



OSSセキュリティ&コンプライアンス管理ツール

WhiteSource

今、利用しているオープンソースのライセンスご存知ですか？



株式会社OPENスクエア
営業担当

sales_os@opensquare.co.jp

本日、お伝えしたいこと

オープンソースソフトウェア(OSS)は管理する必要があり、使用しているOSSの正確なリストを作成する必要があります。

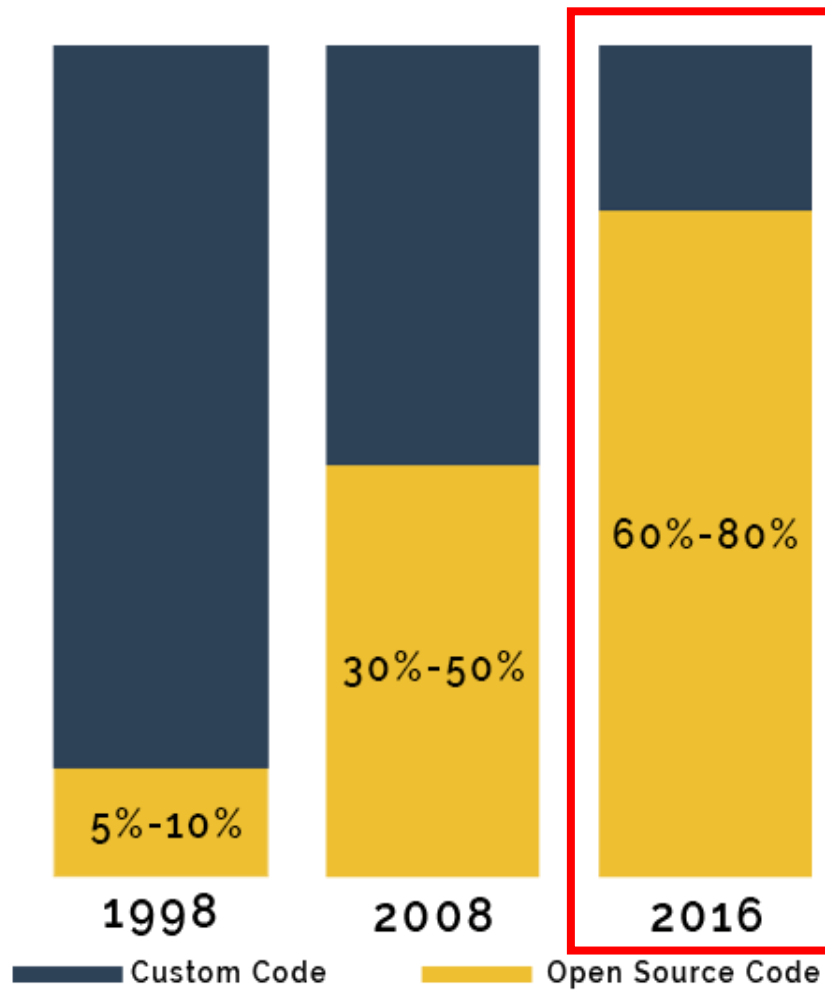
2016年末、米オラクルがJavaを無料で使用している顧客に対し監査を開始し、使用料を請求し始めたというニュースが流れ、多くの利用企業が身じろぎました。

オラクルの Web サイトからダウンロードできる「Java Standard Edition」は、Java アプリケーションを作成するだけなら「無料」です。

しかし、そのアプリケーションを何百ものWindows 環境にインストールするための「Enterprise JRE インストーラ」は無料では使えません。他にも、無料で使用できない Java の要素やエディションがあります。

使用しているOSSを正しく把握していないと「急に使用料を請求される」、「提訴される」こともあるかもしれません。

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

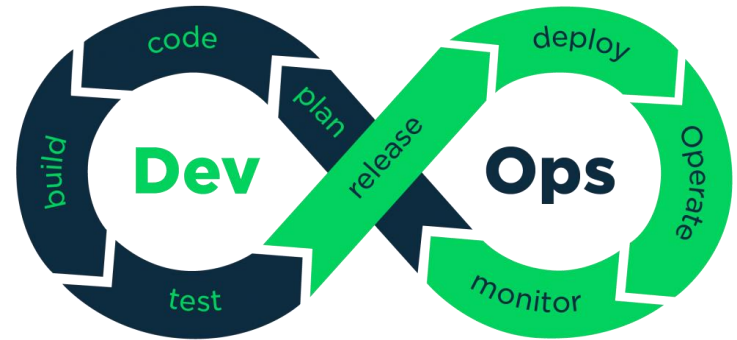


**Forrester developer survey 2015*

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？

オープンソースの主なライセンス種類

ライセンス種類は70以上ありますが、主なものを表にすると、、、

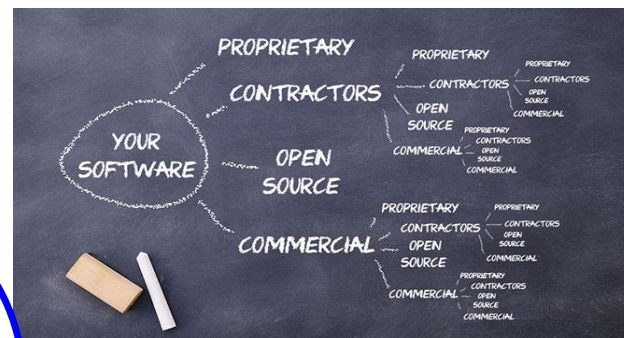
ライセンス	Required(必須)	Permitted(許可)	Forbidden(禁止)
Apache v2	著作権の表示、変更箇所の明示	商用利用、修正、配布、サブライセンス、特許許可	トレードマークの使用、責任免除
GPL v2	著作権の表示、変更箇所の明示、ソースの明示	商用利用、修正、配布、特許許可	責任免除、サブライセンス
MIT	著作権の表示	商用利用、修正、配布、サブライセンス	責任免除
Mozilla Public v 2.0	ソースの明示、著作権の表示	商用利用、修正、配布、サブライセンス、特許許可	責任免除、トレードマークの使用
LGPL v2.1	著作権の表示、ライブラリの使用、ソースの明示	商用利用、修正、配布、サブライセンス、特許許可	責任免除
The BSD 3-Clause	著作権の表示	商用利用、修正、配布、サブライセンス	責任免除、トレードマークの使用
Artistic 2.0	著作権の表示、変更箇所の明示、ソースの明示	商用利用、修正、配布、サブライセンス、個人利用	責任免除、トレードマークの使用
GPL v3	著作権の表示、変更箇所の明示、ソースの明示	商用利用、修正、配布、特許許可	責任免除、サブライセンス
LGPL v3	著作権の表示、ライブラリの使用、ソースの明示	商用利用、修正、配布、サブライセンス、特許許可	責任免除
Affero GPL	著作権の表示、変更箇所の明示、ソースの明示	商用利用、修正、配布	責任免除、サブライセンス
Public Domain	－	個人利用、商用利用、修正、配布、サブライセンス	責任免除
No License	著作権の表示	個人利用、商用利用	修正、配布、サブライセンス
Eclipse Public v1.0	ソースの明示、著作権の表示	商用利用、修正、配布、サブライセンス、特許許可	責任免除
BSD 2-Clause	著作権の表示	商用利用、修正、配布、サブライセンス	責任免除

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.

Google Beats Oracle on Copyright, Defeating \$9 Billion Claim

Oracle vs. Google: The Copyright Case Over Java Code

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

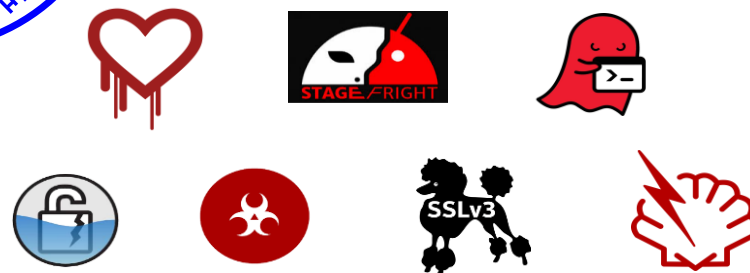
VMware says "Linux is without merit," company is "committed" to open source.

Cisco settles FSF GPL lawsuit, appoints compliance officer

The Free Software Foundation (FSF) has settled its lawsuit against hardware vendor...

③ 法令・規則（ライセンス条項）の順守

② 製品のセキュリティ確保



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
gradle-android-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 udson.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

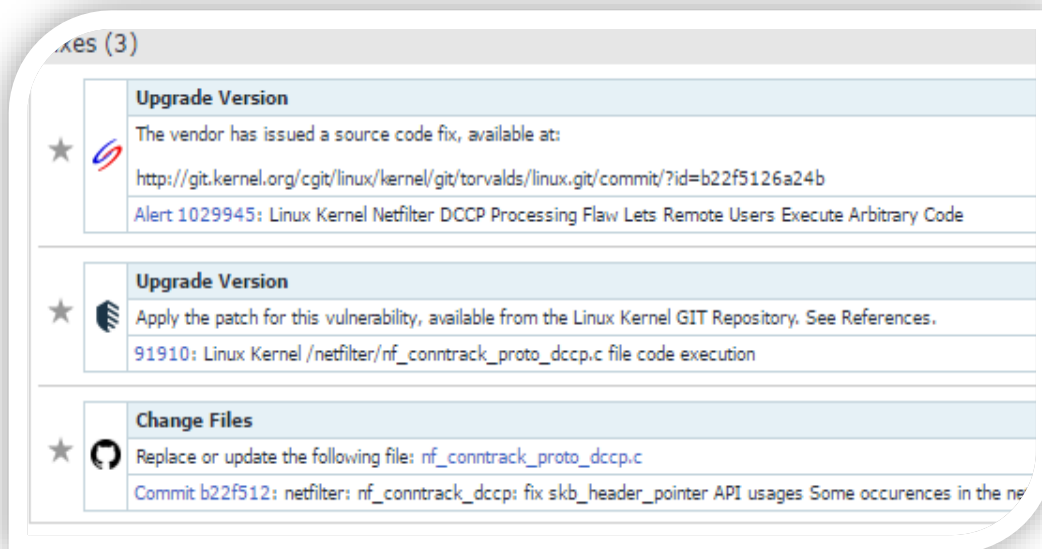
①使用している「モノ」を知る

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

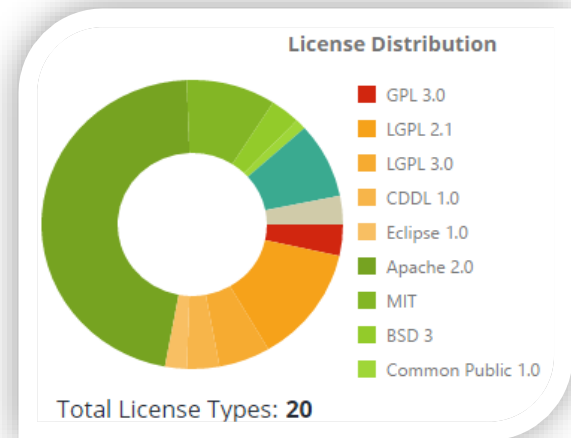
①使用している「モノ」を知る

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

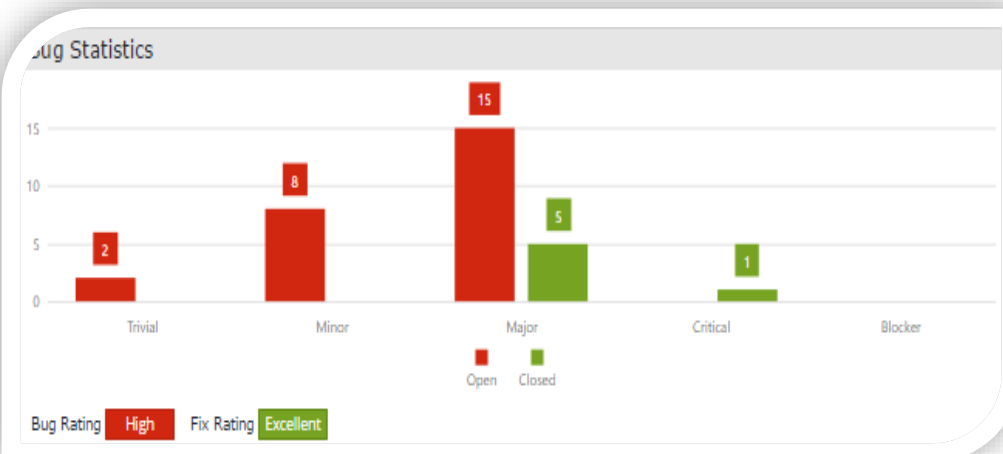
①使用している「モノ」を知る

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

統合可能なツールや環境

Repositories



Build Tools



CI Servers



Jenkins



Issue Trackers



Application Security Testing Tools



全てのプログラミング言語をカバー

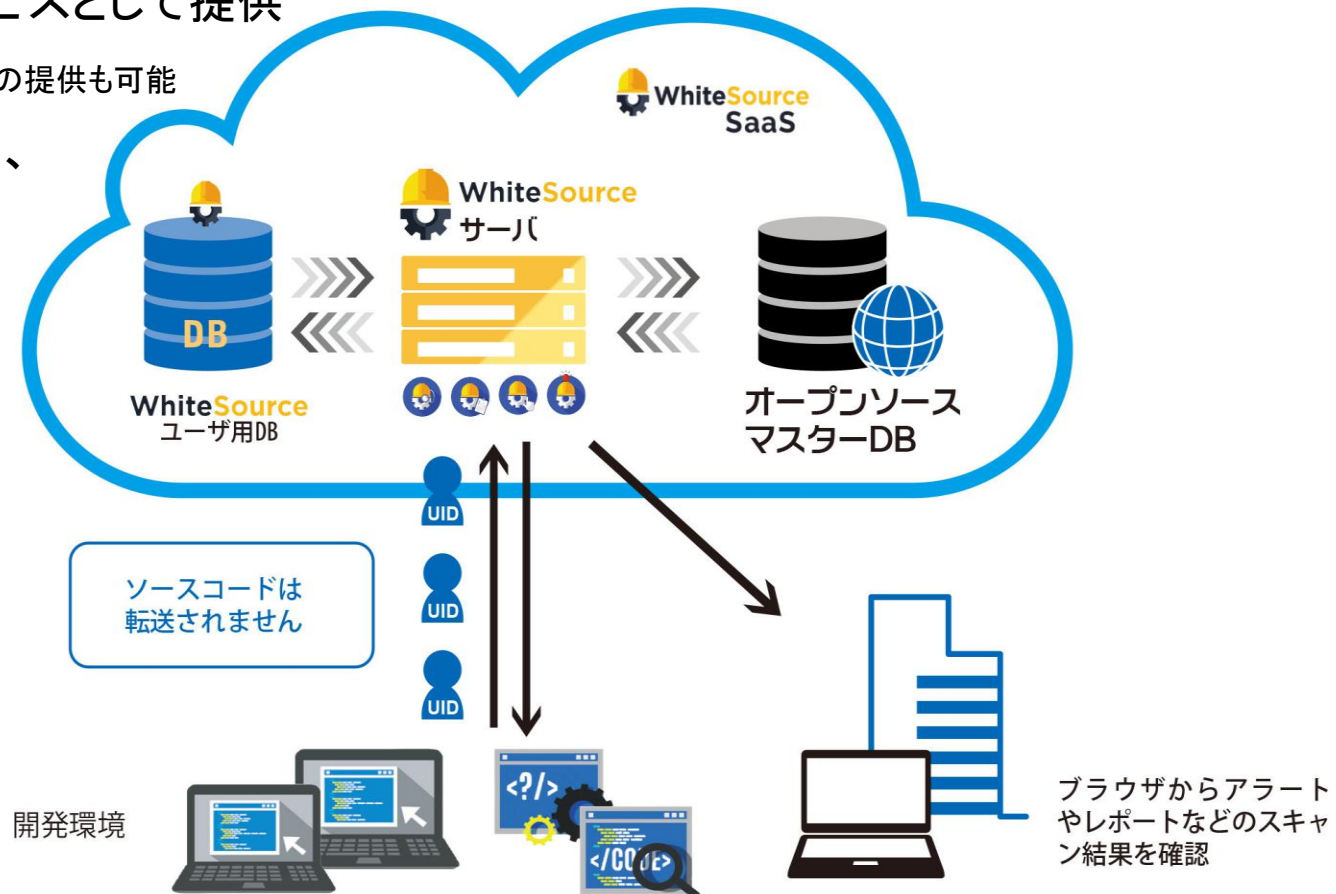


SaaSとしてのサービス提供

- 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。

主要顧客



COMMUNICATION

ENTERPRISE

HEALTHCARE

IOT + EMBEDDED



INTERNET

BANKING & FINTECH

GAMING

SECURITY



WhiteSource の特徴

高精度マッチン手法による脆弱性分析

WhiteSource SaaS

WhiteSource Users Database

WhiteSource Server (WildFly Application Server)

WhiteSource データベース

豊富なデータベース

継続的に12のデータベース、3百万のオープンソースコンポーネント、7千万のオープンソースファイルを監視しています。WhiteSource社のデータベースは競合と比べ、最も豊富なものとなっています。

正確なデータベース

WhiteSource のアルゴリズムは、時間を無駄にするような誤検出がなく、正確なマッチングを行います。競合製品では、多くの誤検出によって無駄な警告が発生し、開発者の時間を浪費してしまいます。

ほとんどのデータベースに対しての実行可能な解決策の提示

WhiteSource はオープンソースコミュニティを基にした実行可能な解決策を、データベースに対し提示します。

開発期間の短縮とコスト削減を達成するツールの選択

開発時ばかりでなく、リリース後も検出。SDLCに組み込む WhiteSource によりシフトレフトを実現。

サービスによる手軽な展開とコストパフォーマンス

コスパ・・・
何よりも重要

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。