

第90回スクエアfreeセミナー



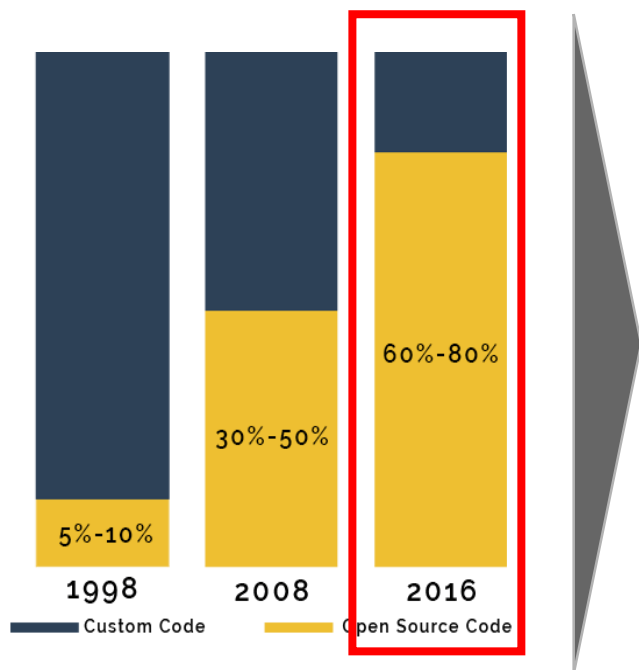
WhiteSourceで実現する オープンソース・マネージメント

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

オープンソースの利用急増！！



オープンソース（OSS）は、ソースコードが公開されていて、簡単に入手できるため、積極的に使われているが、

課題も多い！

- 1 OSS のセキュリティ脆弱性を突かれる事件が絶えない
- 2 OSS のライセンスポリシーは多様。遵守しないと係争も
GPL v2, GPL v3, LGPL v2.1, LGPL v3, Apache v2, Artistic 2.0, Mozilla Public v 2.0, BSD 3-Clause, BSD 2-Clause 等
- 3 バグやアップデート情報がタイムリーに把握できない
- 4 そもそも、どこで、どんなオープンソースが使われているのか把握するのが難しい

ソフトウェアに含まれる
60～80%
のコードはオープンソース

*Forrester developer survey 2015

コンプライアンス:オープンソースの複雑なライセンス

オープンソースにも使用許諾条件があります。著作権、リスク管理の点からの管理が必要です

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

出展 : <https://qiita.com/tukiyo3/items/58b8b3f51e9dc8e96886>

情報セキュリティ強化：日々報告される脆弱性

オープンソースの脆弱性は日々報告されており、この脆弱性がサイバー攻撃のターゲットになります

CVE-2018-7600	Drupalのリモートから任意のコードが実行可能となる脆弱性。この脆弱性を悪用することで、遠隔の第三者が、非公開データを窃取したり、システムデータを改変したりするなどの可能性がある。
JVNDB-2018-002404	ChakraCore および Microsoft Edge には、Chakra スクリプトエンジンのメモリ内のオブジェクト処理に不備があるため、リモートでコードを実行される脆弱性が存在
CVE-2018-7489	FasterXML Jackson-databind には、不完全なブラックリストに関する脆弱性、および信頼性のないデータのデシリアライゼーションに関する脆弱性が存在
CVE-2017-18214 / WS-2017-0422	Node.js 用 moment モジュールには、リソースの枯渇に関する脆弱性が存在
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	WordPressの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

脆弱性の脅威：EQUIFAXで何が起こったのか？

Equifaxが2017年9月7日の発表で、消費者の個人情報が大量に流出していた事実を公表

3月9日

社内メールでStrutsを更新するよう担当者に指示

48時間以内の対応を定めたセキュリティ部門の規定があったにもかかわらず、この時点では社内でStrutsの脆弱性は発見されず、対応も行われなかった。

3月15日

情報セキュリティ部門が脆弱性スキャン実施 スキャンでもStrutsの脆弱性は検出されず

5月13日－7月30日

5月13日にこの脆弱性を突く不正アクセスが初めて発生

7月30日までの間に何度もセンシティブな情報に不正アクセスが発生その時点でEquifaxのセキュリティツールでは不正アクセスを検出できなかった。

7月29日

同社のセキュリティ部門が消費者向けWebサイトに関連した不審なネットワークトラフィックに気付いてこのトラフィックをブロック

7月30日

再び不審な挙動が確認されたことから、問題のWebアプリケーションを完全に停止

9月7日

不正アクセスにより個人情報が流出した可能性のある対象者にメールで通知

参考資料 (IPA発表より)

■「情報セキュリティ 10 大脅威 2018」

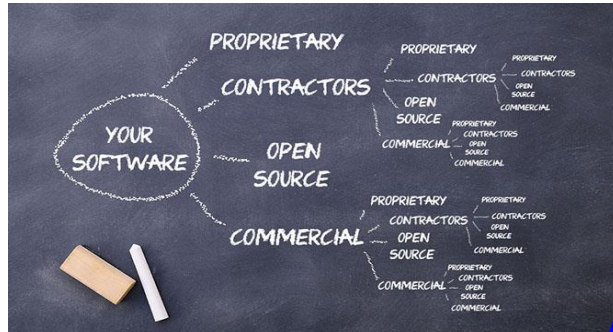
NEW : 初めてランクインした脅威

昨年 順位	「個人」の 10 大脅威	順位	「組織」の 10 大脅威	昨年 順位
1 位	インターネットバンキングや クレジットカード情報の不正利用	1 位	標的型攻撃による情報流出	1 位
2 位	ランサムウェアによる被害	2 位	ランサムウェアによる被害	2 位
7 位	ネット上の誹謗・中傷	3 位	ビジネスメール詐欺 NEW	ランク 外
3 位	スマートフォンやスマートフォン アプリを狙った攻撃の可能性	4 位	脆弱性対策情報の公開に伴い 公知となる脆弱性の悪用増加	ランク 外
4 位	ウェブサービスへの不正ログイン	5 位	セキュリティ人材の不足 NEW	ランク 外
6 位	公開されて脆弱性を突いた攻撃は1日でサイバー攻撃に利用されます。 早期発見、早期対応が重要になります。	6 位	ウェブサービスからの個人情報の窃取	3 位
8 位		7 位	IT 機器の脆弱性の顕在化	8 位
5 位	ワンクリック請求等の不当請求	8 位	内部不正による情報漏えい	5 位
10 位	IoT 機器の不適切な管理	9 位	サービス妨害攻撃による サービスの停止	4 位
ランク 外	偽警告 NEW	10 位	犯罪のビジネス化 (アンダーグラウンドサービス)	9 位

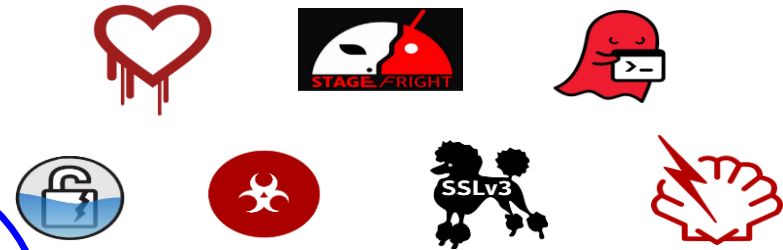
まずは、自社使用しているオープンソースを把握



1 ソフトウェアのどこに、どのオープンソースが使用されているかが、一目瞭然



2 セキュリティ確保のため、脆弱性を持つオープンソースを指摘し、解決策を提示



回避
把握
課題
遵守
確保



4 バグ情報やアップデートを、可能な限り早く知ること、修正にかかる手間・コストを削減

Wix gets caught "stealing" GPL code from WordPress

In which Wix forgets what happens when you add GPL code to your closed source app.
Last Friday, Automatic founder Arvid Kauter—the founding developer of the WordPress open source blogging and content management platform—[sued an open source app for stealing his code](#).

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

by Jack Reardon
May 26, 2016, 1:47 PM EDT
U.S. Judge: Android didn't need Oracle's Java code
Software developer's lawsuit to challenge Google's suit

FSF Files Lawsuit against Cisco on Behalf of the FSP
December 11, 2008

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

VMware says "lawsuit is without merit," company is "committed" to open source.
by [The Free Software Foundation](#) 12/11/08, 3:07 PM

Cisco settles FSF GPL lawsuit, appoints compliance officer

The Free Software Foundation (FSF) has settled a GPL compliance lawsuit with network hardware vendor Cisco.
by [The Free Software Foundation](#) 12/11/08, 3:07 PM

3 法令・規則（オープンソースライセンス条項）の確実な順守

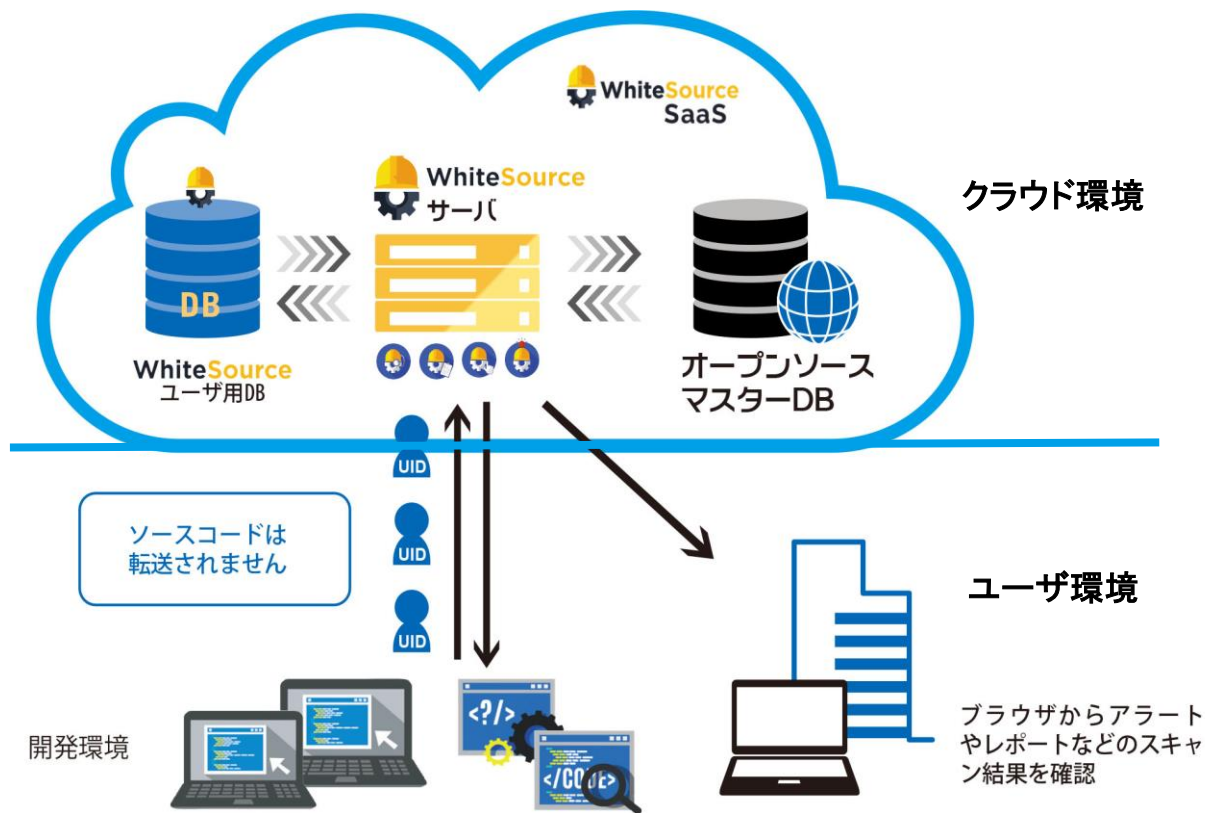


WhiteSource で課題解決

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、ローカルにエージェントもしくは開発環境用プラグインを導入
- エージェントもしくはプラグインがソースコード内、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) を計算して、クラウド環境上の **WhiteSource** サーバに送ります。
- **WhiteSource** ユーザアカウントの情報が更新され、すべての解析レポートがブラウザで利用可能となります。



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。

WhiteSourceのダッシュボード

ブラウザベースの見やすいユーザインタフェース

✓ Security

Vulnerability Score



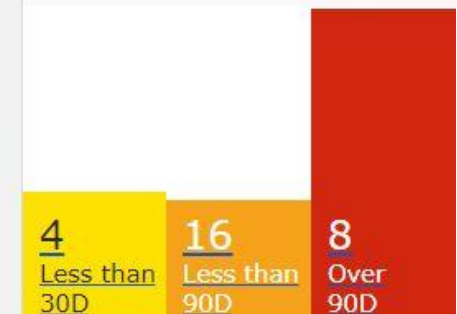
Vulnerable Libraries



Severity Distribution

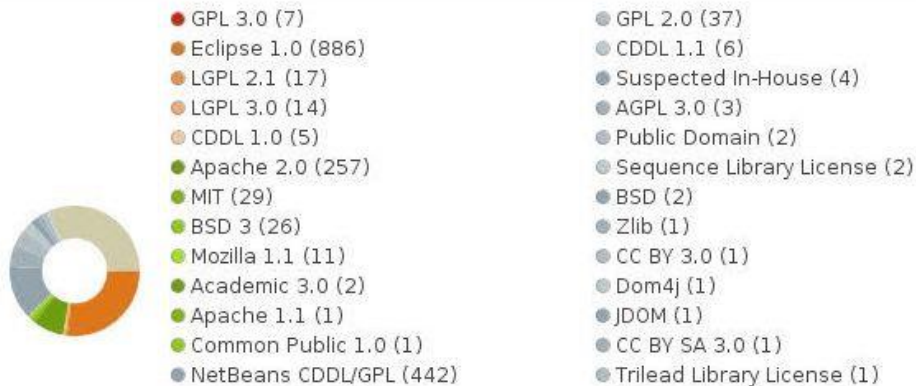


Aging Security Vulnerabilities



⚙ License Risks and Compliance

License Distribution



License Risk Distribution



Outdated Versions



WhiteSource からSAM管理台帳への登録

Libraries (320)			Show as Hierarchy	Actions	Export
☐	Library Name	Description	▲ Licenses		Excel XML
☐	avalon-framework-4.1.3.jar		Apache 1.1		
☐	xpp3-1.1.4c.jar	MXP1 is a stable XmlPull pars...	Apache 1.1, Indiana Universit...		
☐	xml-apis-1.3.02.jar		Apache 2.0		
☐	cloudservers-1.2.1.jar	jclouds components to acces...	Apache 2.0		
☐	commons-httpclient-3.1.jar	The HttpClient component su...	Apache 2.0		
☐	apache-solr-core-3.5.0.jar	apache-solr	Apache 2.0		
☐	commons-cli-1.2.jar	Commons CLI provides a sim...	Apache 2.0		
☐	apache-solr-velocity-3.5.0.jar	apache-solr	Apache 2.0		
☐	maven-toolchain-2.2.1.jar	Maven is a project developm...	Apache 2.0		
☐	cxfr-common-schemas-2.2.7.jar		Apache 2.0		
☐	nekohtml-1.9.6.2.jar		Apache 2.0		
☐	wagon-ssh-common-1.0-beta...	Tools to manage artifacts an...	Apache 2.0		
☐	lucene-core-3.5.0.jar	Apache Lucene Java Core	Apache 2.0		

S

- source code library

P

- pending

R

- rejected



XML形式でのExport

```

?>
0.2.Final.jar</name>
/artifact>
>
d273ecfc9c1743b46bf5d6</sha1>
n Server: Parent Aggregator</description>
e>
atchType>
ctDependency>
/name>
131414d60b5c307aace975</sha1>
- <licenses>
  <license>Apache 2.0</license>
</licenses>
<matchType>Exact Match</matchType>
<directDependency>true</directDependency>
</library>
- <library>

```

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した豊富な脆弱性情報、且つ誤検知無し



- ◆ 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
- ◆ 一般的なビルドツール や CI サーバと 統合可能



- ◆ 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



正確 横断的な
チームをサポート

システム開発ライフサイクル
をフルカバー

統合可能な
多くのツールや環境 全てのプログラミング
言語をカバー 多様な顧客

会社概要

- ・2011年に最初のバージョンをリリース
- ・オープンソースのセキュリティ面におけるマーケット初のソリューション
- ・本社はイスラエル。北米、欧州、アジアでビジネス展開



ご清聴ありがとうございました

いまやアプリケーション開発では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。また、OSSの脆弱性を常に監視し、対処しなければ情報漏えいなどの事故に繋がる可能性があります。

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

WhiteSourceを活用頂くことで、OSSのメリットを活かした効率的なシステム構築の実現をご支援させて頂きたく、宜しくご検討お願い致します。



<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

資料をご覧頂き、ありがとうございました。

END