OSS の利活用及びそのセキュリティ確保に向けた管理手法に関する事例集

経済産業省　商務情報政策局
サイバーセキュリティ課

令和４年５月 10 日

目次

1. 目的

産業活動のサービス化に伴い、産業に占めるソフトウェアの重要性は高まっている。特に、近年は、産業機械や自動車等の制御にもソフトウェアの導入が進んでおり、汎用的なハードウェア上にシステムを構築し、ソフトウェアにより多様な機能を実現することで、様々な付加価値を創出していくことが期待されている。

なかでも、ソースコードが一般に公開され、商用か非商用かを問わずソースコードの利用・修正・再配布が可能なオープンソースソフトウェア（OSS）については、汎用ライブラリや Linux システム等を中心に、近年、企業の商用製品・サービスにも積極的に採用されており、今や OSS を用いずに製品・サービスを構築することは困難と言える。

ソフトウェアのセキュリティ確保に向けた取組として、産業サイバーセキュリティ研究会ワーキンググループ 1（制度・技術・標準化）が 2019 年 4 月に取りまとめた「サイバー・フィジカル・セキュリティ対策フレームワーク」（以下、「CPSF」という。）では、ソフトウェアの構成管理や、完全性確認等について言及しているものの、ソフトウェアの複雑化や OSS の利用拡大等に伴い、ソフトウェアのセキュリティをどのように維持し続けるのか、それをどのように確認するかの具体的な方法までは明確化していない。海外では、米国商務省の電気通信情報局（NTIA）において、2018 年 7 月から Software Component Transparency という官民合同の検討体制を構築し、Software Bill of Materials（SBOM）を用いたソフトウェアの脆弱性の管理手法の在り方についてユースケースを交えた検討を実施している。そのような状況等を踏まえ、経済産業省では、CPSF に基づく具体的なソフトウェアのセキュリティ対策手法等の検討を行うため、「サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース」（以下、「ソフトウェアタスクフォース」という。）[1]を 2019 年 9 月に設置した。

ソフトウェアタスクフォースの議論においては、産業界における OSS 利活用の重要性が高まる一方で、企業が OSS を含むソフトウェアの管理手法、脆弱性対応等に課題を抱えており、それらの課題に対し各企業において様々な対応をしている現状を踏まえ、産業界での知見の共有が有効であるとの認識に至った。

本事例集は、企業の OSS 利活用に関する課題の観点を整理し、その観点ごとに各種事例を取りまとめており、各企業が自社の「OSS の利活用及びそのセキュリティ確保に向けた管理手法」を検討する際の参考情報を提供することで、OSS の留意点を考慮した適切な OSS 利活用を促進することを目的としている。また、企業の OSS 利活用の障壁を取り除くことでより一層の OSS 利活用を促し、産業界において OSS のメリットを享受することで競争力向上につながることを期待するものである。

[1] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/index.html

2. OSS の概要

2.1. OSS とは

OSS とは、ソフトウェアのソースコードが公開され、利用や改変、再配布を行うことが誰に対しても許可されているソフトウェアのことである。OSS の概念及び志向は、世界中のユーザーがソースコードを共有の知的財産として扱い、修正や改良を重ねながらより良いソフトウェアへと磨き上げていくことである。

一般的な OSS の条件として、オープンソースに関する文化の啓発活動を行っている Open Source Initiative[2]が策定、公開している「オープンソースの定義」（The Open Source Definition）と呼ばれるライセンス文書[3]が広く知られている。

「オープンソースの定義」には、OSS が満たすべき条件として、以下があげられている。

1. 自由な再配布を認めること
2. ソースコードの利用の自由を認めること
3. 派生物の利用の自由を認めること
4. 原著作者のソースコードの完全性を示すこと
5. 特定人物・集団に対する差別を禁止すること
6. 使用分野に対する差別を禁止すること
7. ライセンスの権利配分を認めること
8. 特定製品への限定適用を禁止すること
9. OSS と共に配布される他のソフトウェアを制限してはならないこと
10. 技術中立的であること

さらに、OSS の大きな特徴として、OSS コミュニティ（以下、「コミュニティ」という。）による開発や改善、ノウハウの共有等の活動があげられる。コミュニティは、特定の OSS の利用者、開発者、愛好者らによって構

[2] 1998 年に米国で設立された「オープンソース」の利益を啓発、支持し、オープンソースコミュニティの様々な人達との橋渡しを目的とする団体
https://opensource.org/

[3] The Open Source Definition
https://opensource.org/docs/osd

成され、非営利目的で運営されている。世界中のメンバー間でソースコードを共有し、共同で開発に携わったり、メーリングリストで関連情報を発信したり、勉強会を開催したりする等、OSS の利活用を促進するエコシステムにおいて大きな役割を担っている。企業や組織にとって、コミュニティ活動が活発なことで高品質な OSS を利用できるようになることは大きなメリットとなるため、OSS の利活用が進む中、社員のコミュニティ活動を積極的に支援する企業や組織も増えている。主なコミュニティとして、Linux Foundation や Apache Software Foundation があげられる。

なお、OSS に対比するソフトウェアの捉え方として、プロプライエタリソフトウェアがあげられる。これは、ソフトウェア配布者がその知的財産を保持しており、改変や複製が制限されているソフトウェアである。具体的にはソースコードを非公開にしたり、ソフトウェア使用許諾契約によって法的にその使用を制限したりするものを指している。主には、有償の商用ソフトウェアとして市場に流通しているものの、無償で提供されるソフトウェア（フリーソフトウェア）も存在する。

2.2. OSS の利活用領域

OSS の利活用領域は、OS[4]から業務アプリケーション、データベース、ビッグデータ、AI（人工知能）等、多岐に渡る。主要な OSS を理解するために、日本 OSS 推進フォーラム[5]が取りまとめている OSS 鳥瞰図を参照することが有効である。これは、様々な領域で用いられている OSS を俯瞰的に把握できるように図示したものである（図 2.2-1）。

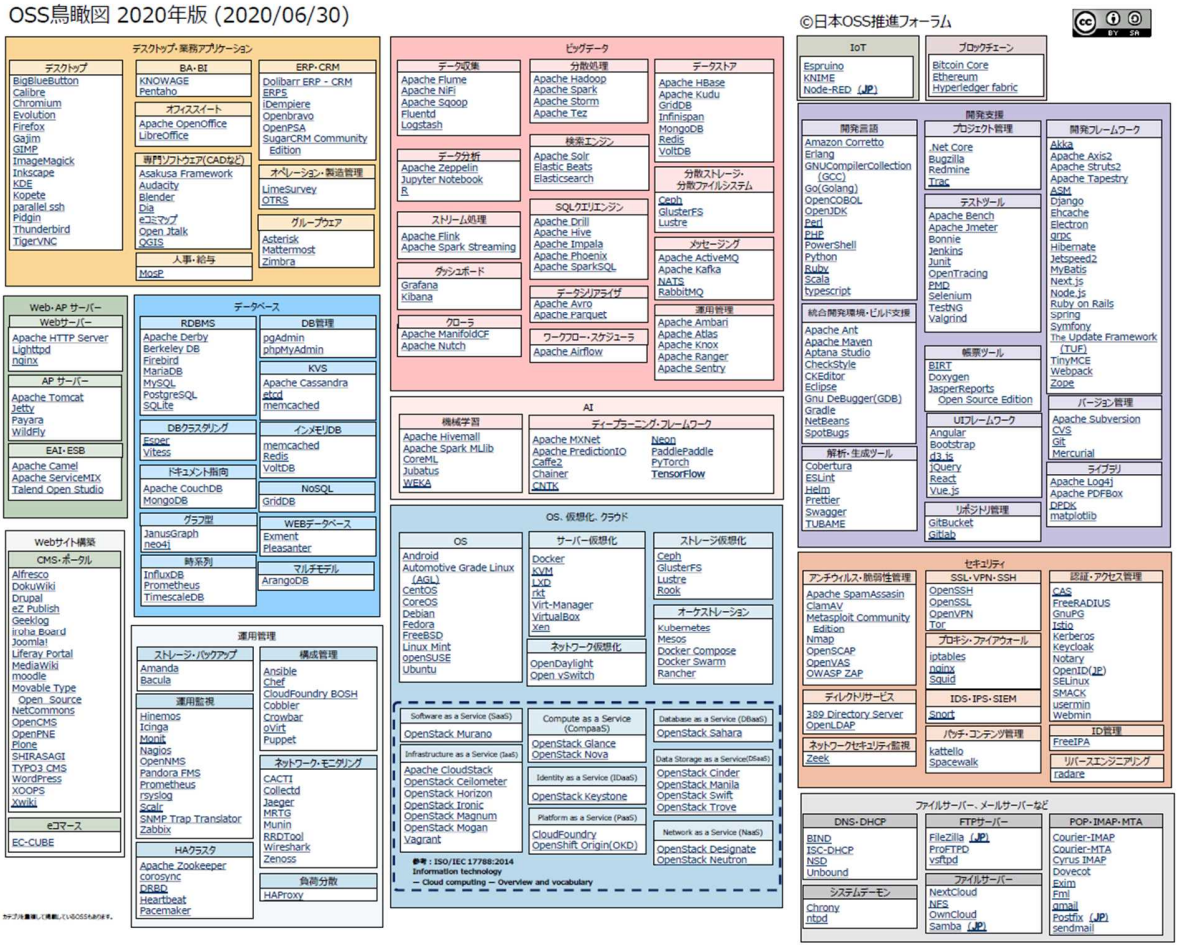


図 2.2-1　OSS 鳥瞰図 2020 年度版[6]

[4] Operating System

[5] 日本 OSS 推進フォーラム
http://ossforum.jp/

[6] OSS 鳥瞰図（2020 年版）

例えば、OS の領域においては、スーパーコンピュータ、サーバ、パーソナルコンピュータ、組み込みシステム（スマートフォンや家電製品等）等、幅広い種類のハードウェアに OSS である Linux が搭載されている。Linux は最も成功した OSS プロジェクトの一つであり、その広範な利活用範囲から、生活を支える製品やサービスに欠かすことのできないソフトウェアと言える。これは、前述のとおり、「無償である」「利用や改変、再配布可能である」等の特徴により、システムや製品を開発する企業に多くの便益があるために OSS が広く受け入れられていることを示している。また、その便益は、システムや製品の最終的なユーザーである企業や一般消費者にも価格面等において還元されている。

---

http://ossforum.jp/node/1332

2.3. OSS 利活用のメリット

OSS を利活用するメリットは多岐に渡る。主なメリットとしては、以下の点があげられる。

① 開発の効率化による開発費の抑制、開発期間短縮

② 高い安定性、品質、透明性の確保

③ 豊富な種類による新たな価値創出、ベンダロックインの回避

以下、各メリットの詳細について記載する。

① 開発の効率化による開発費の抑制、開発期間短縮

開発者が必要とする機能が既に OSS に実装されている場合、それを活用することで開発費用の抑制や開発期間の短縮が期待できる。競争環境、事業環境の変化の激しい ICT 関連産業においては、開発を効率化することで非常に大きなアドバンテージを得ることが可能となる。

② 高い安定性、品質、透明性の確保

OSS はオープンソースの志向に基づき、不特定多数の使用者による改良が重ねられており、ソフトウェアとしての高い安定性、品質を有している。多数のユーザーによる利用実績の積み重ねもあるため、開発者としては安心して使用することができる。また、ソースコードが公開されていることもあり、不正なプログラムや脆弱性などを常に確認できるといった透明性も持ち合わせている。

③ 豊富な種類による新たな価値創出、ベンダロックインの回避

現在では OSS の種類が非常に豊富になっており、多くの機能が OSS で利用可能となっている。AI 等を用いた最新の技術が実装される等、OSS を活用することで、これまでにない新しい価値を創出したり、既存業務を大幅に効率化できる可能性がある。また、ベンダロックイン[7]を回避できるといった側面も持ち合わせている。

以上のメリットから、多くの企業が OSS を採用したシステム、製品の開発を行っている。今後もこの傾向はますます拡大していくものと考えられている。

[7] 特定ベンダ（メーカー）の独自技術に大きく依存した製品、サービス、システム等を採用することにより、他ベンダの提供する同種の製品、サービス、システム等への乗り換えが困難になる事象

2.4. OSS 利活用の留意点

OSS の利活用には、多くのメリットがある反面、留意しなければならない点も複数存在する。主な留意点としては、以下があげられる。

① ライセンスコンプライアンス

② ライフサイクル（サポート期間等）が短い、サポートが十分ではない場合がある

③ サプライチェーンにおける OSS の使用

以下、各留意点の詳細について記載する。

① ライセンスコンプライアンス

OSS は、ソフトウェアごとに個別にライセンスが宣言されているため、利用者は、そのライセンスに準拠した利用が求められる。OSS 使用者は、開発担当者が多く、ライセンス等の法務の知識が十分ではない場合もある。そのような場合、気が付かないうちに OSS ライセンスに違反していた等の事象が発生する可能性があり、企業コンプライアンス上のリスクが発生していると言える。

② ライフサイクル（サポート期間等）が短い、サポートが十分ではない場合がある

OSS は、商用ソフトウェアと比較して、ソフトウェアとしてのライフサイクル（サポート期間等）が比較的短く、またサポートが十分ではない場合がある。このため、バグやソフトウェア脆弱性等が判明した場合にユーザー側で対応しなければならない等、利活用にあたって一定のスキル・ノウハウが必要となる。

③ サプライチェーンにおける OSS の使用

OSS は、自社における使用のみならず、自社の製品やシステム開発のサプライチェーンを構成する企業等において使用されている可能性がある。そのような場合でも、納品物内の使用 OSS を把握し、前述のライセンス対応やバグ・ソフトウェア脆弱性等への対応を自社における OSS 使用時と同じように実施しなければならない。そのため、サプライチェーン各社の使用 OSS に関する情報を適切に吸い上げる必要がある。

これらの留意点に適切に対応することが OSS 利活用を行う上で大変重要になる。なお、これらの留意点に適切に対応する際に発生する課題については、その観点を 3.2 章において整理する。

2.5. OSS に関わる係争及びインシデント事例

2.4 章で述べた留意点を補足する観点で、過去の OSS に関わる係争、及びインシデント事例を以下に示す。

① OSS ライセンスに関わる係争事例 ―航空機内エンターテインメントソフトウェアの例[8]―

2017 年 3 月、某社が開発した航空機内エンターテインメントソフトウェアについて、競合する企業からライセンス違反があるとしてニューヨーク連邦裁判所に提訴された。提訴した企業は、Linux ベースのソフトウェアのソースコードが適切に開示されていないことを指摘し、本件は過失によるライセンス違反ではなく、競合企業が類似のソフトウェアを開発するのを妨害する目的で故意に実施されているとして、1 億ドルの賠償を要求した。2018 年 1 月に両社は和解したものの、賠償額は明かされていない。

② OSS の脆弱性に関わるインシデント事例 ―Heartbleed[9]の例 [8]―

2014 年 4 月、OpenSSL（SSL/TLS[10]プロトコルの OSS ライブラリ）の Heartbeat 機能において脆弱性が見つかったことが公表された。Heartbeat 機能は、機器間で通信が行われていない間も TLS セッションの接続を維持し、通信相手が存在しているかを確認する機能である。脆弱性を含んだバージョンの OpenSSL サーバ宛に、細工をした Heartbeat のリクエストを送ることで、その返答の際にサーバのメモリ上のデータが含まれ、ID/パスワードや SSL サーバ証明書の秘密鍵が漏えいする可能性があった（図 2.5-1）。

[8] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 1 回資料
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf

[9] この脆弱性は「Heartbeat」機能に由来することから「Heartbleed（ハートブリード、心臓出血）」と命名された。

[10] SSL：Secure Sockets Layer TLS：Transport Layer Security
いずれもインターネット上でデータを暗号化して送受信するためのプロトコルの一種である。

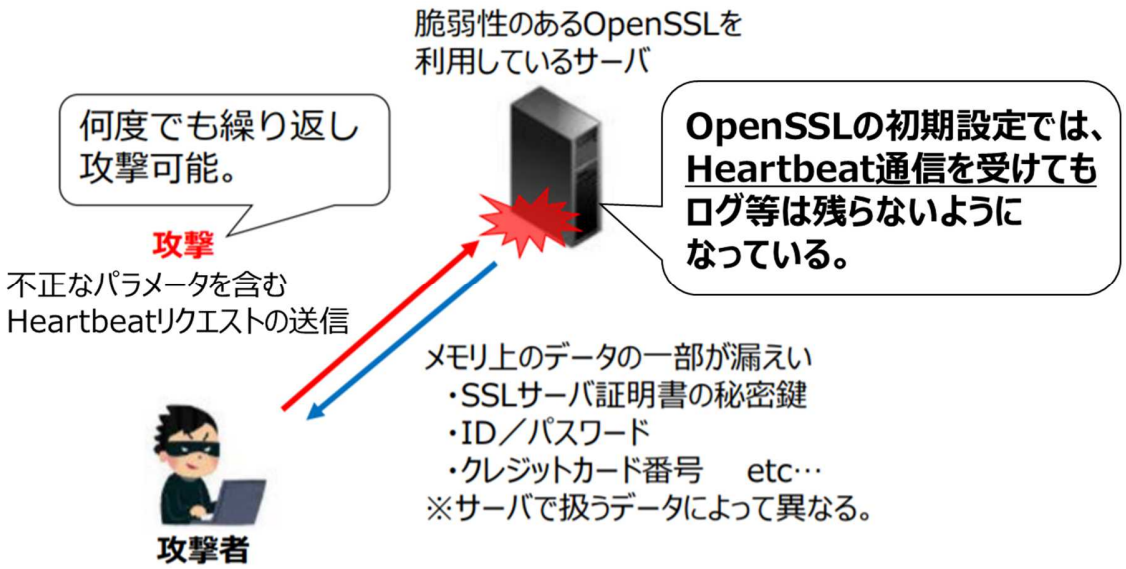


図 2.5-1　Heartbeat 機能を用いた攻撃イメージ[11]

[11] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 1 回資料より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/001_04_00.pdf

2.6. OSS 利活用等に寄与する主な取組

2.6.1. 情報セキュリティ早期警戒パートナーシップ・Japan Vulnerability Notes

OSS の利活用を支援する主な取組として、情報処理推進機構（IPA）及び JPCERT コーディネーションセンター（JPCERT/CC）によって運営されている情報セキュリティ早期警戒パートナーシップ、及び Japan Vulnerability Notes（JVN）があげられる。製品・サービスやシステムに OSS を利活用しており、その OSS に関わる脆弱性が判明した場合、その脆弱性に迅速かつ適切に対応することは、セキュリティを保つ上で大変重要となる。情報システム早期警戒パートナーシップ及び JVN は、これらの一連の対応を行うにあたり必要な情報をユーザーに提供している。

情報セキュリティ早期警戒パートナーシップは、2017 年の経済産業省告示「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」に基づき、国内におけるソフトウェア等の脆弱性関連情報を適切に流通させることを目的に作られている枠組みである。IPA が一般人や研究者が発見したウェブサイト及びソフトウェア製品に関するセキュリティ上の問題（脆弱性）を受け付け、JPCERT/CC が脆弱性の発見者、ソフトウェア製品開発者、ウェブサイト運営者等と協力・連絡調整をしながらその対処を取りまとめている（図 2.6-1）。

JVN は、情報セキュリティ早期警戒パートナーシップに基づき発見された脆弱性情報等を、取りまとめられた対処法等と共に公開する情報ポータルサイトである。情報セキュリティ早期警戒パートナーシップに基づく情報以外に、CERT/CC など海外の調整機関と連携した脆弱性情報も公表している（図 2.6-2）。具体的な公表内容としては、脆弱性が確認された製品とバージョン、脆弱性の詳細や分析結果、製品開発者によって提供された対策や関連情報へのリンク等で、対策にはパッチだけではなく回避策（ワークアラウンド）が含まれることもある。

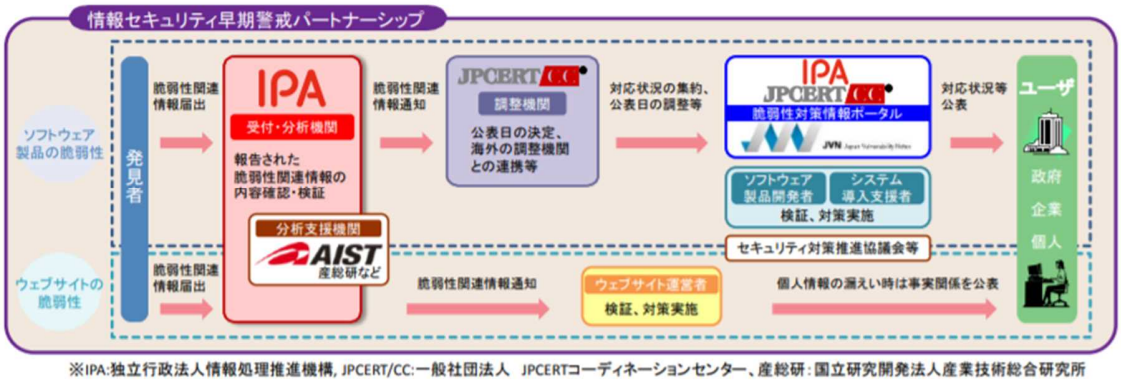


図 2.6-1 情報セキュリティ早期警戒パートナーシップの枠組み[12]

図 2.6-2 JVN のホームページ[13]

2.6.2. 企業のためのオープンソースガイド等（Linux Foundation）

Linux Foundation 配下の TODO グループは、メンバー企業における OSS 利活用に係る知識や経験を共有し、製品・サービス開発等における課題解決を支援している。TODO グループによって、先進企業

[12] 情報セキュリティ早期警戒パートナーシップの紹介より抜粋
https://www.ipa.go.jp/files/000044731.pdf
[13] Japan Vulnerability Notes（JVN）のホームページより抜粋
http://jvn.jp/index.html

の OSS に係る取組を集めたガイド「企業のためのオープンソースガイド」が公開されている（日本語訳版有）。「企業のためのオープンソースガイド」は、「オープンソースプログラムオフィスの運用」と「組織におけるオープンソースプロジェクトの管理」の 2 つのテーマに基づき、以下の 12 のガイドで構成されている[14]。

＜オープンソースプログラムオフィスの運用＞

- オープンソースプログラムの作成
- オープンソース管理ツール
- オープンソースプログラムの成功度を測る
- オープンソースデベロッパーの採用
- オープンソースコミュニティへの参加
- オープンソースコードの使用

＜組織におけるオープンソース プロジェクトの管理＞

- オープンソースプロジェクトを立ち上げる
- オープンソース開発の効果を高める
- オープンソースガイド推奨図書
- オープンソースプロジェクトを終了させる
- オープンソースコミュニティでリーダーシップを構築する
- オープンソース戦略の策定

Linux Foundation では、この他にも OSS 利活用戦略を立案するための実践的アプローチを解説した「エンタープライズオープンソース：実践的入門」[15]や、各業界における OSS の先進活用例を紹介する「ソフ

[14] 企業のためのオープンソースガイド
https://www.linuxfoundation.jp/resources/open-source-guides/
[15] エンタープライズオープンソース：実践的入門
https://www.linuxfoundation.jp/open-source-management/2018/08/enterprise-open-source-practical-introduction/

トウェア定義が進む各業界：オープンソースによる変革」[16]等、有用なガイド、ホワイトペーパーを公開している。

[16] ソフトウェア定義が進む各業界：オープンソースによる変革
https://www.linuxfoundation.jp/blog/2020/09/software-defined-vertical-industries-transformation-through-open-source/

3. 事例の整理方法

3.1. OSS を取り巻く商流・ステークホルダの整理

OSS の商流（サプライチェーン）は、多種多様なステークホルダにより形成されている（図 3.1-1）。OSS は、OSS 開発コミュニティやそのコミュニティ参加企業といった開発ステークホルダによる OSS の開発・提供からその商流が始まる。その後、OSS を商用パッケージとして流通させるディストリビュータ、OSS を用いて製品やシステムを開発する最終製品メーカー、サプライヤ、SIer[17]、OSS を用いたクラウドサービス等を提供するサービス事業者等の中間層を介する。最終的に、製品であれば製品のエンドユーザーとしての企業・消費者、システムであればエンドユーザーが製品やシステムに対価を支払い、その便益を享受する。

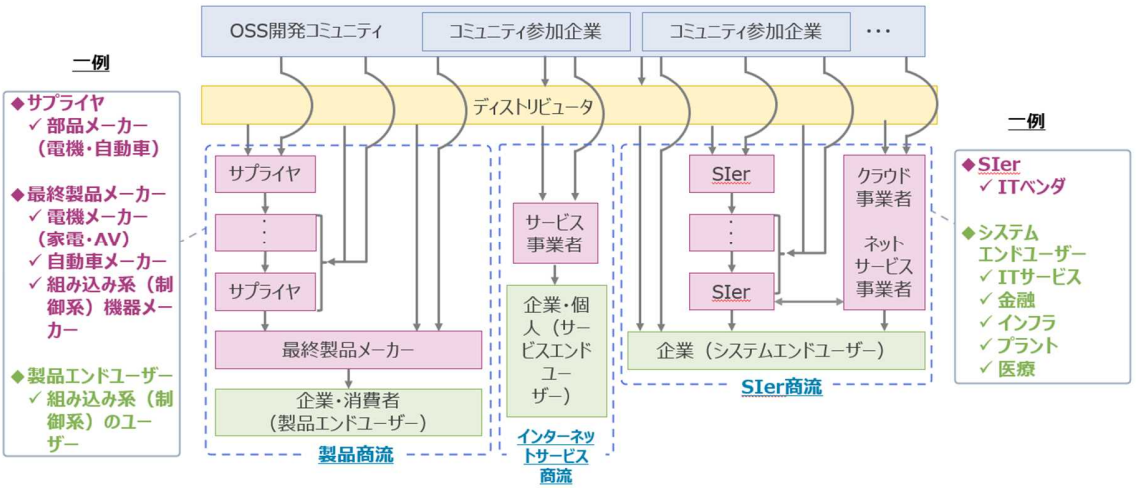


図 3.1-1　OSS の商流とステークホルダ[18]

OSS の商流は、主に最終製品を供給するために発生する商流（製品商流）と企業におけるシステム導入に伴い発生する商流（SIer 商流）に大別することが可能である。本事例集では、OSS を実際に利活用する主体となる、ディストリビュータ以降の製品商流、SIer 商流におけるステークホルダの取組を紹介する。それぞれの商流の概要、及び主なステークホルダは以下のとおりである。

- 製品商流

  最終製品メーカーと最終製品メーカーに部品供給するサプライヤによって形成される商流である。製品は、

[17] システムインテグレータ（Systems Integrator）

[18] ヒアリング等を基に作成

最終的に製品エンドユーザーが購入する。サプライヤは、サプライチェーンを形成しており、重層的に部品供給を受けている場合がある。最終製品メーカーの製品開発、及びサプライチェーン各段階のサプライヤにおける部品開発において広く OSS が利活用されている。製品商流の主なステークホルダは以下のとおりである。

- サプライヤ：
  最終製品メーカーに部品供給するメーカーである。OSS 商流においては、OSS 等を含むソフトウェアを組み込んだ部品（製品）を製造し、納品するメーカーが対象となる。最終製品によって、固有の、もしくは専門性を持つサプライヤが存在する（自動車部品メーカー、電子部品メーカー等）。
- 最終製品メーカー：
  自社で開発した部品、及びサプライチェーン（サプライヤ）から供給された部品を基に最終製品を製造するメーカーである（自動車メーカー、電機メーカー等）。自社開発において OSS を使用する場合もあれば、サプライヤから供給された部品に OSS が使用されている場合もある。
- 製品エンドユーザー：
  最終製品メーカーが製造した製品を購入、使用する組織、個人は全て製品エンドユーザーである。

- SIer 商流

システムエンドユーザー（企業等）からの発注により、SIer が開発を行い、業務システム等を納品する商流である。SIer はサプライチェーンを形成しており、重層的な業務委託により開発を実施している場合がある。あわせて、クラウドサービス等のサービスも組み合わせつつ、最終的にシステムを構築している。サプライチェーン各段階の SIer、及び各サービス事業者において広く OSS が利活用されている。SIer 商流の主なステークホルダは以下のとおりである。

- サービス事業者：
  クラウドサービスやネットサービス等を SIer やシステムエンドユーザーに提供している事業者があげられる。SIer やシステムエンドユーザーはそれらのサービスを活用してシステム構築を行っている。
- SIer：
  情報システムのインテグレーションを行う事業者や、情報システムの開発・構築を受託し納品する事業者等があげられる。自社の IT 製品を持ち、その提供を行いつつ開発を受託する事業者もいる。業界ごとに、使用する業務システムの種類や必要となる特性に共通点があるため、業界ごとに固有の、もしくは専門性を持つ SIer やシステム開発事業者が存在する（金融業向けの SIer、製造業向けの SIer 等）。
- システムエンドユーザー：
  企業や官公庁、自治体等、業務システムを使用する組織は全てシステムエンドユーザーである。

- インターネットサービス商流

インターネットサービス事業者によりサービスを提供するためのシステム開発を行い、インターネットを介してサービスを提供する商流である。あわせて、クラウドサービス等のサービスも組み合わせつつ、最終的にシステムを開発し、サービスの提供を行っている場合がある。インターネットサービス事業者は、広く OSS を利活用してサービスを提供しており、BtoB または BtoC においてサブスクリプション、無償等によるサービス提供を行っている。製品商流や SIer 商流とは異なり、ライセンス違反等の事業リスクに対して素早い対処が可能である。インターネットサービス商流の主なステークホルダは以下のとおりである。

- サービス事業者：
  クラウドサービスやネットサービス等をインターネットサービス事業者に提供している事業者があげられる。
  インターネットサービス事業者はそれらのサービスを活用してサービスの提供を行っている。

- サービスエンドユーザー：
  インターネット事業者が提供したサービスを利用する組織、個人は全てサービスエンドユーザーである。

3.2. OSS の利活用に係る課題観点の抽出

3.2.1. サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォースにおける課題の整理

ソフトウェアタスクフォースでは、過去の国内外におけるソフトウェアにおける管理、脆弱性対応、ライセンス等に関する事例を基に、OSS を含むソフトウェアの利活用及びそのセキュリティ確保に向けた管理手法に係る課題を「検討の方向性」として、図 3.2-1 のとおり整理を行っている。

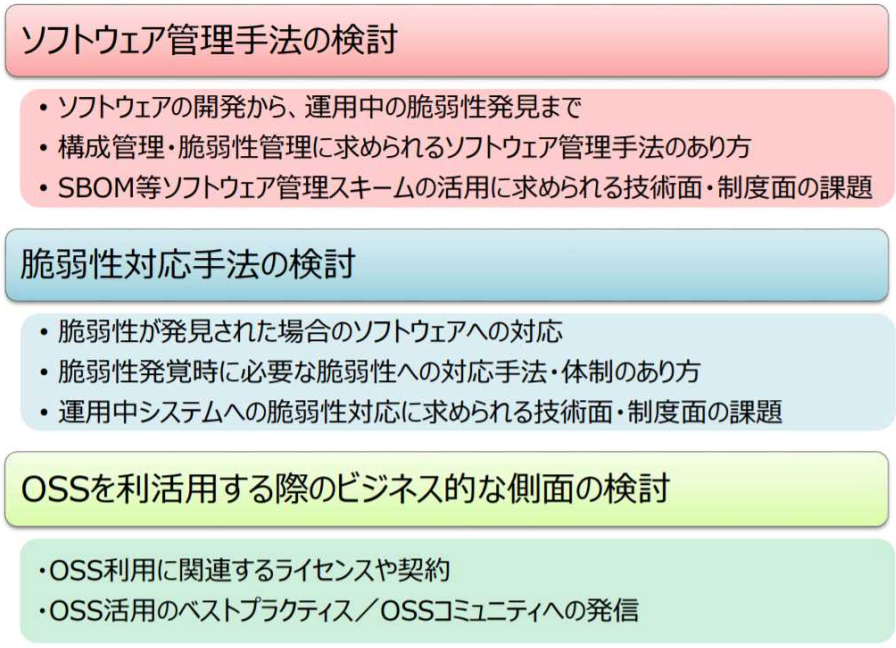


図 3.2-1 タスクフォースにおける検討の方向性[19]

ソフトウェアタスクフォースにおいては、OSS の脆弱性対応、ライセンス対応において、適切な OSS 管理を行う重要性を認識した。また、OSS を管理する粒度や、組織としてどのように取り組むかといった点等を今後の課題としてあげ、OSS 管理に向けた制度面、体制面等の整備の推進を図る必要性があるとした。これら課題への対応として、各社の OSS 管理に係る取組の知見共有が重要であるとし、OSS の利活用及びそ

[19] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 3 回資料より抜粋 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_03_00.pdf

のセキュリティ確保に向けた管理手法に係る事例集等の作成が有効であるという共通認識を得ている。

3.2.2. OSS 利活用に係る課題の観点

OSS の利活用及びそのセキュリティ確保に向けた管理手法に係る課題の観点について、ソフトウェアタスクフォースの議論内容やタスクフォース委員（有識者・企業）へのヒアリングを基に整理を行った。

本事例集では、OSS ステークホルダが OSS を利活用する際に抱える主な課題を以下の観点で分類している。

- 選定評価（Selection Evaluation）
- ライセンス（Licensing）
- 脆弱性対応（Vulnerability Response）
- 保守、品質保証（Maintenance and Quality Assurance）
- サプライチェーン管理（Supply Chain Management）
- 個の能力、教育（Personal Competence and Education）
- 組織体制（Organizational Structure）
- コミュニティ活動（Community Activities）

上記の観点ごとに、その主な課題を整理した表を以下（図 3.2-2）に示す。なお、各観点は、OSS を利活用する際、選定や管理等のプロセスにおいて発生する課題の観点（「プロセス別観点」）、OSS に携わる人材や組織のリテラシー向上、体制整備において発生する課題の観点（「人・組織に関する観点」）、OSS コミュニティ活動等、OSS のエコシステムへの貢献・拡大に対する課題（「コミュニティに関する観点」）に分類している。

図 3.2-2　OSS に係る観点とその課題（一例）[20]

[20] ヒアリング等を基に作成

3.3. 紹介事例一覧

本事例集は、ヒアリングにより収集した国内企業の事例（20 事例）と、公開文献の調査により収集した海外事例（3 事例）を掲載している。

3.1 章における OSS を取り巻く商流・ステークホルダの整理、及び 3.2 章における OSS 課題観点の整理を基に、本事例集における各事例の対応表を以下（表 3.3-1）に示す。各事例の詳細については、次章以降にて記載する。表 3.3-1 には、“L1”、“S1”のように各事例に関連する観点を付与しており、該当する観点の取組の説明箇所へ遷移することが可能としている。なお、表 3.3-1 は本事例集で紹介している取組の観点を一覧として整理したものであり、各社の取組のすべてを網羅的に示したものではない。

表 3.3-1 掲載事例一覧

商流	ステークホルダ	事例企業	事例に関連する観点							
			選定評価（S）	ライセンス（L）	脆弱性対応（V）	保守・品質保証（M）	サプライチェーン管理（S）	個の能力・教育（P）	組織体制（O）	コミュニティ活動（C）
ヒアリング実施企業										
製品商流	最終製品メーカー	トヨタ自動車		L1			S1			C1
		ソニー		L2-1 L2-2	V2		S2		O2	C2
		オリンパス		L3			S3	P3	O3	C3
		日立製作所		L4						C4
		オムロン			V5-1 V5-2		S5	P5	O5-1 O5-2	
		東芝	S6	L6	V6	M6	S6	P6	O6	C6
		三菱電機インフォメーションシステムズ（MDIS）	S16	L16	V16	M16				C16-1 C16-2
	サプライヤ	デンソー		L7	V7		S7			

商流	ステークホルダ	事例企業	事例に関連する観点							
			選定評価（S）	ライセンス（L）	脆弱性対応（V）	保守・品質保証（M）	サプライチェーン管理（S）	個の能力・教育（P）	組織体制（O）	コミュニティ活動（C）
製品商流＆SIer 商流	SIer&最終製品メーカー	富士通	S8	L8	V8-1 V8-2	M8	S8	P8	O8-1 O8-2	C8
		日本電気（NEC）	S9-1 S9-2	L9-1 L9-2	V9-1 V9-2	M9		P9	O9-1 O9-2	
SIer 商流	SIer	日本電信電話（NTT）			V10				O10	
		匿名企業A 社	S11			M11				C11
	SIer＆エンドユーザー	匿名企業B 社			V12			P12		
	エンドユーザー	損害保険ジャパン		L13	V13			P13		
		Visionalグループ			V14					
		サイボウズ	S15	L15	V15			P15	O15	C15
		OSSTech		L17	V17		S17			
		SCSK	S20		V20-1 V20-2		S20	P20	O20	
インターネットサービス事業者		ヤフー	S18	L18	V18	M18	S18	P18	O18	C18
		ラキール	S19	L19	V19				O19	
文献調査実施企業等										
SIer 商流	サービス事業者	マイクロソフト			V20					
	エンドユーザー	ザランド		L21						

商流	ステークホルダ	事例企業	事例に関連する観点							
			選定評価（S）	ライセンス（L）	脆弱性対応（V）	保守・品質保証（M）	サプライチェーン管理（S）	個の能力・教育（P）	組織体制（O）	コミュニティ活動（C）
その他（調査結果）		CensusⅡ プロジェクト			V22					

4. 事例（ヒアリング調査）

4.1. トヨタ自動車　～サプライチェーンにおけるソフトウェア使用状況把握～

■ 企業情報・本事例集における位置づけ

本社	愛知県豊田市
業種	製造（自動車）
従業員数（連結）	370,870 人（2019 年 3 月末現在）
商流	製品商流/最終製品メーカー
観点	「ライセンス」「サプライチェーン管理」「コミュニティ活動」

■ 本事例のエッセンス

- ソフトウェア管理ルール明確化の取組により、ライセンス違反のリスク低減及びサプライチェーン全体における OSS に係るセキュリティ脆弱性への対応力向上に努めている。
- 使用ソフトウェアに関するガイドライン締結においては、サプライヤに対して、OSS コンプライアンスの重要性を強調することで理解を求めた。
- サプライヤからの使用ソフトウェアリスト提供にあたっては、運用面を考慮し、SPDX Lite のフォーマットを採用した。
- OSS 管理に係る社内の取組を、コミュニティ活動において共有・議論することで、オープンな PDCA サイクルを形成し、サプライチェーン全体における OSS コンプライアンスの底上げに貢献している。

■ 背景・課題

自動車業界は、最終製品メーカーのみならず、重層的なサプライヤが存在し、多数の企業がサプライチェーンを形成している。サプライチェーン各企業においては、OSS が使用されており、OSS ライセンスを遵守するために、その使用状況を正確に把握することが求められる。しかしながら、サプライチェーン各社において、使用ソフトウェアの管理粒度、ガバナンス体制は異なっているため、それらをいかに統一的な運用に落とし込むかが課題となっている。

■ 取組

＜【ライセンス(L1)】【サプライチェーン管理(S1)】サプライチェーンにおけるソフトウェア（OSS 含む）使用状況把握＞

トヨタ自動車では、OSSコンプライアンスに係る運用ルール、監査ルール、帳票等の社内プロセス、権限、組織体制等の整備を全社直轄組織の下で取り組んでいる。特に、サプライチェーンにおける使用ソフトウェアの把握については、サプライヤ（Tier 1[21]）に対して、以下の 2 点の取組を実施している（表 4.1-1）。

① 各サプライヤと使用ソフトウェアに関するガイドラインを合意

② 部品供給に際して、自社と各サプライヤのエンジニア部門同士で使用ソフトウェア報告の運用規則を合意

表 4.1-1 ガイドライン、運用規則における規定項目[22]

ガイドライン（会社間のベーシックなルールの合意）	● サプライチェーンにおけるOSSコンプライアンスの役割 ● 責任分界 ● 各ライセンスの取り扱い方法 ● 使用ソフトウェアリスト提供の合意
運用規則（実務レベルの運用ルールの合意）	● リストのフォーマット ● ワークフロー ● 報告のタイミング ● 連絡先

以下、各取組の詳細について記載する。

① 各サプライヤと使用ソフトウェアに関するガイドラインを合意

サプライチェーンにおける OSS コンプライアンスの役割をはじめ、使用ソフトウェアリスト提供をすることや注意を払うべきライセンス等について会社間でガイドラインの合意を行っている。それまでの自動車業界では、供給先に対して必要以上の情報提供を避ける商習慣が一部存在していたものの、ガイドラ

[21] 最終製品メーカーに直接部品を供給するメーカー

[22] Open Compliance Summit 2019 の資料を基に作成
https://static.sched.com/hosted_files/ocs19/d3/Open%20Source%20Compliance%20in%20Supply%20Chains.pdf

インの合意に向けて、特にライセンス面におけるコンプライアンスの重要性を強調し、各サプライヤへ理解を求めた。

② 部品供給に際して、自社と各サプライヤのエンジニア部門同士で使用ソフトウェア報告の運用規則を合意

前述のガイドラインに基づき、各サプライヤとの供給関係（プロジェクト）ごとに実務（エンジニア）レベルで、供給部品における使用ソフトウェアリスト提供に関する運用規則の合意を行っている。具体的には、規則の適用範囲（製品、サービス等）、使用ソフトウェアリストの報告方法（誰から誰へ報告するか、報告のタイミング（開発段階の報告含む）等）、フォーマット、ライセンスで要求されている著作権情報、ソースコード開示の具体的な対応方法（マニュアルへの掲載、Web での公開等）等をプロジェクトごとに定めている。

各サプライヤにおけるハンドリングのしやすさを考慮した結果、使用ソフトウェアリストのフォーマットは OpenChain[23]で議論されている SPDX Lite を採用している。SPDX Lite は、SPDX[24]の簡易バージョンであり、Excel 等での管理も可能である（図 4.1-1）。SPDX Lite においてリスト化する情報や記載ルールは、最善の運用を目指し、継続的に改善が検討されている。

SPDX Liteの項目例
-パッケージ名
-パッケージSPDX識別子
-パッケージバージョン
-パッケージファイル名
-パッケージダウンロード位置（入手先）
-解析したファイル（手作業の場合false）
-ホームページ（開発コミュニティサイト）
-結論されたライセンス
-宣言されたライセンス
-ライセンスへのコメント
-著作権テキスト
-改変の有無
-パッケージに関するコメント
-ライセンス識別子

SPDXサンプルの一部抜粋

	3.1	3.2	3.3	3.4	3.7	3.8	3.11	3.13	3.15
	PackageName	Package SPDX Identifier	Package Version	PackageFileName	PackageDownloadLocation	Files Analyzed	PackageHomePage	Concluded License	Declared License
項	パッケージ名	パッケージSPDX識別子	パッケージバージョン	パッケージファイル名	パッケージダウンロード位置（入手先）	解析したファイル（手作業の場合false）	ホームページ（OSS開発コミュニティサイト）	結論されたライセンス	宣言されたライセンス
	LibXML2		2.99	libxml2-2.9.9.tar.gz	ftp://xmlsoft.org/libxml2/	FALSE	http://xmlsoft.org/	MIT	MIT
	PCRE		8.4343	pcre-8.43.tar.gz	ftp://ftp.pcre.org/pub/pcre/	FALSE	https://www.pcre.org/	BSD-3-Clause	BSD-3-Clause
	SQLite		3300100.tartar	sqlite-autoconf-3300100.tar.gz	https://www.sqlite.org/download.html	FALSE	https://www.sqlite.org/index.html	その他（ライセンス名を記載）	その他（ライセンス名を記載）
	Zlib (1.2.3)		1.2.11	zlib-1.2.11.tar.gz	https://www.zlib.net/	FALSE	https://www.zlib.net/	Zlib	Zlib
	cURL (7.41.0)		7.66.0	curl-7.66.0.tar.bz2	https://github.com/curl/curl/releases	FALSE	https://curl.haxx.se/	MIT	MIT

図 4.1-1　SPDX Lite フォーマット（サンプル）[25]

[23] Linux Foundation のプロジェクト。サプライチェーン全体にわたって OSS コンプライアンスを実現するための業界標準の作成、普及を目的としている。
https://www.openchainproject.org/ja/

[24] ソフトウェアパッケージデータ交換形式（SPDX：Software Package Data Exchange）は、Linux Foundation が支援するソフトウェアパッケージに関連するコンポーネントやライセンス、コピーライト等の情報をやり取りするための標準的なフォーマットである。

[25] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 3 回資料より抜粋

以上のような取組により、ソフトウェア管理に対する重要性の認識が高まったとともに、その管理ルールが明確となり、サプライヤごとのソフトウェア管理品質のバラつき低減が可能となった。これによりライセンス違反のリスクが低減するのみならず、サプライチェーン全体における OSS に係るセキュリティ脆弱性への対応力が高まっている。

＜【コミュニティ活動(C1)】OSS 利活用促進に向けたコミュニティ等における活動＞

トヨタ自動車では、サプライチェーンにおけるソフトウェア使用状況把握の取組と並行して、それらの取組に関する標準化に貢献している。一例として、OpenChain の活動があげられる。

OpenChain は、サプライチェーン全体にわたって OSS コンプライアンスを実現する業界標準の作成・普及を目的とした Linux Foundation のプロジェクトである。日本からは、電機、情報通信機器メーカーを中心に多くの企業が参加している。プロジェクトの主な成果物[26]（図 4.1-2）は、以下の 3 点である。

① 仕様（Specification）：企業が組織内に確立すべきコンプライアンスプログラムの要件を定義

② 適合（Conformant）：仕様に適合しているか否かを Web アンケートで回答することで、認証を取得可能。原則、自己認証だが第三者認証もある

③ カリキュラム（Curriculum）：仕様への適合のために各社内で利用可能な教育資料集

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf

[26] トヨタ自動車はこれらの成果物を基に、前述の OSS コンプライアンスに係る社内体制を構築している。

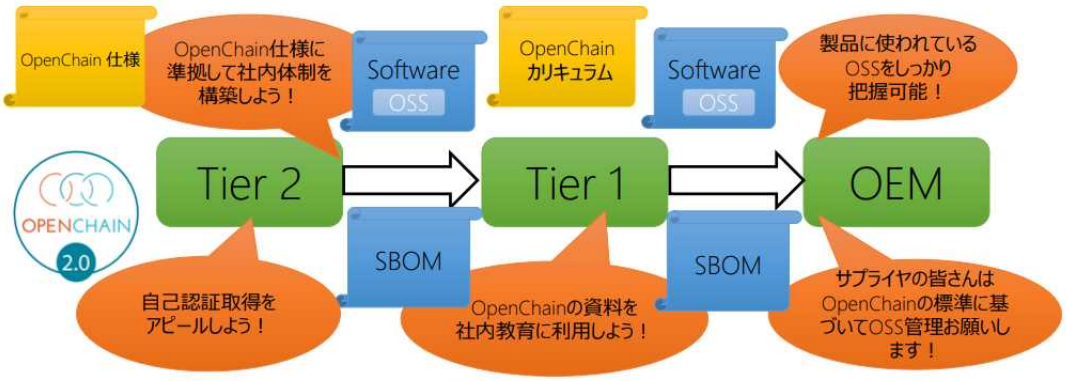


図 4.1-2　OpenChain の成果物の活用イメージ[27]

①の仕様については、2020 年 12 月に ISO/IEC5230 として国際標準化された。国際標準化により認知度が向上することで、より多くの企業が仕様への適合について認証を取得することが期待されている。トヨタ自動車では、自社の OSS 管理の取組について、国際標準化の前から OpenChain 仕様に合わせたチェックと不足部分の対応を進めており、国際標準化後、世界で初めて仕様への適合（自己認証）を発表している。現在、仕様に適合している部署が一部に限られているため、全社に広めるべく、取組が進められている。

OpenChain には、複数のワーキンググループ（WG）があり、トヨタ自動車は、Japan WG[28]や Automotive WG[29]において中心的な役割を担い、貢献している（表 4.1-2）。Japan WG では SPDX Lite の議論をはじめ、7 つのサブワーキンググループ（SWG）がそれぞれのテーマの下に活動している。Automotive WG では、ベストプラクティスの共有や OSS コンプライアンスの重要性に関する周知活動等を実施している。

[27] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 3 回資料より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf
トヨタ自動車では図中の SBOM（Software Bill of materials）に SPDX Lite を採用している。

[28] OpenChain に参加する日本企業が主体となっている WG である。

[29] OpenChain に参加する自動車関連企業が主体となっている WG である。

表 4.1-2 各 WG の概要[30]

WG 名称	**OpenChain Japan WG**	**OpenChain Automotive WG**
設立時期	2017 年 12 月	2019 年 7 月
参加企業	トヨタ自動車、ソニー、日立等、 国内 70 社以上	トヨタ自動車、ボッシュ、パナソニック等 （国内外 12 の自動車メーカー含む）
目的	OSS コンプライアンスに関して、日本企業ならではの課題や解決策を日本語で情報交換する場所を作ることを目的としている。	3 つの目的が設定されている。 • 自動車業界内のベストプラクティス共有 • OSS サプライチェーンマネジメントの自動車業界標準の検討 • OSS コンプライアンスの重要性の業界内での周知活動
活動内容	企業や組織がオープンソースライセンスのコンプライアンスを遵守していくための基準や支援、各情報の翻訳等を実施している。また、SWG レベルでテーマを設定し、それぞれ活動を行っている。	参加企業間で各企業の取組紹介等を実施している。2020 年度は、プラクティス集の作成等を予定している。
SWG	• Planning SWG • FAQ SWG • Leaflet to Supplier SWG • Education material for roles SWG • License information exchange SWG ※ • Tooling SWG • Promotion SWG ※SPDX Lite について議論	−

各参加企業の OSS コンプライアンスに関する取組結果は OpenChain にフィードバックされ、より良い

[30] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 3 回資料及びヒアリングを基に作成
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf

成果物を生み出すために議論される。これによって、各参加企業によるオープンな PDCA サイクルが形成されている。

また、OpenChain には、自動車業界のサプライヤ企業も参加している。したがって、最終製品メーカーのみの意図によって業界標準を策定しているわけではない。そのため、サプライヤ側からの理解も得られやすく、今後の拡大が期待されている。

トヨタ自動車は、自社の取組結果に対して、前述のオープンな PDCA サイクルを回すことによって、以降の取組の精度を高めている。あわせて、その PDCA サイクルの恩恵は、サプライチェーン全体に波及し、サプライチェーン全体における OSS コンプライアンスの取組を底上げする効果が発揮されている（図 4.1-3）。

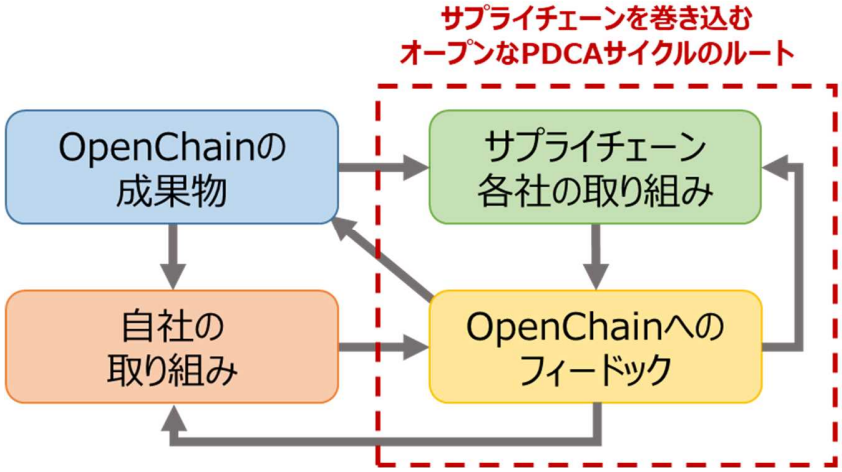


図 4.1-3　OpenChain におけるオープンな PDCA サイクル[31]

さらに、トヨタ自動車は、OpenChain の活動以外にも、OSS 利活用の促進に向けて、以下の活動を実施している。

① OSS ライセンス解釈の負荷を軽減するためのツールの共同開発

② 展示会等における SBOM の普及活動

以下、各取組の詳細について記載する。

① OSS ライセンス解釈の負荷を軽減するためのツールの共同開発

トヨタ自動車は、日立製作所及び日立ソリューションズと OSS ライセンス解釈の負荷を軽減するた

[31] ヒアリングを基に作成

めのツール「OSS License Simple Viewer」を共同開発した。これは、OSS ライセンスが英語記載で複雑なものがある中、ライセンスの種類やその OSS の用途を入力するだけで、そのライセンスの責務・免責事項が表示され、簡単にその内容を把握できるツールとなっている。また、企業ごとのライセンス解釈によって、表示される責務・免責事項をカスタマイズすることも可能である。

本ツールは、より多くの企業に使用してもらい、OSS 利活用の助けとなることを目的に、ツール自体も OSS として公開[32]されている。今後は、本ツールが企業における OSS 管理の仕組みやシステム等と連携しつつ、より付加価値のあるツールに改良されていくことが期待されている。

② 展示会等における SBOM の普及活動

トヨタ自動車は、OSS 利活用に伴う SBOM 作成について、展示会等でその必要性等をアピールする活動にも貢献している。一例として、2020 年 1 月に開催された CES2020[33]の際に、トヨタがサポートする Linux Foundation プロジェクトである Automotive Grade Linux のブースにて、OpenChain Automotive WG の活動の一環として SPDX Lite 作成のデモを行った。無償ツールを活用して SPDX Lite を簡単に作成できること等をアピールし、来場者に SBOM 利用の啓発を図った。他にも、SBOM 作成ツールを提供している企業のセミナー等で SBOM の重要性を訴求する等の活動を行っている。トヨタ自動車としては、このような場を通じて、引き続き SBOM 管理の必要性等を含む OSS 利活用に向けた情報発信を行いたいと考えている。

[32] OSS License Simple Viewer
https://github.com/OLSV-oss/OSSLicenseSimpleViewer
[33] 毎年 1 月に米国ラスベガズで開催される電子機器の見本市

4.2. ソニー　～各事業部による主体性のある取組～

■ 企業情報・本事例集における位置づけ

本社	東京都港区
業種	電気機器
従業員数（連結）	111,700 人（2020 年 3 月末現在）
商流	製品商流/最終製品メーカー
観点	「ライセンス」「脆弱性対応」「サプライチェーン管理」「組織体制」「コミュニティ活動」

■ 本事例のエッセンス

- OSS 管理において、一定の基準を設けることで品質は担保しつつ、各事業部の裁量に任せることで、ソニーの多様な製品群をフォローすることが可能となっている。
- OSS ライセンスコンプライアンス対応として、組織横断型の対応体制を構築するとともに、OpenChain Japan WG[34]への参画を通じたサプライチェーン管理の強化に取り組んでいる。

■ 背景・課題

ソニーでは、多様な製品ラインナップを持つ中で、それぞれの事業部がそれぞれの製品市場に対して最適な対応を取れるよう、プロセスやルールを定めている。OSS のライセンス対応、ソフトウェア管理についても、企業として製品の品質を担保しながら、各製品の競争力を失わないよう事業部ごとに柔軟にその手法を検討・採択しなくてはならない。

■ 取組

＜【ライセンス(L2-1)】【脆弱性対応(V2)】OSS 管理（製品セキュリティ）における各事業部の柔軟な対応＞

ソニーは、2000 年頃から OSS 利活用のメリットを認識し、OSS を利用してきた。当初は、OSS の適切なライセンス対応に必要となる取組から実施し始め、その知見も活かしながら OSS 管理（製品セキュ

[34] OpenChain Japan WG の具体的な取組については、トヨタ自動車の事例に記載

リティ）にも取組を拡大してきた。

製品セキュリティの取組としては、全社の品質マネジメントシステム（QMS）[35]に基づき、各事業部にて各製品の使用 OSS の把握、リスト管理及び定期的な更新を徹底している。

また、OSS の脆弱性が発見された際は、Sony PSIRT[36]が中心となり、そのハンドリング[37]を実施する。

なお、QMS に基づく製品セキュリティの取組は、各事業部の状況に合わせて裁量を持たせる形で運用されている。

これは、各事業部の製品によって、開発プロセスや保有するリソースが異なる中で、柔軟にその方法を選択できることが最も効率的なためである。これにより、QMS の情報品質を担保しつつ、ソニーが持つ多様な製品群をフォローすることが可能となっている。

＜【ライセンス(L2-2)】【サプライチェーン管理(S2)】【組織体制(O2)】【コミュニティ活動(C2)】OSS ライセンスコンプライアンス対応に係る体制とコミュニティ活動＞

ソニーでは、OSS ライセンスのコンプライアンス体制について、2010 年には組織横断型の対応組織を構築し、現在に至っている。これは、法務、知財、広報、品質管理のコーポレート部門、ほぼすべての事業部、海外事業拠点から選出されたメンバーが参画する社内委員会を形成し、OSS ライセンスのコンプライアンスに係る取組を推進している（図 4.2-1）。これにより、社内の様々なノウハウが活用できるとともに、取組の推進主体が各事業部に分散することで、その事業部の状況に沿った柔軟な展開が期待できる。

[35] Quality Management System:製造物や提供されるサービスの品質を管理・監督するシステム 品質管理を中心とした組織の活動で顧客満足を達成し継続的な改善を意図する。

[36] Product Security Incident Response Team: 自社で製造・開発する製品やサービスを対象に、セキュリティレベルの向上やインシデント発生時の対応を行う組織。Sony PSIRT では、各事業部と緊密に連携し、ソニー全社の多様な製品群に対応するため、定期的に関係者とのコミュニケーションの場を設定する等の工夫をしている。

[37] 製品脆弱性に関する情報の収集、受付窓口、対応判断、関係部署への伝達等を実施

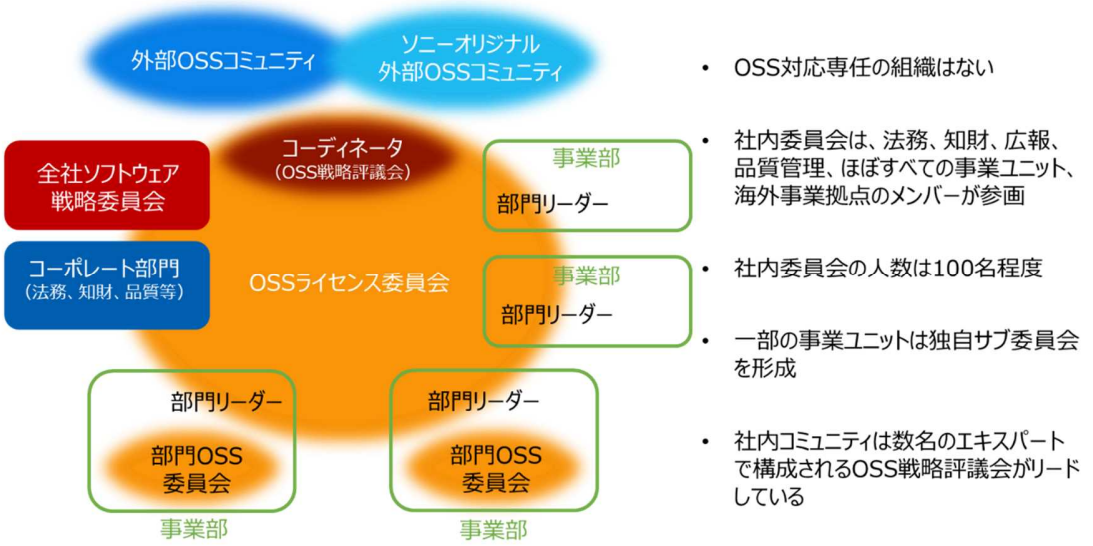


図 4.2-1 ライセンス対応における組織横断型体制のイメージ[38]

なお、現在のライセンス対応における具体的な取組としては、OpenChain Japan WG のプラチナメンバーとして、その活動をリードすることによりサプライチェーン管理を強化している点があげられる。これは、ソニー製品の SoC[39]ベンダ、OEM[40]/ODM[41]ベンダ等のサプライヤから提供されるソフトウェアに含まれる OSS を、適切に把握しなくてはならないという課題意識が基となっている。ソニーでは、これまで特に海外サプライヤにおける OSS 使用状況の把握に苦労をしてきた経緯があった。その中で、ソニー単体でサプライヤに対応を働きかけるよりも、OpenChain Japan WGとして、連携して働きかけることが有効であるとの考えに至っている。

例えば、OpenChain Japan WG で作成した成果物（OSS ライセンスコンプライアンスに関する啓発資料等）を、日本国内のみならず、英語、さらに中国語（繁体字、簡体字）、ベトナム語に翻訳の上で広くグローバルに発信をしている（図 4.2-2）。また、OpenChain Japan WG として、海外のメ

[38] OpenChain Japan WG 会合資料を基に作成
https://wiki.linuxfoundation.org/_media/openchain/openchainjwg_organization_lt_20180419_jpen_.pdf

[39] System on a Chip:一個の半導体チップ上にシステムの動作に必要な機能の多く、あるいは全てを実装するという設計手法

[40] Original Equipment Manufacturing（Manufacturer）:他社ブランドの製品を製造すること、あるいはその企業

[41] Original Design Manufacturing（Manufacturer）: 他社ブランドの製品を設計・製造すること、あるいはその企業

ーカー・サプライヤ等と積極的に交流する活動も続けている。そのかいもあり、韓国、中国、インド、ドイツ、英国において同様の WG が立ち上がる等、OSS のコンプライアンスに対する認識の高まりが広がっている。その中で、使用ソフトウェアの開示等の対応に海外サプライヤが理解を示す等の変化が現れ始めている。

現在、OpenChain Japan WG の活動は大企業中心となっているものの、今後はその活動の裾野を広げ、中小企業も取り込むことで、更に効果を高めることが期待されている。

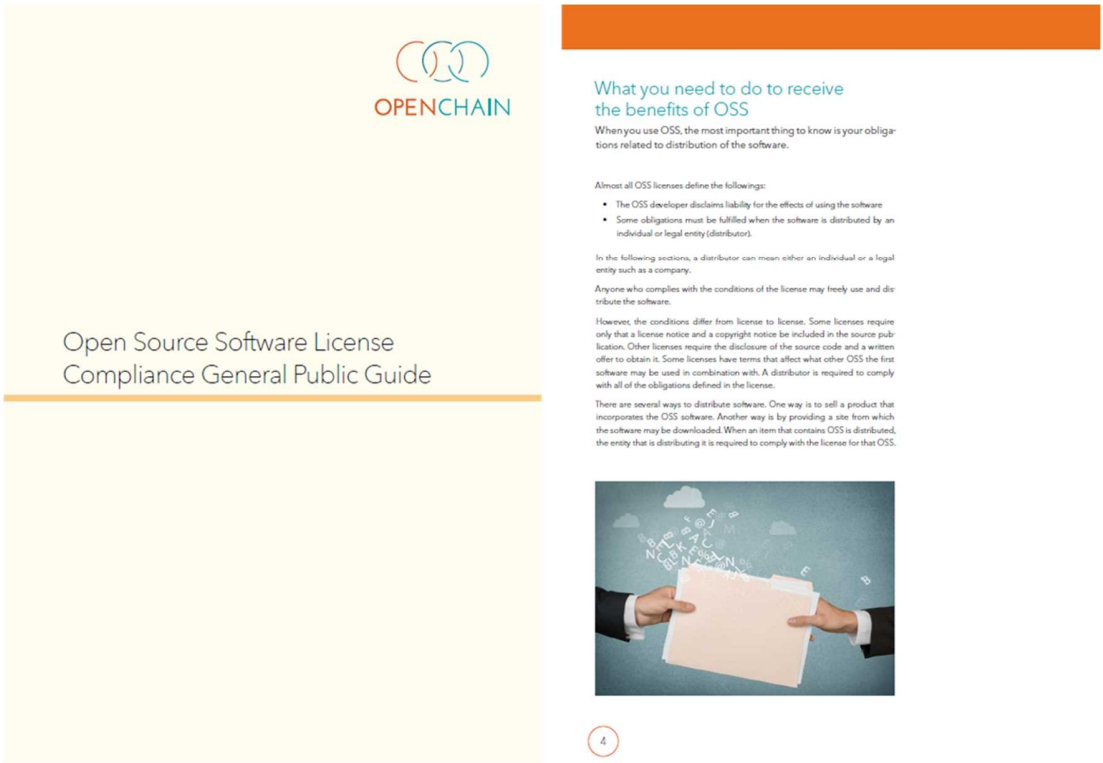


図 4.2-2　OSS ライセンスコンプライアンスの重要性を周知するリーフレット（英語版）[42]

[42] サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース 第 3 回資料より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_bunyaodan/software/pdf/003_04_00.pdf
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/tree/master/supplier-leaflet

4.3. オリンパス　～ヒヤリ・ハット事象を契機とした全社的取組～

■ 企業情報・本事例集における位置づけ

本社	東京都新宿区
業種	精密機器
従業員数（連結）	35,174 人（2020 年 3 月末現在）
商流	製品商流/最終製品メーカー
観点	「ライセンス」「サプライチェーン管理」「個の能力・教育」「組織・体制」「コミュニティ活動」

■ 本事例のエッセンス

- 過去のヒヤリ・ハット事象を契機に、OSS ライセンスのコンプライアンス対応に向けたソフトウェア管理を全社的な取組へと発展させた。
- 「体制」「プロセス」「ツール」「教育」「サプライチェーン管理」の観点において、重点的に仕組み作りを行い、OSS ライセンスのコンプライアンス体制を整えた。

■ 背景・課題

オリンパスの製品は、医療、映像、科学と多岐にわたる。また、それら製品は多様なサプライチェーンからの部品・ソフトウェア供給を基に製造されている。その中で、納入品における OSS ライセンスのヒヤリ・ハット事象発生を契機に、全社統一で適切なソフトウェア管理の必要性が認識されていた。

■ 取組

＜【ライセンス(L3)】【サプライチェーン管理(S3)】【個の能力・教育(P3)】【組織・体制(O3)】【コミュニティ活動(C3)】ヒヤリ・ハット事象を契機とした全社的取組＞

オリンパスでは、過去、サプライヤに開発依頼をしたソフトウェアにライセンス違反となりかねない形で OSS が用いられていたことが発覚するヒヤリ・ハット事象が発生していた。当該ソフトウェアを搭載した製品の出荷直前で至急 OSS ライセンスに係る対応を実施し、事無きを得たものの、この事象を受け、OSS ライセンスのコンプライアンスへの取組を徹底することとなった。

取組の方針として、OSS を使用するのであればライセンスを遵守すること、及び使用する意図のない OSS の混入を防ぐこと、の 2 点を念頭に置いた仕組み作りが目指された。具体的には、主に以下 5 つの観点において取組が進められた。

① 体制

② プロセス

③ ツール

④ 教育

⑤ サプライチェーン管理

以下、各取組の詳細について記載する。

① 体制

体制面においては、OSS ライセンスに係る全社委員会（OSS 推進会議[43]）を立ち上げた。各事業部及びコーポレート部門から代表メンバーを出し、OSS コンプライアンスに関する施策の意思決定や情報共有等を行っている（図 4.3-1）。

特に、各事業部（医療、映像、科学）では、それぞれの市場の特性があるため、全社統一的な方針等の決定においては全社委員会における意見の擦り合わせが重要になってくる。また、全社委員会においては、原則的な事項（OSS 利用方針等）は意思決定するものの、具体的な部分は各事業部の裁量に委ねるといった形で柔軟性を持たせる工夫も行っている。

[43] メンバーの規模は 10 名程度で、月 1 回程度定期的に開催している。事務局は OSS 対応専任組織である OSS コンプライアンス室が担っている。

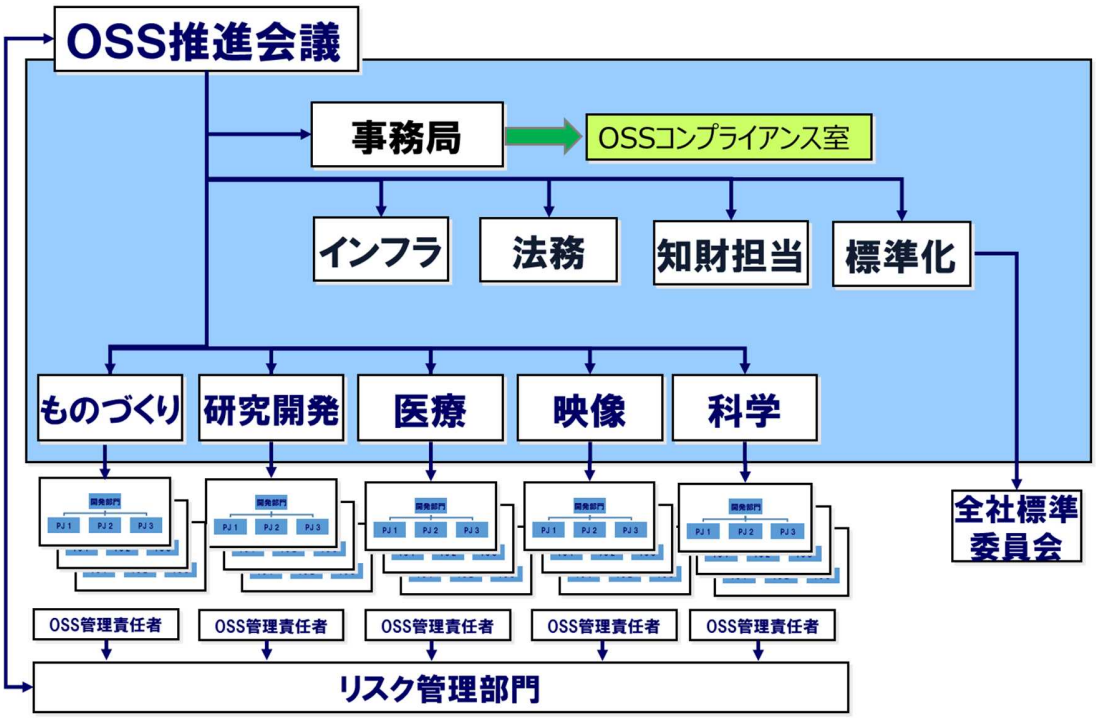


図 4.3-1 全社委員会の体制図[44]

② プロセス

プロセス面においては、OSS 対応手順としての一連のプロセスを定め、既にあった全社の製品化に係るプロセス（以下、「標準プロセス」という。）に組み込んだ（図 4.3-2）。

[44] オリンパス提供資料を基に作成

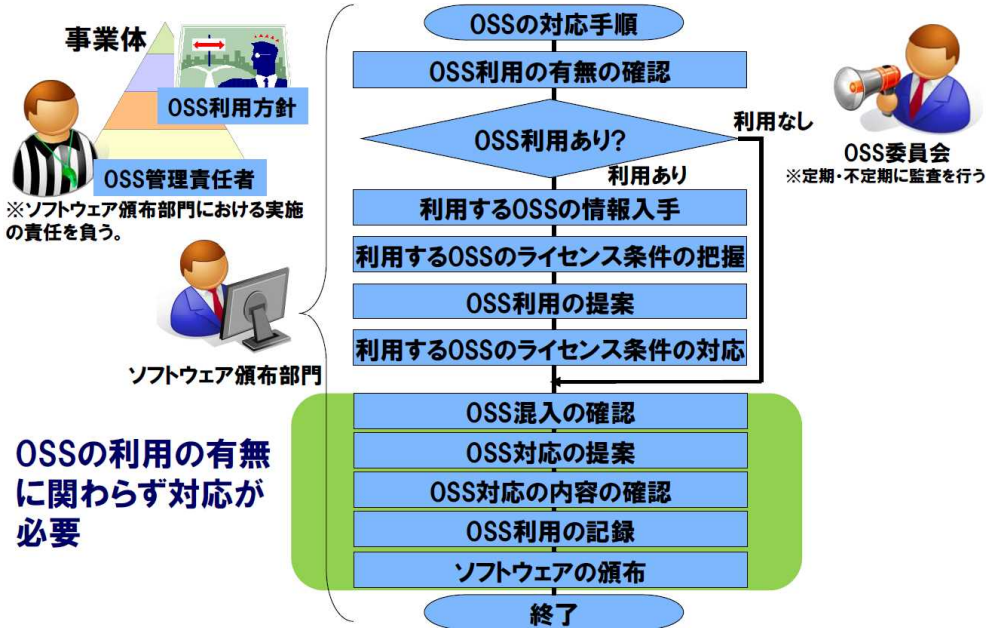


図 4.3-2 全社標準プロセスに含まれた OSS 関連プロセス[45]

そのプロセスにおいては、OSS 利用申告の有無に関わらず、商用ツールを用いて、全ての製品に対して OSS の混入がないかを確認しなくてはならない。また、その確認結果（使用 OSS 情報）やライセンス対応方法は、定められたフォーマット（OSS 報告書（図 4.3-3））に基づき事業部で取りまとめ、OSS コンプライアンス室に提出をしなくてはならない。OSS コンプライアンス室では、それらの情報を最終確認し、記録、管理する。事業部によっては、それらの記録をソフトウェア脆弱性対応時に参照先として活用している。

新しいプロセスが追加されることに開発現場等から負荷が増えるとして反発はあったものの、もともと標準プロセスを遵守する企業文化は醸成されていたため、OSS に係るプロセスを標準プロセスに組み込むことで自然と遵守されていった。また、あるグループ会社で先行して本プロセスを実践し、その効果を明確にすることで納得感を得る工夫も行った。

[45] オリンパス提供資料より抜粋

<table>
<tr><th>#</th><th colspan="6">OSS ごとの情報</th></tr>
<tr><td rowspan="12">1</td><td colspan="6">基本情報</td></tr>
<tr><td colspan="2">名称</td><td colspan="4"></td></tr>
<tr><td colspan="2">バージョン</td><td colspan="4"></td></tr>
<tr><td colspan="2">開発者（著作権者）名</td><td colspan="4"></td></tr>
<tr><td colspan="2">取得元の URL</td><td colspan="4"></td></tr>
<tr><td colspan="2">ライセンス条件</td><td colspan="4"></td></tr>
<tr><td colspan="2">ライセンス名称</td><td colspan="4"></td></tr>
<tr><td colspan="2">ライセンスタイプ</td><td>GPL タイプ</td><td>LGPL タイプ</td><td>MPL タイプ</td><td>BSD タイプ</td></tr>
<tr><td colspan="6">利用方法</td></tr>
<tr><td colspan="2">リンク形式</td><td>静的リンク</td><td>動的リンク</td><td>プロセス間通信</td><td>独立したプログラム</td></tr>
<tr><td colspan="2">ソースコードの改変</td><td colspan="2">あり</td><td colspan="2">なし</td></tr>
<tr><td colspan="6">ライセンス条件の具体的対応方法</td></tr>
<tr><td colspan="2">著作権の表示方法</td><td colspan="4"></td></tr>
<tr><td colspan="2">ライセンス本文の表示方法</td><td colspan="4"></td></tr>
<tr><td colspan="2">免責事項・無保証・特許などに関する記載の表示方法</td><td colspan="4"></td></tr>
</table>

図 4.3-3　OSS 報告書に記載する OSS に関する情報[46]

③ ツール

ツールについては、2 つのツールを活用している。1 つは、前述のとおり、OSS 混入を確認する商用ツールである。なお、②と同様、あるグループ会社で先行してそのツールを活用し、効果を確かめた上で全社展開するといった工夫も行った。現在では、グループ全体でそのツールを利用しなくてはならない。

もう 1 つは、OSS に関する情報集約のためのナレッジサイトを構築している。OSS 利用に際しての注意点、ライセンスの種類、社内の製品の OSS の利用状況等の情報を提供している。

④ 教育

OSS コンプライアンス遵守に係るプロセスや各種ツールの使い方を周知するための教育プログラムも充実させている（図 4.3-4）。実務者のみならず、経営層[47]やパートナー向けの OSS 教育[48]も実施している。また、英語の教材等も用意することで、海外拠点の社員も教育を受けることが可能である。

[46] オリンパス提供資料より抜粋

[47] 執行役員及び事業部の幹部向けに技術者認定団体のトップによる講演会等を開催

[48] 社員向けの基礎教育資料「OSS 基礎」（図 4.3-4 内）と同様の内容を一部社外向けにカスタマイズした教育メニューである。

図 4.3-4 多様な対象者を想定した教育メニュー[49]

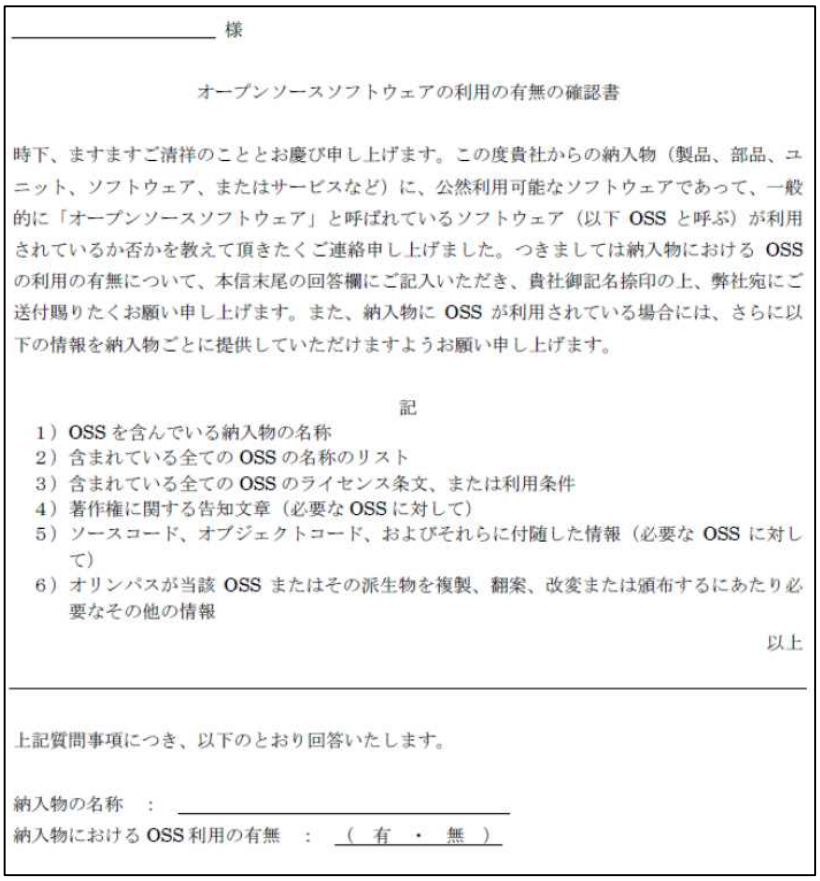
⑤ サプライチェーン管理

サプライチェーン全体に対して OSS コンプライアンスの啓発を実施する目的で、OpenChain Japan WG[50]に参加している。これは、前述のようなヒヤリ・ハット事象を防ぐには、社内、グループ内の取組だけではなく、サプライチェーンへの働きかけが必要との課題意識が契機となっている。

オリンパスでは、サプライヤからの部品・ソフトウェア納入の際に、確認書（OSS 利用の有無の確認書（図 4.3-5））の提出を求めている。このような対応等に対するサプライヤの理解を得るため、OpenChain Japan WG を活用して発信を行っている。具体的な発信の一例として、OpenChain Japan WG において、前述の OSS 報告書フォーマットの運用について共有を行ったことがあげられる。それがきっかけとなり、OpenChain Japan WG 発信の SBOM フォーマット（SPDX Lite）検討につながった。

[49] オリンパス提供資料より抜粋

[50] OpenChain Japan WG の具体的な取組については、トヨタ自動車の事例に記載



＿＿＿＿＿＿＿＿＿＿ 様

オープンソースソフトウェアの利用の有無の確認書

時下、ますますご清祥のこととお慶び申し上げます。この度貴社からの納入物（製品、部品、ユニット、ソフトウェア、またはサービスなど）に、公然利用可能なソフトウェアであって、一般的に「オープンソースソフトウェア」と呼ばれているソフトウェア（以下 OSS と呼ぶ）が利用されているか否かを教えて頂きたくご連絡申し上げました。つきましては納入物における OSS の利用の有無について、本信末尾の回答欄にご記入いただき、貴社御記名捺印の上、弊社宛にご送付賜りたくお願い申し上げます。また、納入物に OSS が利用されている場合には、さらに以下の情報を納入物ごとに提供していただけますようお願い申し上げます。

記

1）OSS を含んでいる納入物の名称
2）含まれている全ての OSS の名称のリスト
3）含まれている全ての OSS のライセンス条文、または利用条件
4）著作権に関する告知文章（必要な OSS に対して）
5）ソースコード、オブジェクトコード、およびそれらに付随した情報（必要な OSS に対して）
6）オリンパスが当該 OSS またはその派生物を複製、翻案、改変または頒布するにあたり必要なその他の情報

以上

上記質問事項につき、以下のとおり回答いたします。

納入物の名称　：　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

納入物における OSS 利用の有無　：　（ 有 ・ 無 ）

図 4.3-5　OSS 利用の有無の確認書[51]

[51] オリンパス提供資料より抜粋

4.4. 日立製作所　～製品化の過程における徹底したOSS管理～

■ 企業情報・本事例集における位置づけ

本社	東京都千代田区
業種	電気機器
従業員数（連結）	約301,000人（2020年3月末現在）
商流	製品商流/最終製品メーカー
観点	「ライセンス」「コミュニティ活動」

■ 本事例のエッセンス

- IT製品においては、その製品化の過程で、ソフトウェア部品構成表（SBOM）による管理と商用ツールによるOSSのチェックを必ず実施することで、OSS管理の一元化・効率化、及びライセンスコンプライアンスの徹底を実現している。
- コミュニティ活動における幅広い貢献を行い、その成果を自社の事業展開に還元している。

■ 背景・課題

日立製作所は、1990年代後半より、Linux等へのコミュニティ貢献をはじめ、OSSの普及促進に尽力してきた。現在でも、OSSの利活用を成長戦略の重要な要素と位置づけ、OSSに対する取組を一層強化している。

■ 取組

＜【ライセンス(L4)】製品化の過程におけるソフトウェア部品構成表（SBOM）活用と商用ツール利用＞

日立製作所では、OSS対応専任組織であるOSSソリューションセンタとコーポレート部門（知的財産、法務、調達、QA[52]部門）等が連携し、OSS利活用の普及促進及び支援等を行っている。また、OSSセキュリティにおける技術的な側面（脆弱性対応、ツール開発・運用等）については、セキュリティ事業統括本部と連携して対応している。

[52] Quality Assurance：品質保証

日立製作所における OSS の利活用は多岐に渡る。特に、情報処理機器や通信機器、ソフトウェア等の IT 製品、及びサービス分野、SI 分野においては、多くの OSS が使用されているため、ライセンスコンプライアンスの面等から、OSS 管理を徹底している。具体的には、以下の 2 点の取組を行っている（図 4.4-1）。

① ソフトウェア部品構成表（SBOM）を活用したシステムによる管理

② 商用ツール活用による OSS の効果的な把握

以下、各取組の詳細について記載する。

① ソフトウェア部品構成表（SBOM）を活用したシステムによる管理

日立製作所は、自社にとって最適な管理を実現するため、SBOM を活用した管理システムを自社開発し、2013 年にソフトウェア開発部門で稼働させた。現在では、IT セクター（IT 製品、サービス分野、SI 分野）で活用されている。

現在の IT セクターにおいては、この管理システムによって OSS が一元管理され、OSS 利用に関する社内外の情報を集約することで、効率的なライセンス調査等が実施できている。また、使用 OSS のデータベース化やワークフローシステムの機能により、トレーサビリティの確保や手続き面の効率化も可能となっている。

開発チームは、製品開発段階において、使用する OSS を管理システムに登録する。登録された OSS は、過去の使用実績等も踏まえながら、審査ワークフローシステムを通じて、ライセンス面で使用することが適切であるかチェックされる。各プロジェクトの使用 OSS は、SBOM が作成された上でデータベースに登録、使用実績として蓄積され、次期開発にフィードバックされる。

② 商用ツールの活用による OSS の効果的な把握

日立製作所の IT セクターにおいては、開発初期段階における OSS のライセンス調査や、開発委託品[53]及びリリース前の製品に未認識の OSS が含まれてないかチェックする目的で商用ツールを導入している。これにより、管理システムへの登録だけでは把握しきれなかった OSS によるライセンス違反を防止している。また、商用ツールによって検知された OSS は、前述の管理システムに自動登録される。なお、製品リリース後のソフトウェア脆弱性対応においても商用ツールの機能（脆弱性発生時のメール通知機能）が活用されている。

[53] 開発委託品については、OSS を使用する場合は事前通知する旨を委託先との基本契約書に盛り込むことや、開発委託をする際に OSS の使用可否を発注の条件書に記載する等の対応も行っている。

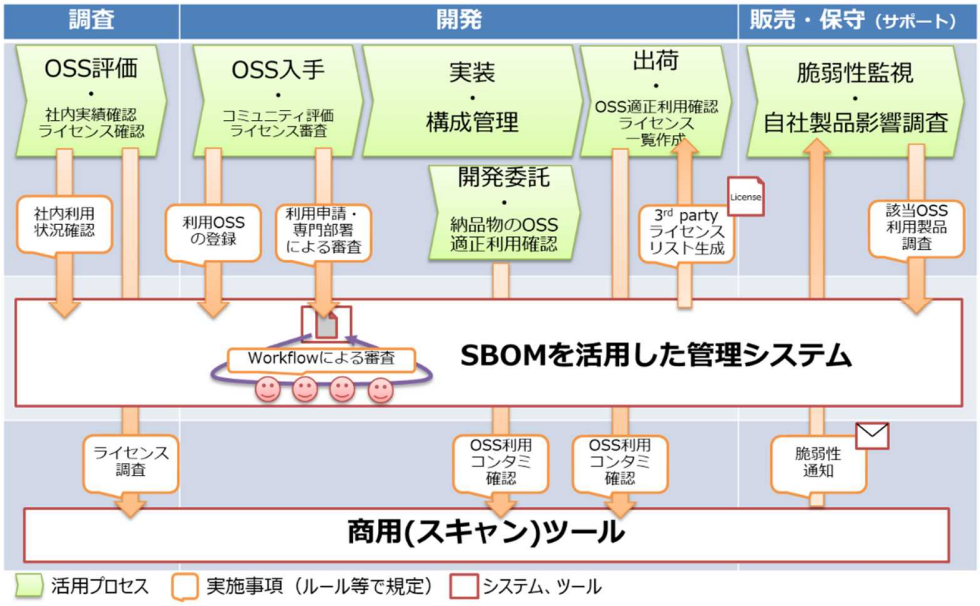


図 4.4-1 開発プロセスにおける管理システム及び商用ツールの活用状況[54]

IT 製品においては、これらの管理システム及びツールを用いることが社内規則として定められており、製品化に至るための必須実施項目となっている。一方で、開発現場からは OSS の登録作業等に作業負荷がかかるといった声もあがっていたため、ソフトウェアの開発支援を主に行っている部署が一部 OSS の登録を代行するメニューを設ける等の工夫も行っている。

さらに、OSS 管理の中で、システム、ツール、情報サイト等における OSS の名称が統一されておらず、その判別に苦労する場面が発生している。その対応として、AI を用いて各名称を整理する仕組みの構築についても検討を進めている。

現在、OT （Operational Technology）分野の事業でも、独自のソフトウェア構成管理や脆弱性対応の仕組みはあるものの、IT 製品と同等のレベルにまで達するよう、これらの管理システム及びツール利用を拡大している最中である。

＜【コミュニティ活動(C4)】コミュニティ活動における幅広い貢献＞

[54] 日立製作所提供資料を基に作成

日立製作所は、OSS の利活用の更なる拡大を目的に、 OSS の開発、調査・検証、普及促進に係る各種コミュニティ活動に、社員をメンバーとして参画させる等、幅広い貢献をしている（図 4.4-2）。

図 4.4-2 日立製作所が参画する主なコミュニティ[55]

日立製作所では、自社の持つ多様な事業領域との関連性を見極めながら、多数のコミュニティに参画している。結果的に、それらのコミュニティ活動の成果は、日立製作所自身の事業展開にも還元されている。具体的には、それらのコミュニティにおける OSS 開発の実績を社外講演等でアピールすることで顧客から案件の引き合いを得たり、コミュニティ活動の中で把握した先進的な取組やベストプラクティスを自社プロセスの効率化や研修内容の見直し等に繋げている。

また、国内外の様々なイベントでの講演や各種メディアを使った情報発信[56]を積極的に実施する等、日立製作所は OSS 利活用の普及促進の流れをリードしている。OSS の利活用支援のソリューションも提供しており、その提供先は金融、公共、通信、ヘルスケア等と多岐に渡っている。

[55] 日立製作所提供資料より抜粋

[56] OSS に対する自社の取組や OSS 活用の具体的なユースケースの紹介等を行っている。

4.5. オムロン　～PSIRT の連携を通じた OSS 対応～

■ 企業情報・本事例集における位置づけ

本社	京都府京都市
業種	電気機器
従業員数（連結）	28,006 名（2020 年 3 月末時点）
商流	製品商流/最終製品メーカー
観点	「脆弱性対応」「サプライチェーン管理」「個の能力・教育」「組織体制」

■ 本事例のエッセンス

- 本社部門と各事業体からメンバーを集めて PSIRT を組織し、役割分担を明確にした上で連携をしながら、OSS に係る管理や教育、脆弱性対応等を実施している。
- 本社部門と各事業体の連携のための協議体としてワーキンググループを設置し、製品セキュリティ等に係る改善策やグループ統一のルールに係る議論、定期的な情報交換等を実施している。

■ 背景・課題

オムロンでは、制御機器・FA システム、電子部品、ヘルスケア、社会システム等、多様な事業ポートフォリオを、一部分社化も含めたカンパニー制にて展開している。その中で、OSS 対応等を含むセキュリティの取組について、本社部門と各事業体が適切に連携しつつ実施する必要がある。

■ 取組

＜【脆弱性対応(V5-1)】【サプライチェーン管理(S5)】【個の能力・教育(P5)】【組織体制(O5-1)】PSIRT 体制及び本社部門と各事業体の連携＞

オムロンでは、本社部門と各事業体（カンパニー及び事業子会社）からメンバーを集めて PSIRT が組織されており、OSS 対応等を含む製品セキュリティへの取組を進めている。本社部門では、製品の品質、セキュリティに対するグループ統一のルール策定、及び調整を実施している。一方、各事業体では、担当製品に係るセキュリティについて実務的な対応等を行う体制となっている。

本社部門と各事業体は、定期的に製品セキュリティに関するワーキンググループ（協議体）を開催し、

製品セキュリティ等に係る改善策やグループ統一のルールに係る議論、脆弱性情報等に対する対処事項の周知徹底、及びその他情報交換を実施している（図 4.5-1）。

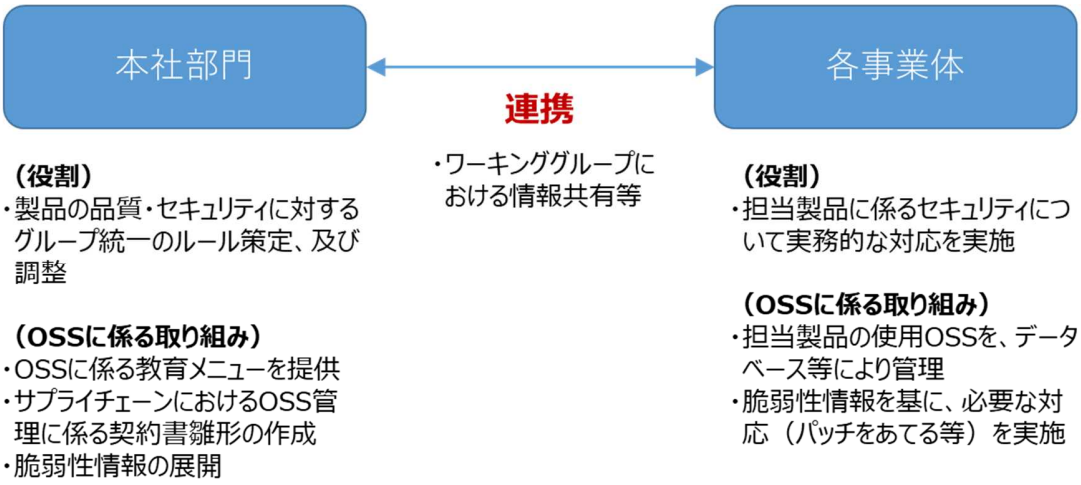


図 4.5-1 本社部門と各事業体の役割分担及び OSS に係る取組[57]

具体的な OSS 対応に係る取組は、各事業体において、担当製品の使用 OSS をデータベース等によって管理することにより実施されている。事業体によってセキュリティの要求レベルや OSS の使用頻度が異なっているため、セキュリティに対するグループ統一のルールには沿いつつも、OSS の管理粒度やその手法については事業体ごとに判断している。商用ツールを用いて管理を実施する事業体もある。

一方、本社部門においては、各事業体の OSS 管理を補完している。具体的には、開発者向けに、OSS の概要、OSS の管理リスク（OSS が意図せず混入するケース等）、ライセンスコンプライアンス等を中心とした、OSS に係る教育を実施[58]している。教育の内容に応じて、法務部門や開発プロセス改善部門の担当者が講師を担う等、より実務に即する工夫もなされている。また、マネージャー層等、開発者以外が受講するケースもあり、全社のリテラシーの底上げにも寄与している。

また、本社部門では、サプライチェーンの中で意図せず OSS が混入することのないよう、外部の委託開発先と取り交わす契約書の雛形も整備している。雛形では、委託開発先に対し、OSS を原則使用しないこと、使用する場合にはその OSS を通告すること等を定めている。各事業体の担当者は、この雛形を活用しつつサプライチェーンの OSS についても適切に管理している。

[57] ヒアリングを基に作成

[58] 対面、もしくは Web による教育を実施している。

＜【脆弱性対応(V5-2)】【組織体制(O5-2)】ソフトウェア脆弱性対応に係る PSIRT の連携＞

オムロンでは、本社部門の PSIRT 担当者が定常的に OSS の脆弱性情報を収集しており、OSS の脆弱性が判明した際には、関連する事業体の PSIRT 担当者にその情報をメールで展開している。情報セキュリティ早期警戒パートナーシップから取得した脆弱性情報にはテクノロジーキーワード[59]が付されているため、そのキーワードを基に関連する事業体を特定する他、本社部門の PSIRT 担当者の判断の下、重要な脆弱性については対応の優先度を高めるようフラグを付けて展開する等の工夫を行っている。各事業体では、展開された情報を基に対象の OSS にパッチを当てる等の対応をとっている。また、その対応状況はリスクの程度に応じて本社部門にも報告がされる。なお、脆弱性情報は、情報セキュリティ早期警戒パートナーシップだけでなく、社内外からの情報が本社部門と各事業体で連携され、脆弱性リスクの評価及び対策が実施されるルールになっている。

現在、オムロンでは、各事業体で実施している脆弱性情報の管理を本社部門にて一元化するシステムの導入を検討している。その目的は、本社部門が一括して管理することによる業務効率化と、過去の OSS に係る対応履歴を全グループで参照可能にすることによる対応判断の精度向上にある。あわせて、脆弱性情報取得時の周知メールの展開についても、当該システムと連携させ、そのフローを自動化させたいと考えている。

[59] JPCERT/CC が、脆弱性情報を受け付ける各ベンダに対して登録を求めている技術用語。ベンダごとにリスト化されており、脆弱性関連情報が報告された際、JPCERT/CC が連絡すべきベンダを選出するための参考情報となる。

4.6. 東芝　～グループにおける一貫した OSS 対応体制～

■ 企業情報・本事例集における位置づけ

本社	東京都港区
業種	電気機器
従業員数（連結）	125,648 名（2020 年 3 月末時点）
商流	製品商流/最終製品メーカー
観点	「脆弱性対応」「組織体制」「選定評価」「ライセンス」「保守・品質保証」「コミュニティ活動」

■ 本事例のエッセンス

- 東芝 SIRT が一次窓口となり、グループにおけるソフトウェア脆弱性対応に関する一貫した対応体制を構築している。
- 共創ソフトウェア開発プラットフォームを構築し、開発成果や OSS コンプライアンスプロセスの成果の再利用による効率化、品質向上、OSS 利活用促進等を図っている。
- 自社の強みである社会インフラ領域で OSS の利活用を拡大させるため、関連するコミュニティ活動に参加している。

■ 背景・課題

東芝は、エネルギー、社会インフラ、電子デバイス、デジタルソリューションを中心とした事業を展開しており、特に社会インフラ領域におけるデジタルトランスフォーメーションを推進している。クリティカルな品質が求められる事業領域の中で、多くの人が安心して東芝の製品・システム・サービスを利用できるよう製品セキュリティに対する取組を強化している。

■ 取組

＜【脆弱性対応(V6)】【組織体制(O6)】東芝 SIRT を中心としたソフトウェア脆弱性対応と SIRT 支援システム＞

東芝では、CISO[60]が製品セキュリティに関する権限を持っている。製品セキュリティの強化に向けて、CISO の下、サイバーセキュリティセンターに設置した東芝 SIRT[61]及び主要なグループ会社の PSIRT が連携するサイバーセキュリティ管理体制を構築し、ソフトウェア脆弱性やセキュリティインシデントへの対応、セキュア開発マネジメント等に重点を置いて取り組んでいる。特に、ソフトウェア脆弱性対応においては、情報セキュリティ早期警戒パートナーシップに参加し、外部機関と積極的に連携しながら、迅速かつ確実な対応をするために東芝グループ全体で一貫した対応体制を構築している。

具体的には、東芝グループの製品・システム・サービスに何らかの脆弱性が発見された場合、東芝 SIRT が一次窓口として脆弱性情報を集約し、社内外への情報共有を図る体制となっている。製品に使用されている OSS 等、ソフトウェアの脆弱性が判明した場合も、東芝 SIRT は、その製品の事業主体であるグループ会社の PSIRT、及び対象製品の事業部と連携し、その対応にあたる（図 4.6-1）。対応した結果を、自社 Web サイトや JVN 等において公表する取組も実施している。

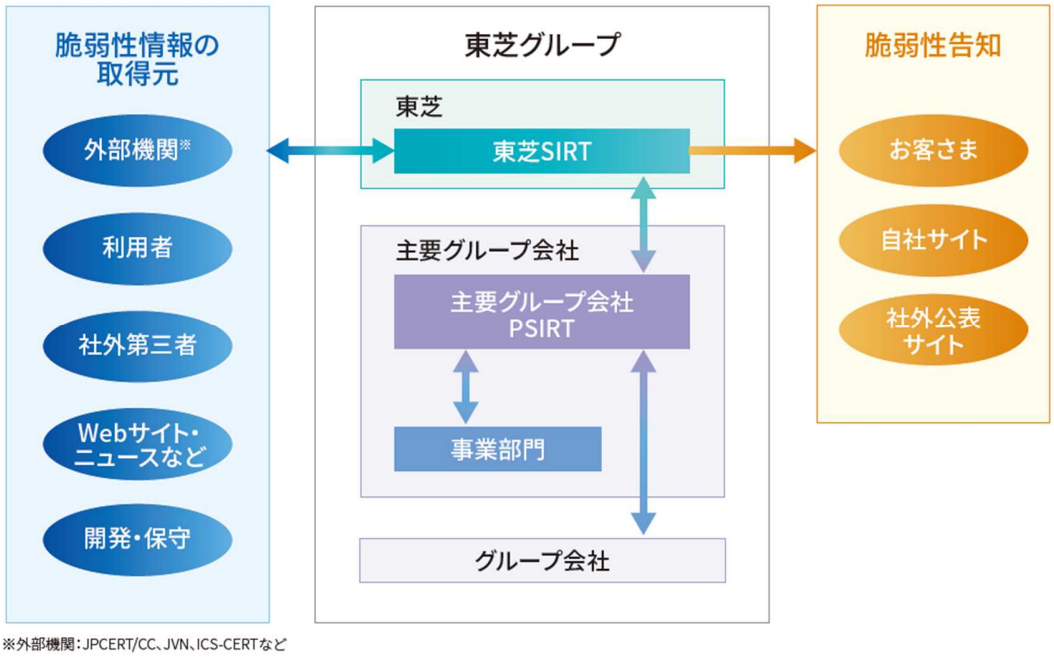


図 4.6-1 東芝グループ脆弱性対応の体制[62]

[60] Chief Information Security Officer：最高情報セキュリティ責任者

[61] Security Incident Response Team：コンピューターシステムなどにセキュリティ上の脅威が発生した際に対応する組織

[62] 東芝グループ サイバーセキュリティ報告書２０２０より抜粋
https://www.global.toshiba/content/dam/toshiba/migration/corp/securityPrivacyAsse

また、東芝では、東芝 SIRT が収集したソフトウェア脆弱性情報をグループ会社や事業部に通知するシステム（SIRT 支援システム）を構築している。これは、登録されたソフトウェア構成情報と脆弱性情報を、CPE[63]もしくは製品名称によって紐づけ、関係個所へ自動的に通知するシステムである（図 4.6-2）。ソフトウェア構成情報については、各グループ会社、各事業部が管理しており、SIRT 支援システムにあらかじめ登録しておく。グループ会社が自社でソフトウェア構成情報を管理するシステムを持っている場合は、その情報を自動連携し SIRT 支援システムに登録できるようにする取組も進めている。脆弱性情報は、JVN や NVD[64]等の脆弱性情報データベースと API 連携し自動収集するほか、顧客等から報告されたものについては手入力により登録する。

また、通知されたソフトウェア脆弱性情報が、グループ会社や事業部でどのように対応されたかをシステム上で管理できる機能を備えており、設計・開発部門、事業部、主要グループ会社のそれぞれの階層に責任者を設け、その責任者を中心にアフターフォローする仕組みとしている。

2020 年 10 月現在、SIRT 支援システムは試行運用中であり、各グループ会社、各事業部にて活用が始まったところである。特に、セキュリティ感度の高い製品を扱うグループ会社（社会インフラ系等）においては、ツール等も用いながらソフトウェア構成情報を漏れなく取得し、SIRT 支援システムに登録を行うなど、活用が進んでいる。

---

ts/security/files/CyberSecurityReport2020.pdf

[63] Common Platform Enumeration：ベンダ名、製品名、バージョンまでを一意に特定できる ID

[64] National Vulnerability Database: アメリカ国立標準技術研究所（NIST）が管理する脆弱性の情報を集めたデータベース

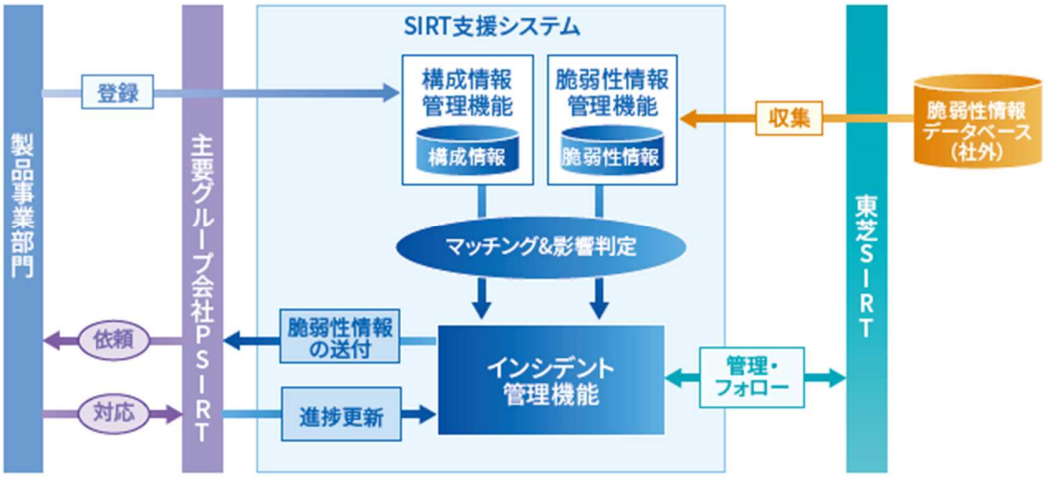


図 4.6-2　SIRT 支援システムの概要[65]

＜【選定評価(S6)】【ライセンス(L6)】【保守・品質保証(M6)】共創ソフトウェア開発プラットフォームを活用した開発成果及び OSS の再利用＞

東芝では、更なる OSS 利活用を見据え、ソフトウェア技術センターが中心となり、共創ソフトウェア開発プラットフォームを構築している。これは、先行している開発で得られた技術的成果や OSS コンプライアンスプロセスの成果を記録・管理し、別の開発で再利用することを可能とする仕組みである。これにより、製品・システム・サービスの開発工数削減や機能改善、品質向上、及び OSS 利活用の促進を図ることが可能となる。共創ソフトウェア開発プラットフォームは、①ソフトウェア開発管理システム、②ソフトウェア資産管理システム、の 2 つから構成されており、従来のソフトウェア開発運用プロセスと、OSS を利用するための OSS コンプライアンスプロセスの手順を同時に遂行させることが可能となっている（図 4.6-3）。共創ソフトウェア開発プラットフォームは、東芝グループ全体での利用を見据えて整備が進められている。

[65] 東芝グループ サイバーセキュリティ報告書 2020 より抜粋
https://www.global.toshiba/content/dam/toshiba/migration/corp/securityPrivacyAssets/security/files/CyberSecurityReport2020.pdf

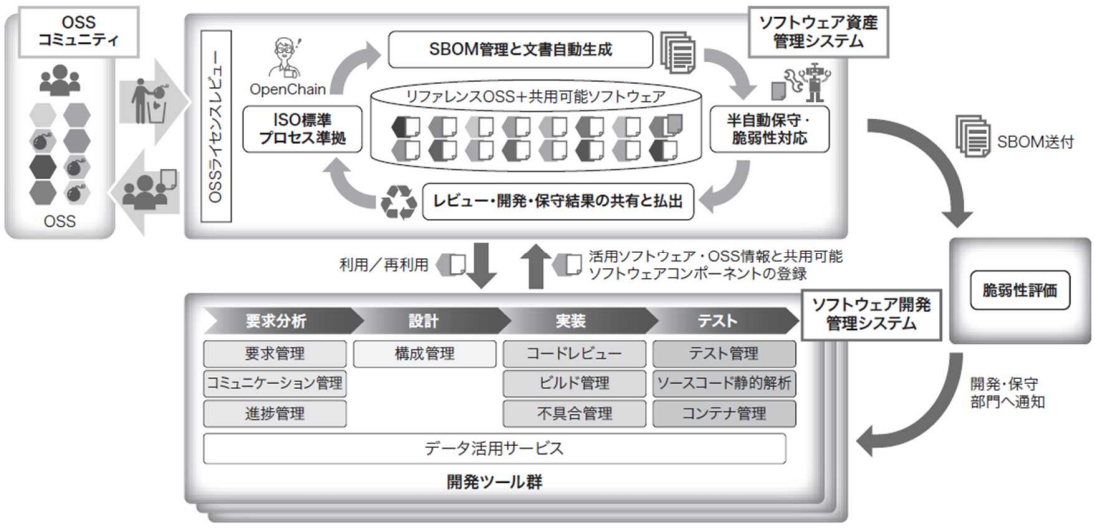


図 4.6-3 共創ソフトウェア開発プラットフォームの構成[66]

共創ソフトウェア開発プラットフォームを構成する 2 つのシステムの機能は以下のとおりである。

① ソフトウェア開発管理システム

ソフトウェア開発管理システムは、OSS を活用したソフトウェア開発ツールチェーンで構成されており、ソースコード静的解析や、トレーサビリティ確保を効率化する要求管理、脆弱性検出等の開発管理機能を持つツールがサービスとして提供されている。

② ソフトウェア資産管理システム

ソフトウェア資産管理システムは、OSS を利用する際のライセンスレビューから、ライセンスコンプライアンスにおいて必要となる SBOM によるソフトウェア管理等、OSS に係る一連のプロセスで使用するツール等が提供されている。

現在、東芝では、特に SBOM によるソフトウェア管理に力を入れており、各グループ会社に対してソフトウェア構成管理の重要性を啓発することをはじめ、セキュリティ対応の際にも活用できる高い精度の SBOM 運用を目指して標準化や運用の改善を図っている。また、各事業部で実施される OSS 等のライ

[66] 東芝レビューVol. 75 No. 5（2020 年 9 月）「開発効率を向上させる共創ソフトウェア開発プラットフォーム」より抜粋
https://www.global.toshiba/content/dam/toshiba/migration/corp/techReviewAssets/tech/review/2020/05/75_05pdf/a07.pdf

センスレビューの際には、知財部門等の関係者も出席し、「コミュニティの活動状況」「採用実績はあるか」といった観点や「評価で使用するか」「製品で使用するか」といった用途の観点を踏まえて OSS の採用可否を丁寧に判断している。なお、この際に必要に応じてソフトウェア技術センターが支援する。

＜【サプライチェーン管理(S6)】開発委託と受入＞

ソフトウェアに限らず外部から調達するものについては、利用許諾を含む知的財産関係、脆弱性や品質などを確認することとしている。そのため、OSS を含む第三者によるソフトウェアを利用、調達する際も、その構成などを含めて確認している。こうした点は、自社が利用する場合でも、顧客等へ提供する場合でも、変わることはない。従って、開発初期や企画段階から、OSS のライセンスや脆弱性については重要事項として扱うこととなる。OSS の選定や利用においては、OSS のライセンス条件や機能、および事業運用に関する要件などの諸事情を考慮することが必要である。さらに、脆弱性の対応や将来的なアップデートへの対応について顧客や取引先との合意を形成することが重要である。

＜【個の能力・教育(P6)】OSS 利活用に関する教育＞

東芝では、OSS に関するマニフェストを定め、OSS コミュニティの知的財産を受け利活用する以上、OSS コミュニティに還元し、オープンソースのエコシステムの発展に寄与すべきであるといったカルチャーや考え方等の浸透を図っている。そうした理念に基づき、すべての職種向けの入門的な教育をはじめ、主にソフトウェア開発者向けのより詳細な内容を含む基礎的な教育など、実務に応じた段階的な教育を用意している。また、各グループ会社は必要に応じて独自の教育を行っている。例えば、入門的な教育では、オープンソースの特徴や企業活動における OSS の重要性とあわせて、知的財産、ライセンスコンプライアンスや脆弱性管理など、活用での留意事項に触れている。また、基礎的な教育以降では、オープンソースコンプライアンスのためのプロセスマネジメント標準である ISO/IEC 5230（OpenChain Specification）を考慮した OSS を活用するためのプロセスマネジメントとあわせて、GPL 等の具体的な事例を示してオープンソースライセンスへの理解を深めるようにしつつ、ライセンスコンプライアンスの実務を踏まえた内容を盛り込んでいる。さらに、東芝では、オープンソースの開発スタイルを組織に導入するインナーソースの推進にも取り組んでおり、OSS を含むソフトウェア開発のトレーニングプログラムとして、ハンズオン形式の実践的な教育も用意している。

＜【コミュニティ活動(C6)】OSS の利活用に向けた社内での連携及びコミュニティを通じた社外とのコラボレーション＞

東芝では、OSS 利活用に係る体制として、グループ内の様々な事業部（法務等のコーポレート部門

も含む）からなる委員会を設置している。OSS ライセンスコンプライアンスの事例等の情報共有や、ポリシーやガイドラインの整備等、幅広く議論を行っている。

また、コミュニティへの参加等、社外とのコラボレーションも行っている。自社で利用している OSS ツールの開発コミュニティに参加し、機能改善等の提案を実施したり、OpenChain[67]に参加し、サプライチェーンにおける OSS コンプライアンスの実現に寄与している。

さらに、東芝が中心メンバーの 1 つとなり、Linux Foundation 配下に Civil Infrastructure Platform（CIP）という OSS プロジェクトを立ち上げている。これは、社会インフラのような長期的に使われ、高い信頼性の求められるシステムにおいて OSS を安全に使っていくために共通の課題を解決していこうとするプロジェクトである。一例として、社会インフラシステムや工場などで使われている産業機器では、OS として Linux を利用するケースが増加しているものの、Linux のサポート期間が数年程度である事が課題となっている。CIP では、10 年以上の長期間運用を想定して OSS を使用できる仕組み等を議論している。東芝は、社会インフラ領域における事業を強化する中で、CIP の活動を通じて、OSS 利活用メリットの最大化を目指している。

[67] OpenChain の活動概要については、トヨタ自動車の事例に記載

4.7. デンソー　～サプライチェーン全体における最適な OSS 管理～

■ 企業情報・本事例集における位置づけ

本社	愛知県刈谷市
業種	輸送用機器
従業員数（連結）	170,932 人（2020 年 3 月末現在）
商流	製品商流/サプライヤ
観点	「ライセンス」「サプライチェーン管理」「脆弱性対応」

■ 本事例のエッセンス

- サプライチェーン全体のライセンス管理のため、自社内のルール整備、Tier2[68]サプライヤとの取決めとその調整・合意、サプライヤと共有するためソフトウェアリストのフォーマットの統一を行っている。
- OSS の脆弱性対応について、商用ツールや外部リソースの活用をしつつ脆弱性調査システムを運用している。

■ 背景・課題

自動車業界は、最終製品メーカーのみならず、重層的にサプライヤが存在し、多数の企業がサプライチェーンを形成している。主に Tier1 のサプライヤであるデンソーにおいては、自社における製品開発で OSS を使用することもあれば、Tier2 以降のサプライヤから供給される製品に OSS が使用されている場合もあり、それらの使用状況を統合的に管理する必要がある。

■ 取組

＜【ライセンス(L7)】【サプライチェーン管理(S7)】サプライチェーン全体を含む OSS ライセンスに係る取組＞

デンソーでは、カーナビゲーション等のマルチメディア製品において、先行して OSS の利活用が始まり、徐々にその利活用製品の範囲を拡大させてきた。その中で、OSS ライセンスについて適切な対応を行うために、全社的なルールの整備や管理体制の構築を進めてきた。

[68] Tier1 のサプライヤに部品等を納入するサプライヤ

現在、OSS ライセンスに関する取組については、技術管理部門が全社事務局として統括しており、設計開発に関わるルールの 1 つとして、OSS ライセンスに関するルールを整備している。また、各事業部門の技術部には OSS 管理事務局、及び製品ごとに OSS 管理リーダー/担当者が設定されており、技術管理部門で定めたルール等を一体となって技術部内に展開している。

具体的な OSS 管理ルールとして、開発チームにて OSS を使用する際、技術部の OSS 管理事務局及び OSS 管理リーダーに申請を行い、必ず承認を得なくてはならない。申請書を作成する際は、技術管理部門が用意する商用ツールを用いて、開発チームにて OSS の使用状況を把握する。OSS 管理事務局及び OSS 管理リーダーは、全社の OSS ライセンスに関するルールにて定めている各開発段階で確認すべき事項や OSS ライセンスごとの使用可否に基づき、申請書に記載された OSS のライセンスに問題がないかをチェックする。また、承認された申請書はデータベースに格納され、OSS 管理事務局／管理リーダー及び技術管理部門から参照出来るようになっている（図 4.7-1）。

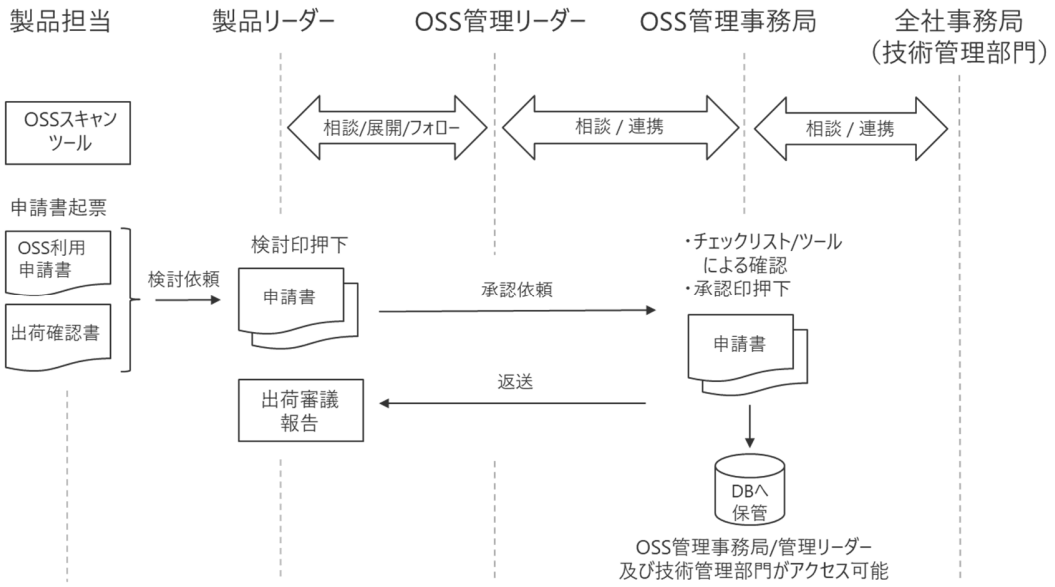


図 4.7-1　OSS 利用申請承認フロー[69]

また、デンソーでは、自社の製品開発における OSS 使用だけではなく、サプライヤ（Tier2）から供給された部品等の中に OSS が使用されているケースも多々あり、それらに対しても OSS ライセンスのチェックが必要となる。ソースコードを入手できる場合には、前述の商用ツール等を用いてチェックできるものの、バイナリデータのみが納品されるケースが多い。したがって、契約等の取決めによって使用 OSS の情報提供

[69] デンソー提供資料を基に作成

を受けられるようOSSの情報提供を盛り込んだ契約書の雛形を基に各サプライヤと調整を進めている。なお、サプライチェーンの下流（Tier2 以降）から上流（最終製品メーカー）において、ソフトウェア情報の共有を容易にする観点から、使用ソフトウェアリストのフォーマットを統一しており、フォーマットとしてはOpenChain[70]でトヨタ自動車等が利用を推進していることを理由に SPDX Lite を利用している。サプライヤ（Tier2）との使用OSSの情報提供に係る調整は、時に難航することもあるものの、コンプライアンスの重要性の理解を得る等の工夫を図るとともに、各サプライヤが対応可能な範囲の妥協点を探り、取決め等の合意を丁寧に進めることで対応している。

＜【脆弱性対応(V7)】脆弱性調査システムを用いた脆弱性対応＞

OSS の脆弱性対応については、情報セキュリティ推進部門が運用する脆弱性調査システムを用いた取組を進めている。

具体的には、各事業部門の製品設計者に、その製品の使用 OSS のソフトウェア部品構成情報（SBOM）を作成し脆弱性調査システムへ登録してもらうことで、SBOM の情報をデータベース化し管理している。ソフトウェアの脆弱性情報は、NVD や JVN 等の情報を自動収集するほか、情報セキュリティ推進部門が Auto-ISAC や JPCERT/CC 等から収集し、脆弱性調査システムに連携している。脆弱性調査システムでは、これらの脆弱性情報と登録された SBOM の情報を照合し、一致度合の高い情報を製品の設計者に自動通知する。製品設計者は、情報の該否判断を行い、必要な対応を実施する。仮に、一定期間経っても対応が取られていないようであれば、脆弱性調査システムから自動で再度催促の通知を送る等の機能も備わっている（図 4.7-2）。

[70] OpenChain の活動概要については、トヨタ自動車の事例に記載

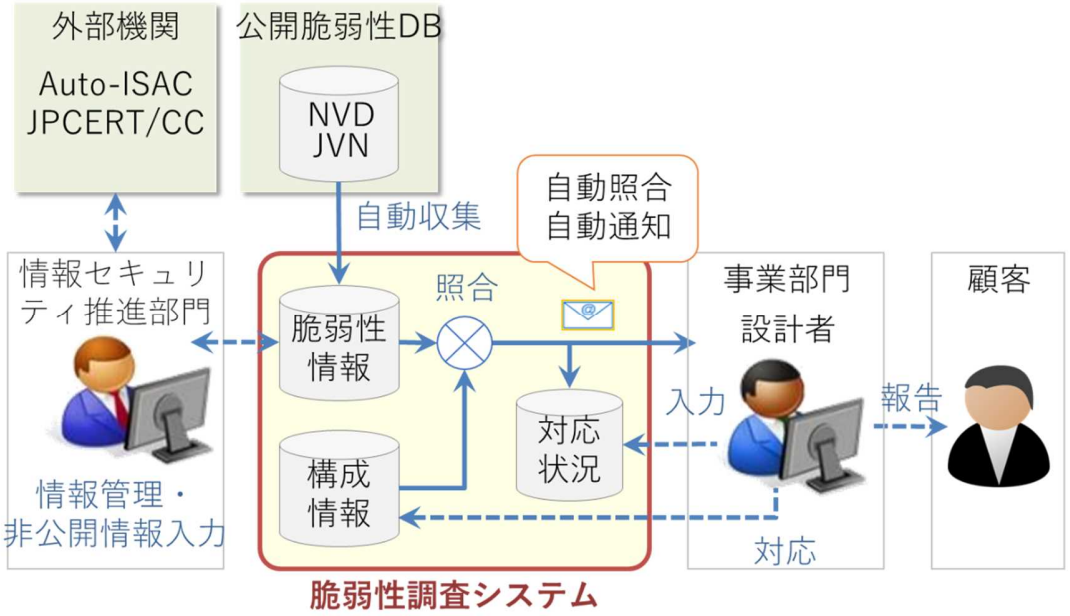


図 4.7-2 脆弱性調査システムの概要[71]

脆弱性対応では、一部商用ツールや外部リソースの活用もしており、情報セキュリティ推進部門では、各設計者が SBOM を作成する際、商用ツールを使用可能な環境を提供している。製品によっては多くの OSS を利用することもあり、そのような場合に、この商用ツールを用いて SBOM を作成することができるため、負荷を低減することが可能となる。

なお、OSS の名称づけは統一されていないため、収集したソフトウェア脆弱性情報が自社 SBOM の情報と名称等において完全一致しない場合がある。機械照合では、アラートが出されるためには完全一致が必要となるため、このことが原因となり、うまく自動通知されない等の抜け漏れが発生する可能性がある。これを防ぐために、同一の OSS だが名称が異なるために別のソフトウェアだと判定されているものがないか、外部リソースを用いて手動で情報照合する形を採っている。

さらに、啓発・教育等の面においても工夫をしている。デンソーの製品群が高度の安全性を要求される自動車部品である特性上、各設計者は品質に対する高い意識を持っている。ソフトウェア脆弱性についても、品質問題として啓発することで、一連の取組に対する設計者のモチベーションを高めるようにしている。あわせて、OSS に係る対応は、通常の品質問題とは異なる知識が必要となるため、設計者に対して関連する教育プログラムも実施している。

[71] デンソー提供資料を基に作成

デンソーでは、Tier2 以降のサプライヤが中小企業も多いために、いかに OSS 管理の負担を抑えながら運用ができるかを業界全体で検討する必要があると考えている。

ライセンス管理の面では、利用している商用の OSS 検出ツールによって検出される OSS の件数が多く、いかに効率的に管理をするかが課題である。

また、現在、脆弱性対応とライセンス管理は、必要な粒度が異なることや社内の取組の歴史的経緯から、別個に情報が管理されているものの、これらの共通化に向けて検討を始めている。その第一段階として、工数をかけずに SBOM を作成できるよう項目を統一する方向で議論している。

4.8. 富士通　～部門横断の OSS 対応体制と全社統一的なソフトウェア管理～

■ 企業情報・本事例集における位置づけ

本社	東京都港区
業種	製造（電気機器）
従業員数	132,138 名（2019 年 3 月末現在）
商流	SIer 商流/SIer & 製品商流/最終製品メーカー
観点	「ライセンス」「サプライチェーン管理」「個の能力・教育」「組織体制」「コミュニティ活動」「選定評価」「脆弱性対応」「保守・品質保証」

■ 本事例のエッセンス

- OSS 対応体制を、OSS 対応組織のみならず、開発部門、管理部門等と密接に連携し、部門横断的に構築した。
- コミュニティ活動参加のルールを明確化するとともに、参加者がコミュニティに貢献できるような教育等を行っている。
- ソフトウェアライフサイクルの中で、全社統一的なツール、サービスを用いて、使用 OSS の見える化及びリスク検知を徹底している。
- ソフトウェア製品のセキュリティ確保に向けた取組において、OSSの使用状況管理と連携した対応を行っている。

■ 背景・課題

富士通は、国内大手の SIer、情報通信機器メーカーとして、常時 1000 以上の開発プロジェクトが進行しており、各プロジェクトでは OSS が多数使用されている。膨大な使用 OSS の管理を行うために、各フェーズにおいて、適切な対応を実施するのみならず、全社的な体制を整備し、社員のリテラシー向上を図るなど、総合的、多面的に対応をしなくてはならない。

■ 取組

＜【サプライチェーン管理(S8)】【個の能力・教育(P8)】【組織体制(O8-1)】【コミュニティ活動(C8)】OSS 対

応に係る組織体制や教育体系の整備とコミュニティ活動＞

富士通では、OSS の専門組織として OSS 技術センター[72]を設置しており、OSS の普及促進、技術支援、ガバナンス、リスクマネジメント、セキュリティといった多岐にわたる側面で取組を実施している。

一方で、全社的な OSS 対応体制としては、OSS 技術センターだけにとどまらず、開発部門、管理部門、社内コミュニティ[73]とも連携するフォーメーションを組んでいる。具体的には、各部門、組織の専門知識を持った担当者が OSS の取組ごとに組織横断の対応プロジェクトを作り、課題解決に向けて定期的に活動を行っている。プロジェクトが一定の目的を達成した際には、既存の組織にその役割を引き継ぐ場合もある。

例えば、OSS のライセンスやセキュリティのリスクにおいては、管理部門の知財担当者、管理部門及び開発部門のセキュリティ担当者等がワーキンググループを作り、組織横断の体制で対応に当たっている（図 4.8-1）。その他、特定の OSS への対応強化を目的に、開発部門、SE 部門、OSS 技術センター等で実施している組織横断の活動等がある。

このような体制をとっているのは、OSS に係る問題解決が単一の知識領域のみで対応することが不可能なためである。中核となる組織、担当者を置きながらも、他部門の必要な組織、担当者と連携する部門横断の体制を築くことで、OSS リスクに対して高い対応力を発揮することを可能とした。

[72] OSS ミドルウェアによるシステム構築から運用までを支援するため、2005 年 11 月に設置された。富士通グループや OSS ベンダをはじめ、コミュニティ、政府・OSS 団体と協力して OSS を活用したシステムのニーズに応える幅広い OSS ソリューションを提供するエンジニアが主体の組織である

[73] OSS の利活用促進、人材育成、支援体制拡充等の目的に基づき、社員主導で組織される複数の活動主体である

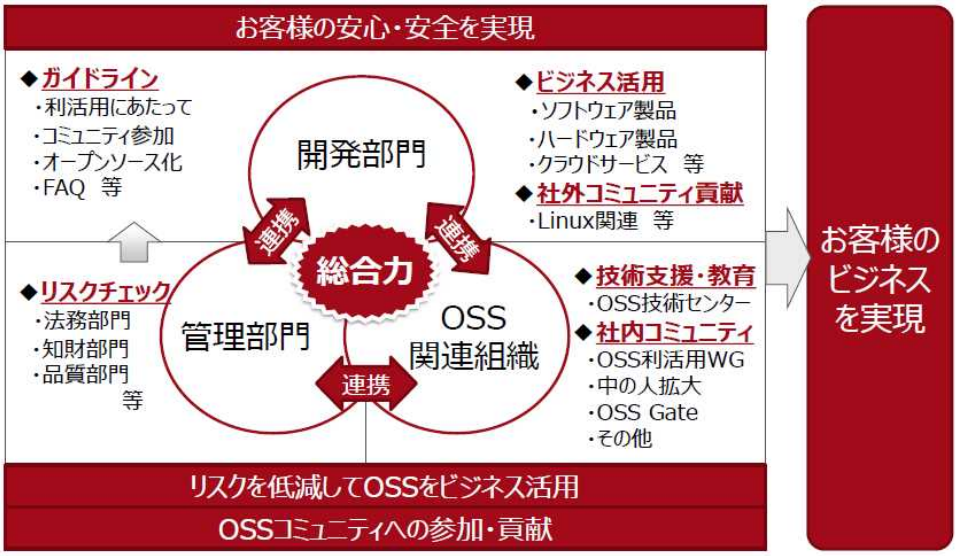


図 4.8-1 全社的な OSS 利活用を支援する体制・仕組みづくり[74]

組織面での対応に加え、教育にも注力がされている。富士通では、OSS を利用するにあたり必要となる知識を学習する教育コースを、e ラーニングを通じて提供している。各分野を詳細に学べる技術者向けの講座をきめ細かく用意することに加え、OSS の知識は全社の DX 戦略と関係するため、OSS を含むシステムの利用者向けの講座も用意している。これらの e ラーニングに加え、OSS 開発者向けに、自身が OSS 開発者になったり、GitHub[75]に参加する等の場面で必要となる知識についての教育も併せて実施している。

また、富士通は、外部のコミュニティ活動を OSS のビジネス利活用に貢献する有効な手段であると明確に位置づけている。しかしながら、社外活動であるために、社員のコミュニティ活動に対して適切なガバナンスを実施することが求められる。一例として、ある事業部門にとって有益であるコミュニティ活動が、別部門にとっては不利益となる可能性があるために、参加コミュニティを企業として管理する必要がある。したがって、富士通では、OSS コミュニティ参加ガイドラインを整備し、適正なコミュニティ活動が実施されるようコントロールしている（表 4.8-1）。

74 富士通提供資料より抜粋

75 ソースコードをホスティングするソフトウェア開発のプラットフォームサービス

表 4.8-1 OSS コミュニティ参加ガイドラインの概要[76]

目的	OSSコミュニティへプログラム等を投稿する際の社内手続き、ソフトウェア開発者が遵守すべき事項、及び社内関連部門の役割を明確にする
対象	富士通Gにて、既存のOSSに反映するためにOSSコミュニティへプログラムやドキュメント等の投稿を行う部門、及び開発者等の関係者
構成	<第1章 OSSコミュニティへの参加申請> ● コミュニティの評価 対象OSSのライセンスに不都合はないか、コミュニティ活動は活発か ● 申請手続き 社内Webから、法務部門の契約チェック、技術部門の承認を受ける ● 申請部門の運用決定 申請部門において、投稿先、投稿者、投稿手順等を決定 <第2章 プログラム投稿時の自己チェック> ● 著作権 他社の著作物やOSSを含んでいないか ● 秘密情報 自社、他社の秘密情報を含んでいないか ● 機能追加を行う場合 特許侵害はないか、特許出願は可能か ● 投稿 部門にて設定した手順で投稿。投稿管理は投稿部門の幹部社員の責任

また、コミュニティ参加者に対して、社外活動における情報漏洩等のリスクに関する研修に加えて、コミュニティに参加する動機付けやコミュニティ内でプレゼンス発揮可能となる研修等、コミュニティに貢献するための教育も行われている。これらの一連の取組により、コミュニティ活動の活性化とそれによる自社 OSS 利活用の発展が持続することを目指している。

参加しているコミュニティの具体例として、OpenChain[77]があげられる。富士通は、OSS が商用代替ソフトから、業種を問わず市場で広く期待され、デファクトや標準を生み出すものへと役割を拡大する中、その潮流を掴み、将来動向の早期把握を実現すること等を目的に、2019 年 3 月にプラチナメンバーとして

[76] Japan Technical Jamboree 60（2017 年）資料を基に作成
https://elinux.org/images/e/e7/%E3%80%90CEWG%E3%80%91OSS%E3%82%B3%E3%83%9F%E3%83%A5%E3%83%8B%E3%83%86%E3%82%A3%E5%8F%82%E5%8A%A0%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6.pdf

[77] OpenChain の活動概要については、トヨタ自動車の事例に記載

OpenChain に加入した。具体的には、Japan WG[78]、及び配下の Sub-WG（Tooling SWG[79]、FAQ SWG[80]、 Planning SWG[81]）において議論を主導しているほか、2019 年 11 月には、OSS を管理するためのコンプライアンスの要件である OpenChain2.0 の「仕様」への適合を自己認証している[82]。富士通では OSS を積極的に製品に組み込む部門等から認証取得を開始しており、特にサプライチェーン管理に関係する部署に認証取得の輪を広げ、グループ会社でも認証が取得されることを目指し、取組を進めている。

＜【選定評価(S8)】【ライセンス(L8)】【脆弱性対応(V8-1)】ソフトウェアのライフサイクル管理＞

富士通では、ガイドラインや規約の整備を行い、各フェーズにおける OSS の適正使用がなされているかチェックするように定めている。以下は、プロジェクトにおいて OSS を適用する際のガイドライン（OSS 利活用ガイド）の構成である（図 4.8-2）。特に、第 2 章「各開発フェーズと目的」では、企画段階における適切な OSS 選定、開発の各フェーズにおけるライセンスのコンプライアンス徹底、出荷前の必要アクション実施に係るエビデンス保存及びサポート体制構築等の実施を義務付けている。

78 OpenChain Japan WG の具体的な取組については、トヨタ自動車の事例に記載

79 OSS コンプライアンス用のツールの検討や検証が行われる SWG

80 OSS ライセンス関連の FAQ が共有される SWG

81 Japan WG の進め方についての議論が行われる SWG

82 OpenChain2.0 とほぼ同内容の OpenChain2.1 が ISO 化（ISO/IEC 5230:2020）されており、OpenChain2.0 に準拠した認証を取得している企業は、自動的に ISO/IEC 5230:2020 の要求事項に適合する。
https://www.openchainproject.org/featured/2020/12/15/openchain-2-1-is-iso5230

図 4.8-2 OSS 利活用ガイドの構成及び第 2 章の詳細[83]

また、各プロジェクトにおける OSS の使用状況（使用 OSS、バージョン、ライセンス）等を全社的に管理している。具体的には、開発の各フェーズにおいて、管理部門や OSS 技術センター、さらには CSIRT[84] チームが連携し、以下のサービスをプロジェクトに提供している（図 4.8-3）。

① 検討・設計段階では、OSS のライセンス等に関する自己チェックツールを提供。

② 開発・導入段階では、OSS の混入を診断するサービスを提供。

③ 保守・運用段階では、機能面の重大バグを含む脆弱性や EOL[85]を管理し、関連部署にアラートを通知するサービスを提供。

[83] 富士通提供資料より抜粋

[84] Computer Security Incident Response Team:コンピュータセキュリティインシデントに対応するための専門チーム

[85] End of Life

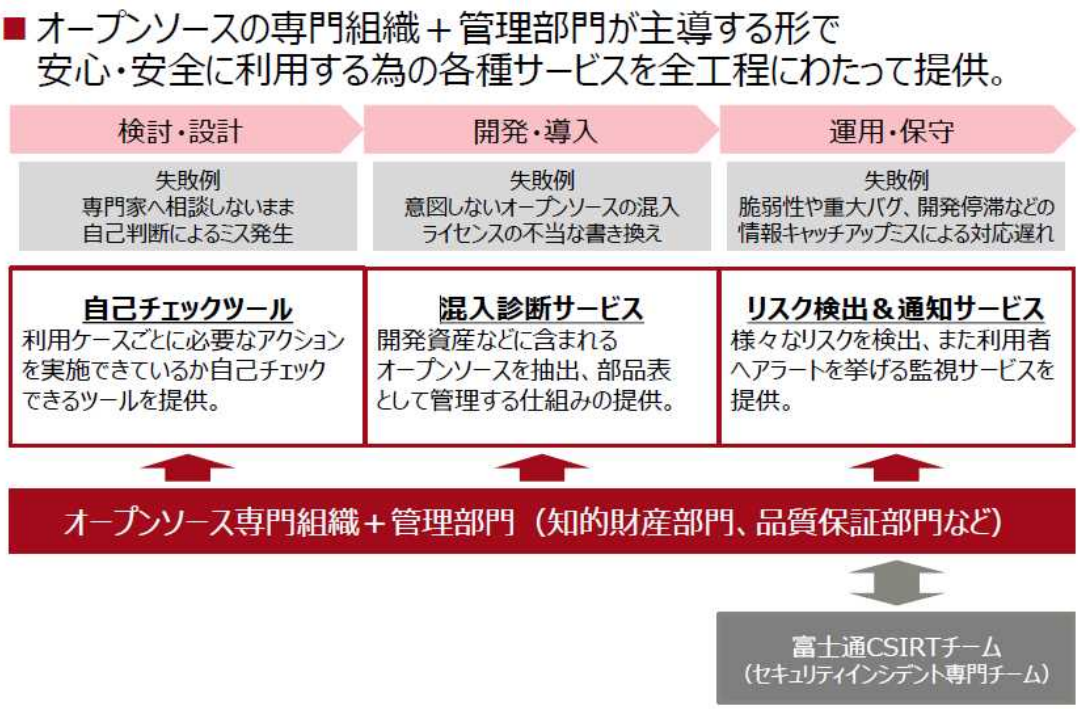


図 4.8-3 OSS 管理の一例[86]

あわせて、①におけるサービスとして、適切な OSS の選定をサポートすることを目的に、自社で使用するであろう OSS の開発傾向、ライセンス、過去に発生した脆弱性（傾向やクローズまでの期間等の情報）等をデータベース化して、社内向けに公開している。これらの各種のツール、サービスも規約等で使用が定められており、全社全てのプロジェクトへの適用が徹底されている。

以上のとおり、全社的にツール、サービスを提供し、企業として統一された運用を行うことにより、セキュリティ脆弱性リスクやライセンスリスクの低いソフトウェアライフサイクルを実現している。

＜【脆弱性対応(V8-2)】【保守・品質保証(M8)】【組織体制(O8-2)】セキュリティ確保に向けた各種取組における OSS への対応＞

富士通では、構築したシステムを顧客へ納入する前に、社内の独立したセキュリティ監査部門によるセキュリティ監査を実施している。システムに OSS を使用している場合には、前述の OSS 管理において用いられるツールと連携し、OSS のバージョン、当該バージョンに内在する脆弱性の有無、対応漏れの有無等を確認している。

86 富士通提供資料より抜粋

また、富士通は、OSS ベースのクラウドサービスを数多く提供しているため、クラウドサービス専門のセキュリティインシデント対応を目的とした、富士通クラウド CERT[87]を組織している。OSS に起因するセキュリティインシデントが発生した場合、富士通クラウド CERT が OSS 技術センター等の社内関連部署と連携して、応急対応を行うこととなっている。

さらに、ソフトウェア製品に含まれる未検知の脆弱性を、AI により評価・検出する技術を用いた検証サービスを提供している[88]。富士通の一部製品・サービスでは、この検証サービスを用いてセキュリティ品質を高める取組を開始している。

[87] Compute Emergency Response Team：セキュリティ、インターネット上の不正アクセス、ソフトウェアの脆弱性などの情報収集や情報提供を行う組織

[88] 「脆弱性検証サービス」を提供開始
https://www.fujitsu.com/jp/group/fct/resources/news/press-releases/2016/1101.html

4.9. 日本電気（NEC） ～事業部ごとの取組から全社的取組へ～

■ 企業情報・本事例集における位置づけ

本社	東京都港区
業種	製造（電気機器）
従業員数（連結）	112,638 人（2020 年 4 月末現在）
商流	SIer 商流/SIer & 製品商流/最終製品メーカー
観点	「選定評価」「ライセンス」「脆弱性対応」「個の能力・教育」「保守・品質保証」「組織体制」

■ 本事例のエッセンス

- 統一的なガイドライン、OSS 情報共有システム等を構築することにより、事業部ごとの OSS への取組を全社的な取組へと昇華させた。
- 全社の OSS 使用状況を一元管理し、企画から運用・保守の工程で必要な対策についてワンストップなサポートを実現するため、ツールやワークフローシステムを活用した「OSS 利活用プロセス」を構築した。
- OSS 利活用プロセスを全社ルール化して、トップダウンで適用を指示することで、適用プロジェクトを増やし、高い効果をあげた。
- PSIRT を設立し、脆弱性情報の収集、対応方針の整理、対応の社内調整を行っている。また、脆弱性管理を効率的に実施するためのシステムを開発し運用している。

■ 背景・課題

NEC では、国内大手の SIer として、常時多数の開発プロジェクトが進行している。一方で、ソフトウェアや情報通信機器等の製品提供、SaaS[89]形式のサービス提供等も展開している。それら多様な価値提供を行う中において、それぞれの事業の状況に合致しつつも全社統一的である OSS の管理/対応が求められる。

自社製品や顧客システムの脆弱性管理を個別に対応するには、体制やコスト面で負荷が高い状況が続いている。また、NEC グループとして適切な脆弱性対応が求められる。

[89] Software as a Service：クラウドで提供されるソフトウェア

■ 取組

＜【選定評価(S9-1)】【ライセンス(L9-1)】【組織体制(O9-1)】事業部ごとの取組から全社的な取組へ＞

NEC では、2000 年代初頭から Linux サーバビジネスにおいて、OSS の利用を開始した。また、ライセンスに配慮する必要[90]がある点から、主に組み込み系製品（携帯電話等）や B2B2C[91]の SI ビジネスにおいても、早くから事業部独自で OSS 管理の取組を実施していた。2010 年以降、OSS 利活用のメリットが認識され、その利用が増える中、事業部ごとであった OSS 利活用及び管理の取組を全社的なものに昇華させる必要性を認識した。そのため、2014 年にタスクフォースを結成し、全社的な OSS 管理の取組を開始した。現在では全社的な OSS 対応組織である先端 SI 技術開発本部 OSS 推進センター（以下、「OSS 推進センター」という。）が事業横断的に OSS 利活用及び管理を推進している。これまでに実施してきた主な取組は以下のとおりである。

① ガイドラインの整備

② 推奨 OSS リスト等の整備、非推奨 OSS のリスク調査

③ OSS 情報共有システムの整備

④ OSS コード検証、OSS ライセンス遵守支援

以下、各取組の詳細について記載する。

① ガイドラインの整備

OSS 使用の際の遵守事項について、ソフトウェア関連プロジェクトの各フェーズにて参照するガイドライン群を段階的に整備した（図 4.9-1）。一例として、OSS 使用判断ガイドラインでは、企画や開発フェーズにおける OSS の導入可否やライセンス検討の基準を定めている。各ガイドラインは個別に定義されたものであるため、全体がより統一的なものとなるよう継続的に見直しが図られている。また、契約書雛形等の共有も実施している。

[90] 製品提供によってソフトウェア（OSS）が再配布されることからライセンスを遵守する必要がある。

[91] Business to Business to Consumer：企業が他の企業へ商品やサービスを提供し、提供を受けた側の企業がさらに一般消費者へ提供する商取引の形態

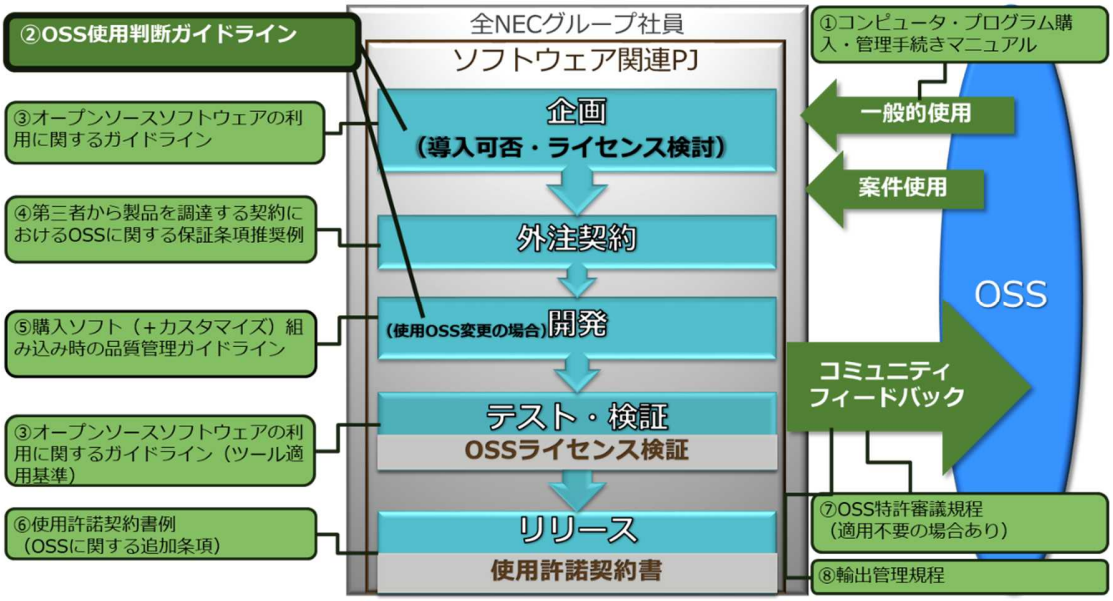


図 4.9-1 ソフトウェア関連プロジェクトの各フェーズにて参照するガイドライン群[92]

② 推奨 OSS リストの整備、非推奨 OSS のリスク調査

使用を推奨する OSS をリスト化し、社内提供することで、後々のリスク（ライセンス違反、脆弱性、EOL 等）を大幅に低減させている。使用を推奨する OSS はサポートの有無、サポート実施主体、社内の利用実績に基づいて判断している。あわせて、「ハイリスク」「非推奨」のリストも整備し、使用を控えるべき OSS も明確化している[93]。重大な脆弱性がある、もしくは EOL の場合は「ハイリスク」、サポートが完全にない場合は「非推奨」に分類している。また、非推奨である OSS についても、要望や質問を受けた場合は OSS 推進センターが調査を行い、リスク回避のアドバイス等を実施している。

③ OSS 情報共有システムの整備

②の推奨 OSS リストの他、各ソフトウェア分野[94]のメジャーな OSS に関する公知情報[95]、及び当該 OSS の自社内使用実績に基づく情報（サポート体制等）を Web ポータル（情報共有システム）上で提供している。それらの情報は OSS 推進センターが定期的にアップデートしている。

---

92 NEC 提供資料より抜粋

93 各リストは、定期的（数か月ごと）に更新をしている。

94 日本 OSS 推進フォーラム作成の OSS 鳥瞰図から、各ソフトウェア分野を参照している。

95 Black Duck Open Hub、JVN iPedia、各 OSS のホームページ等を情報源に、Version、規模、言語、ライセンス、脆弱性、Activity の情報を収集している。

④ OSS コード検証、OSS ライセンス遵守支援

実際の製品・システムに、外部流用等によって混入した認識外の OSS が含まれていないか、商用ツールによって検出するサービスを社内提供している。また、ドキュメント作成、ソースコード開示等、OSS ライセンスに対する適切な対応・遵守を支援する相談窓口を設置している。

＜【選定評価(S9-2)】【ライセンス(L9-2)】【組織体制(O9-2)】網羅的な OSS 管理の実現＞

上述のように、NEC では OSS の利活用及びその管理について全社的な取組を進めてきた。現在では、アジャイルや DevSecOps[96]の開発スピードへの対応における課題意識から、より網羅的に OSS を管理するため「OSS 利活用プロセス」を構築している（図 4.9-2）。これは、全社の OSS の使用状況を OSS 推進センターが把握することで、同センターによるワンストップなサポートを実現するものである。OSS 利活用プロセスの構築に当たっては、ソフトウェア関連プロジェクトの既存プロセスに新たな対応を追加する形が採られており、適用対象は NEC の製品・サービス・SI 全般に渡っている。

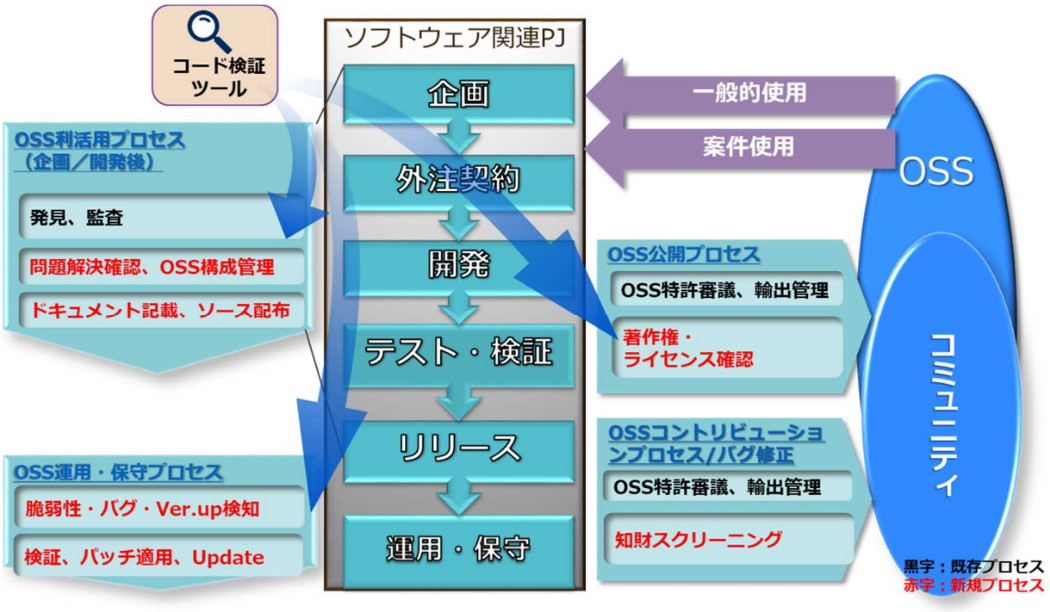


図 4.9-2　OSS 利活用プロセスの全体像[97]

OSS 利活用プロセスはワークフローシステム上で進行する。一例として、開発後の OSS ライセンス遵守

[96] アプリケーションとインフラストラクチャのセキュリティを、開始時点から考慮すること

[97] NEC 提供資料より抜粋

に関する流れは、以下のとおりである。

① 使用 OSS リストのワークフローシステムへの取り込み、及び OSS リスク情報の提供

② OSS リスクへの対処、及び OSS 構成情報の記録

③ OSS ライセンス遵守のフォロー

④ 開示する OSS コード等の管理

以下、各取組の詳細について記載する。

① 使用 OSS リストのワークフローシステムへの取り込み、及び OSS リスク情報の提供

プロジェクトで使用する OSS は、申請（OSS リスク管理票の提出）、もしくはコード検証ツールによる OSS 検知を起点にワークフローシステムに取り込まれる。OSS 推進センターはプロジェクトに対して、使用する OSS に関するリスク等の情報提供を行う。

② OSS リスクへの対処、及び OSS 構成情報の記録

OSS にリスク等がある場合は、プロジェクトにおいて対処方法を決定し、それを OSS 推進センターが確認する。確認の結果が問題ない場合、もしくは元々リスク等がない場合は、OSS 推進センターがソフトウェア構成情報を記録し一元管理する。

③ OSS ライセンス遵守のフォロー

OSS ライセンスを遵守する上で必要となる通知文等の作成を OSS 推進センターが支援する。また、プロジェクトでは開示を要するソースコードを準備する。OSS 推進センターにてそれらを最終確認した後、OSS とともに頒布、または所定の掲載場所に公開する。

④ 開示する OSS コード等の管理

OSS 推進センターにて、頒布または公開したソースコード等の管理をフォローする。

この他にも、コード検証ツールの機能を用いて、脆弱性、バグ、バージョンアップ情報等を各プロジェクトが確認でき、必要に応じ OSS 推進センターがその対応を促す運用フローも OSS 利活用プロセスには含まれている。

また、当初、OSS 利活用プロセスは、各プロジェクトへの「お願い」ベースで草の根的に展開していたものの、その効果を高めるため、OSS 利活用プロセス適用を全社ルールとして定め、経営層が参加する会議においても周知した。全社ルール化とトップダウンの指示により、社内における OSS 利活用プロセス適用に対する意識が高まり、適用件数は増加傾向にある。現在、OSS 利活用プロセスの運用によって得られた知見を次の開発に活かす PDCA サイクルを構築する目的で、利用実績の多い OSS や組み合わせて利用される OSS などの情報を、推奨 OSS リストや次世代 OSS 情報共有システムへフィードバックする仕組

みづくりを検討している（図 4.9-3）。

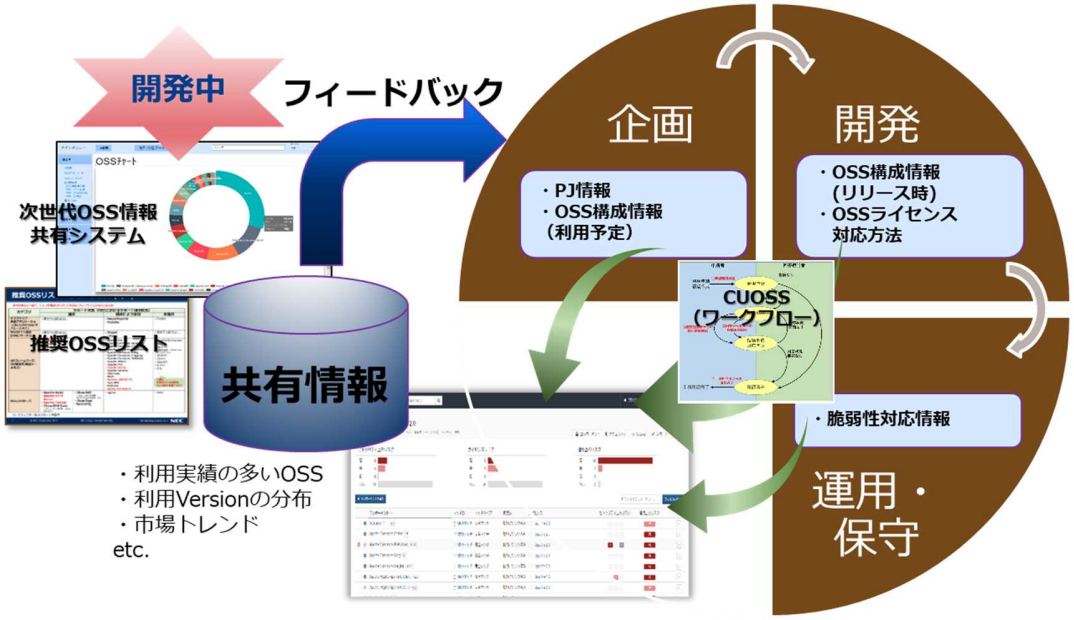


図 4.9-3　OSS 利活用プロセスの PDCA サイクル（検討例）[98]

今後の取組として、新たなツールの PoC[99]等も検討している。また、各ツール独自の OSS 名前マスターを統一することや各種フローの自動化等、効率化の策も検討しつつ、社内の OSS に対する更なる意識向上等、多面的に取組を進めている。

＜【脆弱性対応(V9-1)】【個の能力・教育(P9)】PSIRT の設立＞

NEC グループでは、2004 年に PSIRT を設立した。当時、Code Red/Nimda などの脅威、SQL インジェクションなど経営を脅かすサイバー攻撃が増加していた。また、自社製品や顧客システムの脆弱性管理を担当者が個別に対応することに、体制やコスト面でも限界を感じていた。そこで、専門組織を設立し、仕組み開発（後述する VPS などを参照）に着手することになった。また、PSIRT 設立当初は参考となる情報がなく手探り状態であったが、FIRST の PSIRT Services Framework[100] が公開された後は、PSIRT 構築や

[98] NEC 提供資料より抜粋

[99] Proof of Concept: 新しい概念や理論、原理、アイディアの実証を目的とした、試作開発の前段階における検証やデモンストレーション

[100] 製品やサービスを開発し提供する組織が PSIRT を設置し、継続的に運用し、その能力の向上を支援するためのガイド、FIRST publishes Security Incident Response Teams (SIRTs) Services Framework Version 1.0, 30 Mar 2016、Press Releases 2016、

対応内容等において参考情報として活用した。

PSIRT は、JPCERT/CC、外部ベンダ、個人などとの窓口となり、脆弱性情報（公開済み情報と未公開情報を含む）を取得している。取得した脆弱性情報を基に、影響する製品、対応方針を整理し、関係する開発側の責任者と脆弱性の調査や対処を行う。

また、脆弱性の早期警戒情報やインディケータ情報 の収集および社内関係者への発信、世の中で流行している脆弱性の注意喚起やレポートの作成、社内公開も行っている。

加えて、インシデント発生時に説明責任を果たせるよう、NEC グループ製品の脆弱性を発見した際の報告や対処方法について PSIRT が一元的に相談を受け付けている。NEC グループとして適切な脆弱性対応を行うように取組んでいる。

＜【脆弱性対応(V9-2)】【保守・品質保証(M9)】脆弱性予防管理システム（VPS）＞

PSIRT では、脆弱性予防管理システムである Vulnerability Preventive management System（VPS）を構築している。VPS は、開発するシステムの構成情報を登録し、構成情報とともに脆弱性対策を管理するシステムである。発見・公開された脆弱性情報を収集し、登録されている構成情報の何れかに影響する場合に社内の関係者へ脆弱性情報を配信する仕組みである。配信後、対応が漏れないよう、対処予定情報を VPS に登録しておき、実際の対応状況を月次で事業責任者へ報告する。なお、脆弱性情報の収集については、NEC の関連会社である NEC ソリューションイノベータの脆弱性情報収集サービスを利用しており、日本語訳された脆弱性情報がタイムリー（毎日 1 回以上配信）に連携されている。

図 4.9-4 脆弱性予防管理システム（VPS）のしくみ

2006 年頃からサービス開始・段階的な機能拡張を行い、2011 年からは現在の仕組みで図 4.9-4 のとおり稼働している。具体的には、利用する OSS 等の構成情報入力・管理機能、脆弱性情報の収集・閲覧機能、脆弱性情報のマッチング及び配信機能、パッチなど対応・適用判断の入力機能、事業責任者への定期報告機能を追加した。

＜https://www.first.org/newsroom/releases/2016＞

VPS へ事前に登録するシステムの構成情報は、OS、ミドルウェア、モジュール等の粒度となっている。その理由は、VPS は人が直接管理・運用することを前提としており、最低限管理すべき脆弱性対象の粒度としてOS、ミドルウェア、モジュール等の単位にフォーカスしているためである。なお、製品やプロジェクトによって、製品やプロジェクトの担当者から特定コンポーネントの脆弱性情報配信や構成情報管理希望があった場合は、より詳細な単位であるコンポーネントを管理することにしている。

VPS で登録されている製品と脆弱性情報のマッチングは、製品情報のソフトウェア名とバージョンを基に、脆弱性情報を一覧から検索する。VPS の良い点は、日本国内の拠点で使用する場合、脆弱性情報が日本語であるため、現場レベルでの理解が容易なことである。海外ベンダの構成管理ツールの場合、コンポーネントレベルまでの把握が可能であっても、脆弱性情報が英語表記であるため、現場レベルでの理解は難しい。そのため、NEC としては、VPS と海外ベンダの構成管理ツールを併用している。

現在も機能拡張は継続しており、直近では、VPS への構成情報や対処状況データを取得し VPS へ登録する作業負荷が高い点を解消するため、構成情報を収集するスクリプトを配布し、構成情報を登録代行するサービスを導入した。今後は、出荷前に行う脆弱性スキャンの結果等を VPS に取り込むことで、DevOps[101]の考え方を反映することも検討している。

[101] ソフトウェアの開発担当と運用担当が協力する開発手法

4.10. 日本電信電話（NTT） ～OSS サポートに係る適切な役割分担～

■ 企業情報・本事例集における位置づけ

本社	東京都千代田区
業種	情報通信
従業員数（連結）	303,350 名（2019 年 3 月末時点）
商流	SIer 商流/SIer
観点	「脆弱性対応」「組織体制」

■ 本事例のエッセンス

- 各グループ企業の OSS 対応組織等を適切に役割分担した上で、OSS に係る対応体制を整備した。

■ 背景・課題

NTT は、国内大手の情報通信企業として、多数のグループ企業を有している。NTT、各グループ企業双方で、常時多くの開発プロジェクトが進行しており、各プロジェクトでは OSS が多数使用されている。OSS に係る対応は、企業の枠を超えて、適切な役割分担の下、グループとして一体となった取組を行う必要がある。

■ 取組

＜【脆弱性対応(V10)】【組織体制(O10)】OSS 対応に係る体制の整備＞

NTT では、OSS に係るサポートの専門組織として、NTT OSS センタ（以下、「OSS センタ」という。）を設置している。プロジェクトの設計、開発、運用における OSS 問い合わせ対応、トラブルシューティングサービス、技術検証済の OSS 組み合わせパターンの整理（OSSVERT[102]）、情報提供サービス等を実施している。また、OSS センタは、研究機能も有しており、革新的 ICT サービスの創生及びソリューションの拡大もミッションとし、各種コミュニティにおける開発連携等も積極的に行っている。

OSS センタは、NTT グループ企業に対して、それぞれの企業のニーズに合わせたサービスを提供してい

[102] OSs Suites VERified Technically：複数の OSS 等を組み合わせる場合に、その性能や適切な設定を動作検証し、参照情報として技術資料に取りまとめる活動、及びその情報提供

る。一例として、ソフトウェアライフサイクル管理の取組において、OSS センタは、NTT 本体には各グループ企業へガバナンスを効かせる目的で保守期間が終了したソフトウェアのリストを提供する一方、各グループ企業には OSS のバージョンアップ・移行等の現場支援を行い、連動性がありつつも各企業に即した対応等を行っている。

さらに、OSS センタの問い合わせ窓口であるポータルサイト上では、まだサポート対象になっていない OSS に関しても、旬であれば積極的に技術情報を発信している。要望があれば技術支援を行うとともに、情報提供ページのアクセス状況を分析し、OSS センタからアプローチする取組も行っている。進化の速い OSS 市場に対応した最適なサービスを提供し、各グループ企業のニーズに俊敏に応えることで OSS の利活用を促している。

また、OSS センタは、サポート面においては NTT の研究部門やサポートベンダと連携するとともに、OSS 関連の脆弱性が発生した場合は、NTT の技術部門やグループ内 CSIRT（NTT-CERT）と連携して対応する等、他部門との協力関係も構築している。具体的な一例として、前述のとおり、OSS センタのメンバーが様々なコミュニティで活動しているために、最新の脆弱性情報やセキュリティ関連情報をいち早く入手する機会がある。その場合、OSS センタが NTT-CERT の脅威情報配信のスキームに参画して当該情報を共有している。

OSS センタの活動概要・位置付け及び NTT グループのセキュリティ脅威情報配信スキームへの参画状況は以下のとおりである（図 4.10-1、図 4.10-2）。

図 4.10-1 OSS センタの活動概要・位置付け[103]

[103] NTT 提供資料より抜粋

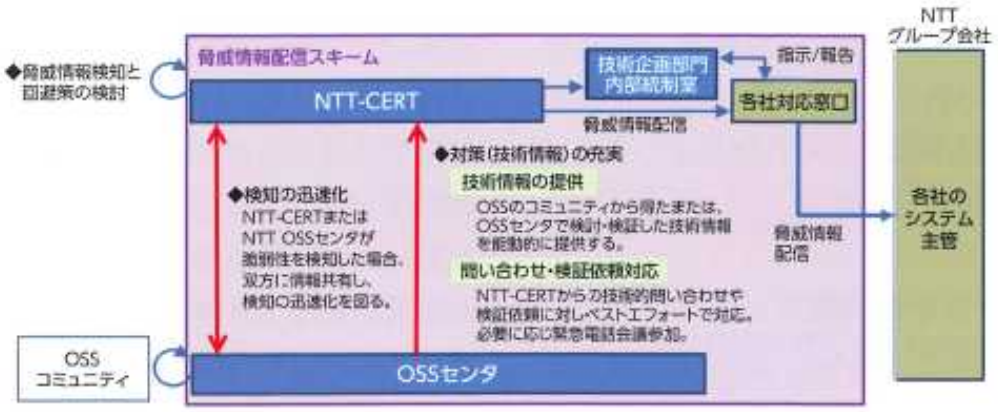


図 4.10-2 OSS センタの NTT グループのセキュリティ脅威情報配信スキームへの参画状況[104]

一方で、各グループ企業においても、それぞれ OSS 対応組織が存在している。OSS センタと各グループ企業の OSS 対応組織は、協力関係にあり、適切な役割分担の下にそれぞれの対応を行っている。例えば、サポート業務において、OSS センタは、各グループ企業の OSS 対応組織がエスカレーション[105]してきた問い合わせ対応等を行っている。

[104] NTT 提供資料より抜粋

[105] 各グループ企業の OSS 対応組織はその問い合わせの内容に応じて、自組織対応をするか、OSS センタへエスカレーションするかを決めている。

4.11. 匿名企業 A 社　～OSS 選定基準の明確化とコミュニティ活動～

■ 企業情報・本事例集における位置づけ

本社	―
業種	情報通信
従業員数	―
商流	SIer 商流/SIer
観点	「選定評価」「保守・品質保証」「コミュニティ活動」

■ 本事例のエッセンス

- 使用を推奨する OSS リストと使用を禁止する OSS リストを整備し、OSS 選定基準を明確化している。
- コミュニティ活動を自社業務の範囲内として捉え、参加を全面的に支援している。

■ 背景・課題

A 社の開発プロジェクトでは OSS が多数使用されている。そのため、OSS に係る対応は全社統一的なルールの下実施される必要がある。

■ 取組

＜【選定評価(S11)】【保守・品質保証(M11)】全社統一的な OSS 選定＞

A 社は、OSS のリスクマネジメントにおいて、OSS 選定フェーズが最も重要であると考えている。具体的には、使用を推奨する OSS リストと使用を禁止する OSS リストを整備し、社内共有している。この内、使用を推奨する OSS の選定基準は概ね以下のとおりである。

① 商流にディストリビュータ等を介しているために、サポート等の対応が担保されている。

② 当該 OSS のコミュニティ活動が活性化している。

③　A 社内の技術者がソースへの対応が可能で、ワークアラウンド[106]を行える。

各リストは、定期的に審議の場が設けられており、その場において対象 OSS の追加や削除等の更新が行われている。各リストは A 社内において、OSS を選定する上での基準となっている[107]。なお、A 社の OSS 対応部署[108]においては、使用を推奨する OSS リストに記載されている OSS のみをサポートする形[109]をとっている。

A 社における OSS に対する長い取組の歴史も相まって、これらのリストは社内で高い信頼性を持っている。これらの取組が一因となり、A 社内においては、OSS 利活用に対する抵抗感は低い。

＜【コミュニティ活動(C11)】コミュニティ活動の支援＞

A 社は、コミュニティ活動に多数参加している。コミュニティの活性化や自社ソフトウェアの OSS 化が A 社のビジネスにおける OSS 利活用に有効であるとの考えから、A 社はコミュニティ活動を自社業務の範囲内として捉え、参加を全面的に支援している。

A 社では、コミュニティ活動に関する内部発表の場や表彰制度を設けることで、その啓発も行っている。また、各コミュニティ活動におけるエキスパート社員が、コミュニティ活動へ若手社員等と一緒に参加することで、OJT による開発スキル等の伝承を行っている。

106 迂回措置、一時対処

107 クライアント要望等の都合により、これらのリストに準拠しない OSS を使用する場合もある。

108 システム開発及び運用の経験や、研究部門におけるソフトウェア研究開発の経験を持つエンジニアが主となる部署である。

109 例外として、ソフトウェアの種類やプロジェクトの状況に応じ、サポート対応する場合もある。その際は、サポートベンダとの連携やコミュニティの情報活用、ソースコードを確認すること等で問題解決を図る。

4.12. 匿名企業 B 社　～グループ内 SIer を中心としたセキュリティ強化～

■ 企業情報・本事例集における位置づけ

本社	ー
業種	情報通信（化学メーカー子会社の SIer）
従業員数	ー
商流	SIer 商流/SIer & エンドユーザー（化学メーカー）
観点	「個の能力・教育」「脆弱性対応」

■ 本事例のエッセンス

- B 社が、グループ各社と深く連携しつつ、一体となったセキュリティ強化策を推進している。
- 使用 OSS を一元的に管理する体制の導入に向け、検討を進めている。

■ 背景・課題

B 社は、化学メーカー子会社の SIer であり、化学プラント等を現場に持つプロセス産業に対して IT ソリューションを提供している。

■ 取組

＜【個の能力・教育(P12)】グループ内 SIer を中心としたセキュリティ強化＞

B 社は、某化学メーカー及びそのグループ内における IT 機能の中核を担う会社であり、グループ各社に対する IT ソリューション提供や、システム管理を担う中で、セキュリティ強化も推進している。一例として、親会社である化学メーカーにおいては、情報システム部門に B 社社員が出向し、エンドポイントからサーバサイドまで、あらゆる領域でセキュリティに関する取組を一体となって行っている。そのようなセキュリティに対する活動の一環として、OSS セキュリティに関する取組も進めている。

後述の OSS の使用状況の管理に係る一連の対応においては、ソフトウェア脆弱性情報の正確性の確認や具体的対策検討及び実施等、人の判断を介する場面が多くある。そのため、グループ内においてセキュリティ強化の中核を担う B 社社員には、OSS のみならずセキュリティに関する高いリテラシーが必要不

可欠となる。B 社は、セキュリティに関する Web 教育体系を 10 年以上前から整備し、人材教育に力を入れており、試験で一定の得点を取るまで社員へ教育を行う等、リテラシーの底上げを図っている。なお、親会社がグローバル展開している拠点の IT 関連業務の担当者に対しても、B 社社員と同等レベルの教育を行うことを目指している。

<【脆弱性対応(V12)】OSS の使用状況の一元管理に向けた検討>

B 社の親会社である化学メーカー及びそのグループ内では、オフィスや化学プラント等において使用されるシステム（生産に関わるクリティカルなシステム含む）において、多くの OSS が使用されている。それらのシステム管理を担う B 社においては、現在、アプリケーションを所管する事業部とシステムインフラを所管する事業部が、それぞれにアプリケーション単位、サービス単位で OSS の使用状況を管理している。脆弱性情報の収集もそれぞれの事業部において手動で行われており、IPA やコミュニティ、Black Duck Open Hub 等が発信するソフトウェア脆弱性情報を定常的に収集している。必要な場合にはセキュリティパッチを適用する等の対応を実施しているが、あまりに対応が頻繁であると、アプリケーションのメンテナンス調整が難しいため、緊急の対応が必要でない限り、年 1 回程度を目安にセキュリティパッチの適用を含むマイナーバージョンアップを行うこととしている。

近年、パッケージマネージャー等の機能が発展し、有用なものとなった結果、OSS に開発者が認識していない OSS コンポーネントが含まれてしまうことがある。そのため、B 社では、OSS の使用状況を全社的に可視化できていないとの問題意識が高まり、約 2 年前から、バージョン、ライセンス、脆弱性を含めた OSS 使用状況の一元管理に向けて検討を開始した。

OSS の使用状況の一元管理を可能とする商用ツールの検討を進めたところ、ツールにより、アプリケーションで使用されている OSS や、当該 OSS ライセンスや脆弱性情報の把握までは自動化できるとの認識が得られた。一方、発見された脆弱性に対し、ツールが複数の対応方法を提示する場合があり、対応方法の選定に際して人の判断が必要となることが明らかになった。

この検討結果を踏まえ、B 社のセキュリティ所管部門が、商用ツールによって、各アプリケーション、サービスの OSS 使用状況についてのデータを一元管理しつつ、脆弱性情報取得時等にはそのデータをもとに各アプリケーションのチームが対応し、その対応の妥当性についてセキュリティ所管部門が精査するという体制を目指している。

4.13. 損害保険ジャパン　～ソフトウェア部品構成表を活用した脆弱性管理～

■ 企業情報・本事例集における位置づけ

本社	東京都新宿区
業種	金融（保険業）
従業員数	24,689 人（2020 年 4 月末現在）
商流	SIer 商流/システムエンドユーザー（金融）
観点	「個の能力・教育」「ライセンス」「脆弱性対応」

■ 本事例のエッセンス

- ソフトウェア部品構成表（SBOM）を活用し、脆弱性やライセンス等について、抜け漏れのないリスク管理を実施している。
- 経営層がサイバーセキュリティの重要性を強く認識しており、脆弱性対応においてトップダウンの啓発を行う等、必要性を理解してもらう工夫を行っている。

■ 背景・課題

損害保険ジャパンでは、多様化する金融サービスへのニーズに対応するため、2015 年より、システム子会社とともに、次期基幹系システムの刷新、及び様々な側面でデジタルトランスフォーメーション（DX）を推進している。これらを進める上では、OSS 等を含む広範な技術を取り扱う必要があり、また、業界の特性上、クリティカルなサービスレベルが要求されるため、そのシステム開発/運用において高度なソフトウェア管理が必要である。

■ 取組

＜【個の能力・教育(P13)】CIO を起点としたサイバーセキュリティに対する取組＞

損害保険ジャパンでは、CIO が起点となり、サイバーセキュリティへの取組を推進している。具体的には、CIO 自ら国内外の先進企業、IT ベンダ等からの情報収集を実施するとともに、社外人材の採用や人材教育等、サイバーセキュリティ体制の整備にも継続的に関与している。

その中で、損害保険ジャパンのOSS対応組織[110]では、システム関連子会社と連携しつつ、スキルのある人材の登用等を通じてソフトウェア管理や脆弱性管理を強化している。特にシステム関連子会社においては、ソフトウェア管理専任組織を構築しており、変化の激しいDXに追従するための体制を組んでいる。

一方で、現場（システム運用担当者）レベルでは、急速に進むDXへの対応等に伴う業務繁忙により、セキュリティに対する優先度が相対的に低下し、システムに脆弱性等による影響が出る可能性があったとしても、そのリスクを正しく認識してもらえない場合がある。このような状況を防ぐために、CIO等からトップダウンで啓発を行う等、危機意識を高める工夫も行っている。

また、2018年には、イスラエルのテルアビブにデジタルラボを立ち上げ、サイバーセキュリティに関するソリューションやノウハウを収集している。

＜【ライセンス(L13)】【脆弱性対応(V13)】ソフトウェア部品構成表（SBOM）の活用＞

損害保険ジャパンでは、近年構築したシステムにおいて、内製、ベンダ等から納品を受ける場合を問わず、多数のOSSモジュールが利用されている。その中で、OSSの脆弱性管理やリスク管理の観点から、ソフトウェア部品構成表（SBOM）を用いたOSS管理を徹底している。具体的にはシステムの「開発前」「開発中」「最終納品及び運用」の3つのフェーズに分けて管理を行っている。

① 開発前のフェーズでは、調達管理に組み込む形で、申請ベースにてOSS使用状況の大枠を把握する。

② 開発中のフェーズでは、工程管理に組み込む形で、スキャンツールを用いたOSS使用状況の詳細把握を行い、SBOMを作成する。

③ 最終納品及び運用のフェーズでは、把握したSBOMをシステムごとにデータベースに蓄積し、脆弱性管理、リスク管理に活用する。

以下、各フェーズの詳細について記載する。

①開発前

各プロジェクトからの申請に基づき、OSSの使用状況（利用箇所・バージョン等）を把握する。また、その申請内容を基に「バージョン」「品質（脆弱性・コミュニティの活動状況）」「輸出管理の要否[111]」「ライセンス（義務の発生有無）」といった観点でリスク分析及び評価を行う（図 4.13-1）。さ

[110] 主に社内の情報セキュリティに対して、リスクを把握、管理することが主なタスクであり、ソフトウェア利用に係る戦略策定等を行っている。

[111] OSSをシステムに利用する際、それらのシステムが今後海外利用されるかを確認し、海外利用される場

らに、その評価とシステムの重要度[112]を踏まえ、必要に応じて対応策を検討する。これは開発前の段階で把握できるライセンス問題等のリスクに対して早期に対処する意図がある。この一連の業務は、調達フローに組み込まれる形で管理されている。

図 4.13-1　開発前の申請時に作成する OSS リスクに係るチェックリストフォーマット[113]

②開発中

開発段階では、実際のソフトウェアに対して、商用ツールを用いて、その OSS 使用状況を把握する。この過程において、①の際に把握しきれなかった OSS 情報の取得をするとともに、静的解析によるリスク検出を行う。損害保険ジャパンでは、これら取得した OSS 情報を SBOM として利用している。ツール上では、SBOM を用いて、ライブラリ単位で OSS のリスク及び脆弱性を可視化できる。アプリケーションごとにそれらのリスク等の解析を行い、問題の早期発見・対応につなげている。これらの一連の業務は、開発工程のフローに組み込まれる形で管理されている（図 4.13-2）。

合は、日本の輸出規制に抵触しないように使用 OSS に暗号モジュール等が含まれないか確認している。

[112] システムが業務で使用されるようなクリティカルなものなのか、もしくは生産性を高めるといったレベルの影響度が小さいものなのかといった観点から重要度が判断されている。

[113] 損害保険ジャパン提供資料を基に作成
リスク分類欄の「✖」印は対策を打つ必要性があることを示している。

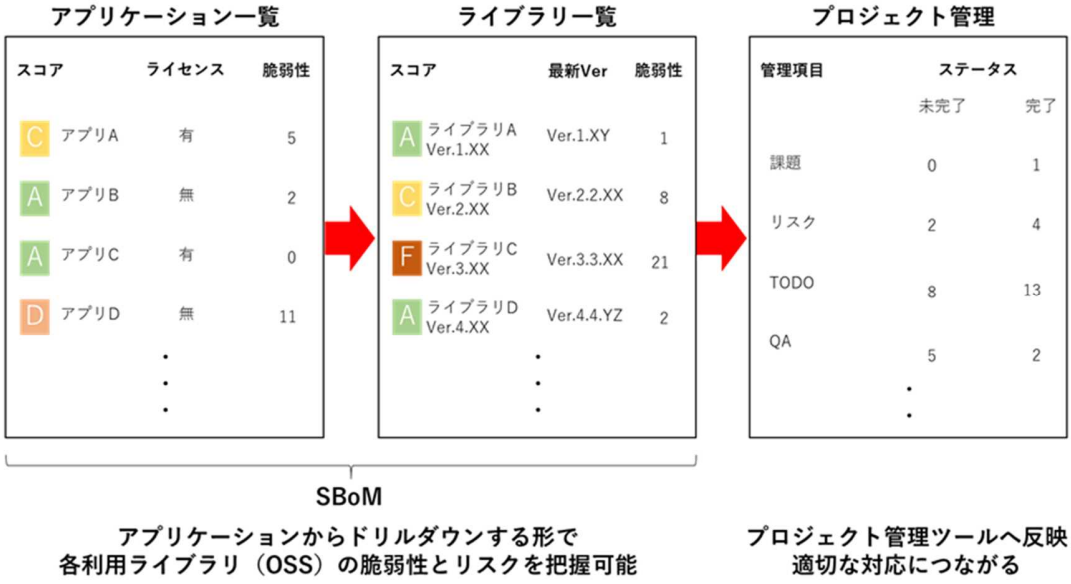


図 4.13-2 開発中、ツールにて作成される SBOM の利活用イメージ[114]

③最終納品及び運用

システムの納品前に、認識外の OSS がないか、システム全体をツールで再スキャンし、最終確認を行う。同時に、システムを稼働させた状態で解析（動的解析）を行うことで、②の静的解析で確認できなかったリスクの検出も行う。最終確認の結果を反映した SBOM は、システムごとにデータベースに蓄積され、日々の脆弱性管理に活用される。具体的には、当該ツールが日々取得する外部からの脆弱性等に関する情報を基に、その脆弱性等の影響を受ける可能性があるシステムの担当者に対して自動でアラートが発出される。

また、必要に応じて、損害保険ジャパンの OSS 対応組織が、アラートが発出されたシステム担当者に対してフォローを行う等、脆弱性対応が適切に完遂されるような仕組みづくりがなされている。

なお、以前は使用 OSS を手作業で管理しており、データベース上に登録される OSS の名称が統一されていないために使用状況の確認が煩雑であった。しかし、②③における商用ツールを用いたデータベース作成の自動化を実施してからは、そういった運用面の問題も解決された。

[114] 損害保険ジャパン提供資料を基に作成

4.14. Visional グループ　～自社状況に対して最適なツールの利用～

■ 企業情報・本事例集における位置づけ

本社	東京都渋谷区
業種	情報・通信業
従業員数（グループ従業員数）	1,385 名人（2021 年 1 月末時点現在）
商流	SIer 商流/システムエンドユーザー（IT サービス）
観点	「脆弱性対応」

■ 本事例のエッセンス

- 開発現場で OSS 利用が比較的自由に行える中で、一度に多数の脆弱性が検知される自社の状況に合ったツールを開発し、事業化した。
- ツールの自社開発にあたっては、社内外におけるテストを繰り返してフィードバックを得ることで、その機能をブラッシュアップした。
- ツールを利用した OSS 管理をルール化し、セキュリティ部門が中心となった脆弱性対応態勢を整えた。

■ 背景・課題

ビズリーチ[115]（現・Visional グループ[116]）では、IT 企業として、開発現場のエンジニアが最適な技術を自由に選択・利用してサービスを生み出せる点を大切な価値観と捉えている。その中で、開発工数の削減等の理由から、OSS は積極的に利用されていた。

一方で、事業が複数軌道に乗っていく中で、各サービスにおける使用 OSS が多岐にわたり、手作業の管理では、多量に発生するソフトウェア脆弱性に対応し切れない状況となっていた。

[115]ビズリーチは、Visonal のグループ会社である。本事例で取り上げる OSS 脆弱性管理ツール「yamory」は、当初、ビズリーチから 2019 年にリリースされている。その後、グループ経営体制への移行に伴い、Visional グループが誕生し、新規事業開発を担うビジョナル・インキュベーションが設立された。現在は、ビジョナル・インキュベーションが yamory の開発・販売を担っている。

[116] ビジョナル・インキュベーション、ビズリーチなどを含む企業グループ

■ 取組

＜自社状況に対して最適なツールの開発と事業化＞

ビズリーチでは、ソフトウェア脆弱性にしっかりと対応を行い、セキュリティを担保しなくてはならないとの課題意識から、最適な OSS 管理手法を模索した。これまでの自由に技術を選択可能な風土を尊重しつつ、最低限遵守すべきセキュリティ基準や管理の仕組みを作る必要があった。

そのような中、OSS 管理に課題を感じていたビズリーチの技術者が、複数の企業に対して OSS 管理に関するヒアリングを実施したところ、他社も同様の課題認識を持っていることが判明し、セキュリティリスクを効率的に管理するための新しいツール開発が必要との認識が芽生えた。

自社内で使用するツールの開発では、社内リソースを確保することが難しいが、他の企業にもニーズがあるのであれば、セキュリティ対策ソフトウェア事業として開発すれば良いのではないかと考え、社内の新規事業立案制度を活用し、OSS 脆弱性管理ツール「yamory（ヤモリ―）」の開発がスタートした。

＜社内外のフィードバックを基にしたツール機能のブラッシュアップ＞

yamory の開発では、プロトタイプ作成と社内テストによるフィードバックを何度も繰り返すことでその性能を高めていった。さらに、製品コンセプトが固まった段階においては、製品化に向けた社外テストも実施した。社内テストの実績を踏まえて提案を行うことで、テストに参画した企業は数十社にのぼり、結果として多くのフィードバック[117]を得ることができた。

これらのフィードバックを基に、脆弱性を多量に検知した際、その緊急度に応じて脆弱性のトリアージ（緊急度に応じた分類）を支援する機能や、それら脆弱性情報を分かりやすく一覧化して表示するダッシュボードにおいて工夫を凝らすことができた（図 4.14-1）。これらの機能により、OSS 管理や脆弱性対応を格段に効率化することが可能となった。

[117] ライセンスのリスクやミドルウェア/OS レイヤの脆弱性の管理機能の実装等の要望を得ている。

図 4.14-1 トリアージ機能によりレベルごとの脆弱性が明示されている yamory のダッシュボード[118]

＜【脆弱性対応(V14)】開発したツールを用いた社内ルールの整備＞

現在、Visional グループでは、yamory を使用した OSS 管理をグループ全体でルール化している。サービスの開発チームは、リリースまでに必ず yamory を用いて OSS のスキャンを実施しなくてはならない。さらに、開発及びソースコードの管理をしている GitHub に連携し、使用している OSS を日々自動でスキャンする。スキャンにより作成された OSS リストは、日々収集される OSS の脆弱性情報と組み合わせることで、リリース後も自社サービスにおける脆弱性有無の検知に利用される。

脆弱性情報は、yamory のダッシュボード上でリスクレベルに応じて分類（トリアージ）され、サービスごと、もしくは全社俯瞰的に表示される（図 4.14-2）。これを各事業部、及びグループ全体のセキュリティ部門が定常的に確認しており、脆弱性が検知された場合、セキュリティ部門が中心となって各サービスの事業部に必要な対応を指示している。また、半年に 1 度、同じくセキュリティ部門が中心となり、各サービスのセキュリティチェック[119]をグループ全体で実施している。その際に、yamory を用いて、OSS に係る脆弱性が全て解決されている旨のレポートを作成し、提出しなくてはならない。

[118] Visional グループ提供資料より抜粋

[119] OSS に関する脆弱性に関するチェックのみならず、製品セキュリティチェックをトータルに行っている。ツールで管理しきれない OS、主要なミドルウェア、ソフトウェアの EOL 等のチェックもこの際に行う。

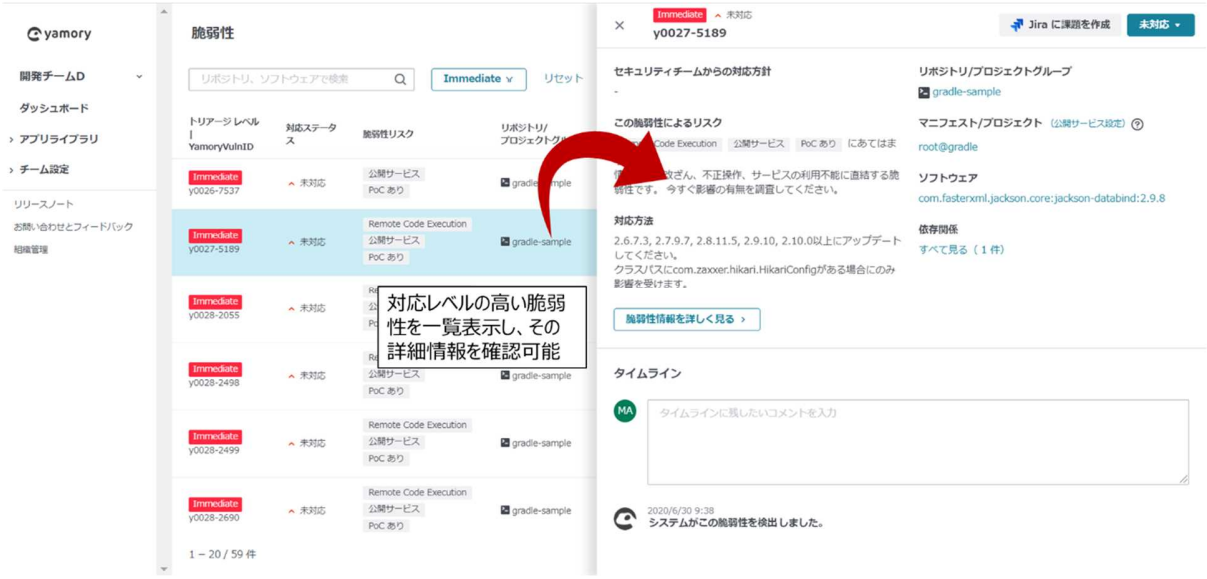


図 4.14-2 対応方針等を含め詳細を確認することが可能な脆弱性の一覧画面[120]

yamory を使用した OSS 管理をグループ全体でルール化するにあたり、開発チームは、トリアージ機能によって OSS に係る脆弱性対応の負荷軽減につながることを、各サービスの開発現場に実績を示してアピールした。実際に、各開発現場で独自に脆弱性管理を行うことが負荷となっていた事実もあり、ツール利用が受け入れられていった。最終的に、セキュリティ部門も巻き込むことで OSS の適切な管理を効率的に行わなければならないという意識が高まり、グループ全体でのルール化に至った。

＜今後の展望＞

今後は、まだ yamory でカバーできていない EOL の管理、ミドルウェアや OS の脆弱性管理についても機能を追加し、より集約的に OSS を管理できるよう研究開発を進める予定である。

なお、yamory の営業現場には、顧客の OSS 管理に対する様々な声（機能追加の要望や運用に関する相談等）が寄せられている。そこから、OSS 管理における各社の対応は、その企業が扱う情報の質や業種等によって様々であり、OSS 管理に対応し切れていない企業も一定数ある状況が分かっている。ビジョナル・インキュベーションでは、引き続き、製品（ツール）、及び自グループ内の運用手法のブラッシュアップを通じて顧客提供価値の向上につなげたいと考えている。

[120] Visional グループ提供資料を基に作成

4.15. サイボウズ　～OSS エコシステムに貢献する OSS ポリシー～

■ 企業情報・本事例集における位置づけ

本社	東京都中央区
業種	情報・通信業
従業員数（連結）	741 人（2019 年 12 月末現在）
商流	SIer 商流/システムエンドユーザー（IT サービス）
観点	「ライセンス」「個の能力・教育」「コミュニティ活動」「選定評価」「脆弱性対応」「組織体制」

■ 本事例のエッセンス

- OSS のエコシステムに貢献するため、部門横断的な組織を立ち上げ、全社的な OSS ポリシーを策定した。
- PSIRT が中心となり、ソフトウェア脆弱性情報のハンドリングや脆弱性報奨金制度の運用等を行い、自社サービスのソフトウェア脆弱性撲滅に向けた取組を徹底している。

■ 背景・課題

サイボウズでは、主力の Web サービスである kintone や cybozu.com のインフラ等において、多量の OSS を使用している。一方、数年前までは、OSS を利用する際には、個別に開発者及び法務がライセンスを確認し上長承認のもと、ライセンスを遵守するといった形で利用しており、OSS の開発を含む全社的な方針はなかった。

■ 取組

＜【ライセンス(L15)】【個の能力・教育(P15)】【コミュニティ活動(C15)】OSS のエコシステムに貢献する OSS ポリシーの策定＞

サイボウズでは、OSS の発展に寄与する存在でありたいとの思いから、社員のオープンソース活動を支援し、貢献を促すような OSS ポリシーの策定を目的として 2017 年に OSS 準備室を設立した。OSS 準備室は、OSS に関係する全社各部門の代表者からなる部門横断型の組織である。

OSS 準備室は、主に OSS ポリシーの策定及びその全社ルール化と OSS ポリシーを補完する細則である OSS ガイドラインの整備を行った。OSS ポリシーは、著作権、特許、商標のライセンス等の取り扱いについて定めている。なお、サイボウズの OSS ポリシーはパブリックドメイン（CC0）で公開されている（表 4.15-1）。

表 4.15-1 サイボウズの OSS ポリシーの章構成[121]

0. 本文書について	-
1. 前文	-
2. 著作権	2.1. 著作権の帰属
	2.2. 著作権の譲渡
3. 従業員個人の著作物のオープンソース化および当社商標の使用	3.1. Disclaimer（免責条項）の記載
	3.2. 当社商標の使用
4. 当社著作物のオープンソース化	4.1. OSS ライセンスでの公開
	4.2. 他者 OSS への提供
5. 他者 OSS の利用	5.1. 他者 OSS のライセンスの確認
	5.2. ライセンス文書等の取扱い
	5.3. 他者 OSS の不具合に関する報告
6. 当社 OSS への他者著作物の取り込み	6.1. 他者著作物の提供があった場合
	6.2. コントリビューターリストの管理
7. ライセンス違反への対応	7.1. 当社 OSS のライセンスに違反する利用への対応
	7.2. 当社内での OSS ライセンス違反への対応

サイボウズでは、自社開発したソフトウェアを OSS 化する機会も多くあるため、OSS ポリシーではその際に遵守すべき事項も定めている。その中には、簡略な承認ステップで OSS 化を可能とする規定もあり、OSS エコシステムへの貢献の姿勢が反映されている。さらに、OSS の利活用促進に向けて開発者のモチベーションを高めるため、社員が自発的に作成したソフトウェアは、サイボウズのライセンスや極秘情報を含まない限り、開発した社員の著作物とする規定もある。以上のように、OSS ポリシーは、OSS の幅広い利活用を想定した内容となっている。

こういった OSS 利活用に対する積極的な姿勢は、OSS 化したソフトウェアのバグに関するフィードバックを外部からも得られるといった実務的なメリットの享受や、採用活動における技術力や自由な社内風土のアピール材料としての活用等、さまざまな効果を生んでいる。

サイボウズは、kintone 等のグループウェアを主力サービスとする会社であり、グループウェアを通じて全社員が容易に意思疎通できる環境が備わっていた。その中で、OSS 準備室の立ち上げや、ポリシーの策定・公開においては、当時の運用本部長が中心となって、トップダウンで必要性を啓発し、取組を強力に

[121] サイボウズの OSS ポリシー
https://cybozu-oss-policy.readthedocs.io/ja/latest/

推進した。

なお、OSS 準備室は、新設された OSS 推進室[122]にその機能を引き継ぎ 2018 年に発展的に解散している。現在は、OSS 推進室が OSS ポリシーと細則を定めた OSS ガイドラインのメンテナンスを行っている。

＜【選定評価(S15)】【脆弱性対応(V15)】【組織体制(O15)】PSIRT が軸となった多様なソフトウェア脆弱性対応＞

サイボウズでは、サービスにおいて OSS を利用する際には、前述の OSS ポリシー、OSS ガイドラインに従って、開発チームが利用したい OSS の調査を行わなくてはならない。調査の結果、ライセンスが社内で定めているガイドラインに合致すること、定期的にアップデートされていることが確認されれば、その OSS を利用することができる。ライセンスがガイドラインに合致しない場合や定期的なアップデートがされていない場合でも、法務による審査や自社でバグ等の対応ができるかというチェックを経ることで、その OSS は利用できる場合もある。

各開発チームは、それらの調査等を経た後に、使用 OSS の情報をデータベースに登録する。その情報は、最終的に開発チーム内のコードレビューを経て、抜け漏れがないことが担保される。サイボウズの PSIRT は、そのデータベースを定期的に参照しており、バージョンアップ等の情報があった場合に開発チームへフィードバックするサイクルができている。

あわせて、PSIRT は、OSS のレポジトリやサイト等の一次情報や JVN、セキュリティニュースサイト等からソフトウェア脆弱性の情報を日々収集している。ソフトウェア脆弱性情報が得られた際には、関連する OSS を使用しているサービスがあるか、PSIRT がデータベースを検索し、確認をしている。該当するサービスがある場合、PSIRT が中心となり情報をハンドリングし、そのサービスの責任者にグループウェア（kintone）上でアラートを出している。

また、社内である OSS を新たに使用する際、その OSS をマスター登録し、そのマスターを起点にデータベース内でサービスとその使用 OSS を一元的に紐づけている。そのため、ソフトウェア脆弱性情報における OSS の名前情報にばらつきがあった場合でも、社内では迅速に対応することができる。

さらに、サイボウズの PSIRT では、脆弱性報奨金制度を運用している（図 4.15-1）。これは、サイボウズの自社製品の脆弱性を発見、報告した外部の方に報奨金を支払う制度であり、サービス自体の脆弱性や、脆弱性のある OSS 使用の指摘等がその対象となっている。指摘に対しては検証用の環境を提供する等、真摯な対応の下に報奨金支払いの判定を行っている。また、報奨金支給額が高額にならないよう、自助努力として自社でセキュリティ専門企業の脆弱性診断を受ける等、外部からの指摘を極

[122] 2021 年 1 月現在 7 名が所属している。

力減らす工夫や、外部からの指摘に対して適切に対応できる社員のスキル・リテラシーを養う等、脆弱性を撲滅するため、この報奨金制度を起点とした PDCA サイクルを回している。

- サービスのセキュリティ品質向上に向けて2014年から実施している取り組み
- 2019年度は、489件の着信、193件の認定数（暫定）、1,535万円の報奨金支払金額(暫定)であった
- バグハンターの方を集め、脆弱性を見つけてもらうイベント等も開催

図 4.15-1 脆弱性報奨金制度のホームページ及びその概要[123]

[123] 脆弱性報奨金制度のホームページ
https://cybozu.co.jp/products/bug-bounty/
2019 年報奨金制度の結果
https://blog.cybozu.io/entry/2020/05/07/110331

4.16. 三菱電機インフォメーションシステムズ（MDIS）　～OSS の特性を踏まえたソリューション展開～

■ 企業情報・本事例集における位置づけ

本社	東京都港区
業種	情報・通信業
従業員数	1,279 人（2021 年 3 月末時点）
商流	製品商流/最終製品メーカー
観点	「選定評価」「保守・品質保証」「コミュニティ活動」「脆弱性対応」「ライセンス」

■ 本事例のエッセンス

- OSS を含んだソリューションを提供するにあたり、OSS を長期間利用する上での脆弱性管理やアップデート対応に係るコストの考え方を顧客と事前に合意している。
- 利用する OSS を適切に把握し、管理するためには、コミュニティとの関わりが重要であり、バグを発見した際はコミュニティに対してバグを報告するだけではなく、改善策も含め連絡することで貢献している。

■ 背景・課題

三菱電機グループでは、開発する製品やソリューションにおいて OSS を活用しており、全社的にも OSS 管理のための組織体制を組み、研究活動も進めている。

MDIS は、OSS を活用した通信事業者、サービスプロバイダー向けのソリューションを提供している。通信業界では、多くの顧客に対して大規模なサービス（携帯電話の SMS/MMS サービス等）を提供するため、有償のソフトウェアを使用すると莫大なライセンス費用を負担することとなってしまう。そのため、通信業界は、有償のソフトウェアではなく、無償の OSS の活用に積極的である。

■ 取組

＜【選定評価(S16)】オープンソース活用ソリューションの提供＞

MDIS では、サービスプロバイダー向けのオープンソース活用ソリューションを提供しており、OSS ベースの

システムライフサイクル全般を支援している。ソリューションの提供先である通信業界では前述のとおり、OSS の活用に積極的であり、提供先からの要求に基づき、MDIS から OSS を活用したシステムやソリューションを提供している。OSS の活用においては、OSS の調査や選定、開発後の運用維持を重要視している。MDIS では、システムやソリューションを 5 年程度使用することを前提に、その間の運用を維持するため、OSS コミュニティに関わりながら、パッチや脆弱性情報を監視し、必要に応じてパッチの適用等を行っている。

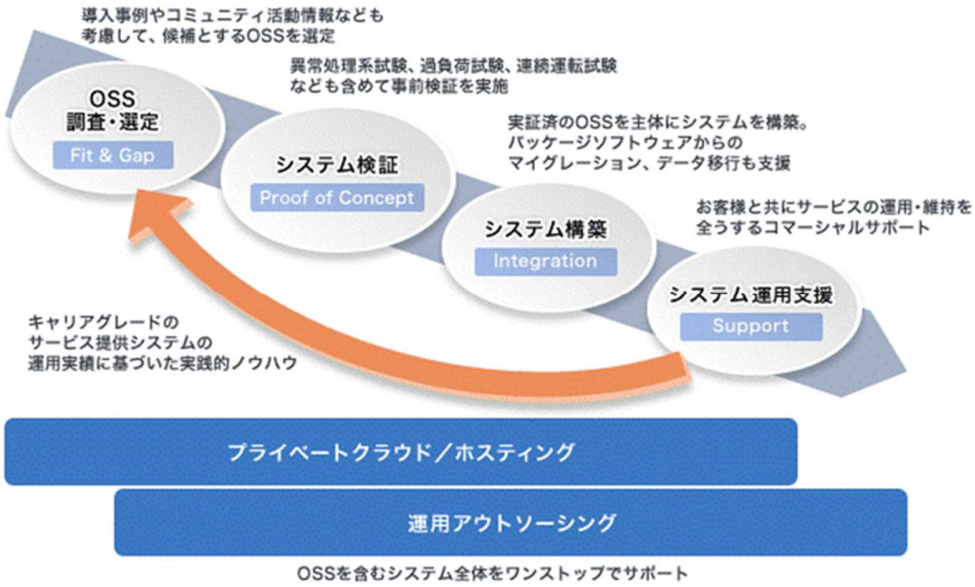


図 4.16-1 オープンソース活用ソリューション（通信事業者、サービスプロバイダー向け）概要イメージ[124]

＜【保守・品質保証(M16)】【コミュニティ活動(C16-1)】オープンソース活用ソリューションの提供＞

OSS を 5 年という長期間使用するにあたっては、OSS コミュニティが開発や脆弱性対応を含むサポートを終了するというリスクがある。そのため、開発の初期段階で推測されるリスクを洗い出し、発生し得る事態と対策する場合の保守コストについて、顧客に事前に説明し合意している。特に、開発・サポートが終了した後も対策コストが発生するリスクがあることを顧客も理解して運用していくことが重要である。

OSS を改修した際、開発コミュニティへどのように還元するかに苦労した経験もある。OSS のコミュニティや Github は個人開発者を前提として仕組みを作っているため、企業が組織的に改修した場合でも、そのまま組織の成果物として扱うことが難しい。そのため、改修に関わる設計～プログラミング～試験に関与した社員や協力会社の間で貢献度を算定し、また契約にも照らし合わせた上で、メンバー同で納得感がある還元方法を決定する必要があった。また、以降のサポート体制・分担も想定し、連絡先の表示方法を決定する必要

[124] 通信事業者、サービスプロバイダー向けオープンソース活用ソリューション紹介ページより抜粋
https://www.mdis.co.jp/service/oss/

があった。

＜【脆弱性対応(V16)】脆弱性情報の管理＞

構成管理ツールに付属している脆弱性情報のプッシュ機能も参考に、OSS の脆弱性を公開している様々なサイトで情報収集している。また、OSSコミュニティから脆弱性を含む情報を発信するメーリングリストがあり、MDIS の開発メンバーのメーリングリストで加入している。他方、コミュニティ活動が無く、OSS コミュニティから脆弱性情報を把握できないような場合は、脆弱性管理ツールを利用して、使用する OSS の脆弱性解析を行うこともある。

＜【ライセンス(L16)】構成管理の方法＞

OSS の利用が多くない、自らがソフトウェアを選定している、及び事業部門内で開発が完結しているという部門では、SBOM を積極的には利用していない。ただし、外部委託した場合は、知らずに OSS が組み込まれている場合もあるため、構成管理ツールでソフトウェアを解析し、OSS が組み込まれているかを確認している。ライセンス違反を防ぐことがコンプライアンス面、ビジネス面でも重要と考え、構成管理ツールを使用したソフトウェア解析を、ライセンス違反の自己防衛策として取り組んでいる。

＜【コミュニティ活動(C16-2)】OSS コミュニティへの関与＞

OSS コミュニティは、SIer の立場で参加し、主に OSS の選定評価や運用維持のために情報を収集する場として活用している。OSS コミュニティへの貢献は、OSS のバグを発見した際、単なる指摘だけではなく改善策も含めて連絡し、コミュニティと連携するようにしている。

MDIS が提供するソリューションは、“継続的なコマーシャルサポート”を特長としており、OSS 自体のサポート、もしくは商用レベルにパッケージして商用ディストリビューションとして展開することが、MDIS の役割と考えている。役割を担うには、OSS に関する情報を十分に獲得することが必要である。そのためにも、バグや脆弱性情報を発見した際は、OSS コミュニティと連携し改善するなど積極的に関わるようにしている。

4.17. OSSTech ～OSS を活用したソフトウェア管理～

■ 企業情報・本事例集における位置づけ

本社	東京都品川区
業種	情報・通信業
従業員数（連結）	19 人（2021 年 8 月時点）
商流	SIer 商流/システムエンドユーザー（IT サービス）
観点	「ライセンス」「脆弱性対応」「サプライチェーン管理」

■ 本事例のエッセンス

- OSS を利用したソリューションでは、提供先であるユーザーとの OSS の取り扱い方法や契約形態で留意する点が存在する。
- 構成管理では、ビルドシステム等の OSS に備わっている機能を活用しながら、ソフトウェアの依存関係を管理している。

■ 背景・課題

OSSTech では、認証系の OSS である OpenAM[125]を利用したソリューションを提供しており、セキュリティに配慮した利用や運用が求められる。また、専門的な OSS 利活用を行いつつ、少人数でも管理できるような手法が求められている。この手法のひとつとして、開発環境の機能を活用した管理に取組んでいる。

■ 取組

＜【ライセンス(L17)】取引企業と契約に関する取り決め＞

一般的な受託開発によるソフトウェアと比較して、OSS を利用する際にはユーザーに提供するコンポーネントのライセンスや、関連して開発した著作物の扱い（サブモジュールや開発した部分のドキュメント等）を含む契約などの点に注意が必要である。

OSSTech ではユーザー向けに開発する機能やモジュールのライセンス形態を、GPL や Apache License

[125] シングルサインオン環境を提供する OSS

など、コアコンポーネントに基づくライセンス形態に合わせているが、自社の優位性として利用条件を限定したいユーザー側の思惑とズレが生じることがあるため、契約の段階で OSS のライセンスを適用する範囲を明確にして合意しておくことが重要である。

＜【脆弱性対応(V17)】脆弱性情報の管理＞

OSSTech で利用及び提供している OpenAM など最近の OSS は、GitHub を利用することで、コミュニティが共同で開発、管理している。また、GitHub のサービスで、リポジトリに登録されている OSS の脆弱性情報が送られてくるため、それらの OSS を利用している開発者は送られてきた情報を確認し、必要に応じて対処している。このようにサービスや仕組みを利用してソフトウェアの安全性を担保できるようになっている。

脆弱性管理において確認・対応すべき箇所は OSS や製品によって異なるため、各製品の開発担当者が OSS のアップストリームからの情報を収集している。開発担当者が情報収集することで効率的で的確に脆弱性を収集し、管理することが可能である。また、アップストリームにおける脆弱性情報を、開発者同士のメーリングリストや BTS（バグトラッキングシステム）[126] で確認することで対処漏れを防止している。

＜【サプライチェーン管理(S17)】OSS を利用したソフトウェアの管理＞

OSSTech では、OSS を利用したソフトウェアの管理について、ソフトウェアのユーザーへ SBOM を提供する場合には、同時に自動で脆弱性の確認を実行するツールも提供し、脆弱性のアップデートが実施できることが重要であると考えている。また、ユーザー自らが実施できない場合は、専門企業のサポート体制を含めたアウトソースが現実的であると考えている。その理由は下記のとおりである。

- 多くのユーザーは、OSS の脆弱性アップデートを含めたすべての対応をサポート費でベンダ側に任せたいと考える。ユーザーは、セキュリティを担保することが目的であり、ソフトウェアのコンポーネントを管理することの意識は高くない。
- 組み込み製品の場合は、SBOM を Excel で管理することは可能と考えるが、依存ライブラリが 100 や 1,000 を超える場合は、管理負荷が高くなり困難となる。
- 製品のアップデートがなければ SBOM は基本的に変わらない。しかし、例えば、製品が OS 標準ライブラリをダイナミックリンクしている場合、依存ライブラリ側に変更があれば、SBOM の更新が必要になることがある。そのため、ユーザーに SBOM を提供しても SBOM を活用し、適切に管理、脆弱性のアップデート等を行えるか不明である。

[126] ソフトウェアの開発や保守を進める際、プログラムなどに含まれるバグを管理、共有するシステム

4.18. ヤフー　～社員が正しくOSSを使うための体制整備～

■ 企業情報・本事例集における位置づけ

本社	東京都千代田区
業種	情報・通信業
従業員数（連結）	単体：7,167 人（2021 年 3 月末現在）
商流	インターネットサービス事業者
観点	「選定評価」「ライセンス」「脆弱性対応」「個の能力・教育」「組織体制」「保守・品質保証」「サプライチェーン管理」「コミュニティ活動」

■ 本事例のエッセンス

- ヤフー全体で OSS の取り扱いに関するガバナンスが取れており、複数の審査を経たうえで OSS の利用が可能となっている。
- 技術規定に紐づくガイドラインの中で、利用してよいOSSの基準を定めている。
- 複数のツールを用いることで、抜け漏れのないOSS管理、ソフトウェア脆弱性対応を行っている。
- 開発において外注することはないが、外注する場合は、発注要件の中に OSS のリストを明示することでOSSの管理、把握を行っている。
- 人事規定の改定や OSS デベロッパー認定制度等、OSS に貢献している社員が使いやすい制度を整備し、社員のコミュニティへの参画を支援している。

■ 背景・課題

ヤフーでは、より良いサービスを素早く提供するために、サービスやそれらを支えるプラットフォームにおいて、非常に多くの OSS を利用している。そのため、OSS 利用に関するガイドラインを定め、OSS 選定から導入、保守運用に至るまで様々な規定を設け、遵守することで高品質なサービスを提供可能としている。また、コミュニティへの積極的参画を通じて自社事業の発展にも大きく影響を与える状況となっている。

■ 取組

＜【選定評価(S18)】開発部門、法務部門の連携によるOSS承認＞

OSS の選定についてヤフーでは、ガイドラインに法務確認を行った利用してよい OSS を定めている。法務確認が済んでいないライセンスは、基本的に利用できない。規定の審査を受け、オープンソースとして問題の無いもの等を確認する審査プロセスを踏まえた上で、さらに技術責任者の承認プロセスを得た上でなければ利用ができない運用になっている。利用が許可されていない OSS については、上記の審査を早期に行い、問題ない場合は、利用を承認するとともに、下位規則に新たに利用可能になった OSS を追加する運用である。

＜【ライセンス(L18)】【脆弱性対応(V18)】【個の能力・教育(P18)】【組織体制(O18)】OSS 利活用のコンプライアンス体制と運用の効率化＞

ヤフーが展開する Web サービスでは、OSS なくしてはそのサービスが成り立たない程に多量の OSS が利用されている。その中で、2009 年頃、変化の激しいインターネット業界において、社内での OSS 利用がそれまでにも増して急増したことから、社員の適切な利活用を強化する目的で仕組みづくりが開始された。また、世の中のコンプライアンスへの意識の高まりにも配慮し、著作権に関する全社員向けコンプライアンス研修の中で、写真や音楽の他、ソフトウェアについても教育や試験を行っている。ヤフーでは OSS に関する基本的な方針として

・オープンソースの利用に関する規定

・OSS に対する貢献

・ヤフーの中からオープンソースを公開

の 3 点を置き、これらを遵守し開発を進めていくことで高品質なサービス提供を行っている。

現在、ヤフーが開発するサービスにおいて、OSS を利用する際には、ガイドラインで定められたプロセスに沿って利用 OSS を申告した上で、一定のチェックを経なければ利用許可が下りない形となっている。具体的には、ライセンスに規定された権利や義務を遵守できるか、また将来に渡って安定的に利用できるか等、OSS 利用者一人一人がコンプライアンス的な観点を含む様々なチェックが出来るよう教育を実施している。

OSS の具体的な選定について、前提となる OSS ライセンスの利用可否は、条文の内容を法務部で確認し、利用してよい OSS ライセンスの場合、確認済みライセンスとしてリスト化して社内公開するようガイドラインに定めている。OSS 利用者は、利用したい OSS のライセンスがリストの中に含まれているかを OSS の利用前に確認する。法務部の確認が済んでいないライセンスは基本的に利用できない。

また、ライセンス以外にも著作権や知的財産権などの様々な面で利用に問題が無い OSS かどうかを確認する選定コストを下げるため、全社的に利用する頻度も高く、そうした選定コストも高い OSS については、専門の部隊が事前に審査し、選定作業をせずとも利用可能な OSS として、ガイドラインの下位規則に新たに追加していく運用である。

それ以外の OSS については、確認済みライセンスか確認し、利用しても問題ないかの選定作業を終えた

上で、OSS 利用を申請し、その内容に問題がないかを技術責任者が確認し、承認するプロセスとなっている。なお、選定時のライセンス、その他のチェックには、様々なツールを組み合わせて利用している。

また、ソフトウェア脆弱性対応の取組として、CSIRT を中心とした対応とツールを利用した対応の 2 つがあげられる。リスクの高い脆弱性の場合は、CSIRT が中心となり規定に基づく必要な対応を各事業部に要請している。一方、それ以外の脆弱性の場合は、ツールによって脆弱性情報が自動で検知され開発者自身にアラートが出る仕組みとなっており、ソフトウェア脆弱性に迅速に対応可能となる。ヤフーでは、抜け漏れを防ぐため、開発から運用までの各フェーズで複数のツールを使用して脆弱性チェックを行っている。

さらに、ヤフーでは、自社または他社とのコラボレーションにより開発したソフトウェアを OSS として公開する機会がある。そういったコミュニティへ貢献をする場合、ライセンス違反や第三者の権利を侵害することがないよう、技術責任者によるチェックを経なくてはならない仕組みも構築している（図 4.18-1）。

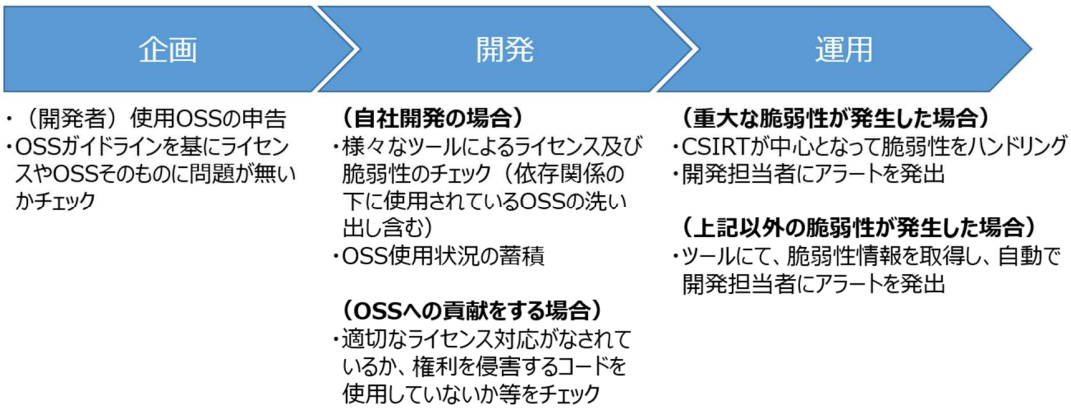


図 4.18-1 ヤフーにおける OSS 管理の全体像[127]

これらの運用を軌道に乗せるため、CTO[128]からトップダウンで各事業部門を統制し、開発者向けの研修プログラム等を実施していった。コンプライアンスやセキュリティへの意識を浸透させるため、開発者や事業推進担当者に対して説明会等を開催し、その中で対応の必要性を論理的に訴え、丁寧にコミュニケーションを取ることで理解を得た。

[127] ヒアリングを基に作成

[128] Chief Technology Officer:最高技術責任者

＜【保守・品質保証(M18)】コミュニティが定義したライフタイムサイクルの準拠＞

OSS を利用したサービスの使用年数については、OSS コミュニティが定めるライフサイクルに沿って使用するよう運用方法を示したリファレンスを提供しており、基本的にはそのライフサイクルに準拠する前提で利用している。しかし、切り替えができない場合など EOL を過ぎても自社の責任の下、利用を続けるケースはある。EOL を過ぎても継続利用するものについては、他社の有償サポートの利用も検討することとしている。

＜【サプライチェーン管理(S18)】社外への開発委託＞

ヤフーは自社開発が多く、実際に社外へ開発委託するケースは基本的にはないが、仮に外注する場合は、発注要件の中に OSS のリストを明示することを記載し、これを受け入れ条件にすることとしている。リストに記載する OSS の粒度については、明示的に利用しているライブラリ、フレームワークベースとし、ツールを利用することによって詳細の OSS を把握する想定である。

＜【コミュニティ活動(C18)】OSS に貢献している社員が使いやすい制度＞

ヤフーは、前述した自社開発ソフトウェアの OSS 化や、他社とのコラボレーションによる OSS 開発、もしくはコミュニティへの積極的参画を通じて OSS のエコシステム発展に貢献している。これらの活動は、OSS の改善による自社事業への還元のみならず、開発者の技術力向上にも効果をあげている。

コミュニティ活動に係る特筆すべき取組として、OSS への貢献を社員が自由に行えるようにするため、会社が認めた場合に、職務上作成した成果物であっても個人に帰属させることができるよう、人事規程上で手当てを行っている。また、OSS デベロッパー認定制度を運用している。これは、ヤフーが戦略的に利用する OSS への貢献の機会や、自社製の OSS を開発するような社員が増えてきたことから、社内外で活動・活躍しやすい環境を整備するために設けられた制度である。具体的には、ヤフーが戦略的に採用している OSS に対して、コミッタとして貢献している社員をデベロッパーとして認定している。また、対象 OSS 開発や関連する活動について一定額の活動予算枠[129]を付与する等、そのコミュニティにおいてコミッタとして活動できる環境を提供している。認定は、CTO 直轄のデベロッパー認定制度事務局が、「対象となる OSS の重要度」「コミュニティからのコミッタとしての評価」「コミュニティにおけるコミッタとしての活動実績」等を総合的に判断した上で行う。2021 年 10 月までに、のべ 28 名[130]のデベロッパーが認定されている。

さらに、The Linux Foundation 及びその下部団体にあたる Cloud Native Computing Foundation（CNCF）等、いくつかのコミュニティに対してスポンサード（金銭的な支援）も実施している。

---

[129] 開発機器の購入費用や、書籍執筆費用、カンファレンスの参加費や、渡航費や宿泊費など幅広く利用できる。

[130] ヤフーが戦略的に利用している OSS のコミュニティで実績を積み上げて認定される場合もあれば、そのコミュニティにおいて既に実績を積み上げている人材を採用し、認定をする場合もある。

4.19. ラキール　～OSS の選定会議と検証ツールの併用による開発と管理の効率化～

■ 企業情報・本事例集における位置づけ

本社	東京都港区
業種	情報・通信業
従業員数（連結）	単体：402 名　連結：474 名（2021 年 4 月現在）
商流	インターネットサービス事業者
観点	「組織体制」「選定評価」「ライセンス」「脆弱性対応」

■ 本事例のエッセンス

- OSS の利用を全社的に促進しており、新しい OSS を利用する際には、開発部と OSS 管理部門のリーダー同士がリスクの確認や懸念点を議論する会議で利用可否を決定する。
- OSS 管理の抜け漏れを防ぎ、開発者と OSS 管理者の業務を効率化するために検証ツール（ソフトウェア構成分析やライセンスの検証を行うツール。以下、同様。）を導入している。

■ 背景・課題

OSS はコミュニティがライセンスを変更する場合もあり、自らが利用している OSS を正確に把握し、最新の OSS ライセンス情報を収集しないと、知らぬうちにライセンスに違反してしまう可能性がある。この解決方法として検証ツールを導入し、OSS 管理の確実性の向上や効率化に取り組んでいる。

■ 取組

＜【組織体制(O19)】OSS を管理する組織体制＞

OSS に関係する部門として、OSS を自社サービスに利用するプロダクト開発本部がある。プロダクト開発本部には約 100 名が在籍し、各プロダクトの開発を行うとともに、開発プロダクト毎に管理者（兼任）を置いている。また、本部内の開発者向けのツール管理やプロダクト管理機能の開発を行う部門（プラットフォームグループ）が、OSS 管理を兼任しており、すべての開発プロダクトで使用されている OSS の管理及び棚卸を行っている。

＜【選定評価(S19)】新しい OSS の選定会議＞

ラキールでは、開発において積極的に OSS を利用していこうという意識があり、開発の効率化のため、開発者が新しい OSS を利用することを止めるのではなく、新しい OSS の利用を促進し、かつライセンスを守り、安全に管理できる方法を目指した。

利用する OSS を選定する際は、OSS を利用するプロダクト開発本部のメンバや関係者及びプラットフォームグループのメンバによる会議において OSS の利用可否を決定することとしており、OSS を利用する企画が上がってきた時に、各プロダクト開発本部とプラットフォームグループのリーダー同士でリスクの確認や懸念点を議論する。会議では、OSS のライセンス、シェア、コミュニティの活性度など各種の情報が共有され、特に、コミュニティの開発がストップしてしまった場合の対応策を検討、確認する。例えば、OSS に脆弱性が見つかっても対処されない場合の対応等である。これまで、選定した OSS のコミュニティの開発がストップしてしまったケースはないが、リスクとして認識しているため、万が一の対応を含め、OSS の利用可否の判断における重要な指標として、コミュニティの活性度等を確認している。なお、上記の運用をルール化して実施している現状に留まらず、今後は OSS の利用や選定に関する体系立てたガイドラインを作成し、明文化による更なる効率化の計画が進行している。

＜【ライセンス(L19)】検証ツールの導入による効率化＞

ある OSS のライセンス変更を知ったことが、OSS 管理の意識向上のきっかけになった。そのライセンス変更は、商用利用するにはソースコードの公開義務が発生するという内容であった。当該 OSS は、事前に利用用途などを把握できていたため、結果的に影響がなかった。一方で、今後も OSS 利用が増えていく傾向がある中で、他の OSS でも同様に知らないうちにライセンス変更され、ライセンスに違反してしまうケースがあるのではないかという懸念が大きくなっていった。このような状況を未然に防ぐため、“確実な OSS の管理”と“OSS ライセンスの最新情報の収集”が急務であった。

そこで、OSS の管理の徹底を図ろうとしたが、大量の OSS を利用しているため、Excel による管理では抜け漏れが発生し、結果としてライセンス違反に気付けないリスクも感じていた。そのため、検証ツールを導入することとし、その選定・導入に当たっては、現状の管理における抜け漏れの検出可否を評価項目とした。また、検証ツールを導入することで、再帰的に使用されている OSS を検出できるようになった。あるプロダクトでは、利用している OSS を 20～30 程度と想定していたが、検証ツールを利用して検出した OSS は再帰的なものも含めると数百あった。

プラットフォームグループが OSS の管理を一手に担っている体制となっており、従来は開発側が新たに OSS を使用するたびに管理工程が増えていく状態だった。しかし、検証ツールを利用することによって OSS 検知処理および情報整理が自動化されたため格段に工数が軽減された。OSS 管理者の体感的には

1/10 程度になったと感じている。

＜【脆弱性対応(V19)】DevSecOps[131]による脆弱性対応＞

プロダクト開発では、ソースコード管理に GitLab を利用しており、CI/CD[132]と検証ツールを連携させることで、使用している OSS の検出と、検出した OSS の脆弱性有無のチェックを自動化している。開発サイクルに OSS の検出と脆弱性のチェックを組み込んだことで、OSS 管理及び脆弱性対応の抜け漏れがなくなり、DevSecOps 体制を構築でき、開発スピードが加速した。

[131] 開発(Development)と運用(Operations)が連携する DevOps にセキュリティ対策を組み込むこと。

[132] Continuous Delivery（継続的デリバリー）、Continuous Deployment（継続的デプロイメント）

4.20. SCSK ～オープンソースソフトウェアへの取組～

■ 企業情報・本事例集における位置づけ

本社	東京都江東区
業種	情報・通信業
従業員数（連結）	14,550 人（2021 年 3 月末現在）
商流	SIer 商流/システムエンドユーザー（IT サービス）
観点	「組織体制」「個の能力・教育」「サプライチェーン管理」「脆弱性対応」「選定評価」

■ 本事例のエッセンス

- OSS の利活用は全社的に重要事項として位置付けられている。開発プロジェクトにおけるリスクの第三者チェック機能である PMO 組織の設立や各事業グループに OSS 管理担当者を設置することで組織体制を構築している。また、e ラーニングや OSS 利活用に関する勉強会を実施している。
- ソフトウェアの部品となる OSS を再帰的に使用することで意図しない OSS が混入していないかを検査するシステム、OSS を調達する際に安全な OSS を選定するシステムを導入し、OSS 利活用に係る課題やリスクに対応している。

■ 背景・課題

OSS を利活用するためには、OSS 利活用に係る課題やリスクを認識した上で、必要な対応を全社的に実施する必要がある。また、ソフトウェア開発において OSS を利用する場合は、利用する OSS が安全かどうか、どのような OSS であるかを把握する必要がある。また、これらの運用を継続していくためにも、体制や仕組みの構築が求められる。

■ 取組

＜【組織体制(O20)】OSS 管理の組織体制＞

開発プロジェクトのリスクを第三者の立場でチェックしプロジェクトの健全な運営を支援する組織として、PMO 組織を設置している。PMO 組織は、各事業グループに設置されている部門 PMO と PMO 施策を統

括･推進する全社 PMO で構成されている。

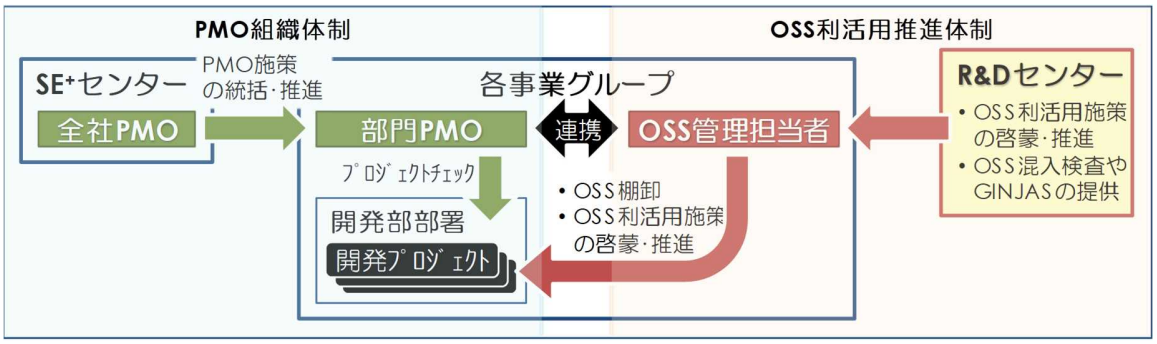


図 4.20-1　PMO 組織と OSS 利活用推進体制の関係[133]

PMO 組織では、システム開発の計画段階から OSS の利用について問題ないかを確認している。具体的には、お客様の要望等によりシステムで利用が想定される OSS を OSS 選定調達支援システム（Ginjas）に登録し、OSS 一覧を PMO に提出することを求めている。さらに、Ginjas にそのシステムで利用する予定の OSS を登録する際には、ライセンスに記載されている OSS の利用条件をプロジェクトで確認するようにしている。

各事業グループに OSS 管理担当者を設けて、OSS 管理の活動を推進している。具体的には、担当している部署を対象に、四半期ごとに利用している OSS の棚卸を実施している。棚卸のタイミングで、OSS 混入検査の実施確認（実施予定時期、予定通り実施したかどうか、実施していない場合はその理由）、Ginjas 利用の周知を実施している。

システム開発する技術者でも、自らが使用している OSS で求められる対処方法（例えば、GPL ライセンスを利用した頒布の対処等）がわからない場合もあるため、専用の問い合わせ窓口を設けて問い合わせ対応を実施している。問い合わせ窓口は、施策の主管部署である R&D センターに、OSS に熟知した技術者とライセンス情報を確認するメンバーを配置している。問い合わせ窓口の担当者の育成は、e ラーニングや OSS 活用ガイドラインにより OSS ライセンス基礎知識を習得し、他社との勉強会に参加する等の活動も通して、OSS ライセンスの理解を深めている。問い合わせ窓口には、ライセンスの使い方、自社製品に OSS を活用してリリースできるか、お客様と共同で開発した製品の取り扱いなどに関する問い合わせがある。

[133] SCSK 提供資料より抜粋

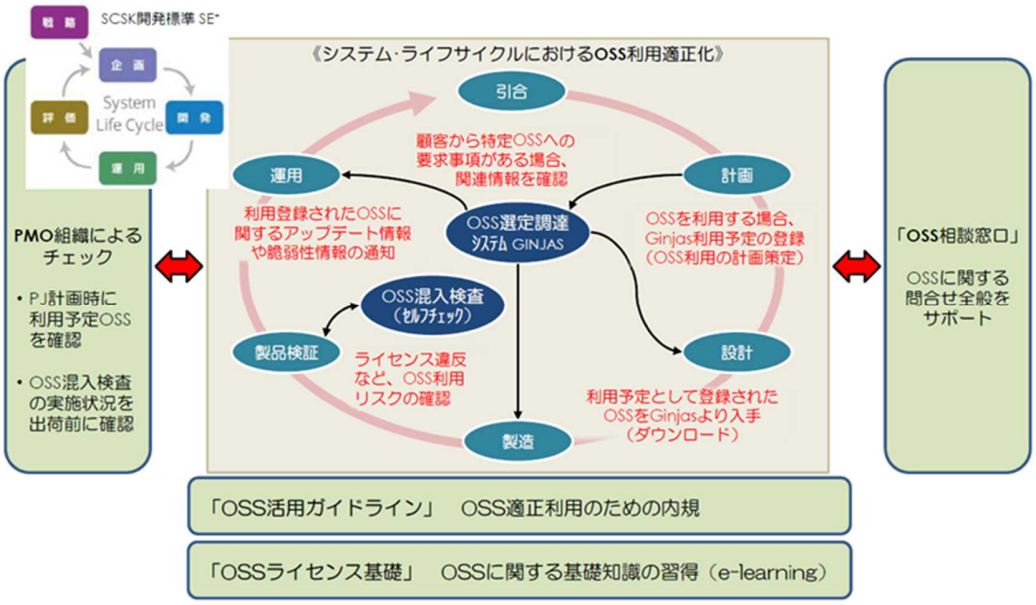


図 4.20-2　OSS 適正利活用施策の全体像[134]

＜【個の能力・教育(P20)】OSS 管理の方針や知識の社内外への取組＞

当社の「情報セキュリティガイドライン」で OSS を含むソフトウェア・ライセンスの適正な利用を定めると共に、開発組織向けに OSS 活用ガイドラインを作成し、グループ全体の現場レベルまで周知している。

また、社内研修の e ラーニングに、OSS ライセンスの解説も掲載し、事務スタッフ以外の社員は全員受講している。なお、研修内容は、問い合わせ窓口に相談のあった中でも重要度が高いものや最新の問合せ内容、最新の相談内容を取り入れ、更新している。

社外向けの OSS に関する啓発活動としては、OSS X Users Meeting[135]という勉強会を開催ししている。この勉強会は、OSS 利用者や開発者を対象にし、OSS の最新動向や使い方の説明など、情報共有している。

＜【サプライチェーン管理(S20)】委託企業への取組＞

委託企業に SCSK の OSS 管理に関する取組や仕組みを説明する。委託企業への発注には、SCSK の OSS ガイドラインの確認、受入検証、検証後のフォローの周知徹底や理解が条件になる。

また、社内向け e ラーニングの OSS に関する内容を共有している。さらに、具体的なフォーマットは決めていないが、使用している OSS の開示を委託企業へ求めている。

---

134 SCSK 提供資料より抜粋

135 https://technomado.jp/tech/5417/

＜【脆弱性対応(V20-1)】OSS 混入検査＞

SCSK は、開発ライフサイクルの製品検証で、OSS の混入検査を実施する。製品開発を外注した場合、受入検証で混入検査を全件チェックしている。OSS 混入検査システムに、コード検査ツール[136]を組み込んでいるが、現場でのセルフチェックを行う上で以下の問題があった。

1 点目は、コード検査ツールは混入の可能性がある OSS 候補を出力するが、候補の OSS 数が膨大な場合、コード検査ツールの出力結果の確認・検証負荷が高い。

2 点目は、出力されるレポートには多くの項目があり、取り扱いに留意が必要となるような OSS を現場レベルで特定することが困難で、作業負荷が高い点である。

これらの問題点を解決するため、SCSK のグループ企業であるベリサーブに依頼し、コード検査ツールをラッピングし、簡単な UI にした。具体的には、様々なオプションが表示される検査ツールの操作画面は使用せず、当社の検査に必要な項目に絞ってプロジェクト名、検査実施者のメールアドレス（検査完了通知用）、ソースコード（ZIP ファイル）登録の 3 ステップで検査を開始できる画面を用意した。さらに、検査結果についても検査ツールの画面で確認するのではなく、Excel のレポート形式で確認できるようにした。Excel のレポートは、利用 OSS ライセンスの利用条件に応じて色分けした検査結果のサマリー、ファイル単位のライセンス情報を記載した一覧シート、確認結果報告用のシート（確認結果報告書）の 3 シートで構成されている。

また、Excel でレポートを出力するセルフチェックシステムへ改修した。さらに、このシステム改修で、検査終了後に通知する機能、検査対象に含まれている可能性の高い OSS を自動判定する機能、対応の優先順位が高いライセンスをもつ OSS を提示する機能を備えることで、開発現場によるセルフチェックが行えるようになった。検査対象に含まれる OSS の判定では、検査ツールが出力する OSS 候補で、一致率が最も高い OSS を選択している。一致率が同じ OSS が複数ある場合は、その中で最も条件が厳しいライセンスの OSS を選択している。対応の優先順位は、利用条件が厳しい順に付けている。コピーレフト型（GPL、AGPL 等）が最優先で、準コピーレフト型（EPL、MPL 等）、非コピーレフト型（Apache、MIT、BSD 等）の順となる。

SCSK での混入検査の精度については、OSS から再帰的に利用される部品についても、納品物に含まれるすべてのファイルを検査することで検出している。なお、ツールには限界があると考えており、ツールでの検査後に、開発者で最終確認を実施するようにしている。具体的には、検査者には、検査結果レポートの内容を鵜呑みにするのではなく、判定結果を確認した上で、OSS ライセンスへの対応方法を確認結果報告書に記載して提出するよう求めている。その確認結果報告書を施策主管部署（R&D センター）への提出をもって最終確認としている。

[136] OSS 情報データベースとの照合により、検査対象のコードに対して OSS コードを検出する機能がある。

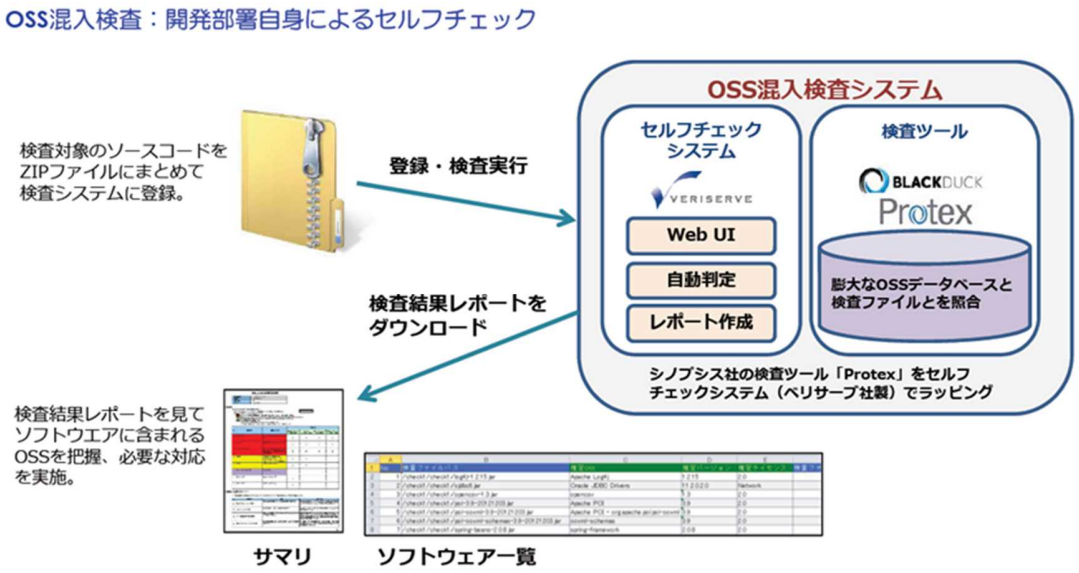


図 4.20-3　OSS 混入検査システムのイメージ[137]

図 4.20-4　OSS 混入検査システムの画面（解析対象ファイルの登録）[138]

[137] SCSK 提供資料より抜粋

[138] SCSK 提供資料より抜粋

図 4.20-5　OSS 混入検査システムの画面（解析結果ステータス）[139]

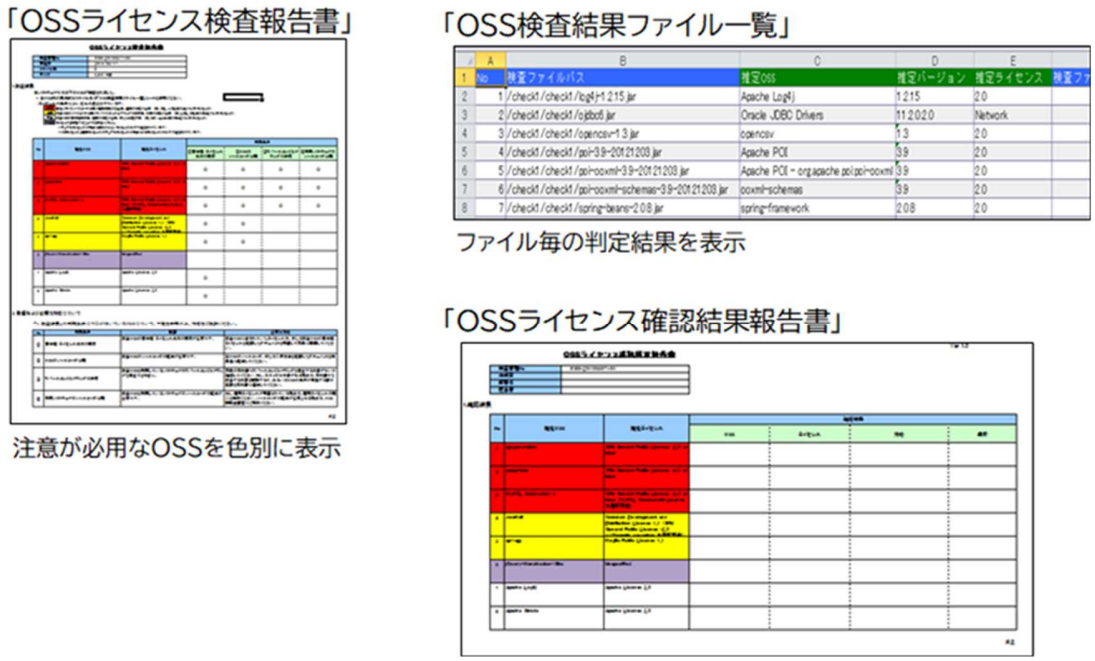


図 4.20-6　OSS 混入検査システムの画面（解析結果レポート）[140]

[139] SCSK 提供資料より抜粋

[140] SCSK 提供資料より抜粋

＜【脆弱性対応(V20-2)】OSS の選定調達支援システム（Ginjas）＞

OSS を安全に利活用できるよう Ginjas と呼ぶ OSS の選定調達支援システムを構築している。Ginjas は、製品開発の計画、設計、運用などの各フェーズで OSS の安全な利活用をサポートしている。Ginjas では、事前に安全性が確認できた OSS について、OSS と OSS 自体の SBOM を登録しておく。この OSS を利用する場合は、Ginjas から OSS をダウンロードし、使用する。Ginjas 以外から OSS を入手して使用しないように教育している。

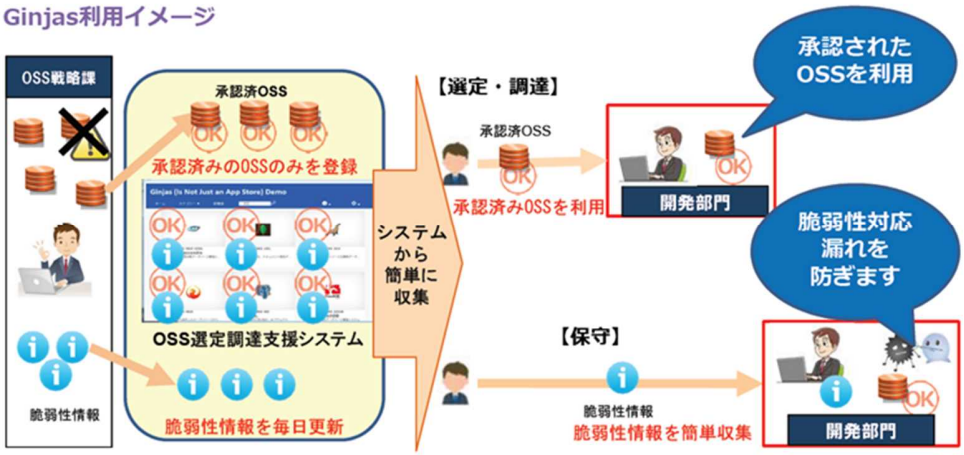


図 4.20-7　Ginjas の利用イメージ[141]

Ginjas は、脆弱性情報を IPA 等の情報サイトから自動で取り込み、その脆弱性と開発製品を突合して評価結果をレポートとして出力する。この脆弱性情報の取り込みには、脆弱性検知ツールである Vuls を利用し、OSS の脆弱性を確認するようにしている。脆弱性等で問題ある場合は、アラートを通知する。

[141] SCSK 提供資料より抜粋

図 4.20-8　Ginjas の主な画面（登録された OSS 一覧と OSS ダウンロード）[142]

Ginjas に登録している OSS の SBOM は、SCSK 独自の形式である。具体的には、OSS の種類、バージョン、ライセンス、入手先など項目を管理している（表 4.16 1 参照）。Ginjas の目的を実現するために必要な項目を管理するため SPDX Lite 等で標準化されているフォーマットは参考にしているが、SCSK 独自のフォーマットで管理している。

[142] SCSK 提供資料より抜粋

表 4.20-1　Ginjas で管理している OSS の項目[143]

分類	項目	内容
基本情報	名称	OSSの名称
	画像	OSSのアイコン画像
	カテゴリ	ライブラリ、フレームワーク等の分類
	ジャンル	Web開発、データアクセス等、主な用途
	ライセンス	ライセンス種別
	プロジェクトURL	プロジェクト公式HPのURL
	リポジトリ	OSSを公開しているリポジトリ
	概要	OSSの説明
	開発元	OSSを開発している企業・団体の名称
	開発元URL	開発企業・団体の公式HPのURL
	組織タイプ	企業、専用基金、個人等の種別
バージョン情報 ひとつのOSSに複数登録	バージョン	バージョン番号、名称
	リリース日	当該バージョンのリリース日
	安定版	当該バージョンが安定版か（True/False）
	アクティブ	EOLになっておらず有効か（True/False）
	アップデート	アップデートが継続されているか（True/False）
	パッケージタイプ	Zip、tar.gz等のGinjasからのダウンロード形式
	URL	当該バージョンを公開しているURL
	プラットフォーム	Windows、Linux等の対応プラットフォーム
CPE情報	CPEベンダ	CPEベンダ名。脆弱性情報の検索用。
	CPE製品	CPE製品名。脆弱性情報の検索用。

＜【選定評価(S20)】よりよい OSS が簡単に見つけられる“物差し”があれば失敗を回避できる＞

SCSK では、情報や知識が少なくても、よりよい OSS が簡単に見つけられる“物差し”によって、無駄な失敗を回避し、OSS を効率的に活用できるツールとして OSS Radar Scope®を開発した。OSS の選定は、選択肢が多く、情報収集にもコツが必要になるが、OSS Radar Scope では、Web で公開されている OSS の成熟度、品質、サービス概要などの一般情報を集積し、SCSK の知見も含め、わかりやすい形式で提示することを目指した。

143 SCSK 提供資料より抜粋

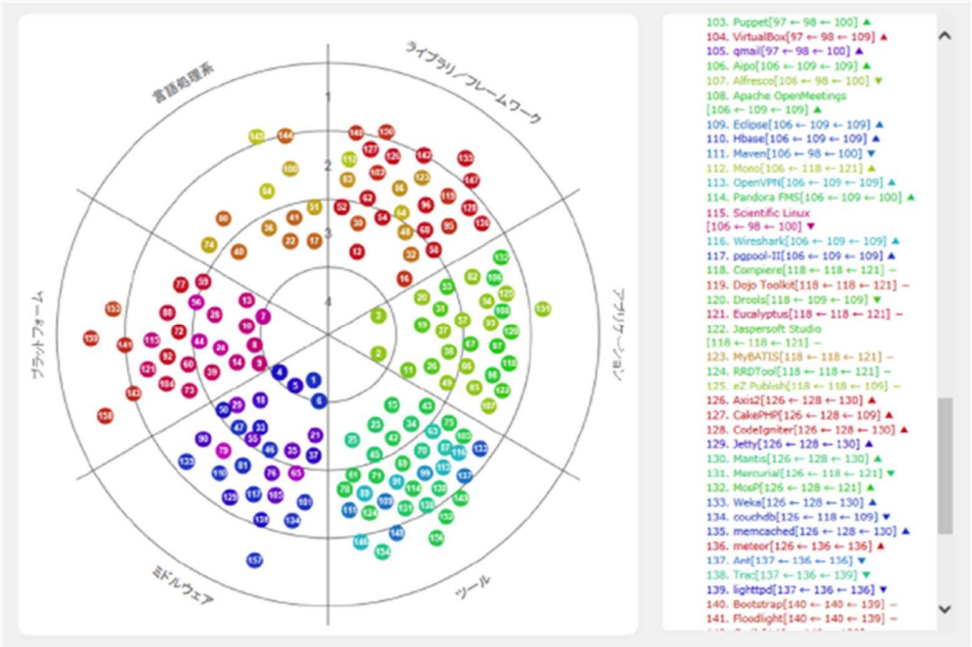


図 4.20-9　OSS Radar Scope®の構造[144]

OSS Radar Scope®では、以下の２つの仮説に基づき、５つの視点に関する客観的なデータを収集し、月次で情報を更新し、レーティングを行っている。

仮説 1）計画的なバージョンアップを経ている OSS は良質の OSS である可能性が高い

仮説 2）出版された書籍の冊数が多い OSS は良質の OSS である可能性が高い

視点 1）リリース履歴

- 計画的なバージョンアップを経ている OSS は良質の OSS である可能性が高いと考えられ、パッチリリースの頻度が適切な OSS は良質の OSS である可能性が高いと考えられる。

視点 2）ドキュメント／関連出版物

- ユーザー向けドキュメントの質／量に力を入れているのは良質の OSS である可能性が高いと考えられ、また出版された書籍の冊数が多い OSS はユーザーが利用しやすく良質の OSS である可能性が高いと考えられる。

視点 3）サポート情報

- サービスを提供する「ベンダの数」×「提供されるサービスの品揃え」と OSS の質は比例すると考えられる。

[144] オープンソースソフトウェアへの取り組み：開発エピソードや運営の裏話
https://www.scsk.jp/product/oss/radarscope_1.html

視点 4）コミュニティの活動状況

- 開発者間でのオープンなコミュニケーションやユーザーからのフィードバックが多い OSS は良質の OSS である可能性が高いと考えられる。

視点 5）プロジェクトの継続性

- 初期リリースからの経過年数の長い OSS は成熟し、安定性と信頼性が高いと考えられる。

5. 事例（文献調査）

5.1. マイクロソフト　～OSS に係るセキュリティリスク緩和策～

■ 企業情報・本事例集における位置づけ

本社	米国
業種	情報・通信業
従業員数	163,000 人（2020 年 8 月時点）
商流	SIer 商流/サービス事業者
観点	「脆弱性対応」

■ 取組

＜【脆弱性対応(V20)】OSS を利用する際のセキュリティリスク緩和策＞

マイクロソフトは、OSS を利用する際、以下 4 つのセキュリティリスク緩和策を実施している[145]。

① 使用している OSS を明確にする

② OSS の使用状況をデータベース等で集中管理する

③ 使用している OSS が安全か確認する

④ セキュリティ面の脆弱性に対応する

以下、各取組の詳細について記載する。

[145] Who Wants a Thousand Free Puppies?
https://download.microsoft.com/download/C/5/E/C5E50D16-6E0B-453A-9A69-195CF3D2C823/LocoMocoSec-2019%20-%20Who%20Wants%20a%20Thousand%20Free%20Puppies%20-%20Michael%20Scovetta%20-%20Microsoft.pdf

① 使用している OSS を明確にする

ソフトウェアを"discover"と呼ばれるツールを用いてソースコードのスキャンすることで、使用 OSS を検知し、レポート（Bill of materials（BOM））を作成する。このプロセスは、ソフトウェア開発者の手間を削減するために高度に自動化されている。

② OSS の使用状況をデータベース等で集中管理する

①において把握された OSS の使用状況は、データベース等で集中的に管理され、いつでも参照できるようになっている。これにより、各組織の OSS の使用状況を可視化するとともに、OSS に脆弱性等が判明した際の対応におけるレスポンスタイム向上とコスト削減を図っている（図 5.1-1）。

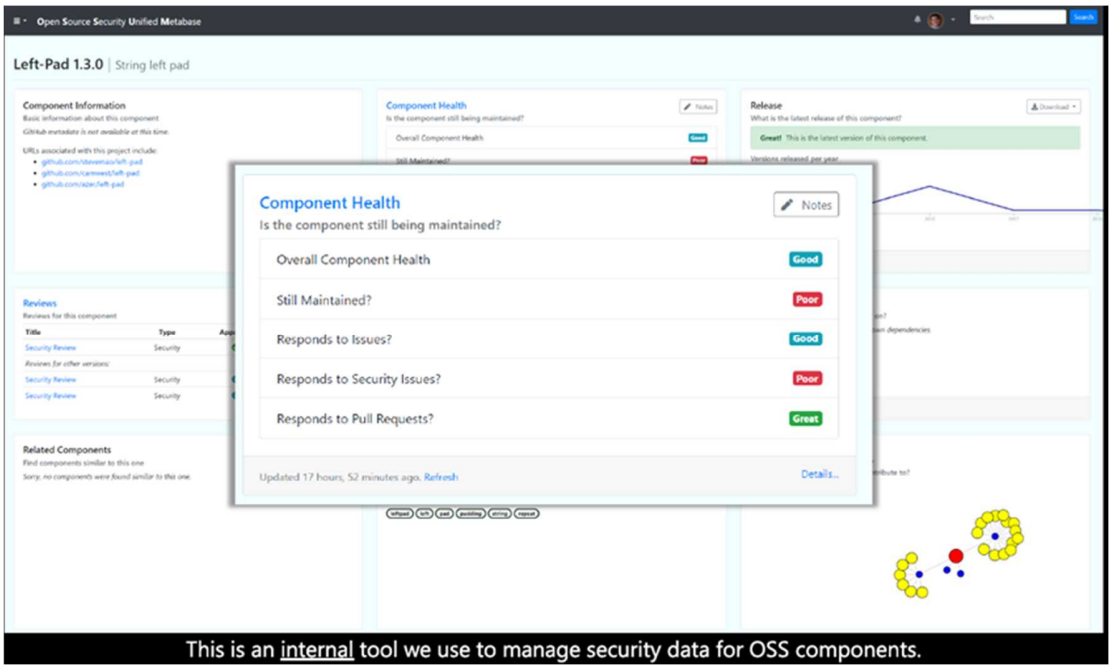


図 5.1-1　OSS コンポーネント関連データを管理する社内ツール [145]
（画面上に OSS コンポーネントのメンテナンス状況が表示されており、参照することで OSS に潜むリスクを把握することが可能）

③ 使用している OSS が安全か確認する

認識された OSS は、社内各組織のリスク許容度に応じて、その安全性の検証が行われる。全ての OSS コンポーネントに対して、公開情報や商用データベース情報の収集、及びツール使用を通して脆

弱性の有無が確認される。更に高いセキュリティが求められる場合は、前述のツール使用に加えてセキュリティレビュー（In-Depth Security Reviews）を実施することでその OSS コンポーネントが安全であるか確認される（図 5.1-2）。In-Depth Security Reviews は、エンジニアチームに支援されたレビューチームが携わる。コストはかかるものの、セキュリティ面における高い保証を得られる。

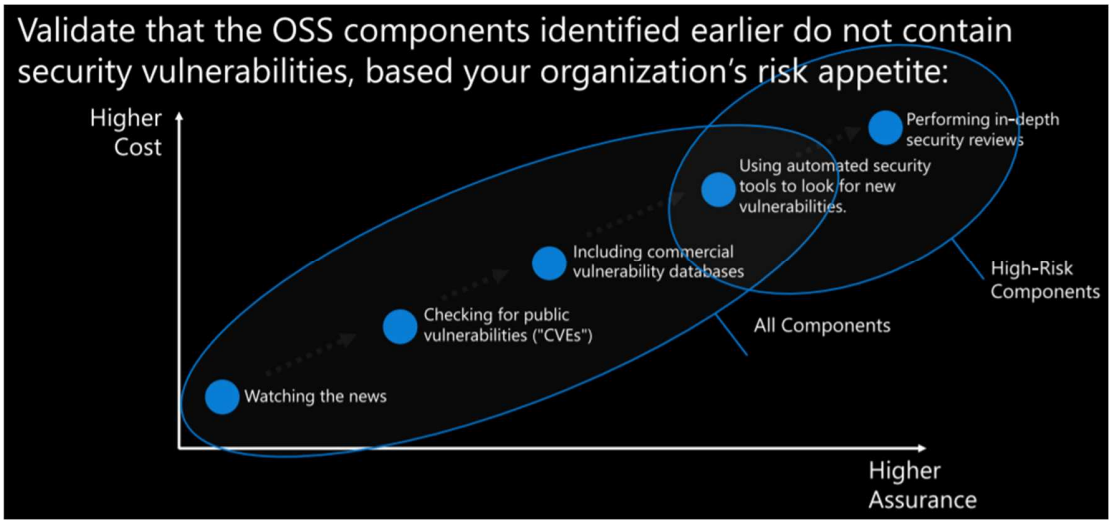


図 5.1-2 求めるセキュリティレベルとコストとのバランスに応じた OSS の安全性確認 [145]

また、その他にもセキュリティアセスメントや統計分析の活用等、様々な手段を用いて脆弱性情報の把握に努め、どの OSS が安全であるかは社内で常にアップデートされている。

④ セキュリティ面の脆弱性に対応する

マイクロソフトでは、組織的なセキュリティプログラムを運営している Microsoft Security Response Center が、OSS のセキュリティ面における脆弱性対応を統合的に実施している。Microsoft Security Response Center の特筆すべき取組として、Microsoft バグ報奨金プログラムを通じた新たな脆弱性発見のためのエコシステム構築や、判明した脆弱性やその対応策に関する情報公開等があげられる。

5.2. ザランド ～OSS プロジェクトの全社的な推進～

■ 企業情報・本事例集における位置づけ

本社	ドイツ
業種	情報・通信業（ファッション製品等の通販サイト運営）
従業員数	13,825 人（2020 年 5 月時点）
商流	SIer 商流/エンドユーザー（IT サービス）
観点	「ライセンス」

■ 取組

＜【ライセンス(L21)】OSS プロジェクトの全社的な推進＞

ザランドでは、OSS プロジェクトの促進、ライセンス遵守、コミュニティへの貢献を目指すため、OSS に係る以下 3 つの理念を掲げている[146]。

- 参加（Participate）：
  社員の OSS プロジェクトへの貢献を促進する。
- 共有（Share）：
  技術がより多くの人の役に立つよう、コードやプロセスを共有する。
- プロモーション（Promote）：
  エンジニアチームにおけるオープンソースコードの使用を奨励し、オープンソースに関するプラクティスを発信する。

また、ザランドのオープンソースチームは OSS の利活用及び開発の奨励、ベストプラクティスの共有等を目的として部門横断的な活動を展開している。具体的には、OSS に関する以下のドキュメントを作成し、社内外に展開・公表している[147]。

---

[146] ザランドホームページ
https://opensource.zalando.com/

[147] ザランドホームページ Documentation
https://opensource.zalando.com/docs

- ライセンスガイド（Open Source Licensing Guide）
- オープンソースコードの採用（Adopting open source code）
- オープンソースプロジェクトのリリース（Releasing an open source project）
- 2018 年次レポート（State of open source at Zalando 2018 Report）
- アンチハラスメントポリシー（Anti-Harassment Policy）

この内、OSS の利活用及び開発に関連するガイドラインである①「ライセンスガイド」及び②「オープンソースプロジェクトのリリース」について、以下概説する。

①ライセンスガイド[148]

ライセンスガイドでは、使用可能なライセンス、使用を控えるべきライセンス等について説明をしている。具体的には、ザランドでは、以下 3 類型のライセンスに該当する OSS の使用を認めている。

- 許可型ライセンス（Permissive licenses）：
  コピーライトとライセンス情報を付することで、使用、改変、配布が可能なライセンス。
  AFL、Apache、BSD、MIT、MS-PL、ISC、PHP License 等。
- 弱コピーレフトライセンス（Weak copyleft licenses）：
  コピーライト、ライセンス、変更記録、ソースコード、インストール方法の情報を付することで、使用、改変、配布が可能なライセンス。
  APSL、CDDL、CPL、EPL、IPL、MPL 等。
- 強コピーレフトライセンス（Strong copyleft licenses）：
  コピーライト、ライセンス、変更記録、ソースコード、インストール方法の情報、オリジナルソースを付することで、使用、改変、配布が可能なライセンス。ザランドでは社内用にのみ使用可能となっている。
  BCL、GPL、LGPL、NPL、OSL、QPL 等。

一方、ザランドでは AGPL 関連ライセンス、共通条項（Commons Clause）ライセンス及びライセンスなしのコードの使用は認めていない 。

[148] ザランドホームページ Licensing
https://opensource.zalando.com/docs/resources/licensing/

②オープンソースプロジェクトのリリース[149]

ザランドの社員は、Zalando-Incubator[150]を通じて、新規オープンソースプロジェクトをリリースすることが可能である。プロジェクトを実施するために従うべきルールとして以下の項目を定めている。

- 既存業務の調整（Get sign off）：
  プロジェクトを開始する社員は、新しいオープンソースプロジェクトに業務時間を割くことについて、所属するチームのリーダーとメンバーから承認を得る必要がある。
- コンプライアンス（Be Compliant）：
  全てのオープンソースプロジェクトはザランドのルールブック（Rules Of Play）やベストプラクティスに従ってコードをリリースしなくてはならない。具体的には、ライセンス等に関連して必要となるファイルを作成することや、成果物のバージョン名を有意に設定すること等が求められる。
- レポジトリの準備（Prepare your repository）：
  リリースに向けて、コードの保守性・可読性を高めたり、必要なドキュメントを準備する等、レポジトリの準備をする。また、コードが前述のルール等に準拠しているか、ザランド外の環境でも動作するか、コード内に機密情報が含まれていないか等、いくつかの観点でチェックする。
- レビューの実施（Get Reviewed）：
  リリースの準備ができたコードは、オープンソースレビューグループのレビューを受けなくてはならない。レビューに合格すれば、Zalando-Incubator を通じてリリースされる。

---

[149] ザランドホームページ Releasing a new open source project
https://opensource.zalando.com/docs/releasing/index/

[150] Zalando-Incubator とは、新規オープンソースプロジェクトの立ち上げを支援するザランドの GitHub コミュニティである。ザランド社員が新規オープンソースプロジェクトをリリースする場合、Zalando-Incubator において試験的にオープンソースプロジェクトを立ち上げ、当該プロジェクトのレビューと持続可能性の評価が行われる。ザランドのオープンソースレビューグループが Zalando-Incubator のプロジェクトの評価を担い、アクティビティやコミュニティ参加状況に関して一定の水準をクリアすれば Zalando-Incubator を卒業し、ザランドのメイン GitHub コミュニティにおけるオープンソースプロジェクトとして昇格するシステムとなっている。
https://opensource.zalando.com/docs/releasing/incubation/
https://opensource.zalando.com/docs/releasing/graduation/

5.3. Linux Foundation とハーバード大学による Census Ⅱ プロジェクトの予備的レポート ～アプリケーションに最も利用されている FOSS コンポーネントに関する調査～[151]

■ 本事例集における位置づけ

観点	「脆弱性対応」

■ 本事例のエッセンス

- Census Ⅱ プロジェクトを通じて、現代のソフトウェアの大半を占める FOSS（Free and Open Source Software）に関し、特に、広く利用されている FOSS コンポーネントが特定された。
- FOSS の上位貢献者のうち、4 分の 3 以上が企業の従業員であることが明らかになった。
- 調査の過程で、ソフトウェアコンポーネントの標準化された命名規則の欠如、個人の開発アカウントのセキュリティの重要性の増大、OSS におけるレガシーソフトウェアの持続性という課題が明らかになった。

■ Census Ⅱ の背景

現代のソフトウェアの 8～9 割は FOSS コンポーネントで構成されているとされている。しかし、FOSS の品質やメンテナンスを保証する機関が存在しないことや、自由に複製や改変が可能であることから、どのような FOSS が最も広く使われているのかは不明瞭である。

FOSS のエコシステムの将来の健全性と安全性を確保するために、民間及び公的機関でどのような FOSS が利用されているのか、それらがどの程度メンテナンスされ、サポートされているのかを理解することが非常に重要であるとの認識の下、Linux Foundation の Core Infrastructure Initiative（CII）[152] とハーバード大学イノベーションサイエンス研究所により Census Ⅱ プロジェクトが立ち上げられた。

---

[151] Vulnerabilities in the Core Preliminary Report and Census II of Open Source Software
https://www.coreinfrastructure.org/wp-content/uploads/sites/6/2020/02/census_ii_vulnerabilities_in_the_core.pdf

[152] Heartbleed 問題（OpenSSL 脆弱性）の問題を受け、Linux Foundation により 2014 年に設立された機関

■ レポートの概要（【脆弱性対応(V22)】）

CensusⅡプロジェクトの予備的なレポートとして、2020 年 2 月に「Vulnerabilities in the Core Preliminary Report and Census II of Open Source Software」が公表された。レポートの概要を以下に記載する。

＜調査の目的＞

① 製品アプリケーションにおいて最も一般的に使われている FOSS コンポーネントを特定すること

② それらの FOSS コンポーネントについて、以下に起因する潜在的な脆弱性を調査すること

- 古いバージョンの広範な利用
- プロジェクトの人員不足
- セキュリティ上の脆弱性が知られていること

③ これらにより得られた情報を、FOSS の健全性と安全性をサポートするための投資における優先順位付けに活用すること。

＜調査結果＞

パートナーであるソフトウェア構成分析をする企業やアプリケーションのセキュリティ企業から提供を受けたデータセットについて依存関係の分析を実施し、その中で最も利用されている FOSS コンポーネントを明らかにした。レポートでは、付録として最も使用頻度の高い 10 のパッケージがアルファベット順に列挙されている（表 6）。なお、JavaScript パッケージが圧倒的に多かったため、JavaScript パッケージを除外した場合の上位パッケージを特定するために、JavaScript と JavaScript 以外のそれぞれについて抽出されている。ただし、非推奨であったり、数年間更新されていないいわゆる「レガシーソフトウェア」が利用されている場合に、それが現在も積極的に使われているのかについては更なる深い調査が必要であることや、調査に用いられたデータセットは量的にも質的にも限定的なものであったことから、予備的レポートの調査結果は、どの FOSS パッケージが最も重要であるかを主張するものではない旨、補足されている。

表 5.3-1 最も利用されている FOSS パッケージ

JavaScript パッケージ	JavaScript 以外のパッケージ
async	com.fasterxml.jackson.core:jackson-core
inherits	com.fasterxml.jackson.core:jackson-databind
isarray	com.google.guava:guava

JavaScript パッケージ	JavaScript 以外のパッケージ
kind-of	commons-codec
lodash	commons-io
minimist	httpcomponents-client
natives	httpcomponents-core
qs	logback-core
readable-stream	org.apache.commons:commons-lang3
string_decoder	slf4j:slf4j

また、FOSS の開発者について、上位貢献者のうち、企業に雇用されている者として特定された者は 75%、個人事業主として特定された者は 15%（残り 10%は不明）であり、企業の従業員の割合が高いことが明らかとなった。2017 年の GitHub のデータを分析したところ、最もアクティブな FOSS 開発者の中には、マイクロソフト、グーグル、IBM、インテルの従業員用のメールアドレスでプロジェクトに貢献している者がいることが判明した。付録に記載されているプロジェクトへの貢献者が、これらのパッケージ開発のために雇用元の企業から直接報酬を受け取っていないとしても、FOSS コミュニティのメンバーとしての彼らの地位が、雇用のための資格を裏付けるものであった可能性があることを指摘している。ただし、貢献者がどのような状況で活動しているのかをより明確にし、それらの仮説を裏付ける直接的なデータがなければ結論を出すことはできない旨、補足されている。

＜調査によって得られた課題＞

Census II プロジェクトの初期段階に、当プロジェクトの取組とは別に、以下の課題が明らかになった。レポートでは、これらの課題は、調査の結果に影響を与えるものではないとしつつ、より広範な議論がされるべき重要なものであり、調査に値するものであるとしている。

① ソフトウェアコンポーネントの標準化された命名規則の欠如

ソフトウェアコンポーネントの命名規則が標準化されていないため、データセットを分析するためのデータセットの統合に際して多大な労力が必要とされた。NIST[153]や NTIA のプロジェクトでも明らかとなったように、ソフトウェアサプライチェーンの透明性とセキュリティへの取組が発展し、より複雑になるにつれて、命名規則の欠如は、産業界や政府によるソフトウェアベースのインシデントから自身を守るための取組

[153] National Institute of Standards and Technology：アメリカ国立標準技術研究所

を阻害する脅威となっていることを指摘している。

② 個人の開発アカウントのセキュリティの重要性の増大

最も利用されているソフトウェアパッケージの上位 10 件のうち、7 つのパッケージが個人の開発者アカウントにより開発されているなど、多くのプログラムが個人の開発アカウントに存在することが明らかになった。個人の開発アカウントは、企業のアカウントと比べて脆弱である可能性があるため、個人の開発アカウントの管理下にあるコードの変更はかなり容易に、しかも検出されずに行うことができる旨指摘されている。これはリスクに留まるものでなく、実際に発生しており、悪意ある者が正当な管理権限を委譲されてバックドアを仕掛けた Copay[154]の事例は、厳密にいうと乗っ取りではないが、個人の開発アカウントは侵入や乗っ取りの危険性もあることが指摘されている。また、Left-pad[155]の事例では、パッケージの命名争いを発端として開発者がコードをレポジトリから削除したことにより、たとえそれが一見些細なコードであるように見えても、当該コードに依存していた多くのパッケージが機能しなくなったなど、開発者本人の行動が大きな影響を及ぼした例も挙げられている。

③ OSS におけるレガシーソフトウェアの持続性

基本的に同じ機能を有する新しいパッケージが存在するにもかかわらず、古いパッケージの利用率の方が高いケースがある。互換性のバグへの懸念や、改修にかかる時間やコストの制約から、新しいソフトウェアへの切り替えが進みにくいことが原因と想定されている。古いパッケージの開発者は時間とともに減少するため、FOSS のレガシー問題についても認識する必要がある旨指摘されている。

[154] bitpay 社が手掛けるモバイルウォレットアプリ

[155] 文字列の調整を行う機能を持つ JavaScript で書かれたライブラリ

6. まとめ

本事例集では、ヒアリングにより収集した国内企業の事例（20 事例）と、公開文献の調査により収集した海外事例（3 事例）を紹介した。本章においては、3.2.2 章において取りまとめた観点ごとに各事例における取組のポイント等を取りまとめる。

■ 選定評価

OSS の選定評価においては、選定基準の明確化が重要視されていた。例えば、使用可能もしくは使用不可な OSS をリスト化し、社内もしくはグループ内の OSS 選定においてそのリストへ準拠することをルール化する手法を採る企業や選定調達を支援するシステムを構築している企業が見られた。その他、使用 OSS に関するポリシーを定め、そのポリシーに則り OSS を選定することをルール化する方法も採られていた。さらに、よりよい OSS が簡単に見つけられる物差しを独自に定め、物差しに基づき情報収集し、一般公開する取組もあった。

これらのリストやポリシーが常に最適な OSS の使用基準となるよう、専門的な知識を持ったメンバーによる定期的なレビューやメンテナンス等の工夫が見られた。また、各 OSS の使用可否の判断やポリシーの設定においては、後述の「ライセンス」「保守、品質管理」等の観点や、当該 OSS の社内もしくはグループ内の使用実績、コミュニティの活動状況等が考慮されていた。

■ ライセンス

ライセンス対応は、特に製品商流において重点的に取り組まれており、OSS 管理に関する取組を開始するきっかけとしてライセンスコンプライアンスをあげる企業も多かった。その対応においては、OSS を使用する際に当該 OSS のライセンスの内容を組織として把握し、対応要件を遵守可能か等の観点から審査する手法が採られていた。あわせて、一連のワークフローのシステム化、ツール等を用いた未認識の OSS の有無の確認、特定の開発段階での承認のルール化等、確実なライセンス対応を担保するための工夫も見られた。ワークフローシステムに使用 OSS の情報を蓄積し、後述の「脆弱性対応」において活用している事例もあった。

また、ライセンス対応においては法務の知見が必須となる。ワークフロー上に法務部門がレビューする機会を設けたり、必要に応じて法務部門が事業部にアドバイスを行う等の対応が見られた。

さらに、ライセンス管理や構成管理として、ビルドシステム等の OSS に備わっている機能を活用しながら、ソフトウェアの依存関係を管理している取組や検証ツールの自動化による早期検証や省力化が考慮されていた。

■ 脆弱性対応

脆弱性対応においては、SBOM を活用する企業が多く見られた。SBOM の作成は、前述のライセンス対応で得られた使用 OSS 情報の活用や、ツールの利用等により行われていた。収集した OSS の脆弱性情報を SBOM と突合して影響を把握し、必要に応じて当該 OSS を使用している製品やサービスの担当部署によって適切な対応がなされていた。OSS の脆弱性情報の収集は、JVN 等からの情報に加え、一般的な情報ソース（ニュースサイトやブログ等）からも収集することで、より迅速な対応を可能にするといった工夫も見られた。複数の企業で、脆弱性のハンドリング対応において中心的な役割を果たす PSIRT 等の組織を設け、各部署と円滑に連携して対応する体制が採られていた。

他方、SBOM で管理している情報と収集した脆弱性情報における、OSS 名称や情報粒度に差異があるため、適切に突合ができないという課題も認識されていた。一部企業では、AI 等の先進技術を用いて解決を模索していた。

■ 保守、品質保証

保守、品質保証においては、SBOM 等を含む OSS 管理の仕組みの中で、EOL の時期も管理することで、適切な対応が実施されるよう工夫する企業が見られた。また、保守可能なディストリビュータを介した OSS の調達や、社内人材でワークアラウンドできる OSS の使用をルール化するといった手法も採られていた。

社会インフラ系のシステム等に使用される OSS においては、その分野的特性から長期保守を実現させるための議論も実施されている。また、通信事業では、長期的な OSS の活用におけるリスクとして、特に脆弱性管理やアップデート対応に関するコスト等について、予め顧客と SIer が事前に合意する取組があった。

■ サプライチェーン管理

サプライチェーン管理においては、サプライチェーンの各社で使用されている OSS を把握するために、サプライヤ企業や委託先との取決めや契約の中で、使用 OSS の申告を義務付けている企業が見られた。そうした取決め・契約の締結の際には、サプライヤ企業や委託先からの理解を得るため、サプライチェーンにおける OSS 使用状況把握の必要性を丁寧に説明する等、地道な努力が行われていた。

また、特筆すべき活動として、OpenChain の自己認証取得や OpenChain を通じた情報共有・発信が挙げられ、ライセンスコンプライアンスの重要性に関する共通認識の醸成に取り組む企業が多く見られた。このような企業の壁を越えた取組が、サプライチェーン全体の OSS に対するリテラシー向上に寄与している。

■ 個の能力、教育

社員の OSS に対するリテラシー向上のために教育メニューを整備している企業が見られた。具体的には、OSS の利活用啓発、OSS を利用した開発の進め方、ライセンスコンプライアンス対応等について多彩な教育メニューが用意されていた。社員に高いリテラシーを身に付けさせるため、一定の得点を目標とした試験を実施する工夫も見られた。また、海外拠点においても国内の社員と同等レベルのリテラシーを確保するために、英語教材を整備している企業もあった。

さらに、経営層のキーマンが理解を示したことで、OSS の取組が加速された企業が複数あった。このことから、OSS 利活用を進めるためには、現場レベルのリテラシー向上だけではなく、経営層に対する啓発や情報共有によって理解を得ることが重要であると推察される。

■ 組織体制

OSS 対応に係る組織体制に関しては、OSS 対応を主なミッションとする専門組織を持つ企業がある一方、各部門から代表者が集まり部門横断的でコミュニティのような対応組織を持つ企業がある等、様々な形が見られた[156]。さらに、OSS の利用可否の意思決定を効率的に行うため、開発部門と OSS 管理部門のリーダー同士がリスクの確認や懸念点を議論して決定する取組もあった。また、セキュリティ対応を担う部署の社員が OSS 対応を兼任する体制も、OSS に対する取組が発展途上である場合に多く見られた。

OSS 対応には、OSS 自体や OSS を利活用している自社の製品・サービスの十分な理解に加え、セキュリティや法務、調達、品質管理といった複数部門にまたがる広い知見が求められる。また、製品・サービスの事業環境によっても適切な体制は異なるため、各企業は、自社の各製品・サービスの事業環境も考慮したうえで、企業内、グループ内の各部署と適切に連携する体制の構築に努めていた。

■ コミュニティ活動

OSS の利活用においては、コミュニティ活動への積極的な参加が重要な意義を持つと認識している企業が見られた。そのような企業では、社員のコミュニティ活動を業務の範囲として扱ったり、コミュニティ参加に関するガイドラインを整備する等、社員のコミュニティ活動への参加を後押しし、所属企業の利活用に問題がない場合は、社員が個人としてコミュニティに還元することも認める取組もあった。その理由は、OSS の場合、コミュニティ活動が活発化することでその性能や品質が向上するため、社員のコミュニティ活動への参加・貢献が、その OSS を利用する企業側のメリットにつながるためである。さらに、社員がコミュニティ活動において

[156] 経済産業省で取りまとめた「サイバーセキュリティ体制構築・人材確保の手引き」に整理されているセキュリティ統括機能の形態である「専門組織型」「委員会型」が存在していると捉えられる。
https://www.meti.go.jp/press/2020/09/20200930004/20200930004-1.pdf

最大限の成果をあげられるよう、コミュニティ型開発の進め方に関する研修メニューを用意している企業や、自社開発したソフトウェアを OSS 化し、コミュニティ型開発による性能向上を図る企業等、OSS のエコシステムを戦略的に活用する工夫も見られた。