



リリースノート  
バージョン2021.2.0

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2021.2.0を対象としています。

本ドキュメントは2021年4月1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 © 2021 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。

<b>章 1: 製品発表</b>	<b>1</b>
バージョン2021. 2. 0の発表	1
Azureをご利用のお客様へのお知らせ	1
外部データベース用のPostgreSQLバージョン9. 6のサポート廃止	1
Internet Explorer 11はサポートされなくなりました	1
廃止されたページ	1
日本語	1
バージョン2020. 12. 0の発表	2
新しいコンテナとシステム要件の変更	2
Internet Explorer 11のサポートの終了	2
日本語	2
バージョン2020. 10. 0の発表	2
2020. 12. 0リリースまで延期された新しいコンテナとシステム要件の変更	2
日本語	3
バージョン2020. 8. 0の発表	3
外部データベース用のPostgreSQLバージョン9. 6のサポート廃止	3
2020. 10. 0リリースで廃止されたAPI	3
日本語	3
バージョン2020. 6. 1の発表	3
Internet Explorer 11のサポートの終了	3
バージョン2020. 6. 0の発表	4
今後のリリースでの新しいコンテナとシステム要件の変更	4
Internet Explorer 11のサポートの廃止	5
PostgreSQL 11の外部データベースのサポート	5
バージョン2020. 2. 0の発表	5
個別のファイルマッチ	5
Docker Composeのサポート	6
バージョン2019. 12. 0の発表	6
Black Duckのアップグレード	6
今後の2020. 2. 0リリースでの個別のファイルマッチ	7
Docker Composeのサポート	8
<b>章 2: リリース情報</b>	<b>9</b>
バージョン2021. 2. 0	9

バージョン2021. 2. 0の新機能および変更された機能 .....	9
2021. 2. 0で修正された問題 .....	14
バージョン2020. 12. 0 .....	16
バージョン2020. 12. 0の新機能および変更された機能 .....	16
2020. 12. 0で修正された問題 .....	20
バージョン2020. 10. 1 .....	21
バージョン2020. 10. 1の新機能および変更された機能 .....	21
2020. 10. 1で修正された問題 .....	22
バージョン2020. 10. 0 .....	22
バージョン2020. 10. 0の新機能および変更された機能 .....	22
2020. 10. 0で修正された問題 .....	27
バージョン2020. 8. 2 .....	29
バージョン2020. 8. 2の新機能および変更された機能 .....	29
2020. 8. 2で修正された問題 .....	29
バージョン2020. 8. 1 .....	29
バージョン2020. 8. 1の新機能および変更された機能 .....	29
2020. 8. 1で修正された問題 .....	30
バージョン2020. 8. 0 .....	30
バージョン2020. 8. 0の新機能および変更された機能 .....	30
2020. 8. 0で修正された問題 .....	36
バージョン2020. 6. 2 .....	38
バージョン2020. 6. 2の新機能および変更された機能 .....	38
2020. 6. 2で修正された問題 .....	38
バージョン2020. 6. 1 .....	38
バージョン2020. 6. 1の新機能および変更された機能 .....	38
2020. 6. 1で修正された問題 .....	38
バージョン2020. 6. 0 .....	39
バージョン2020. 6. 0の新機能および変更された機能 .....	39
2020. 6. 0で修正された問題 .....	44
バージョン2020. 4. 2 .....	45
バージョン2020. 4. 2の新機能および変更された機能 .....	45
2020. 4. 2で修正された問題 .....	45
バージョン2020. 4. 1 .....	45
バージョン2020. 4. 1の新機能および変更された機能 .....	45
2020. 4. 1で修正された問題 .....	45
バージョン2020. 4. 0 .....	46
バージョン2020. 4. 0の新機能および変更された機能 .....	46
2020. 4. 0で修正された問題 .....	50
バージョン2020. 2. 1 .....	52
バージョン2020. 2. 1の新機能および変更された機能 .....	52
2020. 2. 1で修正された問題 .....	52

バージョン2020. 2. 0 .....	52
バージョン2020. 2. 0の新機能および変更された機能 .....	52
2020. 2. 0で修正された問題 .....	56
バージョン2019. 12. 1 .....	57
バージョン2019. 12. 1の新機能および変更された機能 .....	57
2019. 12. 1で修正された問題 .....	57
バージョン2019. 12. 0 .....	58
バージョン2019. 12. 0の新機能および変更された機能 .....	58
2019. 12. 0で修正された問題 .....	61
<b>章 3: 既知の問題と制限事項 .....</b>	<b>63</b>

## 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。

サポートケースを開くには、Synopsys Software Integrityコミュニティサイト (<https://community.synopsys.com/s/contactsupport>) にログインしてください。

常時対応している便利なリソースとして、[オンラインカスタマポータル](#)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>を参照するか、Black Duckのヘルプに

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



## バージョン2021. 2. 0の発表

### Azureをご利用のお客様へのお知らせ

Black Duckバージョン2021. 2. 0は、Azure Kubernetes Services (AKS) で展開し、Azure Database for PostgreSQLを外部データベースとして使用するお客様に影響を与える既知の問題とともにリリースされています。これは、Azureプラットフォーム上のBlack Duckのお客様に推奨される標準構成であることに注意してください。現時点では、外部データベースを備えたAzureプラットフォームで実行しているお客様が2021. 2. 0にアップグレードすることはお勧めしません。これを行うと、システムが動作不能のままになり、インストールを前の状態に戻すように強制されます。

この問題は今後のBlack Duckリリースで解決される予定であり、リリースの詳細が判明した時点で発表されます。

AKS上で実行しており、内部PostgreSQLデータベースを使用する場合は、問題はなく、システムは期待どおりに動作します。ただし、これは、AKSプラットフォームでの変則的なインストールです。

ご不明な点やご質問がある場合は、Black Duckサポートにお問い合わせください。

### 外部データベース用のPostgreSQLバージョン9. 6のサポート廃止

Synopsysは、Black Duck 2021. 6. 0リリース以降で、外部データベース用のPostgreSQLバージョン9. 6のサポートを廃止する予定です。

Black Duck 2021. 6. 0リリース以降では、Black Duckは、外部データベース用にPostgreSQLバージョン11. xのみをサポートします。

### Internet Explorer 11はサポートされなくなりました

SynopsysはInternet Explorer 11のサポートを終了しました。

### 廃止されたページ

[スキャン] > [コンポーネント] ページは、2021. 2. 0リリースで廃止され、今後のリリースでは削除される予定です。

### 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2020. 12. 0が日本語にローカライズされました。

## バージョン2020.12.0の発表

### 新しいコンテナとシステム要件の変更

新しいコンテナが2つ追加されています。2020.12.0リリース向けのBOM EngineおよびRabbitMQ（今後は必須コンテナ）です。

すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のとおりです。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

**Note:** binaryscannerコンテナを1個追加するごとに、1 CPU、2GB RAM、100GBの空きディスク容量の追加が必要になります。

### Internet Explorer 11のサポートの終了

Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

### 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2020.10.0が日本語にローカライズされました。

## バージョン2020.10.0の発表

### 2020.12.0リリースまで延期された新しいコンテナとシステム要件の変更

以前にBlack Duckは、2020.10.0リリース向けに、BOM EngineおよびRabbitMQ（現在は必須コンテナ）という2つのコンテナが追加されると発表しました。この要件は、2020.12.0リリースに延期されました。

2020.12.0リリースでは、すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のようになります。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合

は29 GB RAM

- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

2020.12.0リリースでは、Black Duck – Binary AnalysisでBlack Duckを実行するために必要とされる最小ハードウェアは次のようになります。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

**Note:** binaryscannerコンテナを1個追加するごとに、1 CPU、2GB RAM、100GBの空きディスク容量の追加が必要になります。

## 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2020.8.0が日本語にローカライズされました。

## バージョン2020.8.0の発表

### 外部データベース用のPostgreSQLバージョン9.6のサポート廃止

Synopsysは、Black Duck 2021.6.0リリース以降で、外部データベース用のPostgreSQLバージョン9.6のサポートを廃止する予定です。

Black Duck 2021.6.0リリース以降では、Black Duckは、外部データベース用にPostgreSQLバージョン11.xのみをサポートします。

### 2020.10.0リリースで廃止されたAPI

Black Duck 2020.10.0リリースでは、/api/catalog-risk-profile-dashboard APIは、HTTP 410 (GONE) を返します。Black Duck 2020.12.0リリース以降で、このAPIは使用できなくなります。

/api/catalog-risk-profile-dashboardを置き換える新しいAPIは、2020.10.0リリースで発表されます。

## 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2020.6.0が日本語にローカライズされました。

## バージョン2020.6.1の発表

### Internet Explorer 11のサポートの終了

Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降で

のInternet Explorer 11のサポートを終了します。

## バージョン2020. 6. 0の発表

### 今後のリリースでの新しいコンテナとシステム要件の変更

#### 2020. 8. 0リリース

2020. 8. 0リリースでは、新しいRedisコンテナがBlack Duckに追加されます。このコンテナでは、Black Duckのキャッシュ機能の整合性が向上し、アプリケーションのパフォーマンスが改善します。

以下は、すべてのコンテナの単一インスタンスの実行に必要な最小ハードウェアです。

- 5 CPU
- Redisの最小構成の場合は21 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は24 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250GBの空きディスク容量
- データベースバックアップに適した容量

以下は、Black Duck – Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアです。

- 6 CPU
- Redisの最小構成の場合は25 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は28 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

**Note:** binaryscannerコンテナを1個追加するごとに、CPU、2GB RAM、100GBの空きディスク容量の追加が必要です。

#### 2020. 10. 0リリース

2020. 10. 0リリースでは、Black Duckは次の2つのコンテナを追加します。BOM EngineとRabbitMQは必須コンテナです。これらのコンテナは、アプリケーションのパフォーマンスを向上させるために使用され、主にプロジェクトバージョンの構成表パフォーマンスを向上させます。

初期テストで示される、すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

初期テストで示される、Black Duck – Binary AnalysisでBlack Duckを実行させるために必要な最小ハードウェアは次のとおりです。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

**Note:** binaryscannerコンテナを1個追加することにより、CPU、2GB RAM、100GBの空きディスク容量の追加が必要です。

これらのシステム要件は、初期テスト結果に基づいていることに注意してください。最終的なシステム要件は、この記載内容よりも小さい場合がありますが、記載内容より大きくなることはありません。

## Internet Explorer 11のサポートの廃止

Synopsysは、Black Duck 2021.2.0リリース以降でInternet Explorer 11のサポートを廃止する予定です。

## PostgreSQL 11の外部データベースのサポート

Black Duckは、外部PostgreSQLを使用する新規インストール用にPostgreSQL 11.7をサポートするようになりました。PostgreSQL 9.6は引き続き外部PostgreSQLインスタンスに対して完全にサポートされていますが、Synopsysは、外部PostgreSQLを使用する新規インストールには、PostgreSQL 11.7を推奨しています。

内部PostgreSQLコンテナのユーザーの場合は、PostgreSQL 9.6が引き続きBlack Duck 2020.6.0でサポートされるバージョンです。

## 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2021. 2. 0

#### バージョン2021. 2. 0の新機能および変更された機能

##### 新しいカスタム脆弱性ダッシュボード

2021. 2. 0では、セキュリティダッシュボードが、保存済み脆弱性検索を使用できるカスタム脆弱性ダッシュボードに切り替わり、重要な脆弱性を簡単に表示できるようになりました。Black Duckでは、さまざまな属性を使用してプロジェクトおよび/またはBlack Duckナレッジベース内で使用される脆弱性を検索し、検索を保存してから、この[ダッシュボード] ページを使用して保存済み検索からダッシュボードを表示できるようになりました。

脆弱性ごとに、カスタム脆弱性ダッシュボードに次の情報が表示されます。

- BDSAまたはNVDの脆弱性ID。脆弱性IDを選択すると、追加のスコア値など、脆弱性に関する詳細情報が表示されます。
- この脆弱性の影響を受けるプロジェクトのバージョンの数と、この脆弱性の影響を受けるプロジェクトのバージョンが一覧表示された脆弱性の[影響を受けるプロジェクト]タブを表示するリンク。
- 全体的なリスクスコア。
- ソリューション、回避策、または攻撃が利用可能かどうか。
- 脆弱性が最初に検出、公開、および最終変更された日付。
- このセキュリティ脆弱性の共通脆弱性タイプ一覧（CWE）番号。

##### 脆弱性検索の機能強化

脆弱性の検索は、脆弱性の検索に使用できる属性と、検索結果に表示される情報によって強化されています。プロジェクトの脆弱性を検索するか、Black Duckナレッジベースの脆弱性を検索するかどうかを選択できます。

脆弱性を検索する場合は、次の属性を使用できます。

- 影響を与えるプロジェクト
- デフォルトの修正
- 到達可能
- 悪用
- 最初の検出
- 修正ステータス

- 解決方法
- ベーススコア
- 攻撃される可能性のスコア
- 影響スコア
- 総合スコア
- 公開された年
- 重大度
- ソース (BDSAまたはNVD)
- 一時スコア
- 回避策

これらの脆弱性は、前述のように、検索結果を保存して[ダッシュボード]ページに表示できるようになりました。

## プロジェクトのライセンス競合を管理する機能

ライセンス違反のリスクを軽減するため、構成表内のコンポーネントに、プロジェクトの宣言されたライセンスに対して齟齬がある条項を含むライセンスがある場合を理解する必要があります。Black Duckでは、これらのライセンス条項の競合を特定し、それを[法]タブにある新しい[ライセンス競合]に表示するようになりました。

コンポーネントのライセンスがプロジェクトバージョンのライセンスと競合する場合にトリガーされるポリシールールを設定することもできます。

Black Duckは、ライセンスのリスクが高いコンポーネントバージョンのライセンス競合のみを判断することに注意してください。Black Duckライセンスリスクモデルでは、「高リスク」とは、このビジネスシナリオ（配布タイプとコンポーネントの使用法の組み合わせ）の下で、このファミリのライセンスが競合する傾向があることを意味します。中程度または低リスクとは、ビジネスシナリオが変更された場合（または誤って定義された場合）、またはライセンス以外の競合要因が原因でリスクが発生する可能性があることを意味します。

## 依存関係

Synopsys Detectスキャンで直接的または推移的な依存関係が検出された場合、Black Duckは、プロジェクトバージョンの[セキュリティ]タブで、依存関係の各タイプの一致数を一覧表示するようになりました。

推移的な依存関係の場合、依存関係ツリーには、この依存関係をもたらしたコンポーネント、重大度レベル別の脆弱性、およびその依存関係パスでコンポーネントが導入された回数のマッチ数が表示されます。

## レポートデータベースの機能強化

無視されたコンポーネントの新しいテーブル（`component_ignored`）がレポートデータベースに追加されました。次のカラムがあります。

- `id`。ID
- `project_version_id`。プロジェクトバージョンID。
- `component_id`。コンポーネントID。
- `component_version_id`。コンポーネントバージョンID。

- `component_name`。コンポーネント名。
- `component_version_name`。コンポーネントバージョン名。
- `version_origin_id`。バージョン取得元ID。
- `origin_id`。取得元ID。
- `origin_name`。取得元名。
- `ignored`。コンポーネントが無視されるかどうかを示すブール値。
- `policy_approval_status`。ポリシーの承認ステータス。
- `review_status`。コンポーネントのレビューステータス。
- `reviewed_by`。コンポーネントをレビューしたユーザー。
- `reviewed_on`。コンポーネントがレビューされた日時。
- `security_critical_count`。重要なセキュリティ脆弱性の数。
- `security_high_count`。高セキュリティ脆弱性の数。
- `security_medium_count`。中程度のセキュリティ脆弱性の数。
- `security_low_count`。低セキュリティ脆弱性の数。
- `security_ok_count`。セキュリティの脆弱性が存在しない数。
- `license_high_count`。高ライセンスリスクの数。
- `license_medium_count`。中ライセンスリスクの数。
- `license_low_count`。低ライセンスリスクの数。
- `license_ok_count`。ライセンスリスクなしの数。
- `operational_high_count`。高い運用リスクの数。
- `operational_medium_count`。中程度の運用リスクの数。
- `operational_low_count`。低い運用リスクの数。
- `operational_ok_count`。運用リスクなしの数。

ユーザー情報の新しいテーブル (`user`) がレポートデータベースに追加されました。次のカラムがあります。

- `id`。ID。
- `first_name`。ユーザーの名。
- `last_name`。ユーザーの姓。
- `username`。Black Duckのユーザーのユーザー名。
- `email`。ユーザーの電子メールアドレス。
- `active`。このユーザーがアクティブかどうかを示すブール値。
- `last_login`。ユーザーがBlack Duckに最後にログインした時刻。

## ライセンス編集の機能強化

構成表でライセンスを編集する際に、次の機能強化が行われました。

- コンポーネントのライセンスを編集するときに、Black Duckでは、ルートレベルまたは元のライセンスと同じレベルで構成表内のコンポーネントの新しい複数ライセンスシナリオを簡単に作成したり、既存の複数ライセンスシナリオを編集したりすることができるようになりました。

- コンポーネントに別のライセンスを選択した場合は、Black Duckナレッジベースで定義されたとおりに、ライセンスを元のライセンスに戻すことができます。
- [＜コンポーネント名 バージョン＞コンポーネントライセンス] ダイアログボックスの新しいオプションにより、編集モードがあることを容易に識別できます。

## レポートの機能強化

source\_date\_time.csv プロジェクトバージョンレポートの最後に、新しいカラム[アーカイブのコンテンツとパス]が追加されました。このカラムは、既存のパスとアーカイブコンテンツのカラムに表示される情報を連結して、各コンポーネントのフルパスを提供します。

## 通知ファイルレポート

通知ファイルレポートが改善され、著作権データに単一のコンポーネント取得元の重複情報が含まれなくなりました。

## バイナリスキンの機能拡張

バイナリスキンでは、完全一致に加えて部分一致が返されるようになりました。


## ディープライセンスデータの機能拡張

ファイル内のディープライセンスデータの証拠を確認するときに、Black Duckでは、ライセンステキストの一致をトリガーしたライセンステキストが強調表示されるようになりました。

## BOM Engine

Black Duck UIの応答時間を改善するために、ライセンスの更新はBOM Engineによって実行されるようになりました。このプロセスは、構成表からアクセス可能な[構成表処理ステータス] ダイアログボックスで、[ライセンスの更新] または [ライセンス条項の履行の更新] イベントとして表示されます。

## Black Duckチュートリアル

Black Duckのトレーニングを簡単に表示するには、Black Duck UIの[ヘルプ] メニュー (  ) から、[Black Duckチュートリアル] を選択します。

## パスワードの構成の変更

システム管理者の役割を持つユーザーは、ローカルBlack Duckアカウントのパスワード要件を設定できるようになりました。スーパーユーザーの役割を持つユーザーは、パスワード要件を構成できなくなりました。

## ポリシールールの機能強化

ポリシー管理では、ブール値、日付、ドロップダウン、複数選択、単一選択、およびテキストフィールドタイプのプロジェクトバージョンのカスタムフィールドに基づいて、ポリシールールを作成する機能が提供されるようになりました。

## Synopsys Detectのホスティングロケーション

外部接続が制限されているBlack Duckのお客様は、Synopsys Detectの内部ホスティングロケーションを定義できるようになりました。これらのユーザーは、この情報を使用して、Code Sightを利用して開発者

ベース全体に展開し、オンデマンドのソフトウェアコンポジション解析 (SCA) スキャンを実行できます。

### 保存済み検索ダッシュボードの機能強化

[ダッシュボード] ページに表示される保存済み検索ごとに、検索が最後に更新された日時がBlack Duckに一覧表示されるようになりました。ポップアップに保存された検索フィルタとリンクが表示されるので、[検索] ページを開いて、改訂された保存済み検索を編集および保存できます。

### スニペットのトリアージの機能拡張

未確認スニペット (🚩)、確認済みスニペット (✅)、無視されたスニペット (❌) を区別しやすくするために、[ソース] タブにアイコンが追加されました。

### サポートされるブラウザのバージョン

- Safariバージョン14.0.3 (15610.4.3.1.6, 15610)
- Chromeバージョン88.0.4324.150 (公式ビルド) (x86\_64)
- Firefoxバージョン85.0.2 (64ビット)
- Microsoft Edgeバージョン88.0.705.63 (公式ビルド) (64ビット)

### コンテナバージョン

- blackducksoftware/blackduck-postgres: 1.0.16
- blackducksoftware/blackduck-authentication: 2021.2.0
- blackducksoftware/blackduck-webapp: 2021.2.0
- blackducksoftware/blackduck-scan: 2021.2.0
- blackducksoftware/blackduck-jobrunner: 2021.2.0
- blackducksoftware/blackduck-cfssl: 1.0.1
- blackducksoftware/blackduck-logstash: 1.0.9
- blackducksoftware/blackduck-registration: 2021.2.0
- blackducksoftware/blackduck-nginx: 1.0.30
- blackducksoftware/blackduck-documentation: 2021.2.0
- blackducksoftware/blackduck-upload-cache: 1.0.15
- blackducksoftware/blackduck-redis: 2021.2.0
- blackducksoftware/blackduck-bomengine: 2021.2.0
- sigsynopsys/bdba-worker: 2020.12-1
- blackducksoftware/rabbitmq: 1.2.2

### サポートされるDockerのバージョン

Black Duckのインストールでは、Dockerバージョン18.09.x、19.03.x、および20.10.x (CEまたはEE) がサポートされています。

### Docker webapp-volume

Docker webapp-volumeは、オーケストレーションでは使用されなくなりました。必要に応じて、ユーザーはDocker webapp-volumeをバックアップおよびプルーニングできます。それ以外の場合は、アクションは

必要ありません。

## APIの機能強化

- APIドキュメントは、<https://<Black Duck server URL>/api-doc/public.html>でのみ入手できるようになりました。
- 作成日でコードの場所 (/api/codelocations) をフィルタリングする機能が追加されました。
- 以前のバージョンで正しく動作していなかったSAML IDプロバイダのメタデータXMLファイル (api/sso/idp-metadataエンドポイント) のダウンロードに使用されるAPIを修正しました。
- remediation-guidanceエンドポイント (GET /api/components/{componentId}/versions/{componentVersionId}/remediating) は、「410 GONE」応答を返さなくなりました。upgrade-guidanceエンドポイント (GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidance) に切り替える必要があります。このエンドポイントは、削除されたremediation-guidanceエンドポイントと互換性がありません。
- コンポーネントの依存関係パスを表示するために、レポートのdependency-pathsエンドポイントが追加されました。

```
/api/project/{projectId}/version/{projectVersionId}/origin/{originId}/dependency-paths
```

- [システム設定] ページでSynopsys Detect URIの読み取りを設定または更新するためにのみ使用されるSynopsys Detect URIエンドポイントが追加されました。

```
/external-config/detect-uri
```

## Ubuntuオペレーティングシステム

UbuntuのDocker環境にBlack Duckをインストールするための推奨オペレーティングシステムは、バージョン18.04.x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2021.12.0が日本語にローカライズされました。

## 2021.2.0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-22103)。ライセンスステータスを更新するときに、Black Duckサーバーが時間内に応答しなかった問題が修正されました。
- (Hub-22623)。UIにロードするときに、概要ダッシュボードが企業顧客に対して頻繁にタイムアウトする問題を修正しました。
- (Hub-24332)。同じコードの場所をスキャンすると通知が重複する問題が修正されました。
- (Hub-25374)。データベースazure\_maintenanceの許可エラーを修正しました。
- (Hub-25580)。構成表に表示されているコンポーネントが9ページ以降に正しくソートされない問題を修正しました。
- (Hub-25666)。エンドポイント/usergroups/<group #>/rolesのページネーションの問題を修正しました。

- (Hub-26030)。アクションの実行後に、ダッシュボードのソートオプションがプロジェクト名で保持されない問題を修正しました。
- (Hub-26324)。エラー「java.lang.IllegalStateException: Parent of [file:/C:/src/External/PackageManager/ProjectTemplates/com.unity.template.universal-10.1.0.tgz] does not exist」がスキャンのアップロード時に発生する問題を修正しました。
- (Hub-26343)。登録コンテナのヒープ領域が不足しているため、Black Duckを登録できない問題が修正されました。
- (Hub-26493)。ユーザーがプロジェクトのメンバーとして自分自身を削除したときに表示される紛らわしいエラーメッセージが修正されました。
- (Hub-26501)。[コンポーネントの編集] ダイアログボックスでcordova-plugin-inappbrowserコンポーネントを選択できない問題を修正しました。
- (Hub-26536)。ウォッチするプロジェクトがページヘッダーにウォッチしないアイコン (  ) を表示する問題を修正しました。
- (Hub-26540)。Black Duckを再起動しないとSAMLの初期構成が有効にならないという問題を修正しました。
- (Hub-26615)。プロジェクトAでプロジェクトマネージャの役割を持ち、プロジェクトBでプロジェクトマネージャとプロジェクトコードスキャナの役割を持つユーザーが、スキャンをプロジェクトAにアップロードできるという問題が修正されました。
- (Hub-26616)。スニペットを無視しようとする、次のエラーメッセージで失敗する問題が修正されました。「コンシューマ、プロデューサー、調整タイプ、開始行、終了行の変更がサポートされていないため、既存のスニペット調整を更新できません。」
- (Hub-26712、26962)。スニペットマッチが確認された後、[ソース] タブのツリービューに表示されるスニペットアイコンがクリアされない問題を修正しました。
- (Hub-26726)。ポリシールールを作成するときに、カスタムフィールドで「not in」オプションを使用できない問題が修正されました。
- (Hub-26807)。構成表コンポーネントバージョンのカスタムフィールドを取得しようとしたときに、HTMLステータスコード404を受信する問題が修正されました。
- (Hub-26815)。SAML統合設定を保存するとページが再ロードされ、IDプロバイダのメタデータ設定が切り替わる問題が修正されました。
- (Hub-26904)。[設定] タブのプロジェクトバージョンの[アクティビティ] セクションに表示されるマッチ数値が[スキャン名] ページと異なる問題が修正されました。
- (Hub-26930)。コンポーネントの通知がトリガーされない問題を修正しました。
- (Hub-27002)。クローン作成されたプロジェクトが作成されたときに誤った通知が送信される問題を修正しました。
- (Hub-27049)。ユーザーにライセンスマネージャの役割が割り当てられていないと、プロジェクトバージョンレポートのライセンス条項カテゴリが、Black Duck UIに表示されないという問題が修正されました。
- (Hub-27208)。SAMLの構成時にSynopsys Alertの読み込みに失敗するblackduck-nginxの問題を修正しました。
- (Hub-27227)。スニペットのマッチングが完了するまでに時間がかかる問題を修正しました。
- (Hub-27264)。コンポーネントを確認すると、その使用状況がデフォルト値にリセットされる問題



が修正されました。

- (Hub-27681)。カスタムセキュリティコンテキストを使用してKubernetesに展開するときに、ルートユーザーがBOM Engineを起動する必要がある問題を修正しました。

## バージョン2020. 12. 0

### バージョン2020. 12. 0の新機能および変更された機能

#### 新しいコンテナとシステム要件の変更

新しいコンテナが2つ追加されています。2020. 12. 0リリース向けのBOM EngineおよびRabbitMQ（今後は必須コンテナ）です。

すべてのコンテナの単一インスタンスを実行するための最小システム要件は次のとおりです。

- 6 CPU
- Redisの最小構成の場合は26 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は29 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250 GBの空きディスク容量
- データベースバックアップに適した容量

Black Duck - Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のとおりです。

- 7 CPU
- Redisの最小構成の場合は30 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は33 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

**Note:** binaryscannerコンテナを1個追加するごとに、1 CPU、2GB RAM、100GBの空きディスク容量の追加が必要になります。

#### パスワードの構成

スーパーユーザーの役割を持つユーザーが、ローカルBlack Duckアカウントのパスワード要件を設定できるようになりました。有効にすると、新しいパスワードがお客様の要件を満たしていることが、Black Duckにより確認されます。また、脆弱と見なされるパスワード（「password」、「blackduck」、ユーザーのユーザー名や電子メールアドレスなど）は拒否されます。

スーパーユーザーは次の操作を実行できます。

- 最小パスワード長を定義します。
- パスワードの最小文字種数を定義します。使用可能な文字種は、小文字、大文字、数字、特殊文字です。
- 現在のユーザーがBlack Duckにログインするときにパスワード要件を適用するかどうかを選択します。

デフォルトでは、パスワード要件は有効で、次のように設定されています。



- 最小パスワード長は8文字です。
- 必要な文字種は1つだけです。
- Black Duckにログインしている現在のユーザーにはパスワード要件が適用されません。

## ライセンスの機能強化

ライセンスリスクを適切に管理できるように、Black Duckでは、構成表のコンポーネントについてマルチライセンスシナリオを新規に作成したり既存のものを編集したりできるようになりました。

## 脆弱性の影響解析の機能強化

- 新しいプロジェクトバージョンレポート `vulnerability_matches_date_time.csv` が追加されました。脆弱性によって到達される可能性のあるコンポーネントごとに、コンポーネント、脆弱性データ、および脆弱性の影響解析データが一覧表示されます。このレポートには、次のカラムがあります。
  - コンポーネント名
  - コンポーネントID
  - 使用中
  - コンポーネントバージョン名
  - バージョンID
  - チャネルバージョン取得元
  - 取得元ID
  - 取得元名ID
  - 脆弱性ID
  - 脆弱性ソース
  - CVSSバージョン
  - セキュリティ上のリスク
  - ベーススコア
  - 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
  - 攻撃が利用可能
  - 呼び出された関数
  - 修飾名
  - 行番号
- 新しいテーブルとして、脆弱性メソッドマッチ (`vulnerability_method_matches`) がレポートデータベースに追加されました。次のカラムがあります。
  - `id`。ID。
  - `project_version_id`。到達可能な脆弱性があるプロジェクトバージョンのUUID。
  - `vuln_source`。脆弱性のソース。脆弱性の影響解析の場合、値はBDSAです。
  - `vuln_id`。脆弱性ID (BDSA-2020-1234など)。

- `qualified_name`。関数が呼び出されるクラスの名前。
  - `called_function`。コード内で脆弱性を到達可能にする脆弱な関数呼び出しの名前。
  - `line_number`。コード内で脆弱な関数が呼び出される行番号。
- 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、および脆弱性更新レポート）には、セキュリティ脆弱性が到達可能か（真）、または到達不能か（偽）を示すために、レポートの末尾に[到達可能]という新しいカラムが追加されました。

## 構成表の計算情報

Black Duckでは、プロジェクトバージョン構成表の計算ステータスに関する詳細情報が提供されるようになりました。

Black Duck UIのプロジェクトバージョンヘッダーにある新しい[ステータス]インジケータ（[コンポーネント]インジケータに代わるもの）は、構成表の現在のステータスを示し、構成表イベントの処理の状態を通知します。更なる情報として、新しい[構成表処理ステータス]ダイアログボックスに、保留中、処理中、または失敗したイベントが表示されます。

また、Black Duckでは、構成表イベントクリーンアップジョブ（VersionBomEventCleanupJob）の頻度も構成できます。このジョブは、処理エラーまたはトポロジ変更によってスタックした可能性のある構成表イベントをクリアします。

## ポリシーの機能強化

- ポリシー管理では、次のカスタムフィールド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。
  - ブール、日付、ドロップダウン、複数選択、単一選択、テキストの各フィールドタイプ用のコンポーネントカスタムフィールド。
  - ブール、日付、ドロップダウン、複数選択、単一選択、テキストの各フィールドタイプ用のコンポーネントバージョンカスタムフィールド。
- これらの条件のポリシールールを作成する際に、宣言されたライセンスデータとディープ（埋め込み）ライセンスデータを区別できるようになりました。
  - ライセンス
  - ライセンスの有効期限
  - ライセンスファミリ

**Note:** これらのライセンス条件を使用する既存のポリシールールは、宣言されたライセンスにのみ適用されるようになりました。これらのライセンス条件に対しては、ディープ（埋め込み）ライセンス用に、個別のポリシールールを作成する必要があります。

## レポートの機能強化

以前はグローバルレベルまたはプロジェクトレベルでのみ利用可能だった脆弱性レポート（脆弱性修正レポート、脆弱性ステータスレポート、および脆弱性更新レポート）が、プロジェクトバージョンで利用できるようになりました。

## スニペットファイルサイズの構成

スニペットでスキャンされるデフォルトの最大ファイルサイズが可能になり、1MBから16MBまでの値を選択できるようになりました。

## マップされていないコードの場所のクリーンアップ構成

Black Duckでは、マップされていないコードの場所データを365日ごとにパージします。この機能を無効にして、マップされていないコードの場所データがパージされないようにすることができます。また、定期的にスキャンしてデータを頻繁に破棄するために、保持期間の日数をより短く設定することもできます。

## アクセストークン

ユーザーアクセストークンのスコープのオプションは、読み取りまたは読み書きになりました。

## サポートされるブラウザのバージョン

- Safariバージョン14.0.1 (14610.2.11.51.10)
- Chromeバージョン87.0.4280.88 (公式ビルド) (x86\_64)
- Firefox 83.0 (64ビット)
- Internet Explorer 11 11.630.19041.0

Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck2021.2.0リリース以降でのInternet Explorer 11のサポートを終了します。

- Microsoft Edge 87.0.664.60 (公式ビルド) (64ビット)

## コンテナバージョン

- blackducksoftware/blackduck-postgres : 1.0.16
- blackducksoftware/blackduck-authentication:2020.12.0
- blackducksoftware/blackduck-webapp:2020.12.0
- blackducksoftware/blackduck-scan:2020.12.0
- blackducksoftware/blackduck-jobrunner:2020.12.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash : 1.0.8
- blackducksoftware/blackduck-registration:2020.12.0
- blackducksoftware/blackduck-nginx : 1.0.26
- blackducksoftware/blackduck-documentation:2020.12.0
- blackducksoftware/blackduck-upload-cache : 1.0.15
- blackducksoftware/blackduck-redis:2020.12.0
- blackducksoftware/blackduck-bomengine:2020.12.0
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq : 1.2.2

## APIの機能強化

- createdAtフィールドでプロジェクト (api/projects) を並べ替える機能が追加されました。
- ある日付の前後に作成されたプロジェクトのapi/projectsエンドポイントにフィルタを適用する機能が追加されました。
- 脆弱性の影響解析機能の一部として、脆弱性マッチを表示するAPIが追加されました。

```
GET /api/projects/{projectId}/versions/{projectVersionId}/vulnerabilities/  
{vulnerabilityId}/vulnerability-matches
```

■ 次の構成表エンドポイントが追加されました。

- 構成表ステータス概要の取得 :

```
GET /api/projects/{projectId}/versions/{projectVersionId}/bom-status
```

- 構成表のイベントのリスト :

```
GET /api/projects/{projectId}/versions/{projectVersionId}/bom-events
```

- 失敗した構成表イベントの削除 :

```
DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events/  
{bomEventId}
```

- 失敗したすべてのイベントの構成表からの削除 :

```
DELETE /api/projects/{projectId}/versions/{projectVersionId}/bom-events
```

■ 新しいパスワード設定エンドポイント :

- パスワード設定の取得 :

```
GET /api/password/security/settings
```

- システムパスワード設定の取得 :

```
GET /api/password/management/settings
```

- システムパスワード設定の更新 :

```
PUT /api/password/management/settings
```

- パスワードの検証 :

```
POST /api/password/security/validate
```

■ /api/catalog-risk-profile-dashboard APIは、HTTP 404 (Not Found) を返すようになりました。

## 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2020.10.0が日本語にローカライズされました。

## 2020.12.0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-24839) 。[コンポーネントの追加/編集] ダイアログボックスで一部のコンポーネントのオリジナルIDを選択できなかった問題を修正しました。
- (Hub-24911) 。KBUUpdateJobが失敗してコンポーネントの更新がスキップされる問題を修正しまし

た。

- (Hub-25230)。ユーザーがライセンステキストを開いたり編集したりする際に、ライセンステキストウィンドウが表示されない問題を修正しました。
- (Hub-25452)。[ソース] タブでライセンス検索結果ページを表示する際にライセンスタイプを選択すると、[検出タイプ] フィルタが自動的に追加される問題を修正しました。
- (Hub-25489)。サブフォルダが変更されたときに[ソース] タブのフィルタがリセットされる問題を修正しました。
- (Hub-25603)。別のパスを選択したときに、[スニペットビュー] ダイアログボックスの[ソース] タブにある[マッチしたファイルパス] フィールドに表示されるパスが更新されるように、問題を修正しました。
- (Hub-25681)。汎用/未指定コンポーネントバージョンのライセンスをProtex BOMツールでインポートできない問題を修正しました。
- (Hub-25715)。マウスを使用しない限り、[カスタムフィールドの管理] ページの[アクティブ] ステータスを変更できない問題を修正しました。
- (Hub-25739)。構成表コンポーネントのすべてのコメントを表示できない問題を修正しました。
- (Hub-25874)。データが同じカラム名にあるにもかかわらず、`bom_component_custom_fields_date_time.csv` レポートに `components_date_time.csv` レポートと異なるデータがリストされる問題を修正しました。
- (Hub-26442)。プロジェクト所有者がスキャンをプロジェクトバージョン内から削除できない問題を修正しました。
- (Hub-26496)。コンポーネントの使用法が変更されたときにライセンスリスクが変更されたにもかかわらず、ライセンスリスクに対するポリシー違反が引き続きトリガーされる問題を修正しました。

## バージョン2020. 10. 1

### バージョン2020. 10. 1の新機能および変更された機能

#### コンテナバージョン

- blackducksoftware/blackduck-postgres : 1.0.13
- blackducksoftware/blackduck-authentication:2020.10.1
- blackducksoftware/blackduck-webapp:2020.10.1
- blackducksoftware/blackduck-scan:2020.10.1
- blackducksoftware/blackduck-jobrunner:2020.10.1
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash : 1.0.8
- blackducksoftware/blackduck-registration:2020.10.1
- blackducksoftware/blackduck-nginx : 1.0.26
- blackducksoftware/blackduck-documentation:2020.10.1
- blackducksoftware/blackduck-upload-cache : 1.0.15
- blackducksoftware/blackduck-redis:2020.10.1
- sigsynopsys/bdba-worker:2020.09-1
- blackducksoftware/rabbitmq : 1.2.2

## 2020. 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-25489)。別のフォルダを選択したときに[ソース]タブで選択されているフィルタがリセットされる問題を修正しました。
- (Hub-25515)。ホストインスタンスでTLS 1.3が動作している場合に、アップロード時に署名スキャナが失敗し、エラーメッセージ「エラー：ホストへの接続を保護できません」が表示される問題を修正しました。
- (Hub-25791)。バージョン2020. 4. 2からバージョン2020. 6. 1/2020. 6. 2にアップグレードした後に、スキャンにかかる時間が大幅に増加する問題を修正しました。
- (Hub-26027)。エラーメッセージ「エラー：アプリケーションに不明なエラーが発生しました。(正しくないリクエスト) エラー。error. {core.rest.common\_error}」が、Synopsys Detectスキャンのアップロード時にBlack Duckに表示される問題を修正しました。
- (Hub-26085)。バイナリスキャンで2番目の空のスキャンが追加される問題を修正しました。

## バージョン2020. 10. 0

### バージョン2020. 10. 0の新機能および変更された機能

#### 新しいカスタムコンポーネントダッシュボード

2020. 10. 0では、コンポーネントダッシュボードが、保存済みコンポーネント検索を使用できるカスタムコンポーネントダッシュボードに切り替わり、重要なコンポーネントバージョンを簡単に表示できるようになりました。Black Duckでは、さまざまな属性を使用してプロジェクト内で使用されるコンポーネントを検索し、検索を保存してから、この[ダッシュボード]ページを使用して保存済み検索からダッシュボードを表示できるようになりました。

カスタムコンポーネントダッシュボードでは、コンポーネントバージョンごとに次の情報が表示されます。

- 当該コンポーネントバージョンを使用しているプロジェクトバージョンの数、および各プロジェクトバージョンのフェーズ、ライセンス、レビューステータス、セキュリティ上のリスク
- リスクカテゴリ別の脆弱性の数
- ライセンスおよび運用上のリスク
- ポリシー違反
- 承認済みステータス
- 当該コンポーネントバージョンが最初に検出された日付
- Black Duckナレッジベースに基づく、コンポーネントがリリースされた日付
- 新しいバージョンの数
- このコンポーネントの脆弱性が最後に更新された日時

#### コンポーネント検索およびBlack Duckナレッジベース検索の機能強化

コンポーネントの検索は、コンポーネントの検索に使用できる属性と、検索結果に表示される情報によって強化されています。プロジェクトで使用されるコンポーネント検索とBlack Duckナレッジベースでのコンポーネント検索を簡単に区別できるように、UIも機能強化されました。

Black Duckナレッジベース検索の検索属性は変更されていませんが、Black Duckプロジェクトで使用され

ているコンポーネントバージョンを検索する場合に、次の属性を使用できます。

- セキュリティ上のリスク
- ライセンスリスク
- 運用上のリスク
- ポリシールール
- ポリシー違反の重大度
- レビューステータス
- コンポーネントの承認済みステータス
- 最初の検出
- ライセンスファミリ
- カスタムフィールドデータがない
- リリース日
- ライセンス
- 脆弱性CWE
- 脆弱性報告日

検索条件に一致するコンポーネントバージョンごとに、次の情報が表示されます。

- 当該コンポーネントバージョンを使用しているプロジェクトバージョンの数、および各プロジェクトバージョンのフェーズ、ライセンス、レビューステータス、セキュリティ上のリスク
- リスクカテゴリ別の脆弱性の数
- ライセンスおよび運用上のリスク
- ポリシー違反
- 承認済みステータス
- 当該コンポーネントバージョンが最初に検出された日付
- Black Duckナレッジベースに基づく、コンポーネントがリリースされた日付
- 新しいバージョンの数
- このコンポーネントの脆弱性が最後に更新された日時

これらのコンポーネントは、前述のように、検索結果を保存して[ダッシュボード]ページに表示できるようになりました。

ナレッジベースコンポーネント検索結果ごとに、次の情報が表示されます。

- 当該コンポーネントを使用しているプロジェクトバージョンの数、各プロジェクトバージョンのリスト、フェーズ、使用されているコンポーネントバージョン、関連するセキュリティ上のリスク
- コミットアクティビティ推移
- 最終コミット日
- コンポーネントバージョンの数
- このコンポーネントのタグ

### 保存済み検索の機能強化

Black Duckの[ダッシュボード]ページでは、保存済み検索をフィルタにかけたり並べ替えたりできるよう

になりました。

## ライセンスの競合

2020.10.0リリースでは、齟齬があるカスタムライセンス条項を指定できるようになりました。Black Duckナレッジベース条項またはユーザーのカスタムライセンス条項と競合している禁止/必須アクションに対しては、カスタムのライセンス条項を定義できます。

**Note:** 現在、プロジェクトバージョン構成表では、齟齬があるライセンス条項を表示することはできません。この機能は、将来のBlack Duckリリースで利用可能になる予定です。

## ライセンス管理の機能強化

次の新しい3つのフィルタが、[ライセンス管理]の[ライセンス条項]タブに追加されました。

- ライセンスに関連付けられている
- 齟齬がある条項が含まれている
- 責任

## 新しいコンポーネントの使用状況

Black Duckは、コンポーネントの使用状況を調べる必要があることを示すためにユーザーが使用できる使用法[未指定]を追加しました。[動的にリンク]などの既存のデフォルト値の代わりに、この使用法をデフォルト値として使用すると便利な場合があります。この場合、コンポーネントに正しい使用法値またはデフォルト値が割り当てられているかどうかの混乱が解消されます。

## 新しい階層

Black Duckは、最重要階層として指定できる階層0を追加しました。

この新しい階層により、次のデフォルトポリシールールが階層0を含むように変更されました。

- 脆弱性が高1よりも大きい外部階層0、階層1、または階層2プロジェクトなし
- 脆弱性が中3よりも大きい外部階層0、階層1、または階層2プロジェクトなし

既存の階層に変更はありません。

## カスタムフィールドの機能強化

カスタムフィールドに対して、次の機能拡張が行われました

- Black Duckで、カスタムフィールドが必須であることを示す機能が追加されました。
  - ・ カスタムフィールド情報を表示すると、警告メッセージ「\*その他のフィールドは必須です」が表示されます。ただし、必須のカスタムフィールドにデータが入力されていない場合でも、ユーザーは、カスタム以外のフィールド情報と必須以外のカスタムフィールドの情報をページで表示したり保存したりできます。
  - ・ 情報が欠落しているプロジェクトバージョン構成表内のコンポーネントを表示できるように、新しいフィルタ[カスタムフィールドデータがない]が構成表に追加されました。
- ブール型や単一選択フィールドタイプで、カスタムフィールド情報を表示する際にも、選択を解除できるオプションが追加されました。



## 許可された署名リスト

スキャンしたコードに含まれるオープンソースソフトウェアを判定するために、署名リストで、Black DuckがBlack Duckナレッジベースウェブサービスに送信する署名を定義します。署名スキャナに、新しい2つのパラメータが追加されました。このパラメータを使用して、バイナリファイル拡張子またはソースファイル拡張子の許可された署名リストを作成できます。各リストはオプションであり、他のリストとは独立して動作します。

- `--BinaryAllowedList x, y, z` (`x`、`y`、`z`は、SHA-1 (バイナリ) ファイルの承認済みファイル拡張子です)
- `--SourceAllowedList a, b, c` (`a`、`b`、`c`は、クリーンなSHA-1 (ソースコード) ファイルの承認済みファイル拡張子です)

## 脆弱性の影響解析の機能強化

脆弱性の影響解析に対して、次の機能強化が行われました。

- セキュリティ脆弱性が到達可能 (真) であるか到達不能 (偽) であるかを示すために、`security_date_time.csv` プロジェクトバージョンレポートの最後に新しい列 [到達可能] が追加されました。
- 新しいフィルタ [到達可能] がプロジェクトバージョンの [セキュリティ] タブに追加されました。

## レポートの機能強化

次のレポート機能が強化されました。

- `components_date_time.csv` プロジェクトバージョンレポートの最後に新しい列 [コメント] が追加され、各コンポーネントのコメントが一覧表示されるようになりました。
- マッチタイプを判定するために、`vulnerability-status-report_date_time.csv` レポートの最後に新しい列 [マッチタイプ] が追加されました。

## レポートデータベースの機能強化

次のカラムがコンポーネントマッチ表 (`component_matches`) に追加されました。

- `match_confidence`。スニペット、バイナリ、または部分的なファイルマッチを除いたうえで、マッチの信頼性を表します。
- `match_archive_context`。プロジェクトのルートディレクトリを基準とした、アーカイブ済みファイルへのローカルパスです。
- `snippet_confirmation_status`。スニペットマッチのステータスをレビューします。

## HTTP/2およびTLS 1.3

ブラウザに表示されるBlack Duck UIのセキュリティとレンダリングを改善するために、Black Duckは、Black Duck NGINXウェブサーバーでHTTP/2およびTLS 1.3をサポートするようになりました。Black Duck NGINXウェブサーバーは、HTTP/1.1およびTLS 1.2も引き続きサポートします。

## スキャンページのためのジョブに対する変更

BomVulnerabilityNotificationJobとLicenseTermFulfillmentJobでも、古い監査イベントが削除されました。

## APIの機能強化

- Black Duckのシングルサインオン (SSO) ステータスを確認するためのエンドポイントが追加されました。

GET /api/sso/status

- SAML/LDAP構成を取得するためのエンドポイントが追加されました (管理者専用)。

- SSO構成の読み取り:

GET /api/sso/configuration

- IDPメタデータファイルのダウンロード:

GET /api/sso/idp-metadata

- また以下のSSOエンドポイントも追加されました。

- SSO構成の更新:

POST /api/sso/configuration

- IDPメタデータファイルのアップロード:

POST /api/sso/idp-metadata

- 次の構成表階層型コンポーネントエンドポイントが追加されました。

- 階層型ルートコンポーネントのリスト:

GET /api/projects/{projectId}/versions/{projectVersionId}/hierarchical-components

- 階層型子コンポーネントのリスト:

GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/hierarchical-components/{hierarchicalId}/children

- 階層型子コンポーネントバージョンのリスト:

GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/hierarchical-components/{hierarchicalId}/children

- 脆弱性の通知APIに新しいフィールドが追加され、通知をさらに分類できるようになりました。これらの通知には、構成表で変更された脆弱性情報が含まれ、次のフィールドが含まれます。

- vulnerabilityNotificationCause

発生し、通知をトリガーした脆弱性イベントの種類についての情報。脆弱性の追加/削除、コメントの変更、修正の詳細の変更、脆弱性の重大度の変更、ステータスの変更などです。

- eventSource

通知を生成したソースの情報。スキャン、Black Duck KB更新、ユーザーアクション（修正、優先順位の変更、調整）などです。

- `/api/catalog-risk-profile-dashboard` APIは、HTTP 410 (GONE) を返すようになりました。

## サポートされるブラウザのバージョン

- Safariバージョン13.1.2 (14609.3.5.1.5)
- Chromeバージョン86.0.4240.80
- Firefox 82 (64ビット)
- Internet Explorer 11.572.19041.0

Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

- Microsoft Edge 86.0.622.51 (公式ビルド) (64ビット)

## コンテナバージョン

- `blackducksoftware/blackduck-postgres` : 1.0.13
- `blackducksoftware/blackduck-authentication`:2020.10.0
- `blackducksoftware/blackduck-webapp`:2020.10.0
- `blackducksoftware/blackduck-scan`:2020.10.0
- `blackducksoftware/blackduck-jobrunner`:2020.10.0
- `blackducksoftware/blackduck-cfssl`:1.0.1
- `blackducksoftware/blackduck-logstash` : 1.0.6
- `blackducksoftware/blackduck-registration`:2020.10.0
- `blackducksoftware/blackduck-nginx` : 1.0.26
- `blackducksoftware/blackduck-documentation`:2020.10.0
- `blackducksoftware/blackduck-upload-cache` : 1.0.15
- `blackducksoftware/blackduck-redis`:2020.10.0
- `sigsynopsys/bdba-worker` : 2020.09
- `blackducksoftware/rabbitmq` : 1.2.2

## 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2020.8.0が日本語にローカライズされました。

## 2020.10.0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-20559, 22100)。異なるルートディレクトリから同じコードの場所をスキャンしたとき、またはプロジェクトバージョンを複製したときに、スニペットの調整が失われていた問題を修正しました。
- (Hub-21421)。大規模プロジェクトで印刷機能が動作しない問題を修正しました。

- (Hub-23705、25560)。ユーザーが作成したレポートをユーザーが削除できなかった問題を修正しました。
- (Hub-23709)。スキャン時に次の`scan.cli.sh`警告メッセージが表示されていた問題を修正しました。「すべてのマニフェストからマニフェストを検出できません」
- (Hub-24330)。ProtexプロジェクトをBlack Duckバージョン2019.10.3にインポートしようとする、エラーメッセージ「キー値の重複は一意の制約に違反しています」が表示されていましたが、この問題を修正しました。
- (Hub-24673)。コンポーネント数が32,000を超えていると、[ダッシュボード]ページから移動するときに失敗する問題を修正しました。
- (Hub-24675)。`root_bom_consumer_node_id`が正しく設定されていなかった問題を修正しました。
- (Hub-24871)。リリース2019.10.0以降のPostgreSQLデータベースの拡張に関する問題を修正しました。
- (Hub-24772)。構成表印刷時のデフォルト.pdfファイル名がプロジェクト名とバージョン名でなかった問題を修正しました。
- (Hub-24839)。[コンポーネントの追加/編集]ダイアログボックスで一部のコンポーネントのオリジナルIDを選択できなかった問題を修正しました。
- (Hub-24947)。構成表にプロジェクトを追加した際に、検索結果の表示で一貫性が損なわれていた問題を修正しました。
- (Hub-25171)。APIを使用して修正した場合に、再スキャン (PUT /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/origins/{originId}/vulnerabilities/{vulnerabilityId}/remediation) するまで、脆弱性の件数が更新されなかった問題を修正しました。
- (Hub-25219)。APIを使用してレポートを作成する際の問題 (localeに指定したja\_JPが無視されるなど、locale指定時の問題) を修正しました。生成レポートの言語は、localeフィールドで正しく設定されるようになりました。
- (Hub-25234)。構成表を印刷する[印刷]ボタンに、バーグラフのカウントが表示されないことがあった問題を修正しました。
- (Hub-25240)。ブラウザまたはAPIが特定の脆弱性 (BDSA-2020-1674) の呼び出しで失敗していた問題を修正しました。
- (Hub-25241)。VersionBomComputationJobが次のエラーメッセージでスキャンに失敗する問題を修正しました。「データ整合性違反 (Constraint: not\_null, Detail: on column source\_start\_lines)」。
- (Hub-25244)。Black Duckリリース2020.4.2にアップグレードした後に、手動で追加したコンポーネントが構成表から削除されていた問題を修正しました。
- (Hub-25247)。Black Duck PostgreSQLログに、次のエラーメッセージが表示されていた問題を修正しました。エラー: キー値の重複は一意の制約「scan\_component\_scan\_id\_bdio\_node\_id\_key」に違反しています。
- (Hub-25321)。構成表ページをスクロールすると、テキストを表示すべきでないページ領域にテキストが表示されていた問題を修正しました。
- (Hub-25324)。[スキャン名]ページで、ワードラップが行われなかった問題を修正しました。
- (Hub-25478)。[セキュリティ]ページのセキュリティリスクフィルタが表示されなかった問題を修正しました。

- (Hub-25508)。以前のメディアタイプ (v4およびv5) がポリシールールAPI (GET /api/projects/{projectId}/versions/{projectVersionId}/components/{componentId}/versions/{componentVersionId}/policy-rules) に対して機能しないことがあった問題を修正しました。
- (Hub-25522、25523)。Chrome for Black Duckバージョン2020. 8. 0の構成表印刷プレビューウィンドウで発生していた表示形式の問題を修正しました。
- (Hub-25548)。階層ビューで新しいコンポーネントマッチを選択しても、ソースビューのコンポーネントマッチが更新されなかった問題を修正しました。
- (Hub-25570)。[セキュリティダッシュボード] ページで一部の領域が読み込まれなかった問題を修正しました。
- (Hub-25608)。脆弱性更新レポートの[新しい脆弱性] および[新たに修正された脆弱性] カテゴリで、脆弱性が2回カウントされていた問題を修正しました。
- (Hub-25649)。[ダッシュボード] ページのポリシー違反ポップアップウィンドウが閉じなかった問題を修正しました。
- (Hub-25841)。テキストデータ型のカスタムフィールドに入力した数値が日付形式に変換されていた問題を修正しました。

## バージョン2020. 8. 2

### バージョン2020. 8. 2の新機能および変更された機能

Black Duckバージョン2020. 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。

### 2020. 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。

- (Hub-24871)。リリース2019. 10. 0以降のPostgreSQLデータベースの拡張に関する問題を修正しました。
- (Hub-25967)。コンポーネントの使用法変更に整合性がなかった問題が修正されました。

## バージョン2020. 8. 1

### バージョン2020. 8. 1の新機能および変更された機能

#### マッピングされていないコードの場所を時間でクリーンアップする機能

Black Duckでは、Docker Swarmの実装のために、`blackduck-config.env` ファイル内に `blackduck.scan.processor.scanpurge.cronstring` 変数を設定して、スキャンパーシcronジョブを設定できるようになりました。

#### ポリシーの機能強化

Black Duckでは、脆弱性の修正ステータスに対して、ポリシーを作成できるようになりました。

#### コンテナバージョン

- `blackducksoftware/blackduck-postgres` : 1.0.13
- `blackducksoftware/blackduck-authentication` : 2020. 8. 1

- blackducksoftware/blackduck-webapp:2020. 8. 1
- blackducksoftware/blackduck-scan:2020. 8. 1
- blackducksoftware/blackduck-jobrunner:2020. 8. 1
- blackducksoftware/blackduck-cfssl:1. 0. 1
- blackducksoftware/blackduck-logstash:1. 0. 6
- blackducksoftware/blackduck-registration:2020. 8. 1
- blackducksoftware/blackduck-nginx:1. 0. 25
- blackducksoftware/blackduck-documentation:2020. 8. 1
- blackducksoftware/blackduck-upload-cache:1. 0. 15
- blackducksoftware/blackduck-redis:2020. 8. 1
- sigsynopsys/bdba-worker:2020. 06-2
- blackducksoftware/rabbitmq:1. 2. 1

## 2020. 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-24149)。実行した操作に関係なく「エラー: StatusLoggerが認識されていません...」というエラーメッセージが表示される、Protex構成表ツールの問題を修正しました。
- (Hub-24480)。Black Duckをバージョン2020. 4. 1にアップグレードした場合に、Protexからインポートしたコンポーネントが、無視済みステータスを失っていた問題を修正しました。
- (Hub-25254)。配布タイプの変更にポリシー違反が誤ってトリガーされていた問題を修正しました。
- (Hub-25269、25416)。長時間実行中のクエリにより、スキャンがブロックされたり、PostgreSQLデータベースでデッドロックが発生したりする問題を修正しました。
- (Hub-25387)。KbUpdateJobが断続的に失敗する問題を修正しました。
- (Hub-25509)。Black Duckバージョン2020. 4. 2でデータベースサイズが急増していた問題を修正しました。

## バージョン2020. 8. 0

### バージョン2020. 8. 0の新機能および変更された機能

#### 脆弱性の影響を解析する機能

Black Duckでは、最初に対処すべき脆弱性を優先できるように、Javaアプリケーションから呼び出される外部のパブリックメソッドが既知の脆弱性に関与している可能性があるかどうかを判別できるようになりました。Black Duckは、ソースコード内で呼び出される完全修飾パブリック機能名を判定し、脆弱性によって悪用される既知の関数名と照合できます。自分のJavaアプリケーションから呼び出す外部パブリックメソッドが既知の脆弱性に関与している可能性があるかどうかを把握することで、どの脆弱性に集中する必要がありますかを優先付けできます。

この機能は、Synopsys Detectバージョン6. 5以降（およびSynopsys Detect6. 5以降を使用するSynopsys Detect (Desktop)）で、Javaアプリケーションのみを対象に使用できます。

次の点に注意してください。

- Synopsys Detectが検出できるのは、脆弱な可能性のある関数を呼び出すJavaパブリックメソッド内の脆弱性のみです。
- この機能では、BDSAでの到達可能な関数のみが表示されます。

## 新しいコンテナおよびシステム要件

新しいRedisコンテナがBlack Duckに追加されました。このコンテナにより、Black Duckのキャッシュ機能の整合性が向上し、アプリケーションのパフォーマンスが改善します。

すべてのコンテナの単一インスタンスを実行するために必要な現在の最小ハードウェアは次のようになりました。

- 5 CPU
- Redisの最小構成の場合は21 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は24 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に250GBの空きディスク容量
- データベースバックアップに適した容量

Black Duck - Binary AnalysisでBlack Duckを実行するために必要な最小ハードウェアは次のようになりました。

- 6 CPU
- Redisの最小構成の場合は25 GB RAM、Redis駆動キャッシュ用のより可用性の高い最適化構成の場合は28 GB RAM
- データベースおよびその他のBlack Duckコンテナ用に350 GBの空きディスク容量
- データベースバックアップに適した容量

**Note:** binaryscannerコンテナを1個追加するごとに、CPU、2GB RAM、100GBの空きディスク容量の追加が必要です。

## カスタムシステムアナウンス

システム管理者は、Black Duckユーザーに対して、カスタムのサインオンメッセージやサインオン後メッセージを作成できるようになりました。

たとえば、近日中に実施されるイベントについてユーザーに通知する場合や、不正使用により引き起こされる事態を示す免責事項を表示する必要がある場合に、システムアナウンスを使用できます。

次の4種類のメッセージを作成できます。

- ログイン。ユーザーがBlack Duckにログインするときに表示されるメッセージ。
- バナー。すべてのページの上部に表示されるメッセージ。
- フッター。すべてのページのフッターに表示されるメッセージ。
- ようこそ。ユーザーがBlack Duckにログインした後に表示されるメッセージ。

## プロジェクトバージョンレポートの機能強化

### 新しいアップグレードガイダンス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に、新しいレポート、`project_version_upgrade_guidance_`



`date_time.csv`が追加されました。

このレポートの内容：

- コンポーネントバージョンの詳細（取得元の情報や脆弱性の総数を含む）
- アップグレード先のバージョン/取得元、およびその詳細（脆弱性の総数など）を含むコンポーネント（存在する場合）の短期的なアップグレードガイダンス
- アップグレード先のバージョン/取得元、およびその詳細（脆弱性の総数など）を含むコンポーネント（存在する場合）の長期的なアップグレードガイダンス

このレポートの列：

- コンポーネントID
- コンポーネントバージョンID
- コンポーネント取得元ID
- コンポーネント名
- コンポーネントバージョン名
- コンポーネント取得元名
- コンポーネント取得元ID
- コンポーネント取得元バージョン名
- 既知の脆弱性の総数
- 短期推奨バージョンID
- 短期推奨バージョン名
- 短期推奨コンポーネント取得元ID
- 短期推奨取得元名
- 短期推奨取得元ID
- 短期推奨取得元バージョン名
- 短期的に緊急の脆弱性
- 短期的に高の脆弱性
- 短期的に中の脆弱性
- 短期的に低の脆弱性
- 長期推奨バージョンID
- 長期推奨バージョン名
- 長期推奨コンポーネント取得元ID
- 長期推奨取得元名
- 長期推奨取得元ID
- 長期推奨取得元バージョン名
- 長期的に緊急の脆弱性
- 長期的に高の脆弱性
- 長期的に中の脆弱性
- 長期的に低の脆弱性



### security\_date\_time.csvレポートに追加された新しい列

security\_date\_time.csvプロジェクトバージョンレポートに追加された新しい列:

- CVSSバージョン。脆弱性評価システムのバージョン: CVSS 2.0またはCVSS 3.x。
- マッチタイプ。

### 署名スキャナの機能強化

署名スキャナからBlack Duckにスキャンデータをストリーム（バッファ）する方法を制御する2つの新しいプロパティが署名スキャナに追加されました。まれに、ネットワークに合わせてこれらの値の変更が必要になることがあります。たとえば、ネットワークに問題がある場合は値を下げ、ネットワークが非常に安定している場合はデフォルト値を大きくします。

- **max-request-body-size**。スキャンされたパスのスキャンデータをアップロードするメインリクエストのサイズ。
- **max-update-size**。署名スキャナが個別のURI（スキャンされたパス）のデータの更新を完了したときに、Black Duckに通知する更新リクエストのバッファサイズ。

### APIの機能強化

- 特定のBlack Duckユーザーの最終ログイン日を取得します。

```
GET /api/users/{userId}/last-login
```

2020.8.0へのアップグレードに伴い、すべてのユーザーのデフォルトの最終ログイン日がアップグレード日になりますが、それ以降は実際のログインデータが使用されます。デフォルトでは、このエンドポイントには、過去30日間にログインしていないすべてのユーザーが表示されますが、`?sinceDays=クエリパラメータ`を追加して、検索期間を任意の日数に変更できます。また、作成済みのユーザーの内、システムにログインしたことのないユーザーも表示されます。

- 活動していないユーザーを検索します。

```
GET /api/dormant-users
```

- アナウンス用に新しく追加されたエンドポイント:

- ログインアナウンスを作成します。

```
POST /api/manage-announcement/login
```

- ようこそアナウンスを作成します。

```
POST /api/manage-announcement/welcome
```

- バナーアナウンスを作成します。

```
POST /api/manage-announcement/banner
```

- フッターアナウンスを作成します。

```
POST /api/manage-announcement/footer
```

- ログインアナウンスを編集します。

PUT /api/manage-announcement/login/{announcementId}

- ようこそアナウンスを編集します。

PUT /api/manage-announcement/welcome/{announcementId}

- バナーアナウンスを編集します。

PUT /api/manage-announcement/banner/{announcementId}

- フッターアナウンスを編集します。

PUT /api/manage-announcement/footer/{announcementId}

- ログインアナウンスを削除します。

DELETE /api/manage-announcement/login/{announcementId}

- ようこそアナウンスを削除します。

DELETE /api/manage-announcement/welcome/{announcementId}

- バナーアナウンスを削除します。

DELETE /api/manage-announcement/banner/{announcementId}

- フッターアナウンスを削除します。

DELETE /api/manage-announcement/footer/{announcementId}

- ログインアナウンスを取得します。

GET /api/manage-announcement/login

- ようこそアナウンスを取得します。

GET /api/manage-announcement/welcome

- バナーアナウンスを取得します。

GET /api/manage-announcement/banner

- フッターアナウンスを取得します。

GET /api/manage-announcement/footer

- ID別にログインアナウンスを取得します。

GET /api/manage-announcement/login/{announcementId}

- ID別にようこそアナウンスを取得します。

GET /api/manage-announcement/welcome/{announcementId}

- ID別にバナーアナウンスを取得します。

GET /api/manage-announcement/banner/{announcementId}

- ID別にフッターアナウンスを取得します。
- GET /api/manage-announcement/footer/{announcementId}
- ユーザーログインアナウンスを取得します。

GET /api/announcement/login

- ユーザーようこそアナウンスを取得します。

GET /api/announcement/welcome

- ユーザーバナーアナウンスを取得します。

GET /api/announcement/banner

- ユーザーフッターアナウンスを取得します。

GET /api/announcement/footer

- ID別にユーザーログインアナウンスを取得します。

GET /api/announcement/login/{announcementId}

- ID別にユーザーようこそアナウンスを取得します。

GET /api/announcement/welcome/{announcementId}

- ID別にバナーアナウンスを取得します。

GET /api/announcement/banner/{announcementId}

- ID別にユーザーフッターアナウンスを取得します。

GET /api/announcement/footer/{announcementId}

- ようこそアナウンスを抑制します。

POST /api/announcement/welcome/{announcementId}/suppress

- API取得元応答に、新しいオプションのoriginUrlフィールドが追加されました。
- api/projects/id/versions/id/referencesに、構成表API (api/projects/id/versions/id/components) リファレンスが追加されました。
- api/codelocations/id/scan-summariesの応答に、createdByUserNameが追加されました。
- /api/projects/versions/hierarchical-componentsにcomponentTypeフィールドが追加され、アイテムのcomponentTypeがSUB\_PROJECTの場合、メタデータにprojectおよびprojectVersionリンクを含むようになりました。
- vulnerabilityWithRemediationブロックの下にある/api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-componentsに、relatedVulnerabilityリンクが追加されました。
- /api/projects/{projectId}/versions/{projectVersionId}/vulnerable-bom-componentsに、

remediationCreatedByおよびremediationUpdatedByが追加されました。

- 非推奨のエンドポイント:

- 修正オプションの一覧表示: GET /api/components/{componentId}/versions/{componentVersionId}/remediating.

このエンドポイントは、GET /api/components/{componentId}/versions/{componentVersionId}/upgrade-guidanceで置き換えられました。

## サポートされるブラウザのバージョン

- Safariバージョン13.1.2 (14609.3.5.1.5)
- Chromeバージョン84.0.4147.125 (公式ビルド) (64ビット)
- Firefox 79.0 (64ビット)
- Internet Explorer 11.450.19041.0

Internet Explorer 11のサポートは廃止されます。Synopsysは、Black Duck 2021.2.0 リリース以降でのInternet Explorer 11のサポートを終了します。

- Microsoft Edge 44.19041.423.0
- Microsoft EdgeHTML 18.19041

## コンテナバージョン

- blackducksoftware/blackduck-postgres: 1.0.13
- blackducksoftware/blackduck-authentication: 2020.8.0
- blackducksoftware/blackduck-webapp: 2020.8.0
- blackducksoftware/blackduck-scan: 2020.8.0
- blackducksoftware/blackduck-jobrunner: 2020.8.0
- blackducksoftware/blackduck-cfssl: 1.0.1
- blackducksoftware/blackduck-logstash: 1.0.6
- blackducksoftware/blackduck-registration: 2020.8.0
- blackducksoftware/blackduck-nginx: 1.0.25
- blackducksoftware/blackduck-documentation: 2020.8.0
- blackducksoftware/blackduck-upload-cache: 1.0.15
- blackducksoftware/blackduck-redis: 2020.8.0
- sigsynopsys/bdba-worker: 2020.03-1
- blackducksoftware/rabbitmq: 1.2.1

## 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2020.6.0が日本語にローカライズされました。

## 2020.8.0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-23467)。マッチ数が1,300件以上ある場合に、[スキャン] ページに「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る問題を修正しました。
- (Hub-23892)。[スキャン] ページの[スキャンサイズ] 列が空だった問題を修正しました。
- (Hub-23937、24799)。[ライセンス管理] ページのロードが失敗する問題を修正しました。
- (Hub-24009)。Synopsys Detectの出力で、コード400で構成表インポートが直ちに失敗し、hub\_scan\_errors.logに「ドキュメントnullのドキュメントデータの保存に失敗しました」というメッセージが表示される問題を修正しました。
- (Hub-24112)。プロジェクトバージョンの[ソース] タブで選択されているノードがなくなったときでも、ユーザーがマッチ数フィルタビューに戻ることができるように、問題を修正しました。
- (Hub-24278)。バイナリスキャンファイルのアップロードが、次のエラーメッセージが表示されて失敗する問題を修正しました: 「バイナリスキャンのアップロード時の不明なステータスコード: 0, null」。
- (Hub-24291)。32,767を超えるコンポーネントを表示しようとしたときに、[構成表] ページに「アプリケーションに不明なエラーが発生しました」と表示される問題を修正しました。
- (Hub-24407)。スニペットのクローンを作成するときに「文字列からシリアル化を解除できません」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-24432)。32,000を超えるプロジェクトを表示しようとしたときに[ダッシュボード] ページが読み込まれない問題を修正しました。
- (Hub-24451)。認証プロキシを使用してBlack Duckナレッジベースを呼び出したときに、HUB\_PROXY\_PASSWORD\_FILE docker secretが無視される問題を修正しました。
- (Hub-24480)。ProtexをBlack Duck 2020.4.1にインポートしたときにコンポーネントの変更が失われる問題を修正しました。
- (Hub-24529)。Black Duckナレッジベースで「パッチ適用済み」ステータスが示されているコンポーネントに対して、誤ってポリシー違反がトリガーされる問題を修正しました。
- (Hub-24583、25244)。Black Duckナレッジベースが更新されたときに手動で追加したコンポーネントが削除される問題を修正しました。
- (Hub-24646)。Black Duckのアップグレード時に発生していた、[ライセンス管理] ページでナレッジベースライセンスが更新されても、その変更を行ったユーザーが識別されない問題を修正しました。
- (Hub-24673)。コンポーネント数が32,000を超えていると、[ダッシュボード] ページから[コンポーネント] ページに移動するときに失敗する問題を修正しました。
- (Hub-24716)。無視しているコンポーネントの脆弱性通知が表示される問題を修正しました。
- (Hub-24739)。LDAPユーザーの電子メールアドレスを変更できない問題を修正しました。
- (Hub-24740)。bom\_component\_custom\_fields\_date\_time.csvレポートに、無視しているコンポーネントのみが表示される問題を修正しました。
- (Hub-24758)。スニペットを並列表示したときに、プロジェクトバージョンの[ソース] タブの左側で、マッチしたコードが完全には強調表示されない問題を修正しました。
- (Hub-24845)。[概要] タブの[統計情報] セクションが更新されない問題を修正しました。
- (Hub-24866)。ルートのサブディレクトリの一部を除外して、ディスク上のルート全体をスキャンしようとしたときに、署名スキャナが「正しくないリクエスト」エラーを報告する問題を修正しました。
- (Hub-24885)。階層ビューでプロジェクトバージョンの[ソース] タブにマッチを表示しようとする

と、「アプリケーションに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-24968)。セキュリティダッシュボードを表示しようとしたときに、「Black Duck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る問題を修正しました。
- (Hub-25072)。名前にチルダ文字 (~) が含まれるコンポーネントのポリシーを作成すると、「アプリケーションに不明なエラーが発生しました」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。
- (Hub-25115)。パラメータの数が32,767個を超えるとスキャンが失敗する問題を修正しました。
- (Hub-25166)。Istio環境でのpostgres-initポッドの問題を修正するために、pre-およびpost-コマンドを追加しました。

## バージョン2020. 6. 2

### バージョン2020. 6. 2の新機能および変更された機能

Black Duckバージョン2020. 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。

### 2020. 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-24918)。BdioDataTransferJobおよびVersionBomComputationジョブがスキャンデータを正しく読み取っていなかったことが原因でスキャンの結果が返されないことがある問題を修正しました。

## バージョン2020. 6. 1

### バージョン2020. 6. 1の新機能および変更された機能

Black Duckバージョン2020. 6. 1はメンテナンスリリースであり、新機能や変更された機能はありません。

### 2020. 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-23970)。著作権オプションが選択されていると通知ファイルを生成できない問題を修正しました。
- (Hub-24106)。ナレッジベースサービスにアクセスできないことが原因でKbUpdateジョブが失敗する問題を修正しました。
- (Hub-24651)。プロジェクトマネージャおよび構成表マネージャの役割を持つユーザーが /api/projects/ ページでリリースフェーズフィルタを使用できない問題を修正しました。
- (Hub-24721)。Black Duckセキュリティアドバイザリ (BDSA) がライセンスされたモジュールではない場合に、構成表コンポーネントレポートが失敗する問題を修正しました。
- (Hub-24739)。LDAPユーザーの電子メールアドレスを変更できない問題を修正しました。
- (Hub-24765)。SNIPPET\_MATCHINGオプションを使用してスキャンしたときにスニペットが識別されないことがある問題を修正しました。

## バージョン2020. 6. 0

### バージョン2020. 6. 0の新機能および変更された機能

#### 保存された検索を含む新しいプロジェクトダッシュボード

Black Duckには、プロジェクトの1つ以上のバージョンに含まれるコンポーネントに関連する、リスクのタイプと重大度およびポリシー違反を表示できるように、ダッシュボードが用意されています。ダッシュボードは、すべてのプロジェクトとプロジェクトバージョンにわたる全体的なビューです。

重要なプロジェクトとプロジェクトのバージョンを表示できるように、2020. 6. 0では、プロジェクトダッシュボードが2つの新しいデフォルトダッシュボードに代わり、無制限の数のカスタムダッシュボードを作成できるようになりました。

Black Duckには、次の2つのデフォルトのダッシュボードが表示されます。

- **ウォッチ**。ウォッチするプロジェクト。
- **マイプロジェクト**。ウォッチしていないプロジェクトを含むすべてのプロジェクト。

これらのダッシュボードは、プロジェクトレベルの新しい[ダッシュボード]ページに情報を表示します。[プロジェクトダッシュボード]ページが、この[ダッシュボード]ページに代わりました。

さらに、重要なプロジェクトバージョンをすばやく表示できるように、カスタムダッシュボードを作成することもできます。Black Duckでは、さまざまな属性を使用してプロジェクトを検索し、検索を保存してから、このページを使用して保存された検索からダッシュボードを表示できるようになりました。保存された検索に基づくダッシュボードには、プロジェクトのバージョンレベルで情報が表示されます。

[ウォッチ]ダッシュボードと[マイプロジェクト]ダッシュボードに表示される情報は、リアルタイムに更新されます。新しいジョブSearchDashboardRefreshJobは、5分ごとにカスタムダッシュボードを更新します。



をクリックすると、ダッシュボードが表示されます。表示されていない場合は、[ダッシュボード]を選択してこれらのダッシュボードを表示します。

#### プロジェクト検索の機能強化

プロジェクトの検索は、プロジェクトの検索に使用できる属性と、検索結果に表示される情報によって強化されています。

次の属性を使用して、Black Duckでプロジェクトを検索できるようになりました。

- **ウォッチ**。このプロジェクトがウォッチするプロジェクトかどうかを選択します。
- **セキュリティリスク**。
- **ライセンスリスク**。
- **運用リスク**。
- **ポリシールール**。リストからポリシールールを選択して、このポリシーに違反するプロジェクトを検索します。
- **ポリシー違反**。ポリシールールの重大度レベル。
- **配布**。

- 最終スキャン日。
- リリースフェーズ。
- 階層。

検索結果には、検索条件を満たすプロジェクトバージョンが表示されます。プロジェクトのバージョンごとに、次の数を表示できます。

- 検出された結果とデータベースが最後に更新された時刻。
- セキュリティ、ライセンス、または運用リスクが最も高いレベルにあるコンポーネント。
- リスクカテゴリごとのコンポーネント。
- このプロジェクトバージョンのポリシーの重大度が最も高いコンポーネント。
- 重大度レベル別のポリシー違反のあるコンポーネント。

プロジェクトバージョンごとに、検索結果に次の情報も表示されます。

- このプロジェクトバージョンのコンポーネントの数。
- 最終スキャン日。
- このプロジェクトバージョンが最後に更新された日時です。
- このプロジェクトバージョンのライセンス。
- このプロジェクトバージョンのフェーズ。
- このプロジェクトバージョンの配布。

前述のように、検索結果を保存してダッシュボードに表示できるようになりました。

## 埋め込み著作権情報の検出

Black Duckでは、埋め込み著作権情報のインスタンスを検出できるようになりました。コードのスキャン時に著作権データ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、オープンソースソフトウェアや専有著作権情報を検出して管理することで、ライセンスコンプライアンスのリスクを軽減できます。

この機能を使用して、Black Duckは著作権文字列のテキスト検索を実行し、見つかったテキストを[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、レビュー担当者が検出されたファイル内の著作権テキストを[ソース]タブ内から表示できるようにします。

## プロジェクトのクローン作成

Black Duckでは、プロジェクトのクローンを作成する機能が提供されるようになりました。プロジェクトのクローン作成を使用して、既存のプロジェクトを新しいプロジェクトにフォークします。クローンの作成により、既存のプロジェクトで定義したデータ、分析、および解決策を、新しいプロジェクト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。

プロジェクトを作成できるユーザーは、プロジェクトのクローンを作成できます。プロジェクトごとに、クローンを作成するバージョンとプロジェクトの属性（プロジェクトの設定、プロジェクトメンバー、グループなど）を選択します。



## ポリシー管理の機能強化

- ポリシー管理では、次に基づいてポリシールールを作成する機能が提供されるようになりました。
  - ・ ライセンスの有効期限
  - ・ ブール、日付の構成表コンポーネントカスタムフィールド。ドロップダウン、複数選択、単一選択、およびテキストフィールドタイプ。
  - ・ プロジェクトフィルタに、ブール型、複数選択型、テキストフィールド型のプロジェクトカスタムフィールドが含まれるようになりました。
- 複数のライセンスを持つコンポーネントのライセンスポリシー条件を評価するためのロジックが変更され、新しいポリシー違反が発生したり、コンポーネントがポリシー違反をトリガーしなくなったりする可能性があります。

1つ以上のライセンス条件（ライセンス、ライセンスステータス、ライセンスファミリ、および/またはライセンス有効期限）を使用して作成されたポリシールールに対して複数のライセンスを持つコンポーネントを評価する場合、各ライセンスが評価され、ポリシー違反に対してすべてのライセンス条件が真でなければなりません。ライセンスリスクがポリシー条件として含まれている場合、ライセンスリスクは個別に評価されます。他のライセンスポリシー条件を満たすライセンスだけでなく、コンポーネントのすべてのライセンスが評価されます。したがって、あるライセンスが複数の条件のポリシールールを満たし、そのコンポーネントの別のライセンスがライセンスリスク条件を満たしている場合に、ポリシー違反がトリガーされることがあります。

## 外部データベースでサポートされるPostgreSQL 11.7

Black Duckは、外部PostgreSQLを使用する新規インストール用にPostgreSQL 11.7をサポートするようになりました。PostgreSQL 9.6は引き続き外部PostgreSQLインスタンスに対して完全にサポートされていますが、Synopsysは、外部PostgreSQLを使用する新規インストールには、PostgreSQL 11.7を推奨しています。

内部PostgreSQLコンテナのユーザーの場合は、PostgreSQL 9.6が引き続きBlack Duck 2020.6.0でサポートされるバージョンです。

## 数値ユーザー名は、外部PostgreSQLデータベースでサポートされます

外部PostgreSQLインスタンスは、数字のみで構成されるユーザー名がサポートされるようになりました。

## 通知ファイルレポートの機能強化

不明なライセンスファミリのライセンスは、通知ファイルレポートから除外されるようになりました。

## 個々のプロジェクトで利用可能になった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は、アクセス権を持つ1つ以上のプロジェクトに対して実行できるようになりました。

レポートがグローバルレベルかプロジェクトレベルかを区別するために、これらのレポートのファイル名は次のように変更されています。

- レポートのグローバルバージョンの場合、`vulnerability-remediation-report_all_assigned_projects_YYYY-MM-DD_HHMMSS` (UTCのタイムスタンプ)
- 1つ以上のプロジェクトの場合、`vulnerability-remediation-report_YYYY-MM-DD_HHMMSS` (UTCのタイムスタンプ)

- レポートのグローバルバージョンの場合、`vvulnerability-status-report_all_assigned_projects_YYYY-MM-DD_HHMMSS` (UTCのタイムスタンプ)
- 1つ以上のプロジェクトの場合、`vulnerability-status-report_YYYY-MM-DD_HHMMSS` (UTCのタイムスタンプ)
- レポートのグローバルバージョンの場合、`vulnerability-update-report_all_assigned_projects_YYYY-MM-DD_HHMMSS` (UTCのタイムスタンプ)
- 1つ以上のプロジェクトの場合、`vulnerability-update-report_YYYY-MM-DD_HHMMSS` (UTCのタイムスタンプ)

## ソース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

`source_date_time.csv` レポートは次の情報で拡充されました。

- [スキャン] 列がレポートの最後に追加されました。プロジェクトバージョンの構成表には、プロジェクトバージョンにマッピングされた複数のスキャンを含めることができるため、この列には、この一致が見つかったスキャンが一覧表示されます。
- [パス] 列に依存関係マッチに関する情報が表示されるようになりました。直接的な依存関係の場合、列に依存関係のIDが表示され、一致コンテンツ値が表示されます。推移的な依存関係の場合、列には最上位レベルのコンポーネントから宣言されたコンポーネントへの完全な依存関係パスが表示されず。

## CVSSv3.1のサポート

Black DuckはCVSS v3.1スコアをサポートするようになりました。CVSSv3.1では、スコアリングの実行方法を明確にするスコア基準が更新されました。新しいメトリックベクトルや値はありませんが、明確化により全体的なスコアが変化する可能性があります。

## レポートデータベースの機能強化

CVSS 3.xをサポートするために、`component_vulnerability`の表に次の列が追加されました。

- `severity_cvss3`
- `base_score_cvss3`
- `exploit_score_cvss3`
- `impact_score_cvss3`
- `temporal_score_cvss3`

## 再スキャン時に部分的なスニペット調整を保持するオプション

Black Duckでは、ファイルを再スキャンするときに部分的なスニペットマッチから識別情報を適用できるように設定することができるようになりました。これにより、再識別が必要なスニペットの数が最小限に抑えられます。


## 新しい監査イベント

監査イベントは、ユーザーが次の操作を行うと表示されるようになりました。

- ポリシーを作成し、Black Duckがプロジェクトバージョンを評価します。
- ポリシーを更新し、Black Duckがプロジェクトバージョンを評価します。
- ポリシーを有効化し、Black Duckがプロジェクトバージョンを評価します。

- ポリシーを無効化し、Black Duckは対応するポリシー違反をクリアします。
- ポリシーを削除し、Black Duckは対応するポリシー違反をクリアします。

## 構成表ページの新しい情報アイコン

[構成表] ページでは、情報アイコン (  ) を使用して、調整フィールドまたはカスタムフィールドの追加情報があるかどうかを示します。

- アイコンにカーソルを合わせると、調整があるか、追加のフィールドがあるかが表示されます。
- アイコンを選択して、追加情報を表示する[コンポーネントの詳細] ダイアログボックスを開きます。

## APIの機能強化

- 一致操作中に発生するコンポーネントインポートイベントのリストを提供する新しいエンドポイントが追加されました。

```
GET /api/bom-import/{graphId}/component-import-events
```

- 一致操作中に発生するコンポーネントインポートイベントの数 (ステータス別) を提供する新しいエンドポイントが追加されました。

```
GET /api/bom-import/{graphId}/component-import-events-count
```

- 構成表がどのスキャンに属しているかを調べるためのAPIが追加されました。このAPIは、関連するスキャンによって検出されたエントリのリストを提供します。

```
GET /api/scan/{scanId}/bom-entries
```

- 著作権検索のサポートが追加され、ソースビューAPIの著作権検索用に新しいフィルタが追加されました。
- 最新のスキャンサマリAPIを改善しました。

```
GET /api/codeLocations/{codeLocationId}/latest-scan-summary
```

## サポートされるブラウザのバージョン

- Safariバージョン13.1.1 (14609.2.9.1.3)
- Chromeバージョン83.0.4103.97 (公式ビルド) (64ビット)
- Firefox 77.0.1 (64ビット)
- Internet Explorer 11.836.18362.0
- Microsoft Edge 44.18362.449.0

## コンテナバージョン

- blackducksoftware/blackduck-postgres:1.0.13
- blackducksoftware/blackduck-authentication:2020.6.0
- blackducksoftware/blackduck-webapp:2020.6.0
- blackducksoftware/blackduck-scan:2020.6.0
- blackducksoftware/blackduck-jobrunner:2020.6.0
- blackducksoftware/blackduck-cfssl:1.0.1

- blackducksoftware/blackduck-logstash : 1.0.6
- blackducksoftware/blackduck-registration:2020.6.0
- blackducksoftware/blackduck-nginx : 1.0.25
- blackducksoftware/blackduck-documentation:2020.6.0
- blackducksoftware/blackduck-upload-cache : 1.0.14
- sigsynopsys/bdba-worker:2020.03-1
- 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2020.4.0が日本語にローカライズされました。

## 2020.6.0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-20003)。[コンポーネントの追加] ダイアログボックスでカスタムコンポーネントが識別されるように問題を修正しました。
- (Hub-22599) プロジェクトバージョンのクローン作成時にUIがタイムアウトになる問題を修正しました。
- (Hub-22695) プロジェクトバージョンをクローン作成して再スキャンした後、手動で識別されたコンポーネントが欠落していた問題を修正しました。
- (HUB-22812) 構成表の印刷時にフィルタが無視される問題を修正しました。
- (HUB-23502) --certificate-file-pathパラメータを指定せずにBlack DuckをOpenShiftネイティブモードで展開した場合、証明書に「サブジェクトの別名」が生成されない問題を修正しました。
- (HUB-23601) プロジェクト名[設定]タブの[所有者]ドロップダウンメニューに、可能なすべての選択項目が表示されるように問題を修正しました。
- (HUB-23736) HierarchicalVersionBomJobが正常に実行されない問題を修正しました。
- (HUB-23798) サブプロジェクトを[コンポーネント]ダッシュボードからコンポーネントとして編集するときに404エラーが表示される問題を修正しました。
- (HUB-23909、23925) プロジェクトバージョンの[セキュリティ]タブで、ステータスに関係なく脆弱性を表示できない問題を修正しました。
- (Hub-23984) 役割が割り当てられていないユーザーのGET /api/projectsエンドポイントに対して、すべてのプロジェクトが返される問題を修正しました。
- (Hub-23985) 一致を選択するか、[ファイルツリーに表示]オプションを使用しても、ソースツリー内のファイルまでスクロールしない問題を修正しました。
- (Hub-23994) Black Duck - Binary Analysisが、アップロードされたバイナリファイルをクリーンアップしなかった問題を修正しました。
- (Hub-24011) スニペットスキャンで「413リクエストのエンティティが大きすぎます」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-24040) jobrunnerがハングし、ジョブが完了しない問題を修正しました。
- (Hub-24097) コンポーネントのバージョンを更新した後、使用法の編集内容が保持されない問題を修正しました。

- (Hub-24107) 著作権オプションを選択したときに、通知ファイルレポートがパラメータが多すぎて失敗する問題を修正しました。
- (Hub-24239) `api/projects/<projectid>/versions/<versionid>/policy-status`に400エラーが表示される問題を修正しました。
- (Hub-24286) [コンポーネント名バージョン]ページに、コンポーネントバージョンがソフト削除されたにもかかわらず、表示される問題を修正しました。
- (Hub-24308) 空のサブプロジェクトが[構成表]ページのソースとして「componentCountコンポーネント」を表示する問題を修正しました。

## バージョン2020. 4. 2

### バージョン2020. 4. 2の新機能および変更された機能

#### コンテナバージョン

- `sigsynopsys/bdba-worker`:2020. 03-1

### 2020. 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-22837)。プロジェクトバージョンの構成表のすべてのコンポーネントが新しい脆弱性データで更新されていないという問題を修正しました。
- (Hub-23581)。webAppコンテナが再起動し続ける問題を修正しました。
- (Hub-23869)。ソースのアップロードのオプションも有効にしていると、スニペットスキャンを有効にしたときに、埋め込みライセンスの検索結果が表示されない問題を修正しました。
- (Hub-24006)。[ライセンス管理]ページを使用して多数のコンポーネントでライセンスを更新すると、webappコンテナがクラッシュする問題が修正されました。

## バージョン2020. 4. 1

### バージョン2020. 4. 1の新機能および変更された機能

Black Duckバージョン2020. 4. 1では、スキャン機能が強化されています。

### 2020. 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。

- (Hub-22188)。「Parent of <path> does not exist.」というエラーメッセージが表示されて、スキャンが失敗する問題が修正されました。
- (Hub-22251)。Black Duckナレッジベースの通信の問題が原因の、スキャンエラーの問題が修正されました。通信の問題を回避するために、Black Duckナレッジベース通信とBlack Duckサーバーの間の通信の再試行は、現在、増分間隔で行われます。
- (Hub-22559)。スキャンがポストスキャンフェーズであっても、処理結果がBlack Duckに正常にアップロードされていた問題が修正されました。
- (Hub-23465)。大規模プロジェクトのUPDATE `scan_composite_leaf`クエリが遅い問題が修正されました。

## バージョン2020. 4. 0

### バージョン2020. 4. 0の新機能および変更された機能

#### 著作権情報の管理機能の強化

新しいグローバル著作権編集者の役割を持つユーザーは、組織のオープンソース著作権情報を簡単に管理できるようになり、全著作権所有者のリストを通知ファイルレポートに含めることができます。

著作権エディタの役割を持つユーザーは、次のことができます。

- コンポーネントバージョンのすべての著作権情報を表示する。
- カスタム著作権情報を作成または編集する。
- Black Duckナレッジベース著作権情報を編集する。
- 編集したBlack Duckナレッジベース著作権情報を元のテキストに戻す。
- 著作権情報を有効にしたり無効にしたりする。

Black Duckでは、コンポーネントバージョンの取得元の名前/IDで著作権情報を管理しています。そのため、コンポーネントバージョンの取得元の著作権情報を編集すると、そのコンポーネントバージョンの取得元を使用するすべての構成表に適用されます。データが組織全体に適用されるため、作業負担を軽減することができます。

#### グローバル修正ステータス

Black Duckで新しいグローバルセキュリティマネージャの役割を持つユーザーは、セキュリティ脆弱性に対するグローバルなデフォルト修正ステータスを設定できるようになりました。グローバル修正ステータスを設定すると、新しい構成表にその脆弱性が表示されると、定義してあるグローバル修正ステータスが自動的に設定されます。

グローバルに修正された脆弱性を簡単に見つけることができるように、セキュリティダッシュボードに[デフォルトの修正ステータス]フィルタが追加されました。

#### ポリシーカテゴリ

Black Duckには、ポリシーをグループ化するためのカテゴリが用意されています。[ポリシー管理]ページと[構成表]ページにある新しいカテゴリフィルタを使用すると、簡単にポリシー（[ポリシー管理]ページ）やポリシー違反（[構成表]ページ）を見つけることができます。

使用できるカテゴリには、コンポーネント、セキュリティ、ライセンス、運用、未分類（デフォルト値）があります。

2020. 4. 0リリースより前に作成されたポリシーはすべて、未分類カテゴリにグループ分けされます。

#### レポートデータベースの機能強化

レポートデータベースの次のテーブルに、新しい列が追加されました。

- コンポーネントテーブル
  - review\_status
  - reviewed\_by

- security\_critical\_count
- security\_high\_count
- security\_medium\_count
- security\_low\_count
- security\_ok\_count
- license\_high\_count
- license\_medium\_count
- license\_low\_count
- license\_ok\_count
- operational\_high\_count
- operational\_medium\_count
- operational\_low\_count
- operational\_ok\_count
- コンポーネントポリシーテーブル
  - overridden\_at
  - description
  - severity
- コンポーネント脆弱性テーブル
  - temporal\_score
  - attack\_vector
  - solution\_available
  - workaround\_available
  - published\_on
  - updated\_on
- プロジェクトテーブル
  - created\_at
- プロジェクトバージョンテーブル
  - created\_on
  - updated\_at
  - security\_critical\_component\_count
  - security\_high\_component\_count
  - security\_medium\_component\_count
  - security\_low\_component\_count
  - security\_ok\_component\_count
  - license\_high\_component\_count
  - license\_medium\_component\_count
  - license\_low\_component\_count



- `license_ok_component_count`
- `operational_high_component_count`
- `operational_medium_component_count`
- `operational_low_component_count`
- `operational_ok_component_count`

コンポーネントコメントに対する**bds\_hub**の**reporting**スキーマには、新しいビューも追加されました。

レポートデータベースはマテリアライズドビューを使用します。Excelはマテリアライズドビューをサポートしていないため、レポートデータベースでのExcelの使用はサポートされなくなりましたが、Excelの使用に関するドキュメントは、『レポートデータベースガイド』から削除されました。

## 取得元一括修正

取得元IDが複数ある単一コンポーネントの脆弱性に対して一括修正が簡単に実行できるように、BDSAおよびCVEレコードの[影響を受けるプロジェクト]タブが拡張されて、各プロジェクトバージョンで使用されている取得元が表示されるようになりました。

## 修正ガイダンス

構成表内の脆弱性のあるコンポーネント向けに、Black Duckでは、利用可能な他のコンポーネントバージョンに関するガイダンスと、構成表で使用されているコンポーネントバージョンよりもセキュリティ脆弱性が少ないバージョンがあるかどうかに関するガイダンスが提供されます。この情報を元にして、セキュリティ脆弱性の修正方法を決定することができます。

この機能はベータ版ではなくなり、すべてのお客様が利用できるようになりました。

## LDAPおよびSAML認証を完了したユーザーの作成を無効にする機能

Black Duckに、LDAPまたはSAML認証を完了したユーザーの自動作成を無効にする機能ができました。

## カスタムフィールドの機能強化

Black Duckでは、ドロップダウン、単一、複数の各選択カスタムフィールドに、新しいオプションを追加したり、既存のオプションを編集したりできるようになりました。

## 新しいジョブ

次のジョブがBlack Duckに追加されました。

- **JobMaintenanceJob** : 既存のジョブのデータの保持とクリーンアップを管理します。
- **NotificationPurgeJob** : 既存の通知のデータ保持を管理します。
- **ReportPurgeJob** : 既存のレポートのデータ保持を管理します。
- **SystemMaintenanceJob** : システム関連のアクティビティを維持します。

## APIの機能強化

- カスタムコンポーネントAPIのログまたはプライマリ言語フィールドが追加されました。
- CVSS 3スコアの使用時に重大なリスクを表示する重大リスク優先度が、`/api/components`エンドポイントに追加されました。
- 修正コメントの機能が、`/api/projects/:projectId/versions/:versionId/vulnerable-bom-`



componentsに追加されました。

- ソースIDがナレッジベースから返された取得済みIDと異なる場合に、応答ボディーのコンポーネントおよびバージョンの応答に「移行済み」フラグが追加されました。
- 前回のスキャンの概要に対するパブリックAPIが追加されました : /api/codelocations/:codeLocationId/latest-scan-summary
- 次のエンドポイントに新しいフィールドが追加されました : KB\_COMPONENT、CUSTOM\_COMPONENT、SUB\_PROJECTなど、各エントリーのコンポーネントタイプを表示するための、GET /api/projects/{projectId}/versions/{projectVersionId}/components

## zookeeper コンテナの削除

zookeeper コンテナが削除されました。

- 2020. 04. 0にアップグレードすると、次のボリュームを手動で削除できます。これらのボリュームは使用されず、参照もされません。
  - zookeeper-data-volume
  - zookeeper-data-log-volume

- jobrunner APIは廃止されました。

今後のリリースで削除され置き換えられるため、このAPIを使用して新しいクエリを作成しないでください。

- ジョブの停止にJobs APIのterminateJob機能を使用している場合、呼び出し時にfalseしか返されなくなります。

現在、ジョブをキャンセルすることはできません。この機能は、今後のリリースで別のメカニズムを使用して再度実装される予定です。

## コンテナバージョン

- blackducksoftware/blackduck-postgres : 1.0.13
- blackducksoftware/blackduck-authentication:2020.4.0
- blackducksoftware/blackduck-webapp:2020.4.0
- blackducksoftware/blackduck-scan:2020.4.0
- blackducksoftware/blackduck-jobrunner:2020.4.0
- blackducksoftware/blackduck-cfssl:1.0.1
- blackducksoftware/blackduck-logstash : 1.0.6
- blackducksoftware/blackduck-registration:2020.4.0
- blackducksoftware/blackduck-nginx : 1.0.23
- blackducksoftware/blackduck-documentation:2020.4.0
- blackducksoftware/blackduck-upload-cache : 1.0.13
- sigsynopsys/bdba-worker : 2020.03
- blackducksoftware/rabbitmq : 1.0.3

コンテナsigsynopsys/appcheck-worker-**<version>**の名前が、sigsynopsys/bdba-worker-**<version>**に変更されています。注意してください。

## bdioデータベースの削除

2019. 10. 0のリリースノートに記載されているように、bdioデータベースはBlack Duckから完全に削除されました。

## 外部PostgreSQL用external-postgres-init.pgsql初期化ファイルの変更

external-postgres-init.pgsql初期化ファイルが変更され、Kubernetesなどの他の導入方法との互換性が向上しました。

外部PostgreSQLインスタンスを設定する場合は、docker-swarmディレクトリのexternal-postgres-init.pgsqlファイルを編集して、次の手順を実行する必要があります。

- POSTGRES\_USERをblackduckで置き換える
- HUB\_POSTGRES\_USERをblackduck\_userで置き換える
- BLACKDUCK\_USER\_PASSWORDをblackduck\_userに使用しているパスワードで置き換える

## KubernetesまたはOpenShiftを使用した、Black Duckのsynopsysctlによるインストールまたはアップグレード

2020. 4. 0リリース以降、KubernetesまたはOpenShiftを使用したBlack Duckのインストールまたはアップグレードには、synopsysctlが推奨方法になりました。

この変更により、Synopsysは、クラスタ内のアプリケーション管理のための全機能のサポートに加えて、今後のリリースでは幅広いBlack Duck製品の拡張機能を追加できるようになります。

synopsysctlの詳細については、[こちら](#)をクリックしてください。

## サポートされるブラウザのバージョン

- Safariバージョン13.1 (14609.1.20.111.8)
- Chromeバージョン80.0.3987.162 (公式ビルド) (64ビット)
- Firefoxバージョン74.0 (64ビット)
- Internet Explorer 11.657.18362.0
- Microsoft Edge 44.18362.449.0
- Microsoft EdgeHTML 18.18363

## 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2020. 2. 0が日本語にローカライズされました。

## 2020. 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。

- (Hub-15549)。構成表のポリシールールフィルタが無効ポリシーを表示する問題を修正しました。
- (Hub-19745)。HTTPヘッダーにコンテンツセキュリティプロトコル (CSP) を組み込みました。
- (Hub-21044)。importおよびincludeステートメントへのマッチの誤検出を無視するように、スニペットマッチを修正しました。
- (Hub-21299)。プロジェクトバージョンの[設定]タブに新しい[スキャンファイルのアップロード]

ボタンが追加されました。プロジェクトコードスキャナの役割しかないユーザーも、表示する権限がない情報を表示せずにスキャンをアップロードできるようになりました。

- (Hub-21395)。bz2ファイルのスキャンサイズが正しく計算されない問題を修正しました。
- (Hub-22187)。[マイプロファイル] ページでユーザーに対してアクティブでないグループの役割が表示される問題を修正しました。
- (Hub-22609)。BDBAによるOVAファイルのスキャン時にスキャンが失敗する問題を修正しました。
- (Hub-22657)。署名スキャナCLIが「ERROR StatusLogger...」というエラーメッセージを表示する問題を修正しました。
- (Hub-22675)。crypto\_date\_time.csvファイルが「In Use」列で間違った値をレポートする問題を修正しました。
- (Hub-22692)。スキャンがライセンス制限を超えても通知を受信しない問題を修正しました。
- (Hub-22753)。通知が正しくブルーニングされなかった問題を修正しました。
- (Hub-22852)。ディープライセンスデータ検索で特定ファイルタイプのソースコードが表示されない問題を修正しました。
- (Hub-22937)。関連脆弱性の間違った検索結果が表示される問題を修正しました。
- (Hub-22988)。[ライセンス管理] でライセンスに表示される[使用した場所] の値に、バージョンがないコンポーネントの間違ったコンポーネント数が表示される問題を修正しました。
- (Hub-23097)。プロジェクトバージョンのクローンを作成すると、ポリシー上書き情報に間違ったレビュー担当者が表示される問題を修正しました。
- (Hub-23139)。ユーザーが脆弱性更新レポートをHTML形式で開くことができない問題を修正しました。
- (Hub-23175)。検索結果でコンポーネントバージョンのリンクを選択してもページが読み込まれない問題を修正しました。
- (Hub-23217)。構成表が再構築されるタイミングを示すメッセージが構成表ページに表示されるようになりました。
- (Hub-23237)。プロジェクトバージョンにアクセスすると、「Error: cannot accumulate arrays of different dimensionality」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-23258)。audit\_eventによりクエリがブロックされ、タイムアウトが発生する問題を修正しました。
- (Hub-23296)。ディープライセンスデータが有効になっていると、ライセンスのポリシー違反がトリガーされない問題を修正しました。
- (Hub-23306)。エンドポイントapi/search/componentsのページングが中断される問題を修正しました。
- (Hub-23333)。ツールチップに推移的な依存関係のファイルパスが表示されない問題を修正しました。
- (Hub-23378)。署名スキャナを有効にした状態でSynopsys Detectのインスタンスを複数実行すると、スキャンが失敗して次のエラーが発生する問題を修正しました: 「ERROR: zip END header not found」
- (Hub-23523)。ReportingDatabaseTransferJobが失敗して、キーが重複していることを示すエラーが発生する問題を修正しました。
- (Hub-23602)。ディープライセンスデータを表示するときに、プロジェクトマネージャの役割を持

ユーザーは、[参照ファイル] ダイアログボックス内の取得元IDの情報を表示する権限がない問題を修正しました。

- (Hub-23845)。Internet Explorer 11とBlack Duckに互換性がない問題を修正しました。

## バージョン2020. 2. 1

### バージョン2020. 2. 1の新機能および変更された機能

#### 埋め込みライセンス検索のパフォーマンスが向上しました

Black Duckでは、埋め込みライセンス検出用ソースファイルをアップロードする際のパフォーマンスが向上しました。

### 2020. 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。

- (Hub-22325)。空のフォルダをスキャンすると、Black Duckスニペットスキャンが失敗する問題を修正しました。
- (HUB-22955)。KBComponentUpdateJobが次のエラーで失敗する問題を修正しました：そのIDのオブジェクトは存在しません。
- (Hub-22982)。構成表ページのセキュリティ脆弱性のコンポーネント数が、Black Duckの旧バージョンでの計算方法と一致しない問題を修正しました。

## 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では、コンポーネントについて、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ディープライセンスデータ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。ディープライセンスデータ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ディープライセンスデータ

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、ディープライセンスデータ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。

- ディープライセンスID
- ディープライセンス名
- ディープライセンスファミリ

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。

またはディープライセンスデータは、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。

## 新規プロジェクトバージョンの構成表フィルタ

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。



- **Dashboard**。最後に表示したダッシュボードが表示されます。



- **Find**。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。



- **Scans**。[スキャン] ページを表示します。



- **Reports**。[レポート] ページを表示します。



- **Manage**。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。



- **Admin**。[管理] ページを表示します。



- **Manage** 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ディープライセンス（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。このディープライセンスデータを管理することで、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ディープライセンス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。

ディープライセンスデータはデフォルトでは無効になっています。ディープライセンスデータ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ディープライセンス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ディープライセンスの数によっては、ディープライセンスデータ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。ディープライセンスデータ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ー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表示されます。

## 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`.yaml`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
- blackducksoftware/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、`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。

## 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。

- 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。