AXIS Q1656-DLE Radar-Video Fusion Camera

ユーザーマニュアル

目次

ソリューションの概要 5
..... 5
なぜ融合なのか 5
レーダービデオ融合の説明 5
インストール 7
プレビューモード 7
インストールガイド 7
検討事項 7
製品の取り付け場所 7
レーダーのカバー範囲 9
レーダービデオ融合の検知範囲 11
エリア設置 13
エリア設置例 13
エリア監視の使用例 14
道路設置 16
道路設置例 16
道路監視の使用例 18
使用に当たって 21
ネットワーク上のデバイスを検索する 21
ブラウザーサポート 21
装置のwebインターフェースを開く 21
管理者アカウントを作成する 21
安全なパスワード 22
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 22
webインターフェースの概要 22
デバイスを構成する 23
基本設定 23
画像を調整する 23
露出モードを選択する 23
赤外線照明を最適化する 23
ナイトモードを使用して低光量下で赤外線照明からメリットを得る 24
低照度環境でノイズを減らす 24
低光量下で動きによる画像のブレを減らす 24
最大限に詳細な画像を撮影する 24
逆光の強いシーンを処理する 25
揺れる映像を動体ブレ補正によって安定させる 25
プライバシーマスクで画像の一部を非表示にする 26
画像オーバーレイを表示する 26
画像内にレーダーのライブビューを表示する 26
画像に街路名とコンパス方位を追加する 27
ビデオを録画して見る 27
ビデオを表示する、録画する 27
帯域幅とストレージ容量を削減する 27
ネットワークストレージを設定する 28
レーダーの設定 28
レーダープロファイルの選択 28
取り付け高さの設定 28
取り付け高さを検証する 29
参照マップを使用してキャリブレーションを行う 29
検知ゾーンの設定 30
装置の自動キャリブレーション 32
レーダーのチルト角度をテキストオーバーレイに表示する 33
AXIS Object Analyticsの設定 33

シナリオを作成します....33
速度を使用してトリガーする....34
検知感度の選択....34
誤報を最小限に抑える....35
イベントのルールを設定する....36
動きが検知されないときに電力を節約する....36
誰かが筐体を開いた場合にアラームをトリガーする....36
誰かがレーダーを金属製の物体で覆った場合に電子メールを送信する....37
レーダーでPTZカメラを制御する....38
MQTTを使用してレーダーデータを送信する....39
カメラが物体を検知したときにビデオを録画する....40
進行中のイベントを視覚的に示します....40
装置が物体を検知したときにビデオストリームにテキストオーバーレイを表示する....41
PIR検知器が動きを検知したときにビデオを録画する....42
カメラが音量の大きいノイズを検知したときにビデオを録画する....43
入力信号でいたずらを検知する....43
音声....44
録画に音声を追加する....44
webインターフェース....45
ステータス....45
ビデオ....47
インストール....49
画像....51
ストリーム....57
オーバーレイ....60
プライバシーマスク....62
レーダー....62
設定....62
ストリーム....64
マップキャリブレーション....66
除外範囲....67
シナリオ....68
オーバーレイ....69
レーダーPTZオートトラッキング:....71
自動キャリブレーション....72
分析機能....73
AXIS Object Analytics....73
AXIS Image Health Analytics....73
メタデータの可視化....73
メタデータの設定....73
音声....74
デバイスの設定....74
ストリーム....74
音声クリップ....75
音声エンハンスメント....75
録画....75
アプリ....77
システム....77
時刻と位置....77
ネットワーク....79
セキュリティ....83
アカウント....89
イベント....91
MQTT....96
ストレージ....99
ストリームプロファイル....101

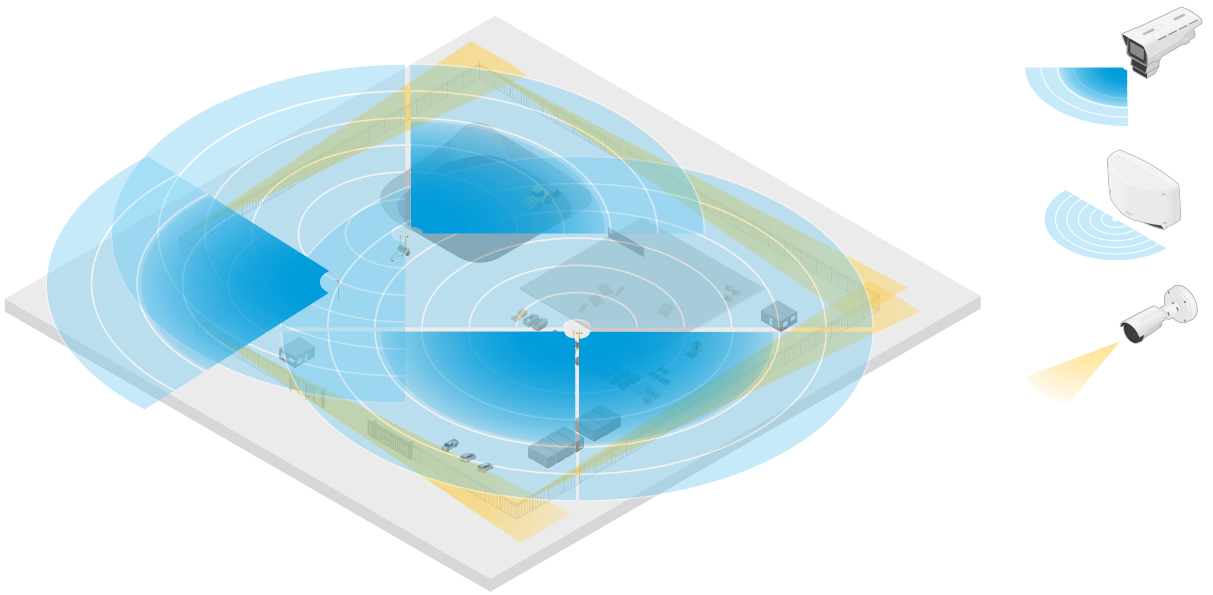
ONVIF 102
検知器 105
アクセサリー 105
エッジツーエッジ 106
ログ 107
プレイン設定 108
メンテナンス 109
メンテナンス 109
トラブルシューティング 110
詳細情報 111
長距離接続 111
キャプチャーモード 111
リモートフォーカス/ズーム 112
プライバシーマスク 112
オーバーレイ 112
ストリーミングとストレージ 113
ビデオ圧縮形式 113
画像、ストリーム、およびストリームプロファイルの各設定の相互関連性について 113
ビットレート制御 114
アプリケーション 115
AXIS Object Analytics 115
AXIS Image Health Analytics 115
メタデータの可視化 116
サイバーセキュリティ 116
署名付きOS 116
セキュアブート 116
Axis Edge Vault 116
TPMモジュール 116
AxisデバイスID 116
署名付きビデオ 117
仕様 118
製品概要 118
LEDインジケーター 119
ブザー 119
フォーカスアシスタントのブザー信号 119
SDカードスロット 119
ボタン 119
コントロールボタン 119
侵入アラームスイッチ 120
コネクター 120
ネットワーク コネクター 120
音声コネクター 120
I/Oコネクター 120
電源コネクター 121
RS485/RS422コネクター 122
トラブルシューティング 123
工場出荷時の設定にリセットする 123
AXIS OSのオプション 123
AXIS OSの現在のバージョンを確認する 123
AXIS OSをアップグレードする 124
技術的な問題、ヒント、解決策 124
パフォーマンスに関する一般的な検討事項 127
サポートに問い合わせる 127

ソリューションの概要

レーダービデオ融合カメラは、完全統合型のレーダーモジュールを搭載したビジュアルカメラです。そのため、レーダーとビデオを個別に、または組み合わせて使用して、物体を検知および分類できます。

レーダービデオ融合の利点は、より正確な検知と分類が可能になり、アラームの誤作動や見逃しが少なくなることです。2つの技術の融合は、AXIS Object Analyticsに集約されています。これは、レーダービデオ融合にアクセスして設定するための主要なインターフェースです。

AXIS Q1656-DLEは、奥行きのある広いエリアで物体を検知し分類するため、エリア監視や道路監視に使用できます。さらに、AXIS Q1656-DLEは、他の装置と組み合わせたサイト設計にも適しています。AXIS Q1656-DLEのレーダーの検知範囲がカメラの視野よりも広いため、IR照明を備えたPTZカメラと組み合わせることで、レーダーの検知範囲全体での映像による確認が可能になります。また、細長いエリアの物体を検知して分類できるサーマルカメラと組み合わせることもできます。



建設現場の例では、2台のスタンドアロンレーダーが現場のオープンエリアをカバーし、4台のレーダービデオ融合カメラがより複雑なオープンエリアをカバーしています。さらに、4台のサーマルカメラがフェンス沿いの狭い通路をカバーしています。

なぜ融合なのか

ビデオとレーダーは、それぞれ単独で使用する場合、固有の長所と短所があります。

- コントラストが十分であり、物体がカメラに近づくように動いている場合、通常、ビデオの分類はより正確になります。また、レーダーよりも詳細な分類が可能です。ただし、カメラは物体を視認するために良好な照明条件が必要です。
- 一方、レーダーは厳しい照明条件でも物体を検知でき、その検知および分類範囲はより長くなります。天候条件に関係なく、レーダーは動く物体の速度や方向、距離を測定できます。しかし、映像による確認ができないため、レーダーによる分類は脆弱になることがあります。揺らめいている物体や反射面は誤報の原因となることがあるため、サイトの設計やレーダーの設定時に考慮する必要があります。

レーダーとビデオの融合カメラの2つの技術は、それぞれ単独でも使用できますが、両方の技術からの分析が合わされば、相乗効果が生まれ、検知と分類の信頼性が高まります。

レーダービデオ融合の説明

本製品はレーダーデータとビデオデータを2つの方法で融合します。

- **映像による融合**:レーダー検知と分類を融合してビデオ画像にします。これは、ビデオ分析が利用できない場合に、ビデオストリーム内のレーダーデータを可視化する方法です。
  たとえば、50 m離れた場所に物体が現れた場合、ビデオ分析では小さすぎて検知できない可能性がありますが、レーダーでは識別できます。その場合、レーダー検知は融合されて画像平面となり、AXIS Object Analyticsの内部でアラームをトリガーするのに使用できます。
- **分析による融合**:レーダーによる検知と分類が、ビデオ分析による検知と分類に融合されます。これにより、両方の技術のそれぞれの強みを融合した複合的な分析出力を得ることができます。この方法では、レーダーによる距離と速度、ビデオによる位置と分類が使用されます。
  上の例では、物体が近づくと、ビデオ分析もそれを検知します。レーダー検知はその後にビデオ分析出力と融合されて、これらの2つの技術が個別に実現するよりも品質が高く情報量が多い出力が生成されます。

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。

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。

インストールガイド

本製品のインストールガイドおよび他のドキュメントは、*axis.com/products/axis-q1656-dle/support#support-resources*から入手できます。

検討事項

製品の取り付け場所

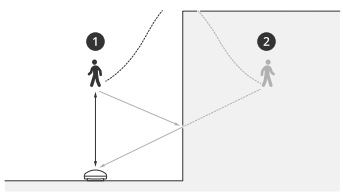
ビデオとレーダーのカバー範囲を最適に保つには、製品を適切に取り付ける必要があります。レーダービデオ融合カメラを取り付けるときは、次の点を考慮してください。

エリアまたは道路の監視

本製品はオープンエリアの監視を目的としており、エリア監視にも道路監視にも使用できます。設置例や使用例については、およびを参照してください。

固形物や反射物を避ける

固体や金属はAXIS Q1656-DLEのレーダーのパフォーマンスに影響することがあります。対象範囲内のほとんどの固体 (壁、フェンス、樹木、大きな茂みなど) は、その背後に死角 (レーダーシャドウ) を作り出します。視野内の金属の物体は反射を引き起こし、レーダーの分類機能に影響します。これにより、レーダーストリームでゴースト追跡や誤報が発生することがあります。



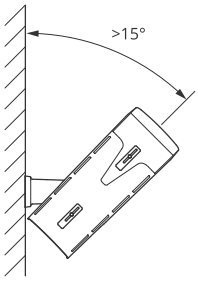
1 実際の検知
2 反射の検知 (ゴースト追跡)

レーダーの対象範囲内の固形物と反射物の取り扱い方法については、を参照してください。

設置位置

製品を安定したポールに設置するか、壁面上で他の物体や設置された装置がない場所に設置します。製品の左右1 m以内にある物体は、電波を反射するため、AXIS Q1656-DLEのレーダーのパフォーマンスに影響します。

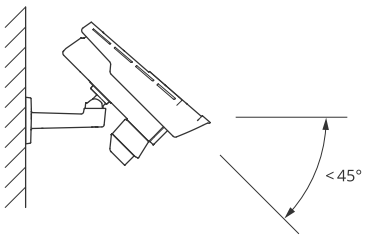
製品を壁に設置する場合は、15°以上の角度で壁から離れた方向を向くようにする必要があります。



また、取り付け高さはビデオとレーダーの両方の検知距離および範囲に影響します。

チルト角度

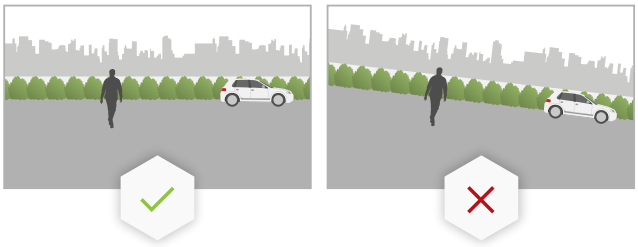
画像の中心が水平線より下になるように、製品を十分に地面に向ける必要があります。推奨される取り付け角度は15～45°です。



レーダーのライブビューに、製品のチルト角を示すオーバーレイを追加できます。手順については、を参照してください。

ロール角度

製品のロール角度はほぼ0にしてください。画像が水平になる必要があるためです。



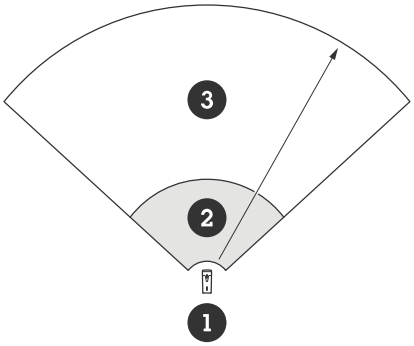
共存

60 GHzの周波数帯域で動作する8台を超えるレーダーまたはレーダービデオ融合カメラを互いに近くに取り付けると、互いに干渉する可能性があります。干渉を避けるには、を参照してください。

複数のAxisレーダー装置の設置

共存

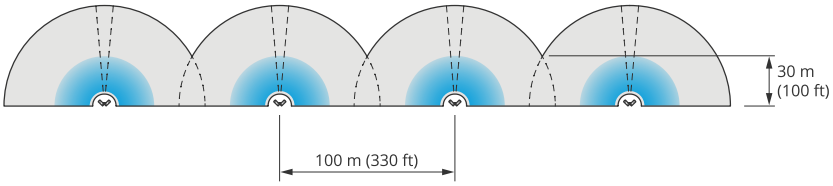
AXIS Q1656-DLEのレーダーの電波が検知エリアを越えて進み、最大350 m離れた他のレーダーに干渉する可能性があります。これを共存ゾーンと呼びます。



1 融合カメラ
2 検知領域
3 共存ゾーン

AXIS Q1656-DLEは、60 GHzの周波数バンドで動作します。60 GHzバンドのAxisレーダーまたはレーダービデオ融合カメラは、最大8台までは互いに近くに設置しても、向かい合わせに設置しても、問題はありません。組み込みの共存アルゴリズムにより、干渉を最小限に抑えるための適切な時間帯と周波数チャンネルを見つけることができます。

同じ周波数帯で動作するレーダー装置が8台を超えて設置されていても、それらの多くが互いに反対方向を向いている場合、干渉のリスクは低くなります。一般に、レーダー干渉によってレーダーの機能が停止することはありません。レーダーには、干渉がある場合でもレーダー信号を修復しようとする干渉軽減アルゴリズムが内蔵されています。同じ共存ゾーンに同じ周波数帯で動作するレーダーが多数ある環境では、干渉に関する警告の発生が予想されます。干渉による主な影響は、検知パフォーマンスの劣化であり、時にゴースト追跡も生じます。



4組のAXIS Q1656-DLEを並べて設置。

レーダービデオ融合カメラは異なる周波数バンドで動作するAxisレーダーと、共存を懸念することなく組み合わせることができます。異なる周波数バンドで動作するAxisレーダー装置は互いに干渉しません。

レーダーのカバー範囲

AXIS Q1656-DLEのレーダーの水平検知領域は95°です。レーダーの検知範囲は、シーン、製品の設置の高さやチルト角度、移動物体の大きさや速度などの要因によって異なります。

検知範囲は、選択した**監視プロファイル**によっても異なります。AXIS Q1656-DLEはエリアまたは道路監視に使用でき、レーダーにはシナリオごとに最適化された2つのプロファイルがあります。

- **エリア監視プロファイル**: レーダーは55 km/h (34 mph)未満の速度で移動する人、車両、不明の物体を追跡して分類します。検知範囲の詳細については、を参照してください。
- **道路監視プロファイル**: レーダーは主に、最大200 km/h (125 mph) の速度で移動する車両を追跡して分類します。検知範囲の詳細については、を参照してください。

注

AXIS Object Analyticsでレーダーとビデオを組み合わせると、AXIS Q1656-DLEは車両のサブクラス (バス、乗用車、バイク、トラックなど) を分類できます。

製品のwebインターフェースでエリアまたは監視プロファイルを選択します。手順については、を参照してください。

カバー範囲

この装置のレーダーの水平検知領域は95°です。カバー範囲は、人の場合は2,700 m^2 (29,000 ft^2)、車両の場合は6,100 m^2 (65600 ft^2) に相当します。

注

製品が3.5～7 mの高さに取り付けられている場合、最適なカバー範囲が適用されます。設置の高さは、レーダーの下の死角の大きさに影響します。

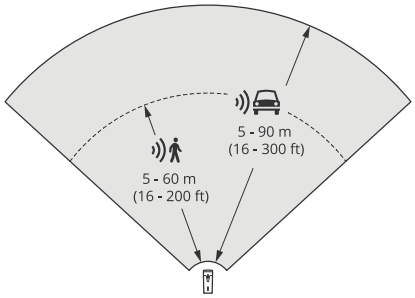
エリア検知範囲

検知範囲は、物体を追跡してアラームをトリガーできる距離です。検知範囲は、近距離検知限界 (装置にどれだけ近づいて検知できるか) から遠距離検知限界 (装置からどれだけ離れて検知できるか) までの間で測定されます。

[area monitoring profile (エリア監視プロファイル)] は人の検知用に最適化されていますが、最大55 km/hで走行する車両やその他の物体を+/- 2 km/hの速度精度で追跡するためにも使用できます。

最適な高さに設置した場合、検知範囲は次のとおりです。

- 人の検知時は5～60 m
- 車両の検知時hは5～90 m



注

- レーダーのキャリブレーションを行うときに、webインターフェースで取り付け高さを入力します。
- 検知範囲はシーンや製品のチルト角度によって影響されます。
- 検知範囲は動く物体のタイプとサイズによって影響されます。

レーダーの検知範囲は以下の条件下で測定されました。

- 範囲は地面に沿って計測されています。
- 物体は、身長170 cm (5 ft 7 in) の人でした。
- この人はレーダーの前をまっすぐ歩いていました。
- これらの値は、人が検知ゾーンに入ったときに計測されました。
- レーダー感度は [Medium (中)] に設定されていました。

取り付け位置の高さ	チルト 15°	チルト 20°	チルト 25°	チルト 30°	チルト 35°	チルト 40°	チルト 45°
3.5 m (11 ft)	6.0～60+ m (19～196 + ft)	5.0～60+ m (16～196 + ft)	4.0～60+ m (13～196 + ft)	4.0～60 m (13～196 ft)	4.0～55 m (13～180 ft)	4.0～40 m (13～131 ft)	4.0～30 m (13～98 ft)
4.5 m (14 ft)	6.0～60+ m	6.0～60+ m	5.0～60+ m	4.0～60+ m	4.0～60 m	4.0～45 m	4.0～40 m

取り付け位置の高さ	チルト 15°	チルト 20°	チルト 25°	チルト 30°	チルト 35°	チルト 40°	チルト 45°
	(19〜196 + ft)	(19〜196 + ft)	(16〜196 + ft)	(13〜96+ ft)	(13〜196 ft)	(13〜147 ft)	(13〜131 ft)
6 m (19 ft)	10〜60+ m (32〜196 + ft)	9.0〜60+ m (29〜196 + ft)	7.0〜60+ m (22〜196 + ft)	6.0〜60+ m (19〜196 + ft)	6.0〜60 m (19〜196 ft)	5.0〜55 m (16〜180 ft)	5.0〜55 m (16〜180 ft)
8 m (26 ft)	16〜60 m (52〜196 ft)	14〜60 m (45〜196 ft)	10〜60 m (32〜196 ft)	8.0〜60+ m (26〜196 + ft)	8.0〜60+ m (26〜196 + ft)	7.0〜60 m (22〜196 ft)	7.0〜60 m (22〜196 ft)
10 m (32 ft)	21〜60 m (68〜196 ft)	19〜60 m (62〜196 ft)	14〜60 m (45〜196 ft)	12〜60+ m (39〜196 + ft)	10〜60+ m (32〜196 + ft)	9.0〜60 m (29〜196 ft)	9.0〜60 m (29〜196 ft)
12 m (39 ft)	25〜60 m (82〜196 ft)	23〜60 m (75〜196 ft)	19〜60 m (62〜196 ft)	16〜60+ m (52〜196 + ft)	13〜60+ m (42〜196 + ft)	11〜60 m (36〜196 ft)	11〜55 m (36〜180 ft)

注

- レーダー感度を [**Low (低)**] に設定すると検知範囲は20%狭くなり、[**High (高)**] に設定すると検知範囲は20%広くなります。
- 設置場所で融合ゾーンの外側に小動物が現れることが予想される場合、レーダー感度を [**Low (低)**] に設定することで、誤報を最小限に抑えることができます。ただし、これにより検知範囲は狭くなります。

道路検知範囲

[**road monitoring profile (道路監視プロファイル)**] は、車両の検知用に最適化されており、最大200 km /hで走行する車両を+/- 2 km/hの速度精度で監視するために使用されます。

レーダービデオ融合カメラの取り付け高さと車両の速度はレーダーの検知範囲に影響します。取り付け高さが最適であれば、レーダーは次の範囲内で+/- 2 km/hの速度精度で近づく車両と離れる車両を検知します。

- 50 km/h (31 mph) で走行する車両の場合は**25〜100 m (82〜328 ft)**。
- 100 km/h (62 mph) で走行する車両の場合は**40〜80 m (131〜262 ft)**。
- 200 km/h (125 mph) で走行する車両の場合は**50〜70 m (164〜230 ft)**。

注

高速で走行する車両の検知漏れのリスクを最小限に抑えるには、物体タイプ [**Vehicle (車両)**] と [**Unknown (不明)**] でトリガーされるシナリオをレーダーに設定します。シナリオの設定方法の詳細については、を参照してください。

レーダービデオ融合の検知範囲

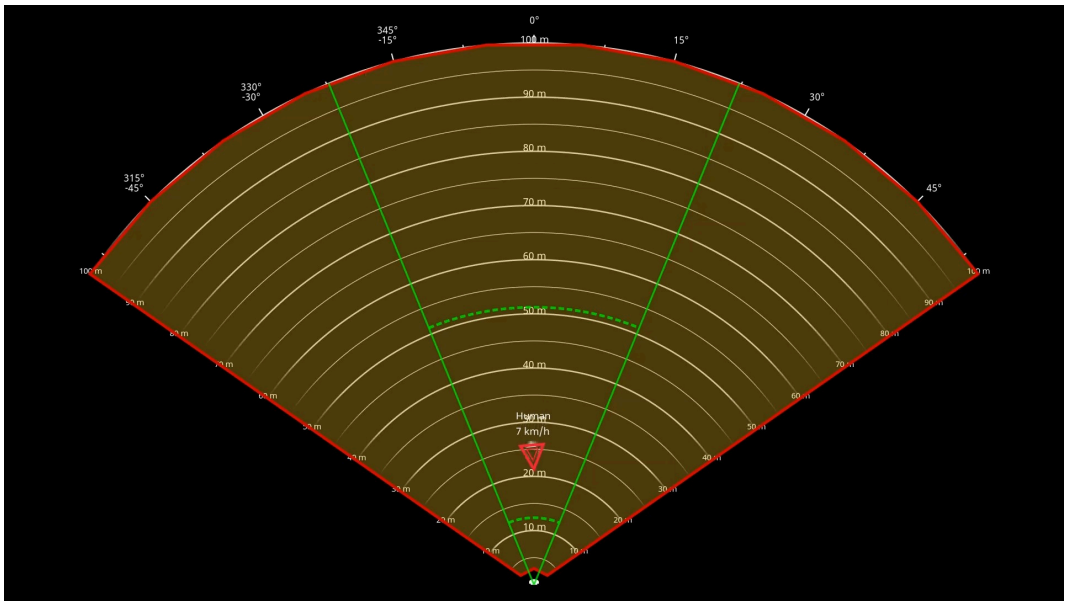
両方の技術によって物体を検知および分類できる分析融合ゾーンは、次のような要因によって変わります。

- カメラの取り付け高さ。
- カメラのチルト角度。

- カメラレンズのズームレベル。
- 周辺環境の照明条件、およびカメラ自体とサイトの他の装置からの光。
- 動く物体までの距離。

レーダービデオ融合カメラが設置されると、レーダーの検知範囲は固定されます。ただし、カメラの視野角はレンズのズームレベルによって異なります。

カメラの視野角をレーダーの検知範囲と関連付けて可視化するために、レーダーストリームには、カメラのおおよその視野を表す2本の緑色の線が表示されます。この線は、カメラがズームインまたはズームアウトすると調整されます。さらに、2本の点線は、カメラが視認できるおおよその範囲を表します。装置に近い点線は近距離検知限界を表し、より遠くの点線は遠距離検知限界を表します。



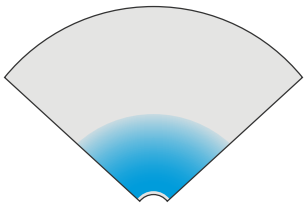
緑色の実線はカメラのおおよその視野を表し、緑色の点線は近距離と遠距離のおおよその検知限界を表します。

ズームレベルの例

分析融合ゾーンのサイズは、AXIS Q1656-DLEのレンズのズームレベルに影響されます。ズームレベルの2つの極値について以下に説明します。

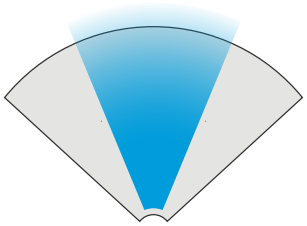
レンズズームアウト (最大視野角)

AXIS Q1656-DLEでレンズを最大にズームアウトすると、物体が小さくなりすぎてビデオ分析で検知できないことがあります。このシナリオでは、広範囲をカバーするレーダーによって物体が検知されても、ビデオ分析機能によって検知されない可能性が高くなります。レーダーの検知範囲全体で映像による確認を行う場合、AXIS Q1656-DLEを1台以上のPTZカメラとペアリングできます。



レンズズームイン (最大望遠)

レンズを最大にズームインすると、カメラの視野角が大幅に制限されます。ただし、レンズを最大にズームアウトした場合に比べて遠くにある物体が拡大されるため、装置からはるかに離れた場所にある物体をビデオ分析で検知できるようになります。このシナリオでは、ビデオ分析で物体が検知されてもレーダー分析では検知されない可能性があります。



レーダーとビデオ分析の両方で物体が正確に分類される確率を最大限に高めるには、可能であれば、対象範囲内の物体がビデオ分析で検知できるほどの大きさになるように、ズームを調整します。

レーダービデオによる検知と分類

AXIS Q1656-DLEは、レーダーとビデオ、あるいはどちらか一方の技術を使用して物体を検知および分類できますが、いくつかの注意点があります。

- 2人が近くを歩いていてレーダーで検知されたがビデオ分析では検知されなかった場合、2人は1人として分類され、2人を囲む境界ボックスが1つのみ表示されます。分析融合ゾーンに入り、映像による確認ができれば、正確に分類されます。AXIS Q1656-DLEのレーダーの空間分化能力は3 m (9 ft)です。
- 物体がカメラの視野外にある場合、AXIS Q1656-DLEは検知や分類を画像平面に統合できません。これは、AXIS Object Analyticsがアラームをトリガーできないことを意味します。レーダーのみで物体を検知した場合にアラームがトリガーされるようにするには、レーダーのwebインターフェースでシナリオを設定し、条件を使用して、レーダーシナリオ内の動きでトリガーされるようにします。
- レーダーのwebインターフェースで追加する除外ゾーンはグローバルで、これらのゾーンで検知された動きは常に無視されます。これは、除外ゾーンがAXIS Object Analyticsの分析融合ゾーンと重なっている場合でも同じです。ただし、AXIS Object Analyticsで追加した除外ゾーンでは、AXIS Object Analyticsのシナリオでのみ動きが無視されます。

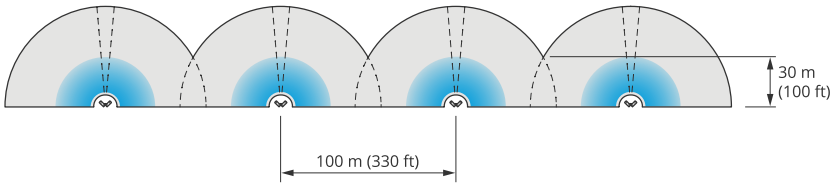
エリア設置

エリア設置で最高のレーダーパフォーマンスを得るには、AXIS Q1656-DLEで [
area monitoring profile (エリア監視プロファイル)] を選択します。詳細については、を参照してください。

エリア設置例

たとえば、建物に沿って、または建物の周りに、仮想フェンスを作成するには、複数のレーダービデオ融合カメラを横に並べて設置できます。

レーダーが180°の範囲をカバーできるようにするには、2台のAXIS Q1656-DLEを隣り合わせに設置します。複数のレーダービデオ融合カメラを並べて設置する場合は、例に示すように、各ペアの間を100 m空けることをお勧めします。



4組のAXIS Q1656-DLEを並べて設置。

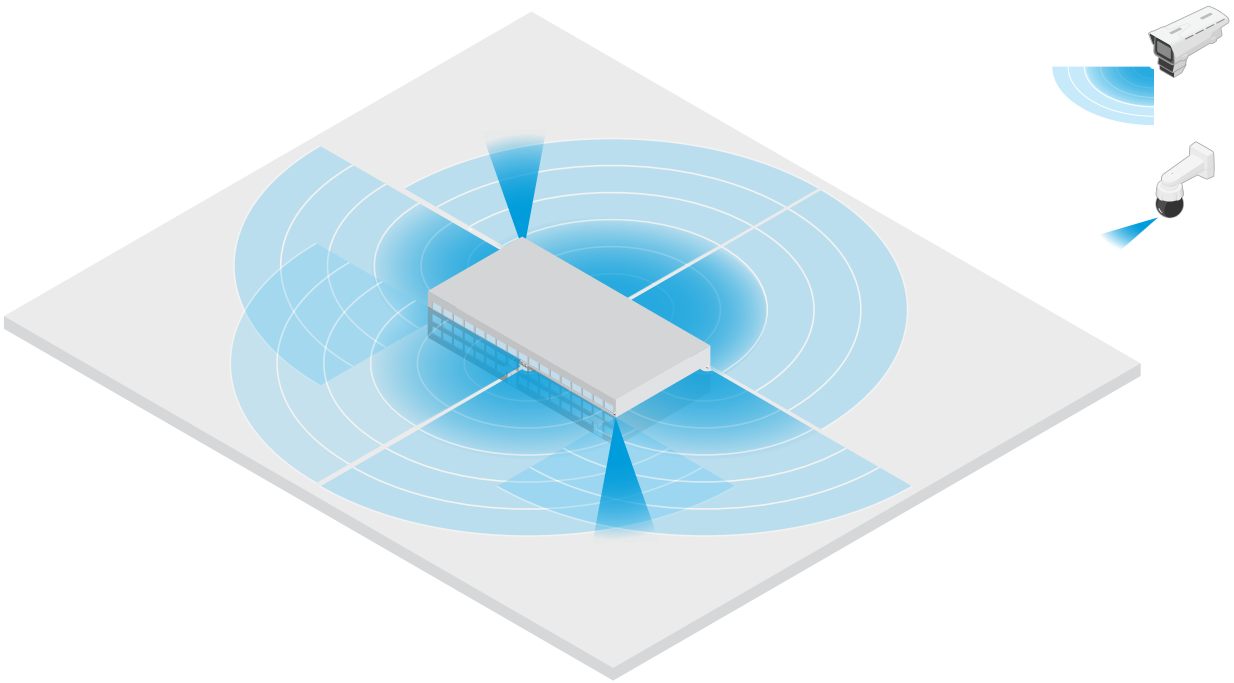
最大8台のレーダービデオ融合カメラをレーダー間で互いに干渉することなく近接して設置できます。Axisレーダー装置を近くに配置する方法の詳細については、を参照してください。

エリア監視の使用例

建物の周囲の開けた現場をカバーする

オフィスビル内のある会社は、特に勤務時間後や週末や祝日に、敷地内を侵入や破壊行為から守る必要があります。建物の周囲をカバーするために、レーダービデオ融合カメラとPTZカメラを組み合わせて設置しています。人や車両が建物に近づくとアラームがトリガーされるようにレーダービデオ融合カメラを設定しています。可能な限り信頼性の高い検知と分類を行うために、AXIS Object Analyticsでそのエリアに適した検知感度を選択しています。動体検知感度の詳細については、を参照してください。

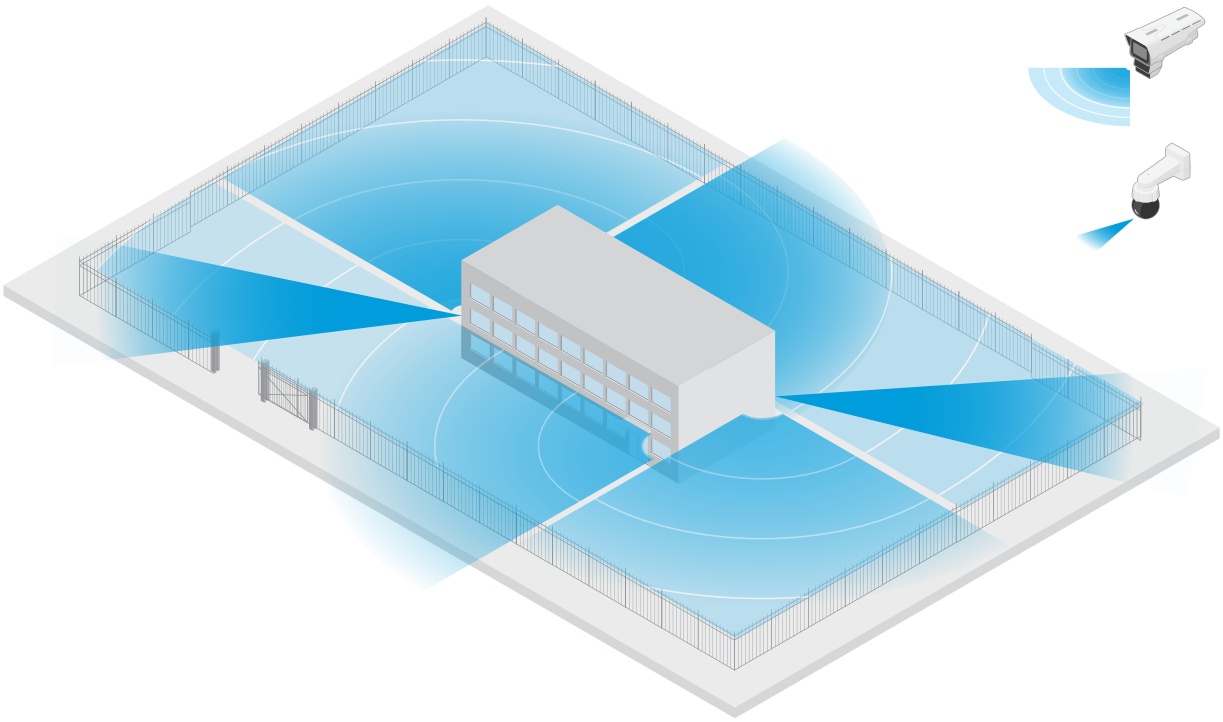
レーダーの検知範囲全体で侵入の疑いがある人を映像により確認できるようにするために、IR内蔵の2台のPTZカメラを建物の反対側の角に追加しています。レーダーは*AXIS Radar Autotracking for PTZ*を通じてPTZカメラを操作し、内蔵IRはレーダービデオ融合カメラにより多くの光を提供するため、より遠距離にいる侵入者を検知して識別することが可能になります。



フェンスで囲まれた建物をカバーする

通常、敷地内に商品を保管する倉庫は、侵入者を防ぐためにフェンスで囲まれています。侵入の疑いがある人を検知するために、レーダービデオ融合カメラとIR内蔵のPTZカメラを組み合わせて設置し、敷地内の安全を確保しています。レーダービデオ融合カメラが信頼性の高い検知とアラームのトリガーを行い、PTZカメラが視覚的なカバー範囲を拡大します。また、IR内蔵のPTZカメラは、レーダービデオ融合カメラにより多くの光を提供するため、より遠くからの侵入者の検知と識別を行うことができます。

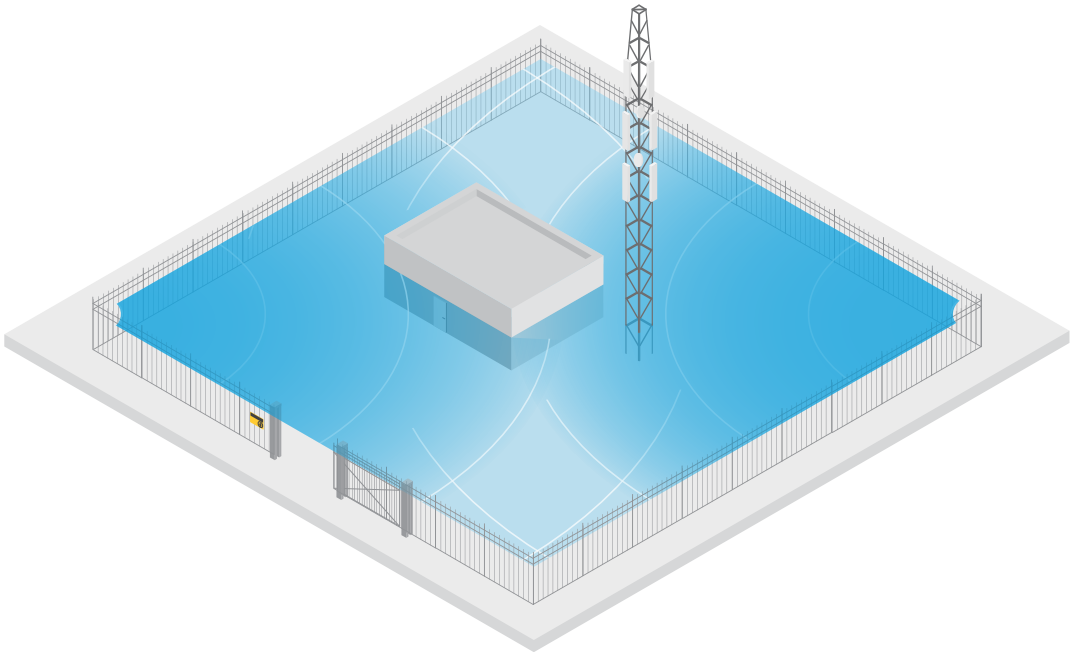
このシーンでは、フェンスの外側のエリアは誤報をトリガーする可能性がある混雑したエリアであるため、カバーしていません。人通りが少ないシーンでは、フェンスの外側のエリアもカバーできます。このようなシーンでは、侵入の疑いがある人を阻止するために、フェンスの外側で動きが検知されたときに外部ライトをトリガーするようにカメラを設定することが可能です。また、実際にフェンス内に侵入者が検知された場合にアラームをトリガーすることもできます。フェンスの外側での動きを検知できるようにするには、カメラを十分な高さに取り付ける必要があります。



重要な資産をカバーする

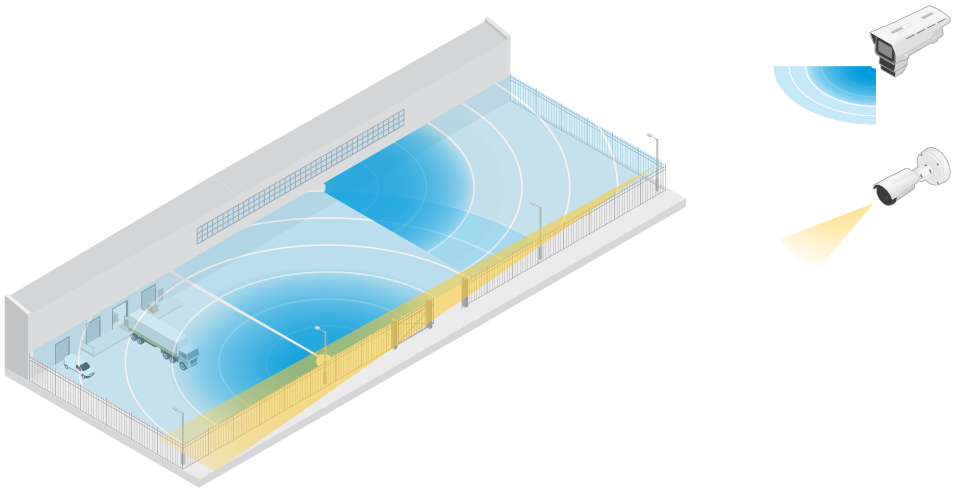
重要な機器やケーブルが設置されている通信シェルターは、侵入者を防ぐためにフェンスで囲まれています。改ざんや妨害行為を避けるために、さらなる保護が必要です。誤報を最小限に抑えることが重要であるため、サイトの対角線上に2台のレーダービデオ融合カメラを設置しました。これらのカメラは、シェルター、アンテナ、敷地全体をカバーできます。レーダービデオ融合カメラでレーダーとビデオの両方のテクノロジーを使用することで、カメラは侵入の疑いがある人を確実に検知し分類できます。

このようにレーダービデオ融合カメラを向かい合わせに設置しても、レーダー間の干渉はありません。ただし、ビデオテクノロジーにより正確な検知と分類を確実に行うには、良好な照明条件が必要です。



搬入口周辺をカバーする

商業ビルの搬入口は、敷地内を保護するためにフェンスで囲まれています。セキュリティ強化のために、同社は敷地内にサーマルカメラと3台のレーダービデオ融合カメラを設置しています。侵入の疑いがある人を検知するために、フェンスに沿ってサーマルカメラを設置しています。フェンスをすり抜けた侵入者を検知するために、レーダービデオ融合カメラを2台、搬入口に面したポールに設置しています。これらのカメラは、搬入口周辺を移動する人や車両を検知して分類でき、勤務時間後はアラームをトリガーできます。右側の旋回ポイントを通過する侵入者を検知するために、追加のレーダービデオ融合カメラをそのエリアに向けて設置しています。最後に、フェンスの近くに設置された2台のカメラに対するいたずらの試みを検知できるように、サーマルカメラを設置しています。



道路設置

道路設置で最高のレーダーパフォーマンスを得るには、AXIS Q1656-DLEで [road monitoring profile (道路監視プロファイル)] を選択します。詳細については、を参照してください。

道路設置例

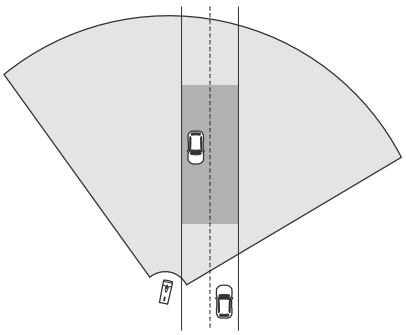
道路や高速道路を監視する際には、車両の後方に死角 (レーダー陰) ができないように、レーダービデオ融合カメラを十分な高さに取り付けてください。

注

レーダー陰の大きさは、レーダービデオ融合カメラの取り付け高さ、車両の高さ、レーダーからの距離によって異なります。たとえば、高さ4.5 mの車両が、高さ8 mに取り付けられているレーダービデオ融合カメラから50 m離れている場合、車両後方のレーダー陰は50 mになります。ただし、レーダービデオ融合カメラが高さ12 mに取り付けられている場合、同じ車両でも後方のレーダー陰は23 mにしかなりません。

サイド取り付け

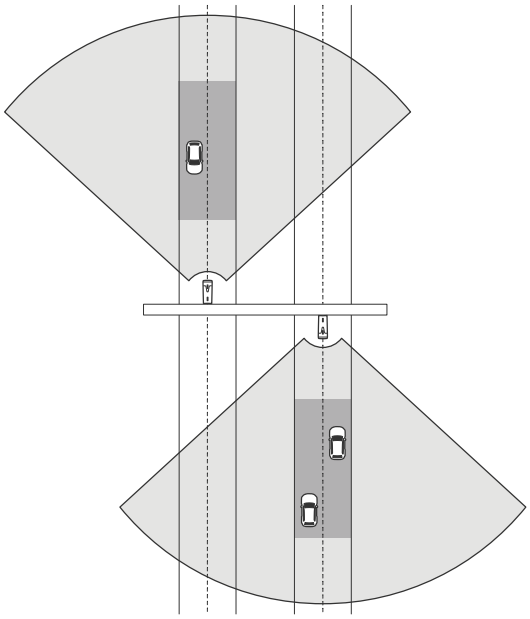
道路を走行する車両を監視するには、レーダービデオ融合カメラを道路の脇、たとえばポールに取り付けることができます。このタイプの設置では、パン角度を最大25° にすることをお勧めします。



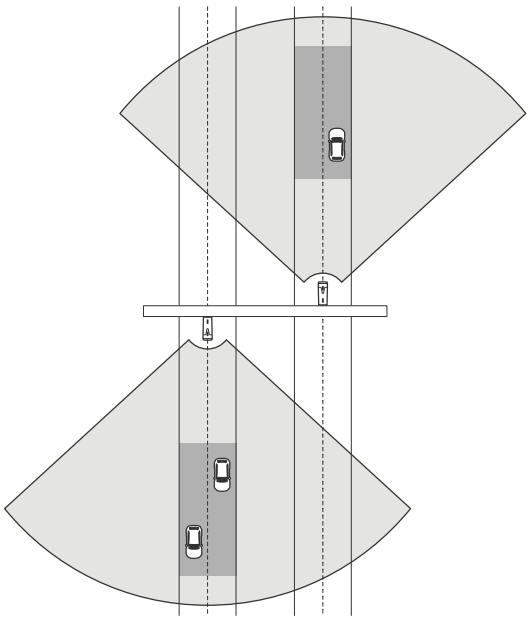
AXIS Q1656-DLEのレーダーで高速走行を正確に測定するには、レーダービデオ融合カメラを車両から横方向で10 m以内に配置します。検知範囲と速度精度の詳細については、を参照してください。

センター取り付け

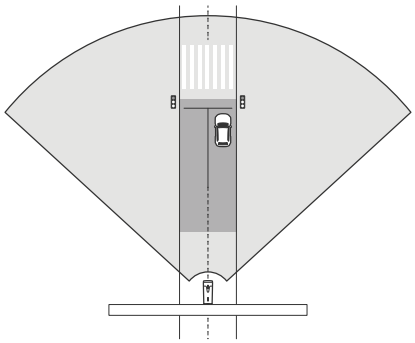
複数車線の道路で車両を監視するためには、道路上方のガントリーに1台以上のレーダービデオ融合カメラを取り付けることができます。



レーダーに向かってくるのではなく、レーダービデオ融合カメラから遠ざかる車両を監視する場合も、同じタイプの設置が可能です。



また、信号機のある横断歩道を見下ろすガントリーにレーダービデオ融合カメラを設置して、たとえば発進する車両の速度を記録したり、速度違反を検知したりすることもできます。

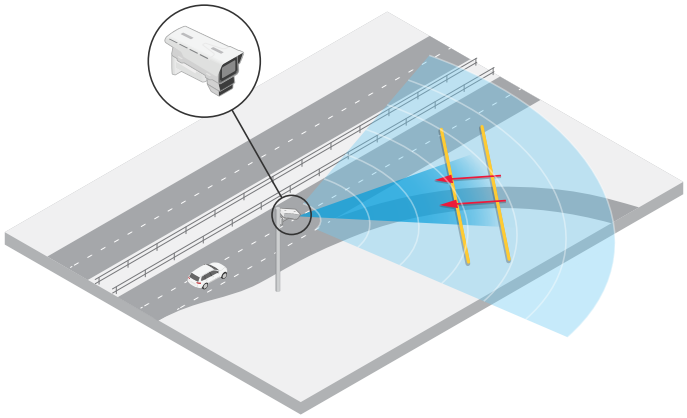


AXIS Q1656-DLEのレーダーで高速走行を正確に測定するには、レーダービデオ融合カメラを車両から横方向で10 m以内に配置します。検知範囲と速度精度の詳細については、を参照してください。

道路監視の使用例

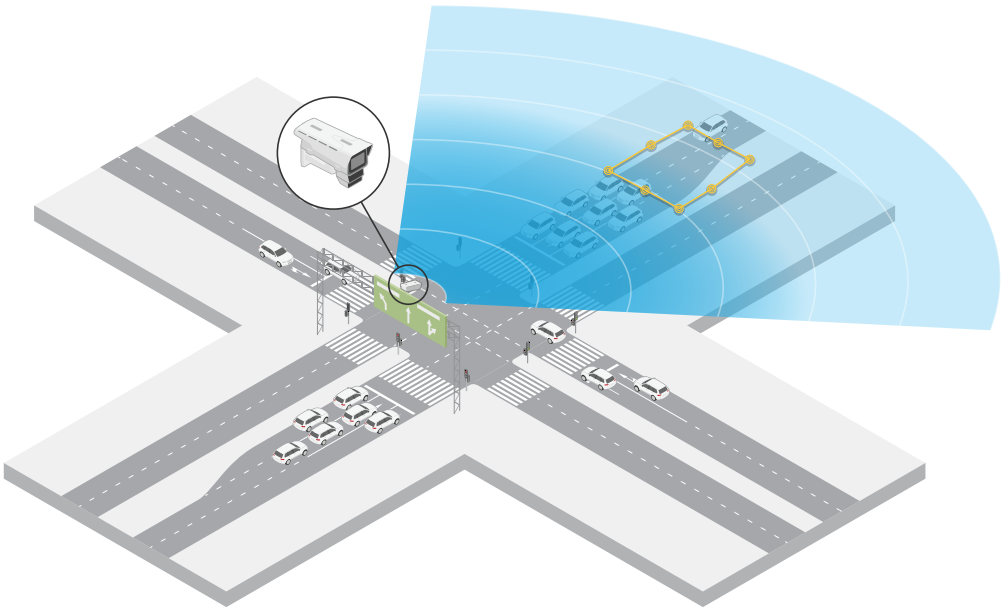
高速道路のランプでの逆走の検知

高速道路のランプで逆走車両を検知して識別するために、交通管制はランプに面したポールにAXIS Q1656-DLEを取り付けています。信頼性の高い検知を行うため、装置のwebインターフェースのレーダーページでライン横断シナリオを設定し、車両が2本のラインを横切ったときにのみアラームがトリガーされるように設定します。レーダーシナリオで、図に示すようにランプ上に2本のラインを配置し、アラームをトリガーする走行方向と速度を指定しています。この設定では、レーダーがアラームをトリガーし、カメラがランプ上の車両を映像により識別します。レーダーシナリオの設定方法の詳細については、を参照してください。



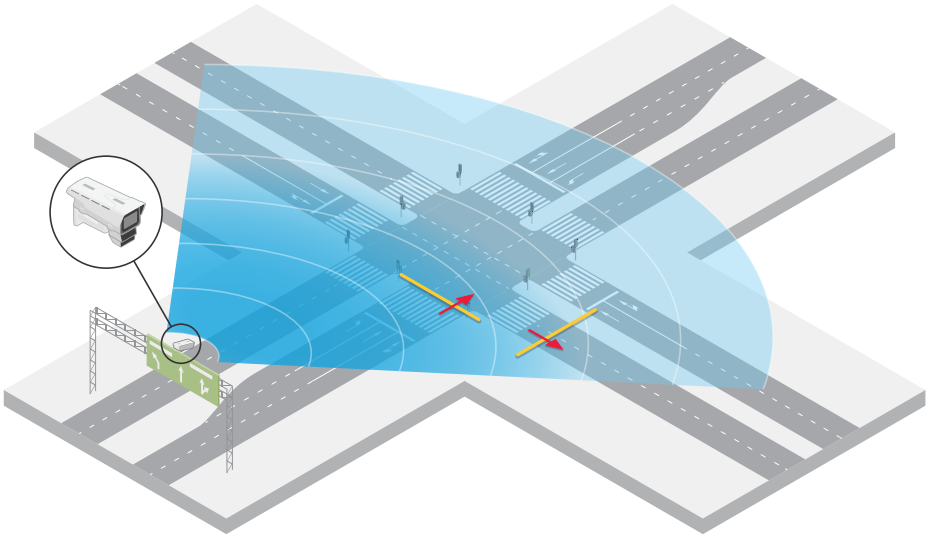
交差点での交通の流れの監視 - 渋滞発生

交通量の多い交差点で渋滞がいつ、どのように発生するかを監視するために、交通管制は交差点上方のガントリーにAXIS Q1656-DLEを設置しています。AXIS Object Analyticsで範囲内の物体シナリオを設定して、範囲内を移動する車両でトリガーされるようにしています。交差点までの道路の一部のみをカバーするようにシナリオを設定し、シーンに適した検知感度を選択しています。渋滞が発生し始めたときにアラームをトリガーするために、シナリオを設定して、5 km/h未満で走行する車両でアラームがトリガーされるようにしています。AXIS Object Analyticsのシナリオを設定し、適切な検知感度を選択する方法については、を参照してください。



交差点での交通の流れの監視 - 方向

交通量の多い交差点での交通の流れと車両の進行方向の概要を把握するために、交通管制は交差点に向かう道路上方のガントリーにAXIS Q1656-DLEを設置しています。装置のwebインターフェースのレーダーページでライン横断シナリオを設定して、車両が2本のラインを横切ったときにのみアラームがトリガーされるようにしています。レーダーシナリオを設定する際、1本目のラインは交差点に向かう車線上、横断歩道の真後ろに配置します。これは、ライン上で停止する車両を避けるためです。2本目のラインを右側に向かう車線上に配置します。車両がアラームをトリガーするには、指定した方向の両方のラインを横切る必要があります。複数の車両が横断ごとにアラームをトリガーしないように、レーダーシナリオの最小トリガー継続時間を2秒から0秒に短縮しています。



全方向の交通の流れを監視するために、各方向に1つのレーダーシナリオを作成しています。レーダーシナリオの設定方法の詳細については、を参照してください。

注

このレーダーシナリオでは、ラインを横切る車両はカウントされませんが、代わりに装置のwebインターフェースのイベントシステムを使用してカウントできます。車両をカウントする1つの方法として、レーダーシナリオがトリガーされるたびにMQTTメッセージを送信し、MQTT受信側でトリガーをカウントしています。

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

* iOS 15またはiPadOS 15でAXIS OS Webインターフェースを使用するには、**[Settings (設定)]** > **[Safari]** > **[Advanced (詳細)]** > **[Experimental Features (実験的機能)]**に移動し、[NSURLSession Websocket]を無効にします。

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、ネットワーク上で装置を見つけます。
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。を参照してください。

装置のwebインターフェースにあるすべてのコントロールとオプションの説明については、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。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。を参照してください。

安全なパスワード

重要

Axisデバイスは、最初に設定されたパスワードをネットワーク上で平文で送信します。最初のログイン後にデバイスを保護するために、安全で暗号化されたHTTPS接続を設定してからパスワードを変更してください。

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。を参照してください。
   リセットを行うと、セキュアブートによって装置の状態が保証されます。
2. デバイスを設定し、インストールします。

webインターフェースの概要

このビデオでは、装置のwebインターフェースの概要について説明します。

Axis装置のwebインターフェース

デバイスを構成する

基本設定

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. [Change (変更)] をクリックします。
3. 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。

キャプチャーモードを設定する

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

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。

赤外線照明を最適化する

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

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

ナイトモードを使用して低光量下で赤外線照明からメリットを得る

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

1. [Video > Image > Day and night (設定 > 画像 > デイナイト)] に移動し、[IR cut filter (IR カットフィルター)] が [Auto (自動)] に設定されていることを確認します。
2. [Allow illumination (照明を許可)] と [Synchronize illumination (照明の同期)] を有効にすると、ナイトモードのときにカメラ内蔵の赤外線照明を使用できます。

低照度環境でノイズを減らす

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

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

注

最大シャッター値が高いと、動きによる画像のブレが生じる場合があります。

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

注

最大ゲインを下げると、画像が暗くなる場合があります。

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

低光量下で動きによる画像のブレを減らす

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

注

ゲインを大きくすると、画像のノイズが多くなります。

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

それでも動きによる画像のブレに問題がある場合は、

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

最大限に詳細な画像を撮影する

重要

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

- 解像度が最大のキャプチャーモードを選択したことを確認してください。
- [Video (ビデオ) > Stream (ストリーム) > General (一般)] に移動し、圧縮率を可能な限り低く設定します。

- ライブビュー画像で をクリックし、[Video format (ビデオ形式)] で [MJPEG] を選択します。
- Video > Stream > Zipstream (ビデオ > ストリーム > Zipstream)に移動し、[Off (オフ)] を選択します。

逆光の強いシーンを処理する

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

WDRを使用していない画像。

WDRを使用している画像。

注

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

1. [Settings > Image > Wide dynamic range (設定 > 画像 > ワイドダイナミックレンジ)] に移動します。
2. WDR をオンにします。
3. [Local contrast (ローカルコントラスト)] スライダーを使用して、WDRの量を調整します。
4. それでも問題が発生する場合は、[Exposure (露出)] に移動して [Exposure zone (露出エリア)] を調整し、対象範囲をカバーします。

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

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。

プライバシーマスクで画像の一部を非表示にする

1つ以上のプライバシーマスクを作成して、画像の一部を隠すことができます。

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

も参照してください。

画像オーバーレイを表示する

ビデオストリームのオーバーレイとして画像を追加することができます。

1. [Video (ビデオ)] > [Overlays (オーバーレイ)] に移動します。
2. [Image (画像)]を選択し、 + をクリックします。
3. [Images (画像)] をクリックします。
4. 画像をドラッグアンドドロップします。
5. [Upload (アップロード)] をクリックします。
6. [Manage overlay (オーバーレイの管理)] をクリックします。
7. 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。

画像内にレーダーのライブビューを表示する

画面上のコントロールを使用して、同じストリームでビデオのライブビューとレーダーの両方を表示できます。

1. [Video > Image (ビデオ > 画像)] に移動します。
2. ライブビューで をクリックして、製品の画面上のコントロールにアクセスします。
3. [Predefined controls (既定のコントロール)] を選択します。
4. [Radar picture-in-picture (レーダーピクチャーインピクチャー)] をオンにします。
5. [Enable picture-in-picture (ピクチャーインピクチャーを有効にする)] をクリックします。
6. レーダー投影のサイズを変更する場合は、[Resize picture-in-picture (ピクチャーインピクチャーのサイズを変更する)] をクリックします。
7. レーダー投影の位置を変更するには、[Move picture-in-picture (ピクチャーインピクチャーを移動する)] をクリックします。

画像に街路名とコンパス方位を追加する

注

すべてのビデオストリームと録画に、街路名とコンパス方位が表示されます。

1. [Apps] (アプリ) に移動します。
2. [Axis-orientationaid] をを選択します。
3. [Open] (開く) をクリックします。
4. ストリートの名前を追加するには、[Add text (テキストの追加)] をクリックし、そのストリートに合うようにテキストを変更します。
5. コンパスを追加するには、[Add compass (コンパスを追加する)] をクリックし、画像に合わせてコンパスを変更します。

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 > Image (ビデオ > 画像)] 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、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。

レーダーの設定

注

レーダービデオ融合カメラは、カメラとレーダーモジュールが完全に整合するように工場でキャリブレーションされています。レンズ、光学ユニット、レーダーモジュールを動かしたり、取り外したりすると、キャリブレーションと整合が元に戻ってしまうため、絶対に行わないでください。

レーダープロファイルの選択

このレーダービデオ融合カメラのレーダーには、エリア監視用に最適化されたプロファイルと、道路監視用に最適化されたプロファイルがあります。設置タイプに適したプロファイルを選択してください。

webインターフェース:

1. [Radar (レーダー)] > [Settings (設定)] > [Detection (検知)] に移動します。
2. [Radar profiles (レーダープロファイル)] でプロファイルを選択します。

取り付け高さの設定

レーダーのWebインターフェースで装置の取り付け高さを設定します。この設定によって、レーダーは通過する物体を検知し、その速度を正確に測定できます。

地面から装置までの高さをできるだけ正確に測定してください。表面に凹凸があるシーンでは、シーンの平均高さを表す値を設定します。

注

高さが正しく設定されていないと、物体が検知されたときにAXIS Object Analyticsで表示される境界ボックスが正確な位置に表示されません。

1. [Radar (レーダー)] > [Settings (設定)] > [General (全般)] に移動します。
2. [Mounting height (取り付け高さ)] で高さを設定します。

AXIS Object Analyticsでも取り付け高さを設定できます。ある場所で高さを設定すると、別の場所での取り付け高さが自動的に入力されます。

1. [Apps (アプリ) > AXIS Object Analytics] に移動します。
2. アプリケーションを起動し、[Open (開く)] をクリックします。
3. [Settings (設定)] をクリックします。
4. [Mounting height (取り付け高さ)] で高さを設定します。

取り付け高さを検証する

装置の正しい取り付け高さを測定して設定したことを検証するには、カメラのライブビューに拡張オーバーレイを追加します。オーバーレイは、動く物体の周りに投影された白い境界ボックスで構成されています。

1. [Video > Image (ビデオ > 画像)] に移動します。
2. ライブビューで をクリックして、装置の画面上のコントロールにアクセスします。
3. [Predefined controls (既定のコントロール)] を展開します。
4. [Augmented overlay (radar) (拡張オーバーレイ (レーダー))] をオンにします。
5. [Toggle augmented bounding boxes (拡張境界ボックスを切り替え)] をクリックします。
6. 監視シーン内で誰かに移動してもらい、カメラのライブビューで境界ボックスが動いている物体の周囲に投影されており、動いている物体の上、下、または横に投影されていないことを確認します。
7. 必要に応じて、取り付け高さを再測定して設定を調整し、再度確認します。

検証が完了したら、拡張オーバーレイをオフにします。

注

シーンに高低差がある場合は、オートキャリブレーション機能を使用してレーダー検知に基づく境界ボックスの精度を向上させます。詳細については、を参照してください。

参照マップを使用してキャリブレーションを行う

検知された物体が移動している場所を確認しやすくするために、参照マップをアップロードします。接地された平面図や、レーダーがカバーする範囲を示す航空写真を使用することができます。レーダー探知範囲が地図の位置、方向、縮尺に合うように地図をキャリブレーションし、レーダー探知範囲の特定の部分に興味があれば地図をズームする。

マップキャリブレーションを段階的に行う設定アシスタントを使用するか、各設定を個別に編集することができます。

設定アシスタントを使用する:

1. [Radar (レーダー)] > [Map calibration (マップのキャリブレーション)] に移動します。
2. [Setup assistant (設定アシスタント)]をクリックし、手順に従ってください。

アップロードしたマップと追加した設定を削除するには、[Reset calibration (キャリブレーションをリセット)]をクリックします。

各設定を個別に編集する:

各設定を調整すると、マップは徐々にキャリブレーションされます。

1. [Radar (レーダー)] > [Map calibration (マップのキャリブレーション)] > [Map (マップ)] に移動します。

2. アップロードしたい画像を選択するか、指定エリアにドラッグアンドドロップしてください。
   現在のパンとズームの設定でマップ画像を再利用するには、**[Download map (マップをダウンロード)]**をクリックします。
3. [**Rotate map (マップを回転)**] で、スライダーを使用してマップを回転させます。
4. **[Scale and distance on a map (マップ上の縮尺と距離)]**にアクセスし、マップ上のあらかじめ決めた2点をクリックします。
5. **[Distance (距離)]**の下に、マップに追加した2点間の実際の距離を追加します。
6. **[Pan and zoom map (マップのパンとズーム)]**にアクセスし、ボタンを使ってマップ画像をパンしたり、拡大・縮小したりします。

注

ズーム機能ではレーダーのカバー範囲は変わりません。ズーム後、カバー範囲の一部がビューから外れても、レーダーはカバー範囲全体内の動く物体を検知します。撮影シーン内の動きを除外する唯一の方法は、除外範囲を追加することです。詳細については、を参照してください。

7. **[Radar position (レーダーの位置)]**に移動し、ボタンを使ってマップ上のレーダーの位置を移動または回転させます。

アップロードしたマップと追加した設定を削除するには、**[Reset calibration (キャリブレーションをリセット)]**をクリックします。

このビデオでは、AXISレーダーまたはレーダービデオ融合カメラの参照マップをキャリブレーションする方法の例を確認できます。

検知ゾーンの設定

動きを検知する場所を決定するには、1つ以上の検知ゾーンを追加します。ゾーンによってトリガーするアクションが異なります。

ゾーンには次の2種類があります。

- **scenario (シナリオ)** (以前は対象範囲と呼ばれていた) は、動く物体によってルールがトリガーされるエリアです。デフォルトのシナリオはレーダーによってカバーされるエリア全体です。
- [**exclude zone (除外範囲)**] は、動く物体が無視されるエリアです。シナリオ内に不要なアラームが何度もトリガーされる範囲がある場合に、除外範囲を使用します。

シナリオの追加

シナリオは、トリガー条件と検知設定の組み合わせであり、イベントシステムでルールを作成するために使用できます。シーンの部分別に異なるルールを作成する場合は、シナリオを追加します。

シナリオを追加する:

1. [**Radar > Scenarios (レーダー > シナリオ)**] に移動します。
2. [**Add scenario (シナリオの追加)**] をクリックします。
3. シナリオの名前を入力します。
4. 物体がエリアに侵入した場合にトリガーするか、1本または2本のラインを横切った場合にトリガーするかを選択します。

エリア内で動く物体でトリガーする:

1. [Movement in area (エリアへの侵入)] を選択します。
2. **[Next (次へ)]** をクリックします。
3. シナリオに含めるゾーンのタイプを選択します。
   レーダー画像または参照マップの目的の部分が覆われるように、マウスを使用してゾーンを移動し、形状を設定します。
4. **[Next (次へ)]** をクリックします。
5. 検知設定を追加します。
1. [Ignore short-lived objects (一時的な物体を無視)] で、トリガーを発動するまでの秒数を追加します。
2. [Trigger on object type (物体タイプでトリガー)] で、トリガーを発動する物体のタイプを選択します。
3. [Speed limit (速度制限)] で、速度制限の範囲を追加します。
6. **[Next (次へ)]** をクリックします。
7. [Minimum trigger duration (最小トリガー継続時間)] でアラームの最小継続時間を設定します。
8. [保存] をクリックします。

ラインを横断する物体でトリガーする:

1. [Line crossing (ライン横断)] を選択します。
2. **[Next (次へ)]** をクリックします。
3. シーン内にラインを配置します。
   マウスを使用して、ラインを移動したり形状を変更したりします。
4. 検知方向を変更するには、[Change direction (方向の変更)] をオンにします。
5. **[Next (次へ)]** をクリックします。
6. 検知設定を追加します。
   6.1. [Ignore short-lived objects (一時的な物体を無視)] で、トリガーを発動するまでの秒数を追加します。
   6.2. [Trigger on object type (物体タイプでトリガー)] で、トリガーを発動する物体のタイプを選択します。
   6.3. [Speed limit (速度制限)] で、速度制限の範囲を追加します。
7. **[Next (次へ)]** をクリックします。
8. [Minimum trigger duration (最小トリガー継続時間)] でアラームの最小継続時間を設定します。
   デフォルト値は2秒に設定されています。物体がラインを横切るたびにシナリオをトリガーする場合は、継続時間を0秒にします。
9. [保存] をクリックします。

2本のラインを横切る物体でトリガー:

1. [Line crossing (ライン横断)] を選択します。
2. **[Next (次へ)]** をクリックします。
3. 物体が2本のラインを横切ったときにアラームがトリガーされるようにするには、[Require crossing of two lines (2本のラインを横断することが必要)] をオンにします。
4. シーン内にラインを配置します。
   マウスを使用して、ラインを移動したり形状を変更したりします。
5. 検知方向を変更するには、[Change direction (方向の変更)] をオンにします。
6. **[Next (次へ)]** をクリックします。
7. 検知設定を追加します。

7.1. [Max time between crossings (ライン横断間の最大時間)] で、最初のラインを横切ってから2番目のラインを横切るまでの最大時間を設定します。

7.2. [Trigger on object type (物体タイプでトリガー)] で、トリガーを発動する物体のタイプを選択します。

7.3. [Speed limit (速度制限)] で、速度制限の範囲を追加します。

8. **[Next (次へ)]** をクリックします。
9. [Minimum trigger duration (最小トリガー継続時間)] でアラームの最小継続時間を設定します。
   デフォルト値は2秒に設定されています。物体が2本のラインを横切るたびにシナリオをトリガーする場合は、継続時間を0秒にします。
10. [保存] をクリックします。

除外範囲の追加

除外範囲は、動く物体が無視されるエリアです。除外範囲を追加して、たとえば道路脇の揺れる葉が無視されるようにします。除外範囲を追加して、レーダーを反射する素材 (金属フェンスなど) によるゴースト追跡が無視されるようにすることもできます。

除外範囲を追加する:

1. **[Radar (レーダー)] > [Exclude zones (除外範囲)]** に移動します。
2. [Add exclude zone (除外範囲の追加)] をクリックします。
   レーダービューまたは参照マップの目的の部分が覆われるように、マウスを使用してゾーンを移動し、形状を設定します。

装置の自動キャリブレーション

レーダーとビデオの融合カメラの自動キャリブレーションにより、AXIS Object Analyticsで検知された物体の周囲に表示される境界ボックスの精度が向上します。自動キャリブレーションにより、装置は、レーダー検知に基づく境界ボックスの位置決めを改善するために、高さや角度精度などのビデオからの情報を使用します。

注

自動キャリブレーションは検知には影響せず、境界ボックスの視覚化のみに影響します。

高度キャリブレーションを行うには、以下の手順に従います。

1. [Radar > Autocalibration > Elevation (レーダー > 自動キャリブレーション > 高度)] に進みます。
2. [Autocalibration (自動キャリブレーション)] をオンにします。
   自動キャリブレーションは、キャリブレーションデータが利用可能になるとすぐに行われます。
3. [Smoothing (スムージング)] オプションを選択します。
   - シーンで高度の変動が少ない場合は、[Smoothing (スムージング)] を [High (高)] のままにします。
   - シーンが、丘の多いまたは傾いている場合、または階段や高い建物がある場合は、[Smoothing (スムージング)] を [Low (低)] に設定し、高度差を維持します。
4. 以下のオプションを使用して、webインターフェースでキャリブレーションの結果を視覚化します。
   - [Show elevation pattern (高度パターンを表示する)] により、地面からカメラまでの垂直距離が色付きドットのパターンで示されます。
   - [Show color legend (色の凡例を表示する)] により、高度パターンの色と各色が示す垂直距離を含む凡例が表示されます。
   - [Show reference area (参照エリアを表示する)] により、キャリブレーションの基準となるエリアが表示されます。

方位角キャリブレーションを行うには、以下の手順に従います。

1. [Radar > Autocalibration > Azimuth (レーダー > 自動キャリブレーション > 方位角)] に移動します。
2. [Autocalibration (自動キャリブレーション)] をオンにします。
   自動キャリブレーションは、キャリブレーションデータが利用可能になるとすぐに行われます。

レーダーのチルト角度をテキストオーバーレイに表示する

レーダーのライブビューに、レーダーのチルト角度を示すオーバーレイを追加できます。これは、設置時や装置のチルト角度を知る必要がある場合に役立ちます。

注

装置が水平な場合、チルト角度のオーバーレイには「90」と表示されます。オーバーレイに「75」と表示されている場合、レーダーのチルト角度は地平線から15°下になります。

1. [Radar > Overlays (レーダー > 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. 「#op」と入力します。
   [Modifier (修飾子)] をクリックし、リストから [#op] を選択することもできます。
4. 位置を選択します。ライブビューのオーバーレイフィールドをドラッグして位置を変更することもできます。

AXIS Object Analyticsの設定

AXIS Object Analyticsは、動く物体を検知して分類するAIベースのアプリケーションです。また、AXIS Q1656-DLEののレーダーとビデオの融合を設定するための主要なインターフェースでもあります。融合のリアルタイム出力は、アプリケーションで設定したシナリオ内のビデオストリームでのみ見ることができます。

シナリオを作成します

AXIS Object Analyticsのシナリオを使用して、レーダービデオ融合カメラの検知設定とトリガー条件を定義します。

1. 装置のwebインターフェースで、[Apps (アプリ)] > [AXIS Object Analytics] に移動します。
2. アプリケーションを起動し、[Open (開く)] をクリックします。
3. ようこそ画面で、[Step-by-step (段階的な手順)] をクリックし、推奨される設定手順に従います。
4. [Considerations (考慮事項)] で情報を読み、[Finish (完了)] をクリックします。
5. [+ New scenario (+新規シナリオ)] をクリックします。

注

デフォルトでは、[Object in area (物体の対象範囲への侵入)] と [Line crossing (ライン横断)] シナリオは、ビデオとレーダーの両方の入力を使用します。AXIS Object Analyticsの他のシナリオでは、ビデオ入力のみを使用します。

6. 要件に基づいてシナリオを選択します。
7. アプリケーションで検知する物体のタイプを選択します。
8. シナリオを設定します。
9. 設定を確認し、[Finish (完了)] をクリックします。

注

動く物体の周囲に境界ボックスを表示するには、[Settings (設定)] で [Metadata overlay (メタデータオーバーレイ)] をオンにします。ビデオ入力とレーダー入力の両方を使用するシナリオ

と、ビデオ入力のみを使用するシナリオの2つのシナリオを作成すると、動く物体の周囲に2つの境界ボックスが表示されます。この動作は正常です。

これで、AXIS Object Analyticsでシナリオが作成されました。シナリオを変更し、追加の設定を適用するには、[**Open (開く)**] をクリックします。レーダーとビデオの両方の入力を使用するシナリオでは、速度をトリガーとして使用し、検知感度を選択できます。手順については、以下を参照してください。

-
- .

AXIS Object Analyticsとその全般設定の詳細については、*AXIS Object Analyticsユーザーマニュアル*を参照してください。

注

AXIS Object Analyticsユーザーマニュアルに記載されている考慮事項と機能の一部は、レーダービデオ融合カメラには適用されません。

速度を使用してトリガーする

AXIS Object Analyticsで [**Object in area (範囲内の物体)**] または [Line crossing (ライン横断)] シナリオを作成した場合は、設定した速度範囲内、またはそれ以上および以下で移動する物体をトリガーできます。

1. [**Apps (アプリ) > AXIS Object Analytics**] に移動します。
2. アプリケーションを起動し、[**Open (開く)**] をクリックします。
3. 変更するシナリオを選択し、[**Open (開く)**] をクリックします。
4. [**Object speed (物体の速度)**] に進み、[**Use speed to trigger (トリガーに速度を使用する)**] をオンにします。
5. トリガーする速度範囲を設定します。
6. 設定した範囲を上回るまたは下回る速度でトリガーするには、[**Invert (反転)**] をクリックします。

検知感度の選択

検知感度を選択することで、ビデオとレーダーのどちらか一方、または両方での検知をトリガーとすることができます。また、融合アルゴリズムに基づいて装置自体が、どちらか一方の技術に依存するか、あるいは両方に依存するかを決定するようにもできます。

このオプションは [**Object in area (範囲内の物体)**] および [**Line crossing (ライン横断)**] シナリオで使用できます。

1. [**Apps (アプリ) > AXIS Object Analytics**] に移動します。
2. アプリケーションを起動し、[**Open (開く)**] をクリックします。
3. 変更するシナリオを選択し、[**Open (開く)**] をクリックします。
4. [**Detection sensitivity (検知感度)**] に移動し、以下のオプションのいずれかを選択します。
   - **Low sensitivity (低感度)**:レーダーとカメラの両方が物体を検知する必要があります。誤報のリスクは低くなりますが、検知漏れのリスクは高くなります。
     両方の技術で物体を検知できるようにするには、シーンがあまり複雑にならないようにしてください。照明条件が良好であり、検知エリアが両方の技術の検知範囲内にあることが必要で、できれば木や低木などの邪魔になる要素がないことが望まれます。
   - **Automatic (自動)**:物体の検知にレーダーとカメラの両方が必要か、どちらかだけで良いかをアプリケーションが判断します。これはデフォルトのオプションです。
   - **High sensitivity (高感度)**:レーダーとカメラのいずれかが物体を検知する必要があります。誤報のリスクは高くなりますが、検知漏れのリスクは低くなります。

高感度を選択した場合、物体の検知にはどちらか一方の技術だけが必要なため、照明条件や検知エリアのサイズはあまり重要ではありません。

注

自動キャリブレーション機能を使用すると、AXIS Object Analyticsで物体の周囲に表示される境界ボックスの精度を向上させることができます。自動キャリブレーションは検知には影響せず、境界ボックスの表示のみに影響します。

詳細については、を参照してください。

誤報を最小限に抑える

誤報が多すぎるときは、特定の種類の動きや物体をフィルター処理するか、対象範囲を変更する、あるいは検知感度を調節してください。環境に対する最適な設定を特定してください。

- AXIS Object Analyticsの検知感度を調整:
  [Apps > AXIS Object Analytics (アプリ > AXIS Object Analytics)] に移動し、シナリオを開いて、現在より低いDetection sensitivity (検知感度) を選択します。
  - Low sensitivity (低感度):レーダーとカメラの両方が物体を検知する必要があります。誤報のリスクは低くなりますが、検知漏れのリスクは高くなります。
  - Automatic (自動):物体の検知にレーダーとカメラの両方が必要か、どちらかだけでよいかをアプリケーションが判断します。
  - High sensitivity (高感度):レーダーとカメラのいずれかが物体を検知する必要があります。誤報のリスクが増しますが、検知を見逃すリスクは低くなります。
- レーダーの検知感度を調整:
  [Radar > Settings> Detection (レーダー > 設定 > 検知)] に移動して、現在より低い Detection sensitivity (検知感度) を選択します。これにより誤報のリスクは下がりますが、レーダーが特定の動きの検知を見逃すことがあります。
  - 低:この感度は、エリア内に金属物体や大型車両が多いときに使用します。レーダーが物体を追跡および分類するには、より長い時間がかかります。この感度では、特に高速で動く物体の検知範囲が狭くなります。
  - 中間:デフォルトの設定です。
  - 高:この感度は、レーダーの前に金属物体のない広い場所があるときに使用します。この感度では、人の検知範囲が広くなります。
- シナリオと除外範囲を変更する:
  シナリオに金属製の壁などの硬い表面が含まれている場合、1つの物体に対して複数の検知が行われるような反射が生じることがあります。シナリオの形状を変更することも、シナリオの特定の部分を無視する除外ゾーンを追加することもできます。詳細については、および を参照してください。
- 物体が1本のラインではなく2本のラインを横切るとトリガーします。
  ライン横断シナリオに揺らめいている物体や動き回る動物が含まれている場合、物体がたまたまラインを横切って誤報をトリガーするリスクがあります。この場合、物体が2本のラインを横切ったときにのみシナリオをトリガーするように設定できます。詳細については、を参照してください。
- 動きのフィルター処理:
  - [Radar > Settings > Detection (レーダー > 設定 > 検知)] に移動し、[Ignore swaying objects (揺らめいている物体を無視)] を選択します。この設定では、検知対象ゾーン内の木、茂み、旗竿などによる誤報が最小限に抑えられます。
  - [Radar (レーダー)] > [Settings (設定)] > [Detection (検知)] に移動し、[Ignore small objects (小さな物体を無視)] を選択します。この設定では、検知対象ゾーン内の猫やウサギなどの小さな物体による誤報が最小限に抑えられます。
- 時間のフィルター処理:
  - [Radar > Scenarios (レーダー > シナリオ)] に移動します。

  - シナリオを選択し、 ⋮ をクリックして設定を変更します。
  - [Seconds until trigger (トリガーまでの秒数)] で高い値を選択します。これは、レーダーが物体の追跡を開始してから、アラームをトリガーできるまでの遅延時間です。タイマーは、物体がシナリオの指定されたゾーンに入ったときではなく、レーダーが最初に物体を検知したときに開始されます。
- 物体のタイプのフィルター処理:
  - [Radar > Scenarios (レーダー > シナリオ)] に移動します。
  - シナリオを選択し、 ⋮ をクリックして設定を変更します。
  - 特定の物体のタイプでトリガーされないようにするには、このシナリオでイベントをトリガーする物体のタイプの選択を解除します。

注
物体タイプの設定は、レーダーにのみ影響します。これはAXIS Object Analyticsによって無視されます。

イベントのルールを設定する

詳細については、ガイド「*イベントのルールの使用開始*」を参照してください。

動きが検知されないときに電力を節約する

この例では、シーン内で動きが検知されないときに省電力モードをオンにする方法について説明します。

注
省電力モードをオンすると、赤外線照明の範囲が小さくなります。

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

ルールの作成:
1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. [Application (アプリケーション)] の [Object Analytics] を選択します。
4. [Invert this condition (この条件を逆にする)] を選択します。
5. [Power saving mode (省電力モード)] のアクションのリストで、[Use power saving mode while the rule is active (ルールがアクティブである間、省電力モードを使用する)] を選択します。
6. [保存] をクリックします。

誰かが筐体を開いた場合にアラームをトリガーする

この例では、誰かが装置のハウジングまたはケーシングを開けた場合にアラームをトリガーする方法を説明します。

Add a recipient (送信先の追加):
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. [Email (電子メール)] を選択します。

4. 電子メールの送信先のメールアドレスを入力します。
5. 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。
6. 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。
7. [保存] をクリックします。

ルールの作成:

8. [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。
9. ルールの名前を入力します。
10. 条件のリストで、[Casing open (ケーシング開放)] を選択します。
11. 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。
12. リストから送信先を選択します。
13. メールの件名とメッセージを入力します。
14. [保存] をクリックします。

誰かがレーダーを金属製の物体で覆った場合に電子メールを送信する

この例では、金属箔や金属板などの金属製の物体でレーダーを覆うことで誰かがレーダーにいたずらした場合に電子メール通知を送信するルールを作成する方法について説明します。

注

レーダーに対するいたずらイベントのルールを作成するオプションは、AXIS OS 11.11から使用できます。

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. [Email (電子メール)] を選択します。
4. 電子メールの送信先のメールアドレスを入力します。
5. 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。
6. 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。
7. [保存] をクリックします。

ルールの作成:

8. [System > Events (システム > イベント)] に移動し、ルールを追加します。
9. ルールの名前を入力します。
10. 条件リストの [Device status (デバイスステータス)] で、[Radar data failure (レーダーデータの障害)] を選択します。
11. [Reason (理由)] で [Tampering (いたずら)] を選択します。
12. アクションのリストから、[Notifications (通知)] の下の [Send notification to email (電子メールに通知を送信する)] を選択します。
13. 作成した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。

レーダーでPTZカメラを制御する

レーダーからの物体の位置に関する情報を使用して、PTZカメラで物体を追跡することができます。これを行うには、以下の2つの方法があります。

- . 内蔵オプションは、PTZカメラとレーダーを非常に近くに取り付ける場合に適しています。
- . Windowsアプリケーションは、複数のPTZカメラとレーダーを使用して物体を追跡する場合に適しています。

注

NTPサーバーを使用して、カメラとWindowsコンピューターの時刻を同期します。時計が同期していない場合は、追跡の遅延やゴースト追跡が発生する場合があります。

内蔵レーダーオートトラッキングサービスを使用してPTZカメラを制御する

内蔵レーダーオートトラッキングにより、レーダーがPTZカメラを直接制御するエッジツーエッジソリューションが実現します。このサービスはすべてのAxis PTZカメラに対応しています。

注

内蔵レーダーオートトラッキングサービスを使用して、1台のレーダーを1台のPTZカメラに接続できます。複数のレーダーまたはPTZカメラを使用する設定では、AXIS Radar Autotracking for PTZを使用します。詳細については、を参照してください。

この手順では、レーダーとPTZカメラをペアリングする方法、装置を調整する方法、物体の追跡を設定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。

- レーダーに除外範囲を設定することで、対象範囲を定義し、不要なアラームを回避することができます。PTZカメラが無関係な物体を追跡しないように、レーダーを反射する素材や揺らめいている物体 (樹木など) があるゾーンを除外してください。手順については、を参照してください。

レーダーをPTZカメラとペアリングする:

1. [**System > Edge-to-edge > PTZ pairing (システム > エッジツーエッジ > PTZペアリング)**] に移動します。
2. PTZカメラのIPアドレス、ユーザー名、パスワードを入力します。
3. [**接続**] をクリックします。
4. [**Configure Radar autotracking (レーダーオートトラッキングの設定)**] をクリックするか、[**Radar > Radar PTZ autotracking (レーダー > レーダーPTZオートトラッキング)**] に移動して、レーダーオートトラッキングを設定します。

レーダーとPTZカメラのキャリブレーションを行う:

5. [**Radar > Radar PTZ autotracking (レーダー > レーダーPTZオートトラッキング)**] に移動します。
6. カメラの取り付け高さを設定するには、[**Camera mounting height (カメラの取り付け高さ)**] に移動します。
7. レーダーと同じ方向を向くようにPTZカメラをパンするには、[**Pan alignment (パン位置合わせ)**] に移動します。
8. 傾斜した地面を補正するためにチルトを調整する必要がある場合は、[**Ground incline offset (地面の傾斜オフセット)**] に移動し、度単位でオフセットを追加します。

PTZトラッキングを設定する:

9. [**Track (追跡)**] に移動して、人、車両、未知の物体を追跡するかどうかを選択します。
10. PTZカメラで物体のトラッキングを開始するには、[**Tracking (トラッキング)**] をオンにします。
    トラッキングでは、物体または物体グループがカメラの視野に収まるように自動的にズームインされます。

11. 複数の物体がカメラビューに収まらないと予想される場合は、[Object switching (物体の切り替え)] をオンにします。
この設定では、レーダーが追跡する物体に優先順位を付けます。
12. 各物体を何秒間追跡するかを決定するには、[Object hold time (物体の追跡期間)] を設定します。
13. レーダーが物体の追跡を終えたときにPTZカメラをホームポジションに戻すには、[Return to home (ホームに復帰)] をオンにします。
14. PTZカメラがホームに復帰する前に、追跡していた物体を最後に検知した位置にとどまる時間を決定するには、[Return to home timeout (ホームに復帰するまでのタイムアウト)] を設定します。
15. PTZカメラのズームを微調整するには、スライダーでズームを調整します。

AXIS Radar Autotracking for PTZを使用してPTZカメラを制御する

AXIS Radar Autotracking for PTZはサーバーベースのソリューションであり、物体を追跡するときのさまざまな設定に対応できます。

- 1つのレーダーで複数のPTZカメラを制御する。
- 複数のレーダーで1つのPTZカメラを制御する。
- 複数のレーダーで複数のPTZカメラを制御する。
- 同じエリアをカバーする異なる位置に取り付けられているときに、1つのレーダーで1つのPTZカメラを制御する。

このアプリケーションは、特定のPTZカメラに対応しています。詳細については、*axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*を参照してください。

アプリケーションをダウンロードします。アプリケーションの設定方法については、ユーザーマニュアルを参照してください。詳細については、*axis.com/products/axis-radar-autotracking-for-ptz/support*を参照してください。

MQTTを使用してレーダーデータを送信する

レーダービデオ融合カメラとAXIS Speed Monitorアプリケーションを使用して、検知された物体のレーダーデータを収集し、MQTTを介してデータを送信します。

この例では、AXIS Speed Monitorをインストールした装置でMQTTクライアントを設定する方法と、AXIS Speed Monitorで収集したレーダーデータをペイロードとしてMQTTブローカーにパブリッシュする条件を作成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。

- AXIS Speed Monitorをレーダービデオ融合カメラにインストールするか、レーダービデオ融合カメラのレーダーに接続するカメラにインストールします。
詳細については、*AXIS Speed Monitorユーザーマニュアル*を参照してください。
- MQTTブローカーを設定し、ブローカーのIPアドレス、ユーザー名、パスワードを取得します。
MQTTおよびMQTTブローカーの詳細については、*AXIS OS knowledge base (AXIS OS知識ベース)*を参照してください。

AXIS Speed Monitorをインストールした装置のwebインターフェースで、以下のようにMQTTクライアントを設定します。

1. [System (システム)] > [MQTT] > [MQTT client (MQTTクライアント)] > [Broker (ブローカー)] に移動し、次の情報を入力します。
   - [ホスト]:ブローカーのIPアドレス
   - Client ID (クライアントID): 装置のID
   - Protocol (プロトコル):ブローカーが設定したプロトコル
   - ポート:ブローカーが使用するポート番号

– ブローカーの Username (ユーザー名) と Password (パスワード)

2. [Save (保存)]をクリックし、[Connect (接続)]をクリックします。

以下のように、レーダーデータをペイロードとしてMQTTブローカーにパブリッシュする条件を作成します。

3. [System > MQTT > MQTT publication (システム > MQTT > MQTTパブリッシュ)] に移動し、[+ Add condition (+ 条件の追加)] をクリックします。
4. [Application (アプリケーション)] の条件のリストで、[Speed Monitor: Track exited zone (Speed Monitor: 出たゾーンを追跡)] を選択します。

これで、装置はシナリオから出る動く物体ごとにレーダー航跡に関する情報を送信できます。すべての物体には、rmd_zone_name、tracking_id、trigger_countなどの独自のレーダー航跡パラメーターがあります。パラメーターの全リストは、*AXIS Speed Monitorユーザーマニュアル*に記載されています。

カメラが物体を検知したときにビデオを録画する

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

開始する前に、以下をご確認ください。

- SDカードが装着されていることを確認します。

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

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

ルールの作成:

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

進行中のイベントを視覚的に示します

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

必要なハードウェア

- AXIS I/O Indication LED
- Axisネットワークビデオカメラ

注

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

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

1. [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. AXIS I/O Indication LEDの接続先ポートについては、をクリックして方向を[Output (出力)]に設定し、をクリックして通常の状態を[Circuit open (開回路)]に設定します。
3. [System > Events (システム > イベント)] に移動します。
4. 新しいルールを作成します。
5. カメラをトリガーして録画を開始するために満たす必要がある [Condition (条件)] を選択します。たとえば、タイムスケジュールや動体検知などを行うことができます。
6. アクションのリストで、[Record video (ビデオを録画する)] を選択します。ストレージスペースを選択します。ストリームプロファイルを選択するか、新しく作成します。必要に応じて、[Prebuffer (プリバッファ)] と [Postbuffer (ポストバッファ)] も設定します。
7. ルールを保存します。
8. 2番目のルールを作成し、最初のルールと同じ [Condition (条件)] を選択します。
9. アクションのリストから、[Toggle I/O while the rule is active (ルールがアクティブである間、I/Oを切り替える)] を選択し、AXIS I/O Indication LEDに接続されているポートを選択します。状態を [Active (アクティブ)] に設定します。
10. ルールを保存します。

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

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

装置が物体を検知したときにビデオストリームにテキストオーバーレイを表示する

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

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

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

オーバーレイテキストの追加:

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

ルールの作成:

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

4. アクションのリストで [Overlay text (オーバーレイテキスト)] で、[Use overlay text (オーバーレイテキストを使用する)] を選択します。
5. ビデオチャンネルを選択します。
6. [Text (テキスト)] に「動体検知」と入力します。
7. 期間を設定します。
8. [保存] をクリックします。

注

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

PIR検知器が動きを検知したときにビデオを録画する

この例では、Axis PIR検知器 (NC (Normally Closed)) を装置に接続し、検知器が動きを感知したときにビデオ録画を開始するように装置を設定する方法について説明します。

必要なハードウェア

- 3ワイヤーケーブル (アース、電源、I/O)
- PIR検知器、NC (Normally Closed)

注意

ワイヤーを接続する前に、装置を電源から切り離します。すべての接続が完了した後に電源に再接続します。

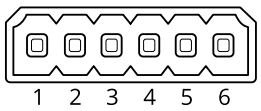
装置のI/Oコネクターにワイヤーを接続する

注

I/Oコネクターについては、を参照してください。

1. アース線をピン1 (GND/-) に接続します。
2. 電源ワイヤーをピン2 (12 V DC出力) に接続します。
3. I/Oワイヤーをピン3 (I/O入力) に接続します。

PIR検知器のI/Oコネクターに配線を接続します



1. アース線のもう一方の端をピン1 (GND/-) に接続します。
2. 電源ワイヤーのもう一方の端をピン2 (DC入力/+) に接続します。
3. I/Oワイヤーのもう一方の端をピン3 (I/O出力) に接続します。

装置のwebインターフェースでI/Oポートを設定する

1. [System > Accessories > I/O ports (システム > アクセサリー > I/O ポート)] に移動します。
2. をクリックして、ポート1の入力方向を設定します。
3. 入力モジュールに分かりやすい名前を付けます (「PIR detector」など)。
4. PIR検知器で動きが感知されるたびにイベントがトリガーされるようにする場合は、 をクリックして、通常状態を閉回路に設定します。

ルールを作成する

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件の一覧で、[PIR detector (PIR検知器)] を選択します。

4. アクションのリストで、[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。

カメラが音量の大きいノイズを検知したときにビデオを録画する

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

注

以下の手順では、マイクが音声入力に接続されている必要があります。

音声をオンにする:

1. 音声を含めるようにストリームプロファイルを設定します (参照)。

音声検知をオンにする:

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

ルールの作成:

1. [System > Events (システム > イベント)] に移動し、ルールを追加します。
2. ルールの名前を入力します。
3. 条件のリストで、[Audio (音声)] の [Audio Detection (音声検知)] を選択します。
4. アクションのリストで、[Recordings (録画)] の [Record video (ビデオを録画する)] を選択します。
5. ストレージオプションのリストで、[SD_DISK] を選択します。
6. 音声がオンになっている場合のストリームプロファイルを選択します。
7. プリバッファ時間を5秒に設定します。
8. ポストバッファ時間を 2分に設定します。
9. [保存] をクリックします。

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、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. [Email (電子メール)] を選択します。
4. 電子メールの送信先のメールアドレスを入力します。
5. デバイス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。
6. 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。

7. [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. 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。

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

装置のwebインターフェースにアクセスするには、Webブラウザーで装置のIPアドレスを入力します。

注

このセクションで説明する機能と設定のサポートは、装置によって異なります。このアイコン は、機能または設定が一部の装置でのみ使用できることを示しています。

メインメニューの表示/非表示を切り取ります。

リリースノートにアクセスします。

製品のヘルプにアクセスします。

言語を変更します。

ライトテーマまたはダークテーマを設定します。

ユーザーメニューは以下を含みます。

- ログインしているユーザーに関する情報。
- **アカウントの変更**:現在のアカウントからログアウトし、新しいアカウントにログインします。
- **ログアウト**:現在のアカウントからログアウトします。

コンテキストメニューは以下を含みます。

- **Analytics data (分析データ)**:個人以外のブラウザーデータの共有に同意します。
- **フィードバック**:フィードバックを共有して、ユーザーエクスペリエンスの向上に役立てます。
- **法的情報**:Cookieおよびライセンスについての情報を表示します。
- **詳細情報**:AXIS OSのバージョンやシリアル番号などの装置情報を表示します。

ステータス

セキュリティ

アクティブな装置へのアクセスのタイプ、使用されている暗号化プロトコル、未署名のアプリが許可されているかが表示されます。設定に関する推奨事項はAXIS OS強化ガイドに基づいています。

強化ガイド:Axis装置でのサイバーセキュリティとベストプラクティスをさらに学習できる*AXIS OS強化ガイド*へのリンクです。

時刻同期ステータス

装置がNTPサーバーと同期しているかどうかや、次の同期までの残り時間など、NTP同期情報を表示します。

NTP settings (NTP設定):NTP設定を表示および更新します。NTPの設定を変更できる [**Time and location (時刻と場所)**] のページに移動します。

進行中の録画

進行中の録画と指定されたストレージ容量を表示します。

録画: 進行中でフィルター処理された録画とそのソースを表示します。詳細については、を参照してください

録画を保存するストレージの空き容量を表示します。

デバイス情報

AXIS OSのバージョンとシリアル番号を含む装置情報を表示します。

Upgrade AXIS OS (AXIS OSのアップグレード):装置のソフトウェアをアップグレードします。アップグレードができる [Maintenance (メンテナンス)] ページに移動します。

接続されたクライアント

接続数と接続されているクライアントの数を表示します。

View details (詳細を表示):接続されているクライアントのリストを表示および更新します。リストには、各接続のIPアドレス、プロトコル、ポート、状態、PID/プロセスが表示されます。

AXIS Image Health Analytics

プリインストールされているアプリケーションのAXIS Image Health Analyticsのステータス、およびアプリケーションで問題が検知されたかどうかが表示されます。

アプリに移動：インストールされているアプリケーションを管理できる**アプリ**ページに移動します。

アプリケーションを開く：新しいブラウザタブでAXIS Image Health Analyticsが開きます。

ビデオ

クリックすると、ライブビデオストリームが再生されます。

クリックすると、ライブビデオストリームが静止します。

クリックすると、ライブビデオストリームのスナップショットを撮影できます。ファイルはご使用のコンピューターの [ダウンロード] フォルダーに保存されます。画像ファイルの名前は、[snapshot_YYYY_MM_DD_HH_MM_SS.jpg] となります。スナップショットの実際のサイズは、スナップショットを受け取るWebブラウザーエンジンから適用される圧縮レベルによって異なります。したがって、スナップショットのサイズは、装置で設定されている実際の圧縮設定とは異なる場合があります。

クリックすると、I/O出力ポートが表示されます。スイッチを使ってポートの回路を開閉し、外部装置のテストなどを行います。

クリックして手動で赤外線照明をオン/オフします。

クリックして手動で白色光を点灯または消灯します。

クリックして画面上のコントロールにアクセスします。

- **Predefined controls (既定のコントロール)**:オンにすると、使用可能な画面上のコントロールが有効になります。
- **Custom controls (カスタムコントロール)**: **[Add custom control (カスタムコントロールの追加)]**をクリックして、画面上のコントロールを追加します。

ウォッシャーを開始します。シーケンスが始まると、カメラは設定された位置に移動し、洗浄スプレーが噴射されます。洗浄シーケンスがすべて終了すると、カメラは元の位置に戻ります。このアイコンは、ウォッシャーが接続され設定されている場合にのみ表示されます。

ワイパーを開始します。

ライブビューのプリセットポジションに移動するには、プリセットポジションをクリックして選択します。または、[**Setup (設定)**] をクリックしてプリセットポジションページに移動します。

フォーカスリコールエリアを追加または削除します。フォーカスリコールエリアを追加すると、カメラは指定したパン/チルト範囲でフォーカス設定を保存します。フォーカスリコールエリアを設定して、カメラがライブビューでそのエリアに入ると、カメラは以前に保存したフォーカスをリコールします。エリアの半分だけでも、カメラはフォーカスをリコールします。

クリックしてガードツアーを選択し、**[Start (スタート)]**をクリックしてガードツアーを再生します。または、[**Setup (設定)**] をクリックしてガードツアーページに移動します。

クリックして、選択した時間の間、手動でヒーターをオンにします。

クリックすると、ライブビデオストリームの連続録画が開始します。録画を停止するには、もう一度クリックします。録画が進行中の場合、再起動後に自動的に再開されます。

クリックすると、装置に設定されているストレージが表示されます。ストレージを設定するには管理者権限が必要です。

クリックすると、その他の設定にアクセスできます。

- **ビデオ形式**:ライブビューで使用するエンコード方式を選択します。
- **自動再生**:オンにすると、この装置を新しいセッションで開くたびにミュートでビデオストリームを自動再生します。
- **クライアントストリームの情報**:オンにすると、ライブビデオストリームを表示するブラウザーで使用されるビデオストリームの動的な情報が表示されます。ビットレートの情報は、情報源が異なるため、テキストオーバーレイで表示される情報とは異なります。クライアントのストリーム情報に含まれるビットレートは、最後の1秒間のビットレートであり、装置のエンコーディングドライバーから取得される数値です。オーバーレイのビットレートは、過去5秒間の平均ビットレートであり、ブラウザーから提供されます。どちらの値も、rawビデオストリームのみを対象としており、UDP/TCP/HTTPを介してネットワーク上で転送される際に発生する追加の帯域幅は含まれていません。
- Adaptive stream (**適応ストリーム**):オンにすると、表示クライアントの実際のディスプレイ解像度に画像解像度が適応し、ユーザーエクスペリエンスが向上し、クライアントのハードウェアの過負荷を防ぐことができます。適応ストリームが適用されるのは、ブラウザーを使用してwebインターフェースにライブビデオストリームを表示しているときだけです。適応ストリームをオンにすると、最大フレームレートは30フレーム/秒になります。適応ストリームをオンにしている間にスナップショットを撮影すると、そのスナップショットには、適応ストリームで選択した画像解像度が使用されます。
- Level grid (**レベルグリッド**): をクリックすると、レベルグリッドが表示されます。このグリッドは、画像が水平方向に配置されているかどうかを判断するのに役立ちます。非表示にするには、 をクリックします。
- Pixel counter (**ピクセルカウンター**): をクリックすると、ピクセルカウンターが表示されます。ボックスをドラッグしてサイズを変更し、特定エリアを含めます。[**Width (幅)**] と [**Height (高さ)**] フィールドでボックスのピクセルサイズを定義することもできます。
- Refresh (**更新**): をクリックすると、ライブビューの静止画像を更新できます。
- **PTZコントロール** :オンにすると、PTZコントロールがライブビューに表示されます。

クリックすると、ライブビューがフル解像度で表示されます。フル解像度が画面サイズより大きい場合は、小さい画像を使って画像内を移動してください。

クリックすると、ライブビデオストリームが全画面表示されます。ESCキーを押すと、全画面モードが終了します。

インストール

キャプチャーモード:キャプチャーモードは、カメラが画像をキャプチャーする方法を定義するプリセット設定です。キャプチャーモードを変更すると、ビューエリアやプライバシーマスクなど、他の多くの設定に影響を与える場合があります。

取り付け位置:カメラのマウント方法によって、画像の向きが変わる場合があります。

Power line frequency (電源周波数):画像のちらつきを最小限に抑えるために、お使いの地域で使用されている周波数を選択してください。アメリカ地域では、通常60 Hzが使用されています。世界の他の部分では、ほとんどの場合50 Hzで使用されています。お客様の地域の電源周波数がわからない場合は、地方自治体に確認してください。

Zoom (ズーム):スライダーを使用してズームレベルを調整します。

Autofocus after zooming (ズーム後にオートフォーカス):ズーム後のオートフォーカスを有効にするにはオンにします。

フォーカス:スライダーを使用してフォーカスを手動で設定します。

Autofocus (オートフォーカス):クリックすると、選択したエリアにカメラのフォーカスを合います。オートフォーカスエリアを選択しない場合、エリア全体にカメラのフォーカスが合わせられます。

Autofocus area (オートフォーカスエリア): をクリックすると、オートフォーカスエリアが表示されます。このエリアには、対象範囲を含める必要があります。

Reset focus (フォーカスのリセット):クリックすると、フォーカスが元の位置に戻ります。

注

寒冷な環境では、ズームとフォーカスが使用可能になるまで数分かかることがあります。

映像補正

重要

複数の画像補正機能を同時に使用することはお勧めできません。使用した場合、パフォーマンスが低下する可能性があります。

たる型歪曲の補正 (BDC) :樽型の歪みが気になる場合はオンにすると、画像がよりまっすぐに補正されます。バレル歪曲 (たる型歪曲) とは、映像が外側に向かって曲がったように見えるレンズ効果のことです。この状態は、映像がズームアウトされたときにより明らかに見られます。

クロップ :スライダーを使用して補正レベルを調整します。レベルを低くすると、映像の幅は保持されますが、映像の高さと解像度に影響が出ます。レベルを高くすると、映像の高さと解像度は保持されますが、映像の幅に影響が出ます。

歪みの除去 :スライダーを使用して補正レベルを調整します。[収縮] にすると、映像の幅は保持されますが、映像の高さと解像度に影響が出ます。[膨張] にすると、映像の高さと解像度は保持されますが、映像の幅に影響が出ます。

動体ブレ補正 :オンにすると、ブレが少なく、よりスムーズで安定した映像が表示されます。ブレ補正は、装置が露出した場所で、たとえば、風や車の通過などによる振動を受ける環境で使用することをお勧めします。

焦点距離 :スライダーを使用して焦点距離を調整します。値を大きくすると倍率が高くなり、画角が狭くなります。値を小さくすると倍率が低くなり、画角が広くなります。

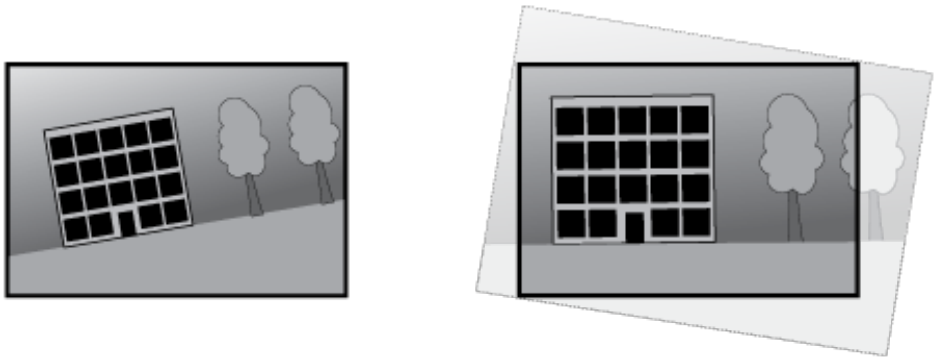
スタビライザーマージン: :スライダーを使用して、ブレを補正する振動のレベルを決める、スタビライザーマージンのサイズを調整します。振動の多い環境に本製品を設置する場合は、スライダーを [**Max (最大)**] 方向に移動します。その結果、より小さなシーンがキャプチャーされます。環境の振動が少ない場合は、スライダーを [**最小 (Min)**] 方向に移動します。

Focus breathing correction (フォーカスブリージング補正) :オンにすると、フォーカスを変更しても画角を一定に保つことができます。この機能を有効にすると、最大までズームインできない場合があります。

画像の歪み補正 :オンにし、スライダーを使用して、画像をデジタルに回転およびトリミングして、水平方向にまっすぐにすることができます。この機能は、カメラを完全に水平に取り付けることができない場合に便利です。ただし、設置時に画像を真っ直ぐになるように調整するのが理想的です。

:クリックすると、画像上にガイドとなるグリッドが表示されます。

:クリックすると、グリッドが非表示になります。



画像が矯正される前と後の画像。

画像

表示

シーンプロファイル:監視シナリオに適したシーンプロファイルを選択します。シーンプロファイルは、カラーレベル、輝度、シャープネス、コントラスト、ローカルコントラストなどの画像設定を、特定の環境や目的に合わせて最適化します。

- **フォレンジック**：監視目的での使用に適したシーンプロファイルです。
- **屋内向け**:屋内環境での使用に適したシーンプロファイルです。
- **屋外対応**:屋外環境での使用に適したシーンプロファイルです。
- **ビビッド**:デモ目的での使用に最適なシーンプロファイルです。
- **トラフィックオーバービュー**:車両の交通監視に適したシーンプロファイルです。
- **ナンバープレート**：ナンバープレートのキャプチャーに最適。

彩度:スライダーを使用して色の強さを調整します。たとえば、グレースケール画像にすることができます。

コントラスト:スライダーを使用して、明暗の差を調整します。

輝度:スライダーを使用して光の強度を調整します。これにより、対象物が見やすくなります。輝度は画像キャプチャーの後で適用され、画像内の情報には影響しません。暗い場所でより詳細に表示するには、ゲインや露光時間を増やすのが一般的です。

Sharpness (シャープネス):スライダーを使ってエッジのコントラストを調整することで、画像内の物体をよりシャープに見せることができます。シャープネスを上げると、ビットレートが上がり、必要なストレージ容量も増加する可能性があります。

ワイドダイナミック レンジ

WDR : 画像の暗い部分と明るい部分の両方が見えるようにする場合にオンにします。

ローカルコントラスト:スライダーで画像のコントラストを調整します。値が大きいほど、暗い部分と明るい部分のコントラストが高くなります。

トーンマッピング:スライダーを使用して、画像に適用されるトーンマッピングの量を調整します。この値を0に設定すると、標準のガンマ補正のみが適用され、この値を大きくすると、画像内の最も暗い部分と最も明るい部分の可視性が高くなります。

ホワイトバランス

届いた光の色温度がカメラで検知される場合は、その色がより自然に見えるように画像を調整することができます。これで十分でない場合は、リストから適切な光源を選択できます。

ホワイトバランスの自動設定では、色のゆらぎを抑えるため、ホワイトバランスが緩やかに変更されます。光源が変わったときや、カメラの電源を初めて投入したときは、新しい光源に適合するまでに最大で30秒かかります。シーン内に色温度が異なる複数のタイプの光源がある場合は、最も支配的な光源が自動ホワイトバランスアルゴリズムの基準になります。この動作を変更するには、基準として使用する光源に合った固定ホワイトバランスの設定を選択してください。

照度環境:

- **Automatic (自動)**:光源の色を自動的に識別し、それに合わせて色を補正します。通常はこの設定をお勧めします。ほとんどの状況で使用できます。
- **自動 - 屋外**:光源の色を自動的に識別し、それに合わせて色を補正します。通常はこの設定をお勧めします。屋外のほとんどの状況で使用できます。
- **カスタム - 屋内**:蛍光灯以外の人工照明がある部屋向けの固定カラー調整。通常の色温度が約2800 Kの場合に適しています。
- **カスタム - 屋外**:色温度が約5500 Kの晴天気象条件向けの固定カラー調整。
- **Fixed - fluorescent 1 (固定 - 蛍光灯1)**:色温度が約4000 Kの蛍光灯向けの固定カラー調整。
- **Fixed - fluorescent 2 (固定 - 蛍光灯2)**:色温度が約3000 Kの蛍光灯向けの固定カラー調整。
- **固定 - 屋内**:蛍光灯以外の人工照明がある部屋向けの固定カラー調整。通常の色温度が約2800 Kの場合に適しています。
- **固定 - 屋外1**:色温度が約5500 Kの晴天気象条件向けの固定カラー調整。
- **固定 - 屋外2**:色温度が約6500 Kの曇天気象条件向けの固定カラー調整。
- **街灯 - 水銀灯**:街灯で一般的に使用される水銀灯の紫外線発光に対する固定カラー調整。
- **街灯 - ナトリウム灯**:街灯で一般的に使用されるナトリウム灯の黄色・オレンジ色を補正する固定カラー調整。
- **Hold current (現在の状態で固定)**:現在の設定を保持し、照度が変化しても補正を行いません。
- **手動**:白色の被写体を利用して、ホワイトバランスを修正します。ライブビュー画像の中で、カメラに白として解釈させる物体に円をドラッグします。[Red balance (レッドバランス)] と [Blue balance (ブルーバランス)] スライダーを使用して、ホワイトバランスを手動で調整します。

デイナイトモード

IR-cut filter (IRカットフィルター):

- [オート]:選択すると、IRカットフィルターのオンとオフが自動的に切り替わります。カメラがデイモードになっていると、IRカットフィルターが有効になり、入射する赤外線照明がフィルターで除去されます。ナイトモードになっていると、IRカットフィルターが無効になり、カメラの光感度が上がります。

注

- 一部の装置では、ナイトモードでIR/パスフィルターが使用されます。IR/パスフィルターは赤外線照明感度を高めますが、可視光を遮断します。
- On (オン):IRカットフィルターをオンにする場合に選択します。画像はカラーですが、光感度は低下します。
- Off (オフ):IRカットフィルターをオフにする場合に選択します。光感度が高くなると、画像は白黒になります。

Threshold (閾値):スライダーを使用して、カメラがデイモードからナイトモードに移行する光の閾値を調整します。

- IRカットフィルターの閾値を低くするには、バーを [Bright (明るい)] の方向に移動します。カメラがナイトモードに変わるタイミングは早くなります。
- IRカットフィルターの閾値を高くするには、スライダーを [Dark (暗い)] の方に移動します。これにより、カメラがナイトモードに変わるタイミングが遅くなります。

赤外線照明

照明が内蔵されていないデバイスでは、これらのコントロールは対応するAxisイルミネーターが接続されている場合にのみ利用できます。

Allow illumination (照明を許可):オンにすると、カメラが内蔵照明をナイトモードで使用できます。

Synchronize illumination (照明の同期):オンにすると、周囲の明るさに合わせて自動的に照明が同期します。昼と夜の同期は、IRカットフィルターが [自動] または [オフ] に設定されている場合にのみ機能します。

自動照明角度:オンにすると、自動照明角度が使用されます。照明角度を手動で設定するには、オフにします。

照明角度:カメラの画角とは異なる角度で照明する必要がある場合などは、スライダーを使って手動で照明の角度を設定できます。カメラが広角であれば、照明の角度をより狭角 (望遠側) に設定できます。ただし、映像の隅の部分が暗くなります。

IR波長:赤外線照明の波長を選択します。

白色光

照明を許可:オンにすると、カメラはナイトモードで白色光を使用します。

照明を同期:オンにすると、周囲の明るさに合わせて自動的に白色光が同期します。

露出

露出モードを選択すると、さまざまなタイプの光源によって生じるちらつきなど、画像内で急速に変化する不規則な影響を緩和できます。自動露出モード、または電源ネットワークと同じ周波数を使用することをお勧めします。

露出モード:

- Automatic (自動):カメラが開口、ゲイン、シャッターを自動的に調整します。
- 自動開口 :カメラが開口とゲインを自動的に調整します。シャッターは固定です。
- 自動シャッター :カメラがシャッターとゲインを自動的に調整します。開口は固定です。
- 現在の状態で固定:現在の露出設定に固定します。
- ちらつき防止 :カメラが開口とゲインを自動的に調整し、次のシャッター速度のみを使用します。1/50秒 (50 Hz) と1/60秒 (60 Hz)。
- ちらつき防止 (50Hz) :カメラが開口とゲインを自動的に調整し、シャッター速度は1/50秒を使用します。
- ちらつき防止 (60Hz) :カメラが開口とゲインを自動的に調整し、シャッター速度は1/60秒を使用します。
- ちらつき低減 :これはちらつき防止と同じですが、明るいシーンでは1/100秒 (50 Hz) および1/120秒 (60 Hz) より速いシャッター速度を使用できます。
- ちらつき低減 (50 Hz) :ちらつき防止と同じですが、明るいシーンでは1/100秒より速いシャッター速度を使用できます。
- ちらつき低減 (60 Hz) :ちらつき防止と同じですが、明るいシーンでは1/120秒より速いシャッター速度を使用できます。
- 手動録画 :開口、ゲイン、シャッターは固定です。

露出エリア :露出エリアを使用すると、入口のドアの前のエリアなど、シーンの選択した部分の露出を最適化できます。

注

露出エリアは元の画像 (回転していない状態) に関連付けられているため、エリアの名前が元の画像に適用されます。つまり、たとえばビデオストリームが90°回転した場合、ストリーム内のゾーンの [Upper (上)] は [Right (右)] になり、[Left (左)」は「Lower (下)」になります。

- Automatic (自動):ほとんどの状況に適しています。
- 中央:画像の中央部の固定エリアを使用して露出が計算されます。このエリアは、ライブビュー内でサイズと位置が固定されています。
- フル :ライブビュー全体を使用して露出が計算されます。
- 上 :画像の上部にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- 下 :画像の下部にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- 左 :画像の左にあるサイズと位置が固定されたエリアを使用して露出が計算されます。

- **右**:画像の右にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- **スポット**:ライブビュー内にあるサイズと位置が固定されたエリアを使用して露出が計算されます。
- **カスタム**:ライブビュー内の一部のエリアを使用して露出が計算されます。エリアのサイズと位置を調整できます。

最大シャッター:最良の画質が得られるように、シャッター速度を選択します。シャッター速度が遅いと (露出が長いと)、動きがあるときに動きによる画像のブレが生じることがあり、シャッター速度が速すぎると画質に影響を与えることがあります。最大ゲインで最大シャッターが機能すると、画質が向上します。

最大ゲイン:適切な最大ゲインを選択します。最大ゲインを増やすと、暗い画像で細部を確認できるレベルは向上しますが、ノイズレベルも増加します。ノイズが多くなると、帯域幅とストレージの使用も多くなる可能性があります。最大ゲインを高い値に設定した場合、昼と夜で照明環境がかなり異なっていると、画像が大きく変化する可能性があります。最大シャッターで最大ゲインが機能すると、画質が向上します。

動き適応型の露出機能:これを選択して低光量下で動きによる画像のブレを減らします。

Blur-noise trade-off (ブレとノイズのトレードオフ):スライダーを使用して動きによる画像のブレとノイズの間で優先度を調整します。動く物体の細部が不鮮明になっても、帯域幅の使用とノイズが少ないことを優先する場合は、このスライダーを [**低ノイズ**] の方に移動します。帯域幅の使用とノイズが多くなっても、動く物体の細部を鮮明に保つことを優先する場合は、スライダーを [**動きによる画像のブレが少ない**] の方に移動します。

注

露出の変更は、露出時間を調整して行うこともゲインを調整しても行うこともできます。露出時間を長くすると動きによる画像のブレが増し、ゲインを大きくするとノイズが増えます。[Blur-noise trade-off (ブレとノイズのトレードオフ)] を [Low noise (低ノイズ)] 側に調整した場合、自動露出にするとゲインを上げることよりも露出時間を長くすることが優先され、トレードオフを [Low motion blur (動きによる画像のブレが少ない)] 側に調整するとその逆になります。低光量の条件下では、設定された優先度にかかわらず、最終的にはゲインと露出時間の両方が最大値に達します。

開口のロック:オンにすると、[Aperture (開口)] スライダーで設定された開口サイズが維持されます。オフにすると、開口サイズをカメラで自動的に調整できます。たとえば、点灯した状態が継続しているシーンで開口をロックすることができます。

開口:スライダーを使用して開口サイズ (レンズからどれだけ光を取り込むか) を調整します。暗い場所でより多くの光をセンサーに取り込み、より明るい画像を得るには、スライダーを [Open (開く)] 方向に移動します。開口を開くと被写界深度は減少し、カメラの近くまたは遠くにある物体はフォーカスが合っていないように見える可能性があります。画像のフォーカスを拡大するには、スライダーを [Closed (閉じる)] 方向に移動します。

露出レベル:スライダーを使用して画像の露出を調整します。

デフォグ機能:オンにすると、霧の影響を検知して自動的に霧を除去するため、より鮮明な画像が得られます。

注

コントラストが低い、光のレベルの変動が大きい、オートフォーカスがわずかにオフの場合は、[Defog (デフォッグ)] をオンにすることをお勧めします。その場合は、映像のコントラストが増大するなど、画質に影響することがあります。また、光量が多すぎる場合にも、デフォッグがオンになると画質に悪影響が出るおそれがあります。

光学知識

温度補正 ：光学部品の温度に基づいてフォーカス位置を補正する場合は、オンにします。

IR補正 ：IRカットフィルターがオフのとき、および赤外線照明があるときに、フォーカス位置を補正する場合は、オンにします。

Calibrate zoom and focus (ズームとフォーカスのキャリブレーション):クリックして、光学部品とズーム/フォーカスの設定を工場出荷時の設定に戻します。輸送中に光学部品のキャリブレーションが失われた場合や、装置が極端な振動にさらされた場合にこれを行う必要があります。

ストリーム

概要

解像度:監視シーンに適した画像の解像度を選択します。解像度が高いと、帯域幅とストレージが増大します。

フレームレート:ネットワーク上の帯域幅の問題を避けるため、またはストレージサイズを削減するために、フレームレートを固定値に制限できます。フレームレートをゼロのままにすると、フレームレートは現在の状況で可能な最大値となります。フレームレートを高くすると、より多くの帯域幅とストレージ容量が必要になります。

Pフレーム:Pフレームは、前のフレームからの画像の変化のみを示す予測画像です。適切なPフレーム数を入力します。値が大きいほど、必要な帯域幅は小さくなります。ただし、ネットワークが輻輳している場合には、ビデオ画質が著しく劣化する可能性があります。

圧縮:スライダーを使用して画像の圧縮率を調整します。圧縮率が高いほどビットレートが低くなり、画質が低下します。圧縮率が低いと画質が向上しますが、録画時により多くの帯域幅とストレージを必要とします。

署名付きビデオ :オンにすると、署名付きビデオ機能がビデオに追加されます。署名付きビデオは、ビデオに暗号化署名を追加することでビデオをいたずらから保護します。

Zipstream

Zipstreamテクノロジーは映像監視用に最適化されたビットレート低減テクノロジーで、H.264またはH.265ストリームの平均ビットレートをリアルタイムで削減します。Axis Zipstream テクノロジーは、動く物体を含むシーンなど、画像内に関心領域が複数あるシーンに対して高いビットレートを適用します。シーンがより静的であれば、Zipstreamは低いビットレートを適用し、ストレージの使用量を削減します。詳細については、「*Axis Zipstreamによるビットレートの低減*」を参照してください。

ビットレート低減の [Strength (強度)] を選択します。
- Off (オフ):ビットレート低減はありません。
- 低:ほとんどのシーンで認識できる画質低下なし。これはデフォルトのオプションです。あらゆるタイプのシーンでビットレートの低減に使用できます。
- 中間:一部のシーンでは、動きのない部分など、関心の低い領域でノイズが少なく、ディテールレベルがやや低くなることで、目に見える効果が得られます。
- 高:一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディテールレベルが低くなることで、目に見える効果が得られます。クラウドに接続された装置やローカルストレージを使用する装置にはこのレベルを推奨します。
- Higher (さらに高):一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディテールレベルが低くなることで、目に見える効果が得られます。
- Extreme (極限):大部分のシーンで目に見える効果が得られます。ビットレートは、可能な限り小さなストレージに最適化されています。

Optimize for storage (ストレージ用に最適化する):オンにし、画質を維持しながらビットレートを最小限に抑えます。この最適化は、Webクライアントに表示されるストリームには適用されません。この機能は、VMSがBフレームをサポートしている場合のみ使用できます。
[Optimize for storage (ストレージ用に最適化)] をオンにすると、[Dynamic GOP (ダイナミックgroup of pictures)] もオンになります。

Dynamic FPS (ダイナミックFPS) (フレーム/秒):オンにすると、シーン内のアクティビティのレベルに応じて帯域幅が変化します。動きが多い場合、より多くの帯域幅が必要です。

下限:シーンの動きに応じて、最小フレーム/秒とストリームのデフォルトフレーム/秒の間でフレームレートを調整するための値を入力します。フレーム/秒が1以下になるような動きの少ないシーンでは、下限を設定することをお勧めします。

Dynamic GOP (ダイナミック group of pictures):オンにすると、シーン内のアクティビティのレベルに応じて、I-フレームの間隔が動的に調整されます。

上限:最大GOP長 (2つのI-フレーム間のP-フレームの最大数) を入力します。Iフレームは、他のフレームとは無関係の自己完結型の画像フレームです。

ビットレート制御

- Average (平均):より長い時間をかけてビットレートを自動的に調整し、使用可能なストレージに基づいて最適な画質を提供する場合に選択します。
  - クリックすると、利用可能なストレージ、保存時間、ビットレート制限に基づいて目標ビットレートが計算されます。
  - Target bitrate (目標ビットレート):目標とするビットレートを入力します。
  - Retention time (保存期間):録画を保存する日数を入力します。
  - ストレージ:ストリームに使用できるストレージの概算が表示されます。
  - Maximum bitrate (最大ビットレート):オンにすると、ビットレートの制限が設定されます。
  - Bitrate limit (ビットレートの制限):目標ビットレートより高いビットレートの制限を入力してください。
- Maximum (最大):オンにすると、ネットワーク帯域幅に基づいてストリームの最大瞬時ビットレートが設定されます。
  - Maximum (最大):最大ビットレートを入力します。
- Variable (可変):オンにすると、シーン内のアクティビティのレベルに基づいてビットレートが変化します。動きが多い場合、より多くの帯域幅が必要です。ほとんどの場合、このオプションをお勧めします。

音声

Include (対象):オンにすると、ビデオストリームで音声が使用されます。

ソース :使用する音声ソースを選択します。

ステレオ :オンにすると、内蔵の音声だけでなく、外部のマイクからの音声も取り込むことができます。

オーバーレイ

+:クリックするとオーバーレイが追加されます。ドロップダウンリストからオーバーレイの種類を次の中から選択します。

- **テキスト**:テキストをライブビュー画像に統合し、すべてのビュー、録画、スナップショットに表示する場合に選択します。独自のテキストを入力することもできます。また、あらかじめ設定された修飾子を含めることで、時間、日付、フレームレートなどを自動的に表示することもできます。
  - : クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - : クリックすると、時間の修飾子%Xを追加して、hh:mm:ss (24時間制) を表示できます。
  - **Modifiers (修飾子)**:クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - **表示**:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- **Image (画像)**:ビデオストリームに静止画像を重ねて表示する場合に選択します。.bmp、.png、.jpeg、または.svgファイルを使用できます。
  画像をアップロードするには、[**Images (画像)**] をクリックします。画像をアップロードする前に、以下の方法を選択できます。
  - **Scale with resolution (解像度に伴う拡大/縮小)**:選択すると、解像度に合わせてオーバーレイ画像のサイズを自動的に変更できます。
  - **Use transparency (透明色を使用する)**:その色のRGB 16進値を選択して入力します。RRGGBB形式を使用します。16進数値の例:FFFFFF - 白、000000 - 黒、FF0000 - 赤、6633FF - 青、669900 - 緑。.bmp画像の場合のみ。
- **シーンの注釈** :カメラが別の方向にパンまたはチルトした場合でも、ビデオストリームに同じ位置に留まるテキストオーバーレイを表示する場合に選択します。特定のズームレベル内でのみオーバーレイを表示するように選択できます。
  - : クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - : クリックすると、時間の修飾子%Xを追加して、hh:mm:ss (24時間制) を表示できます。
  - **Modifiers (修飾子)**:クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - **表示**:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。オーバーレイは保存され、この位置のパンとチルトの座標に残ります。

- Annotation between zoom levels (%) (ズームレベル (%) 間に注釈を表示する): オーバーレイが表示されるズームレベルを設定します。
- Annotation symbol (注釈記号):カメラが設定したズームレベル内にない場合に、オーバーレイの代わりに表示される記号を選択します。

- ストリーミングインジケーター :ビデオストリームに重ね合わせてアニメーションを表示する場合に選択します。このアニメーションは、シーンに動きがなくても、ビデオストリームがライブであることを示します。
  - 表示:アニメーションの色と背景色を選択します。たとえば、透明な背景に赤いアニメーション (デフォルト) などです。
  - サイズ:フォントサイズを選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- Widget:折れ線グラフ :測定値が時間の経過とともにどのように変化しているかを示すグラフを表示します。
  - タイトル:ウィジェットのタイトルを入力します。
  - Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後に配置されます。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
  - サイズ:オーバーレイのサイズを選択します。
  - Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選択しているチャンネルのみに表示されます。オンにすると、アクティブなチャンネルすべてに表示されます。
  - Update interval (更新間隔):データの更新間隔を選択します。
  - Transparency (透明度):オーバーレイ全体の透明度を設定します。
  - Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設定します。
  - Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加されます。
  - X軸
    - ラベル:X軸のテキストラベルを入力します。
    - Time window (時間ウィンドウ):データが表示される時間の長さを入力します。
    - Time unit (時間単位):X軸の時間単位を入力します。
  - Y軸
    - ラベル:Y軸のテキストラベルを入力します。
    - Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ値に自動的に適応します。オフにして、固定スケールの値を手動で入力します。
    - Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大アラーム閾値):これらの値によってグラフに水平基準線が追加され、データ値が高すぎる場合や低すぎる場合に確認しやすくなります。
- Widget:メーター :最近測定されたデータ値を示す棒グラフを表示します。

- タイトル:ウィジェットのタイトルを入力します。
- Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後に配置されます。
- : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- サイズ:オーバーレイのサイズを選択します。
- Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選択しているチャンネルのみに表示されます。オンにすると、アクティブなチャンネルすべてに表示されます。
- Update interval (更新間隔):データの更新間隔を選択します。
- Transparency (透明度):オーバーレイ全体の透明度を設定します。
- Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設定します。
- Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加されます。
- Y軸
  - ラベル:Y軸のテキストラベルを入力します。
  - Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ値に自動的に適応します。オフにして、固定スケールの値を手動で入力します。
  - Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大アラーム閾値):これらの値によって棒グラフに水平基準線が追加され、データ値が高すぎる場合や低すぎる場合に確認しやすくなります。

プライバシーマスク

:クリックすると、新しいプライバシーマスクを作成できます。

Privacy masks (プライバシーマスク):クリックすると、すべてのプライバシーマスクの色を変更したり、すべてのプライバシーマスクを永久に削除したりすることができます。

Cell size (セルのサイズ):モザイクカラーを選択すると、プライバシーマスクはピクセルのようなパターンで表示されます。スライダーを使用して、ピクセルのサイズを変更します。

マスクx: クリックすると、マスクの名前変更、無効化、永久削除を行うことができます。

レーダー

設定

概要

レーダー伝送:これを使用してレーダーモジュールを完全にオフにします。

チャンネル: :複数の装置が互いに干渉する問題が発生した場合は、互いに近い最大4台の装置に対して同じチャンネルを選択します。ほとんどのインストールでは、[**自動 (Auto)**] を選択すると、使用するチャンネルを装置が自動的にネゴシエーションします。

取り付け高さ:製品の取り付け高さを入力します。

注

取り付け高さを入力する際は、できる限り具体的に指定してください。これは、装置が画像内の正しい位置でレーダー検知を可視化するのに役立ちます。

検知

検知感度:レーダーの感度を選択します。値が大きいほど検知範囲は長くなりますが、誤報のリスクも高くなります。感度を低くすると誤報の数は減りますが、検知範囲が短くなる可能性があります。

Radar profile (**レーダープロファイル**):対象範囲に適したプロファイルを選択します。

- Area monitoring (**エリア監視**):オープンエリアで低速で移動する大小両方の物体を追跡します。
  - Ignore stationary rotating objects (**静止した回転物体を無視する**) :ファンやタービンなど、回転運動をする静止物体による誤報を最小限に抑える場合は、オンにします。
  - Ignore small objects (**小さな物体を無視**):猫やウサギなどの小さな物体による誤報を最小限に抑える場合は、オンにします。
  - Ignore swaying objects (**揺らめいている物体を無視**):木、茂み、旗竿などの揺らめいている物体による誤報を最小限に抑える場合は、オンにします。
- Road monitoring (**道路監視**):市街地や郊外の道路で高速で走行する車両を追跡します。
  - Ignore stationary rotating objects (**静止した回転物体を無視する**) :ファンやタービンなど、回転運動をする静止物体による誤報を最小限に抑える場合は、オンにします。
  - Ignore swaying objects (**揺らめいている物体を無視**):木、茂み、旗竿などの揺らめいている物体による誤報を最小限に抑える場合は、オンにします。

表示

情報の凡例:レーダーが検知および追跡できる物体のタイプを示す凡例を表示する場合にオンにします。情報凡例を移動するには、ドラッグアンドドロップします。

ゾーンの不透明度:検知ゾーンの不透明度または透明度を選択します。

グリッドの不透明度:グリッドの透明度または不透明度を選択します。

配色:レーダーの可視化に使用するテーマを選択します。

回転 :希望するレーダー画像の向きを選択します。

物体の可視化

Trail lifetime (証跡の存続時間):追跡対象の物体の証跡をレーダービューに表示されたままにする時間を選択します。

アイコンのスタイル:レーダービューで追跡する物体のアイコンスタイルを選択します。三角定規の場合は、[**Triangle (三角形)**] を選択します。代表的な記号の場合は、[**Symbol (記号)**] を選択します。アイコンは、スタイルに関係なく、追跡する物体が動く方向を指します。

Show information with icon (アイコンで情報を表示):追跡対象の物体のアイコンの横に表示する情報を選択します。

- **Object type (物体のタイプ)**:レーダーが検知した物体のタイプを表示します。
- **Classification probability (等級確率)**:レーダーがどのくらいの確度で物体を分類したかを表示します。
- **Velocity (速度)**:物体がどのくらいの速度で移動しているかを表示します。

ストリーム

概要

解像度:監視シーンに適した画像の解像度を選択します。解像度が高いと、帯域幅とストレージが増大します。

フレームレート:ネットワーク上の帯域幅の問題を避けるため、またはストレージサイズを削減するために、フレームレートを固定値に制限できます。フレームレートをゼロのままにすると、フレームレートは現在の状況で可能な最大値となります。フレームレートを高くすると、より多くの帯域幅とストレージ容量が必要になります。

Pフレーム:Pフレームは、前のフレームからの画像の変化のみを示す予測画像です。適切なPフレーム数を入力します。値が大きいほど、必要な帯域幅は小さくなります。ただし、ネットワークが輻輳している場合には、ビデオ画質が著しく劣化する可能性があります。

圧縮:スライダーを使用して画像の圧縮率を調整します。圧縮率が高いほどビットレートが低くなり、画質が低下します。圧縮率が低いと画質が向上しますが、録画時により多くの帯域幅とストレージを必要とします。

署名付きビデオ :オンにすると、署名付きビデオ機能がビデオに追加されます。署名付きビデオは、ビデオに暗号化署名を追加することでビデオをいたずらから保護します。

Zipstream

Zipstreamテクノロジーは映像監視用に最適化されたビットレート低減テクノロジーで、H.264またはH.265ストリームの平均ビットレートをリアルタイムで削減します。Axis Zipstream テクノロジーは、動く物体を含むシーンなど、画像内に関心領域が複数あるシーンに対して高いビットレートを適用します。シーンがより静的であれば、Zipstreamは低いビットレートを適用し、ストレージの使用量を削減します。詳細については、「*Axis Zipstreamによるビットレートの低減*」を参照してください。

ビットレート低減の [Strength (強度)] を選択します。
- Off (オフ):ビットレート低減はありません。
- 低:ほとんどのシーンで認識できる画質低下なし。これはデフォルトのオプションです。あらゆるタイプのシーンでビットレートの低減に使用できます。
- 中間:一部のシーンでは、動きのない部分など、関心の低い領域でノイズが少なく、ディテールレベルがやや低くなることで、目に見える効果が得られます。
- 高:一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディテールレベルが低くなることで、目に見える効果が得られます。クラウドに接続された装置やローカルストレージを使用する装置にはこのレベルを推奨します。
- Higher (さらに高):一部のシーンでは、動きのない部分など、関心の低い範囲でノイズが少なく、ディテールレベルが低くなることで、目に見える効果が得られます。
- Extreme (極限):大部分のシーンで目に見える効果が得られます。ビットレートは、可能な限り小さなストレージに最適化されています。

Optimize for storage (ストレージ用に最適化する):オンにし、画質を維持しながらビットレートを最小限に抑えます。この最適化は、Webクライアントに表示されるストリームには適用されません。この機能は、VMSがBフレームをサポートしている場合のみ使用できます。
[Optimize for storage (ストレージ用に最適化)] をオンにすると、[Dynamic GOP (ダイナミックgroup of pictures)] もオンになります。

Dynamic FPS (ダイナミックFPS) (フレーム/秒):オンにすると、シーン内のアクティビティのレベルに応じて帯域幅が変化します。動きが多い場合、より多くの帯域幅が必要です。

下限:シーンの動きに応じて、最小フレーム/秒とストリームのデフォルトフレーム/秒の間でフレームレートを調整するための値を入力します。フレーム/秒が1以下になるような動きの少ないシーンでは、下限を設定することをお勧めします。

Dynamic GOP (ダイナミック group of pictures):オンにすると、シーン内のアクティビティのレベルに応じて、I-フレームの間隔が動的に調整されます。

上限:最大GOP長 (2つのI-フレーム間のP-フレームの最大数) を入力します。Iフレームは、他のフレームとは無関係の自己完結型の画像フレームです。

ビットレート制御

- Average (平均):より長い時間をかけてビットレートを自動的に調整し、使用可能なストレージに基づいて最適な画質を提供する場合に選択します。
  - クリックすると、利用可能なストレージ、保存時間、ビットレート制限に基づいて目標ビットレートが計算されます。
  - Target bitrate (目標ビットレート):目標とするビットレートを入力します。
  - Retention time (保存期間):録画を保存する日数を入力します。
  - ストレージ:ストリームに使用できるストレージの概算が表示されます。
  - Maximum bitrate (最大ビットレート):オンにすると、ビットレートの制限が設定されます。
  - Bitrate limit (ビットレートの制限):目標ビットレートより高いビットレートの制限を入力してください。
- Maximum (最大):オンにすると、ネットワーク帯域幅に基づいてストリームの最大瞬時ビットレートが設定されます。
  - Maximum (最大):最大ビットレートを入力します。
- Variable (可変):オンにすると、シーン内のアクティビティのレベルに基づいてビットレートが変化します。動きが多い場合、より多くの帯域幅が必要です。ほとんどの場合、このオプションをお勧めします。

音声

Include (対象):オンにすると、ビデオストリームで音声が使用されます。

ソース :使用する音声ソースを選択します。

ステレオ :オンにすると、内蔵の音声だけでなく、外部のマイクからの音声も取り込むことができます。

マップキャリブレーション

マップキャリブレーションを使用して、参照マップをアップロードし、キャリブレーションします。キャリブレーションの結果、レーダーのカバー範囲を適切な縮尺で表示する参照地図ができるため、物体が移動している場所を容易に確認できます。

設定アシスタント:クリックすると設定アシスタントが開き、キャリブレーションをステップバイステップでガイドします。

キャリブレーションのリセット:クリックすると、現在のマップ画像とマップ上のレーダー位置が削除されます。

マップ

Upload map (マップのアップロード):アップロードするマップ画像を選択するか、ドラッグアンドドロップします。

Download map (マップをダウンロード):クリックしてマップをダウンロードします。

Rotate map (地図を回転):スライダーを使用してマップを回転させます。

マップ上の縮尺と距離

Distance (距離):マップに追加した2点間の実際の距離を追加します。

マップのパンとズーム

パン:ボタンをクリックするとマップ画像がパンします。

ズーム:ボタンをクリックすると、マップ画像がズームインまたはズームアウトします。

パンとズームをリセット:クリックすると、パンとズームの設定が削除されます。

レーダーの位置

位置:ボタンをクリックすると、マップ上のレーダーが移動します。

回転:ボタンをクリックすると、マップ上のレーダーが回転します。

除外範囲

[exclude zone (除外範囲)] は、動く物体が無視されるエリアです。シナリオ内に不要なアラームが何度もトリガーされる範囲がある場合に、除外範囲を使用します。

＋ :クリックして、新しい除外範囲を作成します。

除外範囲を変更するには、リストから除外範囲を選択します。

Track passing objects (通過する物体を追跡する):除外範囲を通過する物体を追跡する場合にオンにします。通過する物体はトラックIDを保持し、ゾーン全体で表示されます。除外範囲内から現れる物体は追跡されません。

Zone shape presets (範囲形状のプリセット):除外範囲の初期形状を選択します。

- Cover everything (すべてをカバー):レーダーの検知範囲全体をカバーする除外範囲を設定する場合に選択します。
- Reset to box (ボックスにリセット):検知範囲の中央に四角形の除外範囲を配置する場合に選択します。

範囲の形状に変更を加えるには、ライン上の任意のポイントをドラッグアンドドロップします。ポイントを削除するには、ポイント上で右クリックします。

シナリオ

シナリオは、トリガー条件と、シーンおよび検知設定との組み合わせです。

＋:クリックすると、新しいシナリオが作成されます。シナリオは最大20個まで作成できます。

Triggering conditions (トリガー条件):アラームをトリガーする条件を選択します。
- Movement in area (エリアへの侵入):物体がエリアに侵入したらシナリオをトリガーする場合に選択します。
- ライン横断:物体が1本または2本のラインを横切ったらシナリオをトリガーする場合に選択します。

Scene (シーン):移動する物体がアラームをトリガーするシナリオ内のエリアまたはラインを定義します。
- [Movement in area (エリアへの侵入)] では、形状プリセットのいずれかを選択してエリアに修正を加えます。
- [Line crossing (ライン横断)] では、シーン内にラインをドラッグアンドドロップします。ライン上にさらにポイントを作成するには、ライン上の任意の場所をクリックしてドラッグします。ポイントを削除するには、ポイント上で右クリックします。
  - Require crossing of two lines (2本のラインを横断することが必要):シナリオがアラームをトリガーするまでに物体が2本のラインを横切る必要がある場合は、オンにします。
  - Change direction (方向の変更): 物体が反対方向にラインを横切ったらシナリオがアラームをトリガーする場合に、オンにします。

Detection settings (検知設定):シナリオのトリガー条件を定義します。
- [Movement in area (エリアへの侵入)] の場合:
  - Ignore short-lived objects (一時的な物体を無視):レーダーが物体を検知してからシナリオがアラームをトリガーするまでの遅延時間を秒単位で設定します。これにより、誤報を減らすことができます。
  - Trigger on object type (トリガーとなる物体のタイプ):シナリオをトリガーする物体のタイプ (人、車両、不明) を選択します。
  - Speed limit (速度制限):特定の速度範囲内で移動する物体でトリガーします。
    - Invert (反転する):設定した速度制限を上回ったか下回ったらトリガーする場合に選択します。
- [Line crossing (ライン横断)] の場合:
  - Ignore short-lived objects (一時的な物体を無視):レーダーが物体を検知してからシナリオがアクションをトリガーするまでの遅延時間を秒単位で設定します。これにより、誤報を減らすことができます。このオプションは、2本のラインを横切る物体には使用できません。
  - Max time between crossings (ライン横断間の最大時間):最初のラインを横切ってから2番目のラインを横切るまでの最大時間を設定します。このオプションは、2本のラインを横切る物体にのみ使用できます。
  - Trigger on object type (トリガーとなる物体のタイプ):シナリオをトリガーする物体のタイプ (人、車両、不明) を選択します。
  - Speed limit (速度制限):特定の速度範囲内で移動する物体でトリガーします。
    - Invert (反転する):設定した速度制限を上回ったか下回ったらトリガーする場合に選択します。

Alarm settings (アラーム設定):アラームの条件を定義します。
- Minimum trigger duration (最小トリガー継続時間):トリガーされるアラームの最小継続時間を設定します。

オーバーレイ

+:クリックするとオーバーレイが追加されます。ドロップダウンリストからオーバーレイの種類を次の中から選択します。

- **テキスト**:テキストをライブビュー画像に統合し、すべてのビュー、録画、スナップショットに表示する場合に選択します。独自のテキストを入力することもできます。また、あらかじめ設定された修飾子を含めることで、時間、日付、フレームレートなどを自動的に表示することもできます。
  - : クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - : クリックすると、時間の修飾子%Xを追加して、hh:mm:ss (24時間制) を表示できます。
  - **Modifiers (修飾子)**:クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - **表示**:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- **Image (画像)**:ビデオストリームに静止画像を重ねて表示する場合に選択します。.bmp、.png、.jpeg、または.svgファイルを使用できます。
  画像をアップロードするには、[**Images (画像)**] をクリックします。画像をアップロードする前に、以下の方法を選択できます。
  - **Scale with resolution (解像度に伴う拡大/縮小)**:選択すると、解像度に合わせてオーバーレイ画像のサイズを自動的に変更できます。
  - **Use transparency (透明色を使用する)**:その色のRGB 16進値を選択して入力します。RRGGBB形式を使用します。16進数値の例:FFFFFF - 白、000000 - 黒、FF0000 - 赤、6633FF - 青、669900 - 緑。.bmp画像の場合のみ。
- **シーンの注釈** :カメラが別の方向にパンまたはチルトした場合でも、ビデオストリームに同じ位置に留まるテキストオーバーレイを表示する場合に選択します。特定のズームレベル内でのみオーバーレイを表示するように選択できます。
  - : クリックすると、日付の修飾子%Fを追加して、yyyy-mm-ddを表示できます。
  - : クリックすると、時間の修飾子%Xを追加して、hh:mm:ss (24時間制) を表示できます。
  - **Modifiers (修飾子)**:クリックすると、リストに表示された修飾子から選択して、テキストボックスに追加できます。たとえば、%aを選択すると曜日が表示されます。
  - **サイズ**:フォントサイズを選択します。
  - **表示**:黒い背景に白いテキスト (デフォルト) など、背景色とテキストの色を選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。オーバーレイは保存され、この位置のパンとチルトの座標に残ります。

- Annotation between zoom levels (%) (ズームレベル (%) 間に注釈を表示する): オーバーレイが表示されるズームレベルを設定します。
- Annotation symbol (注釈記号):カメラが設定したズームレベル内にない場合に、オーバーレイの代わりに表示される記号を選択します。

- ストリーミングインジケーター :ビデオストリームに重ね合わせてアニメーションを表示する場合に選択します。このアニメーションは、シーンに動きがなくても、ビデオストリームがライブであることを示します。
  - 表示:アニメーションの色と背景色を選択します。たとえば、透明な背景に赤いアニメーション (デフォルト) などです。
  - サイズ:フォントサイズを選択します。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- Widget:折れ線グラフ :測定値が時間の経過とともにどのように変化しているかを示すグラフを表示します。
  - タイトル:ウィジェットのタイトルを入力します。
  - Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後に配置されます。
  - : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
  - サイズ:オーバーレイのサイズを選択します。
  - Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選択しているチャンネルのみに表示されます。オンにすると、アクティブなチャンネルすべてに表示されます。
  - Update interval (更新間隔):データの更新間隔を選択します。
  - Transparency (透明度):オーバーレイ全体の透明度を設定します。
  - Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設定します。
  - Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加されます。
  - X軸
    - ラベル:X軸のテキストラベルを入力します。
    - Time window (時間ウィンドウ):データが表示される時間の長さを入力します。
    - Time unit (時間単位):X軸の時間単位を入力します。
  - Y軸
    - ラベル:Y軸のテキストラベルを入力します。
    - Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ値に自動的に適応します。オフにして、固定スケールの値を手動で入力します。
    - Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大アラーム閾値):これらの値によってグラフに水平基準線が追加され、データ値が高すぎる場合や低すぎる場合に確認しやすくなります。
- Widget:メーター :最近測定されたデータ値を示す棒グラフを表示します。

- タイトル:ウィジェットのタイトルを入力します。
- Overlay modifier (オーバーレイ修飾子):データソースとしてオーバーレイ修飾子を選択します。MQTTオーバーレイを作成済みである場合、これらはリストの最後に配置されます。
- : 画像内でオーバーレイの位置を選択したり、オーバーレイをクリック＆ドラッグしてライブビュー内で移動させたりできます。
- サイズ:オーバーレイのサイズを選択します。
- Visible on all channels (すべてのチャンネルで表示する):オフにすると、現在選択しているチャンネルのみに表示されます。オンにすると、アクティブなチャンネルすべてに表示されます。
- Update interval (更新間隔):データの更新間隔を選択します。
- Transparency (透明度):オーバーレイ全体の透明度を設定します。
- Background transparency (背景の透明度):オーバーレイの背景のみの透明度を設定します。
- Points (ポイント):オンにすると、データ更新時にグラフラインにポイントが追加されます。
- Y軸
  - ラベル:Y軸のテキストラベルを入力します。
  - Dynamic scale (ダイナミックスケール):オンにすると、スケールがデータ値に自動的に適応します。オフにして、固定スケールの値を手動で入力します。
  - Min alarm threshold (最小アラーム閾値) とMax alarm threshold (最大アラーム閾値):これらの値によって棒グラフに水平基準線が追加され、データ値が高すぎる場合や低すぎる場合に確認しやすくなります。

レーダーPTZオートトラッキング:

レーダーをPTZカメラとペアリングして、レーダーオートトラッキングを使用します。接続を確立するには、[System (システム)] > [Edge-to-edge (エッジツーエッジ)] に移動します。

初期設定を構成する:

Camera mounting height (カメラの取り付け高さ):地面から取り付けたPTZカメラの高さまでの距離です。

Pan alignment (パン位置合わせ):PTZカメラがレーダーと同じ方向を向くようにパンします。PTZカメラのIPアドレスをクリックすると、そのカメラにアクセスします。

Save pan offset (パンオフセットの保存):クリックして、パン位置合わせを保存します。

Ground incline offset (地面の傾斜オフセット):地面の傾斜オフセットを使用して、カメラのチルトを微調整します。地面が傾いていたり、カメラが水平に取り付けられていないと、物体のトラッキング時にカメラが上下を向きすぎる場合があります。

Done (完了):クリックして、設定を保存し、構成を続行します。

PTZオートトラッキングの設定:

トラック:人、車両、未知の物体を追跡するかどうかを選択します。

トラッキング:PTZカメラで物体のトラッキングを開始する場合は、オンにします。トラッキングでは、物体または物体グループがカメラの視野に収まるように自動的にズームインされます。

物体の切り替え:レーダーがPTZカメラの視野に収まらない複数の物体を検知すると、PTZカメラは最も優先度の高い物体を追跡し、その他の物体は無視します。

物体の追跡期間:PTZカメラが各物体を追跡する秒数を指定します。

ホームに復帰:レーダーが物体を追跡しなくなったらPTZカメラをホームポジションに戻す場合は、オンにします。

Return to home timeout (ホームに復帰するまでのタイムアウト):PTZカメラがホームに復帰する前に、追跡していた物体を最後に検知した位置に留まる時間を決定します。

ズーム:スライダーを使用してPTZカメラのズームを微調整します。

Reconfigure installation (インストールを再設定):クリックすると、すべての設定がクリアされ、初期設定に戻ります。

自動キャリブレーション

仰角

Status (ステータス):キャリブレーションデータが使用可能かどうかを示します。カメラとレーダーは、継続的にキャリブレーションデータを収集します。

Autocalibration (自動キャリブレーション):オンにすると、シーンの自動キャリブレーションを行います。自動キャリブレーションは、キャリブレーションデータが利用可能になるとすぐに行われます。利用可能かどうかのステータスを確認してください。

Smoothing (スムージング):高度差を滑らかにします。

- **高**:高度差が小さいシーンでは、スムージングを [**High (高)**] に設定します。
- **低**:高度差が大きいシーン (丘や階段など) では、スムージングを [**Low (低)**] に設定します。

Reset (リセット):自動キャリブレーションと収集されたキャリブレーションデータをリセットします。

Show elevation pattern (高度パターンを表示する):オンにすると、キャリブレーションが視覚化されます。色のついた点のパターンで、地面からカメラまでの垂直距離を表示します。このパターンは、このページにのみ表示され、ビデオストリームやレーダーストリームには表示されません。

Show color legend (色の凡例を表示する):オンにすると、高度パターンの色と各色が示す垂直距離を表す凡例が表示されます。凡例はこのページにのみ表示され、ビデオストリームやレーダーストリームには表示されません。

カラー:高度パターンの色を選択します。

Show reference area (参照エリアを表示する):オンにすると、キャリブレーションの基準となるエリアが表示されます。このエリアはこのページにのみ表示され、ビデオストリームやレーダーストリームには表示されません。

Azimuth (方位角)

Status (ステータス):キャリブレーションデータが使用可能かどうかを示します。カメラとレーダーは、継続的にキャリブレーションデータを収集します。

Autocalibration (自動キャリブレーション):オンにすると、シーンの自動キャリブレーションを行います。自動キャリブレーションは、キャリブレーションデータが利用可能になるとすぐに行われます。利用可能かどうかのステータスを確認してください。

Reset (リセット):自動キャリブレーションと収集されたキャリブレーションデータをリセットします。

分析機能

AXIS Object Analytics

開始:クリックして、AXIS Object Analyticsを開始します。アプリケーションはバックグラウンドで実行され、アプリケーションの現在の設定に基づいてイベントのルールを作成できます。

開く:クリックして、AXIS Object Analyticsを開きます。アプリケーションは新しいブラウザタブで開き、そこで設定を行うことができます。

- **インストールされていません**:この装置にはAXIS Object Analyticsがインストールされていません。AXIS OSを最新バージョンにアップグレードし、最新バージョンのアプリケーションを入手してください。

AXIS Image Health Analytics

開始:クリックして、AXIS Image Health Analyticsを起動します。アプリケーションはバックグラウンドで実行され、アプリケーションの現在の設定に基づいてイベントのルールを作成できます。

開く:クリックして、AXIS Image Health Analyticsを開きます。アプリケーションは新しいブラウザタブで開き、そこで設定を行うことができます。

- **インストールされていません**:この装置にはAXIS Image Health Analyticsがインストールされていません。AXIS OSを最新バージョンにアップグレードし、最新バージョンのアプリケーションを入手してください。

メタデータの可視化

カメラは動く物体を検知し、物体のタイプに応じて分類します。ビューでは、分類された物体の周りに色付きの境界ボックスが表示され、その物体に割り当てられたIDも示されます。

Id：識別された物体とそのタイプに対応する一意の識別番号。この番号はリストとビューの両方に示されます。

タイプ:動く物体を人、顔、自動車、バス、トラック、自転車、またはナンバープレートとして分類します。境界ボックスの色は、分類されたタイプによって異なります。

Confidence (信頼度):バーは物体のタイプの分類における信頼度を示します。

メタデータの設定

RTSPメタデータプロデューサー

メタデータをストリーミングするアプリと、それらのアプリが使用するチャンネルが一覧表示されます。

注

これは、ONVIF XMLを使用しているRTSPメタデータストリームの設定です。ここで行った変更は、メタデータ視覚化ページには影響しません。

Producer (プロデューサー):メタデータを生成するアプリ。アプリの下には、アプリが装置からストリーミングするメタデータのタイプのリストがあります。

チャンネル:アプリが使用するチャンネル。メタデータストリームを有効にするには、選択します。互換性またはリソース管理の理由から選択を解除します。

音声

デバイスの設定

入力:音声入力のオン/オフを切り替えます。入力のタイプを表示します。

入力タイプ:内蔵マイクやライン入力など、入力のタイプを選択します。

電源タイプ:入力の電源タイプを選択します。

変更を適用する:選択した内容を適用します。

エコーキャンセル:オンにすると、双方向通信時のエコーが除去されます。

個別のゲインコントロール:オンにすると、入力タイプごとに個別にゲインを調整することができます。

自動ゲインコントロール:オンにすると、サウンドの変化に合わせてゲインが動的に調整されます。

Gain (ゲイン):スライダーを使用してゲインを変更します。マイクのアイコンをクリックすると、ミュート、ミュート解除ができます。

出力:出力のタイプを表示します。

Gain (ゲイン):スライダーを使用してゲインを変更します。スピーカーのアイコンをクリックすると、ミュート、ミュート解除ができます。

自動音量制御:これをオンにすると、デバイスで周囲の騒音レベルに基づいてゲインが自動的かつ動的に調整されるようになります。自動音量制御は、ラインとテレコイルを含め、すべての音声出力に影響します。

ストリーム

エンコード方式:入力ソースストリーミングに使用するエンコード方式を選択します。エンコード方式は、音声入力がオンになっている場合にのみ選択できます。音声入力がオフになっている場合は、[Enable audio input (音声入力を有効にする)] をクリックしてオンにします。

音声クリップ

クリップを追加:新しい音声クリップを追加します。au、.mp3、.opus、.vorbis、.wavファイルを使用できます。

音声クリップを再生します。

音声クリップの再生を停止します。

コンテキストメニューは以下を含みます。

- **Rename (名前の変更)**:オーディオクリップの名前を変更します。
- **Create link (リンクを作成)**:使用する場合は、音声クリップを装置上で再生するURLを作成します。クリップの音量と再生回数を指定します。
- **Download (ダウンロード)**:音声クリップをコンピューターにダウンロードします。
- **削除**:装置から音声クリップを削除します。

音声エンハンスメント

入力

Ten Band Graphic Audio Equalizer (10バンドグラフィック音声イコライザー):オンに設定して、音声信号内の異なる周波数帯域のレベルを調整します。この機能は、音声の設定経験のある上級ユーザー向けです。

トークバック範囲:音声コンテンツを収集する動作範囲を選択します。動作範囲を広げると、同時双方向通信機能が低下します。

音声強化:オンにすると、他の音声との関連で音声コンテンツが強化されます。

録画

進行中の録画:装置で進行中のすべての録画を表示します。

装置で録画を開始します。

保存先のストレージ装置を選択します。

装置で録画を停止します。

トリガーされた録画は、手動で停止したとき、または装置がシャットダウンされたときに終了します。

連続録画は、手動で停止するまで続行されます。装置がシャットダウンされた場合でも、録画は装置が再起動されるときまで続行されます。

録画を再生します。

録画の再生を停止します。

録画に関する情報とオプションを表示または非表示にします。

Set export range (エクスポート範囲の設定):録画の一部のみをエクスポートする場合は、時間範囲を入力します。装置の位置とは異なるタイムゾーンで作業する場合は、時間範囲が装置のタイムゾーンに基づくことに注意してください。

Encrypt (暗号化):エクスポートする録画のパスワードを設定する場合に選択します。エクスポートしたファイルをパスワードなしで開くことができなくなります。

クリックすると、録画が削除されます。

Export (エクスポート):録画の全体または一部をエクスポートします。

クリックして録画にフィルターを適用します。

From (開始):特定の時点以降に行われた録画を表示します。

To (終了):特定の時点までに行われた録画を表示します。

ソース:ソースに基づいて録画を表示します。ソースはセンサーを指します。

Event (イベント):イベントに基づいて録画を表示します。

ストレージ:ストレージタイプに基づいて録画を表示します。

アプリ

アプリを追加:新しいアプリをインストールします。

さらにアプリを探す:インストールする他のアプリを見つける。Axisアプリの概要ページに移動します。

署名されていないアプリを許可 :署名なしアプリのインストールを許可するには、オンにします。

AXIS OSおよびACAPアプリのセキュリティ更新プログラムを表示します。

注
複数のアプリを同時に実行すると、装置のパフォーマンスが影響を受ける可能性があります。

アプリ名の横にあるスイッチを使用して、アプリを起動または停止します。

開く:アプリの設定にアクセスする。利用可能な設定は、アプリケーションよって異なります。一部のアプリケーションでは設定が設けられていません。

コンテキストメニューに、以下のオプションが1つ以上含まれていることがあります。

- Open-source license (オープンソースライセンス):アプリで使用されているオープンソースライセンスに関する情報が表示されます。
- App log (アプリのログ):アプリイベントのログが表示されます。このログは、サポートにご連絡いただく際に役立ちます。
- **キーによるライセンスのアクティブ化**:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできない場合は、このオプションを使用します。
  ライセンスキーがない場合は、*axis.com/products/analytics*にアクセスします。ライセンスキーを入手するには、ライセンスコードとAxis製品のシリアル番号が必要です。
- **ライセンスの自動アクティブ化**:アプリにライセンスが必要な場合は、ライセンスを有効にする必要があります。装置がインターネットにアクセスできる場合は、このオプションを使用します。ライセンスをアクティブ化するには、ライセンスコードが必要です。
- Deactivate the license (ライセンスの非アクティブ化):試用ライセンスから正規ライセンスに変更する場合など、別のライセンスと交換するために現在のライセンスを無効にします。ライセンスを非アクティブ化すると、ライセンスはデバイスから削除されます。
- Settings (設定):パラメーターを設定します。
- **削除**:デバイスからアプリを完全に削除します。ライセンスを最初に非アクティブ化しない場合、ライセンスはアクティブのままです。

システム

時刻と位置

日付と時刻

時刻の形式は、Webブラウザーの言語設定によって異なります。

注
装置の日付と時刻をNTPサーバーと同期することをお勧めします。

Synchronization (同期):装置の日付と時刻を同期するオプションを選択します。

- Automatic date and time (manual NTS KE servers) (日付と時刻の自動設定 (手動NTS KEサーバー)):DHCPサーバーに接続された安全なNTPキー確立サーバーと同期します。
  - Manual NTS KE servers (手動NTS KEサーバー):1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - Max NTP poll time (最長NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - Min NTP poll time (最短NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- Automatic date and time (NTP servers using DHCP) (日付と時刻の自動設定 (DHCPを使用したNTPサーバー)):DHCPサーバーに接続されたNTPサーバーと同期します。
  - Fallback NTP servers (フォールバックNTPサーバー):1台または2台のフォールバックサーバーのIPアドレスを入力します。
  - Max NTP poll time (最長NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - Min NTP poll time (最短NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- Automatic date and time (manual NTP servers) (日付と時刻の自動設定 (手動NTPサーバー)):選択したNTPサーバーと同期します。
  - Manual NTP servers (手動NTPサーバー):1台または2台のNTPサーバーのIPアドレスを入力します。2台のNTPサーバーを使用すると、両方からの入力に基づいて装置が同期し、時刻を調整します。
  - Max NTP poll time (最長NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最長待機時間を選択します。
  - Min NTP poll time (最短NTPポーリング時間):装置がNTPサーバーをポーリングして最新の時刻を取得するまでの最短待機時間を選択します。
- Custom date and time (日付と時刻のカスタム設定):日付と時刻を手動で設定する[Get from system (システムから取得)] をクリックして、コンピューターまたはモバイル装置から日付と時刻 の設定を1回取得します。

タイムゾーン:使用するタイムゾーンを選択します。時刻が夏時間と標準時間に合わせて自動的に調整されます。

- DHCP:DHCPサーバーのタイムゾーンを採用します。このオプションを選択する前に、装置がDHCPサーバーに接続されている必要があります。
- 手動:ドロップダウンリストからタイムゾーンを選択します。

注

システムは、すべての録画、ログ、およびシステム設定で日付と時刻の設定を使用します。

デバイスの位置

デバイスの位置を入力します。ビデオ管理システムはこの情報を使用して、地図上にデバイスを配置できます。

- Format (形式):デバイスの緯度と経度を入力するときに使用する形式を選択します。
- Latitude (緯度):赤道の北側がプラスの値です。
- Longitude (経度):本初子午線の東側がプラスの値です。
- 向き:デバイスが向いているコンパス方位を入力します。真北が0です。
- ラベル:分かりやすいデバイス名を入力します。
- Save (保存):クリックして、装置の位置を保存します。

地域の設定

すべてのシステム設定で使用する測定系を設定します。

メートル (m、km/h)：距離をメートル単位で、速度を時速キロメートル単位で測定する場合に選択します。

米国で使用されている単位 (ft、mph)：距離をフィート単位で、速度を時速マイル単位で測定する場合に選択します。

ネットワーク

IPv4

Assign IPv4 automatically (IPv4自動割り当て):ネットワークルーターが自動的にデバイスにIPアドレスを割り当てる場合に選択します。ほとんどのネットワークでは、自動IP (DHCP) をお勧めします。

IPアドレス:装置の固有のIPアドレスを入力します。孤立したネットワークの内部であれば、アドレスの重複がないことを条件に、静的なIPアドレスを自由に割り当てることができます。アドレスの重複を避けるため、固定IPアドレスを割り当てる前に、ネットワーク管理者に連絡することを推奨します。

サブネットマスク:サブネットマスクを入力して、ローカルエリアネットワーク内部のアドレスを定義します。ローカルエリアネットワークの外部のアドレスは、ルーターを経由します。

Router (ルーター):さまざまなネットワークやネットワークセグメントに接続された装置を接続するために使用するデフォルトルーター (ゲートウェイ) のIPアドレスを入力します。

Fallback to static IP address if DHCP isn't available (DHCPが利用できない場合は固定IPアドレスにフォールバックする):DHCPが利用できず、IPアドレスを自動的に割り当てることができない場合に、フォールバックとして使用する固定IPアドレスを追加するときに選択します。

注

DHCPが使用できず、装置が静的アドレスのフォールバックを使用する場合、静的アドレスは限定された範囲で設定されます。

IPv6

Assign IPv6 automatically (IPv6自動割り当て):IPv6をオンにし、ネットワークルーターに自動的に装置にIPアドレスを割り当てさせる場合に選択します。

ホスト名

Assign hostname automatically (ホスト名自動割り当て):ネットワークルーターに自動的に装置にホスト名を割り当てさせる場合に選択します。

ホスト名:装置にアクセスする別の方法として使用するホスト名を手動で入力します。サーバーレポートとシステムログはホスト名を使用します。使用できる文字は、A～Z、a～z、0～9、-、_です。

DNSの動的更新： IPアドレスの変更時に、デバイスでのドメインネームサーバーレコードの自動更新が可能となります。

DNS名の登録：デバイスのIPアドレスを指す一意のドメイン名を入力します。使用できる文字は、A～Z、a～z、0～9、-、_です。

TTL：TTL（Time to Live）とは、DNSレコードの更新が必要となるまでの有効期間を指します。

DNSサーバー

Assign DNS automatically (DNS自動割り当て):DHCPサーバーに自動的に装置に検索ドメインとDNSサーバーアドレスを割り当てさせる場合に選択します。ほとんどのネットワークでは、自動DNS (DHCP) をお勧めします。

Search domains (検索ドメイン):完全修飾でないホスト名を使用する場合は、[**Add search domain (検索ドメインの追加)**] をクリックし、装置が使用するホスト名を検索するドメインを入力します。

DNS servers (DNSサーバー):[**Add DNS server (DNSサーバーを追加)**] をクリックして、DNSサーバーのIPアドレスを入力します。このサーバーは、ホスト名からローカルネットワーク上のIPアドレスへの変換を行います。

HTTPとHTTPS

HTTPSは、ユーザーからのページ要求とWebサーバーから返されたページの暗号化を提供するプロトコルです。サーバーの真正性 (サーバーが本物であること) を保証するHTTPS証明書が使用されます。

デバイスでHTTPSを使用するには、HTTPS証明書をインストールする必要があります。[**System (システム) > Security (セキュリティ)**] に移動し、証明書の作成とインストールを行います。

Allow access through (次によってアクセスを許可):ユーザーが [**HTTP**]、[**HTTPS**]、または [**HTTP and HTTPS (HTTPおよびHTTPS)**] プロトコルを介して装置に接続することを許可するかどうかを選択します。

注

暗号化されたWebページをHTTPS経由で表示する場合、特に初めてページを要求するときに、パフォーマンスが低下することがあります。

HTTP port (HTTPポート):使用するHTTPポートを入力します。装置はポート80または1024～65535の範囲のポートを許可します。管理者としてログインしている場合は、1～1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

HTTPS port (HTTPSポート):使用するHTTPSポートを入力します。装置はポート443または1024～65535の範囲のポートを許可します。管理者としてログインしている場合は、1～1023の範囲の任意のポートを入力することもできます。この範囲のポートを使用すると、警告が表示されます。

Certificate (証明書):装置のHTTPSを有効にする証明書を選択します。

グローバルプロキシー

Https proxy (HTTPプロキシー):許可された形式に従って、グローバルプロキシーホストまたはIPアドレスを指定します。

Https proxy (HTTPSプロキシー):許可された形式に従って、グローバルプロキシーホストまたはIPアドレスを指定します。

httpおよびhttpsプロキシーで許可されるフォーマット:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

注

装置を再起動し、グローバルプロキシー設定を適用します。

No proxy (プロキシーなし):グローバルプロキシーをバイパスするには、No proxy (プロキシーなし)を使用します。リスト内のオプションのいずれかを入力するか、コンマで区切って複数入力します。

- 空白にする
- IPアドレスを指定する
- CIDR形式でIPアドレスを指定する
- ドメイン名を指定する (www.<ドメイン名>.comなど)
- 特定のドメイン内のすべてのサブドメインを指定する (.<ドメイン名>.comなど)

ネットワーク検出プロトコル

Bonjour®: オンにしてネットワーク上で自動検出を可能にします。

Bonjour名:ネットワークで表示されるフレンドリ名を入力します。デフォルト名はデバイス名とMACアドレスです。

UPnP®: オンにしてネットワーク上で自動検出を可能にします。

UPnP名:ネットワークで表示されるフレンドリ名を入力します。デフォルト名はデバイス名とMACアドレスです。

WS-Discovery:オンにしてネットワーク上で自動検出を可能にします。

LLDP and CDP (LLDPおよびCDP):オンにしてネットワーク上で自動検出を可能にします。LLDPとCDPをオフにすると、PoE電力ネゴシエーションに影響する可能性があります。PoE電力ネゴシエーションに関する問題を解決するには、PoEスイッチをハードウェアPoE電力ネゴシエーションのみに設定してください。

ワンクリックによるクラウド接続

One-Click cloud connection (O3C) とO3Cサービスを共に使用すると、インターネットを介して、ライブビデオや録画ビデオにどこからでも簡単かつ安全にアクセスできます。詳細については、*axis.com/end-to-end-solutions/hosted-services*を参照してください。

Allow O3C (O3Cを許可):

- [ワンクリック]:デフォルトの設定です。インターネットを介してO3Cサービスに接続するには、装置のコントロールボタンを押し続けます。コントロールボタンを押してから24時間以内に装置をO3Cサービスに登録する必要があります。登録しない場合、デバイスはO3Cサービスから切断されます。装置を登録すると、[Always (常時)] が有効になり、装置はO3Cサービスに接続されたままになります。
- [常時]:装置は、インターネットを介してO3Cサービスへの接続を継続的に試行します。装置を登録すると、装置はO3Cサービスに接続したままになります。デバイスのコントロールボタンに手が届かない場合は、このオプションを使用します。
- [なし]:O3Cサービスを無効にします。

Proxy settings (プロキシ設定)：必要な場合は、プロキシサーバーに接続するためのプロキシ設定を入力します。

[ホスト]:プロキシサーバーのアドレスを入力します。

ポート:アクセスに使用するポート番号を入力します。

[ログイン] と [パスワード]:必要な場合は、プロキシーサーバーのユーザー名とパスワードを入力します。

Authentication method (認証方式):

- [ベーシック]:この方法は、HTTP用の最も互換性のある認証方式です。ユーザー名とパスワードを暗号化せずにサーバーに送信するため、Digest (ダイジェスト) 方式よりも安全性が低くなります。
- [ダイジェスト]:この認証方式は、常に暗号化されたパスワードをネットワークに送信するため、高いセキュリティレベルが得られます。
- [オート]:このオプションを使用すると、デバイスはサポートされている方法に応じて認証方法を選択できます。ダイジェスト方式がベーシック方式より優先されます。

Owner authentication key (OAK) (オーナー認証キー、OAK)：[Get key (キーを取得)]をクリックして、所有者認証キーを取得します。これは、デバイスがファイアウォールやプロキシを介さずにインターネットに接続されている場合にのみ可能です。

SNMP

SNMP (Simple Network Management Protocol) を使用すると、離れた場所からネットワーク装置を管理できます。

SNMP:使用するSNMPのバージョンを選択します。

- v1 and v2c (v1およびv2c)：
  - Read community (読み取りコミュニティ):サポートされているSNMPオブジェクトすべてに読み取り専用のアクセスを行えるコミュニティ名を入力します。デフォルト値はpublicです。
  - Write community (書き込みコミュニティ):サポートされている (読み取り専用のものを除く) SNMPオブジェクトすべてに読み取りアクセス、書き込みアクセスの両方を行えるコミュニティ名を入力します。デフォルト設定値はwriteです。
  - Activate traps (トラップの有効化):オンに設定すると、トラップレポートが有効になります。デバイスはトラップを使用して、重要なイベントまたはステータス変更のメッセージを管理システムに送信します。webインターフェースでは、SNMP v1およびv2cのトラップを設定できます。SNMP v3に変更するか、SNMPをオフにすると、トラップは自動的にオフになります。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
  - Trap address (トラップアドレス):管理サーバーのIPアドレスまたはホスト名を入力します。
  - Trap community (トラップコミュニティ):装置がトラップメッセージを管理システムに送信するときに使用するコミュニティを入力します。
  - Traps (トラップ):
    - Cold start (コールドスタート):デバイスの起動時にトラップメッセージを送信します。
    - Link up (リンクアップ):リンクの状態が切断から接続に変わったときにトラップメッセージを送信します。
    - Link down (リンクダウン):リンクの状態が接続から切断に変わったときにトラップメッセージを送信します。
    - 認証失敗:認証に失敗したときにトラップメッセージを送信します。

注

SNMP v1およびv2cトラップをオンにすると、すべてのAXIS Video MIBトラップが有効になります。詳細については、*AXIS OSポータル > SNMP*を参照してください。

- v3:SNMP v3は、暗号化と安全なパスワードを使用する、より安全性の高いバージョンです。SNMP v3を使用するには、HTTPSを有効化し、パスワードをHTTPSを介して送信することをお勧めします。これにより、権限のない人が暗号化されていないSNMP v1およびv2cトラップにアクセスすることも防止できます。SNMP v3を使用する際は、SNMP v3管理アプリケーションでトラップを設定できます。
  - Password for the account "initial" (「initial」アカウントのパスワード):「initial」という名前のアカウントのSNMPパスワードを入力します。HTTPSを有効化せずにパスワードを送信できますが、推奨しません。SNMP v3のパスワードは1回しか設定できません。HTTPSが有効な場合にのみ設定することをお勧めします。パスワードの設定後は、パスワードフィールドが表示されなくなります。パスワードを設定し直すには、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。

セキュリティ

証明書

証明書は、ネットワーク上のデバイスの認証に使用されます。この装置は、次の2種類の証明書をサポートしています。

- Client/server Certificates (クライアント/サーバー証明書)
  クライアント/サーバー証明書は装置のIDを認証します。自己署名証明書と認証局 (CA) 発行の証明書のどちらでも使用できます。自己署名証明書による保護は限られていますが、認証局発行の証明書を取得するまで利用できます。
- CA証明書
  CA証明書はピア証明書の認証に使用されます。たとえば、装置をIEEE 802.1Xで保護されたネットワークに接続するときに、認証サーバーのIDを検証するために使用されます。装置には、いくつかのCA証明書がプリインストールされています。

以下の形式がサポートされています:

- 証明書形式:.PEM、.CER、.PFX
- 秘密鍵形式:PKCS#1、PKCS#12

重要
デバイスを工場出荷時の設定にリセットすると、すべての証明書が削除されます。プリインストールされたCA証明書は、再インストールされます。

証明書を追加:クリックして証明書を追加します。ステップバイステップのガイドが開きます。

- **その他** :入力または選択するフィールドをさらに表示します。
- **セキュアキーストア**:[Trusted Execution Environment (SoC TEE)]、[Secure element (セキュアエレメント)] または [Trusted Platform Module 2.0] を使用して秘密鍵を安全に保存する場合に選択します。どのセキュアキーストアを選択するかの詳細については、*help.axis.com/en-us/axis-os#cryptographic-support*にアクセスしてください。
- **Key type (キーのタイプ)**:ドロップダウンリストから、証明書の保護に使用する暗号化アルゴリズムとしてデフォルトかその他のいずれかを選択します。

コンテキストメニューは以下を含みます。

- **Certificate information (証明書情報)**:インストールされている証明書のプロパティを表示します。
- **Delete certificate (証明書の削除)**:証明書の削除。
- **Create certificate signing request (証明書の署名要求を作成する)**:デジタルID証明書を申請するために登録機関に送信する証明書署名要求を作成します。

セキュアキーストア:

- Trusted Execution Environment (SoC TEE): 安全なキーストアにSoC TEEを使用する場合に選択します。
- **セキュアエレメント (CC EAL6+)**:セキュアキーストアにセキュアエレメントを使用する場合に選択します。
- Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2):セキュアキーストアにTPM 2.0を使用する場合に選択します。

暗号化ポリシー

暗号化ポリシーは、データ保護のために暗号化がどのように使用されるかを定義します。

Active (アクティブ):デバイスに適用する暗号化ポリシーを選択します：

- Default (デフォルト) - OpenSSL: 一般的な使用向けのバランスの取れたセキュリティとパフォーマンス。
- FIPS - FIPS 140-2に準拠したポリシー: 規制対象業界向けのFIPS 140-2に準拠した高セキュリティの暗号化。

Network access control and encryption (ネットワークのアクセスコントロールと暗号化)

IEEE 802.1x

IEEE 802.1xはポートを使用したネットワークへの接続を制御するIEEEの標準規格で、有線およびワイヤレスのネットワークデバイスを安全に認証します。IEEE 802.1xは、EAP (Extensible Authentication Protocol) に基づいています。

IEEE 802.1xで保護されているネットワークにアクセスするネットワーク装置は、自己の証明を行う必要があります。認証は認証サーバーによって行われます。認証サーバーは通常、FreeRADIUSやMicrosoft Internet Authentication ServerなどのRADIUSサーバーです。

IEEE 802.1AE MACsec

IEEE 802.1AE MACsecは、メディアアクセスコントロール (MAC) セキュリティのためのIEEE標準であり、メディアアクセス独立プロトコルのためのコネクションレスデータ機密性と整合性を定義しています。

証明書

CA証明書なしで設定されている場合、サーバー証明書の検証は無効になり、デバイスは接続先のネットワークに関係なく自己の認証を試みます。

証明書を使用する場合、Axisの実装では、装置と認証サーバーは、EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) を使用してデジタル証明書で自己を認証します。

装置が証明書で保護されたネットワークにアクセスできるようにするには、署名されたクライアント証明書を装置にインストールする必要があります。

Authentication method (認証方式):認証に使用するEAPタイプを選択します。

Client certificate (クライアント証明書)：IEEE 802.1xを使用するクライアント証明書を選択します。認証サーバーは、この証明書を使用してクライアントの身元を確認します。

CA certificates (CA証明書):認証サーバーの身元を確認するためのCA証明書を選択します。証明書が選択されていない場合、デバイスは、接続されているネットワークに関係なく自己を認証しようとします。

EAP識別情報:クライアント証明書に関連付けられているユーザーIDを入力します。

EAPOLのバージョン:ネットワークスイッチで使用されるEAPOLのバージョンを選択します。

Use IEEE 802.1x (IEEE 802.1xを使用):IEEE 802.1xプロトコルを使用する場合に選択します。

これらの設定は、認証方法として**IEEE 802.1x PEAP-MSCHAPv2**を使用する場合にのみ使用できます。

- **パスワード**:ユーザーIDのパスワードを入力します。
- **Peap version (Peapのバージョン)**:ネットワークスイッチで使用するPeapのバージョンを選択します。
- **ラベル**:クライアントEAP暗号化を使用する場合は1を選択し、クライアントPEAP暗号化を使用する場合は2を選択します。Peapバージョン1を使用する際にネットワークスイッチが使用するラベルを選択します。

これらの設定を使用できるのは、認証方法として**IEEE 802.1ae MACsec (静的CAK/事前共有キー)** を使用する場合のみです。

- **Key agreement connectivity association key name (キー合意接続アソシエーションキー名)**:接続アソシエーション名 (CKN) を入力します。2～64文字 (2で割り切れる文字数) の16進文字である必要があります。CKNは、接続アソシエーションで手動で設定する必要があり、最初にMACsecを有効にするには、リンクの両端で一致している必要があります。
- **Key agreement connectivity association key (キー合意接続アソシエーションキー)**:接続アソシエーションキー (CAK) を入力します。32文字または64文字の16進数である必要

があります。CAKは、接続アソシエーションで手動で設定する必要があり、最初にMACsecを有効にするには、リンクの両端で一致している必要があります。

ブルートフォース攻撃を防ぐ

Blocking (ブロック):オンに設定すると、ブルートフォース攻撃がブロックされます。ブルートフォース攻撃では、試行錯誤を繰り返す総当たり攻撃でログイン情報や暗号化キーを推測します。

Blocking period (ブロック期間)：ブルートフォース攻撃をブロックする秒を入力します。

Blocking conditions (ブロックの条件)：ブロックが開始されるまでに1秒間に許容される認証失敗の回数を入力します。ページレベルとデバイスレベルの両方で許容される失敗の数を設定できます。

ファイアウォール

Activate (アクティブ化):ファイアウォールをオンにします。

Default Policy (デフォルトポリシー):ファイアウォールのデフォルト状態を選択します。

- Allow: (許可:) 装置へのすべての接続を許可します。このオプションはデフォルトで設定されています。
- Deny (拒否): 装置へのすべての接続を拒否します。

デフォルトポリシーに例外を設定するために、特定のアドレス、プロトコル、ポートから装置への接続を許可または拒否するルールを作成できます。

- アドレス:アクセスを許可または拒否するアドレスをIPv4/IPv6またはCIDR形式で入力します。
- Protocol (プロトコル):アクセスを許可または拒否するプロトコルを選択します。
- ポート:アクセスを許可または拒否するポート番号を入力します。1～65535のポート番号を追加できます。
- Policy (ポリシー)：ルールのポリシーを選択します。

＋:クリックして、別のルールを作成します。

Add rules: (ルールの追加:) クリックして、定義したルールを追加します。

- Time in seconds: (時間 (秒):) ルールのテストに制限時間を設定します。デフォルトの制限時間は300秒に設定されています。ルールをすぐに有効にするには、時間を0秒に設定します。
- Confirm rules (ルールを確認): ルールとその制限時間を確認します。1秒を超える制限時間を設定した場合、ルールはこの時間内に有効になります。時間を0に設定した場合、ルールはすぐに有効になります。

Pending rules (保留中のルール):まだ確認していない最新のテスト済みルールの概要です。

注

時間制限のあるルールは、表示されたタイマーが切れるか、確認されるまで、[Active rules (アクティブなルール)] に表示されます。確認されない場合、タイマーが切れると、それらのルールは [Pending rules (保留中のルール)] に表示され、ファイアウォールは以前の設定に戻ります。それらのルールを確認すると、現在アクティブなルールが置き換えられます。

Confirm rules (ルールを確認):クリックして、保留中のルールをアクティブにします。

Active rules (アクティブなルール):装置で現在実行中のルールの概要です。

:クリックして、アクティブなルールを削除します。

:クリックして、保留中のルールとアクティブなルールの両方をすべて削除します。

カスタム署名付きAXIS OS証明書

Axisのテストソフトウェアまたはその他のカスタムソフトウェアを装置にインストールするには、カスタム署名付きAXIS OS証明書が必要です。証明書は、ソフトウェアが装置の所有者とAxisの両方によって承認されたことを証明します。ソフトウェアは、一意のシリアル番号とチップIDで識別される特定の装置でのみ実行できます。署名用のキーはAxisが保有しており、カスタム署名付きAXIS OS証明書はAxisしか作成できません。

Install (インストール):クリックして、証明書をインストールします。ソフトウェアをインストールする前に、証明書をインストールする必要があります。

⋮ コンテキストメニューは以下を含みます。

- Delete certificate (証明書の削除):証明書の削除。

アカウント

アカウント

＋アカウントを追加:クリックして、新しいアカウントを追加します。最大100個のアカウントを追加できます。

Account (アカウント):固有のアカウント名を入力します。

New password (新しいパスワード):アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32～126) のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力):同じパスワードを再び入力します。

Privileges (権限):

- **Administrator (管理者)**:すべての設定へ全面的なアクセス権をもっています。管理者は他のアカウントを追加、更新、削除することもできます。
- **Operator (オペレーター)**:次の操作を除く、すべての設定へのアクセス権があります。
  - すべての [**System settings (システムの設定)**]。

⋮ コンテキストメニューは以下を含みます。

Update account (アカウントの更新):アカウントのプロパティを編集します。

Delete account (アカウントの削除):アカウントを削除します。rootアカウントは削除できません。

匿名アクセス

Allow anonymous viewing (匿名の閲覧を許可する):アカウントでログインせずに誰でも閲覧者として装置にアクセスできるようにする場合は、オンにします。

匿名のPTZ操作を許可する:オンにすると、匿名ユーザーに画像のパン、チルト、ズームを許可します。

SSHアカウント

+ Add SSH account (SSHアカウントを追加):クリックして、新しいSSHアカウントを追加します。

- Enable SSH (SSHの有効化):SSHサービスを使用する場合は、オンにします。

Account (アカウント):固有のアカウント名を入力します。

New password (新しいパスワード):アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32～126) のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力):同じパスワードを再び入力します。

コメント:コメントを入力します (オプション)。

⋮ コンテキストメニューは以下を含みます。

Update SSH account (SSHアカウントの更新):アカウントのプロパティを編集します。

Delete SSH account (SSHアカウントの削除):アカウントを削除します。rootアカウントは削除できません。

Virtual host (仮想ホスト)

+ Add virtual host (仮想ホストを追加):クリックして、新しい仮想ホストを追加します。

Enabled (有効):この仮想ホストを使用するには、選択します。

Server name (サーバー名):サーバーの名前を入力します。数字0～9、文字A～Z、ハイフン (-) のみを使用します。

ポート:サーバーが接続されているポートを入力します。

タイプ:使用する認証のタイプを選択します。[Basic (ベーシック)]、[Digest (ダイジェスト)]、[Open ID] から選択します。

⋮ コンテキストメニューは以下を含みます。

- Update (更新):仮想ホストを更新します。
- 削除:仮想ホストを削除します。

Disabled (無効):サーバーが無効になっています。

OpenID設定

重要

OpenIDを使用してサインインできない場合は、OpenIDを設定したときに使用したダイジェストまたはベーシック認証情報を使用してサインインします。

Client ID (クライアントID)：OpenIDユーザー名を入力します。

Outgoing Proxy (発信プロキシ):OpenID接続でプロキシサーバーを使用する場合は、プロキシアドレスを入力します。

Admin claim (管理者請求):管理者権限の値を入力します。

Provider URL (プロバイダーURL):APIエンドポイント認証用のWebリンクを入力します。形式はhttps://[URLを挿入]/.well-known/openid-configurationとしてください。

Operator claim (オペレーター請求):オペレーター権限の値を入力します。

Require claim (必須請求):トークンに含めるデータを入力します。

Viewer claim (閲覧者請求):閲覧者権限の値を入力します。

Remote user (リモートユーザー):リモートユーザーを識別する値を入力します。これは、装置のwebインターフェースに現在のユーザーを表示するのに役立ちます。

Scopes (スコープ):トークンの一部となるオプションのスコープです。

Client secret (クライアントシークレット):OpenIDのパスワードを入力します。

Save (保存):クリックして、OpenIDの値を保存します。

Enable OpenID (OpenIDの有効化):現在の接続を閉じ、プロバイダーURLからの装置認証を許可する場合は、オンにします。

イベント

ルール

ルールは、製品がアクションを実行するためのトリガーとなる条件を定義します。このリストには、本製品で現在設定されているすべてのルールが表示されます。

注

最大256のアクションルールを作成できます。

ルールを追加:ルールを作成します。

名前:アクションルールの名前を入力します。

Wait between actions (アクション間の待ち時間):ルールを有効化する最短の時間間隔 (hh:mm:ss) を入力します。たとえば、デイナイトモードの条件によってルールが有効になる場合、このパラメーターを設定することで、日の出や日没時のわずかな光の変化によりルールが反復的に有効になるのを避けられます。

Condition (条件):リストから条件を選択します。装置がアクションを実行するためには、条件を満たす必要があります。複数の条件が定義されている場合、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。特定の条件については、「*イベントのルールの使用開始*」を参照してください。

Use this condition as a trigger (この条件をトリガーとして使用する):この最初の条件を開始トリガーとしてのみ機能させる場合に選択します。つまり、いったんルールが有効になると、最初の条件の状態に関わらず、他のすべての条件が満たされている限り有効のままになります。このオプションを選択しない場合、ルールは単純にすべての条件が満たされたときに有効化されます。

Invert this condition (この条件を逆にする):選択した条件とは逆の条件にする場合に選択します。

条件を追加:新たに条件を追加する場合にクリックします。

Action (アクション):リストからアクションを選択し、必要な情報を入力します。特定のアクションについては、「*イベントのルールの使用開始*」を参照してください。

送信先

イベントについて受信者に通知したり、ファイルを送信したりするように装置を設定できます。

注

FTPまたはSFTPを使用するように装置を設定した場合、ファイル名に付加される固有のシーケンス番号を変更したり削除したりしないでください。その場合、イベントごとに1つの画像しか送信できません。

このリストには、製品で現在設定されているすべての送信先とそれらの設定に関する情報が示されます。

注

最大20名の送信先を作成できます。

送信先を追加:クリックすると、送信先を追加できます。

名前:送信先の名前を入力します。

タイプ:リストから選択します:

- FTP
  - **[ホスト]**:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[**System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)**] で DNS サーバーを指定します。
  - **ポート**:FTPサーバーに使用するポート番号。デフォルトは21です。
  - **Folder (フォルダー)**:ファイルを保存するディレクトリのパスを入力します。FTPサーバー上に存在しないディレクトリを指定すると、ファイルのアップロード時にエラーメッセージが表示されます。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Use temporary file name (一時ファイル名を使用する)**:選択すると、自動的に生成された一時的なファイル名でファイルがアップロードされます。アップロードが完了した時点で、ファイル名が目的の名前に変更されます。アップロードが中止/中断されても、破損したファイルが発生することはありません。ただし、一時ファイルが残る可能性はあります。これにより、目的の名前を持つすべてのファイルが正常であると確信できます。
  - **Use passive FTP (パッシブFTPを使用する)**:通常は、製品がFTPサーバーに要求を送ることでデータ接続が開かれます。この接続では、対象サーバーとのFTP制御用接続とデータ用接続の両方が装置側から開かれます。一般に、装置と対象FTPサーバーの間にファイアウォールがある場合に必要となります。
- HTTP
  - **URL**:HTTPサーバーのネットワークアドレスと、要求の処理を行うスクリプトを入力します。たとえば、http://192.168.254.10/cgi-bin/notify.cgiと入力します。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Proxy (プロキシ)**:HTTPサーバーに接続するためにプロキシサーバーを渡す必要がある場合は、これをオンにし、必要な情報を入力します。
- HTTPS
  - **URL**:HTTPSサーバーのネットワークアドレスと、要求の処理を行うスクリプトを入力します。たとえば、https://192.168.254.10/cgi-bin/notify.cgiと入力します。
  - **Validate server certificate (サーバー証明書を検証する)**:HTTPSサーバーが作成した証明書を検証する場合にオンにします。
  - **Username (ユーザー名)**:ログインのユーザー名を入力します。
  - **パスワード**:ログインのパスワードを入力します。
  - **Proxy (プロキシ)**:HTTPSサーバーに接続するためにプロキシサーバーを渡す必要がある場合にオンにして、必要な情報を入力します。
- ネットワークストレージ
  NAS (network-attached storage) などのネットワークストレージを追加し、それを録画ファイルの保存先として使用することができます。ファイルは.mkv (Matroska) 形式で保存されます。
  - **[ホスト]**:ネットワークストレージのIPアドレスまたはホスト名を入力します。
  - **共有**:ホスト上の共有の名を入力します。

- Folder (フォルダー):ファイルを保存するディレクトリのパスを入力します。
- Username (ユーザー名):ログインのユーザー名を入力します。
- パスワード:ログインのパスワードを入力します。

- SFTP
  - [ホスト]:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)] で DNS サーバーを指定します。
  - ポート:SFTPサーバーに使用するポート番号。デフォルトは22です。
  - Folder (フォルダー):ファイルを保存するディレクトリのパスを入力します。SFTPサーバー上に存在しないディレクトリを指定すると、ファイルのアップロード時にエラーメッセージが表示されます。
  - Username (ユーザー名):ログインのユーザー名を入力します。
  - パスワード:ログインのパスワードを入力します。
  - SSH host public key type (MD5) (SSHホスト公開鍵タイプ (MD5)):リモートホストの公開鍵のフィンガープリント (32桁の16進数) を入力します。SFTPクライアントは、RSA、DSA、ECDSA、およびED25519ホストキータイプによるSSH-2を使用するSFTPサーバーをサポートします。RSAは、ネゴシエーション時の推奨方式です。その後には、ECDSA、ED25519、DSAが続きます。SFTPサーバーで使用されている正しいMD5ホストキーを入力してください。AxisデバイスはMD5とSHA-256の両方のハッシュキーをサポートしていますが、MD5よりもセキュリティが強いため、SHA-256を使用することをお勧めします。AxisデバイスでSFTPサーバーを設定する方法の詳細については、*AXIS OSポータル*にアクセスしてください。
  - SSH host public key type (SHA256) (SSHホスト公開鍵タイプ (SHA256)):リモートホストの公開鍵のフィンガープリント (43桁のBase64エンコード文字列) を入力します。SFTPクライアントは、RSA、DSA、ECDSA、およびED25519ホストキータイプによるSSH-2を使用するSFTPサーバーをサポートします。RSAは、ネゴシエーション時の推奨方式です。その後には、ECDSA、ED25519、DSAが続きます。SFTPサーバーで使用されている正しいMD5ホストキーを入力してください。AxisデバイスはMD5とSHA-256の両方のハッシュキーをサポートしていますが、MD5よりもセキュリティが強いため、SHA-256を使用することをお勧めします。AxisデバイスでSFTPサーバーを設定する方法の詳細については、*AXIS OSポータル*にアクセスしてください。
  - Use temporary file name (一時ファイル名を使用する):選択すると、自動的に生成された一時的なファイル名でファイルがアップロードされます。アップロードが完了した時点で、ファイル名が目的の名前に変更されます。アップロードが中止/中断されても、ファイルが破損することはありません。ただし、一時ファイルが残る可能性はあります。これにより、目的の名前を持つすべてのファイルが正常であると確信できます。

- SIPまたはVMS :
  SIP:選択してSIP呼び出しを行います。
  VMS:選択してVMS呼び出しを行います。
  - 送信元のSIPアカウント:リストから選択します。
  - 送信先のSIPアドレス:SIPアドレスを入力します。
  - テスト:クリックして、呼び出しの設定が機能することをテストします。
- 電子メール
  - 電子メールの送信先:電子メールの宛先のアドレスを入力します。複数のアドレスを入力するには、カンマで区切ります。
  - 電子メールの送信元:送信側サーバーのメールアドレスを入力します。

- Username (ユーザー名):メールサーバーのユーザー名を入力します。認証の必要のないメールサーバーの場合は、このフィールドを空にします。
- パスワード:メールサーバーのパスワードを入力します。認証の必要のないメールサーバーの場合は、このフィールドを空にします。
- Email server (SMTP) (電子メールサーバー (SMTP)):SMTPサーバーの名前 (smtp.gmail.com、smtp.mail.yahoo.comなど) を入力します。
- ポート:SMTPサーバーのポート番号を0～65535の範囲で入力します。デフォルト設定値は587です。
- [暗号化]:暗号化を使用するには、SSL または TLS を選択します。
- Validate server certificate (サーバー証明書を検証する):暗号化を使用している場合にこれを選択すると、装置の身元を検証できます。この証明書は、自己署名または認証局 (CA) 発行の証明書のどちらでも可能です。
- POP authentication (POP認証):オンにすると、POPサーバーの名前 (pop.gmail.comなど) を入力できます。

注

一部の電子メールプロバイダーでは、大量の添付ファイルやスケジュール設定済みメールなどがセキュリティフィルターによって受信または表示できないようになっています。電子メールプロバイダーのセキュリティポリシーを確認し、メールアカウントのロックや、必要な電子メールの不着などが起こらないようにしてください。

- TCP
  - [ホスト]:サーバーのIPアドレスまたはホスト名を入力します。ホスト名を入力した場合は、必ず、[System (システム) > Network (ネットワーク) > IPv4 and IPv6 (IPv4 と IPv6)] で DNS サーバーを指定します。
  - ポート:サーバーへのアクセスに使用したポート番号を入力します。

Test (テスト):クリックすると、セットアップをテストすることができます。

⋮ コンテキストメニューは以下を含みます。

View recipient (送信先の表示):クリックすると、すべての送信先の詳細が表示されます。

Copy recipient (送信先のコピー):クリックすると、送信先をコピーできます。コピーする際、新しい送信先に変更を加えることができます。

Delete recipient (送信先の削除):クリックすると、受信者が完全に削除されます。

スケジュール

スケジュールとパルスは、ルールで条件として使用することができます。このリストには、製品で現在設定されているすべてのスケジュールとパルス、およびそれらの設定に関する情報が示されます。

＋ スケジュールを追加:クリックすると、スケジュールやパルスを作成できます。

手動トリガー

手動トリガーを使用すると、ルールを手動でトリガーできます。手動トリガーは、本製品の設置、設定中にアクションを検証する目的などで使用します。

MQTT

MQTT (Message Queuing Telemetry Transport) はモノのインターネット (IoT) で使われる標準の通信プロトコルです。IoTの統合を簡素化するために設計されており、小さなコードフットプリントと最小限のネットワーク帯域幅でリモートデバイスを接続するために、さまざまな業界で使用されています。Axis装置のソフトウェアに搭載されているMQTTクライアントは、装置で生成されたデータやイベントを、ビデオ管理ソフトウェア (VMS) ではないシステムに統合することを容易にします。

デバイスをMQTTクライアントとして設定します。MQTTの通信は、2つのエンティティ (クライアントとブローカー) に基づいています。クライアントは、メッセージの送受信を行うことができます。ブローカーは、クライアント間でメッセージをルーティングする役割を担います。

MQTTの詳細については、*AXIS OSナレッジベース*を参照してください。

ALPN

ALPNは、クライアントとサーバー間の接続のハンドシェイクフェーズ中にアプリケーションプロトコルを選択できるようにするTLS/SSL拡張機能です。ALPNは、HTTPなどの他のプロトコルで使用される同じポート経由でMQTTトラフィックを有効にするために使用されます。場合によっては、MQTT通信のための専用ポートが開かれていない可能性があります。このような場合の解決策は、ALPNを使用して、ファイアウォールによって許可される標準ポートで、アプリケーションプロトコルとしてMQTTを使用するようネゴシエーションすることです。

MQTT クライアント

Connect (接続する):MQTTクライアントのオン/オフを切り替えます。

Status (ステータス):MQTTクライアントの現在のステータスを表示します。

ブローカー

[ホスト]:MQTTサーバーのホスト名またはIPアドレスを入力します。

Protocol (プロトコル):使用するプロトコルを選択します。

ポート:ポート番号を入力します。

- 1883はMQTTオーバTCPのデフォルト値です。
- 8883はMQTTオーバSSLのデフォルト値です。
- 80はMQTTオーバWebSocketのデフォルト値です。
- 443はMQTTオーバWebSocket Secureのデフォルト値です。

ALPN protocol (ALPNプロトコル):ご使用のMQTTブローカープロバイダーが提供するALPNプロトコル名を入力します。これは、MQTTオーバーSSLとMQTTオーバーWebSocket Secureを使用する場合にのみ適用されます。

Username (ユーザー名):クライアントがサーバーにアクセスするために使用するユーザー名を入力します。

パスワード:ユーザー名のパスワードを入力します。

Client ID (クライアントID)：クライアントIDを入力します。クライアントがサーバーに接続すると、クライアント識別子がサーバーに送信されます。

Clean session (クリーンセッション):接続時と切断時の動作を制御します。選択した場合、接続時と切断時にステータス情報が破棄されます。

HTTP proxy (HTTPプロキシ):最大長が255バイトのURL。HTTPプロキシを使用しない場合、このフィールドは空白のままで構いません。

HTTPS proxy (HTTPSプロキシ):最大長が255バイトのURL。HTTPSプロキシを使用しない場合、このフィールドは空白のままで構いません。

Keep alive interval (キープアライブの間隔):長時間のTCP/IPタイムアウトを待たずに、サーバーを使用できなくなったことをクライアントに検知させます。

Timeout (タイムアウト):接続を終了する時間の間隔(秒)です。デフォルト値:60

装置トピックの接頭辞:MQTTクライアントタブの接続メッセージやLWTメッセージ、MQTT公開タブの公開条件におけるトピックのデフォルト値で使用されます。

Reconnect automatically (自動再接続):切断された場合に、クライアントを自動的に再接続するかどうかを指定します。

接続メッセージ

接続が確立されたときにメッセージを送信するかどうかを指定します。

Send message (メッセージの送信):オンにすると、メッセージを送信します。

Use default (デフォルトを使用):オフに設定すると、独自のデフォルトメッセージを入力できます。

Topic (トピック):デフォルトのメッセージのトピックを入力します。

Payload (ペイロード):デフォルトのメッセージの内容を入力します。

Retain (保持する):クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

QoS:パケットフローのQoS layerを変更します。

最終意思およびテスタメントメッセージ

最終意思テスタメント(LWT) を使用すると、クライアントはブローカーへの接続時、認証情報と共にテスタメントを提供します。後ほどいずれかの時点でクライアントが予期せず切断された場合(電源の停止など)、ブローカーから他のクライアントにメッセージを送信できます。このLWTメッセージは通常のメッセージと同じ形式で、同一のメカニズムを経由してルーティングされます。

Send message (メッセージの送信):オンにすると、メッセージを送信します。

Use default (デフォルトを使用):オフに設定すると、独自のデフォルトメッセージを入力できます。

Topic (トピック):デフォルトのメッセージのトピックを入力します。

Payload (ペイロード):デフォルトのメッセージの内容を入力します。

Retain (保持する):クライアントの状態をこのTopic (トピック)に保存する場合に選択します。

QoS:パケットフローのQoS layerを変更します。

MQTT公開

Use default topic prefix (デフォルトのトピックプレフィックスを使用):選択すると、[MQTT client (MQTTクライアント)] タブの装置のトピックプレフィックスで定義されたデフォルトのトピックプレフィックスが使用されます。

Include topic name (トピック名を含める):選択すると、条件を説明するトピックがMQTTトピックに含まれます。

Include topic namespaces (トピックの名前空間を含める):選択すると、ONVIFトピックの名前空間がMQTTトピックに含まれます。

シリアル番号を含める:選択すると、装置のシリアル番号が、MQTTペイロードに含まれます。

＋ 条件を追加:クリックして条件を追加します。

Retain (保持する):保持して送信するMQTTメッセージを定義します。

- None (なし):すべてのメッセージを、保持されないものとして送信します。
- Property (プロパティ):ステートフルメッセージのみを保持として送信します。
- All (すべて):ステートフルメッセージとステートレスメッセージの両方を保持として送信します。

QoS:MQTT公開に適切なレベルを選択します。

MQTTサブスクリプション

＋ **サブスクリプションを追加**:クリックして、新しいMQTTサブスクリプションを追加します。

サブスクリプションフィルター:購読するMQTTトピックを入力します。

装置のトピックプレフィックスを使用:サブスクリプションフィルターを、MQTTトピックのプレフィックスとして追加します。

サブスクリプションの種類:

- **ステートレス**:選択すると、エラーメッセージがステートレスメッセージに変換されます。
- **ステートフル**:選択すると、エラーメッセージが条件に変換されます。ペイロードが状態として使用されます。

QoS:MQTTサブスクリプションに適切なレベルを選択します。

MQTTオーバーレイ

注
MQTTオーバーレイ修飾子を追加する前に、MQTTブローカーに接続します。

＋ **オーバーレイ修飾子を追加**:クリックして新しいオーバーレイ修飾子を追加します。

Topic filter (トピックフィルター):オーバーレイに表示するデータを含むMQTTトピックを追加します。

Data field (データフィールド):オーバーレイに表示するメッセージペイロードのキーを指定します。メッセージはJSON形式であるとします。

Modifier (修飾子):オーバーレイを作成するときに、生成された修飾子を使用します。

- **#XMP**で始まる修飾子は、トピックから受信したすべてのデータを示します。
- **#XMD**で始まる修飾子は、データフィールドで指定されたデータを示します。

ストレージ

ネットワークストレージ

使用しない:オンにすると、ネットワークストレージは使用されません。

Add network storage (ネットワークストレージの追加):クリックして、録画を保存できるネットワーク共有を追加します。

- アドレス:ホストサーバーのホスト名 (通常はNAS (network-attached storage) またはIPアドレスを入力します。DHCPではなく固定IPアドレスを使用するようにホストを設定するか (動的IPアドレスは変わる可能性があるため、DHCPは使用しない)、DNS名を使用することをお勧めします。Windows SMB/CIFS名はサポートされていません。
- Network share (ネットワーク共有):ホストサーバー上の共有場所の名前を入力します。各Axis装置にはそれぞれのフォルダーがあるため、複数の装置で同じネットワーク共有を使用できます。
- User (ユーザー):サーバーにログインが必要な場合は、ユーザー名を入力します。特定のドメインサーバーにログインするには、`DOMAIN\username` を入力します。
- パスワード:サーバーにログインが必要な場合は、パスワードを入力します。
- SMB version (SMBバージョン):NASに接続するSMBストレージプロトコルのバージョンを選択します。[Auto (自動)] を選択すると、装置は、セキュアバージョンであるSMB3.02、3.0、2.1 のいずれかにネゴシエートを試みます。1.0または2.0を選択すると、上位バージョンをサポートしない旧バージョンのNASに接続できます。Axis装置でのSMBサポートの詳細については、こちらをご覧ください。
- Add share without testing (テストなしで共有を追加する):接続テスト中にエラーが検出された場合でも、ネットワーク共有を追加する場合に選択します。サーバーにパスワードが必要な場合でも、パスワードを入力しなかったなど、エラーが発生する可能性があります。

ネットワークストレージを削除する:クリックして、ネットワーク共有への接続をマウント解除、バインド解除、削除します。これにより、ネットワーク共有のすべての設定が削除されます。

Unbind (バインド解除):クリックして、ネットワーク共有をアンバインドし、切断します。
Bind (バインド):クリックして、ネットワーク共有をバインドし、接続します。

Unmount (マウント解除):クリックして、ネットワーク共有をマウント解除します。
Mount (マウント):クリックしてネットワーク共有をマウントします。

Write protect (書き込み禁止):オンに設定すると、ネットワーク共有への書き込みが停止され、録画が削除されないように保護されます。書き込み保護されたネットワーク共有はフォーマットできません。

Retention time (保存期間):録画の保存期間を選択し、古い録画の量を制限したり、データストレージに関する規制に準拠したりします。ネットワークストレージがいっぱいになると、設定した時間が経過する前に古い録画が削除されます。

ツール

- 接続をテストする:ネットワーク共有への接続をテストします。
- Format (形式):ネットワーク共有をフォーマットします。たとえば、すべてのデータをすばやく消去する必要があるときです。CIFSをファイルシステムとして選択することもできます。

Use tool (ツールを使用)クリックして、選択したツールをアクティブにします。

オンボードストレージ

重要

データ損失や録画データ破損の危険があります。装置の稼働中はSDカードを取り外さないでください。SDカードを取り外す前に、SDカードをマウント解除します。

Unmount (マウント解除):SDカードを安全に取り外す場合にクリックします。

Write protect (書き込み禁止):オンにすると、SDカードへの書き込みが防止され、録画が削除されなくなります。書き込み保護されたSDカードはフォーマットできません。

Autoformat (自動フォーマット):オンにすると、新しく挿入されたSDカードが自動的にフォーマットされます。ファイルシステムをext4にフォーマットします。

使用しない:オンにすると、録画のSDカードへの保存が停止します。SDカードを無視すると、装置はカードがあっても認識しなくなります。この設定は管理者のみが使用できます。

Retention time (保存期間):録画の保存期間を選択し、古い録画の量を制限したり、データストレージの規制に準拠したりします。SDカードがいっぱいになると、保存期間が切れる前に古い録画が削除されます。

ツール

- **Check (チェック)**:SDカードのエラーをチェックします。
- **Repair (修復)**:ファイルシステムのエラーを修復します。
- **Format (形式)**:SDカードをフォーマットしてファイルシステムを変更し、すべてのデータを消去します。SDカードはext4ファイルシステムにのみフォーマットすることができます。Windows®からファイルシステムにアクセスするには、サードパーティ製のext4ドライバーまたはアプリケーションが必要です。
- **Encrypt (暗号化)**:このツールを使用して、暗号化ありでSDカードをフォーマットします。これにより、SDカードに保存されているデータはすべて削除されます。SDカードに保存する新規データはすべて暗号化されます。
- **Decrypt (復号化)**:このツールを使用して、暗号化なしでSDカードをフォーマットします。これにより、SDカードに保存されているデータはすべて削除されます。SDカードに保存する新規データは暗号化されません。
- **Change password (パスワードの変更)**:SDカードの暗号化に必要なパスワードを変更します。

Use tool (ツールを使用)クリックして、選択したツールをアクティブにします。

Wear trigger (消耗トリガー):アクションをトリガーするSDカードの消耗レベルの値を設定します。消耗レベルは0～200%です。一度も使用されていない新しいSDカードの消耗レベルは0%です。消耗レベルが100%になると、SDカードの寿命が近い状態にあります。消耗レベルが200%に達すると、SDカードが故障するリスクが高くなります。消耗トリガーを80～90%の間に設定することをお勧めします。これにより、SDカードが消耗し切る前に、録画をダウンロードしたり、SDカードを交換したりする時間ができます。消耗トリガーを使用すると、イベントを設定し、消耗レベルが設定値に達したときに通知を受け取ることができます。

ストリームプロファイル

ストリームプロファイルは、ビデオストリームに影響する設定のグループです。ストリームプロファイルは、たとえばイベントを作成するときや、ルールを使って録画するときなど、さまざまな場面で使うことができます。

ストリームプロファイルを追加:クリックして、新しいストリームプロファイルを作成します。

Preview (プレビュー):選択したストリームプロファイル設定によるビデオストリームのプレビューです。ページの設定を変更すると、プレビューは更新されます。装置のビューエリアが異なる場合は、画像の左下隅にあるドロップダウンリストでビューエリアを変更できます。

名前:プロファイルの名前を追加します。

Description (説明):プロファイルの説明を追加します。

Video codec (ビデオコーデック):プロファイルに適用するビデオコーデックを選択します。

解像度:この設定の説明については、を参照してください。

フレームレート:この設定の説明については、を参照してください。

圧縮:この設定の説明については、を参照してください。

Zipstream:この設定の説明については、を参照してください。

ストレージ用に最適化する:この設定の説明については、を参照してください。

ダイナミックFPS:この設定の説明については、を参照してください。

ダイナミックGOP:この設定の説明については、を参照してください。

ミラーリング:この設定の説明については、を参照してください。

GOP長:この設定の説明については、を参照してください。

ビットレート制御:この設定の説明については、を参照してください。

オーバーレイを含める:含めるオーバーレイのタイプを選択します。オーバーレイを追加する作成方法については、を参照してください。

音声を含める:この設定の説明については、を参照してください。

ONVIF

ONVIFアカウント

ONVIF (Open Network Video Interface Forum) は、エンドユーザー、インテグレーター、コンサルタント、メーカーがネットワークビデオ技術が提供する可能性を容易に利用できるようにするグローバルなインターフェース標準です。ONVIFによって、さまざまなベンダー製品間の相互運用、柔軟性の向上、コストの低減、陳腐化しないシステムの構築が可能になります。

ONVIFアカウントを作成すると、ONVIF通信が自動的に有効になります。装置とのすべてのONVIF通信には、アカウント名とパスワードを使用します。詳細については、*axis.com*にあるAxis開発者コミュニティを参照してください。

+ アカウントを追加:クリックして、新規のONVIFアカウントを追加します。

Account (アカウント):固有のアカウント名を入力します。

New password (新しいパスワード):アカウントのパスワードを入力します。パスワードの長は1~64文字である必要があります。印刷可能なASCII文字 (コード32～126) のみを使用できます。これには、英数字、句読点、および一部の記号が含まれます。

Repeat password (パスワードの再入力):同じパスワードを再び入力します。

Role (権限):

- Administrator (管理者):すべての設定へ全面的なアクセス権をもっています。管理者は他のアカウントを追加、更新、削除することもできます。
- Operator (オペレーター):次の操作を除く、すべての設定へのアクセス権があります。
  - すべての [System settings (システムの設定)]。
  - アプリを追加しています。
- Media account (メディアアカウント):ビデオストリームの参照のみを行えます。

⋮ コンテキストメニューは以下を含みます。

Update account (アカウントの更新):アカウントのプロパティを編集します。

Delete account (アカウントの削除):アカウントを削除します。rootアカウントは削除できません。

ONVIFメディアプロファイル

ONVIFメディアプロファイルは、メディアストリーム設定の変更に使用する一連の設定から構成されています。独自の設定を使用して新しいプロファイルを作成することも、設定済みのプロファイルを使用してすばやく設定することもできます。

メディアプロファイルを追加:クリックすると、新しいONVIFメディアプロファイルを追加できます。

プロファイル名:メディアプロファイルに名前を付けます。

Video source (ビデオソース):設定に使用するビデオソースを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択します。ドロップダウンリストに表示される設定は、マルチビュー、ビューエリア、バーチャルチャンネルなど、装置のビデオチャンネルに対応しています。

Video encoder (ビデオエンコーダ):設定に使用するビデオエンコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、エンコード方式の設定を調整します。ドロップダウンリストに表示される設定は、ビデオエンコーダの設定の識別子/名前となります。ユーザー0～15を選択して、独自の設定を適用します。または、デフォルトユーザーのいずれかを選択して、特定のエンコード方式の既定の設定を使用します。

注

装置で音声を有効にすると、音声ソースと音声エンコーダ設定を選択するオプションが有効になります。

音声ソース:設定に使用する音声入力ソースを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、音声設定を調整します。ドロップダウンリストに表示される設定は、装置の音声入力に対応しています。装置に1つの音声入力がある場合、それはuser0です。装置に複数の音声入力がある場合、リストには追加のユーザーが表示されます。

音声エンコーダ:設定に使用する音声エンコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、音声エンコード方式の設定を調整します。ドロップダウンリストに表示される設定は、音声エンコーダの設定の識別子/名前として機能します。

音声デコーダ:設定に使用する音声デコード方式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、設定を調整します。ドロップダウンリストに表示される設定は、設定の識別子/名前として機能します。

音声出力:設定に使用する音声出力形式を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、設定を調整します。ドロップダウンリストに表示される設定は、設定の識別子/名前として機能します。

Metadata (メタデータ):設定に含めるメタデータを選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、メタデータ設定を調整します。ドロップダウンリストに表示される設定は、メタデータの設定の識別子/名前となります。

PTZ: 設定に使用するPTZ設定を選択します。

- **Select configuration (設定の選択)**:リストからユーザー定義の設定を選択し、PTZ設定を調整します。ドロップダウンリストに表示される設定は、PTZをサポートする装置のビデオチャンネルに対応しています。

[**Create (作成)**]:クリックして、設定を保存し、プロファイルを作成します。

Cancel (キャンセル):クリックして、設定をキャンセルし、すべての設定をクリアします。

profile_x:プロファイル名をクリックして、既定のプロファイルを開き、編集します。

検知器

カメラに対するいたずら

カメラに対するいたずら検知器は、レンズが覆われたり、スプレーをかけられたり、ひどいピンボケになったりしてシーンが変わり、[Trigger delay (トリガー遅延)] に設定された時間が経過したときにアラームが発生します。いたずら検知器は、カメラが10秒以上動かなかった場合にのみ作動します。この間に、映像からいたずらを比較検知するためのシーンモデルが検知器によって設定されます。シーンモデルを正しく設定するには、カメラのピントを合わせ、適切な照明状態にして、輪郭が乏しい情景 (殺風景な壁など) にカメラが向かないようにする必要があります。「カメラに対するいたずら」は、アクションを作動させる条件として使用できます。

Trigger delay (トリガー遅延):「いたずら」条件が有効になってからアラームがトリガーされるまでの最小時間を入力します。これにより、映像に影響する既知の条件に関する誤ったアラームが発せられるのを防ぐことができます。

Trigger on dark images (暗い画像でトリガー):レンズにスプレーが吹き付けられた場合にアラームを生成するのは困難です。照明の条件の変化などによって同じように映像が暗くなる場合と区別できないからです。映像が暗くなるすべての場合にアラームが発生させるには、このパラメーターをオンにします。オフにした場合は、画像が暗くなってもアラームが発生しません。

注

動きのないシーンや混雑していないシーンでのいたずら検知用。

音声検知

これらの設定は、音声入力ごとに利用できます。

Sound level (音声レベル):音声レベルは0～100の範囲で調整します。0が最も感度が高く、100が最も感度が低くなります。音声レベルの設定時には、アクティビティインジケーターをガイドとして使用します。イベントを作成する際に、音声レベルを条件として使用することができます。音声レベルが設定値より高くなった場合、低くなった場合、または設定値を通過した場合にアクションを起こすように選択できます。

衝撃検知

衝撃検知機能:オンにすると、装置が物が当たったり、いたずらされたときにアラームが生成されます。

感度レベル:スライダーを動かして、装置がアラームを生成する感度レベルを調整します。値を低くすると、衝撃が強力な場合にのみ、装置がアラームを生成します。値を大きな値に設定すると、軽いいたずらでもアラームが生成されます。

アクセサリー

I/Oポート

デジタル入力を使用すると、開回路と閉回路の切り替えが可能な外部装置 (PIRセンサー、ドアまたは窓の接触、ガラス破損検知器など) を接続できます。

デジタル出力を使用して、リレーやLEDなどの外部デバイスを接続します。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またはwebインターフェースから有効化できます。

ポート

名前:テキストを編集して、ポートの名前を変更します。

方向: は、ポートが入力ポートであることを示します。 は、出力ポートであることを示します。ポートが設定可能な場合は、アイコンをクリックして入力と出力を切り替えることができます。

標準の状態:開回路には を、閉回路には をクリックします。

現在の状態:ポートの現在のステータスを表示します。入力または出力は、現在の状態が通常の状態とは異なる場合に有効化されます。デバイスの接続が切断されているか、DC 1Vを超える電圧がかかっている場合に、デバイスの入力は開回路になります。

注

再起動中、出力回路は開かれます。再起動が完了すると、回路は正常位置に戻ります。このページの設定を変更した場合、有効なトリガーに関係なく出力回路は正常位置に戻ります。

監視済み :オンに設定すると、誰かがデジタルI/Oデバイスへの接続を改ざんした場合に、そのアクションを検出してトリガーできます。入力が開いているか閉じているかを検知するだけでなく、誰かが改ざんした場合 (つまり、切断または短絡) も検知することができます。接続を監視するには、外部I/Oループ内に追加のハードウェア (終端抵抗器) が必要です。

エッジツーエッジ

ペアリング中

ペアリングにより、互換性のあるAxisデバイスをメインデバイスの一部であるかのように使用できます。

[Audio pairing (音声ペアリング)] では、ネットワークスピーカーやマイクとペアリングすることができます。ペアリングすると、ネットワーク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。ネットワーク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) で使用するには、まずカメラをネットワークスピーカーや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。

イベントルールの [音声検知] 条件にネットワークペアリングされた音声装置を使用し、かつ [音声クリップを再生] アクションを設定している場合、イベントルールに [アクション間隔の待機 (hh:mm:ss)] 制限を設定します。この設定は、音声キャプチャーマイクがスピーカー音声を拾うことによるループ検知の回避に役立ちます。

Add (追加):ペアリングするデバイスを追加します。

(ペアリングタイプの選択):ドロップダウンリストから選択します。

Speaker pairing (スピーカーのペアリング):選択して、ネットワークスピーカーをペアリングします。

マイクのペアリング :選択して、マイクロフォンをペアリングします。

アドレス:ネットワークスピーカーのホスト名またはIPアドレスを入力します。

Username (ユーザー名):ユーザー名を入力します。

パスワード:ユーザーのパスワードを入力します。

Close (閉じる)：クリックして、すべてのフィールドをクリアします。

Connect (接続する):クリックすると、ペアリングするデバイスとの接続が確立されます。

PTZ pairing (PTZペアリング) により、レーダーをPTZカメラとペアリングしてオートトラッキングを使用できます。レーダーPTZオートトラッキングでは、PTZカメラはレーダーからの物体の位置情報に基づいて物体を追跡します。

Add (追加):ペアリングするデバイスを追加します。

(ペアリングタイプの選択):ドロップダウンリストから選択します。

アドレス:PTZカメラのホスト名またはIPアドレスを入力します。

Username (ユーザー名):PTZカメラのユーザー名を入力します。

パスワード:PTZカメラのパスワードを入力します。

Close (閉じる)：クリックして、すべてのフィールドをクリアします。

Connect (接続する):クリックして、PTZカメラへの接続を確立します。

Configure radar autotracking (レーダーオートトラッキングの設定):クリックして、オートトラッキングを開き、設定します。[Radar > Radar PTZ autotracking (レーダーPTZオートトラッキング)] に移動して設定することもできます。

ログ

レポートとログ

レポート

- View the device server report (デバイスサーバーレポートを表示):製品ステータスに関する情報をポップアップウィンドウに表示します。アクセスログは自動的にサーバーレポートに含まれます。
- Download the device server report (デバイスサーバーレポートをダウンロード):これによって、UTF-8形式で作成された完全なサーバーレポートのテキストファイルと、現在のライブビュー画像のスナップショットを収めた.zipファイルが生成されます。サポートに連絡する際には、必ずサーバーレポート .zipファイルを含めてください。
- Download the crash report (クラッシュレポートをダウンロード):サーバーの状態に関する詳細情報が付随したアーカイブをダウンロードします。クラッシュレポートには、サーバーレポートに記載されている情報と詳細なバグ情報が含まれます。レポートには、ネットワークトレースなどの機密情報が含まれている場合があります。レポートの生成には数分かかることがあります。

ログ

- View the system log (システムログを表示):装置の起動、警告、重要なメッセージなど、システムイベントに関する情報をクリックして表示します。
- View the access log (アクセスログを表示):誤ったログインパスワードの使用など、本装置への失敗したアクセスをすべてクリックして表示します。

リモートシステムログ

syslogはメッセージログ作成の標準です。これによって、メッセージを生成するソフトウェア、メッセージを保存するシステム、およびそれらを報告して分析するソフトウェアを分離することができます。各メッセージには、メッセージを生成したソフトウェアの種類を示す設備コードがラベル付けされ、重大度レベルが割り当てられます。

＋ サーバー:クリックして新規サーバーを追加します。

[ホスト]:サーバーのホスト名またはIPアドレスを入力します。

Format (形式):使用するsyslogメッセージの形式を選択します。

- Axis
- RFC 3164
- RFC 5424

Protocol (プロトコル):使用するプロトコルを選択します。

- UDP (デフォルトポートは514)
- TCP (デフォルトポートは601)
- TLS (デフォルトポートは6514)

ポート:別のポートを使用する場合は、ポート番号を編集します。

重大度:トリガー時に送信するメッセージを選択します。

CA証明書設定:現在の設定を参照するか、証明書を追加します。

プレイン設定

[Plain Config] (プレイン設定) は、Axis装置の設定経験のある上級ユーザー向けのページです。ほとんどのパラメーターは、このページから設定、編集することができます。

メンテナンス

メンテナンス

Restart (再起動):デバイスを再起動します。再起動しても、現在の設定には影響がありません。実行中のアプリケーションは自動的に再起動されます。

Restore (リストア):ほとんどの設定が工場出荷時の値に戻ります。その後、装置とアプリを再設定し、プリインストールしなかったアプリを再インストールし、イベントやプリセットを再作成する必要があります。

重要

復元後に保存される設定は以下の場合のみです。

- ブートプロトコル (DHCPまたは静的)
- 静的IPアドレス
- デフォルトのルータ
- サブネットマスク
- 802.1Xの設定
- O3C settings (O3Cの設定)
- DNSサーバーIPアドレス

Factory default (工場出荷時設定):すべての設定を工場出荷時の値に戻します。その後、装置にアクセス可能なIPアドレスをリセットする必要があります。

注

検証済みのソフトウェアのみを装置にインストールするために、すべてのAxisの装置のソフトウェアにデジタル署名が付け加えられます。これによって、Axis装置の全体的なサイバーセキュリティの最低ラインがさらに上がります。詳細については、*axis.com*でホワイトペーパー「Axis Edge Vault」を参照してください。

AXIS OS upgrade (AXIS OSのアップグレード):AXIS OSの新しいバージョンにアップグレードします。新しいリリースには、機能の改善やバグの修正、まったく新しい機能が含まれています。常にAXIS OSの最新のリリースを使用することをお勧めします。最新のリリースをダウンロードするには、*axis.com/support*に移動します。

アップグレード時には、以下の3つのオプションから選択できます。

- **Standard upgrade (標準アップグレード)**:AXIS OSの新しいバージョンにアップグレードします。
- **Factory default (工場出荷時設定)**:アップグレードすると、すべての設定が工場出荷時の値に戻ります。このオプションを選択すると、アップグレード後にAXIS OSを以前のバージョンに戻すことはできません。
- **Autorollback (オートロールバック)**:設定した時間内にアップグレードを行い、アップグレードを確認します。確認しない場合、装置はAXIS OSの以前のバージョンに戻されます。

AXIS OS rollback (AXIS OSのロールバック):AXIS OSの以前にインストールしたバージョンに戻します。

トラブルシューティング

Reset PTR (PTRのリセット) :何らかの理由で、**パン**、**チルト**、または**ロール**の設定が想定どおりに機能していない場合は、PTRをリセットします。新品のカメラの場合、PTRモーターは常にキャリブレーションされています。しかし、カメラの電源が失われたり、モーターが手で動かされたりした場合など、キャリブレーションが失われることがあります。PTRをリセットすると、カメラは再キャリブレーションされ、工場出荷時の設定の位置に戻ります。

Calibration (キャリブレーション) :[Calibrate (キャリブレート)] をクリックすると、パン、チルト、ロールモーターがデフォルト位置に再較正されます。

Ping：Pingを実行するホストのホスト名またはIPアドレスを入力して、**[開始]** をクリックすると、デバイスから特定のアドレスへの通信経路が適切に機能しているかどうかを確認することができます。

ポートチェック：チェックするホスト名またはIPアドレスとポート番号を入力して、**[開始]** をクリックすると、デバイスから特定のIPアドレスとTCP/UDPポートへの接続が可能かどうかを確認することができます。

ネットワークトレース

重要
ネットワークトレースファイルには、証明書やパスワードなどの機密情報が含まれている場合があります。

ネットワークトレースファイルはネットワーク上のアクティビティを録画するので、トラブルシューティングに役立ちます。

Trace time (追跡時間):秒または分でトレースの期間を選択し、[**ダウンロード**] をクリックします。

詳細情報

長距離接続

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

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

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

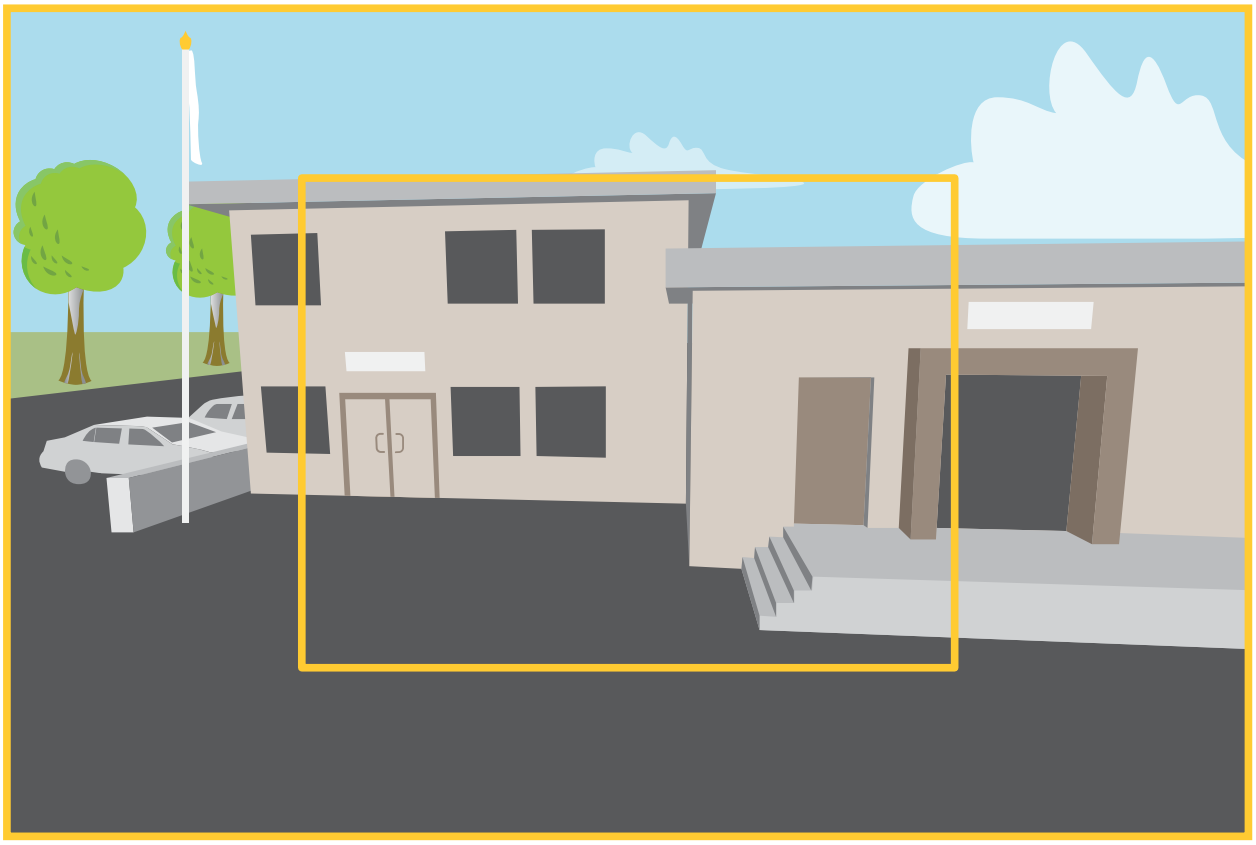
メディアコンバータの設置方法の詳細については、本製品の『インストールガイド』を参照してください。

キャプチャーモード

キャプチャーモードは、カメラが画像をキャプチャーする方法を定義するプリセット設定です。

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

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



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

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

リモートフォーカス/ズーム

リモートフォーカス/ズーム機能を使用すると、コンピューターからカメラのフォーカスとズームを調整することができます。カメラの設置場所に行かなくても、シーンのフォーカス、画角、解像度を最適化できる便利な方法です。

プライバシーマスク

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

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

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

重要

複数のプライバシーマスクを使用すると、製品のパフォーマンスに影響する場合があります。

複数のプライバシーマスクを作成できます。各マスクには3〜10個のアンカーポイントを設定できます。

オーバーレイ

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

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。

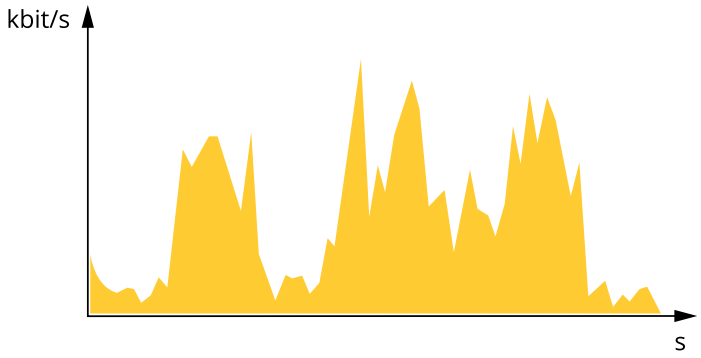
[Stream (ストリーム)] タブには、ビデオストリームの設定が含まれています。解像度やフレームレートなどを指定せずに、製品からのビデオストリームを要求している場合は、これらの設定が使用されます。[Stream (ストリーム)] タブで設定を変更すると、実行中のストリームには影響しませんが、新しいストリームを開始したときに有効になります。

[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。

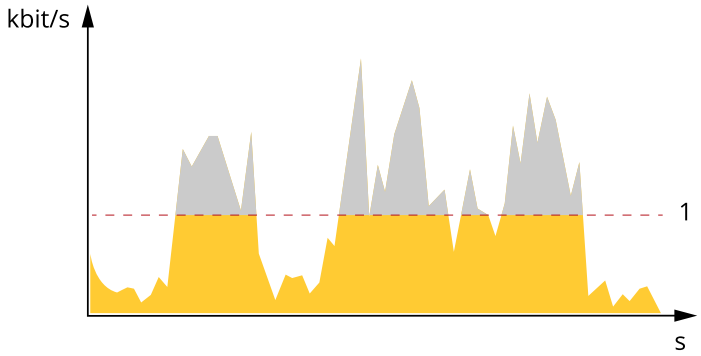
ビットレート制御

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。



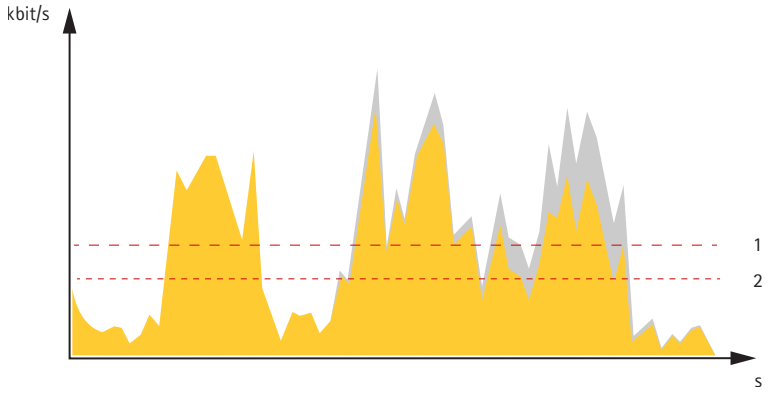
最大ビットレート（MBR）
最大ビットレートでは、目標ビットレートを設定してシステムのビットレートを制限することができます。瞬間的なビットレートが指定した目標ビットレート以下に保たれていると、画質またはフレームレートが低下することがあります。画質とフレームレートのどちらを優先するかを選択することができます。目標ビットレートは、予期されるビットレートよりも高い値に設定することをお勧めします。これにより、シーン内で活動レベルが高い場合にマージンを確保します。



1 目標ビットレート

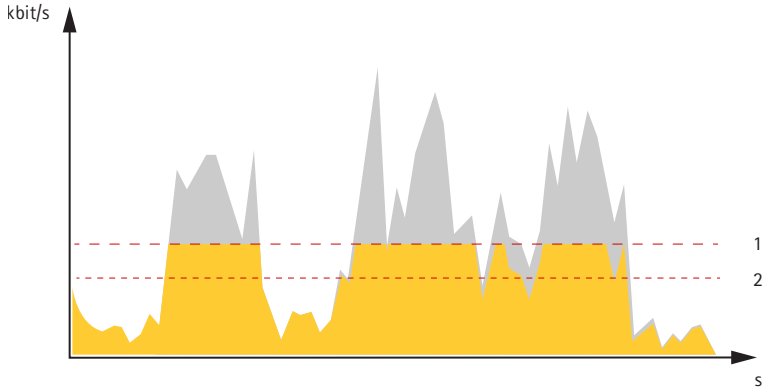
平均ビットレート（ABR）
平均ビットレートでは、より長い時間スケールにわたってビットレートが自動的に調整されます。これにより、指定した目標を達成し、使用可能なストレージに基づいて最高画質のビデオを得ることができます。動きの多いシーンでは、静的なシーンと比べてビットレートが高くなります。平均ビットレートオプションを使用すると、多くのアクティビティがあるシーンで画質が向上する可能性が高くなります。指定した目標ビットレートに合わせて画質が調整されると、指定した期間 (保存期間)、ビデオストリームを保存するために必要な総ストレージ容量を定義できます。次のいずれかの方法で、平均ビットレートの設定を指定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

- 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

アプリケーション

アプリケーションを使用することで、Axis装置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装置向けの分析アプリケーションやその他のアプリケーションの開発を可能にするオープンプラットフォームです。アプリケーションとしては、装置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アプリケーションのユーザーマニュアルについては、*help.axis.com*を参照してください。

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、各アプリケーションを組み合わせて実行できることを確認してください。

AXIS Object Analytics

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

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。

メタデータの可視化

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

サイバーセキュリティ

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

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

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。

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。

TPMモジュール

TPM (トラステッドプラットフォームモジュール) は、不正アクセスから情報を保護するための暗号化機能を提供するコンポーネントです。常に有効になっていて、変更できる設定はありません。

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。

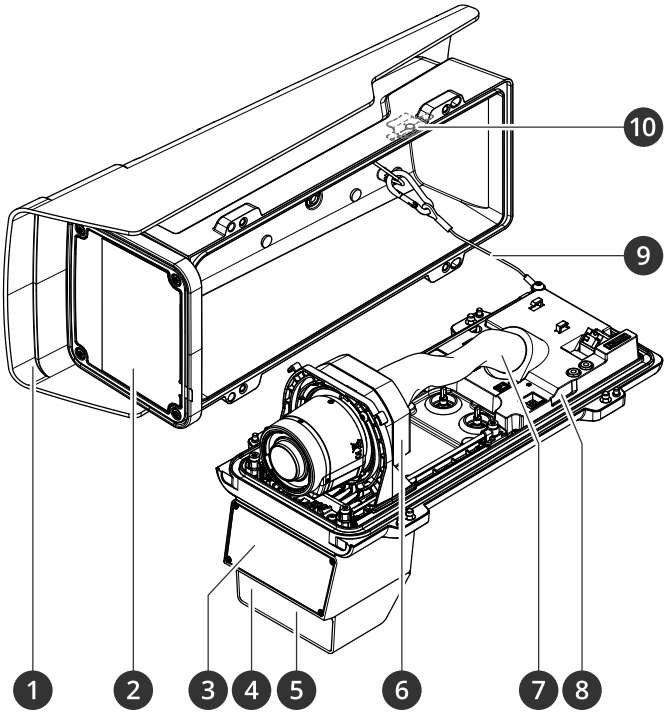
署名付きビデオ

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。

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。

仕様

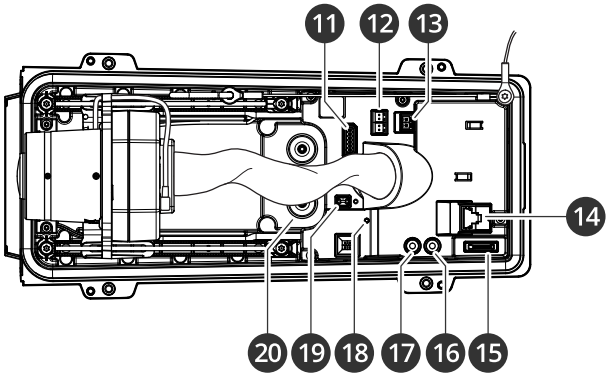
製品概要



1 ウェザーシールド
2 ウィンドウ
3 レーダー
4 光センサー
5 赤外線照明LED
6 光学ユニット
7 ケーブルカバー
8 侵入アラームセンサー
9 安全ワイヤー
10 侵入アラームマグネット

注意

ケーブルカバーを付けたまま本製品を持ち上げないでください。



1 I/Oコネクター
2 RS485/422コネクター
3 電源コネクター
4 ネットワークコネクタ (PoE)
5 microSDカードスロット
6 音声出力

7 音声入力
8 ステータスLED
9 コントロールボタン
10 ケーブルガスケットM20 (×2)

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	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。

ブザー

フォーカスアシスタントのブザー信号

注

オプションのPアイリスレンズ、DCアイリスレンズ、または手動アイリスレンズでのみ有効です。

ブザー	レンズ
短い間隔	最適に調節されています
中程度の間隔	もう少しで最適になります
長い間隔	適切に調節されていません

SDカードスロット

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。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。

侵入アラームスイッチ

侵入警告スイッチを使用して、誰かが装置のハウジングを開いたときに通知を受け取ることができます。スイッチがアクティブになったときに装置がアクションを実行するようにするためのルールを作成します。を参照してください。

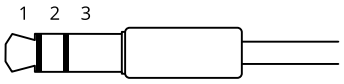
コネクター

ネットワーク コネクター

Power over Ethernet Plus (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** - 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
バランス型マイクロフォン (ファントム電源あり、なし) またはライン入力、「ホット」信号	バランス型マイクロフォン (ファントム電源あり、なし) またはライン入力、「コールド」信号	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

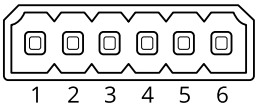
I/Oコネクターに外部装置を接続し、動体検知、イベントトリガー、アラーム通知などと組み合わせて使用することができます。I/Oコネクターは、0 VDC基準点と電力 (12 V DC出力) に加えて、以下のインターフェースを提供します。

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。

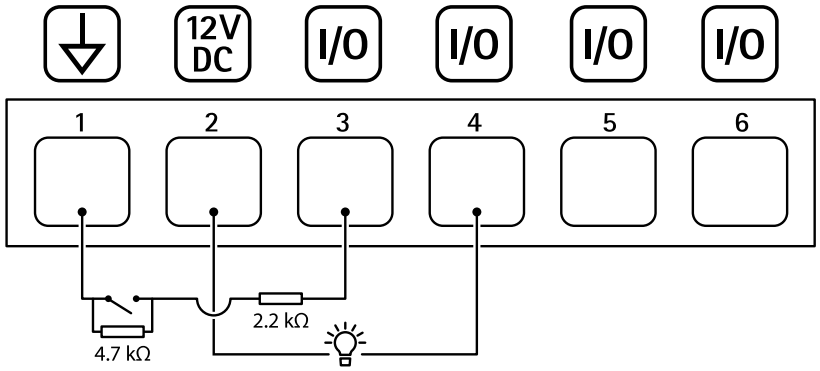
デジタル出力 - リレーやLEDなどの外部装置を接続します。接続された装置は、VAPIX®アプリケーションプログラミングインターフェースを通じたイベントまたは本装置のwebインターフェースから有効にすることができます。

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

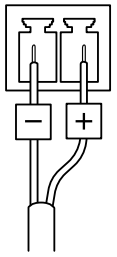
例:



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。

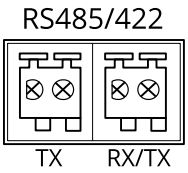


RS485/RS422コネクター

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)	

トラブルシューティング

工場出荷時の設定にリセットする

⚠警告

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

重要

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

本製品を工場出荷時の設定にリセットするには、以下の手順に従います。

1. 本製品の電源を切ります。
2. コントロールボタンを押した状態で電源を再接続します。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

- 事前設定済みの設定とカスタム設定は、装置のソフトウェアのアップグレード時に保存されます (その機能が新しいAXIS OSで利用できる場合)。ただし、この動作をAxis Communications ABが保証しているわけではありません。
- 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。

技術的な問題、ヒント、解決策

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。

AXIS OSのアップグレード時の問題

AXIS OSのアップグレードに失敗する	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

デバイスが別のサブネット上にある	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。

IPアドレスが別のデバイスで使用されている	デバイスをネットワークから切断します。pingコマンドを実行します (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)。 • `Reply from <IP address>: bytes=32; time=10...`が表示された場合は、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。 • `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アドレスが競合している可能性がある	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。

ブラウザーから装置にアクセスできない

ログインできない	HTTPSが有効になっているときは、ログインを試み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てください。場合によっては、ブラウザー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、装置を工場出荷時の設定にリセットする必要があります。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。

装置にローカルにアクセスできるが、外部からアクセスできない

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 5:30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。
- 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。

MQTTオーバSSLを使用してポート8883経由で接続できない

ファイアウォールによって、ポート8883が安全ではないと判断されたため、ポート8883を使用するトラフィックがブロックされています。	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を使用できる可能性があります。 • 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。

レーダービデオ融合の問題

境界ボックスが物体を正確にカバーしていない	ビデオ分析検知を使わない場合、カメラは画像内のレーダー検知の投影を表示しており、ビデオ分析境界ボックスほど正確ではありません。また、傾斜した道路、山、くぼみなど、シーンの高低差が原因の可能性もあります。 ボックスが高すぎるまたは低すぎる場合は、取り付け高さが正しく設定されていることを確認します。また、自動キャリブレーション機能を使用して、境界ボックスの精度を向上させることもできます。自動キャリブレーションを使用するには、[Radar > Autocalibration (レーダー > 自動キャリブレーション)] に移動します。
境界ボックスに1人が表示されているが、実際には2人いる	2人が一緒に歩いており、レーダーでのみ検知される場合、1人として分類され、境界ボックスは1つしか表示されません。分析融合ゾーンに入ると、正確に分類されます。
物体を追跡する際に境界ボックスの位置が変わる	レーダーとカメラの分析機能の両方によって同じ物体が検知される場合や、カメラの分析によってのみ物体が検知される場合、境界ボックスはカメラ情報を使用して物体の周囲にしっかりと引き寄せられます。 ビデオ検知が失われた場合、境界ボックスはレーダー投影の位置に引き寄せられ、精度が低くなります。ビデオ検知を再度選択すると、境界ボックスが正しい位置に再び描画されます。 また、自動キャリブレーション機能を使用して、境界ボックスの精度を向上させることもできます。自動キャリブレーションを使用するには、[Radar > Autocalibration (レーダー > 自動キャリブレーション)] に移動します。
マニュアルに記載されているとおりの検知距離が得られない	検知距離に影響を与える要因にはいくつかあります。 • 設定に正しい高さが入力されていることを確認してください。 • 物体が設置ポイントに近づく際の角度に応じて、検知距離が変化する場合があります。視野の外側では、レーダーの地点からの検知感度が低くなります。侵入者が最も遠くまで行ける方向に、AXIS Q1656-DLEを向けることを検討してください。

誤報を最小限に抑える方法は?	誤報を最小限に抑えるためのヒントを以下に示します。 • ビデオ分析の検知率を最大化するため、シーン内に十分な明かりを確保する • AXIS Object Analyticsで感度を [Low (低)] に設定します。この場合、アラームをトリガーする前に、ビデオとレーダーの分析が一致する必要があります。 • レーダー内の除外範囲を使用して、揺らめいている植物や建物など、既知の誤検知の発生源が無視されるようにします。 • レーダーを設定し、低感度を使用します。 • AXIS Object Analytics内で除外範囲を使用する • サイト内の草を短く保ってください。
レーダー干渉	本装置は、2つのレーダーチャンネルの片方を使用します。各チャンネル内では、最大4台のレーダーが、その周波数の使用に関する最適な方法についてネゴシエーションを行います。この機能を使用しても、カメラからの干渉に関する警告メッセージが表示される場合があります。その場合、装置ごとにチャンネルを手動で選択できます。 物理的に互いに近い装置は、同じチャンネルに設定する必要があります。これにより、装置の干渉が避けやすくなります。

パフォーマンスに関する一般的な検討事項

最も重要な検討事項には次のようなものがあります。

- 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。

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。

T10180975_ja

2025-04 (M22.2)

© 2022 – 2025 Axis Communications AB