

AXIS M31 Dome Camera Series

AXIS M3125-LVE Dome Camera

AXIS M3126-LVE Dome Camera

AXIS M3128-LVE Dome Camera

目次

インストール.....	4
プレビューモード.....	4
使用に当たって.....	5
ネットワーク上のデバイスを検索する.....	5
ブラウザサポート.....	5
装置のwebインターフェースを開く.....	5
管理者アカウントを作成する.....	5
安全なパスワード.....	6
デバイスのソフトウェアが改ざんされていないことを確認する.....	6
webインターフェースの概要.....	6
デバイスを構成する.....	7
基本設定.....	7
画像を調整する.....	7
カメラを水平にする.....	7
露出モードを選択する.....	7
ナイトモードを使用して低光量下で赤外線照明からメリットを得る.....	8
赤外線照明を最適化する.....	8
低照度環境でノイズを減らす.....	8
低光量下で動きによる画像のブレを減らす.....	8
最大限に詳細な画像を撮影する.....	9
逆光の強いシーンを処理する.....	9
細長いエリアを監視する.....	10
ピクセル解像度の確認.....	10
プライバシーマスクで画像の一部を非表示にする.....	11
画像オーバーレイを表示する.....	11
テキストオーバーレイを表示する.....	12
ビデオを表示する、録画する.....	12
帯域幅とストレージ容量を削減する.....	12
ネットワークストレージを設定する.....	12
ビデオを録画して見る.....	13
ビデオが改ざんされていないことを確認する.....	13
イベントのルールを設定する.....	13
アクションをトリガーする.....	14
カメラが物体を検知したときにビデオを録画する.....	14
装置が物体を検知したときにビデオストリームにテキストオーバーレイを表示する.....	14
カメラレンズに対するいたずらがあったときに通知をトリガーする.....	15
音声.....	16
録画に音声を追加する.....	16
ポートキャストを使用した本製品への音声機能の追加.....	16
ネットワークスピーカーに接続する.....	17
webインターフェース.....	18
詳細情報.....	19
長距離接続.....	19
表示エリア.....	19
キャプチャーモード.....	19
プライバシーマスク.....	20
オーバーレイ.....	20
パン、チルト、ズーム (PTZ).....	21
ガードツアー.....	21
ストリーミングとストレージ.....	21
ビデオ圧縮形式.....	21
画像、ストリーム、およびストリームプロファイルの各設定の相互関連性について.....	22

ビットレート制御	22
エッジツーエッジ技術	23
スピーカーのペアリング	23
分析機能とアプリ	24
AXIS People Counter	24
AXIS ブロックビュー検知	24
AXIS Object Analytics	25
メタデータの可視化	25
サイバーセキュリティ	25
Axis Edge Vault	25
署名付きOS	26
セキュアブート	26
安全なキーストア	26
AxisデバイスID	26
署名付きビデオ	26
EFS（暗号化ファイルシステム）	26
Axisセキュリティ通知サービス	27
脆弱性の管理	27
Axis装置のセキュアな動作	27
仕様	28
製品概要	28
.....	28
LEDインジケータ	28
フォーカスアシスタント用ステータスLEDの動作	29
SDカードスロット	29
ボタン	29
コントロールボタン	29
コネクタ	29
ネットワーク コネクタ	29
装置を清掃する	30
トラブルシューティング	31
工場出荷時の設定にリセットする	31
AXIS OSのオプション	31
AXIS OSの現在のバージョンを確認する	31
AXIS OSをアップグレードする	32
技術的な問題と解決策	32
パフォーマンスに関する一般的な検討事項	35
サポートに問い合わせる	36

インストール

以下のビデオでは、AXIS M3125-LVE/ M3126-LVE/M3128-LVE Dome Cameraの設置方法の例を説明しています。

すべての設置シナリオの詳細な手順と重要な安全情報については、axis.com/products/axis-m3125-lve/supportで設置ガイドを参照してください。



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

プレビューモード

プレビューモードは、設置担当者が設置中にカメラビューを微調整する際に最適です。プレビューモードでは、カメラビューにアクセスするのにログインする必要はありません。このモードは、装置の電源投入から一定時間、工場出荷時の設定状態でのみ使用できます。



このビデオを見るには、このドキュメントのWebバージョンにアクセスしてください。

このビデオでは、プレビューモードの使用方法について説明しています。

使用に当たって

ネットワーク上のデバイスを検索する

Windows®で検索したAxisデバイスにIPアドレスの割り当てを行うには、AXIS IP UtilityまたはAXIS Device Managerを使用します。いずれのアプリケーションも無料で、axis.com/supportからダウンロードできます。

IPアドレスの検索や割り当てを行う方法の詳細については、*IPアドレスの割り当てとデバイスへのアクセス方法を参照してください。*

ブラウザーサポート

以下のブラウザーでデバイスを使用できます。

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
その他のオペレーティングシステム	*	*	*	*

✓: 推奨:

*: 制限付きでサポート

装置のwebインターフェースを開く

1. ブラウザーを開き、Axis装置のIPアドレスまたはホスト名を入力します。本製品のIPアドレスが不明な場合は、AXIS IP UtilityまたはAXIS Device Managerを使用して、ネットワーク上のデバイスを見つけます。
2. ユーザー名とパスワードを入力します。装置に初めてアクセスする場合は、管理者アカウントを作成する必要があります。管理者アカウントを作成する, *on page 5*を参照してください。

AXIS OS搭載デバイスのWebインターフェースのすべての機能および設定に関する説明は、AXIS OS Webインターフェースのヘルプを参照してください。

管理者アカウントを作成する

装置に初めてログインするときには、管理者アカウントを作成する必要があります。

1. ユーザー名を入力してください。
2. パスワードを入力します。安全なパスワード, *on page 6*を参照してください。
3. パスワードを再入力します。
4. 使用許諾契約書に同意します。
5. [Add account (アカウントを追加)] をクリックします。

重要

装置にはデフォルトのアカウントはありません。管理者アカウントのパスワードを紛失した場合は、装置をリセットする必要があります。工場出荷時の設定にリセットする, *on page 31*を参照してください。

安全なパスワード

重要

ネットワーク上でパスワードやその他の機密設定を行う場合は、HTTPS (デフォルトで有効になっています) を使用してください。HTTPSを使用すると、安全で暗号化された形でネットワークに接続できるため、パスワードなどの機密データを保護できます。

デバイスのパスワードは主にデータおよびサービスを保護します。Axisデバイスは、さまざまなタイプのインストールで使用できるようにするためパスワードポリシーを強制しません。

データを保護するために、次のことが強く推奨されています。

- 8文字以上のパスワードを使用する (できればパスワード生成プログラムで作成する)。
- パスワードを公開しない。
- 一定の期間ごとにパスワードを変更する (少なくとも年に1回)。

デバイスのソフトウェアが改ざんされていないことを確認する

装置に元のAXIS OSが搭載されていることを確認するか、またはセキュリティ攻撃が行われた後に装置を完全に制御するには、以下の手順に従います。

1. 工場出荷時の設定にリセットします。工場出荷時の設定にリセットする, on page 31を参照してください。
リセットを行うと、セキュアブートによって装置の状態が保証されます。
2. デバイスを設定し、インストールします。

webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。



Axis装置のwebインターフェース

デバイスを構成する

このセクションでは、ハードウェアのインストールが完了した後に製品を起動して実行するために、設置者が行う必要のあるすべての重要な設定について説明しています。

基本設定

取り付け位置を設定する

1. [Video (ビデオ)] > 「Installation (インストール)」 > [Mounting position (取り付け位置)] に移動します。
2. [Change (変更)] をクリックします。
3. 取り付け位置を選択し、[Save and restart (保存して再起動)] をクリックします。

電源周波数を設定する

1. [Video (ビデオ)] > [Installation (インストール)] > [Power line frequency (電源周波数)] に移動します。
2. 電源周波数を選択し、[Save and restart (保存して再起動)] をクリックします。

Set the orientation (向きを設定する)

1. [Video > Installation > Rotate (ビデオ > インストール > 回転)] に移動します。
2. [0]、[90]、[180]、または [270] 度を選択します。
細長いエリアを監視する, on page 10も参照してください。

画像を調整する

このセクションでは、デバイスの設定について説明します。特定の機能の詳細については、詳細情報, on page 19を参照してください。

カメラを水平にする

参照エリアまたは物体との関係で表示を調整するには、レベルグリッドとカメラの機械的な調整を組み合わせ使用します。

1. [Video (ビデオ)] > [Image (画像)] > に移動して、 をクリックします。
2.  をクリックすると、レベルグリッドが表示されます。
3. 参照エリアまたは物体の位置がレベルグリッドと揃うまで、カメラを機械的に調整します。

露出モードを選択する

監視カメラのシーンに合わせて画質を向上させるには、露出モードを使用します。露出モードでは、開口、シャッター、ゲインを制御できます。[Video (ビデオ)] > Image (画像) > Exposure (露出)] に移動し、以下の露出モードから選択します。

- ほとんどの用途では、[Automatic (自動)] 露出を選択します。
- 蛍光灯など、特定の人工照明がある環境では、[Flicker-free (ちらつき防止)] を選択します。
電源周波数と同じ周波数を選択します。
- 蛍光灯照明がある夜間の屋外や太陽光が射す日中の屋外など、特定の人工照明や明るい光がある環境では、[Flicker-reduced (ちらつき低減)] を選択します。
電源周波数と同じ周波数を選択します。
- 現在の露出設定を固定するには、[Hold current (現在の状態で固定)] を選択します。

ナイトモードを使用して低光量下で赤外線照明からメリットを得る

日中、カメラは可視光を利用してカラー画像を提供します。しかし、可視光線が薄くなると、色の画像は明るく鮮明になります。この場合、ナイトモードに切り替えた場合、カメラは可視光と近赤外線の両方の光を使用して、代わりに明るい画像と詳細な白黒画像を提供します。カメラが自動的にナイトモードに切り替わります。

1. [Video > Image > Day and night (設定 > 画像 > デイナイト)] に移動し、[IR cut filter (IR カットフィルター)] が [Auto (自動)] に設定されていることを確認します。
2. カメラがナイトモードに切り替わる光量レベルを設定するには、[Threshold (閾値)] スライダーを [Bright (明るい)] または [Dark (暗い)] の方に動かします。
3. [Allow illumination (照明を許可)] と [Synchronize illumination (照明の同期)] を有効にすると、ナイトモードのときにカメラ内蔵の赤外線照明を使用できます。

注

明るいときにナイトモードにスイッチ設定した場合、低光量ノイズが少ないため画像のシャープさが残ります。暗いときにスイッチ設定した場合、画像のカラーはより長く維持されますが、低光量ノイズによる画像のブレが多くなります。

赤外線照明を最適化する

シーン内の外部光源など、設置環境やカメラの周囲の状況に応じてLEDの強度を手動で調整すると、画質が向上する場合があります。LEDからの反射に問題がある場合は、強度を下げてください。

1. [Video (ビデオ)] > [Image (画像)] > [Day-night mode (デイトナイトモード)] に移動します。
2. [Allow illumination (照明を許可)] をオンにします。
3. ライブビューで  をクリックし、[Manual (手動)] を選択します。
4. 強度を調整します。

低照度環境でノイズを減らす

低照度の条件下でノイズを少なくするために、以下のうち1つ以上の設定ができます。

- ノイズと動きによる画像のブレの間のトレードオフを調整します。[Settings > Image > Exposure (設定 > 画像 > 露出)] に移動し、[Blur-noise trade-off (ブレとノイズのトレードオフ)] スライダーを [Low noise (低ノイズ)] の方に動かします。
- [露出モード] を [自動] に設定します。

注

最大シャッター値が高いと、動きによる画像のブレが生じる場合があります。

- シャッター速度を遅くするには、最大シャッターをできるだけ大きな値に設定します。

注

最大ゲインを下げると、画像が暗くなる場合があります。

- 最大ゲインをより低い値に設定します。
- 開口部スライダーがある場合は、開口部の方向に動かします。
- [Video (ビデオ)] > [Image (画像)] > [Appearance (外観)] で、画像のシャープネスを下げます。

低光量下で動きによる画像のブレを減らす

低光量の条件下で画像のブレを少なくするために、[Video (ビデオ)] > [Image (画像)] > [Exposure (露出)] で次の1つ以上の設定を調整することができます。

- [Exposure mode (露出モード)] を [Automatic (自動)] に設定し、[Motion-adaptive exposure (動き適応露出)] をオンにします。

注

ゲインを大きくすると、画像のノイズが多くなります。

- [Max shutter (最大シャッター)] を短い時間に設定し、[Max gain (最大ゲイン)] をより高い値に設定します。

それでも動きによる画像のブレに問題がある場合は、

- シーン内の光源レベルを上げます。
- 物体が横向きではなく、カメラの方へ移動するか、カメラから離れるように移動するようにカメラを取り付けます。

最大限に詳細な画像を撮影する

重要

最大限に詳細な画像を撮影すると、ビットレートが増加し、フレームレートが低下する場合があります。

- 解像度が最大のキャプチャーモードを選択したことを確認してください。
- [Video (ビデオ) > Stream (ストリーム) > General (一般)] に移動し、圧縮率を可能な限り低く設定します。
- ライブビュー画像で  をクリックし、[Video format (ビデオ形式)] で [MJPEG] を選択します。
- Video > Stream > Zipstream (ビデオ > ストリーム > Zipstream) に移動し、[Off (オフ)] を選択します。

逆光の強いシーンを処理する

ダイナミックレンジとは、画像内の明るさのレベルの差のことです。最も暗い部分と最も明るい部分の差がかなり大きい場合があります。その場合、暗い部分が明るい部分の画像だけが見えることがよくあります。ワイドダイナミックレンジ (WDR) を使用すると、画像の暗い部分と明るい部分の両方が見えるようになります。



WDRを使用していない画像。



WDRを使用している画像。

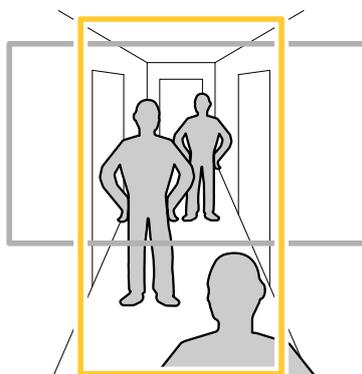
注

- WDRを使用すると、画像にノイズが発生することがあります。
 - WDRは、一部のキャプチャーモードでは使用できない場合があります。
1. [Settings > Image > Wide dynamic range (設定 > 画像 > ワイドダイナミックレンジ)] に移動します。
 2. WDR をオンにします。
 3. それでも問題が発生する場合は、[Exposure (露出)] に移動して [Exposure zone (露出エリア)] を調整し、対象範囲をカバーします。

WDRとその使用方法の詳細については、axis.com/web-articles/wdrをご覧ください。

細長いエリアを監視する

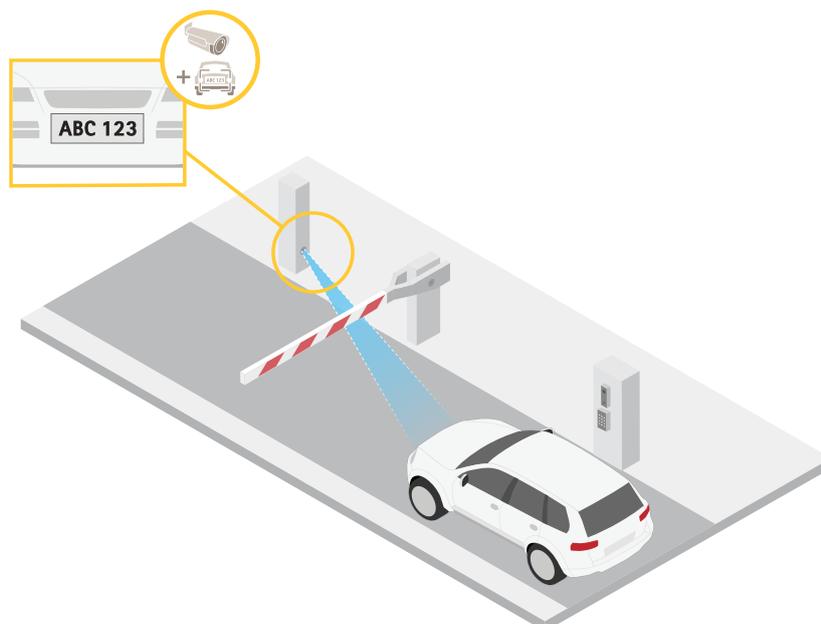
階段、廊下、道路またはトンネルなどの細長いエリアにおける視野をすべてよりよく活用するためには、Corridor Formatを使用します。



1. デバイスによって、カメラまたはカメラの3軸レンズの向きを90° または270° 回転します。
2. 装置がビューの自動回転を行わない場合は、[Video (ビデオ) > Installation (インストール)] に移動します。
3. 視野を90° または270° 回転させます。

ピクセル解像度の確認

画像の定義された部分に、ナンバープレートなどを認識するのに十分なピクセルが含まれていることを確認するには、ピクセルカウンターを使用します。



1. [Video > Image (ビデオ > 画像)] に移動します。
2.  をクリックします。
3. ピクセルカウンターの  をクリックします。
4. カメラのライブビューで、ナンバープレートが表示されると予想される位置など、対象範囲の四角形のサイズおよび位置を調整します。
5. 四角形の各辺 (XとY) のピクセル数が表示され、値がニーズを満たすのに十分かどうかを決定することができます。

プライバシーマスクで画像の一部を非表示にする

1つ以上のプライバシーマスクを作成して、画像の一部を隠すことができます。

1. [Video (ビデオ) > Privacy masks (プライバシーマスク)] に移動します。
2.  をクリックします。
3. 新しいマスクをクリックし、名前を入力します。
4. 必要に応じて、プライバシーマスクのサイズと位置を調整します。
5. すべてのプライバシーマスクの色を変更するには、[Privacy masks (プライバシーマスク)] をクリックし、色を選択します。

プライバシーマスク, on page 20も参照してください。

画像オーバーレイを表示する

ビデオストリームのオーバーレイとして画像を追加することができます。

1. [Video (ビデオ)] > [Overlays (オーバーレイ)] に移動します。
2. 画像管理をクリックします。
3. 画像をアップロードまたはドラッグアンドドロップします。
4. [Upload (アップロード)] をクリックします。
5. ドロップダウンリストから画像を選択して、 をクリックします。

6. 画像と位置を選択します。ライブビューのオーバーレイ画像をドラッグして位置を変更することもできます。

テキストオーバーレイを表示する

ビデオストリームにオーバーレイとしてテキストフィールドを追加することができます。これは、ビデオストリームに日付、時刻、会社名を表示する場合に便利です。

1. [Video (ビデオ)] > [Overlays (オーバーレイ)] に移動します。
2. [Text (テキスト)]を選択し、**+** をクリックします。
3. 表示したいテキストを入力するか、修飾子を選択して現在の日付などを表示します。
4. 位置を選択します。ライブビューのオーバーレイをクリックし、ドラッグして位置を変更することもできます。

ビデオを表示する、録画する

このセクションでは、デバイスの設定について説明します。ストリーミングとストレージの動作の詳細については、*ストリーミングとストレージ, on page 21*を参照してください。

帯域幅とストレージ容量を削減する

重要

帯域幅を削減すると、画像の詳細が失われる場合があります。

1. [Video (ビデオ) > Stream (ストリーム)] に移動します。
2. ライブビューで  をクリックします。
3. 装置がAV1をサポートしている場合は、[Video format (ビデオ形式) AV1] を選択します。サポートしていない場合は [H.264] を選択します。
4. [Video (ビデオ) > Stream (ストリーム) > General (一般)] に移動し、[Compression (圧縮率)] を上げます。
5. [Video > Stream > Zipstream (ビデオ > ストリーム > Zipstream)] に移動し、以下の1つまたは複数の手順を実行します。

注

[Zipstream] の設定は、MJPEGを除くすべてのビデオエンコーディングに使用されます。

- 使用するZipstreamの**Strength (強度)**を選択します。
- [Optimize for storage (ストレージ用に最適化)] をオンにします。この機能は、ビデオ管理ソフトウェアがBフレームをサポートしている場合にのみ使用できます。
- [Dynamic FPS (ダイナミックFPS)] をオンにする。
- [Dynamic GOP (ダイナミックGOP)] をオンにし、GOP 長を高い [Upper limit (上限)] に設定する。

注

ほとんどのWebブラウザはH.265のデコードに対応していないため、装置はwebインターフェースでH.265をサポートしていません。その代わりに、H.265デコーディングに対応したビデオ管理システムやアプリケーションを使用できます。

ネットワークストレージを設定する

ネットワーク上に録画を保存するには、以下のようにネットワークストレージを設定する必要があります。

1. [System > Storage (システム > ストレージ)] に移動します。

2. [Network storage (ネットワークストレージ)]で  [Add network storage (ネットワークストレージを追加)]をクリックします。
3. ホストサーバーのIPアドレスを入力します。
4. [Network Share (ネットワーク共有)] で、ホストサーバー上の共有場所の名前を入力します。
5. ユーザー名とパスワードを入力します。
6. SMBバージョンを選択するか、[Auto (自動)] のままにします。
7. 一時的な接続の問題が発生した場合や、共有がまだ設定されていない場合は、[Add share without testing (テストなしで共有を追加する)] を選択します。
8. [追加] をクリックします。

ビデオを録画して見る

カメラから直接ビデオを録画する

1. [Video (ビデオ) > Stream (ストリーム)] に移動します。
2. 録画を開始するには、  をクリックします。

ストレージを設定していない場合は、  および  をクリックします。ネットワークストレージの設定手順については、ネットワークストレージを設定する, on page 12を参照してください。

3. 録画を停止するには、もう一度  をクリックします。

ビデオを見る

1. [Recordings (録画)] に移動します。
2. リスト内で録画の  をクリックします。

ビデオが改ざんされていないことを確認する

署名付きビデオであれば、カメラで録画されたビデオが誰にも改ざんされていないことを確認することができます。

1. [Video > Stream > General (ビデオ > ストリーム > 全般)] に移動し、[Signed video (署名付きビデオ)] をオンにします。
2. AXIS Camera Station (5.46以降) または互換性のある別のビデオ管理ソフトウェアを使用してビデオを録画します。手順については、AXIS Camera Stationユーザーマニュアルを参照してください。
3. 録画したビデオをエクスポートします。
4. AXIS File Playerを使用してビデオを再生します。AXIS File Playerをダウンロードします。

 は、ビデオが改ざんされていないことを示しています。

注

ビデオの詳細な情報を得るには、ビデオを右クリックして、[Show digital signature (デジタル署名を表示)] を選択します。

イベントのルールを設定する

特定のイベントが発生したときにデバイスにアクションを実行させるように、ルールを作成することができます。ルールは条件とアクションで構成されます。条件を使用して、アクションをトリガーすることができます。たとえば、デバイスは動きを検知したときに、録画を開始したり、電子メールを送信したりすることができ、デバイスが録画をしている間にオーバーレイテキストを表示することができます。

詳細については、「イベントのルールの使用開始」を参照してください。

アクションをトリガーする

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。このルールでは、装置が特定のアクションを実行するタイミングを定義します。ルールは、スケジュールや繰り返しとして設定することも、手動でトリガーするように設定することもできます。
2. [Name (名前)] に入力します。
3. アクションをトリガーするために満たす必要がある [Condition (条件)] を選択します。ルールに複数の条件を指定した場合は、すべての条件が満たされたときにアクションがトリガーされます。
4. 条件が満たされたら実行する Action (アクション) を選択します。

注

- アクティブなルールを変更する場合は、ルールを再度オンにして変更内容を有効にする必要があります。
- ルールに使用されるストリームプロファイルの定義を変更する場合は、そのストリームプロファイルを使用するすべてのルールを再び開始する必要があります。

カメラが物体を検知したときにビデオを録画する

この例では、カメラが物体を検知したときにSDカードへの録画を開始するようにカメラを設定する方法について説明します。録画には、検知開始前の5秒と検知終了後の1分の映像が含まれます。

開始する前に、以下をご確認ください。

- SDカードが装着されていることを確認します。

AXIS Object Analyticsが実行されていることを確認します。

1. [Apps (アプリ) > AXIS Object Analytics] に移動します。
2. アプリケーションが実行されていない場合は、起動します。
3. ニーズに合わせてアプリケーションを設定していることを確認します。

ルールの作成:

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. [Application (アプリケーション)] の [Object Analytics] を選択します。
4. アクションのリストで、[Recordings (録画)] の [Record video while the rule is active (ルールがアクティブである間、ビデオを録画する)] を選択します。
5. ストレージオプションのリストで、[SD_DISK] を選択します。
6. カメラとストリームプロファイルを選択します。
7. プリバッファ時間を5秒に設定します。
8. ポストバッファ時間を [1 minute(1分)] に設定します。
9. [保存] をクリックします。

装置が物体を検知したときにビデオストリームにテキストオーバーレイを表示する

この例では、装置が物体を検知したときに「動体検知」というテキストを表示する方法を示します。

AXIS Object Analyticsが実行されていることを確認します。

1. [Apps (アプリ) > AXIS Object Analytics] に移動します。

2. アプリケーションが実行されていない場合は、起動します。
3. ニーズに合わせてアプリケーションを設定していることを確認します。

オーバーレイテキストの追加:

1. **[Video (ビデオ)] > [Overlays (オーバーレイ)]** に移動します。
2. **[Overlays (オーバーレイ)]** で **[Text (テキスト)]** を選択し、**+** をクリックします。
3. テキストフィールドに #D と入力します。
4. テキストのサイズと外観を選択します。
5. テキストオーバーレイを配置するには、 をクリックしてオプションを選択します。

ルールの作成:

1. **[System > Events (システム > イベント)]** に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. **[Application (アプリケーション)]** の **[Object Analytics]** を選択します。
4. アクションのリストで **[Overlay text (オーバーレイテキスト)]** で、**[Use overlay text (オーバーレイテキストを使用する)]** を選択します。
5. ビデオチャンネルを選択します。
6. **[Text (テキスト)]** に「動体検知」と入力します。
7. 期間を設定します。
8. **[保存]** をクリックします。

注

オーバーレイテキストを更新すると、自動的にすべてのビデオストリームでテキストが動的に更新されます。

カメラレンズに対するいたずらがあったときに通知をトリガーする

この例では、カメラのレンズにスプレーが吹き付けられたり、レンズが覆われたり、汚されたりしたときの電子メール通知を設定する方法を説明します。

いたずら検知をアクティブにする:

1. **[System > Detectors > Camera tampering (システム > 検知 > カメラに対するいたずら)]** に移動します。
2. **[Trigger delay (トリガー遅延)]** の値を設定します。この値は、メールが送信される前に経過する必要がある時間を示します。
3. **Trigger on dark images (暗い画像でトリガー)** をオンにすると、レンズにスプレーが吹き付けられたり、覆われたり、フォーカスがぼやけた場合に検知します。

メール送信先を追加する:

4. **[System > Events > Recipients (システム > イベント > 送信先)]** に移動し、送信先を追加します。
5. 送信先の名前を入力します。
6. 通知のタイプとして **電子メール** を選択します。
7. 送信先の電子メールアドレスを入力します。
8. カメラが通知を送信する際の、送信元電子メールアドレスを入力します。
9. 電子メール送信用アカウントのログイン詳細とSMTPホスト名、ポート番号を入力します。
10. 電子メールの設定をテストするには、**[Test (テスト)]** をクリックします。
11. **[保存]** をクリックします。

ルールの作成:

12. [System > Events > Rules (システム > イベント > ルール)] に移動し、ルールを追加します。
13. ルールの名前を入力します。
14. 条件のリストで、[Video (ビデオ)]の[Tampering (いたずら)] を選択します。
15. [Notifications (通知)] のアクションのリストで、[Send notification to email (電子メールに通知を送る)] を選択し、リストから送信先を選択します。
16. 電子メールの件名とメッセージを入力します。
17. [保存] をクリックします。

音声

録画に音声を追加する

音声をオンにする:

1. [Video > Stream > Audio (ビデオ > ストリーム > 音声)] に移動し、音声を対象に含めます。
2. 装置に複数の入力ソースがある場合は、ソースで適切な ソースを選択します。
3. [Audio > Device settings (音声 > デバイスの設定)] に移動し、適切な入力ソースをオンにします。
4. 入力ソースを変更する場合は、[Apply changes (変更を適用する)] をクリックします。

録画に使用するストリームプロファイルを編集します:

5. [System (システム) > Stream profiles (ストリームプロファイル)] に移動し、ストリームプロファイルを選択します。
6. **Include audio (音声を含める)** を選択してオンにします。
7. [保存] をクリックします。

ポートキャストを使用した本製品への音声機能の追加

ポートキャストテクノロジーを使用すると、本製品に音声機能を追加できます。カメラとインターフェースの間のネットワークケーブルを通じた音声およびI/Oのデジタル通信が可能になります。

Axisネットワークビデオ装置に音声機能を追加するには、装置と電力を供給するPoEスイッチの間に、ポートキャスト対応のAxis audio device and I/O Interfaceを接続します。

1. Axisネットワークビデオ装置 (1) とAxisポートキャスト装置 (2) をPoEケーブルで接続します。
2. Axisポートキャスト装置 (2) とPoEスイッチ (3) をPoEケーブルで接続します。



- 1 Axisネットワークビデオデバイス
- 2 Axisポートキャスト装置
- 3 スイッチ

デバイスを接続すると、Axisネットワークビデオデバイスの設定に音声タブが表示されるようになります。その音声タブに移動し、[Allow audio (音声を有効にする)] をオンにします。

詳細については、Axisポートキャスト装置のユーザーマニュアルを参照してください。

ネットワークスピーカーに接続する

ネットワークスピーカーペアリングを使用すると、対応するAxisネットワークスピーカーを、カメラに直接接続されているかのように使用できます。ペアリングされると、スピーカーは音声出力装置として機能し、カメラを通して音声クリップを再生したり、音声を送信したりできます。

重要

この機能をビデオ管理ソフトウェア (VMS) と共に使用するには、まずカメラをネットワークスピーカーとペアリングしてから、カメラをVMSに追加する必要があります。

カメラをネットワークスピーカーとペアリングする

1. [System > Edge-to-edge > Pairing (システム > エッジツーエッジ > ペアリング)] に移動します。
2.  **Add (追加)** をクリックし、ドロップダウンリストからペアリングタイプの **[Audio (音声)]** を選択します。
3. **[Speaker pairing (スピーカーのペアリング)]** を選択します。
4. ネットワークスピーカーのIPアドレス、ユーザー名とパスワードを入力します。
5. **[接続]** をクリックします。確認メッセージが表示されます。

webインターフェース

AXIS OS搭載デバイスのWebインターフェースで利用可能なすべての機能と設定については、*AXIS OS Webインターフェースのヘルプ*に移動します。

詳細情報

長距離接続

本製品は、メディアコンバータを経由した光ファイバーケーブルの設置に対応しています。光ファイバーケーブルを設置すると、次のようなメリットが得られます。

- 長距離接続
- 高速
- 長寿命
- 大容量のデータ送信
- 電磁干渉耐性

光ファイバーケーブルの設置の詳細については、axis.com/learning/white-papersのホワイトペーパー「長距離監視 - ネットワークビデオにおける光ファイバー通信」を参照してください。

メディアコンバータの設置方法の詳細については、本製品の『インストールガイド』を参照してください。

表示エリア

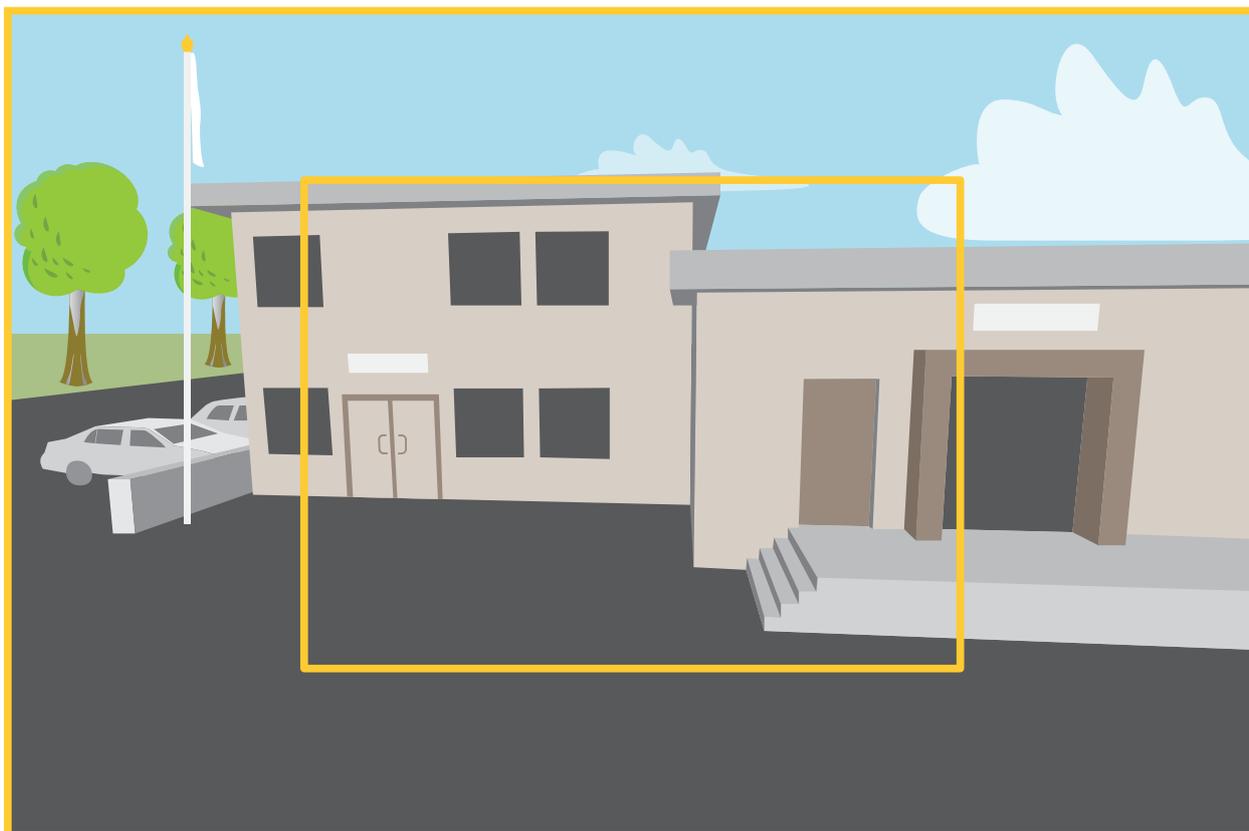
ビューエリアは、全体画像から一部をクリッピングした画像です。全体画像の代わりにビューエリアをストリーミングおよび保存することで、必要な帯域幅とストレージ容量を最小限に抑えることができます。ビューエリアに対してPTZを有効にすると、そのビューエリア内でパン/チルト/ズームを行うことができます。ビューエリアを使用すると、空など全体画像の一部を削除することができます。

ビューエリアを設定するときは、ビデオストリームの解像度をビューエリアのサイズ以下のサイズにすることをお勧めします。ビデオストリームの解像度をビューエリアのサイズより大きいサイズに設定すると、センサーがキャプチャーした後にビデオがデジタルで拡大されるため、画像情報の追加なしでも必要な帯域幅が増えます。

キャプチャーモード

キャプチャーモードは、カメラが画像をキャプチャーする方法を定義するプリセット設定です。キャプチャーモードの設定は、カメラの視野とアスペクト比に影響する場合があります。また、シャッタースピードにも影響するため、ひいては光感度にも影響します。

低解像度のキャプチャーモードは、オリジナルの解像度からサンプリングする場合もあれば、オリジナルから切り出す場合もあり、その場合は視野も影響を受けることになります。



画像は、2種類のキャプチャーモードで視野とアスペクト比をどのように変えることができるかを示しています。

どのキャプチャーモードを選択するかは、特定の監視設定でのフレームレートと解像度の要件によって異なります。利用できるキャプチャーモードの仕様については、axis.comで製品のデータシートを参照してください。

プライバシーマスク

プライバシーマスクは、監視領域の一部をユーザーに非表示にするユーザー定義のエリアです。ビデオストリームで、プライバシーマスクは塗りつぶされたブロックとして表示されます。

プライバシーマスクは、すべてのスナップショット、録画されたビデオ、ライブストリームに表示されます。

VAPIX®アプリケーションプログラミングインターフェース (API) を使用して、プライバシーマスクを非表示にすることができます。

重要

複数のプライバシーマスクを使用すると、製品のパフォーマンスに影響する場合があります。複数のプライバシーマスクを作成できます。各マスクには3~10個のアンカーポイントを設定できます。

オーバーレイ

オーバーレイは、ビデオストリームに重ねて表示されます。オーバーレイは、タイムスタンプなどの録画時の補足情報や、製品のインストール時および設定時の補足情報を表示するために使用します。テキストまたは画像を追加できます。

パン、チルト、ズーム (PTZ)

ガードツアー

ガードツアーを使用して、さまざまなプリセットポジションからのビデオストリームを、設定した時間中、あらかじめ決められた順序またはランダムな順序で表示することができます。ガードツアーを開始すると、映像を視聴しているクライアント (Webブラウザ) が存在しなくなったとしても、停止されるまで動作が継続されます。

注

連続してガードツアーを行う場合、ツアー間の休止時間として最低10分が必要で、固定最短表示時間は10秒です。

ストリーミングとストレージ

ビデオ圧縮形式

使用する圧縮方式は、表示要件とネットワークのプロパティに基づいて決定します。以下から選択を行うことができます。

Motion JPEG

Motion JPEGまたはMJPEGは、個々のJPEG画像の連続で構成されたデジタルビデオシーケンスです。これらの画像は、十分なレートで表示、更新されることで、連続的に更新される動きを表示するストリームが作成されます。人間の目に動画として認識されるためには、1秒間に16以上の画像を表示するフレームレートが必要になります。フルモーションビデオは、1秒間に30フレーム (NTSC) または25フレーム (PAL) で動画と認識されます。

Motion JPEGストリームは、かなりの帯域幅を消費しますが、画質に優れ、ストリームに含まれるすべての画像にアクセスできます。

H.264またはMPEG-4 Part 10/AVC

注

H.264はライセンスされた技術です。このAxis製品には、H.264閲覧用のクライアントライセンスが1つ添付されています。ライセンスされていないクライアントのコピーをインストールすることは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わせください。

H.264を使用すると、画質を損なうことなく、デジタル映像ファイルのサイズを削減でき、Motion JPEG形式の場合と比較すると80%以上、従来のMPEG形式と比較すると50%以上を削減できます。そのため、ビデオファイルに必要なネットワーク帯域幅やストレージ容量が少なくなります。また、別の見方をすれば、より優れた映像品質が同じビットレートで得られることとなります。

H.265またはMPEG-H Part 2/HEVC

H.265を使用すると、画質を損なうことなくデジタルビデオファイルのサイズを削減でき、H.264に比べて25%以上縮小することができます。

注

- H.265はライセンスされた技術です。このAxis製品には、H.265閲覧用のクライアントライセンスが1つ添付されています。ライセンスされていないクライアントのコピーをインストールすることは禁止されています。ライセンスを追加購入するには、Axisの販売代理店までお問い合わせください。
- ほとんどのWebブラウザはH.265のデコードに対応していないため、カメラはWebインターフェースでH.265をサポートしていません。その代わりに、H.265のデコーディングに対応した映像管理システムやアプリケーションを使用できます。

画像、ストリーム、およびストリームプロファイルの各設定の相互関連性について

[Image (画像)] タブには、製品からのすべてのビデオストリームに影響を与えるカメラ設定が含まれています。このタブで変更した内容は、すべてのビデオストリームと録画にすぐに反映されます。

[Stream (ストリーム)] タブには、ビデオストリームの設定が含まれています。解像度やフレームレートなどを指定せずに、製品からのビデオストリームを要求している場合は、これらの設定が使用されます。[Stream (ストリーム)] タブで設定を変更すると、実行中のストリームには影響しませんが、新しいストリームを開始したときに有効になります。

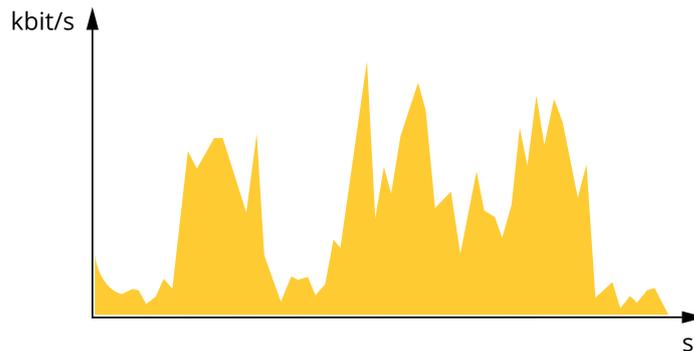
[Stream profiles (ストリームプロファイル)] の設定は、[Stream (ストリーム)] タブの設定よりも優先されます。特定のストリームプロファイルを持つストリームを要求すると、ストリームにそのプロファイルの設定が含まれます。ストリームプロファイルを指定せずにストリームを要求した場合、または製品に存在しないストリームプロファイルを要求した場合、ストリームに [Stream (ストリーム)] タブの設定が含まれます。

ビットレート制御

ビットレート制御で、ビデオストリームの帯域幅の使用量を管理することができます。

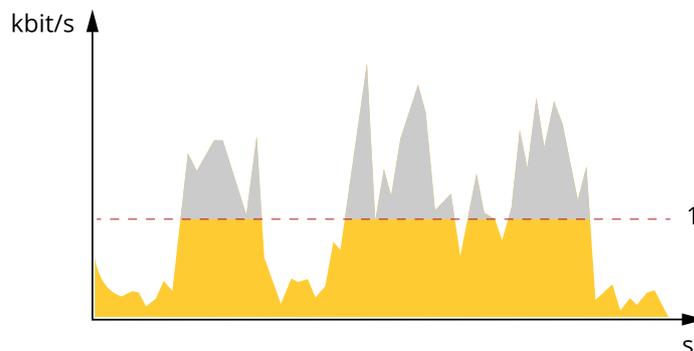
可変ビットレート (VBR)

可変ビットレートでは、シーン内の動きのレベルに基づいて帯域幅の使用量が変化します。シーン内の動きが多いほど、多くの帯域幅が必要です。ビットレートが変動する場合は、一定の画質が保証されますが、ストレージのマージンを確認する必要があります。



最大ビットレート (MBR)

最大ビットレートでは、目標ビットレートを設定してシステムのビットレートを制限することができます。瞬間的なビットレートが指定した目標ビットレート以下に保たれていると、画質またはフレームレートが低下することがあります。画質とフレームレートのどちらを優先するかを選択することができます。目標ビットレートは、予期されるビットレートよりも高い値に設定することをお勧めします。これにより、シーン内で活動レベルが高い場合にマージンを確保します。

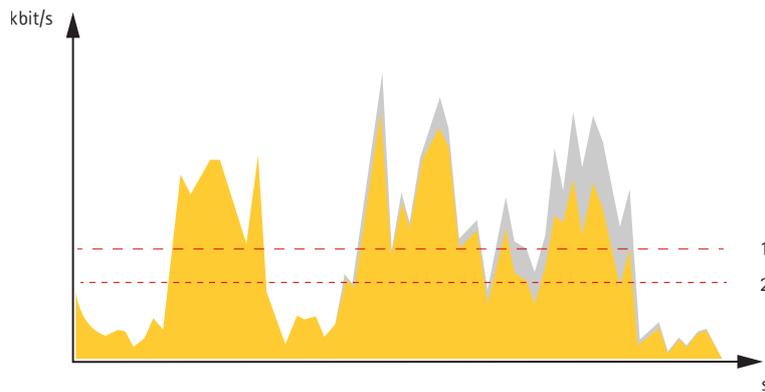


1 目標ビットレート

平均ビットレート (ABR)

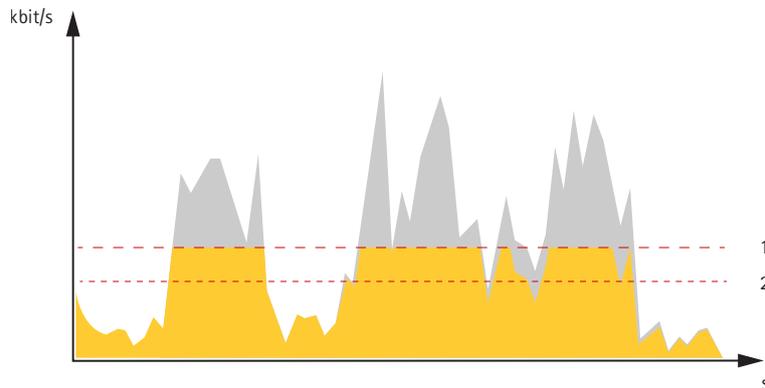
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できません。次のいずれかの方法で、平均ビットレートの設定を指定します。

- 必要なストレージの概算を計算するには、目標ビットレートと保存期間を設定します。
- 使用可能なストレージと必要な保存期間に基づいて平均ビットレートを計算するには、目標ビットレートカリキュレーターを使用します。



1 目標ビットレート
2 実際の平均ビットレート

平均ビットレートオプションの中で、最大ビットレートをオンにし、目標ビットレートを指定することもできます。



1 目標ビットレート
2 実際の平均ビットレート

エッジツーエッジ技術

エッジツーエッジは、IP装置が相互に直接通信できるようにする技術です。たとえば、AxisのカメラとAxisの音声/レーダー製品との間のスマートペアリング機能を提供します。

注

ペアリングされたデバイスが同じAXIS OSバージョンで動作していることを確認してください。

詳しくは、whitepapers.axis.com/edge-to-edge-technology でホワイトペーパー“Edge-to-edge technology”(エッジツーエッジ技術)を参照してください。

スピーカーのペアリング

エッジツーエッジのスピーカーペアリングにより、対応するAxisネットワークスピーカーをカメラの一部であるかのように使用できます。ペアリングすると、スピーカーの機能はカメラのwebイン

ターフェースに統合され、ネットワークスピーカーは音声出力装置として機能し、音声クリップを再生したり、カメラを介して音声を送信したりすることができます。

カメラはVMSで音声出力を内蔵したカメラであると識別され、再生された音声をスピーカーにリダイレクトします。

分析機能とアプリ

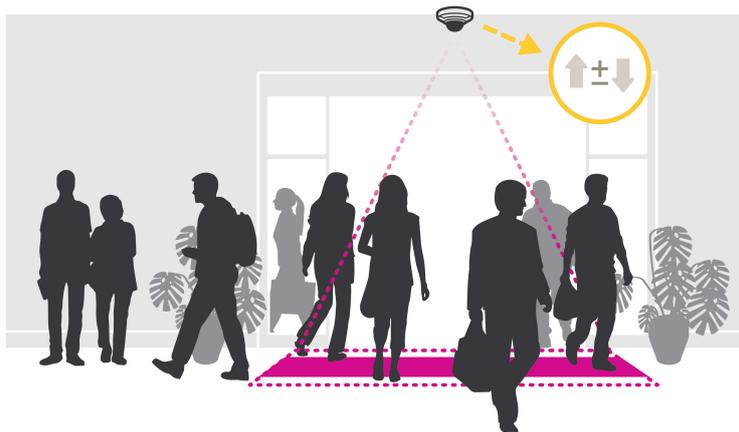
分析機能とアプリを使用することで、Axisデバイスをより活用できます。AXIS Camera Application Platform (ACAP) は、サードパーティによるAxisデバイス向けの分析アプリケーションやその他のアプリの開発を可能にするオープンプラットフォームです。アプリとしては、デバイスにプリインストール済み、無料でダウンロード可能、またはライセンス料が必要なものがあります。

Axisの分析機能とアプリのユーザーマニュアルは、help.axis.comから参照できます。

AXIS People Counter

AXIS People Counterは、ネットワークカメラにインストールできる分析アプリケーションです。アプリケーションを使用して、入り口を通過する人の数、通過する方向、および既定の間隔の間に複数の人が通過した場合に数えることができます。また、この機能を使用して、現在エリアを占有している人の数と平均訪問時間を推定することもできます。

アプリケーションはカメラに内蔵されているため、アプリケーションを実行するために専用のコンピューターは必要ありません。AXIS People Counterは、店舗、図書館、ジムなど、あらゆる屋内環境に適しています。



占有率の推定はどのように機能するのでしょうか。

アプリケーションを使用して、1つまたは複数の入口と出口のあるエリアの占有率を推定することができます。各入口と出口には、AXIS People Counterが設置されたネットワークカメラを装備する必要があります。複数のカメラがある場合は、各カメラはプライマリおよびセカンダリの構成でネットワークを経由し、互いに通信します。プライマリカメラは、継続的にセカンダリカメラからデータを取得し、ライブビューにデータを表示します。15分ごとに、プライマリカメラが統計データをAXIS Store Data Managerに送信します。その結果、AXIS Store Data Managerから生成されるレポートで、最低15分の時間間隔でデータを示すことができます。

AXIS ブロックビュー検知

AXISブロックビュー検知は、レンズが覆われる、スプレーが吹き付けられるなど、カメラに対するいたずらが検知された場合にアラームを発するアプリケーションです。

最適なパフォーマンスを得るには、カメラビューに検知可能な物体、パターンやラインを含めることをお勧めします。



理想的な状況

被写体が少ない場所では、床や天井などは避けてください。



理想的ではない状況

感度の調整やいたずら検知の比率を変更することで、トリガーレベルを設定できます。

AXIS Object Analytics

AXIS Object Analyticsは、カメラにあらかじめ組み込まれている分析アプリケーションです。AXIS Object Analyticsは、シーン内で動く物体を検知し、人や車両などとして分類します。さまざまなタイプの物体にアラームを送信するようにアプリケーションを設定できます。アプリケーションの動作の詳細については、*AXIS Object Analytics*ユーザーマニュアルを参照してください。

メタデータの可視化

分析メタデータは、シーン内の動く物体に使用できます。サポートされている物体クラスが、物体のタイプと分類の信頼度に関する情報と共に、物体を囲む境界ボックスにより、ビデオストリームに可視化されます。分析メタデータの設定および使用方法の詳細については、*AXIS Scene Metadata統合ガイド*を参照してください。

サイバーセキュリティ

サイバーセキュリティに関する製品固有の情報については、axis.comの製品データシートを参照してください。

AXIS OSのサイバーセキュリティの詳細情報については、『*AXIS OS強化ガイド*』を参照してください。

Axis Edge Vault

ハードウェアベースのサイバーセキュリティプラットフォーム「Axis Edge Vault」により、Axisデバイスを保護することができます。装置のIDと整合性を保証し、不正アクセスから機密情報を保護する機能を提供します。これは、エッジデバイスセキュリティに関する専門知識を駆使して、暗

号コンピューティングモジュール（セキュアエレメントやTPM）とSoCセキュリティ（TEEやセキュアブート）に基づき構築された強力な基盤により成り立っています。

署名付きOS

署名付きOSは、ソフトウェアベンダーがAXIS OSイメージを秘密鍵で署名することで実装されます。オペレーティングシステムに署名が付けられると、装置はインストール前にソフトウェアを検証するようになります。装置でソフトウェアの整合性が損なわれていることが検出された場合、AXIS OSのアップグレードは拒否されます。

セキュアブート

セキュアブートは、暗号化検証されたソフトウェアの連続したチェーンで構成される起動プロセスで、不変メモリ（ブートROM）から始まります。署名付きOSの使用に基づいているため、セキュアブートを使うと、装置は認証済みのソフトウェアを使用した場合のみ起動できます。

安全なキーストア

秘密鍵の保護と暗号化動作のセキュアな実行のための改ざん防止環境です。これにより、セキュリティ侵害が発生した場合も、不正アクセスや悪質な抽出を防止することができます。セキュリティ要件に応じて、Axisデバイスには、ハードウェアで保護された安全なキーストアが可能となるハードウェアベースの暗号コンピューティングモジュールを1つまたは複数搭載することができます。セキュリティ要件に応じて、Axis装置は、TPM 2.0 (Trusted Platform Module) やセキュアエレメント、および/またはTEE (Trusted Execution Environment) などのハードウェアベースの暗号コンピューティングモジュールを1台以上持つことができ、ハードウェアで保護されたセキュリティキーストアを提供します。さらに、一部のAxis製品には、FIPS 140-2 Level 2認定のセキュアキーストアを備えています。

AxisデバイスID

デバイスIDの信頼性を確立するには、デバイスの出所を確認できることが鍵となります。Axis Edge Vaultを搭載したデバイスには、生産工程で、工場でのプロビジョニングされ、国際規格（IEEE 802.1AR）に準拠した一意のAxisデバイスID証明書が割り当てられます。これがデバイスの出所を証明するパスポートのような役割を果たします。デバイスIDは、Axisルート証明書により署名された証明要素として、セキュリティで保護されたキーストアに安全かつ永続的に格納されます。お客様のITインフラストラクチャーでデバイスIDを活用し、装置のセキュアな自動化オンボーディングや、装置のセキュアな識別に役立てることが可能です。

署名付きビデオ

署名付きビデオにより、ビデオファイルの管理のチェーンを証明することなく、映像の証拠が改ざんされていないことを確認できるようになります。セキュリティで保護されたキーストアに安全に格納されている独自のビデオ署名キーにより、各カメラのビデオストリームに署名が追加されます。ビデオを再生する際に、ビデオが改ざんされていないかどうかをファイルプレーヤーに表示されます。ビデオに署名が付いていることで、映像を元のカメラまで遡って追跡し、映像がカメラから出た後に改ざんされていないことを確認することが可能となります。

EFS（暗号化ファイルシステム）

安全なキーストアにより、ファイルシステムに強力な暗号化を適用することで、悪質な情報の抽出や設定の改ざんを防止することができます。これにより、装置が使用されていないときや、装置への認証されていないアクセスが行われたとき、Axis装置が盗難されたときに、ファイルシステムに保存されているデータが抽出されたり改ざんされたりすることがなくなります。セキュアブートプロセス中、読み書き可能なファイルシステムは復号化され、Axis装置でマウントして使用できるようになります。

Axis装置のサイバーセキュリティ機能の詳細については、axis.com/learning/white-papers/にアクセスし、サイバーセキュリティを検索してください。

Axisセキュリティ通知サービス

Axisは、Axis装置に関する脆弱性やその他のセキュリティ関連事項についての情報を提供する通知サービスを運営しています。通知を受け取るには、axis.com/security-notification-serviceで購読手続きを行うことができます。

脆弱性の管理

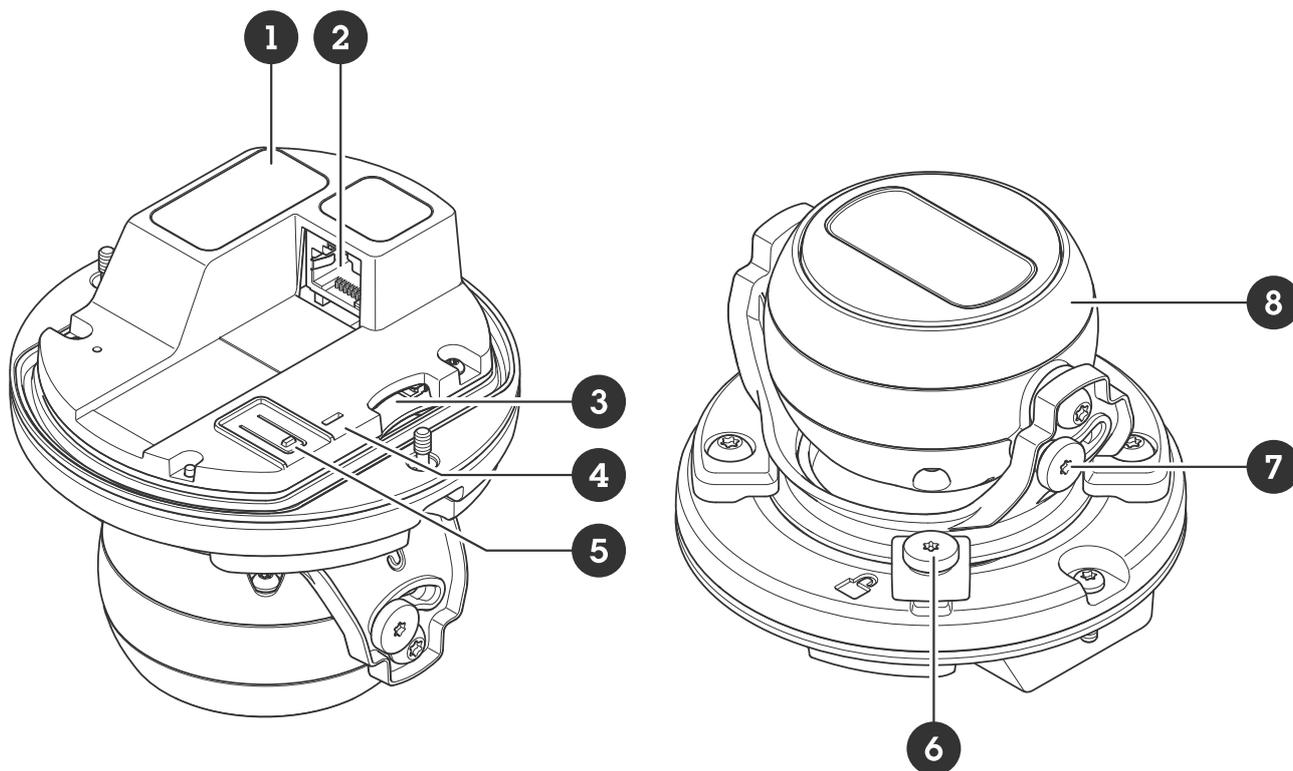
お客様の脆弱性リスクを最小限に抑えるため、Axisは**CVE (共通脆弱性識別子) 採番機関**として業界標準に従って、装置、ソフトウェア、およびサービスで発見された脆弱性の管理と対応を行っています。Axisの脆弱性管理ポリシー、脆弱性の報告方法、すでに公開されている脆弱性、対応するセキュリティ勧告の詳細については、axis.com/vulnerability-managementをご覧ください。

Axis装置のセキュアな動作

工場出荷時の設定のAxis装置は、セキュアなデフォルトの保護メカニズムで事前に設定されています。装置の設置時には、より多くのセキュリティ設定を使用することをお勧めします。装置のセキュリティを確保するためのベストプラクティス、リソース、ガイドラインなど、Axisのサイバーセキュリティに対する取り組みの詳細については、axis.com/about-axis/cybersecurityをご覧ください。

仕様

製品概要



- 1 型番 (P/N) とシリアル番号 (S/N)
- 2 ネットワーク コネクタ (PoE)
- 3 SDカードスロット
- 4 ステータスインジケータLED
- 5 コントロールボタン
- 6 パンの固定ネジ
- 7 チルトの固定ネジ
- 8 回転リング

LEDインジケータ

ステータスLED	説明
消灯	接続時および正常動作時です。
緑	起動後正常に動作する場合、10秒間、緑色に点灯します。
オレンジ	起動時に点灯し、装置のソフトウェアのアップグレード中、または工場出荷時の設定にリセット中に点滅します。
オレンジ/赤	ネットワーク接続が利用できないか、失われた場合は、オレンジ色/赤色で点滅します。
赤	装置のソフトウェアのアップグレードに失敗しました。

ネットワークLED	説明
緑	100メガビット/秒のネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。

オレンジ	10Mbit/sネットワークに接続している場合、点灯します。ネットワークパケットを送受信した場合、点滅します。
消灯	ネットワーク接続なし。

フォーカスアシスタント用ステータスLEDの動作

フォーカスアシスタントが有効のとき、ステータスLEDが点滅します。

カラー	説明
赤	画像がピンぼけしています。 レンズを調整してください。
オレンジ	画像が近すぎてピンぼけしています。 レンズの微調整を行う必要があります。
緑	画像のピントが合っています。

SDカードスロット

注意

- SDカード損傷の危険があります。SDカードの挿入と取り外しの際には、鋭利な工具や金属性の物を使用したり、過剰な力をかけたりしないでください。カードの挿入や取り外しは指で行ってください。
- データ損失や録画データ破損の危険があります。SDカードを取り外す前に、装置のwebインターフェースからマウント解除してください。本製品の稼働中はSDカードを取り外さないでください。

本装置は、microSD/microSDHC/microSDXCカードに対応しています。

推奨するSDカードについては、axis.comを参照してください。

 microSD、microSDHC、およびmicroSDXCロゴは、SD-3C LLCの商標です。microSD、microSDHC、microSDXCは、米国および/または他の国々におけるSD-3C, LLCの商標または登録商標です。

ボタン

コントロールボタン

コントロールボタンは、以下の用途で使用します。

- 製品を工場出荷時の設定にリセットする。工場出荷時の設定にリセットする, *on page 31*を参照してください。
- インターネット経由でワンクリッククラウド接続 (O3C) サービスに接続します。接続するには、ボタンを押してから放し、ステータスLEDが緑色に3回点滅するまで待ちます。

コネクタ

ネットワーク コネクタ

Power over Ethernet (PoE) 対応RJ45イーサネットコネクタ

RJ45 イーサネットサービスポート。

装置を清掃する

装置はぬるま湯で洗浄できます。

注意

- 強力な化学薬品は装置を損傷する可能性があります。窓ガラス用洗剤やアセトンなどの化学薬品を使用して装置をクリーニングしないでください。
 - シミの原因となるため、直射日光や高温下での清掃は避けてください。
1. 圧縮空気を使用すると、装置からほこりやごみを取り除くことができます。
 2. 必要に応じて、ぬるま湯に浸した柔らかいマイクロファイバーの布で装置を清掃してください。
 3. シミを防ぐために、きれいな非研磨性の布で装置から水分を拭き取ってください。

トラブルシューティング

工場出荷時の設定にリセットする

▲ 警告

⚠ 本製品は有害な光を放射することがあります。眼に有害となる可能性があります。動作ランプを凝視しないでください。

重要

工場出荷時の設定へのリセットは慎重に行ってください。工場出荷時の設定へのリセットを行うと、IPアドレスを含むすべての設定が工場出荷時の値にリセットされます。

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。製品概要, on page 28を参照してください。
3. ステータスLEDインジケータがオレンジで点滅するまでコントロールボタンを15~30秒間押し続けます。
4. コントロールボタンを放します。プロセスが完了すると、ステータスLEDが緑色に変わります。ネットワーク上にDHCPサーバーがない場合、装置のIPアドレスのデフォルトは次のいずれかになります。
 - **AXIS OS 12.0以降の装置:** リンクローカルアドレスサブネット (169.254.0.0/16) から取得
 - **AXIS OS 11.11以前の装置:** 192.168.0.90/24
5. インストールおよび管理ソフトウェアツールを使用して、IPアドレスの割り当て、パスワードの設定、装置へのアクセスを行います。
axis.com/supportのサポートページに、インストールおよび管理ソフトウェアツールが用意されています。

装置のwebインターフェースを使用して、各種パラメーターを工場出荷時の設定に戻すこともできます。[Maintenance (メンテナンス) > Factory default (工場出荷時の設定)] に移動し、[Default (デフォルト)] をクリックします。

AXIS OSのオプション

Axisは、アクティブトラックまたは長期サポート (LTS) トラックのどちらかに従って、装置のソフトウェアの管理を提供します。アクティブトラックでは、最新の製品機能すべてに常時アクセスできますが、LTSトラックの場合、バグフィックスやセキュリティ更新に重点を置いた定期的リリースが提供される固定プラットフォームを使用します。

最新の機能にアクセスする場合や、Axisのエンドツーエンドシステム製品を使用する場合は、アクティブトラックのAXIS OSを使用することをお勧めします。最新のアクティブトラックに対して継続的な検証が行われないサードパーティの統合を使用する場合は、LTSトラックをお勧めします。LTSにより、大きな機能的な変更や既存の統合に影響を与えることなく、サイバーセキュリティを維持することができます。Axis装置のソフトウェア戦略の詳細については、axis.com/support/device-softwareにアクセスしてください。

AXIS OSの現在のバージョンを確認する

装置の機能はAXIS OSによって決まります。問題のトラブルシューティングを行う際は、まずAXIS OSの現在のバージョンを確認することをお勧めします。最新バージョンには、特定の問題の修正が含まれていることがあります。

AXIS OSの現在のバージョンを確認するには:

1. 装置のwebインターフェース > [Status (ステータス)] に移動します。
2. [Device info (デバイス情報)] で、AXIS OSのバージョンを確認します。

AXIS OSをアップグレードする

重要

- デバイスソフトウェアのアップグレードでは、既定の設定とカスタマイズ設定が保存されます。Axis Communications ABは、新しいAXIS OSバージョンで機能が利用可能であっても、設定が保存されることを保証できません。
- AXIS OS 12.6以降、お使いのデバイスの現在のバージョンからアップグレードバージョンまでのすべてのLTSバージョンをインストールする必要があります。たとえば、現在インストールされているデバイスソフトウェアのバージョンがAXIS OS 11.2の場合、デバイスをAXIS OS 12.6にアップグレードする前に、LTSバージョンであるAXIS OS 11.11をインストールする必要があります。詳しくは、*AXIS OS Portal: アップグレードパス*を参照してください。
- アップグレードプロセス中は、デバイスを電源に接続したままにしてください。

注

- アクティブトラックのAXIS OSの最新バージョンで装置をアップグレードすると、製品に最新機能が追加されます。アップグレードする前に、AXIS OSと共に提供されるアップグレード手順とリリースノートを必ずお読みください。AXIS OSの最新バージョンとリリースノートについては、axis.com/support/device-software/にアクセスしてください。
1. AXIS OSのファイルをコンピューターにダウンロードします。これらのファイルはaxis.com/support/device-software/から無料で入手できます。
 2. デバイ스에 管理者としてログインします。
 3. **[Maintenance (メンテナンス)] > [AXIS OS upgrade (AXIS OSのアップグレード)]** に移動し、**[Upgrade (アップグレード)]** をクリックします。

アップグレードが完了すると、製品は自動的に再起動します。

AXIS Device Managerを使用すると、複数の装置を同時にアップグレードできます。詳細については、axis.com/products/axis-device-manager/をご覧ください。

技術的な問題と解決策

AXIS OSのアップグレード時の問題

AXIS OSアップグレード失敗

アップグレードに失敗した場合、装置は前のバージョンを再度読み込みます。最も一般的な理由は、AXIS OSの間違ったファイルがアップロードされた場合です。装置に対応したAXIS OSのファイル名であることを確認し、再試行してください。

AXIS OSのアップグレード後の問題

アップグレード後に問題が発生する場合は、**[Maintenance (メンテナンス)]** ページから、以前にインストールされたバージョンにロールバックします。

IPアドレスの設定で問題が発生する

IPアドレスを設定できない

- デバイス用のIPアドレスと、デバイスへのアクセスに使用するコンピューターのIPアドレスが異なるサブネットにある場合は、IPアドレスを設定することはできません。ネットワーク管理者に連絡して、適切なIPアドレスを取得してください。
- そのIPアドレスは別のデバイスで使用されている可能性があります。以下の手順で確認してください。
 1. デバイスをネットワークから切断します。
 2. コマンドウィンドウまたはDOSウィンドウで、pingコマンドとデバイスのIPアドレスを入力します。
 3. Reply from <IP address>: bytes=32; time=10...という応答を受取った場合は、ネットワーク上の別のデバイスでそのIPアドレスがすでに使われている可能性があります。ネットワーク管理者から新しいIPアドレスを取得し、デバイスを再度インストールしてください。
 4. Request timed outが表示された場合は、AxisデバイスでそのIPアドレスを使用できません。この場合は、すべてのケーブル配線をチェックし、デバイスを再度インストールしてください。
- 同じサブネット上の別のデバイスとIPアドレスの競合が発生している可能性があります。DHCPサーバーによって動的アドレスが設定される前は、Axisデバイスは静的IPアドレスを使用します。つまり、デフォルトの静的IPアドレスが別のデバイスでも使用されていると、デバイスへのアクセスに問題が発生する可能性があります。

デバイスへのアクセスの問題

ブラウザからデバイスにアクセスする際、ログインできない

HTTPSが有効になっている場合、ログインを試行するときに正しいプロトコル (HTTPまたはHTTPS) を使用していることを確認します。場合によっては、ブラウザのアドレスフィールドに手動でhttpまたはhttpsを入力する必要があります。

rootアカウントのパスワードを忘れた場合は、デバイスを工場出荷時の設定にリセットする必要があります。手順については、工場出荷時の設定にリセットする, *on page 31*を参照してください。

DHCPによってIPアドレスが変更された

DHCPサーバーから取得したIPアドレスは動的なアドレスであり、変更されることがあります。IPアドレスが変更された場合は、AXIS IP UtilityまたはAXIS Device Managerを使用してデバイスのネットワーク上の場所を特定してください。デバイスのモデルまたはシリアル番号、あるいはDNS名 (設定されている場合) を使用してデバイスを識別します。

必要に応じて、静的なIPアドレスを手動で割り当てることができます。手順については、axis.com/supportにアクセスしてください。

IEEE 802.1X使用時の証明書エラー

認証を正しく行うには、Axisデバイスの日付と時刻をNTPサーバーと同期させなければなりません。[System (システム) > Date and time (日付と時刻)] に移動します。

ブラウザがサポートされていません

推奨ブラウザの一覧は、[ブラウザサポート](#), *on page 5*を参照してください。

外部からデバイスにアクセスできません

装置に外部からアクセスする場合は、以下のいずれかのWindows®向けアプリケーションを使用することをお勧めします。

- AXIS Camera Station Edge：無料で使用でき、最小限の監視が必要な小規模システムに最適です。
- AXIS Camera Station Pro:90日間の試用版を無料で使用でき、中小規模のシステムに最適です。

手順とダウンロードについては、axis.com/vmslにアクセスしてください。

ストリーミングの問題

ローカルクライアントしかマルチキャストH.264にアクセスできない

ルーターがマルチキャストをサポートしているかどうか、またはクライアントと装置の間のルーター設定を行う必要があるかどうかを確認してください。TTL (Time To Live) 値を上げる必要がある場合もあります。

H.264のマルチキャスト画像がクライアントで表示されない

Axisデバイスで使用されたマルチキャストアドレスが有効かどうか、ネットワーク管理者に確認してください。

ファイアウォールが表示を妨げていないかどうか、ネットワーク管理者に確認してください。

H.264画像のレンダリング品質が悪い

グラフィックカードで最新の装置ドライバーが使用されていることを確認してください。最新のドライバーは、通常、メーカーのWebサイトからダウンロードできます。

彩度がH.264とMotion JPEGで異なる

グラフィックアダプターの設定を変更します。詳細については、グラフィックカードのマニュアルを確認してください。

フレームレートが予期したレートより低い

- パフォーマンスに関する一般的な検討事項, on page 35を参照してください。
- クライアントコンピュータで実行されているアプリケーションの数を減らします。
- 同時閲覧者の数を制限します。
- 使用可能な帯域幅が十分かどうか、ネットワーク管理者に確認します。
- 画像の解像度を下げます。
- 装置のwebインターフェースにログインし、フレームレートを優先するキャプチャーモードを設定します。フレームレートを優先するようにキャプチャーモードを変更すると、使用する装置と利用可能なキャプチャーモードによっては、最大解像度が低下することがあります。
- Axisデバイスの電源周波数 (60/50Hz) によって、最大フレーム/秒は異なります。

ライブビューでH.265エンコード方式を選択できない

WebブラウザーではH.265のデコーディングをサポートしていません。H.265のデコーディングに対応した映像管理システムまたはアプリケーションを使用してください。

MQTTの問題

MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールは、ポート8883を使用する通信を安全ではないとみなし、ブロックします。

場合によっては、サーバー/ブローカーによってMQTT通信用に特定のポートが提供されていない可能性があります。この場合でも、HTTP/HTTPSトラフィックに通常使用されるポート経由でMQTTを使用できる場合もあります。

- サーバー/ブローカーが、通常はポート443経由で、WebSocket/WebSocket Secure (WS/WSS) をサポートしている場合は、代わりにこのプロトコルを使用してください。サーバー/ブローカープロバイダーに問い合わせ、WS/WSSがサポートされているかどうか、どのポートと基本パスを使用するかを確認してください。
- サーバー/ブローカーがALPNをサポートしている場合、MQTTの使用は443などのオープンポートでネゴシエートできます。ALPNのサポートの有無、使用するALPNプロトコルとポートについては、サーバー/ブローカーのプロバイダーに確認してください。

デバイスの動作に関する問題

フロントヒーターとワイパーが作動していない

フロントヒーターまたはワイパーがオンにならない場合は、上部カバーがハウジングユニットの底部に正しく固定されているか確認してください。

このページで解決策が見つからない場合は、axis.com/supportのトラブルシューティングセクションに記載されている方法を試してみてください。

パフォーマンスに関する一般的な検討事項

システムを設定する際には、さまざまな設定や条件がシステムのパフォーマンスにどのように影響するかを検討することが重要です。帯域幅 (ビットレート) に影響を与える要因もあれば、フレームレートに影響を与える要因もあり、両方に影響する要因もあります。

考慮すべき最も重要な要因:

- 画像解像度が高い、または圧縮レベルが低いと、画像のファイルサイズが増大し、結果的に帯域幅に影響を及ぼします。
- GUIで画像を回転させると、本製品のCPU負荷が増加することがあります。
- 多数のMotion JPEGクライアントまたはユニキャストH.264/H.265/AV1クライアントによるアクセスは帯域幅に影響します。
- 様々なクライアントが様々な解像度や圧縮方式が異なるストリームを同時に閲覧すると、フレームレートと帯域幅の両方に影響を及ぼします。フレームレートを高く維持するために、できる限り同一ストリームを使用してください。ストリームプロファイルを使用すると、ストリームの種類が同一であることを確認できます。
- 異なるコーデックのビデオストリームへの同時アクセスが発生すると、フレームレートと帯域幅の両方に影響が及ぼされます。最適な性能が実現するように、同じコーデックのストリームを使用してください。
- イベント設定を多用すると、製品のCPU負荷に影響が生じ、その結果、フレームレートに影響します。
- 特に、Motion JPEGのストリーミングでは、HTTPSを使用するとフレームレートが低くなる場合があります。
- 貧弱なインフラによるネットワークの使用率が高いと帯域幅に影響します。

- パフォーマンスの低いクライアントコンピューターで閲覧するとパフォーマンスが低下し、フレームレートに影響します。
- 複数のAXIS Camera Application Platform (ACAP) アプリケーションを同時に実行すると、フレームレートと全般的なパフォーマンスに影響する場合があります。

サポートに問い合わせる

さらにサポートが必要な場合は、axis.com/supportにアクセスしてください。

T10204362_ja

2026-02 (M9.2)

© 2024 – 2026 Axis Communications AB