンツールであるprotobomを発表しました。

   » **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政策サミットを成 功裏に開催し、その存在感を強め、EU機関や加盟国とのサイバーレジリエンス法（CRA）に関する協力を開始しました。それ以来、OpenSSFは様々なイベントに積極的に参加し、ブリュッセルにおける欧州標準化とオープンソース協力のキープレイヤーとしての地位を確立しています。さらに、OpenSSFはFSFE Youth Hackathonのスポンサーを務め、開発者コミュニティの新たな才能にOpenSSFを紹介しました。

   » **協議。** OpenSSF は、NIS2 実施法のための公共協議会に貢献し、オープンソースとそのサプライヤーに関する NIS2 と CRA の見解の相違を強調し、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的とするための共同回答に協力しました。これは、欧州委員会とのフォローアップ会合につながり、今後のCRA関連業務への洞察を提供しました。

» **OpenSSFと標準化。** OpenSSFは、CRA実装のための Linux Foundationのワークストリームに深く関わっています。ブリュッセルで活動する最も技術的な財団の一つとして、OpenSSF は技術的な議論をサポートするためのツール、ガイダンス、コラボレーションを提供しています。OpenSSF はまた、CRA コンプライアンスに関する Linux Foundation Research にも協力しており、Linux Foundation Europe と共同で CRA 専用のワークショップを計画しています。

» **他のステークホルダーとの協力。** ブリュッセルにおけるOpenSSFの活動には、主にCRAの議論に参加する規制関係者やOpenSSFのメンバー、また他のオープンソースグループとはあまり関わりのない幅広いステークホルダーが参加しています。技術的な専門知識と実践的な貢献で知られるOpenSSFは、CRAの実施にとどまらない知識の共有を促進し、サイバーセキュリティ規制に関する真のグローバルな視点をもたらしています。OpenSSFは、欧州委員会のCRAに関する専門家グループに、170の組織の中から選ばれました。

» **課題。** CRAの関与には主に2つの課題があります。第一に、現実的な成果を得るために適切なステークホルダー間の議論を調整すること、第二に、ヨーロッパのメンバーシップとコミュニティ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、Linux Foundation Europe 内のパートナーとともに、強固なヨーロッパの聴衆とメンバーベースを構築するためには、的を絞ったメディアおよびアウトリーチ戦略が必要です。

2. **OpenSSFイベント。** 2024年、OpenSSF Community Dayプログラムはインドに拡大し、北米、ヨーロッパ、日本での年次会議に加わりました。OpenSSFはまた、ブリュッセルで第1回欧州政策サミットを開催し、次回の米国政策サミットの計画も進行中です。これらのイベントは、私たちの情熱的な地域コミュニティに参加し、私たちの大規模なサイバーセキュリティ専門家コミュニティにアクセスすることを可能にしました。

これらの「Community Day」で好評を博しているのが、コミュニティ向けのサイバーセキュリティの卓上演習の実施です。このような模擬インシデントは、実際のインシデントを経験する前に、プロジェクトや保守担当者の意識と心構えを高めるのに役立っています。

3. **ソフトウェアセキュリティ教育。**2024年、OpenSSFは、安全なソフトウェアの開発 (LFD121) の基礎に関するコースにラボを追加し、実践的で詳細な学習を改善しました。これらの追加により、9,300人以上の新しい開発者がコースに登録し、全期間（全プラットフォームおよび自然言語）で29,000人以上が受講しました。以下のコースも教育ポートフォリオに追加されました。
   - » Sigstoreを使用したソフトウェア サプライチェーンのセキュリティ保護 (LFS182)
   - » OpenSSF Scorecardを使用したプロジェクトのセキュリティ保護 (LFEL1006)
4. **セキュリティ ガイド。**開発とサプライチェーン セキュリティのベストプラクティスに関する知識の共有は、財団の多くの活動の基礎となっています。メンバーは、長年にわたってさまざまなガイドの開発と改善に協力してきました。これらのガイドは、開発者、消費者、セキュリティ コミュニティがセキュリティを改善するのに役立ちます。
   - » よりセキュアなソフトウェア開発のためのコンサイス ガイド
   - » オープンソース ソフトウェア評価のためのコンサイス ガイド
   - » パッケージ リポジトリのセキュリティの原則
   - » 正規表現を正しく使用して安全な入力検証を行う
   - » CとC++のためのコンパイラー オプション ハードニング ガイド
   - » ソースコード管理 (SCM) プラットフォーム構成のベストプラクティス
   - » Pythonのセキュアコーディングワンストップショップ
   - » すべてのパッケージ リポジトリの信頼できる発行者
5. **OSSのセキュリティ評価。**OSSに関するセキュリティ情報の入手を簡素化し、消費者や保守者がOSSのセキュリティをより効率的に評価できるようにします。

   » **OpenSSFスコアカード。**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ます。スコアは、OSS の利用者が OSS のセキュリティを推定するのに役立ち、また、OSS の保守者がプロジェクトのセキュリティ体制を改善するための道筋を示すことで、OSS の保守者を支援します。Allstar は、開発中の組織やプロジェクト内でのスコアカードの使用を合理化するための補完的な取り組みです。Scorecard は、GitHub と GitLab をサポートしており、毎週、100 万を超える OSS プロジェクトの Scorecard スキャンを実行しています。

   » **OpenSSF ベストプラクティス バッジ**。OSSプロジェクトが自らの取り組みをより深く評価し、OSSの利用者がその状況を理解するのに役立つセキュリティおよび持続性の基準です。例えば、少なくとも1人の開発者が安全なソフトウェア設計や一般的な脆弱性への対策方法を理解していることを求めたり、新たな重要な機能が追加される際に、開発者が自動テストスイートにテストを追加することを義務付けたりします。現在、7,900以上のプロジェクトが参加しています。

   » **ソフトウェア アーティファクトのサプライチェーン レベル (SLSA)。**SLSAは、改ざんを防止し、整合性を改善し、パッケージとインフラストラクチャを保護するための基準を定義するフレームワークです。SLSA バージョン1.0は、ビルド プロセスの保護に重点を置いて2023年4月にリリースされました。SLSAはその後、パッケージの整合性のためにnpmによって採用されました。

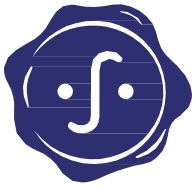
» **アーティファクトの構成を理解するためのグラフ（GUAC）**。GUACは、ソフトウェアサプライチェーン内のソフトウェアの依存関係に関する SBOM、脆弱性、認証、その他のメタデータを取り込むツールです。GUACは、ソフトウェア コンシューマが、使用しているソフトウェアに関する大量のメタデータを迅速に理解し、より効果的なリスクベースの意思決定を行えるようにします。

» **セキュリティ ベースライン**。 グローバルなサイバーセキュリティの枠組みと規制に基づき、セキュリティ ベースラインは、オープンソース ソフトウェアの生産者と消費者の双方が、そのプロジェクトと運用のセキュリティを向上させるために活用できる、開発中の一連の基準を提供します。

» **セキュリティ レビュー コレクション**。OSSの既知のセキュリティ評価一式を収集し、他の人がこれらの情報を素早く見つけてレビューできるようにしました。

6. **OSSインフラとツールの改善。**インフラとツールの改善は、セキュリティの改善に広く影響します。

» **sigstore。** デジタル署名は、ソフトウェアの信頼性を 検証し、悪意のあるパッケージ攻撃に対抗するのに役立ちます。ただし、過去のソリューションはオープンソースでは実用的ではないことがよくありました。無料のデジタル署名および検証サービスである Sigstore は、この課題に対処し、2022 年 10 月の一般提供 (GA) リリース以来、幅広く採用されています。現在、SLSA の出所には npm、ワークフロー実行の出所には GitHub Artifact Attestations、homebrew-core (Alpha-Omegaが資金提供) のすべてのボトルに署名して検証する Homebrew で使用されています。PyPI は Sigstore 署名のアテステーションに PEP 740を採用し、Maven Central は Sigstore 署名バンドルをサポートし、PEP 761 は CPython リリースの PGP署名を Sigstore に置き換えることを提案しています。Sigstore の透明性ログには現在、Kubernetes、CPython、LLVM を含む 17,000 を超える OSS プロジェクトで 1 億 7,000 万を超える署名が保存されています。Sigstore の使用方法を学習するための無料コースが用意されています。



» **セキュリティで保護されたソフトウェア リポジトリ。**多くのOSSパッケージはリポジトリを介して取得されるため、リポジトリと協力してセキュリティを向上させています。オープンソースパッケージリポジトリがセ キュリティ ロードマップを開発するのを支援するために、CISAと共同で「Principles for Package Repository Security」を公開しました。RSTUF は、パッケージリポジトリインデックスを保護することを目的として、実験的なシステムから本番環境への展開に適したMVPリリースに進化しました。さらに、プラットフォーム間でパイプラインを構築する際の秘密管理を強化するための実装ガイドである「Trusted Publishers for All Package Repositories」を公開しました。パッケージリポジトリセキュリティの原則に関する文書は、CISAがオープンソースソフトウェアセキュリティサミットを主催するきっかけとなりました。

» **より良いツール。** OpenSSFはファジングテストと関連ツールの改善を目的としてFuzz Introspector をリリースし、攻撃者が脆弱性に先んじて脆弱性を検出できるようにしました。

7. **脆弱性の発見と報告**

» **Alpha-Omega。** これは、未発見の脆弱性を体系的に発見・修正し、全体的な プロセスを改善するために、OSSのメンテナと提携するための、1,250万ドルの企業スポンサーを得た重要な取り組みです。現在のパートナーには、Python Software Foundation（Python security developer-inresidenceへの資金提供など）、OpenJS FoundationとjQuery、Eclipse Foundation、Node.js、Rust Foundationが含まれます。これらのパートナーはすべて、重要で広く利用されているOSSを管理しているため、私たちがともに実施するセキュリティ改善は、すべての人のセキュリティを大幅に改善することになります。

» **セキュリティ監査。** Eclipse Equinox P2 (広く使用されているプロビジョニングプラットフォーム)、sigstore、Jackson-CoreとJackson-Databind、slf4j (ログフレームワーク)、Symfony (広く使用されているPHPフレームワーク) など、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います。

» **オープンソースの脆弱性 (OSV) スキーマ。** OSVは、脆弱性をオープンソースのパッケージバージョンまたはコミットハッシュに正確にマップす る、機械読み取り可能な形式です。OSVを使用すると、脆弱なコンポーネントを迅速に自動識別できるため、プロジェクトや組織はこれらのコンポーネントを更新できます。OSVは現在、Rust、Go、Python、Java、JavaScript、C#、PH P、Ruby、AlmaLinux、Rocky Linux、Haskellプログラミング言語など、多くのエコシステムをサポートしており、現在合計30のエコシステムがあります。

8. **調査**

» OpenSSFは、最も広く利用されているOSSアプリケーション ライブラリを特定するための「Census III of Free and Open Source Software -Application Libraries」や、「SecureSoftware Development Education 2024 Survey」などの調査を統括してきました。これは、「Addressing Cybersecurity Challenges in OpenSource Software（オープンソース ソフトウェアにおけるサイバーセキュリティの課題への取り組み）」に関する調査など、これまでの成果を基にしたものです。

9. **コミュニティの構築とアウトリーチ**

» OpenSSFリソースの使用を促進するために、北米、ヨーロッパ、インド、日本で公式のOpenSSF Community Daysを開催しています。また、世界中でローカル ミートアップを開催しています。また、いくつかのOpenSSFの取り組みは業界カンファレンス（例: KubeCon North America 2024で取り上げられたGUAC）で紹介され、プロジェクトの利点や、 オープンソース プロジェクトがOpenSSFの資料をどのように活用できるかが強調されました。さらに、さまざまなイベントでワークショップを開催し、SLSAセキュア サプライチェーン仕様の認知度と貢献を高めるとともに、ユーザーが日々使用し依存しているOSSソフトウェアのセキュリティ特性を理解するための「OpenSSF Scorecard」ツールの活用を促進しています。

OpenSSFの計画とパートナーシップの可能性

私たちは、私たちがやろうとしていることと、可能性のある新しい仕事の両方について、協力する機会がたくさんあると信じています。コラボレーションは、米国政府がオープンソース ソフトウェアのセキュリティ イニシアチブを加速し、取り組みの重複を回避し (リソースをプールすることで無駄を排除し、結果を強化します)、米国政府と業界の両方が重要な問題を解決するために協力しているパートナーと見なされることを可能にします。

OpenSSFは次のことを行う予定です。

1. **OSSセキュリティ教育。**私たちは、Linux Foundation Educationと協力し、OpenSSFの教育ポートフォリオを拡充しています。現在進行中の新しいコースには、「Security for Managers of Software Developers (LFD125)」や「European Union (EU) Cyber Resilience Act (CRA) (LFEL1001)」、さらにはセキュリティ アーキテクチャに関する中級コースが含まれています。また、OpenSSFはLinux Foundation Educationチームと提携し、グローバルなITサイバーセキュリティ スキル マトリックスの開発にも取り組んでいます。このフレームワークは、実務者が自身のキャリアのさまざまな段階で求められるスキルや経験の共通基準を簡単に理解できるようにすることを目的としています。このスキル フレームワークは、NIST NICEフレームワークのよ うな、より正式な手法を補完するものです。（NIST NICEフレームワークも本フレームワークのレビューに関与しています）
2. **セキュリティ ガイド。**OpenSSFは、セキュア・バイ・デザインおよびセキュア・バイ・デフォルトの技術の開発と普及を促進するフレームワークや国際標準の活用を容易にするため、ベストプラクティス ガイドの開発する機会を引き続き模索していきます。
3. **改善されたOSSセキュリティ評価。**これらは、ソフトウェアのセキュリティ体制を評価し、より安全な設計と既定のテクノロジのための方法を提供するのに役立ちます。

» **サプライチェーンの整合性。**私たちは、既存のフレームワークSLSAとS2C2Fを進化させて、より広範な機能上の懸念事項をカバーし、オープンソースの利用者がアップストリームの脅威をより徹底的に評価し、依存関係ポートフォリオ全体のサプライチェーンのリスクをより適切に管理できるようにするつもりです。

» **アーティファクトの構成を理解するためのグラフツール。**GUACは、SBOMや脆弱性レポートなどのソフトウェア依存関係アーティファクトに関するメタデータを分析し、ソフトウェア利用者が毎日使用するオープンソース ソフトウェアに関するより実用的なインテリジェンスを提供するツールです。

» **OpenSSF スコアカード。**セキュリティツールとプロセスの検出を改善し、構造化された結果 (プローブ) と管理者の注釈機能を通じてポリシーごとのカスタマイズを可能にすることを計画しています。

» **OpenSSFセキュリティ ベースライン。**セキュリティ ベースラインは、オープンソース プロジェクトが実装できる標準ベースの基準のセットであり、ダウンストリームのコンシューマーはより高度なセキュリティ保証を求めることができます。ベースラインは、Scorecard、Best Practices Badges、Security Insights、Minder、SLSA、GUACなど、OpenSSFの多くのツールと連携します。

4. **OSSインフラストラクチャとツールの改善**

» **統合ツールの改善。**OSSの広範な採用を促進し、サポートのないソフトウェアのリスクを軽減するためには、ソフトウェア部品表（SBOM）の生成と活用を簡素化することが必要です。protobomやbomctlプロジェクトは、SBOMの作成と移植性を簡単にするものであり、OpenSSFはソフトウェアのライフサイクル全体を通じてSBOMの生成、変換、評価を支援するツールやプロセスのライブラリを保有しています。このグループは、リファレンス アーキテクチャや実装パターンに関する協力を計画しており、上流プロジェクトが有用なマニフェストを作成し、下流の利用者がそれらを取り込み、解釈し、評価できるよう支援することを目指しています。

» **メモリの安全性の向上。**メモリの安全性グループは、重要なOSSプロジェクトが既定でメモリセーフな言語に移行することを奨励します。それが不可能または現実的でない場合は、メモリの安全性の脆弱性を減らすようにプロジェクトを奨励します。

» **セキュリティ強化されたソフトウェア リポジトリ。**現在、PyPI、NuGet、PHP Composer、Rust Cratesなどのパッケージ マネージャー エコシステムのセキュリティ向上に向けた取り組みが進められています。私たちは、さらなるセキュリティ機能の拡充の可能性を引き続き検討していく予定です。

5. **脆弱性の発見と報告。**これらは、「協調的な脆弱性の開示」と連携しています。

» **オープンソース ソフトウェア セキュリティ インシデント対応チーム (OSS-SIRT)。**OSS-SIRTは、OSSメンテナーが影響の大きいセキュリティ脆弱性と関連するセキュリティ緊急事態を修復するのを支援するために利用できる、提案されたプロセスと調整された業界横断の専門家グループです。この計画は、Alpha- Omegaとの強力なパートナーシップのもう1つの例です。

» **机上演習。**私たちは、参加者が架空の脆弱性の発生をナビゲートする実践的なシミュレーションを引き続き開催し、独自の演習を作成したいチームにはガイダンスを提供しています。

» **脆弱性の共有メーリングリスト。**OSSの脆弱性の調整に広く使用されているOpenWallのメーリングリスト インフラストラクチャを改善し、Sirenとして知られる脅威インテリジェンス共有リストを引き続き推進することを計画しています。このリストでは、コミュニティ メンバーが脅威、侵害の兆候を共有し、プロジェクト内で観察された疑わしいアクティビティについて議論できます。

» **OpenVEX。**OpenVEXは、脆弱性交換 (VEX) データの仕様です。Cybersecurity and Infrastructure Security Agency (CISA) Minimum Elements for VEXを実装しています。その仕様とvexctlツールを更新する予定です。セキュリティ スキャナー ベンダーがOpenVEXおよびその他の VEXステートメントを活用してVEXドキュメントを効果的に取り込むためのガイダンスに取り組んでいます。

» **Vulnerability Disclosures（脆弱性の開示）ワーキング グループ。**Vulnerability Disclosures ワーキング グループは、アップストリーム プロジェクトとの対話に最適なアップストリーム メンテナーやセキュリティ研究者向けに、いくつかのCoordinated Vulnerability Disclosure (CVD) ガイドを作成しています。グループは、オープンソース プロジェクトがCNA (CVE Numbering Authority) になるためのガイドなど、他の関連資料を作成しています。

6. **人工知能/機械学習 (AI/ML) のセキュリティ。**OSSの脆弱性を発見して修正するシステムを開発することを目的としたDARPAの2年間のArtificial Intelligence Cyber Challenge (AIxCC) コンペティションは、8月の決勝戦で終了します。OpenSSFは、研究からOSSプロジェクトとしてリリースするための技術移転を支援するコンペティションのコラボレーターであり、重要なインフラストラクチャの保護を支援します。より広い意味では、OpenSSFはLF AI & Data財団と協力し、AI/MLがOSSのセキュリティを (低下させるのではなく) 向上させるための指針を確立するアプローチを開発しています。

7. **調査。**私たちは引き続きLinux Foundation Researchと協力して、2025年の活動に役立つ情報を提供するために、年初に公開することを目標とした二つの調査を行います。CRA Readiness SurveyはOpenSSFプログラミングを活性化する触媒となり、CRA Best Practices reportは特定のプロジェクトがCRAに準拠するためのギャップを埋める方法を調査します。

8. **コミュニティの構築とアウトリーチ。**OpenSSFは、すべての人のためにオープンソース ソフトウェアのセキュリティを向上させるという共通の使命の下で協力している人々の素晴らしいコミュニティと継続的に関わ り、拡大しています。ここ数か月で行った具体的なアクションには、次のようなものがあります。

» 2つのDARPAプログラム、AIxCCとE-BOSSとの関わりを通じて、AIxCCコンペティションの主催者を Fuzzing Collaboration Special Interest Groupに、E- BOSSプログラムの研究チームをSecurity Tooling Working Groupに参加させました。

» オープンソース ソフトウェア開発とサイバーセキュリティの世界に学生や転職者を引き込むための指導プログラムを開発しています。

» コミュニティワークショップを開催して、財団内外に存在する多くのオープンソースSBOMツールの相乗効果とコラボレーションについて議論しています。

» Alpha-Omegaプロジェクトやその他のオープンソーススチュワードや財団などのエンティティとの長年にわたるコラボレーションは、私たちの共同作業の範囲を拡大し、コミュニティのセキュリティに実際の影響を与えるのに役立ちました。2024 Alpha- Omega report（日本語版はこちら）は、最近の成果をまとめたものです。

» 国際的には、OpenSSFとLinux Foundationは、オープンソースコミュニティをさらに増やすために大きく前進しました。私たちは、インド、日本、韓国、その他の国で積極的に活動しており、コミュニティによって作成および維持されている知識とツールを提供しています。

» グローバルな公共政策に関して言えば、OpenSSFは政策サミットを開催し、業界関係者、規制当局、および公共政策の専門家を招集してきました。これまでにワシントンD.C.（2023年）やブリュッセル（2024年）で開催し、サイバーセキュリティが世界的な課題となる中、日本や韓国などの地域にもこの協力関係を拡大する計画です。

9. 今後の展望

» サイバーセキュリティは常に進化し続けるチームスポーツです。私たちは進化に投資し、技術の水平線に目を光らせ、オープンソース開発者、消費者、政府の多くの課題を解決するために、新しい技術の出現や新しいソリューションの出現に適応していま す。来年、OpenSSFは以下の分野で新たな取り組みや改良を行う予定です。

» 私たちのAI/MLワーキング グループは、このまだ新興の分野に存在するセキュリティ上の課題について議論を続けています。グループは、AI/ML/LLM/生成AIにDevSecOpsプラクティスを実装するためのリファレンス アーキテクチャを開発し、これらのコミュニティにおける認知度を高めて、これらの重要な新技術の開発にセキュリティのベストプラクティスを組み込めるようにすることを計画しています。

» 私たちのセキュリティベースラインを形成する標準ベースの基準に基づいて、他のコミュニティと協力し、機械読み取り可能な証明書を作成し、セキュリティ実践者の証拠を収集する手段を開発して、下流のコミュニティが上流のソースで使用されているプラクティスを保証できるようにすることを計画しています。

» 私たちの主要な能力の一つは、メンバーやコミュニティが協力し合い、将来的に国際的に認められる標準となる可能性のある仕様を策定するための、オープンで透明性が高く中立的なフォーラムを提供することです。これらの取り組みは、エコシステム全体で望ましいセキュリティ成果を調整する上で極めて重要です。OpenSSFおよびLinux Foundation全体は、コミュニティの複数の仕様を、認定された標準やベストプラクティスへと導く支援を行っていきます。このプロセスの対象として、OpenChain、SLSA、OpenVEX、オープンソース脆弱性スキーマ、およびセキュリティ ベースラインなどのフレームワークが検討されています。

» NIST SP 800-53（サイバーセキュリティ フレームワーク）NIST SP 800-218（セキュアソフトウェア開発フレームワーク）のようなセキュリティ フレームワークなどは、企業がソフトウェアを開発、取り込み、展開する方法を形成する上で重要な要素です。セキュリティ ベースラインは、これらのさまざまなフレームワークや規制を統合し、どこでセキュリティ活動が適用されるかを明示します。このベースラインは、すべてのLinux Foundationプロジェクトに採用される標準として提案され、セキュリティ活動がどこで下流の消費者の理解と自らのプログラムの正当化に役立つかを示すことを目的としています。

» 私たちのメンバーとコミュニティが新たな規制に備え、教育を受ける手助けをする取り組みの一環として、OpenSSFのグローバルサイバー政策作業部会は、グローバルな規制およびサイバーセキュリティ フレームワークに焦点を当てた一連の教育コースを作成します。これらのコースの最初の提供は、今年後半に「CRA 101」指導コースとして公開される予定です。このコースでは、2027年に欧州で本格的に施行される予定のサイバーレジリエンス法 (CRA) に関する要素と、その法律が施行される際に利害関係者がコンプライアンスを主張するために開発すべき重要な能力について説明します。これは、オープンソース開発者とオープンソース利用者の両方の準備を支援するための多くの教育的取り組みの最初となるでしょう。

» Cloud Native Computing Foundation（CNCF）との提携により、OpenSSFは学術認定プログラムを開始します。このプログラムでは、大学や専門教育機関が申請し、業界の専門家によって決定され、厳選されたクラウドおよびセキュリティのコースを教える資格を得ることができます。このプログラムは、学生が現代の労働力のニーズに応えるためのスキルを学ぶ手助けをすることを目的としています。

本訳文について

この日本語文書は、Secure Open Source Software Vision Brief 2025の参考訳として、The Linux Foundation Japanが便宜上提供するものです。

翻訳協力：木下 兼一

openssf.org