

Linux/OSSを製品適用する際の7つのポイント

2020 Nov

富士通コンピュータテクノロジーズ

浅羽 鉄平



\$ whoami

- 名前: 浅羽 鉄平 (あさば てっぺい)
- 所属: 富士通コンピュータテクノロジーズ
- 仕事: 組込みシステム向けLinuxディストリビューションのメンテナンス。最近はLinuxであれば、「組込み」と付けなくてもよいのではと思う今日この頃。
- 好きなライセンス: GPL-3.0



The names of products are the product names, trademarks or registered trademarks of the respective companies. Trademark notices ((R),TM) are not necessarily displayed on system names and product names in this material.

こんな経験ありませんか？

開発中の製品に仕様が追加された。

実現方法をWebで調べていたら、あるOSSが見つかった。

そのOSSを製品に組み込めばOK!?

こんな経験ありませんか？

OSSを製品適用する際に意識すべき
ポイントを解説します。

0. 願望

動作環境が異なるアプリケーションを複数動かしたい

1. 方式を検討

VM or コンテナ

セキュリティ？
オーバーヘッド？
フットプリント？

KVM or Xen or seL4...

2. 実装レベルで検討

systemd or LXD or runc...

ゲスト間通信？
リソース共有？
オーケストレーション？

3. 静的評価で候補を絞る

4. 動的評価でパッケージを決定

5. 採用パッケージのバージョンを決定

2.実装レベルで検討

■ 必要な機能を満たしているか評価

機能\実装	要件	systemd (nspawn)	LXC	LXD	runC	Kata
セキュリティ	✓					
オーバーヘッド	✓					
フットプリント						
アイソレーション	✓					
ゲスト間通信						
リソース共有	✓					
ライブマイグレーション	✓					
オーケストレーション	✓					

3. 静的評価で候補を絞る

■ コミュニティの健全性を評価

➤ Open Hub

<https://www.openhub.net/>

➤ 社内のOSS評価情報共有サイト

➤ リポジトリ

➤ NATIONAL VULNERABILITY DATABASE (脆弱性サーチ)

<https://nvd.nist.gov/vuln/search>

ケーススタディ①: cups

The screenshot shows the Open Hub project page for CUPS. The page header includes the project name 'Common Unix Printing System (CUPS)' and a 'Moderate Activity' badge. A red circle highlights the '1,057' user count badge, with a callout bubble containing the text 'アクティビティユーザー数'. Another callout bubble points to the 'Moderate Activity' badge with the text '似たソフトウェアで検討漏れがないか'. The page content includes a project summary, a 'In a Nutshell' section with commit statistics, and a 'Quick Reference' section with project links and managers.

Project Summary

CUPS provides a portable printing layer for Unix(r)-based operating systems. It has been developed to promote a standard printing solution for all Unix vendors and users. CUPS provides the System V and Berkeley command line interfaces, and uses the Internet Printing Protocol ("IPP") as the basis for managing print jobs and queues. The Line Printer Daemon (LPD) Server Message Block (SMB), and AppSocket (a.k.a. JetDirect) protocols are also supported with reduced functionality. CUPS adds network printer browsing and PostScript Printer Description ("PPD") based printing options to support real world printing under UNIX. It includes an image file RIP that supports printing of image files to non-PostScript printers. A customized version of GNU Ghostscript 7.05 for CUPS called ESP Ghostscript is

Tags

desktop_environment documentation git Hardware installation linux networking disk print

In a Nutshell, Common Unix Printing System (CUPS)...

- has had 1,376 commits made by 50 contributors representing 208,148 lines of code
- is mostly written in C with an average number of source code comments
- has a well established, mature codebase maintained by a very large development team with increasing Y-O-Y commits
- took an estimated 53 years of effort (COCOMO model) starting with its first commit in January, 2006 ending with its most recent commit 6 days ago

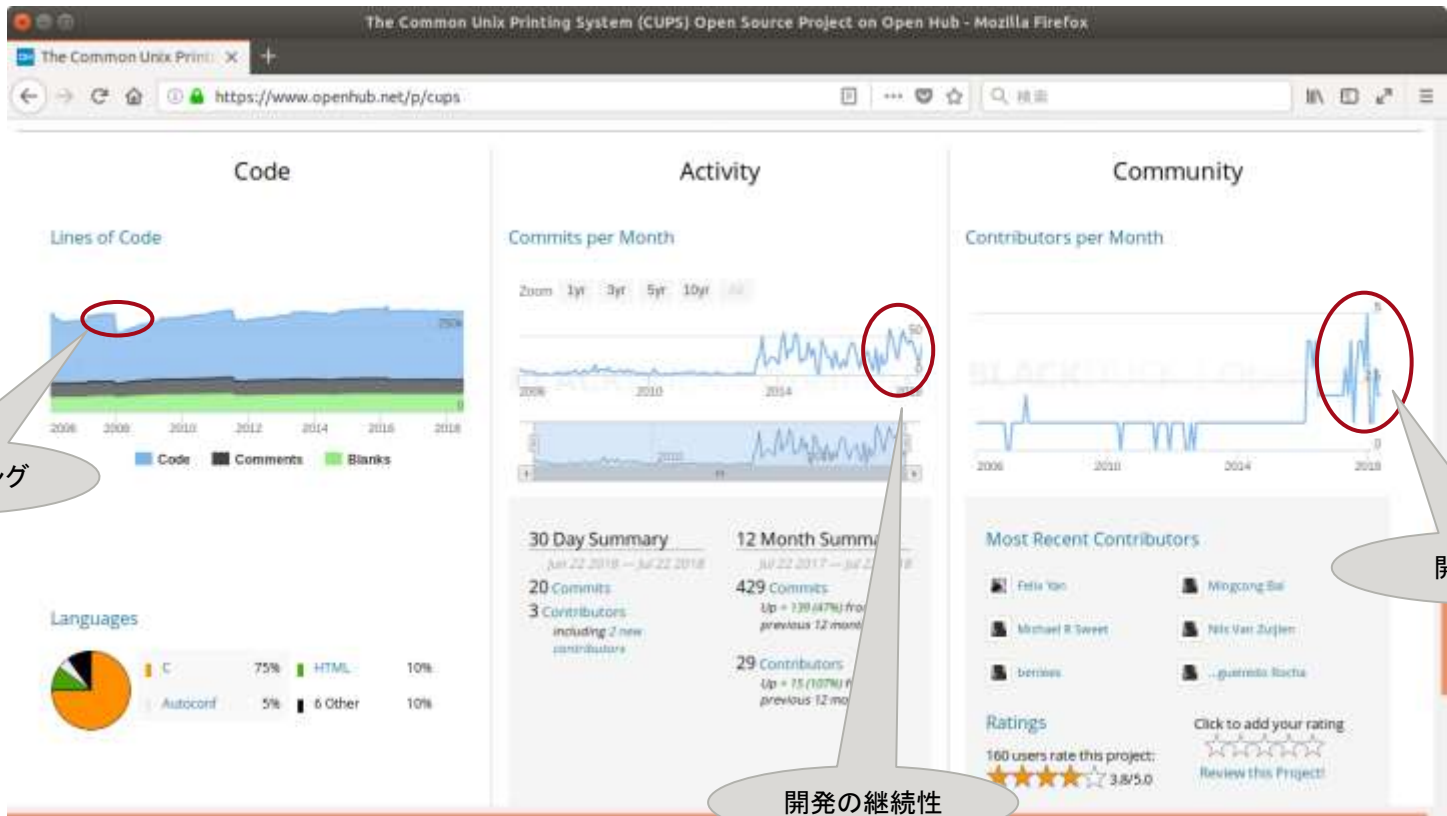
Quick Reference

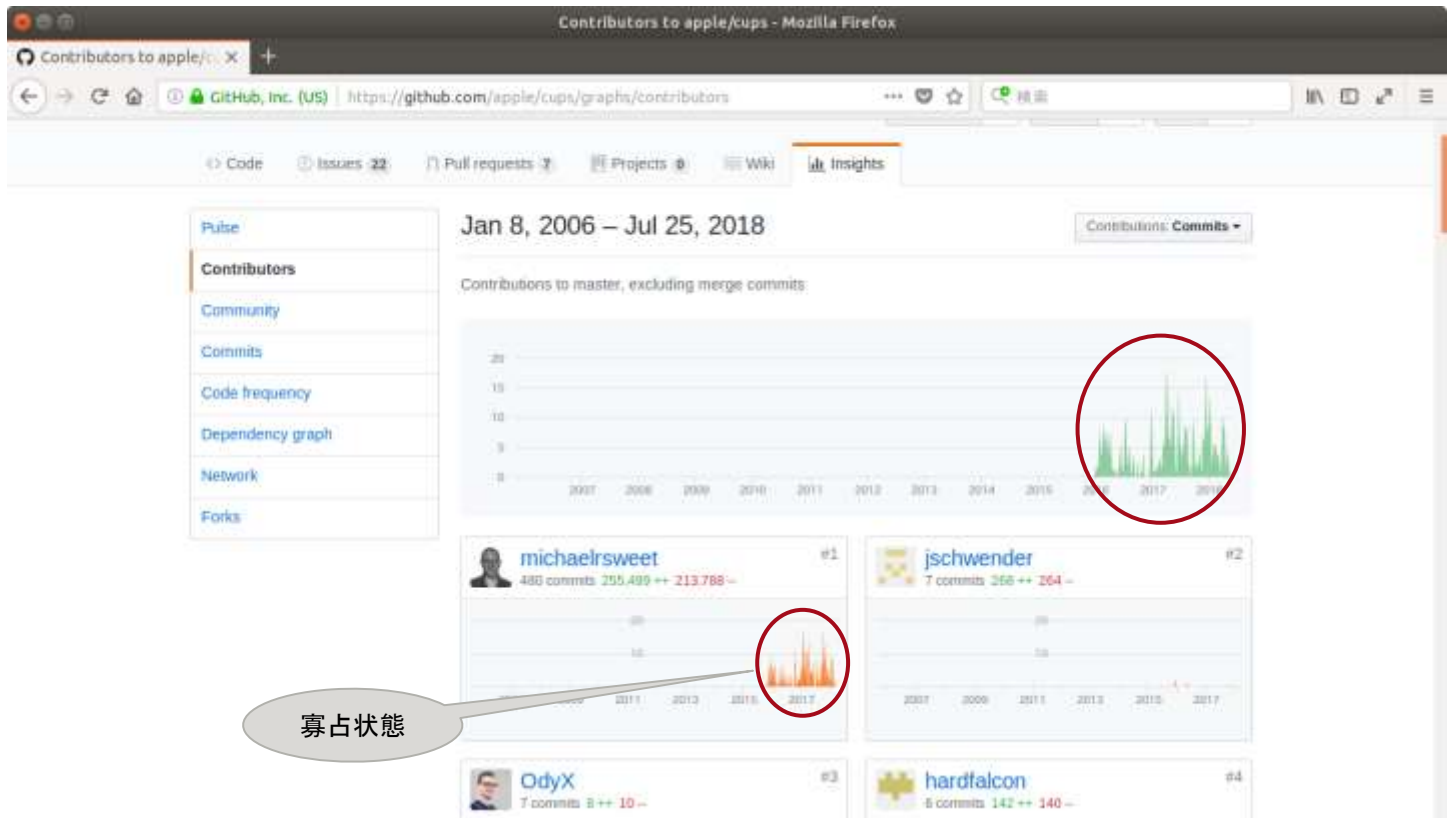
Project Links: [Homepage](#)

Code Locations: [git://github.com/apple/cups.git](#)

Similar Projects: [Bifrost Print...](#) [Project 6224](#)

Managers: [Become the first manager for Common Unix Printing System \(CUPS\)](#)





The screenshot shows a Mozilla Firefox browser window displaying the GitHub profile of Michael R Sweet. The browser's address bar shows the URL `https://github.com/michaelsweet`. The GitHub navigation bar includes links for Pull requests, Issues, Marketplace, and Explore. The profile header shows the name Michael R Sweet, the username `michaelsweet`, and statistics for Repositories (14), Stars (5), Followers (50), and Following (1). The bio states: "I currently work for Apple Inc. and am probably best known as the creator of CUPS and author of many IPP specifications." A "Follow" button is visible. Below the bio, the user is associated with the organization `@apple`, which is circled in red, and is located in Sudbury, ON. The profile lists six pinned repositories: `apple/cups` (Official CUPS Sources, 536 stars, 164 forks), `mxml` (Tiny XML library, 87 stars, 40 forks), `htmldoc` (HTML Conversion Software, 27 stars, 9 forks), `istppwg/ippsample` (IPP sample implementations, 30 stars, 17 forks), `mrend` (Miniature markdown library, 2 stars, 1 fork), and `moauth` (Basic OAuth2 clientserver implementation, 0 stars, 0 forks). The profile also shows 1,056 contributions in the last year.

mozilla (Michael R Sweet) - Mozilla Firefox


michaelsweet (Michael R Sweet) X +

GitHub, Inc. (US) `https://github.com/michaelsweet`

Search or jump to

Pull requests Issues Marketplace Explore

Overview Repositories 14 Stars 5 Followers 50 Following 1




Michael R Sweet
`michaelsweet`

I currently work for Apple Inc. and am probably best known as the creator of CUPS and author of many IPP specifications.

Follow

Block or report user

 `@apple`

Sudbury, ON

1,056 contributions in the last year

`apple/cups`
Official CUPS Sources
● C ★ 536 🍴 164

`mxml`
Tiny XML library
● C ★ 87 🍴 40

`htmldoc`
HTML Conversion Software
● C ★ 27 🍴 9

`istppwg/ippsample`
IPP sample implementations.
● C ★ 30 🍴 17

`mrend`
Miniature markdown library
● C ★ 2 🍴 1

`moauth`
Basic OAuth2 clientserver implementation.
● C

CUPS.org [Blog](#) [Bugs](#) [Help](#) [Lists](#) [Software](#) [Search](#)

CUPS

CUPS is the standards-based, open source printing system developed by [Apple Inc.](#) for macOS[®] and other UNIX[™]-like operating systems. CUPS uses the Internet Printing Protocol (IPP) to support printing to local and network printers.

[Download CUPS](#) [Github Repository](#) [License](#) [? Frequently Asked Questions](#)

Demystifying CUPS Development 06 Jun 2018

We often get questions about CUPS development, the different versions of CUPS, and the timelines for changes that we have announced. This article attempts to answer some of those questions and provide some context for the changes that are coming for CUPS.

[Read](#)

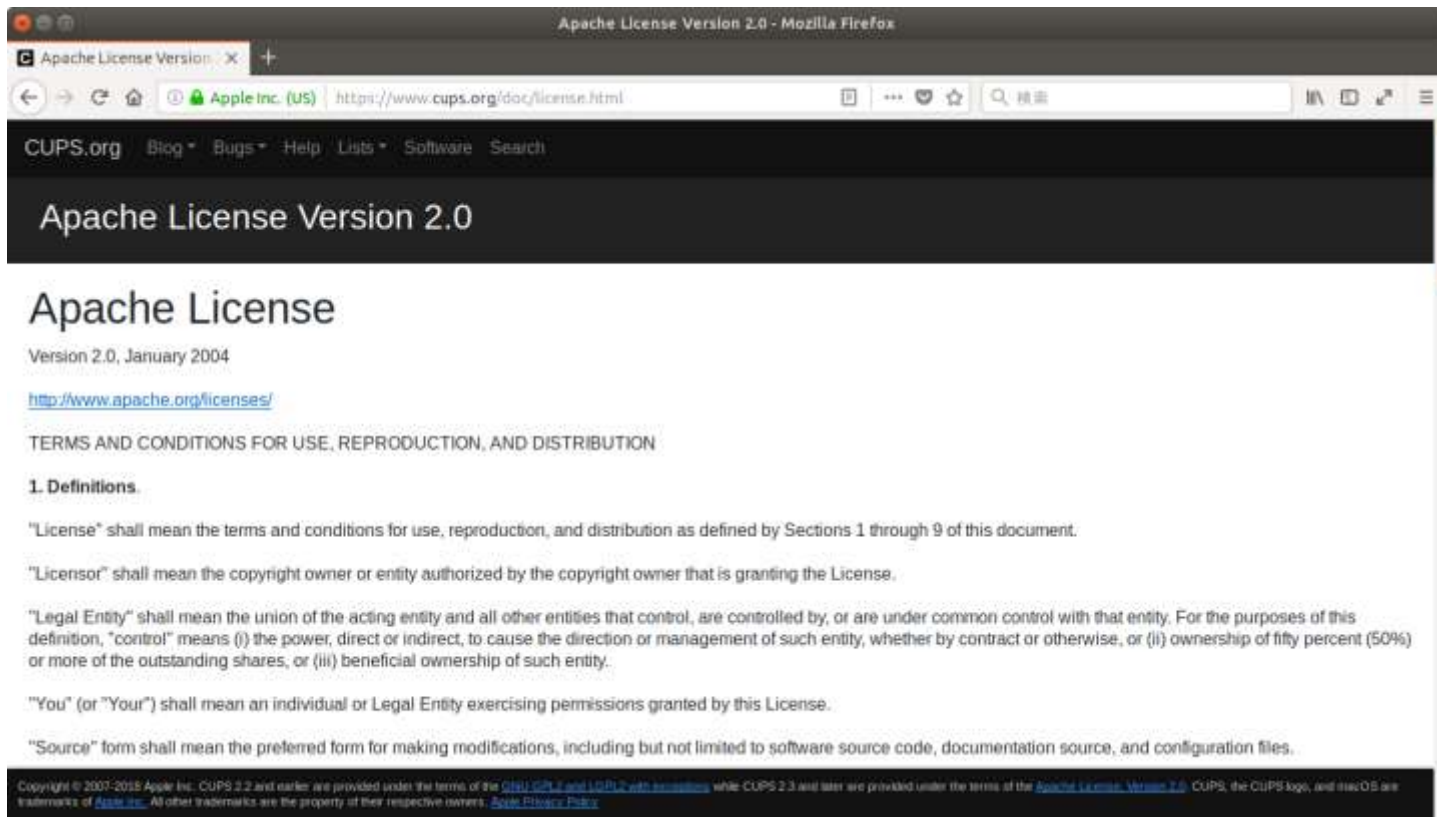
CUPS 2.3b5 05 Jun 2018

CUPS 2.3b5 is now available for download. This is the fifth beta of the CUPS 2.3 series which adopts the new CUPS license, adds support for IPP presets and finishing templates, and fixes a number of bugs and "polish" issues. A detailed list of changes can be found in the change log included in the download.

Enjoy!

Copyright © 2007-2018 Apple Inc. CUPS 2.2 and earlier are provided under the terms of the [GNU GPL 2](#) and [LGPL 2](#) with exceptions while CUPS 2.3 and later are provided under the terms of the [Apache License, Version 2.0](#). CUPS, the CUPS logo, and macOS are trademarks of [Apple Inc.](#) All other trademarks are the property of their respective owners. [Apple Privacy Policy](#)

ライセンス変更



The screenshot shows a Mozilla Firefox browser window displaying the Apache License Version 2.0 page. The browser's address bar shows the URL <https://www.cups.org/doc/license.html>. The page header includes navigation links for CUPS.org, Blog, Bugs, Help, Lists, Software, and Search. The main heading is "Apache License Version 2.0". Below this, the text reads "Apache License" followed by "Version 2.0, January 2004". A link to <http://www.apache.org/licenses/> is provided. The page content is titled "TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION" and includes a section "1. Definitions." with the following text:

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

At the bottom of the page, a copyright notice states: "Copyright © 2007-2015 Apple Inc. CUPS 2.2 and earlier are provided under the terms of the [GNU GPL 2](#) and [LGPL 2](#) with exceptions while CUPS 2.3 and later are provided under the terms of the [Apache License, Version 2.0](#). CUPS, the CUPS logo, and macOS are trademarks of [Apple Inc.](#) All other trademarks are the property of their respective owners. [Apple Privacy Policy](#)"

ケーススタディ②: SQLite

The screenshot shows the NIST National Vulnerability Database (NVD) detail page for CVE-2015-3717. The page is titled "CVE-2015-3717 Detail" and is categorized as "VULNERABILITIES". The main content area is divided into several sections:

- MODIFIED:** A section indicating that the vulnerability has been modified since its last analysis. The text states: "This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided."
- Current Description:** A section describing the vulnerability: "Multiple buffer overflows in the printf functionality in SQLite, as used in Apple iOS before 8.4 and OS X before 10.10.4, allow remote attackers to execute arbitrary code or cause a denial of service (application-crash) via unspecified vectors." The source is cited as MITRE, with a link to the analysis description.
- Severity:** A section showing the CVSS version (3.x) and the severity level (N/A). It also includes a table for CVSS 3.x Severity and Metrics, with columns for NIST: NVD, Base Score: N/A, and NVD score not yet provided.
- QUICK INFO:** A sidebar section providing key information: "CVE Dictionary Entry: CVE-2015-3717", "NVD Published Date: 07/02/2015", and "NVD Last Modified: 09/21/2017".
- References to Advisories, Solutions, and Tools:** A section at the bottom with a disclaimer: "By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this information."

The URL for the page is <https://nvd.nist.gov/vuln/detail/CVE-2015-3717>.

ケーススタディ③: Berkeley DB

NIST Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2017-3617 Detail

Current Description

Vulnerability in the Data Store component of Oracle Berkeley DB. The supported version that is affected is Prior to 6.2.32. Effort: to exploit, vulnerability allows unauthenticated attacker with login to the infrastructure where Data Store executes to compromise Data Store. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Data Store. CVSS 3.0 Base Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AWL/ACH/PRN/URS/SU/CH/H/A/H).

Source: MITRE
[View Analysis Description](#)

Severity

CVSS Version 3.0 CVSS Version 2.0

CVSS 3.0 Severity and Metrics:

MIST: NVD Base Score: **7.0 High** Vector: CVSS:3.0/AWL/ACH/PRN/URS/SU/CH/H/A/H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on

QUICK INFO

CVE Dictionary Entry:
CVE-2017-3617
NVD Published Date:
04/24/2017
NVD Last Modified:
10/02/2018

<https://nvd.nist.gov/vuln/detail/CVE-2017-3617>

ケーススタディ④: PostgreSQL

PostgreSQL: Re: How can we submit code patches that implement our (pending) patents?

Home About Download Documentation Community Developers Support Donate Your account

Search for...

Quick Links

- Community
- Contributors
- Mailing Lists
- JRC
- Slack
- Local User Groups
- Events
- International Sites

Re: How can we submit code patches that implement our (pending) patents?

From: Craig Ringer <craig@2ndquadrant.com>
To: "Tsuyukawa, Takayuki" <tsuyukawa@stakobots.jp>
Cc: "pgpq-hackers@lists dot postgresql dot org" <pgpq-hackers@lists dot postgresql dot org>
Subject: Re: How can we submit code patches that implement our (pending) patents?
Date: 2018-07-04 01:48:30
Message-ID: CAMsr+9HAcS-XUSV7k6FBzf3rBnJmiwQbjgXKXoWkzz9cJKBKA%40mail.gmail.com
Views: Raw Message | Whole Thread | Download mbox | Resend email
Thread: <2018-07-04 01:48:30 from Craig Ringer <craig@2ndquadrant.com>
Lists: pgpq-hackers

On 4 July 2018 at 09:17, Tsuyukawa, Takayuki <tsuyukawa@stakobots.jp> (mailto:tsuyukawa@stakobots.jp) wrote:

> Hello,

>

> As I asked at the PGOn developer meeting this year, we'd like to offer

> our company's patents and patent applications license to the

> PostgreSQL community free of charge. If I heard correct in all that line, we

> could continue this discussion during the conference, but I missed that

> opportunity (I'm sorry). So, please let us confirm the consultation

> here. If some other mailing list is appropriate such as pgpq-core, let us

> know. But I hope open discussion will lead to better and fair license and

> conclusion.)

>

> There are three ideas. Is there any effective idea?

>

My big hesitation with all those approaches is that they seem to exclude derivative and transformation works.

PostgreSQL is BSD-licensed. Routinely implementing patented work with a patent grant accorded to PostgreSQL would effectively change that license, require that derivatives identify and remove the patented parts, or require that derivatives license their.

It's seeming you don't want to offer a grant that lets anyone use them for anything. But if you have a really broad grant to PostgreSQL, all someone would have to do is liberate the grant to re-use some part of PostgreSQL.

I guess there's a middle ground somewhere that protects substantial derivatives and extracts but does you giving some Pd code snippets to a FreeBSD license.

<https://www.postgresql.org/message-id/CAMsr%2BYHA8cB-XUSV7k6FBzf3rBnJmiwQbjgXKXoWkzz9cJKBKA%40mail.gmail.com>

万能なOSSライセンスはない。ユース ケースに最適なものを選ぶ。

Choose an open source license | Choose a License - Mozilla Firefox

Choose an open source license

An open source license protects contributors and users. Businesses and savvy developers won't touch a project without this protection.

Which of the following best describes your situation?

I need to work in a community.

Use the [license preferred by the community](#) you're contributing to or depending on. Your project will fit right in. If you have a dependency that doesn't have a license, ask its maintainers to [add a license](#).

I want it simple and permissive.

The [MIT License](#) is short and to the point. It lets people do almost anything they want with your project, including to make and distribute closed source versions. [Babel](#), [.NET Core](#), and [Rails](#) use the MIT License.

I care about sharing improvements.

The [GNU GPLv3](#) also lets people do almost anything they want with your project, except to distribute closed source versions. [Ansible](#), [Bash](#), and [GIMP](#) use the GNU GPLv3.

- コミュニティがアクティブか (メンテナンスされているか)
- ユーザー (仲間) がたくさんいるか (他Distroでの採用状況)
- コミュニティをリードしているのは誰か (自分との関係は?)
- 買収リスクがないか
- 競合ソフトはあるか (スタンダードはどちらか)
- ライセンスに共感できるか
- 脆弱性が適度に出ているか

4.動的評価でパッケージを決定

■ ビルド チェック

- Yoctoのrecipeがあるか

■ ライセンス チェック

- ライセンス スキャナーを利用

■ 動作確認

- 一般的な使い方で自分のやりたいことが実現できるか

5.採用パッケージのバージョンを決定

■ 採用パッケージの

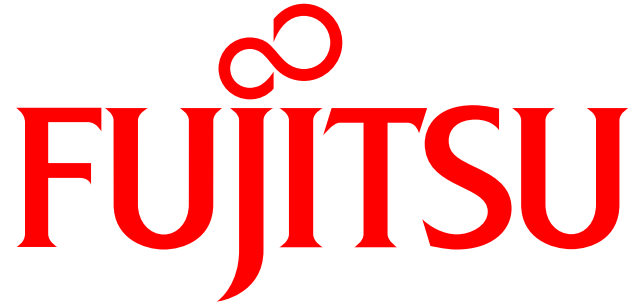
- リリース サイクル
- メンテナンス サイクル
- 他ディストリビューションの採用バージョン

を考慮し、バージョンを決定する。

■ 重要なのは、コミュニティの健全性

- OSSライセンスはコミュニティの方向性を理解する重要な指針。
- ビルドできないとかは論外だが、バグなんて小さな問題。健全なコミュニティならすぐに直る。足りない機能もいつのまにか追加される。
- 数値は見るが、数値の基準は作れない。

■ 結局のところ、目利き力が重要



shaping tomorrow with you