【MTG】
OSSのセキュリティ・ライセンスリスクを回避してOSSを有効活用するには

2021年10月22日(金) 13:00~13:45

NEC 先端SI技術開発本部 OSS推進センター
米嶋 大志

自己紹介

- 氏名：米嶋 大志（よねしま たいし）

- 所属： NEC
  先端SI開発本部　OSS推進センター

- 社内の業務：NECグループへのOSS活用促進
  OSSリスク検出ツールの社内促進＆製品担当

- コミュニティ参加：日本OSS推進フォーラム
  OpenChain JapanWG

年度	業務
入社 2015年度～	BigData系OSS検証
2016年度～	社内OSS活用支援 日本OSS推進フォーラム
2018年度～	同上 ＋OSSリスク検証ツール関係
2019年度～	同上 +OpenChain JapanWG

OSS推進センター 社内での役割

社長

取締役会

- クロスインダストリーユニット
- グローバルビジネスユニット
  - RHQ（地域統括会社）
- 社会公共ビジネスユニット
  - 支社・支店
- 社会基盤ビジネスユニット
- エンタープライズビジネスユニット
- ネットワークサービスビジネスユニット
- デジタルサービス & エンジニアリングユニット
- デジタルビジネスプラットフォームユニット
- システムプラットフォームビジネスユニット
- グローバルイノベーションユニット
- コーポレート

(2021年4月1日現在)

Table of Contents

本題にはいる前に…

Q. 世の中にはいくつのＯＳＳがあるだろう？

① ~1,000　　② 1,000~　　③10,000~　　④100,000 ~　　⑤1,000,000~

A. ④か⑤

- Githubに登録されているリポジトリ数：1億
  Github. リポジトリ数が1億件に達しました！.https://github.blog/jp/2018-11-09-state-of-the-octoverse/　(2018.11)
- Open Hubに登録されているProject数：490,380
  Synopsys BlackDuck OpenHub. https://www.openhub.net/ (2021.10)
- SourceForgeに登録されているProject数：110,000
  SourceForge.net. https://sourceforge.net/ (2021.10)

OSSの粒度

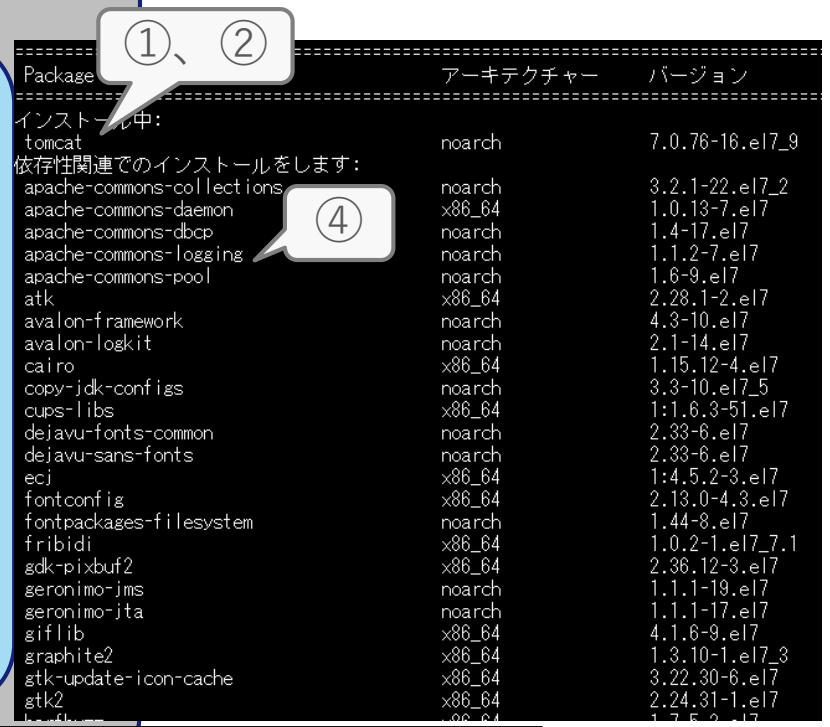
⑤ 世の中の有象無象
:1億～

④ ソフトウェアに関連する
依存パッケージを含むソフトウェア
(RHEL8.4の場合7,944,903)

③ リポジトリサイトに登録されるソフトウェア
：100,000～

② インストール作業で指定する単位

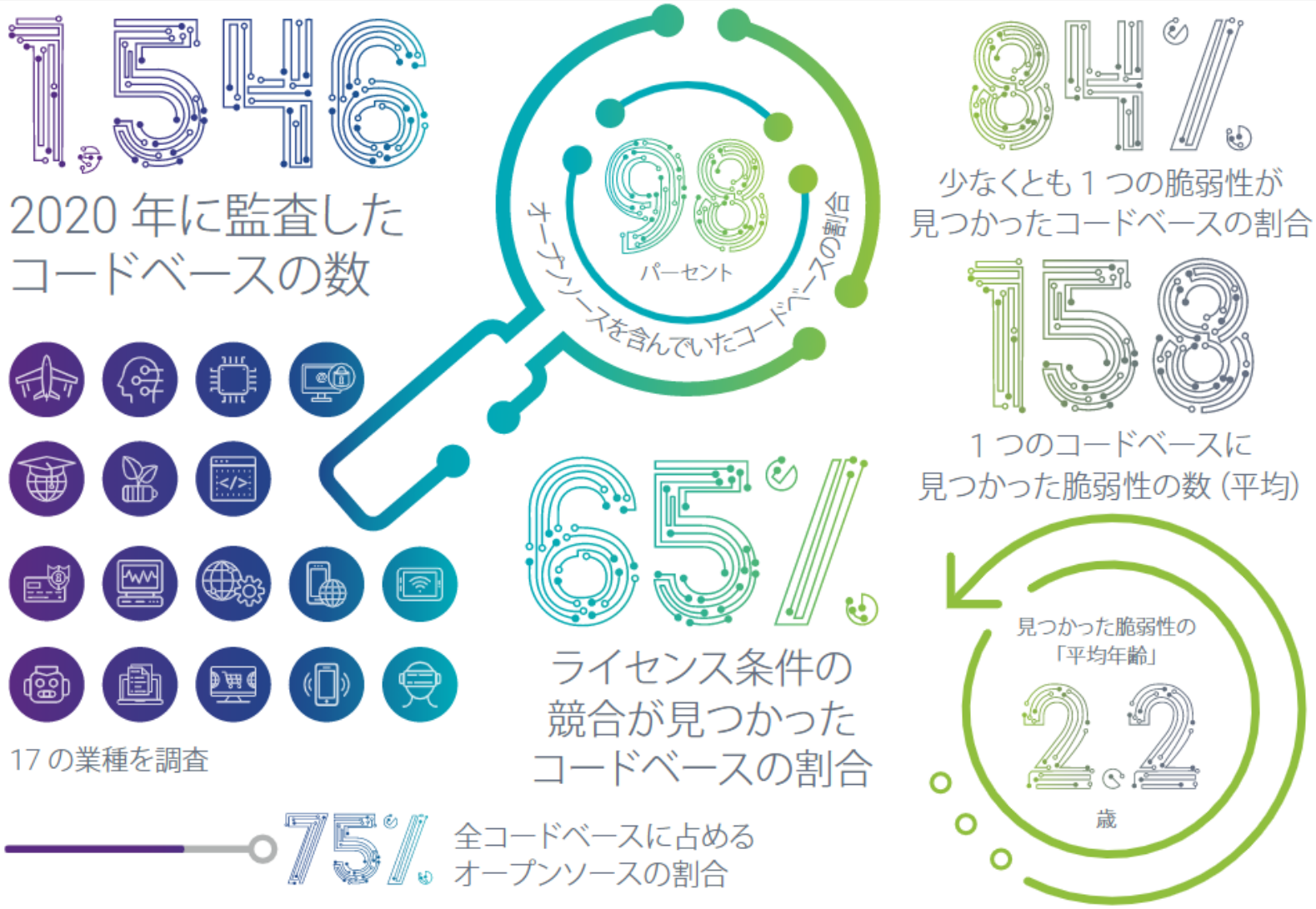
① 会議で名前が出る単位



OSSだと思われている範囲は①～②、③の一部くらい？
意外と少ないと思っている人が多いのでは。

一般的なOSSのリスクとは

第三者情報：2020年OSSライセンス、脆弱性の状況



オープンソース・セキュリティ＆リスク分析レポート（2021年5月公開）.
https://www.synopsys.com/ja-jp/software-integrity/resources/reports/open-source-security-risk-analysis.html

OSS利用におけるリスク

OSSライセンス違反による

著作権侵害・コンプライアンス問題

脆弱性の存在・対策遅れによる

情報セキュリティ事故・情報漏洩

メンテナンス不備・バグの放置による

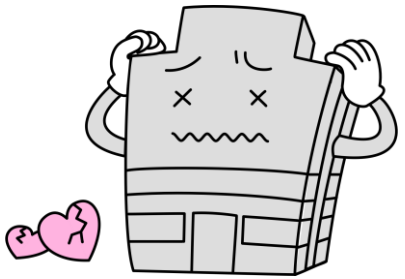
障害の発生・今後の製品アップデートが困難

企業の損失・ダメージ

刑事罰、賠償・訴訟

製品出荷停止の損害

ブランドイメージの低下



OSSライセンスの違反事例

著作権侵害・コンプライアンス問題

製品の一部にGPL(=OSSのメジャーなライセンスの1つ。OSS部分と組み合わせて動作する自製部分も含めたソース開示が必要)のOSSを利用したが、ライセンスの定めている条件を満たしていなかった

国内

- 掲示板等でOSSライセンス違反を指摘された事例
  T社:MP3プレーヤー、S社:プレイステーション2用ゲーム

海外

- 著作権侵害により提訴され、多額の費用を支払うことになった事例
  SFLCとBusyBox:ユーティリティツール
- 開発業者・開発依頼元それぞれで確認をしたが、OSSライセンス違反に気づかなかった事例
  米マイクロソフト社「USB版Windows 7」作成ツール

企業の損失・ダメージのリスク

- 刑事罰、賠償・訴訟費用
- 製品出荷停止の損害
- ブランドイメージの低下

OSS脆弱性に起因する個人情報漏えい事例

情報セキュリティ事故・情報漏洩　**障害の発生・今後の製品アップデートが困難**

脆弱性を突いた攻撃で不正アクセスされ、個人情報が漏えいした

- 2014/04　M社）OpenSSLの脆弱性を突かれ不正アクセス
  - 日本で初「Heartbleed」の悪用
  - 顧客情報の漏えい
- 2017/03　G社等）Apache Strutsの脆弱性を突かれ不正アクセス
  - 脆弱性発覚後10日程度で7組織、
    計約72万件以上の個人情報が流出
- 2019/11　PHP脆弱性狙うランサムウェア攻撃
  - ランサムウェア「NextCry」のサーバへ攻撃

企業の損失・ダメージのリスク

- 刑事罰、賠償・訴訟費用
- 製品出荷停止の損害
- ブランドイメージの低下

OSSコンプライアンスに関する世間の動向

サプライチェーン上での問題の連鎖

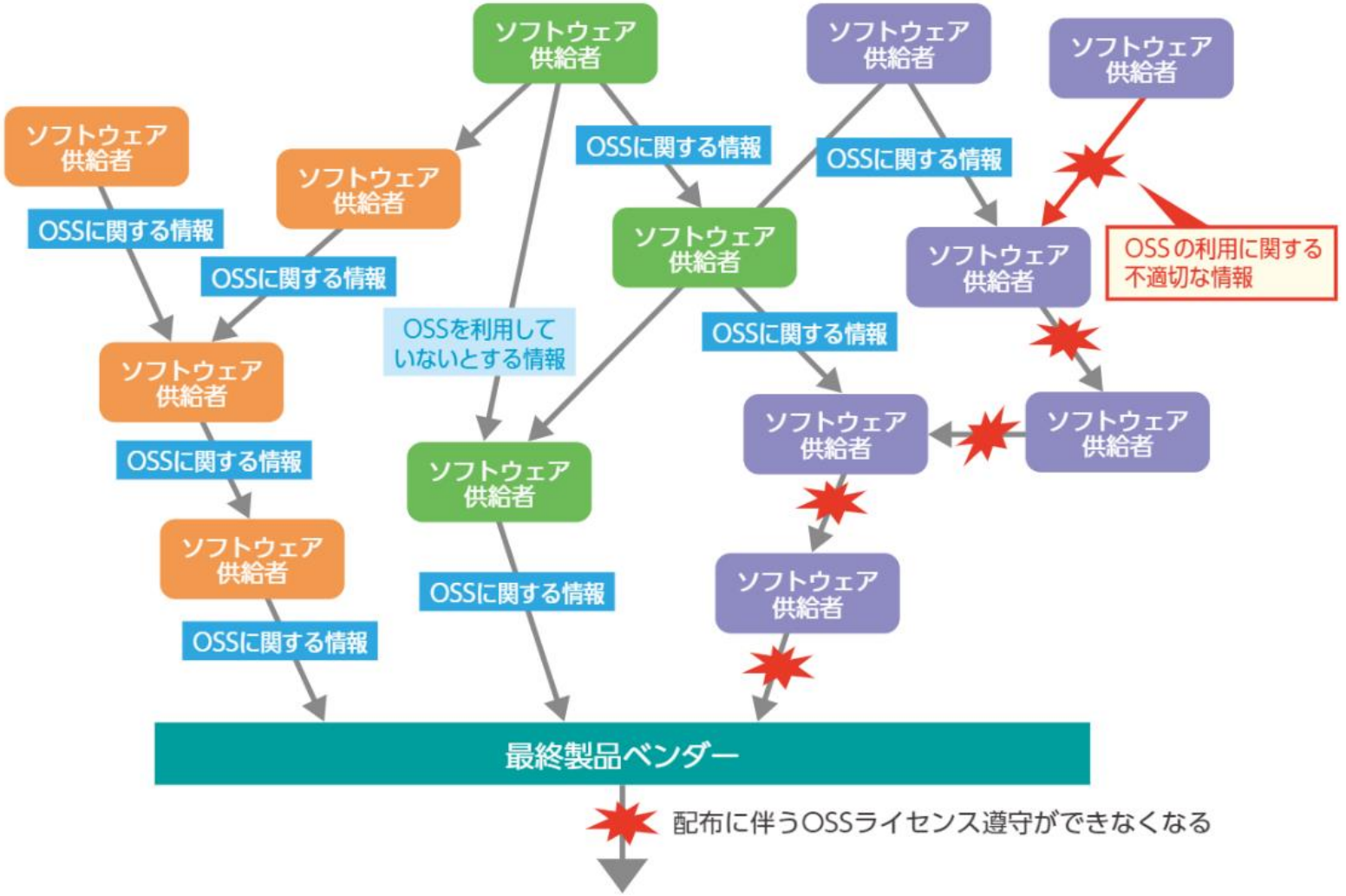


図1　サプライチェーン問題の発生

オープンソースソフトウェアライセンス遵守に関する一般公衆ガイド.
https://github.com/OpenChain-Project/Curriculum/blob/master/supplier-leaflet/supplier-leaflet-1.0-ja.pdf

コンプライアンス観点

OpenChain認証取得が日本発の動きとして世界にひろがりつつあり

- OpenChain(ISO/IEC 5230:2020)とは
  - 主にOSSコンプライアンス観点でソフトウェアサプライチェーン参加企業が満たすべき事項を明文化したもの

- 大企業中心に認証取得の動きが広がっている
  - BOSCH、CISCO、IBM、Microsoft、SONY、TOYOTA

世間的な動向

「国家のサイバーセキュリティ改善に関する大統領令」とは

「国家のサイバーセキュリティ改善に関する大統領令」は、一連のセキュリティ事件(SolarWinds社の大規模な情報漏えい事件やColonial Pipeline社のサイバー攻撃など)を受けて発表されたものです。この大統領令には、連邦政府および連邦政府と連携する民間業者が満たすべき高度なセキュリティ基準が以下の7つの側面から示されています。

- 脅威情報の共有を阻む障害を取り除く
- 連邦政府のサイバーセキュリティの近代化
- ソフトウェアのサプライチェーンセキュリティの強化
- 政府が運営するサイバー安全審査委員会の設立
- サイバーセキュリティの脆弱性やインシデントに対する政府の対応の標準化
- 政府のネットワークにおける脆弱性と問題の検出の強化
- 調査および修復能力の向上

ここで注目したいのは「ソフトウェアのサプライチェーンセキュリティの強化」です。もう少し詳しく言うと「各製品のソフトウェア部品表(SBOM(Software Bill of Materials))を購入者に直接または公開Webサイトで提供すること」を要求しており、「製品の一部に使用されているオープンソースソフトウェアの完全性と出所を実行可能な範囲で確保し、証明すること」が必要となります。また、この大統領令の中で、国家通信情報管理局(NTIA)は最低限のSBOM要件を定義するために幅広く意見を求めています。これに対してLinux Foundationでは「What is an SBOM?」というタイトルで回答しています。

その中で、昨年12月にオープンソースライセンスコンプライアンスに関するISO国際規格(OpenChain)では、提供されたSBOMを管理するプロセスが重要で、これはソフトウェアの透明性を高めるNTIAの目標と一致しており、SBOMのベストプラクティスであると主張しています。

https://thinkit.co.jp/article/18611.
米国のバイデン大統領が署名したことで話題となった「国家のサイバーセキュリティ改善に関する大統領令」とは

本ブログは、*What is an SBOM? (By Shane Coughlan)* の参考訳です。

National Telecommunications and Information Administration (NTIA) は最近、最小限のソフトウェア部品表 (SBOM: Software Bill of Materials) を定義するために、幅広いレベルでのフィードバックを求めました。それは、単純な1つの質問（「SBOMとは何ですか？」）で構成されており、ソフトウェアのセキュリティに関する非常に重要なステップで、かつオープン スタンダードにとって重要な契機になるものです。

NTIAのSBOM FAQには、「ソフトウェア部品表 (SBOM) は、特定のソフトウェア、およびそれらの間のサプライチェーンの関係を構築（たとえば、コンパイルやリンク）するために必要なコンポーネント、ライブラリ、モジュールの完全で、かつ正確に構成されたリストです。これらのコンポーネントは、オープンソースでもプロプライエタリなものでよく、また無償のもでも有償ものでも

https://www.linuxfoundation.jp/blog/2021/07/what-is-an-sbom/.
What is SBOM

SBOM(Software Bill of Materials)とは

集合的ソフトウェアの成分表(ソフトウェアを構成する要素ソフトウェアのリスト)

- SBOMフォーマットは標準化されているものも含め複数あり
  - SWID ISO/IEC 19770-2:2015
  - SPDX ISO/IEC 5960:2021
  - CycloneDX
- 表の要素(用途により議論あり)
  - 開発元
  - 名称
  - バージョン
  - コンポーネント間の関連
  - ライセンス

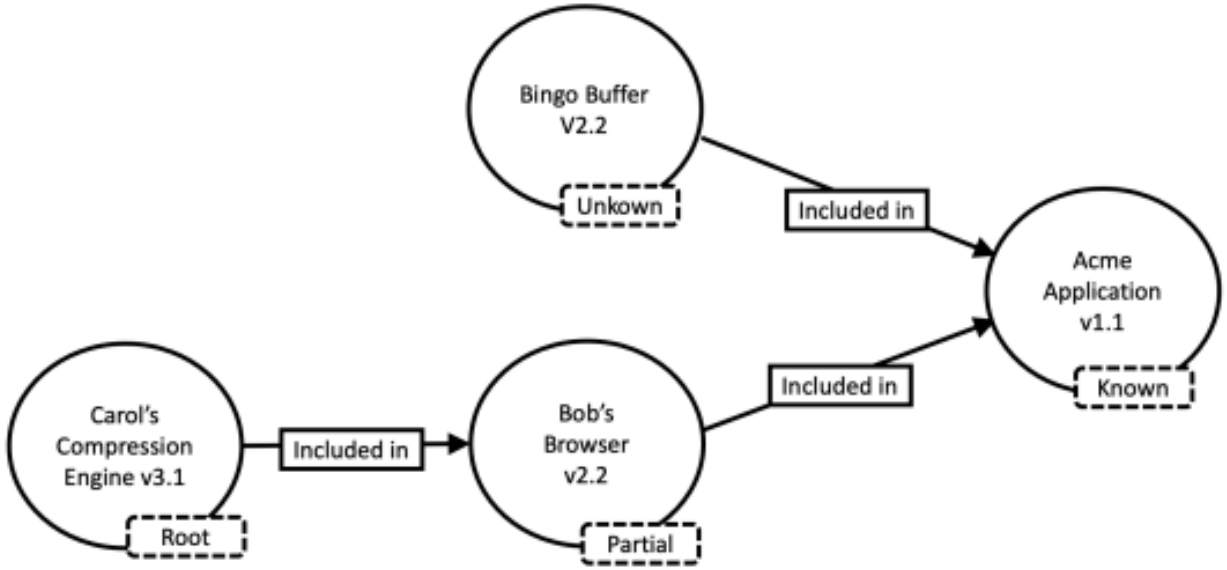


図: コンポーネント間の依存関係を記述したSBOMツリーの例

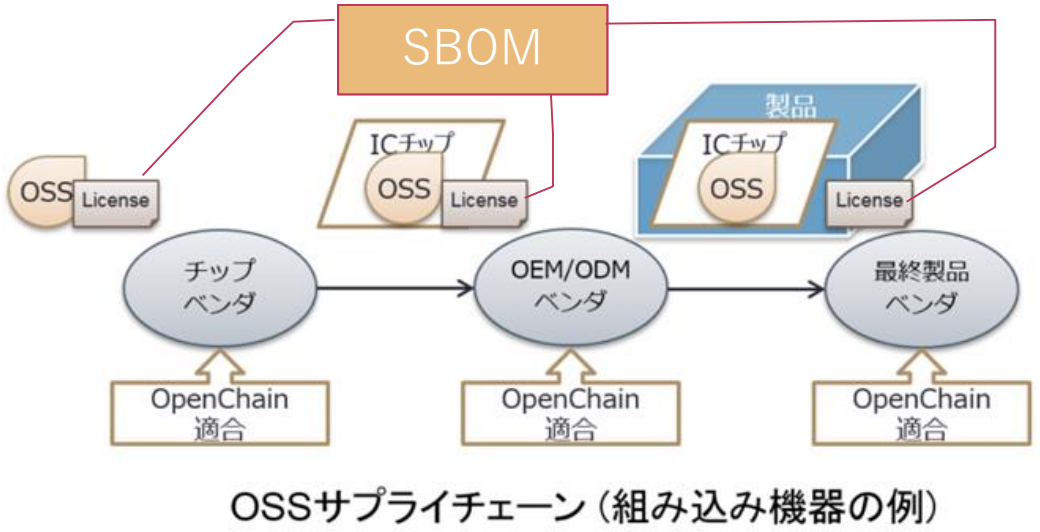
[図の引用元] https://www.ntia.gov/files/ntia/publications/sbom_at_a_glance_ja.pdf

SBOMへの期待

OSSコンプライアンス管理の効率化やセキュリティ脆弱性対応の容易化においてSBOMが注目を集めている

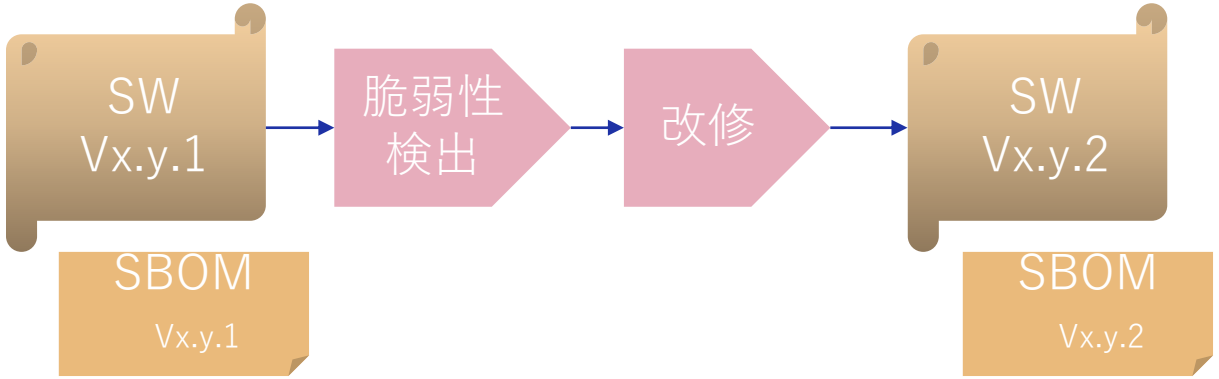
◆ SBOMの利用が想定されるシーン

(1) 企業間でのOSSコンプライアンス



OSSサプライチェーン（組み込み機器の例）

(2) セキュリティ脆弱性管理(識別の容易化)



セキュリティ脆弱性管理観点

米国で連邦政府納入案件へのSBOM義務化の動きあり。日本は研究中も米国メインプレーヤーのNTIAとの関係あり、今後加速の可能性あり

- 米国政府の動き：SBOMに言及した大統領令を発令(2021/5/12)


THE WHITE HOUSE

MENU

BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

- 日本政府の動き
  - 経済産業省 がNTIAと連携し、研究中(2019～)

NTIA:
National Telecommunications and Information Administration

OSSコンプライアンスの動向まとめ

- SBOMをキーワードに、OSSコンプライアンスへの注目が高まっている

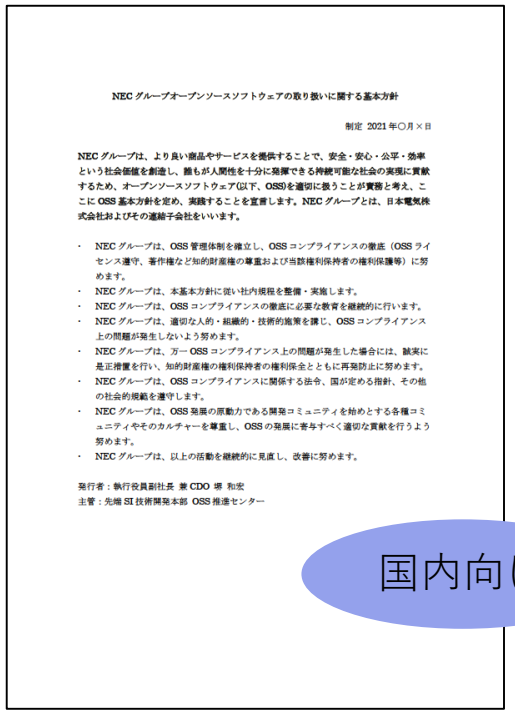
NEC社内で実施しているOSS管理体制について

【最近のトピック】「OSSグローバルポリシー」の制定

- 2021年9月 海外含むNECグループ全社に対し発行
- OSSコンプライアンス徹底を中心とした極めて基本的な事項の宣言

内容

- OSSコンプライアンスを徹底
- 社内規定を整備・実施
- 継続的に教育を実施
- 適切な人的・組織的・技術的施策
- 問題発生時の誠実な是正処置と再発防止
- 法令・指針・社会的規範を遵守
- コミュニティのカルチャー尊重、発展に寄与する貢献
- 継続的な活動見直し・改善



NECグループ オープンソースソフトウェアの取り扱いに関する基本方針

NEC グループオープンソースソフトウェアの取り扱いに関する基本方針

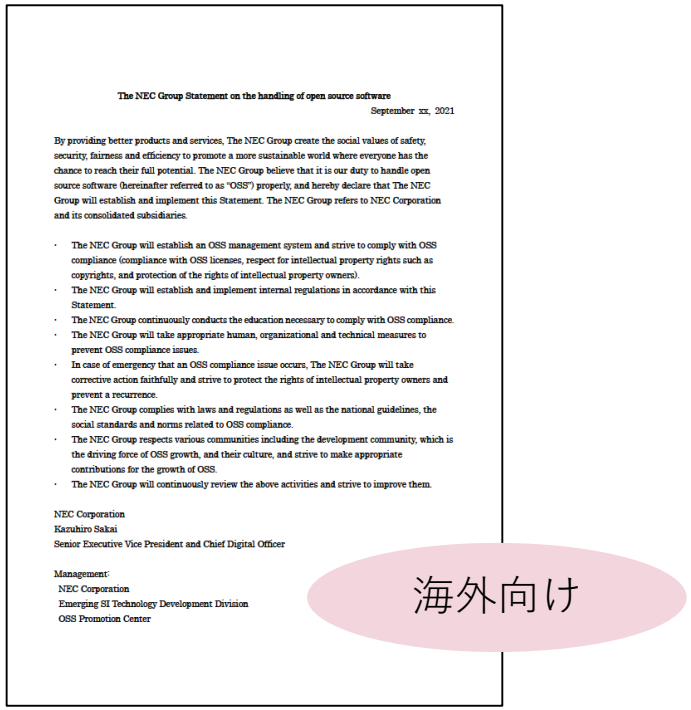
制定 2021 年〇月×日

NEC グループは、より良い商品やサービスを提供することで、安全・安心・公平・効率という社会価値を創造し、誰もが人間性を十分に発揮できる持続可能な社会の実現に貢献するため、オープンソースソフトウェア(以下、OSS)を適切に扱うことが責務と考え、ここに OSS 基本方針を定め、実践することを宣言します。NEC グループとは、日本電気株式会社およびその連結子会社をいいます。

- NEC グループは、OSS 管理体制を確立し、OSS コンプライアンスの徹底（OSS ライセンス遵守、著作権など知的財産権の尊重および当該権利保持者の権利保護等）に努めます。
- NEC グループは、本基本方針に従い社内規程を整備・実施します。
- NEC グループは、OSS コンプライアンスの徹底に必要な教育を継続的に行います。
- NEC グループは、適切な人的・組織的・技術的施策を講じ、OSS コンプライアンス上の問題が発生しないよう努めます。
- NEC グループは、万一 OSS コンプライアンス上の問題が発生した場合には、誠実に是正措置を行い、知的財産権の権利保持者の権利保全とともに再発防止に努めます。
- NEC グループは、OSS コンプライアンスに関係する法令、国が定める指針、その他の社会的規範を遵守します。
- NEC グループは、OSS 発展の原動力である開発コミュニティを始めとする各種コミュニティやそのカルチャーを尊重し、OSS の発展に寄与すべく適切な貢献を行うよう努めます。
- NEC グループは、以上の活動を継続的に見直し、改善に努めます。

発行者：執行役員副社長 兼 CDO 堺 和宏
主管：先端 SI 技術開発本部 OSS 推進センター

国内向け



The NEC Group Statement on the handling of open source software

September xx, 2021

By providing better products and services, The NEC Group create the social values of safety, security, fairness and efficiency to promote a more sustainable world where everyone has the chance to reach their full potential. The NEC Group believe that it is our duty to handle open source software (hereinafter referred to as "OSS") properly, and hereby declare that The NEC Group will establish and implement this Statement. The NEC Group refers to NEC Corporation and its consolidated subsidiaries.

- The NEC Group will establish an OSS management system and strive to comply with OSS compliance (compliance with OSS licenses, respect for intellectual property rights such as copyrights, and protection of the rights of intellectual property owners).
- The NEC Group will establish and implement internal regulations in accordance with this Statement.
- The NEC Group continuously conducts the education necessary to comply with OSS compliance.
- The NEC Group will take appropriate human, organizational and technical measures to prevent OSS compliance issues.
- In case of emergency that an OSS compliance issue occurs, The NEC Group will take corrective action faithfully and strive to protect the rights of intellectual property owners and prevent a recurrence.
- The NEC Group complies with laws and regulations as well as the national guidelines, the social standards and norms related to OSS compliance.
- The NEC Group respects various communities including the development community, which is the driving force of OSS growth, and their culture, and strive to make appropriate contributions for the growth of OSS.
- The NEC Group will continuously review the above activities and strive to improve them.

NEC Corporation
Kazuhiro Sakai
Senior Executive Vice President and Chief Digital Officer

Management:
NEC Corporation
Emerging SI Technology Development Division
OSS Promotion Center

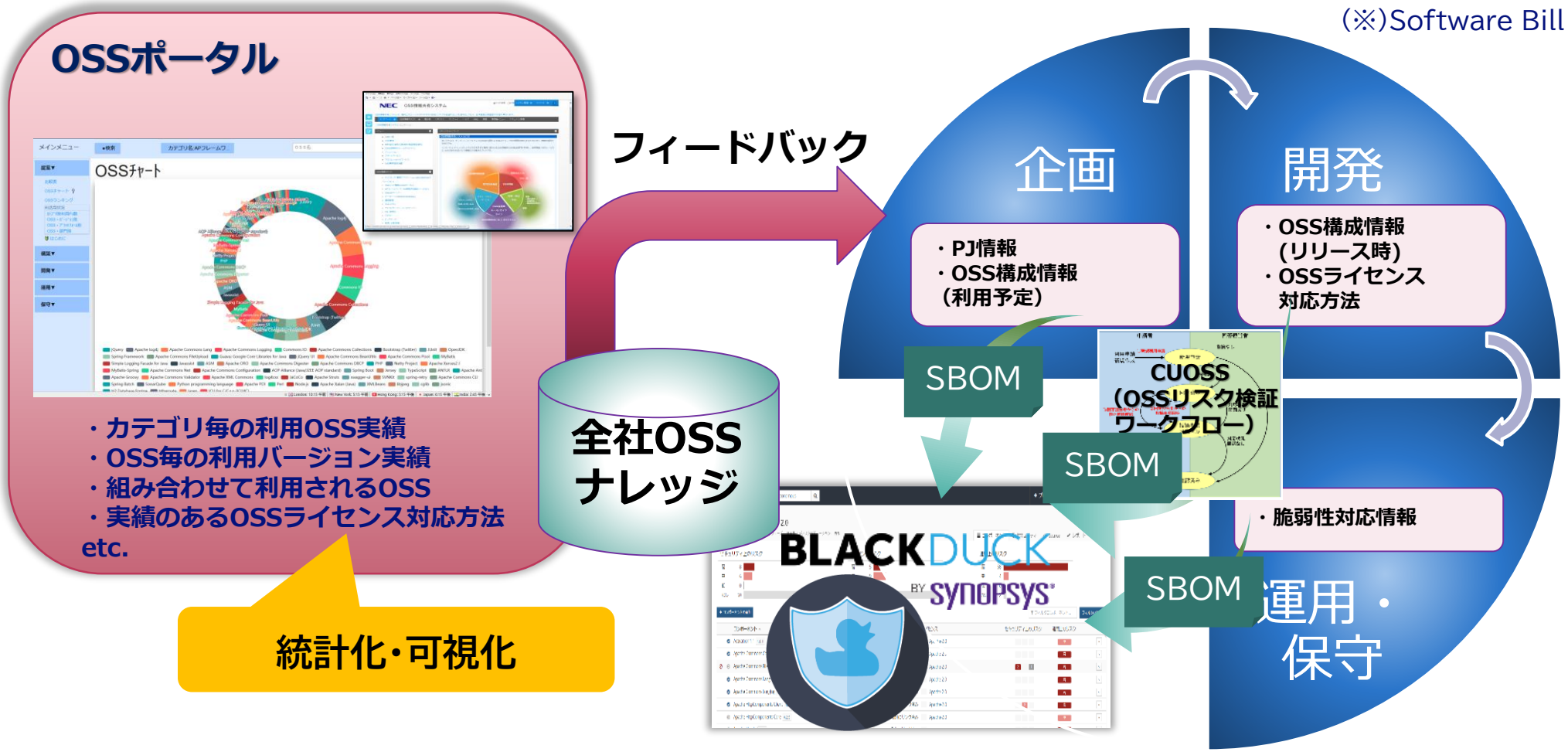
海外向け

The NEC Group Statement on the handling of open source software

OSSに関連するシステム連携の継続強化

Black DuckをコアとしたSBOM(※)情報集積-統計化・可視化システムを構築

(※)Software Bill Of Materials



NECがご支援できるソリューション紹介

Black Duckが提供する主な機能

BLACKDUCK
BY SYNOPSYS®

1. **OSSスキャン&リスト化**
   膨大なKBを基OSSコンポーネントを認識
2. **リスク情報の紐付け**
   ライセンス・セキュリティ・運用のリスクを可視化
3. **対応・修正状況の管理**
   ポリシーを管理し、違反への早期対応が可能
4. **モニタ・アラート機能**
   最新の脆弱性をウォッチし、アラートを発信！

顧客課題を解決するNEC商流BlackDuckサポートの強み

BlackDuck機能

- **OSSスキャン&リスト化**
- **リスク情報の紐付け**
- **対応・修正状況の管理**
- **モニタ・アラート機能**

NEC強み

トータルソリューション提案力

- HW・OS・AP一気通貫サポートのトータルソリューション（Linuxプラットフォームはシェア国内トップクラス）

活用ノウハウ

- 自社でのBlack Duck活用実績(10年以上)
- Partner Award(*)を受賞した高品質のサポート＋導入支援、解析支援

(*)「FY2020 Best Customer Support of the Year」

OSSライセンスコンサル

※製品サポートと独立提供

- ネットに散在する都市伝説に惑わされないOSSライセンスの正しい理解、正しい判断ができる組織育成を支援。

【事例】OSSライセンス・コンサル

オリンパスグループ 様 - 導入事例

OLYMPUS

NECのOSSライセンス・コンプライアンス コンサルティング・サービスを活用されたオリンパスグループ様。
その成功事例をご紹介します。

主要3事業

医療　科学　映像

業種	製造業	業務	精密機械器具の製造販売

精密機械機器メーカー最大手のオリンパス株式会社（以下、オリンパス）様とそのグループ会社オリンパスソフトウェアテクノロジー株式会社(以下、O-Soft)様では、グループ全体でのソフトウェア開発量が急激に増大すると共にOSSを利用する機会も増えてきました。いまや、OSSを製品に利用することは、世の中の流れ的に当たり前になってきており、自社内でも自然発生的に利用が当たり前になってきました。
そこで、オープンソースソフトウェア(OSS)の適正な活用を推進するため、NECの「OSSライセンス・コンプライアンス コンサルティング・サービス」を導入後、グローバルも含めたオリンパスグループ全体の仕組みを構築されています。

ご利用サービス	OSSライセンス教育(セミナー)推進者向け(2010年度) OSS利用ガイドライン作成支援(2011年度) OSSライセンス教育(セミナー)開発者向け(2011年度) 開発管理プロセス改善支援(2011年度)

事例のポイント

課題

オリンパスグループ 様 - 導入事例.
https://jpn.nec.com/oss/osslc/Olympus/caseOlympus.html


Orchestrating a brighter world
NEC