



# 使用する前に

Black Duck SCA 2025.7.0

Copyright ©2025 by Black Duck.

All rights reserved.このドキュメントの使用はすべて、Black Duck Software, Inc.とライセンシー間のライセンス契約に従うものとします。本ドキュメントのいかなる部分も、Black Duck Software, Inc.の書面による許諾を受けることなく、どのような形態または手段によっても、複製・譲渡することが禁じられています。

Black Duck、Know Your Code、およびBlack Duckロゴは、米国およびその他の国におけるBlack Duck Software, Inc.の登録商標です。Black Duck Code Center、Black Duck Code Sight、Black Duck Hub、Black Duck Protex、Black Duck Suiteは、Black Duck Software, Inc.の商標です。他の商標および登録商標はすべてそれぞれの所有者が保有しています。

04-11-2025

# 目次

まえがき.....	4
Black Duck documentation.....	4
カスタマサポート.....	5
Black Duck コミュニティ.....	5
トレーニング.....	5
Black Duck 包括性と多様性に関する声明.....	6
Black Duck セキュリティへの取り組み.....	6
1. 概要 Black Duck.....	7
2. ログイン: Black Duck.....	9
3. コードのスキャン.....	11
4. 構成表(BOM)の表示.....	12

# まえがき

## Black Duck documentation

Black Duckのドキュメントは、オンラインヘルプと次のドキュメントで構成されています：

タイトル	ファイル	説明
リリースノート	release_notes.pdf	新機能と改善された機能、解決された問題、現在のリリースおよび以前のリリースの既知の問題に関する情報が記載されています。
Docker Swarmを使用したBlack Duckのインストール	install_swarm.pdf	Docker Swarmを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
Kubernetesを使用したBlack Duckのインストール	install_kubernetes.pdf	Kubernetesを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
OpenShiftを使用したBlack Duckのインストール	install_openshift.pdf	OpenShiftを使用したBlack Duckのインストールとアップグレードに関する情報が記載されています。
使用する前に	getting_started.pdf	初めて使用するユーザーにBlack Duckの使用法に関する情報を提供します。
スキャンベストプラクティス	scanning_best_practices.pdf	スキャンのベストプラクティスについて説明します。
SDKを使用する前に	getting_started_sdk.pdf	概要およびサンプルのユースケースが記載されています。
レポートデータベース	report_db.pdf	レポートデータベースの使用に関する情報が含まれています。
ユーザーガイド	user_guide.pdf	Black DuckのUI使用に関する情報が含まれています。

KubernetesまたはOpenShiftの環境にBlack Duckソフトウェアをインストールするには、Helmを使用します。次のリンクをクリックすると、マニュアルが表示されます。

- ・ [Helm](#)は、Black Duckのインストールに使用できるKubernetesのパッケージ マネージャです。Black Duck はHelm3をサポートしており、Kubernetesの最小バージョンは1.13です。

Black Duck 統合に関するドキュメントは、次のリンクから入手できます：

- ・ <https://sig-product-docs.blackduck.com/bundle/detect/page/integrations/integrations.html>
- ・ [https://documentation.blackduck.com/category/cicd\\_integrations](https://documentation.blackduck.com/category/cicd_integrations)

## カスタマサポート

ソフトウェアまたはマニュアルについて問題がある場合は、次の Black Duck カスタマー サポートに問い合わせてください。

- ・ オンライン: <https://community.blackduck.com/s/contactsupport>
- ・ サポート ケースを開くには、Black Duck コミュニティ サイト (<https://community.blackduck.com/s/contactsupport>) にログインしてください。
- ・ 常時対応している便利なリソースとして、[オンライン コミュニティ ポータル](#)を利用できます。

## Black Duck コミュニティ

Black Duck コミュニティは、カスタマー サポート、ソリューション、情報を提供する主要なオンライン リソースです。コミュニティでは、サポート ケースをすばやく簡単に開いて進捗状況を監視したり、重要な製品情報を確認したり、ナレッジベースを検索したり、他の Black Duck のお客様から情報を得ることができます。コミュニティセンターには、共同作業に関する次の機能があります。

- ・ つながる – サポートケースを開いて進行状況を監視するとともに、エンジニアリング担当や製品管理担当の支援が必要になる問題を監視します。
- ・ 学ぶ – 他の Black Duck 製品ユーザーの知見とベスト プラクティスを通じて、業界をリードするさまざまな企業から貴重な教訓を学ぶことができます。さらに、Customer Hubでは、Black Duckからの最新の製品ニュースやアップデートをいつでもご覧いただけます。これは、当社製品やサービスをより有効に活用し、オープン ソースの価値を組織内で最大限に高めることができます。
- ・ 解決する – Black Duck の専門家や Knowledgebase が提供する豊富なコンテンツや製品知識にアクセスして、探している回答をすばやく簡単に得ることができます。
- ・ 共有する – Black Duckのスタッフや他のお客様とのコラボレーションを通じて、クラウドソースソリューションに接続し、製品の方向性について考えを共有できます。

[Customer Successコミュニティにアクセスしましょう](#)。アカウントをお持ちでない場合や、システムへのアクセスに問題がある場合は、[こちら](#)をクリックして開始するか、[community.manager@blackduck.com](mailto:community.manager@blackduck.com) にメールを送信してください。

## トレーニング


Black Duck Customer Education は、Black Duck の教育ニーズをすべて満たすワンストップ リソースです。ここでは、オンライントレーニングコースやハウツービデオへの24時間365日のアクセスを利用できます。

新しいビデオやコースが毎月追加されます。

Black Duck Education では、次を行えます。

- ・ 自分のペースで学習する。
- ・ 希望する頻度でコースを復習する。
- ・ 試験を受けて自分のスキルをテストする。
- ・ 終了証明書を印刷して、成績を示す。

詳細については、<https://blackduck.skilljar.com/page/black-duck> を確認してください。また、Black Duck に関する

ヘルプについては、ヘルプ メニューの [Black Duck チュートリアル]()(Black Duck UIに表示)を選択してください。

## Black Duck 包括性と多様性に関する声明

Black Duck は、すべての従業員、お客様、パートナー様が歓迎されていると感じられる包括的な環境の構築に取り組んでいます。当社では、製品およびお客様向けのサポート資料から排他的な言葉を確認して削除しています。また、当社の取り組みには、設計および作業環境から偏見のある言葉を取り除く社内イニシアチブも含まれ、これはソフトウェアやIPに組み込まれている言葉も対象になっています。同時に、当社は、能力の異なるさまざまな人々が当社のWebコンテンツおよびソフトウェアアプリケーションを利用できるように取り組んでいます。なお、当社のIPは、排他的な言葉を削除するための現在検討中である業界標準仕様を実装しているため、当社のソフトウェアまたはドキュメントには、非包括的な言葉の例がまだ見つかる場合があります。

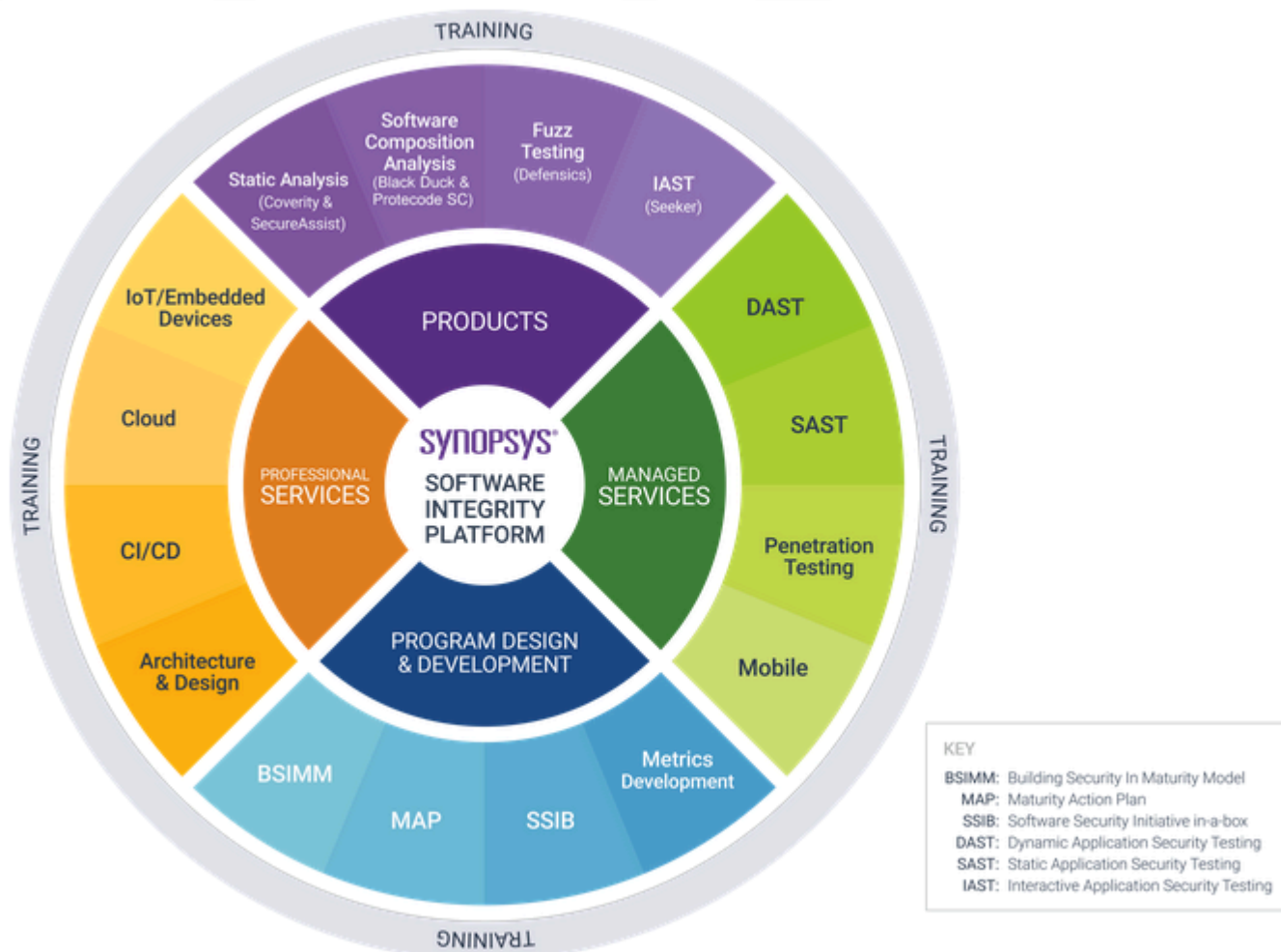
## Black Duck セキュリティへの取り組み

Black Duckは、お客様のアプリケーションの保護とセキュリティの確保に専念する組織として、お客様のデータ セキュリティとプライバシーにも同様に取り組んでいます。この声明は、Black Duckのお客様と将来のお客様に、当社のシステム、コンプライアンス認証、プロセス、その他のセキュリティ関連活動に関する最新情報をお届けすることを目的としています。

この声明は次の場所で入手できます。[セキュリティへの取り組み | Black Duck](#)

# 1. 概要 Black Duck

Black Duck は、お客様のセキュリティをサポートする包括的なサービスとツールのスイートを提供します。セキュリティを始めたばかりのお客様から、確立されたプログラムを強化するお客様まで、Black Duck は成功に必要な専門知識、スキル、製品を備えています。



## Black Duck SCAについて

Black Duck SCAはソフトウェア構成分析(SCA)ソリューションであり、組織はコードベース内のオープンソースコンポーネントを特定、追跡、管理できるようになります。自動ライセンスコンプライアンス、セキュリティの脆弱性検出、リスク評価が用意されているため、チームはソフトウェアのセキュリティと整合性を確保できるようになります。

## 主な機能

- ・ オープンソース管理: プロジェクトでオープンソースコンポーネントを特定して追跡します。
- ・ 脆弱性検出: National Vulnerability Database (NVD) と Black Duck Security Advisories (BD SA) を使用し、セキュリティの脆弱性を自動でスキャンします。

## 1. 概要 Black Duck

- ・ **ライセンスコンプライアンス**: オープンソースライセンスを分析し、企業ポリシーへのコンプライアンスを確保します。
- ・ **リスク評価とポリシー強制**: セキュリティ、法的、運用上の各リスクを軽減するポリシーを定義して強制します。
- ・ **ソフトウェア構成表 (SBOM) の生成**: SBOMを生成・管理し、ソフトウェアの依存関係に対する透明性を維持します。

### Black Duck SCAの仕組み

- ・ **コードのスキャン**: Black Duckスキャンツール (Detect、統合、またはAPI) を使用し、コードベースを分析します。
- ・ **コンポーネントの特定**: Black Duck では、コードの依存関係は、KnowledgeBase (KB) 内にある既知のオープンソースライブラリにマッピングされます。
- ・ **リスクの評価**: Black Duck では、セキュリティの脆弱性、ライセンスの問題、ポリシー違反がチェックされます。
- ・ **対処**: レポートを表示し、リスクに優先順位を付け、修正を適用し、コンプライアンスに準拠するSBOMを生成します。

### まず初めに

1. **アカウントの設定**: Black Duckインスタンスまたはクラウドホスト環境にログインします。
2. **最初のスキャンを実行**: サンプルプロジェクトを分析し、結果をレビューします。
3. **結果のレビュー**: UIの脆弱性、ライセンスリスク、ポリシー違反を確認します。

### Black Duck SCAを利用してみる

- ・ [Detectを使用するスキャンの実行方法](#)
- ・ [脆弱性レポートについて](#)
- ・ [ポリシー違反の管理](#)
- ・ [SBOMの生成](#)

### 次のステップ


Black Duckの基本に慣れたら、以下のコミュニティリソースを参考に、高度な機能と技術構成も利用してみましょう。

- ・ [インターフェイスの操作](#)
- ・ [スキャン結果の活用](#)
- ・ [Black Duckの技術仕様](#)
- ・ **詳細**: [ドキュメント](#)と[トレーニング](#)の各リソースをご覧ください。



## 2. ログイン: Black Duck


Black Duck SCAにアクセスするには、ブラウザからログインする必要があります。ログインすると、プロジェクトデータにアクセスできます(チームと組織に限定されている可能性のあるプロジェクトを含む)。

 注: 有効なログイン認証情報が必要になります。ユーザー名またはパスワードがない場合は、Black Duck管理者にお問い合わせください。

### ログインオプション

組織が認証を構成した方法により、以下を使用してログインできる場合があります。

- ・ ローカルBlack Duck認証情報: 管理者作成のユーザー名とパスワード。
- ・ LDAP認証情報: 組織のディレクトリサービスログイン(LDAPが有効になっている場合)。
- ・ SAMLベースのシングルサインオン(SSO): 自社のログインプロバイダーにリダイレクトされる場合があります(SAMLが構成されている場合)。

 注: 多要素認証(MFA)が有効になっていても、適用されるのはローカル認証情報でログインするユーザーのみです。SAMLまたはLDAPで認証するユーザーには、MFAは適用されません。

どの方法が適用されるかわからない場合は、管理者にガイダンスをお問い合わせください。

### ログイン手順

1. ブラウザを開き、システム管理者から提供されるBlack DuckのURLに移動します。通常、URLは以下の形式になります。

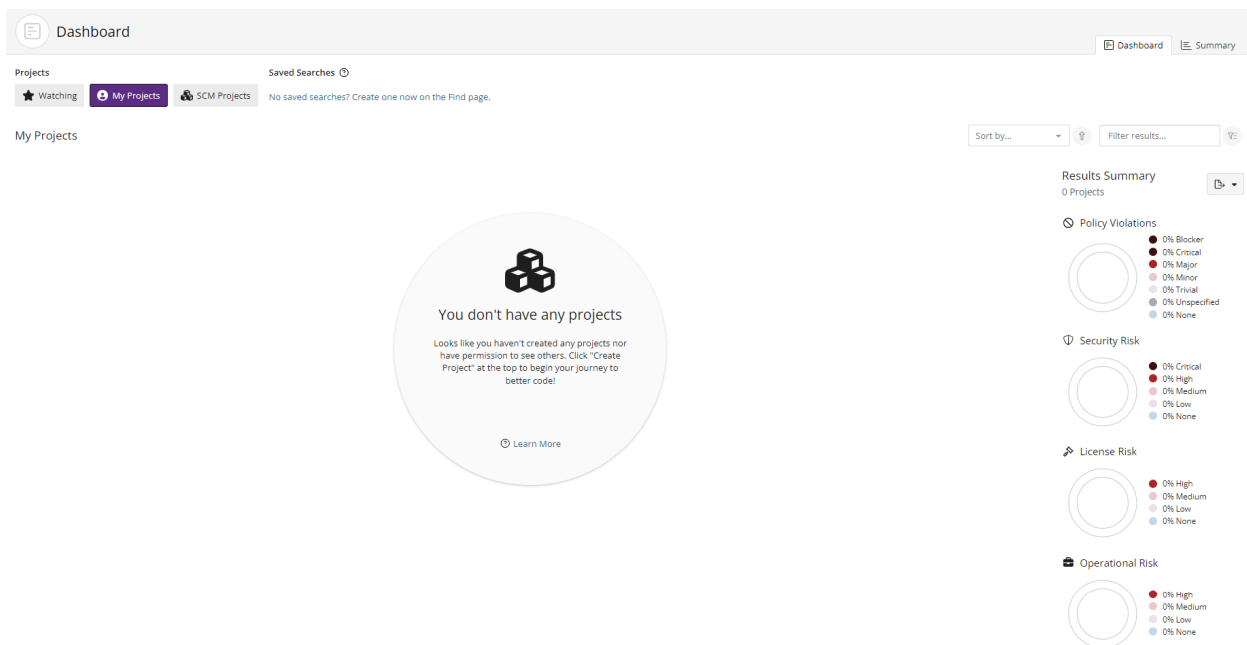
```
https://<your-black-duck-server-hostname>
```

2. ユーザー名とパスワードを入力します。
  - ・ パスワードでは大文字と小文字が区別されます。
  - ・ 初回ログインまたはパスワードがシステムのセキュリティ要件を満たしていない場合は、パスワードの変更を求められます。画面上のパスワードルールに従い、更新を完了します。
3. [ログイン]をクリックします。
4. インスタンスでMFAが有効になっている場合は、初回ログイン時に**構成する**ように求められます。
  - ・ QRコードが表示されます。
  - ・ サポート対象認証アプリ(Google Authenticatorなど)で、QRコードをスキャンします。
  - ・ アプリに表示される6桁のコードを入力し、セットアップを完了します。

### ログイン後

初回ログイン後は、空のダッシュボードにリダイレクトされます。

## 2. ログイン: Black Duck



ダッシュボードにデータを入力するには、**コードをスキャンしてプロジェクトバージョンにマッピング**する必要があります。これらの手順については、当ガイドの次のセクションで説明します。

デフォルトでは、ダッシュボードには以下が表示されます。

- ・ **マイプロジェクト**: 自分が作成した、または自分に割り当てられているプロジェクト。
- ・ **ウォッチ**: 監視するためにマークしたプロジェクトまたはコンポーネント。

また、目的の特定プロジェクト、バージョン、またはコンポーネントの検索設定を保存することで、**カスタムダッシュボード**の作成もできます。保存した検索設定はダッシュボードに表示されるため、すぐに利用できます。

## 3. コードのスキャン

スキャンは、Black Duckによってコードベース内にあるオープンソースコンポーネント、ライセンス、既知の脆弱性を識別する主な方法です。スキャンを実行すると、Black Duckによってプロジェクトファイルが分析されて包括的な構成表(BOM)が生成されるため、コンプライアンス、安全、最新情報を維持できるようになります。

Black Duckスキャンで行われること

Black Duck ではコードベースをスキャンし、以下を行います。


- ・ オープンソースコンポーネントとそのバージョンの特定
- ・ ソース(National Vulnerability Database(NVD)やBlack Duck Security Advisories(BDSA)など)を使用し、既知のセキュリティ脆弱性を検出
- ・ ライセンス上のリスクとコンプライアンスを評価
- ・ 監査・レポート作成用にBOMを生成
- ・ 組織のリスク許容度に基づき、カスタムポリシーを強制

Black Duckの統合方法に応じ、開発中、CI/CDパイプライン内、または手動でスキャンをトリガーさせることができます。

利用可能なスキャンツール

Black Duck では、さまざまな環境とワークフローに対応するさまざまなツールが用意されています。

- ・ **Black Duck Detect (CLI)**: 柔軟なコマンドラインツールで、ソースコード、バイナリ、コンテナをスキャンできます。ローカル開発やCI/CDパイプラインに統合できます。Black Duck Detectは、Black Duckに推奨されるスキャンツールです。
- ・ **シグネチャスキャナ (CLI)**: シグネチャベースのスキャンを実行するための専用コマンドラインツール。Detectが向いていない、またはスキャン構成を直接制御する必要がある環境に最適です。
- ・ **Black Duckプラグインの統合**: 以下のような人気のあるツールに事前構築されている統合です。
  - ・ Jenkins
  - ・ Azure DevOps
  - ・ GitHub Actions
  - ・ Bitbucket Pipelines
- ・ **SCAスキャンサービス (SCASS)**: ソース、バイナリ、コンテナ分析用のスケーラブルなクラウドベースのスキャンサービス。適切なライセンスを持つお客様が利用できます。
- ・ **REST API**: 上級ユーザーはBlack Duck APIを使用すると、スキャンのアップロード、結果の取得、プロジェクトデータの管理を自動化できます。

 **注**: 一部の機能では、特定のライセンスや構成が必要になる場合があります。ご自身の環境で利用できるスキャンツールがわからない場合は、管理者にお問い合わせください。

## 4. 構成表(BOM)の表示

コードベースをスキャンしてプロジェクトバージョンに結果をマッピングすると、Black Duckによって構成表(BOM)が自動で生成されます。BOMには、該当するプロジェクトバージョンで検出されたすべてのオープンソースコンポーネントが、関連データ(ライセンス、脆弱性、ポリシーステータスなど)と併せて一覧表示されます。

ソフトウェアに何があるか、リスクやコンプライアンスの問題に対処する必要があるかどうかを把握するうえで、BOMは一元的なビューの役目を果たします。

### BOMの表示方法

1. Black Duckにログインします。
2. [ダッシュボード]で、[ウォッチ]または[マイプロジェクト]タブのいずれかを使用してプロジェクトを選択します。
3. プロジェクトページで、表示するバージョンを選択します。これで、BOMが表示されている[コンポーネント]タブにリダイレクトされます。

Black Duck Project Groups  
Sample Project ▶ 1.0.0

Project ★ Phase: In Development Scans: Up to Date Status: Up to Date Last Updated: 10:21 AM

Components Security Source Reports Details Legal Settings

Security Risk  
Number of Components

Critical	4
High	3
Medium	4
Low	0
None	17

License Risk  
Number of Components

High	6
Medium	2
Low	0
None	20

Operational Risk  
Number of Components

High	24
Medium	3
Low	0
None	1

Snippets  
78 Unconfirmed

Unmatched Components  
1 Unmatched

Print Add Bulk Actions Compare to...

Ignore Not Ignored Snippet Match Status Confirmed Match Ignore Not Ignored + Filter

Filter Components...

Component	Source	Match Type	Match Score	Usage	License	Security Risk	Operational Risk
AOP Alliance (Java/J2EE AOP standard) 1.0	1 Match	Transitive Dependency	100%	Dynamically Linked	Public Domain		High
Apache Commons DBCP 1.2.2	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0		High
Apache Commons FileUpload 1.3.3	1 Match	Direct Dependency	100%	Dynamically Linked	Apache-2.0	1	High
Apache Commons IO 2.2	1 Match	Transitive Dependency	100%	Dynamically Linked	Apache-2.0	1	High

### BOMビューについて

- ・ BOMには、選択されているプロジェクトバージョンのオープンソースコンポーネントがすべて表示されます。
- ・ デフォルトではフラットビューで表示されるため、コードベースに導入された方法に関係なく、単一のリストにすべてのコンポーネントが表示されます。
- ・ 各コンポーネントエントリには重要な詳細(コンポーネントの名前とバージョン、マッチタイプ、ライセンス、セキュリティと運用上のリスクなど)が含まれています。これらのコンポーネントの特性に関する詳細については、[こちら](#)をご覧ください。

BOM内で並び替え、フィルタ、検索を行うと、リスクの高いコンポーネントやポリシーに違反しているコンポーネントに焦点を当てることができます。

### BOMを利用する

- ・ コンポーネントをクリックすると、以下を含むより詳細な情報が記載されているスライドアウトパネルが開きます。
  - ・ 脆弱性

- ・ ライセンス
- ・ 取得元ID (例:PURL、CPE)
- ・ その他の詳細 (説明や承認ステータスなど)
- ・ 適切な権限がある場合は、BOMから[ポリシー上書き](#)や[修正](#)アクションを直接適用できます。
- ・ サポート対象形式 (SPDXやCycloneDXなど)を使用することで、[システムBOMレポートを生成](#)できます。

さらに利用する

- ・ BOMの詳しい利用方法については、[Black Duckドキュメント](#)のプロジェクトバージョンBOMを参照してください。
- ・ 脆弱性の解釈方法については、[セキュリティリスクを管理](#)を参照してください。
- ・ ポリシーの設定については、[ポリシーを管理](#)を参照してください。