



## リリースノート BlueXP classification

NetApp  
April 03, 2024

# 目次

リリースノート .....	1
BlueXP分類の新機能 .....	1
既知の制限 .....	8

# リリースノート

## BlueXP分類の新機能

BlueXP分類の新機能（Cloud Data Sense）をご紹介します。

**2024年4月1日（バージョン1.30）**

### RHEL v8.8およびv9.3 BlueXPの分類のサポートの追加

このリリースでは、以前サポートされていた9.xに加えて、Red Hat Enterprise Linux v8.8およびv9.3がサポートされます。9.xにはDockerエンジンではなくPodmanが必要です。これは、手動でオンプレミスにBlueXPをインストールした場合にも当てはまります。

次のオペレーティングシステムでは、Podmanコンテナエンジンを使用する必要があります。また、BlueXP分類バージョン1.30以降（Red Hat Enterprise Linuxバージョン8.8、9.0、9.1、9.2、9.3）が必要です。

の詳細を確認してください ["BlueXPの分類環境の概要"](#)。

監査ログ収集をアクティブ化するオプションが削除されました

監査ログ収集をアクティブ化するオプションが無効になりました。

### スキャン速度の向上

セカンダリスキャナードでのスキャンパフォーマンスが改善されました。スキャンの処理能力を高める必要がある場合は、スキャナードを追加できます。詳細については、を参照してください ["インターネットにアクセスできるホストにBlueXP分類をインストールします"](#)。

### ジドウアップグレード

インターネットにアクセスできるシステムにBlueXP分類を導入している場合は、システムが自動的にアップグレードされます。以前は、最後のユーザアクティビティから特定の時間が経過したあとにアップグレードが実行されていました。このリリースでは、現地時間が午前1時から午前5時の場合、BlueXPの分類が自動的にアップグレードされます。ローカル時間がこの時間外の場合は、最後のユーザアクティビティから特定の時間が経過したあとにアップグレードが実行されます。詳細については、を参照してください ["インターネットにアクセスできるLinuxホストにインストールします"](#)。

インターネットアクセスを使用せずにBlueXP分類を導入した場合は、手動でアップグレードする必要があります。詳細については、を参照してください ["インターネットアクセスのないLinuxホストにBlueXP分類をインストールする"](#)。

**2024年3月4日（バージョン1.29）**

特定のデータソースディレクトリにあるスキャンデータを除外できるようになりました。

BlueXPの分類で、特定のデータソースディレクトリにあるスキャンデータを除外する場合は、BlueXPの分類で処理する構成ファイルにこれらのディレクトリ名を追加します。この機能を使用すると、不要なディレクトリや、個人データの誤検出結果が返されるディレクトリのスキャンを回避できます。

["詳細はこちら。"](#)。

特大規模インスタンスのサポートが認定されました

BlueXPの分類で2億5、000万を超えるファイルをスキャンする必要がある場合は、クラウド環境またはオンプレミス環境で特大規模なインスタンスを使用できます。このタイプのシステムは、最大5億個のファイルをスキャンできます。

["詳細はこちら。"](#)。

## 2024年1月10日（バージョン1.27）

調査ページの結果に、項目の合計数に加えて合計サイズが表示されるようになりました。

[Investigation]ページでフィルタ処理された結果に、ファイルの合計数に加えてアイテムの合計サイズが表示されるようになりました。これは、ファイルの移動、ファイルの削除などを行うときに役立ちます。

追加のグループIDを[Open to Organization]として設定します。

グループに最初にその権限が設定されていなかった場合に、BlueXPの分類から直接、NFSのグループIDを「Open to Organization」とみなされるように設定できるようになりました。これらのグループIDが添付されているファイルおよびフォルダは、[Investigation Details]ページで[Open to Organization]として表示されます。方法を参照してください ["追加のグループIDを「組織にオープン」として追加"](#)。

## 2023年12月14日（バージョン1.26.6）

このリリースには、いくつかのマイナーな機能拡張が含まれ

また、次のオプションも一時的に削除されました。

- 監査ログ収集をアクティブ化するオプションが無効になりました。を参照してください ["ファイルアクセスイベントを監視および管理します"](#)。
- ディレクトリ調査中に、ディレクトリごとの個人識別情報（PII）データの数进行計算するオプションは使用できません。を参照してください ["組織に保存されているデータを調査します"](#)。
- Azure Information Protection（AIP）ラベルを使用してデータを統合するオプションが無効になりました。を参照してください ["プライベートデータを整理します"](#)。

## 2023年11月6日（バージョン1.26.3）

このリリースで解決された問題は次のとおりです。

- システムによってスキャンされたファイル数をダッシュボードに表示する際の不一致を修正しました。
- 名前とメタデータに特殊文字が含まれるファイルとディレクトリを処理およびレポートすることで、スキャンの動作が改善されました。

## 2023年10月4日（バージョン1.26）

## RHELバージョン9でのBlueXP分類のオンプレミスインストールのサポート

Red Hat Enterprise Linuxバージョン8および9は、BlueXP分類のインストールに必要なDockerエンジンをサポートしていません。コンテナインフラとしてPodmanバージョン4以降を使用したRHEL 9.0、9.1、9.2でのBlueXP分類のインストールがサポートされるようになりました。最新バージョンのRHELを使用する必要がある環境では、Podmanを使用する際にBlueXP分類（バージョン1.26以降）をインストールできるようになりました。

現時点では、RHEL 9.xを使用している場合、ダークサイトのインストールや分散スキャン環境（マスターノードとリモートスキャナノードを使用）はサポートされていません。

## 2023年9月5日（バージョン1.25）

小規模および中規模の導入が一時的に利用できない

現時点では、BlueXP分類のインスタンスをAWSに導入する場合、\*[Deploy]>[Configuration]\*を選択してSmallまたはMedium sizedインスタンスを選択するオプションは使用できません。[Deploy]>[Deploy]\*を選択して、大きなインスタンスサイズを使用してインスタンスを導入することもできます。

**[Investigation Results]**ページから最大**100,000**項目にタグを適用

これまでは、[Investigation Results]ページ（20項目）で一度に1つのページにタグを適用することしかできませんでした。[調査結果（Investigation Results）]ページで\*すべての\*項目を選択し、すべての項目（一度に最大100,000項目）にタグを適用できるようになりました。 ["方法を参照してください"](#)。

最小ファイルサイズが**1MB**の重複ファイルを特定する

BlueXPの分類では、ファイルが50MB以上の場合にのみ重複ファイルが特定されます。1MBで始まる重複ファイルを識別できるようになりました。[Investigation]ページフィルタの[File Size]と[Duplicates]を使用して、環境内で特定のサイズのファイルが重複しているかどうかを確認できます。

## 2023年7月17日（バージョン1.24）

**BlueXP**の分類では、ドイツの**2つ**の新しいタイプの個人データが特定されています。

BlueXPの分類では、次のタイプのデータを含むファイルを特定して分類できます。

- ドイツ語ID（Personalausweisnummer）
- ドイツ社会保障番号（Sozialversicherungsnummer）

["BlueXPの分類によってデータから特定できるすべてのタイプの個人データを確認できます"](#)。

**BlueXP**の分類は制限モードとプライベートモードで完全にサポートされています。

インターネットアクセスがないサイト（プライベートモード）とアウトバウンドのインターネットアクセスが制限されているサイト（制限モード）で、BlueXPの分類が完全にサポートされるようになりました。 ["コネクタのBlueXP導入モードの詳細"](#)。

**BlueXP**分類のプライベートモードインストールをアップグレードするときにバージョンをスキップする機能シーケンシャルでなくても、新しいバージョンのBlueXP分類にアップグレードできるようになりました。つ

まり、BlueXPの分類を1つのバージョンにアップグレードするという現行の制限は不要になりました。この機能は、バージョン1.24以降で該当します。

## BlueXP分類APIを利用できるようになりました

BlueXP分類APIを使用すると、スキャンするデータに関する操作の実行、クエリの作成、情報のエクスポートを行うことができます。Swaggerを使用して対話型ドキュメントを利用できます。ドキュメントは、調査、コンプライアンス、ガバナンス、構成など、複数のカテゴリに分かれています。各カテゴリは、BlueXP分類用UIのタブを表しています。

["BlueXP分類APIの詳細"](#)。

## 2023年6月6日（バージョン1.23）

データ主体名の検索で日本語がサポートされるようになりました

データ主体アクセス要求（DSAR）に回答して、被験者の名前を検索する際に日本語名を入力できるようになりました。を生成できます ["Data Subject Access Request レポート"](#) 結果の情報を使用して。に日本語の名前を入力することもできます ["\[Data Investigation ページの\[Data Subject\]フィルタ\]"](#) サブジェクト名を含むファイルを識別します。

Ubuntuがサポート対象のLinuxディストリビューションになり、BlueXP分類をインストールできるようになりました

Ubuntu 22.04は、BlueXPのサポート対象オペレーティングシステムとして認定されています。BlueXP分類は、ネットワーク内のUbuntu Linuxホストにインストールすることも、バージョン1.23のインストーラを使用している場合はクラウドのLinuxホストにインストールすることもできます。 ["UbuntuがインストールされているホストにBlueXP分類をインストールする方法を参照してください"](#)。

新しいBlueXP分類のインストールでは、Red Hat Enterprise Linux 8.6および8.7はサポートされなくなりました

Red Hatでは前提条件であるDockerがサポートされなくなるため、新規導入ではこれらのバージョンはサポートされません。RHEL 8.6または8.7で既存のBlueXP分類マシンを実行している場合、NetAppでは引き続き構成がサポートされます。

BlueXPの分類は、ONTAPシステムからFPolicyイベントを受信するFPolicyコレクタとして設定できます

作業環境内のボリュームで検出されたファイルアクセスイベントについて、BlueXP分類システムでファイルアクセス監査ログの収集を有効にすることができます。BlueXPの分類では、次のタイプのFPolicyイベントと、ファイルに対してアクションを実行したユーザ（Create、Read、Write、Delete、Rename、所有者/権限を変更し、SACL/DACLを変更します。 ["ファイルアクセスイベントを監視および管理する方法を参照してください"](#)。

ダークサイトでData Sense BYOLライセンスがサポートされるようになりました

ダークサイトのBlueXPデジタルウォレットにData Sense BYOLライセンスをアップロードして、ライセンスの残量が少なくなったときに通知を受け取ることができます。 ["Data Sense BYOLライセンスの入手方法とアップロード方法をご確認ください"](#)。

## 2023年4月3日（バージョン1.22）

### 新しいデータ検出評価レポート

Data Discovery Assessment Reportでは、スキャンされた環境の概要を分析して、システムの調査結果を強調し、懸念領域と潜在的な修復手順を示します。このレポートの目的は、データガバナンスの懸念、データセキュリティの危険性、データセットのデータコンプライアンスギャップに対する認識を高めることです。"[Data Discovery Assessment Reportを生成して使用方法を説明します](#)"。

クラウド内の小規模インスタンスにBlueXPの分類機能を導入できます

AWS環境のBlueXP ConnectorからBlueXPの分類を導入する際に、デフォルトのインスタンスよりも小さい2つのインスタンスタイプから選択できるようになりました。小規模な環境をスキャンする場合は、クラウドコストを節約できます。ただし、小さいインスタンスを使用する場合はいくつかの制限があります。"[使用可能なインスタンスタイプと制限事項を参照してください](#)"。

BlueXPの分類をインストールする前に、スタンドアロンスクリプトを使用してLinuxシステムを認定できるようになりました

BlueXP分類インストールとは別に、Linuxシステムがすべての前提条件を満たしていることを確認する場合は、前提条件のみをテストするスクリプトをダウンロードできます。"[LinuxホストでBlueXPのインストール準備が完了しているかどうかを確認する方法を説明します](#)"。

## 2023年3月7日（バージョン1.21）

### BlueXPの分類UIから独自のカスタムカテゴリを追加する新機能

BlueXPの分類で独自のカスタムカテゴリを追加できるようになりました。これにより、それらのカテゴリに該当するファイルがBlueXPの分類で識別されます。BlueXPには多くの種類があります"[事前定義されたカテゴリ](#)"。そのため、この機能を使用すると、カスタムカテゴリを追加して、組織固有の情報がデータ内のどこにあるかを特定できます。

"[詳細はこちら](#)。"

### BlueXPの分類UIからカスタムキーワードを追加できるようになりました

BlueXPの分類では、今後のスキャンでBlueXPの分類によって特定されるカスタムキーワードを追加できます。ただし、BlueXP分類Linuxホストにログインし、コマンドラインインターフェイスを使用してキーワードを追加する必要がありました。今回のリリースでは、BlueXPの分類UIでカスタムキーワードを追加できるようになり、キーワードの追加や編集が非常に簡単になりました。

"[BlueXPの分類UIからカスタムキーワードを追加する方法については、こちらをご覧ください](#)"。

「最終アクセス時間」が変更されるときに、**BlueXPの分類\***がファイルをスキャンすることはできません

デフォルトでは、BlueXPの分類に適切な「書き込み」権限がないと、BlueXPの分類では「最終アクセス時間」を元のタイムスタンプに戻すことができないため、ボリューム内のファイルはスキャンされません。ただし、最終アクセス時刻がファイルの元の時刻にリセットされていてもかまわない場合は、[設定]ページでこの動作を無効にして、権限に関係なくBlueXPの分類でボリュームがスキャンされるようにすることができます。

この機能と併せて、「Scan Analysis Event」という新しいフィルタが追加され、BlueXPの分類で最終アクセ



ス時刻を元に戻すことができなかったために分類されなかったファイルや、BlueXPの分類で最終アクセス時刻を元に戻すことができなかったにもかかわらず分類されたファイルを表示できるようになりました。

["「最終アクセス時間のタイムスタンプ」とBlueXPの分類に必要な権限について詳しくは、こちらをご覧ください"](#)。

**BlueXPは、3つの新しいタイプの個人データを分類しています**

BlueXPの分類では、次のタイプのデータを含むファイルを特定して分類できます。

- ボツワナIDカード（Omang）番号
- ボツワナパスポート番号
- シンガポール国民登録IDカード（NRIC）

["BlueXPの分類によってデータから特定できるすべてのタイプの個人データを確認できます"](#)。

ディレクトリの機能が更新されました

- データ調査レポートの[Light CSV Report]オプションに、ディレクトリからの情報が含まれるようになりました。
- [Last Accessed]時間フィルタに、ファイルとディレクトリの両方の最終アクセス時刻が表示されるようになりました。

インストールの機能拡張

- インターネットアクセスがないサイト（ダークサイト）用のBlueXP分類インストーラで、インストールを成功させるためにシステムとネットワークの要件が満たされていることを確認するための事前チェックが実行されるようになりました。
- インストール監査ログファイルは保存され、に書き込まれます `/ops/netapp/install_logs`。

## 2023年2月5日（バージョン1.20）

任意のEメールアドレスにポリシーベースの通知Eメールを送信できます

以前のバージョンのBlueXP分類では、特定のクリティカルポリシーが結果を返したときに、アカウントのBlueXPユーザにEメールアラートを送信できました。この機能を使用すると、オンラインでないときにデータを保護するための通知を受け取ることができます。また、ポリシーから、BlueXPアカウントに登録されていない最大20個の電子メールアドレスを持つ他のユーザーに電子メールアラートを送信することもできます。

["ポリシーの結果に基づいて電子メールアラートを送信する方法については、こちらをご覧ください"](#)。

**BlueXPの分類UIから個人用パターンを追加できるようになりました**

BlueXPの分類では、カスタムの「個人データ」を追加できるようになりました。BlueXPの分類で今後のスキャンで特定できるようになります。ただし、BlueXP分類Linuxホストにログインし、コマンドラインを使用してカスタムパターンを追加する必要があります。このリリースでは、BlueXPの分類UIで正規表現を使用して個人用パターンを追加できるようになり、カスタムパターンの追加と編集が非常に簡単になりました。

["BlueXPの分類UIからカスタムパターンを追加する方法については、こちらをご覧ください"](#)。



## BlueXPの分類を使用して1、500万個のファイルを移動できます

これまで、BlueXPの分類では、最大100、000個のソースファイルを任意のNFS共有に移動できました。一度に最大1,500万個のファイルを移動できるようになりました。"[BlueXPによる分類を使用したソースファイルの移動の詳細については、こちらをご覧ください](#)"。

## SharePoint Onlineファイルへのアクセス権を持つユーザーの数を表示する機能

フィルタ「アクセス権を持つユーザー数」で、SharePoint Onlineリポジトリに保存されているファイルがサポートされるようになりました。これまでは、CIFS共有上のファイルのみがサポートされていました。現時点では、Active DirectoryベースでないSharePointグループはこのフィルタにカウントされません。

新しい「部分的成功」ステータスがアクションステータスパネルに追加されました

新しい「Partial Success」ステータスは、BlueXPの分類処理が完了し、一部の項目が失敗し、一部の項目が成功したことを示します（100個のファイルを移動または削除する場合など）。さらに、「終了」ステータスが「成功」に変更されました。以前は、「終了」ステータスに成功した処理と失敗した処理が表示されることがありました。現在、「Success」ステータスは、すべての項目に対するすべてのアクションが成功したことを意味します。"[アクションステータスパネルの表示方法を参照してください](#)"。

## 2023年1月9日（バージョン1.19）

### 機密データが含まれ、過度に許容されるファイルのグラフを表示する機能

Governanceダッシュボードには、機密データ（機密性の高い個人データと機密性の高い個人データの両方を含む）を含むファイルのヒートマップを提供するnew\_sensitive DataおよびWide Permissive\_areaが追加されています。これにより、機密データを含むリスクがある場所を確認できます。"[詳細はこちら](#)"。

### Data Investigationページでは、3つの新しいフィルタを使用できます

[データ調査]ページに表示する結果を絞り込むための新しいフィルタを使用できます。

- 「アクセス権を持つユーザの数」フィルタは、特定の数のユーザに対して開かれているファイルやフォルダを表示します。数値の範囲を選択して結果を絞り込むことができます。たとえば、51~100ユーザがアクセスできるファイルを確認できます。
- 「作成日時」、「検出日時」、「最終変更日時」、「最終アクセス日時」の各フィルタを使用して、事前に定義された日範囲だけを選択するのではなく、カスタムの日付範囲を作成できるようになりました。たとえば、「作成日時」が6か月を超えているファイルや、「最終更新日時」が「過去10日間」の日付になっているファイルを探することができます。
- 「ファイルパス」フィルタで、フィルタリングされたクエリ結果から除外するパスを指定できるようになりました。対象に含めるデータと除外するデータの両方のパスを入力すると、BlueXPの分類によって、対象に含めるパス内のすべてのファイルが最初に検出され、除外するパスからファイルが削除されて結果が表示されます。

"[データの調査に使用できるすべてのフィルタのリストを確認します](#)"。

### BlueXPの分類では、日本の個人番号を識別できます

BlueXPの分類では、日本語の個人番号（「マイナンバー」とも呼ばれます）を含むファイルを特定して分類できます。これには、個人用電話番号と会社用電話番号の両方が含まれます。"[BlueXPの分類によってデータから特定できるすべてのタイプの個人データを確認できます](#)"。

# 既知の制限

既知の制限事項には、このリリースの製品でサポートされていない機能、またはこのリリースと正しく相互運用できない機能が記載されています。これらの制限事項を慎重に確認してください

## BlueXP分類リリースで一時的に削除されたオプション

2023年12月（バージョン1.26.6）リリースでは、次のオプションが一時的に削除されました。

- 監査ログ収集をアクティブ化するオプションが無効になりました。
- ディレクトリ調査中に、ディレクトリごとの個人識別情報（PII）データの数进行計算するオプションは使用できません。
- Azure Information Protection（AIP）ラベルを使用してデータを統合するオプションが無効になりました。

## BlueXPの分類スキヤンの制限事項

BlueXPの分類では、ボリュームの下にある共有は1つだけスキャンされます

1つのボリュームに複数のファイル共有がある場合は、最上位階層の共有がスキャンされます。たとえば、次のような共有があるとします。

- /A
- /A/B
- /C
- /D/E

その後、/A内のデータがスキャンされます。/Cおよび/Dのデータはスキャンされません。

### 回避策

ボリューム内のすべての共有からデータをスキャンしていることを確認する回避策があります。次の手順を実行します。

1. 作業環境で、スキャンするボリュームを追加します。
2. BlueXPの分類によるボリュームのスキャンが完了したら、\_Data Investigation\_pageに移動し、どの共有がスキャンされているかを確認するフィルタを作成します。

「Working Environment Name」および「Directory Type = Share」でデータをフィルタリングして、どの共有がスキャンされているかを確認します。

3. ボリューム内に存在する共有の完全なリストを取得して、スキャンされていない共有を確認します。
4. **"残りの共有を共有グループに追加します"。**

次のように、すべての共有を個別に追加する必要があります。

/C

/D

5. 複数の共有を含む作業環境内のボリュームごとに、次の手順を実行します。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。