

# MIRACLE Vul Hammer

## 製品紹介資料



# MIRACLE Vul Hammer とは



## SBOM を活用した脆弱性管理サービス ～コンポーネントと脆弱性を一元管理～

### 脆弱性管理工数の肥大化

脆弱性の手動管理による  
人的ミスや対応工数を削減したい

網羅的な  
脆弱性情報の  
収集

脆弱性を  
定期的に  
チェック

属人化

### 不透明なシステム管理

どこに何のソフトウェアが使われているか  
分からない

脆弱性内在  
ソフトウェア

ライセンス  
違反

ソフトウェア  
製作者不明

### 各種業界規制

SBOM を活用したリスク管理が必要

IMDRF

サイバー  
レジリエンス法

経産省  
SBOM導入の  
手引き

#### 特徴① 脆弱性管理を自動化

- ✓ 毎日自動でスキャン、検知時にメールで通知
- ✓ 工数を約 70 %削減 (※)

#### 特徴② 構成情報を可視化

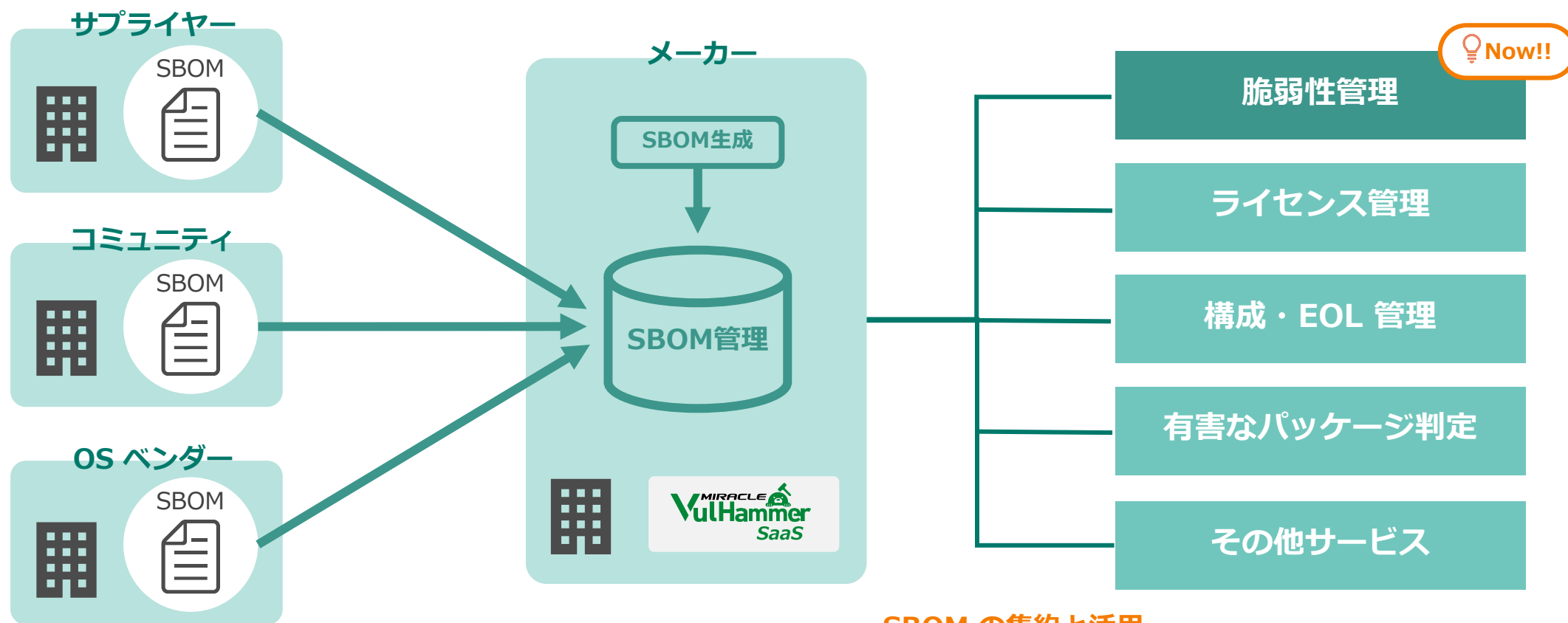
- ✓ ツールを用いた構成情報の収集と可視化
- ✓ 複数のシステムをグループで一元管理

#### 特徴③ 様々な SBOM を一元管理

- ✓ SBOM の生成と他社生成 SBOM も取込み可能
- ✓ CSV や JSON の構成情報も取込み、SBOM 化

※ 【参考】経産省ソフトウェア管理にむけた SBOM 導入に関する手引き

様々な SBOM を集約し、リスク管理に活用。今後も機能を拡張し、サービスを展開予定



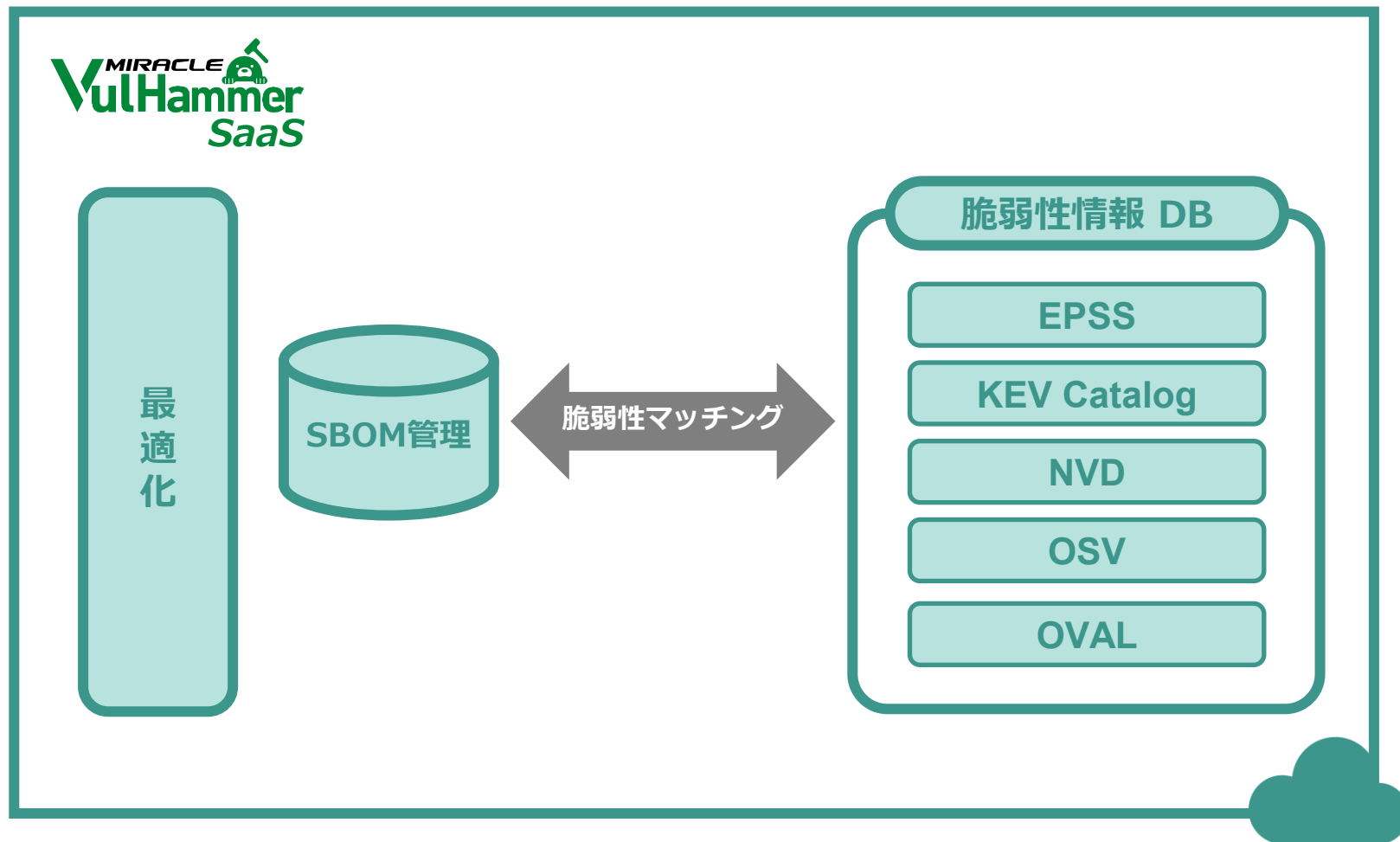
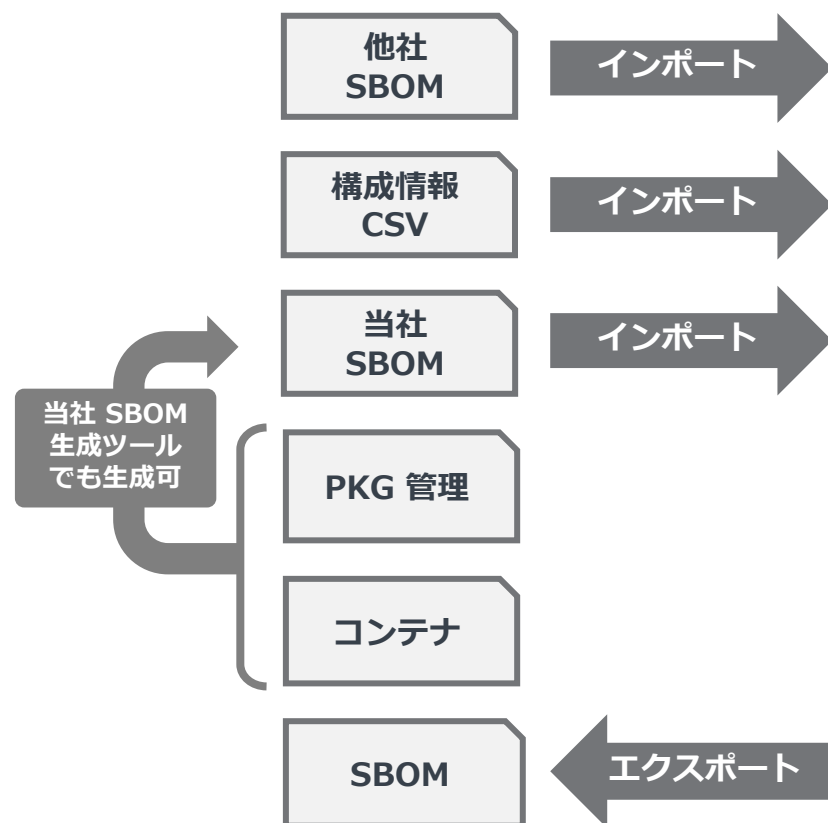
SBOM を生成

SBOM を集約

SBOM を活用

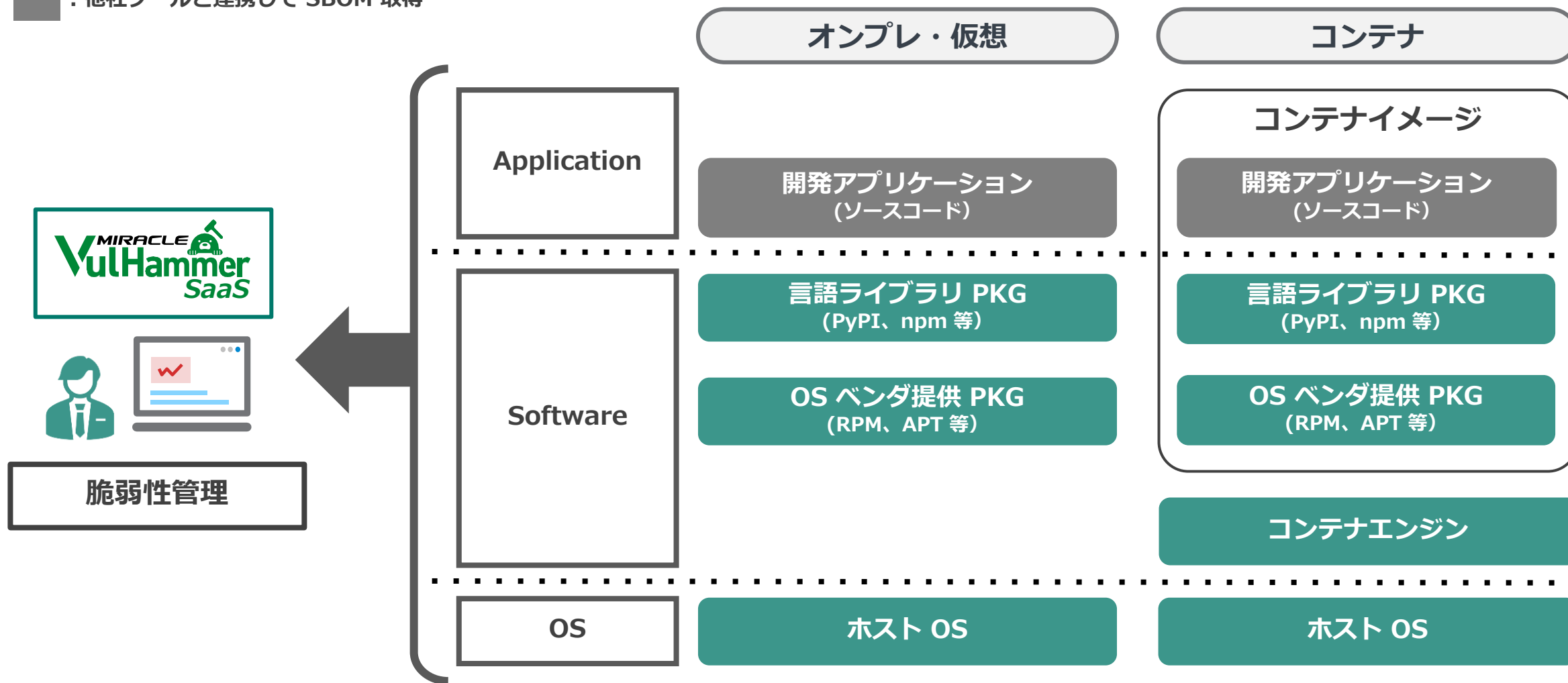
様々な構成情報を WEB 管理画面からインポートし、脆弱性を管理

運用に合わせて入力形式は選択可



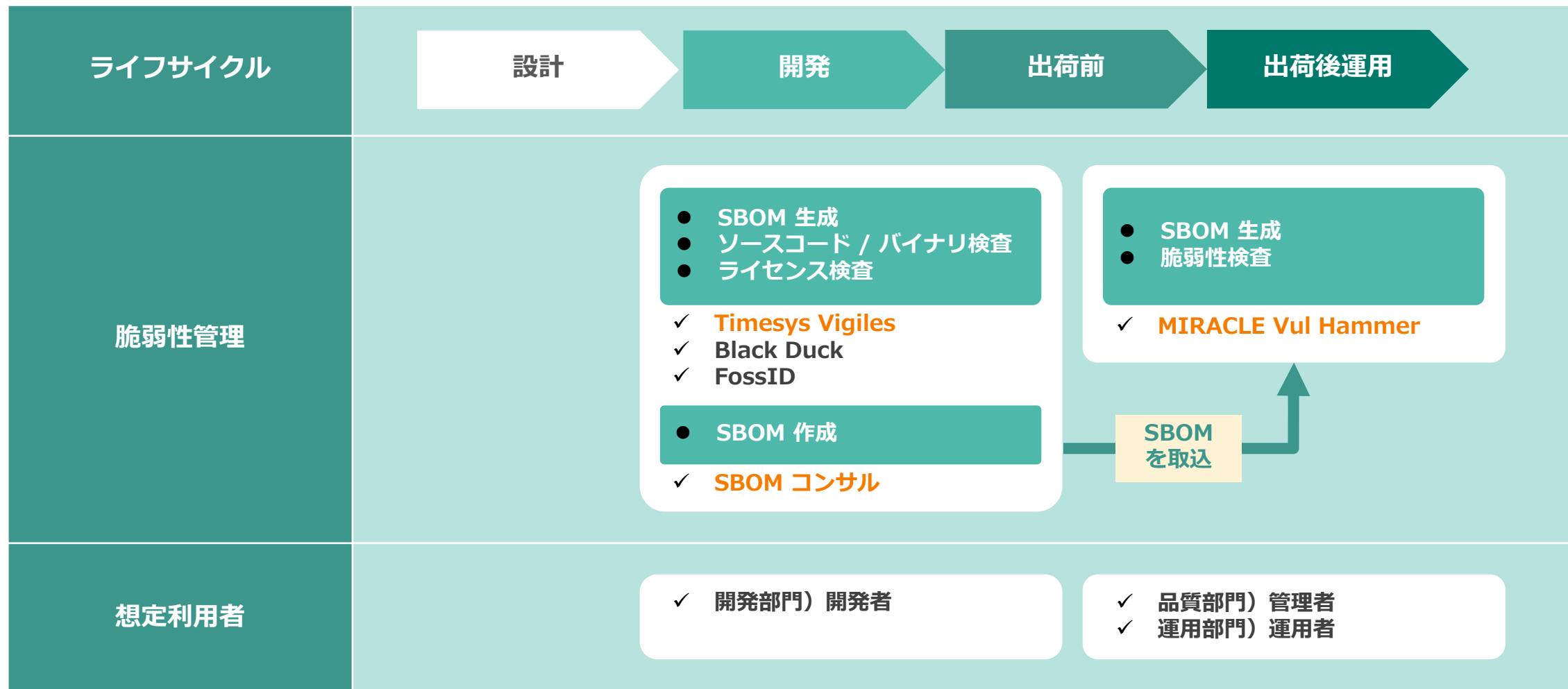
# 製品の強み①：幅広いレイヤーの脆弱性を管理

-  : 当社ツールで SBOM 生成可
-  : 他社ツールと連携して SBOM 取得



## 製品の強み②：様々なツールで生成した SBOM を活用

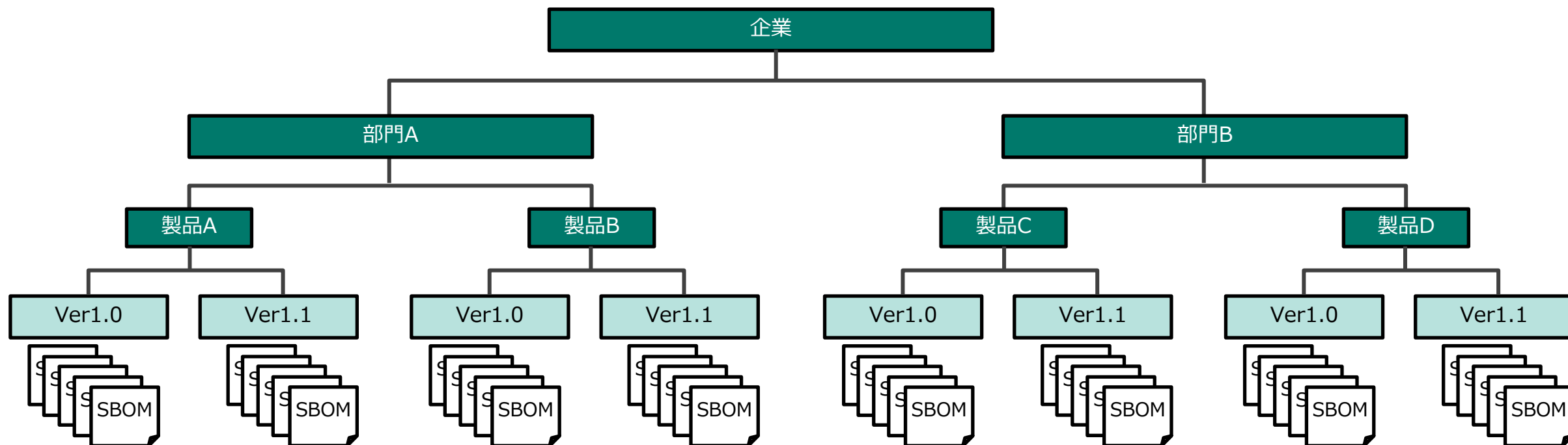
- 開発・出荷前工程：様々なツールやサービスで、ソースコードやライセンスを検査
- 運用工程：開発工程で生成した SBOM を活用し Vul Hammer を用いて脆弱性を管理



# 製品の強み③：システム群を一元的に把握・管理

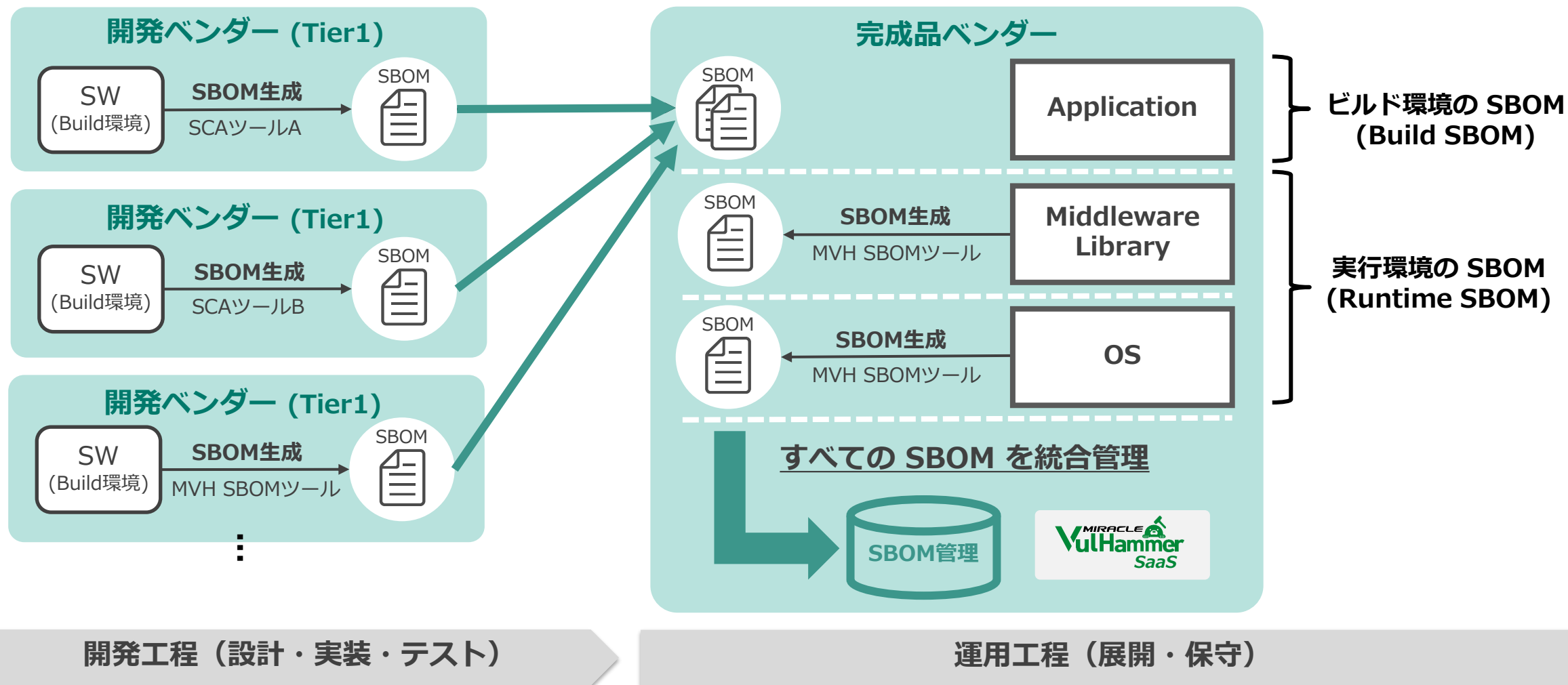
## 組織体系・製品群に応じて SBOM と脆弱性を階層的に管理

- グループ化・階層管理で組織体制に合わせた管理が可能
- 2025年10月のリリースバージョンでは、各階層毎にユーザー権限を付与可能



# 運用工程における統合的な SBOM 管理を支援

サプライチェーンにおいて開発ベンダーが生成した SBOM も運用フェーズで統合管理



# サポート範囲（OS・言語）

## SBOM ツールで SBOM 生成可能な OS と言語

### OS

| ディストリビューション              | サポートバージョン          |
|--------------------------|--------------------|
| MIRACLE LINUX            | 8 , 9              |
| AlmaLinux                | 8 , 9              |
| Debian                   | 12                 |
| Oracle Linux             | 8 , 9              |
| Red Hat Enterprise Linux | 8 , 9              |
| Rocky Linux              | 8 , 9              |
| Ubuntu                   | 20 , 22            |
| Windows Server           | 2016 , 2019 , 2022 |
| Windows                  | 10 , 11            |

### 言語ライブラリ

| 言語                    | パッケージマネージャ |
|-----------------------|------------|
| C#                    | NuGet      |
| Dart                  | Pub        |
| Erlang                | Erlang     |
| Go                    | Gomod      |
| Haskell               | Hackage    |
| Java                  | Maven      |
| Javascript/Typescript | Npm        |
| PHP                   | Packagist  |
| Python                | PyPI       |
| R                     | CRAN       |
| Ruby                  | RubyGems   |
| Rust                  | crates.io  |
| Swift                 | SwiftURL   |

# サポート範囲（脆弱性情報・SBOM）

## サポートする脆弱性情報と SBOM フォーマット

### 脆弱性情報

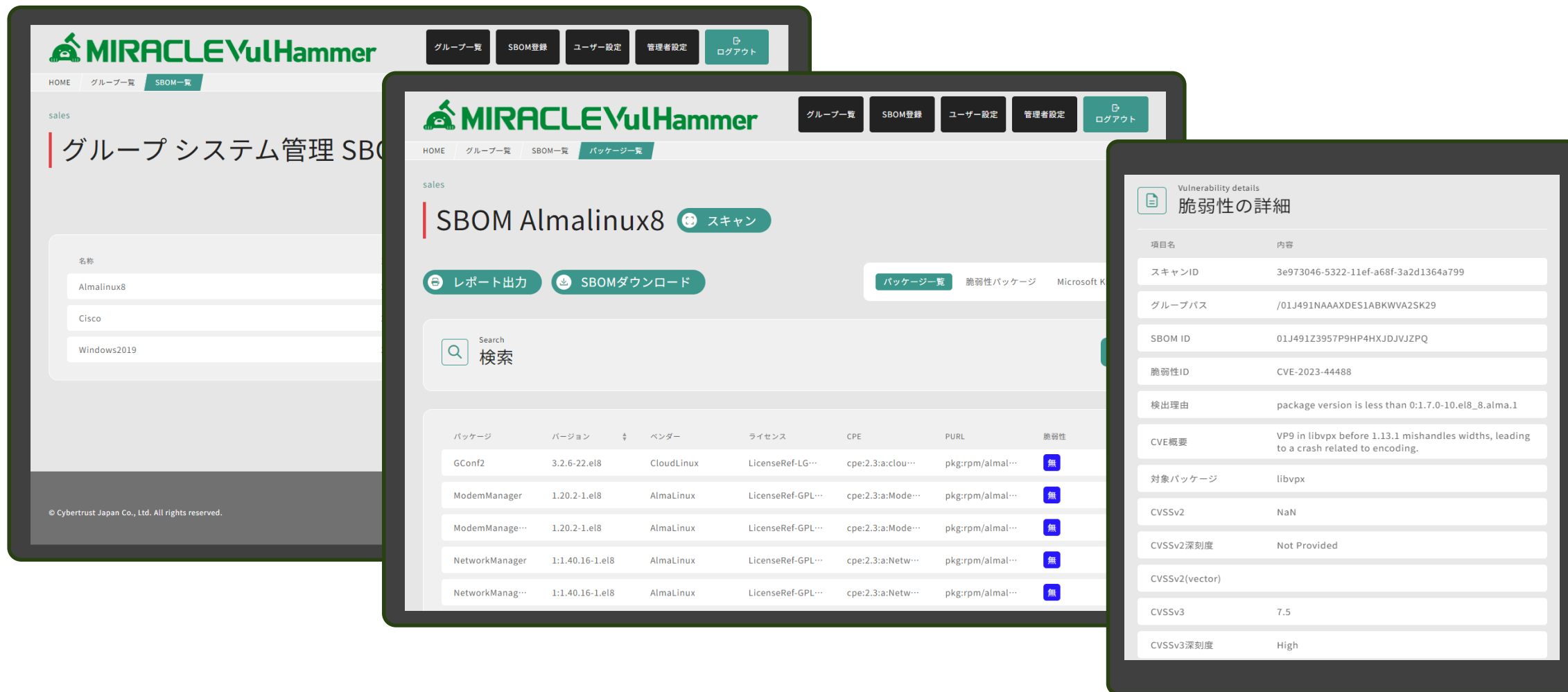
| 脆弱性情報       | 詳細                                                                                   |
|-------------|--------------------------------------------------------------------------------------|
| EPSS        | FIRST が公開する、今後30日以内に脆弱性が悪用される可能性を数値化した指標<br>EPSS : Exploit Prediction Scoring System |
| KEV Catalog | CISA が公開する、実際に悪用が確認された脆弱性を掲載したリスト<br>KEV : Known Exploited Vulnerabilities Catalog   |
| NVD         | NIST が公開する、脆弱性の深刻度を評価する汎用的な指標<br>NVD : National Vulnerability Database               |
| OSV         | Google が公開する脆弱性情報<br>OSV : Open Source Vulnerabilities                               |
| OVAL        | OS ベンダーが公開する脆弱性情報<br>OVAL : Open Vulnerability and Assessment Language               |

### SBOM フォーマット

| フォーマット    | サポートバージョン       |
|-----------|-----------------|
| CycloneDX | 1.4 , 1.5 , 1.6 |
| SPDX      | 2.3             |

# MIRACLE Vul Hammer の管理画面

管理画面は感覚的に利用できるシンプルな構成



The image displays three overlapping screenshots of the MIRACLE Vul Hammer management interface. The top-left screenshot shows the 'グループシステム管理 SBOM' page with a search bar and a list of systems. The top-right screenshot shows the 'SBOM Almalinux8' page with a 'スキャン' button and a table of packages. The bottom-right screenshot shows the '脆弱性の詳細' (Vulnerability details) page for CVE-2023-44488.

**SBOM Almalinux8**

| パッケージ           | バージョン           | ベンダー       | ライセンス             | CPE               | PURL             | 脆弱性 |
|-----------------|-----------------|------------|-------------------|-------------------|------------------|-----|
| GConf2          | 3.2.6-22.el8    | CloudLinux | LicenseRef-LG...  | cpe:2.3:a:clou... | pkg:rpm/almal... | 無   |
| ModemManager    | 1.20.2-1.el8    | AlmaLinux  | LicenseRef-GPL... | cpe:2.3:a:Mode... | pkg:rpm/almal... | 無   |
| ModemManage...  | 1.20.2-1.el8    | AlmaLinux  | LicenseRef-GPL... | cpe:2.3:a:Mode... | pkg:rpm/almal... | 無   |
| NetworkManager  | 1:1.40.16-1.el8 | AlmaLinux  | LicenseRef-GPL... | cpe:2.3:a:Netw... | pkg:rpm/almal... | 無   |
| NetworkManag... | 1:1.40.16-1.el8 | AlmaLinux  | LicenseRef-GPL... | cpe:2.3:a:Netw... | pkg:rpm/almal... | 無   |

**脆弱性の詳細**

| 項目名            | 内容                                                                                     |
|----------------|----------------------------------------------------------------------------------------|
| スキャンID         | 3e973046-5322-11ef-a68f-3a2d1364a799                                                   |
| グループパス         | /01J491NAAAXDES1ABKWVA2SK29                                                            |
| SBOM ID        | 01J491Z3957P9HP4HXJDJVVZPQ                                                             |
| 脆弱性ID          | CVE-2023-44488                                                                         |
| 検出理由           | package version is less than 0:1.7.0-10.el8_8.alma.1                                   |
| CVE概要          | VP9 in libvpx before 1.13.1 mishandles widths, leading to a crash related to encoding. |
| 対象パッケージ        | libvpx                                                                                 |
| CVSSv2         | NaN                                                                                    |
| CVSSv2深刻度      | Not Provided                                                                           |
| CVSSv2(vector) |                                                                                        |
| CVSSv3         | 7.5                                                                                    |
| CVSSv3深刻度      | High                                                                                   |

# MIRACLE Vul Hammer サービスロードマップ

サービスの  
継続提供

製品・サービスの機能拡充

- ✓ フィードバックの収集
- ✓ 機能追加・改善

ステージ ①

サービスの  
サポート対象拡充

提供価値の継続更新

- ✓ 法規制への対応強化
- ✓ サービス提供形態の拡充

ステージ ②

サプライチェーン全体の  
安全・安心を支える  
ソリューション提供

サプライチェーンの課題解決

- ✓ CTJ サービスを統合
- ✓ サービス⇒ソリューション

ステージ ③

# MIRACLE Vul Hammer の開発ロードマップ

## Ver1.3 (2025年5月リリース済)

- 脆弱性データベースの強化
  - EMLinuxの脆弱性データを追加
- SBOM管理機能の強化
  - SBOMの階層管理
  - SBOMの表記ゆれ対応(CPE/Purl未記載の場合の類推)



## Ver1.4 (2025年11月頃)

- 脆弱性トレーサビリティの向上
  - 脆弱性スキャン結果の状態管理（要対応、対応不要など）
  - 脆弱性スキャン結果の検索・フィルタ機能の強化
  - 脆弱性通知機能の強化
    - 通知時の条件設定機能の追加
- 組み込みOSの脆弱性データを追加
- SBOM管理機能の強化
  - SBOMのインポート機能の拡張（RDF/XML形式のインポート・エクスポート対応）

## Ver1.5 (2026年1月頃)

- SSVCベースとしたトリアーザ機能

## Ver1.6 (2026年4月頃)

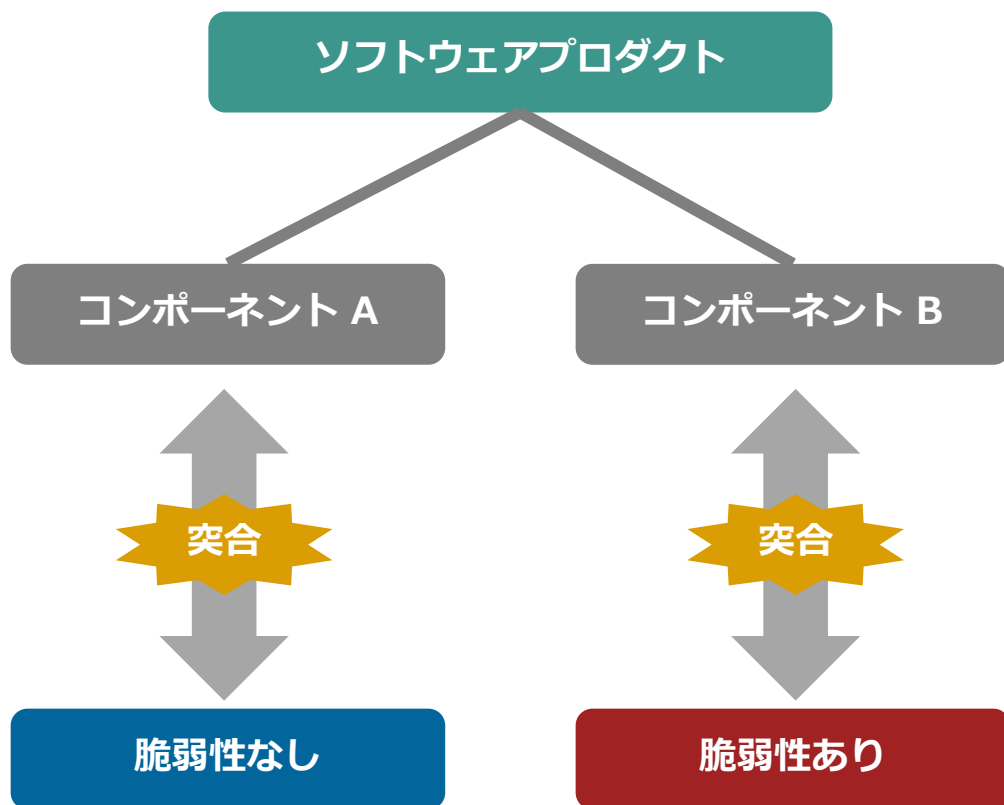
- 3rd Partyサービス連携
  - 3rd Partyのタスク管理機能との連携
  - 3rd Partyの構成管理機能との連携
- テナント毎の独自機能
  - テナント毎に脆弱性データの追加
  - テナント毎に重大インシデントのセキュリティリストの追加

※ 開発ロードマップは変更になる可能性があります

# APPENDIX

# SBOM (Software Bill of Materials) とは

製品やシステムがどのようなコンポーネントで構成されているかを機械処理を可能に一覧化したもの。  
ソフトウェアの「部品表」に相当し、ソフトウェアの透明性を高め、リスク管理を容易にするために活用。



| SBOM 最小要素     | イメージ (例)            |
|---------------|---------------------|
| サプライヤー名       | Cybertrust          |
| コンポーネント名      | Library A           |
| コンポーネントのバージョン | 1.0                 |
| そのたの一意の識別子    | CPE or PURL         |
| 依存関係          | Include             |
| SBOM 作成者      | Cybertrust          |
| タイムスタンプ       | 05-09-2022 13:00:00 |

| 脆弱性情報       | イメージ (例)      |
|-------------|---------------|
| CVE ID      | CVE-2025-0001 |
| 概要          | XXXX          |
| CVSS ベーススコア | 8.0           |

MIRACLE Vul Hammer のご契約者様には SBOM 生成ツールを別途提供

## ■ 使い方（Linux の例）

```
## SBOM 生成ツール（バイナリ）をサーバに配置
## SBOM 生成ツールはカスタマーポータルよりダウンロード（ファイル名は任意に変更可）
# mv ./linux-agent /usr/local/bin/
# chmod +x /usr/local/bin/linux-agent

## SBOM 生成
# linux-agent
```



出力



sbom.json

```
{"spdxVersion":"SPDX-2.3","dataLicense":"CC0-1.0","SPDXID":"SPDXRef-DOCUMENT","name":"Server01","documentNamespace":"..."}
```

※ 詳細はユーザーズガイドを参照

# CSV インポートについて

SBOM のほか、独自で作成した構成情報（CSV , JSON）のインポートが可能。

CSV や JSON ファイルに必要な各種パラメータについては以下に記載。

| 項目名              | 必須 | 概要                                                         |
|------------------|----|------------------------------------------------------------|
| os_name          | ●  | ホストにインストールされている OS の名称                                     |
| os_vendor        | ●  | [os_name] で示される OS の製造元                                    |
| os_version       |    | [os_name] で示される OS のバージョン                                  |
| os_buildid       |    | 将来の Windows 対応の拡張領域、現時点では使用不可（※）                           |
| pkg_name         | ●  | ホストにインストールされているソフトウェアの名称                                   |
| pkg_vendor       |    | [pkg_name] で示されるソフトウェアの製造元                                 |
| pkg_version      | ●  | [pkg_name] で示されるソフトウェアのバージョン                               |
| cpe              |    | [pkg_name] で示されるソフトウェアの CPE 情報                             |
| modularity_label |    | [pkg_name] で示されるソフトウェアが RPM モジュールストリームに属する場合のモジュールストリームの名称 |

※ Windows の構成情報（CSV）の取込みは不可。Windows では SBOM 生成ツールの利用が必須。



すべてのヒト、モノ、コトに 信頼を

## 留意事項

本資料に記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。

その他本資料に記載されているイラスト・ロゴ・写真・動画・ソフトウェア等は、当社または第三者が有する知的財産権やその他の権利により守られております。

お客様は、当社が著作権を有するコンテンツについて、特に定めた場合を除き、複製、改変、頒布などを行うことはできません。

本資料に記載されている情報は予告なしに変更されることがあります。また、時間の経過などにより記載内容が不正確となる場合がありますが、当社は、当該情報を更新する義務を負うものではありません。