OPEN SQUARE

WhiteSource

シフトレフトで実現する効率的なセキュリティ対策

オープンソース利用によるソフト開発のリスクを、簡単に回避する方法

～ セキュリティ脆弱性、ライセンス違反、バグ… リスクは一気につぶす！～

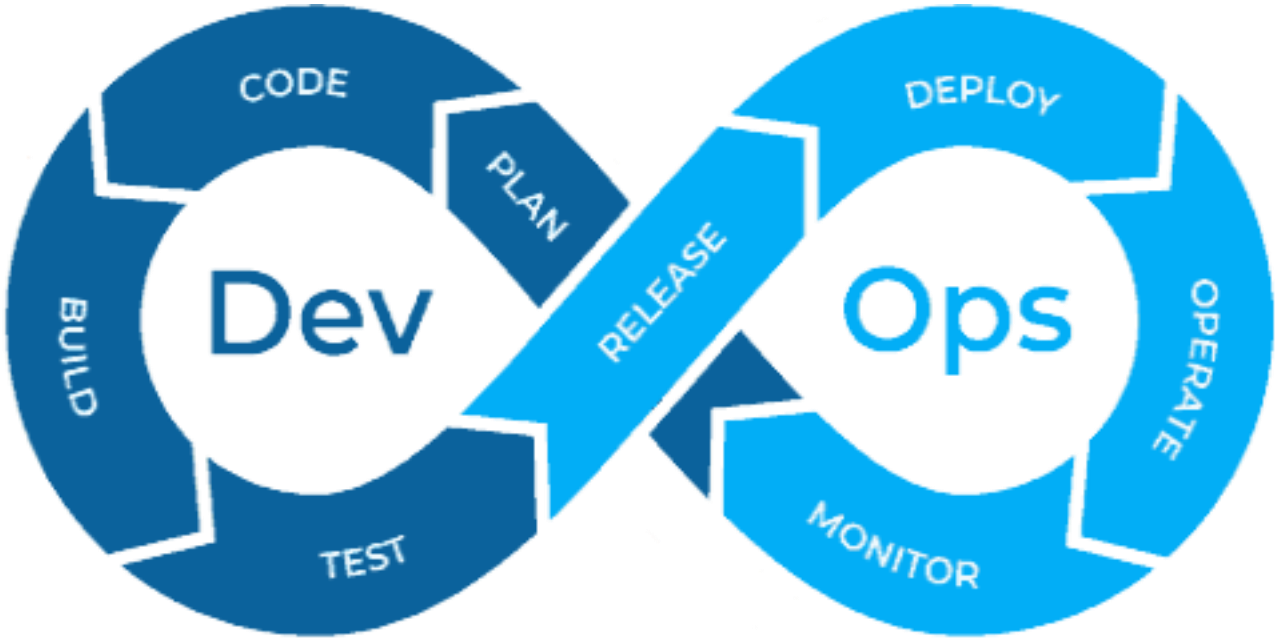
株式会社OPENスクエア
田中　昭造

アプリケーションのリリース頻度

- 数回/1日 2%
- 1回/1日(平均) 2%
- 1回/1週(平均) 8%
- 1回/1ヵ月(平均) 21%
- 1回/四半期(平均) 26%
- 2回/1年(平均) 16%
- 1回以下/1年間 11%
- OS,ミドルウェアと同期(新バージョン対応) 10%
- その他 6%

(四捨五入により合計が100%以上になっている)
＊対象：635人

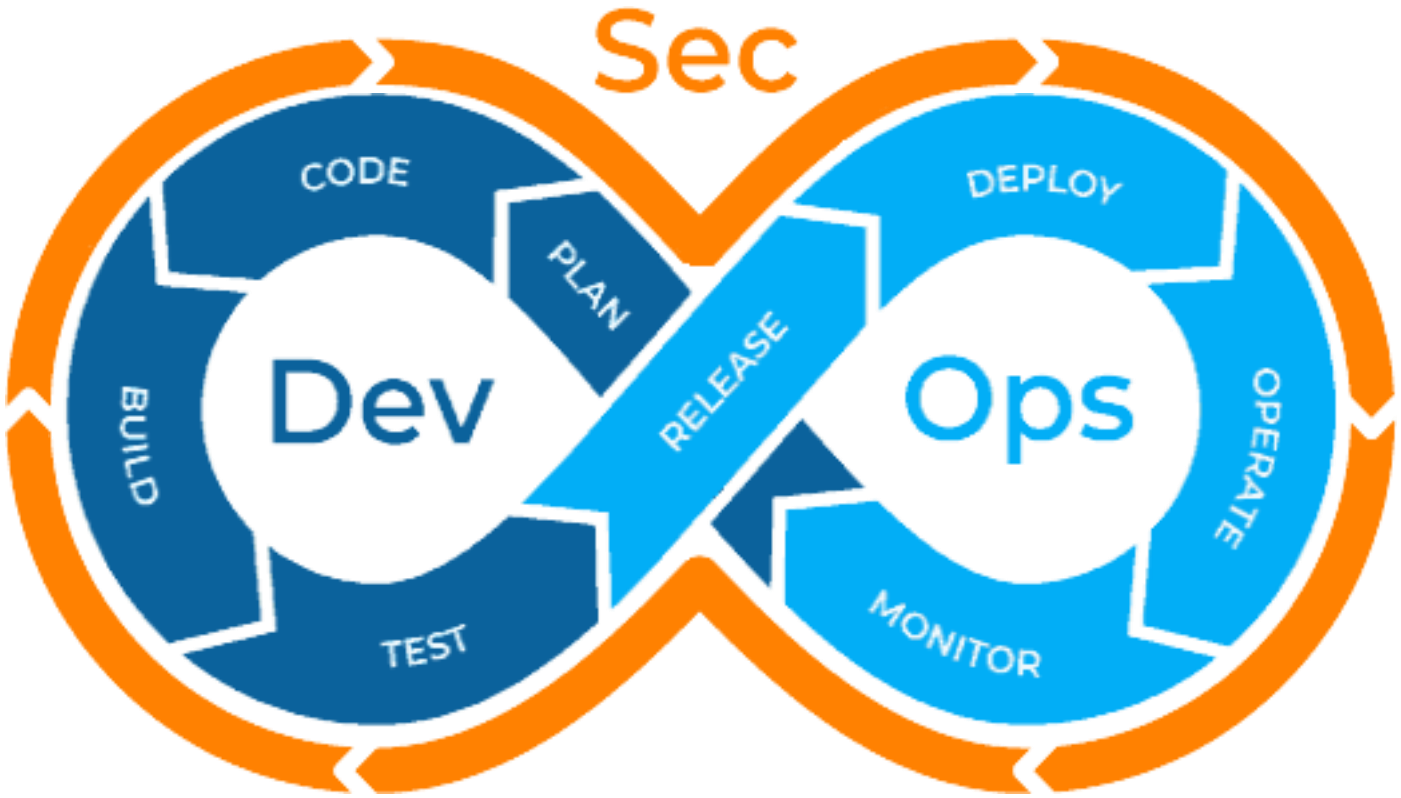
出展：WhiteSource Webiner on 25 june 2017



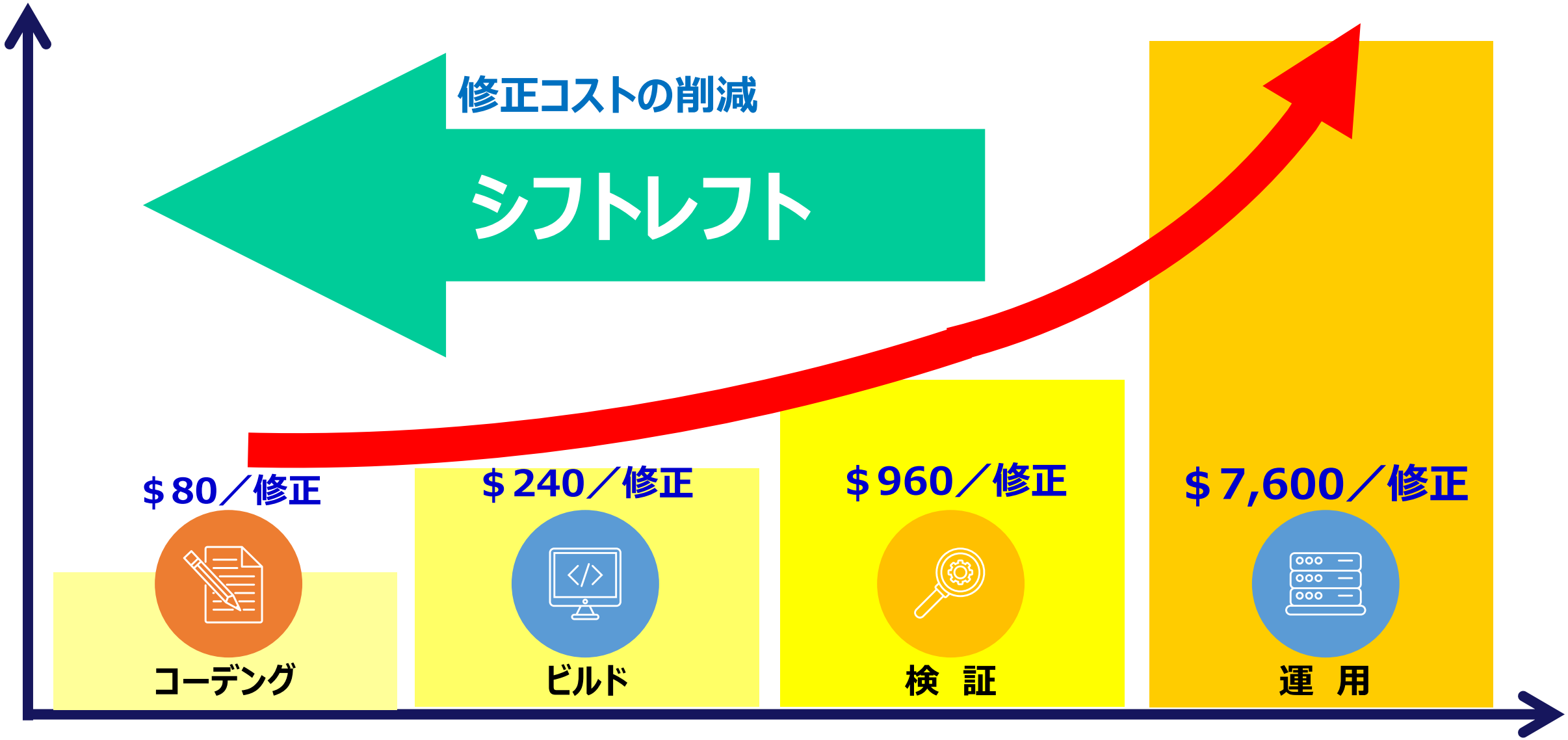
オープンソース利用時の注意点

- Security 53%
- Licensing 38%
- Quality 9%
- その他 0%

出展：WhiteSource Webiner on 25 june 2017



DevSecOpsに必要不可欠なシフトレフト



60-80%

近年の調査ではシステムのコードに含まれるオープンソースの割合は60%～80%との結果が報告されています。

つまり、
独自のコードは
40%～20%

シフトレフトを実現するには
オープンソースの管理が必須!!

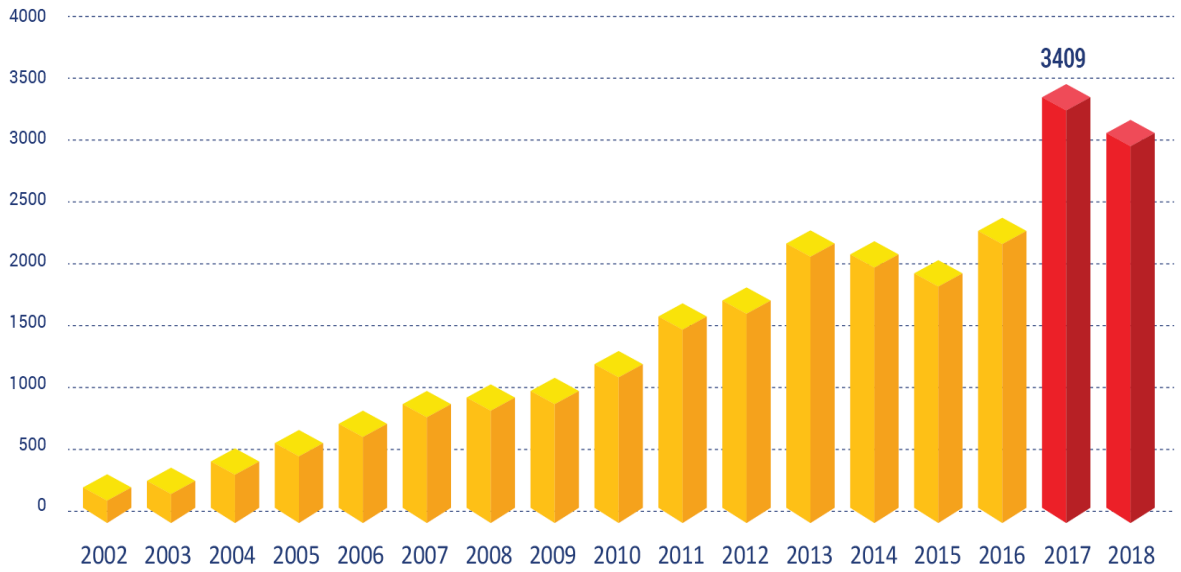
既知の脆弱性が含まれいないこと、、

既知の不具合が含まれていないこと、、

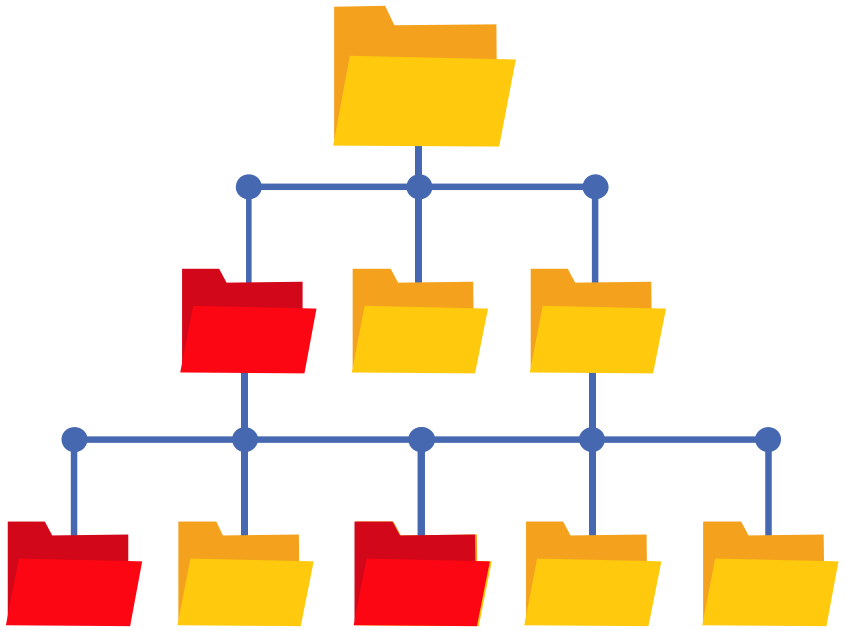
会社のポリシーに準拠していること、、

オープンソースの管理は簡単ではないらしい。
なぜなら、、

報告される脆弱性数の増加



推移的な依存関係の増加



手動管理

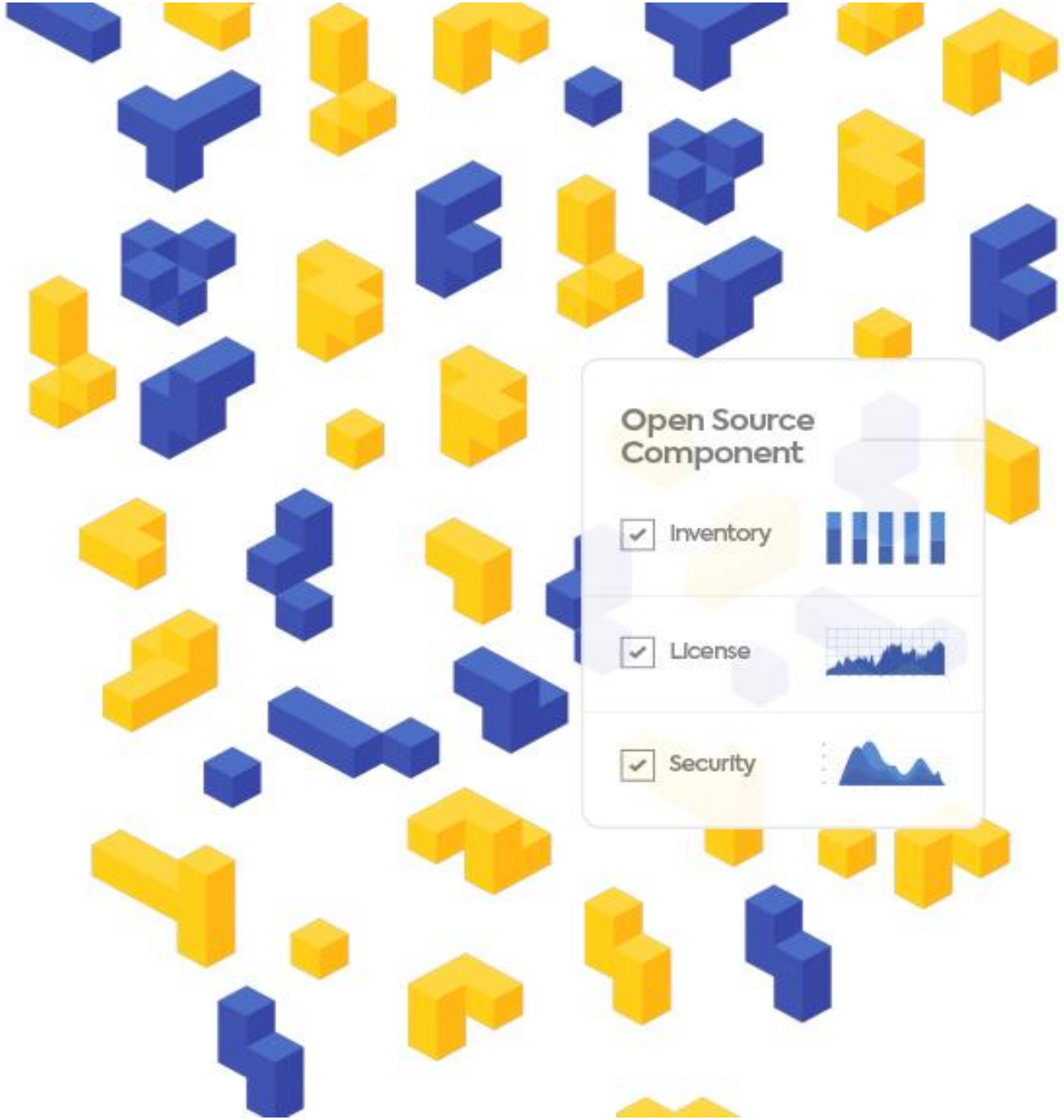
手動でオープンソースの各コンポーネントを検証するのは、速度と精度に限界があります。

放　置

手を付けないでいると、より大きな問題に発展します。

自動化

でも、どうやって
オープンソースの管理を
自動化するればいいの？



その課題

が解決します。

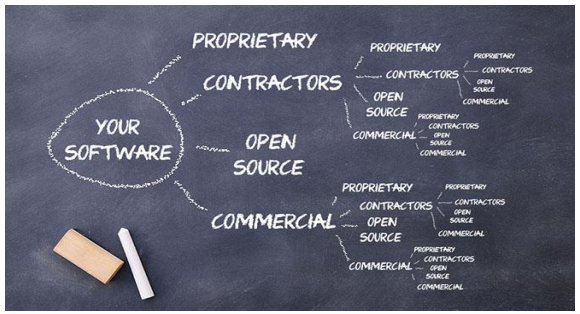
WhiteSource

WhiteSource
for Developers

WhiteSource
Core

オープンソース管理のベースライン

Inventory



利用しているオープンソースの洗出し

Security

オープンソースの脆弱性を指摘し、解決策を提示

Quality

オープンソースのバグやアップデート情報を、リアルタイムに通知

Licenses

企業ルール、法令・規則の順守

リアルタイムアラート

企業ポリシーの適用

オープンソースの検出

各種レポート

WHITESOURCE
CORE

WhiteSource の動作環境

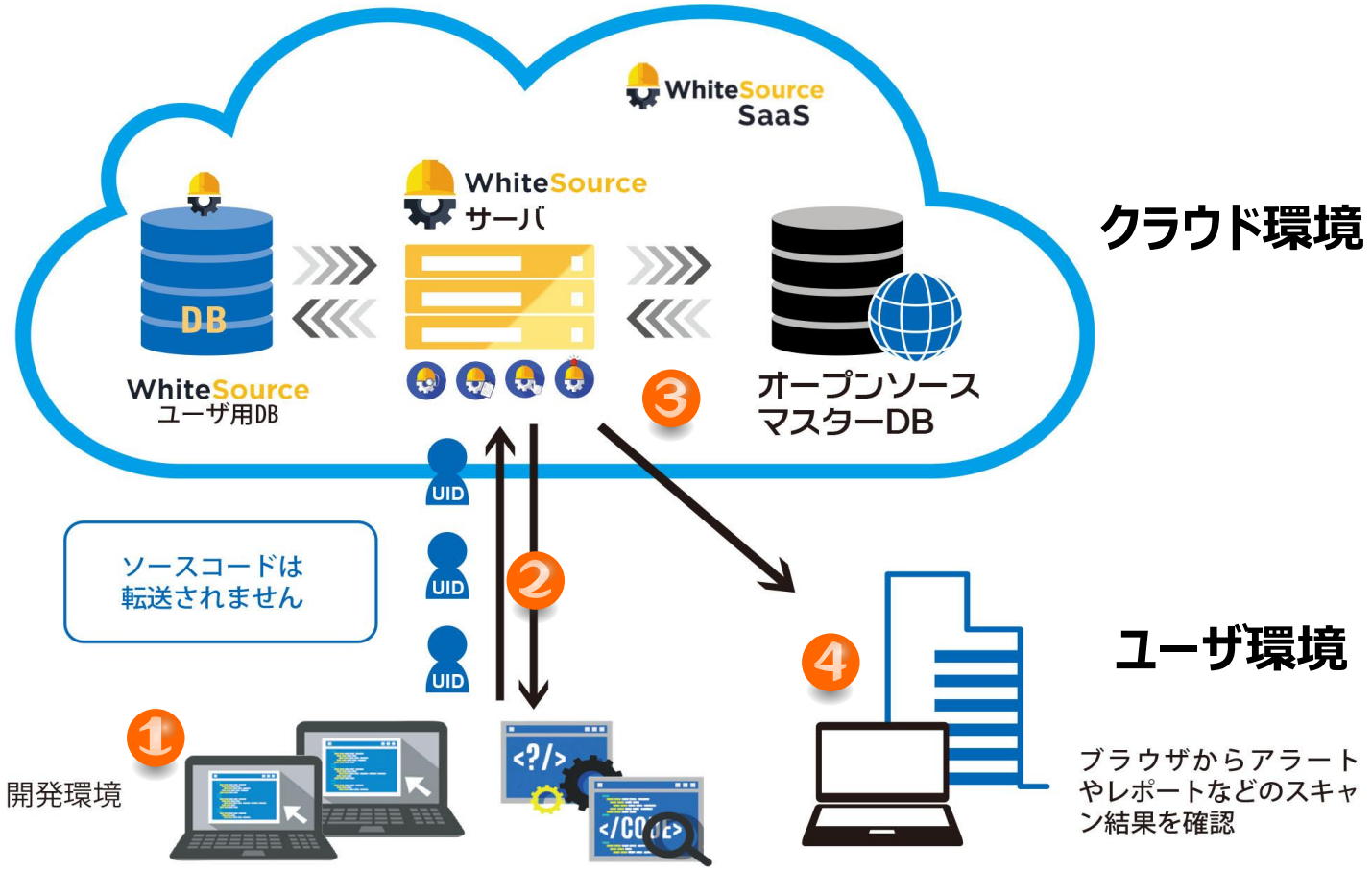
WhiteSource は、サービスとして提供
（※オプションで、オンプレミスでの提供も可能）

❶ 開発環境にエージェントをインストール
エージェントはソースコード、バイナリーコードを検査して各ファイルを一意に識別するUIDを生成します。

❷ 生成したUIDをクラウドに送付

❸ オープンソースマスターDBとマッチング

❹ 自社のオープンソース情報にアクセス
ブラウザから各種情報の利用可能が可能になります。



WhiteSource では、全ての通信データは TLS（HTTPS）を利用

サービス提供なので簡単に導入して、直ぐに利用開始できます。

ユーザ環境

ステップ 1

- 開発環境に置かれたエージェントがソースコード内、バイナリコード内のそれぞれのファイルに対する独自の識別子（UID）を計算します。
- すべての識別子（UID）が、WhiteSource のサーバへと送付されます。

ソースコードは送付されません

クラウド環境

ステップ 2

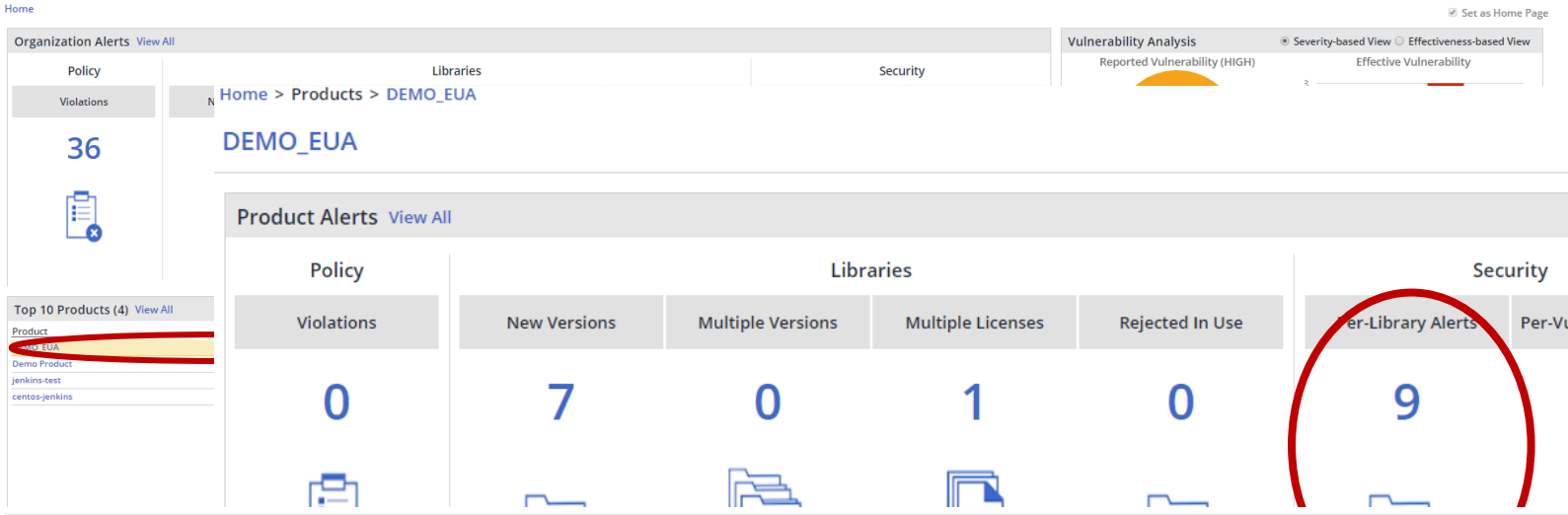
- UID は WhiteSource のマスターデータベースとマッチングされます。
- OSS と認識されたものに対して、セキュリティ、ライセンス、品質といった関連するすべてのデータが、ユーザ特定の OSS インベントリーに蓄積されます。

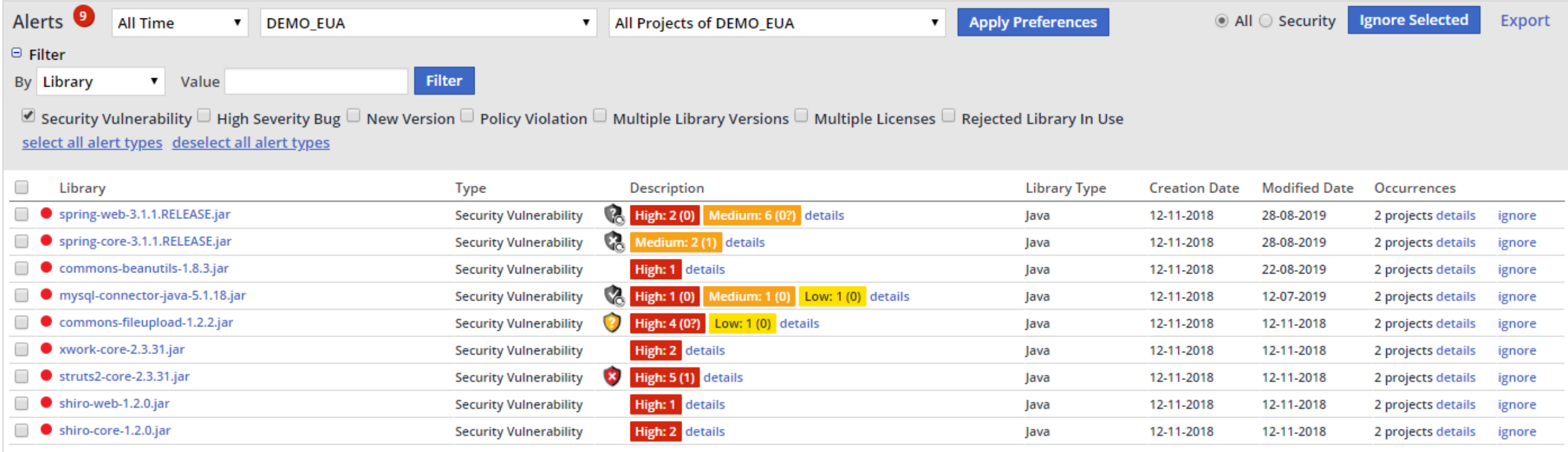
ユーザ環境

ステップ 3

- ユーザアカウントの情報がアップデートされます。
- すべての解析データがオンラインで利用可能となります。

WhiteSource 画面イメージ（ブラウザーベース）





Library	Type	Description	Library Type	Creation Date	Modified Date	Occurrences
spring-web-3.1.1.RELEASE.jar	Security Vulnerability	High: 2 (0) Medium: 6 (0?) details	Java	12-11-2018	28-08-2019	2 projects details ignore
spring-core-3.1.1.RELEASE.jar	Security Vulnerability	Medium: 2 (1) details	Java	12-11-2018	28-08-2019	2 projects details ignore
commons-beanutils-1.8.3.jar	Security Vulnerability	High: 1 details	Java	12-11-2018	22-08-2019	2 projects details ignore
mysql-connector-java-5.1.18.jar	Security Vulnerability	High: 1 (0) Medium: 1 (0) Low: 1 (0) details	Java	12-11-2018	12-07-2019	2 projects details ignore
commons-fileupload-1.2.2.jar	Security Vulnerability	High: 4 (0?) Low: 1 (0) details	Java	12-11-2018	12-11-2018	2 projects details ignore
xwork-core-2.3.31.jar	Security Vulnerability	High: 2 details	Java	12-11-2018	12-11-2018	2 projects details ignore
struts2-core-2.3.31.jar	Security Vulnerability	High: 5 (1) details	Java	12-11-2018	12-11-2018	2 projects details ignore
shiro-web-1.2.0.jar	Security Vulnerability	High: 1 details	Java	12-11-2018	12-11-2018	2 projects details ignore
shiro-core-1.2.0.jar	Security Vulnerability	High: 2 details	Java	12-11-2018	12-11-2018	2 projects details ignore

メールによる変更内容の通知

Security

Vulnerability Score

Vulnerable Libraries

348	7	30
No Known Vul.	Vulnerable & Updated	Vulnerable & Outdated

Severity Distribution

0	15	22
Low	Med	High

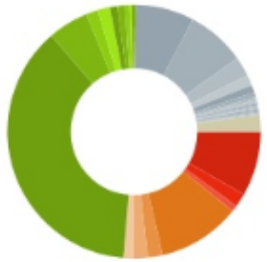
Aging Security Vulnerabilities

0	0	37
Less than 30D	Less than 90D	Over 90D

License Risks and Compliance

Quality

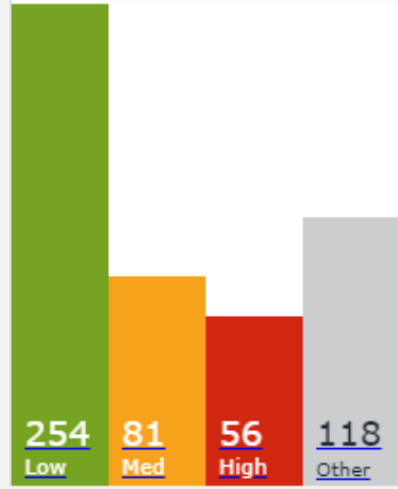
License Distribution



- GPL 2.0 (43)
- GPL 3.0 (9)
- GPL 2.0 Classpath (4)
- LGPL 3.0 (55)
- CDDL 1.0 (10)
- LGPL 2.1 (9)
- Eclipse 1.0 (7)
- Apache 2.0 (194)
- MIT (27)
- BSD 3 (8)
- Public Domain (8)
- CDDL 1.1 (5)
- BSD 2 (5)
- Apache 1.1 (3)
- Common Public 1.0 (2)
- Mozilla 2.0 (1)
- Mozilla 1.1 (1)
- Proprietary (39)
- Enterprise Dist... (39)
- Suspected Comme... (13)
- BSD (7)
- Unspecified Lic... (5)
- LGPL (3)
- Scala License (2)
- CDDL or GPLv2 w... (2)
- JTidy License (1)
- H2 License (1)
- W3C (1)
- CC BY 3.0 (1)
- Sax PD (1)
- Crypto (1)
- Dom4j (1)
- Bouncy Castle L... (1)
- Requires Review (11)

Total License Types: 33, Total Libraries: 385

License Risk Distribution



254	81	56	118
Low	Med	High	Other

36 Policy Violations

Outdated Versions

147 3+ versions

51 2 versions ago

26 Previous

234 Outdated Libraries

161 Up-to-Date Libraries

10 Libraries w/ Multiple Versions

New for the week Sep 17 - Sep 24:

0 New Libraries	0 New Security Vulnerabilities	0 New Policy Violations

多様なツールと連携可能

Repositories

JFrog Artifactory

JFrog Xray

Build Tools

Apache maven

gradle

Setuptools

Bundler

GRUNT

Nant

<APACHE ANT>

npm

CI Servers

Jenkins

TeamCity

Atlassian Bamboo

Visual Studio

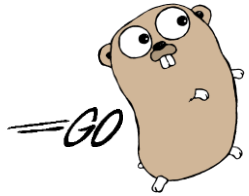
Issue Trackers

JIRA

Technology Partners

MICRO FOCUS

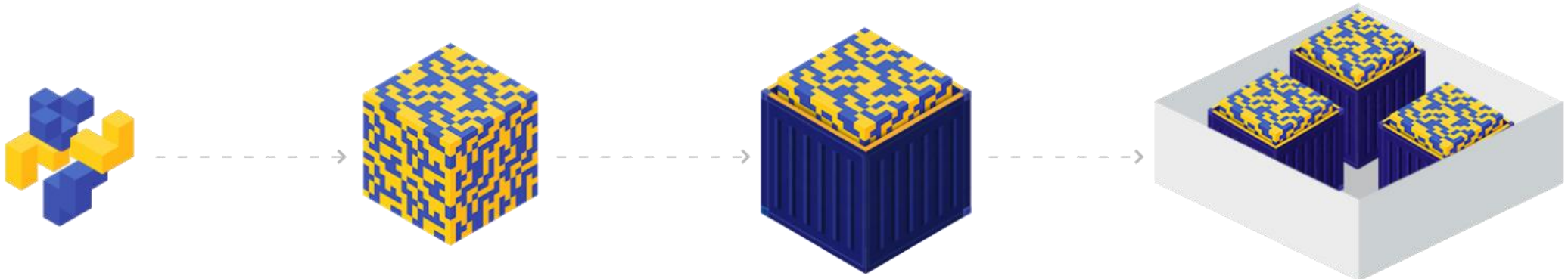
多数の言語をサポート



Objective-C

WhiteSourceはコンテナもサポート

コンテナ開発のための包括的なソリューションを提供



開発　構築　コンテナレジストリ　展開

一般的なコンテナレジストリとの高度な統合

Kubernetesとの統合によるポリシーの自動的な適用と継続的な監視

DevSecOpsに求められる3要素

■ オートメーション
- ➢ 既存開発環境へのシームレスな統合

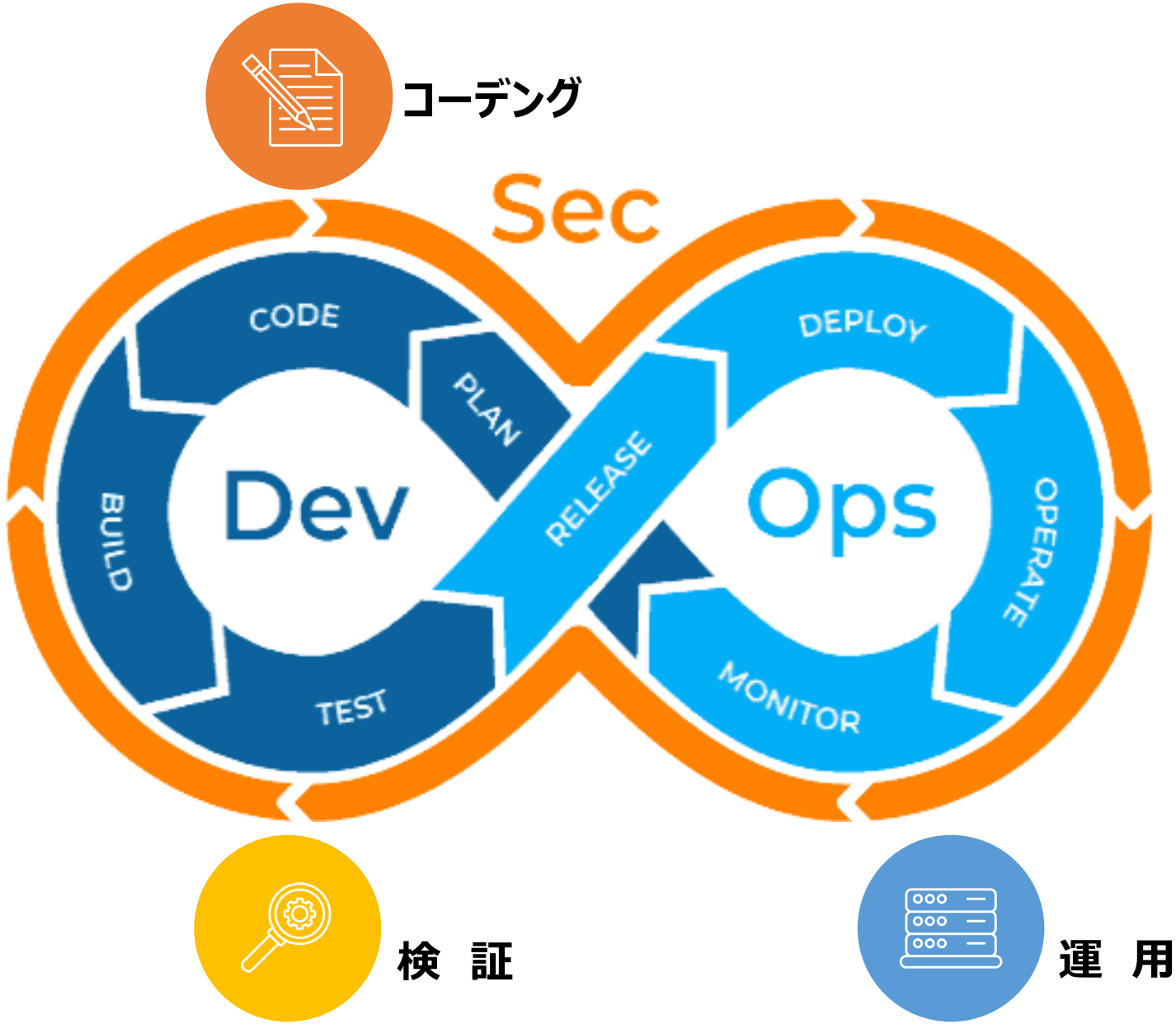
多数のリポジトリー、ビルドツール、CI サーバ等をサポートしています。

■ スピード
- ➢ 結果は継続的に、且つ数分で報告

開発サイクルの中で適切にオープンソースの分析を行い、迅速にレポートします。

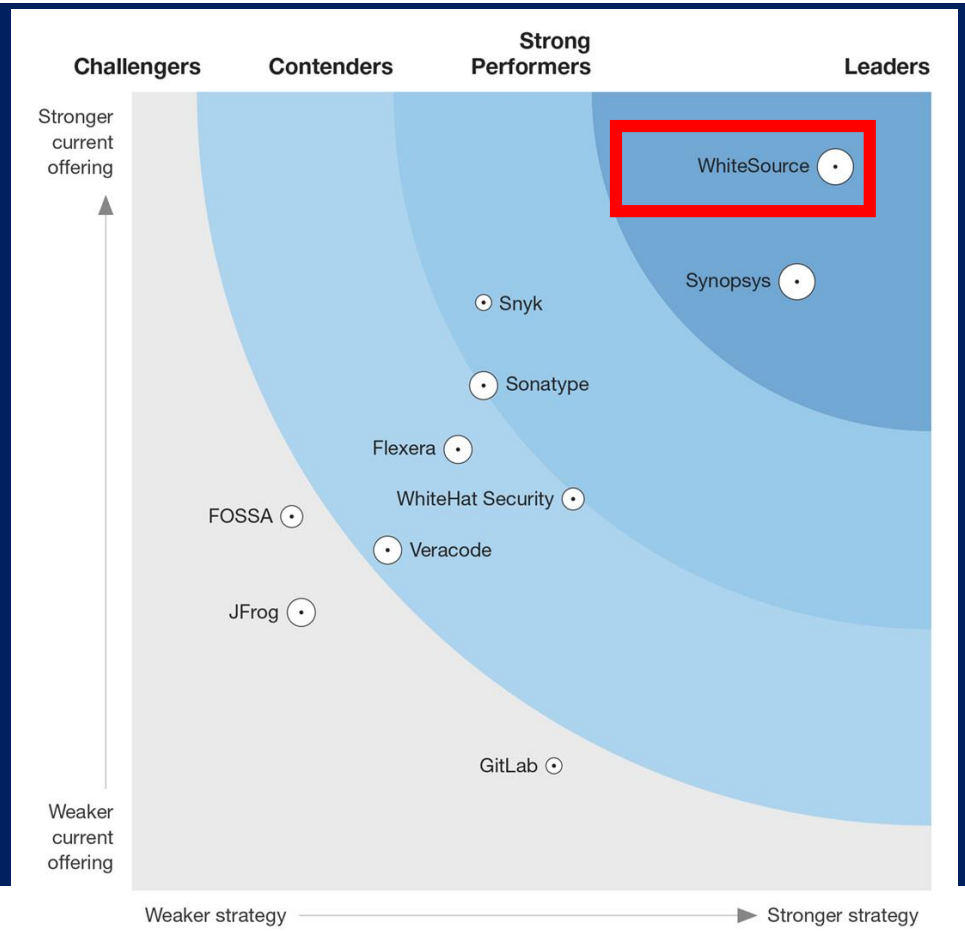
■ カバレッジ
- ➢ 幅広く、深い分析

200以上の言語サポートと７０Mの オープンソースファイルの情報により詳細に 分析をします。



WhiteSource Software

THE LEADER
OF SOFTWARE COMPOSITION ANALYSIS



2011年に設立
オフィス：ニューヨーク、ボストン、ロンドン テルアビブ

700+
顧客

1.2 M
以上の開発者を支援

フォーチュン100社の23%が利用

前年比3Xの成長

OVER 700 CUSTOMERS

ご清聴ありがとうございました。

現在のアプリケーション開発では、開発工数の削減、品質の高いアプリケーションの作成など多くのメリットがあることからオープンソースソフトウェア（OSS）の利用が前提となっています。一方、OSSとうまく付き合うための取組が注目されています。

特にOSSの脆弱性を狙ったサイバー攻撃が急増しています。また、ライセンスを正しく理解しないで利用するとライセンス違反として訴訟を起こされることも考えられます。

WhiteSourceはOSSと上手に付き合うことを支援するソリューションです。

WhiteSourceを利用頂くことで、OSSのメリットを活かしたシステム構築の実現をご支援させて頂きます。

＜お問い合せ先＞

株式会社OPENスクエア

営業担当

E-Mail： sales_os@opensquare.co.jp
TEL： 03-6413-1840

無料トライアルをお試しください

資料をご覧頂き、ありがとうございました。

END