

AXIS P3818-PVE Network Camera

目次

使用に当たって	4
ネットワーク上のデバイスを検索する	4
ブラウザーサポート	4
装置のwebインターフェースを開く	4
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	4
管理者アカウントを作成する	4
安全なパスワード	5
webインターフェースの概要	5
インストール	6
プレビューモード	6
デバイスを構成する	7
画像を調整する	7
カメラを水平にする	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	7
低照度環境でノイズを減らす	7
低光量下で動きによる画像のブレを減らす	7
最大限に詳細な画像を撮影する	8
逆光の強いシーンを処理する	8
ピクセル解像度の確認	9
プライバシーマスクで画像の一部を非表示にする	9
画像オーバーレイを表示する	9
ビデオを表示する、録画する	10
帯域幅とストレージ容量を削減する	10
ネットワークストレージを設定する	10
ビデオを録画して見る	11
イベントのルールを設定する	11
アクションをトリガーする	11
カメラが物体を検知したときにビデオを録画する	11
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	12
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	12
カメラが衝撃を検知したときにビデオを録画する	13
進行中のイベントを視覚的に示します	13
近くに人がいるときにゲートのロックを開ける	14
囲いが開かれたときに通知をトリガーする	15
侵入アラームの設定	16
入力信号でいたずらを検知する	17
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	17
音声	18
録画に音声を追加する	18
ネットワークスピーカーに接続する	18
webインターフェース	19
詳細情報	20
長距離接続	20
プライバシーマスク	20
オーバーレイ	20
ストリーミングとストレージ	20
ビデオ圧縮形式	20
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	21
ビットレート制御	21
分析機能とアプリ	23
ワンクリックPTZコントロール	23
仕様	25
製品概要	25

LEDインジケーター	25
SDカードスロット	26
ボタン	26
コントロールボタン	26
コネクタ	26
ネットワーク コネクタ	26
I/Oコネクタ	26
装置を清掃する	28
トラブルシューティング	29
工場出荷時の設定にリセットする	29
AXIS OSのオプション	29
AXIS OSの現在のバージョンを確認する	29
AXIS OSをアップグレードする	30
技術的な問題と解決策	30
パフォーマンスに関する一般的な検討事項	33
サポートに問い合わせる	34
サイバーセキュリティ	35
脆弱性の管理	35
セキュリティ通知	35
安全な製品ライフサイクル管理	35

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 4*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。

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 29*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。

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 5*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 29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)。

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

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。

デバイスを構成する

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 20*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、A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。

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。

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。

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。
- 画像のシャープネスを下げます。

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。

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。

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。
- ライブビュー画像の下で  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

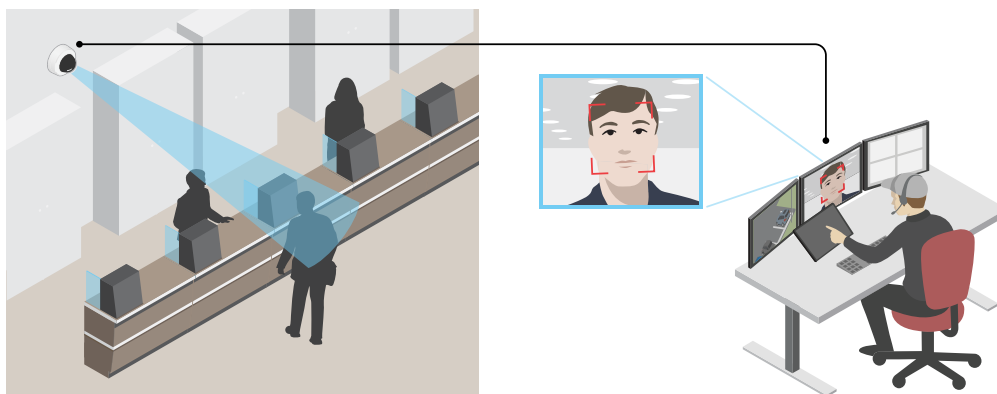
- WDRを使用すると、画像にノイズが発生することがあります。
- WDRは、一部のキャプチャーモードでは使用できない場合があります。

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. [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。

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

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 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。

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 20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 10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 18 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。

カメラが衝撃を検知したときにビデオを録画する

衝撃検知機能を利用すると、カメラで振動または衝撃によるいたずらを検知することができます。環境または物体による振動は、0から100まで設定可能な衝撃感度範囲に応じてアクションをトリガーすることができます。このシナリオでは、誰かが営業時間外にカメラに向かって石を投げていて、そのイベントの映像ビデオを入手したいとします。

衝撃検知をオンにする:

1. [System > Detectors > Shock detection (システム > 検知 > 衝撃検知)] に移動します。
2. 衝撃検知をオンにし、衝撃感度を設定します。

ルールの作成:

3. [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。
4. ルールの名前を入力します。
5. 条件のリストで、[Device status (デバイスのステータス)] の [Shock detected (衝撃検知)] を選択します。
6. [+] をクリックして、2つ目の条件を追加します。
7. 条件のリストで、[Scheduled and recurring (スケジュールおよび繰り返し)] の [Schedule (スケジュール)] を選択します。
8. スケジュールのリストで、[After hours (就労時間外)] を選択します。
9. 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。
10. 録画を保存する場所を選択します。
11. [Camera (カメラ)] を選択します。
12. プリバッファ時間を5秒に設定します。
13. ポストバッファ時間を50秒に設定します。
14. Save (保存) をクリックします。

進行中のイベントを視覚的に示します

AXIS I/O Indication LEDをネットワークカメラに接続するオプションがあります。このLEDは、カメラ内で特定のイベントが発生したときにオンになるように設定できます。たとえば、映像の録画が進行中であることを人に知らせる場合。

必要なハードウェア

- AXIS I/O Indication LED

- Axisネットワークビデオカメラ

注

AXIS I/O Indication LEDを接続する手順については、本製品に付属のインストールガイドを参照してください。

次の例では、AXIS I/O Indication LEDをオンにして、カメラが録画中であることを示すルールを設定する方法を示します。

1. **[Settings (設定)] > [System (システム)] > [I/O ports (I/Oポート)]** の順に移動します。
2. AXIS I/O Indication LEDの接続先ポートについては、方向を **[Output (出力)]** に設定し、通常の状態を **[Open circuit (NO) (開路)]** に設定します。
3. **[設定 > システム > イベント]** の順に移動します。
4. 新しいルールを作成します。
5. カメラをトリガーして録画を開始するために満たす必要がある **[Condition (条件)]** を選択します。たとえば、タイムスケジュールや動体検知などを行うことができます。
6. アクションのリストで、**[Record video (ビデオを録画する)]** を選択します。ストリームプロファイルを選択するか、新しく作成します。必要に応じて、**[Prebuffer (プリバッファ)]** と **[Postbuffer (ポストバッファ)]** も設定します。
7. ルールを保存します。
8. 2番目のルールを作成し、最初のルールと同じ **[Condition (条件)]** を選択します。
9. アクションのリストから、**[Toggle I/O while the rule is active (ルールがアクティブである間、I/Oを切り替える)]** を選択し、AXIS I/O Indication LEDに接続されているポートを選択します。状態を **[Active (アクティブ)]** に設定します。
10. ルールを保存します。

その他にも、AXIS I/O Indication LEDを使用できるシナリオを以下に示します。

- カメラの存在を示すために、カメラの起動時にオンになるようにLEDを構成します。条件として **[System ready (システムの準備完了)]** を選択します。
- 人物またはプログラムがカメラからのストリームにアクセスしていることを示すために、ライブストリームがアクティブなときにLEDがオンになるように構成します。条件として **[Live stream accessed (ライブストリームのアクセス)]** を選択します。

近くに人がいるときにゲートのロックを開ける

この例では、日中に誰かが入ろうとする際にカメラを向け、ゲートのロックを解除する方法について説明します。PIR検知器を本製品の入力ポートに接続し、スイッチリレーを本製品の出力ポートに接続することによって実行されます。

必要なハードウェア

- 取り付け済みPIR検知器
- スwitchリレーがゲートロックに接続されている場合、スイッチはノーマルクローズ (NC) になっています。
- ワイヤーの接続

物理接続

1. PIR検知器から入力ピンにワイヤーを接続する方法については、*I/Oコネクタ, on page 26* を参照してください。
2. スwitchから出力ピンにワイヤーを接続する方法については、*I/Oコネクタ, on page 26* を参照してください。

I/Oポートの設定

カメラのwebインターフェースから、スイッチリレーをカメラに接続する必要があります。まず、I/Oポートを設定します。

入力ポートにPIR検知器を設定

1. [System > Accessories > I/O ports (システム > アクセサリー > I/O ポート)] に移動します。
2.  をクリックして、ポート1の入力方向を設定します。
3. 入力モジュールに分かりやすい名前を付けます (「PIR detector」など)。
4. PIR検知器が動きを感知するたびにイベントをトリガーするようにしたい場合は、 をクリックして通常状態を開回路に設定します。

出力ポートにスイッチリレーを設定

1.  をクリックして、ポート2の出力方向を設定します。
2. 出力モジュールに分かりやすい名前を付けます (「Gate switch」など)。
3. イベントがトリガーされるたびにゲートを開くように設定するには、 をクリックして通常状態を閉回路に設定します。

ルールの作成

1. [Settings > System > Events (設定 > 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 (たとえば「Open gate」) を入力します。
3. 条件の一覧で、[PIR detector (PIR検知器)] を選択します。
4. アクションのリストから、[Toggle I/O once (I/Oを1回切り替え)] を選択します。
5. ポートのリストから [Gate switch (ゲートスイッチ)] を選択します。
6. 状態を [Active (アクティブ)] に設定します。
7. 期間を設定します。
8. [保存] をクリックします。

囲いが開かれたときに通知をトリガーする

この例では、デバイスのハウジングまたはケーシングが開けられたときの電子メール通知を設定する方法を説明します。

メール送信先を追加する:

1. [System (システム)] > [Events (イベント)] > [Recipients (送信先)] に移動し、[Add recipient (送信先の追加)] をクリックします。
2. 送信先の名前を入力します。
3. 通知のタイプとして電子メールを選択します。
4. 送信先の電子メールアドレスを入力します。
5. 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。
6. 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。
7. 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。
8. [保存] をクリックします。

ルールの作成:

9. [System > Events > Rules (システム > イベント > ルール)] に移動し、[Add a rule (ルールの追加)] をクリックします。
10. ルールの名前を入力します。
11. 条件のリストで、[Casing open (ケーシング開放)] を選択します。
12. アクションのリストで、[Send notification to email (電子メールに通知を送信する)] を選択します。
13. リストから送信先を選択します。
14. 電子メールの件名とメッセージを入力します。
15. [保存] をクリックします。

侵入アラームの設定

開始する前に

- 侵入アラームスイッチをカメラのI/Oコネクターのピン1 (アース) とピン3 (デジタルI/O) に接続します。

入力ポートの設定:

1. [System > Accessories > I/O ports (システム > アクセサリー > I/O ポート)] に移動します。
2. [Port 1 (ポート1)] の場合:
 - 2.1. [Input (入力)] を選択します。
 - 2.2. [Circuit closed (閉回路)] を選択します。

メール送信先を追加する:

3. [System (システム)] > [Events (イベント)] > [Recipients (送信先)] に移動し、[Add recipient (送信先の追加)] をクリックします。
4. 送信先の名前を入力します。
5. 通知のタイプとして電子メールを選択します。
6. 送信先の電子メールアドレスを入力します。
7. 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。
8. 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。
9. 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。
10. [保存] をクリックします。

ルールの作成:

11. [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。
12. ルールの名前を入力します。
13. [I/O] 下にある条件の一覧で、[Digital input (デジタル入力)] を選択します。
14. ポートのリストから [Port 1 (ポート1)] を選択します。
15. アクションのリストで、[Notifications (通知)] の下の [Send notification to email (通知を電子メールに送信)] を選択します。
16. リストから送信先を選択するか、[Recipients (送信先)] を選択して新しい送信先を作成します。

新しい送信先を作成するには、 をクリックします。既存の送信先をコピーするには、 をクリックします。

17. 電子メールの件名とメッセージを入力します。

18. [保存] をクリックします。

入力信号でいたずらを検知する

この例では、入力信号が切断された場合やショートした場合に電子メールを送信する方法について説明します。I/Oコネクタの詳細については、page 26を参照してください。

1. **System (システム) > Accessories (アクセサリ) > I/O ports (I/Oポート)** に移動し、該当するポートで **Supervised (状態監視)** をオンにします。

メール送信先を追加する:

1. **[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。
2. 送信先の名前を入力します。
3. 通知のタイプとして **電子メール** を選択します。
4. 送信先の電子メールアドレスを入力します。
5. 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。
6. 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。
7. 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。
8. **[保存]** をクリックします。

ルールの作成:

1. **[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。
2. ルールの名前を入力します。
3. **[I/O (入力/出力)]** の条件のリストで、**[Supervised input tampering is active (いたずら状態監視を有効化する)]** を選択します。
4. 該当するポートを選択します。
5. **[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。
6. 電子メールの件名とメッセージを入力します。
7. **[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。

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

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。

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。

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。

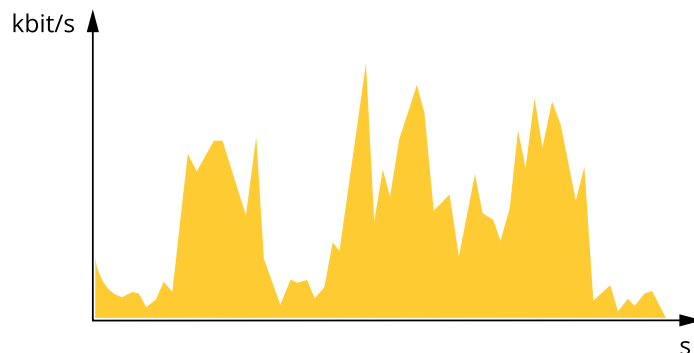
[Stream profiles (ストリームプロファイル)] の設定は、**[Stream (ストリーム)]** タブの設定よりも優先されます。特定のストリームプロファイルを持つストリームを要求すると、ストリームにそのプロファイルの設定が含まれます。ストリームプロファイルを指定せずにストリームを要求した場合、または製品に存在しないストリームプロファイルを要求した場合、ストリームに **[Stream (ストリーム)]** タブの設定が含まれます。

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。

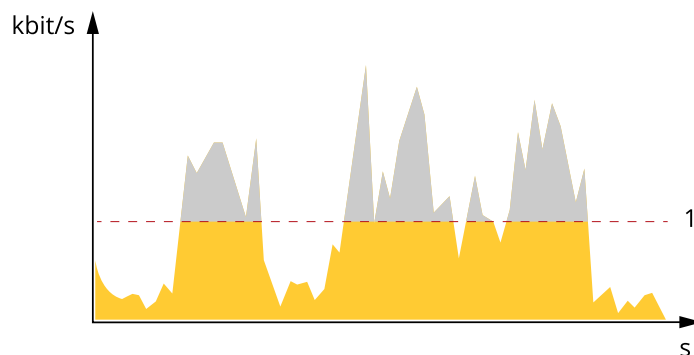
可変ビットレート (VBR)

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。

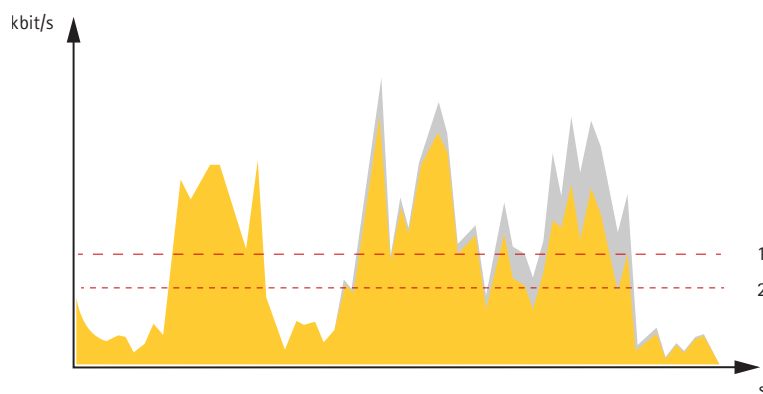


1 目標ビットレート

平均ビットレート (ABR)

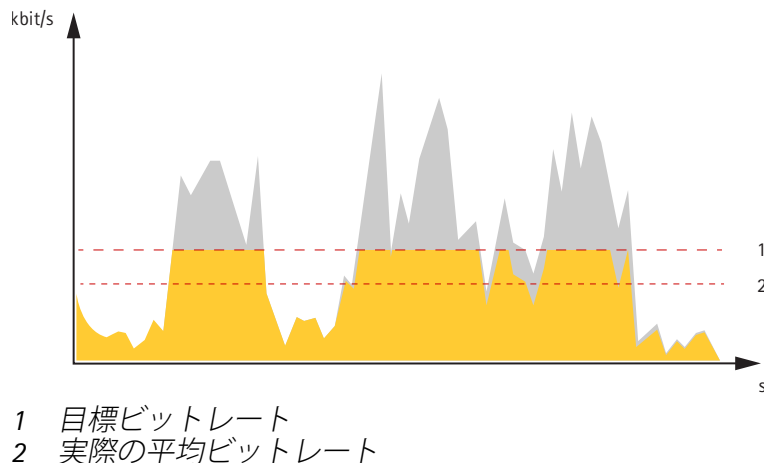
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できます。次のいずれかの方法で、平均ビットレートの設定を指定します。

- 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。



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で実行できることを確認してください。

ワンクリックPTZコントロール

ワンクリックPTZコントロールにより、パノラマカメラをリモートのAxis PTZカメラに接続し、ライブビューから制御できます。これにより、パノラマカメラの広い撮影範囲とPTZ機能 (動く物体の追尾、ズームイン/アウトなど) を組み合わせることができます。

注

ワンクリックPTZコントロールを使用する場合は、パノラマカメラから1 m以内にPTZカメラを設置してください。

ワンクリックPTZコントロールを設定する



AxisパノラマカメラでワンクリックPTZコントロールを設定する方法。

- 必要な設定アプリをダウンロードしてインストールする:
 - ⋮ をクリックし、**[Legacy device interface (レガシー装置インターフェース)]** を選択します。

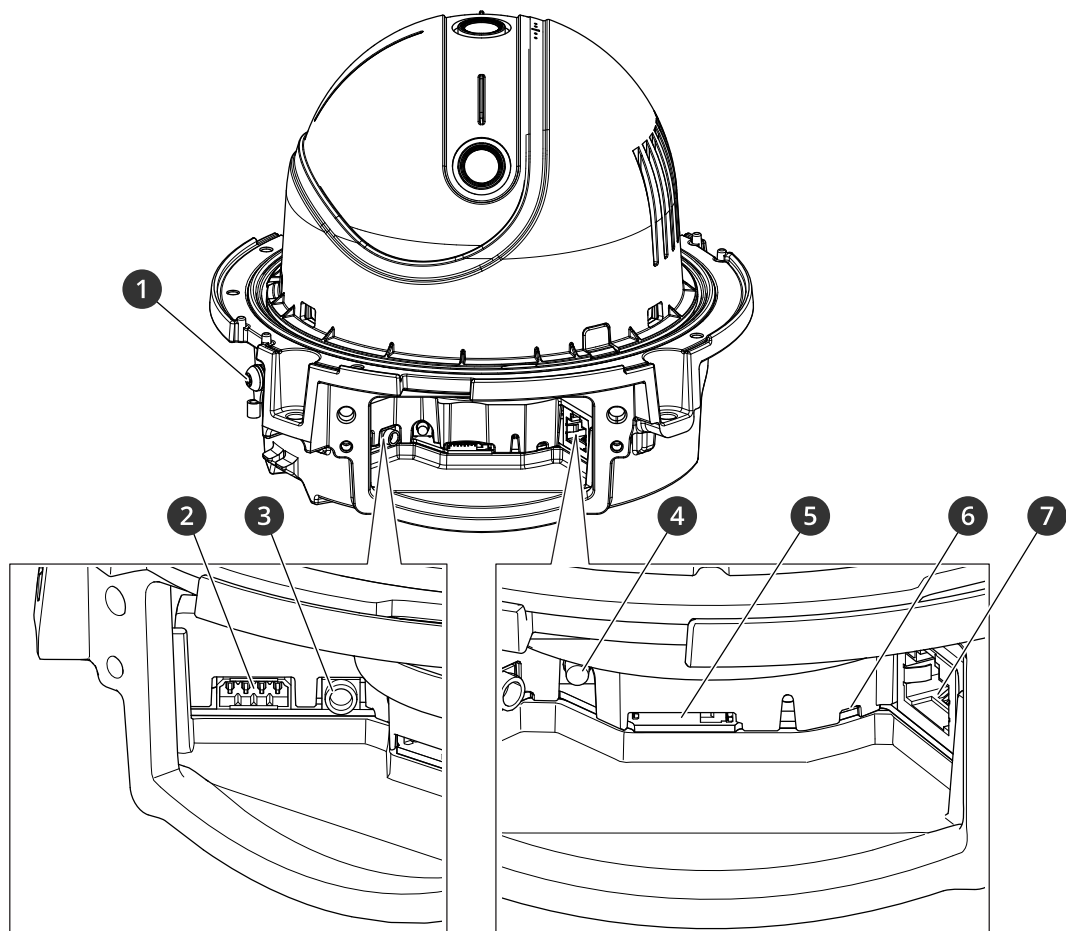
- 1.2. [Settings (設定)] > [System (システム)] > [One-click PTZ control (ワンクリック PTZコントロール)] に移動し、インストールパッケージの手順に従います。
2. リモートPTZカメラを接続する:
 - 2.1. [Settings (設定)] > [System (システム)] > [One-click PTZ control (ワンクリック PTZコントロール)] に移動し、[Configure (設定)] をクリックします。
 - 2.2. [One-click PTZ control (ワンクリックPTZコントロール)] > [PTZ remote connection (PTZリモート接続)] に移動し、[Configure (設定)] をクリックします。
 - 2.3. リモートPTZカメラのIPアドレスとパスワードを追加します。
 - 2.4. [Connect (接続)] をクリックし、接続ステータスを確認します。
 - 2.5. [One-click PTZ control (ワンクリックPTZコントロール)] をオンにし、[Close (閉じる)] をクリックします。
3. PTZカメラを自動的にキャリブレーションする:
 - 3.1. [One-click PTZ control (ワンクリックPTZコントロール)] > [PTZ positioning calibration (PTZ位置キャリブレーション)] に移動し、[Start application (アプリケーションの起動)] をクリックします。
 - 3.2. [Auto (自動)] をクリックします。
自動キャリブレーションには数分かかります。
 - 3.3. Done (完了) をクリックします。
 - 3.4. パノラマカメラのライブビューに移動し、画像内をクリックして、PTZカメラが正しい位置に移動することを確認します。

自動キャリブレーションで正確な位置が得られない場合は、PTZカメラを手動でキャリブレーションできます。

1. [One-click PTZ control (ワンクリックPTZコントロール)] > [PTZ positioning calibration (PTZ位置キャリブレーション)] に移動し、[Manual (手動)] をクリックします。
2. [Re-calibrate (再キャリブレーション)] をクリックします。
3. パノラマカメラのライブビューでポイントを定義し、リモートPTZカメラを同じ位置に向け
ます。
4. [Save (保存)] をクリックします。この手順を3回繰り返します。
5. Done (完了) をクリックします。

仕様

製品概要



- 1 保護アースターミナル
- 2 入出力ポート
- 3 音声入力
- 4 コントロールボタン
- 5 microSDカードスロット
- 6 ステータスLED
- 7 PoEコネクタ

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 29を参照してください。

コネクター

ネットワーク コネクター

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

I/Oコネクター

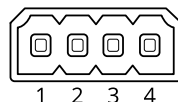
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

デジタル入力 - 開回路と閉回路の切り替えが可能な装置 (PIRセンサー、ドア/窓の接触、ガラス破損検知器など) を接続するための入力です。

状態監視入力 - デジタル入力のいたずらを検知する機能が有効になります。

デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

4ピンターミナルブロック

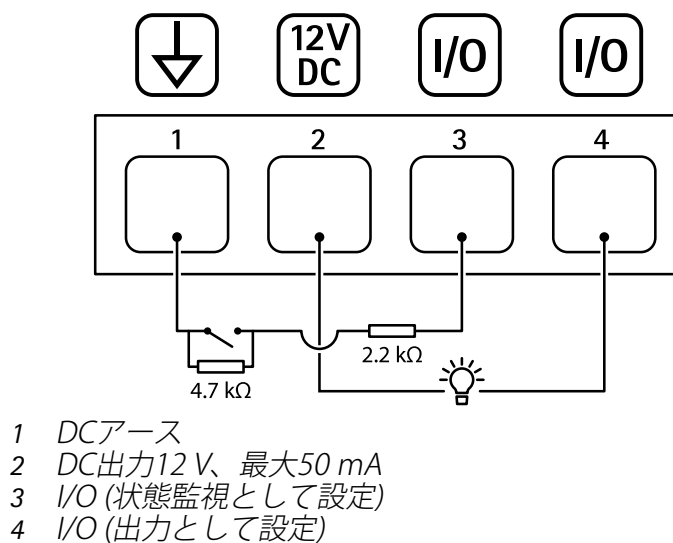


I/Oコネクタ表

機能	ピン	メモ	仕様
DCアース	1		0 V DC

DC出力	2	補助装置の電源供給に使用できます。 注:このピンは、電源出力としてのみ使用できません。	12 V DC 最大負荷 = 50 mA
設定可能 (入力または出力)	3-4	デジタル入力/状態監視 – 動作させるにはピン1に接続し、動作させない場合はフロート状態 (未接続) のままにします。状態監視を使用するには、終端抵抗器を設置します。抵抗器を接続する方法については、接続図を参照してください。	0～最大28 V DC
		デジタル出力 – アクティブ時はピン1 (DCアース) に内部で接続し、非アクティブ時はフロート状態 (未接続) になります。リレーなどの誘導負荷とともに使用する場合は、過渡電圧から保護するために、負荷と並列にダイオードを接続します。	0～28 V DC (最大)、 オープンドレイン、 100 mA

例:



装置を清掃する

装置はぬるま湯と低刺激、非研磨性の石鹼で洗浄できます。

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、ぬるま湯と低刺激、非研磨性の石鹼で湿らせ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. 残った洗浄剤を除去するには、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拭いてください。
 4. 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

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 25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 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 29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 4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 33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。

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。

T10172043_ja

2026-07 (M22.2)

© 2021 – 2025 Axis Communications AB