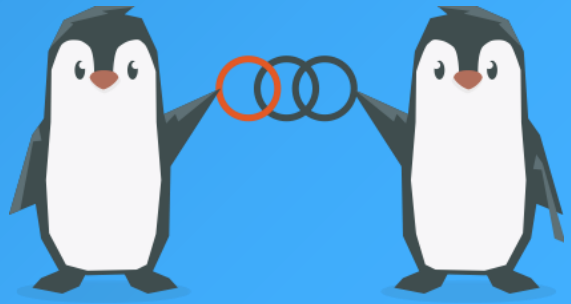
OpenChain Japan SBOM SG

2026-02-09

THE LINUX FOUNDATION

OPENCHAIN



Anti-Trust Policy Notice

- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.
- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/ antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

FOSS license and security compliance tools workshop

FOSDEM 2026 Fringe Event

- CRAに対応するためのSBOM生成、運用に関するツール本イベントは、**ツール開発者が発表する計画と、利用者が提示する現状の課題や要望を共有**し、双方の視点から連携・協業の可能性を模索して、SBOM生成・運用向上への道筋を探るワークショップ。

FOSDEM 2026 Fringe: FOSS license and security compliance tools workshop Fri, Jan. 30, 2026

Interested in open source license and security compliance? Join us for a one-day workshop for developers and users of open source compliance tools on Friday, January 30th, 2026 in Brussels just before FOSDEM 2026.

Our goal is for open source developers, users, and contributors to exchange requirements, plans, and collaboration opportunities around FOSS tools for software provenance detection, vulnerability management, license detection and regulatory compliance like CRA, code scanning, package dependency analysis, container analysis, SBOM creation and consumption, and license or vulnerability databases - basically, all the tools you need to figure out which FOSS code you use, where it is from, what is license, how to comply with the license, and whether it contains vulnerable code.

Previous attendees include developers from ORT, ScanCode, ClearlyDefined, FOSSology, Tern, FSFE REUSE, SW360, BANG, Hermine, Opossum, SPDX tools, DoubleOpen, OpenChain, and AboutCode projects along with users from leading technology and industrial companies, open source foundations, and government institutions worldwi
Whether you are a developer or user interested in the tools for Software Supply Chain and SBOMs, a FOSS license-savvy lawyer, a compliance or security analyst, or an OSPO member: **you will be warmly welcomed**.

<https://workshop.aboutcode.org/>

Schedule – All times CET (UTC+1)

The day will be split in two:
1) The morning will focus on **tool developers** to announce and share their plans, and discuss opportunities for collaboration across projects.
2) The afternoon will focus on **tool users** to share their concerns, problems and requirements, and address these in the represented projects.

8:30 Registration with coffee and light breakfast

9:00 Welcome and introductions

9:30 FOSS compliance tool developers, present your plans!

Each open source project will present their plans for releases and upcoming features with a 5 minute lightning talk.
We likely already know what your tool does, though a short intro is OK. We will use flip charts, big post-its, and markers to support the presentations and discussions – there will not be a projector/beamer, so do not plan for it.

11:15 Discuss collaboration opportunities

How can we work together to overcome shared challenges, and make tools interoperable and compatible so we can deliver better value to all our users?

12:15 Lunch break

This is funded by attendees and our generous sponsors!

13:15 FOSS compliance tool users, give us your requirements!

Each user presents their concerns, problems and requirements

15:00 Coffee break

15:30 Discuss collaboration and joint development opportunities

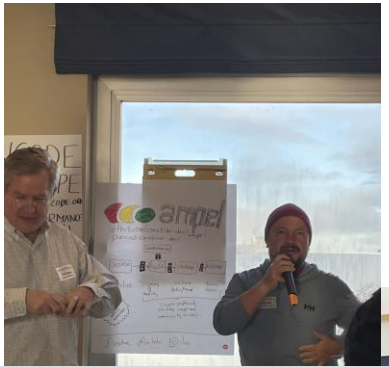
16:30 Workshop conclusion and recap

17:00 Drinks at rooftop bar (inside)

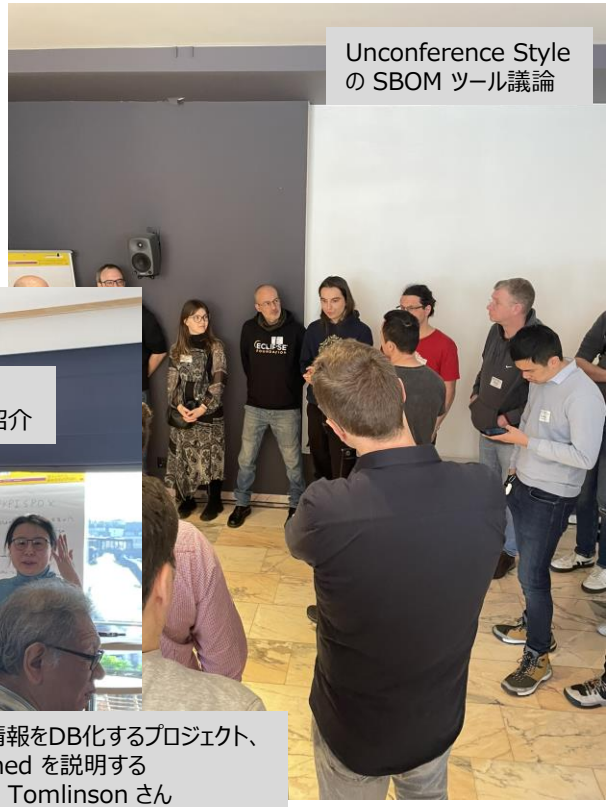
THE LINUX FOUNDATION

OPENCHAIN

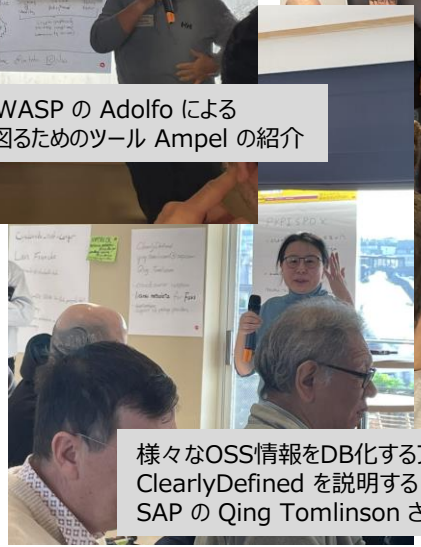
FOSS license and security compliance tools workshop (AboutCode workshop)



OpenSSF, OWASP の Adolfo による
SBOM品質を図るためのツール Ampel の紹介



Unconference Style
の SBOM ツール議論



様々なOSS情報をDB化するプロジェクト、
ClearlyDefined を説明する
SAP の Qing Tomlinson さん

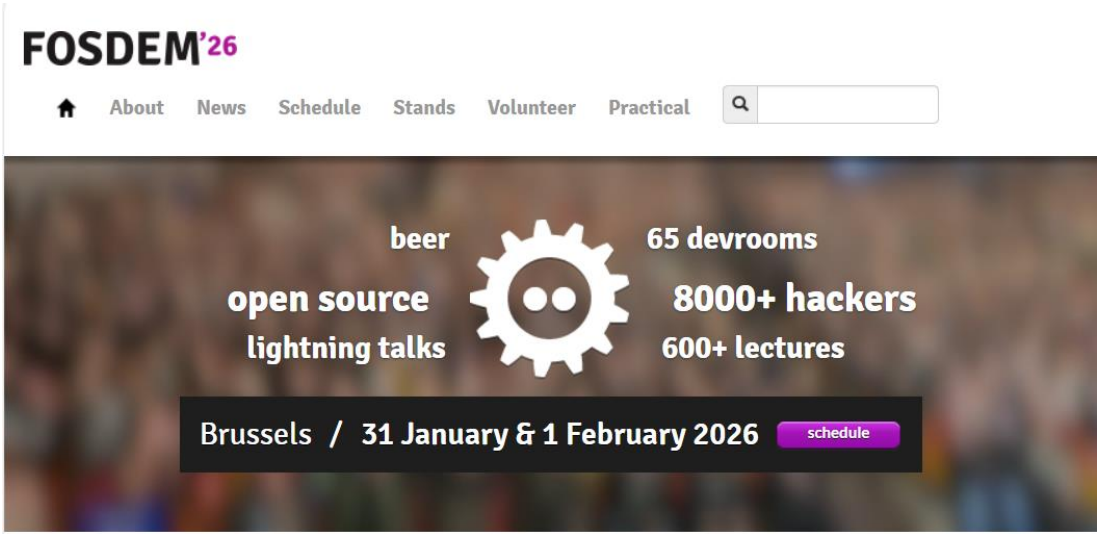
Curl の Daniel と
Linux Kernel Greg K.H.

このワークショップでは、OSSツールの紹介、課題を議論するUnconference、そして著名開発者による講演の三部構成でした。特に最後の講演で、従来のOSS利用開発を覆す警告が伝えられました。

Linuxカーネル等の重鎮が強調したのは「**OSSコミュニティに脆弱性修正の義務はない**」という事実です。これは、CRA (サイバーレジリエンス法) を目前に、**脆弱性対応をコミュニティに依存する従来姿勢が、致命的なリスクになる**ことを意味します。

単なる「利用者」ではなく、自ら脆弱性を修正しコミュニティに貢献する「当事者」となる必要があります。**OSSコミュニティと連携した開発体制の構築と、社内プロセスの改善**を、最優先の課題として考慮していくべきです。

THE LINUX FOUNDATION
OPENCHAIN



- Devroom: 特定テーマに特化した開発者のセッションルーム。深い技術的な議論や最新動向の発表
  (例：プログラミング言語、OS、カーネル、セキュリティ、開発ツール、Web技術、AI/MLなど)
- 基調講演
- 展示ブース

Devrooms
SBOM and Supply Chain, CRA in practice,
Legal & Policy

Welcome to FOSDEM 2026

FOSDEM is a free event for software developers to meet, share ideas and collaborate. Every year, thousands of developers of free and open source software from all over the world gather at the event in Brussels. You don't need to register. Just turn up and join in!

<https://fosdem.org/2026/>

SPONSORS

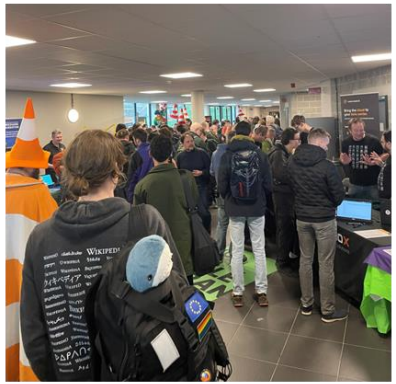
Google Red Hat arm colt dstny element Grafana Labs LMAX PERCONA ULB ZABBIX

THE LINUX FOUNDATION OPENCHAIN

FOSDEM 会場の様子

毎年会場となっているブリュッセル自由大学(Université Libre de Bruxelles / ULB)は約12ヘクタール(東京ドームの2.5個分ほど)の広さを持つ。周辺にホテルはあまりなく、中心街のホテルからバスやトラムで30分ほどかけていく必要がある。

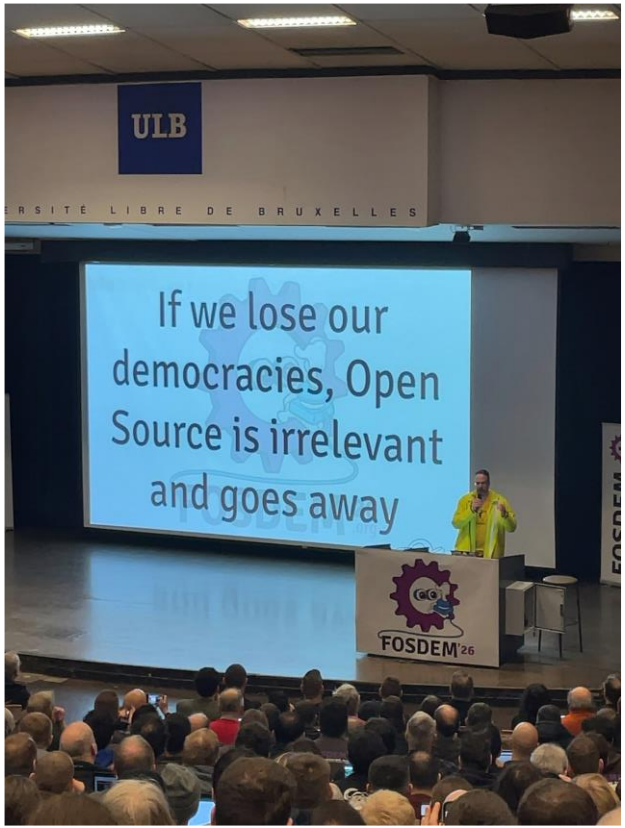
会場にはフードバンが多く滞在しているが、昼食を買うことも難しい。前日や当日朝に軽食を購入、持っていくことが推奨される。
近くの会場には Stands と呼ばれるコミュニティブースが並び、様々なグッズが売られており、イベント運営費などに充てられている。



キーノート会場などの様子。1500名収容可能な建物だが入れなくて外にも長い列ができるなど、どこも人でいっぱい。

Opening Keynote

https://fosdem.org/2026/schedule/event/SFKNTZ-welcome_to_fosdem_2026/



FOSDEMの真髄は、講義室の外にこそあります！

オープニングで語られた「デジタル主権と民主主義」という高潔な理念に千人を超える会場から、地響きのような喝采が送られる一方で、**主催者は「Hallway Track (廊下での議論) 」こそが本番**であると話します。

1,000超のセッション、100ほどのコミュニティブース、Wi-Fiネットワークの構築から分散プロトコル「Matrix」を用いたプライバシー重視のオンラインコミュニケーション。これらが**毎年すべて無料、ボランティアのみで自律運営**される圧倒的なエコシステム。欧州圏の学生から企業幹部、小さな親子連れまでが対等にオープンソースについて会話している姿がそこかしこで見られ、OSSが単なるツールではなく、**欧州の次世代を育む社会インフラ** になっていることを再認識。

技術や情報の習得以上に、**オープンソースコミュニティの熱量に直接触れることの大切さ**がわかるキーノートでした。

THE LINUX FOUNDATION

OPENCHAIN

Legal &Policy Devroom

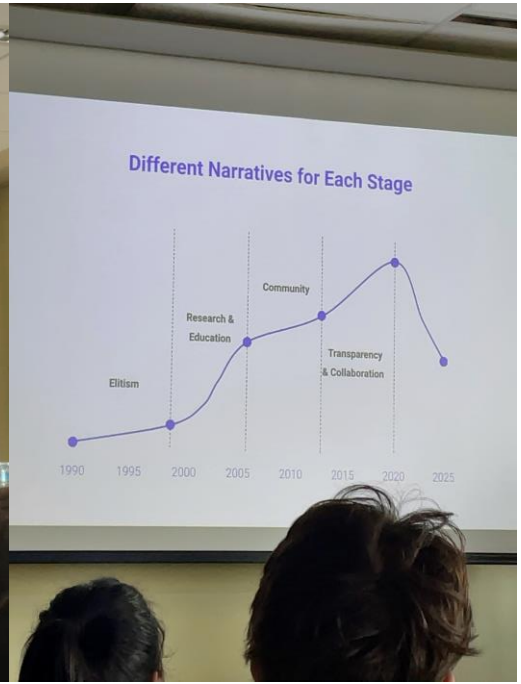
流石、CRAを控えた2026という感じで、Legal & Policy devroomが満員になる場面も。向かって一番左でポケットに手を突っ込んでるのが Bradley Kuhn。SFC の Karen も非常にテンション高く司会進行、発表していたのが印象深い。

SBOMとは別の文脈、Ada & Zangemannの翻訳の話などで、FSFEのMatthiasと一緒に朝食。これから進めていくからね、とこちらの状況を共有。

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/9HAMJC-fork_the_government_the_back_and_forth_open_source_advocacy_road_in_taiwan/

Fork the Government : The Back and Forth Open Source Advocacy Road in Taiwan



台湾 Open Culture Foundationの Rosalind Liuのセッション。

- ✓ 台湾におけるオープンソース文化の歴史とコミュニティの成長
- ✓ 政府による「Public Code」政策とその課題
- ✓ 産業・経済的な視点と今後の方向性

オープンソースコミュニティ活動は、1990年代から始まり、教育機関や若いエンジニアへの普及、g0v などのコミュニティや 2014 年の立法院占拠などを通じて、市民運動・デジタル民主主義と結びつきながら発展してきたが、コスト・透明性・主権テックなど**目的が乱立して一貫したナラティブを欠いた**ことに加え、**産業・経済政策との連携不足**や、TSMC などハードウェア優位の産業構造による人材・インセンティブのミスマッチが重なった結果だと分析。

THE LINUX FOUNDATION
OPENCHAIN

Eclipse Foundationとの情報交換

Mike Milinkovich
Executive Director

Eclipse Foundation、Open Regulatory Compliance WGの文脈で会合を依頼。（FOSDEM前）
NEC 及び CNCF から 武藤さん、ルネサスから伊藤さんにもご参加いただき、1時間超の打ち合わせを実施。
SBOM SGの話題ではないですが、企業OSPOは率先してこういった機会を創出すべきですし、また、その結果を会社の上層に報告、アクションを求めるべきです。OSPOとしても動かれてる方は是非ご協力ください。

大きく分類して以下3つの観点で議論しました。

1. CRA と ORC(Eclipse Foundation) の役割・位置づけの共有
2. CRAが製品・サプライチェーンに与える影響と責任分担の議論
3. SBOMとその品質証明、および関連ツールチェーンをどう実務に落とすかの議論

SBOM に「どこまで／どの粒度で」情報を入れるべきか、ビルドチェーン全体の依存関係や由来情報をどこまで追跡すべきかといった技術的・運用的課題が議論された。あわせて、ソフトウェアを作る側・使う側が、自社の開発プロセスやセキュリティ対応の状況を、どのような証拠や文書の形で第三者（規制当局・顧客・パートナー）に示すべきかが話題となった。さらに、Eclipse Foundation が関与する中小企業向け CRA 対応支援プロジェクト (OCCTET) や、**OpenChain SBOM WGの取り組みと連携しながら、実務で使えるガイドやツールチェーンを整備していく**方向性が共有されました。

THE LINUX FOUNDATION
OPENCHAIN

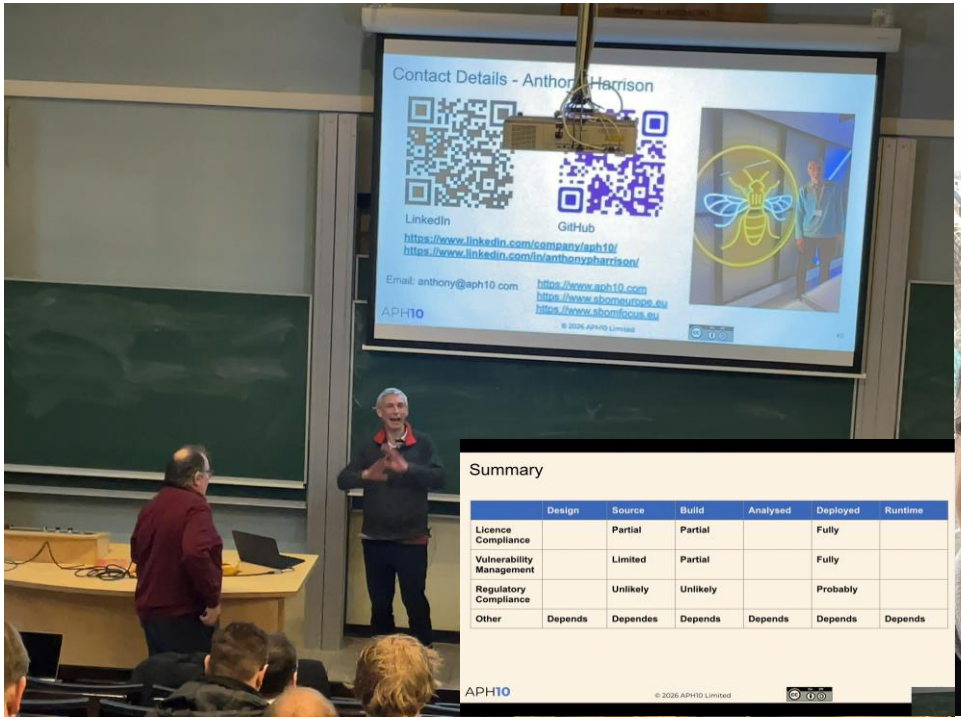
SBOM Devroom

Auditorium 1室を借り切って終日 SBOMのセッション。午前の早い時間は待たずに入れることもあったが、前評判通り会場は満員。一度外に出ると次には入れるのは１時間後、という状況に。
司会進行を Adolfo と Thomas, Alexiosなどが行っていた。日本からは伊藤さんとソニー組しか居なかったはず。

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/DVPCJC-the_day_in_a_life_of_a_sbom/

The day in a life of a SBOM

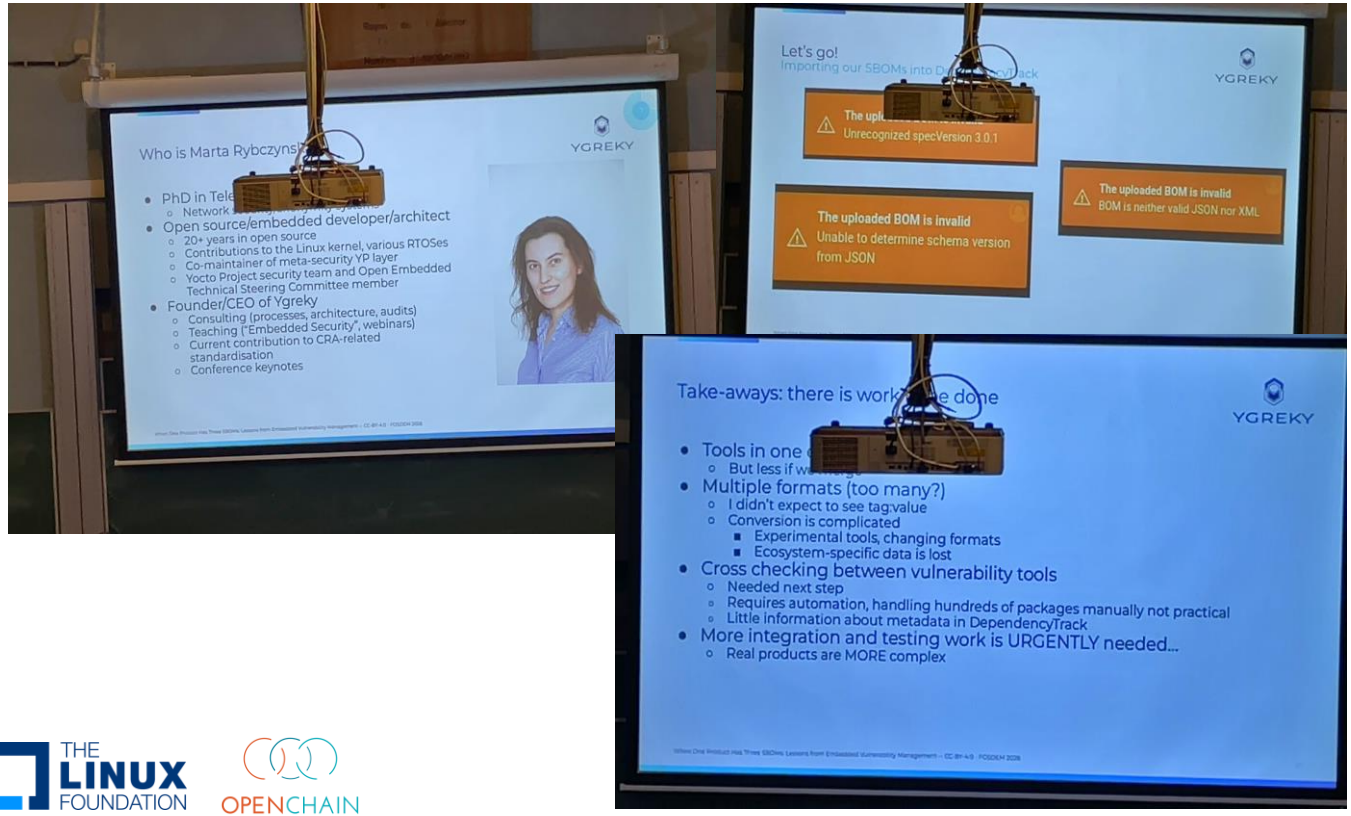


SBOM WGにもたびたび参加してくれて、コメントをくれる Anthonyさんとin-personでお会いできました。(AboutCode workshopでの写真)
セッションは残念ながら終わったタイミングでの参加となりましたが、ビデオで聴講しました。 SBOM は **Usecase毎にそのサポート内容が違い、特にRuntimeをサポートしてるツールが無い**ので今作ってるよとのこと。また、SBOMは**書かれている内容が一番重要**だよね! OpenChain Quality Guideにも期待してるよ、と会話を交わしました。

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/7YG9H7-embedded-product-with-three-sboms/

When One Product Has Three SBOMs: Lessons from Embedded Vulnerability Management

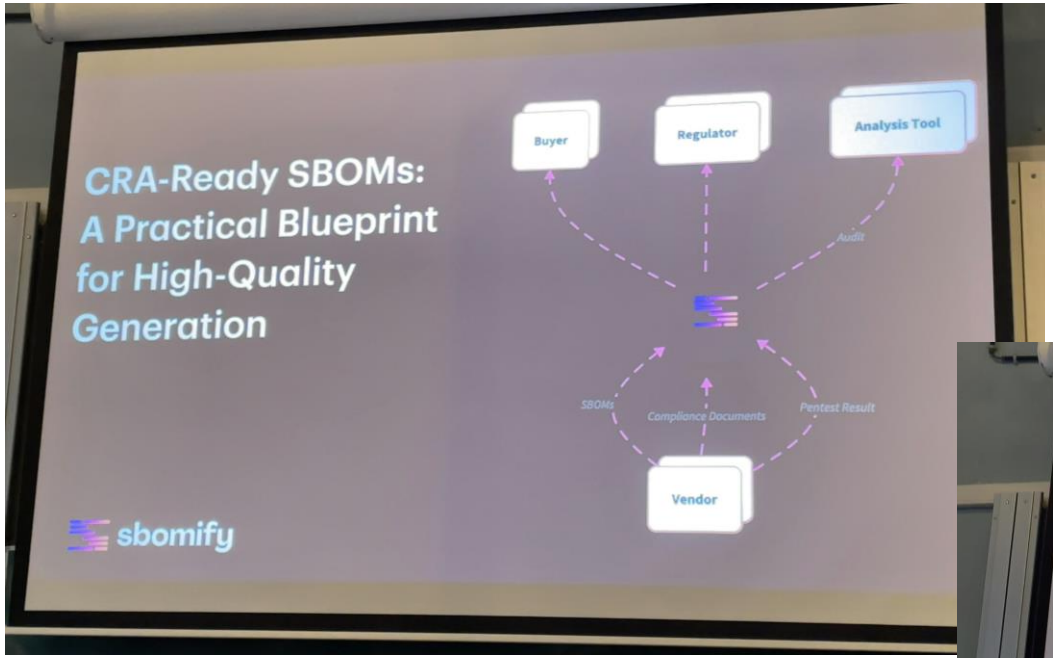


Kernel, Yocto, Zephyerなどで生成されるSBOMを、実際に運用しようとした結果が共有されました。
組込み向けSBOM (SPDX/CycloneDX等) の**形式差と変換時の情報欠落**が大きな課題として挙げられています。
複数フォーマット間の変換で、パッケージ名やバージョンが失われ、依存関係や脆弱性分析結果が不完全・不正確になる点が問題です。そのため、可能な限り**各ツール／プロジェクトがネイティブにSBOMを出力**すること、フォーマット変換を行う場合は**複数の脆弱性ツールでクロスチェック**し、結果の妥当性を検証することが推奨されました。また、ツール間の**相互運用性向上と統合テストをコミュニティで継続的に進める必要性**も強調されていました。

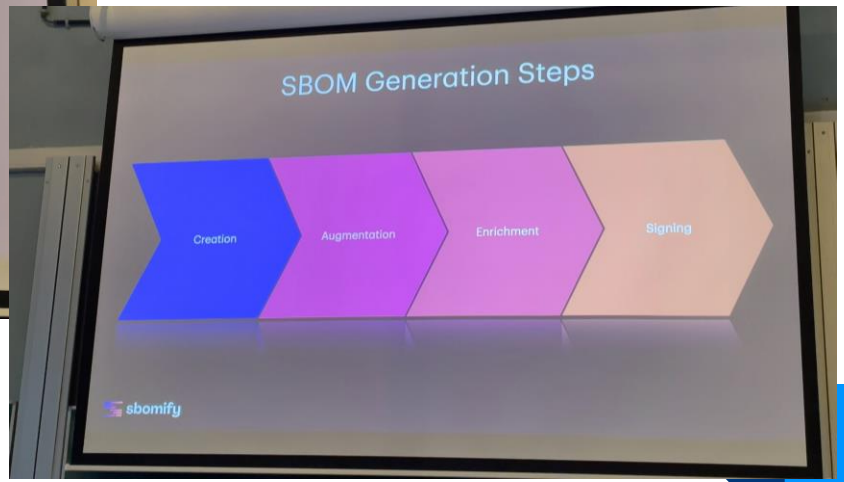
THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/UYTGWA-sbom-generation/

CRA-Ready SBOMs: A Practical Blueprint for High-Quality Generation



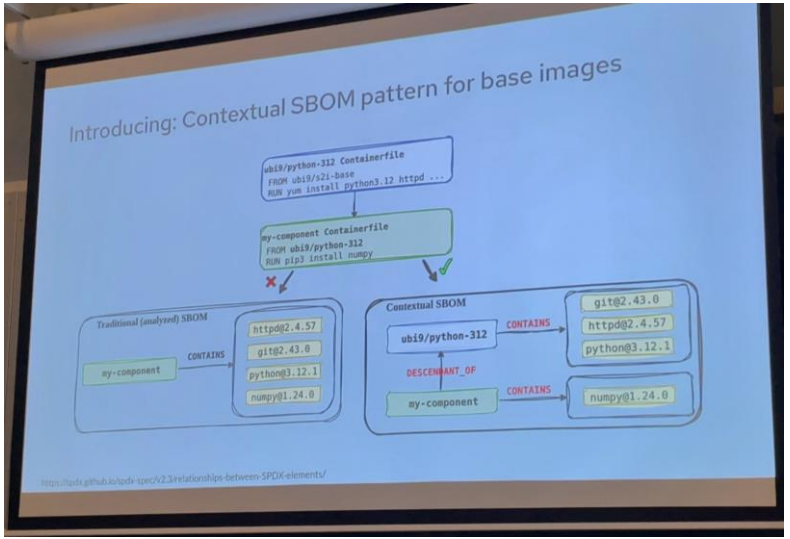
sbomifyを利用した CRA-ReadyなSBOMとは?というセッション。
「完璧」ではなく「ゼロから何かへ」：実務的なCRA対応
法律論や理想論ではなく、「30分でできる現実的な一歩」を重視。
が、個人的には、サプライチェーンが考えられていない点が気になった。



THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/8R99HP-contextual-sbom/

Contextual SBOMs and impact on vulnerability management

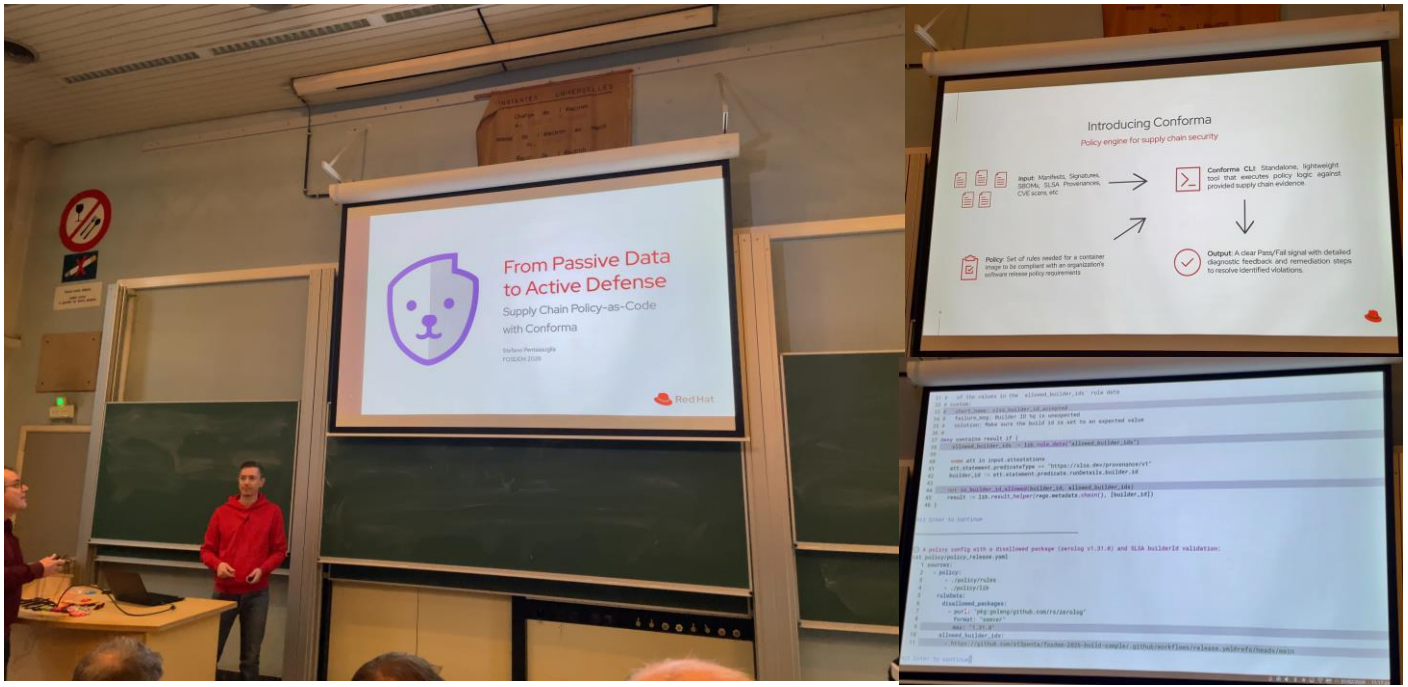


Quality Guideで考えているサプライチェーンに相性の良い考え方。従来SBOMは最終イメージの中身は見えても、各パッケージがどのベース／ビルダーイメージ由来か不明。SPDXのdescendant of等でコンテキストを付与し、由来と責任範囲を明確化すべきという主張。

THE LINUX FOUNDATION
OPENCHAIN

https://fosdem.org/2026/schedule/event/UGRZNA-conforma-supply-chain-policy-as-code/

From Passive Data to Active Defense: Supply Chain Policy-as-Code with Conforma

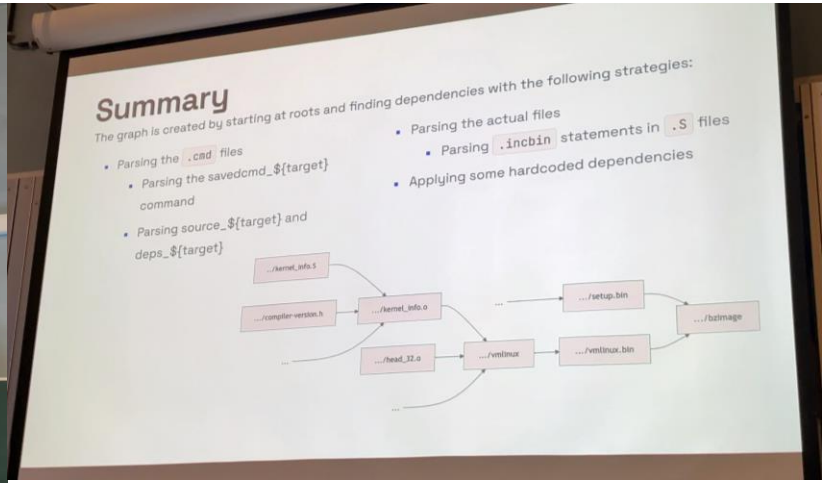


私が一番興味を持ったセッション。

ソフトウェア供給チェーンで生成されるSBOMやアテステーションを自動検証し、パイプラインでPass/Fail判定と人間が読める違反内容を出力するポリシーエンジン「Conforma」の仕組みとデモを紹介。

https://fosdem.org/2026/schedule/event/938CKB-how_to_create_the_sbom_for_the_linux_kernel/

How to create the SBOM for the Linux kernel



kernel SBOMの紹介。SPDX v3.0.1で生成されている。YoctoとkernelがSPDX v3.0.1を正しく表現できているツール。ただし、kernel SBOMもComment fieldにbuild optionが書かれているなど、互換性に課題が残る印象。

おまけ CISA SBOM

AboutCode workshop前日のDinnerで、CISA Victoria と再会。びっくり。

CISA SBOM は稼働を始めており、4月にはpublic commentへの回答を行い、新しいバージョンを出そうとしてるようです。
SBOM a Rama の開催もお願いしておきました。（という話の流れで、CISA SBOM ステッカーを10枚ほど頂きました ☺

ただ、会話した２日後(?) また動きがあったのでどうなるのか読めない状況です。なお、Victoriaさんは、下のJonoさんと一緒に AboutCode Workshop、FOSDEM に参加してました。

JonoさんはSSVCというセキュリティに関係するオープンソースの開発、推進を行っています。
https://www.linkedin.com/in/jono-spring/