OPENCHAIN

OpenChain Security Assurance Reference Guide

OpenChain セキュリティアシュアランスリファレンスガイド

Version 1.0

（日本語仮訳　β-0.5.0 版）

Establishing trust in the Open Source from which Software Solutions are built

オープンソースソフトウェアで構成されたソフトウェアソリューションの信頼性の確立

目次

序文

OpenChain Specification WG の中心となるミッションは、現代のソフトウェアによるソリューションを構築するオープンソースに対する信頼を確立するための、”プログラム”標準を開発することです。OpenChain プロジェクトの最重要仕様である、オープンソース・コンプライアンスに関する ISO/IEC 5230 国際標準は、オープンソース・ライセンスに関連する信頼を確立することに焦点を当てています。より幅広いミッションを達成するための自明な次のステップは、セキュリティアシュアランスに関するプログラムが当然満たすべき、オープンソースソフトウェアの使用に関する、最小限の中核要件を特定することでした。当初は、最小限の中核要件の範囲は、一般に公開されている既知のセキュリティ脆弱性問題（CVE や GitHub/GitLab の脆弱性警告、パッケージマネージャの警告等）に関して、組織がオープンソースを審査することに限定しています。 このガイドの範囲は、コミュニティからのフィードバックに基づいて、時間とともに拡大し得るものです。

このリファレンスガイドに適合することで、使用するオープンソースに関して、信頼できるレベルのセキュリティアシュアランスを確立するために必要な、期待される手順を実行するプログラムを、対象の組織が実施していることを保証することができます。この文書では、プログラムに関する”how”や”when”よりも、”what”や”why”の側面に焦点を当てています。これにより、様々な業界の様々な規模の組織が、その規模や目標、プログラムの範囲に合わせて、特定のポリシーやプロセスの内容を選択できる柔軟性を確保しています。例えば、ガイドに適合したプログラムは、単一の製品ラインを対象とする場合もあれば、組織全体を対象とする場合もあります。

この文書の構成は以下の通りです：「序文」では、本ガイドの目的を説明します。第2章では、本書で使用する主要な用語を定義しています。第3章では、プログラムがコアレベルのセキュリティアシュアランスを達成するために満たさなければならない要求事項を定義しています。各要件は、その要件を満たすために作成しなければならない、1つ以上の検証資料（たとえば記録）により構成されています。検証資料が公開されている必要は無く、組織が検証資料を他者に提供する場合でも、秘密保持契約（NDA）に基づいたものとなるでしょう。

OpenChain セキュリティアシュアランスリファレンスガイド

1 適用範囲

この文書は、オープンソースソフトウェアで構成されたソフトウェアソリューションを供給する組織の信頼を確立するための、高品質なオープンソースセキュリティアシュアランスプログラムの主要な要件を規定する。

2 用語と定義

本文書では、以下の用語および定義を適用する。

2.1 CVE
CVE(Common Vulnerabilities and Exposures)は、公開されているソフトウェアのセキュリティ上の問題や欠陥を集めた公開データベースである。CVE と言えば、データベース内で CVE ID 番号が割り当てられた特定のセキュリティ脆弱性を意味する。CVE データベースは、DHS(Department of Homeland Security:米国国土安全保障省)と CISA(Cybersecurity and Infrastructure Security Agency)によって運営されている。

2.2 既知の脆弱性
一般に公開されているオープンソースコンポーネントに発見されたセキュリティ脆弱性。公開されている脆弱性には、CVE、GitHub/GitLab の脆弱性警告、パッケージマネージャの警告などが含まれる。

2.3 オープンソース
Open Source Initiative が発行する Open Source Definition(詳細は opensource.org/osd を参照)または Free Software Foundation が発行する Free Software Definition(詳細は gnu.org/philosophy/free-sw.html を参照)などのライセンスを満たす、1 つ以上のライセンスの対象となるソフトウェア。

2.4 プログラム
組織のセキュリティアシュアランス活動を構成する一連のポリシー、プロセス、およびメンバー。

2.5 プログラム関係者
供給ソフトウェアを定義、提供、または準備する責任を持つ組織の従業員または請負業者。

注:組織によって、ソフトウェア開発者、リリースエンジニア、品質エンジニア、製品マーケティングおよび製品管理などが含まれる。

2.6 セキュリティのアシュアランス
システムがセキュリティのベストプラクティスの要件を満たし、既知の脆弱性への耐性を備えているという信頼性。

2.7 SPDX
Linux Foundation の SPDX (Software Package Data Exchange) ワーキンググループが策定した、ライセンス、著作権情報、既知の脆弱性など、特定のソフトウェアパッケージの部品表情報を供給するためのフォーマット標準 (詳細は spdx.org を参照)。

2.8 供給ソフトウェア

組織が第三者(他の組織や個人など)に対して配布、または利用可能な状態とするソフトウェア。

2.9 検証資料
リファレンスガイドの既定の要件が満たされていることを示す資料。

3 要求事項

3.1 プログラムの基盤

3.1.1 ポリシー

供給ソフトウェアに対するオープンソースセキュリティのアシュアランスを管理する文書化されたポリシーが存在していること。ポリシーが組織の内部で周知されること。

検証資料:

- 3.1.1.1 文書化されたオープンソースセキュリティのアシュアランスポリシー。
- 3.1.1.2 プログラム参加者にオープンソースセキュリティのアシュアランスポリシーの存在を(例えば、トレーニング、社内 wiki、またはその他の実践的なコミュニケーション手法を通じて)認識させる文書化された手順。

理由:

オープンソースポリシーを作成、記録、またプログラム参加者にオープンソースポリシーの存在を認識させるための手順が取られていることを確実にするため。ポリシーにどんな内容を含めるべきかの要求事項がここに提示されていないが、他のセクションで要求事項が課せられる場合がある。

3.1.2 力量

組織は以下を行うこと。

- 当該プログラムの遂行とその効果に影響を及ぼす役割、および、その役割に対応した責任の特定;
- 各役割を果たすプログラム参加者の必要な力量の決定
- プログラム参加者が適切な教育、トレーニング、および/または経験に基づいて十分な力量を 持っていることの確認;
- 状況に応じて、必要な力量を獲得するための措置を実施
- 文書化された記録を力量のエビデンスとして保持

検証資料:

- 3.1.2.1 プログラム参加者の役割とその責任の文書化されたリスト。
- 3.1.2.2 各役割の力量を特定する文書。
- 3.1.2.3 各プログラム参加者の力量の評価を文書化した証拠。

理由:

プログラム参加者がプログラムにおけるそれぞれの役割と責任を果たす十分なレベルの力量を有していることを確認するため。

3.1.3 認識

組織はこのプログラム参加者が以下を認識していることを確認すること:

- オープンソースセキュリティアシュアランスポリシー;
- 関連するプログラムの目標;
- プログラムの有効性に対する参加者の貢献;
- プログラムの要求事項を遵守しないことの意味

検証資料:

- 3.1.3.1 プログラムの目的、プログラムにおける参加者の貢献、プログラムの不適合の影響を含む、プログラム参加者の認識を評価した証拠の文書。

理由:

プログラム参加者がプログラムにおけるそれぞれの役割と責任を果たす十分なレベルの認識度を有していることを確認するため。

3.1.4 プログラムの適用範囲

さまざまなプログラムは異なったレベルの適用範囲で管理することができる。例えば、単一の製品ライン、部署全体、あるいは、組織全体をプログラムが管理することが可能である。それぞれのプログラムに対する適用範囲の指定が明記されること。

検証資料:

- 3.1.4.1 プログラムの適用範囲と境界を明確に定義する文書。

理由:

組織のニーズの範囲に最も適したプログラムを構築するための柔軟性を提供するため。特定の製品ラインのためのプログラムを維持することを選択する組織もあれば、組織全体で提供されるソフトウェアを管理するためのプログラムを実施する組織もある。

3.1.5 標準的な実践の実装

- 既知の脆弱性に関する組織の知識が存在する
- 供給ソフトウェア内の既知の脆弱性の存在を検出する方法
- 特定された既知の脆弱性を継続的に追跡する方法
- 保証されている場合、特定された既知の脆弱性を顧客層に伝える方法
- リリース後に新しく公開された既知の脆弱性について供給ソフトウェアを解析する方法

上に列挙されたセキュリティアシュアランスの方法のためのプロセスが存在していること。

検証資料:

- 3.1.5.1 上記の方法それぞれの手順が文書化されていること。

理由:

供給ソフトウェアの既知の脆弱性を検出し継続的に追跡する適切なプロセスが存在することを確実にするため。

3.2 関連タスクと定義のサポート

3.2.1 アクセス

組織外からの既知の脆弱性に関する問合せに適切に対応するためのプロセスを維持すること。第三者が特定のソフトウェアに関する既知の脆弱性についての問合せを行う方法が公に示されていること。

検証資料:

- 3.2.1.1 第三者が既知の脆弱性に関する問合せを行うための公に示された方法（例えば公開された電子メールアドレス（security@company.com や opensource@company.com など）を通じて）。
- 3.2.1.2 既知の脆弱性関する第三者からの問合せに対応するための内部手続き文書。

理由:

セキュリティ脆弱性に関する問合せについて、第三者がその組織にコンタクトできる合理的な手段があり、またその組織が当該問合せに対して適切に対応するように準備がされていること。

3.2.2 効果的なリソース

プログラム関連業務を定義し、リソースを提供する:

- プログラム関連業務を確実に実行するための責任者をアサインする
- プログラム関連業務に十分なリソースが提供されていること:
  - 業務を遂行するための時間が割り当てられている
  - 適切な予算が割り当てられている
- ポリシーおよびサポート業務に対するレビューおよび更新するプロセスがあること
- 必要とする人が、既知の脆弱性に関する技術的な専門知識を利用できること

検証資料:

- 3.2.2.1 プログラム関連の役割を担当する個人、グループまたは職務の名前が記載された文書
- 3.2.2.2 プログラム関連の役割に対して人員が適切に配置され、適切な予算が割り当てられていること
- 3.2.2.3 特定された既知の脆弱性に対応するための専門知識が提供されていること
- 3.2.2.4 セキュリティアシュアランスの内部責任者をアサインするための手続き文書

- 3.2.2.5 既知の脆弱性に関する特定のケースについて、レビューと救済策を実施するための手続き文書

理由:

i) プログラム責任者が効果的にサポートされリソースが提供されていること、ii) セキュリティアシュアランスのベストプラクティスにおける変化に追従するため、ポリシーおよびサポート業務が定期的に更新されていること。

3.3 オープンソースコンテンツのレビューと承認

3.3.1 部品表(Bill of Materials)

供給されるソフトウェアを構成するオープンソースコンポーネントを含む部品表の作成、管理を行うプロセスが存在するものとする。

検証資料:

- 3.3.1.1 供給されるソフトウェアを構成するオープンソースコンポーネントの特定、追跡、レビュー、承認及び情報保管のための手順書
- 3.3.1.2 手順書が適切に遵守されていることを示す、供給されたソフトウェアを構成するオープンソースコンポーネントの記録

理由:

供給されるソフトウェアを構築するために使用されたオープンソースコンポーネントの部品表を作成、管理するためのプロセスが存在することを確実にするため。部品表は、既知の脆弱性が存在するかどうかを把握するための各コンポーネントの体系的なレビューをサポートするため。

3.3.2 セキュリティーアシュアランス

- レビュー対象の供給されるソフトウェア・リリースの部品表に含まれる各オープンソース・コンポーネントについて
  - 既知の脆弱性の存在を検出する方法の適用
  - 特定された「既知の脆弱性」ごとに、リスク／インパクトのスコアを付与する。
  - リスク/インパクトのスコアに応じて、適切なアクションを取る(例:必要に応じてお客様に連絡、コンポーネントのアップグレード、対応必要なし、など)
  - 過去に配布された供給ソフトウェアに既知の脆弱性が存在する場合、リスクと影響のスコアに応じて適切な措置を講じる(例:必要に応じて顧客に連絡する)
- ソフトウェアソリューションのリリース後、供給されたソフトウェアソリューションに影響を与える可能性のある既知の脆弱性が新たに報告された場合、それを特定し、それに応じて対応を行う

検証資料:

- 3.3.2.1 供給されるソフトウェアのオープンソースコンポーネントに関する既知の脆弱性の検出および解決を処理するための文書化された手順。

- 3.3.2.2 各オープンソース・コンポーネントについて、特定された既知の脆弱性と対策(対策が必要なかった場合も含む)の記録が維持される。

理由:

供給されるソフトウェアが構成されているオープンソースについて、特定された既知の脆弱性を処理するために、プログラムが十分に堅牢であることを確認すること。この活動を支援するための手順が存在し、その手順が遵守されていることを確実にするため。

3.4 ガイドライン要求事項の遵守

3.4.1 完全性

プログラムがこのリファレンスガイドに適合しているとみなされるために、組織は、当該プログラムがこの文書に示された要求事項を満たしていることを確認するものとする。

検証資料:

- 3.4.1.1 § 3.1.4 で規定されたプログラムが本文書のすべての要求事項を満たしていることを確認する文書。

理由:

組織が準拠[1] したプログラムがあると宣言した場合、そのプログラムが本文書のすべての要求事項を満たしていることを確実にするため。それら要求事項のサブセットを満たしているだけでは不十分である。

3.4.2 期間

本版のリファレンスガイドに適合したプログラムは、適合認証の取得日[2]から 18 ヶ月間有効であるものとする。

検証資料:

- 3.4.2.1 プログラムが、適合認証の取得から過去 18 ヶ月以内で、本ガイドのすべての要求事項を満たしていることを確認する文書。

[1] 訳注:「本版のリファレンスガイドに」準拠の意

[2] 訳注:セキュリティアシュアランスリファレンスガイドについてその適合取得を登録する手段は特にない。なお、リファレンスガイドはセキュリティアシュアランスに焦点をあてており、OpenChain 仕様とは関連性があるとはいえ、独立して運用できる。そのため、OpenChain とリファレンスガイドの双方に適合する場合、その期間は個別に管理される。実務的には、OpenChain 仕様適合しているプログラムが新たにセキュリティアシュアランスリファレンスガイドに適合する場合、OpenChain 仕様適合の更新を同時に行ってもよいし、または、リファレンスガイドの認証を一旦は実施し、その後、次回の OpenChain 仕様適合の認証に合わせてこのリファレンスガイドへの適合の認証を更新することで、適合の期間を同じとする運用などが考えられる。

Rationale/ 理由:

組織が長期的に適合性を主張したい場合、プログラムが最新のリファレンスガイドに準拠した状態を保つことが重要である。本要求事項は組織が継続してプログラム適合性を主張する場合に、プログラムの支援プロセスや制御が損なわれることを防ぐ。

Translated by OpenChain Japan Work Group Promotion Sub Group

Atsutaka Kida, Ayumi Watanabe, Hiroyuki Fukuchi, Masato Endo, Satoru Koizumi,

Tadayuki Osaki, Takashi Ninjouji, Tomo Dote, Yasushi Osonoi, Yuhei Uno