BLACKDUCK

BY SYNOPSYS®

リリースノート

バージョン2020.2.0

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2020.2.0を対象としています。

本ドキュメントは2020年4月9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

目次

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 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。

章 1: 製品発表

バージョン2020.2.0の発表

個別のファイルマッチ

事前に通知したとおり、あいまいマッチによる誤検出を減らすために、署名スキャンの一環としての個別のファイルマッチの実行は、Black Duck CLIおよびSynopsys Detectスキャンのデフォルト動作ではなくなりました。

個別のファイルマッチでは、1つのファイルのチェックサム情報のみに基づいてコンポーネントを識別します。Black Duckでは、少数のファイル拡張子のセット（.js、.apklib、.bin、.dll、.exe、.o、.so）を対象に、定期的に署名スキャンを行い、1つのファイルに一致するチェックサムに基づいてファイルとコンポーネントをマッチングします。残念ながら、このマッチは常に正確であるとは限らず、かなりの量の誤検出が発生しました。広範なSynopsys顧客ベース全体にわたり開発者のエクスペリエンスを向上させるために、個別のファイルマッチはデフォルト動作ではなくなり、現在では、オプション機能になっています。

2020.2.0にアップグレードすると、個別のファイルマッチがオフになり、一部のコンポーネントが構成表から削除される場合があります。構成表への影響を推定するには、マッチタイプを「完全ファイル」に限定してコンポーネントを探し、構成表から削除される可能性のあるコンポーネントを確認してください。Dockerイメージをスキャンする場合、「完全ファイル」マッチはこの変更の影響を受けません。ご注意ください。

署名スキャナには、個別のファイルマッチを有効にする新しいパラメータがあります。スキャンにSynopsys Detectを使用している場合、バージョン6.2には、個別のファイルマッチのオン/オフをサポートする新しいパラメータがあり、デフォルトは[オフ]になっています。

Docker Composeのサポート

事前に通知したとおり、2020.2.0リリースでDocker Composeはサポートされるオーケストレーションメソッドではなくなりました。

バージョン2019.12.0の発表

Black Duckのアップグレード

アップグレードプロセス中には、レポートデータベースに加えられた変更の一環として、移行スクリプトが実行され、使用しなくなったaudit_eventテーブルの行が削除されます。この移行スクリプトは、audit_eventテーブルのサイズに応じて、実行に多少時間がかかる場合があります。目安としては、サイズが350 GBのaudit_eventテーブルで約20分かかりました。

監査イベントテーブルのサイズを確認するには、次の手順に従います。

次のいずれかを実行します。

- bds_hubデータベースから次のコマンドを実行します。

  ```
  SELECT pg_size_pretty( pg_total_relation_size('st.audit_event') );
  ```

- システム管理者の役割でBlack Duck UIにログインし、次の手順を実行します。

  1. 展開式のメニューアイコン  をクリックして、**[管理]**を選択します。

     [管理]ページが表示されます。

  2. **[システム管理]**を選択して[システム情報]ページを表示します。
  3. ページの左側の列で**[db]**を選択します。
  4. **[テーブルサイズ]**セクションまでスクロールします。audit_eventテーブル名のtotal_tbl_size値を見ます。

オンプレミスのKubernetesおよびOpenShiftユーザーの場合は、アップグレードする前にライブネスチェック（--liveness-probes false）を無効にし、Black Duckをアップグレードしてから、ユーザーインターフェイスが表示されるまで待ちます。ユーザーインターフェイスが表示されたら、ライブネスチェック（--liveness-probes true）を有効にします。

Synopsysでは、移行スクリプトの実行後に、audit_eventテーブルでVACUUMコマンドを実行して、PostgreSQLのパフォーマンスを最適化することを*強くお勧め*します。

- システムの使用法によっては、VACUUMコマンドを実行すると、Black Duckで使用されなくなった大容量のディスク領域を再利用できます。
- このコマンドを実行すると、クエリのパフォーマンスが向上します。

Note: VACUUMコマンドを実行しないと、パフォーマンスが低下する場合があります。

このコマンドには、audit_eventテーブルが現在使用しているディスク領域の2倍のディスク領域が必要になる点に注意してください。

Important: VACUUMコマンドを実行するのに十分なスペースがあることを確認する必要があります。領域が不足すると、ディスク領域を使い果たして、データベース全体を破損させる可能性があります。

コンテナ化されたPostgreSQLデータベースの導入を使用しているDocker ComposeおよびDocker Swarmerユーザーの場合は、次の手順でVACUUMコマンドを実行します。

1. 前述のとおり、audit_eventテーブルのサイズを確認します。
2. 次のコマンドを実行して、PostgreSQLコンテナのコンテナIDを確認します。

   ```
   docker ps
   ```

3. PostgreSQLコンテナを管理するには、次のコマンドを実行します。

```
docker exec -it <container_ID> psql bds_hub
```

4. 次のコマンドを実行します。

```
VACUUM FULL ANALYZE st.audit_event;
```

外部PostgreSQLデータベースの導入を使用しているDocker ComposeおよびDocker Swarmユーザーの場合：audit_eventテーブルのサイズを確認して、VACUUMコマンドを実行し、完了したら、導入を再起動します。

オンプレミスのKubernetesおよびOpenShiftユーザーの場合、詳細については、Synopsys Operatorのアップグレード手順を参照してください。

今後の2020.2.0リリースでの個別のファイルマッチ

あいまい一致による誤検出を減らすために、Black Duckバージョン2020.2以降では、署名スキャンの一環としての個別のファイルマッチの実行は、Black Duck CLIおよびSynopsys Detectスキャンのデフォルト動作ではなくなりました。

個別のファイルマッチでは、1つのファイルのチェックサム情報のみに基づいてコンポーネントを識別します。Black Duckでは、少数のファイル拡張子のセット（.js、.apklib、.bin、.dll、.exe、.o、.so）を対象に、定期的に署名スキャンを行い、1つのファイルに一致するチェックサムに基づいてファイルとコンポーネントをマッチングします。残念ながら、このマッチングは常に正確であるとは限らず、かなりの量の誤検出が発生します。このような誤検出が発生すると、構成表の確認と調整にさらに労力を費やす必要があります。構成表でこのレベルの精度と粒度を必要とするユーザーもいますが、大半の顧客はこのレベルのマッチングは望んでいないか、必要としていません。したがって、顧客および現場からの意見に基づき、広範なSynopsys顧客ベース全体にわたり開発者のエクスペリエンスを向上させるために、個別のファイルマッチはデフォルト動作ではなくなりオプション機能になります。

これにより、一部のコンポーネントが構成表から削除される可能性があります。これらのコンポーネントは必要な場合もあれば、不要な場合もあります。したがって、Synopsysでは、Black Duck 2020.2リリースから、CLI、Synopsys Detect、Synopsys Detect（Desktop）を含む個別のファイルマッチを再度有効にできるようにするためのメカニズムを提供します。

Docker Composeのサポート

2019年12月31日付けで、Docker Composeのサポートは終了となります。

バージョン2019.10.0の発表

レポートデータベースの再設計

レポートデータベースは、お客様がBlack Duckからのデータに対してサードパーティのBI/レポートツールを使用できるようにする、Black Duckの機能です。レポートデータベースの管理、安定性、機能性を向上させるために、2019.10.0リリースでは、レポートデータベースにいくつかの重要な変更が加えられました。レポートデータベースを使用する場合、レポートデータベースを中断することなく継続的に使用するためには、これらの更新についてお客様の側で作業と変更が必要になります。

レポートデータベースを素早く作成、使用、バックアップ、リストアできるように、別個のレポートデータ

ベース（bd_hub_report）の表が、Black Duckデータベース（bds_hub）のreportingスキーマに移動されました。デフォルトの更新頻度は8時間ごと（この値は調整可能）です。さらに、レポートデータベースに新しい情報も追加し、ファイル/ディレクトリマッチおよびパッケージマッチ情報を含むレポートも作成できるようになりました。この機能強化の結果、レポートデータベースをご使用のお客様には、任意のツール/ユーティリティ/クエリのデータベース接続文字列を、bds_hubデータベースを指すようにして、bd_hub_reportデータベースを使用しなくなるように変更していただく必要があります。古いデータベースの表は削除されているため、データベース接続文字列がbds_hubデータベースを指すように変更しない限り、レポート（またはクエリ）は失敗します。

2019.10.0リリース以降、Black Duckで行った変更がレポートデータベースに反映されるまでには遅延が生じることに注意してください。この遅延の時間は、新しいBLACKDUCK_REPORTING_DELAY_MINUTES環境変数を使用して指定した値（デフォルトでは8時間）に応じて異なります。オンプレミス環境にBlack Duckをインストールしているお客様は、この頻度の変更方法について、ご使用のプラットフォームに該当するインストールガイドでご確認いただけます。ホストされるお客様がこの値を変更する場合は、Synopsysサポートにご連絡いただく必要があります。

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VulnerabilityRepriortizationJob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、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ーです。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。

章 2: リリース情報

バージョン2020.2.0

バージョン2020.2.0の新機能および変更された機能

個別のファイルマッチ

署名スキャンの一環としての個別のファイルマッチは、Black Duck CLIおよびSynopsys Detectスキャンのデフォルト動作ではなくなりました。

この変更により、一部のコンポーネントが構成表から削除される可能性があります。これらのコンポーネントは必要な場合もあれば、不要な場合もあります。したがって、Black Duck 2020.2.0リリースでは、個別のファイルマッチを再度有効にできます。

署名スキャナに新しいパラメーター**--individualFileMatching**が追加されました。これには、個別のファイルマッチを有効にできる3つのオプションがあります。

- **source**。次の拡張子のファイルでのみ、個別のファイルマッチを実行します。 `.js`.
- **binary**。次の拡張子のファイルで、個別のファイルマッチを実行します。`.apklib`、`.bin`、`.dll`、`.exe`、`.o`、`.so`
- **all**。次の拡張子の全ファイルで、個別のファイルマッチを実行します。`.js`、`.apklib`、`.bin`、`.dll`、`.exe`、`.o`、`.so`

スキャンにSynopsys Detectを使用している場合、バージョン6.2には、個別のファイルマッチのオン/オフをサポートする新しいパラメータがあり、デフォルトは[オフ]になっています。

Docker Compose

Docker Composeのサポートが終了したため、Docker Composeディレクトリがディストリビューションから削除され、『*Docker Composeを使用したBlack Duckのインストール*』ガイドが提供されなくなりました。

埋め込みライセンスの検出

Black Duckコンポーネントに対してBlack Duckナレッジベースで宣言されていない埋め込みオープンソースライセンスのインスタンスを検出できるようになりました。

コードスキャン時にDeep License Dataの検出を有効にすることで、ライセンスコンプライアンスに重点を置いたユーザーは、オープンソースで検出されたライセンスを表示して、問題のあるライセンスがないこと、およびすべてのライセンスが構成表に記述されていることを確認できます。

この機能を使用して、Black Duckはライセンス文字列のテキスト検索を実行し、見つかったライセンスを

[ソース]タブに表示します。

必要に応じてソースファイルをアップロードし、構成表レビュー担当者が検出されたライセンステキストを**[ソース]**タブ内から表示できるようにします。

署名スキャナには、埋め込みライセンスの検索を可能にする新しいパラメーター**--license-search**があります。Deep License Dataの検出を有効にするプロパティは、Synopsys Detectバージョン6.2以降で使用できます。

レポートに追加されたDeep License Data

コンポーネントプロジェクトバージョンレポートcomponents_*date*_#.csv、およびコンポーネント追加フィールドレポートbom_component_custom_fields_*date*_#.csvが機能強化され、Deep License Dataが含まれるようになりました。

新しい列は次のとおりです。

- Deep License ID
- Deep License名
- Deep Licenseファミリ

これらのフィールドは、components_*date*_#.csvレポートの最後、およびbom_component_custom_fields_*date*_#.csvレポートのカスタムフィールド列の前に追加されました。

またはDeep License Dataは、通知ファイルレポートに追加されました。この情報は、コンポーネントに対して表示されるライセンスリスト（レポートの**[コンポーネント]**セクションの表示と同じ）、およびレポートで表示されるライセンステキストで確認できます。

セキュリティプロジェクトバージョンレポートに追加された詳細情報

security_*date_time*.csvレポートが拡張され、次のフィールドがレポートの最後に追加されました。

- 総合スコア
- CWE ID
- ソリューションが利用可能
- 回避策が利用可能
- 攻撃が利用可能

通知レポートにおける著作権レポートの表示形式の改善 - ベータ版

通知レポートでは、著作権レポートの表示形式がさらに改善されました。この機能は*オプション*で、現在はベータ版の機能です。

新プロジェクトのバージョン構成表フィルタ

構成表ページに新しいフィルタが追加され、表示するコンポーネントをコメントの有無で絞り込めるようになりました。

プロジェクトバージョン[セキュリティ]タブ

プロジェクトバージョンの**[セキュリティ]**タブに表示されるテーブルに、**[公開済み]**列が追加されました。

統合されたジョブ

ジョブのスケジュールを改善するため、次のジョブに代わって新しいジョブKbUpdateJobが導入されます。

- KbComponentUpdateJob
- KbVersionUpdateJob
- KbVulnerabilityUpdateJob
- KbVulnerabilityBdsaUpdateJob

外部のPostgreSQLデータベース

外部のPostgreSQLデータベースを使用している場合、Synopsysは、パフォーマンス関連の修正が含まれているため、バージョン9.6.16へのアップグレードを推奨しています。これは、データベースコンテナ内のバージョンです。

また、サードパーティのデータベースプロバイダが許可している場合、Synopsysは、外部のPostgreSQLユーザーが次のコマンドを実行してデータベースを調整することを推奨しています。

```
alter system set autovacuum_max_workers = 8 ;
alter system set autovacuum_vacuum_cost_limit = 800 ;
```

次にPostgreSQLを再起動します。

サードパーティのデータベースプロバイダが調整を許可していない場合は、何もする必要はありません。

マップされていないコードの場所

Black Duckは現在、プロジェクトバージョンにマップされていないコードの場所を対象として、クリーンアップのスケジュール機能を提供しています。`blackduckconfig.env`ファイルでBLACKDUCK_HUB_UNMAPPED_CODE_LOCATION_CLEANUPおよびBLACKDUCK_HUB_UNMAPPED_CODE_LOCATION_RETENTION_DAYSプロパティを設定します。

APIの拡張機能

- マッチした新しいコンポーネントのエンドポイント：

  /api/projects/{projectId}/versions/{projectVersionId}/matched-components

- ここで、次のエンドポイントはmatchConfidencePercentageを返します。

  /projects/{projectId}/versions/{projectVersionId}/matched-files

- 次の新しい脆弱性レポートエンドポイントでは、作成されたすべての脆弱性レポートのステータスが表示されます。

  /api/vulnerability-reports

- 次のエンドポイントの目的は、既存の修正ガイダンス機能を代替することです。

  /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance

  /api/components/{componentId}/versions/{componentVersionId}/origins/{originId}/upgrade-guidance

- 無視されたフィールドを脆弱な構成表コンポーネントエンドポイントに追加しました。この追加により、無視されたコンポーネントと無視されないコンポーネントに基づいて、フィルタにかけられるようになります。

  GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-components

サポートされるブラウザのバージョン

- Safariバージョン13.0.4（14608.4.9.1.4）
- Chromeバージョン80.0.3987.100（公式ビルド）（64ビット）
- Firefoxバージョン72.0.2（64ビット）
- Internet Explorer 11.657.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

コンテナのバージョン

- blackducksoftware/blackduck-postgres：1.0.11
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash：1.0.6
- blackducksoftware/blackduck-zookeeper：1.0.3
- blackducksoftware/blackduck-nginx：1.0.17
- blackducksoftware/blackduck-upload-cache：1.0.12
- blackducksoftware/blackduck-authentication:2020.2.0
- blackducksoftware/blackduck-webapp:2020.2.0
- blackducksoftware/blackduck-scan:2020.2.0
- blackducksoftware/blackduck-jobrunner:2020.2.0
- blackducksoftware/blackduck-registration:2020.2.0
- blackducksoftware/blackduck-documentation:2020.2.0
- sigsynopsys/appcheck-worker：2019.12
- blackducksoftware/rabbitmq：1.0.3

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2019.12.0が日本語にローカライズされました。

2020.2.0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。

- （Hub-20742）。[影響を受けるプロジェクト]ページのデータを取得するために、クエリを最適化しました。
- （Hub-20821）。コンポーネントまたはプロジェクトを追加すると、Black Duck検索サービスが利用できなくなると通知するエラーメッセージが表示されていましたが、このメッセージの原因となる問題を修正しました。

- （Hub-21833）。ユーザーが自分のプロジェクトだけでなく、すべてのプロジェクトのコンポーネントを表示できたというフィルタの問題を修正しました。
- （Hub-22181）。**[ソース]**タブでコンポーネント名とバージョンのリンクが欠落していた問題を修正しました。
- （Hub-22267）。脆弱性レポートの**[作成者列]**が空であった問題を修正しました。
- （Hub-22310）。脆弱性のベーススコアがUIとエクスポートされたレポートで異なっていた問題を修正しました。
- （Hub-22335）。グローバルプロジェクトビューアの役割が割り当てられていない場合、ユーザーはカスタムフィールドを表示できませんでしたが、この問題を修正しました。
- （Hub-22380）。プロジェクトバージョンのクローン作成後、ポリシーが上書きされたにもかかわらず、ポリシー違反の通知がトリガーされていましたが、この問題を修正しました。
- （Hub-22466）。プロジェクト所有者の選択時に非アクティブユーザーが非表示にならなかった問題を修正しました。
- （Hub-22510）。コンポーネントを追加または編集するときにカスタムコンポーネントが見つからなかった問題を修正しました。
- （Hub-22615）。KBreleaseupdatejobが継続的に失敗する問題を修正しました。
- （Hub-22626）。スキャンがポストスキャンフェーズであったにもかかわらず、処理結果がBlack Duckに正常にアップロードされていた問題を修正しました。
- （Hub-22677）。コンポーネントの無視を解除できない問題を修正しました。
- （Hub-22681）。スニペットを含むサブプロジェクトを追加すると、サブプロジェクトのコンポーネント数が不適切に変化していた問題を修正しました。
- （Hub-22709）。ポリシーの作成時にドロップダウンプロジェクトのカスタムフィールドに10個の値しか表示されなかった問題を修正しました。
- （Hub-22805）。`source_date_time.csv`レポートが空であった問題を修正しました。
- （Hub-22811）。外部データベースと一緒にBlack Duckをインストールしようとすると、「役割 "blackduck_user"が存在しません」というメッセージが表示されていましたが、この問題を修正しました。
- （Hub-22850）。`license_term_fulfillment_date_time.csv`レポートが空であった問題を修正しました。

バージョン2019.12.1

バージョン2019.12.1の新機能および変更された機能

SSOセキュリティの強化

Black Duckは、Black Duckとシングルサインオン（SSO）プロバイダ間の通信セキュリティを強化しました。現在、Black Duckでは、SSO IDプロバイダ（IdP）の設定時に、署名付き応答の一部としてアサーション署名を提供する必要があります。Synopsysは推奨していませんが、IdPがこの署名を提供できない場合、この追加されたセキュリティを無効にすることができます。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。

APIの機能強化

- 新しいAPIでは、脆弱性の修正ステータスが更新されます。構成表コンポーネントバージョンの脆弱性修正により、ユーザーは脆弱性修正ステータスの読み取り/更新を実行したり、コメントを追加したりできるようになりました。

  取得元の情報なしで追加されたコンポーネントには、次の方法でアクセスできます。

  ```
  https://.../api/projects/{projectId}/versions/{versionId}/components/
  {componentId}/versions/{componentVersionId}/vulnerabilities/
  {vulnerabilityId}/remediation
  ```

  取得元の情報とともに追加されたコンポーネントには、次の方法でアクセスできます。

  ```
  https://.../api/projects/{projectId}/versions/{versionId}/components/
  {componentId}/versions/{componentVersionId}/origins/{originID}/vulnerabilities/
  {vulnerabilityId}/remediation
  ```

コンテナ情報

2019.12.0リリースノートには、誤ったバージョンでblackducksoftware/blackduck-upload-cacheコンテナがリストされていました。正しいバージョンはblackducksoftware/blackduck-upload-cache:1.0.12です。

2019.12.1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。

- （Hub-21861）。アップグレード後にコードの場所が「破損した」問題を修正しました。
- （Hub-22091）。バージョン2019.12.0へのアップグレード後に、`scan.cli`でスキャンが失敗していた問題が修正されました。
- （Hub-22737、22851）。パラメータが多過ぎることを通知するエラーメッセージでジョブが失敗していましたが、この問題を修正しました。
- （Hub-22781）。[コンポーネントの編集]ダイアログボックスにコンポーネント情報またはライセンス情報が読み込まれなかった問題を修正しました。

バージョン2019.12.0

バージョン2019.12.0の新機能および変更された機能

Black Duck UIの機能強化

このリリースでは、Black Duck UIのナビゲーションが全般的に改善されています。強化された機能には、次のような機能があります。

- 新しい固定のナビゲーションシステムがページの左側のセクションに表示されます。メニューオプションは次のとおりです。
  - 

。最後に表示したダッシュボードが表示されます。

- 

。直近の検索結果を表示するための新しいメニューオプション。
- 

。[スキャン]ページを表示します。
- 

。[レポート]ページを表示します。
- 

。新しいメニューオプションでは、次の項目を選択できます。コンポーネント管理、カスタムフィールド管理、ライセンス管理、またはポリシー管理。
- 

。[管理]ページを表示します。 

オプションを使用してカスタムフィールドを管理できるようになりました。

- 上部のナビゲーションバーにある新しい[ヘルプ]メニューから、Black Duckのオンラインヘルプ、統合ヘルプ、APIドキュメントに簡単にアクセスできます。
- ユーザーアクセストークンの管理は、[マイプロファイル]ページから個別のページに移動されました。このページには、上部のナビゲーションバーにあるユーザーメニューからアクセスできます。
- [ツール]ページが更新されました。
- 新しいフィルタオプションとして[Ignoreパターンをマッチ]が[構成表]ページに追加されました。

プロジェクトバージョンの[セキュリティ]タブの再設計

プロジェクトバージョンの**[セキュリティ]**タブが再設計され、新しいレイアウト、新しいフィルタ、新しい列が脆弱性テーブルに追加されました。

CWE IDと、脆弱性に対する攻撃、回避策、またはソリューションが存在するかどうかを、ドリルダウンしてこの情報を表示する必要なく、すばやく確認できるようになりました。

ディープレベルのライセンスデータ

Black Duckでは、オープンソースコンポーネントに存在する可能性のあるDeep License（サブライセンスまたは埋め込みライセンスとしても知られる）を管理する機能が提供されます。このDeep License Dataを管理することで、ライセンス違反のリスクが軽減され、使用しているオープンソースでのDeep Licenseとそのリスクをより容易に把握してレポートすることができます。

Deep License Dataはデフォルトでは無効になっています。Deep License Dataを構成表コンポーネントに含めることを有効にする必要があります。有効にすると、Black Duckナレッジベースによって決定されたDeep Licenseが自動的にアクティブになります。

Note: コンポーネントの数とDeep Licenseの数によっては、Deep License Dataの表示を有効にすると、構成表の計算スキャン時間に影響する場合があります。Deep License Dataを構成表に追加すると、ライセンスリスクに影響を及ぼし、ポリシー違反が発生する可能性があります。

著作権データを通知レポートに含める - ベータ版

Black Duckナレッジベースから取得した重複排除された著作権情報を通知レポートに含めるオプションが利用できるようになりました。これにより、通知レポートに、使用するオープンソースコンポーネントの著

作権保有者の完全なリストを容易に含めることができます。

この機能はオプションで、現在はベータ版の機能であるため、結果として書式化が不十分な著作件情報が含まれたり、著作件情報が欠落したりしている場合があります。既知の問題は、特殊文字を含む著作権情報が途中で切り捨てられてしまうことです。Synopsysは、今後のリリースで、著作権の検出とレポート作成に関する機能を追加していく予定です。

エラーや改善点に関するご意見/ご要望は、Synopsysの担当者またはカスタマーサポート部門宛てにお送りください。

カスタムライセンスファミリの機能強化

- 混乱を避けるために、制限付きサードパーティプロプライエタリライセンスファミリーは限定的サードパーティプロプライエタリに名称が変更されました。
- ナレッジベースライセンスは、限定的サードパーティプロプライエタリライセンスファミリに関連付けられるようになりました。これはライセンスのリスクに影響し、ポリシー違反を引き起こす可能性があります。

ポリシー管理の機能強化

ポリシー管理では、次の脆弱性の条件に基づいてポリシールールを作成する機能が提供されます。

- CWE ID
- 攻撃が利用可能
- 総合スコア
- ソリューションが利用可能
- 回避策が利用可能

レポートデータベースの機能強化

プロジェクト、プロジェクトバージョン、構成表コンポーネントのカスタムフィールドの`bds_hub`の`reporting`スキーマに新しいビューが追加されました。

構成表ステータス

プロジェクトバージョンの構成表ページ（プロジェクトバージョン**[コンポーネント]**タブとしても知られる）のヘッダーには、コンポーネントのステータスが含まれ、構成表を更新する処理が行われているかどうかが示されます。

カスタムスキャン署名

カスタムスキャン署名機能をすべてのお客様が利用できるようになりました。

カスタムフィールドの機能強化

Black Duckでは、カスタムフィールドを削除する機能が提供されるようになりました。

APIの機能強化

- カスタムフィールドがポリシーで使用されている場合、それらのカスタムフィールドは削除されません。

カスタムフィールドがポリシーで使用されている場合は、カスタムフィールドの削除エンドポイントがエラーを返します。

非ルートユーザーID/グループIDのサポート

このリリースでは、Kubernetesの.yml構成ファイルで、非ルートユーザーID/グループIDを使用したBlack Duckイメージの実行がサポートされるようになりました。

サポートされるブラウザのバージョン

- Safariバージョン13.0.3（14608.3.10.10.1）
- Chromeバージョン78.0.3904.108（公式ビルド）（64ビット）
- Firefoxバージョン71.0（64ビット）
- Internet Explorer 11.476.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

コンテナの変更

- blackducksoftware/blackduck-postgres：1.0.10
- blackducksofware/blackduck-cfssl：1.0.1
- blackducksoftware/blackduck-logstash：1.0.5
- blackducksoftware/blackduck-zookeeper：1.0.3
- blackducksoftware/blackduck-nginx：1.0.14
- blackducksoftware/blackduck-upload-cache：1.0.11
- sigsynopsys/appcheck-worker：2019.12
- blackducksoftware/rabbitmq：1.0.2

名前が変更されたジョブ

KbReleaseUpdateJobは、ジョブの目的をより明確にするために、KbVersionUpdateJobに名前が変更されました。

新しい監査イベント

Black Duckナレッジベースでコンポーネントまたはコンポーネントバージョンが非推奨になると、監査イベントが表示されるようになりました。

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2019.10.0が日本語にローカライズされました。

2019.12.0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。

- （Hub-13468）。Black Duck UIに表示される使用回数の値が正しくなかった問題が修正されました。

- （Hub-16211、16713、17562）。構成表は最新と表示されるにもかかわらず、処理が引き続き行われていた問題が修正されました。
- （Hub-16950）。webappコンテナから外部イメージを削除しました。
- （HUB-17685）。レビュー済みコンポーネントのポリシー違反が発生しなくなった後に、ポリシー違反ステータスが更新されなかった問題を修正しました。
- （Hub-17841）。scans.csvプロジェクトバージョンレポートで、[スキャンID]フィールドにコードの場所IDが表示されていた問題が修正されました。
- （Hub-18257）。Black Duckからgravatarを削除しました。
- （Hub-18978）。コンポーネントをプロジェクトバージョンから削除できなかった問題が修正されました。
- （Hub-20997、21968）。すべてのマッチしたコンポーネントが[スキャン]>[コンポーネント]ページに表示されなかった問題が修正されました。
- （Hub-21205）。**[ソース]**タブでマッチ結果を表示しようとすると、入力解析リクエストエラーが発生していた問題が修正されました。
- （Hub-21319）。スキャン履歴にはマッチが表示されるにもかかわらず、[スキャン]>[コンポーネント]ページには結果が表示されなかった問題が修正されました。
- （Hub-21353）。コンポーネントバージョンのライセンスが変更できなかった問題が修正されました。
- （Hub-21369）。プライマリ言語によるコンポーネント検索のフィルタリングが正しく機能しなかった問題が修正されました。
- （Hub-21538）。EdgeおよびIE 11ブラウザを使用しているときに、**[ソース]**タブの[スニペットビュー]ウィンドウが表示されなかった問題が修正されました。
- （Hub-21606）。「今週作成された新しいプロジェクト」フィルタがすべてのプロジェクトを返していた問題が修正されました。
- （Hub-21614）。並列比較でマッチしたコードが**[ソース]**タブの[スニペットビュー]ウィンドウで強調表示されなかった問題が修正されました。
- （Hub-21664）。**[ソース]**タブで代替マッチを選択しても、ソースコードペインの対応するマッチした行が変更されなかった問題が修正されました。
- （Hub-21735）。**[ソース]**タブで空の依存関係のコンポーネントを更新しようとすると、「createOrUpdateMany.arg1.compositePath required」エラーが表示されていた問題が修正されました。
- （Hub-21751）。SAMLログアウトページのテキストを改訂しました。
- （Hub-21785）。**[ソース]**タブのフィルタで既存のファイルやディレクトリがすべて表示されなかった問題が修正されました。
- （Hub-21793）。Black Duck 2019.8.0 AMIでイメージが欠落していた問題が修正されました。
- （Hub-21796）。子ディレクトリに加えられたファイルまたはディレクトリへの変更が、**[ソース]**タブの親ディレクトリに伝播されていた問題が修正されました。
- （Hub-21817）。[ツール]ページでアイコンが欠落していた問題が修正されました。
- （Hub-21960）。VersionBomComputationJobが、エラーメッセージ「duplicate key value violates unique constraint "uidx_vuln_remediation_release_vuln_id」で失敗していた問題が修正されました。
- （Hub-22042）。[ツール]ページに非推奨の統合へのリンクが引き続き表示されていた問題が修正さ

れました。

- （Hub-22090）。コンポーネントバージョンの**[設定]**タブでコンポーネントバージョンのステータスを更新できなかった問題が修正されました。
- （Hub-22094、22477）。バージョン2019.10.0へのアップグレード後に、LDAP認証が失敗していた問題が修正されました。
- （Hub-22165）。APIエンドポイントのGET /api/vulnerabilities/{vulnerabilityId}/affected-projectsでアクセス制御が失われていた問題が修正されました。
- （Hub-22167）。[ライセンス管理]テーブルから空のライセンスを選択すると404エラーが表示されていた問題が修正されました。
- （Hub-22175）。**[ソース]**タブでマッチしたファイルの上にカーソルを合わせると、ファイルパスが表示されなくなる問題が修正されました。

バージョン2019.10.3

バージョン2019.10.3の新機能および変更された機能

Black Duckバージョン2019.10.3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。

2019.10.3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-22803）。Black DuckとSSOプロバイダ間の通信でセキュリティを強化することにより、Black Duck SSO統合の潜在的な問題を修正しました。

バージョン2019.10.2

バージョン2019.10.2の新機能および変更された機能

Black Duckバージョン2019.10.2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。

2019.10.2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-22091）。バージョン2019.10.0へのアップグレード後に、`scan.cli`でスキャンが失敗していた問題が修正されました。

バージョン2019.10.1

バージョン2019.10.1の新機能および変更された機能

Black Duckバージョン2019.10.1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。

2019.10.1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-21912）。Docker Swarmを読み取り専用の導入環境で使用すると、ドキュメントとWebappコンテナが起動しない問題を修正しました。
- （Hub-21965）。Black Duckがプロキシ証明書の設定で動作しない問題を修正しました。
- （Hub-21970）。**[法]**タブがライセンスマネージャにしか表示されない問題を修正しました。
- （Hub-22002）。blackduck_reporterユーザーに、bds_hubのreportingスキーマを使用したデータへのアクセス権限がない問題を修正しました。
- （Hub-22056）。プロジェクトバージョンレポートが検証例外で失敗していた問題が修正されました。

バージョン2019.10.0

バージョン2019.10.0の新機能および変更された機能

レポートデータベースの再設計

レポーティングデータベースの作成、使用、バックアップ、リストアを簡単に実行できるように、2019.10.0リリースの時点で、別個のレポーティングデータベース（bd_hub_report）の表は、レポーティングデータベースのpublicスキーマから、Black Duckデータベース（bds_hub）のreportingスキーマに移動されました。

Black Duckデータベースのreportingスキーマの表は次のとおりです。

- コンポーネント
- コンポーネントライセンス
- コンポーネントマッチタイプ
- コンポーネントマッチ
- コンポーネントポリシー
- コンポーネントの使用法
- コンポーネントの脆弱性
- プロジェクト
- プロジェクトマッピング
- プロジェクトバージョン
- プロジェクトバージョンコードの場所

Black Duckで行った変更がレポートデータベースに表示されるまでには遅延が生じます。この遅延の時間は、新しいBLACKDUCK_REPORTING_DELAY_MINUTES環境変数を使用して指定した値（デフォルトでは8時間）に応じて異なります。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。

Black Duckには、bds_hubデータベースのレポーティングスキーマへの読み取り専用アクセス権のみを持つblackduck_reporterユーザーがありますが、blackduck_reporterと同じ権限を持つ追加のユーザーを構成できます。詳細については、『*レポートデータベースガイド*』を参照してください。

Note: Synopsysでは、VulnDBユーザーまたは以前のVulnDBユーザーはbds_hub_reportデータベースをバックアップすることを推奨しています。その他すべてのユーザーについては、bds_hub_reportデータベースにあったデータが、現在はbds_hubデータベースに保存されています。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。

LDAP/SSOのユーザー管理の機能強化

ローカルユーザー（内部ユーザーアカウント）または外部ユーザー（LDAPなどの外部ソースにより管理されるユーザーなど）に、Black Duckユーザーアカウントを作成できるようになりました。

外部ユーザーアカウントの場合は、次のようになります。

- ユーザーを作成して、ユーザーがBlack Duckにログインしていなくても役割を割り当てることができます。
- 名や姓などのユーザー情報はBlack Duckで変更できますが、パスワードはBlack Duckで管理されません。
- 外部ユーザーの名、姓、および電子メールアドレスは、ログイン時に外部サーバー（LDAPサーバーなど）に存在する情報でオーバーライドされます。

Note: 2019.10.0リリースより前に作成されたすべてのユーザーアカウントは、内部ユーザーです。

グループ管理の機能強化

Black Duckでは、1つ以上のデフォルトグループを作成できるようになりました。後続の新規ユーザーは自動的にこのグループに追加され、すべての役割と、このグループに構成されているすべてのプロジェクトへのアクセス権が付与されます。

セキュリティ上のリスクが緊急および高のBlack Duck UIの機能強化

Black Duck UIで、緊急および高のセキュリティ上のリスク値が別のカテゴリで示されるようになりました。

Note: CVSS 2.0を表示するよう選択した場合、グラフには、緊急リスクカテゴリが0の値で表示されます。

「限定顧客向け提供」機能となった、カスタムスキャン署名のスキャンレベル数を指定する機能。

カスタムスキャン署名は、デフォルトではディレクトリ構造の上位5つのレベルに制限されています。このリリースでは、システム管理者がこのグローバルデフォルト値を変更できるようになりました。また、スーパーユーザーまたはプロジェクトマネージャが、特定のプロジェクトの設定を変更できるようになっています。

この機能は、Black Duckの特定のお客様が利用できる、「限定顧客向け提供」機能となりました。カスタムスキャン署名機能は、フル製品サポートで完全に機能しますが、Synopsysでは実稼働環境での使用を、ベータプログラムに参加した一部のお客様に限定しています。そのため、この機能は実稼働環境レベルのワークロードを実行することになると想定されます（必ずそうであるとは限りません）。お客様は、特定の環境やワークロードに対応できるように、この機能の使用法を調整することが必要になる場合があります。ベータプログラムに参加しておらず、この機能を実稼働環境以外でテストしたいというお客様は、自社の製品担当者に連絡して機能を有効化するよう依頼してください。

ライセンスおよびコンポーネント管理の追加ステータス値

ライセンス管理に次のステータスが追加されました。

- レビュー中
- レビュー済み
- 廃止済み

コンポーネント管理に次のステータスが追加されました。

- レビュー中
- レビュー済み

これらの追加により、ライセンス管理およびコンポーネント管理で使用可能なステータス値は次のようになります。

- 未レビュー
- レビュー中
- レビュー済み
- 承認済み
- 制限付き承認
- 拒否
- 廃止済み

ナレッジベースコンポーネントを追加する場合、未レビューステータスは使用できません。

追加されたライセンスファミリ

制限付きサードパーティプロプライエタリおよび内部プロプライエタリの2つの新しいライセンスファミリが、Black Duckに追加されました。Black Duckのこのリリースでは、これらの新しいライセンスファミリに関連付けられたナレッジベースライセンスはありません。

Note: ライセンスマネージャが、2019.10.0リリースより前に「Restricted Third Party Proprietary（制限付きサードパーティプロプライエタリ）」または「Internal Proprietary（内部プロプライエタリ）」というラベルのカスタムライセンスファミリを作成した場合、それらのカスタムライセンスファミリ名には末尾に「(1)」が追加されます。

これらのライセンスファミリに関連するリスクを表示する方法については、ドキュメントを参照してください。

コンポーネントプロジェクトバージョンレポートおよびコンポーネント追加フィールドのプロジェクトバージョンレポートの機能強化

コンポーネントプロジェクトバージョンレポート`components_date_#.csv`、およびコンポーネント追加フィールドレポート`bom_component_custom_fields_date_#.csv`が機能強化され、詳細情報が含まれるようになりました。次の列が追加されました。

- ファイルマッチ数
- ライセンス上のリスク
- コンポーネントステータス
- コンポーネントメモ
- 履行が必要

- バージョンメモ
- 緊急脆弱性の数
- 高程度の脆弱性の数
- 中程度の脆弱性の数
- 低程度の脆弱性の数
- リリース日
- 新規バージョン
- コミットアクティビティ
- 過去12か月間のコミット
- 過去12か月間のコントリビュータ

これらのフィールドが、コンポーネントプロジェクトバージョンレポートの末尾に追加されました。コンポーネント追加フィールドレポートの場合、これらのフィールドは、BOMコンポーネント、コンポーネント、およびコンポーネントバージョンカスタムフィールド情報の前に表示されます。

新しいAPIドキュメントと機能強化

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
```

以前のバージョンのAPIドキュメントも引き続きご利用いただけます。表示するには、https://<Black Duckサーバー>/api.htmlに移動します。

APIのその他の拡張機能には、次のようなものがあります。

- 無視されるフラグ、inAttributionReport、attributionStatementの構成表コンポーネントAPIへのPUTサポートが追加されました。
- 構成表ライセンスモーダルのライセンステキストを更新するためのパブリックAPIが追加されました（api/projects/id/versions/id/components/id/versions/id/licenses/id/text）。
- /api/jobsおよび/api/jobs/{jobId}のジョブとやり取りするための新しいパブリックAPIが追加されました。
- /api/user APIが、externalUserNameおよびタイプフィールドを追加/編集できるように更新されました。

ユーザーセッションタイムアウト値を設定する機能

Black Duckでは、Black Duckサーバーからユーザーを自動的にログアウトするユーザーセッションタイムアウト値を設定できるようになりました。

現在のタイムアウト値を変更するには、PUTリクエスト本文で次のPUTリクエストを実行します。

```
PUT https://<hub-server>/api/system-oauth-client
{
 "accessTokenValiditySeconds": <time in seconds>
}
```

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。

bdioデータベースの削除

クライアントからBlack Duckへのスキャンアップロードのパフォーマンスを向上させるために、bdioデータベースは使用されなくなり、今後のリリースでは削除される予定です。その結果、ScanGraphJobも削除されました。

容量を再利用したい場合は、bdioデータベースのバックアップや、すべての表データの切り捨てを行うことができます。

サポートされるブラウザのバージョン

- Safariバージョン13.0.1（14608.2.11.1.11）
- Chromeバージョン77.0.3865.90（公式ビルド）（64ビット）
- Firefoxバージョン69.0.2（64ビット）
- Internet Explorer 11.1006.17134.0
- Microsoft Edge 42.17134.1.0
- Microsoft EdgeHTML 17.17134

コンテナの変更

更新されたコンテナ：

- uploadcache: image: blackducksoftware/appcheck-worker:2019.09
- webserver: image: blackducksoftware/blackduck-nginx:1.0.9

変更されたネームスペース：

- binaryscanner: image:sigsynopsys/appcheck-worker:2019.09

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2019.8.0が日本語にローカライズされました。

2019.10.0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-19787）。1つのプロジェクトバージョンに対して4つのVersionBomComputationJobsを同時に開始すると、これらのジョブすべてが失敗する問題を修正しました。
- （Hub-20000）。**[ソース]**タブのスニペットビューにファイルのフルパス情報が表示されない問題を修正しました。
- （Hub-20040）。SSOアカウントからログアウトしたときにログアウトページが表示されない問題を修正しました。
- （Hub-20366）。ユーザーがBlack Duck UIの使用時に.jsonファイルをアップロードしようとしてタイムアウトが発生することがないように問題を解決しました。
- （Hub-20421）。アップグレードバージョンが利用できない場合にBlack Duck UIにアップグレードガイダンス情報が表示されないように問題を修正しました。
- （Hub-20770）。**[ソース]**タブのスニペットビューに、一致するコンポーネントのファイル名が表示

されない問題を修正しました。

- （Hub-20879）。ファイルまたはフォルダがアーカイブファイル内にある場合に、**[ソース]**タブにフルパスが表示されない問題を修正しました。
- （Hub-19534、HUB-20800、HUB-20926）。KbReleaseUpdateJobが繰り返し失敗するために、重複するコンポーネントがコンポーネントダッシュボードに表示される問題を修正しました。
- （Hub-21075）。スキャンが誤ったプロジェクトバージョンにマッピングされ、削除されたプロジェクトバージョンが復元される問題を修正しました。
- （Hub-21217）。「サーバーが時間内に応答しませんでした」というエラーメッセージが表示され、プロジェクトのクローンの作成に失敗する問題を修正しました。
- （Hub-21264）。SSOとBlack Duckを統合する際の無効なポートの問題を修正しました。
- （Hub-21276）。ポリシー違反がオーバーライドされた後、AGPLライセンス違反がクリアされない問題を修正しました。
- （Hub-21298、HUB-21549）。構成表で無視されたコンポーネントを編集すると404エラーが発生する問題を修正しました。
- （Hub-21421）。大規模プロジェクトの構成表の印刷に失敗する問題を修正しました。
- （Hub-21464）。[ユーザー管理]ページに、ユーザーあたり最大10のグループが表示される問題を修正しました。
- （Hub-21488）。Azure AFDS SAMLでのログイン時に外部ユーザーがグループから削除される問題を修正しました。
- （Hub-21538）。Edge 11およびInternet Explorer 11で表示したときに、スニペットの代替マッチが破損する問題を修正しました。
- （Hub-21541）。AWSでKubernetesを実行していると、認証コンテナで誤ったポートが返される問題を修正しました。

バージョン2019.8.1

バージョン2019.8.1の新機能および変更された機能

APIの拡張機能

- スニペットマッチを無視、確認、編集するためのAPIエンドポイントが利用できるようになりました。
- Black Duckスキャンのチェックサムファイルマッチデータと比較できるように、Protex BOMインポート用のファイルマッチのチェックサムデータを取得できるようになりました。

2019.8.1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-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-21057）。バージョン2019.6.1へのアップグレード後に発生するパフォーマンスの問題を修正しました。
- （Hub-21372）。notification_subscriber状態の更新に非常に時間がかかるという問題を修正しました。

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の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機能拡張され、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。

スニペットのスキャンの機能拡張

スキャンのパフォーマンスと結果を向上させるために、スニペットスキャンの実行を選択した場合、スニペットスキャンは、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ャンが実行されます。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}

非推奨のエンドポイント:

- 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と、「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。

- VulnerabilityRepriortizationJob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。

- BOMagGregatePointHandsJob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BDSA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。

Keepalive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る必要があります。

Docker SwarmとKubernetesの新しい制限事項

Black DuckDocker 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に、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 enhancements

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。
- SSO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。

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することが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への名前の変更にともない、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。
- [ポリシールールの編集]ダイアログボックスで**[キャンセル]**を選択しても、ポリシール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ルールの作成を防止できない問題が修正されました。
- ポリシールールに[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ジビューとソースビュー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

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。

直接的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。
- Kbernetes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ように選択した場合、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。

章 3: 既知の問題と制限事項

Black Duckの既知の問題と制限事項は次のとおりです。

- 署名スキャナCLISynopsys Detect（Desktop）またはSynopsys Detectでスキャンすると、次のエラーメッセージが表示される場合があります。

  ```
  ERROR StatusLogger Unrecognized
  ```

  これらのメッセージは無視できます。これらのエラーはスキャンに影響を与えず、スキャンが失敗することはありません。

- *[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。
- 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。