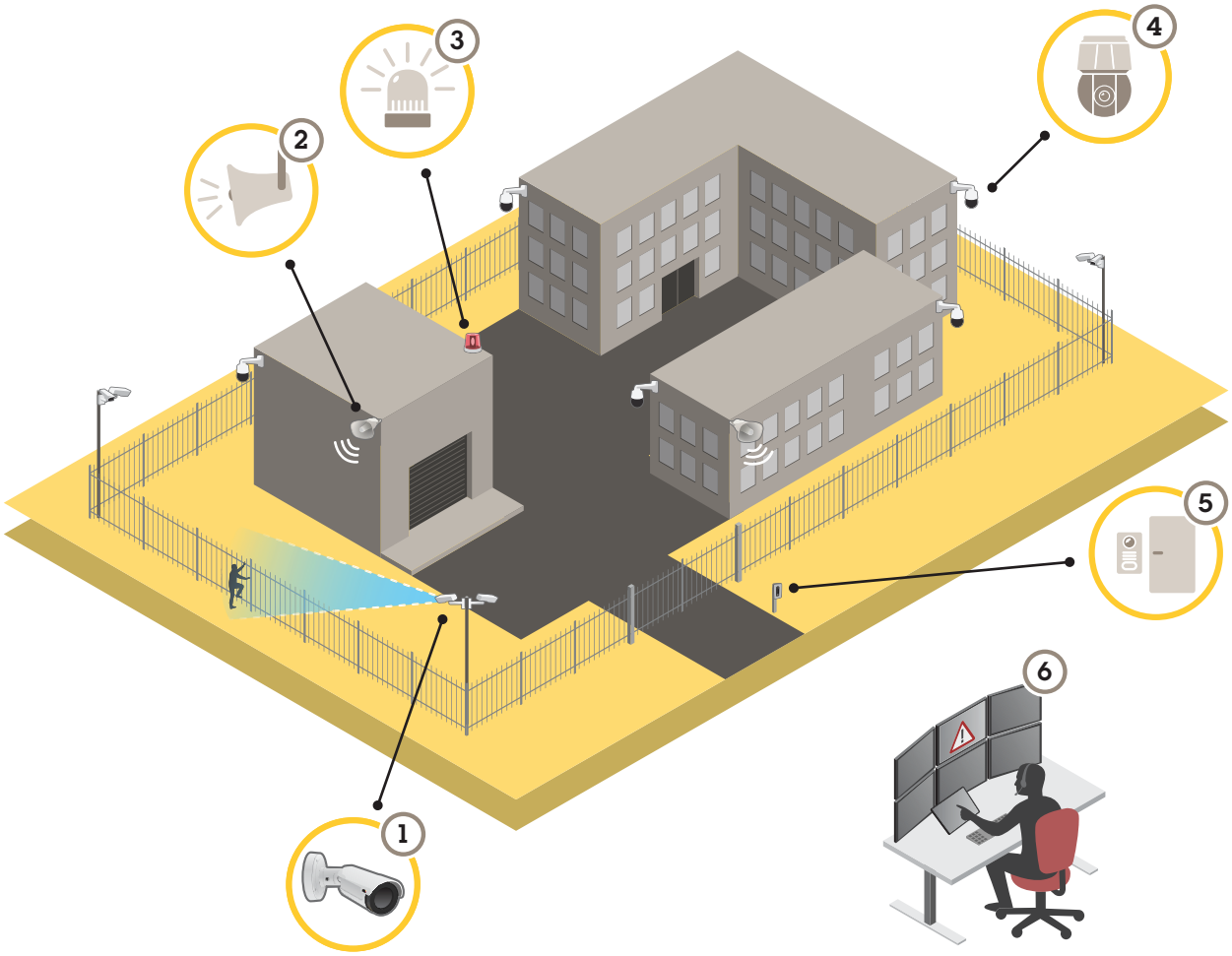
AXIS Q21 サーマルカメラシリーズ

AXIS Q2111-E Thermal Camera
AXIS Q2112-E Thermal Camera

ユーザーマニュアル

目次

ソリューションの概要



1 *AXIS Perimeter Defenderを搭載したサーマルカメラ*
2 *ホーンスピーカー*
3 *Flashing beacon (点滅ビーコン)*
4 *PTZネットワークカメラ*
5 *ドアコントローラー*
6 *監視センター*

周辺保護

侵入検知が必要なエリアでは、分析ソフトウェア内蔵のサーマルカメラを使用して周辺保護を設定することができます。周辺保護の主な目的は、脅威や実際の侵入をできるだけ早い段階で検知することです。

周辺保護を設定するには、境界線の監視と周辺保護のための分析アプリケーションをサーマルカメラにインストールする必要があります。Axisでは、この目的でAXIS Perimeter Defenderアプリケーションを提供しています。AXIS Perimeter Defenderの詳細については、*axis.com/products/axis-perimeter-defenderを参照してください*

- 侵入者になりそうな人に周辺が保護されていることを知らせるには、点滅ビーコン (3) を使用します。*点滅ビーコンにより侵入者を阻止する, on page 11*を参照してください。
- 警告を発して侵入を思いとどまらせるには、事前に録音された警告メッセージを再生するホーンスピーカー (2) を接続します。*音声により侵入者を阻止する, on page 12*を参照してください。

インストール

デバイスのインストールビデオ。

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 6*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 7*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 35*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 35*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。

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

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 8*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 18*を参照してください。

揺れる映像を動体ブレ補正によって安定させる

動体ブレ補正は、例えば風や通行車両による振動が発生するような、露出した場所に本製品が設置されている環境に適しています。

この機能を使用すると、画像がより滑らかになり、安定し、ブレにくくなります。また、圧縮された画像のファイルサイズが削減され、ビデオストリームのビットレートも低くなります。

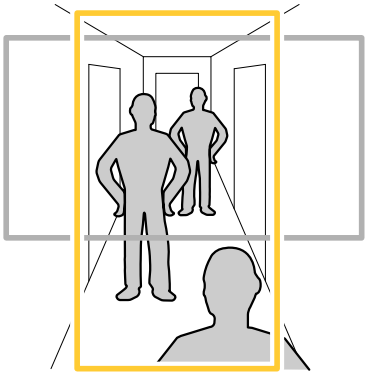
注

動体ブレ補正を有効にすると、画像がわずかにトリミングされて、最大解像度が低下します。

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. [Image stabilization (動体ブレ補正)] をオンにします。

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。

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 18*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ブラウザーは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、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。

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。

点滅ビーコンにより侵入者を阻止する

点滅ビーコンを使用して、侵入者になりそうな人に周辺が保護されていることを知らせます。

この例では、点滅ビーコン灯を接続し、サーマルカメラが侵入を検知したときに点灯するように設定する方法について説明します。この例では、ビーコンは営業時間外 (月曜～金曜の18:00～08:00) にのみ点滅を有効にすることができ、有効になるたびに30秒間点滅します。

必要なハードウェア

- 接続ワイヤー (青1本と赤1本、最小面積: 0.25 mm^2、最大面積: 0.5 mm^2)
- 点滅ビーコン (12 V DC、最大25 mA)

注

接続ワイヤーの最大長は、ワイヤーの面積と点滅ビーコンの電力消費によって異なります。

装置を物理的に接続する

1. 赤いワイヤーをカメラのI/Oコネクターのピン2 (DC出力、12 V DC) に接続します。
2. 赤いワイヤーのもう一方の端を、点滅ビーコンの+マーク付きコネクタに接続します。
3. 青いワイヤーをカメラのI/Oコネクターのピン4 (デジタル出力) に接続します。
4. 青いワイヤーのもう一方の端を、点滅ビーコンの-マーク付きコネクターに接続します。

I/Oポートの設定

カメラのwebインターフェースで、点滅ビーコンをカメラに接続します。

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. ポート2に、「Flashing beacon (点滅ビーコン)」と名前を付けます。
3. [Normal state (通常状態)] で、をクリックしてポートの通常状態を [Open circuit (NO) (開回路 (NO))] に設定します。これにより、イベントが発生するとビーコンが点滅し始めます。

ルールを作成する

何かが検知されたときにカメラからビーコンに通知を送って点滅を開始するには、カメラでルールを作成する必要があります。

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. [Name (名前)] に「Flashing beacon」と入力します。
3. [Wait between actions (アクション間の待ち時間)] (hh:mm:ss形式) を30秒に設定します。

4. [Application (アプリケーション)] の条件のリストで、Perimeter Defenderアプリケーションを選択します。
5. [Use this condition as a trigger (この条件をトリガーとして使用する)] を選択します。
6. ＋ をクリックして、別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. [I/O] のアクションのリストで、[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)] を選択します。
10. ポートのリストから [Flashing beacon (点滅ビーコン)] ポートを選択します。
11. [State (状態)] を [Active (アクティブ)] に設定します。
12. [保存] をクリックします。

音声により侵入者を阻止する

ネットワークホーンスピーカーは、侵入者になりそうな人に警告したり侵入を防いだりするために使用します。

この例では、Axisネットワークホーンスピーカーを接続し、サーマルカメラが侵入を検知したときに音声クリップを再生するように設定する方法について説明します。この例では、ホーンスピーカーは営業時間外 (月曜～金曜の18:00～08:00) にのみ有効にすることができます。

デバイスを接続する

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. スピーカーのIPアドレス、ユーザー名、パスワードを入力します。管理者またはオペレーターのアカウントを使用する必要があります。
3. [接続] をクリックします。

音声クリップをカメラにアップロードする

1. [Audio (音声)] > [Audio clip (音声クリップ)] に移動し、⚙ をクリックします。
2. [+ Add clip (クリップを追加)] をクリックします。
3. 音声クリップを見つけてアップロードします。
4. [閉じる] をクリックします。

ルールを作成する

何かが検知されたときにカメラからスピーカーで音声クリップを再生するには、カメラでルールを作成する必要があります。

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. [Name (名前)] に「Deter with audio」と入力します。
3. [Application (アプリケーション)] の条件のリストで、Perimeter Defenderアプリケーションを選択します。
4. [Use this condition as a trigger (この条件をトリガーとして使用する)] を選択します。
5. ＋ をクリックして、別の条件を追加します。
6. 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。
7. スケジュールのリストで、[After hours (就労時間外)] を選択します。

8. アクションのリストで、[Audio clips (音声クリップ)] の [Play audio clip (音声クリップの再生)] を選択します。
9. [Clip (クリップ)] で、アップロードした音声クリップを選択します。
10. [Audio output (音声出力)] で、ペアリングされたネットワークスピーカーに対応する [1] を選択します。
11. [保存] をクリックします。

カメラが動きを検知したときに仮想入力によりストロボサイレンをアクティブにする

Axisのストロボサイレンを使用すると、敷地周辺が保護されていることを侵入者に知らせることができます。

この例では、AXIS Motion Guardが動きを検知するたびに、ストロボサイレンのプロファイルをアクティブにする方法について説明します。

開始する前に、以下をご確認ください。

- ストロボサイレンでオペレーター、または管理者権限を持つ新しいアカウントを作成します。
- ストロボサイレンにプロファイルを作成します。
- カメラでAXIS Motion Guardを設定し、「カメラプロファイル」というプロファイルを作成します。

カメラで2人の送信先を作成する:

1. カメラの装置インターフェースで [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. 以下の情報を入力します。
   - 名前:Activate virtual port (仮想ポートのアクティブ化)
   - Type (タイプ): HTTP
   - URL: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
<IPaddress>の部分をストロボサイレンのアドレスに置き換えます。
   - 新しく作成したストロボサイレンアカウントのアカウント名とパスワード。
3. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
4. [保存] をクリックします。
5. 次の情報を含む2番目の送信先を追加します。
   - 名前:仮想ポートの非アクティブ化
   - Type (タイプ): HTTP
   - URL: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
<IPaddress>の部分をストロボサイレンのアドレスに置き換えます。
   - 新しく作成したストロボサイレンアカウントのアカウント名とパスワード。
6. [Test (テスト)] をクリックして、すべてのデータが有効であることを確認します。
7. [保存] をクリックします。

カメラに2つのルールを作成する:

1. [Rules (ルール)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:仮想IO1のアクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]

- Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
- Recipient (送信先): Activate virtual port (仮想ポートのアクティブ化)
- Query string suffix (クエリ文字列のサフィックス): schemaversion=1&port=1

3. [保存] をクリックします。
4. 次の情報を含む別のルールを追加します。
   - 名前:仮想IO1の非アクティブ化
   - Condition (条件): [Applications (アプリケーション)] > [Motion Guard: Camera profile (Motion Guard: カメラプロファイル)]
   - [Invert this condition (この条件を逆にする)] を選択します。
   - Action (アクション): Notifications > Send notification through HTTP (通知 > HTTPで通知を送信する)
   - Recipient (送信先): 仮想ポートの非アクティブ化
   - Query string suffix (クエリ文字列のサフィックス): schemaversion=1&port=1
5. [保存] をクリックします。

ストロボサイレンにルールを作成する:

1. ストロボサイレンのwebインターフェースで、[System (システム)] > [Events (イベント)] に移動し、ルールを追加します。
2. 以下の情報を入力します。
   - 名前:仮想入力1のトリガー
   - Condition (条件): [I/O] > [Virtual input (仮想入力)]:
   - ポート: 1
   - Action (アクション): Light and siren > Run light and siren profile while the rule is active (ライトとサイレン > ルールがアクティブである間は、ライトとサイレンのプロファイルを実行)
   - Profile (プロファイル): 新しく作成したプロファイルを選択する
3. [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コネクターの詳細については、*page 28*を参照してください。

1. System (システム) > Accessories (アクセサリー)> 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。

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。

レンズにスプレーを吹き付けられた場合に自動的にメールを送信する

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。

メール送信先を追加する:

3. [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。
4. 送信先の名前を入力します。

5. [Email (電子メール)] を選択します。
6. 電子メールの送信先のメールアドレスを入力します。
7. カメラには独自のメールサーバーがないため、電子メールを送信するには別のメールサーバーにログインする必要があります。メールプロバイダーに従って、残りの情報を入力します。
8. テストメールを送信するには、[Test (テスト)] をクリックします。
9. [保存] をクリックします。

ルールの作成:

10. [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。
11. ルールの名前を入力します。
12. 条件のリストで、[Video (ビデオ)]の[Tampering (いたずら)] を選択します。
13. [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。
14. 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。

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。

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

カラーパレット

サーマル画像の細部を人間の目で区別できるようにするために、画像にカラーパレットを適用できます。パレット内の色は、温度の違いを強調するために人工的に作り出された疑似カラーです。

本製品には選択可能な複数のカラーパレットがあります。オペレーターがビデオストリームを見る場合は、いずれかのパレットを選択できます。ビデオストリームをアプリケーションでのみ使用する場合は、ホワイトホットパレットを選択します。

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ーは、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。

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

注

Opus音声コーデックを確実にサポートするために、Motion JPEGストリームが常にRTP経由で送信されます。

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、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。

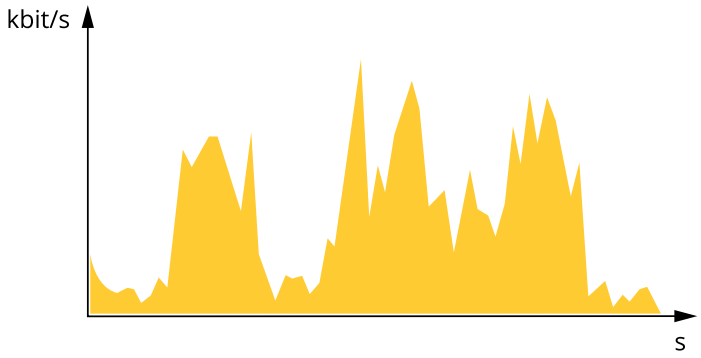
[Stream (ストリーム)] タブには、ビデオストリームの設定が含まれています。解像度やフレームレートなどを指定せずに、製品からのビデオストリームを要求している場合は、これらの設定が使用されます。[Stream (ストリーム)] タブで設定を変更すると、実行中のストリームには影響しませんが、新しいストリームを開始したときに有効になります。

[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。

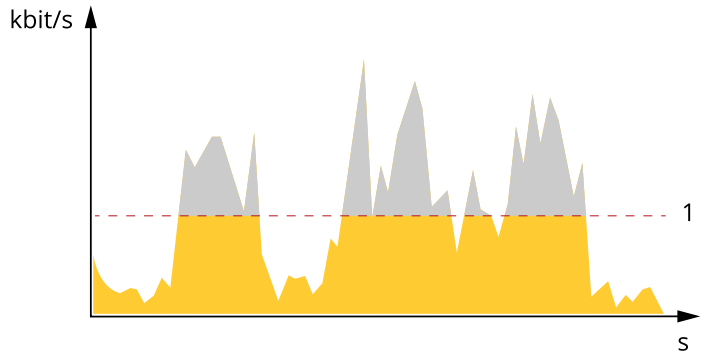
ビットレート制御

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。

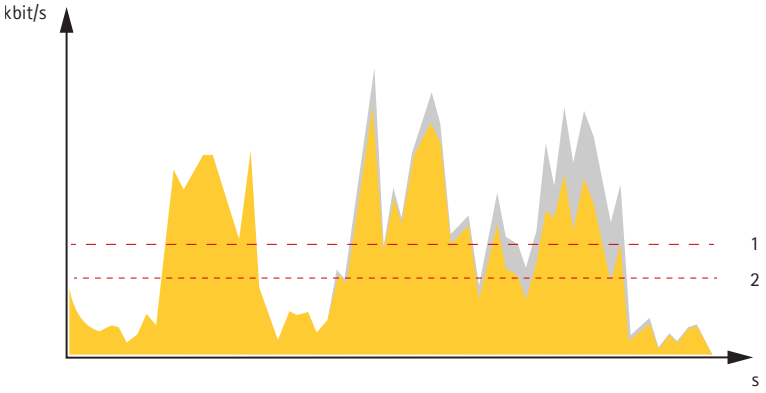


1 目標ビットレート

平均ビットレート（ABR）

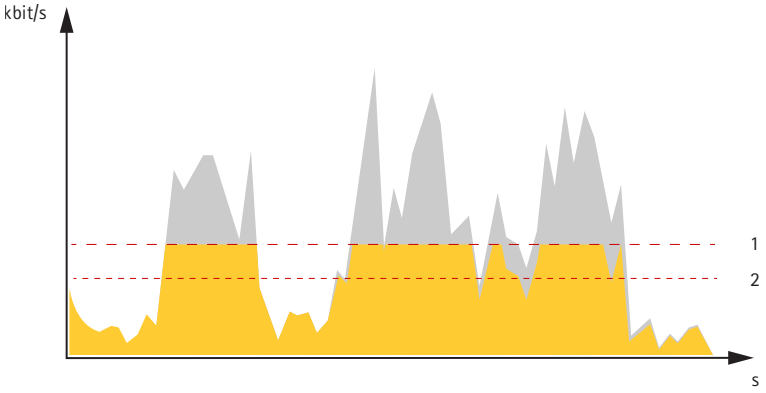
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できます。次のいずれかの方法で、平均ビットレートの設定を指定します。

- 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。

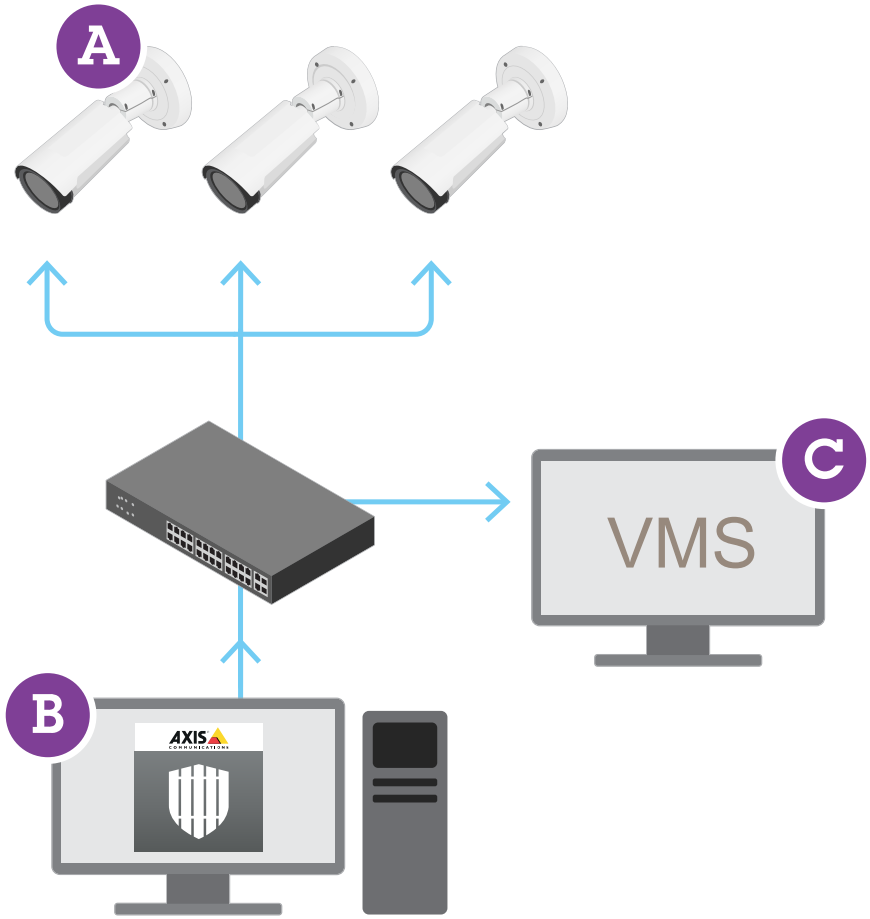
AXIS Perimeter Defender

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

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

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

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



このカメラでは、キャリブレーションモード、AIモード、または両モードの組み合わせでアプリケーションを実行できます。AIモードでのみの動作を選択した場合、カメラの取り付けはより柔軟になり、カメラをキャリブレーションする必要はありません。

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

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

重要

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

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

- **Intrusion (侵入)**：人物または車両が地面上の定義されたゾーンに (任意の方向と軌道により) 入ると、アラームをトリガーします。
- **Loitering (徘徊)**：人物または車両が地面上の定義されたゾーンに、あらかじめ定義した秒数より長く留まるとアラームをトリガーします。

- Zone-crossing (ゾーン横断)：人物または車両が地面上の2つ以上の定義されたゾーンを指定されたシーケンスで通過するときにアラームをトリガーします。
- Conditional (条件付き)：人物または車両が最初に地面上の定義された他のゾーンを通過することなく地面上の定義ゾーンに入ると、アラームをトリガーします。

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できます。

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が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

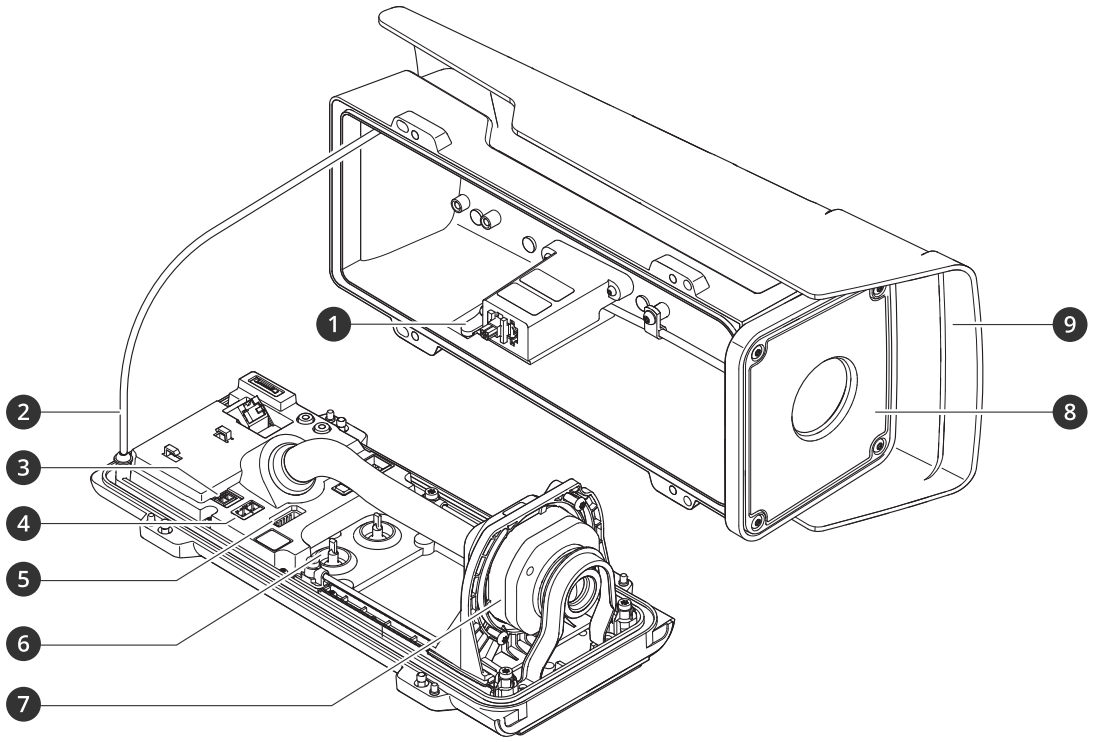
お客様の脆弱性リスクを最小限に抑えるため、Axisは**CVE (共通脆弱性識別子) 採番機関**として業界標準に従って、装置、ソフトウェア、およびサービスで発見された脆弱性の管理と対応を行っています。 Axisの脆弱性管理ポリシー、脆弱性の報告方法、すでに公開されている脆弱性、対応するセキュリティ勧告の詳細については、*axis.com/vulnerability-management*をご覧ください。

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。

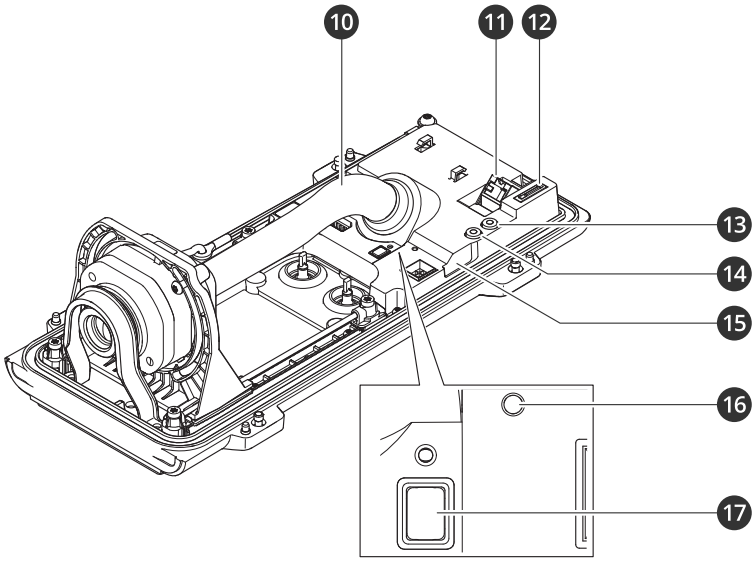
仕様

製品概要



1 侵入アラームマグネット
2 安全ワイヤー
3 電源コネクター
4 RS485/422コネクター
5 I/Oコネクター
6 ケーブルガスケットM20 (×2)
7 光学ユニット*
8 正面ウィンドウ
9 ウェザーシールド

*光学ユニットの外観は、選択したレンズによって異なります。



1 *ケーブルカバー*
2 *ネットワークコネクタ (PoE)*
3 *microSDカードスロット*
4 *音声出力*
5 *音声入力*
6 *侵入アラームセンサー*
7 *ステータスLED*
8 *コントロールボタン*

LEDインジケーター

注

- ステータスLEDは、イベントの発生時に点滅させることができます。
- ケーシングを閉じると、LEDは消灯します。

ステータスLED	説明
消灯	接続時および正常動作時です。
緑	接続時および正常動作時です。
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。

ブザー

レベルアシスタントのブザー信号

画像のレベル調整に使用するコントロールボタンの詳細については、*page 27*を参照してください。

ブザー	カメラの位置
連続音	水平
高速なブザー音	ほぼ水平
中程度の速さのブザー音	水平ではない
低速なブザー音	かなり傾いている

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 35*を参照してください。
- カメラを確実に水平にする。ボタンを約2秒間押し続けると水平化アシスタントが起動し、もう一度押すと停止します。ブザー信号 (レベルアシスタント*page 26*を参照) は、カメラの水平化を支援します。カメラが水平になると、ブザーが連続音になります。

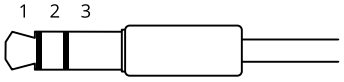
コネクター

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

音声コネクター

- **音声入力** - デジタルマイクロフォン、アナログモノラルマイクロフォンまたはラインインモノラル信号用 (左チャンネルはステレオ信号で使用) 3.5 mm入力。
- **音声出力** - 3.5 mm音声 (ラインレベル) 出力 (パブリックアドレス (PA) システムまたはアンプ内蔵アクティブスピーカーに接続可能)。音声出力には、ステレオコネクタを使用する必要があります。



音声入力

1 チップ	2 リング	3 スリーブ
アンバランス型マイクロフォン (エレクトレット電源あり、なし) またはライン入力	選択されている場合、エレクトレット電源	アース
デジタル信号	選択されている場合、リング電源	アース

音声出力

1 チップ	2 リング	3 スリーブ
チャンネル1、アンバランス型ライン、モノラル	チャンネル1、アンバランス型ライン、モノラル	アース

I/Oコネクター

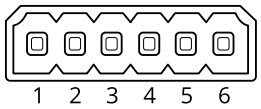
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

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。

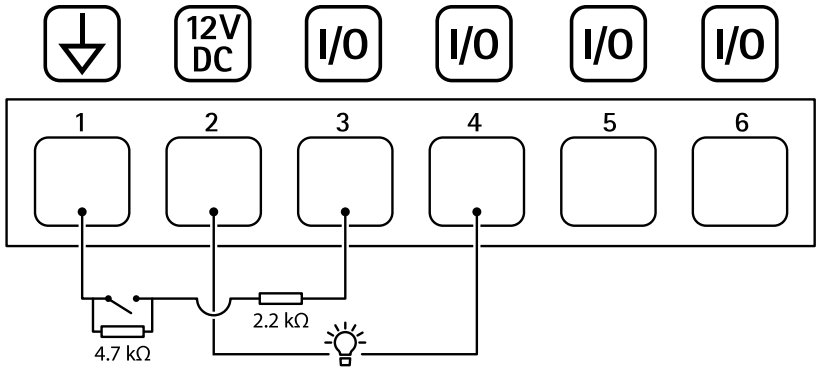
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

6ピンターミナルブロック



機能	ピン	メモ	仕様
DCアース	1		0 VDC
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す。	12VDC 最大負荷 = 50 mA
設定可能 (入力または出力)	3–6	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。	0～30 VDC (最大)
		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。	0～30 VDC (最大)、オープンドレイン、100 mA

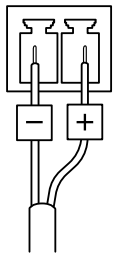
例:



1 *DCアース*
2 *DC出力12 V、最大50 mA*
3 *I/O (状態監視として設定)*
4 *I/O (出力として設定)*
5 *設定可能I/O*
6 *設定可能I/O*

電源コネクター

DC電源入力用2ピンターミナルブロック。定格出力が100 W以下または5 A以下の安全特別低電圧 (SELV) に準拠した有限電源 (LPS) を使用してください。

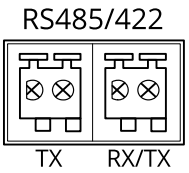


RS485/RS422コネクター

RS485/RS422シリアルインターフェース用2ピンターミナルブロック×2。

シリアルポートの設定により、次のモードをサポート可能。

- 2ワイヤーRS485半二重
- 4ワイヤーRS485全二重
- 2ワイヤーRS422単方向
- 4ワイヤーRS422全二重ポイントツーポイント通信



機能	メモ
RS485/RS422 TX(A)	RS422および4ワイヤーRS485のTXペア
RS485/RS422 TX(B)	
RS485AまたはRS485/422 RX(A)	すべてのモードのRXペア (2ワイヤーRS485のRX/TXペア)

RS485BまたはRS485/ 422 RX(B)	

注
カメラをAXIS T99 Positioning Unitで使用するには、RS485AおよびRS485B (RX/TX) に接続します。

PTZドライバー

APTP

これは、このドライバーでサポートされるモデルの一覧です。物理的な設置方法は、Axis製品とPTZユニットによって異なります。

重要
Axis製品とPTZユニットがサポートするシリアル通信を確認してください。

RS485 2ワイヤーインターフェース搭載のサポートされるモデル:
- AXIS T99A Positioning Unitシリーズ。
  対応するAxis製品については、*axis.com*を参照してください。

他のモデルがサポートされている可能性がありますが、これはAxisによって検証されていません。

技術的な情報

PTZドライバーのデフォルトの機能:

ドライバー	APTP
バージョン	1.1.0

デフォルトのシリアル設定:

ポートモード	RS485
ボーレート	115,200
データビット	8
ストップビット	1
パリティ	ありません

このPTZドライバーでサポートされるデフォルトの機能:

注
PTZユニットによっては、他の機能がいくつか備わっている場合があります。

動きあり	絶対動作	相対動作	連続録画
パン	有	有	有
チルト	有	有	有

Pelco

これは、このドライバーでサポートされるモデルの一覧です。物理的な設置方法は、Axis製品とPTZユニットによって異なります。

重要

Axis製品とPTZユニットがサポートするシリアル通信を確認してください。

サポートされるモデル:

- Pelco DD5-C
- Pelco Esprit ES30C/ES31C
- Pelco LRD41C21
- Pelco LRD41C22
- Pelco Spectra III
- Pelco Spectra IV
- Pelco Spectra Mini
- Videotec DTRX3/PTH310P
- Videotec ULISSE
- PTK AMB
- YP3040

他のモデルがサポートされている可能性がありますが、これはAxisによって検証されていません。

技術的な情報

PTZドライバーのデフォルトの機能:

ドライバー	Pelco
バージョン	4.17

デフォルトのシリアル設定:

ポートモード	RS485
ボーレート	2,400
データビット	8
ストップビット	1
パリティ	ありません

このPTZドライバーでサポートされるデフォルトの機能:

注

PTZユニットによっては、他の機能がいくつか備わっている場合があります。

動きあり	絶対動作	相対動作	連続録画
パン	なし	有	有
チルト	なし	有	有
ズーム	なし	有	有
フォーカス	なし	有	有
虹彩	なし	有	有

オートアイリス	有
オートフォーカス	有

IRカットフィルター	なし
逆光	有
OSDメニュー	有

Visca

これは、このドライバーでサポートされるモデルの一覧です。物理的な設置方法は、Axis製品とPTZユニットによって異なります。

重要

Axis製品とPTZユニットがサポートするシリアル通信を確認してください。

RS422 4ワイヤー有線インターフェース搭載のサポートされるモデル:

- Sony EVI-D70/D70P
- WISKA DCP-27 (PTヘッド)

RS232インターフェース搭載のサポートされるモデル (外部RS422-4ワイヤー/RS232コンバータが必要な場合があります):

- Axis EVI-D30/D31
- Sony EVI-G20/G21
- Sony EVI-D30/D31
- Sony EVI-D100/D100P
- Sony EVI-D70/D70P

他のモデルがサポートされている可能性がありますが、これはAxisによって検証されていません。

技術的な情報

PTZドライバーのデフォルトの機能:

ドライバー	Visca/EVI
バージョン	4.11

デフォルトのシリアル設定:

ポートモード	RS422
ボーレート	9,600
データビット	8
ストップビット	1
パリティ	ありません

このPTZドライバーでサポートされるデフォルトの機能:

注

PTZユニットによっては、他の機能がいくつか備わっている場合があります。

動きあり	絶対動作	相対動作	連続録画
パン	有	有	有
チルト	有	有	有
ズーム	有	有	有

動きあり	絶対動作	相対動作	連続録画
フォーカス	有	有	有
虹彩	有	有	なし

オートアイリス	有
オートフォーカス	有
IRカットフィルター	有
逆光	有
OSDメニュー	なし

装置を清掃する

装置はぬるま湯と低刺激、非研磨性の石鹸で洗浄できます。

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。
- 装置に洗剤を直接スプレーしないでください。代わりに、非研磨性の布に洗剤をスプレーし、その布で装置を清掃してください。
- 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、非研磨性の石鹸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. 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

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 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. デバイスに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 35*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 6*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/vms*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。

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て、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。
- パレットを使用すると、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。

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。

T10208523_ja

2026-02 (M7.2)