AXIS Perimeter Defender

AXIS Perimeter Defender

AXIS Perimeter Defender PTZ Autotracking

ユーザーマニュアル

AXIS Perimeter Defender

目次

AXIS Perimeter Defender

AXIS Perimeter Defender

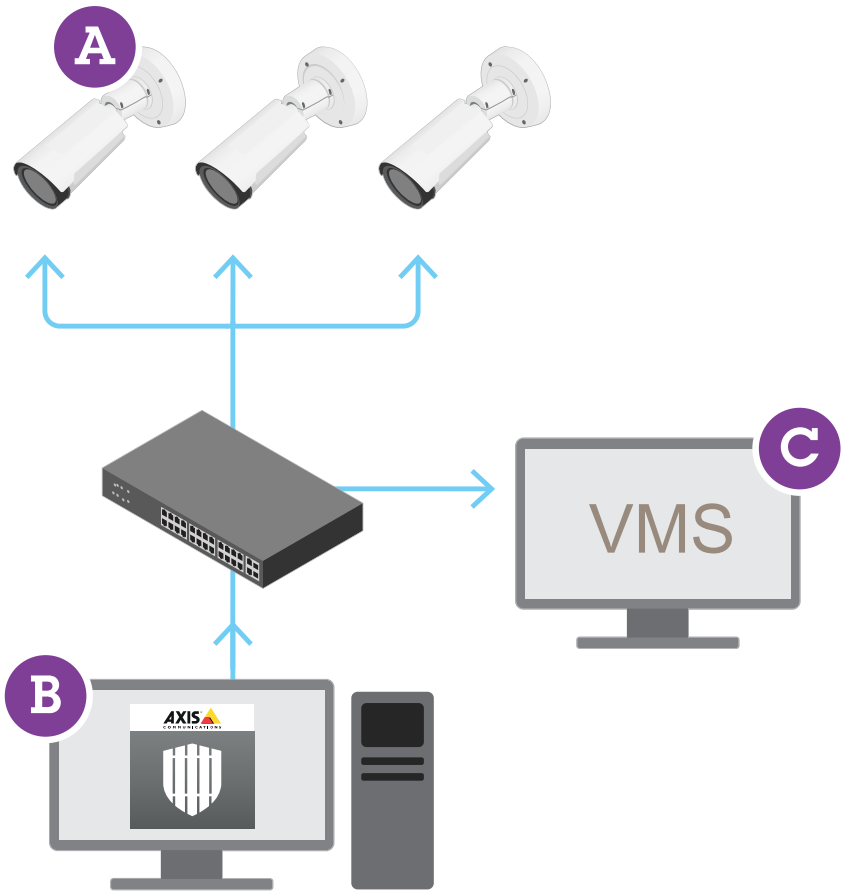
AXIS Perimeter Defender

AXIS Perimeter Defenderは、周辺監視および周辺保護に適したアプリケーションです。信頼性の高い侵入検知であるため、物理アクセスコントロールシステムを強化する必要がある高度なセキュリティエリアの周辺保護に最適です。

AXIS Perimeter Defenderは、境界を示すフェンス沿いなど、主に立入制限ゾーンの保護を目的として設計されています。「立入制限ゾーン」とは、普段人がいるべきでないエリアのことです。

屋外環境でAXIS Perimeter Defenderは次の用途に使用できます。

- 移動する人物を検知する。
- 移動する車両を検知する。車両のタイプは区別しない。



AXIS Q1951-EおよびAXIS Q1952-Eサーマルカメラは、アプリケーションをキャリブレーションモード、AIモード、またはそれら両方のモードの組み合わせで実行できます。AIモードでのみの動作を選択した場合、カメラの取り付けはより柔軟になり、カメラをキャリブレーションする必要はありません。

AXIS Perimeter Defender

AXIS Perimeter Defender

AXIS Perimeter Defenderの構成内容にはデスクトップインターフェース (B) が含まれ、ここからカメラ (A) のアプリケーションをインストールして設定します。その後、ビデオ管理ソフトウェア (C) にアラームを送信するようにシステムを設定します。

AXIS Perimeter Defender PTZ Autotracking は、同じデスクトップインターフェースを使用するAXIS Perimeter Defenderアプリケーション用のプラグインです。プラグインを使用すると、固定のビジュアルカメラまたはサーマルカメラをAxis Q-line PTZカメラとペアリングできます。これにより、固定カメラを使用してシーンの継続的な検知範囲を維持しながら、PTZカメラを使用して自動追跡し、検知した物体をより詳細に確認することができます。

重要

AXIS Perimeter Defender PTZ Autotrackingには、固定カメラとPTZカメラの両方のキャリブレーションが必要です。

AXIS Perimeter Defenderは以下のタイプの検知シナリオを提供しています。

- **侵入**: 人物または車両が地面上の定義されたゾーンに (任意の方向と軌道により) 入ると、アラームをトリガーします。
- **徘徊**: 人物または車両が地面上の定義されたゾーンに、あらかじめ定義した秒数より長く留まるとアラームをトリガーします。
- **ゾーン横断**: 人物または車両が地面上の2つ以上の定義されたゾーンを指定されたシーケンスで通過するときにアラームをトリガーします。
- **条件付き**: 人物または車両が最初に地面上の定義された他のゾーンを通過することなく地面上の定義ゾーンに入ると、アラームをトリガーします。

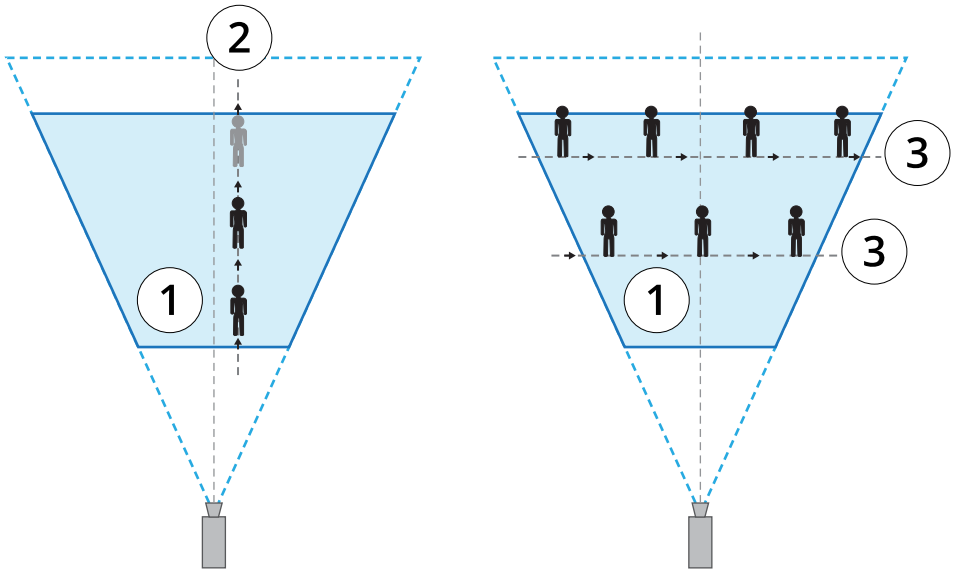
仕組み

物体の検知

AXIS Perimeter Defenderは、移動する人物や車両を検知できます。検知されるには :

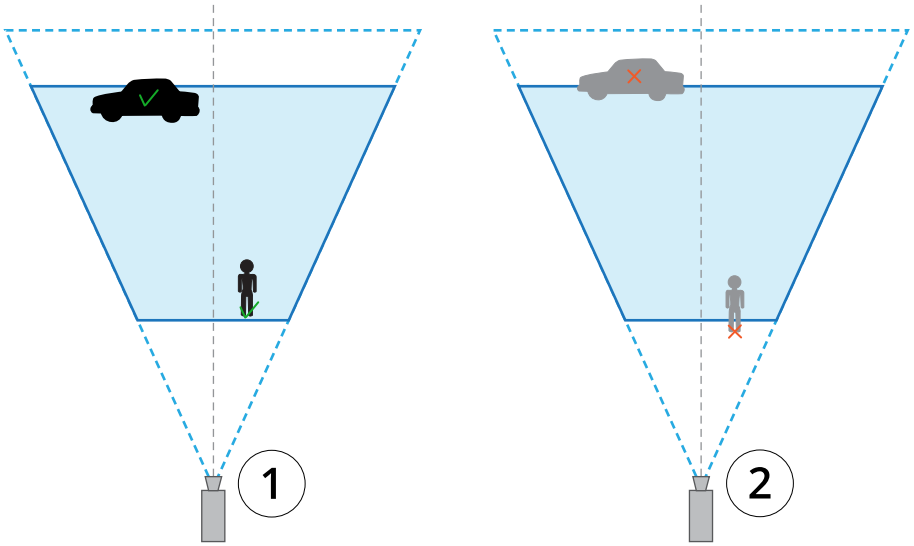
- 人物または車両は、少なくとも3秒間、検知ゾーンで完全に表示されている必要があります。
- 最大12メートルの長さの車両まで検出できます (AIモードでは、最大長はありません)。
- カメラの視野から見て、人物や車両の移動が見えている必要があります。つまり、カメラの視野に対して垂直に歩行する人物より、カメラに対して直線的に近づいたり遠ざかったりする人物の方が検知率が低くなります。

AXIS Perimeter Defender



1 検知ゾーン
2 カメラから遠ざかる人物
3 カメラの視野に対して垂直に歩行する人物

- 検出ポイントは検知ゾーンの内側になければなりません。検知ポイントは、人物の場合は足元、車両の場合はその中心です。



1 検知ポイントが検知ゾーンの内側にある
2 検知ポイントが検知ゾーンの外側にある

AXIS Perimeter Defenderは一度検出すると、たとえば人物の体が車の後ろに隠れていて、その人物の頭だけが見えているといった、部分的に隠れてる状態でも人または車の追跡を続けます。

検知された人物や車両が数秒間動いていない場合、AXIS Perimeter Defenderは追跡を停止します。15秒間以内に移動を再開した場合、アプリケーションは追跡を継続します。その人物がゾーン横断ゾーンにいた場合は、シナリオが正しくトリガーされる保証はありません。

AXIS Perimeter Defender

PTZ Autotrackingの仕組み

AXIS Perimeter Defender PTZ Autotrackingでは、固定カメラとPTZカメラが連携して動作します。固定カメラが移動する人物や車両を検知すると、その物体の場所データをペアリングされたPTZカメラに送信します。これにより、PTZカメラで以下を自動的に行うことができます。

- 物体を追跡する、および
- ズームレベルを調整し、すべての物体がビューに収まり続けるようにする

物体が固定カメラの視野内にある限り行われます。

検知が遅延または見逃される状況

- 霧
- カメラへの直接の光の照射
- 照明が不適切
- 過度にノイズが多い画像

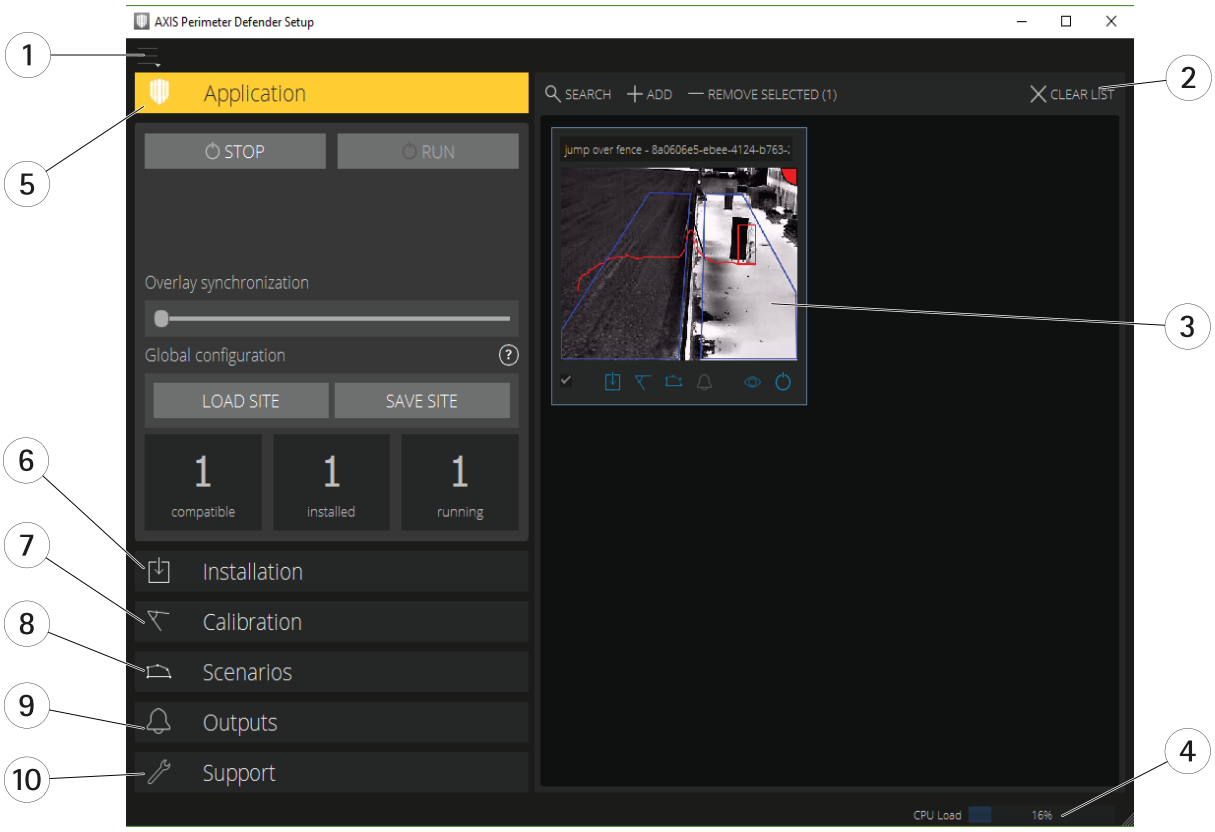
誤報をトリガーする可能性がある状況

- 人物または車両が一部隠れている。たとえば、壁の後ろから見える小型のバンは、目に見える部分が高く幅が狭いため、人物のように見えることがあります。
- カメラレンズ上の昆虫。赤外線スポットライトを搭載したデイナイトカメラは、昆虫やクモを引き寄せることに注意してください。
- 車のヘッドライトと激しい雨の組み合わせ。
- サイズが人と同じくらいの動物。特に**シナリオ**タブで、追加のアプローチタイプとしてしゃがむ/這う、または寝転がるが選択されている場合
- 影の原因となる強い照明。

ユーザーインターフェース

AXIS Perimeter Defenderインターフェースでは、デバイスのキャリブレーション、シナリオの設定、複数のデバイスに対するアクションの実行などを行うことができます。リモート設定を使用すると、ネットワーク接続があればどこからでも設定を行うことができます。

AXIS Perimeter Defender



1 7ページインターフェースの設定
2 デバイスを処理します。18ページデバイスを追加する を参照してください。
3 8ページライブビュー
4 CPU loadインジケーター。12ページCPU負荷 を参照してください。
5 9ページアプリケーションタブ
6 10ページインストールタブ
7 10ページキャリブレーションタブ
8 10ページシナリオタブ
9 11ページ出力タブ
10 11ページサポートタブ

インターフェースの設定

インターフェース設定メニューには以下が含まれます。

フォルダーの設定 -
デバイス設定パス: 一時ファイルとキャリブレーション映像の保存場所を選択します。
サイト設定パス: 読み込みパスからの設定ファイルの保存場所を選択します。

カメラのパスワード - 使用されるパスワードの確認と、新しいパスワードを追加することができます。ユーザーがアプリケーションを終了すると、パスワードは破棄されます。

デモクリップパッケージの管理 - デモクリップをインポートまたは削除します。

フルフレームレートモードを有効にする - ライブビューのフレームレートを変更します。*12ページCPU負荷* を参照してください。

フィートとインチの表示 - メートル法とヤード法の単位を変更します。

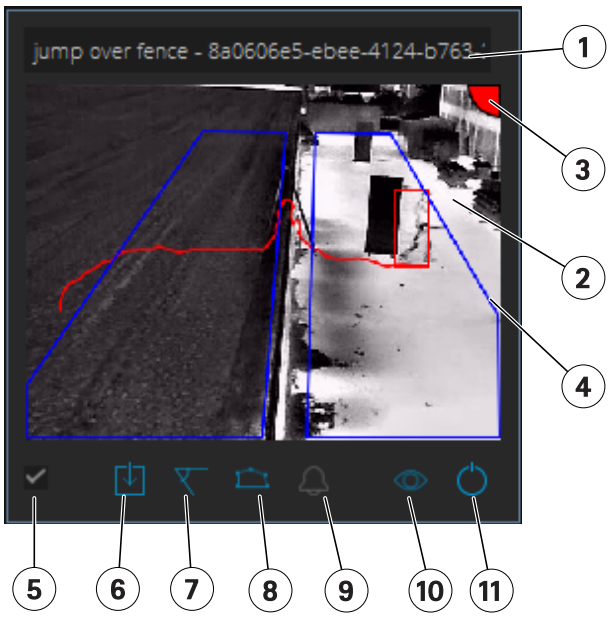
言語を変更 - アプリケーションの言語を変更します。

AXIS Perimeter Defender

バージョン情報 - AXIS Perimeter Defender Setupのバージョン番号を表示します。

ライブビュー

メインのインターフェースで、接続された各デバイスのライブ映像を確認できます。ライブビューではデバイスステータスを確認したり、主要機能に簡単にアクセスしたりすることができます。



1. **デバイス名** - デバイス名を編集するにはクリックします。デバイスのIPアドレスとMACアドレスが含まれます。名前にマウスポインターを置くと、分析に使用するアスペクト比が表示されます。これにより最大の視野範囲が得られ、また、デバイスがリモート接続上にあるかどうかを確認できます。

2. **ライブ映像** - オーバービューモードでは、フレームレートは1 fpsです。ダブルクリックすると画像が最大化され、フレームレートが8 fpsになります。

3. **アラームステータス** - アラームステータスは、オーバーレイがアクティブで、AXIS Perimeter Defenderがインストール、設定、および実行されている場合にのみ表示されます。灰色は、アラーム機能がアクティブでないか、構成設定を読み込み中であることを意味します。緑色は、アラーム機能がアクティブであることを意味します。赤色は、アラームがトリガーされたことを意味します。

4. **検知ゾーン** - 検知ゾーンは、オーバーレイがアクティブであり、AXIS Perimeter Defenderがインストール、設定、および実行されている場合にのみ表示されます。

5. **選択チェックボックス** - 複数のデバイスを選択できるようにするには、このチェックボックスを使用します。

6. **インストールステータスとクイックアクセスボタン** - マウスポインターを置くと、デバイスにインストールされているAXIS Perimeter Defenderのバージョンが表示されます。アイコンが に置き換えられている場合は、より新しいバージョンがあることを表します。クリックすると、デバイスのインストールタブが開きます。灰色は、デバイスがインストールされていないことを意味します。オレンジ色は、デバイスがインストールされているものの、有効なライセンスを持っていないことを意味します。青色は、デバイスがインストールされ、有効なライセンスがあることを意味します。

7. **キャリブレーションステータスとクイックアクセスボタン** - クリックすると、デバイスのキャリブレーションタブが開きます。灰色は、デバイスがキャリブレーションされていないことを意味します。青色は、デバイスがキャリブレーションされていることを意味します。

AXIS Perimeter Defender

8. シナリオのステータスとクイックアクセスボタン - クリックすると、デバイスのシナリオタブが開きます。灰色は、シナリオが定義されていないことを意味します。青色は、少なくとも1つのシナリオが定義されていることを意味します。

9. 出力ステータスとクイックアクセスボタン - クリックすると、デバイスの出力タブが開きます。灰色は、出力が設定されていないことを意味します。青色は、少なくとも1つの出力が設定されていることを意味します。

10. オーバーレイステータスとトグルボタン - クリックすると、オーバーレイのオン/オフを切り替えます。灰色は、オーバーレイが非アクティブであることを意味します。青色は、オーバーレイがアクティブであることを意味します。オーバーレイは、検知した物体を囲う境界ボックス、および物体の軌道を示す「スネイルトレイル」として表示されます。

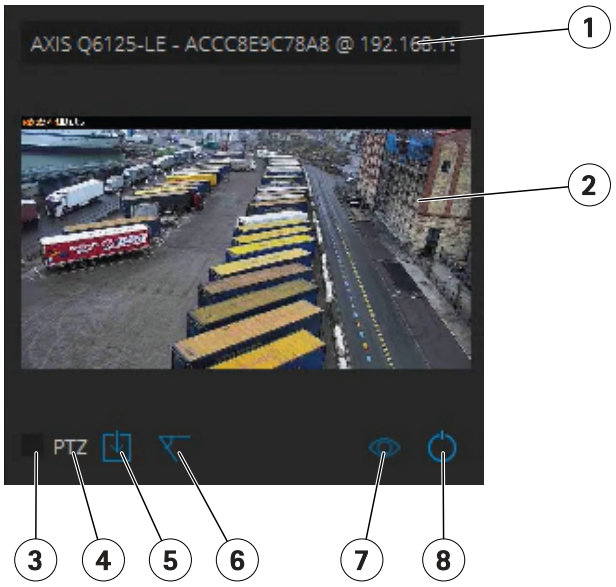
11. 実行中ステータスとトグルボタン - クリックすると、デバイス上のアプリケーションを実行/停止します。灰色は、アプリケーションが停止していることを意味します。青色は、実行中であることを意味します。

注

オーバーレイは、デバイスからユーザーのコンピューターへの直接接続が使用可能な場合、つまり、デバイス上のオーバーレイポートへの接続を妨げるファイアウォールなどがない場合にのみ使用できます。

ライブビュー - PTZ Autotracking

AXIS Perimeter Defender PTZ Autotrackingがインストールされているデバイスのライブビューは、通常のライブビューとはわずかに異なります。



1 *デバイス名*
2 *ライブ映像*
3 *選択チェックボックス*
4 *デバイスがAXIS Perimeter Defender PTZ Autotrackingを使用することを示します*
5 *インストールステータスとクイックアクセスボタン*
6 *キャリブレーションステータスとクイックアクセスボタン*
7 *オーバーレイステータスとトグルボタン*
8 *実行中ステータスとトグルボタン*

アプリケーションタブ

- **Run (実行)** – 選択したデバイスで分析を開始します。

AXIS Perimeter Defender

- **Stop (停止)** – 選択したデバイスで分析を中止します。
- **Load Site (拠点の読み込み)** – 以前に保存した拠点 (デバイスと各設定ファイル) を読み込みます
- **Save Site (拠点の保存)** – 現在の拠点 (すべてのデバイス情報と各設定ファイル) を保存します
- **Overlay synchronization (オーバーレイ同期)** - AXIS Perimeter Defenderのメタデータオーバーレイ同期を制御します。このスライダーは、メタデータオーバーレイと受信画像の間の遅延をコントロールし、メタデータと比べて画像ストリーミングが低速の場合に補正を行います。スライダーの値は、現在選択されているカメラの遅延設定を示します。複数のカメラが接続されている場合は、最初に選択したカメラの値が示されます。スライダーの値を変更すると、選択したすべてのカメラで遅延が変化します。

また、互換性のある追加デバイスの数、AXIS Perimeter Defenderがインストールされているデバイスの合計数、および分析が実行中であるデバイスの数を確認することもできます。

インストールタブ

- **アプリケーション : インストール** — 選択したデバイスにアプリケーションをインストールします。
- **アプリケーション : アンインストール** — 選択したデバイスからアプリケーションをアンインストールします。
- **ライセンス : インストール** — 選択したデバイスにライセンスをインストールします。

キャリブレーションタブ

- **Automatic (自動)** — 選択したデバイスの自動キャリブレーションを実行します。
- **Manual (手動)** — 選択したデバイスの手動キャリブレーションを実行します。

シナリオタブ

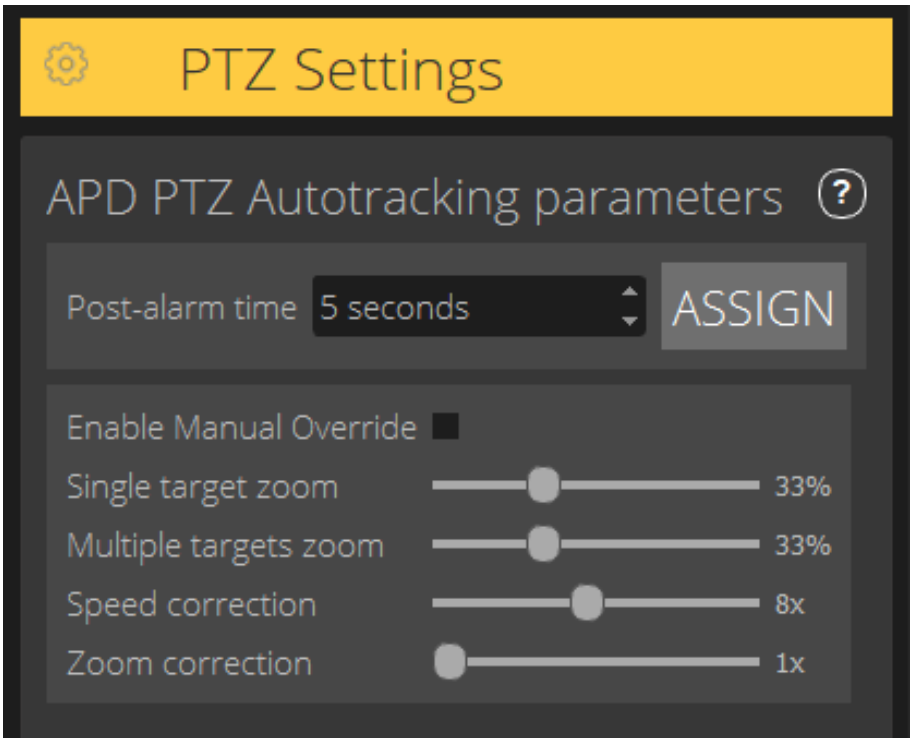
- **グローバルパラメーター** — すべてのシナリオに適用します。
- **高度なシナリオ** — 侵入、徘徊、ゾーン横断、および条件付きシナリオを作成します。

PTZ設定タブ

注

このタブは、プラグインのAXIS Perimeter Defender PTZ Autotrackingを使用している場合にのみ表示されます。

AXIS Perimeter Defender



- **Post-alarm time (ポストアラーム時間)** – 追跡した物体がビューから消えた後、PTZカメラがホームポジションに戻るまでの時間を定義します。
- **Enable manual override (手動オーバーライドの有効化)** – オンにすると、オペレーターはジョイスティックを使用し、VMSまたはカメラのWebページでPTZカメラの制御を行うことができます。
- **Single target zoom (単一ターゲットのズーム)** – 単一ターゲットを追跡するズームレベルを調整します。値を大きくすると識別が向上する可能性がありますが、急速に移動する物体を見失うリスクも高まります。
- **Multiple target zoom (複数ターゲットのズーム)** – 複数のターゲットを追跡するズームレベルを調整します。
- **Speed correction (スピード補正)** – 追跡速度を調整し、急速に移動する物体をPTZカメラ画像の中央に収め続けます。値を大きくすると、追跡が不安定になる可能性があります。
- **Zoom correction (ズーム補正)** – 値を大きくすると、PTZカメラの視野の端に近い物体に対するズームアウトが大きくなります。

出力タブ

- **設定** — デバイスのWebページを開き、アラームを作成して設定します。
- **テストアラーム** — デバイスで設定されたアラームをテストします。
- **ポストアラーム時間: 割り当て** — ポストアラーム時間を設定します。

サポートタブ

- **Load (読み込み)** — 選択したデバイスのバックアップ設定を読み込みます。デバイスに障害が発生した場合や誤ってアンインストールしてしまった場合に迅速にリストアするのに特に役立ちます。この設定に含まれるもの :

- ライセンス
- パラメーター
- キャリブレーションとシナリオ
- キャリブレーション映像

- **Save (保存)** — 選択したデバイスの設定のバックアップを作成します。
- **Clear (クリア)** — 選択したデバイスからキャリブレーションとシナリオを消去します。これは、カメラが移動した場合に役立ちます。カメラを移動するとキャリブレーションや検知ゾーンが有効でなくなるためです。
- **View application log (アプリケーションログの表示)** — AXIS Perimeter Defenderの内部ログを表示します。
- **Export support log (サポートログのエクスポート)** — 詳細な情報を含むサポートファイルを生成します。このファイルは常にサポートリクエストと共に含めます。

CPU負荷

CPU負荷インジケーターは、現在のコンピューターのCPU負荷をリアルタイムで示します。CPU負荷が高すぎると、コンピューターまたはアプリケーションが応答しなくなる可能性があります。AXIS Perimeter Defender Setupを使用する際には他のアプリケーションを閉じ、CPUの割り当てを最大化するようにしてください。CPU負荷が高すぎる状態でデバイスを追加しようとすると、システムで警告が出されます。

追加されているデバイスはホストコンピューターのCPUリソースを使用し、カメラからのビデオストリームをデコードして表示します。ホストコンピューターへの影響を制限するため、追加デバイスからのビデオストリームは、デフォルトではフレームレートを下げた状態 (約1 fps) で表示されます。ストリーム映像を最大化したとき、またはキャリブレーション処理中は通常のフレームレート (約8 fps) が復元されます。

重要

[Enable full frame rate mode (フルフレームレートモードを有効にする)] は、多数のカメラに接続する場合や処理能力の低いコンピューターを使用する場合、インターフェースが応答しなくなる可能性があります。

AXIS Perimeter Defenderのデモを表示する

デモに使用できるよう、AXIS Perimeter DefenderおよびAXIS Perimeter Defender PTZ Autotrackingには、設置済みのアクティブなカメラがなくても分析のデモに使用できるいくつかのデモクリップがプリインストールされています。デモクリップは、さまざまな環境で予想される検知の種類とオートトラッキングの結果を表示します。

1. [Application > Add > Demo Clips (アプリケーション > 追加 > デモクリップ)] をクリックし、以下の操作を1つまたは複数行います。
   - タイプに応じてデモクリップをフィルタリングします。
   - 少なくとも1つのデモクリップを選択してください。
2. デモクリップを追加するには、[Add Selected Demo Clips (選択したデモクリップを追加)] をクリックします。

追加すると、デモクリップは標準のビデオストリームとしてインターフェースに表示されます。キャリブレーションは完了し、分析もすでに有効になっているため、ユーザーはビデオストリームで分析とオートトラッキングの結果をすぐに確認できます。ライブビューで実行中ステータスをクリックするか、左側のペインで [Run (実行)] ボタンまたは [Stop (停止)] ボタンをクリックすると、分析やオートトラッキングを停止したり、開始したりすることができます。

キャリブレーションとペアリングは、変更してやり直すことができます。同様に、検知シナリオも追加、削除、変更することができます。

AXIS Perimeter Defender

左ペインの [Support (サポート)] タブにある [Clear (クリア)] ボタンをクリックすると、キャリブレーションやシナリオを元の値に戻すことができます。キャリブレーションを完全に削除することはできません。

AXIS Perimeter Defender

はじめに

はじめに

AXIS Perimeter DefenderとAXIS Perimeter Defender PTZ Autotrackingのインストール手順はわずかに異なります。

AXIS Perimeter Defenderで作業を開始する

AXIS Perimeter Defenderを使用してサイトを立ち上げるには、次の手順を実行する必要があります :

1. カメラを設置します。*15ページカメラを取り付ける* を参照してください。
2. お使いのコンピューターにソフトウェアをダウンロードしてインストールします。*18ページコンピューターにソフトウェアをインストールする* を参照してください。
3. デバイスに接続します。*18ページデバイスを追加する* を参照してください。
4. AXIS Perimeter Defenderを各デバイスにインストールします。*20ページデバイスにソフトウェアをインストールする* を参照してください。

注

AIモードでのみ動作するデバイスをキャリブレーションする必要はありません。デバイスをキャリブレーションモードとAIモードで同時に実行するには、デバイスをキャリブレーションする必要があります。

5. デバイスをキャリブレーションします。*20ページキャリブレーション - AXIS Perimeter Defender* を参照してください。
6. シナリオを追加して、アラームをトリガーする対象のルールを定義します。*29ページシナリオを定義する* を参照してください。
7. 送信するアラームを設定します。*34ページ出力を定義する* を参照してください。

AXIS Perimeter Defender PTZ Autotrackingで作業を開始する

AXIS Perimeter Defender PTZ Autotrackingを使用してサイトを立ち上げ実行するには、次の手順を実行する必要があります :

1. カメラを取り付けます。詳細については、*15ページカメラを取り付ける* および *17ページPTZカメラを取り付ける* を参照してください。
2. お使いのコンピューターにソフトウェアをダウンロードしてインストールします。*18ページコンピューターにソフトウェアをインストールする* を参照してください。
3. デバイスに接続します。*18ページデバイスを追加する* を参照してください。
4. 固定カメラにAXIS Perimeter Defenderバージョン2.5.0以降をインストールし、PTZカメラにAXIS Perimeter Defender PTZ Autotrackingをインストールします。*20ページデバイスにソフトウェアをインストールする* を参照してください。
5. デバイスをキャリブレーションしてシナリオを設定します。*28ページキャリブレーション - PTZ Autotracking* を参照してください。
6. デバイスをペアリングします。*32ページカメラをペアリングする - PTZ Autotracking* を参照してください。
7. 送信するアラームを設定します。*34ページ出力を定義する* を参照してください。

はじめに

カメラを取り付ける

設計ツールについて

現場でのカメラの配置を指定するには、AXIS Perimeter Defender用の設計ツール (Design Tool for AXIS Perimeter Defender) を使用することをお勧めします。このツールではAxisカメラとAXIS Perimeter Defenderの両方の要件が考慮されています。このツールは次のことを決定するのに役立ちます :

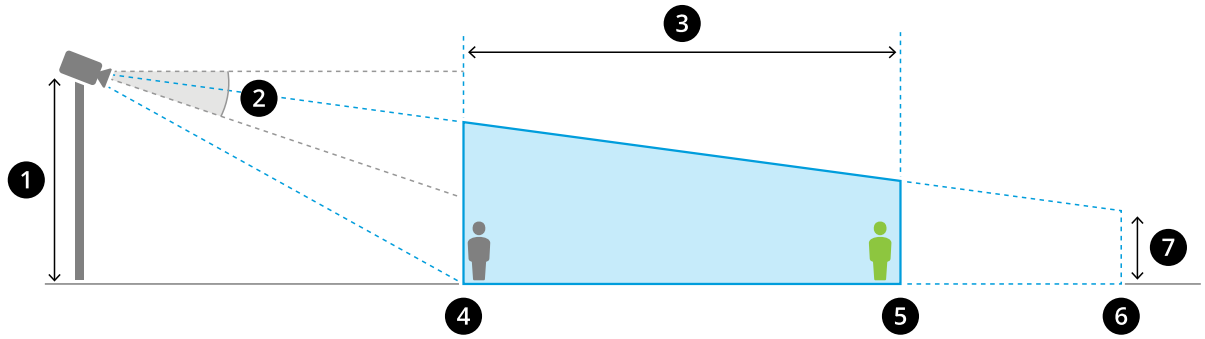
- カメラの設置高さ
- チルト角度
- 最小検知距離
- 最大検知距離

ツールをダウンロードするには、*axis.com/products/axis-perimeter-defender*にアクセスしてください

カメラの取り付けに関する推奨事項

注

AIモードでのみ動作するカメラの場合、取り付けに関する推奨事項はアプリケーションで参照できます。



適切に取り付けられたカメラ。

1 取り付け位置の高さ
2 チルト
3 検知ゾーン
4 最小検知距離
5 最大検知距離
6 視野の距離
7 視野の仰角

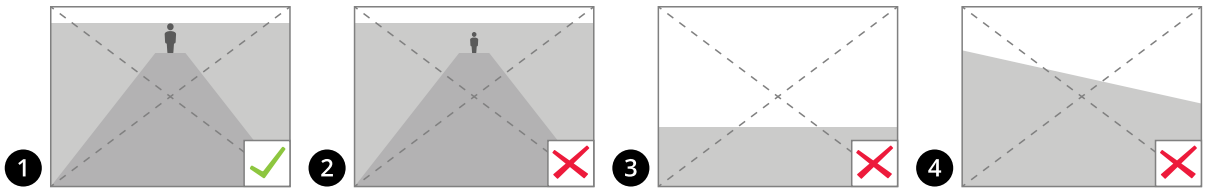
最大検知距離にある物体の高さ - 最大検知距離に立っている人を検知するには、ピクセルの高さが画像全体の高さの5%以上 (サーマルカメラでは3.5%以上) である必要があります。たとえば、写っている画像の高さが576ピクセルの場合、検知ゾーンの終端に立っている人の高さは28ピクセル (サーマルカメラでは20ピクセル) 以上である必要があります。

最小検知距離にある物体の高さ - 最小検知距離に立っている人を検知するには、ピクセルの高さが画像全体の高さの60%以下でなければいけません。

AIモードで実行時の物体の高さ - アプリケーションをAIモードで実行するとき、物体は検出されるアバターと同じかそれ以上のサイズであることが必要です。

チルト角度 - カメラは画像の中心が水平線より下に来るように、十分地面の方に向ける必要があります。最小検知距離がカメラの設置高さの半分より長くなるようにカメラを取り付けます (最小検知距離 > カメラの設置高さ/2)。

ロール角 - カメラのロール角はほぼ0にする必要があります。



1 物体の高さ、チルト角度、ロール角が適切です。
2 最大検知距離にある物体の高さが、画像の高さの5%未満 (サーマルカメラの場合は3.5%未満) になってしまっています。
3 画像の中心が水平線より上にきてしまっています。
4 カメラのロール角がほぼ0ではありません。

最大検知距離は次の条件に依存します :

- カメラの種類とモデル
- カメラレンズ。焦点距離が長ければ長いほど、検知距離も長くなります。
- 検知するために必要な、人物の最小ピクセルサイズ。立っている人のピクセルの高さが、可視光カメラでは画像の高さの最低5%、サーマルカメラでは最低3.5%である必要があります。
- 気象条件
- 照明
- カメラの負荷

カメラを取り付けるときは、次の点を考慮してください :

- 振動。本アプリケーションはカメラの小さな振動を許容しますが、カメラが振動の影響を受けない場合に最高のパフォーマンスが得られます。
- 視野。カメラの視野は固定する必要があります。

シーンの要件

注

AIモードでのみ動作するカメラの場合、シーン要件はアプリケーションで参照できます。

検知ゾーンは以下の条件を満たす必要があります。

- 視野がはっきりとしている
- 地面が平坦であるか、わずかな傾斜しかない
- 動きによって照明がトリガーされない
- 視野がはっきりとしている
- 可視光カメラの場合、人物、車両、背景の間で十分なコントラストが得られるだけの十分な照明レベルと画像の設定である必要があります。
  - 人工照明でAxisのデイナイトカメラを使用する場合は、検知ゾーン全体が50ルクス以上であることをお勧めします。
  - 外付けの赤外線スポットライトを使用する場合、最大検知距離は80 mとし、赤外線スポットライトの照射範囲は最大検知距離の2倍以上にすることをお勧めします。

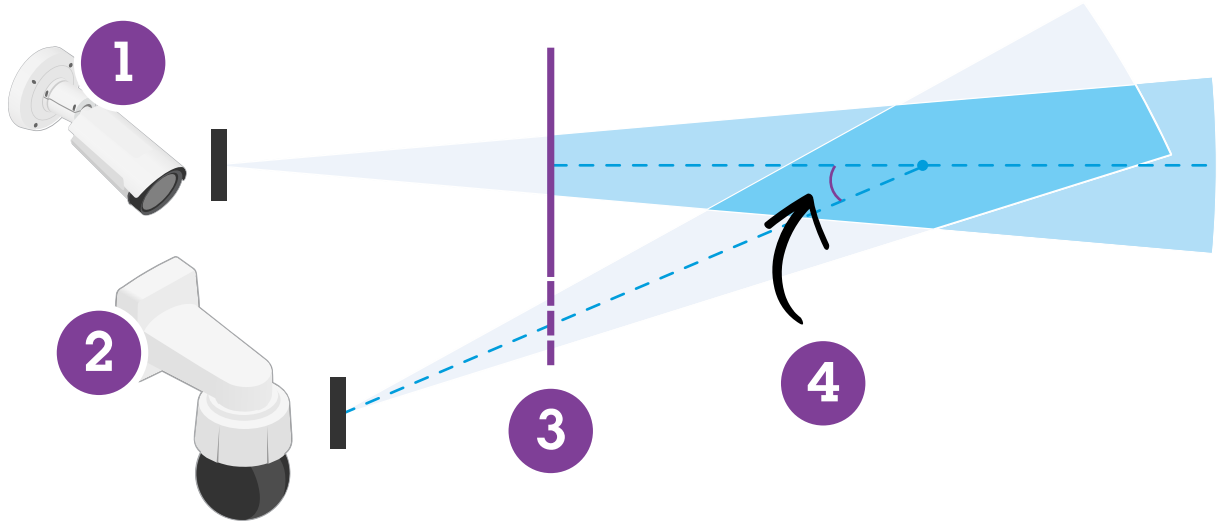
- カメラ内蔵の赤外線照明を使用する場合、カメラと環境に応じて、最大検知距離が最大20 mに制限されます。

- サーマルカメラの場合、背景と前景の間に高いコントラストが必要となります

検知パフォーマンスを最適化するため、AXIS Perimeter Defenderは日中と夜間の差を自動的に学習し、この情報を使用して検知アルゴリズムを微調整します。微調整には約24時間かかるため、アプリケーションをその時間実行すると、日中と夜間の両方で最適な検知が行われます。

PTZカメラを取り付ける

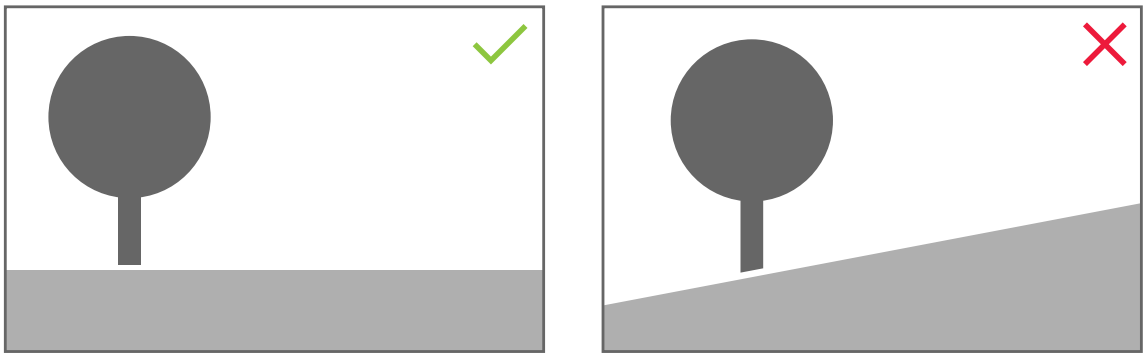
この章では、固定カメラに関連してPTZカメラを取り付ける方法について説明します。固定カメラの取り付け方法については、*15ページカメラを取り付ける*を参照してください。



1 固定ネットワークカメラ
2 PTZネットワークカメラ
3 最小検知距離
4 カメラ間の角度

- PTZカメラのホームプリセットポジションは、固定カメラの検知ゾーンの60%超をカバーする必要があります。
- PTZカメラで追跡するには、起立している人物がPTZカメラの画像の高さの4%以上をカバーする必要があります。
- PTZカメラは、固定カメラの最小検知距離より手前に配置する必要があります (C)。
- 固定カメラとPTZカメラの間の角度は、30°未満でなければなりません (D)。

はじめに



- 地面は平坦でなければなりません。

コンピューターにソフトウェアをインストールする

1. *axis.com/products/axis-perimeter-defender*からAXIS Perimeter Defenderソフトウェアをダウンロードします
2. お使いのコンピューターにソフトウェアをインストールします。

デバイスを追加する

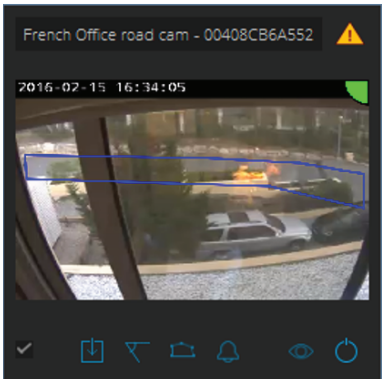
AXIS Perimeter Defenderアプリケーションへのデバイスの追加は、次の3つの方法で行えます。

- ネットワークスキャンにより自動的に実行する。*19ページデバイスを自動で追加する*を参照してください。
- 接続設定を指定して手動で実行する。*19ページデバイスを手動で追加する*を参照してください。
- 以前保存したサイトを読み込んで自動的に実行する。*20ページ既存のサイトを読み込む*を参照してください。

デバイスを追加すると、デバイスにインストールされている他のアプリケーションのリストが表示されます。必須でないアプリケーションはカメラのCPUリソースを消費し、AXIS Perimeter Defenderのパフォーマンスに影響を与え正しくインストールできくなる可能性があるため、不要なアプリケーションは停止することをお勧めします。

他のアプリケーションが実行中であるなどの理由でデバイスに十分なCPUリソースがない場合、AXIS Perimeter Defenderはフレームレートを低下させます。フレームレートが5フレーム/秒未満の場合、警告を示す黄色の三角形がライブビューのデバイス名の隣に表示されます。三角形にマウスポインターを置くと、現在のフレームレートが表示されます。

はじめに



注

フレームレートが5 fps未満になると、ビデオ分析のパフォーマンスが大幅に低下する可能性があります。これは、検知漏れや誤検知を引き起こす要因となります。

詳細については、*12ページCPU負荷*を参照してください。

デバイスを自動で追加する

重要

検索機能はネットワーク間では機能しません。つまり、AXIS Perimeter Defender Setupは、ソフトウェアを実行しているクライアントと同じサブネットワークに接続されたデバイスのみを検索できます。別のサブネットワークに接続されているデバイスを追加するには、手動でそのデバイスを追加します。ネットワークルーターまたはスイッチがマルチキャストをフィルタリングするように設定されている場合、検索機能が失敗する可能性があります。

1. 周辺のネットワークでデバイスをスキャンするには、[**Application（アプリケーション）**] に移動して [**Search（検索）**] をクリックします。

   初めて検索を実行し、使用可能なパスワードがない場合は、パスワードダイアログが開きます。それ以外の場合は、使用可能なパスワードを使用してデバイスに接続します。

2. デバイスを選択し、[**Add selected devices（選択したデバイスの追加）**] をクリックします。

   パスワードが正しい場合は、デバイスの選択時にユーザーをガイドする静的画像が表示されます。

デバイスを手動で追加する

1. [**Application（アプリケーション）**] に移動し、[**Add（追加）**] をクリックします。
2. 次を入力します。
   - デバイスのIPアドレスまたはホスト名。
   - デバイスのルートパスワード。AXIS Perimeter Defenderはルートアクセスを必要とするため。
   - 接続に使用するHTTPポート。デフォルトポートは80です。
   - 認識しやすくするためのオプションのデバイス名。
   - デバイスが接続速度が遅いリモートネットワーク上にある場合は、[**Device on remote network（リモートネットワーク上のデバイス）**] をオンにします。低速接続がリモートとして設定されていないと、動作しなくなったり、キャリブレーションが失敗する可能性があります。

注

リモート接続ではユーザーはHTTPを介してデバイスに接続できる必要があります。HTTPポートを正しく設定していることを確認してください。接続の帯域幅が不十分または不安定な場合、リモート設定が失敗する可能性があります。

3. [OK] をクリックします。

注

ホスト名でカメラを追加できない場合は、ネットワークとDNSの設定を検証するか、IPアドレスを使用してデバイスを追加します。

既存のサイトを読み込む

以前に保存したサイト設定を読み込むには、以下を実行します。

1. [Application (アプリケーション)] に移動し、[Load site (サイトを読み込み)] をクリックします。
2. サイト設定ファイルを参照ボタンで指定し、[Open (開く)] をクリックします。ライブビューが自動的に表示されます。

デバイスにソフトウェアをインストールする

各デバイスにAXIS Perimeter Defenderをインストールする必要があります。

デバイスにインストールされているAXIS Perimeter Defenderのバージョンを確認する必要がある場合は、ライブビューで [Installation status (インストールステータス)] にマウスポインターを置きます。

デバイスにAXIS Perimeter Defenderがインストールされていない場合は、ライブビュー内のすべてのアイコンが灰色になります。

デバイスにソフトウェアをインストールする

1. [インストール] に移動します。
2. アプリケーションをインストールするデバイスを選択します。
3. 最新バージョンのAXIS Perimeter Defenderを選択し、**インストール**をクリックします。

   選択したデバイスにAXIS Perimeter Defenderがインストールされ、自動的に起動します。
4. ライセンスで参照をし、以下のいずれかの手順を実行します :
   - 1台のデバイスにインストールする場合: そのデバイスのライセンスファイルを選択します。
   - 複数のデバイスにインストールする場合: ライセンスファイルが保存されているフォルダーを選択します。
5. **インストール**をクリックします。

キャリブレーション - AXIS Perimeter Defender

キャリブレーション

注

AIモードでのみ動作するデバイスをキャリブレーションする必要はありません。デバイスをキャリブレーションモードとAIモードで同時に実行するには、デバイスをキャリブレーションする必要があります。

はじめに

AXIS Perimeter Defenderがシーンを正しく解釈するには、すべてのデバイスをキャリブレーションする必要があります。キャリブレーションの際、プロセッサーに対して奥行きと高さの情報を提供する基準点を指定します。また、対象ゾーンの定義も行います。

キャリブレーションには次の2つのタスクがあります。

1. キャリブレーションを実行します。
   - 自動 — ほとんどの場合に推奨されます。*21ページ自動キャリブレーションを実行する* を参照してください。
   - 手動 — 推奨されるのは、カメラで自動キャリブレーションが失敗した場合、微調整を行いたい場合、あるいは設置担当者がシーン内を歩き回るのが難しいが、高さがわかっている物体があるような場合です。具体的な例としては、一定の高さの支柱が等間隔に並ぶフェンスが設置された場所である場合などがあります。*26ページ手動キャリブレーションを実行する* を参照してください。
2. キャリブレーションの結果を検証します。*23ページキャリブレーションの品質を検証する* を参照してください。

大規模な拠点の設定を高速化するため、複数のデバイスを同時にキャリブレーションすることができます。キャリブレーションを単一のカメラの場合と同様に、自動または手動で実行できます。複数のデバイスを同時にキャリブレーションする前に、以下の点を考慮してください。

- 同時にインストールして設定できるデバイスの最大数は、コンピューターで使用可能なCPUの処理能力とメモリによって異なります。AXIS Perimeter Defender Setupで指定するデバイスが多すぎると、クラッシュする可能性があります。CPU過負荷の警告が表示される場合には、保存サイト機能を使用し、デバイスの一部をインストールして設定します。
- 複数のデバイスを自動キャリブレーションするには、単一デバイスの場合より多くのCPUリソースとRAMが必要になります。スペックが低いシステムでは、コンピューターがしばらく応答しなくなったり、アプリケーションがクラッシュしたりする場合があります。クラッシュする場合には、キャプチャーされた映像をその後の単一カメラのキャリブレーションに使用できます。

注

- AXIS Perimeter Defenderは、カメラで提供される最大解像度に応じ、さまざまなアスペクト比をサポートしています。そのため、解像度を変更する場合は、以前行ったキャリブレーションをすべてやり直す必要があります。ただし、カメラのWebページでストリームの解像度を変更する場合は、再キャリブレーションを行う必要はありません。
- AXIS Perimeter DefenderとVMSで同じ画像アスペクト比を使用し、表示されている情報が画像の内容に合っているようにすることをお勧めします。アスペクト比を確認するには、ライブビューでカメラ名にマウスポインターを置きます。
- キャリブレーション後にカメラが移動した場合、正しい分析結果を得るために再キャリブレーションを行う必要があります。

自動キャリブレーションを実行する

自動キャリブレーションを使用する場合、人物に撮影エリアを歩行させることで、1台以上のカメラをキャリブレーションできます。カメラは、自身のキャリブレーションに必要な情報を自動的に収集します。

自動キャリブレーションを成功させるには :

- 視野内に多くの人がいるときはキャリブレーションしないでください。
- 視野内に多数の車両が通過する場合はキャリブレーションしないでください。
- 視野内に他の移動する物体がある場合はキャリブレーションしないでください。風にあおられて動く木や旗など。
- 地面に平行に取り付けられていないカメラをキャリブレーションしないでください。

はじめに

- シーンを歩く人は、視野全体を手前から奥までカバーするように歩く必要があります。それが不可能な場合は、手動キャリブレーションに切り替えることをお勧めします。
- カメラがリモートネットワーク上にあるがリモート接続していない場合は、シーンを歩行する人物は約5分間歩行し、十分な画像がキャプチャーされるようにする必要があります。通常、リモートネットワーク上のデバイスはフレームレートが低いためです。

1. [**Calibration（キャリブレーション）**] に移動します。
2. キャリブレーションするデバイスを選択します。
3. [**Automatic（自動）**] をクリックします。
4. 録画開始時刻を設定します。キャプチャーは、シーンを歩行する人物が視野に入る少なくとも10秒前に開始する必要があります。
5. 録画時間を設定します。次の点を考慮に入れてください：
   - 人物がシーン全体を行き来するのに十分な時間が必要であること。
   - ビデオの長さは、キャリブレーションの計算に影響すること。
6. シーンを歩行する人物の身長 (cm) を入力し、[**Capture（キャプチャー）**] をクリックします。

   以前にキャプチャーした映像を再利用するには、[**Use previous capture（以前のキャプチャーを使用）**] をクリックします。
7. 以下の指示に従い、人物にシーンを歩いてもらいます：
   - シーンの手前から奥まで、検知ゾーンを可能な限り網羅するよう、ジグザグに歩く。撮影視野を横切るよう、V字型に歩くのがお勧め。
   - 視野では頭から足までほぼ完全に見える状態を保つ。
   - 直線にゆっくり進む。
   - 常に直立姿勢を保つ。
   - 方向転換する前に1～2秒間停止する。

歩行シーケンスの例。

8. 人物が正確に検知されていることを確認し、自動キャリブレーションが成功していることを検証します。*23ページキャリブレーションの品質を検証する*を参照してください。
9. キャリブレーションを保存するには [**Accept (同意)**] をクリックします。

   新しいキャリブレーションを実行するには [**New (新規)**] をクリックします。

   手動キャリブレーションを実行するには [**Manual (手動)**] をクリックします。

キャリブレーションに同意すると、最大検知ゾーンが青色の境界で示されます。最大検知ゾーンは、監視可能な最大エリアです。このエリアの外で侵入者を検知する可能性もありますが、その保証はありません。

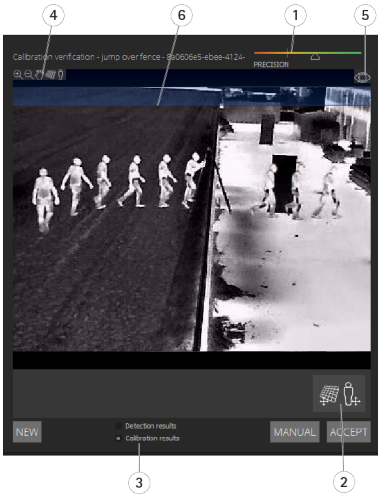
キャリブレーションの品質を検証する

キャリブレーション後、いくつかの場所にシーンを歩行する人物が表示されているはずです。人物がまったく表示されていない場合は、自動キャリブレーションに失敗しているため、やり直す必要があります。

キャリブレーションの品質は、次のいくつかの方法で検証することができます:

- キャリブレーション精度インジケーターを確認します。これは自動的に計算された精度レベルを反映しており、人がシーンをどれだけよくカバーしているか、どのくらいうまく検出されるかを表すものです。精度インジケーターが赤色ゾーン内にある場合、キャリブレーションは失敗しているため [**Accept (同意)**] をクリックできません。*26ページ手動キャリブレーションを実行する*を参照してください。
- グリッドツールを使用できます。*24ページグリッドを使用してキャリブレーションを検証する*を参照してください。
- アバターツールを使用できます。*25ページアバターを使用してキャリブレーションを検証する*を参照してください。
- 検知結果を確認できます。*26ページ検知結果を使用してキャリブレーションを検証する*を参照してください。

はじめに



1 キャリブレーション精度インジケーター
2 グリッドツールとアバターツール
3 動的ビューまたは静的ビュー
4 ビュー設定変更ツール
5 キャリブレーション画像とライブビューの切り替え
6 水平線

水平線とは、シーン内の目に見える地面の端を表します。シナリオを定義する場合、地平線より上の青い領域にシナリオゾーンを配置することはできません。青色のエリアは地面より上を指しており、定義上、シナリオゾーンは地面上にあるためです。

グリッドを使用してキャリブレーションを検証する

グリッドは地面上の正方形グリッドに対応する必要があります。グリッドの表示は、グリッドビュー設定変更アイコンをクリックすると切り替えできます。

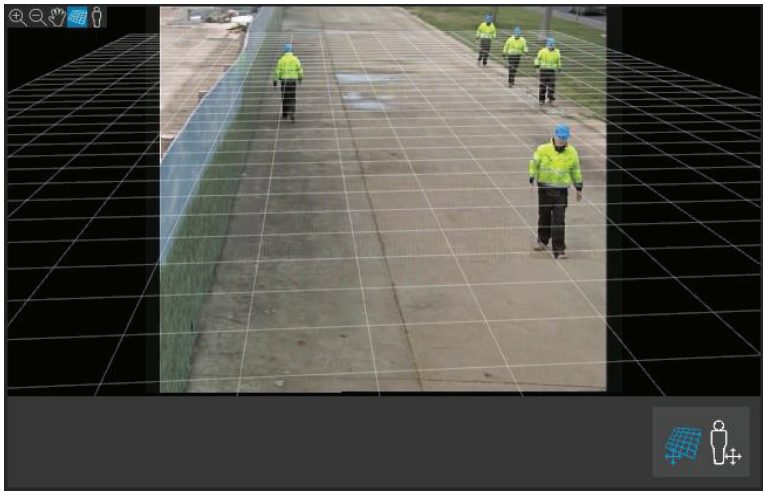
重要

グリッドがキャリブレーションに影響を与えることはありません。これはキャリブレーションが正しいことを確認するためのツールです。

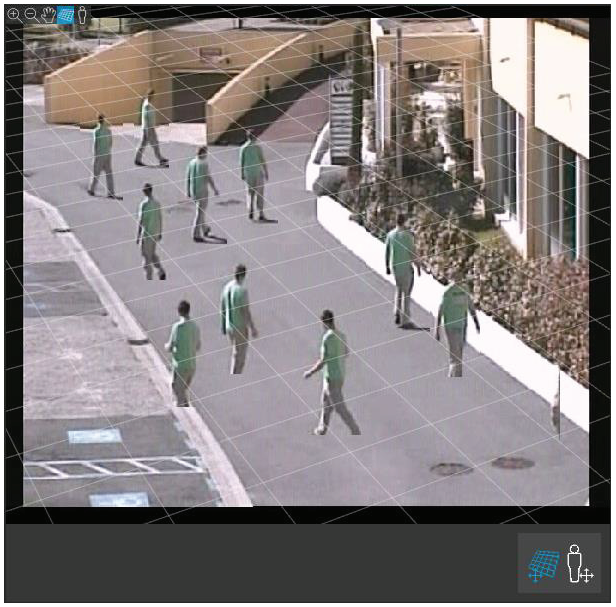
グリッドの向きはプレビューペインでドラッグして変更できます。シーン内の何らかの構造に合わせて調整し、結果が妥当と思われるかどうかを確認してください。

グリッドが地面に平行で、異様な傾斜がなく、必要な回転を適用後に実際の世界で平行な人工物とも平行になっている場合、そのキャリブレーションは良好です。

はじめに



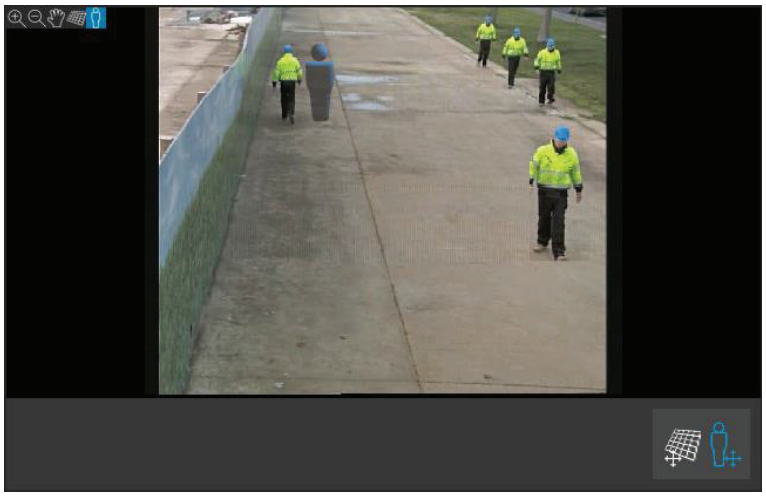
グリッドが道路の路肩に合わせて正しく調整されている例。



グリッドが道路の路肩に合わせて正しく調整されていない例。

アバターを使用してキャリブレーションを検証する

アバターを使用すると、シーン内に平均身長の3D人物アバターを配置することができます。アバターの表示は、アバタービュー設定変更アイコンをクリックすると切り替えできます。



ビューペインでのアバターのサイズは、現在のキャリブレーションでその位置にいる平均的なサイズの人物に対応しています。アバターをその周辺で移動させると、シーン内の他の物体や人物と比較してそのサイズが妥当であることを確認できます。アバターのサイズが画像内のある位置では正しくても、別の場所ではサイズが誤っている場合があるため、異なる位置でアバターを確認する必要があります。

検知結果を使用してキャリブレーションを検証する

検知結果を使用すると、人物が歩行している様子のビデオ映像をライブストリームとして受信した場合に、AXIS Perimeter Defenderが最新のキャリブレーションでどのように動作しているかを確認することができます。

1. [**Calibration results (キャリブレーション結果)**] から [**Detection results (検知結果)**] に切り替えます。
2. 人や車両が監視シーンに入る際の検知結果を確認する :
   - キャリブレーションが正常な場合、人は赤色の長方形、車両は青色の長方形でマークされます。
   - 人や車両にマークが付いていないことが多い場合、高い確率で自動キャリブレーションに失敗しています。
   - 赤色のゾーンは、計算後のキャリブレーションでの検知限界ゾーンを示します。つまり、このエリアは画像内の人物の高さに関する前提条件が考慮されないゾーンです。このゾーンではターゲットのサイズの関係で検知に失敗する場合があります。

注

- 計算後のキャリブレーションに誤りがある場合、赤色のゾーンも誤っています。
- 人物がはるか遠くにいる場合は、マークが付けられていない場合があります。検知が機能するには、最小限のサイズが必要です。詳細については、*15ページカメラを取り付ける*を参照してください。
- キャプチャーのフレームレートが低すぎる可能性があることが原因で、検知結果の確認がリモート接続されたカメラではうまくいかない場合があります。設定が失敗したということではありません。代わりに、アバターとグリッドを使用してキャリブレーションを検証してください。

手動キャリブレーションを実行する

自動キャリブレーションを試行していない場合は、手動キャリブレーションを実行する前に、短いビデオをキャプチャーして合成画像を作成する必要があります。自動キャリブレーション (*21ページ自動キャリブレーションを実行する*) とほぼ同じ手順ですが、**キャリブレーション** タブでは **自動**ではなく **手動**を選択してください。映像をキャプチャーした後に合成画像を作成するには、以下を実行します :

- スライダーを動かしてビデオクリップ内を移動します
- キーとなるポジションでカメラアイコンをクリックし、画像を追加して合成します

はじめに

合成画像にシーンの全断面 (前後左右) が映っていることを確認します。

手動または自動で作成した合成画像がある場合は、手動キャリブレーションを続行できます。

キャリブレーションエンジンは、次の要素を推定しキャリブレーションを行います :

- 水平
- 画像内の垂直線の広がり方、または扇形の広がり
- シーンのスケール

手動キャリブレーションを実行する場合は、キャリブレーション要素を通じてこの情報をキャリブレーションエンジンに提供する必要があります。キャリブレーション要素には、次の3種類があります。

- **人物スティック**は、シーン内のさまざまな位置で平均的な人物の既知の高さをマークするのに使用します。自動キャリブレーションを試行済みの場合、編集画面に表示される画像には、同じ人のインスタンスがいくつか表示される可能性が非常に高くなります。人物スティックを地面に配置し、1つ以上の位置で人の高さと方向をマークします。人物スティックは実際の世界では地面に接地し、垂直である必要があります。人物スティックの長さは、編集画面の [**Person (人物)**] ボタンの横に示す高さに準じなければなりません。人物スティックには薄青色の半透明の記号が付いています。

  人物スティックを最適な場所に配置する方法

  - 人物スティックの配置は両足をそろえている人に行うことをお勧めします。
  - 足を離した状態で地面に立っている人に人物スティックを配置する場合には、人物のかかととかかとの間の地面の低い位置に配置します。
  - 人物スティックを人物の胴体に揃えます。ただし、人物がどちらかの方向に傾いている場合 (一般的には歩行中に前方へ傾く)は、人物スティックを直立して配置することで傾きを補正するよう試みてください。木、フェンス、街頭の柱など、基準となるシーン内の手がかりを使用します。
  - シーンのスケール調整のためには、人物の高さに対応した人物スティックが少なくとも1つ必要です。シーンに人物が表示されていない場合は、高さが分かっている他の垂直な物体 (3 mのフェンス柱など) に人物スティックを配置し、人物の高さをその物体の高さに設定してください。

- **平行な水平線 (H線)** は、シーン内の既知の水平線と平行線をマークするのに使用します。これらの線は地面または壁面、またはその両方に配置できますが、すべて平行である必要があります。H線を追加する場合、少なくとも2本追加する必要があります。直線道路の端や標識、直線線路の一連の車線、壁面上の目に見える構造物、または並んでいるフェンス柱の上部と下部に配置できます。H線は薄い青色でマークされます。

- **垂直線 (V線)** はシーン内の既知の垂直線をマークするのに使用します。V線は実際の世界にあるいくつかの垂直構造物をマークする必要があります。フェンスの柱、建物の角、標識などです。V線は地面に接地する必要はありません。V線は濃い青色でマークされます。垂直方向が少しでも変わるとキャリブレーションが劇的に変化する可能性があるため、V線は非常に敏感です。大まかに言うと、V線は画像の右側では右に傾き、左側では左に傾く傾向があります。

1 人物スティック
2 垂直線 (V線)
3 平行な水平線 (H線)
4 グリッドツールとアバターツール

キャリブレーション要素の数

一般に、シーン内への人物スティック、H線、V線の追加が多いほど優れた結果が得られます。キャリブレーションエンジンは線が非常に少なくてもキャリブレーションを実行できますが、通常、キャリブレーション品質は、描画した線や人物スティックの数が多いほど向上します。人物スティックを追加する場合、近い場所、遠い場所、左エリア、右エリアに配置することをお勧めします。

画像内の垂直構造

*15ページカメラの取り付けに関する推奨事項*に従い、すべてのカメラは若干下向きにする必要があります。これにより、実際の世界のすべての垂直構造物は、画像内で孔雀の尾のように散開するように見えます。つまり、すべての人物スティックとV線は画像の端に向かって傾く必要があります。画像の右半分のスティックは右側に傾き、左側のスティックは左側に傾く必要があります。キャリブレーションが機能するには、配置したうち少なくとも1本の人物スティックまたはV線が「正しく傾いている」必要があります。

精度インジケーターからは、シーンに追加した内容の水平さと品質に関し、視覚的なフィードバックが得られます。手動キャリブレーションを成功させるには、シーンの前後左右にマークが含まれている必要があります。これは緑色の精度インジケーターで示されます。

キャリブレーション品質

キャリブレーション品質は、グリッドまたはアバターの操作ツールを使用して確認できます。*23ページキャリブレーションの品質を検証する*を参照してください。または、[**Review (確認)**] をクリックします。これにより、実行中のAXIS Perimeter Defenderにおける、現在の手動キャリブレーションを使用してキャプチャーされたビデオの結果が表示されます。

キャリブレーション - PTZ Autotracking

重要

良好な結果を得るには、キャリブレーションが高品質である必要があります。ガイドラインと手順に慎重に従ってください。

注

キャリブレーションは、両方のカメラを同時に行うことも1台ずつ行うこともできます。

1. 固定カメラとPTZカメラの両方を選択します。
2. **キャリブレーション**に移動し、[**Setup PTZ position (PTZ位置の設定)**] をクリックします。固定カメラのビューを含むポップアップが表示されます。

   PTZカメラは、アプリケーションの起動時に少しの間パン、チルト、ズームします。
3. 2台のカメラのビューの位置が互いに合っていることを確認してください。

   合っていない場合は、ライブビュー画像をクリックして、固定カメラのビューに一致するようにPTZカメラのビューを調整します。ロールがないことを確認します。
4. [**Setup PTZ position (PTZ位置の設定)**] をクリックします。

   ボタンが表示されていない場合は、固定カメラのビューを含むポップアップを移動します。
5. [**Automatic (自動)**] をクリックします。
6. *21ページ自動キャリブレーションを実行する* の手順に従って自動キャリブレーションを実行します。
7. アバターを使用し、固定カメラのキャリブレーションの品質を検証します。*25ページアバターを使用してキャリブレーションを検証する* を参照してください。

   品質が十分良好な場合は、[**Accept (同意)**] をクリックします。

   品質が十分に良好でない場合には、自動キャリブレーションの映像を使用して手動でキャリブレーションを行ってください。[**Manual (手動)**] をクリックし、*26ページ手動キャリブレーションを実行する* の手順に従います。
8. **シナリオ**では、何に対してアラームをトリガーするかのルールを定義します。*29ページシナリオを定義する* を参照してください。
9. **キャリブレーション**で、PTZカメラのライブビューで [**Review (確認)**] をクリックします。
10. アバターを使用し、PTZカメラのキャリブレーションの品質を検証します。*25ページアバターを使用してキャリブレーションを検証する* を参照してください。

    品質が十分良好な場合は、[**Accept (同意)**] をクリックします。

    品質が十分に良好でない場合には、自動キャリブレーションの映像を使用して手動でキャリブレーションを行ってください。[**Manual (手動)**] をクリックし、*26ページ手動キャリブレーションを実行する* の手順に従います。
11. カメラをペアリングします。*32ページカメラをペアリングする - PTZ Autotracking* を参照してください。

シナリオを定義する

シナリオ

AXIS Perimeter Defenderには、機密エリアを保護および監視するように構成できる一般的な検知ゾーンシナリオが含まれています。キャリブレーションの段階では、侵入/徘徊タイプのデフォルトシナリオとして大きな検知エリアが作成されました。このステップでは、以下の3つのタイプのより高度な検知シナリオを定義できます :

- 侵入/徘徊。*30ページ侵入/徘徊シナリオを設定する* を参照してください
- ゾーン横断。*31ページゾーン横断シナリオを設定する* を参照してください
- 条件付き。*31ページ条件付きシナリオを設定する* を参照してください

はじめに

!記号がシナリオ名で表示されている場合、シナリオの設定が完了していないことを意味します。よくある問題としては、検知ゾーンがまだ定義されていないことが挙げられます。

グローバルパラメーター

ユーザーインターフェースで設定するグローバルパラメーターは、すべてのシナリオに適用されます。

Camera type (カメラタイプ) - 可視光カメラをお使いの場合は、[**Color - Day-Night (カラー - デイ-ナイト)**] を選択します。サーマルカメラの場合、カメラタイプは自動的にサーマルに設定されます。

注

- その他のアプローチタイプを使用すると、動物などによる誤報のリスクが増大する可能性があります。
- その他のアプローチタイプには、AIモードでのみ動作するデバイスは対応していません。

Additional approach types (その他のアプローチタイプ) - 検知シナリオで対応する必要があるタイプを選択します。

Advanced mitigation (高度な軽減) - AIモードで動作するデバイスの場合、[**AI**] チェックボックスをオンにしてください。シーンに車両、ヘッドライト、ヘッドライトによる反射の影響がある場合は、[**Headlights/vehicles in scene (シーン内にヘッドライト/車両あり)**] を使用できます。この設定を使用すると、通常条件下でのパフォーマンスが低下する場合があります。デフォルトでは、すべてのシナリオで車両、またはヘッドライトの影響は含まれています。[**Insects/droplets on lens (レンズ上の昆虫/水滴)**] を使用して、雨滴または昆虫によるトリガーを無視し、誤報を減らすことができます。

感度 - システムの感度を高めるには、スライダーを右に動かします。感度を高くすると検知漏れのリスクは減りますが、誤報リスクが高くなります。

ターゲットサイズのフィルタリング - AIモードで動作するデバイスの場合、ターゲットサイズよりも小さい物体を除外できます。

期間パラメーター

作成したシナリオごとに期間パラメーターを設定できます。

ゾーンの最小の存在 - ゾーンをアクティブにするために物体がゾーン内に留まる必要がある時間を設定します。

狭いゾーン - ゾーンが狭くて1～2秒で通過できる場合は、アラームを見逃してしまうおそれがあります。これは [**Narrow zone (狭いゾーン)**] 機能を使用して軽減することができます。この機能は、[**Min presence in zone (ゾーンでの最小滞在時間)**] と組み合わせることはできません。

侵入/徘徊シナリオを設定する

侵入/徘徊シナリオは、物体が特定ゾーンに入り、事前に定義した時間を経過してもその検知ゾーンに残っている場合にアラームをトリガーするように設計されています。

キャリブレーション手順で作成されるデフォルトのシナリオは、侵入/徘徊のタイプであり、最大検知ゾーンが使用されます。このシナリオを現状のまま使用するには、[**Scenarios (シナリオ)**] タブで [**Accept (同意)**] をクリックします。

デフォルトのシナリオを変更するには、次の手順に従ってください。

1. [**Scenarios > Advanced scenarios (シナリオ > 高度なシナリオ)**] に移動します。
2. デフォルトの検知ゾーンは次の手順で変更します:
   - 検知ゾーン内の既存のポイントを移動するには、マウスでクリックしてドラッグします。
   - 追加ポイントを作成するには、マウスで既存セグメントのどれかをクリックしてドラッグします。
3. [**Detect (検知)**] で検知する物体のタイプを選択します。

4. 物体がゾーンに入ってもすぐにアラームをトリガーしないようにする必要がある場合は、[Duration parameters (期間パラメーター)] の [Min presence in zone (ゾーンでの最小滞在時間)] で徘徊時間を設定します。
5. ゾーンが狭くて1〜2秒で通過できる場合でもアラームをトリガーする場合は、[Narrow zone (狭いゾーン)] を選択します。この設定は、[Min presence in zone (ゾーンでの最小滞在時間)] と組み合わせることはできません。詳細については、*30ページ期間パラメーター*を参照してください。
6. 変更内容をカメラにアップロードしてメインビューに戻すには、[Accept (同意)] をクリックします。

ゾーン横断シナリオを設定する

ゾーン横断シナリオは、物体が指定されたシーケンスで2つの検知ゾーンを通過する場合にアラームをトリガーするように設計されています。

重要

ゾーン横断シナリオには以下の制限があります。シナリオをトリガーする物体が起点ゾーンで数秒間移動を停止してから終点ゾーンに移動する場合、シナリオはトリガーされません。

[Duration parameters (期間パラメーター)] では、そのシナリオでゾーンごとの最小存在時間を定義することができます。T_A が起点ゾーンでの最小時間で、T_B が終点ゾーンでの最小時間の場合、物体が起点ゾーンにT_A よりも長い時間留まっており、終点ゾーンにT_B よりも長い時間留まっている場合にのみアラームがトリガーされます。

1. [Scenarios > Advanced scenarios (シナリオ > 高度なシナリオ)] に移動します。
2. [New (新規)] をクリックし、[Zone-crossing (ゾーン横断)] を選択します。
3. 1メートル以上離れた2つの検知ゾーンを作成します。
   - 検知ゾーンを作成するには、画像内を何度かクリックします。
   - ゾーン作成を終了するには、画像を右クリックします。
4. 禁止する横断方向を指定するには、[Select origin (起点の選択)] をクリックし、ゾーンの1つをクリックします。
5. [Detect (検知)] で検知する物体のタイプを選択します。
6. 物体が入ってもすぐにゾーンを有効にしない場合には、[Duration parameters (期間パラメーター)] で片方または両方のゾーンの [Min presence in zone (ゾーンでの最小滞在時間)] を設定します。
7. ゾーンが狭くて1〜2秒で通過できる場合でもアラームをトリガーする場合は、[Narrow zone (狭いゾーン)] を選択します。この設定は、[Min presence in zone (ゾーンでの最小滞在時間)] と組み合わせることはできません。詳細については、*30ページ期間パラメーター*を参照してください。
8. 変更内容をカメラにアップロードしてメインビューに戻すには、[Accept (同意)] をクリックします。

条件付きシナリオを設定する

条件付きシナリオは、物体が最初に他のゾーンを通過することなく特定ゾーンに入る場合にアラームをトリガーするように設計されています。

[Duration parameters (期間パラメーター)] では、そのシナリオでゾーンごとの最小存在時間を定義することができます。T_A が許可されたゾーンでの最小時間で、T_B が侵入ゾーンでの最小時間の場合、物体が次に該当する場合にのみアラームがトリガーされます。

- 最初に許可されたゾーンに入ることなく、侵入ゾーンにT_B よりも長い時間留まっている。
- 許可されたゾーンにT_A 許可されたゾーンに入り、Tよりも長い時間留まる$_B$ よりも長い時間留まっている。

次の場合はアラームはトリガーされません。

- 侵入ゾーンに入らないか、T_B よりも短い時間留まっている。

- 許可されたゾーンにT_A よりも長い時間留まっており、その後侵入ゾーンに入る (物体が留まる時間は関係ない)。

1. [Scenarios > Advanced scenarios (シナリオ > 高度なシナリオ)] に移動します。
2. [New (新規)] をクリックし、[Conditional (条件付き)] を選択します。
3. 1メートル以上離れた2つ以上の検知ゾーンを作成します。
   - 検知ゾーンを作成するには、画像内を何度かクリックします。
   - ゾーン作成を終了するには、画像を右クリックします。
4. 許可されている横断方向を指定するには、[Select intrusion zone (侵入ゾーンの選択)] をクリックし、ゾーンの1つをクリックします。
5. [Detect (検知)] で検知する物体のタイプを選択します。
6. 物体が入ってもすぐにゾーンを有効にしない場合には、[Duration parameters (期間パラメーター)] で片方または両方のゾーンの [Min presence in zone (ゾーンでの最小滞在時間)] を設定します。
7. ゾーンが狭くて1〜2秒で通過できる場合でもアラームをトリガーする場合は、[Narrow zone (狭いゾーン)] を選択します。この設定は、[Min presence in zone (ゾーンでの最小滞在時間)] と組み合わせることはできません。詳細については、*30ページ期間パラメーター*を参照してください。
8. 変更内容をカメラにアップロードしてメインビューに戻すには、[Accept (同意)] をクリックします。

カメラをペアリングする - PTZ Autotracking

PTZカメラで動体が効率的に追跡されるよう、AXIS Perimeter Defender PTZ Autotrackingの設定で固定カメラとPTZカメラを互いにペアリングする必要があります。

自動キャリブレーションを実行すると、2台のカメラの*32ページ自動ペアリングを実行する*ことができます。それ以外の場合には、*33ページ手動ペアリングを実行する*必要があります。

自動ペアリングを実行する

ペアリング映像で赤い線は人物を表し、オレンジ色の境界ボックスはPTZカメラのズームイン画像を表します。

1. [キャリブレーション > PTZ Pairing review (PTZペアリングの確認) より、2台のカメラからのペアリング映像を検証します。
   - 2つの画像の赤色の線が映像全体で揃っていることを確認します
   - 赤色の線が常に人物の足元から頭まであることを確認します
   - 人物がPTZカメラ映像のオレンジ色の境界ボックス内で常に中央に配置されていることを確認します
2. 手順1の条件を満たす場合、[Interactive pairing review (対話式によるペアリングの確認)] を選択します。

   条件を満たしていない場合、[Manual (手動)] をクリックし、*33ページ手動ペアリングを実行する*の手順に従います。
3. スライダーを動かしてビデオクリップ内で移動します。以下を確認してください:
   - 2つの画像の青色の線が映像全体で揃っていること
   - 人物がPTZカメラ映像のオレンジ色の境界ボックス内で常に中央にいること
4. オレンジ色の境界ボックスが欠落しているシーンがある場合には、以下の操作を行います。

   4.1 固定カメラ画像でアバターをアクティブにします。

4.2 スライダーを使用して、映像内を前後に移動します。アバターを固定カメラビューの人物に配置し、PTZカメラの画像内の人物の足元に赤色のドットがあることを確認します。

5. 自動ペアリングによって青色の線が追加されないシーンがある場合は、[**Manual (手動)**] をクリックして、人物に赤色の線を手動で追加します。詳しい手順については、*33ページ手動ペアリングを実行する*を参照してください。
6. [**Accept (同意)**]、[**Exit (終了)**] をクリックします。

手動ペアリングを実行する

手動ペアリングを実行する際に、キャリブレーション手順の監視シーンを歩いている人物の足元から頭までに、縦方向の赤色の線を追加します。シーン全体をカバーするには、映像全体に線を追加する必要があります。

すでに自動ペアリングを実行している場合、映像にはすでに青色の線が表示されています。

次のような青色と赤色の線は削除します :

- 人物の足元が起点になっていない
- 人物の頭までのびていない
- PTZカメラの画像に対応する線が含まれていない

線を削除するには、クリックして [Delete (削除)] を押します.

1. スライダーを動かして、人物が表示されているビデオクリップ内の画像に移動します。
2. 固定カメラ画像の人物に赤色の線を追加します。人物の足元より線を開始します。線にはID番号が付けられます。
3. PTZカメラ画像の同じ物体に対応する赤色の線を追加します。ID番号が固定カメラ画像のID番号と一致することを確認してください。
4. シーン全体をカバーするまで、手順1～3を繰り返します。

   ビデオクリップに有効なペアリングを行えるだけの十分な数の線が含まれている場合:

   - [**Accept (同意)**] ボタンがアクティブになります
   - PTZカメラの画像にオレンジ色の境界ボックスが表示されます
5. 人物が常にオレンジ色の境界ボックスの中心にいることを確認します。そうでないシーンがある場合は、赤色の線を追加します。
6. 固定カメラ画像でアバターをアクティブにします。
7. スライダーを動かしてビデオクリップ内で移動します。アバターを使用し、以下のことを確認してください。

   - 固定カメラ画像で、アバターのサイズがさまざまな位置にいる人物のサイズに対応していること
   - PTZカメラ画像で、赤色のドットが人物の足元にあること
   - PTZカメラ画像で、人物がオレンジ色の境界ボックス内で常に中央にいること
8. [**Accept (同意)**] をクリックします。ボタンがアクティブでない場合は、まず赤色の線を追加する必要があります。
9. [**Exit (終了)**] をクリックします。

はじめに

出力を定義する

侵入が検知されたときにAXIS Perimeter Defenderの出力アラームが出るようにするには、そのルールを定義する必要があります。システムはVMSなどにアラームを送信することができます。

AXIS Perimeter Defenderはさまざまなインターフェースを通じてアラームを送信できます。

アプリケーション自体から:

- TCP/IPを介したXMLまたはプレーンテキストのアラーム通知
- multipart HTTPを介したXMLメタデータストリーム

デバイスから:

- TCP/IPを介したベーシックなフリーテキストのアラーム通知
- 電気的出力 (無電圧接点または有電圧接点)
- メール通知
- アラーム画像のFTPアップロード

複数のインターフェースを同時にアクティブにすることができます。

より詳細な情報については、*35ページ出力*を参照してください。

デバイスからのアラーム送信ルールを定義するには、次の手順を実行します。

1. [**Outputs (出力)**] に移動し、[**Configure (設定)**] をクリックします。Webブラウザーでデバイスのページが開きます。
2. 新しいアクションルールを作成します。
3. トリガーのリストより [**Applications (アプリケーション)**]、[**AXISPerimeterDefender**]、アクションをトリガーするシナリオを選択します。

注

定義したすべてのシナリオで同じアクションをトリガーするには、[**ALL_SCENARIOS**] を選択します。

4. アクションのリストから、条件を満たすときに実行するアクションを選択します。
5. [**OK**] をクリックします。

アクションルールの作成方法の詳細については、デバイスのユーザーズマニュアルを参照してください。

高度な設定

出力

XML/テキストアラーム通知

このインターフェースを使用すると、TCP/IP送信先は、アラームごとにより完全で記述的なXMLまたはテキストメッセージを受信することができます。フリーテキストインターフェースに関し、XML/テキストインターフェースには以下の利点があります :

- 通知はアラーム開始時、アラーム終了時、およびアラームが出ている間の10秒ごとに送信されます。
- タイムスタンプ: アラーム開始時とアラーム終了時の通知にはカメラの時計と同期されているタイムスタンプが含まれ、イベントの正確な日時が示されます。
- アラームタイプ: AXIS Perimeter Defenderは、複数のアラームタイプをサポートしています。*29ページシナリオを定義する*を参照してください。XML/テキスト通知には、トリガーされたアラームタイプに関する情報が含まれています。注意点 : "zone crossing (ゾーン横断)"シナリオには""passage(通過)"タイプがあり、徘徊シナリオには"presence(存在)"タイプがあります
- アラーム生成に関係するゾーン。AXIS Perimeter Defenderの各シナリオが1つ以上のゾーンに関連付けられている場合、XML/テキスト通知にはアラームに関連付けられているゾーンが含まれます (たとえば、侵入検知では、人物が検知された侵入ゾーン)。

フリーテキストインターフェースに関し、XML/テキストインターフェースには以下の制限があります :

- メッセージテキストは固定されており、フリーテキストフィールドはありません。
- 一度にサポートされるのはカメラ1台あたり1つの送信先のみです。

XML/テキスト通知の受信者は、次の4つのタイプのメッセージを受信します :

- AXIS Perimeter Defenderは、XML通知が設定されると、受信者との通信が期待どおりに動作することを検証するため、CONNECTION_TESTメッセージを送信します。
- AXIS Perimeter Defenderがアラームをトリガーすると、ALARM_STARTメッセージが送信されます。
- アラームが出ている間、AXIS Perimeter Defenderは、10秒ごとに1回、"アラームを実行中です"という旨のメッセージを送信します。これらのメッセージのGUIDタグはすべて同じであり、同じアラームに関連しているALARM_STARTメッセージおよびALARM_STOPメッセージのGUIDタグと同一です
- アラーム終了時にAXIS Perimeter DefenderはALARM_STOPアラームを送信します。

XMLとテキスト形式の両方のこれらのメッセージの形式の説明については*35ページXMLとテキスト形式の例*を参照してください。

XMLとテキスト形式の例

XML形式は、TCP/IP通知のデフォルトフォーマットです。ただし、通知サイズが重要な場合には、短いメッセージを生成するテキスト形式を使用できます。テキスト形式を選択するには、AXIS Perimeter Defenderの設定ページで[**Do not use XML for alarms parameter (アラームパラメーターにXMLを使用しない)**] を選択します。

例

XML形式のCONNECTION_TESTメッセージは、以下の例のようになります。

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="1"
         TYPE="CONNECTION_TEST"
```

```
          SENDER_IP="192.168.1.40"
          SENDER_PORT="0">
  <REFERENTIAL>45</REFERENTIAL>
</KEENEO_MESSAGE>
```

- VERSIONは、XMLシンタックスとプロトコルの内部バージョンです。
- IDはメッセージの識別番号です。IDが一意であること、また連続していることは保証されていません。
- TYPEはメッセージのタイプであり、ここでは“CONNECTION_TEST“です。メッセージタイプによりメッセージのサブタグが決定されます (タイプが "CONNECTION_TEST"のメッセージではなし)。
- SENDER_IPは、XML通知を送信するAxisカメラのIPアドレスです。
- SENDER_PORTは常に0です。カメラはメッセージを受信することはできません。
- REFERENTIALはカメラに関連付けられている数値IDです

テキスト形式を選択すると、通知メッセージには7つのフィールドが含まれ、各フィールドは「パイプ」文字列（|）で区切られます。フィールドを指定できない場合 (たとえば、そのメッセージタイプで意味をなさない場合など) は、"-"に置き換えられます。

7つのフィールドは最初から順番に以下のとおりです (括弧内は、形式がXMLの場合の対応するXMLフィールドです)。

1. メッセージの数値ID (XMLの"KEENEO_MESSAGE"ヘッダーの"ID"属性)。
2. カメラのIPv4アドレス (XMLの"KEENEO_MESSAGE"ヘッダーの"SENDER_IP"属性)。
3. AXIS Perimeter Defenderのインスタンスに関連付けられている参照番号 (“REFERENTIAL”タグ)。
4. メッセージのタイプ (XMLの"KEENEO_MESSAGE"ヘッダーの"TYPE"属性)。
5. アラームのタイプ ("TYPE"タグ)。
6. アラームをトリガーしたシナリオ名 (“SCENARIO_NAME”タグ)。
7. タイムスタンプ (“TIMESTAMP”タグ)。タイムスタンプの形式は、XML形式の場合と同じです。

前述のTEXT形式でのCONNECTION_TESTメッセージは以下のようになります：

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

例

XML形式のALARM_STARTメッセージは、以下の例のようになります。

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xmlns:xsd="http://www.w3.org/2001/XMLSchema"
          VERSION="5.0.0"
          ID="9999"
          TYPE="ALARM_START"
          SENDER_IP="192.168.1.40"
          SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <EXTRA_DATA>zone=testzone</EXTRA_DATA>
  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- メッセージヘッダーは"CONNECTION_TEST"メッセージと同じです。

- メッセージタイプは"ALARM_START"であり、一連のサブタグが含まれています。
  - REFERENTIALはカメラに関連付けられている数値IDです。
  - TYPEはAXIS Perimeter Defenderによってトリガーされたアラームのタイプであり、この例では“INTRUSION”です。その他のタイプとして、“PRESENCE”、“PASSAGE”、“CONDITIONAL”があります。
  - SCENARIO_NAMEは、設定インターフェースで定義されている、アラームをトリガーしたシナリオの名前です。*30ページ侵入/徘徊シナリオを設定する*を参照してください
  - EXTRA_DATAは、侵入ゾーンなど、アラームに関連したゾーン名 (またはゾーン名のリスト) です。
  - TIMESTAMPはアラームの開始日時で、フォーマットはYYYY-MM-DDTHH:mm:ss.zzzです。それぞれ以下の意味となります :

    – YYYYは4桁の西暦です。(例:2014)

    – MMは2桁で月を表します。(例:1月=01)

    – DDは2桁で日にちを表します。(例: 3日=03)

    – 'T'は固定文字です

    – HHは24時間形式の時間で、00～23で表します

    – mmは2桁で分です。00～59で表します。

    – ssは2桁で秒です。00～59で表します

    – zzzは3桁でミリ秒です。000～999で表します。

    AXIS Perimeter Defenderはアラームのタイムスタンプを生成するのにカメラ内部の日時を使用します。そのため、カメラを何らかの外部時計と同期させることが重要です。
  - GUIDは、同じアラームに関連するすべてのメッセージ (ALARM_START、ALARM_IN_PROGRESS、ALARM_STOP) に共通する一意の識別子です。

以下は、テキスト形式のALARM_STARTメッセージの例です :

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

例

XML形式のALARM_IN_PROGRESSメッセージは、以下の例のようになります。

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_IN_PROGRESS"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- メッセージヘッダーは、"CONNECTION_TEST"および"ALARM_START"のメッセージと同じです。
- メッセージタイプは"ALARM_IN_PROGRESS"で、一連のサブタグが含まれています。
  - REFERENTIALはカメラに関連付けられている数値IDです。

- TYPEは、AXIS Perimeter Defenderによってトリガーされたアラームのタイプで、対応するALARM_STARTと同じです。
- SCENARIO_NAMEはアラームをトリガーしたシナリオ名で、対応するALARM_STARTと同じです。
- GUIDは対応するALARM_STARTと同じです。

このALARM_IN_PROGRESSはTEXT形式では以下のようになります :

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

例

XML形式のALARM_STOPメッセージは、以下の例のようになります。

```
<?xml version="1.0"?>
<KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xmlns:xsd="http://www.w3.org/2001/XMLSchema"
         VERSION="5.0.0"
         ID="9999"
         TYPE="ALARM_STOP"
         SENDER_IP="192.168.1.40"
         SENDER_PORT="0">
  <REFERENTIAL>0</REFERENTIAL>
  <TYPE>INTRUSION</TYPE>
  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>
  <EXTRA_DATA>zone=testzone</EXTRA_DATA>
  <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>
  <GUID>77acddf9-e0d4-402e-a497-231aeee22788</GUID>
</KEENEO_MESSAGE>
```

- メッセージヘッダーは前述のメッセージと同じです。
- メッセージタイプは"ALARM_STOP"で、ALARM_STARTメッセージと一連のサブタイプは同じです。

このALARM_IN_PROGRESSメッセージは、TEXT形式では以下のようになります :

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

TCP/IP接続は常に各メッセージの後に閉じられます。そのため、送信先は、その後の通知を受信できるように、リッスン状態のソケットを常に開いたままにしておく必要があります。

通信エラー

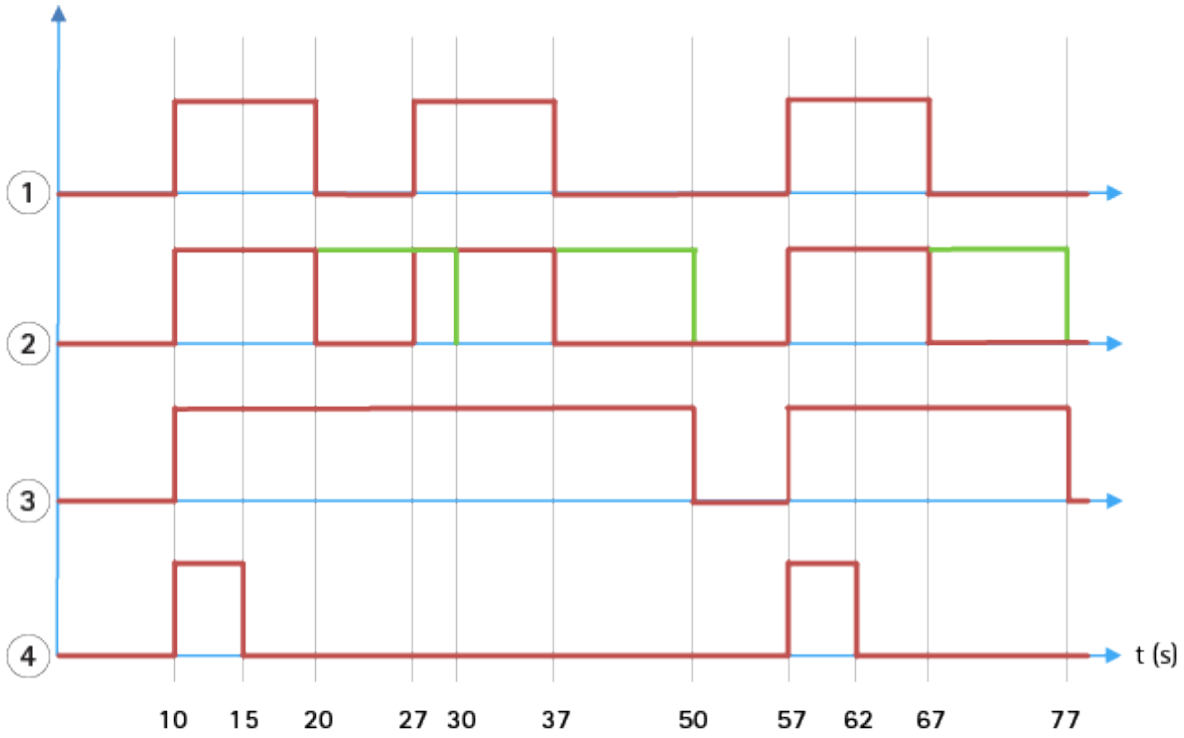
ネットワークが切断されているなどの理由でXML通知のリモート受信者に到達できない場合、AXIS Perimeter Defenderは未配信のアラームのバッファリングを内部的に開始し、定期的 (少なくとも10秒ごと)に再配信を試行します。新しいメッセージの配信が連続して失敗すると (バッファからのメッセージの再配信の失敗は含みません)、AXIS Perimeter Defenderは送信先を"完全にオフライン"であると宣言し、送信先へのXML通知の送信を停止します。連続失敗数は20に固定されており、これは、平均継続時間が40秒間である侵入アラーム4回、5回に概ね相当します。以下のイベントのいずれかが発生すると、AXIS Perimeter Defenderは同じ送信先への通知の送信を再開します :

- AXIS Perimeter Defenderが再起動される。
- Alarm streaming url(アラームストリーミングURL)パラメーターが再び同じ値で保存される。

ポストアラーム時間

AXIS Perimeter Defenderは、"ポストアラーム時間"の概念を実装しています。これはアラーム停止後の持続時間を定義するもので、この期間に別のアラームがトリガーされると両方のアラームが1個のアラームに統合されます。

高度な設定



1 *AXIS Perimeter Defenderによって、10、27、57の3つの時間に3つのアラームがトリガーされています。各アラームの継続時間は10秒です。つまり、侵入者が侵入ゾーンを通過するのに10秒間かかっています。*
2 *10秒間のポストアラーム時間が追加されます。*
3 *XML通知とXMLメタデータによるアラーム*
4 *メール通知、FTP画像アップロード、電気的接点、TCP/IP通知によるアラーム*

(2) 10秒間のポストアラーム時間 (緑色) によって、各アラームの持続時間が長くなり、これにより10秒以下に区切られた2つのアラームが融合 (マージ) することに注目してください。

(3) XML通知とXMLメタデータを使用し、AXIS Perimeter Defenderが発行したアラーム番号と継続時間を表示できます。ポストアラーム時間は、短い複数の連続するアラームの代わりに、長く少ないアラームを取得したいときに使用します。

(4) メール通知、FTP画像アップロード、電子的連絡、TCP/IP通知で、10秒間のポストアラーム時間を使用した場合の結果は異なります。これらの通知はアラーム開始のみが考慮されており、アラーム停止については考慮していません。そのため、これらの通知を使用する場合は"アラーム継続時間"の概念はありません。従って、ポストアラーム時間によって通知そのものの継続時間は変化しないということになります。通知の継続時間は、それぞれの通知の設定時にユーザーが選択した値に固定されます。ポストアラーム時間の影響で連続するアラームが1つに統合された場合は、1つの通知のみが送信されます。このAXIS Perimeter Defenderのグラフでは、最初の2つのアラームを統合し、通知を1つにしていることがわかります。最終的に、メール通知、FTP画像アップロード、電気的接点、TCP/IP通知は、トータルで 2 つだけ送信されています。グラフによると、これらのアラートには5秒間の固定時間が設定されています。

ポストアラーム時間を設定する方法

1. AXIS Perimeter Defender Setupを開きます。
2. [**Outputs (出力)**] に移動します。
3. [**Post-alarm time (ポストアラーム時間)**] の設定を変更します。デフォルト値は7秒間です。

4. [Assign (適用)] をクリックします。

メタデータ

Burnt-in Metadata Overlay (画面内に埋め込まれたメタデータのオーバーレイ)

画面内に埋め込まれたメタデータのオーバーレイは、選択したライブストリームに分析による検知内容を直接描画する機能です。検知内容は、境界ボックスと軌跡の形で画像のオーバーレイとして描画されます。ストリームは解像度に基づいて選択されます。デバイスがビューエリアをサポートしている場合にはビューエリアに基づいて選択されます。画面内に埋め込まれたメタデータはライブビューと録画再生時の両方に表示されます。

選択したストリームでの画面内に埋め込まれたメタデータのオーバーレイ

たとえば、解像度が640×480のすべてのストリームにオーバーレイを追加するようアプリケーションを設定したとします。この場合、この解像度のストリームのみにオーバーレイが表示され、他のストリームは表示されません。

選択したビューエリアでの画面内に埋め込まれたメタデータオーバーレイ

カメラがサポートしていれば、解像度とともにビューエリアも指定することができます。たとえば、解像度1280x720のビューエリア番号3から取得したストリームにオーバーレイを含めるよう選択することができます。この場合、この設定と一致するストリームだけにオーバーレイが存在し、ビューエリア3から取得したが異なる解像度のストリーム、あるいは1280x720で取得しているがビューエリア3ではないストリームといった他のストリームは変更されません。

画面内に埋め込まれたメタデータをビデオストリームに追加する

注

この機能はファームウェア7.30以降を搭載したデバイスでのみ使用できます。

この例では、解像度640×480のすべてのビデオストリームで画面内に埋め込まれたメタデータのオーバーレイを有効にする方法について説明しています。他の解像度のビデオストリームへの影響はありません。

1. ライブビューのパネルよりカメラを選択します。
2. [Outputs > Burnt-in Metadata Overlay (出力 > 画面内に埋め込まれたメタデータのオーバーレイ)] に移動します。
3. [Enabled (有効)] を選択します。
4. ドロップダウンリストで解像度640x480を選択します。
5. [Apply (適用)] をクリックします。
6. メタデータがその解像度のライブビューに表示されていることを確認してください。

VMSへの統合

AXIS Perimeter Defenderは、以下のビデオ管理システム (VMS) とシームレスに統合されています。

- Genetec™のSecurity Center
- MilestoneのXProtect®

サポートされているVMSのバージョンの詳細については、
*axis.com/products/axis-perimeter-defender/support-and-documentation*を参照してください

AXIS Perimeter Defenderによってトリガーされたアラームは VMS内で自動的にイベントに変換され、これにより、幅広いアクションをトリガーし、VMSの能力を最大限に活用することができます。同時に、AXIS Perimeter Defenderによって生成されたライブメタデータは、ライブ表示および録画用にVMSに送信されます。このため、録画されたビデオシーケンスを再生モードで再生する場合にもメタデータを利用できます。

実際の自動化された侵入検知システムは、アラームをトリガーし、警備が介入すべきかどうかの判断を助ける情報を提供するように設計されるべきです。カメラから検知アラートを受け取り、モバイルデバイスにプロンプトを表示するようなシステムや、VMS上でアラームイベントが画面上で強調表示されるような仕組みを作ることによってこれを実現することができます。

標準的なイベントの統合

AXIS Perimeter Defenderは、ネイティブのACAPインターフェースと機能を活用し、アラームおよび補足情報を外部デバイスやVMSに送信できる機能があります。AXIS Perimeter Defenderが出力するイベントは、カメラのアクションルールを経由することにより、VMSに対するメッセージに変換することができます。

カメラからVMSへの以下のアラームチャンネルが利用可能です :

- フリーテキストのアラーム通知 (TCP/IP)
- 電気的出力 (無電圧接点または有電圧接点)
- メール通知
- アラーム画像のFTPアップロード

これらの統合はカメラ上で設定することができます。*38ページポストアラーム時間*を参照してください。

VMSブリッジ

以下のビデオ管理システムでは、"ブリッジ"というあらかじめ開発済みの統合モジュールを提供しています。

- Milestone XProtect® 2014および2016 Corporate/Expert/Enterprise/Professional/Express。Enterprise/Professional/Expressエディションはメタデータをサポートしていません (ライブまたは再生によるメタデータの表示は行われません)
- Genetec™ Service Center 5.3および5.4 Pro/Enterprise/SV32/SV16

ブリッジでは以下の2つの統合を行えます :

- VMSでカスタムアラームイベントを作成し、AXIS Perimeter Defenderが出力するイベントに一致させる。
- アラームオーバーレイ (境界ボックス) をライブ映像および録画映像の素材の上に表示する (Milestone XProtect® Enterprise/Professional/Expressエディションを除く)。

VMSブリッジは別個のアプリケーションとしてダウンロードしてインストールする必要があります。これらのブリッジをインストールおよび設定する方法の詳細については、特定のブリッジのユーザーズマニュアルを参照してください。

AXIS Camera Stationでルールを作成する

このセクションでは、AXIS Perimeter DefenderをAxis Camera Stationのイベントシステムと統合する方法について説明します。以下に関する方法を習得します。

- 侵入発生時にトリガーするAXIS Camera Stationルールを設定します。
- 設定が正しく行われたかどうか確認します。

1. AXIS Perimeter Defender SetupソフトウェアでAXIS Perimeter Defenderを設定し、キャリブレーションを行います。AXIS Perimeter Defenderのインストールとキャリブレーションの詳細については、AXIS Perimeter Defenderユーザーズマニュアル、*または製品ページ*を参照してください。
2. [**Add Camera (カメラを追加する)**] ウィザードに従って、カメラをAXIS Camera Stationに追加します。
3. 次のようにデバイスイベントトリガーを設定します。
   3.1 [**Configuration (設定)**] > [**Recording & Events (録画とイベント)**] を選択し、[**Advanced rules (高度なルール)**] タブを開きます。

3.2 新しいルールを作成し、[**Device Event (デバイスイベント)**] トリガーを選択します。

3.3 AXIS Perimeter Defenderがインストールされたカメラを選択します。

3.4 [**Event (イベント)**] リストで [**AXISPerimeterDefender**] を選択します。

3.5 [**Feature (機能)**] リストで設定した侵入の名前を選択します (この場合は "Intrusion-1")。設定したすべてのシナリオでルールをトリガーする場合は、[**ALL_SCENARIOS**] を選択します。

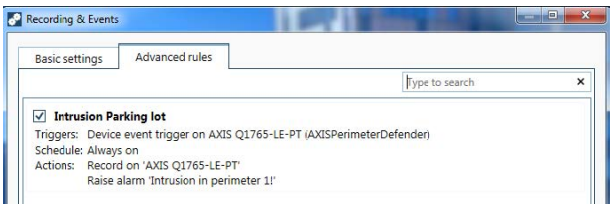
3.6 侵入を検知した時点でトリガーを有効にする場合は、[**Yes (はい)**] を選択します。侵入が検知されると、設定が正しいか確認できるステータスの変更が [アクティビティ] ウィンドウに表示されます。

3.7 [**OK**] と [**Next (次へ)**] をクリックしてアクションを設定します。

3.8 [**Add Action (アクションを追加)**] ダイアログで、ルールで使用するアクションを 1 つ以上追加できます。

この例では、録画のアクションとアラームのアクションを追加します。

3.9 [**Finish (完了)**] をクリックします。



例では、侵入発生時に2つのアクションをトリガーするAXIS Camera Stationルールを示しています。

4. 監視対象エリアに実際に入ることで侵入をシミュレーションして、想定したとおりに設定が機能するかをテストします。

トラブルシューティング

すべての機能が想定どおりに機能するためには、次のAxisパラメーターを設定する必要があります。

- Network (ネットワーク) / TCP-IP / Basic (基本設定) / Default router (デフォルトルーター)
- Network (ネットワーク) / TCP-IP / Advanced (詳細設定) / Domain name (ドメイン名)
- Network (ネットワーク) / TCP-IP / Primary DNS Server (プライマリDNSサーバー)
- Network (ネットワーク) / TCP-IP / Secondary DNS Server (セカンダリDNSサーバー)
- Network (ネットワーク) / TCP-IP / NTP server address (NTPサーバーのアドレス)
- Network (ネットワーク) / TCP-IP / SMTP (email) (SMTP (電子メール))
- System Options (システムオプション) / Date & Time (日付と時間) / Time Zone (タイムゾーン)
- System Options (システムオプション) / Date & Time (日付と時間) / Synchronize with NTP server (NTPサーバーとの同期)

最新バージョンに更新する

シナリオを再キャリブレーションして再定義する必要なく最新の機能改善を利用するには、最新バージョンのAXIS Perimeter Defenderにアップグレードすることをお勧めします。

1. 最新バージョンのAXIS Perimeter Defenderをダウンロードしてインストールします。
2. [**Install (インストール)**] をクリックします。AXIS Perimeter Defender Setupは、インストールを完了するために必要な手順を自動的に実行します。
   - 既存のキャリブレーション、シナリオ、パラメーター、ライセンスをバックアップします。
   - 新しいバージョンをインストールします。
   - ライセンスをリストアします。
   - キャリブレーションとシナリオをリストアします。
   - パラメーターをリストアします。
   - アプリケーションが実行中の場合は、再起動されます。

カメラのファームウェアをアップグレードする

注

カメラのファームウェアをアップグレードする前に、AXIS Perimeter Defenderの設定をすべて保存してください。ファームウェアをアップグレードすると、カメラからアプリケーションとその設定が削除されます。設定が保存されていれば、AXIS Perimeter Defender Setupを使用してリストアすることができます。

1. AXIS Perimeter Defender Setupを使用し、サイトの設定を保存します。
2. カメラのファームウェアをアップグレードします。詳細については、カメラのユーザーズマニュアルを参照してください。
3. AXIS Perimeter Defender Setupを起動します。
4. サイト読み込みオプションを使用すると、アップグレードしたカメラごとに保存済みの設定を自動的に読み込むことができます。

トラブルシューティング

インストールのトラブルシューティング

問題	考えられる理由	対処法
ソフトウェアをインストールできないことを知らせるWindows®メッセージが表示されます。	ノートPCまたはPCのオペレーティングシステムとの互換性がありません。	要件に指定されているWindows®オペレーティングシステムを確認します。
正しくインストールされていないことを知らせるWindows®メッセージが表示されます。	インストールに問題がある可能性がWindows®互換性アシスタントによって検出されました。	インストールが正しいことを確認して続行します。
XVIDのインストール中にインストールが失敗します。	XVIDの古いインストールの一部がコンピューターに残っているため、XVIDのインストールに失敗します。	XVIDフォルダーをC:\Program Files (x86) から削除してから、もう一度インストールしてください。
ソフトウェア利用許諾契約の表示後にインストーラーパッケージが突然クラッシュします。アプリケーションが通常とは異なる方法で終了したことを知らせるWindows®エラーメッセージが表示されます。インストーラーを閉じることができません。	状況によっては、インストーラーの既知の問題によって、アプリケーションのクラッシュが発生することがあります。	タスクマネージャーを開き、すべての "msiexec.exe" プロセスを強制終了します。その後、インストーラープロセスを中止し、インストーラーを再起動してください。

設定のトラブルシューティング

問題	考えられる理由	対処法
AXIS Perimeter Defenderを開くときに問題が発生します。	適切なWindows®ユーザー権限がありません。	管理者権限を持っていることを確認してください。
検索機能でカメラが検出されません。	ファイアウォール	ファイアウォールやウィルス対策ソフトウェアは、カメラの検出をブロックする場合があります。必要に応じて、AXIS Perimeter Defenderとネットワーク間の双方向のトラフィックを許可するよう、ファイアウォールを設定してください。それでも問題が解決しない場合は、次のポートを許可するよう、ファイアウォールを設定してください：UDPポート5353とTCPポート80。
	IPアドレスの問題	ネットワーク中のデバイスは、その他のデバイスと通信できるように固有のIPアドレスを持つ必要があります。AXIS Perimeter Defenderを使用している場合は、カメラで固定IPアドレスを使用することをお勧めします。ネットワーク上のすべてのIPデバイスが独自のIPアドレスを持ち、IPアドレスが重複して利用していないことを確認してください。
	ユーザーのコンピューターからカメラを利用できません。	カメラが使用可能かどうかを確認するには、ブラウザーでカメラのIPアドレスにアクセスします。アクセスできない場合は、カメラがネットワーク上で正しくインストールされ

トラブルシューティング

問題	考えられる理由	対処法
		ていないか、コンピューターにカメラへのアクセス権がありません。
カメラを追加することができません。	カメラの接続パラメーター (IPアドレス、パスワード、HTTPポートなど) が正しくありません。	入力したパラメーターが正しいかどうかを確認し、再入力します。
	ユーザーのコンピューターからカメラを見ることができません。	カメラが使用可能かどうかを確認するには、ブラウザーでカメラのIPアドレスに移動します。アクセスできない場合は、カメラがネットワーク上で正しくインストールされていないか、コンピューターにカメラがインストールされているネットワークへのアクセス権がありません。
AXIS Perimeter Defender Setupでビデオストリームの損失が発生しています。	ビデオソースが利用できなくなっています。	ビデオソースが中断され、ディスプレイ上での更新が行われていません。
	ブラウザーを使用し、カメラが利用可能かどうかを確認してください。	ストリームが表示されるはずのタイルをクリックしてインターフェースのサイズを変更すると、ストリームが回復することがあります。
自動キャリブレーションが機能しないか、結果に問題があります。	必要条件が満たされていません。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。
	カメラがロールしています。	ロールしているカメラをキャリブレーションすることはできません。
	リモートとして設定されていないカメラの接続が遅いです。	カメラをリモートデバイスとして接続し、帯域幅の要件を下げます。
	自動キャリブレーションに使用されるシーンに、車、木、他の人物といった他の動く物体があります。	自動キャリブレーションをやり直すか、手動でキャリブレーションしてください。
	視野が雑然とした状態のため、カメラの前を歩いている人物の一部が長い時間見えなくなっています。	デバイスのキャリブレーションを手動で行ってください。
	視野は入口と同じ小ささです。	デバイスのキャリブレーションを手動で行ってください。
	ディスク容量が不足しているため、キャプチャー映像が正しく録画されませんでした。	十分なディスク容量があり、アプリケーションにAXIS Perimeter Defenderインターフェースを実行しているコンピューターへビデオ録画を保存する権限があることを確認してください。

トラブルシューティング

動作のトラブルシューティング

問題	考えられる理由	対処法
設定には問題がないにも関わらず、アプリケーションが実行されません。	カメラのファームウェアが最新ではありません。	カメラで最新のファームウェアを使用していることを確認してください。
分析が実行されているにも関わらず、オーバーレイがAXIS Perimeter Defender Setupに表示されていません。	アプリケーションが動作の開始後または停止後、あるいはAXIS Perimeter Defenderパッケージのアップグレード後にブロックされています。	カメラを再起動します。
	ファイアウォールがカメラのメタデータリスニングポートへの接続をブロックしています。	設定インターフェースがカメラのメタデータリスニングポートに接続できるようにファイアウォールを設定してください。
	ウイルス対策プログラムがオーバーレイの受信をブロックしています。	ウイルス対策ソフトウェアの設定でオーバーレイの受信を許可してください。
分析が実行されており、オーバーレイが表示されているにも関わらず、設定したコンピューターのAXIS Perimeter Defender Setupでアラームがトリガーされません。	ターゲットはシーン内にありますが、条件付きシナリオとは一致しません。たとえば、ゾーン横断シナリオでゾーン間を移動しないなどです。	条件を含め、シナリオが正しく指定されていることを確認してください。
	検知状況がよくありません。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。また、キャリブレーションの精度が十分であり、感度が十分高いことを確認してください。

パフォーマンスのトラブルシューティング

問題	考えられる理由	対処法
OSDと分析のオンオフが続いています。	カメラのCPU負荷が高すぎます。	考えられる対処法: • カメラストリームの映像表示はCPU負荷を増加させるため、カメラのストリームが不要な場所で表示されていないことを確認してください。 • 内蔵のモーション検知で録画が有効になっている場合は、録画品質を下げてCPUを解放してください。 • 内蔵のモーション検知で録画を無効にし、内蔵の動体検知が無効になっていることを確認します。
ターゲットが検知エリアに入ると、複数のアラームが発生します。	ポストアラーム時間の長さが短すぎます。	ポストアラーム時間を調整します。AXIS Perimeter Defender Setupより、[**Outputs (出力)**] に移動します。

トラブルシューティング

問題	考えられる理由	対処法
ターゲットが検知エリアに入ってもアラートが発生しません (検知漏れ)。	被写体とシーンの背景のコントラストが低すぎます。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。
	シーン内の照明が不十分であるか、カメラの低照度性能が十分ではありません。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。
	AXIS Perimeter Defenderの感度設定が低すぎます。	シナリオのグローバルパラメーターで感度を上げてください。
	カメラが移動し、キャリブレーションが不正確になりました。	キャリブレーションをやり直してください。
	キャリブレーションの精度が十分ではありません。	カメラのキャリブレーションを確認してください。 AXIS Perimeter Defender Setupに移動します。
	ターゲットがシーン内にいるにも関わらず、条件付きシナリオに適合しません。例えばゾーン横断シナリオで、あるゾーンから別のゾーンに移動しないなど。	条件を含め、シナリオが正しく指定されていることを確認してください。
ターゲットは検知されていますが、分類が間違っています (車両を人物、または人物を車両と認識する)。	カメラの高さ、位置、向きが正しくありません。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。
	カメラがゾーンから離れすぎています。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。
	キャリブレーションの精度が十分ではありません。	カメラのキャリブレーションを確認してください。 AXIS Perimeter Defender Setupに移動します。
検知エリアへの侵入がないのに、AXIS Perimeter Defenderによりアラームが生成されます。	分析の感度が高すぎます。	感度を低くしてください。 AXIS Perimeter Defender Setupに移動します。
	キャリブレーションの精度が十分ではありません。	カメラのキャリブレーションを検証してください。 AXIS Perimeter Defender Setupに移動します。
	カメラが移動し、キャリブレーションが不正確になりました。	キャリブレーションをやり直してください。
	カメラの高さ、位置、向きが正しくありません。	取り付け要件を満たしていることを確認してください。*15ページカメラを取り付ける*を参照してください。
	カメラが動いています (揺れている、振動しているなど)。	カメラをより安定した環境に設置してください。

トラブルシューティング

問題	考えられる理由	対処法
	植物や旗など他の動体がカメラの近くにあります。	カメラの視野を妨げる物を取り除きます。シーン内に常に存在するがカメラと近くない物体は、AXIS Perimeter Defenderで無視されます。
	昆虫がカメラレンズの上または近くを歩いています。	可能な限り、昆虫がカメラレンズの上または近くを侵害しないようにしてください。

本マニュアルは、AXIS Perimeter Defenderの管理者およびユーザーを対象としています。本マニュアルには、製品をネットワーク上で使用し、管理するための手順を記載しています。ネットワークに関する経験があると、本製品を使用する上で役に立ちます。

商標

ユーザーマニュアル
AXIS Perimeter Defender

Ver. M15.5
日付: 2021年8月
文書番号 T10068952