AXIS P1465-LE-3 License Plate Verifier Kit

ユーザーマニュアル

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 2*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 3*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 48*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 48*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。

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。

Axis装置のwebインターフェース

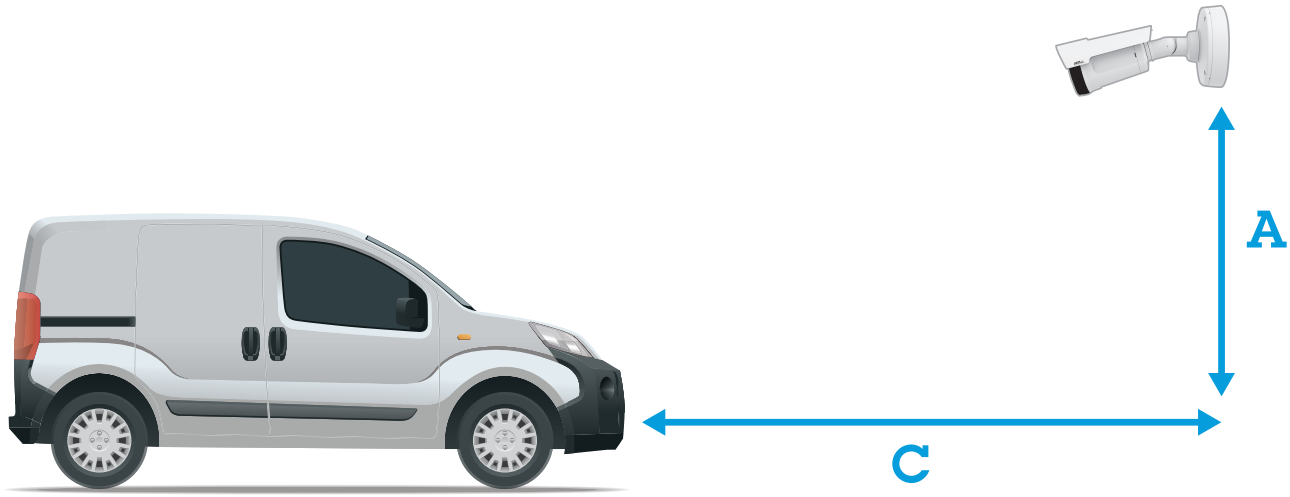
基本設定

以下の設定手順は、すべてのシナリオで有効です。

1.
2.
3. *対象範囲を調整する, on page 8*
4. *地域の選択, on page 9*
5. *イベントストレージを設定する, on page 10*

カメラ取り付けの推奨事項

- 設置場所を選択するときは、日の出や日の入りの間などに、直射日光が画像に影響を及ぼす可能性があることに注意してください。
- [Access control (アクセスコントロール)] シナリオでのカメラの取り付け高さは、車両とカメラとの間の距離の半分にする必要があります。
- [Free flow (フリーフロー)] (低速走行車両のナンバープレート認識) シナリオでのカメラの取り付け高さは、車両とカメラとの間の距離の半分未満にする必要があります。



アクセスコントロール キャプチャー距離: 2〜7 m (6.6〜23 ft)。この例は、AXIS P3265-LVE-3 License Plate Verifier Kitに基づいています。

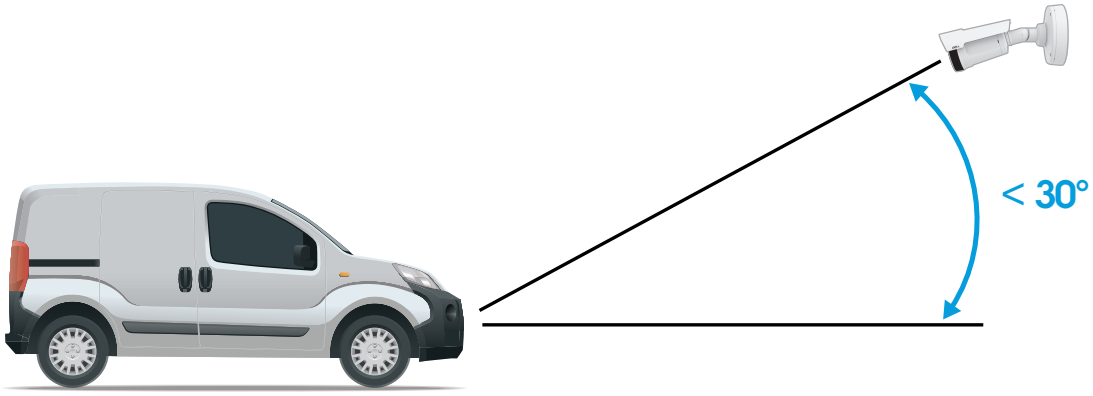
キャプチャー距離: (C)	取り付け高さ (A)
2.0 m (6.6 ft)	1.0 m (3.3 ft)
3.0 m (9.8 ft)	1.5 m (4.9 ft)
4.0 m (13 ft)	2.0 m (6.6 ft)
5.0 m (16 ft)	2.5 m (8.2 ft)
7.0 m (23 ft)	3.5 m (11 ft)

フリーフロー キャプチャー距離: 7〜20m（23〜65 ft）。この例は、AXIS P1465-LE-3 License Plate Verifier Kitに基づいています。

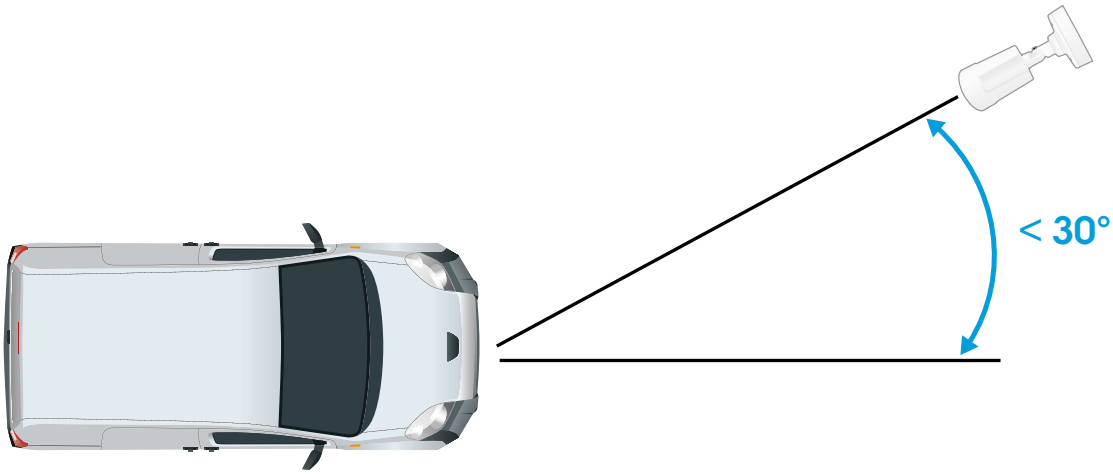
キャプチャー距離 (C)	取り付け高さ (A)
7.0 m (23 ft)	3.0 m (9.8 ft)
10.0 m (33 ft)	4.0 m (13 ft)

15.0 m (49 ft)	6.0 m (19.5 ft)
20.0 m (65 ft)	10.0 m (33 ft)

- カメラの取り付け角度は、いずれの方向でも30°より大きくしないでください。

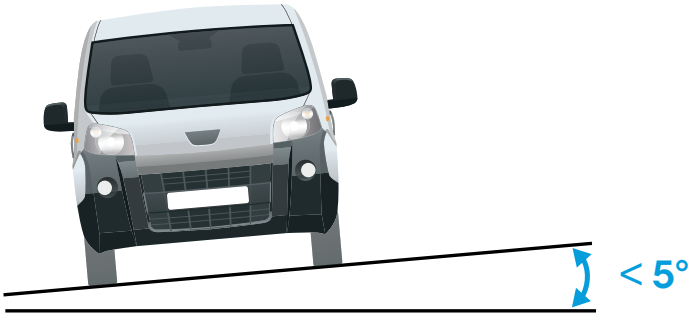


横からの取り付け角度。



上からの取り付け角度。

- ナンバープレートの画像は、水平方向に5°を超えてチルトさせないでください。画像が5°を超えてチルトしている場合は、ライブストリームでナンバープレートが水平に表示されるように、カメラを調整することをお勧めします。



ロール角度。

設定アシスタント

アプリケーションを最初に実行するときは、設定アシスタントを使用して [Free flow (フリーフロー)] または [Access control (アクセスコントロール)] を設定します。後で変更する場合は、[Settings (設定)] > [Maintenance (メンテナンス)] に移動し、[Setup assistant (設定アシスタント)] で [Start(開始)] を押します。

フリーフロー

フリーフローでは、このアプリケーションは大規模な連絡道路、市街地のほか、キャンパス、港、空港などの閉鎖されたエリアで、低速走行車両のナンバープレートを検知して読み取ることができます。これにより、VMSでLPRフォレンジック検索やLPRトリガーイベントが可能になります。

1. [Free flow (フリーフロー)] を選択し、[Next (次へ)] をクリックします。
2. カメラの取り付け方法に応じて画像の回転を選択します。
3. 対象範囲の数を選択します。1つの範囲で、両方向でプレートを検知できることに注意してください。
4. カメラが配置されている範囲を選択します。
5. キャプチャータイプを選択します。
   - License plate crop (ナンバープレートのクロップ): ナンバープレートのみが保存されます。
   - Vehicle crop (車両のクロップ): キャプチャーされた車両全体が保存されます。
   - Frame downsized 480x270 (480x270にダウンサイズされたフレーム): 画像全体が保存され、解像度は480x270に下げられます。
   - Full frame (フルフレーム): 画像全体がフル解像度で保存されます。
6. アンカーポイントをドラッグして、対象範囲を調整します。*対象範囲を調整する, on page 8*を参照してください。
7. 対象範囲の方向を調整します。矢印をクリックして回転させて、方向を設定します。方向により、対象範囲に出入りする車両がアプリケーションで登録される方法が決まります。
8. [Next (次へ)] をクリックします。
9. [Protocol (プロトコル)] ドロップダウンリストで、以下のいずれかのプロトコルを選択します。
   - TCP

- HTTP POST

10. [Server URL (サーバーのURL)] フィールドに、次の形式でサーバーのアドレスとポートを入力します: `127.0.0.1:8080`
11. [Device ID (デバイスID)] フィールドに装置の名前を入力するか、そのままにします。
12. [Event types (イベントタイプ)] で、以下のオプションから1つ以上選択します。
    - [New (新規)] は、ナンバープレートが初めて検知されたことを意味します。
    - [Update (更新)] は、以前に検知されたナンバープレートの文字を修正する場合と、プレートの移動に伴って方向が検知され、画像上で追跡される場合のどちらかです。
    - [Lost (消失)] は、ナンバープレートが画像から出る前の最後の追跡イベントです。これには、ナンバープレートの方向も含まれます。
13. この機能をオンにするには、[Send event data to server (イベントデータをサーバーに送信する)] を選択します。
14. HTTP POSTを使用する際に帯域幅を削減するには、[Do not to send images through HTTP POST (HTTP POST で画像を送信しない)] を選択します。
15. [Next (次へ)] をクリックします。
16. 登録済みのプレートのリストがすでにある場合は、[blocklist (ブロックリスト)] としてインポートするか、[allowlist (許可リスト)] としてインポートするかを選択します。
17. Finish (終了) をクリックします。

アクセスコントロール

セットアップウィザードを使用すると、すばやく簡単に設定できます。[Skip (スキップ)] を選択して、いつでもガイドを読み飛ばすことができます。

1. [Access control (アクセスコントロール)] を選択し、[Next (次へ)] をクリックします。
2. 使用するアクセスコントロールのタイプを選択します。
    - カメラでリストを管理する場合は、[Internal I/O (内部I/O)] を選択します。*既知の車両の場合に、カメラのI/Oを使用してゲートを開く, on page 28*を参照してください。
    - ドアコントローラーを接続する場合は、[Controller (コントローラー)] を選択します。を参照してください。
    - リレーモジュールに接続する場合は、[Relay (リレー)] を選択します。を参照してください。
3. [Barrier mode (ゲートモード)] ドロップダウンリストの [Open from lists (リストから開く)] で、[Allowlist (許可リスト)] を選択します。
4. [Vehicle direction] (車両の方向) ドロップダウンリストから [out] (出庫) を選択します。
5. [ROI] ドロップダウンリストで、使用する対象範囲を選択するか、すべての対象範囲を使用するかを選択します。
6. [Next (次へ)] をクリックします。

[Image settings (画像設定)] ページで、次の設定を行います。

1. 対象範囲の数を選択します。
2. カメラが配置されている範囲を選択します。
3. キャプチャータイプを選択します。*画像キャプチャーの設定を調整する, on page 9*を参照してください。
4. アンカーポイントをドラッグして、対象範囲を調整します。*対象範囲を調整する, on page 8*を参照してください。

5. 対象範囲の方向を調整します。方向により、対象範囲に出入りする車両がアプリケーションで登録される方法が決まります。
6. [Next (次へ)] をクリックします。

[Event data (イベントデータ)] ページ で、次の処理を行います。

注

詳細な設定については、*サードパーティ製ソフトウェアへのイベント情報のプッシュ, on page 37*を参照してください。

1. [Protocol (プロトコル)] ドロップダウンリストで、以下のいずれかのプロトコルを選択します。
   - TCP
   - HTTP POST
2. [Server URL (サーバーのURL)] フィールドに、次の形式でサーバーのアドレスとポートを入力します: `127.0.0.1:8080`。
3. [Device ID (デバイスID)] フィールドに装置の名前を入力するか、そのままにします。
4. [Event types (イベントタイプ)] で、以下のオプションから1つ以上選択します。
   - [New (新規)] は、ナンバープレートが初めて検知されたことを意味します。
   - [Update (更新)] は、以前に検知されたナンバープレートの文字を修正する場合と、プレートの移動に伴って方向が検知され、画像上で追跡される場合のどちらかです。
   - [Lost (消失)] は、ナンバープレートが画像から出る前の最後の追跡イベントです。これには、ナンバープレートの方向も含まれます。
5. この機能をオンにするには、[Send event data to server (イベントデータをサーバーに送信する)] を選択します。
6. HTTP POSTを使用する際に帯域幅を削減するには、[Do not to send images through HTTP POST (HTTP POST で画像を送信しない)] を選択します。
7. [Next (次へ)] をクリックします。

[Import list from a .csv file (.csvファイルからリストをインポート)] ページで、次の操作を行います。

1. 登録済みのプレートのリストがすでにある場合は、[blocklist (ブロックリスト)] としてインポートするか、[allowlist (許可リスト)] としてインポートするかを選択します。
2. Finish (終了) をクリックします。

アプリケーションの設定にアクセスする

1. カメラのwebインターフェースで、[Apps (アプリ)] に移動し、アプリケーションを起動して、[Open (開く)] をクリックします。

対象範囲を調整する

対象範囲は、アプリケーションがナンバープレートを探すライブビュー内のエリアです。最適なパフォーマンスを得るには、対象範囲をできるだけ小さく保ってください。対象範囲を調整するには、以下の手順に従います。

1. [Settings (設定)] に移動します。
2. [Image (画像)] をクリックします。
3. 1:1をクリックすると、監視したい場所やアクセスコントロールを管理したい場所をズームできます。
4. 検証とキャプチャー画像の品質を高めるには、[AF] をクリックします。

5. 車両に自動でフォーカスを合わせるには、[AF]をクリックします。手動でフォーカスを合わせる場合は、スライダーで調整します。
6. [Area of interest (対象範囲)] をクリックして、ビューエリアに表示します。
7. 対象範囲を移動するには、その範囲内の任意の場所をクリックして選択し、ナンバープレートが最も見えやすい場所にドラッグします。設定を保存した後、対象範囲が適切な位置にとどまっていることを確認してください。
8. 対象範囲を調整するには、範囲内の任意の場所をクリックして選択し、青色で強調表示されているアンカーポイントをドラッグします。
   - 対象範囲をリセットするには、左下の数字アイコンの横のリセットボタンをクリックします。
   - アンカーポイントを追加するには、暗色のアンカーポイントのいずれかをクリックします。アンカーポイントが黄色に変わり、操作できることを示します。黄色のアンカーポイントの隣に新しい暗色のポイントが自動的に追加されます。黄色のアンカーポイントの最大数は8です。
9. 対象範囲の外部のどこかをクリックすると、変更が保存されます。
10. [Event log (イベントログ)] で正しい方向のフィードバックを取得するには、矢印を運転方向に向ける必要があります。
    10.1. 矢印アイコンをクリックします。
    10.2. アンカーポイントを選択し、矢印を回転させて、運転方向に合わせます。
    10.3. 対象範囲の外部でクリックすると、変更が保存されます。

1つの範囲で、両方向でプレートを検知できることに注意してください。方向のフィードバックは、[Direction] (方向) 列に表示されます。

11. 対象範囲が最適な効果を得るために十分な大きさかどうかを確認するには、ピクセルカウンターを使用します。
    - ピクセルカウンターを表示するには、電卓のアイコンをクリックします。
    - フルサイズのピクセルカウンターエリアを調整するには、黄色でハイライト表示されているエリアの右下のコーナーをドラッグします。
    - ピクセルカウンターエリアを移動するには、そのエリア内の任意の場所をクリックし、移動先にドラッグします。

- 2つ目の対象範囲を追加するには、1の横の+をクリックします。
- スタンドアロンのカメラを使用している場合は、アプリでナンバープレート認識の推奨設定を適用できます。
  1. 魔法の杖のアイコンをクリックすると、ナンバープレート認識用に設定が最適化されます。
  2. 魔法の杖の横にあるメニューボタンをクリックすると、設定値が表示されます。

地域の選択

1. [Settings (設定)] > [Recognition (認識)] に移動します。
2. [Region (地域)] ドロップダウンリストから地域を選択します。

画像キャプチャーの設定を調整する

1. [Settings (設定)] > [Image (画像)] に移動します。
2. キャプチャーされた画像の解像度を変更するには、[Image resolution (画像解像度)] に移動します。
3. キャプチャーされた画像の回転を変更するには、[Rotation (回転)] に移動します。

イベントストレージを設定する

イベントは、キャプチャーした画像、ナンバープレート、関心領域番号、車の方向、アクセス、日付と時刻で構成されます。

この使用事例では、許可リストに追加されたナンバープレート番号のイベントを30日間、保存する方法について説明します。

要件:

- カメラがネットワークに物理的に設置および接続されている。
- カメラでAXIS License Plate Verifierが起動され実行されている。
- 内部ストレージまたはカメラに取り付けられたSDカード。

1. [Settings (設定)] > [Storage (ストレージ)] に移動します。
2. [Retain events (イベントの保持)] で、[Allowlisted (許可リスト)] を選択します。
3. [Retention period (保持期間)] で、[30 days (30日)] を選択します。
4. キャプチャーされた画像の保存方法を変更するには、[Save full frame (フルフレームを保存)] に移動します。
   - License plate crop (ナンバープレートのクロップ): ナンバープレートのみが保存されます。
   - Vehicle crop (車両のクロップ): キャプチャーされた車両全体が保存されます。
   - Frame downsized 480x270 (480x270にダウンサイズされたフレーム): 画像全体が保存され、解像度は480x270に下げられます。
   - Full frame (フルフレーム): 画像全体がフル解像度で保存されます。

注

アプリの実行中に挿入されたSDカードを検知するには、アプリを再起動する必要があります。カメラにSDカードが取り付けられている場合、デフォルトストレージとしてSDカードが自動的に選択されます。

AXIS License Plate Verifierは、カメラの内部メモリを利用して、ナンバープレートのクロップをフレームとして使って最大1,000件のイベントを保存します。大型のフレームを使用する場合、保存できるイベントの量が変わります。

SDカードは、任意のタイプのフレームを使用して最大100,000件のイベントを保存できます。

インストール

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。

製品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

AXIS Camera Stationのユーザー向け

AXIS License Plate Verifierの設定

装置がAXIS License Plate Verifierで設定されている場合、その装置はビデオ管理システムの外部データソースと見なされます。表示をデータソースに接続し、装置でキャプチャーされたナンバープレートを検索して関連する画像を表示できます。

注

- AXIS Camera Station 5.38以降が必要です。
- AXIS License Plate Verifierにはライセンスが必要です。

1. アプリケーションをダウンロードして装置にインストールします。
2. アプリケーションの設定を行います。『*AXIS License Plate Verifierユーザーマニュアル*』を参照してください。
3. 既存のAXIS Camera Stationインストールの場合は、クライアントとの通信に使用されるサーバー証明書を更新します。*証明書の更新*を参照してください。
4. 時刻同期をオンにして、AXIS Camera StationサーバーをNTPサーバーとして使用します。*サーバーの設定*を参照してください。
5. デバイスをAXIS Camera Stationに追加する。*装置の追加*を参照してください。
6. 最初のイベントを受信すると、データソースは [**Configuration > Devices > External data sources (設定 > デバイス > 外部データソース)**] の下に自動的に追加されます。
7. データソースをビューに接続します。*外部データソース*を参照してください。
8. 装置によってキャプチャーされたナンバープレートを検索します。「*データ検索*」を参照してください。
9. をクリックして、検索結果を.txtファイルにエクスポートします。

基本設定

シーンプロファイルの設定

1. [**Video > Image > Appearance (ビデオ > 画像 > 外観)**] に移動します。
2. [**Scene profile (シーンプロファイル)**] で、[**Change (変更)**] をクリックします。

電源周波数を設定する

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

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。

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て使用します。

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。

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。

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、直線の曲がりが現れる現象です。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。

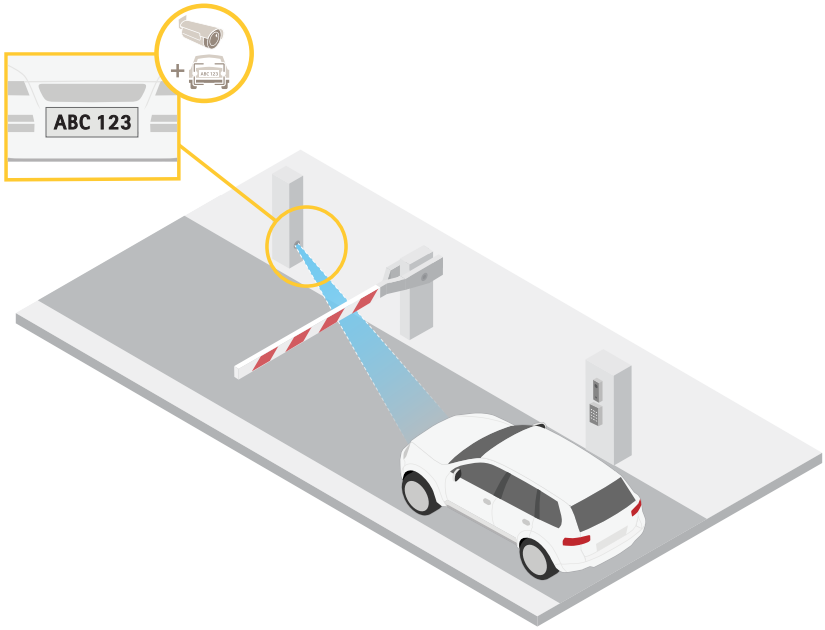
注

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



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

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、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 15*を参照してください。
3. 録画を停止するには、もう一度 ● をクリックします。

ビデオを見る

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

ビデオが改ざんされていないことを確認する

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

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

4. AXIS File Playerを使用してビデオを再生します。*AXIS File Playerをダウンロードします。*

   は、ビデオが改ざんされていないことを示しています。

注

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

イベントのルールを設定する

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

詳細については、「*イベントのルールの使用開始*」を参照してください。

アクションをトリガーする

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

注

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

カメラがナンバープレートを検知した場合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。

次の手順に従って、AXIS Licence Plate Verifierが動作していることを確認します。

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

ルールの作成:

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Application (アプリケーション)] の [ALPV.PlateInView] を選択します。

4. アクションのリストで、[Recordings (録画)] の [Record video while the rule is active (ルールがアクティブである間、ビデオを録画する)] を選択します。
5. ストレージオプションのリストで、[SD_DISK] を選択します。
6. カメラとストリームプロファイルを選択します。
7. プリバッファ時間を5秒に設定します。
8. ポストバッファ時間を [1 minute(1分)] に設定します。
9. [保存] をクリックします。

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

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。

ネットワークマイクロフォンに接続する

ネットワークマイクロフォンのペアリングにより、対応するAxisネットワークマイクロフォンを、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、マイクロフォンは周辺エリアからの音声を取り込み、音声入力装置として使用し、メディアストリームや録画で使用できます。

重要

この機能をビデオ管理ソフトウェア (VMS) とともに使用するには、まずカメラをネットワークマイクロフォンとペアリングしてからVMSに追加する必要があります。

カメラをネットワークマイクロフォンとペアリングする

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. [Microphone pairing (マイクロフォンのペアリング)] を選択します。
4. ネットワークマイクロフォンの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。

リストの管理

検知されたナンバープレートをリストに追加する

アプリケーションによって検知されたナンバープレートはリストに直接追加できます。

1. [Home (ホーム)] をクリックします。
2. [Live (ライブ)] に移動します。
3. リスト内の登録済みプレートの矢印アイコンをクリックします。
4. [Append plate to list (プレートをリストに追加する)] をクリックします。
5. ダイアログで、ナンバープレートを追加するリストを選択します。
6. [Append (追加)] をクリックします。

注

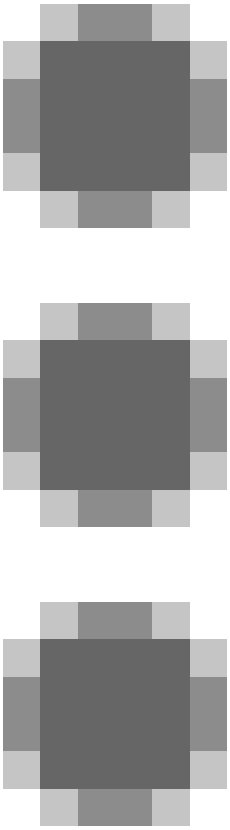
ナンバープレートと説明のどちらにも<, >と&の記号が使用されていないことを確認します。

ナンバープレートに説明を追加する

リストのナンバープレートに説明を追加する方法:

- [List management (リスト管理)] に移動します。

- ナンバープレートを選択し、



をクリックし、ドロップダウンメニューから [Edit (編集)] を選択します。
- 該当する情報を [Description (説明)] のフィールドに入力します。
- [保存] をクリックします。

注

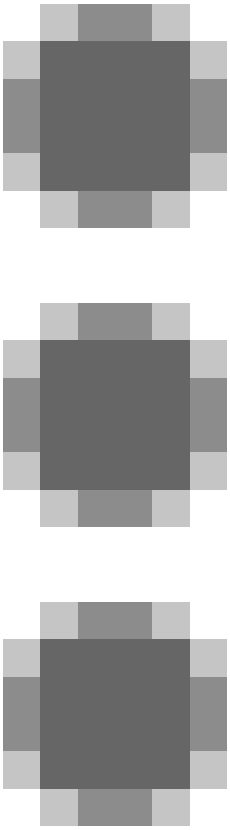
ナンバープレートと説明、どちらにも<、>、&の記号が使用されていないことを確認してください。

リスト名のカスタマイズ

特定の使用事例に合わせて、任意のリストの名前を変更できます。

1. [List management (リスト管理)] に移動します。

2. 変更するリストの横の



をクリックします。
3. [Edit (編集)] を選択します。
4. リストの名前を入力します。
5. [Submit (送信)] をクリックします。

新しいリスト名が既存のすべての設定で更新されます。

許可リストに含まれるナンバープレート番号をインポートする

コンピューター上の.csvファイルから、許可リストに含まれるライセンスプレート番号をインポートすることができます。ナンバープレート番号に加えて、番号ごとに.csvファイルにコメントを追加することもできます。

.csvファイルの構造は、次のようにする必要があります: `license plate,date,description`

例:
ナンバープレートのみ: `AXIS123`

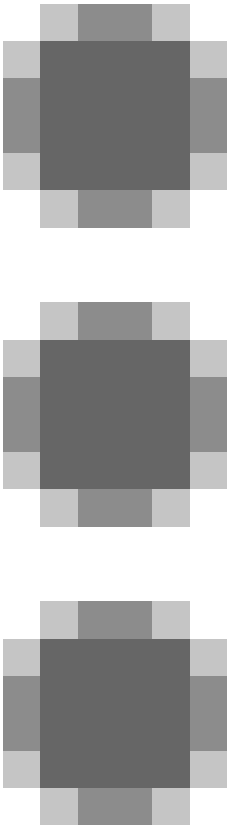
ナンバープレート + 説明: `AXIS123,,John Smith`

ナンバープレート + 日付 + 説明: `AXIS123,2022-06-08,John Smith`

注

ナンバープレートと説明、どちらにも<、>、&の記号が使用されていないことを確認してください。

1. [List management (リスト管理)] に移動します。
2. [Allowlist (許可リスト)] の横の



をクリックし、ドロップダウンメニューから [Import (インポート)] を選択します。
3. コンピューター上の.csvファイルに移動して選択します。
4. [OK] をクリックします。
5. [Allowlist (許可リスト)] に、インポートしたナンバープレート番号が表示されていることを確認します。

ナンバープレートリストを他のカメラと共有する

ネットワーク上でナンバープレートリストを他のカメラと共有することができます。同期すると、他のカメラにある現在のナンバープレートリストがすべて上書きされます。

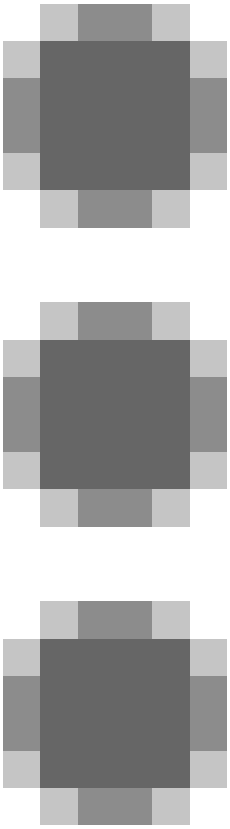
1. [List management (リスト管理)] > [List synchronization (リスト同期)] に移動します。
2. [Remote connected devices (リモート接続されたデバイス)] で、IPアドレス、ユーザー名、パスワードを入力します。

3. [追加] をクリックします。
4. [Synchronize list (リストを同期する)] をクリックします。
5. [Last sync (最後の同期)] の日付と時刻が適切に更新されていることを確認してください。

スケジュールリスト

リストは、特定の曜日の特定の時間帯にのみアクティブになるようにスケジュール設定することができます。リストをスケジュール設定する方法:

- [List management (リスト管理)] に移動します。
- 変更するリストの横の



をクリックします。
- ドロップダウンメニューで [Schedule (スケジュール)] を選択します。
- 開始時刻と終了時刻、リストをアクティブにする日を選択します。
- Enabled (有効化) の隣にあるボタンをクリックします。
- [保存] をクリックします。

追加設定

テキストオーバーレイの設定

テキストオーバーレイでは、ライブビューに次のイベント情報が表示されます: `weekday, month, time, year, license plate number`。

1. [Settings (設定)] > [Image (画像)] に移動します。
2. [Text overlay (テキストオーバーレイ)] を有効にします。
3. [Timestamp and license plate (タイムスタンプとナンバープレート)] または [License plate only (ナンバープレートのみ)] のいずれかを選択します。
4. [Overlay duration (オーバーレイ期間)] を1～9秒の値に設定します。
5. オーバーレイがライブビューに表示されていることを確認します。

低照度下でナンバープレートを検知する

検知のたびに、アルゴリズムによってスコアがつけられます。これは信頼閾値と呼ばれます。選択した感度よりスコアが低い検知は、イベントのリストに表示されません。

低照度のシーンでは、信頼閾値を低く設定することで、より多くのプレートを検知することが可能になります。

1. [Settings (設定)] > [Recognition (認識)] に移動します。
2. [Confidence threshold (信頼閾値)] でスライダーを調整します。
3. アルゴリズムが期待どおりにナンバープレートを検知することを確認します。

ナンバープレートで少ない文字数を許可する

このアプリケーションには、ナンバープレートを検知するときのデフォルトの最小文字数があります。デフォルトの最小文字数は5です。より少ない文字数でナンバープレートを検知するように、アプリケーションを設定できます。

1. [Settings (設定)] > [Recognition (認識)] に移動します。
2. [Number of characters (文字数)] で、スライダーを調整して許可する最小文字数を設定します。
3. アプリケーションが期待どおりにナンバープレートを検知することを確認します。

ナンバープレートの完全一致のみを許可する

マッチングアルゴリズムは、検知されたナンバープレートを許可リストやブロックリストと照合するとき、1文字の逸脱を自動的に許可します。しかし、シナリオによっては、ナンバープレートのすべての文字が完全に一致している必要があります。

1. [List management (リスト管理)] に移動します。
2. [Strict matching (厳密な一致)] をクリックして有効にします。
3. アプリケーションが期待どおりにナンバープレートを照合することを確認します。

ナンバープレートの照合時に複数の文字の逸脱を許可する

マッチングアルゴリズムは、検知されたナンバープレートを許可リストやブロックリストと照合するとき、1文字の逸脱を自動的に許可します。ただし、複数の文字の逸脱を許可することもできます。

1. [Settings (設定)] > [Recognition (認識)] に移動します。

2. [Allowed character deviation (許可される文字の逸脱)] で、異なることが許可される文字の数を選択します。
3. アプリケーションが期待どおりにナンバープレートを照合することを確認します。

オペレーターに制限付きアクセス権を付与する

オペレーターには、URLを介したアプリへの制限付きのアクセス権を付与することができます。これにより、イベントログとリスト管理のみへのアクセスが可能になります。このURLは、[Settings > User rights (設定 > ユーザー権限)] で確認できます。

安全な接続を設定する

カメラとドアコントローラーとの間など、デバイス間の通信とデータを保護するために、証明書を使用してHTTPSによる安全な接続を設定します。

1. [Settings (設定)] > [Security (セキュリティ)] に移動します。
2. HTTPSで、[Self-signed (自己署名)] または [CA-signed (CA署名)] のいずれかを選択します。

注

HTTPSの詳細と使用方法については、 で確認できます。

アプリ設定のバックアップとリストア

画像取り込み、セキュリティ、検出、統合に関連するアプリで行った設定のバックアップとリストア (復元) ができます。問題の発生時にも、バックアップした設定を復元することができます。

アプリの設定をバックアップする方法:

- [Settings > Maintenance (設定 > メンテナンス)] に移動します。
- [Download backup configuration (バックアップの設定をダウンロードする)] をクリックします。

JSONファイルがダウンロードフォルダにダウンロードされます。

アプリの設定をリストアする方法:

- [Settings > Maintenance (設定 > メンテナンス)] に移動します。
- [Restore configuration (設定のリストア)] をクリックします。

バックアップを含むJSONファイルを選択します。

設定が自動的に復元されます。

すべてのイベントをクリアする

アプリを設定した後は、設定時の画像や取得したプレートの記録を消去しておくことを推奨します。

データベースからすべての画像とプレートを消去する方法:

[Settings > Maintenance (設定 > メンテナンス)] に移動します。

- [すべての認識結果のクリア] をクリックします。
- [Yes (はい)] をクリックします。

仮想ポートを使用したアクションのトリガー

仮想ポートをアクセスコントロールと組み合わせて使用して、任意の種類のアクションをトリガーできます。この例では、仮想ポートとカメラのI/Oポートを使用してテキストオーバーレイを表示するように、AXIS License Plate Verifierを設定する方法について説明します。

要件:

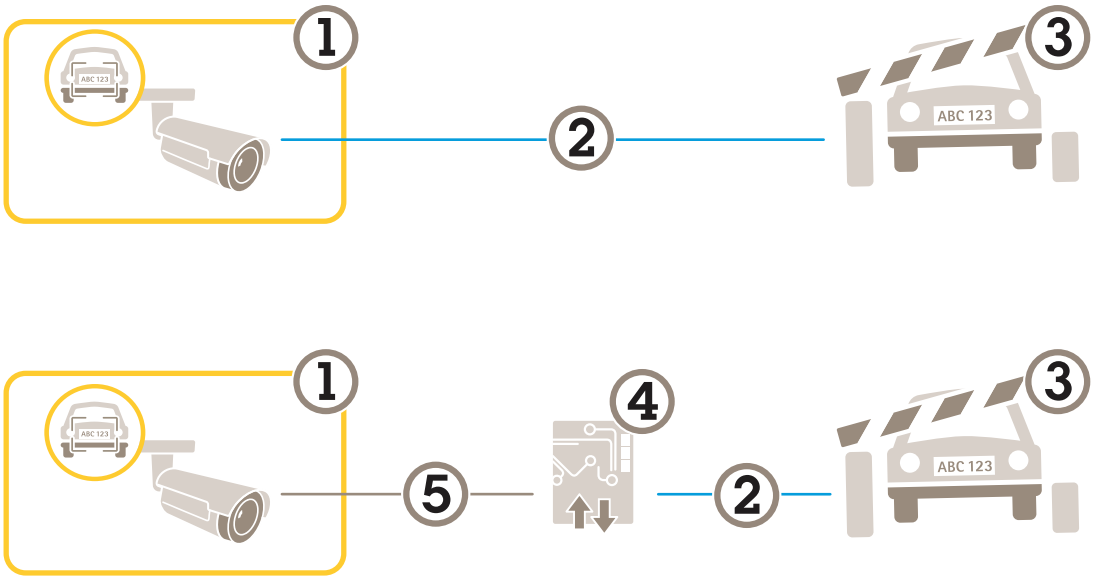
- カメラがネットワークに物理的に設置および接続されている。
- カメラでAXIS License Plate Verifierが起動され実行されている。
- ゲートとカメラのI/Oポートの間にケーブルが接続されている。
- 基本的な設定が終了している。を参照してください。

1. アプリケーションのWebページに移動し、[Settings] (設定) タブを選択します。
2. [Access control (アクセスコントロール)] に移動します。
3. [Access control (アクセスコントロール)] で、[Internal I/O (内部I/O)] を選択します。
4. [I/O output # (I/O出力番号)] を選択します。
5. [Virtual port (仮想ポート)] ドロップダウンリストでポートを選択します。
6. [Barrier mode (バリアモード)] で、[Open to all (すべてに開放)] を選択します。
7. [Vehicle direction (車両の進行方向)] で、[Any (指定なし)] を選択します。
8. 使用する [Area of interest (対象範囲)] を選択します。
9. カメラのWebページで、[System (システム)] > [Events (イベント)] に移動します。
10. [Add rule (ルールの追加)] をクリックします。
11. [Condition (条件)] で、[Virtual input is active (仮想入力がアクティブ)]、指定したポート番号を選択します。
12. [Action (アクション)] 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。
13. [Video channels (ビデオチャンネル)] を選択します。
14. 表示するテキストを入力します。
15. テキストの継続時間を追加します。
16. [保存] をクリックします。
17. [Video (ビデオ)] > [Overlays (オーバーレイ)] に移動します。
18. [Overlays (オーバーレイ)] に移動します。
19. ドロップダウンメニューで [Text (テキスト)] を選択し、[+] をクリックします。
20. 「#D」と入力するか、[Modifiers (修飾子)] ドロップダウンリストで修飾子を選択します。
21. ライブビューで車両が関心領域に入ると、テキストオーバーレイが表示されることを確認します。

車両の入出庫のシナリオ

車両の入出庫のシナリオでは、アプリケーションはカメラにキャプチャーされた車両のナンバープレートを読み取り、カメラに保存されている許可されたナンバープレート番号のリスト、または許可されていないもののリストに照らしてナンバープレートを検証します。

このシナリオでは、ゲートを開閉するためにI/O機能をサポートしているカメラ、あるいはI/Oリレーモジュールと組み合わせて、カメラにアプリケーションをインストールすることが必要です。



車両の入出庫のシナリオで可能な2つの設定。

1. *AXIS License Plate Verifierが搭載されたAxisカメラ*
2. *I/O通信*
3. *ゲート*
4. *Axis I/Oリレーモジュール*
5. *IP通信*

既知の車両の場合に、リレーモジュールを使用してゲートを開く

この使用事例では、AXIS License Plate Verifier をリレーモジュールと共に設定して、特定の関心領域 (ROI) を通過して駐車場などに入っていく既知の車両に対してゲートを開く方法を説明します。

要件:

- カメラがネットワークに物理的に設置および接続されている。
- カメラでAXIS License Plate Verifierが起動され実行されている。
- バリアとリレーモジュールの間にケーブルが接続されている。
- 基本的な設定が終了している。*基本設定, on page 4*を参照してください。

1. カメラのWebページに移動し、**[Settings] (設定)** を選択してAXIS License Plate Verifierを開きます。
2. リレーモジュールのWebページに移動し、リレーポートがカメラのI/Oポートに接続されていることを確認します。
3. リレーモジュールのIPアドレスをコピーします。
4. AXIS License Plate Verifierに戻ります。
5. [**Settings (設定)**] > [**Access control (アクセスコントロール)**] に移動します。
6. [**Type (タイプ)**] に移動し、ドロップダウンリストで [**Type (リレー)**] を選択します。
7. [**I/O output (I/O出力)**] ドロップダウンリストで、バリアに接続されているI/Oポートを選択します。

8. [Barrier mode (ゲートモード)] ドロップダウンリストで [Open from lists (リストから開く)] を選択し、[Allowlist (許可リスト)] をオンにします。
9. [Vehicle direction] (車両の方向) ドロップダウンリストから [in] (入庫) を選択します。
10. [ROI] ドロップダウンリストから、目的の車線をカバーする対象範囲を選択します。
11. 以下の情報を入力します。
    - リレーモジュールのIPアドレスを`192.168.0.0`の形式で入力
    - リレーモジュールのユーザー名
    - リレーモジュールのパスワード
12. 接続が機能することを確認し、[Connect] (接続) をクリックします。
13. 接続をアクティブにするには、[Turn on integration (統合を有効にする)] をクリックします。
14. [List management (リスト管理)] タブに移動します。
15. [Allowlist (許可リスト)] フィールドにナンバープレート番号を入力します。

注

リレーモジュール上の物理的な入力ポート1～8が、ドロップダウンリストのポート1～8に対応します。ただし、リレーモジュール上のリレーポート1～8は、ドロップダウンリストのポート9～16に対応します。これは、リレーモジュールにポートが8個しかない場合も同じです。

16. アプリケーションが、許可リストに含まれるナンバープレート番号を既知の車両として識別し、ゲートが正常に開くことを確認してください。

既知の車両の場合に、カメラのI/Oを使用してゲートを開く

この例では、既知の車両が駐車場に入るような場合に、カメラのI/Oポートを使用してゲートを開くようにAXIS License Plate Verifierを設定する方法について説明します。

要件:

- カメラがネットワークに物理的に設置および接続されている。
- カメラでAXIS License Plate Verifierが起動され実行されている。
- ゲートとカメラのI/Oポートの間にケーブルが接続されている。
- 基本的な設定が終了している。を参照してください。

1. アプリケーションのWebページに移動し、[Home (ホーム)] に移動して、検知されたナンバープレートをリストに追加します。「*検知されたナンバープレートをリストに追加する, on page 19*」を参照してください。
2. リストを直接編集するには、[List management (リスト管理)] に移動します。
3. [Allowlist (許可リスト)] フィールドに許可されたナンバープレート番号を入力します。
4. [Settings (設定)] に移動します。
5. [Access control (アクセスコントロール)] で、[Internal I/O (内部I/O)] を選択します。
6. [I/O output # (I/O出力番号)] を選択します。
7. [Barrier mode (バリアモード)] で、[Open from lists (リストから開く)] を選択し、[Allowlist (許可リスト)] を確認します。
8. [Vehicle direction] (車両の方向) ドロップダウンリストから [in] (入庫) を選択します。
9. [Area of interest (対象範囲)] で、使用する対象範囲を選択するか、すべての対象範囲を使用するかを選択します。
10. アプリケーションが、許可リストに含まれるナンバープレート番号を既知の車両として識別し、ゲートが正常に開くことを確認してください。

注

特定の使用事例に合わせて、任意のリストの名前を変更できます。

許可されていない車両に関する通知を受け取る

この例では、カメラで通知をトリガーするイベントを作成できるように、アプリケーションを設定する方法について説明します。

要件:

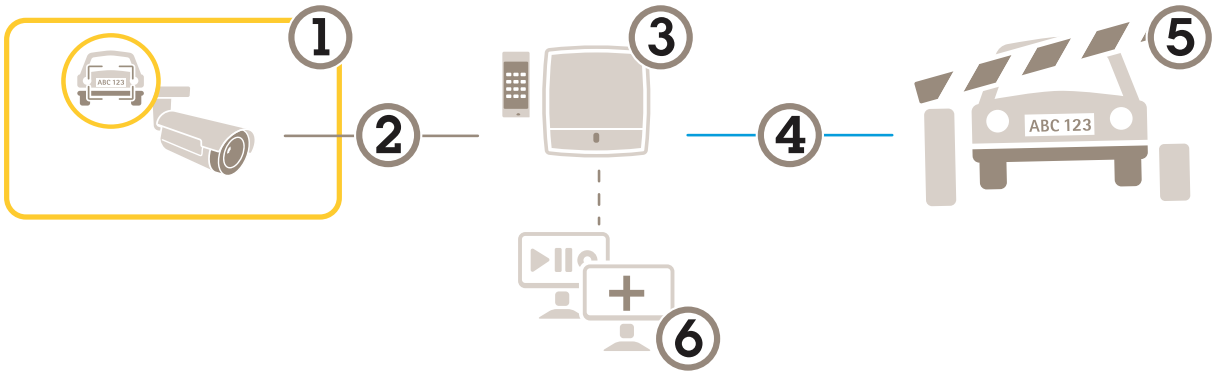
- 基本的な設定が終了している。*基本設定, on page 4*を参照してください。

1. [List management (リスト管理)] に移動します。
2. [Blocklist (ブロックリスト)] フィールドにナンバープレート番号を入力します。
3. カメラのWebページに移動します。
4. [Settings (設定)] > [Events (イベント)] に移動し、アプリケーションを条件とし、通知をアクションとするアクションルールを設定します。
5. アプリケーションが、追加されたナンバープレート番号を許可されていない車両として識別し、アクションルールが正常に実行されることを確認してください。

車両アクセスコントロールのシナリオ

車両のアクセスコントロールのシナリオでは、アプリケーションをAxisネットワークドアコントローラーに接続して、アクセスルールを設定し、アクセス時間のスケジュールを作成し、従業員だけでなく訪問者やサプライヤーの車両アクセスも処理することができます。

バックアップ用に、ドアコントローラーとカードリーダーを含むアクセスシステムを使用します。ドアコントローラーとカードリーダーを設定する方法については、*axis.com*にあるユーザードキュメントを参照してください。



1 AXIS License Plate Verifierが搭載されたAxisカメラ
2 IP通信
3 カードリーダーを備えたAxisネットワークドアコントローラー
4 I/O通信
5 ゲート
6 オプションのサードパーティ製ソフトウェア

ドアコントローラーに接続する

この例では、カメラをネットワークドアコントローラーに接続します。つまり、カメラがセンサーとして機能します。カメラはコントローラーに情報を転送し、コントローラーは情報を分析し、イベントをトリガーします。

注

AXIS License Plate VerifierとAXIS Entry Managerを切り替えたときは、すべてのパラメーターにアクセスできるように必ずWebページを更新してください。

要件:

- カメラとドアコントローラーが物理的に設置され、ネットワークに接続されている。
- カメラでAXIS License Plate Verifierが起動され実行されている。
- 基本的な設定が終了している。*基本設定, on page 4*を参照してください。

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

AXIS A1001 Door Controllerでこのアプリケーションを起動して実行する方法。

AXIS Entry Managerでのハードウェアの設定

1. AXIS Entry Managerに移動し、**[Setup] (設定)** で新しいハードウェア設定を開始します。
2. ハードウェアの設定で、ネットワークドアコントローラーの名前を「ゲート ローラー」に変更します。
3. **[Next (次へ)]** をクリックします。

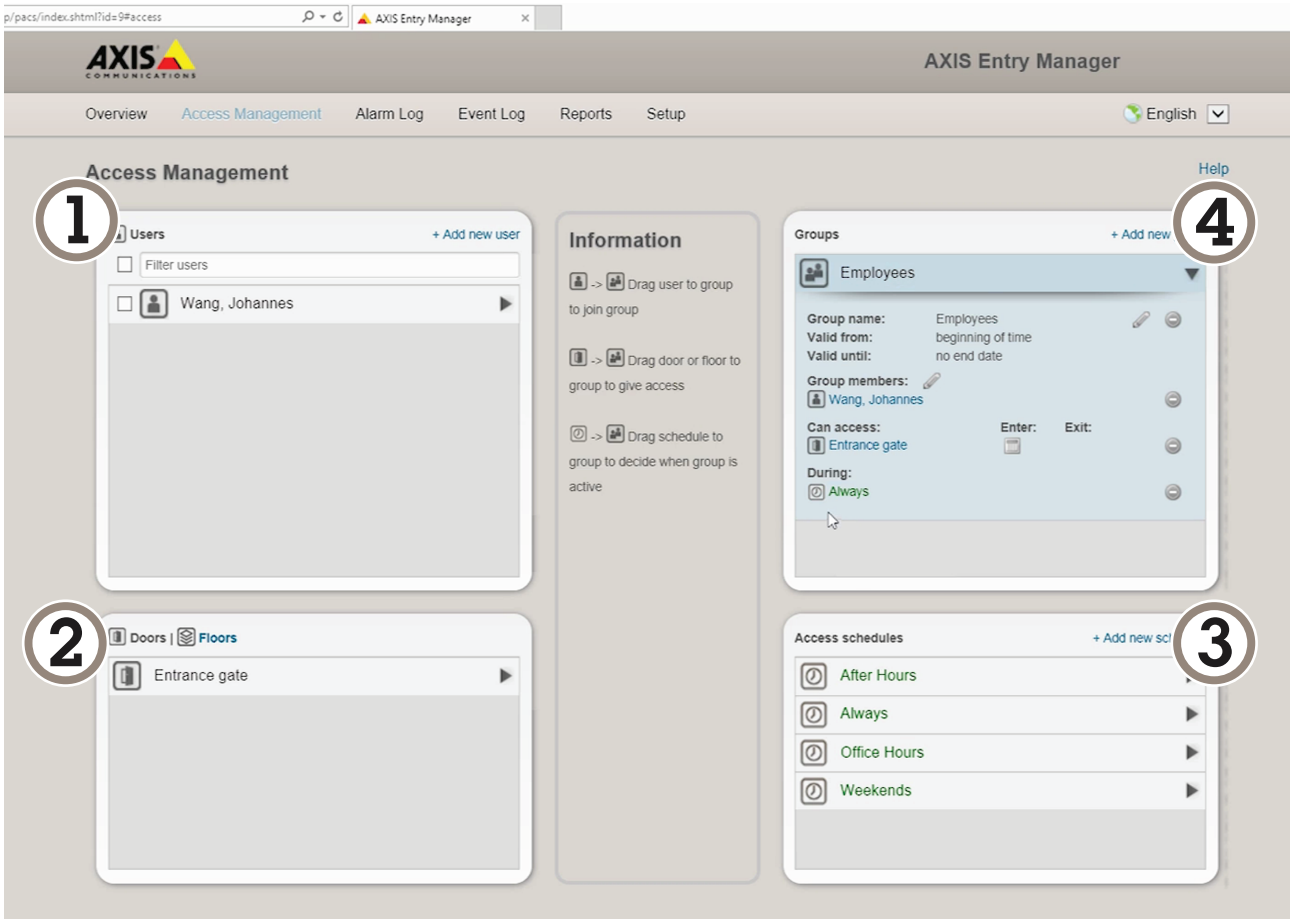
4. [Configure locks connected to this controller] (このコントローラーに接続されているロックを設定する) で、[Door monitor] (ドアモニター) オプションをクリアします。
5. [Next (次へ)] をクリックします。
6. [Configure readers connected to this controller] (このコントローラーに接続されているリーダーを設定する) で、[Exit reader] (外部リーダー) オプションをクリアします。
7. Finish (終了) をクリックします。

Configuration in AXIS License Plate Verifierでの設定

1. AXIS License Plate VerifierのWebページに移動します。
2. [Settings (設定)] > [Access control (アクセスコントロール)] に移動します。
3. [Type (タイプ)] に移動し、ドロップダウンリストで [Controller (コントローラー)] を選択します。
4. 以下の情報を入力します。
   - コントローラーのIPアドレスを`192.168.0.0`の形式で入力
   - コントローラーのユーザー名
   - コントローラーのパスワード
5. [接続] をクリックします。
6. 接続が成功した場合は、[Network Door Controller name] (ネットワークドアコントローラー名) ドロップダウンリストに "Gatecontroller" が表示されます。[Gatecontroller] を選択します。
7. [Reader name (リーダー名)] ドロップダウンリストで、ドア"Gatecontroller"に接続されているリーダーを選択します ("Reader entrance"など)。これらの名前は、AXIS Entry Managerで変更できます。
8. 接続をアクティブにするには、[Turn on integration (統合を有効にする)] を選択します。
9. ユーザーのナンバープレート番号の1つを入力するか、デフォルトを使用し、[Test integration (統合をテスト)] をクリックします。テストが成功したことを確認します。

AXIS Entry Managerで、ユーザー、グループ、ドア、およびスケジュールを設定する

1. Go to AXIS Entry Managerに移動します。
2. [Access Management] (アクセス管理) に移動します。
3. [Doors > Add identification type] (ドア > 識別タイプを追加) に移動します。
4. [Credentials needed] (必要な認証情報) ドロップダウンリストで、[License plate only] (ナンバープレートのみ) を選択します。
5. 識別タイプを使用できる時期に制限を設定するには、[Schedule] (スケジュール) をドアにドラッグアンドドロップします。
6. ユーザーを追加し、ユーザーごとに認証情報の [License plate] (ナンバープレート) を追加します。
7. 再度 [Add credential] (認証情報を追加) クリックし、ナンバープレート情報を入力します。
8. [Add new group] (新しいグループを追加) をクリックし、情報を入力します。
9. ユーザーをグループに追加するには、[Users (ユーザー)] をユーザーグループにドラッグアンドドロップします。
10. ユーザーにアクセス権を付与するには、[Door] (ドア) をユーザーグループにドラッグアンドドロップします。
11. アクセス時間を制限するには、[Schedule] (スケジュール) をユーザーグループにドラッグアンドドロップします。



AXIS Entry Managerのユーザーインターフェースの概要。

1 ユーザー
2 ドア
3 スケジュール
4 ユーザーグループ

AXIS Secure Entryへの接続

この例では、AXIS Licence Plate Verifierを使用して、AXIS Camera Station内のAxisドアコントローラーとAXIS Secure Entryを接続する方法について説明します。

要件:

- カメラとドアコントローラーが物理的に設置され、ネットワークに接続されている。
- カメラでAXIS License Plate Verifierが起動され実行されている。
- AXIS Camera Stationクライアントバージョン5.49.449以上。
- 基本的な設定が終了している。*基本設定, on page 4*を参照してください。

AXIS Camera Stationで、「*リーダーの追加*」を参照してください。

AXIS License Plate Verifierアプリで、次の操作を行います。

1. [Settings (設定)] タブで、[Configuration wizard (設定ウィザード)] に移動し、[Start (開始)] をクリックします。
2. [Access Control (アクセスコントロール)] を選択します。
3. [Secure Entry] を選択し、[Next (次へ)] をクリックします。

AXIS Camera Stationで、以下の手順に従います。

4. [AXIS Camera Station>Configuration>Other Devices (AXIS Camera Station>設定>その他の装置)] の装置リストに表示されるドアコントローラーのIPアドレスを入力します。

5. 認証キーを追加するには、[AXIS Camera Station>Configuration>Encrypted communication (AXIS Camera Station>設定>暗号化通信)] に移動します。
6. [External Peripheral Authentication Key (外部周辺機器認証キー)] に移動し、[Show authentication key (認証キーの表示)] をクリックします。
7. [Copy key (キーのコピー)] をクリックします。

AXIS License Plate Verifierアプリで、次の操作を行います。

8. 設定ウィザードの [Authentication key (認証キー)] に移動し、キーを貼り付けます。
9. [接続] をクリックします。
10. ドロップダウンメニューで、[Door controller name (ドアコントローラー名)] を選択します。
11. ドロップダウンメニューで、[Reader name (リーダー名)] を選択します。
12. [Turn on integration (統合を有効にする)] をオンにします。
13. [Next (次へ)] をクリックします。
14. 対象範囲を調整します。「*対象範囲を調整する, on page 8*」を参照してください。
15. [Next (次へ)] を2回クリックし、[Finish (完了)] をクリックします。

速度測定によるフリーフローシナリオ

速度測定によるフリーフローシナリオでは、カメラはエッジツーエッジテクノロジーによってAxisレーダーとペアリングされます。カメラは2車線をカバーし、通過車両のナンバープレートを読み取り、ペアリングされたレーダーも同じ2車線をカバーし、車両の速度を測定します。さらに、*AXIS Speed Monitor*アプリケーションは、カメラのライブビューのオーバーレイを介して各車線の最高速度を表示できます。

エッジツーエッジの詳細については、*エッジツーエッジ技術, on page 43*を参照してください。

要件:

- AXIS License Plate Verifierカメラキットと*AXIS D2210-VE Radar*がインストールされ、ネットワークに接続されていること。

シナリオを設定する

4つのステップでシナリオを設定します。まずカメラを設定し、次にレーダーをペアリングおよび設定して、最後にAXIS Speed Monitorを使ってオーバーレイを追加します。

開始する前に、以下をご確認ください。

- カメラとレーダーが同じ対象範囲に向けられていることを確認します。
- カメラとレーダーの時刻が同期していることを確認します。ステータスを確認するには、各装置の [**Installation > Time sync status (インストール > 時刻同期ステータス)**] に移動します。
- ペアリング後にレーダーがカメラの2番目のビューエリア (**View area 2 (ビューエリア2)**) を使用するため、そのビューエリアが使用されていないことを確認してください。

カメラを設定する:

1. *基本設定, on page 4*の手順に従ってカメラを設定します。
2. 設定アシスタントに従うときは、必ずフリーフローを選択してください。詳細については、*フリーフロー, on page 6*を参照してください。

カメラをレーダーとペアリングする:

1. カメラのwebインターフェースで、[**System > Edge-to-edge > Radar pairing (システム > エッジツーエッジ > レーダーペアリング)**] に移動します。
2. レーダーのホスト名、ユーザー名、パスワードを入力します。
3. [**Connect (接続)**] をクリックして装置をペアリングします。
   接続が確立されると、カメラのwebインターフェースでレーダーの設定を利用できます。

注

ペアリングされたレーダーのデフォルトの解像度は1280x720です。レーダーをVMSに追加する場合、カメラのwebインターフェースでレーダーのデフォルト解像度を維持します。

レーダーの設定:

1. カメラのwebインターフェースで、[**Radar > Scenarios (レーダー > シナリオ)**] に移動します。
2. 片方の車線をカバーするレーダーシナリオと、もう片方の車線をカバーするレーダーシナリオを追加します。
3. どちらのシナリオでも、[**Movement in area (エリアへの侵入)**] を選択し、[**Vehicles (車両)**] をトリガーして [**Speed limit (制限速度)**] を設定します。
   詳細については、*AXIS D2210-VE* Radarユーザーマニュアルのシナリオを追加するを参照してください。

注

AXIS License Plate Verifierからのナンバープレート情報を含むオーバーレイを追加する場合は、AXIS Speed Monitorでオーバーレイを追加する前に、これらのオーバーレイを追加してください。

以下の手順に従って、AXIS Speed Monitorを使用して、速度オーバーレイを追加します。

1. AXIS Speed Monitorをカメラにダウンロードしてインストールします。
2. 各車線に1つのオーバーレイを追加すると、カメラのライブビューで最大速度が表示されます。
   インストールと設定の手順については、*AXIS Speed Monitorユーザーマニュアル*を参照してください。

特定のイベントの検索

複数の条件を使用してイベントを検索するには、検索機能を使用します。

1. アプリケーションのWebページに移動し、[Search (検索)] ページを選択します。
2. [From (開始)] および [To (終了)] カレンダーメニューで日付を選択し ます。
3. [AOI] のドロップダウンメニューをクリックし、検索対象範囲を選択します。
4. [Direction (方向)] を選択して、入場または退出でフィルターします。
5. ナンバープレートを検索する場合は、[Plate (ナンバープレート)] フィールドにナンバープレートを入力します。
6. 特定の国に属するナンバープレートを検索するには、[Country (国)] のドロップダウンリストから国を選択します。
7. 車両のビューに基づいて画像を絞り込むには、[Vehicle view] のドロップダウンリストから [Front (前)] または [Rear (後)] を選択します。
8. 車両のメーカー、モデル、タイプ、またはカラーに基づいて検索結果を絞り込むには、[Vehicle details (車両の詳細)] のドロップダウンメニューから該当項目を選択します。
9. [Apply filters (フィルターを適用する)] をクリックし、検索結果を表示します。

検索結果のエクスポートと共有

検索結果を、その時点での統計情報と共にCSVファイルとしてエクスポートするには、[Export (エクスポート)] をクリックして結果をcsvファイルとして保存します。

サードパーティシステムにデータをエクスポートするためのリンクとしてAPIをコピーするには、[Copy search link (検索リンクをコピー)] をクリックします。

統合

プロファイルを使用して、複数のサーバーにイベントをプッシュする

プロファイルを使用すると、異なるプロトコルを使用する異なるサーバーに、同時にイベントをプッシュすることができます。プロファイルを使用する方法:

1. [Integration (統合)] および [Push events (イベントのプッシュ)] ページに移動します。
2. [Profile 1 (プロファイル1)] を選択します。
3. ルールを設定します。*サードパーティ製ソフトウェアへのイベント情報のプッシュ, on page 37*を参照してください。
4. ルールをテストします。
5. 新しいプロファイルのタブを選択し、新しいルールを設定します。

サードパーティ製ソフトウェアへのイベント情報のプッシュ

注

アプリケーションは、JSON形式でイベント情報を送信します。詳細については、*MyAxisアカウントを使用してログインし*、*AXIS VAPIXライブラリに*移動して、AXIS License Plate Verifierを選択してください。

この機能を使用すると、TCPまたはHTTP POSTでイベントデータをプッシュして、サードパーティ製ソフトウェアを統合することができます。

開始する前に、以下をご確認ください。

- カメラはネットワークに物理的に設置および接続されている必要があります。
- カメラでAXIS License Plate Verifierが起動されて実行されている必要があります。

1. [Integration (統合)] > [Push events (イベントのプッシュ)] に移動します。
2. 空のプロファイルを選択します。
3. [Protocol (プロトコル)] ドロップダウンリストで、[HTTP POST] を選択します。
4. [Server URL (サーバーのURL)] フィールドに、次の形式でサーバーのアドレスとポートを入力します: `127.0.0.1:8080`
5. ユーザー名とパスワードを入力します。
6. プロキシーを使用している場合は、プロキシーをオンにし、ホスト名、ユーザー名、パスワードを入力します。
7. [Device ID (デバイスID)] フィールドに装置の名前を入力するか、そのままにします。
8. [Push conditions (プッシュ条件)] でプッシュイベントをトリガーする方向を選択します。
9. [LPR Event types (LPRイベントタイプ)] で、以下のオプションから1つ以上選択します。
   - [New (新規)] は、ナンバープレートが初めて検知されたことを意味します。
   - [Update (更新)] は、以前に検知されたナンバープレートの文字を修正する場合と、プレートの移動に伴って方向が検知され、画像上で追跡される場合のどちらかです。
   - [Lost (消失)] は、ナンバープレートが画像から出る前の最後の追跡イベントです。これには、ナンバープレートの方向も含まれます。
   - [Conditional (条件付き)] は、条件が満たされた場合に、1つのオブジェクトに対して1つのイベントをプッシュします。
10. HTTP POSTを使用する際に帯域幅を削減するには、[Do not to send images (画像を送信しない)] を選択します。
11. [Event buffer (イベントバッファ)] を有効にし、サーバーがダウンした場合にイベントをバッファリングしてサーバーが利用可能になったら送信するようにします。

12. [Retention settings (保持設定)] で選択している場合、画像に加えてナンバープレートの切り取り画像を含めるには、[Send two images (2つの画像を送信)] を選択します。
13. Base64形式ではなくmulitpart形式でイベントを送信するには、[Multipart] を選択します。
14. [Test (テスト)] をクリックし、仮想ナンバープレートを使用して統合テストを行います。
15. この機能をオンにするには、[Activate (オンにする)] を選択します。

注

HTTP POSTを使用してイベントをプッシュするには、ユーザー名とパスワードの代わりに認証ヘッダーを使用し、[Auth-Header (認証ヘッダー)] に移動し、認証APIへのパスを追加します。

サーバーへのナンバープレートの画像の送信

この機能を使用すると、FTPを介してナンバープレートの画像をサーバーにプッシュできます。

開始する前に、以下をご確認ください。

- カメラはネットワークに物理的に設置および接続されている必要があります。
- カメラでAXIS License Plate Verifierが起動されて実行されている必要があります。

1. [Integration (統合)] > [Push events (イベントのプッシュ)] に移動します。
2. [Protocol (プロトコル)] ドロップダウンリストで、[FTP] を選択します。
3. [Server URL (サーバーのURL)] フィールドに、以下の形式でサーバーのアドレスを入力します: `ftp://10.21.65.77/LPR`
4. FTPサーバーのユーザー名とパスワードを入力します。
5. ファイル名のパスと名前の修飾子を選択します。
6. [Device ID (デバイスID)] フィールドにデバイスの名前を入力します。この名前のフォルダーが画像用に作成されます。画像は次の形式で作成されます: timestamp_area of interest_direction_carID_license plate text_country.jpg
7. [Push conditions (プッシュ条件)] でプッシュイベントをトリガーする方向を選択します。
8. [Event types (イベントタイプ)] で、以下のオプションから1つ以上選択します。
   - [New (新規)] は、ナンバープレートが初めて検知されたことを意味します。
   - [Update (更新)] は、以前に検知されたナンバープレートの文字を修正する場合と、プレートの移動に伴って方向が検知され、画像上で追跡される場合のどちらかです。
   - [Lost (消失)] は、ナンバープレートが画像から出る前の最後の追跡イベントです。これには、ナンバープレートの方向も含まれます。
   - [Conditional (条件付き)] は、条件が満たされた場合に、1つのオブジェクトに対して1つのイベントをプッシュします。

   注

   [Lost (消失)] または [Update (更新)] が選択されている場合、方向はファイル名にのみ含まれます。
9. [Test (テスト)] をクリックし、仮想ナンバープレートを使用して統合テストを行います。
10. この機能をオンにするには、[Activate (オンにする)] をクリックします。

注

選択したキャプチャーモードのタイプによって画像が異なることに注意してください (*画像キャプチャーの設定を調整する, on page 9*を参照してください)。

注

プッシュイベントが失敗した場合、アプリは失敗した最初の100件までをサーバーに再送信します。

Windowsサーバーへのプッシュイベントで FTPを使用する場合、画像の名前に日付と時刻を示す「%c」を使用しないでください。これは、Windowsが日付と時刻に対して関数「%c」で設定された名前を許容していないためです。 Linuxサーバーを使用する場合には、この問題は発生しません。

2Nとの直接統合

この例では、2N IP装置との直接統合について説明します。

2Nデバイスで、次のようにアカウントを設定します。

1. 2N IP Versoに移動します。
2. [Services (サービス)] > [HTTP API] > [Account 1 (アカウント1)] に移動します。
3. [Enable account (アカウントを有効にする)] を選択します。
4. [Camera access (カメラアクセス)] を選択します。
5. [License plate recognition (ナンバープレート認識)] を選択します。
6. IPアドレスをコピーします。

AXIS License Plate Verifierアプリで、次の操作を行います。

1. [Integration (統合)] > [Direct integration (直接統合)] に移動します
2. [2N IP Device] を選択します。
3. IPアドレスまたはURLを2Nデバイスに追加します。
4. ユーザー名とパスワードを入力します。
5. [Connection type (接続タイプ)] を選択します。
6. [Barrier is used for (ゲートの使用目的)] で該当する目的を選択します。
7. [Enable integration (統合を有効にする)] をクリックします。
8. 車両の進行方向を選択します。
9. この機能をオンにするには、[Activate (オンにする)] を選択します。

統合が機能していることを確認するには、次の操作を行います。

1. 2N IP Versoに移動します。
2. [Status (ステータス)] > [Events (イベント)] に移動します。

Genetec Security Centerとの統合

この例では、Genetec Security Centerとの直接統合の設定について説明します。

Genetec Security Centerで、次の操作を行います。

1. [Overview (概要)] に移動します。
2. Database (データベース)、Directory (ディレクトリ)、License (ライセンス) がオンラインであることを確認します。オンラインでない場合は、WindowsですべてのGenetecサービスとSQLEXPRESSサービスを実行します。
3. [Genetec Config Tool] > [Plugins (プラグイン)] に移動します。
4. [Add an entity (エンティティの追加)] をクリックします。
5. [Plugin (プラグイン)] に移動し、[LPR plugin (LPRプラグイン)] を選択します。
6. [Next (次へ)] をクリックします。
7. [Next (次へ)] をクリックします。
8. [Next (次へ)] をクリックします。
9. 追加したLPRプラグインを選択し、[Data sources (データソース)] に移動します。

[ALPR reads API] で、次の操作を行います。

10. [Enabled (有効)] チェックボックスをオンにします。
11. [Name (名前)] に、次のように入力します。Plugin REST API。
12. [API path prefix (APIパスのプレフィックス)] に、次のように入力します: lpr。
13. [REST port (RESTポート)] で、[443] を選択します。
14. [WebSDK host (WebSDKホスト)] に、次のように入力します: localhost。
15. [WebSDK port (WebSDKポート)] で、[443] を選択します。
16. [Allow self-signed certificates (自己署名証明書を許可する)] チェックボックスをオンにします。

[Security Center events data source (Security Centerイベントデータソース)] で、次の操作を行います。

17. [Enabled (有効)] チェックボックスをオンにします。
18. [Name (名前)] に、「Security Center Lpr Events」と入力します。
19. [Processing frequency (処理頻度)] で、ドロップダウンメニューから [5 sec (5秒)] を選択します。
20. [Data sinks (データシンク)] タブに移動します。
21. [+] をクリックします。
22. [Type (タイプ)] で [Database (データベース)] を選択します。
23. データベースを選択し、次のように設定します。
    - [Enabled (有効)] チェックボックスをオンにします。
    - [Source (ソース)] で、[Plugin REST API] と [Native ALPR Events (ネイティブALPRイベント)] チェックボックスをオンにします。
    - [Name (名前)] に、「Reads DB」と入力します。
    - [Include (含める)] で、[Reads]、[Hits]、[Images] チェックボックスをオンにします。
    - [Resources (リソース)] タブに移動します。
    - [Delete the database (データベースの削除)] をクリックした後、[Create a database (データベースの作成)] をクリックします。

Create an API user (APIユーザーの作成):

24. [Config Tool] > [User Management (ユーザー管理)] に移動します。
25. [Add an entity (エンティティの追加)] をクリックします。
26. [User (ユーザー)] を選択します。
27. ユーザー名とパスワードを入力します。他のフィールドは変更しないでください。
28. 追加したユーザーを選択し、[Privileges (権限)] タブに移動します。
29. [Application privileges (アプリケーション権限)] で、すべてを許可するチェックボックスをオンにします。
30. Third-party ALPR reads API (サードパーティ製ALPR reads API) を許可するチェックボックスをオンにします。
31. [適用] をクリックします。

AXIS License Plate Verifierアプリで、次の操作を行います。

1. [Integration (統合)] > [Direct integration (直接統合)] に移動します。
2. [Genetec Security Center] を選択します。
3. [URL/IP] に、このテンプレートに従ってアドレスを入力します: `https://server-address/api/V1/lpr/lpringestion/reads`。

4. Genetecのユーザー名とパスワードを入力します。
5. [**Connection type (接続タイプ)**] を選択します。
6. この機能をオンにするには、[**Activate (オンにする)**] を選択します。
7. [**Test (テスト)**] をクリックし、仮想ナンバープレートを使用して統合テストを行います。
8. HTTPSを選択している場合は、[**Settings (設定)**] タブに移動します。
9. [**Security (セキュリティ)**] > [**HTTPS**] で、次の操作を行います。
10. Genetec Security Centerの設定に応じて、[**Self-signed (自己署名)**] または [**CA-signed (CA署名)**] を選択します。

Genetec Security Centerで、次の操作を行います。

1. [**Genetec Security desk**] に移動します
2. [**Investigation (調査)**] で、[**Reads (読み取り)**] をクリックします。
3. [**Reads (読み取り)**] タブに移動します。
4. ニーズに合わせて結果をフィルター処理します。
5. [**レポートを生成する**] をクリックします。

注

Genetecのサードパーティ製ALPRプラグインの統合に関するドキュメントも読むことができます。*この操作は、ここで行います (登録が必要)。*

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

エッジツーエッジ技術

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

注

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

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

スピーカーのペアリング

エッジツーエッジのスピーカーペアリングにより、対応するAxisネットワークスピーカーをカメラの一部であるかのように使用できます。ペアリングすると、スピーカーの機能はカメラのwebインターフェースに統合され、ネットワークスピーカーは音声出力装置として機能し、音声クリップを再生したり、カメラを介して音声を送信したりすることができます。

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

マイクのペアリング

エッジツーエッジのマイクペアリングにより、対応するマイクをカメラの一部であるかのように使用できます。ペアリングされると、マイクロフォンは周辺エリアからの音声を取り込み、音声入力装置として使用し、メディアストリームや録画で使用できます。

レーダーペアリング

エッジツーエッジレーダーペアリングにより、カメラを互換性のあるAxisレーダーに接続し、速度検知などの統合レーダー機能を利用することができます。

レーダーペアリングは一方向の設定で、1台のカメラと1台のレーダーをペアリングし、カメラを使って両方の装置の設定と保守を行います。ペアリングすると、カメラのwebインターフェースで直接レーダーの設定にアクセスし、レーダー固有のイベントルールを作成できます。このカメラは、VMSではレーダー機能が統合されているカメラとしても識別されます。

また、レーダーストリームはカメラの2番目のビューエリア、**View area 2 (ビューエリア2)** に表示されます。レーダーによって生成されたメタデータは、**チャンネル2**と呼ばれるカメラの2番目のメタデータ生成チャンネルから利用できます。

表示エリア

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

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

注

カメラとレーダーをエッジツーエッジでペアリングした場合、レーダーストリームはカメラの2番目のビューエリアに表示されます。

分析機能とアプリ

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

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

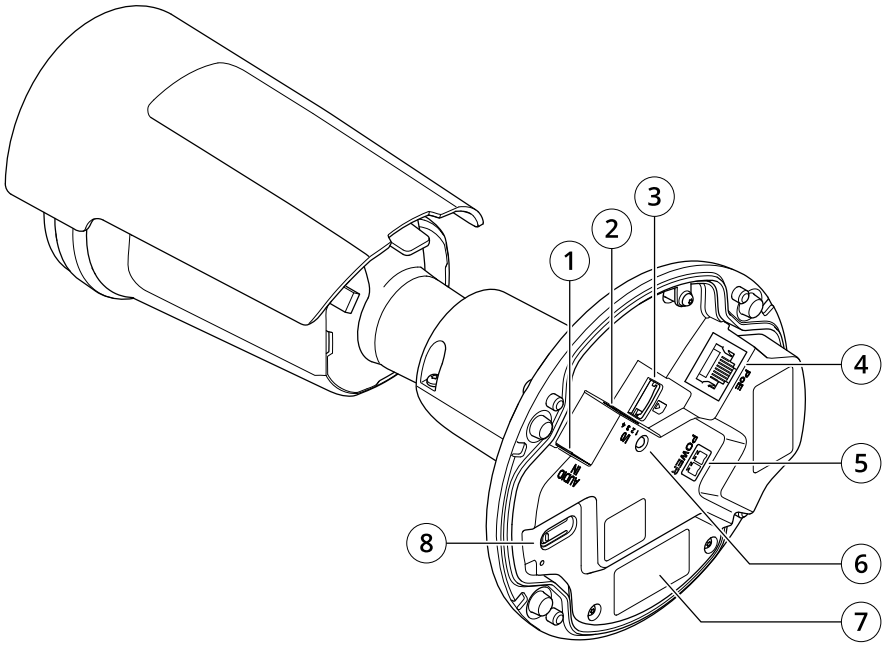
AXIS Image Health Analytics

AIベースのアプリケーション「AXIS Image Health Analytics」により、画像の劣化や改ざんの試みを検知することができます。このアプリケーションにより、シーンの動作を分析して学習すること、画像のぼやけや露出不足を検知すること、また遮られた視界や方向転換した視界を検知することができます。検知された対象に対してイベントを送信するようにアプリケーションを設定し、カメラのイベントシステムまたはサードパーティ製ソフトウェアを通じてアクションをトリガーすることができます。

アプリケーションの動作の詳細については、*AXIS Image Health Analyticsユーザーマニュアル*を参照してください。

仕様

製品概要



1 音声コネクター
2 I/Oコネクター
3 microSDカードスロット
4 ネットワーク コネクター
5 DC電源入力
6 ステータスLEDインジケーター
7 型番 (P/N) とシリアル番号 (S/N)
8 コントロールボタン

LEDインジケーター

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

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 48*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。

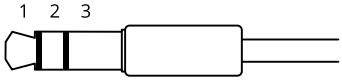
コネクター

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** - 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。
- **音声入力** - 2つのモノラルマイクロフォンまたは2つのライン入力モノラル信号用 (付属のステレオ-モノラルアダプターを使用) 3.5 mm入力。



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

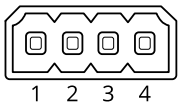
I/Oコネクター

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。

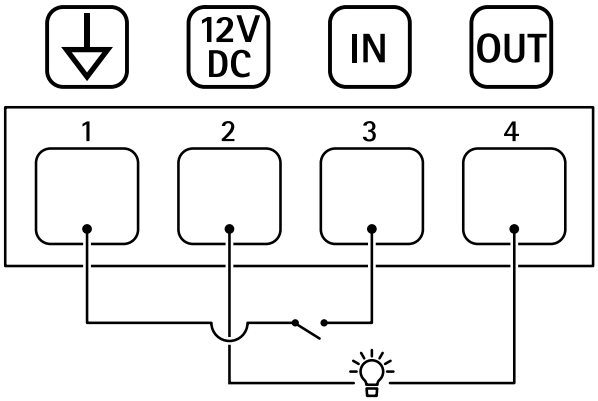
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

4ピンターミナルブロック



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 = 25mA
デジタル入力	3	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。	0～最大30 VDC
デジタル出力	4	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:

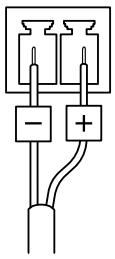


1 DCアース
2 DC出力12 V、最大25 mA
3 デジタル入力
4 デジタル出力

接続例

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。



トラブルシューティング

工場出荷時の設定にリセットする

警告

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

重要

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

注

カメラにはAXIS License Plate Verifierがあらかじめ設定されています。工場出荷時の設定に戻した場合、ライセンスキーは保持されます。工場出荷時の設定にリセットした後、アプリケーションを再インストールする必要はありません。

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 45*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。これで本製品は工場出荷時の設定にリセットされました。ネットワーク上に利用可能なDHCPサーバーがない場合、デフォルトのIPアドレスは`192.168.0.90`になります。
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ページを使用して、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 48*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 2*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。

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 53*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。

未知の車両が受け入れとしてにマークされる

アプリケーションが、許可リストに含まれないナンバープレートの車両を受け入れる場合、考えられる理由の1つは、比較の際に1文字の逸脱が許可されていることです。

たとえば、AXI S1234が許可リストに含まれている場合、アプリケーションはAXI SI234を受け入れます。

同様に、AXIS 1234が許可リストに含まれている場合、アプリケーションはAXI 1234を受け入れます。

追加設定, on page 24 に移動して、許可される文字を設定します。

アプリケーションとコントローラーまたはリレーモジュールの間の接続が機能しない

コントローラーまたはリレーモジュールでHTTP経由のデータトラフィックが許可されていることを確認してください。この設定を変更する方法については、対応するデバイスのユーザーズマニュアルを参照してください。

レーダーのペアリングでの問題	
カメラとレーダーをペアリングできない	レーダーは自動的に割り当てられるため、カメラの2番目のビューエリア (**View area 2 (ビューエリア2)**) が使用されていないことを確認してください。 2番目のビューエリアが使用されている場合は、**Video > View areas (ビデオ > ビューエリア)**] に移動してビューエリアを削除してから、装置のペアリングを再試行します。

カメラビューの移動車両が、速度オーバーレイやレーダービューの軌跡と同期していない	カメラとレーダーの時刻が同期していることを確認します。 ステータスを確認するには、各装置のwebインターフェースの [Status > Time sync status (ステータス > 時刻同期ステータス)] に移動します。ステータスが「Synchronized: No (同期済み: いいえ)」と表示されている場合は、[NTP settings (NTP設定)] をクリックし、装置を同期するタイムソースを選択します。両方の装置に同じタイムソースを使用していることを確認します。
カメラの2番目のビューエリアにレーダーストリームが正しく表示されない	エッジツーエッジでペアリングされた後のレーダーのデフォルト解像度は、カメラのWebインターフェースでもVMSでも1280x720です。別の解像度を選択すると、レーダーストリームが正しく表示されません。 レーダーの解像度を調整するには、カメラのwebインターフェースで [Video > Stream > General (ビデオ > ストリーム > 一般)] に移動し、[View area 2 (ビューエリア2)] を選択します。

オーバーレイの問題	
カメラのwebインターフェースで追加したオーバーレイがレーダーペアリング後に消える	カメラに複数のビューエリアを追加した場合、以前に追加したオーバーレイはカメラのwebインターフェースから消えます。レーダーのペアリング後、レーダーは2番目のビューエリアを占有するため、カメラのwebインターフェースにある既存のオーバーレイはすべて消えます。 オーバーレイが消えるのはwebインターフェースからだけです。VMSなどでは、オーバーレイを含むストリームを要求することができます。
AXIS License Plate Verifierで追加したナンバープレートのオーバーレイが表示されない	AXIS Speed Monitorで車速を表示するオーバーレイを追加し、AXIS License Plate Verifierでナンバープレートオーバーレイをオンにした場合、ナンバープレートオーバーレイは表示されません。 AXIS Speed Monitorで速度オーバーレイを追加する前に、まずAXIS License Plate Verifierでオーバーレイをオンにしてください。

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。

T10191704_ja

2026-02 (M17.2)

© 2023年 – 2026 Axis Communications AB