BlueXP分類を使用

BlueXP classification

NetApp
April 03, 2024

目次

BlueXP分類を使用 1
組織に保存されているデータに関するガバナンスの詳細を表示する 1
組織に保存されているデータに関するコンプライアンスの詳細を表示する 7
プライベートデータのカテゴリ 14
組織に保存されているデータを調査します 21
プライベートデータを整理します 30
データにポリシーを割り当てます 39
プライベートデータを管理 50
コンプライアンスレポートを表示する 61

BlueXP分類を使用

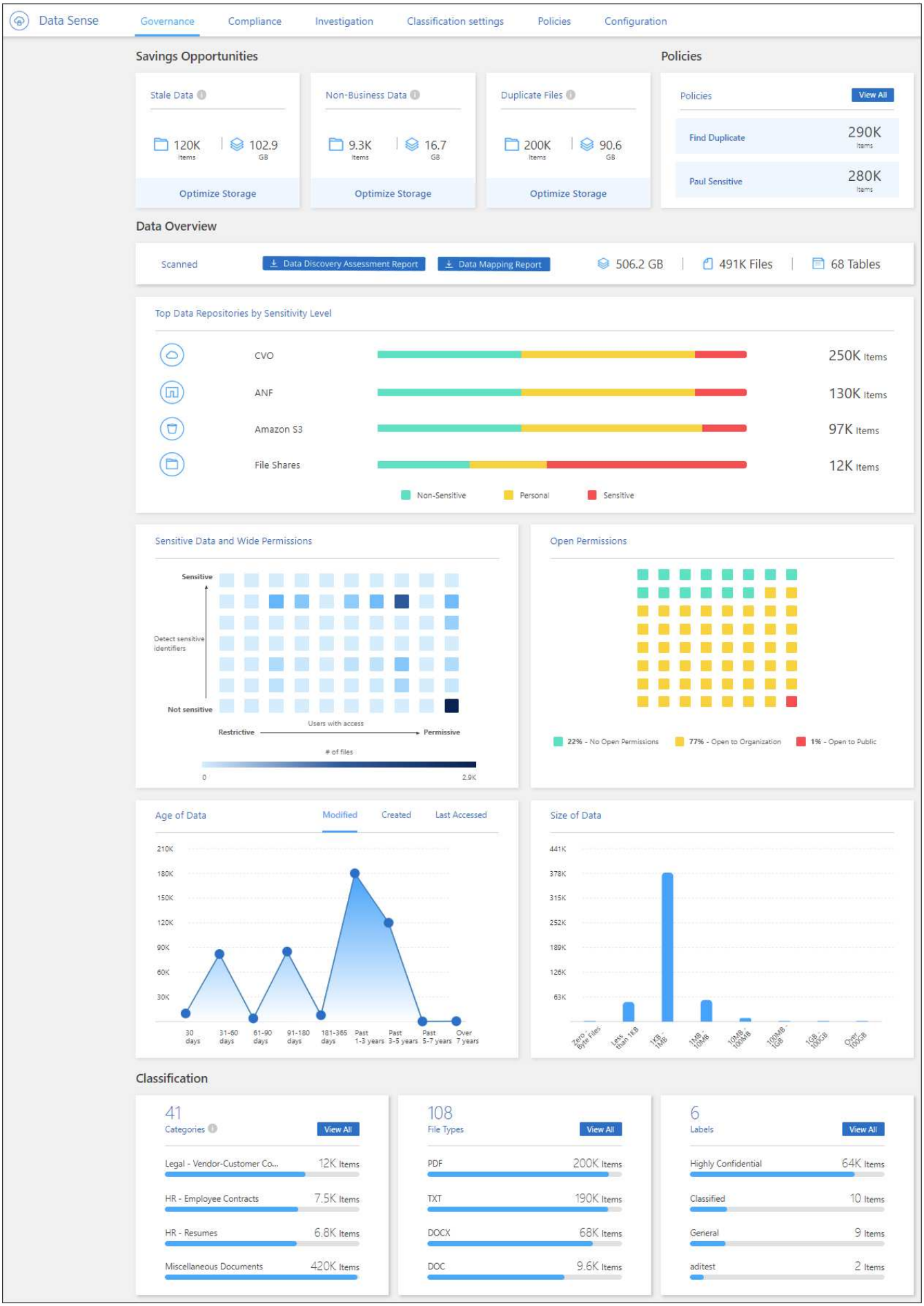
組織に保存されているデータに関するガバナンスの詳細を表示する

組織のストレージリソース上のデータに関連するコストを管理できます。BlueXPは分類されるため、システム内の古いデータ、ビジネス以外のデータ、重複ファイル、大容量ファイルの量が特定されるため、一部のファイルを削除するか、低コストのオブジェクトストレージに階層化するかを判断できます。

さらに、オンプレミスの場所からクラウドにデータを移行する予定の場合は、データのサイズと、データを移動する前に機密情報が含まれているかどうかを確認できます。

Governance ダッシュボード

Governance ダッシュボードには情報が表示されるため、ストレージリソースに保存されているデータの効率性を高め、コストを管理できます。


Data Sense
Governance
Compliance
Investigation
Classification settings
Policies
Configuration
Savings Opportunities
Stale Data
120K Items
102.9 GB
Optimize Storage
Non-Business Data
9.3K Items
16.7 GB
Optimize Storage
Duplicate Files
200K Items
90.6 GB
Optimize Storage
Policies
Policies
View All
Find Duplicate 290K Items
Paul Sensitive 280K Items
Data Overview
Scanned
Data Discovery Assessment Report
Data Mapping Report
506.2 GB
491K Files
68 Tables
Top Data Repositories by Sensitivity Level
CVO 250K Items
ANF 130K Items
Amazon S3 97K Items
File Shares 12K Items
Non-Sensitive
Personal
Sensitive
Sensitive Data and Wide Permissions
Sensitive
Detect sensitive identifiers
Not sensitive
Users with access
Restrictive
Permissive
# of files
0
2.9K
Open Permissions
22% - No Open Permissions
77% - Open to Organization
1% - Open to Public
Age of Data
Modified
Created
Last Accessed
210K
180K
150K
120K
90K
60K
30K
30 days
31-60 days
61-90 days
91-180 days
181-365 days
Past 1-3 years
Past 3-5 years
Past 5-7 years
Over 7 years
Size of Data
441K
378K
315K
252K
189K
126K
63K
Zero Byte Files
Less than 1KB
1KB - 1MB
1MB - 10MB
10MB - 100MB
100MB - 1GB
1GB - 10GB
Over 10GB
Classification
41
Categories
View All
Legal - Vendor-Customer Co... 12K Items
HR - Employee Contracts 7.5K Items
HR - Resumes 6.8K Items
Miscellaneous Documents 420K Items
108
File Types
View All
PDF 200K Items
TXT 190K Items
DOCX 68K Items
DOC 9.6K Items
6
Labels
View All
Highly Confidential 64K Items
Classified 10 Items
General 9 Items
aditest 2 Items

機会の節約

_Saving Opportunities 領域内の項目を調査して、削除または階層化してより安価なオブジェクトストレージにする必要があるデータがないかどうかを確認できます。各項目をクリックすると、 ［ 調査 ］ ページにフィルタリングされた結果が表示されます。

- **Stale Data**- 3 年前に最後に変更されたデータ。
- * ビジネス以外のデータ * - カテゴリまたはファイルタイプに基づいて、ビジネスに関連していないと見なされるデータ。これには、次のもの
  - アプリケーションデータ
  - 音声
  - 実行可能ファイル
  - イメージ
  - ログ
  - ビデオ
  - その他（一般的な「その他」カテゴリ）
- * 重複ファイル * - スキャンしているデータソース内の他の場所に複製されているファイル。 "表示される重複ファイルの種類を確認します"。

  注

  いずれかのデータソースでデータ階層化が実装されている場合は、オブジェクトストレージにすでに存在する古いデータを_Stale Data_categoryで特定できます。

検索結果が最も多いポリシーです

[_Policies]領域では、結果の数が最も多いポリシーがリストの先頭に表示されます。[調査]ページに結果を表示するには、ポリシーの名前をクリックします。[すべて表示 *] をクリックして、使用可能なすべてのポリシーのリストを表示します。

をクリックします "こちらをご覧ください" ポリシーの詳細については、を参照してください。

データの概要

Data Overview_Sectionには、スキャンされるすべてのデータの概要が表示されます。ボタンをクリックして、使用容量、経過時間、データサイズ、すべての作業環境およびデータソースのファイルタイプを含むデータマッピングレポートをダウンロードします。を参照してください データマッピングレポート 詳細については、を参照してください。

データの機密性に基づいて上位のデータリポジトリが表示されます

_Top Data Repositories by Sensitivity Level_領域には、最も機密性の高い項目を含む上位4つのデータリポジトリ（作業環境およびデータソース）が表示されます。各作業環境の棒グラフは、次のように分割されています。

- 機密性のないデータ
- 個人データ

- 機密性の高い個人データ

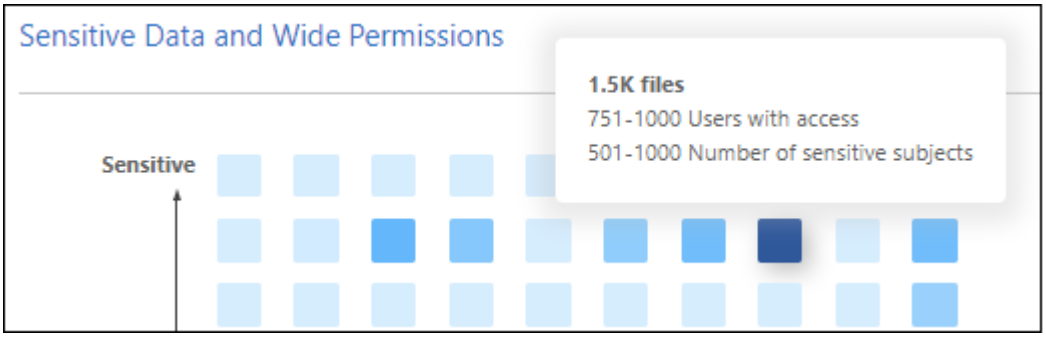
各セクションにカーソルを合わせると、各カテゴリの項目の総数を確認できます。

各領域をクリックすると、 [調査] ページにフィルタリングされた結果が表示され、詳細を調査できます。

機密性と幅広い権限に基づいてリストされたデータ

_Sensitive DataおよびWide Permissions_領域には、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）が含まれ、過度に許容されるファイルのヒートマップが表示されます。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。

ファイルは、X軸（最小から最大）上のファイルへのアクセス権を持つユーザの数、およびY軸（最小から最大）上のファイル内の機密識別子の数に基づいて評価されます。ブロックは、X軸とY軸のアイテムに一致するファイルの数を表します。明るい色のブロックは適切で、ファイルにアクセスできるユーザーが少なく、ファイルごとの機密識別子が少なくなります。濃いブロックは、調査する項目です。たとえば、下の画面には、濃い青色のブロックのマウスオーバーテキストが表示されます。751-100ユーザがアクセスできるファイルが1、500個あり、ファイルごとに501-100の機密識別子があることが示されています。



[調査]ページで、影響を受けるファイルのフィルタリングされた結果を表示するには、対象となるブロックをクリックします。これにより、詳細な調査が可能になります。

アイデンティティサービスをBlueXP分類に統合していない場合、このパネルにデータは表示されません。"Active DirectoryサービスとBlueXPの分類を統合する方法をご紹介します"。

> このパネルでは、CIFS共有、OneDrive、SharePointのデータソースのファイルをサポートしています。現在、データベース、Googleドライブ、Amazon S3、汎用オブジェクトストレージはサポートされていません。

オープンアクセス権のタイプ別に一覧表示されるデータ

Open Permissions 領域には、スキャンされるすべてのファイルに存在する各タイプの権限の割合が表示されます。このチャートには、次の種類の権限が表示されます。

- オープンアクセス権がありません
- 組織に開く（ Open to Organization ）
- [パブリック] に移動します
- 不明なアクセスです

各セクションにカーソルを合わせると、各カテゴリのファイルの総数が表示されます。各領域をクリックする

と、 [調査] ページにフィルタリングされた結果が表示され、詳細を調査できます。

データの経過時間とデータのサイズのグラフ

_Age および _Size_Graphs の項目を調査して、削除または階層化してコストの低いオブジェクトストレージにする必要のあるデータがないかどうかを確認することができます。

グラフの特定のポイントにカーソルを合わせると、そのカテゴリのデータの経過時間やサイズの詳細を確認できます。クリックすると、その年齢またはサイズの範囲でフィルタされたすべてのファイルが表示されます。

- *Age of Data グラフ *- データが作成された時刻、アクセスされた最終時刻、またはデータが変更された最終時刻に基づいてデータを分類します。
- * データサイズグラフ * - サイズに基づいてデータを分類します。

注

いずれかのデータソースでデータ階層化が実装されている場合は、オブジェクトストレージにすでに存在する古いデータをData_graphの_Ageで特定できます。

最も識別されているデータ分類

_Classification_area には ' 最も識別されたリストが表示されます "カテゴリ"、 "ファイルの種類"および "AIP ラベル" をスキャンしたデータに保存します。

カテゴリ

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、「履歴書」や「従業員契約書」などのカテゴリには機密データを含めることができます。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。

を参照してください "カテゴリ別にファイルを表示します" を参照してください。

ファイルの種類

ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。

を参照してください "ファイルタイプを表示しています" を参照してください。

AIP ラベル

Azure Information Protection （ AIP ）に加入している場合は、コンテンツにラベルを適用することで、ドキュメントとファイルを分類して保護できます。ファイルに割り当てられている最も使用されている AIP ラベルを確認すると、ファイルで最も使用されているラベルを確認できます。

を参照してください "AIP ラベル" を参照してください。

データマッピングレポート

データマッピングレポートには、企業データソースに保存されているデータの概要が表示され、移行、バックアップ、セキュリティ、コンプライアンスの各プロセスの決定に役立ちます。このレポートには、まずすべての作業環境とデータソースの概要が表示され、次に各作業環境の内訳が表示されます。

このレポートには次の情報が含まれます。

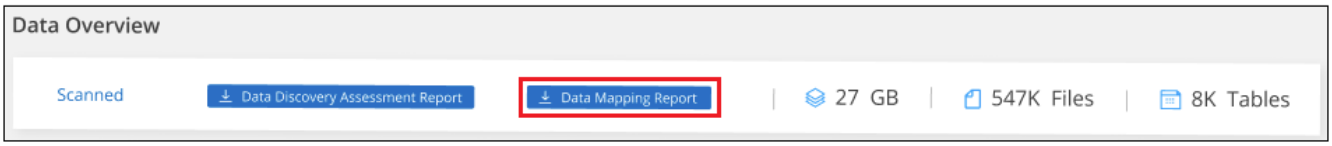
カテゴリ	説明
使用容量	すべての作業環境：各作業環境のファイル数と使用済み容量が表示されます。単一の作業環境の場合：容量が最も多いファイルが表示されます。
データの経過時間	ファイルが作成されたとき、最終変更されたとき、または最後にアクセスされたときのグラフとグラフが 3 つ表示されます。特定の日付範囲に基づいて、ファイル数とその使用済み容量が表示されます。
データのサイズ	作業環境の特定のサイズ範囲内に存在するファイルの数を示します。
ファイルの種類	作業環境に保存されているファイルタイプごとのファイルの総数と使用容量が表示されます。

データマッピングレポートの生成

このレポートは、BlueXPの[ガバナンス]タブで生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. をクリックし、[データマッピングレポート]*ボタンをクリックします。



結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

レポートのサイズが1MBを超える場合は、BlueXP分類インスタンスにPDFファイルが保持され、正確な場所に関するポップアップメッセージが表示されます。BlueXP分類がオンプレミスのLinuxマシンまたはクラウドに導入したLinuxマシンにインストールされている場合は、PDFファイルに直接移動できます。BlueXP分類をクラウドに導入したら、BlueXP分類インスタンスにSSHでアクセスしてPDFファイルをダウンロードする必要があります。 "「分類インスタンスのデータにアクセスする方法」を参照してください"。

BlueXPの分類ページの上部にあるをクリックすると、レポートの最初のページに表示される会社名をカスタマイズできます ボタン"] [会社名の変更]をクリックします。次回レポートを生成するときに、新しい名前が含まれます。

Data Discovery Assessment Reportの略

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。結果は、データのマッピングと分類の両方に基づいています。このレポートの目的は、データセットの次の3つの重要な側面についての認知度を高めることです。

フィーチャー（ **Feature** ）	説明
データガバナンスの懸念	所有しているすべてのデータと、コストを節約するためにデータ量を削減できる可能性のある領域の詳細な画像。
データセキュリティのリスク	広範なアクセス権限により、内部または外部の攻撃からデータにアクセスできる領域。
データコンプライアンスのギャップ	お客様の個人情報または機密性の高い個人情報が、セキュリティとDSAR（データ主体アクセス要求）の両方の目的で保管されている場所。

評価後、このレポートでは次のことが可能な領域を特定します。

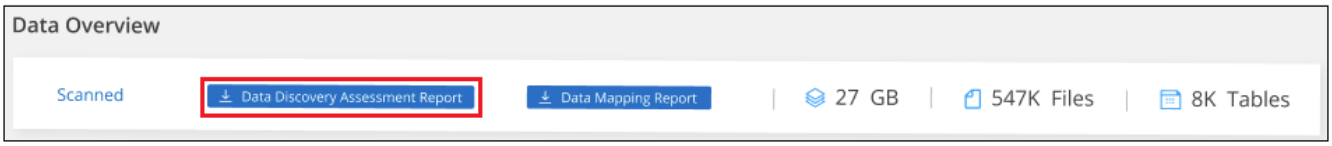
- 保持ポリシーを変更したり、特定のデータ（古いデータ、重複データ、ビジネス以外のデータ）を移動または削除したりすることで、ストレージコストを削減
- グローバルグループ管理ポリシーを改訂して、幅広い権限を持つデータを保護します
- PIIをより安全なデータストアに移動することで、個人情報または機密性の高い個人情報を含むデータを保護します

データ検出評価レポートの生成

このレポートは、BlueXPの[ガバナンス]タブで生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. Governance（ガバナンス）をクリックし、 Data Discovery Assessment Report（データ検出評価レポート）*ボタンをクリックします。



結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

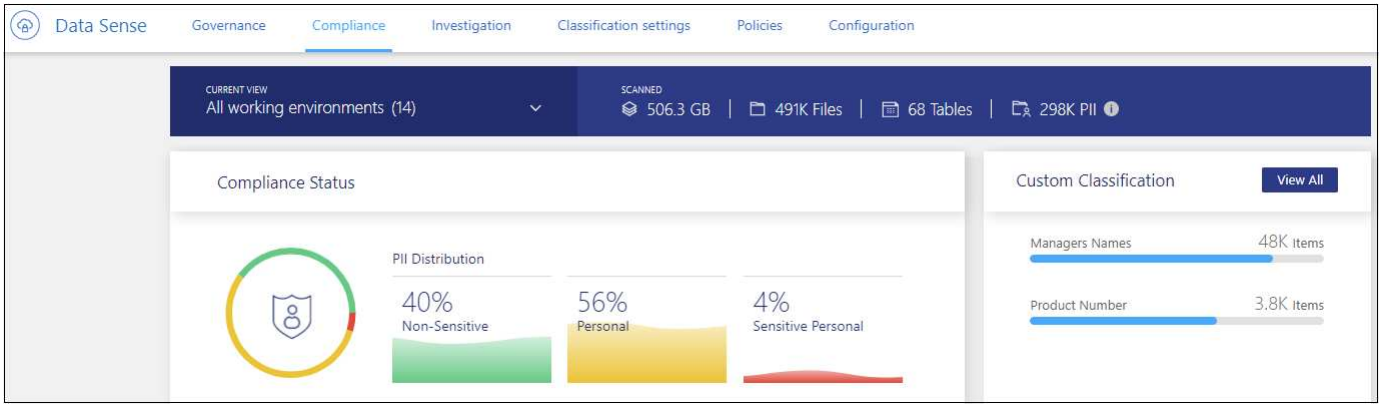
BlueXPの分類ページの上部にあるをクリックすると、レポートの最初のページに表示される会社名をカスタマイズできます ボタン"] [会社名の変更]をクリックします。次回レポートを生成するときに、新しい名前が含まれます。

組織に保存されているデータに関するコンプライアンスの詳細を表示する

組織内の個人データと機密性の高い個人データに関する詳細を表示することで、個人データを管理できます。BlueXPで分類されたデータのカテゴリやファイルタイプを確認することで、データを可視化することもできます。

このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

デフォルトでは、BlueXPの分類ダッシュボードには、すべての作業環境とデータベースのコンプライアンスデータが表示されます。



一部の作業環境のデータだけを表示する場合は、 それらの作業環境を選択します。

また、 [データ調査] ページから結果をフィルタリングして、結果のレポートを CSV ファイルとしてダウンロードすることもできます。を参照してください "[データ調査 ページでデータをフィルタリングします"] を参照してください。

個人データを含むファイルを表示する

BlueXPの分類では、データ内の特定の単語、文字列、パターン（正規表現）が自動的に識別されます。たとえば、個人識別情報（ PII ）、クレジットカード番号、社会保障番号、銀行口座番号、パスワード、 その他。"すべてのリストを参照してください"。BlueXPの分類では、個 々 のファイル、ディレクトリ（共有とフォルダ）内のファイル、およびデータベーステーブルでこのような情報が識別されます。

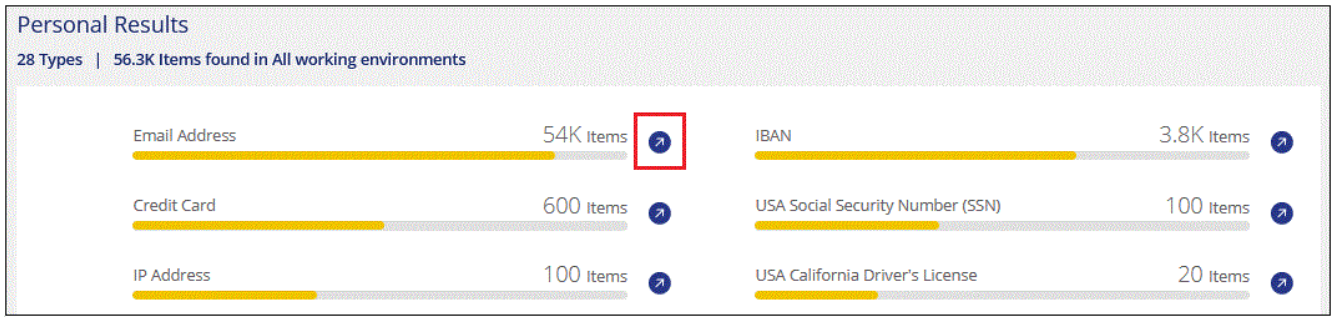
また、スキャン対象のデータベースサーバを追加した場合、 Data Fusion の機能を使用してファイルをスキャンし、データベースから一意の識別子がこれらのファイルまたは他のデータベースのいずれに存在するかを特定できます。を参照してください "Data Fusion を使用して個人データ識別子を追加する" を参照してください。

BlueXPの分類では、一部のタイプの個人データについて、*proximity validation_*を使用して検出結果が検証されます。検証は、見つかった個人データに近接した *1* つまたは複数の定義済みキーワードを検索することによって行われます。たとえば、*BlueXP*は米国を表しますソーシャルセキュリティ番号（ *SSN* ）は、 *IT* の横に近接語（ *_SSN_or_social security* など）が表示されている場合、 SSN として表示されます。 "個人データのテーブル" は、BlueXPの分類で近接検証を使用する状況を示しています。

手順

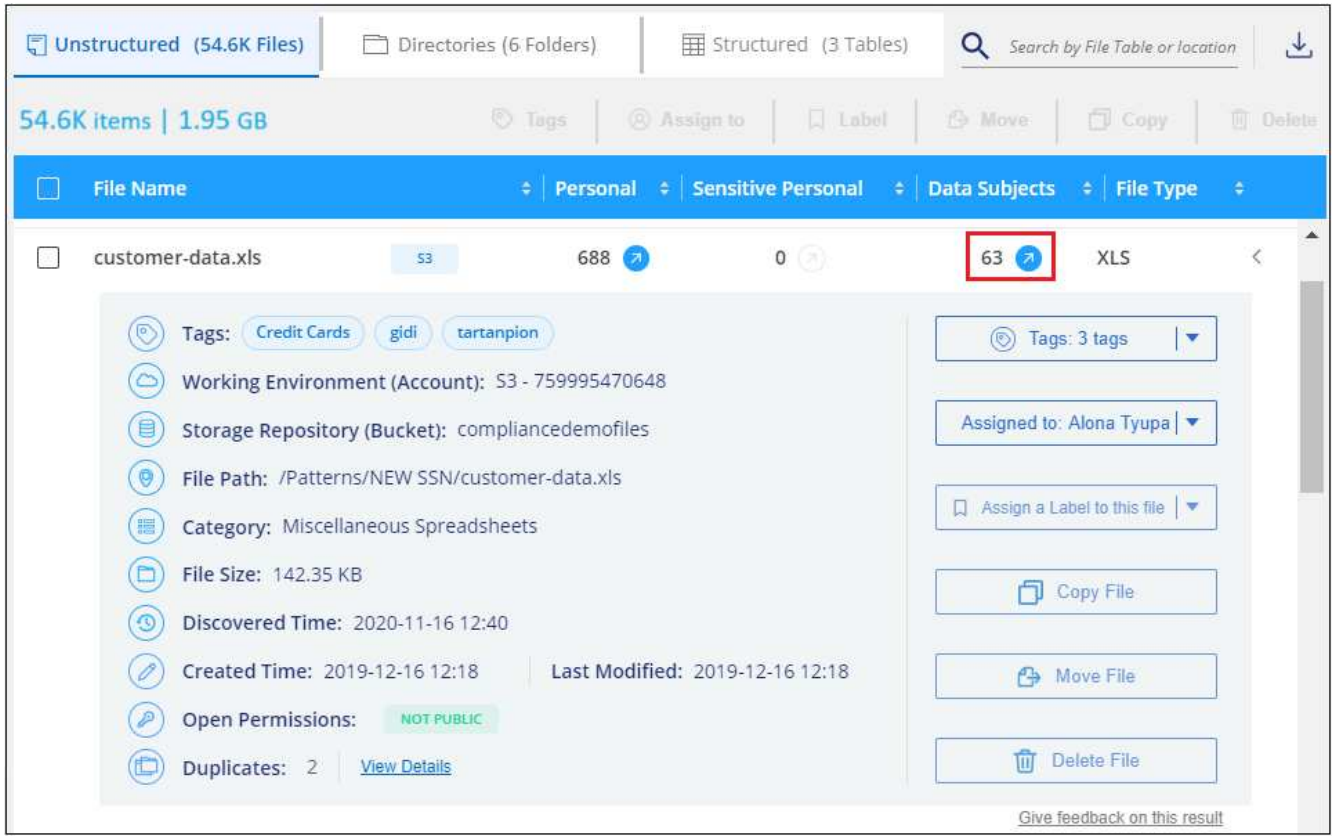
1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. すべての個人データの詳細を調査するには、個人データの割合の横にあるアイコンをクリックします。

3. 特定の種類の個人データの詳細を調査するには、 [* すべて表示 *] をクリックしてから、特定の種類の個人データの [調査結果 *] アイコン（電子メールアドレスなど）をクリックします。

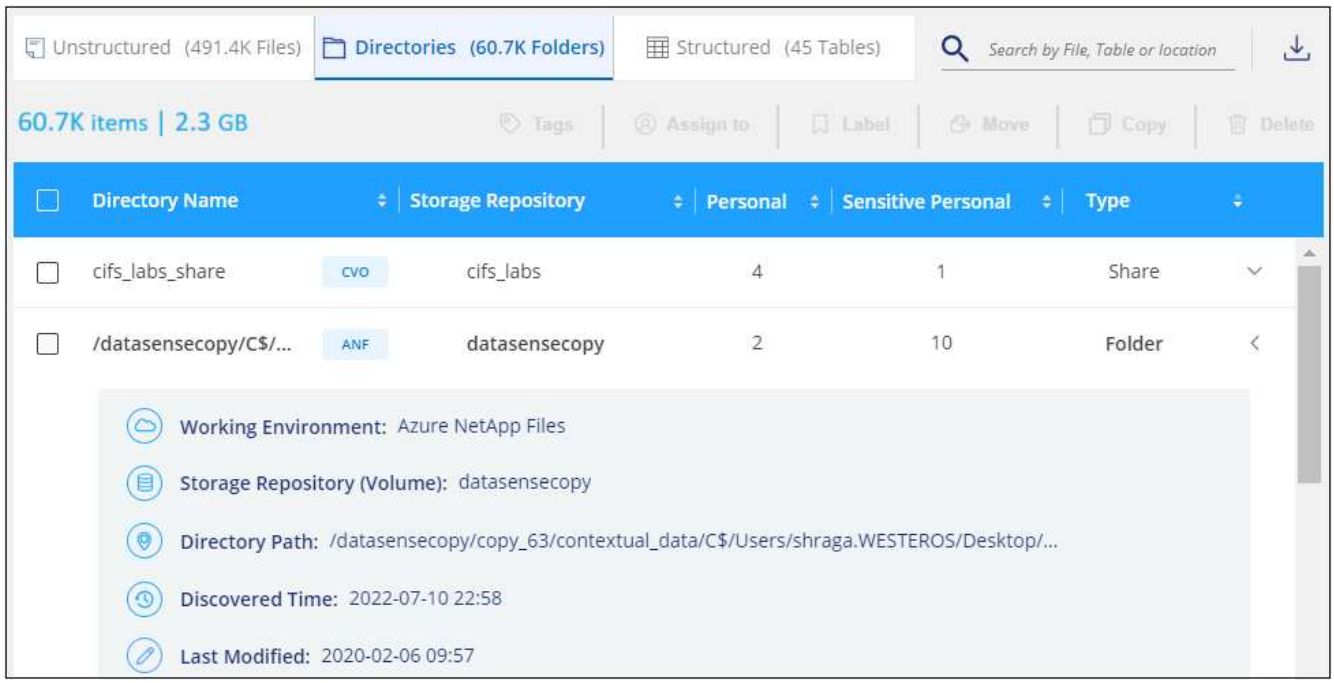


4. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

   以下の2つのスクリーンショットは、個々のファイルに保存されている個人データを示しています。これらのデータは、ディレクトリ（共有およびフォルダ）内のファイルに保存されています。[構造化*]タブを選択して、データベース内で検出された個人データを表示することもできます。



をクリックした後にファイルで見つかった詳細情報のスクリーンショット。"]



をクリックした後にディレクトリで見つかった詳細情報のスクリーンショット。"]

機密性の高い個人データを含むファイルを表示する

BlueXPは、などのプライバシー規制で定義されている特別な種類の機密個人情報を自動的に識別します "GDPR の第 9 、 10 記事"。たとえば、人の健康、民族の起源、性的指向に関する情報などです。 "すべてのリストを参照してください"。BlueXPの分類では、個 々 のファイル、ディレクトリ（共有とフォルダ）内の

ファイル、およびデータベーステーブルでこのような情報が識別されます。

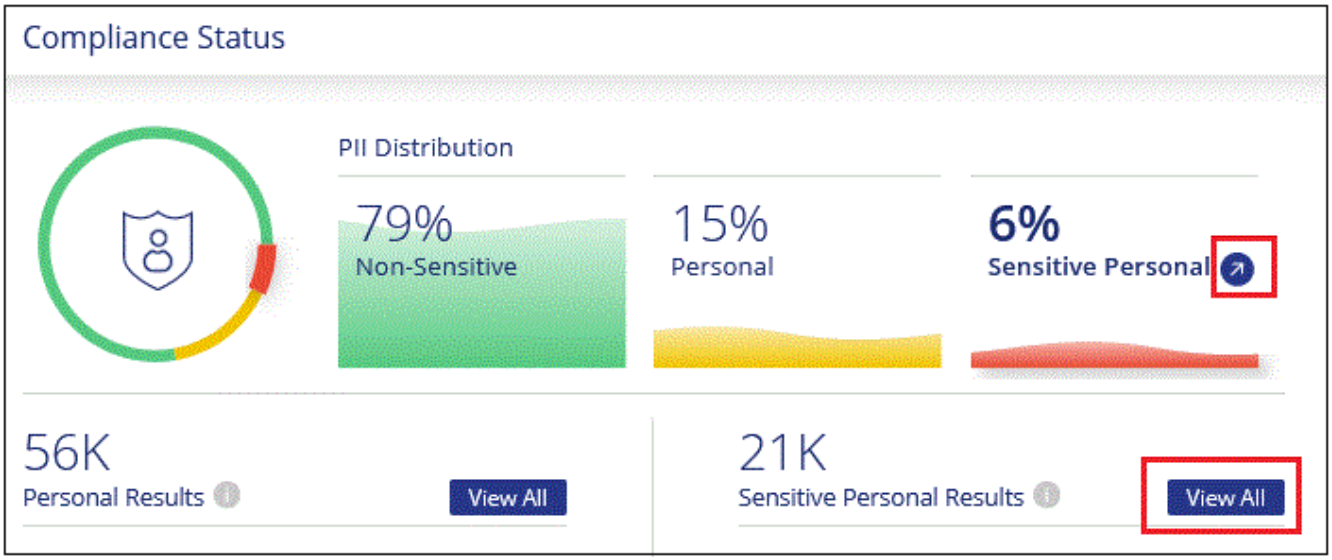
BlueXPは、人工知能（AI）、自然言語処理（NLP）、機械学習（ML）、コグニティブコンピューティング（CC）を使用してスキャンするコンテンツの意味を理解し、エンティティを抽出して適切に分類します。

たとえば、機密性の高い GDPR データカテゴリの 1 つは民族起源です。自然言語処理能力を備えたBlueXPの分類では、「George is Mexican」（GDPR第9条に規定されている機密データを示しています）と「George is Eating Mexican food」（ジョージはメキシコ料理を食べています）の違いを区別できます。

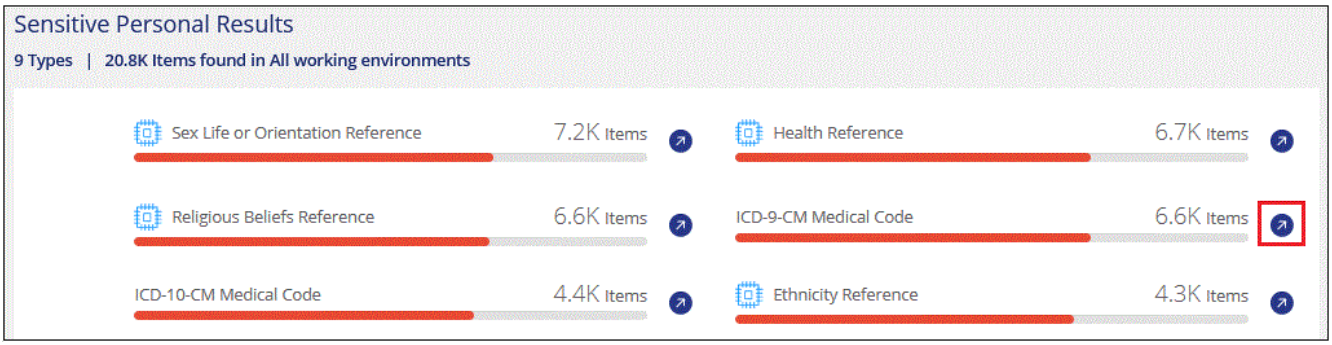
> 機密性の高い個人データをスキャンする場合は、英語のみがサポートされます。言語のサポートは、あとで追加されます。

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. 機密性の高い個人データの詳細を調べるには、個人データの割合の横にあるアイコンをクリックします。



3. 特定のタイプの機密個人データの詳細を調べるには、 [* すべて表示 *] をクリックし、特定のタイプの機密個人データの [調査結果 *] アイコンをクリックします。



4. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

カテゴリ別にファイルを表示

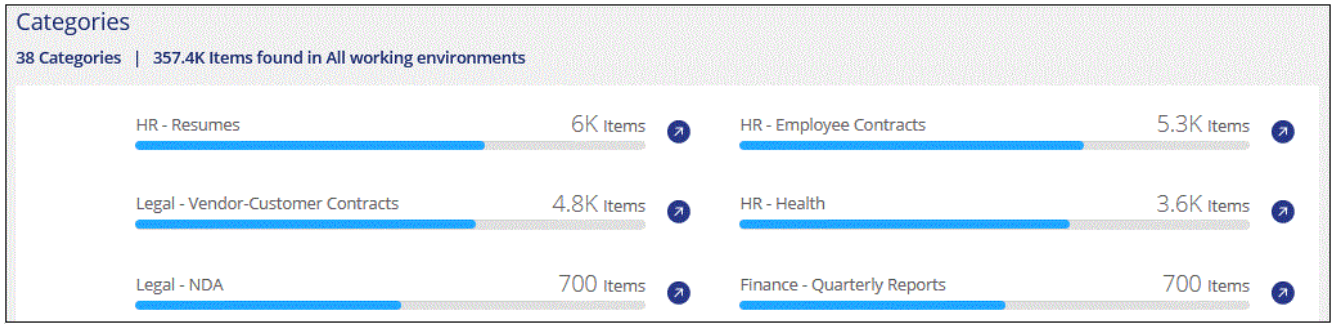
BlueXPは、スキャンしたデータをさまざまなカテゴリに分類します。カテゴリは、各ファイルのコンテンツとメタデータの AI 分析に基づくトピックです。 "カテゴリのリストを参照してください"。

カテゴリを使用すると、保有している情報の種類を表示して、データの状況を把握することができます。たとえば、履歴書や従業員契約などのカテゴリには機密データを含めることができます。結果を調査すると、従業員契約が安全でない場所に保存されていることがわかります。その後、その問題を修正できます。

> 英語、ドイツ語、およびスペイン語は、カテゴリでサポートされています。言語のサポートは、あとで追加されます。

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. メイン画面から上位 4 つのカテゴリのいずれかの * 調査結果 * アイコンを直接クリックするか、 * すべて表示 * をクリックして、いずれかのカテゴリのアイコンをクリックします。



3. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

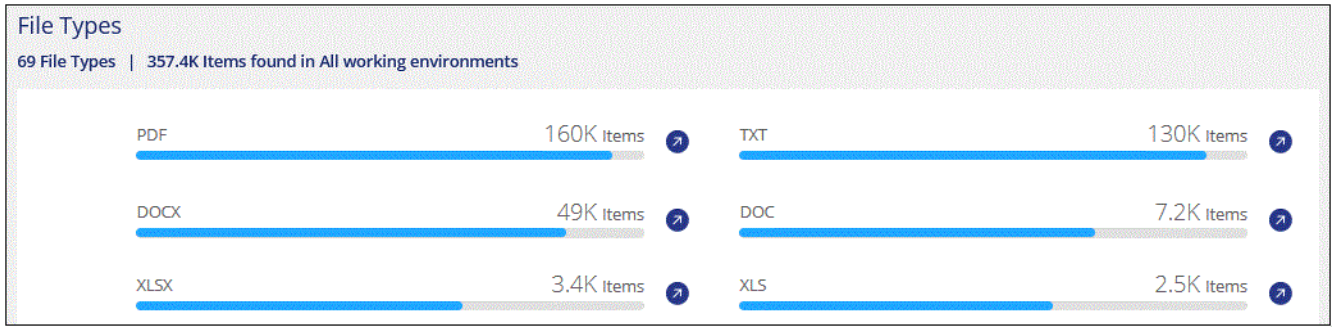
ファイルタイプ別のファイルの表示

BlueXPは、スキャンしたデータをファイルタイプ別に分類して分類します。ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。 "ファイルタイプのリストを参照してください"。

たとえば ' 組織に関する非常に機密性の高い情報を含む CAD ファイルを保存する場合がありますセキュリティで保護されていない場合は、権限を制限するか、ファイルを別の場所に移動することで、機密データを制御できます。

手順

1. BlueXPの左ナビゲーションメニューで、* Governance > Classification をクリックし、 Compliance *タブをクリックします。
2. メイン画面で上位 4 つのファイルタイプのうちの 1 つに対応する * 調査結果 * アイコンをクリックするか、 * すべて表示 * をクリックして、任意のファイルタイプのアイコンをクリックします。



3. 特定のファイルの検索、ソート、詳細の展開、 * 調査結果 * をクリックしてマスクされた情報を表示、またはファイルリストをダウンロードして、データを調査します。

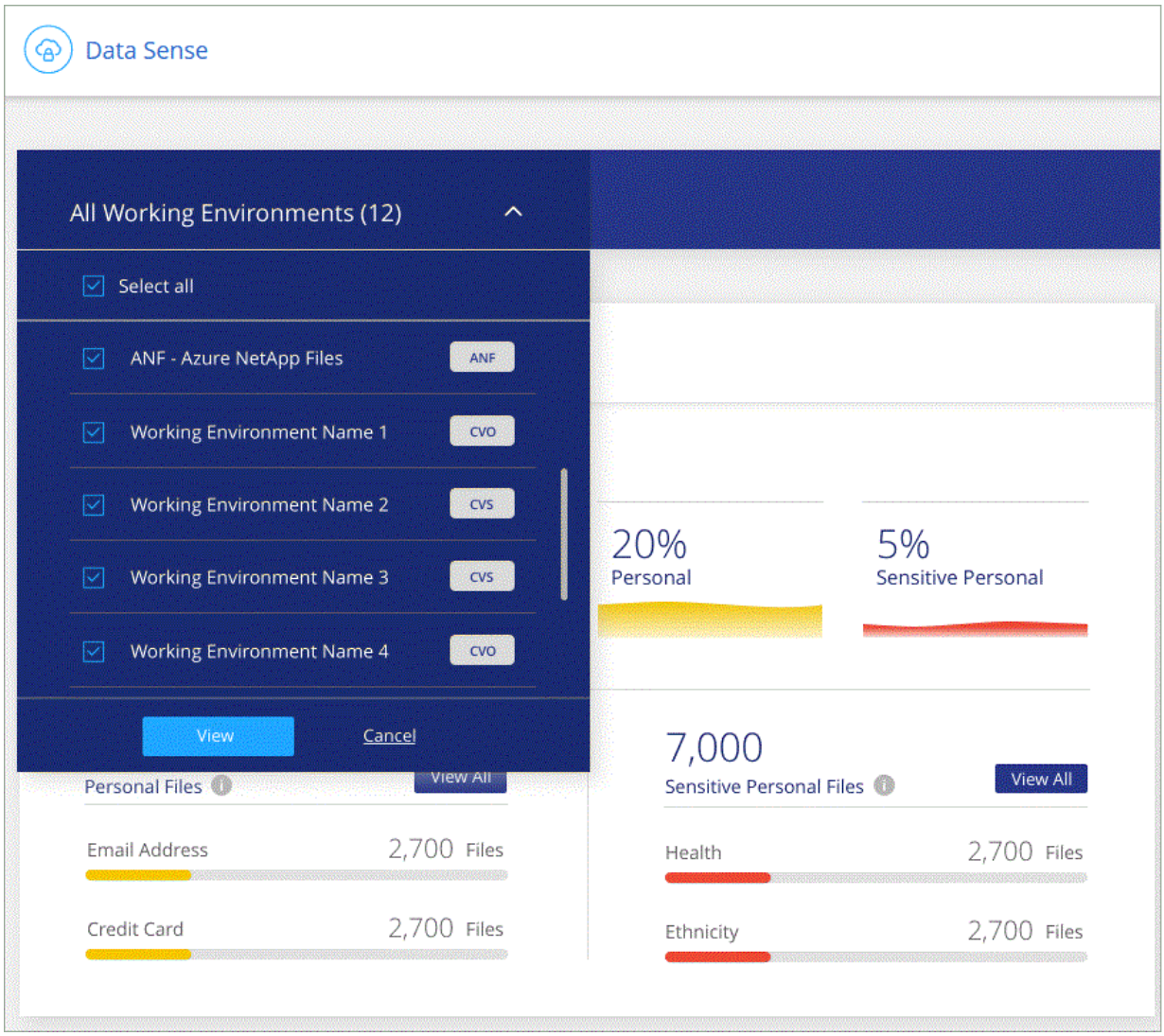
特定の作業環境のダッシュボードデータを表示する

BlueXPの分類ダッシュボードの内容をフィルタリングして、すべての作業環境とデータベース、または特定の作業環境のコンプライアンスデータを表示できます。

ダッシュボードをフィルタすると、BlueXPの分類によって、選択した作業環境のみに準拠データとレポートの範囲が限定されます。

手順

1. フィルタドロップダウンをクリックし、データを表示する作業環境を選択して、 * 表示 * をクリックします。



プライベートデータのカテゴリ

BlueXPの分類によってボリューム、Amazon S3バケット、データベース、OneDriveフォルダ、SharePointアカウントなど、さまざまな種類のプライベートデータを特定できます。 およびGoogleドライブアカウント。以下のカテゴリを参照してください。

> 国別ID番号や医療用IDなど、他のプライベートデータタイプを識別するためにBlueXPの分類が必要な場合は、ng-contact-data-sense@netapp.comまでリクエストをEメールで送信してください。

個人データの種類

ファイルに含まれる個人データは、一般的な個人データまたは国 ID です。次の表の3列目は、BlueXPの分類でが使用されているかどうかを示しています "近接性検証" 識別子の調査結果を検証します。

これらの項目を認識できる言語が表に示されています。

ファイル内にある個人データのリストに追加できます。データベースサーバをスキャンする場合、_Data

Fusion _機能を使用すると、データベーステーブルの列を選択して、BlueXP分類のスキャンで検索する追加の識別子を選択できます。また、カスタムキーワードをテキストファイルから追加したり、正規表現を使用してカスタムパターンを追加したりすることもできます。を参照してください "BlueXPの分類スキャンに個人データ識別子を追加します" を参照してください。

を入力します	識別子	近接性検証：	英語	ドイツ語	スペイン語	フランス語	日本語
全般	クレジットカード番号	いいえ	✓	✓	✓		✓
	データ主体	いいえ	✓	✓	✓		
	E メールアドレス	いいえ	✓	✓	✓		✓
	IBAN番号（国際銀行口座番号）	いいえ	✓	✓	✓		✓
	IP アドレス	いいえ	✓	✓	✓		✓
	パスワード	はい。	✓	✓	✓		✓

を入力します	識別子	近接性検証：	英語	ドイツ語	スペイン語	フランス語	日本語
国家識別番号							
16							

を入力します	識別子	近接性検証	英語	ドイツ語	スペイン語	フランス語	日本語
	ギリシャ ID	はい。	✓	✓	✓		
	ハンガリー語税識別番号	はい。	✓	✓	✓		
	アイルランド ID （ PPS ）	はい。	✓		✓		
	イスラエルの身分証明書	はい。	✓	✓	✓		
	イタリアの税識別番号	はい。	✓	✓	✓		
	日本の個人識別番号（個人および会社）	はい。	✓	✓	✓		✓
	ラトビア ID	はい。	✓	✓	✓		
	リトアニア ID	はい。	✓	✓	✓		
	ルクセンブルク iD	はい。	✓	✓	✓		
	マルタ ID	はい。	✓	✓	✓		
	National Health Service （ NHS ）番号	はい。	✓	✓	✓		
	ニュージーランド銀行口座	はい。	✓	✓	✓		
	ニュージーランド・ドライバー・ライセンス	はい。	✓	✓	✓		
	ニュージーランドIRD番号（税ID）	はい。	✓	✓	✓		
	ニュージーランドNHI（National Health Index）番号	はい。	✓	✓	✓		
	ニュージーランドパスポート番号	はい。	✓	✓	✓		
	ポーランド ID （ PESEL ）	はい。	✓	✓	✓		
	ポルトガル語税識別番号（ NIF ）	はい。	✓	✓	✓		
	ルーマニア語 ID （ CNP ）	はい。	✓	✓	✓		
	シンガポール国民登録IDカード（NRIC）	はい。	✓	✓	✓		
	スロベニア語 ID （ EMSO ）	はい。	✓	✓	✓		
	南アフリカ ID	はい。	✓	✓	✓		
	スペイン語税識別番号	はい。	✓	✓	✓		
	スウェーデン語 ID	はい。	✓	✓	✓		
	Texas Driver’s License	はい。	✓	✓	✓		
	英国ID （ニーノ）	はい。	✓	✓	✓		
	米国カリフォルニア州運転免許証	はい。	✓	✓	✓		
	USAインディアナ運転免許証	はい。	✓	✓	✓		
	米国ニューヨーク運転免許証	はい。	✓	✓	✓		
	米国社会保障番号（ SSN ）	はい。	✓	✓	✓		

機密性の高い個人データのタイプ

BlueXPの分類でファイルに含まれる機密性の高い個人データには、次のリストが含まれます。

このカテゴリの項目は、現時点では英語でのみ認識されます。

刑事手続きの参照
　天然人の犯罪に関するデータ。

『民族リファレンス』を参照してください
　自然な人の人種または民族の起源に関するデータ。

健全性リファレンス
　自然な人の健康に関するデータ。

ICD-9-CM Medical Codes
　医療および医療業界で使用されるコード。

ICD-10-CM Medical Codes
　医療および医療業界で使用されるコード。

哲学の信仰の参照
　自然な人の哲学的信条に関するデータ。

政治的見解参照
　自然界の政治的意見に関するデータ。

宗教的信条参照
　自然な人の宗教的信条に関するデータ。

性別生命または方向の参照
　自然な人の性生活や性的指向に関するデータ。

カテゴリのタイプ

BlueXPの分類では、データは次のように分類されます。

これらのカテゴリのほとんどは、英語、ドイツ語、スペイン語で認識されます。

カテゴリ	を入力します	英語	ドイツ語	スペイン語
財務	貸借対照表	✓	✓	✓
	注文書	✓	✓	✓
	請求書	✓	✓	✓
	四半期ごとのレポート	✓	✓	✓

カテゴリ	を入力します	英語	ドイツ語	スペイン語
時間	バックグラウンドチェック	✓		✓
	報酬プラン	✓	✓	✓
	従業員の契約	✓		✓
	従業員レビュー	✓		✓
	健常性	✓		✓
	再開します	✓	✓	✓
法律	NDAS	✓	✓	✓
	ベンダー - お客様との契約	✓	✓	✓
マーケティング	キャンペーン	✓	✓	✓
	会議	✓	✓	✓
処理	監査レポート	✓	✓	✓
営業	SO 番号	✓	✓	
サービス	RFI （ RFI ）	✓		✓
	RFP	✓		✓
	SOW の作成	✓	✓	✓
	トレーニング	✓	✓	✓
サポート	苦情やチケット	✓	✓	✓

次のメタデータも分類され、同じサポート対象言語で識別されます。

- アプリケーションデータ
- アーカイブファイル
- 音声
- ビジネスアプリケーションデータ
- CAD ファイル
- コード
- 壊れています
- データベースおよびインデックス・ファイル
- BlueXPの分類：パンくずリスト
- デザインファイル（ Design Files ）
- E メールアプリケーションデータ
- 暗号化（エントロピースコアが高いファイル）
- 実行可能ファイル
- 財務アプリケーションデータ

- ヘルスアプリケーションデータ
- イメージ
- ログ
- その他の文書
- その他のプレゼンテーション
- その他のスプレッドシート
- その他 " 不明 "
- パスワードで保護されたファイル
- 構造化データ
- ビデオ
- 0 バイトのファイル

ファイルのタイプ

BlueXPの分類は、すべてのファイルをスキャンしてカテゴリやメタデータの分析情報を取得し、ダッシュボードの[File Types]セクションにすべてのファイルタイプを表示します。

ただし、BlueXPの分類でPersonal Identifiable Information（PII）が検出された場合や、DSAR検索が実行された場合は、次のファイル形式のみがサポートされます。

「+.csv」、「.dcm」、「.dom」、「.DOC」、「.DOCX」、 .json、.pdf、.PPTX、.rtf、.TXT、 .XLS、.xlsx、Docs、Sheets、Slides +`

見つかった情報の正確性

ネットアップは、BlueXPの分類によって特定される個人データや機密性の高い個人データの正確性を100%保証することはできません。必ずデータを確認して情報を検証してください。

ネットアップのテストに基づいて、BlueXPで分類された情報の正確さを次の表に示します。精度 _ と _ リコール _ で分解します。

精度（ **Precision** ）

BlueXPの分類で検出された内容が正しく特定された可能性。たとえば、個人データの正確な割合が 90% の場合、個人情報を含むと識別された 10 個中 9 個のファイルに個人情報が実際に含まれていることを意味します。10 個のファイルのうち 1 個はフォールスポジティブです。

取り消し

BlueXPで分類して何が必要かを判断できる確率。たとえば、個人データのリコール率が70%の場合、BlueXPの分類では、組織内の個人情報が実際に含まれているファイルの10個中7個を特定できます。BlueXPの分類ではデータの30%が失われ、ダッシュボードには表示されません。

私たちは、常に結果の正確さを改善しています。これらの改善点は、今後のBlueXP分類リリースで自動的に提供される予定です。

を入力します	精度（ **Precision** ）	取り消し
個人データ - 一般	90% ~ 95%	60% ～ 80%
個人データ - 国 ID	30% ~ 60%	40% ~ 60%
機密性の高い個人データ	80% ~ 95%	20% ~ 30%
カテゴリ	90% ~ 97%	60% ～ 80%

組織に保存されているデータを調査します

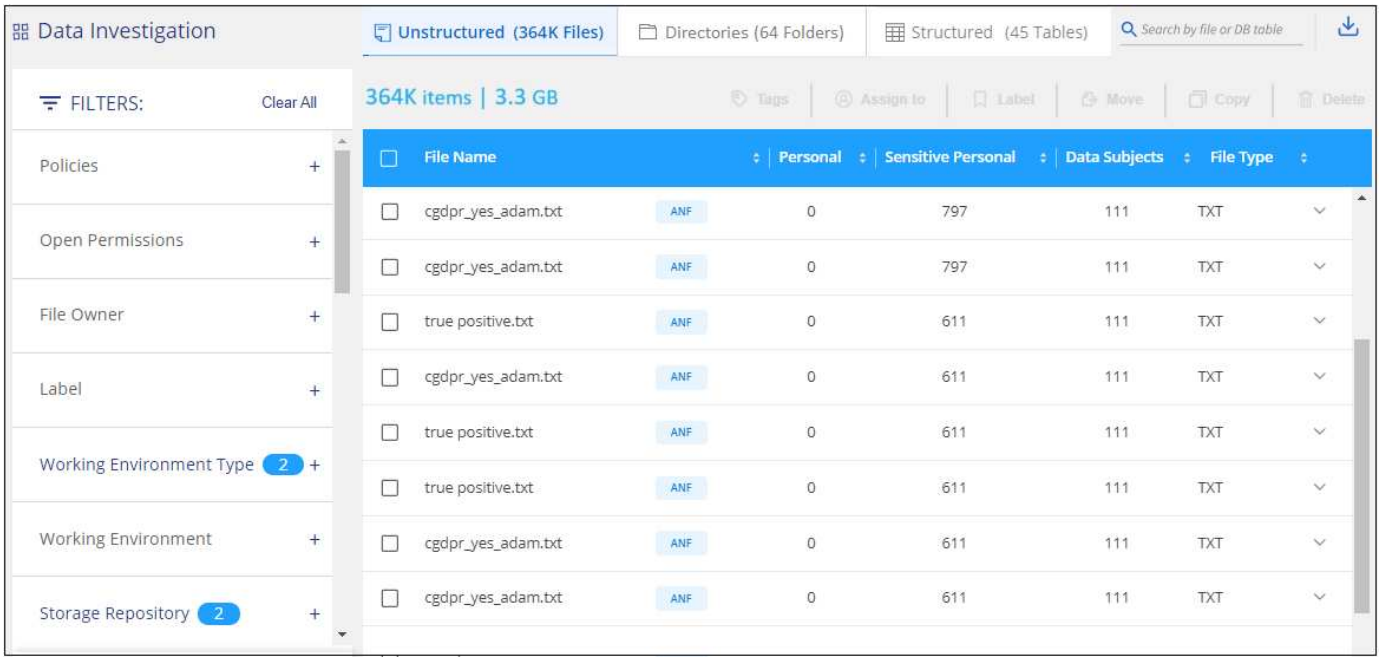
[データ調査]ページで詳細を表示すると、組織のデータを調査できます。このページには、ガバナンスダッシュボードやコンプライアンスダッシュボードなど、BlueXPの分類UIのさまざまな領域から移動できます。

> このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

[Data Investigation]ページでのデータのフィルタリング

調査ページの内容をフィルタリングして、表示する結果のみを表示できます。これは非常に強力な機能です。データをリファインした後、ページ上部のボタンバーを使用して、ファイルのコピー、ファイルの移動、ファイルへのタグまたはAIPラベルの追加など、さまざまなアクションを実行できます。

ページをリファインした後で、そのページの内容をレポートとしてダウンロードする場合は、をクリックします ボタン"] ボタンを押します。 データ調査レポートの詳細については、こちらをご覧ください。



- トップレベルのタブでは、ファイル（非構造化データ）、ディレクトリ（フォルダおよびファイル共有）、またはデータベース（構造化データ）のデータを表示できます。
- 各列の上部にあるコントロールを使用して、結果を数値またはアルファベット順に並べ替えることができ

ます。

- 左側のペインフィルタを使用すると、以降のセクションで説明する属性を選択して、結果を絞り込むことができます。

感度と内容でデータをフィルタリングします

データに含まれている機密情報の量を表示するには、次のフィルタを使用します。

フィルタ	詳細
カテゴリ	を選択します "カテゴリのタイプ"。
感度レベル	感度レベルを選択します。個人レベル、個人レベル、または非機密レベルを選択します。
IDの数	検出された機密識別子のファイルごとの範囲を選択します。個人データと機密性の高い個人データが含まれます。ディレクトリでフィルタリングする場合、BlueXPの分類では、各フォルダ（およびサブフォルダ）内のすべてのファイルに一致するものが合計されます。 注: 2023年12月(バージョン1.26.6)リリースでは、ディレクトリごとの個人識別情報(PII)データの数を計算するオプションが一時的に削除されました。
個人データ	を選択します "個人データの種類"。
機密性の高い個人データ	を選択します "機密性の高い個人データのタイプ"。
データの件名	データ主体のフルネームまたは既知の識別子を入力します "データ主体の詳細については、こちらをご覧ください"。

ユーザの所有者とユーザの権限でデータをフィルタリングします

次のフィルタを使用して、ファイルの所有者とデータにアクセスするための権限を表示します。

フィルタ	詳細
[アクセス許可] を開きます	データ内およびフォルダ/共有内の権限のタイプを選択します。
ユーザ / グループの権限	1つ以上のユーザ名またはグループ名を選択するか、または名前の一部を入力してください。
ファイルの所有者	ファイル所有者名を入力します。
アクセス権を持つユーザの数	1つまたは複数のカテゴリ範囲を選択して、特定の数のユーザーに対してどのファイルおよびフォルダが開かれているかを表示します。

時間でデータをフィルタリングします

次のフィルタを使用して、条件に基づいてデータを表示します。

フィルタ	詳細
作成時刻（ Created Time ）	ファイルを作成したときの期間を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。

フィルタ	詳細
検出時刻	BlueXPの分類でファイルが検出された期間を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。
最終更新日	ファイルが最後に変更された時間範囲を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。
最後にアクセスした	ファイルまたはディレクトリ（CIFSまたはNFSのみ）が最後にアクセスされた時間範囲を選択します。カスタムの期間を指定して、検索結果をさらに絞り込むこともできます。BlueXP分類でスキャンされるファイルの種類については、BlueXP分類でファイルがスキャンされるのはこれが最後です。 BlueXPの分類では、SharePoint Online、SharePointオンプレミス（SharePoint Server）、OneDrive、Google Drive、Amazon S3の各データソースから「最終アクセス時刻」は抽出されません。

メタデータでデータをフィルタリングします

次のフィルタを使用して、場所、サイズ、およびディレクトリまたはファイルタイプに基づいてデータを表示します。

フィルタ	詳細
ファイルパス	クエリに含めるか除外するパスの一部または全部を20個まで入力します。対象パスと除外パスの両方を入力すると、対象パス内のすべてのファイルが最初に検出され、除外パスからファイルが削除されて結果が表示されます。このフィルタで「*」を使用しても効果はなく、特定のフォルダをスキャンから除外することはできません。設定された共有の下にあるすべてのディレクトリとファイルがスキャンされます。
ディレクトリタイプ（Directory Type）	ディレクトリタイプとして「共有」または「フォルダ」を選択します。
ファイルタイプ	を選択します "ファイルのタイプ"。
ファイルサイズ	ファイルサイズの範囲を選択します。
ファイル・ハッシュ	ファイルのハッシュを入力し、名前が異なる場合でも特定のファイルを検索します。

ストレージタイプでデータをフィルタリングします

ストレージタイプ別にデータを表示するには、次のフィルタを使用します。

フィルタ	詳細
作業環境タイプ（ Working Environment Type ）	作業環境のタイプを選択します。OneDrive、SharePoint、Google Driveは、[アプリ]に分類されます。
作業環境名	特定の作業環境を選択します。
ストレージリポジトリ	ボリュームやスキーマなどのストレージリポジトリを選択します。

タグ、ラベル、割り当てられたユーザ、およびポリシーでデータをフィルタリングします

AIPラベルまたはタグでデータを表示するには、次のフィルタを使用します。

フィルタ	詳細
ポリシー	ポリシーを選択します。実行します "こちらをご覧ください" をクリックして、既存のポリシーのリストを表示し、独自のカスタムポリシーを作成します。
ラベル	選択するオプション "AIP ラベル" ファイルに割り当てられます。
タグ	選択するオプション "タグ" ファイルに割り当てられます。
割り当て先	ファイルが割り当てられているユーザーの名前を選択します。

分析ステータスでデータをフィルタリングします

次のフィルタを使用して、BlueXPの分類スキャンステータス別にデータを表示します。

フィルタ	詳細
解析ステータス（Analysis Status）	オプションを選択して、[最初のスキャン保留中]、[スキャン完了]、[再スキャン保留中]、または[スキャンに失敗しました]のファイルのリストを表示します。
スキャン分析イベント	BlueXPの分類で最終アクセス時刻を復元できなかったために分類されなかったファイルを表示するか、BlueXPの分類で最終アクセス時刻を復元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するかを選択します。

"「最終アクセス時刻」のタイムスタンプの詳細を参照してください" スキャン分析イベントを使用してフィルタリングするときに[Investigation]ページに表示される項目の詳細については、を参照してください。

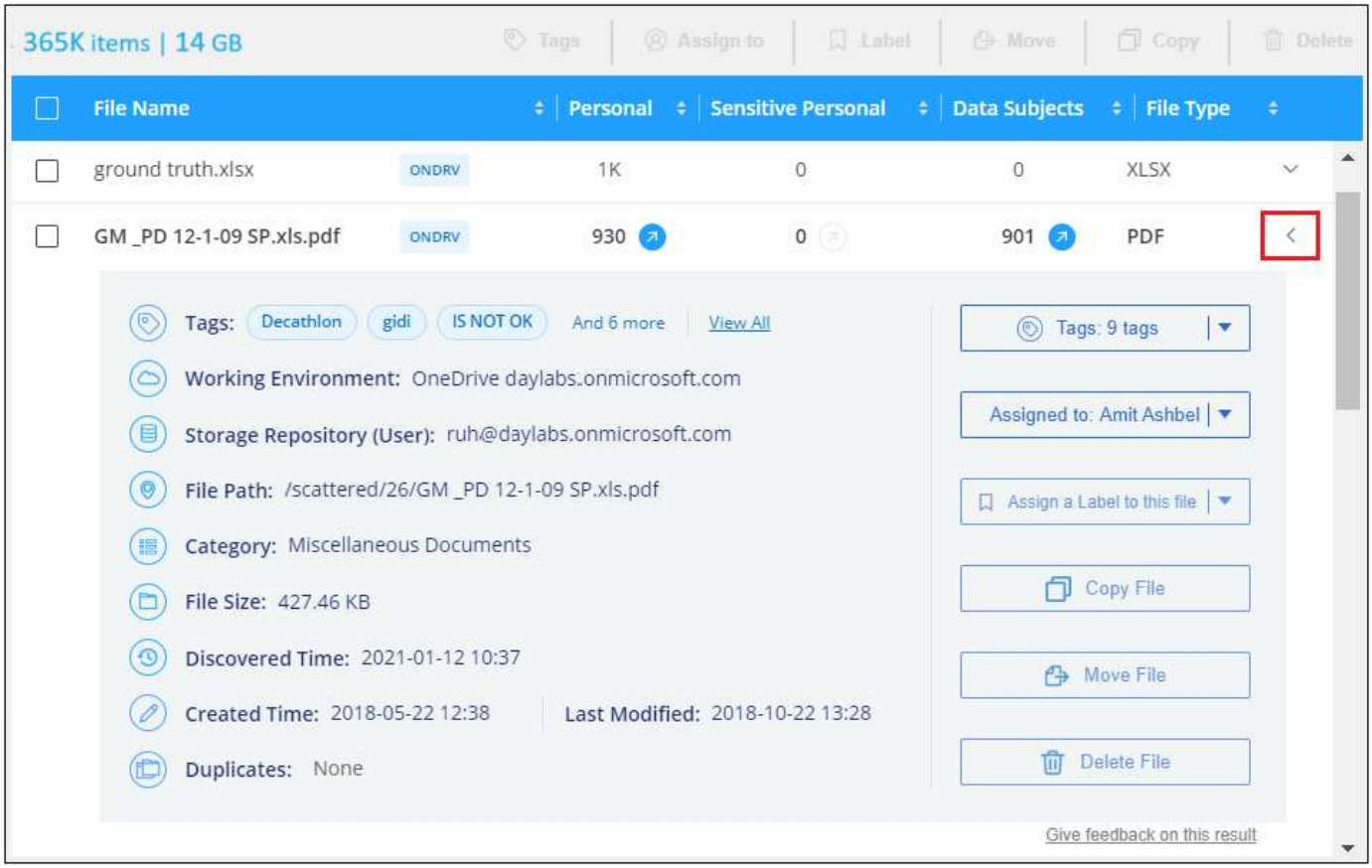
重複でデータをフィルタリングします

ストレージ内で複製されているファイルを表示するには、次のフィルタを使用します。

フィルタ	詳細
重複	リポジトリ内でファイルを複製するかどうかを選択します。

ファイルメタデータの表示

[データ調査結果] ペインで、をクリックできます ⌄ をクリックすると、単一のファイルについてファイルのメタデータが表示されます。



ページのファイルのメタデータの詳細を示すスクリーンショット。"]

ファイルが存在する作業環境とボリュームを表示するだけでなく、メタデータには、ファイル権限、ファイルの所有者、このファイルの重複がないかどうか、および AIP ラベルが割り当てられている場合など、より多くの情報が表示されます "BlueXPに統合されたAIPです"）。この情報は、を計画している場合に役立ちます "ポリシーを作成します" データのフィルタリングに使用できるすべての情報が表示されます。

すべてのデータソースについて、すべての情報が表示されるわけではなく、そのデータソースに適した情報だけが表示されることに注意してください。たとえば、ボリューム名、権限、および AIP ラベルは、データベースファイルには関係ありません。

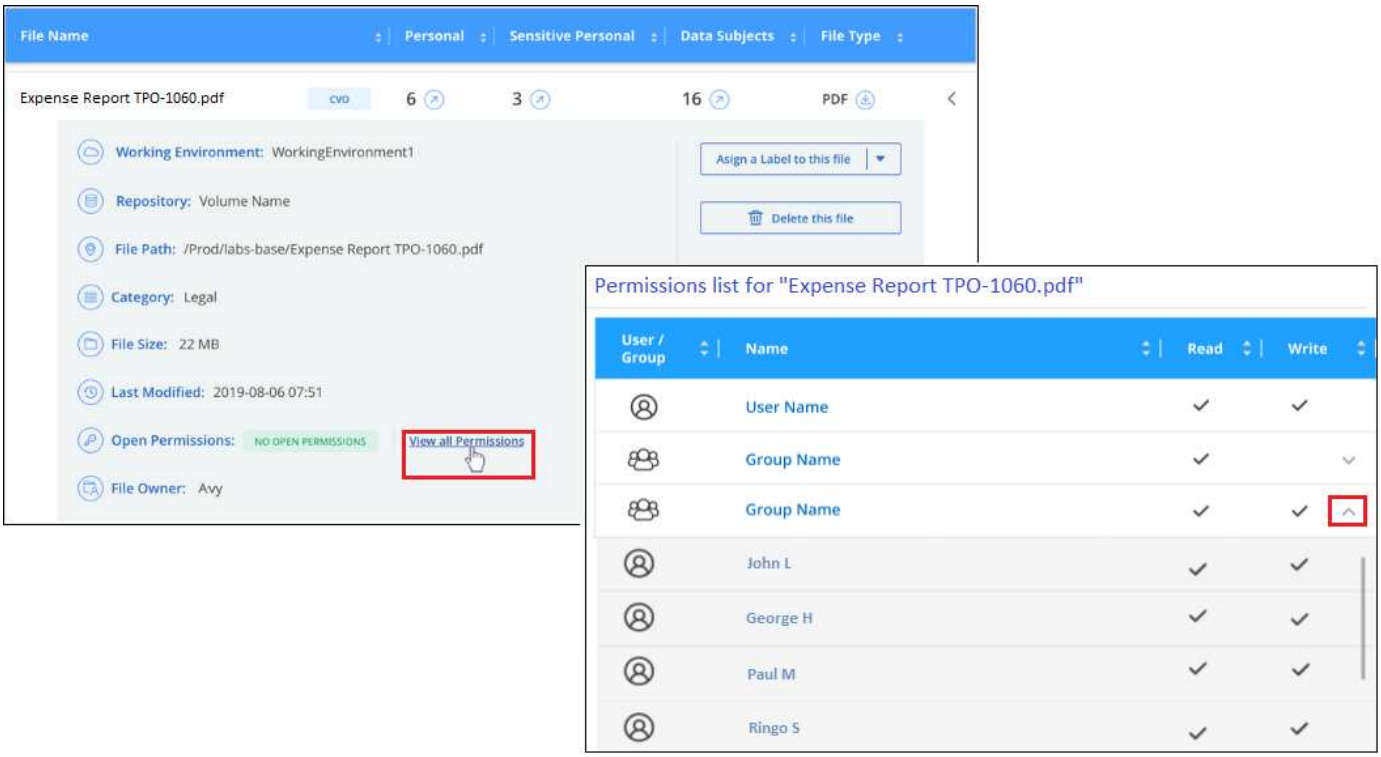
単一のファイルの詳細を表示する場合は、ファイルに対していくつかの操作を実行できます。

- ファイルは任意の NFS 共有に移動またはコピーできます。を参照してください "ソースファイルを NFS 共有に移動しています" および "ソースファイルを NFS 共有にコピーしています" を参照してください。
- ファイルを削除できます。を参照してください "ソースファイルを削除しています" を参照してください。
- ファイルに特定のステータスを割り当てることができます。を参照してください "タグの適用" を参照してください。
- このファイルをBlueXPユーザーに割り当てることで、ファイルに対して実行する必要があるフォローアップアクションを実行できます。を参照してください "ファイルへのユーザの割り当て" を参照してください。
- AIPラベルをBlueXPに統合した場合は、このファイルにラベルを割り当てることができます。また、すでに存在する場合は別のラベルに変更することもできます。を参照してください "AIP ラベルを手動で割り当てる" を参照してください。

ファイルおよびディレクトリの権限を表示する

ファイルまたはディレクトリへのアクセス権を持つすべてのユーザーまたはグループのリスト、およびそれらが持っているアクセス権のタイプを表示するには、*すべてのアクセス権を表示*をクリックします。このボタンは、CIFS共有、SharePoint Online、SharePoint On-Premise、OneDriveのデータに対してのみ使用できます。

ユーザ名とグループ名の代わりにSID（セキュリティ識別子）が表示される場合は、Active DirectoryをBlueXPに統合する必要があります。 "詳細については、「方法」を参照してください"。



をクリックできます をクリックすると、グループの一部であるユーザのリストが表示されます。

さらに、 ユーザまたはグループの名前をクリックすると、[調査]ページにそのユーザまたはグループの名前が表示され、[ユーザ/グループの権限]フィルタに入力されます。これにより、そのユーザまたはグループがアクセスできるすべてのファイルとディレクトリを表示できます。

ストレージシステム内の重複ファイルのチェック

重複ファイルがストレージシステムに保存されているかどうかを確認できます。これは、ストレージスペースを節約できる領域を特定する場合に便利です。また、特定の権限や機密情報を持つファイルが、ストレージシステム内で不必要に重複しないようにすることもできます。

1MB以上で、個人情報または機密情報を含むすべてのファイル（データベースを除く）が比較され、重複がないかどうかが確認されます。[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範囲のどのファイルが重複しているかを確認できます。

BlueXPの分類では、ハッシュテクノロジを使用して重複ファイルが特定されます。ハッシュコードが別のファイルと同じファイルがある場合、ファイル名が異なる場合でも、ファイルが完全に重複していることを100% 確認できます。

重複ファイルのリストをダウンロードし、ストレージ管理者に送信して、削除可能なファイルをユーザが判別

できるようにします。または "ファイルを削除します" 特定のバージョンのファイルが不要であることが確信できる場合は、自分自身で実行します。

重複ファイルをすべて表示

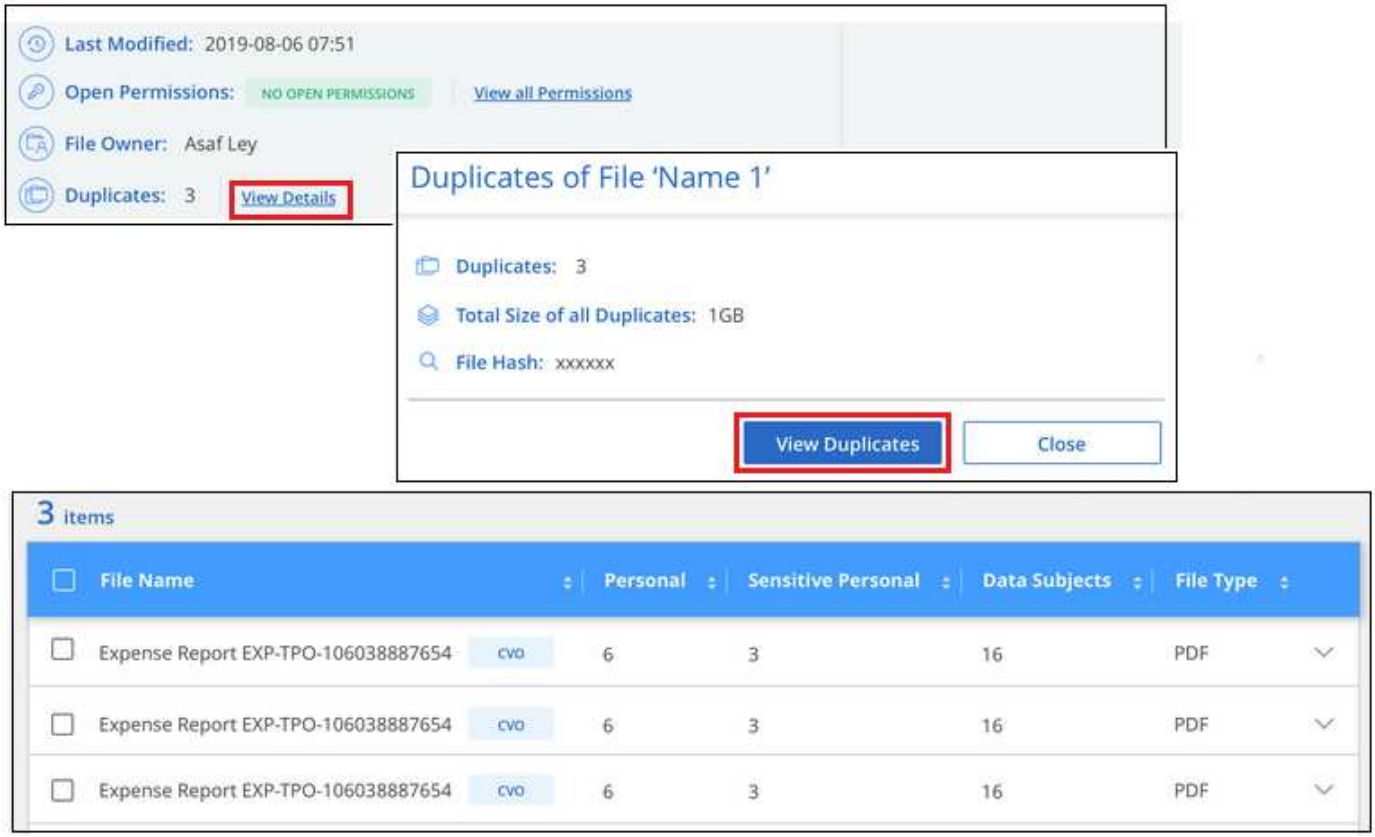
スキャンする作業環境およびデータソースで複製されているすべてのファイルのリストが必要な場合は、 [データの調査] ページで、 [重複] > [重複しているもの] というフィルタを使用できます。

複製されたすべてのファイルが結果ページに表示されます。

特定のファイルが重複しているかどうかを表示する

1 つのファイルに重複があるかどうかを確認するには、 [データ調査結果] ペインでをクリックします ⌄ をクリックすると、単一のファイルについてファイルのメタデータが表示されます。特定のファイルが重複している場合、この情報は _Duplicats_field の横に表示されます。

重複したファイルとその場所のリストを表示するには、 [* 詳細の表示 *] をクリックします。次のページで、 [重複の表示 *] をクリックして、 [調査] ページでファイルを表示します。



このページで指定されている「ファイルハッシュ」値を使用して、 ［調査］ ページに直接入力すると、特定の重複ファイルをいつでも検索できます。また、ポリシーで使用することもできます。

データ調査レポート

Data Investigation Reportは、Data Investigationページのフィルタリングされた内容をダウンロードしたものです。

レポートには、次の2つの形式があります。

- ローカルマシンに保存できる.csvファイル。

  このレポートには、最大10,000行のデータを含めることができます。

- NFS共有にエクスポートする.jsonファイルとして指定します。

  25万行を超えるデータがある場合は、追加の.jsonファイルが作成されます。

  ファイル共有にエクスポートする場合は、BlueXPの分類にエクスポートアクセス用の正しい権限が割り当てられていることを確認してください。

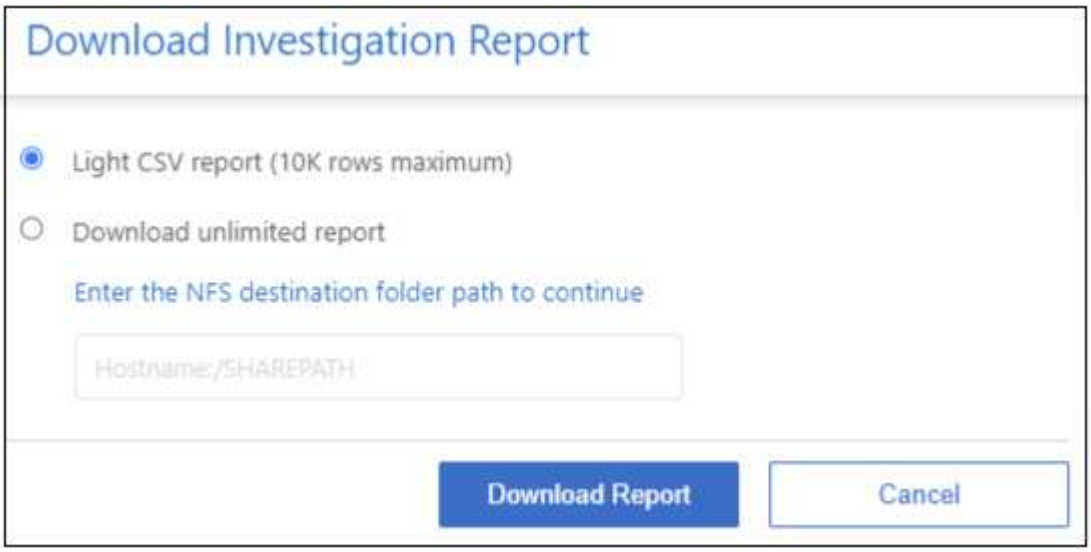
BlueXPの分類でファイル（非構造化データ）、ディレクトリ（フォルダとファイル共有）、データベース（構造化データ）をスキャンしている場合は、最大3つのレポートファイルをダウンロードできます。

データ調査レポートの生成

手順

1. [データ調査]ページで、をクリックします ボタン"] ボタンをクリックします。
2. データの.csvレポートと.jsonレポートのどちらをダウンロードするかを選択し、*レポートのダウンロード*をクリックします。

   JSONレポートを選択するときは、レポートをダウンロードするNFS共有の名前を「<host_name>：/<share_path>`」の形式で入力します。



結果

レポートをダウンロード中であることを示すメッセージがダイアログに表示されます。

JSONレポートの生成の進捗状況は、で確認できます "[アクションステータス（ Actions Status ） パネル"]。

各データ調査レポートに含まれる情報

非構造化ファイルデータレポート*には、ファイルに関する次の情報が含まれています。

- ファイル名
- 場所のタイプ
- 作業環境の名前
- ストレージリポジトリ（ボリューム、バケット、共有など）
- リポジトリタイプ
- ファイルパス
- ファイルタイプ
- ファイルサイズ（MB）
- 時刻を作成しました
- 最終更新日
- 最後にアクセスした
- ファイルの所有者
- カテゴリ
- 個人情報
- 機密性の高い個人情報
- オープンアクセス権
- スキャン分析エラー
- 削除の検出日

  削除の検出日は、ファイルが削除または移動された日付を示します。これにより、機密ファイルがいつ移動されたかを識別できます。削除されたファイルは、ダッシュボードまたは [調査] ページに表示されるファイル番号カウントの一部ではありません。ファイルは CSV レポートにのみ表示されます。

非構造化ディレクトリデータレポート*には、フォルダおよびファイル共有に関する次の情報が含まれています。

- 作業環境のタイプ
- 作業環境の名前
- ディレクトリ名
- ストレージリポジトリ（フォルダ、ファイル共有など）
- ディレクトリ所有者
- 時刻を作成しました
- 検出時刻
- 最終更新日
- 最後にアクセスした
- オープンアクセス権
- ディレクトリタイプ

構造化データレポート*には、データベーステーブルに関する次の情報が含まれています。

- DB テーブル名
- 場所のタイプ
- 作業環境の名前
- ストレージリポジトリ（スキーマなど）
- 列数
- 行数
- 個人情報
- 機密性の高い個人情報

プライベートデータを整理します

BlueXPの分類では、プライベートデータをさまざまな方法で管理、整理できます。これにより、最も重要なデータを簡単に確認できます。

- に登録している場合は "Azure 情報保護（ AIP ）" ファイルを分類して保護するには、BlueXPの分類を使用してAIPラベルを管理します。

> 2023年12月（v1.26.6）リリースでは、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一時的に削除されました。

- 組織または特定の種類のフォローアップのためにマークするファイルにタグを追加できます。
- BlueXPユーザーを特定のファイルまたは複数のファイルに割り当てることで、ユーザーがファイルの管理を担当できるようになります。
- 「ポリシー」機能を使用すると、 1 つのボタンをクリックして簡単に結果を表示できるように、独自のカスタム検索クエリを作成できます。
- 特定の重要なポリシーの結果が返された場合は、BlueXPユーザーまたはその他の電子メールアドレスに電子メールアラートを送信できます。

> このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。

タグまたはラベルを使用する必要がありますか？

以下は、BlueXPの分類タギングとAzure Information Protectionのラベル付けの比較です。

タグ	ラベル
ファイルタグはBlueXPに統合された分類機能です。	Azure Information Protection （ AIP ）に加入している必要があります。

タグ	ラベル
タグはBlueXP分類データベースにのみ保存され、ファイルには書き込まれません。ファイル、アクセス日時または変更日時は変更されません。	ラベルはファイルの一部であり、ラベルが変更されるとファイルが変更されます。この変更によって、アクセス日時や変更日時も変更されます。
1 つのファイルに複数のタグを設定できます。	1 つのファイルに 1 つのラベルを付けることができます。
このタグは、BlueXPの内部分類アクション（コピー、移動、削除、ポリシーの実行、 など	ファイルを読み取ることができる他のシステムでは、ラベルを確認できます。このラベルは、自動化のために使用できます。
ファイルにタグが設定されているかどうかを確認するために使用される API 呼び出しは 1 つだけです。	

AIP ラベルを使用してデータを分類します

サブスクライブ済みの場合は、BlueXP分類でスキャンするファイルでAIPラベルを管理できます "Azure 情報保護（ AIP ）"。AIP を使用すると、コンテンツにラベルを適用することで、ドキュメントやファイルを分類して保護できます。BlueXPでは、ファイルにすでに割り当てられているラベルの表示、ファイルへのラベルの追加、既存のラベルの変更を行うことができます。

BlueXPの分類では、.DOC、.DOCX、.PDF、.PPTX、.XLSの各ファイルタイプでAIPラベルがサポートされます。 .XLSX。

- 現在、 30MB を超えるファイルのラベルは変更できません。OneDrive、SharePoint 、Google Driveアカウントの場合、最大ファイルサイズは4 MBです。
- AIPに存在しないラベルがファイルに含まれている場合、BlueXPの分類ではラベルのないファイルとみなされます。
- 政府機関の地域、またはインターネットアクセスのないオンプレミスの場所（ダークサイトとも呼ばれます）にBlueXPの分類を導入している場合は、AIPラベル機能を使用できません。

ワークスペースに**AIP**ラベルを統合

AIPラベルを管理するには、既存のAzureアカウントにサインインして、AIPラベル機能をBlueXPの分類に統合する必要があります。有効にすると、すべてのファイルの AIP ラベルを管理できます "データソース" を選択します。

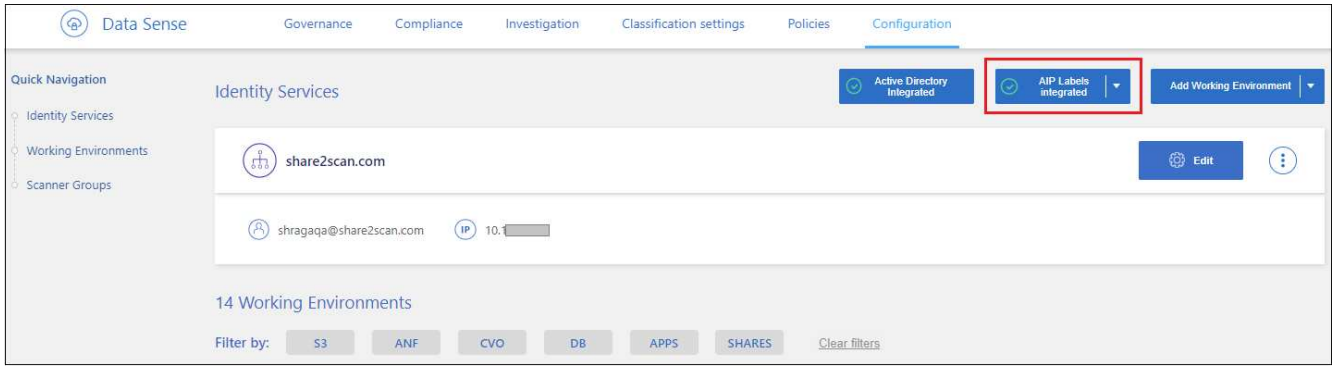
要件

- アカウントと Azure Information Protection のライセンスが必要です。
- Azure アカウントのログインクレデンシャルが必要です。
- Amazon S3 バケット内のファイルのラベルを変更する場合は、権限「 3 ： PutObject 」が IAM ロールに含まれていることを確認します。を参照してください "IAM ロールを設定します"。

手順

1. BlueXPの分類の[設定]ページで、*[Integrate AIP Labels]*をクリックします。

2. [Integrate AIP Labels （ AIP ラベルの統合）] ダイアログで、 [* Sign in to Azure* （ Azure にサインイン ）]
3. 表示される Microsoft ページで、アカウントを選択し、必要なクレデンシャルを入力します。
4. BlueXPの分類タブに戻り、「_AIP Labels were integrated successfully with the account <account_name> _」というメッセージが表示されます。
5. [* 閉じる] をクリックすると、ページの上部に「 *AIP* ラベル *integrated_* 」というテキストが表示されます。



結果

AIP ラベルは、 ［ 調査 ］ ページの結果ペインで表示および割り当てることができます。また、ポリシーを使用して AIP ラベルをファイルに割り当てることもできます。

ファイル内の**AIP**ラベルの表示

ファイルに割り当てられている現在の AIP ラベルを表示できます。

[データ調査結果] ペインで、をクリックします ⌄ をクリックします。

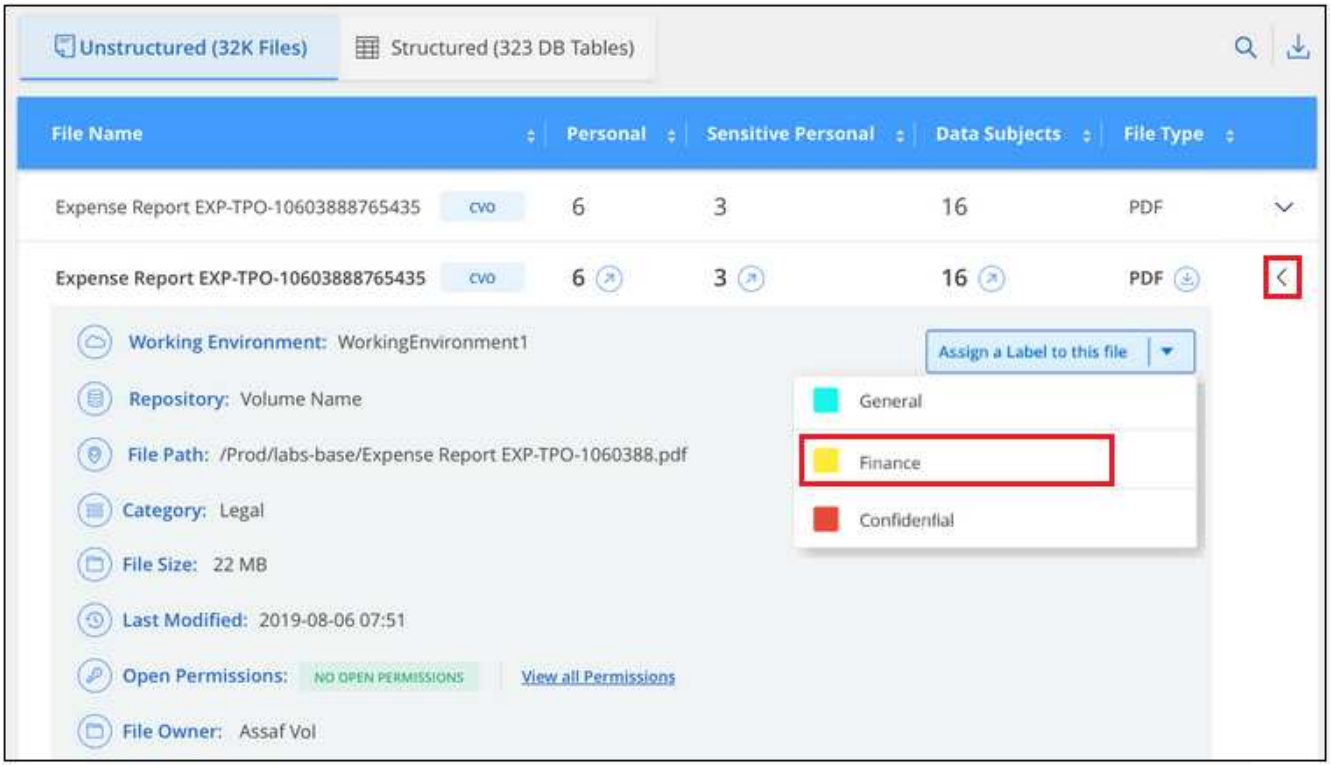
AIPラベルの手動割り当て

BlueXPの分類を使用して、ファイルのAIPラベルを追加、変更、削除できます。

AIP ラベルを 1 つのファイルに割り当てる手順は、次のとおりです。

手順

1. [データ調査結果] ペインで、をクリックします をクリックします。



ページのファイルのメタデータの詳細を示すスクリーンショット。"]

2. [* このファイルにラベルを割り当て *] をクリックして、ラベルを選択します。

   ラベルがファイルメタデータに表示されます。

AIPラベルを複数のファイルに割り当てる手順は、次のとおりです。AIPラベルは、一度に最大20個のファイル（UIの1ページ）に割り当てることができます。

手順

1. [データ調査結果] ペインで、ラベル付けするファイルを選択します。

ページの [ラベル] ボタン。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。

2. ボタンバーの * Label * をクリックし、 AIP ラベルを選択します。

AIP ラベルが、選択したすべてのファイルのメタデータに追加されます。

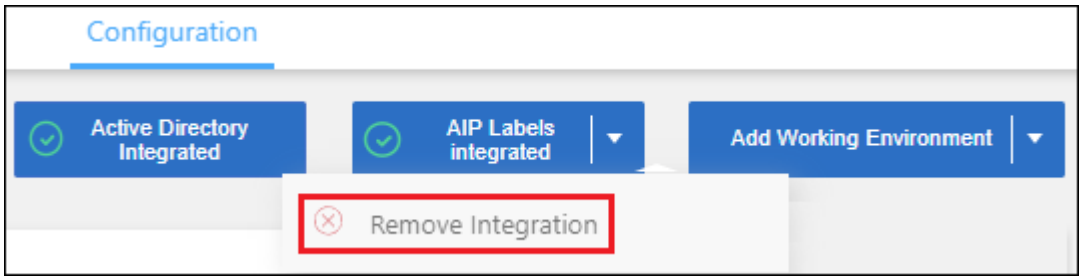
AIP統合の削除

ファイル内のAIPラベルを管理する必要がなくなった場合は、BlueXPの分類インターフェイスからAIPアカウントを削除できます。

BlueXPの分類を使用して追加したラベルは変更されません。ファイルに存在するラベルは、現在存在しているラベルのままになります。

手順

1. _Configuration_page で、 *AIP ラベル統合 > 統合の削除 * をクリックします。



2. 確認ダイアログで、 [統合の削除（ Remove Integration ）] をクリックします。

タグを適用してスキャンしたファイルを管理

特定の種類のフォローアップでマークするファイルにタグを追加できます。たとえば、重複するファイルがいくつか見つかった場合に、それらのファイルを 1 つ削除する必要がありますが、削除するファイルを確認する必要があります。このファイルに「削除するチェック」というタグを追加すると、このファイルに何らかの調査と将来のアクションが必要であることがわかります。

BlueXPでは、ファイルに割り当てられているタグの表示、ファイルに対するタグの追加と削除、名前の変更や既存のタグの削除を行うことができます。

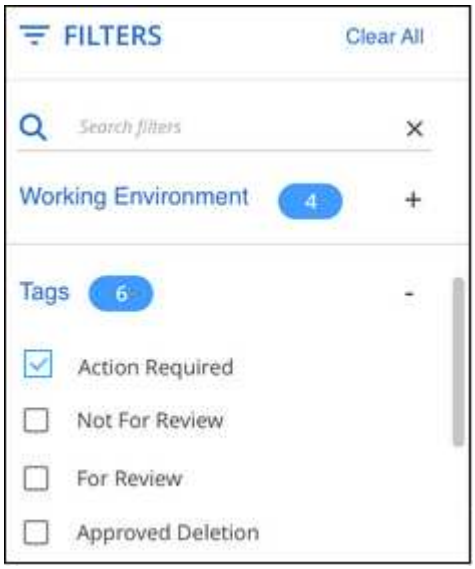
AIP ラベルがファイルメタデータの一部であるのと同じ方法で、タグがファイルに追加されないことに注意してください。このタグはBlueXPユーザのみがBlueXP分類を使用して確認できるため、ファイルを削除する必要があるかどうか、または何らかのフォローアップが必要かどうかを確認できます。

> BlueXPで分類されたファイルに割り当てられたタグは、リソース（ボリュームや仮想マシンインスタンスなど）に追加できるタグとは関係ありません。BlueXPの分類タグはファイルレベルで適用されます。

特定のタグが適用されているファイルを表示する

特定のタグが割り当てられているすべてのファイルを表示できます。

1. BlueXP分類の*[Investigation]*タブをクリックします。
2. [データ調査] ページで、 [フィルタ] ペインの [* タグ] をクリックし、必要なタグを選択します。



ペインからタグを選択する方法を示すスクリーンショット。"]

[調査結果] ペインには、これらのタグが割り当てられているすべてのファイルが表示されます。

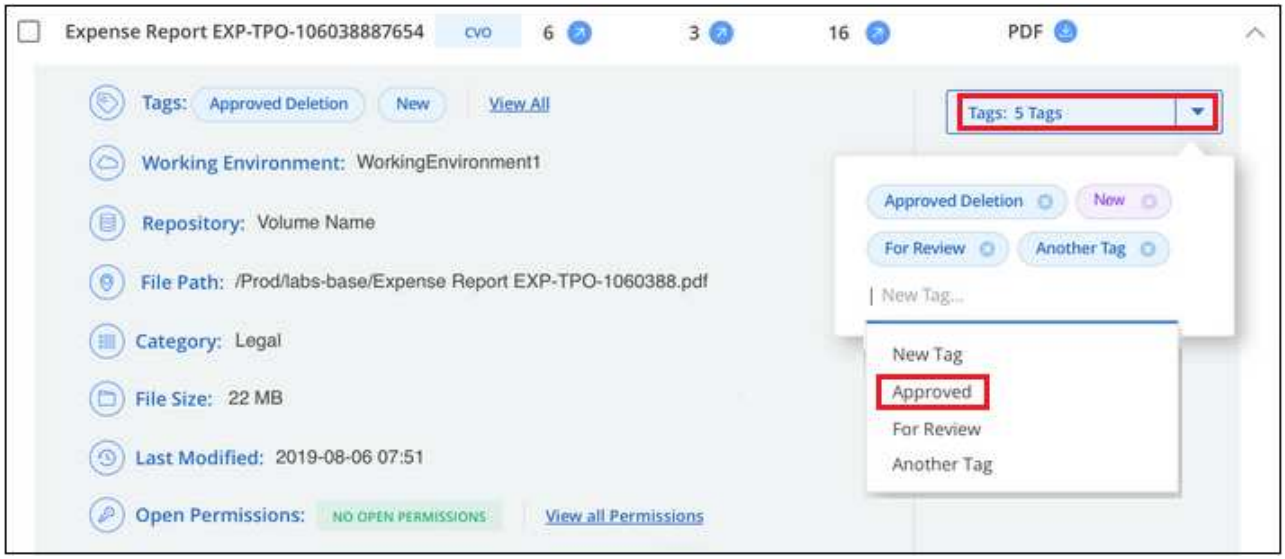
ファイルへのタグの割り当て

タグは、単一のファイルまたはファイルのグループに追加できます。

タグを 1 つのファイルに追加するには：

手順

1. [データ調査結果] ペインで、をクリックします をクリックします。
2. [* タグ * （ * Tags * ）] フィールドをクリックすると、現在割り当てられているタグが表示されます。
3. タグを追加します。
   - 既存のタグを割り当てるには、「 * 新しいタグ … 」フィールドをクリックして、タグの名前を入力します。探しているタグが表示されたら、そのタグを選択して * Enter * を押します。
   - 新しいタグを作成してファイルに割り当てるには、 [新しいタグ …] * フィールドをクリックし、新しいタグの名前を入力して、 **Enter** キーを押します。



ページでファイルにタグを割り当てる方法を示すスクリーンショット。"]

タグがファイルメタデータに表示されます。

複数のファイルにタグを追加するには：

手順

1. [データ調査結果] ペインで、タグを付けるファイルを選択します。

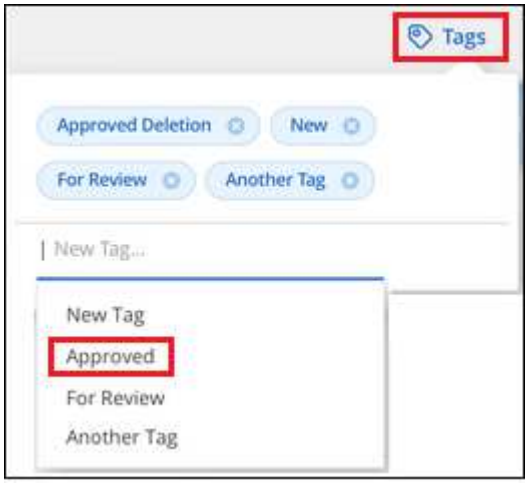
ページから、タグを付けるファイルの選択方法と [タグ] ボタンを示すスクリーンショット。"]

   - 個々のファイルを選択するには、各ファイル（ Volume_1）。
   - 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。

- すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

  一度に最大100,000個のファイルにタグを適用できます。

2. ボタンバーで * タグ * をクリックすると、現在割り当てられているタグが表示されます。
3. タグを追加します。
   - 既存のタグを割り当てるには、「 * 新しいタグ … 」フィールドをクリックして、タグの名前を入力します。探しているタグが表示されたら、そのタグを選択して * Enter * を押します。
   - 新しいタグを作成してファイルに割り当てるには、 [新しいタグ …] * フィールドをクリックし、新しいタグの名前を入力して、 **Enter** キーを押します。



ページで複数のファイルにタグを割り当てる方法を示すスクリーンショット。"]

4. 確認ダイアログでタグの追加を承認し、選択したすべてのファイルのメタデータにタグを追加します。

ファイルからタグを削除

不要になったタグは削除できます。

既存のタグの * x * をクリックするだけです。

複数のファイルを選択した場合、タグはすべてのファイルから削除されます。

特定のファイルを管理するためのユーザの割り当て

BlueXPユーザーを特定のファイルまたは複数のファイルに割り当てることができるため、ユーザーはファイルに対して実行する必要があるフォローアップアクションを実行できます。この機能は、多くの場合、カスタムステータスタグをファイルに追加する機能で使用されます。

たとえば、特定の個人データを含むファイルで、読み取りおよび書き込みアクセス（オープン権限）を大量に許可する場合などです。したがって、 Status タグ「 Change permissions 」を割り当て、このファイルをユーザー「 Joan Smith 」に割り当てて、問題の修正方法を決定することができます。問題を修正すると、 Status

タグが「 Completed 」に変更されることがあります。

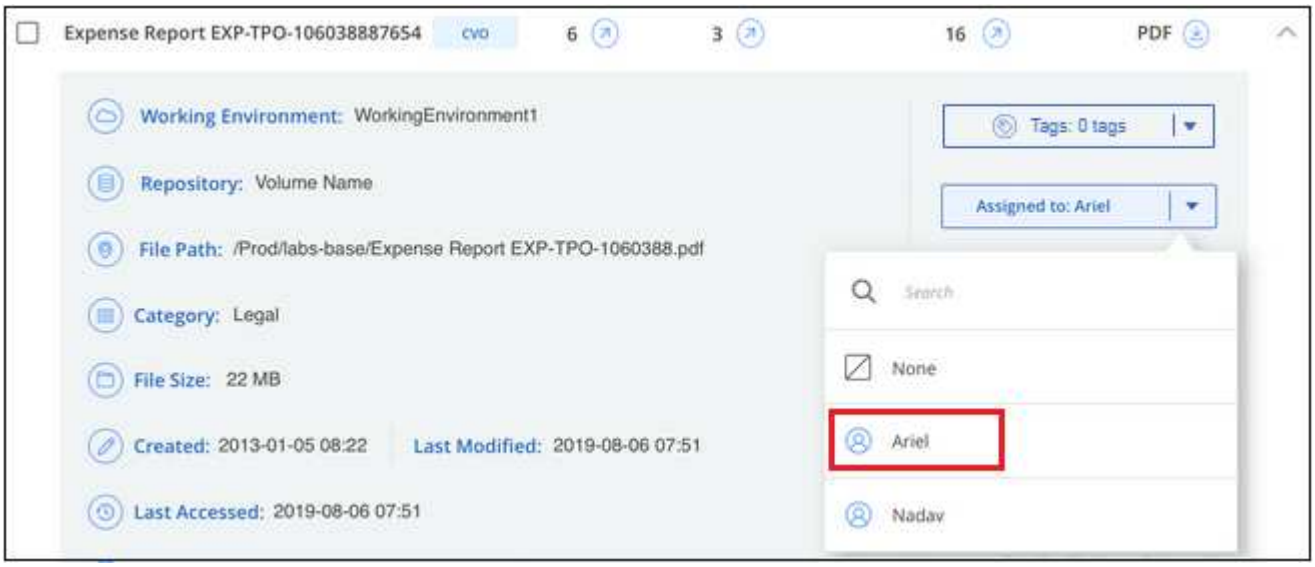
ユーザ名はファイルメタデータの一部としてファイルに追加されるわけではなく、BlueXPユーザがBlueXP分類を使用している場合にのみ表示されます。

[調査] ページの新しいフィルタを使用すると、 [割り当て先] フィールドに同じユーザーを持つすべてのファイルを簡単に表示できます。

ユーザを単一のファイルに割り当てる手順は、次のとおりです。

手順

1. [データ調査結果] ペインで、をクリックします をクリックします。
2. [**Assigned To**] フィールドをクリックして、ユーザ名を選択します。



ページでファイルにユーザーを割り当てる方法を示すスクリーンショット。"]

ユーザ名がファイルメタデータに表示されます。

ユーザーを複数のファイルに割り当てるには、次の手順を実行します。一度に最大20個のファイルにユーザを割り当てることができます（UIの1ページ）。

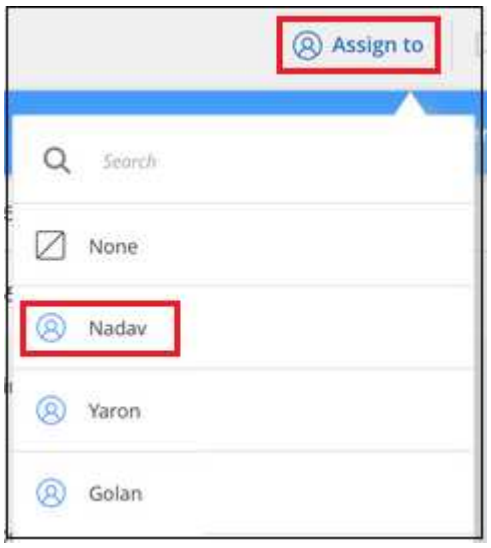
手順

1. [データ調査結果] ペインで、ユーザーに割り当てるファイルを選択します。

ページから、ユーザーに割り当てるファイルの選択方法と [割り当て先] ボタンを示すスクリーンショット。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。

2. ボタンバーで * Assign to * をクリックし、ユーザー名を選択します。



ページでユーザーを複数のファイルに割り当てる方法を示すスクリーンショット。"]

選択したすべてのファイルのメタデータにユーザが追加されます。

データにポリシーを割り当てます

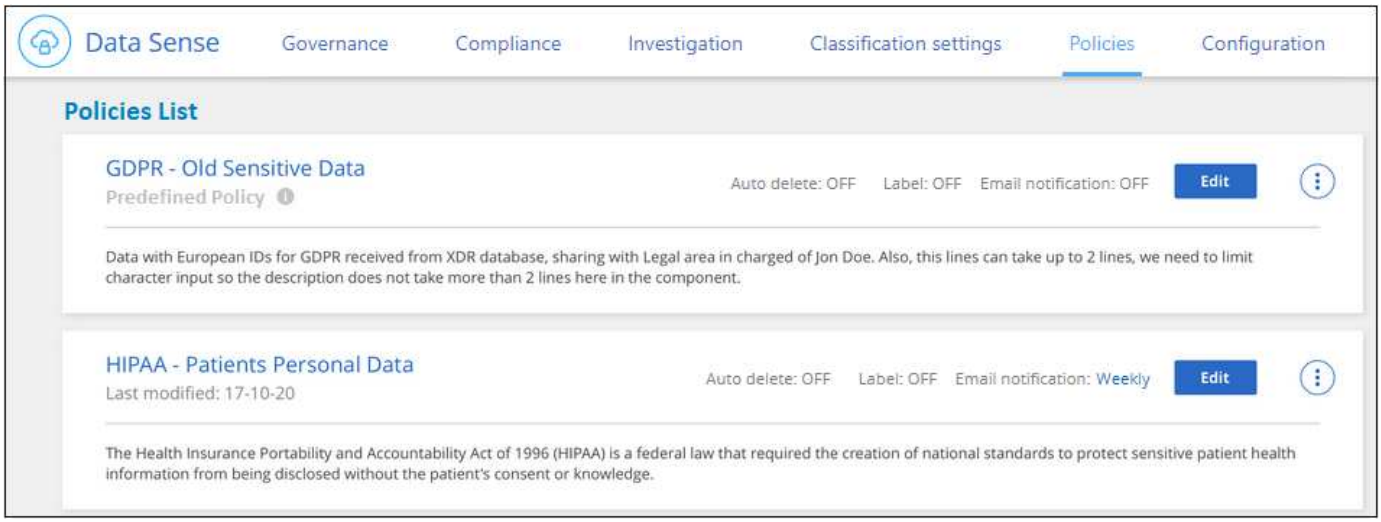
ポリシーは、よく要求されるコンプライアンスクエリーの [調査] ページで検索結果を表示するカスタムフィルタのお気に入りリストのようなものです。BlueXPは分類されており、一般的なお客様の要望に基づいて一連のポリシーが事前定義されています。組織固有の検索結果を提供するカスタムポリシーを作成できます。

ポリシーには次の機能があります。

- 事前定義されたポリシー ユーザの要求に基づいて作成されます
- 独自のカスタムポリシーを作成できます
- ポリシーの結果を含む [調査] ページを起動します ワンクリックで
- 特定の重要なポリシーが結果を返すときに、BlueXPユーザーやその他の電子メールアドレスに電子メールアラートを送信して、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
- AIP の割り当て（ Azure 情報保護） 定義された条件に一致するすべてのファイルに自動的にラベルを付けます ポリシー内
- 特定のポリシーで結果が返されたときにファイルを自動的に削除して（ 1 日に 1 回）、データを自動的に保護できます

コンプライアンスダッシュボードの*[ポリシー]*タブには、BlueXP分類のこのインスタンスで使用可能な事前

定義済みポリシーとカスタムポリシーがすべて表示されます。

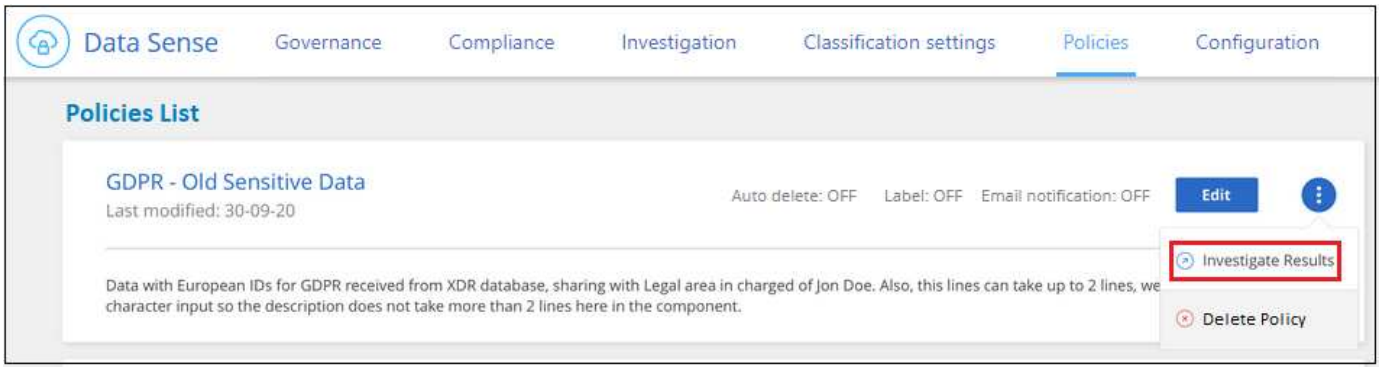


タブのスクリーンショット。"]

さらに、 [調査] ページの [フィルタ] リストにポリシーが表示されます。

[Investigation]ページでのポリシー結果の表示

[調査] ページでポリシーの結果を表示するには、をクリックします ボタン"] ボタンをクリックして特定のポリシーを選択し、 * 調査結果 * を選択します。



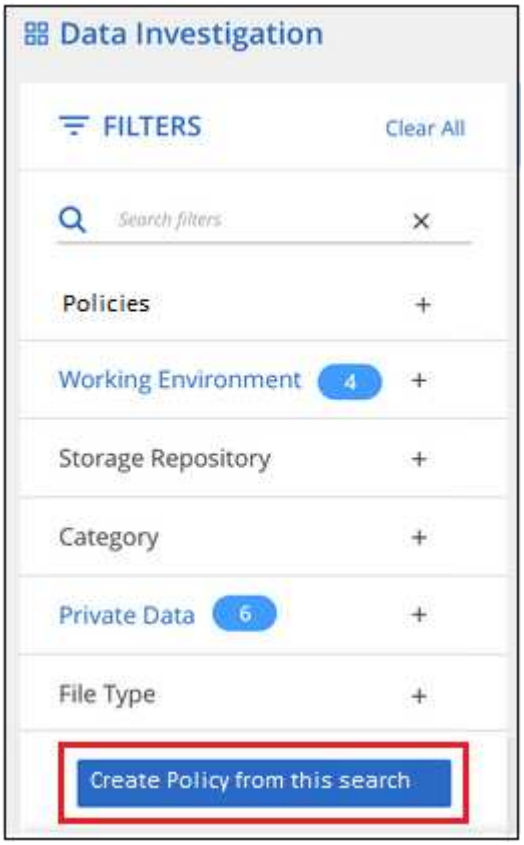
カスタムポリシーの作成

組織固有の検索結果を提供する独自のカスタムポリシーを作成できます。検索条件に一致するすべてのファイルとディレクトリ（共有とフォルダ）の結果が返されます。

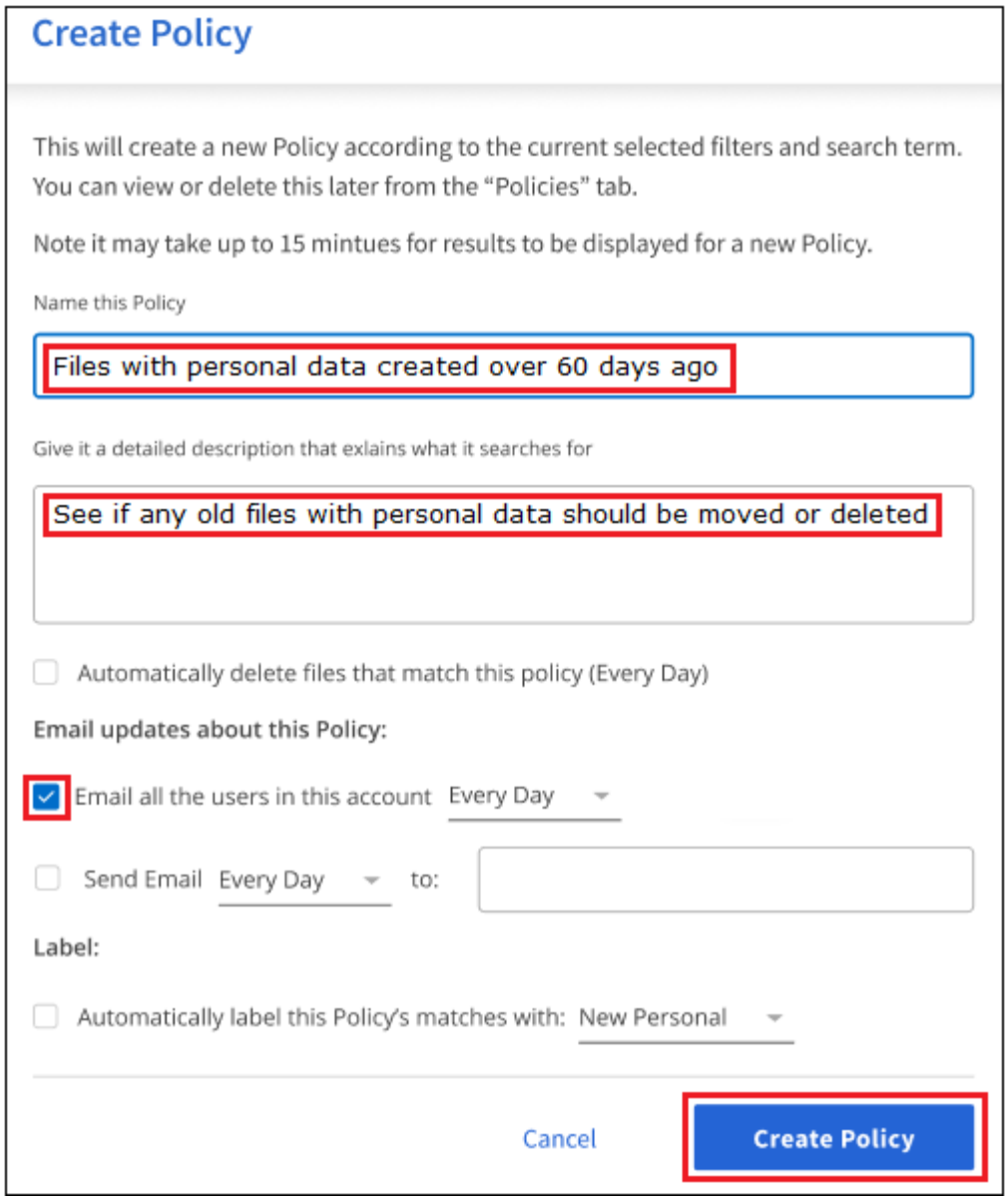
データを削除し、ポリシーの結果に基づいてAIPラベルを割り当てるアクションは、ファイルに対してのみ有効です。検索条件に一致するディレクトリは、自動的に削除することも、AIPラベルを割り当てることもできません。

手順

1. [データ調査] ページで、使用するすべてのフィルタを選択して検索を定義します。を参照してください "[データ調査 ページでデータをフィルタリングします"^] を参照してください。
2. 必要な方法でフィルタ特性をすべて設定したら、 [この検索からポリシーを作成する *] をクリックします。



3. ポリシーに名前を付け、そのポリシーで実行できるその他のアクションを選択します。
   a. 一意の名前と説明を入力します。
   b. 必要に応じて、このチェックボックスをオンにすると、ポリシーのパラメータに一致するファイルが自動的に削除されます。の詳細を確認してください ポリシーを使用してソースファイルを削除しています。
   c. 必要に応じて、アカウントのBlueXPユーザーに通知メールを送信する場合は、このチェックボックスをオンにして、メールの送信間隔を選択します。の詳細を確認してください ポリシーの結果に基づいて E メールアラートを送信する。
   d. 必要に応じて、他のユーザに通知Eメールを送信する場合はチェックボックスをオンにし、Eメールアドレスを20個まで入力して、Eメールの送信間隔を選択します。
   e. 必要に応じて、このチェックボックスをオンにすると、ポリシーパラメータに一致するファイルに AIP ラベルが自動的に割り当てられ、ラベルが選択されます。（AIP ラベルがすでに統合されている場合のみ。の詳細を確認してください "AIP ラベル". ）
   f. [ポリシーの作成 *] をクリックします。



結果

[ポリシー] タブに新しいポリシーが表示されます。

準拠していないデータが見つかった場合にEメールアラートを送信

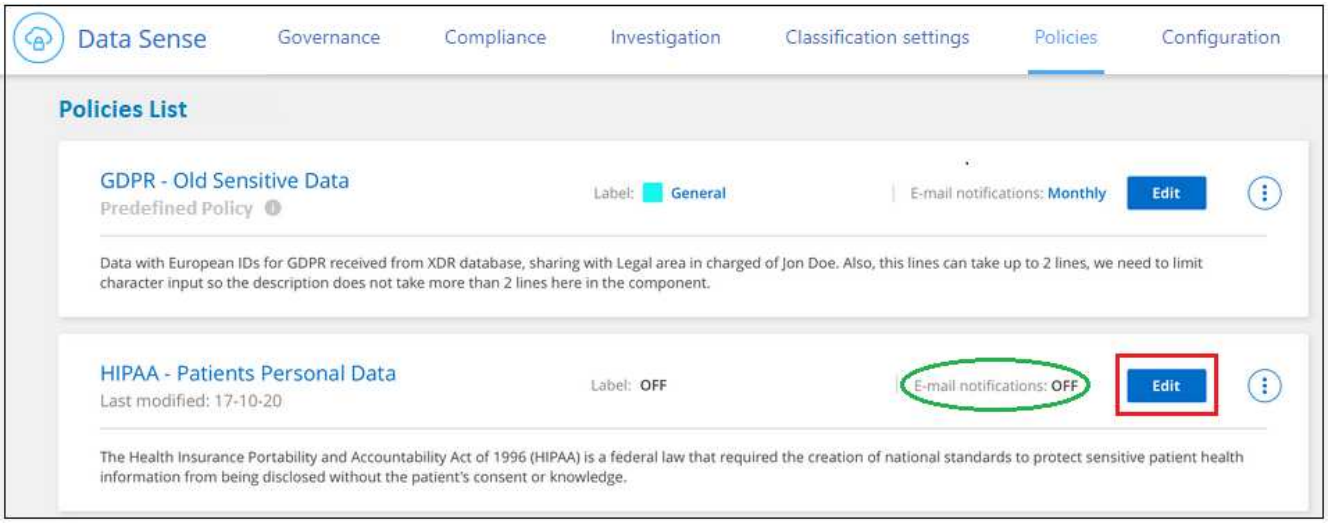
BlueXPの分類では、特定の重要なポリシーで結果が返されたときにアカウントのBlueXPユーザにEメールアラートを送信できるため、データを保護するための通知を受け取ることができます。E メール通知は、日単位、週単位、または月単位で送信することができます。また、BlueXPアカウントではなく、最大20個のメールアドレスに電子メールアラートを送信することもできます。

この設定は、ポリシーの作成時または任意のポリシーの編集時に設定できます。

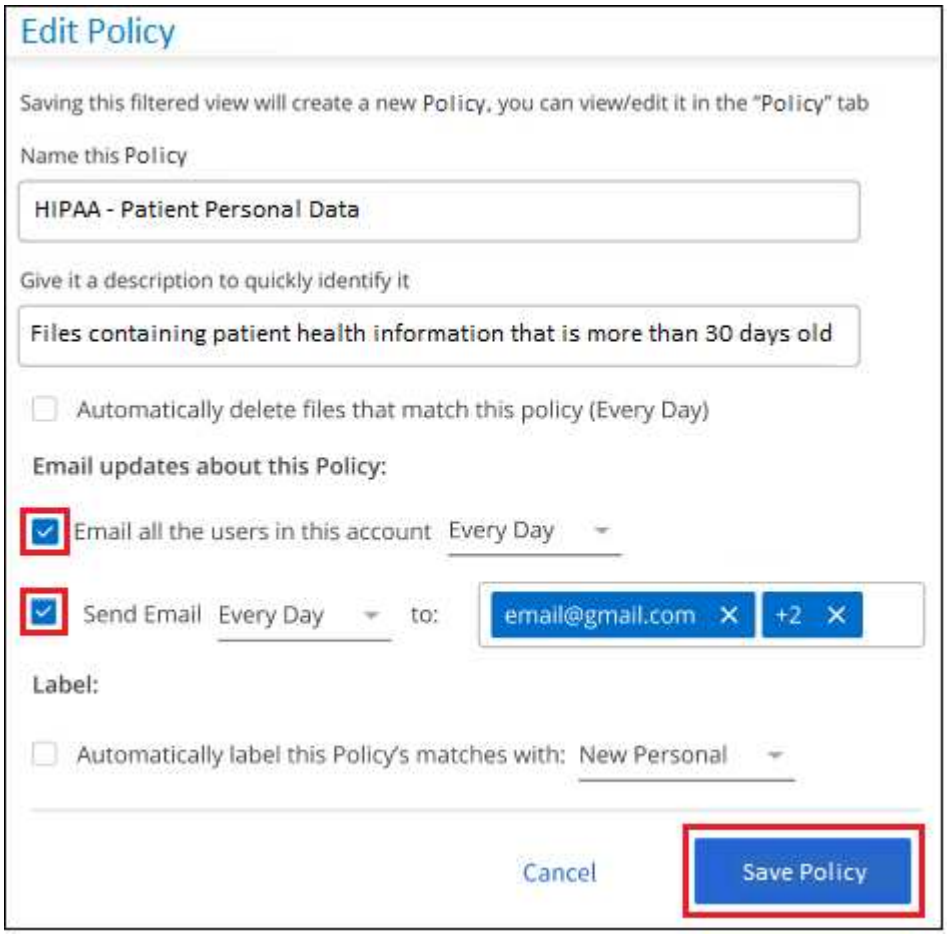
既存のポリシーにメールの更新を追加するには、次の手順を実行します。

手順

1. [ポリシーリスト] ページで、電子メール設定を追加（または変更）するポリシーの [編集 *] をクリックします。



2. Edit Policyページで、次の手順を実行します。
   a. BlueXPアカウントのユーザーに通知メールを送信する場合は、[このアカウントのすべてのユーザーに電子メールを送信する]チェックボックスをオンにし、電子メールの送信間隔を選択します(たとえば、**Every Day**)。
   b. 他のユーザに通知メールを送信する場合は、[電子メールの送信]チェックボックスをオンにし、電子メールを送信する間隔を選択して、最大20個の電子メールアドレスを入力します。



3. ［* ポリシーの保存 *］ をクリックすると、電子メールの送信間隔が ［ ポリシー概要 ］ に表示されます。

結果

最初の電子メールは、ポリシーからの結果がある場合に送信されます。ただし、ポリシーの条件を満たすファイルがある場合に限ります。通知メールに個人情報は送信されません。E メールには、ポリシーの条件に一致するファイルがあり、ポリシーの結果へのリンクが記載されています。

ポリシーを使用したソースファイルの自動削除

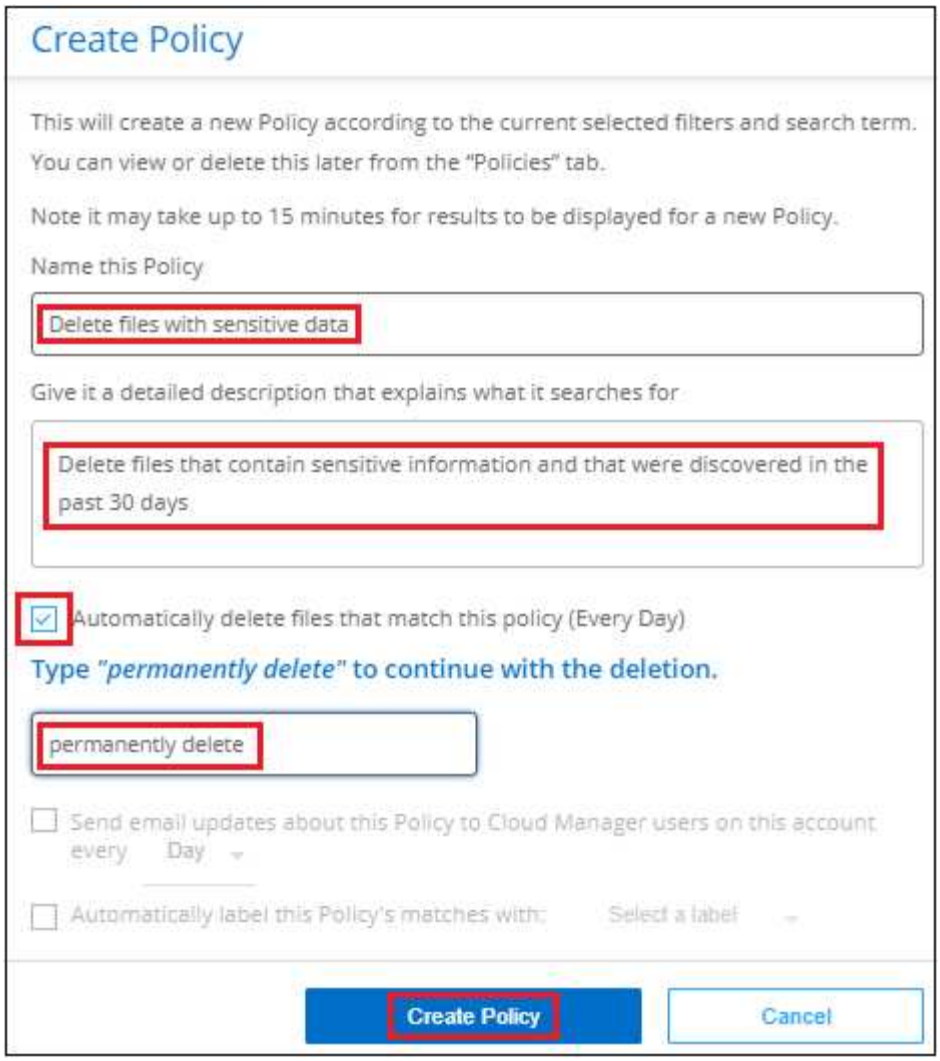
カスタムポリシーを作成して、ポリシーに一致するファイルを削除できます。たとえば、過去30日間にBlueXPの分類によって検出された機密情報を含むファイルを削除できます。

ファイルを自動的に削除するポリシーを作成できるのはアカウント管理者だけです。

ポリシーに一致するすべてのファイルは、 1 日に 1 回完全に削除されます。

手順

1. [データ調査] ページで、使用するすべてのフィルタを選択して検索を定義します。を参照してください "[データ調査 ページでデータをフィルタリングします"^] を参照してください。
2. 必要な方法でフィルタ特性をすべて設定したら、 [この検索からポリシーを作成する *] をクリックします。
3. ポリシーに名前を付け、そのポリシーで実行できるその他のアクションを選択します。
   a. 一意の名前と説明を入力します。
   b. このポリシーに一致するファイルを自動的に削除する] チェックボックスをオンにし、「 * permanently delete * 」と入力して、このポリシーによってファイルが完全に削除されることを確認します。
   c. [ポリシーの作成 *] をクリックします。



結果

[ポリシー] タブに新しいポリシーが表示されます。ポリシーに一致するファイルは、ポリシーの実行時に 1 日に 1 回削除されます。

で削除されたファイルのリストを確認できます "[アクションステータス（ Actions Status ） パネル"]。

ポリシーを使用した**AIP**ラベルの自動割り当て

AIP ラベルは、ポリシーの条件を満たすすべてのファイルに割り当てることができます。ポリシーの作成時に AIP ラベルを指定することも、ポリシーの編集時にラベルを追加することもできます。

BlueXPで分類されたファイルがスキャンされると、ラベルがファイルに追加または更新され続けます。

ラベルがすでにファイルに適用されているかどうか、およびラベルの分類レベルによって、ラベルを変更するときに次のアクションが実行されます。

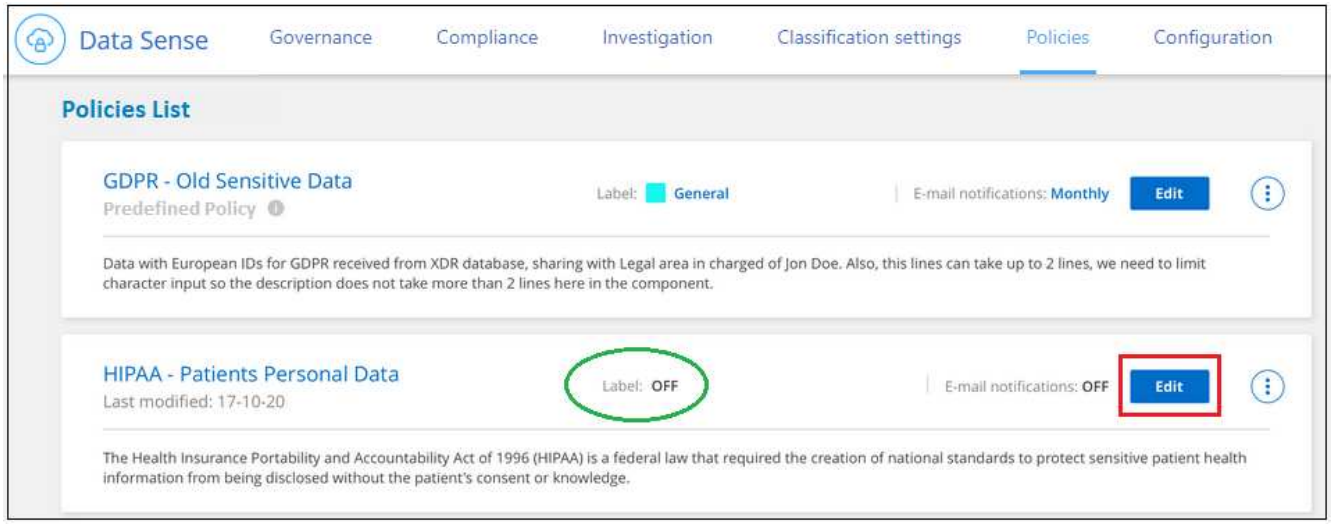
ファイルの内容	作業
にはラベルがありません	ラベルが追加されます
下位レベルの分類の既存のラベルがあります	上位レベルのラベルが追加されます

ファイルの内容	作業
より高いレベルの分類の既存のラベルがあります	上位レベルのラベルが保持されます
手動とポリシーの両方でラベルが割り当てられます	上位レベルのラベルが追加されます
2 つのポリシーによって 2 つの異なるラベルが割り当てられます	上位レベルのラベルが追加されます

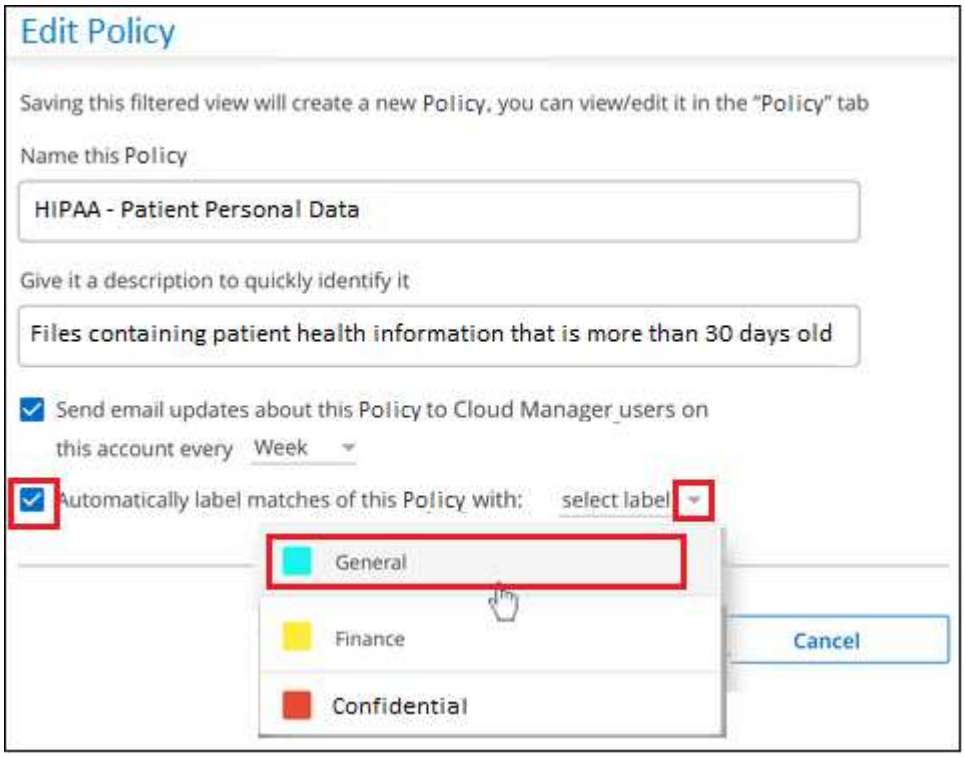
AIP ラベルを既存のポリシーに追加する手順は、次のとおりです。

手順

1. [ポリシーリスト] ページで、 AIP ラベルを追加（または変更）するポリシーの **Edit** をクリックします。



2. [ポリシーの編集] ページで、 [ポリシー] パラメータに一致するファイルの自動ラベルを有効にするチェックボックスをオンにして、ラベル（ **General** など）を選択します。



3. [ポリシーの保存 *] をクリックすると、 [ポリシー概要] にラベルが表示されます。

> ポリシーにラベルが設定されていても、ラベルが AIP から削除されている場合、ラベル名はオフになり、ラベルは割り当てられなくなります。

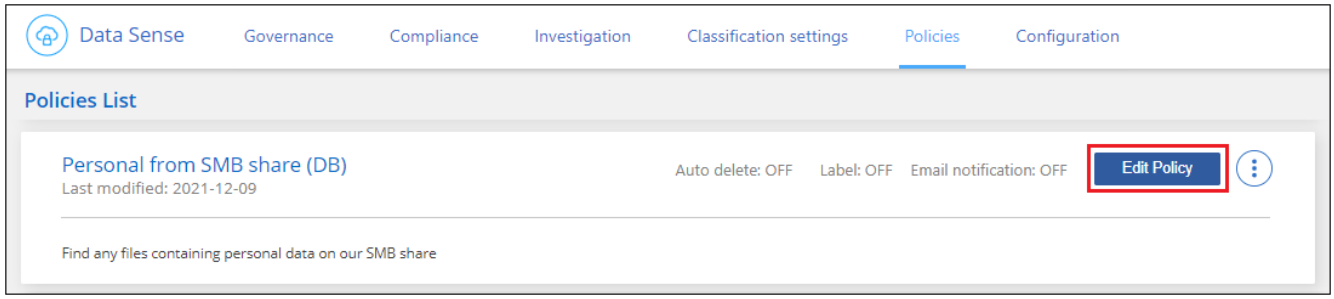
ポリシーの編集

前の手順で作成した既存のポリシーの条件を変更できます。これは、特定のパラメータを追加または削除するためにクエリ（フィルタを使用して定義した項目）を変更する場合に特に便利です。

定義済みポリシーでは、電子メール通知が送信されるかどうか、およびAIPラベルが追加されるかどうかだけを変更できます。その他の値は変更できません。

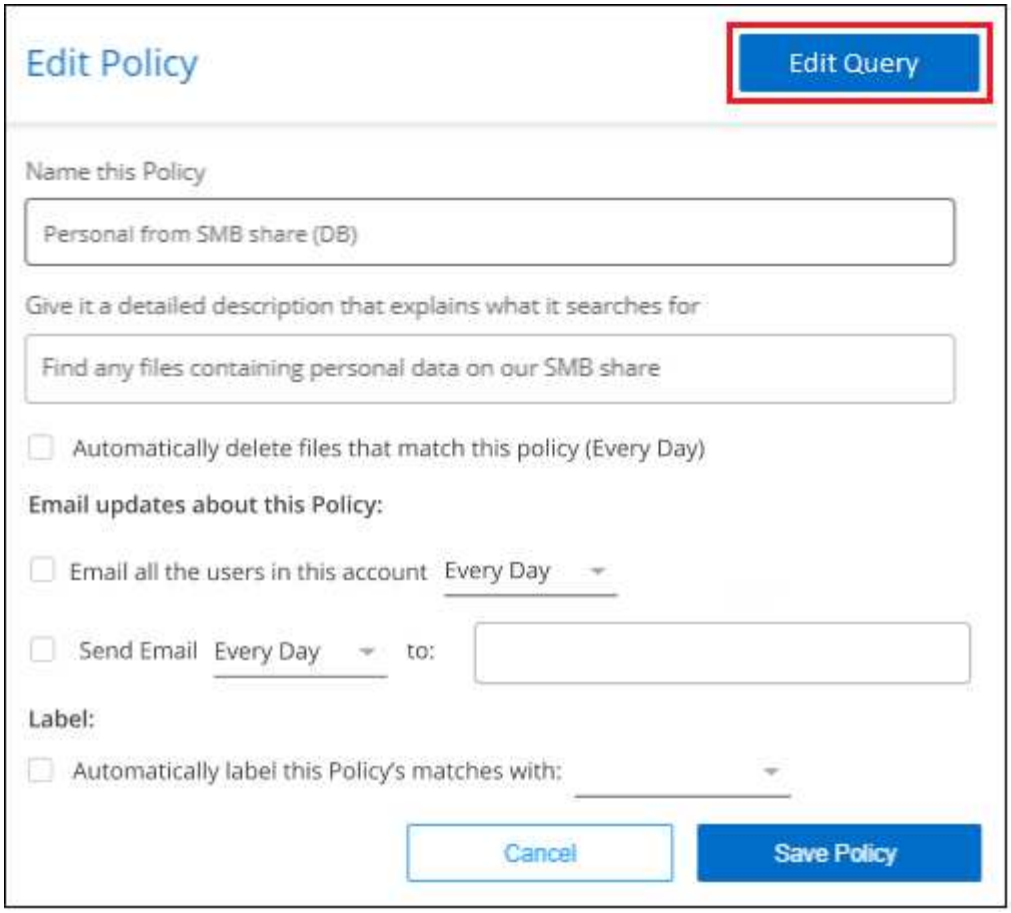
手順

1. [ポリシーリスト]ページで、変更するポリシーの*Edit*をクリックします。



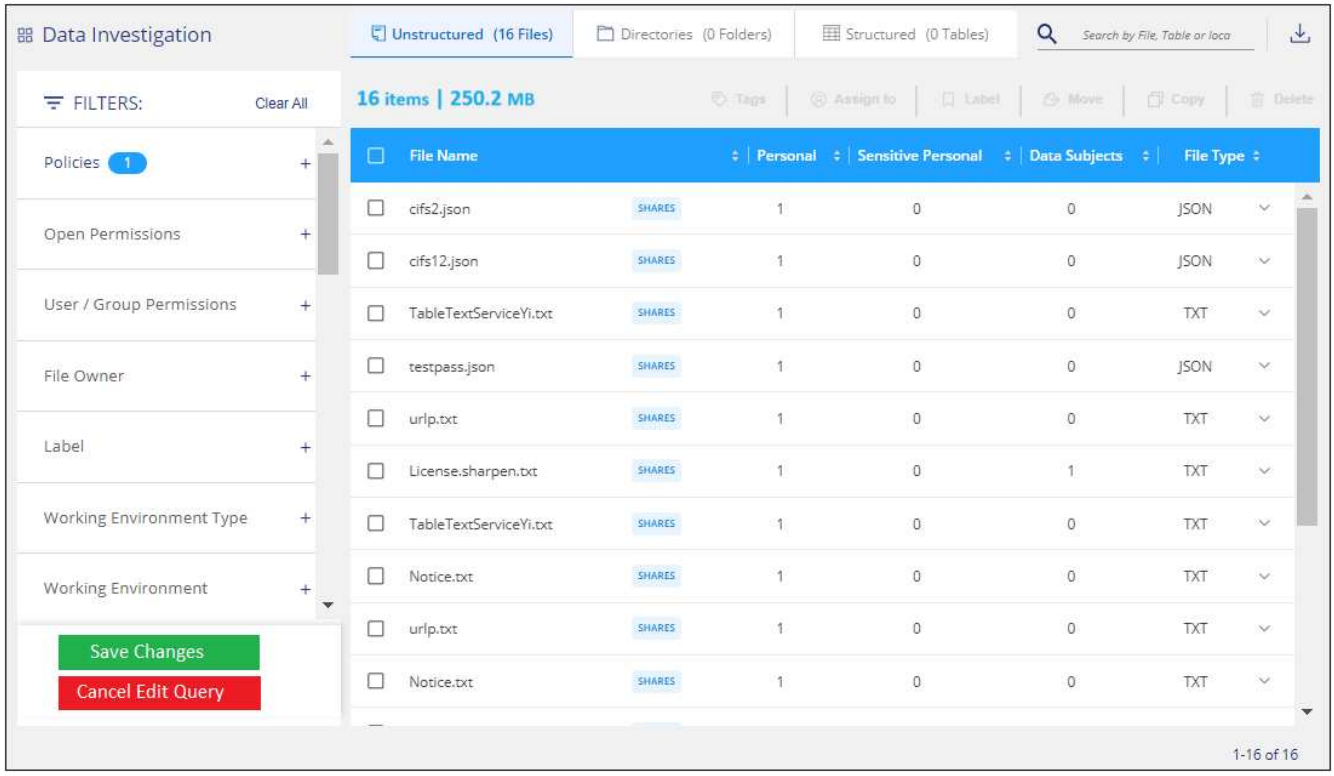
2. このページの項目（名前、概要 、電子メール通知が送信されているかどうか、およびAIPラベルが追加されているかどうか）を変更する場合は、変更を行って*ポリシーの保存*をクリックします。

   保存されたクエリのフィルタを変更する場合は、[クエリの編集]をクリックします。



ページの[クエリの編集]ボタンを選択するスクリーンショット。"]

3. そのクエリーを定義する[調査]ページで、フィルタを追加、削除、またはカスタマイズしてクエリーを編集し、[変更の保存*]をクリックします。



結果

ポリシーはただちに変更されます。そのポリシーに定義されたアクションは、電子メールの送信、AIPラベルの追加、またはファイルの削除のいずれかが、次の内部で実行されます。

ポリシーの削除

作成したカスタムポリシーが不要になった場合は削除できます。事前定義されたポリシーは削除できません。

ポリシーを削除するには、をクリックします ボタン"] ボタンをクリックして特定のポリシーを削除し、確認ダイアログでもう一度 ［ * ポリシーの削除 * ］ をクリックします。

事前定義されたポリシーのリスト

BlueXPは分類され、次のシステム定義のポリシーが提供されます。

名前	説明	ロジック
S3公開プライベートデータ	個人または機密性の高い個人情報を含む S3 オブジェクト。オープンなパブリック読み取りアクセスが許可されます。	S3 Public となり、個人情報または機密情報が含まれます
PCI DSS - 30日間の古いデータ	クレジットカード情報を含むファイル。最終更新日は 30 日前です。	クレジットカードと最終変更日が 30 日以上含まれます
HIPAA：30日間のデータを停滞させます	ヘルス情報が含まれるファイル。最終更新日は 30 日前です。	健康データを含む（ HIPAA レポートと同様に定義されている） そして、最終変更日は 30 日です
プライベートデータ：7年以上前に停滞しています	個人情報または機密性の高い個人情報を含むファイル。最終更新日は 7 年前に変更されました。	個人情報または機密性の高い個人情報を含むファイル。最終更新日は 7 年前に変更されました
GDPR -欧州市民	EU加盟国の市民の5つ以上のIDを含むファイル、またはEU加盟国の市民のIDを含むDBテーブル。	（1）EU市民またはDBテーブルの5つ以上の識別子を含むファイル。列の15%を超える行と、1つの国のEU識別子が含まれています。（欧州諸国のいずれかの国の識別子。ブラジル、カリフォルニア、米国 SSN 、イスラエル、南アフリカを含まない）
CCPA -カリフォルニア州在住	この識別子を持つ10を超えるカリフォルニアドライバのライセンス識別子またはDBテーブルを含むファイル。	カリフォルニアドライバのライセンスIDが10個を超えるファイル、またはカリフォルニアドライバのライセンスを含むDBテーブルが含まれているファイル
データ主体名-高リスク	50 を超えるデータ主体名を持つファイル。	50 を超えるデータ主体名を持つファイル
Eメールアドレス-リスクが高くなっています	E メールアドレスが 50 を超えるファイル、または E メールアドレスを含む行の 50% を超える DB 列	E メールアドレスが 50 を超えるファイル、または E メールアドレスを含む行の 50% を超える DB 列
個人データ-高いリスク	個人データ識別子が 20 個を超えるファイル、または個人データ識別子を含む行の 50% を超える DB 列。	20 以上の個人用のファイル、または個人を含む行の 50% を超える DB 列を持つファイル

名前	説明	ロジック
機密性の高い個人データ-高いリスク	機密性の高い個人データ識別子が 20 を超えるファイル、または機密性の高い個人データを含む行の 50% を超える DB 列。	機密性の高い個人用のファイル、または機密性の高い個人を含む行の 50% 以上を含む DB 列

プライベートデータを管理

BlueXPは、さまざまな方法でプライベートデータを管理できます。一部の機能を使用すると、データの移行準備が簡単になります。また、他の機能を使用してデータを変更することもできます。

- 特定のデータのコピーを作成して別の NFS の場所に移動する場合は、デスティネーションの NFS 共有にファイルをコピーできます。
- ONTAP ボリュームを新しいボリュームにクローニングしたり、選択したファイルだけをソースボリュームから新しいクローンボリュームに含めたりできます。これは、データを移行する際に元のボリュームから特定のファイルを除外する場合に便利です。
- ソースリポジトリから特定の保存先にあるディレクトリにファイルをコピーして同期できます。これは、ソースファイルに対して何らかの最終的なアクティビティが行われている間に、あるソースシステムから別のソースシステムにデータを移行する場合に便利です。
- BlueXP分類でスキャンするソースファイルを任意のNFS共有に移動できます。
- 安全でないようであるか危険すぎると思われるファイルを削除して、ストレージシステムに残すことも、重複として識別したファイルを削除することもできます。

> - このセクションで説明する機能は、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピングのみのスキャンを実行したデータソースでは、ファイルレベルの詳細は表示されません。
> - Google Driveアカウントのデータでは、現時点でこれらの機能を使用することはできません。

ソースファイルをコピーします

BlueXP分類でスキャンしている任意のソースファイルをコピーできます。実行しようとしている処理に応じて、次の 3 種類のコピー処理があります。

- * 同一または異なるボリュームまたはデータソースからデスティネーション NFS 共有にファイル * をコピーします。

  これは、特定のデータのコピーを作成して別の NFS の場所に移動する場合に便利です。

- * ONTAP ボリュームのクローンを同じアグリゲート内の新しいボリュームに作成します。新しいクローンボリュームには、ソースボリュームから選択されたファイルのみを含めます。

  これは、データを移行する際に元のボリュームから特定のファイルを除外する場合に便利です。このアクションではを使用します "NetApp FlexClone" ボリュームをすばやく複製し、 * 選択しなかったファイルを削除する機能。

- * 単一のソースリポジトリ（ ONTAP ボリューム、 S3 バケット、 NFS 共有など）から特定のデスティネーション（ターゲット）にあるディレクトリにファイルをコピーして同期します。

  これは、あるソースシステムから別のシステムにデータを移行する場合に便利です。最初のコピーの後、設定したスケジュールに基づいて変更されたデータが同期されます。このアクションではを使用します "NetApp BlueXPのコピーと同期" データをソースからターゲットにコピーおよび同期する機能。

ソースファイルを**NFS**共有にコピーする

BlueXP分類でスキャンしているソースファイルは、任意のNFS共有にコピーできます。NFS共有をBlueXPに統合する必要はありません。選択したすべてのファイルがコピーされるNFS共有の名前を指定するだけです `<host_name>:/<share_path>`。

データベースに存在するファイルはコピーできません。

要件

- ファイルをコピーするには、アカウント管理者またはワークスペース管理者の役割が必要です。
- ファイルをコピーするには、デスティネーションNFS共有でBlueXP分類インスタンスからのアクセスが許可されている必要があります。
- 一度に1～100,000個のファイルをコピーできます。

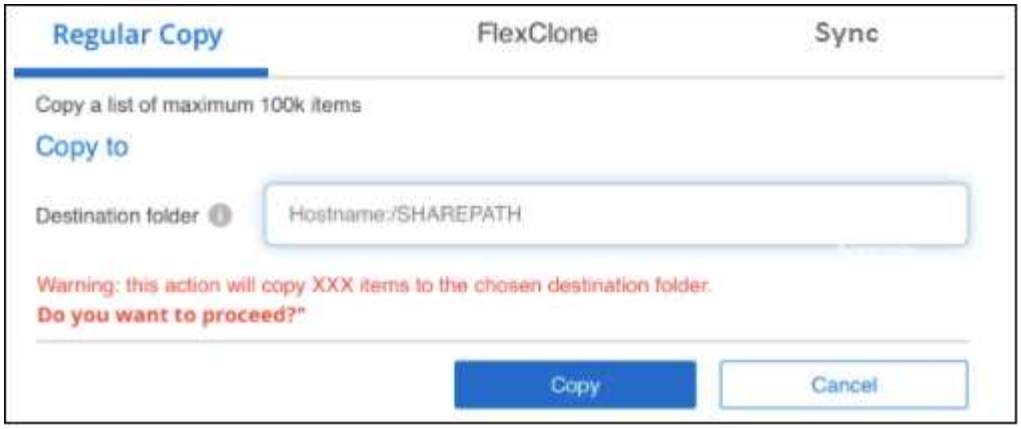
手順

1. [データ調査結果] ペインで、コピーするファイルを選択し、 [* コピー] をクリックします。

ページからコピーするファイルを選択する方法と、 [コピー] ボタンを示すスクリーンショット。"]

   - 個々のファイルを選択するには、各ファイル（ Volume_1）。
   - 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
   - すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

2. _ ファイルのコピー _ ダイアログで * 標準コピー * タブを選択します。



3. 選択したすべてのファイルをコピーする NFS 共有の名前を「 <host_name> ： /<share_path>` 」の形式で入力し、「 * Copy * 」をクリックします。

   コピー処理のステータスを示すダイアログが表示されます。

コピー処理の進捗状況はで確認できます "[アクションステータス（ Actions Status ） パネル"]。

ファイルのメタデータの詳細を表示するときに、個々のファイルをコピーすることもできます。[ファイルのコピー] をクリックします。

ページのファイルのメタデータ詳細から [ファイルのコピー] ボタンを選択したことを示すスクリーンショット。"]

新しいボリュームへのボリュームデータのクローニング

BlueXPでスキャンしている既存のONTAP ボリュームは、netapp_FlexClone_functionalityを使用してクローニングできます。これにより、選択したファイルのみを含めて、ボリュームをすばやく複製できます。この機能は、データを移行する際に元のボリュームから特定のファイルを除外する場合や、テスト用にボリュームのコピーを作成する場合に便利です。

新しいボリュームは、ソースボリュームと同じアグリゲート内に作成されます。このタスクを開始する前に、アグリゲート内にこの新しいボリューム用の十分なスペースがあることを確認してください。必要に応じて、ストレージ管理者にお問い合わせください。

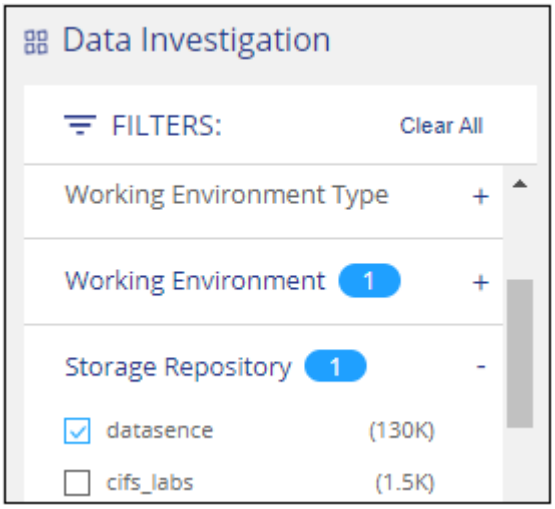
- 注： * FlexGroup ボリュームは FlexClone でサポートされていないため、クローンを作成できません。

要件

- ファイルをコピーするには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 少なくとも20個のファイルを選択する必要があります。
- 選択したファイルはすべて同じボリュームにあり、ボリュームがオンラインである必要があります。
- ボリュームは、 Cloud Volumes ONTAP またはオンプレミスの ONTAP システムから選択する必要があります。他のデータソースは現在サポートされていません。
- クラスタに FlexClone ライセンスがインストールされている必要があります。このライセンスは、 Cloud Volumes ONTAP システムにデフォルトでインストールされます。

手順

1. [データ調査] ペインで、 1 つの * 作業環境 * と 1 つの * ストレージリポジトリ * を選択してフィルタを作成し、すべてのファイルが同じ ONTAP ボリュームにあることを確認します。



新しいボリュームにクローニングするファイルだけが表示されるように、他のフィルタを適用します。

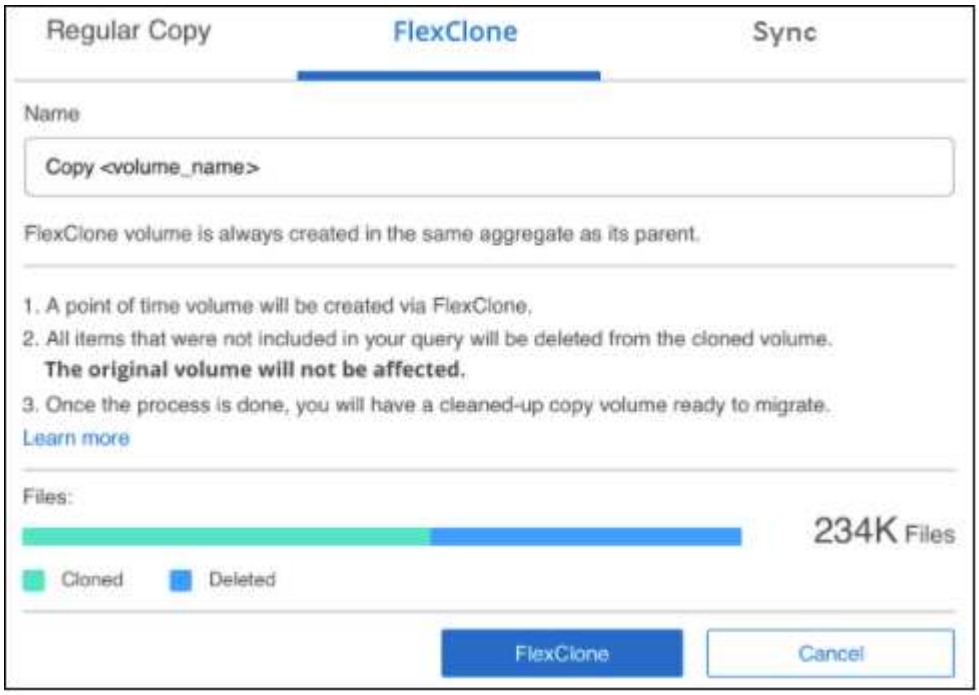
2. ［調査結果］ ペインで、複製するファイルを選択し、 ［* コピー *］ をクリックします。

ページからコピーするファイルを選択する方法と、 [コピー] ボタンを示すスクリーンショット。"]

   - 個々のファイルを選択するには、各ファイル（ Volume_1）。
   - 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
   - すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をク

リックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

3. _ ファイルのコピー _ ダイアログで * FlexClone * タブを選択します。このページには、ボリュームからクローニングされるファイル（選択したファイル）の総数と、クローンボリュームに含まれている / 削除されていないファイル（選択しなかったファイル）の数が表示されます。



4. 新しいボリュームの名前を入力し、 * FlexClone * をクリックします。

   クローン処理のステータスを示すダイアログが表示されます。

結果

新しいクローンボリュームは、ソースボリュームと同じアグリゲート内に作成されます。

クローニング処理の進捗状況はで確認できます "[アクションステータス（ Actions Status ） パネル"]。

ソースボリュームが配置されている作業環境でBlueXPの分類を有効にしたときに最初に*[すべてのボリュームをマッピングして分類]*を選択した場合は、新しいクローンボリュームが自動的にスキャンされます。最初にこれらのいずれかを使用しなかった場合は、この新しいボリュームをスキャンする必要があります "ボリュームのスキャンを手動で有効にします"。

ソースファイルをターゲットシステムにコピーして同期する

BlueXP分類でスキャンしているソースファイルを、サポートされている非構造化データソースから特定のターゲットデスティネーションの場所にあるディレクトリにコピーできます ("BlueXPのコピーと同期でサポートされるターゲットの場所"）。最初のコピー後、ファイル内で変更されたデータは、設定したスケジュールに基づいて同期されます。

これは、あるソースシステムから別のシステムにデータを移行する場合に便利です。このアクションではを使用します "NetApp BlueXPのコピーと同期" データをソースからターゲットにコピーおよび同期する機能。

> データベース、 OneDrive アカウント、 SharePoint アカウントにあるファイルはコピーおよび同期できません。

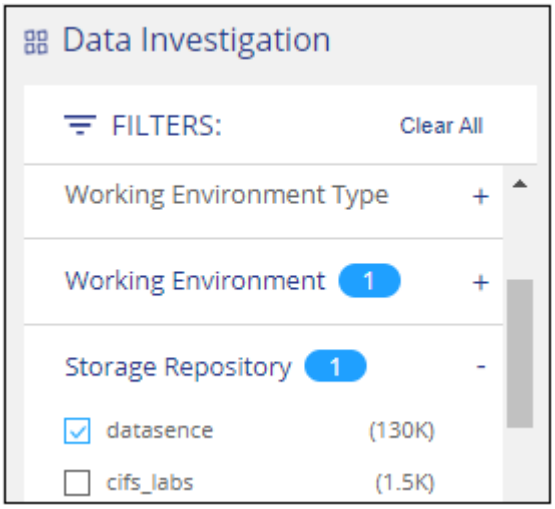
要件

- ファイルをコピーして同期するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 少なくとも20個のファイルを選択する必要があります。
- 選択したファイルはすべて、同じソースリポジトリ（ ONTAP ボリューム、 S3 バケット、 NFS 共有、 CIFS 共有など）にある必要があります。
- BlueXPのコピーおよび同期サービスをアクティブ化し、ソースシステムとターゲットシステム間でファイルを転送するためのデータブローカーを少なくとも1つ設定する必要があります。から、BlueXPのコピーと同期の要件を確認します "Quick Start 概要 の略"。

  BlueXPのコピーおよび同期サービスでは、同期関係ごとにサービス料金が別途発生します。データブローカーをクラウドに導入した場合はリソース料金が発生します。

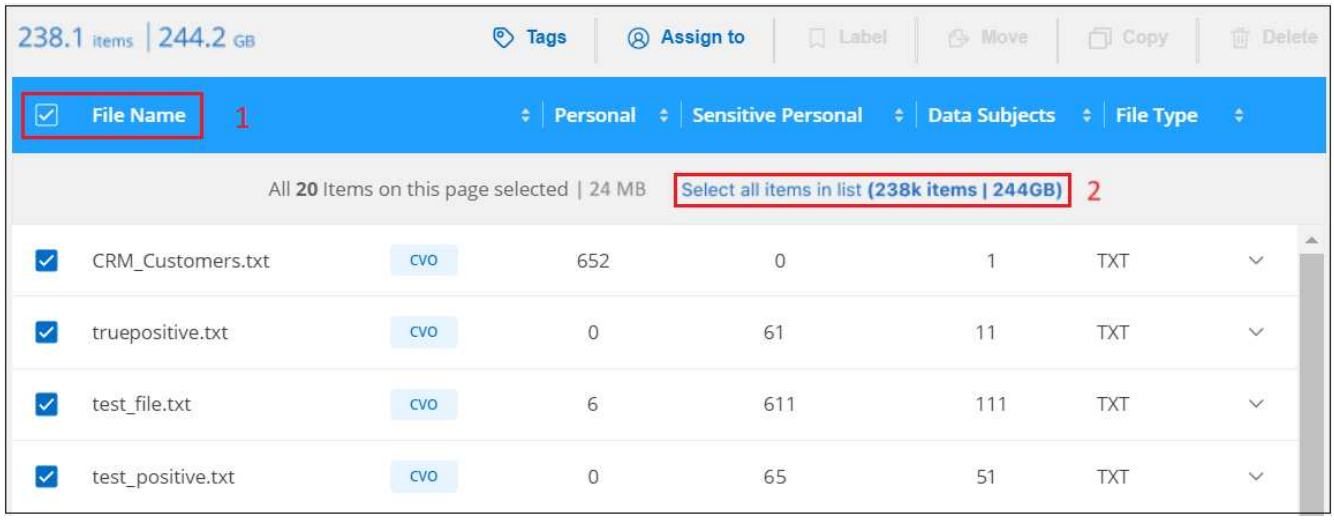
手順

1. [データの調査] ペインで、 1 つの * 作業環境 * と 1 つの * ストレージリポジトリ * を選択してフィルタを作成し、すべてのファイルが同じリポジトリにあることを確認します。



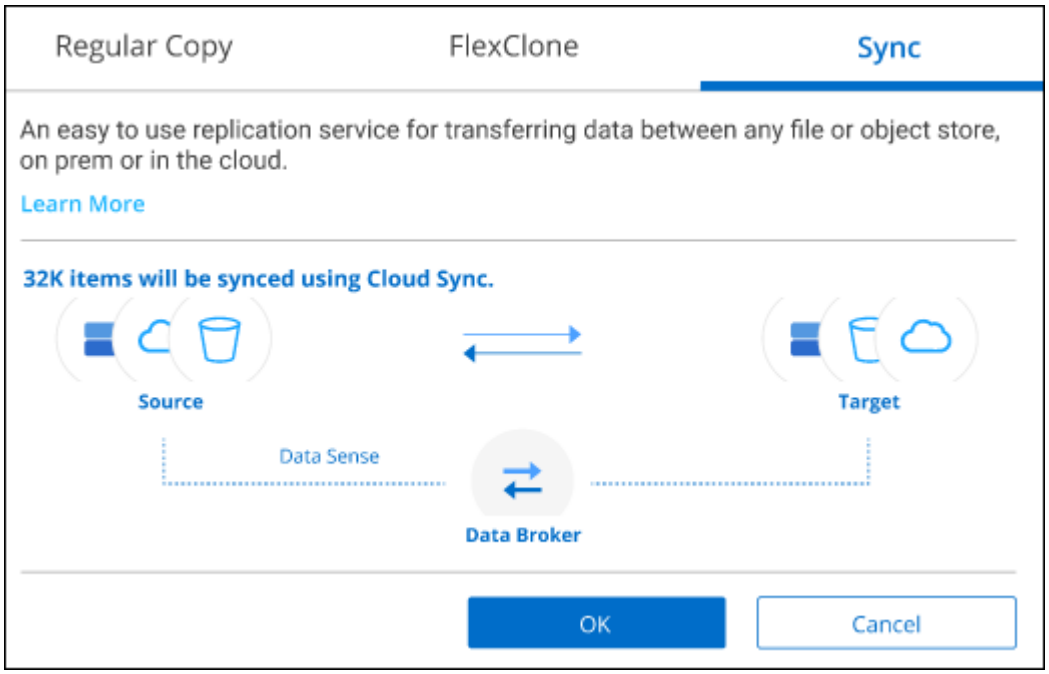
   他のフィルタを適用して、コピー先システムに同期するファイルだけが表示されるようにします。

2. [調査結果] ウィンドウ枠で、タイトル行のボックスをオンにして、すべてのページのすべてのファイルを選択します（ File Name ）をクリックし、ポップアップメッセージに入力します All 20 Items on this page selected Select all Items in list (63K Items) [リスト内のすべての項目を選択（ * xxx 項目）] をクリックし、 [* コピー *] をクリックします。



ページからコピーするファイルを選択する方法と、 [コピー] ボタンを示すスクリーンショット。"]

3. _ ファイルのコピー _ ダイアログで * 同期 * タブを選択します。



ダイアログを示すスクリーンショットで、 [同期] オプションを選択できます。"]

4. 選択したファイルを保存先に同期してもよい場合は、「 * OK * 」をクリックします。

   BlueXPのコピーと同期のUIがBlueXPで開きます。

   同期関係を定義するよう求められます。ソースシステムには、BlueXPの分類で選択したリポジトリとファイルがあらかじめ設定されています。

5. ターゲットシステムを選択し、使用するデータブローカーを選択（または作成）する必要があります。から、BlueXPのコピーと同期の要件を確認します "Quick Start 概要 の略"。

結果

ファイルはターゲットシステムにコピーされ、定義したスケジュールに基づいて同期されます。1 回限りの同期を選択した場合、ファイルは 1 回だけコピーされ、同期されます。定期的な同期を選択した場合は、スケ

ジュールに基づいてファイルが同期されます。フィルタを使用して作成したクエリに一致する新しいファイルがソースシステムによって追加されると、これらの _new_files がコピー先にコピーされ、後で同期されることに注意してください。

BlueXPの分類から起動すると、通常のBlueXPのコピー処理と同期処理の一部が無効になることに注意してください。

- 「ソース上のファイルを削除」または「ターゲット上のファイルを削除」ボタンは使用できません。
- レポートの実行が無効になっています。

ソースファイルを**NFS**共有に移動する

BlueXP分類でスキャンするソースファイルを任意のNFS共有に移動できます。NFS共有をBlueXPの分類と統合する必要はありません。

必要に応じて、移動したファイルの場所にブレッドクラムファイルを残すことができます。ブレッドクラムファイルは、ファイルが元の場所から移動された理由をユーザーが理解するのに役立ちます。移動された各ファイルについて、システムは「<filename>-ブレッドクラム-<date>.txt」という名前のソース位置にブレッドクラムファイルを作成します。ダイアログボックスで、ブレッドクラムファイルに追加されるテキストを追加して、ファイルが移動された場所とファイルを移動したユーザを示すことができます。

ソースファイルのサブディレクトリ構造は、ファイルの移動時に移動先の共有に再作成されるため、ファイルの移動元がわかりやすくなります。同じ名前のファイルがコピー先に存在する場合、そのファイルは移動されません。

データベースに存在するファイルは移動できません。

要件

- ファイルを移動するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- ソースファイルは、オンプレミスのONTAP 、Cloud Volumes ONTAP 、Azure NetApp Files 、ファイル共有、SharePoint Onlineのデータソースに配置できます。
- 一度に移動できるファイルの最大数は1、500万です。
- 50 MB以下のファイルのみが移動されます。
- デスティネーションNFS共有で、BlueXP分類インスタンスのIPアドレスからのアクセスを許可する必要があります。

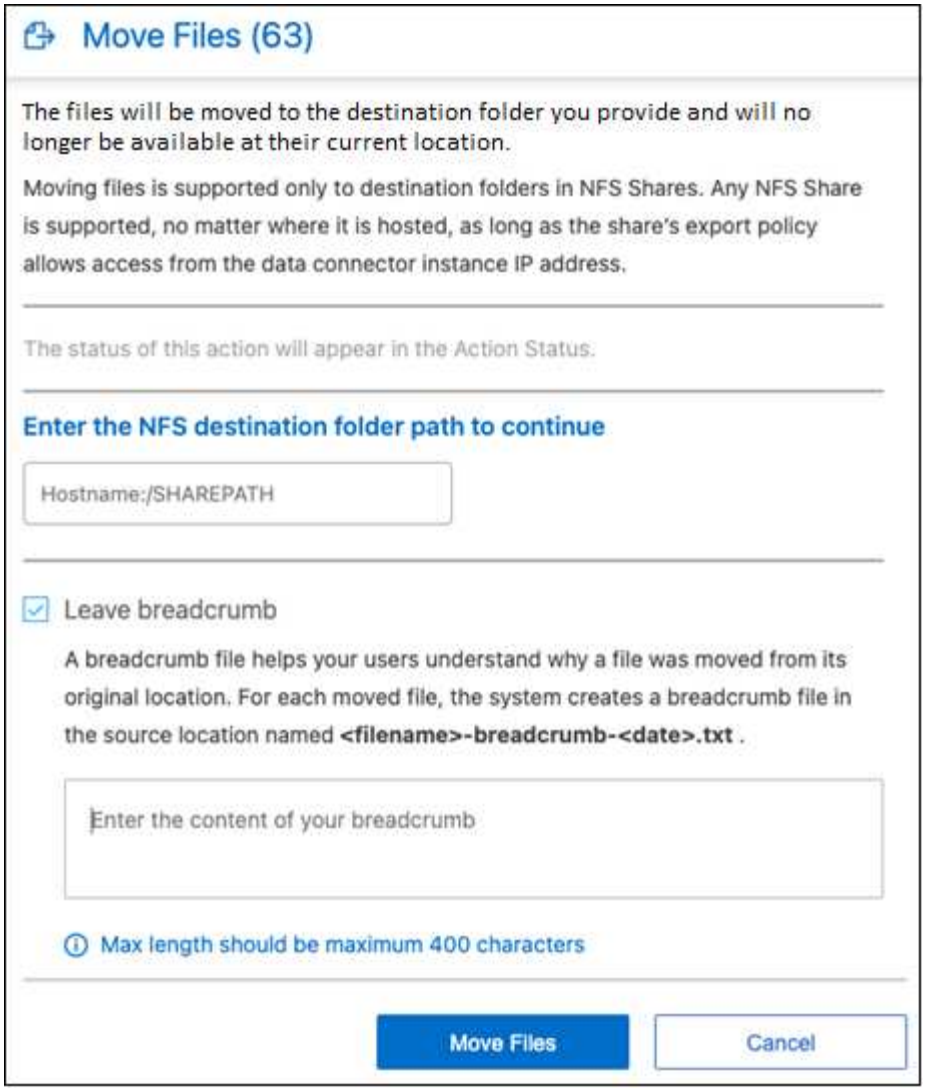
手順

1. [データ調査結果] ペインで、移動するファイルを選択します。

ページから [移動] ボタンをクリックします。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
- すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

2. ボタンバーで、 * 移動 * をクリックします。



3. _Move Files_Dialogに、選択したすべてのファイルを移動するNFS共有の名前を「<host_name>：/<share_path>`」の形式で入力します。
4. ブレッドクラムファイルを残す場合は、_ブレッドクラム履歴_ボックスをオンにします。ダイアログボックスにテキストを入力して、ファイルが移動された場所、ファイルを移動したユーザー、およびファイルが移動された理由などのその他の情報を指定できます。
5. 「ファイルの移動」をクリックします。

ファイルのメタデータの詳細を表示するときに、個々のファイルを移動することもできます。「 * ファイルを移動 * 」をクリックします。

ページのファイルのメタデータ詳細から [ファイルの移動] ボタンを選択したことを示すスクリーンショット。"]

ソースファイルを削除します

ストレージ・システムに残すのに安全でない ' またはリスクが高すぎるソース・ファイルを完全に削除したり ' 重複として識別したソース・ファイルを削除したりすることができますこの操作は永続的であり、元に戻すことも復元することもできません。

［調査］ペインから手動でファイルを削除することも、手動でファイルを削除することもできます "ポリシーを使用して自動的に作成"。

> データベースに存在するファイルは削除できません。その他のすべてのデータソースがサポートされます。

ファイルを削除するには、次の権限が必要です。

- NFSデータの場合-書き込み権限でエクスポートポリシーを定義する必要があります。
- CIFSデータの場合- CIFSクレデンシャルに書き込み権限が必要です。
- S3 データの場合 - IAM ロールに次の権限を含める必要があります。「 3 ： DeleteObject 」

ソースファイルを手動で削除する

要件

- ファイルを削除するには、アカウント管理者またはワークスペース管理者の役割が必要です。
- 一度に削除できるファイルの最大数は 100 、 000 です。

手順

1. [データ調査結果] ペインで、削除するファイルを選択します。

ページの [削除] ボタン。"]

- 個々のファイルを選択するには、各ファイル（ Volume_1）。
- 現在のページのすべてのファイルを選択するには、タイトル行（ File Name ）。
- すべてのページのすべてのファイルを選択するには、タイトル行（ File Name ）をクリックし、ポップアップメッセージにと入力します All 20 Items on this page selected Select all Items in list (63K Items)をクリックし、リスト（ xxx 項目）のすべての項目を選択 * をクリックします。

2. ボタンバーで、 * 削除 * をクリックします。
3. 削除操作は永続的であるため ' 後続の _Delete File_Dialog に「 * permanently delete * 」と入力し ' * ファイルの削除 * をクリックする必要があります

削除処理の進捗状況はで確認できます "[アクションステータス（ Actions Status ） パネル"]。

ファイルのメタデータの詳細を表示するときに、個々のファイルを削除することもできます。[ファイルの削除] をクリックします。

ページのファイルのメタデータ詳細から [ファイルの削除] ボタンを選択したことを示すスクリーンショット。"]

コンプライアンスレポートを表示する

BlueXPの分類では、組織のデータプライバシープログラムのステータスを詳しく把握するために使用できるレポートが提供されます。

BlueXPの分類ダッシュボードには、デフォルトで、すべての作業環境、データベース、データソースのコン

プライアンスとガバナンスのデータが表示されます。一部の作業環境のデータのみを含むレポートを表示する場合は、 それらの作業環境を選択します。

- このセクションで説明するレポートは、データソースに対して完全な分類スキャンを実行することを選択した場合にのみ使用できます。マッピング専用スキャンを実行したデータソースでは、データマッピングレポートのみが生成されます。
- ネットアップは、BlueXPの分類によって特定される個人データや機密性の高い個人データの正確性を100%保証することはできません。必ずデータを確認して情報を検証してください。

プライバシーリスク評価レポート

プライバシーリスクアセスメントレポートには、GDPRやCCPAなどのプライバシー規制に必要な、組織のプライバシーリスクステータスの概要が記載されています。このレポートには次の情報が含まれます。

準拠ステータス

A 重要度スコア 機密性、個人、機密性の高い個人のいずれであっても、データの配信は可能です。

評価の概要

検出された個人データの種類とデータのカテゴリの内訳。

この評価のデータ主体

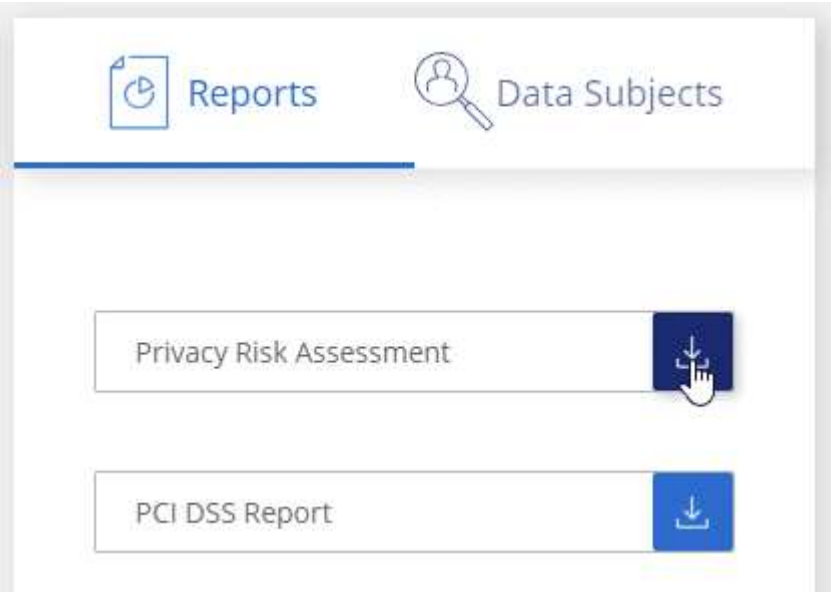
国 ID が見つかった場所別の人の数。

プライバシーリスクアセスメントレポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. **[Compliance]** をクリックし、 **[*Reports]** の下にある **[*Privacy Risk Assessment]** の横にあるダウンロードアイコンをクリックします。



タブのスクリーンショット。[レポート]

ペインに、[プライバシーリスクアセスメント]をクリックできることが示されています。"]

結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

重要度スコア

BlueXPの分類では、プライバシーリスク評価レポートの重大度スコアが、次の3つの変数に基づいて計算されます。

- すべてのデータの個人データの割合。
- すべてのデータの機密性の高い個人データの割合。
- データ主体を含むファイルの割合。国 ID 、社会保障番号、税務 ID 番号などの国 ID によって決定されます。

スコアの決定に使用されるロジックは次のとおりです。

重要度スコア	ロジック
0	3 つの変数はすべて 0% です
1.	変数の 1 つが 0% を超えています
2.	変数の 1 つが 3% を超えています
3.	2 つの変数が 3% を超えています
4.	3 つの変数が 3% を超えています
5.	変数の 1 つが 6% を超えています
6.	2 つの変数が 6% を超えています
7.	3 つの変数が 6% を超えています
8.	変数の 1 つが 15% を超えています
9.	2 つの変数が 15% を超えています
10.	3 つの変数が 15% を超えています

PCI DSS レポート

Payment Card Industry Data Security Standard （ PCI DSS ） Report は、クレジットカード情報のファイルへの配布を識別するのに役立ちます。このレポートには次の情報が含まれます。

概要

クレジットカード情報を含むファイル数と、作業環境。

暗号化

暗号化された作業環境または暗号化されていない作業環境にあるクレジットカード情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

ランサムウェアからの保護

ランサムウェアからの保護が有効になっている、または有効になっていない作業環境でのクレジットカード情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

保持

ファイルが最後に変更された期間。これは、クレジットカード情報を処理するよりも長く保持する必要がないために役立ちます。

クレジットカード情報の配布

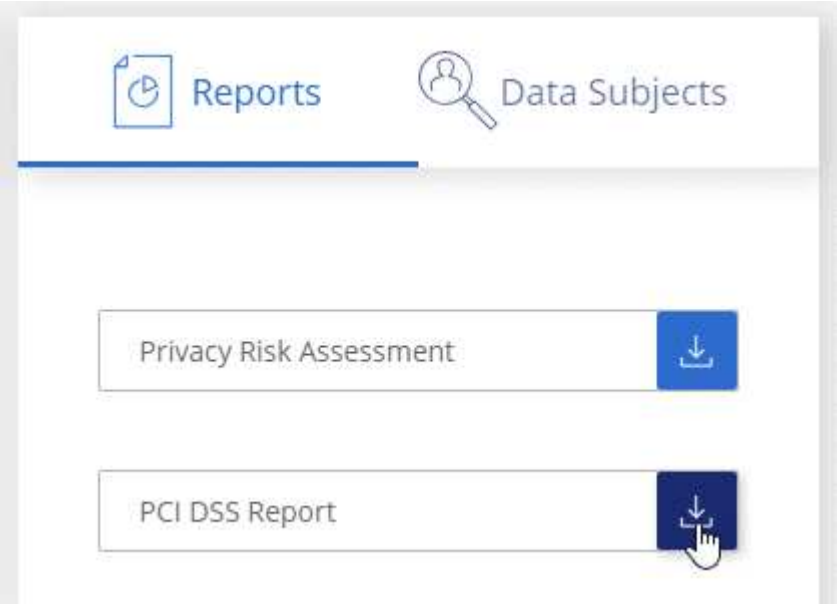
クレジットカード情報が見つかった作業環境、および暗号化とランサムウェアによる保護が有効になっているかどうか。

PCI DSSレポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. [* コンプライアンス *] をクリックし、 [* レポート] の下の [* PCI DSS レポート *] の横にあるダウンロード・アイコンをクリックします。



タブのスクリーンショット。[レポート]ペインに、[プライバシーリスクアセスメント]をクリックできることが示されています。"]

結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

HIPAA レポート

Health Insurance Portability and Accountability Act （ HIPAA ：医療保険の携行性と責任に関する法律）レポートは、健康に関する情報を含むファイルを特定するのに役立ちます。HIPAAデータプライバシー法を遵守するという組織の要件を支援するように設計されています。BlueXPの分類では、次のような情報が検索されます。

- ヘルス参照パターン
- ICD-10-CM 医療コード
- ICD-9-CM 医療コード
- HR -健全性カテゴリ
- ヘルスアプリケーションデータカテゴリ

このレポートには次の情報が含まれます。

概要

ヘルス情報が含まれているファイルの数と、作業環境。

暗号化

暗号化された作業環境または暗号化されていない作業環境にあるヘルス情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

ランサムウェアからの保護

ランサムウェアからの保護が有効になっている、または有効になっていない作業環境でのヘルス情報を含むファイルの割合。この情報は Cloud Volumes ONTAP に固有のものです。

保持

ファイルが最後に変更された期間。健常性の情報は、処理するまでに時間がかかることがないため、この方法が便利です。

健康情報の配布

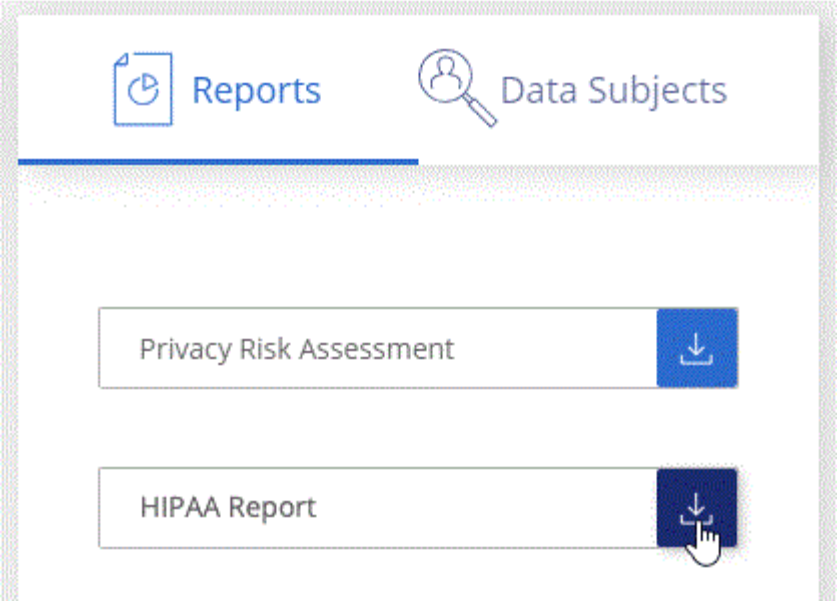
健常性の情報が見つかった作業環境、および暗号化とランサムウェアによる保護が有効になっているかどうか。

HIPAAレポートの生成

コンプライアンスタブに移動してレポートを生成します。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. [**Compliance]** をクリックし、 **[*Reports**] の下にある [**HIPAA Report**] の横にあるダウンロードアイコンをクリックします。



結果

BlueXPの分類によってPDFレポートが生成されます。このレポートを確認して、必要に応じて他のグループに送信できます。

データ主体アクセス要求とは

欧州 GDPR などのプライバシー規制により、データ主体（お客様や従業員など）は個人データにアクセスする権利が付与されます。データ主体がこの情報を要求すると ' これは dsar (データ主体アクセス要求) と呼ばれます組織は、これらの要求に「期日前に」、受領後 1 か月以内に対応する必要があります。

dsarに応答するには、件名のフルネームまたは既知の識別子(電子メールアドレスなど)を検索し、レポートをダウンロードします。このレポートは、企業が GDPR や同様のデータプライバシー法を遵守する必要がある場合に役立つように作成されています。

BlueXPの分類は**DSAR**への対応にどのように役立ちますか？

データ主体の検索を実行すると、BlueXPの分類によって、そのユーザの名前または識別子が含まれているファイル、バケット、OneDrive、SharePointアカウントがすべて検出されます。BlueXPの分類では、インデックスが事前に設定された最新のデータで名前や識別子がチェックされます。新しいスキャンは開始されません。

検索が完了したら、 Data Subject Access Request レポートのファイルリストをダウンロードできます。このレポートでは、データから得た情報を集約して、利用者に返すことができる法的条件にします。

> 現時点では、データベース内でのデータの件名検索はサポートされていません。

データ主体の検索とレポートのダウンロード

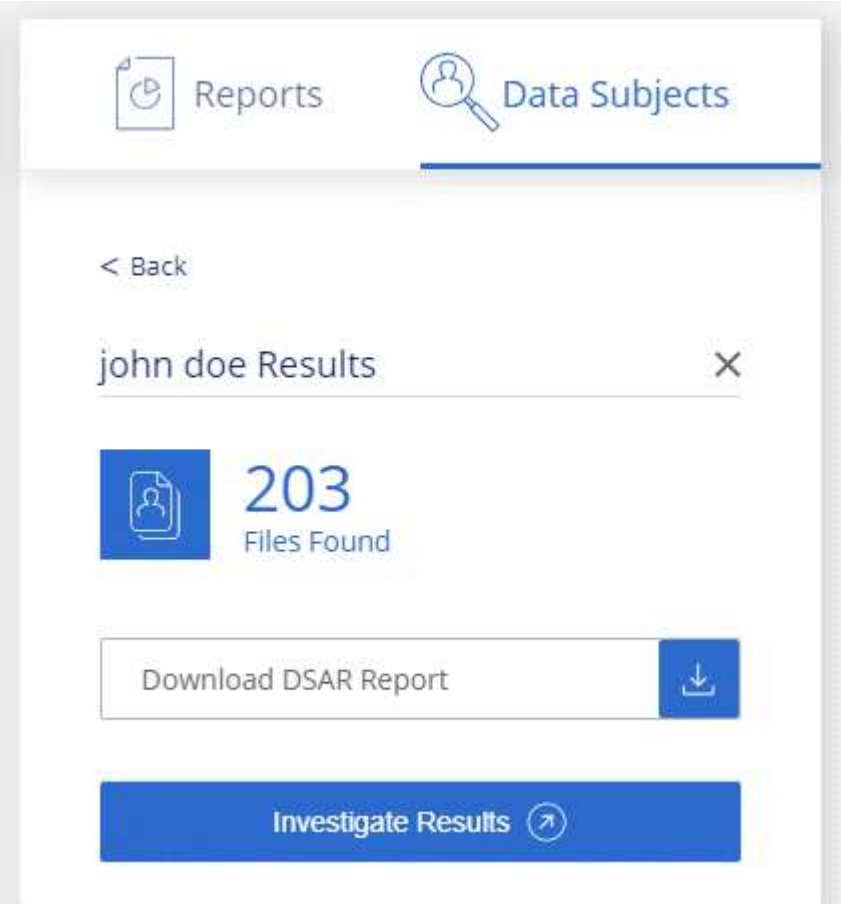
データ主体のフルネームまたは既知の識別子を検索し、ファイルリストレポートまたは dsar レポートをダウンロードします。で検索できます "個人情報の種類"。

> データ主体の名前を検索する際には、英語、ドイツ語、日本語、スペイン語がサポートされています。言語のサポートは、あとで追加されます。

手順

1. BlueXPメニューで、* Governance > Classification *をクリックします。
2. [* データ主体 *] をクリックします。
3. データ主体のフルネームまたは既知の識別子を検索します

   次の例では、 name *John doe*: を検索しています。



4. 次のいずれかのオプションを選択します。
   - **Download dsar Report**: アクセス要求に対する正式な応答で、データ主体に送信できます。このレポートには、対象データについてBlueXPで分類されたデータに基づいて自動的に生成される情報が含まれ、テンプレートとして使用できるように設計されています。データ主体に送信する前に、フォームに必要事項を記入して内部で確認してください。
   - * 調査結果 * ：特定のファイルの検索、ソート、詳細の展開、およびファイルリストのダウンロードによってデータを調査できるページ。

     10 、 000 件を超える結果がある場合は、ファイルリストに上位 10 、 000 件のみが表示されます。

レポートの作業環境を選択

BlueXPの分類[Compliance]ダッシュボードの内容をフィルタリングして、すべての作業環境とデータベース、または特定の作業環境のコンプライアンスデータを表示できます。

ダッシュボードをフィルタすると、BlueXPの分類によって、選択した作業環境のみに準拠データとレポートの範囲が限定されます。

手順

1. フィルタドロップダウンをクリックし、データを表示する作業環境を選択して、 * 表示 * をクリックします。