Alpha-Omega

2024 アニュアル レポート

もくじ

エグゼクティブ サマリー

オープンソース ソフトウェアは、単なるテクノロジーの 1 つではなく、政府の主要な業務から私たちが日常的に使用するスマートフォン アプリまで、あらゆるものを支えるデジタル基盤です。その強みは、オープンソース プロジェクトの作成やメンテナンスに時間と専門知識を注いでいる、無報酬であることも多い献身的なボランティアによるグローバル ネットワークにあります。しかし、重要なインフラのセキュリティを確保するためにこうした個人に頼っている以上、彼らが担っている大きな責任を認識し、単に彼らの負担を増やすだけで終わらないようにしなければなりません。リソースへの投資、サポートの提供、持続可能なコントリビューションの経路の構築を通じて、オープンソース ソフトウェアを保護し、強化することができます。

2024 年にオープンソース プロジェクトを立ち上げ、メンテナンスし、コントリビュートしてくださったすべての方々に感謝いたします。

2024 年、Alpha-Omega は主要なオープンソース プロジェクトのセキュリティ改善のために、約 450 万ドルの助成金を交付しました。特に、私たちは以下を行いました。

- Python Software Foundation、OpenJS、RubyGems、Rust Foundation など、最も重要なオープンソース組織 10 社のスタッフ セキュリティチームを支援
- Linux カーネルや Homebrew など、クリティカルなインフラを強化するための助成金を支給
- OpenSSL を含むファウンデーション テクノロジーのセキュリティ監査費用を負担
- 脆弱性の発見と修正に対する段階的なアプローチを試行し、Rust による TLS と AV1 コーデックの実装をサポート
- 助成金受給者との座談会を 4 回開催し、専門知識の交換を行い、2025 年に向けた戦略を策定

Alpha-Omega は、Amazon Web Services (AWS)、Google、Microsoft からの寛大かつ重要な寄付によって運営されています。これらの助成金により、世界で最も重要なオープンソース プロジェクトやエコシステムの多くにおいて、長年のセキュリティ上の課題に対処し、プロセスを改善し、インフラを強化することが可能になりました。さらに重要なことは、私たちが協力するコミュニティにおいて、持続可能なセキュリティ文化を確立することができたことです。

Alpha-Omega の助成金と、受賞者のエネルギー、リーダーシップ、コミットメントの組み合わせは、上手く機能した方法であり、2025 年にも引き続き適用していきます。

Alpha-Omega とは？

Alpha-Omega は、2022 年 2 月に設立された OpenSSF の関連プロジェクトであり、Microsoft、Google、Amazon の資金提供を受け、最も重要なオープンソース ソフトウェア プロジェクトおよび、エコシステムに持続可能なセキュリティ改善を促すことで社会を守ることをミッションとしています。このプロジェクトは、クリティカルなオープンソース プロジェクトがセキュアであり、セキュリティ脆弱性が迅速に発見・修正される世界を構築することを目指しています。

Alpha-Omega は、広範囲にわたって大きな影響を与える可能性のあるプロジェクトへの資金提供の機会を常に探しています。私たちは、関与するプロジェクトや組織において、持続的な変化を促進し、実現することを目指しています。これまでの投資先は、エコシステム、コア プラットフォーム、パッケージ マネージャー、プログラミング言語、そして多くのプロジェクトのセキュリティを向上させる組織的な意思と能力を持つファウンデーションなどです。これは、組織全体のセキュリティ文化を導き、改善するセキュリティ関連の役割を担う人材を確保する形をとることが多いです。時には、簡単な監査から始めることもあります。また、多くのプロジェクトにわたる脆弱性の全体的な発見や解決により、複数のプロジェクトに拡張可能なツールやソリューションにも投資しています。これは、組織や文化の大幅な変革から、数千のプロジェクトに拡張可能なテクノロジーまで、Alpha-Omega の幅広い範囲を象徴しています。

Alpha-Omega プロジェクトは、試行錯誤を重視しています。オープンソース コミュニティにおけるセキュリティ リスクへの最善の対処法が常に明確であるとは限りませんが、私たちは投資を行い、何が有効で何が有効でないかを学び、時間をかけてアプローチを改善していきます。プロジェクトの選択方法や、最も大きな影響を与える活動の種類など、コミュニティからのご意見を歓迎いたします。

スポンサーおよびサポーター

Alpha-Omega プロジェクトのスポンサーおよびサポートをいただいた以下の組織に感謝いたします。
これらの組織の支援により、オープンソース ソフトウェアのセキュリティ向上が可能となりました。

amazon web services
Google
Microsoft
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

エンゲージメント パートナー

また、Alpha の取り組みに関わったパートナー組織にも感謝いたします。これらの組織は、何百万人もの
開発者と何十億ものエンドユーザーが使用するソフトウェアをメンテナーしています。

Apache Airflow
COMPOSER
ECLIPSE FOUNDATION
FreeBSD FOUNDATION
Jenkins
Linux
node JS
Open Refactory
OSTIF.org
PROSSIMO
python SOFTWARE FOUNDATION
Ruby Central
Rust Foundation

2024年の助成金による影響

Airflow

「Airflow Beach Cleaning」プロジェクトは、オープンソース ソフトウェアのサプライチェーン問題に対処するための革新的なアプローチを模索しています。個々のプロジェクトのセキュリティ対策を改善することを目的としたツールやプロセスの既存の基盤をもとに、Airflow Beach Cleaning プロジェクトは、相互に依存するオープンソース プロジェクトのメンテナ間のコミュニティの交流に人間的な要素を取り入れ、意識を高め、貢献し、時間、エネルギー、集中力を注ぎ込み、場合によってはオープンソースのプロジェクト依存の連鎖に資金を投入することを目的としています。

このプロジェクトのゴールは、Apache Airflow Python サプライチェーン（700 以上の依存関係）から始まるエコシステムにおける重要部分のオープンソース サプライチェーン全体のセキュリティを全体的に改善し、効果的に資金を調達することです。また、業界全体で、資金提供を行う企業やオープンソース メンテナーが持続可能な方法で適応し、遵守することを目指しています。

このプロジェクトは進行中で、Airflow の依存関係の初期バッチとの対話がすでに始まっており、メンテナーから肯定的なフィードバックを得た後、セキュリティの改善に取り組む予定です。この作業の初期段階で、Airflow コミッター コミュニティが直接関与する優先順位の高い依存関係プロジェクトが 16 件特定されました。これらの関与により、プロジェクト メンテナーとコラボレートして、新たなインサイトと直接的な改善（例：Trusted Publishing のサポート）がすでに生み出されています。

Rust

2024 年、Rust Foundation は、セキュリティ イニシアチブのサポートとして、OpenSSF の Alpha-Omega プロジェクトから引き続き多額の資金提供を受けました。これにより、Rust Foundation のセキュリティ イニシアチブは、2024 年に Rust エコシステムのセキュリティ インフラを強化することができました。

セキュリティ エンジニアの Walter Pearce とソフトウェア エンジニアの Adam Harvey は、サプライチェーン セキュリティ、脆弱性検出、オープンソース コミュニティを潜在的な脅威から保護するためのツール開発に重点的に取り組みました。

2024 年のハイライト：

- チェーンと信頼性の提供、およびパッケージとリリースに署名を実装するためのアップデート フレームワーク（TUF）の採用と実装を提案する TUF RFC を公開
- 依存関係グラフ データベースを構築するためのオープンソース ツールである Painter をさらに開発
- 上位 5,000 ケースの包括的な出所の追跡を実施

Eclipse Foundation

私たちのゴールは、セキュリティのベスト プラクティスを実証するオープンソース コミュニティのリーダーとして、Eclipse Foundation を確立することです。Alpha-Omega のサポートにより、Eclipse Foundation セキュリティ チームは、Eclipse Foundation (EF) コミュニティにオープンソース ソフトウェアのコラボレーションとイノベーションのためのセキュアな環境を提供しています。また、Eclipse Foundation のプロジェクトでコラボレートする個人や組織がサイバー脅威を理解し、制御、防御の対応ができるように支援しています。2024 年には、チームは EF の 400 以上のプロジェクト全体で一貫性のある効果的な脆弱性管理を確立しました。VulnCon で発表し、規模の大きい脆弱性管理に対する当社のアプローチについて、世界中で講演を続けています。

2024 年には、すべての脆弱性が公開前に解決され、セキュリティ研究者が新しい脆弱性を報告する際には、タイムリーかつ効率的なコミュニケーションが確保されました。さらに、チームは GitHub と GitLab の両方で EF リポジトリの 81% にポリシー評価と強制を実装し、すべての EF リポジトリで MFA の全面的な採用につながりました。EF インフラストラクチャの 40% 以上が新たに統合された IAM、Keycloak に移行され、2025 年にはこれらのアプリケーションで MFA が利用可能になる道筋が整いました。さらに、Sigstore が既存のコード署名インフラストラクチャに追加され、すべての EF プロジェクトで利用可能になりました。

EF セキュリティ チームが確立したセキュリティ体制を活用し、Eclipse Foundation は、サイバーセキュリティの観点から、企業や政府機関にとって重要な関係者としての信頼性を確固たるものにしました。これにより、EF は 2024 年においても主導的な役割を維持し、オープンソース コミュニティが、特に欧州委員会内の政策立案者に対して、サイバーレジリエンス法に関してビジビリティを維持することを可能にしました。2024 年 4 月、Eclipse Foundation はオープン規制コンプライアンス作業部会の創設を主導しました。 このコラボレーションの取り組みは、政府機関と提携し、ソフトウェアのサプライチェーンを通じてオープンソースを活用し続けながら、業界が規制要件を満たせるようにするものです。 さらに、このイニシアチブは、急速に進化する業界のニーズにより適切に対応できるよう、オープンソース プロジェクトを強化します。

FreeBSD

FreeBSD プロジェクトは、FreeBSD Foundation が管理する Alpha Omega からの 13 万 7500 ドルの助成金のサポートを受け、セキュリティ対策の拡張に大きな一歩を踏み出しました。この資金は、2024 年 6 月に 2 つの重要なイニシアチブをローンチする上で極めて重要な役割を果たしました。その 2 つのイニシアチブとは、bhyve hypervisor と Capsicum sandbox の包括的なコード監査、および開発プロセスの継続的なプロセス監査です。これらの取り組みは、脆弱性への対応、セキュリティ慣行の改善、そして世界的なデジタル インフラストラクチャの主要コンポーネントである FreeBSD の長期的なレジリエンスの確保を目的としています。

セキュリティ企業 Synacktiv が実施したコード監査では、bhyve hypervisor に重大な脆弱性があることが判明しました。その中には、攻撃者がゲスト バーチャル マシンからホスト システムに特権をエスカレートさせることを可能にするエクスプロイトも含まれています。Capsicum の保護機能は堅牢であると判断されましたが、1 つのクリティカルなカーネルの問題とオプションのサービスにおける軽微な脆弱性が発見されました。FreeBSD プロジェクトのセキュリティ チームは、これらの脆弱性を迅速に修正し、セキュリティ勧告を発行するとともに、監査結果を基に、今後同様の脆弱性を低減するための戦略を策定しました。

2024 年末までに完了予定のプロセス監査は、FreeBSD の開発手順を拡張し、将来的なセキュリティリスクを最小限に抑えることに焦点を当てています。これらのイニシアチブは、監査結果を公表し、セキュリティ対策の強化に役立てるなど、積極的なセキュリティ対策への FreeBSD Foundation のコミットメントを反映しています。

Jenkins

2024 年 10 月、Alpha Omega Foundation は、Jenkins エコシステム全体におけるコンテンツ セキュリティ ポリシー（CSP）の実装を改善するために、Jenkins プロジェクトに 3 か月間の助成金を支給しました。 クロスサイト スクリプティング（XSS）のようなインジェクション攻撃から Jenkins を保護することで、Jenkins のセキュリティを拡張することがゴールです。

このプロジェクトは、テクニカル リードの Basil Crow、および開発者の Yaroslav Afenkin と Shlomo Dahan を中心に進められています。この 2 か月間、チームは目標に向けて大きな進歩を遂げました。この作業は 2025 年初頭にも継続される予定です。

Linux Kernel

C コンパイラーは、よくある問題を警告し、防止するために、多くの機能を追加してきましたが、Linux のような古いレガシー コードベースで作業する場合、それらの機能を有効にすると、誤検知が数百件発生し、修正が必要になるため、多くの混乱が生じることがあります。OpenSSF は、Linux がこれらの新しいオプションの多くを有効にできるようにするための作業に資金援助を行いました。例えば、正しく設定するのが難しい可変長配列を無効にするなどです。その証拠に、作業中に、メモリの上書きがサイレントに行われるために過去には気づかれなかった多くの重大なバグが発見され修正されました。また、キャスト機能タイプが有効になり、カーネルによって関数へのポインタが渡される際に、常に正しいタイプであることが保証されるようになりました。また、コンパイラーが自動的に追跡できると期待しているものに適切に動作するようにコードをリファクタリングすることで、文字列のオーバーフローを自動的に検出できるようにする作業も行われました。この作業により、主要な C コンパイラーに新しいコンパイラー機能が開発され、厳格な柔軟配列のサポートと、コンパイラーが構造体のフィールドの予想される長さを自動的に追跡できるようになり、これらのセキュリティ機能が C のすべてのユーザーに提供されるようになりました。

コンパイラーで新しいセキュリティ機能を有効にする取り組みと並行して、Linux が LLVM コンパイラー スイートと引き続き適切に動作するようサポートする取り組みが OpenSSF から資金提供を受けました。コンパイラーの新しいバージョンはカーネルのコードベースに対してテストされ、必要に応じてカーネルに必要な修正が実装され、バグがコンパイラー開発者に報告されます。Rust の Linux サポートには LLVM のフルサポートが必要であるため、この継続的な作業は、Rust の統合が長期的に適切に機能することを保証するために、カーネルの将来にとって不可欠です。

OpenJS

2024 年、Nodejs プロジェクトはセキュリティ面で大きな進歩を遂げ、Alpha-Omega プロジェクトによる積極的な対策が注目されました。この取り組みにより、5 月に報告された 34 件の報告に対応するセキュリティ リリースが、MITRE を介した他の言語やランタイムとのコラボレーションを含め、すべてのアクティブな Nodejs ラインで実施されました。OpenJS Foundation のサポートと、AlphaOmega による専任のフルタイム セキュリテ ィエンジニアへの投資により、Nodejs はセキュリティ対応からセキュリティ対策へとスタンスを転換し、対応時間を短縮し、リリース頻度を高めることができました。

今年度の主なアップデートには、セキュリティ リリース プロセスを合理化する自動化の改善が含まれ、いくつかの手動タスクを統合する新しいコマンド「git node security」が追加されました。Nodejs Permission Model はアクティブに開発が進められ、バッファへのサポートが追加され、Nodejs 開発者にとってより使いやすい

ように API が調整されました。Nodejs セキュリティ チームは、エコシステム全体のセキュリティを常に改善しています。Microsoft とのコラボレーションにより、新しいポリシー整合性の機能が開発されており、Nodejs バイナリーにおける脆弱性を特定するツール（is-my-node-vulnerable）がリリースされています。

Nodejs コミュニティは、テストの拡張、Next 10 Working Group による実験的機能の改良、イベントや新しいメンタリング チャネルを通じたコントリビューターの参加促進にも重点的に取り組みました。これらの対策は、技術的な改善とアクティブなコミュニティの関与の両面からセキュリティに強くコミットしていることを反映しています。

OpenRefactory

2024 年、Alpha-Omega は OpenRefactory に 2 つの助成金を交付しました。それらは異なるゴールを持っていました。上半期のゴールは、オープンソースのセキュリティ監査を大規模に行うことでした。下半期のゴールは、3 つのオープンソース プロジェクト（Apache Airflow、Jenkins、Kubernetes）のメンテナーとコラボレートし、これらのプロジェクトの最新リリースのサプライチェーンの依存関係をすべて詳細に分析し、これまで検出されていなかった脆弱性に関する独自のリスク シグナルを提供し、リスクを管理する方法について実行可能なアドバイスを提供することでした。2024 年の間に、9000 以上のパッケージが分析され、30 件の重要度の高いセキュリティおよび信頼性のバグ（合計 75 件中）が報告されました。OpenRefactory チームと Apache Airflow のリーダーシップとのコラボレーションは、報告されたバグに対するメンテナーの対応を改善する上で多大な影響を与えました。

OSTIF

2024 年に Alpha-Omega がオープンソース技術改善基金（OSTIF）と提携した結果、オープンソース エコシステムに大きな影響を与えるセキュリティの改善がもたらされました。Alpha-Omega は、独立した専門家によるカスタマイズされたセキュリティ作業、長期的な強化推奨、プロジェクト用の新しいまたはアップデートされたテスト スイートを含む、2 つのセキュリティ契約をスポンサーしました。OSTIF 監査は、メンテナーに即座にフィードバックとガイダンスを提供するだけでなく、プロジェクトのセキュリティを前進させるためのサポート方法に重点を置いています。将来を見据え、これらのプロジェクトは、OSTIF の取り組みと Alpha-Omega のサポートにより、プロジェクト メンテナーやセキュリティ専門家の努力が確実に反映され、セキュアなオープンソース ソフトウェアを提供できると確信しています。

Prossimo

インターネット セキュリティー 研究グループ（ISRG）の Prossimo プロジェクトのゴールは、インターネット上の最もクリティカルなソフトウェア インフラにメモリの安全性をもたらすことです。メモリ セーフ コードへの移行により、セキュリティ侵害やデータ漏洩につながる脆弱性が排除され、インターネット ユーザーの個人情報や金銭的な被害、不可欠な公共サービスの全面的な拒否、基本的人権や安全に対する脅威を回避することができます。Alpha-Omega の惜しみないサポートのおかげで、2024 年、ISRG は 3 つの Prossimo イニシアチブ、Rustls、Rust for Linux、rav1d の進展によりインターネット セキュリティを改善しました。オープンソースでメモリ セーフな TLS ライブラリである Rustls の開発は、そのパフォーマンスと機能性を向上させ、メモリ セーフではなくバグに脆弱な主要 TLS ライブラリである OpenSSL と競合できるようにすることを中心に展開されました。 何十億もの電話、コンピューター、サーバー、IoT デバイス、およびエンベデッド システムが TLS に依存してネットワーク上でセキュアに通信しているため、OpenSSL の代替としてメモリ セーフな TLS を提供することは、インターネット セキュリティの向上にクリティカルな要素です。

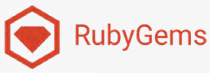
2022 年後半にオープンソースの Linux kernel に組み込まれる予定の、セキュアな Rust プログラミング言語のサポートは、インターネットと Linux に依存するすべてのもののセキュリティ強化に向けた大きなマイルストーンとなりました。2024 年には、Linux 用の Rust の主要メンテナーである Miguel Ojeda と協力し、Rust の Linux kernel へのサポートを継続的に改善することで、Rust の最初の主要な商用ユーザーをアップストリームに統合できるようにしました。

また、映像と画像の両方に使用できる、メモリ セーフな AV1 デコーダー「rav1d」の開発にも取り組みました。複雑なデータの解析は、モダナイゼーションにおけるソフトウェアの最もクリティカルなセキュリティ操作の 1 つであり、AV1 がインターネット上で最も重要なメディア フォーマットの 1 つになる予定であることを考えると、ビデオ デコーダーにとっては特に大きな問題となります。このため、高性能なメモリ セーフ AV1 デコーダーが利用可能であることが重要です。

Python Software Foundation

Alpha-Omega のサポートにより、Python Software Foundation は 2024 年にセキュリティ開発者 Seth Larson を常勤で雇用することができました。Seth は、CVE レコードのアップデートを自動化し、CPython の依存関係を追跡して、正確なソフトウェア部品表（BOM）ドキュメントを生成し公開するためのインフラを構築することができました。また、プロセス全体を監査し、ビルド パイプラインを強化し、Sigstore 検証材料の問題を修正することで、CPython のリリースをセキュアにしました。この作業のおかげで、Python ユーザーは、Python アプリケーションのランタイムとその依存関係のセキュリティと統合性を信頼することができます。

オーサリング ガイドやブログ投稿からカンファレンスでの講演やポッドキャストまで、Seth が Python コミュニティやセキュリティ コミュニティで継続的にコラボレートしてきたことは、Python エコシステムを超えた改善のきっかけとなっています。セスが作成したガイドを使用することで、Linux kernel は CVE ナンバリング オーソリティとなり、Nuget と Cratesio は Trusted Publishers を採用するための提案を作成しました。



RubyGems

Alpha-Omega のサポートにより、Ruby Central は 2024 年に 2 つの重要なプロジェクト、RubyGems.org の外部セキュリティ監査と RubyGems.org への組織アカウントの追加に着手することができました。外部セキュリティ監査 Ruby Central は Trail of Bits と提携し、RubyGems.org Rails アプリケーションとその基盤となる AWS インフラストラクチャの包括的なセキュリティ監査を実施しました。この監査では、中程度の重要度 7 件、高重要度 1 件を含む 33 件の問題が特定されました。注目すべきは、これらの問題のほとんどが実際のセキュリティ侵害には至っていないということです。当社のチームは、報告された問題のひとつひとつに対処し、これらの知見を活用して RubyGems のセキュリティ体制を強化しました。

Trail of Bits

Alpha-Omega の資金提供により、Trail of Bits は Homebrew と Python パッケージング エコシステムの両方において、**大幅なセキュリティと持続可能性の改善**を実現することができました。この 12 か月の資金提供を通じて、私たちは以下のことを行いました。

- Sigstore ベースの認証および証明書の生成を、パッケージ マネージャー「Homebrew」に実装し、公式インデックス内の全パッケージを対象とした **100% の認証適用率を達成した初の主要パッケージ エコシステム**としました。
- すべての Homebrew 認証に対して、**キーや ID の管理**を必要としないユーザー側での認証フローを実装
- Sigstore の Python リファレンス実装に、主要な **UX、API、CLI の改善**を実装し、下流アプリケーション（PyPI 用の PEP 740 インデックス認証）と Ruby および Go Sigstore クライアント用のリファレンス材料としての両方を実現

助成金受給者レポートの全文を表示するにはこちらをクリックしてください。

スタッフの学び

2022 年 2 月に設立された OpenSSF の関連プロジェクトであり、Microsoft、目の前で開発が進むセキュアリング オープンソース コミュニティの様子を見ることができたのは、大きな収穫でした。 シアトルとウィーンで行われた対面式のラウンドテーブルでは、当社が資金援助しているさまざまなグループの人々が、新しいコンセプトや懸念事項を共有し、未来についてブレーンストーミングを行っていました。 これらの会話は、2025 年への当社の資金援助の目標に直接的な影響を与えました。

Alpha がレバレッジを表すなら、Omega は規模を表します。私たちは、数十万のプロジェクトにわたって脆弱性を発見し修正するために自動化を適用しようとして、多くのことを学びました。初期の取り組みは、太平洋ゴミベルトに船を出すようなものでした。多くの作業が行われましたが、全体的な影響は漠然としていました。2024 年、私たちは異なるアプローチを試みました。つまり、1 つずつビーチをきれいにするのです。Apache Airflow から始め、影響を与える特定の領域を定め、脆弱性よりも Airflow の依存関係グラフにある 719 のプロジェクトすべての長期的なセキュリティ対策に焦点を当てました。最も大きな成果が見られたのは、Airflow のメンテナーが依存関係にあるプロジェクトと 1 対 1 のつながりを築いたときでした。驚くべきことに、オープンソースでは人間が重要であることが分かりました。

2024 年、OpenSSF Alpha-Omega プロジェクトは、変革のきっかけとなりました。 オープンソース コミュニティ内で幅広い影響力を発揮し、報われている献身的で情熱的な人々を見るのは感動的でした。 彼らのアイデアを共有し、相互に活用しようという意欲は、彼らのプロジェクトを拡張するだけでなく、エコシステム全体を向上させるという利益をもたらしました。要するに、私たちはボールを転がし、それが勢いを増しながら成長し、加速しながら坂を下っていくのを見守ることができたのです。

オープンソース ソフトウェア（OSS）プロジェクトへの資金不足はしばしば嘆かわしいこととして指摘されますが、それ以上にクリティカルなギャップは、セキュリティ上の懸念に対処するための専任の時間が不足していることです。資金は、プロジェクト自体だけでなく、セキュリティへの集中的な取り組みを可能にするためにも不可欠です。これには、人材、包括的な監査、高度なツールの開発、セキュリティのベスト プラクティスの普及のためのリソースが含まれます。AlphaOmega は、これらの分野に戦略的に投資することで、複数のオープンソース ソフトウェア（OSS）コミュニティに力を与え、システム的なセキュリティ問題の優先順位付けと取り組みを可能にし、最終的には、すべての人の利点となるオープンソース ソフトウェア（OSS）エコシステム全体を強化しています。

私たちの働き方

成功の要因

Alpha-Omega のビジョン達成に向けて、クリティカルなオープンソース プロジェクトの作業に資金を提供しています。資金が利用可能であれば、セキュリティ対策の改善に向けて急速な進歩を遂げることができるプロジェクトです。この両面は重要です。私たちは、限られたリソースを最大限に活用し、社会に最も大きな影響を与えることを目指しています。また、その影響が迅速に示されることを望んでいます。

クリティカルなプロジェクトは次々と発生し、ある一定の粒度以下のプロジェクトのクリティカル度を定量的に測定する方法があるとは確信できません。Nodejs は Python よりもオープンソース エコシステムにとって重要でしょうか？ GCC は React よりも重要でしょうか？興味深い研究分野ではありますが、私たちが答えを出そうとするには重要な質問ではないと考えています。それらのプロジェクトはすべて重要であり、それぞれに資金提供を検討すべきです。とはいえ、私たちは Securing Critical Projects ワーキング グループの作業から情報を得ており、クリティカル プロジェクトのセットに常に注目しています。

そこから、私たちはテコ入れのポイントと「すぐに着手できる状態」を探します。これにより、Rust のようなエコシステムや、Eclipse Foundation のようなファウンデーションへの投資につながりました。これらの組織では、非常に多くのエンドユーザーに影響を与えます。一般的に、これらの組織はすでにセキュリティの才能ある人材と関係があり、彼らの雇用とマネージャーとしての能力を持っています。このアプローチにより、Alpha-Omega プロジェクトでは少ないリソースでより多くのことを行うことができました。

私たちの「不干渉だが、報告は求める」というアプローチはうまく機能しています。 重要なセキュリティ作業を効率的に行う成熟度を備えた組織の変革を促すことに焦点を当てることで、私たちは最も効果的に活動することができます。 私たちが協力する組織が、そこで得た知識や教訓を私たちやより広範なコミュニティに還元できる場合に、私たちは最も多くを学ぶことができます。 私たちは、これらの会話をアクティブに管理し続けていきます。

4 つの戦略

過去の助成金交付とそこから得られた教訓を基に、私たちは助成金の 4 つのカテゴリーを定義しました。

この投資のカテゴリー分けは、アメリカの考え方や助成金交付プロセスにとって、引き続き重要なフレームワークとなっています。これにより、より長期的な計画を立て、期待する効果を明確にすることができます。

セキュリティ スタッフ

コミュニティのセキュリティ文化を変える最も効果的な方法のひとつは、それを誰かのジョブにすることですが、さらに重要なのは、それを適任者に任せることです。 私たちは、設立以来、このことが何度も繰り返されてきたのを見てきましたが、これは驚くことではありません。 オープンソース コミュニティは人々によって成り立っており、コミュニティの信頼されたメンバーが先導することで、すべてが変わります。

もう一つの重要な気づきは、オープンソース コミュニティの集合体自体がコミュニティであるということです。定期的にセキュリティ リーダーを集めて座談会を開くことで、共有ソリューションが導き出されるようになりました。この素晴らしい例として、パッケージ マネージャー全体に広がり、プロジェクトに採用されている、信頼性の高いパブリッシングに関する取り組みが挙げられます。もう一つの例としては、小規模なプロジェクトのライフサイクル終了と危機管理に関する議論が挙げられます。Alpha-Omega チームは、コミュニティ メンバーと定期的にアイデアを議論しており、私たちの仕事は、そこから得られたフィードバックから利点を得ています。

アーティファクト リポジトリ

PyPI や Homebrew のようなパッケージ マネージャーが提供する形のアーティファクト リポジトリは、モダナイゼーション「※見出しのみ 既存システムの刷新 併記」における「App Store」であり、すべての開発者のワークフローにおける信頼のクリティカル ポイントです。2023 年 3 月の XZ Utils 攻撃から、npm に公開されたマルウェアの定期的な報告まで、私たちはこれらの中央リポジトリが悪意のある攻撃者の格好の標的になり得ることを知っています。しかし、その中心的な役割は、Alpha-Omega がスケーラブルな影響力を持つ可能性があることも意味します。

つまり、セキュリティへの投資は、エコシステム内のすべてのパッケージとすべてのユーザーのセキュリティを向上させることができるのです。この素晴らしい例として、私たちが Homebrew と共同で資金提供した、エコシステムを通じて利用可能なほぼすべてのプロジェクトにビルドの由来とコード署名を導入する取り組みが挙げられます。

監査と改善

セキュリティ監査はオープンソース セキュリティの「生命線」であり、当社の業務の多くは監査とその後の改善作業から始まりました。これらの監査はセキュリティ上の欠陥を特定し、対処するだけでなく、セキュリティを恒久的な文化規範とするための組織改革を促す費用対効果の高い手段であることが分かっています。

これらの従来の監査に加えて、私たちは定期的に、多数のプロジェクトを対象とした「ライトウェイト」で狭い範囲の監査にも資金を提供しています。例えば、Apache Airflow による OpenRefactory との「ビーチクリーン」作業や、10,000 件の PyPI プロジェクトのスキャンなどです。

革新と挑戦

Alpha-Omega は挑戦の精神をもって設立され、その精神を維持してきました。そして、創業当初よりも賢明になったとはいえ、まだまだ学ぶべきことはたくさんあります。解決が本当に難しい問題もありますが、特に変化、水平、垂直のいずれかを促進するために使用される場合、挑戦と革新の利点があることを認識しています。

オープンソース セキュリティに関する書籍の多くはまだ執筆されておらず、また、解決すべき重要かつ困難な問題もまだ多く残されています。 特に、私たちが直接対応できない膨大なオープンソースの規模にスケールするイノベーションやソリューションに興味を持っています。

リーダーシップ チーム

Alpha-Omega プロジェクトは、以下のコア リーダーシップ チームによって運営されています。

Michael Scovetta, Microsoft

Michael は、Microsoft 社のオープンソース セキュリティ チームを率いており、新たなソフトウェア サプライチェーン セキュリティの脅威の理解と対処に重点的に取り組んでいます。 セキュリティ ツールの構築、エンジニアリング チームへの助言、およびベスト プラクティスの普及を通じて、この取り組みを行っています。 OpenSSF では、Michael は Alpha-Omega プロジェクトを共同で主導しています。 マイケルは、ソフトウェア エンジニアリングとセキュリティの分野で約 25 年の経験を有しており、Cornell 大学でコンピューター サイエンスのエンジニアリング マスター、Hofstra 大学で理学士の学位を取得しています。

Bob Callaway, Google

Bob Callaway は、Google 社のオープンソース セキュリティ チーム（GOSST）のリーダーであり、オープンソース ソフトウェアのセキュリティ強化に向けたイニシアチブを主導し、Google 社と世界中のコミュニティに利点をもたらしています。彼のリーダーシップの下、GOSST チームはサプライチェーンの完全性、オブザーバビリティー、脆弱性管理などのクリティカルな領域に取り組むプロジェクトの開発とコントリビューションを行っています。GOSST は、OSV、Sigstore、Certificate Transparency ログなど、不可欠なインターネット インフラ サービスの管理においても重要な役割を果たしています。 ボブは、主要な組織の諮問委員会のメンバーも務めており、OpenSSF の技術諮問委員会のメンバー、Sigstore の共同創設者および技術運営委員会のメンバー、Alpha-Omega プロジェクトのリーダーシップ チームにおける Google 社の代表を務めています。

また、Red Hat、NetApp、IBM でのエンジニアリングおよびリーダーとしての豊富な経験も持っています。Bob は NC State 大学でコンピューター エンジニアリングの博士号を取得しており、同大学では ECE 学部の非常勤助教授として専門知識を共有しています。

Henri Yandell, Amazon Web Services

Henri はオープンソースの大規模な組織化を専門としている。2001 年にジャカルタおよび Apache Commons プロジェクトのコミッターとしてキャリアをスタートさせ、その後、Apache Software Foundation の法務委員会およびセキュリティ委員会の委員、および理事会メンバーを務めました。2007 年からは Amazon 社でオープンソースを主導し、ライセンシング、アップストリーム、企業プロジェクト、そして現在ではオープンソース セキュリティの成長分野に取り組んでいます。

Michael Winser, XWind.io

Michael はソフトウェア業界で 40 年の経験を持ち、そのうち 25 年は Google 社と Microsoft 社で働いていました。Google 社在籍中に Alpha-Omega を共同設立しました。Michael はソフトウェア サプライチェーン セキュリティ、ソフトウェア開発、開発者エコシステムにおける業界の専門家です。Alpha-Omega の業務に加え、マイケルは企業やオープンソース組織と協力し、セキュリティ戦略の開発と実行に取り組んでいます。また、Michael は Eclipse Foundation のセキュリティ戦略大使も務めています。

これらの人々がもたらすオープンソース、ソフトウェア開発、セキュリティにおける経験の影響力は、彼らの親組織の戦略的範囲と個人的なネットワークによって大幅に拡張されます。

意思決定は、コラボレートして行われます。今日まで、すべての重要な意思決定は、中核となるリーダーシップ チームの全会一致で決定されています。

Linux Foundation の Michelle Martineau と Tracey Li による知見、知恵、そして継続的なサポートがなければ、Alpha-Omega は立ち止まってしまうでしょう。

また、以下の個人の方々の数多くのコントリビューションと継続的なサポートにも謝意を表したいと思います。 オープンソース セキュリティに対する彼らのサポートと情熱は揺るぎないものです。

Mila Zhou (AWS)
Chris “Crob” Robinson (OpenSSF)
Yesenia Yser (Microsoft)
David Nalley (AWS)
Eric Brewer (Google)
Mark Russinovich (Microsoft)

2024 年 年間レビュー

2024 年のゴール

人材派遣を通じて、すべての主要なオープンソース エコシステム向けの信頼性が高くセキュアなソフトウェア、ランタイム、インフラを促進

影響

Alpha-Omega は、PSF、RubyCentral、Eclipse Foundation、Rust Foundation、OpenJS Foundation（Node 経由）、Rust-for-Linux、Linux Kernel プロジェクトにセキュリティ要員を派遣しました。これは 2023 年からの拡大でした。また、RubyGems、PyPI、Python、Linux Kernel、LLVM、Apache Airflow、PHP Packagist などのプロジェクトのクリティカルな改善や監査にも資金を提供しました。これらの取り組みはすべて、プロジェクト コミュニティによるフォローアップ作業につながりました。

教訓

- 私たちは、セキュリティを確保することを誰かのジョブとし、そのジョブに適任者を配置することが、オープンソース エコシステムにおけるセキュリティの ROI（投資収益率）を最も大きく、かつ持続的なものにするという事実を、引き続き確認しています。
- 自社でセキュリティ要員を確保するまでの道のりは長いですが、私たちが資金援助した取り組みが、隣接するコミュニティや組織からどのようにして継続的な関わりを産み出しているかを見ていきます。

今後の展望

私たちは 2025 年もこれらのスタッフの人員配置を継続します。これらの業務は効果的で、レバレッジが効き、コラボレートし、組織内のセキュリティ文化とプライオリティを変えています。

上位 10,000 のオープンソース プロジェクトは、クリティカルなセキュリティ脆弱性がないようにする

影響

私たちは、最も一般的な脆弱性について、9,000 以上のプロジェクトをスキャンしました。70 件強の脆弱性とバグが報告されました。私たちは、ベスト プラクティスの採用を大規模に推進することを期待していましたが、それは実現しませんでした。比較的小規模なメンテナー層は、「さらに仕事が増える」ことを嫌がるだろうという明確なフィードバックを受けました。

教訓

- オープンソース プロジェクトは非常にセキュアです。問題のほとんどは、時代遅れの依存関係に起因しています。自動化は進歩していますが、これは依然として人間規模の問題であり、比較的小規模なプロジェクトの多くのメンテナーはすでに夜間や週末に作業を行っています。資金追加は即時の修正策にはなりません。
- 依存関係に大きさは関係ありません。依存関係は、それがどれほど大きくても小さくても、それを組み込んだプロジェクトのビルド時およびランタイムにリスクをもたらします。

今後の展望

これはアクティブに開発が進められている分野です。今後も引き続き実験を続けていきます。特に、ツールの改善に役立つ公開データセットや、小規模プロジェクトのメンテナーが AI ベースのソリューションを実用化する方法に注目しています。

意識的な革新と挑戦を通じて、Alpha-Omega のセキュリティ改善効果を拡張

影響

2024 年、私たちはいくつかの新しいプロジェクトと取り組みに資金を提供しました。

- Linux 版 Rust と、Rust への AV1 メディア コーデックの移植のサポートを継続
- いくつかの依存関係グラフに焦点を当てた監査とスキャンでは、プロジェクトの全体的なリスクについてそのコードやプロセスだけでなく、より広い範囲で調査を実施
- 初めて人気のオープンソース AI ライブラリとツールキットの監査を実施
- Jenkins プラグイン経由のクロスサイト スクリプティング攻撃を体系的に防止する Jenkins 用の CSP 実装プロジェクトを実施
- PyPI のプロジェクトの削除、プロジェクトのアップロード、プロジェクトの「ステータス」処理に関連する主要機能の実装と改善を含む PyPI のプロジェクトレベルの「ライフサイクル」機能の改善

教訓

- AI 分野は急速に進化しており、AI ライブラリを安全かつセキュアに利用するための確立されたフレームワークは十分に理解されていない
- セキュリティ関連の機能開発への小規模な投資は、これらのプロジェクトが成果を生むまでに時間がかかるとしても正常

今後の展望

- 小規模から中規模のプロジェクト開発作業や実験への資金提供を継続する予定

運用効率の高い効果的なプログラムの実行

影響

私たちの運営費は最低限に抑えられています。最小限のスタッフと出張費で、スポンサーからの寄付金の 91% 以上を助成金受給者に提供しています。これらのプロジェクトの選択、彼らが受けるサポート、そして私たちが創出するコミュニティの関与は、すべてこれらの助成金の成果にコントリビュートしています。

教訓

つまり、Alpha-Omega は上手く機能しています。

今後の展望

機能しているので、これまでどおりの方針を継続します。

Alpha-Omega

コミュニティの声

「Alpha-Omega は、オープンソース エコシステム全体のセキュリティを劇的に向上させていることは疑いようがありません。技術業界は、イノベーションとコスト効率の高い運用を実現するためにオープンソースに依存しています。 Alpha-Omega によるこれらの投資は、今後何年にもわたって利益を生み出すでしょう。」

– MIKE MILINKOVICH, EXECUTIVE DIRECTOR, ECLIPSE FOUNDATION

「Alpha-Omega は、利用可能な資金を使い、オープンソースのエコシステムとクリティカルなパッケージのセキュア化において、明確な実証可能な進歩を示しました。つまり、資金を明確に実証可能な方法でセキュリティに変えているのです。例えば、Apache AirFlow のセキュア化に向けた取り組みは、クリティカルなオープンソース コンポーネントのセキュリティ対策を大幅に改善しました。一般的なオープンソースへの資金提供は今後もコミュニティを巻き込んでいくでしょうが、AlphaOmega には Citi を含むすべてのオープンソース ユーザーに利点をもたらすセキュリティの針を動かす能力があることは明らかです。」

– JONATHAN MEADOWS, MANAGING DIRECTOR AND TECH FELLOW, CITI

「Alpha-Omega から資金提供を受けているカーネル セキュリティ エンジニアたちは、絶え間ない改善により、Linux を毎月よりセキュアなものにする素晴らしい仕事を行っています。」

– GREG KROAH-HARTMAN, LINUX KERNEL MAINTAINER

「セキュアなオープンソース プロジェクトの維持は、OpenJS Foundation の開発者たちにプレッシャーを与えています。Alpha-Omega が資金提供した IDC の調査では、7 億 5000 万以上の時代遅れのウェブサイトが存在し、その多くが機密情報を収集していることが明らかになりました。また、回答者の 33% が過去 24 か月間にセキュリティ インシデントに直面しています。90% のウェブサイトで使用されている jQuery は、ビジビリティの低さと脆弱性に苦しんでいました。Alpha-Omega は、モダナイゼーション、リスク調査、ウェブ アップグレード キャンペーンに資金を提供しました。同様に、Nodejs ユーザーの 3 分の 2 は、時代遅れのバージョンを使用しています。レガシー ソフトウェアとコントリビューターの限られたセキュリティ専門知識はリスクを増大させますが、Alpha-Omega は重要なサポートを提供しています。」

– ROBIN BENDER GINN, EXECUTIVE DIRECTOR, OPENJS FOUNDATION

「Alpha-Omega は、この取り組みに資金を提供しているだけでなく、アイデアの交換やブレインストーミングを行うプラットフォームも構築しており、これがプロジェクトにとって最も重要なインプットであることが証明されています。 私たちがすでに学んだことから、Airflow サミットや Community over Code で、オープンソース プロジェクトのメンテナーを巻き込み、彼らのサプライチェーンにも同様のアプローチを取るよう促すことができました。」

– JAREK POTIUK, APACHE AIRFLOW PMC AND SECURITY LEAD

「Alpha-Omega は、オープンソース セキュリティへの持続可能な投資が大きな影響をもたらすことを示す、業界全体にとっての強力な実例となっています。私たちは、エコシステムの強化に向けた私たちの取り組みに、より多くの民間および公共の関係者が力を合わせて参加することを期待しています。」

– MIRKO SWILLUS, HEAD OF SOVEREIGN TECH FUND

「Nodejs プロジェクトは、オープンソースのセキュリティにとって、直接的な技術支援が重要であることを示しています。健全なコミュニティ主導のプロジェクトであるにもかかわらず、Nodejs のメンテナーは、Nodejs に依存しながらほとんどコントリビュートしない企業からの要求に圧倒されています。多くのコミュニティ主導の JavaScript プロジェクトは、厳しいスケジュールでセキュリティ脆弱性に対処するための時間、専門知識、リソースが不足しています。 Alpha-Omega の助成金を通じて、セキュリティ対策を行う開発者を資金援助したことは、大きな成果をもたらしました。2021 年当時、Nodejs にはセキュリティ作業グループがありませんでしたが、現在では、ポリシー、自動化、コミュニティの成長を推進するエンジニアへの A-O の資金援助により、セキュリティ リリースが倍増し、離脱率が低下するなど、その体制は強化されています。」

– MATTEO COLLINA, NODE.JS TECHNICAL STEERING COMMITTEE MEMBER, OPENJS BOARD DIRECTOR, CO-FOUNDER & CTO PLATFORMATIC

「わずか数年で、私たちは Linux kernel のメモリ安全性という夢から、開発中の Rust ベース ドライバのポートフォリオ拡大へと進んできました。これは大きな進歩であり、私たちは活動の活性化とコミュニティの成長を目にしてきました。しかし、Linux kernel 自体が継続的な戦略的リーダーシップを必要としてきたように、Rust for Linux が最大のインパクトを達成するためには、アクティブなメンテナンスが必要です。Miguel Ojeda が担う役割は、コミュニティの育成から、重要な技術的コントリビューションの提供、プロジェクトを組織化し前進させるために必要な、地味な「雑用」まで、幅広い責任を伴うものです。この作業は現在クリティカルであり、しばらくの間は継続されるでしょう。」

– JOSH AAS, EXECUTIVE DIRECTOR AND CO-FOUNDER OF ISRG AND PROSSIMO

「Rust エコシステムにおける中核的なセキュリティ作業への資金援助の重要性は、いくら強調してもし過ぎることはありません。Rust のセキュリティ作業をサポートするための資金が確保される前は、3 人のパートタイム ボランティアは対応型のサポートに限定されていました。Alpha-Omega のおかげで、私たちはセキュリティ エンジニアとソフトウェア エンジニアのフルタイム雇用を実現することができました。彼らは協力して、脅威モデル、ツール、セキュリティ インフラに取り組んできました。これにより、Rust メンテナーのセキュリティ負担が大幅に軽減され、コントリビューターがセキュアかつ拡張性のある方法で参加しやすくなりました。経験豊富なセキュリティ エンジニアを専任で雇用することで、Rust Foundation は、先見性と積極性のあるセキュリティ対策への投資を継続し、この分野の新規参入者のオンボーディングとメンタリングを行い、より幅広いコミュニティのための持続可能性と安定性を備えたセキュリティ プロセスを開発することができます。」

– REBECCA RUMBUL, EXECUTIVE DIRECTOR AND CEO, RUST FOUNDATION

「Alpha-Omega チームはオープンソースのセキュリティをレベルアップさせており、FreeBSD Foundation は、この重要な作業にコントリビュートすることを誇りに思っています。FreeBSD 監査レポートで共有された洞察は、FreeBSD プロジェクト内のより強固なセキュリティの足掛かりとなるだけでなく、Alpha-Omega がオープンソース エコシステム全体に真の進歩をもたらしていることを浮き彫りにしています。」

– ED MASTE, FREEBSD FOUNDATION SENIOR DIRECTOR OF TECHNOLOGY

助成金

Alpha-Omega は 2024 年に、セキュリティの改善を推進する 15 の異なる組織に 20 件の助成金を提供しました。助成金の平均額は 227,445 ドルでした。Alpha-Omega が 2024 年に資金援助した活動は、総額 4,548,900 ドルの助成金によってサポートされました。従来、これらのデータ ポイントは、暦年で配布された資金を集計して算出されてきました。しかし、2024 年より、Alpha-Omega は助成金が利用された年を反映するように計算を調整することを決定しました。この調整により、Alpha-Omega の報告書は、セキュリティ改善イニシアチブに資金が利用された暦年をより正確に反映するようになります。

Alpha-Omega が創業以来交付した助成金の総額は、約 860 万ドルに上ります。

A

セキュリティ スタッフ

2024年助成金の
63%
$2,860,000

B

パッケージング リポジトリ

2024年助成金の
15%
$662,400

C

監査と改善

2024年助成金の
14%
$626,500

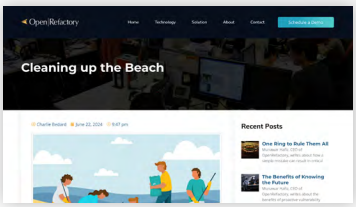
D

革新と挑戦

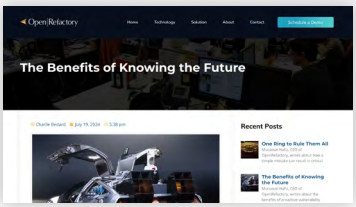
2024年助成金の
9%
$400,000

コンテンツ&アウトリーチ

Alpha-Omega と助成金受給者の多様なグループにより、さまざまなコンテンツが生み出されました。考えさせられるブログ投稿からインパクトのあるプレス リリース、教育的なオープンソース セキュリティ プレゼンテーションまで、当社の助成金は個人に力を与え、有意義なコントリビューションを実現してきました。以下の例は、制作された作品の一部を紹介しており、ポジティブな成果と多様なコンテンツを示しています。

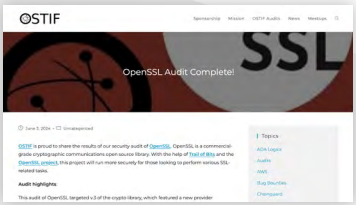


CLEANING UP THE BEACH



THE BENEFITS OF KNOWING THE FUTURE

AMAZON WEB SERVICES & ECLIPSE FOUNDATION SECURITY AUDIT IMPACT REPORT 2023

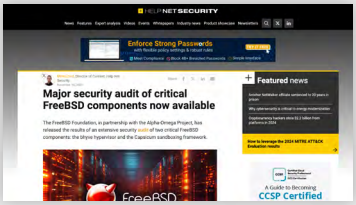


OPENSSL AUDIT COMPLETE!

LESSONS LEARNED FROM OPEN SOURCE SECURITY AUDITS: INSIGHTS FROM OCX 2024

STRENGTHENING FREEBSD: ADDRESSING VULNERABILITIES THROUGH SYNACKTIV'S CODE AUDIT

FREEBSD FOUNDATION RELEASES BHYVE AND CAPSICUM SECURITY AUDIT FUNDED BY ALPHA-OMEGA PROJECT



MAJOR SECURITY AUDIT OF CRITICAL FREEBSD COMPONENTS NOW AVAILABLE

2025 年以降

Alpha-Omega も 3 年目に入り、私たちは自分たちにとって何がうまくいき、何を改善できるかについて多くを学びました。来年の私たちのゴールをいくつかご紹介します。

Alpha Omega OKRs 2025

私たちの目標はほとんど変わっていません。私たちの会議の 1 つで、私たちは、助成金受給者とともに、私たちが作り出している影響について、もっとマーケティングを行うことができるという意見で一致しました。これは話題作りが目的なのではなく、Alpha-Omega の実現を可能にする資金調達を持続可能にし、拡大しやすくするためです。

O1：スタッフの配置を通じて、すべての主要なオープンソース エコシステム向けの信頼性が高くセキュアなソフトウェア、ランタイム、インフラの促進

KR 1.1	2025 年末までに少なくとも 10 のクリティカルなオープンソース組織のセキュリティ改善とイニシアチブを実施。
KR 1.2	各取り組みについて初期およびその後の評価、月次報告、定期的な確認を通じて、セキュリティ向上の成果を確認。
KR 1.3	Alpha-Omega 以外の少なくとも 1 つの組織からセキュリティ資金を得るよう、私たちが連携する組織を動かし、2025 年末までに 33% をターゲットに設定。
KR 1.4	少なくとも 5 つの主要なエコシステムを対象に、情報を共有を行い、つながりを構築し、コラボレートするための四半期ごとの会議を組織し、その結果、2025 年までに少なくとも 1 つの新しいプロジェクトもしくは共同制作を開始。
KR 1.5	採用、利用、OSS セキュリティ プロジェクトの価値を拡大し、持続可能性の転換点への到達。

O2：クリティカルなセキュリティ脆弱性のないオープンソース プロジェクトの上位 10,000 件

KR 2.1	オープンソース プロジェクト用のセキュリティ関連データのオープン データセットを作成し、収集することで、スケーラブルなセキュリティ ツールの開発を容易にし、結果の一貫性を高める。
KR 2.2	「ビーチクリーン」のアプローチを少なくとも 3 つの新規プロジェクトに拡大し、どのプロジェクトでもより簡単かつ安価に実施できるよう、ツールとプレイブックを開発。
KR 2.3	危機的な状況において、コミュニティ内およびコミュニティ間で協力し、小規模なプロジェクトにセキュリティに関するガイダンスを提供できるセキュリティ専門エンジニアのグループ「エンジニア部隊」をオープンソースで作成。

O3：「革新と挑戦」とマーケティングにおける Alpha-Omega の有効性を拡張

KR 3.1	2025 年末までに、オープンソース エコシステム内のセキュリティ リスクを低減するための新しい戦略を模索する 3 つの実験を実施し、その結果 / 学習内容を共有し、2025 年の全体的な戦略と目標を洗練するためにそれらを活用。
KR 3.2	特定のチームを対象とした関係者に対する、インフォグラフィックやマーケティング資産を活用したよりアクティブな社内マーケティングを実施。
KR 3.3	オープンソースのトップ A I ライブラリのセキュリティを監査し、改善するために、2024 年から引き続き進歩を続け、それらをセキュアに利用する組織向けのガイダンスを開発することで実現。

O4：運用効率が高く、成長性があり、効果的なプログラムを実施

KR 4.1	年間支出の少なくとも 85% を、ミッションを直接サポートする活動に割り当てる。
KR 4.2	2025 年に少なくとも 500 万ドルの追加資金を受領。
KR 4.3	各パートナー契約において、定義された期間内に、それぞれの契約で定義された目標の少なくとも 70% を達成。
KR 4.4	四半期ごとの報告書を作成し、提供。 関係者、助成金受給者、その他の対象組織における関与 / 関心を向上。
KR 4.5	他の組織（例：Sovereign Tech Agency）と提携し、3 ～ 5 件の取り組みに共同出資。

参加する

Alpha-Omega チームは、コミュニティのアクティブな参加を歓迎しています。月に一度、公開ミーティングを開催し、パブリックな Slack チャンネルを提供しています。また、GitHub リポジトリで、契約パートナーから詳細なアップデートを収集しています。さらに、OpenSSF 技術諮問委員会（TAC）に定期的にアップデートを提供し、OpenSSF の作業グループやプロジェクトと緊密な関係を維持しています。

また、私たちのビジョンを共有し、私たちのミッション達成に貢献してくださる人々や組織とのコラボレーションにも関心があります。具体的には、以下の主要分野に関心があります。

- **資金調達：**Alpha-Omega プロジェクトに資金提供できる組織を代表されている場合は、ご連絡ください。
- **セキュリティ ツール：**オープンソース プロジェクトの最先端のセキュリティ分析を実施できるセキュリティ ツールまたはベンダーを代表されている場合は、ご連絡ください。
- **クリティカル プロジェクト：**クリティカルなオープンソース プロジェクトを代表されている場合、または実行可能なセキュリティ関連プロジェクトをお持ちの場合は、ご連絡ください。
- **エコシステム、パッケージ マネージャー、インフラ：**オープンソース開発者のための開発者エコシステム、パッケージ マネージャー、共有インフラを代表し、セキュリティ改善のための即戦力となるアイデアをお持ちの方は、ぜひご連絡ください。
- **LinkedIn で参加しましょう：**https://linkedin.com/showcase/alpha-omega-oss

本訳文について

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

翻訳協力：富田明男・富田佑実