SYNOPSYS®
Silicon to Software™

ソフトウェア開発におけるOSSライセンス管理のベストプラクティス

日本シノプシス合同会社
ソフトウェア・インテグリティ・グループ
吉井雅人

OSSの利用の広がり

Struts 2

MySQL

zlib

ソフトウェアに含まれるOSS

75%

全コードベースに占める
オープンソースの割合

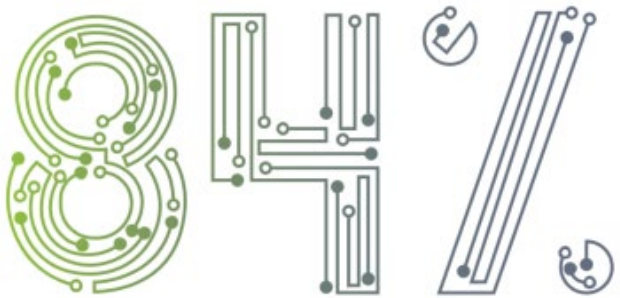
1,546

2020 年に監査した
コードベースの数

出典：2021 年オープンソース・セキュリティ& リスク分析レポート

オープンソースのリスク

脆弱性

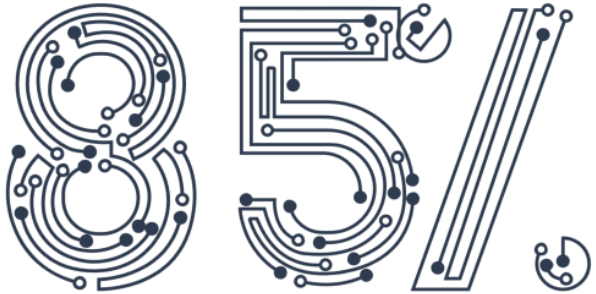


少なくとも1つの脆弱性が見つかったコードベースの割合

ライセンス

ライセンス条件の競合が見つかったコードベースの割合

サステナビリティ



4年以上前のオープンソースコンポーネントを使い続けているコードベースの割合

出典：2021 年オープンソース・セキュリティ& リスク分析レポート

OSSの
ライセンス管理

1. OSSライセンス管理の課題
2. 日本のOSS管理の現状
3. ISO/IEC 5230:2020 OpenChain
4. OSS管理のベストプラクティス

SYNOPSYS®
Silicon to Software™

SYNOPSYS®
Silicon to Software™

OSSの
ライセンス管理

OSSライセンスに対する誤解

誤）OSSは条件なく無償で使える

正）無償で利用できるが、利用するためには条件がある

条件はライセンスによる

ライセンスはソフトウェアの著作権者が決定する

誤）OSSは利用すると訴えられるので使わない

正）条件を守って利用すれば全く問題ない

現在のソフトウエア開発でOSSを使わないということは現実的ではない

著作権者はライセンスを自由に設定できる

ライセンスは、どのようにソフトウェアを利用してほしいか、著作権者の意図を示したもの

```
/*
 * ----------------------------------------------------------------------
 * "THE BEER-WARE LICENSE" (Revision 42):
 * <phk@FreeBSD.ORG> wrote this file. As long as you retain this notice you
 * can do whatever you want with this stuff. If we meet some day, and you think
 * this stuff is worth it, you can buy me a beer in return Poul-Henning Kamp
 * ----------------------------------------------------------------------
 */
```

Copyleftの考え方

- あるプログラムが自由ソフトウェアであるとは、そのプログラムの利用者が、以下の四つの必須の自由を有するときです:

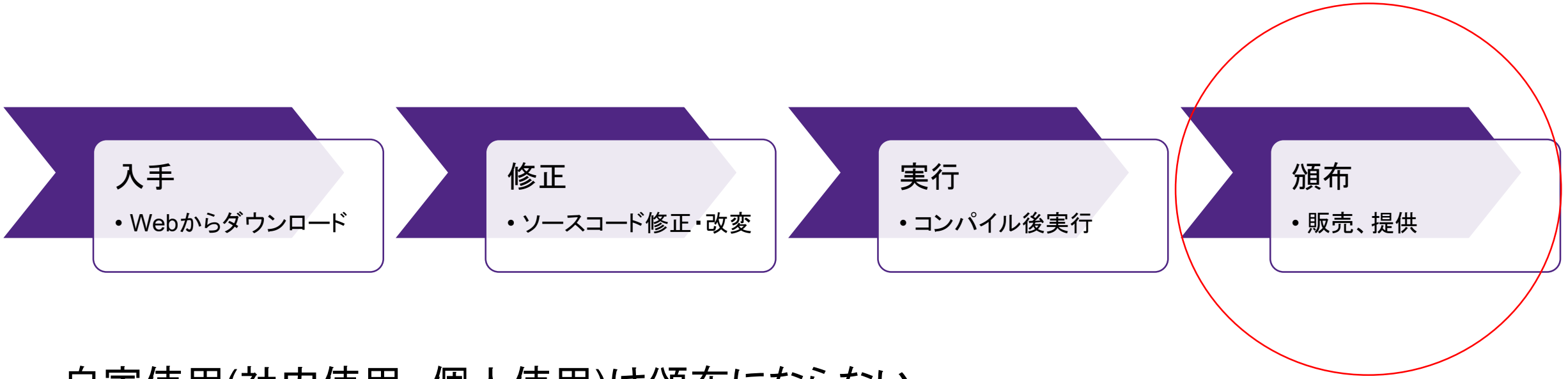
  - どんな目的に対しても、プログラムを望むままに実行する自由（第零の自由）。
  - プログラムがどのように動作しているか研究し、必要に応じて改造する自由（第一の自由）。ソースコードへのアクセスは、この前提条件となります。
  - 身近な人を助けられるよう、コピーを再配布する自由（第二の自由）。
  - 改変した版を他に配布する自由（第三の自由）。これにより、変更がコミュニティ全体にとって利益となる機会を提供できます。ソースコードへのアクセスは、この前提条件となります。

https://www.gnu.org/philosophy/free-sw.ja.html

さまざまなOSSライセンス

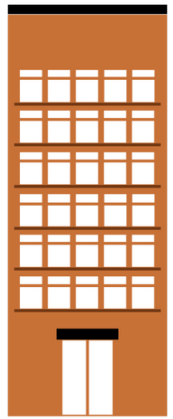
OSSライセンスの類型	代表的なライセンス	利用時にユーザーがしなければならないことの例
Copyleft (コピーレフト)	GPL v2 GPL v3 AGPL	• ライセンステキストの添付 • OSSのソースコードの開示 • OSSを改変した部分のソースコードの開示 • リンクした部分のソースコードの開示
	LGPL v3 LGPL v2.1 MPL 2.0	• ライセンステキストの添付 • OSSのソースコードの開示 • OSSを改変した部分のソースコードの開示
Permissive (寛容型)	BSD 2-clause BSD 3-clause Apache 2.0 MIT License	• ライセンステキストの添付

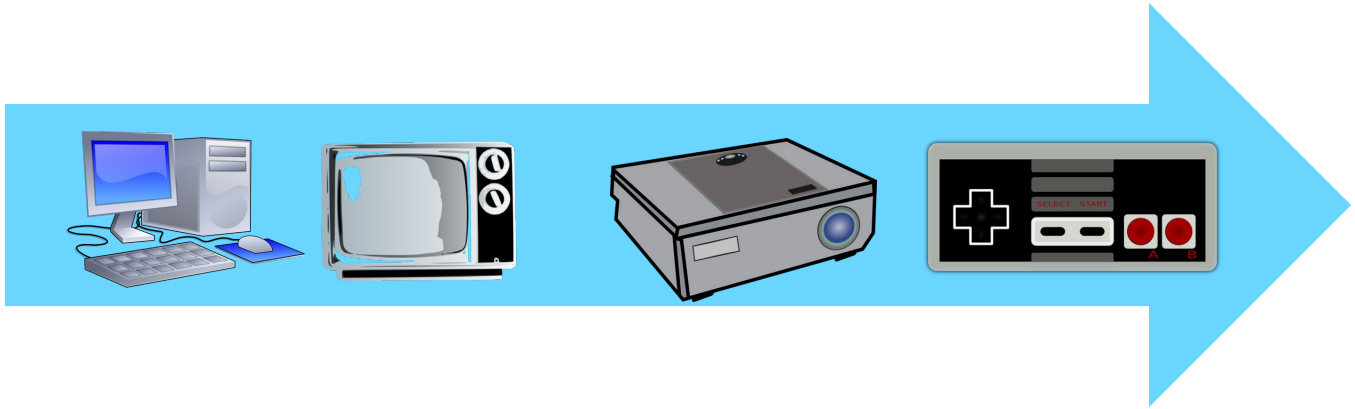
OSSライセンス条件はいつ発動するのか



- 自家使用(社内使用、個人使用)は頒布にならない

頒布の例) 製品の販売、ダウンロード





ここ数年で見られるようになったライセンスの問題

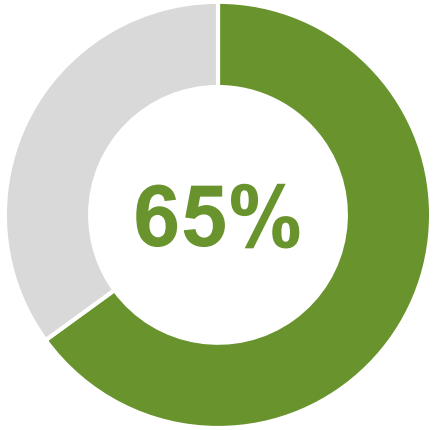
- ライセンスの文言が客観的ではない
  - Hippocratic License

    「誰であれ、このソフトウェアを国連世界人権宣言に反して他の個人や団体の身体的、精神的、経済的、または全体的福祉を積極的かつ意図的に危険にさらしたり、害したり、その他の方法で脅かすようなシステムや活動に使用してはならない」という文言を含むライセンス。

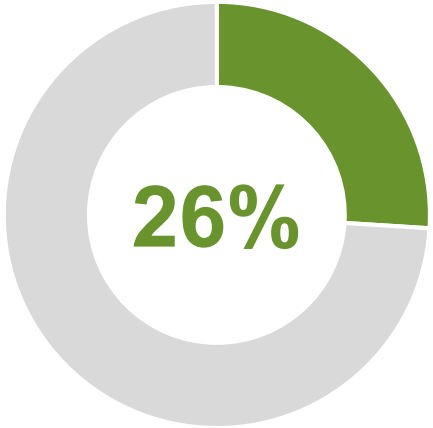
  - 以前から存在する JSON License「このソフトウェアは善い目的に使用されるべきで、邪悪な目的に使用してはならない」と同様の問題

- ライセンスが設定されていない
  - ライセンスが無いので自由に使えるというわけではない
  - どのように使えばよいかが記述されていないので、利用できない

OSSライセンスリスクの推移



ライセンス競合の可能性があるコードベースの割合



「ライセンスなし」またはカスタム・ライセンスのコンポーネントを含むコードベースの割合

出典：数字で見るM&A のオープンソース・リスク

OSSの
ライセンス管理

1 OSSライセンス管理の課題

ライセンス条件を理解する必要がある

SYNOPSYS®
Silicon to Software™

OSSの
ライセンス管理

1 OSSライセンス管理の課題

ライセンス条件を理解する必要がある

2 日本のOSS管理の現状

SYNOPSYS®
Silicon to Software™

OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集

https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html

経済産業省
Ministry of Economy, Trade and Industry

申請・お問合せ | English | サイトマップ | 本文へ | 文字サイズ変更 小 中 大 | アクセシビリティ閲覧支援ツール

ニュースリリース | 会見・談話 | 審議会・研究会 | 統計 | 政策について | 経済産業省について

ホーム ▶ ニュースリリース ▶ ニュースリリースアーカイブ ▶ 2021年度4月一覧 ▶ オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました

English | 印刷

オープンソースソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集を取りまとめました

2021年4月21日

▶ ものづくり/情報/流通・サービス

経済産業省では、オープンソースソフトウェア（OSS）を利活用するに当たって留意すべきポイントを整理し、そのポイントごとに参考となる取組を実施している企業の事例等をとりまとめた「OSSの利活用及びそのセキュリティ確保に向けた管理手法に関する事例集」を公開します。

1. 背景・趣旨

経済産業省では、令和元年9月5日に産業サイバーセキュリティ研究会ワーキンググループ1 （WG1）分野横断サブワーキンググループの下に、サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース（ソフトウェアタスクフォース）を設置し、適切なソフトウェアの管理手法、脆弱性対応やライセンス対応等について検討を行ってきました。

キーワード

- サプライチェーン
- 教育
- 組織体制
- 管理プロセス
- OpenChain
- OSS管理ツール

など

表 1：掲載事例一覧

商流	ステークホルダ	事例企業	事例に関連する観点							
			選定評価	ライセンス	脆弱性対応	保守・品質保証	サプライチェーン管理	個の能力・教育	組織体制	コミュニティ活動
ヒアリング実施企業										
製品商流	最終製品メーカー	トヨタ自動車		○			○			○
		ソニー		○	○		○		○	○
		オリンパス		○			○	○	○	○
		日立製作所		○						○
		オムロン			○		○	○	○	
		東芝	○	○	○	○			○	○
	サプライヤ	デンソー		○	○		○			
製品商流＆SIer 商流	SIer&最終製品メーカー	富士通	○	○	○	○	○	○	○	○
		日本電気（NEC）	○	○						

https://www.meti.go.jp/press/2021/04/20210421001/20210421001.html

頒布という行為が発生する業種

- IoT/組み込み機器
- 自動車
- ゲーム
- モバイルアプリ
- パッケージソフト

特に組み込み機器はLinuxベースの開発が多い

Linux KernelはGPL v2

ライセンスを意識せざるを得ない

頒布という行為が発生しづらい業種

ライセンスよりは、OSSの脆弱性を意識する傾向がある

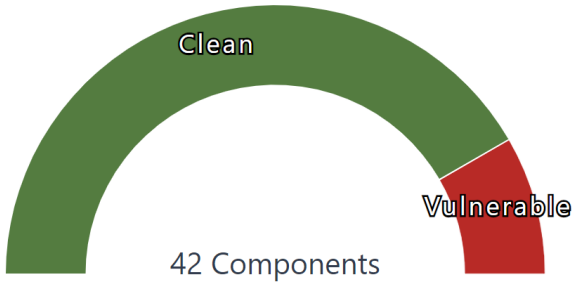
- SIer
  - ソフトウェアの納品は通常頒布とはみなされない
  - 頒布行為が発生しない ＝ ライセンス条件が発動しない

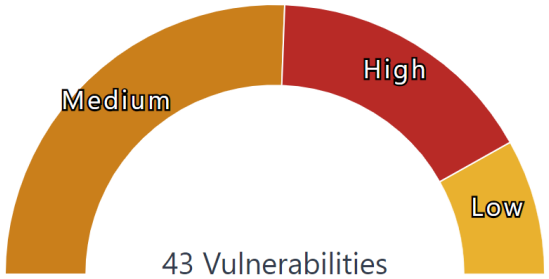
- SaaSでサービスを提供する企業
  - 同様に頒布行為が発生しない
  - 唯一例外的に意識をしないといけないのはAGPLというライセンス(SaaS形式の利用も頒布とみなす)
  - モバイルアプリを提供していれば、それは頒布行為が発生するため、当然OSSライセンスを意識する

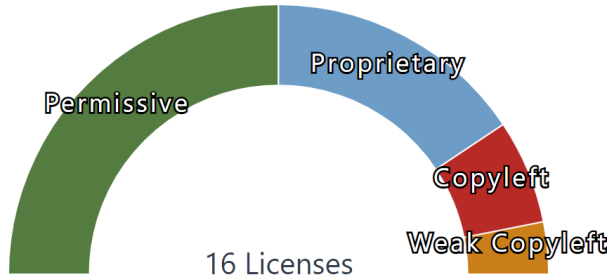
Android ゲーム売り上げトップ20ではどのようなOSSが利用されているのか 3年間の変化を見てみる

apkファイルを解析

Vulnerability analysis | Information leakage | Mobile apps | Feed | Details







Components	42
Vulnerable	7
No known vulnerabilities	35

Vulnerabilities	43
High	14
Medium	22
Low	7

Licenses	16
Permissive	8
Weak Copyleft	1
Copyleft	2
Proprietary	5

CVSS v2 ratings

High 7.0 - 10.0 | Medium 4.0 - 6.9 | Low 0.0 - 3.9 | Clean | Triaged | Historical

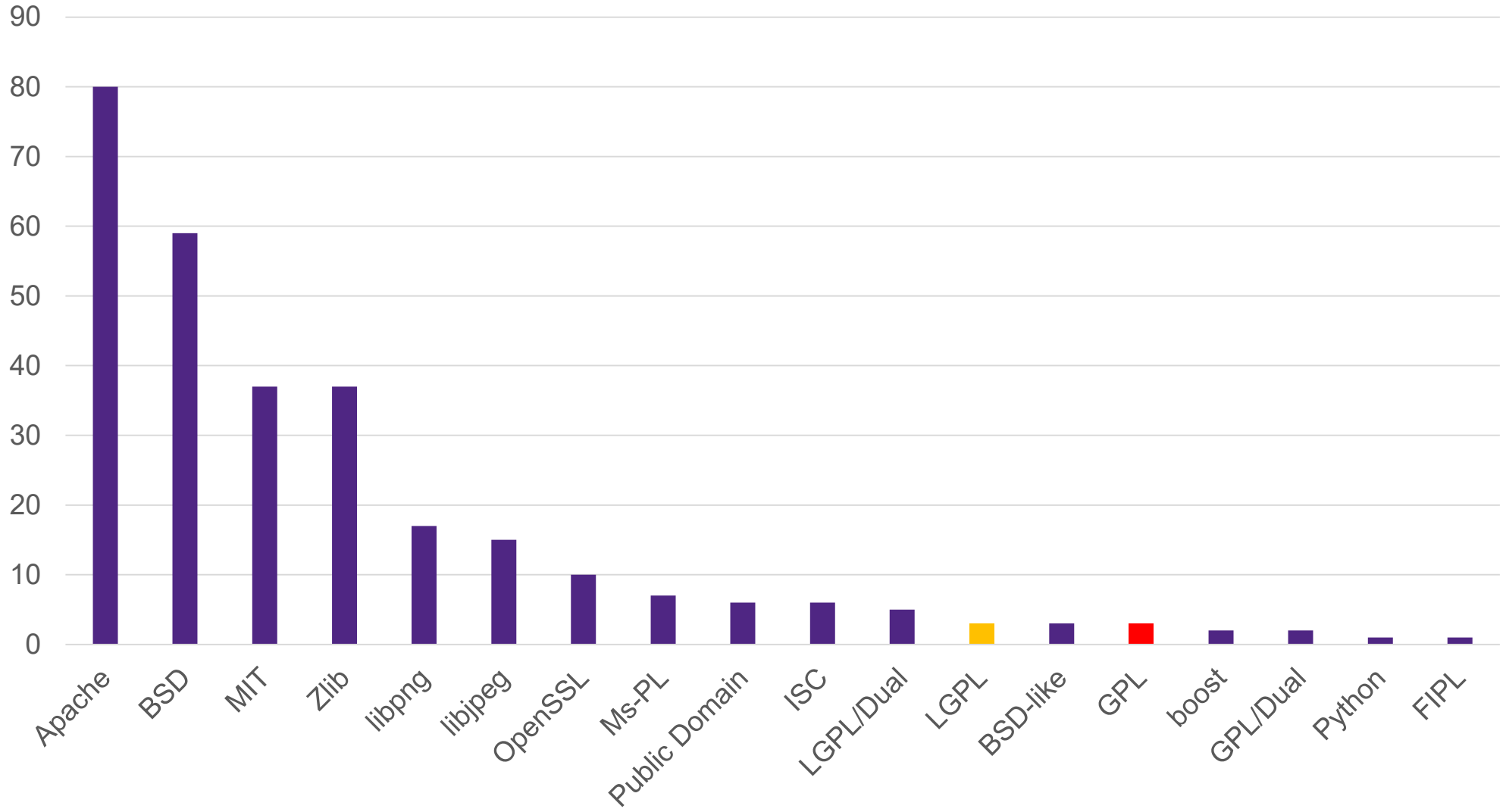
Group by: version | Filters: 0 selected | Sort by: vulns

Components (42)

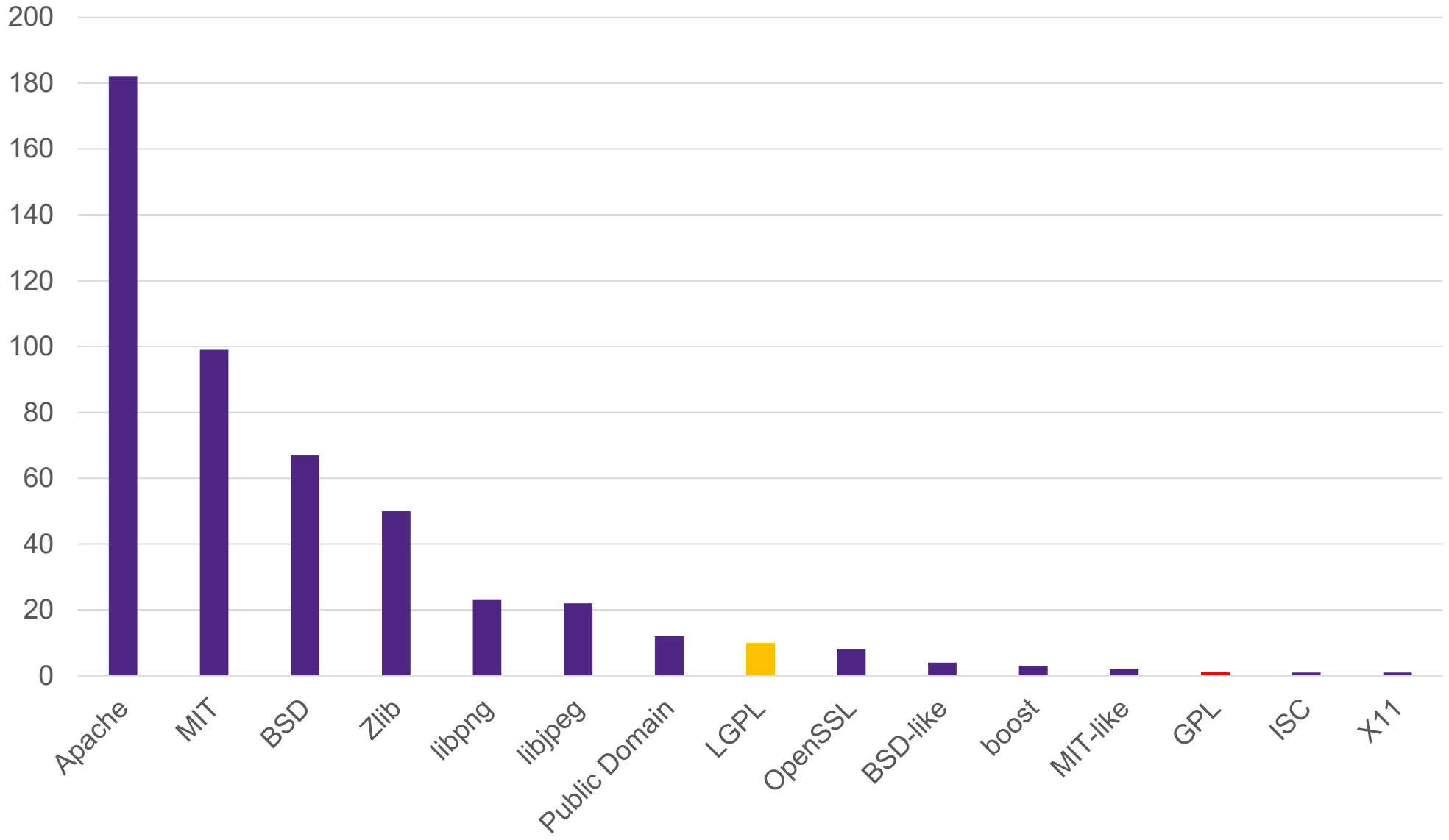
Vulnerabilities (43)

sqlite3 3.7.17	8 7 6 0 25
expat 2.1.0 2 FILES	3 6 0 0 6
zlib 1.2.3.3 2 FILES	2 2 0 0 5

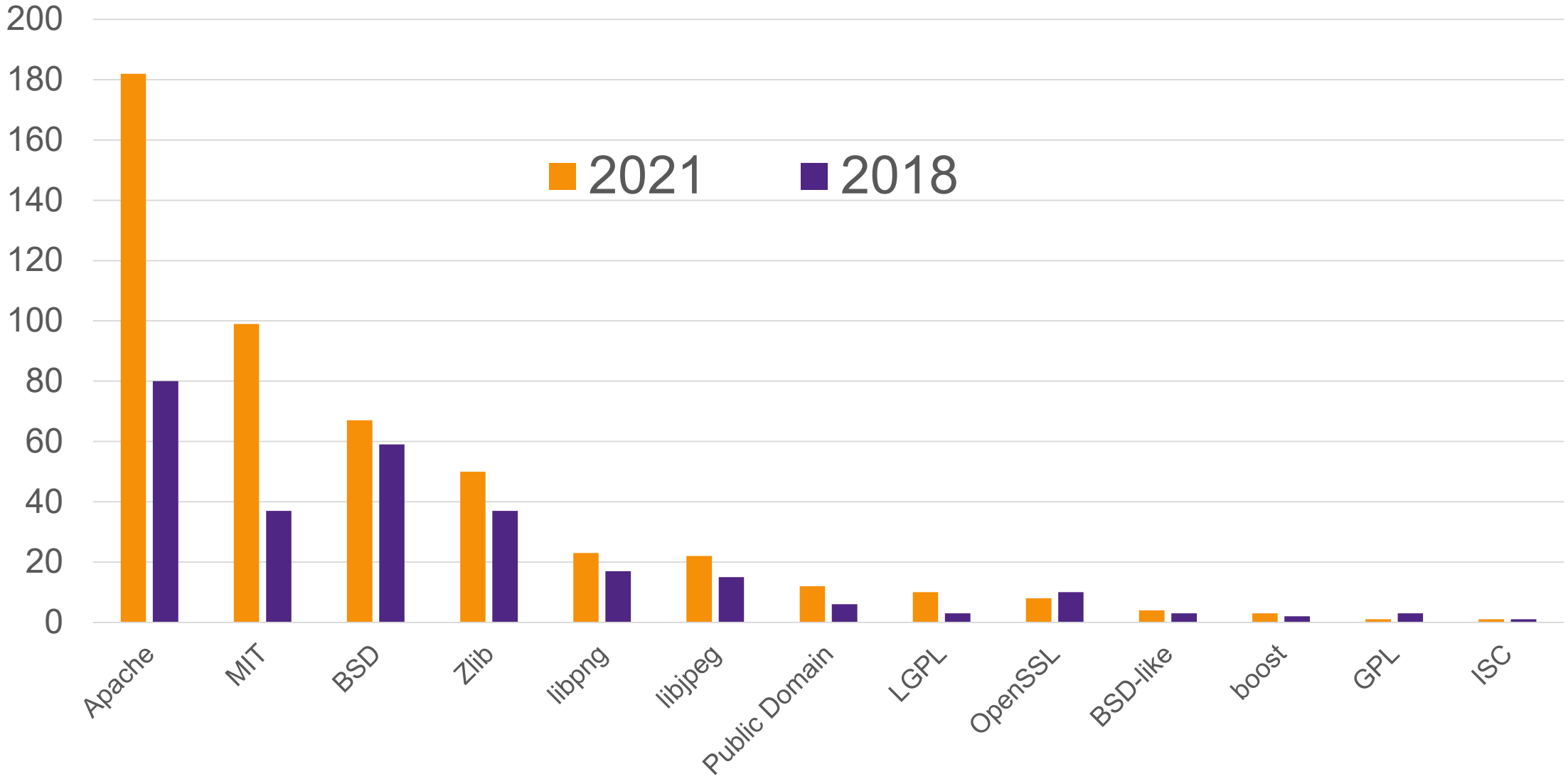
2018年に Top 20 Appで利用されていたOSSのライセンス



2021年に Top 20 Appで利用されていたOSSのライセンス



2018年と2021年の比較



3年間の変化

- 1アプリあたりのオープンソースコンポーネントの数
  - 14.7→24.25
- 特にApache License、MIT Licenseが適用されているオープンソースコンポーネントの利用が2倍以上
- Top 6のライセンスに変更なし
- Permissiveなライセンスの利用が多い
- LGPLのOSSの利用は増加
- 2021年もGPLを利用しているアプリはある

OSSの利用がさらに進んでいる

OSSをきちんと管理しているメーカーがほとんどだが、そうでないところも未だにある

OSSの
ライセンス管理

1 OSSライセンス管理の課題

ライセンス条件を理解する必要がある

2 日本のOSS管理の現状

業種によってコンプライアンス重視

SYNOPSYS®
Silicon to Software™

OSSの
ライセンス管理

1. OSSライセンス管理の課題
   - ライセンス条件を理解する必要がある
2. 日本のOSS管理の現状
   - 業種によってコンプライアンス重視
3. ISO/IEC 5230:2020 OpenChain

SYNOPSYS®
Silicon to Software™

ISO/IEC 5230:2020 OpenChain 主要箇所

3.1.1 Policy
3.1.2 Competence
3.1.3 Awareness
3.1.4 Program Scope
3.1.5 License Obligations

3.2.1 Access
3.2.2 Effectively Resourced

3.3.1 Bills of Material
3.3.2 License Compliance

3.4.1 Compliance artifacts
3.5.1 Contributions

3.6.1 Conformance
3.6.2 Duration


INTERNATIONAL STANDARD

ISO/IEC 5230

First edition
2020-12

Information technology — OpenChain Specification

3.1 Program foundation

- 3.1.1 Policy
  - 文書化されたオープンソースポリシー
  - プログラムの参加者にオープンソースポリシーを認識させる

- 3.1.2 Competence
  - 役割と責任を明確化
  - 役割と責任に対して能力があることを確認する
  - 教育、トレーニングなど

3.1 Program foundation (続き)

- 3.1.3 Awareness
  - オープンソースポリシーを認識していることを確認
  - Awarenessの向上を図る

- 3.1.4 Program Scope
  - プログラムの範囲と制限を定義
  - 組織によってスコープは異なるため

- 3.1.5 Obligation
  - 特定されたライセンスについて、義務や制限、権利を明確にする

3.2 Relevant tasks defined and supported

- 3.2.1 Access
  - 第三者のオープンソースコンプライアンスの問い合わせに効果的に対応する
  - 組織として対応できるか

- 3.2.2 Effectively Resourced
  - 説明責任の割当て
  - プログラムが効果的に実行されるため、リソース、予算、時間が与えられていること

3.3 Open source content review and approval

- 3.3.1 Bills of Material
  - SBOM(Software Bill of Materials)の作成、管理
- 3.3.2 License Compliance
  - オープンソースのユースケース
    - オープンソースを変更したか
    - バイナリ形式で配布するか
    - ソースコード形式で配布するか

3.4 Compliance artifact creation and delivery

- 3.4.1 Compliance artifacts
  - コンプライアンス関連資料
  - ソースコード
  - ビルドおよびインストールスクリプト
  - ライセンスのコピー
  - 著作権表示など

3.5 Understanding open source community engagements

- 3.5.1 Contributions
  - オープンソースプロジェクトに対する貢献を検討している場合のポリシー、手順など

3.6 Adherence to the specification requirements

- 3.6.1 Conformance
  - 適合性の確認
  - この文書のすべての要件を満たすこと
- 3.6.2 Duration
  - 有効期間は適合性の検証が取得された日から18か月間

シノプシスもOpenChainの第三者認証を提供

https://www.synopsys.com/blogs/software-security/openchain-project-third-party-certification/

Announcing Synopsys as an OpenChain Project third-party certifier

Posted by Jacob Wilson on Friday, June 4th, 2021

Synopsys can measure the maturity of security activities within an open source management framework in compliance with the OpenChain standard and ISO/IEC 5230:2020.

OSSの
ライセンス管理

1. OSSライセンス管理の課題
   - ライセンス条件を理解する必要がある
2. 日本のOSS管理の現状
   - 業種によってコンプライアンス重視
3. ISO/IEC 5230:2020 OpenChain
   - ポリシー、プロセスが重要

SYNOPSYS®
Silicon to Software™

OSSの
ライセンス管理

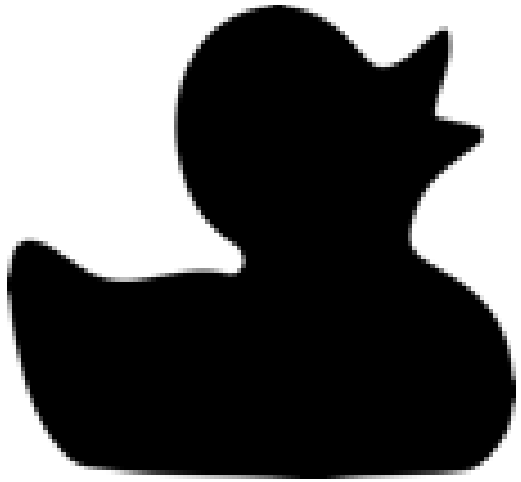
1. OSSライセンス管理の課題
   - ライセンス条件を理解する必要がある
2. 日本のOSS管理の現状
   - 業種によってコンプライアンス重視
3. ISO/IEC 5230:2020 OpenChain
   - ポリシー、プロセスが重要
4. OSS管理のベストプラクティス

SYNOPSYS®
Silicon to Software™

Black DuckによるSBOM作成

様々な手法によりSBOMを自動的に作成

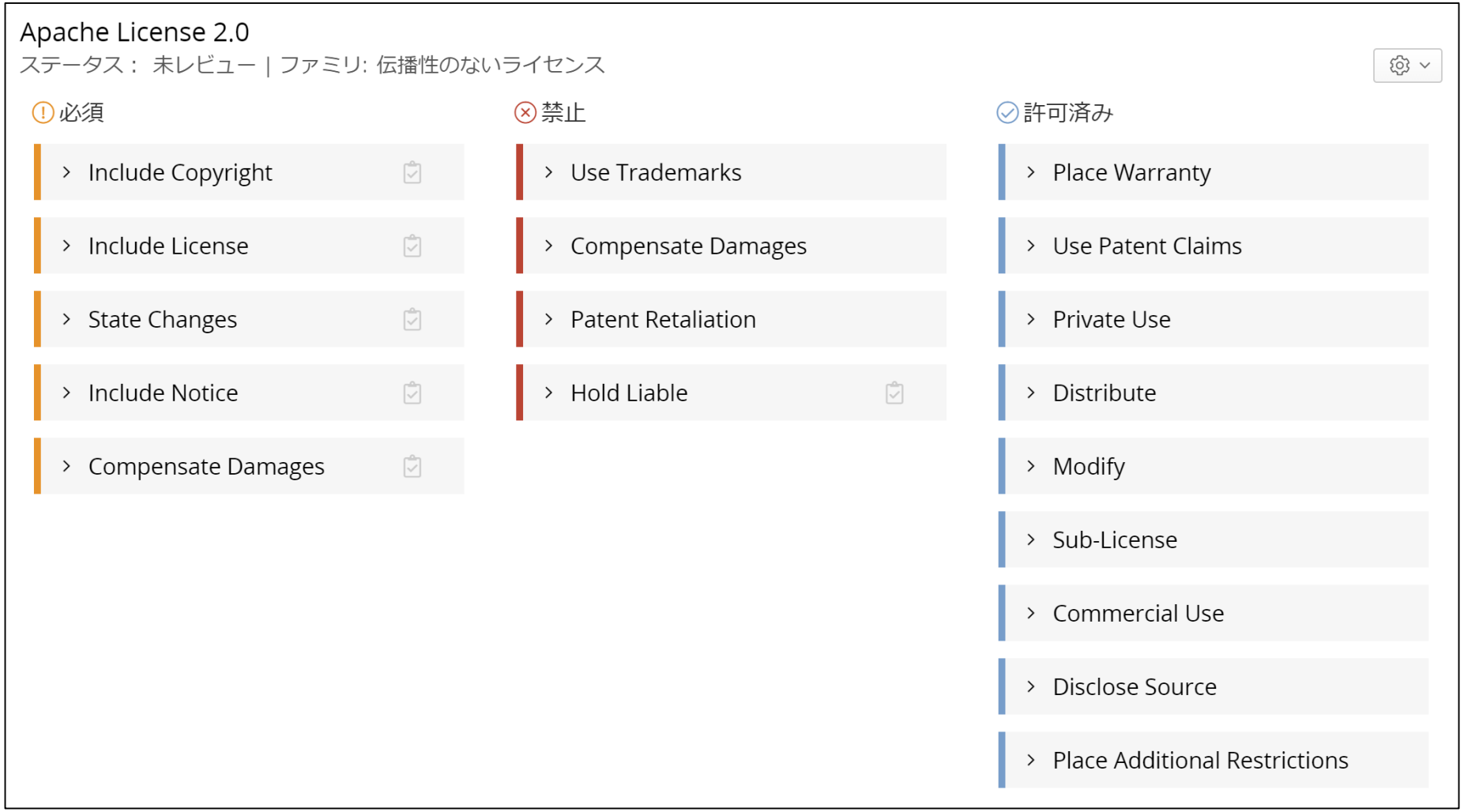
- ディレクトリ構造、ファイル
- 依存関係、パッケージマネージャー
- バイナリ解析



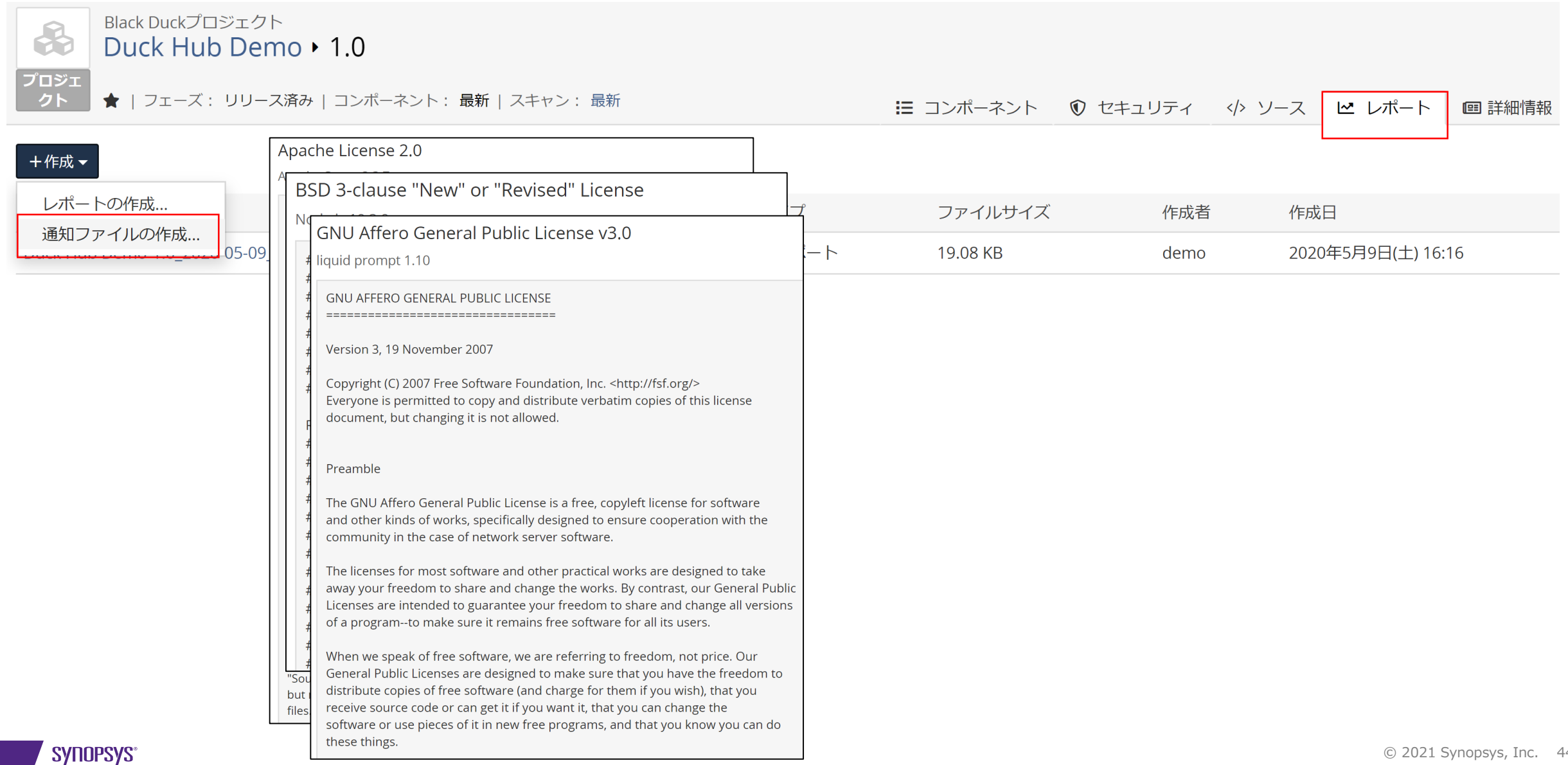
ライセンスリスクが高いOSSコンポーネントを抽出

プロジェクト設定の配布属性によってライセンスリスクを自動的に変更

ライセンスが要求していること、ライセンスによって禁止されていることを容易に把握



Notice Fileを自動的に作成



Black Duckで実現するOSS管理

設計 → 開発 → テスト → リリース

- 設計の段階で、利用を計画しているOSSのライセンスを事前にチェック
- 開発の段階では、日々追加されるソースコードとライブラリを自動的にチェック
- ソフトウェアが完成した段階では、手戻りなく自動的にポリシーに沿ったOSSのみ利用
- Noticeファイルなどを自動的に作成

OSSの
ライセンス管理

1. OSSライセンス管理の課題
   - ライセンス条件を理解する必要がある
2. 日本のOSS管理の現状
   - 業種によってコンプライアンス重視
3. ISO/IEC 5230:2020 OpenChain
   - ポリシー、プロセスが重要
4. OSS管理のベストプラクティス
   - 効率的にOSSを管理

SYNOPSYS®
Silicon to Software™

OSSのライセンス管理のために必要なこと

- OSS利用ポリシー、プロセスの策定
- OSSライセンス教育・トレーニング
- SBOMの作成。Black Duckで自動化するとより効果的

自社の業種業態にあわせたリスクの特定
開発者のリテラシーを向上させることが、リスクを軽減することに繋がる
後の工程になるほど、違反を検出した場合のインパクトは大きい

SYNOPSYS®
Silicon to Software™

Q&A


SYNOPSYS®
Silicon to Software™