



OPENCHAIN

+

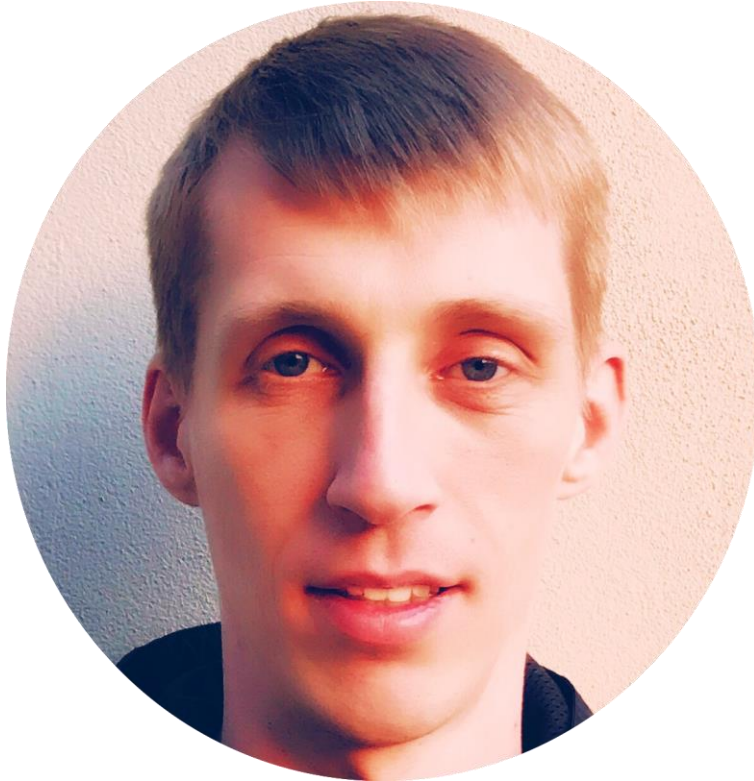





OSS  
Review Toolkit

the why, what and how



# About me



 thomas.steenbergen@here.com  
 @tsteenbe  
 linkedin.com/in/tsteenbe

## Head of Open Source at HERE Technologies HERE TechnologiesのOpen Source責任者

A location data and technology platform company  
位置データとテクノロジープラットフォームの企業

Active contributor 以下のプロジェクトへの貢献活動中



OSS  
Review Toolkit

<http://oss-review-toolkit.org>



SPDX



Open Source  
Tooling Group

 OPENCHAIN



TODO

European Chapter



ClearlyDefined



Work In Progress  
開発途上

OSS Review Toolkit  
is pre-release software

**OSS Review Toolkitは、リリース前版の状態**

First release planned for Q1 of 2020  
**2020年の第1四半期に初版をリリース予定**



The OpenChain Project helps to identify and share the core components of a Free and Open Source Software (Open Source) compliance program.

**OpenChainプロジェクトでは、オープンソースのコンプライアンスプログラムに関する、中心となる要素を特定し共有することを進めている**

A key element to a Open Source Compliance Program is a *Open Source Review* process

**オープンソースのコンプライアンスプログラムに関する、キーとなる要素は、オープンソースをレビューするプロセス**

<https://www.openchainproject.org>

# Why: Open Source Compliance Program

## オープンソースのコンプライアンスプログラムを推進する理由



- **Know your obligations.** You should have a process for identifying and tracking Open Source components that are present in your software
- **遵守事項を知る：**ソフトウェアで使用されているオープンソースのコンポーネントを特定し、追跡するプロセスを持つ必要がある
- **Satisfy license obligations.** Your process should be capable of handling Open Source license obligations that arise from your organization's business practices
- **遵守事項を満たす：**組織におけるビジネス慣行より生じる遵守事項であって、オープンソースにおけるライセンスで規定された遵守事項に、プロセスが対応できる必要がある

Benefits of a robust Open Source Compliance program include:

- Increased understanding of the benefits of Open Source and how it impacts your organization
- Increased understanding of the costs and risks associated with using Open Source
- Increased knowledge of available Open Source solutions
- Reduction and management of infringement risk, increased respect of Open Source developers/owners' licensing choices
- Fostering relationships with the Open Source community and Open Source organizations

# What information do you need to gather?

## どのような情報を収集する必要があるか？



When analyzing Open Source usage, collect information about the identity of the Open Source component, its origin, and how the Open Source component will be used. This may include:

使用するオープンソースを解析する場合、オープンソースが何であるか、どこから入手したか、および、どのようにコンポーネントが利用されるかの情報を収集する必要がある。詳細としては以下の情報：

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>● Package name</li><li>● Status of the community around the package (activity, diverse membership, responsiveness)</li><li>● Version</li><li>● Download or source code URL</li><li>● Copyright owner</li><li>● License and License URL</li><li>● Attribution and other notices and URLs</li><li>● Description of modifications intended to be made</li></ul> | <ul style="list-style-type: none"><li>● List of dependencies</li><li>● Intended use in your product</li><li>● First product release that will include the package</li><li>● Location where the source code will be maintained</li><li>● Possible previous approvals in another context</li><li>● If from an external vendor:<ul style="list-style-type: none"><li>● Development team's point of contact</li><li>● Copyright notices, attribution, source code for vendor modifications if needed to satisfy license obligations</li></ul></li></ul> |
|--|---|

# How: Source Code Scanning Tools

どのように、ソースコードスキャンツールを使うか。



- There are many different automated source code scanning tools.
- 自動のソースコードスキャンツールは複数存在
- All of the solutions address specific needs and - for that reason - none will solve all possible challenges
- それぞれのツールによるソリューションは皆、特定のニーズを満たすものであり、したがって、可能性のある要求事項をすべて満たすツールは無い
- **Companies pick the solution most suited to their specific market area and product**
- それぞれの企業は、自らの市場と製品に最も適したソリューションを選択する
- Many companies use both an automated tool and manual review
- 多くの企業は、自動化されたツールと人手でのレビューを共有している

No solution satisfied our needs so in 2017 we created a new tool...

どのツールもHERE Technologyのニーズを満たせず：2017年に新たなツールを作成



# OSS Review Toolkit

そのツールが  
OSS Review Toolkit

but challenges are too big for single company so...

OSS Review Toolkitが目指すところは、HERE Technologies 1社で開発するにはあまりに壮大、なので

## We work together on

open source standards and tools ecosystem

われわれは、OSSコンプライアンスの標準と、複数のツールそれぞれのエコシステムと協働することにした

 OPENCHAIN



SPDX



Open Source  
Tooling Group



TODO

European Chapter



# Tooling Types

## ツールのタイプ



Main types of tools in the area of license compliance include  
(but are not limited to):

### ライセンス コンプライアンス分野における主なツールの例

- License scanning **ライセンス スキャンツール**

Identifies licenses and license relevant statements, can also copyright statements, author statements, acknowledgements

- Binary scanning **バイナリファイル スキャンツール**

Identifies used software packages in software binaries, can also determine the versions of software packages

- Source code scanning **ソースコード スキャンツール**

Can identify published origin of source code and other files

- Dev Ops integration **Dev Ops 統合形式のツール**

Uses the information from building the software to determine OSS used

- Component management **コンポーネント管理ツール**

Collect information about used software components and their use in products or projects is centrally collected and can be reused



# OSS Review Toolkit

## OSS Review Toolkitの特徴

### Features:

- License scanning **ライセンスの検出(scan)**

Identifies copyrights and licenses by wrapping existing license / copyright scanners like ScanCode to detect findings in local source code directories.

- Best practices / company standards scanning

Align software projects across the organization. **標準的な手法/社内標準に従っているかの検出**

- Policy violations rule engine

Perform highly customizable policy checks against scan results **設定したポリシーへの違反検出**

- Software Bill of Materials / Notices

Generate CycloneDX, SPDX 2.2 files or plain text open source notices **ソフト部品表(SBOM) および共有形式 (SPDX)の生成**

- Dev Ops integration

Designed from the beginning for a CI/CD world **Dev Opsプロセスに統合された形での動作**

- Security scanning (planned) **(計画中) 脆弱性スキャン**

Coming soon: integrations with OSS security vulnerabilities data feeds from various vendors.

- Source code scanning (planned) **(計画中) ソースコードの出所特定**

Working on partnerships with vendors to develop integrations to identify published origin of source code and other files

### Collected Information

- Package name
- Version
- Source code repository URL
- Source and binary artifacts
- Copyright owner
- License and License URL
- Attribution and other notices and URLs
- List / tree of dependencies
- Location where the source code will be maintained



OSS

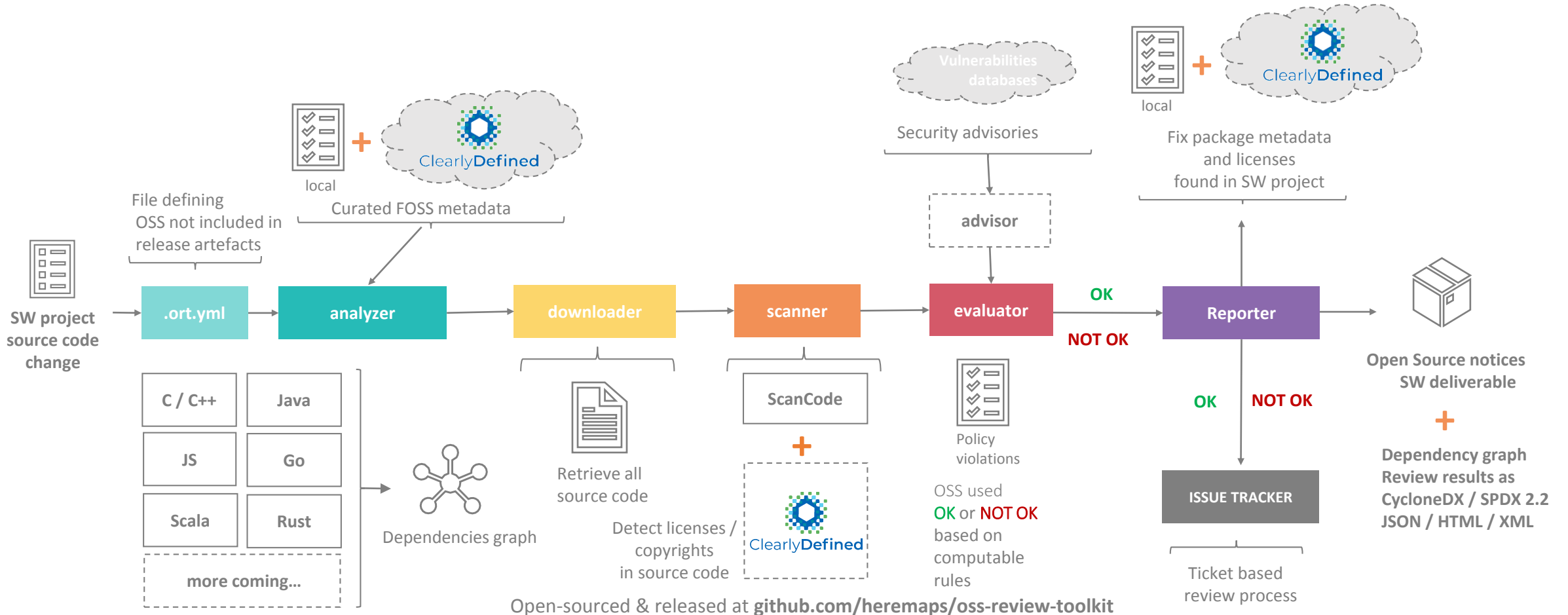
# Review Toolkit: scaling OSS reviews in CI/CD (Q4 2019)

## CI/CDプロセスに合わせた形でOSSのレビューを実現

Goal: enable review **during source creation** by providing **easy, open-source & scalable tooling** for **developers** to do **basic compliance** and share results in **open standard formats**

### 目指すゴール:

開発者に、簡易に操作でき/オープンソースであり/プロセスに合わせて拡張可能なツールを提供することで基本的なコンプライアンスを遵守させ、ソースコード生成の段階でのレビューを可能とし、かつ、その結果を、オープンかつ標準的なフォーマットで共有すること





# OSS **Review Toolkit**

**Demo**





Open Source  
Tooling Group



SPDX



OPENCHAIN

ClearlyDefined

Vulnas

Fossology

Quartermaster

OSS Review Toolkit

SW360



Open Source Tooling for Open Source Compliance



OSS



OSS



OSS



OSS



OSS



OSS  
**Review Toolkit**

+




HERE Technologies has contributed ORT to the Automated Compliance Tooling (ACT)

**HERE TechnologiesはOSS Review Toolkitを、Linux Foundation配下のAutomated Compliance Tooling (ACT)プロジェクトに寄贈しました**

# Thank you

ありがとうございました

Thomas Steenbergen  
HERE Open Source Office

 thomas.steenbergen@here.com

 @tsteenbe

 linkedin.com/in/tsteenbe

OSS Review Toolkit

<https://github.com/heremaps/oss-review-toolkit>

Related OSS Projects

<https://oss-compliance-tooling.org>

<https://clearlydefined.io>

<https://spdx.org>

<https://www.openchainproject.org>

<https://www.doubleopen.org>