

サプライチェーンセキュリティに関する不正機能検証

概要

ソフトウェアサプライチェーンにおける脆弱性対策として、機能レベルの細粒度でソフトウェア構成情報を自動抽出し、解析する技術を開発しました。既存手法の課題である「ライブラリ単位の粗い粒度」を克服し、本当にセキュリティ対策が必要な箇所を特定できるようにします。これにより、深刻な脆弱性に対して、効率的かつ的確な対策を可能にします。

特徴

- セキュリティ脅威と脆弱性情報: サイバー攻撃などのセキュリティ脅威に対し、ソフトウェアの弱点である脆弱性の正確な情報が重要です。OSVといったオープンな脆弱性情報により、効率的な対策が可能です。
- 機能レベルの精密な脆弱性特定と既存フレームワークとの統合: アプリ・ライブラリ単位ではなく機能レベルで脆弱性を特定し、不要なコストを削減します。この細粒度情報をGUACフレームワークへ統合し、サプライチェーンの詳細な可視化と解析を実現します。
- 視認性に優れた可視化機能: 脆弱性のある機能との依存関係の表示を簡素化することで、複雑な構成でも直感的に理解できるようにします。これにより、セキュリティ担当者や開発者の負担を軽減し迅速な状況把握を支援します。

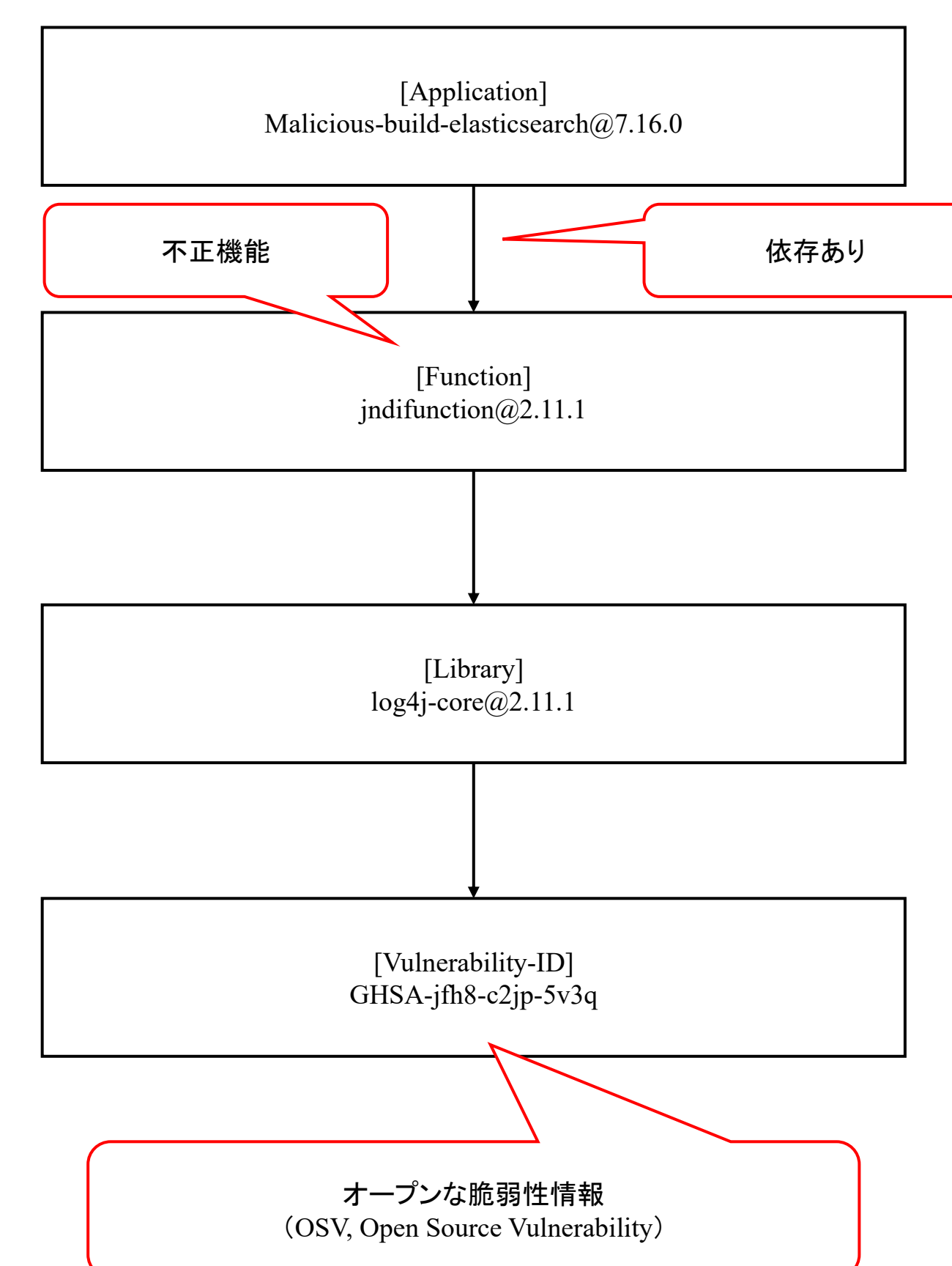
今後の展開

- 他の脆弱性やアプリケーションへの適用を進め、機能レベルの脆弱性管理技術の汎用性を高めていきます。また、自動化技術をさらに発展させることで、より効率的なソフトウェアサプライチェーンセキュリティの実現を目指します。

テーマ「社会課題と向き合う科学技術の最前線」との関連

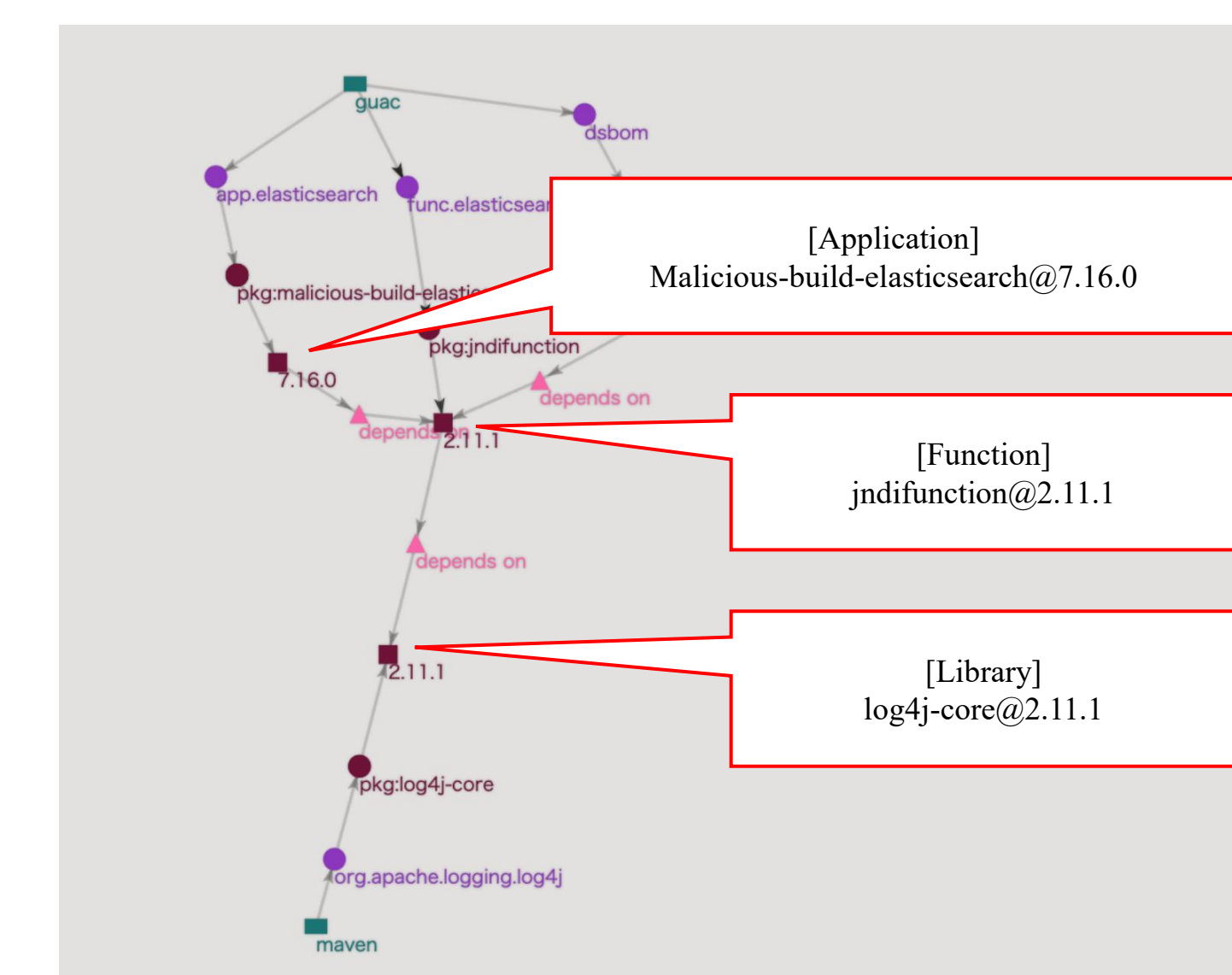
- 本研究開発は、深刻なサイバーセキュリティリスクから社会インフラや経済活動を守るためのものです。ソフトウェアの安全性を高めることで、デジタル社会の信頼性と持続可能性に貢献する最前線の研究開発に、今後も全力で取り組んで参ります。

依存関係の概要

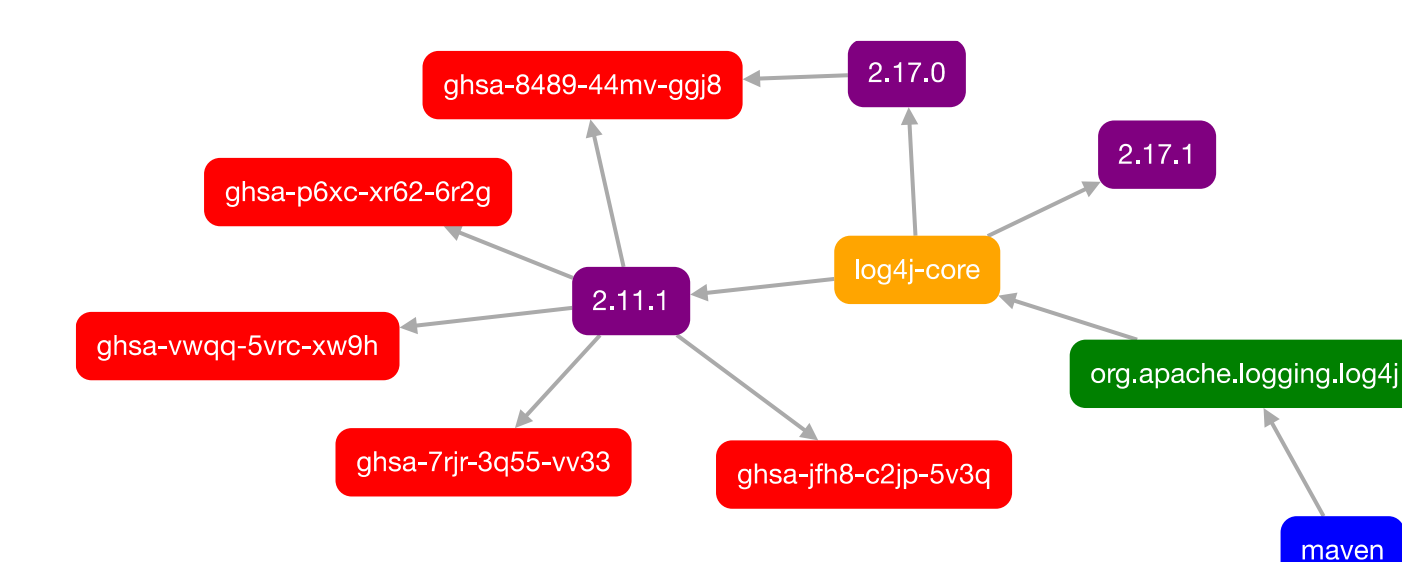


GUAC による依存関係可視化

※GUAC (Graph for Understanding Artifact Composition) : Google が開発したソフトウェアサプライチェーンの深い理解と洞察を提供するオープンソースプロジェクト



可視化機能の視認性向上



株式会社国際電気通信基礎技術研究所
適応コミュニケーション研究所

担当 小津喬 E-Mail: ozu@atr.jp