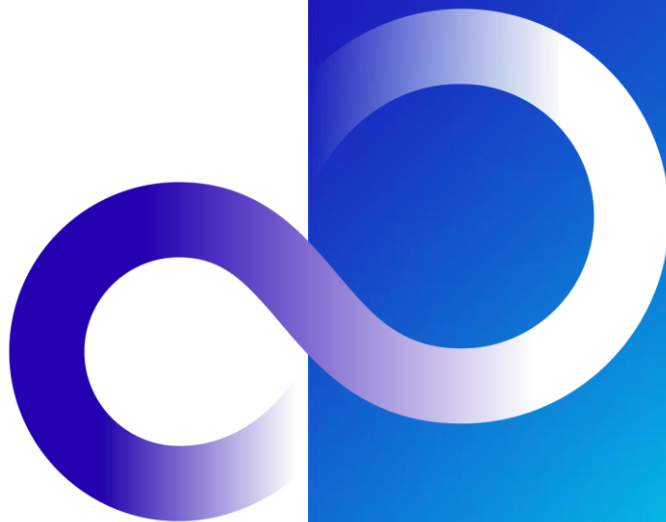


Introducing the OpenSSF SBOM Everywhere SIG (2025/1-2025/10)

Oct 28, 2025

Fujitsu Ltd.

Akihiko Takahashi





富士通株式会社
高橋 明彦

● Account

- Qiita : @flying-pan
- LinkedIn :
<https://www.linkedin.com/in/akihiko-takahashi-26b1a52ab/>

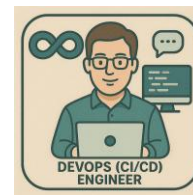
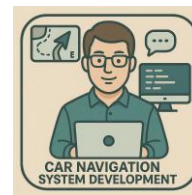
● Job Responsibilities

- Developer of Linux Distributions for Edge Computing
- Infrastructure Engineer for Cloud

● Community

- OpenSSF SBOM Everywhere SIG
- Japan Technical Jamboree
- yocto project
- OpenChain Japan WG

● Technical Background



● Hobby

- Mini 4WD
- Skiing
- Jazz



- OpenSSF概要
- SBOM Everywhere SIG概要
- SBOM Everywhere SIGトピック内容紹介
- 小話（知らない海外の方々とのオンラインミーティング）
- 学生さんにむけて

OpenSSF概要

- Open Source Security Foundation
 - Linux Foundation傘下の団体
- 目的
 - オープンソースソフトウェア全体のセキュリティ強化
- Member
 - <https://openssf.org/about/members/>参照
 - Premier : 25万ドル/年
 - General : 2万ドル/年



- **2014/4/1 セキュリティ脆弱性Heartbleed(CVE-2014-0160)発見**

- OpenSSLに対する脆弱性
- OpenSSLは、資金不足とみなされ、年間約\$2,000しか寄付を受けていないことが判明



- 2014年4/24 Heartbleedを受けて、**Core Infrastructure Initiative (CII)**設立

- OSSPrjに資金を提供、サポートするLinux Foundationのプロジェクト

- 2020年8月 Core Infrastructure Initiative (CII)の後継団体として、OpenSSFを設立

- **2020年12/13 SolarWindsサイバー攻撃発生**

- ネットワーク管理ソフトウェア「Orion」を導入している企業/機関が、ロシアからと見られるサイバー攻撃の被害に遭い、内部情報などを盗まれる。
- 顧客：米国の国務省、商務省、財務省、疾病対策センター（CDC）、連邦捜査局（FBI）、米軍の5部門全て、米国フォーチュン500社のうち425社

- **2021年5/7 コロニアル・パイプライン社へのランサムウェア攻撃発生**

- 1週間にわたって操業停止（アメリカ東海岸への燃料供給の約45%に影響）

- 2021年5/12 米国大統領令発布「[国家のサイバーセキュリティ強化について](#)
[\(Executive Order on Improving the Nation's Cybersecurity\)](#)」



- 2022年1/15 ホワイトハウスが政府および民間部門の関係者(OpenSSFメンバーも参画)とソフトウェアセキュリティに関する会議を開催
- 2022年5/12-13 OpenSSFが、The Open Source Software Security Mobilization Planを発行

●OpenSSF 「2024アニュアルレポート」を見るべし！

- https://www.linuxfoundation.jp/wp-content/uploads/2025/02/OpenSSF_Annual_Report_2024_jp.pdf





Working Groups, Projects, & SIGs

1. Inform

Vulnerability Disclosures

Efficient vulnerability reporting and remediation

- V1. CVD Guides SIGs
- V2. Open Source Vuln Schema (OSV) project
- V3. OpenVEX project
- OpenVEX SIG



Securing Critical Projects

Identification of critical open source projects

- CP1. criticality_score project
- CP2. Package Analysis project

DevRel

Develop Use Cases and help others learn about security

AI/ML Security

AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity

- A1. Model Signing SIG

2. Equip

Best Practices

Identification, awareness, and education of security best practices

- B1. OpenSSF Best Practices Badge project
- B2. OpenSSF Scorecard project
- B3. Education SIG
- B4. Memory Safety SIG
- B5. C/C++ Compiler Options SIG
- B6. Python Hardening SIG
- B7. Security Baseline SIG



Security Tooling

State of the art security tools

- T1. SBOM Everywhere SIG
- T2. QSS Fuzzing SIG
- T3. SBOMit project
- T4. Protobom project
- T5. bomctl project
- T6. Fuzz Introspector project
- T7. Minder project



Diversity, Equity, & Inclusion

Increase representation and strengthen the overall effectiveness of the cybersecurity workforce

3. Engage

Securing Software Repositories

collaboration between repository operators

- R1. RSTUE Project



Supply Chain Integrity

Ensuring the provenance of open source code

- C1. Security Insights project
- C2. Supply-chain Levels for Software Artifacts (SLSA) project
- C3. Secure Supply Chain Consumpt Framework (S2C2F) project
- C4. gittuf project
- C5. GUAC project
- C6. Zarf project



Projects

Category-leading software initiatives

- P1. Alpha-Omega
- P2. Sigstore
- P3. Core Toolchain Infrastructure (CTI)





Working Groups, Projects, & SIGs

1. Inform

Vulnerability Disclosures

Efficient vulnerability reporting and remediation

- V1. CVD Guides SIGs
- V2. Open Source Vuln Schema (OSV) project
- V3. OpenVEX project



本日はココの
お話

DevRel

Develop Use Cases and help others learn about security

AI/ML Security

AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity

- A1. Model Signing SIG

2. Equip

Best Practices

Identification, awareness, and education of security best practices

- B1. OpenSSF Best Practices Badge project
- B2. OpenSSF Scorecard project
- B3. Education SIG
- B4. Memory Safety SIG
- B5. C/C++ Compiler Options SIG
- B6. Python Hardening SIG
- B7. Security Baseline SIG



Security Tooling

State of the art security tools

- T1. SBOM Everywhere SIG
- T2. QSS Fuzzing SIG
- T3. SBOMit project
- T4. Protobom project
- T5. bomctl project
- T6. Fuzz Inspector project
- T7. Minder project



Diversity, Equity, & Inclusion

Increase representation and strengthen the overall effectiveness of the cybersecurity workforce

3. Engage

Securing Software Repositories

collaboration between repository operators

- R1. RSTUE Project



Supply Chain Integrity

Ensuring the provenance of open source code

- C1. Security Insights project
- C2. Supply-chain Levels for Software Artifacts (SLSA) project
- C3. Secure Supply Chain Consumpt Framework (S2C2F) project
- C4. gittuf project
- C5. GUAC project
- C6. Zarf project



Projects

Category-leading software initiatives

- P1. Alpha-Omega
- P2. Sigstore
- P3. Core Toolchain Infrastructure (CTI)



SBOM Everywhere SIG概要

SBOM-Everywhere プロジェクトは、SBOM ツールのカatalog 作成と、SBOMの使用開始に役立つベストプラクティスのドキュメント化に重点的に取り組んでいます。 [1]



Working Groups, Projects, & SIGs [2]

1. Inform

Vulnerability Disclosures

Efficient vulnerability reporting and remediation

- V1. CVD Guides SIGs
- V2. Open Source Vuln Schema (OSV) project
- V3. OpenVEX project
- OpenVEX SIG



Securing Critical Projects

Identification of critical open source projects

- CP1. criticality_score project
- CP2. Package Analysis project

DevRel

Develop Use Cases and help others learn about security

AI/ML Security

AI/ML Security at the Intersection of Artificial Intelligence and Cybersecurity

- A1. Model Signing SIG

2. Equip

Best Practices

Identification, awareness, and education of security best practices

- B1. OpenSSF Best Practices Badge project
- B2. OpenSSF Scorecard project
- B3. Education SIG
- B4. Memory Safety SIG
- B5. C/C++ Compiler Options SIG
- B6. Python Hardening SIG
- B7. Security Baseline SIG



Security Tooling

State of the art security tools

- T1. SBOM Everywhere SIG
- T2. OSS Evaluator SIG
- T3. SBOMs project
- T4. Proteobom project
- T5. bonetti project
- T6. Eura Introspector project
- T7. Minder project



Diversity, Equity, & Inclusion

Increase representation and strengthen the overall effectiveness of the cybersecurity workforce

3. Engage

Securing Software Repositories

collaboration between repository operators

- R1. RSTUE Project



Supply Chain Integrity

Ensuring the provenance of open source code

- C1. Security Insights project
- C2. Supply-chain Levels for Software Artifacts (SLSA) project
- C3. Secure Supply Chain Consumpt Framework (SS2CF) project
- C4. gittuf project
- C5. GUAC project
- C6. Zarf project



Projects

Category-leading software initiatives

- P1. Alpha-Omega
- P2. Signstore
- P3. Core Toolchain Infrastructure (CTI)



[1] OpenSSF 「2024アニュアルレポート」 p25 https://www.linuxfoundation.jp/wp-content/uploads/2025/02/OpenSSF_Annual_Report_2024_jp.pdf

[2] OpenSSF Working Groups <https://openssf.org/community/openssf-working-groups/>

- 開催日

- 隔週火曜 11:05am-11:55am EST
(日本時間25:05-25:55)

- ファシリテーター

- Josh Bressers氏 (Anchore)
- Kate Stewart氏 (Linux Foundation)
- Josh氏欠席時にKate氏がファシリテートを行う。両者欠席時、会はキャンセル。

- 参加人数

- 約10～20人(トピックにより変動)

- OSSF SBOM Everywhere SIG in Github

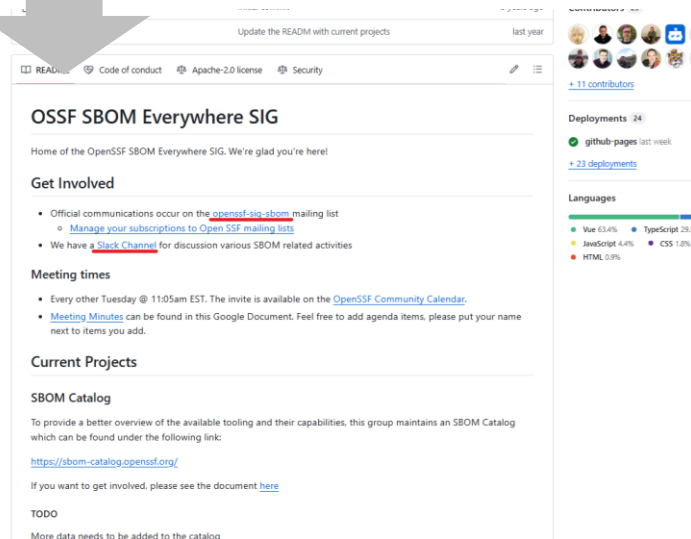
- <https://github.com/ossf/sbom-everywhere?tab=readme-ov-file>

Click

Slackとメーリング
リストを
Let's 登録!!

- 議事録

- <https://docs.google.com/document/d/1wz1mzTkRUPmGtaXAe05hL9agXW5uZ07mdhTfCR1RWQo/edit?tab=t.0> (2025年)
- <https://docs.google.com/document/d/193ODRga1F49WKPYR79SNi9b27mChBqpOf5iiWJcMso/edit?tab=t.0#heading=h.xqitfd6hs1gc> (2024年)



参加者所属企業/組織一覧

カテゴリ	組織名
政府、国際機構	CISA, MITRE, BSI, ISO
研究機関、大学	IEEE, New York University, Indiana University, München University
OSSコミュニティ	Linux Foundation, OpenSSF, CHAOSS, AlektoMetis, The Modem Lisa, OWASP, CPAN Sec, RTEMS Project, Python Software Foundation, Ruby Central
セキュリティ系企業	Anchore, Jfrog, Snyk, Stacklok, Kusari, Interlynk, Source Auditor
軍事・航空宇宙系企業	Lockheed Martin, Honeywell, Defense Unicorns
一般企業	Fujitsu, Honda , Google, Red Hat, Oracle, IBM, AMD, Sopra Steria, Karakun, Ericsson, Resilience, TNG Technology Consulting, Bitergia, Edvina AB, Morgan Stanley, BCG

SBOM Everywhere SIG トピック内容紹介

2025年トピック一覧 (2025.01~03)

Date (EST)	Tittle	Type
2025/1/14	SBOM-Catalog (Marius Biebel氏 (hm.edu)) Acceptability and Accuracy with Software Bills of Material Data and Visualizations (Jean Camp氏, Xinyao Ma氏 (Indiana University))	定例活動 学術研究
2025-01-28	SBOM-Catalog (Marius Biebel氏 (hm.edu)) BSI TR-03183-2 (Michael Schuster氏 (BSI Germany))	定例活動 CRA
2025-02-11	SBOM-Catalog (Marius Biebel氏 (hm.edu)) FOSDEM observations	定例活動 カンファレンス 紹介
2025-02-25	SBOM-Catalog (Marius Biebel氏 (hm.edu)) SBOM Generation Reference Implementations (Ian Dunbar-Hall氏 (Lockheed Martin))	定例活動 コミュニティ紹介
2025-03-11	CRob on the recent policy discussions in Washington DC (Crob氏 (OpenSSF))	カンファレンス 紹介
2025-03-25	CRA Report (CRob氏 (OpenSSF))	CRA

2025年トピック一覧 (2025.04~06)

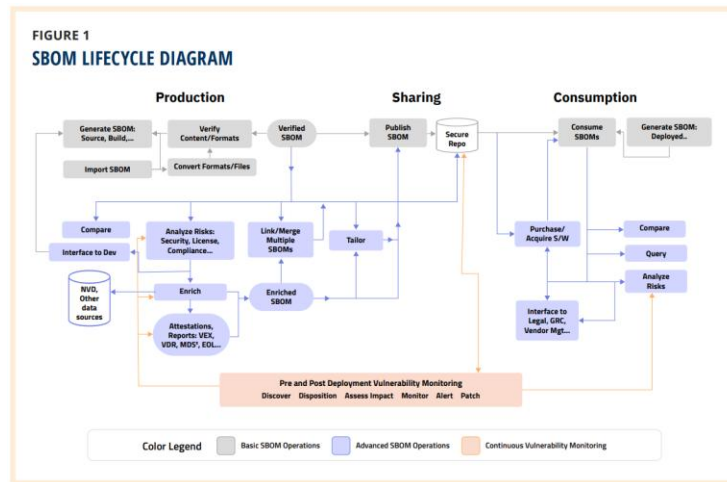
Date (EST)	Tittle	Type
2025-04-08	Show me what you've got: Turning SBOMs into Actions (Georg Link氏 (Bitergia / CHAOSS))	SBOM
2025-04-22	Vulnconの紹介 (Chris Robinson氏 (OpenSSF))	カンファレンス 紹介
2025-05-20	SBOM-Catalog (Marius Biebel氏 (hm.edu)) Improving Risk Management Decisions with SBOM Data	定例活動
		Review
2025-06-03	Improving Risk Management Decisions with SBOM Data	Review
2025-06-17	Improving Risk Management Decisions with SBOM Data	Review

2025年トピック一覧 (2025.07~10)

Date (EST)	Title	Type
2025-07-01	Discussion on SBOM definition evolution Improving Risk Management Decisions with SBOM Data	Discussion Review
2025-07-15	Best times for SBOM generation (Justin氏 (NYU))	学术研究
2025-07-29	Free talk about SBOMs	Discussion
2025-08-12	Indian SBOM guidance (Kate Stewart氏 (Linux Foundation))	SBOM
2025-08-26	Free talk about SBOMs	Discussion
2025-09-09	CISA 2025 Minimum Elements for an SBOM	Review
2025-09-16	CISA 2025 Minimum Elements for an SBOM	Review
2025-09-23	CISA 2025 Minimum Elements for an SBOM	Review
2025-10-07	Free talk about SBOMs	Discussion
2025-10-21	Free talk about SBOMs (SBOM for Docker)	Discussion

Improving Risk Management Decisions with SBOM Data 1/2

- CISA支援のSBOM Operations Tiger TeamからOpenSSFに引継がれ、9/18に公開
- SBOM Everywhere SIGでは、数週間にわたりレビューを実施



Reference

- Improving Risk Management Decisions with SBOM Data
 - <https://openssf.org/blog/2025/09/18/improving-risk-management-decisions-with-sbom-data-a-new-whitepaper-from-the-openssf-sbom-everywhere-sig/>

Improving Risk Management Decisions with SBOM Data 2/2

●SBOMの利用方法について、13のユースケースを提示。

Usecase	成熟度／適用可能性	役割	
	最も成熟している／最も広い適用可能性生産者消費者	生産者	消費者
1	デプロイ前のCVE脆弱性	X	
2	デプロイ後のCVE脆弱性		X
3	ライセンスのリスク	X	X
4	サポート終了（EOL）、メンテナンスされていないコンポーネントのアラート	X	X
5	購入前のリスク評価		X
6	組織全体におけるコンポーネントの使用状況	X	X
	中程度の成熟度／中程度の適用性		
7	インシデント対応		X
8	M&Aと投資リスク評価		X
9	付属ソフトウェアの検証		X
10	ビルドやバージョン間のコンポーネント差分	X	X
	最も成熟していない／適用範囲が絞られている		
11	異なるGRC仕様への適合	X	X
12	OTおよび分離ネットワーク向けの整合性・脅威管理	X	
13	ソフトウェア対応機器のフィールドサービス	X	X

Comments for CISA 2025 Minimum Elements for an SBOM

- 2025/8/22 CISAからMinimum Elements for an SBOM(Draft)が公開
- SBOM Everywhere SIGでは、数週間をかけレビューを実施し、CISAにレビュー結果を提出。

References

- 2025 Minimum Elements for a Software Bill of Materials (SBOM)
 - <https://www.cisa.gov/resources-tools/resources/2025-minimum-elements-software-bill-materials-sbom>
- Comment Submitted by OpenSSF SBOM Everywhere Special Interest Group
 - <https://www.regulations.gov/comment/CISA-2025-0007-0048>
- Sometimes Sequels Are Good: CISA's Update To the 2021 NTIA SBOM Minimum Elements - Victoria Ontiveros, CISA
 - <https://osseu2025.sched.com/event/25Vq6/sometimes-sequels-are-good-cisas-update-to-the-2021-ntia-sbom-minimum-elements-victoria-ontiveros-cisa>
- Discussion for CISA 2025 Minimum Elements for an SBOM at OpenSSF Open Source Security Meetup 2025 #3
 - <https://www.linuxfoundation.jp/events/2025/09/oss-security-meetup-on-september-26/>



2025 Minimum Elements for a Software Bill of Materials (SBOM)

Public Comment Draft
August 2025
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

About this draft: This is a pre-decisional draft for public comment. It does not represent the final position of the U.S. Government and is continuing to undergo updates as feedback is received.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [Traffic Light Protocol \(TLP\) Definitions and Usage](#).

TLP:CLEAR

● 概要

- ドイツ 連邦セキュリティ室 (BSI)が出しているCRAガイドライン(製造業者と製品)の2章(SBOM)についての紹介

● ドキュメントリンク

- https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03183/TR-03183_node.html
- Part 2: Software Bill of Materials (SBOM)参照

● ドキュメントの位置づけ

- このガイドラインはあくまで、BSIから出されている“信頼できる推奨事項”というものであり、**強制力は持たない。**
- CRA(Cyber Resilience Act)に準拠するための**要件を保証するものではない。**



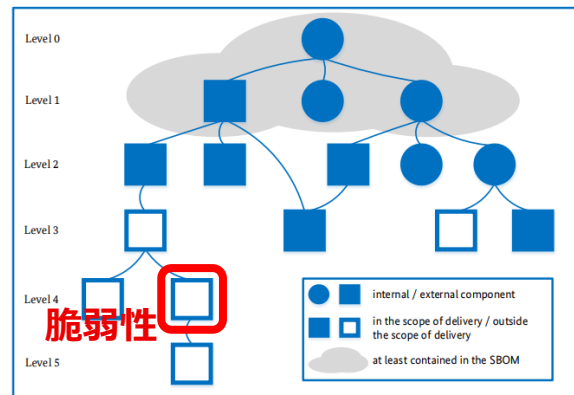
● SBOMの依存関係の深さについて

- CRAの要件としては、製品のトップレベル依存関係をカバーする必要あり
- BSIの見解としては、トップレベルのSBOMだけでは脆弱性管理に不十分（理由：脆弱性が下位レベルの依存関係に存在している場合、トップレベルSBOMではそれを検出できないため）



- 標準化の作業は現在進行中であり、EU欧州委員会が調整を進めている。標準化の方向性によって、SBOMの要件も調整される可能性がある。（深さについてBSI内部で議論中）

トップレベルSBOMでは脆弱性が検出できない例[*3]



[*3] 出典：BSI TR-03183-2 version 2.0.0 (Figure 1: Top-level SBOMより一部改変)

- **質問: ENISAやBSIがTR-03183-2をEUレベル(CRA)に持ち込むことに興味があるか？**
- **回答: 明言は避けていた。興味があることを示唆。**
- **質問: 市場監視当局がまだ決まらない理由や次のステップについての詳細は？**
- **回答: 理由についての回答はなし。次のステップとしては、今まで通り「信頼できる推奨事項」を提供し続けることが現時点でのBSIの方針。**

- インド政府 電子情報技術省にある機関CERT-Inが発行したSBOMガイダンス

- CERT-Inは、非規制当局だが各省庁に影響力のある技術ガイダンスを出せる立場
- 対象BOM : SBOM, QBOM(量子), CBOM(暗号), AIBOM(AI), HBOM(Hardware)
- 各コンポーネントに紐づく脆弱性情報を項目として持つことを求めている。(VEX, CSAF連携推奨)

コメント

インドでは、VEXを要求しているが、国によっては、反対意見がでるかもしれないとの意見。



Technical Guidelines on
| SBOM | QBOM & CBOM | AIBOM | HBOM |
Version 2.0

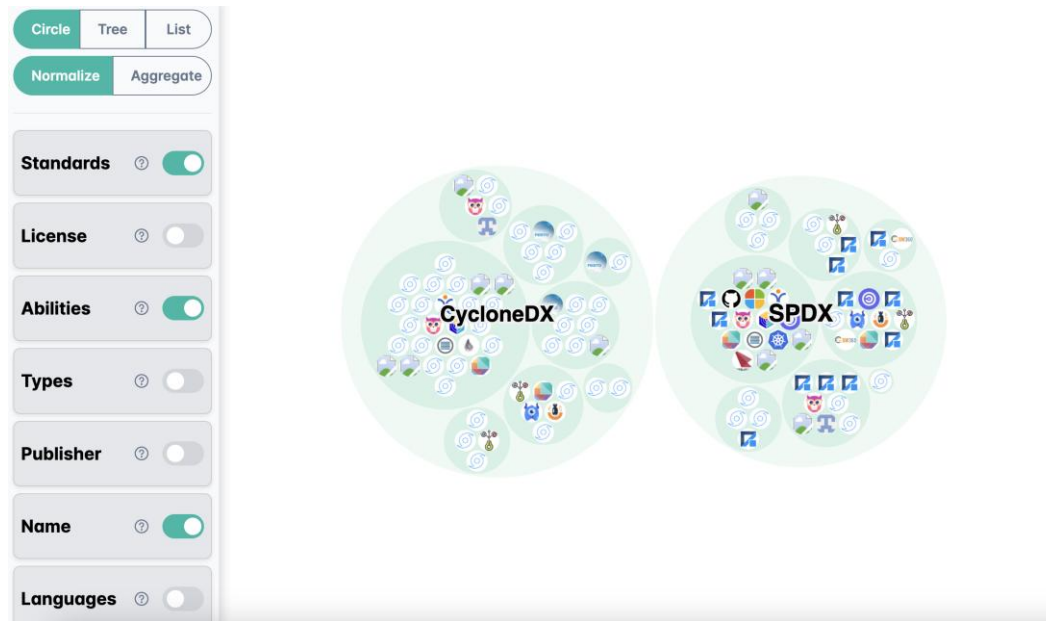


Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Version 2.0 Dated 09.07.2025

- SBOM Everywhere SIGでは、SBOM Catalogをリリース

Let's DEMO



References

- SBOM Catalog
 - <https://sbom-catalog.openssf.org/>
- SBOM関連ツールの一覧情報が絵でわかる！SBOM-Catalogの紹介
 - <https://qiita.com/flying-pan/items/2f48237e144e783f9dbc>

小話 (知らない海外の方々とのオンラインミー ティング)

- The slides have been replaced, but I hope the memories of that presentation still live in everyone's heart.

なんとかなる

- SBOM関連イベントの開催告知の情報が入手できること
- Draft段階のコミュニティ資料にアクセスできること
 - ドキュメントの閲覧
 - レビューの参画
- 中の人々の現場でしか知らない情報が聞けること
- オフラインのOSSイベントで直接あった時に感動が得られる

- OpenSSF SBOM Everywhere SIGへの参加お待ちしております。



- とりあえず興味のある日本のOSSコミュニティにふれてみる
 - コミュニティのSlack/Discord に入ってみる
 - メーリングリスト登録してみる
 - 無料のオフラインのイベントから参加してみる

↓
- 可能なら、日本の仲間をつくる
 - 心理的安全性UP ↑ ↑
 - 情報収集

学生さんにむけて

●情熱をもちつづける

- 自発的に動ける領域を発掘する（興味のあることは、早々見つからないので、最初はなんとなくでふれてみるのがよろし）

●英語

- 最初は、OSSドキュメントやslack, メーリングリストからふれてみる。機械翻訳を駆使してOK。
- 今携わっている専門分野で、学内の外国人と議論してみる。LLMのサポートがない状況（相手が目の前にいるところ）で、即座のやり取りができることが重要。

●コミュニティにふれる/参加し続ける

- 無料で開催されているMeetupに参加
- Meetup後の飲み会（強制ジャナイヨ）に参加
- アウトプット
 - 他人の発表のQA
 - パッチコントリビュート
 - OSSカンファレンスで登壇（学生はtravel fund もらいやすい）
 - etc...

●可能ならインターンに行ってみる

- 複数の企業のインターン（一度就職するとできない体験）

● 気になるタレントさんを見つけて動向を追ってみる

- イベントに参加
- 素敵だと思った開発者の経歴をLinkedInで確認
- 直接実際に話を聞いてみる（どういう状況（性格・職場・対象）で、「没頭できる」「情熱を持てる」「コラボできる」となっているのかを、自分なりに組み立てていく）

スタートダッシュで差を付けるよりも、
お仕事人生そのあとも4,50年は続くわけで、大コケしなければ
あとの方が重要です(`・ω・´)b

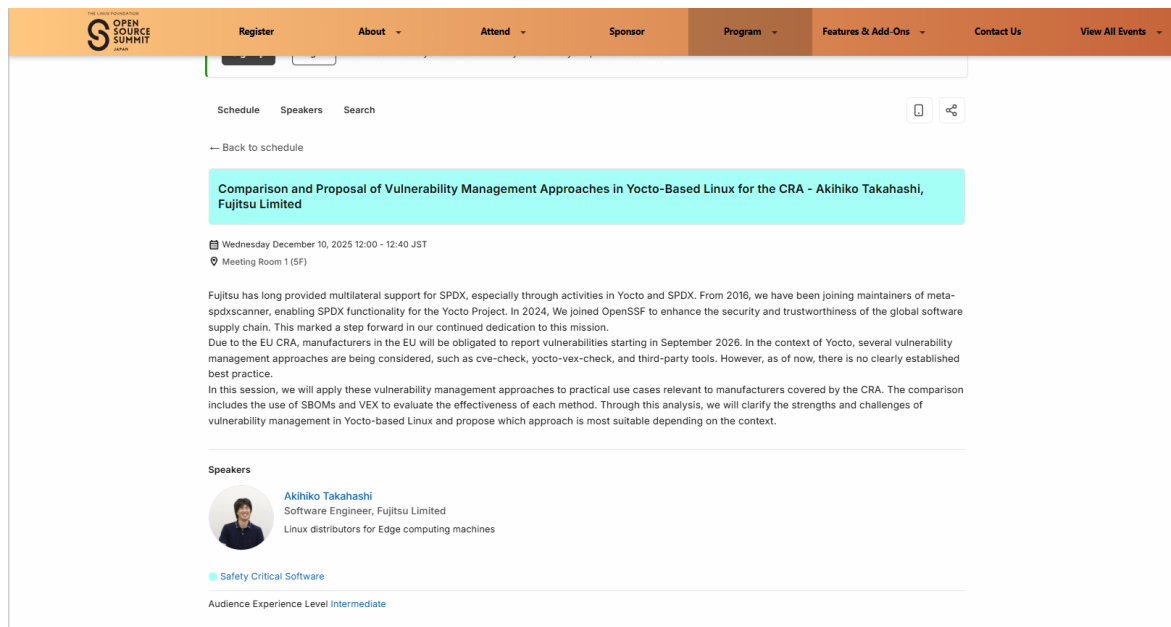
結局は、度胸と愛嬌

らしいです…

OpenSSF Japan WG & 弊社内メンバ5名からのことばでした。

- CRA法案対応にむけたYoctoベースLinuxの脆弱性管理方法の比較と提案

- <https://sched.co/29Fpd>



The screenshot shows the event page for the Open Source Summit Japan 2025. The session title is "Comparison and Proposal of Vulnerability Management Approaches in Yocto-Based Linux for the CRA - Akihiko Takahashi, Fujitsu Limited". It is scheduled for Wednesday, December 10, 2025, from 12:00 to 12:40 JST in Meeting Room 1 (5F). The description states that Fujitsu has long provided multilateral support for SPDX, especially through activities in Yocto and SPDX. From 2016, they have been joining maintainers of meta-spdxscanner, enabling SPDX functionality for the Yocto Project. In 2024, they joined OpenSSF to enhance the security and trustworthiness of the global software supply chain. This marked a step forward in their continued dedication to this mission. Due to the EU CRA, manufacturers in the EU will be obligated to report vulnerabilities starting in September 2026. In the context of Yocto, several vulnerability management approaches are being considered, such as cve-check, yocto-vex-check, and third-party tools. However, as of now, there is no clearly established best practice. In this session, they will apply these vulnerability management approaches to practical use cases relevant to manufacturers covered by the CRA. The comparison includes the use of SBOMs and VEX to evaluate the effectiveness of each method. Through this analysis, they will clarify the strengths and challenges of vulnerability management in Yocto-based Linux and propose which approach is most suitable depending on the context.

Speakers

-  **Akihiko Takahashi**
Software Engineer, Fujitsu Limited
Linux distributors for Edge computing machines

 Safety Critical Software

Audience Experience Level *Intermediate*



Thank you

