



リリースノート
バージョン2019.8.0

このエディションの『リリースノート』は、バージョンBlack Duckの2019.8.0を対象としています。

本ドキュメントは2019年10月2日に作成または更新されました。

コメントおよび提案については、次の宛先までお送りください。

Synopsys
800 District Avenue, Suite 201
Burlington, MA 01803-5061 USA

Copyright © 2019 by Synopsys.

All rights reserved. 本ドキュメントの使用はすべて、Black Duck Software, Inc. とライセンス所有者の間の使用許諾契約に準拠します。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、複製または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、および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。

章 1: 製品発表	1
バージョン2019. 8. 0の発表	1
バージョン2019. 8. 0のアップグレードの発表	1
バージョン2019. 4. 0の発表	1
KubernetesとOpenShiftでのBlack Duckインストールプロセス	1
外部データベースでサポートされるPostgreSQLの導入	1
バージョン2019. 2. 0の発表	2
Black Duckホストされるお客様のアクセスのセキュリティ保護	2
Docker Composeサポートの廃止	2
バージョン2018. 12. 0のアップグレードの発表	2
バージョン2018. 11. 0での発表	2
バージョン5. 0. 0での発表	2
dependencyScanオプション	2
章 2: リリース情報	3
バージョン2019. 8. 0	3
バージョン2019. 8. 0の新機能および変更された機能	3
2019. 8. 0で修正された問題	5
バージョン2019. 6. 2	7
バージョン2019. 6. 2の新機能および変更された機能	7
2019. 6. 2で修正された問題	7
バージョン2019. 6. 1	7
バージョン2019. 6. 1の新機能および変更された機能	7
2019. 6. 1で修正された問題	7
バージョン2019. 6. 0	8
バージョン2019. 6. 0の新機能および変更された機能	8
2019. 6. 0で修正された問題	11
バージョン2019. 4. 3	13
バージョン2019. 4. 3の新機能および変更された機能	13
2019. 4. 3で修正された問題	13
バージョン2019. 4. 2	13
バージョン2019. 4. 2の新機能および変更された機能	13
2019. 4. 2で修正された問題	14
バージョン2019. 4. 1	14

バージョン2019. 4. 1の新機能および変更された機能	14
2019. 4. 1で修正された問題	14
バージョン2019. 4. 0	15
バージョン2019. 4. 0の新機能および変更された機能	15
2019. 4. 0で修正された問題	17
バージョン2019. 2. 2	18
バージョン2019. 2. 2の新機能および変更された機能	18
2019. 2. 2で修正された問題	18
バージョン2019. 2. 1	18
バージョン2019. 2. 1の新機能および変更された機能	18
2019. 2. 1で修正された問題	18
バージョン2019. 2. 0	18
バージョン2019. 2. 0の新機能および変更された機能	18
2019. 2. 0で修正された問題	19
バージョン2018. 12. 4	20
バージョン2018. 12. 4の新機能および変更された機能	20
2018. 12. 4で修正された問題	20
バージョン2018. 12. 3	20
バージョン2018. 12. 3の新機能および変更された機能	20
2018. 12. 3で修正された問題	21
バージョン2018. 12. 2	21
バージョン2018. 12. 2の新機能および変更された機能	21
2018. 12. 2で修正された問題	21
バージョン2018. 12. 1	21
バージョン2018. 12. 1の新機能および変更された機能	21
2018. 12. 1で修正された問題	21
バージョン2018. 12. 0	22
バージョン2018. 12. 0の新機能および変更された機能	22
2018. 12. 0で修正された問題	25
バージョン2018. 11. 1	25
バージョン2018. 11. 1の新機能および変更された機能	25
2018. 11. 1で修正された問題	25
バージョン2018. 11. 0	25
バージョン2018. 11. 0の新機能および変更された機能	25
バージョン2018. 11. 0で修正された問題	27
バージョン5. 0. 2	28
バージョン5. 0. 2の新機能および変更された機能	28
バージョン5. 0. 2で修正された問題	28
バージョン5. 0. 1	28
バージョン5. 0. 1の新機能および変更された機能	28
バージョン5. 0. 1で修正された問題	28

バージョン5.0.0	28
バージョン5.0.0の新機能および変更された機能	28
5.0.0で修正された問題	31
バージョン4.8.3	32
バージョン4.8.3の新機能および変更された機能	32
バージョン4.8.2	32
バージョン4.8.2の新機能および変更された機能	32
バージョン4.8.2で修正された問題	32
バージョン4.8.1	32
バージョン4.8.1の新機能および変更された機能	32
バージョン4.8.0	32
バージョン4.8.0の新機能および変更された機能	32
バージョン4.8.0で修正された問題	33
バージョン4.7.2	34
バージョン4.7.2の新機能および変更された機能	34
バージョン4.7.1	34
バージョン4.7.1の新機能および変更された機能	34
バージョン4.7.1で修正された問題	34
バージョン4.7.0	35
バージョン4.7.0の新機能および変更された機能	35
バージョン4.7.0で修正された問題	36
章 3: 既知の問題と制限事項	38

Black Duck ドキュメント

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 Composeを使用したBlack Duckのインストール	install_compose.pdf	Docker Compose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。
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。

タイトル	ファイル	説明
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。

Black Duck統合のドキュメントは、[Confluence](#)にあります。

カスタマサポート

ソフトウェアまたはドキュメントについて問題がある場合は、Synopsysカスタマサポートに問い合わせてください。

Synopsysサポートには、複数の方法で問い合わせできます。

- オンライン：<https://www.synopsys.com/software-integrity/support.html>
- 電子メール：software-integrity-support@synopsys.com
- 電話：お住まいの地域の電話番号については、[サポートページ](#)の下段にあるお問い合わせのセクションを参照してください。

常時対応している便利なリソースとして、[オンラインカスタマポータル](#)を利用できます。

Synopsys Software Integrityコミュニティ

Synopsys Software Integrityコミュニティは、カスタマサポート、ソリューション、および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Software Integrityグループ (SIG) 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SIG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、最新の製品ニュースやSynopsysの最新情報をすべて指先の操作で確認できます。これは、オープンソースの価値を組織内で最大限に高めるように当社の製品やサービスをより上手に活用するのに役立ちます。
- 解決する - SIGの専門家やナレッジベース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 - Software Integrityグループ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@synopsys.comにメールを送信してください。

トレーニング

Synopsys Software Integrity, Customer Education (SIG Edu) は、すべてのBlack Duck教育ニーズに対応する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。

Synopsys Software Integrity, Customer Education (SIG Edu) では、次のことができます。

- 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://community.synopsys.com/s/education>を参照してください。

バージョン2019. 8. 0の発表

バージョン2019. 8. 0のアップグレードの発表

2019. 8. 0より前のバージョンからアップグレードする場合、2つのジョブ VulnerabilityRepriorizationJobおよびthe VulnerabilitySummaryFetchJobがスタートアップ時に実行され、脆弱性データが同期されます。

これらのジョブの実行には時間がかかる場合があります、既存の構成表の全体的な脆弱性スコアは、これらのジョブが完了するまで使用できません。役割「システム管理者」を持つユーザーは、Black Duckジョブページを使用してこれらのジョブを監視できます。

バージョン2019. 4. 0の発表

KubernetesとOpenShiftでのBlack Duckインストールプロセス

2019. 4. 0 Black Duck リリース以降、KubernetesまたはOpenShiftにBlack Duckをインストールする場合に唯一のサポート機能はSynopsys Operatorです。

Synopsys Operatorは、KubernetesおよびOpenShiftクラスターでSynopsysソフトウェアの導入と管理を支援する、クラウドネイティブの管理ユーティリティです。Synopsys Operatorをインストールした後、それを活用してSynopsysソフトウェアを簡単に展開および管理することができます。

- [ここ](#)をクリックして、Kubernetes/OpenShift用Black Duckの概要を確認してください。
- Synopsys Operatorの概要については、[ここ](#)をクリックしてください。
- Synopsys Operatorのインストールおよび使用方法については、[ここ](#)をクリックしてください。

KubernetesまたはOpenShiftを使用し、Synopsys Operator以外のインストール方法を使用している場合は、Synopsysカスタマーサポートに連絡して移行のサポートを受けてください。Synopsys Operatorへの移行は非常に簡単ですが、Synopsys Operatorへの移行を追加支援するサポートチームもご利用いただけます。

外部データベースでサポートされるPostgreSQLの導入

Black Duckサポート:

- Amazon Relational Database Service (RDS) 経由のPostgreSQL 9.6.x
- Google Cloud SQL経由のPostgreSQL 9.6.x
- PostgreSQL 9.6.x (Community Edition)

パフォーマンス関連の修正を含んでいるため、Synopsysは、バージョン9.6.12へのアップグレードを推奨しています。

バージョン2019.2.0の発表

Black Duckホストされるお客様のアクセスのセキュリティ保護

ホストされるすべてのお客様は、SAMLまたはLDAPを介したシングルサインオン（SSO）の既成サポートを活用して、Black Duckアプリケーションへのアクセスのセキュリティを確保する必要があります。これらのセキュリティ機能を有効にして設定する方法については、インストールガイドを参照してください。さらに、2ファクタ認証を提供しているSAML SSOプロバイダを使用しているお客様は、そのテクノロジーを有効にして活用し、Black Duckアプリケーションへのアクセスのセキュリティをさらに高めることをお勧めします。

Docker Composeサポートの廃止

Synopsysは、Black Duck 2019.2.0リリース以降、Docker Composeのサポートを廃止します。Docker Composeは2019年12月31日までサポートされます。

バージョン2018.12.0のアップグレードの発表

2018.12.0よりも前のバージョンからアップグレードする場合、このリリースの新機能をサポートするためにデータ移行が必要になるため、通常よりも長いアップグレード時間がかかります。アップグレード時間はBlack Duckデータベースのサイズによって異なります。アップグレードプロセスを監視したい場合は、Synopsysのカスタマサポートまでお問い合わせください。

バージョン2018.11.0での発表

他のSynopsys製品との相乗効果がより反映されるように、Black Duckのリリースバージョンが変更されました。リリース番号は、YYYY.MM. 値になります。任意の月にリリースされる最初のバージョンの値は0になります。このため、今回のリリースのリリースバージョンは2018.11.0になります。

バージョン5.0.0での発表

dependencyScanオプション

コマンドライン出力とドキュメントで説明されているように、署名スキャナの--dependencyScanオプションは廃止されました。Black Duck Softwareは、宣言された依存関係を検出するためにSynopsys Detectを使用することをお勧めします。

Black Duckの次のメジャーリリースでは、--dependencyScanオプションは削除されます。

詳細については、Customer Successマネージャにお問い合わせください。

バージョン2019. 8. 0

バージョン2019. 8. 0の新機能および変更された機能

セキュリティの強化

- Black Duck UIに、脆弱性とそれに関連するリスクレベルの総合スコアが表示されるようになりました。[セキュリティダッシュボード]、[コンポーネント名バージョン]ページの[セキュリティ]タブ、Black Duck KB [コンポーネント名バージョン]の[セキュリティ]タブに、[総合スコア]列が表示され、一時スコア（BDSAの場合）またはベーススコア（NVDの場合）が表示されるようになりました。総合スコアの値にカーソルを合わせると、個々の値が表示されます。
 - BDSAの場合、一時スコア、ベーススコア、可能性のスコア、影響スコアが表示されます。
 - NVDの場合、ベーススコア、可能性のスコア、影響スコアが表示されます。

関心のある脆弱性をすばやく見つけるために、新しいフィルタ「X以上の総合スコア」が「コンポーネント名バージョン」の[セキュリティ]タブに追加されました。

- 脆弱性スコアに基づいてポリシールールを作成し、最も重大な脆弱性を特定できるように、新しいポリシー条件である[最高脆弱性スコア]も追加されました。

追加のコンポーネントに関する使用法

このリリースでは、Black Duckに次の使用法が追加されました。

- **単純集合**。プロジェクトでコンポーネントが使用されていません。同じメディアに含まれる場合がありますが、関連付けられていません。コンポーネントは共存しますが、どのような方法でも相互に依存しません。たとえば、関連付けられていない製品のサンプル版を配布に含めている場合や、
- **前提条件**。この使用法は、必要ですが配布で提供されないコンポーネントを対象としています。

コンポーネント管理の拡張機能

コンポーネント管理でコンポーネントのバージョンを管理しやすくするために、新しい[コンポーネントバージョン]タブがあります。

監査情報の機能強化

プロジェクトおよびプロジェクトバージョンの監査情報が拡張され、元のライセンス（元のライセンスが変更された場合）、再スキャン、ライセンス条項の履行に関する情報が含まれるようになりました。

クローン作成の機能強化

[コンポーネントの編集]オプションに、確認済みのスニペット調整のクローン作成、ポリシー違反の上書

き、関連するコメントが含まれるように、クローン作成機能が強化されました。

ユーザー認証情報を保存するためのセキュリティの強化

ユーザー認証情報は、random-salt SHA256を使用して、Black Duckデータベースに保存されるようになりました。

コンポーネントカスタムフィールドプロジェクトバージョンレポート

プロジェクトバージョンレポートが拡張され、新しいオプションが追加されました。**コンポーネント追加フィールド**。このオプションを選択すると、`component_date_#.csv`レポートと同じ情報を含む新しいレポート**bom_component_custom_fields_date_#.csv**が作成されますが、このプロジェクトバージョンの構成表コンポーネント、コンポーネント、コンポーネントバージョンのカスタムフィールドドラベルと値も含まれます。

プロジェクトバージョンカスタムフィールド.csvレポートのオプションは、**プロジェクトバージョンの追加フィールド**に改名されました。

スニペットのスキンの機能拡張

スキンのパフォーマンスと結果を向上させるために、スニペットスキンの実行を選択した場合、スニペットスキンは、スニペットのファイルの内容を確認する前に、ファイルレベルのマッチに対してマッチしなかったファイル候補かどうかを最初に確認します。ファイルレベルのマッチが検出された場合は、その結果セットから候補が生成されます。ファイルレベルのマッチが検出されない場合は、ファイルコンテンツ全体をスキャンする通常のスニペットスキンの実行が実行されます。スニペットマッチ機能に大きく依存し、変更されていないOSSファイルを多数使用するお客様は、スキャンパフォーマンスが大幅に向上するだけでなく、マッチングの結果が向上する可能性があります。さらに、OSSと完全に一致するファイルを表示またはフィルタをかけて、確認/レビュープロセスを容易にできます。

Docker対応バージョン

Black Duckインストールでは、Dockerバージョン18.03.x、18.06.x、18.09.x、19.03.x（CEまたはEE）がサポートされます。

BDBAコンテナのアップグレード

更新されたBlack Duck Binary Analysisコンテナ（現バージョンは2019.06）には、次の機能とバグ修正が含まれています。

機能：

- ディストロパッケージファイルからパッケージ情報を抽出し、.deb、.rpm、.apk、.pkgをサポートします。
- UEFIファームウェアイメージの抽出のサポートが追加されました。
- libmagicの5.37へのアップグレード - ファイルタイプの識別が改善され、CVE-2019-8907が修正されました。
- WindowsおよびMacOSバイナリからのGoコンポーネントの検出のサポートが強化されました。
- uClinuxに多くの一般的なコンポーネントの検出機能が追加されました。
- InstallShield 2016および古い生成済みWindowsインストーラの抽出のサポートが追加されました。

バグ修正：

- 破損したlzma圧縮uImagesの回帰が修正されました。
- tarのVMwareバージョンを抽出する際の回帰が修正されました。
- まれにJWTトークン抽出機能が遅くなる問題が修正されました。
- 内部の起動スクリプトの変更により、docker-entrypoint.shファイルで「command」の使用から「entrypoint」を使用するように変更されました。

更新されたコンテナ

- uploadcache: image: blackducksoftware/blackduck-upload-cache:1.0.9
- webserver: image: blackducksoftware/blackduck-nginx:1.0.8

APIの機能強化

脆弱性の影響を受けるプロジェクトを検出する新しいエンドポイント:

- GET /api/vulnerabilities/{vulnerabilityId}/affected-projects

新しいジョブ関連のエンドポイント:

- ジョブフィルタの取得: GET /api/jobs-filters
- ジョブIDによるジョブの取得: GET /api/jobs/{jobId}
- ジョブIDによるジョブの削除: DELETE /api/jobs/{jobId}
- ジョブIDによるジョブの再スケジュール: PUT /api/jobs/{jobId}

廃止されたエンドポイント:

- GET /api/components/{componentId}/vulnerabilities
- GET /api/projects/{leftProjectId}/versions/{leftVersionId}/compare/projects/{rightProjectId}/versions/{rightVersionId}/components

HTTPS://<Black DuckサーバーURL>/api-doc/public.htmlにある新しいBETA APIドキュメントにAPIが追加されました。

- レポートAPIエンドポイント
- スキャン分析アップロードAPIエンドポイント
- 追加のスキャンコードロケーションAPIエンドポイント

2019. 8. 0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-18804)。グローバルコードスキャナの役割およびプロジェクト作成者の役割を持つユーザーが任意のプロジェクトにアクセスできる問題を修正しました。
- (HUB-18930)。Protex構成表をBlack Duckにインポートできない問題を修正しました。
- (HUB-19690)。プロジェクトコードスキャナの役割を持つユーザーが[スキャン名]ページを表示して、割り当てられたプロジェクトスキャンを表示したり、既存のスキャンのマッピングを解除したりできない問題を修正しました。
- (HUB-19864)。脆弱性レポートが継続的に失敗する問題を修正しました。
- (HUB-19875)。「チャンクコード化されたメッセージ本文の早期終了」が原因でスニペットスキャ

ンが失敗する問題を修正しました。

- (HUB-20064)。SnippetScanAutoBomJobジョブのジョブページの[関連先]カラムに値が設定されない問題を修正しました。
- (HUB-20085)。スニペットスキャンが終了しない問題を修正しました。
- (HUB-20101)。マッチ名に移動したときに[ソース]タブに一貫性がなかった問題を修正しました。
- (HUB-20192)。[ソース]タブで確認済みスニペットやマッチしたスニペットの未確認ステータスが誤って表示される問題を修正しました。
- (HUB-20202、20236)。スキャンCLIがコード70でスキャンを終了する問題を修正しました。
- (HUB-20223)。Protex BOMツールでファイルマッチデータがインポートされない問題を修正しました。
- (HUB-20228)。[ソース]タブの並列比較スニペット機能で左側(ソース)のコンテンツが更新されない問題を修正しました。
- (HUB-20244)。[スキャン名]ページに表示されるマッチしたコンポーネントの数が、source.csvレポート内のコンポーネント数と異なる問題を修正しました。
- (HUB-20358)。「For input string:0.07」エラーが表示され、スキャンが失敗する問題を修正しました。
- (HUB-20370)。[ソース]タブでマッチを選択しても、マッチの場所を表示するようにツリーが展開されない問題を修正しました。
- (HUB-20483)。[ソース]タブでスニペットマッチのマッチ行が表示されない問題を修正しました。
- (HUB-20587)。[ソース]タブでユーザーがコンポーネントを編集する際にプロジェクトをそれ自体に追加できる問題を修正しました。
- (HUB-20588)。メインの検索アルゴリズムを使用してコンポーネント名のモーダル検索を実行できるようにするための問題を修正しました。
- (HUB-20611)。コンポーネントのBlack Duck識別子がないか無効であるためにScanPurgeJobジョブで失敗が記録される問題を修正しました。
- (HUB-20688)。[コンポーネントの編集]ダイアログボックスで異なるコンポーネントバージョンを選択できない問題を修正しました。
- (HUB-20733)。Protex BOMをBlack Duckにインポートしようとする、「アプリケーションで不明なエラーが発生しました」というメッセージが表示される問題を修正しました。
- (HUB-20744)。100のスニペットマッチの編集がタイムアウトになる問題を修正しました。
- (HUB-20749)。プロジェクトコードスキャナの役割を持つユーザーがソースファイルをアップロードできない問題が修正されました。
- (HUB-20755)。プロジェクトバージョン暗号文レポートに未確認または無視されたスニペットが表示される問題を修正しました。
- (HUB-20794)。scan.cli-windows-version.zipファイルからinvisible.vbsファイルを削除しました。
- (HUB-20870)。渡されたアプリケーションIDからプロジェクトIDを提供するAPI呼び出しを修正しました。
- (HUB-20886、20918)。プロジェクトを表示またはアクセスするためのユーザーの読み取り/表示権限が適用されない問題を修正しました。
- (HUB-20969)。ユーザーが入力した脆弱性修正情報がBlack Duck UIで更新されない問題を修正しました。

バージョン2019. 6. 2

バージョン2019. 6. 2の新機能および変更された機能

Black Duckバージョン2019. 6. 2はメンテナンスリリースのため、新機能や変更された機能はありません。

2019. 6. 2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-19716)。次のエラーメッセージが表示される問題を修正しました。「列インデックスが範囲外です: 8、カラムの数: 7」
- (HUB-20899)。KBReleaseUpdateJobジョブが継続的に失敗する問題を修正しました。

バージョン2019. 6. 1

バージョン2019. 6. 1の新機能および変更された機能

kubernetesディレクトリおよびファイルの削除

kubernetesディレクトリとそのディレクトリにあるすべてのファイルが削除されました。

Synopsysは、Synopsys Operatorを使用してKubernetesまたはOpenShiftにBlack Duckをインストールすることを推奨しています。

- [ここ](#)をクリックして、Kubernetes/OpenShift用Black Duckの概要を確認してください。
- Synopsys Operatorの概要については、[ここ](#)をクリックしてください。
- Synopsys Operatorを使用したBlack Duckのインストール方法については、[ここ](#)をクリックしてください。

2019. 6. 1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-19013)。プロジェクトまたはプロジェクトバージョンが削除された後に、VersionBomComputationJobが失敗する問題を修正しました。
- (HUB-20223)。ProtexBOMツール (scan.protex.cli.sh) がファイルマッチデータをインポートしない問題を修正しました。
- (HUB-20463)。ホストされるサーバーで[ソース]タブの左ペインに表示されるファイルツリーがロードされない問題を修正しました。
- (HUB-20484)。プロジェクト内の一部のコンポーネントをレビューまたは無視できない問題を修正しました。
- (HUB-20494)。推移的な依存関係が直接的な依存関係として報告される問題を修正しました。
- (HUB-20540)。KBReleaseUpdateJobが失敗し、「findSnippetAdjustment. arg3は空白にできません」というエラーメッセージが表示される問題を修正しました。
- (HUB-20612)。プロジェクトマネージャまたはプロジェクトコードスキャナの役割を持つユーザーが、[プロジェクトバージョン]の[設定]タブを使用してスキャンを表示やマッピング解除できない問題を修正しました。

バージョン2019. 6. 0

バージョン2019. 6. 0の新機能および変更された機能

Common Vulnerability Scoring System (CVSS) 3.0のセキュリティ上のリスクスコア

Black Duckでは、CVSS 3.0スコアを表示するオプションが追加されました。システム管理者の役割を持つユーザーは、Black Duckがセキュリティの脆弱性のリスクスコアとリスクカテゴリを定義するために使用するセキュリティランキングの順序を再定義できます。デフォルトでは、Black DuckはCVSS 2.0スコアを表示します。

セキュリティリスク構成の順序を変更すると、すべてのプロジェクトバージョンの構成表のセキュリティリスク計算が改訂され、新しいポリシー違反が発生する可能性がある点に注意してください。これらの計算は、完了までにかなりの時間がかかる場合があります。

セキュリティランキングを変更すると、次の2つの新しいジョブが開始されます。

- VulnerabilityReprioritizationJobはすべての構成表を新しい脆弱性優先度設定で再計算します。
- VulnerabilitySummaryFetchJobは欠けているCVSS 3.0データを検出します。

ライセンス条項の履行

ライセンスマネージャは、履行が必要なライセンス条項を定義できるようになりました。ライセンス条項のすべてのインスタンスで履行が必要とは限らないため、ライセンス条項の履行ステータスは、ライセンスレベルの条項に対して定義されます。これにより、ライセンス条項の履行要件を簡単に定義できます。

- 構成表マネージャは、システム管理者が有効にした新しいプロジェクトバージョンの[法]タブを使用して履行が必要なすべてのライセンス条項を表示し、どのライセンス条項が履行されているかを示します。
- ポリシーマネージャは、未履行のライセンス条項がある場合に違反をトリガーするポリシールールを作成できます。
- ライセンス条項の履行ステータスのクローンを作成できます。
- 新しいプロジェクトバージョンレポートlicense_term_fulfillment.csvには、プロジェクトバージョンのライセンス条項と履行ステータスが一覧表示されます。
- 新しいジョブであるLicenseTermFulfillmentJobは、ライセンス条項の履行要件をすべての構成表に適用します。

カスタムフィールドの機能強化

Black Duckでは、構成表コンポーネントおよびコンポーネントバージョンのカスタムフィールドの作成と管理がサポートされるようになりました。

構成表コンポーネントのカスタムフィールド情報は、構成表内のコンポーネントの詳細を表示すると表示されます。

コンポーネントバージョンのカスタムフィールド情報は、コンポーネント名バージョン名の[設定]タブの[その他のフィールド]セクションに表示されます。

レポートの機能強化

レポートに次の機能拡張が行われました。

■ プロジェクトバージョンレポート:

- プロジェクト名またはバージョン名の文字< > ¥ / | : * ? + "は、アンダースコア (_) で置き換えられます。
- アーカイブファイル名は、<プロジェクト名-プロジェクトバージョン>_YYYY-MM-DD-HHMMSS.zip (タイムスタンプはUTC) です。
- ディレクトリとファイル名は、<プロジェクト名-プロジェクトバージョン>_YYYY-MM-DD-HHMMSS/<ファイル名>_YYYY-MM-DD-HHMMSS.csv (アーカイブファイル名と同じタイムスタンプ) です。

■ グローバル脆弱性レポート:

- 脆弱性修正レポート、脆弱性ステータスレポート、脆弱性更新レポートでレポート形式として.csvを選択できるようになりました。

このオプションは、ブラウザでレンダリングして表示できないほどデータセットが大きくなった場合に便利です。

- アーカイブファイル名は、vulnerability-<レポートタイプ>-report_YYYY-MM-DD-HHMMSS.zip (タイムスタンプはUTC) になりました。
- ディレクトリとファイル名は、vulnerability-<レポートタイプ>-report_YYYY-MM-DD-HHMMSS.csv (アーカイブファイル名と同じタイムスタンプ) です。
- 新しく次の列がすべてのグローバル脆弱性レポートに追加されました。
 - 修正更新日
 - セキュリティ上のリスク

これらの新しい列は、レポートの最後の2列に表示されます。

新しいAPI ドキュメント (ベータ版)

新しいAPI ドキュメントが利用可能になりました。このドキュメントでは、API を使いやすくするために、API をグループ化し、より適切な例を提示し、API リンクを追加しました。

このドキュメントは次の場所にあります。

`HTTPS://<Black DuckサーバーURL>/api-doc/public.html`

このドキュメントはベータ版であり、まだすべてのAPI は含まれていない可能性があることに注意してください。

`HTTPS://<Black DuckサーバーURL>/api.html`にある既存のAPI ドキュメントは引き続き使用できます。

ソースビューの機能強化

ソースビューが機能強化され、パスをクリップボードにコピーできるようになりました。また、スニペットに関連付けられているコンポーネントを一括編集できるようになりました。

Swarmサービスの読み取り専用ファイルシステムのサポート

新しいファイル`docker-compose.readonly.yml`がディストリビューションに含まれています。このファイルを使用して、Swarmサービスの読み取り専用ファイルシステムのあるBlack Duckをインストールできます。

この機能はDocker Swarmでのみサポートされています。

Docker Swarmオーケストレーションのバージョン変更

- Docker Composeバージョン : 3.6
- Dockerエンジンバージョン : 18.02.0以降

アーカイブされたプロジェクトバージョンの機能強化

アーカイブフェーズのプロジェクトバージョンでは、セキュリティ脆弱性に関するBlack Duckナレッジベースの更新はアーカイブされたプロジェクトバージョンに適用されます。

ただし、ライセンス情報の更新など、Black Duck KBの他のすべての更新は、アーカイブされたプロジェクトバージョンには適用されません。

新しいジョブ

次のジョブがBlack Duckに追加されました。

- BOMagGregaratePointHandsJobはプロジェクトバージョンに関連付けられていない構成表データを削除します。
- ComponentDashboardRefreshJobはコンポーネントダッシュボードに表示される情報を更新します。
- PolicyRuleModification BomComputationJobはポリシールールの変更の影響を受けるバージョン構成表を計算します。

コードサイズ制限の適用

コードサイズの制限を超えると、スキャンを試行したとき（JenkinsのログファイルやSynopsys Detect (Desktop) の画面などに）、またはスキャンをBlack Duckにアップロードしようとしたときにエラーメッセージが表示されるようになりました。コードサイズの制限を超えてスキャンやスキャンのアップロードをすることはできません。

更新されたBlack Duck – Binary Analysisコンテナ

更新されたBlack Duck Binary Analysisコンテナ（現バージョンは2019.03）には、次のものが含まれます。

- 新しいコンポーネントの検出機能を追加
- InstallAnywhereで作成されたLinuxパッケージの抽出に対するサポートを追加
- zstandard圧縮の抽出に対するサポートを追加
- FreeBSD ufs、uzip、ulzma画像抽出のサポートを追加

Synopsys Detect (Desktop) の機能強化

Synopsys Detect (Desktop)（以前のBlack Duck Detect Desktop）には、次のような機能が追加されています。

- 既存のAPIキーを使用する機能。
- 以前のバージョンのSynopsys Detect (Desktop) からデータを移行するオプション。
- Synopsys Detect (Desktop) の更新をチェックして、新しいバージョンが利用可能かどうかを確認する機能。このオプションは、WindowsおよびMacOSシステムでのみ使用できます。

アプリケーションはその名前に関連するディレクトリにインストールされるため、Synopsys Detect

(Desktop) は、以前のバージョンのBlack Duck Detect Desktopをアンインストールしません。また、デフォルト以外のディレクトリにインストールされたバージョンのSynopsys Detect (Desktop) もアンインストールしません。以前のバージョンのBlack Duck Detect Desktopやデフォルト以外のディレクトリにインストールされているバージョンのSynopsys Detect (Desktop) はすべて手動でアンインストールし、ショートカットを修正または削除する必要があります。

Solrコンテナの削除

検索パフォーマンスを向上させるために、Solrコンテナが削除されました。

個々の企業ポリシーに応じて、既存のDocker Solrボリュームを維持、バックアップ、または削除できます。

コンポーネントダッシュボードのリフレッシュレート

デフォルトでは、コンポーネントダッシュボードは5分ごとに更新されます。変更を加えてもコンポーネントダッシュボードにすぐに表示されない場合は、`blackduck-config.env` ファイルにシステムプロパティ `com.blackducksoftware.bom.aggregate.component_dashboard_refresh_interval_ms` を追加して、コンポーネントダッシュボードのリフレッシュレートを定義できるようになりました。

この機能は、Docker ComposeおよびDocker Swarm用です。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2019. 4. 1が日本語にローカライズされました。

2019. 6. 0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-8192)。180日より古い通知は自動的に削除されるようになりました。
- (HUB-13279)。プロジェクトバージョンAPIの新しいベータAPIドキュメントに、複雑なライセンス表示モデルが含まれるようになりました。
- (HUB-15298)。[コンポーネント] タブにアクセスしたときにパフォーマンスの問題が発生する問題を修正しました。
- (HUB-15698)。[ソース] タブでスニペットのポリシー違反が表示されない問題を修正しました。
- (HUB-16619)。未確認スニペットによって脆弱性通知がトリガーされ、セキュリティリスク値に含まれる問題を修正しました。
- (HUB-16628)。SSOが有効になっているときに直接Black Duckリンクに移動すると、ログイン後に、元のリンク先ではなくプロジェクトダッシュボードに移動する問題が修正されました。
- (HUB-17378)。コードサイズの合計制限に対してスニペットスキャンが二重にカウントされる問題を修正しました。
- (HUB-18221)。グローバルコードスキャナおよびプロジェクト作成者の役割を持つユーザーが[スキャン] ページまたは[スキャン名] ページを表示し、表示権限のないプロジェクトバージョンにアクセスできてしまう問題を修正しました。
- (HUB-18523)。プロジェクトコードスキャナの役割を持つユーザーが割り当てられているプロジェクトのスキャンをダウンロードできない問題を修正しました。
- (HUB-18561)。Internet Explorerの使用時にCVEまたはBDSAレコードの表示を選択すると空の

ページが表示される問題を修正しました。

- (HUB-18623)。ページをがリロードすると運用上のリスクフィルタがライセンスリスクフィルタに変更される問題を修正しました。
- (HUB-18631)。コメントの追加または編集時に404エラーメッセージが表示される問題を修正しました。
- (HUB-18676)。バイナリファイルの解析時に400エラーメッセージが表示される問題を修正しました。
- (HUB-18694)。外部URLをプローブするときに、`system_check.sh`スクリプトがコンテナのプロキシ設定を使用するように問題を修正しました。
- (HUB-18760)。暗号化フィルタが[構成表] ページで正しく動作せず、ポリシー管理のマッチタイプフィルタに不一致オプションがない問題を修正しました。
- (HUB-18911)。[構成表] ページの属性レポートフィルタの名称を通知ファイルレポートに変更しました。
- (HUB-18983)。Synopsys Detectによるスキャン時にポリシーチェックが有効になっていると、プロジェクトレベルの権限は持っていないが完全なグローバル権限を持っているSSOユーザーがエラーを受信する問題を修正しました。
- (HUB-19130)。[スキャン名] ページに表示されるマッチしたコンポーネントの数が、`source.csv` レポート内のコンポーネント数と異なる問題を修正しました。
- (HUB-19141)。確認済みのスニペットコンポーネントのみがコンポーネントダッシュボードに表示されるように問題を修正しました。
- (HUB-19238)。構成表に対する編集がタイムリーに完了しなかったと思われる問題を修正しました。
- (HUB-19274)。Black Duck UIのセキュリティリスクの分類と`security.csv` レポートに不整合が見られる問題を修正しました。
- (HUB-19490)。ページが更新されたときに、[構成表] ページのフィルタに誤った値が表示される問題を修正しました。
- (HUB-19504)。スキャンクライアントCLIがJava JREバージョン11.0.2にパッケージ化されるように問題を修正しました。
- (HUB-19522)。スキャンが完了してBlack Duckにアップロードされているにもかかわらず、プロジェクトコードスキャナの役割を持つユーザーに終了コード77が返される問題を修正しました。
- (HUB-19548)。プロジェクトを再スキャンしない限り、ライセンスファミリに手動で加えた変更がプロジェクトに伝搬しないという問題を修正しました。
- (HUB-19604)。サブプロジェクトを追加しようとしたときに不正確な検索結果が表示される問題を修正しました。
- (HUB-19607)。一部のセキュリティ脆弱性のBDISAレコードで、関連するCVEレコードが[セキュリティ] タブに表示されない問題を修正しました。
- (HUB-19637)。脆弱な構成表コンポーネントAPI応答に、未確認または無視されたスニペットマッチが含まれる問題を修正しました。
- (HUB-19696)。参照、カスタムフィールド、オリジン、リスクプロファイル、および脆弱性への`/api/components/{componentId}` サブリンクが正しくリダイレクトされるよう問題を修正しました。
- (HUB-19728)。プロジェクトバージョンのクローンを作成しようとすると、「エンティティが存在しません」というエラーメッセージが表示される問題を修正しました。

- (HUB-19771)。ディレクトリを選択したときに、[ソース]タブの[編集]セクションの開き方が不安定である問題を修正しました。
- (HUB-19791)。スニペットを管理する場合の[ソース]タブでさまざまなUIの問題を修正しました。
- (HUB-19897)。ユーザーがいずれかのプロジェクトへのアクセス権をすでに持っている場合、そのユーザーを複数のプロジェクトに割り当てることができない問題を修正しました。
- (HUB-19907)。findVulnerableComponents APIで、プロジェクト内の無視されたコンポーネントおよび未確認スニペットの脆弱性と通知が誤って表示される問題を修正しました。
- (HUB-19909)。中規模から大規模のスキャンを実行するときに「ジョブタイプのポリシーでサポートされていないため、処理を管理できません」というメッセージが表示される問題を修正しました。
- (HUB-20033)。[ジョブ]ページがタイムアウトし、「Black Duckサーバーが応答しません」というメッセージが表示される問題を修正しました。
- (HUB-20054)。スニペットマッチに異なるコンポーネントを選択すると、既存のコンポーネントを置き換えるのではなく、コンポーネントが追加される問題を修正しました。
- (HUB-20086)。ファイルライセンスAPIを使用すると、412前提条件の失敗エラーが表示される問題を修正しました。
- (HUB-20146)。プロジェクトのクローンを作成しようとしたときに「プロジェクトがすでに存在するため、コンポーネントの調整を作成できません」というエラーメッセージが表示される問題を修正しました。
- (HUB-20172)。[ソース]タブで、パスを選択しても、宣言されたコンポーネントの正確なパスまたはファイル名が表示されないという問題を修正しました。

バージョン2019. 4. 3

バージョン2019. 4. 3の新機能および変更された機能

LinuxバージョンのSynopsys Detect Desktop

Black Duckで、Linuxバージョン（.debまたは.rpm）のSynopsys Detect Desktopが提供されるようになりました。

このバージョンへのリンクは、Black Duck UIの[ツール]ページにあります。このリンクをクリックすると、Synopsys Detect Desktopのダウンロードが置かれているGoogle Cloud Storageに移動します。

2019. 4. 3で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-19435)。すべてのKbReleaseUpdateJobジョブが失敗する問題を修正しました。
- (HUB-19636)。未確認または無視されたスニペットマッチがコンポーネントおよびコンポーネントバージョンの使用数に含まれる問題を修正しました。

バージョン2019. 4. 2

バージョン2019. 4. 2の新機能および変更された機能

ビルドツールが使用できない場合にパッケージ管理ファイルを解析する機能

ビルドツールが使用できなくても、Synopsys Detectでパッケージ管理ファイルを解析できるようになり

ました。Black Duckは、優先するマッチの決定を試み、構成表内のコンポーネントとコンポーネントバージョンを表示します。

この機能を有効にするには、`docker-compose.local-overrides.yml` ファイル内の`jobrunner`サービスで`HUB_SCAN_ALLOW_PARTIAL`環境変数を`true`に設定します。以下に例を示します。

```
jobrunner:
  environment: {HUB_SCAN_ALLOW_PARTIAL=true}
```

2019. 4. 2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- (HUB-18836)。外部のAzure PostgreSQLインスタンスがあるAzure Kubernetes Service (AKS) 上でBlack Duckを実行する際の構成の問題を修正しました。
- (HUB-18963)。Synopsys Detectによるスキャン時にポリシーチェックが有効になっていると、プロジェクトレベルの権限は持っていないが完全なグローバル権限を持っているSSOユーザーがエラーを受信する問題を修正しました。
- (HUB-19013)。プロジェクトまたはプロジェクトバージョンが削除された後に、`VersionBomComputationJob`が失敗する問題を修正しました。
- (HUB-19840)。コードの場所がすでに存在する場合に`SnippetAutoBomJob`ジョブが失敗する問題を修正しました。

バージョン2019. 4. 1

バージョン2019. 4. 1の新機能および変更された機能

コードサイズ制限の警告

コードサイズの上限に近づいたり、上限を超えたりした場合に、Black Duckはユーザーに警告します。

Docker Swarmの新しい制約

Docker Swarmを使用したBlack Duckのインストールでは、データが失われないようにするために、`blackduck-upload-cache`サービスを常にクラスタ内の同じノードで実行するか、NFSボリュームまたは同様のシステムでバックアップする必要があります。

2019. 4. 1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- `VersionBOMComputationJob`が失敗し、継続的に再起動される問題を修正しました。
- Black Duck UIにスキャン結果が表示されない問題を修正しました。
- Black Duck UIのセキュリティリスクの分類とBDSA脆弱性データの`.CSV`レポートに不整合がある問題を修正しました。
- すべての`KBReleaseUpdateJob`ジョブが失敗する問題を修正しました。

バージョン2019. 4. 0

バージョン2019. 4. 0の新機能および変更された機能

監査記録

Black Duckは、プロジェクトやプロジェクトのバージョンに影響を与えるすべての更新や変更に関する情報を提供するようになりました。この監査記録を使用して、変更を行ったユーザー、またはプロジェクトやプロジェクトバージョンを変更した原因となったイベントを把握します。

この情報はプロジェクト名またはプロジェクト名バージョン名の[設定]タブで確認できます。

ライセンスファミリの管理

Black Duckでは、カスタムライセンス条項を作成し、既存のナレッジベースライセンス条項を管理して、ライセンスに関連する法律上の責務を確実に満たすことができるようになりました。ライセンス条項を管理することで、開発者がライセンスに関連する法律上の責務を理解し、プロジェクトをライセンスの責務に適合させることができます。

ライセンスマネージャの役割を持つユーザーは、次のことができます。

- カスタムライセンス条項を作成、編集、または削除します。
- カスタムまたはナレッジベースのライセンス用語を、1つ以上のカスタムまたはナレッジベースのライセンスに関連付けます。
- カスタムまたはナレッジベースのライセンスからカスタムライセンスの条項を削除します。
- Black Duckナレッジベースで最初に定義されていなかったカスタムライセンスまたはナレッジベースライセンスから、ナレッジベースのライセンス条項を削除します。
- カスタムライセンス条項は非推奨になりました。
- ナレッジベースライセンスのナレッジベースライセンス条項を無効化または回復します。

スニペットの機能強化

このBlack Duckリリースでは、スニペットの管理に関する次の機能強化が行われました。

- Black Duckでは、ソースファイルをアップロードできるようになりました。これにより、構成表レビュー担当者はBlack Duck UI内からファイルの内容を確認できます。

これは、管理者が有効にできるオプション機能です。有効にする場合は、スニペットスキャン時に、スキャンに新しい`--upload-source`パラメータを含める必要があります。

ソースファイルをアップロードすると、構成表レビュー担当者はソースファイルの並列比較を表示し、スニペットマッチを評価およびレビューするのに役立ちます。

この機能は、スニペットスキャンでのみ使用できます。

- スニペットのマッチをトリアージするプロセスが向上し、ソースファイルをアップロードするオプションが有効になっていない場合でも、スニペットマッチを簡単に確認して管理できるようになりました。
- 新しいフィルタのマッチステータスが構成表に追加されました。このフィルタを使用して、構成表に未確認または確認済みのスニペットマッチを表示します。

[ソース]タブの機能強化

[ソース]タブが改善され、部品表コンポーネントに関連付けられたファイルの管理が容易になりました。

カスタムフィールドの機能強化

- Black Duckは、コンポーネントのカスタムフィールドの作成と管理をサポートするようになりました。
- Black Duckは、ドロップダウン、複数選択、または単一選択フィールドタイプを使用するプロジェクトカスタムフィールドのポリシーをサポートします。

[ポリシーの作成]ダイアログボックスの再設計

[ポリシーールールの作成] ダイアログボックスは、すべてのプロジェクトのルールまたはフィルタをかけられたルールを作成しやすくするため、特定のプロジェクトにのみルールが適用されるようにフィルタ処理されるように再設計されました。

APIの機能強化

- ライセンスの使用カウントを取得するようにAggregate-BM-Rest-Server REST APIを機能強化しました。このAPIは機能強化され、プロジェクトバージョンをサブプロジェクトとして追加できるようになりました。
- Component-Rest-Server REST APIは機能強化され、コンポーネントカスタムフィールドをサポートするようになりました。
- custom-field-rest-server REST APIは機能強化され、カスタムフィールドフィルタをサポートするようになりました。
- 監査記録をサポートするために、新しいREST API、journal-rest-serverを追加しました。
- ライセンス条項の関連付けを管理するために、license-rest-server REST APIが機能強化されました。
- ライセンス条項カテゴリを管理するために、新しいREST API、license-term-category-rest-serverが追加されました。
- ライセンス条項を管理するために、新しいREST API、license-term-rest-serverが追加されました。
- スニペットマッチ用のソースファイルのアップロードの管理をサポートするために、新しいREST API、source-upload-rest-serverが追加されました。
- [ソース]タブでのスニペットマッチの向上をサポートするように、source-view-rest-server REST APを機能強化しました。

Synopsys Detect (Desktop)

Synopsys Detect (Desktop) はBlack Duckアプリケーションにパッケージ化されなくなり、Google Cloud Storageから入手できるようになりました。Google Cloud Storageからダウンロードできるため、Synopsysは、Synopsys Detect (Desktop) を使用して迅速に更新を提供し、Synopsys Detectで柔軟性を高めることができます。

Synopsys Detect (Desktop) へのリンクは、Black Duck UIの[ツール]ページにあり、この新しいダウンロード場所に切り替わります。

LDAPトラストストアパスワード

2019. 4. 0Black Duckリリース以降、環境変数を使用したカスタムLDAPトラストストアパスワードの設定は

サポートされなくなりました。その代わりに、docker secretを作成する必要があります。詳細については、『インストールガイド』を参照してください。

Docker対応バージョン

Black Duckインストールでは、Dockerバージョン17.12.x、18.03.x、18.06.x、18.09.x（CEまたはEE）がサポートされます。

ログファイル

ログファイルは、14日後に自動的に削除されるようになりました。

この値を変更するには、『インストール・ガイド』で説明されているように、DAYS_TO_KEEP_LOGS変数を使用します。

jobrunnerの拡張機能

効率を向上させるために、jobrunnerはシステムリソースを確認し、利用可能なリソースに基づいて実行できるジョブの数を動的に調整できるようになりました。

外部拡張

Black Duckは外部拡張機能をサポートしなくなりました。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン2019.2.0が日本語にローカライズされました。

2019.4.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- SSOバックドアURL (<https://<URL>/sso/login>) を使用してローカルユーザーアカウントでログインしようとした場合に、「ページが見つかりません」というエラーメッセージが表示される問題を修正しました。
- 無視されたコンポーネントの構成表でマッチ値を選択した場合に、「不明なエラー」メッセージが表示される問題を修正しました。
- 階層構成表機能が有効になっているときにスキャンが空になっていた問題を修正しました。
- Microsoft Edgeの使用時に、[ソース]タブの左ペインに表示されるファイルツリーが部分的に非表示になる問題を修正しました。
- JSONファイルのインポート時に「コピーへの書き込みの終了に失敗しました」というエラーメッセージが表示される問題を修正しました。
- スニペットに別のマッチを選択したときに調整エラーが発生する問題を修正しました。
- コンポーネントのバージョンを編集できない問題を修正しました。
- Black Duckのアップグレード後もKBComponentUpdateJobジョブが失敗し続ける問題を修正しました。
- スキャンまたはプロジェクト名に日本語の文字が含まれている場合にスキャンが失敗する問題を修正しました。
- bdioデータベースが大幅に増大する問題を修正しました。

- カスタムフィールドで日本語の文字がサポートされない問題を修正しました。
- Black Duck UIを再読み込みした後にInternet Explorer 11にすべてのアイコンが表示されない問題を修正しました。
- スニペットスキャン中にNULLポインタ例外が発生する問題を修正しました。
- 外部データベースを使用するように構成されたBlack Duckシステムが起動しない問題を修正しました。

バージョン2019. 2. 2

バージョン2019. 2. 2の新機能および変更された機能

Black Duckバージョン2019. 2. 2では、スキャンとマッチングの機能が強化されています。

2019. 2. 2で修正された問題

このリリースでは、お客様から報告された問題は修正されていません。

バージョン2019. 2. 1

バージョン2019. 2. 1の新機能および変更された機能

Black Duckバージョン2019. 2. 1はメンテナンスリリースのため、新機能や変更された機能はありません。

2019. 2. 1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- 「GENERATING_SIGNATURESのエラー、このIDのオブジェクトはすでに存在します」というエラーメッセージが表示され、スキャンが失敗した問題を修正しました。

バージョン2019. 2. 0

バージョン2019. 2. 0の新機能および変更された機能

新しいグローバルプロジェクトビューア役割

すべてのプロジェクトに対する読み取り専用アクセス権のある新しい役割[グローバルプロジェクトビューア]が設けられました。この役割を持つユーザーは、すべてのプロジェクトの構成表を表示して、コメントを作成できます。

ユーザーにこの役割を割り当てると、自動的にすべてのプロジェクトに対する読み取り専用アクセス権が与えられます。ユーザーをプロジェクトに割り当てる必要はありません。

Synopsys Detect (Desktop)

Synopsys Detect (Desktop) (以前のBlack Duckスキャナ) は、Synopsys Detectの性能とデスクトップアプリケーションの利便性を兼ね備えるようになりました。

Synopsys Detect (Desktop) は、MacOS 10. 9以降およびWindows 7以降で使用できます。

カスタムフィールド

Black Duckは、プロジェクトおよびプロジェクトバージョンのカスタムフィールドの作成と管理をサポートするようになりました。たとえば、カスタムフィールドを使用して、社内のオープンソースソフトウェアの管理や大規模なプロジェクトの整理に役立つ追加情報を含めることができます。

スキャンベストプラクティスガイドの改良点

スキャンベストプラクティスガイドが改訂され、自動スキャンの設定、スキャンパフォーマンスの最適化、および一般的なスキャンエラーの回避方法に関する情報が含まれるようになりました。

デフォルト値の上書きをサポートする新しい構成ファイル

新しい.ymlファイルであるdocker-compose.local-overrides.ymlがDocker ComposeおよびDocker Swarmディストリビューションに追加されました。

デフォルトのBlack Duck設定をカスタマイズする必要がある場合は、このファイルを使用してローカルの.ymlファイルを編集します。このファイルはアップグレードプロセスを簡素化します。新しいバージョンのBlack Duckにアップグレードしたときに構成の変更は保持されます。

このファイルの使用方法については、docker-composeまたはdocker-swarmディレクトリにあるReadme.mdファイルを参照してください。

ポリシーの強化

コンポーネントに不明なバージョンがある場合にポリシー違反をトリガーするポリシーを作成できるようになりました。

カスタム認証局

Black Duckは、証明書認証に独自の認証局を使用できるようになりました。

この機能は、Docker ComposeおよびDocker Swarmでサポートされています。

データベースのバックアップスクリプトおよび移行スクリプトの強化による手動手順の削減

hub_create_data_dump.shおよびhub_db_migrate.shスクリプトが強化され、すべてのBlack Duckデータベースのバックアップと復元に必要な手動手順が削減されました。

キープアライブの設定

最適なBlack Duckパフォーマンスを得られるように、Synopsysではnet.ipv4.tcp_keepalive_timeシステム設定を600~800秒の値に設定することを推奨しています。

APIの機能強化

- カスタムフィールドを作成および管理するための新しいAPIであるcustom-field-rest-serverが追加されました。
- カスタムフィールドを管理するためのproject-rest-serverおよびproject-version-rest-serverを強化しました。

2019.2.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- [印刷プレビュー]にリスクバーが表示されない問題を修正しました。
- 再スキャンを実行しない限り、ライセンスメタデータの変更が構成表に表示されない問題を修正しました。
- [スキャン] ページで選択したチェックボックスが数秒後にクリアされる問題を修正しました。
- 脆弱性更新レポートに、円グラフの4つの値と一致する4つのセクションが表示されるように問題を修正しました。
- スニペットマッチを編集しても元のライセンスが保持される問題を修正しました。
- スキャナGUIを使用してスキャンを新しいプロジェクトにアップロードするユーザーにプロジェクトマネージャの役割が割り当てられ、ユーザーがプロジェクトの表示およびプロジェクトへのユーザーの追加/編集/削除を行えるように問題を修正しました。
- Black DuckスキャナにJSONファイルを自動的に読み込めない問題を修正しました。
- スニペットのソースコードをコピーできない問題を修正しました。
- スキャン時にWindowsスキャンGUIでプロキシ設定が使用されない問題を修正しました。
- 概要ダッシュボードの[今週作成された新しいプロジェクト]リンクを選択したときにエラーメッセージが表示される問題を修正しました。
- [コンポーネント名バージョン] ページに複数のライセンスが正しく表示されない問題を修正しました。
- 一部のプロジェクトで[ソース]タブをクリックしたときに「アプリケーションで不明なエラーが発生しました。詳細については、ログを確認してください。」というエラーメッセージが表示される問題を修正しました。
- スキャンをプロジェクトにマッピングするときに[バージョンの作成]ボタンが表示されない問題を修正しました。
- ユーザーがどのグループにも属していないときにSAML認証エラーが発生する問題を修正しました。
- スニペットスキャン中にNULLポインタ例外が発生する問題を修正しました。

バージョン2018. 12. 4

バージョン2018. 12. 4の新機能および変更された機能

外部データベースでの複雑なPostgreSQLユーザー名のサポート

外部PostgreSQLデータベースで、複雑なユーザー名（@記号などの特殊文字が含まれた）がサポートされるようになりました。

2018. 12. 4で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- Azure KubernetesクラスタにBlack Duckを導入しようとしたときに、移行スクリプトの構文エラーが発生する問題を修正しました。

バージョン2018. 12. 3

バージョン2018. 12. 3の新機能および変更された機能

このリリースは、Black Duckで見つかった高リスクのセキュリティ脆弱性に対応します。

2018. 12. 3で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- スキャン中に「テーブル「V-project」での更新または削除は、外部キー制約に違反します」というエラーが発生する問題を修正しました。

バージョン2018. 12. 2

バージョン2018. 12. 2の新機能および変更された機能

Black Duckバージョン2018. 12. 2はメンテナンスリリースのため、新機能や変更された機能はありません。

2018. 12. 2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- 再スキャンしないと、ライセンスメタデータに対するBlack Duckナレッジベースの変更が構成表で自動的に更新されない問題を修正しました。

バージョン2018. 12. 1

バージョン2018. 12. 1の新機能および変更された機能

データベースパフォーマンスの向上

PostgreSQLデータベースが改善され、時間の経過に伴うデータベースの増加率が低下しました。

既存の外部のPostgreSQLデータベースを使用するユーザーは、これらの改善を実現するために次の手順を実行する必要があります。

1. 任意のPostgreSQL管理ツールを使用して、次のグローバルシステム変更を行います。

```
autovacuum_max_workers = 20
autovacuum_vacuum_cost_limit = 2000
```

2. PostgreSQLを再起動します。

スキャン性能の改善

スキャンが改善され、パフォーマンスが向上しました。

2018. 12. 1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- 大きいデータベースのReportingDatabaseTransferJobが長時間実行されるという問題を修正しました。
- 多数のScanGraphJobジョブが保留中になるという問題を修正しました。
- Jenkinsを使用してプロジェクトをスキャンするときにポリシー違反と脆弱性の通知がトリガーされないという問題を修正しました。

バージョン2018. 12. 0

バージョン2018. 12. 0の新機能および変更された機能

Docker対応バージョン

このリリースでは、Dockerバージョン17. 06. xはサポートされなくなりました。

Black DuckはDockerバージョン17. 09. x、17. 12. x、18. 03. x、18. 06. x、18. 09. x (CEまたはEE) をサポートします。

Docker Compose対応バージョン

Docker Composeの最小サポートバージョンでは、Docker Compose 2. 3のファイルを読み取ることができます。

Docker SwarmとKubernetesの新しい制限事項

Black Duck Docker Swarmを使用したインストールでは、登録データが失われないようにするために、blackduck-registrationサービスを常にクラスタ内の同じノードで実行する必要があります。

この制限は、永続ボリュームが使用されていない場合のKubernetesを使用するBlack Duckのインストールにも適用されます。

カスタムライセンスファミリ

Black Duckでは、ライセンスマネージャの役割を持つユーザーがカスタムライセンスファミリを作成および管理できるようになりました。この機能を使用すると、構成表がライセンスリスクを正確に表示できるようになります。

カスタムライセンスファミリ：

- 名前、リスクプロファイル、およびオプションの説明で構成されます。
- カスタムライセンスに割り当てられます。
- ポリシールールを作成するために使用できます。
- コンポーネントの使用法と配布の組み合わせを使用し、ライセンスリスクを判定します。

ライセンスの責務情報の表示

[ライセンス管理] ページを使用するとき、または構成表でライセンス情報を表示するとき、ライセンスの責務を表示できるようになりました。

デフォルトの使用法の変更機能

Black Duckではblackduck-config.envファイル内に変数が用意されています。これを使用して、類似するマッチタイプのデフォルトの使用法を変更できます。変数は次のとおりです。

- BLACKDUCK_HUB_FILE_USAGE_DEFAULT。この変数の使用法を定義すると、次のマッチタイプのデフォルト値が設定されます。
 - 完全ディレクトリ
 - 完全ファイル

- 追加/削除されたファイル
 - 変更したファイル
 - 部分
- BLACKDUCK_HUB_DEPENDENCY_USAGE_DEFAULT。この変数の使用法を定義すると、次のマッチタイプのデフォルト値が設定されます。
 - ファイルの依存関係
 - 直接的な依存関係
 - 推移的な依存関係
 - BLACKDUCK_HUB_SOURCE_USAGE_DEFAULT。この変数の使用法を定義すると、次のマッチタイプのデフォルト値が設定されます。
 - バイナリ
 - スニペット
 - BLACKDUCK_HUB_MANUAL_USAGE_DEFAULT。この変数の使用法を定義すると、次のマッチタイプのデフォルト値が設定されます。
 - 手動で追加
 - 手動で判定

カスタムスキャン署名 - ベータ

このリリースでは、カスタムスキャン署名はベータ機能のままです。

このリリースの内容：

- パフォーマンスを向上させるために、カスタムスキャン署名はディレクトリ構造の上位4つのレベルに制限されています。
- プロジェクトダッシュボードと[構成表]ページにカスタム署名フィルタが追加されました。このフィルタを使用して、プロジェクトに対してカスタム署名が有効になっているプロジェクトを検索します。

このベータ版の機能を使用する場合には、機能を有効にするための詳細とパフォーマンススキャンの潜在的な影響に関する詳細について、Synopsysのカスタマーサポート担当者またはアカウントエグゼクティブにお問い合わせください。

PostgreSQLアカウント名を変更する機能

外部のPostgreSQLデータベースのPostgreSQLユーザーおよび管理者のユーザー名をカスタマイズできるようになりました。この機能は、新規インストールとアップグレードに適用されます。

この機能は、Docker ComposeおよびDocker Swarmで使用できます。KubernetesまたはOpenShiftを使用したBlack Duckのインストールについては、Synopsysカスタマーサポートにお問い合わせください。

すべてのBlack Duckデータベースを簡単にバックアップする機能

Black Duckデータベースのバックアップと復元に使用される`hub_create_data_dump.sh`および`hub_db_migrate.sh`スクリプトが、レポートデータベースのバックアップと復元を含むように拡張されました。

スキャンファイルのエクスポート

Black Duck UIで、スキャンファイルのエクスポート機能がサポートされるようになりました。この機能は、スキャンファイルが必要な場合に使用できます。たとえば、スキャンの問題が発生した場合に、カスタマサポートからこのファイルが要求されることがあります。

SAMLの機能強化

このリリースの内容：

- SAMLを有効または無効にするために、Black Duckを再起動する必要がなくなりました。
- SAML管理ページの機能が強化され、SAML統合のためのBlack DuckメタデータXMLを簡単にダウンロードできるようになりました。

追加のデフォルトポリシールール

2つの追加のデフォルトポリシールールがあります。

- 変更対象としてマークされたコンポーネントなし。コンポーネントが変更された場合にポリシー違反をトリガーします。
- 説明のない変更されたコンポーネントなし。コンポーネントが変更された場合および変更の理由について説明が提供されていない場合に、ポリシー違反をトリガーします。

デフォルトポリシールールは、デフォルトで無効です。

構成表フィルタに追加されたポリシールールの重大度フィルタ

新しいフィルタであるポリシールールの重大度が構成表ページに追加され、構成表に表示するポリシールールの重大度を選択できるようになりました。

[ジョブの再編成] ページ

新しい[概要]セクションには、ログを保持している日数（デフォルトでは30日間）の各ジョブの成功数、失敗数、進行中のジョブ数が一覧表示されます。

リリースノートの再編成

新機能、変更された機能、およびリリースで修正された不具合を簡単に見つけることができるように、リリースノートが再編成されました。リリースごとに編成された1つの章に、新機能、変更された機能、およびリリースで修正された不具合が一覧表示されます。

階層構成表の機能強化

このリリースの内容：

- 階層構成表UIが改善され、使いやすくなりました。これには、新しいポリシー違反、上書きアイコン、親/子コンポーネントを示すアイコンが含まれます。
- 依存関係スキャンで検出された構成部品が階層構成表に表示されるようになりました。

APIの拡張機能

- コンポーネント取得元情報用の新しいREST API、component-origin-rest-serverが追加されました。
- コンポーネントバージョンフィルタ用のcomponent-version-rest-server APIが拡張されました。

- ジョブ統計管理用に新しいREST API、`job-rest-server`が追加されました。
- カスタムライセンスファミリの管理をサポートするために、`license-family-rest-server` APIが拡張されました。
- SS0構成情報の再読み込みを行うために、`meta-rest-server` APIが拡張されました。
- プロジェクトバージョンフィルタを取得するために、`project-version-rest-server`が拡張されました。
- ライセンスフィルタを取得するために、`risk-profile-rest-server` APIが拡張されました。
- バージョン構成表のステータスを取得するために、新しいREST API `version-bom-status-rest-server`が追加されました。
- コンポーネントには脆弱性が割り当てられていないので、`vulnerability-rest-server` APIで、コンポーネント別に脆弱性を検出する機能が非推奨になりました。

2018.12.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- 再スキャンが元のプロジェクトの新しいバージョンにマップされた後に構成表の棒グラフが表示されない問題を修正しました。
- 結果がないプロジェクトの構成表を印刷するときに誤った出力が表示される問題を修正しました。
- ホストされているBlack Duckサーバーで`ReportingDatabaseTransferJob`が失敗する問題を修正しました。
- 大きいデータベースの`ReportingDatabaseTransferJob`が長時間実行されるという問題を修正しました。
- マッチしなかったファイルがない場合にスニペットスキャンが完了しないという問題を修正しました。

バージョン2018.11.1

バージョン2018.11.1の新機能および変更された機能

Black Duckバージョン2018.11.1はメンテナンスリリースのため、新機能や変更された機能はありません。

2018.11.1で修正された問題

このリリースでは、お客様から報告された問題は修正されていません。

バージョン2018.11.0

バージョン2018.11.0の新機能および変更された機能

カスタムスキャン署名 - ベータ版

構成表がすべてのコードを追跡できるように、Black Duckではカスタムスキャン署名を提供するようになりました。コードで使用しているサードパーティおよびプロプライエタリソフトウェアの判定に使用できません。

このベータ版の機能を使用する場合には、機能を有効にするための詳細とパフォーマンススキャンの潜在的

な影響に関する詳細について、Synopsysのカスタマーサポート担当者またはアカウントエグゼクティブにお問い合わせください。

Important: これはカスタムコード署名機能のベータ版です。そのため、この機能は期待どおりに機能しない可能性があります。実稼働環境での使用は推奨していません。また、この機能を使用すると、大幅にパフォーマンスが低下する可能性があり、スキャン時間に影響をおよぼす可能性があります。特に多数のスキャン対象プロジェクトがあるシステムやプロジェクトの規模が非常に大きいシステムでは大きな影響を受ける可能性があります。このベータ版の機能を使用する場合には、機能を有効にするための詳細とパフォーマンススキャンの潜在的な影響に関する詳細について、Synopsysのカスタマーサポート担当者またはアカウントエグゼクティブにお問い合わせください。

コンテナのタイムゾーンを設定する機能

新しい環境変数のTZが追加されました。この変数を使用すると、Black Duckコンテナのタイムゾーンを変更できるため、ログのタイムスタンプをローカルタイムゾーンで表示できます。

複数のコンポーネントのバージョン/サブプロジェクトをレビューする機能

構成表レビュープロセスが一括レビューをサポートするようになり、複数の項目を一度にレビューできます。

証明書認証なしでの外部PostgreSQLインスタンスの使用をサポート

Black Duckで、外部PostgreSQLデータベースのSSLを使用した証明書認証、ユーザー名/パスワード認証、のいずれかまたはその両方をサポートするようになりました。

ライセンス管理の拡張機能

ライセンス管理テーブルでライセンスファミリを選択し、そのライセンスファミリの定義とリスクプロファイルを表示できるようになりました。

hub-proxy.envファイルの名前の変更

ファイルが管理する構成オプションが分かりやすいように、hub-proxy.envファイルの名前がblackduck-config.envに変更になりました。

2018. 11. 0にアップグレードする場合は、旧バージョンのhub-proxy.envファイルの内容を新バージョンのblackduck-config.envファイルにコピーする必要があります。

Dockerイメージファイルの名前の変更

- HubからBlack Duckへの変更にもとない、すべてのイメージの名前が変更になりました。
- サードパーティのDockerイメージを共有、再利用しやすいように、次のイメージに対する番号付けシステムが変更になり、1.0.0から開始されるようになりました。
 - cfssl
 - logstash
 - nginx
 - postgres
 - solr
 - zookeeper

APIの拡張機能

- Black Duckの登録情報用のREST API、`registration-rest-server`が新たに追加されました。
- 新しいREST API、`file-level-data-rest-server`が追加されました。ファイルレベルの著作権情報とファイルレベルのライセンスデータを返します。
- ライセンスファミリー情報用の新しいREST API、`license-family-rest-server`が追加されました。
- REST API、`component-rest-server`にフィルタ機能が追加されました。
- REST API、`license-rest-server`にフィルタおよびライセンスの責務機能が追加されました。
- REST API、`notification-rest-server`にフィルタ機能が追加されました。

今回のリリース以降、`policy-rule-rest-server` APIの最初のバージョンはサポートされなくなるので注意してください。

dependencyScanオプション

Black Duck 5.0.0リリースノートに記載されているように、`--dependencyScan`オプションが署名スキャナのコマンドラインから削除されました。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン5.0.0が日本語にローカライズされました。

バージョン2018.11.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- IE11でUIを表示すると、[バージョンの作成] ボタンがプロジェクト名ページに表示されなかった問題が修正されました。
- [ポリシーールの編集] ダイアログボックスで[キャンセル]を選択しても、ポリシーールへの編集が保存される問題が修正されました。
- 構成表を印刷しても、最初の1000コンポーネントしか印刷されない問題が修正されました。
- [グループを追加] ダイアログボックスで、[アクティブのみ] チェックボックスを指定しても、グループにフィルタがかからない問題が修正されました。
- IE11でUIを表示すると、[設定] タブが[プロジェクトのバージョン名]ページに表示されない問題が修正されました。
- カスタムコンポーネントを検索しても、すべてのコンポーネントを表示するオプションが表示されない問題が修正されました。
- 修正更新ガイダンス機能が推奨する最新の修正済みコンポーネントのバージョンが、セキュリティ脆弱性を含むバージョンよりも古いバージョンになる問題が修正されました。
- プロジェクトコードスキャナの役割と構成表マネージャの役割を持つユーザーが、UIを使用するとbdioファイルをアップロードできない問題が修正されました。
- UIで論理的でないポリシーールの作成を防止できない問題が修正されました。
- ポリシーールに[次のコンポーネント]条件を複数選択すると、コンポーネントのバージョンが[ポリシーの作成] ダイアログボックスにハイパーリンクとして表示される問題が修正されました。
- スニペットトリアーჯビュとソースビュに表示される日本語が文字化けする問題が修正されました。
- 構成表のライセンスをユーザーが編集できない問題が修正されました。

- Black Duckリリース4.5以降でコンテナをチェックするには、Black DuckでIPv6を有効にする必要があった問題が修正されました。
- JDBC接続エラーのためスキャンが失敗する問題が修正されました。

バージョン5.0.2

バージョン5.0.2の新機能および変更された機能

Black Duckバージョン5.0.2はメンテナンスリリースのため、新機能や変更された機能はありません。

バージョン5.0.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- Black Duckサーバーが、1時間ごとにJobRunnerログを大量に生成する問題が修正されました。
- プロジェクトをマッピング解除して再マッピングすると、編集が保存されないというスニペットの問題が修正されました。
- スニペットの重複を調整すると、スニペットマッチが失敗する問題が修正されました。

バージョン5.0.1

バージョン5.0.1の新機能および変更された機能

Black Duckバージョン5.0.1はメンテナンスリリースのため、新機能や変更された機能はありません。

バージョン5.0.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ユーザーが表示する権限を持っているプロジェクトが、構成表の**プロジェクトの追加メニュー**に表示されない問題が修正されました。
- `component.csv` プロジェクトバージョンのレポート作成中に、`NullPointerException`が発生する問題が修正されました。
- `ScanGraphJob`が失敗し、「Error in MAPPING_PROJECTS, Graph scan does not exist (MAPPING_PROJECTSでエラーが発生しました。グラフのスキャンが存在しません)」というエラーメッセージが表示される問題が修正されました。

バージョン5.0.0

バージョン5.0.0の新機能および変更された機能

Black Duck Binary Analysis

Black Duck - Binary Analysis (BDBA) はBlack Duckの新しいライセンス機能で、ソフトウェアライブラリ、実行可能ファイル、コードベース内で使用されているベンダー提供のバイナリの、オープンソースのセキュリティ上のリスク、コンプライアンスリスク、品質リスクを識別します。BDBAは、さまざまなファームウェア形式、ファイルシステム/ディスクイメージ、インストール形式、およびさまざまな圧縮およびアーカイブ形式など、幅広いファイルタイプをサポートしています。

Synopsys Detectを使用してソフトウェアまたはファームウェアをスキャンすると、スキャンの結果がプ

プロジェクトバージョンの構成表に表示されます。これらのファイルを容易に判定できるように、構成表にはマッチタイプがバイナリとして表示されます。

Black Duck – Binary Analysisは、Docker Compose、Docker Swarm、Kubernetesでサポートされます。

監査情報

Black Duckでは、次の監査情報を提供します。

- プロジェクトでは、次のユーザーの情報を提供します。
 - このプロジェクトを作成したユーザーおよび作成された日付。
 - このプロジェクトを最後に更新したユーザー（プロジェクト情報を変更するか、メンバーを追加することによって）と、最後に更新された日付。

この情報は、プロジェクトの[概要]タブで利用できます。

- プロジェクトバージョンでは、次の情報を提供します。
 - このプロジェクトバージョンを作成したユーザーおよび作成された日付。
 - このプロジェクトバージョン設定を最後に更新したユーザー、および最後に更新された日付。
 - このプロジェクトバージョンにマッピングされている最新のスキャンが完了した日付と時刻。
 - 最終ナレッジベース更新の日付と時刻。

この情報は、プロジェクトバージョンの[詳細]タブで利用できます。

- 目的。構成表のコンポーネントを追加または変更するときに、目的を指定できるようになりました。
- 変更。構成表にコンポーネントを追加または変更するときに、チェックボックスをオンにし、必要に応じてコンポーネントが変更された理由に関する情報を追加できます。

目的と変更ステータスをコンポーネントの条件として使用して、ポリシールールを作成できます。

ナレッジベースコンポーネントをカスタマイズする機能

構成表がプロジェクトを正確に反映するように、コンポーネントマネージャの役割を持つユーザーは次の操作を行うことができます。

- Black Duckナレッジベースコンポーネントおよび/またはBlack Duckナレッジベースコンポーネントバージョンを変更する。
- ナレッジベースコンポーネントまたはコンポーネントバージョンにメモを追加する。
- これらの変更を元に戻して、ナレッジベースデータを元の値にリセットする。
- Black Duckナレッジベースコンポーネントおよび/またはコンポーネントバージョンのステータスを定義し、承認されたコンポーネント/バージョンのみが構成表に含まれるようにする。

ポリシー管理が拡張され、コンポーネントのステータスまたはコンポーネントバージョンのステータスにポリシールールを作成できるようになりました。

直接および推移的な依存関係

Black Duckでは、直接的な依存関係と推移的な依存関係が区別されるようになりました。このため、2つの新しいマッチタイプである直接的な依存関係と推移的な依存関係が、プロジェクトバージョンの構成表に表

示されるようになりました。

リリース5.0.0より前にスキャンされたファイルについては、「ファイルの依存関係マッチ」タイプが残ります。

ログファイルの自動削除

30日より古いログファイルは、自動的に削除されるようになりました。

Black Duckでは、この値をカスタマイズするために、変数DAYS_TO_KEEP_LOGSを提供しています。

新しいジョブ

新しいジョブCodeLocationDeletionJobが追加されました。このジョブは、コードの場所について、スキャンとコードの場所のマッチを削除します。

カスタムコンポーネント管理の機能拡張

カスタムコンポーネント管理に次の機能拡張が行われました。

- カスタムコンポーネント/バージョンにタグを追加する機能。
- カスタムコンポーネント/バージョンにメモを追加する機能。
- カスタムコンポーネント/バージョンが最後に変更された日付と、最後に変更したユーザーがコンポーネント管理テーブルに追加されました。
- カスタムコンポーネント/コンポーネントのバージョンのステータスを選択する機能。デフォルトでは、カスタムコンポーネント/バージョンには[未レビュー]ステータスが設定されています。

ポリシー管理が拡張され、カスタムコンポーネントのステータス/バージョンステータスにポリシールールを作成できるようになりました。

運用リスクの機能拡張

運用リスクをより適切に管理するために、次の機能拡張が行われました。

- 過去12か月間のコミットの数、最後のコミットの日付、およびコントリビュータの数が、ナレッジベースのコンポーネントバージョンページに追加されました。
- ポリシールールが拡張され、ポリシールールを作成する際、過去1年間のコミットおよび過去1年間のコントリビュータがコンポーネントの条件として含められるようになりました。

SSOでサポートされるローカルログアウト

シングルサインオン用のSAMLを設定する際、Black Duckでローカルログアウトがサポートされるようになりました。

このオプションが有効になっている場合、Black Duckをログアウトすると、IDPのログインページが表示されます。


APIの拡張機能

- 構成表コンポーネントフィルタを取得するために、aggregate-bom-rest-serverが拡張されました。
- コンポーネントの承認ステータスとソースフィルタを取得するために、新しいREST API、component-filter-rest-serverが追加されました。
- コンポーネントバージョンの承認ステータスを取得するために、新しいREST API、component-

version-filter-rest-serverが追加されました。

- ユーザーグループに割り当てられているプロジェクトを取得するために、project-assignment-rest-server APIが拡張されました。
- プロジェクトマッピングを管理するために、新しいREST API、project-mapping-rest-serverが追加されました。
- プロジェクトタグをサポートするために、tag-rest-server APIが拡張されました。
- code-location-rest-server APIのエンドポイントには「型」フィールドがありましたが、これはリリース5.0.0で削除されました。
- コードの場所のURIの形式が変更されました。以前はファイルパスでしたが、現在はUUIDです。これらのURIを受け入れるまたは返す、すべてのAPIが影響を受けます。

構成表の変更アイコン

変更の検出を容易にするために、このアイコン () は構成表が変更されたことを示すようになりました。アイコンをポイントすると、変更の詳細が表示されます。

ライセンス管理ステータスの変更

[条件付きで承認済み] ライセンスステータスが[制限付き承認]に変更されました。

この条件を使用するすべてのポリシールールは、自動的に更新されました。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン4.8.1が日本語にローカライズされました。

5.0.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- SAMLを使用している場合にGoogleのG_Suiteが認証のためにGoogleにリダイレクトされないという問題を修正しました。
- IE 11を使用する場合にプロジェクトおよびプロジェクトバージョン設定が表示されないという問題を修正しました。
- コードスキャン制限の警告が表示されたときに、APIを使用して通知を取得できないという問題を修正しました。
- system_check.shスクリプトが失敗するという問題を修正しました。
- Black Duck UIからダウンロードしたログに、zookeeperログが含まれるようになりました。
- Kubernetesインストールの問題を修正し、webserver initスクリプトが、nginxのためにユーザー指定のsecretsのchownをスキップするようにしました。
- [プロジェクトの追加] ダイアログボックスに10件のプロジェクトのみが表示されるという問題を修正しました。
- 階層構成表をロードする際のパフォーマンスが改善されました。
- 同じプロジェクトをグループに複数回追加しようとしたときにエラーが表示されない問題を修正しました。
- [ユーザーの管理] ページのグループメンバー列に同じグループ名が複数回表示されるという問題を修正しました。

- ユーザーがアクセス権のないプロジェクトを表示できるという、ロールに関する問題を修正しました。
- スニペットマッチングが正常に終了しないという問題を修正しました。
- [プロジェクト名の設定] タブの所有者リストに100人以上のユーザーが表示されるように、問題を修正しました。
- メインプロジェクトに存在しないコンポーネントマッチタイプがサブプロジェクトにある場合に、プロジェクトの脆弱性レポートを生成する問題を修正しました。

バージョン4.8.3

バージョン4.8.3の新機能および変更された機能

Black Duckバージョン4.8.3はメンテナンスリリースのため、新機能や変更された機能はありません。

バージョン4.8.2

バージョン4.8.2の新機能および変更された機能

Black Duckバージョン4.8.2はメンテナンスリリースのため、新機能や変更された機能はありません。

バージョン4.8.2で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- スキャンへの直接リンクにアクセスすると、SSOログインページではなく、Black Duckログインページに移動する問題が修正されました。
- ファイルのスキャン時に、GraphInitializationJobエラーが発生する問題を修正しました。
- Jobrunner コンテナが絶え間なく再起動する問題を修正しました。
- ファイルのスキャンまたはアップロード時に、Black Duckスキャナが「内部サーバーエラー」を表示する問題を修正しました。
- 長い外部IDが切り捨てられる問題を修正しました。
- オフセット値が正しく計算されないという、project-rest-server APIの問題を修正しました。
- スキャンジョブでデッドロックエラーが発生する問題を修正しました。

バージョン4.8.1

バージョン4.8.1の新機能および変更された機能

Black Duckバージョン4.8.1はメンテナンスリリースのため、新機能や変更された機能はありません。

バージョン4.8.0

バージョン4.8.0の新機能および変更された機能

新しい製品名

SynopsysセキュリティポートフォリオとBlack Duck Softwareの整合性を改善するために、HubはBlack

Duckに改名されました。

プロジェクトバージョンのクローンの作成

Black Duckでは、既存のプロジェクトバージョンを選択して、そのコンポーネントやセキュリティ設定のクローンを作成して新しいプロジェクトバージョンに利用できるようになりました。クローンの作成を使用すると、既存のプロジェクトバージョンで定義した分析や解決策を、新しいバージョンのベースラインとして使用することにより作業量を削減できます。

ファイルレベルのライセンスデータ

ファイルレベルのライセンスデータを取得できるように、新しいREST APIのcomponent-license-rest-serverが追加されました。

ユーザーガイド

Black Duckドキュメントには、Black DuckのUIの使用に関する情報を載せたユーザーガイドが含まれています。

新しいジョブ

新しいジョブであるVersionBomComputationJobが追加されました。これは、バージョン構成表の計算を管理します。

プロジェクトバージョンの新しいフェーズ

「プレリリース」が、プロジェクトバージョンの新しいフェーズとして追加されました。このフェーズは、開発済みだがまだリリースされていないプロジェクトに使用できます。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン4.7.0が日本語にローカライズされました。

バージョン4.8.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- 脆弱性APIは、スコアがBlack Duckで利用可能になった時点でCVSS 2スコアを返すようになりました。
- グローバルコードスキャナの役割を持つユーザーが作成したレポートを削除できない問題を修正しました。
- Black Duck UIを使用してLDAPを設定したユーザーが、502エラーコードメッセージを受信する問題を修正しました。
- 行がすでに展開されていると、レポートの行が誤って表示される問題を修正しました。
- データベースのバックアップがシンボリックリンクを受け付けられない問題を修正しました。
- スーパーユーザーの役割を持つユーザーがプロジェクトを表示できない問題を修正しました。
- 構成表比較ページのページレイアウトの問題を修正しました。

バージョン4.7.2

バージョン4.7.2の新機能および変更された機能

階層構成表

階層構成表はデフォルトで無効になっています。この機能を有効にするかどうかを制御する新しい環境変数、`HIERARCHICAL_VERSION_BOM`が追加されました。

バージョン4.7.1

バージョン4.7.1の新機能および変更された機能

コンポーネントダッシュボードのフィルタ

フィルタが適用されたときの、コンポーネントダッシュボードの動作が変更されました。高度なフィルタを使用するか、またはリスクグラフを使用して値を選択することによって、リスクでフィルタにかけられることを選択した場合、次のようになります。

- リスクグラフには、フィルタカテゴリで値が選択されていない場合は0の値が表示されます。
- その他のリスクカテゴリを表す値には、選択したフィルタに対応する値が表示されます。

たとえば、高リスクライセンスのコンポーネントのみを表示するようにコンポーネントダッシュボードをフィルタにかけると選択した場合、ライセンスリスクが中、低、なしのリスクグラフには0の値が表示され、セキュリティ上のリスクと操作上のリスクについてのリスクグラフには、高リスクライセンスのコンポーネントに対応する値が表示されます。

バージョン4.7.1で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- ブラウザの言語設定が日本語の場合に正しく表示されるように、Black Duckスキャナのラベルが修正されています。
- プロジェクトバージョンの[セキュリティ]タブのパフォーマンスが向上しました。
- コメントが保存され、コメントアイコンが表示される前に、構成表テーブルの行が移動する問題を修正しました。
- [構成表]ページのヒントが閉じない問題を修正しました。
- 大きいヘッダーが原因で、NGINXから400の不正な要求エラーが発生する問題が修正されました。
- グローバルコードスキャナまたはプロジェクト作成者の役割を持つユーザーが[影響を受けるプロジェクト]タブに「結果が見つかりません」というメッセージを受信する問題を修正しました。
- 多数のコンポーネントを表示するときの、コンポーネントダッシュボードのパフォーマンスが向上しました。
- 多数のバージョンを表示するときの、[プロジェクトバージョン]ページのパフォーマンスが向上しました。

バージョン4.7.0

バージョン4.7.0の新機能および変更された機能

カスタムコンポーネント

構成表がプロジェクトを正確に反映するように、Black Duckではカスタムコンポーネントを作成できるようになりました。これにより、たとえばプロジェクトでBlack Duck KBによって追跡されていないオープンソースコンポーネントを使用している場合、構成表でBlack Duckナレッジベースにはないコンポーネントを使用できます。

Note: Black Duckナレッジベースで管理されているオープンソースコンポーネントのバージョンがない場合は、Black Duckカスタマサポートにお問い合わせください。

コンポーネントのソースを識別するために、**ソース/タイプ**という新しい列がプロジェクトバージョンレポートの`component.csv`ファイルに追加されました。この列の値は、KB_COMPONENT（Black Duckナレッジベースコンポーネントの場合）またはCUSTOM_COMPONENT（カスタムコンポーネントの場合）です。

新しいコンポーネントマネージャの役割

4.7.0で追加された新しいカスタムコンポーネント機能に対応するために、コンポーネントマネージャという新しい役割がBlack Duckに追加されました。この役割を持つユーザーは、カスタムコンポーネントを作成、編集、または削除することができます。

構成表の階層表示

Black Duckでは、ファイルシステムの関係に基づく階層表示を提供します。この表示を使用して、親コンポーネントと親コンポーネントによって取り込まれた子サブコンポーネントを示します。

構成表の階層表示では、新しいジョブHierarchicalVersionBomJobが作成され、構成表の階層バージョンが更新されました。

新しいプロジェクトフィールド

新しいオプションのフィールドがプロジェクトに追加されました。このフィールド、**アプリケーションID**を使用して、資産管理システムやアプリケーションカタログなどの外部システムに、プロジェクトの外部マッピングIDを格納することができます。

ポリシーの上書きまたは上書きの削除にコメントを追加する機能

Black Duckでは、ポリシーの上書きまたは上書きの削除にコメントを追加する機能をサポートするようになりました。

構成表比較の強化

構成表比較機能が強化され、プロジェクト間で構成表を比較できるようになりました。

スニペットの一括編集機能

スニペットが強化され、[ソース]タブでスニペットの一括編集が可能になりました。

APIの拡張機能

REST APIに、次の改良が加えられました。

- component-rest-server APIとcomponent-version-rest-server APIが拡張され、カスタムコンポーネントを管理できるようになりました。
- 構成表を比較するために、新しいREST API、project-version-bom-comparison-rest-serverを追加しました。

Protex BOMツール

レガシー製品からBlack Duckの最新バージョンにユーザーを移行するための継続的な取り組みの一環として、Protex BOMをインポートする[ツール]ページのリンクが、Black Duckの4.7.0以降のバージョンから削除されています。Protex BOMをインポートするには、次のURLを指定してProtex BOMツールzipファイルをダウンロードします: <https://<Black Duck hostname>/download/scan.protex.cli.zip>

ジョブへの変更

ProtexBomJobは、次のジョブに置き換えられました。

- GraphCompletionJob - 他のスキャン/グラフジョブが終了するまで待機してから、ScanCompletedJobを開始します。
- GraphInitializationJob - Black Duckにアップロードされた各スキャンドキュメントを結合して正規化します。
- ScanCompletedJob - コードの場所をプロジェクトにマップし、ScanAutoBomJobを開始します。
- ScanMappingJob - コンポーネント識別子をBlack Duck識別子にマップします。
- ScanSignatureJob - スキャンしたすべてのファイルの署名を計算します。

日本語

UI、オンラインヘルプ、およびリリースノートのバージョン4.6.1が日本語にローカライズされました。

バージョン4.7.0で修正された問題

このリリースでは、お客様から報告された次の問題が修正されています。

- 再スケジュールされた孤立ジョブのスキャンステータスが「失敗」に更新されないという問題を修正しました。
- 特定の日付範囲の脆弱性レポートに、更新も変更もされていない脆弱性が含まれているという問題を修正しました。
- [スキャン名]ページの[次により開始されたスキャン]フィールドにデータが入力されないという問題を修正しました。
- [ジョブ]ページに表示されているジョブステータスが間違っている場合があるという問題を修正しました。
- アポストロフィなどの特殊文字が、ユーザー名で文字のURLエンコードを表示するという、グループメンバーテーブルの問題を修正しました。
- [影響を受けるプロジェクト]タブの問題が修正され、コンポーネントとプロジェクトが正しくソートされるようになりました。
- Internet Explorer 11を使用している場合、Black Duck UIでスキャンがアップロードされないという問題を修正しました。
- 暗号文が有効になっていないと、createVersionReport APIが正常に動作しないという問題を修正しました。

- 2ステップのプロセスを使用してスキャンした後に、スキャンをプロジェクトにマップすると、構成表に「結果が見つかりません」というメッセージが表示されるという問題が修正されました。
- スキャンの状態が「完了」になった後に、大きなスキャンファイルがアップロードされ、プロジェクトのバージョンにリンクされた場合、構成表にデータが入力されないという問題を修正しました。
- Sysadminユーザーをプロジェクトメンバーとして追加できないという問題を修正しました。
- ポリシールールのコピーを妨げていたUIの問題を修正しました。
- KbReleaseUpdateJobが失敗し、Black Duckナレッジベースが応答しないという問題を修正しました。
- 構成表のコンポーネントバージョンの状態が「レビュー済み」のときに400エラーコードを返す findBomComponentVersion APIの問題を修正しました。

Black Duckの既知の問題と制限事項は次のとおりです。

- [コンポーネント名]ページの[概要]タブには、CVSS 3.0 (NVDまたはBDSA) データの表示を選択した場合でも、CVSS 2.0データが表示されます。
- REST API開発者ガイドのドキュメントに記載されているメディアの種類が完全ではない可能性があります。
- パフォーマンスの問題が発生した場合は、次の手順を実行します。
 1. Dockerコンテナを実行しているサーバーにログインします。
 2. コンテナIDを確認します。

```
docker ps | grep postgres
```
 3. Dockerコンテナに対し、PostgreSQLを起動します。

```
docker exec -it <container id> psql -d bds_hub
```
 4. Postgresプロンプトで、次のクエリを実行します。

```
ALTER SYSTEM SET max_wal_size = '8GB'
```
 5. Black Duckを再起動します。
- ユーザーの認証にLDAPディレクトリサーバーを使用している場合は、次の点を考慮してください。
 - Black Duckは、単一のLDAPサーバーをサポートしています。複数のサーバーはサポートされていません。
 - ユーザーがディレクトリサーバーから削除されても、Black Duckユーザーアカウントはアクティブと表示され続けます。ただし、認証情報は有効ではなくなり、ログインに使用できません。
 - グループがディレクトリサーバーから削除されても、Black Duckグループは削除されません。グループは手動で削除してください。
- タグ付けでは、文字、数字、プラス (+) および下線 (_) のみがサポートされています。
- Black Duckがユーザーを認証している場合、ログイン中にユーザー名の大文字と小文字は区別されません。LDAPユーザー認証が有効になっている場合、ユーザー名の大文字と小文字は区別されます。
- コードの場所に大規模な構成表がある場合、コードの場所を削除すると、ユーザーインターフェイスのタイムアウトエラーで失敗することがあります。