

JSConf JP 2025

"善意"だけでは続かない

——持続可能性の問題に取り組む世界のOSS政策の話

2025/11/16

独立行政法人情報処理推進機構

デジタル基盤センター デジタルエンジニアリング部

ソフトウェアエンジニアリンググループ

今村 かずき

ライセンス表示 License



この資料は 独立行政法人情報処理推進機構 により作成され、2025年に公開されました。
本資料は [Creative Commons 表示 4.0 国際ライセンス](#) の下で提供されています。

This work was created by Information-technology Promotion Agency, Japan
and published in 2025.

It is licensed under the [Creative Commons Attribution 4.0 International License](#).

1. 背景
2. 世界の行政OSSと政策（現在リサーチ中の内容を一部紹介）
3. ケーススタディ
4. 私たちは何を変えるべきか

1. 背景
2. 世界の行政OSSと政策（現在リサーチ中の内容を一部紹介）
3. ケーススタディ
4. 私たちは何を変えるべきか

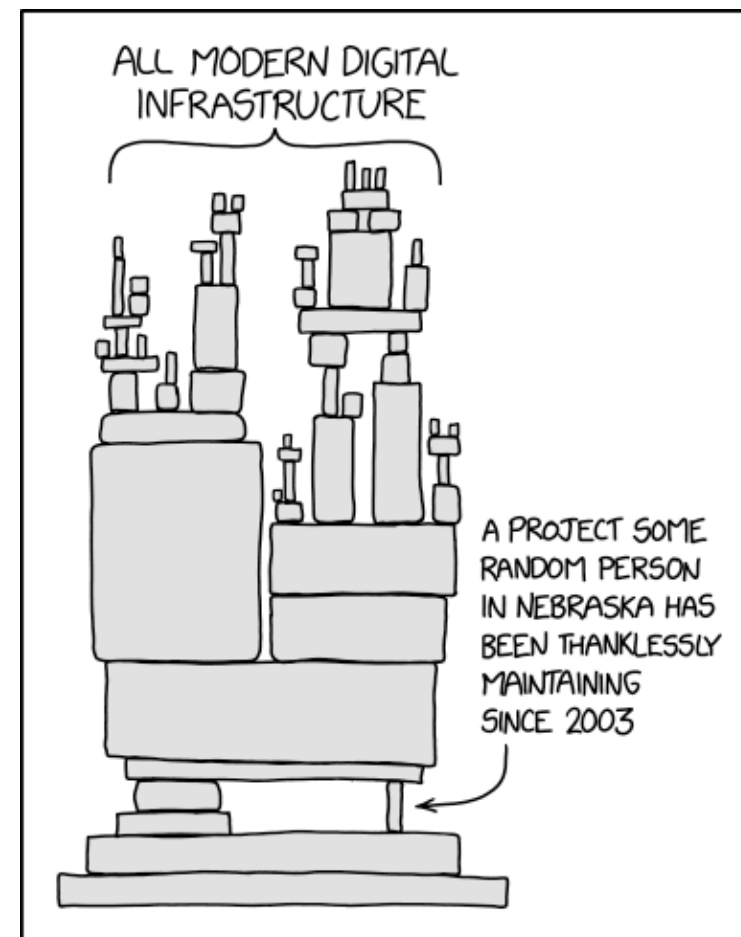
OSSは技術主権と社会の安定を支える基盤であるが...

特定企業・特定国への依存は、**突然の値上げ・障害・サービス停止**といったリスクを伴う。

OSSは依存構造を緩和し、自律的に技術を維持し制御するための共通基盤。

しかし近年、**世界的にOSSプロジェクトやコミュニティの持続性が危ぶまれている。**

- 人材・資金・運営体制の脆弱化
- 政策・市場環境の変化による影響
- 社会インフラを支えるOSSへの過剰な負担



画像: "Dependency" by xkcd is marked with CC BY-NC 2.5.
To view the terms, visit
<https://creativecommons.org/licenses/by-nc/2.5/>.

OSSプロジェクトの危機の一例：Log4j

CVE-2021-44228（通称：Log4Shell）

世界中のシステムが揺れた脆弱性

- ◆ Java ログフレームワーク Log4j で発見されたゼロデイ脆弱性
- ◆ 影響範囲
 - Webサービス、業務システム、クラウド基盤…ほぼあらゆる分野
- ◆ しかし実態は
 - 少人数のメンテナー
 - ボランタリーベースの保守

世界中が乗っているのに、支え方は“善意頼み”だった。

1. 背景
2. 世界の行政OSSと政策（現在リサーチ中の内容を一部紹介）
3. ケーススタディ
4. 私たちは何を変えるべきか

OSS推進に関する行政の介入方法

アメリカ開発銀行のオープンソースイニシアチブCode for Development
「**Open-Source Policy Collection**」

各国のOSS政策の類型

1. 公的機関が持つソフトウェアの**OSSとしての公開**
2. 行政ソフトウェアの移行および**再利用**
3. オープンソースを**共有するためのプラットフォーム**
4. 公共調達における**オープンソースの優先採用**
5. 公共セクターによる**OSSへの修正などの貢献**
6. オープンソースの**セキュリティ基準の策定**
7. **オープンスタード要件の適用**
8. OSSに関する**職員向け研修**
9. **デジタル戦略等重要戦略におけるOSSへの言及**

OSS推進に関する行政の介入方法

アメリカ開発銀行のオープンソースイニシアチブCode for Development 「Open-Source Policy Collection」

各国のOSS政策の類型

1. 公的機関が持つソフトウェアの**OSSとしての公開**
2. 行政ソフトウェアの移行および**再利用**
3. オープンソースを**共有するためのプラットフォーム**
4. 公共調達における**オープンソースの優先採用**
5. 公共セクターによる**OSSへの修正などの貢献**
6. オープンソースの**セキュリティ基準の策定**
7. **オープンスタード要件の適用**
8. OSSに関する**職員向け研修**
9. **デジタル戦略等重要戦略におけるOSSへの言及**

ここにフォーカスして
リサーチを開始

「公的機関が持つソフトウェアのOSSとしての公開」にフォーカス

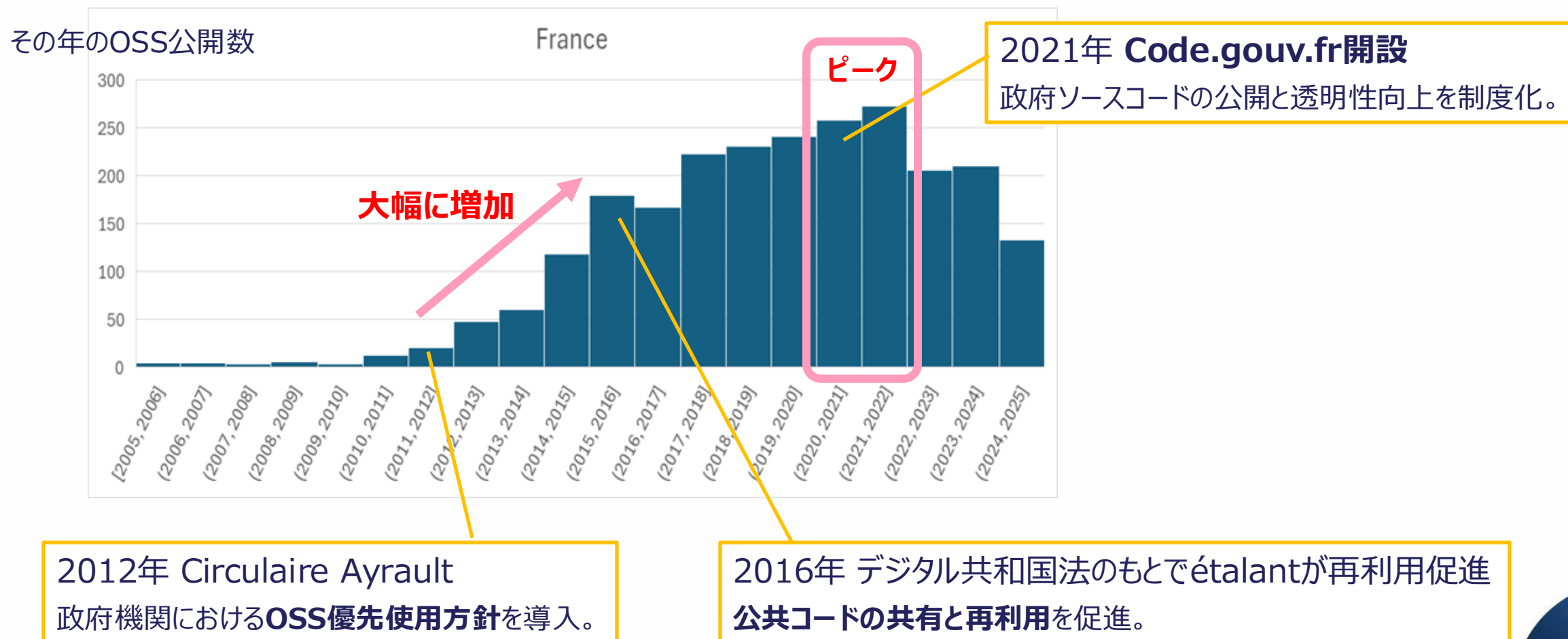
政策とOSS公開数の経年変化を整理、政策が活動に与えた影響を分析

見えてきたこと

- ◆ 米国・英国・フランスなどは、政府系アカウントで合計数千～1万件のリポジトリを所有している。
- ◆ 行政OSSは“趣味レベル”ではなく、政策＋組織で支えられた開発活動になっている。

リサーチの一例：フランス

OSSリポジトリの初回コミット日時を集計し、年ごとのOSS公開数を定量的に算出



1. 背景
2. 世界の行政OSSと政策（現在リサーチ中の内容を一部紹介）
3. ケーススタディ
4. 私たちは何を変えるべきか

ケース① Sovereign Tech Fund × Log4j

ドイツ政府系ファンド「Sovereign Tech Fund」(以下、STF) が Log4j に約60万ユーロを投資

投資対象の内容：メンテナンスに欠かせないタスク

- CI/CD・リリースパイプライン整備
- テスト導入・セキュリティ強化
- SBOM整備・依存関係管理
- API互換性テスト・ドキュメント改善 など

STFがやったこと

- 目立つ新機能ではなく、**基盤整備・セキュリティ強化・運用改善に予算をつける**
- “善意の残業”でやっていたことを、**有償で計画的にやるモデル**に転換

やらかしたプロジェクトを葬り去るのではなく、「**社会インフラとして支え直す**」ことに注力している。

ケース② FOSSEPSのアプローチ

欧州委員会 FOSSEPSパイロットプロジェクト

FOSSEPS : 「Free and Open Source Software for European Public Services」の頭文字

→ 公共機関に組み込まれている“クリティカルなOSS”を調査

Step1. EU公共部門が依存するOSSの棚卸し → Step2. 「クリティカルなOSS」を特定

「クリティカルなOSS」の定義

- 行政サービスや重要インフラで広く利用されている
- 代替が難しい／移行コストが高い
- 脆弱性や停止が社会に直結する
- 例：ログ、XML処理、暗号、パッケージ管理…「地味だけど無いと困る」ライブラリたち

- ◆ 多くのクリティカルOSSが **Bus Factor = 1 or 2**
 - Bus Factor（バスファクター）：プロジェクトの貢献（コミットやPR、レビューなど）のうち、50%程度を担っている人数
 - 言い換えると、「この人たちがいなくなったら、プロジェクトがほぼ止まってしまう人数」
- ◆ 依存関係がブラックボックス
- ◆ 公的機関は大量に使っているのに、**開発者はボランティアベース**

FOSSEPSで提案されている方向性

- クリティカルOSSの継続的な棚卸し
- SBOMや依存関係可視化ツールへの投資
- ファンド・委託・長期サポート契約などの枠組み提案

「どのOSSが本当にあやういのか」という見える化にフォーカスしている。

1. 背景
2. 世界の行政OSSと政策（現在リサーチ中の内容を一部紹介）
3. ケーススタディ
4. 私たちは何を変えるべきか

日本の行政OSSの現状

- リポジトリ数・組織数は**決して少なくはない**
- ただし活動は一部機関・プロジェクトに集中

世界各国とのギャップ

- クリティカルOSSの体系的な棚卸しは未実施
- 公的に支える基金・専任チームも限定的
- 現場の“善意と工夫”に依存しがち

OSSを“善意”から“公共インフラ”の扱いへ

本日の3つのポイント

1. 「世界中が依存しているのに善意頼み」という**構造的なリスク**
2. EUではクリティカルOSSを特定し、公的資金で支える動きが始まっている
3. 日本でも依存しているOSSに対して「**誰がどう責任とコストを分担するか**」を制度として設計する必要がある

OSSを善意頼みにせず、“公共インフラ”として支える制度設計が必要

あなたの組織が依存している
“クリティカルOSS”は何？

みなさんへの
問い

そのプロジェクトが存続するため
には何が必要？

OSSに参加し、育てる社会へ

OSSを“個人頼み”から“組織文化と制度”へと変えていく、それが私たちIPAの次の挑戦です。



Japan Open Source Hub

OSSに参加し、育てる社会へ

Japan Open Source Hubは、オープンソースの価値をひらき、つながり、育てるための入り口です。
OSSに触れるのが初めての方も、導入を進める方も、ここから次の一歩を見つけてください。

🔍 Search for
“IPA OSS”!

IPA