



# ユーザーアクティビティ検出を設定する NetApp Ransomware Resilience

NetApp  
April 13, 2026

# 目次

ユーザーアクティビティ検出を設定する	1
NetApp Ransomware Resilienceのユーザーアクティビティ検出について学ぶ	1
疑わしいユーザーアクティビティのフォレンジック	1
コンポーネント	2
ランサムウェア耐性とData Infrastructure Insights	3
次の手順	3
NetApp Ransomware Resilienceのユーザーアクティビティ検出要件	3
クラウドプロバイダのサポート	3
オペレーティング システム要件	4
サーバー要件	4
クラウドネットワークアクセスルール	5
ネットワーク内ルール	6
次のステップ	8
NetApp Ransomware Resilienceでユーザーアクティビティ検出を設定する	8
開始する前に	9
ユーザーアクティビティエージェントを作成する	9
ユーザーディレクトリコネクタを作成する	11
不審なユーザーアクティビティアラートに応答する	13

# ユーザーアクティビティ検出を設定する

## NetApp Ransomware Resilienceのユーザーアクティビティ検出について学ぶ

ユーザーアクティビティ検出機能により、NetApp Ransomware Resilienceにより、ユーザーレベルでランサムウェア イベントに対処し、データ侵害や大規模な削除などのイベントを阻止できます。

NetApp Ransomware Resilience は、疑わしいユーザーアクティビティを監視することで、AI を活用したデータ侵害検出を実現します。読み取りアクティビティの急激な増加と読み取りアクティビティのアクセスパターンを使用して、悪意のある意図を判断します。検出されると、Ransomware Resilience は NetApp Console、Eメール、および構成された任意のセキュリティエコシステム（SIEM など）で自動的にアラートを生成します。

疑わしいユーザーの行動を検出して警告する NetApp Ransomware Resilience は、疑わしいと思われるデータ侵害や破壊の試みやパターンについて警告します。各アラートで、NetApp Ransomware Resilience はブロックできるユーザーを識別します。

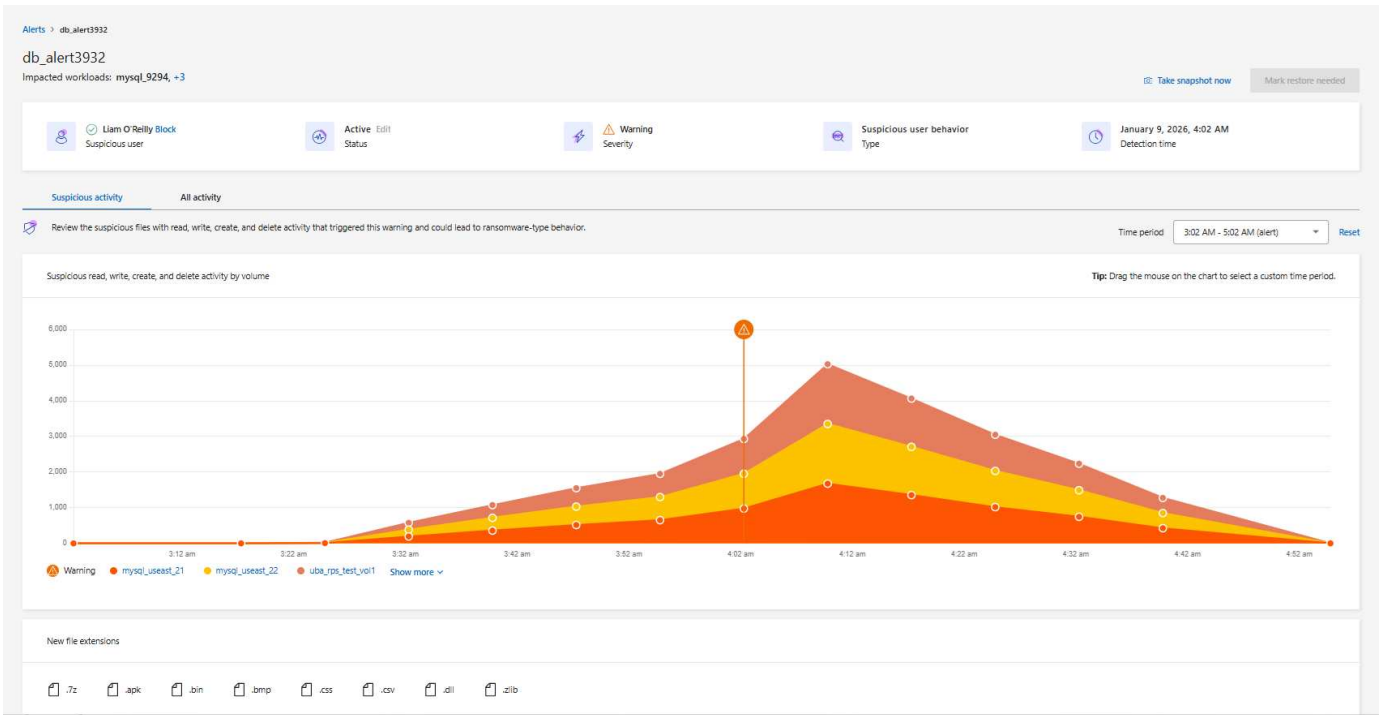
Ransomware Resilience は、ONTAPのFPolicyによって生成されたユーザー アクティビティ イベントを分析して、疑わしいユーザー アクティビティを検出します。ユーザー アクティビティ データを収集するには、1つ以上のユーザー アクティビティ エージェントを展開する必要があります。エージェントは、テナント上のデバイスに接続できる Linux サーバーまたは VM です。



ユーザーアクティビティの検出は現在、SANワークロードではサポートされていません。Amazon FSxN for ONTAP、Cloud Volumes ONTAP、ONTAPのNASワークロードでユーザーアクティビティ検出を使用できます。

## 疑わしいユーザーアクティビティのフォレンジック

Ransomware Resilience は、ユーザーの行動に関するフォレンジックを提供します（疑わしいアクティビティが発生したときや通知が送信されたときを示すリストとグラフ）。これらは、ファイル、ディレクトリ、ボリューム、ワークロードにおける疑わしいアクティビティの頻度を経時的に詳細に示し、イベントのグラフ化に役立ちます。新しいファイル拡張子の出現も確認できます。



○

疑わしいアクティビティをすべてのアクティビティのビューと比較できます。すべてのアクティビティビューでは、アクセスの変更やアクセス拒否のイベントに加えて、読み取り、書き込み、名前の変更、移動、作成、削除のイベントを観察できます。



○

## コンポーネント

NetApp Ransomware Resilience の疑わしいユーザー行動アクティビティ検出には、3つの主要コンポーネントがあります。

- ユーザーアクティビティエージェントは、データコレクター用の実行可能環境です。ユーザーアクティビティエージェントを設定する必要があります。

- データコレクタは、ユーザーアクティビティイベントをRansomware Resilienceと共有します。データコレクタは、"疑わしいユーザーアクティビティの検出によるランサムウェア保護戦略を有効化"ときに自動的に作成されます。
- ユーザーディレクトリコネクタを使用すると、ユーザー名とユーザーID間のマッピングが可能になり、疑わしいユーザーの行動への対応がより明確になります。ユーザーディレクトリコネクタを設定する必要があります。

## ランサムウェア耐性とData Infrastructure Insights

Ransomware Resilienceの疑わしいユーザー行動検出は、Data Infrastructure Insights (DII) Workload Securityとの統合であり、"DIIエンドポイント"を使用します。Ransomware Resilienceでユーザー行動検出を有効にするために、DII構成は必要ありません。ユーザー行動検出を有効にするには、"必要なエージェントとコレクターを作成し、適切なランサムウェア保護戦略を有効にする"。

すでにNetApp Data Infrastructure Insights (DII) Workload Security を使用している場合は、Ransomware Resilience に同じ Workload Security エージェントを使用することをお勧めします。Ransomware Resilience 用に個別の Workload Security エージェントを展開する必要はありませんが、同じ Workload Security エージェントを使用するには、Ransomware Resilience Console 組織と DII Storage Workload Security テナント間のペアリング関係が必要です。このペアリングを有効にするには、アカウント担当者にお問い合わせください。

### 次の手順

- "ユーザー行動アクティビティ検出の要件"
- "ユーザー行動アクティビティエージェントと検出器を設定する"

## NetApp Ransomware Resilienceのユーザーアクティビティ検出要件

NetApp Ransomware Resilienceユーザー行動検出により、ユーザーレベルのランサムウェア イベントに対応できるようになります。ユーザーの動作検出を有効にするには、エージェントのセットを作成する必要があります。検出を有効にする前に、Ransomware Resilienceがイベントを適切に検出して報告できるように、概説されているオペレーティング システム、サーバー、およびネットワークの要件を満たしていることを確認する必要があります。

### クラウドプロバイダのサポート

疑わしいユーザーアクティビティ データは、次のリージョンの AWS および Azure に保存される可能性があります。

クラウド プロバイダ	リージョン
AWS	<ul style="list-style-type: none"> <li>• アジア太平洋 (シドニー) (ap-southeast-2)</li> <li>• ヨーロッパ (フランクフルト) (eu-central-1)</li> <li>• 米国東部 (バージニア北部) (us-east-1)</li> </ul>
Azure	米国東部

## オペレーティング システム要件

疑わしいユーザー行動の検出は、次のオペレーティングシステムでサポートされています：

オペレーティング システム	サポート対象のバージョン
アルマリナックス	9.4 (64 ビット) から 9.5 (64 ビット)、および 10 (64 ビット) (SELinux を含む)
CentOS	CentOS Stream 9 (64 ビット)
Debian	11 (64 ビット)、12 (64 ビット)、SELinux を含む
OpenSUSE リープ	15.3 (64 ビット) から 15.6 (64 ビット)
Oracle Linux	8.10 (64 ビット)、および 9.1 (64 ビット) から 9.6 (64 ビット) (SELinux を含む)
Red Hat	8.10 (64 ビット)、9.1 (64 ビット) から 9.6 (64 ビット)、および 10 (64 ビット) (SELinux を含む)
ロッキーマ	Rocky 9.4 (64 ビット) から 9.6 (64 ビット)、SELinux を含む
SUSEエンタープライズLinux	15 SP4 (64 ビット) から 15 SP6 (64 ビット)、SELinux を含む
Ubuntu	20.04 LTS (64 ビット)、22.04 LTS (64 ビット)、24.04 LTS (64 ビット)



ユーザー アクティビティ エージェントに使用するマシンは、他のアプリケーションレベルのソフトウェアを実行しないでください。専用サーバーをお勧めします。

その unzip インストールにはコマンドが必要です。その `sudo su -` インストール、スクリプトの実行、アンインストールにはコマンドが必要です。

## サーバー要件

サーバーは次の最小要件を満たしている必要があります。

- **CPU:** 4コア
- **RAM:** 16GB RAM
- **ディスク容量:** 36 GB の空きディスク容量

## サーバーの推奨事項

- ファイルシステムの作成を可能にするために追加のディスク領域を割り当てます。ファイルシステムに少なくとも 35 GB の空き領域があることを確認します。+ もし `/opt` NAS ストレージからマウントされたフォルダーであるため、ローカル ユーザーはこのフォルダーにアクセスする必要があります。ローカル ユーザーに必要な権限がない場合、ユーザー アクティビティ エージェントの作成が失敗する可能性があります。
- ユーザーアクティビティエージェントは、Ransomware Resilienceとは別のシステムにインストールすることを推奨します。同じマシンにインストールする場合は、50~55 GBのディスク容量を確保する必要があります。Linuxの場合は、`/opt/netapp``に25~30 GBのスペースを割り当て、``var/log/netapp``に25 GB

を割り当てます。

- Network Time Protocol (NTP) または Simple Network Time Protocol (SNTP) を使用して、ONTAPシステムとユーザー アクティビティ エージェント マシンの両方の時刻を同期することをお勧めします。

## クラウドネットワークアクセスルール

関連する地域 (アジア太平洋、ヨーロッパ、または米国) のクラウド ネットワーク アクセス ルールを確認します。



初期インストール時に、`<site_name>` をワイルドカード (\*) 権限に置き換えます。エージェントがアクティブ化され、完全に動作可能になったら、権限をサイト名に置き換えることができます。サイト名については、NetAppの担当者にお問い合わせください。



ユーザアクティビティエージェントはNetApp Data Infrastructure Insightsテクノロジーを使用するため、`cloudinsights` エンドポイントを使用します。詳細については、次を参照してください。

### APACベースのユーザーアクティビティエージェントの導入

プロトコル	ポート	ソース	デスティネーション	説明
HTTPS (TCP)	443	ユーザーアクティビティエージェント	<ul style="list-style-type: none"><li>• <code>&lt;site_name&gt;.cs01-ap-1.cloudinsights.netapp.com</code></li><li>• <code>&lt;site_name&gt;.c01-ap-1.cloudinsights.netapp.com</code></li><li>• <code>&lt;site_name&gt;.c02-ap-1.cloudinsights.netapp.com</code></li><li>• <code>gentlogin.cs01-ap-1.cloudinsights.netapp.com</code></li></ul>	ランサムウェア耐性へのアクセス

### ヨーロッパを拠点とするユーザーアクティビティエージェントの導入

プロトコル	ポート	ソース	デスティネーション	説明
HTTPS (TCP)	443	ユーザーアクティビティエージェント	<ul style="list-style-type: none"><li>• <code>&lt;site_name&gt;.cs01-eu-1.cloudinsights.netapp.com</code></li><li>• <code>&lt;site_name&gt;.c01-eu-1.cloudinsights.netapp.com</code></li><li>• <code>&lt;site_name&gt;.c02-eu-1.cloudinsights.netapp.com</code></li><li>• <code>agentlogin.cs01-eu-1.cloudinsights.netapp.com</code></li></ul>	ランサムウェア耐性へのアクセス

### 米国ベースのユーザアクティビティエージェントの導入

プロトコル	ポート	ソース	デスティネーション	説明
HTTPS (TCP)	443	ユーザーアクティビティエージェント	<ul style="list-style-type: none"> <li>• &lt;site_name&gt;.cs01.cloudinsights.netapp.com</li> <li>• &lt;site_name&gt;.c01.cloudinsights.netapp.com</li> <li>• &lt;site_name&gt;.c02.cloudinsights.netapp.com</li> <li>• agentlogin.cs01.cloudinsights.netapp.com</li> </ul>	ランサムウェア耐性へのアクセス

## ネットワーク内ルール

プロトコル	ポート	ソース	デスティネーション	説明
TCP	389(LDAP) 636 (LDAP / start-tls)	ユーザーアクティビティエージェント	LDAP Server URL	LDAPに接続する
HTTPS (TCP)	443	ユーザーアクティビティエージェント	クラスタまたは SVM 管理 IP アドレス (SVM コレクターの構成によって異なります)	ONTAPとのAPI通信

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000 - 55000	SVMデータLIF IPアドレス	ユーザーアクティビティエージェント	Fpolicy イベントに関するONTAPからユーザー アクティビティ エージェントへの通信。ONTAP がイベントをユーザー アクティビティ エージェントに送信するには、ユーザー アクティビティ エージェントに対してこれらのポートを開く必要があります。これには、ユーザー アクティビティ エージェント自体のファイアウォール（存在する場合）も含まれます。+ 注意: これらのポートをすべて予約する必要はありませんが、予約するポートはこの範囲内である必要があります。まずは 100 個のポートを予約し、必要に応じて増やすことをお勧めします。

プロトコル	ポート	ソース	デスティネーション	説明
TCP	35000-55000	クラスタ管理IP	ユーザーアクティビティエージェント	ONTAPクラスタ管理 IP から <b>EMS</b> イベントのユーザアクティビティエージェントへの通信。ONTAPがEMSイベントを送信するには、ユーザアクティビティエージェント自体のファイアウォールも含めて、これらのポートをユーザアクティビティエージェントに対して開く必要があります。+ 注意: これらのポートをすべて予約する必要はありませんが、予約するポートはこの範囲内である必要があります。まずは 100 個のポートを予約し、必要に応じて増やすことをお勧めします。
SSH	22	ユーザーアクティビティエージェント	クラスタ管理	CIFS/SMB ユーザーのブロックに必要です。

## 次のステップ

- ["ユーザアクティビティエージェントとコレクタを設定する"](#)

## NetApp Ransomware Resilienceでユーザーアクティビティ検出を設定する

NetApp Ransomware Resilience ユーザー アクティビティ検出は、ユーザー レベルのランサムウェア イベントを防ぐのに役立ちます。Ransomware Resilience で疑わしいユーザー動作の検出を有効にするには、少なくとも 1 つのユーザー アクティビティ エージェントをインストールする必要があります。これにより、ランサムウェア イベントに類似する異常なパターンがないかユーザー動作を監視するデータ収集環境が作成されます。

ユーザー アクティビティ エージェントは、データ コレクターとユーザー ディレクトリ コネクタをホストします。これらの両方がデータを分析のために SaaS の場所に送信します。

- データコレクタは、ONTAPからユーザーアクティビティデータを収集します。ユーザー行動検出を含む保護戦略を作成すると、データコレクタが自動的に作成されます。

- ユーザー ディレクトリ コネクタ はディレクトリに接続して、ユーザー ID をユーザー名にマッピングします。ユーザー ディレクトリ コネクタを設定する必要があります。

ユーザー アクティビティ エージェント、データ コレクター、ユーザー ディレクトリ コネクタはすべて、Ransomware Resilience 設定ダッシュボードから管理できます。



すでにNetApp Data Infrastructure Insights (DII) Workload Security を使用している場合は、Ransomware Resilience に同じ Workload Security エージェントを使用することをお勧めします。Ransomware Resilience 用に個別の Workload Security エージェントを展開する必要はありませんが、同じ Workload Security エージェントを使用するには、Ransomware Resilience Console 組織と DII Storage Workload Security テナント間のペアリング関係が必要です。このペアリングを有効にするには、アカウント担当者にお問い合わせください。

+ DII を使用して\_いない\_場合は、ここでの設定手順に進みます。

## 開始する前に

- "[オペレーティングシステム、サーバ、およびネットワークの要件](#)"を満たしていることを確認してください。

必須のコンソールロール 疑わしいユーザーアクティビティの検出を有効にするには、**Organization admin role**が必要です。その後の疑わしいユーザーアクティビティの設定には、**Ransomware Resilience user behavior admin role**が必要です。"[NetApp Consoleのランサムウェア耐性ロールについて学ぶ](#)"。

各ロールが組織レベルで適用されていることを確認します。

## ユーザーアクティビティエージェントを作成する

ユーザーアクティビティエージェントは、"[データコレクター](#)"の実行可能な環境です。データコレクターは、ユーザーアクティビティイベントをNetApp Ransomware Resilienceと共有します。疑わしいユーザーアクティビティの検出を有効にするには、少なくとも1つのユーザーアクティビティエージェントを作成する必要があります。

### 手順

1. ユーザー アクティビティ エージェントを初めて作成する場合は、ダッシュボード に移動してください。ユーザー アクティビティ タイルで、アクティブ化 を選択します。

追加のユーザー アクティビティ エージェントを追加する場合は、[設定] に移動し、[ユーザー アクティビティ] タイルを見つけて、[管理] を選択します。[ユーザー アクティビティ] 画面で、[ユーザー アクティビティ エージェント] タブを選択し、[追加] を選択します。

2. クラウド プロバイダー を選択し、次に リージョン を選択します。次へを選択します。

3. ユーザー アクティビティ エージェントの詳細を入力します。

- ユーザーアクティビティエージェント名
- コンソール エージェント - コンソール エージェントは、ユーザー アクティビティ エージェントと同じネットワーク内に存在し、ユーザー アクティビティ エージェントの IP アドレスに SSH 接続できる必要があります。
- **VM DNS**名または**IP**アドレス
- **VM SSH** キー - 次の形式で SSH キーを入力します：

```
-----BEGIN OPENSSH PRIVATE KEY-----  
private-key-contents  
-----END OPENSSH PRIVATE KEY-----
```

User activity agent name

Select a Console agent located near the user activity agent to minimize latency when transmitting activity to Ransomware Resilience.

Console agent i

Provide the VM executable environment with "root" access for collectors in this user activity agent.

VM DNS name or IP address

VM SSH key i

4. 次へを選択します。
5. 設定を確認してください。\*アクティブ化\*を選択して、ユーザー アクティビティ エージェントの追加を完了します。
6. ユーザーアクティビティエージェントが正常に作成されたことを確認します。ユーザーアクティビティタイトルでは、デプロイメントが成功すると **実行中** と表示されます。

## 結果

ユーザーアクティビティエージェントが正常に作成されたら、設定メニューに戻り、ユーザーアクティビティタイトルで管理を選択します。ユーザーアクティビティエージェントタブを選択し、ユーザーアクティビティエージェントを選択して、データコレクターやユーザーディレクトリコネクタなどの詳細を表示します。

## データコレクターを追加する

疑わしいユーザー アクティビティの検出を含むランサムウェア保護戦略を有効にすると、データ コレクターが自動的に作成されます。詳細については、["検出ポリシーを追加する"](#)を参照してください。

データコレクターの詳細を表示できます。[設定] から、[ユーザー アクティビティ] タイトルの [管理] を選択します。データ コレクター タブを選択し、データ コレクターを選択して詳細を表示するか、一時停止します。

## ユーザーディレクトリコネクタを作成する

ユーザー ID をユーザー名にマップするには、ユーザー ディレクトリ コネクタを作成する必要があります。

### 手順

1. Ransomware Resilience で、[設定] に移動します。
2. ユーザー アクティビティ タイルで、管理 を選択します。
3. ユーザー ディレクトリ コネクタ タブを選択し、追加 を選択します。
4. 接続を構成します。各フィールドに必要な情報を入力します。

フィールド	説明
名前	ユーザーディレクトリコネクタの一意的名前を入力します
ユーザーディレクトリの種類	ディレクトリタイプ
サーバーのIPアドレスまたはドメイン名	接続をホストするサーバーの IP アドレスまたは完全修飾ドメイン名 (FQDN)
フォレスト名または検索名	ディレクトリ構造のフォレストレベルを直接ドメイン名として指定することができます (例: unit.company.com) または相対識別名のセット (例: DC=unit,DC=company,DC=com) 。また、OU 組織単位または CN 特定のユーザーに限定する (例: CN=user,OU=engineering,DC=unit,DC=company,DC=com) 。
バインドDN	BIND DN は、user@domain.com など、ディレクトリの検索が許可されたユーザー アカウントです。ユーザーにはドメイン読み取り専用権限が必要です。
BINDパスワード	BIND DNで指定されたユーザーのパスワード
プロトコル	プロトコル フィールドはオプションです。LDAP、LDAPS、または LDAP over StartTLS を使用できます。
ポート	選択したポート番号を入力してください

### User directory

Connect to your user directories to identify specific users performing potentially suspicious behavior. [Get help](#)

---

**Connection** ^

<p>Name</p> <input type="text" value="Unique name required"/>	<p>User directory type</p> <div style="border: 1px solid #ccc; padding: 2px;">Active Directory</div>
<p>User activity agent</p> <div style="border: 1px solid #ccc; padding: 2px;">Select...</div>	<p>Server IP or DNS name</p> <input type="text"/>
<p>Forest name or search name <span style="font-size: small;">i</span></p> <input type="text"/>	<p>Bind DN</p> <input type="text"/>
<p>Bind password <span style="float: right;">🙁</span></p> <input type="password"/>	<p>Protocol <span style="float: right;">Optional</span></p> <div style="border: 1px solid #ccc; padding: 2px;">LDAP</div>
<p>Port</p> <input type="text" value="389"/>	

---

**Attribute mapping** v

Not set

属性マッピングの詳細を指定します。

- 表示名
- **SID** (LDAP を使用している場合)
- ユーザー名
- **Unix ID** (NFS を使用している場合)
- オプションの属性を含める\*を選択した場合は、電子メール アドレス、電話番号、役割、州、国、部門、写真、マネージャー **DN**、またはグループも追加できます。オプションの検索クエリを追加するには、[\*詳細] を選択します。

5. 追加を選択します。

6. ユーザー ディレクトリ コネクタ タブに戻り、ユーザー ディレクトリ コネクタのステータスを確認します。正常に作成されると、ユーザー ディレクトリ コネクタのステータスは **実行中** と表示されます。

#### ユーザーディレクトリコネクタを削除する

##### 手順

1. Ransomware Resilience で、[設定] に移動します。
2. ユーザー アクティビティ タイルを見つけて、[管理] を選択します。
3. ユーザー ディレクトリ コネクタ タブを選択します。
4. 削除するユーザー ディレクトリ コネクタを特定します。行末のアクションメニューで、3つの点を選択します。`...`次に削除します。
5. ポップアップダイアログで、削除を選択して確認します。

## アラートからユーザーを除外する

特定の信頼できるユーザーの行動によってユーザー行動アラートがトリガーされる可能性がある場合は、そのユーザーをアラートから除外できます。

### 手順

1. ランサムウェア耐性で、[設定] を選択します。
2. 設定ダッシュボードで、ユーザーアクティビティカードを見つけて、管理を選択します。
3. 除外ユーザータブを選択します。
4. UI で個々のユーザーを確認するには、手動で選択を選択します。除外されたユーザーのリストをアップロードするには、アップロードを選択します。
  - a. 手動で選択を選択した場合は、除外する特定のユーザーの名前の横にあるチェックボックスをオンにします。
  - b. **Upload** を選択した場合は、すべてのユーザーのリストが含まれる CSV または JSON ファイルをダウンロードします。リストにアクセスするには、**Download** を選択します。

ローカルマシンでファイルを確認します。検出を維持するすべてのユーザーの名前を削除します。検出から除外するユーザーの名前のみがリストに含まれたら、保存します。

Ransomware Resilience で、**Upload** を選択します。ファイルを見つけてアップロードします。

5. 除外リストへのユーザーの追加を完了するには、[追加] を選択します。
6. 除外ユーザータブでは、ユーザー行動検出アラートから削除されたユーザーの名前がダッシュボードに表示されるようになりました。



アラートからユーザーを直接除外することもできます。詳細については、"[ランサムウェアの警告に応答する](#)"を参照してください。

## 除外ユーザーリストからユーザーを削除する

後からユーザーを検出対象に再度追加することができます。

### 手順

1. 設定ダッシュボードで、ユーザーアクティビティカードを見つけて、管理を選択します。
2. 除外ユーザータブを選択します。
3. 追加を選択します。
4. UI から個々のユーザーを除外するには、手動で選択を選択します。
5. 除外ユーザーの選択から削除するユーザーの名前を見つけます。ユーザー名の行にあるアクションメニュー (...) を選択し、削除を選択します。
6. ダイアログで、削除を選択して、選択したユーザーを削除することを確認します。

## 不審なユーザーアクティビティアラートに応答する

疑わしいユーザーアクティビティの検出を構成すると、アラートページでイベントを監視できます。詳細については、"[悪意のあるアクティビティや疑わしいユーザーの行動を検出する](#)"を参照してください。

## 著作権に関する情報

Copyright © 2026 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権を有し、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権については、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。