オープンソースソフトウェアをより安全にするための取組み

Yoshiya ETO
Fellow, The Linux Foundation
Oct. 2022

THE LINUX FOUNDATION

本日の内容: 主にオープンソース開発視点の脆弱性対応

- オープンソースソフトウェア利用状況
- オープンソースの脆弱性と影響
- オープンソースコミュニティとしての脆弱性対策
- 脆弱性対策に対する一考察

自己紹介

Linux Foundation Leadership Teams

LEADERSHIP | BOARD OF DIRECTORS | **FELLOWS** | ADVISORY BOARD

GREG KROAH-HARTMAN
Fellow

JANINA SAJKA
Fellow

LINUS TORVALDS
Fellow

RICHARD PURDIE
Fellow

SHUAH KHAN
Fellow

THOMAS GLEIXNER
Fellow

TILL KAMPPETER
Fellow

YOSHIYA ETO
Fellow

THE LINUX FOUNDATION

The Linux Foundationご紹介

- 2007年設立時のメンバー/活動領域
  - 主要メンバー: Fujitsu, Hitachi, HP, IBM, Intel, NEC, Oracle
  - 活動領域: promote, protect, and advance Linux
- 2022年の状況

2,300+
メンバー企業
（41か国から）

100%
Fortune 100
Tech&Telecomから

740,000+
コードを貢献する
開発者

800+
オープンソース
プロジェクト

$100B
共有技術の
資産価値

対象プロジェクト: さまざまな技術分野・業種

THE LINUX FOUNDATION

技術分野

セキュリティ	Let's Encrypt, CORE INFRASTRUCTURE INITIATIVE, OpenSSF, Falco, ./rtp, CONFIDENTIAL COMPUTING CONSORTIUM, seL4, OPEN SECURITY CONTROLLER
ネットワーク	LF NETWORKING, OPEN DAYLIGHT, .io, CLUSTERDUCK PROTOCOL, DENT, DANOS, AKRAINO
クラウド	CLOUD NATIVE COMPUTING FOUNDATION, kubernetes, argo, envoy, KUDO, Crossplane, soda foundation, CLOUD FOUNDRY, Istio
ブロックチェーン	HYPERLEDGER, HYPERLEDGER FABRIC, ACCORD PROJECT, ERGO, DIF
エッジ/IoT	LF EDGE, yocto PROJECT, Zephyr, ACRN, Dronecode, FLEDGE, SOUND OPEN FIRMWARE, OpenEEW
Web	node JS, OpenJS Foundation, GraphQL, appium, jQuery, REACTIVE FOUNDATION, DOJO, ESLint
AI	LF AI, ONNX, DELTA LAKE, ForestFlow, JanusGraph, kepler.gl, LUDWIG, PyTorch
CI/CD	CD FOUNDATION, Jenkins, Spinnaker, TEKTON, TERN, StackStorm, Vitess, etcd, SPIRE
ハードウェア	RISC-V, OpenPOWER, CHIPS ALLIANCE, UNIMATRIX, 3MF CONSORTIUM
標準	ALLIANCE FOR OPEN MEDIA, OPENCHAIN, COMMUNITY DATA LICENSE AGREEMENT, JOINT DEVELOPMENT FOUNDATION, SPDX, OPEN MANUFACTURING PLATFORM, OPEN CONTAINER INITIATIVE

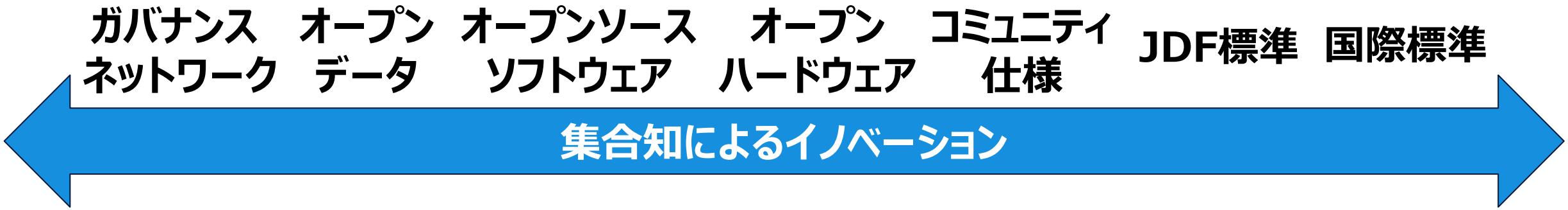
業種

自動車	AUTOMOTIVE GRADE LINUX, ELISA, KernelCI
エネルギー	LF ENERGY, RIAPS, EM2, POWSYBL, GXF, CoMPAS, OPENEEMETER, OPERATORFABRIC
フィルム/映画	ASWF, OpenColorIO, OpenVDB, OpenEXR, OpenTimelineIO, OpenEXR, OSL Open Shading Language
金融/財務	FINOS, EGEND, FDC³, CLOUD SERVICE CERTIFICATION, FATE, PERSPECTIVE, openMAMA, morphir
通信	ONAP, Anuket

The Linux Foundationのプロジェクトで行われていること

- プラットフォームソフト・データをオープンソース化: 重要だが競争領域でない
  - 共通技術で製品差異化/ベンダーソリューションを極小化
    ⇔自社でオープンソースエンジニアを抱えて最大限の価値教授
- 他社と共同開発: ダーウィンの進化論的開発モデル
  - 複数のアイデアを混ぜ合わせて独自な進化/自由に作れない
    他社アイデアでエコシスム拡大する場合もある: K8sのgoogle内議論

オープンコラボレーションに幅広い役割



参画に必要な経験知:

法的な調整や構造
業界別の経験
技術分野毎の経験
成功の実績

拡大していくために必要な経験知:

セルフサービスオプション
アンブレラと柔軟なプロジェクト構造
メンバーシップモデルとネットワーキング効果
システムとプロセスの注力ポイント
厳格なIP管理とセキュリティの注力ポイント

オープンソースソフトウェア利用状況

THE LINUX FOUNDATION

Auditしたソフトウェアの99%にオープンソースが取り込まれている

Auditしたソースコードのうち70%はオープンソースのコード

Source: 2020 Backduck OSSRA

https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/2020-ossra-report.pdf

オープンソースの脆弱性と影響

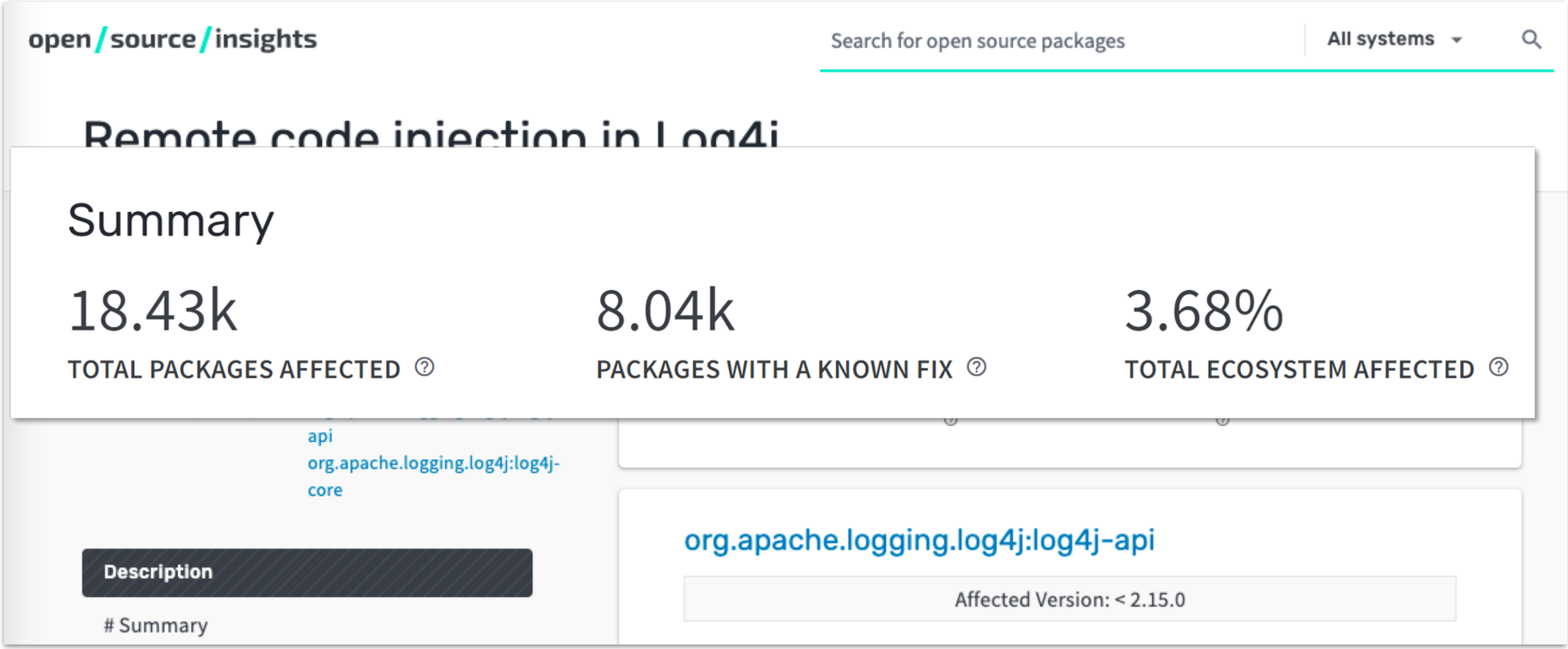
THE LINUX FOUNDATION

- OpenSSL: Heart Bleed: 2013年12月 CVE-2014-0160 record created
- Apache Stratus2: 2017年1月29日 CVE-2017-5638 record created..
- Log4Shell: 2021年11月26日 CVE-2021-44228 record created

オープンソースの脆弱性と経済影響

- Heartbleed=OpenSSLの脆弱性, 2014年4月発覚
  - 三菱UFJニコスのWebから894人分の個人情報流出: 2014/4/18
    source: https://xtech.nikkei.com/it/article/NEWS/20140421/551884/
  - メニコンのWebからクレジットカードなどの個人情報漏洩: 2018/5/17
    source: https://xtech.nikkei.com/atcl/nxt/column/18/00001/00561/
- Apache Struts2: source: https://saas.gmocloud.com/service/websecurity/threat/struts2.html
  ① 国土交通省で約20万件の顧客情報が流出: 2017/6/6
  ② 総務省で2.3万人の個人情報が流出: 2017/4/13
  ③ GMOペイメントゲートウェイが運営しているサイトから個人情報72万件が流出: 2017/4/5
  ④ ぴあが運営するサイトからクレジットカード情報3.2万件が流出の可能性: 2017/3/7
- Log4Shell = Log4jの脆弱性: 進行中

Problem: Scaling up to the Open Source Ecosystem



Source: https://deps.dev/advisory/GHSA/GHSA-jfh8-c2jp-5v3q on 2022/1/10

脆弱性による事故発生の時間感覚

THE LINUX FOUNDATION

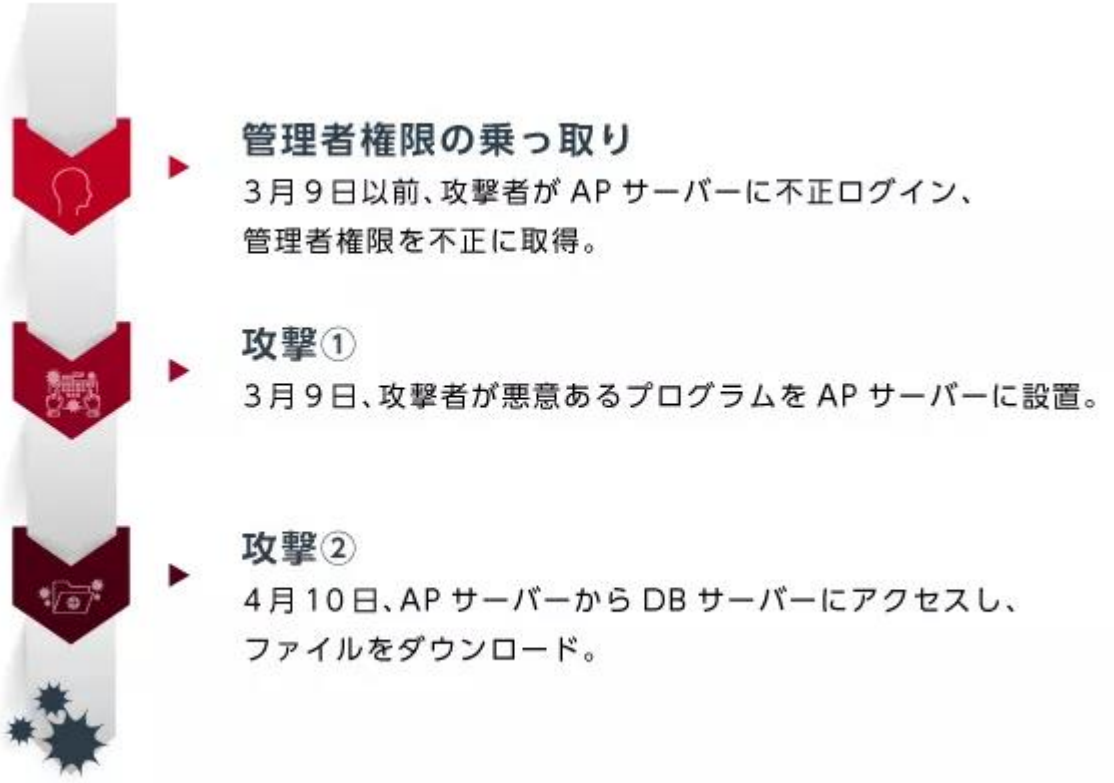
① 国土交通省で約20万件の顧客情報が流出

攻撃の予兆
2017年3月、国土交通省はアンケート回答サイトでの Struts2 使用を確認。

脆弱性を狙った攻撃
2017年3~5月、攻撃者は Struts2 の脆弱性を狙って悪意あるプログラムをサイトに仕込む。

遅れた対応
5月から脆弱性対策のシステム改修を実施。
しかし、すでに攻撃を受けていた。

② 総務省で2.3万人の個人情報が流出



管理者権限の乗っ取り
3月9日以前、攻撃者が AP サーバーに不正ログイン、管理者権限を不正に取得。

攻撃①
3月9日、攻撃者が悪意あるプログラムを AP サーバーに設置。

攻撃②
4月10日、AP サーバーから DB サーバーにアクセスし、ファイルをダウンロード。

source: https://saas.gmocloud.com/service/websecurity/threat/struts2.html

脆弱性による事故発生の時間感覚

THE LINUX FOUNDATION

③ GMOペイメントゲートウェイが運営しているサイトから
個人情報72万件が流出

④ ぴあが運営するサイトから
クレジットカード情報3.2万件が流出

source: https://saas.gmocloud.com/service/websecurity/threat/struts2.html

オープンソースコミュニティとしての脆弱性対策 –第一期

- Core Infrastructure Initiative: Heartbleed及び類似事例対策

  Source: https://internet.watch.impress.co.jp/docs/news/646136.html

  初期メンバー: Amazon Web Services、Cisco、Dell、Facebook、Fujitsu、Google、IBM、Intel、Microsoft、NetApp、Rackspace、VMware

  1. 重要な開発者がフルタイムでオープンソースプロジェクトに取り組むためのフェローシップ、セキュリティ監査、コンピューティングおよびテストインフラ、旅行、対面会議予算
  2. Best Practices Security Badge Program

オープンソースソフトウェア利用者の脆弱性対策 –第二期

› 大統領令により政府調達要件にSBOM必須化: 2021年5月12日に署名

President Biden‘s Cybersecurity Executive Order 14028 any company that sells software to the federal government will be mandated to provide a complete Software Bill of Materials (SBOM)

Open Source Security Summit要約: ホワイトハウス主催

https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

- 本日ホワイトハウスは、政府と民間企業の関係者を招集し、オープンソースソフトウェアのセキュリティを向上させるための取り組みと、新たなコラボレーションによって改善を迅速に進める方法について議論いたしました
- 国家安全保障分野で使用されているソフトウェア含め、主要なソフトウェアパッケージのほとんどはオープンソースソフトウェアを取り込んでいます
  ソフトウェアは、経済の全セクターであらゆる場所に存在し、米国人が毎日使用する製品やサービスの基盤となっています
- オープンソース・ソフトウェアは、独自の価値をもたらすと同時に、その使用範囲の広さと継続的なセキュリティ・メンテナンスに責任を負うボランティアの数から、独自のセキュリティ上の課題も抱えています

Open Source Security Summit要約: ホワイトハウス主催

https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

- 会議には、**Anne Neuberger:** 国家安全保障副顧問（サイバーおよび新技術担当）、**Chris Inglis:** 国家サイバー長官、科学技術政策局、国防総省、商務省、エネルギー省、国土安全保障省、サイバーセキュリティおよびインフラセキュリティ局**(CISA)**、米国標準技術研究所、米国科学財団の職員が参加いたしました
- 民間企業では、**Akamai**、**Amazon**、**Apache Software Foundation**、**Apple**、**Cloudflare**、**Facebook/Meta**、**GitHub**、**Google**、**IBM**、**The Linux Foundation**、**Open Source Security Foundation**、**Microsoft**、**Oracle**、**RedHat**、**VMWare**が参加しています
- バイデン大統領は、ソフトウェアセキュリティを国家的な優先事項としています
  彼のサイバーセキュリティに関する大統領令は、安全なソフトウェア開発ライフサイクル手法を使用し、特定の連邦セキュリティガイダンスを満たした企業のみが連邦政府に販売できるようにすることを要求しています

Open Source Security SummitII要約: 米国行政機関主導

https://www.linuxfoundation.org/press-release/linux-foundation-openssf-gather-industry-government-leaders-open-source-software-security-summit/

- 本会合は米国行政機関主導のもと、**The Linux Foundation**が主催しました
  米国政府機関**(NSC, ONCD, CISA, NIST, DOE, OMB)**及び主要企業**37**社**90**名が参加
- **LF**と**Open Source Security Foundation**は様々な経済セクターから情報提供を受け、**OSS**とソフトウェアのサプライチェーンセキュリティに幅広く対応する初の実践計画を発表
- この計画では**3**つの目標に対する**10**の主要な問題が明らかにされ、解決策実践には、**2**年間で約**1**億**5**千万ドルの資金が必要
  I. セキュアな **OSS** の開発・提供
  II. 脆弱性検出と修復方法の強化
  III. エコシステムにおけるパッチ適用までの時間短縮
- 実践に向け**Amazon,Ericsson,Google,Intel,Microsoft,VMWare**が**3,000**万ドル以上の資金提供
- **OpenSSF**参画企業が **1**億**1000**万ドル以上かけ 実践中の**OSS**セキュリティ対策活動に積み重ねる形で推進

Open Source Security Summit Japan: 2022/8/23

- 経済産業省サイバーセキュリティ・情報課　上村審議官
- 米国ホワイトハウスの国家サイバー長官　**Chris Inglis**
- **The Linux Foundation: Jim Zemlin, OpenSSF: Brian Behlendorf**
- 参加企業: **20**社以上の企業・団体が出席
  - 日立製作所、富士通、**NEC**、**NTT**データ、トヨタ、**LINE**、産総研、**IPA**他

3つの目標

THE LINUX FOUNDATION

1. **OSS開発をセキュアにする**
   - コードとオープンソースパッケージのセキュリティ上の欠陥や脆弱性の防止に注力
2. 脆弱性の検出と修復の強化
   - 欠陥の検出、それらを修正するプロセスの強化
3. エコシステムのパッチ応答時間を短縮
   - 修正の配布、実装のための応答時間を短縮

OSS開発をセキュアにする

THE LINUX FOUNDATION

ストリーム 1：基本基準を満たすセキュアなソフトウェア開発の教育と認定 をすべての人に提供

- **Developing Secure Software (LFD121)**
- **Secure Software Development: Requirements, Design, and Reuse (LFD104x)**
- **Secure Software Development: Implementation (LFD105x)**
- **Secure Software Development: Verification and More Specialized Topics (LFD106x)**

ストリーム 2：10,000以上のOSS コンポーネント対象にリスク評価パブリックダッシュボード開設

- ベンダー中立な指標に基づくリスク評価パブリックダッ シュボード: **LFX.io**

ストリーム 3：ソフトウェアリリースでのデジタル署名の採用を加速

- **Free sigstore Signing Service to Confirm Origin and Authenticity of Software**

ストリーム 4：メモリセーフでない言語を置き換えることで、多くの脆弱性の根本原因を排除

脆弱性の検出と修復の強化

ストリーム 5： OpenSSF内にOpen Source Security Incident Response Team設立

- クリティカルな脆弱性対応時、セキュリティの専門家がオープンソースプロジェクトを支援

ストリーム 6：メンテナーと専門家による新しい脆弱性の検出加速

- 高度なセキュリティツールと専門家のガイダンスをメンテナーに提供

ストリーム 7：1 年に1 度/最大200のクリティカルOSSコンポー ネントをサードパーティコードレビュー

ストリーム 8：クリティカルなOSS コンポーネント決定調査の改善のため、業界全体でデータ共有

エコシステムのパッチ応答時間を短縮

ストリーム9：あらゆるところにSBOMを

- SBOMツールとトレーニングを 改善し採用を促進: SPDX, OpenChain認証

ストリーム 10：最もクリティカルな10のOSS ビルド システム、パッケージマネージャー、およびディストリビューションシステムを強化

オープンソースソフトウェア業界のSBOMの意味

- オープンソースソフトウェアのライセンス間の矛盾
  - 有名な事例: **GPL v.s.** 昔の**BSD**ライセンス
    - **GNU GPL**の第**6**項抜粋
      You may not impose any further restrictions on the recipients' exercise of the rights granted herein.
    - 昔の**BSD**ライセンス
      All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
  - **Apache Software Foundation Web**サイト: **GPLv2**と**Apache License ver2.0**は両立しない
- **Copyleft**
  - インストール条項のあるライセンス: **GPL v.3**
- 商用に使えないライセンス

古からオープンソースを商用利用するには、ライセンス管理する必要があった

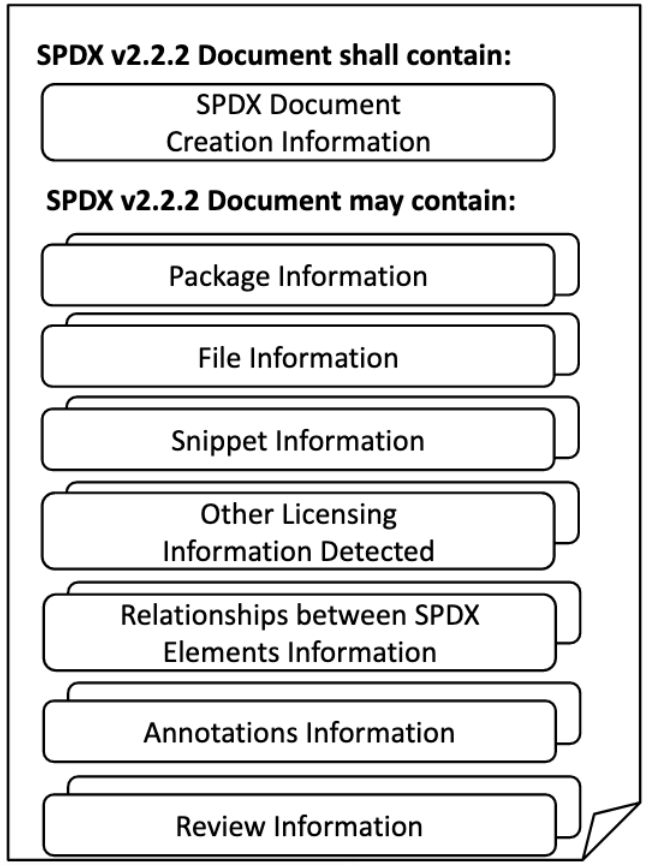
ライセンスを遵守するためのツール

THE LINUX FOUNDATION

SPDX: Software Package Data Exchange

ゴール:　ソフトウェアサプライチェーンを効果的に機能させるため、人間が読め・機械が処理できるソフトウェアパッケージのメタデータを企業・組織が共有できるデータ交換標準セットを作る

- Standard for communicating the component and metadata information associated with software
- 2011年8月に第一版リリース: 日本企業がオープンに企業間協業で貢献する珍しい事例
- 組込みソフトウェア開発ツールとして進化: ISO/IEC 5962:2021
- 提供ツール: SPDX License List, spdx-tools
- SPDX Document:　ライセンス表示する標準フォーマットで記載



SPDX Specification History

- **2010/02** - specification drafting began in a work-group of FOSSBazaar under Linux Foundation that came to be called "SPDX"
- **2010/08** - "SPDX" announced as one of the pillars of the Linux Foundation's Open Compliance Program
- **2011/08** - SPDX 1.0 specification - handles packages
- **2012/08** - SPDX 1.1 specification - fixed flaw in verification algorithm
- **2013/10** - SPDX 1.2 specification - improved interaction with license list, additional fields for documenting project info
- **2015/05** - SPDX 2.0 specification - added ability to handle multiple packages, relationships between packages and files, annotations
- **2016/08** - SPDX 2.1 specification - added snippets, support for associating packages with external reference sources of information about packages, using SPDX License identifiers in files
- **2019/06** - SPDX 2.1.1 - conversion of specification from google docs to github as repository
- **2020/05** - SPDX 2.2 - include SPDX-Lite, more relationships, etc.
- **2020/08** - SPDX 2.2.1 - reformatting and prepared for submission to ISO.
- **2021/08** - ISO/IEC 5962:2021 published

NTIA SBOM Guidance

Minimum Elements	
Data Fields	Document baseline information about each component that should be tracked: Supplier, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of SBOM Data, and Timestamp.
Automation Support	Support automation, including via automatic generation and machine-readability to allow for scaling across the software ecosystem. Data formats used to generate and consume SBOMs include SPDX, CycloneDX, and SWID tags.
Practices and Processes	Define the operations of SBOM requests, generation and use including: Frequency, Depth, Known Unknowns, Distribution and Delivery, Access Control, and Accommodation of Mistakes.

Source:https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.

NTIA SBOM Guidance - Minimum Elements

THE LINUX FOUNDATION

Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

SPDX 2.2 (ISO/IEC 5962:2021) supports all required minimum elements!

and much, much more!

Source:https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf.
See also US Executive Order on Cybersecurity section 4(f)

SPDX Document例: 一部抜粋

THE LINUX FOUNDATION

SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: hello
DocumentNamespace: https://swinslow.net/spdx-examples/example1/hello-v3
Creator: Person: Steve Winslow (steve@swinslow.net)
Creator: Tool: github.com/spdx/tools-golang/builder
Creator: Tool: github.com/spdx/tools-golang/idsearcher
Created: 2021-08-26T01:46:00Z

Package: hello

PackageName: hello
SPDXID: SPDXRef-Package-hello
PackageDownloadLocation: git+https://github.com/swinslow/spdx-examples.git#example1/content
FilesAnalyzed: true
PackageVerificationCode: 9d20237bb72087e87069f96afb41c6ca2fa2a342
PackageLicenseConcluded: GPL-3.0-or-later
PackageLicenseInfoFromFiles: GPL-3.0-or-later
PackageLicenseDeclared: GPL-3.0-or-later
PackageCopyrightText: NOASSERTION

Source: https://github.com/spdx/spdx-examples/blob/master/example1/spdx/example1.spdx

SPDXの今後の仕様拡張

- SPDX 3.0で拡張を予定している項目
  - Licensing profile
  - Defects profile
  - Usage profile
  - Build profile
  - AI model & application profile
  - Dataset profile
- SPDX 3.0は2023年にISO認証取得の見込み

ライセンスを遵守するためのプロセス/教育

- **OpenChain: ISO/IEC 5230:2020**
  - 本規格は全てユーザーコミュニティによってオープンに開発
  - 誰でも自由に利用可能
  - 無料のオンライン自己認証/認証機関による認証
  - 特定の組織を認証: 38項目の遵守事項　以下一部のみ抜粋
    - 供給ソフトウェアのリリースに含まれるすべてのオープンソースコンポーネントに関する情報を特定し、追跡し、リストとして保管するための手順書がありますか？
    - 手順書に適切に従っていることを証明する、各供給ソフトウェアのリリースに関するオープンソースコンポーネントの記録がありますか？
    - 確認ライセンスの要求に基づいて、コンプライアンス関連資料が供給ソフトウェアとともに頒布されることを確実にするプロセスを説明した手順書がありますか？
    - すべてのソフトウェアスタッフにオープンソースポリシーの存在を伝える手順書がありますか？
    - プログラムの性能と有効性に影響のある役割とそれに対応する責任について明確にしていますか？
    - 各役割に必要な能力を特定し、文書化していますか？
    - 各プログラム参加者の能力を評価した証拠を文書化していますか？
    - オープンソースコンプライアンスに関する外部からの問い合わせに対応する責任者（「オープンソース窓口」）を指名していますか？
    - 特定されたプログラムの役割をサポートする人、グループ、または部署を文書化していますか？
    - 特定されたプログラムの役割には、適切に人員が配置され、十分な予算が当てられていますか？

Global Third Party Certification (Mar 2019~)

THE LINUX FOUNDATION

Third-Party Certifiers

BUREAU VERITAS
CAICT 中国信通院
ISCAS
ORCRO
pwc
SYNOPSYS
TÜV SÜD

脆弱性による事故に対する考察: セキュリティ修正適用

- 本当に危ないのは何なのか??
  脆弱性に起因する事故が後を絶たないのはなぜか?
- **Security Problems Are Primarily Just Bugs -- Linus Torvalds**
- https://github.com/kubernetes/committee-security-response/blob/main/private-distributors-list.md
- **LFX.io: 2023年中に主要オープンソースのバグ対応状況見れるようになる計画**

ありがとうございました

THE LINUX FOUNDATION