FUJITSU
shaping tomorrow with you

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

1583ka1

$ whoami

FUJITSU

- 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

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!?

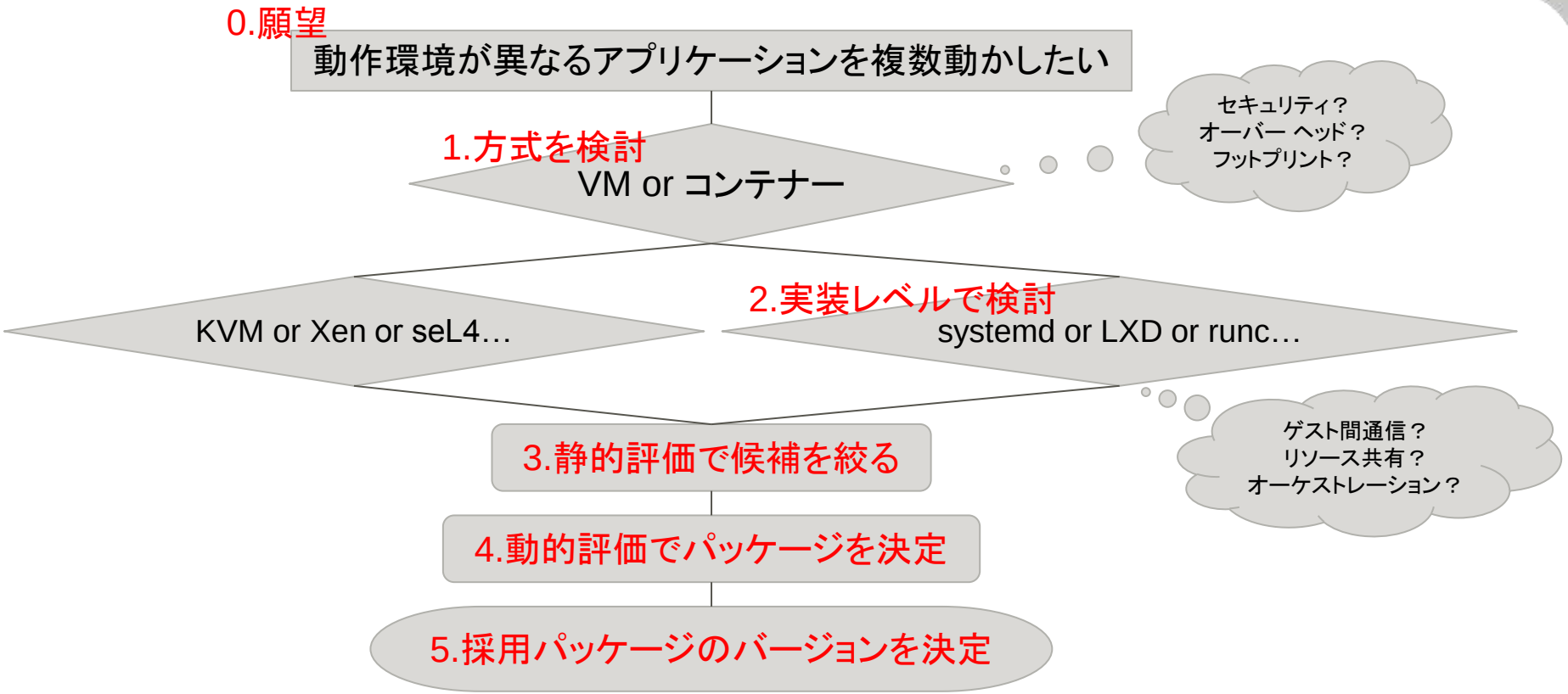
こんな経験ありませんか？

FUJITSU

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。

基本的な流れ

FUJITSU



2.実装レベルで検討

FUJITSU

■ 必要な機能を満たしているか評価

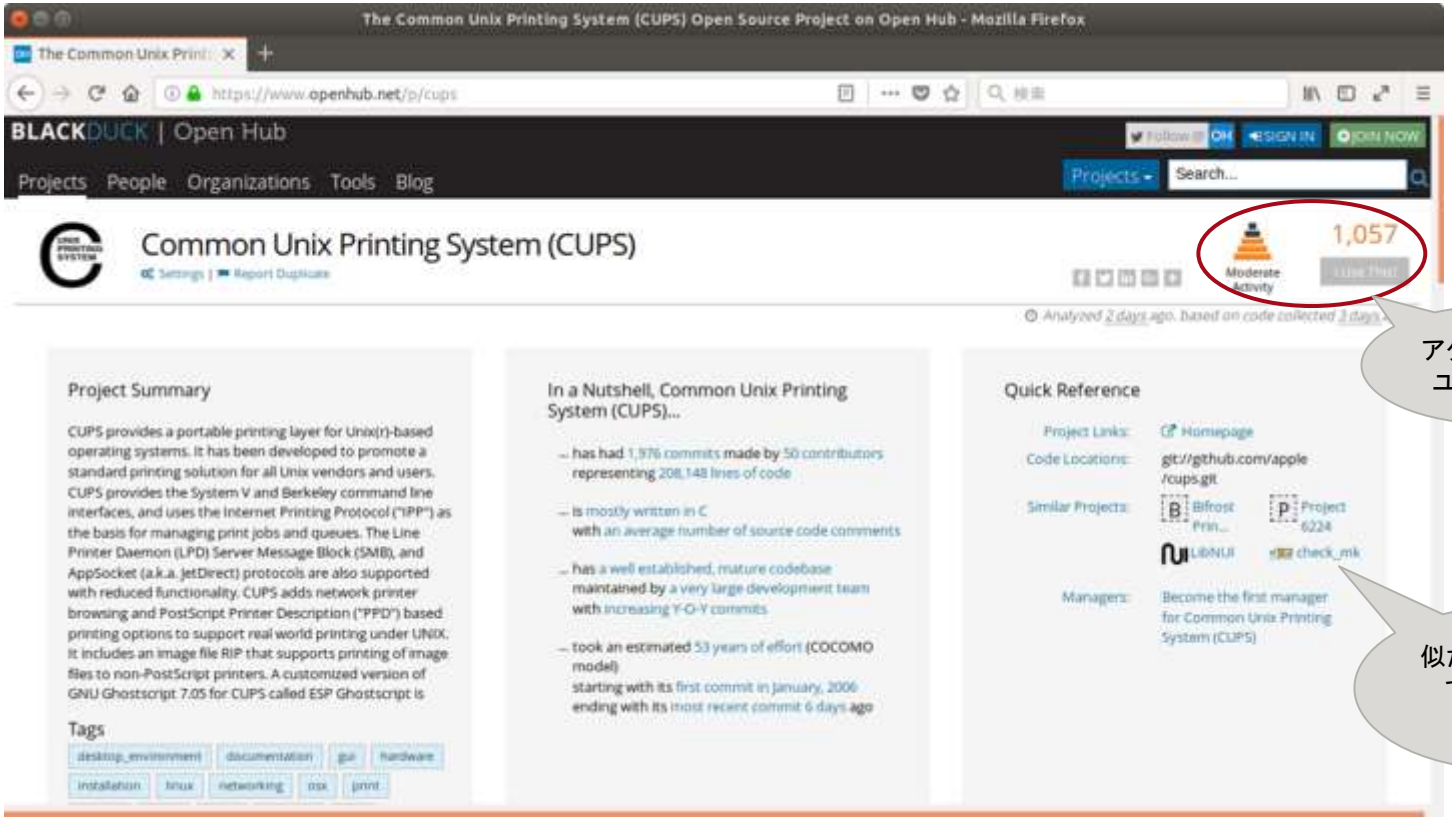
機能＼実装	要件	systemd (nspawn)	LXC	LXD	runC	Kata
セキュリティ	✔					
オーバー ヘッド	✔					
フットプリント						
アイソレーション	✔					
ゲスト間通信						
リソース共有	✔					
ライブ マイグレーション	✔					
オーケストレーション	✔					

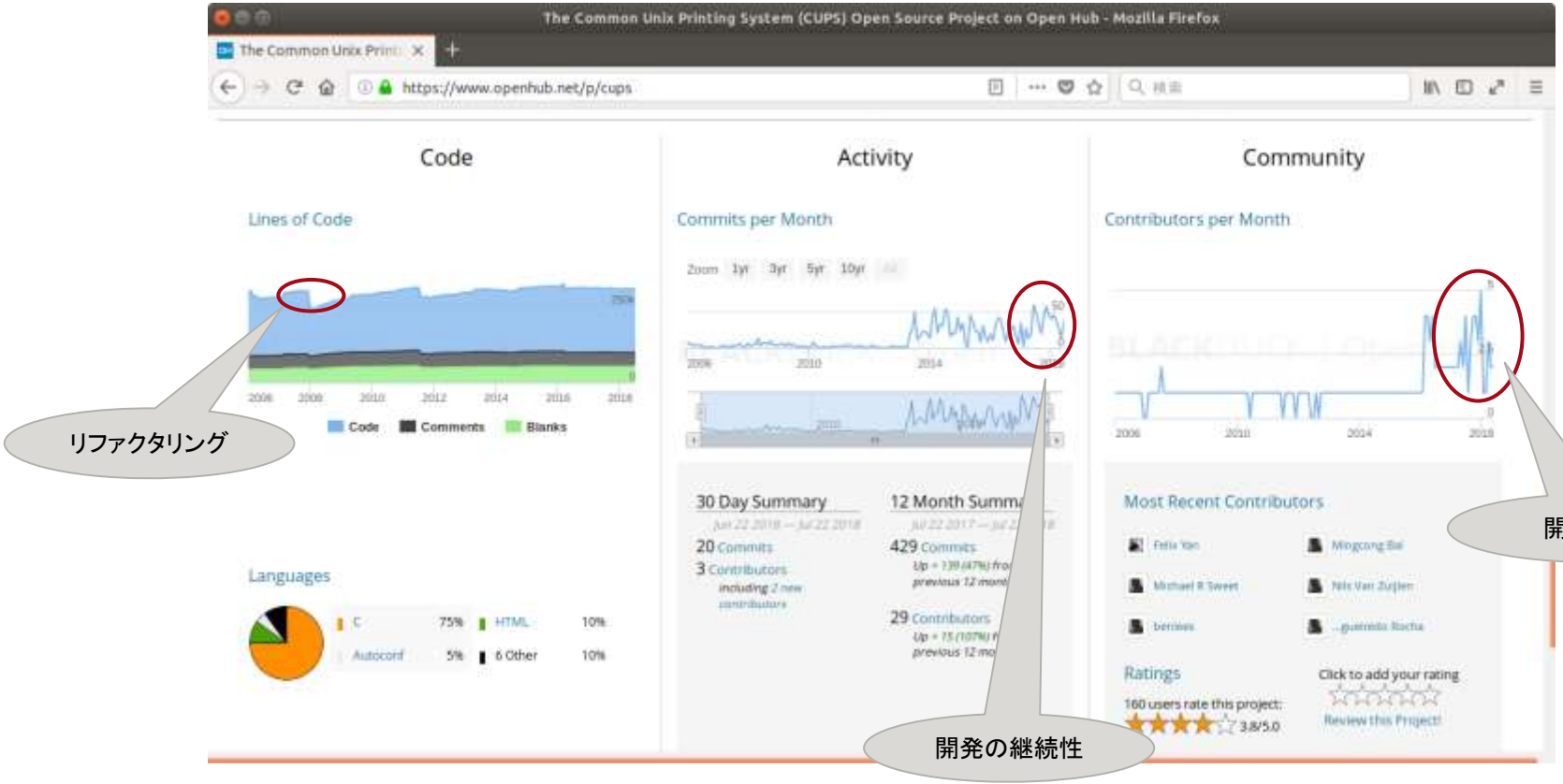
3.静的評価で候補を絞る

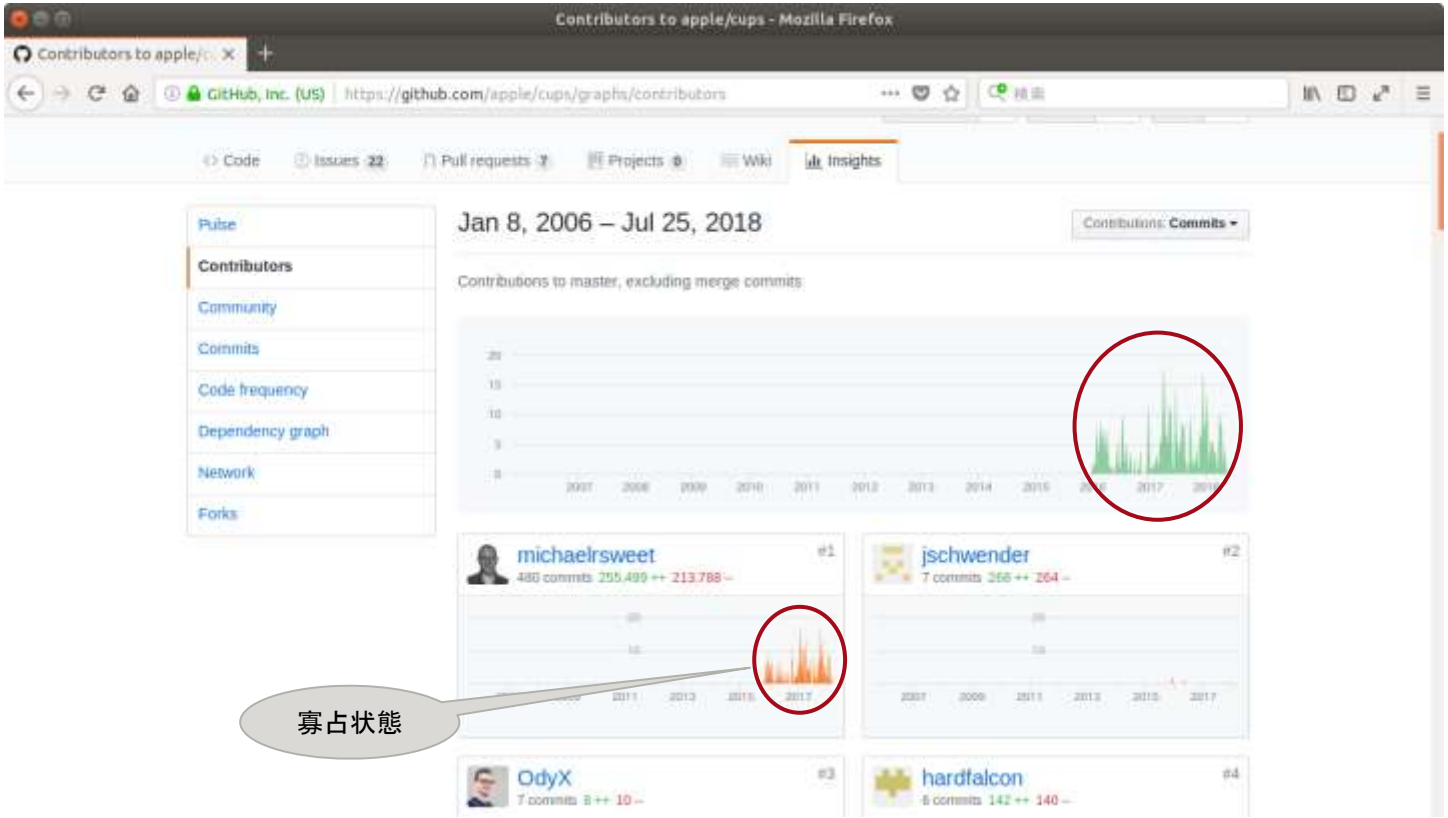
FUJITSU

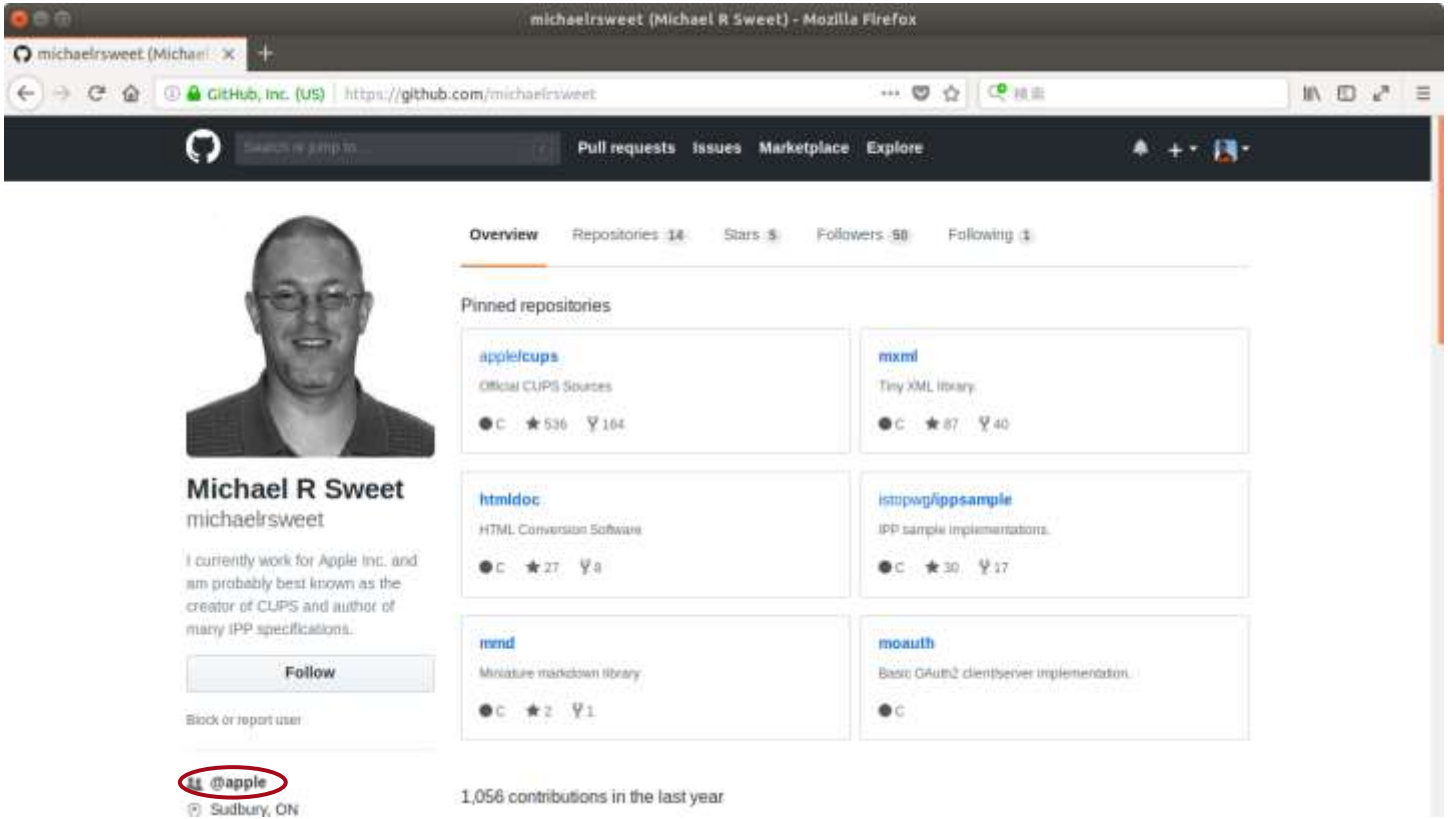
- コミュニティの健全性を評価
  - Open Hub
    https://www.openhub.net/
  - 社内のOSS評価情報共有サイト
  - リポジトリー
  - NATIONAL VULNERABILITY DATABASE (脆弱性サーチ)
    https://nvd.nist.gov/vuln/search

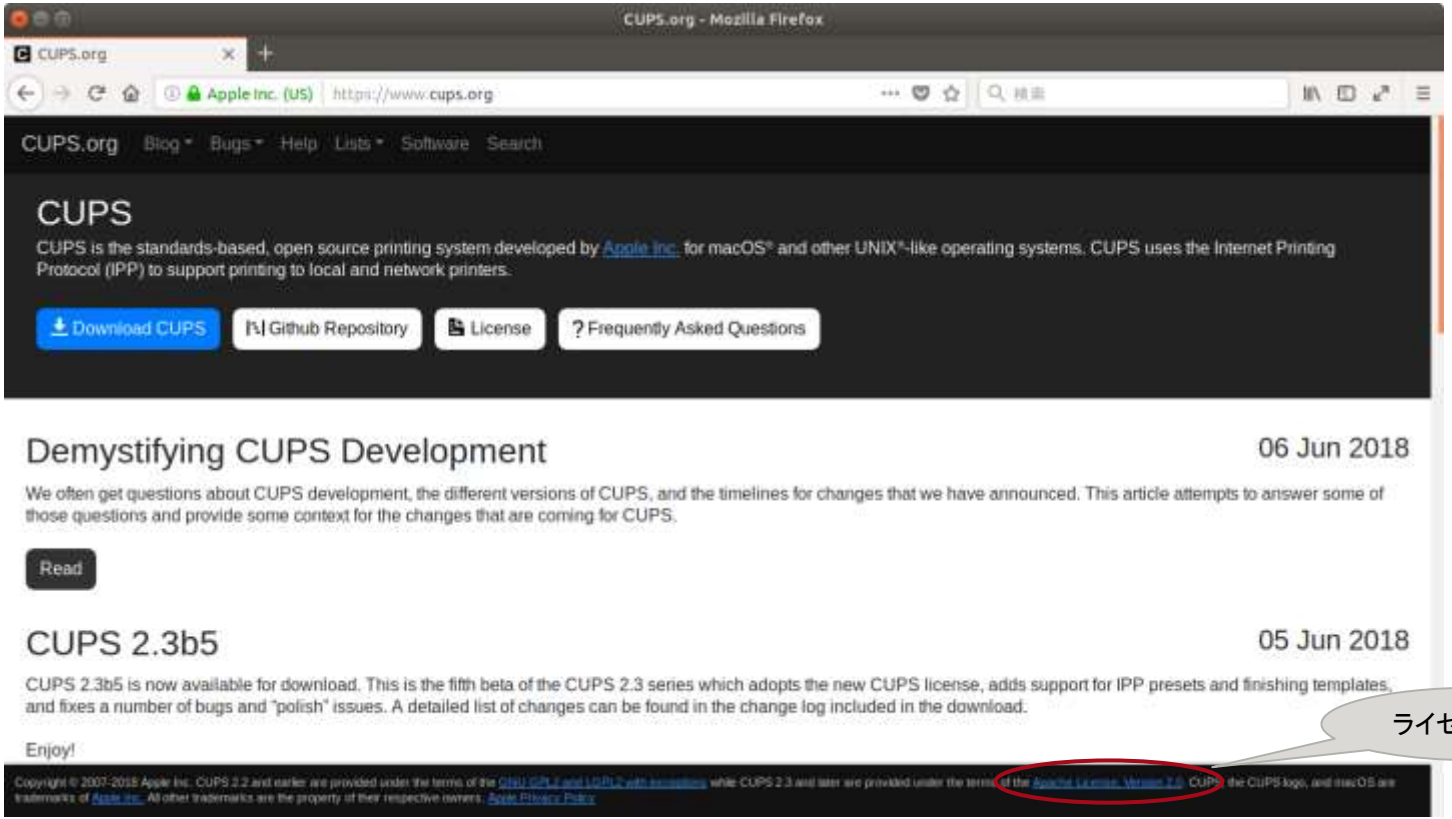
ケース スタディ①：cups

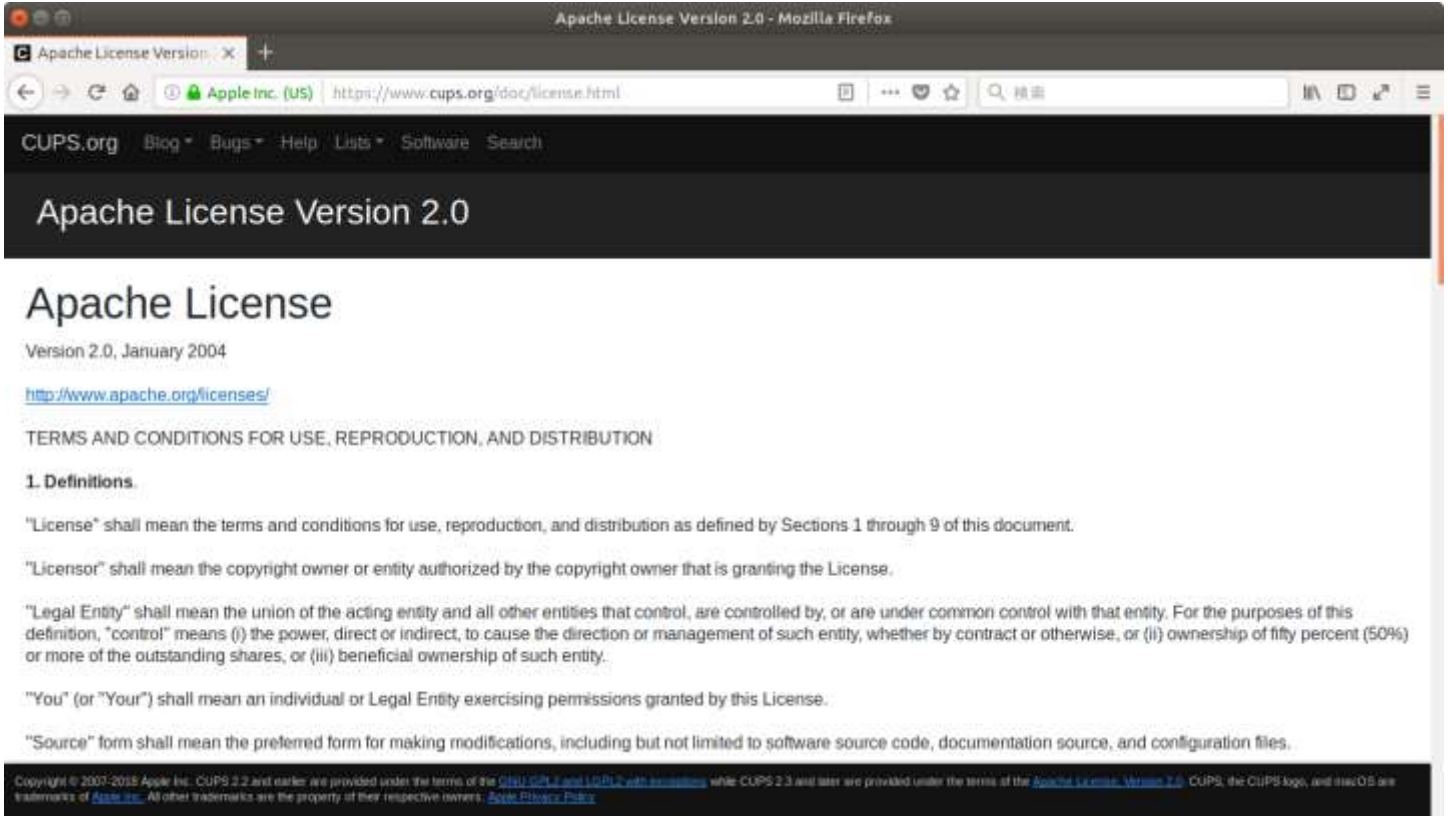




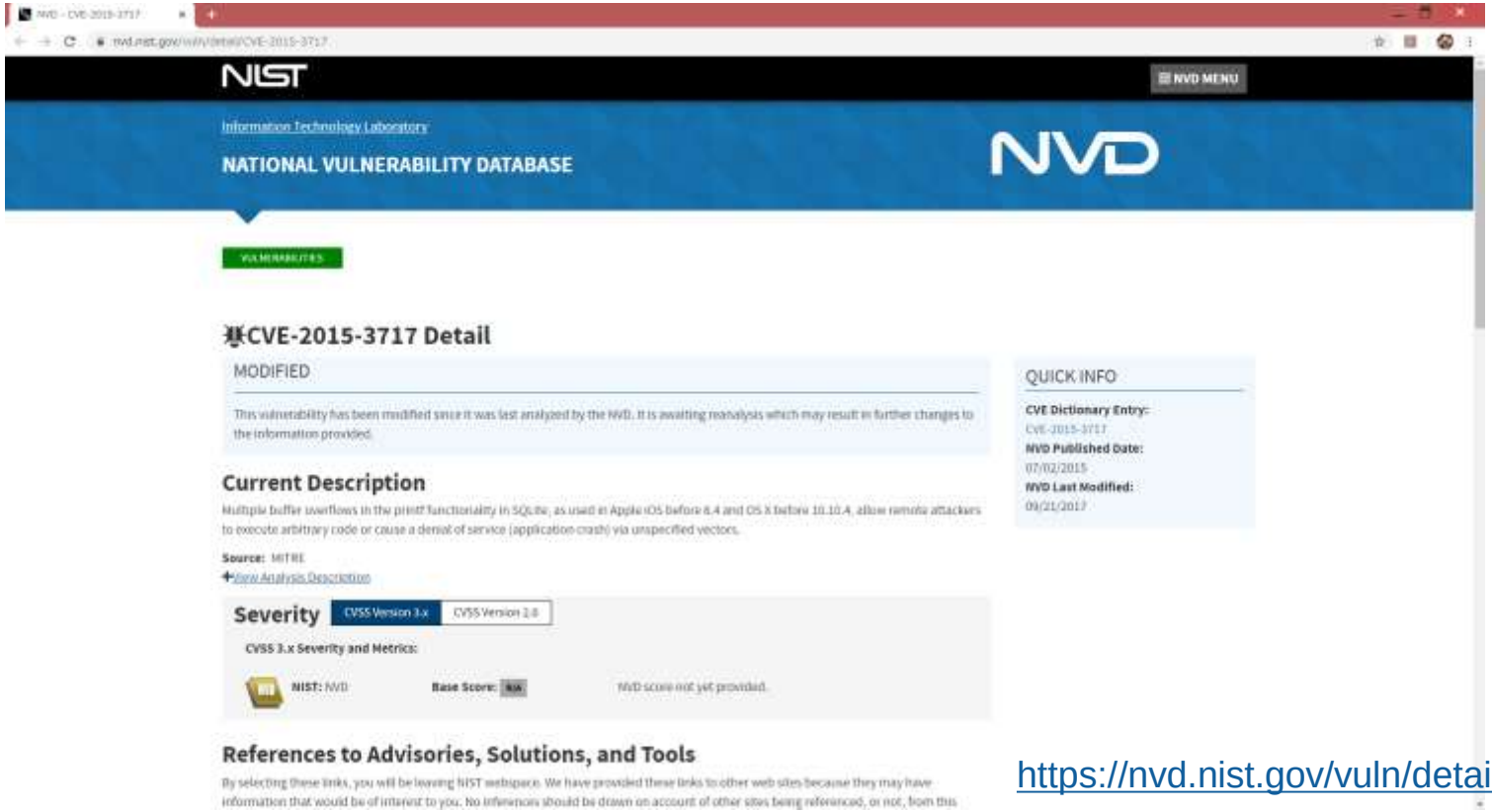






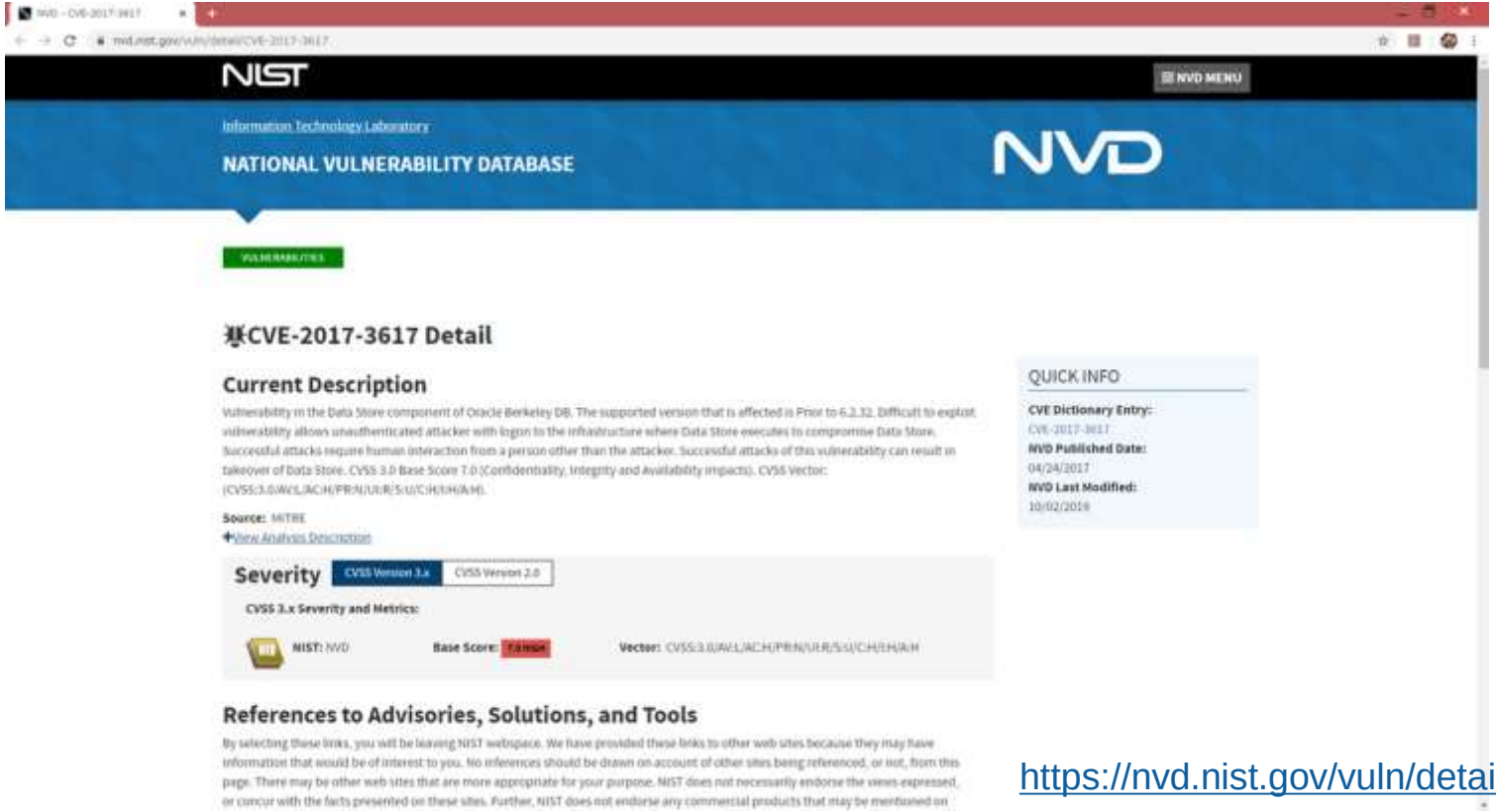


ケース スタディ②：SQLite



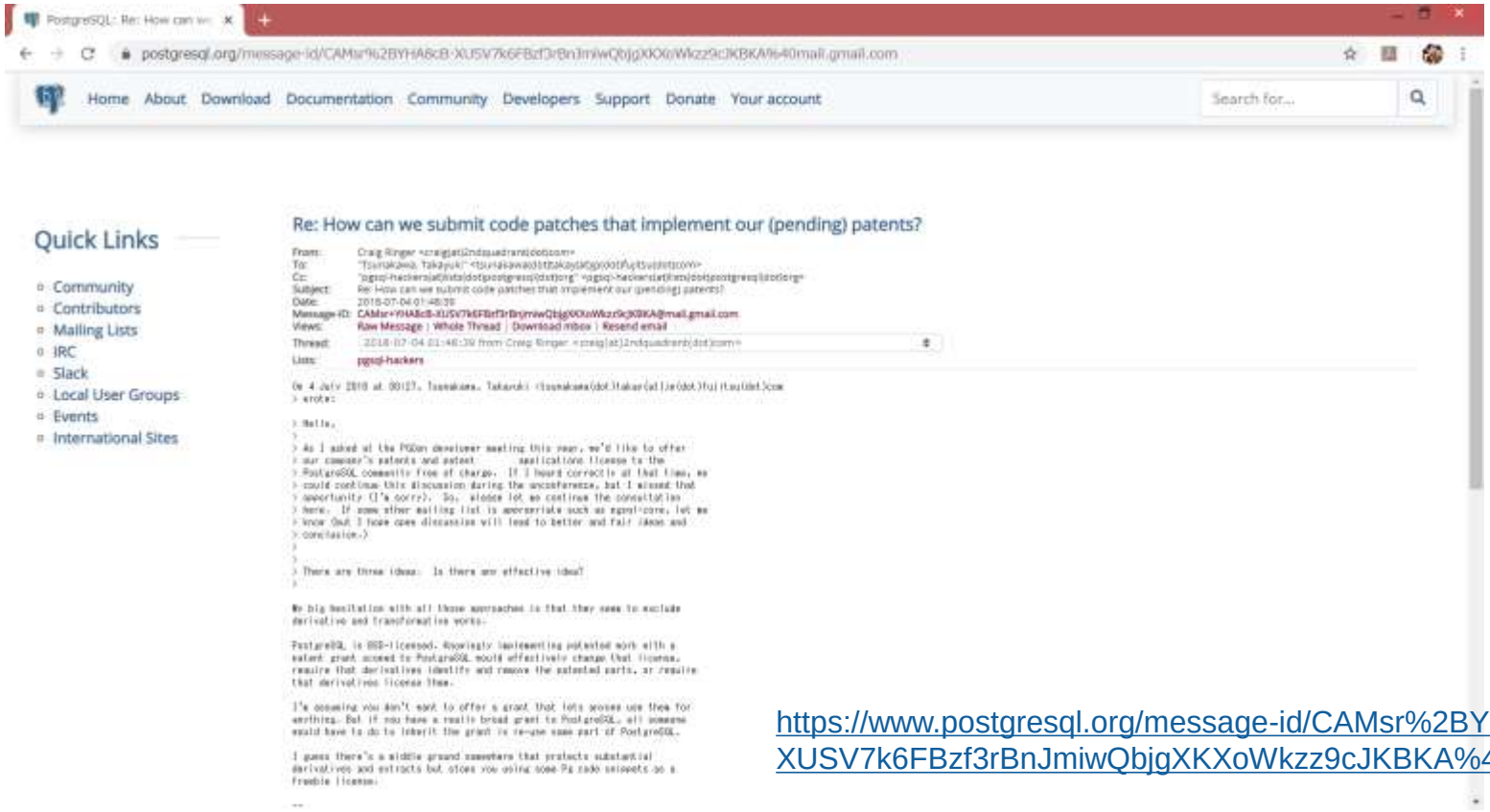
https://nvd.nist.gov/vuln/detail/CVE-2015-3717

ケース スタディ③：Berkeley DB



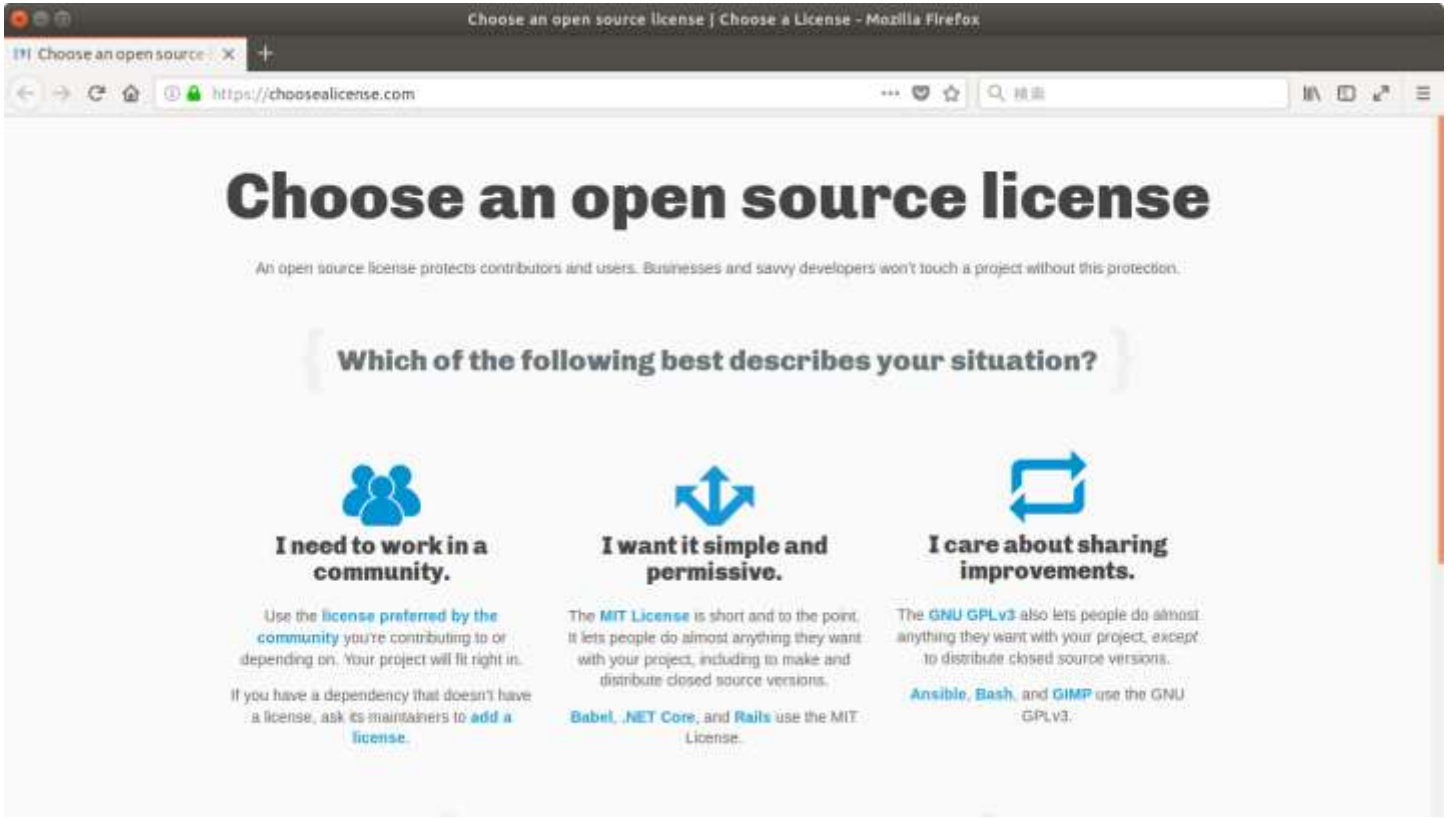
https://nvd.nist.gov/vuln/detail/CVE-2017-3617

ケース スタディ④：PostgreSQL



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。



静的評価の観点まとめ

FUJITSU

- 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

FUJITSU

- 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

FUJITSU

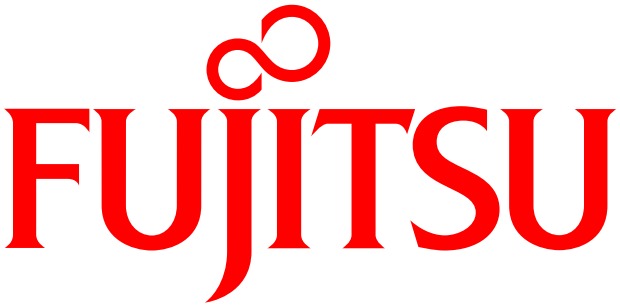
- 採用パッケージの
  - リリース サイクル
  - メンテナンス サイクル
  - 他ディストリビューションの採用バージョン

  を考慮し、バージョンを決定する。

まとめ

FUJITSU

- 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