



OSSセキュリティ&コンプライアンス管理ツール

WhiteSource

その脆弱性がハッカーに狙われる前に

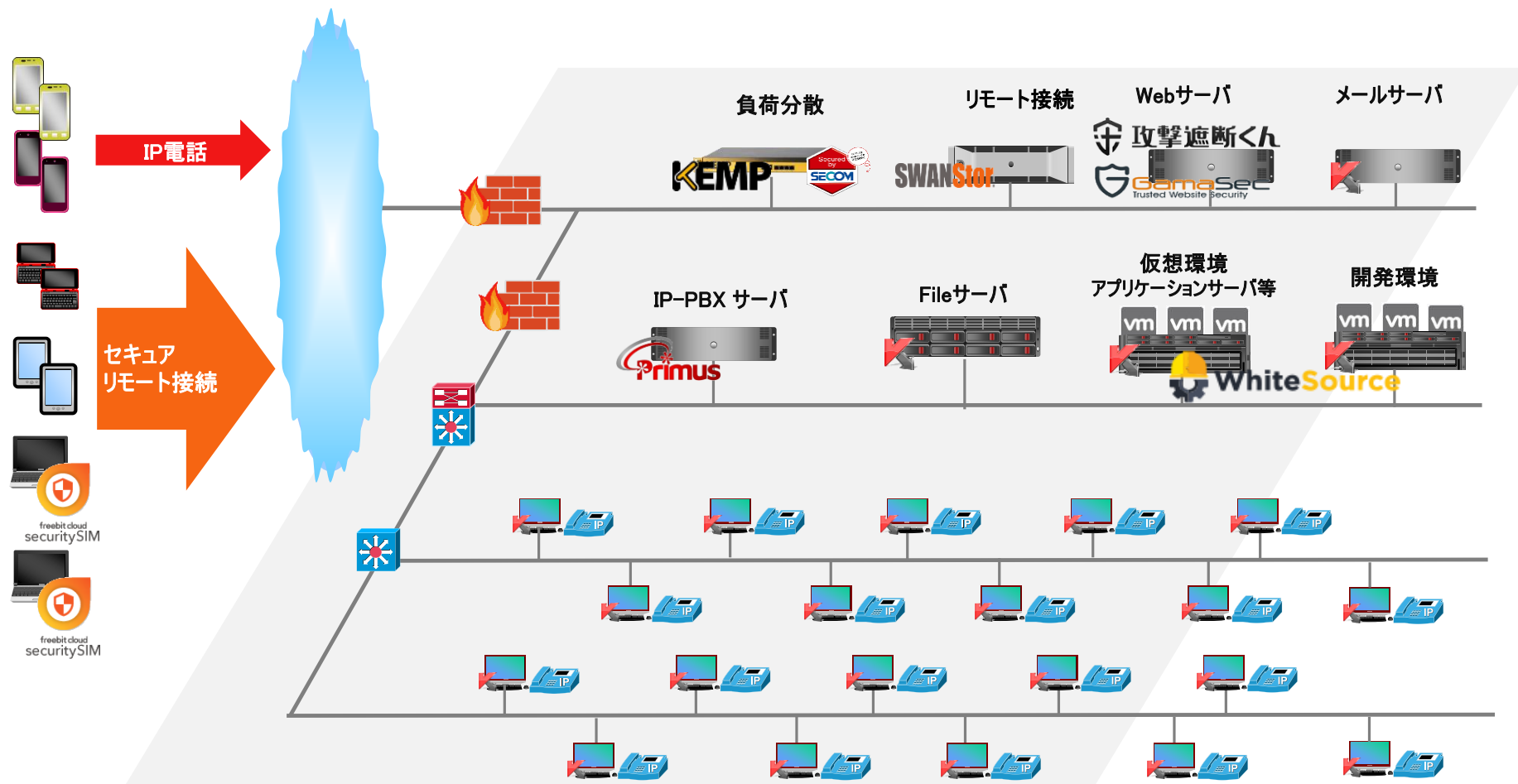


株式会社OPENスクエア
営業担当

sales_os@opensquare.co.jp

最初に、、、OPENスクエアとは

ICT製品の販売、サポートを提供し、お客様のICT活用を支援することで社会貢献します。



本日、お伝えしたいこと

■オープンソースの利用状況

- ✓今やオープンソースはソフト開発に必須になっています。

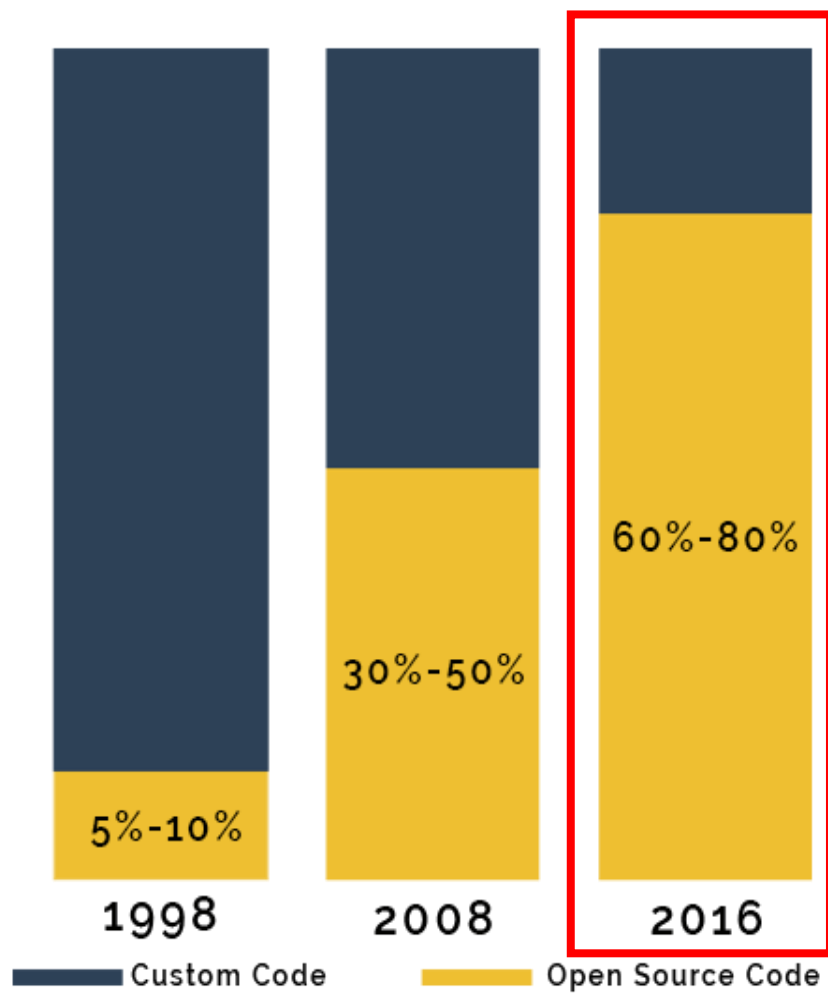
■オープンソース利用時の課題

- ✓オープンソースの脆弱性はハッカーに狙われています。
- ✓何のオープンソースを利用しているか把握していない。

■セキュリティ対策としてのオープンソース管理

- ✓Whitesourceのご紹介
 - OS、ミドルウェアのセキュリティパッチを体系的に管理できます。
 - 人手を介さず自動運用が可能です。

オープンソースの利用状況



今や、ソフトウェア製品に含まれる **60～80%** のコードはオープンソースコンポーネントが占めています

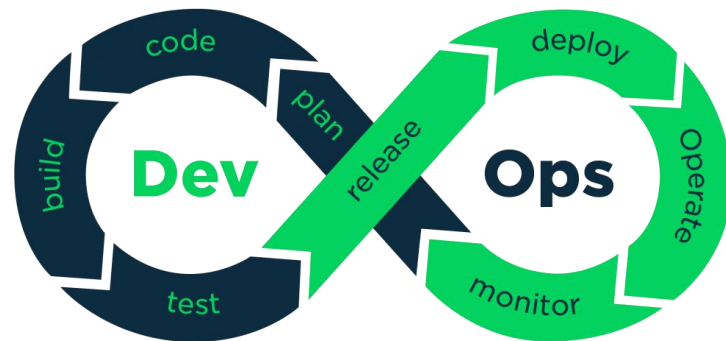


**Forrester developer survey 2015*

なぜオープンソースが使われるのか？

- リリースまでの短いサイクル要求 DevOps
- 開発コスト削減
- 最新技術の早期採用 等

ソフト開発の生産性向上が至上命題！



ソースコードが公開されていて、簡単に入手できる
オープンソース(OSS)を使わない手はない！

オープンソース利用時の課題

何でしょうか？

ライセンス違反

それだけでしょうか？

脆弱性の把握

それだけで十分でしょうか？

新たな不具合情報や
アップデートの把握

そもそも、随所に使われているOSSを完全に把握できていないかも？



日々報告される多くのOSS関連脆弱性

CVE-ID

CVE-2011-3928	テスラモーターズの車載情報端末のブラウザー QtCarBrowser の WebKit エンジンに任意のコードが実行できる脆弱性
CVE-2017-5638	Apache Struts 2 に、Jakarta Multipart parserのファイルアップロード処理に起因する、リモートで任意のコードが実行される脆弱性が存在
CVE-2017-1000367	Linux の sudo コマンドで全特権の取得。
CVE-2017-7925	ネットワーク管理者権限で任意の操作が行われる可能性
CVE-2017-1001000	REST APIの脆弱性によるWebサイトの改ざん
CVE-2016-8747	Tomcatの脆弱性 セッションIDや応答などの情報漏洩の可能性
CVE-2016-6662	OpenSSL の拡張機能 Heartbeat に脆弱性が存在し、情報漏洩
CVE-2015-0235	Ghost - glibc にバッファオーバーフローの脆弱性。DoS状態に陥ったり、リモートからのコード実行が可能になる恐れ
CVE-2014-6271	Shellshock -- bashに存在する脆弱性。遠隔でシェルコマンドを実行することが可能になり、サーバが乗っ取られたり、不正プログラムに感染の恐れ。

オープンソース活用時の課題

④ バグやアップデートされていないコンポーネント使用の回避



① 使用している「モノ」を知る



回避
把握
課題
順守
確保

Wix gets caught "stealing" GPL code from WordPress

In which Wix forgets what happens when you add GPL code to your closed-source app.

185 Last Friday, Automatic Number User Kullerling—the founding developer of the WordPress open source blogging and content management platform—posted an open letter to his company Wix.

FSF Files Lawsuit against Cisco on Behalf of the FSF

December 11, 2008

VMware alleged to have violated Linux's open source license for years

VMware says "Linux is without merit," company is "committed" to open source.

JOHN BROWN - 10/10/11, 8:57 PM

Google Beats Oracle on Copyright Claim

Defeating \$9 Billion Claim

11/10/2012

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

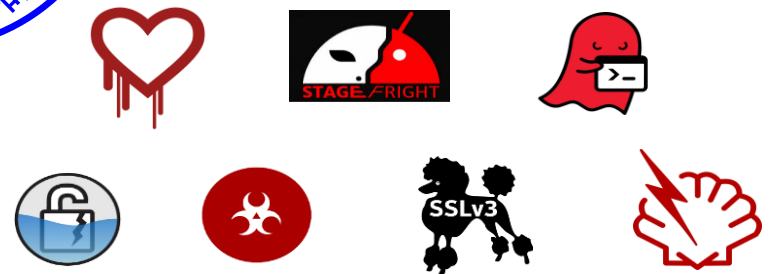
U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

U.S. 9th Circuit Court of Appeals has ruled in favor of Google.

Software developers have sued to address Google's use.

② 製品のセキュリティ確保



③ 法令・規則（ライセンス条項）の順守

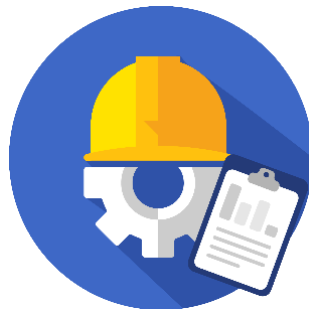
WhiteSourceソリューション

現状を把握



検出

ビルドの実施中にコード内のすべての**オープンソースコンポーネント**を自動的に検出します。



レポート

クリックするだけで、オープンソース活用状況に関する**包括的な最新版のレポート**の作成が可能となります。

継続的な管理



選択

オンラインで検索しながら、**最適なオープンソースコンポーネント**を選択が可能です。



警告

セキュリティリスク、ポリシーの落とし穴、ソフトウェアのバグに関して**リアルタイムに警告**します。

WhiteSource を活用することで課題を克服

①使用している「モノ」を知る

②製品のセキュリティ確保

③法令・規則
(ライセンス条項)の順守

④バグやアップデートされていないコンポーネント使用の回避

- OSS コンポーネントと従属性の **自動** 検出
- 300万のコンポーネントと7000万のソースファイルから構成される **データベース**
- **20以上** のプログラミング言語をサポート

Dependency Path

```

graph TD
    A[udson-core-2.2.0.jar] --> B[commons-beanutils-1.8.0.jar]
  
```

close

Product Summaries (5)

Product	Projects	Libraries
HR	4	328
CRM_Prod	4	80 (183 clusters)
Test	6	50
NewProj	5	22 (4 clusters)
TFS Test	1	8

Inventory Report Organizational

Filter

Library Name	Type	Description	Licenses	Occurrences
gradle-1.4.jar	Java		MIT	1 - client-0.1.2
linux-nfc-next-stable-master-2008-04-23	Source Library		GPL 2.0	2 - core-system-cpp - 2
linux-kvm-arm-kvm-68	Source Library	A standard Linux kernel tree with KVM for ARM patches	GPL 2.0	2 - core-system-cpp - 2
gradleandroid-plugin-1.1.0.jar	Java	Android plugin for the Gradle build system.	Apache 2.0	1 - client-0.1.2
udson-cli-2.2.0.jar	Java	The module that constitutes the main hudson.war	MIT	1 - client-0.1.2
jboss-as-server-7.0.2.Final.jar	Java	JBoss Application Server: Parent Aggregator	LGPL 2.1	1 - client-0.1.2
jboss-as-controller-7.0.2.Final.jar	Java	JBoss Application Server: Parent Aggregator	LGPL 2.1	1 - client-0.1.2

WhiteSource を活用することで課題を克服

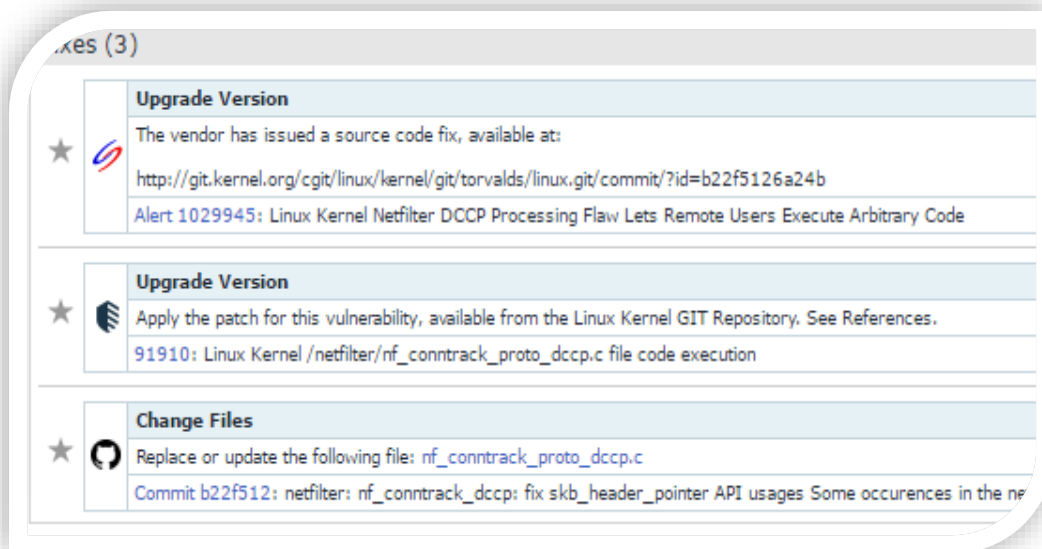
①使用している「モノ」を知る

②製品のセキュリティ確保

③法令・規則
(ライセンス条項)の順守

④バグやアップデートされていないコンポーネント使用の回避

- 多様なソース及びアドバイザリーをベースとした23万以上の脆弱性検出
- 誤検出回避のための独自アルゴリズムによる正確なマッチング
- リリース後に判明した脆弱性やバグも自動トラッキングし、アラート
- 問題点解決のための解決オプション提示(全脆弱性の内70%に対し)



WhiteSource を活用することで課題を克服

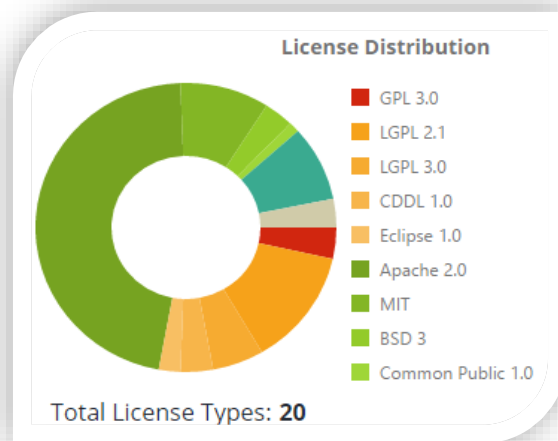
①使用している「モノ」を知る

②製品のセキュリティ確保

③法令・規則
(ライセンス条項)の順守

④バグやアップデートされていないコンポーネント使用の回避

- ライセンス情報とリスクアセスメント
- 様々なライセンスポリシーのサポート
- ユーザがコンプライアンスルールを定めることが可能
違反するライセンス、脆弱性存在時にビルド失敗やアラート通知
- リリースモジュール管理の自動化



GPL 3.0 (Full text)

Information is provided on an as-is basis, please consult your legal advisor

Copyright Risk Score

1. Exception to Section 3 of the GNU GPL. You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL... 3. Object Code Incorporating Material from Library Header Files. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length)... 4. Combined Works. You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications

Patent & Royalty Risk

(taken from GPL V3 and applies to the LGPL as well) 11. Patents. Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

Royalty Free: Yes

Copyright: Partial

0. Additional Definitions. ...The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version. ...1. Exception to Section 3 of the GNU GPL. You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

Linking: Dynamic

3. Object Code Incorporating Material from Library Header Files. The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length)... 4. Combined Works. You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following: ... 0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source. 1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

OSD Compliant: Yes

Open Source Initiative

WhiteSource を活用することで課題を克服

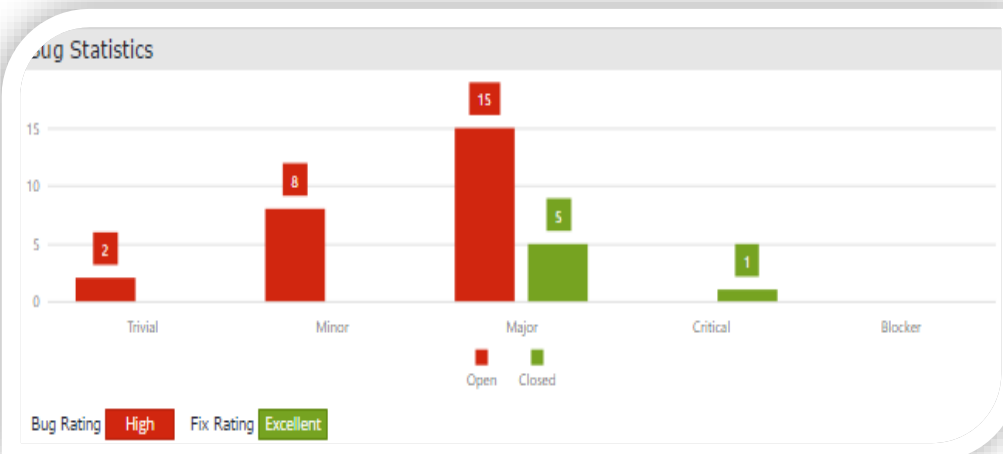
①使用している「モノ」を知る

②製品のセキュリティ確保

③法令・規則
(ライセンス条項)の順守

④バグやアップデートされていないコンポーネント使用の回避

- 重大度別にソフトウェアバグのトラッキング
- OSS バージョン毎の総合品質スコア
- アクティビティとメンテナンスレベルのトラッキング



Quality (details)

Quality Rating	Fair
Bug Rating	High details
Fix Rating	Excellent details
Version Activity	High details

脆弱性は攻撃者が「発見」するからなくなる

- 攻撃者はソフトに対する攻撃アプローチを常に研究している。攻撃者が新たな攻撃手法を生み出すと、その攻撃を可能にしているソフトの状態が脆弱性と呼ばれるようになる。
- あらかじめソフトに存在する脆弱性を攻撃者が「発見」することもあるが、むしろ脆弱性を攻撃者が「発見」していると考えのほうが実態に近い。
- ソフトの開発者が、あらゆる攻撃手法を事前に想定して入力データをチェックすることは事実上不可能だ。このため、攻撃者がいる限り脆弱性はなくならないと考えていいだろう。

出展 <http://itpro.nikkeibp.co.jp/atcl/column/17/090100359/090100001/>

Apatch Struts2の脆弱

2013年から2016年にかけてOGNLインジェクションの対策（パラメータまわり）

2017年 OGNLインジェクションの脆弱性が判明

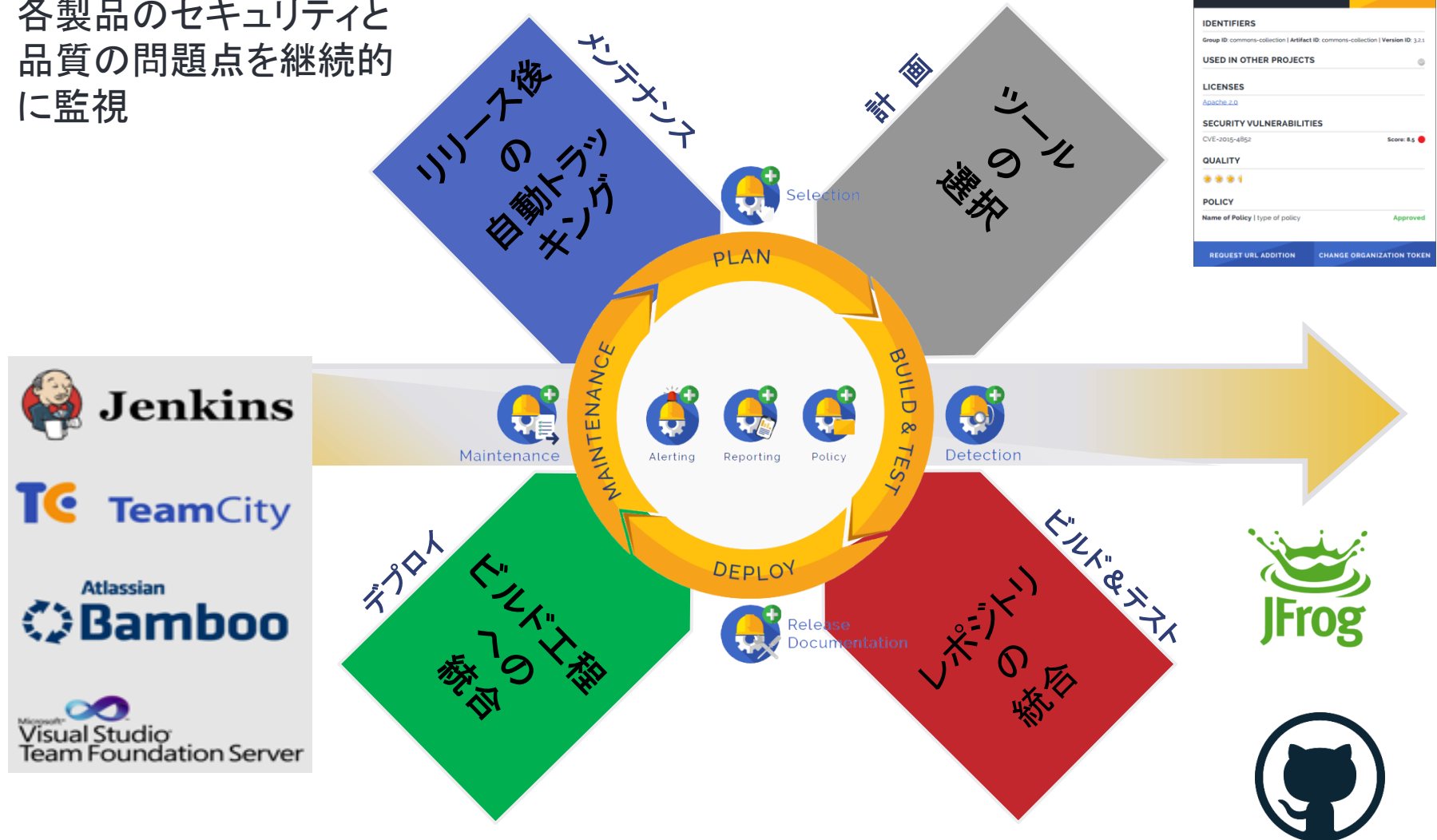
HTTPで送られてきた文字をエラーログに出力する際にコードが実行される

今後もStruts2の新たな脆弱性が発見/発見される可能性がある。

脆弱性対策はシステム開発ライフサイクルに組込むことが重要

SDLC(システム開発ライフサイクル)の各工程で利用

各製品のセキュリティと
品質の問題点を継続的
に監視



統合可能なツールや環境

Repositories



Build Tools



CI Servers



Jenkins



Issue Trackers



ALM



Application Security Testing Tools



全てのプログラミング言語をカバー

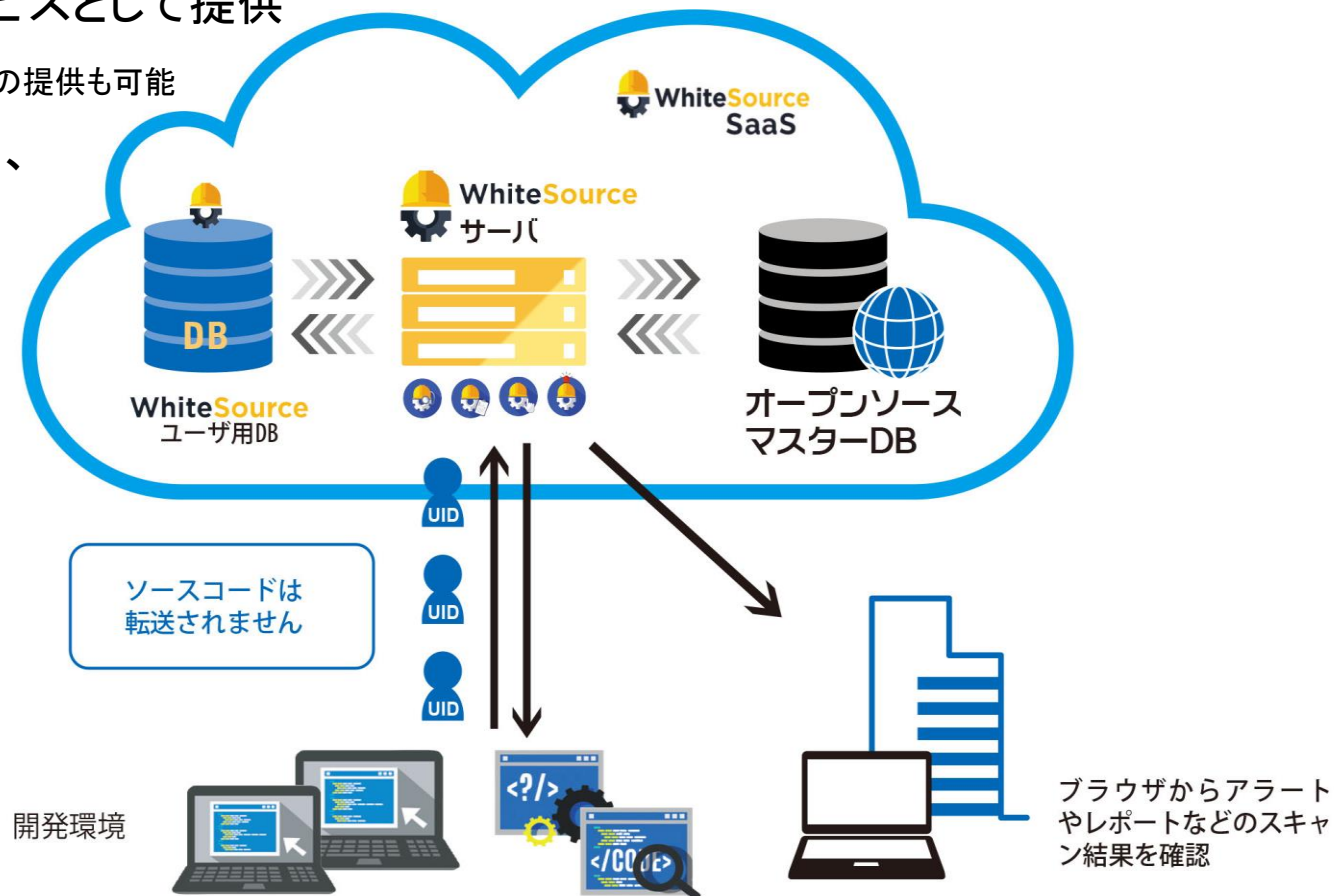


SaaSとしてのサービス提供

- 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

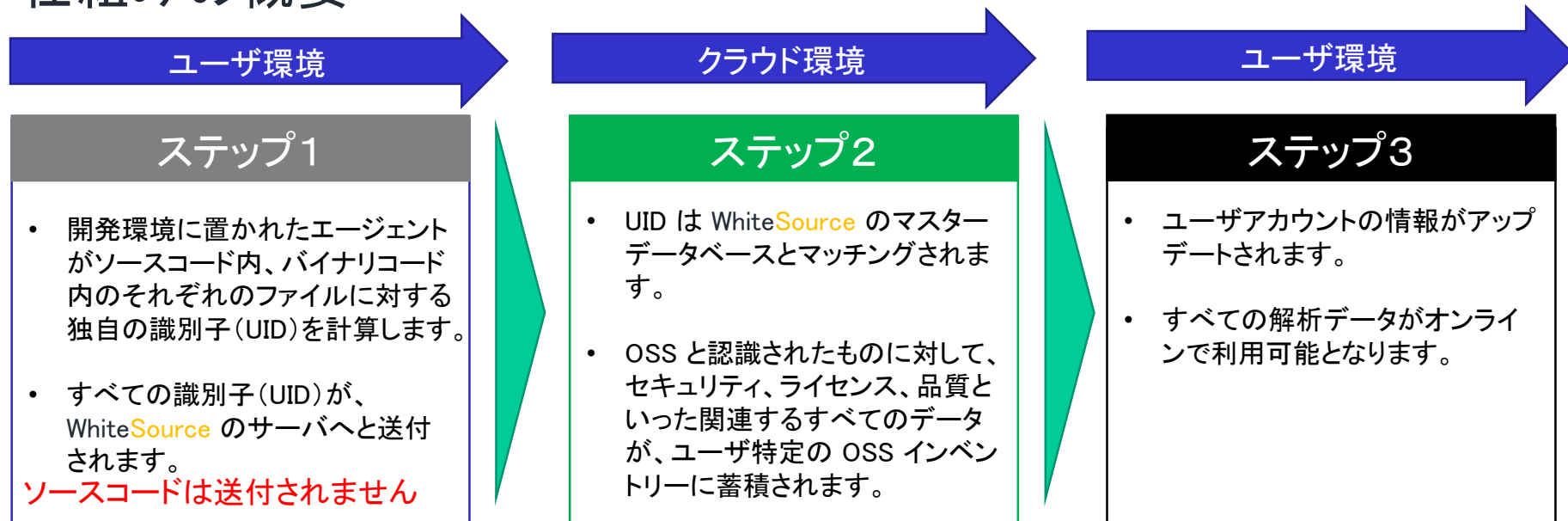
- WhiteSource 利用者は、
ローカルエージェント
もしくは
開発環境プラグイン
を導入



WhiteSource では、全ての通信データは TLS(HTTPS)を利用するため安全です。

SDLC(システム開発ライフサイクル)の各工程で利用

仕組みの概要



WhiteSource 社の概要



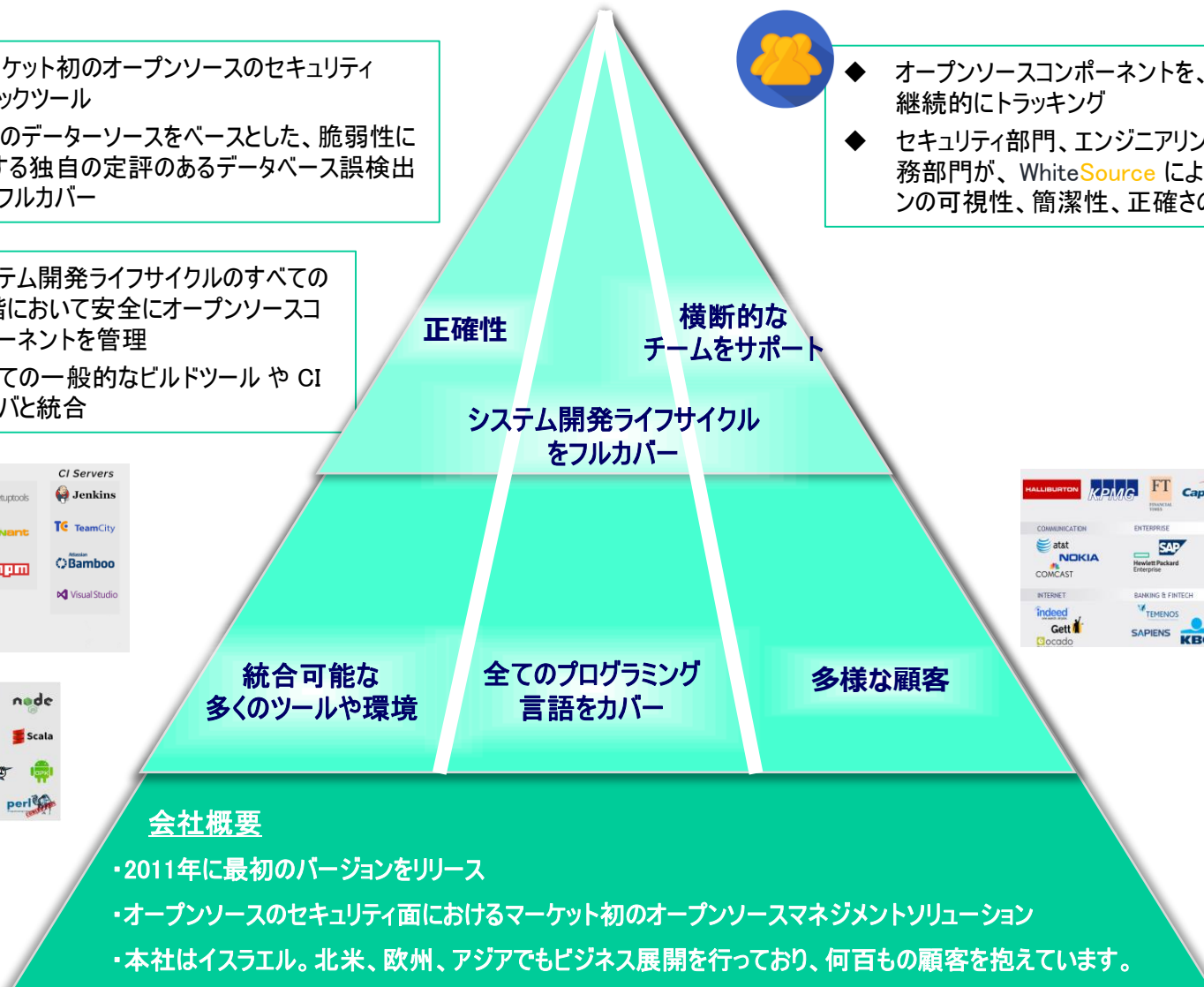
- ◆ マーケット初のオープンソースのセキュリティチェックツール
- ◆ 多くのデータソースをベースとした、脆弱性に関する独自の定評のあるデータベース誤検出なくフルカバー



- ◆ システム開発ライフサイクルのすべての段階において安全にオープンソースコンポーネントを管理
- ◆ すべての一般的なビルドツールやCIサーバと統合



- ◆ オープンソースコンポーネントを、すべての面で継続的にトラッキング
- ◆ セキュリティ部門、エンジニアリング部門や法務部門が、WhiteSource によるソリューションの可視性、簡潔性、正確さの恩恵を享受



主要顧客



COMMUNICATION

ENTERPRISE

HEALTHCARE

IOT + EMBEDDED



INTERNET

BANKING & FINTECH

GAMING

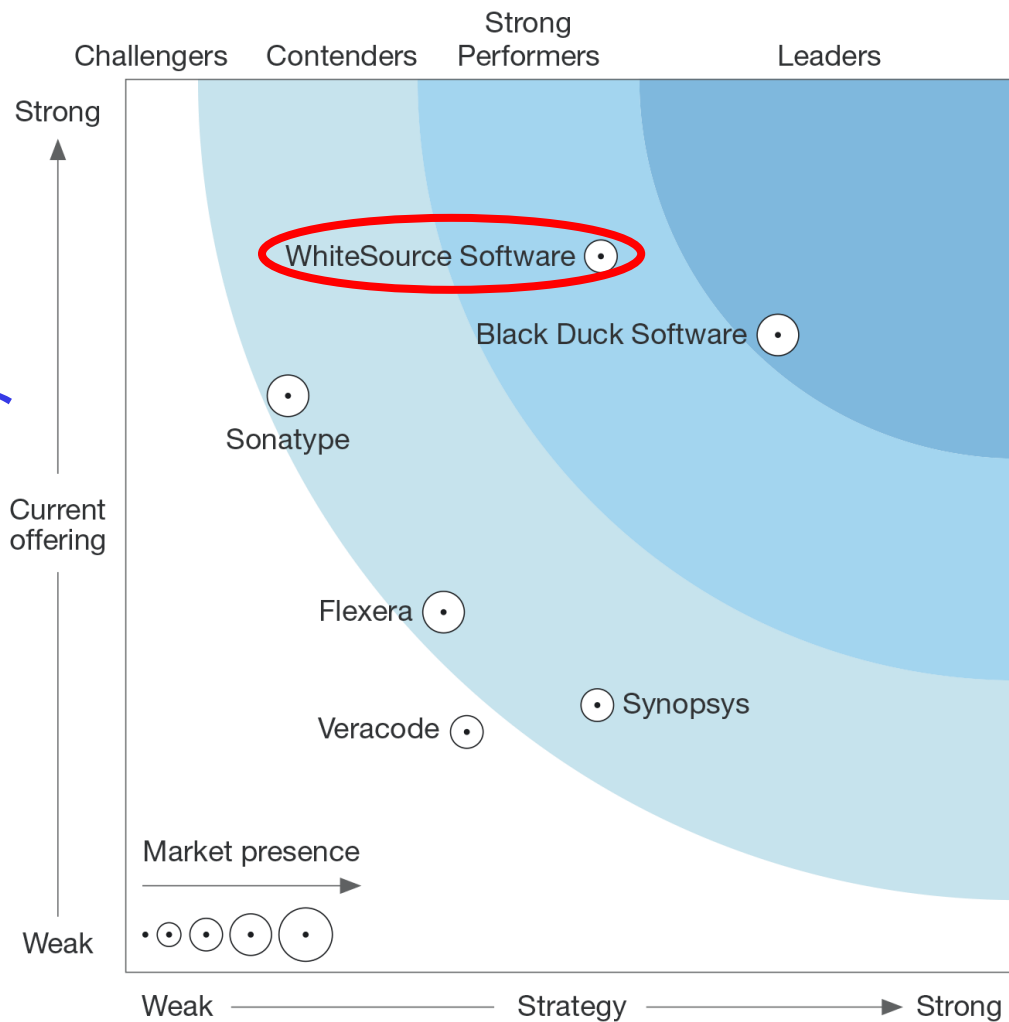
SECURITY



WhiteSource 社の業界内の位置づけ

WhiteSource 社は以下に関しても最も強力なサポートを提供します。

- 予防的な脆弱性マネジメント
- ポリシーマネジメント
- システム開発ライフサイクル統合



フォレスターウェーブによるソフトウェアコンポジション分析
(2017年第一四半期)

WhiteSource の強み1

- ◆ 圧倒的に情報量が多いマッチングデータベース
- ◆ 誤検知がほぼ無いアルゴリズム

	WhiteSource	競合他社
データベース サイズ	300万のコンポーネントと7000万の ソースファイルで構成	150万のオープンソースプロジェクト が登録
脆弱性情報源	12の第三者OSSデータベースとも 連携	主に2つのOSSデータベースからの 情報
脆弱性情報	23万以上	8万以上
解決策の提示	70%以上の脆弱性に対して解決策 提示	僅かな数の脆弱性に対して解決 策提示
データベースの 正確性	誤検知はほぼ無いマッチングのアル ゴリズム	診断結果の重複と誤検知で、手 動による分析のステップが必要

WhiteSource の強み2

SDLC の全工程で利用可能で、シフトレフトを実現。大幅な時間・コスト削減

- ◆ 統合可能なツールや開発環境が多く、また多くのプログラミング言語をカバー
- ◆ ビルドプロセスで、ユーザが定めたコンプライアンスルールの摘要も可能
- ◆ 製品リリース後に発見された脆弱性やバグにアラート

	WhiteSource	競合他社
プログラミング言語	Dockerコンテナを含む22のプログラミング言語とプラットフォームをサポート	プログラミング言語のサポートは限定的
統合化	多くの開発ツールと統合可能。プロセス全体を自動化	一部のビルドツールとは統合可能。
パフォーマンス	ビルドプロセスへの影響はごくわずか	影響が大きい。ビルドプロセスに数時間の影響を与えることもある
企業コンプライアンスの完全順守	ユーザがコンプライアンスルールを定めることが可能	ユーザ独自のコンプライアンスルールは適用できない
リリース後追跡	積極的なアラート通知	不明確

WhiteSource の強み3

- ◆ サービスなので、手軽に始められる
- ◆ 圧倒的なコストパフォーマンス

	WhiteSource	競合他社
提供形態	サービスなので、契約後すぐに始められる。 新規の設備投資も不要	オンプレミスでの提供のため、ユーザ側でサーバやデータベースの導入が必要で、始めるまでにコストも時間もかかる
費用	年間100万円未満から始められる	年間数百万円～ という場合が多い

最後に

いまやアプリケーション開発ではオープンソースソフトウェア(OSS)の利用が前提となっており、実際にアプリケーションの96%がOSSを利用しているとの調査結果もでています。OSSを利用することで開発工数を削減したり、品質の高いアプリケーションを作成できるなどの多くのメリットがありますが、一方ではOSSを上手に活用するための方法が模索されています。

特にOSSの脆弱性を常に把握し、対処しなければサイバー攻撃によるセキュリティ事故に繋がる可能性があります。また、OSSの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あります。

当社ではOSSを活用した、安全で効率的なシステム開発を支援するWhiteSourceをご提案させていただきます。何卒、宜しくご検討お願いいたします。



＜お問合せ先＞

株式会社OPENスクエア
営業担当

E-Mail: sales_os@opensquare.co.jp

TEL: 03-6413-1840

資料を最後までご覧頂き、ありがとうございました。

END