HITACHI
Inspire the Next

SPI Japan 2024

ソフトウェア部品表(SBOM)活用システムによるコンプライアンス・セキュリティの向上

2024/10/17

株式会社 日立製作所
マネージド＆プラットフォームサービス事業部
ソフトウェアエンジニアリングCoE OSSソリューションセンタ
金子 真也

© Hitachi, Ltd. 2024. All rights reserved.

自己紹介

HITACHI
Inspire the Next

金子　真也（かねこ しんや）

- 所属：(株)日立製作所 マネージド＆プラットフォームサービス事業部
  ソフトウェアエンジニアリングCoE OSSソリューションセンタ
- 経歴：
  - 2009～：メインフレーム系、障害情報採取系の社内ツール開発・保守
  - 2014～：銀行営業店・為替システムの開発
  - 2016～：日立社内でOSS活用推進のためのコンプライアンス制度の策定、および支援システム(ソフトウェア部品表(SBOM)活用システム)の開発・運用、日立グループ内への展開に従事

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

ソフトウェア部品表(SBOM)活用システムの開発と適用

■ 課題

- 今やOSSを用いずに製品・サービスを構築することは困難。
- 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、ソフトウェアライセンスおよび脆弱性の管理で、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。

ソフトウェアライセンス、脆弱性の管理などのために独自にSBOM活用システムを開発
これにより、ソフトウェアライセンス・脆弱性調査の工数を削減することが出来た

© Hitachi, Ltd. 2024. All rights reserved.

日立の社会イノベーション事業の推進体制

HITACHI
Inspire the Next

お客さま領域

金融、公共、電力、交通、通信など

パワーグリッド、原子力、鉄道など

ファクトリー、テック、ビル、ホームなど

デジタルシステム＆サービス

最先端のCPSで、
社会を支えるシステムの効率を向上

- **デジタルソリューション**
  コンサルティング、デジタルエンジニアリング、AI、データアナリティクス、システムインテグレーション、制御システム、クラウド・マネージドサービス、セキュリティ
- **ITプロダクツ**
  ストレージ、サーバ
- **ATM**

売上収益：2兆5,986億円
Adjusted EBITA：3,334億円
従業員数：10.7万人

グリーンエナジー＆モビリティ

脱炭素に向けたエネルギー転換と
安全、快適でクリーンな移動を提供

- **エネルギーソリューション**
  パワーグリッド、原子力、再生可能エネルギー、分散電源ソリューション
- **鉄道システム**
  車両、信号、ターンキー、運行・保守

売上収益：3兆523億円
Adjusted EBITA：1,991億円
従業員数：6.5万人

コネクティブインダストリーズ

レジリエントなサプライチェーンを提供し
産業と都市を革新

- **ビルシステム**
  昇降機、ビルソリューション
- **生活・エコシステム**
  家電、空調
- **計測分析システム**
  ヘルスケア、バイオ、半導体、産業
- **産業・流通ソリューション**
- **水・環境ソリューション**
- **産業用機器**

売上収益：3兆579億円
Adjusted EBITA：3,206億円
従業員数：8.2万人

売上収益、Adjusted EBITAは2023年度実績、従業員数は2024年3月末日時点。なお、本社人員他1.5万人は上記に含まれません。

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

Contents

1. 改善背景と課題
2. 改善内容
3. 改善策実施の効果
4. まとめ

© Hitachi, Ltd. 2024. All rights reserved.

1. 改善背景と課題

© Hitachi, Ltd. 2024. All rights reserved.

1-1 改善背景と課題

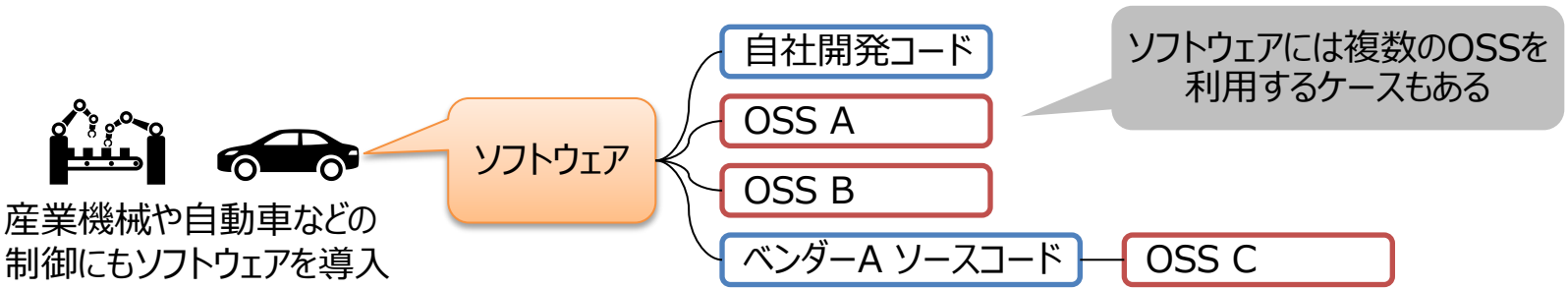
HITACHI
Inspire the Next

■ 背景

- 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の高まり

- 特に、ソースコードが一般に公開され、商用・非商用を問わず利用・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システムなどを中心に、近年、企業の商用製品・サービスにも積極的に採用

今やOSSを用いずに製品・サービスを構築することは困難

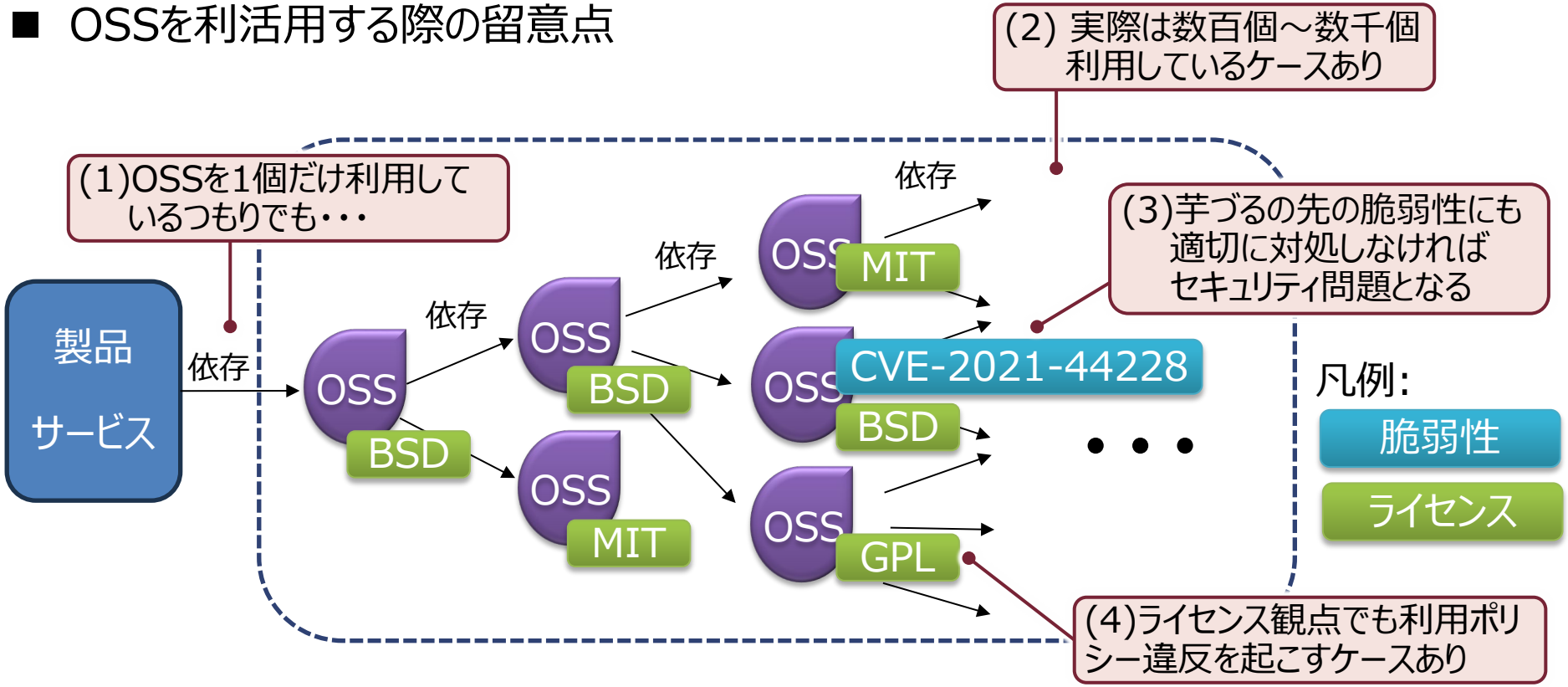


© Hitachi, Ltd. 2024. All rights reserved.

1-2 改善背景と課題

HITACHI
Inspire the Next

■ OSSを利活用する際の留意点



© Hitachi, Ltd. 2024. All rights reserved.

1-3 改善背景と課題

HITACHI
Inspire the Next

■ 課題

① 大量のOSSライセンス調査および脆弱性監視、影響調査に多大な工数を要する。

② 個々の製品・サービス開発プロジェクトにて①を行っており、重複作業が無駄となっている。
また、作業が属人化して正確性にバラつきがある。

■ 改善検討

- サプライチェーン内で利用されるソフトウェアライセンスおよび脆弱性情報を管理する仕組み
- 誰かが一度調査した情報を日立グループ内で共有する仕組み
- 正確性・効率性を向上させるため、機械的なプロセスの構築

ソフトウェア部品表(SBOM)を活用したシステムを開発することで改善を検討

© Hitachi, Ltd. 2024. All rights reserved.

2. 改善内容

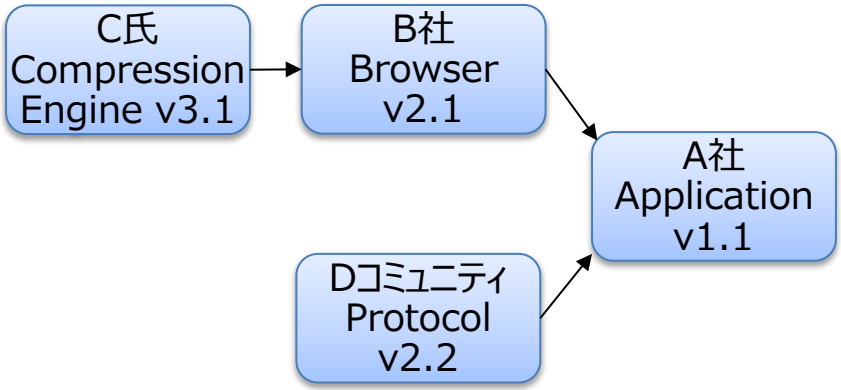
© Hitachi, Ltd. 2024. All rights reserved.

2-1 ソフトウェア部品表（SBOM）とは

HITACHI
Inspire the Next

- SBOM(Software Bill of Materials)とは
  - ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リスト
  - ソフトウェアに含まれるコンポーネントの名称やバージョン情報、コンポーネントの開発者などの情報が含まれる
  - 米国、EUを中心にSBOM管理の義務化の流れがある
    ⇒米国:大統領令(EO 14028), EU:欧州サイバーレジリエンス法, 日本:薬機法

OSSの構成イメージ



ID	コンポーネント名	サプライヤー名	バージョン	UID	依存関係
#1	Application	A社	1.1	234	Primary
#2	Browser	B社	2.1	334	Included in #1
#3	Compression Engine	C氏	3.1	434	Included in #2
#4	Protocol	Dコミュニティ	2.2	534	Included in #1

© Hitachi, Ltd. 2024. All rights reserved.

2-1 ソフトウェア部品表（SBOM）とは

HITACHI
Inspire the Next

■ SBOMのメリット

区分	項目	内容
脆弱性管理	脆弱性残留リスクの低減	脆弱性情報を収集し、SBOMの情報と突合して脆弱性を検出することで**脆弱性が残留するリスクを低減**
	脆弱性対応期間の短縮	SBOMツールなどを用いることにより新規脆弱性をリアルタイムで検出し、影響を判断することで、**初動期間を短縮**
	脆弱性管理コストの低減	SBOMツールを用いた自動管理により**管理コストを低減**
ライセンス管理	ライセンス違反リスクの低減	OSSの特定漏れによる**ライセンス違反のリスクを低減**
	ライセンス管理コストの低減	SBOMツールを用いた自動管理により**管理コストを低減**
開発生産性向上	開発遅延の阻止	コンポーネントに関する問題を早期に特定することで、**開発遅延の発生を防止**
	開発にかかるコストの低減	コンポーネントに関する問題の早期特定による**対応コストの低減**
	開発期間の短縮	使用するコンポーネントを選定する際、類似製品に関する過去のSBOMを参照することで、**選定に関する工数を削減**

© Hitachi, Ltd. 2024. All rights reserved.

2-1 ソフトウェア部品表（SBOM）とは

HITACHI
Inspire the Next

■ SBOMのメリット

課題①
大量のOSSライセンス調査および脆弱性監視、影響調査に多大な工数を要する。

課題②
個々の製品・サービス開発プロジェクトにて①を行っており、重複作業が無駄となっている。また、作業が属人化して正確性にバラつきがある。

区分	項目	内容
		脆弱性情報を収集し、SBOMの情報と突合して脆弱性を検出することで**脆弱性が残留するリスクを低減** ①
		SBOMツールなどを用いることにより新規脆弱性をリアルタイムで検出し、影響を判断することで、**初動期間を短縮** ①
	脆弱性管理コストの低減	SBOMツールを用いた自動管理により**管理コストを低減** ②
ライセンス管理	ライセンス違反リスクの低減	OSSの特定漏れによる**ライセンス違反のリスクを低減** ①
	ライセンス管理コストの低減	SBOMツールを用いた自動管理により**管理コストを低減** ②
		コンポーネントに関する問題を早期に特定することで、**開発遅延の発生を防止**
		コンポーネントに関する問題の早期特定による**対応コストの低減**
		使用するコンポーネントを選定する際、類似製品に関する過去のSBOMを参照することで、**選定に関する工数を削減** ②

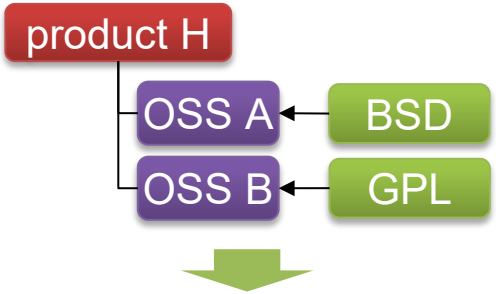
© Hitachi, Ltd. 2024. All rights reserved.

2-2 日立のSBOM活用システムの概要

HITACHI
Inspire the Next

- 日立グループ内で**誰かが一度調査したSBOM情報を共有し、重複して調査するムダを排除**
- **単純作業を排除**し、担当者依存にならないよう一定のレベルを担保（機械化）

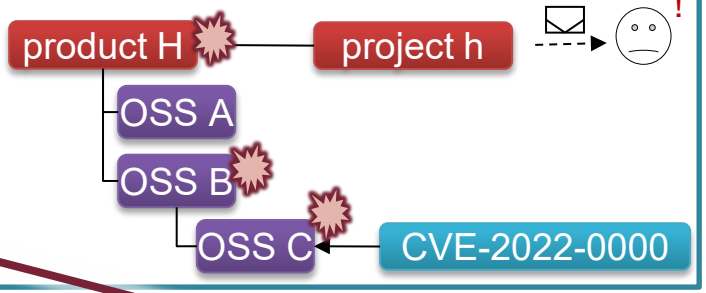
ライセンス遵守確認・一覧自動生成



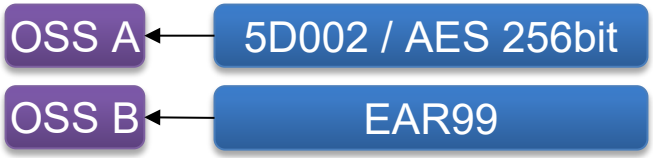
Third party software	Version	License agreement
OSS A	1.0(modified)	BSD 3-Clause "New" or "Revised" License
OSS B	3.3.1	GNU General Public License Version 3
OSS C	5.1	Apache License, Version 2.0
OSS D	1.0(modified)	The MIT License

SBOM活用システム

脆弱性/EOL影響調査・メール通知



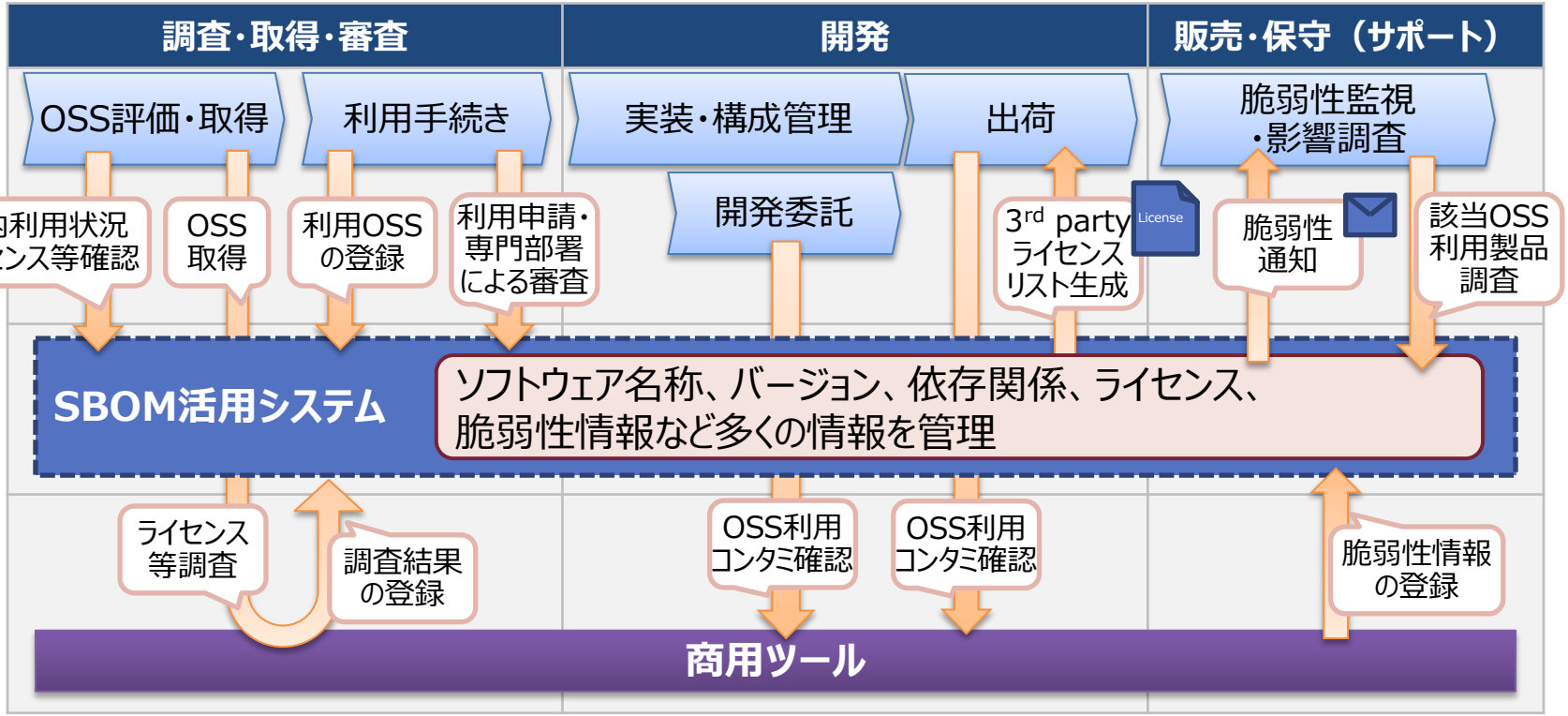
輸管判定支援、エビデンスの共有



- **2011年**：開発に着手
- **2013年**：日立製作所のIT系事業所で活用開始
- **2016年**：日立グループ内適用拡大
- **2023年**：OT系事業所などに適用拡大推進中

© Hitachi, Ltd. 2024. All rights reserved.

2-3 開発プロセスにおけるシステム・ツールの活用

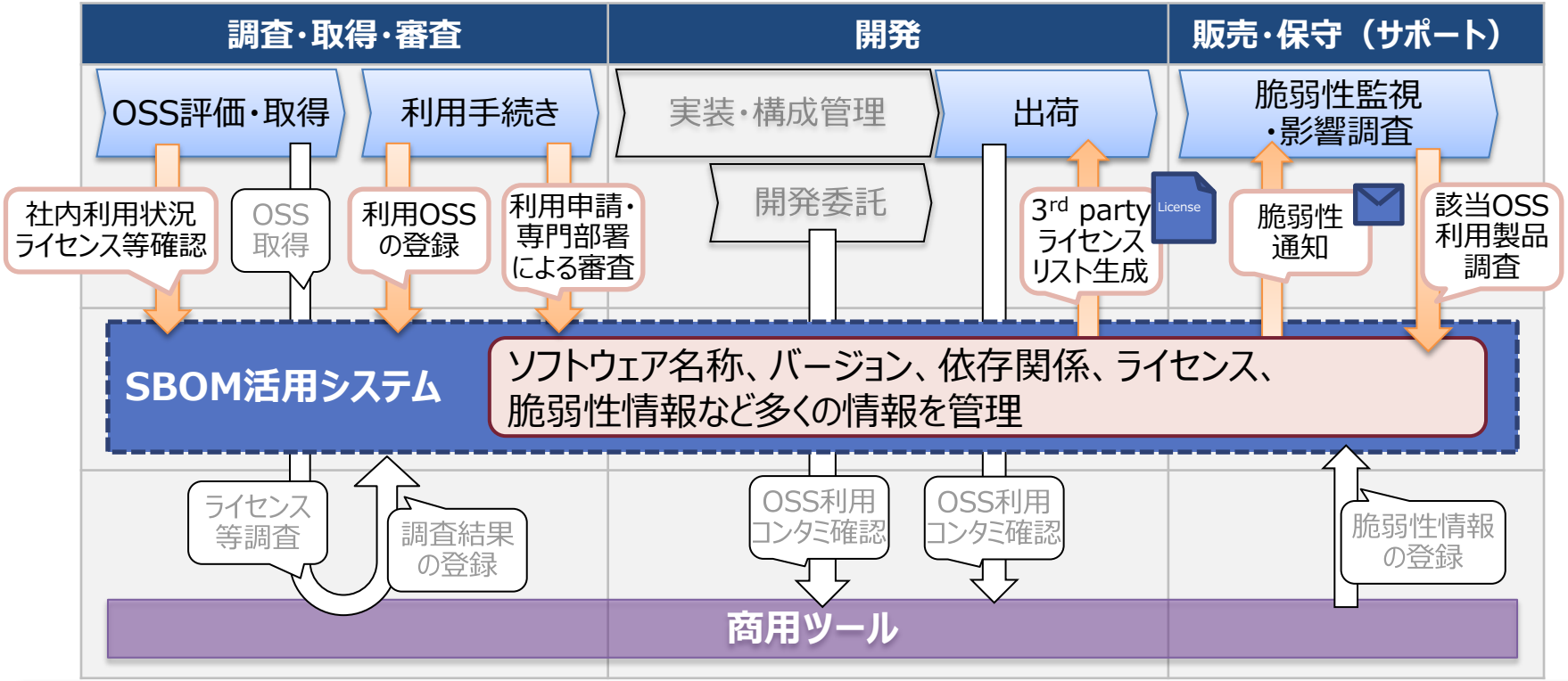


開発したシステム、および商用ツールを開発プロセスに組み込むことで改善を実施

© Hitachi, Ltd. 2024. All rights reserved.

2-3 開発プロセスにおけるシステム・ツールの活用（SBOM活用システム）

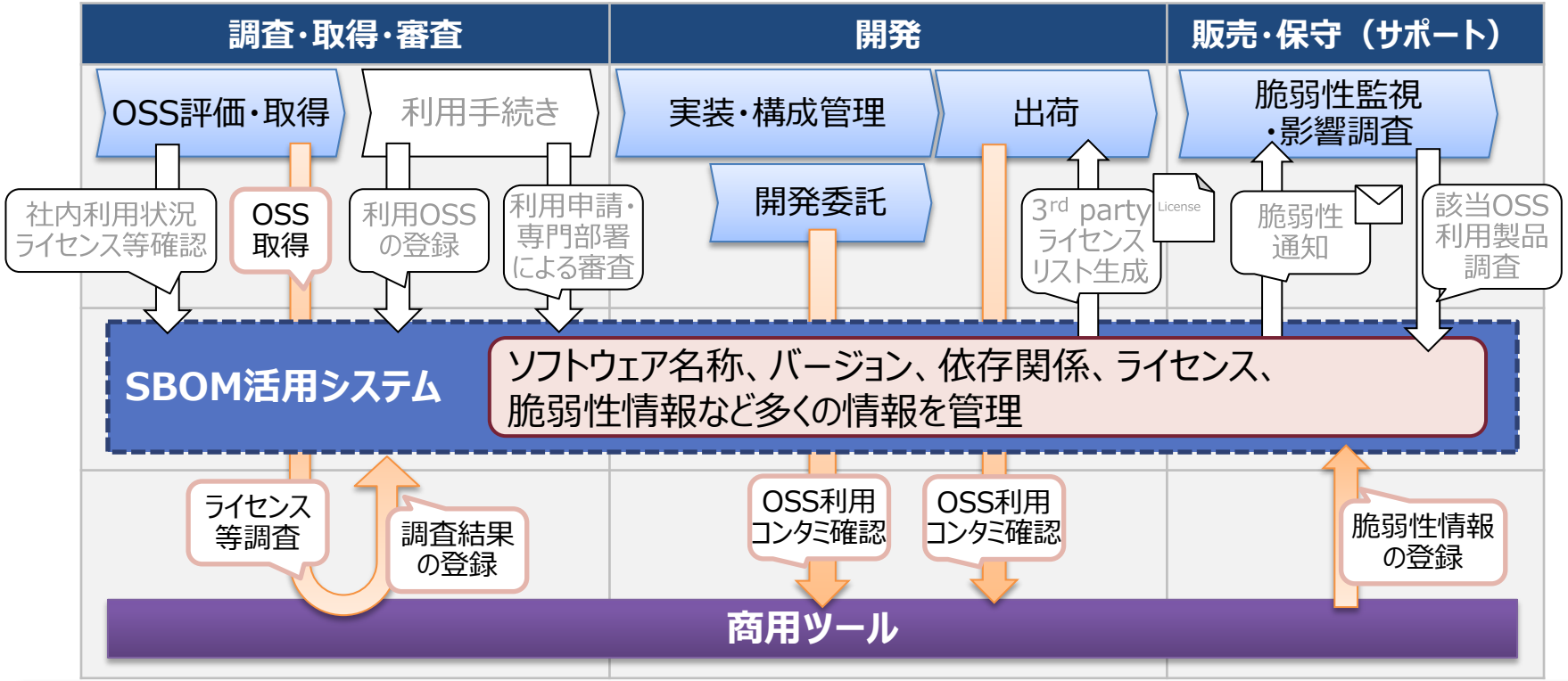
HITACHI
Inspire the Next



- 多くのOSS情報を一元管理し、効率的なライセンス・脆弱性調査などを実現
- 使用OSSのデータベース化やワークフロー機能により、トレーサビリティの確保や手続き面を効率化

© Hitachi, Ltd. 2024. All rights reserved.

2-3 開発プロセスにおけるシステム・ツールの活用（商用ツール）



- ライセンス調査や、開発委託品、およ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
- ツールによるライセンス調査結果や脆弱性情報はシステムに自動登録される仕組みの構築

© Hitachi, Ltd. 2024. All rights reserved.

3. 改善策実施の効果

© Hitachi, Ltd. 2024. All rights reserved.

3-1 改善策実施の効果

HITACHI
Inspire the Next

■ ライセンス調査工数の改善

利用者	DL専門部署	利用者	審査者・決裁者	利用者
SBOM活用システム・ツール適用前				
DL申請	セキュリティ審査・DL	ライセンスチェック取得申請	プロジェクト利用審査・決裁(会合)	利用開始
数日～数週間以上		数日～数週間以上	数週間～1ヵ月	
SBOM活用システム・ツール適用後				
システム・ツール経由のDL	不要	システム・ツールによるライセンス自動チェック	プロジェクト利用審査・決裁(WF)	利用開始
10分		～1時間	1日～数日	

- システムおよびツール適用前は、全件人手による調査を行い紙ベースで審査を実施
- 適用後は、システム蓄積情報＋ツール結果によりライセンス調査工数・取得、審査工数が改善

© Hitachi, Ltd. 2024. All rights reserved.

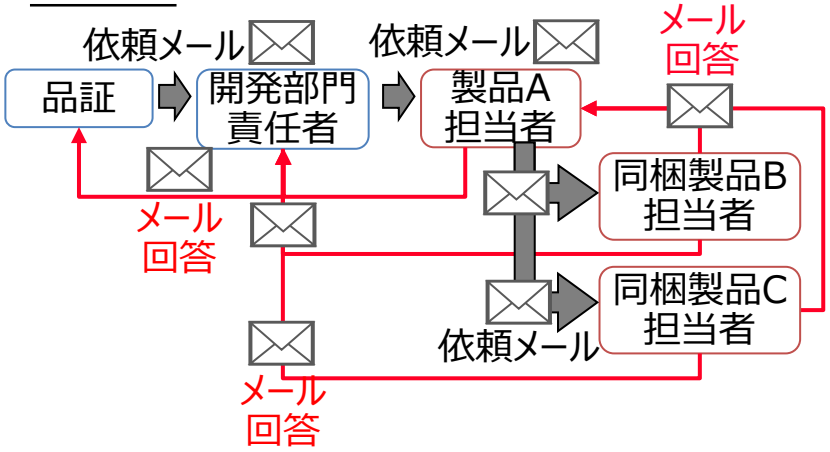
3-2 改善策実施の効果

HITACHI
Inspire the Next

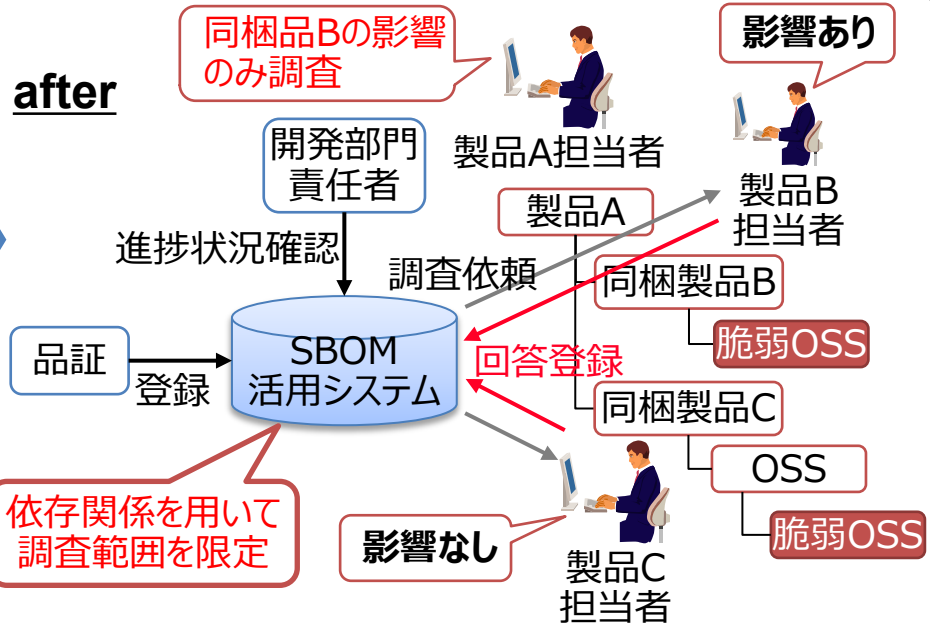
■ 脆弱性調査工数の改善

● 実際の脆弱性情報を用いて比較検証を実施

before



after



脆弱性のあるOSSを使用している製品が分からないため
組織全体にメールで調査依頼。影響製品の調査期間：16日

脆弱性のあるOSSを含んでいる製品の絞り込みは即時
影響製品の調査期間：1日

● システム適用後は脆弱性のあるOSSを含む製品の絞り込みが容易になり、影響範囲調査工数が改善

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

4. まとめ

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

ソフトウェア部品表(SBOM)活用システムの開発と適用

■ 開発プロセスに開発システムと商用ツールを適用することで課題を解決！

① 大量のOSSライセンス調査および脆弱性監視、影響調査に多大な工数を要する。

⇒ システムに蓄積したSBOM情報、およびツールを用いることで工数を削減

② 個々の製品・サービス開発プロジェクトにて①を行っており、重複作業が無駄となっている。
また、作業が属人化して正確性にバラつきがある。

⇒ 誰かが一度調査した情報をシステムにて共有することで重複作業の無駄を排除
処理の機械化や、ツールを用いることで作業の属人化を抑止

- 評価の結果、OSSを製品・システムに利用する際のライセンス・脆弱性調査の工数を大幅に削減できたことを確認。
- 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、これらのシステムおよびツール利用を拡大予定。

© Hitachi, Ltd. 2024. All rights reserved.

参考文献

[1] 経済産業省 商務情報政策局 サイバーセキュリティ課 (2022).
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
https://www.meti.go.jp/policy/netsecurity/wg1/ossjirei_20220801.pdf

[2] 経済産業省 商務情報政策局 サイバーセキュリティ課 (2024).
ソフトウェア管理に向けたSBOM（Software Bill of Materials）の導入に関する手引 ver2.0
https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf

© Hitachi, Ltd. 2024. All rights reserved.

他社商品名，商品などの引用に関する表示

- Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

© Hitachi, Ltd. 2024. All rights reserved.

HITACHI
Inspire the Next

END

ソフトウェア部品表（SBOM）活用システムによる
コンプライアンス・セキュリティの向上

2024/10/17

株式会社 日立製作所
マネージド＆プラットフォームサービス事業部
ソフトウェアエンジニアリングCoE OSSソリューションセンタ
金子 真也

© Hitachi, Ltd. 2024. All rights reserved.


Hitachi Social Innovation is
POWERING GOOD