相関イベントとコンプライアンス イベント

次のトピックでは、相関イベントとコンプライアンスイベントを表示する方法について説明します。

相関イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst

アクティブな相関ポリシーに含まれる相関ルールがトリガーとして使用されると、システムが相関イベントを生成してデータベースにそれを記録します。

（注） アクティブな相関ポリシーに含まれるコンプライアンス ホワイトリストがトリガーとして使用されると、システムがホワイトリスト イベントを生成します。

相関イベントのテーブルを表示し、検索対象の情報に応じてイベント ビューを操作できます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

相関イベントにアクセスしたときに表示されるページは、使用するワークフローによって異なります。相関イベントのテーブル ビューが含まれる定義済みワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 **[Analysis]** > **[Correlation]** > **[Correlation Events]**を選択します。

オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 相関イベントのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え)（(switch workflow)）] をクリックし、[相関イベント（Correlation Events）] を選択します。

ステップ 2 オプションで、時間枠の変更の説明に従って、時間範囲を調整します。

ステップ 3 次のいずれかの操作を実行します。

- 表示されるカラムの詳細については、相関イベントのフィールド （3 ページ）を参照してください。
- IP アドレスのホスト プロファイルを表示するには、IP アドレスの横に表示されるホスト プロファイル アイコンをクリックします。
- To view user identity information, click the user icon that appears next to the user identity ( , or for users associated with IOCs, ).
- 現在のワークフロー ページ内でイベントをソートしたり制限したり、または移動するには、ワークフローの使用を参照してください。
- 現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフローページの左上にある該当するページ リンクをクリックします。
- 特定の値に制限して、ワークフロー内の次のページにドリルダウンするには、ドリルダウン ページの使用を参照してください。
- 一部またはすべての相関イベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 他のイベント ビューに移動して関連イベントを表示するには、ワークフロー間のナビゲーションを参照してください。
- （所属する組織でイベント データを外部の Firepower システムに保存している場合）パケットや履歴データなど、イベントに関連する情報を調査するには、イベントの値を右クリックします。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Cisco Security Packet Analyzerを使用したイベント調査 および Web ベースのリソースを使用したイベントの調査 を参照してください。
- イベントに関するインテリジェンスを収集するには、テーブルでイベントの値を右クリックして、シスコまたはサードパーティのインテリジェンス ソースを選択します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオ

プションは、データタイプやシステムに設定されている統合によって異なります。詳細については、Web ベースのリソースを使用したイベントの調査を参照してください。

関連トピック

データベース イベント数の制限
ワークフローのページ

相関イベントのフィールド

相関ルールがトリガーとして使用されると、システムは相関イベントを生成します。次の表では、表示および検索可能な相関イベント テーブルのフィールドについて説明します。

表 *1*: 相関イベントのフィールド

フィールド	Description
Description	相関イベントについての説明。説明に示される情報は、ルールがどのようにトリガーとして使用されたかによって異なります。 たとえば、オペレーティング システム情報の更新イベントによってルールがトリガーとして使用された場合、新しいオペレーティング システムの名前と信頼度レベルが表示されます。
Device	ポリシー違反をトリガーとして使用したイベントを生成したデバイスの名前。
ドメイン（Domain）	ポリシー違反をトリガーとして使用したモニタ対象トラフィックのデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.
影響（Impact）	侵入データ、ディスカバリ データ、および脆弱性情報の間の相関に基づいて相関イベントに割り当てられた影響レベル。 このフィールドを検索する場合、大文字と小文字を区別しない有効な値は、`Impact 0`、`Impact Level 0`、`Impact 1`、`Impact Level 1`、`Impact 2`、`Impact Level 2`、`Impact 3`、`Impact Level 3`、`Impact 4`、および `Impact Level 4` です。影響アイコンの色または部分文字列は使用しないでください（たとえば、`blue`、`level 1`、または `0` を使用しないでください）。
入力インターフェイス（Ingress Interface）または出力インターフェイス（Egress Interface）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力インターフェイス。

フィールド	Description
入力セキュリティ ゾーン（Ingress Security Zone）または出力セキュリティ ゾーン（Egress Security Zone）	ポリシー違反をトリガーとして使用した侵入イベントまたは接続イベントの入力または出力セキュリティ ゾーン。
インライン結果（Inline Result）	次のいずれかになります。 • 黒の下矢印：侵入ルールをトリガーとして使用したパケットがシステムによってドロップされたことを示します • グレーの下矢印：侵入ポリシー オプション [インライン時にドロップ（Drop when Inline）] を有効にした場合、インライン型、スイッチ型、またはルーティング型展開でパケットがシステムによってドロップされたと想定されることを示します • 空白：トリガーとして使用された侵入ルールが [ドロップしてイベントを生成する（Drop and Generate Events）] に設定されていなかったことを示します 侵入イベントによってトリガーとして使用されたポリシー違反を検索するためにこのフィールドを使用する場合は、次のいずれかを入力します。 • `dropped` は、インライン型、スイッチ型、またはルーティング型展開でパケットがドロップされたかどうかを示します。 • would have dropped は仮定を表します。インライン型、スイッチ型、またはルーティング型展開でパケットをドロップするよう侵入ポリシーが設定されていると仮定した場合、パケットがドロップされるかどうかを示します。 侵入ポリシーのドロップ動作やルール状態とは無関係に、パッシブ展開（インライン セットがタップ モードである場合を含む）ではシステムがパケットをドロップしないことに注意してください。
ポリシー	違反が発生したポリシーの名前。
[プライオリティ（Priority）]	相関イベントのプライオリティ。これは、トリガーとして使用されたルールのプライオリティまたは違反が発生した相関ポリシーのプライオリティによって決まります。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。
ルール（Rule）	ポリシー違反をトリガーとして使用したルールの名前。

フィールド	Description
セキュリティ インテリジェンス カテゴリ（Security Intelligence Category）	ブラックリスト化されたオブジェクトの名前。これは、ポリシー違反をトリガーとして使用したイベントでブラックリスト化された IP アドレスを示す（またはその IP アドレスを含む）オブジェクトです。 このフィールドを検索する場合は、ポリシー違反をトリガーとして使用した相関イベントに関連付けられたセキュリティインテリジェンスのカテゴリを指定します。セキュリティインテリジェンスのカテゴリとして、セキュリティインテリジェンス オブジェクト、グローバル ブラックリスト、カスタム セキュリティ インテリジェンス リストまたはフィード、あるいはインテリジェンス フィードに含まれるいずれかのカテゴリを指定できます。
送信元の大陸（Source Continent）または宛先の大陸（Destination Continent）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホスト IP アドレスに関連付けられた大陸。
送信元の国（Source Country）または宛先の国（Destination Country）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先 IP アドレスに関連付けられた国。
送信元ホストの重大度（Source Host Criticality）または宛先ホストの重大度（Destination Host Criticality）	相関イベントに関連する送信元または宛先ホストにユーザが割り当てたホスト重要度。`None`、`Low`、`Medium`、または `High` のいずれかです。 ディスカバリ イベント、ホスト入力イベント、または接続イベントに基づくルールによって生成された相関イベントにのみ、送信元ホスト重要度が含まれることに注意してください。
送信元 IP（Source IP）または宛先 IP（Destination IP）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストの IP アドレス。
送信元ポート/ICMP タイプ（Source Port/ICMP Type）または宛先ポート/ICMP コード（Destination Port/ICMP Code）	ポリシー違反をトリガーとして使用したイベントに関連付けられた、送信元トラフィックの送信元ポート/ICMP タイプまたは宛先トラフィックの宛先ポート/ICMP コード。
送信元ユーザ（Source User）または宛先ユーザ（Destination User）	ポリシー違反をトリガーとして使用したイベントの送信元または宛先ホストにログインしたユーザの名前。
時刻（Time）	相関イベントが生成された日時。このフィールドは検索できません。
メンバー数（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません

関連トピック

イベントの検索

コンプライアンス ホワイト リスト ワークフローの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst/Discovery Admin

Firepower Management Center は、ネットワークで生成されるホワイト リスト イベントおよびホワイト リスト違反の分析で使用できるワークフローセットを提供します。ワークフローはネットワーク マップやダッシュボードとともに、ネットワーク資産のコンプライアンスに関する主要な情報源になります。

システムは、ホワイト リスト イベントとホワイト リスト違反のために事前定義されたワークフローを提供します。ユーザはカスタム ワークフローを作成することもできます。コンプライアンス ホワイト リスト ワークフローを使用すると、多くの一般的なアクションを実行できます。

手順

ステップ 1 **[分析（Analysis）] > [相関（Correlation）]** メニューを使用してホワイト リスト ワークフローにアクセスします。

ステップ 2 次の選択肢があります。

- ワークフローの切り替え：カスタム ワークフローなどの別のワークフローを使用するには、[(ワークフローの切り替え)（(switch workflow)）] をクリックします。
- 時間範囲：時間範囲を調整（イベントが表示されない場合に役立ちます）する方法については、時間枠の変更を参照してください。
- ホスト プロファイル：IP アドレスのホスト プロファイルを表示するには、ホスト プロファイルのアイコン（  ）をクリックします。アクティブな侵害の兆候（IOC）タグのあるホストの場合は、IP アドレスの横に表示される侵害されたホストのアイコン（  ）をクリックします。
- ユーザ プロファイル（イベントのみ）：To view user identity information, click the user icon that appears next to the user identity ( , or for users associated with IOCs, ).

- 制約：表示されるカラムを制約にするには、非表示にするカラムの見出しにある閉じるアイコン（✖）をクリックします。表示されるポップアップ ウィンドウで、[適用（Apply）] をクリックします。

  ヒント 他のカラムを表示または非表示にするには、[適用（Apply）] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効になったカラムをビューに再び追加するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のカラム名をクリックします。

- ドリル ダウン：ドリルダウン ページの使用を参照してください。
- ソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- このページに移動する：ワークフロー ページのトラバーサル ツールを参照してください。
- ページ間で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページ リンクをクリックします。
- イベント ビュー間で移動する：関連するイベントを表示するためその他のイベント ビューに移動するには、[ジャンプ（Jump to）] をクリックし、ドロップダウン リストからイベント ビューを選択します。
- イベントの削除（イベントのみ）：現在の制約されているビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除（Delete）] または [すべて削除（Delete All）] をクリックします。

関連トピック

ワークフローのページ
イベント ビュー設定の設定

ホワイトリスト イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst/Discovery Admin

最初の評価が行われた後、監視対象ホストがアクティブなホワイト リストに準拠しなくなると、システムはホワイト リスト イベントを生成します。ホワイト リスト イベントは、相関イベントの特殊な形態で、FMC 相関イベント データベースに記録されます。

Firepower Management Center を使用して、コンプライアンス ホワイト リスト イベントのテーブルを表示できます。ここでユーザは、検索する情報に応じてイベント ビューを操作することができます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ホワイト リスト イベントにアクセスしたときに表示されるページは、使用しているワークフローによって異なります。イベントのテーブル ビューで終わる事前定義されたワークフローを使用できます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

手順

ステップ 1 **[Analysis]** > **[Correlation]** > **[White List Events]**を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス ホワイト リスト ワークフローの使用 （6 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、ホワイト リスト イベントのフィールド （8 ページ）を参照してください。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

ホワイト リスト イベントのフィールド

ワークフローを使用して表示および検索できるホワイト リスト イベントには、次のフィールドがあります。

Device

ホワイト リスト違反を検出した管理対象デバイスの名前。

説明

ホワイト リスト違反の説明。次に例を示します。

```
Client “AOL Instant Messenger” is not allowed.
```

アプリケーションプロトコルに関係する違反には、アプリケーションプロトコルの名前とバージョンだけでなく、使用されているポートとプロトコル（TCP または UDP）も示されます。禁止を特定のオペレーティング システムに限定する場合は、説明にオペレーティング システム名が含まれます。次に例を示します。

```
Server "ssh / 22 TCP (OpenSSH 3.6.1p2)" is not allowed on Operating
System “Linux Linux 2.4 or 2.6”.
```

ドメイン（Domain）

ホワイト リストに準拠しなくなったホストのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

ホストの重要度（Host Criticality）

ホワイトリストに準拠していないホストに対してユーザが割り当てた重要度（[なし（None）]、[低（Low）]、[中（Medium）]、または [高（High）]）。

[IPアドレス（IP Address）]

ホワイト リストに準拠しなくなったホストの IP アドレス。

ポリシー

違反した相関ポリシー、つまりホワイト リストを含む相関ポリシーの名前。

[ポート（Port）]

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーした検出イベントに関連付けられているポート（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

[プライオリティ（Priority）]

ポリシーまたはポリシー違反をトリガーしたホワイト リストに指定されている優先度。これは、相関ポリシー内のホワイトリストの優先度または相関ポリシー自体の優先度によって決まります。ホワイトリストの優先度は、そのポリシーの優先度より優先されることに注意してください。このフィールドを検索するとき、プライオリティなしの場合は `none` を入力します。

時刻（Time）

ホワイト リスト イベントが生成された日時。このフィールドは検索できません。

ユーザ（User）

ホワイト リストに準拠しなくなったホストにログインしている既知のユーザのアイデンティティ。

ホワイト リスト（White List）

ホワイト リストの名前。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

ホワイトリスト違反の表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin/Any Security Analyst/Discovery Admin

システムは、ネットワークの現在のホワイトリスト違反のレコードを保持します。違反はそれぞれ、ホストのいずれかで実行することが禁止されている事柄を表します。ホストが準拠するようになると、システムは、修正された違反をデータベースから削除します。

Firepower Management Center を使用して、アクティブなすべてのホワイトリストに対するホワイトリスト違反のテーブルを表示できます。ここでユーザは、検索する情報に応じてイベントビューを操作することができます。

ホワイトリスト違反にアクセスしたときに表示されるページは使用しているワークフローによって異なります。事前定義されたワークフローはホストビューで終了しますが、このホストビューには、制約を満たすすべてのホストに対して1つずつホストプロファイルが含まれています。また、特定のニーズを満たす情報だけを表示するカスタムワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[Analysis]** > **[Correlation]** > **[White List Violations]**を選択します。

ステップ 2 次の選択肢があります。

- 基本的なワークフロー操作を実行するには、コンプライアンス ホワイト リスト ワークフローの使用 （6 ページ）を参照してください。
- テーブルのカラムの内容について詳しく調べるには、ホワイト リスト違反のフィールド（10 ページ）を参照してください。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

ホワイト リスト違反のフィールド

ワークフローを使用して表示および検索できるホワイトリスト違反には、次のフィールドがあります。

ドメイン

非準拠ホストが存在するドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

情報

ホワイトリスト違反に関連付けられたすべての利用可能なベンダー、製品、またはバージョン情報。ホワイトリストに違反するプロトコルの場合、このフィールドには、違反の原因がネットワーク プロトコルとトランスポート プロトコルのどちらであるのかも示されます。

[IPアドレス（IP Address）]

非準拠ホストの IP アドレス。

[ポート（Port）]

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているポート（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

プロトコル

アプリケーション プロトコル ホワイト リスト違反（非準拠アプリケーション プロトコルの結果として発生した違反）をトリガーしたイベントに関連付けられているプロトコル（存在する場合）。他のタイプのホワイト リスト違反の場合、このフィールドは空白です。

時刻（Time）

ホワイト リスト違反が検出された日時。

タイプ（Type）

ホワイト リスト違反のタイプ、つまり、非準拠の結果として違反が発生したかどうか。

- オペレーティング システム（os）（このフィールドを検索する場合は、**os** または **operating system** と入力してください）。
- アプリケーション プロトコル（サーバ）
- クライアント
- プロトコル
- Web アプリケーション（web）（このフィールドを検索する場合は、**web application** と入力してください）。

ホワイト リスト（White List）

違反されたホワイト リストの名前。

メンバー数（Count）

各行に表示される情報と一致するイベントの数。[カウント（Count）] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

修復ステータス イベント

修復がトリガーされると、システムは修復ステータスイベントをデータベースに記録します。これらのイベントは、[修復ステータス（Remediation Status）] ページで確認できます。修復ステータス イベントを検索、表示、削除できます。

関連トピック

修復ステータスのテーブル フィールド （13 ページ）

修復ステータス イベントの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

修復ステータスイベントにアクセスするときに表示されるページは、使用するワークフローにより異なります。修復のテーブル ビューを含む定義済みワークフローを使用できます。テーブル ビューには、各修復ステータス イベントの行が含まれます。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[Analysis]** > **[Correlation]** > **[Status]**を選択します。

ステップ 2 オプションで、時間枠の変更の説明に従って、時間範囲を調整します。

ステップ 3 オプションで、カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] をクリックします。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 4 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド （13 ページ）を参照してください。

- イベントをソートしたり、制約したりするには、ワークフローの使用を参照してください。
- 相関イベント ビューに移動し関連するイベントを確認するには、[相関イベント（Correlation Events）] をクリックします。
- 現在のページにすぐに戻れるようにページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。ブックマークの管理ページに移動するには、[ブックマークの表示（View Bookmarks）] をクリックします。
- テーブル ビューのデータに基づいてレポートを生成するには、イベント ビューからのレポート テンプレートの作成 で説明されているように、[レポート デザイナ（Report Designer）] をクリックします。
- ワークフローの次のページにドリルダウンするには、ドリルダウン ページの使用を参照してください。
- システムから修復ステータスイベントを削除するには、削除するイベントの横にあるチェックボックスをオンにして [削除（Delete）] をクリックするか、[すべて削除（Delete All）] をクリックして現在の制約されているビューにあるすべてのイベントを削除することを確認します。
- 修復ステータス イベントを検索するには、[検索（Search）] をクリックします。

関連トピック

ワークフローの使用

修復ステータスのテーブル フィールド

次の表に、表示および検索できる修復のステート テーブルのフィールドを示します。

表 *2*: 修復ステータス フィールド

フィールド	説明
ドメイン	監視対象のトラフィックがポリシー違反をトリガーとして使用し、次に修復をトリガーとして使用するデバイスのドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.
ポリシー	違反し、修復をトリガーとして使用した相関ポリシーの名前。
修復名	起動された修復の名前。

フィールド	説明
結果メッセージ	修復が起動したときに発生した事象を示すメッセージ。ステータス メッセージには以下が含まれます。 • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error カスタム修復モジュールがインストールされている場合、カスタム モジュールによって実装される追加のステータス メッセージが表示される場合があります。
ルール（Rule）	修復をトリガーとして使用したルールの名前。
時刻（Time）	Firepower Management Centerが修復を起動した日付と時刻。
メンバー数（Count）	各行に表示される情報と一致するイベントの数。[カウント（Count）]フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。このフィールドは検索できません。

関連トピック

イベントの検索

修復ステータス イベント テーブルの使用

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	任意（Any）	任意（Any）	任意（Any）	Admin

イベント ビューのレイアウトを変更したり、ビュー内のイベントをフィールド値で制限したりできます。

カラムを無効にすると、そのカラムは（後で元に戻さない限り）そのセッションの期間中は無効になります。最初のカラムを無効にすると、[カウント（Count）] カラムが追加されます。

テーブル ビューの行内の値をクリックすると、テーブル ビューが制約されます（次のページにはドリルダウンされません）。

ヒント テーブル ビューでは、必ずページ名に「Table View」が含まれます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

手順

ステップ 1 **[Analysis]** > **[Correlation]** > **[Status]**を選択します。

ヒント 修復のテーブル ビューが含まれないカスタム ワークフローを使用する場合、ワークフローのタイトルの横の [(ワークフローの切り替え)（(switch workflow)）] メニューをクリックし、[修復ステータス（Remediation Status）] を選択します。

ステップ 2 次の選択肢があります。

- 表示されるカラムの詳細については、修復ステータスのテーブル フィールド （13 ページ）を参照してください。
- イベントをソートしたり、制約したりするには、ワークフローの使用を参照してください。