



組織に保存されているデータのコンプライアンスの詳細を表示する

Cloud Manager

Tom Onacki
May 06, 2021

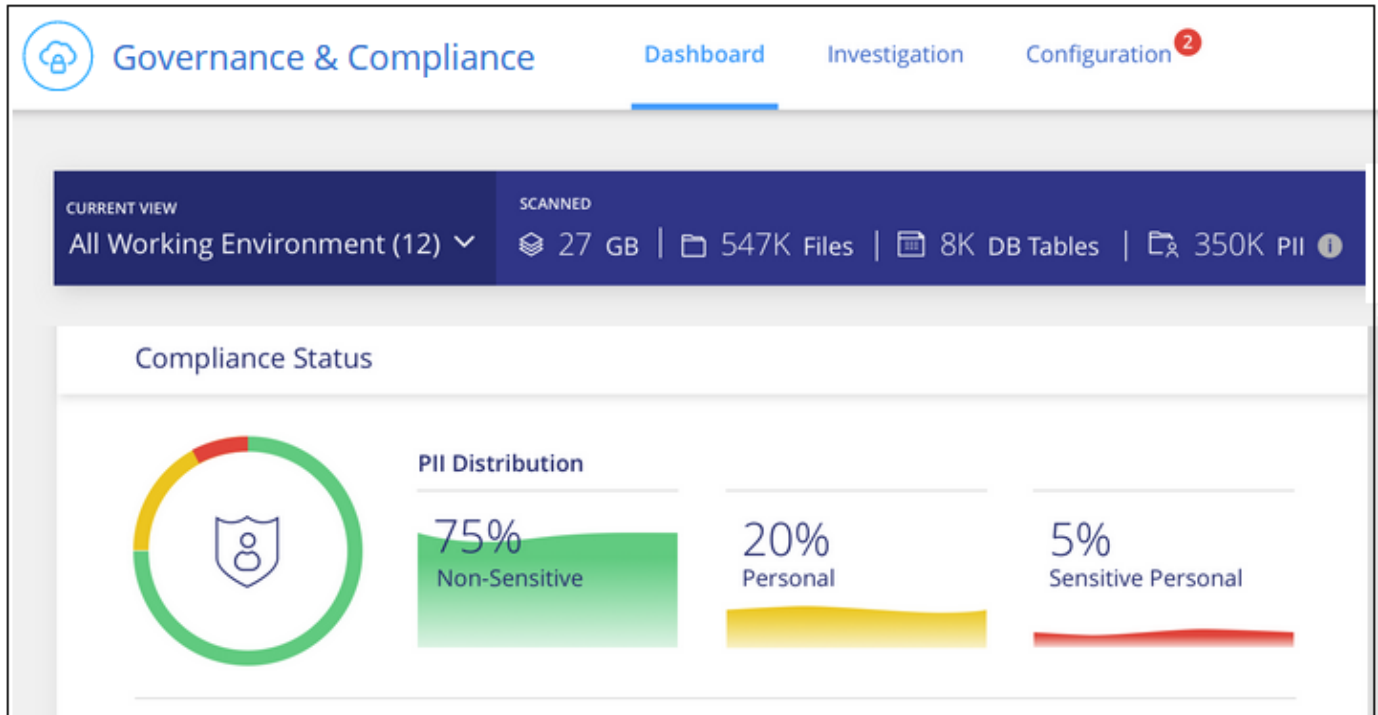
目次

組織に保存されているデータのコンプライアンスの詳細を表示する	1
個人データ	1
機密性の高い個人データ	4
カテゴリ	5
ファイルの種類	6
ファイルメタデータを表示しています	7
特定の作業環境のダッシュボードデータの表示	10
[データ調査] ページでデータをフィルタリングします	11
各ファイルリストレポート (CSV ファイル) に含まれる内容	12

組織に保存されているデータの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。また、データに含まれる Cloud Compliance のカテゴリとファイルタイプを確認して、情報を可視化することもできます。

デフォルトでは、Cloud Compliance 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

Cloud Compliance は、データ内の特定の単語、文字列、パターン（Regex）を自動的に識別します。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、銀行口座番号などです。 ["すべてのリストを参照してください"](#)。

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。

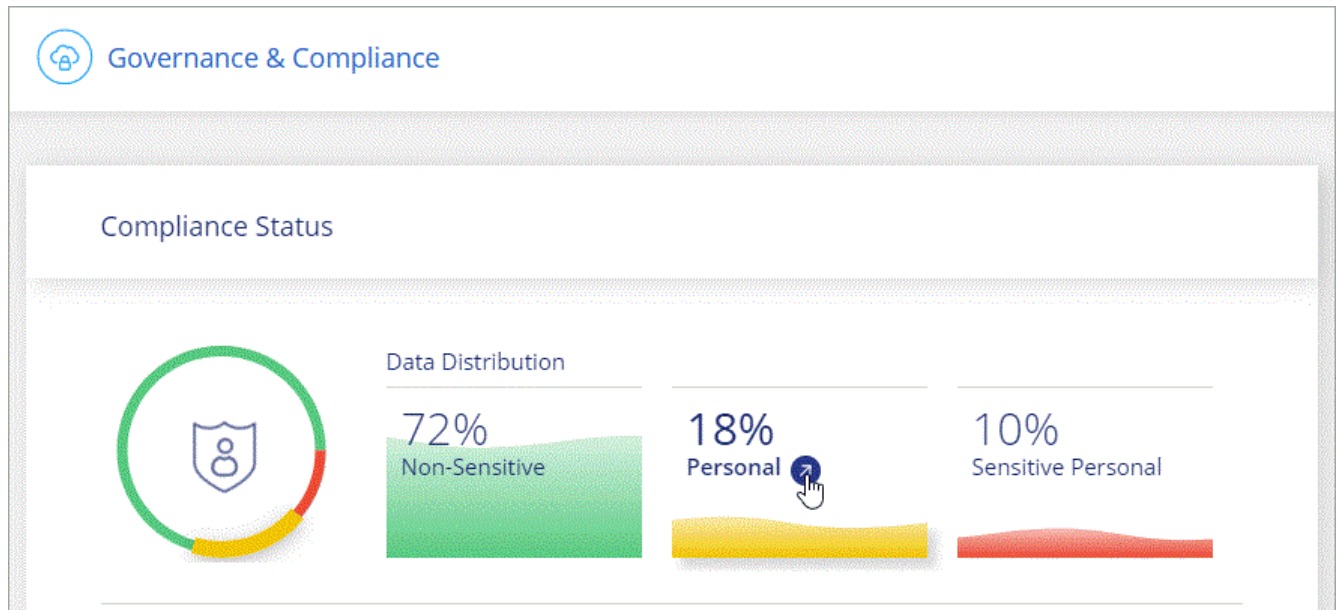
一部のタイプの個人データについては、Cloud Compliance は 近接性検証 を使用してその結果を検証します。検証は、見つかった個人データに近接した 1 つまたは複数の定義済みキーワードを検索することによ

て行われます。たとえば、 Cloud Compliance は米国を識別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" Cloud Compliance がプロキシミティ検証を使用する状況を示します。

個人データを含むファイルを表示する

手順

1. Cloud Manager の上部で、 * コンプライアンス * をクリックし、 * ダッシュボード * 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。

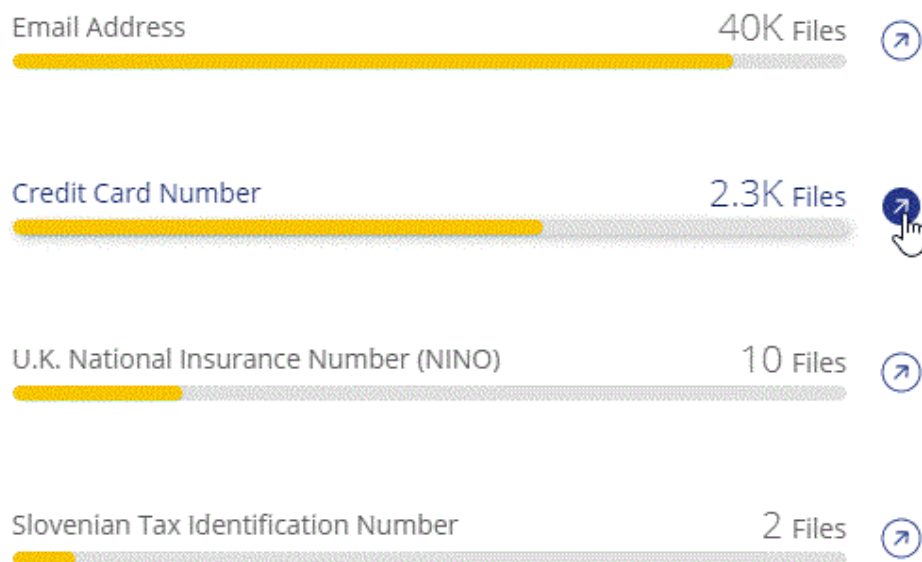


3. 特定の種類の個人データの詳細を調べるには、 [* すべて表示 *] をクリックし、 特定の種類の個人データの [結果の調査 *] アイコンをクリックします。

< Back

Personal Files

7 Types | 41.1K Files



- 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。

Dashboard investigation for 'Credit Card Number'

3.9K files found in All working environments

Search:

File Name ↑↓	Personal	Sensitive Personal	Data Subjects	File Type ↑↓
customer-data.xls	1K	0	63	XLS

[Investigate Results](#)

- Working Environment: Amazon S3
- Storage Repository: compliancedemofiles
- File Path: /Patterns/NEW SSN
- Category: Miscellaneous
- File Size: 142.35 KB
- Last Modified: 2019-12-16 12:18

機密性の高い個人データ

Cloud Compliance は、などのプライバシー規制に従って、機密性の高い特別な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"](#)。

Cloud Compliance 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それに応じて分類します。

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。クラウドコンプライアンスは、 NLP の能力を備えているため、「ジョージ・メキシカン」（ GDPR の第 9 条で規定されている機密データを示す ） と「ジョージ・イメキシカン・フード」を読み取る文との違いを区別できます。

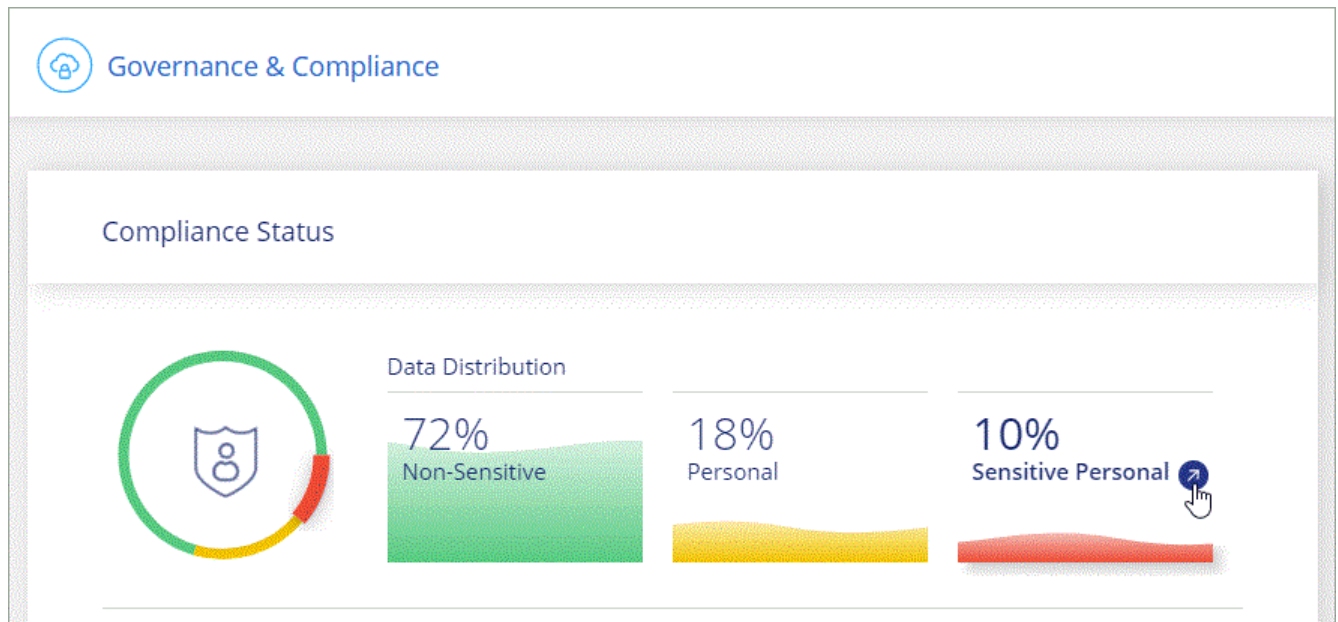


機密性の高い個人データをスキャンする場合は、英語のみがサポートされます。言語のサポートは、あとで追加されます。

機密性の高い個人データを含むファイルを表示する

手順

1. Cloud Manager の上部で、 * Compliance * 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。



< Back

Sensitive Personal Files

7 Types | 23.4K Files

Religious Beliefs Reference

14K Files



Criminal Procedures Reference

12K Files



ICD-10-CM Medical Code

7.9K Files



Sex Life or Orientation Reference

3.9K Files



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

Cloud Compliance は、スキャンしたデータをさまざまなタイプの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。



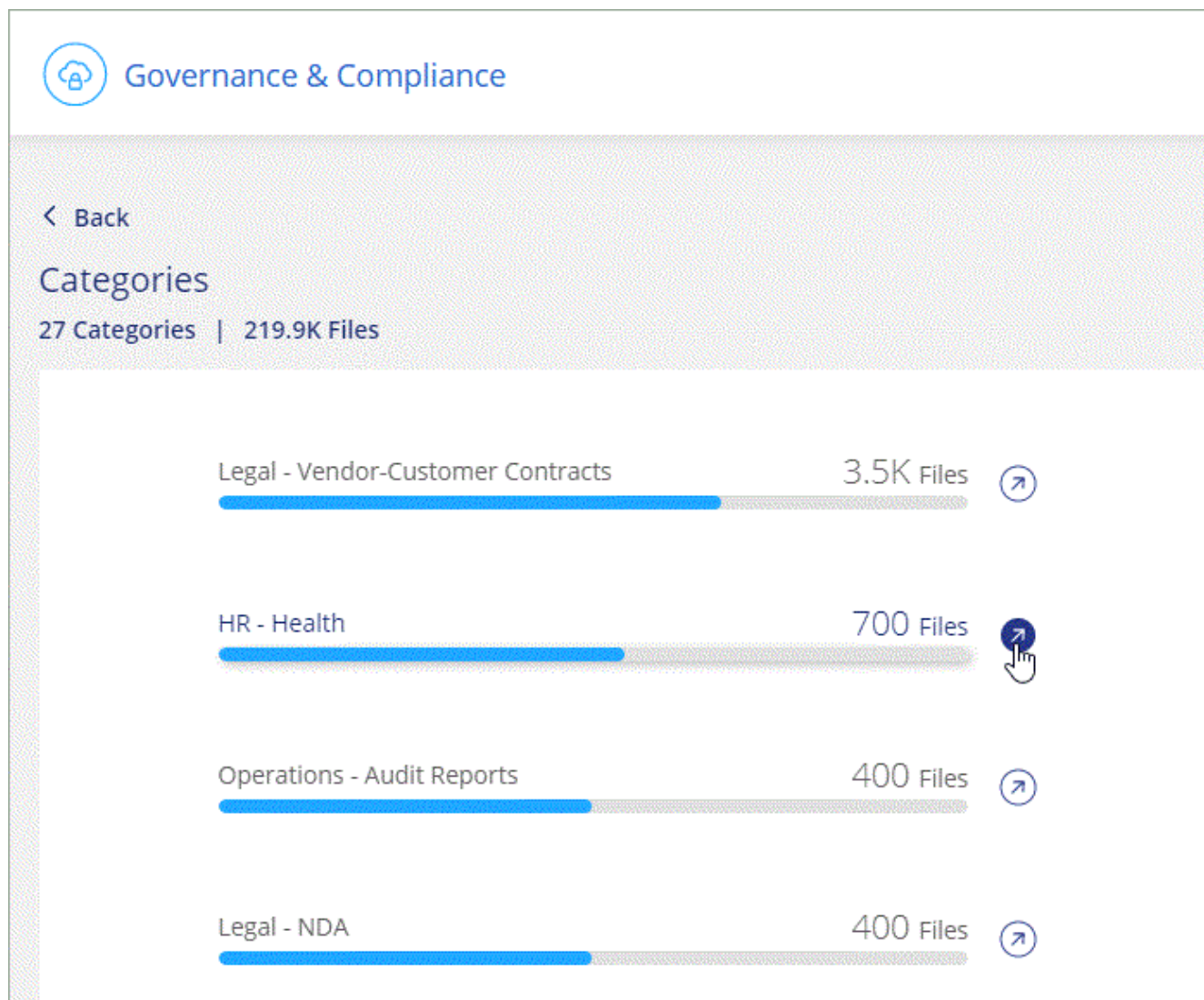
カテゴリでは英語のみがサポートされています。言語のサポートは、あとで追加されます。

カテゴリ別にファイルを表示します

手順

1. Cloud Manager の上部で、* Compliance * 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。

ファイルの種類

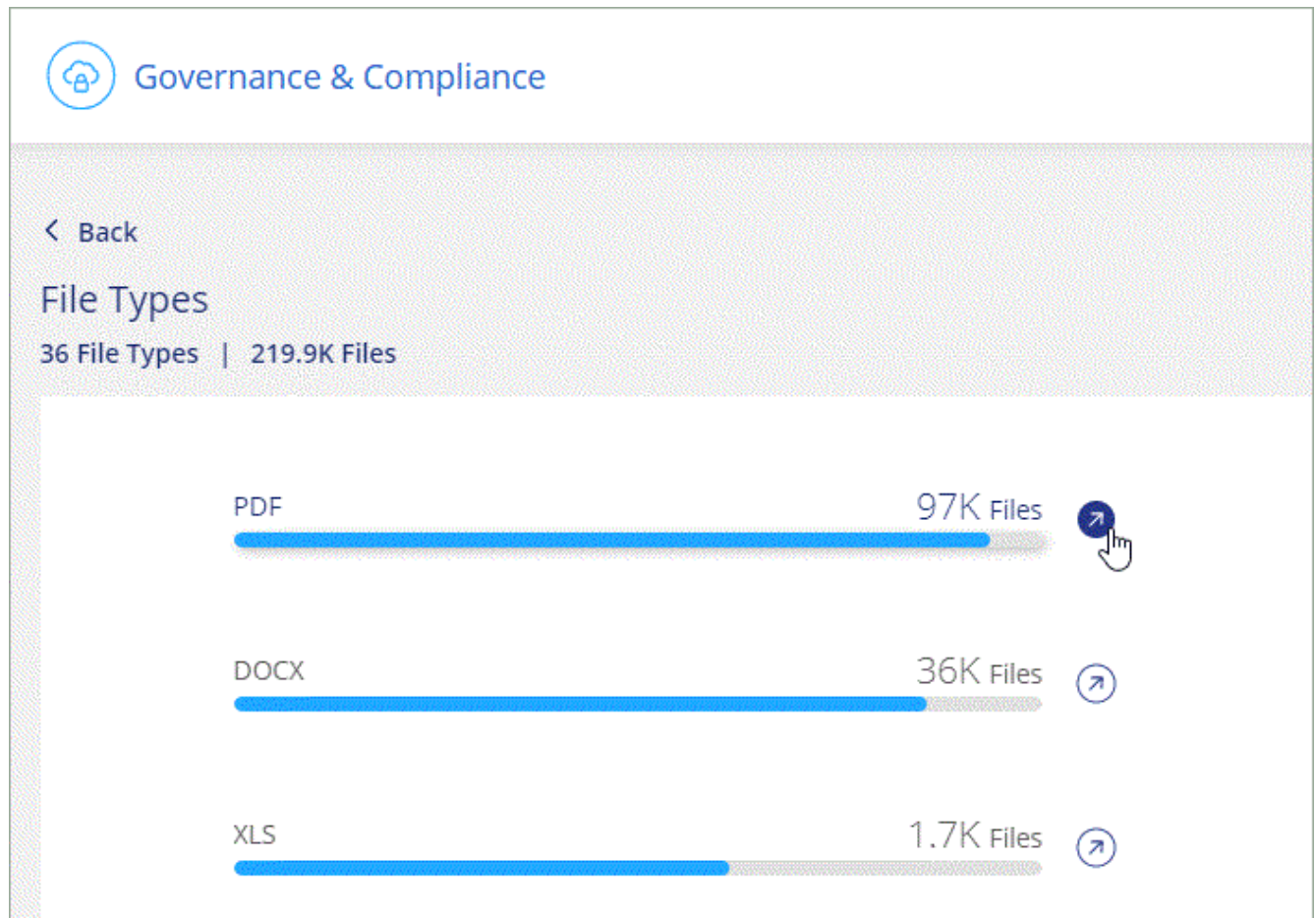
Cloud Compliance は、スキャンしたデータをファイルタイプ別に分類し、ファイルタイプを確認すると、特定のファイルタイプが正しく保存されない可能性があるため、機密データを制御するのに役立ちます。 ["ファイルタイプのリストを参照してください"](#)。

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。

ファイルタイプを表示しています

手順

1. Cloud Manager の上部で、* Compliance * 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。

ファイルメタデータを表示しています

[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。

Unstructured (32K Files)

Structured (323 DB Tables)

🔍

📄

File Name	Personal	Sensitive Personal	Data Subjects	File Type	
Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF
Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF

📁

Working Environment: WorkingEnvironment1

📁

Repository: Volume Name

📁

File Path: /Prod/Expense Report EXP-TPO-1060388.pdf

📁

Category: Legal

📁

File Size: 22 MB

🕒

Last Modified: 2019-08-06 07:51

🔑

Open Permissions: NO OPEN PERMISSIONS

View all Permissions

👤

File Owner: Asaf Ley

📄

Duplicates: 3

View Details

Assign a Label to this file

Delete this file

Give feedback on this result

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 "クラウドコンプライアンスにおける AIP の統合")。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、そのファイルに対して次の 2 つの操作を実行できます。

- 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。
- AIP ラベルを Cloud Compliance と統合している場合は、このファイルにラベルを割り当てることも、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。

ファイルの権限を表示しています

ファイル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と、そのファイルに含まれるアクセス権の種類を表示するには、* すべてのアクセス権を表示 * をクリックします。

File Name

Personal Sensitive Personal Data Subjects File Type

Expense Report TPO-1060.pdf

cvo

6

3

16

PDF

Working Environment: WorkingEnvironment1

Repository: Volume Name

File Path: /Prod/labs-base/Expense Report TPO-1060.pdf

Category: Legal

File Size: 22 MB

Last Modified: 2019-08-06 07:51

Open Permissions: NO OPEN PERMISSIONS

File Owner: Avy

Assign a Label to this file

Delete this file

Permissions list for file Expense Report TPO-1060.pdf

Group or User	Read	Write
user1@company.com	✓	✗
user2@company.com	✓	✓
dist_list_IT@company.com	✓	✗
user4@company.com	✓	✓

Close

このボタンは、CIFS 共有内のファイルに対してのみ使用できます。

ストレージシステムでファイルが複製されているかどうかを表示する

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。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。

重複ファイル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。

🕒

Last Modified: 2019-08-06 07:51

🔑

Open Permissions: NO OPEN PERMISSIONS

[View all Permissions](#)

👤

File Owner: Asaf Ley

📄

Duplicates: 3

[View Details](#)

Duplicates of File 'Name 1'

📄

Duplicates: 3

📦

Total Size of all Duplicates: 1GB

🔍

File Hash: xxxxxxx

[View Duplicates](#)

[Close](#)

3 items

<input type="checkbox"/>	File Name		Personal	Sensitive Personal	Data Subjects	File Type	
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼
<input type="checkbox"/>	Expense Report EXP-TPO-106038887654	cvo	6	3	16	PDF	▼

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。あなたのできる **"ファイルを削除します"** このバージョンのファイルが不要であると確信している場合は、自分自身で実行します。



このページで指定されている「ハッシュ」値を使用して、[調査] ページに直接入力すると、いつでも特定の重複ファイルを検索したり、ポリシーで 사용할 ことができます。

特定の作業環境のダッシュボードデータの表示

Cloud 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、Cloud Compliance は選択した作業環境だけにコンプライアンスデータとレポートをスコープします。

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。



All Working Environments (12) ^

☒ Select all

☒ ANF - Azure NetApp Files

ANF

☒ Working Environment Name 1

CVO

☒ Working Environment Name 2

CVS

☒ Working Environment Name 3

CVS

☒ Working Environment Name 4

CVO

View

Cancel

Personal Files ⓘ

View All

Email Address 2,700 Files



Credit Card 2,700 Files



20%
Personal



5%
Sensitive Personal



7,000

Sensitive Personal Files ⓘ

View All


Health 2,700 Files



Ethnicity 2,700 Files



[データ調査] ページでデータをフィルタリングします

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。CSV バージョンのコンテンツをリファインした後でレポートとして保存する場合は、をクリックします  ボタンを押します。

Data Investigation		Unstructured (32K Files)		Structured (323 DB Tables)			
FILTERS		File Name	Personal	Sensitive Personal	Data Subjects	File Type	
Clear All		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Policies		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Working Environment 4		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Storage Repository		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Category		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
Private Data 6		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	
File Type		> Expense Report EXP-TPO-10603888765435	cvo 6	3	16	PDF	

- トップレベルのタブでは、ファイル（非構造化データ）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ソートできます。
- 左側のペインフィルタを使用すると、作業環境、ストレージリポジトリ、カテゴリ、プライベートデータ、ファイルタイプ、ファイルサイズ、最終変更日、S3 オブジェクトの権限がパブリックアクセスに対して許可されているかどうかなどを指定して、結果を絞り込むことができます。
- [フィルタ] ペインの上部にある `_Policies_filter` には、保存されたデータベースクエリや [お気に入り] リストなど、よく要求されるフィルタの組み合わせを提供するカスタムフィルタがリストされます。実行します ["こちらをご覧ください"](#) 事前定義された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する方法を確認できます。

各ファイルリストレポート（ CSV ファイル）に含まれる内容

各 [調査] ページで、をクリックできます [↓](#) ボタンをクリックして、特定されたファイルの詳細を含むファイルリスト（ CSV 形式）をダウンロードします。10 、 000 件を超える結果がある場合は、上位 10 、 000 件のみがリストに表示されます。

各ファイルリストには、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
- ストレージリポジトリ
- プロトコル
- ファイルパス
- ファイルタイプ
- ファイルサイズ
- 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
- 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。

Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.