

AXIS M5075-G PTZカメラ

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
フォーカスを調整する.....	7
フォーカスリコールエリアを使用してフォーカスを迅速に調整する.....	8
低遅延モードで画像処理時間を短縮する.....	9
露出モードを選択する.....	9
低照度環境でノイズを減らす.....	9
逆光の強いシーンを処理する.....	10
たる型歪曲の補正.....	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
パン位置またはチルト位置をテキストオーバーレイとして表示する.....	11
カメラビューを調整する (PTZ).....	11
パン、チルト、およびズーム動作を制限する.....	11
ビデオを表示する、録画する.....	11
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.....	12
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.....	13
カメラが物体を検知したときにビデオを録画する.....	13
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
カメラが動きを検知したときにカメラをプリセットポジションに向ける.....	14
カメラが音量の大きいノイズを検知したときにビデオを録画する.....	15
ゲートキーパーで特定のエリアに自動的にズームインする.....	15
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
Z-Wave®を設定する.....	16
検討事項.....	16
Turn on Z-Wave (Z-Waveをオンにする).....	17
Add a Z-Wave device (Z-Wave装置の追加).....	17
SmartStartを搭載したZ-Wave装置の追加.....	17
Remove a Z-Wave device through inclusion/exclusion mode (対象/除外モードからのZ-Waveデバイスの削除).....	18
Remove a Z-Wave device through forced process (強制プロセスによるZ-Wave装置の削除).....	18
SmartStartのリストからZ-Wave装置を削除する.....	18
Replace a Z-Wave device (Z-Wave装置の交換).....	19
Reset the Z-Wave network (Z-Waveネットワークのリセット).....	19

Use Z-Wave as I/O (Z-WaveをI/Oとして使用する).....	19
webインターフェース	20
詳細情報	21
キャプチャーモード	21
プライバシーマスク	21
オーバーレイ	22
ワイヤレスI/O (Z-Wave Plus® v2)	22
団体/組織	22
Command classes (コマンドクラス)	22
ストリーミングとストレージ	23
ビデオ圧縮形式.....	23
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	24
ビットレート制御	24
分析機能とアプリ	26
AXIS People Counter.....	26
サイバーセキュリティ	26
署名付きOS	27
仕様	28
製品概要	28
LEDインジケーター	28
SDカードスロット	28
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
サイバーセキュリティ	37
脆弱性の管理	37
セキュリティ通知.....	37
安全な製品ライフサイクル管理	37
セキュアコンポーネント検証 (SCV).....	37

インストール

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。
この装置の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、ネットワーク上でこの装置を見つけてください。
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インターフェースでの全機能と設定に関する説明については、AXIS OS Webインターフェース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

基本設定

キャプチャーモードを設定する

1. [Video (ビデオ)] > [Installation (インストール)] > [Capture mode (キャプチャーモード)] に移動します。
2. [Change (変更)] をクリックします。
3. キャプチャーモードを選択し、[Save and restart (保存して再起動する)] をクリックします。
キャプチャーモード, on page 21も参照してください。

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] 度または [180] 度を選択します。

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 21*を参照してください。

カメラを水平にする

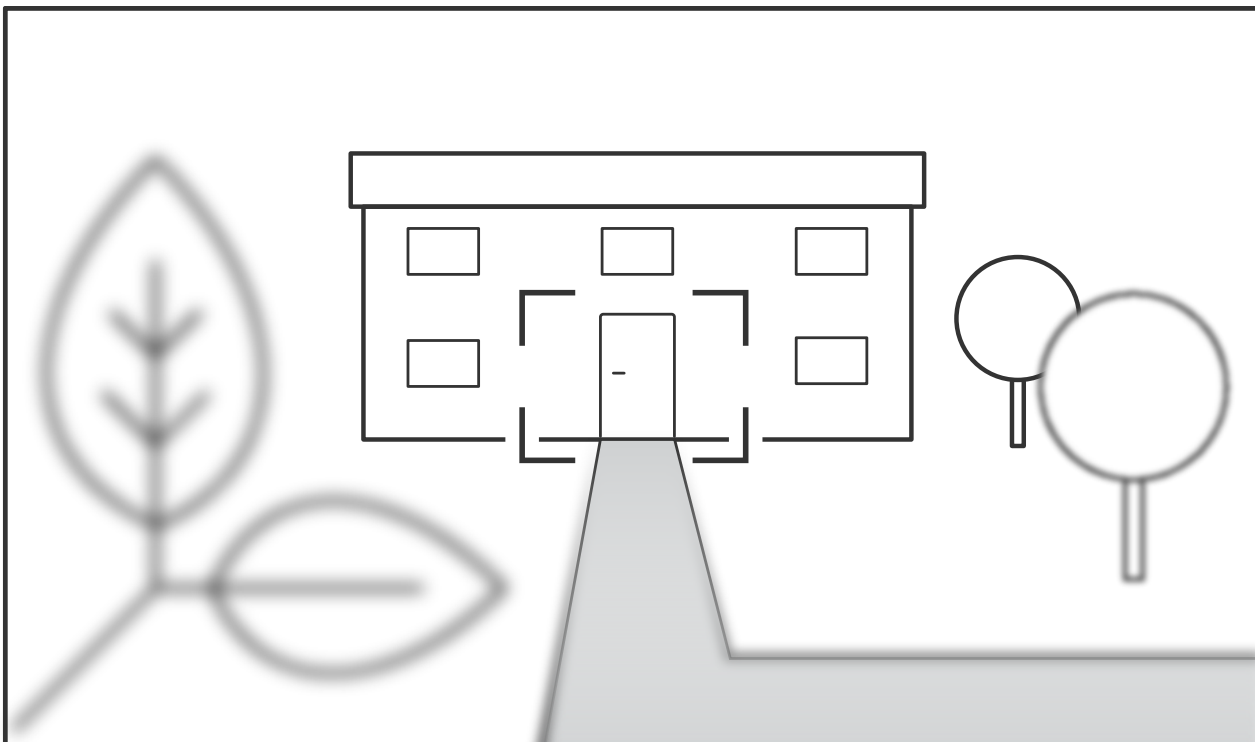
参照エリアまたは物体との関係で表示を調整するには、レベルグリッドとカメラの機械的な調整を組み合わせ使用します。

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。

フォーカスを調整する

本製品には4つのフォーカスモードがあります。

- [オート]:画像全体に基づいて自動的にフォーカスが調整されます。
- Area (エリア):画像の選択したエリアに基づいて、自動的にフォーカスが調整されます。
- 手動:固定距離でフォーカスを手動で設定します。
- スポット:フォーカスは画像中央の固定エリアに設定されます。



フォーカススポット

オートフォーカスをオフにし、フォーカスを手動で調整するには、次のように操作します。

1. ライブビューウィンドウで、[Zoom (ズーム)] スライダーが表示されている場合は、[Zoom (ズーム)] をクリックし、[Focus (フォーカス)] を選択します。

2.  をクリックし、スライダーを使用してフォーカスを設定します。

フォーカスリコールエリアを使用してフォーカスを迅速に調整する

特定のパン/チルト範囲でのフォーカス設定を保存するには、フォーカスリコールエリアを追加します。カメラはそのエリアに移動するたびに、以前に保存したフォーカスをリコールします。ライブビュー内のフォーカスリコールエリアの半分だけでも十分です。

フォーカスリコール機能は、次のシナリオでを使用することをお勧めします。

- ライブビューでジョイスティックなど手動の操作が多い場合。
- フォーカス設定が常に変わる動作など、手動フォーカスのPTZプリセット位置が効率的でない場合。
- 照明環境によりオートフォーカスが難しいような低照度のシナリオ。

重要

- フォーカスリコールは、指定したパン/チルト範囲でカメラのオートフォーカス設定をオーバーライドします。
- プリセット位置は、フォーカスリコールエリアで保存したフォーカス設定をオーバーライドします。
- フォーカスリコールエリアの最大数は20です。

フォーカスリコールエリアの作成

1. フォーカスするエリアにパン、チルト、ズームします。

[フォーカスリコール] ボタンにプラス  が表示されていれば、その位置にフォーカスリコールエリアを追加できます。

2. フォーカスを調整します。

3. [フォーカスリコール] ボタンをクリックします。

フォーカスリコールエリアの削除

1. 削除するフォーカスリコールエリアにパン、チルト、ズームします。
フォーカスリコールエリアが検出されると、[フォーカスリコール] ボタンがマイナスに切り

替わります:

2. [フォーカスリコール] ボタンをクリックします。

低遅延モードで画像処理時間を短縮する

低遅延モードをオンにすることで、ライブストリームの画像処理時間を最適化できます。ライブストリームの遅延が最小限に短縮されます。低遅延モードを使用すると、通常より画質が低下します。

1. [System > Plain config (システム > プレイン設定)] に移動します。
2. ドロップダウンリストから [ImageSource (画像ソース)] を選択します。
3. [ImageSource/I0/Sensor > Low latency mode (画像ソース/I0/センサー > 低遅延モード)] に移動し、[On (オン)] を選択します。
4. [保存] をクリックします。

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。

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。

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。

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. [Local contrast (ローカルコントラスト)] スライダーを使用して、WDRの量を調整します。
3. [Tone mapping (トーンマッピング)] スライダーを使用して、WDRの量を調整します。
4. 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/solutions/wide-dynamic-range-wdr を参照してください。

たる型歪曲の補正

バレル歪曲 (たる型歪曲) とは、フレームの端に近づくにつれて、直線の曲がりが見れる現象です。広い視野では、多くの場合、画像内にバレル歪曲が発生します。バレル歪曲補正では、この歪曲が補正されます。

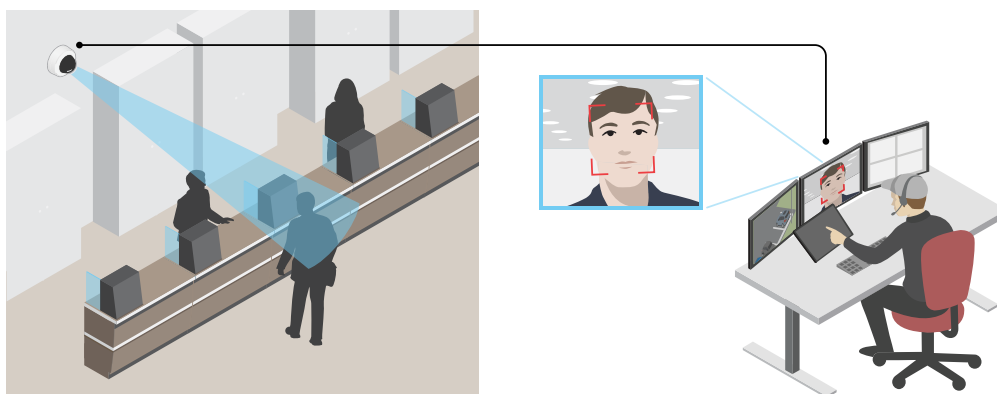
注

バレル歪曲補正は、画像の解像度と視野に影響します。

1. [Video (ビデオ)] > [Installation (インストール)] > [Image correction (画像補正)] に移動します。
2. [Barrel distortion correction (BDC) (バレル歪曲補正 (BDC))] をオンにします。

ピクセル解像度の確認

画像の定義された部分に、たとえば人物の顔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 (ビデオ)] > [Image (画像)] に移動して、 をクリックします。
2. ピクセルカウンターの  をクリックします。
3. カメラのライブビューで、顔が表示されることが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。
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 21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。

パン位置またはチルト位置をテキストオーバーレイとして表示する

パン位置またはチルト位置を、画像内にオーバーレイとして表示することができます。

1. [Video (ビデオ)] > [Overlays (オーバーレイ)] に移動して、**+** をクリックします。
2. パン位置を表示するには、テキストフィールドに#xと入力します。
チルト位置を表示するには、#yと入力します。
3. 外観、テキストサイズ、および位置を選択します。
4. 現在のパンおよびチルト位置がライブビュー画像と録画に表示されます。

カメラビューを調整する (PTZ)

パン、チルト、およびズーム動作を制限する

シーン内にカメラで撮影したくない部分がある場合は、パン、チルト、ズームの動作を制限することができます。たとえば、監視する予定の駐車場に近い場所にあるアパートの居住者のプライバシーを保護する必要がある場合です。

動作を制限する

1. [PTZ > Limits (PTZ > 制限)] に移動します。
2. 必要に応じて制限を設定します。

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 23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。

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。

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。
1. 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。
 2. 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. 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。
4. ストレージオプションのリストで、[SD_DISK] を選択します。
5. カメラとストリームプロファイルを選択します。
6. プリバッファ時間を5秒に設定します。
7. ポストバッファ時間を [1 minute(1分)] に設定します。

8. [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。

1. 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。
2. 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. 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。
4. ビデオチャンネルを選択します。
5. [Text (テキスト)] に「動体検知」と入力します。
6. 期間を設定します。
7. [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。

カメラが動きを検知したときにカメラをプリセットポジションに向ける

この例では、画像内の動きを検知したときにプリセットポジションに移動するようにカメラを設定する方法を示します。

1. 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。
2. 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。

プリセットポジションの追加:

[PTZ (パン/チルト/ズーム)] に移動し、プリセットポジションを作成して、カメラを向ける場所を設定します。

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. アクションのリストで、[Go to preset position (プリセットポジションに移動する)] を選択します。
4. カメラの移動先のプリセットポジションを選択します。
5. Save (保存) をクリックします。

カメラが音量の大きいノイズを検知したときにビデオを録画する

この例では、カメラが音量の大きいノイズを検知する5秒前にSDカードへの録画を開始し、2分後に停止するようにカメラを設定する方法を示します。

音声をオンにする:

1. 音声を含めるようにストリームプロファイルを設定します (録画に音声を追加する, on page 16参照)。

音声検知をオンにする:

1. [System (システム) > Detectors (検知) > Audio detection (音声検知)] に移動します。
2. 必要に応じて、音声レベルを調整します。

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. 条件のリストで、[Audio (音声)] の [Audio Detection (音声検知)] を選択します。
4. アクションのリストで、[Recordings (録画)] の [Record video (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. 音声が入力されている場合の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2分に設定します。
9. [保存] をクリックします。

ゲートキーパーで特定のエリアに自動的にズームインする

ここでは、ゲートキーパーの機能を使用して、ゲートを通る車のナンバープレートにカメラを自動的にズームインする方法について説明します。車が通過すると、カメラはズームアウトしてホームポジションに戻ります。

プリセットポジションの作成:

1. [PTZ(パン/チルト/ズーム) > Preset Positions (プリセットポジション)] に移動します。
2. ゲートの入口を含むホームポジションを作成します。
3. ナンバープレートが現れる位置と想定される画像中のエリアをカバーできるように、ズームインプリセットポジションを作成します。

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 "Gatekeeper" に設定します。
3. アクションのリストで、[Preset positions (プリセットポジション)] の [Go to preset position (プリセットポジションに移動する)] を選択します。
4. [Video channel (ビデオチャンネル)] を選択します。
5. [Preset position (プリセットポジション)] を選択します。
6. ホームポジションに戻るまでカメラを待機させるには、[Home timeout (ホーム復帰タイムアウト)] の時間を設定します。
7. Save (保存) をクリックします。

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。

録画に使用するストリームプロファイルを編集します:

4. [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。
5. Include audio (音声を含める) を選択してオンにします。
6. [保存] をクリックします。

Z-Wave®を設定する

Z-Waveの詳細については、ワイヤレスI/O (Z-Wave Plus® v2), on page 22を参照してください。

検討事項

Z-Wave Plus v2対応のワイヤレスI/Oを使用する前に、以下の点を考慮してください。

- Z-Waveの設定を行うには、管理者である必要があります。
- Z-Waveデバイスの追加、削除、置換やZ-Waveネットワークのリセットなど、製品のWebページでZ-Wave関連のアクションを実行するときには、アクションプロセスの実行中にページを再読み込みしたり、別のページに移動したりしないことをお勧めします。そのようにした場合、アクションの実際のステータスと表示されるステータスが異なる場合があります。回復するには、数分間待ってから、ページをもう一度読み込む必要があります。
- 複製、つまりネットワーク情報の別の制御装置へのコピーは、登録プロセスの一部として実行されます。
- この製品は、基本コマンドクラスのすべてのコマンドを無視します。

Turn on Z-Wave (Z-Waveをオンにする)

1. [System (システム)] > [Z-Wave] に移動します。
2. [Gateway settings wireless I/O (ゲートウェイ設定ワイヤレスI/O)] に移動し、Z-Waveをオンにします。Z-Waveが有効になるまで、数分間待たなければならないことがあります。

Add a Z-Wave device (Z-Wave装置の追加)

Z-Wave Plus v2プロトコルによる制限はありませんが、本製品のイベントシステムでは、いつでもZ-Waveデバイスを追加することができます。最大数に達した場合は、Z-Wave装置を削除してからでなければ、新しいZ-Wave装置を追加できません。Z-Wave装置の最大数に関する情報については、製品のデータシートを参照してください。

1. [System (システム)] > [Z-Wave] に移動します。
2. [Device management (デバイスの管理)] に移動し、**+** [Add device (デバイスを追加)] をクリックします。本製品がZ-WaveネットワークでZ-Waveデバイスの検索を開始します。
3. ユーザーマニュアルの説明に従って、Z-Waveデバイスが対象/除外モードに追加されるように設定します。
4. 必要な場合は、Z-Waveデバイスとともに提供されたPINを入力して、[OK] をクリックします。
5. 追加プロセスが終了して、Webページに通知が表示されるまで待ちます。

追加されたZ-Wave装置が装置管理リストに表示されます。

注

Z-Waveデバイスが見つからなかった場合、追加プロセスは自動的に終了します。

追加されたZ-Wave装置の詳細なステータス情報を表示するには、装置管理リストで装置情報を展開します。

注

追加されたZ-Wave装置のステータス情報は、装置の種類によって異なります。詳細については、オンラインヘルプ^②を参照してください。

本製品を設定することで、指定したZ-Waveのトリガー条件でルールをトリガーできます。使用可能なZ-Waveの条件とアクションは、追加されたZ-Wave装置の種類によって異なります。

SmartStartを搭載したZ-Wave装置の追加

SmartStartを搭載したZ-Wave装置を、Z-Waveネットワークに追加することができます。SmartStartのリストに追加されたZ-Wave装置は、ネットワークの付近で電源投入後10分以内に自動的に装置管理リストに追加されます。

1. [System (システム)] > [Z-Wave] に移動します。
2. [SmartStart] に移動し、**+** [Add device information (デバイス情報の追加)] をクリックします。

3. 装置固有のキーとオプション情報を入力します。
4. [OK] をクリックします。

Remove a Z-Wave device through inclusion/exclusion mode (対象/除外モードからのZ-Waveデバイスの削除)

注

これは推奨される削除手順です。

1. [System (システム)] > [Z-Wave] に移動します。
2. [Device management (デバイスの管理)] に移動し、 をクリックします。本製品がZ-WaveネットワークでZ-Waveデバイスの検索を開始します。
3. ユーザーマニュアルの説明に従って、Z-Wave装置が対象/除外モードで削除されるように設定します。
4. 削除プロセスが終了してWebページに通知が表示されるまで待ちます。

Z-Wave装置が装置管理リストから削除されます。

注

削除されたZ-Wave装置のすべての製品関連情報が削除されます。

注

Z-Waveデバイスが見つからなかった場合、削除プロセスは自動的に終了します。

Remove a Z-Wave device through forced process (強制プロセスによるZ-Wave装置の削除)

バッテリーの消耗などによって通信障害が発生し、対象/除外モードに設定してもZ-Waveデバイスを削除できないことがあります。装置管理リストで [Down (ダウン)] ステータスが表示されているZ-Wave装置の強制削除を実行することができます。

1. [System (システム)] > [Z-Wave] に移動します。
2. [Device management (装置の管理)] に移動し、削除するZ-Wave装置の装置情報を展開します。
3. [Node (ノード)] > [Status (ステータス)] の順に移動し、 をクリックします。
4. 除外プロセスが終了してWebページに通知が表示されるまで待ちます。

Z-Wave装置が装置管理リストから削除されます。

注

削除されたZ-Wave装置内のすべての製品関連情報は保持されます。

SmartStartのリストからZ-Wave装置を削除する

注

Z-Wave装置をSmartStartリストから削除した場合、その装置は装置管理リストリストから削除されません。

1. [System (システム)] > [Z-Wave] に移動します。
2. SmartStartに移動します。
3. リスト内の装置にカーソルを合わせると、ゴミ箱アイコン  が表示されます。
4. SmartStartのリストから削除するZ-Wave装置の横にある  をクリックします。

Replace a Z-Wave device (Z-Wave装置の交換)

たとえば、Z-Wave装置の故障などによって通信障害が発生し、別の装置に交換したい場合があります。装置管理リストで **[Down (ダウン)]** ステータスが表示されているZ-Wave装置を強制的に削除することができます。

1. **[System (システム)] > [Z-Wave]** に移動します。
2. **[Device management (デバイスの管理)]** に移動し、交換するZ-Waveデバイスのデバイス情報を展開します。
3. **[Node (ノード)] > [Status (ステータス)]** の順に移動し、 をクリックします。本製品がZ-WaveネットワークでZ-Waveデバイスの検索を開始します。
4. ユーザーマニュアルの説明に従って、既存の装置と交換するZ-Wave装置を対象/除外モードに設定します。
5. 交換プロセスが終了して、Webページに通知が表示されるまで待ちます。

新しいZ-Waveデバイスがいくつかのステータス情報と共にデバイス管理リストに表示されます。

注

ノードIDとイベントアクション情報が新しいZ-Waveデバイスに受け渡されます。その他の情報はすべて削除されます。

注

Z-Waveデバイスが見つからなかった場合、交換プロセスは自動的に終了します。

Reset the Z-Wave network (Z-Waveネットワークのリセット)

重要

- この手順では、製品からすべてのZ-Wave装置を削除します。
- Z-Waveネットワークをリセットした後、Z-Wave装置をネットワークに再度追加する前に、各装置を削除するか、工場出荷時の設定にリセットする必要もあります。
- この手順は、ネットワークのプライマリコントローラーが見つからないか、操作できないときにのみ使用します。

1. **[System (システム)] > [Z-Wave]** に移動します。
2. **[Device management (デバイスの管理)]** に移動し、 をクリックします。
3. ドロップダウンメニューで **[Reset network (ネットワークのリセット)]** を選択します。

追加されたZ-Waveデバイスが製品からすべて削除され、デバイス管理リストが空になります。

Use Z-Wave as I/O (Z-WaveをI/Oとして使用する)

本製品では物理I/Oコネクタが装備されていませんが、I/Oインターフェースで一部のZ-Wave機能を使用できます。

接続された最大で6台までのZ-Wave装置にI/Oポート番号を割り当てることができます。ポート番号を表示するには、**[System (システム)] > [Accessories (アクセサリ)] > [I/O ports (I/Oポート)]** に移動します。I/Oポート番号は、Z-Wave装置の情報ウィンドウで変更できます。

デジタル入力ポートイベントとして使用する場合、Z-Wave装置の1つの機能しか使用できません。デフォルトの機能は、デバイスのタイプによって異なります。使用する機能を変更するには、装置の情報ウィンドウに移動します。

I/Oポートの使用の詳細については、本製品の内蔵のヘルプを参照してください。

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ウェブインターフェースのヘルプ*を参照してください。

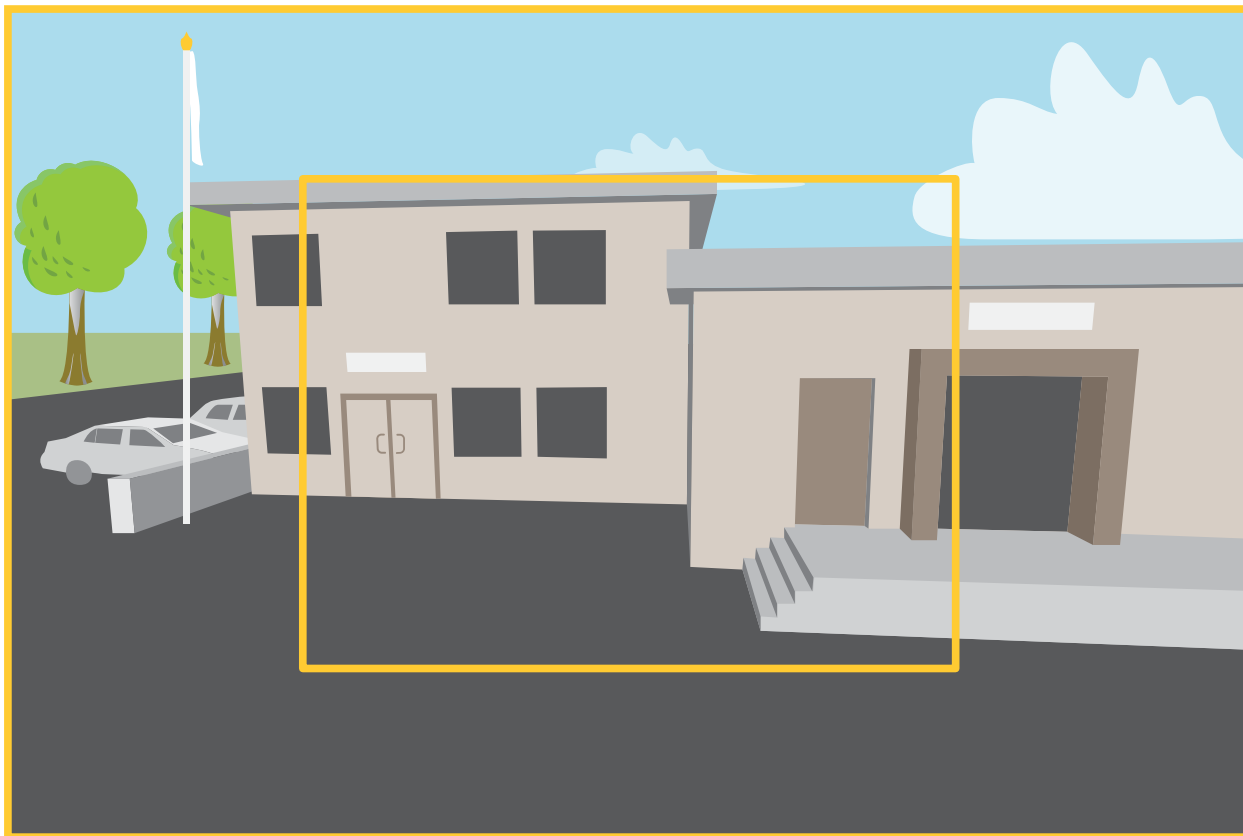
詳細情報

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設定により、本装置で利用可能な最大解像度と最大フレームレートを調整できます。
- 最大解像度よりも低い解像度のキャプチャーモードを使用した場合、視野が狭くなることがあります。
- キャプチャーモードはシャッター速度にも影響し、結果として光感度に影響します。これは、最大フレームレートが高いキャプチャーモードでは光感度が下がり、逆に最大フレームレートが低いキャプチャーモードでは、光感度が上がるためです。
- キャプチャーモードによっては、WDRを使用できません。

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、監視領域の一部を隠すユーザー定義のエリアです。ビデオストリームでは、プライバシーマスクは塗りつぶされたブロックまたはモザイク模様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。

ビデオストリーミングインジケータは、別のタイプのオーバーレイです。これは、ライブビューのビデオストリームが動作中であることを示します。

ワイヤレスI/O (Z-Wave Plus® v2)

このセキュリティ対応のZ-Wave Plus® v2製品は、暗号化されたZ-Wave Plus v2メッセージを使用して、セキュリティ対応のZ-Wave Plus v2装置と通信できます。本製品は、互換性のある他社製のZ-Wave認証機器と一緒に、あらゆるZ-Wave® ネットワークで動作します。ネットワークの信頼性を高めるために、ネットワーク内のすべての非電池駆動式Z-Waveデバイスが、ベンダーに関わらず、リピーターとして機能します。この製品は制御装置として機能し、この製品に追加されたZ-Wave装置はセカンダリ装置として機能します。

団体/組織

- 本製品は、グループ識別子1 (Lifeline) の1つのアソシエーショングループをサポートします。
- アソシエーショングループに追加できる最大装置数 = 1。
- グループ識別子1は、Device Reset Locallyレポートを送信するために使用されます。

Command classes (コマンドクラス)

この製品は、以下のコマンドクラスをサポートしています。

- COMMAND_CLASS_APPLICATION_STATUS
- COMMAND_CLASS_ASSOCIATION_V3 (保護)
- COMMAND_CLASS_ASSOCIATION_GRP_INFO_V3 (保護)
- COMMAND_CLASS_CRC_16_ENCAP
- COMMAND_CLASS_DEVICE_RESET_LOCALLY (保護)
- COMMAND_CLASS_FIRMWARE_UPDATE_MD_V5 (保護)
- COMMAND_CLASS_INCLUSION_CONTROLLER
- COMMAND_CLASS_INDICATOR_V3 (保護)
- COMMAND_CLASS_MANUFACTURER_SPECIFIC_V2 (保護)
- COMMAND_CLASS_MULTI_CHANNEL_ASSOCIATION_V4 (保護)
- COMMAND_CLASS_MULTI_CMD
- COMMAND_CLASS_NETWORK_MANAGEMENT_BASIC_V2 (保護)
- COMMAND_CLASS_NETWORK_MANAGEMENT_INCLUSION_V4 (保護)

- COMMAND_CLASS_NETWORK_MANAGEMENT_INSTALLATION_MAINTENANCE_V4 (保護)
- COMMAND_CLASS_NETWORK_MANAGEMENT_PROXY_V4 (保護)
- COMMAND_CLASS_NODE_PROVISIONING (保護)
- COMMAND_CLASS_POWERLEVEL (保護)
- COMMAND_CLASS_SECURITY
- COMMAND_CLASS_SECURITY_2
- COMMAND_CLASS_SUPERVISION
- COMMAND_CLASS_TIME
- COMMAND_CLASS_TRANSPORT_SERVICE_V2
- COMMAND_CLASS_VERSION_V3 (保護)
- COMMAND_CLASS_ZWAVEPLUS_INFO_V2 (保護)

注

本製品は、COMMAND_CLASS_INDICATOR_V3 に対応していますが、可視インジケータは実装していません。

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になります。

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。

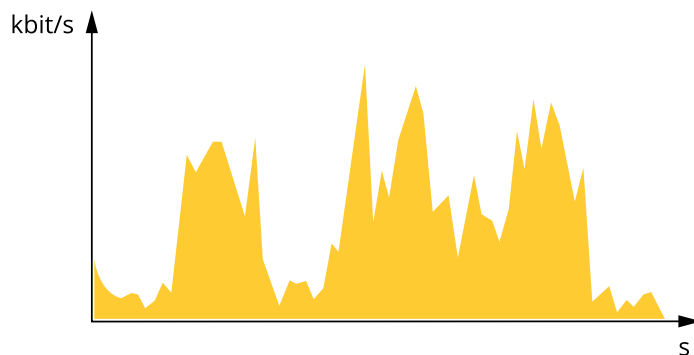
[Stream profiles (ストリームプロファイル)] の設定は、**[Stream (ストリーム)]** タブの設定よりも優先されます。特定のストリームプロファイルを持つストリームを要求すると、ストリームにそのプロファイルの設定が含まれます。ストリームプロファイルを指定せずにストリームを要求した場合、または製品に存在しないストリームプロファイルを要求した場合、ストリームに **[Stream (ストリーム)]** タブの設定が含まれます。

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。

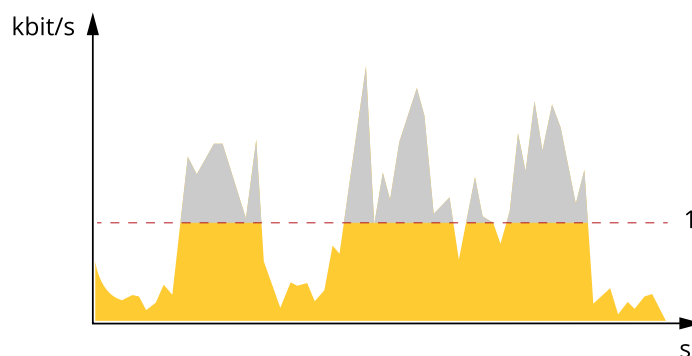
可変ビットレート (VBR)

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。

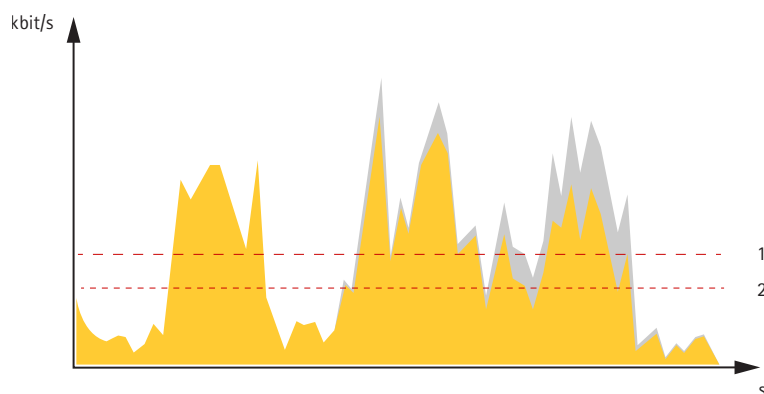


1 目標ビットレート

平均ビットレート (ABR)

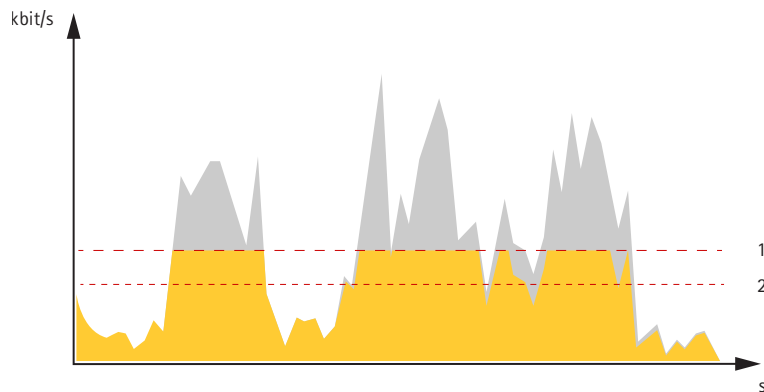
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できます。次のいずれかの方法で、平均ビットレートの設定を指定します。

- 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

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。

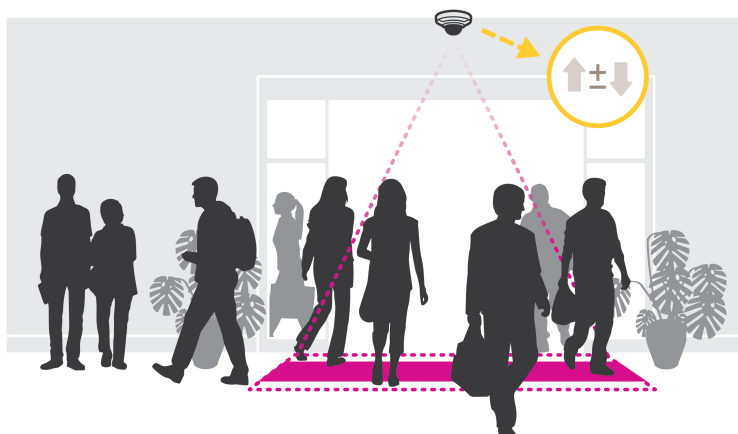
注

- 同時に複数のアプリケーションを実行できますが、互いに互換性がないアプリケーションもあります。アプリケーションの特定の組み合わせによっては、並行して実行すると過度の処理能力やメモリーリソースが必要になる場合があります。展開する前に、各アプリを組み合わせて実行できることを確認してください。

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。

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。

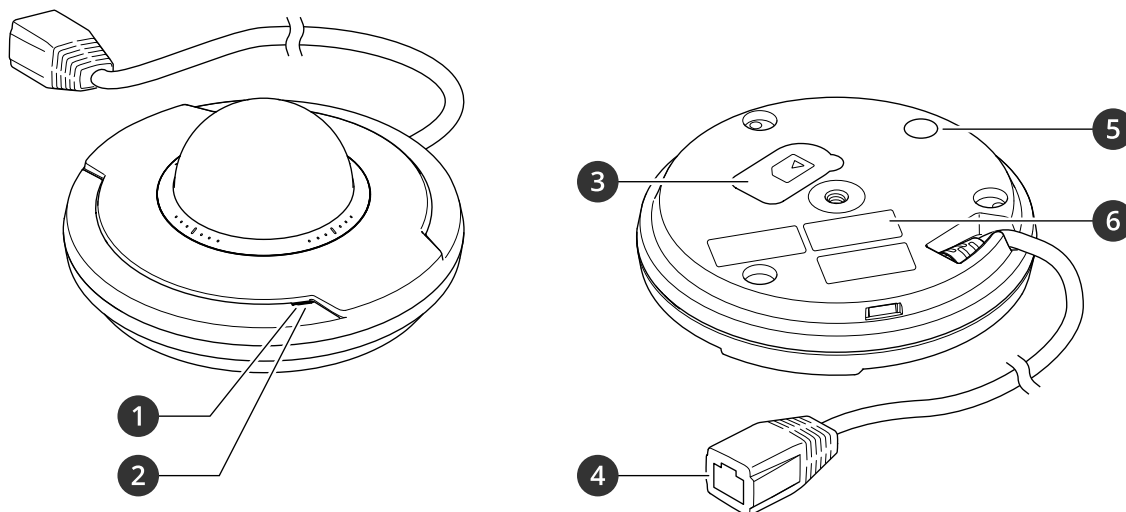
AXIS OSのサイバーセキュリティの詳細情報については、『AXIS OS強化ガイド』を参照してください。

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。

仕様

製品概要



- 1 マイク
- 2 ステータスLEDインジケータ
- 3 microSDカードスロット
- 4 ネットワークコネクタ (PoE)
- 5 コントロールボタン
- 6 型番 (P/N) とシリアル番号 (S/N)

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。

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、以下の用途で使います。

- 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

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。

Axisデバイスの清掃に関する詳細については、ホワイトペーパー「一般的な洗浄剤に対する耐薬品性」をご覧ください。

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

重要

Z-Waveネットワークを使用している場合は、装置を工場出荷時の設定にリセットする前に、Z-Waveネットワークをリセットする必要があります。Reset the Z-Wave network (Z-Waveネットワークのリセット), on page 19を参照してください。

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インジケーター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 Lifecycleガイド: 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、装置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 관리자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す。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、[ブラウザーサポート](#), *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。

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。

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。

サイバーセキュリティ

サイバーセキュリティは、リスクを最小限に抑えながら、健全な製品ライフサイクルを支援します。当社のサイバーセキュリティへの取り組みに関する詳細や文書は、axis.com/about-axis/cybersecurityで確認できます。以下のサイバーセキュリティガイドラインに従って、Axisから製品に関するセキュリティ通知を受け取り、安全なライフサイクルと利用停止を確保するために製品を設定してください。

Axis Trust Centerでは、Axisが実施するセキュリティコンプライアンス、透明性、データ保護、およびプライバシーについての情報をご覧ください。

脆弱性の管理

Axisは、共通脆弱性識別子 (CVE) 採番機関 (CNA)です。当社は、セキュリティリスクを最小限に抑えるため、当社のデバイス、ソフトウェア、およびサービスの脆弱性の特定と修正において業界標準に従って対応しています。当社の脆弱性管理ポリシーに関する詳細や、脆弱性の報告については、axis.com/vulnerability-managementを参照してください。

セキュリティ通知

axis.com/security-notification-serviceでAxisのセキュリティ通知メールを受け取る用に設定してください。お使いのAxis製品に関する脆弱性、関連するセキュリティアドバイザリー、およびその他のセキュリティ関連事項に関する情報を送信いたします。

安全な製品ライフサイクル管理

Axisは、安全なライフサイクル管理を通じて、製品のライフサイクル全体でリスクを最小限に抑えています。help.axis.comに掲載されているハードニングガイドには、Axis製品のより安全な設定と操作に関する情報、および以下の情報が含まれています。

安全な初回使用 - Axis製品は、高度な保護機能がデフォルトで組み込まれているため、初回使用時から安全な初期化と暗号化された通信が可能です。

使用目的とよくある設定ミス - 当社のガイドには、Axis製品の使用目的について記載されています。これには、避けるべきよくあるセキュリティ関連の誤った使用や設定ミスについても含まれています。

脆弱性の管理とサプライチェーンの透明性 - 脆弱性の開示およびサプライチェーンの透明性向上を目的として、ソフトウェアのリリースごとに、axis.comでソフトウェア部品表 (SBOM) を公開しています。

利用停止とデータの安全な消去 - 製品のライフサイクル終了時に安全に利用を停止するために、工場出荷時の設定にリセットしてください。これにより、設定、保存されたデータ、およびセンシティブな情報が消去されます。

セキュアコンポーネント検証 (SCV)

デバイスにはSCVが付属しています。これは、正しいデバイスを受け取ったこと、および工場出荷以降、デバイスが改ざんされていないことを証明する証明書です。この証明書はメーカーによって署名され、iDRACに保存されます。

デバイスを受け取ったら、AXIS Recorder Toolboxを使用して、デバイスのSCV証明書を確認してください。SCVに関する詳細については、dell.comを参照してください。

T10173004_ja

2026-07 (M18.2)

© 2022 – 2026 Axis Communications AB